# 3Com Switch 4200G Family

## Configuration Guide

Switch 4200G 12-Port

Switch 4200G 24-Port

Switch 4200G 48-Port

Switch 4200G PWR 24-Port

Product Version: V3.02.00
Manual Version:
6PW100-20081201
www.3com.com

**3Com Corporation**

350 Campus Drive, Marlborough,
MA, USA 01752 3064

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

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

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

**UNITED STATES GOVERNMENT LEGEND**

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

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

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

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

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

## ENVIRONMENTAL STATEMENT

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

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

Conserving energy, materials and natural resources in all operations.

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

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

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

Improving our environmental record on a continual basis.

### End of Life Statement

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

### Regulated Materials Statement

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

### Environmental Statement about the Documentation

The documentation for this product is printed on paper that comes from sustainable, managed forests; it is fully biodegradable and recyclable, and is completely chlorine-free. The varnish is environmentally-friendly, and the inks are vegetable-based with a low heavy-metal content.

# About This Manual

## Organization

*3Com Switch 4200G Family Configuration Guide* is organized as follows:

| Part | Contents |
|---|---|
| 1 Login | Introduces the ways to log into an Ethernet switch and CLI related configuration. |
| 2 Configuration File Management | Introduces configuration file and the related configuration. |
| 3 VLAN | Introduces VLAN-/Voice VLAN-related configuration. |
| 4 Static Routing | Introduces the static routing configuration. |
| 5 Voice VLAN | Introduces voice VLAN and the related configuration. |
| 6 GVRP | Introduces GVRP and the related configuration. |
| 7 Port Basic Configuration | Introduces basic port configuration. |
| 8 Link Aggregation | Introduces link aggregation and the related configuration. |
| 9 Port Isolation | Introduces port isolation and the related configuration. |
| 10 Port Security-Port Binding | Introduces port security, port binding, and the related configuration. |
| 11 MAC Address Table Management | Introduces MAC address forwarding table management. |
| 12 MSTP | Introduces STP and the related configuration. |
| 13 802.1x and System Guard | Introduces 802.1x and the related configuration. |
| 14 AAA | Introduces AAA, RADIUS, HWTACACS, EAD, and the related configurations. |
| 15 MAC Address Authentication | Introduces centralized MAC address authentication and the related configuration. |
| 16 IP Address and Performance Optimization | Introduces IP address and IP performance optimization related configuration |
| 17 ARP | Introduces ARP and the related configuration. |
| 18 DHCP | Introduces DHCP-Snooping, DHCP Client and the related configuration. |
| 19 DNS | Introduces DNS and the related configuration. |
| 20 ACL | Introduces ACL and the related configuration. |
| 21 QoS-QoS Profile | Introduces QoS and the related configuration. |
| 22 Mirroring | Introduces mirroring and the related configuration. |
| 23 Stack-Cluster | Introduces the related configuration for cluster management by using HGMP V2. |
| 24 SNMP-RMON | Introduces the configuration for network management through SNMP and RMON |
| 25 Multicast | Introduces IGMP snooping and the related configuration. |
| 26 NTP | Introduces NTP and the related configuration. |
| 27 SSH | Introduces SSH2.0 and the related configuration. |

| Part | Contents |
|---|---|
| 28 File System Management | Introduces basic configuration for file system management. |
| 29 FTP-SFTP-TFTP | Introduces basic configuration for FTP, SFTP and TFTP, and the applications. |
| 30 Information Center | Introduces information center configuration. |
| 31 System Maintenance and Debugging | Introduces daily system maintenance and debugging. |
| 32 Remote-ping | Introduces Remote-ping and the related configuration. |
| 33 PoE-PoE Profile | Introduces PoE, PoE profile and the related configuration. |
| 34 Smart Link-Monitor Link | Introduces Smart Link, Monitor Link and the related configuration. |
| 35 IPv6 Management | Introduces IPv6 and the related configuration. |
| 36 UDP Helper | Introduces UDP helper and the related configuration. |
| 37 Access Management | Introduces Access Management and the related configuration. |
| 38 Appendix | Lists the acronyms used in this manual |

## Conventions

The manual uses the following conventions:

### Command conventions

| Convention | Description |
|---|---|
| **Boldface** | The keywords of a command line are in **Boldface**. |
| *italic* | Command arguments are in *italic*. |
| [ ] | Items (keywords or arguments) in square brackets [ ] are optional. |
| { x \| y \| ... } | Alternative items are grouped in braces and separated by vertical bars. One is selected. |
| [ x \| y \| ... ] | Optional alternative items are grouped in square brackets and separated by vertical bars. One or none is selected. |
| { x \| y \| ... } * | Alternative items are grouped in braces and separated by vertical bars. A minimum of one or a maximum of all can be selected. |
| [ x \| y \| ... ] * | Optional alternative items are grouped in square brackets and separated by vertical bars. Many or none can be selected. |
| &<1-n> | The argument(s) before the ampersand (&) sign can be entered 1 to n times. |
| # | A line starting with the # sign is comments. |

### GUI conventions

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

### Symbols

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

## Related Documentation

In addition to this manual, each 3com Switch 4200G documentation set includes the following:

| Manual | Description |
|---|---|
| 3Com Switch 4200G Family Command Reference Guide | Provide detailed descriptions of command line interface (CLI) commands, that you require to manage your switch. |
| 3Com Switch 4200G Family Quick Reference Guide | Provide a summary of command line interface (CLI) commands that are required for you to manage your Stackable Switch. |
| 3Com Switch 4200G Family Getting Started Guide | This guide provides all the information you need to install and use the 3Com Switch 4200G Family. |
| 3Com Switch 4200G 10G Interface Module Installation Guide | Provide detailed descriptions of the 10G Interface Modules used by 3Com Switch 4200G Family. |
| 3Com Switch 4200G Family Release Notes | Contain the latest information about your product. If information in this guide differs from information in the release notes, use the information in the Release Notes. |

## Obtaining Documentation

You can access the most up-to-date 3Com product documentation on the World Wide Web at this URL: http://www.3com.com.

# Table of Contents

# 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

## Logging In to an Ethernet Switch

To manage or configure a Switch 4200G, you can log in to it in one of the following three methods:

- Command Line Interface
- Web-based Network Management Interface
- Network Management Station

The following table shows the configurations corresponding to each method:

| Method | Tasks |
|---|---|
| Command Line Interface | Logging In Through the Console Port |
| | Logging In Through Telnet |
| | Logging In Using a Modem |
| | CLI Configuration |
| Web-based Network Management Interface | Logging In Through the Web-based Network Management Interface |
| Network Management Station | Logging In Through NMS |

## Introduction to the User Interface

### Supported User Interfaces

**Note**

The auxiliary (AUX) port and the console port of a 3Com 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.

Switch 4200G supports 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. |

One user interface corresponds to one user interface view, where you can configure a set of parameters, such as whether to authenticate users at login and the user level after login. When the user logs in through a user interface, the connection follows these parameter settings, thus implementing centralized management of various sessions.

## Relationship Between a User and a User Interface

You can monitor and manage users logging in through different modes by setting different types of user interfaces. Switch 4200G provides one AUX user interface and five VTY user interfaces.

- A user interface does not necessarily correspond to a specific user.
- When a user logs in, the system automatically assigns the user a free user interface with the smallest number based on the user login mode. The login process of the user is restricted by the configurations under this user interface.
- The user interface assigned to a user depending on the login mode and login time.

A user interface can be used by one user at one time, however, the user interface is not dedicated to a specific user. For example, user A can use VTY 0 to log in to the device. When user A logs out, user B can use VTY 0 to log in to the device.

## 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 interface is numbered 0.
- VTY user interface indexes follow AUX user interface indexes. The first absolute VTY user interface is numbered 1, the second is 2, 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 is numbered AUX0.
- VTY user interfaces are numbered VTY0, VTY1, and so on.

## 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<br>Available in user view<br>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<br>Available in user view |
| Free a user interface | **free user-interface** [ *type* ] *number* | Optional<br>Available in user view |
| Enter system view | **system-view** | — |
| Set the banner | **header** [ **incoming** \| **legal** \| **login** \| **shell** ] *text* | Optional<br>By default, no banner is configured |
| Set a system name for the switch | **sysname** *string* | Optional |
| Enable copyright information displaying | **copyright-info enable** | Optional<br>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** [ *type* ] *first-number* [ *last-number* ] | — |
| Display the information about the current user interface/all user interfaces | **display users** [ **all** ] | Optional<br>Available in any view. |
| Display the physical attributes and configuration of the current/a specified user interface | **display user-interface** [ *type number* \| *number* ] | |
| Display the information about the current web users | **display web users** | |

# 2 Logging In Through the Console Port

Go to these sections for information you are interested in:

- Introduction
- Setting Up a Login Environment for Login 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 Switch 4200G 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.

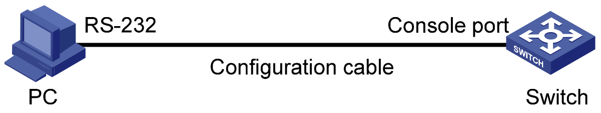
After logging in to a switch, you can perform configuration for AUX users. Refer to Console Port Login Configuration for more.

## Setting Up a Login Environment for Login Through the Console Port

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

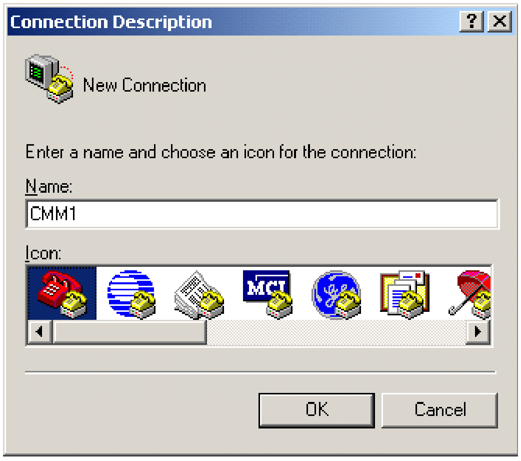
1) Connect the serial port of your PC/terminal to the console port of the switch, as shown in Figure 2-1.

**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



Connection Description

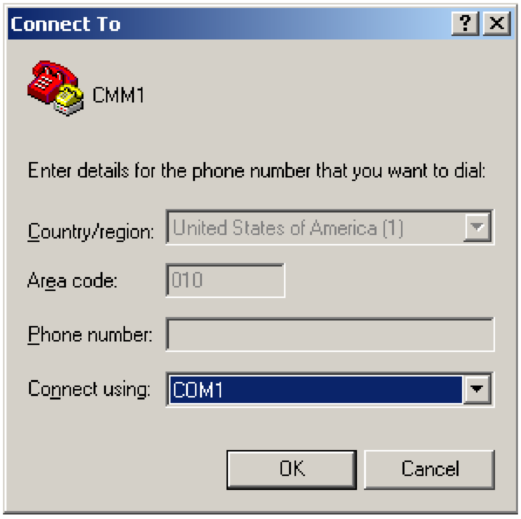
New Connection

Enter a name and choose an icon for the connection:

Name: CMM1

Icon:

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



Connect To

CMM1

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

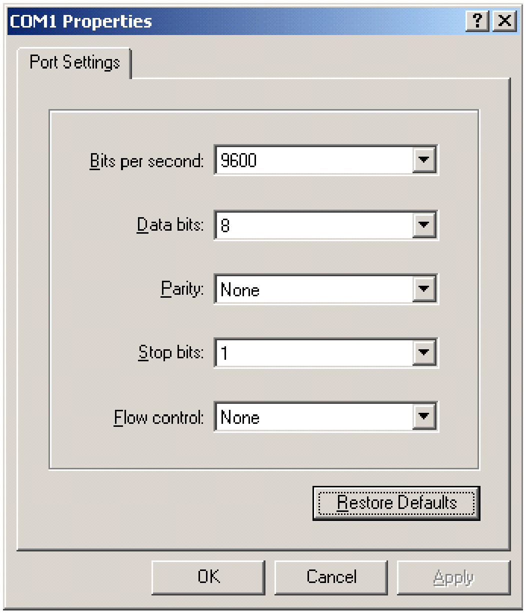
Country/region: United States of America (1)

Area code: 010

Phone number:

Connect using: COM1

**Figure 2-4** Set port parameters



Bits per second: 9600

Data bits: 8

Parity: None

Stop bits: 1

Flow control: None

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 appears after you press the Enter key.

4) You can then configure the switch or check the information about the switch by executing the corresponding commands. You can also acquire help by typing the ? character. 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<br>The default baud rate is 9,600 bps. |
| | Check mode | Optional<br>By default, the check mode of the console port is set to "none", which means no check bit. |
| | Stop bits | Optional<br>The default stop bits of a console port is 1. |
| | Data bits | Optional<br>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<br>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<br>By default, terminal services are available in all user interfaces |

| Configuration | | Remarks |
|---|---|---|
| | Set the maximum number of lines the screen can contain | Optional<br>By default, the screen can contain up to 24 lines. |
| | Set history command buffer size | Optional<br>By default, the history command buffer can contain up to 10 commands. |
| | Set the timeout time of a user interface | Optional<br>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.

Follow these steps to set common configuration of console port login:

| To do… | | Use the command… | Remarks |
|---|---|---|---|
| Enter system view | | **system-view** | — |
| Enter AUX user interface view | | **user-interface aux** 0 | — |
| Configure the console port | Set the baud rate | **speed** *speed-value* | Optional<br>The default baud rate of a console port is 9,600 bps. |
| | Set the check mode | **parity** { **even** \| **none** \| **odd** } | Optional<br>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<br>The stop bits of a console port is 1. |
| | Set the databits | **databits** { **7** \| **8** } | Optional<br>The default databits of a console port is 8. |
| Configure the command level available to users logging in to the user interface | | **user privilege level** *level* | Optional<br>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<br>By default, terminal services are available in all user interfaces. |

| To do… | Use the command… | Remarks |
|---|---|---|
| Set the maximum number of lines the screen can contain | **screen-length** *screen-length* | Optional<br>By default, the screen can contain up to 24 lines.<br>You can use the **screen-length** 0 command to disable the function to display information in pages. |
| Set the history command buffer size | **history-command max-size** *value* | Optional<br>The default history command buffer size is 10, that is, a history command buffer of a user can store up to 10 commands by default. |
| Set the timeout time for the user interface | **idle-timeout** *minutes* [ *seconds* ] | Optional<br>The default timeout time of a user interface is 10 minutes.<br>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.<br>You can use the **idle-timeout** 0 command to disable the timeout function. |

## Console Port Login Configurations for Different Authentication Modes

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

| Authentication mode | Authentication related configuration | Remarks |
|---|---|---|
| None | Set the authentication mode to none | Optional<br>Refer to Console Port Login Configuration with Authentication Mode Being None |
| Password | Set the authentication mode to local password authentication | Refer to Console Port Login Configuration with Authentication Mode Being Password. |
|  | Set the password for local authentication |  |
| Scheme | Set the authentication mode to scheme | Refer to Console Port Login Configuration with Authentication Mode Being Scheme. |
|  | Specify to perform local authentication or remote authentication |  |
|  | Set user names and passwords locally or on AAA Server |  |

**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<br>By default, users logging in through the console port (AUX user interface) are not authenticated. |

## Configuration Example

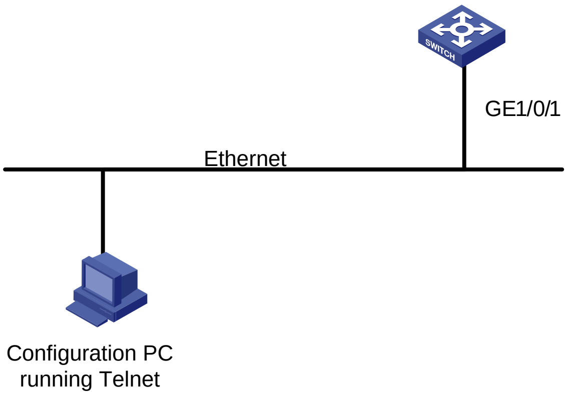
### Network requirements

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 2-5** 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<br>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 |

## Configuration Example

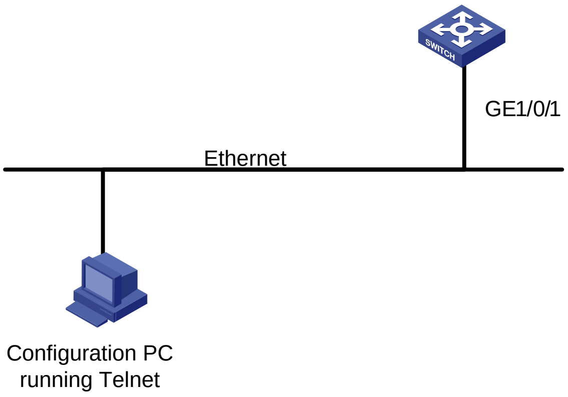
### Network requirements

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 2-6** 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** | — |
| Enter AUX user interface view | **user-interface aux** 0 | — |
| Configure to authenticate users in the scheme mode | **authentication-mode scheme** [ **command-authorization** ] | Required<br>The specified AAA scheme determines what authentication mode is adopted, local, RADIUS or HWTACACS.<br>By default, users logging in through the console port (AUX user interface) are not authenticated. |
| Quit to system view | **quit** | — |

| To do… | | Use the command… | Remarks |
|---|---|---|---|
| Configure the authentication mode | Enter the default ISP domain view | **domain** *domain-name* | Optional<br>By default, the local AAA scheme is applied.<br>If you specify to apply the local AAA scheme, you need to perform the configuration concerning local user as well.<br>If you specify to apply a RADIUS or HWTACACS scheme, you need to perform the following configuration as well:<br>• Perform RADIUS and HWTACACS configuration on the switch. (Refer to the AAA part for more.)<br>• Configure the user name and password accordingly on the AAA server. (Refer to the user manual of AAA server.) |
| | Specify the AAA scheme to be applied to the domain | **scheme** { **local** \| **none** \| **radius-scheme** *radius-scheme-name* [ **local** ] \| **hwtacacs-scheme** *hwtacacs-scheme-name* [ **local** ] } | |
| | Quit to system view | **quit** | |
| Create a local user (Enter local user view.) | | **local-user** *user-name* | Required<br>No local user exists by default. |
| Set the authentication password for the local user | | **password** { **simple** \| **cipher** } *password* | Required |
| Specify the service type for AUX users | | **service-type terminal** [ **level** *level* ] | Required |

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 AAA scheme:

- When the AAA scheme is local authentication, the command level available to users depends on the **service-type terminal** [ **level** *level* ] command.
- When the AAA scheme is RADIUS or HWTACACS authentication, you need to set the corresponding user level on the RADIUS or HWTACACS server.

**Note**

For the introduction to AAA, RADIUS, and HWTACACS, refer to the AAA part of this manual.

## Configuration Example

### Network requirements

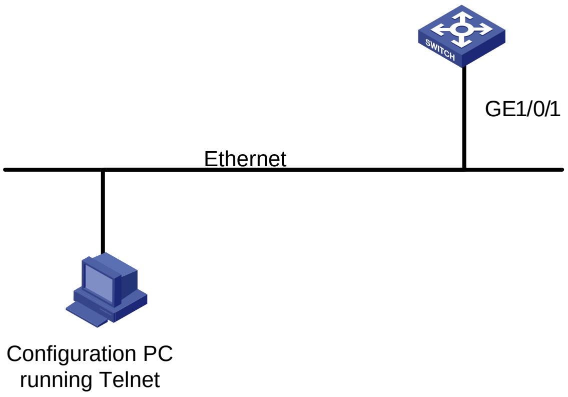
Assume the switch is configured to allow users to log in through Telnet, and the user level is set to the administrator level (level 3). Perform the following configurations for users logging in through the console port (AUX user interface).

- 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 2-7** 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

Switch 4200G supports 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 *IP Address Configuration – IP Performance Configuration* and *Routing Protocol* 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.

### 1.1.1 Common Configuration to Control Telnet Access

**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<br>By default, commands of level 0 are available to users logging in to a VTY user interface. |

| Configuration | | Description |
|---|---|---|
| | Configure the protocols the user interface supports | Optional<br>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<br>By default, no command is executed automatically after a user logs into the VTY user interface. |
| VTY terminal configuration | Make terminal services available | Optional<br>By default, terminal services are available in all user interfaces |
| | Set the maximum number of lines the screen can contain | Optional<br>By default, the screen can contain up to 24 lines. |
| | Set history command buffer size | Optional<br>By default, the history command buffer can contain up to 10 commands. |
| | Set the timeout time of a user interface | Optional<br>The default timeout time is 10 minutes. |

Follow these steps to set common telnet configuration:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter one or more VTY user interface views | **user-interface vty** *first-number* [ *last-number* ] | — |
| Configure the command level available to users logging in to VTY user interface | **user privilege level** *level* | Optional<br>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<br>By default, both Telnet protocol and SSH protocol are supported. |
| Set the commands to be executed automatically after a user logs in to the user interface successfully | **auto-execute command** *text* | Optional<br>By default, no command is executed automatically after a user logs into the VTY user interface. |
| Enable terminal services | **shell** | Optional<br>By default, terminal services are available in all user interfaces. |
| Set the maximum number of lines the screen can contain | **screen-length** *screen-length* | Optional<br>By default, the screen can contain up to 24 lines.<br>You can use the **screen-length** 0 command to disable the function to display information in pages. |

| To do… | Use the command… | Remarks |
|---|---|---|
| Set the history command buffer size | **history-command max-size** *value* | Optional<br>The default history command buffer size is 10, that is, the history command buffer of a user can store up to 10 commands by default. |
| Set the timeout time of the VTY user interface | **idle-timeout** *minutes* [ *seconds* ] | Optional<br>The default timeout time of a user interface is 10 minutes.<br>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.<br>You can use the **idle-timeout** 0 command to disable the timeout function. |

## Telnet Configurations for Different Authentication Modes

**Table 3-3** Telnet configurations for different authentication modes

| Authentication mode | Authentication related configuration | Description |
|---|---|---|
| None | Set the authentication mode to none | Refer to Console Port Login Configuration with Authentication Mode Being None. |
| Password | Set the authentication mode to local password authentication | Refer to Console Port Login Configuration with Authentication Mode Being Password. |
| | Set the password for local authentication | |
| Scheme | Set the authentication mode to scheme | Refer to Console Port Login Configuration with Authentication Mode Being Scheme. |
| | Specify to perform local authentication or remote authentication | |
| | Set user names and passwords locally or on AAA Server | |

**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** *first-number* [ *last-number* ] | — |
| Configure not to authenticate users logging in to VTY user interfaces | **authentication-mode none** | Required<br>By default, VTY users are authenticated after logging in. |

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

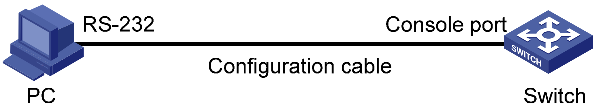
### Network requirements

Assume current user logins 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** *first-number* [ *last-number* ] | — |
| Configure to authenticate users logging in to VTY user interfaces using the local password | **authentication-mode password** | Required |
| Set the local password | **set authentication password** { **cipher** \| **simple** } *password* | Required |

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

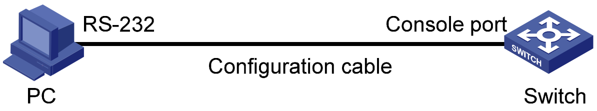
### Network requirements

Assume current user logins 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** | — |
| Enter one or more VTY user interface views | | **user-interface vty** *first-number* [ *last-number* ] | — |
| Configure to authenticate users in the scheme mode | | **authentication-mode scheme** [ **command-authorization** ] | Required<br>The specified AAA scheme determines what authentication mode is adopted, local, RADIUS or HWTACACS.<br>Users are authenticated locally by default. |
| Quit to system view | | **quit** | — |
| Configure the authentication scheme | Enter the default ISP domain view | **domain** *domain-name* | Optional<br>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.<br>If you specify to apply RADIUS or HWTACACS scheme, you need to perform the following configuration as well:<br>• Perform AAA&RADIUS configuration on the switch. (Refer to the AAA part for more.)<br>• 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** *radius-scheme-name* [ **local** ] \| **hwtacacs-scheme** *hwtacacs-scheme-name* [ **local** ] } | |
| | Quit to system view | **quit** | |
| Create a local user and enter local user view | | **local-user** *user-name* | No local user exists by default. |
| Set the authentication password for the local user | | **password** { **simple** \| **cipher** } *password* | Required |
| Specify the service type for VTY users | | **service-type telnet** [ **level** *level* ] | Required |

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 level defined in the AAA scheme.

- When the AAA scheme is local, the user level depends on the **service-type** { **ftp** | **lan-access** | { **ssh** | **telnet** | **terminal** }* [ **level** *level* ] } command.
- When the AAA scheme is RADIUS or HWTACACS, you need to specify the user level of a user on the corresponding RADIUS or HWTACACS server.

Note

Refer to the *AAA* part of this manual for information about AAA, RADIUS, and HWTACACS.

# Configuration Example

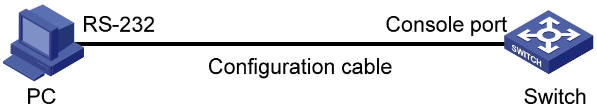
## Network requirements

Assume current user logins 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
```

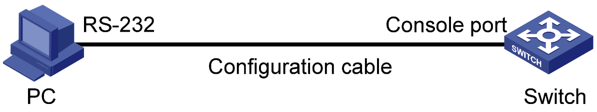
# Telnetting to a Switch

## 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



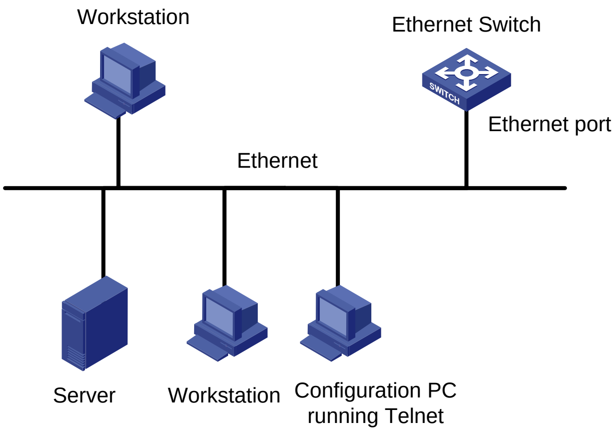
- Launch a terminal emulation utility (such as Terminal in Windows 3.X or HyperTerminal in Windows 95/Windows 98/Windows NT/Windows 2000/Windows XP) on the PC terminal, with the baud rate set to 9,600 bps, data bits set to 8, parity check set to none, and flow control set to none.
- Turn on the switch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

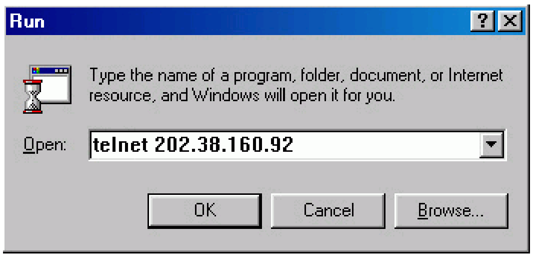
3) Connect your PC/terminal and the Switch to an Ethernet, as shown in Figure 3-5. Make sure the port through which the switch is connected to the Ethernet belongs to VLAN 1 and the route between your PC and VLAN-interface 1 is reachable.

**Figure 3-5** 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 3-6.

**Figure 3-6** Launch Telnet


Run
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
Open:
OK
Cancel
Browse...

```
telnet 202.38.160.92
```

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 3Com 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**

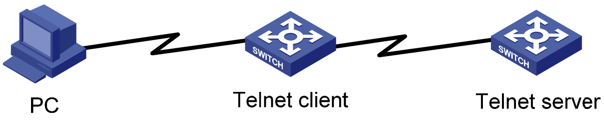
- A Telnet connection is terminated if you delete or modify the IP address of the VLAN interface in the Telnet session.
- By default, commands of level 0 are available to Telnet users authenticated by password. Refer to the CLI part for information about command hierarchy.

## 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 3-7, 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 3-7** Network diagram for Telnetting to another switch from the current switch



1) 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.
2) Telnet to the switch operating as the Telnet client.
3) 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.

1) 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!”.
2) 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.

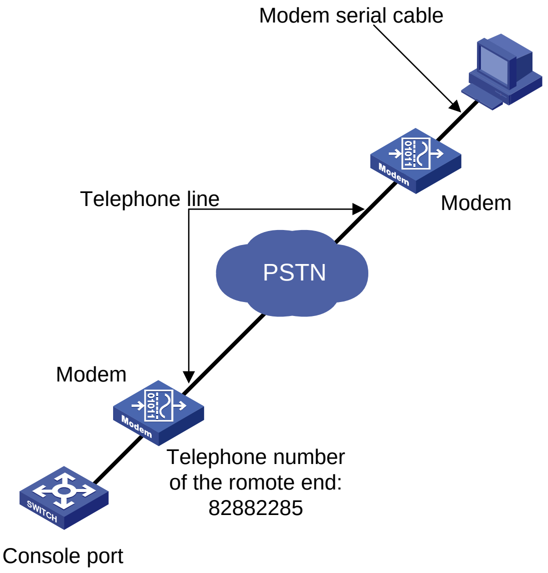
### Configuration on switch when the authentication mode is scheme

Refer to Console Port Login Configuration with Authentication Mode Being Scheme.

# Modem Connection Establishment

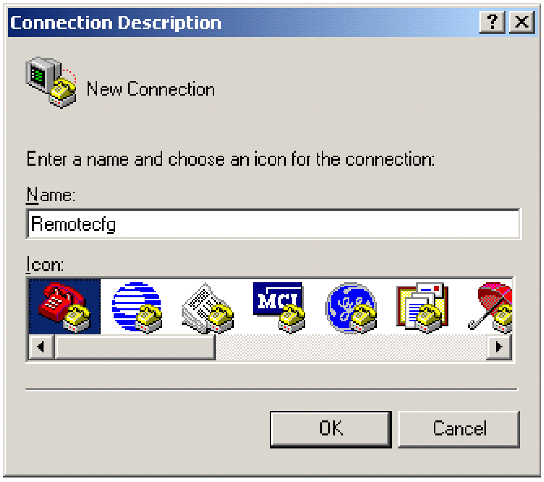
1) Before using Modem to log in the switch, perform corresponding configuration for different authentication modes on the switch. Refer to Console Port Login Configuration with Authentication Mode Being None, Console Port Login Configuration with Authentication Mode Being Password, and Console Port Login 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

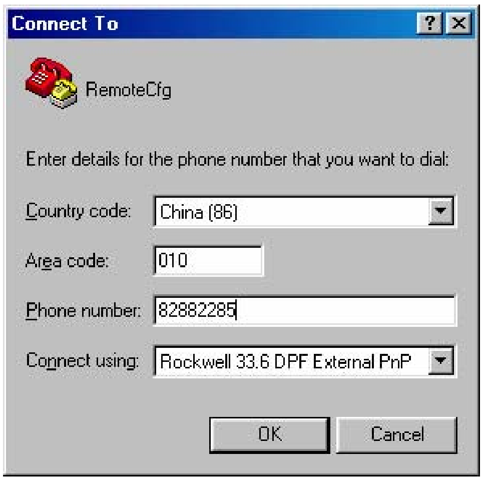


Enter a name and choose an icon for the connection:

Name:

Remotecfg

**Figure 4-3** Set the telephone number



Connect To

RemoteCfg

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

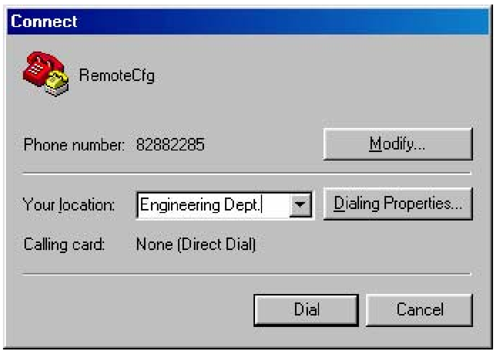
Country code: China (86)

Area code: 010

Phone number: 82882285

Connect using: Rockwell 33.6 DPF External PnP

**Figure 4-4** Call the modem



Connect

RemoteCfg

Phone number: 82882285

Your location: Engineering Dept.

Calling card: None (Direct Dial)

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 CLI Configuration

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

## Introduction to the CLI

A command line interface (CLI) is a user interface to interact with a switch. Through the CLI on a switch, a user can enter commands to configure the switch and check output information to verify the configuration. Each 3com switch 4200G provides an easy-to-use CLI and a set of configuration commands for the convenience of the user to configure and manage the switch.

The CLI on the 3com switch 4200G provides the following features, and so has good manageability and operability.

- Hierarchical command protection: After users of different levels log in, they can only use commands at their own, or lower, levels. This prevents users from using unauthorized commands to configure switches.
- Online help: Users can gain online help at any time by entering a question mark (?).
- Debugging: Abundant and detailed debugging information is provided to help users diagnose and locate network problems.
- Command history function: This enables users to check the commands that they have lately executed and re-execute the commands.
- Partial matching of commands: The system will use partially matching method to search for commands. This allows users to execute a command by entering partially-spelled command keywords as long as the keywords entered can be uniquely identified by the system.

## Command Hierarchy

### Command Level and User Privilege Level

To restrict the different users' access to the device, the system manages the login users and all the commands by their privilege levels.

All the commands and login users are categorized into four levels, which are visit, monitor, system, and manage from low to high, and identified respectively by 0 through 3. After users at different privilege levels log in, they can only use commands at their own, or lower, levels. For example, level 2 users can only use level 0 through level 2 commands, not level 3 commands.

#### Command level

Based on user privilege, commands are classified into four levels, which default to:

- Visit level (level 0): Commands at this level are mainly used to diagnose network, and they cannot be saved in configuration file. For example, **ping**, **tracert** and **telnet** are level 0 commands.

- Monitor level (level 1): Commands at this level are mainly used to maintain the system and diagnose service faults, and they cannot be saved in configuration file. Such commands include **debugging** and **terminal**.
- System level (level 2): Commands at this level are mainly used to configure services. Commands concerning routing and network layers are at this level. These commands can be used to provide network services directly.
- Manage level (level 3): Commands at this level are associated with the basic operation modules and support modules of the system. These commands provide support for services. Commands concerning file system, FTP/TFTP/XModem downloading, user management, and level setting are at this level.

By using the **command-privilege level** command, the administrator can change the level of a command in a specific view as required. For details, refer to Modifying the Command Level.

### User privilege level

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

By default, the Console user (a user who logs into the switch through the Console port) is a level-3 user and can use commands of level 0 through level 3, while Telnet users are level-0 users and can only use commands of level 0.

You can use the **user privilege level** command to set the default user privilege level for users logging in through a certain user interface. For details, refer to *Login Operation*.

**Note**

If a user logs in using AAA authentication, the user privilege level depends on the configuration of the AAA scheme. For details, refer to *AAA Operation*.

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 details, refer to Switching User Level.

## Modifying the Command Level

### Modifying the Command Level

All the commands in a view are defaulted to different levels, as shown in Command level. The administrator can modify the command level based on users' needs to make users of a lower level use commands with a higher level or improve device security.

Follow these steps to set the level of a command in a specific view:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |

| To do… | Use the command… | Remarks |
|---|---|---|
| Configure the level of a command in a specific view | **command-privilege level** *level* **view** *view command* | Required |

⚠ **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.

### 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.

## 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** [ *type* ] *first-number* [ *last-number* ] | — |
| Specify the authentication mode for user level switching | Super password authentication | **super authentication-mode super-password** | Optional<br>These configurations will take effect on the current user interface only.<br>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** [ **level** *level* ] { **cipher** \| **simple** } *password* | Required<br>The configuration will take effect on all user interfaces.<br>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** *domain-name* | — |
| Set the HWTACACS authentication scheme for user level switching | **authentication super hwtacacs-scheme** *hwtacacs-scheme-name* | Required<br>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<br>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.

1) 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
```

2) 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
```

## CLI Views

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 5-1 lists the CLI views provided by the 3com switch 4200G, operations that can be performed in different CLI views and the commands used to enter specific CLI views.

**Table 5-1** 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. |
| Ethernet port view | Configure Ethernet port parameters | 1000 Mbps Ethernet port view:<br>[Sysname-GigabitEthernet1/0/1] | Execute the **interface gigabitethernet** command in system view. | Execute the **quit** command to return to system view.<br>Execute the **return** command to return to user view. |
| | | 10 Gigabit Ethernet port view:<br>[Sysname-TenGigabitEthernet1/1/1] | Execute the **interface tengigabitethernet** command in system view. | |
| Aux1/0/0 port (the console port) view | The 3com switch 4200G does 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. | |

| View | Available operation | Prompt example | Enter method | Quit method |
|---|---|---|---|---|
| User interface view | Configure user interface parameters | [Sysname-ui-aux 0] | 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. | |
| Cluster view | Configure cluster parameters | [Sysname-cluster] | Execute the **cluster** 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] | | |
| 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 **quit** command to return to system view.<br>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. | |
| 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-aaa123.net] | Execute the **domain** command in system view. | |

| View | Available operation | Prompt example | Enter method | Quit method |
|---|---|---|---|---|
| Remote-ping test group view | Configure remote-ping test group parameters | [Sysname-remote-ping-a123-a123] | Execute the **remote-ping** command in system view. | |
| HWTACACS view | Configure HWTACACS parameters | [Sysname-hwtacacs-a123] | Execute the **hwtacacs scheme** 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. | |

**Note**

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

# CLI Features

## Online Help

When configuring the switch, you can use the online help to get related help information. The CLI provides two types of online help: complete and partial.

### Complete online help

1) Enter a question mark (?) in any view on your terminal to display all the commands available in the view and their brief descriptions. The following takes user view as an example.

```
<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
```

<Other information is omitted>

2) Enter a command, a space, and a question mark (?).

If the question mark "?" is at a keyword position in the command, all available keywords at the position and their descriptions will be displayed on your terminal.

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

If the question mark "?" is at an argument position in the command, the description of the argument will be displayed on your terminal.

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

If only <cr> is displayed after you enter "?", it means no parameter is available at the "?" position, and you can enter and execute the command directly.

```
[Sysname] interface vlan-interface 1 ?
  <cr>
```

### Partial online help

1) Enter a character/string, and then a question mark (?) next to it. All the commands beginning with the character/string will be displayed on your terminal. For example:

```
<Sysname> p?
   ping
   pwd
```

2) Enter a command, a space, a character/string and a question mark (?) next to it. All the keywords beginning with the character/string (if available) are displayed on your terminal. For example:

```
<Sysname> display v?
   version
   vlan
   voice
```

3) Enter the first several characters of a keyword of a command and then press <Tab>. If there is a unique keyword beginning with the characters just typed, the unique keyword is displayed in its complete form. If there are multiple keywords beginning with the characters, you can have them displayed one by one (in complete form) by pressing <Tab> repeatedly.

## Terminal Display

The CLI provides the screen splitting feature to have display output suspended when the screen is full. When display output pauses, you can perform the following operations as needed (see Table 5-2).

**Table 5-2** Display-related operations

| Operation | Function |
|---|---|
| Press <Ctrl+C> | Stop the display output and execution of the command. |
| Press any character except <Space>, <Enter>, /, +, and - when the display output pauses | Stop the display output. |
| Press the space key | Get to the next page. |

| Operation | Function |
|---|---|
| Press <Enter> | Get to the next line. |

## Command History

The CLI provides the command history function. You can use the **display history-command** command to view a specific number of latest executed commands and execute them again in a convenient way. By default, the CLI can store up to 10 latest executed commands for each user. You can view the command history by performing the operations listed in the following table:

Follow these steps to view history commands:

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

**Note**

- The Windows 9x HyperTerminal explains the up and down arrow keys in a different way, and therefore the two keys are invalid when you access history commands in such an environment. However, you can use <Ctrl+ P> and <Ctrl+ N> instead to achieve the same purpose.
- When you enter the same command multiple times consecutively, only one history command entry is created by the command line interface.

## Error Prompts

If a command passes the syntax check, it will be successfully executed; otherwise, an error message will be displayed. Table 5-3 lists the common error messages.

**Table 5-3** Common error messages

| Error message | Remarks |
|---|---|
| Unrecognized command | The command does not exist. |
| | The keyword does not exist. |
| | The parameter type is wrong. |
| | The parameter value is out of range. |
| Incomplete command | The command entered is incomplete. |
| Too many parameters | The parameters entered are too many. |
| Ambiguous command | The parameters entered are ambiguous. |

| Error message | Remarks |
|---|---|
| Wrong parameter | A parameter entered is wrong. |
| found at '^' position | An error is found at the '^' position. |

## Command Edit

The CLI provides basic command edit functions and supports multi-line editing. The maximum number of characters a command can contain is 254. Table 5-4 lists the CLI edit operations.

**Table 5-4** Edit operations

| Press… | To… |
|---|---|
| A common key | Insert the corresponding character at the cursor position and move the cursor one character to the right if the command is shorter than 254 characters. |
| Backspace key | Delete the character on the left of the cursor and move the cursor one character to the left. |
| Left arrow key or <Ctrl+B> | Move the cursor one character to the left. |
| Right arrow key or <Ctrl+F> | Move the cursor one character to the right. |
| Up arrow key or <Ctrl+P><br>Down arrow key or <Ctrl+N> | Display history commands. |
| <Tab> | Use the partial online help. That is, when you input an incomplete keyword and press <Tab>, if the input parameter uniquely identifies a complete keyword, the system substitutes the complete keyword for the input parameter; if more than one keywords match the input parameter, you can display them one by one (in complete form) by pressing <Tab> repeatedly; if no keyword matches the input parameter, the system displays your original input on a new line without any change. |

# 6 Logging In Through the Web-based Network Management Interface

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

Switch 4200G has a Web server built in. It enables you to log in to Switch 4200G through a Web browser and then manage and maintain the switch intuitively by interacting with the built-in Web server.

To log in to Switch 4200G through the built-in Web-based network management interface, you need to perform the related configuration on both the switch and the PC operating as the network management terminal.

**Table 6-1** 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 *IP Address Configuration – IP Performance Configuration* and *Routing Protocol* 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.

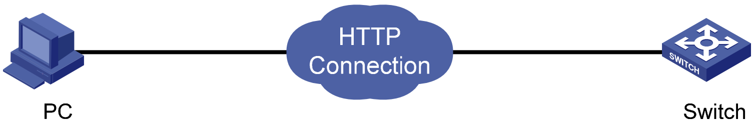
2) Configure the user name and the password on the switch for the Web network management user to log in.

# 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 6-1.

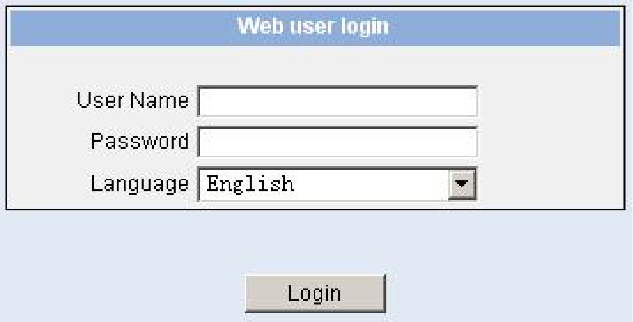
**Figure 6-1** Establish an HTTP connection between your PC and the switch



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 6-2) 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 6-2** The login page of the Web-based network management system



# 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<br>By default, no login banner is configured. |

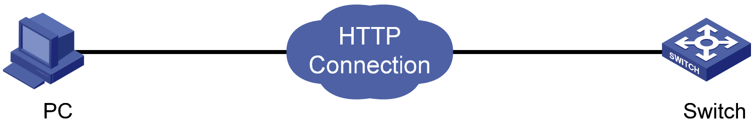
## Configuration Example

### 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 6-3** Network diagram for login banner configuration



### Configuration Procedure

# Enter system view.

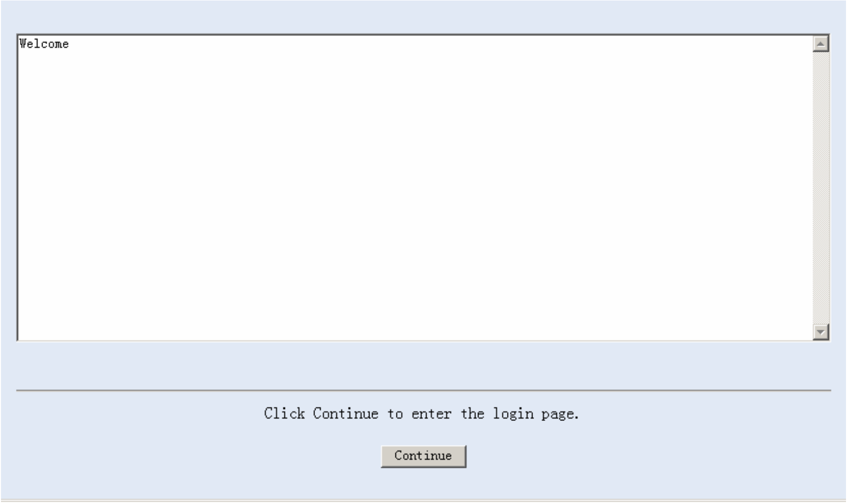
```
<Sysname> system-view
```

# 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 6-4.

**Figure 6-4** Banner page displayed when a user logs in to the switch through Web



Welcome

Click Continue to enter the login page.

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<br>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.

# 7 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 software 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.

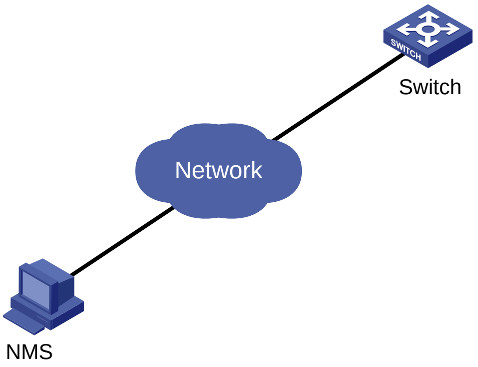
To log in to a switch through an NMS, you need to perform related configuration on both the NMS and the switch.

**Table 7-1** 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 *IP Address Configuration – IP Performance Configuration* and *Routing Protocol* parts for related information.) |
|  | The basic SNMP functions are configured. (Refer to the *SNMP-RMON* 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 7-1** Network diagram for logging in through an NMS



# 8 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 source IP address or source interface for the Telnet server and Telnet client. This provides a way to manage services and enhances security.

The source IP address specified for Telnet service packets is the IP address of an Loopback interface or VLAN interface. After you specify the IP address of a virtual Loopback interface or an unused VLAN interface as the source IP address of Telnet service packets, the IP address is used as the source IP address no matter which interface of the switch is used to transmit packets between the Telnet client and the Telnet server. This conceals the IP address of the actual interface used. As a result, external attacks are guarded and the security is improved. On the other hand, you can configure the Telnet server to accept only Telnet service packets with specific source IP addresses to make sure specific users can log into the switch.

## Configuring Source IP Address for Telnet Service Packets

This feature can be configured in either user view or system view. The configuration performed in user view takes effect for only the current session, while the configuration performed in system view takes effect for all the following sessions.

### Configuration in user view

**Table 8-1** Configure a source IP address for service packets in user view

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

### Configuration in system view

**Table 8-2** Configure a source IP address for service packets in system view

| Operation | Command | Description |
|---|---|---|
| Specify a source IP address for Telnet server | **telnet-server source-ip** *ip-address* | Optional |

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

**Note**

To perform the configurations listed in Table 8-1 and Table 8-2, make sure that:

- The IP address specified is that of the local device.
- The interface specified exists.
- If a source IP address (or source interface) is specified, you need to make sure that the route between the IP addresses (or interface) of both sides is reachable.

# Displaying Source IP Address Configuration

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

**Table 8-3** Display the source IP address configuration

| Operation | Command | Description |
|---|---|---|
| Display the source IP address configured for the Telnet client | **display telnet source-ip** | You can execute the two commands in any view. |
| Display the source IP address configured for the Telnet server | **display telnet-server source-ip** | |

# 9 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 9-1.

**Table 9-1** 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 and destination IP address | Through advanced ACL |  |
|  | By source MAC address | Through Layer 2 ACL |  |
| 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 | Logging Out a Web User |

## Controlling Telnet Users

### Introduction

The controlling policy against Telnet users' access to VTY user interfaces is determined by referencing ACL. For the introduction to ACL, refer to the *ACL* part of this manual.

- If no ACL is configured on the VTY user interface, users are not controlled when establishing a Telnet connection using this user interface.
- If an ACL is configured on the VTY user interface, there will be two possibilities: if the packets for establishing a Telnet connection match the ACL rule configured on the VTY user interface, the connection will be permitted or denied according to the ACL rule; if not, the connection will be denied directly.

## Controlling Telnet Users by ACL

Controlling Telnet users by ACL is achieved by the following two ways:

- **inbound**: Applies the ACL to the users Telnetting to the local switch through the VTY user interface.
- **outbound**: Applies the ACL to the users Telnetting to other devices through the current user interface. This keyword is unavailable to Layer 2 ACLs.

You can configure the following three types of ACLs as needed:

**Table 9-2** ACL categories

| Category | ACL number | Matching criteria |
|---|---|---|
| Basic ACL | 2000 to 2999 | Source IP address |
| Advanced ACL | 3000 to 3999 | Source IP address and destination IP address |
| Layer 2 ACL | 4000 to 4999 | Source MAC address |

**Note**

Source and destination in this manual refer to a Telnet client and a Telnet server respectively.

- If the **inbound** keyword is specified, the Telnet client is the user telnetting to the local switch and the Telnet server is the local switch.
- If the **outbound** keyword is specified, the Telnet client is the local switch, and the Telnet server is another device to which the user is telnetting.

Follow these steps to control Telnet users by ACL:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Create a basic ACL or enter basic ACL view | **acl number** *acl-number* [ **match-order** { **auto** \| **config** } ] | As for the **acl number** command, the **config** keyword is specified by default. |
| Define rules for the ACL | **rule** [ *rule-id* ] { **deny \| permit** } [ *rule-string* ] | Required |
| Quit to system view | **quit** | — |
| Enter user interface view | **user-interface** [ *type* ] *first-number* [ *last-number* ] | — |

| To do… | | Use the command… | Remarks |
|---|---|---|---|
| Apply an ACL to control Telnet users by ACL | Apply a basic or advanced ACL to control Telnet users | **acl** *acl-number* { **inbound** \| **outbound** } | Required<br>Use either command<br>• The **inbound** keyword specifies to filter the users trying to Telnet to the current switch.<br>• The **outbound** keyword specifies to filter users trying to Telnet to other switches from the current switch. |
| | Apply a Layer 2 ACL to control Telnet users | **acl** *acl-number* **inbound** | |

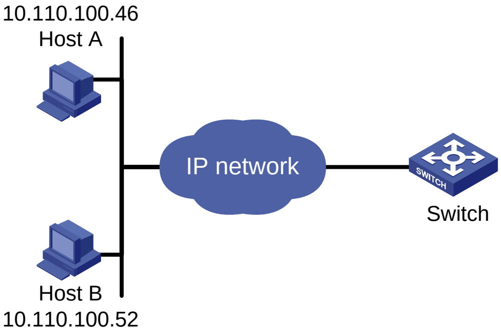
## Configuration Example

### 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 9-1** 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 Switch 4200G 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

To control whether an NMS can manage the switch, you can use this function.

## 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** *acl-number* [ **match-order** { **auto** \| **config** } ] | As for the **acl number** command, the **config** keyword is specified by default. |
| Define rules for the ACL | **rule** [ *rule-id* ] { **deny** \| **permit** } [ *rule-string* ] | Required |
| Quit to system view | **quit** | — |
| Apply the ACL while configuring the SNMP community name | **snmp-agent community** { **read** \| **write** } *community-name* [ **acl** *acl-number* \| **mib-view** *view-name* ]* | Required<br>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 *SNMP-RMON* for more. |
| Apply the ACL while configuring the SNMP group name | **snmp-agent group** { **v1** \| **v2c** } *group-name* [ **read-view** *read-view* ] [ **write-view** *write-view* ] [ **notify-view** *notify-view* ] [ **acl** *acl-number* ]<br>**snmp-agent group v3** *group-name* [ **authentication** \| **privacy** ] [ **read-view** *read-view* ] [ **write-view** *write-view* ] [ **notify-view** *notify-view* ] [ **acl** *acl-number* ] | |
| Apply the ACL while configuring the SNMP user name | **snmp-agent usm-user** { **v1** \| **v2c** } *user-name group-name* [ **acl** *acl-number* ]<br>**snmp-agent usm-user v3** *user-name group-name* [ [ **cipher** ] **authentication-mode** { **md5** \| **sha** } *auth-password* [ **privacy-mode** { **des56** \| **aes128** } *priv-password* ] ] [ **acl** *acl-number* ] | |

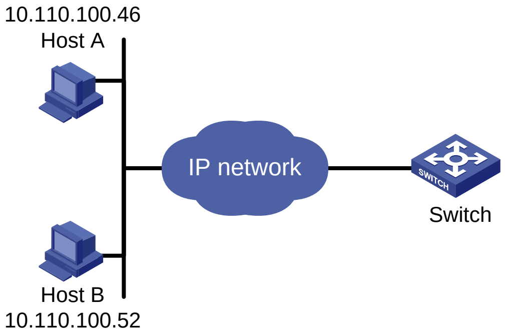
## Configuration Example

### 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 9-2** 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 Switch 4200G 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

To control whether a Web user can manage the switch, you can use this function.

## 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** *acl-number* [ **match-order** { **config** \| **auto** } ] | As for the **acl number** command, the **config** keyword is specified by default. |
| Define rules for the ACL | **rule** [ *rule-id* ] { **deny \| permit** } [ *rule-string* ] | Required |
| Quit to system view | **quit** | — |
| Apply the ACL to control Web users | **ip http acl** *acl-number* | Optional<br>By default, no ACL is applied for Web users. |

## Logging Out a Web User

The administrator can log out a Web user using the related command.

Follow the step below to log out a Web user:

| To do… | Use the command… | Remarks |
|---|---|---|
| Log out a Web user | **free web-users** { **all** \| **user-id** *user-id* \| **user-name** *user-name* } | Required<br>Available in user view |

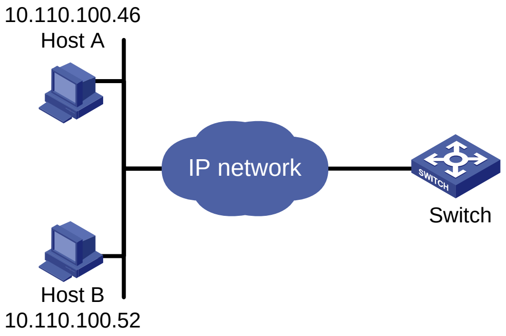
## Configuration Example

### 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 9-3** 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
```

# Table of Contents

# 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.

# 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** [ *cfgfile* \| [ **safely** ] [ **backup** \| **main** ] ] | Required<br>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.
- 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<br>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** *cfgfile* [ **backup** \| **main** ] | Required<br>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** *unit-id* ] [ **by-linenum** ] | Available in any view. |
| Display the configuration file used for this and next startup | **display startup** [ **unit** *unit-id* ] | |
| Display the current VLAN configuration of the switch | **display current-configuration vlan** [ *vlan-id* ] [ **by-linenum** ] | |
| Display the validated configuration in current view | **display this** [ **by-linenum** ] | |
| Display current configuration | **display current-configuration** [ **configuration** [ *configuration-type* ] \| **interface** [ *interface-type* ] [ *interface-number* ] ] [ **by-linenum** ] [ **\|** { **begin** \| **exclude** \| **include** } *regular-expression* ] | |

# Table of Contents

# 1 VLAN Overview

This chapter covers these topics:

- VLAN Overview
- Port-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. A switch builds a table of MAC addresses mapped to associated ports with that address and only sends a known MAC's traffic to one port. 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.
- Related to the point above, someone on a network can monitor broadcast packets and unicast packets and learn of other activities on the network. Then they can attempt to access other resources on the network, whether or not they are authorized to do this.

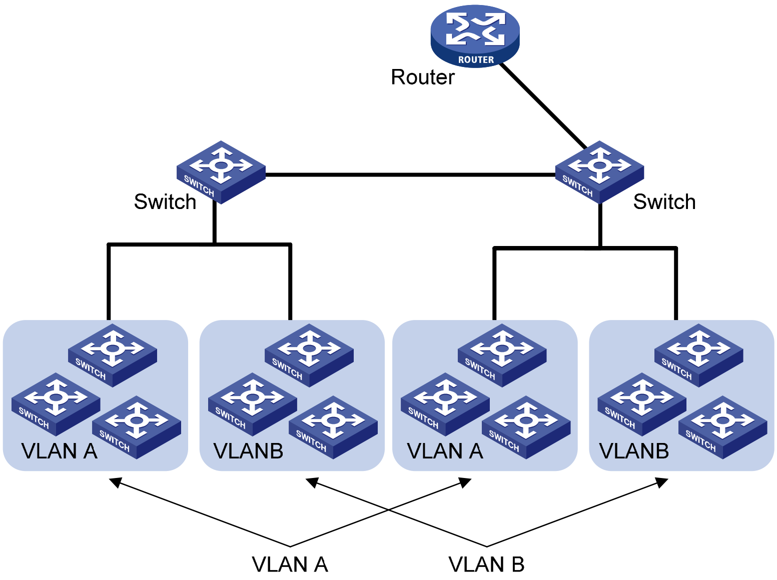
Isolating broadcast domains is the solution for the above problems. The traditional way is to use routers, which forward packets according to the destination IP address and does not forward broadcast packets in the link layer. However, routers are expensive and provide few ports, so they cannot split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

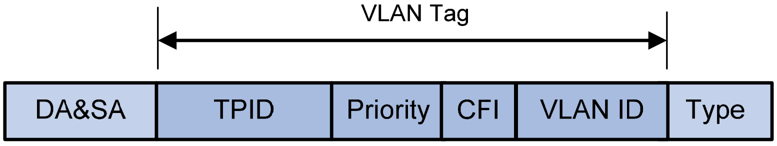
In the header of a traditional Ethernet data frame, the field after the destination MAC address and the source MAC address (DA&SA) is the Type field indicating the upper layer protocol type, as shown in Figure 1-2.

**Figure 1-2** Encapsulation format of traditional Ethernet frames

| | | |
|---|---|---|
| DA&SA | Type | Data |

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 Switch 4200G 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" 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.

**Note**

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.

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 make forwarding decisions based on destination MAC addresses. For this purpose, each switch maintains a MAC address table, of which each entry records the MAC address of a terminal connected to the switch and to which port this terminal is connected, assuming that no VLAN is involved. For the ease of management, a MAC learning mechanism is adopted on switches. With this mechanism, a switch can populate its MAC address table automatically by learning the source MAC address of incoming traffic and on which port the traffic is received. When forwarding traffic destined for the learned MAC address, the switch looks up the table and forwards the traffic according to the entry.

After VLANs are configured, a switch adopts one of the following MAC address learning mechanisms:

- Shared VLAN learning (SVL), where the switch records all learned MAC address entries in one MAC address table, regardless of in which VLAN they are learned. This table is called the shared MAC address forwarding table. Packets received in any VLAN on a port are forwarded according to this table.

- Independent VLAN learning (IVL), where the switch maintains an independent MAC address forwarding table for each VLAN. The source MAC address of a packet received in a VLAN on a port is recorded to the MAC address forwarding table of this VLAN only, and packets received in a VLAN are forwarded according to the MAC address forwarding table for the VLAN.

Currently, the Switch 4200G 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 Switch 4200G 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 Switch 4200G series switches support the port-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

You can configure the link type of a port as access, trunk, or hybrid. The three link types use different VLAN tag handling methods. When configuring the link type of a port, note that:

- An access port can belong to only one VLAN. Usually, ports directly connected to PCs are configured as access ports.
- A trunk port can carry multiple VLANs to receive and send traffic for them. Except traffic of the default VLAN, traffic passes through a trunk port will be VLAN tagged. Usually, ports connecting network devices are configured as trunk ports to allow members of the same VLAN to communicate with each other across multiple network devices.
- Like a trunk port, a hybrid port can carry multiple VLANs to receive and send traffic for them. Unlike a trunk port, a hybrid port allows traffic of all VLANs to pass through VLAN untagged. You can configure a port connected to a network device or user terminal as a hybrid port for access link connectivity or trunk connectivity.

**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.<br>● 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.<br>● 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.<br>● 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.<br>● 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.<br>● 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.<br>● 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). |

# 2 VLAN Configuration

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

- VLAN Configuration
- Configuring a Port-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** { *vlan-id1* **to** *vlan-id2* \| **all** } | Optional |
| Create a VLAN and enter VLAN view | **vlan** *vlan-id* | Required<br>By default, there is only one VLAN, that is, the default VLAN (VLAN 1). |
| Assign a name for the current VLAN | **name** *text* | Optional<br>By default, the name of a VLAN is its VLAN ID. **VLAN 0001** for example. |
| Specify the description string of the current VLAN | **description** *text* | Optional<br>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** *vlan-id* | Required<br>By default, there is no VLAN interface on a switch. |
| Specify the description string for the current VLAN interface | **description** *text* | Optional<br>By default, the description string of a VLAN interface is the name of this VLAN interface. **Vlan-interface1 Interface** for example. |

| To do... | Use the command... | Remarks |
|---|---|---|
| Disable the VLAN interface | **shutdown** | Optional<br>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).<br>If you disable the VLAN interface, the VLAN interface will always be down, regardless of the status of the ports in the VLAN. |
| Enable the VLAN Interface | **undo shutdown** | |

**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** [ *vlan-id* ] | Available in any view. |
| Display the VLAN information | **display vlan** [ *vlan-id* [ **to** *vlan-id* ] \| **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** *interface-type interface-number* | — |
| Configure the port link type | **port link-type** { **access** \| **hybrid** \| **trunk** } | Required<br>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.

## 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** *interface-type interface-number* | — |
| Assign the port to one or multiple VLANs | Access port | **port access vlan** *vlan-id* | Optional<br>By default, all Ethernet ports belong to VLAN 1. |
| | Trunk port | **port trunk permit vlan** { *vlan-id-list* \| **all** } | |
| | Hybrid port | **port hybrid vlan** *vlan-id-list* { **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** *vlan-id* | Required<br>If the specified VLAN does not exist, this command creates the VLAN first. |

| To do… | Use the command… | Remarks |
|---|---|---|
| Assign the specified access port or ports to the current VLAN | **port** *interface-list* | Required<br>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** *interface-type interface-number* | — |
| Configure the default VLAN for the port | Trunk port | **port trunk pvid vlan** *vlan-id* | Optional<br>VLAN 1 is the default VLAN by default. |
| | Hybrid port | **port hybrid pvid vlan** *vlan-id* | |

**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

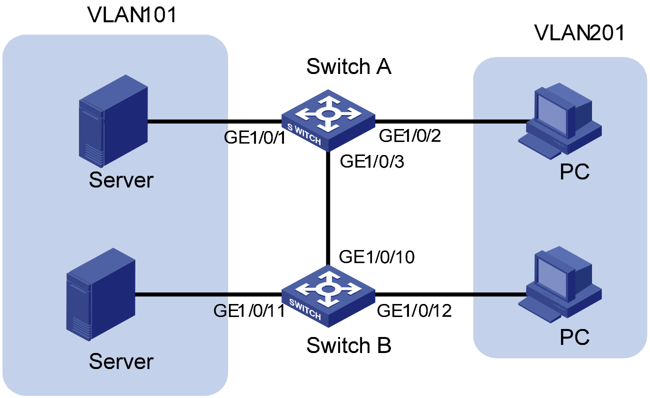
### Network requirements

- As shown in Figure 2-1, Switch A and Switch B each connect to a server and a workstation (PC).
- For data security concerns, the two servers are assigned to VLAN 101 with the descriptive string being “DMZ”, and the PCs are assigned to VLAN 201.

- The devices within each VLAN can communicate with each other but that in different VLANs cannot communicate with each other directly.

## Network diagram

**Figure 2-1** Network diagram for VLAN configuration



## Configuration procedure

- Configure Switch A.

# Create VLAN 101, specify its descriptive string as “DMZ”, and add GigabitEthernet1/0/1 to VLAN 101.

```
<SwitchA> system-view
[SwitchA] vlan 101
[SwitchA-vlan101] description DMZ
[SwitchA-vlan101] port GigabitEthernet 1/0/1
[SwitchA-vlan101] quit
```

# Create VLAN 201, and add GigabitEthernet1/0/2 to VLAN 201.

```
[SwitchA] vlan 201
[SwitchA-vlan201] port GigabitEthernet 1/0/2
[SwitchA-vlan201] quit
```

- Configure Switch B.

# Create VLAN 101, specify its descriptive string as “DMZ”, and add GigabitEthernet1/0/11 to VLAN 101.

```
<SwitchB> system-view
[SwitchB] vlan 101
[SwitchB-vlan101] description DMZ
[SwitchB-vlan101] port GigabitEthernet 1/0/11
[SwitchB-vlan101] quit
```

# Create VLAN 201, and add GigabitEthernet1/0/12 to VLAN 201.

```
[SwitchB] vlan 201
[SwitchB-vlan201] port GigabitEthernet 1/0/12
[SwitchB-vlan201] quit
```

- Configure the link between Switch A and Switch B.

Because the link between Switch A and Switch B need to transmit data of both VLAN 101 and VLAN 102, you can configure the ports at the end of the link as trunk ports and permit packets of the two VLANs to pass through.

# Configure GigabitEthernet1/0/3 of Switch A.

```
[SwitchA] interface GigabitEthernet 1/0/3
[SwitchA-GigabitEthernet1/0/3] port link-type trunk
[SwitchA-GigabitEthernet1/0/3] port trunk permit vlan 101
[SwitchA-GigabitEthernet1/0/3] port trunk permit vlan 201
```

# Configure GigabitEthernet1/0/10 of Switch B.

```
[SwitchB] interface GigabitEthernet 1/0/10
[SwitchB-GigabitEthernet1/0/10] port link-type trunk
[SwitchB-GigabitEthernet1/0/10] port trunk permit vlan 101
[SwitchB-GigabitEthernet1/0/10] port trunk permit vlan 201
```

# Table of Contents

# 1 Static Routing Configuration

## Introduction

### Routing Table

#### Routing table

Routing tables play a key role in routing. Each router maintains a routing table, and each entry in the table specifies which physical interface a packet destined for a certain destination should go out to reach the next hop or the directly connected destination.

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.

#### Contents of a routing table

A routing table includes the following key items:

- Destination address: Destination IP address or destination network.
- Network mask: Specifies, in company with the destination address, the address of the destination network. A logical AND operation between the destination address and the network mask yields the address of the destination network. For example, if the destination address is 129.102.8.10 and the mask 255.255.0.0, the address of the destination network is 129.102.0.0. A network mask is made of a certain number of consecutive 1s. It can be expressed in dotted decimal format or by the number of the 1s.
- Outbound interface: Specifies the interface through which the IP packets are to be forwarded.
- IP address of the next hop: Specifies the address of the next router on the path.
- Priority for the route. Routes to the same destination but having different nexthops may have different priorities and be found by various routing protocols or manually configured. The optimal route is the one with the highest priority (with the smallest metric).

Routes can be divided into two categories by destination:

- Subnet routes: The destination is a subnet.
- Host routes: The destination is a host.

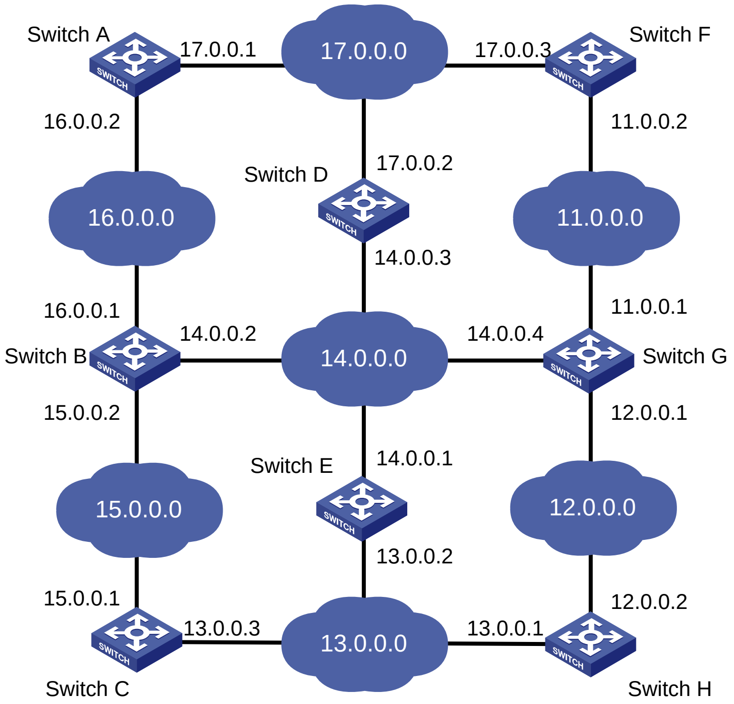
Based on whether the destination is directly connected to a given router, routes can be divided into:

- Direct routes: The destination is directly connected to the router.
- Indirect routes: The destination is not directly connected to the router.

To prevent the routing table from getting too large, you can configure a default route. All packets without matching any entry in the routing table will be forwarded through the default route.

In Figure 1-1, the IP address on each cloud represents the address of the network. Switch G is connected to three networks and therefore has three IP addresses for its three physical interfaces. Its routing table is shown under the network topology.

**Figure 1-1** A sample routing table



| Destination Network | Nexthop | Interface |
|---|---|---|
| 11.0.0.0 | 11.0.0.1 | 2 |
| 12.0.0.0 | 12.0.0.1 | 1 |
| 13.0.0.0 | 12.0.0.2 | 1 |
| 14.0.0.0 | 14.0.0.4 | 3 |
| 15.0.0.0 | 14.0.0.2 | 3 |
| 16.0.0.0 | 14.0.0.2 | 3 |
| 17.0.0.0 | 11.0.0.2 | 2 |

## Static Route

A static route is a manually configured. If a network's topology is simple, you only need to configure static routes for the network to work normally. The proper configuration and usage of static routes can improve network performance and ensure bandwidth for important network applications.

The disadvantage of using static routes is that they cannot adapt to network topology changes. If a fault or a topological change occurs in the network, the routes will be unreachable and the network breaks. In this case, the network administrator has to modify the static routes manually.

## Default Route

If the destination address of a packet fails to match any entry in the routing table, the packet will be discarded.

After a default route is configured on a switch, any packet whose destination IP address matches no entry in the routing table can be forwarded to a designated upstream switch.

A switch selects the default route only when it cannot find any matching entry in the routing table.

- If the destination address of a packet fails to match any entry in the routing table, the switch selects the default route to forward the packet.

- If there is no default route and the destination address of the packet fails to match any entry in the routing table, the packet will be discarded and an ICMP packet will be sent to the source to report that the destination or the network is unreachable.

The network administrator can configure a default route with both destination and mask being 0.0.0.0. The router forwards any packet whose destination address fails to match any entry in the routing table to the next hop of the default static route.

# 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** *ip-address* { *mask* \| *mask-length* } { *interface-type interface-number* \| *next-hop* } [ **preference** *preference-value* ] [ **reject** \| **blackhole** ] [ **description** *text* ] | Required |

# Displaying and Maintaining a Routing Table

| To do… | Use the command… | Remarks |
|---|---|---|
| Display summary information about the routing table | **display ip routing-table** [ **\|** { **begin** \| **exclude** \| **include** } *regular-expression* ] | Optional<br>Available in any view. |
| Display detailed information about the routing table | **display ip routing-table verbose** | |
| Display the routes leading to a specified IP address | **display ip routing-table** *ip-address* [ *mask* ] [ **longer-match** ] [ **verbose** ] | |
| Display the routes leading to a specified IP address range | **display ip routing-table** *ip-address1 mask1 ip-address2 mask2* [ **verbose** ] | |
| Display the routing information of the specified protocol | **display ip routing-table protocol** *protocol* [ **inactive** \| **verbose** ] | |
| Display the routes that match a specified basic access control list (ACL) | **display ip routing-table acl** *acl-number* [ **verbose** ] | |
| Display the routes that match a specified IP prefix | **display ip routing-table ip-prefix** *ip-prefix-name* [ **verbose** ] | |
| Display the routing table in a tree structure | **display ip routing-table radix** | |

| To do… | Use the command… | Remarks |
|---|---|---|
| Display the statistics on the routing table | **display ip routing-table statistics** | |
| Clear statistics about a routing table | **reset ip routing-table statistics protocol** { **all** \| *protocol* } | Use the **reset** command in user view |
| Delete all static routes | **delete static-routes all** | Use the **delete** command in system view. |

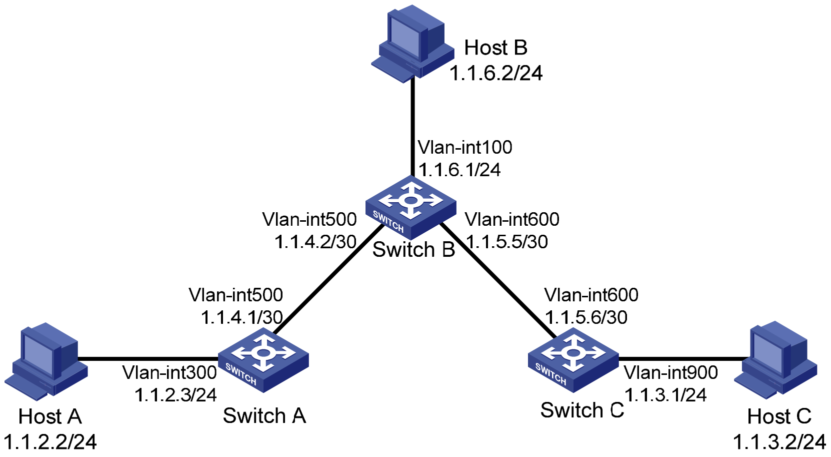
# Static Route Configuration Example

## Basic Static Route Configuration Example

### Network requirements

The IP addresses and masks of the switches and hosts are shown in the following figure. Static routes are required for interconnection between any two hosts.

**Figure 1-2** Network diagram for static route configuration



### Configuration procedure

1) Configuring IP addresses for interfaces (omitted)
2) Configuring static routes

# Configure a default route on Switch A.

```
<SwitchA> system-view
[SwitchA] ip route-static 0.0.0.0 0.0.0.0 1.1.4.2
```

# Configure two static routes on Switch B.

```
<SwitchB> system-view
[SwitchB] ip route-static 1.1.2.0 255.255.255.0 1.1.4.1
[SwitchB] ip route-static 1.1.3.0 255.255.255.0 1.1.5.6
```

# Configure a default route on Switch C

```
<SwitchC> system-view
[SwitchC] ip route-static 0.0.0.0 0.0.0.0 1.1.5.5
```

3) Configure the hosts.

The default gateways for the three hosts A, B and C are 1.1.2.3, 1.1.6.1 and 1.1.3.1 respectively. The configuration procedure is omitted.

4) Display the configuration.

# Display the IP routing table of Switch A.

```
[SwitchA] display ip routing-table
 Routing Table: public net
Destination/Mask    Protocol  Pre  Cost         Nexthop         Interface
0.0.0.0/0           STATIC    60   0            1.1.4.2         Vlan-interface500
1.1.2.0/24          DIRECT    0    0            1.1.2.3         Vlan-interface300
1.1.2.3/32          DIRECT    0    0            127.0.0.1       InLoopBack0
1.1.4.0/30          DIRECT    0    0            1.1.4.1         Vlan-interface500
1.1.4.1/32          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
```

# Display the IP routing table of Switch B.

```
[SwitchB] display ip routing-table
 Routing Table: public net
Destination/Mask    Protocol  Pre  Cost         Nexthop         Interface
1.1.2.0/24          STATIC    60   0            1.1.4.1         Vlan-interface500
1.1.3.0/24          STATIC    60   0            1.1.5.6         Vlan-interface600
1.1.4.0/30          DIRECT    0    0            1.1.4.2         Vlan-interface500
1.1.4.2/32          DIRECT    0    0            127.0.0.1       InLoopBack0
1.1.5.4/30          DIRECT    0    0            1.1.5.5         Vlan-interface600
1.1.5.5/32          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
1.1.6.0/24          DIRECT    0    0            192.168.1.47    Vlan-interface100
1.1.6.1/32          DIRECT    0    0            127.0.0.1       InLoopBack0
```

# Table of Contents

# 1 Voice VLAN Configuration

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 and prioritization 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**

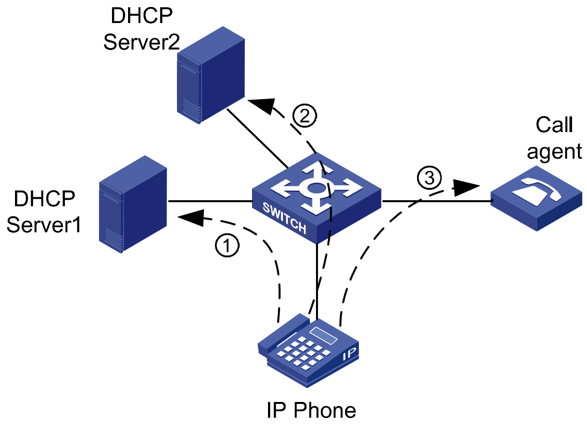
The following part only describes the common way for an IP phone to acquire an IP address. The detailed process may vary by manufacture. Refer to the corresponding user manual for the detailed information.

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

Following describes the way a typical 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 Switch 4200G Series Switches Identify Voice Traffic

Switch 4200G 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. Switch 4200G 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 Switch 4200G 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 the transmission quality of voice traffic, the switch re-marks the precedence of the traffic in the voice VLAN as follows:

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

**Note**

For more information about CoS and DSCP precedence values, refer to the QoS part of the manual.

## 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 Switch 4200G 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<br>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<br>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 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<br>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<br>Make sure the default VLAN of the port exists and is not a voice VLAN, the traffic of the default VLAN is permitted to pass through the port, and the voice VLAN is in the list of the tagged VLANs whose traffic is permitted by the port. |
| | Untagged voice traffic | Access | Supported<br>Make sure the default VLAN of the port is a voice VLAN. |
| | | Trunk | Supported<br>Make sure the default VLAN of the port is a voice VLAN and the port permits the traffic of the VLAN. |
| | | Hybrid | Supported<br>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<br>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<br>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<br>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<br>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

The automatic mode and manual mode described earlier only apply to the process of assigning a port to the voice VLAN. After a port is assigned to the voice VLAN, the switch receives and forwards all voice VLAN-tagged traffic without matching the source MAC address of each received packet against its OUI list. For a port in the manual mode with the default VLAN as the voice VLAN, any untagged packet can be transmitted in the voice VLAN. This makes the voice VLAN vulnerable to flow attacks, because malicious users can create a large amount of voice VLAN-tagged packets to consume the voice VLAN bandwidth, affecting normal voice communication.

Switch 4200G series switches provide the security mode for voice VLAN to address this problem. When the voice VLAN works in security mode, the switch checks the source MAC address of each packet to enter the voice VLAN and drops the packets whose source MAC addresses do not match the OUI list. However, checking packets occupies lots of system resources. Therefore, in a relatively safe network, you can configure the voice VLAN to operate in normal mode.

The following table presents how a packet is handled when the voice VLAN is operating in security mode and normal mode.

**Table 1-4** How a packet is handled when the voice VLAN is operating in different modes

| Voice VLAN Mode | Packet Type | Processing Method |
|---|---|---|
| Security | Untagged packet | If the source MAC address of the packet matches the OUI list, the packet is transmitted in the voice VLAN. Otherwise, the packet is dropped. |
| | Packet carrying the voice VLAN tag | |
| | Packet carrying any other VLAN tag | The packet is forwarded or dropped based on whether the receiving port is assigned to the carried VLAN. The processing method is irrelevant to the voice VLAN mode (security or normal). |
| Normal | Untagged packet | The source MAC address of the packet is not checked. All such packets can be transmitted in the voice VLAN. |
| | Packet carrying the voice VLAN tag | |
| | Packet carrying any other VLAN tag | The packet is forwarded or dropped based on whether the port is assigned to the carried VLAN. The processing method is irrelevant to the voice VLAN mode (security or normal). |

# 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 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** *oui* **mask** *oui-mask* [ **description** *text* ] | Optional<br>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<br>By default, the voice VLAN security mode is enabled. |

| To do… | Use the command… | Remarks |
|---|---|---|
| Set the voice VLAN aging timer | **voice vlan aging** *minutes* | Optional<br>The default aging timer is 1440 minutes. |
| Enable the voice VLAN function globally | **voice vlan** *vlan-id* **enable** | Required |
| Enter Ethernet port view | **interface** *interface-type interface-number* | Required |
| Enable the voice VLAN function on a port | **voice vlan enable** | Required<br>By default, voice VLAN is disabled. |
| Enable the voice VLAN legacy function on the port | **voice vlan legacy** | Optional<br>By default, voice VLAN legacy is disabled. |
| Set the voice VLAN assignment mode of the port to automatic | **voice vlan mode auto** | Optional<br>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, 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 of the voice VLAN but does so immediately after the restart.

## 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:

<table>
<tr><th colspan="3">To do…</th><th>Use the command…</th><th>Remarks</th></tr>
<tr><td colspan="3">Enter system view</td><td>**system-view**</td><td>—</td></tr>
<tr><td colspan="3">Set an OUI address that can be identified by the voice VLAN</td><td>**voice vlan mac-address** *oui* **mask** *oui-mask* [ **description** *text* ]</td><td>Optional<br>Without this address, the default OUI address is used.</td></tr>
<tr><td colspan="3">Enable the voice VLAN security mode</td><td>**voice vlan security enable**</td><td>Optional<br>By default, the voice VLAN security mode is enabled.</td></tr>
<tr><td colspan="3">Set the voice VLAN aging timer</td><td>**voice vlan aging** *minutes*</td><td>Optional<br>The default aging timer is 1,440 minutes.</td></tr>
<tr><td colspan="3">Enable the voice VLAN function globally</td><td>**voice vlan** *vlan-id* **enable**</td><td>Required</td></tr>
<tr><td colspan="3">Enter port view</td><td>**interface** *interface-type interface-number*</td><td>Required</td></tr>
<tr><td colspan="3">Enable voice VLAN on a port</td><td>**voice vlan enable**</td><td>Required<br>By default, voice VLAN is disabled on a port.</td></tr>
<tr><td colspan="3">Enable the voice VLAN legacy function on the port</td><td>**voice vlan legacy**</td><td>Optional<br>By default, voice VLAN legacy is disabled.</td></tr>
<tr><td colspan="3">Set voice VLAN assignment mode on a port to manual</td><td>**undo voice vlan mode auto**</td><td>Required<br>The default voice VLAN assignment mode on a port is automatic.</td></tr>
<tr><td colspan="3">Quit to system view</td><td>**quit**</td><td>—</td></tr>
<tr><td rowspan="5">Add a port in manual voice VLAN assignment mode to the voice VLAN</td><td rowspan="2">Access port</td><td>Enter VLAN view</td><td>**vlan** *vlan-id*</td><td rowspan="4">Required<br>By default, all the ports belong to VLAN 1.</td></tr>
<tr><td>Add the port to the VLAN</td><td>**port** *interface-list*</td></tr>
<tr><td rowspan="3">Trunk or Hybrid port</td><td>Enter port view</td><td>**interface** *interface-type interface-num*</td></tr>
<tr><td>Add the port to the VLAN</td><td>**port trunk permit vlan** *vlan-id*<br>**port hybrid vlan** *vlan-id* { **tagged** \| **untagged** }</td></tr>
<tr><td>Configure the voice VLAN to be the default VLAN of the port</td><td>**port trunk pvid vlan** *vlan-id*<br>**port hybrid pvid vlan** *vlan-id*</td><td>Optional<br>Refer to Table 1-2 to determine whether or not this operation is needed.</td></tr>
</table>

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 3Com 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** *vlan-id* | |

# Voice VLAN Configuration Example

## Voice VLAN Configuration Example (Automatic Mode)

### Network requirements

As shown in Figure 1-2,

- The MAC address of IP phone A is 0011-1100-0001. The phone connects to a downstream device named PC A whose MAC address is 0022-1100-0002 and to GigabitEthernet 1/0/1 on an upstream device named Device A.
- The MAC address of IP phone B is 0011-2200-0001. The phone connects to a downstream device named PC B whose MAC address is 0022-2200-0002 and to Ethernet GigabitEthernet1/0/2 on Device A.
- Device A uses voice VLAN 2 to transmit voice packets for IP phone A and IP phone B.
- Configure GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 to work in automatic voice VLAN assignment mode. In addition, if one of them has not received any voice packet in 30 minutes, the port is removed from the corresponding voice VLAN automatically.

### Network diagram

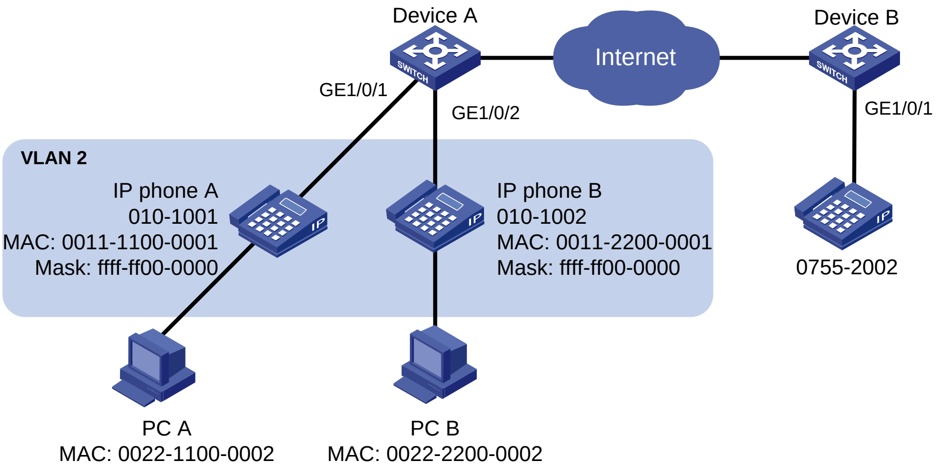


**Figure 1-2** Network diagram for voice VLAN configuration (automatic mode)

### Configuration procedure

# Create VLAN 2.

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

# Set the voice VLAN aging time to 30 minutes.

```
[DeviceA] voice vlan aging 30
```

# Configure VLAN 2 as a voice VLAN.

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

# Since GigabitEthernet 1/0/1 may receive both voice traffic and data traffic at the same time, to ensure the quality of voice packets and effective bandwidth use, configure voice VLANs to work in security mode, that is, configure the voice VLANs to transmit only voice packets. (Optional. By default, voice VLANs work in security mode.)

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

# Configure the allowed OUI addresses as MAC addresses prefixed by 0011-1100-0000 or 0011-2200-0000. In this way, Device A identifies packets whose MAC addresses match any of the configured OUI addresses as voice packets.

```
[DeviceA] voice vlan mac-address 0011-1100-0001 mask ffff-ff00-0000 description IP phone A
[DeviceA] voice vlan mac-address 0011-2200-0001 mask ffff-ff00-0000 description IP phone B
```

# Configure GigabitEthernet 1/0/1 to operate in automatic voice VLAN assignment mode. (Optional. By default, a port operates in automatic voice VLAN assignment mode.)

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] voice vlan mode auto
```

# Configure GigabitEthernet 1/0/1 as a hybrid port.

```
[DeviceA-GigabitEthernet1/0/1] port link-type hybrid
```

# Configure VLAN 2 as the voice VLAN for GigabitEthernet 1/0/1.

```
[DeviceA-GigabitEthernet1/0/1] voice vlan enable
[DeviceA-GigabitEthernet1/0/1] quit
```

# Configure GigabitEthernet 1/0/2.

```
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] voice vlan mode auto
[DeviceA-GigabitEthernet1/0/2] port link-type hybrid
[DeviceA-GigabitEthernet1/0/2] voice vlan enable
```

## Verification

# Display the OUI addresses, OUI address masks, and description strings supported currently.

```
<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
0011-1100-0000  ffff-ff00-0000  IP phone A
0011-2200-0000  ffff-ff00-0000  IP phone B
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 current states of voice VLANs.

```
<DeviceA> display voice vlan state
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
-------------------------------------
GigabitEthernet1/0/1           AUTO
GigabitEthernet1/0/2           AUTO
```

# Voice VLAN Configuration Example (Manual Mode)

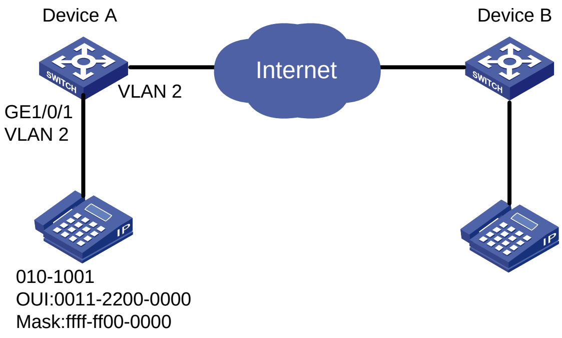
## Network requirements

Create a voice VLAN and configure it to operate in manual 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 GigabitEthernet 1/0/1, a hybrid port. Set this port to operates in manual 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 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 GigabitEthernet 1/0/1 to operate in manual mode.

```
[DeviceA] interface GigabitEthernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] undo voice vlan mode auto
```

# Configure GigabitEthernet 1/0/1 as a hybrid port.

```
[DeviceA-GigabitEthernet1/0/1] port link-type hybrid
```

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

```
[DeviceA-GigabitEthernet1/0/1] port hybrid pvid vlan 2
[DeviceA-GigabitEthernet1/0/1] port hybrid vlan 2 untagged
```

# Enable the voice VLAN function on GigabitEthernet 1/0/1.

```
[DeviceA-GigabitEthernet1/0/1] 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
--------------------------------
GigabitEthernet1/0/1     MANUAL
```

# Table of Contents

# 1 GVRP Configuration

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

## 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

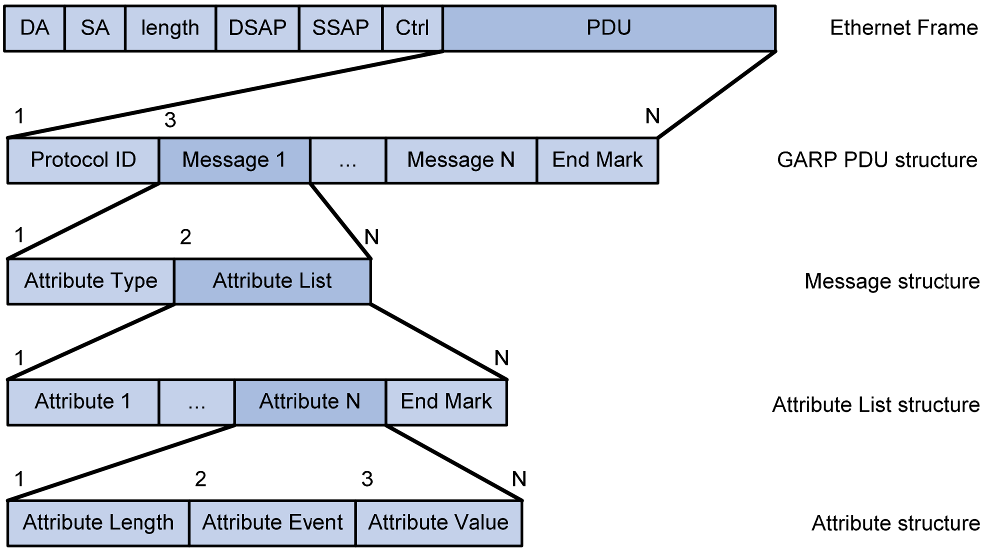
Through the mechanism of GARP, the configuration information on a GARP member will be propagated within the whole LAN. A GARP member can be a terminal workstation or a bridge; it instructs other GARP members to register/deregister its attribute information by declaration/recant, and register/deregister 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.<br>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<br>1: JoinEmpty<br>2: JoinIn<br>3: LeaveEmpty<br>4: LeaveIn<br>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<br>By default, GVRP is disabled globally. |
| Enter Ethernet port view | **interface** *interface-type interface-number* | — |
| Enable GVRP on the port | **gvrp** | Required<br>By default, GVRP is disabled on the port. |

**Note s**

- 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** *timer-value* | Optional<br>By default, the LeaveAll timer is set to 1,000 centiseconds. |
| Enter Ethernet port view | **interface** *interface-type interface-number* | — |
| Configure the Hold, Join, and Leave timers | **garp timer** { **hold** \| **join** \| **leave** } *timer-value* | Optional<br>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** *interface-type interface-number* | — |
| Configure GVRP port registration mode | **gvrp registration** { **fixed** \| **forbidden** \| **normal** } | Optional<br>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** *interface-list* ] | Available in any view |
| Display the settings of the GARP timers | **display garp timer** [ **interface** *interface-list* ] | |
| Display GVRP statistics | **display gvrp statistics** [ **interface** *interface-list* ] | |
| Display the global GVRP status | **display gvrp status** | |
| Clear GARP statistics | **reset garp statistics** [ **interface** *interface-list* ] | |

# GVRP Configuration Example

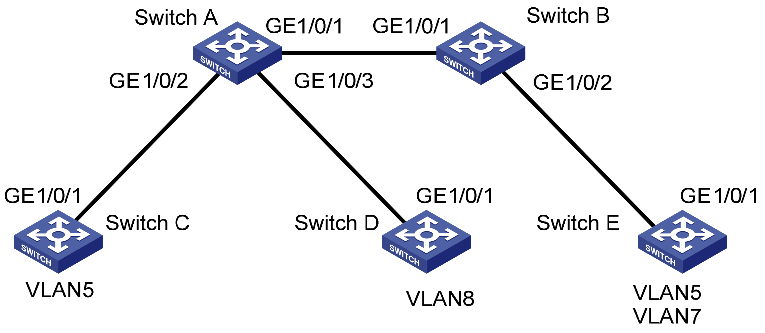
## GVRP Configuration Example

### 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 GigabitEthernet1/0/1 to be a trunk port and to permit the packets of all the VLANs.

```
[SwitchA] interface GigabitEthernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] port link-type trunk
```

```
[SwitchA-GigabitEthernet1/0/1] port trunk permit vlan all
```

# Enable GVRP on GigabitEthernet1/0/1.

```
[SwitchA-GigabitEthernet1/0/1] gvrp
[SwitchA-GigabitEthernet1/0/1] quit
```

# Configure GigabitEthernet1/0/2 to be a trunk port and to permit the packets of all the VLANs.

```
[SwitchA] interface GigabitEthernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] port link-type trunk
[SwitchA-GigabitEthernet1/0/2] port trunk permit vlan all
```

# Enable GVRP on GigabitEthernet1/0/2.

```
[SwitchA-GigabitEthernet1/0/2] gvrp
[SwitchA-GigabitEthernet1/0/2] quit
```

# Configure GigabitEthernet1/0/3 to be a trunk port and to permit the packets of all the VLANs.

```
[SwitchA] interface GigabitEthernet 1/0/3
[SwitchA-GigabitEthernet1/0/3] port link-type trunk
[SwitchA-GigabitEthernet1/0/3] port trunk permit vlan all
```

# Enable GVRP on GigabitEthernet1/0/3.

```
[SwitchA-GigabitEthernet1/0/3] gvrp
[SwitchA-GigabitEthernet1/0/3] 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 GigabitEthernet1/0/1 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 GigabitEthernet1/0/1 on Switch E to operate in fixed GVRP registration mode.

```
[SwitchE] interface GigabitEthernet 1/0/1
[SwitchE-GigabitEthernet1/0/1] 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-GigabitEthernet1/0/1] display vlan dynamic
  No dynamic vlans exist!
```

8) Configure GigabitEthernet1/0/1 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 GigabitEthernet1/0/1 on Switch E to operate in forbidden GVRP registration mode.

```
[SwitchE-GigabitEthernet1/0/1] 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

## Ethernet Port Configuration

### Combo Port Configuration

A Combo port can operate as either an optical port or an electrical port. Inside the device there is only one forwarding interface. For a Combo port, the electrical port and the corresponding optical port are TX-SFP multiplexed. You can specify a Combo port to operate as an electrical port or an optical port. That is, a Combo port cannot operate as both an electrical port and an optical port simultaneously. When one is enabled, the other is automatically disabled

Follow these steps to configure the state of a double Combo port:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter Ethernet interface view | **interface** *interface-type interface-number* | — |
| Enable a specified double Combo port | **undo shutdown** | Optional<br>By default, of the two ports in a Combo port, the one with a smaller port ID is enabled. |

### 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** *interface-type interface-number* | — |
| Enable the Ethernet port | **undo shutdown** | Optional<br>By default, the port is enabled.<br>Use the **shutdown** command to disable the port. |
| Set the description string for the Ethernet port | **description** *text* | Optional<br>By default, the description string of an Ethernet port is null. |
| Set the duplex mode of the Ethernet port | **duplex** { **auto** \| **full** \| **half** } | Optional<br>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<br>By default, the speed of an Ethernet port is determined through auto-negotiation (the auto keyword). |
| Set the medium dependent interface (MDI) mode of the Ethernet port | **mdi** { **across** \| **auto** \| **normal** } | Optional<br>Be 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<br>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 1,522 bytes, use the **undo jumboframe enable** command. |

**Note**

- The **speed** and **mdi** commands are not available on the combo port.
- The **mdi** command is not available on the Ethernet ports of the expansion interface card.

## 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** *interface-type interface-number* | — |
| Configure the available auto-negotiation speed(s) for the port | **speed auto** [ **10** \| **100** \| **1000** ]* | Optional<br>By default, the port speed is determined through auto-negotiation. |

**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 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** { *ratio* \| **pps** *max-pps* } | Optional<br>By default, the switch does not suppress broadcast traffic. |
| Enter Ethernet port view | **interface** *interface-type interface-number* | — |
| Limit broadcast traffic received on the current port | **broadcast-suppression** { *ratio* \| **pps** *max-pps* } | Optional<br>By default, the switch does not suppress broadcast traffic. |

## Enabling Flow Control on a Port

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

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

Follow these steps to enable flow control on a port:

| To do... | Use the command... | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter Ethernet port view | **interface** *interface-type interface-number* | — |

| To do... | Use the command... | Remarks |
|---|---|---|
| Enable flow control on the Ethernet port | **flow-control** | By default, flow control is not enabled on the port. |

## 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** { *interface-type interface-number* \| **aggregation-group** *source-agg-id* } **destination** { *interface-list* [ **aggregation-group** *destination-agg-id* ] \| **aggregation-group** *destination-agg-id* } | Required |

**Note**

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

## Configuring Loopback Detection for an Ethernet Port

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

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

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

Follow these steps to configure loopback detection for an Ethernet port:

| To do... | Use the command... | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enable loopback detection globally | **loopback-detection enable** | Required<br>By default, loopback detection is disabled globally. |
| Set the interval for performing port loopback detection | **loopback-detection interval-time** *time* | Optional<br>The default is 30 seconds. |
| Enter Ethernet port view | **interface** *interface-type interface-number* | — |
| Enable loopback port control on the trunk or hybrid port | **loopback-detection control enable** | Optional<br>By default, loopback port control is not enabled. |
| Configure the system to run loopback detection on all VLANs of the current trunk or hybrid port | **loopback-detection per-vlan enable** | Optional<br>By default, the system runs loopback detection only on the default VLAN of the current trunk or hybrid port. |
| Enable loopback detection on a specified port | **loopback-detection enable** | Required<br>By default, port loopback detection is disabled. |

**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 commands of loopback detection feature cannot be configured with the commands of port link aggregation at the same time.
- 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** *interface-type interface-number* | — |
| 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 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** *interface-type interface-number* | — |
| Enable the system to test connected cables | **virtual-cable-test** | Required |

Note

- Optical port (including Combo optical port) does not support VCT (**virtual-cable-test**) function.
- Combo electrical port supports VCT function only when it is in UP condition (using undo shutdown command), normal Ethernet electrical port always supports 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** *interface-type interface-number* | — |
| Set the interval to perform statistical analysis on port traffic | **flow-interval** *interval* | Optional<br>By default, this interval is 300 seconds. |

## 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** *interface-type interface-number* | — |
| Disable a port from generating UP/Down log | **undo enable log updown** | Required<br>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 GigabitEthernet 1/0/1. The Up/Down log information for GigabitEthernet 1/0/1 is generated and displayed on the terminal.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] shutdown
%Apr  5 07:25:37:634 2000 Sysname L2INF/5/PORT LINK STATUS CHANGE:- 1 -
 GigabitEthernet1/0/1 is DOWN
[Sysname-GigabitEthernet1/0/1] undo shutdown
%Apr  5 07:25:56:244 2000 Sysname L2INF/5/PORT LINK STATUS CHANGE:- 1 -
 GigabitEthernet1/0/1 is UP
```

# Disable GigabitEthernet 1/0/1 from generating Up/Down log information and execute the **shutdown** command or the **undo shutdown** command on GigabitEthernet 1/0/1. No Up/Down log information is generated or output for GigabitEthernet 1/0/1.

```
[Sysname-GigabitEthernet1/0/1] undo enable log updown
[Sysname-GigabitEthernet1/0/1] shutdown
[Sysname-GigabitEthernet1/0/1] undo shutdown
```

## Configuring a Port Group

To make the configuration task easier for users, certain devices allow users to configure on a single port as well as on multiple ports in a port group. In port group view, the user only needs to input the configuration command once on one port and that configuration will apply to all ports in the port group. This effectively reduces redundant configurations.

A Port group could be manually created by users. Multiple Ethernet ports can be added to the same port group but one Ethernet port can only be added to one port group.

**Table 1-1** Configuring a Port Group

| Operation | Command | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Create a port group or enter the specified port group view | **port-group** *group-id* | Required |
| Add an Ethernet port to a specified port group | **port** *interface-list* | Required |

**Note**

A port can not be added to a port group if it has been added to an aggregation group, and vice versa.

## Displaying and Maintaining Basic Port Configuration

| To do... | Use the command... | Remarks |
|---|---|---|
| Display port configuration information | **display interface** [ *interface-type* \| *interface-type interface-number* ] | Available in any view |
| Display the enable/disable status of port loopback detection | **display loopback-detection** | |
| Display information for a specified port group | **display port-group** *group-id* | |
| Display brief information about port configuration | **display brief interface** [ *interface-type* [ *interface-number* ] ] [ **\|** { **begin** \| **include** \| **exclude** } *regular-expression* ] | |
| Display the Combo ports and the corresponding optical/electrical ports | **display port combo** | |
| Display port information about a specified unit | **display unit** *unit-id* **interface** | |
| Clear port statistics | **reset counters interface** [ *interface-type* \| *interface-type interface-number* ] | Available in user view<br>After 802.1x is enabled on a port, clearing the statistics on the port will not work. |

# Table of Contents

# 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)<br>Attribute of the link (point-to-point or otherwise) connected to the port<br>Port path cost<br>STP priority<br>STP packet format<br>Loop protection<br>Root protection<br>Port type (whether the port is an edge port) |
| QoS | 802.1p priority<br>Traffic accounting |
| Link type | Link type of the ports (trunk, hybrid, or access) |
| GVRP | GVRP state on ports (enabled or disabled)<br>GVRP registration type<br>GARP timer settings |

# 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 mater 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.

# 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.
- A port belonging to a port group cannot be added to an aggregation group. Conversely, a port belonging to an aggregation group cannot be added to a port 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** *agg-id* **mode manual** | Required |
| Enter Ethernet port view | **interface** *interface-type interface-number* | — |
| Add the Ethernet port to the aggregation group | **port link-aggregation group** *agg-id* | Required |

Note that:

1) When creating an aggregation group:

- If the aggregation group you are creating already exists but contains no port, its type will change to the type you set.

- If the aggregation group you are creating already exists and contains ports, the possible type changes may be: changing from dynamic or static to manual, and changing from dynamic to static; and no other kinds of type change can occur.
- When you change a dynamic/static group to a manual group, the system will automatically disable LACP on the member ports. When you change a dynamic group to a static group, the system will remain the member ports LACP-enabled.

2) When a manual or static aggregation group contains only one port, you cannot remove the port unless you remove the whole aggregation group.

## 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** *agg-id* **mode static** | Required |
| Enter Ethernet port view | **interface** *interface-type interface-number* | — |
| Add the port to the aggregation group | **port link-aggregation group** *agg-id* | Required |

**Note**

For a static LACP aggregation group or a manual aggregation group, you are recommended not to cross cables between the two devices at the two ends of the aggregation group. For example, suppose port 1 of the local device is connected to port 2 of the peer device. To avoid cross-connecting cables, do not connect port 2 of the local device to port 1 of the peer device. Otherwise, packets may be lost.

## 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** *system-priority* | Optional<br>By default, the system priority is 32,768. |
| Enter Ethernet port view | **interface** *interface-type interface-number* | — |
| Enable LACP on the port | **lacp enable** | Required<br>By default, LACP is disabled on a port. |
| Configure the port priority | **lacp port-priority** *port-priority* | Optional<br>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** *agg-id* **description** *agg-name* | Optional<br>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** [ *agg-id* ] | |
| Display link aggregation details of a specified port or port range | **display link-aggregation interface** *interface-type interface-number* [ **to** *interface-type interface-number* ] | |
| Display local device ID | **display lacp system-id** | |
| Clear LACP statistics about a specified port or port range | **reset lacp statistics** [ **interface** *interface-type interface-number* [ **to** *interface-type interface-number* ] ] | Available in user view |

# Link Aggregation Configuration Example

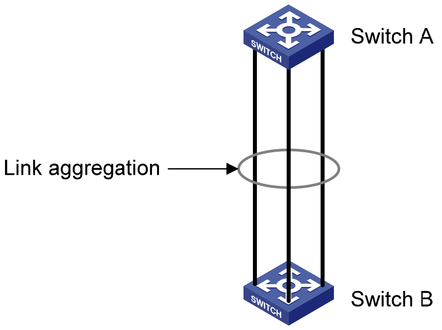
## Ethernet Port Aggregation Configuration Example

### Network requirements

- Switch A connects to Switch B with three ports GigabitEthernet 1/0/1 to GigabitEthernet 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 GigabitEthernet 1/0/1 through GigabitEthernet 1/0/3 to aggregation group 1.

```
[Sysname] interface GigabitEthernet1/0/1
[Sysname-GigabitEthernet1/0/1] port link-aggregation group 1
[Sysname-GigabitEthernet1/0/1] quit
[Sysname] interface GigabitEthernet 1/0/2
[Sysname-GigabitEthernet1/0/2] port link-aggregation group 1
[Sysname-GigabitEthernet1/0/2] quit
[Sysname] interface GigabitEthernet1/0/3
[Sysname-GigabitEthernet1/0/3] 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 GigabitEthernet 1/0/1 through GigabitEthernet 1/0/3 to aggregation group 1.

```
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port link-aggregation group 1
[Sysname-GigabitEthernet1/0/1] quit
[Sysname] interface GigabitEthernet 1/0/2
[Sysname-GigabitEthernet1/0/2] port link-aggregation group 1
[Sysname-GigabitEthernet1/0/2] quit
[Sysname] interface GigabitEthernet1/0/3
[Sysname-GigabitEthernet1/0/3] port link-aggregation group 1
```

3) Adopting dynamic LACP aggregation mode

# Enable LACP on GigabitEthernet 1/0/1 through GigabitEthernet 1/0/3.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] lacp enable
[Sysname-GigabitEthernet1/0/1] quit
[Sysname] interface GigabitEthernet 1/0/2
[Sysname-GigabitEthernet1/0/2] lacp enable
[Sysname-GigabitEthernet1/0/2] quit
```

```
[Sysname] interface GigabitEthernet1/0/3
[Sysname-GigabitEthernet1/0/3] 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

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

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. Thus, you can construct your network in a more flexible way and improve your network security.

Currently, you can create only one isolation group on an 4200G Ethernet switch. The number of Ethernet ports in an isolation group is not limited.

**Note**

- An isolation group only isolates the member ports in it.
- Port isolation is independent of VLAN configuration.

## 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** *interface-type interface-number* | — |
| Add the Ethernet port to the isolation group | **port isolate** | Required<br>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.

# 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

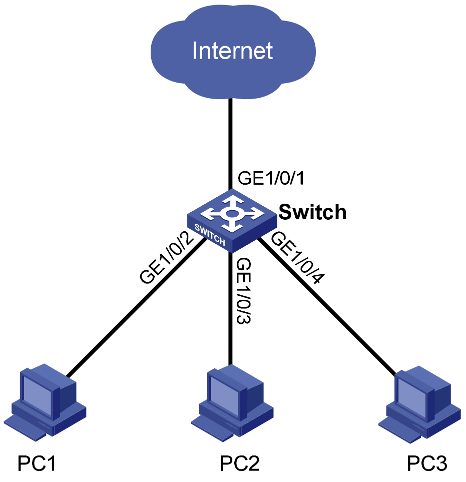
## Network requirements

As shown in Figure 1-1, PC2, PC3 and PC4 connect to the switch ports GigabitEthernet1/0/2, GigabitEthernet1/0/3, and GigabitEthernet1/0/4 respectively. The switch connects to the Internet through GigabitEthernet1/0/1.

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 GigabitEthernet1/0/2, GigabitEthernet1/0/3, and GigabitEthernet1/0/4 to the isolation group.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface GigabitEthernet1/0/2
[Sysname-GigabitEthernet1/0/2] port isolate
[Sysname-GigabitEthernet1/0/2] quit
[Sysname] interface GigabitEthernet1/0/3
[Sysname-GigabitEthernet1/0/3] port isolate
[Sysname-GigabitEthernet1/0/3] quit
[Sysname] interface GigabitEthernet1/0/4
[Sysname-GigabitEthernet1/0/4] port isolate
[Sysname-GigabitEthernet1/0/4] quit
[Sysname] quit
```

# Display information about the ports in the isolation group.

```
<Sysname> display isolate port
 Isolated port(s) on UNIT 1:
 GigabitEthernet1/0/2, GigabitEthernet1/0/3, GigabitEthernet1/0/4
```

# Table of Contents

# 1 Port Security Configuration

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 Example

## 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 address authentication.

Port security allows you to define various security modes that enable devices to learn legal source MAC addresses, so that you can implement different 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.

With port security enabled, upon detecting an illegal packet or illegal event, the system triggers the corresponding port security features and takes pre-defined actions automatically. This reduces your maintenance workload and greatly enhances system security and manageability.

### Port Security Features

The following port security features are provided:

- NTK (need to know) feature: By checking the destination MAC addresses in outbound data frames on the port, NTK ensures that the switch sends data frames through the port only to successfully authenticated devices, thus preventing illegal devices from intercepting network data.
- Intrusion protection feature: By checking the source MAC addresses in inbound data frames or the username and password in 802.1x authentication requests on the port, intrusion protection detects illegal packets or events and takes a pre-set action accordingly. The actions you can set include: disconnecting the port temporarily/permanently, and blocking packets with the MAC address specified as illegal.
- Trap feature: When special data packets (generated from illegal intrusion, abnormal login/logout or other special activities) are passing through the switch port, Trap feature enables the switch to send Trap messages to help the network administrator monitor special activities.

### Port Security Modes

Table 1-1 describes the available port security modes:

**Table 1-1** Description of port security modes

| Security mode | Description | Feature |
|---|---|---|
| **noRestriction** | In this mode, access to the port is not restricted. | In this mode, neither the NTK nor the intrusion protection feature is triggered. |
| **autolearn** | In this mode, the port automatically learns MAC addresses and changes them to security MAC addresses.<br>This security mode will automatically change to the **secure** mode after the amount of security MAC addresses on the port reaches the maximum number configured with the **port-security max-mac-count** command.<br>After the port security mode is changed to the **secure** mode, only those packets whose source MAC addresses are security MAC addresses learned or dynamic MAC addresses configured can pass through the port. | In either mode, the device will trigger NTK and intrusion protection upon detecting an illegal packet. |
| **secure** | In this mode, the port is disabled from learning MAC addresses.<br>Only those packets whose source MAC addresses are security MAC addresses learned and static or dynamic MAC addresses can pass through the port. | |

| Security mode | Description | Feature |
|---|---|---|
| **userlogin** | In this mode, port-based 802.1x authentication is performed for access users. | In this mode, neither NTK nor intrusion protection will be triggered. |
| **userLoginSecure** | MAC-based 802.1x authentication is performed on the access user. The port is enabled only after the authentication succeeds. When the port is enabled, only the packets of the successfully authenticated user can pass through the port.<br>In this mode, only one 802.1x-authenticated user is allowed to access the port.<br>When the port changes from the **noRestriction** mode to this security mode, the system automatically removes the existing dynamic MAC address entries and authenticated MAC address entries on the port. | In any of these modes, the device triggers the NTK and Intrusion Protection features upon detecting an illegal packet or illegal event. |
| **userLoginSecureExt** | This mode is similar to the **userLoginSecure** mode, except that there can be more than one 802.1x-authenticated user on the port. | |
| **userLoginWithOUI** | This mode is similar to the **userLoginSecure** mode, except that, besides the packets of the single 802.1x-authenticated user, the packets whose source MAC addresses have a particular OUI are also allowed to pass through the port.<br>When the port changes from the normal mode to this security mode, the system automatically removes the existing dynamic/authenticated MAC address entries on the port. | |
| **macAddressWithRadius** | In this mode, MAC address–based authentication is performed for access users. | |
| **macAddressOrUserLoginSecure** | In this mode, both MAC authentication and 802.1x authentication can be performed, but 802.1x authentication has a higher priority.<br>802.1x authentication can still be performed on an access user who has passed MAC authentication.<br>No MAC authentication is performed on an access user who has passed 802.1x authentication.<br>In this mode, there can be only one 802.1x-authenticated user on the port, but there can be several MAC-authenticated users. | |
| **macAddressOrUserLoginSecureExt** | This mode is similar to the **macAddressOrUserLoginSecure** mode, except that there can be more than one 802.1x-authenticated user on the port. . | |

| Security mode | Description | Feature |
|---|---|---|
| **macAddressElseUserLoginSecure** | In this mode, a port performs MAC authentication of an access user first. If the authentication succeeds, the user is authenticated. Otherwise, the port performs 802.1x authentication of the user.<br>In this mode, there can be only one 802.1x-authenticated user on the port, but there can be several MAC-authenticated users. | |
| **macAddressElseUserLoginSecureExt** | This mode is similar to the **macAddressElseUserLoginSecure** mode, except that there can be more than one 802.1x-authenticated user on the port. | |
| **macAddressAndUserLoginSecure** | In this mode, a port firstly performs MAC authentication for a user and then performs 802.1x authentication for the user if the user passes MAC authentication. The user can access the network after passing the two authentications.<br>In this mode, up to one user can access the network. | |
| **macAddressAndUserLoginSecureExt** | This mode is similar to the **macAddressAndUserLoginSecure** mode, except that more than one user can access the network. | |

**Note**

- When the port operates in the **userlogin-withoui** mode, Intrusion Protection will not be triggered even if the OUI address does not match.
- On a port operating in either the **macAddressElseUserLoginSecure** mode or the **macAddressElseUserLoginSecureExt** mode, Intrusion Protection is triggered only after both MAC-based 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 MAC Addresses Allowed on a Port | | Optional |
| Setting the Port Security Mode | | Required |
| Configuring Port Security Features | Configuring the NTK feature | Optional<br>Choose one or more features as required. |
| | Configuring intrusion protection | |
| | Configuring the Trap feature | |

| Task | Remarks |
|---|---|
| Ignoring the Authorization Information from the RADIUS Server | Optional |
| Configuring Security MAC Addresses | Optional |

## Enabling Port Security

### Configuration Prerequisites

Before enabling port security, you need to 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<br>Disabled by default |

**Caution**

Enabling port security resets the following configurations on the ports to the defaults (shown in parentheses below):

- 802.1x (disabled), port access control method (**macbased**), and port access control mode (**auto**)
- MAC authentication (disabled)

In addition, you cannot perform the above-mentioned configurations manually because these configurations change with the port security mode automatically.

**Note**

- For details about 802.1x configuration, refer to the sections covering 802.1x and System-Guard.
- For details about MAC authentication configuration, refer to the sections covering MAC authentication configuration.

## Setting the Maximum Number of MAC Addresses Allowed on a Port

Port security allows more than one user to be authenticated on a port. The number of authenticated users allowed, however, cannot exceed the configured upper limit.

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 Security MAC addresses that can be added with port security

This configuration is different from that of the maximum number of MAC addresses that can be leaned by a 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** *interface-type interface-number* | — |
| Set the maximum number of MAC addresses allowed on the port | **port-security max-mac-count** *count-value* | Required<br>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** *OUI-value* **index** *index-value* | Optional<br>In **userLoginWithOUI** mode, a port supports one 802.1x user plus one user whose source MAC address has a specified OUI value. |
| Enter Ethernet port view | **interface** *interface-type interface-number* | — |
| 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<br>By default, a port operates in **noRestriction** mode. In this mode, access to the port is not restricted.<br>You can set a port security mode as needed. |

Note

- Before setting the port security mode to **autolearn**, you need to set the maximum number of 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 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.
- If the port is in a security mode other than **noRestriction**, before you can change the port security mode, you need to restore the port security mode to **noRestriction** with the **undo port-security port-mode** command.

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 MAC addresses that the port can learn
- Reflector port for port mirroring
- 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** *interface-type interface-number* | — |
| Configure the NTK feature | **port-security ntk-mode** { **ntkonly** \| **ntk-withbroadcasts** \| **ntk-withmulticasts** } | Required<br>By default, NTK is disabled on a port, namely all frames are allowed to be sent. |

Note

Currently, the 4200G do not support the **ntkonly** NTK feature.

### 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** *interface-type interface-number* | — |
| Set the corresponding action to be taken by the switch when intrusion protection is triggered | **port-security intrusion-mode** { **blockmac** \| **disableport** \| **disableport-temporarily** } | Required<br>By default, intrusion protection is disabled. |
| Return to system view | **quit** | — |
| Set the timer during which the port remains disabled | **port-security timer disableport** *timer* | Optional<br>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 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 the Trap feature

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<br>By default, no trap is sent. |

## 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** *interface-type interface-number* | — |
| Ignore the authorization information from the RADIUS server | **port-security authorization ignore** | Required<br>By default, a port uses the authorization information from the RADIUS server. |

## Configuring Security MAC Addresses

Security MAC addresses are special MAC addresses that never age out. One security MAC address can be added to only one port in the same VLAN so that you can bind a MAC address to one port in the same VLAN.

Security MAC addresses can be learned by the auto-learn function of port security or manually configured.

Before adding security MAC addresses to a port, you must configure the port security mode to **autolearn**. After this configuration, the port changes its way of learning MAC addresses as follows.

- The port deletes original dynamic MAC addresses;
- If the amount of security MAC addresses has not yet reach the maximum number, the port will learn new MAC addresses and turn them to security MAC addresses;
- If the amount of security MAC addresses reaches the maximum number, the port will not be able to learn new MAC addresses and the port mode will be changed from **autolearn** to **secure**.

**Note**

The security MAC addresses manually configured are written to the configuration file; they will not get lost when the port is up or down. As long as the configuration file is saved, the security MAC addresses can be restored after the switch reboots.

### Configuration prerequisites

- Port security is enabled.
- The maximum number of security MAC addresses allowed on the port is set.
- The security mode of the port is set to **autolearn**.

### Configuring a security MAC address

Follow these steps to configure a security MAC address:

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

| To do... | | Use the command... | Remarks |
|---|---|---|---|
| Add a security MAC address | In system view | **mac-address security** *mac-address* **interface** *interface-type interface-number* **vlan** *vlan-id* | Either is required.<br>By default, no security MAC address is configured. |
| | In Ethernet port view | **interface** *interface-type interface-number* | |
| | | **mac-address security** *mac-address* **vlan** *vlan-id* | |

# Displaying and Maintaining Port Security Configuration

| To do... | Use the command... | Remarks |
|---|---|---|
| Display information about port security configuration | **display port-security** [ **interface** *interface-list* ] | Available in any view |
| Display information about security MAC address configuration | **display mac-address security** [ **interface** *interface-type interface-number* ] [ **vlan** *vlan-id* ] [ **count** ] | |

# Port Security Configuration Example

## Port Security Configuration Example

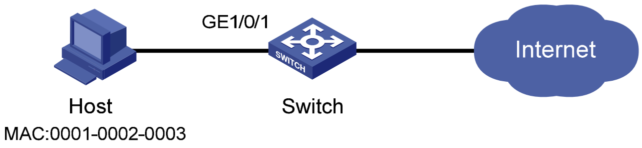
### Network requirements

Implement access user restrictions through the following configuration on GigabitEthernet 1/0/1 of the switch.

- 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 security MAC addresses.
- To ensure that Host can access the network, add the MAC address 0001-0002-0003 of Host as a security MAC address to the port in VLAN 1.
- After the number of security 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 1-1** Network diagram for port security configuration



### Configuration procedure

# Enter system view.

```
<Switch> system-view
```

# Enable port security.

```
[Switch] port-security enable
```

# Enter GigabitEthernet1/0/1 port view.

```
[Switch] interface GigabitEthernet 1/0/1
```

# Set the maximum number of MAC addresses allowed on the port to 80.

```
[Switch-GigabitEthernet1/0/1] port-security max-mac-count 80
```

# Set the port security mode to **autolearn**.

```
[Switch-GigabitEthernet1/0/1] port-security port-mode autolearn
```

# Add the MAC address 0001-0002-0003 of Host as a security MAC address to the port in VLAN 1.

```
[Switch-GigabitEthernet1/0/1] mac-address security 0001-0002-0003 vlan 1
```

# Configure the port to be silent for 30 seconds after intrusion protection is triggered.

```
[Switch-GigabitEthernet1/0/1] port-security intrusion-mode disableport-temporarily
[Switch-GigabitEthernet1/0/1] quit
[Switch] port-security timer disableport 30
```

# 2 Port Binding Configuration

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

Port binding enables the network administrator to bind the MAC address and IP address of a user to a specific port. After the binding, the switch forwards only the packets received on the port whose MAC address and IP address are identical with the bound MAC address and IP address. This improves network security and enhances security monitoring.

### Configuring Port Binding

Follow these steps to configure port binding:

| To do... | | Use the command... | Remarks |
|---|---|---|---|
| Enter system view | | **system-view** | — |
| Bind the MAC address and IP address of a user to a specific port | In system view | **am user-bind mac-addr** *mac-address* **ip-addr** *ip-address* **interface** *interface-type interface-number* | Either is required.<br>By default, no user MAC address or IP address is bound to a port. |
| | In Ethernet port view | **interface** *interface-type interface-number* | |
| | | **am user-bind mac-addr** *mac-address* **ip-addr** *ip-address* | |

**Note**

- An IP address can be bound to only one port at a time.
- A MAC address can be bound to only one port at a time.

## Displaying and Maintaining Port Binding Configuration

| To do... | Use the command... | Remarks |
|---|---|---|
| Display port binding information | **display am user-bind** [ **interface** *interface-type interface-number* \| **ip-addr** *ip-address* \| **mac-addr** *mac-address* ] | Available in any view |

# Port Binding Configuration Example

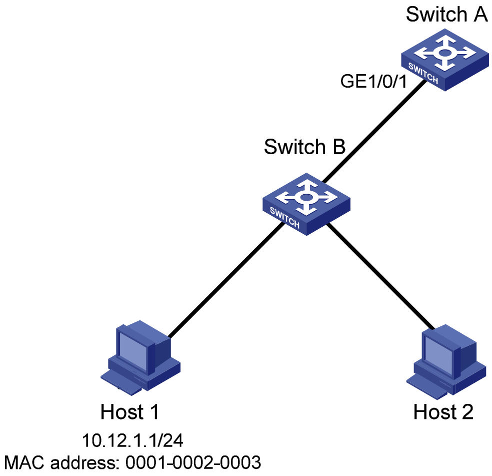
## Port Binding Configuration Example

### Network requirements

It is required to bind the MAC and IP addresses of Host A to GigabitEthernet 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 GigabitEthernet 1/0/1 port view.

```
[SwitchA] interface GigabitEthernet 1/0/1
```

# Bind the MAC address and the IP address of Host A to GigabitEthernet 1/0/1.

```
[SwitchA-GigabitEthernet1/0/1] am user-bind mac-addr 0001-0002-0003 ip-addr 10.12.1.1
```

# Table of Contents

# 1 MAC Address Table Management

**Note**

This chapter describes the management of static, dynamic, and blackhole MAC address entries. For information about the management of multicast MAC address entries, refer to the part related to multicast protocol.

## 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 GigabitEthernet 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)

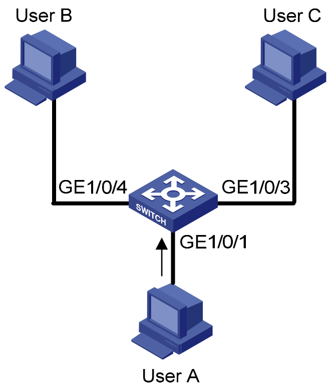
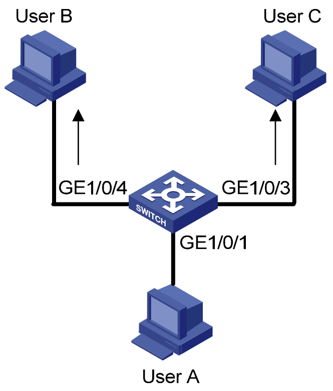


**Figure 1-2** MAC address table entry of the switch (1)

| MAC-address | Port | VLAN ID |
|---|---|---|
| MAC-A | GigabitEthernet1/0/1 | 1 |

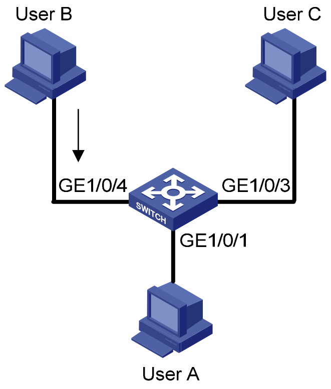
2) After learning the MAC address of User A, the switch starts to forward the packet. Because there is no MAC address and port information of User B in the existing MAC address table, the switch forwards the packet to all ports except GigabitEthernet 1/0/1 to ensure that User B can receive the packet.

**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 GigabitEthernet 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 GigabitEthernet 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 | GigabitEthernet1/0/1 | 1 |
| MAC-B | GigabitEthernet1/0/4 | 1 |

5) After this interaction, the switch directly unicasts the communication packets between 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**

Aging timer only takes effect on dynamic MAC address entries.

### 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

## Configuration Task List

**Table 1-2** Configure MAC address table management

| Task | Remarks |
|---|---|
| Configuring a MAC Address Entry | Required |
| Setting the Aging Time of MAC Address Entries | Optional |
| Setting the Maximum Number of MAC Addresses a Port Can Learn | 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

**Table 1-3** Add a MAC address entry in system view

| Operation | Command | Description |
|---|---|---|
| Enter system view | **system-view** | — |
| Add a MAC address entry | **mac-address** { **static** \| **dynamic** \| **blackhole** } *mac-address* **interface** *interface-type interface-number* **vlan** *vlan-id* | Required |

**Caution**

- When you add a MAC address entry, the port specified by the **interface** argument must belong to the VLAN specified by the **vlan** argument in the command. Otherwise, the entry will not be added.
- If the VLAN specified by the **vlan** argument is a dynamic VLAN, after a static MAC address is added, it will become a static VLAN.

### Adding a MAC address entry in Ethernet port view

**Table 1-4** Add a MAC address entry in Ethernet port view

| Operation | Command | Description |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter Ethernet port view | **interface** *interface-type interface-number* | — |
| Add a MAC address entry | **mac-address** { **static** \| **dynamic** \| **blackhole** } *mac-address* **vlan** *vlan-id* | Required |

**Caution**

- When you add a MAC address entry, the current port must belong to the VLAN specified by the **vlan** argument in the command. Otherwise, the entry will not be added.
- If the VLAN specified by the **vlan** argument is a dynamic VLAN, after a static MAC address is added, it will become a static VLAN.

## Setting the Aging Time of MAC Address Entries

Setting aging time properly helps effective utilization of MAC address aging. The aging time that is too long or too short affects the performance of the switch.

- If the aging time is too long, excessive invalid MAC address entries maintained by the switch may fill up the MAC address table. This prevents the MAC address table from being updated with network changes in time.
- If the aging time is too short, the switch may remove valid MAC address entries. This decreases the forwarding performance of the switch.

**Table 1-5** Set aging time of MAC address entries

| Operation | Command | Description |
|---|---|---|
| Enter system view | **system-view** | — |
| Set the aging time of MAC address entries | **mac-address timer** { **aging** *age* \| **no-aging** } | Required<br>The default aging time is 300 seconds. |

Normally, you are recommended to use the default aging time, namely, 300 seconds. The **no-aging** keyword specifies that MAC address entries do not age out.

**Note**

MAC address aging configuration applies to all ports, but only takes effect on dynamic MAC addresses that are learnt or configured to age.

## 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.

**Table 1-6** Set the maximum number of MAC addresses a port can learn

| Operation | Command | Description |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter Ethernet port view | **interface** *interface-type interface-number* | — |

| Operation | Command | Description |
|---|---|---|
| Set the maximum number of MAC addresses the port can learn | **mac-address max-mac-count** *count* | Required<br>By default, the number of the MAC addresses a port can learn is not limited. |

## Displaying MAC Address Table Information

To verify your configuration, you can display information about the MAC address table by executing the **display** command in any view.

**Table 1-7** Display MAC address table information

| Operation | Command | Description |
|---|---|---|
| Display information about the MAC address table | **display mac-address** [ *display-option* ] | The **display** command can be executed in any view. |
| Display the aging time of the dynamic MAC address entries in the MAC address table | **display mac-address aging-time** | |

## Configuration Example

### Adding a Static MAC Address Entry Manually

#### Network requirements

The server connects to the switch through GigabitEthernet 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 GigabitEthernet 1/0/2.

- The MAC address of the server is 000f-e20f-dc71.
- Port GigabitEthernet 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 GigabitEthernet 1/0/2 vlan 1
```

# Display information about the current MAC address table.

```
[Sysname] display mac-address interface GigabitEthernet 1/0/2
MAC ADDR          VLAN ID  STATE          PORT INDEX           AGING TIME(s)
000f-e20f-dc71    1        Config static  GigabitEthernet1/0/2 NOAGED
000f-e20f-a7d6    1        Learned        GigabitEthernet1/0/2 AGING
000f-e20f-b1fb    1        Learned        GigabitEthernet1/0/2 AGING
000f-e20f-f116    1        Learned        GigabitEthernet1/0/2 AGING
```

```
---  4 mac address(es) found on port GigabitEthernet1/0/2 ---
```

# Table of Contents

# 1 MSTP Configuration

Go to these sections for information you are interested in:

## STP Overview

### Functions of 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 tree topology. As a network with tree topology is loop-free, it prevents packets in it from being duplicated and forwarded endlessly and prevents device performance degradation.

Currently, in addition to the protocol conforming to IEEE 802.1d, STP also refers to the protocols based on IEEE 802.1d, such as RSTP, and MSTP.

### 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. 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 the entire network, and the root bridge can change alone with changes of the network topology. Therefore, the root bridge is not fixed.

Upon network convergence, the root bridge generates and sends out configuration BPDUs periodically. Other devices just forward the configuration BPDUs received. This mechanism ensures the topological stability.

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.

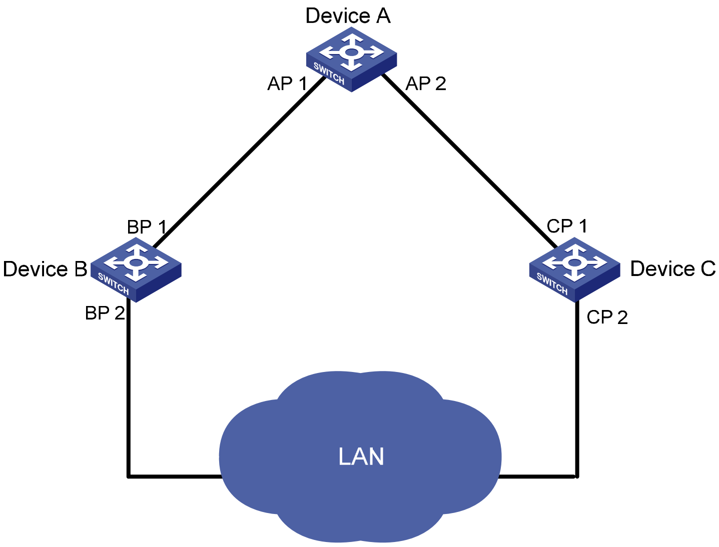
**Table 1-1** Designated bridge and designated port

| 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) Path cost

Path cost is a value used for measuring link capacity. 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.

### 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 name.
- 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**

For the convenience of description, the description and examples below involve only four parts of a configuration BPDU:

- Root bridge ID (in the form of device priority)
- Root path cost
- Designated bridge ID (in the form of device priority)
- Designated port ID (in the form of port name)

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:<br>• 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.<br>• 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**

Principle 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 configuration BPDU priority is compared sequentially: designated bridge IDs, designated port IDs, and then the IDs of the ports on which the configuration BPDUs are received. The switch with a higher priority is elected as the root bridge.

- 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 root bridge ID. The device with the smallest root bridge ID 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. |
| 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.<br>• The root bridge ID is replaced with that of the configuration BPDU of the root port.<br>• 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.<br>• The designated bridge ID is replaced with the ID of this device.<br>• The designated port ID is replaced with the ID of this port. |

| Step | Description |
|---|---|
| 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:<br>• 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.<br>• 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. |

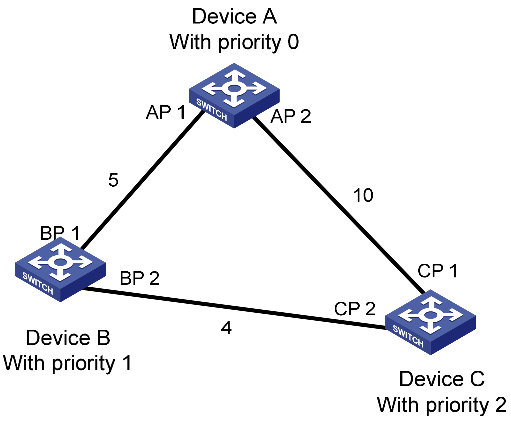
**Note**

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.

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 | Port name | BPDU of port |
|---|---|---|
| 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.

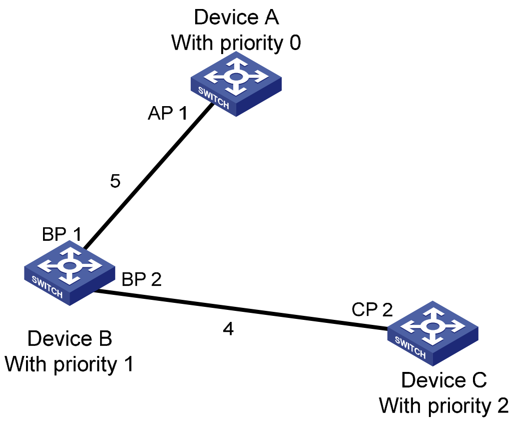
**Table 1-5** Comparison process and result on each device

| 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.<br>• 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.<br>• 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}<br>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.<br>• 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}<br>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.<br>• 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}.<br>• 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:<br>{0, 0, 0, AP1}<br>Designated port BP2:<br>{0, 5, 1, BP2} |
| 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.<br>• 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}<br>CP2: {1, 0, 1, BP2} |

| Device | Comparison process | BPDU of port after comparison |
|---|---|---|
| | By comparison:<br>• 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.<br>• 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:<br>{0, 0, 0, AP2}<br>Designated port CP2:<br>{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.<br>• 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}<br>CP2: {0, 5, 1, BP2} |
| | By comparison:<br>• 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.<br>• 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:<br>{0, 0, 0, AP2}<br>Root port CP2:<br>{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.

2) 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 sends 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.

3) 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.

# MSTP Overview

## Background of MSTP

### 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.)

The 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.

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.

### 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.

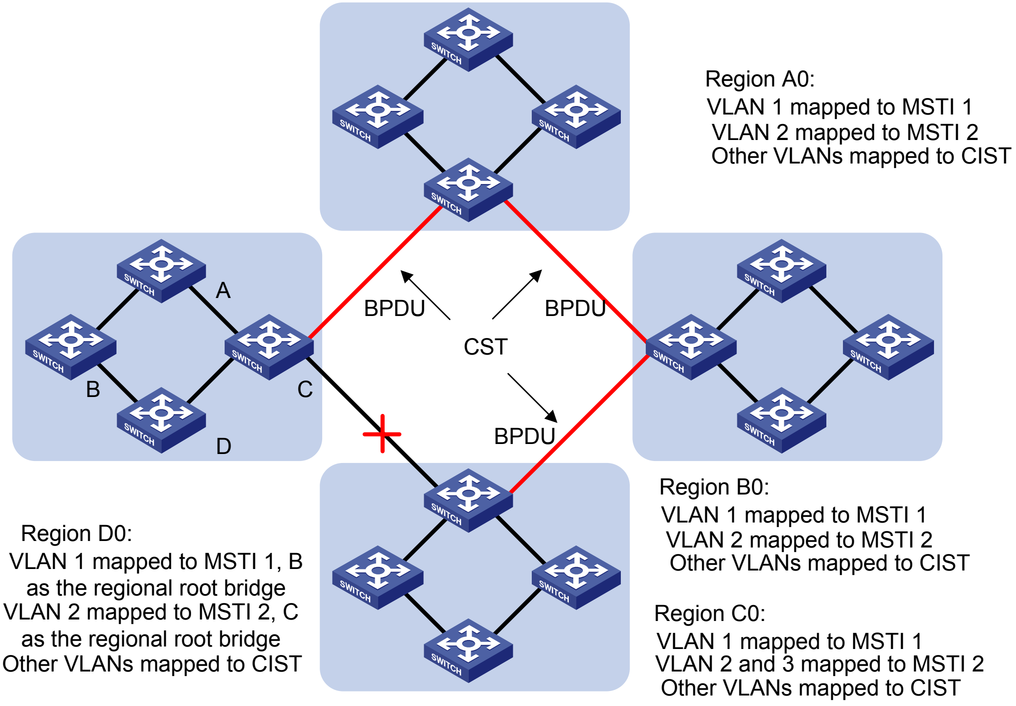
MSTP features the following:

- MSTP supports mapping VLANs to MST instances (MSTIs) by means of a VLAN-to-MSTI mapping table. MSTP introduces **instance** (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 Terminologies

Figure 1-4 illustrates basic MSTP terms (assuming that MSTP is enabled on each switch in this figure).

**Figure 1-4** Basic MSTP terminologies


Region A0:
VLAN 1 mapped to MSTI 1
VLAN 2 mapped to MSTI 2
Other VLANs mapped to CIST
A
B
C
D
BPDU
BPDU
CST
BPDU
Region D0:
VLAN 1 mapped to MSTI 1, B as the regional root bridge
VLAN 2 mapped to MSTI 2, C as the regional root bridge
Other VLANs mapped to CIST
Region B0:
VLAN 1 mapped to MSTI 1
VLAN 2 mapped to MSTI 2
Other VLANs mapped to CIST
Region C0:
VLAN 1 mapped to MSTI 1
VLAN 2 and 3 mapped to MSTI 2
Other VLANs mapped to CIST
SWITCH

### MST region

A multiple spanning tree region (MST region) comprises multiple physically-interconnected MSTP-enabled switches and the corresponding network segments connected to these switches. These switches have the same region name, the same VLAN-to-MSTI mapping configuration and the same MSTP revision level.

A switched network can contain multiple MST regions. You can group multiple switches into one MST region by using the corresponding MSTP configuration commands.

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-MSTI 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)

### 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.

### VLAN-to-MSTI mapping table

A VLAN-to-MSTI 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-MSTI 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-MSTI mapping table.

### 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.

### CST

A CST is a single spanning tree in a switched network that connects all MST regions in the network. If you regard each MST region in the network as a “switch”, then the CST is the spanning tree generated by STP or RSTP running on the "switches".

### CIST

A CIST is the spanning tree in a switched network that connects all switches in the network. It comprises the ISTs and the CST.

In Figure 1-4, the ISTs in the MST regions and the CST connecting the MST regions form the CIST.

### 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.

### 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.

### 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

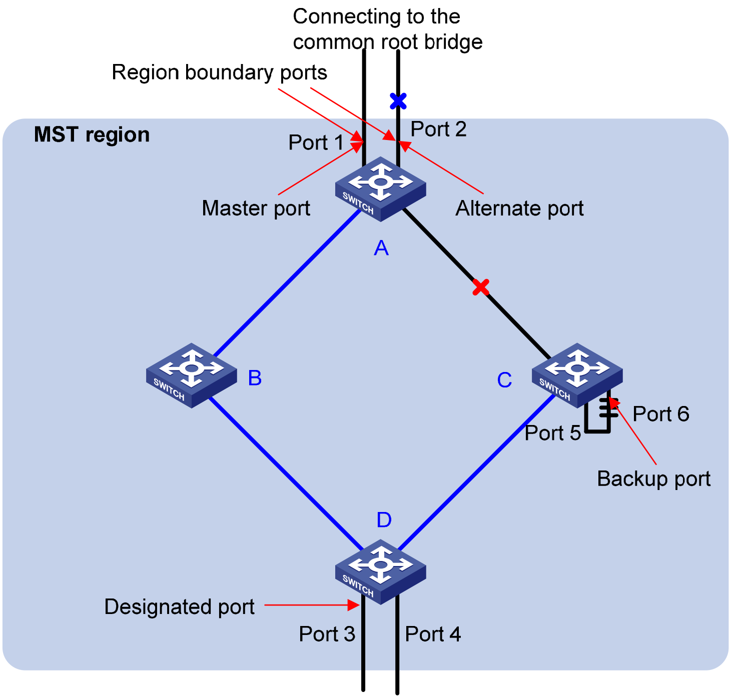
switch blocks one of the two ports to eliminate the loop that occurs. The blocked port is the backup port.

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



## 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<br>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.

### 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.

### Calculate an MSTI

In an MST region, different MSTIs are generated for different VLANs based on the VLAN-to-MSTI mappings. Each spanning tree is calculated independently, in the same way as how STP/RSTP is calculated.

### Implement STP algorithm

In the beginning, each switch regards itself as the root, and generates a configuration BPDU for each port on it as a root, with the root path cost being 0, the ID of the designated bridge being that of the switch, and the designated port being itself.

1) Each switch sends out its configuration BPDUs and operates in the following way when receiving a configuration BPDU on one of its ports from another switch:

- If the priority of the configuration BPDU is lower than that of the configuration BPDU of the port itself, the switch discards the BPDU and does not change the configuration BPDU of the port.
- If the priority of the configuration BPDU is higher than that of the configuration BPDU of the port itself, the switch replaces the configuration BPDU of the port with the received one and compares it with those of other ports on the switch to obtain the one with the highest priority.

2) Configuration BPDUs are compared as follows:

For MSTP, CIST configuration information is generally expressed as follows:

(Root bridge ID, External path cost,Master bridge ID, Internal path cost, Designated bridge ID,ID of sending port,ID of receiving port),so the compared as follows

- The smaller the Root bridge ID of the configuration BPDU is, the higher the priority of the configuration BPDU is.
- For configuration BPDUs with the same Root bridge IDs, the External path costs are compared.

- For configuration BPDUs with both the same Root bridge ID and the same External path costs, Master bridge ID, Internal path cost, Designated bridge ID,ID of sending port,ID of receiving port are compared in turn.

For MSTP, MSTI configuration information is generally expressed as follows:

(Instace bridge ID, Internal path costs, Designated bridge ID,ID of sending port,ID of receiving port),so the compared as follows

- The smaller the Instance bridge ID of the configuration BPDU is, the higher the priority of the configuration BPDU is.
- For configuration BPDUs with the same Instance bridge IDs, Internal path costs are compared.
- For configuration BPDUs with both the same Instance bridge ID and the same Internal path costs, Designated bridge ID,ID of sending port,ID of receiving port are compared in turn.

3) A spanning tree is calculated as follows:

- Determining the root bridge

Root bridges are selected by configuration BPDU comparing. The switch with the smallest root ID is chosen as the root bridge.

- Determining the root port

For each switch in a network, the port on which the configuration BPDU with the highest priority is received is chosen as the root port of the switch.

- Determining the designated port

First, the switch calculates a designated port configuration BPDU for each of its ports using the root port configuration BPDU and the root port path cost, with the root ID being replaced with that of the root port configuration BPDU, root path cost being replaced with the sum of the root path cost of the root port configuration BPDU and the path cost of the root port, the ID of the designated bridge being replaced with that of the switch, and the ID of the designated port being replaced with that of the port.

The switch then compares the calculated configuration BPDU with the original configuration BPDU received from the corresponding port on another switch. If the latter takes precedence over the former, the switch blocks the local port and keeps the port's configuration BPDU unchanged, so that the port can only receive configuration messages and cannot forward packets. Otherwise, the switch sets the local port to the designated port, replaces the original configuration BPDU of the port with the calculated one and advertises it regularly.

## MSTP Implementation on Switches

MSTP is compatible with both STP and RSTP. That is, MSTP-enabled switches can recognize the protocol packets of STP and RSTP and use them for spanning tree calculation. In addition to the basic MSTP functions, 3com 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

## STP-related Standards

STP-related standards include the following.

- IEEE 802.1D: spanning tree protocol
- IEEE 802.1w: rapid spanning tree protocol
- IEEE 802.1s: multiple spanning tree protocol

# Configuring Root Bridge

Complete the following tasks to configure the root bridge:

| Task | Remarks |
|---|---|
| Enabling MSTP | Required<br>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<br>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<br>The default value is recommended. |
| Configuring the MSTP Time-related Parameters | Optional<br>The default values are recommended. |
| Configuring the Timeout Time Factor | Optional |
| Configuring the Maximum Transmitting Rate on the Current Port | Optional<br>The default value is recommended. |
| Configuring the Current Port as an Edge Port | Optional |
| Specifying Whether the Link Connected to a Port Is Point-to-point Link | 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-MSTI mapping table.

## Configuration Prerequisites

The role (root, branch, or leaf) of each switch in each MSTI is determined.

## 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** *name* | Required<br>The default MST region name of a switch is its MAC address. |
| Configure the VLAN-to-MSTI mapping table for the MST region | **instance** *instance-id* **vlan** *vlan-list* | Required<br>Both commands can be used to configure VLAN-to-MSTI mapping tables.<br>By default, all VLANs in an MST region are mapped to MSTI 0. |
| | **vlan-mapping modulo** *modulo* | |
| Configure the MSTP revision level for the MST region | **revision-level** *level* | Required<br>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**

NTDP packets sent by devices in a cluster can only be transmitted within the MSTI where the management VLAN of the cluster resides.

Configuring MST region-related parameters (especially the VLAN-to-MSTI 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-MSTI mapping table, and revision level.
- The 3com switches support only the MST region name, VLAN-to-MSTI 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** *instance-id* ] **root primary** [ **bridge-diameter** *bridgenumber* [ **hello-time** *centi-seconds* ] ] | 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** *instance-id* ] **root secondary** [ **bridge-diameter** *bridgenumber* [ **hello-time** *centi-seconds* ] ] | Required |

Using the **stp root primary**/**stp root secondary** command, you can specify the current switch as the root bridge or the secondary root bridge of the 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** *instance-id* ] **priority** *priority* | Required<br>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 be configured to recognize and send MSTP packets in the following modes.

- Automatic mode. Ports in this mode determine the format of the MSTP packets to be sent according to the format of the received packets.
- Legacy mode. Ports in this mode recognize/send packets in legacy format.
- 802.1s mode. Ports in this mode recognize/send packets in dot1s format.

A port acts as follows according to the format of MSTP packets forwarded by a peer switch or router.

When a port operates in the automatic mode:

- The port automatically determines the format (legacy or dot1s) of received MSTP packets and then determines the format of the packets to be sent accordingly, thus communicating with the peer devices.
- If the format of the received packets changes repeatedly, MSTP will shut down the corresponding port to prevent network storm. A port shut down in this way can only be brought up by the network administrator.

When a port operates in the legacy mode:

- The port recognizes and sends MSTP packets in legacy format. In this case, the port can only communicate with the peer through packets in legacy format.
- If packets in dot1s format are received, the port turns to discarding state to prevent network storm.

When a port operates in the 802.1s mode:

- The port recognizes and sends MSTP packets in dot1s format. In this case, the port can only communicate with the peer through packets in dot1s format.
- If packets in legacy format are received, the port turns to discarding state to prevent network storm.

### 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** | — |
| Configure how a port recognizes and sends MSTP packets | **stp interface** *interface-type interface-number* **compliance** { **auto** \| **dot1s** \| **legacy** } | Required<br>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** *interface-type interface-number* | — |
| Configure how a port recognizes and sends MSTP packets | **stp compliance** { **auto** \| **dot1s** \| **legacy** } | Required<br>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 GigabitEthernet 1/0/1 to recognize and send packets in dot1s format.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] stp compliance dot1s
```

# Restore the default mode for GigabitEthernet 1/0/1 to recognize/send MSTP packets.

```
[Sysname-GigabitEthernet1/0/1] 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<br>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** *hops* | Required<br>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** *bridgenumber* | Required<br>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** *centiseconds* | Required<br>The forward delay parameter defaults to 1,500 centiseconds (namely, 15 seconds). |
| Configure the hello time parameter | **stp timer hello** *centiseconds* | Required<br>The hello time parameter defaults to 200 centiseconds (namely, 2 seconds). |
| Configure the max age parameter | **stp timer max-age** *centiseconds* | Required<br>The max age parameter defaults to 2,000 centiseconds (namely, 20 seconds). |

All switches in a switched network adopt the three time-related parameters configured on the CIST root bridge.

⚠ **Caution**

- The forward delay parameter and the network diameter are correlated. Normally, a large network diameter corresponds to a large forward delay. A too small forward delay parameter may result in temporary redundant paths. And a too large forward delay parameter may cause a network unable to resume the normal state in time after changes occurred to the network. The default value is recommended.
- An adequate hello time parameter enables a switch to detect link failures in time without occupying too many network resources. And a too small hello time parameter may result in duplicated configuration BPDUs being sent frequently, which increases the work load of the switches and wastes network resources. The default value is recommended.
- As for the max age parameter, if it is too small, network congestion may be falsely regarded as link failures, which results in frequent spanning tree recalculation. If it is too large, link problems may be unable to be detected in time, which prevents spanning trees being recalculated in time and makes the network less adaptive. The default value is recommended.

As for the configuration of the three time-related parameters (that is, the hello time, forward delay, and max age parameters), the following formulas must be met to prevent frequent network jitter.

2 x (forward delay – 1 second) >= max age

Max age >= 2 x (hello time + 1 second)

You are recommended to specify the network diameter of the switched network and the hello time by using the **stp root primary** or **stp root secondary** command. After that, the three proper time-related parameters are determined automatically.

### 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** *number* | Required<br>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** *interface-list* **transmit-limit** *packetnum* | Required<br>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** *interface-type interface-number* | — |
| Configure the maximum transmitting rate | **stp transmit-limit** *packetnum* | Required<br>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 GigabitEthernet 1/0/1 to 15.

1) Configure the maximum transmitting rate in system view

```
<Sysname> system-view
[Sysname] stp interface GigabitEthernet 1/0/1 transmit-limit 15
```

2) Configure the maximum transmitting rate in Ethernet port view

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] 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** *interface-list* **edged-port enable** | Required<br>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** | — |
| Enter Ethernet port view | **interface** *interface-type interface-number* | — |
| Configure the port as an edge port | **stp edged-port enable** | Required<br>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 GigabitEthernet 1/0/1 as an edge port.

1) Configure GigabitEthernet 1/0/1 as an edge port in system view

```
<Sysname> system-view
[Sysname] stp interface GigabitEthernet 1/0/1 edged-port enable
```

2) Configure GigabitEthernet 1/0/1 as an edge port in Ethernet port view

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] stp edged-port enable
```

## Specifying Whether the Link Connected to a Port Is Point-to-point Link

A point-to-point link directly connects two switches. If the roles of the two ports at the two ends of a point-to-point link meet certain criteria, the two ports can turn to the forwarding state rapidly by exchanging synchronization packets, thus reducing the forward delay.

You can determine whether or not the link connected to a port is a point-to-point link in one of the following two ways.

### Specify whether the link connected to a port is point-to-point link 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** *interface-list* **point-to-point** { **force-true** \| **force-false** \| **auto** } | Required<br>The **auto** keyword is adopted by default. |

### Specify whether the link connected to a port is point-to-point link 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** *interface-type interface-number* | — |
| Specify whether the link connected to a port is a point-to-point link | **stp point-to-point** { **force-true** \| **force-false** \| **auto** } | Required<br>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 GigabitEthernet 1/0/1 as a point-to-point link.

1) Perform this configuration in system view

```
<Sysname> system-view
[Sysname] stp interface GigabitEthernet 1/0/1 point-to-point force-true
```

2) Perform this configuration in Ethernet port view

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] 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<br>MSTP is enabled by default. |
| Disable MSTP on specified ports | **stp interface** *interface-list* **disable** | Optional<br>By default, MSTP is enabled on all ports.<br>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<br>MSTP is enabled by default. |
| Enter Ethernet port view | **interface** *interface-type interface-number* | — |
| Disable MSTP on the port | **stp disable** | Optional<br>By default, MSTP is enabled on all ports.<br>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

# Disable MSTP on GigabitEthernet 1/0/1.

1) Perform this configuration in system view

```
<Sysname> system-view
[Sysname] stp interface GigabitEthernet 1/0/1 disable
```

2) Perform this configuration in Ethernet port view

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] stp disable
```

# Configuring Leaf Nodes

Complete the following tasks to configure leaf nodes:

| Task | Remarks |
|---|---|
| Enabling MSTP | Required<br>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<br>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 |
| Specifying Whether the Link Connected to a Port Is Point-to-point Link | 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-MSTI mapping table.

## Configuration Prerequisites

The role (root, branch, or leaf) of each switch in each MSTI is determined.

## 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.

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** } | Optional<br>By default, the dot1t 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 |
| 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:

Path cost = 200,000,000 / 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** *interface-list* [ **instance** *instance-id* ] **cost** *cost* | Required<br>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** *interface-type interface-number* | — |
| Configure the path cost for the port | **stp** [ **instance** *instance-id* ] **cost** *cost* | Required<br>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 GigabitEthernet 1/0/1 in MSTI 1 to be 2,000.

1) Perform this configuration in system view

```
<Sysname> system-view
[Sysname] stp interface GigabitEthernet 1/0/1 instance 1 cost 2000
```

2) Perform this configuration in Ethernet port view

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] stp instance 1 cost 2000
```

### Configuration example (B)

# Configure the path cost of GigabitEthernet 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 GigabitEthernet 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 GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] undo stp instance 1 cost
[Sysname-GigabitEthernet1/0/1] 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** *interface-list* **instance** *instance-id* **port priority** *priority* | Required<br>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** *interface-type interface-number* | — |
| Configure port priority for the port | **stp** [ **instance** *instance-id* ] **port priority** *priority* | Required.<br>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 GigabitEthernet 1/0/1 in MSTI 1 to be 16.

1) Perform this configuration in system view

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

```
[Sysname] stp interface GigabitEthernet 1/0/1 instance 1 port priority 16
```

2) Perform this configuration in Ethernet port view

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] stp instance 1 port priority 16
```

## Specifying Whether the Link Connected to a Port Is a Point-to-point Link

Refer to Specifying Whether the Link Connected to a Port Is Point-to-point Link.

## 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.

A port on an MSTP-enabled switch operating as an upstream switch transits to the STP-compatible mode when it has an STP-enabled switch connected to it. When the STP-enabled downstream switch is then replaced by an MSTP-enabled switch, the port cannot automatically transit to the MSTP mode. It remains in the STP-compatible mode. In this case, you can force the port to transit to the MSTP mode by performing the mCheck operation on the port.

Similarly, a port on an RSTP-enabled switch operating as an upstream switch turns to the STP-compatible mode when it has an STP-enabled switch connected to it. When the STP enabled downstream switch is then replaced by an MSTP-enabled switch, the port cannot automatically transit to the MSTP-compatible mode. It remains in the STP-compatible mode. In this case, you can force the port to transit to the MSTP-compatible mode by performing the mCheck operation on the port.

## 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** *interface-list* ] **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** *interface-type interface-number* | — |
| Perform the mCheck operation | **stp mcheck** | Required |

## Configuration Example

# Perform the mCheck operation on GigabitEthernet 1/0/1.

1) Perform this configuration in system view

```
<Sysname> system-view
[Sysname] stp interface GigabitEthernet 1/0/1 mcheck
```

2) Perform this configuration in Ethernet port view

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] stp mcheck
```

# Configuring Guard Functions

## Introduction

The following guard functions are available on an MSTP-enabled switch: BPDU guard, root guard, loop guard, TC-BPDU attack guard, and BPDU drop.

### 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.

### 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.

### 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 turns 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.

⚠ **Caution**

With the loop guard function enabled, the root guard function and the edge port configuration are mutually exclusive.

### TC-BPDU attack guard

Normally, a switch removes its MAC address table and ARP entries upon receiving TC-BPDUs. If a malicious user sends a large amount of TC-BPDUs to a switch in a short period, the switch may be busy in removing 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.

### 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.

## Configuring BPDU Guard

### 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<br>The BPDU guard function is disabled by default. |

### Configuration example

# Enable the BPDU guard function.

```
<Sysname> system-view
[Sysname] stp bpdu-protection
```

## Configuring Root Guard

### 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** *interface-list* **root-protection** | Required<br>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** *interface-type interface-number* | — |
| Enable the root guard function on the current port | **stp root-protection** | Required<br>The root guard function is disabled by default. |

### Configuration example

# Enable the root guard function on GigabitEthernet 1/0/1.

1) Perform this configuration in system view

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

```
[Sysname] stp interface GigabitEthernet 1/0/1 root-protection
```

2) Perform this configuration in Ethernet port view

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] stp root-protection
```

## Configuring Loop Guard

### 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** *interface-type interface-number* | — |
| Enable the loop guard function on the current port | **stp loop-protection** | Required<br>The loop guard function is disabled by default. |

### Configuration example

# Enable the loop guard function on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] stp loop-protection
```

## Configuring TC-BPDU Attack Guard

### 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<br>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** *number* | 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 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 a 3com switch 4200G 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 3com switch 4200G 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 3com switch 4200G 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** *interface-type interface-number* | — |
| Enable the digest snooping feature | **stp config-digest-snooping** | Required<br>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<br>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.

**Note**

- To enable the digest snooping feature, the interconnected switches and another manufacturer's switch adopting proprietary spanning tree protocols must be configured with exactly the same MST region-related configurations (including region name, revision level, and VLAN-to-MSTI mapping).
- The digest snooping feature must be enabled on all the 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-MSTI 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

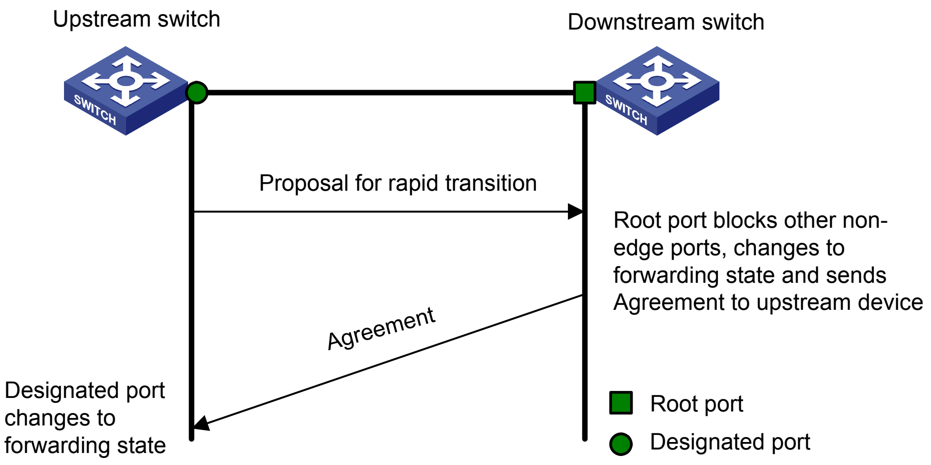
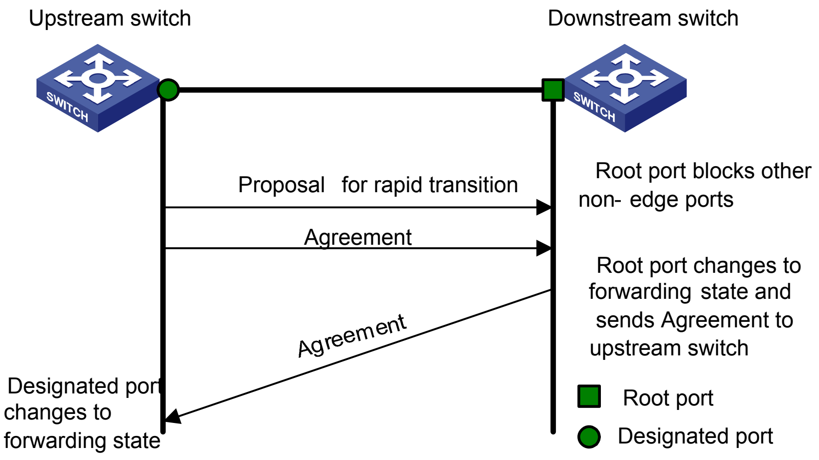

Upstream switch
Downstream switch
SWITCH
SWITCH
Proposal for rapid transition
Root port blocks other non-edge ports, changes to forwarding state and sends Agreement to upstream device
Agreement
Designated port changes to forwarding state
Root port
Designated port

**Figure 1-7** The MSTP rapid transition mechanism


Upstream switch
Downstream switch
SWITCH
SWITCH
Proposal for rapid transition
Root port blocks other non- edge ports
Agreement
Root port changes to forwarding state and sends Agreement to upstream switch
Agreement
Designated port changes to forwarding state
Root port
Designated port

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 3com 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 3com 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 3com 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

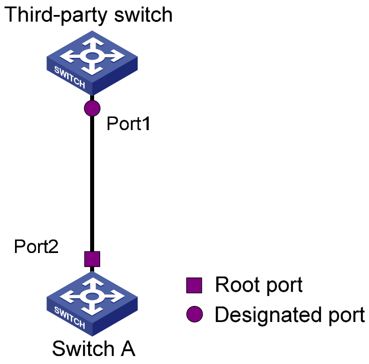
### Configuration prerequisites

As shown in Figure 1-8, a 3com 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 3com 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** *interface-type interface-number* **no-agreement-check** | Required<br>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** *interface-type interface-number* | — |
| Enable the rapid transition feature | **stp no-agreement-check** | Required<br>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.

# STP 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** *instance-id* ] **portlog** | Required<br>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<br>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** *instance-id* ] **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** *instance-id* ] [ **interface** *interface-list* \| **slot** *slot-number* ] [ **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** *interface-list* ] | Available in user view |

# MSTP Configuration Example

### Network requirements

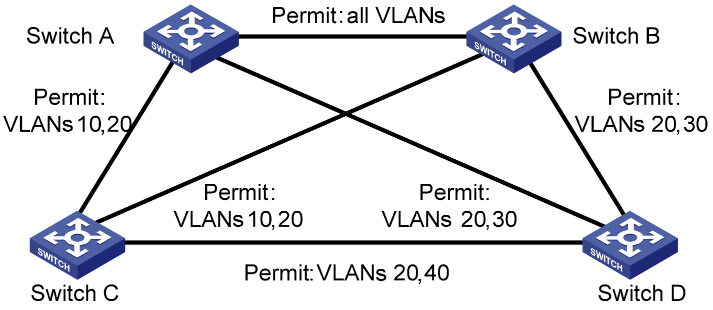
Implement MSTP in the network shown in Figure 1-9 to enable packets of different VLANs to be forwarded along different MSTIs. The detailed configurations are as follows:

- 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 1-9** Network diagram for MSTP configuration



**Note**

The word “permit” shown in Figure 1-9 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-MSTI 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-MSTI 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
```

# Table of Contents

# 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 is used to perform port-level authentication and control of devices connected to the 802.1x-enabled ports. With the 802.1x protocol employed, a user-side device can access the LAN only when it passes the authentication. Those devices that fail to pass the authentication are denied access to the LAN.

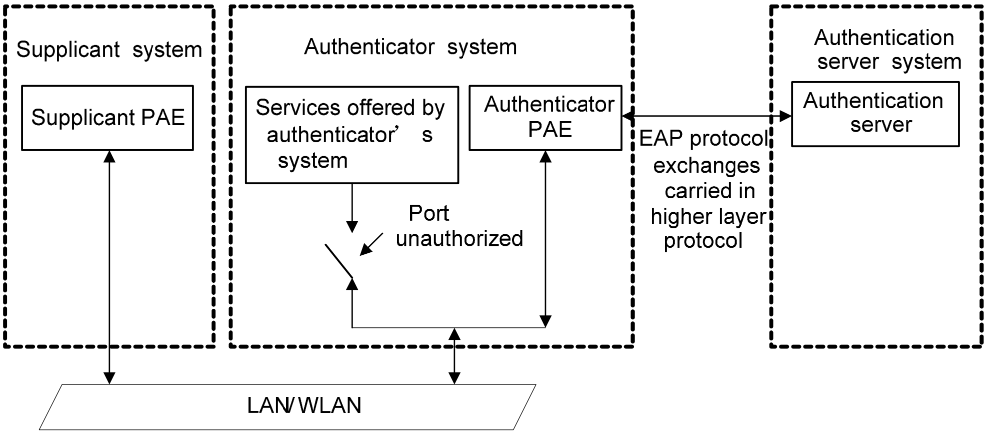
This section covers these topics:

- 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
- Additional 802.1x Features on Switch 4200G

### 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


Supplicant system
Supplicant PAE
Authenticator system
Services offered by authenticator' s system
Authenticator PAE
Port unauthorized
Authentication server system
Authentication server
EAP protocol exchanges carried in higher layer protocol
LAN/WLAN

- The supplicant system is the entity seeking access to the LAN. It resides 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 an 802.1x-capable client program on the supplicant system. Note that the client program must support the extensible authentication protocol over LAN (EAPoL).
- The authenticator system, residing at the other end of the LAN segment, is the entity that authenticates the connected supplicant system. The authenticator system is usually an 802.1x-supported network device, such as a 3Com series switch. It provides the port (physical or logical) for the supplicant system to access the LAN.
- The authentication server system is the entity that provides authentication services to the authenticator system. The authentication server system, usually a RADIUS server, 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 should belong to, priority, and any Access Control Lists (ACLs) to be applied.

There are four additional basic concepts related 802.1x: port access entity (PAE), controlled port and uncontrolled port, the valid direction of a controlled port and the access control method on ports.

### I. 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

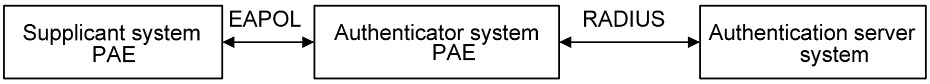
A port of an 3COM series switch can be controlled in the following two ways.

- Port-based control. When a port is under port-based control, 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 control. When a port is under MAC-based control, all supplicant systems connected to the 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



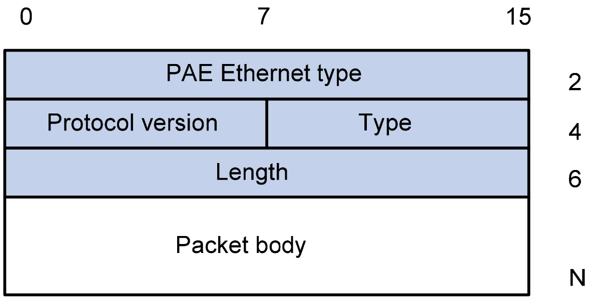
- EAP protocol packets transmitted between the supplicant system PAE and the authenticator system PAE are encapsulated as EAPoL packets.
- EAP protocol packets transmitted between the authenticator system PAE and the RADIUS server can either be encapsulated as EAP over RADIUS (EAPoR) packets or be terminated 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.

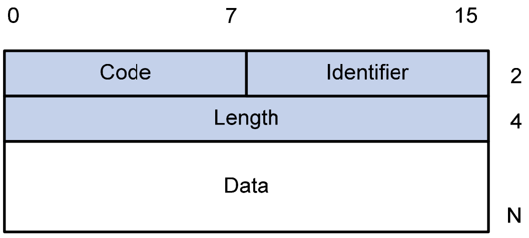
  04: Indicates that the packet is an EAPoL-encapsulated-ASF-Alert packet, which is used to support the alerting messages of Alerting Standards Forum (ASF).
- The Length field indicates the size of the Packet body field. A value of 0 indicates that the Packet Body field does not exist.
- The Packet body 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:

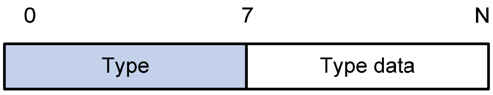
- The Code field indicates the EAP packet type, which can be Request, Response, Success, or Failure.
- The Identifier field is used to match a Response packet with the corresponding Request packet.

- 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



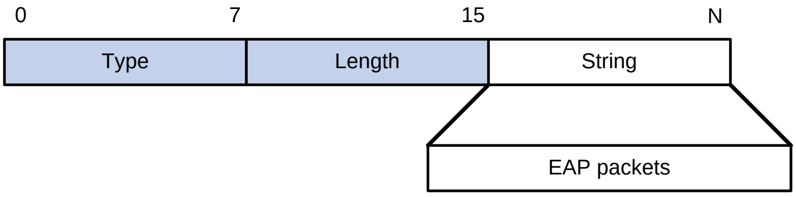
- The Type field indicates the EAP authentication type. A value of 1 indicates Identity and that the packet is used to query the identity of the peer. A value of 4 represents MD5-Challenge (similar to PPP CHAP) and indicates that the packet includes query information.
- The Type Date field differs with types of Request and Response packets.

### Fields added 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.)

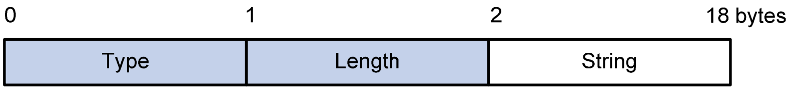
The EAP-message field, whose format is shown in Figure 1-6, is used to encapsulate EAP packets. The maximum size of the string field is 253 bytes. EAP packets with their size larger than 253 bytes are fragmented and are encapsulated in multiple EAP-message fields. The type code of the EAP-message field 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

Switch 4200G can authenticate supplicant systems in EAP terminating mode or EAP relay mode.

### EAP relay mode

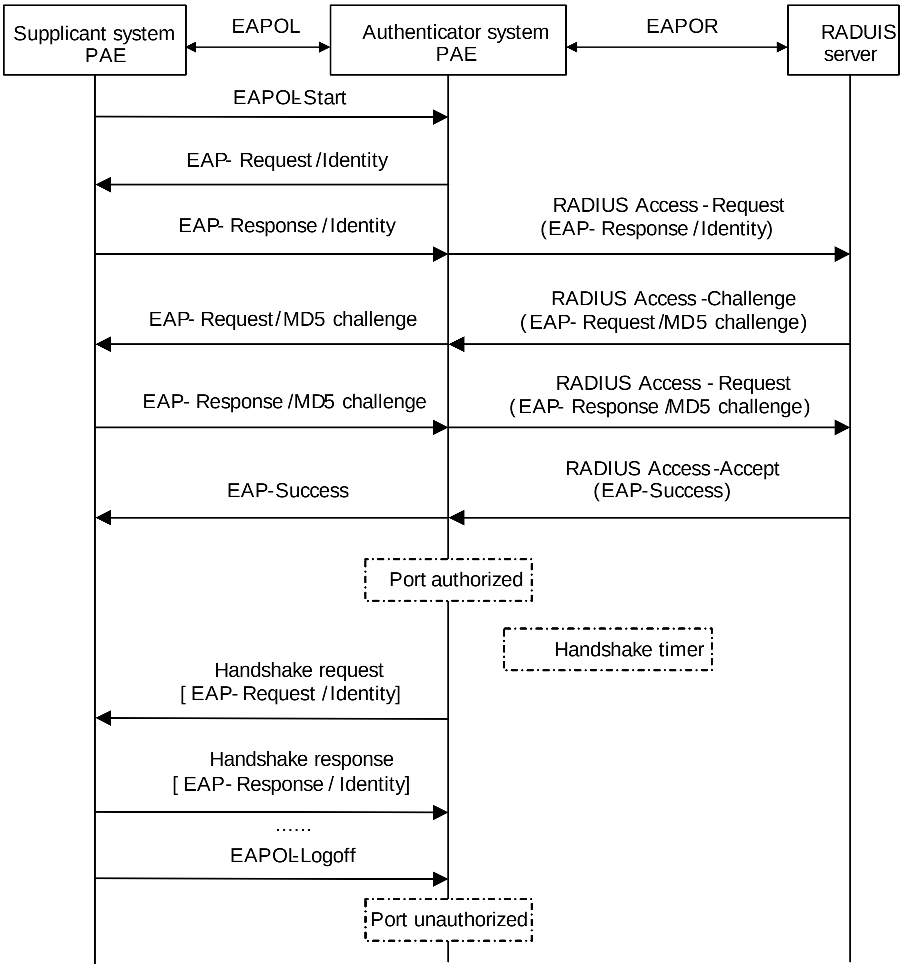
This mode is defined in 802.1x. In this mode, EAP packets are encapsulated in higher level protocol (such as EAPoR) packets to enable them to successfully reach the authentication server. Normally, this mode requires that the RADIUS server support the two newly-added fields: the EAP-message field (with 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)


Supplicant system PAE
EAPOL
Authenticator system PAE
EAPOR
RADUIS server
EAPOL-Start
EAP- Request /Identity
EAP- Response /Identity
RADIUS Access - Request (EAP- Response /Identity)
EAP- Request/MD5 challenge
RADIUS Access -Challenge (EAP- Request/MD5 challenge)
EAP- Response /MD5 challenge
RADIUS Access - Request (EAP- Response /MD5 challenge)
EAP-Success
RADIUS Access -Accept (EAP-Success)
Port authorized
Handshake timer
Handshake request [ EAP- Request / Identity]
Handshake response [ EAP- Response / Identity]
......
EAPOL-Logoff
Port unauthorized

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**

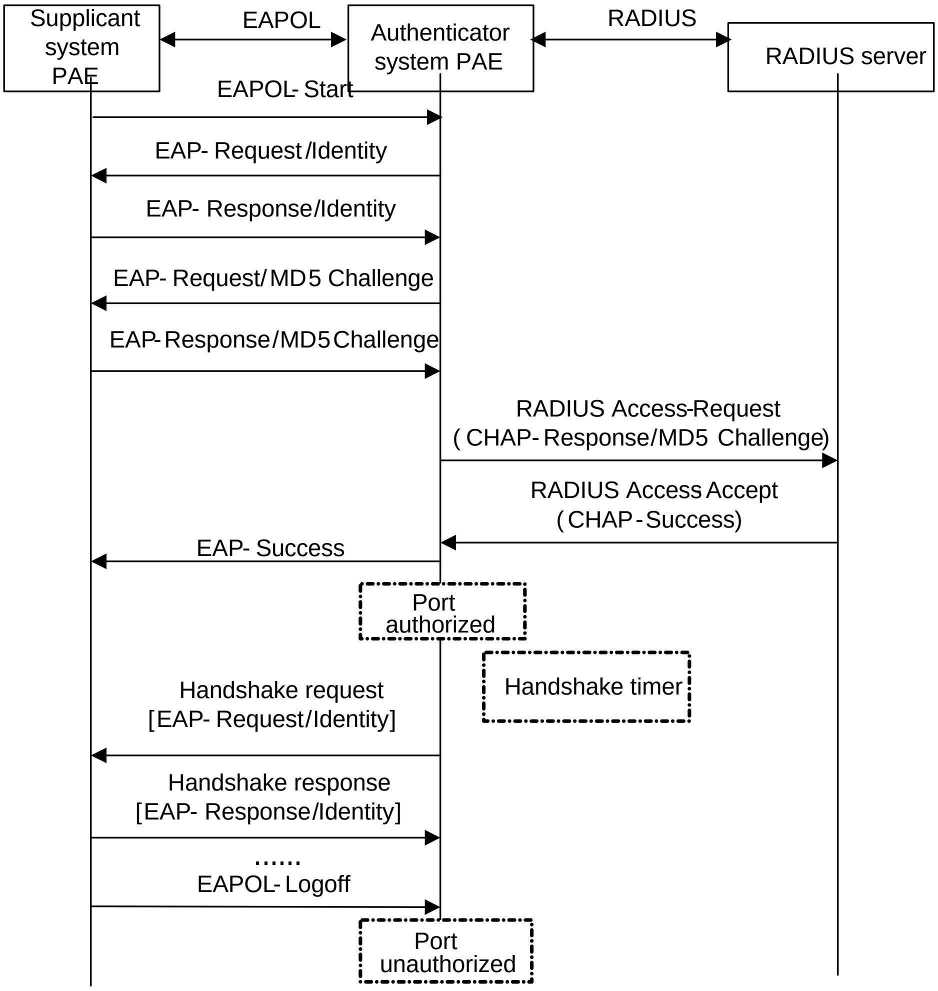
In EAP relay mode, packets are not modified during transmission. Therefore if one of the four ways are used (that is, PEAP, EAP-TLS, EAP-TTLS or EAP-MD5) to authenticate, ensure that the authenticating ways used on the supplicant system and the RADIUS server are the same. However for the switch, you 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 receive version response packets from the supplicant system when the timer expires.

## Additional 802.1x Features on Switch 4200G

In addition to the earlier mentioned 802.1x features, Switch 4200G is also capable of the following:

- Checking supplicant systems for proxies, multiple network adapters, etc. (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

Switch 4200G 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.

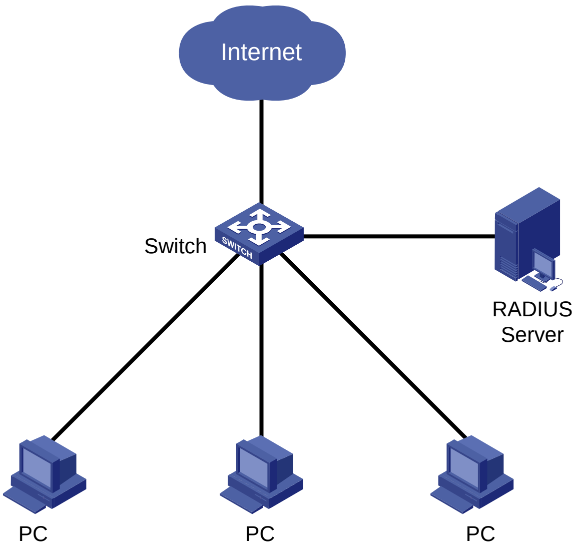
### Enabling 802.1x re-authentication

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.

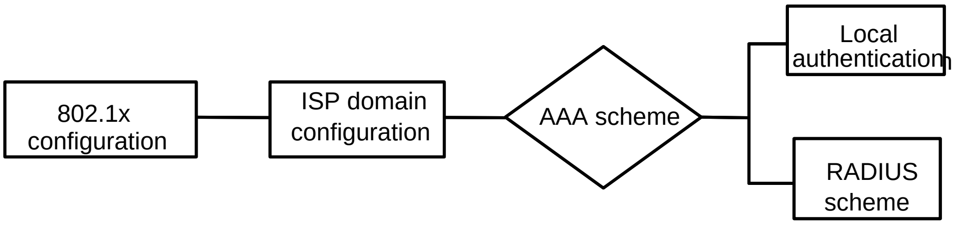
**Note**

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<br>By default, 802.1x is disabled globally. |
| Enable 802.1x for specified ports | In system view | **dot1x interface** *interface-list* | Required<br>By default, 802.1x is disabled on all ports. |
| | In port view | **interface** *interface-type interface-number* | |
| | | **dot1x** | |
| | | **quit** | |
| Set port authorization mode for specified ports | In system view | **dot1x port-control** { **authorized-force** \| **unauthorized-force** \| **auto** } [ **interface** *interface-list* ] | Optional<br>By default, an 802.1x-enabled port operates in the **auto** mode. |
| | In port view | **interface** *interface-type interface-number* | |
| | | **dot1x port-control** { **authorized-force** \| **unauthorized-force** \| **auto** } | |
| | | **quit** | |
| Set access control method for specified ports | In system view | **dot1x port-method** { **macbased** \| **portbased** } [ **interface** *interface-list* ] | Optional<br>The default access control method on a port is MAC-based (that is, the **macbased** keyword is used by default). |
| | In port view | **interface** *interface-type interface-number* | |
| | | **dot1x port-method** { **macbased** \| **portbased** } | |
| | | **quit** | |
| Set authentication method for 802.1x users | | **dot1x authentication-method** { **chap** \| **pap** \| **eap** } | Optional<br>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<br>By default, online user handshaking is enabled. |
| Enter Ethernet port view | **interface** *interface-type interface-number* | — |

**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 the switch itself operates as an authentication server, its authentication method for 802.1x users cannot be configured as EAP.
- Handshake packets are used to test whether a user is online or not. Users need to run the proprietary client software of H3C to respond to the handshake packets.
- As clients not running the H3C client software 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.

## 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** *user-number* [ **interface** *interface-list* ] | Optional<br>By default, a port can accommodate up to 256 users at a time. |
| | In port view | **interface** *interface-type interface-number* | |
| | | **dot1x max-user** *user-number* | |
| | | **quit** | |
| Set the maximum retry times to send request packets | | **dot1x retry** *max-retry-value* | Optional<br>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. |

| To do… | Use the command... | Remarks |
|---|---|---|
| Set 802.1x timers | **dot1x timer** { **handshake-period** *handshake-period-value* \| **quiet-period** *quiet-period-value* \| **server-timeout** *server-timeout-value* \| **supp-timeout** *supp-timeout-value* \| **tx-period** *tx-period-value* \| **ver-period** *ver-period-value* } | Optional<br>The settings of 802.1x timers are as follows.<br>1) handshake-period-value: 15 seconds<br>2) quiet-period-value: 60 seconds<br>3) server-timeout-value: 100 seconds<br>4) supp-timeout-value: 30 seconds<br>5) tx-period-value: 30 seconds<br>6) ver-period-value: 30 seconds |
| Enable the quiet-period timer | **dot1x quiet-period** | Optional<br>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** | — |

| To do... | | Use the command... | Remarks |
|---|---|---|---|
| Enable proxy checking function globally | | **dot1x supp-proxy-check** { **logoff** \| **trap** } | Required<br>By default, the 802.1x proxy checking function is globally disabled. |
| Enable proxy checking for a port/specified ports | In system view | **dot1x supp-proxy-check** { **logoff** \| **trap** } [ **interface** *interface-list* ] | Required<br>By default, the 802.1x proxy checking is disabled on a port. |
| | In port view | **interface** *interface-type interface-number* | |
| | | **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** *interface-list* ] | Required<br>By default, 802.1x client version checking is disabled on a port. |
| | In port view | **interface** *interface-type interface-number* | |
| | | **dot1x version-check** | |
| | | **quit** | |
| Set the maximum number of retires to send version checking request packets | | **dot1x retry-version-max** *max-retry-version-value* | Optional<br>By default, the maximum number of retires to send version checking request packets is 3. |
| Set the client version checking period timer | | **dot1x timer ver-period** *ver-period-value* | Optional<br>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<br>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 the access control method of ports | | **dot1x port-method portbased** | Required<br>The default access control method on a port is MAC-based. That is, the **macbased** keyword is used by default. |
| Enable the guest VLAN function | In system view | **dot1x guest-vlan** *vlan-id* [ **interface** *interface-list* ] | Required<br>By default, the guest VLAN function is disabled. |
| | In port view | **interface** *interface-type interface-number* | |
| | | **dot1x guest-vlan** *vlan-id* | |
| | | **quit** | |

Caution

- The guest VLAN function is available only when the switch operates in the port-based access control 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** *interface-list* ] | Required<br>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** *reauth-period-value* | Optional<br>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

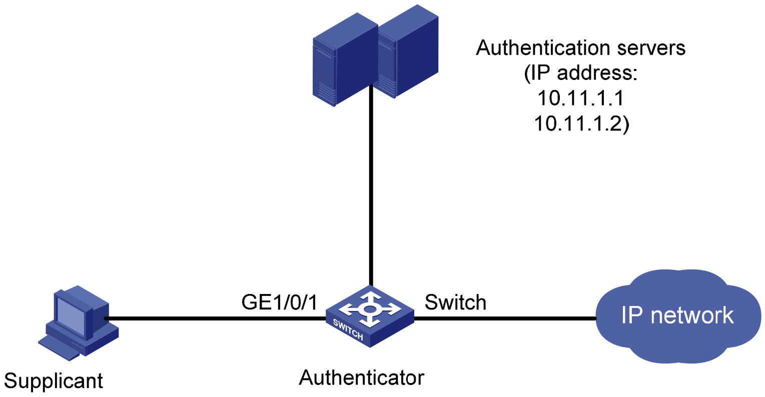
- Authenticate users on all ports to control their accesses to the Internet. The switch operates in MAC-based access control mode.
- All supplicant systems that pass the authentication belong to the default domain named “aabbcc.net”. The domain can accommodate up to 30 users. As for authentication, a 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 GigabitEthernet 1/0/1.

```
[Sysname] dot1x interface GigabitEthernet 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 GigabitEthernet 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 Switch 4200G 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 authorization 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 port authorization mode to **auto** for 802.1x-enabled ports using the **dot1x port-control** command.

## 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** *url-string* | Required |
| Configure a free IP range | **dot1x free-ip** *ip-address* { *mask-address* \| *mask-length* } | Required<br>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 authorization 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** *acl-timeout-value* | Required<br>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 |

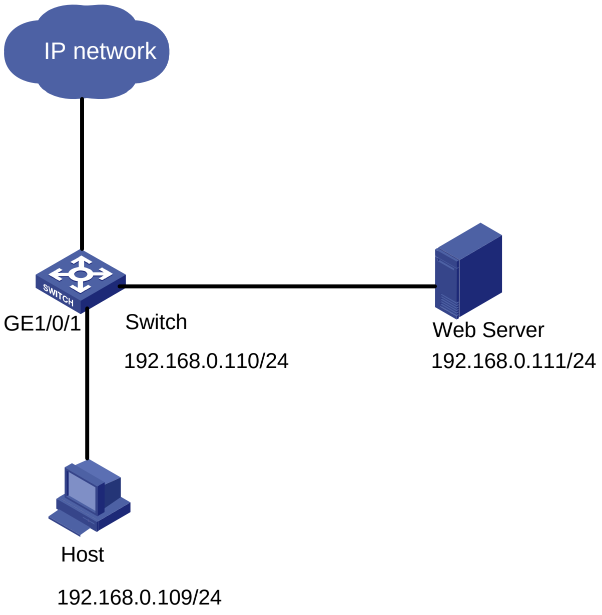
# Quick EAD Deployment Configuration Example

### 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, make sure sure that:

- The Web server is configured properly.
- The default gateway of the PC is configured as the IP address of the Layer-3 virtual interface of the VLAN to which the port that is directly connected with the PC belongs.

# 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 GigabitEthernet 1/0/1.

```
[Sysname] dot1x interface GigabitEthernet 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

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<br>By default, HABP is enabled. |

| To do... | Use the command... | Remarks |
|---|---|---|
| Configure the current switch to be an HABP server | **habp server vlan** *vlan-id* | Required<br>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** *interval* | Optional<br>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<br>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

## System-Guard Overview

At first, you must determine whether the CPU is under attack to implement system guard for the CPU.

You should not determine whether the CPU is under attack just according to whether congestion occurs in a queue. Instead, you must do that in the following ways:

- According to the number of packets processed in the CPU in a time range.
- Or according to the time for one hundred packets to be processed.

If the CPU is under attack, the rate of packets to be processed in the CPU in a certain queue will exceed the threshold value. In this case, you can determine that the CPU is under attack. Through analyzing these packets , you get to know the characteristics of the attack source, and then you can adopt different filtering rules according the characteristics of the attack source. Thus, system guard is implemented.

## Configuring the System-Guard Feature

Through the following configuration, you can enable the system-guard feature, set the threshold for the number of packets when an attack is detected and the length of the isolation after an attack is detected.

### Configuring the System-Guard Feature

**Table 4-1** Configure the system-guard feature

| Operation | Command | Description |
|---|---|---|
| Enter system view | **system-view** | — |
| Enable the system-guard feature | **system-guard enable** | Required<br>By default, the system-guard feature is disabled. |
| Set the threshold for the number of packets when an attack is detected | **system-guard detect-threshold** *threshold-value* | Optional<br>The default threshold value is 200 packets. |
| Set the length of the isolation after an attack is detected | **system-guard timer-interval** *isolate-timer* | Optional<br>By default, the length of the isolation after an attack is detected is 10 minutes. |

## Displaying and Maintaining System-Guard

After the above configuration, execute the **display** command in any view to display the running status of the system-guard feature, and to verify the configuration.

**Table 4-2** Display and maintain system-guard

| Operation | Command |
|---|---|
| Display the record of detected attacks | **display system-guard attack-record** |
| Display the state of the system-guard feature | **display system-guard state** |

# Table of Contents

# 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 3Com switch) acts as the client to communicate with the RADIUS or TACACS server. 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.

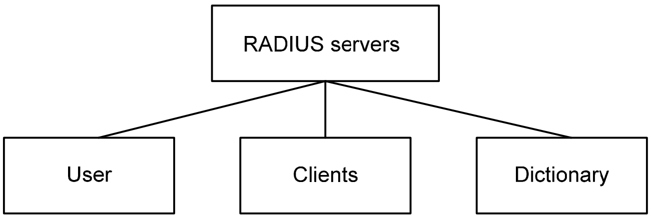
RADIUS operates in the client/server model.

- 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

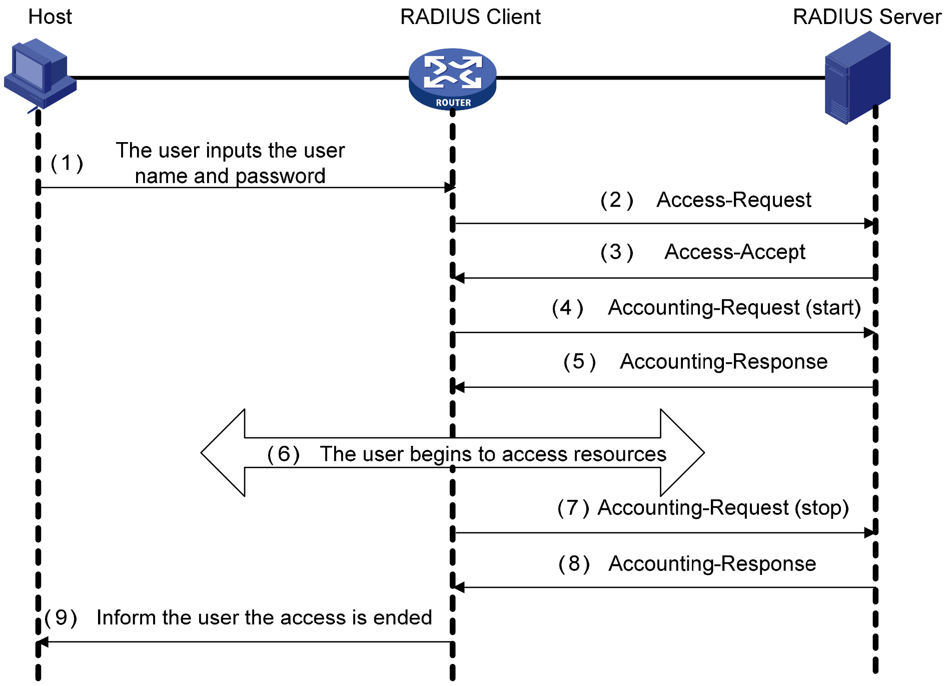


In addition, a RADIUS server can act as a client of some other AAA server to provide authentication or accounting proxy service.

### 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


Host
RADIUS Client
RADIUS Server
ROUTER
(1) The user inputs the user name and password
(2) Access-Request
(3) Access-Accept
(4) Accounting-Request (start)
(5) Accounting-Response
(6) The user begins to access resources
(7) Accounting-Request (stop)
(8) Accounting-Response
(9) Inform the user the access is ended

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.

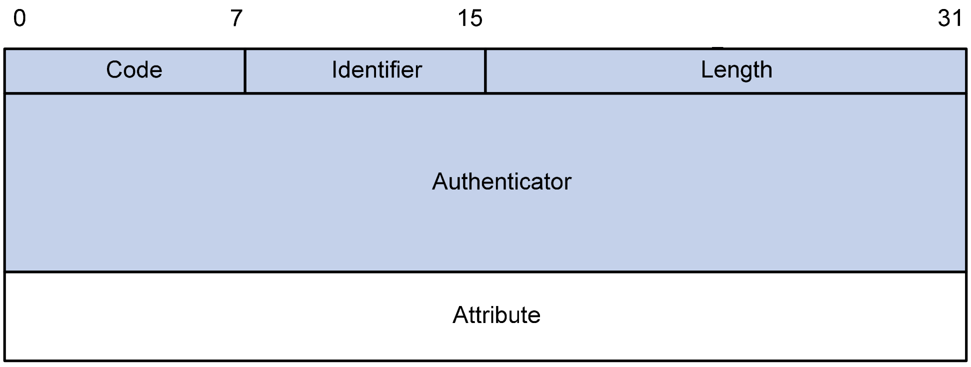
9) The RADIUS server returns a stop-accounting response (Accounting-Response).

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.<br>The client transmits this message to the server to determine if the user can access the network.<br>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.<br>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.<br>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.<br>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).<br>This message carries almost the same attributes as those carried in the Access-Request message. |
| 5 | Accounting-Response | Direction: server->client.<br>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

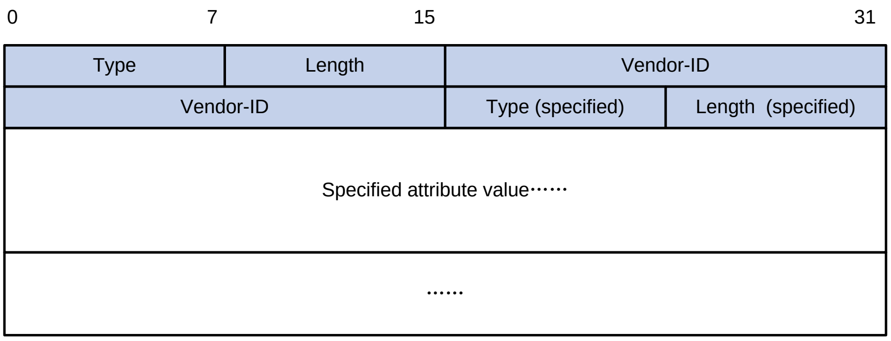
| Type field value | Attribute type | Type field value | Attribute type |
|---|---|---|---|
| 1 | User-Name | 23 | Framed-IPX-Network |
| 2 | User-Password | 24 | State |
| 3 | CHAP-Password | 25 | Class |
| 4 | NAS-IP-Address | 26 | Vendor-Specific |
| 5 | NAS-Port | 27 | Session-Timeout |
| 6 | Service-Type | 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 |

| Type field value | Attribute type | Type field value | Attribute type |
|---|---|---|---|
| 10 | Framed-Routing | 32 | NAS-Identifier |
| 11 | Filter-ID | 33 | Proxy-State |
| 12 | Framed-MTU | 34 | Login-LAT-Service |
| 13 | Framed-Compression | 35 | Login-LAT-Node |
| 14 | Login-IP-Host | 36 | Login-LAT-Group |
| 15 | Login-Service | 37 | Framed-AppleTalk-Link |
| 16 | Login-TCP-Port | 38 | Framed-AppleTalk-Network |
| 17 | (unassigned) | 39 | Framed-AppleTalk-Zone |
| 18 | Reply-Message | 40-59 | (reserved for accounting) |
| 19 | Callback-Number | 60 | CHAP-Challenge |
| 20 | Callback-ID | 61 | NAS-Port-Type |
| 21 | (unassigned) | 62 | Port-Limit |
| 22 | Framed-Route | 63 | Login-LAT-Port |

The RADIUS protocol 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.

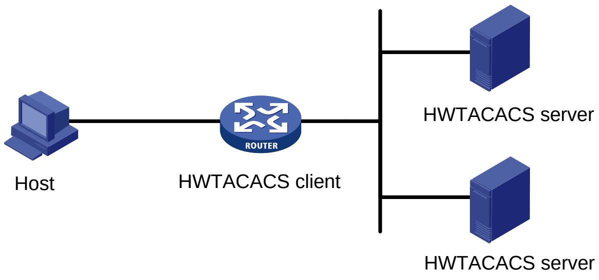
Compared with RADIUS, HWTACACS provides more reliable transmission and encryption, and therefore is more suitable for security control. Table 1-3 lists the primary differences between HWTACACS and RADIUS.

**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 1-50), 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.

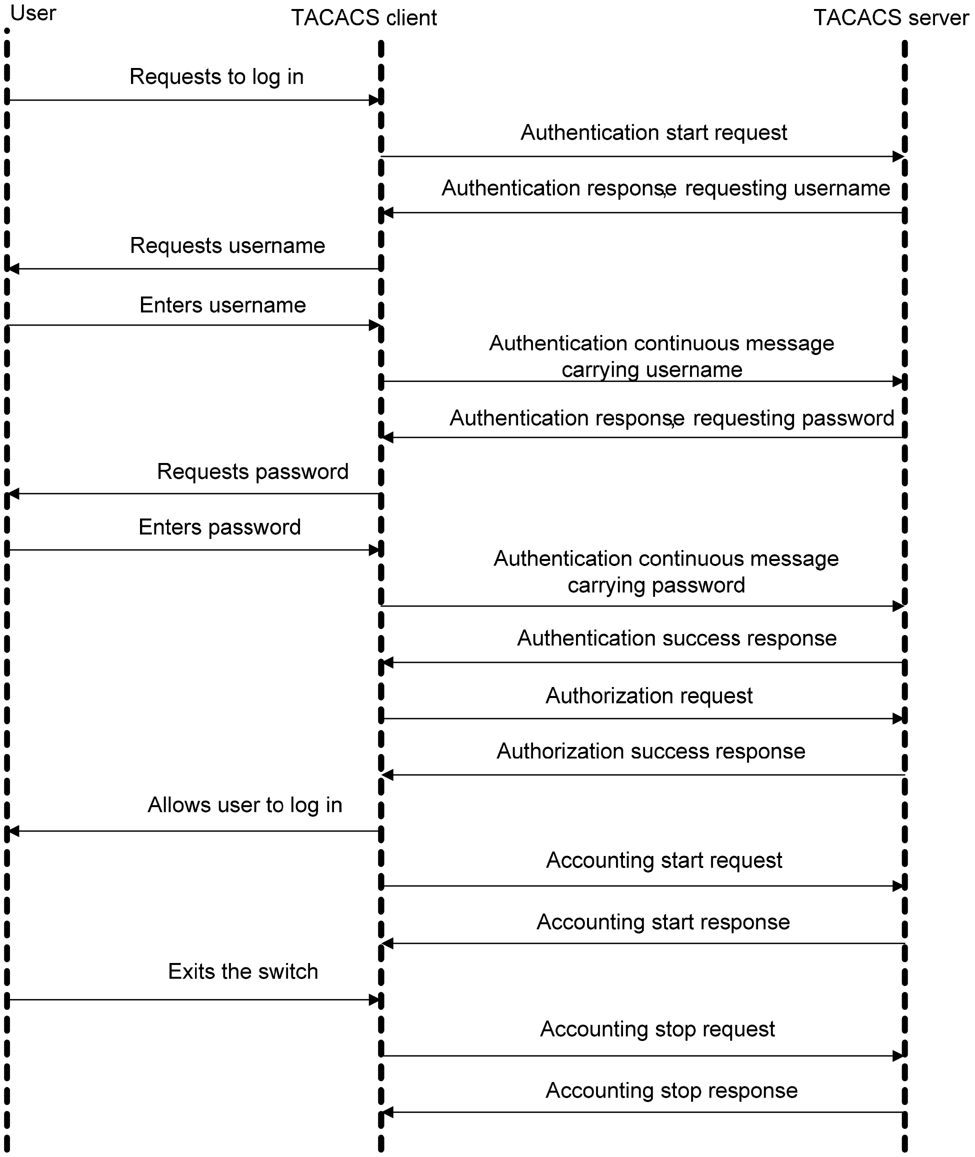
**Figure 1-5** Network diagram for a typical HWTACACS application



### 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


User
TACACS client
TACACS server
Requests to log in
Authentication start request
Authentication response requesting username
Requests username
Enters username
Authentication continuous message carrying username
Authentication response requesting password
Requests password
Enters password
Authentication continuous message carrying password
Authentication success response
Authorization request
Authorization success response
Allows user to log in
Accounting start request
Accounting start response
Exits the switch
Accounting stop request
Accounting stop response

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

## 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<br>• 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<br>With separate AAA schemes, you can specify authentication, authorization and accounting schemes respectively.<br>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<br>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<br>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<br>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<br>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<br>By default, the idle-cut function is disabled. |

| To do… | Use the command… | Remarks |
|---|---|---|
| Set the accounting-optional switch | **accounting optional** | Optional<br>By default, the accounting-optional switch is off. |
| Set the messenger function | **messenger time** { **enable** *limit interval* \| **disable** } | Optional<br>By default, the messenger function is disabled. |

Note that:

- On a Switch 4200G, 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.

**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** | — |
| Create an ISP domain and enter its view, or enter the view of an existing ISP domain | **domain** *isp-name* | Required |
| Configure an AAA scheme for the ISP domain | **scheme** { **local** \| **none** \| **radius-scheme** *radius-scheme-name* [ **local** ] \| **hwtacacs-scheme** *hwtacacs-scheme-name* [ **local** ] } | Required<br>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** *isp-name* | Required |

| To do… | Use the command… | Remarks |
|---|---|---|
| Configure an authentication scheme for the ISP domain | **authentication** { **radius-scheme** *radius-scheme-name* [ **local** ] \| **hwtacacs-scheme** *hwtacacs-scheme-name* [ **local** ] \| **local** \| **none** } | Optional<br>By default, no separate authentication scheme is configured. |
| Configure a HWTACACS authentication scheme for user level switching | **authentication super hwtacacs-scheme** *hwtacacs-scheme-name* | Optional<br>By default, no HWTACACS authentication scheme is configured. |
| Configure an authorization scheme for the ISP domain | **authorization** { **none** \| **hwtacacs-scheme** *hwtacacs-scheme-name* } | Optional<br>By default, no separate authorization scheme is configured. |
| Configure an accounting scheme for the ISP domain | **accounting** { **none** \| **radius-scheme** *radius-scheme-name* \| **hwtacacs-scheme** *hwtacacs-scheme-name* } | Optional<br>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 Switch 4200G adopts 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

The dynamic VLAN assignment feature enables a switch to dynamically add the switch ports of successfully authenticated users to different VLANs according to the attributes assigned by the RADIUS server, so as to control the network resources that different users can access.

Currently, the switch supports the following two types of assigned VLAN IDs: integer and string.

- Integer: If the RADIUS authentication server assigns integer type of VLAN IDs, you can set the VLAN assignment mode to integer on the switch (this is also the default mode on the switch). Then, upon receiving an integer ID assigned by the RADIUS authentication server, the switch adds the port to the VLAN whose VLAN ID is equal to the assigned integer ID. If no such a VLAN exists, the switch first creates a VLAN with the assigned ID, and then adds the port to the newly created VLAN.
- String: If the RADIUS authentication server assigns string type of VLAN IDs, you can set the VLAN assignment mode to string on the switch. Then, upon receiving a string ID assigned by the RADIUS authentication server, the switch compares the ID with existing VLAN names on the switch. If it finds a match, it adds the port to the corresponding VLAN. Otherwise, the VLAN assignment fails and the user fails the authentication.

In actual applications, to use this feature together with Guest VLAN, you should better set port control to port-based mode. 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** *isp-name* | — |
| Set the VLAN assignment mode | **vlan-assignment-mode** { **integer** \| **string** } | Optional<br>By default, the VLAN assignment mode is integer. |
| Create a VLAN and enter its view | **vlan** *vlan-id* | — |
| Set a VLAN name for VLAN assignment | **name** *string* | This operation is required if the VLAN assignment mode is set to string. |

⚠ **Caution**

- In string mode, if the VLAN ID assigned by the RADIUS server is a character string containing only digits (for example, 1024), the switch first regards it as an integer VLAN ID: the switch transforms the string to an integer value and judges if the value is in the valid VLAN ID range; if it is, the switch adds the authenticated port to the VLAN with the integer value as the VLAN ID (VLAN 1024, for example).
- To implement dynamic VLAN assignment on a port where both MSTP and 802.1x are enabled, you must set the MSTP port to an edge port.

## 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** | — |
| Set the password display mode of all local users | **local-user password-display-mode** { **cipher-force** \| **auto** } | Optional<br>By default, the password display mode of all access users is **auto**, indicating the passwords of access users are displayed in the modes set by the **password** command. |
| Add a local user and enter local user view | **local-user** *user-name* | Required<br>By default, there is no local user in the system. |
| Set a password for the local user | **password** { **simple** \| **cipher** } *password* | Required |
| Set the status of the local user | **state** { **active** \| **block** } | Optional<br>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** *level* ] } | Required<br>By default, the system does not authorize the user to access any service. |
| Set the privilege level of the user | **level** *level* | Optional<br>By default, the privilege level of the user is 0. |
| Configure the authorized VLAN for the local user | **authorization vlan** *string* | Required<br>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** *ip-address* \| **mac** *mac-address* \| **idle-cut** *second* \| **access-limit** *max-user-number* \| **vlan** *vlan-id* \| **location** { **nas-ip** *ip-address* **port** *port-number* \| **port** *port-number* } }* | Optional<br>When binding the user to a remote port, you must use **nas-ip** *ip-address* to specify a remote access server IP address (here, *ip-address* is 127.0.0.1 by default, representing this device). When binding the user to a local port, you need not use **nas-ip** *ip-address*. |

⚠ **Caution**

- The following characters are not allowed in the *user-name* string: /:*?<>. And you cannot input more than one "@" in the string.
- After the **local-user password-display-mode cipher-force** command is executed, any password will be displayed in cipher mode even though you specify to display a user password in plain text by using the **password** command.
- If a 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** *isp-name* \| **interface** *interface-type interface-number* \| **ip** *ip-address* \| **mac** *mac-address* \| **radius-scheme** *radius-scheme-name* \| **vlan** *vlan-id* \| **ucibindex** *ucib-index* \| **user-name** *user-name* } | Required |

**Note**

You can use the **display connection** command to view the connections of Telnet users, but you cannot use the **cut connection** command to cut down their connections.

## RADIUS Configuration Task List

3Com'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 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<br>By default, RADIUS authentication port is enabled. |
| Create a RADIUS scheme and enter its view | **radius scheme** *radius-scheme-name* | Required<br>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** | — |

| To do… | Use the command… | Remarks |
|---|---|---|
| Create a RADIUS scheme and enter its view | **radius scheme** *radius-scheme-name* | Required<br>By default, a RADIUS scheme named "system" has already been created in the system. |
| Set the IP address and port number of the primary RADIUS authentication/authorization server | **primary authentication** *ip-address* [ *port-number* ] | Required<br>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** *ip-address* [ *port-number* ] | Optional<br>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 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** *radius-scheme-name* | Required<br>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 accounting server | **primary accounting** *ip-address* [ *port-number* ] | Required<br>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. |

| To do… | Use the command… | Remarks |
|---|---|---|
| Set the IP address and port number of the secondary RADIUS accounting server | **secondary accounting** *ip-address* [ *port-number* ] | Optional<br>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<br>By default, stop-accounting request buffering is enabled. |
| Set the maximum number of transmission attempts of a buffered stop-accounting request. | **retry stop-accounting** *retry-times* | Optional<br>By default, the system tries at most 500 times to transmit a buffered stop-accounting request. |
| Set the maximum allowed number of continuous real-time accounting failures | **retry realtime-accounting** *retry-times* | Optional<br>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** *radius-scheme-name* | Required<br>By default, a RADIUS scheme named "system" has already been created in the system. |
| Set a shared key for RADIUS authentication/authorization messages | **key authentication** *string* | Required<br>By default, no shared key is created. |
| Set a shared key for RADIUS accounting messages | **key accounting** *string* | Required<br>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** *radius-scheme-name* | Required<br>By default, a RADIUS scheme named "system" has already been created in the system. |
| Set the maximum number of RADIUS request transmission attempts | **retry** *retry-times* | Optional<br>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** | — |

| To do… | Use the command… | Remarks |
|---|---|---|
| Create a RADIUS scheme and enter its view | **radius scheme** *radius-scheme-name* | Required<br>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** *radius-scheme-name* | Required<br>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<br>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** *radius-scheme-name* | Required<br>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<br>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<br>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<br>By default, the MAC address format is XXXX-XXXX-XXXX, in lowercase. |
| Set the source IP address of outgoing RADIUS messages | RADIUS scheme view<br>**nas-ip** *ip-address* | Optional<br>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<br>**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<br>By default, the UDP ports for local RADIUS services are enabled. |
| Configure the parameters of the local RADIUS server | **local-server nas-ip** *ip-address* **key** *password* | Required<br>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.

## 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** *radius-scheme-name* | Required<br>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** *seconds* | Optional<br>By default, the response timeout time of RADIUS servers is three seconds. |
| Set the time that the switch waits before it try to re-communicate with primary server and restore the status of the primary server to active | **timer quiet** *minutes* | Optional<br>By default, the switch waits five minutes before it restores the status of the primary server to active. |
| Set the real-time accounting interval | **timer realtime-accounting** *minutes* | Optional<br>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<br>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** *radius-scheme-name* | — |
| Enable the user re-authentication at restart function | **accounting-on enable** [ **send** *times* \| **interval** *interval* ] | By default, this function is disabled.<br>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** *hwtacacs-scheme-name* | Required<br>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** *hwtacacs-scheme-name* | Required<br>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** *ip-address* [ *port* ] | Required<br>By default, the IP address of the primary authentication server is 0.0.0.0, and the port number is 0. |
| Set the IP address and port number of the secondary TACACS authentication server | **secondary authentication** *ip-address* [ *port* ] | Optional<br>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** *hwtacacs-scheme-name* | Required<br>By default, no HWTACACS scheme exists. |
| Set the IP address and port number of the primary TACACS authorization server | **primary authorization** *ip-address* [ *port* ] | Required<br>By default, the IP address of the primary authorization server is 0.0.0.0, and the port number is 0. |
| Set the IP address and port number of the secondary TACACS authorization server | **secondary authorization** *ip-address* [ *port* ] | Optional<br>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** *hwtacacs-scheme-name* | Required<br>By default, no HWTACACS scheme exists. |
| Set the IP address and port number of the primary TACACS accounting server | **primary accounting** *ip-address* [ *port* ] | Required<br>By default, the IP address of the primary accounting server is 0.0.0.0, and the port number is 0. |
| Set the IP address and port number of the secondary TACACS accounting server | **secondary accounting** *ip-address* [ *port* ] | Required<br>By default, the IP address of the secondary accounting server is 0.0.0.0, and the port number is 0. |
| Enable the stop-accounting message retransmission function and set the maximum number of transmission attempts of a buffered stop-accounting message | **retry stop-accounting** *retry-times* | Optional<br>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** *hwtacacs-scheme-name* | Required<br>By default, no HWTACACS scheme exists. |
| Set a shared key for HWTACACS authentication, authorization or accounting messages | **key** { **accounting** \| **authorization** \| **authentication** } *string* | Required<br>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** *hwtacacs-scheme-name* | Required<br>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<br>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<br>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<br>**nas-ip** *ip-address* | Optional<br>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<br>**hwtacacs nas-ip** *ip-address* | |

⚠ **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** *hwtacacs-scheme-name* | Required<br>By default, no HWTACACS scheme exists. |
| Set the response timeout time of TACACS servers | **timer response-timeout** *seconds* | Optional<br>By default, the response timeout time is five seconds. |
| Set the time that the switch must wait before it can restore the status of the primary server to active | **timer quiet** *minutes* | Optional<br>By default, the switch must wait five minutes before it can restore the status of the primary server to active. |
| Set the real-time accounting interval | **timer realtime-accounting** *minutes* | Optional<br>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** [ *isp-name* ] | Available in any view |
| Display information about user connections | **display connection** [ **access-type** { **dot1x** \| **mac-authentication** } \| **domain** *isp-name* \| **interface** *interface-type interface-number* \| **ip** *ip-address* \| **mac** *mac-address* \| **radius-scheme** *radius-scheme-name* \| **hwtacacs-scheme** *hwtacacs-scheme-name* \| **vlan** *vlan-id* \| **ucibindex** *ucib-index* \| **user-name** *user-name* ] | |
| Display information about local users | **display local-user** [ **domain** *isp-name* \| **idle-cut** { **disable** \| **enable** } \| **vlan** *vlan-id* \| **service-type** { **ftp** \| **lan-access** \| **ssh** \| **telnet** \| **terminal** } \| **state** { **active** \| **block** } \| **user-name** *user-name* ] | |

## 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** [ *radius-scheme-name* ] | |
| Display RADIUS message statistics | **display radius statistics** | |
| Display buffered non-response stop-accounting requests | **display stop-accounting-buffer** { **radius-scheme** *radius-scheme-name* \| **session-id** *session-id* \| **time-range** *start-time stop-time* \| **user-name** *user-name* } | |
| Delete buffered non-response stop-accounting requests | **reset stop-accounting-buffer** { **radius-scheme** *radius-scheme-name* \| **session-id** *session-id* \| **time-range** *start-time stop-time* \| **user-name** *user-name* } | Available in user view |
| 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** [ *hwtacacs-scheme-name* [ **statistics** ] ] | Available in any view |

| To do… | Use the command… | Remarks |
|---|---|---|
| Display buffered non-response stop-accounting requests | **display stop-accounting-buffer** { **hwtacacs-scheme** *hwtacacs-scheme-name* | |
| 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** *hwtacacs-scheme-name* | |

# 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

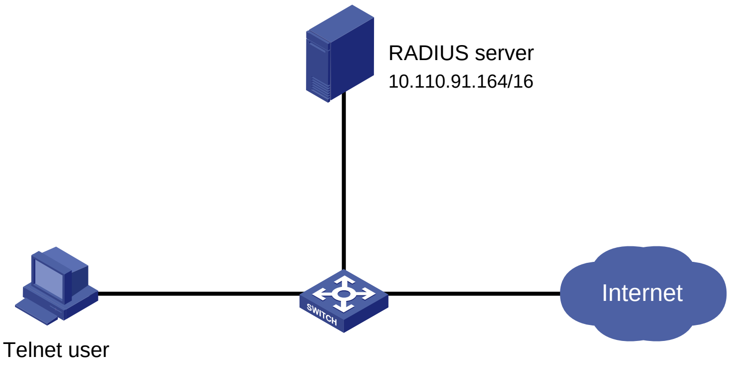
In the network environment shown in Figure 2-1, you are required to configure the switch so that the Telnet users logging into the switch are authenticated by the RADIUS server.

- 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 2-1** 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**

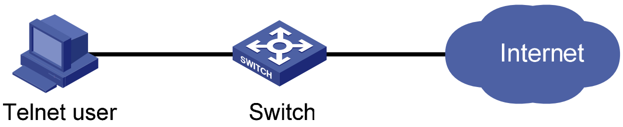
The configuration procedure for local authentication of FTP users is similar to that for Telnet users. The following text only takes Telnet users as example to describe the configuration procedure for local authentication.

### Network requirements

In the network environment shown in Figure 2-2, you are required to configure the switch so that the Telnet users logging into the switch are authenticated locally.

### Network diagram

**Figure 2-2** 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

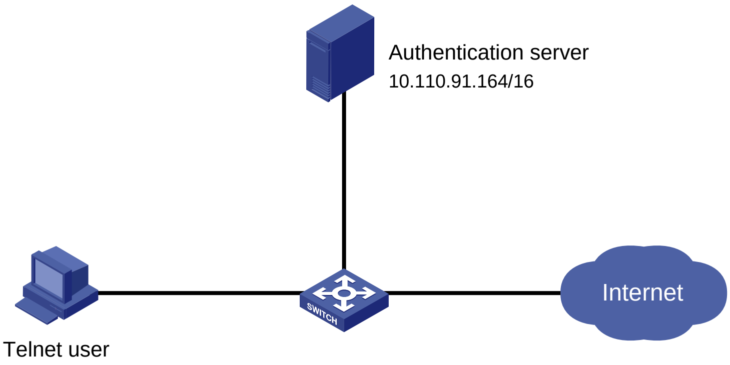
You are required to configure the switch so that the Telnet users logging into the switch are authenticated and authorized by the TACACS server.

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 2-3** 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
```

# 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.

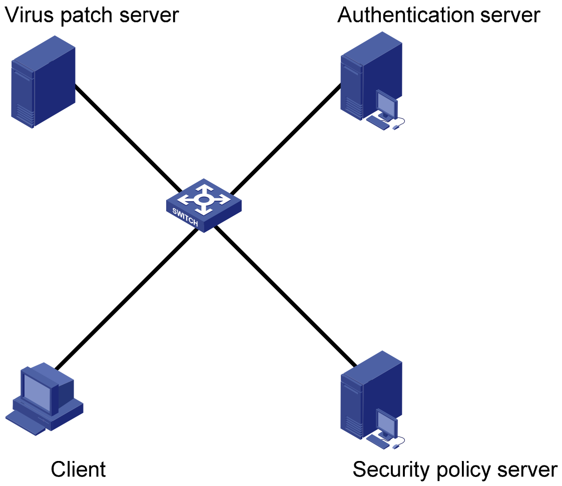
With EAD, a switch:

- 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 and packet scheduling priority 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



## 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** *radius-scheme-name* | — |
| Configure the RADIUS server type to **extended** | **server-type extended** | Required |
| Configure the IP address of a security policy server | **security-policy-server** *ip-address* | Required<br>Each RADIUS scheme supports up to eight IP addresses of security policy servers. |

# EAD Configuration Example

## Network requirements

In Figure 3-2:

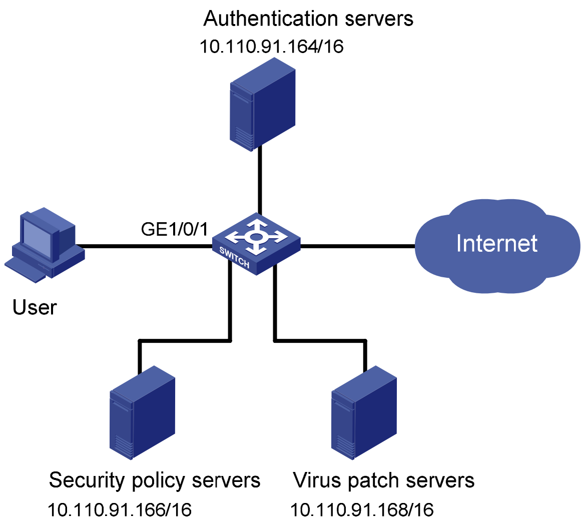
- A user is connected to GigabitEthernet 1/0/1 on the switch.
- The user adopts 802.1x client supporting EAD extended function.
- You are required to configure the switch to use RADIUS server for remote user authentication and use security policy server for EAD control on users.

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 MAC Address Authentication Configuration

When configuring MAC address authentication, go to these sections for information you are interested:

## 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 Switch 4200G, 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 combination of 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.

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<br>Disabled by default |
| Enable MAC address authentication for the specified port(s) or the current port | In system view | **mac-authentication interface** *interface-list* | Use either method<br>Disabled by default |
| | In interface view | **interface** *interface-type interface-number* | |
| | | **mac-authentication** | |

| To do... | Use the command... | | Remarks |
|---|---|---|---|
| | | **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** *password* ] | | Optional<br>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<br>By default, the user name is "mac" and no password is configured. |
| | Configure the user name | **mac-authentication authusername** *username* | |
| | Configure the password | **mac-authentication authpassword** *password* | |
| Specify an ISP domain for MAC address authentication | **mac-authentication domain** *isp-name* | | Required<br>The default ISP domain (default domain) is used by default. |
| Configure the MAC address authentication timers | **mac-authentication timer** { **offline-detect** *offline-detect-value* \| **quiet** *quiet-value* \| **server-timeout** *server-timeout-value* } | | Optional<br>The default timeout values are as follows:<br>300 seconds for offline detect timer;<br>60 seconds for quiet timer; and<br>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** *interface-type interface-number* | — |
| Configure the Guest VLAN for the current port | **mac-authentication guest-vlan** *vlan-id* | Required<br>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** *interval* | Optional<br>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** *interface-type interface-number* | — |
| Configure the maximum number of MAC address authentication users allowed to access a port | **mac-authentication max-auth-num** *user-number* | Required<br>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** *interface-list* ] | Available in any view |
| Clear the statistics of global or on-port MAC address authentication | **reset mac-authentication statistics** [ **interface** *interface-type interface-number* ] | Available in user view |

# MAC Address Authentication Configuration Examples

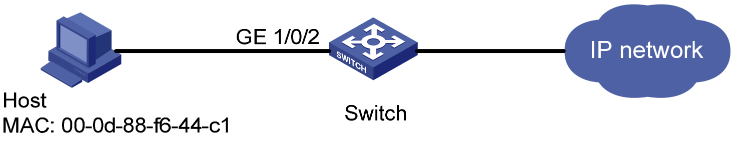
## Network requirements

As illustrated in Figure 1-10, a supplicant is connected to the switch through port GigabitEthernet 1/0/2.

- MAC address authentication is required on port GigabitEthernet 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 GigabitEthernet 1/0/2.

```
<Sysname> system-view
[Sysname] mac-authentication interface GigabitEthernet 1/0/2
```

# Set the user name in MAC address mode for MAC address authentication, requiring hyphened 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 configuaration.)

```
[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 GigabitEthernet 1/0/2.

# Table of Contents

# 1 IP Addressing Configuration

**Note**

The term IP address used throughout this chapter refers to IPv4 address. For details about IPv6 address, refer to *IPv6 Management*.

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

- IP Addressing Overview
- Configuring IP Addresses
- Displaying IP Addressing Configuration
- VLAN Interface IP Address Configuration Examples

## IP Addressing Overview

### IP Address Classes

On an IP network, a 32-bit address is used to identify a host. An example is 00001010000000010000000100000001 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.

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

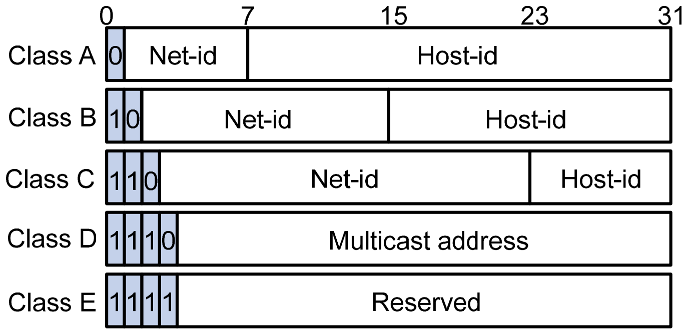


Table 1-1 describes the address ranges of these five classes.

**Table 1-1** IP address classes and ranges

| Class | Address range | Remarks |
|---|---|---|
| A | 0.0.0.0 to 127.255.255.255 | The IP address 0.0.0.0 is used by a host at bootstrap for temporary communication. This address is never a valid destination address.<br>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 addresses |
| E | 240.0.0.0 to 255.255.255.255 | Reserved for future use except for the broadcast address 255.255.255.255. |

## Special IP Addresses

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

- IP address with an all-zero 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-zero host ID: Identifies a network.
- IP address with an all-one 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.

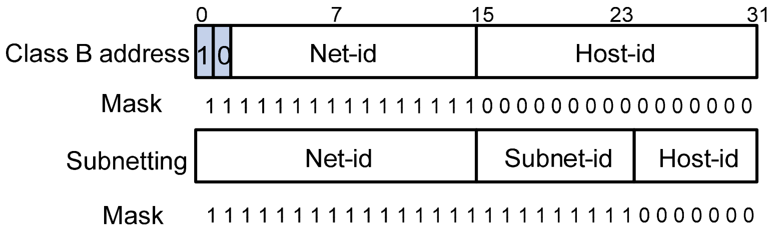
## Subnetting and Masking

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



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 for 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-zero 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.

## Protocols and Standards

- RFC 1366, *Guidelines for Management of IP Address Space*
- RFC 1367, *Schedule for IP Address Space Management Guidelines*

# Configuring IP Addresses

S4200G Series Ethernet Switches support assigning IP addresses to loopback interfaces and VLAN interfaces.

A loopback interface is a virtual interface. The physical layer state and link layer protocols of a loopback interface are always up unless the loopback interface is manually shut down. A loopback interface can be configured with an IP address, so routing protocols can be enabled on a loopback interface, and a loopback interface is capable of sending and receiving routing protocol packets.

Each VLAN needs an IP address so that it can be addressed. For more information about VLAN interfaces, refer to *VLAN Operation* in this manual*.*

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, refer to the part discussing DHCP.

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

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter interface view | **interface** *interface-type interface-number* | — |
| Assign an IP address to the Interface | **ip address** *ip-address* { *mask* \| *mask-length* } | Required<br>No IP address is assigned by default. |

Note

For saving IP address resources, the IP address of a Loopback interface is automatically configured with a 32-bit mask.

## Displaying IP Addressing Configuration

| To do… | Use the command… | Remarks |
|---|---|---|
| Display information about a specified or all Layer 3 interfaces | **display ip interface** [ *interface-type* *interface-number* ] | Available in any view |
| Display brief configuration information about a specified or all Layer 3 interfaces | **display ip interface brief** [ *interface-type* [ *interface-number* ] ] | |

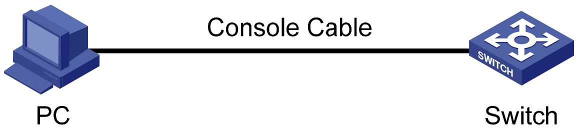
## VLAN Interface IP Address Configuration Examples

### 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
```

# 2 IP Performance Optimization Configuration

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

- IP Performance Overview
- Configuring IP Performance Optimization
- Displaying and Maintaining IP Performance Optimization Configuration

## IP Performance Overview

### Introduction to IP Performance Configuration

In some network environments, you can adjust the IP parameters to achieve best network performance. The IP performance optimization configuration supported by S4200G Series Ethernet Switches includes:

- Configuring TCP attributes
- Disabling ICMP to send error packets

### 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 by viewing the FIB table. Each FIB entry includes: destination address/mask length, next hop, current flag, timestamp, and outbound interface.

When the switch runs normally, its FIB table and routing table have the same contents.

### Protocols and Standards

- RFC 793, *Transmission Control Protocol*
- RFC 1323, *TCP Extensions for High Performance*

## Configuring IP Performance Optimization

### IP Performance Optimization Configuration Task List

Complete the following tasks to configure IP performance Optimization:

| Task | Remarks |
|---|---|
| Configuring TCP Attributes | Optional |
| Disabling Sending of ICMP Error Packets | 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 packet is received within the synwait timer interval, the TCP connection cannot be created.
- finwait timer: When a TCP connection is changed into FIN_WAIT_2 state, the finwait timer is started. If no FIN packet is received within the timer timeout, the TCP connection will be terminated. If a FIN packet is received, the TCP connection state changes to TIME_WAIT. If a non-FIN packet is received, the system restarts the timer upon 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 the TCP synwait timer | **tcp timer syn-timeout** *time-value* | Optional<br>75 seconds by default. |
| Configure the TCP finwait timer | **tcp timer fin-timeout** *time-value* | Optional<br>675 seconds by default. |
| Configure the size of TCP receive/send buffer | **tcp window** *window-size* | Optional<br>8 kilobytes by default. |

## Disabling Sending of ICMP Error Packets

Sending error packets is a major function of the Internet Control Message Protocol (ICMP). 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 management.

### Advantages of sending ICMP error packets

ICMP redirect packets and destination unreachable packets are two kinds of ICMP error packets. Their sending conditions and functions are as follows.

1) Sending ICMP redirect packets

A host may have only a default route to the default gateway in its routing table after startup. The default gateway will send an ICMP redirect packet to the source host, telling it to reselect a better next hop to send the subsequent packets, if the following conditions are satisfied:

- The receiving and forwarding interfaces are the same.
- The selected route has not been created or modified by any ICMP redirect packet.
- The selected route is not the default route.
- There is no source route option in the data packet.

ICMP redirect packets simplify host administration and enables a host to gradually establish a sound routing table.

2) Sending ICMP destination unreachable packets

If a device receives an IP packet with an unreachable destination, it will drop the packet and send an ICMP destination unreachable error packet to the source.

Conditions for sending an ICMP unreachable packet:

- If neither a route nor the default route for forwarding a packet is available, the device will send a “network unreachable” ICMP error packet.

- If the destination of a packet is local while the transport layer protocol of the packet is not supported by the local device, the device sends a “protocol unreachable” ICMP error packet to the source.
- When receiving a packet with the destination being local and transport layer protocol being UDP, if the packet’s port number does not match the running process, the device will send the source a “port unreachable” ICMP error packet.
- If the source uses “strict source routing" to send packets, but the intermediate device finds that the next hop specified by the source is not directly connected, the device will send the source a “source routing failure” ICMP error packet.
- When forwarding a packet, if the MTU of the sending interface is smaller than the packet but the packet has “Don’t Fragment” set, the device will send the source a “fragmentation needed and Don’t Fragment (DF)-set” ICMP error packet.

### Disadvantages of sending ICMP error packets

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 a device receives a lot of malicious packets that cause it to send ICMP error packets, its 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.

To prevent the above mentioned problems, you can disable the device from sending such ICMP error packets.

Follow these steps to disable sending ICMP error packets:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Disable sending of ICMP redirects | **undo icmp redirect send** | Required<br>Enabled by default. |
| Disable sending of ICMP destination unreachable packets | **undo icmp unreach send** | Required<br>Enabled by default. |

## Displaying and Maintaining IP Performance Optimization 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** [ **socktype** *sock-type* ] [ *task-id socket-id* ] | |

| To do… | Use the command… | Remarks |
|---|---|---|
| Display the forwarding information base (FIB) entries | **display fib** | |
| Display the FIB entries matching the destination IP address | **display fib** *ip_address1* [ { *mask1* **\|** *mask-length1* } [ *ip_address2* { *mask2* **\|** *mask-length2* } **\| longer** ] **\| longer** ] | |
| Display the FIB entries permitted by a specific ACL | **display fib acl** *number* | |
| Display the FIB entries in the buffer which begin with, include or exclude the specified character string. | **display fib** \| { **begin \| include \| exclude** } *regular-expression* | |
| Display FIB statistics | **display fib statistics** | |
| 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** | |

# Table of Contents

# 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

## 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

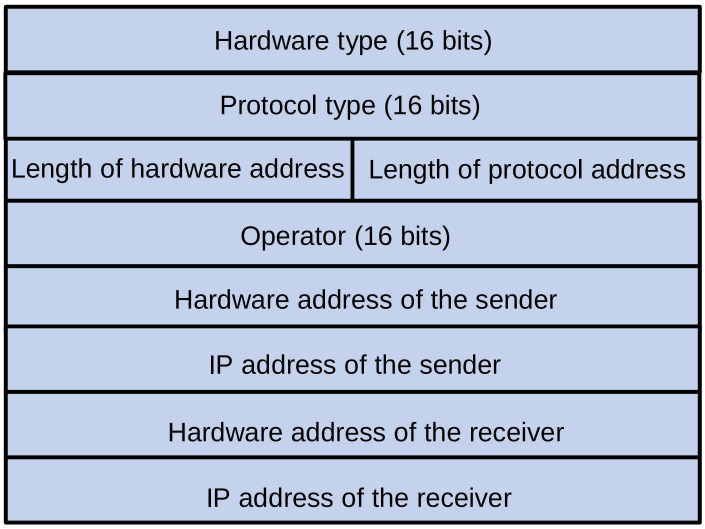

Hardware type (16 bits)
Protocol type (16 bits)
Length of hardware address
Length of protocol address
Operator (16 bits)
Hardware address of the sender
IP address of the sender
Hardware address of the receiver
IP address of the receiver

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:<br>1: ARP request packets<br>2: ARP reply packets<br>3: RARP request packets<br>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.<br>For an ARP reply packet, this field carries the hardware address of the receiver. |
| IP address of the receiver | IP address of the receiver |

**Table 1-2** Description on the values of the hardware type field

| Value | Description |
|---|---|
| 1 | Ethernet |
| 2 | Experimental Ethernet |
| 3 | X.25 |
| 4 | Proteon ProNET (Token Ring) |

| Value | Description |
|---|---|
| 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. S4200G series Ethernet switches provide the **display arp** command to display the information about ARP mapping entries.

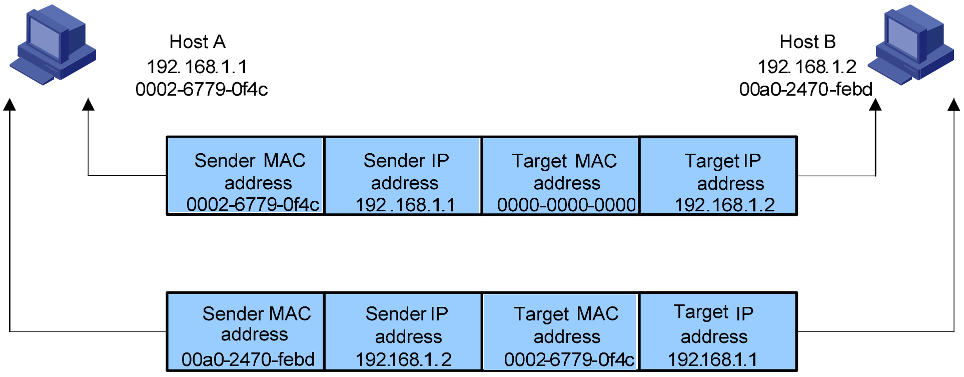
ARP entries in an S4200G series Ethernet switch can either be static entries or dynamic entries, as described in Table 1-3.

**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


Host A
192.168.1.1
0002-6779-0f4c
Host B
192.168.1.2
00a0-2470-febd
Sender MAC address 0002-6779-0f4c
Sender IP address 192.168.1.1
Target MAC address 0000-0000-0000
Target IP address 192.168.1.2
Sender MAC address 00a0-2470-febd
Sender IP address 192168.1.2
Target MAC address 0002-6779-0f4c
Target IP address 192168.1.1

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:

1) 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.

2) 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.

3) 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.
4) 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.

# 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** *ip-address mac-address* [ *vlan-id interface-type interface-number* ] | Optional<br>By default, the ARP mapping table is empty, and entries are created dynamically by ARP. |
| Configure the ARP aging timer | **arp timer aging** *aging-time* | Optional<br>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<br>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** | — |
| Enable the gratuitous ARP packet learning function | **gratuitous-arp-learning enable** | Optional<br>Enabled by default. |

Note

The sending of gratuitous ARP packets is enabled as long as an S4200G 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** \| *ip-address* ] | 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** } *regular-expression* | |
| Display the number of the ARP entries of a specified type | **display arp count** [ [ **dynamic** \| **static** ] [ \| { **begin** \| **include** \| **exclude** } *regular-expression* ] \| *ip-address* ] | |
| Display the statistics about the untrusted ARP packets dropped by the specified port | **display arp detection statistics interface** *interface-type interface-number* | |
| Display the setting of the ARP aging timer | **display arp timer aging** | |

| To do… | Use the command… | Remarks |
|---|---|---|
| Clear specific ARP entries | **reset arp** [ **dynamic** \| **static** \| **interface** *interface-type interface-number* ] | Available in user view |

# ARP Configuration Examples

## Network requirements

- Disable ARP entry check on the switch.
- 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 GigabitEthernet 1/0/10 of VLAN 1.

## Configuration procedure

```
<Sysname> system-view
[Sysname] undo arp check enable
[Sysname] arp timer aging 10
[Sysname] arp static 192.168.1.1 000f-e201-0000 1 GigabitEthernet 1/0/10
```

# Table of Contents

# 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

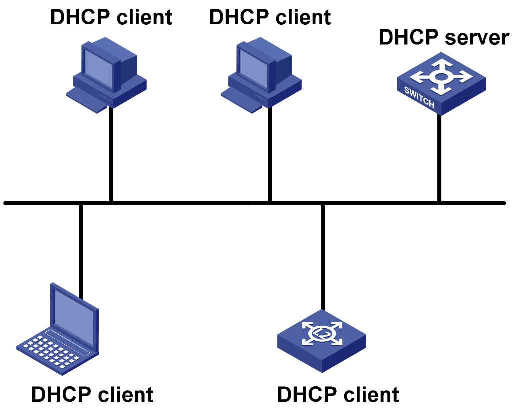
## Introduction to DHCP

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.

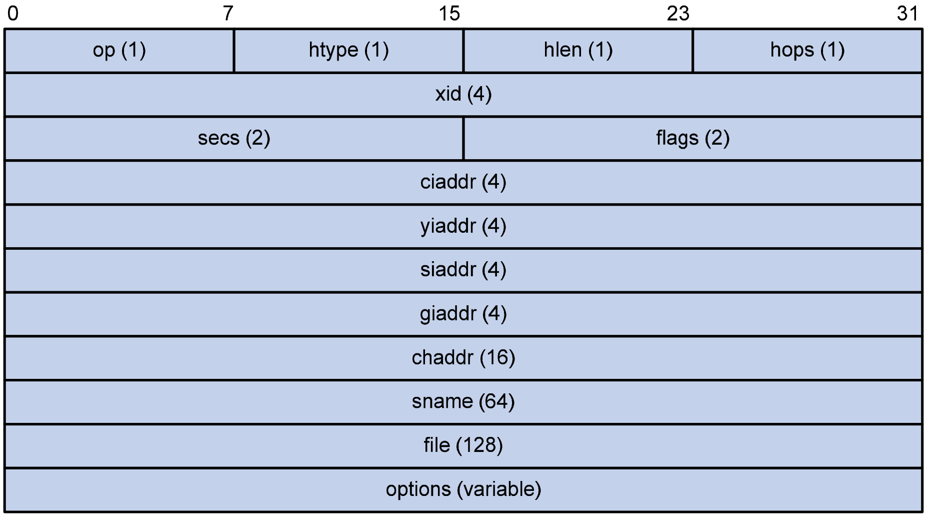
By default, a DHCP client updates its IP address lease automatically by unicasting a DHCP-REQUEST packet to the DHCP server when half of the lease time elapses. The DHCP server responds with a DHCP-ACK packet to notify the DHCP client of a new IP lease if the server can assign the same IP address to 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



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 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 ConfigurationDHCP 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

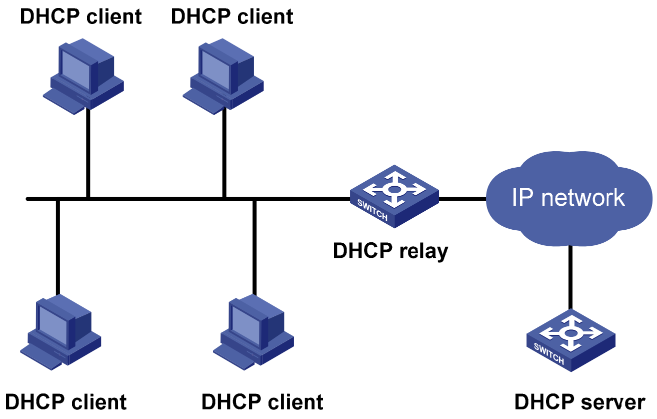
Since the packets are broadcasted in the process of obtaining IP addresses, DHCP is only applicable to the situation that DHCP clients and DHCP servers are in the same network segment, that is, you need to deploy at least one DHCP server for each network segment, which is far from economical.

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 2-1 illustrates a typical DHCP relay agent application.

**Figure 2-1** 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, S4200G 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 2-2 and Figure 2-3. (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 2-2** Padding contents for sub-option 1 of Option 82

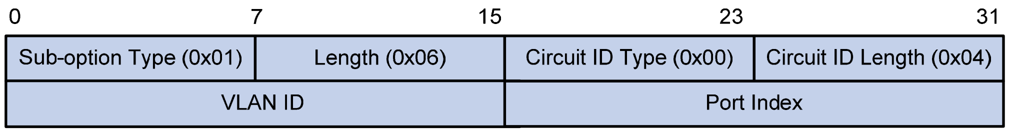
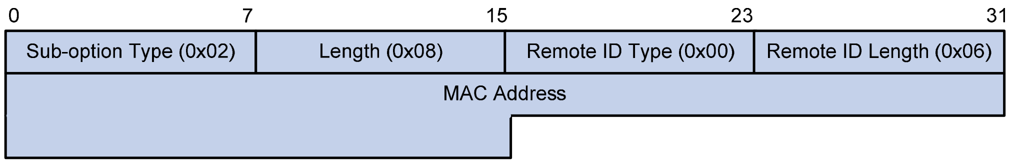


**Figure 2-3** Padding contents for sub-option 2 of Option 82



### 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.

# Configuring the DHCP Relay Agent

## DHCP Relay Agent Configuration Task List

Complete the following tasks to configure the DHCP relay agent:

| Task | Remarks |
|---|---|
| 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 |

## 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** *groupNo* **ip** *ip-address*&<1-8> | Required<br>By default, no DHCP server IP address is configured in a DHCP server group. |
| Map an interface to a DHCP server group | **interface** *interface-type interface-number* | Required<br>By default, a VLAN interface is not mapped to any DHCP server group. |
| | **dhcp-server** *groupNo* | |

**Note**

To improve security and avoid malicious attack to the unused SOCKETs, S4200G 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

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** *ip-address mac-address* | Optional<br>Not created by default. |
| Enter interface view | **interface** *interface-type interface-number* | — |
| Enable the address checking function | **address-check enable** | Required<br>Disabled by default. |

**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.

### 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<br>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<br>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<br>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.

## 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** *groupNo* | 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** *vlan-id* | |
| Display the specified client address entries on the DHCP relay agent | **display dhcp-security** [ *ip-address* \| **dynamic** \| **static** ] | |
| Clear the statistics information of the specified DHCP server group | **reset dhcp-server** *groupNo* | Available in user view |

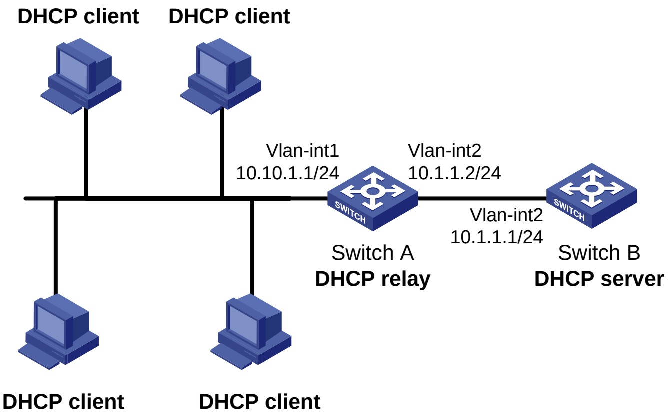
## DHCP Relay Agent Configuration Example

### 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 2-4** 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.

# 3 DHCP/BOOTP Client Configuration

When configuring the DHCP/BOOTP client, go to these sections for information you are interested in:

## 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.

## 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** *vlan-id* | — |
| Configure the VLAN interface to obtain IP address through DHCP or BOOTP | **ip address** { **bootp-alloc** \| **dhcp-alloc** } | Required<br>By default, no IP address is configured for the VLAN interface. |

**Note**

Currently, an S4200G 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.

**Note**

To improve security and avoid malicious attack to the unused SOCKETs, S4200G 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.

# Displaying DHCP/BOOTP Client Configuration

| To do… | Use the command… | Remarks |
|---|---|---|
| Display related information on a DHCP client | **display dhcp client** [ **verbose** ] | Optional<br>Available in any view |
| Display related information on a BOOTP client | **display bootp client** [ **interface Vlan-interface** *vlan-id* ] | |

# DHCP/BOOTP Client Configuration Example

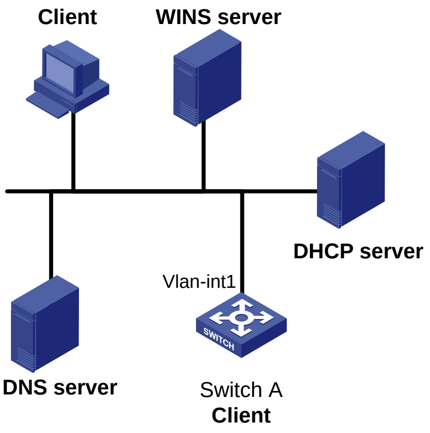
## DHCP Client Configuration Example

### Network requirements

Using DHCP, VLAN-interface 1 of Switch A is connected to the LAN to obtain an IP address from the DHCP server.

### Network diagram

**Figure 3-1** A DHCP network



### Configuration procedure

The following describes only the configuration on Switch A serving as a DHCP client.

# Configure VLAN-interface 1 to dynamically obtain an IP address by using DHCP.

```
<SwitchA> system-view
[SwitchA] interface Vlan-interface 1
[SwitchA-Vlan-interface1] ip address dhcp-alloc
```

## BOOTP Client Configuration Example

### Network requirement

Switch A’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 3-1.

### Configuration procedure

The following describes only the configuration on Switch A serving as a client.

# Configure VLAN-interface 1 to dynamically obtain an IP address from the DHCP server.

```
<SwitchA> system-view
[SwitchA] interface vlan-interface 1
[SwitchA-Vlan-interface1] ip address bootp-alloc
```

# Table of Contents

# 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, S4200G 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

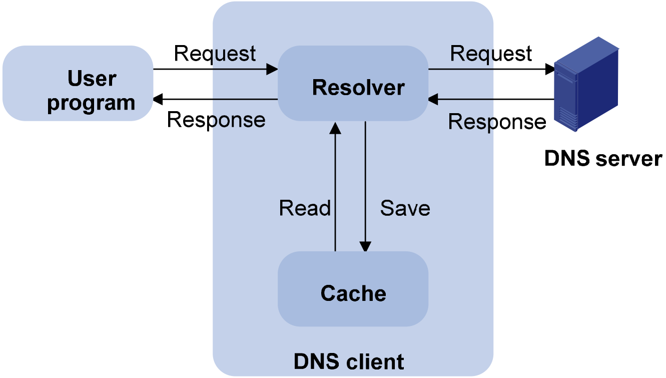


Figure 1-1 shows the relationship between user program, DNS client, and DNS server.

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** *hostname ip-address* | Required<br>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<br>Disabled by default |
| Configure an IP address for the DNS server | **dns server** *ip-address* | Required<br>No IP address is configured for the DNS server by default. |
| Configure DNS suffixes | **dns domain** *domain-name* | Optional<br>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** | |

| To do… | Use the command… | Remarks |
|---|---|---|
| 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

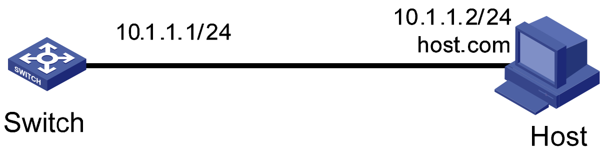
## Static Domain Name Resolution Configuration Example

### 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
```

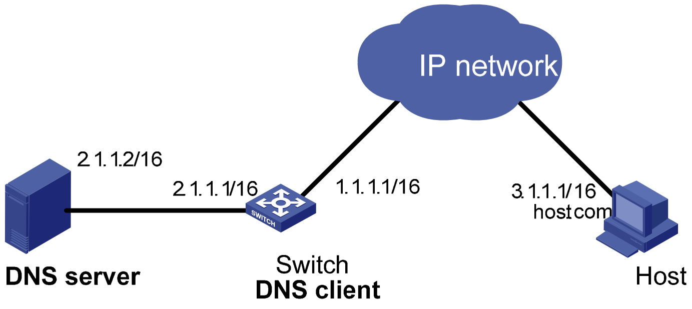
## Dynamic Domain Name Resolution Configuration Example

### 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 ACL Configuration

## 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 (ACL) 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 four types.

- 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.

## 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.

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 Switch 4200G Series, the earlier 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.

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 Switch 4200G Series

Switch 4200G Series support the following types of ACLs.

- Basic ACLs
- Advanced ACLs
- Layer 2 ACLs

Note that ACLs defined on Switch 4200G Series can be applied to hardware directly or referenced by upper-layer software for packet filtering.

# ACL Configuration

## 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 a Switch 4200G can be within the range 1970/1/1 00:00 to 2100/12/31 24:00.

### Configuration Procedure

**Table 1-1** Configure a time range

| Operation | Command | Description |
|---|---|---|
| Enter system view | **system-view** | — |
| Create a time range | **time-range** *time-name* { *start-time* **to** *end-time* *days-of-the-week* [ **from** *start-time start-date* ] [ **to** *end-time end-date* ] \| **from** *start-time start-date* [ **to** *end-time end-date* ] \| **to** *end-time end-date* } | Required |

Note that:

- If only a periodic time section is defined in a time range, the time range is active only when the system time 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 )
 From 15:00 Jan/28/2000 to 15:00 Jan/28/2004
```

## 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 section Configuring Time Range.
- The source IP addresses based on which the ACL filters packets are determined.

### Configuration Procedure

**Table 1-2** Define a basic ACL rule

| Operation | Command | Description |
|---|---|---|
| Enter system view | **system-view** | — |
| Create an ACL and enter basic ACL view | **acl number** *acl-number* [ **match-order** { **auto** \| **config** } ] | Required<br>**config** by default |
| Define an ACL rule | **rule** [ *rule-id* ] { **deny** \| **permit** } [ *rule-string* ] | Required<br>For information about *rule-string*, refer to *ACL Command*. |
| Configure a description string to the ACL | **description** *text* | Optional<br>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 prompts error information.
- 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; 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) priority.

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 of time range configuration, refer to section 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

**Table 1-3** Define an advanced ACL rule

| Operation | Command | Description |
|---|---|---|
| Enter system view | **system-view** | — |
| Create an advanced ACL and enter advanced ACL view | **acl number** *acl-number* [ **match-order** { **auto** \| **config** } ] | Required<br>**config** by default |
| Define an ACL rule | **rule** [ *rule-id* ] { **permit** \| **deny** } *protocol* [ *rule-string* ] | Required<br>For information about *protocol* and *rule-string*, refer to *ACL Commands*. |
| Assign a description string to the ACL rule | **rule** *rule-id* **comment** *text* | Optional<br>No description by default |
| Assign a description string to the ACL | **description** *text* | Optional<br>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 prompts error information.
- 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 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 section 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

**Table 1-4** Define a Layer 2 ACL rule

| Operation | Command | Description |
|---|---|---|
| Enter system view | **system-view** | — |
| Create a Layer 2 ACL and enter layer 2 ACL view | **acl number** *acl-number* | Required |
| Define an ACL rule | **rule** [ *rule-id* ] { **permit** \| **deny** } *rule-string* | Required<br>For information about *rule-string*, refer to *ACL Commands*. |
| Assign a description string to the ACL rule | **rule** *rule-id* **comment** *text* | Optional<br>No description by default |
| Assign a description string to the ACL | **description** *text* | Optional<br>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 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 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
```

## ACL Assignment

On a Switch 4200G, you can assign ACLs to the hardware for packet filtering.

As for ACL assignment, the following four ways are available.

- Assigning ACLs globally, for filtering the inbound packets on all the ports.
- Assigning ACLs to a VLAN, for filtering the inbound packets on all the ports and belonging to a VLAN.
- Assigning ACLs to a port group, for filtering the inbound packets on all the ports in a port group. For information about port group, refer to *Port Basic Configuration*.
- Assigning ACLs to a port, for filtering the inbound packets on a port.

You can assign ACLs in the above-mentioned ways as required.

⚠ **Caution**

- ACLs assigned globally take precedence over those that are assigned to VLANs. That is, when a packet matches a rule of a globally assigned ACL and a rule of an ACL assigned to a VLAN, the device will perform the action defined in the rule of the globally assigned ACL if the actions defined in the two rules conflict.
- When a packet matches a rule of an ACL assigned globally (or assigned to a VLAN) and a rule of an ACL assigned to a port (or port group), the device will deny the packets if the actions defined in the two rules conflict.
- ACLs assigned globally or to a VLAN take precedence over the default ACL. However, assigning ACLs globally or to a VLAN may affect device management that is implemented through Telnet and so on.

## Assigning an ACL Globally

### Configuration prerequisites

Before applying ACL rules to a VLAN, you need to define the related ACLs. For information about defining an ACL, refer to section Configuring Basic ACL, section Configuring Advanced ACL, section Configuring Layer 2 ACL.

### Configure procedure

**Table 1-5** Assign an ACL globally

| Operation | Command | Description |
|---|---|---|
| Enter system view | **system-view** | — |
| Assign an ACL globally | **packet-filter inbound** *acl-rule* | Required<br>For description on the *acl-rule* argument, refer to *ACL Command*. |

### Configuration example

# Apply ACL 2000 globally to filter the inbound packets on all the ports.

```
<Sysname> system-view
[Sysname] packet-filter inbound ip-group 2000
```

## Assigning an ACL to a VLAN

### Configuration prerequisites

Before applying ACL rules to a VLAN, you need to define the related ACLs. For information about defining an ACL, refer to section Configuring Basic ACL, section Configuring Advanced ACL, section Configuring Layer 2 ACL.

### Configuration procedure

**Table 1-6** Assign an ACL to a VLAN

| Operation | Command | Description |
|---|---|---|
| Enter system view | **system-view** | — |
| Apply an ACL to a VLAN | **packet-filter vlan** *vlan-id* **inbound** *acl-rule* | Required<br>For description on the *acl-rule* argument, refer to *ACL Command*. |

**Caution**

An ACL assigned to a VLAN takes effect only for the packets tagged with 802.1Q header. For more information about 802.1Q header, refer to the VLAN part.

### Configuration example

# Apply ACL 2000 to VLAN 10 to filter the inbound packets of VLAN 10 on all the ports.

```
<Sysname> system-view
[Sysname] packet-filter vlan 10 inbound ip-group 2000
```

## Assigning an ACL to a Port Group

### Configuration prerequisites

Before applying ACL rules to a VLAN, you need to define the related ACLs. For information about defining an ACL, refer to section Configuring Basic ACL, section Configuring Advanced ACL, section Configuring Layer 2 ACL.

### Configuration procedure

**Table 1-7** Assign an ACL to a port group

| Operation | Command | Description |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter port group view | **port-group** *group-id* | — |
| Apply an ACL to the port group | **packet-filter inbound** *acl-rule* | Required<br>For description on the *acl-rule* argument, refer to *ACL Command*. |

**Note**

After an ACL is assigned to a port group, it will be automatically assigned to the ports that are subsequently added to the port group.

### Configuration example

# Apply ACL 2000 to port group 1 to filter the inbound packets on all the ports in the port group.

```
<Sysname> system-view
[Sysname] port-group 1
[Sysname-port-group-1] packet-filter inbound ip-group 2000
```

## Assigning an ACL to a Port

### Configuration prerequisites

Before applying ACL rules to a VLAN, you need to define the related ACLs. For information about defining an ACL, refer to section Configuring Basic ACL, section Configuring Advanced ACL, section Configuring Layer 2 ACL.

### Configuration procedure

**Table 1-8** Apply an ACL to a port

| Operation | Command | Description |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter Ethernet port view | **interface** *interface-type interface-number* | — |
| Apply an ACL to the port | **packet-filter inbound** *acl-rule* | Required<br>For description on the *acl-rule* argument, refer to *ACL Command*. |

**Note**

You cannot assign an ACL to a member port of a port group.

### Configuration example

# Apply ACL 2000 to GigabitEthernet 1/0/1 to filter the inbound packets.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] packet-filter inbound ip-group 2000
```

## Displaying ACL Configuration

After the above configuration, you can execute the **display** commands in any view to view the ACL running information and verify the configuration.

**Table 1-9** Display ACL configuration

| Operation | Command | Description |
|---|---|---|
| Display a configured ACL or all the ACLs | **display acl** { **all** \| *acl-number* } | In any view. |
| Display a time range or all the time ranges | **display time-range** { **all** \| *time-name* } | |
| Display the information about packet filtering | **display packet-filter** { **global \| interface** *interface-type interface-number* \| **port-group** [ *group-id* ] **\| unitid** *unit-id* **\| vlan** [ *vlan-id* ] } | |
| Display the information about remaining ACL resources | **display acl remaining entry** | |

# Example for Upper-layer Software Referencing ACLs

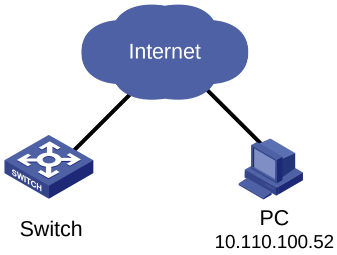
## Example for Controlling Telnet Login Users by Source IP

### 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
```

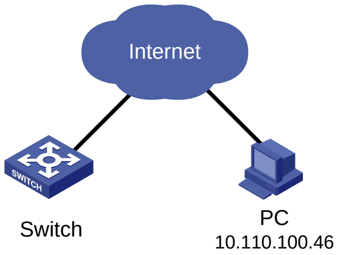
## Example for Controlling Web Login Users by Source IP

### 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
```

# Example for Applying ACLs to Hardware

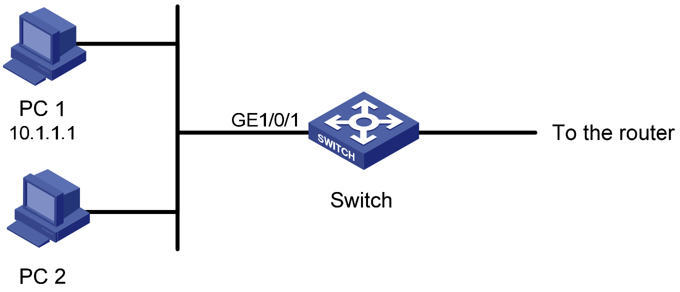
## Basic ACL Configuration Example

### Network requirements

PC 1 and PC 2 connect to the switch through GigabitEthernet 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 GigabitEthernet 1/0/1.

```
[Sysname] interface Ethernet1/0/1
[Sysname-GigabitEthernet1/0/1] packet-filter inbound ip-group 2000
```

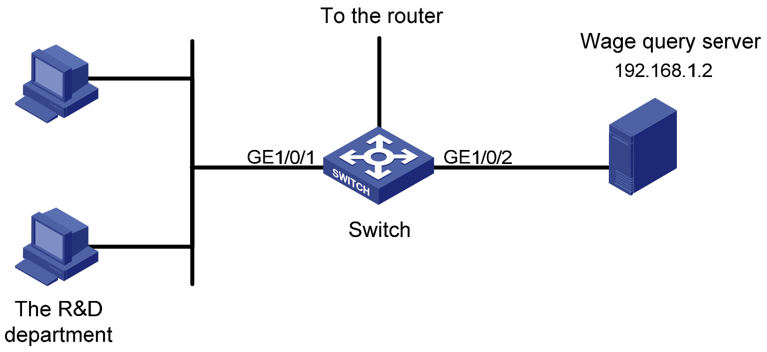
# Advanced ACL Configuration Example

## 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 GigabitEthernet 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 GigabitEthernet 1/0/1.

```
[Sysname] interface Ethernet1/0/1
[Sysname-GigabitEthernet1/0/1] packet-filter inbound ip-group 3000
```

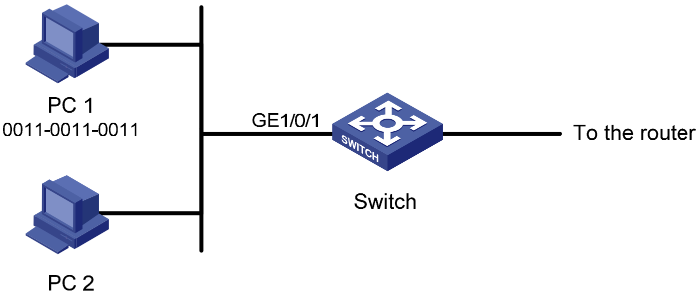
# Layer 2 ACL Configuration Example

## Network requirements

PC 1 and PC 2 connect to the switch through GigabitEthernet 1/0/1. PC1'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 GigabitEthernet 1/0/1.

```
[Sysname] interface GigabitEthernet1/0/1
[Sysname-GigabitEthernet1/0/1] packet-filter inbound link-group 4000
```

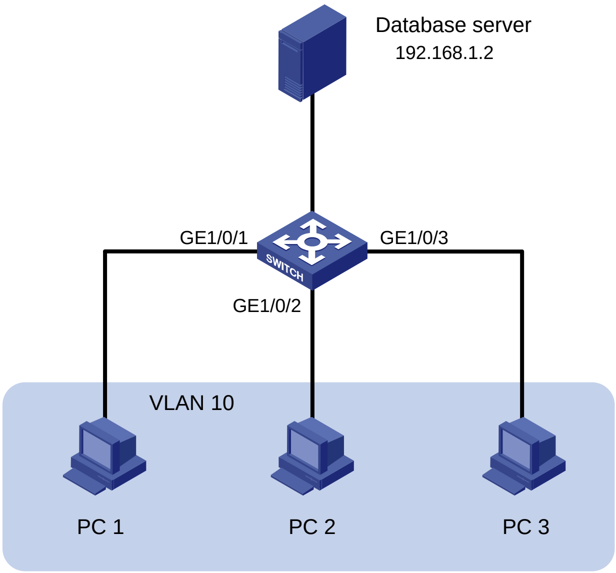
# Example for Applying an ACL to a VLAN

## Network requirements

PC1, PC2 and PC3 belong to VLAN 10 and connect to the switch through GigabitEthernet 1/0/1, GigabitEthernet 1/0/2 and GigabitEthernet 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 1-6** 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

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

- Overview
- QoS Features Supported by the Switch 4200G series
- Introduction to QoS Features
- QoS Configuration
- 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 focuses on improving services under certain conditions rather than grading services precisely.

In an internet, QoS evaluates the ability of the network to forward packets of different services. The evaluation can be based on different criteria 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 Services

On traditional IP networks, devices treat all packets equally and handle them using the first in first out (FIFO) policy. All packets share the resources of the network and devices. How many resources the packets can obtain completely depends on the time they arrive. This service is called best-effort. It delivers packets to their destinations as possibly as it can, without any guarantee for delay, jitter, packet loss ratio, reliability and so on.

This service policy is only suitable for applications insensitive to bandwidth and delay, such as WWW, e-mail, and FTP.

### New Requirements from Emerging Applications

The Internet has been growing along with the fast development of networking technologies. More and more people use the Internet to transmit data, share video and do a lot of other things.

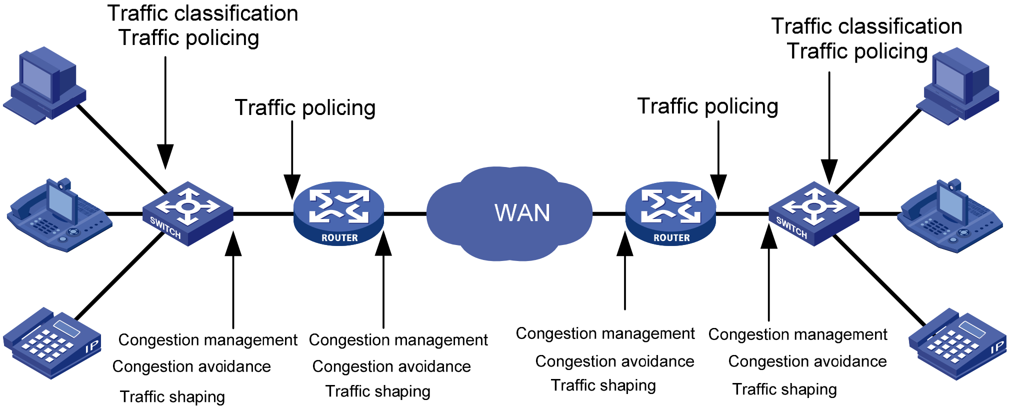
Besides traditional applications such as WWW, e-mail and FTP, network users are experiencing new services, such as tele-education, telemedicine, video telephone, videoconference and Video-on-Demand (VoD). Enterprise users expect to connect their regional branches together with VPN technologies to carry out operational applications, for instance, to access the database of the company or to monitor remote devices through Telnet.

These new applications have one thing in common, that is, they all have special requirements for bandwidth, delay, and jitter. For example, videoconference and VoD require high bandwidth, low delay and jitter. As for mission-critical applications, such as transactions and Telnet, they may not require high bandwidth but do require low delay and preferential service during congestion.

The emerging applications demand higher service performance of IP networks. Better network services during packets forwarding are required, such as providing dedicated bandwidth, reducing packet loss ratio, managing and avoiding congestion, regulating network traffic, and setting the precedence of packets. To meet these requirements, networks must provide more improved services.

## Major Traffic Control Technologies

**Figure 1-1** End-to-end QoS model



As shown in Figure 1-1, traffic classification, traffic policing, traffic shaping, congestion management, and congestion avoidance form the foundation for differentiated service provisioning. They deal with different issues of QoS:

- Traffic classification identifies traffic based on certain match criteria. It is the foundation for providing 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 assigns 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 a certain degree. It relieves network load by adjusting traffic size. Congestion avoidance is usually applied in the outbound direction of a port.

Among these QoS technologies, traffic classification is the foundation for providing differentiated services by classifying packets with certain match criteria. Traffic policing, traffic shaping, congestion management, and congestion avoidance manage network traffic and resources in different ways to realize differentiated services.

# QoS Features Supported by the Switch 4200G series

The Switch 4200G series support the QoS features listed in Table 1-1:

**Table 1-1** QoS features supported by the Switch 4200G series

| QoS Feature | Description | Reference |
|---|---|---|
| Traffic classification | Classify incoming traffic based on ACLs. The Switch 4200G series support the following types of ACLs:<br>• Basic ACLs<br>• Advanced ACLs<br>• Layer 2 ACLs | • For information about ACLs, refer to the *ACL Operation* and *ACL Command* manuals.<br>• For information about traffic classification, refer to Traffic Classification. |
| QoS actions | The Switch 4200G series support performing the following QoS actions on traffic matching the specified ACL:<br>• Traffic policing<br>• Traffic shaping<br>• Traffic accounting | • For information about traffic policing, refer to Traffic Policing and Traffic Shaping.<br>• For information about traffic shaping, refer to Traffic Policing and Traffic Shaping.<br>• For information about traffic accounting, refer to Flow-Based Traffic Accounting. |
|  | You can configure the following QoS actions for traffic separately as required on the Switch 4200G series:<br>• Priority trust mode<br>• Protocol packet priority<br>• Burst | • For information about priority trust mode, refer to Priority Trust Mode.<br>• For information about specifying priority for protocol packets, refer to Protocol Priority.<br>• For information about the burst function, refer to Burst. |
| Congestion management | The Switch 4200G series support SP, WRR, and SDWRR for queuing and support the following three queue scheduling modes:<br>• SP<br>• SDWRR<br>• SP+SDWRR | For information about SP, WRR, and SDWRR, refer to Queue Scheduling. |

# Introduction to QoS Features

## Traffic Classification

Traffic here refers to service traffic, that is, all the packets passing by the switch.

Traffic classification identifies packets conforming to certain characteristics according to certain criteria. It is the foundation for providing differentiated services.

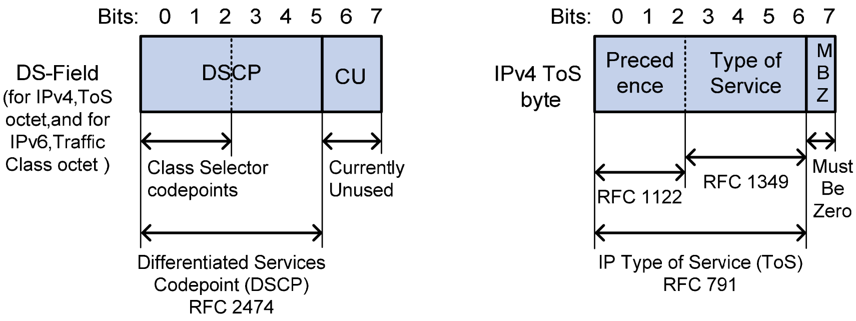
In traffic classification, the priority bits in the type of service (ToS) field in the IP header can be used to identify packets of different priorities. You can also define traffic match criteria to classify packets by the combination of source address, destination address, MAC address, IP protocol or the port number of an application. Contents other than the header information in packets are rarely used for traffic classification. You can define a class for packets with the same quintuple (source address, source port number, protocol number, destination address and destination port number for example), or for all packets to a certain network segment.

## Priority Trust Mode

### Introduction to precedence types

1) IP precedence, ToS precedence, and DSCP

**Figure 1-2** DS field and ToS byte


Bits: 0 1 2 3 4 5 6 7
DS-Field (for IPv4,ToS octet,and for IPv6,Traffic Class octet )
DSCP
CU
Class Selector codepoints
Currently Unused
Differentiated Services Codepoint (DSCP) RFC 2474
Bits: 0 1 2 3 4 5 6 7
IPv4 ToS byte
Preced ence
Type of Service
M B Z
RFC 1122
RFC 1349
Must Be Zero
IP Type of Service (ToS) RFC 791

As shown in Figure 1-2, the ToS field of the IP header contains eight bits: the first three bits (0 to 2) represent IP precedence from 0 to 7 and the subsequent four bits (3 to 6) represent a ToS value from 0 to 15. According to RFC 2474, the ToS field of the IP header is redefined as the DS field, where a DiffServ code point (DSCP) precedence is represented by the first six bits (0 to 5) and is in the range 0 to 63. The remaining two bits (6 and 7) are reserved.

**Table 1-2** Description on IP precedence

| IP precedence value (decimal) | IP precedence value (binary) | Description |
|---|---|---|
| 0 | 000 | Routine |
| 1 | 001 | priority |
| 2 | 010 | immediate |
| 3 | 011 | flash |
| 4 | 100 | flash-override |
| 5 | 101 | critical |
| 6 | 110 | internet |
| 7 | 111 | network |

In a Diff-Serv network, traffic is grouped into the following four classes, and packets are processed according to their DSCP values.

- Expedited Forwarding (EF) class: In this class, packets are 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 the virtual leased line service).
- Assured Forwarding (AF) class: This class is divided into four subclasses (AF1 to AF4), each containing three drop priorities for more granular classification. The QoS level of the AF class is lower than that of the EF class.
- Class Selector (CS) class: This class is derived from the IP ToS field and includes eight subclasses.

- Best Effort (BE) class: This class is a special CS class that does not provide any assurance. AF traffic exceeding the limit is degraded to the BE class. Currently, all IP network traffic belongs to this class by default.

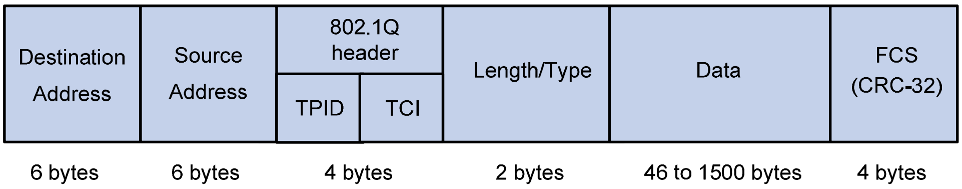
**Table 1-3** Description on DSCP values

| DSCP value (decimal) | DSCP value (binary) | Description |
|---|---|---|
| 46 | 101110 | ef |
| 10 | 001010 | af11 |
| 12 | 001100 | af12 |
| 14 | 001110 | af13 |
| 18 | 010010 | af21 |
| 20 | 010100 | af22 |
| 22 | 010110 | af23 |
| 26 | 011010 | af31 |
| 28 | 011100 | af32 |
| 30 | 011110 | af33 |
| 34 | 100010 | af41 |
| 36 | 100100 | af42 |
| 38 | 100110 | af43 |
| 8 | 001000 | cs1 |
| 16 | 010000 | cs2 |
| 24 | 011000 | cs3 |
| 32 | 100000 | cs4 |
| 40 | 101000 | cs5 |
| 48 | 110000 | cs6 |
| 56 | 111000 | cs7 |
| 0 | 000000 | be (default) |

2) 802.1p precedence

802.1p precedence lies in Layer 2 packet headers and is applicable to occasions where Layer 3 packet analysis is not needed and QoS must be assured at Layer 2.

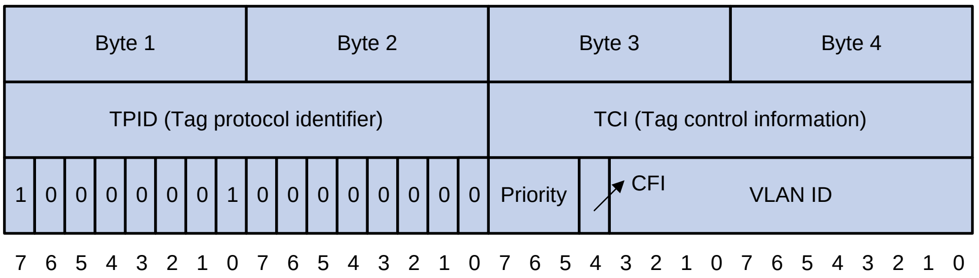
**Figure 1-3** An Ethernet frame with an 802.1q tag header



As shown in Figure 1-3, each host supporting the 802.1q protocol adds a 4-byte 802.1q tag header after the source address field of the former Ethernet frame header when sending packets.

The 4-byte 802.1q tag header consists of a two-byte tag protocol identifier (TPID) field, whose value is 0x8100, and a two-byte tag control information (TCI) field. Figure 1-4 presents the format of the 802.1q tag header.

**Figure 1-4** 802.1q tag header



In Figure 1-4, the three-bit priority field in TCI is 802.1p precedence (also known as CoS precedence), which ranges from 0 to 7.

**Table 1-4** Description on 802.1p precedence

| 802.1p precedence value (decimal) | 802.1p precedence value (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 in the 802.1q tag header is called 802.1p precedence because its use is defined in IEEE 802.1p.

3) Local precedence

Local precedence is a locally significant precedence that the switch assigns to a packet. A local precedence value corresponds to one hardware output queue on the egress port. 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.

4) Drop precedence

Drop precedence is used for making packet drop decisions. Packets with the highest drop precedence are dropped preferentially.

### Priority trust mode

A switch can assign different types of precedence to received packets as configured, such as 802.1p precedence, DSCP values, local precedence, and drop precedence.

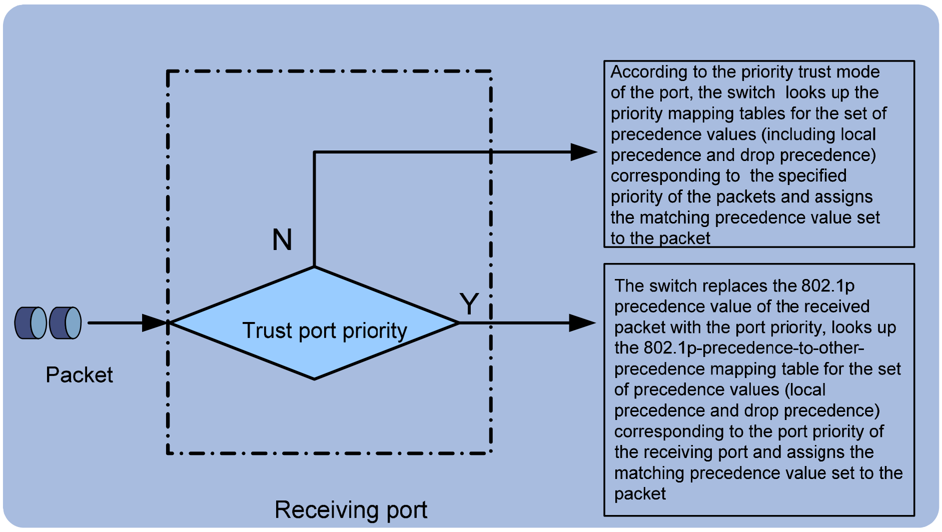
1) For an 802.1q-untagged packet

When a packet carrying no 802.1q tag reaches a port, the switch uses the port priority as the 802.1p precedence value of the received packet, searches for the set of precedence values corresponding to the port priority of the receiving port in the 802.1p-precedence-to-other-precedence mapping table, and assigns the set of matching precedence values to the packet.

2) For an 802.1q-tagged packet

For incoming 802.1q tagged packets, you can configure the switch to trust packet priority with the **priority-trust** command or to trust port priority (the default). The priority mapping process is as shown in Figure 1-5.

**Figure 1-5** Assign precedence to received packets in different trust modes



According to the priority trust mode of the port, the switch looks up the priority mapping tables for the set of precedence values (including local precedence and drop precedence) corresponding to the specified priority of the packets and assigns the matching precedence value set to the packet

The switch replaces the 802.1p precedence value of the received packet with the port priority, looks up the 802.1p-precedence-to-other-precedence mapping table for the set of precedence values (local precedence and drop precedence) corresponding to the port priority of the receiving port and assigns the matching precedence value set to the packet

- Trusting port priority

In this mode, the switch replaces the 802.1p precedence value of the received packet with the port priority, looks up the 802.1p-precedence-to-other-precedence mapping table for the set of precedence values corresponding to the port priority of the receiving port and assigns the matching precedence value set to the packet.

- Trusting packet priority

After configuring the switch to trust packet priority on a port, you can specify the trusted priority type, which can be 802.1p precedence or DSCP precedence. Table 1-5 describes how your switch handles a packet received on the port.

**Table 1-5** Actions performed when packet priority is trusted

| Trusted priority type | Description |
|---|---|
| 802.1p precedence | The switch looks up the 802.1p-precedence-to-other-precedence mapping table for the set of precedence values corresponding to the 802.1p precedence of the packet. |
| DSCP | The switch looks up the DSCP-precedence-to-other-precedence mapping table for the set of precedence values corresponding to the DSCP value of the packet. |

The Switch 4200G series provide CoS-precedence-to-other-precedence, and DSCP-precedence-to-other-precedence mapping tables for priority mapping. Table 1-6 through Table 1-7 list the default settings of these tables.

**Table 1-6** The default CoS-precedence-to-other-precedence mapping table of Switch 4200G series

| 802.1p precedence value | Target local precedence value | Target drop precedence value |
|---|---|---|
| 0 | 2 | 0 |
| 1 | 0 | 0 |
| 2 | 1 | 0 |
| 3 | 3 | 0 |
| 4 | 4 | 0 |
| 5 | 5 | 0 |
| 6 | 6 | 0 |
| 7 | 7 | 0 |

**Table 1-7** The default DSCP -to-other-precedence mapping table of Switch 4200G series

| DSCP values | Target local precedence value | Target drop precedence value |
|---|---|---|
| 0 to 7 | 0 | 1 |
| 8 to 15 | 1 | 1 |
| 16 to 23 | 2 | 1 |
| 24 to 31 | 3 | 1 |
| 32 to 39 | 4 | 0 |
| 40 to 47 | 5 | 0 |
| 48 to 55 | 6 | 0 |
| 56 to 63 | 7 | 0 |

## Protocol Priority

Protocol packets generated by your switch carry their own priority. You can set a new IP precedence or DSCP value for the locally generated traffic of a particular protocol to implement QoS.

## Traffic Policing and Traffic Shaping

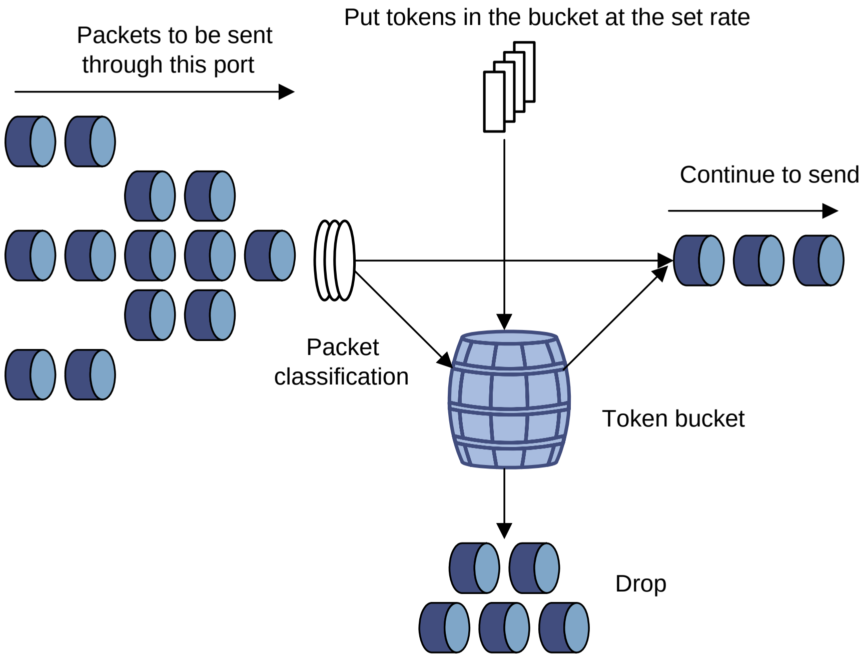
If user traffic is not limited, burst traffic will make your network more congested. To better utilize the network resources and provide better services for more users, you must take actions to control user traffic. For example, you can configure a flow to use only the resources committed to it in a time range, thus avoiding network congestion caused by burst traffic.

Traffic policing and traffic shaping limit traffic rate and resource usage according to traffic specifications. The prerequisite for traffic policing or traffic shaping is to know whether a traffic flow has exceeded the specification. If yes, proper traffic control policies are applied. Generally, token buckets are used to evaluate traffic specifications.

## Token bucket

A token bucket can be considered as a container holding a certain number of tokens. The system puts tokens into the bucket at a set rate. When the token bucket is full, the extra tokens will overflow.

**Figure 1-6** Evaluate the traffic with the token bucket


Packets to be sent through this port
Put tokens in the bucket at the set rate
Continue to send
Packet classification
Token bucket
Drop

## Evaluating the traffic with the token bucket

The evaluation of traffic specification is based on whether the number of tokens in the bucket can meet the need of packet forwarding. If the number of tokens in the bucket is enough for forwarding the packets, the traffic conforms to the specification and is called conforming traffic; otherwise, the traffic does not conform to the specification and is called exceeding traffic.

A token bucket uses the following parameters:

- Average rate: The rate at which tokens are put into the bucket, namely, the permitted average rate of the traffic. It is usually set to the 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 usually set to the committed burst size (CBS). The set burst size must be greater than the maximum packet size.

Evaluation is performed each time a packet arrives. If the number of tokens in the bucket is enough, the traffic conforms to the specification and the tokens for forwarding the packet are taken away; if the number of tokens in the bucket is not enough, it means that too many tokens have been used and the traffic exceeds the specification.

## Traffic policing

A typical application of traffic policing is to supervise the specification of certain traffic entering a network and limit it within a reasonable range, or to "discipline" the exceeding traffic. In this way, the network resources and the interests of the carrier are protected. For example, you can limit the bandwidth for HTTP packets to less than 50% of the total. If the traffic of a certain session exceeds the limit, traffic policing can drop the packets or to re-mark the priority of the packets.

Traffic policing is widely used for policing traffic entering the network of internet service providers (ISPs). It can classify the policed traffic and perform pre-defined policing actions based on different evaluation results. These actions include:

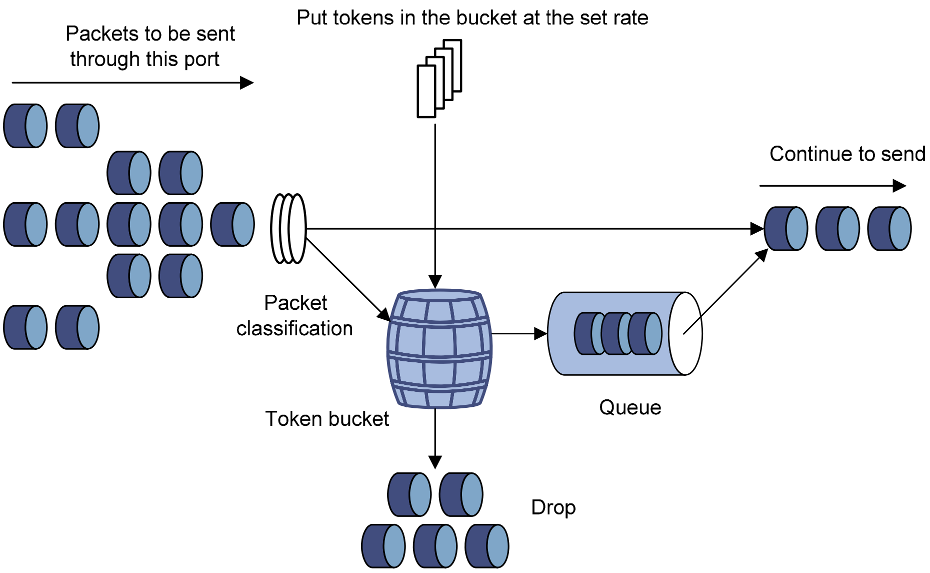
- Dropping the nonconforming packets.
- Forwarding the conforming packets.

### Traffic shaping

Traffic shaping provides measures to adjust the rate of outbound traffic actively. A typical traffic shaping application is to limit the local traffic output rate according to the downstream traffic policing parameters.

The major difference between traffic shaping and traffic policing is that the packets to be dropped in traffic policing are cached in a buffer or queue in traffic shaping, as shown in Figure 1-7. When there are enough tokens in the token bucket, the cached packets are sent out at an even rate. Traffic shaping may introduce an additional delay while traffic policing does not.

**Figure 1-7** Diagram for traffic shaping


Packets to be sent through this port
Put tokens in the bucket at the set rate
Continue to send
Packet classification
Token bucket
Queue
Drop

For example, Device A sends packets to Device B. Device B performs traffic policing on packets from Device A and drops the packets exceeding the limit.

To avoid unnecessary packet loss, you can perform traffic shaping for the packets destined for Device B on the outgoing interface of Device A. Thus, packets exceeding the limit are cached in Device A and sent when enough resources are available. This ensures that all traffic sent to Device B conforms to the traffic specification defined on Device B.

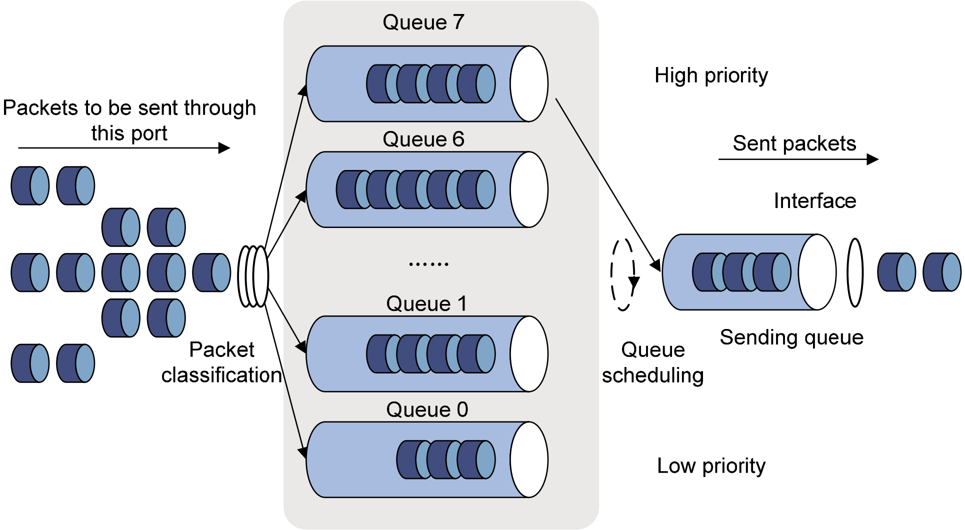
## Queue Scheduling

When the network is congested, the problem that many packets compete for resources must be solved, usually through queue scheduling.

A Switch 4200G supports strict priority (SP) queuing, weighted round robin (WRR) queuing, and shaped deficit WRR (SDWRR) queuing.

1) SP queuing

**Figure 1-8** Diagram for SP queuing



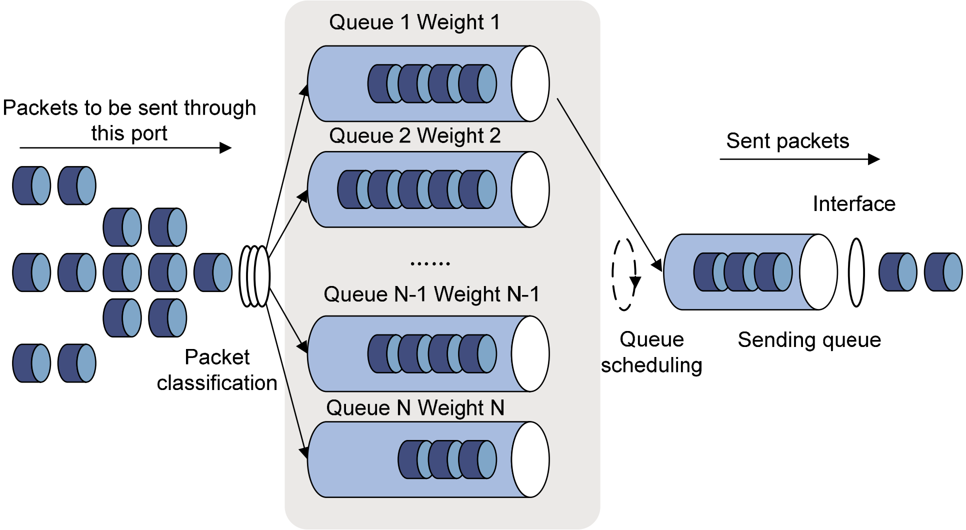
SP queuing is specially designed for mission-critical applications. The key feature of mission-critical applications is that they require preferential service to reduce the response delay when congestion occurs. Assume that there are eight output queues on the port and SP queuing classifies the eight output queues on the port into eight classes, which are queue 7, queue 6, queue 5, queue 4, queue 3, queue 2, queue 1, and queue 0 in the descending order of priority.

SP queuing schedules the eight queues strictly in the descending order of priority. It sends packets in the queue with the highest priority first. When the queue with the highest priority is empty, it sends packets in the queue with the second highest priority, and so on. By assigning mission-critical packets to high priority queues and common service packets to low priority queues, you can ensure that the mission-critical packets are always served prior to common service packets.

The disadvantage of SP queuing is that packets in the lower priority queues cannot get served if there are packets in the higher priority queues for a long time when congestion occurs. This may cause low priority traffic to starve to death.

2) WRR queuing

**Figure 1-9** Diagram for WRR queuing



WRR queuing schedules all the queues in turn and ensure that all of them can be served for a certain time by assigning each queue a weight representing a certain amount of resources. Assume there are eight output queues on the port. WRR assigns queues 7 through 0 the weights w7, w6, w5, w4, w3, w2, w1, and w0.

For example, on a 100 Mbps port, you can configure the weights for WRR queuing to 50, 50, 30, 30, 10, 10, 10, and 10 (corresponding to w7, w6, w5, w4, w3, w2, w1, and w0 in order). In this way, the queue with the lowest priority can get 5 Mbps (100 Mbps × 1/(5 + 5 + 3 + 3 + 1 + 1 + 1 + 1)) bandwidth at least, thus avoiding the disadvantage of SP queuing that the packets in low-priority queues may failed to be served for a long time.

Another advantage of WRR queuing is that though the queues are scheduled in order, the service time for each queue is not fixed. With WRR, if a queue is empty, the next queue will be scheduled immediately. In this way, the bandwidth resources are fully utilized.

3) SDWRR

Compared with WRR, SDWRR reduces scheduling delay and smoothes jitter for lower priority queues.

For example, set the weight values of queue 0 and queue 1 to 5 and 3 respectively. WRR and SDWRR schedule the queues as follows:

- WRR: dequeues the number of packets identical to weight 3 from queue 1 only after the number of packets identical to weight 5 are dequeued from queue 0. If there is a wide difference between the weight values of two queues, great delay and jitter will result for the lower-weight queue.
- SDWRR: schedules the two queues in turn in such a way that packets identical to one weight are dequeued from queue 0 first and then from queue 1. The procedure is repeated until the scheduling for one queue is over. Then, SDWRR schedules the queue with remaining weights to dequeue the number of packets identical to the remaining weights. The detailed scheduling sequence is described in the Table 1-8.

**Table 1-8** Queue-scheduling sequence of SDWRR

| Queue scheduling algorithm | Queue scheduling sequence | Remarks |
|---|---|---|
| WRR | 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1 | 0 indicates packets identical to one weight in queue 0.<br>1 indicates packets identical to one weight in queue 1. |
| SDWRR | 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0 | |

## Flow-Based Traffic Accounting

Flow-based traffic accounting uses ACL rules for traffic classification and collects statistics about ACL matching packets. With this function, you can collect statistics about the packets you are interested in.

## Burst

The burst function improves packet buffering and forwarding performance in the following scenarios:

- Dense broadcast or multicast traffic and massive burst traffic are present.
- High-speed traffic is forwarded over a low-speed link or traffic received from multiple interfaces at the same speed is forwarded through an interface at the same speed.

By enabling the burst function on your device, you can improve the processing performance of the device operating in the above scenarios and thus reduce packet loss rate. Because the burst function may affect the QoS performance of your device, you must make sure that you are fully aware of the impacts when enabling the burst function.

# QoS Configuration

## QoS Configuration Task List

Complete the following tasks to configure QoS:

| Task | Remarks |
|---|---|
| Configuring Priority Trust Mode | Optional |
| Configuring Priority Mapping | Optional |
| Setting the Priority of Protocol Packets | Optional |
| Configuring Traffic Policing | Optional |
| Configuring Traffic Shaping | Optional |
| Configuring Queue Scheduling | Optional |
| Configuring Traffic Accounting | Optional |
| Enabling the Burst Function | Optional |

## Configuring Priority Trust Mode

Refer to Priority Trust Mode for details about available priority trust modes.

### Configuration prerequisites

- The priority trust mode to be used has been determined.
- The port where priority trust mode is to be configured has been determined.
- The port priority value has been determined.

### Configuration procedures

1) Configuring a port to trust port priority

Follow these steps to configure a port to trust port priority:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter Ethernet port view | **interface** *interface-type interface-number* | — |
| Configure to trust port priority and configure the port priority | **priority** *priority-level* | Optional<br>By default, the switch trusts port priority and the priority of a port is 0. |

2) Configuring a port to trust 802.1p precedence of traffic

Follow these steps to configure a port to trust 802.1p precedence:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter Ethernet port view | **interface** *interface-type interface-number* | — |
| Configure to trust 802.1p precedence | **priority-trust cos** | Required<br>By default, port priority is trusted. |

3) Configuring a port to trust DSCP value of traffic

Follow these steps to configure a port to trust DSCP value of traffic:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter Ethernet port view | **interface** *interface-type interface-number* | — |
| Configure to trust DSCP values | **priority-trust dscp** | Required<br>By default, port priority is trusted. |

### Configuration examples

# Configure trusting port priority on GigabitEthernet 1/0/1 and set the priority of GigabitEthernet 1/0/1 to 7.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet1/0/1
[Sysname-GigabitEthernet1/0/1] priority 7
```

# Configure trusting 802.1p precedence on GigabitEthernet 1/0/2.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet1/0/2
[Sysname-GigabitEthernet1/0/2] priority-trust cos
```

# Configure trusting DSCP values on GigabitEthernet 1/0/3.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet1/0/3
[Sysname-GigabitEthernet1/0/3] priority-trust dscp
```

## Configuring Priority Mapping

You can modify the CoS-precedence-to-other-precedence, and DSCP-precedence-to-other-precedence mapping tables as required to mark packets with different priorities.

### Configuration prerequisites

The target CoS-precedence-to-other-precedence, and DSCP-precedence-to-other-precedence mapping tables have been determined.

## Configuration procedures

1) Configuring the CoS-precedence-to-other-precedence mapping table

Follow these steps to configure the CoS-precedence-to-other-precedence mapping table:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Configure the CoS-precedence-to-local-precedence mapping table | **qos cos-local-precedence-map** *cos0-map-local-prec cos1-map-local-prec cos2-map-local-prec cos3-map-local-prec cos4-map-local-prec cos5-map-local-prec cos6-map-local-prec cos7-map-local-prec* | Required |
| Configure the CoS-precedence-to-drop-precedence mapping table | **qos cos-drop-precedence-map** *cos0-map-drop-prec cos1-map-drop-prec cos2-map-drop-prec cos3-map-drop-prec cos4-map-drop-prec cos5-map-drop-prec cos6-map-drop-prec cos7-map-drop-prec* | Required |

2) Configuring the DSCP-precedence-to-other-precedence mapping table

Follow these steps to configure the DSCP-precedence-to-other-precedence mapping table:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Configure DSCP-precedence-to-local-precedence mapping table | **qos dscp-local-precedence-map** *dscp-list* **:** *local-precedence* | Required |
| Configure DSCP-precedence-to-drop-precedence mapping table | **qos dscp-drop-precedence-map** *dscp-list* **:** *drop-precedence* | Required |

## Configuration examples

# Configure the CoS-precedence-to-local-precedence mapping table for a Switch 4200G as follows: 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. Then display the CoS-precedence-to-local-precedence mapping table.

```
<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
```

# Configure the DSCP-precedence-to-local-precedence mapping table for a Switch 4200G as follows: 0 through 7 to 2, 8 through 15 to 3, 16 through 23 to 4, 24 through 31 to 1, 32 through 39 to 7, 40 through 47 to 0, 48 through 55 to 5, and 56 through 63 to 6. Then display the DSCP-precedence-to-local-precedence mapping table.

```
<Sysname> system-view
[Sysname] qos dscp-local-precedence-map 0 1 2 3 4 5 6 7 : 2
```

```
[Sysname] qos dscp-local-precedence-map 8 9 10 11 12 13 14 15 : 3
[Sysname] qos dscp-local-precedence-map 16 17 18 19 20 21 22 23 : 4
[Sysname] qos dscp-local-precedence-map 24 25 26 27 28 29 30 31 : 1
[Sysname] qos dscp-local-precedence-map 32 33 34 35 36 37 38 39 : 7
[Sysname] qos dscp-local-precedence-map 40 41 42 43 44 45 46 47 : 0
[Sysname] qos dscp-local-precedence-map 48 49 50 51 52 53 54 55 : 5
[Sysname] qos dscp-local-precedence-map 56 57 58 59 60 61 62 63 : 6
<Sysname> display qos dscp-local-precedence-map
 dscp-local-precedence-map:
             dscp : local-precedence(queue)
 ----------------------------------------------
                0 :            2
                1 :            2
                2 :            2
                3 :            2
                4 :            2
                5 :            2
                6 :            2
                7 :            2
                8 :            3
                9 :            3
               10 :            3
               11 :            3
               12 :            3
               13 :            3
               14 :            3
               15 :            3
               16 :            4
               17 :            4
               18 :            4
               19 :            4
               20 :            4
               21 :            4
               22 :            4
               23 :            4
               24 :            1
               25 :            1
               26 :            1
               27 :            1
               28 :            1
               29 :            1
               30 :            1
               31 :            1
               32 :            7
               33 :            7
               34 :            7
               35 :            7
```

```
36 :          7
37 :          7
38 :          7
39 :          7
40 :          0
41 :          0
42 :          0
43 :          0
44 :          0
45 :          0
46 :          0
47 :          0
48 :          5
49 :          5
50 :          5
51 :          5
52 :          5
53 :          5
54 :          5
55 :          5
56 :          6
57 :          6
58 :          6
59 :          6
60 :          6
61 :          6
62 :          6
63 :          6
```

## Setting the Priority of Protocol Packets

Refer to 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 of the specific protocol packets:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Set the priority of the specific type of protocol packets | **protocol-priority protocol-type** *protocol-type* { **ip-precedence** *ip-precedence* \| **dscp** *dscp-value* } | Required<br>You can modify the IP precedence values or DSCP values of the corresponding protocol packets.<br>On a Switch 4200G, you can set the priority for protocol packets of Telnet, SNMP, and ICMP. |

### Configuration examples

# Set the IP precedence value of ICMP packets to 3.

```
<Sysname> system-view
[Sysname] protocol-priority protocol-type icmp ip-precedence 3
```

# After completing the above configuration, display the list of protocol priorities manually specified.

```
[Sysname] display protocol-priority
Protocol: icmp
  IP-Precedence: flash(3)
```

## Configuring Traffic Policing

Refer to Traffic Policing and Traffic Shaping 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.

### Configuration procedures

You can configure traffic policing for the incoming packets matching the specific ACL rules globally, in a VLAN, in a port group, or on a port.

1) Configuring traffic policing globally

Follow these steps to configure traffic policing for the incoming packets matching the specific ACL rules globally:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Configure traffic policing | **traffic-limit inbound** *acl-rule target-rate* | Required<br>Disabled by default. |

2) Configuring traffic policing for a VLAN

Follow these steps to configure traffic policing for the incoming packets matching the specific ACL rules in a VLAN:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Configure traffic policing | **traffic-limit vlan** *vlan-id* **inbound** *acl-rule target-rate* | Required<br>Disabled by default. |

3) Configuring traffic policing for a port group

Follow these steps to configure traffic policing for the incoming packets matching the specific ACL rules in a port group:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter port group view | **port-group** *group-id* | — |
| Configure traffic policing | **traffic-limit inbound** *acl-rule target-rate* | Required<br>Disabled by default. |

4) Configuring traffic policing for a port

Follow these steps to configure traffic policing for the incoming packets matching the specific ACL rules on a port:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter Ethernet port view | **interface** *interface-type interface-number* | — |
| Configure traffic policing | **traffic-limit inbound** *acl-rule target-rate* | Required<br>Disabled by default. |

**Caution**

User-defined traffic classification rules configured for traffic policing in the global scope or for a VLAN take precedence over the default rules used for processing protocol packets. The device will execute traffic policing preferentially, which may affect device management implemented through Telnet and so on.

## Configuration example

# Configure traffic policing for the packets from network segment 10.1.1.0/24, setting the rate limit to 128 kbps.

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 GigabitEthernet1/0/1
[Sysname-GigabitEthernet1/0/1] traffic-limit inbound ip-group 2000 128
```

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-limit vlan 2 inbound ip-group 2000 128
```

## Configuring Traffic Shaping

Refer to Traffic Policing and Traffic Shaping for information about traffic shaping.

### Configuration prerequisites

- The queue for which traffic shaping is to be performed has been determined.
- The maximum traffic rate and the burst size have been determined.
- The port where traffic shaping is to be configured has been determined.

### Configuration procedure

Follow these steps to configure traffic shaping:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter Ethernet port view | **interface** *interface-type interface-number* | — |
| Configure traffic shaping | **traffic-shape** [ **queue** *queue-id* ] *max-rate burst-size* | Required<br>Disabled by default.<br>Traffic shaping can be configured in one of the following two modes:<br>• Without **queue** *queue-id* specified, traffic shaping applies to all traffic.<br>• With **queue** *queue-id* specified, traffic shaping applies to traffic in the specified queue. |

### Configuration example

# Configure traffic shaping for all the traffic to be transmitted through GigabitEthernet 1/0/1, with the maximum traffic rate being 640 kbps and the burst size being 16 kbytes.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet1/0/1
[Sysname-GigabitEthernet1/0/1] traffic-shape 640 16
```

## Configuring Queue Scheduling

Refer to Queue Scheduling for information about queue scheduling.

### Configuration prerequisites

The queue scheduling algorithm to be used and the related parameters have been determined.

### Configuration procedures

1) Configuring SP queuing

Follow these steps to configure SP queuing:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |

| To do… | Use the command… | Remarks |
|---|---|---|
| Configure SP queuing | **undo queue-scheduler** [ *queue-id* ] &<1-8> | Optional<br>By default, SP queuing is used on all the output queues of a port. |

2) Configuring SDWRR queuing

Follow these steps to configure SDWRR queuing:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Configure SDWRR queuing | **queue-scheduler wrr** { **group1** { *queue-id* *queue-weight* } &<1-8> \| **group2** { *queue-id* *queue-weight* } &<1-8> }* | Required<br>By default, SP queuing is used on all the output queues of a port. |

The port of a Switch 4200G provides up to eight output queues. You can configure SP queuing, SDWRR queuing, or SP queuing in combination with SDWRR queuing on a port as required.

- With SDWRR queuing adopted, the output queues of a port can be assigned to group 1 and group 2. The two groups are scheduled using the SP algorithm. For example, you can assign queues 0 through 3 to group 1, and queues 4 through 7 to group 2. The queues in group 2 are scheduled preferentially using WRR. The queues in group 1 are scheduled using WRR only when all the queues in group 2 are empty.
- With both SP queuing and SDWRR queuing adopted, groups are scheduled using the SP algorithm. Assume that queue 0 and queue 1 are scheduled using SP queuing; queues 2 through 4 are assigned to group 1; queues 5 through 7 are assigned to group 2. The queues in group 2 are scheduled preferentially using WRR. When all the queues in group 2 are empty, the queues in group 1 are scheduled using WRR. Then, queue 1 is scheduled, and then queue 0.

**Note**

When using SDWRR or SP+SDWRR for queue scheduling, you are recommended to assign queues with successive queue numbers to the same scheduling group.

## Configuration example

# Configure a Switch 4200G to use SP+SDWRR for queue scheduling, assigning queue 3, queue 4, and queue 5 to WRR scheduling group 1, with the weigh of 20, 20 and 30; assigning queue 0, queue 1, and queue 2 to WRR group 2, with the weight of 20, 20, and 40; using SP for scheduling queue 6 and queue 7. Display queue scheduling configuration information after the configuration.

```
<Sysname> system-view
[Sysname] queue-scheduler wrr group1 3 20 4 20 5 30 group2 0 20 1 20 2 40
[Sysname] display queue-scheduler
```

```
QID:   scheduling-group     weight
-----------------------------------
  0 :    wrr , group2          20
  1 :    wrr , group2          20
  2 :    wrr , group2          40
  3 :    wrr , group1          20
  4 :    wrr , group1          20
  5 :    wrr , group1          30
  6 :    sp                     0
  7 :    sp                     0
```

## Configuring Traffic Accounting

Refer to 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.

### Configuration procedures

You can collect/clear traffic statistics about incoming ACL matching packets globally, in a VLAN, in a port group, or on a port.

1) Configuring traffic accounting globally

Follow these steps to collect/clear statistics about the incoming ACL matching packets globally:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Collect statistics of the packets matching a specific ACL rule | **traffic-statistic inbound** *acl-rule* | Required |
| Clear statistics of the packets matching a specific ACL rule | **reset traffic-statistic inbound** *acl-rule* | Optional |

2) Configuring traffic accounting for a VLAN

Follow these steps to collect/clear statistics about the incoming ACL matching packets in a VLAN:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Collect statistics about incoming ACL matching packets | **traffic-statistic vlan** *vlan-id* **inbound** *acl-rule* | Required |
| Clear statistics about the packets matching a specific ACL rule | **reset traffic-statistic vlan** *vlan-id* **inbound** *acl-rule* | Optional |

3) Configuring traffic accounting for a port group

Follow these steps to collect/clear statistics about incoming ACL matching packets in a port group:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter port group view | **port-group** *group-id* | — |
| Collect statistics about ACL matching packets | **traffic-statistic inbound** *acl-rule* | Required<br>By default, traffic accounting is disabled. |
| Clear statistics about ACL matching packets | **reset traffic-statistic inbound** *acl-rule* | Optional |

4) Configuring traffic accounting for a port

Follow these steps to collect/clear statistics about incoming ACL matching packets on a port:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter Ethernet port view | **interface** *interface-type interface-number* | — |
| Collect statistics about incoming ACL matching packets | **traffic-statistic inbound** *acl-rule* | Required |
| Clear statistics about incoming ACL matching packets | **reset traffic-statistic inbound** *acl-rule* | Optional |

**Caution**

User-defined traffic classification rules configured for traffic accounting in the global scope or for a VLAN take precedence over the default rules used for processing protocol packets. The device will collect traffic statistics preferentially, which may affect device management implemented through Telnet and so on.

## Configuration examples

# Collect and then clear the statistics about the incoming packets sourced from network segment 10.1.1.0/24 (assume that GigabitEthernet 1/0/1 is connected to network segment 10.1.1.0/24 and carries VLAN 2).

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 GigabitEthernet1/0/1
[Sysname-GigabitEthernet1/0/1] traffic-statistic inbound ip-group 2000
[Sysname-GigabitEthernet1/0/1] reset traffic-statistic inbound ip-group 2000
```

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-statistic vlan 2 inbound ip-group 2000
[Sysname] reset traffic-statistic vlan 2 inbound ip-group 2000
```

## Enabling the Burst Function

Refer to Burst for information about the burst function.

### Configuration prerequisites

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<br>Disabled by default |

### Configuration example

# Enable the burst function on a Switch 4200G.

```
<Sysname> system-view
[Sysname] burst-mode enable
```

## Displaying and Maintaining QoS

| To do… | Use the command… | Remarks |
|---|---|---|
| Display protocol packet priority configuration | **display protocol-priority** | Available in any view |
| Display the CoS-precedence-to-Drop-precedence mapping | **display qos cos-drop-precedence-map** | Available in any view |
| Display the CoS-precedence-to-local-precedence mapping | **display qos cos-local-precedence-map** | Available in any view |
| Display the DSCP-precedence-to-Drop-precedence mapping | **display qos dscp-drop-precedence-map** | Available in any view |
| Display the DSCP-precedence-to-local-precedence mapping | **display qos dscp-local-precedence-map** | Available in any view |
| Display queue scheduling configuration | **display queue-scheduler** | Available in any view |

| To do… | Use the command… | Remarks |
|---|---|---|
| Display QoS-related configuration of a port or all the ports | **display qos-interface** { *interface-type interface-number* \| *unit-id* } **all** | Available in any view |
| Display the priority trust mode of a port or all the ports | **display qos-interface** { *interface-type interface-number* \| *unit-id* } **priority-trust** | Available in any view |
| Display traffic shaping configuration of a port or all the ports | **display qos-interface** { *interface-type interface-number* \| *unit-id* } **traffic-shape** | Available in any view |
| Display traffic policing configuration of a port or all the ports | **display qos-interface** { *interface-type interface-number* \| *unit-id* } **traffic-limit** | Available in any view |
| Display traffic accounting configuration of a port or all the ports | **display qos-interface** { *interface-type interface-number* \| *unit-id* } **traffic-statistic** | Available in any view |
| Display global QoS configuration of traffic policing or traffic accounting | **display qos-global** { **all** \| **traffic-limit** \| **traffic-statistic** } | Available in any view |
| Display VLAN-level QoS configuration of traffic policing or traffic accounting | **display qos-vlan** [ *vlan-id* ] { **all** \| **traffic-limit** \| **traffic-statistic** } | Available in any view |
| Display port group-level QoS configuration of traffic policing or traffic accounting | **display qos-port-group** [ *group-id* ] { **all** \| **traffic-limit** \| **traffic-statistic** } | Available in any view |

# QoS Configuration Examples

## Traffic Policing Configuration Example

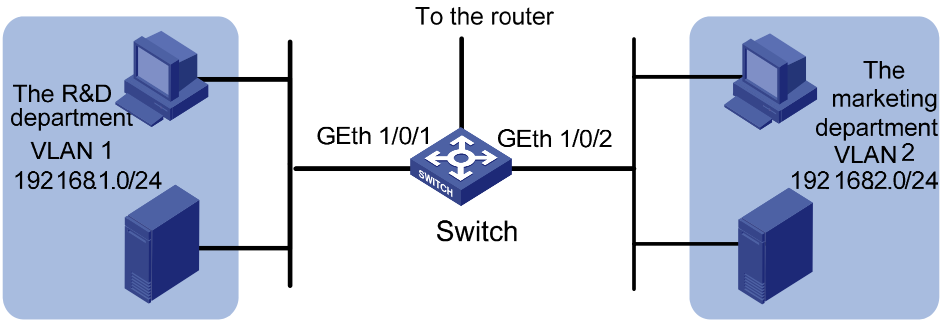
### Network requirements

As shown in Figure 1-10, an enterprise network connects all the departments through a Switch 4200G. PC1 with the IP address 192.168.0.1 belongs to the R&D department and is connected to GigabitEthernet 1/0/1 of the switch. The marketing department is connected to GigabitEthernet 1/0/2 of the switch.

Configure traffic policing to satisfy the following requirements:

- Set the maximum rate of outbound IP packets sourced from the marketing department to 64 kbps.
- Set the maximum rate of outbound IP packets sourced from the R&D department to 128 kbps.

**Figure 1-10** Network diagram for traffic policing configuration



## Configuration procedure

1) Define an ACL for traffic classification

# Create ACL 2000 and enter basic ACL view to match packets sourced from network segment 192.168.1.0/24.

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] rule permit source 192.168.1.0 0.0.0.255
[Sysname-acl-basic-2000] quit
```

# Create ACL 2001 and enter basic ACL view to match packets sourced from network segment 192.168.2.0/24.

```
[Sysname] acl number 2001
[Sysname-acl-basic-2001] rule permit source 192.168.2.0 0.0.0.255
[Sysname-acl-basic-2001] quit
```

2) Configure traffic policing

# Set the maximum rate of outbound IP packets sourced from the marketing department to 64 kbps.

```
[Sysname] traffic-limit vlan 2 inbound ip-group 2001 64
```

# Set the maximum rate of outbound IP packets sourced from the R&D department to 128 kbps.

```
[Sysname] traffic-limit vlan 1 inbound ip-group 2000 128
```

# Table of Contents

# 1 Mirroring Configuration

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

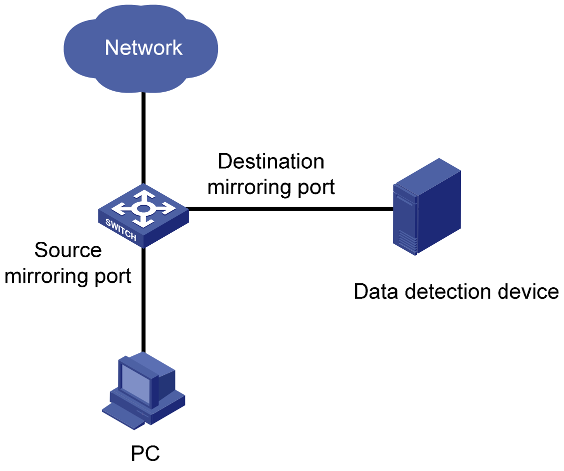
- Mirroring Overview
- Mirroring Configuration
- Displaying Port Mirroring
- Mirroring Configuration Examples

## 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 Switch 4200G series support five two types of port mirroring:

- Local Port Mirroring
- Remote Port Mirroring

They are described in the following sections.

### 1.1.1 Local Port Mirroring

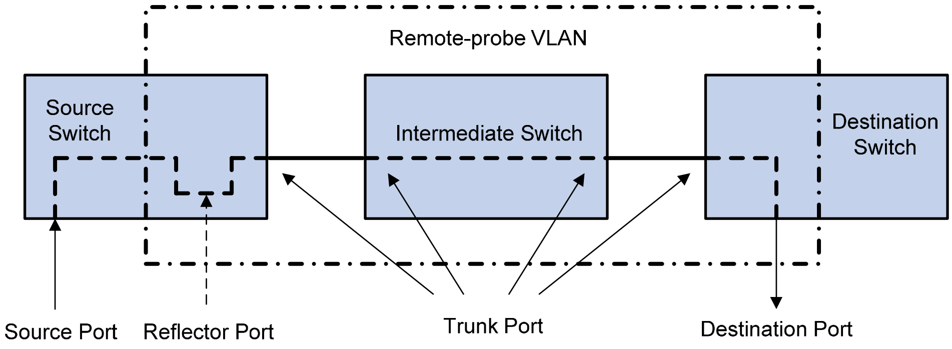
In local port mirroring, packets passing through one or more source ports of a device are copied to the destination port on the same device for packet analysis and monitoring. In this case, the source ports and the destination port must be located on the same device.

## 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. |
| Intermediate switch | Trunk port | Sends mirrored packets to the destination switch.<br>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-prove VLAN and do not use the remote-prove VLAN as the voice VLAN and protocol VLAN; otherwise, remote port mirroring may be affected.

## Mirroring Configuration

Complete the following tasks to configure mirroring:

| Task | Remarks |
|---|---|
| Configuring Local Port Mirroring | Optional |
| Configuring Remote Port Mirroring | Optional |

**Note**

On a Switch 4200G, only one destination port for local port mirroring or one reflector port for remote port mirroring can be configured, and the two kinds of ports cannot both exist.

### 1.1.2 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

**Table 1-2** Follow these steps to configure port mirroring:

| To do… | | Use the command… | Remarks |
|---|---|---|---|
| Enter system view | | **system-view** | — |
| Create a port mirroring group | | **mirroring-group** *group-id* **local** | Required |
| Configure the source port for the port mirroring group | In system view | **mirroring-group** *group-id* **mirroring-port** *mirroring-port-list* { **both** \| **inbound** \| **outbound** } | Use either approach<br>You can configure multiple source ports at a time in system view, or you can configure the source port in specific port view. The configurations in the two views have the same effect. |
| | In port view | **interface** *interface-type interface-number* | |
| | | **mirroring-group** *group-id* **mirroring-port** { **both** \| **inbound** \| **outbound** } | |
| | | **quit** | |
| Configure the destination port for the port mirroring group | In system view | **mirroring-group** *group-id* **monitor-port** *monitor-port-id* | Use either approach<br>The configurations in the two views have the same effect. |
| | In port view | **interface** *interface-type interface-number* | |
| | | **mirroring-group** *group-id* **monitor-port** | |

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 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.

## Configuring Remote Port Mirroring

**Note**

A Switch 4200G 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

**Table 1-3** 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** *vlan-id* | *vlan-id* 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 that connects to the intermediate switch or destination switch | **interface** *interface-type interface-number* | — |
| Configure the current port as trunk port | **port link-type trunk** | Required<br>By default, the port type is Access. |
| Configure the trunk port to permit packets from the remote-probe VLAN | **port trunk permit vlan** *remote-probe-vlan-id* | Required |

| To do… | Use the command… | Remarks |
|---|---|---|
| Return to system view | **quit** | — |
| Create a remote source mirroring group | **mirroring-group** *group-id* **remote-source** | Required |
| Configure source port(s) for the remote source mirroring group | **mirroring-group** *group-id* **mirroring-port** *mirroring-port-list* { **both** \| **inbound** \| **outbound** } | Required |
| Configure the reflector port for the remote source mirroring group | **mirroring-group** *group-id* **reflector-port** *reflector-port* | Required |
| Configure the remote-probe VLAN for the remote source mirroring group | **mirroring-group** *group-id* **remote-probe vlan** *remote-probe-vlan-id* | 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 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 the functions like VLAN-VPN, port loopback detection, 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.

### 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

**Table 1-4** 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** *vlan-id* | *vlan-id* is the ID of the remote-probe VLAN. |
| Configure the current VLAN as the remote-probe VLAN | **remote-probe vlan enable** | Required |

| To do… | Use the command… | Remarks |
|---|---|---|
| Return to system view | **quit** | — |
| Enter the view of the Ethernet port connecting to the source switch, destination switch or other intermediate switch | **interface** *interface-type interface-number* | — |
| Configure the current port as trunk port | **port link-type trunk** | Required<br>By default, the port type is Access. |
| Configure the trunk port to permit packets from the remote-probe VLAN | **port trunk permit vlan** *remote-probe-vlan-id* | Required |

### 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

**Table 1-5** 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** *vlan-id* | *vlan-id* 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** *interface-type interface-number* | — |
| Configure the current port as trunk port | **port link-type trunk** | Required<br>By default, the port type is Access. |
| Configure trunk port to permit packets from the remote-probe VLAN | **port trunk permit vlan** *remote*-probe-*vlan-id* | Required |
| Return to system view | **quit** | — |
| Create a remote destination mirroring group | **mirroring-group** *group-id* **remote-destination** | Required |

| To do… | Use the command… | Remarks |
|---|---|---|
| Configure the destination port for the remote destination mirroring group | **mirroring-group** *group-id* **monitor-port** *monitor-port* | Required |
| Configure the remote-probe VLAN for the remote destination mirroring group | **mirroring-group** *group-id* **remote-probe vlan** *remote-probe-vlan-id* | Required |

When configuring a destination switch, note that:

- The destination port of remote port mirroring cannot be a member port of an existing mirroring group, 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 Port Mirroring

| To do… | Use the command… | Remarks |
|---|---|---|
| Display the information of a mirroring group. | **display mirroring-group** { *group-id* \| **all** \| **local** \| **remote-destination** \| **remote-source** } | Available in any view |

# Mirroring Configuration Examples

## Local Port Mirroring Configuration Example

### Network requirements

The departments of a company connect to each other through Switch 4200G series:

- Research and Development (R&D) department is connected to Switch C through GigabitEthernet 1/0/1.
- Marketing department is connected to Switch C through GigabitEthernet 1/0/2.
- Data detection device is connected to Switch C through GigabitEthernet 1/0/3

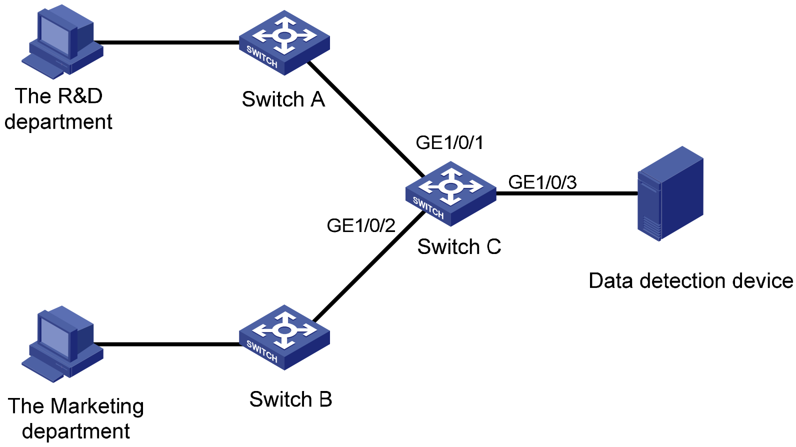
The administrator wants to monitor the packets received on and sent from the R&D department and the marketing department through the data detection device.

Use the local port mirroring function to meet the requirement. Perform the following configurations on Switch C.

- Configure GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 as mirroring source ports.
- Configure GigabitEthernet 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 GigabitEthernet 1/0/1 GigabitEthernet
1/0/2 both
[Sysname] mirroring-group 1 monitor-port GigabitEthernet 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:
        GigabitEthernet1/0/1  both
        GigabitEthernet1/0/2  both
    monitor port: GigabitEthernet1/0/3
```

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 Switch 4200G series:

- Switch A, Switch B, and Switch C are Switch 4200G series.

- Department 1 is connected to GigabitEthernet 1/0/1 of Switch A.
- Department 2 is connected to GigabitEthernet 1/0/2 of Switch A.
- GigabitEthernet 1/0/3 of Switch A connects to GigabitEthernet 1/0/1 of Switch B.
- GigabitEthernet 1/0/2 of Switch B connects to GigabitEthernet 1/0/1 of Switch C.
- The data detection device is connected to GigabitEthernet 1/0/2 of Switch C.

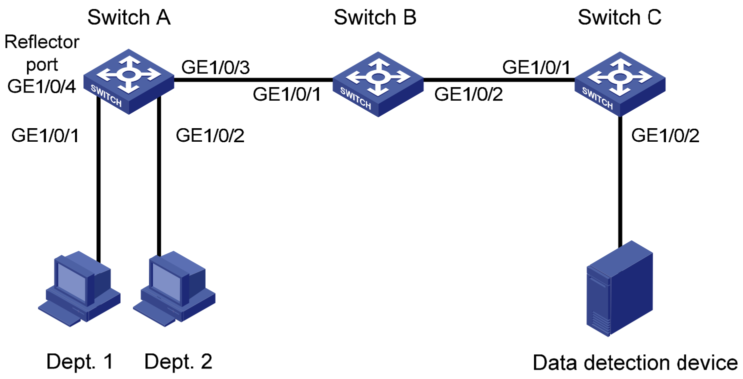
The administrator wants to monitor the packets sent from Department 1 and 2 through the data detection device.

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 GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 as the source ports, and port GigabitEthernet 1/0/4 as the reflector port.
- On Switch B, configure VLAN 10 as the remote-probe VLAN.
- Configure GigabitEthernet 1/0/3 of Switch A, GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 of Switch B, and GigabitEthernet 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 GigabitEthernet 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 GigabitEthernet 1/0/1 GigabitEthernet
1/0/2 inbound
[Sysname] mirroring-group 1 reflector-port GigabitEthernet 1/0/4
[Sysname] mirroring-group 1 remote-probe vlan 10
```

# Configure GigabitEthernet 1/0/3 as trunk port, allowing packets of VLAN 10 to pass.

```
[Sysname] interface GigabitEthernet 1/0/3
[Sysname-GigabitEthernet1/0/3] port link-type trunk
[Sysname-GigabitEthernet1/0/3] port trunk permit vlan 10
[Sysname-GigabitEthernet1/0/3] 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:
        GigabitEthernet1/0/1  inbound
        GigabitEthernet1/0/2  inbound
    reflector port: GigabitEthernet1/0/4
    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 GigabitEthernet 1/0/1 as the trunk port, allowing packets of VLAN 10 to pass.

```
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port link-type trunk
[Sysname-GigabitEthernet1/0/1] port trunk permit vlan 10
[Sysname-GigabitEthernet1/0/1] quit
```

# Configure GigabitEthernet 1/0/2 as the trunk port, allowing packets of VLAN 10 to pass.

```
[Sysname] interface GigabitEthernet 1/0/2
[Sysname-GigabitEthernet1/0/2] port link-type trunk
[Sysname-GigabitEthernet1/0/2] 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 GigabitEthernet 1/0/2
[Sysname] mirroring-group 1 remote-probe vlan 10
```

# Configure GigabitEthernet 1/0/1 as the trunk port, allowing packets of VLAN 10 to pass.

```
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port link-type trunk
[Sysname-GigabitEthernet1/0/1] port trunk permit vlan 10
[Sysname-GigabitEthernet1/0/1] 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: GigabitEthernet1/0/2
    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 Stack

**Note**

Among Switch 4200G series switches, Switch 4200G 24-Port, Switch 4200G PWR 24-Port, and Switch 4200G 48-Port switches support stacks formed by 10GE stack boards.

## Stack Function Overview

A stack is a management domain formed by a group of Ethernet switches interconnected through their stack ports. A stack contains a main switch and multiple slave switches.

Logically, you can consider a stack a single device and manage all the switches in a stack through the main switch.

### The Main Switch of a Stack

You can configure multiple Ethernet switches interconnected through their stack ports to form a stack by performing configurations on one of the switches. In this case, the switch becomes the main switch of the stack.

You can perform the following operations on a main switch:

- Configuring an IP address pool for the stack
- Creating the stack
- Switching to slave switch view

Before creating a stack, you need to configure an IP address pool for the stack on the main switch. When adding a switch to a stack, the main switch picks an IP address from the IP address pool and assigns the IP address to it automatically.

After a stack is created, the main switch automatically adds the switches that connected to its stack ports to the stack. If a stack port connection is disconnected, the corresponding slave switch quits the stack automatically.

### The Slave Switches of a Stack

All the switches in a stack except the main switch are slave switches.

You can configure a slave switch in a stack on the main switch.

### Creating a Stack

The following are the phases undergone when a stack is created.

- Connect the intended main switch and slave switches through stack modules and dedicated stack cables. (Refer to *3Com Switch 4200G 10G Interface Module Installation Guide* for the information about stack modules and stack cables.)
- Configure the IP address pool for the stack and enable the stack function. The main switch then automatically adds the switches connected to its stack ports to the stack.
- When adding a switch joins in a stack, the main switch automatically assigns an IP address to it.
- The main switch automatically adds any switches that are newly connected to the stack through their stack ports to the stack.

## Main Switch Configuration

The main switch configuration includes:

- Configuring the IP Address Pool and Creating the Stack
- Switching to Slave Switch View

### Configuring the IP Address Pool and Creating the Stack

**Table 1-1** Configure the IP address pool and create the stack

| Operation | Command | Description |
|---|---|---|
| Enter system view | **system-view** | — |
| Configure an IP address pool for a stack | **stacking ip-pool** *from-ip-address ip-address-number* [ *ip-mask* ] | Required<br>*from-ip-address*: Start address of the IP address pool.<br>*ip-address-number*: Number of the IP addresses in the IP addresses pool. A pool contains 16 addresses by default.<br>*ip-mask*: Mask of the IP address pool.<br>By default, the IP addresses pool is not configured. |
| Create a stack | **stacking enable** | Required |

**Note**

Remove the IP address configured for the existing Layer 3 interface first if you want to cancel the stack-related configuration, otherwise, IP address conflicts may occur.

As for the stack-related configurations performed on a main switch, note that:

- After a stack is created, the main switch automatically adds the switches connected to its stack ports to the stack.
- If a stack port connection is disconnected, the corresponding slave switch quits the stack automatically.
- The IP address pool of an existing stack cannot be modified.

- To add a switch to a stack successfully, make sure the IP address pool contains at least one unoccupied IP address.
- Make sure the IP addresses in the IP address pool of a stack are successive so that they can be assigned successively. For example, the IP addresses in an IP address pool with its start IP address something like 223.255.255.254 are not successive. In this case, errors may occur when adding a switch to the stack.
- IP addresses in the IP address pool of a stack must be of the same network segment. For example, the 1.1.255.254 is not a qualified start address for a stack IP address pool.
- If the IP address of the management VLAN interface of the main switch (or a slave switch) is not of the same network segment as that of the stack address pool, the main switch (or the slave switch) automatically removes the existing IP address and picks a new one from the stack address pool as its IP address.
- Since both stack and cluster use the management VLAN and only one VLAN interface is available on the Switch 4200G switch, stack and cluster must share the same management VLAN if you want to configure stack within a cluster.

## Switching to Slave Switch View

After creating a stack, you can switch to slave switch view from the main switch to configure slave switches.

**Table 1-2** Switch to slave switch view

| Operation | Command | Description |
|---|---|---|
| Switch to slave switch view | **stacking** *number* | Required<br>*Number*: Number of the slave switch to switch to.<br>This command can be used to switch from user view of the main switch to user view of a slave switch. The user level remains the same while switching. |

You can quit slave switch view after slave switch configuration.

**Table 1-3** Quit slave switch view

| Operation | Command | Description |
|---|---|---|
| Quit slave switch view | **quit** | You can quit slave switch view only by executing this command in user view of a slave switch. |

# Slave Switch Configuration

Just make sure the slave switch is connected to the main switch through the stack ports. No configuration is needed.

# Displaying and Debugging a Stack

Use the **display** command to display the information about a stack. The **display** command can be executed in any view.

**Table 1-4** Display and maintain stack configurations

| Operation | Command | Description |
|---|---|---|
| Display the stack status information on the main switch | **display stacking** [ **members** ] | Optional<br>The **display** command can be executed in any view.<br>When being executed with the **members** keyword not specified, this command displays the main switch and the number of switches in the stack.<br>When being executed with the **members** keyword specified, this command displays the member information of the stack, including stack number , device name, MAC addresses and status of the main switch/slave switches. |
| Display the stack status information on a slave switch | **display stacking** | Optional<br>The **display** command can be executed in any view.<br>The displayed information indicates that the local switch is a slave switch. The information such as stack number of the local switch, and the MAC address of the main switch in the stack is also displayed. |

# Stack Configuration Example

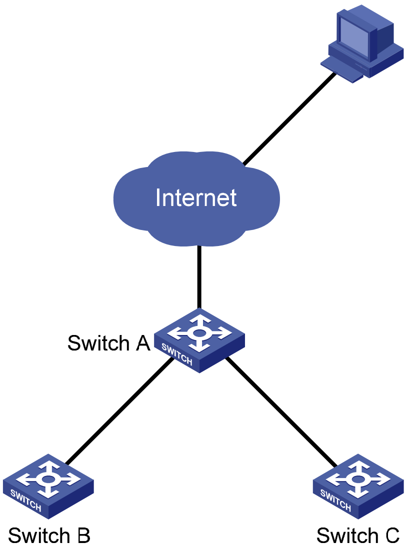
## Network requirements

Connect Switch A, Switch B and Switch C with each other through their stack ports to form a stack, in which Switch A acts as the main switch, while Switches B and C act as slave switches.

Configure Switches B and Switch C through Switch A.

## Network diagram

**Figure 1-1** Network diagram for stack configuration



## Configuration procedure

# Configure the IP address pool for the stack on Switch A.

```
<Sysname> system-view
[Sysname] stacking ip-pool 129.10.1.15 3
```

# Create the stack on switch A.

```
[Sysname] stacking enable
[stack_0.Sysname] quit
<stack_0.Sysname>
```

# Display the information about the stack on switch A.

```
<stack_0.Sysname> display stacking
Main device for stack.
 Total members:3
 Management-vlan:1(default vlan)
```

# Display the information about the stack members on switch A.

```
<stack_0.Sysname> display stacking members
Member number: 0
Name:stack_0.Sysname
Device: 4200G 12-Port
MAC Address:000f-e20f-c43a
Member status:Admin
IP: 129.10.1.15 /16

Member number: 1
Name:stack_1.Sysname
Device: 4200G 12-Port
MAC Address: 000f-e200-3130
Member status:Up
```

```
IP: 129.10.1.16/16

Member number: 2
Name:stack_2.Sysname
Device: 4200G 24-Port
MAC Address: 000f-e200-3135
Member status:Up
IP: 129.10.1.17/16
```

# Switch to Switch B (a slave switch).

```
<stack_0.Sysname> stacking 1
<stack_1.Sysname>
```

# Display the information about the stack on switch B.

```
<stack_1.Sysname> display stacking
Slave device for stack.
Member number:1
Management-vlan:1(default vlan)
Main device mac address: 000f-e20f-c43a
```

# Switch back to Switch A.

```
<stack_1.Sysname> quit
<stack_0.Sysname>
```

# Switch to Switch C (a slave switch).

```
<stack_0.Sysname> stacking 2
<stack_2.Sysname>
```

# Switch back to Switch A.

```
<stack_2.Sysname> quit
<stack_0.Sysname>
```

# 2 Cluster

## 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.

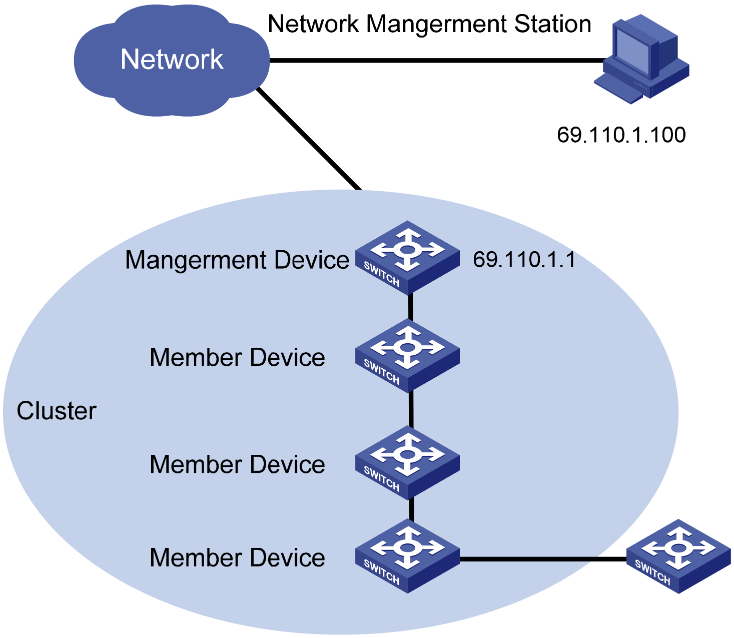
A switch in a cluster plays one of the following three roles:

- 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 2-1 illustrates a cluster implementation.

**Figure 2-1** 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.

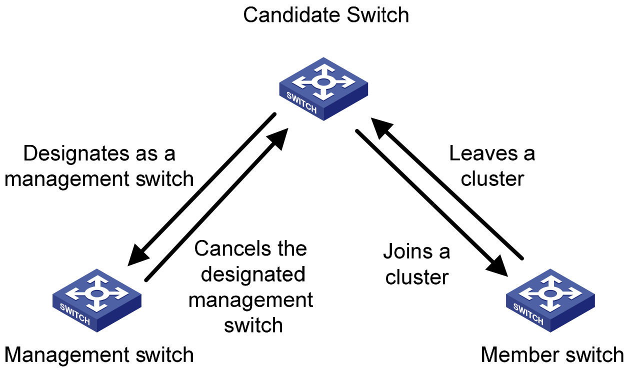
As mentioned above, the three cluster roles are management device, member device, and candidate device.

**Table 2-1** 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<br>• Manages member devices through command redirection, that is, it forwards the commands intended for specific member devices.<br>• Discovers neighbors, collects the information about network topology, manages and maintains the cluster. Management device also supports FTP server and SNMP host proxy.<br>• Processes the commands issued by users through the public network |
| Member device | Normally, a member device is not assigned an external IP address | • Members of a cluster<br>• Discovers the information about its neighbors, processes the commands forwarded by the management device, and reports log. The member devices of a luster 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 2-2 illustrates the state machine of cluster role.

**Figure 2-2** 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 Switch 4200G 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 ages out. You can also clear the current NDP information manually to have neighbor information collected again.
- An NDP-enabled device regularly broadcasts NDP packet through all its active ports. An NDP packet carries a holdtime field, which indicates how long the receiving devices will keep the NDP packet data. The receiving devices store the information carried in the NDP packet into the NDP table but do not forward the NDP packet. When they receive another NDP packet, if the information carried in the packet is different from the stored one, the corresponding entry in the NDP table is updated, otherwise only the holdtime of the entry is updated.

### 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-enable 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

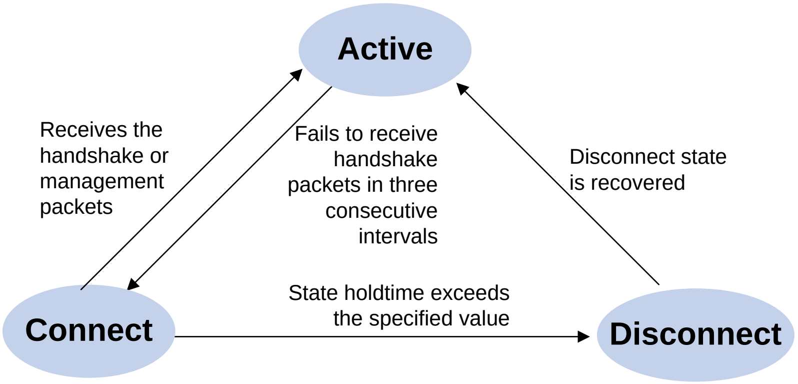
To create a cluster, you need to determine the device to operate as the management device first. The management device discovers and determines candidate devices through NDP and NTDP, and adds them to the cluster. You can also add candidate devices to a cluster manually.

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 2-3 illustrates the state machine of the connection between the management device and a member device.

**Figure 2-3** State machine of the connection between the management device and a member device


Active
Receives the handshake or management packets
Fails to receive handshake packets in three consecutive intervals
Disconnect state is recovered
State holdtime exceeds the specified value
Connect
Disconnect

- 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 Tasks

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.

**Table 2-2** Cluster configuration tasks:

| Configuration 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 |

| Configuration task | Remarks |
|---|---|
| Configuring the Cluster Synchronization Function | Optional |

## Configuring the Management Device

### Management device configuration tasks

**Table 2-3** Management device configuration tasks

| Operation | Description |
|---|---|
| Enabling NDP globally and on specific ports | Required |
| Configuring NTDP-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 |
| Enabling management VLAN synchronization | Optional |

**Note**

To reduce the risk of being attacked by malicious users against opened socket and enhance switch security, the Switch 4200G 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

**Table 2-4** Enable NDP globally and on specific ports

| Operation | Command | Description |
|---|---|---|
| Enter system view | **system-view** | — |
| Enable NDP globally | **ndp enable** | Required<br>By default, NDP is enabled globally. |

| Operation | | | Command | Description |
|---|---|---|---|---|
| Enable NDP on specified Ethernet ports | In system view | | **ndp enable interface** *port-list* | Use either approach.<br>By default, NDP is enabled on a port. |
| | In Ethernet port view | Enter Ethernet port view | **interface** *interface-type interface-number* | |
| | | Enable NDP on the port | **ndp enable** | |

### Configuring NDP-related parameters

**Table 2-5** Configure NDP-related parameters

| Operation | Command | Description |
|---|---|---|
| Enter system view | **system-view** | — |
| Configure the holdtime of NDP information | **ndp timer aging** *aging-in-seconds* | Optional<br>By default, the holdtime of NDP information is 180 seconds. |
| Configure the interval to send NDP packets | **ndp timer hello** *seconds* | Optional<br>By default, the interval to send NDP packets is 60 seconds. |

### Enabling NTDP globally and on a specific port

**Table 2-6** Enable NTDP globally and on a specific port

| Operation | Command | Description |
|---|---|---|
| Enter system view | **system-view** | — |
| Enable NTDP globally | **ntdp enable** | Required<br>Enabled by default |
| Enter Ethernet port view | **interface** *interface-type interface-number* | — |
| Enable NTDP on the Ethernet port | **ntdp enable** | Required<br>Enabled by default |

### Configuring NTDP-related parameters

**Table 2-7** Configure NTDP-related parameters

| Operation | Command | Description |
|---|---|---|
| Enter system view | **system-view** | — |
| Configure the range to collect topology information | **ntdp hop** *hop-value* | Optional<br>By default, the system collects topology information from the devices within three hops. |

| Operation | Command | Description |
|---|---|---|
| Configure the device forward delay of topology collection requests | **ntdp timer hop-delay** *time* | Optional<br>By default, the device forward delay is 200 ms. |
| Configure the port forward delay of topology collection requests | **ntdp timer port-delay** *time* | Optional<br>By default, the port forward delay is 20 ms. |
| Configure the interval to collect topology information periodically | **ntdp timer** *interval-in-minutes* | Optional<br>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

**Table 2-8** Enable the cluster function

| Operation | Command | Description |
|---|---|---|
| Enter system view | **system-view** | — |
| Enable the cluster function globally | **cluster enable** | Required<br>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

**Table 2-9** Establish a cluster and configure cluster parameters in manual mode

| Operation | Command | Description |
|---|---|---|
| Enter system view | **system-view** | — |
| Specify the management VLAN | **management-vlan** *vlan-id* | Required<br>By default, VLAN 1 is used as the management VLAN. |
| Enter cluster view | **cluster** | — |
| Configure a IP address pool for the cluster | **ip-pool** *administrator-ip-address* { *ip-mask* \| *ip-mask-length* } | Required |
| Build a cluster | **build** *name* | Required<br>*name*: cluster name. |

| Operation | Command | Description |
|---|---|---|
| Configure a multicast MAC address for the cluster | **cluster-mac** *H-H-H* | Required<br>By default, the cluster multicast MAC address is 0180-C200-000A. |
| Set the interval for the management device to send multicast packets | **cluster-mac syn-interval** *time-interval* | Optional<br>By default, the interval to send multicast packets is one minutes. |
| Set the holdtime of member switches | **holdtime** *seconds* | Optional<br>By default, the holdtime is 60 seconds. |
| Set the interval to send handshake packets | **timer** *interval* | Optional<br>By default, the interval to send handshake packets is 10 seconds. |

2) Establish a cluster in automatic mode

**Table 2-10** Establish a cluster in automatic mode

| Operation | Command | Description |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter cluster view | **cluster** | — |
| Configure the IP address range for the cluster | **ip-pool** *administrator-ip-address* { *ip-mask* \| *ip-mask-length* } | Required |
| Start automatic cluster establishment | **auto-build** [ **recover** ] | Required<br>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

**Table 2-11** Configure inside-outside interaction for a cluster

| Operation | Command | Description |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter cluster view | **cluster** | Required |

| Operation | Command | Description |
|---|---|---|
| Configure a shared FTP server for the cluster | **ftp-server** *ip-address* | Optional<br>By default, the management device acts as the shared FTP server. |
| Configure a shared TFTP server for the cluster | **tftp-server** *ip-address* | Optional<br>By default, no shared TFTP server is configured. |
| Configure a shared logging host for the cluster | **logging-host** *ip-address* | Optional<br>By default, no shared logging host is configured. |
| Configure a shared SNMP host for the cluster | **snmp-host** *ip-address* | Optional<br>By default, no shared SNMP host is configured. |

### Enabling management VLAN synchronization

By default, VLAN 1 is the management VLAN. To specify another VLAN as the management VLAN for the cluster, you must configure the same management VLAN on all the devices that are about to join the cluster.

By enabling the management VLAN synchronization function on the management device, you can enable the management device to send a management VLAN synchronization packet periodically to the connected devices. After the devices receive the management VLAN synchronization packet, they set their own management VLANs according to the packet. In this way, all devices set the same management VLAN automatically, and thus simplify your configurations.

Follow these steps to enable management VLAN synchronization:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter cluster view | **cluster** | Required |
| Enable management VLAN synchronization | **management-vlan synchronization enable** | Required<br>Disabled by default. |

## Configuring Member Devices

### Member device configuration tasks

**Table 2-12** Member device configuration tasks

| Operation | Description |
|---|---|
| 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 Switch 4200G 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

**Table 2-13** Enable NDP globally and on specific ports

| Operation | | | Command | Description |
|---|---|---|---|---|
| Enter system view | | | **system-view** | — |
| Enable NDP globally | | | **ndp enable** | Required |
| Enable NDP on specified ports | In system view | | **ndp enable interface** *port-list* | Required<br>Use either approach. |
| | In Ethernet port view | Enter Ethernet port view | **interface** *interface-type interface-number* | |
| | | Enable NDP on the port | **ndp enable** | |

### Enabling NTDP globally and on a specific port

**Table 2-14** Enable NTDP globally and a specific port

| Operation | Command | Description |
|---|---|---|
| Enter system view | **system-view** | — |

| Operation | Command | Description |
|---|---|---|
| Enable NTDP globally | **ntdp enable** | Required |
| Enter Ethernet port view | **interface** *interface-type interface-number* | — |
| Enable NTDP on the port | **ntdp enable** | Required |

### Enabling the cluster function

**Table 2-15** Enable the cluster function

| Operation | Command | Description |
|---|---|---|
| Enter system view | **system-view** | — |
| Enable the cluster function globally | **cluster enable** | Optional<br>By default, the cluster function is enabled. |

### Accessing the shared FTP/TFTP server from a member device

Perform the following operations in user view on a member device.

**Table 2-16** Access the shared FTP/TFTP server from a member device

| Operation | Command | Description |
|---|---|---|
| Access the shared FTP server of the cluster | **ftp cluster** | Optional |
| Download a file from the shared TFTP server of the cluster | **tftp cluster get** *source-file* [ *destination-file* ] | Optional |
| Upload a file to the shared TFTP server of the cluster | **tftp cluster put** *source-file* [ *destination-file* ] | Optional |

## 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.

**Table 2-17** Manage a cluster through management device

| Operation | Command | Description |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter cluster view | **cluster** | — |
| Configuring MAC address of Management device | **administrator-address** *mac-address* **name** *name* | Optional |
| Add a candidate device to the cluster | **add-member** [ *member-number* ] **mac-address** *H-H-H* [ **password** *password* ] | Optional |

| Operation | Command | Description |
|---|---|---|
| Remove a member device from the cluster | **delete-member** *member-number* | Optional |
| Reboot a specified member device | **reboot member** { *member-number* \| **mac-address** *H-H-H* } [ **eraseflash** ] | Optional |
| Return to system view | **quit** | — |
| Return to user view | **quit** | — |
| Switch between management device and member device | **cluster switch-to** { *member-number* \| **mac-address** *H-H-H* \| **administrator** \| **sysname** *sysname* } | Optional<br>You can use this command switch to the view of a member device and switch back. |
| Locate device through MAC address and IP address | **tracemac** { **by-mac** *mac-address* **vlan** *vlan-id* \| **by-ip** *ip-address* } [ **nondp** ] | Optional<br>These commands can be executed 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 a topology.top file 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.

### Configure the enhanced cluster features

**Table 2-18** The enhanced cluster feature configuration tasks

| Operation | Description |
|---|---|
| Configure cluster topology management function | Required |
| Configure cluster device blacklist | Required |

### Configure 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

Perform the following configuration on the management device.

**Table 2-19** Configure cluster topology management function

| Operation | Command | Description |
|---|---|---|
| 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** { **ftp-server** \| **local-flash** } ] \| **mac-address** *mac-address* \| **member-id** *member-id* \| **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** *mac-address* | Optional<br>These commands can be executed in any view. |
| Display the topology of the current cluster | **display cluster current-topology** [ **mac-address** *mac-address1* [ **to-mac-address** *mac-address2* ] **\| member-id** *member-id1* [ **to-member-id** *member-id2* ] ] | |
| Display the information about the base topology of the cluster | **display cluster base-topology** [ **mac-address** *mac-address* \| **member** *member-id* ] | |

| Operation | Command | Description |
|---|---|---|
| Display the information about all the devices in the base cluster topology | **display cluster base-members** | |

### Configure cluster device blacklist

Perform the following configuration on the management device.

**Table 2-20** Configure the cluster device blacklist

| Operation | Command | Description |
|---|---|---|
| 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** *mac-address* | Optional<br>By default, the cluster blacklist is empty. |
| Delete the specified MAC address from the cluster blacklist | **black-list delete-mac** *mac-address* | Optional |
| Delete a device from the cluster add this device to the cluster blacklist | **delete-member** *member-id* [ **to-black-list** ] | Optional |
| Displays the information about the devices in the cluster blacklist | **display cluster black-list** | Optional<br>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<br>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<br>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<br>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<br>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> system-view
[test_0.Sysname] cluster
[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** *username* **passward** { **cipher** \| **simple** } *passwardstring* | Required<br>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

After the above configuration, you can execute the **display** commands in any view to display the configuration and running status of cluster, so as to verify your configuration.

**Table 2-21** Display and maintain cluster configuration

| Operation | Command | Description |
|---|---|---|
| Display all NDP configuration and running information (including the interval to send NDP packets, the holdtime, and all neighbors discovered) | **display ndp** | You can execute the **display** command in any view. |
| Display NDP configuration and running information on specified ports (including the neighbors discovered by NDP on the ports) | **display ndp interface** *port-list* | |
| Display global NTDP information | **display ntdp** | |
| Display device information collected by NTDP | **display ntdp device-list** [ **verbose** ] | |
| Display status and statistics information about the cluster | **display cluster** | |
| Display information about the candidate devices of the cluster | **display cluster candidates** [ **mac-address** *H-H-H* \| **verbose** ] | |
| Display information about the member devices of the cluster | **display cluster members** [ *member-number* \| **verbose** ] | |
| Clear the statistics on NDP ports | **reset ndp statistics** [ **interface** *port-list* ] | You can execute the **reset** command in user view. |

# Cluster Configuration Example

## Basic Cluster Configuration Example

### Network requirements

Three switches compose a cluster, where:

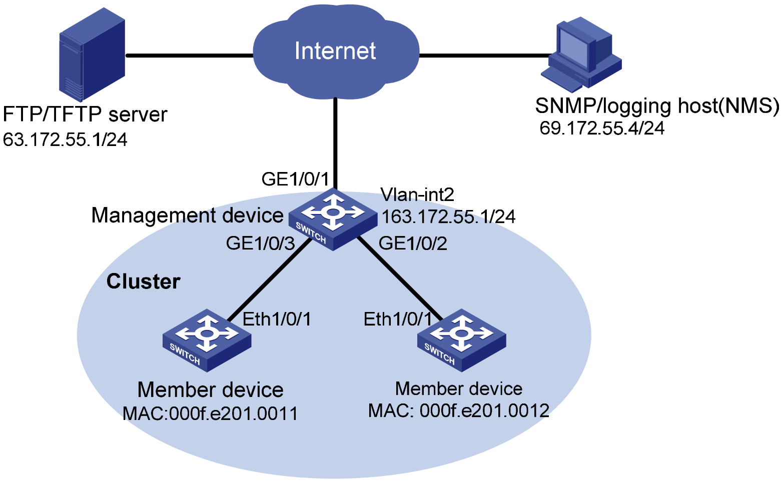
- An Switch 4200G series switch serves as the management device.
- The rest are member devices.

Serving as the management device, the Switch 4200G switch manages the two member devices. The configuration for the cluster is as follows:

- The two member devices connect to the management device through GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3.
- The management device connects to the Internet through GigabitEthernet 1/0/1.
- GigabitEthernet 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 2-4** Network diagram for HGMP cluster configuration



### Configuration procedure

1) Configure the member devices (taking one member as an example)

# Enable NDP globally and on Ethernet1/0/1.

```
<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 Ethernet1/0/1.

```
[Sysname] ntdp enable
[Sysname] interface Ethernet 1/0/1
```

```
[Sysname-Ethernet1/0/1] ntdp enable
[Sysname-Ethernet1/1] quit
```

# Enable the cluster function.

```
[Sysname] cluster enable
```

2) Configure the management device

# Enable NDP globally and on GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3.

```
<Sysname> system-view
[Sysname] ndp enable
[Sysname] interface GigabitEthernet 1/0/2
[Sysname-GigabitEthernet1/0/2] ndp enable
[Sysname-GigabitEthernet1/0/2] quit
[Sysname] interface GigabitEthernet 1/0/3
[Sysname-GigabitEthernet1/0/3] ndp enable
[Sysname-GigabitEthernet1/0/3] quit
```

# Set the holdtime of NDP information to 200 seconds.

```
[Sysname] ndp timer aging 200
```

# Set the interval to send NDP packets to 70 seconds.

```
[Sysname] ndp timer hello 70
```

# Enable NTDP globally and on GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3.

```
[Sysname] ntdp enable
[Sysname] interface GigabitEthernet 1/0/2
[Sysname-GigabitEthernet1/0/2] ntdp enable
[Sysname-GigabitEthernet1/0/2] quit
[Sysname] interface GigabitEthernet 1/0/3
[Sysname-GigabitEthernet1/0/3] ntdp enable
[Sysname-GigabitEthernet1/0/3] quit
```

# Set the topology collection range to 2 hops.

```
[Sysname] ntdp hop 2
```

# Set the member device forward delay for topology collection requests to 150 ms.

```
[Sysname] ntdp timer hop-delay 150
```

# Set the member port forward delay for topology collection requests to 15 ms.

```
[Sysname] ntdp timer port-delay 15
```

# Set the interval to collect 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-e20f-0011
[aaa_0.Sysname-cluster] add-member 17 mac-address 000f-e20f-0012
```

# Set the holdtime of member device information to 100 seconds.

```
[aaa_0.Sysname-cluster] holdtime 100
```

# Set the interval to send handshake packets to 10 seconds.

```
[aaa_0.Sysname-cluster] timer 10
```

# 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 under the management device to the cluster, perform the following operations on a member device.

# Connect the member device to the remote shared FTP server of the cluster.

```
<aaa_1.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.

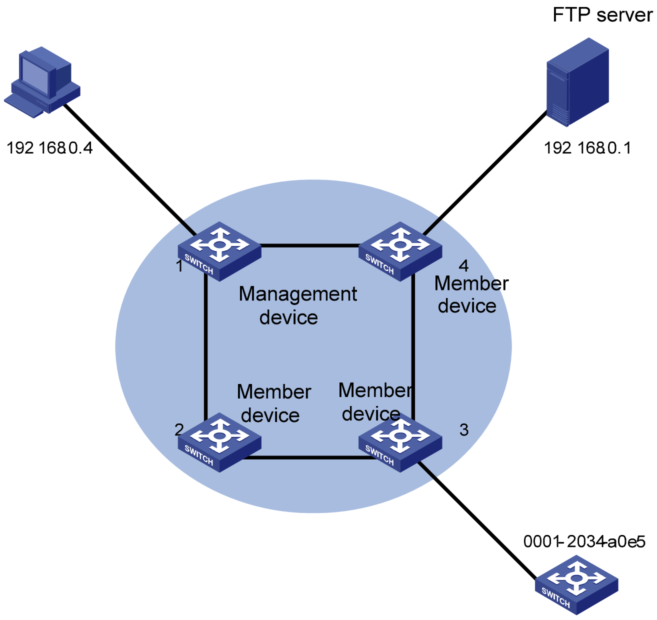
# Enhanced Cluster Feature Configuration Example

## 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 2-5** 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 SNMP Configuration

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

## 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.

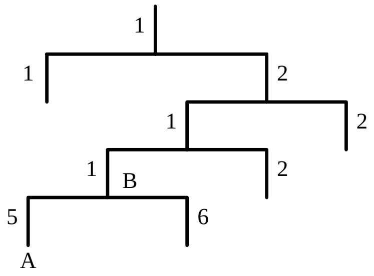
- Specifying MIB view that a community can access.

- 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.

# 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<br>Disabled by default.<br>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** *sys-contact* \| **location** *sys-location* \| **version** { { **v1** \| **v2c** \| **v3** }* \| **all** } } | Required<br>By default, the contact information for system maintenance is " 3Com Corporation.", the system location is " Marlborough, MA 01752 USA ", and the SNMP version is SNMPv3. |
| Set a community name and access permission | Direct configuration | Set a community name | **snmp-agent community** { **read** \| **write** } *community-name* [ **acl** *acl-number* \| **mib-view** *view-name* ]* | Required<br>• You can set an SNMPv1/SNMPv2c community name through direct configuration.<br>• Indirect configuration is compatible with SNMPv3. The added user is equal to the community name for SNMPv1 and SNMPv2c.<br>• You can choose either of them as needed. |
| | Indirect configuration | Set an SNMP group | **snmp-agent group** { **v1** \| **v2c** } *group-name* [ **read-view** *read-view* ] [ **write-view** *write-view* ] [ **notify-view** *notify-view* ] [ **acl** *acl-number* ] | |
| | | Add a user to an SNMP group | **snmp-agent usm-user** { **v1** \| **v2c** } *user-name group-name* [ **acl** *acl-number* ] | |
| Set the maximum size of an SNMP packet for SNMP agent to receive or send | | | **snmp-agent packet max-size** *byte-count* | Optional<br>1,500 bytes by default. |
| Set the device engine ID | | | **snmp-agent local-engineid** *engineid* | Optional<br>By default, the device engine ID is “enterprise number + device information”. |
| Create/Update the view information | | | **snmp-agent mib-view** { **included** \| **excluded** } *view-name oid-tree* [ **mask** *mask-value* ] | Optional<br>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<br>Disabled by default.<br>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** *sys-contact* \| **location** sys-*location* \| **version** { { **v1** \| **v2c** \| **v3** }* \| **all** } } | Optional<br>By default, the contact information for system maintenance is " 3Com Corporation.", the system location is " Marlborough, MA 01752 USA ", and the SNMP version is SNMPv3. |
| Set an SNMP group | **snmp-agent group v3** *group-name* [ **authentication** \| **privacy** ] [ **read-view** *read-view* ] [ **write-view** *write-view* ] [ **notify-view** *notify-view* ] [ **acl** *acl-number* ] | Required |
| Encrypt a plain-text password to generate a cipher-text one | **snmp-agent calculate-password** *plain-password* **mode** { **md5** \| **sha** } { **local-engineid** \| **specified-engineid** *engineid* } | Optional<br>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** *user-name group-name* [ [ **cipher** ] **authentication-mode** { **md5** \| **sha** } *auth-password* [ **privacy-mode** { **des56** \| **aes128** } *priv-password* ] ] [ **acl** *acl-number* ] | Required |
| Set the maximum size of an SNMP packet for SNMP agent to receive or send | **snmp-agent packet max-size** *byte-count* | Optional<br>1,500 bytes by default. |
| Set the device engine ID | **snmp-agent local-engineid** *engineid* | Optional<br>By default, the device engine ID is “enterprise number + device information”. |
| Create or update the view information | **snmp-agent mib-view** { **included** \| **excluded** } *view-name oid-tree* [ **mask** *mask-value* ] | Optional<br>By default, the view name is ViewDefault and OID is 1. |

**Note**

A Switch 4200G 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** \| **standard** [ **authentication** \| **coldstart** \| **linkdown** \| **linkup** \| **warmstart** ]* \| **system** ] | Optional<br>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** *interface-type interface-number* | |
| | 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** { *ip-address* } [ **udp-port** *port-number* ] **params securityname** *security-string* [ **v1** \| **v2c** \| **v3** [ **authentication** \| **privacy** ] ] | Required |
| Set the source address for traps | | **snmp-agent trap source** *interface-type interface-number* | Optional |
| Set the size of the queue used to hold the traps to be sent to the destination host | | **snmp-agent trap queue-size** *size* | Optional<br>The default is 100. |
| Set the aging time for traps | | **snmp-agent trap life** *seconds* | Optional<br>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<br>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<br>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** [ *group-name* ] | |
| Display SNMP user information | **display snmp-agent usm-user** [ **engineid** *engineid* \| **username** *user-name* \| **group** *group-name* ]* | |

| 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

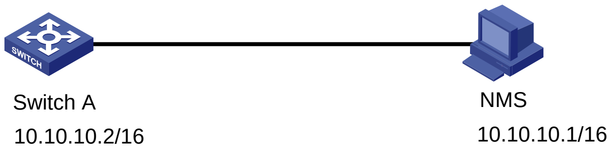
### Network requirements

- 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 **DES**
- 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 des56 cfb128cfb128
```

# Set the VLAN-interface 2 as the interface used by NMS. Add port GigabitEthernet 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 GigabitEthernet 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

Authentication-related configuration on an NMS must be consistent with that of the devices for the NMS to manage the devices successfully. For more information, refer to the corresponding manuals of 3Com's NMS products.

You can query and configure an Ethernet switch through the NMS.

# 2 RMON Configuration

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

## 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.

A Switch 4200G implements RMON in the second way. With an RMON agent embedded in, A Switch 4200G 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** *event-entry* [ **description** *string* ] { **log** \| **trap** *trap-community* \| **log-trap** *log-trapcommunity* \| **none** } [ **owner** *text* ] | Optional |
| Add an alarm entry | **rmon alarm** *entry-number alarm-variable sampling-time* { **delta** \| **absolute** } **rising_threshold** *threshold-value1 event-entry1* **falling_threshold** *threshold-value2 event-entry2* [ **owner** *text* ] | Optional<br>Before adding an alarm entry, you need to use the **rmon event** command to define the event to be referenced by the alarm entry. |
| Add an extended alarm entry | **rmon prialarm** *entry-number prialarm-formula prialarm-des sampling-timer* { **delta** \| **absolute** \| **changeratio** } **rising_threshold** *threshold-value1 event-entry1* **falling_threshold** *threshold-value2 event-entry2* **entrytype** { **forever** \| **cycle** *cycle-period* } [ **owner** *text* ] | Optional<br>Before adding an extended alarm entry, you need to use the **rmon event** command to define the event to be referenced by the extended alarm entry. |
| Enter Ethernet port view | **interface** *interface-type interface-number* | — |
| Add a history entry | **rmon history** *entry-number* **buckets** *number* **interval** *sampling-interval* [ **owner** *text* ] | Optional |
| Add a statistics entry | **rmon statistics** *entry-number* [ **owner** *text* ] | Optional |

Note

- The **rmon alarm** and **rmon prialarm** commands take effect on existing nodes only.
- For each port, only one RMON statistics entry can be created. That is, if an RMON statistics entry is already created for a given port, you will fail to create another statistics entry with a different index for the same port.

# Displaying RMON

| To do… | Use the command… | Remarks |
|---|---|---|
| Display RMON statistics | **display rmon statistics** [ *interface-type interface-number* \| **unit** *unit-number* ] | Available in any view. |
| Display RMON history information | **display rmon history** [ *interface-type interface-number* \| **unit** *unit-number* ] | |
| Display RMON alarm information | **display rmon alarm** [ *entry-number* ] | |
| Display extended RMON alarm information | **display rmon prialarm** [ *prialarm-entry-number* ] | |
| Display RMON events | **display rmon event** [ *event-entry* ] | |
| Display RMON event logs | **display rmon eventlog** [ *event-entry* ] | |

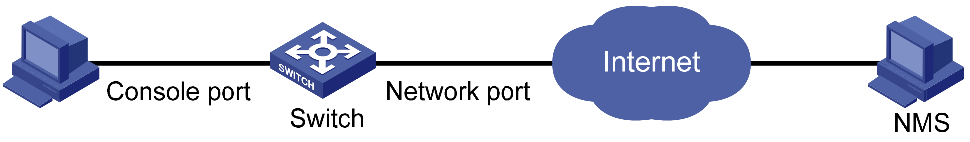
# RMON Configuration Example

## 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 GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] rmon statistics 1
```

```
[Sysname-GigabitEthernet1/0/1] 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 GigabitEthernet 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 Multicast Overview

## Multicast Overview

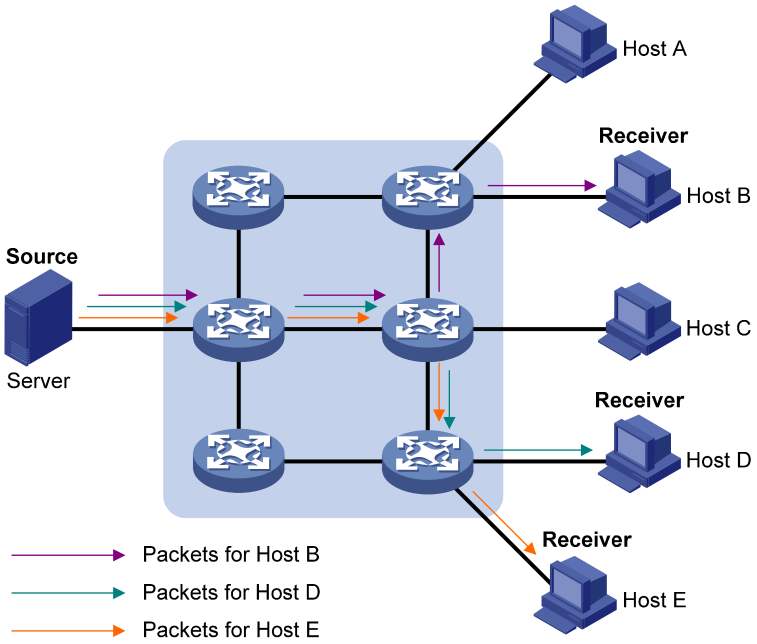
With development of networks on the Internet, more and more interaction services such as data, voice, and video services are running on the networks. In addition, highly bandwidth- and time-critical services, such as e-commerce, Web conference, online auction, video on demand (VoD), and tele-education have come into being. These services have higher requirements for information security, legal use of paid services, and network bandwidth.

In the network, packets are sent in three modes: unicast, broadcast and multicast. The following sections describe and compare data interaction processes in unicast, broadcast, and multicast.

### 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 1-10:

**Figure 1-1** Information transmission in the unicast mode

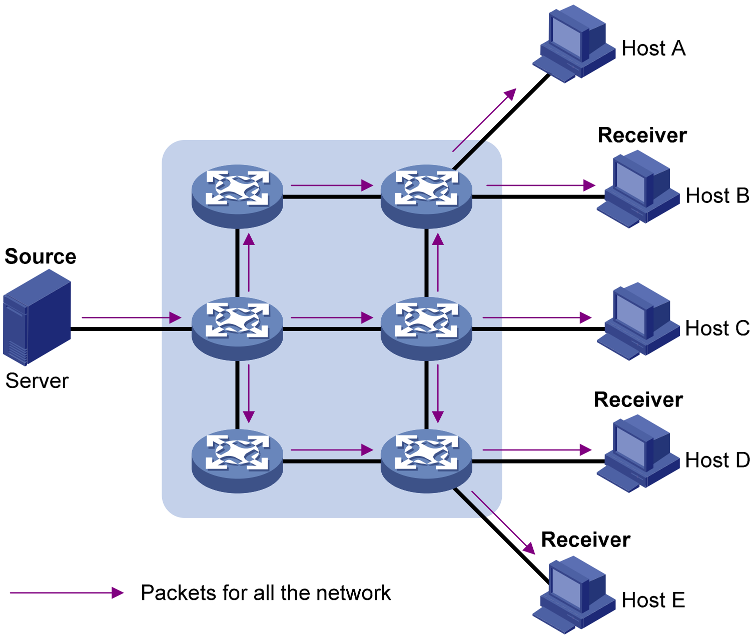


Assume that Hosts B, D and E need this information. The source server establishes transmission channels for the devices of these users respectively. As the transmitted traffic over the network is in direct proportion to the number of users that receive this information, when a large number of users need this information, the server must send many pieces of information with the same content to the users. Therefore, the limited bandwidth becomes the bottleneck in information transmission. This shows that unicast is not good for the transmission of a great deal of information.

## Information Transmission in the Broadcast Mode

When you adopt broadcast, the system transmits information to all users on a network. Any user on the network can receive the information, no matter the information is needed or not. 0 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 routers, and Hosts A and C on the network also receive this information.

As we can see from the information transmission process, the security and legal use of paid service cannot be guaranteed. In addition, when only a small number of users on the same network need the information, the utilization ratio of the network resources is very low and the bandwidth resources are greatly wasted.

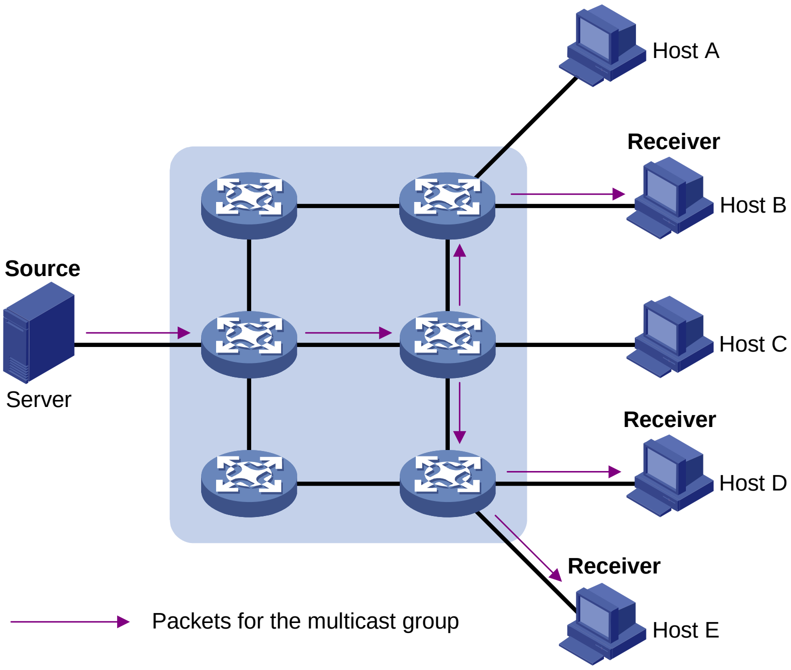
Therefore, broadcast is disadvantageous in transmitting data to specific users; moreover, broadcast occupies large bandwidth.

## Information Transmission in the Multicast Mode

As described in the previous sections, unicast is suitable for networks with sparsely distributed users, whereas broadcast is suitable for networks with densely distributed users. When the number of users requiring information is not certain, unicast and broadcast deliver a low efficiency.

Multicast solves this problem. When some users on a network require specified information, the multicast information sender (namely, the multicast source) sends the information only once. With 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 assimilate multicast transmission to the 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.

## 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 provides the following applications:

- Applications of multimedia and flow media, such as Web TV, Web radio, and real-time video/audio conferencing.
- Communication for training and cooperative operations, such as remote education.
- Database and financial applications (stock), and so on.
- Any point-to-multiple-point data application.

# 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 transports information?
- Multicast routing: How is information transported?

IP multicast is a kind of peer-to-peer service. Based on the protocol layer sequence from bottom to top, the multicast mechanism contains addressing mechanism, host registration, multicast routing, and multicast application:

- 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<br>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. |

| Class D address range | Description |
|---|---|
| 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 |
| 224.0.0.18 | Virtual router redundancy protocol (VRRP) |
| 224.0.0.19 to 224.0.0.255 | Other protocols |

**Note**

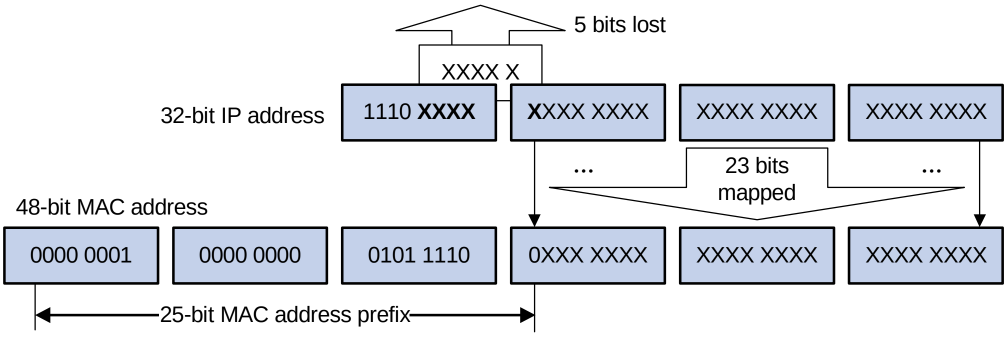
Like having reserved the private network segment 10.0.0.0/8 for unicast, IANA has also reserved the network segment 239.0.0.0/8 for multicast. These are administratively scoped addresses. With the administratively scoped addresses, you can define the range of multicast domains flexibly to isolate IP 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. 0 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.

## 1.1.1 Multicast Protocols

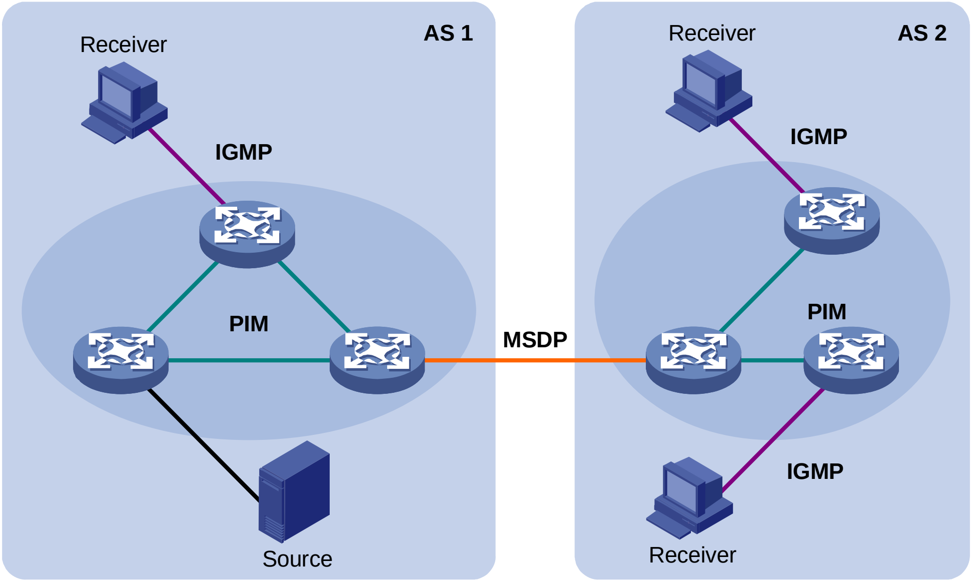
**Note**

- 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. 0 describes where these multicast protocols are in a network.

**Figure 1-5** Positions of Layer 3 multicast protocols



1) 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.

2) 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.

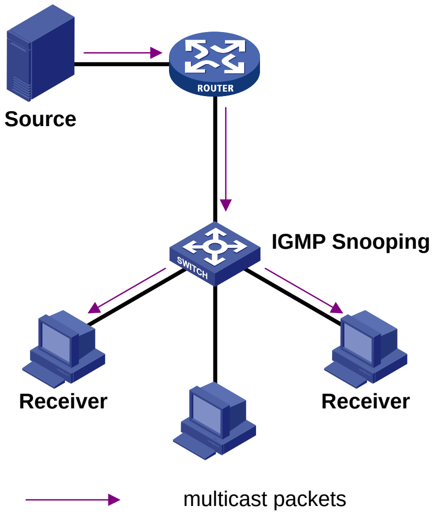
- An intra-domain multicast routing protocol is used to discover multicast sources and build multicast distribution trees within an autonomous system (AS) so as to deliver multicast data to receivers. Among a variety of mature intra-domain multicast routing protocols, protocol independent multicast (PIM) 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 the flooding of multicast data in a Layer 2 network.

# 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.

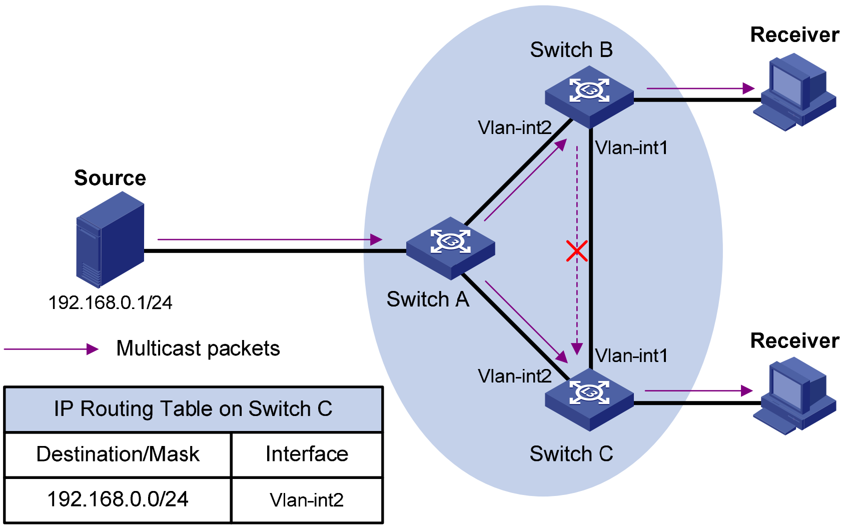
## RPF Check

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



| IP Routing Table on Switch C | |
|---|---|
| Destination/Mask | Interface |
| 192.168.0.0/24 | Vlan-int2 |

- 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 IGMP Snooping Configuration

## IGMP Snooping Overview

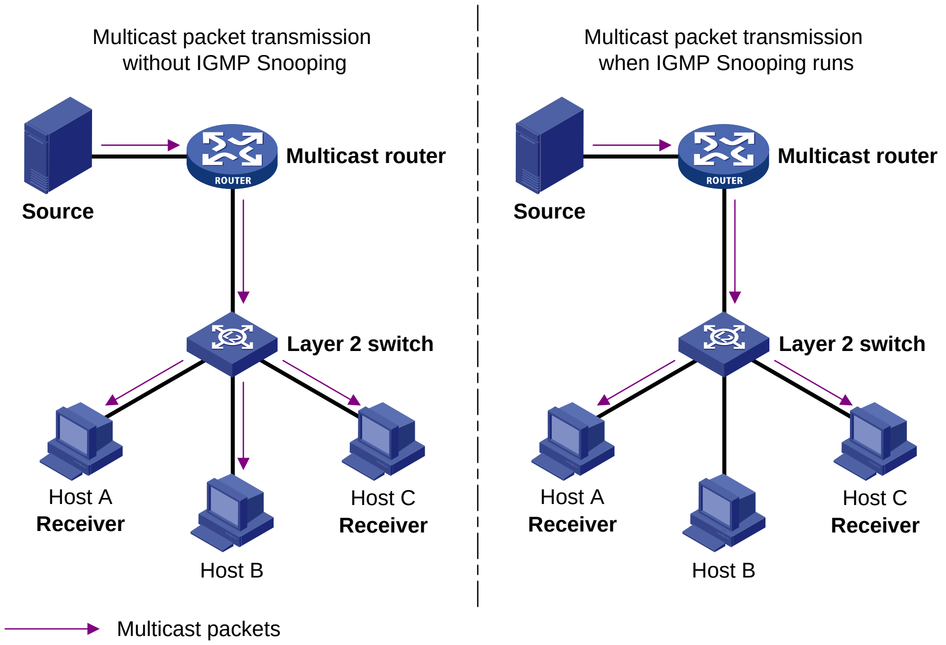
Internet Group Management Protocol Snooping (IGMP Snooping) is a multicast constraining mechanism that runs on Layer 2 devices to manage and control multicast groups.

### 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 2-1, 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.

**Figure 2-1** Before and after IGMP Snooping is enabled on Layer 2 device

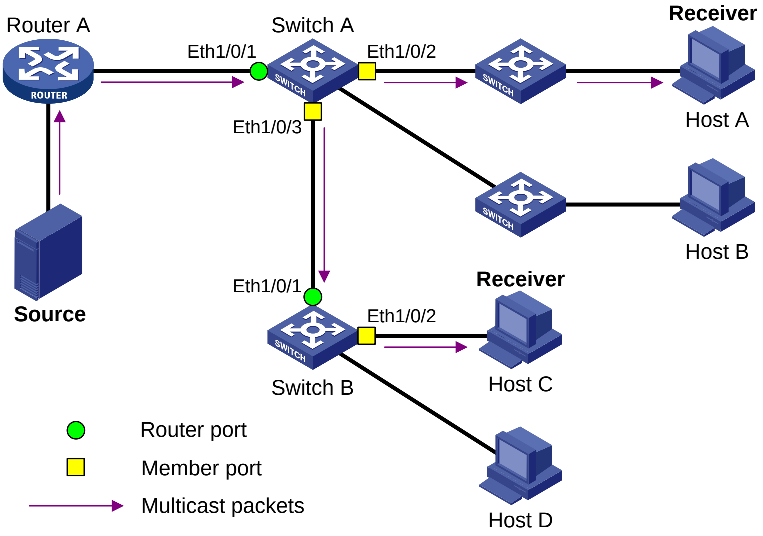


### Basic Concepts in IGMP Snooping

#### IGMP Snooping related ports

As shown in Figure 2-2, 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 2-2** IGMP Snooping related ports



Ports involved in IGMP Snooping, as shown in Figure 2-2, 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 2-1** 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.

### 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 leaf 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.

# IGMP Snooping Configuration

The following table lists all the IGMP Snooping configuration tasks:

**Table 2-2** IGMP Snooping configuration tasks

| Operation | 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 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 |
| Configuring a Port as a Simulated Group Member | Optional |
| Configuring a VLAN Tag for Query Messages | Optional |
| Configuring Multicast VLAN | Optional |

## 1.1.1 Enabling IGMP Snooping

**Table 2-3** Enable IGMP Snooping

| Operation | Command | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enable IGMP Snooping globally | **igmp-snooping enable** | Required<br>By default, IGMP Snooping is disabled globally. |
| Enter VLAN view | **vlan** *vlan-id* | — |
| Enable IGMP Snooping on the VLAN | **igmp-snooping enable** | Required<br>By default, IGMP Snooping is disabled on all the VLANs. |

⚠ **Caution**

- 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 0  Configuring a VLAN Tag for Query Messages.

## Configuring the Version of IGMP Snooping

With the development of multicast technologies, IGMPv3 has found increasingly wide application. In IGMPv3, a host can not only join a specific multicast group but also explicitly specify to receive or reject the information from a specific multicast source. Working with PIM-SSM, IGMPv3 enables hosts to join specific multicast sources and groups directly, greatly simplifying multicast routing protocols and optimizing the network topology.

**Table 2-4** Configure the version of IGMP Snooping

| Operation | Command | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter VLAN view | **vlan** *vlan-id* | — |
| Configure the version of IGMP Snooping | **igmp-snooping version** *version-number* | Optional<br>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.

**Table 2-5** Configure timers

| Operation | Command | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Configure the aging timer of the router port | **igmp-snooping router-aging-time** *seconds* | Optional<br>By default, the aging time of the router port is 105 seconds. |
| Configure the query response timer | **igmp-snooping max-response-time** *seconds* | Optional<br>By default, the query response timeout time is 10 seconds. |
| Configure the aging timer of the multicast member port | **igmp-snooping host-aging-time** *seconds* | Optional<br>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 to improve bandwidth management.

### Enabling fast leave processing in system view

**Table 2-6** Enable fast leave processing in system view

| Operation | Command | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enable fast leave processing | **igmp-snooping fast-leave** [ **vlan** *vlan-list* ] | Required<br>By default, the fast leave processing feature is disabled. |

### Enabling fast leave processing in Ethernet port view

**Table 2-7** Enable fast leave processing in Ethernet view

| Operation | Command | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter Ethernet port view | **interface** *interface-type interface-number* | — |
| Enable fast leave processing for specific VLANs | **igmp-snooping fast-leave** [ **vlan** *vlan-list* ] | Required<br>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).
- If fast leave processing and unknown multicast packet dropping 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.

## 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

**Table 2-8** Configure a multicast group filter in system view

| Operation | Command | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |

| Operation | Command | Remarks |
|---|---|---|
| Configure a multicast group filter | **igmp-snooping group-policy** *acl-number* [ **vlan** *vlan-list* ] | Required<br>No group filter is configured by default, namely hosts can join any multicast group. |

### Configuring a multicast group filter in Ethernet port view

**Table 2-9** Configure a multicast group filter in Ethernet port view

| Operation | Command | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter Ethernet port view | **interface** *interface-type interface-number* | — |
| Configure a multicast group filter | **igmp-snooping group-policy** *acl-number* [ **vlan** *vlan-list* ] | Optional<br>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.

**Table 2-10** Configure the maximum number of multicast groups on a port

| Operation | Command | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter Ethernet port view | **interface** *interface-type interface-number* | — |

| Operation | Command | Remarks |
|---|---|---|
| Limit the number of multicast groups on a port | **igmp-snooping group-limit** *limit* [ **vlan** *vlan-list* [ **overflow-replace** ] ] | Required<br>The system default for Switch 4200G series is 256. |

**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.

## Configuring IGMP Querier

In an IP multicast network running IGMP, a multicast router or Layer 3 multicast switch 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.

However, a Layer 2 multicast switch does not support IGMP, and therefore cannot send general queries by default. By enabling IGMP Snooping on a Layer 2 switch in a VLAN where multicast traffic needs to be Layer-2 switched only and no multicast routers are present, the Layer 2 switch will act as the IGMP Snooping querier to send IGMP general queries, thus allowing multicast forwarding entries to be established and maintained at the data link layer.

You can also configure the source address, maximum response time and interval of general queries to be sent from the IGMP Snooping querier.

**Table 2-11** Configure IGMP Snooping querier

| Operation | Command | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enable IGMP Snooping | **igmp-snooping enable** | Required<br>By default, IGMP Snooping is disabled. |
| Enter VLAN view | **vlan** *vlan-id* | — |
| Enable IGMP Snooping | **igmp-snooping enable** | Required. |
| Enable IGMP Snooping querier | **igmp-snooping querier** | Required<br>By default, IGMP Snooping querier is disabled. |

| Operation | Command | Remarks |
|---|---|---|
| Configure the interval of sending general queries | **igmp-snooping query-interval** *seconds* | Optional<br>By default, the interval of sending general queries is 60 seconds. |
| Configure the source IP address of general queries | **igmp-snooping general-query source-ip** { **current-interface** \| *ip-address* } | Optional<br>By default, the source IP address of general queries is 0.0.0.0. |

## 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.

**Table 2-12** Suppress flooding of unknown multicast traffic in the VLAN

| Operation | Command | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enable unknown multicast flooding suppression | **igmp-snooping nonflooding-enable** | Required<br>By default, unknown multicast flooding suppression |

**Note**

If the function of dropping unknown multicast packets is enabled, you cannot enable unknown multicast flooding suppression.

## 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

**Table 2-13** Configure a static multicast group member port in Ethernet port view

| Operation | Command | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter Ethernet port view | **interface** *interface-type interface-number* | — |

| Operation | Command | Remarks |
|---|---|---|
| Configure the current port as a static member port for a multicast group in a VLAN | **multicast static-group** *group-address* **vlan** *vlan-id* | Required<br>By default, no port is configured as a static multicast group member port. |

### In VLAN interface view

**Table 2-14** Configure a static multicast group member port in VLAN interface view

| Operation | Command | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter VLAN interface view | **interface vlan-interface** *interface-number* | — |
| Configure specified port(s) as static member port(s) of a multicast group in the VLAN | **multicast static-group** *group-address* **interface** *interface-list* | Required<br>By default, no port is configured as a static multicast group 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

**Table 2-15** Configure a static router port in Ethernet port view

| Operation | Command | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter Ethernet port view | **interface** *interface-type interface-number* | — |
| Configure the current port as a static router port | **multicast static-router-port vlan** *vlan-id* | Required<br>By default, no static router port is configured. |

### In VLAN view

**Table 2-16** Configure a static router port in VLAN view

| Operation | Command | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter VLAN view | **vlan** *vlan-id* | — |
| Configure a specified port as a static router port | **multicast static-router-port** *interface-type interface-number* | Required<br>By default, no static router port is configured. |

## Configuring a Port as a Simulated Group Member

Generally, hosts running IGMP respond to the IGMP query messages of the multicast switch. If hosts fail to respond for some reason, the multicast switch may consider that there is no member of the multicast group on the local subnet and remove the corresponding path.

To avoid this from happening, you can configure a port of the VLAN of the switch as a multicast group member. When the port receives IGMP query messages, the multicast switch will respond. As a result, the port of the VLAN 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 switch 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 switch 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.

**Table 2-17** Configure a port as a simulated group member

| Operation | Command | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter Ethernet port view | **interface** *interface-type interface-number* | — |
| Configure the current port as a simulated multicast group member | **igmp host-join** *group-address* [**source-ip** *source-address* ] **vlan** *vlan-id* | Optional<br>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 IMGPv3 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:

**Table 2-18** Configure VLAN Tag for query message

| Operation | Command | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enable IGMP Snooping | **igmp-snooping enable** | Required<br>By default, IGMP Snooping is disabled. |
| Configure a VLAN tag for query messages | **igmp-snooping vlan-mapping vlan** *vlan-id* | Required<br>By default, no VLAN tag is configured for general and group-specific query messages sent or forwarded by IGMP Snooping. |

**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.

**Table 2-19** Configure multicast VLAN on the Layer 3 switch

| Operation | Command | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Create a multicast VLAN and enter VLAN view | **vlan** *vlan-id* | — |
| Return to system view | **quit** | — |
| Enter VLAN interface view | **interface Vlan-interface** *vlan-id* | — |

| Operation | Command | Remarks |
|---|---|---|
| Enable IGMP | **igmp enable** | Required<br>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** *interface-type interface-number* | — |
| Define the port as a trunk or hybrid port | **port link-type** { **trunk** \| **hybrid** } | Required |
| Specify the VLANs to be allowed to pass the Ethernet port | **port hybrid vlan** *vlan-id-list* { **tagged** \| **untagged** } | Required<br>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** *vlan-list* | |

**Table 2-20** Configure multicast VLAN on the Layer 2 switch

| Operation | Command | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enable IGMP Snooping | **igmp-snooping enable** | — |
| Enter VLAN view | **vlan** *vlan-id* | — |
| 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** *interface-type interface-number* | — |
| Define the port as a trunk or hybrid port | **port link-type** { **trunk** \| **hybrid** } | Required |
| Specify the VLANs to be allowed to pass the Ethernet port | **port hybrid vlan** *vlan-list* { **tagged** \| **untagged** } | Required<br>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** *vlan-list* | |
| Enter Ethernet port view for a user device | **interface** *interface-type interface-number* | — |
| Define the port as a hybrid port | **port link-type hybrid** | Required |
| Specify the VLANs to be allowed to pass the port | **port hybrid vlan** *vlan-id-list* { **tagged** \| **untagged** } | Required<br>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.
- When the multicast VLAN is set up, all IGMP report messages are forwarded to the router ports in the multicast VLAN. If no router ports exist in the multicast VLAN, all IGMP report messages are flooded within the multicast VLAN.

# Displaying and Maintaining IGMP Snooping

After the configuration above, you can execute the following **display** commands in any view to verify the configuration by checking the displayed information.

You can execute the **reset** command in user view to clear the statistics information about IGMP Snooping.

**Table 2-21** Display and maintain IGMP Snooping

| Operation | Command | Remarks |
|---|---|---|
| Display the current IGMP Snooping configuration | **display igmp-snooping configuration** | You can execute the **display** commands in any view. |
| Display IGMP Snooping message statistics | **display igmp-snooping statistics** | |
| Display the information about IP and MAC multicast groups in one or all VLANs | **display igmp-snooping group** [ **vlan** *vlanid* ] | |
| Clear IGMP Snooping statistics | **reset igmp-snooping statistics** | You can execute the **reset** command in user view. |

# IGMP Snooping Configuration Examples

## Configuring IGMP Snooping

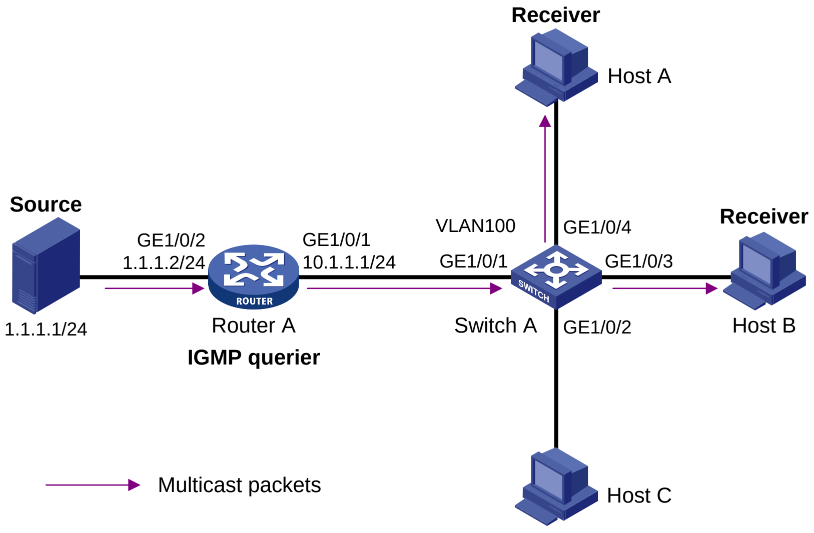
### Network requirements

To prevent multicast traffic from being flooded at Layer 2, enable IGMP snooping on Layer 2 switches.

- As shown in Figure 2-3, Router A connects to a multicast source (Source) through GigabitEthernet1/0/2, and to Switch A through GigabitEthernet1/0/1.
- 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 2-3** 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 2-3. The detailed configuration steps are omitted.

2) Configure Router A

# Enable IP multicast routing, enable PIM-DM on each interface, and enable IGMP on GigabitEthernet1/0/1.

```
<RouterA> system-view
[RouterA] multicast routing-enable
[RouterA] interface GigabitEthernet 1/0/1
[RouterA-GigabitEthernet1/0/1] igmp enable
[RouterA-GigabitEthernet1/0/1] quit
[RouterA] interface GigabitEthernet 1/0/2
[RouterA-GigabitEthernet1/0/2] pim dm
[RouterA-GigabitEthernet1/0/2] quit
```

3) Configure Switch A

# Enable IGMP Snooping globally.

```
<SwitchA> system-view
[SwitchA] igmp-snooping enable
  Enable IGMP-Snooping ok.
```

# Create VLAN 100, assign GigabitEthernet1/0/1 through GigabitEthernet1/0/4 to this VLAN, and enable IGMP Snooping in the VLAN.

```
[SwitchA] vlan 100
[SwitchA-vlan100] port GigabitEthernet 1/0/1 to GigabitEthernet 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):
                     GigabitEthernet1/0/1
    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):
                     GigabitEthernet1/0/3          GigabitEthernet1/0/4
    MAC group(s):
        MAC group address: 0100-5e01-0101
        Host port(s):GigabitEthernet1/0/3          GigabitEthernet1/0/4
```

As shown above, the multicast group 224.1.1.1 is established on Switch A, with the dynamic router port GigabitEthernet1/0/1 and dynamic member ports GigabitEthernet1/0/3 and GigabitEthernet1/0/4. 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 2-4, 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 2-22 describes the network devices involved in this example and the configurations you should make on them.

**Table 2-22** Network devices and their configurations

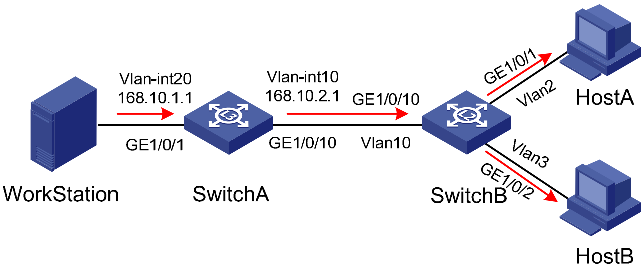
| Device | Device description | Networking description |
|---|---|---|
| Switch A | Layer 3 switch | The interface IP address of VLAN 20 is 168.10.1.1. GigabitEthernet 1/0/1 is connected to the workstation and belongs to VLAN 20.<br>The interface IP address of VLAN 10 is 168.10.2.1. GigabitEthernet 1/0/10 belongs to VLAN 10. GigabitEthernet 1/0/10 is connected to Switch B. |

| Device | Device description | Networking description |
|---|---|---|
| Switch B | Layer 2 switch | • VLAN 2 contains GigabitEthernet 1/0/1 and VLAN 3 contains GigabitEthernet 1/0/2.<br>• The default VLANs of GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 are VLAN 2 and VLAN 3 respectively.<br>• VLAN 10 contains GigabitEthernet 1/0/10, GigabitEthernet 1/0/1, and GigabitEthernet 1/0/2. GigabitEthernet 1/0/10 is connected to Switch A.<br>• VLAN 10 is a multicast VLAN.<br>• GigabitEthernet 1/0/1 sends untagged packets for VLAN 2 and VLAN 10.<br>• GigabitEthernet 1/0/2 sends untagged packets for VLAN 3 and VLAN 10. |
| Host A | User 1 | Host A is connected to GigabitEthernet 1/0/1 on Switch B. |
| Host B | User 2 | Host B is connected to GigabitEthernet 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 2-4** 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 GigabitEthernet 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 GigabitEthernet 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 GigabitEthernet 1/0/10
[SwitchA-GigabitEthernet1/0/10] port link-type hybrid
[SwitchA-GigabitEthernet1/0/10] port hybrid vlan 10 tagged
[SwitchA-GigabitEthernet1/0/10] 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
```

2) Configure Switch B:

# Enable the IGMP Snooping feature on Switch B.

```
<SwitchB> system-view
[SwitchB] igmp-snooping enable
```

# Configure VLAN 10 as the multicast VLAN and enable IGMP Snooping on it.

```
[SwitchB] vlan 10
[SwitchB-vlan10] service-type multicast
[SwitchB-vlan10] igmp-snooping enable
[SwitchB-vlan10] quit
```

# Define GigabitEthernet 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 GigabitEthernet 1/0/10
[SwitchB-GigabitEthernet1/0/10] port link-type hybrid
[SwitchB-GigabitEthernet1/0/10] port hybrid vlan 2 3 10 tagged
[SwitchB-GigabitEthernet1/0/10] quit
```

# Define GigabitEthernet 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 GigabitEthernet 1/0/1
[SwitchB-GigabitEthernet1/0/1] port link-type hybrid
[SwitchB-GigabitEthernet1/0/1] port hybrid vlan 2 10 untagged
[SwitchB-GigabitEthernet1/0/1] port hybrid pvid vlan 2
[SwitchB-GigabitEthernet1/0/1] quit
```

# Define GigabitEthernet 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 GigabitEthernet 1/0/2
[SwitchB-GigabitEthernet1/0/2] port link-type hybrid
[SwitchB-GigabitEthernet1/0/2] port hybrid vlan 3 10 untagged
```

```
[SwitchB-GigabitEthernet1/0/2] port hybrid pvid vlan 3
[SwitchB-GigabitEthernet1/0/2] 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.

# 3 Common Multicast Configuration

## Common Multicast Configuration

### 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.

**Table 3-1** Configure a multicast MAC address entry in system view

| Operation | Command | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Create a multicast MAC address entry | **mac-address multicast** *mac-address* **interface** *interface-list* **vlan** *vlan-id* | Required<br>The *mac-address* argument must be a multicast MAC address. |

**Table 3-2** Configure a multicast MAC address entry in Ethernet port view

| Operation | Command | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enter Ethernet port view | **interface** *interface-type interface-number* | — |
| Create a multicast MAC address entry. | **mac-address multicast** *mac-address* **vlan** *vlan-id* | Required<br>The *mac-address* argument must be a multicast MAC address. |

**Note**

- If the multicast MAC address entry to be created already exists, the system gives you a prompt.
- If you want to add a port to a multicast MAC address entry created through the **mac-address multicast** command, you need to remove the entry first, create this entry again, and then add the specified port to the forwarding ports of this entry.
- 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. 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.

**Table 3-3** Configure dropping unknown multicast packet

| Operation | Command | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Configure dropping unknown multicast packets | **unknown-multicast drop enable** | Required<br>By default, the function of dropping unknown multicast packets is disabled. |

# Displaying Common Multicast Configuration

After the above-described configuration, you can use the **display** command in any view to verify the configuration.

**Table 3-4** Display common multicast configuration

| Operation | Command | Remarks |
|---|---|---|
| Display the created multicast MAC table entries | **display mac-address multicast** [ **static** { { *mac-address* **vlan** *vlan-id* **\| vlan** *vlan-id* } [ **count** ] } \| **count** } ] | You can execute the **display** commands in any view. |

# Table of Contents

# 1 NTP Configuration

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

## 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 and MD5 encrypted 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 S4200G 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.

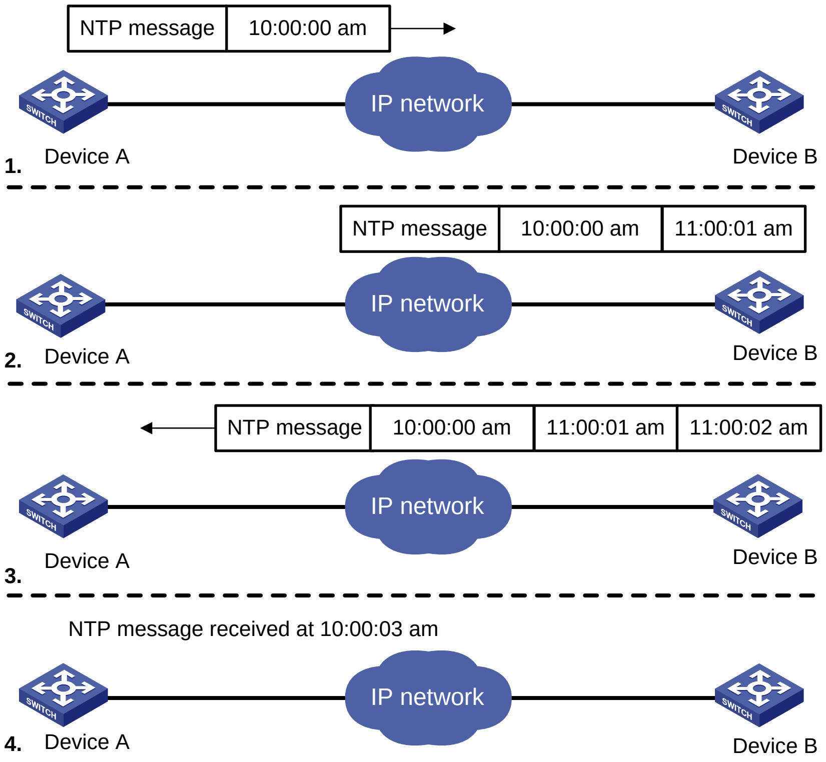
## Implementation Principle of NTP

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 (T4).

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.

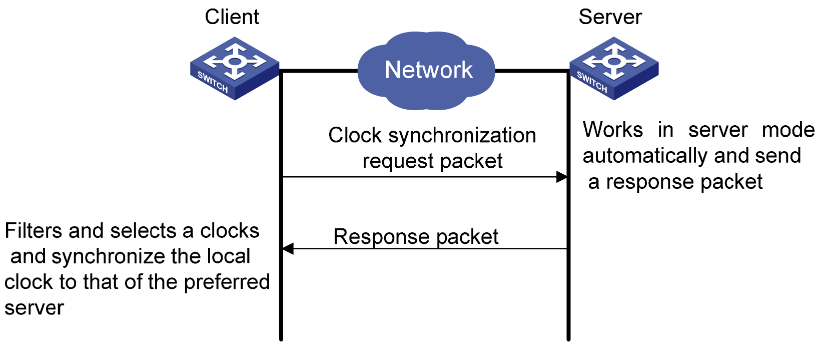
For detailed information, refer to RFC 1305.

## 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.

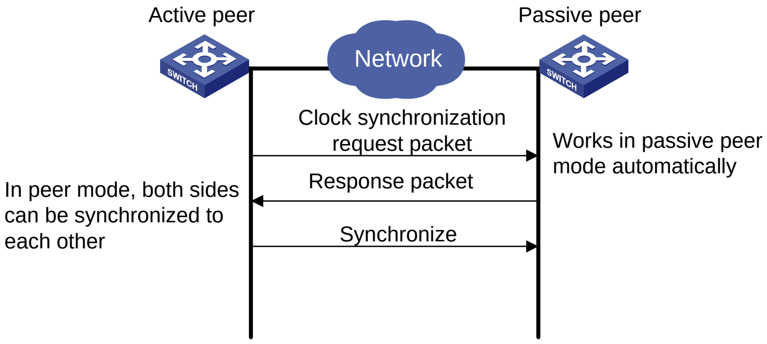
### Server/client mode

**Figure 1-2** Server/client mode


Client
Server
Network
SWITCH
SWITCH
Clock synchronization request packet
Works in server mode automatically and send a response packet
Response packet
Filters and selects a clocks and synchronize the local clock to that of the preferred server

### Symmetric peer mode

**Figure 1-3** Symmetric peer mode

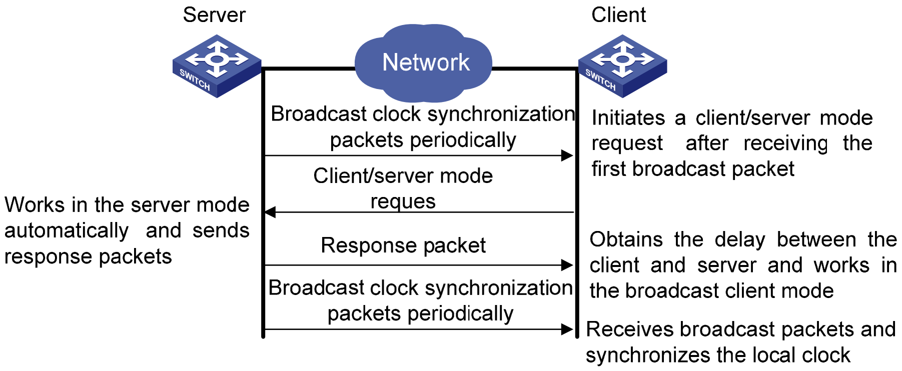

Active peer
Passive peer
Network
SWITCH
SWITCH
Clock synchronization request packet
Works in passive peer mode automatically
Response packet
In peer mode, both sides can be synchronized to each other
Synchronize

In the symmetric peer mode, the local S4200G 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


Server
Client
Network
Broadcast clock synchronization packets periodically
Initiates a client/server mode request after receiving the first broadcast packet
Client/server mode reques
Works in the server mode automatically and sends response packets
Response packet
Obtains the delay between the client and server and works in the broadcast client mode
Broadcast clock synchronization packets periodically
Receives broadcast packets and synchronizes the local clock

### Multicast mode

**Figure 1-5** Multicast mode

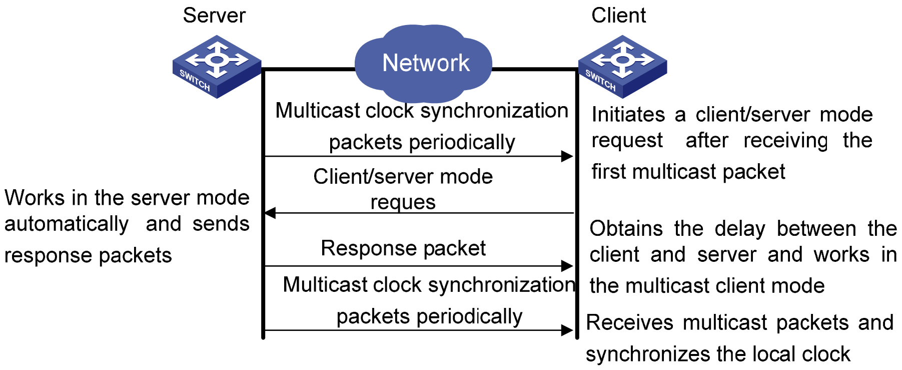

Server
Client
Network
Multicast clock synchronization packets periodically
Initiates a client/server mode request after receiving the first multicast packet
Client/server mode reques
Works in the server mode automatically and sends response packets
Response packet
Obtains the delay between the client and server and works in the multicast client mode
Multicast clock synchronization packets periodically
Receives multicast packets and synchronizes the local clock

Table 1-1 describes how the above mentioned NTP modes are implemented on 3Com S4200G series Ethernet switches.

**Table 1-1** NTP implementation modes on 3Com S4200G series Ethernet switches

| NTP implementation mode | Configuration on S4200G series switches |
|---|---|
| Server/client mode | Configure the local S4200G 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 S4200G switch to work in NTP symmetric peer mode. In this mode, the remote server serves as the symmetric-passive peer of the S4200G switch, and the local switch serves as the symmetric-active peer. |
| Broadcast mode | • Configure the local S4200G 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.<br>• Configure the S4200G switch to work in NTP broadcast client mode. In this mode, the local S4200G switch receives broadcast NTP messages through the VLAN interface configured on the switch. |

| NTP implementation mode | Configuration on S4200G series switches |
|---|---|
| Multicast mode | • Configure the local S4200G 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.<br>• Configure the local S4200G 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 a 3Com S4200G 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 3Com S4200G 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 S4200G 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, 3Com S4200G 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** { *remote-ip* \| *server-name* } [ **authentication-keyid** *key-id* \| **priority** \| **source-interface Vlan-interface** *vlan-id* \| **version** *number* ]* | Required<br>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** { *remote-ip* \| *peer-name* } [ **authentication-keyid** *key-id* \| **priority** \| **source-interface Vlan-interface** *vlan-id* \| **version** *number* ]* | Required<br>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.

**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** *vlan-id* | — |
| Configure the switch to work in the NTP broadcast server mode | **ntp-service broadcast-server** [ **authentication-keyid** *key-id* \| **version** *number* ]* | Required<br>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** *vlan-id* | — |
| Configure the switch to work in the NTP broadcast client mode | **ntp-service broadcast-client** | Required<br>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.

**Note**

- A multicast server can synchronize multicast clients only after its clock has been synchronized.
- An S4200G 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** *vlan-id* | — |
| Configure the switch to work in the NTP multicast server mode | **ntp-service multicast-server** [ *ip-address* ]<br>[ **authentication-keyid** *keyid* \| **ttl** *ttl-number* \| **version** *number* ]* | Required<br>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** *vlan-id* | — |
| Configure the switch to work in the NTP multicast client mode | **ntp-service multicast-client** [ *ip-address* ] | Required<br>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.

From the highest NTP service access-control right to the lowest one 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** | — |

| To do… | Use the command… | Remarks |
|---|---|---|
| Configure the NTP service access-control right to the local switch for peer devices | **ntp-service access** { **peer** \| **server** \| **synchronization** \| **query** } *acl-number* | Optional<br>**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 |

## 1.1.1 Configuration Prerequisites

NTP authentication configuration involves:

- Configuring NTP authentication on the client
- Configuring NTP authentication on the server

Observe the following principles when configuring NTP authentication:

- If the NTP authentication function is not enabled on the client, the 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<br>Disabled by default. |
| Configure the NTP authentication key | | **ntp-service authentication-keyid** *key-id* **authentication-model md5** *value* | Required<br>By default, no NTP authentication key is configured. |
| Configure the specified key as a trusted key | | **ntp-service reliable authentication-keyid** *key-id* | Required<br>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** { *remote-ip* \| *server-name* } **authentication-keyid** *key-id* | Required<br>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** { *remote-ip* \| *peer-name* } **authentication-keyid** *key-id* | |

**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** | — |

| To do… | | Use the command… | Remarks |
|---|---|---|---|
| Enable NTP authentication | | **ntp-service authentication enable** | Required<br>Disabled by default. |
| Configure an NTP authentication key | | **ntp-service authentication-keyid** *key-id* **authentication-mode md5** *value* | Required<br>By default, no NTP authentication key is configured. |
| Configure the specified key as a trusted key | | **ntp-service reliable authentication-keyid** *key-id* | Required<br>By default, no trusted authentication key is configured. |
| Enter VLAN interface view | | **interface Vlan-interface** *vlan-id* | — |
| Associate the specified key with the corresponding broadcast/multicast client | Configure on the NTP broadcast server | **ntp-service broadcast-server authentication-keyid** *key-id* | • In NTP broadcast server mode and NTP multicast server mode, you need to associate the specified key with the corresponding broadcast/multicast client<br>• 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** *key-id* | |

**Note**

- The procedure for configuring NTP authentication on the server is the same as that on the client. Besides, the client and the server must be configured with the same authentication key.
- In NTP server mode and NTP peer mode, you need to associate the specified key with the corresponding NTP server (symmetric-active peer) on the client (symmetric-passive peer). In these two modes, multiple NTP servers (symmetric-active peers) may be configured for a client/passive peer, and therefore, the authentication key is required to determine which NTP server the local clock is synchronized to.

## 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** *vlan-id* | 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** *number* | Required<br>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** *vlan-id* | — |
| Disable an interface from receiving NTP messages | **ntp-service in-interface disable** | Required<br>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

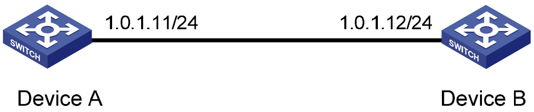
## Configuring NTP Server/Client Mode

### 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 S4200G 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: 60.0002 Hz
 Actual frequency: 60.0002 Hz
 Clock precision: 2^18
 Clock offset: 0.0000 ms
 Root delay: 0.00 ms
 Root dispersion: 0.00 ms
 Peer dispersion: 0.00 ms
 Reference time: 00:00:00.000 UTC Jan 1 1900 (00000000.00000000)
```

# Set 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: 60.0002 Hz
 Actual frequency: 60.0002 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
```

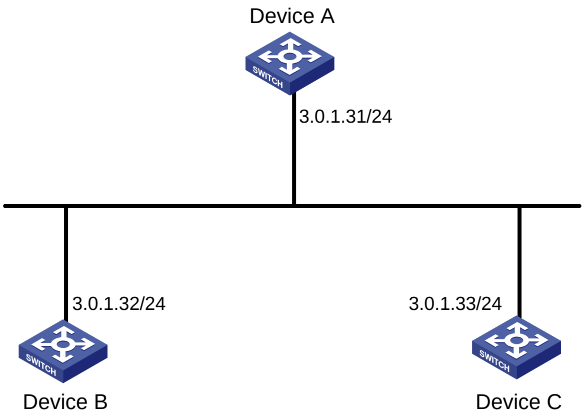
## Configuring NTP Symmetric Peer Mode

### 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 S4200G 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: 60.0002 Hz
 Actual frequency: 60.0002 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       stra 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
```

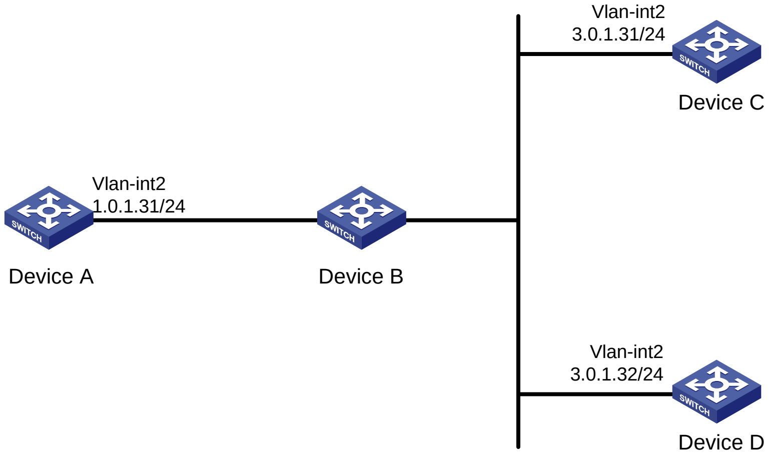
## Configuring NTP Broadcast Mode

### 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 S4200G 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: 60.0002 Hz
 Actual frequency: 60.0002 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
```

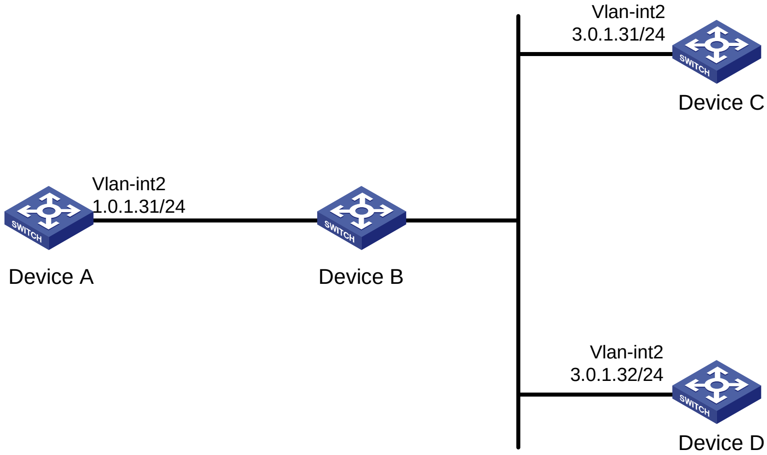
## Configuring NTP Multicast Mode

### 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 S4200G 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: 60.0002 Hz
 Actual frequency: 60.0002 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
```

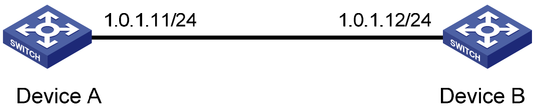
## Configuring NTP Server/Client Mode with Authentication

### 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 S4200G 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
```

# Set Device A as the NTP server.

```
     [DeviceB] ntp-service unicast-server 1.0.1.11
```

# 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 frequence: 60.0002 Hz
 Actual frequence: 60.0002 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

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

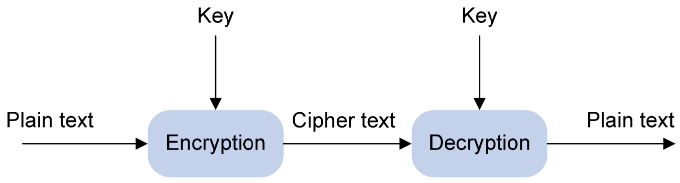
Secure Shell (SSH) is a protocol that provides secure remote login and other security services in insecure network environments, allowing for secure access to the Command Line Interface (CLI) of a switch for configuration and management. In an SSH connection, data are encrypted before being sent out 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.

### 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_SMSG_SUCCESS packet and goes on to the interactive session stage with the client. Otherwise, the server sends back to the client an SSH_SMSG_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

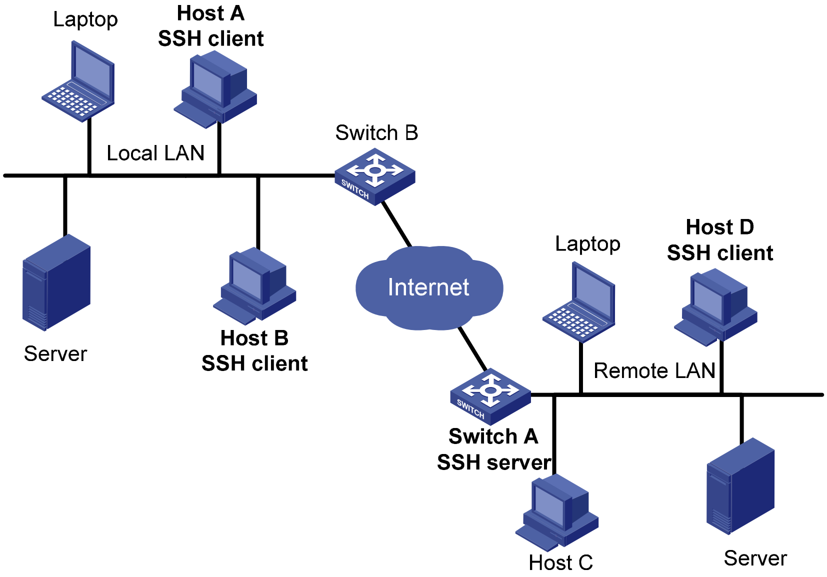
In this stage, the server and the client exchanges data in this way:

- 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 3Com switch acts as the SSH server to cooperate with software that supports the SSH client functions.
- The 3Com switch acts as the SSH server to cooperate with another 3Com 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 |
|---|---|---|---|
| An 3Com switch | Software that supports the SSH client functions | Configuring the SSH Server | Configuring an SSH Client that Runs SSH Client Software |
| An 3Com switch | Another 3Com 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 |
| | Configuring the SSH Management Functions | Optional |
| Version | Configuring the SSH Server to Be Compatible with SSH1 Clients | Optional<br>This task determines which SSH versions the server should support.<br>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<br>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**.<br>• Required when the authentication mode is **publickey**. |
| | Assigning a Public Key to an SSH User | • Not necessary when the authentication mode is **password**.<br>• Required when the authentication mode is **publickey**. |
| | Exporting the Host Public Key to a File | Optional<br>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** *first-number* [ *last-number* ] | — |

| To do... | Use the command... | Remarks |
|---|---|---|
| Configure the authentication mode as scheme | **authentication-mode scheme** [ **command-authorization** ] | Required<br>By default, the user interface authentication mode is password. |
| Specify the supported protocol(s) | **protocol inbound** { **all** \|**ssh** } | Optional<br>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** *seconds* | Optional<br>By default, the SSH authentication timeout time is 60 seconds. |
| Set the number of SSH authentication retry attempts | **ssh server authentication-retries** *times* | Optional<br>By default, the number of SSH authentication retry attempts is 3. |
| Set the RSA server key update interval | **ssh server rekey-interval** *hours* | Optional<br>By default, the system does not update the RSA server keys. |
| Configure a login header | **header shell** *text* | Optional<br>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** *ip-address* | Optional<br>By default, no source IP address is configured. |
| Specify a source interface for the SSH server | **ssh-server source-interface** *interface-type interface-number* | Optional<br>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<br>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<br>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.
- 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 looks 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.<br>By default, no SSH user is created and no authentication type is specified.<br>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. |
|  | **ssh user** *username* |  |
| Create an SSH user, and specify an authentication type for it | **ssh user** *username* **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** *username* **service-type** { **stelnet** \| **sftp** \| **all** } | Required<br>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** *keyname* | 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** *keyname* **import sshkey** *filename* | 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** *username* **assign publickey** *keyname* | Required<br>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** } [ *filename* ] | 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** } [ *filename* ] | 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**

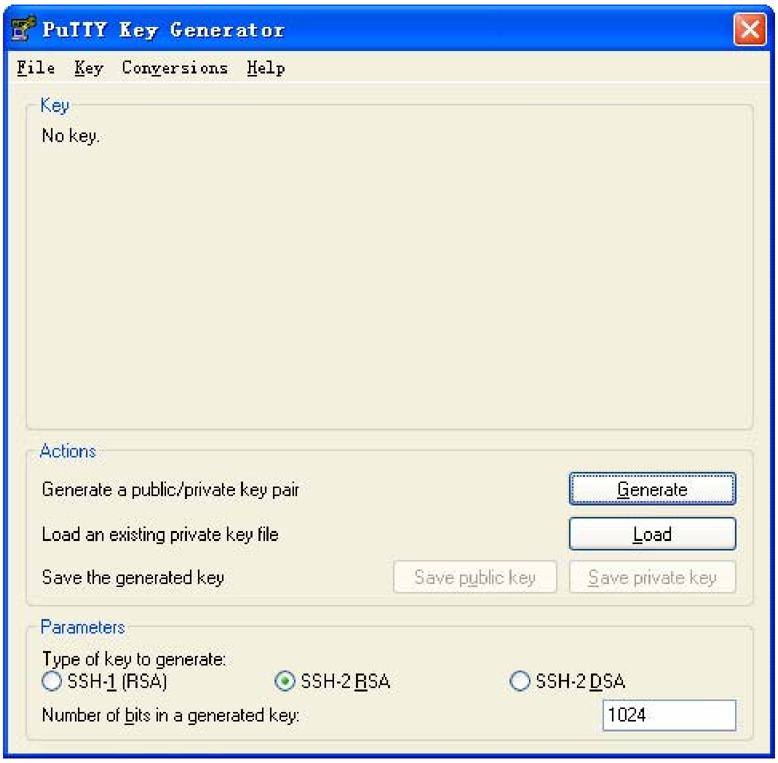
- For putty, it is recommended to use PuTTY release 0.53; PuTTY release 0.58 is also supported. For OpenSSH, it is recommended to use OpenSSH_3.1p1; OpenSSH_4.2p1 is also supported. Any other version or other client, please be careful to use.
- Selecting the protocol for remote connection as SSH. Usually, 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)



PuTTY Key Generator

File Key Conversions Help

Key

No key.

Actions

Generate a public/private key pair [Generate]

Load an existing private key file [Load]

Save the generated key [Save public key] [Save private key]

Parameters

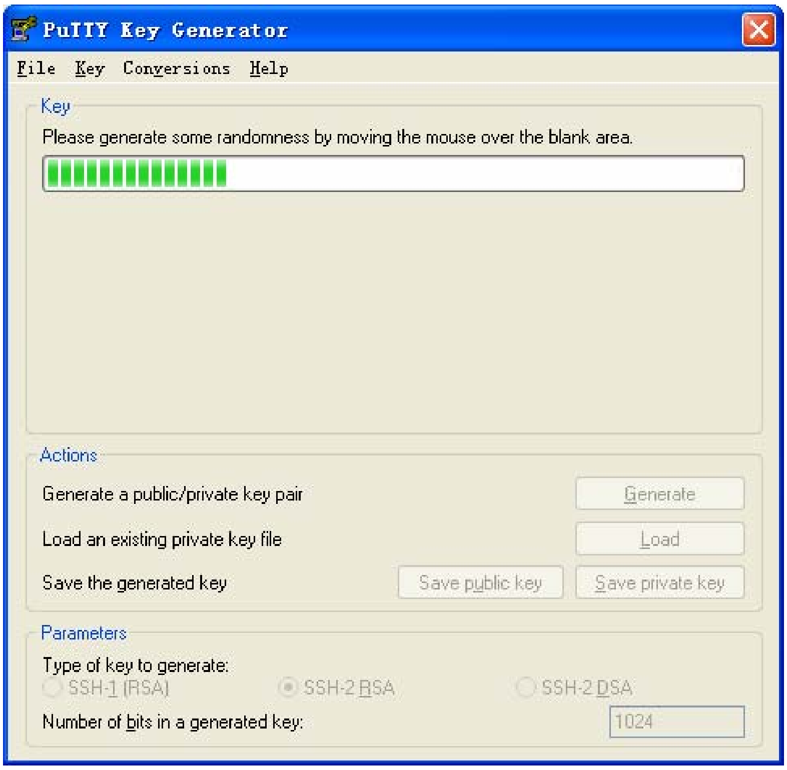
Type of key to generate:

○ SSH-1 (RSA) ● SSH-2 RSA ○ SSH-2 DSA

Number of bits in a generated key: 1024

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)



PuTTY Key Generator

File Key Conversions Help

Key

Please generate some randomness by moving the mouse over the blank area.

Actions

Generate a public/private key pair [Generate]

Load an existing private key file [Load]

Save the generated key [Save public key] [Save private key]

Parameters

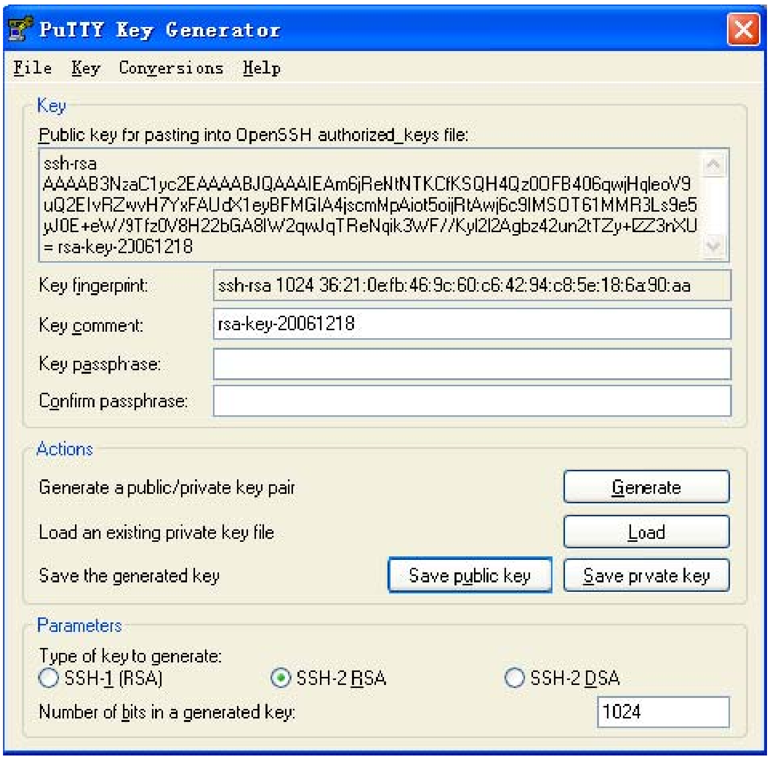
Type of key to generate:

○ SSH-1 (RSA) ● SSH-2 RSA ○ SSH-2 DSA

Number of bits in a generated key: 1024

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)



Public key for pasting into OpenSSH authorized_keys file:

```
ssh-rsa
AAAAB3NzaC1yc2EAAAABJQAAAIEAm6jReNtNTKCfKSQH4Qz0OFB406qwjHqleoV9
uQ2EIvRZwvH7YxFAUdX1eyBFMGIA4jscmMpAiot5oijRtAwj6c9IMSOT61MMR3Ls9e5
yJ0E+eW/9Tfz0V8H22bGA8IW2qwJqTReNqik3WF//Kyl2I2Agbz42un2tTZy+ZZ3nXU
= rsa-key-20061218
```

Key fingerprint: ssh-rsa 1024 36:21:0e:fb:46:9c:60:c6:42:94:c8:5e:18:6a:90:aa

Key comment: rsa-key-20061218

Key passphrase:

Confirm passphrase:

Generate a public/private key pair

Load an existing private key file

Save the generated key

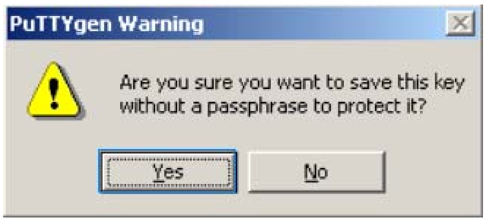
Type of key to generate:

○ SSH-1 (RSA) ● SSH-2 RSA ○ SSH-2 DSA

Number of bits in a generated key: 1024

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.

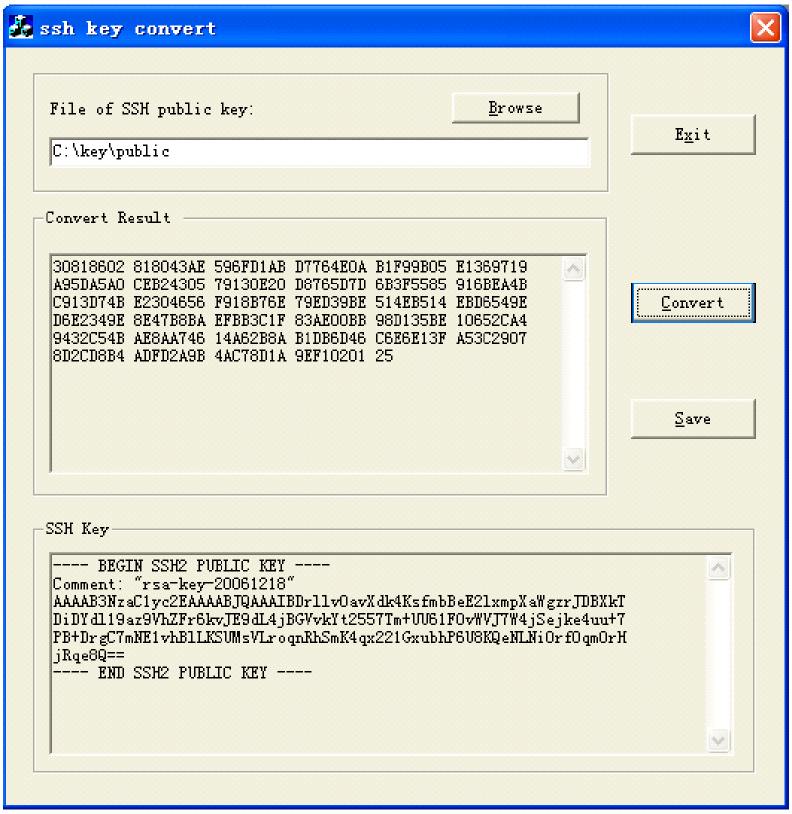
**Figure 1-6** Generate the client keys (4)



Are you sure you want to save this key without a passphrase to protect it?

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)



File of SSH public key: C:\key\public

Convert Result

```
30818602 818043AE 596FD1AB D7764E0A B1F99B05 E1369719
A95DA5A0 CEB24305 79130E20 D8765D7D 6B3F5585 916BEA4B
C913D74B E2304656 F918B76E 79ED39BE 514EB514 EBD6549E
D6E2349E 8E47B8BA EFBB3C1F 83AE00BB 98D135BE 10652CA4
9432C54B AE8AA746 14A62B8A B1DB6D46 C6E6E13F A53C2907
8D2CD8B4 ADFD2A9B 4AC78D1A 9EF10201 25
```

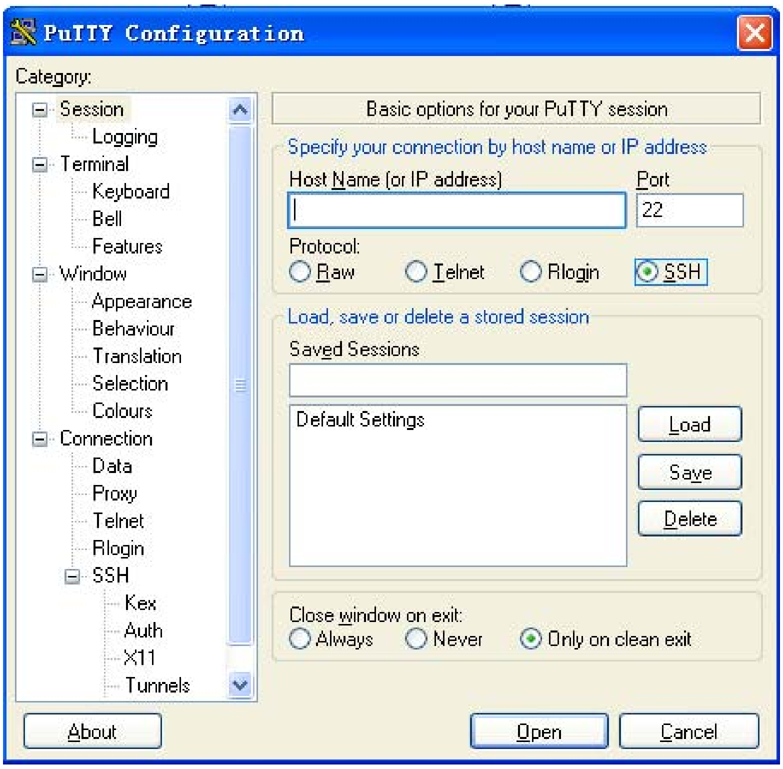
SSH Key

```
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "rsa-key-20061218"
AAAAB3NzaC1yc2EAAAABJQAAAIBDrllvOavXdk4KsfmbBeE2lxmpXaWgzrJDBXkT
DiDYdl19ar9VhZFr6kvJE9dL4jBGVvkYt2557Tm+UU61FOvWVJ7W4jSejke4uu+7
PB+DrgC7mNE1vhBlLKSUMsVLroqnRhSmK4qx221GxubhP6U8KQeNLNiOrfOqmOrH
jRqe8Q==
---- END SSH2 PUBLIC KEY ----
```

## Specifying the IP address of the Server

Launch PuTTY.exe. The following window appears.

**Figure 1-8** SSH client configuration interface 1



Host Name (or IP address):

Port: 22

Protocol: ○ Raw ○ Telnet ○ Rlogin ● SSH

Saved Sessions: Default Settings

Close window on exit: ○ Always ○ Never ● Only on clean exit

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.

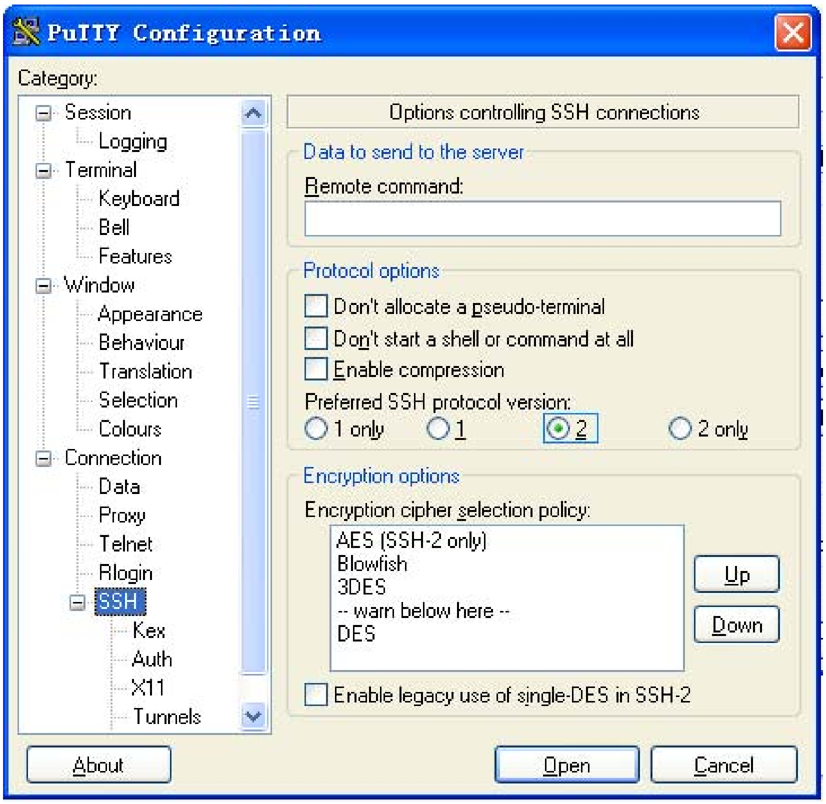
### Selecting a protocol for remote connection

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



Options controlling SSH connections

Data to send to the server

Remote command:

Protocol options

□ Don't allocate a pseudo-terminal

□ Don't start a shell or command at all

□ Enable compression

Preferred SSH protocol version:

○ 1 only ○ 1 ● 2 ○ 2 only

Encryption options

Encryption cipher selection policy:

AES (SSH-2 only)
Blowfish
3DES
-- warn below here --
DES

□ Enable legacy use of single-DES in SSH-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.

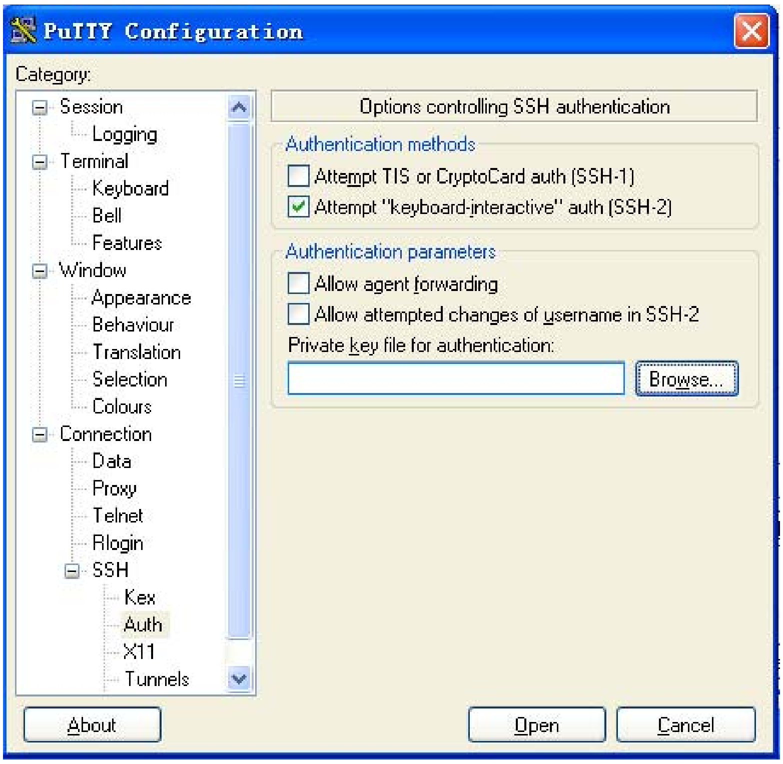
To log out, enter the **quit** command.

### 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



Options controlling SSH authentication

Authentication methods

□ Attempt TIS or CryptoCard auth (SSH-1)

☑ Attempt "keyboard-interactive" auth (SSH-2)

Authentication parameters

□ Allow agent forwarding

□ Allow attempted changes of username in SSH-2

Private key file for authentication:

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 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<br>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<br>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<br>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 souce IP address or the souce 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** *ip-address* | Optional<br>By default, no source IP address is configured. |
| Specify a source interface for the SSH client | **ssh2 source-interface** *interface-type interface-number* | Optional<br>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** | — |

| To do... | Use the command... | Remarks |
|---|---|---|
| Start the client to establish a connection with an SSH server | **ssh2** { *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<br>In this command, you can also specify the preferred key exchange algorithm, encryption algorithms and HMAC algorithms between the server and client.<br>HMAC: Hash-based message authentication code<br>Note that:<br>• The **identity-key** keyword is unnecessary in password authentication and optional in public key authentication.<br>• Support for the 3des keyword depends on the number of encryption bits of the software version. The 168-bit version supports this keyword, while the 56-bit version does not. |

**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** | |

| To do... | Use the command... | Remarks |
|---|---|---|
| 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** |
| Specify on the client the host public key of the server to be connected | **ssh client** { *server-ip* \| *server-name* } **assign rsa-key** *keyname* | **ssh client** { *server-ip* \| *server-name* } **assign publickey** *keyname* |
| Assign a public key to an SSH user | **ssh user** *username* **assign rsa-key** *keyname* | **ssh user** *username* **assign publickey** *keyname* |
| Create an SSH user and specify publickey authentication as its authentication type | **ssh user** *username* **authentication-type rsa** | **ssh user** *username* **authentication-type publickey** |

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

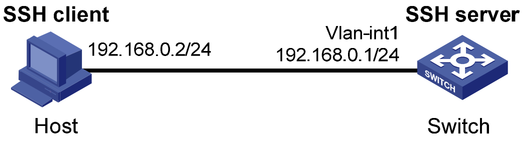
## When Switch Acts as Server for Local Password Authentication

### 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

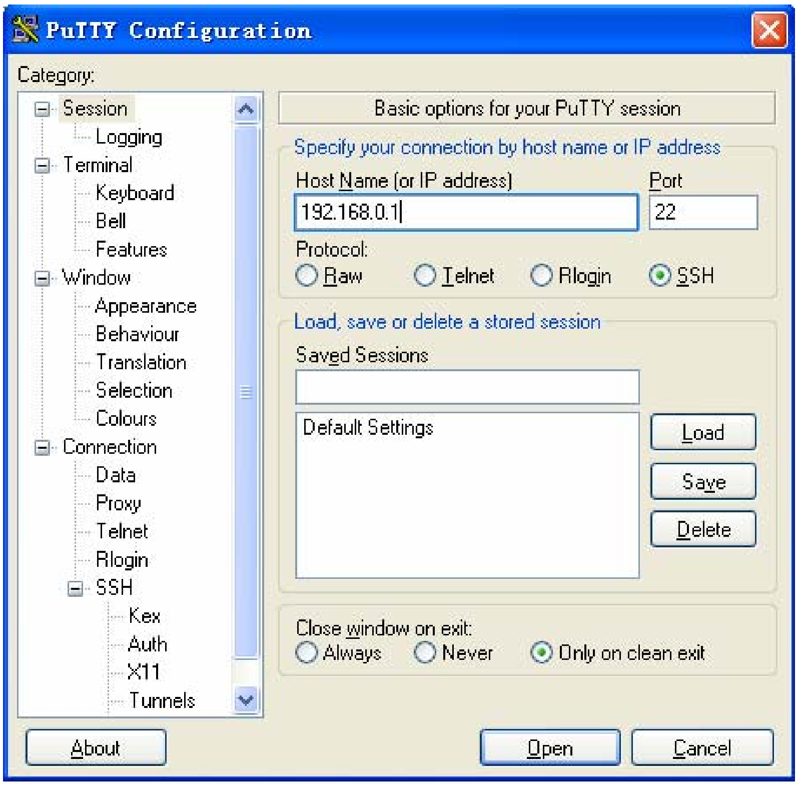
# Configure an IP address (192.168.0.2 in this case) for the SSH client. This IP address and that of the VLAN interface on the switch must be in the same network segment.

# 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)



Basic options for your PuTTY session

Specify your connection by host name or IP address

Host Name (or IP address): 192.168.0.1

Port: 22

Protocol: ○ Raw ○ Telnet ○ Rlogin ● SSH

Load, save or delete a stored session

Saved Sessions

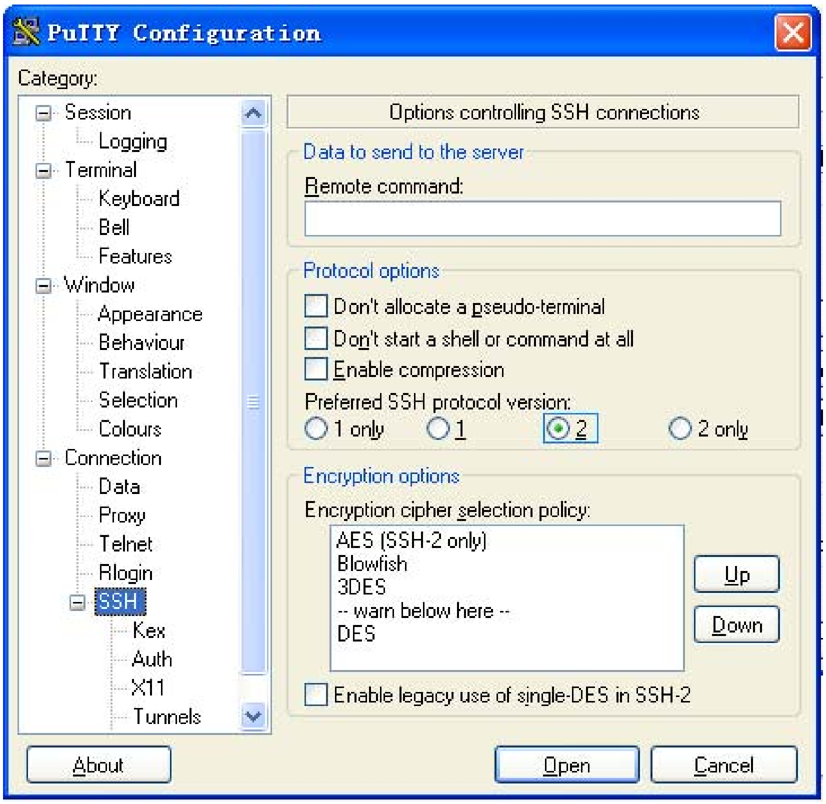
Default Settings

Close window on exit: ○ Always ○ Never ● Only on clean exit

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)



Options controlling SSH connections

Data to send to the server

Remote command:

Protocol options

□ Don't allocate a pseudo-terminal

□ Don't start a shell or command at all

□ Enable compression

Preferred SSH protocol version:

○ 1 only ○ 1 ● 2 ○ 2 only

Encryption options

Encryption cipher selection policy:

AES (SSH-2 only)
Blowfish
3DES
-- warn below here --
DES

□ Enable legacy use of single-DES in SSH-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

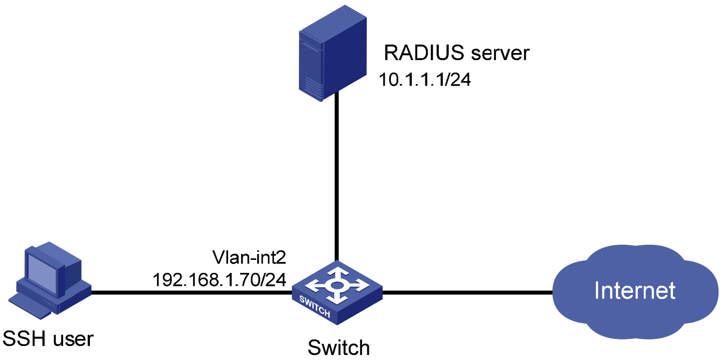
### Network requirements

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

4) Configure the RADIUS server

---

**Note**

This document takes CAMS Version 2.10 as an example to show the basic RADIUS server configurations required.

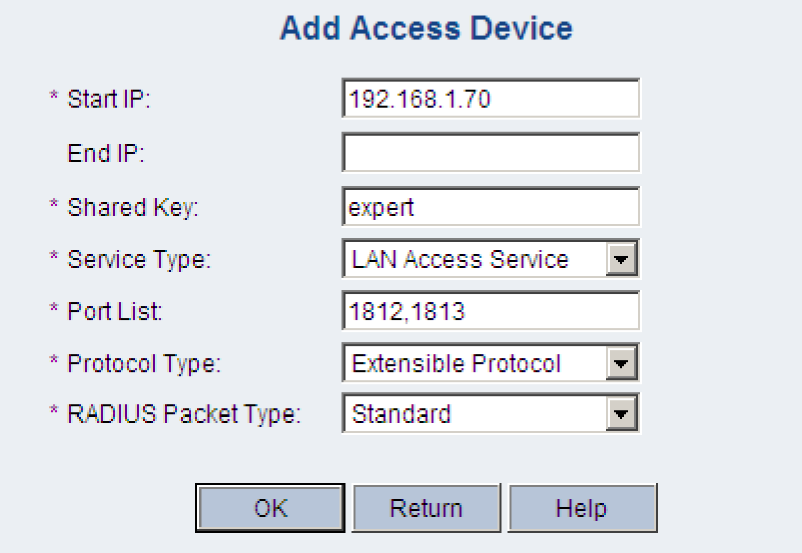
---

# 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 Access Device

* Start IP: 192.168.1.70

End IP:

* Shared Key: expert

* Service Type: LAN Access Service

* Port List: 1812,1813

* Protocol Type: Extensible Protocol

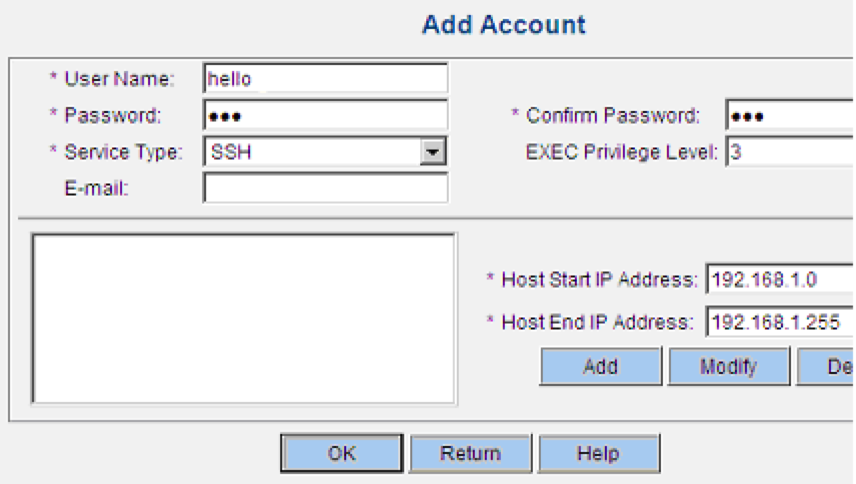
* RADIUS Packet Type: Standard

# 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


Add Account

* User Name: hello

* Password: ●●●

* Confirm Password: ●●●

* Service Type: SSH

EXEC Privilege Level: 3

E-mail:

* Host Start IP Address: 192.168.1.0

* Host End IP Address: 192.168.1.255

5) 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
```

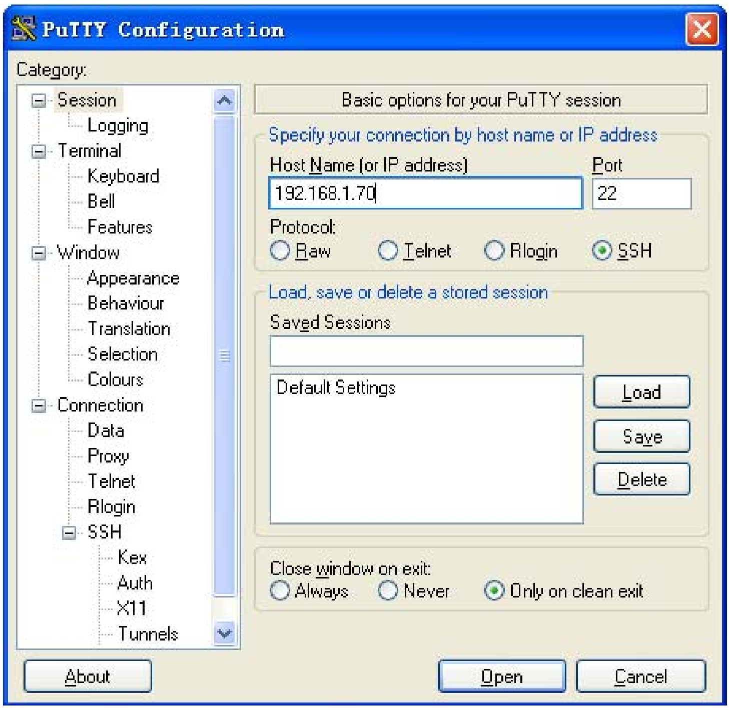
6) Configure the SSH client

# 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)



Host Name (or IP address): 192.168.1.70

Port: 22

Protocol: ○ Raw ○ Telnet ○ Rlogin ● SSH

Saved Sessions:

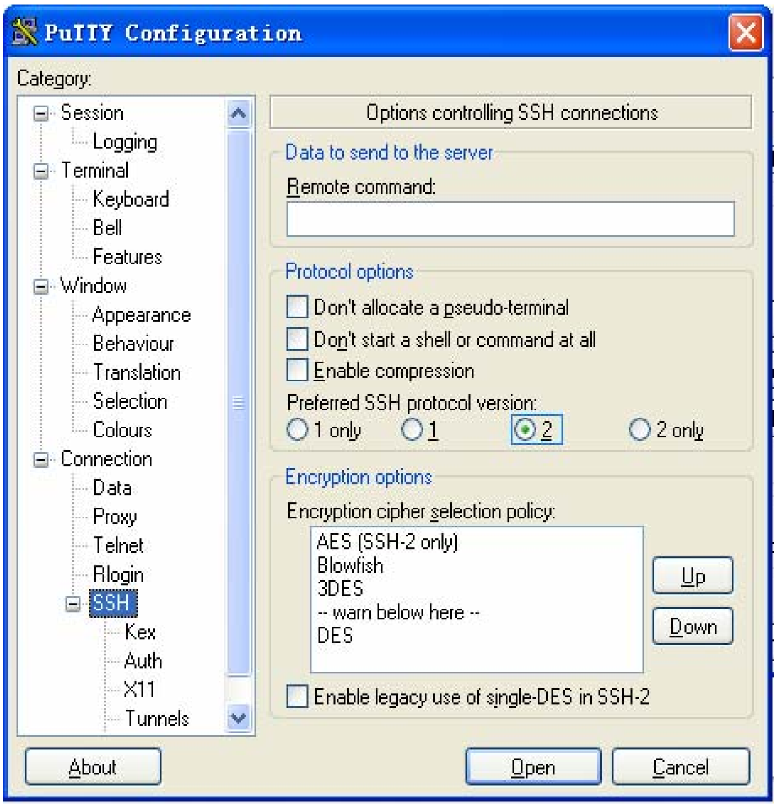
Default Settings

Close window on exit: ○ Always ○ Never ● Only on clean exit

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)



Remote command:

□ Don't allocate a pseudo-terminal

□ Don't start a shell or command at all

□ Enable compression

Preferred SSH protocol version: ○ 1 only ○ 1 ● 2 ○ 2 only

Encryption cipher selection policy:

AES (SSH-2 only)
Blowfish
3DES
-- warn below here --
DES

□ Enable legacy use of single-DES in SSH-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

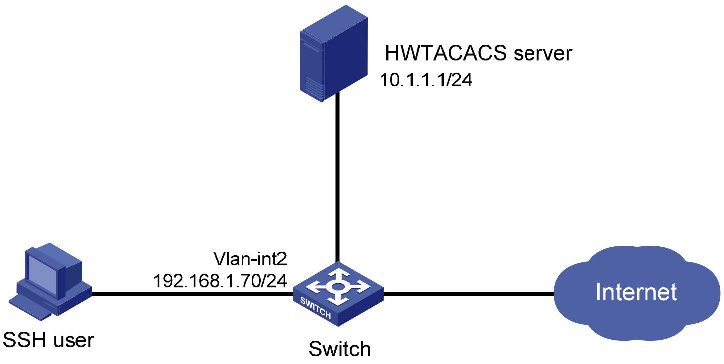
### Network requirements

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
```

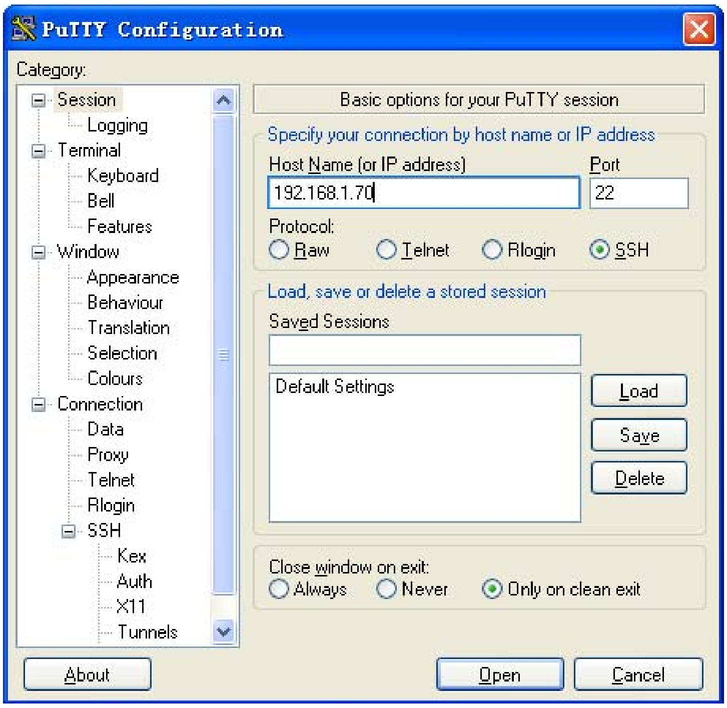
- Configure the SSH client

# 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)



Host Name (or IP address): 192.168.1.70

Port: 22

Protocol: ○ Raw ○ Telnet ○ Rlogin ● SSH

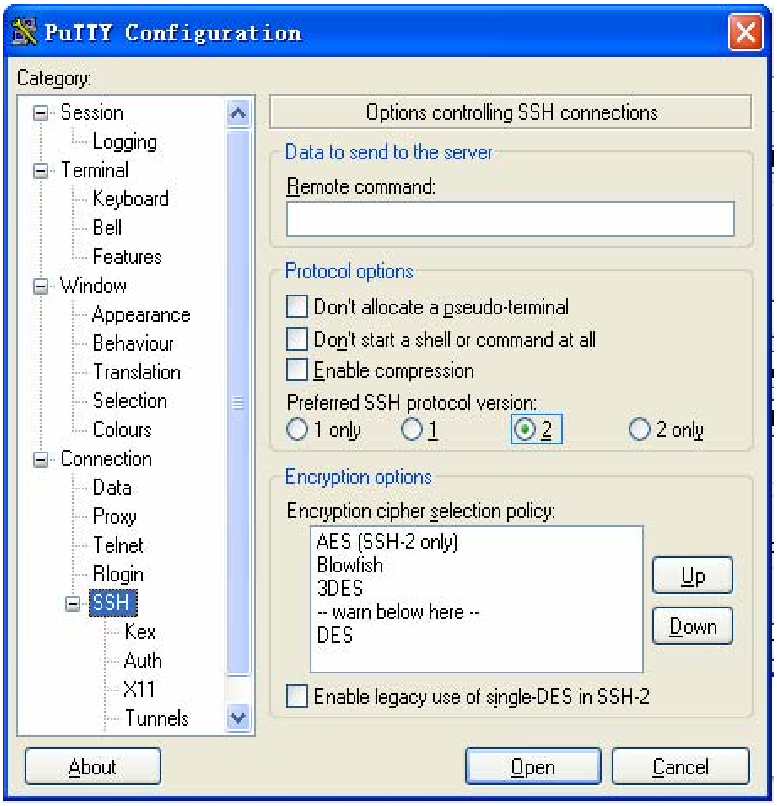
Saved Sessions: Default Settings

Close window on exit: ○ Always ○ Never ● Only on clean exit

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)



Options controlling SSH connections

Data to send to the server

Remote command:

Protocol options

□ Don't allocate a pseudo-terminal

□ Don't start a shell or command at all

□ Enable compression

Preferred SSH protocol version:

○ 1 only ○ 1 ● 2 ○ 2 only

Encryption options

Encryption cipher selection policy:

AES (SSH-2 only)
Blowfish
3DES
-- warn below here --
DES

□ Enable legacy use of single-DES in SSH-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.

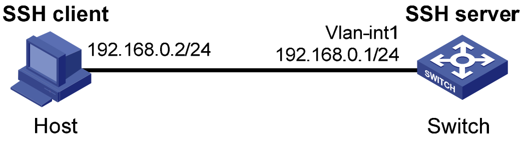
## When Switch Acts as Server for Publickey Authentication

### 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**.

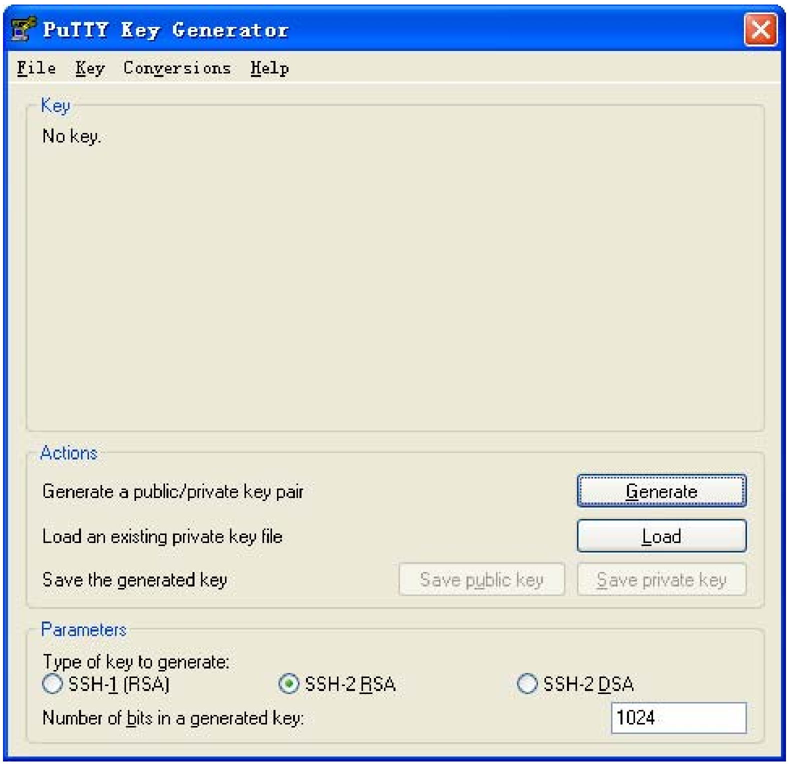
```
[Switch] ssh user client001 assign publickey Switch001
```

- 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)



No key.

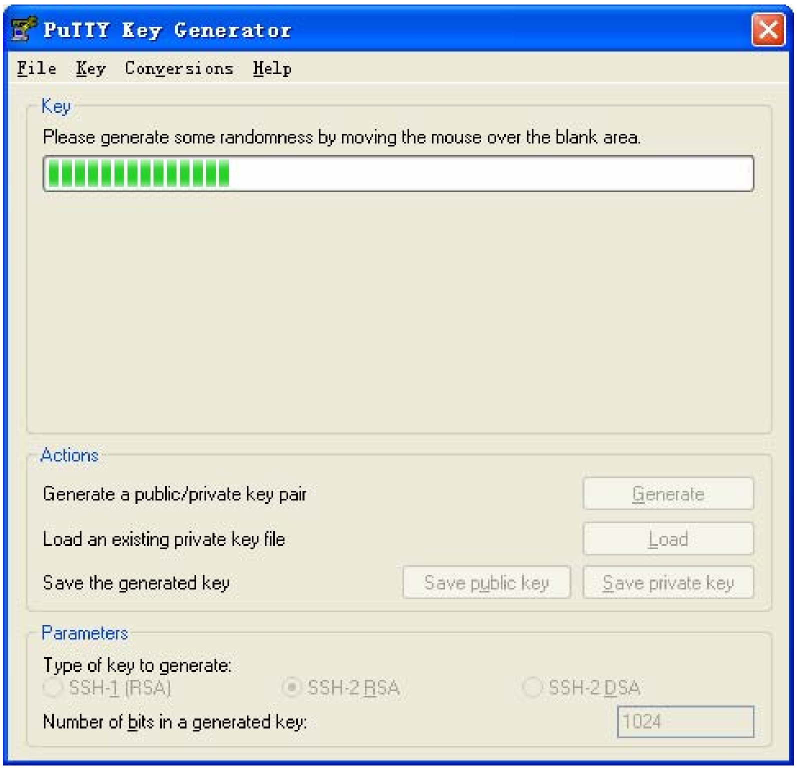
Type of key to generate:
○ SSH-1 (RSA) ● SSH-2 RSA ○ SSH-2 DSA

Number of bits in a generated key: 1024

**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)



Please generate some randomness by moving the mouse over the blank area.

Generate a public/private key pair

Load an existing private key file

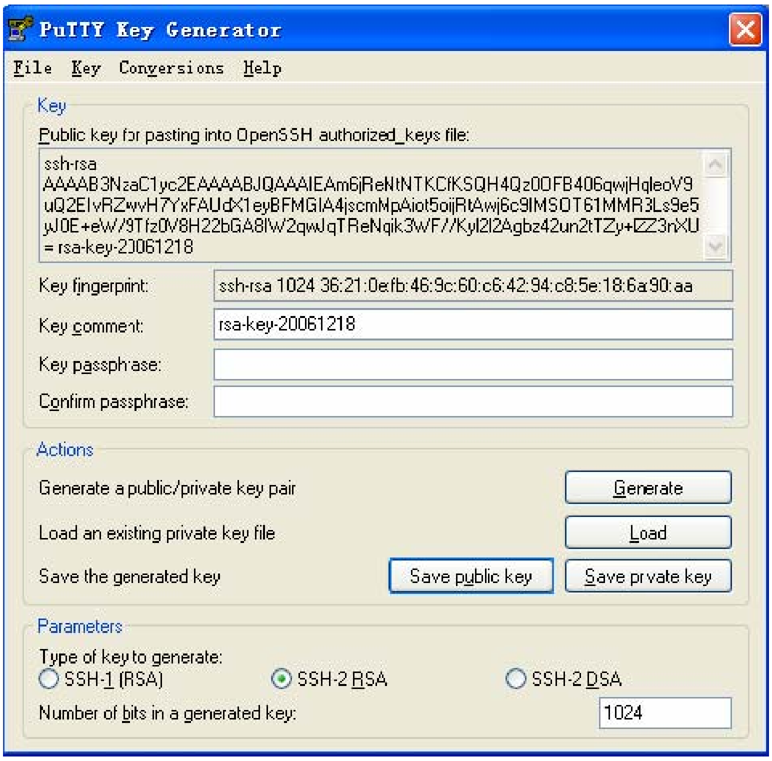
Save the generated key

Type of key to generate:
○ SSH-1 (RSA) ● SSH-2 RSA ○ SSH-2 DSA

Number of bits in a generated key: 1024

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)



Public key fbr pasting into OpenSSH authorized_keys file:

```
ssh-rsa
AAAAB3NzaC1yc2EAAAABJQAAAIEAm6jReNtNTKCfKSQH4Qz0OFB406qwjHqleoV9
uQ2EIvRZwvH7YxFAUdX1eyBFMGIA4jscmMpAiot5oijRtAwj6c9IMSOT61MMR3Ls9e5
yJ0E+eW/9Tfz0V8H22bGA8lW2qwJqTReNqik3WF//KyI2I2Agbz42un2tTZy+lZZ3nXU
= rsa-key-2J061218
```

Key fingerprint: ssh-rsa 1024 36:21:0e:fb:46:9c:60:c6:42:94:c8:5e:18:6a:90:aa

Key comment: rsa-key-20061218

Key passphrase:

Confirm passphrase:

Generate a public/private key pair

Load an existing private key file

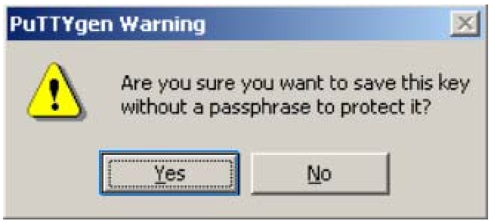
Save the generated key

Type of key to generate:
○ SSH-1 (RSA) ● SSH-2 RSA ○ SSH-2 DSA

Number of bits in a generated key: 1024

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)



PuTTYgen Warning

Are you sure you want to save this key without a passphrase to protect it?

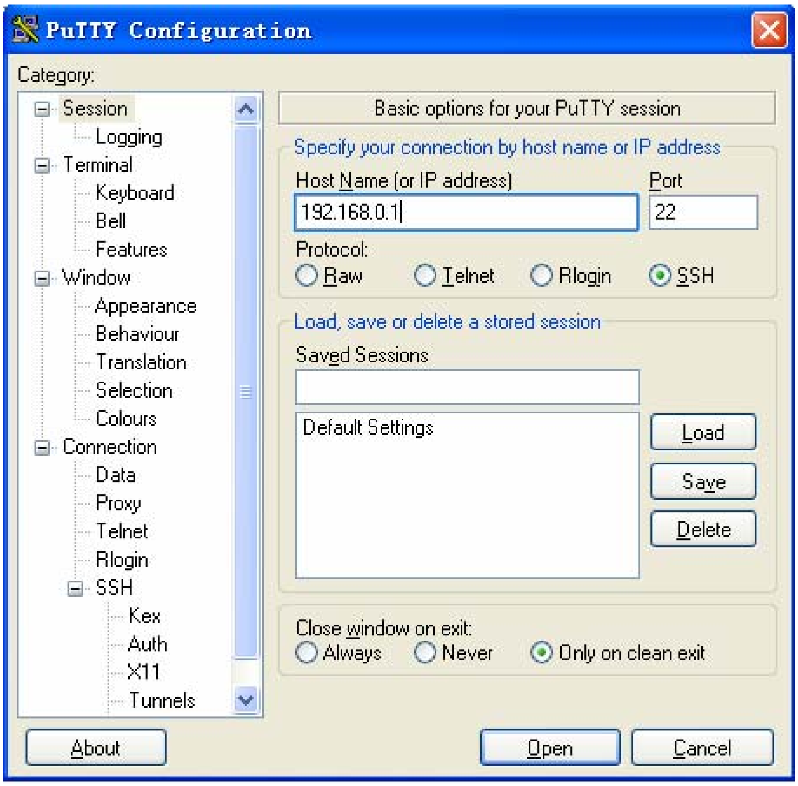
**Note**

After a public key pair is generated, you need to upload the pubic 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)



PuTTY Configuration

Basic options for your PuTTY session

Specify your connection by host name or IP address

Host Name (or IP address): 192.168.0.1

Port: 22

Protocol: ○ Raw ○ Telnet ○ Rlogin ● SSH

Load, save or delete a stored session

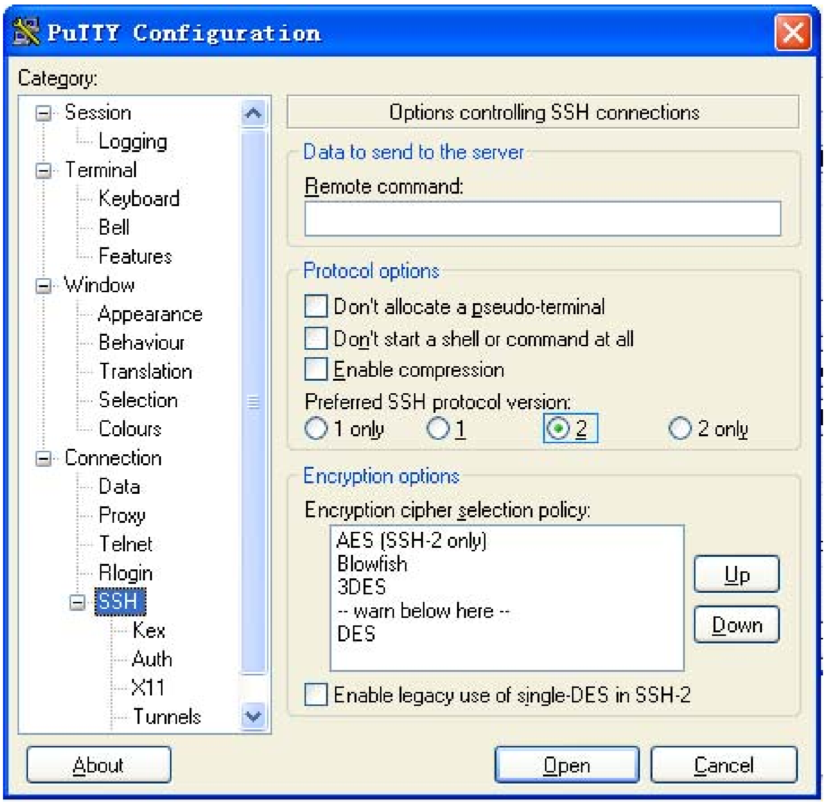
Saved Sessions: Default Settings

Close window on exit: ○ Always ○ Never ● Only on clean exit

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)



Options controlling SSH connections

Data to send to the server

Remote command:

Protocol options

□ Don't allocate a pseudo-terminal

□ Don't start a shell or command at all

□ Enable compression

Preferred SSH protocol version:

○ 1 only ○ 1 ● 2 ○ 2 only

Encryption options

Encryption cipher selection policy:

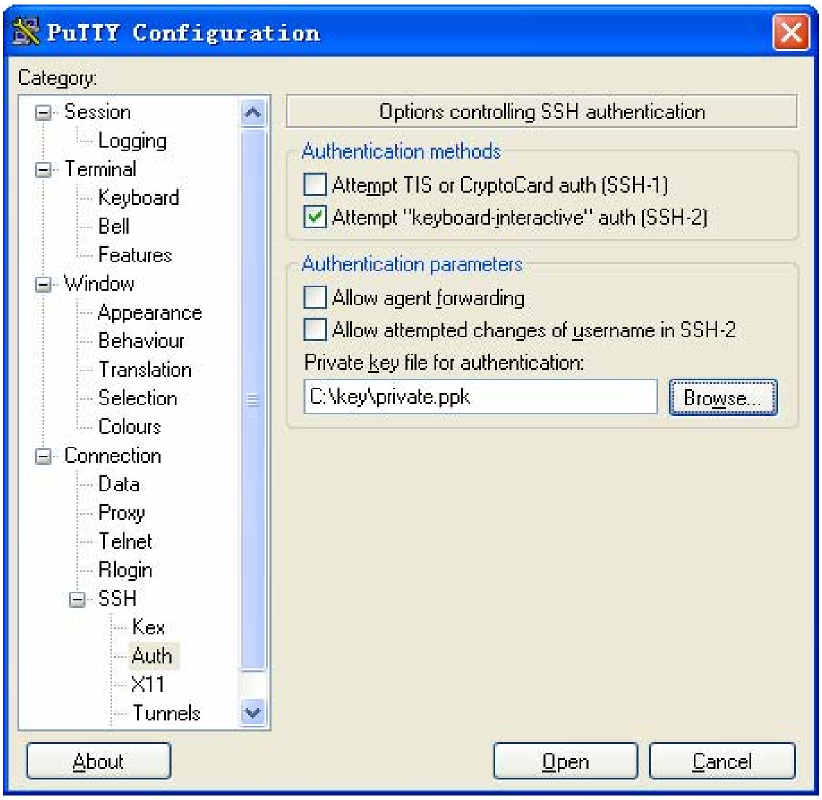
```
AES (SSH-2 only)
Blowfish
3DES
-- warn below here --
DES
```

□ Enable legacy use of single-DES in SSH-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)



Options controlling SSH authentication

Authentication methods

□ Attempt TIS or CryptoCard auth (SSH-1)

☑ Attempt "keyboard-interactive" auth (SSH-2)

Authentication parameters

□ Allow agent forwarding

□ Allow attempted changes of username in SSH-2

Private key file for authentication:

C:\key\private.ppk

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.

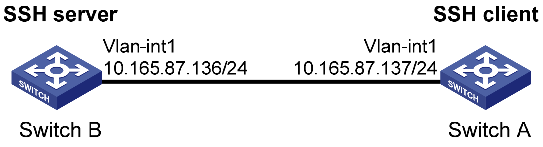
## When Switch Acts as Client for Password Authentication

### 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:

**************************************************************************
*  Copyright(c) 2004-2008 3Com Corp. and its licensors. All rights reserved.
*  Without the owner's prior written consent,                            *
*  no decompiling or reverse-engineering shall be allowed.               *
**************************************************************************

<SwitchB>
```

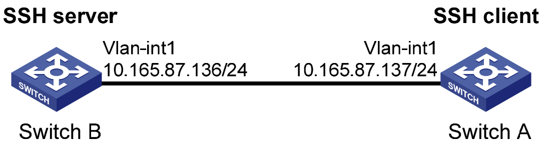
## When Switch Acts as Client for Publickey Authentication

### 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 pubic 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

**************************************************************************
*  Copyright(c) 2004-2008 3Com Corp. and its licensors. All rights reserved.
*  Without the owner's prior written consent,                            *
*  no decompiling or reverse-engineering shall be allowed.               *
**************************************************************************

<SwitchB>
```

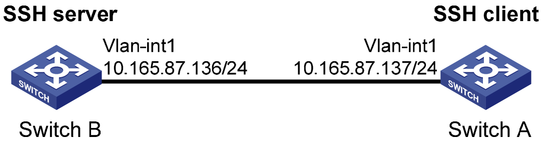
## When Switch Acts as Client and First-Time Authentication is not Supported

### 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
```

**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.

- 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 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 ...

**************************************************************************
*  Copyright(c) 2004-2008 3Com Corp. and its licensors. All rights reserved.
*  Without the owner's prior written consent,                             *
*  no decompiling or reverse-engineering shall be allowed.               *
**************************************************************************

<SwitchB>
```

# Table of Contents

# 1 File System Management Configuration

## File System Configuration

### Introduction to File System

To facilitate management on the switch memory, 3com switches 4200G 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 Tasks

**Table 1-1** Configuration tasks on the file system

| Operation | Remarks |
|---|---|
| Directory Operations | Optional |
| File Operations | Optional |
| Flash Memory Operations | Optional |
| Prompt Mode Configuration | Optional |

**Note**

3com switches 4200G allow you to input a file path and file name in one of the following ways:

- In universal resource locator (URL) format and starting with “unit1>flash:/”. or “flash:/” This method is used to specify a file in the current Flash memory. For example, the URL of a file named **text.txt** in the root directory of the switch is **unit1>flash:/text.txt** or **flash:/text.txt**.
- Entering the path name or file name directly. This method can be used to specify a path or a file in the current work directory. 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

Table 1-2 describes the directory-related operations.

Perform the following configuration in user view.

**Table 1-2** Directory operations

| To do… | Use the command… | Remarks |
|---|---|---|
| Create a directory | **mkdir** *directory* | Optional |
| Delete a directory | **rmdir** *directory* | Optional |
| Display the current work directory | **pwd** | Optional |
| Display the information about specific directories and files | **dir** [ **/all** ] [ *file-url* ] | Optional |
| Enter a specified directory | **cd** *directory* | Optional |

**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

The file system also provides file-related functions listed in Table 1-3.

Perform the following configuration in user view. Note that the **execute** command should be executed in system view.

**Table 1-3** File operations

| To do… | Use the command… | Remarks |
|---|---|---|
| Delete a file | **delete** [ **/unreserved** ] *file-url*<br>**delete** { **running-files** \| **standby-files** } [ **/unreserved** ] | Optional<br>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. |
| Restore a file in the recycle bin | **undelete** *file-url* | Optional |
| Delete a file from the recycle bin | **reset recycle-bin** [ *file-url* ] [ **/force** ] | Optional |
| Rename a file | **rename** *fileurl-source fileurl-dest* | Optional |
| Copy a file | **copy** *fileurl-source fileurl-dest* | Optional |
| Move a file | **move** *fileurl-source fileurl-dest* | Optional |
| Display the content of a file | **more** *file-url* | Optional<br>Currently, the file system only supports displaying the contents of text files. |
| Display the information about a directory or a file | **dir** [ **/all** ] [ *file-url* ] | Optional |

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Execute the specified batch file | **execute** *filename* | Optional<br>This command should be executed in system view. |

**Caution**

- For deleted files whose names are the same, only the latest deleted file is kept in the recycle bin and can be restored.
- The files which are deleted by the **delete** command without the **/unreserved** keyword are actually moved to the recycle bin and thus still take storage space. You can clear the recycle bin by using the **reset recycle-bin** command.
- 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

Perform the following Flash memory operations using commands listed in Table 1-4.

Perform the following configuration in user view.

**Table 1-4** Operations on the Flash memory

| To do… | Use the command… | Remarks |
|---|---|---|
| Format the Flash memory | **format** *device* | Required |
| Restore space on the Flash memory | **fixdisk** *device* | Required |

**Caution**

The format operation leads to the loss of all files, including the configuration files, on the Flash memory and is irretrievable.

## Prompt Mode Configuration

You can set the prompt mode of the current file system to **alert** or **quiet**. In alert mode, the file system will give a prompt for confirmation if you execute a command which may cause data loss, for example, deleting or overwriting a file. In quiet mode, such prompt will not be displayed.

**Table 1-5** Configuration on prompt mode of file system

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |

| To do… | Use the command… | Remarks |
|---|---|---|
| Configure the prompt mode of the file system | **file prompt** { **alert** \| **quiet** } | Required<br>By default, the prompt mode of the file system is **alert**. |

## File System Configuration Example

# Display all the files in the root directory of the file system.

```
<Sysname> dir /all
Directory of unit1>flash:/

   1 (*)   -rw-   3579326  Mar 28 2007 10:51:22   switch.bin
   2 (*)   -rw-      1235  Apr 03 2000 16:04:52   config.cfg
   3       -rwh       151  Apr 03 2000 16:04:55   private-data.txt
   4       -rwh       716  Apr 04 2000 17:27:35   hostkey
   5       -rwh       572  Apr 04 2000 17:27:41   serverkey
   6       -rwh       548  Apr 04 2000 17:30:06   dsakey
   7       drw-         -  Apr 04 2000 23:04:21   test

15367 KB total (3585 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-   3579326  Mar 28 2007 10:51:22   switch.bin
   2 (*)   -rw-      1235  Apr 03 2000 16:04:52   config.cfg
   3       -rwh       151  Apr 03 2000 16:04:55   private-data.txt
   4       -rwh       716  Apr 04 2000 17:27:35   hostkey
   5       -rwh       572  Apr 04 2000 17:27:41   serverkey
   6       -rwh       548  Apr 04 2000 17:30:06   dsakey
   7       drw-         -  Apr 04 2000 23:04:21   test

15367 KB total (3585 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-      1235  Apr 05 2000 01:51:34   test.cfg
   2       -rw-      1235  Apr 05 2000 01:56:44   1.cfg

15367 KB total (3585 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 1-6.

**Table 1-6** 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, 3com 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 startup file used for the next startup of a switch, and change the main or backup attribute of the file.

Perform the configuration listed in Table 1-7 in user view. The **display** commands can be executed in any view.

**Table 1-7** Configure file attributes

| To do… | Use the command… | Remarks |
|---|---|---|
| Configure the app file with the main attribute for the next startup | **boot boot-loader** *file-url* | Optional |
| Configure the app file with the backup attribute for the next startup | **boot boot-loader backup-attribute** *file-url* | Optional |
| Configure the Web file and its attribute | **boot web-package** *webfile* { **backup** \| **main** } | Optional |
| Switch the file attributes between main and backup | **boot attribute-switch** { **all** \| **app** \| **configuration** \| **web** } | Optional |
| Specify to enable user to use the customized password to enter the BOOT menu | **startup bootrom-access enable** | Optional<br>By default, the user is enabled to use the customized password to enter the BOOT menu. |

| To do… | Use the command… | Remarks |
|---|---|---|
| Display the information about the app file used as the startup file | **display boot-loader** [ **unit** *unit-id* ] | Optional<br>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, make sure the file already exists on the device.
- 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.

# Table of Contents

# 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

## 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

A 3com switch 4200G can act as an FTP client or the FTP server in FTP-employed data transmission:

**Table 1-1** Roles that a 3com switch 4200G 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. | |

### 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** *user-name* | Required<br>By default, no local user is configured. |
| Configure a password for the specified user | **password** { **simple** \| **cipher** } *password* | Optional<br>By default, no password is configured. |
| Configure the service type as FTP | **service-type ftp** | Required<br>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<br>Disabled by default. |

**Note**

- Only one user can access a 3com switch 4200G at a given time when the latter operates as an FTP server.
- Operating as an FTP server, a 3com switch 4200G 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.

**Note**

To protect unused sockets against attacks, the 3com switch 4200G 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** *minutes* | Optional<br>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** *interface-type interface-number* | Use either command<br>Not specified by default. |
| Specifying the source IP address for an FTP server | **ftp-server source-ip** *ip-address* | |

**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** *user-name* | Required |

**Note**

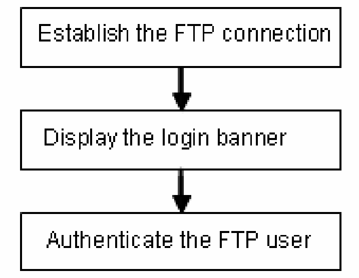
With a 3com switch 4200G acting as the FTP server, if a network administrator attempts to disconnect a user that is uploading/downloading data to/from the FTP server the 3com switch 4200G will disconnect the user after the data transmission is completed.

### 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:

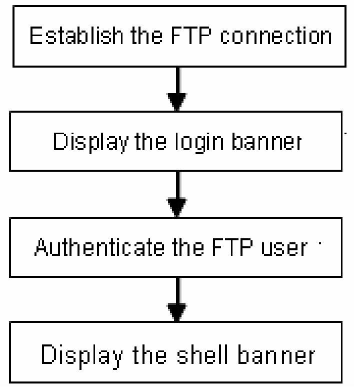
- Login banner: After the connection between an FTP client and an FTP server is established, the FTP server outputs the configured login banner to the FTP client terminal.

**Figure 1-1** 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 1-2** 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<br>Use either command or both.<br>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.<br>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<br>**passive** by default. |
| Change the working directory on the remote FTP server | **cd** *pathname* | 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** *pathname* | |
| Remove a directory on the remote FTP server | **rmdir** *pathname* | |
| Delete a specified file | **delete** *remotefile* | |

| To do… | Use the command… | Remarks |
|---|---|---|
| Query a specified file on the FTP server | **dir** [ *remotefile* ] [ *localfile* ] | Optional<br>If no file name is specified, all the files in the current directory are displayed.<br>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. |
| | **ls** [ *remotefile* ] [ *localfile* ] | |
| Download a remote file from the FTP server | **get** *remotefile* [ *localfile* ] | Optional |
| Upload a local file to the remote FTP server | **put** *localfile* [ *remotefile* ] | |
| Rename a file on the remote server | **rename** *remote-source remote-dest* | |
| Log in with the specified user name and password | **user** *username* [ *password* ] | |
| Connect to a remote FTP server | **open** { *ip-address* \| *server-name* } [ *port* ] | |
| 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** [ *protocol-command* ] | |
| Enable the verbose function | **verbose** | Optional<br>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** *interface-type interface-number* | 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** | — |

| To do… | Use the command… | Remarks |
|---|---|---|
| Specify an interface as the source interface the FTP client uses every time it connects to an FTP server | **ftp source-interface** *interface-type interface-number* | Use either command<br>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

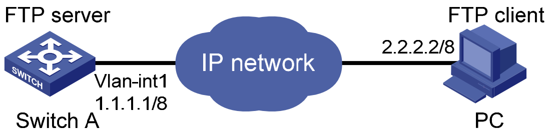
### Network requirements

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 1-3** 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.
- 3com switch 4200G 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

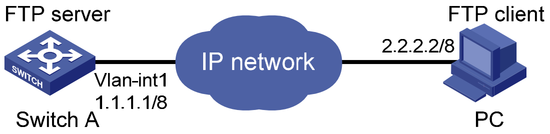
Configure the Ethernet switch as an FTP server and the remote PC as an FTP client. After a connection between the FTP client and the FTP server is established and login succeeds, the banner is displayed on the FTP client.

- 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 1-4** 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

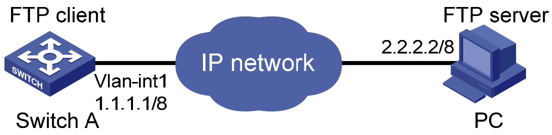
### Network requirements

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 1-5** 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** | — |

| To do… | Use the command… | Remarks |
|---|---|---|
| Enable an SFTP server | **sftp server enable** | Required<br>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** *time-out-value* | Optional<br>10 minutes by default. |

### Supported SFTP client software

A 3com switch 4200G 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 a 3com switch 4200G 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<br>Support for the 3des keyword depends on the number of encryption bits of the software version. The 168-bit version supports this keyword, while the 56-bit version does not. |
| 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<br>Both commands have the same effect. |
| | **remove** *remote-file* | |
| Query a specified file on the SFTP server | **dir** [ **-a** \| **-l** ] [ *remote-path* ] | Optional<br>If no file name is provided, all the files in the current directory are displayed.<br>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. |
| | **ls** [ **-a** \| **-l** ] [ *remote-path* ] | |
| Download a remote file from the SFTP server | **get** *remotefile* [ *localfile* ] | Optional |
| Upload a local file to the remote SFTP server | **put** *localfile* [ *remotefile* ] | |
| Rename a file on the remote server | **rename** *remote-source remote-dest* | |
| Exit SFTP client view and return to system view | **bye** | The three commands have the same effect. |
| | **exit** | |
| | **quit** | |

| To do… | Use the command… | Remarks |
|---|---|---|
| Display the online help about a specified command concerning SFTP | **help** [ **all** \| *command-name* ] | 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** *interface-type interface-number* | Use either command<br>Not specified by default. |
| Specify an IP address as the source IP address of the specified SFTP client | **sftp source-ip** *ip-address* | |
| Display the source IP address used by the current SFTP client | **display sftp source-ip** | Optional<br>Available in any view |

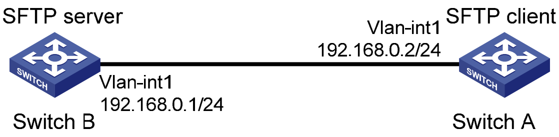
## SFTP Configuration Example

### Network requirements

As shown in Figure 1-6, 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 1-6** 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.

A 3com switch 4200G can act as a TFTP client only.

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<br>Binary by default. |
| Specify an ACL rule used by the specified TFTP client to access a TFTP server | **tftp-server acl** acl-number | Optional<br>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** *interface-type interface-number* { **get** *source-file* [ *dest-file* ] \| **put** *source-file-url* [ *dest-file* ] } | Optional<br>Not specified by default. |
| Specify the source IP address used for the current connection | **tftp** *tftp-server* **source-ip** *ip-address* { **get** *source-file* [ *dest-file* ] \| **put** *source-file-url* [ *dest-file* ] } | Optional<br>Not specified by default. |
| Enter system view | **system-view** | — |

| To do… | Use the command… | Remarks |
|---|---|---|
| Specify an interface as the source interface a TFTP client uses every time it connects to a TFTP server | **tftp source-interface** *interface-type interface-number* | Use either command<br>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** *ip-address* | |
| Display the source IP address used by a TFTP client every time it connects to a TFTP server | **display tftp source-ip** | Optional<br>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

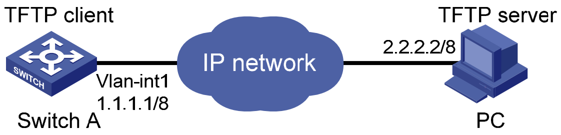
### Network requirements

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

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

## 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 |
| 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 directions of system information

The system supports six information output directions, 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 directions by default. Both the channel names and the associations between the channels and output directions can be changed through commands.

**Table 1-2** Information channels and output directions

| Information channel number | Default channel name | Default output direction |
|---|---|---|
| 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 directions 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 |
| DNS | Domain name system module |
| ETH | Ethernet module |
| FIB | Forwarding module |
| FTPS | FTP server module |
| HA | High availability module |
| HABP | Huawei authentication bypass protocol module |
| HTTPD | HTTP server module |
| HWCM | Huawei Configuration Management private MIB module |
| 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 |
| NAT | Network address translation module |
| NDP | Neighbor discovery protocol module |
| NTDP | Network topology discovery protocol module |
| NTP | Network time protocol 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 |

| Module name | Description |
|---|---|
| SYSMIB | System MIB module |
| TAC | HWTACACS module |
| TELNET | Telnet module |
| TFTPC | TFTP client module |
| VLAN | Virtual local area network 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 directions.

## 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 %%nnmodule/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 “3Com”.

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<br>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 direction 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** *zone-name* { **add** \| **minus** } *time* | Required<br>By default, UTC time zone is set for the system. |
| Enter system view | | **system-view** | — |
| Set the time stamp format in the output direction of the information center to **date** | Log host direction | **info-center timestamp loghost date** | Required<br>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<br>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<br>Enabled by default. |

| To do… | Use the command… | Remarks |
|---|---|---|
| Enable system information output to the console | **info-center console channel** { *channel-number* \| *channel-name* } | Optional<br>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** { *modu-name* \| **default** } **channel** { *channel-number* \| *channel-name* } [ { **log** \| **trap** \| **debug** } { **level** *severity* \| **state** *state* } ]* | Optional<br>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<br>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 directions

| Output direction | 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<br>Enabled by default. |
| Enable debugging information terminal display function | **terminal debugging** | Optional<br>Disabled by default. |
| Enable log information terminal display function | **terminal logging** | Optional<br>Enabled by default. |
| Enable trap information terminal display function | **terminal trapping** | Optional<br>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, VTY, or TTY 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<br>Enabled by default. |
| Enable system information output to Telnet terminal or dumb terminal | **info-center monitor channel** { *channel-number* \| *channel-name* } | Optional<br>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** { *modu-name* \| **default** } **channel** { *channel-number* \| *channel-name* } [ { **log** \| **trap** \| **debug** } { **level** *severity* \| **state** *state* } ]* | Optional<br>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<br>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<br>Enabled by default |
| Enable debugging information terminal display function | **terminal debugging** | Optional<br>Disabled by default |
| Enable log information terminal display function | **terminal logging** | Optional<br>Enabled by default |
| Enable trap information terminal display function | **terminal trapping** | Optional<br>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<br>Enabled by default. |
| Enable system information output to a log host | **info-center loghost** *host-ip-addr* [ **channel** { *channel-number* \| *channel-name* } \| **facility** *local-number* ]* | Required<br>By default, the switch does not output information to the log host.<br>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** *interface-type interface-number* | Optional<br>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** { *modu-name* \| **default** } **channel** { *channel-number* \| *channel-name* } [ { **log** \| **trap** \| **debug** } { **level** *severity* \| **state** *state* } ]* | Optional<br>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<br>By default, the time stamp format of the information output to the log host is **date**. |

**Note**

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<br>Enabled by default. |

| To do… | Use the command… | Remarks |
|---|---|---|
| Enable system information output to the trap buffer | **info-center trapbuffer** [**channel** { *channel-number* \| *channel-name* } \| **size** *buffersize*]* | Optional<br>By default, the switch uses information channel 3 to output trap information to the trap buffer, which can holds up to 256 items by default. |
| Configure the output rules of system information | **info-center source** { *modu-name* \| **default** } **channel** { *channel-number* \| *channel-name* } [ { **log** \| **trap** \| **debug** } { **level** *severity* \| **state** *state* } ]* | Optional<br>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<br>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<br>Enabled by default. |
| Enable information output to the log buffer | **info-center logbuffer** [ **channel** { *channel-number* \| *channel-name* } \| **size** *buffersize* ]* | Optional<br>By default, the switch uses information channel 4 to output log information to the log buffer, which can holds up to 512 items by default. |
| Configure the output rules of system information | **info-center source** { *modu-name* \| **default** } **channel** { *channel-number* \| *channel-name* } [ { **log** \| **trap** \| **debug** } { **level** *severity* \| **state** *state* } ]* | Optional<br>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<br>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** | — |

| To do… | Use the command… | Remarks |
|---|---|---|
| Enable the information center | **info-center enable** | Optional<br>Enabled by default. |
| Enable information output to the SNMP NMS | **info-center snmp channel** { *channel-number* \| *channel-name* } | Optional<br>By default, the switch outputs trap information to SNMP through channel 5. |
| Configure the output rules of system information | **info-center source** { *modu-name* \| **default** } **channel** { *channel-number* \| *channel-name* } [ { **log** \| **trap** \| **debug** } { **level** *severity* \| **state** *state* } ]* | Optional<br>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<br>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.

# Displaying and Maintaining Information Center

| To do… | Use the command… | Remarks |
|---|---|---|
| Display information on an information channel | **display channel** [ *channel-number* \| *channel-name* ] | Available in any view |
| Display the operation status of information center, the configuration of information channels, the format of time stamp | **display info-center** [ **unit** *unit-id* ] | |
| Display the status of log buffer and the information recorded in the log buffer | **display logbuffer** [ **unit** *unit-id* ] [ **level** *severity* \| **size** *buffersize* ]* [ \| { **begin** \| **exclude** \| **include** } *regular-expression* ] | |
| 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** [ **unit** *unit-id* ] [ **size** *buffersize* ] | |
| Clear information recorded in the log buffer | **reset logbuffer** [ **unit** *unit-id* ] | Available in user view |
| Clear information recorded in the trap buffer | **reset trapbuffer** [ **unit** *unit-id* ] | |

# Information Center Configuration Examples

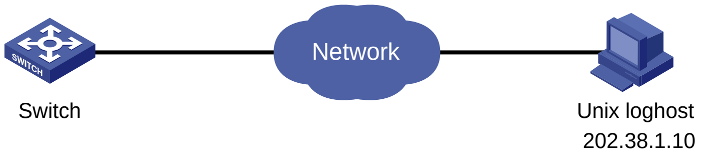
## Log Output to a UNIX Log Host

### 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.

```
[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.

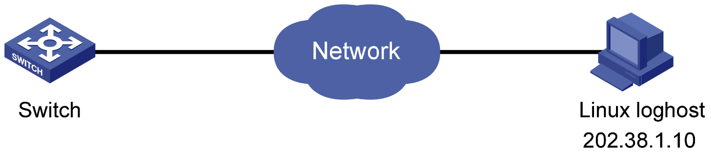
## Log Output to a Linux Log Host

### 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.

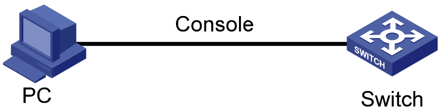
# Log Output to the Console

## 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
```

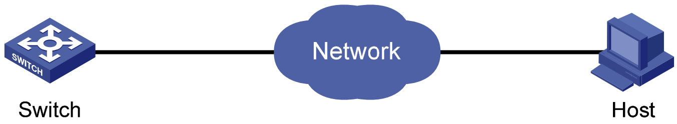
# Configuration Example

## 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

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......



            ************************************************************
            *                                                          *
            *         Switch 4200G 12-Port BOOTROM, Version 2.00       *
            *                                                          *
            ************************************************************

            Copyright (c) 2004-2007 3Com Corporation and its licensors.
            Creation date   : Nov 20 2007, 17:02:48
            CPU Clock Speed : 200MHz
            BUS Clock Speed : 33MHz
            Memory Size     : 64MB
            Mac Address     : 00e0fc005100


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 bps
Please change the terminal's baudrate to 115200 bps and select XMODEM protocol
Press enter key when ready
```

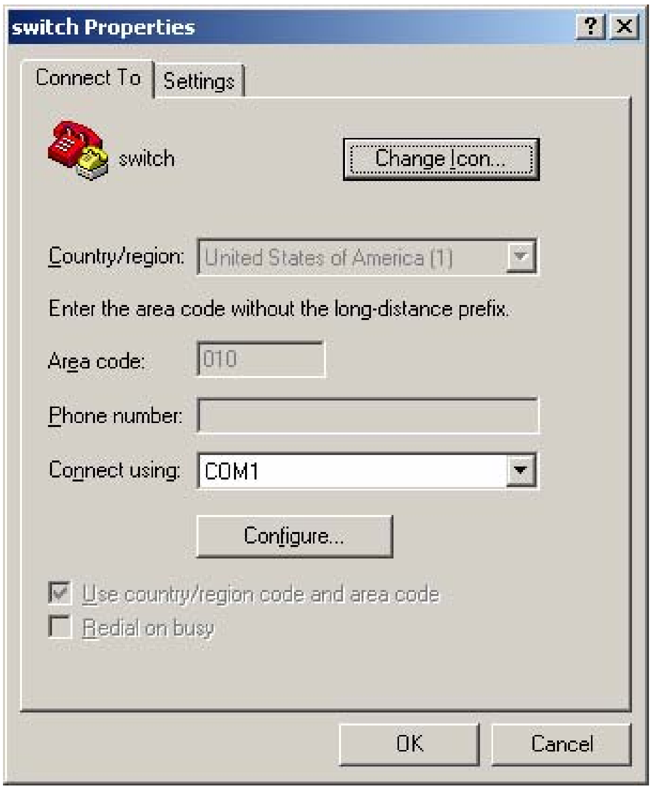
**Note**

If you have chosen 9600 bps as the download baudrate, you need not modify the HyperTerminal's baudrate, and therefore you can skip Step 4 and 5 below and proceed to Step 6 directly. In this case, the system will not display the above information.

Following are configurations on PC. Take the HyperTerminal in Windows 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



switch Properties

Country/region: United States of America (1)

Enter the area code without the long-distance prefix.

Area code: 010

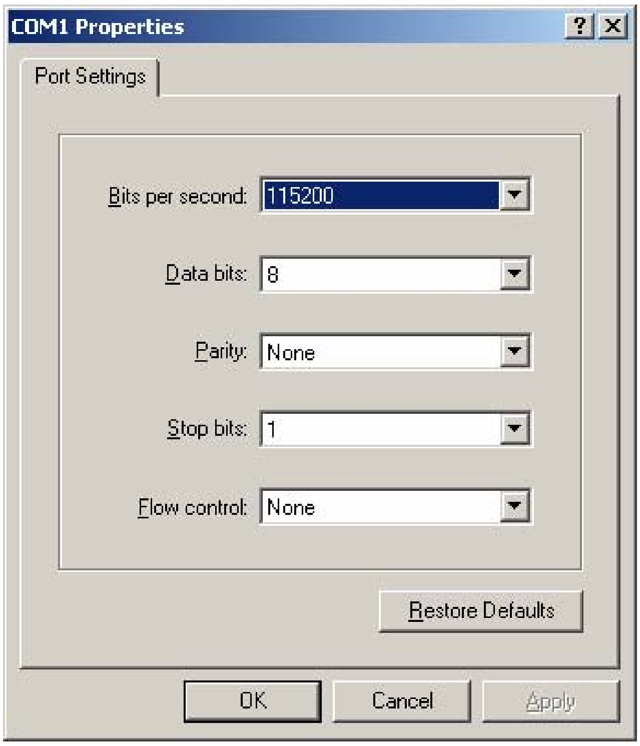
Phone number:

Connect using: COM1

☑ Use country/region code and area code

□ Redial on busy

**Figure 1-2** Console port configuration dialog box



Bits per second: 115200

Data bits: 8

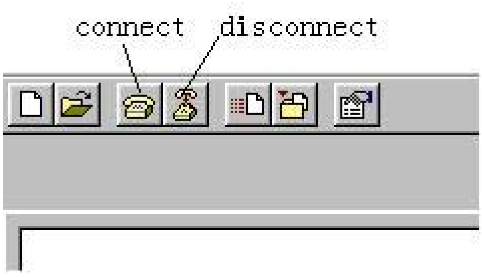
Parity: None

Stop bits: 1

Flow control: None

Step 5: Click the <Disconnect> button to disconnect the HyperTerminal from the switch and then click the <Connect> button to reconnect the HyperTerminal to the switch, as shown in Figure 1-3.

**Figure 1-3** Connect and disconnect buttons



**Note**

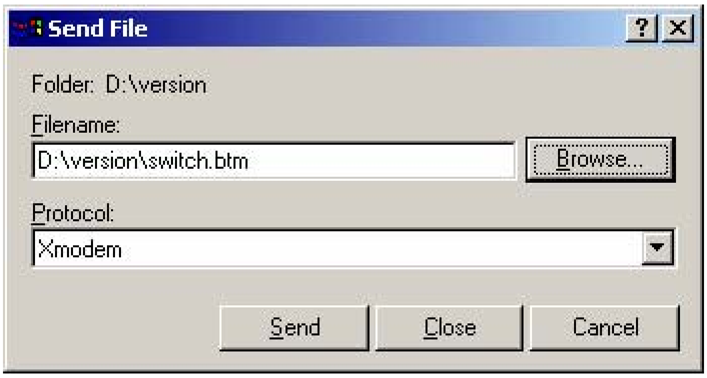
The new baudrate takes effect after you disconnect and reconnect the HyperTerminal program.

Step 6: Press <Enter> to start downloading the program. The system displays the following information:

```
Now please start transfer file with XMODEM protocol.
If you want to exit, Press <Ctrl+X>.
Loading ...CCCCCCCCCC
```

Step 7: Choose [Transfer/Send File] in HyperTerminal, and click <Browse> in pop-up dialog box, as shown in Figure 1-4. Select the software file that you need to load to the switch, and set the protocol to XModem.

**Figure 1-4** Send file dialog box



Send File

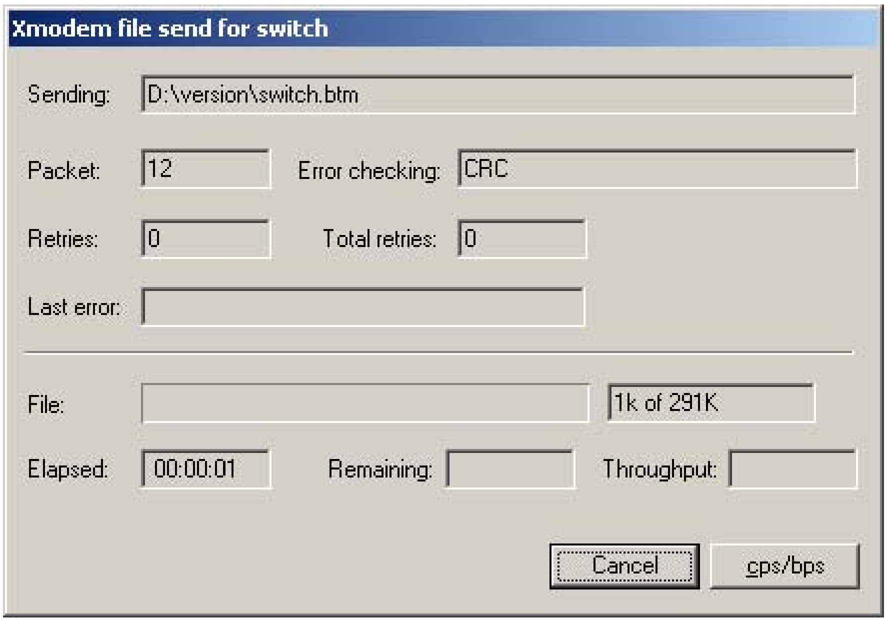
Folder: D:\version

Filename: D:\version\switch.btm

Protocol: Xmodem

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:

Step 9: After the sending process completes, the system displays the following information:

```
Loading ...CCCCCCCCCC done!
```

Step 10: Reset HyperTerminal's baudrate to 9600 bps (refer to Step 4 and 5). Then, press any key as prompted. The system will display the following information when it completes the loading.

```
Bootrom updating.....................................done!
```

**Note**

- If the HyperTerminal's baudrate is not reset to 9600 bps, the system prompts "Your baudrate should be set to 9600 bps again! Press enter key when ready".
- You need not reset the HyperTerminal's baudrate and can skip the last step if you have chosen 9600 bps. In this case, the system upgrades 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.

**Note**

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.

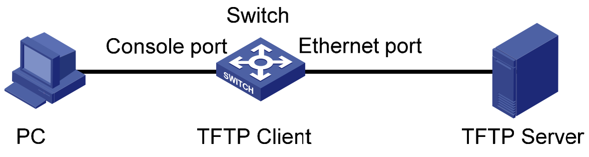
## Loading by TFTP through Ethernet Port

### 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.

**Note**

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 3Com 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

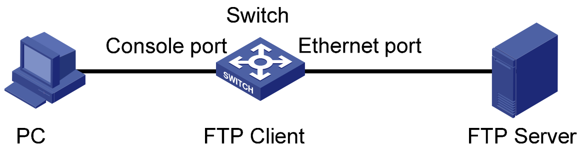
FTP is an application-layer protocol in the TCP/IP protocol suite. It is used for file transfer between server and client, and is widely used in IP networks.

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.

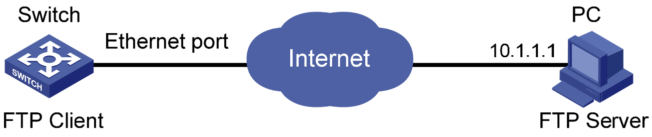
## Remote Loading Using FTP

### 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:

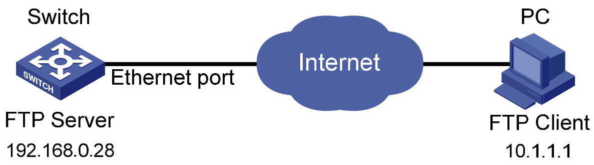
- The loading of Boot ROM and host software takes effect only after you restart the switch with the **reboot** command.
- If the space of the Flash memory is not enough, you can delete the unused files in the Flash memory before software downloading. For information about deleting files, refer to *File 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.

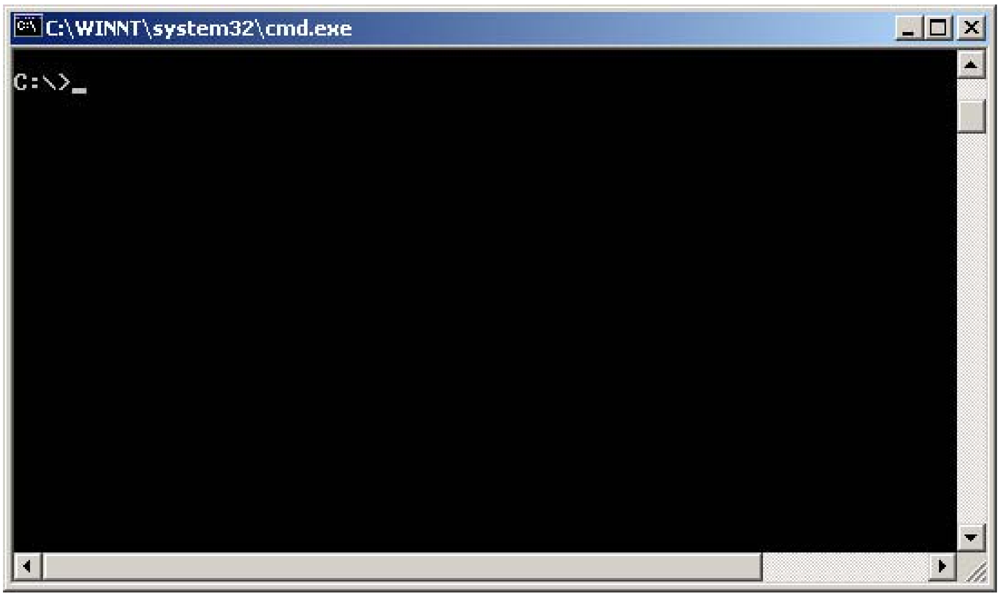
```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface Vlan-interface 1
[Sysname-Vlan-interface1] ip address 192.168.0.28 255.255.255.0
```

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.

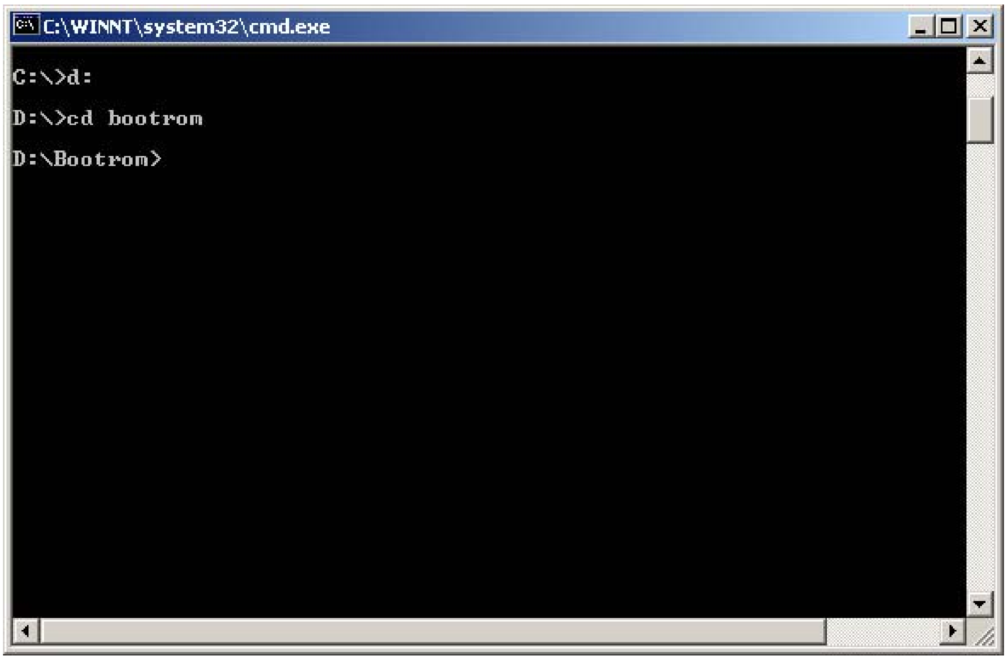
**Figure 1-10** Command line interface



```
C:\>_
```

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 1-110.

**Figure 1-11** Enter Boot ROM directory



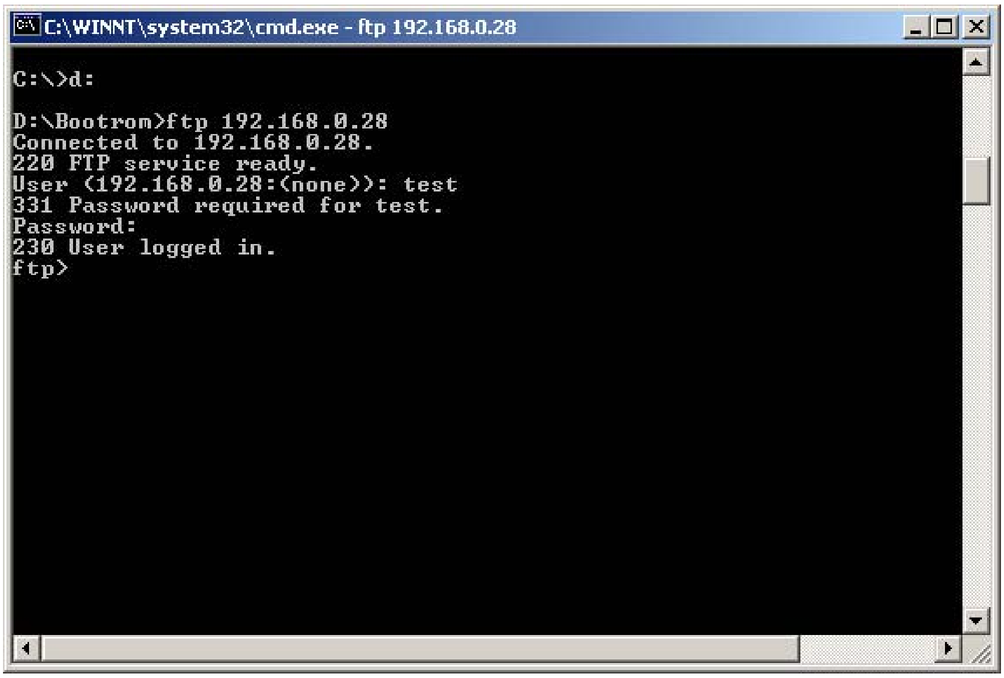
```
C:\>d:

D:\>cd bootrom

D:\Bootrom>
```

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

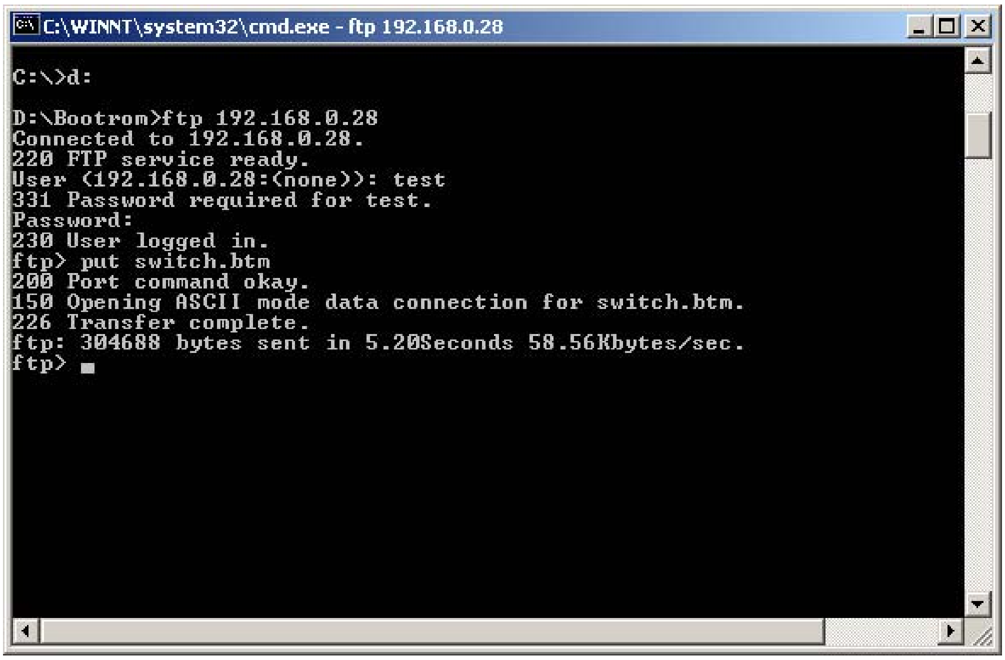


```
C:\>d:

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:\>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** *HH:MM:SS* { *YYYY/MM/DD* \| *MM/DD/YYYY* } | Required<br>Execute this command in user view.<br>The default value is 23:55:00 04/01/2000 when the system starts up. |
| Set the local time zone | **clock timezone** *zone-name* { **add** \| **minus** } *HH:MM:SS* | Optional<br>Execute this command in user view.<br>By default, it is the UTC time zone. |
| Set the name and time range of the summer time | **clock summer-time** *zone_name* { **one-off** \| **repeating** } *start-time start-date end-time end-date offset-time* | Optional<br>Execute this command in user view.<br>• 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.<br>• 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** *sysname* | Optional<br>By default, the name is 3Com. |
| Return from current view to lower level view | **quit** | Optional<br>If the current view is user view, you will quit the current user interface. |

| To do… | Use the command… | Remarks |
|---|---|---|
| Return from current view to user view | **return** | Optional<br>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

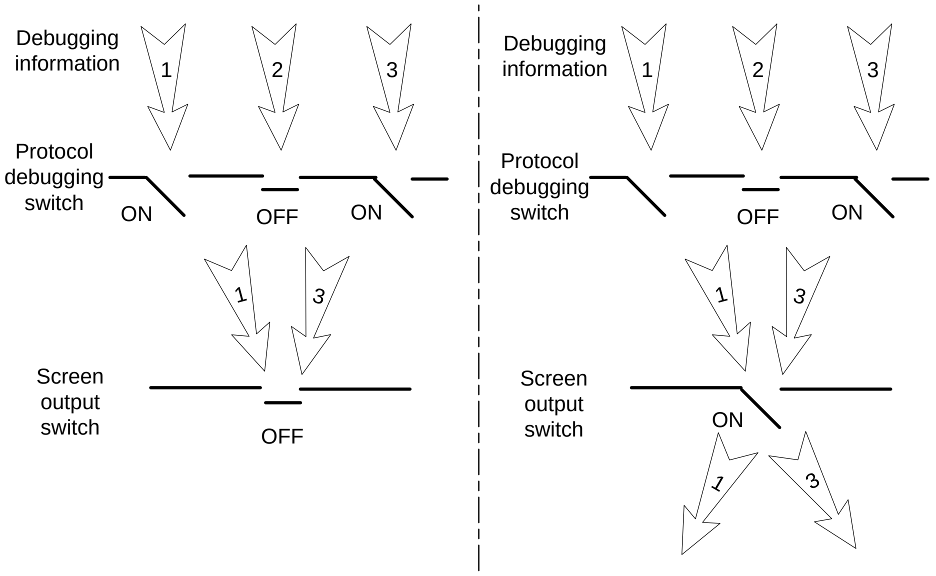
The device provides various debugging functions. For the majority of protocols and features supported, the system provides corresponding debugging information to help users diagnose errors.

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** *module-name* [ *debugging-option* ] | Required<br>Disabled for all modules by default. |
| Enable terminal display for debugging | **terminal debugging** | Required<br>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** [ **unit** *unit-id* ] [ **interface** *interface-type interface-number* ] [ *module-name* ] | Available in any view. |

## 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.<br>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** *ip-address* ] [**-c** *count* ] [ **-d** ] [ **-f** ] [ **-h** *ttl* ] [ **-i** *interface-type interface-number* ] [ **ip** ] [ **-n** ] [ **- p** *pattern* ] [ **-q** ] [ **-s** *packetsize* ] [ **-t** *timeout* ] [ **-tos** *tos* ] [ **-v** ] *host* | You can 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** *source-ip* ] [ **-f** *first-ttl* ] [ **-m** *max-ttl* ] [ **-p** *port* ] [ **-q** *num-packet* ] [ **-w** *timeout* ] *string* | You can execute the **tracert** command in any view. |

# 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
- 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 |
| 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** *unit-id* ] | 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** *hh:mm* [ *mm/dd/yyyy* \| *yyyy/mm/dd* ] | Optional |
| Schedule a reboot on the switch, and set the delay time for reboot | **schedule reboot delay** { *hh:mm* \| *mm* } | Optional |
| Enter system view | **system-view** | — |
| Schedule a reboot on the switch, and set the reboot period | **schedule reboot regularity at** *hh:mm period* | Optional |

**Note**

The switch timer can be set to precision of one minute, that is, the switch will reboot within one minute after the specified reboot date and time.

## 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<br>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** ] { *file-url* \| *device-name* } | 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** { *file-url* \| *device-name* } | Required |

## 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 4-1.

**Table 4-1** 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 |

| Transceiver type | Applied environment | Whether can be an optical transceiver | Whether can be an electrical transceiver |
|---|---|---|---|
| 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 |

## 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** [ *interface-type* *interface-number* ] | 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** [ *interface-type* *interface-number* ] | 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** [ *interface-type* *interface-number* ] | Available for all pluggable transceivers |

| To do… | Use the command… | Remarks |
|---|---|---|
| Display the currently measured value of the digital diagnosis parameters of the anti-spoofing optical transceiver(s) customized by H3C | **display transceiver diagnosis interface** [ *interface-type interface-number* ] | 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** [ **unit** *unit-id* ] | Available in any view. |
| Display the module type and operating status of each board | **display device** [ **manuinfo** \| **unit** *unit-id* ] | |
| Display CPU usage of a switch | **display cpu** [ **unit** *unit-id* ] | |
| Display the operating status of the fan | **display fan** [ **unit** *unit-id* [ *fan-id* ] ] | |
| Display memory usage of a switch | **display memory** [ **unit** *unit-id* ] | |
| Display the operating status of the power supply | **display power** [ **unit** *unit-id* [ *power-id* ] ] | |
| Display system diagnostic information or save system diagnostic information to a file with the extension .diag into the Flash memory | **display diagnostic-information** | |
| Display enabled debugging on a specified switch | **display debugging** { **unit** *unit-id* } [ **interface** *interface-type interface-number* ] [ *module-name* ] | |

# 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.

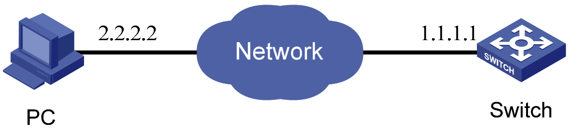
Perform the following configuration on the FTP server.

- 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.app 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.app and boot.btm files from the FTP server to the switch.

## Network diagram

**Figure 4-1** 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.app and boot.btm files on the FTP server to the Flash memory of the switch.

```
[ftp] get switch.app
[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.app
 The specified file will be booted next time on unit 1!
<Sysname> display boot-loader
 Unit 1:
   The current boot app is: switch.app
   The main boot app is:    switch.app
   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
```

# Table of Contents

# 1 remote-ping Configuration

When configuring remote-ping, go to these sections for information you are interested in:

- remote-ping Overview
- remote-ping Configuration
- remote-ping Configuration Examples

## remote-ping Overview

### Introduction to remote-ping

remote-ping is a network diagnostic tool. It is used to test the performance of various protocols running in networks. remote-ping 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, remote-ping 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 remote-ping client and sometimes the corresponding remote-ping servers as well to perform various remote-ping tests.

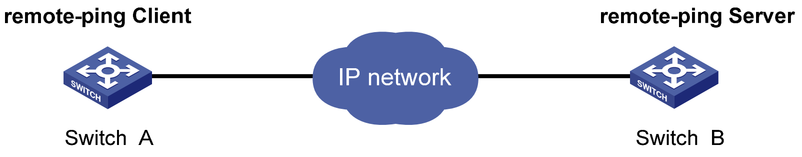
All remote-ping tests are initiated by a remote-ping client and you can view the test results on the remote-ping client only.

When performing a remote-ping test, you need to configure a remote-ping test group on the remote-ping client. A remote-ping test group is a set of remote-ping test parameters. A test group contains several test parameters and is uniquely identified by an administrator name and a test tag.

After creating a remote-ping test group and configuring the test parameters, you can then perform a remote-ping test by the **test-enable** command.

- Being different from the **ping** command, remote-ping 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 remote-ping test operation, you need to execute the **display remote-ping** command.
- remote-ping also allows you to set parameters for remote-ping test groups, start remote-ping tests and view statistical test results through a network management device.

**Figure 1-1** remote-ping illustration



## Test Types Supported by remote-ping

**Table 1-1** Test types supported by remote-ping

| Supported test types | | Description |
|---|---|---|
| ICMP test | | For these types of tests, you need to configure the remote-ping 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 remote-ping client and remote-ping server.<br>• Do not perform a TCP, UDP or jitter test on a well-known port (ports with a number ranging from 1 to 1023) or on a port with a port number greater than 50000. Otherwise, your remote-ping test may fail or the service corresponding to the well-known port may become unavailable. |
| TCP test | Tcppublic test | |
| | Tcpprivate test | |
| UDP test | Udppublic test | |
| | Udpprivate test | |

## remote-ping Test Parameters

You need to configure corresponding test parameters for each type of remote-ping test. remote-ping test parameters can be configured on remote-ping client only. For the configurations on the remote-ping client, refer to section remote-ping Client Configuration.

**Table 1-2** remote-ping 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 remote-ping server. |
| Destination port (**destination-port**) | For a tcpprivate/udpprivate/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 remote-ping server. |
| Source interface (**source-interface**) | • For a DHCP test, you must specify a source interface, which will be used by the remote-ping client to send DHCP requests. If no source interface is specified for the DHCP test, the test will not succeed.<br>• After a source interface is specified, the remote-ping client uses this source interface to send DHCP requests during the DHCP test.<br>• The IP address of the specified source interface will be used as the source IP address of DHCP requests. |
| Source address (**source-ip**) | For remote-ping 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 remote-ping 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 parameter | Description |
|---|---|
| Test type (**test-type**) | - You can use remote-ping to test a variety of protocols, see Table 1-1 for details.<br>- To perform a type of test, you must first create a test group of this type. One test group can be of only one remote-ping test type.<br>- 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.<br>- For ICMP test, the ICMP packet size refers to the length of ECHO-REQUEST packets (excluding IP and ICMP headers) |
| 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, remote-ping discards some earliest records. |
| Automatic test interval (**frequency**) | This parameter is used to set the interval at which the remote-ping client periodically performs the same test automatically. |
| Probe timeout time (**timeout**) | - The probe timeout timer is started after the remote-ping client sends out a test packet.<br>- 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. |
| **dns** | This parameter is used to specify a DNS domain name in a remote-ping DNS test group. |
| **dns-server** | This parameter is used to set the DNS server IP address in a remote-ping DNS test group. |
| HTTP operation type (**http-operation**) | This parameter is used to set the type of HTTP interaction operation between remote-ping client and HTTP server. |
| FTP operation type (**ftp-operation**) | This parameter is used to set the type of FTP interaction operation between remote-ping 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 remote-ping client and FTP server |
| 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<br>- In a jitter probe, the remote-ping client sends a series of packets to the remote-ping server at regular intervals (you can set the interval). Once receiving such a packet, the remote-ping server marks it with a timestamp, and then sends it back to the remote-ping client. Upon receiving a packet returned, the remote-ping client computes the delay jitter time. The remote-ping 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. |

| Test parameter | Description |
|---|---|
| **Trap** | • A remote-ping 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.<br>• You can set the number of consecutive failed remote-ping tests before Trap output. You can also set the number of consecutive failed remote-ping probes before Trap output. |

# remote-ping Configuration

The TCP/UDP/jitter tests need the cooperation of remote-ping client and remote-ping server. Other types of tests need to configure remote-ping client and corresponding different servers.

You can enable both the remote-ping client and remote-ping server functions on an Switch 4200G, that is, the switch can serve as a remote-ping client and server simultaneously.

## remote-ping Server Configuration

The following table describes the configuration on remote-ping server, which is the same for remote-ping test types that need to configure remote-ping server.

Follow these steps to perform remote-ping server configurations:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enable the remote-ping server function | **remote-ping-server enable** | Required<br>Disabled by default. |
| Configure a UDP listening service | **remote-ping-server udpecho** *ip-address port-num* | Required for UDP and jitter tests<br>By default, no UDP listening service is configured. |
| Configure a TCP listening service | **remote-ping-server tcpconnect** *ip-address port-num* | Required for TCP tests<br>By default, no TCP listening service is configured. |

Note that:

- The remote-ping server function is needed only for jitter, TCP, and UDP tests.
- You can configure multiple TCP/UDP listening services on one remote-ping server, with each listening service corresponding to a specific destination IP address and port number.

## remote-ping Client Configuration

### remote-ping client configuration

After remote-ping client is enabled, you can create multiple test groups for different tests, without the need to enable remote-ping client repeatedly for each test group.

Different types of remote-ping tests are somewhat different in parameters and parameter ranges. The following text describes the configuration on remote-ping client for different test types.

1) Configuring ICMP test on remote-ping client

Follow these steps to configure ICMP test on remote-ping client:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enable the remote-ping client function | **remote-ping-agent enable** | Required<br>By default, the remote-ping client function is disabled. |
| Create a remote-ping test group and enter its view | **remote-ping** *administrator-name operation-tag* | Required<br>By default, no test group is configured. |
| Configure the destination IP address | **destination-ip** *ip-address* | Required<br>By default, no destination address is configured. |
| Configure the source IP address | **source-ip** *ip-address* | Optional<br>By default, no source IP address is configured. |
| Configure the test type | **test-type icmp** | Optional<br>By default, the test type is ICMP. |
| Configure the number of probes per test | **count** *times* | Optional<br>By default, each test makes one probe. |
| Configure the packet size | **datasize** *size* | Optional<br>By default, the packet size is 56 bytes. |
| Configure the maximum number of history records that can be saved | **history-records** *number* | Optional<br>By default, the maximum number is 50. |
| Configure the automatic test interval | **frequency** *interval* | Optional<br>By default, the automatic test interval is zero seconds, indicating no automatic test will be made. |
| Configure the probe timeout time | **timeout** *time* | Optional<br>By default, a probe times out in three seconds. |
| Configure the type of service (ToS) | **tos** *value* | Optional<br>By default, the service type is zero. |
| Start the test | **test-enable** | Required |
| Display test results | **display remote-ping results** [ *admin-name operation-tag* ] | Required<br>Available in any view. |

2) Configuring DHCP test on remote-ping client

Follow these steps to configure DHCP test on remote-ping client:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |

| To do… | Use the command… | Remarks |
|---|---|---|
| Enable the remote-ping client function | **remote-ping-agent enable** | Required<br>By default, the remote-ping client function is disabled. |
| Create a remote-ping test group and enter its view | **remote-ping** *administrator-name operation-tag* | Required<br>By default, no test group is configured. |
| Configure the source interface | **source-interface** *interface-type interface-number* | Required<br>You can only configure a VLAN interface as the source interface.<br>By default, no source interface is configured. |
| Configure the test type | **test-type dhcp** | Required<br>By default, the test type is ICMP. |
| Configure the number of probes per test | **count** *times* | Optional<br>By default, each test makes one probe. |
| Configure the maximum number of history records that can be saved | **history-records** *number* | Optional<br>By default, the maximum number is 50. |
| Configure the probe timeout time | **timeout** *time* | Optional<br>By default, a probe times out in three seconds. |
| Start the test | **test-enable** | Required |
| Display test results | **display remote-ping results** [ *admin-name operation-tag* ] | Required<br>You can execute the command in any view. |

3) Configuring FTP test on remote-ping client

Follow these steps to configure FTP test on remote-ping client:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enable the remote-ping client function | **remote-ping-agent enable** | Required<br>By default, the remote-ping client function is disabled. |
| Create a remote-ping test group and enter its view | **remote-ping** *administrator-name operation-tag* | Required<br>By default, no test group is configured. |
| Configure the destination IP address | **destination-ip** *ip-address* | Required<br>By default, no destination address is configured. |
| Configure the source IP address | **source-ip** *ip-address* | Required<br>By default, no source IP address is configured. |
| Configure the source port | **source-port** *port-number* | Optional<br>By default, no source port is configured. |

| To do… | Use the command… | Remarks |
|---|---|---|
| Configure the test type | **test-type ftp** | Required<br>By default, the test type is ICMP. |
| Configure the number of probes per test | **count** *times* | Optional<br>By default, each test makes one probe. |
| Configure the maximum number of history records that can be saved | **history-records** *number* | Optional<br>By default, the maximum number is 50. |
| Configure the automatic test interval | **frequency** *interval* | Optional<br>By default, the automatic test interval is zero seconds, indicating no automatic test will be made. |
| Configure the probe timeout time | **timeout** *time* | Optional<br>By default, a probe times out in three seconds. |
| Configure the type of service | **tos** *value* | Optional<br>By default, the service type is zero. |
| Configure the type of FTP operation | **ftp-operation** { **get** \| **put** } | Optional<br>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** *name* | Required<br>By default, neither username nor password is configured. |
| Configure an FTP login password | **password** *password* | |
| Configure a file name for the FTP operation | **filename** *file-name* | Required<br>By default, no file name is configured for the FTP operation |
| Start the test | **test-enable** | Required |
| Display test results | **display remote-ping results** [ *admin-name operation-tag* ] | Required<br>You can execute the command in any view. |

4) Configuring HTTP test on remote-ping client

Follow these steps to configure HTTP test on remote-ping client:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enable the remote-ping client function | **remote-ping-agent enable** | Required<br>By default, the remote-ping client function is disabled. |
| Create a remote-ping test group and enter its view | **remote-ping** *administrator-name operation-tag* | Required<br>By default, no test group is configured. |

| To do… | Use the command… | Remarks |
|---|---|---|
| Configure the destination IP address | **destination-ip** *ip-address* | Required<br>You can configure an IP address or a host name.<br>By default, no destination address is configured. |
| Configure dns-server | **dns-server** *ip-address* | Required when you use the **destination-ip** command to configure the destination address as the host name.<br>By default, no IP address of the DNS server is configured. |
| Configure the source IP address | **source-ip** *ip-address* | Optional<br>By default, no source IP address is configured. |
| Configure the source port | **source-port** port-number | Optional<br>By default, no source port is configured. |
| Configure the test type | **test-type http** | Required<br>By default, the test type is ICMP. |
| Configure the number of probes per test | **count** *times* | Optional<br>By default, each test makes one probe. |
| Configure the maximum number of history records that can be saved | **history-records** *number* | Optional<br>By default, the maximum number is 50. |
| Configure the automatic test interval | **frequency** *interval* | Optional<br>By default, the automatic test interval is zero seconds, indicating no automatic test will be made. |
| Configure the probe timeout time | **timeout** *time* | Optional<br>By default, a probe times out in three seconds. |
| Configure the type of service | **tos** *value* | Optional<br>By default, the service type is zero. |
| Configure the type of HTTP operation | **http-operation** { **get** \| **post** } | Optional<br>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** *string version* | Optional<br>By default, no HTTP operation string and HTTP version are configured. |
| Start the test | **test-enable** | Required |
| Display test results | **display remote-ping results** [ *admin-name operation-tag* ] | Required<br>You can execute the command in any view. |

5) Configuring jitter test on remote-ping client

Follow these steps to configure jitter test on remote-ping client:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enable the remote-ping client function | **remote-ping-agent enable** | Required<br>By default, the remote-ping client function is disabled. |
| Create a remote-ping test group and enter its view | **remote-ping** *administrator-name operation-tag* | Required<br>By default, no test group is configured. |
| Configure the destination IP address | **destination-ip** *ip-address* | Required<br>The destination address must be the IP address of a UDP listening service on the remote-ping server.<br>By default, no destination address is configured. |
| Configure the destination port | **destination-port**<br>*Port-number* | Required<br>The destination port must be the port of a UDP listening service on the remote-ping server.<br>By default, no destination port is configured. |
| Configure the source IP address | **source-ip** *ip-address* | Optional<br>By default, no source IP address is configured. |
| Configure the source port | **source-port** *port-number* | Optional<br>By default, no source port is configured. |
| Configure the test type | **test-type jitter** | Required<br>By default, the test type is ICMP. |
| Configure the number of probes per test | **count** *times* | Optional<br>By default, each test makes one probe. |
| Configure the maximum number of history records that can be saved | **history-records** *number* | Optional<br>By default, the maximum number is 50. |
| Configure the packet size | **datasize** *size* | Optional<br>By default, the packet size is 68 bytes. |
| Configure the automatic test interval | **frequency** *interval* | Optional<br>By default, the automatic test interval is zero seconds, indicating no automatic test will be made. |
| Configure the probe timeout time | **timeout** *time* | Optional<br>By default, a probe times out in three seconds. |

| To do… | Use the command… | Remarks |
|---|---|---|
| Configure the type of service | **tos** *value* | Optional<br>By default, the service type is zero. |
| Configure the number of test packets that will be sent in each jitter probe | **jitter-packetnum** *number* | Optional<br>By default, each jitter probe will send 10 packets. |
| Configure the interval to send test packets in the jitter test | **jitter-interval** *interval* | Optional<br>By default, the interval is 20 milliseconds. |
| Start the test | **test-enable** | Required |
| Display test results | **display remote-ping results** [ *admin-name operation-tag* ] | Required<br>You can execute the command in any view. |

6) Configuring SNMP test on remote-ping client

Follow these steps to configure SNMP test on remote-ping client:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enable the remote-ping client function | **remote-ping-agent enable** | Required<br>By default, the remote-ping client function is disabled. |
| Create a remote-ping test group and enter its view | **remote-ping** *administrator-name operation-tag* | Required<br>By default, no test group is configured. |
| Configure the destination IP address | **destination-ip** *ip-address* | Required<br>By default, no destination address is configured. |
| Configure the source IP address | **source-ip** *ip-address* | Optional<br>By default, no source IP address is configured. |
| Configure the source port | **source-port** port-number | Optional<br>By default, no source port is configured. |
| Configure the test type | **test-type snmpquery** | Required<br>By default, the test type is ICMP. |
| Configure the number of probes per test | **count** *times* | Optional<br>By default, each test makes one probe. |
| Configure the maximum number of history records that can be saved | **history-records** *number* | Optional<br>By default, the maximum number is 50. |

| To do… | Use the command… | Remarks |
|---|---|---|
| Configure the automatic test interval | **frequency** *interval* | Optional<br>By default, the automatic test interval is zero seconds, indicating no automatic test will be made. |
| Configure the probe timeout time | **timeout** *time* | Optional<br>By default, a probe times out in three seconds. |
| Configure the type of service | **tos** *value* | Optional<br>By default, the service type is zero. |
| Start the test | **test-enable** | Required |
| Display test results | **display remote-ping results** [ *admin-name operation-tag* ] | Required<br>You can execute the command in any view. |

7) Configuring TCP test on remote-ping client

Follow these steps to configure TCP test on remote-ping client:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enable the remote-ping client function | **remote-ping-agent enable** | Required<br>By default, the remote-ping client function is disabled. |
| Create a remote-ping test group and enter its view | **remote-ping** *administrator-name operation- tag* | Required<br>By default, no test group is configured. |
| Configure the destination address | **destination-ip** *ip-address* | Required<br>This IP address and the one configured on the remote-ping server for listening services must be the same.<br>By default, no destination address is configured. |
| Configure the destination port | **destination-port** *port-number* | Required in a Tcpprivate test<br>A Tcppublic test is a TCP connection test on port 7. Use the **remote-ping-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.<br>By default, no destination port number is configured. |
| Configure the source IP address | **source-ip** *ip-address* | Optional<br>By default, the source IP address is not specified. |

| To do… | Use the command… | Remarks |
|---|---|---|
| Configure the source port | **source-port** *port-number* | Optional<br>By default, no source port is specified. |
| Configure the test type | **test-type { tcpprivate \| tcppublic** *}* | Required<br>By default, the test type is ICMP. |
| Configure the number of probes per test | **count** *times* | Optional<br>By default, one probe is made per time. |
| Configure the automatic test interval | **frequency** *interval* | Optional<br>By default, the automatic test interval is zero seconds, indicating no automatic test will be made. |
| Configure the probe timeout time | **timeout** *time* | Optional<br>By default, a probe times out in three seconds. |
| Configure the maximum number of history records that can be saved | **history-records** *number* | Optional<br>By default, the maximum number is 50. |
| Configure the type of service | **tos** *value* | Optional<br>By default, the service type is zero. |
| Start the test | **test-enable** | Required |
| Display test results | **display remote-ping results** [ *admin-name operation-tag* ] | Required<br>The **display** command can be executed in any view. |

8) Configuring UDP test on remote-ping client

Follow these steps to configure UDP test on remote-ping client:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enable the remote-ping client function | **remote-ping-agent enable** | Required<br>By default, the remote-ping client function is disabled. |
| Create a remote-ping test group and enter its view | **remote-ping** *administrator-name operation- tag* | Required<br>By default, no test group is configured. |
| Configure the destination address | **destination-ip** *ip-address* | Required<br>This IP address and the one configured on the remote-ping server for listening service must be the same.<br>By default, no destination address is configured. |

| To do… | Use the command… | Remarks |
|---|---|---|
| Configure the destination port | **destination-port** *port-number* | • Required in a Udpprivate test<br>• A Udppublic test is a UDP connection test on port 7. Use the remote-ping-server udpecho 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.<br>• By default, no destination port number is configured. |
| Configure the source IP address | **source-ip** *ip-address* | Optional<br>By default, no source IP address is configured. |
| Configure the source port | **source-port** *port-number* | Optional<br>By default, no source port is specified. |
| Configure the test type | **test-type** *{* **udpprivate** \| **udppublic** *}* | Required<br>By default, the test type is ICMP. |
| Configure the number of probes per test | **count** *times* | Optional<br>By default, one probe is made per test. |
| Configure the maximum number of history records that can be saved | **history-records** *number* | Optional<br>By default, the maximum number is 50. |
| Configure the data packet size | **datasize** *size* | Optional<br>By default, the data packet size is 100 bytes. |
| Configure the automatic test interval | **frequency** *interval* | Optional<br>By default, the automatic test interval is zero seconds, indicating no automatic test will be made. |
| Configure the probe timeout time | **timeout** *time* | Optional<br>By default, a probe times out in three seconds. |
| Configure the service type | **tos** *value* | Optional<br>By default, the service type is zero. |
| Start the test | **test-enable** | Required |
| Display test results | **display remote-ping results** [ *admin-name operation-tag* ] | Required<br>The **display** command can be executed in any view. |

9) Configuring DNS test on remote-ping client

Follow these steps to configure DNS test on remote-ping client:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | system-view | — |

| To do… | Use the command… | Remarks |
|---|---|---|
| Enable the remote-ping client function | **remote-ping-agent enable** | Required<br>By default, the remote-ping client function is disabled. |
| Create a remote-ping test group and enter its view | **remote-ping** *administrator-name operation-tag* | Required<br>By default, no test group is configured. |
| Configure the source IP address | **source-ip** *ip-address* | Optional<br>By default, no source IP address is specified. |
| Configure the test type | **test-type dns** | Required<br>By default, the test type is ICMP. |
| Configure the number of probes per test | **count** *times* | Optional<br>By default, one probe is made per test. |
| Configure the maximum number of history records that can be saved | **history-records** *number* | Optional<br>By default, the maximum number is 50. |
| Configure the automatic test interval | **frequency** *interval* | Optional<br>By default, the automatic test interval is zero seconds, indicating no automatic test will be made. |
| Configure the probe timeout time | **timeout** *time* | Optional<br>By default, a probe times out in three seconds. |
| Configure the type of service | **tos** *value* | Optional<br>By default, the service type is zero. |
| Configure the domain name to be resolved | **dns resolve-target** *domain-name* | Required<br>By default, the domain name to be resolved by DNS is not specified. |
| Configure the IP address of the DNS server | **dns-server** *ip-address* | Required<br>By default, no DNS server address is configured. |
| Start the test | **test-enable** | Required |
| Display test results | **display remote-ping results** [ *admin-name operation-tag* ] | Required<br>The **display** command can be executed in any view. |

### Configuring remote-ping client to send Trap messages

Trap messages are generated regardless of whether the remote-ping test succeeds or fails. You can specify whether to output Trap messages by enabling/disabling Trap sending.

Follow these steps to configure the remote-ping client to send Trap messages:

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Enable the remote-ping client function | **remote-ping-agent enable** | Required<br>By default, the remote-ping client function is disabled. |
| Create a remote-ping test group and enter its view | **remote-ping** *administrator-name operation-tag* | Required<br>By default, no test group is configured. |
| Enable the remote-ping client to send Trap messages | **send-trap** { **all** \| { **probefailure** \| **testcomplete** \| **testfailure** }* } | Required<br>By default, Trap sending is disabled. |
| Configure the number of consecutive unsuccessful remote-ping tests before Trap output | **test-failtimes** *times* | Optional<br>By default, Trap messages are sent each time a test fails. |
| Configure the number of consecutive unsuccessful remote-ping probes before Trap output | **probe-failtimes** *times* | Optional<br>By default, Trap messages are sent each time a probe fails. |

## Displaying remote-ping Configuration

| To do… | Use the command… | Remarks |
|---|---|---|
| Display test history | **display remote-ping history** [ *administrator-name operation-tag* ] | Available in any view |
| Display the results of the latest test | **display remote-ping results** [ *administrator-name operation-tag* ] | |

# remote-ping Configuration Examples

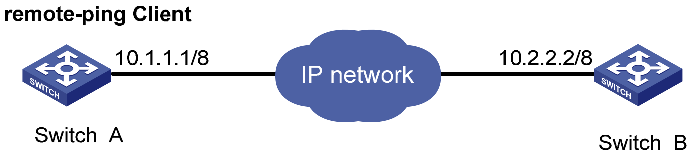
## ICMP Test

### Network requirements

An Switch 4200G serves as the remote-ping client. A remote-ping ICMP test between the switch and another switch uses ICMP to test the round trip time (RTT) for packets generated by the remote-ping client to travel to and back from the destination switch.

### Network diagram

**Figure 1-2** Network diagram for the ICMP test



## Configuration procedure

- Configure remote-ping Client (Switch A):

# Enable the remote-ping client.

```
<Sysname> system-view
[Sysname] remote-ping-agent enable
```

# Create a remote-ping test group, setting the administrator name to **administrator** and test tag to **ICMP**.

```
[Sysname] remote-ping administrator icmp
```

# Configure the test type as **icmp**.

```
[Sysname-remote-ping-administrator-icmp] test-type icmp
```

# Configure the destination IP address as 10.2.2.2.

```
[Sysname-remote-ping-administrator-icmp] destination-ip 10.2.2.2
```

# Configure to make 10 probes per test.

```
[Sysname-remote-ping-administrator-icmp] count 10
```

# Set the probe timeout time to 5 seconds.

```
[Sysname-remote-ping-administrator-icmp] timeout 5
```

# Start the test.

```
[Sysname-remote-ping-administrator-icmp] test-enable
```

# Set the maximum number of history records that can be saved to 5.

```
[Sysname-remote-ping-administrator-icmp] history-records 5
```

# Display test results.

```
[Sysname-remote-ping-administrator-icmp] display remote-ping results administrator icmp
remote-ping 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-remote-ping-administrator-icmp] display remote-ping history administrator icmp
remote-ping 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.

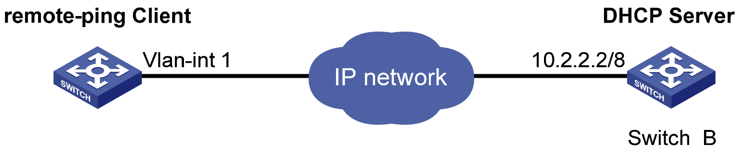
## DHCP Test

### Network requirements

Both the remote-ping client and the DHCP server are 4200G Ethernet switches. Perform a remote-ping DHCP test between the two switches to test the time required for the remote-ping 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 remote-ping Client (Switch A):

# Enable the remote-ping client.

```
<Sysname> system-view
[Sysname] remote-ping-agent enable
```

# Create a remote-ping test group, setting the administrator name to **administrator** and test tag to **DHCP**.

```
[Sysname] Remote-ping administrator dhcp
```

# Configure the test type as **dhcp**.

```
[Sysname-remote-ping-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-remote-ping-administrator-dhcp] source-interface Vlan-interface 1
```

# Configure to make 10 probes per test.

```
[Sysname-remote-ping-administrator-dhcp] count 10
```

# Set the probe timeout time to 5 seconds.

```
[Sysname-remote-ping-administrator-dhcp] timeout 5
```

# Start the test.

```
[Sysname-remote-ping-administrator-dhcp] test-enable
```

# Display test results

```
[Sysname-remote-ping-administrator-dhcp] display remote-ping results administrator dhcp
```

```
remote-ping 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-remote-ping-administrator-dhcp] display remote-ping history administrator dhcp
remote-ping 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 a remote-ping 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 remote-ping DHCP test failure.

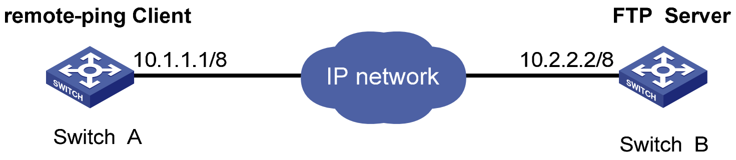
## FTP Test

### Network requirements

Both the remote-ping client and the FTP server are 4200G Ethernet switches. Perform a remote-ping 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 remote-ping Client (Switch A):

# Enable the remote-ping client.

```
<Sysname> system-view
[Sysname] remote-ping-agent enable
```

# Create a remote-ping test group, setting the administrator name to **administrator** and test tag to **FTP**.

```
[Sysname] remote-ping administrator ftp
```

# Configure the test type as **ftp**.

```
[Sysname-remote-ping-administrator-ftp] test-type ftp
```

# Configure the IP address of the FTP server as 10.2.2.2.

```
[Sysname-remote-ping-administrator-ftp] destination-ip 10.2.2.2
```

# Configure the FTP login username.

```
[Sysname-remote-ping-administrator-ftp] username admin
```

# Configure the FTP login password.

```
[Sysname-remote-ping-administrator-ftp] password admin
```

# Configure the type of FTP operation.

```
[Sysname-remote-ping-administrator-ftp] ftp-operation put
```

# Configure a file name for the FTP operation.

```
[Sysname-remote-ping-administrator-ftp] filename cmdtree.txt
```

# Configure to make 10 probes per test.

```
[Sysname-remote-ping-administrator-ftp] count 10
```

# Set the probe timeout time to 30 seconds.

```
[Sysname-remote-ping-administrator-ftp] timeout 30
```

# Configure the source IP address

```
[Sysname-remote-ping-administrator-ftp] source-ip 10.1.1.1
```

# Start the test.

```
[Sysname-remote-ping-administrator-ftp] test-enable
```

# Display test results

```
[Sysname-remote-ping-administrator-ftp] display remote-ping results administrator ftp
remote-ping 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-remote-ping-administrator-ftp] display remote-ping history administrator ftp
remote-ping 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 remote-ping client.

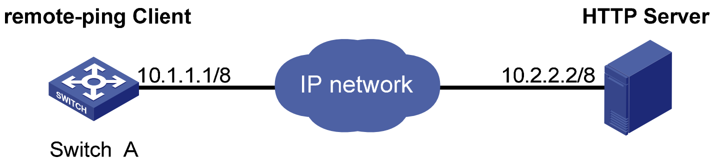
## HTTP Test

### Network requirements

An Switch 4200G serves as the remote-ping client, and a PC serves as the HTTP server. Perform a remote-ping 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 remote-ping Client (Switch A):

# Enable the remote-ping client.

```
<Sysname> system-view
[Sysname] remote-ping-agent enable
```

# Create a remote-ping test group, setting the administrator name to **administrator** and test tag to **HTTP**.

```
[Sysname] Remote-ping administrator http
```

# Configure the test type as **http**.

```
[Sysname-remote-ping-administrator-http] test-type http
```

# Configure the IP address of the HTTP server as 10.2.2.2.

```
[Sysname-remote-ping-administrator-http] destination-ip 10.2.2.2
```

# Configure to make 10 probes per test.

```
[Sysname-remote-ping-administrator-http] count 10
```

# Set the probe timeout time to 30 seconds.

```
[Sysname-remote-ping-administrator-http] timeout 30
```

# Start the test.

```
[Sysname-remote-ping-administrator-http] test-enable
```

# Display test results

```
[Sysname-remote-ping-administrator-http] display remote-ping results administrator http
  remote-ping 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-remote-ping-administrator-http] display remote-ping history administrator http
remote-ping 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.

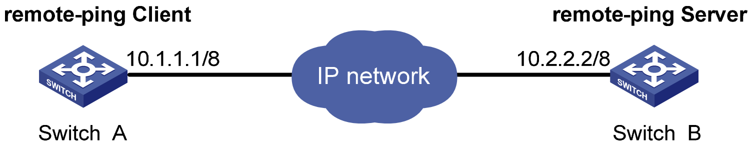
## Jitter Test

### Network requirements

Both the remote-ping client and the remote-ping server are 4200G Ethernet switches. Perform a remote-ping jitter test between the two switches to test the delay jitter of the UDP packets exchanged between this end (remote-ping client) and the specified destination end (remote-ping server).

## Network diagram

**Figure 1-6** Network diagram for the Jitter test



## Configuration procedure

- Configure remote-ping Server (Switch B):

# Enable the remote-ping server and configure the IP address and port to listen on.

```
<Sysname> system-view
[Sysname] remote-ping-server enable
[Sysname] remote-ping-server udpecho 10.2.2.2 9000
```

- Configure remote-ping Client (Switch A):

# Enable the remote-ping client.

```
<Sysname> system-view
[Sysname] remote-ping-agent enable
```

# Create a remote-ping test group, setting the administrator name to **administrator** and test tag to **Jitter**.

```
[Sysname] remote-ping administrator Jitter
```

# Configure the test type as **jitter**

```
[Sysname-remote-ping-administrator-Jitter] test-type Jitter
```

# Configure the IP address of the remote-ping server as 10.2.2.2.

```
[Sysname-remote-ping-administrator-Jitter] destination-ip 10.2.2.2
```

# Configure the destination port on the remote-ping server.

```
[Sysname-remote-ping-administrator-Jitter] destination-port 9000
```

# Configure to make 10 probes per test.

```
[Sysname-remote-ping-administrator-http] count 10
```

# Set the probe timeout time to 30 seconds.

```
[Sysname-remote-ping-administrator-Jitter] timeout 30
```

# Start the test.

```
[Sysname-remote-ping-administrator-Jitter] test-enable
```

# Display test results

```
[Sysname-remote-ping-administrator-Jitter]  display  remote-ping  results  administrator
Jitter
remote-ping 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-remote-ping-administrator-Jitter] display remote-ping history administrator Jitter
remote-ping 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.

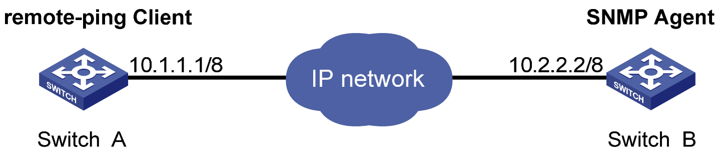
## SNMP Test

### Network requirements

Both the remote-ping client and the SNMP Agent are 4200G Ethernet switches. Perform remote-ping 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 remote-ping Client (Switch A):

# Enable the remote-ping client.

```
<Sysname> system-view
[Sysname] remote-ping-agent enable
```

# Create a remote-ping test group, setting the administrator name to **administrator** and test tag to **snmp**.

```
[Sysname] Remote-ping administrator snmp
```

# Configure the test type as **snmp**.

```
[Sysname-remote-ping-administrator-snmp] test-type snmpquery
```

# Configure the destination IP address as 10.2.2.2.

```
[Sysname-remote-ping-administrator-snmp] destination-ip 10.2.2.2
```

# Configure to make 10 probes per test.

```
[Sysname-remote-ping-administrator-snmp] count 10
```

# Set the probe timeout time to 30 seconds.

```
[Sysname-remote-ping-administrator-snmp] timeout 30
```

# Start the test.

```
[Sysname-remote-ping-administrator-snmp] test-enable
```

# Display test results

```
[Sysname-remote-ping-administrator-snmp] display remote-ping results administrator snmp
remote-ping 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-remote-ping-administrator-snmp] display remote-ping history administrator snmp
remote-ping 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.

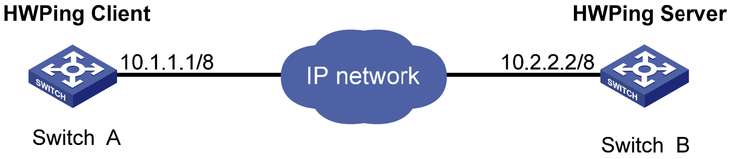
## TCP Test (Tcpprivate Test) on the Specified Ports

### Network requirements

Both the remote-ping client and the remote-ping server are 4200G Ethernet switches. Perform a remote-ping Tcpprivate 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 remote-ping Server (Switch B):

# Enable the remote-ping server and configure the IP address and port to listen on.

```
<Sysname> system-view
[Sysname] remote-ping-server enable
[Sysname] remote-ping-server tcpconnect 10.2.2.2 8000
```

- Configure remote-ping Client (Switch A):

# Enable the remote-ping client.

```
<Sysname> system-view
[Sysname] remote-ping-agent enable
```

# Create a remote-ping test group, setting the administrator name to **administrator** and test tag to **tcpprivate**.

```
[Sysname] remote-ping administrator tcpprivate
```

# Configure the test type as **tcpprivate**.

```
[Sysname-remote-ping-administrator-tcpprivate] test-type tcpprivate
```

# Configure the IP address of the remote-ping server as 10.2.2.2.

```
[Sysname-remote-ping-administrator-tcpprivate] destination-ip 10.2.2.2
```

# Configure the destination port on the remote-ping server.

```
[Sysname-remote-ping-administrator-tcpprivate] destination-port 8000
```

# Configure to make 10 probes per test.

```
[Sysname-remote-ping-administrator-tcpprivate] count 10
```

# Set the probe timeout time to 5 seconds.

```
[Sysname-remote-ping-administrator-tcpprivate] timeout 5
```

# Start the test.

```
[Sysname-remote-ping-administrator-tcpprivate] test-enable
```

# Display test results.

```
[Sysname-remote-ping-administrator-tcpprivate] display remote-ping results administrator
tcpprivate
remote-ping 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                   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-remote-ping-administrator-tcpprivate] display remote-ping history administrator
tcpprivate
remote-ping entry(admin administrator, tag tcpprivate) 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.

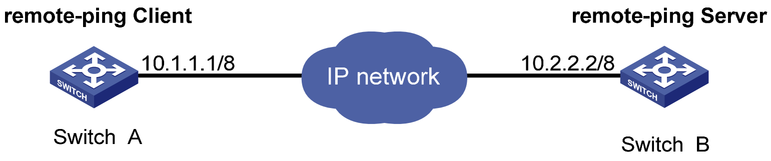
## UDP Test (Udpprivate Test) on the Specified Ports

### Network requirements

Both the remote-ping client and the remote-ping server are 4200G Ethernet switches. Perform a remote-ping Udpprivate test on the specified ports between the two switches to test the RTT of UDP packets between this end (remote-ping client) and the specified destination end (remote-ping server).

### Network diagram

**Figure 1-9** Network diagram for the Udpprivate test



### Configuration procedure

- Configure remote-ping Server (Switch B):

# Enable the remote-ping server and configure the IP address and port to listen on.

```
<Sysname> system-view
[Sysname] remote-ping-server enable
[Sysname] remote-ping-server udpecho 10.2.2.2 8000
```

- Configure remote-ping Client (Switch A):

# Enable the remote-ping client.

```
<Sysname> system-view
[Sysname] remote-ping-agent enable
```

# Create a remote-ping test group, setting the administrator name to **administrator** and test tag to **udpprivate**.

```
[Sysname] remote-ping administrator udpprivate
```

# Configure the test type as **udpprivate**.

```
[Sysname-remote-ping-administrator-udpprivate] test-type udpprivate
```

# Configure the IP address of the remote-ping server as 10.2.2.2.

```
[Sysname-remote-ping-administrator-udpprivate] destination-ip 10.2.2.2
```

# Configure the destination port on the remote-ping server.

```
[Sysname-remote-ping-administrator-udpprivate] destination-port 8000
```

# Configure to make 10 probes per test.

```
[Sysname-remote-ping-administrator-udpprivate] count 10
```

# Set the probe timeout time to 5 seconds.

```
[Sysname-remote-ping-administrator-udpprivate] timeout 5
```

# Start the test.

```
[Sysname-remote-ping-administrator-udpprivate] test-enable
```

# Display test results.

```
[Sysname-remote-ping-administrator-udpprivate] display remote-ping results administrator
udpprivate
remote-ping 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-remote-ping-administrator-udpprivate] display remote-ping history administrator
udpprivate
remote-ping 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.

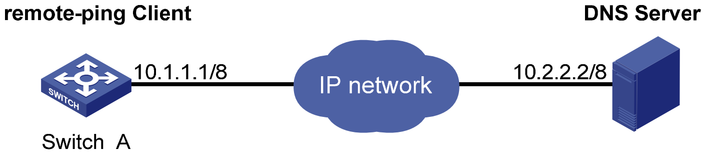
## DNS Test

### Network requirements

An Switch 4200G serves as the remote-ping client, and a PC serves as the DNS server. Perform a remote-ping 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 remote-ping Client (Switch A)

# Enable the remote-ping client.

```
<Sysname> system-view
[Sysname] remote-ping-agent enable
```

# Create a remote-ping test group, setting the administrator name to **administrator** and test tag to **dns**.

```
[Sysname] remote-ping administrator dns
```

# Configure the test type as **dns**.

```
[Sysname-remote-ping-administrator-dns] test-type dns
```

# Configure the IP address of the DNS server as 10.2.2.2.

```
[Sysname-remote-ping-administrator-dns] dns-server 10.2.2.2
```

# Configure to resolve the domain name www.test.com.

```
[Sysname-remote-ping-administrator-dns] dns resolve-target www.test.com
```

# Configure to make 10 probes per test.

```
[Sysname-remote-ping-administrator-dns] count 10
```

# Set the probe timeout time to 5 seconds.

```
[Sysname-remote-ping-administrator-dns] timeout 5
```

# Start the test.

```
[Sysname-remote-ping-administrator-dns] test-enable
```

# Display test results.

```
[Sysname-remote-ping-administrator-dns] display remote-ping results administrator dns
remote-ping 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-remote-ping-administrator-dns] display remote-ping history administrator dns
remote-ping 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 PoE Configuration

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

- PoE Overview
- PoE Configuration
- PoE Configuration Example

## 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 Switch 4200G

Switch 4200G PWR 24-Port is a PoE-capable switch.

A PoE-capable Switch 4200G 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-capable Switch 4200G to supply power, the PDs need no external power supply.
- If a remote PD has an external power supply, the PoE-capable Switch 4200G and the external power supply will backup each other for the PD.
- Only the 100 Mbps Ethernet electrical ports of the PoE-capable Switch 4200G 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 a PD Disconnection Detection Mode | Optional |
| Configuring PoE Over-Temperature Protection on the Switch | Optional |
| Upgrading the PSE Processing Software 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** *interface-type interface-number* | — |
| 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-capable Switch 4200G 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** *interface-type interface-number* | — |
| Set the maximum output power on the port | **poe max-power** *max-power* | Required<br>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. Switch 4200G supports 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<br>**auto** by default. |
| Enter Ethernet port view | **interface** *interface-type interface-number* | — |
| Se the PoE priority of a port | **poe priority** { **critical** \| **high** \| **low** } | Required<br>**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, Switch 4200G does 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** *interface-type interface-number* | — |
| Set the PoE mode on the port to signal | **poe mode signal** | Optional<br>**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<br>Disabled by default. |

## Configuring a PD Disconnection Detection Mode

To detect the PD connection with PSE, PoE provides two detection modes: AC detection and DC detection. The AC detection mode is energy saving relative to the DC detection mode.

Follow these steps to configure a PD disconnection detection mode

| To do… | Use the command… | Remarks |
|---|---|---|
| Enter system view | **system-view** | — |
| Configure a PD disconnection detection mode | **poe disconnect** { **ac** \| **dc** } | Optional<br>The default PD disconnection detection mode is AC. |

⚠ **Caution**

If you adjust the PD disconnection detection mode when the switch is running, the connected PDs will be powered off. Therefore, be cautious to do so.

## 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<br>Enabled by default. |

**Note**

- When the internal temperature of the switch decreases from X (X>65°C, or X>149°F) to Y (60°C≤Y<65°C, or 140°F≤Y<149°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°C, or X<140°F) to Y (60°C<Y≤65°C, or 140°F<Y≤149°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<br>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.

## Displaying PoE Configuration

| To do… | Use the command… | Remarks |
|---|---|---|
| Display the current PD disconnection detection mode of the switch | **display poe disconnect** | Available in any view |
| Display the PoE status of a specific port or all ports of the switch | **display poe interface** [ *interface-type interface-number* ] | |
| Display the PoE power information of a specific port or all ports of the switch | **display poe interface power** [ *interface-type interface-number* ] | |
| Display the PSE parameters | **display poe powersupply** | |
| Display the status (enabled/disabled) of the PoE over-temperature protection feature on the switch | **display poe temperature-protection** | |

# PoE Configuration Example

## PoE Configuration Example

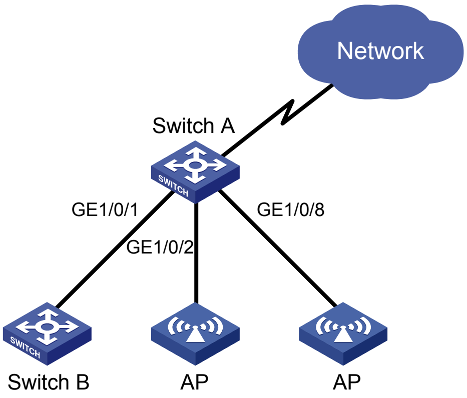
### Network requirements

Switch A is a Switch 4200G supporting PoE, Switch B can be PoE powered.

- The GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 ports of Switch A are connected to Switch B and an AP respectively; the GigabitEthernet 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 GigabitEthernet 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 GigabitEthernet 1/0/1, and set the PoE maximum output power of GigabitEthernet 1/0/1 to 12,000 mW.

```
[SwitchA] interface GigabitEthernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] poe enable
[SwitchA-GigabitEthernet1/0/1] poe max-power 12000
[SwitchA-GigabitEthernet1/0/1] quit
```

# Enable the PoE feature on GigabitEthernet 1/0/2, and set the PoE maximum output power of GigabitEthernet 1/0/2 to 2500 mW.

```
[SwitchA] interface GigabitEthernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] poe enable
[SwitchA-GigabitEthernet1/0/2] poe max-power 2500
[SwitchA-GigabitEthernet1/0/2] quit
```

# Enable the PoE feature on GigabitEthernet 1/0/8, and set the PoE priority of GigabitEthernet 1/0/8 to critical.

```
[SwitchA] interface GigabitEthernet 1/0/8
[SwitchA-GigabitEthernet1/0/8] poe enable
[SwitchA-GigabitEthernet1/0/8] poe priority critical
[SwitchA-GigabitEthernet1/0/8] 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, Switch 4200G provides 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** *profilename* | Required<br>If the PoE file is created, you will enter PoE profile view directly through the command. |

<table>
<tr><th colspan="3">To do…</th><th>Use the command…</th><th>Remarks</th></tr>
<tr><td rowspan="4">Configure the relevant features in PoE profile</td><td colspan="2">Enable the PoE feature on a port</td><td><b>poe enable</b></td><td>Required<br>Disabled by default.</td></tr>
<tr><td colspan="2">Configure PoE mode for Ethernet ports</td><td><b>poe mode</b> { <b>signal</b> | <b>spare</b> }</td><td>Optional<br><b>signal</b> by default.</td></tr>
<tr><td colspan="2">Configure the PoE priority for Ethernet ports</td><td><b>poe priority</b> { <b>critical</b> | <b>high</b> | <b>low</b> }</td><td>Optional<br><b>low</b> by default.</td></tr>
<tr><td colspan="2">Configure the maximum power for Ethernet ports</td><td><b>poe max-power</b> <i>max-power</i></td><td>Optional<br>15,400 mW by default.</td></tr>
<tr><td colspan="3">Quit system view</td><td><b>quit</b></td><td>—</td></tr>
<tr><td rowspan="3">Apply the existing PoE profile to the specified Ethernet port</td><td colspan="2">In system view</td><td><b>apply poe-profile</b> <i>profile-name</i> <b>interface</b> <i>interface-type interface-number</i> [ <b>to</b> <i>interface-type interface-number</i> ]</td><td rowspan="3">Use either approach.</td></tr>
<tr><td rowspan="2">In Ethernet port view</td><td>Enter Ethernet port view</td><td><b>interface</b> <i>interface-type interface-number</i></td></tr>
<tr><td>Apply the existing PoE profile to the port</td><td><b>apply poe-profile</b> <i>profile-name</i></td></tr>
</table>

Note the following during the configuration:

1) 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 Switch 4200G 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.

# 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** *interface-type interface-number* \| **name** *profile-name* } | Available in any view |

# PoE Profile Configuration Example

## PoE Profile Application Example

### Network requirements

Switch A is a Switch 4200G supporting PoE.

GigabitEthernet 1/0/1 through GigabitEthernet 1/0/10 of Switch A are used by users of group A, who have the following requirements:

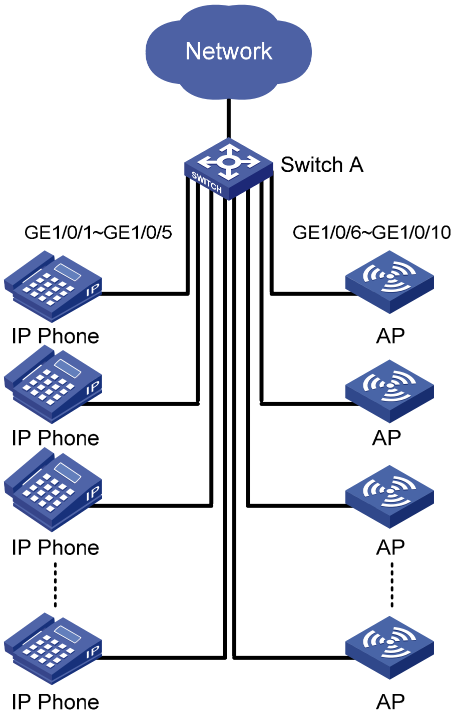
- The PoE function can be enabled on all ports in use.
- Signal mode is used to supply power.
- The PoE priority for GigabitEthernet 1/0/1 through GigabitEthernet 1/0/5 is Critical, whereas the PoE priority for GigabitEthernet 1/0/6 through GigabitEthernet 1/0/10 is High.
- The maximum power for GigabitEthernet 1/0/1 through GigabitEthernet 1/0/5 ports is 3000 mW, whereas the maximum power for GigabitEthernet 1/0/6 through GigabitEthernet 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 GigabitEthernet 1/0/1 through GigabitEthernet 1/0/5;
- Apply PoE profile 2 for GigabitEthernet 1/0/6 through GigabitEthernet 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 GigabitEthernet 1/0/1 through GigabitEthernet 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 GigabitEthernet 1/0/6 through GigabitEthernet 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 GigabitEthernet 1/0/1 through GigabitEthernet 1/0/5 ports.

```
[SwitchA] apply poe-profile Profile1 interface GigabitEthernet1/0/1 to GigabitEthernet1/0/5
```

# Apply the configured Profile 2 to GigabitEthernet 1/0/6 through GigabitEthernet 1/0/10 ports.

```
[SwitchA] apply poe-profile Profile2 interface GigabitEthernet1/0/6 to
GigabitEthernet1/0/10
```

# Table of Contents

# 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:

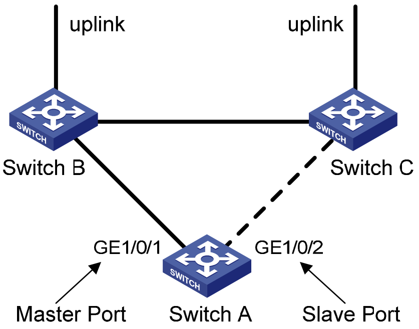
- Active/standby backup for dual-uplink networking
- Simple configuration and operation

### 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, GigabitEthernet 1/0/1 and GigabitEthernet 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 GigabitEthernet 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 GigabitEthernet 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

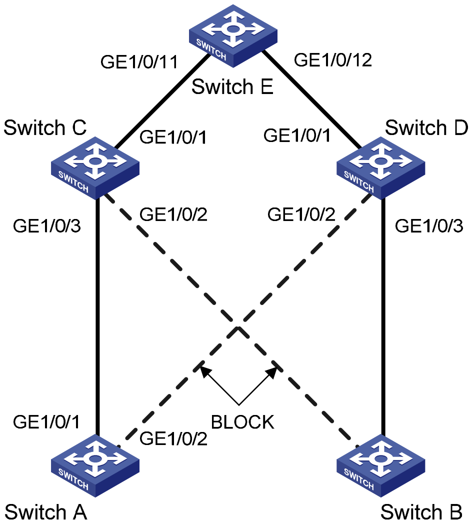
This control VLAN is used for receiving and processing flush messages. When link switching occurs, the devices (Switch B and Switch C in Figure 1-1) receive and process flush messages of this control VLAN, and then refresh MAC forwarding table entries and ARP entries.

**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, GigabitEthernet 1/0/1 on Switch A is active and GigabitEthernet 1/0/2 on Switch A is blocked. When the link connected to GigabitEthernet 1/0/1 fails, GigabitEthernet 1/0/1 is blocked automatically, and the state of GigabitEthernet 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** *group-id* | Required |
| Enable the function of sending flush messages in the specified control VLAN | | **flush enable control-vlan** *vlan-id* | Required<br>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** *interface-type interface-number* { **master** \| **slave** } | Required<br>Use either approach |
| | Ethernet port view | **quit** | |
| | | **interface** *interface-type interface-number* | |
| | | **port smart-link group** *group-id* { **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** *group-id* | Required |
| Configure a link aggregation group as a member of the smart link group | **link-aggregation group** *group-id* { **master** \| **slave** } | Optional |

| To do… | Use the command… | Remarks |
|---|---|---|
| Enable the function of sending flush messages in the specified control VLAN | **flush enable control-vlan** *vlan-id* | Optional<br>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 GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3 of Switch C, GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3 of Switch D, and GigabitEthernet 1/0/11 and GigabitEthernet 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** *vlan-id* **port** *interface-type interface-number* [ **to** *interface-type interface-number* ] | Required, use either approach.<br>By default, no control VLAN for receiving flush messages is specified. |
| | Ethernet port view | **interface** *interface-type interface-number* | |
| | | **smart-link flush enable control-vlan** *vlan-id* | |

## 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) 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.

6) When you copy a port, the smart link/monitor link group member information configured on the port will not be copied to other ports.

7) 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.

8) If no control VLAN is configured for flush message processing, the device will forward received flush messages without processing them.

9) 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.

10) 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.

11) 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** { *group-id* \| **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

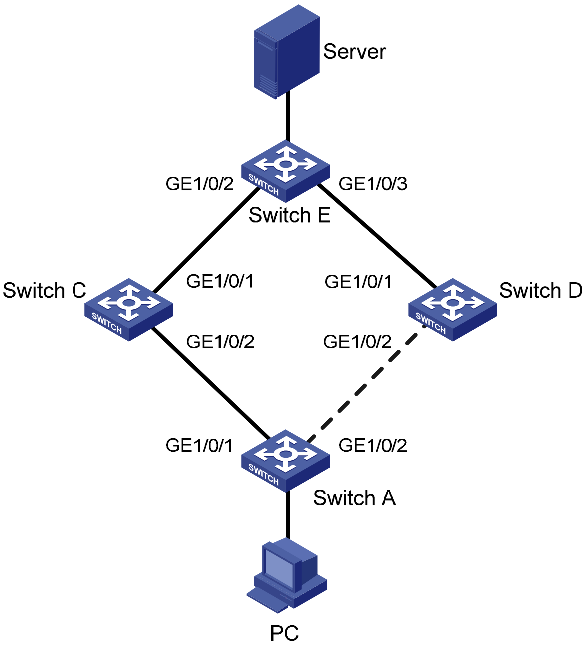
## Implementing Link Redundancy Backup

### Network requirements

As shown in Figure 1-3, Switch A is an 3Com S4200G 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 GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2.

```
[SwitchA] interface GigabitEthernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] stp disable
[SwitchA-GigabitEthernet1/0/1] quit
[SwitchA] interface GigabitEthernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] stp disable
```

# Return to system view.

```
[SwitchA-GigabitEthernet1/0/2] quit
```

# Create smart link group 1 and enter the corresponding smart link group view.

```
[SwitchA] smart-link group 1
```

# Configure GigabitEthernet 1/0/1 as the master port and GigabitEthernet 1/0/2 as the slave port for smart link group 1.

```
[SwitchA-smlk-group1] port GigabitEthernet 1/0/1 master
[SwitchA-smlk-group1] port GigabitEthernet 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 GigabitEthernet 1/0/2.

```
<SwitchC> smart-link flush enable control-vlan 1 port GigabitEthernet 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 GigabitEthernet 1/0/2.

```
[SwitchD] smart-link flush enable control-vlan 1 port GigabitEthernet 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 GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3.

```
[SwitchE] smart-link flush enable control-vlan 1 port GigabitEthernet 1/0/2 to
GigabitEthernet 1/0/3
```

# 2 Monitor Link Configuration

When configuring Monitor Link, go to these sections for information you are interested in:

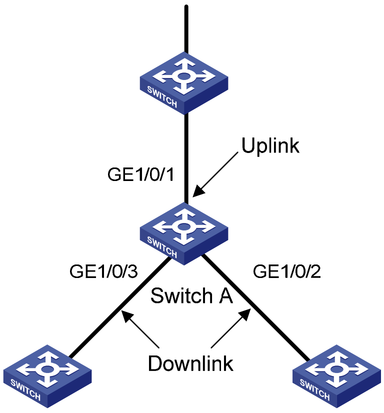
- Introduction to Monitor Link
- Configuring Monitor Link
- Displaying Monitor Link Configuration
- Monitor Link Configuration Example

## 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.

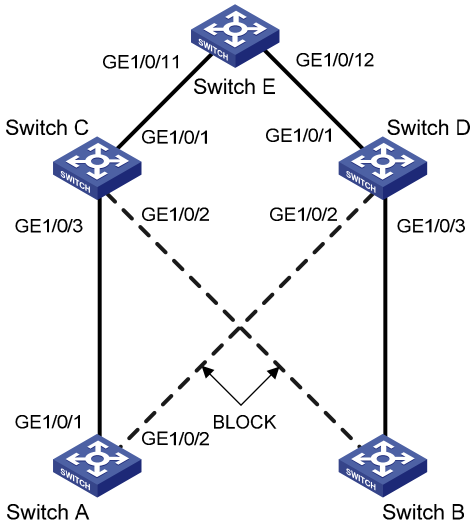
**Figure 2-1** Network diagram for a monitor link group implementation



As shown in Figure 2-1, the monitor link group configured on the device Switch A consists of an uplink port (GigabitEthernet 1/0/1) and two downlink ports (GigabitEthernet 1/0/2 and GigabitEthernet 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 GigabitEthernet 1/0/1 is the uplink port, while GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3 are the downlink ports. Switch A is configured with a smart link group, where GigabitEthernet 1/0/1 is the master port and GigabitEthernet 1/0/2 is the slave port.

- If Switch C is not configured with monitor link group, when the link for the uplink port GigabitEthernet 1/0/1 on Switch C fails, the links in the smart link group are not switched because the link for the master port GigabitEthernet 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 GigabitEthernet 1/0/1.
- If Switch C is configured with monitor link group and monitor link group detects that the link for the uplink port GigabitEthernet 1/0/1 fails, all the downlink ports in the group are shut down; therefore, GigabitEthernet 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 GigabitEthernet 1/0/1. Then, Smart Link immediately activates the slave port GigabitEthernet 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** *group-id* | 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** *group-id* | — |
| 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** *group-id* **uplink** | Required<br>Use any of the three approaches |
| | Configure the specified smart link group as the uplink port of the monitor link group | **smart-link group** *group-id* **uplink** | |

| To do… | | | Use the command… | Remarks |
|---|---|---|---|---|
| | Configure the specified Ethernet port as the uplink port of the monitor link group | Monitor link group view | **port** *interface-type interface-number* **uplink** | |
| | | Ethernet port view | **quit** | |
| | | | **interface** *interface-type interface-number* | |
| | | | **port monitor-link group** *group-id* **uplink** | |

## 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** *group-id* | 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** *group-id* **downlink** | Required<br>Use either approach |
| | Configure the specified Ethernet port as a downlink port of the monitor link group | Monitor link group view | **port** *interface-type interface-number* **downlink** | |
| | | Ethernet port view | **quit** | |
| | | | **interface** *interface-type interface-number* | |
| | | | **port monitor-link group** *group-id* **downlink** | |

⚠ 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 remote 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** { *group-id* \| **all** } | Available in any view. |

# Monitor Link Configuration Example

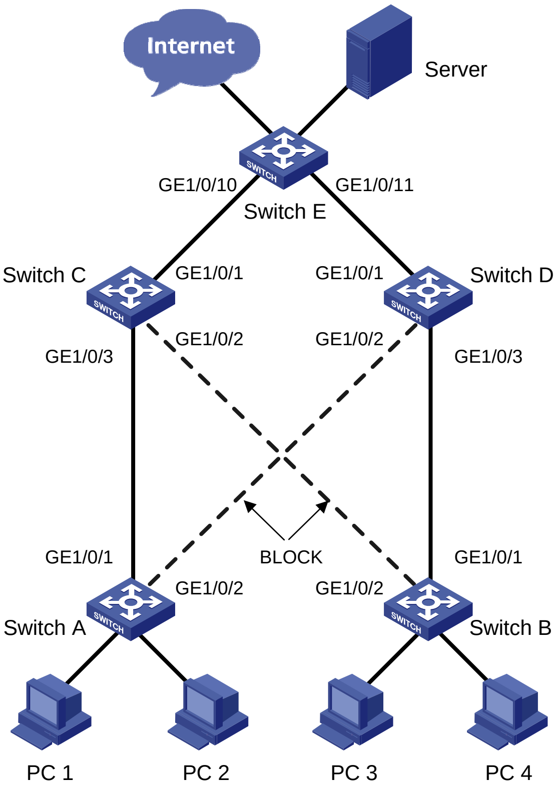
## Implementing Collaboration Between Smart Link and Monitor Link

### 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 GigabitEthernet1/0/1 and GigabitEthernet1/0/2.

```
[SwitchA] interface GigabitEthernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] stp disable
[SwitchA-GigabitEthernet1/0/1] quit
[SwitchA] interface GigabitEthernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] stp disable
```

# Return to system view.

```
[SwitchA-GigabitEthernet1/0/2] quit
```

# Create smart link group 1 and enter smart link group view.

```
[SwitchA] smart-link group 1
```

# Configure GigabitEthernet 1/0/1 as the master port of the smart link group and GigabitEthernet 1/0/2 as the slave port.

```
[SwitchA-smlk-group1] port GigabitEthernet 1/0/1 master
[SwitchA-smlk-group1] port GigabitEthernet 1/0/2 slave
```

# Configure to send flush messages in VLAN 1.

```
[SwitchA-smlk-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 GigabitEthernet 1/0/1 as the uplink port of the monitor link group and GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3 as the downlink ports.

```
[SwitchC-mtlk-group1] port GigabitEthernet 1/0/1 uplink
[SwitchC-mtlk-group1] port GigabitEthernet 1/0/2 downlink
[SwitchC-mtlk-group1] port GigabitEthernet 1/0/3 downlink
```

# Return to system view. Enable the function of processing flush messages received from VLAN 1 on GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3.

```
[SwitchC-mtlk-group1] quit
[SwitchC] smart-link flush enable control-vlan 1 port GigabitEthernet 1/0/2 to GigabitEthernet 1/0/3
```

3) Enable the function of processing flush messages received from VLAN 1 on GigabitEthernet 1/0/10 and GigabitEthernet 1/0/11 of Switch E.

# Enter system view.

```
<SwitchE> system-view
```

# Enable the function of processing flush messages received from VLAN 1 on GigabitEthernet 1/0/10 and GigabitEthernet 1/0/11.

```
[SwitchE] smart-link flush enable control-vlan 1 port GigabitEthernet 1/0/10 to GigabitEthernet 1/0/11
```

# Table of Contents

# 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.
- 3com Switch 4200G supports IPv6 management features, but do not support IPv6 forwarding and related features.

## IPv6 Overview

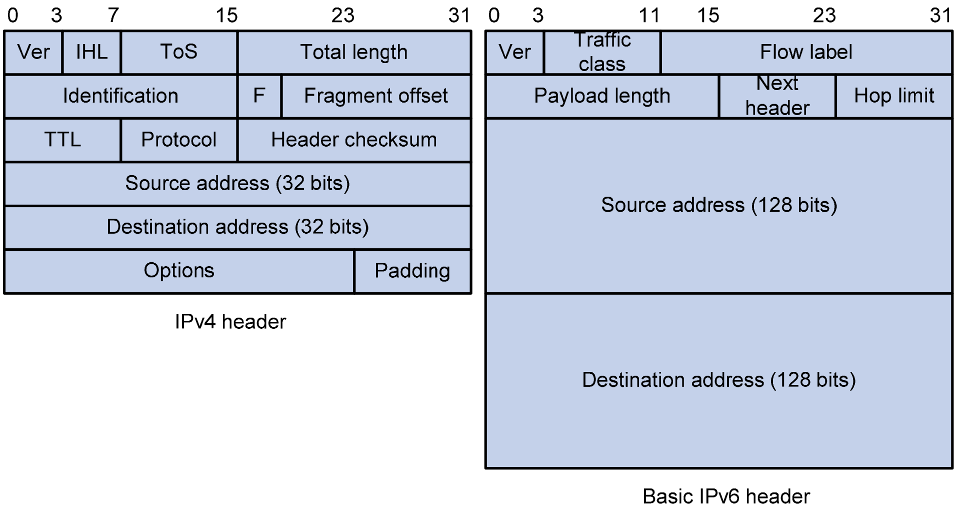
Internet Protocol Version 6 (IPv6), also called IP next generation (IPng), was designed by the Internet Engineering Task Force (IETF) as the successor to Internet Protocol Version 4 (IPv4). The significant difference between IPv6 and IPv4 is that IPv6 increases the IP address size from 32 bits to 128 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.

**Figure 1-1** Comparison between IPv4 header format and IPv6 header format



IPv4 header

Basic IPv6 header

### Adequate address space

The source IPv6 address and the destination IPv6 address are both 128 bits (16 bytes) long. IPv6 can provide 3.4 x $10^{38}$ addresses to completely meet the requirements of hierarchical address division as well as allocation of public and private addresses.

### Hierarchical address structure

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.

### Automatic address configuration

To simplify the host configuration, IPv6 supports stateful address configuration and stateless address configuration.

- Stateful address configuration means that a host acquires an IPv6 address and related information from the server (for example, DHCP server).
- Stateless address configuration means that the host automatically configures an IPv6 address and related information based on its own link-layer address and the prefix information issued by the router.

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.

### Built-in security

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.

### Support for QoS

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:

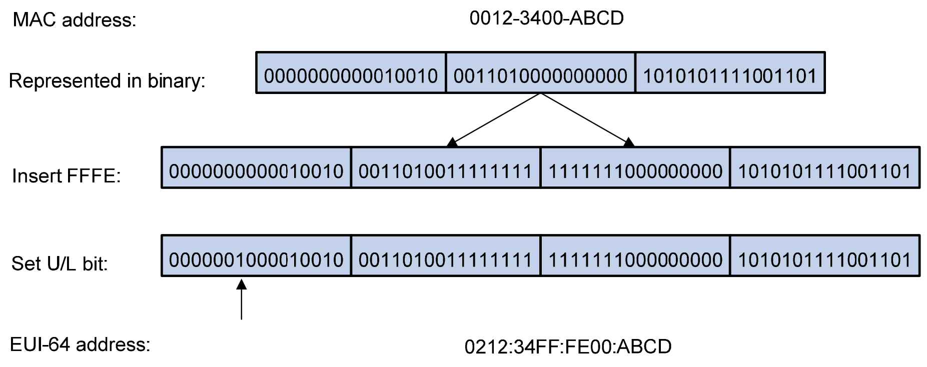
FF02:0:0:0:0:1:FFXX:XXXX

Where, FF02:0:0:0:0:1: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**

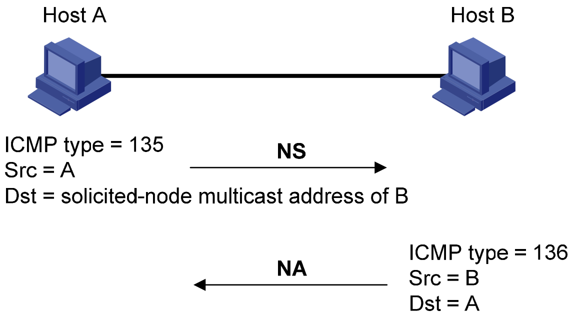
- 3com Switch 4200G does not support the RS, RA, or Redirect message.
- Of the above mentioned IPv6 NDP functions, 3com Switch 4200G supports the following three functions: address resolution, neighbor unreachability detection, and duplicate address detection. The subsequent sections present a detailed 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

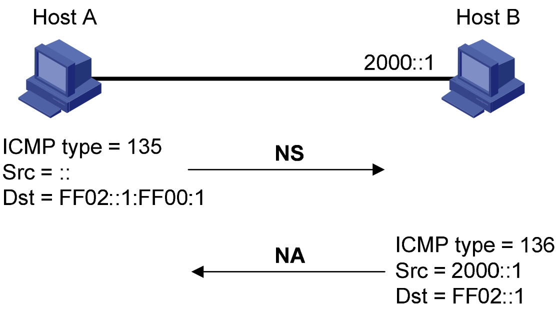
After node A acquires the link-layer address of its neighbor node B, node A can verify whether node B is reachable according to NS and NA messages.

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** *interface-type interface-number* | — |

| To do... | | Use the command... | Remarks |
|---|---|---|---|
| Configure an IPv6 global unicast address or site-local address | Manually assign an IPv6 address | **ipv6 address** { *ipv6-address prefix-length* **\|** *ipv6-address***/***prefix-length* } | Use either command<br>By default, no site-local address or global unicast address is configured for an interface.<br>Note that the prefix specified by the *prefix-length* argument in an EUI-64 address cannot exceed 64 bits in length. |
| | Adopt the EUI-64 format to form an IPv6 address | **ipv6 address** *ipv6-address*/*prefix-length* **eui-64** | |
| Configure an IPv6 link-local address | Automatically generate a link-local address | **ipv6 address auto link-local** | Optional<br>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** *ipv6-address* **link-local** | |

**Note**

- IPv6 unicast addresses can be configured for only one VLAN interface on a 3com switch 4200G. 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** *ipv6-address mac-address* { *vlan-id port-type port-number* \| **interface** *interface-type interface-number* } | 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** *interface-type interface-number* | — |
| Configure the maximum number of neighbors dynamically learned by an interface | **ipv6 neighbors max-learning-num** *number* | Optional<br>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** *interface-type interface-number* | — |
| Configure the attempts to send an NS message for duplicate address detection | **ipv6 nd dad attempts** *value* | Optional<br>1 by default. When the *value* 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** *interface-type interface-number* | — |
| Specify the NS interval | **ipv6 nd ns retrans-timer** *value* | Optional<br>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** *interface-type interface-number* | — |
| Configure the neighbor reachable timeout time | **ipv6 nd nud reachable-time** *value* | Optional<br>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** | — |

| To do… | Use the command… | Remarks |
|---|---|---|
| Configure a static IPv6 route | **ipv6 route-static** *ipv6-address prefix-length* [ *interface-type interface-number*] *nexthop-address* | Required<br>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** *wait-time* | Optional<br>675 seconds by default. |
| Set the synwait timer of IPv6 TCP packets | **tcp ipv6 timer syn-timeout** *wait-time* | Optional<br>75 seconds by default. |
| Configure the size of IPv6 TCP receiving/sending buffer | **tcp ipv6 window size** | Optional<br>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<br>By default, the capacity of a token bucket is 10 and the update period to 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<br>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<br>Disabled by default. |
| Configure an IPv6 DNS server | **dns server ipv6** *ipv6-address* [ *interface-type interface-number* ] | Required<br>If the IPv6 address of the DNS server is a link-local address, the *interface-type* and *interface-number* arguments are required. |
| Configure the domain suffix. | **dns domain** *domain-name* | Required<br>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** [ *interface-type interface-number* \| **brief** ] | |
| Display neighbor information | **display ipv6 neighbors** [ *ipv6-address* \| **all** \| **dynamic** \| **interface** *interface-type interface-number* \| **static** \| **vlan** *vlan-id* ] [ **\|** { **begin** \| **exclude** \| **include** } *regular-expression* ] | |
| Display the total number of neighbor entries satisfying the specified conditions | **display ipv6 neighbors** { **all** \| **dynamic** \| **static** \| **interface** *interface-type interface-number* \| **vlan** *vlan-id* } **count** | |
| Display information about the routing table | **display ipv6 route-table** [ **verbose** ] | |
| Display information related to a specified socket | **display ipv6 socket** [ **socktype** *socket-type* ] [ *task-id socket-id* ] | |

| To do… | Use the command… | Remarks |
|---|---|---|
| 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** *interface-type interface-number* \| **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

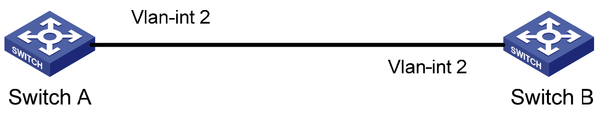
## IPv6 Unicast Address Configuration

### 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 a 3com Switch 4200G 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<br>Available in any view |

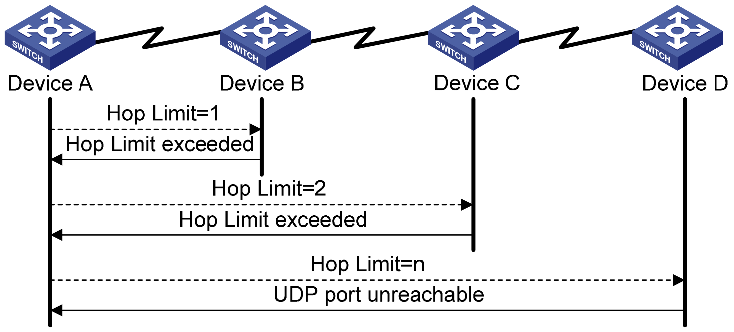
**Caution**

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** *first-ttl* \| **-m** *max-ttl* \| **-p** *port* \| **-q** *packet-num* \| **-w** *timeout* ]* *remote-system* | Required<br>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 *FTP-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** *remote-system* [ **-i** *interface-type interface-number* ] { **get** \| **put** } *source-filename* [ *destination-filename* ] | Required<br>Available in user view |

**Caution**

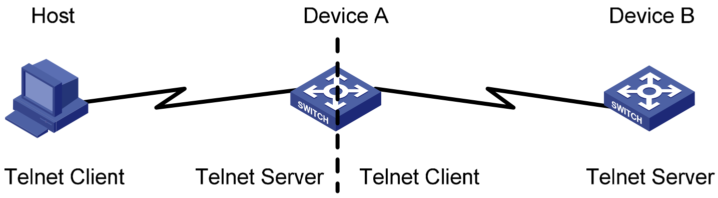
When you use the **tftp ipv6** command to connect to the TFTP server, you must specify the "**–i**" keyword if the destination address is a link-local address.

## 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** *remote-system* [ **-i** *interface-type interface-number* ] [ *port-number* ] | Required<br>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

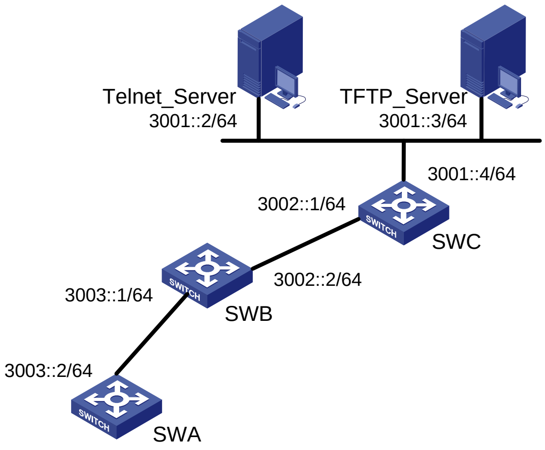
## IPv6 Applications

### Network requirements

In Figure 2-3, SWA, SWB, and SWC are three switches, among which SWA is a 3com switch 4200G, 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> tracert 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 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

## 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, S4200G 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.

**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 |

| Protocol | UDP port number |
|---|---|
| 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<br>Disabled by default. |
| Specify a UDP port number | **udp-helper port** { *port-number* \| **dns** \| **netbios-ds** \| **netbios-ns** \| **tacacs** \| **tftp** \| **time** } | Optional<br>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. |
| Enter VLAN interface view | **interface Vlan-interface** *vlan-id* | — |
| Specify the destination server to which the UDP packets are to be forwarded | **udp-helper server** *ip-address* | Required<br>No destination server is specified by default. |

**Note**

- 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** *vlan-id* ] | Available in any view |

| To do… | Use the command… | Remarks |
|---|---|---|
| Clear statistics about packets forwarded by UDP Helper | **reset udp-helper packet** | Available in user view |

# UDP Helper Configuration Example

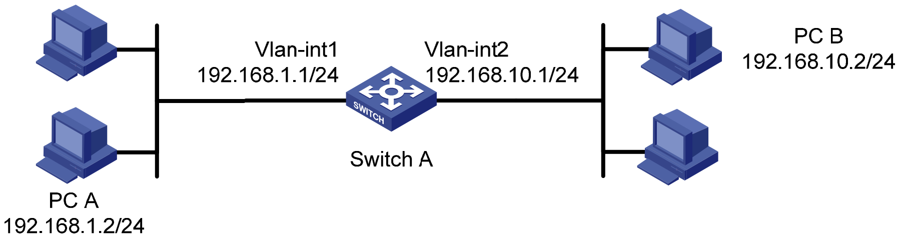
## Cross-Network Computer Search Through UDP Helper

### 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 UDP Helper on Switch A.

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

# Table of Contents

# 1 Access Management Configuration

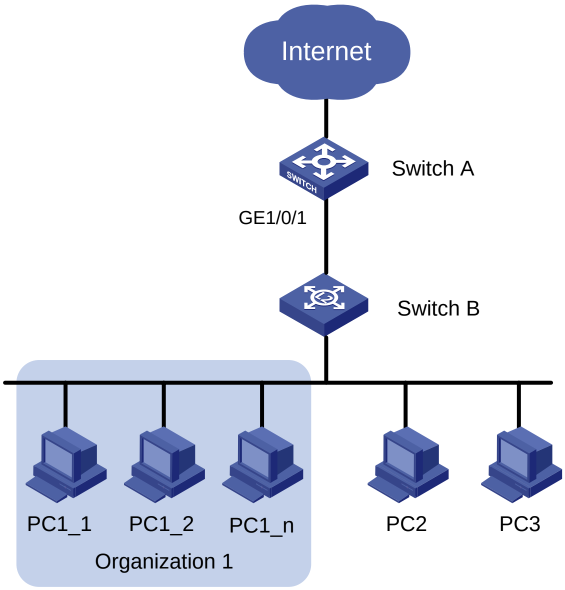
When configuring access management, go to these sections for information you are interested in:

- 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<br>By default, the system disables the access management function. |
| Enable access management trap | **am trap enable** | Required<br>By default, access management trap is disabled |
| Enter Ethernet port view | **interface** *interface-type interface-number* | — |
| Configure the access management IP address pool of the port | **am ip-pool** *address-list* | Required<br>By default, no access management IP address pool is configured. |
| Display current configuration of access management | **display am** [ *interface-list* ] | 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

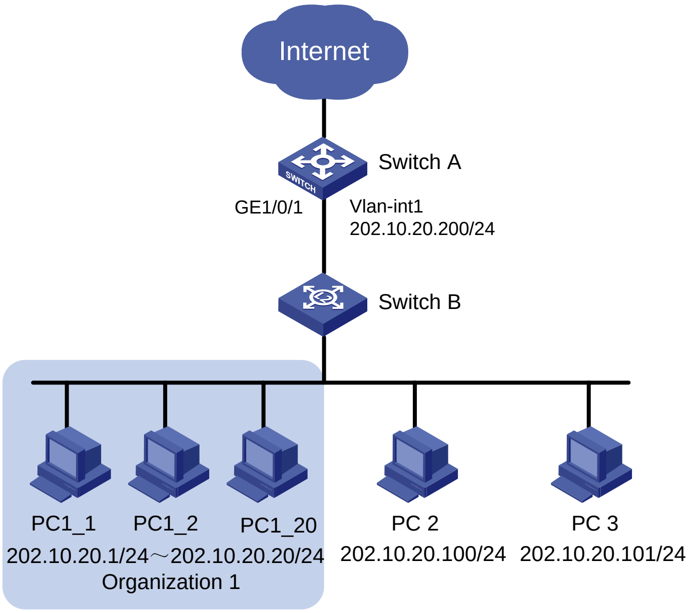
### Network requirements

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 GigabitEthernet 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 GigabitEthernet 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 GigabitEthernet 1/0/1.

```
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] am ip-pool 202.10.20.1 20
```

## Combining Access Management with Port Isolation

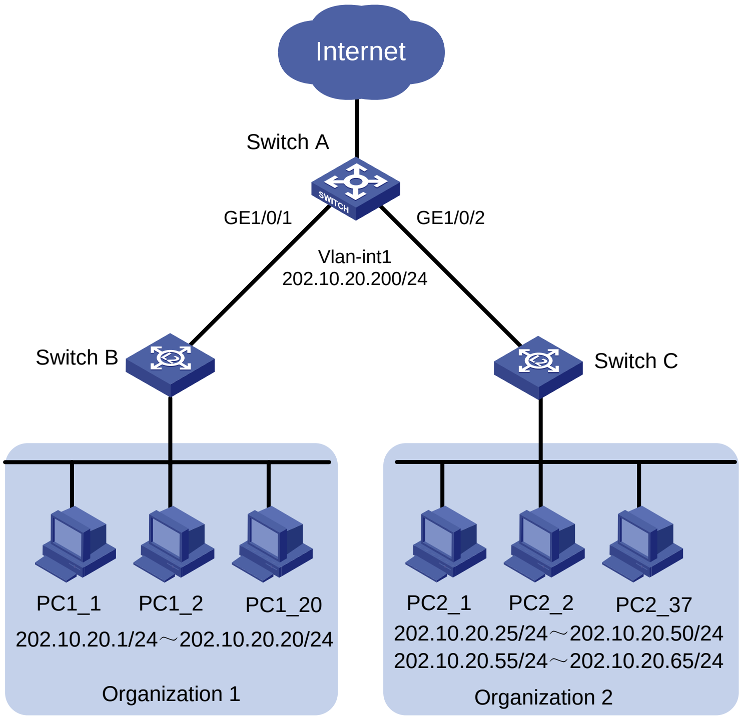
### Network requirements

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 GigabitEthernet 1/0/1 of Switch A.
- Allow the PCs of Organization 2 to access the external network through GigabitEthernet 1/0/2 of Switch A.
- GigabitEthernet 1/0/1 and GigabitEthernet 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 GigabitEthernet 1/0/1.

```
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] am ip-pool 202.10.20.1 20
```

# Add GigabitEthernet 1/0/1 to the port isolation group.

```
[Sysname-GigabitEthernet1/0/1] port isolate
[Sysname-GigabitEthernet1/0/1] quit
```

# Configure the access management IP address pool on GigabitEthernet 1/0/2.

```
[Sysname] interface GigabitEthernet 1/0/2
[Sysname-GigabitEthernet1/0/2] am ip-pool 202.10.20.25 26 202.10.20.55 11
```

# Add GigabitEthernet 1/0/2 to the port isolation group.

```
[Sysname-GigabitEthernet1/0/2] port isolate
[Sysname-GigabitEthernet1/0/2] quit
```

# Table of Contents

# Appendix A Acronyms

| | |
|---|---|
| A | |
| AAA | Authentication, Authorization and Accounting |
| ABR | Area Border Router |
| ACL | Access Control List |
| ARP | Address Resolution Protocol |
| AS | Autonomous System |
| ASBR | Autonomous System Border Router |
| B | |
| BDR | Backup Designated Router |
| C | |
| CAR | Committed Access Rate |
| CLI | Command Line Interface |
| CoS | Class of Service |
| D | |
| DHCP | Dynamic Host Configuration Protocol |
| DR | Designated Router |
| D-V | Distance Vector Routing Algorithm |
| E | |
| EGP | Exterior Gateway Protocol |
| F | |
| FTP | File Transfer Protocol |
| G | |
| GARP | Generic Attribute Registration Protocol |
| GE | Gigabit Ethernet |
| GVRP | GARP VLAN Registration Protocol |
| GMRP | GARP Multicast Registration Protocol |
| H | |
| HGMP | Huawei Group Management Protocol |
| I | |
| IAB | Internet Architecture Board |
| ICMP | Internet Control Message Protocol |
| IGMP | Internet Group Management Protocol |
| IGP | Interior Gateway Protocol |
| IP | Internet Protocol |

| | |
|---|---|
| L | |
| LSA | Link State Advertisement |
| LSDB | Link State DataBase |
| M | |
| MAC | Medium Access Control |
| MIB | Management Information Base |
| N | |
| NBMA | Non Broadcast MultiAccess |
| NIC | Network Information Center |
| NMS | Network Management System |
| NVRAM | Nonvolatile RAM |
| O | |
| OSPF | Open Shortest Path First |
| P | |
| PIM | Protocol Independent Multicast |
| PIM-DM | Protocol Independent Multicast-Dense Mode |
| PIM-SM | Protocol Independent Multicast-Sparse Mode |
| PoE | Power over Ethernet |
| Q | |
| QoS | Quality of Service |
| R | |
| RIP | Routing Information Protocol |
| RMON | Remote Network Monitoring |
| RSTP | Rapid Spanning Tree Protocol |
| S | |
| SNMP | Simple Network Management Protocol |
| SP | Strict Priority |
| STP | Spanning Tree Protocol |
| T | |
| TCP/IP | Transmission Control Protocol/ Internet Protocol |
| TFTP | Trivial File Transfer Protocol |
| ToS | Type of Service |
| TTL | Time To Live |
| U | |
| UDP | User Datagram Protocol |
| V | |
| VLAN | Virtual LAN |

| | |
|---|---|
| VOD | Video On Demand |
| W | |
| WRR | Weighted Round Robin |
| X | |
| XID | eXchange Identification |
| XRN | eXpandable Resilient Networking |