



3Com[®] Switch 4210 Family Configuration Guide

Switch 4210 PWR 9-port
Switch 4210 PWR 18-port
Switch 4210 PWR 26-port

Switch 4210 9-port
Switch 4210 18-port
Switch 4210 26-port

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

Copyright © 2006-2007, 3Com Corporation. All rights reserved. No part of this documentation may be reproduced in any form or by any means or used to make any derivative work (such as translation, transformation, or adaptation) without written permission from 3Com Corporation.

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

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

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

UNITED STATES GOVERNMENT LEGEND

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

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

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

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

Cisco is a registered trademark of Cisco Systems, Inc.

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

Aegis is a registered trademark of Aegis Group PLC.

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

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

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

ENVIRONMENTAL STATEMENT

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

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

Conserving energy, materials and natural resources in all operations.

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

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

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

Improving our environmental record on a continual basis.

End of Life Statement

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

Regulated Materials Statement

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

CONTENTS

ABOUT THIS GUIDE

- Conventions 9
- Related Documentation 10

1 CLI CONFIGURATION

- Introduction to the CLI 11
- Command Hierarchy 11
- CLI Views 14
- CLI Features 16

2 LOGGING INTO AN ETHERNET SWITCH

- Supported User Interfaces 21
- Logging in through the Console Port 23
- Logging in through Telnet 37
- Telnet Configuration with Authentication Mode Being Scheme 44
- Logging in Using a Modem 52
- Logging in through the Web-based Network Management System 56
- Managing from an NMS 59
- User Control 60

3 CONFIGURATION FILE MANAGEMENT

- Introduction to Configuration File 67
- Management of Configuration File 68

4 VLAN OVERVIEW

- VLAN Overview 73
- Port-Based VLAN 76

5 VLAN CONFIGURATION

- VLAN Configuration 77
- Configuring a Port-Based VLAN 79

6 MANAGING THE VLAN

- VLAN Overview 83
- Configuring VLAN Management 84
- Displaying and Maintaining management VLAN configuration 86

7 IP ADDRESSING CONFIGURATION

- IP Addressing Overview 87
- Configuring IP Addresses 89
- Displaying IP Addressing Configuration 90
- IP Address Configuration Examples 90

8 IP PERFORMANCE CONFIGURATION

- IP Performance Overview 91
- Configuring IP Performance 91
- Displaying and Maintaining IP Performance Configuration 93

9 PORT BASIC CONFIGURATION

- Ethernet Port Overview 95
- Ethernet Port Configuration 96
- Configuring the Interval to Perform Statistical Analysis on Port Traffic 102
- Disabling Up/Down Log Output on a Port 103
- Ethernet Port Configuration Example 104
- Troubleshooting Ethernet Port Configuration 105

10 LINK AGGREGATION CONFIGURATION

- Overview 107
- Link Aggregation Classification 108
- Aggregation Group Categories 110
- Link Aggregation Configuration 111
- Displaying and Maintaining Link Aggregation Configuration 114
- Link Aggregation Configuration Example 114

11 PORT ISOLATION CONFIGURATION

- Port Isolation Overview 117
- Port Isolation Configuration 117
- Displaying Port Isolation Configuration 118
- Port Isolation Configuration Example 118

12 PORT SECURITY CONFIGURATION

- Port Security Overview 121
- Port Security Configuration 124
- Displaying Port Security Configuration 129
- Port Security Configuration Example 129

13 MAC ADDRESS TABLE MANAGEMENT

- Introduction to the MAC Address Table 131
- Managing MAC Address Table 133
- Configuring MAC Address Table Management 134
- Displaying MAC Address Table Information 136

Configuration Example 137

14 MSTP CONFIGURATION

STP Overview 139
MSTP Overview 147
Configuring Root Bridge 153
Configuring Leaf Nodes 167
Performing mCheck Operation 172
Configuring Guard Functions 173
Configuring Digest Snooping 177
Configuring Rapid Transition 178
STP Maintenance Configuration 181
Enabling Trap Messages Conforming to 802.1d Standard 181
Displaying and Maintaining MSTP 182
MSTP Configuration Example 182

15 MULTICAST OVERVIEW

Multicast Overview 185
Multicast Models 189
Multicast Architecture 189
Multicast Packet Forwarding Mechanism 195

16 IGMP SNOOPING CONFIGURATION

IGMP Snooping Overview 197
IGMP Snooping Configuration 200
Displaying and Maintaining IGMP Snooping 207
IGMP Snooping Configuration Examples 208
Troubleshooting IGMP Snooping 210
Configuring Dropping Unknown Multicast Packets 210

17 802.1X CONFIGURATION

Introduction to 802.1x 211
802.1x Configuration 223
Basic 802.1x Configuration 223
Advanced 802.1x Configuration 226
Displaying and Debugging 802.1x 229
Configuration Example 229

18 HABP CONFIGURATION

Introduction to HABP 233
HABP Server Configuration 233
HABP Client Configuration 234
Displaying HABP 234

19 SYSTEM-GUARD CONFIGURATION

- System-Guard Configuration 235
- Displaying and Maintaining the System-Guard Function 236

20 AAA OVERVIEW

- Introduction to AAA 237
- Introduction to AAA Services 238

21 AAA CONFIGURATION

- AAA Configuration Task List 245
- RADIUS Configuration Task List 251
- Displaying and Maintaining AAA 262
- AAA Configuration Examples 263
- Troubleshooting AAA 266

22 MAC AUTHENTICATION CONFIGURATION

- MAC Authentication Overview 269
- Related Concepts 270
- Configuring Basic MAC Authentication Functions 270
- MAC Address Authentication Enhanced Function Configuration 271
- Displaying and Debugging MAC Authentication 274
- MAC Authentication Configuration Example 275

23 ARP CONFIGURATION

- Introduction to ARP 277
- ARP Configuration 279
- Displaying and Debugging ARP 279
- ARP Configuration Example 280

24 DHCP OVERVIEW

- Introduction to DHCP 281
- DHCP IP Address Assignment 281
- DHCP Packet Format 283
- Protocol Specification 284

25 DHCP SNOOPING CONFIGURATION

- Introduction to DHCP Snooping 285
- DHCP Snooping Configuration 286
- DHCP Snooping Configuration Example 286

26 DHCP/BOOTP CLIENT CONFIGURATION

- Introduction to DHCP Client 287
- Introduction to BOOTP Client 287

Configuring a DHCP/BOOTP Client	287
Displaying DHCP/BOOTP Client Configuration	288
DHCP Client Configuration Example	288

27 ACL CONFIGURATION

ACL Overview	291
ACL Configuration	293
Example for Upper-layer Software Referencing ACLs	297

28 QoS CONFIGURATION

Overview	299
QoS Supported By Switch 4210 Family	300
QoS Configuration	307

29 MIRRORING CONFIGURATION

Mirroring Overview	313
Mirroring Configuration Example	314

30 CLUSTER

Cluster Overview	317
Cluster Configuration Tasks	325
Displaying and Maintaining Cluster Configuration	333
Cluster Configuration Example	333

31 PoE CONFIGURATION

PoE Overview	339
PoE Configuration	340
PoE Configuration Example	344

32 PoE PROFILE CONFIGURATION

Introduction to PoE Profile	347
PoE Profile Configuration	347
Displaying PoE Profile Configuration	348
PoE Profile Configuration Example	349

33 SNMP CONFIGURATION

SNMP Overview	351
Configuring Basic SNMP Functions	353
Configuring Trap Parameters	355
Enabling Logging for Network Management	357
Displaying SNMP	357
SNMP Configuration Examples	357

34 RMON CONFIGURATION

- Introduction to RMON 361
- RMON Configuration 363
- Displaying RMON 364
- RMON Configuration Examples 364

35 NTP CONFIGURATION

- Introduction to NTP 367
- NTP Configuration Tasks 371
- Configuring NTP Implementation Modes 372
- Configuring Access Control Right 375
- Configuring NTP Authentication 376
- Configuring Optional NTP Parameters 378
- Displaying NTP Configuration 379
- Configuration Example 379

36 SSH CONFIGURATION

- SSH Overview 387
- Configuring the SSH Server 390
- Configuring the SSH Client 396
- Displaying SSH Configuration 406
- SSH Configuration Examples 406

37 FILE SYSTEM MANAGEMENT CONFIGURATION

- File System Configuration 423
- File Attribute Configuration 426

38 FTP AND SFTP CONFIGURATION

- Introduction to FTP and SFTP 429
- FTP Configuration 430
- SFTP Configuration 438

39 TFTP CONFIGURATION

- Introduction to TFTP 445
- TFTP Configuration 446

40 INFORMATION CENTER

- Information Center Overview 451
- Information Center Configuration 456
- Displaying and Maintaining Information Center 462
- Information Center Configuration Examples 463

41 BOOT ROM AND HOST SOFTWARE LOADING

- Introduction to Loading Approaches 469
- Local Boot ROM and Software Loading 469
- Remote Boot ROM and Software Loading 478

42 BASIC SYSTEM CONFIGURATION AND DEBUGGING

- Basic System Configuration 483
- Displaying the System Status 484
- Debugging the System 484

43 NETWORK CONNECTIVITY TEST

- Network Connectivity Test 487

44 DEVICE MANAGEMENT

- Device Management Configuration 489
- Displaying the Device Management Configuration 491
- Remote Switch APP Upgrade Configuration Example 491

45 REMOTE-PING CONFIGURATION

- Remote-Ping Overview 495
- Remote-Ping Configuration 498
- Remote-Ping Configuration Example 511

46 IPV6 MANGEMENT CONFIGURATION

- IPv6 Overview 525
- IPv6 Configuration Task List 532
- IPv6 Configuration Example 540

47 IPV6 APPLICATION CONFIGURATION

- Introduction to IPv6 Application 543
- IPv6 Application Configuration 543
- IPv6 Application Configuration Example 546
- Troubleshooting IPv6 Application 547

48 DNS CONFIGURATION

- DNS Overview 549
- Configuring Domain Name Resolution 551
- Displaying and Maintaining DNS 551
- DNS Configuration Example 552
- Troubleshooting DNS 554

49 PASSWORD CONTROL CONFIGURATION OPERATIONS

- Introduction to Password Control Configuration 555

Password Control Configuration	556
Displaying Password Control	563
Password Control Configuration Example	564

ABOUT THIS GUIDE

This guide describes the 3Com® Switch 4210 and how to install hardware, configure and boot software, and maintain software and hardware. This guide also provides troubleshooting and support information for your switch.

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



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

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

Conventions

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

Table 1 Notice Icons

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

Table 2 lists text conventions that are used throughout this guide.

Table 2 Text Conventions

Convention	Description
Screen displays	This typeface represents information as it appears on the screen.
Keyboard key names	If you must press two or more keys simultaneously, the key names are linked with a plus sign (+), for example: Press Ctrl+Alt+Del
The words "enter" and "type"	When you see the word "enter" in this guide, you must type something, and then press Return or Enter. Do not press Return or Enter when an instruction simply says "type."

Table 2 Text Conventions

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

Related Documentation

The following manuals offer additional information necessary for managing your Switch 4210:

- *Switch 4210 Command Reference Guide* — Provides detailed descriptions of command line interface (CLI) commands, that you require to manage your Switch 4210.
- *Switch 4210 Configuration Guide*— Describes how to configure your Switch 4210 using the supported protocols and CLI commands.
- *Switch 4210 Release Notes* — Contains the latest information about your product. If information in this guide differs from information in the release notes, use the information in the *Release Notes*.

These documents are available in Adobe Acrobat Reader Portable Document Format (PDF) on the CD-ROM that accompanies your router or on the 3Com World Wide Web site:

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

1

CLI CONFIGURATION

Introduction to the CLI

A command line interface (CLI) is a user interface to interact with a switch. Through the CLI on a switch, you can enter commands to configure the switch and check output information to verify the configuration. Each Switch 4210 provides an easy-to-use CLI and a set of configuration commands for configuring and managing your switch.

The CLI on the Switch 4210 Family provides the following features:

- **Hierarchical command protection:** You can control the commands that specific users can execute to prevent unauthorized users from configuring the switch.
- **Online help:** Users can gain online help at any time by entering a question mark (?) at the command line prompt.
- **Debugging:** Detailed debugging information is provided to help diagnose and locate network problems.
- **Command history function:** This feature enables users to check most recently executed commands and makes it easier to execute those commands again.
- **Partial matching of commands:** The system allows you to enter partially matching text to search for commands. This allows you to execute a command by entering partially-spelled command keywords as long as the system can uniquely identify the keywords entered.

Command Hierarchy

The Switch 4210 uses hierarchical command protection for command lines, to prevent users with fewer access rights from using higher-level commands to change the switch's configuration. Based on user privilege, commands are classified in four levels:

- **Visitor level (level 0):** Commands at this level are mainly used to diagnose the network, and cannot be saved in a 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, They cannot be saved in a configuration file. Such commands include **debugging** and **terminal**.
- **System level (level 2):** Commands at this level are mainly used to configure services and include routing and network layer commands. These commands can be used to provide network services directly.
- **Manage level (level 3):** Commands at this level are associated with the basic operation 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 default, the Console user (a user who logs into the switch through the Console port) is a level-3 user and Telnet users are level-0 users.

Switching User Levels

After logging into the switch, users can change their current user levels through a command. Note that:

- If a switching password is set for a specific user level by the `super password` command, all users must enter the password correctly when they switch from lower user levels to this level (if a wrong password is entered, they will remain at their original levels).
- If no switching password is set for a specific user level, the Console user can directly switch to the level, while the Telnet users at lower levels will fail to switch to the level (they will remain at their original levels) and the information like the following will be displayed: % Password is not set.

Adopting super password authentication for user level switching

Table 1 Set a password for use level switching

Operation	Command	Remarks
Enter system view	system-view	-
Set the super password for user level switching	super password [level] {cipher simple} password	Required By default, the super password is not set.

Switching to a specific user level

Table 2 Switch to a specific user level

Operation	Command	Remarks
Switch to a specified user level	super [level]	Required Execute this command in user view.



- If no user level is specified in the `super password` command or the `super` command, level 3 is used by default.
- For security purposes, 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, the user level is 0. The network administrator can allow general users to switch to level 3 so that they are able to configure the switch.

A level 3 user sets a switching password for user level 3.

```
<4210> system-view
[4210] super password level 3 simple 123
```

A general user telnets to the switch, and then uses the `set password` to switch to user level 3.

```

<4210> 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.
<4210> 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

```

Setting the Level of a Command in a Specific View

Setting the level of a command in a specific view

Commands fall into four levels:

- visit (level 0)
- monitor (level 1)
- system (level 2)
- manage (level 3).

By using the following command, the administrator can change the level of a command in a specific view as required.

Table 3 Set the level of a command in a specific view

Operation	Command	Remarks
Enter system view	system-view	-
Configure the level of a command in a specific view	command-privilege level level view view command	Required



CAUTION:

- 3Com recommends that you do not to change the level of a command arbitrarily, for it may cause problems when operating and maintaining the switch.
- When you change the level of a command with multiple keywords, you should input the keywords one by one in the order they appear in the command syntax. Otherwise, your configuration will not take effect.

Configuration example

The network administrator (a level 3 user) changes 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. (By default, only level 3 users can change the level of a command.)

```

<4210> system-view
[4210] command-privilege level 0 view shell tftp
[4210] command-privilege level 0 view shell tftp 192.168.0.1
[4210] command-privilege level 0 view shell tftp 192.168.0.1 get
[4210] command-privilege level 0 view shell tftp 192.168.0.1 get bootrom.btm

```

This allows general Telnet users to use the **tftp get** command to download file bootrom.btm and other files from TFTP server 192.168.0.1 and other TFTP servers.

CLI Views

CLI views are designed for different configuration tasks. When you first log into the switch, you are in user view, where you can perform simple operations such as checking the operation status and statistics information of the switch. To enter the system view, execute the **system-view** command.

Table 4 lists the CLI views provided by the Switch 4210 Family, operations that can be performed in each view, and the commands used to enter each view.

Table 4 CLI views

View	Available operation	Prompt example	Enter method	Quit method
User view	Display operation status and statistical information of the switch	<4210>	Enter user view once logging into the switch.	Execute the quit command to log out of the switch.
System view	Configure system parameters	[4210]	Execute the system-view command in user view.	Execute the quit or return command to return to user view.

Table 4 CLI views

View	Available operation	Prompt example	Enter method	Quit method
Ethernet port view	Configure Ethernet port parameters	100 Mbps Ethernet port view: [4210-Ethernet1/0/1] 1000 Mbps Ethernet port view: [4210-GigabitEthernet1/1/1]	Execute the interface ethernet command in system view. Execute the interface gigabitethernet command in system view.	Execute the quit command to return to system view. Execute the return command to return to user view.
VLAN view	Configure VLAN parameters	[4210-vlan1]	Execute the vlan command in system view.	
VLAN interface view	Configure VLAN interface parameters	[4210-Vlan-interface 1]	Execute the interface Vlan-interface command in system view.	
Loopback interface view	Configure loopback interface parameters	[4210-LoopBack0]	Execute the interface loopback command in system view.	
NULL interface view	Configure NULL interface parameters	[4210-NULL0]	Execute the interface null command in system view.	
Local user view	Configure local user parameters	[4210-luser-user1]	Execute the local-user command in system view.	
User interface view	Configure user interface parameters	[4210-ui-aux0]	Execute the user-interface command in system view.	
FTP client view	Configure FTP client parameters	[ftp]	Execute the ftp command in user view.	
SFTP client view	Configure SFTP client parameters	sftp-client>	Execute the sftp command in system view.	
MST region view	Configure MST region parameters	[4210-mst-region]	Execute the stp region-configuration command in system view.	
Cluster view	Configure cluster parameters	[4210-cluster]	Execute the cluster command in system view.	
Public key view	Configure the RSA public key for SSH users	[4210-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	[4210-peer-public-key]	Execute the public-key peer command in system view.	
Public key editing view	Edit the RSA public key for SSH users	[4210-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	[4210-peer-key-code]		

Table 4 CLI views

View	Available operation	Prompt example	Enter method	Quit method
Basic ACL view	Define rules for a basic ACL (with ID ranging from 2000 to 2999)	[4210-acl-basic-2000]	Execute the acl number command in system view.	Execute the quit command to return to system view. Execute the return command to return to user view.
Advanced ACL view	Define rules for an advanced ACL (with ID ranging from 3000 to 3999)	[4210-acl-adv-3000]	Execute the acl number command in system view.	
RADIUS scheme view	Configure RADIUS scheme parameters	[4210-radius-1]	Execute the radius scheme command in system view.	
ISP domain view	Configure ISP domain parameters	[4210-isp-aaa123.net]	Execute the domain command in system view.	
Remote-ping view	Configure Remote-ping parameters	[4210-remote-ping-a123-a123]	Execute the remote-ping command in system view.	
PoE profile view	Configure PoE profile parameters	[4210-poe-profile-a123]	Execute the poe-profile command in system view.	



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 to display all the commands available in the view and a brief description for each command, for example:

```
<4210> ?
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
```

- 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.

```
<4210> 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 displays:

```
[4210] 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.

```
[4210] interface vlan-interface 1 ?
<cr>
```

Partial online help

- 1 Enter a character/string, and followed by a question mark (?). All the commands beginning with the character/string display, for example:

```
<4210> p?
  ping
  pwd
```

- 2 Enter a command, a space, and a character/string followed by a question mark (?). All the keywords beginning with the character/string (if available) display, for example:

```
<4210> display u?
  udp
  unit
  user-interface
  users
```

- 3 Enter the first several characters of a command's keyword 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 display then one by one (in complete form) by pressing <Tab> repeatedly.

Terminal Display

The CLI provides the screen splitting feature display output suspended when the screen is full. When display output pauses, you can perform the following operations as needed.

Table 5 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.
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. By default, the CLI stores up to 10 most recently executed commands for each user. You can view the command history by performing the operations listed in Table 6.

Table 6 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	Pressing the down arrow key or <Ctrl+N>	This operation recalls the next history command (if available).



- The Windows 9x HyperTerminal defines 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 stored in the CLI.

Error Prompts

If a command passes the syntax check, it is executed; otherwise, an error message displays. Table 7 lists the most common error messages.

Table 7 Common error messages

Error message	Description
Unrecognized command	The command does not exist. The keyword does not exist. The parameter type is wrong. The parameter value is out of range.
Incomplete command	The command entered is incomplete.
Too many parameters	You entered too many parameters.
Ambiguous command	The parameters entered are ambiguous.
Wrong parameter found at '^' position	A parameter entered is wrong. 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 8 lists the CLI edit operations.

Table 8 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.

Table 8 Edit operations

Press...	To...
Right arrow key or <Ctrl+F>	Move the cursor one character to the right.
Up arrow key or <Ctrl+P>	Display history commands.
Down arrow key or <Ctrl+N>	
<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.

2

LOGGING INTO AN ETHERNET SWITCH

You can log into a Switch 4210 in one of the following ways:

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

Supported User Interfaces



The Console port is also known as the auxiliary (AUX) port.

The Switch 4210 Family supports two types of CLI-driven user interfaces, AUX and VTY.

- **AUX user interface:** The view when you log in through the console or AUX port.
- **Virtual type terminal (VTY) user interface:** The view when you log in locally through an Ethernet port or remotely over the network using Telnet or SSH. The VTY port is the logical port associated with your management session.

Table 9 Description of the user interface

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

User Interface Index

Index numbers are used to distinguish between multiple users accessing the switch for management at the same time. There are two types of user interface indexes, 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 interface is numbered 0.
 - VTY user interfaces are numbered VTY0, VTY1, and so on.

Common User Interface Configuration

Table 10 Common user interface configuration

Operation	Command	Description
Lock the current user interface	lock	Optional Execute this command in user view. A user interface is not locked by default.
Specify to send messages to all user interfaces/a specified user interface	send { all number type number }	Optional Execute this command in user view.
Free a user interface	free user-interface [type] number	Optional Execute this command in user view.
Enter system view	system-view	-
Set the banner	header [incoming legal login shell] text	Optional By default, no banner is configured
Set a system name for the switch	sysname string	Optional By default, the system name is 4210 .
Enable copyright information displaying	copyright-info enable	Optional By default, one word 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 You can execute the display command in any view.
Display the physical attributes and configuration of the current/a specified user interface	display user-interface [type number number]	
Display the information about the current web users	display web users	

Logging in through the Console Port

Logging in through the Console port is the most common way to log into a switch. If you do not know the IP address of the switch, it is the only way to log-in to the switch. It is also the prerequisite to configure other login methods, and is used to recover the switch in certain circumstances.

Table 11 lists the default settings of a Console port.

Table 11 The default settings of a Console port

Setting	Default
Baud rate	19,200 bps
Flow control	None
Check mode (Parity)	None
Stop bits	1
Data bits	8

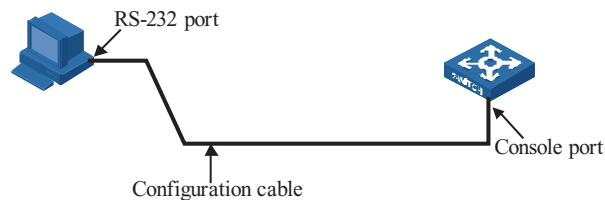
To log into a switch through the Console port, make sure the settings of both the Console port and the user terminal are the same.

After logging into a switch, you can perform configuration for AUX users. Refer to “Common Configurations” on page 26.

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 1.

Figure 1 Diagram for connecting to the Console port of a switch



- 2 the terminal emulation utility you are most familiar with. Be sure to configure the console port software to match the settings in Table 11. The following example demonstrates the use of the Windows XP terminal emulator.

Figure 2 Create a connection

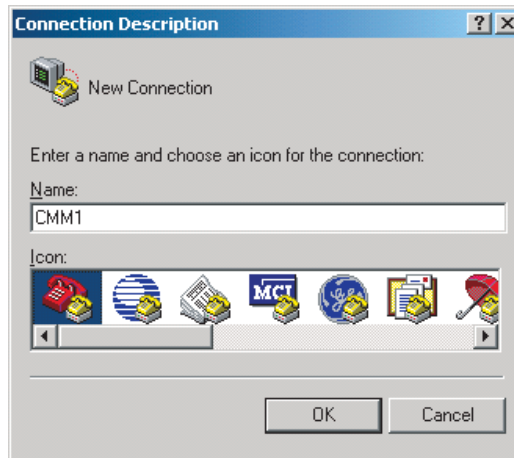
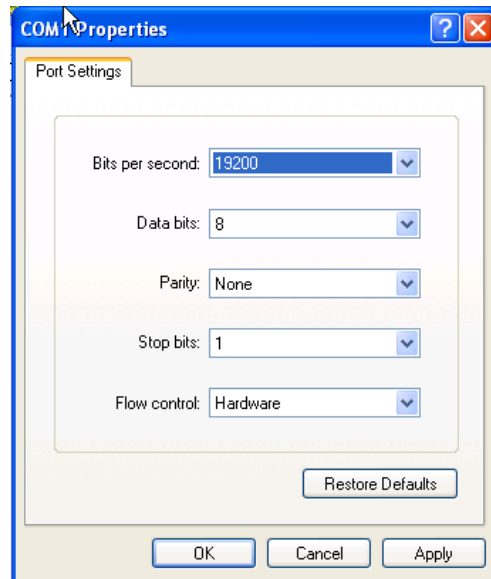
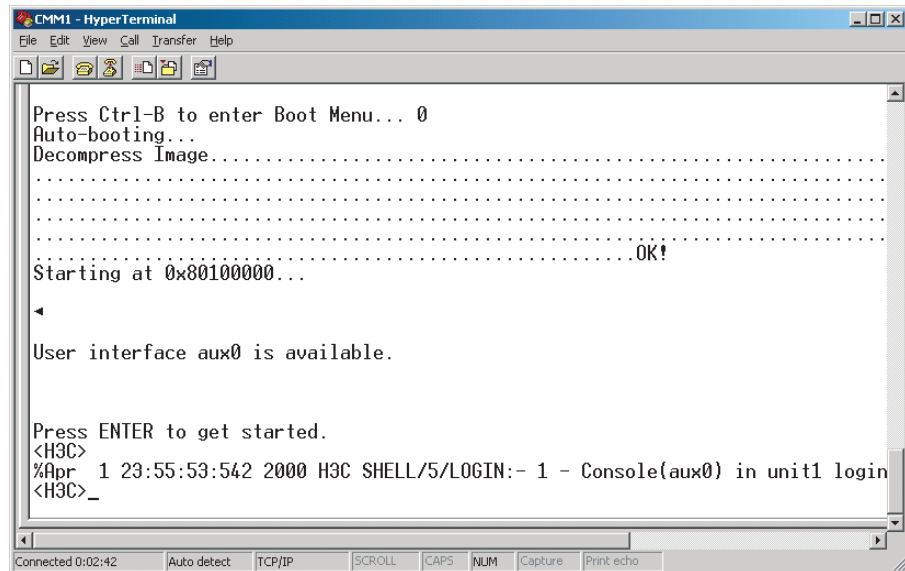


Figure 3 Specify the port used to establish the connection



Figure 4 Set port parameters

- 3 Plug in the switch so it has power. You will be prompted to press the Enter key if the switch successfully completes POST (power-on self test). The prompt (such as <4210>) appears after you press the Enter key, as shown in Figure 5.

Figure 5 HyperTerminal CLI

- 4 You can then configure the switch or check the information about the switch by executing the corresponding commands. You can also acquire help by typing the ? character.

Common Configurations Table 12 lists the common configurations of Console port login.

Table 12 Common configuration of Console port login

Configuration		Remarks
Console port configuration	Baud rate	Optional The default baud rate is 19,200 bps.
	Check mode	Optional By default, the check mode of the Console port is set to "none", which means no check bit.
	Stop bits	Optional The default stop bits of a Console port is 1.
	Data bits	Optional The default data bits of a Console port is 8.
AUX user interface configuration	Configure the command level available to the users logging into the AUX user interface	Optional By default, commands of level 3 are available to the users logging into the AUX user interface.
Terminal configuration	Make terminal services available	Optional By default, terminal services are available in all user interfaces
	Set the maximum number of lines the screen can contain	Optional By default, the screen can contain up to 24 lines.
	Set history command buffer size	Optional By default, the history command buffer can contain up to 10 commands.
	Set the timeout time of a user interface	Optional The default timeout time is 10 minutes.



CAUTION: *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 into the switch in other ways. To log into 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 4.*

Console Port Login Configurations for Different Authentication Modes

Table 13 lists Console port login configurations for different authentication modes.

Table 13 Console port login configurations for different authentication modes

Authentication mode	Console port login configuration		Remarks
None	Perform common configuration	Perform common configuration for Console port login	Optional Refer to Table 12.

Table 13 Console port login configurations for different authentication modes

Authentication mode	Console port login configuration		Remarks
Password	Configure the password	Configure the password for local authentication	Required
	Perform common configuration	Perform common configuration for Console port login	Optional Refer to Table 12.
Scheme	Specify to perform local authentication or remote RADIUS authentication	AAA configuration specifies whether to perform local authentication or RADIUS authentication	Optional Local authentication is performed by default. Refer to "AAA Configuration" on page 245
	Configure user name and password	Configure user names and passwords for local/RADIUS users	Required <ul style="list-style-type: none"> ■ The user name and password of a local user are configured on the switch. ■ The user name and password of a RADIUS user are configured on the RADIUS server. Refer to the RADIUS server's user manual for more information.
	Manage AUX users	Set service type for AUX users	Required
	Perform common configuration	Perform common configuration for Console port login	Optional Refer to Table 12.



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

Configuring Console Port Login with no Authentication

Table 14 Console port login configuration with the authentication mode being none

Operation	Command	Description
Enter system view	system-view	-
Enter AUX user interface view	user-interface aux 0	-
Configure not to authenticate users	authentication-mode none	Required By default, users logging in through the Console port (AUX user interface) are not authenticated.

Table 14 Console port login configuration with the authentication mode being none

Operation		Command	Description
Configure the Console port	Set the baud rate	speed <i>speed-value</i>	Optional The default baud rate of a Console port is 19,200 bps.
	Set the check mode	parity { even none odd }	Optional By default, the check mode of a Console port is none , that is, no check is performed.
	Set the stop bits	stopbits { 1 1.5 2 }	Optional The stop bits of a Console port is 1.
	Set the data bits	databits { 7 8 }	Optional The default data bits of a Console port is 8.
Configure the command level available to users logging into the user interface		user privilege level <i>level</i>	Optional By default, commands of level 3 are available to users logging into the AUX user interface, and commands of level 0 are available to users logging into the VTY user interface.
Enable terminal services		shell	Optional By default, terminal services are available in all user interfaces.
Set the maximum number of lines the screen can contain		screen-length <i>screen-length</i>	Optional By default, the screen can contain up to 24 lines. You can use the screen-length 0 command to disable the function to display information in pages.
Set the history command buffer size		history-command max-size <i>value</i>	Optional The default history command buffer size is 10. That is, a history command buffer can store up to 10 commands by default.

Table 14 Console port login configuration with the authentication mode being none

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

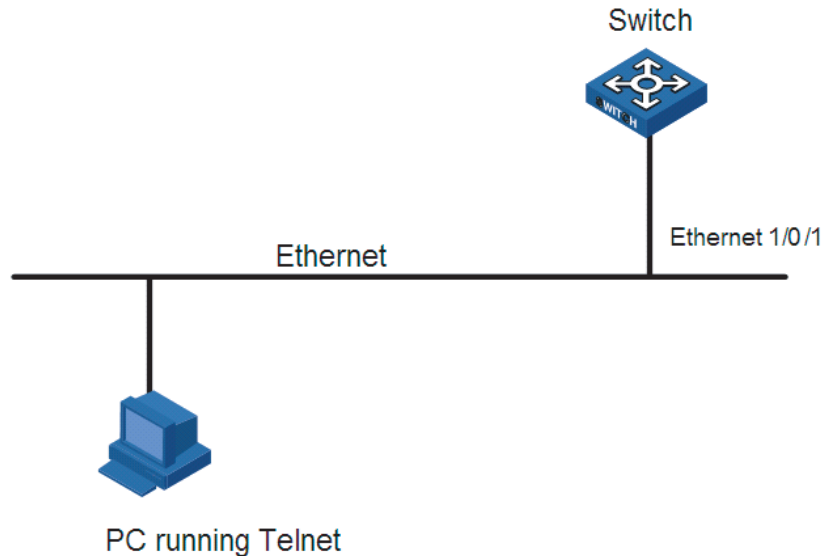
Configuration Example **Network requirements**

Assume that the switch is configured to allow users to log in through Telnet, and the 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 into the AUX user interface.
- The baud rate of the Console port is 19,200 bps.
- The screen can contain up to 30 lines.
- The history command buffer can contain up to 20 commands.
- The timeout time of the AUX user interface is 6 minutes.

Network diagram

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



Configuration procedure

Enter system view.

```
<4210> system-view
```

Enter AUX user interface view.

```
[4210] user-interface aux 0
```

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

```
[4210-ui-aux0] authentication-mode none
```

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

```
[4210-ui-aux0] user privilege level 2
```

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

```
[4210-ui-aux0] speed 19200
```

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

```
[4210-ui-aux0] screen-length 30
```

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

```
[4210-ui-aux0] history-command max-size 20
```

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

```
[4210-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 4 to log into the switch successfully.

Configuring Console Port Login to Require a Password

Configuration Procedure

Table 15 Console port login configuration with the authentication mode being password

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

Table 15 Console port login configuration with the authentication mode being password

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

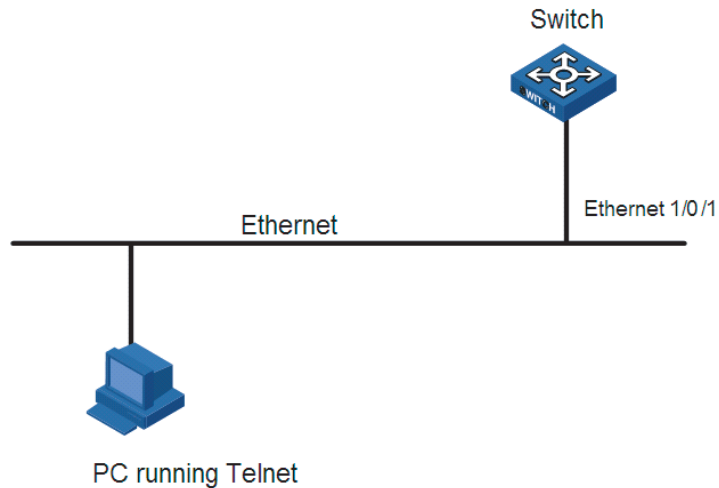
Configuration Example **Network requirements**

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

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

Network diagram

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



Configuration procedure

Enter system view.

```
<4210> system-view
```

Enter AUX user interface view.

```
[4210] user-interface aux 0
```

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

```
[4210-ui-aux0] authentication-mode password
```

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

```
[4210-ui-aux0] set authentication password simple 123456
```

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

```
[4210-ui-aux0] user privilege level 2
```

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

```
[4210-ui-aux0] speed 19200
```

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

```
[4210-ui-aux0] screen-length 30
```

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

```
[4210-ui-aux0] history-command max-size 20
```

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

```
[4210-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 4 to log into the switch successfully.

Console Port Login Configuration with Authentication Mode Being Scheme

Configuration Procedure

Table 16 Console port login configuration with the authentication mode being scheme

Operation	Command	Description	
Enter system view	system-view	-	
Configure the authentication mode	Enter the default ISP domain view Specify the AAA scheme to be applied to the domain Quit to system view	domain <i>domain-name</i> scheme { local none radius-scheme <i>radius-scheme-name</i> [local] hwtacacs-scheme <i>hwtacacs-scheme-name</i> [local] } quit	Optional By default, the local AAA scheme is applied. If you specify to apply the local AAA scheme, you need to perform the configuration concerning local user as well. If you specify to apply an existing scheme by providing the <i>radius-scheme-name</i> argument, you need to perform the following configuration as well: <ul style="list-style-type: none"> Perform AAA&RADIUS configuration on the switch. (Refer to “AAA Configuration” on page 245 for more information.) Configure the user name and password accordingly on the AAA server. (Refer to the AAA server’s user manual.)
Create a local user (Enter local user view.)	local-user <i>user-name</i>	Required No local user exists by default.	
Set the authentication password for the local user	password { simple cipher } <i>password</i>	Required	
Specify the service type for AUX users	service-type terminal [level <i>level</i>]	Required	
Quit to system view	quit	-	
Enter AUX user interface view	user-interface aux 0	-	
Configure to authenticate users locally or remotely	authentication-mode scheme [command-authorization]	Required The specified AAA scheme determines whether to authenticate users locally or remotely. By default, users logging in through the Console port (AUX user interface) are not authenticated.	

Table 16 Console port login configuration with the authentication mode being scheme

Operation		Command	Description
Configure the Console port	Set the baud rate	speed <i>speed-value</i>	Optional The default baud rate of the AUX port (also the Console port) is 9,600 bps.
	Set the check mode	parity { even none odd }	Optional By default, the check mode of a Console port is set to none , that is, no check bit.
	Set the stop bits	stopbits { 1 1.5 2 }	Optional The default stop bits of a Console port is 1.
	Set the data bits	databits { 7 8 }	Optional The default data bits of a Console port is 8.
Configure the command level available to users logging into the user interface		user privilege level <i>level</i>	Optional By default, commands of level 3 are available to users logging into the AUX user interface.
Make terminal services available to the user interface		shell	Optional By default, terminal services are available in all user interfaces.
Set the maximum number of lines the screen can contain		screen-length <i>screen-length</i>	Optional By default, the screen can contain up to 24 lines. You can use the screen-length 0 command to disable the function to display information in pages.
Set history command buffer size		history-command max-size <i>value</i>	Optional The default history command buffer size is 10. That is, a history command buffer can store up to 10 commands by default.
Set the timeout time for the user interface		idle-timeout <i>minutes</i> [<i>seconds</i>]	Optional The default timeout time of a user interface is 10 minutes. With the timeout time being 10 minutes, the connection to a user interface is terminated if no operation is performed in the user interface within 10 minutes. You can use the idle-timeout 0 command to disable the timeout function.

Note that if you configure to authenticate the users in the scheme mode, the command level available to users logging into a switch depends on the command level specified in the **service-type terminal** [**level** *level*] command.

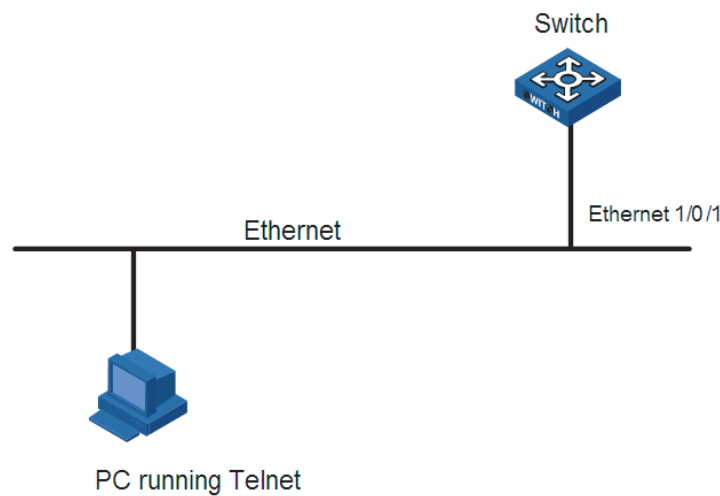
Configuration Example Network requirements

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

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

Network diagram

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

**Configuration procedure**

Enter system view.

```
<4210> system-view
```

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

```
[4210] local-user guest
```

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

```
[4210-luser-guest] password simple 123456
```

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

```

[4210-luser-guest] service-type terminal level 2
[4210-luser-guest] quit

# Enter AUX user interface view.

[4210] user-interface aux 0

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

[4210-ui-aux0] authentication-mode scheme

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

[4210-ui-aux0] speed 19200

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

[4210-ui-aux0] screen-length 30

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

[4210-ui-aux0] history-command max-size 20

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

[4210-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 4 to log into the switch successfully.

Logging in through Telnet

The Switch 4210 Family supports Telnet. You can manage and maintain a switch remotely by using Telnet to access the switch. To log into a switch through Telnet, the corresponding configuration is required on both the switch and the Telnet terminal.

You can also log into a switch through SSH. SSH is a secure shell added to Telnet. Refer to “SSH Configuration” on page 387 for related information.

Table 17 Requirements for using Telnet to access 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 “Configuring IP Addresses” on page 89, and “Configuring IP Performance” on page 91.) The authentication mode and other settings are configured. Refer to Table 18 and Table 19.
Telnet terminal	Telnet is running. The IP address of the VLAN of the switch is available.



Telnetting to a switch using IPv6 protocols is similar to Telnetting to a switch using IPv4 protocols. Refer to "IPv6 Management Configuration" on page 525 for related information.

Common Configuration Table 18 lists the common Telnet configuration.

Table 18 Common Telnet configuration

Configuration		Description
VTY user interface configuration	Configure the command level available to users logging into the VTY user interface	Optional By default, commands of level 0 are available to users logging into a VTY user interface.
	Configure the protocols the user interface supports	Optional By default, Telnet and SSH protocol are supported.
	Set the commands to be executed automatically after a user log into the user interface successfully	Optional By default, no command is executed automatically after a user logs into the VTY user interface.
VTY terminal configuration	Make terminal services available	Optional By default, terminal services are available in all user interfaces
	Set the maximum number of lines the screen can contain	Optional By default, the screen can contain up to 24 lines.
	Set history command buffer size	Optional By default, the history command buffer can contain up to 10 commands.
	Set the timeout time of a user interface	Optional The default timeout time is 10 minutes.

Telnet Configurations for Different Authentication Modes

Table 19 lists Telnet configurations for different authentication modes.

Table 19 Telnet configurations for different authentication modes

Authentication mode	Telnet configuration		Description
None	Perform common configuration	Perform common Telnet configuration	Optional Refer to Table 18.
Password	Configure the password	Configure the password for local authentication	Required
	Perform common configuration	Perform common Telnet configuration	Optional Refer to Table 18.

Table 19 Telnet configurations for different authentication modes

Authentication mode	Telnet configuration		Description
Scheme	Specify to perform local authentication or remote RADIUS authentication	AAA configuration specifies whether to perform local authentication or RADIUS authentication	Optional Local authentication is performed by default. Refer to “AAA Configuration” on page 245.
		Configure user name and password	Required <ul style="list-style-type: none"> The user name and password of a local user are configured on the switch. The user name and password of a remote user are configured on the RADIUS server. Refer to the RADIUS server’s user manual.
	Manage VTY users	Set service type for VTY users	Required
	Perform common configuration	Perform common Telnet configuration	Optional Refer to Table 18.



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 without Authentication

Configuration Procedure

Table 20 Telnet configuration with the authentication mode being none

Operation	Command	Description
Enter system view	system-view	-
Enter one or more VTY user interface views	user-interface vty <i>first-number</i> [<i>last-number</i>]	-
Configure not to authenticate users logging into VTY user interfaces	authentication-mode none	Required By default, VTY users are authenticated after logging in.

Table 20 Telnet configuration with the authentication mode being none

Operation	Command	Description
Configure the command level available to users logging into VTY user interface	user privilege level <i>level</i>	Optional By default, commands of level 0 are available to users logging into VTY user interfaces.
Configure the protocols to be supported by the VTY user interface	protocol inbound { all ssh telnet }	Optional By default, both Telnet protocol and SSH protocol are supported.
Set the commands to be executed automatically after a user login to the user interface successfully	auto-execute command <i>text</i>	Optional By default, no command is executed automatically after a user logs into the VTY user interface.
Make terminal services available	shell	Optional By default, terminal services are available in all user interfaces.
Set the maximum number of lines the screen can contain	screen-length <i>screen-length</i>	Optional By default, the screen can contain up to 24 lines. You can use the screen-length 0 command to disable the function to display information in pages.
Set the history command buffer size	history-command max-size <i>value</i>	Optional The default history command buffer size is 10. That is, a history command buffer can store up to 10 commands by default.
Set the timeout time of the VTY user interface	idle-timeout <i>minutes</i> [<i>seconds</i>]	Optional The default timeout time of a user interface is 10 minutes. With the timeout time being 10 minutes, the connection to a user interface is terminated if no operation is performed in the user interface within 10 minutes. You can use the idle-timeout 0 command to disable the timeout function.

Note that if you configure not to authenticate the users, the command level available to users logging into a switch depends on the **user privilege level** *level* command

Configuration Example **Network requirements**

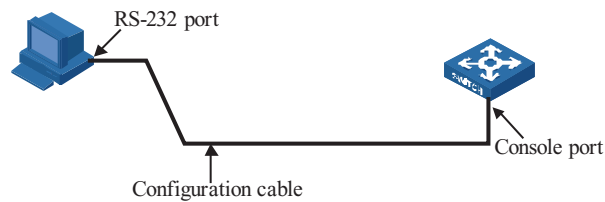
Assume current user logins through the Console port, and the user level is set to the administrator level (level 3). Perform the following configurations for users logging in through VTY 0 using Telnet.

- 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 9 Network diagram for Telnet configuration (with the authentication mode being none)



Configuration procedure

Enter system view.

```
<4210> system-view
```

Enter VTY 0 user interface view.

```
[4210] user-interface vty 0
```

Configure not to authenticate Telnet users logging into VTY 0.

```
[4210-ui-vty0] authentication-mode none
```

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

```
[4210-ui-vty0] user privilege level 2
```

Configure Telnet protocol is supported.

```
[4210-ui-vty0] protocol inbound telnet
```

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

```
[4210-ui-vty0] screen-length 30
```

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

```
[4210-ui-vty0] history-command max-size 20
```

Set the timeout time to 6 minutes.

```
[4210-ui-vty0] idle-timeout 6
```

Telnet Configuration with Authentication Requiring a Password

Configuration Procedure

Table 21 Telnet configuration with the authentication mode being password

Operation	Command	Description
Enter system view	system-view	-
Enter one or more VTY user interface views	user-interface vty <i>first-number</i> [<i>last-number</i>]	-
Configure to authenticate users logging into VTY user interfaces using the local password	authentication-mode password	Required
Set the local password	set authentication password { cipher simple } <i>password</i>	Required
Configure the command level available to users logging into the user interface	user privilege level <i>level</i>	Optional By default, commands of level 0 are available to users logging into VTY user interface.
Configure the protocol to be supported by the user interface	protocol inbound { all ssh telnet }	Optional By default, both Telnet protocol and SSH protocol are supported.
Set the commands to be executed automatically after a user login to the user interface successfully	auto-execute command <i>text</i>	Optional By default, no command is executed automatically after a user logs into the VTY user interface.
Make terminal services available	shell	Optional By default, terminal services are available in all user interfaces.
Set the maximum number of lines the screen can contain	screen-length <i>screen-length</i>	Optional By default, the screen can contain up to 24 lines. You can use the screen-length 0 command to disable the function to display information in pages.
Set the history command buffer size	history-command max-size <i>value</i>	Optional The default history command buffer size is 10. That is, a history command buffer can store up to 10 commands by default.

Table 21 Telnet configuration with the authentication mode being password

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

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

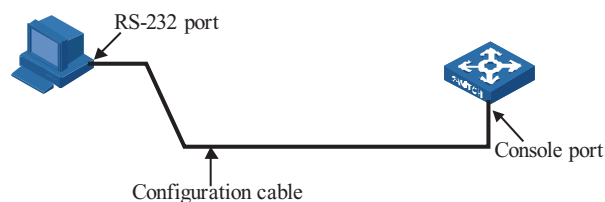
Configuration Example Network requirements

The current user logs in through the Console port and the user level is set to the administrator level (level 3). Perform the following configuration for users logging into VTY 0 using Telnet.

- 1 Authenticate users using the local password.
- 2 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 10 Network diagram for Telnet configuration (with the authentication mode being password)



Configuration procedure

```
# Enter system view.
<4210> system-view
```

```

# Enter VTY 0 user interface view.
[4210] user-interface vty 0

# Configure to authenticate users logging into VTY 0 using the password.
[4210-ui-vty0] authentication-mode password

# Set the local password to 123456 (in plain text).
[4210-ui-vty0] set authentication password simple 123456

# Specify commands of level 2 are available to users logging into VTY 0.
[4210-ui-vty0] user privilege level 2

# Configure Telnet protocol is supported.
[4210-ui-vty0] protocol inbound telnet

# Set the maximum number of lines the screen can contain to 30.
[4210-ui-vty0] screen-length 30

# Set the maximum number of commands the history command buffer can store
to 20.
[4210-ui-vty0] history-command max-size 20

# Set the timeout time to 6 minutes.
[4210-ui-vty0] idle-timeout 6

```

Telnet Configuration with Authentication Mode Being Scheme

Configuration Procedure

Table 22 Telnet configuration with the authentication mode being scheme

Operation	Command	Description
Enter system view	system-view	-

Table 22 Telnet configuration with the authentication mode being scheme

Operation		Command	Description
Configure the authentication scheme	Enter the default ISP domain view	domain <i>domain-name</i>	Optional
	Configure the AAA scheme to be applied to the domain	scheme { local none radius-scheme <i>radius-scheme-name</i> [local] hwtacacs-scheme <i>hwtacacs-scheme-name</i> [local] }	By default, the local AAA scheme is applied. If you specify to apply the local AAA scheme, you need to perform the configuration concerning local user as well. If you specify to apply an existing scheme by providing the <i>radius-scheme-name</i> argument, you need to perform the following configuration as well:
	Quit to system view	quit	<ul style="list-style-type: none"> ■ Perform AAA&RADIUS configuration on the switch. (Refer to “AAA Configuration” on page 245.) ■ Configure the user name and password accordingly on the AAA server. (Refer to “AAA Configuration” on page 245.)
	Create a local user and enter local user view	local-user <i>user-name</i>	No local user exists by default.
	Set the authentication password for the local user	password { simple cipher } <i>password</i>	Required
	Specify the service type for VTY users	service-type telnet [level <i>level</i>]	Required
	Quit to system view	quit	-
	Enter one or more VTY user interface views	user-interface vty <i>first-number</i> [<i>last-number</i>]	-
	Configure to authenticate users locally or remotely	authentication-mode scheme [command-authorization]	Required The specified AAA scheme determines whether to authenticate users locally or remotely. Users are authenticated locally by default.
	Configure the command level available to users logging into the user interface	user privilege level <i>level</i>	Optional By default, commands of level 0 are available to users logging into the VTY user interfaces.
	Configure the supported protocol	protocol inbound { all ssh telnet }	Optional Both Telnet protocol and SSH protocol are supported by default.
	Set the commands to be executed automatically after a user login to the user interface successfully	auto-execute command <i>text</i>	Optional By default, no command is executed automatically after a user logs into the VTY user interface.
	Make terminal services available	shell	Optional Terminal services are available in all use interfaces by default.

Table 22 Telnet configuration with the authentication mode being scheme

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

Note that if you configure to authenticate the users in the scheme mode, the command level available to the users logging into the switch depends on the **user privilege level** *level* command and the **service-type** { **ftp** | **lan-access** | { **ssh** | **telnet** | **terminal** }* [**level** *level*] } command, as listed in Table 23.

Table 23 Determine the command level when users logging into switches are authenticated in the scheme mode

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



Refer to “AAA Configuration” on page 245 and “SSH Configuration” on page 387 for information about AAA, RADIUS, and SSH.

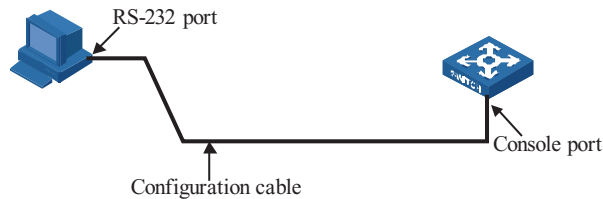
Configuration Example Network requirements

Assume current user logs in through the Console port and the user level is set to the administrator level (level 3). Perform the following configurations for users logging into 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 into 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 11 Network diagram for Telnet configuration (with the authentication mode being scheme)

**Configuration procedure**

Enter system view.

```
<4210> system-view
```

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

```
[4210] local-user guest
```

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

```
[4210-luser-guest] password simple 123456
```

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

```
[4210-luser-guest] service-type telnet level 2
[4210-luser-guest] quit
```

Enter VTY 0 user interface view.

```
[4210] user-interface vty 0
```

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

```
[4210-ui-vty0] authentication-mode scheme
```

Configure Telnet protocol is supported.

```
[4210-ui-vty0] protocol inbound telnet
```

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

```
[4210-ui-vty0] screen-length 30
```

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

```
[4210-ui-vty0] history-command max-size 20
```

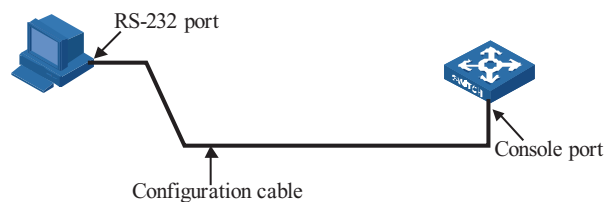
Set the timeout time to 6 minutes.

```
[4210-ui-vty0] idle-timeout 6
```

Telnetting to a Switch **Telnetting to a Switch from a Terminal**

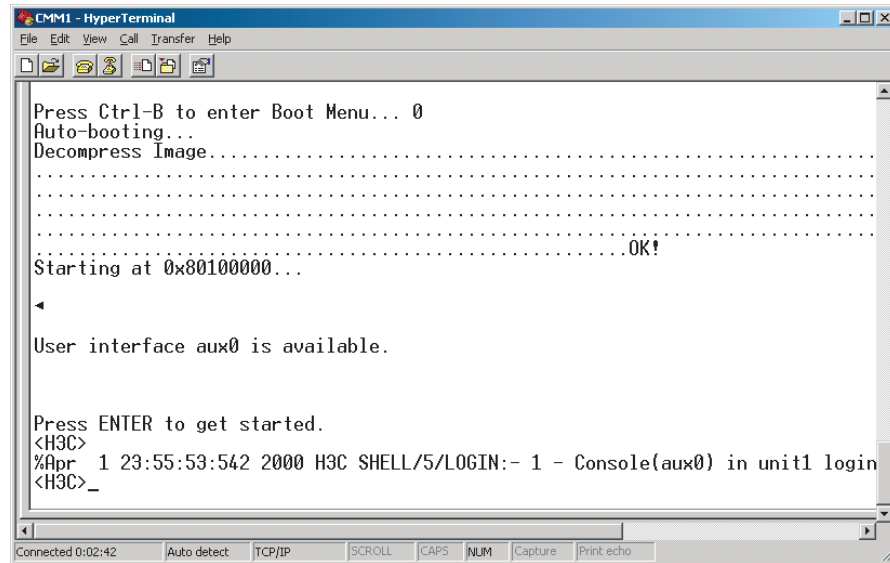
- 1 Assign an IP address to VLAN-interface 1 of the switch (VLAN 1 is the default VLAN of the switch).
 - Connect the serial port of your PC/terminal to the Console port of the switch, as shown in Figure 12.

Figure 12 Diagram for establishing connection to a Console port



- Launch a terminal emulation utility (such as Terminal in Windows 3.X or HyperTerminal in Windows 95/Windows 98/Windows NT/Windows 2000/Windows XP) on the PC terminal, with the baud rate set to 9,600 bps, data bits set to 8, parity check set to none, and flow control set to none.
- Turn on the switch and press Enter as prompted. The prompt (such as <4210>) appears, as shown in the following figure.

Figure 13 The terminal window

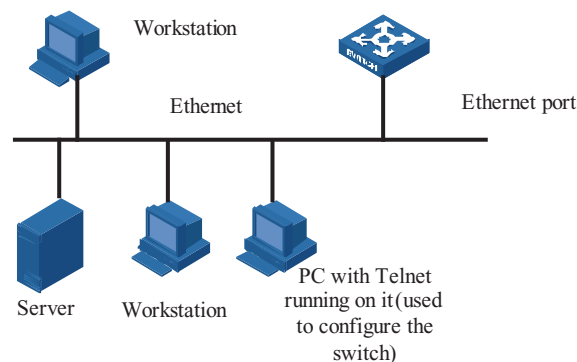


- Perform the following operations in the terminal window to assign IP address 202.38.160.92/24 to VLAN-interface 1 of the switch.

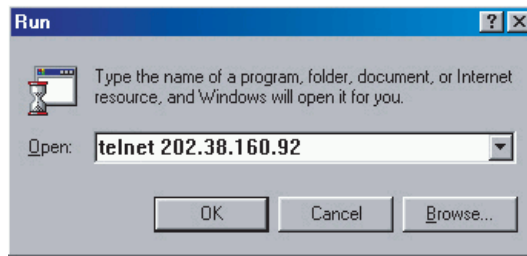
```
<4210> system-view
[4210] interface Vlan-interface 1
[4210-Vlan-interface1] ip address 202.38.160.92 255.255.255.0
```

- 2 Perform Telnet-related configuration on the switch according to instructions earlier in this chapter.
- 3 Connect your PC/terminal and the switch to an Ethernet, as shown in Figure 14. 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 14 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 15.

Figure 15 Launch Telnet

- 5 If the password authentication mode is specified, enter the password when the Telnet window displays "Login authentication" and prompts for login password. The CLI prompt (such as <4210>) 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 series Ethernet switch can accommodate up to five Telnet connections at same time.
- 6 After successfully Telnetting to the switch, you can configure the switch or display the information about the switch by executing corresponding commands. You can also type ? at any time for help.



- 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 "Command Hierarchy" on page 11 and "CLI Views" on page 14 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 16, 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 16 Network diagram for Telnetting to another switch from the current switch

- 1 Perform Telnet-related configuration on the switch operating as the Telnet server using the instructions earlier in this chapter.
- 2 Telnet to the switch operating as the Telnet client.
- 3 Execute the following command on the switch operating as the Telnet client:

```
<4210> telnet xxxx
```

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

- 4 After successful login, the CLI prompt (such as <4210>) 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!".
- 5 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.

Logging in Using a Modem

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

Table 24 Requirements for logging into a switch using a modem

Item	Requirement
Administrator side	The PC can communicate with the modem connected to it. The modem is properly connected to PSTN. The telephone number of the switch side is available.
Switch side	The modem is connected to the Console port of the switch properly. The modem is properly configured. The modem is properly connected to PSTN and a telephone set. The authentication mode and other related settings are configured on the switch. Refer to Table 13.

Configuring the Switch 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.



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



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

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

The configuration on the switch depends on the authentication mode the user is in. Refer to Table 13 for the information about authentication mode configuration.

Configuration on switch when the authentication mode is none

Refer to “Configuring Console Port Login with no Authentication” on page 27.

Configuration on switch when the authentication mode is password

Refer to “Configuring Console Port Login to Require a Password” on page 31.

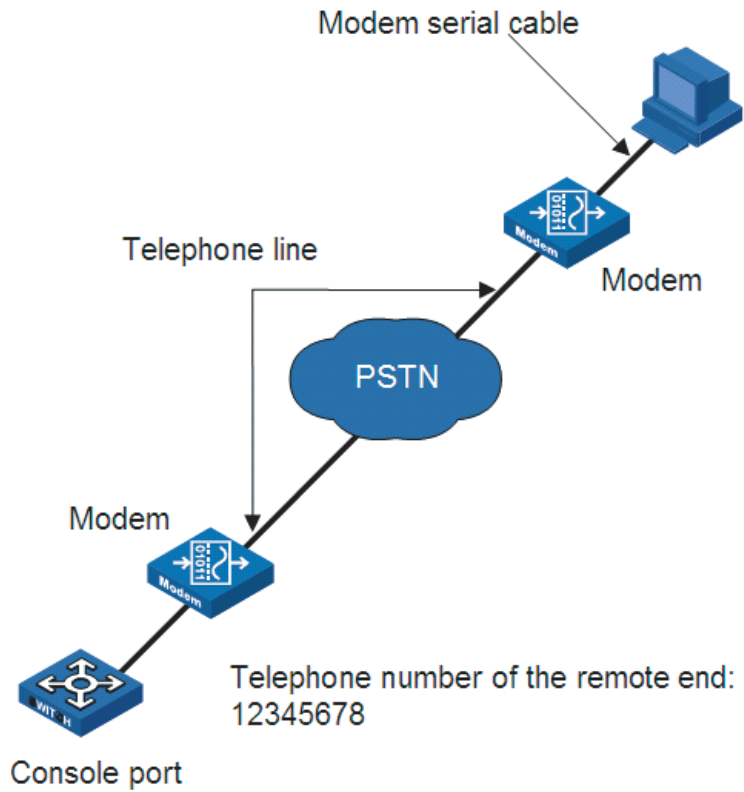
Configuration on switch when the authentication mode is scheme

Refer to “Console Port Login Configuration with Authentication Mode Being Scheme” on page 34.

Establishin a Modem Connection

- 1 Before using Modem to log in the switch, perform corresponding configuration for different authentication modes on the switch. Refer to “Configuring Console Port Login with no Authentication”, “Configuring Console Port Login to Require a 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 17. Make sure the modems are properly connected to telephone lines.

Figure 17 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 18 through Figure 20. Note that you need to set the telephone number to that of the modem directly connected to the switch.

Figure 18 Create a connection

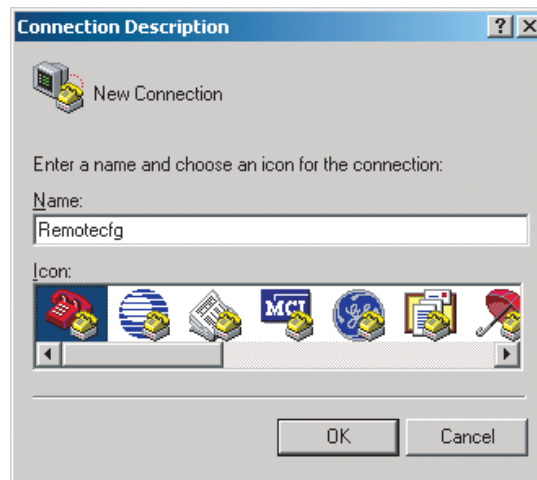
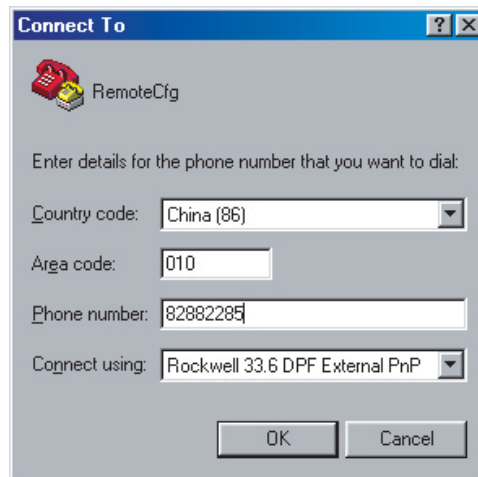
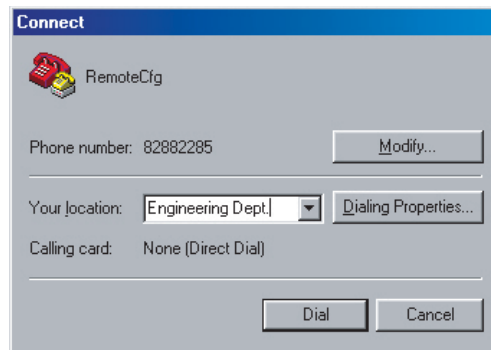


Figure 19 Set the telephone number**Figure 20** Call the modem

- 5 If the password authentication mode is specified, enter the password when prompted. If the password is correct, the prompt (such as <4210>) appears. You can then configure or manage the switch. You can also enter the character ? at anytime for help.



If you perform no AUX user-related configuration on the switch, the commands of level 3 are available to modem users. Refer to "CLI Configuration" on page 11 for information about the command line interface.

Logging in through the Web-based Network Management System

A Switch 4210 has a Web server built in. It enables you to log into a Switch 4210 through a Web browser and then manage and maintain the switch intuitively by interacting with the built-in Web server.

To log into a Switch 4210 through the built-in Web-based network management system, you need to perform the related configuration on both the switch and the PC operating as the network management terminal.

Table 25 Requirements for logging into a switch through the Web-based network management system

Item	Requirement
Switch	<p>The web-based interface code is loaded onto the switch. This file has a .web extension (e.g., s4p01_00c01.web) and can be found in the file management system of the switch. It is loaded and resident by default.</p> <p>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 "IP Addressing Configuration" on page 87 and "IP Performance Configuration" on page 91.)</p> <p>The user name and password for logging into the Web-based network management system are configured.</p>
PC operating as the network management terminal	<p>Internet Explorer or another supported browser is available.</p> <p>The IP address of the VLAN interface of the switch, the user name, and the password are available.</p>

Establishing an HTTP Connection

- 1 Ensure that an IP address is assigned 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 Have available the user name and the password on the switch for the Web network management user to log in. By default, the web interface user name is "admin" and the password is left blank.

To create a web user name and password, you will need to access the switch via the console port or telnet. This is an example of creating a Web user account with the user name and password set to "admin" with level 3 privileges.

```
<4210> system-view
[4210] local-user admin
[4210-luser-admin] service-type telnet level 3
[4210-luser-admin] password simple admin
```

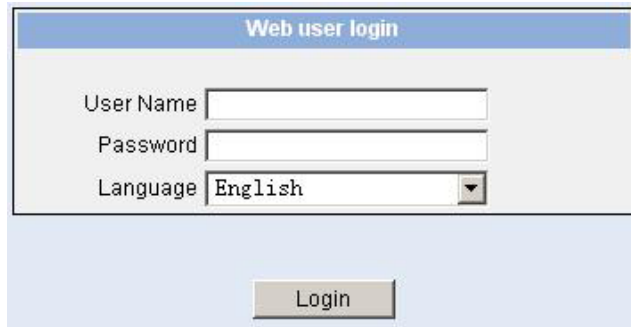
- 3 Establish an HTTP connection between your PC and the switch, as shown in Figure 21.

Figure 21 Establish an HTTP connection between your PC and the switch



- 4 Log into the switch through IE. Launch IE on the Web-based network management terminal (your PC) and enter the IP address of the management VLAN interface of the switch 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 22) 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 22 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.

Table 26 Configure the login banner

Operation	Command	Description
Enter system view	system-view	-
Configure the banner to be displayed when a user logs in through Web	header login text	Required By default, no login banner is configured.

Configuration Example

Network requirements

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

Network diagram

Figure 23 Network diagram for login banner configuration



Configuration Procedure

Enter system view.

```
<4210> system-view
```

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

```
[4210] 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 24.

Figure 24 Banner page displayed when a user logs in to the switch through Web



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

Enabling/Disabling the WEB Server

Table 27 Enable/Disable the WEB Server

Operation	Command	Description
Enter system view	system-view	-
Enable the Web server	ip http shutdown	Required By default, the Web server is enabled.

Table 27 Enable/Disable the WEB Server

Operation	Command	Description
Disable the Web server	undo ip http shutdown	Required



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.

Managing from an NMS

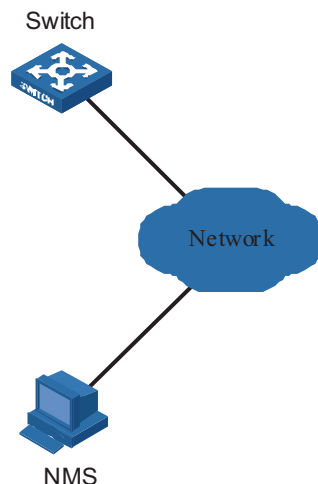
You can access your switch from a network management station (NMS), and then configure and manage the switch through the switch’s management agent. Simple network management protocol (SNMP) is applied between the NMS and the agent. Refer to “SNMP Configuration” on page 351 and “RMON Configuration” on page 361 for related information.

To manage your switch from an NMS, you need to perform related configuration on both the NMS and the switch.

Table 28 Requirements for logging into 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 “IP Addressing Configuration” on page 87.) The basic SNMP functions are configured. (“SNMP Configuration” on page 351 and “RMON Configuration” on page 361 for related information.)
NMS	The NMS is properly configured. (Refer to the user manual of your NMS for related information.)

Figure 25 Network diagram for logging in through an NMS



User Control



Refer to “Password Control Configuration Operations” on page 555 for information about the ACL.

A switch provides ways to control different types of login users, as listed in Table 29.

Table 29 Ways to control different types of login users

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

Controlling Telnet Users

Prerequisites

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

Controlling Telnet Users by Source IP Addresses

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

Table 30 Control Telnet users by source IP addresses

Operation	Command	Description
Enter system view	system-view	-
Create a basic ACL or enter basic ACL view	acl number <i>acl-number</i> [match-order { config auto }]	As for the acl number command, the config keyword is specified by default.
Define rules for the ACL	rule [<i>rule-id</i>] { deny permit } [<i>rule-string</i>]	Required
Quit to system view	quit	-
Enter user interface view	user-interface [<i>type</i>] <i>first-number</i> [<i>last-number</i>]	-

Table 30 Control Telnet users by source IP addresses

Operation	Command	Description
Apply the ACL to control Telnet users by source IP addresses	acl <i>acl-number</i> { inbound outbound }	Required The inbound keyword specifies to filter the users trying to Telnet to the current switch. The outbound keyword specifies to filter users trying to Telnet to other switches from the current switch.

Controlling Telnet Users by Source and Destination IP Addresses

Controlling Telnet users by source and destination IP addresses is achieved by applying advanced ACLs, which are numbered from 3000 to 3999.

Table 31 Control Telnet users by source and destination IP addresses

Operation	Command	Description
Enter system view	system-view	-
Create an advanced ACL or enter advanced ACL view	acl number <i>acl-number</i> [match-order { config auto }]	As for the acl number command, the config keyword is specified by default.
Define rules for the ACL	rule [<i>rule-id</i>] { deny permit } <i>protocol</i> [<i>rule-string</i>]	Required You can define rules as needed to filter by specific source and destination IP addresses.
Quit to system view	quit	-
Enter user interface view	user-interface [<i>type</i>] <i>first-number</i> [<i>last-number</i>]	-
Apply the ACL to control Telnet users by specified source and destination IP addresses	acl <i>acl-number</i> { inbound outbound }	Required The inbound keyword specifies to filter the users trying to Telnet to the current switch. The outbound keyword specifies to filter users trying to Telnet to other switches from the current switch.

Controlling Telnet Users by Source MAC Addresses

Controlling Telnet users by source MAC addresses is achieved by applying Layer 2 ACLs, which are numbered from 4000 to 4999.

Table 32 Control Telnet users by source MAC addresses

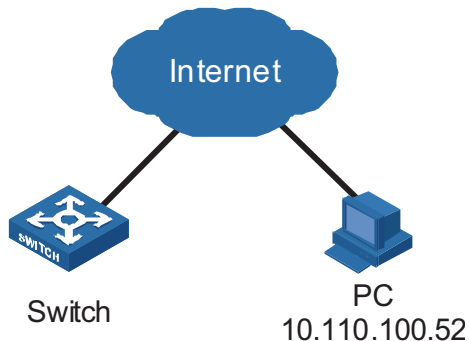
Operation	Command	Description
Enter system view	system-view	-
Create or enter Layer 2 ACL view	acl number <i>acl-number</i>	-
Define rules for the ACL	rule [<i>rule-id</i>] { deny permit } [<i>rule-string</i>]	Required You can define rules as needed to filter by specific source MAC addresses.
Quit to system view	quit	-

Table 32 Control Telnet users by source MAC addresses

Operation	Command	Description
Enter user interface view	user-interface [<i>type</i>] <i>first-number</i> [<i>last-number</i>]	-
Apply the ACL to control Telnet users by specified source MAC addresses	acl <i>acl-number</i> inbound	Required By default, no ACL is applied for Telnet users.

Configuration Example **Network requirements**

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

Network diagram**Figure 26** Network diagram for controlling Telnet users using ACLs**Configuration procedure**

Define a basic ACL.

```
<4210> system-view
[4210] acl number 2000
[4210-acl-basic-2000] rule 1 permit source 10.110.100.52 0
[4210-acl-basic-2000] quit
```

Apply the ACL.

```
[4210] user-interface vty 0 4
[4210-ui-vty0-4] acl 2000 inbound
```

Controlling Network Management Users by Source IP Addresses

You can manage a Switch 4210 through network management software. Network management users can access switches through SNMP.

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

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

Prerequisites

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

Controlling Network Management Users by Source IP Addresses

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

Table 33 Control network management users by source IP addresses

Operation	Command	Description
Enter system view	system-view	-
Create a basic ACL or enter basic ACL view	acl number <i>acl-number</i> [match-order { config auto }]	As for the acl number command, the config keyword is specified by default.
Define rules for the ACL	rule [<i>rule-id</i>] { deny permit } [<i>rule-string</i>]	Required
Quit to system view	quit	-
Apply the ACL while configuring the SNMP community name	snmp-agent community { read write } <i>community-name</i> [mib-view <i>view-name</i> acl <i>acl-number</i>]*	Optional By default, SNMPv1 and SNMPv2c use community name to access.
Apply the ACL while configuring the SNMP group name	snmp-agent group { v1 v2c } <i>group-name</i> [read-view <i>read-view</i>] [write-view <i>write-view</i>] [notify-view <i>notify-view</i>] [acl <i>acl-number</i>] snmp-agent group v3 <i>group-name</i> [authentication privacy] [read-view <i>read-view</i>] [write-view <i>write-view</i>] [notify-view <i>notify-view</i>] [acl <i>acl-number</i>]	Optional By default, the authentication mode and the encryption mode are configured as none for the group.
Apply the ACL while configuring the SNMP user name	snmp-agent usm-user { v1 v2c } <i>user-name</i> <i>group-name</i> [acl <i>acl-number</i>] snmp-agent usm-user v3 <i>user-name</i> <i>group-name</i> [cipher] [authentication-mode { md5 sha } <i>auth-password</i>] [privacy-mode des56] [priv-password] [acl <i>acl-number</i>]	Optional



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

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

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

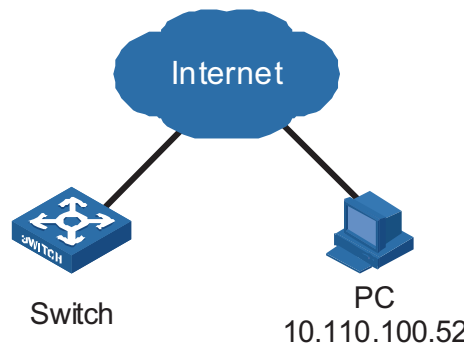
ACLs in the commands, the network management users are filtered by the SNMP group name and SNMP user name.

Configuration Example Network requirements

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

Network diagram

Figure 27 Network diagram for controlling SNMP users using ACLs



Configuration procedure

Define a basic ACL.

```
<4210> system-view
[4210] acl number 2000
[4210-acl-basic-2000] rule 1 permit source 10.110.100.52 0
[4210-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.

```
[4210] snmp-agent community read aaa acl 2000
[4210] snmp-agent group v2c groupa acl 2000
[4210] snmp-agent usm-user v2c usera groupa acl 2000
```

Controlling Web Users by Source IP Address

You can manage a Switch 4210 remotely through Web. Web users can access a switch through HTTP connections.

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

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

Prerequisites

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

Controlling Web Users by Source IP Addresses

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

Table 34 Control Web users by source IP addresses

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

Disconnecting a Web User by Force

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

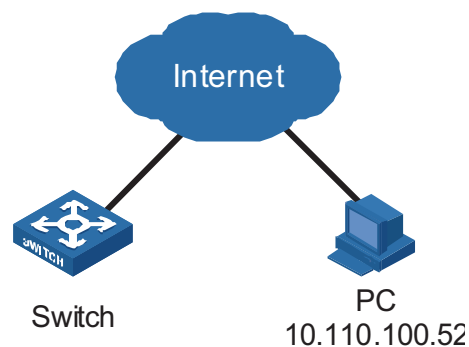
Table 35 Disconnect a Web user by force

Operation	Command	Description
Disconnect a Web user by force	free web-users { all user-id <i>user-id</i> user-name <i>user-name</i> }	Required Execute this command 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 28 Network diagram for controlling Web users using ACLs

Configuration procedure

Define a basic ACL.

```
<4210> system-view
[4210] acl number 2030
[4210-acl-basic-2030] rule 1 permit source 10.110.100.52 0
[4210-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.

```
[4210] ip http acl 2030
```


3

CONFIGURATION FILE MANAGEMENT

Introduction to Configuration File

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

Types of configuration

The configuration of a device falls into two types:

- Saved configuration, a configuration file used for initialization. If this file does not exist, the device starts up without loading any configuration file.
- Current configuration, which refers to the user's configuration during the operation of a device. When you make configuration changes to your switch, you are changing the current configuration. You must save these changes for them to be made permanent, as the current configuration resides in dynamic random-access memory (DRAM) and is lost when the switch is powered down or rebooted.

Format of configuration file

Configuration files are saved as text files for ease of reading. The saved configuration file has the file extension .cfg. The:

- Saved configuration in the form of commands.
- Save only non-default configuration settings.
- 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 "#".)
- 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 device. 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 device 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 device.

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 device, 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 .cfg 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, switch initializes with the default configuration file which ends in a .def file extension (e.g., 3comoscfg-26Port.def). This has factory-loaded default settings recommended by 3Com. There is a specific .def file for each switch type.

Management of Configuration File

If the default (.def) configuration file does not exist, the switch will come up with the switch internal defaults.

Table 36 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 device 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.

Table 37 Save current configuration

Operation	Command	Description
Save current configuration	save [<i>cfgfile</i>] [safely] [backup main]]	Required Available in any view

Modes in saving the configuration


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



CAUTION: The configuration file to be used for next startup may be lost if the device reboots or the power fails during the configuration file saving process. In this case, the device reboots without loading any configuration file. After the device reboots, you need to specify a configuration file for the next startup. Refer to “Specifying a Configuration File for the Next Startup ” on page 70 for details.

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 device.
 - 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 device.
 - 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.
-  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 device through commands. After you clear the configuration files, the device starts up without loading the configuration file the next time it is started up.

Table 38 Erase the configuration file

Operation	Command	Description
Erase the startup configuration file from the storage device	reset saved-configuration [backup main]	Required Available in user view

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

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

The following two situations exist:

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



CAUTION: *This command will permanently delete the configuration file from the device.*

Specifying a Configuration File for the Next Startup

Table 39 Specify a configuration file for next startup

Operation	Command	Description
Specify a configuration file for next startup	startup saved-configuration <i>cfgfile</i> [backup main]	Required Available in user view

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

Assign 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.

Assign 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 device.*

Displaying Device Configuration

After the above configuration, you can execute the **display** command in any view to display the current and initial configurations of the device, so as to verify your configuration.

Table 40 Display Device Configuration

Operation	Command	Description
Display the initial configuration file saved in the storage device	display saved-configuration [unit <i>unit-id</i>] [by-linenum]	
Display the configuration file used for this and next startup	display startup [unit <i>unit-id</i>]	
Display the current VLAN configuration of the device	display current-configuration vlan [<i>vlan-id</i>] [by-linenum]	
Display the validated configuration in current view	display this [by-linenum]	You can execute the display command in any view.
Display current configuration	display current-configuration [configuration [<i>configuration-type</i>]] [interface [<i>interface-type</i>] [<i>interface-number</i>]] [by-linenum] [] { begin include exclude } [<i>regular-expression</i>]	

4

VLAN OVERVIEW

VLAN Overview

Introduction to VLAN

The traditional Ethernet is a broadcast network, where all hosts are in the same broadcast domain and connected with each other through hubs or switches. Hubs and switches, which are the basic network connection devices, have limited forwarding functions.

- A hub is a physical layer device without the switching function, so it forwards the received packet to all ports except the inbound port of the packet.
- A switch is a link layer device which can forward a packet according to the MAC address of the packet. However, when the switch receives a broadcast packet or an unknown unicast packet whose MAC address is not included in the MAC address table of the switch, it will forward the packet to all the ports except the inbound port of the packet.

The above scenarios could result in the following network problems.

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

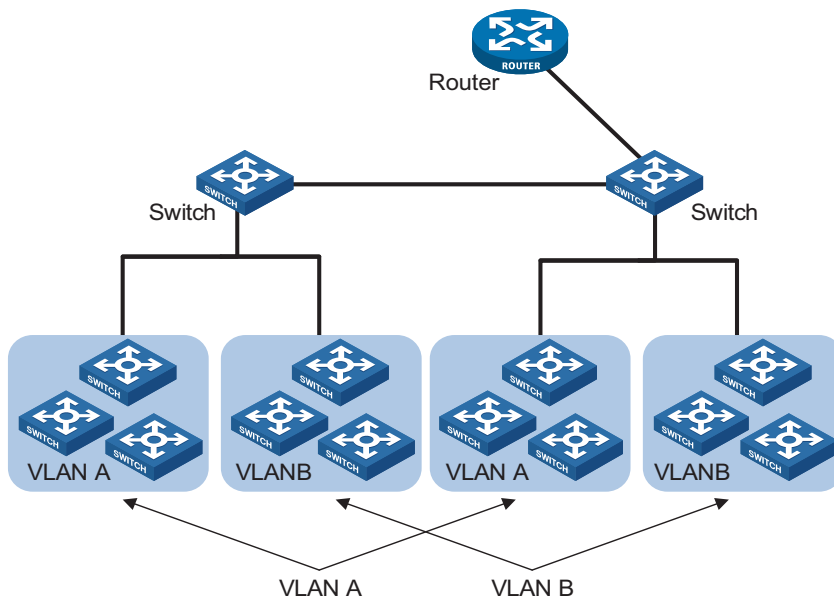
Isolating broadcast domains is the solution for the above problems. The traditional way is to use routers, which forward packets according to the destination IP address and does not forward broadcast packets in the link layer. However, routers are expensive and provide few ports, so they cannot split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

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

A VLAN can span across 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 29 illustrates a VLAN implementation.

Figure 29 A VLAN implementation



Advantages of VLANs

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

- Broadcasts are confined to VLANs. This decreases bandwidth consumption and improves network performance.
- Network security is improved. Because each VLAN forms a broadcast domain, hosts in different VLANs cannot communicate with each other directly unless routers or Layer 3 switches are used.
- A more flexible way to establish virtual workgroups. VLAN can be used to create a virtual workgroup spanning physical network segments. When the physical position of a host changes within the range of the virtual workgroup, the host can access the network without changing its network configuration.

VLAN Principles

VLAN tag

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

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

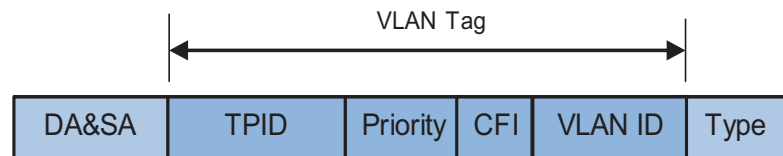
In traditional Ethernet data frames, the type field of the upper layer protocol is encapsulated after the destination MAC address and source MAC address, as shown in Figure 30.

Figure 30 Encapsulation format of traditional Ethernet frames



In Figure 30 DA refers to the destination MAC address, SA refers to the source MAC address, and Type refers to the upper layer protocol type of the packet. IEEE 802.1Q protocol defines that a 4-byte VLAN tag is encapsulated after the destination MAC address and source MAC address to show the information about VLAN.

Figure 31 Format of VLAN tag



As shown in Figure 31, a VLAN tag contains four fields, including the tag protocol identifier (TPID), priority, canonical format indicator (CFI), and VLAN ID.

- TPID is a 16-bit field, indicating that this data frame is VLAN-tagged. By default, it is 0x8100 in 3Com series Ethernet switches.
- Priority is a 3-bit field, referring to 802.1p priority. Refer to “QoS Configuration” on page 299 for details.
- CFI is a 1-bit field, indicating whether the MAC address is encapsulated in the standard format. 0 (the value of the CFI field) indicates the MAC address is encapsulated in the standard format and 1 indicates the MAC address is not encapsulated in the standard format. The value is 0 by default.
- VLAN ID is a 12-bit field, indicating the ID of the VLAN to which this packet belongs. It is in the range of 0 to 4,095. Generally, 0 and 4,095 is not used, so the field is in the range of 1 to 4,094.

VLAN ID identifies the VLAN to which a packet belongs. When 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.

MAC address learning mechanism of VLANs

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

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

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

Currently, the 3Com Switch 4210 Family adopts the IVL mode only. For more information about the MAC address forwarding table, refer to “MAC Address Table Management” on page 131.

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

The Switch 4210 currently supports 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. For details, refer to “Port Basic Configuration” on page 95.

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

5

VLAN CONFIGURATION

VLAN Configuration

VLAN Configuration Tasks

Table 41 VLAN configuration tasks

Configuration tasks	Description	Related section
Basic VLAN configuration	Required	"Basic VLAN Configuration"
Basic VLAN interface configuration	Optional	"Basic VLAN Interface Configuration"
Displaying VLAN configuration	Optional	"Displaying VLAN Configuration"

Basic VLAN Configuration

Table 42 Basic VLAN configuration

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



CAUTION:

- *VLAN 1 is the system default VLAN, which needs not to be created and cannot be removed, either.*

Basic VLAN Interface Configuration

Configuration prerequisites

Before configuring a VLAN interface, create the corresponding VLAN.

Configuration procedure

Table 43 Basic VLAN interface configuration

Operation	Command	Description
Enter system view	system-view	-
Create a VLAN interface and enter VLAN interface view	interface Vlan-interface <i>vlan-id</i>	Required By default, there is no VLAN interface on a switch.
Specify the description string for the current VLAN interface	description <i>text</i>	Optional By default, the description string of a VLAN interface is the name of this VLAN interface. "Vlan-interface1 Interface" for example.
Disable the VLAN interface	shutdown	Optional
Enable the VLAN Interface	undo shutdown	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). If you disable the VLAN interface, the VLAN interface will always be down, regardless of the status of the ports in the VLAN.



- *The operation of enabling/disabling a VLAN's VLAN interface does not influence the physical status of the Ethernet ports belonging to this VLAN.*
- *A Switch 4210 can be configured with a single VLAN interface only, and the VLAN must be the management VLAN. For details about the management VLAN, refer to "Managing the VLAN" on page 83.*

Displaying VLAN Configuration

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

Table 44 Display VLAN configuration

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

Configuring a Port-Based VLAN

Configuring a Port-Based VLAN

Configuration prerequisites

Create a VLAN before configuring a port-based VLAN.

Configuration procedure

Table 45 Configure a port-based VLAN

Operation	Command	Description
Enter system view	system-view	-
Enter VLAN view	vlan <i>vlan-id</i>	-
Add Ethernet ports to the specific VLAN	port <i>interface-list</i>	Required By default, all the ports belong to the default VLAN (VLAN 1).



CAUTION: The commands above are effective for access ports only. If you want to add trunk ports or hybrid ports to a VLAN, you need to use the **port trunk permit vlan** command or the **port hybrid vlan** command in Ethernet port view. For the configuration procedure, refer to "Ethernet Port Configuration" on page 96.

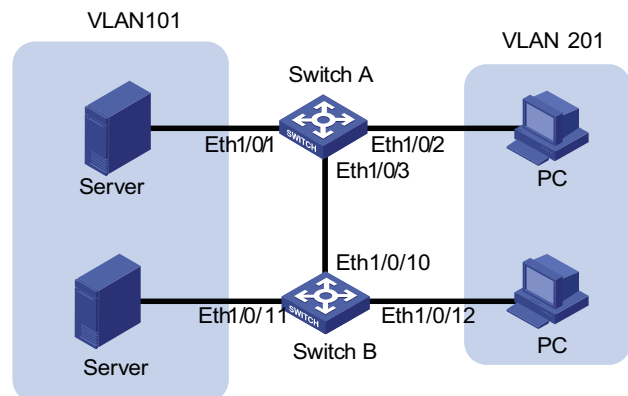
Port-Based VLAN Configuration Example

Network requirements

- As shown in Figure 32, 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 32 Network diagram for VLAN configuration



Configuration procedure

- Configure Switch A.

Create VLAN 101, specify its descriptive string as "DMZ", and add Ethernet1/0/1 to VLAN 101.

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

Create VLAN 201, and add Ethernet1/0/2 to VLAN 201.

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

- Configure Switch B.

Create VLAN 101, specify its descriptive string as "DMZ", and add Ethernet1/0/11 to VLAN 101.

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

Create VLAN 201, and add Ethernet1/0/12 to VLAN 201.

```
[SwitchB] vlan 201
[SwitchB-vlan201] port Ethernet 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 Ethernet1/0/3 of Switch A.

```
[SwitchA] interface Ethernet 1/0/3
[SwitchA-Ethernet1/0/3] port link-type trunk
[SwitchA-Ethernet1/0/3] port trunk permit vlan 101
[SwitchA-Ethernet1/0/3] port trunk permit vlan 201
```

Configure Ethernet1/0/10 of Switch B.

```
[SwitchB] interface Ethernet 1/0/10
[SwitchB-Ethernet1/0/10] port link-type trunk
[SwitchB-Ethernet1/0/10] port trunk permit vlan 101
[SwitchB-Ethernet1/0/10] port trunk permit vlan 201
```



For the command of configuring a port link type (**port link-type**) and the command of allowing packets of certain VLANs to pass through a port (**port trunk permit**), refer to “Ethernet Port Configuration” on page 96 .

6

MANAGING THE VLAN

VLAN Overview

To manage an Ethernet switch remotely through Telnet or the built-in Web server, the switch need to be assigned an IP address, and make sure that a route exists between the user and the switch. For the Switch 4210, only the management VLAN interface can be assigned an IP address.

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

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

The three ways of obtaining an IP address cannot be configured at the same time. That is, the latest IP address obtained causes the previously IP address to be released. For example, if you assign an IP address to a VLAN interface by using the corresponding commands and then apply for another IP address through BOOTP (using the **ip address bootp-alloc** command), the former OIP address will be released, and the final IP address of the VLAN interface is the one obtained through BOOTP.



For details of DHCP, refer to the DHCP module.

Static Route

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

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

Default Route

The switch uses the default route when it fails to find a matching entry in the routing table:

- If the destination address of a packet fails to match any entry in the routing table, the switch uses the default route;
- If no default route exists and the destination address of the packet is not in the routing table, the packet is discarded, and an ICMP destination unreachable message is returned to the source.

The default route can be configured through a static route and exists in the routing table as a route destined to the network 0.0.0.0 (with the mask 0.0.0.0).

Configuring VLAN Management

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

Overview

Table 46 Configure the management VLAN

Operation	Command	Remarks
Enter system view	system-view	-
Configure a specified VLAN to be the management VLAN	management-vlan <i>vlan-id</i>	Required. By default, VLAN 1 operates as the management VLAN.
Create the management VLAN interface and enter the corresponding VLAN interface view	interface vlan-interface <i>vlan-id</i>	Required
Assign an IP address to the management VLAN interface	ip address <i>ip-address mask</i>	Required. By default, no IP address is assigned to the management VLAN interface.
Configure a static route	ip route-static <i>ip-address</i> { <i>mask</i> <i>mask-length</i> } { <i>interface-type</i> <i>interface-number</i> <i>next-hop</i> } [preference <i>preference-value</i>] [reject blackhole] [description <i>text</i>]	Optional



Caution: To create the VLAN interface for the management VLAN on a switch operating as the management device in a cluster, make sure that the management VLAN ID is consistent with the cluster management VLAN ID configured with the `management-vlan vlan-id` command. Otherwise, the configuration fails. Refer to the *Cluster Operation Manual* for detailed introduction to the cluster. Refer to the *VLAN module* for detailed introduction to VLAN interfaces.

Configuration Example Network requirements

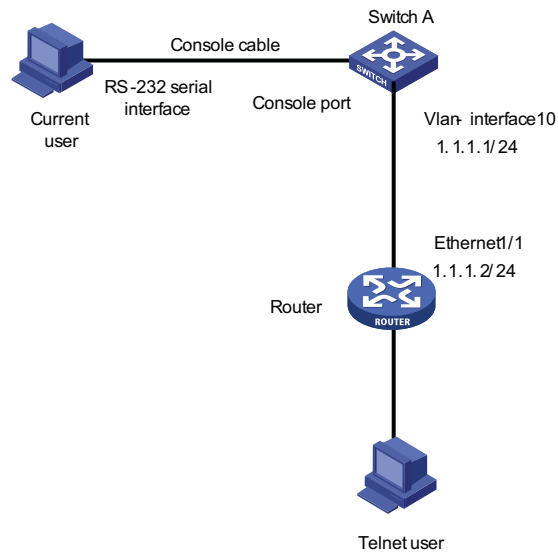
For a user to manage Switch A remotely through Telnet, these requirements are to be met: Switch A has an IP address, and the remote Telnet user is reachable.

You need to configure the switch as follows:

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

Network diagram

Figure 33 Network diagram for management VLAN configuration



Configuration procedure



Perform the following configurations after the current user logs in to Switch A through the Console port.

Enter system view.

```
<4210> system-view
```

Create VLAN 10 and configure VLAN 10 as the management VLAN.

```
[4210] vlan 10
[4210-vlan10] quit
[4210] management-vlan 10
```

Create the VLAN 10 interface and enter VLAN interface view.

```
[4210] interface vlan-interface 10
```

Configure the IP address of VLAN 10 interface as 1.1.1.1/24.

```
[4210-Vlan-interface10] ip address 1.1.1.1 255.255.255.0
[4210-Vlan-interface10] quit
```

Configure the default route.

```
[4210] ip route-static 0.0.0.0 0.0.0.0 1.1.1.2
```

Displaying and Maintaining management VLAN configuration

Table 1-2 Displaying and Maintaining management VLAN configuration

Table 47

Operation	Command	Remarks
Display the IP-related information about a management VLAN interface	display ip interface [Vlan-interface <i>vlan-id</i>]	Optional Available in any view.
Display brief configuration information about a management VLAN interface	display ip interface brief [Vlan-interface [<i>vlan-id</i>]]	
Display the information about a management VLAN interface	display interface [Vlan-interface [<i>vlan-id</i>]]	
Display summary information about the routing table	display ip routing-table [{ begin exclude include } <i>regular-expression</i>]	
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 <i>ip-address</i> [<i>mask</i>] [longer-match] [verbose]	
Display the routes leading to a specified IP address range	display ip routing-table <i>ip-address1 mask1 ip-address2 mask2</i> [verbose]	
Display the routing information of the specified protocol	display ip routing-table protocol <i>protocol</i> [inactive] [verbose]	
Display the routes that match a specified basic access control list (ACL)	display ip routing-table acl <i>acl-number</i> [verbose]	
Display the routing table in a tree structure	display ip routing-table radix	
Display the statistics on the routing table	display ip routing-table statistics	
Clear statistics about a routing table	reset ip routing-table statistics protocol { all <i>protocol</i> }	Use the reset command in user view.
Delete all static routes	delete static-routes all	Use the delete command in system view.

7

IP ADDRESSING CONFIGURATION

IP Addressing Overview

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

Each IP address breaks down into two parts:

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

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

Figure 34 IP address classes

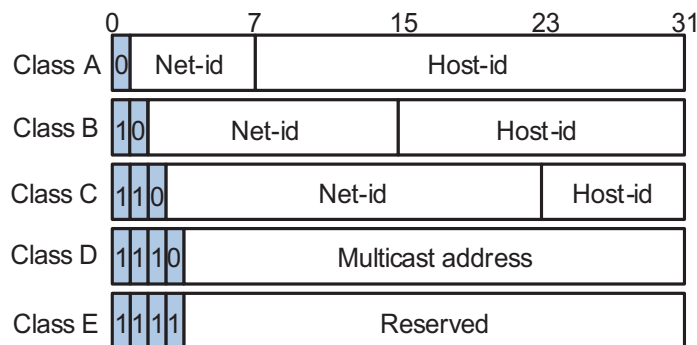


Table 48 describes the address ranges of these five classes. Currently, the first three classes of IP addresses are used in quantity.

Table 48 IP address classes and ranges

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

Special Case IP Addresses

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

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

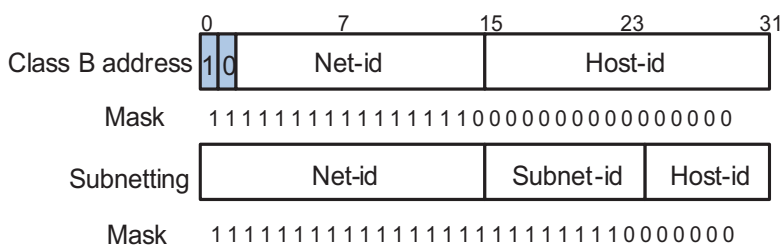
Subnetting and Masking

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

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

Figure 35 shows how a Class B network is subnetted.

Figure 35 Subnet a Class B network



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

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

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

Configuring IP Addresses

Switch 4210 Family support assigning IP addresses to VLAN interfaces and loopback interfaces. Besides directly assigning an IP address to a VLAN interface, you may configure a VLAN interface to obtain an IP address through BOOTP or DHCP as alternatives. If you change the way an interface obtains an IP address, from manual assignment to BOOTP for example, the IP address obtained from BOOTP will overwrite the old one manually assigned.



This chapter only covers how to assign an IP address manually. For the other two approaches to IP address assignment, refer to "DHCP Overview" on page 281 and subsequent chapters.

Table 49 Configure an IP address to an interface

Operation	Command	Remarks
Enter system view	system-view	--
Enter interface view	interface <i>interface-type</i> <i>interface-number</i>	--
Assign an IP address to the Interface	ip address <i>ip-address</i> { <i>mask</i> <i>mask-length</i> } [sub]	Required No IP address is assigned by default.



- *A newly specified IP address overwrites the previous one if there is any.*
- *The IP address of a VLAN interface must not be on the same network segment as that of a loopback interface on a device.*

Displaying IP Addressing Configuration

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

Table 50 Display IP addressing configuration

Operation	Command	Remarks
Display information about a specified or all Layer 3 interfaces	display ip interface [<i>interface-type</i> [<i>interface-number</i>]	Available in any view
Display brief configuration information about a specified or all Layer 3 interfaces	display ip interface brief [<i>interface-type</i> [<i>interface-number</i>]]	

IP Address Configuration Examples

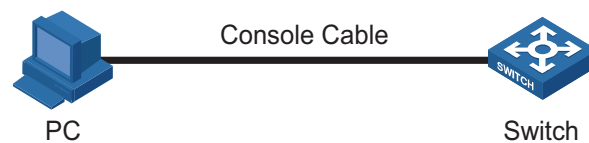
IP Address Configuration Example I

Network requirement

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

Network diagram

Figure 36 Network diagram for IP address configuration



Configuration procedure

Configure an IP address for VLAN interface 1.

```
<4210> system-view
[4210] interface Vlan-interface 1
[4210-Vlan-interface1] ip address 129.2.2.1 255.255.255.0
```


8

IP PERFORMANCE CONFIGURATION

IP Performance Overview

Introduction to IP Performance Configuration

In some network environments, you need to adjust the IP parameters to achieve best network performance. The IP performance configuration supported by Switch 4210 Family includes:

- Configuring TCP attributes
- Disabling ICMP to send error packets

Introduction to the Forwarding Table

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

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

When the switch is running normally, the contents of the FIB and the routing table are the same.

Configuring IP Performance

Introduction to IP Performance Configuration Tasks

Table 51 Introduction to IP performance configuration tasks

Configuration task	Description	Related section
Configure TCP attributes	Optional	"Configuring TCP Attributes"
Disable ICMP to send error packets	Optional	"Disabling ICMP to Send Error Packets"

Configuring TCP Attributes

TCP optional parameters that can be configured include:

- synwait timer: When sending a SYN packet, TCP starts the synwait timer. If no response packets are received before the synwait timer times out, the TCP connection is not successfully created.
- finwait timer: When the TCP connection is changed into FIN_WAIT_2 state, finwait timer will be started. If no FIN packets are received within the timer timeout, the TCP connection will be terminated. If FIN packets are received, the TCP connection state changes to TIME_WAIT. If non-FIN packets are received,

the system restarts the timer from receiving the last non-FIN packet. The connection is broken after the timer expires.

- Size of TCP receive/send buffer

Table 52 Configure TCP attributes

Operation	Command	Remarks
Enter system view	system-view	-
Configure TCP synwait timer's timeout value	tcp timer syn-timeout <i>time-value</i>	Optional By default, the timeout value is 75 seconds.
Configure TCP finwait timer's timeout value	tcp timer fin-timeout <i>time-value</i>	Optional By default, the timeout value is 675 seconds.
Configure the size of TCP receive/send buffer	tcp window <i>window-size</i>	Optional By default, the buffer is 8 kilobytes.

Disabling ICMP to Send Error Packets

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

By default, Switch 4210 Family support sending ICMP redirect and destination unreachable 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 receiving a lot of malicious packets that cause it to send ICMP error packets, the device's performance will be reduced.
- As the ICMP redirection function increases the routing table size of a host, the host's performance will be reduced if its routing table becomes very large.
- If a host sends malicious ICMP destination unreachable packets, end users may be affected.

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

Table 53 Disable sending ICMP error packets

Operation	Command	Remarks
Enter system view	system-view	-
Disable sending ICMP redirects	undo icmp redirect send	Required Enabled by default
Disable sending ICMP destination unreachable packets	undo icmp unreach send	Required Enabled by default

Displaying and Maintaining IP Performance Configuration

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

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

Table 54 Display and maintain IP performance

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

9

PORT BASIC CONFIGURATION

Ethernet Port Overview

Link Types of Ethernet Ports

An Ethernet port on an Switch 4210 can be of the following three link types.

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



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

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

Configuring the Default VLAN ID for an Ethernet Port

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

After you configure default VLAN IDs for Ethernet ports, the packets passing through the ports are processed in different ways depending on different situations. See Table 55 for details.

Table 55 Processing of incoming/outgoing packets

Processing of an incoming packet			
Port type	If the packet does not carry a VLAN tag	If the packet carries a VLAN tag	Processing of an outgoing packet
Access	Receive the packet and add the default tag to the packet.	<ul style="list-style-type: none"> If the VLAN ID is just the default VLAN ID, receive the packet. If the VLAN ID is not the default VLAN ID, discard the packet. 	Deprive the tag from the packet and send the packet.
Trunk		<ul style="list-style-type: none"> If the VLAN ID is just the default VLAN ID, receive the packet. If the VLAN ID is not the default VLAN ID but is one of the VLAN IDs allowed to pass through the port, receive the packet. 	<ul style="list-style-type: none"> If the VLAN ID is just the default VLAN ID, deprive the tag and send the packet. If the VLAN ID is not the default VLAN ID, keep the original tag unchanged and send the packet.
Hybrid		<ul style="list-style-type: none"> If the VLAN ID is neither the default VLAN ID, nor one of the VLAN IDs allowed to pass through the port, discard the packet. 	Send the packet if the VLAN ID is allowed to pass through the port. Use the port hybrid vlan command to configure whether the port tags the packet when sending a packet in this VLAN (including default VLAN).



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

Adding an Ethernet Port to Specified VLANs

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

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



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

Ethernet Port Configuration

Initially Configuring a Port

Table 56 Initially configure a port

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

Table 56 Initially configure a port

Operation	Command	Remarks
Enable the Ethernet port	undo shutdown	Optional By default, the port is enabled. Use the shutdown command to disable the port.
Set the description string for the Ethernet port	description text	Optional By default, the description string of an Ethernet port is null.
Set the duplex mode of the Ethernet port	duplex { auto full half }	Optional By default, the duplex mode of the port is auto (auto-negotiation).
Set the speed of the Ethernet port	speed { 10 100 1000 auto }	Optional <ul style="list-style-type: none"> ■ By default, the speed of an Ethernet port is determined through auto-negotiation (the auto keyword). ■ Use the 1000 keyword for Gigabit Ethernet ports only.
Set the medium dependent interface (MDI) mode of the Ethernet port	mdi { across auto normal }	Optional By default, the MDI mode of an Ethernet port is auto .

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**.

Table 57 Configure auto-negotiation speeds for a port

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

Table 57 Configure auto-negotiation speeds for a port

Operation	Command	Remarks
Configure the available auto-negotiation speed(s) for the port	speed auto [10 100 1000]*	Optional <ul style="list-style-type: none"> By default, the port speed is determined through auto-negotiation. Use the 1000 keyword for Gigabit Ethernet ports only.



- Only ports on the front panel of the device support the auto-negotiation speed configuration feature. And ports on the extended interface card do not support this feature currently.
- After you configure auto-negotiation speed(s) for a port, if you execute the **undo speed** command or the **speed auto** command, the auto-negotiation speed setting of the port restores to the default setting.
- The effect of executing **speed auto 10 100 1000** equals to that of executing **speed auto**, that is, the port is configured to support all the auto-negotiation speeds: 10 Mbps, 100 Mbps, and 1000 Mbps.

Limiting Traffic on Individual Ports

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

Table 58 Limit traffic on port

Operation	Command	Remarks
Enter system view	system-view	-
Limit broadcast traffic received on each port	broadcast-suppression <i>ratio</i>	Optional By default, the switch does not suppress broadcast traffic.
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	-
Limit broadcast traffic received on the current port	broadcast-suppression { <i>ratio</i> bps <i>max-bps</i> }	Optional By default, the switch does not suppress broadcast traffic.
Limit unknown multicast and unknown unicast traffic received on the current port	multicast-suppression { <i>ratio</i> bps <i>max-bps</i> }	Optional The switch will suppress the unknown multicast and unknown unicast traffic simultaneously after the configuration. By default, the switch does not suppress unknown multicast and unknown unicast 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.

Table 59 Enable flow control on a port

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

Configuring an Access Port

Table 60 Configure access port attribute

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

Configuring a Hybrid Port

Table 61 Configure hybrid port attribute

Operation	Command	Remarks
Enter system view	system-view	-
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	-
Set the link type of the port to hybrid	port link-type hybrid	Required
Set the default VLAN ID for the port	port hybrid pvid vlan <i>vlan-id</i>	Optional If no default VLAN ID is set for a hybrid port, VLAN 1 (system default VLAN) is used as the default VLAN of the port.
Add the port to specified VLANs	port hybrid vlan <i>vlan-id-list</i> { tagged untagged }	Optional The tagged/untagged keyword specifies to keep/remove the VLAN tags carried in the packets of specific VLANs when the packets are forwarded through the port.

Configuring a Trunk Port

Table 62 Configure trunk port attribute

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

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. For the detailed copy content, refer to the Switch 4210 Family Command Reference Guide.

Table 63 Duplicate the configuration of a port to specific ports

Operation	Command	Remarks
Enter system view	system-view	-
Duplicate the configuration of a port to specific ports	copy configuration source { <i>interface-type</i> <i>interface-number</i> aggregation-group <i>source-agg-id</i> } destination { <i>interface-list</i> [aggregation-group <i>destination-agg-id</i>] aggregation-group <i>destination-agg-id</i> }	Required



- 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.

Table 64 Configure loopback detection for an Ethernet port

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

**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.

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.

Table 65 Enable loopback test

Operation	Command	Remarks
Enter system view	system-view	-
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	-
Enable loopback test	loopback { external internal }	Optional



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

Note that:

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

Enabling the System to Test a Connected Cable

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

Table 66 Enable the system to test connected cables

Operation	Command	Remarks
Enter system view	system-view	-
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	-
Enable the system to test connected cables	virtual-cable-test	Required



- *Currently, the device is only capable of testing the cable status and cable length. For the testing items that are currently not supported, "-" is displayed in the corresponding fields of the virtual-cable-test command.*
- *Cable test cannot be performed on an optical port.*

Configuring the Interval to Perform Statistical Analysis on Port Traffic

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

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

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

Table 67 Set the interval to perform statistical analysis on port traffic

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

Disabling Up/Down Log Output on a Port

An Ethernet port has two physical link statuses: UP and Down. When the physical link status of an Ethernet port changes, the switch will send log to the log server, which in turn acts accordingly. If the status of Ethernet ports in a network changes frequently, large amount of log information may be sent, which increases work load of the log server and consumes more network resources.

You can limit the amount of the log information sent to the log server by disabling the Up/Down log output function on Ethernet ports.



After you allow a port to output the Up/Down log information, if the physical link status of the port does not change, the switch does not send log information to the log server but monitors the port in real time.

Disable Up/Down log output on a port

Table 68 Disable UP/Down log output on a port

Operation	Command	Remarks
Enter system view	system-view	-
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	-
Disable a port from outputting UP/Down Log Information	undo enable log updown	Required

By default, UP/Down log information output is enabled.

Configuration example

By default, a port is allowed to output the Up/Down log information. Execute the **shutdown** command or the **undo shutdown** command on Ethernet 1/0/1, and the system outputs Up/Down log information of Ethernet 1/0/1.

```
<4210> system-view
System View: return to User View with Ctrl+Z.
[4210] interface Ethernet 1/0/1
[4210-Ethernet1/0/1] shutdown
%Apr 5 07:25:37:634 2000 4210 L2INF/5/PORT LINK STATUS CHANGE:- 1 -
Ethernet1/0/1 is DOWN
[4210-Ethernet1/0/1] undo shutdown
%Apr 5 07:25:56:244 2000 4210 L2INF/5/PORT LINK STATUS CHANGE:- 1 -
Ethernet1/0/1 is UP
```

After you disable Ethernet 1/0/1 from outputting Up/Down log information and execute the **shutdown** command or the **undo shutdown** command on Ethernet 1/0/1, no Up/Down log information is output for Ethernet 1/0/1.

```
[4210-Ethernet1/0/1] undo enable log updown
[4210-Ethernet1/0/1] shutdown
[4210-Ethernet1/0/1] undo shutdown
```

Displaying and Maintaining Basic Port Configuration

Table 69 Display and maintain basic port configuration

Operation	Command	Remarks
Display port configuration information	display interface [<i>interface-type</i> <i>interface-type interface-number</i>]	You can execute the display commands in any view.
Display information about SFP module on a specified port	display transceiver-information interface <i>interface-type interface-number</i>	
Display the enable/disable status of port loopback detection	display loopback-detection	
Display brief information about port configuration	display brief interface [<i>interface-type</i> [<i>interface-number</i>]] [{ begin include exclude } <i>regular-expression</i>]	
Display the ports that are of a specific type	display port { hybrid trunk combo }	
Display port information about a specified unit	display unit <i>unit-id interface</i>	
Clear port statistics	reset counters interface [<i>interface-type</i> <i>interface-type interface-number</i>]	You can execute the reset command in user view. After 802.1x is enabled on a port, clearing the statistics on the port will not work.

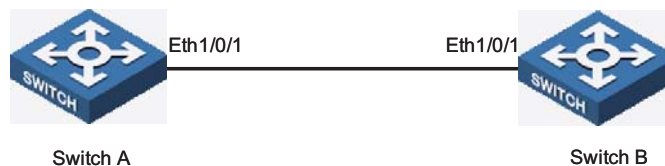
Ethernet Port Configuration Example

Network requirements

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

Network diagram

Figure 37 Network diagram for Ethernet port configuration



Configuration procedure



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

Enter Ethernet 1/0/1 port view.

```
<4210> system-view
[4210] interface ethernet1/0/1
```

Set Ethernet 1/0/1 as a trunk port.

```
[4210-Ethernet1/0/1] port link-type trunk
```

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

```
[4210-Ethernet1/0/1] port trunk permit vlan 2 6 to 50 100
```

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

```
[4210-Ethernet1/0/1] port trunk pvid vlan 100
```

Troubleshooting Ethernet Port Configuration

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

Solution: Take the following steps.

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

10

LINK AGGREGATION CONFIGURATION

Overview

Introduction to Link Aggregation

Link aggregation can aggregate multiple Ethernet ports together to form a logical aggregation group. To upper layer entities, all the physical links in an aggregation group are a single logical link.

Link aggregation is designed to increase bandwidth by implementing outgoing/incoming load sharing among the member ports in an aggregation group. Link aggregation group also allows for port redundancy, which improves connection reliability.

Introduction to LACP

Link aggregation control protocol (LACP) is designed to implement dynamic link aggregation and deaggregation. This protocol is based on IEEE802.3ad and uses link aggregation control protocol data units (LACPDU) to interact with its peer.

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.

Operation key is generated by the system. It is determined by port settings such as port speed, duplex state, basic configuration, and so on.

- Selected ports in a manual aggregation group or a static aggregation group have the same operation key.
- Member ports in a dynamic aggregation group have the same operation key.

Requirements on Ports for Link Aggregation

To achieve outgoing/incoming load sharing in an aggregation group, the following configuration of the member ports must be the same: STP, QoS, VLAN, port attributes, as described below.

- STP configuration, including STP status (enabled or disabled), link attribute (point-to-point or not), STP priority, STP path cost, STP packet format, loop guard status, root guard status, edge port or not.
- QoS configuration, including traffic limit, 802.1p priority, and so on.
- VLAN configuration, including permitted VLANs, and default VLAN ID.
- Port attribute configuration, including port rate, duplex mode, and link type (trunk, hybrid, or access).

Link Aggregation Classification

Depending on different aggregation modes, the following three types of link aggregation exist:

- Manual aggregation
- Static LACP aggregation
- Dynamic LACP aggregation

Manual Aggregation Group

Introduction to manual aggregation group

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

LACP is disabled on the member ports of manual aggregation groups, and you cannot enable LACP on ports in a manual aggregation group.

Port status in manual aggregation group

A port in a manual aggregation group can be in one of the two states: selected or unselected. In a manual aggregation group, only the selected ports can forward user service packets.

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

- Among the ports in an aggregation group that are in up state, the system determines the master port with one of the following settings being the highest (in descending order) as the master port: full duplex/high speed, full duplex/low speed, half duplex/high speed, half duplex/low speed. The ports with their rate, duplex mode and link type being the same as that of the master port are selected ports, and the rest are unselected ports.
- The system sets the ports unable to aggregate with the master port (due to some hardware limit) 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.

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 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 ports unable to aggregate with the master port (due to some hardware limit) 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. A port can participate in dynamic link aggregation only when it is LACP-enabled. Ports can be aggregated into a dynamic aggregation group only when they are connected to the same peer device and have the same basic configuration (such as rate and duplex mode).

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

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.



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, 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 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.

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.

Table 70 Configure a manual aggregation group

Operation	Command	Remarks
Enter system view	system-view	-
Create a manual aggregation group	link-aggregation group <i>agg-id mode manual</i>	Required
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	-
Add the Ethernet port to the aggregation group	port link-aggregation group <i>agg-id</i>	Required

Note that:

- 1 When creating an aggregation group:
 - If the aggregation group you are creating already exists but contains no port, its type will change to the type you set.
 - If the aggregation group you are creating already exists and contains ports, the possible type changes may be: changing from dynamic or static to manual, and changing from dynamic to static; and no other kinds of type change can occur.
 - When you change a dynamic/static group to a manual group, the system will automatically disable LACP on the member ports. When you change a dynamic group to a static group, the system will remain the member ports LACP-enabled.
- 2 When a manual or static aggregation group contains only one port, you cannot remove the port unless you remove the whole aggregation group.

Configuring a Static LACP Aggregation Group

You can create a static LACP aggregation group, or remove an existing static LACP aggregation group (after that, the system will re-aggregate the original member ports in the group to form one or multiple dynamic aggregation groups.).

For a static aggregation group, a port can only be manually added/removed to/from the static aggregation group.



When you add an LACP-enabled port to a manual aggregation group, the system will automatically disable LACP on the port. Similarly, when you add an LACP-disabled port to a static aggregation group, the system will automatically enable LACP on the port.

Table 71 Configure a static LACP aggregation group

Operation	Command	Remarks
Enter system view	system-view	-
Create a static aggregation group	link-aggregation group <i>agg-id mode static</i>	Required

Table 71 Configure a static LACP aggregation group

Operation	Command	Remarks
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	-
Add the port to the aggregation group	port link-aggregation group <i>agg-id</i>	Required



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.



You cannot enable LACP on a port which is already in a manual aggregation group.

Table 72 Configure a dynamic LACP aggregation group

Operation	Command	Remarks
Enter system view	system-view	-
Configure the system priority	lacp system-priority <i>system-priority</i>	Optional By default, the system priority is 32,768.
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	-
Enable LACP on the port	lacp enable	Required By default, LACP is disabled on a port.
Configure the port priority	lacp port-priority <i>port-priority</i>	Optional By default, the port priority is 32,768.



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

Perform the following tasks to configure a description for an aggregation group.

Table 73 Configure a description for an aggregation group

Operation	Command	Remarks
Enter system view	system-view	-

Table 73 Configure a description for an aggregation group

Operation	Command	Remarks
Configure a description for an aggregation group	link-aggregation group <i>agg-id</i> description <i>agg-name</i>	Optional By default, no description is configured for an aggregation group.



CAUTION: If you have saved the current configuration with the **save** command, after system reboot, the configuration concerning manual and static aggregation groups and their descriptions still exists, but that of dynamic aggregation groups and their descriptions gets lost.

Displaying and Maintaining Link Aggregation Configuration

After the above configuration, you can execute the **display** command in any view to display the running status after the link aggregation configuration and verify your configuration. Execute the **reset** command in user view to clear LACP statistics on ports.

Table 74 Display and maintain link aggregation configuration

Operation	Command	Remarks
Display summary information of all aggregation groups	display link-aggregation summary	Available in any view
Display detailed information of a specific aggregation group or all aggregation groups	display link-aggregation verbose [<i>agg-id</i>]	
Display link aggregation details of a specified port or port range	display link-aggregation interface <i>interface-type</i> <i>interface-number</i> [to <i>interface-type</i> <i>interface-number</i>]	
Display local device ID	display lacp system-id	
Clear LACP statistics about a specified port or port range	reset lacp statistics [interface <i>interface-type</i> <i>interface-number</i> [to <i>interface-type</i> <i>interface-number</i>]]	Available in user view

Link Aggregation Configuration Example

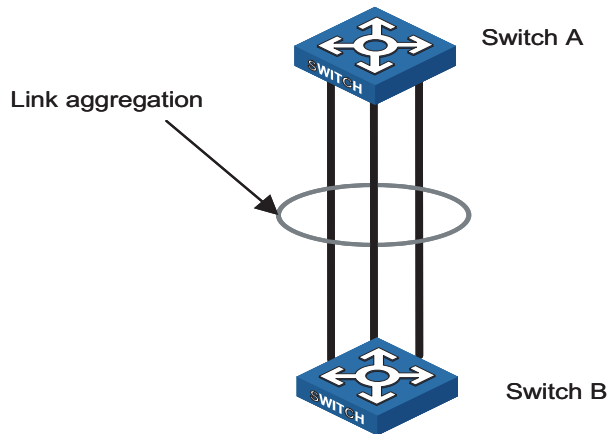
Ethernet Port Aggregation Configuration Example

Network requirements

- Switch A connects to Switch B with three ports Ethernet1/0/1 to Ethernet1/0/3. It is required that incoming/outgoing load between the two switches can be shared among the three ports.
- Adopt three different aggregation modes to implement link aggregation on the three ports between switch A and B.

Network diagram

Figure 38 Network diagram for link aggregation configuration



Configuration procedure



The following example only lists the configuration required on Switch A; you must perform the same configuration procedure on Switch B to implement link aggregation.

1 Adopting manual aggregation mode

Create manual aggregation group 1.

```
<4210> system-view
[4210] link-aggregation group 1 mode manual
```

Add Ethernet1/0/1 through Ethernet1/0/3 to aggregation group 1.

```
[[4210] interface Ethernet1/0/1
[4210-Ethernet1/0/1] port link-aggregation group 1
[4210-Ethernet1/0/1] quit
[4210] interface Ethernet1/0/2
[4210-Ethernet1/0/2] port link-aggregation group 1
[4210-Ethernet1/0/2] quit
[4210] interface Ethernet1/0/3
[4210-Ethernet1/0/3] port link-aggregation group 1
```

2 Adopting static LACP aggregation mode

Create static aggregation group 1.

```
<4210> system-view
[4210] link-aggregation group 1 mode static
```

Add Ethernet1/0/1 through Ethernet1/0/3 to aggregation group 1.

```
[4210] interface Ethernet1/0/1
[4210-Ethernet1/0/1] port link-aggregation group 1
[4210-Ethernet1/0/1] quit
[4210] interface Ethernet1/0/2
[4210-Ethernet1/0/2] port link-aggregation group 1
[4210-Ethernet1/0/2] quit
[4210] interface Ethernet1/0/3
```

```
[4210-Ethernet1/0/3] port link-aggregation group 1
```

3 Adopting dynamic LACP aggregation mode

Enable LACP on Ethernet1/0/1 through Ethernet1/0/3.

```
<4210> system-view
[4210] interface Ethernet1/0/1
[4210-Ethernet1/0/1] lacp enable
[4210-Ethernet1/0/1] quit
[4210] interface Ethernet1/0/2
[4210-Ethernet1/0/2] lacp enable
[4210-Ethernet1/0/2] quit
[4210] interface Ethernet1/0/3
[4210-Ethernet1/0/3] lacp enable
```



CAUTION: *The three LACP-enabled ports can be aggregated into one dynamic aggregation group to implement load sharing only when they have the same basic configuration (such as rate, duplex mode, and so on).*

11

PORT ISOLATION CONFIGURATION

Port Isolation Overview

Through the port isolation feature, you can add the ports to be controlled into an isolation group to isolate the Layer 2 and Layer 3 data between each port in the isolation group. Thus, you can construct your network in a more flexible way and improve your network security.

Currently, you can create only one isolation group on the Switch 4210. This feature is also known as a Protected Port or an Isolated Port. The number of Ethernet ports in an isolation group is not limited.



- 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 ports to an isolation group, thus isolating Layer 2 and Layer 3 data among the ports in the isolation group.

Table 75 Configure port isolation

Operation	Command	Description
Enter system view	system-view	-
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	-
Add the Ethernet port to the isolation group	port isolate	Required By default, an isolation group contains no port.



- When a member port of an aggregation group joins/leaves an isolation group, the other ports in the same aggregation group on the local device 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 a port of an isolation group to an aggregation group causes all the ports in the aggregation group being added to the isolation group.

Displaying Port Isolation Configuration

After the above configuration, you can execute the **display** command in any view to display the result of your port isolation configuration, thus verifying your configuration.

Table 76 Display port isolation configuration

Operation	Command	Description
Display information about the Ethernet ports added to the isolation group	display isolate port	You can execute the display command in any view.

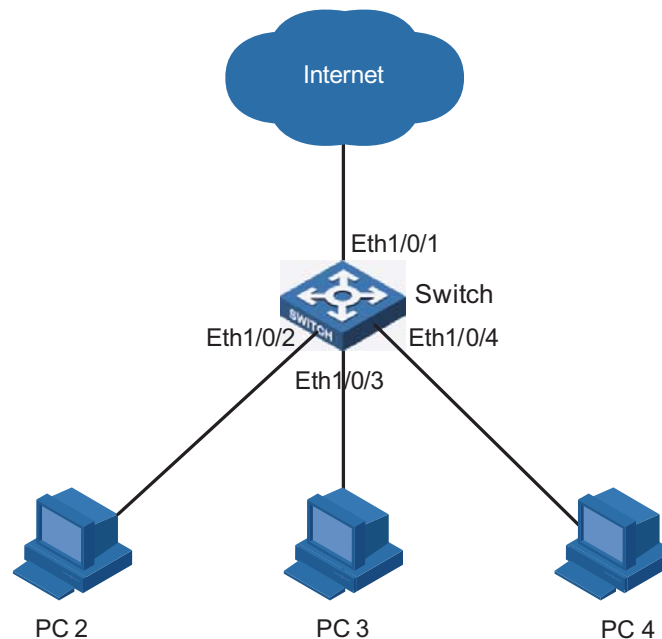
Port Isolation Configuration Example

Network requirements

- PC2, PC3 and PC4 connect to the switch ports Ethernet1/0/2, Ethernet1/0/3, and Ethernet1/0/4 respectively.
- The switch connects to the Internet through Ethernet1/0/1.
- It is desired that PC2, PC3 and PC4 are isolated from each other so that they cannot communicate with each other.

Network diagram

Figure 39 Network diagram for port isolation configuration



Configuration procedure

Add Ethernet1/0/2, Ethernet1/0/3, and Ethernet1/0/4 to the isolation group.

```

<4210> system-view
System View: return to User View with Ctrl+Z.
[4210] interface ethernet1/0/2
[4210-Ethernet1/0/2] port isolate
[4210-Ethernet1/0/2] quit
[4210] interface ethernet1/0/3
[4210-Ethernet1/0/3] port isolate
[4210-Ethernet1/0/3] quit
  
```

```
[4210] interface ethernet1/0/4  
[4210-Ethernet1/0/4] port isolate  
[4210-Ethernet1/0/4] quit  
[4210] quit
```

Display information about the ports in the isolation group.

```
<4210> display isolate port  
Isolated port(s) on UNIT 1:  
Ethernet1/0/2, Ethernet1/0/3, Ethernet1/0/4
```


12

PORT SECURITY CONFIGURATION

Port Security Overview

Introduction Port security is a security mechanism for network access control. It brings together both 802.1x access control and MAC address authentication and allows for combinations of these technologies.

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, the Trap feature enables the switch to send Trap messages to help the network administrator monitor special activities.

Port Security Modes Table 77 describes the available port security modes:

Table 77 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	<p>In this mode, the port automatically learns MAC addresses and changes them to security MAC addresses.</p> <p>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.</p> <p>After the port security mode is changed to the secure mode, only those packets whose source MAC addresses are security MAC addresses learned can pass through the port.</p>	In either mode, the device will trigger NTK and intrusion protection upon detecting an illegal packet.
secure	<p>In this mode, the port is disabled from learning MAC addresses.</p> <p>Only those packets whose source MAC addresses are security MAC addresses learned and static MAC addresses can pass through the port.</p>	
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.

Table 77 Description of port security modes

Security mode	Description	Feature
userLoginSecure	<p>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.</p> <p>In this mode, only one 802.1x-authenticated user is allowed to access the port.</p> <p>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.</p>	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	<p>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.</p> <p>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.</p>	
macAddressWithRadius	In this mode, MAC address-based authentication is performed for access users.	
macAddressOrUserLoginSecure	<p>In this mode, a port performs MAC authentication or 802.1x authentication of an access user. If either authentication succeeds, the user is authenticated.</p> <p>In this mode, there can be only one authenticated user on the port.</p>	
macAddressOrUserLoginSecureExt	This mode is similar to the macAddressOrUserLoginSecure mode, except that there can be more than one authenticated user on the port.	

Table 77 Description of port security modes

Security mode	Description	Feature
macAddressElseUserLoginSecure	MAC authentication is performed first on the access user. If the MAC authentication succeeds, the access user has the accessibility; otherwise, 802.1x authentication is performed on the access user. In this mode, there can be only one authenticated user on the port.	
macAddressElseUserLoginSecureExt	This mode is similar to the macAddressElseUserLoginSecure mode, except that there can be more than one authenticated user on the port.	
macAddressAndUserLoginSecure	To perform 802.1x authentication on the access user, MAC authentication must be performed first. 802.1x authentication can be performed on the access user only if MAC authentication succeeds. In this mode there can be only one authenticated user on the port.	
macAddressAndUserLoginSecureExt	This mode is similar to the macAddressAndUserLoginSecure mode, except that there can be more than one authenticated user on the port.	



- When the port operates in the **userlogin-withouti** mode, Intrusion Protection will not be triggered even if the OUI address does not match.
- In the **macAddressElseUserLoginSecure** or **macAddressElseUserLoginSecureExt** security mode, the MAC address of a user failing MAC authentication is set as a quiet MAC address. If the user initiates 802.1x authentication during the quiet period, the switch does not authenticate the user.

Port Security Configuration

Table 78 Port security configuration tasks

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 "Configuring intrusion protection" Choose one or more features as required. "Configuring the Trap feature"
"Ignoring the Authorization Information from the RADIUS Server"	Optional

Table 78 Port security configuration tasks

Task	Remarks
"Configuring Security MAC Addresses"	Optional

Enabling Port Security

Before enabling port security, you need to disable 802.1x and MAC authentication globally.

Table 79 Enable port security

Operation	Command	Remarks
Enter system view	system-view	-
Enable port security	port-security enable	Required Disabled by default



CAUTION: Enabling port security resets the following configurations on 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.



- For details about 802.1x configuration, refer to "802.1x Configuration" on page 211 and "System-Guard Configuration" on page 235.
- For details about MAC Authentication configuration, refer to "MAC Authentication Configuration" on page 269.

**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 learned by a port in MAC address management.

Table 80 Set the maximum number of MAC addresses allowed on a port

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

Table 80 Set the maximum number of MAC addresses allowed on a port

Operation	Command	Remarks
Set the maximum number of MAC addresses allowed on the port	port-security max-mac-count <i>count-value</i>	Required Not limited by default



- Assume that, in the **macAddressOrUserLoginSecureExt** port security mode, you have configured to allow up to n authenticated users to access the network. When all of these n authenticated users are connected to the network and one or more of them are MAC-authenticated, to perform 802.1x authentication on the MAC-authenticated user(s), the number of maximum MAC addresses allowed on the port must be set to $n + 1$. Similarly, in the case of the **macAddressOrUserLoginSecure** security mode, the maximum number of MAC addresses allowed on the port must be set to 2.
- In the **macAddressAndUserLoginSecureExt** port security mode, to allow up to n authenticated users to be connected to the network at the same time and the n th user to be 802.1x-authenticated, the maximum number of MAC addresses allowed on the port must be set to at least $n + 1$. Similarly, in the case of the **macAddressAndUserLoginSecure** security mode, the maximum number of MAC addresses allowed on the port must be set to 2.

Setting the Port Security Mode

Table 81 Set the port security mode

Operation	Command	Remarks
Enter system view	system-view	-
Set the OUI value for user authentication	port-security oui <i>OUI-value</i> index <i>index-value</i>	Optional In userLoginWithOUI mode, a port supports one 802.1x user plus one user whose source MAC address has a specified OUI value.
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	-
Set the port security mode	port-security port-mode { autolearn mac-and-userlogin-secure mac-and-userlogin-secure-ext mac-authentication mac-else-userlogin-secure mac-else-userlogin-secure-ext secure userlogin userlogin-secure userlogin-secure-ext userlogin-secure-or-mac userlogin-secure-or-mac-ext userlogin-withoui }	Required By default, a port operates in noRestriction mode. In this mode, access to the port is not restricted. You can set a port security mode as needed.



- 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

Table 82 Configure the NTK feature

Operation	Command	Remarks
Enter system view	system-view	-
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	-
Configure the NTK feature	port-security ntk-mode { ntkonly ntk-withbroadcasts ntk-withmulticasts }	Required By default, NTK is disabled on a port, namely all frames are allowed to be sent.

Configuring intrusion protection

Table 83 Configure the intrusion protection feature

Operation	Command	Remarks
Enter system view	system-view	-
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	-
Set the corresponding action to be taken by the switch when intrusion protection is triggered	port-security intrusion-mode { blockmac disableport disableport-temporarily}	Required By default, intrusion protection is disabled.
Return to system view	quit	-
Set the timer during which the port remains disabled	port-security timer disableport timer	Optional 20 seconds by default



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

Table 84 Configure port security trapping

Operation	Command	Remarks
Enter system view	system-view	-
Enable sending traps for the specified type of event	port-security trap { addresslearned dot1xlogfailure dot1xlogoff dot1xlogon intrusion ralmlogfailure ralmlogoff ralmlogon }	Required By default, no trap is sent.

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.

Table 85 Configure a port to ignore the authorization information from the RADIUS server

Operation	Command	Remarks
Enter system view	system-view	-
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	-
Ignore the authorization information from the RADIUS server	port-security authorization ignore	Required By default, a port uses the authorization information from the RADIUS server.

Configuring 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**.



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.

Before continuing, make sure that:

- 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**.

Table 86 Configure a security MAC address

Operation	Command	Remarks
Enter system view	system-view	-
Add a security MAC address	In system view mac-address security <i>mac-address interface</i> <i>interface-type</i> <i>interface-number</i> vlan <i>vlan-id</i>	Either is required. By default, no security MAC address is configured.
	In Ethernet port view interface <i>interface-type</i> <i>interface-number</i> mac-address security <i>mac-address</i> vlan <i>vlan-id</i>	

Displaying Port Security Configuration

After the above configuration, you can use the **display** command in any view to display port security information and verify your configuration.

Table 87 Display port security configuration

Operation	Command	Remarks
Display information about port security configuration	display port-security [interface <i>interface-list</i>]	You can execute the display command in any view.
Display information about security MAC address configuration	display mac-address security [interface <i>interface-type</i> <i>interface-number</i>] [vlan <i>vlan-id</i>] [count]	

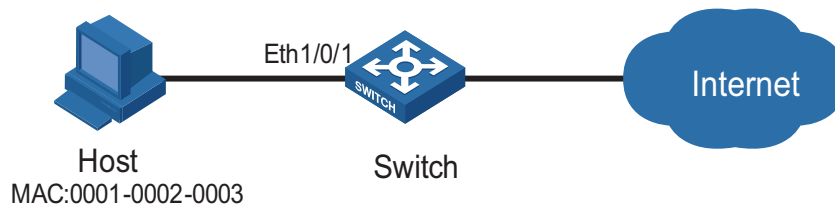
Port Security Configuration Example

Port Security Configuration Example

Network requirements

Implement access user restrictions through the following configuration on Ethernet1/0/1 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 40** Network diagram for port security configuration**Configuration procedure**

Enter system view.

```
<4210> system-view
```

Enable port security.

```
[4210] port-security enable
```

Enter Ethernet1/0/1 port view.

```
[4210] interface Ethernet1/0/1
```

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

```
[4210-Ethernet1/0/1] port-security max-mac-count 80
```

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

```
[4210-Ethernet1/0/1] 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.

```
[4210-Ethernet1/0/1] mac-address security 0001-0002-0003 vlan 1
```

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

```
[4210-Ethernet1/0/1] port-security intrusion-mode disableport-temporarily
```

```
[4210-Ethernet1/0/1] quit
```

```
[4210]port-security timer disableport 30
```


13

MAC ADDRESS TABLE MANAGEMENT



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 “Multicast Overview” on page 185.

Introduction to the 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 41, User A and User B are both in VLAN 1. When User A communicates with User B, the packet from User A needs to be transmitted to Ethernet 1/0/1. At this time, the switch records the source MAC address of the

packet, that is, the address "MAC-A" of User A to the MAC address table of the switch, forming an entry shown in Figure 42.

Figure 41 MAC address learning diagram (1)

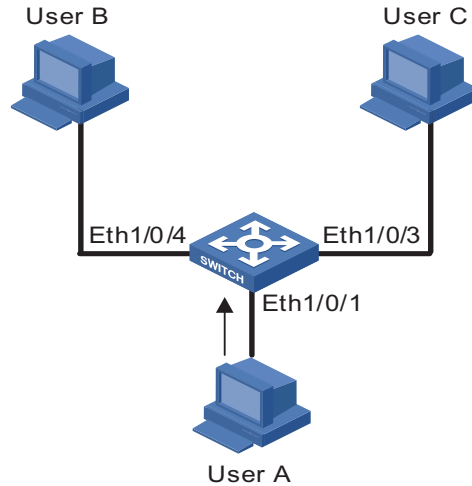
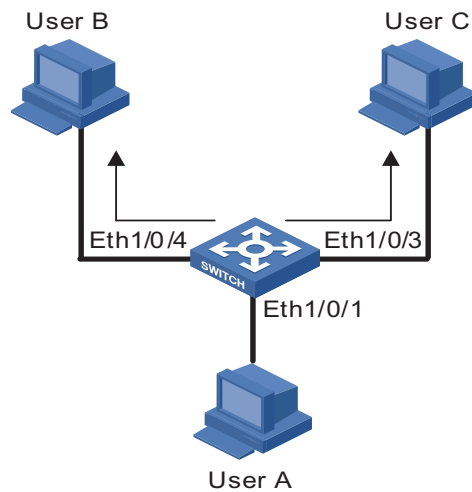


Figure 42 MAC address table entry of the switch (1)

MAC-address	Port	VLAN ID
MAC-A	Ethernet1/0/1	1

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

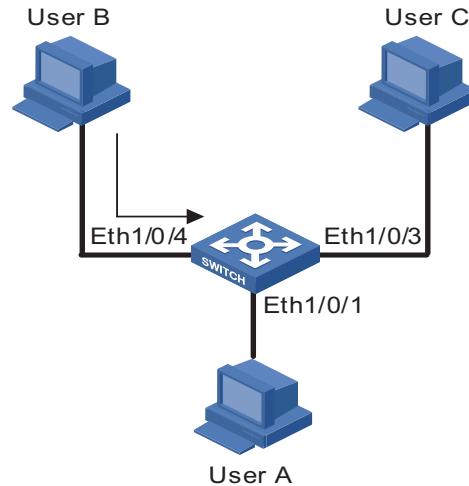
Figure 43 MAC address learning diagram (2)



- 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 44. When the response packet from User B is sent to Ethernet 1/0/4, the

switch records the association between the MAC address of User B and the corresponding port to the MAC address table of the switch.

Figure 44 MAC address learning diagram (3)



- 4 At this time, the MAC address table of the switch includes two forwarding entries shown in Figure 45. When forwarding the response packet, the switch unicasts the packet instead of broadcasting it to User A through Ethernet 1/0/1, because MAC-A is already in the MAC address table.

Figure 45 MAC address table entries of the switch (2)

MAC-address	Port	VLAN ID
MAC-A	Ethernet1/0/1	1
MAC-B	Ethernet1/0/4	1

- 5 After this interaction, the switch directly unicasts the communication packets between User A and User B based on the corresponding MAC address table entries.



- 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.



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 88 lists the different types of MAC address entries and their characteristics.

Table 88 Characteristics of different types of MAC address entries

MAC address entry	Configuration method	Aging time	Reserved or not at reboot (if the configuration is saved)
Static MAC address entry	Manually configured	Unavailable	Yes
Dynamic MAC address entry	Manually configured or generated by MAC address learning mechanism	Available	No
Blackhole MAC address entry	Manually configured	Unavailable	Yes

Configuring MAC Address Table Management

MAC Address Table Management Configuration Tasks

Table 89 Configure MAC address table management

Operation	Description	Related section
Configure a MAC address entry	Required	"Configuring a MAC Address Entry".
Set the aging time of MAC address entries	Optional	"Setting the Aging Time of MAC Address Entries".
Set the maximum number of MAC addresses a port can learn	Optional	"Setting the Maximum Number of MAC Addresses a Port Can Learn".

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 90 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 } <i>mac-address interface interface-type interface-number</i> vlan <i>vlan-id</i>	Required



CAUTION:

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

Adding a MAC address entry in Ethernet port view

Table 91 Add a MAC address entry in Ethernet port view

Operation	Command	Description
Enter system view	system-view	-
Enter Ethernet port view	interface <i>interface-type interface-number</i>	-
Add a MAC address entry	mac-address { static dynamic blackhole } <i>mac-address</i> vlan <i>vlan-id</i>	Required



CAUTION:

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

Setting the 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 92 Set aging time of MAC address entries

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

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.



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 93 Set the maximum number of MAC addresses a port can learn

Operation	Command	Description
Enter system view	system-view	-
Enter Ethernet port view	interface interface-type interface-number	-
Set the maximum number of MAC addresses the port can learn	mac-address max-mac-count count	Required By default, the number of the MAC addresses a port can learn is not limited.

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 94 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 Ethernet 1/0/2. To prevent the switch from broadcasting packets destined for the server, it is required to add the MAC address of the server to the MAC address table of the switch, which then forwards packets destined for the server through Ethernet 1/0/2.

- The MAC address of the server is 000f-e20f-dc71.
- Port Ethernet 1/0/2 belongs to VLAN 1.

Configuration procedure

Enter system view.

```
<4210> system-view
[4210]
```

Add a MAC address, with the VLAN, ports, and states specified.

```
[4210] mac-address static 000f-e20f-dc71 interface Ethernet 1/0/2 vlan 1
```

Display information about the current MAC address table.

```
[4210] display mac-address interface Ethernet 1/0/2
MAC ADDR          VLAN ID STATE          PORT INDEX          AGING TIME(s)
000f-e20f-dc71    1          Config static      Ethernet1/0/2      NOAGED
000f-e20f-a7d6    1          Learned            Ethernet1/0/2      300
000f-e20f-b1fb    1          Learned            Ethernet1/0/2      300
000f-e20f-f116    1          Learned            Ethernet1/0/2      300
--- 4 mac address(es) found on port Ethernet1/0/2 ---
```


14

MSTP CONFIGURATION

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 along 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 Table 95 for the description of designated bridge and designated port.

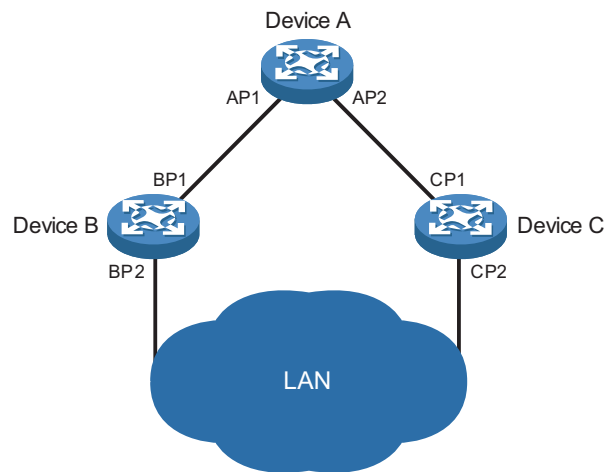
Table 95 Designated bridge and designated port

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 46 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 46 A schematic diagram of designated bridges and designated ports



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.



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 96 Selection of the optimum configuration BPDU

Step	Description
1	<p>Upon receiving a configuration BPDU on a port, the device performs the following processing:</p> <ul style="list-style-type: none"> ■ If the received configuration BPDU has a lower priority than that of the configuration BPDU generated by the port, the device will discard the received configuration BPDU without doing any processing on the configuration BPDU of this port. ■ If the received configuration BPDU has a higher priority than that of the configuration BPDU generated by the port, the device will replace the content of the configuration BPDU generated by the port with the content of the received configuration BPDU.
2	The device compares the configuration BPDUs of all the ports and chooses the optimum configuration BPDU.



Principle for configuration BPDU comparison:

- *The configuration BPDU that has the lowest root bridge ID has the highest priority.*
- *If all the 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 97 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. <ul style="list-style-type: none"> ■ The root bridge ID is replaced with that of the configuration BPDU of the root port. ■ The root path cost is replaced with that of the configuration BPDU of the root port plus the path cost corresponding to the root port. ■ The designated bridge ID is replaced with the ID of this device. ■ The designated port ID is replaced with the ID of this port.
3	The device compares the calculated configuration BPDU with the configuration BPDU on the port whose role is to be determined, and acts as follows based on the comparison result: <ul style="list-style-type: none"> ■ If the calculated configuration BPDU is superior, this port will serve as the designated port, and the configuration BPDU on the port will be replaced with the calculated configuration BPDU, which will be sent out periodically. ■ If the configuration BPDU on the port is superior, the device stops updating the configuration BPDUs of the port and blocks the port, so that the port only receives configuration BPDUs, but does not forward data or send configuration BPDUs.

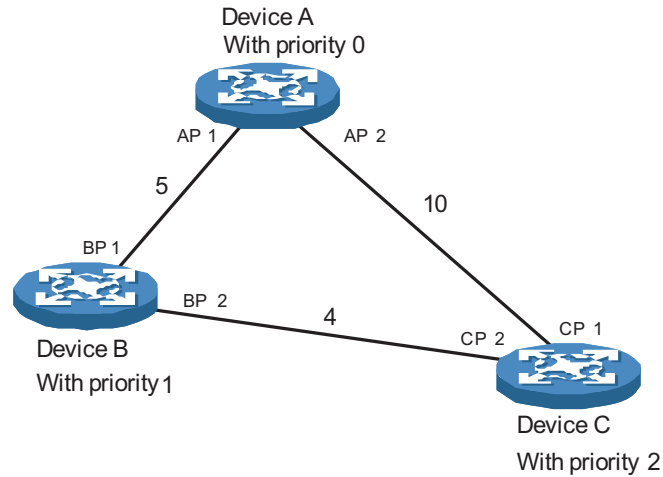


When the network topology is stable, only the root port and designated ports forward traffic, while other ports are all in the blocked state - they only receive STP packets but do not forward user traffic.

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 47. 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 47 Network diagram for STP algorithm



- Initial state of each device

The following table shows the initial state of each device.

Table 98 Initial state of each device

Device	Port name	BPDU of port
Device A	AP1	{0, 0, 0, AP1}
	AP2	{0, 0, 0, AP2}
Device B	BP1	{1, 0, 1, BP1}
	BP2	{1, 0, 1, BP2}
Device C	CP1	{2, 0, 2, CP1}
	CP2	{2, 0, 2, CP2}

- Comparison process and result on each device

The following table shows the comparison process and result on each device.

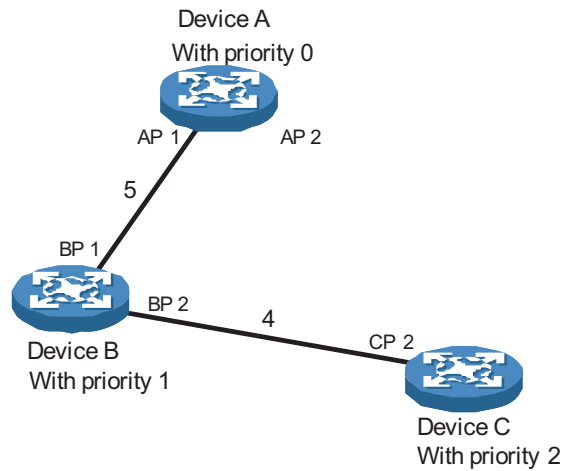
Table 99 Comparison process and result on each device

Device	Comparison process	BPDU of port after comparison
Device A	<ul style="list-style-type: none"> ■ Port AP1 receives the configuration BPDU of Device B {1, 0, 1, BP1}. Device A finds that the configuration BPDU of the local port {0, 0, 0, AP1} is superior to the configuration received message, and discards the received configuration BPDU. ■ Port AP2 receives the configuration BPDU of Device C {2, 0, 2, CP1}. Device A finds that the BPDU of the local port {0, 0, 0, AP2} is superior to the received configuration BPDU, and discards the received configuration BPDU. ■ Device A finds that both the root bridge and designated bridge in the configuration BPDUs of all its ports are Device A itself, so it assumes itself to be the root bridge. In this case, it does not make any change to the configuration BPDU of each port, and starts sending out configuration BPDUs periodically. 	AP1: {0, 0, 0, AP1} AP2: {0, 0, 0, AP2}
Device B	<ul style="list-style-type: none"> ■ Port BP1 receives the configuration BPDU of Device A {0, 0, 0, AP1}. Device B finds that the received configuration BPDU is superior to the configuration BPDU of the local port {1, 0, 1, BP1}, and updates the configuration BPDU of BP1. ■ Port BP2 receives the configuration BPDU of Device C {2, 0, 2, CP2}. Device B finds that the configuration BPDU of the local port {1, 0, 1, BP2} is superior to the received configuration BPDU, and discards the received configuration BPDU. ■ Device B compares the configuration BPDUs of all its ports, and determines that the configuration BPDU of BP1 is the optimum configuration BPDU. Then, it uses BP1 as the root port, the configuration BPDUs of which will not be changed. ■ Based on the configuration BPDU of BP1 and the path cost of the root port (5), Device B calculates a designated port configuration BPDU for BP2 {0, 5, 1, BP2}. ■ Device B compares the calculated configuration BPDU {0, 5, 1, BP2} with the configuration BPDU of BP2. If the calculated BPDU is superior, BP2 will act as the designated port, and the configuration BPDU on this port will be replaced with the calculated configuration BPDU, which will be sent out periodically. 	BP1: {0, 0, 0, AP1} BP2: {1, 0, 1, BP2} Root port BP1: {0, 0, 0, AP1} Designated port BP2: {0, 5, 1, BP2}

Table 99 Comparison process and result on each device

Device	Comparison process	BPDU of port after comparison
Device C	<ul style="list-style-type: none"> ■ Port CP1 receives the configuration BPDU of Device A {0, 0, 0, AP2}. Device C finds that the received configuration BPDU is superior to the configuration BPDU of the local port {2, 0, 2, CP1}, and updates the configuration BPDU of CP1. ■ Port CP2 receives the configuration BPDU of port BP2 of Device B {1, 0, 1, BP2} before the message was updated. Device C finds that the received configuration BPDU is superior to the configuration BPDU of the local port {2, 0, 2, CP2}, and updates the configuration BPDU of CP2. <p>By comparison:</p> <ul style="list-style-type: none"> ■ The configuration BPDUs of CP1 is elected as the optimum configuration BPDU, so CP1 is identified as the root port, the configuration BPDUs of which will not be changed. ■ Device C compares the calculated designated port configuration BPDU {0, 10, 2, CP2} with the configuration BPDU of CP2, and CP2 becomes the designated port, and the configuration BPDU of this port will be replaced with the calculated configuration BPDU. ■ Next, port CP2 receives the updated configuration BPDU of Device B {0, 5, 1, BP2}. Because the received configuration BPDU is superior to its old one, Device C launches a BPDU update process. ■ At the same time, port CP1 receives configuration BPDUs periodically from Device A. Device C does not launch an update process after comparison. <p>By comparison:</p> <ul style="list-style-type: none"> ■ Because the root path cost of CP2 (9) (root path cost of the BPDU (5) + path cost corresponding to CP2 (4)) is smaller than the root path cost of CP1 (10) (root path cost of the BPDU (0) + path cost corresponding to CP2 (10)), the BPDU of CP2 is elected as the optimum BPDU, and CP2 is elected as the root port, the messages of which will not be changed. ■ After comparison between the configuration BPDU of CP1 and the calculated designated port configuration BPDU, port CP1 is blocked, with the configuration BPDU of the port remaining unchanged, and the port will not receive data from Device A until a spanning tree calculation process is triggered by a new condition, for example, the link from Device B to Device C becomes down. 	<p>CP1: {0, 0, 0, AP2}</p> <p>CP2: {1, 0, 1, BP2}</p> <p>Root port CP1: {0, 0, 0, AP2}</p> <p>Designated port CP2: {0, 10, 2, CP2}</p> <p>CP1: {0, 0, 0, AP2}</p> <p>CP2: {0, 5, 1, BP2}</p> <p>Blocked port CP2: {0, 0, 0, AP2}</p> <p>Root port CP2: {0, 5, 1, BP2}</p>

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 48.

Figure 48 The final calculated spanning tree

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 send out its better configuration BPDU in response.
- If a path becomes faulty, the root port on this path will no longer receive new configuration BPDUs and the old configuration BPDUs will be discarded due to timeout. In this case, the device generates configuration BPDUs with itself as the root bridge and sends configuration BPDUs and TCN BPDUs. This triggers a new spanning tree calculation so that a new path is established to restore the network connectivity.

However, the newly calculated configuration BPDU will not be propagated throughout the network immediately, so the old root ports and designated ports that have not detected the topology change continue forwarding data through the old path. If the new root port and designated port begin to forward data as soon as they are elected, a temporary loop may occur.

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.



- *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.

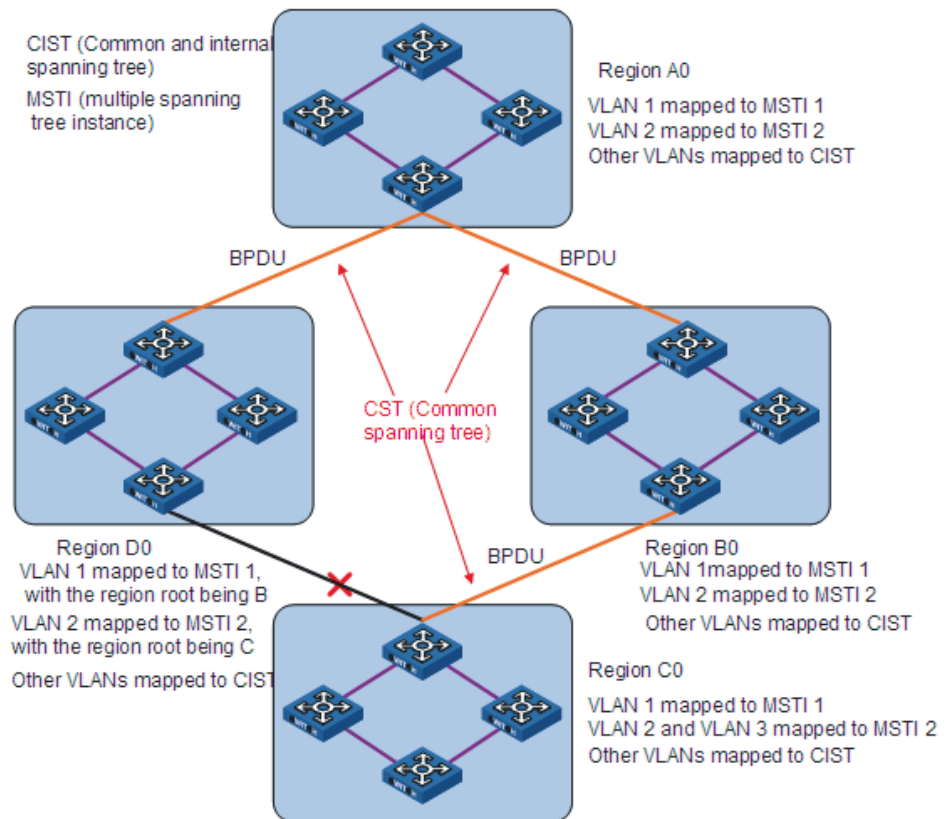
MSTP features the following:

- MSTP supports mapping VLANs to MST instances by means of a VLAN-to-instance 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 49 illustrates basic MSTP terms (assuming that MSTP is enabled on each switch in this figure).

Figure 49 Basic MSTP terminologies



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 49, 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 instance 2, and the other VLANs are mapped to CIST.)
- MSTP revision level (not shown in Figure 49)

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 49 contains multiple spanning trees known as MSTIs. Each of these spanning trees corresponds to a VLAN.

VLAN mapping table

A VLAN mapping table is a property of an MST region. It contains information about how VLANs are mapped to MSTIs. For example, in Figure 49, the VLAN mapping table of region A0 is: VLAN 1 is mapped to MSTI 1; VLAN 2 is mapped to MSTI 2; and other VLANs are mapped to CIST. In an MST region, load balancing is implemented according to the VLAN mapping table.

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 49, 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 49, 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 49, 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 49 is a switch in region A0.

Port role

During MSTP calculation, the following port roles exist: root port, designated port, master port, region edge port, alternate port, and backup port.

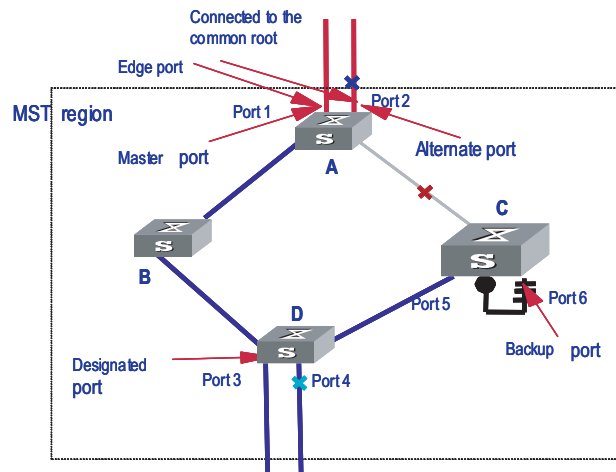
- A root port is used to forward packets to the root.
- A designated port is used to forward packets to a downstream network segment or switch.
- A master port connects an MST region to the common root. The path from the master port to the common root is the shortest path between the MST region and the common root.
- A region edge port is located on the edge of an MST region and is used to connect one MST region to another MST region, an STP-enabled region or an RSTP-enabled region
- An alternate port is a 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 50, 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.



- *A port can play different roles in different MSTIs.*
- *The role a region edge port plays is consistent with the role it plays in the CIST. For example, port 1 on switch A in Figure 50 is a region edge port, and it is a master port in the CIST. So it is a master port in all MSTIs in the region.*

Figure 50 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.
- Discarding state. Ports in this state can only receive BPDU packets.

Port roles and port states are not mutually dependent. Table 100 lists possible combinations of port states and port roles.

Table 100 Combinations of port states and port roles

Port role/ Port state	Root/ port/Master port	Designated port	Region edge port	Alternate port	Backup port
Forwarding	,X	,X	,X	-	-
Learning	,X	,X	,X	-	-
Discarding	,X	,X	,X	,X	,X

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)
 - 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:
(Instance bridge ID, Internal path costs, Designated bridge ID, ID of sending port, ID of receiving port)
 - 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 series switches also provide the following functions for users to manage their switches.

- Root bridge hold
- Root bridge backup
- Root guard
- BPDU guard
- Loop guard
- TC-BPDU attack guard
- BPDU packet drop

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

Table 101 lists the tasks to configure a root bridge.

Table 101 Configure a root bridge

Operation	Description	Related section
Enable MSTP	Required To prevent network topology jitter caused by other related configurations, you are recommended to enable MSTP after other related configurations are performed.	"Enabling MSTP"
Configure an MST region	Required	"Configuring an MST Region"
Specify the current switch as a root bridge/secondary root bridge	Required	"Specifying the Current Switch as a Root Bridge/Secondary Root Bridge"
Configure the bridge priority of the current switch	Optional The priority of a switch cannot be changed after the switch is specified as the root bridge or a secondary root bridge.	"Configuring the Bridge Priority of the Current Switch"
Configure the mode a port recognizes and sends MSTP packets	Optional	"Configuring the Mode a Port Recognizes and Sends MSTP Packets"
Configure the MSTP operation mode	Optional	"Configuring the MSTP Operation Mode"
Configure the maximum hop count of an MST region	Optional	"Configuring the Maximum Hop Count of an MST Region"
Configure the network diameter of the switched network	Optional The default value is recommended.	"Configuring the Network Diameter of the Switched Network"
Configure the MSTP time-related parameters	Optional The default values are recommended.	"Configuring the MSTP Time-related Parameters"
Configure the timeout time factor	Optional	"Configuring the Timeout Time Factor"
Configure the maximum transmitting speed of the port	Optional The default value is recommended.	"Configuring the Maximum Transmitting Speed on the Current Port"
Configure the current port as an edge port	Optional	"Configuring the Current Port as an Edge Port"
Specify whether the link connected to a port is a point-to-point link	Optional	"Specifying Whether the Link Connected to a Port Is Point-to-point Link"



In a network containing switches with both GVRP and MSTP enabled, GVRP packets are forwarded along the CIST. If you want to advertise packets of a specific VLAN through GVRP, be sure to map the VLAN to the CIST when configuring the MSTP VLAN mapping table (the CIST of a network is spanning tree instance 0).

Configuration Prerequisites

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

Configuring an MST Region

Configuration procedure

Table 102 Configure an MST region

Operation	Command	Description
Enter system view	system-view	-
Enter MST region view	stp region-configuration	-
Configure the name of the MST region	region-name <i>name</i>	Required The default MST region name of a switch is its MAC address.
Configure the VLAN mapping table for the MST region	instance <i>instance-id</i> vlan <i>vlan-list</i> vlan-mapping modulo <i>modulo</i>	Required Both commands can be used to configure VLAN mapping tables. By default, all VLANs in an MST region are mapped to spanning tree instance 0.
Configure the MSTP revision level for the MST region	revision-level <i>level</i>	Required The default revision level of an MST region is level 0.
Activate the configuration of the MST region manually	active region-configuration	Required
Display the configuration of the current MST region	check region-configuration	Optional
Display the currently valid configuration of the MST region	display stp region-configuration	You can execute this command in any view.



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

Configuring MST region-related parameters (especially the VLAN mapping table) results in spanning tree recalculation and network topology jitter. To reduce network topology jitter caused by the configuration, MSTP does not recalculate spanning trees immediately after the configuration; it does this only after you perform one of the following operations, and then the configuration can really take effect:

- Activate the new MST region-related settings by using the **active region-configuration** command
- Enable MSTP by using the **stp enable** command



Switches belong to the same MST region only when they have the same MST region name, VLAN mapping table, and MSTP revision level.

Configuration example

Configure an MST region, with the name being "info", the MSTP revision level being level 1, VLAN 2 through VLAN 10 being mapped to spanning tree instance 1, and VLAN 20 through VLAN 30 being mapped to spanning tree 2.

```
<4210> system-view
[4210] stp region-configuration
[4210-mst-region] region-name info
[4210-mst-region] instance 1 vlan 2 to 10
```

```
[4210-mst-region] instance 2 vlan 20 to 30
[4210-mst-region] revision-level 1
[4210-mst-region] active region-configuration
```

Verify the above configuration.

```
[4210-mst-region] check region-configuration
Admin configuration
  Format selector      :0
  Region name         :info
  Revision level      :1

Instance   Vlans Mapped
  0         11 to 19, 31 to 4094
  1         1 to 10
  2         20 to 30
```

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

Table 103 Specify the current switch as the root bridge of a spanning tree

Operation	Command	Description
Enter system view	system-view	-
Specify the current switch as the root bridge of a spanning tree	stp [instance <i>instance-id</i>] root primary [bridge-diameter <i>bridgenumber</i> [hello-time <i>centi-seconds</i>]]	Required

Specify the current switch as the secondary root bridge of a spanning tree

Table 104 Specify the current switch as the secondary root bridge of a spanning tree

Operation	Command	Description
Enter system view	system-view	-
Specify the current switch as the secondary root bridge of a specified spanning tree	stp [instance <i>instance-id</i>] root secondary [bridge-diameter <i>bridgenumber</i> [hello-time <i>centi-seconds</i>]]	Required

Using the **stp root primary/stp root secondary** command, you can specify the current switch as the root bridge or the secondary root bridge of the spanning tree instance identified by the *instance-id* argument. If the value of the *instance-id* argument is set to 0, the **stp root primary/stp root secondary** command specify the current switch as the root bridge or the secondary root bridge of the CIST.

A switch can play different roles in different spanning tree instances. That is, it can be the root bridges in a spanning tree instance and be a secondary root bridge in another spanning tree instance at the same time. But in the same spanning tree instance, a switch cannot be the root bridge and the secondary root bridge simultaneously.

When the root bridge fails or is turned off, the secondary root bridge becomes the root bridge if no new root bridge is configured. If you configure multiple secondary root bridges for a spanning tree instance, the one with the smallest MAC address replaces the root bridge when the latter fails.

You can specify the network diameter and the hello time parameters while configuring a root bridge/secondary root bridge. Refer to “Configuring the Network Diameter of the Switched Network” on page 161 and “Configuring the Timeout Time Factor” on page 162 for information about the network diameter parameter and the hello time parameter.



- You can configure a switch as the root bridges of multiple spanning tree instances. But you cannot configure two or more root bridges for one spanning tree instance. So, do not configure root bridges for the same spanning tree instance on two or more switches using the **stp root primary** command.
- You can configure multiple secondary root bridges for one spanning tree instance. That is, you can configure secondary root bridges for the same spanning tree instance on two or more switches using the **stp root secondary** command.
- You can also configure the current switch as the root bridge by setting the priority of the switch to 0. Note that once a switch is configured as the root bridge or a secondary root bridge, its priority cannot be modified.

Configuration example

Configure the current switch as the root bridge of spanning tree instance 1 and a secondary root bridge of spanning tree instance 2.

```
<4210> system-view
[4210] stp instance 1 root primary
[4210] 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 spanning tree instances.

Configuration procedure

Table 105 Configure the bridge priority of the current switch

Operation	Command	Description
Enter system view	system-view	-
Set the bridge priority for the current switch	stp [instance <i>instance-id</i>] priority <i>priority</i>	Required The default bridge priority of a switch is 32,768.



CAUTION:

- Once you specify a switch as the root bridge or a secondary root bridge by using the **stp root primary** or **stp root secondary** command, the bridge priority of the switch cannot be configured any more.

- During the selection of the root bridge, if multiple switches have the same bridge priority, the one with the smallest MAC address becomes the root bridge.

Configuration example

Set the bridge priority of the current switch to 4,096 in spanning tree instance 1.

```
<4210> system-view
[4210] stp instance 1 priority 4096
```

Configuring the Mode 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 only 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 only 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

Table 106 Configure the mode a port recognizes and sends MSTP packets (in system view)

Operation	Command	Description
Enter system view	system-view	-

Table 106 Configure the mode a port recognizes and sends MSTP packets (in system view)

Operation	Command	Description
Configure the mode a port recognizes and sends MSTP packets	stp interface <i>interface-type</i> <i>interface-number</i> compliance { auto dot1s legacy }	Required By default, a port recognizes and sends MSTP packets in the automatic mode. That is, it determines the format of packets to be sent according to the format of the packets received.

Table 107 Configure the mode a port recognizes and sends MSTP packets (in Ethernet port view)

Operation	Command	Description
Enter system view	system-view	-
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	-
Configure the mode a port recognizes and sends MSTP packets	stp compliance { auto dot1s legacy }	Required By default, a port recognizes and sends MSTP packets in the automatic mode. That is, it determines the format of packets to be sent according to the format of the packets received.

Configuration example

Configure Ethernet 1/0/1 to recognize and send packets in dot1s format.

```
<4210> system-view
[4210] interface Ethernet1/0/1
[4210-Ethernet1/0/1] stp compliance dot1s
```

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

```
[4210-Ethernet1/0/1] undo stp compliance
```

Configuring the MSTP Operation Mode

To make a 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

Table 108 Configure the MSTP operation mode

Operation	Command	Description
Enter system view	system-view	-
Configure the MSTP operation mode	stp mode { stp rstp mstp }	Required An MSTP-enabled switch operates in the MSTP mode by default.

Configuration example

Specify the MSTP operation mode as STP-compatible.

```
<4210> system-view
[4210] 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

Table 109 Configure the maximum hop count for an MST region

Operation	Command	Description
Enter system view	system-view	-
Configure the maximum hop count of the MST region	stp max-hops hops	Required By default, the maximum hop count of an MST region is 20.

The bigger the maximum hop count, the larger the MST region is. Note that only the maximum hop settings on the switch operating as a region root can limit the size of the MST region.

Configuration example

Configure the maximum hop count of the MST region to be 30.

```
<4210> system-view
[4210] 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

Table 110 Configure the network diameter of the switched network

Operation	Command	Description
Enter system view	system-view	-
Configure the network diameter of the switched network	stp bridge-diameter <i>bridgenumber</i>	Required The default network diameter of a network is 7.

The network diameter parameter indicates the size of a network. The bigger the network diameter is, the larger the network size is.

After you configure the network diameter of a switched network, an MSTP-enabled switch adjusts its hello time, forward delay, and max age settings accordingly to better values.

The network diameter setting only applies to CIST; it is invalid for MSTIs.

Configuration example

Configure the network diameter of the switched network to 6.

```
<4210> system-view
[4210] 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

Table 111 Configure MSTP time-related parameters

Operation	Command	Description
Enter system view	system-view	-
Configure the forward delay parameter	stp timer forward-delay <i>centiseconds</i>	Required The forward delay parameter defaults to 1,500 centiseconds (namely, 15 seconds).
Configure the hello time parameter	stp timer hello <i>centiseconds</i>	Required The hello time parameter defaults to 200 centiseconds (namely, 2 seconds).
Configure the max age parameter	stp timer max-age <i>centiseconds</i>	Required The max age parameter defaults to 2,000 centiseconds (namely, 20 seconds).

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



CAUTION:

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

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

$$2 \times (\text{forward delay} - 1 \text{ second}) \geq \text{max age}$$

$$\text{Max age} \geq 2 \times (\text{hello time} + 1 \text{ second})$$

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

Configuration example

Configure the forward delay parameter to be 1,600 centiseconds, the hello time parameter to be 300 centiseconds, and the max age parameter to be 2,100 centiseconds (assuming that the current switch operates as the CIST root bridge).

```
<4210> system-view
[4210] stp timer forward-delay 1600
[4210] stp timer hello 300
[4210] 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 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

Table 112 Configure the timeout time factor

Operation	Command	Description
Enter system view	system-view	-
Configure the timeout time factor for the switch	stp timer-factor <i>number</i>	Required The timeout time factor defaults to 3.

For a steady network, the timeout time can be five to seven times of the hello time.

Configuration example

Configure the timeout time factor to be 6.

```
<4210> system-view
[4210] stp timer-factor 6
```

Configuring the Maximum Transmitting Speed on the Current Port

The maximum transmitting speed of a port specifies the maximum number of configuration BPDUs a port can transmit in a period specified by the hello time parameter. It depends on the physical state of the port and network structure. You can configure this parameter according to the network.

Configure the maximum transmitting speed for specified ports in system view

Table 113 Configure the maximum transmitting speed for specified ports in system view

Operation	Command	Description
Enter system view	system-view	-
Configure the maximum transmitting speed for specified ports	stp interface <i>interface-list</i> transmit-limit <i>packetnum</i>	Required The maximum transmitting speed of all Ethernet ports on a switch defaults to 10.

Configure the maximum transmitting speed in Ethernet port view

Table 114 Configure the maximum transmitting speed in Ethernet port view

Operation	Command	Description
Enter system view	system-view	-
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	-
Configure the maximum transmitting speed	stp transmit-limit <i>packetnum</i>	Required The maximum transmitting speed of all Ethernet ports on a switch defaults to 10.

As the maximum transmitting speed parameter determines the number of the configuration BPDUs transmitted in each hello time, set it to a proper value to

prevent MSTP from occupying too many network resources. The default value is recommended.

Configuration example

Set the maximum transmitting speed of Ethernet 1/0/1 to 15.

- 1 Configure the maximum transmitting speed in system view

```
<4210> system-view
[4210] stp interface Ethernet1/0/1 transmit-limit 15
```

- 2 Configure the maximum transmitting speed in Ethernet port view

```
<4210> system-view
[4210] interface Ethernet1/0/1
[4210-Ethernet1/0/1] stp transmit-limit 15
```

Configuring the Current Port as an Edge Port

Edge ports are ports that neither directly connects to other switches nor indirectly connects to other switches through network segments. After a port is configured as an edge port, the rapid transition mechanism is applicable to the port. That is, when the port changes from the blocking state to the forwarding state, it does not have to wait for a delay.

You can configure a port as an edge port in one of the following two ways.

Configure a port as an edge port in system view

Table 115 Configure a port as an edge port in system view

Operation	Command	Description
Enter system view	system-view	-
Configure the specified ports as edge ports	stp interface <i>interface-list</i> edged-port enable	Required By default, all the Ethernet ports of a switch are non-edge ports.

Configure a port as an edge port in Ethernet port view

Table 116 Configure a port as an edge port in Ethernet port view

Operation	Command	Description
Enter system view	system-view	-
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	-
Configure the port as an edge port	stp edged-port enable	Required By default, all the Ethernet ports of a switch are non-edge ports.

On a switch with BPDU guard disabled, an edge port becomes a non-edge port again once it receives a BPDU from another port.



You are recommended to configure the Ethernet ports connected directly to terminals as edge ports and enable the BPDU guard function at the same time. This not only enables these ports to turn to the forwarding state rapidly but also secures your network.

Configuration example

Configure Ethernet 1/0/1 as an edge port.

- 1 Configure Ethernet1/0/1 as an edge port in system view

```
<4210> system-view
[4210] stp interface Ethernet1/0/1 edged-port enable
```

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

```
<4210> system-view
[4210] interface Ethernet1/0/1
[4210-Ethernet1/0/1] 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

Table 117 Specify whether the link connected to a port is point-to-point link in system view

Operation	Command	Description
Enter system view	system-view	-
Specify whether the link connected to a port is point-to-point link	stp interface <i>interface-list</i> point-to-point { force-true force-false auto }	Required The auto keyword is adopted by default.

Specify whether the link connected to a port is point-to-point link in Ethernet port view

Table 118 Specify whether the link connected to a port is point-to-point link in Ethernet port view

Operation	Command	Description
Enter system view	system-view	-
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	-
Specify whether the link connected to a port is a point-to-point link	stp point-to-point { force-true force-false auto }	Required The auto keyword is adopted by default.



- 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 spanning tree instances the port belongs to. If the actual physical

link of a port is not a point-to-point link and you forcibly configure the link as a point-to-point link, loops may occur temporarily.

Configuration example

Configure the link connected to Ethernet 1/0/1 as a point-to-point link.

- 1 Perform this configuration in system view

```
<4210> system-view
[4210] stp interface Ethernet1/0/1 point-to-point force-true
```

- 2 Perform this configuration in Ethernet port view

```
<4210> system-view
[4210] interface Ethernet1/0/1
[4210-Ethernet1/0/1] stp point-to-point force-true
```

Enabling MSTP Configuration procedure

Table 119 Enable MSTP in system view

Operation	Command	Description
Enter system view	system-view	-
Enable MSTP	stp enable	Required MSTP is disabled by default.
Disable MSTP on specified ports	stp interface <i>interface-list</i> disable	Optional By default, MSTP is enabled on all ports after you enable MSTP in system view. To enable a switch to operate more flexibly, you can disable MSTP on specific ports. As MSTP-disabled ports do not participate in spanning tree calculation, this operation saves CPU resources of the switch.

Table 120 Enable MSTP in Ethernet port view

Operation	Command	Description
Enter system view	system-view	-
Enable MSTP	stp enable	Required MSTP is disabled by default.
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	-

Table 120 Enable MSTP in Ethernet port view

Operation	Command	Description
Disable MSTP on the port	stp disable	Optional By default, MSTP is enabled on all ports after you enable MSTP in system view. To enable a switch to operate more flexibly, you can disable MSTP on specific ports. As MSTP-disabled ports do not participate in spanning tree calculation, this operation saves CPU resources of the switch.

Other MSTP-related settings can take effect only after MSTP is enabled on the switch.

Configuration example

Enable MSTP on the switch and disable MSTP on Ethernet 1/0/1.

1 Perform this configuration in system view

```
<4210> system-view
[4210] stp enable
[4210] stp interface Ethernet1/0/1 disable
```

2 Perform this configuration in Ethernet port view

```
<4210> system-view
[4210] stp enable
[4210] interface Ethernet1/0/1
[4210-Ethernet1/0/1] stp disable
```

Configuring Leaf Nodes

Table 121 lists the tasks to configure a leaf node.

Table 121 Configure leaf nodes

Operation	Description	Related section
Enable MSTP	Required To prevent network topology jitter caused by other related configurations, you are recommended to enable MSTP after performing other configurations.	"Enabling MSTP"
Configure the MST region	Required	"Configuring an MST Region"
Configure the mode a port recognizes and sends MSTP packets	Optional	"Configuring the Mode a Port Recognizes and Sends MSTP Packets"
Configure the timeout time factor	Optional	"Configuring the Timeout Time Factor"
Configure the maximum transmitting speed on the current port	Optional The default value is recommended.	"Configuring the Maximum Transmitting Speed on the Current Port"

Table 121 Configure leaf nodes

Operation	Description	Related section
Configure the current port as an edge port	Optional	"Configuring the Current Port as an Edge Port"
Configure the path cost for a port	Optional	"Configuring the Path Cost for a Port"
Configure the port priority	Optional	"Configuring Port Priority"
Specify whether the link connected to a port is point-to-point link	Optional	"Specifying Whether the Link Connected to a Port Is Point-to-point Link"



In a network containing switches with both GVRP and MSTP enabled, GVRP packets are forwarded along the CIST. In this case, if you want to broadcast packets of a specific VLAN through GVRP, be sure to map the VLAN to the CIST when configuring the MSTP VLAN mapping table (the CIST of a network is spanning tree instance 0).

Configuration Prerequisites

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

Configuring the MST Region

Refer to "Configuring an MST Region" on page 155.

Configuring the Mode a Port Recognizes and Sends MSTP Packets

Refer to "Configuring the Mode a Port Recognizes and Sends MSTP Packets" on page 158.

Configuring the Timeout Time Factor

Refer to "Configuring the Timeout Time Factor" on page 162.

Configuring the Maximum Transmitting Speed on the Current Port

Refer to "Configuring the Maximum Transmitting Speed on the Current Port" on page 163.

Configuring a Port as an Edge Port

Refer to "Configuring the Current Port as an Edge Port" on page 164.

Configuring the Path Cost for a Port

The path cost parameter reflects the rate of the link connected to the port. For a port on an MSTP-enabled switch, the path cost may be different in different spanning tree instances. You can enable flows of different VLANs to travel along different physical links by configuring appropriate path costs on ports, so that VLAN-based load balancing can be implemented.

Path cost of a port can be determined by the switch or through manual configuration.

Standards for calculating path costs of ports

Currently, a switch can calculate the path costs of ports based on one of the following standards:

- **dot1d-1998**: Adopts the IEEE 802.1D-1998 standard to calculate the default path costs of ports.
- **dot1t**: Adopts the IEEE 802.1t standard to calculate the default path costs of ports.
- **legacy**: Adopts the proprietary standard to calculate the default path costs of ports.

Table 122 Specify the standard for calculating path costs

Operation	Command	Description
Enter system view	system-view	-
Specify the standard for calculating the default path costs of the links connected to the ports of the switch	stp pathcost-standard { dot1d-1998 dot1t legacy }	Optional By default, the legacy standard is used to calculate the default path costs of ports.

Table 123 Transmission speeds and the corresponding path costs

Transmission speed	Operation mode (half-/full-duplex)	802.1D-1998	IEEE 802.1t	Proprietary standard
0	-	65,535	200,000,000	200,000
10 Mbps	Half-duplex/Full-duplex	100	200,000	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	200,000	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	200,000	2
	Aggregated link 2 ports	1	1,000	1
	Aggregated link 3 ports	1	666	1
	Aggregated link 4 ports	1	500	1

Normally, the path cost of a port operating in full-duplex mode is slightly less than that of the port operating in half-duplex mode.

When calculating the path cost of an aggregated link, the 802.1D-1998 standard does not take the number of the ports on the aggregated link into account,

whereas the 802.1T standard does. The following formula is used to calculate the path cost of an aggregated link:

$$\text{Path cost} = 200,000 / \text{link transmission speed},$$

where "link transmission speed" is the sum of the speeds of all the unblocked ports on the aggregated link measured in 100 Kbps.

Configure the path cost for specific ports

Table 124 Configure the path cost for specified ports in system view

Operation	Command	Description
Enter system view	System-view	-
Configure the path cost for specified ports	stp interface <i>interface-list</i> [instance <i>instance-id</i>] cost <i>cost</i>	Required An MSTP-enabled switch can calculate path costs for all its ports automatically.

Table 125 Configure the path cost for a port in Ethernet port view

Operation	Command	Description
Enter system view	System-view	-
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	-
Configure the path cost for the port	stp [instance <i>instance-id</i>] cost <i>cost</i>	Required A MSTP-enabled switch can calculate path costs for all its ports automatically.

Changing the path cost of a port may change the role of the port and put it in state transition. Executing the **stp cost** command with the *instance-id* argument being 0 sets the path cost on the CIST for the port.



The range of the path cost of an Ethernet port varies by the standard used for path cost calculation as follows:

- *With the IEEE 802.1d-1998 standard adopted, the path cost ranges from 1 to 65535.*
- *With the IEEE 802.1t standard adopted, the path cost ranges from 1 to 20000000.*
- *With the proprietary standard adopted, the path cost ranges from 1 to 200000.*

Configuration example (A)

Configure the path cost of Ethernet 1/0/1 in spanning tree instance 1 to be 2,000.

1 Perform this configuration in system view

```
<4210> system-view
[4210] stp interface Ethernet1/0/1 instance 1 cost 2000
```

2 Perform this configuration in Ethernet port view


```
<4210> system-view
[4210] interface Ethernet1/0/1
[4210-Ethernet1/0/1] stp instance 1 cost 2000
```

Configuration example (B)

Configure the path cost of Ethernet 1/0/1 in spanning tree instance 1 to be calculated by the MSTP-enabled switch according to the IEEE 802.1D-1998 standard.

1 Perform this configuration in system view

```
<4210> system-view
[4210] undo stp interface Ethernet1/0/1 instance 1 cost
[4210] stp pathcost-standard dot1d-1998
```

2 Perform this configuration in Ethernet port view

```
<4210> system-view
[4210] interface Ethernet1/0/1
[4210-Ethernet1/0/1] undo stp instance 1 cost
[4210-Ethernet1/0/1] quit
[4210] 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 spanning tree instances. This enables packets of different VLANs to be forwarded along different physical paths, so that VLAN-based load balancing can be implemented.

You can configure port priority in one of the following two ways.

Configure port priority in system view

Table 126 Configure port priority in system view

Operation	Command	Description
Enter system view	system-view	-
Configure port priority for specified ports	stp interface <i>interface-list</i> instance <i>instance-id</i> port priority <i>priority</i>	Required The default port priority is 128.

Configure port priority in Ethernet port view

Table 127 Configure port priority in Ethernet port view

Operation	Command	Description
Enter system view	system-view	-
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	-
Configure port priority for the port	stp [instance <i>instance-id</i>] port priority <i>priority</i>	Required. The default port priority is 128.

Changing port priority of a port may change the role of the port and put the port into state transition.

A smaller port priority value indicates a higher possibility for the port to become the root port. If all the ports of a switch have the same port priority value, the port priorities are determined by the port indexes. Changing the priority of a port will cause spanning tree recalculation.

You can configure port priorities according to actual networking requirements.

Configuration example

Configure the port priority of Ethernet1/0/1 in spanning tree instance 1 to be 16.

1 Perform this configuration in system view

```
<4210> system-view
[4210] stp interface Ethernet1/0/1 instance 1 port priority 16
```

2 Perform this configuration in Ethernet port view

```
<4210> system-view
[4210] interface Ethernet1/0/1
[4210-Ethernet1/0/1] 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” on page 165.

Enabling MSTP

Refer to “Enabling MSTP” on page 166.

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**Table 128** Perform the mCheck operation in system view

Operation	Command	Description
Enter system view	system-view	-
Perform the mCheck operation	stp [interface <i>interface-list</i>] mcheck	Required

Perform the mCheck operation in Ethernet port view**Table 129** Perform the mCheck operation in Ethernet port view

Operation	Command	Description
Enter system view	system-view	-
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	-
Perform the mCheck operation	stp mcheck	Required

Configuration Example # Perform the mCheck operation on Ethernet 1/0/1.

- 1 Perform this configuration in system view

```
<4210> system-view
[4210] stp interface Ethernet1/0/1 mcheck
```

- 2 Perform this configuration in Ethernet port view

```
<4210> system-view
[4210] interface Ethernet1/0/1
[4210-Ethernet1/0/1] 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 spanning tree instances. When a port of this type receives configuration BPDUs with higher priorities, it turns to the discarding state (rather than become a non-designated port) and stops forwarding packets (as if it is disconnected from the link). It resumes the normal state if it does not receive any configuration BPDUs with higher priorities for a specified period.

Loop guard

A switch maintains the states of the root port and other blocked ports by receiving and processing BPDUs from the upstream switch. These BPDUs may get lost because of network congestions or unidirectional link failures. If a switch does not receive BPDUs from the upstream switch for certain period, the switch selects a new root port; the original root port becomes a designated port; and the blocked ports turn to the forwarding state. This may cause loops in the network.

The loop guard function suppresses loops. With this function enabled, if link congestions or unidirectional link failures occur, both the root port and the blocked ports become designated ports and turn to the discarding state. In this case, they stop forwarding packets, and thereby loops can be prevented.



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.

Configuration Prerequisites MSTP runs normally on the switch.

Configuring BPDU Guard Configuration procedure

Table 130 Configure BPDU guard

Operation	Command	Description
Enter system view	system-view	-
Enable the BPDU guard function	stp bpdu-protection	Required The BPDU guard function is disabled by default.

Configuration example

Enable the BPDU guard function.

```
<4210> system-view
[4210] stp bpdu-protection
```

Configuring Root Guard Configuration procedure

Table 131 Configure the root guard function in system view

Operation	Command	Description
Enter system view	system-view	-
Enable the root guard function on specified ports	stp interface <i>interface-list</i> root-protection	Required The root guard function is disabled by default.

Table 132 Enable the root guard function in Ethernet port view

Operation	Command	Description
Enter system view	system-view	-
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	-
Enable the root guard function on the current port	stp root-protection	Required The root guard function is disabled by default.

Configuration example

Enable the root guard function on Ethernet 1/0/1.

- 1 Perform this configuration in system view

```
<4210> system-view
[4210] stp interface Ethernet1/0/1 root-protection
```

- 2 Perform this configuration in Ethernet port view

```
<4210> system-view
[4210] interface Ethernet1/0/1
[4210-Ethernet1/0/1] stp root-protection
```

Configuring Loop Guard Configuration procedure

Table 133 Configure loop guard

Operation	Command	Description
Enter system view	system-view	-
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	-
Enable the loop guard function on the current port	stp loop-protection	Required The loop guard function is disabled by default.

Configuration example

Enable the loop guard function on Ethernet 1/0/1.

```
<4210> system-view
[4210] interface Ethernet1/0/1
[4210-Ethernet1/0/1] stp loop-protection
```

Configuring TC-BPDU Attack Guard

Configuration prerequisites

MSTP runs normally on the switch.

Configuration procedure

Table 134 Configure the TC-BPDU attack guard function

Operation	Command	Description
Enter system view	system-view	-
Enable the TC-BPDU attack guard function	stp tc-protection enable	Required The TC-BPDU attack guard function is disabled by default.
Set the maximum times that a switch can remove the MAC address table within each 10 seconds	stp tc-protection threshold <i>number</i>	Optional

Configuration example

Enable the TC-BPDU attack guard function

```
<4210> system-view
[4210] stp tc-protection enable
```

Set the maximum times for the switch to remove the MAC address table within 10 seconds to 5.

```
<4210> system-view
[4210] stp tc-protection threshold 5
```

Configuring Digest Snooping

Introduction According to IEEE802.1s, 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 Switch 4210 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 Switch 4210 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 other manufacturer's switch. In this way, the Switch 4210 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

Table 135 Configure digest snooping

Operation	Command	Description
Enter system view	system-view	-
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	-
Enable the digest snooping feature	stp config-digest-snooping	Required The digest snooping feature is disabled on a port by default.
Return to system view	quit	-
Enable the digest snooping feature globally	stp config-digest-snooping	Required The digest snooping feature is disabled globally by default.

Table 135 Configure digest snooping

Operation	Command	Description
Display the current configuration	display current-configuration	You can execute this command in any view.



- *When the digest snooping feature is enabled on a port, the port state turns to the discarding state. That is, the port will not send BPDU packets. The port is not involved in the STP calculation until it receives BPDU packets from the peer port.*
- *The digest snooping feature is needed only when your switch is connected to another manufacturer's switches adopting proprietary spanning tree protocols.*
- *To enable the digest snooping feature successfully, you must first enable it on all the ports of your switch that are connected to another manufacturer's switches adopting proprietary spanning tree protocols and then enable it globally.*
- *To enable the digest snooping feature, the interconnected switches and another manufacturer's switch adopting proprietary spanning tree protocols must be configured with exactly the same MST region-related configurations (including region name, revision level, and VLAN-to-MSTI mapping).*
- *The digest snooping feature must be enabled on all the 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 51 and Figure 52 illustrate the rapid transition mechanisms on designated ports in RSTP and MSTP.

Figure 51 The RSTP rapid transition mechanism

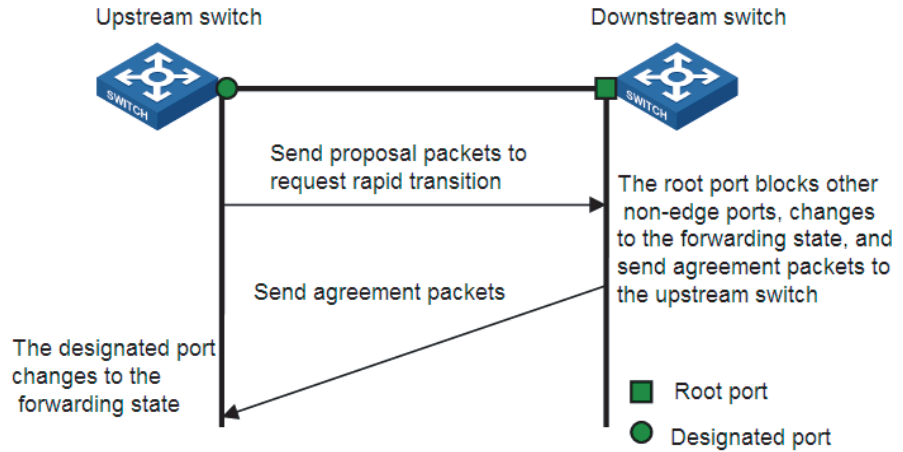
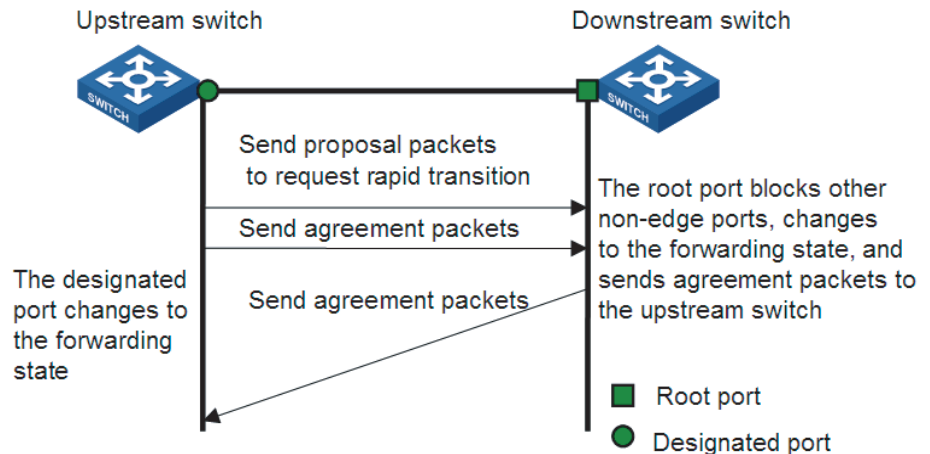


Figure 52 The MSTP rapid transition mechanism



The cooperation between MSTP and RSTP is limited in the process of rapid transition. For example, when the upstream switch adopts RSTP, the downstream switch adopts MSTP and the downstream switch does not support RSTP-compatible mode, the root port on the downstream switch receives no agreement packet from the upstream switch and thus sends no agreement packets to the upstream switch. As a result, the designated port of the upstream switch fails to transit rapidly and can only turn to the forwarding state after a period twice the forward delay.

Some other manufacturers' switches adopt proprietary spanning tree protocols that are similar to RSTP in the way to implement rapid transition on designated ports. When a switch of this kind operating as the upstream switch connects with a 3Com series switch running MSTP, the upstream designated port fails to change its state rapidly.

The rapid transition feature is developed to resolve this problem. When a 3Com series switch running MSTP is connected in the upstream direction to another

manufacturer’s switch running proprietary spanning tree protocols, you can enable the rapid transition feature on the ports of the 3Com series switch operating as the downstream switch. Among these ports, those operating as the root ports will then send agreement packets to their upstream ports after they receive proposal packets from the upstream designated ports, instead of waiting for agreement packets from the upstream switch. This enables designated ports of the upstream switch to change their states rapidly.

Configuring Rapid Transition

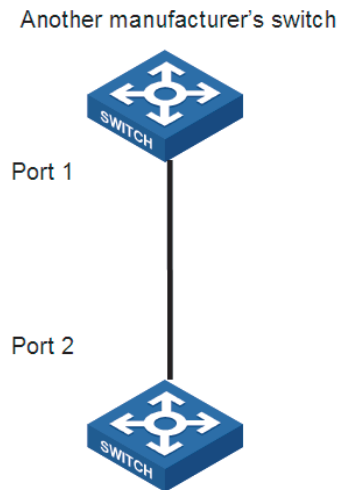
Configuration prerequisites

As shown in Figure 53, a 3Com series switch is connected to another manufacturer’s switch. The former operates as the downstream switch, and the latter operates as the upstream switch. The network operates normally.

The upstream switch is running a proprietary spanning tree protocol that is similar to RSTP in the way to implement rapid transition on designated ports. Port 1 is the designated port.

The downstream switch is running MSTP. Port 2 is the root port.

Figure 53 Network diagram for rapid transition configuration



Configuration procedure

- 1 Configure the rapid transition feature in system view

Table 136 Configure the rapid transition feature in system view

Operation	Command	Description
Enter system view	system-view	-
Enable the rapid transition feature	stp interface <i>interface-type</i> <i>interface-number</i> no-agreement-check	Required By default, the rapid transition feature is disabled on a port.

- 2 Configure the rapid transition feature in Ethernet port view

Table 137 Configure the rapid transition feature in Ethernet port view

Operation	Command	Description
Enter system view	system-view	-

Table 137 Configure the rapid transition feature in Ethernet port view

Operation	Command	Description
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	-
Enable the rapid transition feature	stp no-agreement-check	Required By default, the rapid transition feature is disabled on a port.



- *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

Table 138 Enable log/trap output for ports of MSTP instance

Operation	Command	Description
Enter system view	system-view	-
Enable log/trap output for the ports of a specified instance	stp [instance <i>instance-id</i>] portlog	Required By default, log/trap output is disabled for the ports of all instances.
Enable log/trap output for the ports of all instances	stp portlog all	Required By default, log/trap output is disabled for the ports of all instances.

Configuration Example

Enable log/trap output for the ports of instance 1.

```
<4210> system-view
[4210] stp instance 1 portlog
```

Enable log/trap output for the ports of all instances.

```
<4210> system-view
[4210] 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

Table 139 Enable trap messages conforming to 802.1d standard

Operation	Command	Description
Enter system view	system-view	-
Enable trap messages conforming to 802.1d standard in an instance	stp [instance <i>instance-id</i>] dot1d-trap [newroot topologychange] enable	Required

Configuration example

Enable a switch to send trap messages conforming to 802.1d standard to the network management device when the switch becomes the root bridge of instance 1.

```
<4210> system-view
[4210] stp instance 1 dot1d-trap newroot enable
```

Displaying and Maintaining MSTP

You can verify the above configurations by executing the **display** commands in any view.

Execute the **reset** command in user view to clear statistics about MSTP.

Table 140 Display and maintain MSTP

Operation	Command
Display the state and statistics information about spanning trees of the current device	display stp [instance <i>instance-id</i>] [interface <i>interface-list</i> slot <i>slot-number</i>] [brief]
Display region configuration	display stp region-configuration
Display information about the ports that are shut down by STP protection	display stp portdown
Display information about the ports that are blocked by STP protection	display stp abnormalport
Display information about the root port of the instance where the switch reside	display stp root
Clear statistics about MSTP	reset stp [interface <i>interface-list</i>]

MSTP Configuration Example

Network requirements

Implement MSTP in the network shown in Figure 54 to enable packets of different VLANs to be forwarded along different spanning tree instances. The detailed configurations are as follows:

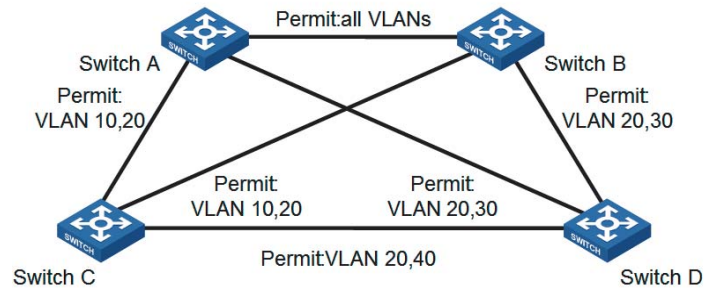
- All switches in the network belong to the same MST region.
- Packets of VLAN 10, VLAN 30, VLAN 40, and VLAN 20 are forwarded along spanning tree instance 1, instance 3, instance 4, and instance 0 respectively.

In this network, Switch A and Switch B operate on the convergence layer; Switch C and Switch D operate on the access layer. VLAN 10 and VLAN 30 are limited in the convergence layer and VLAN 40 is limited in the access layer. Switch A and

Switch B are configured as the root bridges of spanning tree instance 1 and spanning tree instance 3 respectively. Switch C is configured as the root bridge of spanning tree instance 4.

Network diagram

Figure 54 Network diagram for MSTP configuration



The word "permit" shown in Figure 54 means the corresponding link permits packets of specific VLANs.

Configuration procedure

1 Configure Switch A

Enter MST region view.

```
<4210> system-view
[4210] stp region-configuration
```

Configure the region name, VLAN-to-MSTI mapping table, and revision level for the MST region.

```
[4210-mst-region] region-name example
[4210-mst-region] instance 1 vlan 10
[4210-mst-region] instance 3 vlan 30
[4210-mst-region] instance 4 vlan 40
[4210-mst-region] revision-level 0
```

Activate the settings of the MST region manually.

```
[4210-mst-region] active region-configuration
```

Specify Switch A as the root bridge of spanning tree instance 1.

```
[4210] stp instance 1 root primary
```

2 Configure Switch B

Enter MST region view.

```
<4210> system-view
[4210] stp region-configuration
```

Configure the region name, VLAN-to-MSTI mapping table, and revision level for the MST region.

```
[4210-mst-region] region-name example
[4210-mst-region] instance 1 vlan 10
[4210-mst-region] instance 3 vlan 30
[4210-mst-region] instance 4 vlan 40
[4210-mst-region] revision-level 0
```

Activate the settings of the MST region manually.

```
[4210-mst-region] active region-configuration
# Specify Switch B as the root bridge of spanning tree instance 3.
[4210] stp instance 3 root primary
```

3 Configure Switch C.

Enter MST region view.

```
<4210> system-view
[4210] stp region-configuration
```

Configure the MST region.

```
[4210-mst-region] region-name example
[4210-mst-region] instance 1 vlan 10
[4210-mst-region] instance 3 vlan 30
[4210-mst-region] instance 4 vlan 40
[4210-mst-region] revision-level 0
```

Activate the settings of the MST region manually.

```
[4210-mst-region] active region-configuration
```

Specify Switch C as the root bridge of spanning tree instance 4.

```
[4210] stp instance 4 root primary
```

4 Configure Switch D

Enter MST region view.

```
<4210> system-view
[4210] stp region-configuration
```

Configure the MST region.

```
[4210-mst-region] region-name example
[4210-mst-region] instance 1 vlan 10
[4210-mst-region] instance 3 vlan 30
[4210-mst-region] instance 4 vlan 40
[4210-mst-region] revision-level 0
```

Activate the settings of the MST region manually.

```
[4210-mst-region] active region-configuration
```

15

MULTICAST OVERVIEW

Multicast Overview

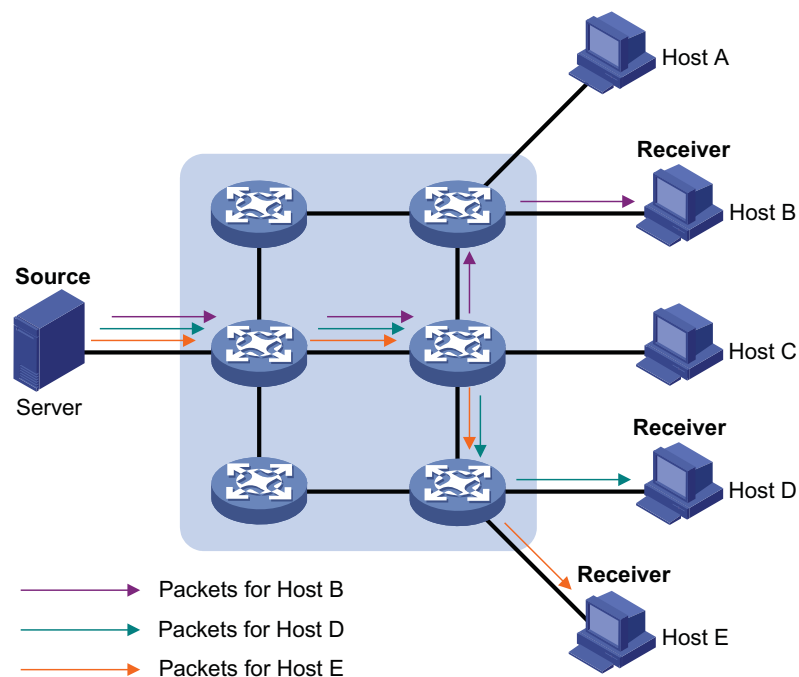
With development of networks on the Internet, more and more interaction services such as data, voice, and video services are running on the networks. In addition, highly bandwidth- and time-critical services, such as e-commerce, Web conference, online auction, video on demand (VoD), and tele-education 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 55:

Figure 55 Information transmission in the unicast mode



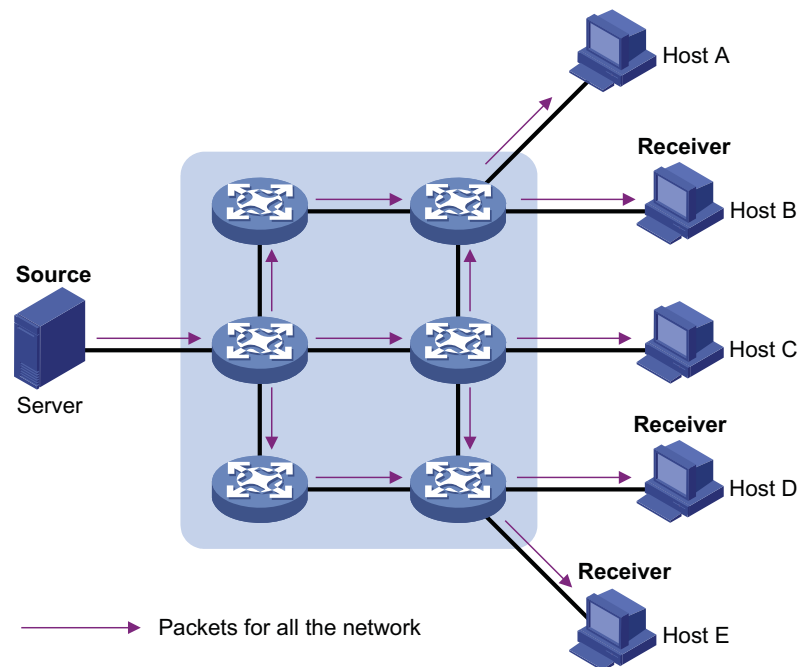
Assume that Hosts B, D and E need this information. The source server establishes transmission channels for the devices of these users respectively. As the transmitted traffic over the network is in direct proportion to the number of users that receive this information, when a large number of users need 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. Figure 56 shows information transmission in broadcast mode.

Figure 56 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.

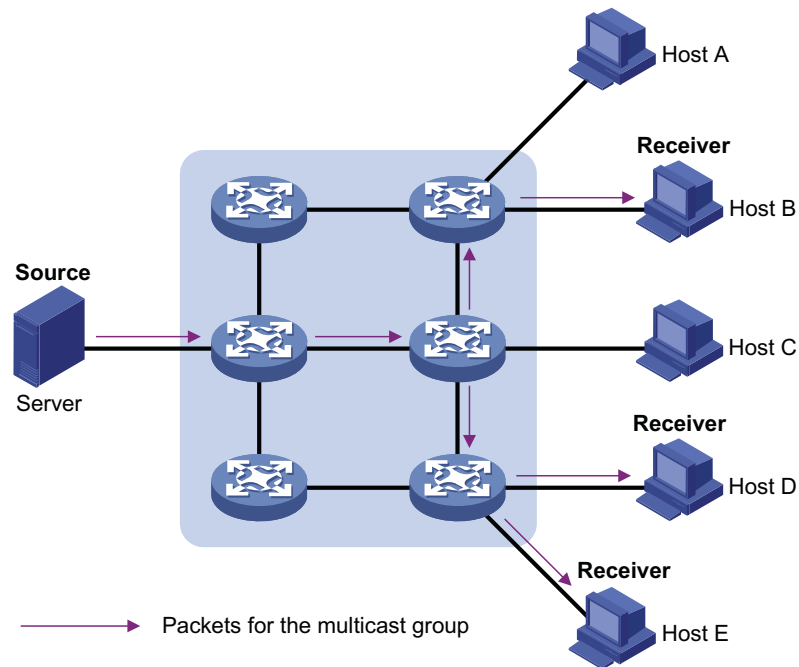
Information Transmission in the Multicast Mode

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 57:

Figure 57 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 57).
- Each receiver is a multicast group member ("Receiver" in Figure 57).

- 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 141.

Table 141 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.



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 transport information?
- Multicast routing: How is information transported?

IP multicast is a kind of peer-to-peer service. Based on the protocol layer sequence from bottom to top, the multicast mechanism contains addressing mechanism, host registration, multicast routing, and multicast application:

- Addressing mechanism: Information is sent from a multicast source to a group of receivers through multicast addresses.

- Host registration: A receiving host joins and leaves a multicast group dynamically using the membership registration mechanism.
- Multicast routing: A router or switch transports packets from a multicast source to receivers by building a multicast distribution tree with multicast routes.
- Multicast application: A multicast source must support multicast applications, such as video conferencing. The TCP/IP protocol suite must support the function of sending and receiving multicast information.

Multicast Address As receivers are multiple hosts in a multicast group, you should be concerned about the following questions:

- What destination should the information source send the information to in the multicast mode?
- How to select the destination address?

These questions are about multicast addressing. To enable the communication between the information source and members of a multicast group (a group of information receivers), network-layer multicast addresses, namely, IP multicast addresses must be provided. In addition, a technology must be available to map IP multicast addresses to link-layer MAC multicast addresses. The following sections describe these two types of multicast addresses:

IP multicast address

Internet Assigned Numbers Authority (IANA) categorizes IP addresses into five classes: A, B, C, D, and E. Unicast packets use IP addresses of Class A, B, and C based on network scales. Class D IP addresses are used as destination addresses of multicast packets. Class D address must not appear in the IP address field of a source IP address of IP packets. Class E IP addresses are reserved for future use.

In unicast data transport, a data packet is transported hop by hop from the source address to the destination address. In an IP multicast environment, there are a group of destination addresses (called group address), rather than one address. All the receivers join a group. Once they join the group, the data sent to this group of addresses starts to be transported to the receivers. All the members in this group can receive the data packets. This group is a multicast group.

A multicast group has the following characteristics:

- The membership of a group is dynamic. A host can join and leave a multicast group at any time.
- A multicast group can be either permanent or temporary.
- A multicast group whose addresses are assigned by IANA is a permanent multicast group. It is also called reserved multicast group.



- *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 142.

Table 142 Range and description of Class D IP addresses

Class D address range	Description
224.0.0.0 to 224.0.0.255	Reserved multicast addresses (IP addresses for permanent multicast groups). The IP address 224.0.0.0 is reserved. Other IP addresses can be used by routing protocols.
224.0.1.0 to 231.255.255.255 233.0.0.0 to 238.255.255.255	Available any-source multicast (ASM) multicast addresses (IP addresses for temporary groups). They are valid for the entire network.
232.0.0.0 to 232.255.255.255	Available source-specific multicast (SSM) multicast group addresses.
239.0.0.0 to 239.255.255.255	Administratively scoped multicast addresses, which are for specific local use only.

As specified by IANA, the IP addresses ranging from 224.0.0.0 to 224.0.0.255 are reserved for network protocols on local networks. Table 143 lists commonly used reserved IP multicast addresses:

Table 143 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



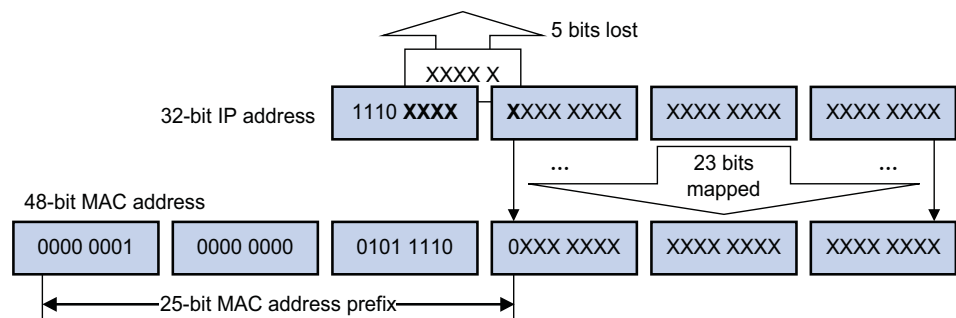
Like having reserved the private network segment 10.0.0.0/8 for unicast, IANA has also reserved the network segment 239.0.0.0/8 for multicast. These are administratively scoped addresses. With the administratively scoped addresses, you can define the range of multicast domains flexibly to isolate IP addresses between different multicast domains, so that the same multicast address can be used in different multicast domains without causing collisions.

Ethernet multicast MAC address

When a unicast IP packet is transported in an Ethernet network, the destination MAC address is the MAC address of the receiver. When a multicast packet is transported in an Ethernet network, a multicast MAC address is used as the destination address because the destination is a group with an uncertain number of members.

As stipulated by IANA, the high-order 24 bits of a multicast MAC address are 0x01005e, while the low-order 23 bits of a MAC address are the low-order 23 bits of the multicast IP address. Figure 58 describes the mapping relationship:

Figure 58 Multicast address mapping



The high-order four bits of the IP multicast address are 1110, representing the multicast ID. Only 23 bits of the remaining 28 bits are mapped to a MAC address. Thus, five bits of the multicast IP address are lost. As a result, 32 IP multicast addresses are mapped to the same MAC address.

Multicast Protocols

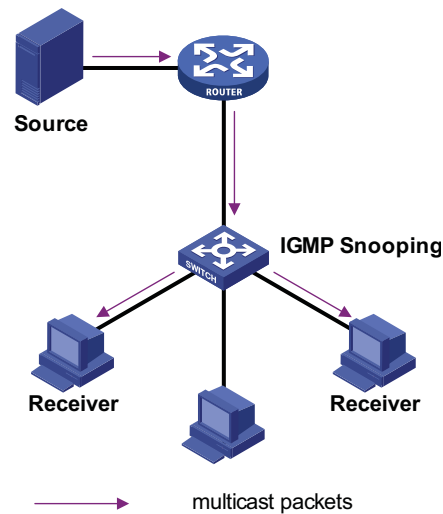
This section provides only general descriptions about applications and functions of the Layer 2 and Layer 3 multicast protocols in a network. For details about these protocols, refer to the related chapters of this manual.

Layer 2 multicast protocols

Layer 2 multicast protocols include IGMP Snooping and multicast VLAN. Figure 59 shows where these protocols are in the network.



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. The Switch 4210 does support IGMP snooping.

Figure 59 Positions of Layer 2 multicast protocols

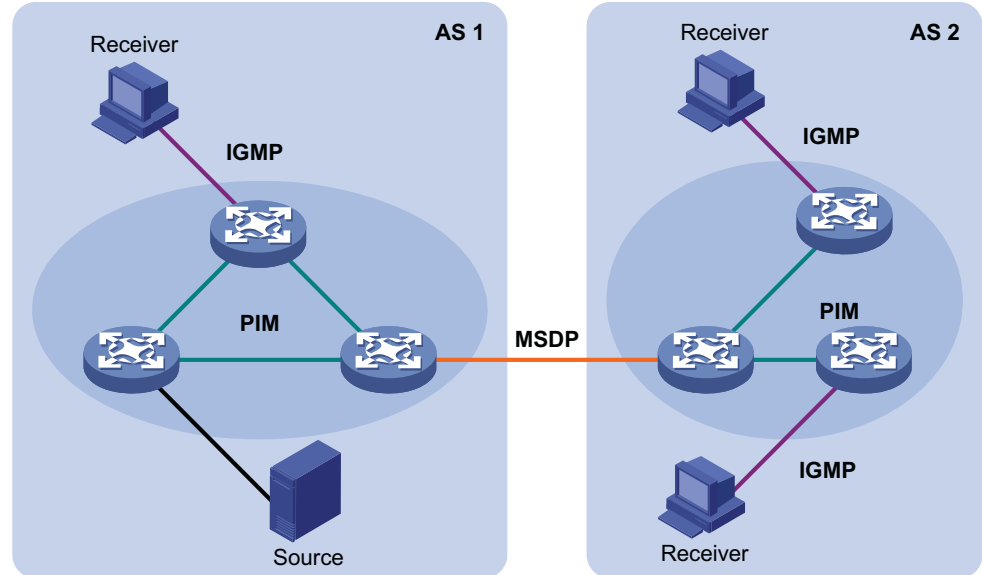
Running on Layer 2 devices, Internet Group Management Protocol Snooping (IGMP Snooping) are multicast constraining mechanisms that manage and control multicast groups by listening to and analyzing IGMP messages exchanged between the hosts and Layer 3 multicast devices, thus effectively controlling the flooding of multicast data in a Layer 2 network.

Layer 3 multicast protocols



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 among others. Note that the Switch 4210 does not support Layer 3 multicast protocols.

Layer 3 multicast protocols include multicast group management protocols and multicast routing protocols. Figure 60 describes where these multicast protocols are in a network.

Figure 60 Positions of Layer 3 multicast protocol

- 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.

- 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.

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.

Implementing 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:

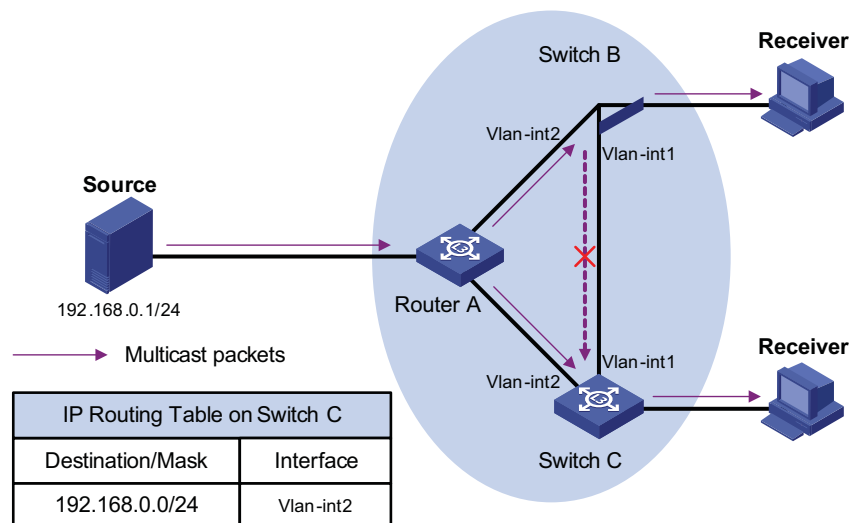
- If the corresponding (S, G) entry exists, and the interface on which the packet actually arrived is the incoming interface in the multicast forwarding table, the router forwards the packet to all the outgoing interfaces.
- If the corresponding (S, G) entry exists, but the interface on which the packet 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.
- 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 59. Multicast packets travel along the SPT from the multicast source to the receivers.

Figure 61 RPF check process



- A multicast packet from Source arrives to VLAN-interface 1 of Switch C, and the corresponding forwarding entry does not exist in the multicast forwarding table of Switch C. Switch C performs an RPF check, and finds in its unicast routing table that the outgoing interface to 192.168.0.0/24 is VLAN-interface 2. This means that the interface on which the packet actually arrived is not the RPF interface. The RPF check fails and the packet is discarded.
- A multicast packet from Source arrives to VLAN-interface 2 of Switch C, and the corresponding forwarding entry does not exist in the multicast forwarding table of Switch C. The router performs an RPF check, and finds in its unicast routing table that the outgoing interface to 192.168.0.0/24 is the interface on which the packet actually arrived. The RPF check succeeds and the packet is forwarded.

16

IGMP SNOOPING CONFIGURATION

IGMP Snooping Overview

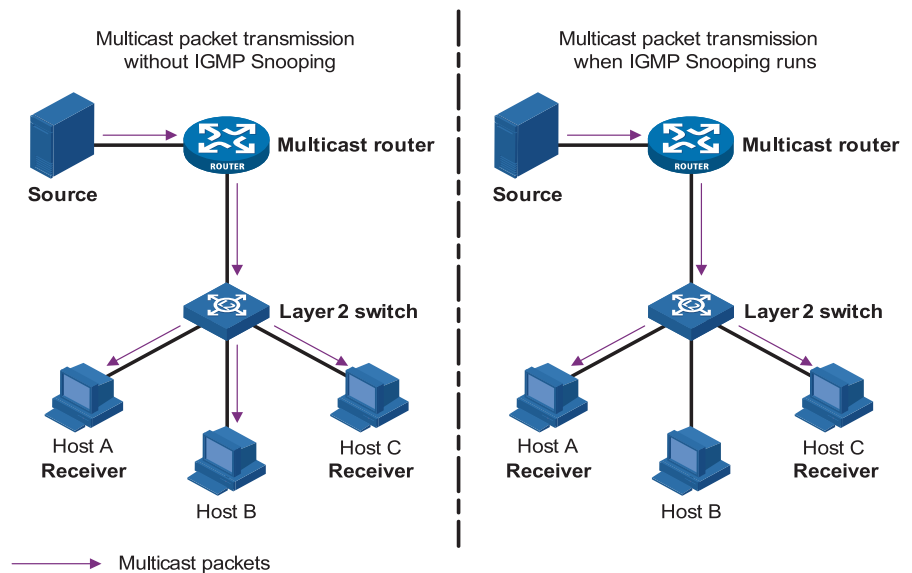
Internet Group Management Protocol Snooping (IGMP Snooping) is a multicast constraining mechanism that runs on Layer 2 devices to manage and control multicast groups.

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 62, when IGMP Snooping is not running on the switch, multicast packets are broadcast to all devices at Layer 2. When IGMP Snooping is running on the switch, multicast packets for known multicast groups are multicast to the receivers, rather than broadcast to all hosts, at Layer 2. However, multicast packets for unknown multicast groups are still broadcast at Layer 2.

Figure 62 Before and after IGMP Snooping is enabled on Layer 2 device

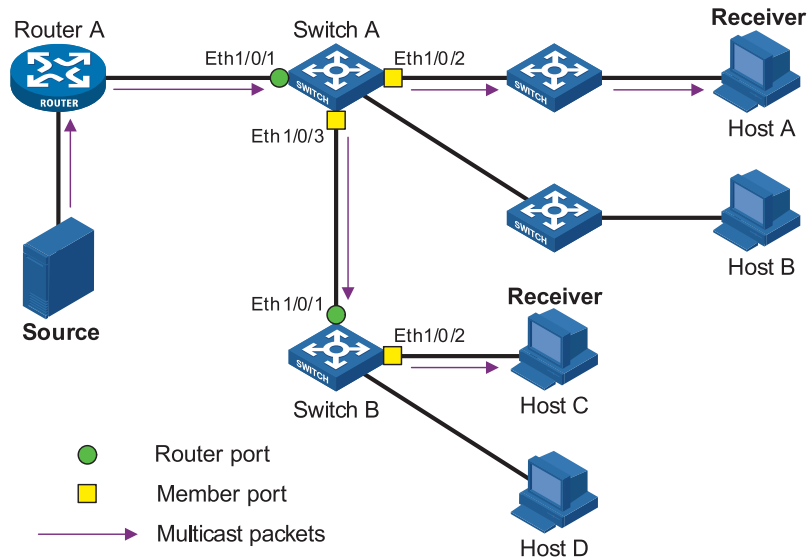


Basic Concepts in IGMP Snooping

IGMP Snooping related ports

As shown in Figure 63, 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 63 IGMP Snooping related ports



Ports involved in IGMP Snooping, as shown in Figure 63, 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 Figure 63, 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 Figure 63, 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 144 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.



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 left the multicast group.

Upon receiving an IGMP leave message on the last member port, a switch forwards it out all router ports in the VLAN. Because the switch does not know whether any other member hosts of that multicast group still exists under the port to which the IGMP leave message arrived, the switch does not immediately delete

the forwarding entry corresponding to that port from the forwarding table; instead, it resets the aging timer of the member port.

Upon receiving the IGMP leave message from a host, the IGMP querier resolves from the message the address of the multicast group that the host just left and sends an IGMP group-specific query to that multicast group through the port that received the leave message. Upon receiving the IGMP group-specific query, a switch forwards it through all the router ports in the VLAN and all member ports of that multicast group, and performs the following to the receiving port:

- If any IGMP report in response to the group-specific query arrives to the member port before its aging timer expires, this means that some other members of that multicast group still exist under that port: the switch resets the aging timer of the member port.
- If no IGMP report in response to the group-specific query arrives to the member port before its aging timer expires as a response to the IGMP group-specific query, this means that no members of that multicast group still exist under the port: the switch deletes the forwarding entry corresponding to the port from the forwarding table when the aging timer expires.



Caution: After an Ethernet switch enables IGMP Snooping, when it receives the IGMP leave message sent by a host in a multicast group, it judges whether the multicast group exists automatically. If the multicast group does not exist, the switch drops this IGMP leave message.

IGMP Snooping Configuration

The following table lists all the IGMP Snooping configuration tasks:

Table 145 IGMP Snooping configuration tasks

Operation	Remarks
Enabling IGMP Snooping	Required
Configuring the Version of IGMP Snooping	Optional
Configuring Timers	Optional
Configuring Fast Leave	Optional
Configuring a Multicast Group Filter	Optional
Configuring the Maximum Number of Multicast Groups on a Port	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 Message	Optional

Enabling IGMP Snooping

Table 146 Enable IGMP Snooping

Operation	Command	Remarks
Enter system view	system-view	-
Enable IGMP Snooping globally	igmp-snooping enable	Required By default, IGMP Snooping is disabled globally.

Table 146 Enable IGMP Snooping

Operation	Command	Remarks
Enter VLAN view	vlan <i>vlan-id</i>	-
Enable IGMP Snooping on the VLAN	igmp-snooping enable	Required By default, IGMP Snooping is disabled on all the VLANs.

**Caution:**

- Before enabling IGMP Snooping in a VLAN, be sure to enable IGMP Snooping globally in system view; otherwise the IGMP Snooping settings will not take effect.
- If IGMP Snooping and VLAN VPN are enabled on a VLAN at the same time, IGMP queries are likely to fail to pass the VLAN. You can solve this problem by configuring VLAN tags for queries. For details, see *Configuring a VLAN Tag for Query Messages*.

Configuring the Version of IGMP Snooping

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 147 Configure the version of IGMP Snooping

Operation	Command	Remarks
Enter system view	system-view	-
Enter VLAN view	vlan <i>vlan-id</i>	-
Configure the version of IGMP Snooping	igmp-snooping version <i>version-number</i>	Optional

The default IGMP Snooping version is version 2.

**Caution:**

- Before configuring related IGMP Snooping functions, you must enable IGMP Snooping in the specified VLAN.
- Different multicast group addresses should be configured for different multicast sources because IGMPv3 Snooping cannot distinguish multicast data from different sources to the same multicast group.

Configuring Timers

This section describes how to configure the aging timer of the router port, the aging timer of the multicast member ports.

Table 148 Configure timers

Operation	Command	Remarks
Enter system view	system-view	-
Configure the aging timer of the router port	igmp-snooping router-aging-time <i>seconds</i>	Optional By default, the aging time of the router port is 105 seconds.

Table 148 Configure timers

Operation	Command	Remarks
Configure the aging timer of the multicast member port	igmp-snooping host-aging-time <i>seconds</i>	Optional By default, the aging time of multicast member ports is 260 seconds

Configuring Fast Leave Processing

With fast leave processing enabled, when the switch receives an IGMP leave message on a port, the switch directly removes that port from the forwarding table entry for the specific group. If only one host is attached to a 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

Table 149

Operation	Command	Remarks
Enter system view	system-view	-
Enable fast leave processing	igmp-snooping fast-leave [vlan <i>vlan-list</i>]	Required By default, the fast leave processing feature is disabled

Enabling fast leave processing in Ethernet port view

Table 150 Enable fast leave processing in Ethernet view

Operation	Command	Remarks
Enter system view	system-view	-
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	-
Enable fast leave processing for specific VLANs	igmp-snooping fast-leave [vlan <i>vlan-list</i>]	Required By default, the fast leave processing feature is disabled.



- *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 151 Configure a multicast group filter in system view

Operation	Command	Remarks
Enter system view	system-view	-
Configure a multicast group filter	igmp-snooping group-policy <i>acl-number</i> [vlan <i>vlan-list</i>]	Required No group filter is configured by default, namely hosts can join any multicast group.

Configuring a multicast group filter in Ethernet port view

Table 152 Configure a multicast group filter in Ethernet port view

Operation	Command	Remarks
Enter system view	system-view	-
Enter Ethernet port view	interface <i>interface-type interface-number</i>	-
Configure a multicast group filter	igmp-snooping group-policy <i>acl-number</i> [vlan <i>vlan-list</i>]	Optional No group filter is configured by default, namely hosts can join any multicast group.



- *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 153 Configure the maximum number of multicast groups on a port

Operation	Command	Remarks
Enter system view	system-view	-
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	-
Configure the maximum number of multicast groups allowed on the port	igmp-snooping group-limit <i>limit</i> [vlan <i>vlan-list</i> [overflow-replace]]	Required default value is 128



- *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 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 154** Configure a static multicast group member port in Ethernet port view

Operation	Command	Remarks
Enter system view	system-view	-
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	-
Configure the current port as a static member port for a multicast group in a VLAN	multicast static-group <i>group-address</i> vlan <i>vlan-id</i>	Required By default, no port is configured as a static multicast group member port.

In VLAN interface view**Table 155** 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 <i>interface-number</i>	-
Configure specified port(s) as static member port(s) of a multicast group in the VLAN	multicast static-group <i>group-address</i> interface <i>interface-list</i>	Required By default, no port is configured as a static multicast group member port.

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 156** Configure a static router port in Ethernet port view

Operation	Command	Remarks
Enter system view	system-view	-
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	-
Configure the current port as a static router port	multicast static-router-port <i>vlan</i> <i>vlan-id</i>	Required By default, no static router port is configured.

In VLAN view**Table 157** Configure a static router port in VLAN view

Operation	Command	Remarks
Enter system view	system-view	-
Enter VLAN view	vlan <i>vlan-id</i>	-
Configure a specified port as a static router port	multicast static-router-port <i>interface-type</i> <i>interface-number</i>	Required 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 158 Configure a port as a simulated group member

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

Table 158 Configure a port as a simulated group member

Operation	Command	Remarks
Configure the current port as a simulated multicast group member	igmp host-join group-address [source-ip source-address] vlan vlan-id	Optional Simulated joining is disabled by default.


Caution:

- Before configuring a simulated host, enable IGMP Snooping in VLAN view first.
- The port to be configured must belong to the specified VLAN; otherwise the configuration does not take effect.
- You can use the source-ip source-address command to specify a multicast source address that the port will join as a simulated host. This configuration takes effect when IGMPv3 Snooping is enabled in the VLAN.

Configuring a VLAN Tag for Query Messages

By configuring the VLAN in which IGMP general and group-specific queries forwarded and sent by IGMP Snooping switches are transmitted and by configuring the VLAN mapping function, you can enable multicast packet forwarding between different VLANs in a Layer-2 multicast network environment.

For description about VLAN mapping, see "VLAN-VPN"

Table 159 Configure VLAN Tag for query message

Operation	Command	Remarks
Enter system view	system-view	-
Enable IGMP Snooping	igmp-snooping enable	Required By default, IGMP Snooping is disabled
Configure a VLAN tag for query messages	igmp-snooping vlan-mapping vlan vlan-id	Required



It is not recommended to configure this function while the multicast VLAN function is in effect.

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 160 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]	

Table 160 Display and maintain IGMP Snooping

Operation	Command	Remarks
Clear IGMP Snooping statistics	reset igmp-snooping statistics	You can execute the reset command in user view.

IGMP Snooping Configuration Examples

Configuring IGMP Snooping

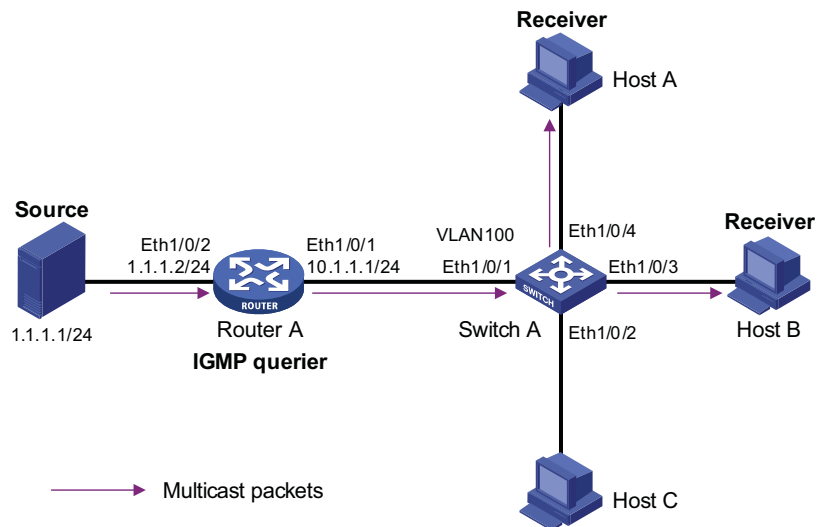
Network requirements

To prevent multicast traffic from being flooded at Layer 2, enable IGMP snooping on Layer 2 switches.

- As shown in Figure 64, Router A connects to a multicast source (Source) through Ethernet1/0/2, and to Switch A through Ethernet1/0/1.
- 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 64 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 shown in Figure 64. The detailed configuration steps are omitted.

- 2 Configure Router A

Enable IP multicast routing, enable PIM-DM on each interface, and enable IGMP on Ethernet1/0/1.

```
<RouterA> system-view
[RouterA] multicast routing-enable
[RouterA] interface Ethernet 1/0/1
[RouterA-Ethernet1/0/1] igmp enable
[RouterA-Ethernet1/0/1] pim dm
[RouterA-Ethernet1/0/1] quit
[RouterA-Ethernet1/0/1] quit
[RouterA] interface Ethernet 1/0/2
[RouterA-Ethernet1/0/2] pim dm
[RouterA-Ethernet1/0/2] quit
```

3 Configure Switch A

Enable IGMP Snooping globally.

```
<SwitchA> system-view
[SwitchA] igmp-snooping enable
    Enable IGMP-Snooping ok.
```

Create VLAN 100, assign Ethernet1/0/1 through Ethernet1/0/4 to this VLAN, and enable IGMP Snooping in the VLAN.

```
[SwitchA] vlan 100
[SwitchA-vlan100] port Ethernet 1/0/1 to Ethernet 1/0/4
[SwitchA-vlan100] igmp-snooping enable
[SwitchA-vlan100] quit
```

4 Verify the configuration

View the detailed information of the multicast group in VLAN 100 on Switch A.

```
<SwitchA> display igmp-snooping group
Total 1 IP Group(s).
Total 1 MAC Group(s).

Vlan(id):100.
    Total 1 IP Group(s).
    Total 1 MAC Group(s).
    Static Router port(s):
    Dynamic Router port(s):
        Ethernet1/0/1
    IP group(s):the following ip group(s) match to one mac group.
        IP group address: 224.1.1.1
        Static host port(s):
        Dynamic host port(s):
            Ethernet1/0/3          Ethernet1/0/4
    MAC group(s):
        MAC group address: 0100-5e01-0101
        Host port(s):Ethernet1/0/3          Ethernet1/0/4
```

As shown above, the multicast group 224.1.1.1 is established on Switch A, with the dynamic router port Ethernet1/0/1 and dynamic member ports Ethernet1/0/3 and Ethernet1/0/4. This means that Host A and Host B have joined the multicast group 224.1.1.1.

Troubleshooting IGMP Snooping

Symptom: Multicast function does not work on the switch.

Solution: Possible reasons are:

- 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.
- 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.

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 161 Configure dropping unknown multicast packet

Operation	Command	Remarks
Enter system view	system-view	-
Configure dropping unknown multicast packets	unknown-multicast drop enable	Required By default, the function of dropping unknown multicast packets is disabled.

17

802.1X CONFIGURATION



- The online user handshaking function is added. See “Configuring Basic 802.1x Functions”.
- The configuration of 802.1x re-authentication is added. See “Configuring 802.1x Re-Authentication”.
- The configuration of the 802.1x re-authentication interval is added. See “Configuring the 802.1x Re-Authentication Timer” .

Introduction to 802.1x

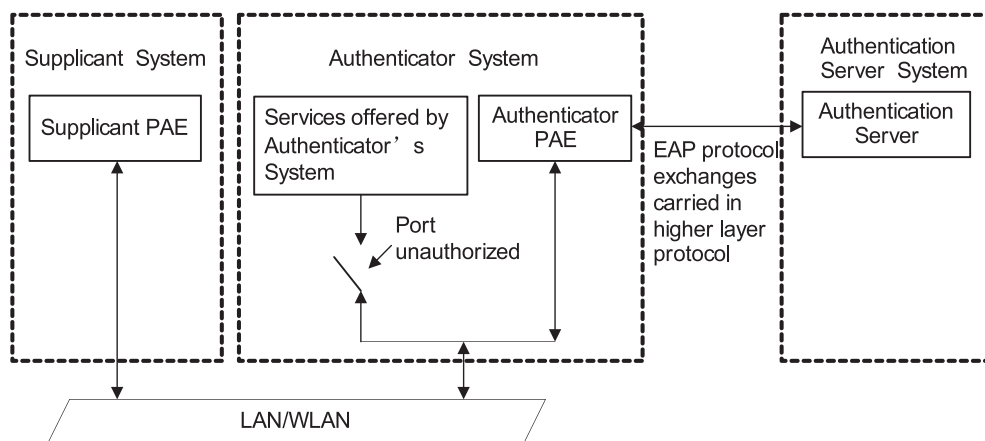
The 802.1x protocol (802.1x for short) was developed by IEEE802 LAN/WAN committee to address security issues of wireless LANs. It was then used in Ethernet as a common access control mechanism for LAN ports to address mainly authentication and security problems.

802.1x is a port-based network access control protocol. It authenticates and controls devices requesting for access in terms of the ports of LAN access devices. With the 802.1x protocol employed, a user-side device can access the LAN only when it passes the authentication. Those fail to pass the authentication are denied when accessing the LAN.

Architecture of 802.1x Authentication

As shown in Figure 65, 802.1x adopts a client/server architecture with three entities: a supplicant system, an authenticator system, and an authentication server system.

Figure 65 Architecture of 802.1x authentication



- The supplicant system is an entity residing at one end of a LAN segment and is authenticated by the authenticator system at the other end of the LAN segment. The supplicant system is usually a user terminal device. An 802.1x authentication is triggered when a user launches client program on the

supplicant system. Note that the client program must support extensible authentication protocol over LAN (EAPoL).

- The authenticator system is another entity residing at one end of a LAN segment. It authenticates the connected supplicant systems. The authenticator system is usually an 802.1x-supported network device (such as a 3Com series switch). It provides the port (physical or logical) for the supplicant system to access the LAN.
- The authentication server system is an entity that provides authentication service to the authenticator system. Normally in the form of a RADIUS server, the authentication server system serves to perform AAA (authentication, authorization, and accounting) services to users. It also stores user information, such as user name, password, the VLAN a user belongs to, priority, and the ACLs (access control list) applied.

The four basic concepts related to the above three entities are PAE, controlled port and uncontrolled port, the valid direction of a controlled port and the way a port is controlled.

PAE

A PAE (port access entity) is responsible for implementing algorithms and performing protocol-related operations in the authentication mechanism.

- The authenticator system PAE authenticates the supplicant systems when they log into the LAN and controls the status (authorized/unauthorized) of the controlled ports according to the authentication result.
- The supplicant system PAE responds to the authentication requests received from the authenticator system and submits user authentication information to the authenticator system. It also sends authentication requests and disconnection requests to the authenticator system PAE.

Controlled port and uncontrolled port

The Authenticator system provides ports for supplicant systems to access a LAN. Logically, a port of this kind is divided into a controlled port and an uncontrolled port.

- The uncontrolled port can always send and receive packets. It mainly serves to forward EAPoL packets to ensure that a supplicant system can send and receive authentication requests.
- The controlled port can be used to pass service packets when it is in authorized state. It is blocked when not in authorized state. In this case, no packets can pass through it.
- Controlled port and uncontrolled port are two properties of a port. Packets reaching a port are visible to both the controlled port and uncontrolled port of the port.

The valid direction of a controlled port

When a controlled port is in unauthorized state, you can configure it to be a unidirectional port, which sends packets to supplicant systems only.

By default, a controlled port is a unidirectional port.

The way a port is controlled

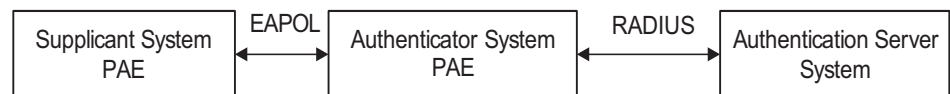
A port of a 3Com series switch can be controlled in the following two ways.

- Port-based authentication. When a port is controlled in this way, all the supplicant systems connected to the port can access the network without being authenticated after one supplicant system among them passes the authentication. And when the authenticated supplicant system goes offline, the others are denied as well.
- MAC address-based authentication. All supplicant systems connected to a port have to be authenticated individually in order to access the network. And when a supplicant system goes offline, the others are not affected.

The Mechanism of an 802.1x Authentication System

IEEE 802.1x authentication system uses the extensible authentication protocol (EAP) to exchange information between supplicant systems and the authentication servers.

Figure 66 The mechanism of an 802.1x authentication system



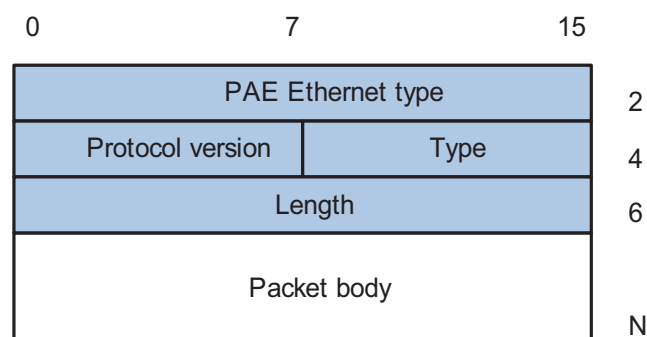
- EAP protocol packets transmitted between the supplicant system PAE and the authenticator system PAE are encapsulated as EAPoL packets.
- EAP protocol packets transmitted between the authenticator system PAE and the RADIUS server can either be encapsulated as EAP over RADIUS (EAPoR) packets or be terminated 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 67 The format of an EAPoL packet



In an EAPoL packet:

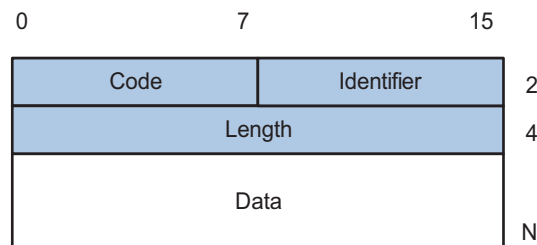
- The PAE Ethernet type field holds the protocol identifier. The identifier for 802.1x is 0x888E.
- The Protocol version field holds the version of the protocol supported by the sender of the EAPoL packet.
- The Type field can be one of the following:
 - 00: Indicates that the packet is an EAP-packet, which carries authentication information.
 - 01: Indicates that the packet is an EAPoL-start packet, which initiates the authentication.
 - 02: Indicates that the packet is an EAPoL-logoff packet, which sends logging off requests.
 - 03: Indicates that the packet is an EAPoL-key packet, which carries key information.
 - 04: Indicates that the packet is an EAPoL-encapsulated-ASF-Alert packet, which is used to support the alerting messages of ASF (alerting standards forum).
- The Length field indicates the size of the Packet body field. A value of 0 indicates that the Packet Body field does not exist.
- The Packet body field differs with the Type field.

Note that EAPoL-Start, EAPoL-Logoff, and EAPoL-Key packets are only transmitted between the supplicant system and the authenticator system. EAP-packets are encapsulated by RADIUS protocol to allow them successfully reach the authentication servers. Network management-related information (such as alarming information) is encapsulated in EAPoL-Encapsulated-ASF-Alert packets, which are terminated by authenticator systems.

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 68.

Figure 68 The format of an EAP packet



In an EAP packet:

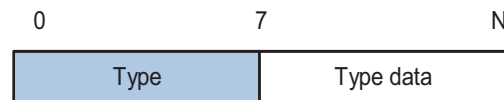
- The Code field indicates the EAP packet type, which can be Request, Response, Success, or Failure.
- The Identifier field is used to match a Response packet with the corresponding Request packet.

- The Length field indicates the size of an EAP packet, which includes the Code, Identifier, Length, and Data fields.
- The Data field contains information about an EAP packet. Its format is different than the Code field.

A Success or Failure packet does not contain the Data field, so the Length field of it is 4.

Figure 69 shows the format of the Data field of a Request packet or a Response packet.

Figure 69 The format of the Data field of a Request packet or a Response packet



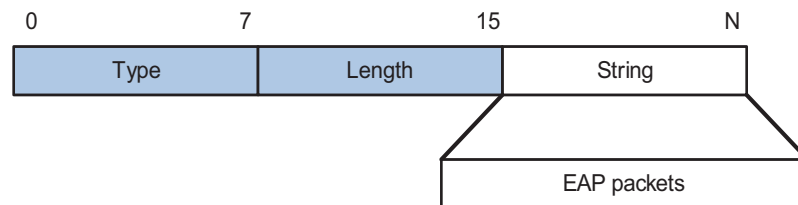
- The Type field indicates the EAP authentication type. A value of 1 indicates Identity and that the packet is used to query the identity of the peer. A value of 4 represents MD5-Challenge (similar to PPP CHAP) and indicates that the packet includes query information.
- The Type Date field differs with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

Newly added fields for EAP authentication

Two fields, EAP-message and Message-authenticator, are added to a RADIUS protocol packet for EAP authentication.

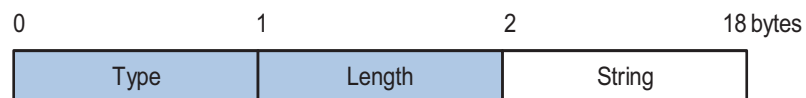
The EAP-message field, whose format is shown in Figure 70, is used to encapsulate EAP packets. The maximum size of the string field is 253 bytes. EAP packets with their size larger than 253 bytes are fragmented and are encapsulated in multiple EAP-message fields. The type code of the EAP-message field is 79.

Figure 70 The format of an EAP-message field



The Message-authenticator field, whose format is shown in Figure 71, 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 71 The format of an Message-authenticator field



802.1x Authentication Procedure The Switch 4210 can authenticate supplicant systems in EAP terminating mode or EAP relay mode.

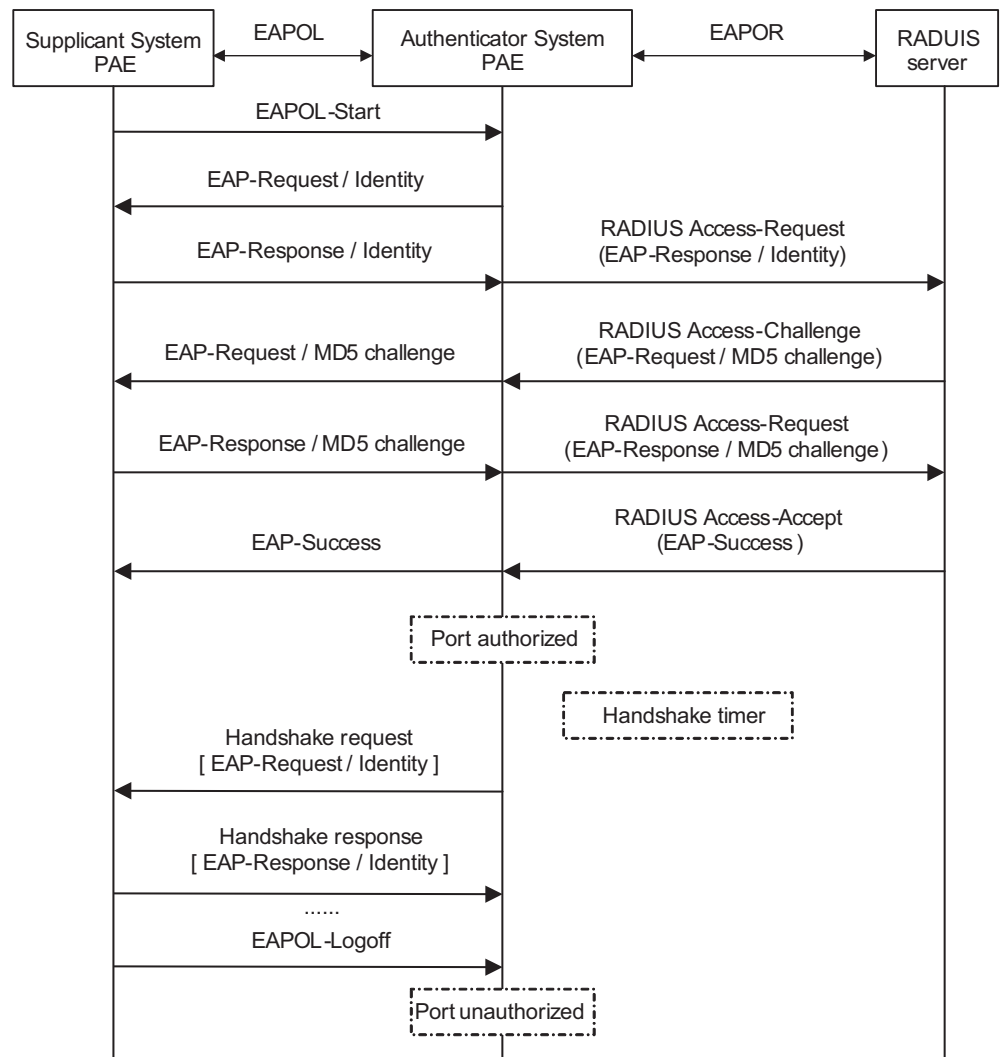
EAP relay mode

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 PEAP (protected extensible authentication protocol), are available in the EAP relay mode.

- EAP-MD5 authenticates the supplicant system. The RADIUS server sends MD5 keys (contained in EAP-request/MD5 challenge packets) to the supplicant system, which in turn encrypts the passwords using the MD5 keys.
- EAP-TLS 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 72 describes the basic EAP-MD5 authentication procedure.

Figure 72 802.1x authentication procedure (in EAP relay mode)

The detailed procedure is as follows.

- A supplicant system launches an 802.1x client to initiate an access request by sending an EAPoL-start packet to the switch, with its user name and password provided. The 802.1x client program then forwards the packet to the switch to start the authentication process.
- Upon receiving the authentication request packet, the switch sends an EAP-request/identity packet to ask the 802.1x client for the user name.
- The 802.1x client responds by sending an EAP-response/identity packet to the switch with the user name contained in it. The switch then encapsulates the packet in a RADIUS Access-Request packet and forwards it to the RADIUS server.
- Upon receiving the packet from the switch, the RADIUS server retrieves the user name from the packet, finds the corresponding password by matching the user name in its database, encrypts the password using a randomly-generated key, and sends the key to the switch through an RADIUS access-challenge packet. The switch then sends the key to the 802.1x client.

- Upon receiving the key (encapsulated in an EAP-request/MD5 challenge packet) from the switch, the client program encrypts the password of the supplicant system with the key and sends the encrypted password (contained in an EAP-response/MD5 challenge packet) to the RADIUS server through the switch. (Normally, the encryption is irreversible.)
- The RADIUS server compares the received encrypted password (contained in a RADIUS access-request packet) with the locally-encrypted password. If the two match, it will then send feedbacks (through a RADIUS access-accept packet and an EAP-success packet) to the switch to indicate that the supplicant system is authenticated.
- The switch changes the state of the corresponding port to accepted state to allow the supplicant system to access the network.
- The supplicant system can also terminate the authenticated state by sending EAPoL-Logoff packets to the switch. The switch then changes the port state from accepted to rejected.

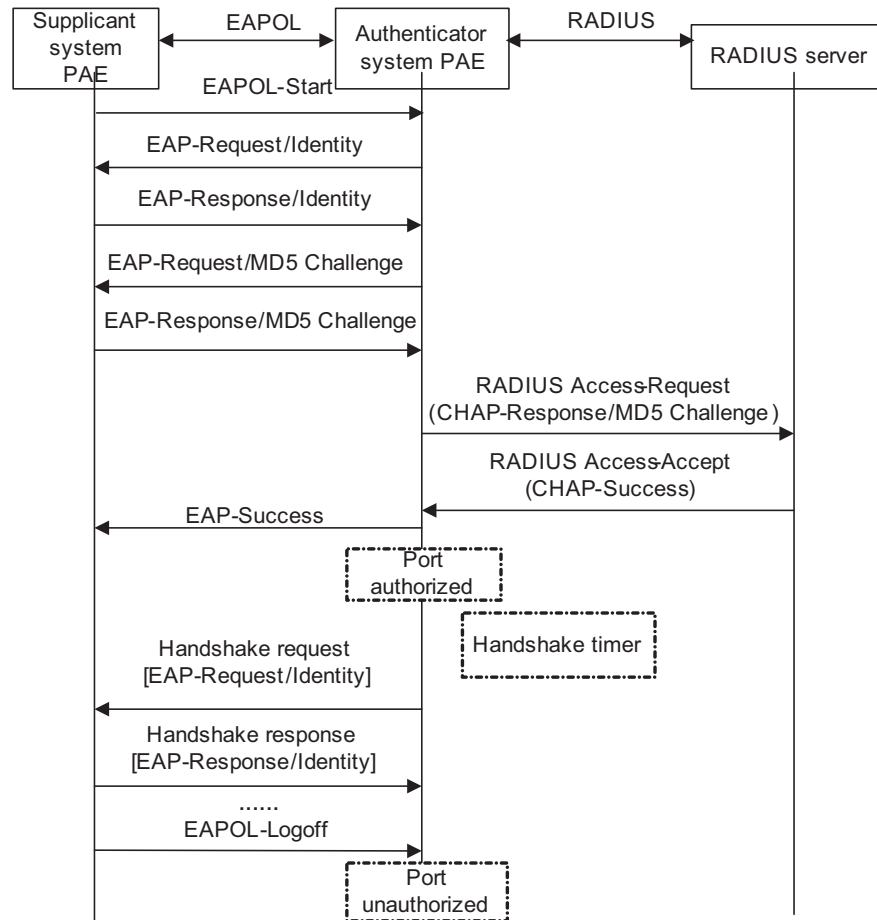


*In EAP relay mode, packets are not modified during transmission. Therefore if one of the four ways are used (that is, PEAP, EAP-TLS, EAP-TTLS or EAP-MD5) to authenticate, ensure that the authenticating ways used on the supplicant system and the RADIUS server are the same. However for the switch, you 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 73 illustrates the authentication procedure (assuming that CHAP is employed between the switch and the RADIUS server).

Figure 73 802.1x 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 number of retries by using the **dot1x retry** command. An online user will be considered offline when the switch has not received any response packets after a certain number of handshake request transmission retries.
- **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 will initiate 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.

802.1x Implementation on an Switch 4210 Family

In addition to the earlier mentioned 802.1x features, the Switch 4210 is also capable of the following:

- Checking supplicant systems for proxies, multiple network adapters, and so on (This function needs the cooperation of a CAMS server.)
- Checking client version
- The Guest VLAN function



3Com'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

The Switch 4210 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.



- The client-checking function needs the support of 3Com'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.



- The 802.1x client version-checking function needs the support of 3Com'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 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.

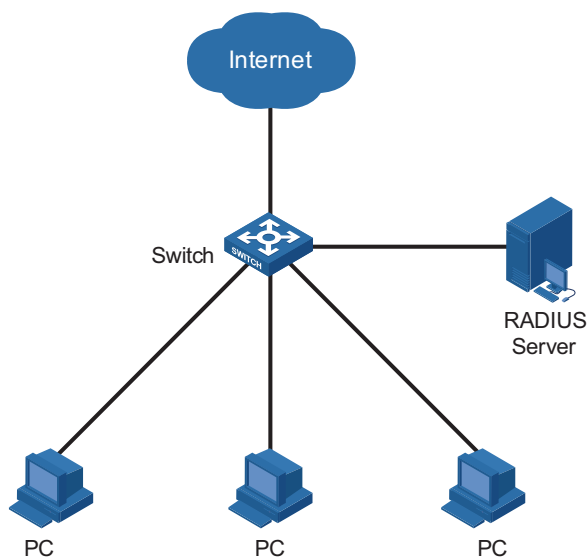
Normally, the Guest VLAN function is coupled with the dynamic VLAN delivery function.

Refer to “Introduction to AAA” on page 237 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.

Figure 74 802.1x re-authentication



802.1x re-authentication can be enabled in one of the following two ways:

- The RADIUS server triggers the switch to perform 802.1x user re-authentication. The RADIUS server sends the switch an Access-Accept packet with the Termination-Action field of 1. Upon receiving the packet, the switch re-authenticates users periodically.
- You enable 802.1x re-authentication on the switch. With 802.1x re-authentication enabled, the switch re-authenticates users periodically.

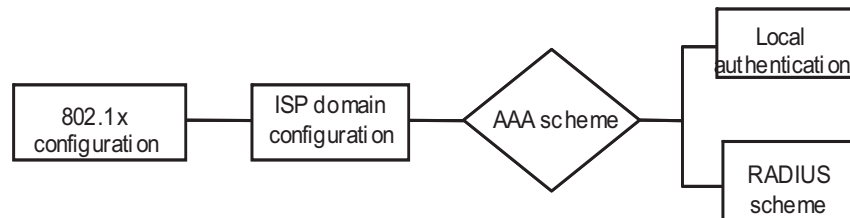


802.1x re-authentication fails if a CAMS server is configured to perform authentication but not accounting because a CAMS server establishes a user session after it begins to perform accounting. Therefore, to enable 802.1x re-authentication, do not configure the accounting none command in the domain. This restriction does not apply to other types of servers.

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, HWTACACS or local authentication scheme).

Figure 75 802.1x 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 adopt a local authentication scheme, you need to configure user names and passwords manually on the switches. Users can pass the authentication through 802.1x client if they provide user names and passwords that match those configured on the switches.
- If you use the RADIUS scheme, the supplicant systems are authenticated by a remote RADIUS server. In this case, you need to configure the user names and passwords on the RADIUS server and perform RADIUS client-related configuration on the switch.
- 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 “AAA Configuration” on page 245 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, a HWTACACS 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

Table 162 Configure basic 802.1x functions

Operation	Command	Remarks
Enter system view	system-view	-
Enable 802.1x globally	dot1x	Required By default, 802.1x is disabled globally.

Table 162 Configure basic 802.1x functions

Operation	Command	Remarks
Enable 802.1x for specified ports	In system view dot1x interface <i>interface-list</i> In port view interface <i>interface-type</i> <i>interface-number</i> dot1x quit	Required By default, 802.1x is disabled on all ports.
Set port access control mode for specified ports	dot1x port-control { authorized-force unauthorized-force auto } [interface <i>interface-list</i>]	Optional By default, an 802.1x-enabled port operates in the auto mode.
Set port access method for specified ports	dot1x port-method { macbased portbased } [interface <i>interface-list</i>]	Optional The default port access method is MAC-address-based (that is, the macbased keyword is used by default).
Set authentication method for 802.1x users	dot1x authentication-method { chap pap eap }	Optional By default, a switch performs CHAP authentication in EAP terminating mode.
Enable online user handshaking	dot1x handshake enable	Optional By default, online user handshaking is enabled.
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	-
Enable the handshaking packet secure function	dot1x handshake secure	Optional By default, the handshaking secure function is disabled.

**CAUTION:**

- 802.1x configurations take effect only after you enable 802.1x both globally and for specified ports.
- If you enable 802.1x for a port, you cannot set the maximum number of MAC addresses that can be learnt for the port. Meanwhile, if you set the maximum number of MAC addresses that can be learnt for a port, it is prohibited to enable 802.1x for the port.
- If you enable 802.1x for a port, it is not available to add the port to an aggregation group. Meanwhile, if a port has been added to an aggregation group, it is prohibited to enable 802.1x for the port.
- Changing the access control method on a port by the **dot1x port-method** command will forcibly log out the online 802.1x users on the port.
- When a device operates as an authentication server, its authentication method for 802.1x users cannot be configured as EAP.
- Handshaking packets need the support of the 3Com-proprietary client. They are used to test whether or not a user is online.
- As clients that are not of 3Com do not support the online user handshaking function, switches cannot receive handshaking 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.

- For the handshaking packet secure function to take effect, the clients that enable the function need to cooperate with the authentication server. If either the clients or the authentication server does not support the function, disabling the handshaking packet secure function is needed.

Timer and Maximum User Number Configuration

Table 163 Configure 802.1x timers and the maximum number of users

Operation	Command	Remarks
Enter system view	system-view	-
Set the maximum number of concurrent on-line users for specified ports	In system view dot1x max-user <i>user-number</i> [interface <i>interface-list</i>] In port view interface <i>interface-type interface-number</i> dot1x max-user <i>user-number</i> quit	Optional By default, a port can accommodate up to 256 users at a time.
Set the maximum retry times to send request packets	dot1x retry <i>max-retry-value</i>	Optional By default, the maximum retry times to send a request packet is 2. That is, the authenticator system sends a request packet to a supplicant system for up to two times by default.
Set 802.1x timers	dot1x timer { handshake-period <i>handshake-period-value</i> quiet-period <i>quiet-period-value</i> server-timeout <i>server-timeout-value</i> supp-timeout <i>supp-timeout-value</i> tx-period <i>tx-period-value</i> ver-period <i>ver-period-value</i> }	Optional The settings of 802.1x timers are as follows. <ul style="list-style-type: none"> ■ handshake-period-value: 15 seconds ■ quiet-period-value: 60 seconds ■ server-timeout-value: 100 seconds ■ supp-timeout-value: 30 seconds ■ tx-period-value: 30 seconds ■ ver-period-value: 30 seconds
Enable the quiet-period timer	dot1x quiet-period	Optional By default, the quiet-period timer is disabled.



- 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 802.1x features.

Configuring Proxy Checking

Table 164 Configure proxy checking

Operation	Command	Remarks
Enter system view	system-view	-
Enable proxy checking function globally	dot1x supp-proxy-check { logoff trap }	Required By default, the 802.1x proxy checking function is globally disabled.
Enable proxy checking for a port/specified ports	In system view dot1x supp-proxy-check { logoff trap } [interface interface-list] In port view interface interface-type interface-number dot1x supp-proxy-check { logoff trap } quit	Required By default, the 802.1x proxy checking is disabled on a port.



- The proxy checking function needs the cooperation of 3Com'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 Table 164 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

Table 165 Configure client version checking

Operation	Command	Remarks
Enter system view	system-view	-

Table 165 Configure client version checking

Operation	Command	Remarks
Enable 802.1x client version checking	In system view dot1x version-check [interface <i>interface-list</i>] In port view interface <i>interface-type</i> <i>interface-number</i> dot1x version-check quit	Required By default, 802.1x client version checking is disabled on a port.
Set the maximum number of retries to send version checking request packets	dot1x retry-version-max <i>max-retry-version-value</i>	Optional By default, the maximum number of retries to send version checking request packets is 3.
Set the client version checking period timer	dot1x timer ver-period <i>ver-period-value</i>	Optional By default, the timer is set to 30 seconds.



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.

Table 166 Enable DHCP-triggered authentication

Operation	Command	Remarks
Enter system view	system-view	-
Enable DHCP-triggered authentication	dot1x dhcp-launch	Required By default, DHCP-triggered authentication is disabled.

Configuring Guest VLAN

Table 167 Configure Guest VLAN

Operation	Command	Remarks
Enter system view	system-view	-
Configure port access method	dot1x port-method portbased	Required The default port access method is MAC-address-based. That is, the macbased keyword is used by default.
Enable the Guest VLAN function	In system view dot1x guest-vlan <i>vlan-id</i> [interface <i>interface-list</i>] In port view interface <i>interface-type</i> <i>interface-number</i> dot1x guest-vlan <i>vlan-id</i> quit	Required By default, the Guest VLAN function is disabled.

**CAUTION:**

- The Guest VLAN function is available only when the switch operates in the port-based authentication mode.
- Only one Guest VLAN can be configured for each switch.
- The Guest VLAN function cannot be implemented when the switch executes the **dot1x dhcp-launch** command to enable DHCP-triggered authentication. This is because that in that case the switch does not send authentication packets.

Configuring 802.1x Re-Authentication**Table 168** Enable 802.1x re-authentication

Operation	Command	Remarks
Enter system view	system-view	-
Enable 802.1x re-authentication on port(s)	In system view dot1x re-authenticate [interface <i>interface-list</i>] In port view dot1x re-authenticate	Required By default, 802.1x re-authentication is disabled on a port.



To enable 802.1x re-authentication on a port, you must first enable 802.1x globally and on the port.

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:

- 1 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.
- 2 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.

Table 169 Configure the re-authentication interval

Operation	Command	Remarks
Enter system view	system-view	-
Configure a re-authentication interval	dot1x timer reauth-period <i>reauth-period-value</i>	Optional By default, the re-authentication interval is 3,600 seconds.

Displaying and Debugging 802.1x

After performing the above configurations, you can display and verify the 802.1x-related configuration by executing the **display** command in any view.

You can clear 802.1x-related statistics information by executing the **reset** command in user view.

Table 170 Display and debug 802.1x

Operation	Command	Remarks
Display the configuration, session, and statistics information about 802.1x	display dot1x [sessions statistics] [interface interface-list]	This command can be executed in any view.
Clear 802.1x-related statistics information	reset dot1x statistics [interface interface-list]	Execute this command in user view.

Configuration Example

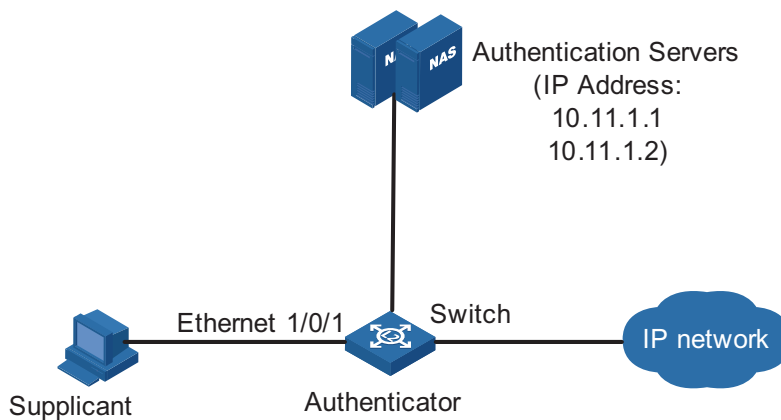
802.1x Configuration Example

Network requirements

- Authenticate users on all ports to control their accesses to the Internet. The switch operates in MAC address-based access control mode.
- All supplicant systems that pass the authentication belong to the default domain named "aabbcc.net". The domain can accommodate up to 30 users. As for authentication, a supplicant system is authenticated locally if the RADIUS server fails. And as for accounting, a supplicant system is disconnected by force if the RADIUS server fails. The name of an authenticated supplicant system is not suffixed with the domain name. A connection is terminated if the total size of the data passes through it during a period of 20 minutes is less than 2,000 bytes.
- The switch is connected to a server comprising of two RADIUS servers whose IP addresses are 10.11.1.1 and 10.11.1.2. The RADIUS server with an IP address of 10.11.1.1 operates as the primary authentication server and the secondary accounting server. The other operates as the secondary authentication server and primary accounting server. The password for the switch and the authentication RADIUS servers to exchange message is "name". And the password for the switch and the accounting RADIUS servers to exchange message is "money". The switch sends another packet to the RADIUS servers again if it sends a packet to the RADIUS server and does not receive response for 5 seconds, with the maximum number of retries of 5. And the switch sends a real-time accounting packet to the RADIUS servers once in every 15 minutes. A user name is sent to the RADIUS servers with the domain name truncated.
- The user name and password for local 802.1x authentication are "localuser" and "localpass" (in plain text) respectively. The idle disconnecting function is enabled.

Network diagram

Figure 76 Network diagram for AAA configuration with 802.1x and RADIUS enabled



Configuration procedure



Following configuration covers the major AAA/RADIUS configuration commands. Refer to "AAA Configuration" on page 245 for the information about these commands. Configuration on the client and the RADIUS servers is omitted.

Enable 802.1x globally.

```
<4210> system-view
System View: return to User View with Ctrl+Z.
[4210] dot1x
```

Enable 802.1x on Ethernet 1/0/1 port.

```
[4210] dot1x interface Ethernet 1/0/1
```

Set the access control method to be MAC-address-based (This operation can be omitted, as MAC-address-based is the default).

```
[4210] dot1x port-method macbased interface Ethernet 1/0/1
```

Create a RADIUS scheme named "radius1" and enter RADIUS scheme view.

```
[4210] radius scheme radius1
```

Assign IP addresses to the primary authentication and accounting RADIUS servers.

```
[4210-radius-radius1] primary authentication 10.11.1.1
[4210-radius-radius1] primary accounting 10.11.1.2
```

Assign IP addresses to the secondary authentication and accounting RADIUS server.

```
[4210-radius-radius1] secondary authentication 10.11.1.2
[4210-radius-radius1] secondary accounting 10.11.1.1
```

Set the password for the switch and the authentication RADIUS servers to exchange messages.

```
[4210-radius-radius1] key authentication name

# Set the password for the switch and the accounting RADIUS servers to exchange
messages.

[4210-radius-radius1] key accounting money

# Set the interval and the number of the retries for the switch to send packets to
the RADIUS servers.

[4210-radius-radius1] timer 5
[4210-radius-radius1] retry 5

# Set the timer for the switch to send real-time accounting packets to the RADIUS
servers.

[4210-radius-radius1] timer realtime-accounting 15

# Configure to send the user name to the RADIUS server with the domain name
truncated.

[4210-radius-radius1] user-name-format without-domain
[4210-radius-radius1] quit

# Create the domain named "aabbcc.net" and enter its view.

[4210] domain enable aabbcc.net

# Specify to adopt radius1 as the RADIUS scheme of the user domain. If RADIUS
server is invalid, specify to adopt the local authentication scheme.

[4210-isp-aabbcc.net] scheme radius-scheme radius1 local

# Specify the maximum number of users the user domain can accommodate to
30.

[4210-isp-aabbcc.net] access-limit enable 30

# Enable the idle disconnecting function and set the related parameters.

[4210-isp-aabbcc.net] idle-cut enable 20 2000
[4210-isp-aabbcc.net] quit
# Set the default user domain to be "aabbcc.net".
[4210] domain default enable aabbcc.net

# Create a local access user account.

[4210] local-user localuser
[4210-luser-localuser] service-type lan-access
[4210-luser-localuser] password simple localpass
```


18

HABP CONFIGURATION

Introduction to HABP

With 802.1x enabled, a switch authenticates and then authorizes 802.1x-enabled ports. Packets can be forwarded only by authorized ports. Received packets are, therefore, filtered for ports connected to a switch that is not authenticated and authorized by 802.1x. This means that you cannot manage the attached switches. 3Com authentication bypass protocol (HABP) is designed to address this problem.

An HABP packet carries the MAC addresses of the attached switches with it. It can bypass the 802.1x authentications when traveling between HABP-enabled switches, through which management devices can obtain the MAC addresses of the attached switches and thus the management of the attached switches is feasible.

HABP is implemented by HABP server and HABP client. Normally, an HABP server sends HABP request packets regularly to HABP clients to collect the MAC addresses of the attached switches. HABP clients respond to the HABP request packets and forward the HABP request packets to lower-level switches. HABP servers usually reside on management devices and HABP clients usually on attached switches.

For ease of switch management, it is recommended that you enable HABP for 802.1x-enabled switches.

HABP Server Configuration

With the HABP server launched, a management device sends HABP request packets regularly to the attached switches to collect their MAC addresses. You need also to configure the interval on the management device for an HABP server to send HABP request packets.

Table 171 Configure an HABP server

Operation	Command	Remarks
Enter system view	system-view	-
Enable HABP	habp enable	Optional By default, HABP is enabled.
Configure the current switch to be an HABP server	habp server vlan <i>vlan-id</i>	Required By default, a switch operates as an HABP client after you enable HABP on the switch. If you want to use the switch as a management switch, you need to configure the switch to be an HABP server.

Table 171 Configure an HABP server

Operation	Command	Remarks
Configure the interval to send HABP request packets.	habp timer <i>interval</i>	Optional The default interval for an HABP server to send HABP request packets is 20 seconds.

HABP Client Configuration

HABP clients reside on switches attached to HABP servers. After you enable HABP for a switch, the switch operates as an HABP client by default. So you only need to enable HABP on a switch to make it an HABP client.

Table 172 Configure an HABP client

Operation	Command	Remarks
Enter system view	system-view	-
Enable HABP	habp enable	Optional HABP is enabled by default. And a switch operates as an HABP client after you enable HABP for it.

Displaying HABP

After performing the above configuration, you can display and verify your HABP-related configuration by execute the **display** command in any view.

Table 173 Display HABP

Operation	Command	Remarks
Display HABP configuration and status	display habp	These commands can be executed in any view.
Display the MAC address table maintained by HABP	display habp table	
Display statistics on HABP packets	display habp traffic	

19

SYSTEM-GUARD CONFIGURATION

The system-guard function checks system-guard-enabled ports regularly to determine if the ports are under attack. With this function enabled, if the number of the packets received by a system-guard-enabled port exceeds the set threshold, the port is regarded to be under attack. The switch then limits the rate of the port and resumes port checking operation after a specific period elapses.

System-Guard Configuration

The system guard configuration includes:

- Enabling the system-guard function
- Configuring system-guard-related parameters
- Specifying system-guard-enabled ports

Enabling the System-Guard function

Table 174 lists the operations to enable the system-guard function.

Table 174 Enable the system-guard function

Operation	Commands	Description
Enter system view	system-view	-
Enable the system-guard function	system-guard enable	Required By default, The system-guard function is disabled.

Configuring System-Guard-Related Parameters

Table 175 lists the operations to configure system-guard-related parameters, including system-guard mode, checking interval, threshold (in terms of the number of the received packets), and controlling period. Note that the configuration takes effect only after you enable the system-guard function.

Table 175 Configure system-guard related parameters

Operation	Command	Description
Enter system view	system-view	-
Configure system-guard-related parameters	system-guard mode rate-limit interval-time threshold timeout	Required The default system-guard-related parameters are as follows. interval-time: 5 seconds threshold: 64 timeout: 60 seconds

Enabling System-Guard on Ports

Table 176 lists the operations to enable system-guard on ports.

Table 176 Enable system-guard on ports

Operation	Command	Description
Enter system view	system-view	-
Enable system-guard on specified ports	system-guard permit interface-list	Required



After system-guard is enabled on a port, if the number of packets the port received and sent to the CPU in a specified interval exceeds the specified threshold, the system considers that the port is under attack and begins to limit the packet receiving rate on the port (this function is also called inbound rate limit). If the rate of incoming packets on the port exceeds the threshold of inbound rate limit, any service packets, including BPDU packets, are possible to be dropped at random, which may result in state transition of STP.

Displaying and Maintaining the System-Guard Function

After the above configuration, you can display and verify your configuration by performing the operation listed in Table 177.

Table 177 Display and debug the system-guard function

Operation	Command	Description
Display system-guard configuration	display system-guard config	This command can be executed in any view.

20

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 user name, password, and some other attributes) is configured on this device, and users are authenticated on this device instead of on a remote device. Local authentication is fast and requires lower operational cost, but has the deficiency that information storage capacity is limited by device hardware.
- Remote authentication: Users are authenticated remotely through the RADIUS protocol. This device (for example, a 3Com series switch) acts as the client to communicate with the RADIUS server. You can use standard or extended RADIUS protocols in conjunction with such systems as iTELLIN/CAMS for user authentication. Remote authentication allows convenient centralized management and is feature-rich. However, to implement remote authentication, a server is needed and must be configured properly.

Authorization

AAA supports the following authorization methods:

- Direct authorization: Users are trusted and directly authorized.
- Local authorization: Users are authorized according to the related attributes configured for their local accounts on this device.
- RADIUS authorization: Users are authorized after they pass RADIUS authentication. In RADIUS protocol, authentication and authorization are combined together, and authorization cannot be performed alone without authentication.

- 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 server.

Introduction to ISP Domain An Internet service provider (ISP) domain is a group of users who belong to the same ISP. For a user name in the format of `userid@isp-name`, the `isp-name` following the "@" character is the ISP domain name. The access device uses `userid` as the user name for authentication, and `isp-name` as the domain name.

In a multi-ISP environment, the users connected to the same access device may belong to different domains. Since the users of different ISPs may have different attributes (such as different forms of user name and password, different service types/access rights), it is necessary to distinguish the users by setting ISP domains.

You can configure a set of ISP domain attributes (including AAA policy, RADIUS scheme, and so on) for each ISP domain independently in ISP domain view.

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

RADIUS (remote authentication dial-in user service) 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.

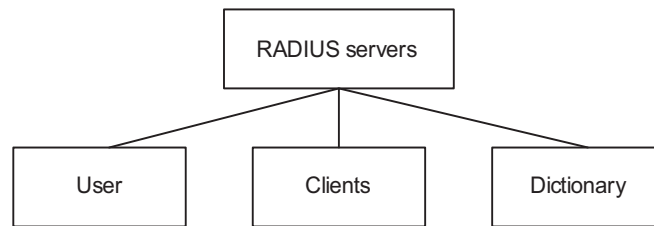
RADIUS operates in the client/server model.

- 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 77):

- Users: This database stores information about users (such as user name, password, protocol adopted and IP address).
- Clients: This database stores information about RADIUS clients (such as shared key).
- Dictionary: The information stored in this database is used to interpret the attributes and attribute values in the RADIUS protocol.

Figure 77 Databases in a RADIUS server

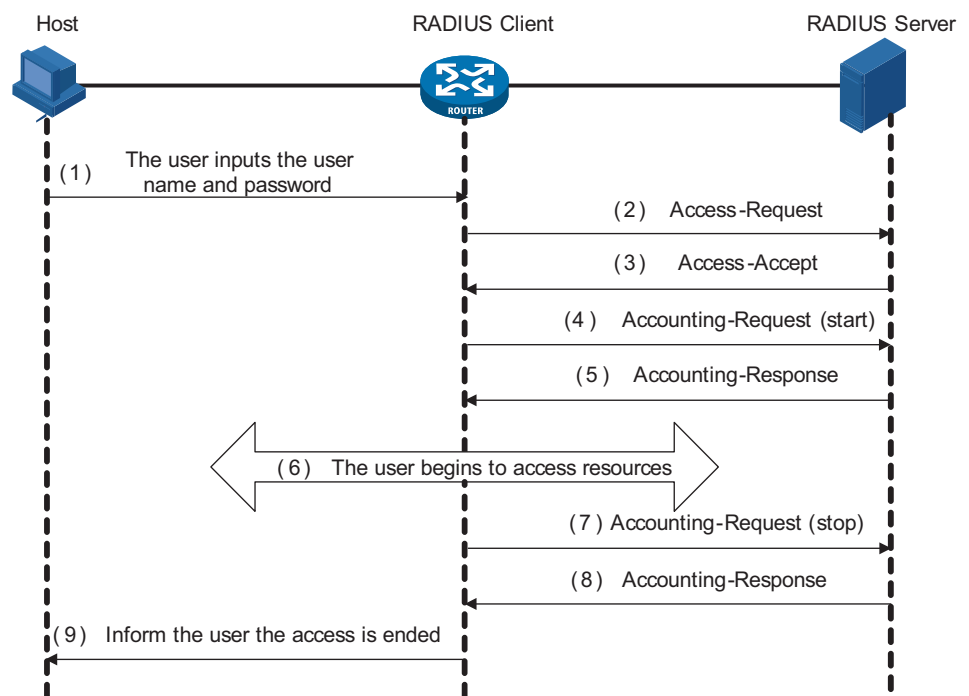


In addition, a RADIUS server can act as a client of some other AAA server to provide authentication or accounting proxy service.

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 78 depicts the message exchange procedure between user, switch and RADIUS server.

Figure 78 Basic message exchange procedure of RADIUS

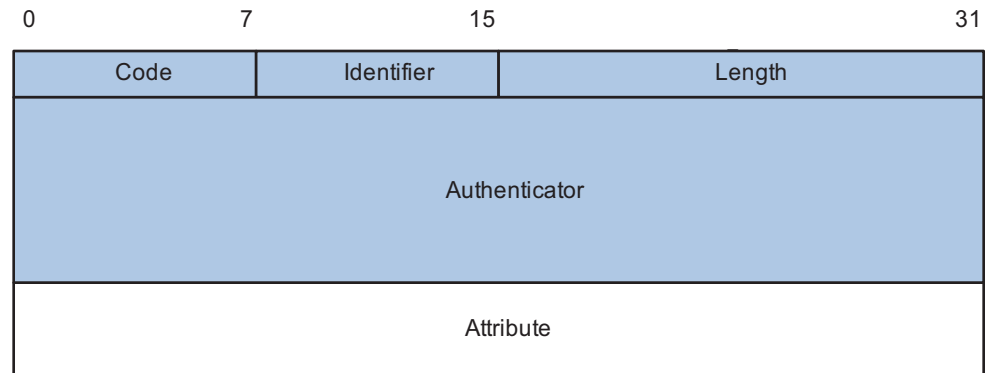


The basic message exchange procedure of RADIUS is as follows:

- 1 The user enters the user name and password.
- 2 The RADIUS client receives the user name and password, and then sends an authentication request (Access-Request) to the RADIUS server.
- 3 The RADIUS server compares the received user information with that in the Users database to authenticate the user. If the authentication succeeds, the RADIUS server sends back to the RADIUS client an authentication response (Access-Accept), which contains the user's authorization information. If the authentication fails, the server returns an Access-Reject response.
- 4 The RADIUS client accepts or denies the user depending on the received authentication result. If it accepts the user, the RADIUS client sends a start-accounting request (Accounting-Request, with the Status-Type attribute value = start) to the RADIUS server.
- 5 The RADIUS server returns a start-accounting response (Accounting-Response).
- 6 The user starts to access network resources.
- 7 The RADIUS client sends a stop-accounting request (Accounting-Request, with the Status-Type attribute value = stop) to the RADIUS server.
- 8 The RADIUS server returns a stop-accounting response (Accounting-Response).
- 9 The access to network resources is ended.

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 79 depicts the format of RADIUS messages.

Figure 79 RADIUS message format

- 1 The Code field (one byte) decides the type of RADIUS message, as shown in Table 178.

Table 178 Description of the major values of the Code field

Code	Message type	Message description
1	Access-Request	<p>Direction: client->server.</p> <p>The client transmits this message to the server to determine if the user can access the network.</p> <p>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.</p>
2	Access-Accept	<p>Direction: server->client.</p> <p>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).</p>
3	Access-Reject	<p>Direction: server->client.</p> <p>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).</p>
4	Accounting-Request	<p>Direction: client->server.</p> <p>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).</p> <p>This message carries almost the same attributes as those carried in the Access-Request message.</p>
5	Accounting-Response	<p>Direction: server->client.</p> <p>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.</p>

- 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 179 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.

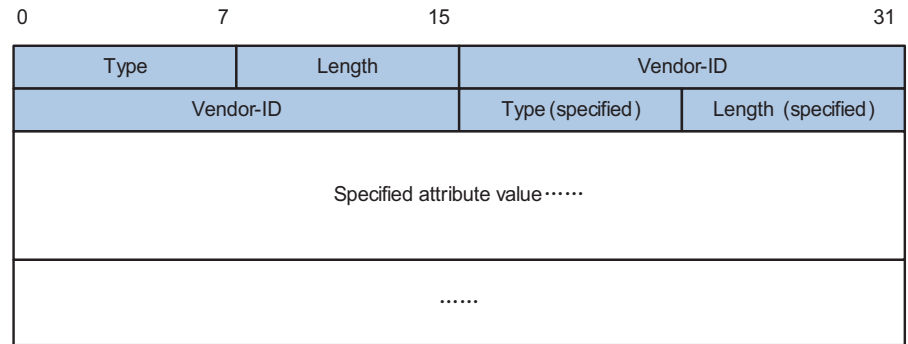
Table 179 RADIUS attributes

Type field value	Attribute type	Type field value	Attribute type
1	User-Name	23	Framed-IPX-Network
2	User-Password	24	State
3	CHAP-Password	25	Class
4	NAS-IP-Address	26	Vendor-Specific
5	NAS-Port	27	Session-Timeout
6	Service-Type	28	Idle-Timeout
7	Framed-Protocol	29	Termination-Action
8	Framed-IP-Address	30	Called-Station-Id
9	Framed-IP-Netmask	31	Calling-Station-Id
10	Framed-Routing	32	NAS-Identifier
11	Filter-ID	33	Proxy-State
12	Framed-MTU	34	Login-LAT-Service
13	Framed-Compression	35	Login-LAT-Node
14	Login-IP-Host	36	Login-LAT-Group
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 80 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 80 Vendor-specific attribute format



21

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.

Table 180 AAA configuration tasks (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 Local authentication RADIUS authentication Use one of the authentication methods You need to configure RADIUS before performing RADIUS authentication
	"Configuring Dynamic VLAN Assignment" Optional
	"Configuring the Attributes of a Local User" Optional
	"Cutting Down User Connections Forcibly" Optional

Table 181 AAA configuration tasks (configuring separate AAA schemes for an ISP domain)

Task	Remarks
AAA configuration	"Creating an ISP Domain and Configuring Its Attributes" Required
	"Configuring separate AAA schemes" Required
"Configuring an AAA Scheme for an ISP Domain"	Required With separate AAA schemes, you can specify authentication, authorization and accounting schemes respectively. You need to configure RADIUS before performing RADIUS 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

Table 182 Create an ISP domain and configure its attributes

Operation	Command	Remarks
Enter system view	system-view	-
Configure the form of the delimiter between the user name and the ISP domain name	domain delimiter { at dot }	Optional By default, the delimiter between the user name and the ISP domain name is "@".
Create an ISP domain or set an ISP domain as the default ISP domain	domain { isp-name default { disable enable isp-name } }	Required If no ISP domain is set as the default ISP domain, the ISP domain "system" is used as the default ISP domain.
Set the status of the ISP domain	state { active block }	Optional By default, an ISP domain is in the active state, that is, all the users in the domain are allowed to request network service.
Set the maximum number of access users that the ISP domain can accommodate	access-limit { disable enable max-user-number }	Optional By default, there is no limit on the number of access users that the ISP domain can accommodate.
Set the idle-cut function	idle-cut { disable enable minute flow }	Optional By default, the idle-cut function is disabled.
Set the accounting-optional switch	accounting optional	Optional By default, the accounting-optional switch is off.
Set the messenger function	messenger time { enable limit interval disable }	Optional By default, the messenger function is disabled.
Set the self-service server location function	self-service-url { disable enable url-string }	Optional By default, the self-service server location function is disabled.



Note that:

- On the Switch 4210, each access user belongs to an ISP domain. You can configure up to 16 ISP domains on the switch. When a user logs in, if no ISP domain name is carried in the user name, the switch assumes that the user belongs to the default ISP domain.
- If you have configured to use "." as the delimiter, for a user name 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 user name.
- If the system does not find any available accounting server or fails to communicate with any accounting server when it performs accounting for a user, it does not disconnect the user as long as the accounting optional

command has been executed, though it cannot perform accounting for the user in this case.

- The self-service server location function needs the cooperation of a RADIUS server that supports self-service, such as comprehensive access management server (CAMS). Through self-service, users can manage and control their account or card numbers by themselves. A server installed with self-service software is called a self-service server.
- 3Com'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 of the following AAA schemes:

Configuring a combined AAA scheme

You can use the **scheme** command to specify an AAA scheme for an ISP domain. If you specify a RADIUS scheme, the authentication, authorization and accounting will be uniformly implemented by the RADIUS server(s) specified in the RADIUS scheme. In this way, you cannot specify different schemes for authentication, authorization and accounting respectively.

Table 183 Configure a combined AAA scheme

Operation	Command	Remarks
Enter system view	system-view	-
Create an ISP domain and enter its view, or enter the view of an existing ISP domain	domain <i>isp-name</i>	Required
Configure an AAA scheme for the ISP domain	scheme { local none radius-scheme <i>radius-scheme-name</i> [local] }	Required By default, an ISP domain uses the local AAA scheme.



CAUTION:

- You can execute the **scheme radius-scheme** *radius-scheme-name* command to adopt an already configured RADIUS scheme to implement all the three AAA functions. If you adopt the local scheme, only the authentication and authorization functions are implemented, the accounting function cannot be implemented.
- If you execute the **scheme radius-scheme** *radius-scheme-name* **local** command, the local scheme is used as the secondary scheme in case no RADIUS server is available. That is, if the communication between the switch and a RADIUS server is normal, no local authentication is performed; otherwise, local authentication is performed.
- If you execute the **scheme local** or **scheme none** command to adopt **local** or **none** as the primary scheme, the local authentication is performed or no authentication is performed. In this case you cannot specify any RADIUS scheme at the same time.
- If you execute the **scheme none** command, the FTP users in the domain will not pass the authentication. So, to allow users to use the FTP service, you should not use **none** scheme.

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, or none.
 - Authorization: none.
 - Accounting: RADIUS 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 or local.

Table 184 Configure separate AAA schemes

Operation	Command	Remarks
Enter system view	system-view	-
Create an ISP domain and enter its view, or enter the view of an existing ISP domain	domain <i>isp-name</i>	Required
Configure an authentication scheme for the ISP domain	authentication { radius-scheme <i>radius-scheme-name</i> [local] local none }	Optional By default, no separate authentication scheme is configured.
Configure an accounting scheme for the ISP domain	accounting { none radius-scheme <i>radius-scheme-name</i> }	Optional By default, no separate accounting scheme is configured.



- *If a combined AAA scheme is configured as well as the separate authentication, authorization and accounting schemes, the separate ones will be adopted in precedence.*
- *RADIUS scheme and local scheme do not support the separation of authentication and authorization. Therefore, pay attention when you make authentication and authorization configuration for a domain: When the **scheme radius-scheme** or **scheme local** command is executed and the **authentication** command is not executed, the authorization information returned from the RADIUS or local scheme still takes effect even if the **authorization none** command is executed.*

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 “802.1x Configuration” on page 211.

Table 185 Configure dynamic VLAN assignment

Operation	Command	Remarks
Enter system view	system-view	-
Create an ISP domain and enter its view	domain <i>isp-name</i>	-
Set the VLAN assignment mode	vlan-assignment-mode { integer string }	Optional By default, the VLAN assignment mode is integer.
Create a VLAN and enter its view	vlan <i>vlan-id</i>	-
Set a VLAN name for VLAN assignment	name <i>string</i>	This operation is required if the VLAN assignment mode is set to string.



CAUTION:

- *In string mode, if the VLAN ID assigned by the RADIUS server is a character string containing only digits (for example, 1024), the switch first regards it as an integer VLAN ID: the switch transforms the string to an integer value and judges if the value is in the valid VLAN ID range; if it is, the switch 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 user name. To make a user who is requesting network service pass local authentication, you should add an entry in the local user database on the switch for the user.

Table 186 Configure the attributes of a local user

Operation	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 By default, the password display mode of all access users is auto , indicating the passwords of access users are displayed in the modes set by the password command.
Add a local user and enter local user view	local-user user-name	Required By default, there is no local user in the system.
Set a password for the local user	password { simple cipher } password	Required
Set the status of the local user	state { active block }	Optional By default, the user is in active state, that is, the user is allowed to request network services.
Authorize the user to access specified type(s) of service	service-type { ftp lan-access { telnet ssh terminal }* [level level] }	Required By default, the system does not authorize the user to access any service.
Set the privilege level of the user	level level	Optional By default, the privilege level of the user is 0.
Configure the authorization VLAN for the local user	authorization vlan string	Required By default, no authorization 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 When binding the user to a remote port, you must use nas-ip ip-address to specify a remote access server IP address (here, <i>ip-address</i> is 127.0.0.1 by default, representing this device). When binding the user to a local port, you need not use nas-ip ip-address .

**CAUTION:**

- The following characters are not allowed in the user-name string: !:*?<>. And you cannot input more than one "@" in the string.
- After the **local-user password-display-mode cipher-force** command is executed, any password will be displayed in cipher mode even though you specify to display a user password in plain text by using the **password** command.
- If a user name and password is required for user authentication (RADIUS authentication as well as local authentication), the command level that a user

can access after login is determined by the privilege level of the user. For SSH users using RSA shared key for authentication, the commands they can access are determined by the levels set on their user interfaces.

- If the configured authentication method is none or password authentication, the command level that a user can access after login is determined by the level of the user interface.
- If the clients connected to a port have different authorization VLANs, only the first client passing the MAC address authentication can be assigned with an authorization VLAN. The switch will not assign authorization 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 authorization VLAN to a port.
- For local **RADIUS** authentication or **local** authentication to take effect, the VLAN assignment mode must be set to **string** after you specify authorization VLANs for local users.

Cutting Down User Connections Forcibly

Table 187 Cut down user connections forcibly

Operation	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



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.

Table 188 RADIUS configuration tasks (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
Configuring the RADIUS server	"Enabling the User Re-Authentication at Restart Function"	Optional
	Refer to "Configuring the Type of RADIUS Servers to be Supported" on page 257.	-

Table 189 RADIUS configuration tasks (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 network access server and shared key enabled and allowed on 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 "Configuring the Type of RADIUS Servers to be Supported" on page 257 -	

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.



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 Task List” on page 245).

Creating a RADIUS Scheme

The RADIUS protocol configuration is performed on a RADIUS scheme basis. You should first create a RADIUS scheme and enter its view before performing other RADIUS protocol configurations.

Table 190 Create a RADIUS scheme

Operation	Command	Remarks
Enter system view	system-view	-
Enable RADIUS authentication port	radius client enable	Optional By default, RADIUS authentication port is enabled.
Create a RADIUS scheme and enter its view	radius scheme <i>radius-scheme-name</i>	Required By default, a RADIUS scheme named "system" has already been created in the system.



A RADIUS scheme can be referenced by multiple ISP domains simultaneously.

Configuring RADIUS Authentication/Authorization Servers

Table 191 Configure RADIUS authentication/authorization servers

Operation	Command	Remarks
Enter system view	system-view	-
Create a RADIUS scheme and enter its view	radius scheme <i>radius-scheme-name</i>	Required By default, a RADIUS scheme named "system" has already been created in the system.
Set the IP address and port number of the primary RADIUS authentication/authorization server	primary authentication <i>ip-address [port-number]</i>	Required By default, the IP address and UDP port number of the primary server are 0.0.0.0 and 1812 respectively for a newly created RADIUS scheme.
Set the IP address and port number of the secondary RADIUS authentication/authorization server	secondary authentication <i>ip-address [port-number]</i>	Optional By default, the IP address and UDP port number of the secondary server are 0.0.0.0 and 1812 respectively for a newly created RADIUS scheme.



- 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

Table 192 Configure RADIUS accounting servers

Operation	Command	Remarks
Enter system view	system-view	-
Create a RADIUS scheme and enter its view	radius scheme <i>radius-scheme-name</i>	Required By default, a RADIUS scheme named "system" has already been created in the system.
Set the IP address and port number of the primary RADIUS accounting server	primary accounting <i>ip-address [port-number]</i>	Required By default, the IP address and UDP port number of the primary accounting server are 0.0.0.0 and 1813 for a newly created RADIUS scheme.
Set the IP address and port number of the secondary RADIUS accounting server	secondary accounting <i>ip-address [port-number]</i>	Optional By default, the IP address and UDP port number of the secondary accounting server are 0.0.0.0 and 1813 for a newly created RADIUS scheme.
Enable stop-accounting request buffering	stop-accounting-buffer enable	Optional By default, stop-accounting request buffering is enabled.
Set the maximum number of transmission attempts of a buffered stop-accounting request.	retry stop-accounting <i>retry-times</i>	Optional By default, the system tries at most 500 times to transmit a buffered stop-accounting request.
Set the maximum allowed number of continuous real-time accounting failures	retry realtime-accounting <i>retry-times</i>	Optional By default, the maximum allowed number of continuous real-time accounting failures is five. If five continuous failures occur, the switch cuts down the user connection.



- *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.

Table 193 Configure shared keys for RADIUS messages

Operation	Command	Remarks
Enter system view	system-view	-
Create a RADIUS scheme and enter its view	radius scheme <i>radius-scheme-name</i>	Required By default, a RADIUS scheme named "system" has already been created in the system.
Set a shared key for RADIUS authentication/authorization messages	key authentication <i>string</i>	Required By default, no shared key is created.
Set a shared key for RADIUS accounting messages	key accounting <i>string</i>	Required By default, no shared key is created.



CAUTION: The authentication/authorization shared key and the accounting shared key you set on the switch must be respectively consistent with the shared key on the authentication/authorization server and the shared key on the accounting server.

Configuring the Maximum Number of RADIUS Request Transmission Attempts

The communication in RADIUS is unreliable because this protocol uses UDP packets to carry its data. Therefore, it is necessary for the switch to retransmit a RADIUS request if it gets no response from the RADIUS server after the response timeout timer expires. If the switch gets no answer after it has tried the maximum number of times to transmit the request, the switch considers that the request fails.

Table 194 Configure the maximum transmission attempts of a RADIUS request

Operation	Command	Remarks
Enter system view	system-view	-

Table 194 Configure the maximum transmission attempts of a RADIUS request

Operation	Command	Remarks
Create a RADIUS scheme and enter its view	radius scheme <i>radius-scheme-name</i>	Required By default, a RADIUS scheme named "system" has already been created in the system.
Set the maximum number of RADIUS request transmission attempts	retry <i>retry-times</i>	Optional By default, the system can try three times to transmit a RADIUS request.

Configuring the Type of RADIUS Servers to be Supported

Table 195 Configure the type of RADIUS servers to be supported

Operation	Command	Remarks
Enter system view	system-view	-
Create a RADIUS scheme and enter its view	radius scheme <i>radius-scheme-name</i>	Required By default, a RADIUS scheme named "system" has already been created in the system.
Configure the type of RADIUS servers to be supported	server-type { extended standard }	Optional



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.

Table 196 Set the status of RADIUS servers

Operation	Command	Remarks
Enter system view	system-view	-

Table 196 Set the status of RADIUS servers

Operation	Command	Remarks
Create a RADIUS scheme and enter its view	radius scheme <i>radius-scheme-name</i>	Required By default, a RADIUS scheme named "system" has already been created in the system.
Set the status of the primary RADIUS authentication/authorization server	state primary authentication { block active }	Optional By default, the primary RADIUS servers in the default RADIUS scheme "system" are in the active state, the secondary servers in the scheme are in the block state, and all RADIUS servers in all other RADIUS schemes are in the block state.
Set the status of the primary RADIUS accounting server	state primary accounting { block active }	
Set the status of the secondary RADIUS authentication/authorization server	state secondary authentication { block active }	
Set the status of the secondary RADIUS accounting server	state secondary accounting { block active }	

Configuring the Attributes of Data to be Sent to RADIUS Servers

Table 197 Configure the attributes of data to be sent to RADIUS servers

Operation	Command	Remarks
Enter system view	system-view	-
Create a RADIUS scheme and enter its view	radius scheme <i>radius-scheme-name</i>	Required By default, a RADIUS scheme named "system" has already been created in the system.
Set the format of the user names to be sent to RADIUS server	user-name-format { with-domain without-domain }	Optional By default, the user names sent from the switch to RADIUS server carry ISP domain names.
Set the units of data flows to RADIUS servers	data-flow-format data { byte giga-byte kilo-byte mega-byte } packet { giga-packet kilo-packet mega-packet one-packet }	Optional By default, in a RADIUS scheme, the data unit and packet unit for outgoing RADIUS flows are byte and one-packet respectively.
Set the MAC address format of the Calling-Station-Id (Type 31) field in RADIUS packets	calling-station-id mode { mode1 mode2 } { lowercase uppercase }	Optional By default, the MAC address format is XXXX-XXXX-XXXX, in lowercase.
Set the source IP address of outgoing RADIUS messages	RADIUS scheme view nas-ip ip-address System view radius nas-ip ip-address	Optional By default, no source IP address is set; and the IP address of the corresponding outbound interface is used as the source IP address.



- Generally, the access users are named in the *userid@isp-name* format. Here, *isp-name* after the "@" character represents the ISP domain name, by which the device determines which ISP domain a user belongs to. However, some old

RADIUS servers cannot accept the user names that carry ISP domain names. In this case, it is necessary to remove domain names from user names before sending the user names to RADIUS server. For this reason, the **user-name-format** command is designed for you to specify whether or not ISP domain names are carried in the user names to be sent to RADIUS server.

- For a RADIUS scheme, if you have specified to remove ISP domain names from user names, you should not use this RADIUS scheme in more than one ISP domain. Otherwise, such errors may occur: the RADIUS server regards two different users having the same name but belonging to different ISP domains as the same user (because the usernames sent to it are the same).
- In the default RADIUS scheme "system", ISP domain names are removed from user names by default.
- 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 Authentication Server Function

The switch provides the local RADIUS server function (including authentication and authorization), also known as the local RADIUS authentication server function, in addition to RADIUS client service, where separate authentication/authorization server and the accounting server are used for user authentication.

Table 198 Configure the local RADIUS authentication server function

Operation	Command	Remarks
Enter system view	system-view	-
Enable UDP port for local RADIUS authentication server	local-server enable	Optional By default, the UDP port for local RADIUS authentication server is enabled.
Configure the parameters of the local RADIUS server	local-server nas-ip ip-address key password	Required By default, a local RADIUS authentication server is configured with an NAS IP address of 127.0.0.1.



CAUTION:

- If you adopt the local RADIUS authentication server function, the UDP port number of the authentication/authorization server must be 1645, the UDP port number of the accounting server must be 1646, and the IP addresses of the servers must be set to the addresses of this switch.
- The message encryption key set by the **local-server nas-ip ip-address key password** command must be identical with the authentication/authorization message encryption key set by the **key authentication** command in the RADIUS scheme view of the RADIUS scheme on the specified NAS that uses this switch as its authentication server.
- The switch supports IP addresses and shared keys for up to 16 network access servers (NAS). That is, when acting as the local RADIUS authentication 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 authentication 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.

Table 199 Set timers for RADIUS servers

Operation	Command	Remarks
Enter system view	system-view	-
Create a RADIUS scheme and enter its view	radius scheme <i>radius-scheme-name</i>	Required By default, a RADIUS scheme named "system" has already been created in the system.
Set the response timeout time of RADIUS servers	timer response-timeout <i>seconds</i>	Optional By default, the response timeout time of RADIUS servers is three seconds.
Set the time that the switch waits before it try to re-communicate with primary server and restore the status of the primary server to active	timer quiet <i>minutes</i>	Optional By default, the switch waits five minutes before it restores the status of the primary server to active.
Set the real-time accounting interval	timer realtime-accounting <i>minutes</i>	Optional By default, the real-time accounting interval is 12 minutes.

Enabling Sending Trap Message when a RADIUS Server Goes Down

Table 200 Specify to send trap message when a RADIUS server goes down

Operation	Command	Remarks
Enter system view	system-view	-
Enable the sending of trap message when a RADIUS server is down	radius trap { authentication-server-down accounting-server-down }	Optional By default, the switch does not send trap message when a RADIUS server is down.



- *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



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.



*The switch can automatically generate the main attributes (NAS-ID, NAS-IP-address and session ID) contained in Accounting-On messages. However, you can also manually configure the NAS-IP-address with the **nas-ip** command. If*

you choose to manually configure the attribute, be sure to configure an appropriate valid IP address. If this attribute is not configured, the switch will automatically choose the IP address of a VLAN interface as the NAS-IP-address.

Table 201 Enable the user re-authentication at restart function

Operation	Command	Remarks
Enter system view	system-view	-
Enter RADIUS scheme view	radius scheme <i>radius-scheme-name</i>	-
Enable the user re-authentication at restart function	accounting-on enable [send times interval interval]	By default, this function is disabled. If you use this command without any parameter, the system will try at most 15 times to send an Accounting-On message at the interval of three seconds.

Displaying and Maintaining AAA

After the above configurations, you can execute the **display** commands in any view to view the configuration result and operation status of AAA, RADIUS and HWTACACS and verify your configuration.

You can use the **reset** command in user view to clear the corresponding statistics.

Table 202 Display AAA information

Operation	Command	Remarks
Display configuration information about one specific or all ISP domains	display domain [<i>isp-name</i>]	You can execute the display command in any view.
Display information about user connections	display connection [access-type { dot1x mac-authentication } domain <i>isp-name</i> interface <i>interface-type</i> <i>interface-number</i> ip <i>ip-address</i> mac <i>mac-address</i> radius-scheme <i>radius-scheme-name</i> vlan <i>vlan-id</i> ucibindex <i>ucib-index</i> user-name <i>user-name</i>]	
Display information about local users	display local-user [domain <i>isp-name</i> idle-cut { disable enable } vlan <i>vlan-id</i> service-type { ftp lan-access ssh telnet terminal } state { active block } user-name <i>user-name</i>]	

Table 203 Display and maintain RADIUS protocol information

Operation	Command	Remarks
Display RADIUS message statistics about local RADIUS authentication server	display local-server statistics	You can execute the display command in any view.
Display configuration information about one specific or all RADIUS schemes	display radius scheme [<i>radius-scheme-name</i>]	
Display RADIUS message statistics	display radius statistics	
Display buffered non-response stop-accounting requests	display stop-accounting-buffer { radius-scheme <i>radius-scheme-name</i> session-id <i>session-id</i> time-range <i>start-time</i> <i>stop-time</i> user-name <i>user-name</i> }	
Delete buffered non-response stop-accounting requests	reset stop-accounting-buffer { radius-scheme <i>radius-scheme-name</i> session-id <i>session-id</i> time-range <i>start-time</i> <i>stop-time</i> user-name <i>user-name</i> }	You can execute the reset command in user view.
Clear RADIUS message statistics	reset radius statistics	

AAA Configuration Examples

Remote RADIUS Authentication of Telnet/SSH Users



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 81, you are required to configure the switch so that the Telnet users logging into the switch are authenticated by the RADIUS server.

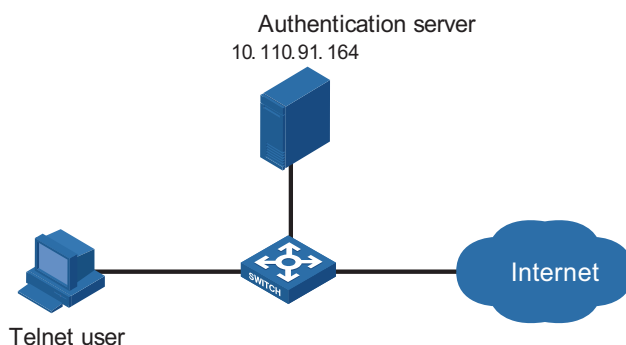
- A RADIUS authentication server with IP address 10.110.91.164 is connected to the switch.
- On the switch, set the shared key it uses to exchange messages with the authentication RADIUS server to "aabbcc".
- A CAMS server is used as the RADIUS server. You can select **extended** as the server-type in 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 user names and login passwords.

The Telnet user names added to the RADIUS server must be in the format of *userid@isp-name* if you have configured the switch to include domain names in the user names to be sent to the RADIUS server in the RADIUS scheme.

Network diagram

Figure 81 Remote RADIUS authentication of Telnet users



Configuration procedure

Enter system view.

```
<4210> system-view
```

Adopt AAA authentication for Telnet users.

```
[4210] user-interface vty 0 4
[4210-ui-vty0-4] authentication-mode scheme
[4210-ui-vty0-4] quit
```

Configure an ISP domain.

```
[4210] domain cams
[4210-isp-cams] access-limit enable 10
[4210-isp-cams] quit
```

Configure a RADIUS scheme.

```
[4210] radius scheme cams
[4210-radius-cams] accounting optional
[4210-radius-cams] primary authentication 10.110.91.164 1812
[4210-radius-cams] key authentication aabbcc
[4210-radius-cams] server-type Extended
[4210-radius-cams] user-name-format with-domain
[4210-radius-cams] quit
```

Associate the ISP domain with the RADIUS scheme.

```
[4210] domain cams
[4210-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



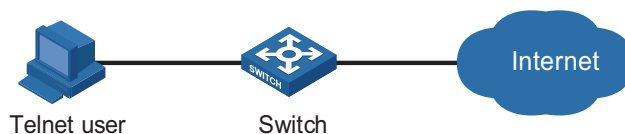
The configuration procedure for local authentication of FTP users is similar to that for Telnet users. The following text only takes Telnet users as example to describe the configuration procedure for local authentication.

Network requirements

In the network environment shown in Figure 82, you are required to configure the switch so that the Telnet users logging into the switch are authenticated locally.

Network diagram

Figure 82 Local authentication of Telnet users



Configuration procedure

Method 1: Using local authentication scheme.

Enter system view.

```
<4210> system-view
```

Adopt AAA authentication for Telnet users.

```
[4210] user-interface vty 0 4
[4210-ui-vty0-4] authentication-mode scheme
[4210-ui-vty0-4] quit
```

Create and configure a local user named "telnet".

```
[4210] local-user telnet
[4210-luser-telnet] service-type telnet
[4210-luser-telnet] password simple aabbcc
[4210-luser-telnet] quit
```

Configure an authentication scheme for the default "system" domain.

```
[4210] domain system
[4210-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.

Troubleshooting AAA

The RADIUS protocol operates at the application layer in the TCP/IP protocol suite. This protocol prescribes how the switch and the RADIUS server of the ISP exchange user information with each other.

Symptom 1: User authentication/authorization always fails.

Possible reasons and solutions:

- The user name is not in the userid@isp-name or userid.isp-name format, or the default ISP domain is not correctly specified on the switch - Use the correct user name format, or set a default ISP domain on the switch.
- The user is not configured in the database of the RADIUS server - Check the database of the RADIUS server, make sure that the configuration information about the user exists.
- The user input an incorrect password - Be sure to input the correct password.
- The switch and the RADIUS server have different shared keys - Compare the shared keys at the two ends, make sure they are identical.
- The switch cannot communicate with the RADIUS server (you can determine by pinging the RADIUS server from the switch) - Take measures to make the switch communicate with the RADIUS server normally.

Symptom 2: RADIUS packets cannot be sent to the RADIUS server.

Possible reasons and solutions:

- The communication links (physical/link layer) between the switch and the RADIUS server is disconnected/blocked - Take measures to make the links connected/unblocked.
- None or incorrect RADIUS server IP address is set on the switch - Be sure to set a correct RADIUS server IP address.
- One or all AAA UDP port settings are incorrect - Be sure to set the same UDP port numbers as those on the RADIUS server.

Symptom 3: The user passes the authentication and gets authorized, but the accounting information cannot be transmitted to the RADIUS server.

Possible reasons and solutions:

- The accounting port number is not properly set - Be sure to set a correct port number for RADIUS accounting.

- The switch requests that both the authentication/authorization server and the accounting server use the same device (with the same IP address), but in fact they are not resident on the same device - Be sure to configure the RADIUS servers on the switch according to the actual situation.

22

MAC AUTHENTICATION CONFIGURATION

MAC Authentication Overview

MAC 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.

You can implement MAC authentication locally or on a RADIUS server. When combined with RADIUS Authentication, this feature is referred to as RADIUS Authenticated Device Access, or RADA.

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 both the user name and the password.
- 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 Configuration” on page 245* for information about local user attributes.

Performing MAC Authentication on a RADIUS Server

When authentications are performed on a RADIUS server, the switch serves as a RADIUS client and completes MAC 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.
- 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 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. 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 Authentication Timers

The following timers function in the process of MAC 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 authentication, the switch does not initiate any MAC 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 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 Authentication Functions

Table 204 Configure basic MAC authentication functions

Operation	Command	Remarks
Enter system view	system-view	-
Enable MAC authentication globally	mac-authentication	Required Disabled by default
Enable MAC authentication for the specified port(s) or the current port	In system view mac-authentication interface interface-list In interface view interface interface-type interface-number mac-authentication quit	Use either method Disabled by default
Set the user name in MAC address mode for MAC authentication	mac-authentication authmode usernameasmacaddress [usernameformat { with-hyphen without-hyphen } { lowercase uppercase } fixedpassword password]	Optional By default, the MAC address of a user is used as the user name.

Table 204 Configure basic MAC authentication functions

Operation	Command	Remarks
Set the user name in fixed mode for MAC authentication	Set the user name in fixed mode for MAC authentication	mac-authentication authmode usernamefixed Optional By default, the user name is "mac" and no password is configured.
	Configure the user name	mac-authentication authusername <i>username</i>
	Configure the password	mac-authentication authpassword <i>password</i>
Specify an ISP domain for MAC authentication	mac-authentication domain <i>isp-name</i>	Required The default ISP domain (default domain) is used by default.
Configure the MAC authentication timers	mac-authentication timer { offline-detect <i>offline-detect-value</i> quiet <i>quiet-value</i> server-timeout <i>server-timeout-value</i> }	Optional The default timeout values are as follows: 300 seconds for offline detect timer; 60 seconds for quiet timer; and 100 seconds for server timeout timer

**CAUTION:**

- If MAC 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 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 authentication on a port before enabling it globally. However, the configuration will not take effect unless MAC authentication is enabled globally.

MAC Address Authentication Enhanced Function Configuration

MAC Address Authentication Enhanced Function Configuration Tasks

Table 205 MAC address authentication enhanced function configuration tasks

Operation	Description	Related section
Configure a Guest VLAN	Optional	"Configuring a Guest VLAN"
Configure the maximum number of MAC address authentication users allowed to access a port	Optional	"Configuring the Maximum Number of MAC Address Authentication Users Allowed to Access a Port"

Configuring a Guest VLAN



Different from Guest VLANs described in the 802.1x and System-Guard chapters, Guest VLANs mentioned in this section refer to Guest VLANs dedicated to MAC address authentication.

After completing configuration tasks in “Configuring Basic MAC Authentication Functions” on page 270 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.

Table 206 Configure a Guest VLAN

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

Table 206 Configure a Guest VLAN

Operation	Command	Description
Configure the Guest VLAN for the current port	mac-authentication guest-vlan <i>vlan-id</i>	Required By default, no Guest VLAN is configured for a port by default.
Return to system view	quit	-
Configure the interval at which the switch re-authenticates users in Guest VLANs	mac-authentication timer guest-vlan-reauth <i>interval</i>	Optional By default, the switch re-authenticates the users in Guest VLANs at the interval of 30 seconds by default.

**CAUTION:**

- If more than one client are connected to a port, you cannot configure a Guest VLAN for this port.
- When a Guest VLAN is configured for a port, only one MAC address authentication user can access the port. Even if you set the limit on the number of MAC address authentication users to more than one, the configuration does not take effect.
- The undo vlan command cannot be used to remove the VLAN configured as a Guest VLAN. If you want to remove this VLAN, you must remove the Guest VLAN configuration for it. Refer to “VLAN Configuration” on page 77 for a description of 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 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.

Table 207 Configure the maximum number of MAC address authentication users allowed to access a port

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

Table 207 Configure the maximum number of MAC address authentication users allowed to access a port

Operation	Command	Description
Configure the maximum number of MAC address authentication users allowed to access a port	mac-authentication max-auth-num <i>user-number</i>	Required By default, the maximum number of MAC address authentication users allowed to access a port is 256.

**CAUTION:**

- If both the limit on the number of MAC address authentication users and the limit on the number of users configured in the port security function are configured for a port, the smaller value of the two configured limits is adopted as the maximum number of MAC address authentication users allowed to access this port. Refer to “Port Security Configuration” on page 121 the *Port Security manual* for a description of 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

Configuring the Quiet MAC Function on a Port

You can configure whether to enable the quiet MAC function on a port. When this function is enabled, the MAC address connected to this port will be set as a quiet MAC address if its authentication fails. When this function is disabled, the MAC address will not become quiet no matter whether the authentication is failed.

Table 208 Configure the quiet MAC function on a port

Operation	Command	Description
Enter system view	system-view	-
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	-
Configure quiet MAC function on the port	mac-authentication intrusion-mode block-mac enable	Required Enabled by default.

Displaying and Debugging MAC Authentication

After the above configuration, you can execute the **display** command in any view to display system running of MAC Authentication configuration, and to verify the effect of the configuration. You can execute the **reset** command in user view to clear the statistics of MAC Authentication.

Table 209 Display and debug MAC Authentication

Operation	Command	Description
Display global or on-port information about MAC authentication	display mac-authentication [interface <i>interface-list</i>]	Available in any view
Clear the statistics of global or on-port MAC authentication	reset mac-authentication statistics [<i>interface</i> <i>interface-type</i> <i>interface-number</i>]	Available in user view

MAC Authentication Configuration Example

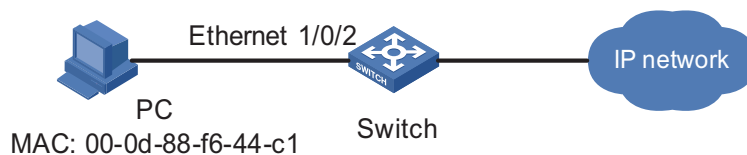
Network requirements

As illustrated in Figure 83, a supplicant is connected to the switch through port Ethernet 1/0/2.

- MAC authentication is required on port Ethernet 1/0/2 to control user access to the Internet.
- All users belong to domain aabbcc.net. The authentication performed is locally and the MAC address of the PC (00-0d-88-f6-44-c1) is used as both the user name and password.

Network Diagram

Figure 83 Network diagram for MAC authentication configuration



Configuration Procedure

Enable MAC authentication on port Ethernet 1/0/2.

```
<4210> system-view
[4210] mac-authentication interface Ethernet 1/0/2
```

Set the user name in MAC address mode for MAC authentication, requiring hyphenated lowercase MAC addresses as the usernames and passwords.

```
[4210] mac-authentication authmode usernameasmacaddress usernameformat with-hyphen lowercase
```

Add a local user.

- Specify the user name and password.

```
[4210] local-user 00-0d-88-f6-44-c1
[4210-luser-00-0d-88-f6-44-c1] password simple 00-0d-88-f6-44-c1
```

- Set the service type to "lan-access".

```
[4210-luser-00-0d-88-f6-44-c1] service-type lan-access
[4210-luser-00-0d-88-f6-44-c1] quit
```

Add an ISP domain named aabbcc.net.

```
[4210] domain aabbcc.net
New Domain added.
```

Specify to perform local authentication.

```
[4210-isp-aabbcc.net] scheme local
[4210-isp-aabbcc.net] quit
```

Specify aabbcc.net as the ISP domain for MAC authentication

```
[4210] mac-authentication domain aabbcc.net
```

Enable MAC authentication globally (This is usually the last step in configuring access control related features. Otherwise, a user may be denied of access to the networks because of incomplete configuration.)

```
[4210] mac-authentication
```

After doing so, your MAC authentication configuration will take effect immediately. Only users with the MAC address of 00-0d-88-f6-44-c1 are allowed to access the Internet through port Ethernet 1/0/2.

23

ARP CONFIGURATION

Introduction to ARP

ARP Function Address Resolution Protocol (ARP) is used to resolve an IP address into a data link layer address.

An IP address is the address of a host at the network layer. To send a network layer packet to a destination host, the device must know the data link layer address (MAC address, for example) of the destination host or the next hop. To this end, the IP address must be resolved into the corresponding data link layer address.



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 84 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 84 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 210 describes the fields of an ARP packet.

Table 210 Description of the ARP packet fields

Field	Description
Hardware Type	Type of the hardware interface. Refer to Table 211 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: <ul style="list-style-type: none"> ■ 1: ARP request packets ■ 2: ARP reply packets ■ 3: RARP request packets ■ 4: RARP reply packets
Hardware address of the sender	Hardware address of the sender
IP address of the sender	IP address of the sender
Hardware address of the receiver	<ul style="list-style-type: none"> ■ For an ARP request packet, this field is null. ■ For an ARP reply packet, this field carries the hardware address of the receiver.
IP address of the receiver	IP address of the receiver

Table 211 Description of the values of the hardware type field

Value	Description
1	Ethernet
2	Experimental Ethernet
3	X.25
4	Proteon ProNET (Token Ring)
5	Chaos
6	IEEE802.X
7	ARC network

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. The Switch 4210 provides the **display arp** command to display the information about ARP mapping entries.

ARP entries in the Switch 4210 can either be static entries or dynamic entries, as described in Table 212.

Table 212 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 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.

ARP Configuration

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.*

Displaying and Debugging ARP

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

You can execute the **reset** command in user view to clear ARP entries.

Table 213 Display and debug ARP

Operation	Command	Remarks
Display specific ARP mapping table entries	display arp [static dynamic] <i>ip-address</i>]	Available in any view.
Display the ARP mapping entries related to a specified string in a specified way	display arp [dynamic static] [{ begin include exclude } <i>text</i>]	
Display the number of the ARP entries of a specified type	display arp count [[dynamic static] [[{ begin include exclude } <i>text</i>]] <i>ip-address</i>]	
Display the setting of the ARP aging timer	display arp timer aging	
Clear specific ARP entries	reset arp [dynamic static] interface <i>interface-type</i> <i>interface-number</i>]	Available in user view.

ARP Configuration Example

Network requirement

- 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 Ethernet1/0/10 of VLAN 1.

Configuration procedure

```
<4210> system-view
[4210] undo arp check enable
[4210] arp timer aging 10
[4210] arp static 192.168.1.1 00e0-fc01-0000 1 Ethernet1/0/10
```

24

DHCP OVERVIEW

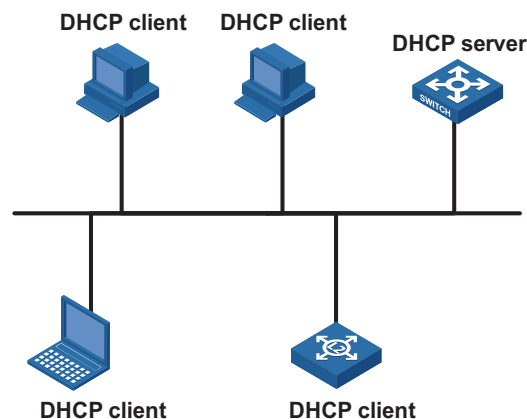
Introduction to DHCP

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 85.

Figure 85 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 “DHCP Packet Format” on page 283 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.



- *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 86 DHCP packet format

0	7	15	23	31
op (1)	htype (1)		hlen (1)	hops (1)
xid (4)				
secs (2)			flags (2)	
ciaddr (4)				
yiaddr (4)				
siaddr (4)				
giaddr (4)				
chaddr (16)				
sname (64)				
file (128)				
options (variable)				

The fields are described as follows:

- op: Operation types of DHCP packets, 1 for request packets and 2 for response packets.
- htype, hlen: Hardware address type and length of the DHCP client.
- hops: Number of DHCP relay agents which a DHCP packet passes. For each DHCP relay agent that the DHCP request packet passes, the field value increases by 1.
- xid: Random number that the client selects when it initiates a request. The number is used to identify an address-requesting process.
- secs: Elapsed time after the DHCP client initiates a DHCP request.
- flags: The first bit is the broadcast response flag bit, used to identify that the DHCP response packet is a unicast (set to 0) or broadcast (set to 1). Other bits are reserved.
- ciaddr: IP address of a DHCP client.
- yiaddr: IP address that the DHCP server assigns to a client.
- siaddr: IP address of the DHCP server.
- giaddr: IP address of the first DHCP relay agent that the DHCP client passes after it sent the request packet.
- chaddr: Hardware address of the DHCP client.

- sname: Name of the DHCP server.
- file: Path and name of the boot configuration file that the DHCP server specifies for the DHCP client.
- option: Optional variable-length fields, including packet type, valid lease time, IP address of a DNS server, and IP address of the WINS server.

Protocol Specification

Protocol specifications related to DHCP include:

- RFC2131: Dynamic Host Configuration Protocol
- RFC2132: DHCP Options and BOOTP Vendor Extensions
- RFC1542: Clarifications and Extensions for the Bootstrap Protocol
- RFC3046: DHCP Relay Agent Information option

25

DHCP SNOOPING CONFIGURATION

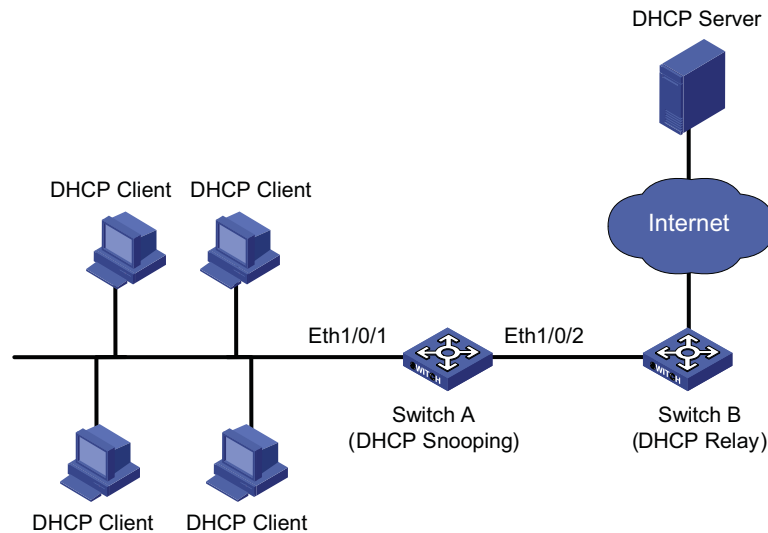
Introduction to DHCP Snooping

For the sake of security, the IP addresses used by online DHCP clients need to be tracked for the administrator to verify the corresponding relationship between the IP addresses the DHCP clients obtained from DHCP servers and the MAC addresses of the DHCP clients.

- Switches can track DHCP clients' IP addresses through the security function of the DHCP relay agent operating at the network layer.
- Switches can track DHCP clients' IP addresses through the DHCP snooping function at the data link layer.

Figure 87 illustrates a typical network diagram for DHCP snooping application, where Switch A is a Switch 4210.

Figure 87 Typical network diagram for DHCP snooping application



DHCP snooping listens the DHCP-REQUEST packets to retrieve the IP addresses the DHCP clients obtain from DHCP servers and the MAC addresses of the DHCP clients:

DHCP Snooping Configuration

Table 214 Configure DHCP snooping

Operation	Command	Description
Enter system view	system-view	-
Enable DHCP snooping	dhcp-snooping	Required By default, the DHCP snooping function is disabled.
Display the user IP-MAC address mapping entries recorded by the DHCP snooping function	display dhcp-snooping [unit unit-id]	You can execute the display command in any view

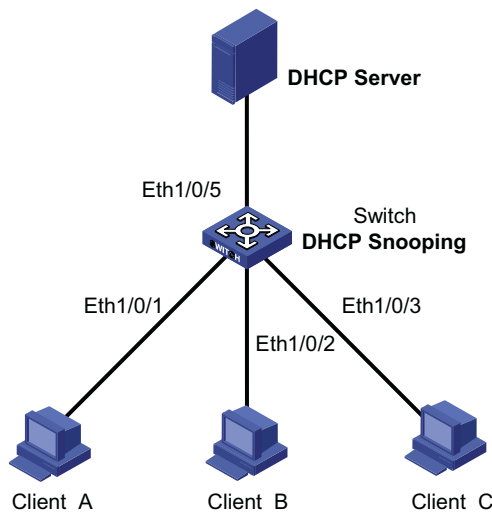


After DHCP snooping is enabled on an Ethernet switch, clients connected with this switch cannot obtain IP addresses dynamically through BOOTP.

DHCP Snooping Configuration Example

Network requirements As shown in Figure 88, Ethernet1/0/5 of the switch is connected to the DHCP server, and Ethernet1/0/1, Ethernet1/0/2, and Ethernet1/0/3 are respectively connected to Client A, Client B, and Client C. Enable DHCP snooping on the switch.

Network diagram **Figure 88** Network diagram for DHCP snooping configuration



Configuration procedure # Enable DHCP snooping on the switch.

```
<4210> system-view
[4210] dhcp-snooping
```

26

DHCP/BOOTP CLIENT CONFIGURATION

Introduction to DHCP Client

After you specify a VLAN interface as a DHCP client, the device can use DHCP to obtain parameters such as IP address dynamically from the DHCP server, which facilitates user configuration and management.

“Obtaining IP Addresses Dynamically” on page 282 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.



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

Table 215 Configure a DHCP/BOOTP client

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

Table 215 Configure a DHCP/BOOTP client

Operation	Command	Description
Configure the VLAN interface to obtain IP address through DHCP or BOOTP	ip address { bootp-alloc dhcp-alloc }	Required By default, no IP address is configured for the VLAN interface.



Currently, the Switch 4210 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.



To improve security and avoid malicious attack to the unused SOCKETS, the Switch 4210 provides 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:

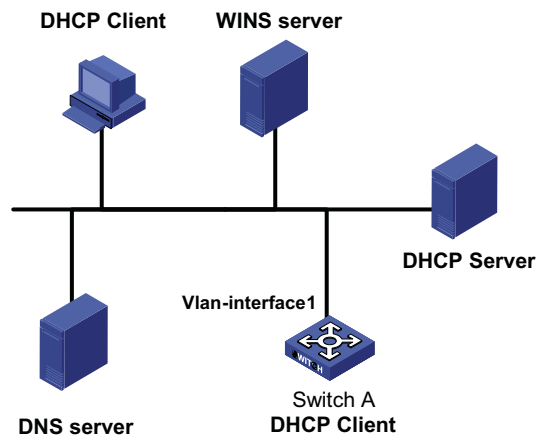
- Using the `ip address dhcp-alloc` command enables the DHCP client, and UDP port 68.
- Using the `undo ip address dhcp-alloc` command disables the DHCP client, and UDP port 68.

Displaying DHCP/BOOTP Client Configuration

Operation	Command	Description
Display related information on a DHCP client	display dhcp client [verbose]	Optional Available in any view
Display related information on a BOOTP client	display bootp client [interface Vlan-interface vlan-id]	

DHCP Client Configuration Example

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

Network diagram Figure 89 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.

```
<4210> system-view
[4210] interface Vlan-interface 1
[4210-Vlan-interface1] ip address dhcp-alloc
```

ACL Overview

The Switch 4210 supports software-based ACLs for the purpose of controlling management access into the Switch 4210 from Telnet and SNMP management stations. 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

Applying it 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.

ACLs are directly applied to hardware when they are used for:

- Implementing QoS
- Filtering the packets to be forwarded

Referencing it from 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



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 4210 Family

The Switch 4210 supports the following ACL types:

- Basic ACLs
- Advanced ACLs



ACLs defined on the Switch 4210 can be referenced by upper-layer software for packet filtering. They cannot be applied to hardware

ACL Configuration

Configuring a 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.



An absolute time range on the Switch 4210 Family can be within the range 1970/1/1 00:00 to 2100/12/31 24:00.

Configuration Procedure

Table 216 Configure a time range

Operation	Command	Description
Enter system view	system-view	-
Create a time range	time-range <i>time-name</i> { <i>start-time to end-time</i> <i>days-of-the-week</i> [from <i>start-time start-date</i>] [to <i>end-time end-date</i>] from <i>start-time start-date</i> [to <i>end-time end-date</i>] to <i>end-time end-date</i> }	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.

```
<4210> system-view
[4210] time-range test 8:00 to 18:00 working-day
[4210] 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.

```
<4210> system-view
[4210] time-range test from 15:00 1/28/2006 to 15:00 1/28/2008
[4210] display time-range test
Current time is 13:30:32 Apr/16/2005 Saturday
```

```
Time-range : test ( Inactive )
From 15:00 Jan/28/2006 to 15:00 Jan/28/2008
```

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 configuring the time , refer to “Configuring a Time Range” on page 293.
- The source IP addresses based on which the ACL filters packets are determined.

Configuration Procedure

Table 217 Define a basic ACL rule

Operation	Command	Description
Enter system view	system-view	-
Create an ACL and enter basic ACL view	acl number <i>acl-number</i> [match-order { auto config }]	Required config by default
Define an ACL rule	rule [<i>rule-id</i>] { deny permit } [<i>rule-string</i>]	Required For information about <i>rule-string</i> , refer to the ACL command in the Switch 4210 Command REference Guide.
Configure a description string to the ACL	description <i>text</i>	Optional Not configured by default

Note that:

- With the **config** match order specified for the basic ACL, you can modify any existent rule. The unmodified part of the rule remains. With the **auto** match order specified for the basic ACL, you cannot modify any existent rule; otherwise the system 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, it is the maximum rule number plus one.
- 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.

```
<4210> system-view
[4210] acl number 2000
[4210-acl-basic-2000] rule deny source 192.168.0.1 0
```

Display the configuration information of ACL 2000.

```
[4210-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, create the corresponding time ranges first, as described in the section entitled “Configuring a Time Range” on page 293.
- Determine the settings to be specified in the rule, such as source and destination IP addresses, the protocols carried by IP, and protocol-specific features.

Configuration Procedure

Table 218 Define an advanced ACL rule

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

Note that:

- With the **config** match order specified for the advanced ACL, you can modify any existent rule. The unmodified part of the rule remains. With the **auto** match order specified for the ACL, you cannot modify any existent rule; otherwise the system 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, it is the maximum rule number plus one.
- 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.

```
<4210> system-view
[4210] acl number 3000
[4210-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.

```
[4210-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 (0 times matched)
```

Displaying ACL Configuration

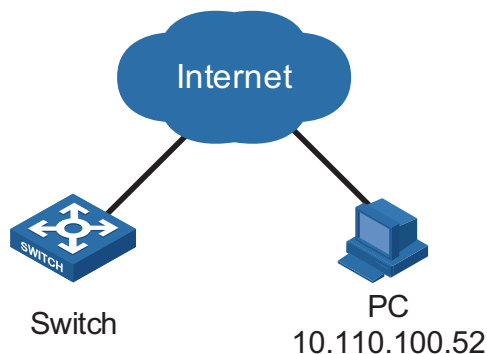
After the above configuration, you can execute the **display** commands in any view to view the ACL running information and verify the configuration.

Table 219 Display ACL configuration

Operation	Command	Description
Display a configured ACL or all the ACLs	display acl { all <i>acl-number</i> }	In any view.
Display a time range or all the time ranges	display time-range { all <i>time-name</i> }	

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 90** Network diagram for controlling Telnet login users by source IP

Configuration procedure

```
# Define ACL 2000.
```

```
<4210> system-view
[4210] acl number 2000
[4210-acl-basic-2000] rule 1 permit source 10.110.100.52 0
[4210-acl-basic-2000] quit
```

```
# Reference ACL 2000 on VTY user interface to control Telnet login users.
```

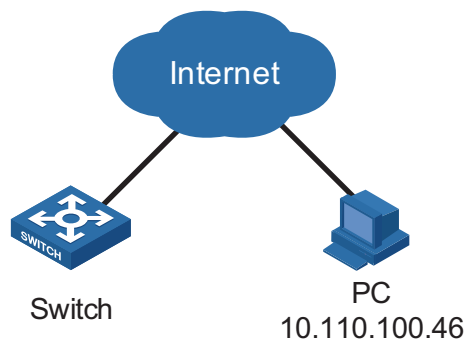
```
[4210] user-interface vty 0 4
[4210-ui-vty0-4] acl 2000 inbound
```

**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 91 Network diagram for controlling Web login users by source IP

**Configuration procedure**

```
# Define ACL 2001.
```

```
<4210> system-view
[4210] acl number 2001
[4210-acl-basic-2001] rule 1 permit source 10.110.100.46 0
[4210-acl-basic-2001] quit
```

```
# Reference ACL 2001 to control users logging in to the Web server.
```

```
[4210] ip http acl 2001
```

Overview**Introduction to QoS**

Quality of service (QoS) is a concept generally existing in occasions with service supply and demand. It evaluates the ability to meet the need of the customers in service. Generally, the evaluation is not to grade precisely. Its purpose is to analyze the conditions where the service is the best and the conditions where the service still needs improvement and then to make improvements in the specified aspects.

In an internet, QoS evaluates the ability of the network to deliver packets. The evaluation on QoS can be based on different aspects because the network provides various services. Generally speaking, QoS is the evaluation on the service ability to support the core requirements such as delay, jitter, and packet loss ratio in the packet delivery.

Traditional Packet Forwarding Service

In traditional IP networks, packets are treated equally. That is, the FIFO (first in first out) policy is adopted for packet processing. Network resources required for packet forwarding is determined by the order in which packets arrive. All the packets share the resources of the network. Network resources available to the packets completely depend on the time they arrive. This service policy is known as Best-effort, which delivers the packets to their destination with the best effort, with no assurance and guarantee for delivery delay, jitter, packet loss ratio, reliability, and so on.

The traditional Best-Effort service policy is only suitable for applications insensitive to bandwidth and delay, such as WWW, file transfer and E-mail.

New Applications and New Requirements

With the expansion of computer network, more and more networks become part of the Internet. The Internet gains rapid development in terms of scale, coverage and user quantities. More and more users use the Internet as a platform for their services and for data transmission.

Besides the traditional applications such as WWW, E-mail, and FTP, new services are developed on the Internet, such as tele-education, telemedicine, video telephone, videoconference and Video-on-Demand (VoD). Enterprise users expect to connect their regional branches together using VPN techniques for coping with daily business, for instance, accessing databases or manage remote equipments through Telnet.

All these new applications have one thing in common, that is, they have special requirements for bandwidth, delay, and jitter. For instance, bandwidth, delay, and jitter are critical for videoconference and VoD. As for other applications, such as transaction processing and Telnet, although bandwidth is not as critical, a too long

delay may cause unexpected results. That is, they need to get serviced in time even if congestion occurs.

Newly emerging applications demand higher service performance from IP networks. In addition to simply delivering packets to their destinations, better network services are demanded, such as allocating dedicated bandwidth, reducing packet loss ratio, avoiding congestion, regulating network traffic, and setting priority of the packets. To meet those requirements, the network should be provided with better service capability.

Major Traffic Control Techniques

Traffic identifying, traffic policing (TP), traffic shaping (TS), congestion management, and congestion avoidance are the foundations for a network to provide differentiated services. Mainly they implement the following functions.

- Traffic identifying identifies specific packets based on certain matching rules. It is a prerequisite for differentiated service.
- TP confines traffics to a specific specification. You can configure restriction or punishment measures against the traffics exceeding the specification to protect the benefits of carriers and to prevent network resources from being abused.
- TS actively adjusts the output rate of traffics. It can enable the traffics to match the capacity of the downstream network devices, so as to prevent packets from being dropped and network congestion.
- Congestion management handles resource competition during network congestion. Generally, it adds packets to queues first, and then forwards the packets by using a scheduling algorithm.
- Congestion avoidance monitors the use of network resources and drops packets actively when congestion reaches certain degree. It relieves network load by adjusting traffics.

Traffic identifying is the basis of all the above-mentioned traffic management technologies. It identifies packets using certain rules and makes differentiated services possible. TP, TS, congestion management, and congestion avoidance are methods for implementing network traffic control and network resource management. They are occurrences of differentiated services.

QoS Supported By Switch 4210 Family

Traffic Identifying

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

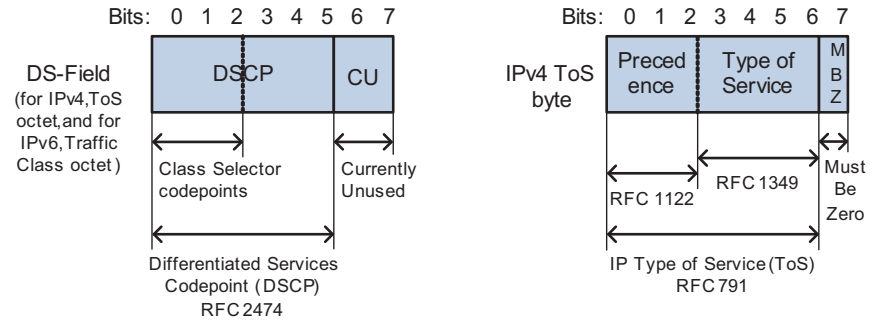
Traffic identifying means identifying packets that conform to certain characteristics according to certain rules. It is the foundation for providing differentiated services.

In traffic identifying, the priority bit in the type of service (ToS) field in IP packet header can be used to identify packets of different priorities. The network administrator can also define traffic identifying policies to identify packets by the combination of source address, destination address, MAC address, IP protocol or the port number of an application. Normally, traffic identifying is done by checking the information carried in packet header. Packet payload is rarely adopted for traffic identifying. The identifying rule is unlimited in range. It can be a quintuplet

consisting of source address, source port number, protocol number, destination address, and destination port number. It can also be simply a network segment.

Precedence IP precedence, ToS precedence, and DSCP precedence

Figure 92 DS field and ToS byte



The ToS field in an IP header contains eight bits numbered 0 through 7, among which,

- The first three bits indicate IP precedence in the range 0 to 7.
- Bit 3 to bit 6 indicate ToS precedence in the range of 0 to 15.
- In RFC2474, the ToS field in IP packet header is also known as DS field. The first six bits (bit 0 through bit 5) of the DS field indicate differentiated service codepoint (DSCP) in the range of 0 to 63, and the last two bits (bit 6 and bit 7) are reserved.

Table 220 Description of IP Precedence

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

In a network providing differentiated services, traffics are grouped into the following four classes, and packets are processed according to their DSCP values.

- Expedited Forwarding (EF) class: In this class, packets can be forwarded regardless of link share of other traffic. The class is suitable for preferential services with low delay, low packet loss ratio, low jitter, and assured bandwidth (such as virtual leased line);
- Assured forwarding (AF) class: This class is further divided into four subclasses (AF1/2/3/4) and a subclass is further divided into three drop priorities, so the AF service level can be segmented. The QoS rank of the AF class is lower than that of the EF class;

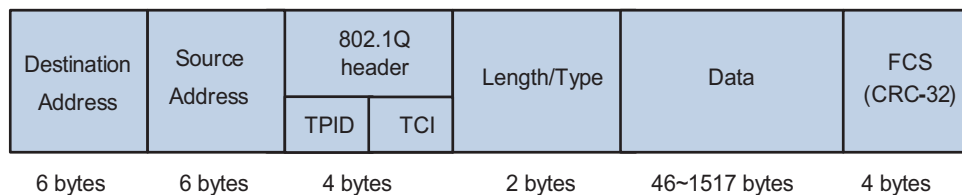
- Class selector (CS) class: This class comes from the IP ToS field and includes eight subclasses;
- Best Effort (BE) class: This class is a special class without any assurance in the CS class. The AF class can be degraded to the BE class if it exceeds the limit. Current IP network traffic belongs to this class by default.

Table 221 Description of DSCP precedence values

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

802.1p priority

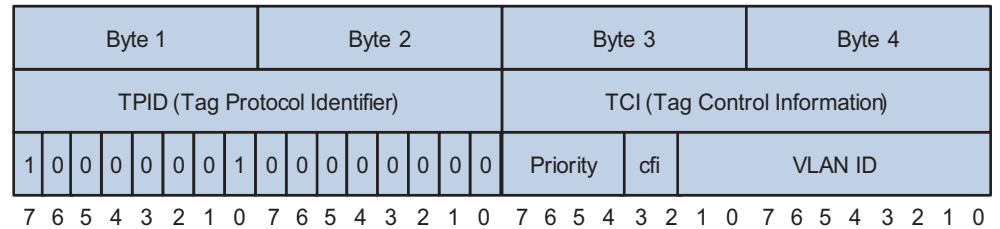
802.1p priority lies in Layer 2 packet headers and is applicable to occasions where the Layer 3 packet header does not need analysis but QoS must be assured at Layer 2.

Figure 93 An Ethernet frame with an 802.1Q tag header

As shown in the figure above, each host supporting 802.1Q protocol adds a 4-byte 802.1Q tag header after the source address of the former Ethernet frame header when sending packets.

The 4-byte 802.1Q tag header consists of the tag protocol identifier (TPID, two bytes in length), whose value is 0x8100, and the tag control information (TCI, two bytes in length). Figure 94 describes the detailed contents of an 802.1Q tag header.

Figure 94 802.1Q tag headers



In the figure above, the priority field (three bits in length) in TCI is 802.1p priority (also known as CoS precedence), which ranges from 0 to 7.

Table 222 Description of 802.1p priority

802.1p priority (decimal)	802.1p priority (binary)	Description
0	000	best-effort
1	001	background
2	010	spare
3	011	excellent-effort
4	100	controlled-load
5	101	video
6	110	voice
7	111	network-management

The precedence is called 802.1p priority because the related applications of this precedence are defined in detail in the 802.1p specifications.

Priority Trust Mode

After a packet enters a switch, the switch sets the 802.1p priority and local precedence for the packet according to its own capability and the corresponding rules. The local precedence is locally significant precedence that the switch assigns to the packet. It corresponds to an output queue. Packets with higher local precedence values take precedence over those with lower precedence values and will be processed preferentially.

By default, a Switch 4210 processes a received packet as follows:

- For a packet without an 802.1q tag header, the switch uses the priority of the receiving port as the 802.1p precedence of the packet and looks up it in the 802.1p-precedence-to-local-precedence mapping table for the local precedence, and then assigns the local precedence to the packet for it to be added to a output queue.
- For a packet with an 802.1q tag header, the switch replaces the 802.1p precedence of the packet with the priority of the receiving port and looks up the latter in the 802.1p-precedence-to-local-precedence mapping table for the local precedence, and then assigns the local precedence to the packet for it to be added to an output queue.

You can also configure to trust packet priority. In this case, a received packet is processed in one of the following three ways:

- With the 802.1p precedence of a packet trusted, the switch obtains the corresponding local precedence by looking up the 802.1p precedence of the packet in the 802.1p-precedence-to-local-precedence mapping table and assigns the local precedence to the packet.
- With the DSCP precedence trusted, the switch obtains the corresponding local precedence by looking up the DSCP precedence of the packet in the DSCP-precedence-to-local-precedence mapping table and assigns the local precedence to the packet.
- With the IP precedence trusted, the switch obtains the corresponding local precedence by looking up the IP precedence of the packet in the IP-precedence-to-local-precedence mapping table and assigns the local precedence to the packet.

The Switch 4210 provide COS-precedence-to-local-precedence, DSCP-precedence-to-local-precedence and IP-precedence-to-local-precedence mapping tables for priority mapping. Table 1-4 through Table 1-6 list the default settings of these tables.

Table 223 COS-precedence-to-local-precedence mapping table

COS	Local precedence
0	1
1	0
2	0
3	1
4	2
5	2
6	3
7	3

Table 224 DSCP-precedence-to-local-precedence mapping table

DSCP	Local precedence
0 to 15	0
16 to 31	1
32 to 47	2
48 to 63	3

Table 225 IP-precedence-to-local-precedence mapping table

IP precedence	Local precedence
0	1
1	0

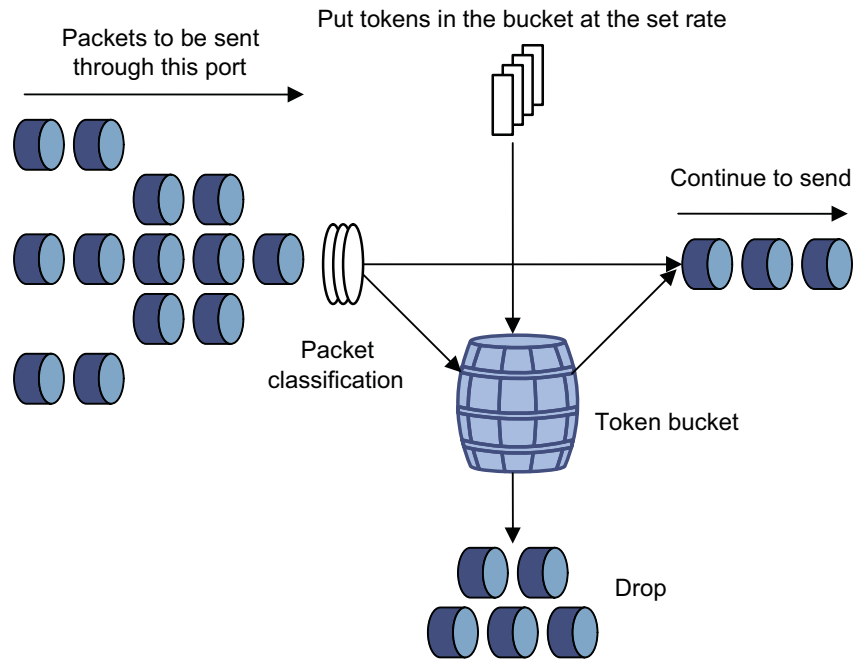
Table 225 IP-precedence-to-local-precedence mapping table

IP precedence	Local precedence
2	0
3	1
4	2
5	2
6	3
7	3

Port Rate Limiting Port rate limiting refers to limiting the total rate of inbound or outbound packets on a port.

Port rate limiting can be implemented through token buckets. The token bucket can be considered as a container with a certain capacity to hold tokens. The system puts tokens into the bucket at the set rate. When the token bucket is full, the extra tokens will overflow and the number of tokens in the bucket stops increasing.

Figure 95 Diagram for LR



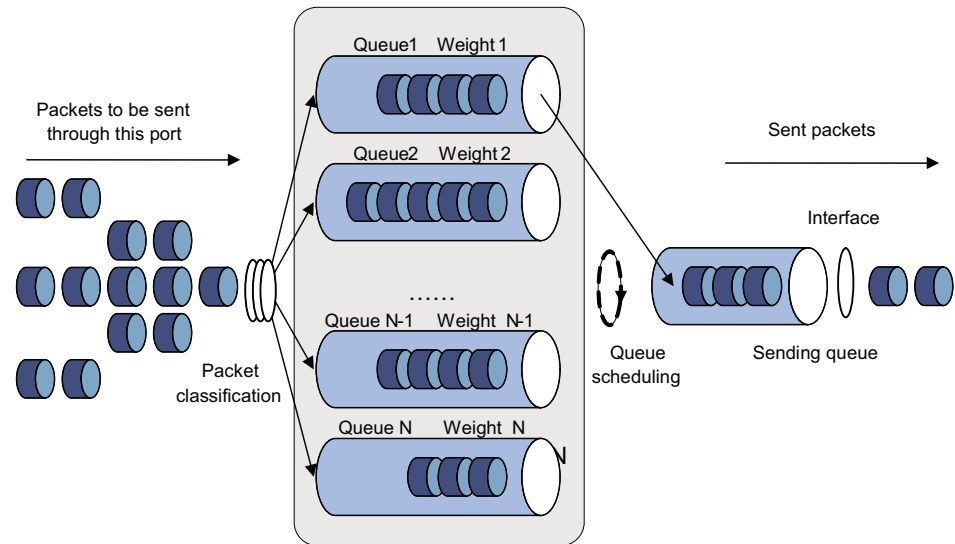
If you perform port rate limiting configuration for a port, the token bucket determines the way to process the packets to be sent by this port or packets reaching the port. Packets can be sent or received if there are enough tokens in the token bucket; otherwise, they will be dropped.

Queue Scheduling When the network is congested, the problem that many packets compete for resources must be solved, usually through queue scheduling.

In the following section, weighted round robin (WRR), and HQ-WRR (High Queue-WRR) queues are introduced.

WRR queuing

Figure 96 Diagram for WRR queuing



WRR queue-scheduling algorithm schedules all the queues in turn and every queue can be assured of a certain service time. Assume there are eight priority queues on a port. WRR configures a weight value for each queue, which is w_7 , w_6 , w_5 , w_4 , w_3 , w_2 , w_1 , and w_0 . The weight value indicates the proportion of obtaining resources. On a 100 M port, configure the weight value of WRR queue-scheduling algorithm to 50, 50, 30, 30, 10, 10, 10, and 10 (corresponding to w_7 , w_6 , w_5 , w_4 , w_3 , w_2 , w_1 , and w_0 in order). In this way, the queue with the lowest priority can get 5 Mbps bandwidth at least. Another advantage of WRR queue is that: though the queues are scheduled in order, the service time for each queue is not fixed; that is to say, if a queue is empty, the next queue will be scheduled. In this way, the bandwidth resources are made full use.

HQ-WRR queuing

HQ-WRR is an improvement over WRR. With queue 3 allocated with the highest priority, the switch will ensure that this queue get served first and will perform round-robin scheduling to the other three queues when the traffic has exceeded the bandwidth capacity of a port.

Burst The Burst function can provide better packet cache function and traffic forwarding performance. It is suitable for networks where

- Large amount of broadcast/multicast packets and large burst traffic exist.
- Packets of high-rate links are forwarded to low-rate links or packets of multiple links with the equal rates are forwarded to a single link that is of the same rate as that of the incoming links.

Although the burst function helps reduce the packet loss ratio and improve packet processing capability in the networks mentioned above, it may affect QoS performance. So, use this function with caution.

QoS Configuration

Table 226 QoS configuration tasks

Task	Remarks
Configuring Port Priority	Optional
Configuring to Trust the 802.1p Precedence of the Received Packets	Optional
Configuring Priority Trust Mode	Optional
Configuring Priority Mapping	Optional
Configuring Port Rate Limiting	Optional
Configuring Queue Scheduling	Optional
Enabling the Burst Function	Optional
Displaying QoS	Optional

Configuring Port Priority

By default, for a packet with an 802.1q tag header, a switch replaces the 802.1p precedence of a packet with the priority of the receiving port and looks up the new 802.1p precedence in the 802.1p-precedence-to-local-precedence mapping table for the corresponding local precedence, and then assigns the local precedence to the packet for it to be added an output queue.

Configuration prerequisites

- The port whose port priority is to be configured is determined.
- The target priority value is determined.

Configuration procedure

Table 227 Configure port priority

Operation	Command	Description
Enter system view	system-view	
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	
Configure port priority	priority <i>priority-level</i>	Optional 0 by default

Configuration example

- Configure port priority on Ethernet 1/0/1 and set the priority of Ethernet 1/0/1 to 7.

```
<4210> system-view
[4210] interface Ethernet1/0/1
[4210-Ethernet1/0/1] priority 7
```

Configuring to Trust the 802.1p Precedence of the Received Packets

You can configure the switch to trust the 802.1p precedence of the received packets. In this case, the priority of the receiving port is not used as the 802.1p precedence of the received packet.

Configuration prerequisites

To trust the 802.1p precedence of the received packets is determined.

Configuration procedure

Table 228 Configure to trust the 802.1p precedence of the received packets

Operation	Command	Description
Enter system view	system-view	-
Configure to trust the 802.1p precedence of the received packets	priority trust	Required By default, for a packet with an 802.1q tag header, the priority of the receiving port is used as the 802.1p precedence of the received packets.

Configuration example

Configure the switch to trust the 802.1p precedence of the received packets.

```
<4210> system-view
[4210] priority trust
```

Configuring Priority Trust Mode

Refer to section 1.2.3 "Priority Trust Mode" for introduction to priority trust mode.

Configuration prerequisites

The priority trust mode to be adopted is determined.

Configuration procedure

Table 229 Configure the priority trust mode

Operation	Command	Description
Enter system view	system-view	-
Configure the priority trust mode	priority-trust { cos dscp ip-precedence }	Required By default, the switch trusts the 802.1p precedence of the received packets. In this case, the switch obtains the local precedence by looking up the 802.1p precedence in the 802.1p-precedence-to-local-precedence mapping table and then assigns the local precedence to the packet.

Configuration example

Configure the switch to trust the DSCP precedence of the received packets.

```
<4210> system-view
[4210] priority-trust dscp
```

Configuring Priority Mapping

You can modify the COS-precedence-to-local-precedence, DSCP-precedence-to-local-precedence and IP-precedence-to-local-precedence mapping tables as required to mark packets with different priorities.

Configuration prerequisites

The target COS-precedence-to-local-precedence, DSCP-precedence-to-local-precedence and IP-precedence-to-local-precedence mapping tables are determined.

Configuration procedure

Table 230 Configure COS-precedence-to-local-precedence mapping table

Operation	Command	Description
Enter system view	<code>system-view</code>	-
Configure COS-precedence-to-local-precedence mapping table	qos cos-local-precedence-map <code>cos0-map-local-prec</code> <code>cos1-map-local-prec</code> <code>cos2-map-local-prec</code> <code>cos3-map-local-prec</code> <code>cos4-map-local-prec</code> <code>cos5-map-local-prec</code> <code>cos6-map-local-prec</code> <code>cos7-map-local-prec</code>	Required

Table 231 Configure DSCP-precedence-to-local-precedence mapping table

Operation	Command	Description
Enter system view	system-view	-
Configure DSCP-precedence-to-local-precedence mapping table	qos dscp-local-precedence-map <code>dscp-list : local-precedence</code>	Required

Table 232 Configure IP-precedence-to-local-precedence mapping table

Operation	Command	Description
Enter system view	system-view	-
Configure IP-precedence-to-local-precedence mapping table	qos ip-precedence-local-precedence-map <code>ip0-map-local-prec ip1-map-local-prec</code> <code>ip2-map-local-prec ip3-map-local-prec</code> <code>ip4-map-local-prec ip5-map-local-prec</code> <code>ip6-map-local-prec ip7-map-local-prec</code>	Required

Configuration example

- Configure the COS-precedence-to-local-precedence mapping relationship as follows: 0 to 0, 1 to 0, 2 to 1, 3 to 1, 4 to 2, 5 to 2, 6 to 3, and 7 to 3.
- Display the configuration.

```
<4210> system-view
[4210] qos cos-local-precedence-map 0 0 1 1 2 2 3 3
[4210] display qos cos-local-precedence-map
cos-local-precedence-map:
```

cos (802.1p) :	0	1	2	3	4	5	6	7

local precedence (queue) :	0	0	1	1	2	2	3	3

Configuring Port Rate Limiting

Refer to “Port Rate Limiting” on page 305 for information about port rate limiting.

Configuration prerequisites

- The port on which port rate limiting configuration is to be performed is determined.
- The target rate and the direction of rate limiting (inbound or outbound) are determined.

Configuration procedure

Table 233 Configure port rate limiting

Operation	Command	Description
Enter system view	system-view	-
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	-
Configure port rate limiting	line-rate { inbound outbound } <i>target-rate</i>	Required By default, port rate limiting is disabled.

Configuration example

- Configure port rate limiting for inbound packets on Ethernet 1/0/1.
- The rate limit is 1,024 Kbps

Configuration procedure:

```
<4210> system-view
[4210] interface Ethernet1/0/1
[4210-Ethernet1/0/1] line-rate inbound 1024
```

Configuring Queue Scheduling

Refer to “Queue Scheduling” on page 305 for information about queue scheduling.

Configuration prerequisites

The algorithm for queue scheduling to be used and the related parameters are determined.

Configuration procedure

Table 234 Configure queue scheduling

Operation	Command	Description
Enter system view	<code>system-view</code>	-
Configure queue scheduling	<code>queue-scheduler { hq-wrr <i>queue0-weight queue1-weight queue2-weight</i> wrr <i>queue0-weight queue1-weight queue2-weight queue3-weight</i> }</code>	Required By default, all the ports adopt the WRR queue scheduling algorithm, with the weight for queue 0, queue 1, queue 2, and queue 3 as 1, 2, 3, and 4.

Configuration example

Adopt the WRR queue scheduling algorithm, with the weight for queue 0, queue 1, queue 2, and queue 3 as 12, 8, 4, and 1.

Display the configuration information after configuration.

Configuration procedure:

```
<4210> system-view
[4210] queue-scheduler wrr 12 8 4 1
[4210] display queue-scheduler
Queue scheduling mode: weighted round robin
weight of queue 0: 12
weight of queue 1: 8
weight of queue 2: 4
weight of queue 3: 1
```

Enabling the Burst Function

Refer to "Burst" on page 306 for information about the burst function.

Configuration prerequisites

The burst function is required.

Configuration procedure

Table 235 Enable the burst function

Operation	Command	Description
Enter system view	<code>system-view</code>	-
Enable the burst function	<code>burst-mode enable</code>	Required By default, the burst function is disabled.

Configuration example

- Enable the burst function

```
<4210> system-view
[4210] burst-mode enable
```

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

Table 236 Display QoS

Operation	Command	Description
Display the COS-precedence-to-local-precedence mapping relationship	display qos cos-local-precedence-map	Available in any view
Display the DSCP-precedence-to-local-precedence mapping relationship	display qos dscp-local-precedence-map	Available in any view
Display the IP-precedence-to-local-precedence mapping relationship	display qos ip-precedence-local-precedence-map	Available in any view
Display queue scheduling algorithm and related parameters	display queue-scheduler	Available in any view
Display the 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 rate limiting configuration of a port or all the ports	display qos-interface { interface-type interface-number unit-id } line-rate	Available in any view

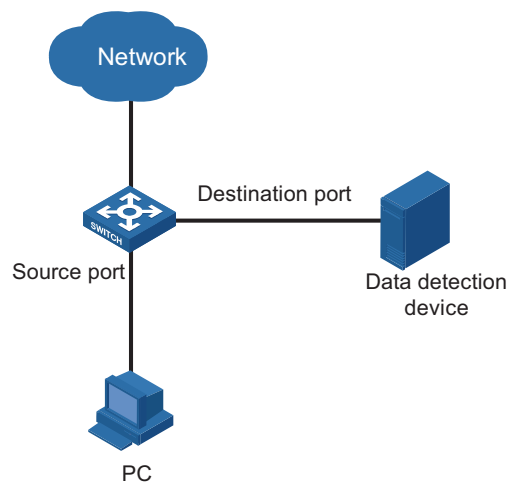
29

MIRRORING CONFIGURATION

Mirroring Overview

Mirroring refers to the process of copying packets of one or more ports (source ports) to a destination port which is connected to a data detection device. Users can then use the data detection device to analyze the mirrored packets on the destination port for monitoring and troubleshooting the network.

Figure 97 Implementing Port Mirroring



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.

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 237 Configuring local port mirroring

Operation	Command	Description
Enter system view	system-view	-
Create a port mirroring group	mirroring-group <i>group-id</i> local	Required

Table 237 Configuring local port mirroring

Operation		Command	Description
Configure the source port for the port mirroring group	In system view	mirroring-group <i>group-id</i> mirroring-port <i>mirroring-port-list</i> { both inbound outbound }	Use either approach You can configure multiple source ports at a time in system view, or you can configure the source port in specific port view. The configurations in the two views have the same effect.
	In port view	interface <i>interface-type</i> <i>interface-number</i> mirroring-group <i>group-id</i> mirroring-port { both inbound outbound } quit	
Configure the destination port for the port mirroring group	In system view	mirroring-group <i>group-id</i> monitor-port <i>monitor-port-id</i>	Use either approach The configurations in the two views have the same effect.
	In port view	interface <i>interface-type</i> <i>interface-number</i> mirroring-group <i>group-id</i> monitor-port	

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 destination port cannot be a member port of an aggregation group or a port enabled with LACP or STP.

Displaying Port Mirroring

After performing the configurations above, you can execute the **display** commands in any view to view the mirroring running information, so as to verify your configurations.

Table 238 Display configuration of mirroring

Operation	Command	Description
Display port mirroring configuration	display mirroring-group { <i>group-id</i> all local }	Available in any view

Mirroring Configuration Example

Network requirements

The departments of a company connect to each other through the Switch 4210:

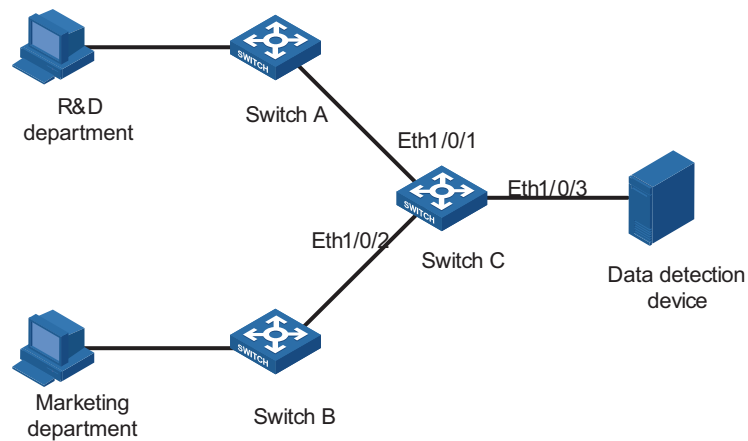
- Research and Development (R&D) department is connected to Switch C through Ethernet 1/0/1.
- Marketing department is connected to Switch C through Ethernet 1/0/2.
- Data detection device is connected to Switch C through Ethernet 1/0/3

The administrator wants to monitor the packets received on and sent from the R&D department and the marketing department through the data detection device.

Use the local port mirroring function to meet the requirement. Perform the following configurations on Switch C.

- Configure Ethernet 1/0/1 and Ethernet 1/0/2 as mirroring source ports.
- Configure Ethernet 1/0/3 as the mirroring destination port.

Network diagram Figure 98 Network diagram for local port mirroring



Configuration procedure Configure Switch C:

Create a local mirroring group.

```
<4210> system-view
[4210] mirroring-group 1 local
```

Configure the source ports and destination port for the local mirroring group.

```
[4210] mirroring-group 1 mirroring-port Ethernet 1/0/1 Ethernet 1/0/2 both
[4210] mirroring-group 1 monitor-port Ethernet 1/0/3
```

Display configuration information about local mirroring group 1.

```
[4210] display mirroring-group 1
mirroring-group 1:
  type: local
  status: active
  mirroring port:
    Ethernet1/0/1 both
    Ethernet1/0/2 both
  monitor port: Ethernet1/0/3
```

After the configurations, you can monitor all packets received on and sent from the R&D department and the marketing department on the data detection device.

Cluster Overview

Introduction to Switch Clustering

A cluster contains a group of switches. Through cluster management, you can manage multiple geographically dispersed in a centralized way.

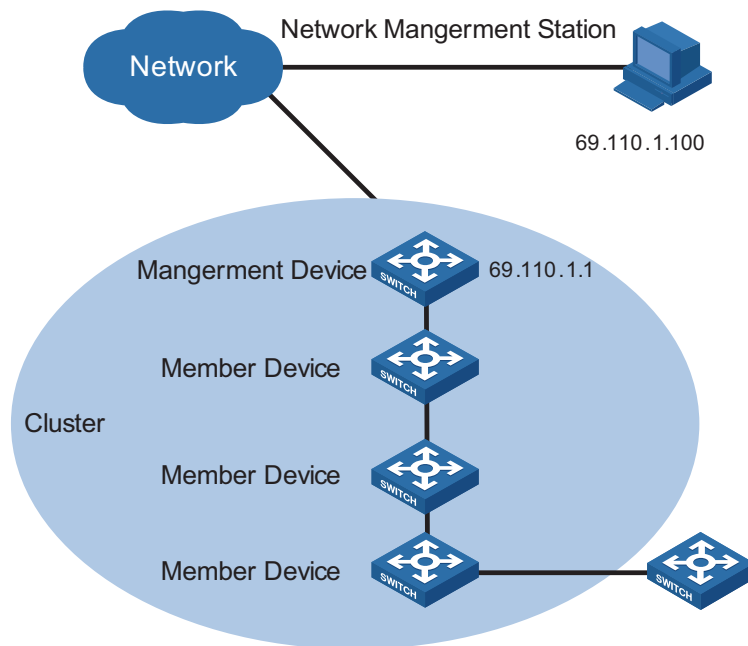
Cluster management is implemented through 3Com group management protocol (Switch Clustering). Switch Clustering version 2 (Switch Clusteringv2) is used at present.

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 99 illustrates a cluster implementation.

Figure 99 A cluster implementation

Switch Clustering 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

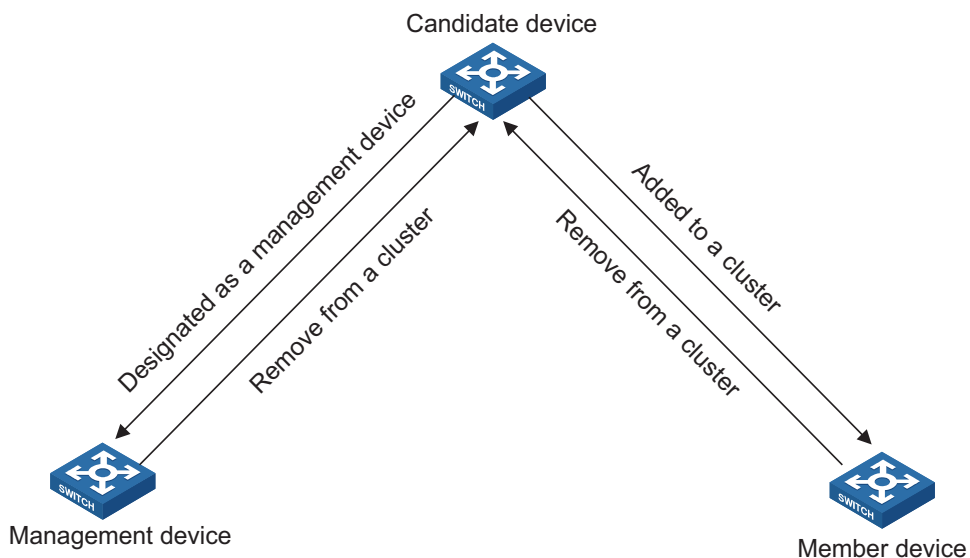
The switches in a cluster play different roles according to their functions and status. You can specify the role a switch plays. A switch in a cluster can also switch to other roles under specific conditions.

As mentioned above, the three cluster roles are management device, member device, and candidate device.

Table 239 Description of cluster roles

Role	Configuration	Function
Management device	Configured with a external IP address	<ul style="list-style-type: none"> ■ Provides an interface for managing all the switches in a cluster ■ Manages member devices through command redirection, that is, it forwards the commands intended for specific member devices. ■ Discovers neighbors, collects the information about network topology, manages and maintains the cluster. Management device also supports FTP server and SNMP host proxy. ■ Processes the commands issued by users through the public network
Member device	Normally, a member device is not assigned an external IP address	<ul style="list-style-type: none"> ■ Members of a cluster ■ Discovers the information about its neighbors, processes the commands forwarded by the management device, and reports log. The member devices of a 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 100 illustrates the state machine of cluster role.

Figure 100 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.



After you create a cluster on a Switch 4210, 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

Switch Clusteringv2 consists of the following three protocols:

- Neighbor discovery protocol (NDP)
- Neighbor topology discovery protocol (NTDP)
- Cluster

A cluster configures and manages the devices in it through the above three protocols.

Cluster management involves topology information collection and the establishment/maintenance of a cluster. Topology information collection and cluster establishment/maintenance are independent from each other. The former, as described below, starts before a cluster is established.

- All devices use NDP to collect the information about their neighbors, including software version, host name, MAC address, and port name.
- The management device uses NTDP to collect the information about the devices within specific hops and the topology information about the devices. It also determines the candidate devices according to the information collected.
- The management device adds the candidate devices to the cluster or removes member devices from the cluster according to the candidate device information collected through NTDP.

Introduction to NDP

NDP is a protocol used to discover adjacent devices and provide information about them. NDP operates on the data link layer, and therefore it supports different network layer protocols.

NDP is able to discover directly connected neighbors and provide the following neighbor information: device type, software/hardware version, and connecting port. In addition, it may provide the following neighbor information: device ID, port full/half duplex mode, product version, the Boot ROM version and so on.

- An NDP-enabled device maintains an NDP neighbor table. Each entry in the NDP table can automatically age out. You can also clear the current NDP information manually to have neighbor information collected again.
- An NDP-enabled device regularly broadcasts NDP packet through all its active ports. An NDP packet carries a holdtime field, which indicates how long the receiving devices will keep the NDP packet data. The receiving devices store the information carried in the NDP packet into the NDP table but do not forward the NDP packet. When they receive another NDP packet, if the information carried in the packet is different from the stored one, the corresponding entry in the NDP table is updated, otherwise only the holdtime of the entry is updated.

Introduction to NTDP

NTDP is a protocol used to collect network topology information. NTDP provides information required for cluster management: it collects topology information about the switches within the specified hop count, so as to provide the information of which devices can be added to a cluster.

Based on the neighbor information stored in the neighbor table maintained by NDP, NTDP on the management device advertises NTDP topology collection requests to collect the NDP information of each device in a specific network range as well as the connection information of all its neighbors. The information collected will be used by the management device or the network management software to implement required functions.

When a member device detects a change on its neighbors through its NDP table, it informs the management device through handshake packets, and the management device triggers its NTDP to perform specific topology collection, so that its NTDP can discover topology changes timely.

The management device collects the topology information periodically. You can also launch an operation of topology information collection by executing related commands. The process of topology information collection is as follows.

- The management device sends NTDP topology collection requests periodically through its NTDP-enabled ports.
- Upon receiving an NTDP topology collection request, the device returns a NTDP topology collection response to the management device and forwards the request to its neighbor devices through its NTDP-enabled ports. The topology collection response packet contains the information about the local device and the NDP information about all the neighbor devices.
- The neighbor devices perform the same operation until the NTDP topology collection request is propagated to all the devices within the specified hops.

When an NTDP topology collection request is propagated in the network, it is received and forwarded by large numbers of network devices, which may cause network congestion and the management device busy processing of the NTDP topology collection responses. To avoid such cases, the following methods can be used to control the NTDP topology collection request advertisement speed.

- Configuring the devices not to forward the NTDP topology collection request immediately after they receive an NTDP topology collection request. That is, configure the devices to wait for a period before they forward the NTDP topology collection request.
- Configuring each NTDP-enabled port on a device to forward an NTDP topology collection request after a specific period since the previous port on the device forwards the NTDP topology collection request.



- *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.



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

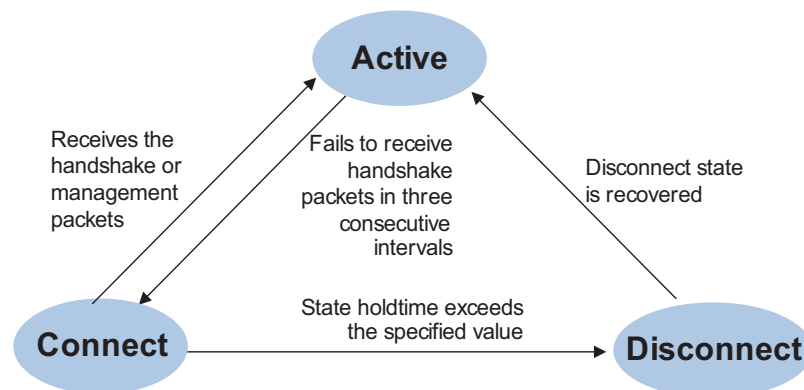
To create a cluster, you need to determine the device to operate as the management device first. The management device discovers and determines candidate devices through NDP and NTDP, and adds them to the cluster. You can also add candidate devices to a cluster manually.

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 101 illustrates the state machine of the connection between the management device and a member device.

Figure 101 State machine of the connection between the management device and a member device



- After a cluster is created and a candidate device is added to the cluster as a member device, both the management device and the member device store the state information of the member device and mark the member device as Active.
- The management device and the member devices exchange handshake packets periodically. Note that the handshake packets exchanged keep the states of the member devices to be Active and are not responded.
- If the management device does not receive a handshake packet from a member device after a period three times of the interval to send handshake packets, it changes the state of the member device from Active to Connect. Likewise, if a member device fails to receive a handshake packet from the management device after a period three times of the interval to send handshake packets, the state of the member device will also be changed from Active to Connect.
- If the management device receives a handshake packet or management packet from a member device that is in Connect state within the information holdtime, it changes the state of the member device to Active; otherwise, it changes the state of the member device (in Connect state) to Disconnect, in

which case the management device considers the member device disconnected. Likewise, if this member device, which is in Connect state, receives a handshake packet or management packet from the management device within the information holdtime, it changes its state to Active; otherwise, it changes its state to Disconnect.

- If the connection between the management device and a member device in Disconnect state is recovered, the member device will be added to the cluster again. After that, the state of the member device will turn to Active both locally and on the management device.

Besides, handshake packets are also used by member devices to inform the management device of topology changes.

Additionally, on the management device, you can configure the FTP server, TFTP server, logging host and SNMP host to be shared by the whole cluster. When a member device in the cluster communicates with an external server, the member device first transmits data to the management device, which then forwards the data to the external server. The management device serves as the default shared FTP server when no shared FTP 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.



- *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.*

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 240 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

Configuring the Management Device

Management device configuration tasks

Table 241 Management device configuration tasks

Operation	Description	Related section
Enable NDP globally and on specific ports	Required	"Enabling NDP globally and on specific ports"
Configure NDP-related parameters	Optional	"Configuring NDP-related parameters"
Enable NTDP globally and on a specific port	Required	"Enabling NTDP globally and on a specific port"
Configure NTDP-related parameters	Optional	"Configuring NTDP-related parameters"
Enable the cluster function	Required	"Enabling the cluster function"
Configure cluster parameters	Required	"Configuring cluster parameters"



To reduce the risk of being attacked by malicious users against opened socket and enhance switch security, the Switch 4210 provides 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 242 Enable NDP globally and on specific ports

Operation	Command	Description
Enter system view	system-view	-

Table 242 Enable NDP globally and on specific ports

Operation	Command	Description
Enable NDP globally	ndp enable	Required By default, NDP is enabled globally.
Enable NDP on specified Ethernet ports	In system view ndp enable interface <i>port-list</i> In Ethernet port view Enter Ethernet port view interface <i>interface-type</i> <i>interface-number</i> Enable NDP on the port ndp enable	Use either approach. By default, NDP is enabled on a port.

Configuring NDP-related parameters

Table 243 Configure NDP-related parameters

Operation	Command	Description
Enter system view	system-view	-
Configure the holdtime of NDP information	ndp timer aging <i>aging-in-seconds</i>	Optional By default, the holdtime of NDP information is 180 seconds.
Configure the interval to send NDP packets	ndp timer hello <i>seconds</i>	Optional By default, the interval to send NDP packets is 60 seconds.

Enabling NTDP globally and on a specific port

Table 244 Enable NTDP globally and on a specific port

Operation	Command	Description
Enter system view	system-view	-
Enable NTDP globally	ntdp enable	Required Enabled by default
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	-
Enable NTDP on the Ethernet port	ntdp enable	Required Enabled by default

Configuring NTDP-related parameters

Table 245 Configure NTDP-related parameters

Operation	Command	Description
Enter system view	system-view	-
Configure the range to collect topology information	ntdp hop <i>hop-value</i>	Optional By default, the system collects topology information from the devices within three hops.

Table 245 Configure NTDP-related parameters

Operation	Command	Description
Configure the device forward delay of topology collection requests	ntdp timer hop-delay <i>time</i>	Optional By default, the device forward delay is 200 ms.
Configure the port forward delay of topology collection requests	ntdp timer port-delay <i>time</i>	Optional By default, the port forward delay is 20 ms.
Configure the interval to collect topology information periodically	ntdp timer <i>interval-in-minutes</i>	Optional By default, the topology collection interval is one minute.
Quit system view	quit	-
Launch topology information collection manually	ntdp explore	Optional

Enabling the cluster function

Table 246 Enable the cluster function

Operation	Command	Description
Enter system view	system-view	-
Enable the cluster function globally	cluster enable	Required By default, the cluster function is enabled.

Configuring cluster parameters

The establishment of a cluster and the related configuration can be accomplished in manual mode or automatic mode, as described below.

1 Establishing a cluster and configuring cluster parameters in manual mode

Table 247 Establish a cluster and configure cluster parameters in manual mode

Operation	Command	Description
Enter system view	system-view	-
Specify the management VLAN	management-vlan <i>vlan-id</i>	Required By default, VLAN 1 is used as the management VLAN.
Enter cluster view	cluster	-
Configure a IP address pool for the cluster	ip-pool <i>administrator-ip-address</i> { <i>ip-mask</i> <i>ip-mask-length</i> }	Required
Build a cluster	build <i>name</i>	Required <i>name</i> : cluster name.
Configure a multicast MAC address for the cluster	cluster-mac <i>H-H-H</i>	Required By default, the cluster multicast MAC address is 0180-C200-000A.
Set the interval for the management device to send multicast packets	cluster-mac syn-interval <i>time-interval</i>	Optional By default, the interval to send multicast packets is one minutes.

Table 247 Establish a cluster and configure cluster parameters in manual mode

Operation	Command	Description
Set the holdtime of member switches	holdtime <i>seconds</i>	Optional By default, the holdtime is 60 seconds.
Set the interval to send handshake packets	timer <i>interval</i>	Optional By default, the interval to send handshake packets is 10 seconds.

2 Establish a cluster in automatic mode

Table 248 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 <i>administrator-ip-address</i> { <i>ip-mask</i> <i>ip-mask-length</i> }	Required
Start automatic cluster establishment	auto-build [recover]	Required Follow prompts to establish a cluster.



- 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 Member Devices

Member device configuration tasks

Table 249 Member device configuration tasks

Operation	Description	Related section
Enable NDP globally and on specific ports	Required	"Enabling NDP globally and on specific ports"
Enable NTDP globally and on a specific port	Required	"Enabling NTDP globally and on a specific port"
Enable the cluster function	Required	"Enabling the cluster function"
Access shared FTP/TFTP server from a member device	Optional	"Accessing the shared FTP/TFTP server from a member device"



To reduce the risk of being attacked by malicious users against opened socket and enhance switch security, the Switch 4210 provides 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 250 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	ndp enable interface port-list	Required Use either approach.
In system view	interface interface-type interface-number	
In Ethernet port view	Enter Ethernet port view ndp enable	Enable NDP on the port

Enabling NTDP globally and on a specific port

Table 251 Enable NTDP globally and a specific port

Operation	Command	Description
Enter system view	system-view	-
Enable NTDP globally	ntdp enable	Required
Enter Ethernet port view	interface interface-type interface-number	-
Enable NTDP on the port	ntdp enable	Required

Enabling the cluster function

Table 252 Enable the cluster function

Operation	Command	Description
Enter system view	system-view	-

Table 252 Enable the cluster function

Operation	Command	Description
Enable the cluster function globally	cluster enable	Optional By default, the cluster function is enabled.

Accessing the shared FTP/TFTP server from a member device

Perform the following operations in user view on a member device.

Table 253 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 <i>source-file</i> [<i>destination-file</i>]	Optional
Upload a file to the shared TFTP server of the cluster	tftp cluster put <i>source-file</i> [<i>destination-file</i>]	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 254 Manage a cluster through management devices

Operation	Command	Description
Enter system view	system-view	-
Enter cluster view	cluster	-
Configuring MAC address of Management device	administrator-address <i>mac-address name name</i>	Optional
Add a candidate device to the cluster	add-member [<i>member-number</i>] mac-address <i>H-H-H</i> [password <i>password</i>]	Optional
Remove a member device from the cluster	delete-member <i>member-number</i>	Optional
Reboot a specified member device	reboot member { <i>member-number</i> mac-address <i>H-H-H</i> } [eraseflash]	Optional
Return to system view	quit	-
Return to user view	quit	-
Switch between management device and member device	cluster switch-to { <i>member-number</i> mac-address <i>H-H-H</i> administrator }	Optional You can use this command switch to the view of a member device and switch back.
Locate device through MAC address and IP address	tracemac { by-mac <i>mac-address</i> vlan <i>vlan-id</i> by-ip <i>ip-address</i> } [nondp]	Optional These commands can be executed in any view.



- When using the `tracemac` command to locate a device by its IP address, the switch will query the corresponding ARP entry of the IP address, and then query the MAC address based on the ARP entry to locate the specified device finally.
- If the IP address has its corresponding ARP entry, but its corresponding MAC address is not in the MAC address table, the switch will fail to locate the specified device.
- If you build a cluster from the CLI or web interface and then you disable clustering for the commander, you may lose the cluster configuration and need to rebuild this if you wish to keep the cluster.

Configuring the Enhanced Cluster Features

Enhanced cluster feature overview

To configure the enhanced cluster features:

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.



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 255 The enhanced cluster feature configuration tasks

Operation	Description	Related section
Configure cluster topology management function	Required	"Configure cluster topology management function"
Configure the cluster device blacklist	Required	"Configure cluster device blacklist"

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 256 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 <i>mac-address</i> member-id <i>member-id</i> administrator }	Required
Save the standard topology to the Flash memory of the administrative device	topology save-to local-flash	Required
Restore the standard topology from the Flash memory of the administrative device	topology restore-from local-flash	Optional
Display the detailed information about a single device	display ntdp single-device mac-address <i>mac-address</i>	Optional
Display the topology of the current cluster	display cluster current-topology [mac-address <i>mac-address1</i> [to-mac-address <i>mac-address2</i>]] member-id <i>member-id1</i> [to-member-id <i>member-id2</i>]]	These commands can be executed in any view.
Display the information about the base topology of the cluster	display cluster base-topology [mac-address <i>mac-address</i> member <i>member-id</i>]	
Display the information about all the devices in the base cluster topology	display cluster base-members	

Configure cluster device blacklist

Perform the following configuration on the management device.

Table 257 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 <i>mac-address</i>	Optional By default, the cluster blacklist is empty.

Table 257 Configure the cluster device blacklist

Operation	Command	Description
Delete the specified MAC address from the cluster blacklist	black-list delete-mac <i>mac-address</i>	Optional
Delete a device from the cluster add this device to the cluster blacklist	delete-member <i>member-id</i> [to-black-list]	Optional
Displays the information about the devices in the cluster blacklist	display cluster black-list	Optional This command can be executed in any view.

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 258 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 <i>port-list</i>	
Display global NTDP information	display ntdp	
Display device information collected by NTDP	display ntdp device-list [verbose]	
Display status and statistics information about the cluster	display cluster	
Display information about the candidate devices of the cluster	display cluster candidates [mac-address <i>H-H-H</i>] verbose]	
Display information about the member devices of the cluster	display cluster members [<i>member-number</i> verbose]	
Clear the statistics on NDP ports	reset ndp statistics [interface <i>port-list</i>]	You can execute the reset command in user view.

Cluster Configuration Example

Basic Cluster Configuration Example

Network requirements

Three switches compose a cluster, where:

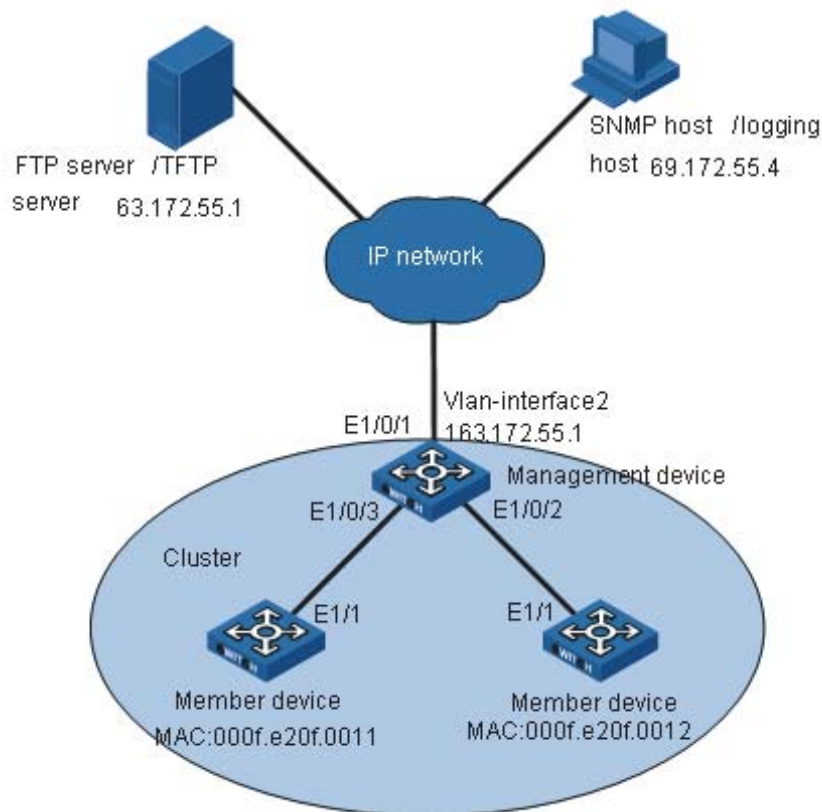
- The Switch 4210 serves as the management device.
- The rest are member devices.

Serving as the management device, the Switch 4210 manages the two member devices. The configuration for the cluster is as follows:

- The two member devices connect to the management device through Ethernet 1/0/2 and Ethernet 1/0/3.
- The management device connects to the Internet through Ethernet 1/0/1.
- Ethernet 1/0/1 belongs to VLAN 2, whose interface IP address is 163.172.55.1.
- All the devices in the cluster share the same FTP server and TFTP server.
- The FTP server and TFTP server use the same IP address: 63.172.55.1.
- The NMS and logging host use the same IP address: 69.172.55.4.

Network diagram

Figure 102 Network diagram for Switch Clustering cluster configuration



Configuration procedure

- 1 Configure the member devices (taking one member as an example)

Enable NDP globally and on Ethernet1/1.

```
<4210> system-view
[4210] ndp enable
[4210] interface Ethernet 1/1
[4210-Ethernet1/1] ndp enable
[4210-Ethernet1/1] quit
```

Enable NTDP globally and on Ethernet1/1.

```
[4210] ntdp enable
[4210] interface Ethernet 1/1
[4210-Ethernet1/1] ntdp enable
[4210-Ethernet1/1] quit
```

Enable the cluster function.

```
[4210] cluster enable
```

2 Configure the management device

Enable NDP globally and on Ethernet 1/0/2 and Ethernet 1/0/3.

```
<4210> system-view
[4210] ndp enable
[4210] interface Ethernet 1/0/2
[4210-Ethernet1/0/2] ndp enable
[4210-Ethernet1/0/2] quit
[4210] interface Ethernet 1/0/3
[4210-Ethernet1/0/3] ndp enable
[4210-Ethernet1/0/3] quit
```

Set the holdtime of NDP information to 200 seconds.

```
[4210] ndp timer aging 200
```

Set the interval to send NDP packets to 70 seconds.

```
[4210] ndp timer hello 70
```

Enable NTDP globally and on Ethernet 1/0/2 and Ethernet 1/0/3.

```
[4210] ntdp enable
[4210] interface Ethernet 1/0/2
[4210-Ethernet1/0/2] ntdp enable
[4210-Ethernet1/0/2] quit
[4210] interface Ethernet 1/0/3
[4210-Ethernet1/0/3] ntdp enable
[4210-Ethernet1/0/3] quit
```

Set the topology collection range to 2 hops.

```
[4210] ntdp hop 2
```

Set the member device forward delay for topology collection requests to 150 ms.

```
[4210] ntdp timer hop-delay 150
```

Set the member port forward delay for topology collection requests to 15 ms.

```
[4210] ntdp timer port-delay 15
```

Set the interval to collect topology information to 3 minutes.

```
[4210] ntdp timer 3
```

Enable the cluster function.

```
[4210] cluster enable
```

Enter cluster view.

```
[4210] cluster
[4210-cluster]
```

Configure a private IP address pool for the cluster. The IP address pool contains six IP addresses, starting from 172.16.0.1.

```
[4210-cluster] ip-pool 172.16.0.1 255.255.255.248
```

```

# Name and build the cluster.
[4210-cluster] build aaa
[aaa_0.3Com-cluster]

# Add the attached two switches to the cluster.
[aaa_0.3Com-cluster] add-member 1 mac-address 000f-e20f-0011
[aaa_0.3Com-cluster] add-member 17 mac-address 000f-e20f-0012

# Set the holdtime of member device information to 100 seconds.
[aaa_0.3Com-cluster] holdtime 100

# Set the interval to send handshake packets to 10 seconds.
[aaa_0.3Com-cluster] timer 10

# Configure the shared FTP server, TFTP server, Logging host and SNMP host for
the cluster.
[aaa_0.3Com-cluster] ftp-server 63.172.55.1
[aaa_0.3Com-cluster] tftp-server 63.172.55.1
[aaa_0.3Com-cluster] logging-host 69.172.55.4
[aaa_0.3Com-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_1.3Com> ftp cluster
```

Download the file named aaa.txt from the shared TFTP server of the cluster to the member device.

```
<aaa_1.3Com> tftp cluster get aaa.txt
```

Upload the file named bbb.txt from the member device to the shared TFTP server of the cluster.

```
<aaa_1.3Com> tftp cluster put bbb.txt
```



- 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

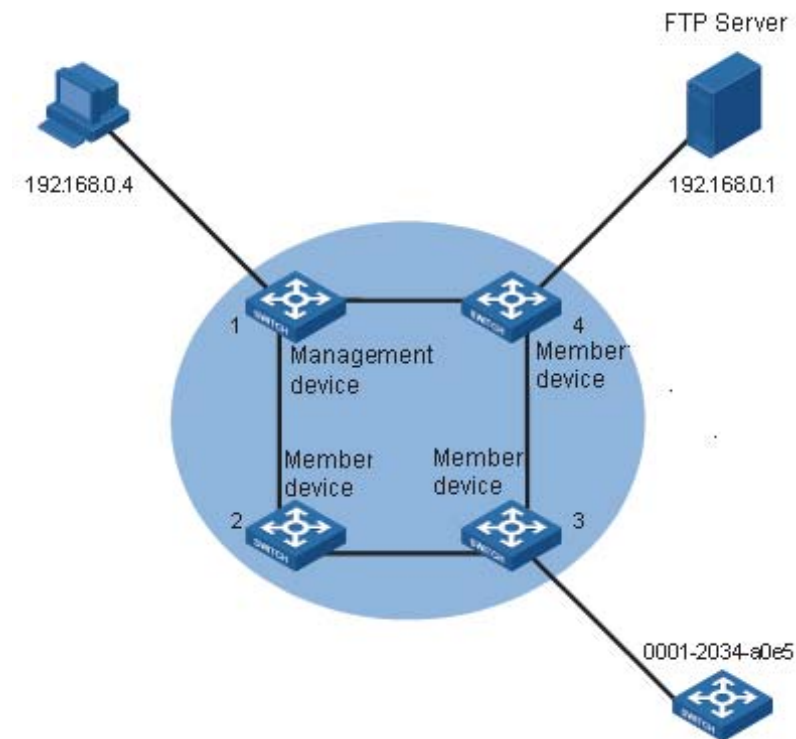
Network requirements

- 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 103 Network diagram for the enhanced cluster feature configuration



Configuration procedure

Enter cluster view.

```
<aaa_0.3Com> system-view
[aaa_0.3Com] cluster
```

Add the MAC address 0001-2034-a0e5 to the cluster blacklist.

```
[aaa_0.3Com-cluster] black-list add-mac 0001-2034-a0e5
```

Backup the current topology.

```
[aaa_0.3Com-cluster] topology accept all save-to local-flash
```


31

POE CONFIGURATION

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 the Switch 4210

PoE-enabled Switch 4210s:

- Switch 4210 PWR 9-Port
- Switch 4210 PWR 18-Port
- Switch 4210 PWR 26-Port

Table 259 Power supply parameters of PoE switches

Switch	Input power supply	Number of electrical ports supplying power	Maximum PoE distance	Maximum power provided by each electrical port	Total Maximum PoE output power
4210 PWR 9-Port	AC input	8	100 m	15400 mW	70 W
4210 PWR 18-Port	AC input	16			135 W
4210 PWR 26-Port	DC input	24			370 W
	AC input				370 W

A PoE-enabled Switch 4210 has the following features:

- As the PSE, it supports the IEEE802.3af standard. It can also supply power to some PDs that do not support the 802.3af standard.
- It can deliver data and current simultaneously through data wires (1,2,3,6) of 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.



- *When you use the PoE-enabled Switch 4210 to supply power, the PDs need no external power supply.*
- *If a remote PD has an external power supply, the PoE-enabled Switch 4210 and the external power supply will backup each other for the PD.*
- *Only the Ethernet electrical ports of the PoE-enabled Switch 4210 support the PoE feature.*

PoE Configuration

PoE Configuration Tasks

Table 260 PoE configuration tasks

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

Table 260 PoE configuration tasks

Task	Remarks
"Configuring the PD Compatibility Detection Function"	Optional
"Configuring PoE Over-Temperature Protection on the Switch"	Optional
"Upgrading the PSE Processing Software Online"	Optional
"Upgrading the PSE Processing Software Online"	Optional
"Displaying PoE Configuration"	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

Table 261 Enable the PoE feature on a port

Operation	Command	Description
Enter system view	system-view	-
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	-
Enable the PoE feature on a port	poe enable	Required



CAUTION:

- *By default, the PoE function on a port is enabled by the default configuration file 3comoscfg-xxport.def when the device is delivered.*
- *If you delete the default configuration file without specifying another one, the PoE function on a port will be disabled after you restart the device.*

Setting the Maximum Output Power on a Port

The maximum power that can be supplied by each Ethernet electrical port of a PoE-enabled Switch 4210 to its PD is 15,400 mW. In practice, you can set the maximum power on a port depending on the actual power of the PD, in the range of 1,000 to 15,400 mW and in the granularity of 100 mW.

Table 262 Set the maximum output power on a port

Operation	Command	Description
Enter system view	system-view	-
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	-
Set the maximum output power on the port	poe max-power <i>max-power</i>	Required 15,400 mW by default.

Setting PoE Management Mode and PoE Priority of a Port

When a switch is close to its full load in supplying power, you can adjust the power supply of the switch through the cooperation of the PoE management mode and the port PoE priority settings. The Switch 4210 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.

Table 263 Set the PoE management mode and PoE priority of a port

Operation	Command	Description
Enter system view	system-view	-
Set the PoE management mode for the switch	poe power-management { auto manual }	Required auto by default.
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	-
Set the PoE priority of a port	poe priority { critical high low }	Required low by default.

Setting the PoE Mode on a Port

PoE mode of a port falls into two types, signal mode and spare mode.

- Signal mode: DC power is carried over the data pairs (1,2,3,6) of category-3/5 twisted pairs.
- Spare mode: DC power is carried over the spare pairs (4,5,7,8) of category-3/5 twisted pairs.

Currently, the Switch 4210 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.

Table 264 Set the PoE mode on a port

Operation	Command	Description
Enter system view	system-view	-
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	-
Set the PoE mode on the port to signal	poe mode signal	Optional signal by default.

Configuring the PD Compatibility Detection Function

After the PD compatibility detection function is enabled, the switch can detect the PDs that do not conform to the 802.3af standard and supply power to them.

After the PoE feature is enabled, perform the following configuration to enable the PD compatibility detection function.

Table 265 Configure the PD compatibility detection function

Operation	Command	Description
Enter system view	system-view	-
Enable the PD compatibility detection function	poe legacy enable	Required 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.

Table 266 Configure a PD disconnection detection mode

Operation	Command	Description
Enter system view	system-view	-
Configure a PD disconnection detection mode	poe disconnect { ac dc }	Optional The default PD disconnection detection mode is AC.



Caution: If you adjust the PD disconnection detection mode when the device is running, the connected PDs will be powered off. Therefore, be cautious when doing 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).

Table 267 Configure PoE over-temperature protection on the switch

Operation	Command	Description
Enter system view	system-view	-
Enable PoE over-temperature protection on the switch	poe temperature-protection enable	Optional Enabled by default.



- *When the internal temperature of the switch decreases from X ($X > 65^{\circ}\text{C}$, or $X > 149^{\circ}\text{F}$) to Y ($60^{\circ}\text{C} \leq Y < 65^{\circ}\text{C}$, or $140^{\circ}\text{F} \leq Y < 149^{\circ}\text{F}$), the switch still keeps the PoE function disabled on all the ports.*
- *When the internal temperature of the switch increases from X ($X < 60^{\circ}\text{C}$, or $X < 140^{\circ}\text{F}$) to Y ($60^{\circ}\text{C} < Y \leq 65^{\circ}\text{C}$, or $140^{\circ}\text{F} < Y \leq 149^{\circ}\text{F}$), the switch still keeps the PoE function enabled on all the ports.*

Upgrading the PSE Processing Software Online

The online upgrading of PSE processing software can update the processing software or repair the software if it is damaged. Before performing the following configuration, download the PSE processing software to the Flash of the switch.

Table 268 Upgrade PSE processing software online

Operation	Command	Description
Enter system view	system-view	-
Upgrade the PSE processing software online	poe update { refresh full } filename	Required The specified PSE processing software is a file with the extension .s19.



- 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

After the above configuration, execute the **display** command in any view to see the operation of the PoE feature and verify the effect of the configuration.

Table 269 Display PoE configuration

Operation	Command	Description
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

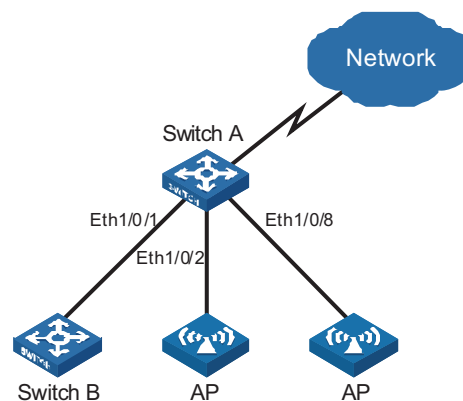
Networking requirements

Switch A is a Switch 4210 that supports PoE, Switch B can be PoE powered.

- The Ethernet 1/0/1 and Ethernet 1/0/2 ports of Switch A are connected to Switch B and an AP respectively; the Ethernet 1/0/8 port is intended to be connected with an important AP.
- The PSE processing software of Switch A is first upgraded online. The remotely accessed PDs are powered by Switch A.
- The power consumption of the accessed AP is 2,500 mW, and the maximum power consumption of Switch B is 12,000 mW.
- It is required to guarantee the power feeding to the PDs connected to the Ethernet 1/0/8 port even when Switch A is under full load.

Networking diagram

Figure 104 Network diagram for PoE



Configuration procedure

Upgrade the PSE processing software online.

```
<SwitchA> system-view
[SwitchA] poe update refresh 0290_021.s19
```

Enable the PoE feature on Ethernet 1/0/1, and set the PoE maximum output power of Ethernet 1/0/1 to 12,000 mW.

```
[SwitchA] interface Ethernet 1/0/1
[SwitchA-Ethernet1/0/1] poe enable
[SwitchA-Ethernet1/0/1] poe max-power 12000
[SwitchA-Ethernet1/0/1] quit
```

Enable the PoE feature on Ethernet 1/0/2, and set the PoE maximum output power of Ethernet 1/0/2 to 2500 mW.

```
[SwitchA] interface Ethernet 1/0/2
[SwitchA-Ethernet1/0/2] poe enable
[SwitchA-Ethernet1/0/2] poe max-power 2500
[SwitchA-Ethernet1/0/2] quit
```

Enable the PoE feature on Ethernet 1/0/8, and set the PoE priority of Ethernet 1/0/8 to critical.

```
[SwitchA] interface Ethernet 1/0/8
[SwitchA-Ethernet1/0/8] poe enable
```

```
[SwitchA-Ethernet1/0/8] poe priority critical  
[SwitchA-Ethernet1/0/8] quit
```

Set the PoE management mode on the switch to auto (it is the default mode, so this step can be omitted).

```
[SwitchA] poe power-management auto
```

Enable the PD compatibility detect of the switch to allow the switch to supply power to part of the devices noncompliant with the 802.3af standard.

```
[SwitchA] poe legacy enable
```


32

POE PROFILE CONFIGURATION

Introduction to PoE Profile

On a large-sized network or a network with mobile users, to help network administrators monitor the switch's PoE features, the Switch 4210 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

Table 270 Configure PoE profile

Operation	Command	Description
Enter system view	system-view	-
Create a PoE profile and enter PoE profile view	poe-profile <i>profilename</i>	Required If the PoE file is created, you will enter PoE profile view directly through the command.
Configure the relevant features in PoE profile	Enable the PoE feature on a port poe enable	Required Disabled by default.
	Configure PoE mode for Ethernet ports poe mode { signal spare }	Optional signal by default.
	Configure the PoE priority for Ethernet ports poe priority { critical high low }	Optional low by default.
	Configure the maximum power for Ethernet ports poe max-power <i>max-power</i>	Optional 15,400 mW by default.
Quit system view	quit	-

Table 270 Configure PoE profile

Operation		Command	Description
Apply the existing PoE profile to the specified Ethernet port	In system view	apply poe-profile <i>profile-name</i> interface <i>interface-type</i> <i>interface-number</i> [to <i>interface-type</i> <i>interface-number</i>]	Use either approach.
	In Ethernet port view	Enter Ethernet port view Apply the existing PoE profile to the port interface <i>interface-type</i> <i>interface-number</i> apply poe-profile <i>profile-name</i>	

Note the following during the configuration:

- When the **apply poe-profile** command is used to apply a PoE profile to a port, some PoE features in the PoE profile can be applied successfully while some cannot. PoE profiles are applied to the Switch 4210 according to the following rules:
 - When the **apply poe-profile** command is used to apply a PoE profile to a port, the PoE profile is applied successfully only if one PoE feature in the PoE profile is applied properly. When the **display current-configuration** command is used for query, it is displayed that the PoE profile is applied properly to the port.
 - If one or more features in the PoE profile are not applied properly on a port, the switch will prompt explicitly which PoE features in the PoE profile are not applied properly on which ports.
 - The **display current-configuration** command can be used to query which PoE profile is applied to a port. However, the command cannot be used to query which PoE features in a PoE profiles are applied successfully.
- PoE profile configuration is a global configuration, and applies synchronously in the intelligent resilient framework (IRF) system.
- Combination of Unit creates a new Fabric. In the newly created Fabric, the PoE profile configuration of the Unit with the smallest Unit ID number will become the PoE profile configuration for the Fabric currently in use.
- Split of Fabric results in many new Fabrics. In each newly created Fabric, the PoE profile configuration of each Unit remains the same as it was before the split.

Displaying PoE Profile Configuration

After the above configuration, execute the **display** command in any view to see the running status of the PoE profile and verify the effect of the configuration by checking the displayed information.

Table 271 Display the PoE profile configuration

Operation	Command	Description
Display the detailed information about the PoE profiles created on the switch	display poe-profile { all-profile interface <i>interface-type</i> <i>interface-number</i> name <i>profile-name</i> }	Available in any view

PoE Profile Configuration Example

PoE Profile Application Example

Network requirements

Switch A is a Switch 4210 that supports PoE.

Ethernet 1/0/1 through Ethernet 1/0/10 of Switch A are used by users of group A, who have the following requirements:

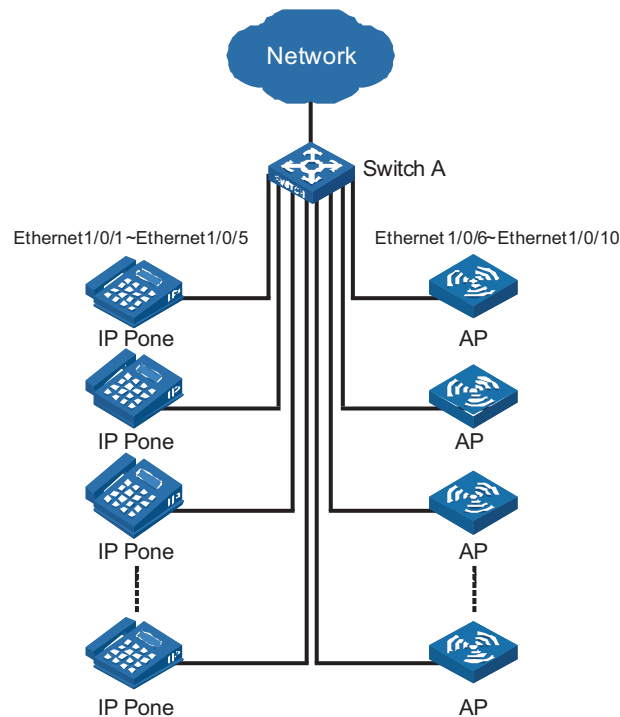
- The PoE function can be enabled on all ports in use.
- Signal mode is used to supply power.
- The PoE priority for Ethernet 1/0/1 through Ethernet 1/0/5 is Critical, whereas the PoE priority for Ethernet 1/0/6 through Ethernet 1/0/10 is High.
- The maximum power for Ethernet 1/0/1 through Ethernet 1/0/5 ports is 3,000 mW, whereas the maximum power for Ethernet 1/0/6 through Ethernet 1/0/10 is 15,400 mW.

Based on the above requirements, two PoE profiles are made for users of group A.

- Apply PoE profile 1 for Ethernet 1/0/1 through Ethernet 1/0/5;
- Apply PoE profile 2 for Ethernet 1/0/6 through Ethernet 1/0/10.

Network diagram

Figure 105 PoE profile application



Configuration procedure

Create Profile1, and enter PoE profile view.

```
<SwitchA> system-view
[SwitchA] poe-profile Profile1
```

In Profile1, add the PoE policy configuration applicable to Ethernet 1/0/1 through Ethernet 1/0/5 ports for users of group A.

```
[SwitchA-poe-profile-Profile1] poe enable
[SwitchA-poe-profile-Profile1] poe mode signal
[SwitchA-poe-profile-Profile1] poe priority critical
[SwitchA-poe-profile-Profile1] poe max-power 3000
[SwitchA-poe-profile-Profile1] quit
```

Display detailed configuration information for Profile1.

```
[SwitchA] display poe-profile name Profile1
Poe-profile: Profile1, 3 action
poe enable
poe max-power 3000
poe priority critical
```

Create Profile2, and enter PoE profile view.

```
[SwitchA] poe-profile Profile2
```

In Profile2, add the PoE policy configuration applicable to Ethernet 1/0/6 through Ethernet 1/0/10 ports for users of group A.

```
[SwitchA-poe-profile-Profile2] poe enable
[SwitchA-poe-profile-Profile2] poe mode signal
[SwitchA-poe-profile-Profile2] poe priority high
[SwitchA-poe-profile-Profile2] poe max-power 15400
[SwitchA-poe-profile-Profile2] quit
```

Display detailed configuration information for Profile2.

```
[SwitchA] display poe-profile name Profile2
Poe-profile: Profile2, 2 action
poe enable
poe priority high
```

Apply the configured Profile1 to Ethernet 1/0/1 through Ethernet 1/0/5 ports.

```
[SwitchA] apply poe-profile Profile1 interface Ethernet1/0/1 to Ethernet1/0/5
```

Apply the configured Profile2 to Ethernet 1/0/6 through Ethernet 1/0/10 ports.

```
[SwitchA] apply poe-profile Profile2 interface Ethernet1/0/6 to Ethernet1/0/10
```

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 Sun NetManager and IBM NetView.
- 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 trap messages 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

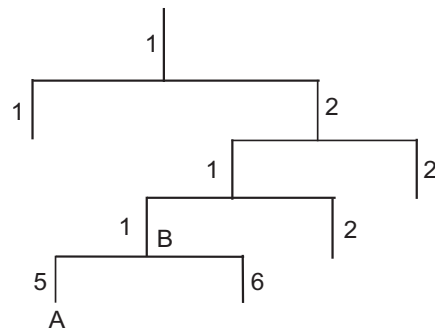
information, while those with read-write permission can configure the switch as well.

- 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 106. Each node in this tree can be uniquely identified by a path starting from the root.

Figure 106 Architecture of the MIB tree



The management information base (MIB) describes the hierarchical architecture of the tree and it is the set defined by the standard variables of the monitored network devices. In the above figure, the managed object B can be uniquely identified by a string of numbers {1.2.1.1}. The number string is the object identifier (OID) of the managed object.

The common MIBs supported by switches are listed in Table 272.

Table 272 Common MIBs

MIB attribute	MIB content	Related RFC
Public MIB	MIB II based on TCP/IP network device	RFC 1213
	BRIDGE MIB	RFC 1493
		RFC 2675
	RIP MIB	RFC 1724
	RMON MIB	RFC 2819
	Ethernet MIB	RFC 2665
	OSPF MIB	RFC 1253
	IF MIB	RFC 1573

Table 272 Common MIBs

MIB attribute	MIB content	Related RFC
Private MIB	DHCP MIB QACL MIB MSTP MIB VLAN MIB IPV6 ADDRESS MIB MIRRORGROUP MIB QINQ MIB 802.x MIB Switch Clustering MIB NTP MIB Device management Interface management	-

Configuring Basic SNMP Functions

SNMPv3 configuration is quite different from that of SNMPv1 and SNMPv2c. Therefore, the configuration of basic SNMP functions is described by SNMP versions, as listed in Table 273 and Table 274.

Table 273 Configure basic SNMP functions (SNMPv1 and SNMPv2c)

Operation	Command	Description
Enter system view	system-view	-
Enable SNMP agent	snmp-agent	Optional Disabled by default. You can enable SNMP agent by executing this command or any of the commands used to configure SNMP agent.
Set system information, and specify to enable SNMPv1 or SNMPv2c on the switch	snmp-agent sys-info { contact <i>sys-contact</i> location <i>sys-location</i> version { { v1 v2c v3 }* all }	Required By default, the contact information for system maintenance is "R&D Hangzhou, 3Com Technology Co., Ltd.", the system location is "Hangzhou China", and the SNMP version is SNMPv3.

Table 273 Configure basic SNMP functions (SNMPv1 and SNMPv2c)

Operation			Command	Description
Set a community name and access permission	Direct configuration	Set a community name	snmp-agent community { read write } <i>community-name [acl acl-number mib-view view-name]*</i>	Required <ul style="list-style-type: none"> You can set an SNMPv1/SNMPv2c community name through direct configuration.
	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]	<ul style="list-style-type: none"> Indirect configuration is compatible with SNMPv3. The added user is equal to the community name for SNMPv1 and SNMPv2c.
		Add a user to an SNMP group	snmp-agent usm-user { v1 v2c } user-name group-name [acl acl-number]	<ul style="list-style-type: none"> You can choose either of them as needed.
Set the maximum size of an SNMP packet for SNMP agent to receive or send			snmp-agent packet max-size byte-count	Optional 1,500 bytes by default.
Set the device switch fabric ID			snmp-agent local-switch fabricid switch fabricid	Optional By default, the device switch fabric ID is "enterprise number + device information".
Create/Update the view information			snmp-agent mib-view { included excluded } <i>view-name oid-tree [mask mask-value]</i>	Optional By default, the view name is "ViewDefault" and OID is 1.

Table 274 Configure basic SNMP functions (SNMPv3)

Operation			Command	Description
Enter system view			system-view	-
Enable SNMP agent			snmp-agent	Optional Disabled by default. You can enable SNMP agent by executing this command or any of the commands used to configure SNMP agent.
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 } }	Required By default, the contact information for system maintenance is "R&D Hangzhou, 3Com Technology Co., Ltd.", the system location is "Hangzhou China", and the SNMP version is SNMPv3.
Set an SNMP group			snmp-agent group v3 group-name [authentication privacy] [read-view read-view] [write-view write-view] [notify-view notify-view] [acl acl-number]	Required

Table 274 Configure basic SNMP functions (SNMPv3)

Operation	Command	Description
Encrypt a plain-text password to generate a cipher-text one	snmp-agent calculate-password <i>plain-password mode { md5 sha } { local-switch fabricid specified-switch fabricid switch fabricid }</i>	Optional This command is used if password in cipher-text is needed for adding a new user.
Add a user to an SNMP group	snmp-agent usm-user v3 <i>user-name group-name [cipher] [authentication-mode { md5 sha } auth-password [privacy-mode { des56 } priv-password]] [acl acl-number]</i>	Required
Set the maximum size of an SNMP packet for SNMP agent to receive or send	snmp-agent packet max-size <i>byte-count</i>	Optional 1,500 bytes by default.
Set the device switch fabric ID	snmp-agent local-switch fabricid <i>switch fabricid</i>	Optional By default, the device switch fabric ID is "enterprise number + device information".
Create or update the view information	snmp-agent mib-view { included excluded } <i>view-name oid-tree [mask mask-value]</i>	Optional By default, the view name is "ViewDefault" and OID is 1.



A Switch 4210 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 and UDP port 1024 used by SNMP agents and SNMP trap clients respectively.
- Executing the **undo snmp-agent** command disables the SNMP function and closes UDP port 161 and UDP port 1024 as well.

Configuring Trap Parameters

Configuring Basic Trap

Trap messages are 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.

Table 275 Configure basic Trap

Operation	Command	Description
Enter system view	system-view	-

Table 275 Configure basic Trap

Operation		Command	Description
Enable the switch to send Trap messages to NMS		snmp-agent trap enable [configuration flash standard authentication coldstart linkdown linkup warmstart]* system]	Optional By default, a port is enabled to send all types of Traps.
Enable the port to send Trap messages	Enter port view or interface view Enable the port or interface to send Trap messages Quit to system view	interface <i>interface-type</i> <i>interface-number</i> enable snmp trap updown quit	
Set the destination for Trap messages		snmp-agent target-host trap address udp-domain { <i>ip-address</i> } [udp-port <i>port-number</i>] params securityname <i>security-string</i> [v1 v2c v3 { authentication privacy }]	Required
Set the source address for Trap messages		snmp-agent trap source <i>interface-type</i> <i>interface-number</i>	Optional
Set the size of the queue used to hold the Traps to be sent to the destination host		snmp-agent trap queue-size <i>size</i>	Optional The default is 100.
Set the aging time for Trap messages		snmp-agent trap life <i>seconds</i>	Optional 120 seconds by default.

Configuring Extended Trap

The extended Trap includes the following.

- Interface description " and "interface type" are added into the linkUp/linkDown Trap message. When receiving this extended Trap message, NMS can immediately determine which interface on the device fails according to the interface description and type.
- In all Trap messages sent from the information center to the log server, a MIB object name is added after the OID field of the MIB object. The name is for your better understanding of the MIB object.

Table 276 Configure extended Trap

Operation	Command	Description
Enter system view	system-view	-
Configure extended Trap	snmp-agent trap ifmib link extended	Optional By default, the linkUp/linkDown Trap message adopts the standard format defined in IF-MIB. For details, refer to RFC 1213.

Enabling Logging for Network Management

Table 277 Enable logging for network management

Operation	Command	Description
Enter system view	system-view	-
Enable logging for network management	snmp-agent log { set-operation get-operation all }	Optional Disabled by default.



Use the **display logbuffer** command to view the log of the get and set operations requested by the NMS.

Displaying SNMP

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

Table 278 Display SNMP

Operation	Command	Description
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 switch fabric ID of the current device	display snmp-agent { local-switch fabricid remote-switch fabricid }	
Display group information about the device	display snmp-agent group [group-name]	
Display SNMP user information	display snmp-agent usm-user [switch fabricid switch fabricid username user-name group group-name]	
Display Trap list information	display snmp-agent trap-list	
Display the currently configured community name	display snmp-agent community [read write]	
Display the currently configured MIB view	display snmp-agent mib-view [exclude include viewname view-name]	

SNMP Configuration Examples

SNMP Configuration Examples

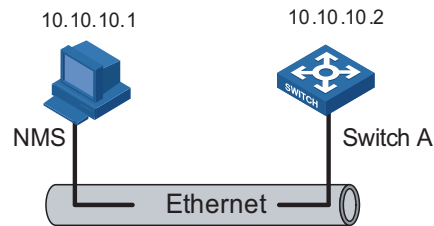
Network requirements

- 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 trap messages.

Thus, the NMS is able to access Switch A and receive the trap messages sent by Switch A.

Network diagram

Figure 107 Network diagram for SNMP configuration



Network procedure

Enable SNMP agent, and set the SNMPv1 and SNMPv2c community names.

```
<4210> system-view
[4210] snmp-agent
[4210] snmp-agent sys-info version all
[4210] snmp-agent community read public
[4210] snmp-agent community write private
```

Set the access right of the NMS to the MIB of the SNMP agent.

```
[4210] 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

```
[4210] snmp-agent group v3 managev3group privacy write-view internet
[4210] snmp-agent usm-user v3 managev3user managev3group authentication
-mode md5 passmd5 privacy-mode des128 cfb128cfb128
```

Set the VLAN-interface 2 as the interface used by NMS. Add port Ethernet 1/0/2, which is to be used for network management, to VLAN 2. Set the IP address of VLAN-interface 2 as 10.10.10.2.

```
[4210] vlan 2
[4210-vlan2] port Ethernet 1/0/2
[4210-vlan2] quit
[4210] interface Vlan-interface 2
[4210-Vlan-interface2] ip address 10.10.10.2 255.255.255.0
[4210-Vlan-interface2] quit
```

Enable the SNMP agent to send Trap messages to the NMS whose IP address is 10.10.10.1. The SNMP community name to be used is "public".

```
[4210] snmp-agent trap enable standard authentication
[4210] snmp-agent trap enable standard coldstart
[4210] snmp-agent trap enable standard linkup
[4210] snmp-agent trap enable standard linkdown
[4210] snmp-agent target-host trap address udp-domain 10.10.10.1 udp
-port 5000 params securityname public
```

Configuring the NMS

The Switch 4210 supports 3Com's Network Management System (NMS). SNMPv3 adopts user name and password authentication. When you use 3Com's NMS, you need to set user names and choose the security level in [Authentication Parameter]. For each security level, you need to set authorization mode, authorization password, encryption mode, encryption password, and so on. In addition, you need to set timeout time and maximum retry times.

You can query and configure an Ethernet switch through the NMS. For more information, refer to the corresponding documentation provided by the NMS product.



Authentication-related configuration on an NMS must be consistent with that of the devices for the NMS to manage the devices successfully.

34

RMON CONFIGURATION

Introduction to RMON

Remote monitoring (RMON) is a kind of management information base (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.

The 3Com Switch 4210 implements RMON in the second way. With an RMON agent embedded, the Switch 4210 can serve as a network device with the RMON probe function. Through the RMON-capable SNMP agents running on the 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 trap messages to the NMS
- Logging the event and sending trap messages 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 “Configuring Basic SNMP Functions” on page 353.

Table 279 Configure RMON

Operation	Command	Description
Enter system view	system-view	-
Add an event entry	rmon event <i>event-entry</i> [description <i>string</i>] { log trap <i>trap-community</i> log-trap <i>log-trapcommunity</i> none } [owner <i>text</i>]	Optional
Add an alarm entry	rmon alarm <i>entry-number</i> <i>alarm-variable</i> <i>sampling-time</i> { delta absolute } rising_threshold <i>threshold-value1</i> <i>event-entry1</i> falling_threshold <i>threshold-value2</i> <i>event-entry2</i> [owner <i>text</i>]	Optional Before adding an alarm entry, you need to use the rmon event command to define the event to be referenced by the alarm entry.
Add an extended alarm entry	rmon prialarm <i>entry-number</i> <i>prialarm-formula</i> <i>prialarm-des</i> <i>sampling-timer</i> { delta absolute changeratio } rising_threshold <i>threshold-value1</i> <i>event-entry1</i> falling_threshold <i>threshold-value2</i> <i>event-entry2</i> entrytype { forever cycle } <i>cycle-period</i> [owner <i>text</i>]	Optional Before adding an extended alarm entry, you need to use the rmon event command to define the event to be referenced by the extended alarm entry.
Enter Ethernet port view	interface <i>interface-type</i> <i>interface-number</i>	-
Add a history entry	rmon history <i>entry-number</i> buckets <i>number</i> interval <i>sampling-interval</i> [owner <i>text</i>]	Optional
Add a statistics entry	rmon statistics <i>entry-number</i> [owner <i>text</i>]	Optional



- 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

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

Table 280 Display RMON

Operation	Command	Description
Display RMON statistics	display rmon statistics [<i>interface-type</i> <i>interface-number</i> unit <i>unit-number</i>]	Available in any view.
Display RMON history information	display rmon history [<i>interface-type</i> <i>interface-number</i> unit <i>unit-number</i>]	
Display RMON alarm information	display rmon alarm [<i>entry-number</i>]	
Display extended RMON alarm information	display rmon prialarm [<i>prialarm-entry-number</i>]	
Display RMON events	display rmon event [<i>event-entry</i>]	
Display RMON event logs	display rmon eventlog [<i>event-entry</i>]	

RMON Configuration Examples

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 108 Network diagram for RMON configuration



Configuration procedures

Add the statistics entry numbered 1 to take statistics on Ethernet 1/0/1.

```
<4210> system-view
[4210] interface Ethernet 1/0/1
```

```
[4210-Ethernet1/0/1] rmon statistics 1
[4210-Ethernet1/0/1] quit
```

Add the event entries numbered 1 and 2 to the event table, which will be triggered by the following extended alarm.

```
[4210] rmon event 1 log
[4210] rmon event 2 trap 10.21.30.55
```

Add an entry numbered 2 to the extended alarm table to allow the system to calculate the alarm variables with the (.1.3.6.1.2.1.16.1.1.1.9.1+.1.3.6.1.2.1.16.1.1.1.10.1) formula to get the numbers of all the oversize and undersize packets received by Ethernet 1/0/1 that are in correct data format and sample it in every 10 seconds. When the change ratio between samples reaches the rising threshold of 50, event 1 is triggered; when the change ratio drops under the falling threshold, event 2 is triggered.

```
[4210] 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 fo
rever owner user1
```

Display the RMON extended alarm entry numbered 2.

```
[4210] 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
```

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 “Applications of NTP”).

A local system running NTP can not only be synchronized by other clock sources, but also serve as a clock source to synchronize other clocks. Besides, it can synchronize, or be synchronized by other systems by exchanging NTP messages.

Applications of NTP

As setting the system time manually in a network with many devices leads to a lot of workload and cannot ensure accuracy, it is unfeasible for an administrator to perform the operation. However, an administrator can synchronize the clocks of devices in a network with required accuracy by performing NTP configuration.

NTP is mainly applied to synchronizing the clocks of all devices in a network. For example:

- In network management, the analysis of the log information and debugging information collected from different devices is meaningful and valid only when network devices that generate the information adopts the same time.
- The billing system requires that the clocks of all network devices be consistent.
- Some functions, such as restarting all network devices in a network simultaneously require that they adopt the same time.
- When multiple systems cooperate to handle a rather complex transaction, they must adopt the same time to ensure a correct execution order.
- To perform incremental backup operations between a backup server and a host, you must make sure they adopt the same time.

NTP has the following advantages:

- Defining the accuracy of clocks by stratum to synchronize the clocks of all devices in a network quickly
- Supporting access control (See “Configuring Access Control Right”) and MD5 encrypted authentication (See “Configuring NTP Authentication”)
- Sending protocol packets in unicast, multicast, or broadcast mode
- 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 a Switch 4210 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.

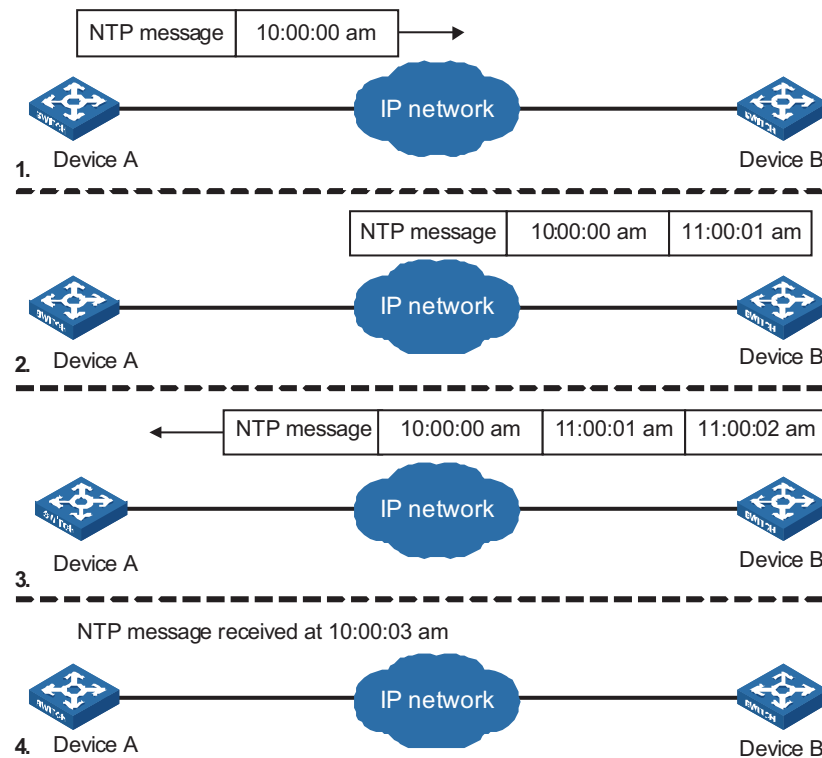
Implementation Principle of NTP

Figure 109 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 109 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 receiving a response packet, the local time of Device A is 10:00:03 am (T_4)

At this time, Device A has enough information to calculate the following two parameters:

- Delay for an NTP message to make a round trip between Device A and Device B:

$$\text{Delay} = (T_4 - T_1) - (T_3 - T_2).$$
- Time offset of Device A relative to Device B:

$$\text{Offset} = ((T_2 - T_1) + (T_3 - T_4))/2.$$

Device A can then set its own clock according to the above information to synchronize its clock to that of Device B.

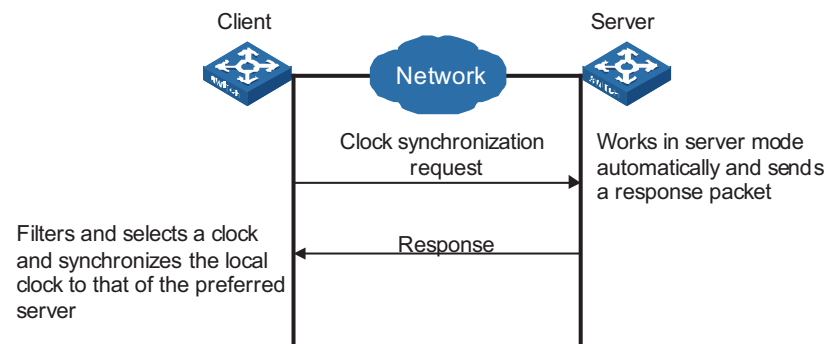
For detailed information, refer to RFC 1305.

NTP Implementation Modes

According to the network structure and the position of the local Ethernet switch in the network, the local Ethernet switch can work in multiple NTP modes to synchronize the clock.

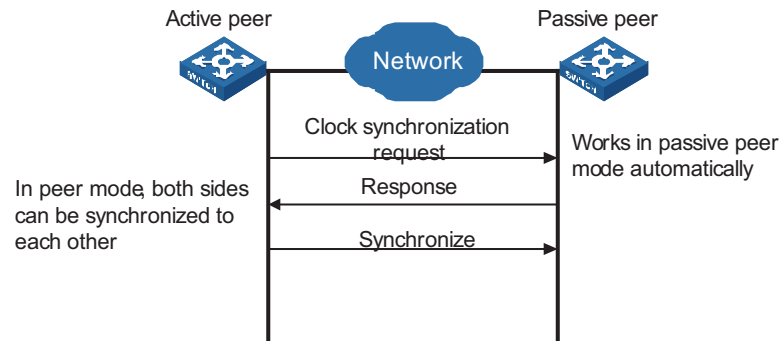
Server/client mode

Figure 110 Server/client mode



Symmetric peer mode

Figure 111 Symmetric peer mode

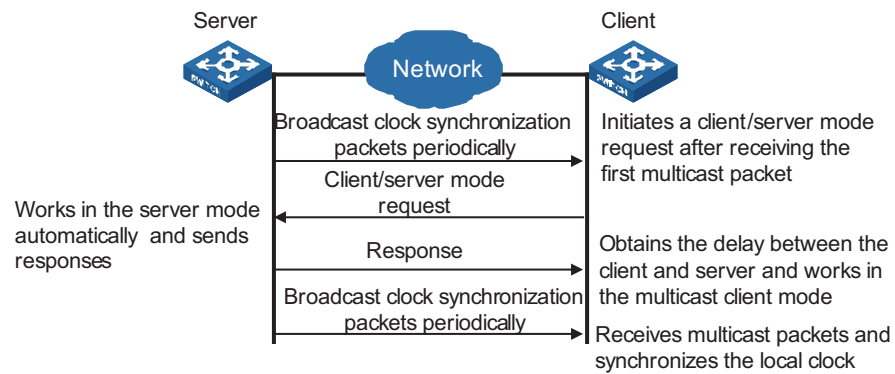


In the symmetric peer mode, the local Switch 4210 serves as the symmetric-active peer and sends clock synchronization request first, while the remote server serves as the symmetric-passive peer automatically.

If both of the peers have reference clocks, the one with a smaller stratum number is adopted.

Broadcast mode

Figure 112 Broadcast mode



Multicast mode

Figure 113 Multicast mode

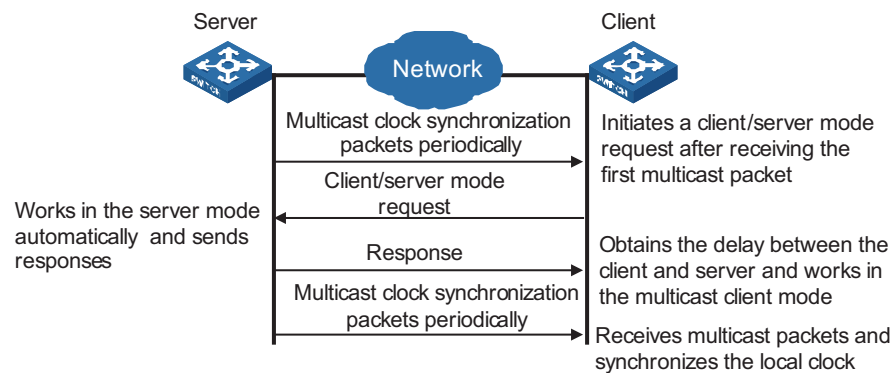


Table 281 describes how the above mentioned NTP modes are implemented on the 3Com Switch 4210 Family.

Table 281 NTP implementation modes on the 3Com Switch 4210 Family

NTP implementation mode	Configuration on the Switch 4210
Server/client mode	Configure the local Switch 4210 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 Switch 4210 to work in NTP symmetric peer mode. In this mode, the remote server serves as the symmetric-passive peer of the Switch 4210, and the local switch serves as the symmetric-active peer.
Broadcast mode	Configure the local Switch 4210 to work in NTP broadcast server mode. In this mode, the local switch broadcasts NTP messages through the VLAN interface configured on the switch. Configure the Switch 4210 to work in NTP broadcast client mode. In this mode, the local Switch 4210 receives broadcast NTP messages through the VLAN interface configured on the switch.
Multicast mode	Configure the local Switch 4210 to work in NTP multicast server mode. In this mode, the local switch sends multicast NTP messages through the VLAN interface configured on the switch. Configure the local Switch 4210 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 the Switch 4210 is in server mode or symmetric passive mode, you need not perform related configurations on this switch, but 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 Switch 4210 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 Tasks

Table 282 NTP configuration tasks

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

A Switch 4210 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”



To protect unused sockets against attacks by malicious users and improve security, the 3Com Switch 4210 Family provides 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.

Table 283 Configure an NTP client

Operation	Command	Description
Enter system view	system-view	-
Configure an NTP client	ntp-service unicast-server { <i>remote-ip</i> <i>server-name</i> } [authentication-keyid <i>key-id</i> priority source-interface <i>Vlan-interface</i> <i>vlan-id</i> version <i>number</i>]*	Required By default, the switch is not configured to work in the NTP client mode.



- 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.

Table 284 Configure a symmetric-active switch

Operation	Command	Description
Enter system view	system-view	-
Specify a symmetric-passive peer for the switch	ntp-service unicast-peer { <i>remote-ip</i> <i>peer-name</i> } [authentication-keyid <i>key-id</i> priority source-interface Vlan-interface <i>vlan-id</i> version <i>number</i>]*	Required By default, a switch is not configured to work in the symmetric mode.



- In the symmetric peer mode, you need to execute the related NTP configuration commands (refer to “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.

A 3Com Switch 4210 can operate as a broadcast server or a broadcast client.

- Refer to Table 285 for configuring a switch to work in the NTP broadcast server mode.
- Refer to Table 286 for configuring a switch to work in the NTP broadcast client mode.



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

Table 285 Configure a switch to work in the NTP broadcast server mode

Operation	Command	Description
Enter system view	system-view	-
Enter VLAN interface view	interface Vlan-interface <i>vlan-id</i>	-
Configure the switch to work in the NTP broadcast server mode	ntp-service broadcast-server [authentication-keyid <i>key-id</i> version <i>number</i>]*	Required Not configured by default.

Configuring a switch to work in the NTP broadcast client mode


Table 286 Configure a switch to work in the NTP broadcast client mode

Operation	Command	Description
Enter system view	system-view	-
Enter VLAN interface view	interface Vlan-interface <i>vlan-id</i>	-
Configure the switch to work in the NTP broadcast client mode	ntp-service broadcast-client	Required Not configured by default.

Configuring NTP Multicast Mode

For switches working in the multicast mode, you need to configure both the server and clients. The multicast server periodically sends NTP multicast messages to multicast clients. The switches working in the NTP multicast client mode will respond to the NTP messages, so as to start the clock synchronization.

A 3Com Switch 4210 can work as a multicast server or a multicast client.

- Refer to Table 287 for configuring a switch to work in the NTP multicast server mode.
 - Refer to Table 288 for configuring a switch to work in the NTP multicast client mode.
-  ■ A multicast server can synchronize multicast clients only after its clock has been synchronized.
- The Switch 4210 working in the multicast server mode supports up to 1,024 multicast clients.

Configuring a switch to work in the multicast server mode

Table 287 Configure a switch to work in the NTP multicast server mode

Operation	Command	Description
Enter system view	system-view	-
Enter VLAN interface view	interface Vlan-interface <i>vlan-id</i>	-
Configure the switch to work in the NTP multicast server mode	ntp-service multicast-server [<i>ip-address</i>] [authentication-keyid <i>keyid</i> ttl <i>tvl-number</i> version <i>number</i>]*	Required Not configured by default.

Configuring a switch to work in the multicast client mode

Table 288 Configure a switch to work in the NTP multicast client mode

Operation	Command	Description
Enter system view	system-view	-
Enter VLAN interface view	interface Vlan-interface <i>vlan-id</i>	-
Configure the switch to work in the NTP multicast client mode	ntp-service multicast-client [<i>ip-address</i>]	Required Not configured by default.

Configuring Access Control Right

With the following command, you can configure the NTP service access-control right to the local switch for a peer device. There are four access-control rights, as follows:

- **query**: Control query right. This level of right permits the peer device to perform control query to the NTP service on the local device but does not permit the peer device to synchronize its clock to the local device. The so-called "control query" refers to query of state of the NTP service, including alarm information, authentication status, clock source information, and so on.
- **synchronization**: Synchronization right. This level of right permits the peer device to synchronize its clock to the local switch but does not permit the peer device to perform control query.
- **server**: Server right. This level of right permits the peer device to perform synchronization and control query to the local switch but does not permit the local switch to synchronize its clock to the peer device.
- **peer**: Peer access. This level of right permits the peer device to perform synchronization and control query to the local switch and also permits the local switch to synchronize its clock to the peer device.

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. To configure an ACL, refer to "ACL Configuration" on page 291.

Configuration Procedure

Table 289 Configure the NTP service access-control right to the local device for peer devices

Operation	Command...	Description
Enter system view	system-view	-
Configure the NTP service access-control right to the local switch for peer devices	ntp-service access { peer server synchronization query } acl-number	Optional peer by default



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 290 shows the roles of devices in the NTP authentication function.

Table 290 Description of the device roles in NTP authentication function

Role of device	Working mode
Client	Client in the server/client mode
	Client in the broadcast mode
	Client in the multicast mode
	Symmetric-active peer in the symmetric peer mode
Server	Server in the server/client mode
	Server in the broadcast mode
	Server in the multicast mode
	Symmetric-passive peer in the symmetric peer mode

Configuration Prerequisites

NTP authentication configuration involves:

- Configuring NTP authentication on the client
- Configuring NTP authentication on the server

Observe the following principles when configuring NTP authentication:

- If the NTP authentication function is not enabled on the client, the clock of the client can be synchronized to a server no matter whether the NTP authentication function is enabled on the server (assuming that other related configurations are properly performed).
- For the NTP authentication function to take effect, a trusted key needs to be configured on both the client and server after the NTP authentication is enabled on them.
- The local clock of the client is only synchronized to the server that provides a trusted key.
- In addition, for the server/client mode and the symmetric peer mode, you need to associate a specific key on the client (the symmetric-active peer in the symmetric peer mode) with the corresponding NTP server (the symmetric-passive peer in the symmetric peer mode); for the NTP broadcast/multicast mode, you need to associate a specific key on the broadcast/multicast server with the corresponding NTP broadcast/multicast client. Otherwise, NTP authentication cannot be enabled normally.
- Configurations on the server and the client must be consistent.

Configuration Procedure **Configuring NTP authentication on the client**

Table 291 Configure NTP authentication on the client

Operation	Command	Description
Enter system view	system-view	-
Enable the NTP authentication function	ntp-service authentication enable	Required Disabled by default.
Configure the NTP authentication key	ntp-service authentication-keyid <i>key-id</i> authentication-model md5 <i>value</i>	Required By default, no NTP authentication key is configured.
Configure the specified key as a trusted key	ntp-service reliable authentication-keyid <i>key-id</i>	Required By default, no trusted key is configured.
Associate the specified key with the corresponding NTP server	Configure on the client in the server/client mode ntp-service unicast-server { <i>remote-ip</i> <i>server-name</i> } authentication-keyid <i>key-id</i> Configure on the symmetric-active peer in the symmetric peer mode ntp-service unicast-peer { <i>remote-ip</i> <i>peer-name</i> } authentication-keyid <i>key-id</i>	Required For the client in the NTP broadcast/multicast mode, you just need to associate the specified key with the client on the corresponding server.



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

Table 292 Configure NTP authentication on the server

Operation	Command	Description
Enter system view	system-view	-
Enable NTP authentication	ntp-service authentication enable	Required Disabled by default.
Configure an NTP authentication key	ntp-service authentication-keyid <i>key-id</i> authentication-mode md5 <i>value</i>	Required By default, no NTP authentication key is configured.
Configure the specified key as a trusted key	ntp-service reliable authentication-keyid <i>key-id</i>	Required By default, no trusted authentication key is configured.
Enter VLAN interface view	interface <i>Vlan-interface</i> <i>vlan-id</i>	-

Table 292 Configure NTP authentication on the server

Operation	Command	Description
Associate the specified key with the corresponding broadcast/multicast client	Configure on the NTP broadcast server ntp-service broadcast-server authentication-keyid <i>key-id</i> Configure on the NTP multicast server ntp-service multicast-server authentication-keyid <i>key-id</i>	<ul style="list-style-type: none"> In NTP broadcast server mode and NTP multicast server mode, you need to associate the specified key with the corresponding broadcast/multicast client You can associate an NTP broadcast/multicast client with an authentication key while configuring NTP mode. You can also use this command to associate them after configuring the NTP mode.



The procedure for configuring NTP authentication on the server is the same as that on the client. Besides, the client and the server must be configured with the same authentication key.

Configuring Optional NTP Parameters

Table 293 Optional NTP parameters configuration tasks

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

Table 294 Configure an interface on the local switch to send NTP messages

Operation	Command	Description
Enter system view	system-view	-
Configure an interface on the local switch to send NTP messages	ntp-service source-interface Vlan-interface <i>vlan-id</i>	Required



CAUTION: *If you have specified an interface in the **ntp-service unicast-server** or **ntp-service unicast-peer** command, this interface will be used for sending NTP messages.*

Configuring the Number of Dynamic Sessions Allowed on the Local Switch

A single device can have a maximum of 128 associations at the same time, including static associations and dynamic associations. A static association refers to an association that a user has manually created by using an NTP command, while a dynamic association is a temporary association created by the system during operation. A dynamic association will be removed if the system fails to receive messages from it over a specific long time. In the server/client mode, for example, when you carry out a command to synchronize the time to a server, the system will create a static association, and the server will just respond passively

upon the receipt of a message, rather than creating an association (static or dynamic). In the symmetric mode, static associations will be created at the symmetric-active peer side, and dynamic associations will be created at the symmetric-passive peer side; In the broadcast or multicast mode, static associations will be created at the server side, and dynamic associations will be created at the client side.

Table 295 Configure the number of dynamic sessions allowed on the local switch

Operation	Command	Description
Enter system view	system-view	-
Configure the maximum number of dynamic sessions that can be established on the local switch	ntp-service max-dynamic-sessions <i>number</i>	Required By default, up to 100 dynamic sessions can be established locally.

Disabling an Interface from Receiving NTP messages

Table 296 Disable an interface from receiving NTP messages

Operation	Command	Description
Enter system view	system-view	-
Enter VLAN interface view	interface <i>Vlan-interface</i> <i>vlan-id</i>	-
Disable an interface from receiving NTP messages	ntp-service in-interface disable	Required By default, a VLAN interface receives NTP messages.

Displaying NTP Configuration

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

Table 297 Display NTP configuration

Operation	Command	Description
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 Example

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 (a Switch 4210)

- Configure Device B to work in the client mode, and then Device A will automatically work in the server mode.

Network diagram

Figure 114 Network diagram for the NTP server/client mode configuration



Configuration procedure

Perform the following configurations on Device B.

View the NTP status of Device B before synchronization.

```

<DeviceB> display ntp-service status
Clock status: unsynchronized
Clock stratum: 16
Reference clock ID: none
Nominal frequency: 100.0000 Hz
Actual frequency: 100.0000 Hz
Clock precision: 2^18
Clock offset: 0.0000 ms
Root delay: 0.00 ms
Root dispersion: 0.00 ms
Peer dispersion: 0.00 ms
Reference time: 00:00:00.000 UTC Jan 1 1900 (00000000.00000000)
  
```

Set Device A as the NTP server of Device B.

```

<DeviceB> system-view
[DeviceB] ntp-service unicast-server 1.0.1.11
  
```

(After the above configurations, Device B is synchronized to Device A.) View the NTP status of Device B.

```

[DeviceB] display ntp-service status
Clock status: synchronized
Clock stratum: 3
Reference clock ID: 1.0.1.11
Nominal frequency: 100.0000 Hz
Actual frequency: 100.0000 Hz
Clock precision: 2^18
Clock offset: 0.66 ms
Root delay: 27.47 ms
Root dispersion: 208.39 ms
Peer dispersion: 9.63 ms
Reference time: 17:03:32.022 UTC Thu 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
```

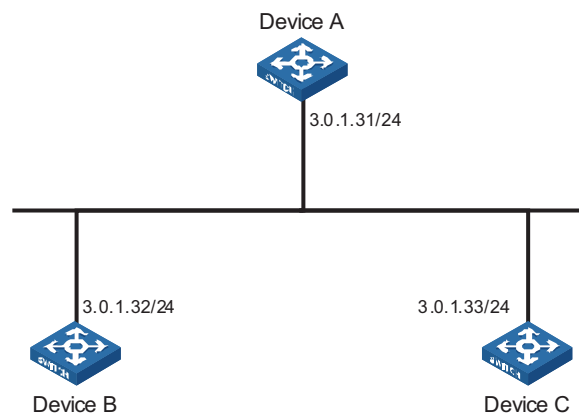
Configuring NTP Symmetric Peer Mode

Network requirements

- The local clock of Device A is set as the NTP master clock, with the clock stratum level of 2.
- Device C (a Switch 4210) 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 115 Network diagram for NTP peer mode configuration



Configuration procedure

1 Configure Device C.

Set Device A as the NTP server.

```
<DeviceC> system-view
[DeviceC] ntp-service unicast-server 3.0.1.31
```

2 Configure Device B (after the Device C is synchronized to Device A).

Enter system view.

```
<DeviceB> system-view
# Set Device C as the peer of Device B.
[DeviceB] ntp-service unicast-peer 3.0.1.33
```

Device C and Device B are symmetric peers after the above configuration. Device B works in symmetric active mode, while Device C works in symmetric passive mode. Because the stratum level of the local clock of Device B is 1, and that of Device C is 3, the clock of Device C is synchronized to that of Device B.

View the status of Device C after the clock synchronization.

```
[DeviceC] display ntp-service status
Clock status: synchronized
```

```

Clock stratum: 2
Reference clock ID: 3.0.1.32
Nominal frequency: 100.0000 Hz
Actual frequency: 100.0000 Hz
Clock precision: 2^18
Clock offset: 0.66 ms
Root delay: 27.47 ms
Root dispersion: 208.39 ms
Peer dispersion: 9.63 ms
Reference time: 17:03:32.022 UTC Thu 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

```

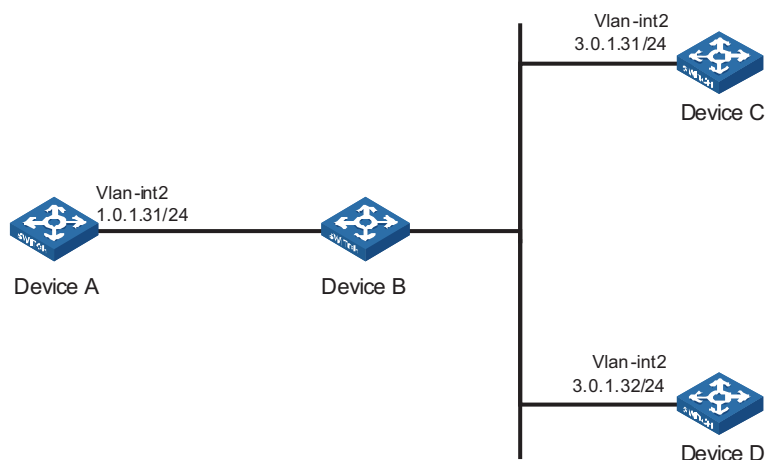
Configuring NTP Broadcast Mode

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-interface2.
- Device A and Device D are two Switch 4210s. Configure Device A and Device D to work in the NTP broadcast client mode and listen to broadcast messages through their own Vlan-interface2.

Network diagram

Figure 116 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-interface2.
```

```
[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-interface2, and Device C will send broadcast messages through Vlan-interface2. Because Device A and Device C do not share the same network segment, Device A cannot receive broadcast messages from Device C, while Device D is synchronized to Device C after receiving broadcast messages from Device C.

View the NTP status of Device D after the clock synchronization.

```
[DeviceD] display ntp-service status
Clock status: synchronized
Clock stratum: 3
Reference clock ID: 3.0.1.31
Nominal frequency: 100.0000 Hz
Actual frequency: 100.0000 Hz
Clock precision: 2^18
Clock offset: 198.7425 ms
Root delay: 27.47 ms
Root dispersion: 208.39 ms
Peer dispersion: 9.63 ms
Reference time: 17:03:32.022 UTC Thu 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
```

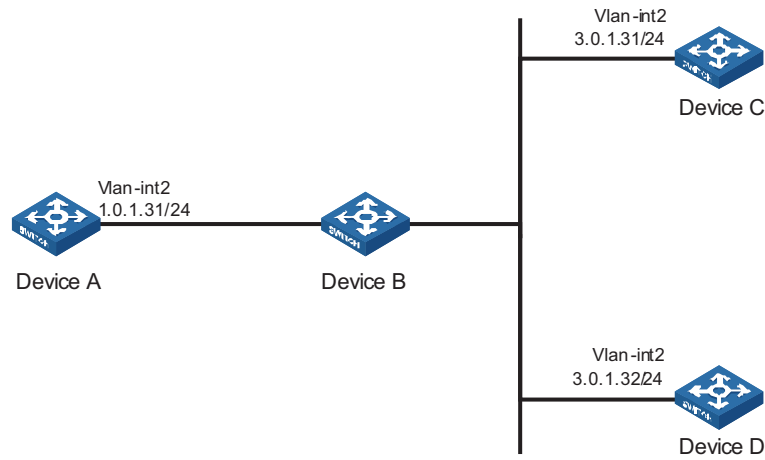
Configuring NTP Multicast Mode

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-interface2.
- Device A and Device D are two Switch 4210s. Configure Device A and Device D to work in the NTP multicast client mode and listen to multicast messages through their own Vlan-interface2.

Network diagram

Figure 117 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-interface2.

```
[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-interface2.

```
[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-interface2, and Device C advertises multicast messages through Vlan-interface2. Because Device A and Device C do not share the same network segment, Device A cannot receive multicast messages from Device C, while Device D is synchronized to Device C after receiving multicast messages from Device C.

View the NTP status of Device D after the clock synchronization.

```
[DeviceD] display ntp-service status
Clock status: synchronized
Clock stratum: 3
Reference clock ID: 3.0.1.31
Nominal frequency: 100.0000 Hz
Actual frequency: 100.0000 Hz
Clock precision: 2^18
Clock offset: 198.7425 ms
Root delay: 27.47 ms
```

```

Root dispersion: 208.39 ms
Peer dispersion: 9.63 ms
Reference time: 17:03:32.022 UTC Thu 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 To
tal associations : 1

```

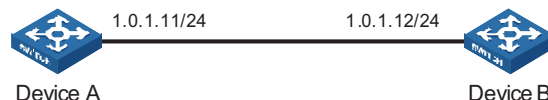
Configuring NTP Server/Client Mode with Authentication

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 a Switch 4210 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 118 Network diagram for NTP server/client mode with authentication configuration



Configuration procedure

1 Configure Device B.

Enter system view.

```
<DeviceB> system-view
```

Enable the NTP authentication function.

```
[DeviceB] ntp-service authentication enable
```

Configure an MD5 authentication key, with the key ID being **42** and the key being **aNiceKey**.

```
[DeviceB] ntp-service authentication-keyid 42 authentication-mode md5 aNiceKey
```

Specify the key 42 as a trusted key.

```
[DeviceB] ntp-service reliable authentication-keyid 42
```

Associate the trusted key with the NTP server (Device A).

```
[DeviceB] ntp-service unicast-server 1.0.1.11 authentication-keyid 42
```

After the above configurations, Device B is ready to synchronize with Device A. Because the NTP authentication function is not enabled on Device A, the clock of Device B will fail to be synchronized to that of Device A.

- 2 To synchronize Device B, you need to perform the following configurations on Device A.

Enable the NTP authentication function.

```
[DeviceA] system-view
[DeviceA] ntp-service authentication enable
```

Configure an MD5 authentication key, with the key ID being **42** and the key being **aNiceKey**.

```
[DeviceA] ntp-service authentication-keyid 42 authentication-mode md5 aNiceKey
```

Specify the key 42 as a trusted key.

```
[DeviceA] ntp-service reliable authentication-keyid 42
```

(After the above configurations, the clock of Device B can be synchronized to that of Device A.) View the status of Device B after synchronization.

```
[DeviceB] display ntp-service status
Clock status: synchronized
Clock stratum: 3
Reference clock ID: 1.0.1.11
Nominal frequency: 100.0000 Hz
Actual frequency: 100.1000 Hz
Clock precision: 2^18
Clock offset: 0.66 ms
Root delay: 27.47 ms
Root dispersion: 208.39 ms
Peer dispersion: 9.63 ms
Reference time: 17:03:32.022 UTC Thu 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 of 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
```


36

SSH CONFIGURATION

SSH Overview

Introduction to SSH

Secure Shell (SSH) is a protocol that provides secure remote login and other security services in insecure network environments. 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. Besides, SSH also provides powerful user authentication functions that prevent attacks such as DNS and IP spoofing.

SSH adopts the client-server model. The device can be configured as an SSH client or an SSH server. In the former case, the device establishes a remote SSH connection to an SSH server. In the latter case, the device provides connections to multiple clients.

Furthermore, SSH can also provide data compression to increase transmission speed, take the place of Telnet or provide a secure "channel" for FTP.

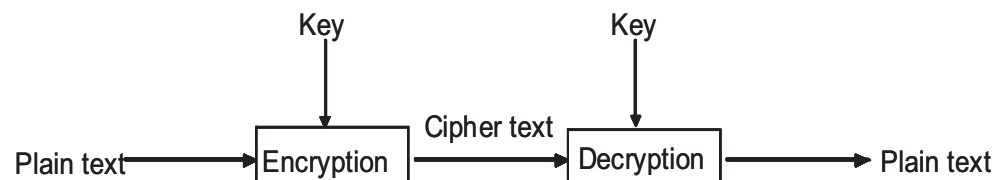


CAUTION: Currently, the Switch 4210 device supports only SSH2. when functioning as either an SSH client or an SSH server. Unless otherwise noted, SSH refers to SSH2 throughout this document.

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 119 Encryption and decryption



Key-based algorithm is usually classified into symmetric key algorithm and asymmetric key algorithm.

Asymmetric Key Algorithm

Asymmetric key algorithm means that a key pair exists at both ends. The key pair consists of a private key and a public key. The public key is effective for both ends,

while the private key is effective only for the local end. Normally you cannot use the private key through the 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, SSH supports both RSA and DSA.

SSH Operating Process

The session establishment between an SSH client and the SSH server involves the following five stages:

Table 298 Stages in establishing a session between the SSH client and server

Stages	Description
Version negotiation	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.

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.



- All the packets above are transferred in plain text.

Key negotiation

- The server and the client send algorithm negotiation packets to each other, which contain public key algorithm lists supported by the server and the client, encrypted algorithm list, message authentication code (MAC) algorithm list, and compressed algorithm list.
- The server and the client calculate the final algorithm according to the algorithm lists supported.
- The server and the client generate the session key and session ID based on the Diffie-Hellman (DH) exchange algorithm and the host key pair.
- Then, the server and the client get the same session key and use it for data encryption and decryption to secure data communication.

Authentication negotiation

The negotiation steps are as follows:

- The client sends an authentication request to the server. The authentication request contains username, authentication type, and authentication-related information. For example, if the authentication type is **password**, the content is the password.
- The server starts to authenticate the user. If authentication fails, the server sends an authentication failure message to the client, which contains the list of methods used for a new authentication process.
- The client selects an authentication type from the method list to perform authentication again.
- The above process repeats until the authentication succeeds, or the connection is torn down when the authentication times reach the upper limit.

SSH provides two authentication methods: password authentication and publickey authentication.

- In password authentication, the client encrypts the username and password, encapsulates them into a password authentication request, and sends the request to the server. Upon receiving the request, the server decrypts the username and password, compares them with those it maintains, and then informs the client of the authentication result.
- The publickey authentication method authenticates clients using digital signatures. Currently, the device supports two publickey algorithms to implement digital signatures: RSA and DSA. The client sends to the server a publickey authentication request containing its user name, public key and algorithm. The server verifies the public key. If the public key is invalid, the authentication fails; otherwise, the server generates a digital signature to authenticate the client, and then sends back a message to inform the success or failure of the authentication.?

Session request

After passing authentication, the client sends a session request to the server, while the server listens to and processes the request from the client. If the client passes authentication, the server sends back to the client an SSH_MSG_SUCCESS packet

and goes on to the interactive session stage with the client. Otherwise, the server sends back to the client an `SSH_MSG_FAILURE` packet, indicating that the processing fails or it cannot resolve the request. The client sends a session request to the server, which processes the request and establishes a session.

Data exchange

In this stage, the server and the client exchanges data in this way:

- The client encrypts and sends the command to be executed to the server.
- The server decrypts and executes the command, and then encrypts and sends the result to the client.
- The client decrypts and displays the result on the terminal.

Configuring the SSH Server

You must perform necessary configurations on the SSH server for SSH clients to access.

SSH Server Configuration Tasks

Table 299 SSH server configuration tasks

Tasks	Description
Configuring the SSH server	Configuring the Protocol Support for the User Interface Generating/Destroying a RSA or DSA Key Pair Exporting the RSA or DSA Public Key Creating an SSH User and Specify an Authentication Type Specifying a Service Type for an SSH User Configuring SSH Management
	Required Required Optional Required Optional Optional
	Configuring the Client Public Key on the Server
	Required for publickey authentication; unnecessary for password authentication
	Assigning a Public Key to an SSH User
	Required for publickey authentication; unnecessary for password authentication

Configuring the Protocol Support for the User Interface

You must configure the supported protocol(s) for SSH remote login. Note that the configuration does not take effect immediately, but will be effective for subsequent login requests.

Table 300 Configure the protocol(s) that a user interface supports

Operation	Command	Description
Enter system view	system-view	-
Enter the view of one or multiple user interfaces	user-interface [<i>type</i>] <i>first-number</i> [<i>last-number</i>]	-
Configure the authentication mode as scheme	authentication-mode scheme [command-authorization]	Required By default, the user interface authentication mode is password

Table 300 Configure the protocol(s) that a user interface supports

Operation	Command	Description
Specify the supported protocol(s)	protocol inbound { all ssh telnet }	Optional By default, both Telnet and SSH are supported.

**CAUTION:**

- If you have configured a user interface to support SSH protocol, 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.

Generating/Destroying a RSA or DSA Key Pair

This configuration task lets you generate or destroy a key pair. You must generate an RSA or DSA key pair on the server for an SSH client to log in successfully. When generating a key pair, you will be prompted to enter the key length in bits, which is between 512 and 2048. In case a key pair already exists, the system will ask whether to replace the existing key pair.

Table 301 Create or destroy a key pair

Operation	Command	Remarks
Enter system view	system-view	
Generate an RSA key pair	rsa local-key-pair create public-key local create rsa	Required Use either command By default, no RSA key pair is created.
Destroy the RSA key pair	rsa local-key-pair destroy public-key local destroy rsa	Optional Use either command to destroy the configured RSA key pair.
Generate a DSA key pair	public-key local create dsa	Required By default, no DSA key pair is created.
Destroy the DSA key pair	public-key local destroy dsa	Optional Use the command to destroy the configured DSA key pair.



- The command for generating a key pair can survive a reboot. You only need to configure it once.
- Some third-party software, for example, WinSCP, requires that the modulo of a public key be greater than or equal to 768. Therefore, a local key pair of more than 768 bits is recommended.

Exporting the RSA or DSA Public Key

You can display the generated RSA or DSA key pair on the screen in a specified format, or export it to a specified file for configuring the key at a remote end.

Table 302 Export the RSA public key

Operation	Command	Remarks
Enter system view	system-view	
Display the RSA key on the screen in a specified format or export it to a specified file	public-key local export rsa { openssh ssh1 ssh2 } [<i>filename</i>]	Required

Table 303 Export the DSA public key

Operation	Command	Remarks
Enter system view	system-view	
Display the DSA key on the screen in a specified format or export it to a specified file	public-key local export dsa { openssh ssh2 } [<i>filename</i>]	Required



The DSA public key format can be SSH2 and OpenSSH, while the RSA public key format can be SSH1, SSH2 and OpenSSH.

Creating an SSH User and Specify an Authentication Type

This task is to create an SSH user and specify an authentication type for it. Specifying an authentication type for a new user is a must to get the user login.

Table 304 Configure an SSH user and specify an authentication type for it

Operation	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 rsa }	Use either command. By default, no SSH user is created and no authentication type is specified.
Create an SSH user, and specify an authentication type for it	ssh user <i>username</i> ssh user <i>username</i> authentication-type { all password password-publickey publickey rsa }	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.

**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.

- Both **publickey** and **rsa** indicate public key authentication. They are implemented with the same method.
- 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

Table 305 Specify the service type of an SSH user:

Operation	Command	Remarks
Enter system view	system-view	-
Specify a service type for an SSH user	ssh user <i>username</i> service-type { stelnet sftp all }	Required stelnet by default



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 SSH Management

The SSH server provides a number of management functions that prevent illegal operations such as malicious password guess, to further guarantee the security of SSH connections.

Table 306 Configure SSH management

Operation	Command	Description
Enter system view	system-view	-
Set SSH authentication timeout time	ssh server timeout <i>seconds</i>	Optional By default, the timeout time is 60 seconds.
Set SSH authentication retry times	ssh server authentication-retries <i>times</i>	Optional By default, the number of retry times is 3.
Configure a login header	header shell <i>text</i>	Optional By default, no login header is configured.



CAUTION:

- You can configure a login header only when the service type is **stelnet**. For configuration of service types, see “Specifying a Service Type for an SSH User”.

- For details of the **header** command, see the corresponding section in *Login Command*.

Configuring the Client Public Key on the Server



*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.

Table 307 Configure the client's public key manually

Operation	Command	Description
Enter system view	system-view	
Enter public key view	public-key peer <i>keyname</i>	Required
Enter public key edit view	public-key-code begin	
Configure a public key for the client	Enter the content of the public key	When you input the key data, spaces are allowed between the characters you input (because the system can remove the spaces automatically); you can also press <Enter> to continue your input at the next line. But the key you input should be a hexadecimal digit string coded in the public key format.
Return to public key view from public key edit view	public-key-code end	-
Exit public key view and return to system view	peer-public-key end	-

Table 308 Import the public key from a public key file

Operation	Command	Description
Enter system view	system-view	-
Import the public key from a public key file	public-key peer <i>keyname</i> import sshkey <i>filename</i>	Required

You can also use the following commands to configure the client's RSA public key on the server.

Table 309 Configure the client RSA public key manually

Operation	Command	Description
Enter system view	system-view	
Enter public key view	rsa peer-public-key <i>keyname</i>	Required
Enter public key edit view	public-key-code begin	
Configure the client RSA public key	Enter the content of the RSA public key	The content must be a hexadecimal string that is generated randomly by the SSH-supported client software and coded compliant to PKCS. Spaces and carriage returns are allowed between characters.
Return from public key code view to public key view	public-key-code end	When you exit public key code view, the system automatically saves the public key.
Return from public key view to system view	peer-public-key end	



The result 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 result of the **display public-key local rsa public** command be used in the **rsa peer-public-key** command directly.

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.

Table 310 Assign a public key for an SSH user

Operation	Command	Remarks
Enter system view	system-view	
Assign a public key to an SSH user	ssh user <i>username</i> assign { publickey rsa-key } <i>keyname</i>	Required If you issue this command multiple times, the last command overrides the previous ones.



Both the keywords **publickey** and **rsa-key** represent the public key, and have the same implementation.

Configuring the SSH Client

An SSH client software or SSH2-capable switch can serve as an SSH client to access the SSH server.

SSH Client Configuration Tasks

Table 311 SSH client configuration tasks

Tasks	Description
Configuring the SSH client	Using an SSH client software On an SSH2-capable switch

Configuring the SSH Client Using an 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:

Table 312 Configuration tasks for using a client software

Tasks	Description
"Generate a client key"	Required for publickey authentication; unnecessary for password authentication
"Specify the IP address of the Server"	Required
"Select a protocol for remote connection"	Required
"Select an SSH version"	Required
"Open an SSH connection with publickey authentication"	Required for publickey authentication; unnecessary for password authentication
"Open an SSH connection with password authentication"	Required for publickey authentication; unnecessary for password authentication

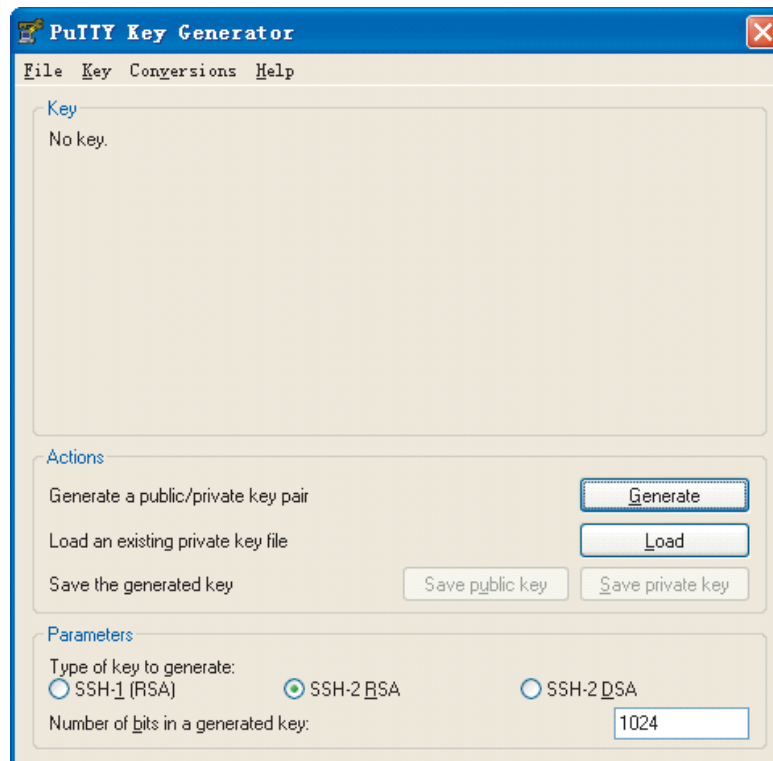


- Selecting the protocol for remote connection as SSH. Usually, a client can use a variety of remote connection protocols, such as Telnet, Rlogin, and SSH. To establish an SSH connection, you must select SSH
- When a Switch 4210 acts as the SSH server, select 2.0 for the clients.
- Specifying the private 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, PuTTYGen and SSHKEY as examples to illustrate how to configure the SSH client:

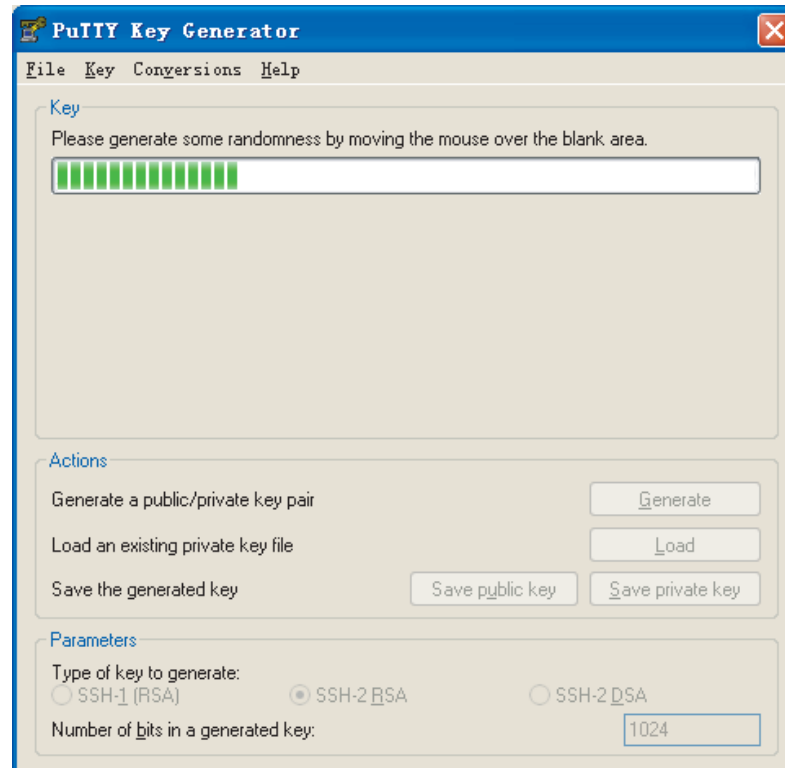
Generate a client key

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 120 Generate a client key (1)

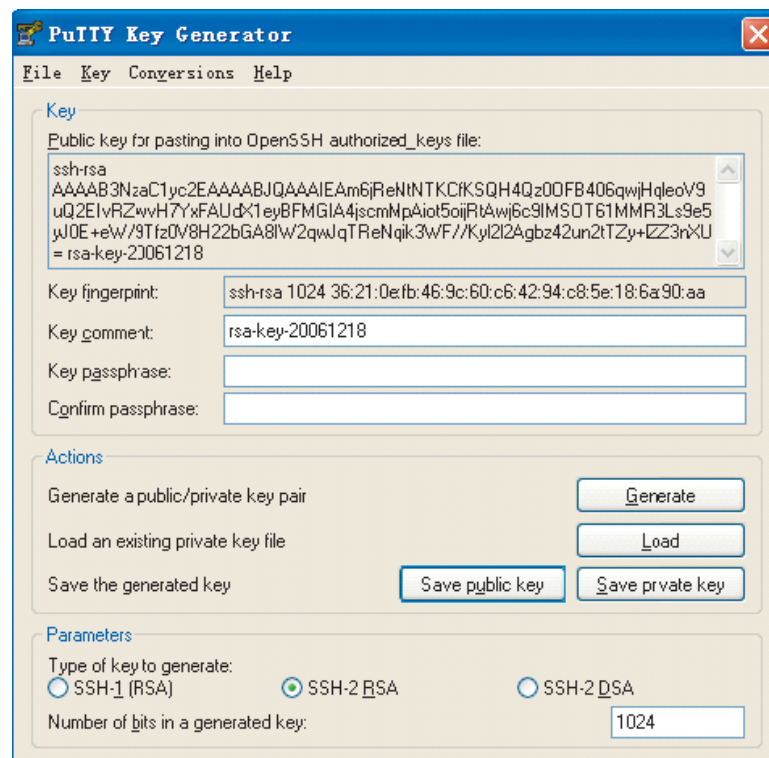
Note that while generating the key pair, you must move the mouse continuously and keep the mouse off the green process bar in the blue box of shown in Figure 121. Otherwise, the process bar stops moving and the key pair generating process is stopped.

Figure 121 Generate the client keys (2)



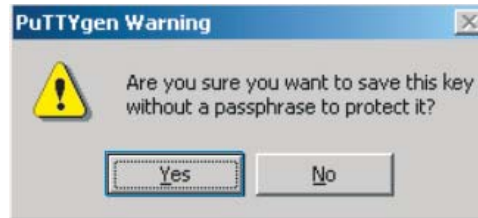
After the key pair is generated, click **Save public key** and enter the name of the file for saving the public key (**public** in this case) to save the public key.

Figure 122 Generate the client keys (3)



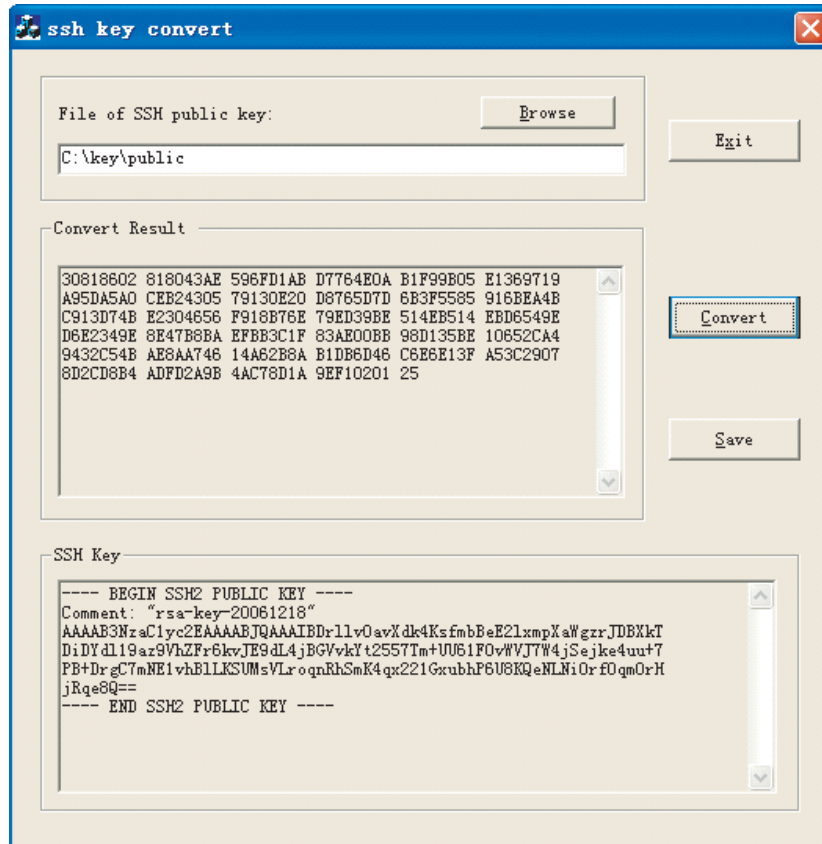
Likewise, to save the private key, click **Save private key**. A warning window pops up to prompt you whether to save the private key without any precaution. Click **Yes** and enter the name of the file for saving the private key ("private" in this case) to save the private key.

Figure 123 Generate the client keys (4)



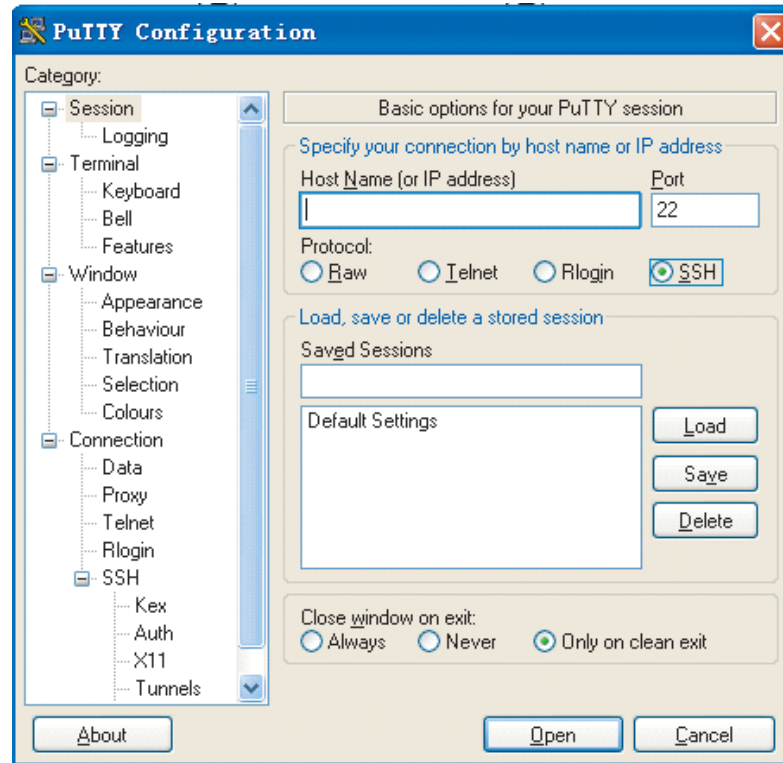
To generate RSA public key in PKCS format, run SSHKEY.exe, click **Browse** and select the public key file, and then click **Convert**.

Figure 124 Generate the client keys (5)



Specify the IP address of the Server

Launch PuTTY.exe. The following window appears.

Figure 125 SSH client configuration interface 1

In the **Host Name (or IP address)** text box, enter the IP address of the server. Note that there must be a route available between the IP address of the server and the client.

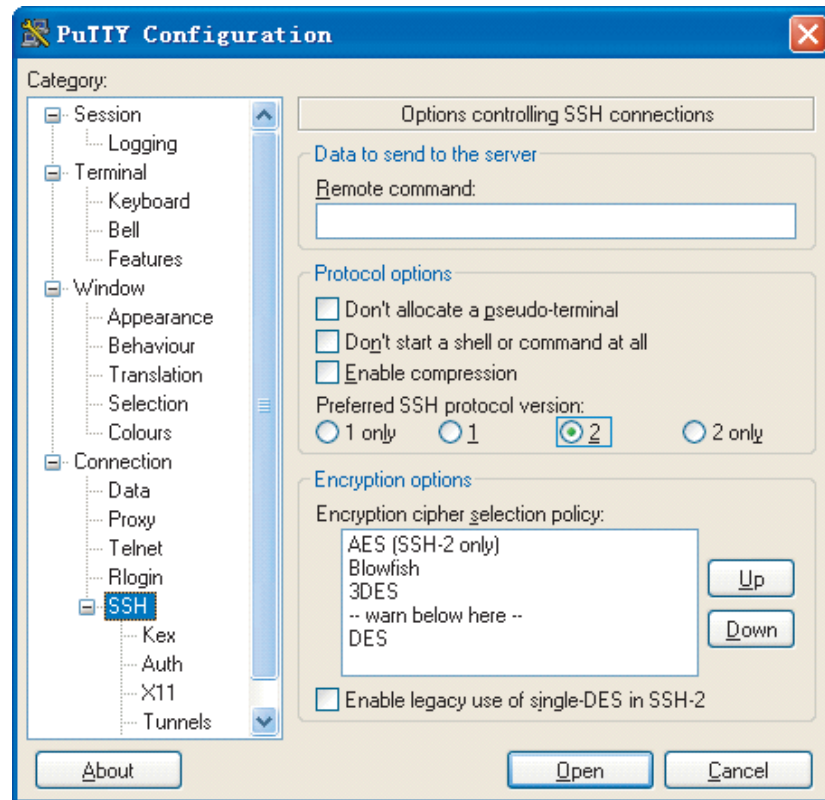
Select a protocol for remote connection

As shown in Figure 125, select **SSH** under **Protocol**.

Select an SSH version

From the category on the left pane of the window, select **SSH** under **Connection**. The window as shown in Figure 126 appears.

Figure 126 SSH client configuration interface 2



Under **Protocol options**, select **2** from **Preferred SSH protocol version**.

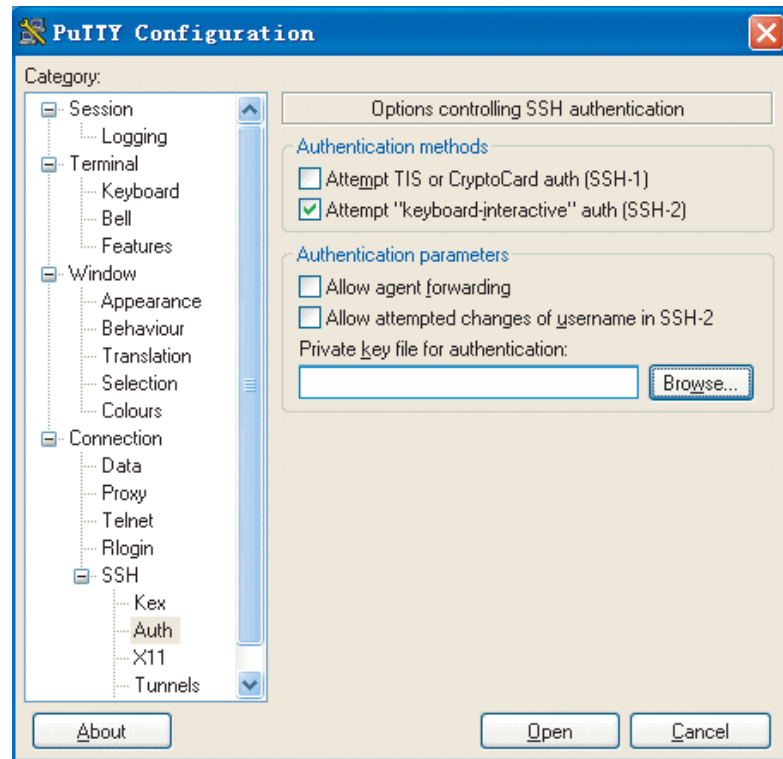


Some SSH client software, for example, Tectia client software, supports the DES algorithm only when the ssh1 version is selected. The PuTTY client software supports DES algorithm negotiation ssh2.

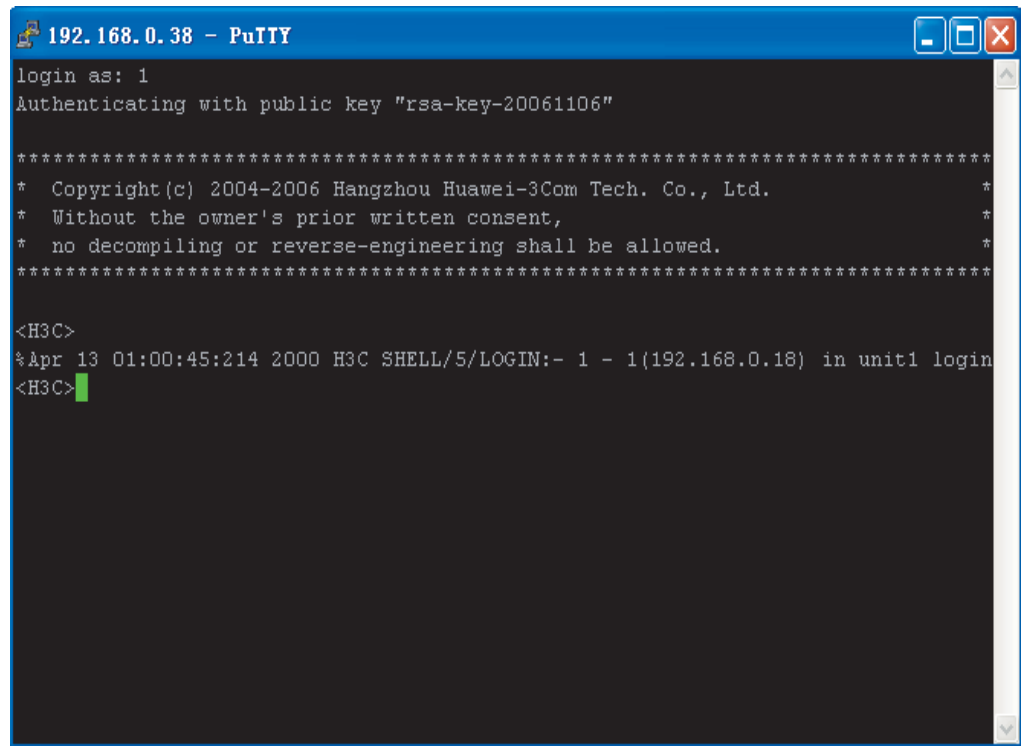
Open an SSH connection with publickey authentication

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 127 SSH client configuration interface 3

Click **Browse...** to bring up the file selection window, navigate to the private key file and click **Open** to enter the following SSH client interface. If the connection is normal, a user will be prompted for a username. Once passing the authentication, the user can log onto the server.

Figure 128 SSH client interface (1)

```
192.168.0.38 - PuTTY
login as: 1
Authenticating with public key "rsa-key-20061106"

*****
* Copyright(c) 2004-2006 Hangzhou Huawei-3Com Tech. Co., Ltd. *
* Without the owner's prior written consent, *
* no decompiling or reverse-engineering shall be allowed. *
*****

<H3C>
%Apr 13 01:00:45:214 2000 H3C SHELL/5/LOGIN:- 1 - 1(192.168.0.18) in unit1 login
<H3C>
```

Open an SSH connection with password authentication

From the window shown in Figure 127, click Open. The following SSH client interface appears. If the connection is normal, you will be prompted to enter the username and password, as shown in Figure 129.

Figure 129 SSH client interface (2)

```

192.168.0.90 - PuTTY
login as: 1
1@192.168.0.90's password:

*****
* Copyright (c) 2004-2006 Hangzhou Huawei-3Com Tech. Co., Ltd.
* Without the owner's prior written consent,
* no decompiling or reverse-engineering shall be allowed.
*****

<H3C>
%Apr 2 02:08:13:391 2000 H3C SHELL/5/LOGIN:- 1 - 1(192.168.0.18) in unit1 login
<H3C>

```

Enter the username and password to establish an SSH connection.

To log out, enter the **quit** command.

Configuring the SSH Client on an SSH2-Capable Switch

Table 313 Configuration tasks when an SSH2-capable switch is used as the client

Tasks	Description
"Configure whether first-time authentication is supported"	Optional
Establish the connection between the SSH client and server	Required

Configure 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.

- First-time authentication means that when the SSH client accesses the server for the first time and is not configured with the server host public key, the user can continue accessing the server, and will save the host public key on the client for use in subsequent authentications.
- When first-time authentication is not supported, a client, if 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.

Table 314 Enable the device to support first-time authentication

Operation	Command	Description
Enter system view	system-view	
Enable the device to support first-time authentication	ssh client first-time enable	Optional By default, the client is enabled to run initial authentication.

Table 315 Disable first-time authentication support

Operation	Command	Description
Enter system view	system-view	
Disable first-time authentication support	undo ssh client first-time	Required By default, the client is enabled to run first-time authentication.
Configure server public key	Refer to “Configuring the Client Public Key on the Server” on page 394	Required The method of configuring server public key on the client is similar to that of configuring client public key on the server.
Specify the host key name of the server	ssh client { <i>server-ip</i> <i>server-name</i> } assign { publickey rsa-key } <i>keyname</i>	Required

Establish 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. See Table 316 for details.

Table 316 Establish an SSH connection

Operation	Command	Description
Enter system view	system-view	
Start the client to establish a connection with an SSH server	ssh2 { <i>host-ip</i> <i>host-name</i> } [<i>port-num</i>] [identity-key { dsa rsa }] [prefer_kex { dh_group1 dh_exchange_group }] [prefer_ctos_cipher { des aes128 }] [prefer_stoc_cipher { des aes128 }] [prefer_ctos_hmac { sha1 sha1_96 md5 md5_96 }] [prefer_stoc_hmac { sha1 sha1_96 md5 md5_96 }] *	Required In this command, you can also specify the preferred key exchange algorithm, encryption algorithms and HMAC algorithms between the server and client. HMAC: Hash-based message authentication code Note that: The identity-key keyword is unnecessary in password authentication and optional in public key authentication.



When logging into the SSH server using public key authentication, an SSH client needs to read the 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 SSH Configuration

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

Table 317 Display SSH configuration

Operation	Command	Description
Display host and server public keys	display rsa local-key-pair public	You can execute the display command in any view.
Display client RSA public key(s)	display rsa peer-public-key [brief name <i>keyname</i>]	
Display local public key(s)	display public-key local { dsa rsa } public	
Display remote public key(s)	display public-key peer [brief name <i>pubkey-name</i>]	
Display SSH status and session information	display ssh server { session status }	
Display SSH user information	display ssh user-information [<i>username</i>]	
Display the mappings between host public keys and SSH servers saved on a client	display ssh server-info	

SSH Configuration Examples

When the Switch Acts as the SSH Server and the Authentication Type is Password

Network requirements

As shown in Figure 130, 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 130 Network diagram of SSH server configuration using 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.

```

<4210> system-view
[4210] interface vlan-interface 1
[4210-Vlan-interface1] ip address 192.168.0.1 255.255.255.0
[4210-Vlan-interface1] quit
  
```



Generating the RSA and DSA key pairs on the server is prerequisite to SSH login.

```
# Generate RSA and DSA key pairs.
[4210] public-key local create rsa
[4210] public-key local create dsa

# Set the authentication mode for the user interfaces to AAA.
[4210] user-interface vty 0 4
[4210-ui-vty0-4] authentication-mode scheme

# Enable the user interfaces to support SSH.
[4210-ui-vty0-4] protocol inbound ssh
[4210-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.
[4210] local-user client001
[4210-luser-client001] password simple abc
[4210-luser-client001] service-type ssh level 3
[4210-luser-client001] quit

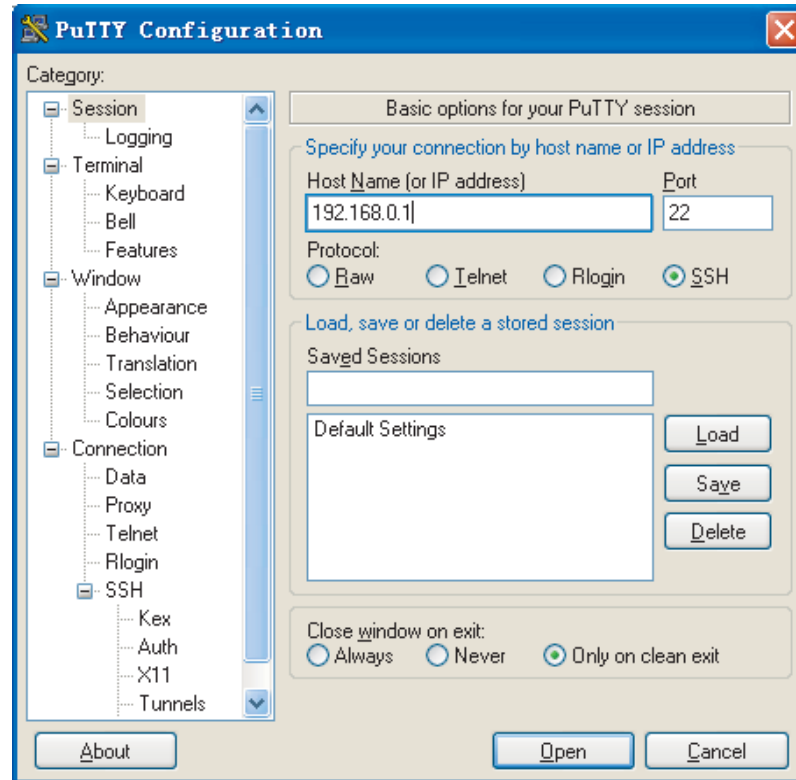
# Specify the authentication method of user client001 as password.
[4210] ssh user client001 authentication-type password
```

- 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.

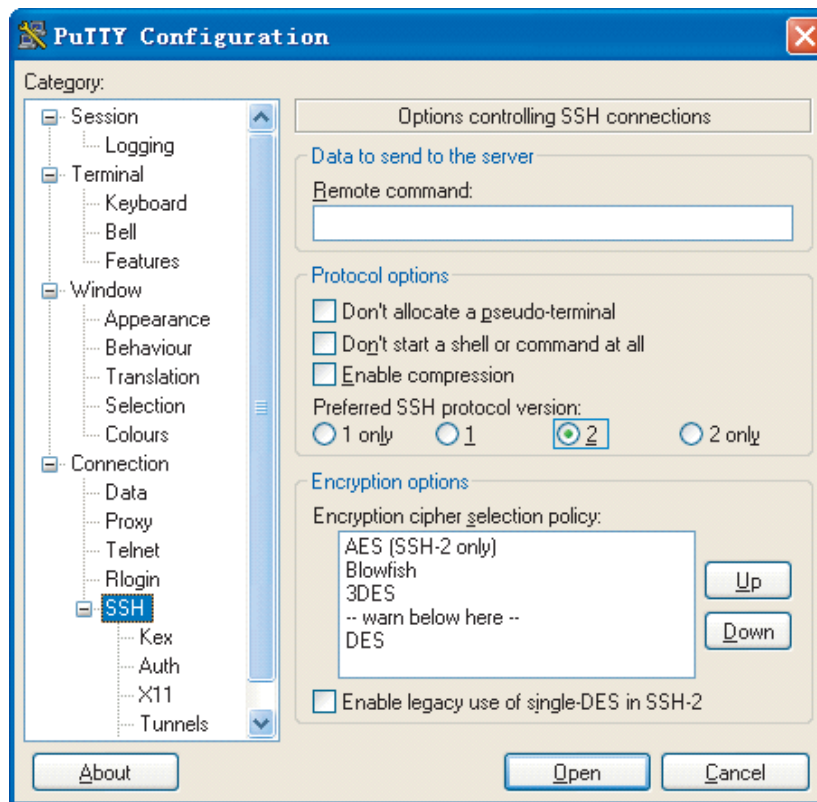
Figure 131 SSH client configuration interface



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 132 appears.

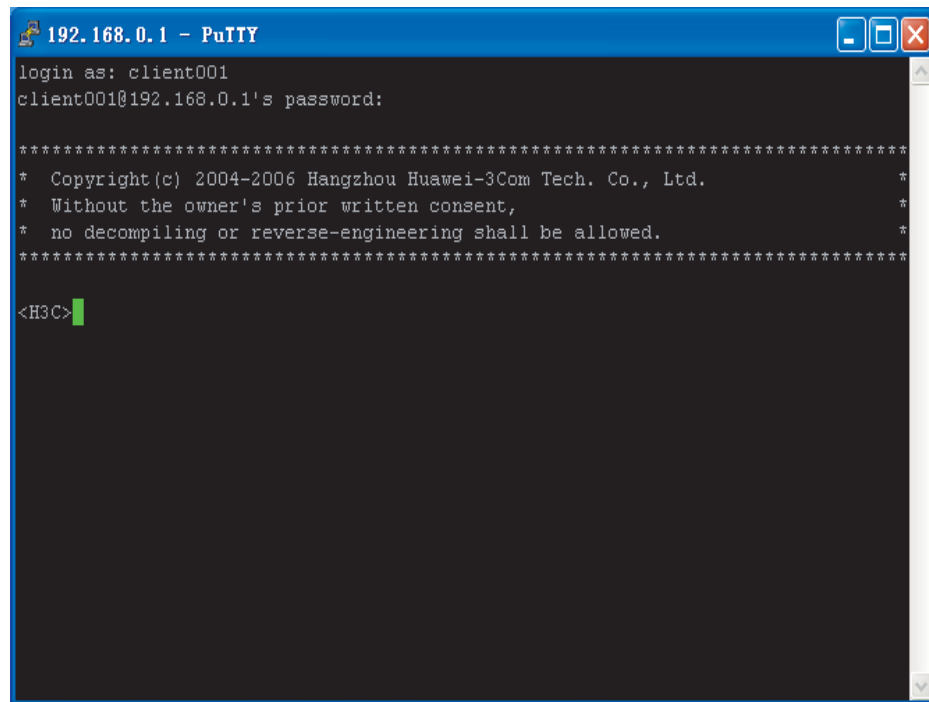
Figure 132 SSH client configuration interface 2



Under **Protocol options**, select **2** from **Preferred SSH protocol version**.

- As shown in Figure 131, click **Open** to enter the following interface. If the connection is normal, you will be prompted to enter the user name "client001" and password "abc". Once authentication succeeds, you will log onto the server.

Figure 133 SSH client interface



When the Switch Acts as an SSH Server and the Authentication Type is Publickey

Network requirements

As shown in Figure 134, 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 134 Network diagram of SSH server configuration



Configuration procedure



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.

```

<4210> system-view
[4210] interface vlan-interface 1
[4210-Vlan-interface1] ip address 192.168.0.1 255.255.255.0
[4210-Vlan-interface1] quit
  
```



Generating the RSA and DSA key pairs on the server is prerequisite to SSH login.


```

# Generate RSA and DSA key pairs.
[4210] public-key local create rsa
[4210] public-key local create dsa

# Set the authentication mode for the user interfaces to AAA.
[4210] user-interface vty 0 4
[4210-ui-vty0-4] authentication-mode scheme

# Enable the user interfaces to support SSH.
[4210-ui-vty0-4] protocol inbound ssh

# Set the client's command privilege level to 3
[4210-ui-vty0-4] user privilege level 3
[4210-ui-vty0-4] quit

# Configure the authentication type of the SSH client named client 001 as
publickey.
[4210] ssh user client001 authentication-type publickey

```



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 "Configuring the SSH Client" on page 396.

```

# Import the client's public key named "Switch001" from file "public".
[4210] public-key peer Switch001 import sshkey public

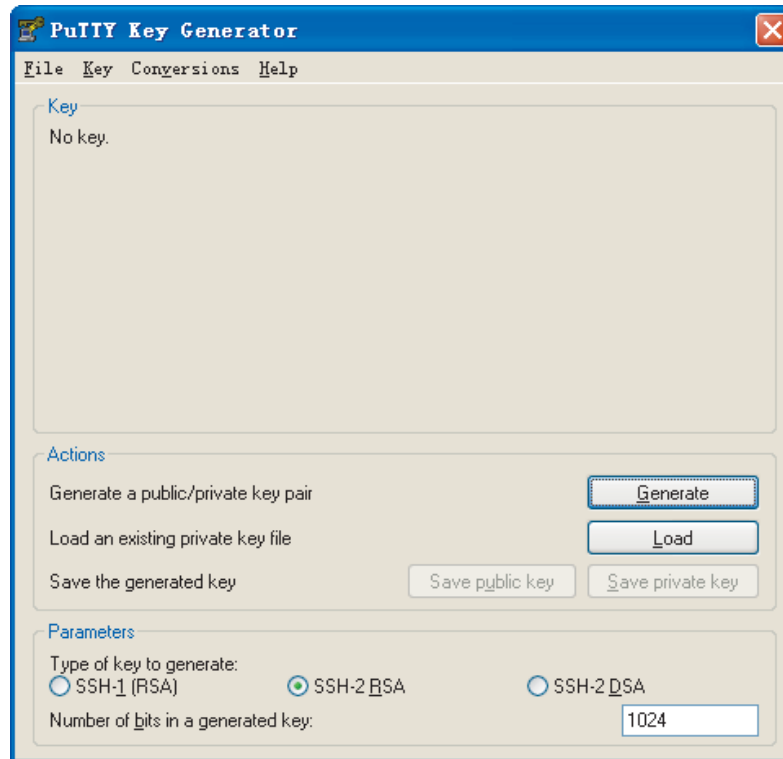
# Assign the public key "Switch001" to client "client001".
[4210] ssh user client001 assign publickey Switch001

```

- Configure the SSH client

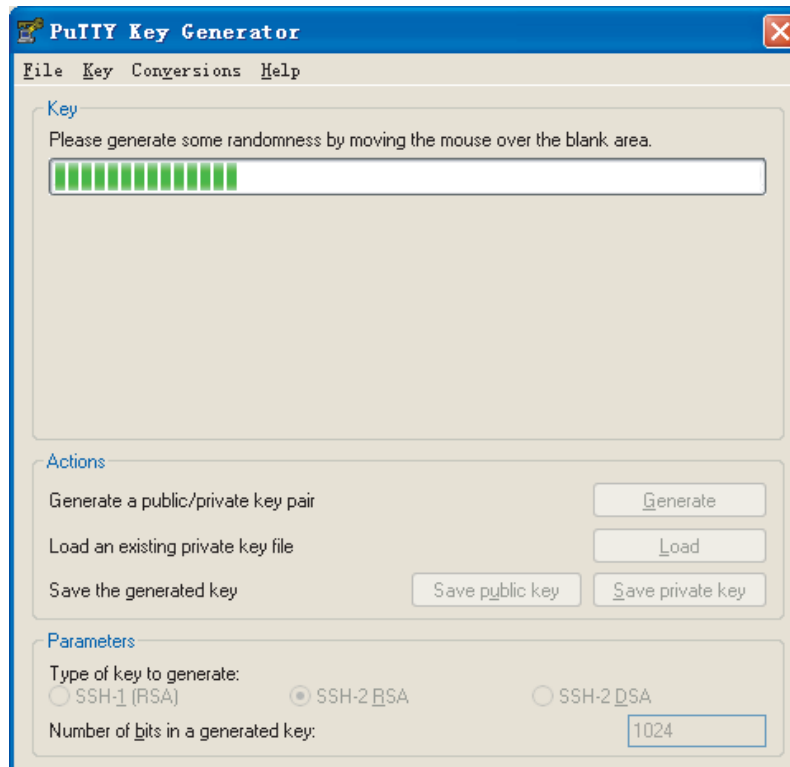
- # Generate an RSA key pair, taking PuTTYGen as an example.
- 1 Run PuTTYGen.exe, choose **SSH2(RSA)** and click **Generate**.

Figure 135 Generate a client key pair (1)



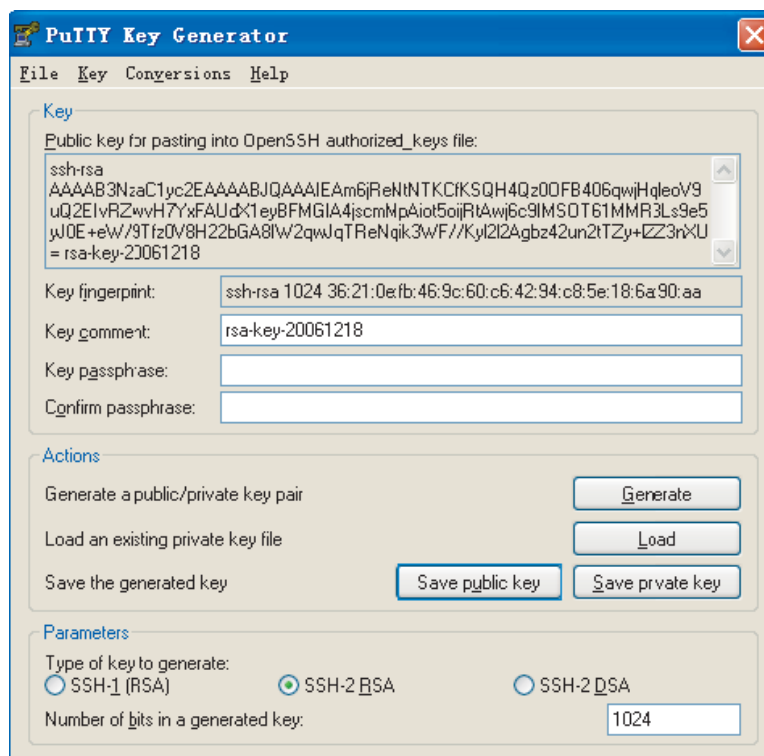
While generating the key pair, you must move the mouse continuously and keep the mouse off the green process bar shown in Figure 136. Otherwise, the process bar stops moving and the key pair generating process is stopped.

Figure 136 Generate a client key pair (2)



After the key pair is generated, click **Save public key** and enter the name of the file for saving the public key ("public" in this case).

Figure 137 Generate a client key pair (3)



Likewise, to save the private key, click **Save private key**. A warning window pops up to prompt you whether to save the private key without any protection. Click **Yes** and enter the name of the file for saving the private key ("private.ppk" in this case).

Figure 138 Generate a client key pair (4)



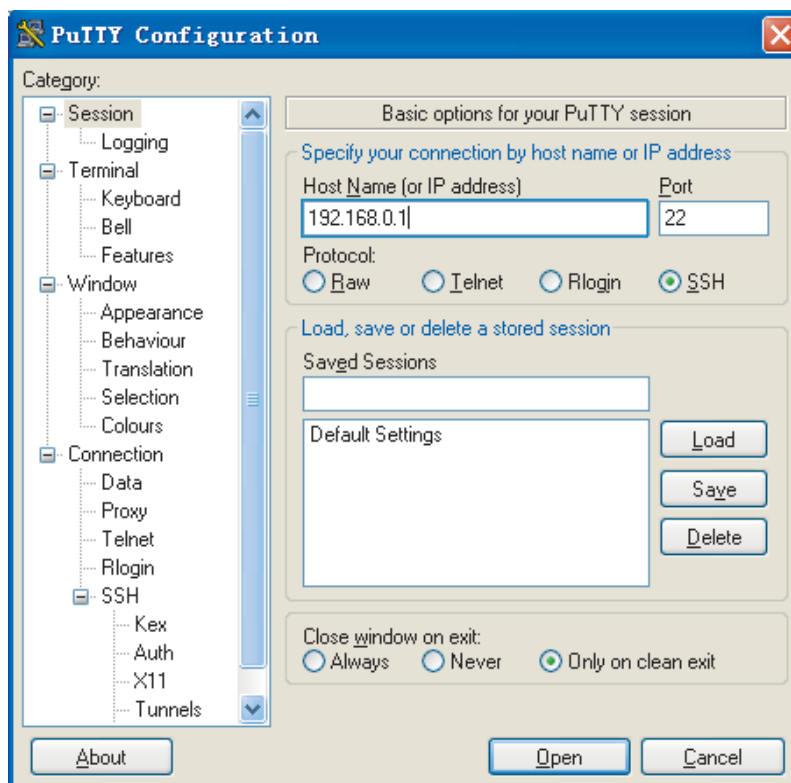
After a public key pair is generated, you need to upload the public key file to the server through FTP or TFTP, and complete the server end configuration before you continue to configure the client.

Establish a connection with the SSH server

- The following takes the SSH client software Putty (version 0.58) as an example.

- 1 Launch PuTTY.exe to enter the following interface.

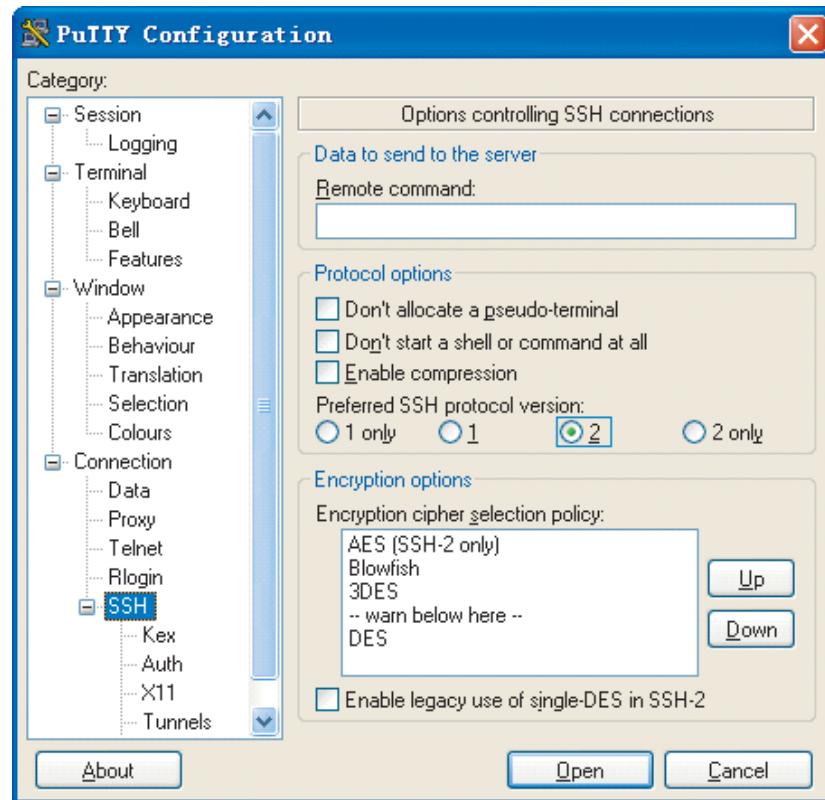
Figure 139 SSH client configuration interface 1



In the **Host Name (or IP address)** text box, enter the IP address of the server.

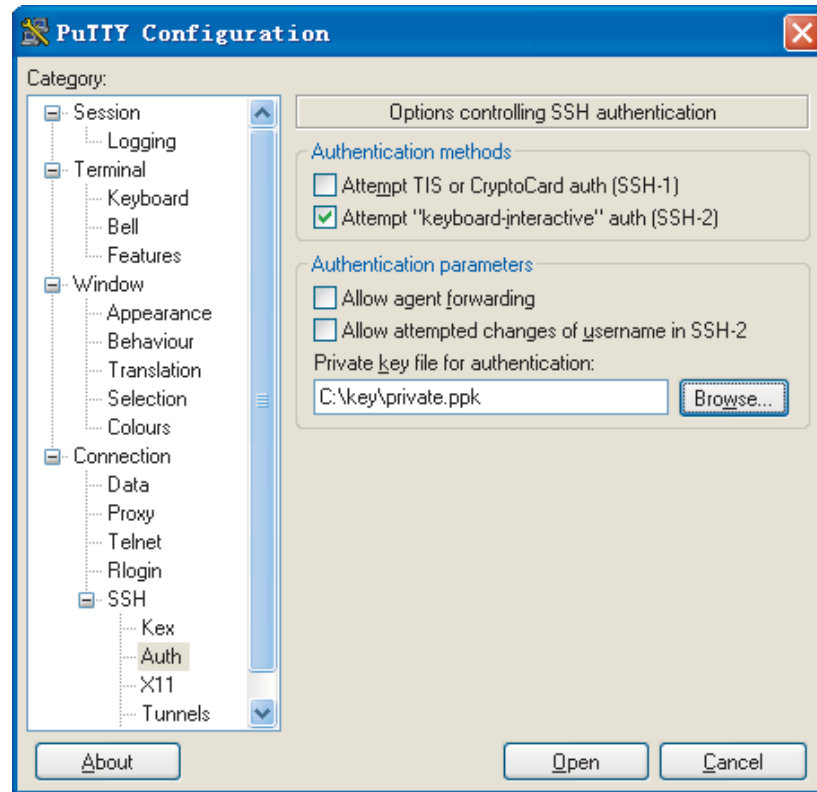
- 2 From the category on the left pane of the window, select **SSH** under **Connection**. The window as shown in Figure 140 appears.

Figure 140 SSH client configuration interface 2



Under **Protocol options**, select **2** from **Preferred SSH protocol version**.

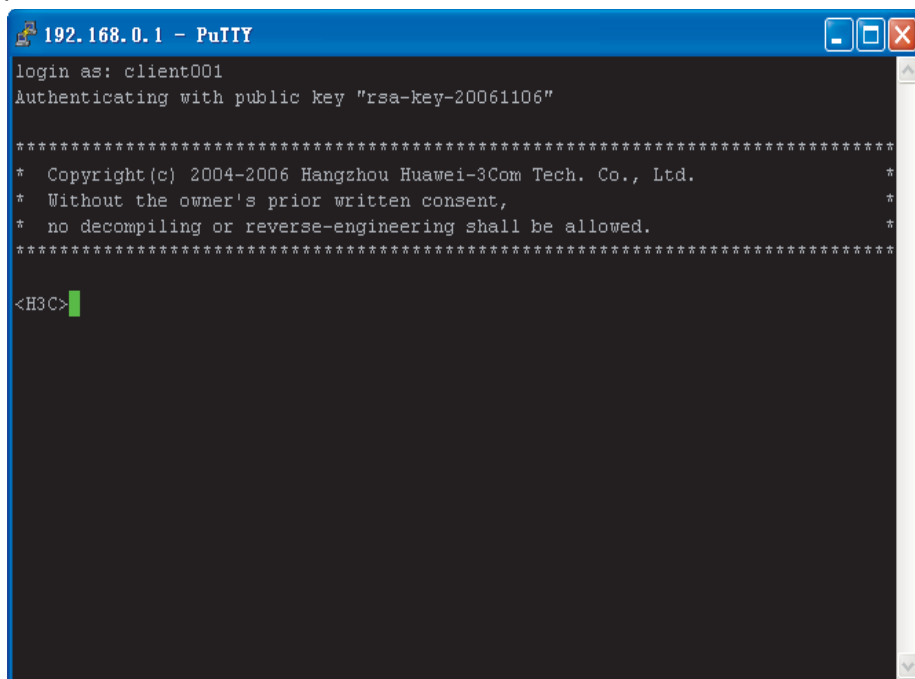
3 Select **Connection/SSH/Auth**. The following window appears.

Figure 141 SSH client configuration interface (2)

Click **Browse...** to bring up the file selection window, navigate to the private key file and click **OK**.

- 4 From the window shown in Figure 141, click **Open**. The following SSH client interface appears. If the connection is normal, you will be prompted to enter the username and password, as shown in Figure 142.

Figure 142 SSH client interface



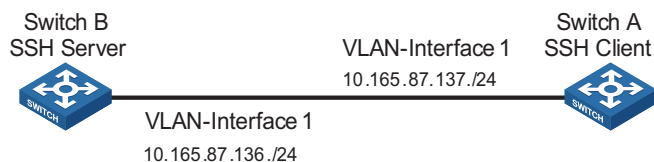
When the Switch Acts as an SSH Client and the Authentication Type is Password

Network requirements

As shown in Figure 143, 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 143 Network diagram of SSH client configuration when using 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.

```

<4210> system-view
[4210] interface vlan-interface 1
[4210-Vlan-interface1] ip address 10.165.87.136 255.255.255.0
[4210-Vlan-interface1] quit
  
```



Generating the RSA and DSA key pairs on the server is prerequisite to SSH login.

```

# Generate RSA and DSA key pairs.
[4210] public-key local create rsa
[4210] public-key local create dsa

# Set the authentication mode for the user interfaces to AAA.
[4210] user-interface vty 0 4
[4210-ui-vty0-4] authentication-mode scheme

# Enable the user interfaces to support SSH.
[4210-ui-vty0-4] protocol inbound ssh
[4210-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.
[4210] local-user client001
[4210-luser-client001] password simple abc
[4210-luser-client001] service-type ssh level 3
[4210-luser-client001] quit

# Configure the authentication type of user client001 as password.
[4210] 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.

```

<4210> system-view
[4210] interface vlan-interface 1
[4210-Vlan-interface1] ip address 10.165.87.137 255.255.255.0
[4210-Vlan-interface1] quit

# Establish a connection to the server 10.165.87.136.

[4210] ssh2 10.165.87.136
Username: client001
Trying 10.165.87.136 ...
Press CTRL+K to abort
Connected to 10.165.87.136 ...

The Server is not authenticated. Do you continue to access it?(Y/N):y
Do you want to save the server's public key?(Y/N):n
Enter password:

*****
* Copyright(c) 2004-2007 3Com Corporation. *
* Without the owner's prior written consent, *
* no decompiling or reverse-switch fabricering shall be allowed. *
*****

<4210>

```

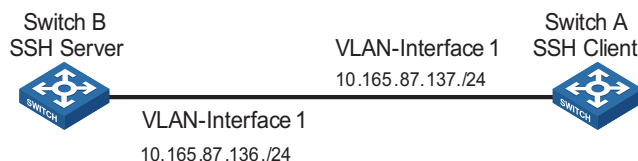
When the Switch Acts as an SSH Client and the Authentication Type is Publickey

Network requirements

As shown in Figure 144, 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 144 Network diagram of SSH client configuration when using publickey authentication



Configuration procedure



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.

```

<4210> system-view
[4210] interface vlan-interface 1
[4210-Vlan-interface1] ip address 10.165.87.136 255.255.255.0
[4210-Vlan-interface1] quit
  
```



Generating the RSA and DSA key pairs on the server is prerequisite to SSH login.

Generate RSA and DSA key pairs.

```

[4210] public-key local create rsa
[4210] public-key local create dsa
  
```

Set the authentication mode for the user interfaces to AAA.

```

[4210] user-interface vty 0 4
[4210-ui-vty0-4] authentication-mode scheme
  
```

Enable the user interfaces to support SSH.

```

[4210-ui-vty0-4] protocol inbound ssh
  
```

Set the user command privilege level to 3.

```

[4210-ui-vty0-4] user privilege level 3
[4210-ui-vty0-4] quit
  
```

Specify the authentication type of user client001 as publickey.

```

[4210] ssh user client001 authentication-type publickey
  
```



Before doing the following steps, you must first generate a DSA key pair on the client and save the public 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" below.

Import the client key pair named Switch001 from the file Switch001.

```

[4210] public-key peer Switch001 import sshkey Switch001
  
```

Assign the public key Switch001 to user client001.

```

[4210] 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.
```

```
<4210> system-view
[4210] interface vlan-interface 1
[4210-Vlan-interface1] ip address 10.165.87.137 255.255.255.0
[4210-Vlan-interface1] quit
```

```
# Generate a DSA key pair
```

```
[4210] public-key local create dsa
```

```
# Export the generated DSA host public key to a file named Switch001.
```

```
[4210] public-key local export dsa ssh2 Switch001
```



After the key pair is generated, you need to upload the public key file to the server through FTP or TFTP and complete the server end configuration before you continue to configure the client.

```
# Establish an SSH connection to the server 10.165.87.136.
```

```
[4210] 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) 2004-2007 3Com Corporation *
* Without the owner's prior written consent, *
* no decompiling or reverse-switch fabricering shall be allowed. *
*****
```

```
<4210>
```

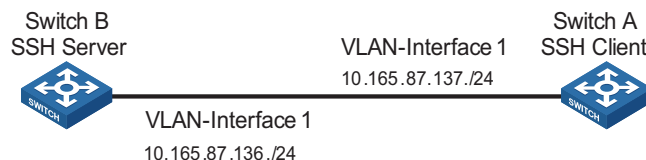
When the Switch Acts as an SSH Client and First-time authentication is not Supported

Network requirements

As shown in Figure 145, 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 145 Network diagram of SSH client configuration



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.
```

```
<4210> system-view
[4210] interface vlan-interface 1
[4210-Vlan-interface1] ip address 10.165.87.136 255.255.255.0
[4210-Vlan-interface1] quit
```



Generating the RSA and DSA key pairs on the server is prerequisite to SSH login.

```
# Generate RSA and DSA key pairs.

[4210] public-key local create rsa
[4210] public-key local create dsa

# Set AAA authentication on user interfaces.

[4210] user-interface vty 0 4
[4210-ui-vty0-4] authentication-mode scheme

# Configure the user interfaces to support SSH.

[4210-ui-vty0-4] protocol inbound ssh

# Set the user command privilege level to 3.

[4210-ui-vty0-4] user privilege level 3
[4210-ui-vty0-4] quit

# Specify the authentication type for user client001 as publickey.

[4210] ssh user client001 authentication-type publickey
```



Before performing the following steps, you must first generate a DSA key pair on the client and save the public key 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.

[4210] public-key peer Switch001 import sshkey Switch001

# Assign public key Switch001 to user client001

[4210] ssh user client001 assign publickey Switch001

# Export the generated DSA host public key to a file named Switch002.

[4210] public-key local export dsa ssh2 Switch002
```



When first-time authentication is not supported, you must first generate a DSA public key 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.

```
<4210> system-view
[4210] interface vlan-interface 1
[4210-Vlan-interface1] ip address 10.165.87.137 255.255.255.0
[4210-Vlan-interface1] quit
```

```
# Generate a DSA key pair

[4210] public-key local create dsa

# Export the generated DSA host public key to a file named Switch001.

[4210] public-key local export dsa ssh2 Switch001
```



After generating the public key, 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.

```
[4210] undo ssh client first-time
```



When first-time authentication is not supported, you must first generate a DSA key pair on the server and save the public key in a file named Switch002, and then upload the file to the SSH client through FTP or TFTP. For details, refer to the above section "Configure Switch B".

Import the public key named Switch002 from the file Switch002.

```
[4210] public-key peer Switch002 import sshkey Switch002
```

Specify the host public key name of the server.

```
[4210] ssh client 10.165.87.136 assign publickey Switch002
```

Establish the SSH connection to server 10.165.87.136.

```
[4210] 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) 2004-2007 3Com Corporation. *
* Without the owner's prior written consent, *
* no decompiling or reverse-switch fabricering shall be allowed. *
*****
```

```
<4210>
```

37

FILE SYSTEM MANAGEMENT CONFIGURATION

File System Configuration

To facilitate management on the switch's memory, the Switch 4210 provides 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 318 Configuration tasks on the file system

Configuration task	Description
Directory operation	Optional
File operation	Optional
Flash memory operation	Optional
Prompt mode configuration	Optional



the Switch 4210 supports intelligent resilient framework (IRF), and allows 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*
- *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.*

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 319 describes the directory-related operations.

Perform the following configuration in user view.

Table 319 Directory operations

To do...	Use the command...	Remarks
Create a directory	mkdir <i>directory</i>	Optional
Delete a directory	rmdir <i>directory</i>	Optional
Display the current work directory	pwd	Optional
Display the information about specific directories and files	dir [/all] [<i>file-url</i>]	Optional
Enter a specified directory	cd <i>directory</i>	Optional



- 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 320.

Perform the following configuration in user view. Note that the **execute** command should be executed in system view.

Table 320 File operations

To do...	Use the command...	Remarks
Delete a file	delete [/unreserved] <i>file-url</i> delete { running-files standby-files } [/unreserved]	Optional A deleted file can be restored by using the undelete command if you delete it by executing the delete command without specifying the /unreserved keyword.
Restore a file in the recycle bin	undelete <i>file-url</i>	Optional
Delete a file from the recycle bin	reset recycle-bin [<i>file-url</i>] [/force]	Optional
Rename a file	rename <i>fileurl-source</i> <i>fileurl-dest</i>	Optional
Copy a file	copy <i>fileurl-source</i> <i>fileurl-dest</i>	Optional
Move a file	move <i>fileurl-source</i> <i>fileurl-dest</i>	Optional
Display the content of a file	more <i>file-url</i>	Optional Currently, the file system only supports displaying the contents of text files.
Display the information about a directory or a file	dir [/all] [<i>file-url</i>]	Optional
Enter system view	system-view	-
Execute the specified batch file	execute <i>filename</i>	Optional This command should be executed in system view.



CAUTION:

- For deleted files whose names are the same, only the latest deleted file is kept in the recycle bin and can be restored.
- The files which are deleted by the **delete** command without the **/unreserved** keyword are actually moved to the recycle bin and thus still take storage space. You can clear the recycle bin by using the **reset recycle-bin** command.
- 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 321.

Perform the following configuration in user view.

Table 321 Operations on the Flash memory

To do...	Use the command...	Remarks
Format the Flash memory	format <i>device</i>	Required
Restore space on the Flash memory	fixdisk <i>device</i>	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 322 Configuration on prompt mode of file system

To do...	Use the command...	Remarks
Enter system view	system-view	-
Configure the prompt mode of the file system	file prompt { alert quiet }	Required By default, the prompt mode of the file system is alert .

File System Configuration Example

Display all the files in the root directory of the file system.

```
<4210> dir /all
Directory of unit1>flash:/
1 (*)  -rw-   3579326  Mar 28 2007 10:51:22  s3100.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
```

7239 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.

```
<4210> 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.

```

<4210> dir /all
Directory of unit1>flash:/

1 (*)  -rw-   3579326  Mar 28 2007 10:51:22  s3100.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

7239 KB total (3585 KB free)

(*) -with main attribute   (b) -with backup attribute
(*b) -with both main and backup attribute
<4210> 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

7239 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 323.

Table 323 Descriptions on file attributes

Attribute name	Description	Feature	Identifier
main	Identifies main startup files. The main startup file is used first for a switch to start up.	In the Flash memory, there can be only one app file, one configuration file and one Web file with the main attribute.	(*)
backup	Identifies backup startup files. The backup startup file is used after a switch fails to start up using the main startup file.	In the Flash memory, there can be only one app file, one configuration file and one Web file with the backup attribute.	(b)

Table 323 Descriptions on file attributes

Attribute name	Description	Feature	Identifier
none	Identifies files that are neither of main attribute nor backup attribute.	-	None



*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.

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 324 in user view. The **display** commands can be executed in any view.

Table 324 Configure file attributes

To do...	Use the command...	Remarks
Configure the app file with the main attribute for the next startup	boot boot-loader <i>file-url</i>	Optional
Configure the app file with the backup attribute for the next startup	boot boot-loader backup-attribute <i>file-url</i>	Optional
Configure the Web file and its attribute	boot web-package <i>webfile</i> { 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 By default, the user is enabled to use the customized password to enter the BOOT menu.

Table 324 Configure file attributes

To do...	Use the command...	Remarks
Display the information about the app file used as the startup file	display boot-loader [unit <i>unit-id</i>]	Optional Available in any view
Display information about the Web file used by the device	display web package	

**CAUTION:**

- *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 “Configuration File Management” on page 67.*

Introduction to FTP and SFTP

Introduction to FTP FTP (file transfer protocol) is commonly used in IP-based networks to transmit files. Before World Wide Web comes into being, files are transferred through command lines, and the most popular application is FTP. At present, although E-mail and Web are the usual methods for file transmission, FTP still has its strongholds.

As an application layer protocol, FTP is used for file transfer between remote server and local 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 4210 can operate as an FTP client or the FTP server in FTP-employed data transmission:

Table 325 The Switch 4210 FTP Roles

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

Table 326 FTP configuration tasks

Item	Configuration task	Description
"FTP Configuration: A Switch Operating as an FTP Server"	"Creating an FTP user"	Required
	"Enabling an FTP server"	Required
	"Configuring connection idle time"	Optional
	"Configuring the banner for an FTP server"	Optional
"FTP Configuration: A Switch Operating as an FTP Client"	"Displaying FTP server information"	Optional
	"Basic configurations on an FTP client"	-

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.

Table 327 Create an FTP user

Operation	Command	Description
Enter system view	system-view	-
Add a local user and enter local user view	local-user <i>user-name</i>	Required By default, no local user is configured.
Configure a password for the specified user	password { simple cipher } <i>password</i>	Optional By default, no password is configured.
Configure the service type as FTP	service-type ftp	Required By default, no service is configured.

Enabling an FTP server

Table 328 Enable an FTP server

Operation	Command	Description
Enter system view	system-view	-
Enable the FTP server function	ftp server enable	Required Disabled by default.



- Only one user can access the Switch 4210 at a given time when the latter operates as an FTP server.

- Operating as an FTP server, the Switch 4210 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.



To protect unused sockets against attacks, the Switch 4210 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.

Table 329 Configure connection idle time

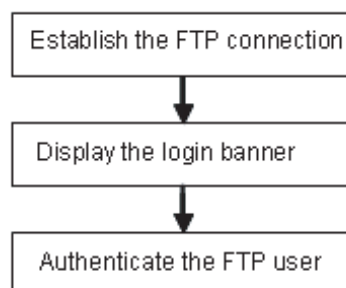
Operation	Command	Description
Enter system view	system-view	-
Configure the connection idle time for the FTP server	ftp timeout <i>minutes</i>	Optional 30 minutes by default

Configuring the banner for an FTP server

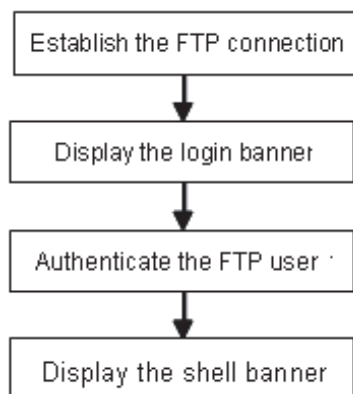
Displaying a banner: With a banner configured on the FTP server, when you access the FTP server through FTP, the configured banner is displayed on the FTP client. Banner falls into the following two types:

- 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 146 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 147 Process of displaying a shell banner**Table 330** Configure the banner display for an FTP server

Operation	Command	Description
Enter system view	system-view	-
Configure a login banner	header login text	Required
Configure a shell banner	header shell text	Use either command or both. By default, no banner is configured.



For details about the **header** command, refer to “Logging into an Ethernet Switch” on page 21.

Displaying FTP server information

After the above configurations, you can execute the **display** commands in any view to display the running status of the FTP server and verify your configurations.

Table 331 Display FTP server information

Operation	Command	Description
Display the information about FTP server configurations on a switch	display ftp-server	Available in any view
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. Table 332 lists the operations that can be performed on an FTP client.

Table 332 Basic configurations on an FTP client

Operation	Command	Description
Enter FTP client view	ftp [cluster remote-server [port-number]]	-

Table 332 Basic configurations on an FTP client

Operation	Command	Description
Specify to transfer files in ASCII characters	ascii	Use either command
Specify to transfer files in binary streams	binary	By default, files are transferred in ASCII characters.
Set the data transfer mode to passive	passive	Optional passive by default.
Change the working directory on the remote FTP server	cd <i>pathname</i>	Optional
Change the working directory to be the parent directory	cdup	
Get the local working path on the FTP client	lcd	
Display the working directory on the FTP server	pwd	
Create a directory on the remote FTP server	mkdir <i>pathname</i>	
Remove a directory on the remote FTP server	rmdir <i>pathname</i>	
Delete a specified file	delete <i>remotefile</i>	
Query a specified file on the FTP server	dir [<i>remotefile</i>] [<i>localfile</i>] ls [<i>remotefile</i>] [<i>localfile</i>]	Optional If no file name is specified, all the files in the current directory are displayed. The difference between these two commands is that the dir command can display the file name, directory as well as file attributes; while the ls command can display only the file name and directory.
Download a remote file from the FTP server	get <i>remotefile</i> [<i>localfile</i>]	Optional
Upload a local file to the remote FTP server	put <i>localfile</i> [<i>remotefile</i>]	
Rename a file on the remote server	rename <i>remote-source</i> <i>remote-dest</i>	
Log in with the specified user name and password	user <i>username</i> [<i>password</i>]	
Connect to a remote FTP server	open { <i>ip-address</i> <i>server-name</i> } [<i>port</i>]	
Terminate the current FTP connection without exiting FTP client view	disconnect close	
Terminate the current FTP connection and return to user view	quit bye	
Display the online help about a specified command concerning FTP	remotehelp [<i>protocol-command</i>]	
Enable the verbose function	verbose	Optional Enabled by default

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 user name "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 148 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 user name as "switch", the password as "hello", and the service type as FTP.

```

<4210>
<4210> system-view
[4210] ftp server enable
[4210] local-user switch
[4210-luser-switch] password simple hello
[4210-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 user name "switch" and password "hello" to log in and enter FTP view.

```
C:\> ftp 1.1.1.1
Connected to 1.1.1.1.
220 FTP service ready.
User (1.1.1.1:(none)): switch
331 Password required for switch.
Password:
230 User logged in.
ftp>
```

Upload the **switch.bin** file.

```
ftp> put switch.bin
200 Port command okay.
150 Opening ASCII mode data connection for switch.bin.
226 Transfer complete.
```

Download the **config.cfg** file.

```
ftp> get config.cfg
200 Port command okay.
150 Opening ASCII mode data connection for config.cfg.
226 Transfer complete.
ftp: 3980 bytes received in 8.277 seconds 0.48Kbytes/sec.
```

This example uses the command line window tool provided by Windows. Follow the instructions in the appropriate section for logging into other FTP clients.



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 series switch is not shipped with FTP client application software. You need to purchase and install it by yourself.

3 Configure Switch A (FTP server)

After uploading the application, use the **boot boot-loader** command to specify the uploaded file (**switch.bin**) to be the startup file used when the switch starts the next time, and restart the switch. Thus the switch application is upgraded.

```
<4210> boot boot-loader switch.bin
<4210> reboot
```



For information about the **boot boot-loader** command and how to specify the startup file for a switch, refer to the "Basic System Configuration and Debugging" on page 483.

FTP Banner Display Configuration Example

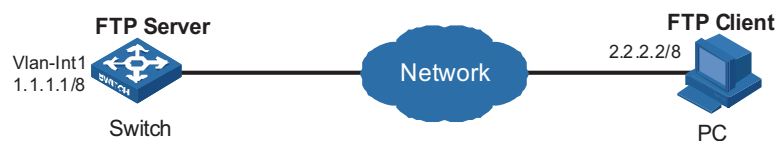
Network requirements

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 named "switch" and the password "hello" have 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 149 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 "Configuration Example: A Switch Operating as an FTP Server".

```

<4210> system-view
[4210] header login %login banner appears%
[4210] header shell %shell banner appears%
[4210]
  
```

2 Configure the PC (FTP client)

Access the Ethernet switch through FTP. Enter the user name "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 the "switch" directory of the PC to back up the configuration file.

- Create a user account on the FTP server with the user name "switch" and password "hello", and grant the user "switch" read and write permissions for the directory named "Switch" on the PC.
- Configure the IP address 1.1.1.1 for a VLAN interface on the switch, and 2.2.2.2 for the PC. Ensure a route exists between the switch and the PC.

Network diagram

Figure 150 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 user name "switch" and password "hello".

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.)

```
<4210>
```



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.

```
<4210> ftp 2.2.2.2
```

```
Trying ...
```

```
Press CTRL+K to abort
```

```
Connected.
```

```
220 FTP service ready.
```

```
User(none):switch
```

```
331 Password required for switch.
```

```

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
<4210>
```

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.

```

<4210> boot boot-loader switch.bin
<4210> reboot

```



For information about the **boot boot-loader** command and how to specify the startup file for a switch, refer to “Basic System Configuration and Debugging” on page 483.

SFTP Configuration

Table 333 SFTP configuration tasks

Item	Configuration task	Description
“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”	-

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 section of this manual.

Table 334 Enable an SFTP server

Operation	Command	Description
Enter system view	system-view	-
Enable an SFTP server	sftp server enable	Required Disabled by default

Configuring connection idle time

After the idle time is configured, if the server does not receive service requests from a client within a specified time period, it terminates the connection with the client, thus preventing a user from occupying the connection for a long time without performing any operation.

Table 335 Configure connection idle time

Operation	Command	Description
Enter system view	system-view	-
Configure the connection idle time for the SFTP server	ftp timeout <i>time-out-value</i>	Optional 10 minutes by default

Supported SFTP client software

A Switch 4210 operating as an SFTP server can interoperate with SFTP client software, including SSH Tectia Client v4.2.0 (SFTP), v5.0, and WINS SCP.

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.



- Currently a Switch 4210 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 WINS SCP, 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. Table 336 lists the operations that can be performed on an SFTP client.

Table 336 Basic configurations on an SFTP client

Operation	Command	Description
Enter system view	system-view	-
Enter SFTP client view	sftp { <i>host-ip</i> <i>host-name</i> } [<i>port-num</i>] [identity-key { dsa rsa }] prefer_kex { dh_group1 dh_exchange_group } prefer_ctos_cipher { des aes128 } prefer_stoc_cipher { des aes128 } prefer_ctos_hmac { sha1 sha1_96 md5 md5_96 } prefer_stoc_hmac { sha1 sha1_96 md5 md5_96 }] *	Required
Change the working directory on the remote SFTP server	cd <i>pathname</i>	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 <i>pathname</i>	
Remove a directory on the remote SFTP server	rmdir <i>pathname</i>	
Delete a specified file	delete <i>remotefile</i> remove <i>remote-file</i>	Optional Both commands have the same effect.
Query a specified file on the SFTP server	dir [<i>remotefile</i>] [<i>localfile</i>] ls [<i>remotefile</i>] [<i>localfile</i>]	Optional If no file name is provided, all the files in the current directory are displayed. The difference between these two commands is that the dir command can display the file name, directory as well as file attributes; while the ls command can display only the file name and directory.
Download a remote file from the SFTP server	get <i>remotefile</i> [<i>localfile</i>]	Optional
Upload a local file to the remote SFTP server	put <i>localfile</i> [<i>remotefile</i>]	
Rename a file on the remote server	rename <i>remote-source</i> <i>remote-dest</i>	
Exit SFTP client view and return to system view	bye exit quit	The three commands have the same effect.
Display the online help about a specified command concerning SFTP	help [all <i>command-name</i>]	Optional



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*.

SFTP Configuration Example

Network requirements

As shown in Figure 151, 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 user name "client001" and password "abc" exists on the SFTP server.

Network diagram

Figure 151 Network diagram for SFTP configuration



Configuration procedure

1 Configure the SFTP server (switch B)

Create key pairs.

```
<4210> system-view
[4210] public-key local create rsa
[4210] 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.

```
[4210] interface vlan-interface 1
[4210-Vlan-interface1] ip address 192.168.0.1 255.255.255.0
[4210-Vlan-interface1] quit
```

Specify the SSH authentication mode as AAA.

```
[4210] user-interface vty 0 4
[4210-ui-vty0-4] authentication-mode scheme
```

Configure the protocol through which the remote user logs in to the switch as SSH.

```
[4210-ui-vty0-4] protocol inbound ssh
[4210-ui-vty0-4] quit
```

Create a local user client001.

```
[4210] local-user client001
[4210-luser-client001] password simple abc
[4210-luser-client001] service-type ssh
[4210-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.

```
[4210] ssh user client001 authentication-type password
```

Specify the service type as SFTP.

```
[4210] ssh user client001 service-type sftp
```

Enable the SFTP server.

```
[4210] 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.

```
<4210> system-view
[4210] interface vlan-interface 1
[4210-Vlan-interface1] ip address 192.168.0.2 255.255.255.0
[4210-Vlan-interface1] quit
```

Connect to the remote SFTP server. Enter the user name "client001" and the password "abc", and then enter SFTP client view.

```
[4210] 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 ngroup 1759 Aug 23 06:52 config.cfg
-rwxrwxrwx 1 noone ngroup 225 Aug 24 08:01 pubkey2
-rwxrwxrwx 1 noone ngroup 283 Aug 24 07:39 pubkey1
drwxrwxrwx 1 noone ngroup 0 Sep 01 06:22 new
-rwxrwxrwx 1 noone ngroup 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 ngroup 1759 Aug 23 06:52 config.cfg
-rwxrwxrwx 1 noone ngroup 225 Aug 24 08:01 pubkey2
-rwxrwxrwx 1 noone ngroup 283 Aug 24 07:39 pubkey1
drwxrwxrwx 1 noone ngroup 0 Sep 01 06:22 new
-rwxrwxrwx 1 noone ngroup 225 Sep 01 06:55 pub
drwxrwxrwx 1 noone ngroup 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 ngroup 1759 Aug 23 06:52 config.cfg
-rwxrwxrwx 1 noone ngroup 225 Aug 24 08:01 pubkey2
-rwxrwxrwx 1 noone ngroup 283 Aug 24 07:39 pubkey1
drwxrwxrwx 1 noone ngroup 0 Sep 01 06:22 new
-rwxrwxrwx 1 noone ngroup 225 Sep 01 06:55 pub
drwxrwxrwx 1 noone ngroup 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 the 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 ngroup 1759 Aug 23 06:52 config.cfg
-rwxrwxrwx 1 noone ngroup 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

[4210]

Introduction to TFTP

Compared with FTP, TFTP (trivial file transfer protocol) features simple interactive access interface and no authentication control. Therefore, TFTP is applicable in the networks where client-server interactions are relatively simple. TFTP is implemented based on UDP. It transfers data through UDP port 69. Basic TFTP operations are described in 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.

The Switch 4210 can operate 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.



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

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. Table 337 lists the operations that can be performed on a TFTP client.

Table 337 Basic configurations on a TFTP client

Operation	Command	Description
Download a file from a TFTP server	tftp [<i>tftp-server</i> ipv6 <i>ipv6-tftp-server</i> [-i <i>interface-type interface-number</i>]] get <i>source-file</i> [<i>dest-file</i>]	Optional
Upload a file to a TFTP server	tftp [<i>tftp-server</i> ipv6 <i>ipv6-tftp-server</i> [-i <i>interface-type interface-number</i>]] put <i>source-file</i> [<i>dest-file</i>]	Optional
Enter system view	system-view	-
Set the file transmission mode	tftp { ascii binary }	Optional Binary by default
Specify an ACL rule used by the specified TFTP client to access a TFTP server	tftp-server acl <i>acl-number</i>	Optional Not specified by default

TFTP Configuration Example

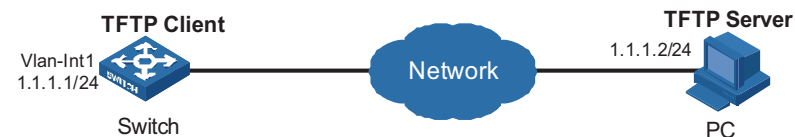
Network requirements

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 1.1.1.2 respectively. The port through which the switch connects with the PC belongs to the VLAN.

Network diagram

Figure 152 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.)



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

```
<4210> system-view
[4210]
```

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.)

```
[4210] interface Vlan-interface 1
[4210-Vlan-interface1] ip address 1.1.1.1 255.255.255.0
[4210-Vlan-interface1] quit
```

Download the switch application named **switch.bin** from the TFTP server to the switch.

```
<4210> tftp 1.1.1.2 get switch.bin switch.bin
```

Upload the switch configuration file named **config.cfg** to the TFTP server.

```
<4210> tftp 1.1.1.2 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.

```
<4210> boot boot-loader switch.bin
<4210> reboot
```



*For information about the **boot boot-loader** command and how to specify the startup file for a switch, refer to "Basic System Configuration and Debugging" on page 483.*

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 338 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 339 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)



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 340.

Table 340 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
FTM	Fabric topology management module
FTPS	FTP server module
HA	High availability module
HABP	3Com authentication bypass protocol module
HTTPD	HTTP server module
HWCM	3Com Configuration Management private MIB module
HWP	Remote Ping 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
PKI	Public key infrastructure module
RDS	Radius module
RMON	Remote monitor module
RSA	Revest, Shamir and Adleman encryption module
SHELL	User interface module
SNMP	Simple network management protocol module
SOCKET	Socket module
SSH	Secure shell module
SYSMIB	System MIB module
TAC	HWTACACS module
TELNET	Telnet module

Table 340 Source module name list

Module name	Description
TFTP	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

System information has the following format:

```
<priority>timestamp sysname module/level/digest:content
```



- The closing set of angle brackets < >, the space, the forward slash /, and the colon are all required in the above format.
- Before the <priority> 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 log host:

```
% <188>Dec 6 10:44:55:283 2006 3Com NTP/5/NTP_LOG:- 1 - NTP service enable
```

("-1-" indicates that the unit number of the device is 1.)

What follows is a detailed explanation of the fields involved:

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 338 details the value and meaning associated with each severity.

Note that there is no space between the priority and timestamp fields and 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.



There is a space between the timestamp and sysname (host name) fields.

The time stamp has the following two formats.

- Without the universal time coordinated (UTC) time zone, the time stamp is in the format of "Mmm dd hh:mm:ss:ms yyyy".

- 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.
- "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 direction 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] 4210 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 "4210".

You can use the **sysname** command to modify the system name. Refer to *"Basic System Configuration and Debugging"* on page 483.

Note that there is a space between the sysname and module fields.

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 340 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 338 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.

Content

This field provides the content of the system information.



The above section describes the log information format sent to a log host by a switch. Some log host software will resolve the received information as well as its format, so that you may see the log format displayed on the log host is different from the one described in this manual.

Information Center Configuration

Introduction to the Information Center Configuration Tasks

Table 341 Information center configuration tasks

Task	Remarks
"Configuring Synchronous Information Output" on page 456	Optional
"Displaying the Time Stamp with the UTC Time Zone" on page 457	
"Setting to Output System Information to the Console" on page 457	Optional
"Setting to Output System Information to a Monitor Terminal" on page 459	Optional
"Setting to Output System Information to a Log Host" on page 460	Optional
"Setting to Output System Information to the Trap Buffer" on page 461	Optional
"Setting to Output System Information to the Log Buffer" on page 461	Optional
"Setting to Output System Information to the SNMP NMS" on page 462	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.

Table 342 Configure synchronous information output

Operation	Command	Description
Enter system view	system-view	-
Enable synchronous information output	info-center synchronous	Required Disabled by default



- 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.

Displaying 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

Table 343 Configure to display time stamp with the UTC time zone

Operation	Command	Description
Set the time zone for the system	clock timezone zone-name { add minus } time	Required 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 Non log host direction info-center timestamp { log trap debugging } date	Required Use either command
Set to display the UTC time zone in the output information of the information center	info-center timestamp utc	Required By default, no UTC time zone is displayed in the output information

Setting to Output System Information to the Console

Setting to output system information to the console

Table 344 Set to output system information to the console

Operation	Command	Description
Enter system view	system-view	-
Enable the information center	info-center enable	Optional Enabled by default.

Table 344 Set to output system information to the console

Operation	Command	Description
Enable system information output to the console	info-center console channel { <i>channel-number</i> <i>channel-name</i> }	Optional By default, the switch uses information channel 0 to output log/debugging/trap information to the console.
Configure the output rules of system information	info-center source { <i>modu-name</i> default } channel { <i>channel-number</i> <i>channel-name</i> } [{ log trap debug } { level <i>severity</i> state <i>state</i> }]*	Optional Refer to Table 345 for the default output rules of system information.
Set the format of time stamp in the output information	info-center timestamp { log trap debugging } { boot date none }	Optional By default, the time stamp format of the log and trap output information is date , and that of the debugging output information is boot .



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 345 Default output rules for different output directions

Output direction	Modules allowed	LOG		TRAP		DEBUG	
		Enabled/d/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.

Table 346 Enable the system information display on the console:

Operation	Command	Description
Enable the debugging/log/trap information terminal display function	terminal monitor	Optional Enabled by default.

Table 346 Enable the system information display on the console:

Operation	Command	Description
Enable debugging information terminal display function	terminal debugging	Optional Disabled by default.
Enable log information terminal display function	terminal logging	Optional Enabled by default.
Enable trap information terminal display function	terminal trapping	Optional Enabled by default.



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

Table 347 Set to output system information to a monitor terminal

Operation	Command	Description
Enter system view	system-view	-
Enable the information center	info-center enable	Optional Enabled by default.
Enable system information output to Telnet terminal or dumb terminal	info-center monitor channel { <i>channel-number</i> <i>channel-name</i> }	Optional By default, a switch outputs log/debugging/trap information to a user terminal through information channel 1.
Configure the output rules of system information	info-center source { <i>modu-name</i> default } channel { <i>channel-number</i> <i>channel-name</i> } [{ log trap debug } { level <i>severity</i> state <i>state</i> }]*	Optional Refer to Table 345 for the default output rules of system information.
Set the format of time stamp in the output information	info-center timestamp { log trap debugging } { boot date none }	Optional By default, the time stamp format of the log and trap output information is date , and that of the debugging output information is boot .



- 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.

Table 348 Enable the display of system information on a monitor terminal

Operation	Command	Description
Enable the debugging/log/trap information terminal display function	terminal monitor	Optional Enabled by default
Enable debugging information terminal display function	terminal debugging	Optional Disabled by default
Enable log information terminal display function	terminal logging	Optional Enabled by default
Enable trap information terminal display function	terminal trapping	Optional Enabled by default



*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

Table 349 Set to output system information to a log host

Operation	Command	Description
Enter system view	system-view	-
Enable the information center	info-center enable	Optional Enabled by default.
Enable system information output to a log host	info-center loghost <i>host-ip-addr</i> [channel { <i>channel-number</i> <i>channel-name</i> }] facility <i>local-number</i>]*	Required By default, the switch does not output information to the log host. After you configure the switch to output information to the log host, the switch uses information channel 2 by default.
Configure the source interface through which log information is sent to the log host	info-center loghost source <i>interface-type</i> <i>interface-number</i>	Optional By default, no source interface is configured, and the system automatically selects an interface as the source interface.

Table 349 Set to output system information to a log host

Operation	Command	Description
Configure the output rules of system information	info-center source { <i>modu-name</i> default } channel { <i>channel-number</i> <i>channel-name</i> } [{ log trap debug } { level severity state state }]*	Optional Refer to Table 345 for the default output rules of system information.
Set the format of the time stamp to be sent to the log host	info-center timestamp loghost { date no-year-date none }	Optional By default, the time stamp format of the information output to the log host is date .



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

Table 350 Set to output system information to the trap buffer

Operation	Command	Description
Enter system view	system-view	-
Enable the information center	info-center enable	Optional Enabled by default.
Enable system information output to the trap buffer	info-center trapbuffer [channel { <i>channel-number</i> <i>channel-name</i> } size <i>buffersize</i>]*	Optional By default, the switch uses information channel 3 to output trap information to the trap buffer, which can hold up to 256 items by default.
Configure the output rules of system information	info-center source { <i>modu-name</i> default } channel { <i>channel-number</i> <i>channel-name</i> } [{ log trap debug } { level severity state state }]*	Optional Refer to Table 345 for the default output rules of system information.
Set the format of time stamp in the output information	info-center timestamp { log trap debugging } { boot date none }	Optional By default, the time stamp format of the output trap information is date .

Setting to Output System Information to the Log Buffer

Table 351 Set to output system information to the log buffer

Operation	Command	Description
Enter system view	system-view	-
Enable the information center	info-center enable	Optional Enabled by default.
Enable information output to the log buffer	info-center logbuffer [channel { <i>channel-number</i> <i>channel-name</i> } size <i>buffersize</i>]*	Optional By default, the switch uses information channel 4 to output log information to the log buffer, which can hold up to 512 items by default.

Table 351 Set to output system information to the log buffer

Operation	Command	Description
Configure the output rules of system information	info-center source { <i>modu-name</i> default } channel { <i>channel-number</i> <i>channel-name</i> } [{ log trap debug } { level <i>severity</i> state <i>state</i> }]*	Optional Refer to Table 345 for the default output rules of system information.
Set the format of time stamp in the output information	info-center timestamp { log trap debugging } { boot date none }	Optional By default, the time stamp format of the output log information is date .

Setting to Output System Information to the SNMP NMS

Table 352 Set to output system information to the SNMP NMS

Operation	Command	Description
Enter system view	system-view	-
Enable the information center	info-center enable	Optional Enabled by default.
Enable information output to the SNMP NMS	info-center snmp channel { <i>channel-number</i> <i>channel-name</i> }	Optional By default, the switch outputs trap information to SNMP through channel 5.
Configure the output rules of system information	info-center source { <i>modu-name</i> default } channel { <i>channel-number</i> <i>channel-name</i> } [{ log trap debug } { level <i>severity</i> state <i>state</i> }]*	Optional Refer to Table 345 for the default output rules of system information.
Set the format of time stamp in the output information	info-center timestamp { log trap debugging } { boot date none }	Optional By default, the time stamp format of the information output to the SNMP NMS is date .



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

After the above configurations, you can execute the **display** commands in any view to display the running status of the information center, and thus validate your configurations. You can also execute the **reset** commands in user view to clear the information in the log buffer and trap buffer.

Table 353 Display and maintain information center

Operation	Command	Description
Display information on an information channel	display channel [<i>channel-number</i> <i>channel-name</i>]	Available in any view
Display the operation status of information center, the configuration of information channels, the format of time stamp	display info-center [<i>unit unit-id</i>]	
Display the status of log buffer and the information recorded in the log buffer	display logbuffer [<i>unit unit-id</i>] [<i>level severity</i> <i>size buffersize</i>]* [[{ begin exclude include } <i>regular-expression</i>]]	
Display the summary information recorded in the log buffer	display logbuffer summary [<i>level severity</i>]	
Display the status of trap buffer and the information recorded in the trap buffer	display trapbuffer [<i>unit unit-id</i>] [<i>size buffersize</i>]	
Clear information recorded in the log buffer	reset logbuffer [<i>unit unit-id</i>]	Available in user view
Clear information recorded in the trap buffer	reset trapbuffer [<i>unit unit-id</i>]	

Information Center Configuration Examples

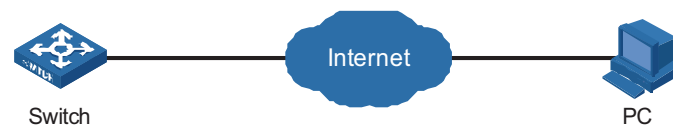
Log Output to a UNIX Log Host

Network requirements

The switch sends the following log information to the Unix log host whose IP address is 202.38.1.10: the log information of the two modules ARP and IP, with severity higher than "informational".

Network diagram

Figure 153 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
```



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.



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.

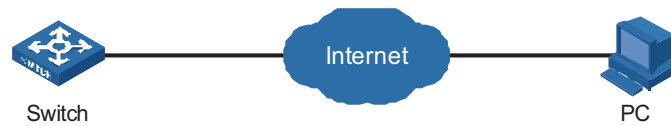
Log Output to a Linux Log Host

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 154 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 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.



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.

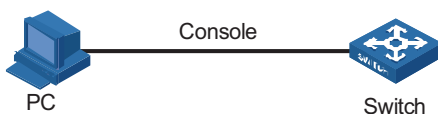
Log Output to the Console

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 155 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 156 Network diagram



Configuration procedure

Name the local time zone z8 and configure it to be eight hours ahead of UTC time.

```
<4210> 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.

```
<4210> system-view
```

System View: return to User View with Ctrl+Z.

```
[4210] info-center timestamp loghost date
```

Configure to add UTC time to the output information of the information center.

```
[4210] info-center timestamp utc
```


41

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.

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



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.



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.....

```
*****
*
*           3Com Switch 4210 26-Port BOOTROM, Version 507*
*
*****
```

Copyright (c) 2004-2007 3Com Corporation

Creation date : Apr 17 2007, 10:12:36
 CPU Clock Speed : 200MHz
 BUS Clock Speed : 33MHz
 Memory Size : 64MB
 Mac Address : 000fe2123456

Press Ctrl-B to enter Boot Menu...

Press <Ctrl+B>. The system displays:

Password :



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
```



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 157, Figure 158.

Figure 157 Properties dialog box

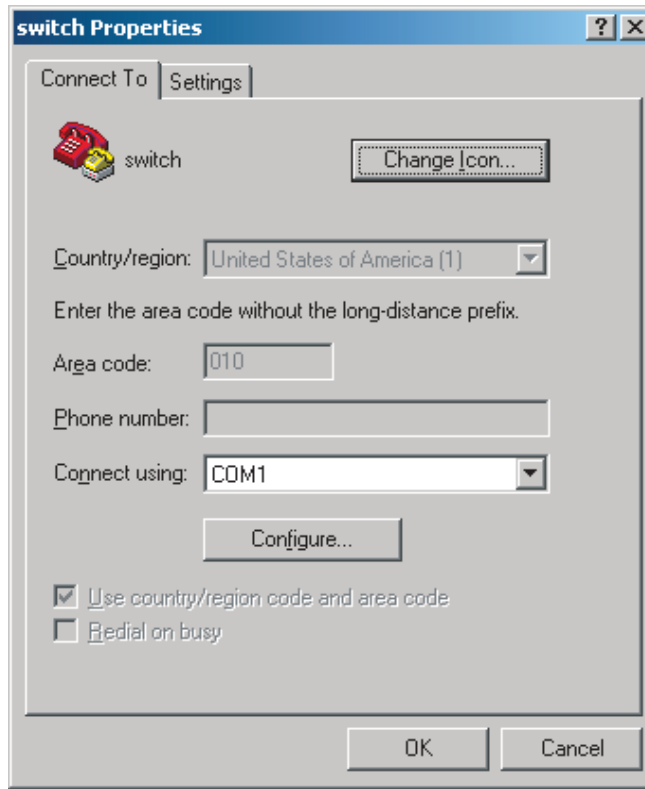
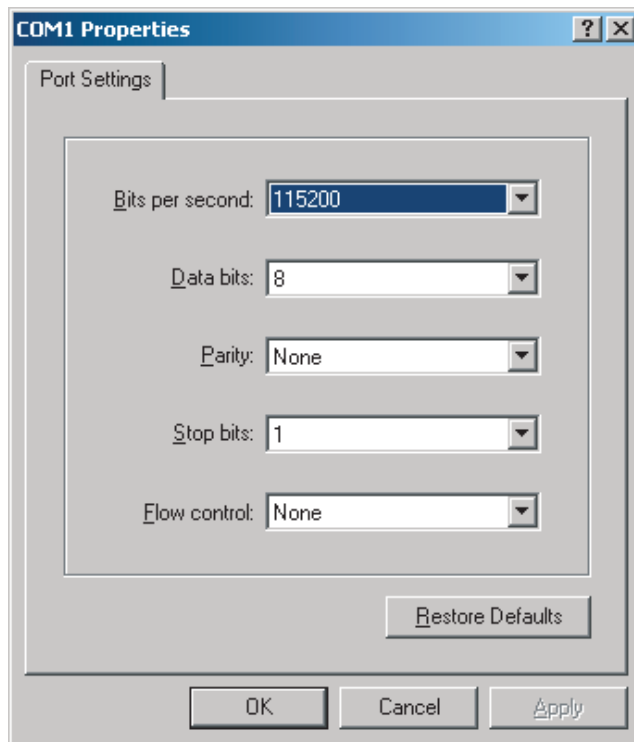
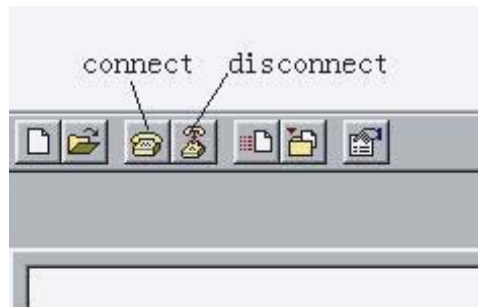


Figure 158 Console port configuration dialog box



Step 5: Click the <Disconnect> button to disconnect the HyperTerminal from the switch and then click the <Connect> button to reconnect the HyperTerminal to the switch, as shown in Figure 159.

Figure 159 Connect and disconnect buttons



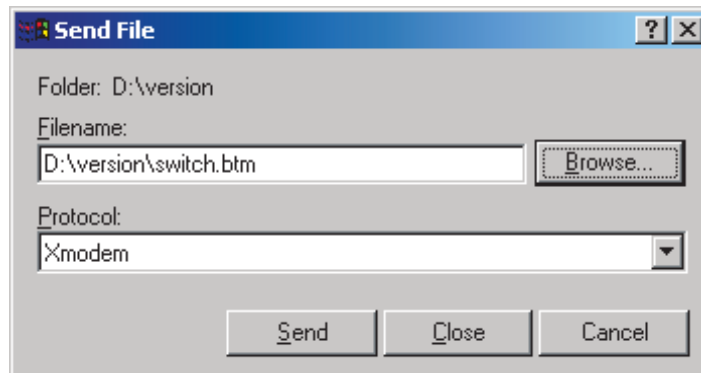
The new baudrate takes effect after you disconnect and reconnect the HyperTerminal program.

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
```

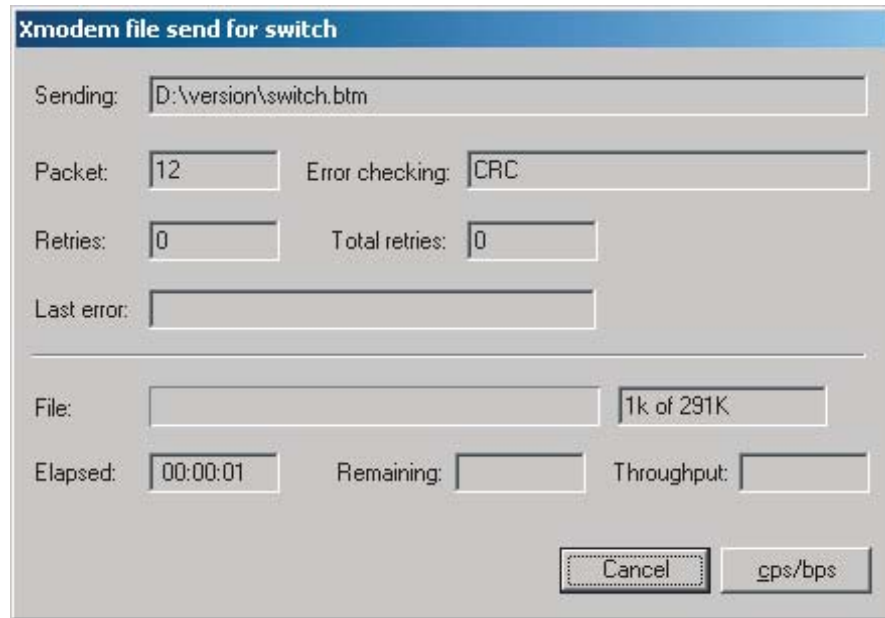
Step 7: Choose [Transfer/Send File] in HyperTerminal, and click <Browse> in pop-up dialog box, as shown in Figure 160. Select the software file that you need to load to the switch, and set the protocol to XModem.

Figure 160 Send file dialog box



Step 8: Click <Send>. The system displays the page, as shown in Figure 161.

Figure 161 Sending file page



Step 9: After the sending process completes, the system displays the following information:

```
Loading ...CCCCCCCCC done!
```

Step 10: Reset HyperTerminal's baudrate to 9600 bps (refer to Step 4 and 5). Then, press any key as prompted. The system will display the following information when it completes the loading.

```
Bootrom updating.....done!
```



- If the HyperTerminal's baudrate is not reset to 9600 bps, the system prompts "Your baudrate should be set to 9600 bps again! Press enter key when ready".
- You need not reset the HyperTerminal's baudrate and can skip the last step if you have chosen 9600 bps. In this case, the system upgrades the Boot ROM automatically and prompts "Bootrom updating now.....done!".

Loading host software

Follow these steps to load the host software:

Step 1: Select <1> in BOOT Menu and press <Enter>. The system displays the following information:

1. Set TFTP protocol parameter
2. Set FTP protocol parameter
3. Set XMODEM protocol parameter
0. Return to boot menu

```
Enter your choice(0-3):
```

Step 2: Enter 3 in the above menu to load the host software by using XModem.

The subsequent steps are the same as those for loading the Boot ROM, except that the system gives the prompt for host software loading instead of Boot ROM loading.



You can also use the **xmodem get** command to load host software through the Console port (of AUX type). The load procedures are as follows (assume that the PC is connected to the Console port of the switch, and logs onto the switch through the Console port):

- Step 1: Execute the **xmodem get** command in user view. In this case, the switch is ready to receive files.
- Step 2: Enable the HyperTerminal on the PC, and configure XModem as the transfer protocol, and configure communication parameters on the Hyper Terminal the same as that on the Console port.
- Step 3: Choose the file to be loaded to the switch, and then start to transmit the file.

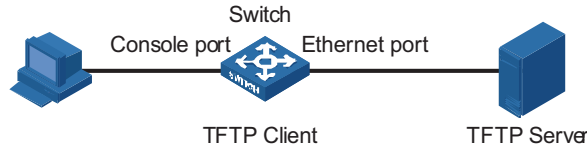
Loading by TFTP through Ethernet Port

Introduction to TFTP

TFTP, a protocol in TCP/IP protocol suite, is used for trivial file transfer between client and server. It is over UDP to provide unreliable data stream transfer service.

Loading the Boot ROM

Figure 162 Local loading using TFTP



Step 1: As shown in Figure 162, connect the switch through an Ethernet port to the TFTP server, and connect the switch through the Console port to the configuration PC.



You can use one PC as both the configuration device and the TFTP server.

Step 2: Run the TFTP server program on the TFTP server, and specify the path of the program to be downloaded.



CAUTION: TFTP server program is not provided with the 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_02.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):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

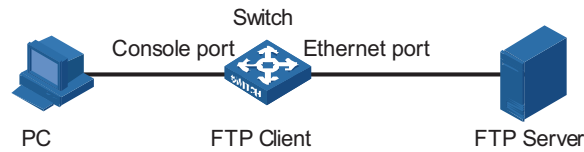
Introduction to FTP

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 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 163 Local loading using FTP client

- 1 As shown in Figure 163, connect the switch through an Ethernet port to the FTP server, and connect the switch through the Console port to the configuration PC.



You can use one computer as both configuration device and FTP server.

- 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.
- 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):

- 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

```

- 5 Press <Enter>. The system displays the following information:

```
Are you sure to update your bootrom?Yes or No(Y/N)
```

- 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:

- 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):

- 2 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 164, 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 164 Remote loading using FTP Client



Step 1: Download the program to the switch using FTP commands.

```

<4210> ftp 10.1.1.1
Trying ...
Press CTRL+K to abort
Connected.
220 WFTPD 2.0 service (by Texas Imperial Software) ready for new use
r
User(none):abc
331 Give me your password, please
Password:
230 Logged in successfully
[ftp] get switch.btm
[ftp] bye

```



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.

```

<4210> 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.

```
<4210> reboot
```



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.

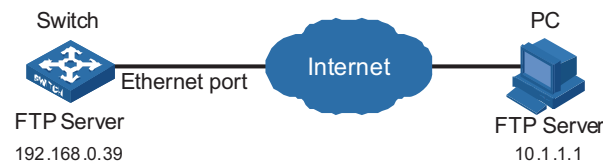
Pay attention to the following:

- 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 Configuration” on page 423.
- Ensure that the power supply is available during software loading.

Loading Procedure Using FTP Server

As shown in Figure 165, 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.

Figure 165 Remote loading using FTP server



1 To load the Boot ROM.

- a As shown in Figure 165, connect the switch through an Ethernet port to the PC (whose IP address is 10.1.1.1)
- b Configure the IP address of VLAN-interface 1 on the switch to 192.168.0.28, and subnet mask to 255.255.255.0.



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.

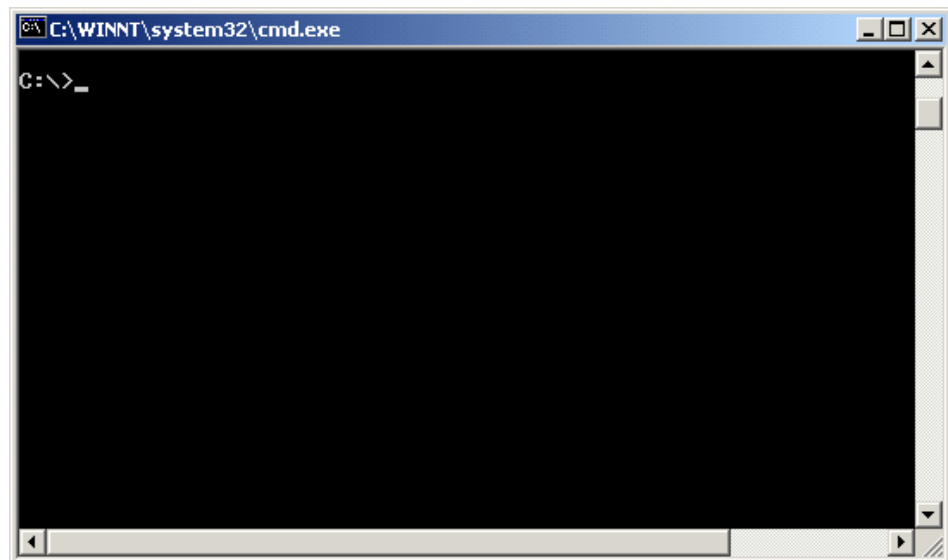
```
<4210> system-view
System View: return to User View with Ctrl+Z.
[4210] interface Vlan-interface 1
[4210-Vlan-interface1] ip address 192.168.0.28 255.255.255.0
```

- c Enable FTP service on the switch, and configure the FTP user name to test and password to pass.

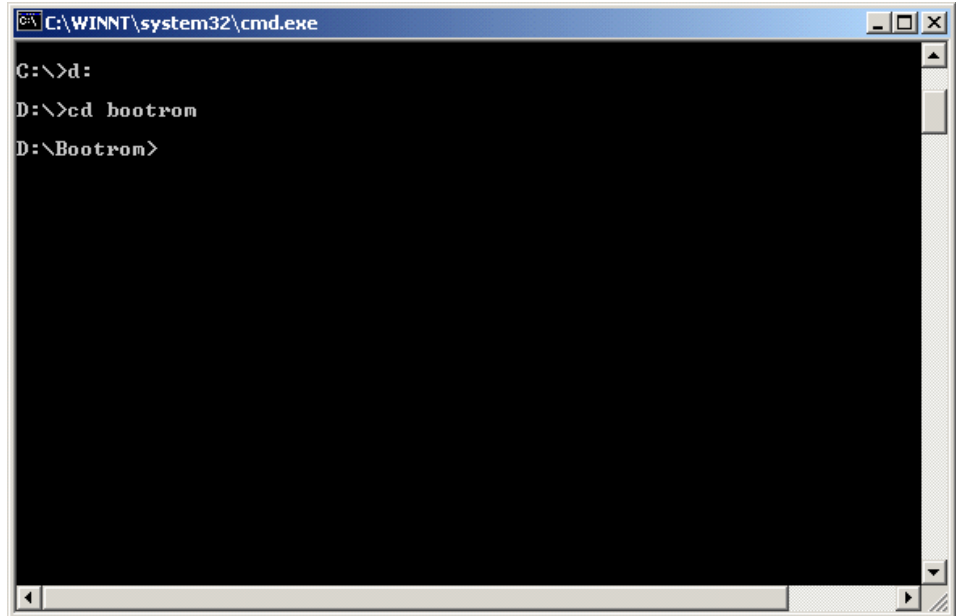
```
[4210-Vlan-interface1] quit
[4210] ftp server enable
[4210] local-user test
New local user added.
[4210-luser-test] password simple pass
[4210-luser-test] service-type ftp
```

- d Enable FTP client software on the PC. Refer to Figure 166 for the command line interface in Windows operating system.

Figure 166 Command line interface

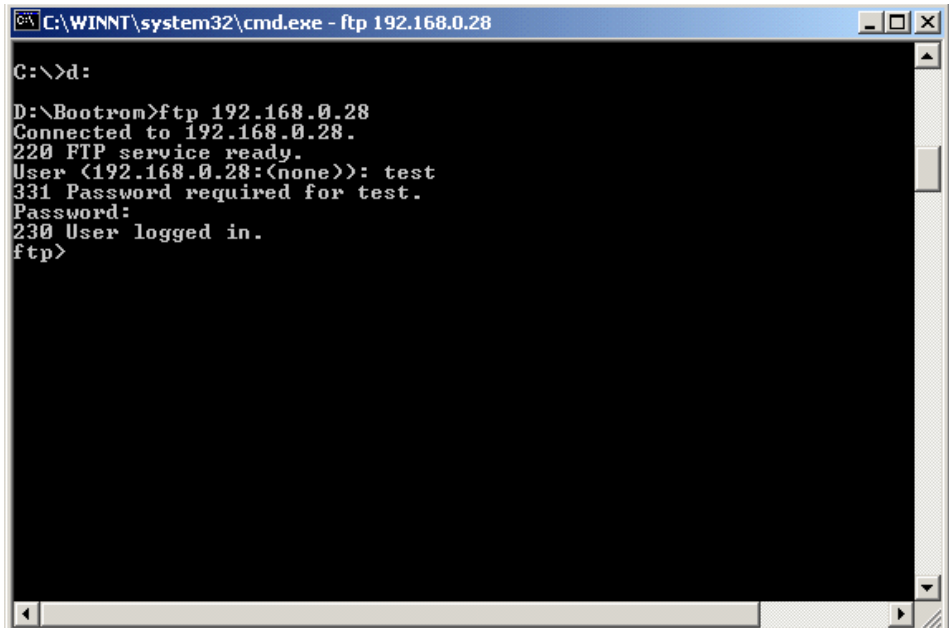


- e Use the **cd** command on the interface to enter the path that the Boot ROM upgrade file is to be stored. Assume the name of the path is D:Bootrom, as shown in Figure 167.

Figure 167 Enter Boot ROM directoryA screenshot of a Windows command prompt window. The title bar reads "C:\WINNT\system32\cmd.exe". The command history shows: "C:\>d:", "D:\>cd bootrom", and "D:\Bootrom>".

```
C:\WINNT\system32\cmd.exe
C:\>d:
D:\>cd bootrom
D:\Bootrom>
```

- f Enter **ftp 192.168.0.28** and enter the user name test, password pass, as shown in Figure 168, to log on to the FTP server.

Figure 168 Log on to the FTP serverA screenshot of a Windows command prompt window. The title bar reads "C:\WINNT\system32\cmd.exe - ftp 192.168.0.28". The command history shows: "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.", and "ftp>".

```
C:\WINNT\system32\cmd.exe - ftp 192.168.0.28
C:\>d:
D:\Bootrom>ftp 192.168.0.28
Connected to 192.168.0.28.
220 FTP service ready.
User (192.168.0.28:(none)): test
331 Password required for test.
Password:
230 User logged in.
ftp>
```

- g Use the **put** command to upload the file switch.btm to the switch, as shown in Figure 169.

Figure 169 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>

```

- h** Configure switch.btm to be the Boot ROM at next startup, and then restart the switch.

```

<4210> boot bootrom switch.btm
This will update Bootrom on unit 1. Continue? [Y/N] y
Upgrading Bootrom, please wait...
Upgrade Bootrom succeeded!
<4210> 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.

Only the configuration steps concerning loading are listed here. For detailed description of the corresponding configuration commands, refer to the “FTP and SFTP Configuration” on page 429 and “TFTP Configuration” on page 445.

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.

Basic System Configuration

Table 354 Basic System Configuration

Operation	Command	Description
Set the current date and time of the system	clock datetime <i>HH:MM:SS</i> { <i>YYYY/MM/DD</i> <i>MM/DD/YYYY</i> }	Required Execute this command in user view. The default value is 23:55:00 04/01/2000 when the system starts up.
Set the local time zone	clock timezone <i>zone-name</i> { add minus } <i>HH:MM:SS</i>	Optional Execute this command in user view. By default, it is the UTC time zone.
Set the name and time range of the summer time	clock summer-time <i>zone_name</i> { one-off repeating } <i>start-time start-date end-time end-date offset-time</i>	Optional Execute this command in user view. <ul style="list-style-type: none">■ When the system reaches the specified start time, it automatically adds the specified offset to the current time, so as to toggle the system time to the summer time.■ When the system reaches the specified end time, it automatically subtracts the specified offset from the current time, so as to toggle the summer time to normal system time.
Enter system view from user view	system-view	-
Set the system name of the switch	sysname <i>sysname</i>	Optional By default, the name is 4210.
Return from current view to lower level view	quit	Optional If the current view is user view, you will quit the current user interface.
Return from current view to user view	return	Optional The composite key <Ctrl+Z> has the same effect with the return command.

Displaying the System Status

You can use the following **display** commands to check the status and configuration information about the system. For information about protocols and ports, and the associated **display** commands, refer to relevant sections.

Table 355 System information display commands

Operation	Command	Description
Display the current date and time of the system	display clock	You can execute the display commands 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

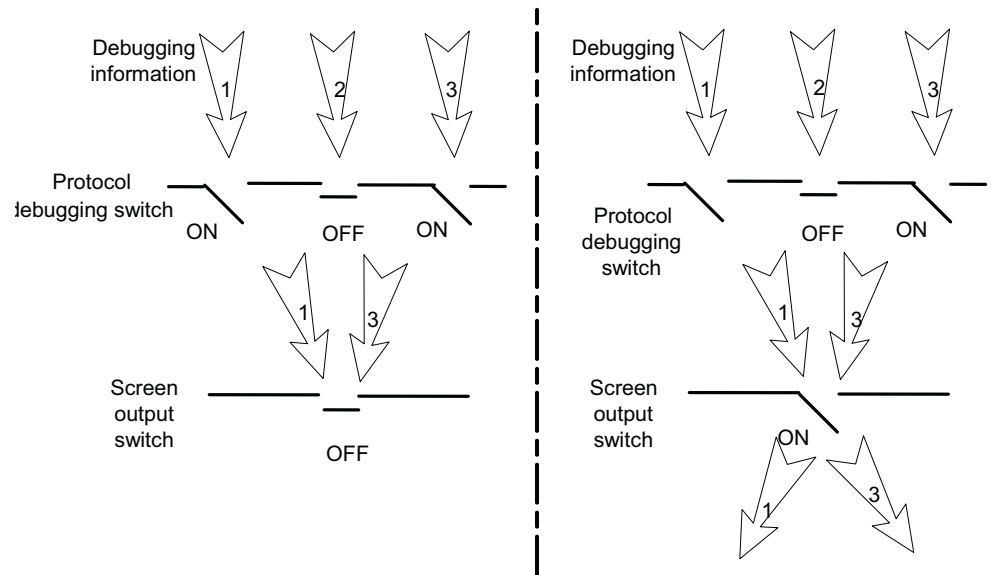
The device provides various debugging functions. For the majority of protocols and features supported, the system provides corresponding debugging information to help users diagnose errors.

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 170 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 170 The relationship between the protocol and screen debugging switch



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” on page 451.

You can use the following commands to enable the two switches.

Table 356 Enable debugging and terminal display for a specific module

Operation	Command	Description
Enable system debugging for specific module	debugging <i>module-name</i> [<i>debugging-option</i>]	Required Disabled for all modules by default.
Enable terminal display for debugging	terminal debugging	Required Disabled by default.



CAUTION: The output of debugging information affects the system operation. Disable all debugging after you finish the system debugging.

Displaying Debugging Status

Table 357 Display the current debugging status in the system

Operation	Command	Description
Display all enabled debugging on the switch	display debugging [<i>unit unit-id</i>] [interface <i>interface-type interface-number</i>] [<i>module-name</i>]	You can execute the display command 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.

Table 358 Display the current operation information about the modules in the system.

Operation	Command	Description
Display the current operation information about the modules in the system.	display diagnostic-information	You can use this command in any view. You should execute this command twice to find the difference between the two executing results, thus helping locate the problem.

43

NETWORK CONNECTIVITY TEST

Network Connectivity Test

ping You can use the **ping** command to check the network connectivity and the reachability of a host.

Table 359 The ping command

Operation	Command	Description
Check the IP network connectivity and the reachability of a host	ping [-a <i>ip-address</i>] [-c <i>count</i>] [-d] [-f] [-h <i>tth</i>] [-i <i>interface-type</i>] [-i <i>interface-number</i>] [ip] [-n] [-p <i>pattern</i>] [-q] [-s <i>packet-size</i>] [-t <i>timeout</i>] [-tos <i>tos</i>] [-v] <i>host</i>	You can execute this command in any view.

This command can output the following results:

- Response status for each ping packet. If no response packet is received within the timeout time, the message "Request time out" is displayed. Otherwise, the number of data bytes, packet serial number, TTL (time to live) and response time of the response packet are displayed.
- Final statistics, including the numbers of sent packets and received response packets, the irresponsive packet percentage, and the minimum, average and maximum values of response time.

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.

Table 360 The `tracert` command

Operation	Command	Description
View the gateways that a packet passes from the source host to the destination	tracert [-a <i>source-ip</i>] [-f <i>first-ttl</i>] [-m <i>max-ttl</i>] [-p <i>port</i>] [-q <i>num-packet</i>] [-w <i>timeout</i>] <i>string</i>	You can execute the tracert command in any view.

Device Management Configuration

Device Management Configuration Tasks

Table 361 Device management configuration tasks

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

Rebooting the Ethernet Switch

You can perform the following operation in user view when the switch is faulty or needs to be rebooted.



Before rebooting, the system checks whether there is any configuration change. If yes, it prompts whether or not to proceed. This prevents the system from losing the configurations in case of shutting down the system without saving the configurations

Table 362 Reboot the Ethernet switch

Operation	Command	Description
Reboot the Ethernet switch	reboot [unit <i>unit-id</i>]	Available in user view

Scheduling a Reboot on the Switch

After you schedule a reboot on the switch, the switch will reboot at the specified time.

Table 363 Schedule a reboot on the switch

Operation	Command	Description
Schedule a reboot on the switch, and set the reboot date and time	schedule reboot at <i>hh:mm</i> [<i>mm/dd/yyyy</i> <i>yyyy/mm/dd</i>]	Optional
Schedule a reboot on the switch, and set the delay time for reboot	schedule reboot delay { <i>hh:mm</i> <i>mm</i> }	Optional
Enter system view	system-view	-
Schedule a reboot on the switch, and set the reboot period	schedule reboot regularity at <i>hh:mm period</i>	Optional



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.

Table 364 Configure real-time monitoring of the running status of the system

Operation	Command	Description
Enter system view	system-view	-
Enable real-time monitoring of the running status of the system	system-monitor enable	Optional Enabled by default.



CAUTION: Enabling of this function consumes some amounts of CPU resources. Therefore, if your network has a high CPU usage requirement, you can disable this function to release your CPU resources.

Specifying the APP to be Used at Reboot

APP is the host software of the switch. If multiple APPs exist in the Flash memory, you can use the command here to specify the one that will be used when the switch reboots.

Table 365 Specify the APP to be used at reboot

Operation	Command	Description
Specify the APP to be used at reboot	boot boot-loader [backup-attribute] { <i>file-url</i> [fabric] <i>device-name</i> }	Required

Upgrading the Boot ROM

You can use the Boot ROM program saved in the Flash memory of the switch to upgrade the running Boot ROM. With this command, a remote user can conveniently upgrade the BootRom by uploading the Boot ROM to the switch through FTP and running this command. The Boot ROM can be used when the switch restarts.

Table 366 Upgrade the Boot ROM

Operation	Command	Description
Upgrade the Boot ROM	boot bootrom { <i>file-url</i> <i>device-name</i> }	Required

Displaying the Device Management Configuration

After the above configurations, you can execute the **display** command in any view to display the operating status of the device management to verify the configuration effects.

Table 367 Display the operating status of the device management

Operation	Command	Description
Display the APP to be adopted at next startup	display boot-loader [unit <i>unit-id</i>]	You can execute the display command in any view.
Display the module type and operating status of each board	display device [manuinfo [unit <i>unit-id</i>]	
Display CPU usage of a switch	display cpu [unit <i>unit-id</i>]	
Display memory usage of a switch	display memory [unit <i>unit-id</i>]	
Display the operating status of the fan	display fan [unit <i>unit-id</i> [fan-id]]	
Display the environment temperature of the switch	display environment	
Display the operating status of the power supply	display power [unit <i>unit-id</i> [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 the switch	display debugging [unit <i>unit-id</i>] [interface <i>interface-type</i> <i>interface-number</i>] [<i>module-name</i>]	

Remote Switch APP Upgrade Configuration Example

Network requirements

Telnet to the switch from a PC remotely and download applications from the FTP server to the Flash memory of the switch. Update the switch software by using the device management commands through CLI.

The switch acts as the FTP client, and the remote PC serves as both the configuration PC and the FTP server.

Perform the following configuration on the FTP server.

- Configure an FTP user, whose name is switch and password is hello. Authorize the user with the read-write right on the directory Switch on the PC.
- Make configuration so that the IP address of a VLAN interface on the switch is 1.1.1.1, the IP address of the PC is 2.2.2.2, and the switch and the PC is reachable to each other.

The host software switch.bin and the Boot ROM file boot.btm of the switch are stored in the directory **switch** on the PC. Use FTP to download the switch.bin and boot.btm files from the FTP server to the switch.

Network diagram

Figure 171 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.



Refer to “Logging into an Ethernet Switch” on page 21 for configuration commands and steps about using telnet.

- 3 Execute the **telnet** command on the PC to log into the switch. The following prompt appears:

```
<4210>
```



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.

```

<4210> ftp 2.2.2.2
Trying ...
Press CTRL+K to abort
Connected.
220 WFTPD 2.0 service (by Texas Imperial Software) ready for new user
User(none):switch
331 Give me your password, please
Password:*****
230 Logged in successfully
[ftp]
  
```

- 5 Enter the authorized path on the FTP server.

```
[ftp] cd switch
```

- 6 Execute the **get** command to download the switch.bin and boot.btm files on the FTP server to the Flash memory of the switch.

```

[ftp] get switch.bin
[ftp] get boot.btm
  
```

- 7 Execute the **quit** command to terminate the FTP connection and return to user view.

```

[ftp] quit
<4210>
  
```

- 8 Upgrade the Boot ROM.

```

<4210> 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.

```
<4210> boot boot-loader switch.bin
The specified file will be booted next time on unit 1!
<4210> display boot-loader
Unit 1:
The current boot app is: switch.bin
The main boot app is:   switch.bin
The backup boot app is:
```

Reboot the switch to upgrade the Boot ROM and host software of the switch.

```
<4210> 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
```


45

REMOTE-PING CONFIGURATION

Remote-Ping Overview

Introduction to Remote-Ping

Remote-Ping (pronounced Hua'Wei 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.

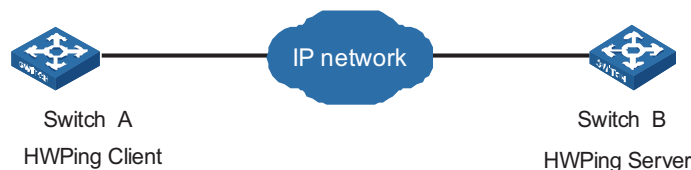
All Remote-Ping tests are initiated by Remote-Ping client and you can view the test results on Remote-Ping client only.

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 172 Remote-Ping illustration



Test Types Supported by Remote-Ping

Table 368 Test types supported by Remote-Ping

Supported test types	Description
ICMP test	For these types of tests, you need to configure Remote-Ping client and corresponding servers.
DHCP test	
FTP test	
HTTP test	
DNS test	
SNMP test	
Jitter test	
TCP test	<ul style="list-style-type: none"> ■ These types of tests need the cooperation of Remote-Ping client and Remote-Ping Server. ■ Do not perform TCP or UDP test on port 1 to 1023 (well-known ports). Otherwise your Remote-Ping test may fail or cause the service corresponding to the well-known port (1 to 1023) being unavailable.
Tcppublic test	
Tcprivate test	
UDP test	
Udppublic test	
Udprivate test	



Caution: The Switch 4210 does not support Remote-Ping DNS tests.

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 Remote-Ping client, refer to “Remote-Ping Client Configuration” on page 499.

Table 369 Remote-Ping test parameters

Test parameter	Description
Destination address (destination-ip)	For 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 tcprivate/udprivate/jitter test, you must specify a destination port number, and the destination port number must be the port number of a TCP or UDP listening service configured on the Remote-Ping server.
Source interface (source-interface)	<ul style="list-style-type: none"> ■ For DHCP test, you must specify a source interface, which will be used by Remote-Ping client to send DHCP requests. If no source interface is specified for a DHCP test, the test will not succeed. ■ After a source interface is specified, Remote-Ping client uses this source interface to send DHCP requests during a DHCP test. ■ The IP address of the specified source interface will be used as the source IP address of DHCP requests.

Table 369 Remote-Ping test parameters

Test parameter	Description
Source address (source-ip)	For Remote-Ping tests other than DHCP test, 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 type (test-type)	<ul style="list-style-type: none"> ■ You can use Remote-Ping to test a variety of protocols, see Table 368 for details. ■ To perform a type of test, you must first create a test group of this type. One test group can be of only one Remote-Ping test type.
Number of probes per test (count)	<ul style="list-style-type: none"> ■ 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)	<ul style="list-style-type: none"> ■ For ICMP/UDP/jitter test, you can configure the size of test packets. ■ For ICMP test, the ICMP packet size refers to the length of ECHO-REQUEST packets (excluding IP and ICMP headers)
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)	<ul style="list-style-type: none"> ■ The probe timeout timer is started after the Remote-Ping client sends out a test packet. ■ This parameter is in seconds.
Type of service (tos)	Type of service is the value of the ToS field in IP header in the test packets.
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.
HTTP operation string and version (http-string) and FTP server.	This parameter is used to set the HTTP operation string and version in an HTTP test.

Table 369 Remote-Ping test parameters

Test parameter	Description
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)	<ul style="list-style-type: none"> ■ Jitter test is used to collect statistics about delay jitter in UDP packet transmission ■ 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.
Trap	<ul style="list-style-type: none"> ■ 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. ■ 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.

Configuration on a Remote-Ping Server

You can enable both the Remote-Ping client and Remote-Ping server functions on a Switch 4210, that is, the switch can serve as a Remote-Ping client and server simultaneously.

Remote-Ping server configuration tasks

Table 370 Remote-Ping server configuration tasks

Item	Description	Related section
Enable the Remote-Ping server function	The Remote-Ping server function is needed only for jitter, TCP, and UDP tests.	"Remote-Ping server configuration"
Configure a listening service on the Remote-Ping server	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 server configuration"

Remote-Ping server configuration

Table 371 describes the configuration on Remote-Ping server, which is the same for Remote-Ping test types that need to configure Remote-Ping server.

Table 371 Remote-Ping server configuration

Operation	Command	Description
Enter system view	system-view	-
Enable the Remote-Ping server function	Remote-Ping-server enable	Required Disabled by default.
Configure a UDP listening service	Remote-Ping-server udpecho <i>ip-address port-num</i>	Required for UDP and jitter tests By default, no UDP listening service is configured.
Configure a TCP listening service	Remote-Ping-server tcpconnect <i>ip-address port-num</i>	Required for TCP tests By default, no TCP listening service is configured.

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

Table 372 Configure ICMP test on Remote-Ping client

Operation	Command	Description
Enter system view	system-view	-
Enable the Remote-Ping client function	Remote-Ping-agent enable	Required By default, the Remote-Ping client function is disabled.

Table 372 Configure ICMP test on Remote-Ping client

Operation	Command	Description
Create a Remote-Ping test group and enter its view	Remote-Ping <i>administrator-name</i> <i>operation-tag</i>	Required By default, no test group is configured.
Configure the destination IP address	destination-ip <i>ip-address</i>	Required By default, no destination address is configured.
Configure the source IP address	source-ip <i>ip-address</i>	Optional By default, no source IP address is configured.
Configure the test type	test-type icmp	Optional By default, the test type is ICMP.
Configure the number of probes per test	count <i>times</i>	Optional By default, each test makes one probe.
Configure the packet size	datasize <i>size</i>	Optional By default, the packet size is 56 bytes.
Configure the maximum number of history records that can be saved	history-records <i>number</i>	Optional By default, the maximum number is 50.
Configure the automatic test interval	frequency <i>interval</i>	Optional By default, the automatic test interval is zero seconds, indicating no automatic test will be made.
Configure the probe timeout time	timeout <i>time</i>	Optional By default, a probe times out in three seconds.
Configure the type of service (ToS)	tos <i>value</i>	Optional By default, the service type is zero.
Start the test	test-enable	Required
Display test results	display Remote-Ping results [<i>admin-name</i> <i>operation-tag</i>]	Required Available in any view.



For a Remote-Ping ICMP test, if no IP address is configured for the source interface configured through the source-interface command, the test cannot be performed; if a source IP address has already been configured through the source-ip command, the source-interface command does not take effect.

2 Configuring DHCP test on Remote-Ping client

Table 373 Configure DHCP test on Remote-Ping client

Operation	Command	Description
Enter system view	system-view	-

Table 373 Configure DHCP test on Remote-Ping client

Operation	Command	Description
Enable the Remote-Ping client function	Remote-Ping-agent enable	Required By default, the Remote-Ping client function is disabled.
Create a Remote-Ping test group and enter its view	Remote-Ping <i>administrator-name</i> <i>operation-tag</i>	Required By default, no test group is configured.
Configure the source interface	source-interface <i>interface-type</i> <i>interface-number</i>	Required You can only configure a VLAN interface as the source interface. By default, no source interface is configured.
Configure the test type	test-type dhcp	Required By default, the test type is ICMP.
Configure the number of probes per test	count <i>times</i>	Optional By default, each test makes one probe.
Configure the maximum number of history records that can be saved	history-records <i>number</i>	Figure 173 Optional By default, the maximum number is 50.
Configure the probe timeout time	timeout <i>time</i>	Optional By default, a probe times out in three seconds.
Start the test	test-enable	Required
Display test results	display Remote-Ping results [<i>admin-name</i> <i>operation-tag</i>]	Required You can execute the command in any view.

3 Configuring FTP test on Remote-Ping client

Table 374 Configure FTP test on Remote-Ping client

Operation	Command	Description
Enter system view	system-view	-
Enable the Remote-Ping client function	Remote-Ping-agent enable	Required By default, the Remote-Ping client function is disabled.
Create a Remote-Ping test group and enter its view	Remote-Ping <i>administrator-name</i> <i>operation-tag</i>	Required By default, no test group is configured.
Configure the destination IP address	destination-ip <i>ip-address</i>	Required By default, no destination address is configured.
Configure the source IP address	source-ip <i>ip-address</i>	Required By default, no source IP address is configured.

Table 374 Configure FTP test on Remote-Ping client

Operation	Command	Description
Configure the source port	source-port <i>port-number</i>	Optional By default, no source port is configured.
Configure the test type	test-type ftp	Required By default, the test type is ICMP.
Configure the number of probes per test	count <i>times</i>	Optional By default, each test makes one probe.
Configure the maximum number of history records that can be saved	history-records <i>number</i>	Figure 174 Optional By default, the maximum number is 50.
Configure the automatic test interval	frequency <i>interval</i>	Optional By default, the automatic test interval is zero seconds, indicating no automatic test will be made.
Configure the probe timeout time	timeout <i>time</i>	Optional By default, a probe times out in three seconds.
Configure the type of service	tos <i>value</i>	Optional By default, the service type is zero.
Configure the type of FTP operation	ftp-operation { get put }	Optional By default, the type of FTP operation is get , that is, the FTP operation will get a file from the FTP server.
Configure an FTP login username	username <i>name</i>	Required
Configure an FTP login password	password <i>password</i>	By default, neither username nor password is configured.
Configure a file name for the FTP operation	filename <i>file-name</i>	Required By default, no file name is configured for the FTP operation
Start the test	test-enable	Required
Display test results	display Remote-Ping results [<i>admin-name operation-tag</i>]	Required You can execute the command in any view.

4 Configuring HTTP test on Remote-Ping client

Table 375 Configure HTTP test on Remote-Ping client

Operation	Command	Description
Enter system view	system-view	-

Table 375 Configure HTTP test on Remote-Ping client

Operation	Command	Description
Enable the Remote-Ping client function	Remote-Ping-agent enable	Required By default, the Remote-Ping client function is disabled.
Create a Remote-Ping test group and enter its view	Remote-Ping <i>administrator-name</i> <i>operation-tag</i>	Required By default, no test group is configured.
Configure the destination IP address	destination-ip <i>ip-address</i>	Required When you use Switche 4210 as Remote-Ping Client for http test, the destination address can be host name or IP address. When you use Switche 4210 as Remote-Ping Client for http test, the destination address can only be IP address.
Configure dns-server	dns-server <i>ip-address</i>	Required: When you use 3Com's Switche 4210 Family as a Remote-Ping Client for http test and set the destination address as host name.
Configure the source IP address	source-ip <i>ip-address</i>	Optional By default, no source IP address is configured.
Configure the source port	source-port <i>port-number</i>	Optional By default, no source port is configured.
Configure the test type	test-type http	Required By default, the test type is ICMP.
Configure the number of probes per test	count <i>times</i>	Optional By default, each test makes one probe.
Configure the maximum number of history records that can be saved	history-records <i>number</i>	Optional By default, the maximum number is 50.
Configure the automatic test interval	frequency <i>interval</i>	Optional By default, the automatic test interval is zero seconds, indicating no automatic test will be made.
Configure the probe timeout time	timeout <i>time</i>	Optional By default, a probe times out in three seconds.
Configure the type of service	tos <i>value</i>	Optional By default, the service type is zero.

Table 375 Configure HTTP test on Remote-Ping client

Operation	Command	Description
Configure the type of HTTP operation	http-operation { get post }	Optional By default, the type of HTTP operation is get , that is, the HTTP operation will get data from the HTTP server.
Configure the HTTP operation string and version in an HTTP test	http-string <i>string</i> <i>version</i>	Required By default, HTTP operation string and version are not configured.
Start the test	test-enable	Required
Display test results	display Remote-Ping results [<i>admin-name</i> <i>operation-tag</i>]	Required You can execute the command in any view.

5 Configuring jitter test on Remote-Ping client

Table 376 Configure jitter test on Remote-Ping client

Operation	Command	Description
Enter system view	system-view	-
Enable the Remote-Ping client function	Remote-Ping-agent enable	Required By default, the Remote-Ping client function is disabled.
Create a Remote-Ping test group and enter its view	Remote-Ping <i>administrator-name</i> <i>operation-tag</i>	Required By default, no test group is configured.
Configure the destination IP address	destination-ip <i>ip-address</i>	Required The destination address must be the IP address of a UDP listening service on the Remote-Ping server. By default, no destination address is configured.
Configure the destination port	destination-port <i>Port-number</i>	Required The destination port must be the port of a UDP listening service on the Remote-Ping server. By default, no destination port is configured.
Configure the source IP address	source-ip <i>ip-address</i>	Optional By default, no source IP address is configured.
Configure the source port	source-port <i>port-number</i>	Optional By default, no source port is configured.
Configure the test type	test-type jitter	Required By default, the test type is ICMP.

Table 376 Configure jitter test on Remote-Ping client

Operation	Command	Description
Configure the number of probes per test	count <i>times</i>	Optional By default, each test makes one probe.
Configure the maximum number of history records that can be saved	history-records <i>number</i>	Figure 175 Optional By default, the maximum number is 50.
Configure the packet size	datasize <i>size</i>	Optional By default, the packet size is 68 bytes.
Configure the automatic test interval	frequency <i>interval</i>	Optional By default, the automatic test interval is zero seconds, indicating no automatic test will be made.
Configure the probe timeout time	timeout <i>time</i>	Optional By default, a probe times out in three seconds.
Configure the type of service	tos <i>value</i>	Optional By default, the service type is zero.
Configure the number of test packets that will be sent in each jitter probe	jitter-packetnum <i>number</i>	Optional By default, each jitter probe will send 10 packets.
Configure the interval to send test packets in the jitter test	jitter-interval <i>interval</i>	Optional By default, the interval is 20 milliseconds.
Start the test	test-enable	Required
Display test results	display Remote-Ping results [<i>admin-name operation-tag</i>]	Required You can execute the command in any view.

6 Configuring SNMP test on Remote-Ping client

Table 377 Configure SNMP test on Remote-Ping client

Operation	Command	Description
Enter system view	system-view	-
Enable the Remote-Ping client function	Remote-Ping-agent enable	Required By default, the Remote-Ping client function is disabled.
Create a Remote-Ping test group and enter its view	Remote-Ping <i>administrator-name operation-tag</i>	Required By default, no test group is configured.
Configure the destination IP address	destination-ip <i>ip-address</i>	Required By default, no destination address is configured.

Table 377 Configure SNMP test on Remote-Ping client

Operation	Command	Description
Configure the source IP address	source-ip <i>ip-address</i>	Optional By default, no source IP address is configured.
Configure the source port	source-port <i>port-number</i>	Optional By default, no source port is configured.
Configure the test type	test-type snmpquery	Required By default, the test type is ICMP.
Configure the number of probes per test	count <i>times</i>	Optional By default, each test makes one probe.
Configure the maximum number of history records that can be saved	history-records <i>number</i>	Figure 176 Optional By default, the maximum number is 50.
Configure the automatic test interval	frequency <i>interval</i>	Optional By default, the automatic test interval is zero seconds, indicating no automatic test will be made.
Configure the probe timeout time	timeout <i>time</i>	Optional By default, a probe times out in three seconds.
Configure the type of service	tos <i>value</i>	Optional By default, the service type is zero.
Start the test	test-enable	Required
Display test results	display Remote-Ping results [<i>admin-name operation-tag</i>]	Required You can execute the command in any view.

7 Configuring TCP test on Remote-Ping client

Table 378 Configure TCP test on Remote-Ping client

Operation	Command	Description
Enter system view	system-view	-
Enable the Remote-Ping client function	Remote-Ping-agent enable	Required 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 By default, no test group is configured.

Table 378 Configure TCP test on Remote-Ping client

Operation	Command	Description
Configure the destination address	destination-ip ip-address	Required This IP address and the one configured on the Remote-Ping server for listening services must be the same. By default, no destination address is configured.
Configure the destination port	destination-port port-number	Required in a Tcpprivate test 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. By default, no destination port number is configured.
Configure the source IP address	source-ip ip-address	Optional By default, the source IP address is not specified.
Configure the source port	source-port port-number	Optional By default, no source port is specified.
Configure the test type	test-type { tcpprivate tcppublic }	Required By default, the test type is ICMP.
Configure the number of probes per test	count times	Optional By default, one probe is made per time.
Configure the automatic test interval	frequency interval	Optional By default, the automatic test interval is zero seconds, indicating no automatic test will be made.
Configure the probe timeout time	timeout time	Optional By default, a probe times out in three seconds.
Configure the maximum number of history records that can be saved	history-records number	Figure 177 Optional By default, the maximum number is 50.
Configure the type of service	tos value	Optional By default, the service type is zero.
Start the test	test-enable	Required

Table 378 Configure TCP test on Remote-Ping client

Operation	Command	Description
Display test results	display Remote-Ping results [admin-name operation-tag]	Required The display command can be executed in any view.

8 Configuring UDP test on Remote-Ping client

Table 379 Configure UDP test on Remote-Ping client

Operation	Command	Description
Enter system view	system-view	-
Enable the Remote-Ping client function	Remote-Ping-agent enable	Required 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 By default, no test group is configured.
Configure the destination address	destination-ip ip-address	Required This IP address and the one configured on the Remote-Ping server for listening service must be the same. By default, no destination address is configured.
Configure the destination port	destination-port port-number	<ul style="list-style-type: none"> ■ Required in a Udpprivate test ■ 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. ■ By default, no destination port number is configured.
Configure the source IP address	source-ip ip-address	Optional By default, no source IP address is configured.
Configure the source port	source-port port-number	Optional By default, no source port is specified.
Configure the test type	test-type { udpprivate udppublic }	Required By default, the test type is ICMP.

Table 379 Configure UDP test on Remote-Ping client

Operation	Command	Description
Configure the number of probes per test	count times	Optional By default, one probe is made per test.
Configure the maximum number of history records that can be saved	history-records <i>number</i>	Figure 178 Optional By default, the maximum number is 50.
Configure the data packet size	datasize size	Optional By default, the data packet size is 100 bytes.
Configure the automatic test interval	frequency interval	Optional By default, the automatic test interval is zero seconds, indicating no automatic test will be made.
Configure the probe timeout time	timeout time	Optional By default, a probe times out in three seconds.
Configure the service type	tos value	Optional 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 The display command can be executed in any view.

9 Configuring DNS test on Remote-Ping client

Table 380 Configure DNS test on Remote-Ping client

Operation	Command	Description
Enter system view	system-view	-
Enable the Remote-Ping client function	Remote-Ping-agent enable	Required 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 By default, no test group is configured.
Configure the source IP address	source-ip ip-address	Optional By default, no source IP address is specified.
Configure the test type	test-type dns	Required By default, the test type is ICMP.
Configure the number of probes per test	count times	Optional By default, one probe is made per test.

Table 380 Configure DNS test on Remote-Ping client

Operation	Command	Description
Configure the maximum number of history records that can be saved	history-records <i>number</i>	Figure 179 Optional By default, the maximum number is 50.
Configure the automatic test interval	frequency interval	Optional By default, the automatic test interval is zero seconds, indicating no automatic test will be made.
Configure the probe timeout time	timeout time	Optional By default, a probe times out in three seconds.
Configure the type of service	tos value	Optional By default, the service type is zero.
Configure the domain name to be resolved	dns resolve-targetdomainname	Required 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 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 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.

Table 381 Configure the Remote-Ping client to send Trap messages

Operation	Command	Description
Enter system view	system-view	-
Enable the Remote-Ping client function	Remote-Ping-agent enable	Required 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 By default, no test group is configured.
Enable the Remote-Ping client to send Trap messages	send-trap { all { probefailure testcomplete testfailure }* }	Required By default, Trap sending is disabled.
Configure the number of consecutive unsuccessful Remote-Ping tests before Trap output	test-failtimes times	Optional By default, Trap messages are sent each time a test fails.

Table 381 Configure the Remote-Ping client to send Trap messages

Operation	Command	Description
Configure the number of consecutive unsuccessful Remote-Ping probes before Trap output	probe-failtimes times	Optional By default, Trap messages are sent each time a probe fails.

Displaying Remote-Ping Configuration

After the above-mentioned configuration, you can use the **display** commands to view the results of the latest test and history information.

Table 382 Display Remote-Ping test results

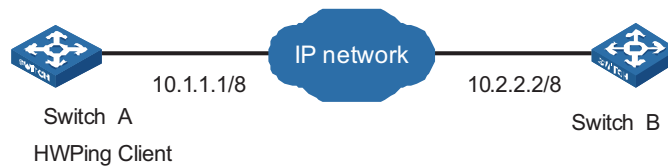
Operation	Command	Description
Display test history	display Remote-Ping history [administrator-name operation-tag]	Available in any view.
Display the results of the latest test	display Remote-Ping results [administrator-name operation-tag]	

Remote-Ping Configuration Example

ICMP Test Network requirements

The Switch 4210 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 180 Network diagram for the ICMP test

Configuration procedure

- Configure Remote-Ping Client (Switch A):

Enable Remote-Ping client.

```
<4210> system-view
[4210] Remote-Ping-agent enable
```

Create a Remote-Ping test group, setting the administrator name to "administrator" and test tag to "ICMP".

```
[4210] Remote-Ping administrator icmp
```

Configure the test type as **icmp**.

```
[4210-Remote-Ping-administrator-icmp] test-type icmp
# Configure the destination IP address as 10.2.2.2.
[4210-Remote-Ping-administrator-icmp] destination-ip 10.2.2.2
# Configure to make 10 probes per test.
[4210-Remote-Ping-administrator-icmp] count 10
# Set the probe timeout time to 5 seconds.
[4210-Remote-Ping-administrator-icmp] timeout 5
# Start the test.
[4210-Remote-Ping-administrator-icmp] test-enable
# Set the maximum number of history records that can be saved to 5.
[4210-Remote-Ping-administrator-icmp] history-records 5
# Display test results.

[4210-Remote-Ping-administrator-icmp] display Remote-Ping results administrator i
cmp
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
[4210-Remote-Ping-administrator-icmp] display Remote-Ping history administrator i
cmp
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
```

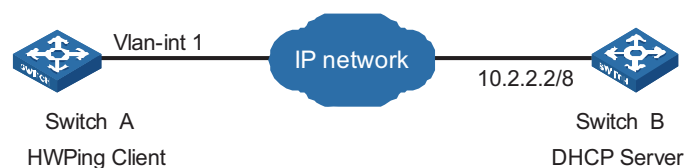
For detailed output description, see the corresponding command manual.

DHCP Test Network requirements

Both the Remote-Ping client and the DHCP server are Switch 4210s. 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 181 Network diagram for the DHCP test



Configuration procedure

- Configure DHCP Server(Switch B):
- Configure Remote-Ping Client (Switch A):

Enable the Remote-Ping client.

```
<4210> system-view
[4210] Remote-Ping-agent enable

# Create a Remote-Ping test group, setting the administrator name to
"administrator" and test tag to "DHCP".

[4210] Remote-Ping administrator dhcp

# Configure the test type as dhcp.

[4210-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.

[4210-Remote-Ping-administrator-dhcp] source-interface Vlan-interface 1

# Configure to make 10 probes per test.

[4210-Remote-Ping-administrator-dhcp] count 10

# Set the probe timeout time to 5 seconds.

[4210-Remote-Ping-administrator-dhcp] timeout 5

# Start the test.

[4210-Remote-Ping-administrator-dhcp] test-enable

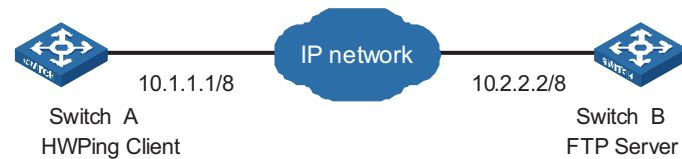
# Display test results

[4210-Remote-Ping-administrator-dhcp] display Remote-Ping results administra
tor 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
[4210-Remote-Ping-administrator-dhcp] display Remote-Ping history administra
tor 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.

FTP Test Network requirements

Both the Remote-Ping client and the FTP server are Switch 4210s. 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 182** 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 "TFTP Configuration" on page 445.
- Configure Remote-Ping Client (Switch A):
Configure the IP address for the Ethernet interface.

```
<4210> system-view
[4210] interface Vlan-interface 1
[4210-Vlan-interface1] ip address 10.1.1.1 8
# Enable the Remote-Ping client.
[4210] Remote-Ping-agent enable
# Create a Remote-Ping test group, setting the administrator name to
"administrator" and test tag to "FTP".
[4210] Remote-Ping administrator ftp
# Configure the test type as ftp.
[4210-Remote-Ping-administrator-ftp] test-type ftp
# Configure the IP address of the FTP server as 10.2.2.2.
[4210-Remote-Ping-administrator-ftp] destination-ip 10.2.2.2
# Configure the FTP login username.
[4210-Remote-Ping-administrator-ftp] username admin
# Configure the FTP login password.
[4210-Remote-Ping-administrator-ftp] password admin
# Configure the type of FTP operation.
[4210-Remote-Ping-administrator-ftp] ftp-operation put
# Configure a file name for the FTP operation.
[4210-Remote-Ping-administrator-ftp] filename cmdtree.txt
# Configure to make 10 probes per test.
[4210-Remote-Ping-administrator-ftp] count 10
```



```

# Set the probe timeout time to 30 seconds.
[4210-Remote-Ping-administrator-ftp] timeout 30
# Configure the source IP address
[4210-Remote-Ping-administrator-ftp] source-ip 10.1.1.1
# Start the test.
[4210-Remote-Ping-administrator-ftp] test-enable
# Display test results
[4210-Remote-Ping-administrator-ftp] display Remote-Ping results administrat
or 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
[4210-Remote-Ping-administrator-ftp] display Remote-Ping history administrat
or 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.



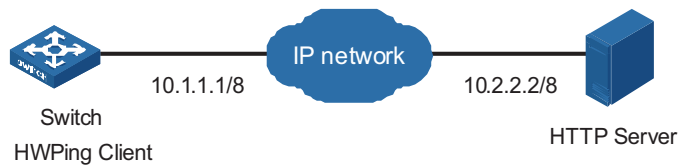
If you are downloading a file from the server, you do not need to specify an FTP operation type. For details, see "Configuring FTP test on Remote-Ping client".

HTTP Test Network requirements

A 3Com Switch 4210 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 183 Network diagram for the HTTP test



Configuration procedure

- Configure the HTTP Server. Use a Windows 2003 Server as the HTTP server and follow the instructions in your Windows 2003 Server documentation.
- Configure Remote-Ping Client (Switch A):
 - # Enable the Remote-Ping client.

```

<4210> system-view
[4210] Remote-Ping-agent enable

# Create a Remote-Ping test group, setting the administrator name to
"administrator" and test tag to "HTTP".

[4210] Remote-Ping administrator http

# Configure the test type as http.

[4210-Remote-Ping-administrator-http] test-type http

# Configure the IP address of the HTTP server as 10.2.2.2.

[4210-Remote-Ping-administrator-http] destination-ip 10.2.2.2

# Configure to make 10 probes per test.

[4210-Remote-Ping-administrator-http] count 10

# Set the probe timeout time to 30 seconds.

[4210-Remote-Ping-administrator-http] timeout 30

# Start the test.

[4210-Remote-Ping-administrator-http] test-enable

# Display test results

[4210-Remote-Ping-administrator-http] display Remote-Ping results administrator h
ttp
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
TCP Connect Min Time: 5
TCP Connect Max Time: 20
TCP Connect Timeout Times: 0
HTTP Operation Min Time: 27
HTTP Operation Max Time: 80
[4210-Remote-Ping-administrator-http] display Remote-Ping history administrator h
ttp
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.



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 Switch 4210s. 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 184 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.

```

<4210> system-view
[4210] Remote-Ping-server enable
[4210] Remote-Ping-server udpecho 10.2.2.2 9000

```

- Configure Remote-Ping Client (Switch A):

Enable the Remote-Ping client.

```

<4210> system-view
[4210] Remote-Ping-agent enable

# Create a Remote-Ping test group, setting the administrator name to
"administrator" and test tag to "Jitter".
[4210] Remote-Ping administrator Jitter

```

```

# Configure the test type as jitter
[4210-Remote-Ping-administrator-Jitter] test-type Jitter
# Configure the IP address of the Remote-Ping server as 10.2.2.2.
[4210-Remote-Ping-administrator-Jitter] destination-ip 10.2.2.2
# Configure the destination port on the Remote-Ping server.
[4210-Remote-Ping-administrator-Jitter] destination-port 9000
# Configure to make 10 probes per test.
[4210-Remote-Ping-administrator-http] count 10
# Set the probe timeout time to 30 seconds.
[4210-Remote-Ping-administrator-Jitter] timeout 30
# Start the test.
[4210-Remote-Ping-administrator-Jitter] test-enable
# Display test results
[4210-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
[4210-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

```

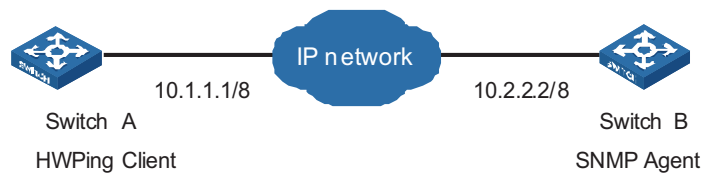
For detailed output description, see the corresponding command manual.

SNMP Test Network requirements

Both the Remote-Ping client and the SNMP Agent are Switch 4210s. 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 185 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
  
```



- 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.

```

<4210> system-view
[4210] Remote-Ping-agent enable

# Create a Remote-Ping test group, setting the administrator name to
"administrator" and test tag to "snmp".
[4210] Remote-Ping administrator snmp

# Configure the test type as snmp.
[4210-Remote-Ping-administrator-snmp] test-type snmpquery

# Configure the destination IP address as 10.2.2.2.
[4210-Remote-Ping-administrator-snmp] destination-ip 10.2.2.2

# Configure to make 10 probes per test.
[4210-Remote-Ping-administrator-snmp] count 10

# Set the probe timeout time to 30 seconds.
  
```

```
[4210-Remote-Ping-administrator-snmp] timeout 30
# Start the test.
[4210-Remote-Ping-administrator-snmp] test-enable
# Display test results
[4210-Remote-Ping-administrator-snmp] display Remote-Ping results administrator s
nmp
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
[4210-Remote-Ping-administrator-snmp] display Remote-Ping history administrator s
nmp
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 (Tcprivate Test) on the Specified Ports

Network requirements

Both the Remote-Ping client and the Remote-Ping server are Switch 4210s. Perform a Remote-Ping Tcprivate test to test time required to establish a TCP connection between this end (Switch A) and the specified destination end (Switch B), with the port number set to 8000.

Network diagram

Figure 186 Network diagram for the Tcprivate test



Configuration procedure

- Configure Remote-Ping Server (Switch B):
 - # Enable the Remote-Ping server and configure the IP address and port to listen on.

```

<4210> system-view
[4210] Remote-Ping-server enable
[4210] Remote-Ping-server tcpconnect 10.2.2.2 8000
■ Configure Remote-Ping Client (Switch A):
  # Enable the Remote-Ping client.

<4210> system-view
[4210] Remote-Ping-agent enable

  # Create a Remote-Ping test group, setting the administrator name to
  "administrator" and test tag to "tcpprivate".

[4210] Remote-Ping administrator tcpprivate

  # Configure the test type as tcpprivate.

[4210-Remote-Ping-administrator-tcpprivate] test-type tcpprivate

  # Configure the IP address of the Remote-Ping server as 10.2.2.2.

[4210-Remote-Ping-administrator-tcpprivate] destination-ip 10.2.2.2

  # Configure the destination port on the Remote-Ping server.

[4210-Remote-Ping-administrator-tcpprivate] destination-port 8000

  # Configure to make 10 probes per test.

[4210-Remote-Ping-administrator-tcpprivate] count 10

  # Set the probe timeout time to 5 seconds.

[4210-Remote-Ping-administrator-tcpprivate] timeout 5

  # Start the test.

[4210-Remote-Ping-administrator-tcpprivate] test-enable

  # Display test results.

[4210-Remote-Ping-administrator-tcpprivate] display Remote-Ping results administr
ator 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
[4210-Remote-Ping-administrator-tcpprivate] display Remote-Ping history administr
ator 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.

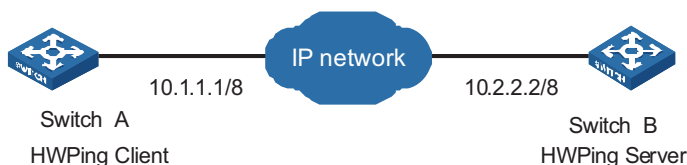
UDP Test (Udpprivate Test) on the Specified Ports

Network requirements

Both the Remote-Ping client and the Remote-Ping server are Switch 4210s. 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 187 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.

```

<4210> system-view
[4210] Remote-Ping-server enable
[4210] Remote-Ping-server udpecho 10.2.2.2 8000
  
```

- Configure Remote-Ping Client (Switch A):
 - # Enable the Remote-Ping client.

```

<4210> system-view
[4210] Remote-Ping-agent enable

# Create a Remote-Ping test group, setting the administrator name to
"administrator" and test tag to "udpprivate".
[4210] Remote-Ping administrator udpprivate

# Configure the test type as udpprivate.
[4210-Remote-Ping-administrator-udpprivate] test-type udpprivate

# Configure the IP address of the Remote-Ping server as 10.2.2.2.
[4210-Remote-Ping-administrator-udpprivate] destination-ip 10.2.2.2

# Configure the destination port on the Remote-Ping server.
[4210-Remote-Ping-administrator-udpprivate] destination-port 8000

# Configure to make 10 probes per test.
[4210-Remote-Ping-administrator-udpprivate] count 10

# Set the probe timeout time to 5 seconds.
[4210-Remote-Ping-administrator-udpprivate] timeout 5

# Start the test.
[4210-Remote-Ping-administrator-udpprivate] test-enable

# Display test results.
  
```



```
[4210-Remote-Ping-administrator-udpprivate] display Remote-Ping results administr
ator 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
[4210-Remote-Ping-administrator-udpprivate] display Remote-Ping history administr
ator 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
```

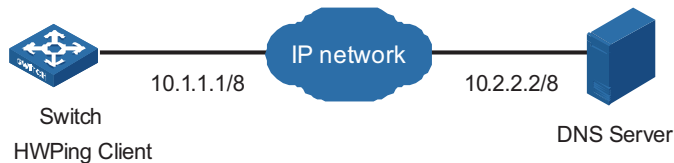
For detailed output description, see the corresponding command manual.

DNS Test Network requirements

A Switch 4210 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 188 Network diagram for the DNS test



Configuration procedure

- Use a Windows 2003 Server as the DNS server and follow the instructions in your Windows 2003 Server documentation to configure that server.
- Configure Remote-Ping Client (Switch A)
 - # Enable the Remote-Ping client.

```
<4210> system-view
[4210] Remote-Ping-agent enable

# Create a Remote-Ping test group, setting the administrator name to
"administrator" and test tag to "dns".

[4210] Remote-Ping administrator dns
```

```

# Configure the test type as dns.
[4210-Remote-Ping-administrator-dns] test-type dns
# Configure the IP address of the DNS server as 10.2.2.2.
[4210-Remote-Ping-administrator-dns] dns-server 10.2.2.2
# Configure to resolve the domain name www.test.com.
[4210-Remote-Ping-administrator-dns] dns resolve-target www.test.com
# Configure to make 10 probes per test.
[4210-Remote-Ping-administrator-dns] count 10
# Set the probe timeout time to 5 seconds.
[4210-Remote-Ping-administrator-dns] timeout 5
# Start the test.
[4210-Remote-Ping-administrator-dns] test-enable
# Display test results.
[4210-Remote-Ping-administrator-dns] display Remote-Ping results administrator dn
s
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
[4210-Remote-Ping-administrator-dns] display Remote-Ping history administrator dn
s
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.

46

IPv6 MANGEMENT CONFIGURATION



- The term "router" in this document refers to a router in a generic sense or an Ethernet switch running a routing protocol.
- 3Com Switch 4210 Family supports IPv6 management features, but does not support IPv6 forwarding and related features.

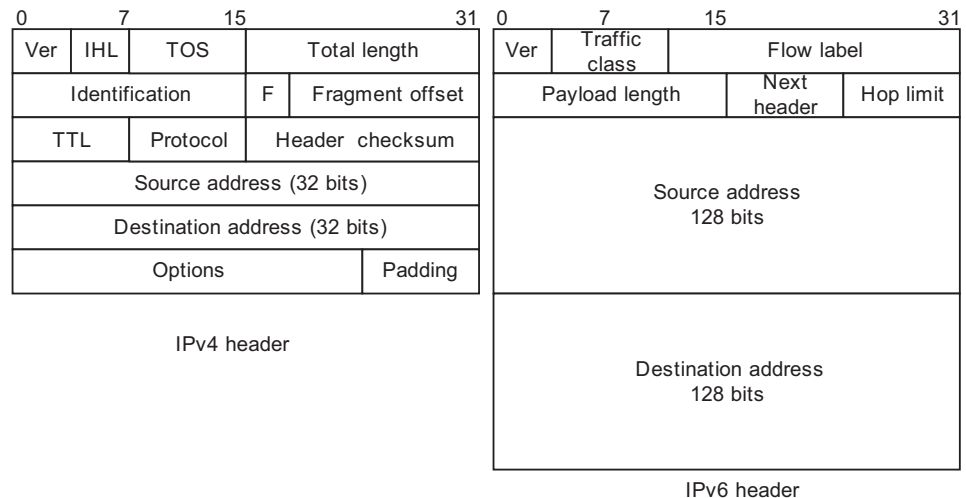
IPv6 Overview

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 move them to extension headers to reduce the load of basic IPv6 headers. 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 basic IPv6 headers is only twice that of IPv4 headers (excluding the Options field). For the specific IPv6 header format, see Figure 189.

Figure 189 Comparison between IPv4 header format and IPv6 header format



Adequate address space

The source IPv6 address and the destination IPv6 address are both 128 bits (16 bytes) long. IPv6 can provide 3.4×10^{38} addresses to completely meet the requirements of hierarchical address division as well as allocation of public and private addresses.

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).



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 383 lists the mapping between major address types and format prefixes.

Table 383 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

Table 383 Mapping between address types and format prefixes

Type	Format prefix (binary)	IPv6 prefix ID
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 for the neighbor discovery protocol as well as communication between link-local nodes in stateless autoconfiguration. 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 384 are reserved for special purpose.

Table 384 Reserved IPv6 multicast addresses

Address	Application
FF01::1	Node-local scope all-nodes multicast address
FF02::1	Link-local scope all-nodes multicast address
FF01::2	Node-local scope all-routers multicast address
FF02::2	Link-local scope all-routers multicast address
FF05::2	Site-local scope all-routers multicast address

Besides, there is another type of multicast address: solicited-node address. The solicited-node multicast address is used to acquire the link-layer addresses of neighbor nodes on the same link and is also used for duplicate address detection. Each IPv6 unicast or anycast address has one corresponding solicited-node address. The format of a solicited-node multicast address is as follows:

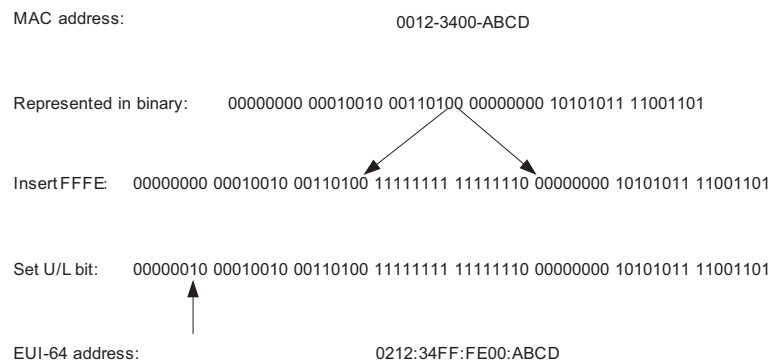
FF02:0:0:0:1:FFXX:XXXX

Where, FF02:0:0:0:1:FF is permanent and consists of 104 bits, and XX:XXXX is the last 24 bits of an IPv6 address.

Interface identifier in IEEE EUI-64 format

Interface identifiers in IPv6 unicast addresses are used to identify interfaces on a link and they are required to be unique on that link. Interface identifiers in IPv6 unicast addresses are currently required to be 64 bits long. An interface identifier is derived from the link-layer address of that interface. Interface identifiers in IPv6 addresses are 64 bits long, while MAC addresses are 48 bits long. Therefore, the hexadecimal number FFFE needs to be inserted in the middle of MAC addresses (behind the 24 high-order bits). To ensure the interface identifier obtained from a MAC address is unique, it is necessary to set the universal/local (U/L) bit (the seventh high-order bit) to "1". Thus, an interface identifier in EUI-64 format is obtained.

Figure 190 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 385 lists the types and functions of ICMPv6 messages used by the NDP.

Table 385 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

Table 385 Types and functions of ICMPv6 messages

ICMPv6 message	Function
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.

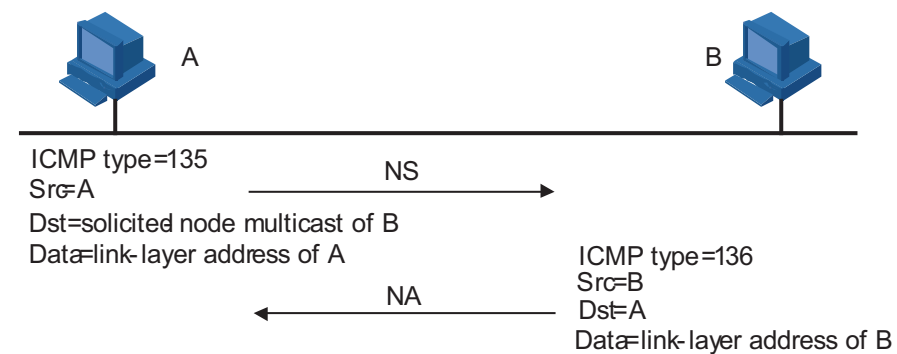


- 3Com Switch 4210 Family do not support RS, RA, or Redirect message.
- Of the above mentioned IPv6 NDP functions, 3Com Switch 4210 Family support the following three functions: address resolution, neighbor unreachability detection, and duplicate address detection. The subsequent sections present a detailed description of these three functions and relevant configuration.

The NDP mainly provides the following functions:

Address resolution

Similar to the ARP function in IPv4, a node acquires the link-layer address of neighbor nodes on the same link through NS and NA messages. Figure 191 shows how node A acquires the link-layer address of node B.

Figure 191 Address resolution

The address resolution procedure is as follows:

- 1 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.

- 2 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.
- 3 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

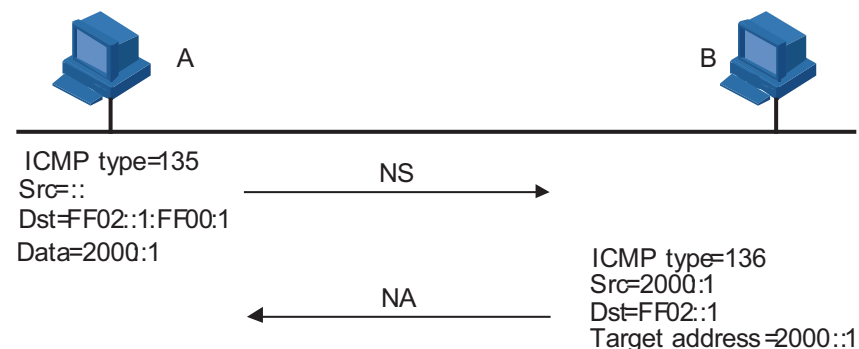
After node A acquires the link-layer address of its neighbor node B, node A can verify whether node B is reachable according to NS and NA messages.

- 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 192 shows the duplicate address detection procedure.

Figure 192 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 Configuration” on page 549.

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

Table 386 Complete these 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 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.

Table 387 Configure an IPv6 unicast address

To do...		Use the command...	Remarks
Enter system view		system-view	-
Enter VLAN interface view		interface <i>interface-type</i> <i>interface-number</i>	-
Configure an IPv6 global unicast address or site-local address	Manually assign an IPv6 address	ipv6 address { <i>ipv6-address prefix-length</i> <i>ipv6-address/prefix-length</i> h }	Use either command By default, no site-local address or global unicast address is configured for an interface.
	Adopt the EUI-64 format to form an IPv6 address	ipv6 address <i>ipv6-address/prefix-length</i> eui-64	Note that the prefix specified by the <i>prefix-length</i> argument in an EUI-64 address cannot exceed 64 bits in length.
Configure an IPv6 link-local address	Automatically generate a link-local address	ipv6 address auto link-local	Optional
	Manually assign a link-local address for an interface.	ipv6 address <i>ipv6-address link-local</i>	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.



- IPv6 unicast addresses can be configured for only one Switch 4210 VLAN interface. Only one global unicast address or one site-local address can be configured for an interface.
- 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. If a link-local address is manually assigned to an interface, this link-local address takes effect. If the

manually assigned link-local address is deleted, the automatically generated link-local address takes effect.

- *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 **Configure 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.

Table 388 Configure a static neighbor entry

To do...	Use the command...	Remarks
Enter system view	system-view	-
Configure a static neighbor entry	ipv6 neighbor <i>ipv6-address mac-address</i> { <i>vlan-id</i> <i>port-type port-number</i> interface <i>interface-type interface-number</i> }	Required

Configure 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.

Table 389 Configure the maximum number of neighbors dynamically learned:

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

Table 389 Configure the maximum number of neighbors dynamically learned:

To do...	Use the command...	Remarks
Enter VLAN interface view	interface <i>interface-type</i> <i>interface-number</i>	-
Configure the maximum number of neighbors dynamically learned by an interface	ipv6 neighbors max-learning-num <i>number</i>	Optional The default value is 2,048

Configure 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.

Table 390 Configure the attempts to send an NS message for duplicate address detection

To do...	Use the command...	Remarks
Enter system view	system-view	-
Enter VLAN interface view	interface <i>interface-type</i> <i>interface-number</i>	-
Configure the attempts to send an NS message for duplicate address detection	ipv6 nd dad attempts <i>value</i>	Optional 1 by default. When the <i>value</i> argument is set to 0, the duplicate address detection is disabled.

Configure the hop limit

When sending an IPv6 packet, the device will use this argument to fill in the Hop Limit field in the IPv6 packet header. Upon receipt of the packet, the receiver will also respond a packet carrying with this argument in the Hop Limit field.

Table 391 Configure the hop limit

To do...	Use the command...	Remarks
Enter system view	system-view	-
Configure the hop limit	ipv6 nd hop-limit <i>value</i>	Optional 64 by default.

Configure 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.

Table 392 Configure the NS interval

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

Table 392 Configure the NS interval

To do...	Use the command...	Remarks
Specify the NS interval	ipv6 nd ns retrans-timer <i>value</i>	Optional 1,000 milliseconds by default

Configure 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.

Table 393 Configure the neighbor reachable timeout time on an interface

To do...	Use the command...	Remarks
Enter system view	system-view	-
Enter VLAN interface view	interface <i>interface-type interface-number</i>	-
Configure the neighbor reachable timeout time	ipv6 nd nud reachable-time <i>value</i>	Optional 30,000 milliseconds

Configuring a Static IPv6 Route

You can configure static IPv6 routes for network interconnection in a small sized IPv6 network. Compared with dynamic routes, static routes save bandwidth significantly.

Table 394 Configure a static IPv6 route

To do...	Use the command...	Remarks
Enter system view	system-view	-
Configure a static IPv6 route	ipv6 route-static <i>ipv6-address prefix-length [interface-type interface-number] nexthop-address</i>	Required By default, no static IPv6 route is configured.

Configuring IPv6 TCP Properties

The IPv6 TCP properties you can configure include:

- **synwait timer:** When a SYN packet is sent, the synwait timer is triggered. If no response packet is received before the synwait timer expires, the IPv6 TCP connection establishment fails.
- **finwait timer:** When the IPv6 TCP connection status is FIN_WAIT_2, the finwait timer is triggered. If no packet is received before the finwait timer expires, the IPv6 TCP connection is terminated. If FIN packets are received, the IPv6 TCP connection status becomes TIME_WAIT. If other packets are received, the finwait timer is reset from the last packet and the connection is terminated after the finwait timer expires.
- **Size of IPv6 TCP receiving/sending buffer.**

Table 395 Configure IPv6 TCP properties

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

Table 395 Configure IPv6 TCP properties

To do...	Use the command...	Remarks
Set the finwait timer of IPv6 TCP packets	tcp ipv6 timer fin-timeout <i>wait-time</i>	Optional 675 seconds by default
Set the synwait timer of IPv6 TCP packets	tcp ipv6 timer syn-timeout <i>wait-time</i>	Optional 75 seconds by default
Configure the size of IPv6 TCP receiving/sending buffer	tcp ipv6 window size	Optional 8 KB by default

Configuring the Maximum Number of IPv6 ICMP Error Packets Sent within a Specified Time

If too many IPv6 ICMP error packets are sent within a short time in a network, network congestion may occur. To avoid network congestion, you can control the maximum number of IPv6 ICMP error packets sent within a specified time. Currently, the token bucket algorithm is adopted.

You can set the capacity of a token bucket, namely, the number of tokens in the bucket. In addition, you can set the update period of the token bucket, namely, the interval for updating the number of tokens in the token bucket to the configured capacity. One token allows one IPv6 ICMP error packet to be sent. Each time an IPv6 ICMP error packet is sent, the number of tokens in a token bucket decreases by 1. If the number of the IPv6 ICMP error packets that are continuously sent out reaches the capacity of the token bucket, the subsequent IPv6 ICMP error packets cannot be sent out until new tokens are put into the token bucket based on the specified update frequency.

Table 396 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 <i>bucket-size</i> ratelimit <i>interval</i> }*	Optional 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 IPv6 DNS

Configure a static host name to IPv6 address mapping

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 one IPv6 address.

Table 397 Configure a static host name to IPv6 address mapping

To do...	Use the command...	Remarks
Enter system view	system-view	-
Configure a static host name to IPv6 address mapping	ipv6 host <i>hostname</i> <i>ipv6-address</i>	Required

Configure 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.

Table 398 Configure dynamic DNS resolution

To do...	Use the command...	Remarks
Enter system view	system-view	-
Enable the dynamic domain name resolution function	dns resolve	Required Disabled by default.
Configure an IPv6 DNS server	dns server ipv6 <i>ipv6-address</i> [<i>interface-type</i> <i>interface-number</i>]	Required If the IPv6 address of the DNS server is a link-local address, the <i>interface-type</i> and <i>interface-number</i> arguments are required.
Configure the domain suffix.	dns domain <i>domain-name</i>	Required By default, no domain name suffix is configured, that is, the domain name is resolved according to the input information.



The **dns resolve** and **dns domain** commands are the same as those of IPv4 DNS. For details about the commands, refer to “DNS Configuration” on page 549.

Displaying and Maintaining IPv6

Table 399 Display and maintain IPv6

To do...	Use the command...	Remarks
Display DNS domain name suffix information	display dns domain [dynamic]	Available in any view
Display IPv6 dynamic domain name cache information.	display dns ipv6 dynamic-host	
Display DNS server information	display dns server [dynamic]	
Display the FIB entries	display ipv6 fib	
Display the mapping between host name and IPv6 address	display ipv6 host	
Display the brief IPv6 information of an interface	display ipv6 interface [<i>interface-type</i> <i>interface-number</i> brief]	
Display neighbor information	display ipv6 neighbors [<i>ipv6-address</i> all dynamic interface <i>interface-type</i> <i>interface-number</i> static vlan <i>vlan-id</i>] [[{ begin exclude include } <i>text</i>]	
Display the total number of neighbor entries satisfying the specified conditions	display ipv6 neighbors { all dynamic static interface <i>interface-type</i> <i>interface-number</i> vlan <i>vlan-id</i> } count	
Display information about the routing table	display ipv6 route-table [verbose]	
Display information related to a specified socket	display ipv6 socket [sockettype <i>socket-type</i>] [<i>task-id</i> <i>socket-id</i>]	
Display the statistics of IPv6 packets and IPv6 ICMP packets	display ipv6 statistics	
Display the statistics of IPv6 TCP packets	display tcp ipv6 statistics	
Display the IPv6 TCP connection status	display tcp ipv6 status	
Display the statistics of IPv6 UDP packets	display udp ipv6 statistics	
Clear IPv6 dynamic domain name cache information	reset dns ipv6 dynamic-host	Available in user view
Clear IPv6 neighbor information	reset ipv6 neighbors [all dynamic interface <i>interface-type</i> <i>interface-number</i> static]	
Clear the statistics of IPv6 packets	reset ipv6 statistics	
Clear the statistics of all IPv6 TCP packets	reset tcp ipv6 statistics	
Clear the statistics of all IPv6 UDP packets	reset udp ipv6 statistics	



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 Configuration” on page 549.

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. IPv6 addresses are configured for the interface Vlan-interface2 on each switch to verify the connectivity between the two switches. 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 193 Network diagram for IPv6 address configuration



Configuration procedure

1 Configure Switch A.

Configure an automatically generated link-local address for the interface Vlan-interface2.

```
<SwitchA> system-view
[SwitchA] interface Vlan-interface 2
[SwitchA-Vlan-interface2] ipv6 address auto link-local
```

Configure a global unicast address for the interface Vlan-interface2.

```
[SwitchA-Vlan-interface2] ipv6 address 3001::1/64
```

2 Configure Switch B.

Configure an automatically generated link-local address for the interface Vlan-interface2.

```
<SwitchA> system-view
[SwitchB] interface Vlan-interface 2
[SwitchB-Vlan-interface2] ipv6 address auto link-local
```

Configure a global unicast address for the interface Vlan-interface2.

```
[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:FE47:4CA3
Global unicast address(es):
  3001::1, subnet is 3001::/64 [DUPLICATE]
```

```

Joined group address(es):
  FF02::1:FF00:1
  FF02::1:FF47:4CA3
  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::2E0:FCFF:FE00:2006
Global unicast address(es):
  3001::2, subnet is 3001::/64
Joined group address(es):
  FF02::1:FF00:2
  FF02::1:FF00:2006
  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 and global unicast address of Switch B. If the configurations are correct, the above two 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 “IPv6 Ping” on page 543.

```

[SwitchA-Vlan-interface2]ping ipv6 FE80::2E0:FCFF:FE00:2006 -i Vlan-interface 2
PING FE80::2E0:FCFF:FE00:2006 : 56 data bytes, press CTRL_C to break
  Reply from FE80::2E0:FCFF:FE00:2006
  bytes=56 Sequence=1 hop limit=64 time = 77 ms
  Reply from FE80::2E0:FCFF:FE00:2006
  bytes=56 Sequence=2 hop limit=64 time = 6 ms
  Reply from FE80::2E0:FCFF:FE00:2006
  bytes=56 Sequence=3 hop limit=64 time = 6 ms
  Reply from FE80::2E0:FCFF:FE00:2006
  bytes=56 Sequence=4 hop limit=64 time = 7 ms
  Reply from FE80::2E0:FCFF:FE00:2006
  bytes=56 Sequence=5 hop limit=64 time = 14 ms

--- FE80::2E0:FCFF:FE00:2006 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 6/22/77 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=64 time = 79 ms
  Reply from 3001::2
  bytes=56 Sequence=2 hop limit=64 time = 6 ms
  Reply from 3001::2

```

```
bytes=56 Sequence=3 hop limit=64 time = 6 ms
Reply from 3001::2
bytes=56 Sequence=4 hop limit=64 time = 5 ms
Reply from 3001::2
bytes=56 Sequence=5 hop limit=64 time = 6 ms

--- 3001::2 ping statistics ---
 5 packet(s) transmitted
 5 packet(s) received
 0.00% packet loss
round-trip min/avg/max = 5/20/79 ms
```

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 3Com Switch 4210 Family are:

- Ping
- Traceroute
- TFTP
- Telnet

IPv6 Application Configuration

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 “Basic System Configuration and Debugging” on page 483.

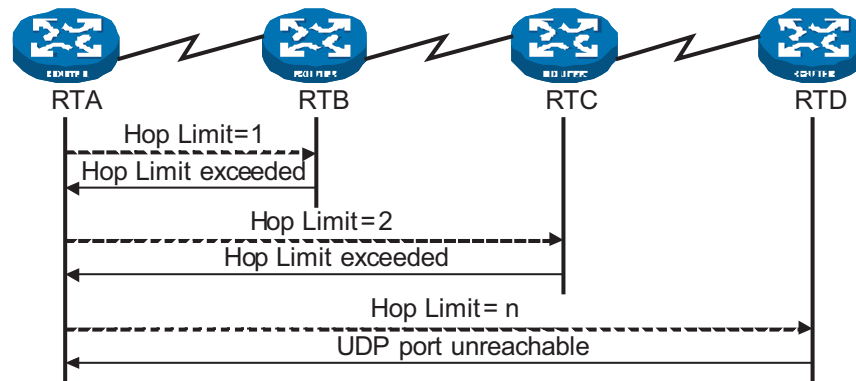
Table 400 Ping IPv6

To do...	Use the command...	Remarks
Ping IPv6	ping ipv6 [-a <i>source-ipv6</i> -c <i>count</i> -m <i>interval</i> -s <i>packet-size</i> -t <i>timeout</i>]* <i>remote-system</i> [-i <i>interface-type interface-number</i>]	Required Available in any view



CAUTION: When you use the **ping ipv6** command to verify the reachability of the destination, you must specify the **"-i"** keyword if the destination address is a link-local address.

IPv6 Traceroute The **traceroute ipv6** command is used to record the route of IPv6 packets from source to destination, so as to check whether the link is available and determine the point of failure.

Figure 194 Traceroute process

As Figure 194 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.

Table 401 Traceroute IPv6

To do...	Use the command...	Remarks
Traceroute IPv6	tracert ipv6 [-f <i>first-ttl</i> -m <i>max-ttl</i> -p <i>port</i> -q <i>packet-num</i> -w <i>timeout</i>]* <i>remote-system</i>	Required Available in any view

IPv6 TFTP IPv6 supports TFTP (Trivial File Transfer Protocol). As a client, the device can download files from or upload files to a TFTP server. For details about TFTP, see *File System Management*.

Configuration preparation

Enable TFTP on the TFTP server and specify the path to download or upload files. For specific operations, refer to TFTP server's configuration specifications.

IPv6 TFTP configuration

You can use the commands listed in Table 402 to download files from a TFTP server or upload files to a TFTP server.

Table 402 Download/upload files to TFTP servers

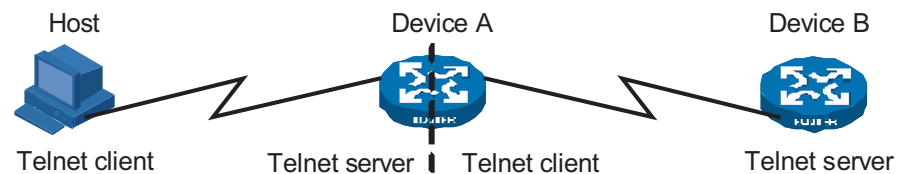
To do...	Use the command...	Remarks
Download/ Upload files from TFTP server	tftp ipv6 <i>remote-system</i> [-i <i>interface-type interface-number</i>] { get put } <i>source-filename</i> [<i>destination-filename</i>]	Required Available in user view



CAUTION: When you use the **tftp ipv6** command to connect to the TFTP server, you must specify the **"-i"** keyword if the destination address is a link-local address.

IPv6 Telnet Telnet protocol belongs to application layer protocols of the TCP/IP protocol suite, and is used to provide remote login and virtual terminals. The device can be used either as a Telnet client or a Telnet server.

As the following figure shows, the Host is running Telnet client application of IPv6 to set up an IPv6 Telnet connection with Device A, which serves as the Telnet server. If Device A again connects to Device B through Telnet, the Device A is the Telnet client and Device B is the Telnet server.

Figure 195 Provide Telnet services

Configuration prerequisites

Enable Telnet on the Telnet server and configure the authentication method. For details, refer to "You can log into a Switch 4210 in one of the following ways:" on page 21.

Table 403 Set up IPv6 Telnet connections

To do...	Use the command...	Remarks
Perform the telnet command on the Telnet client to log in to other devices	telnet ipv6 <i>remote-system</i> [-i <i>interface-type interface-number</i>] [<i>port-number</i>]	Required Available in user view



CAUTION: When you use the **telnet ipv6** command to connect to the Telnet server, you must specify the **"-i"** keyword if the destination address is a link-local address.

Display and maintain IPv6 Telnet

Table 404 Display and maintain 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

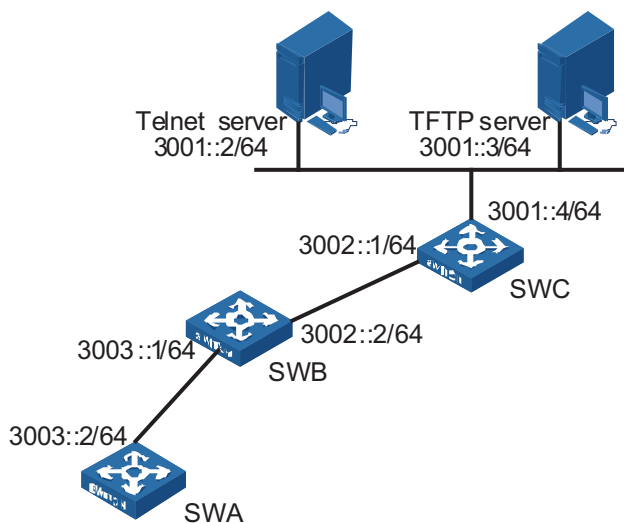
IPv6 Application Configuration Example

IPv6 Applications Network requirements

In Figure 196, SWA, SWB, and SWC are three switches, among which SWA is an Switch 4210, 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 196 Network diagram for IPv6 applications



Configuration procedure



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
tracert 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.



This chapter covers only IPv4 DNS configuration. For details about IPv6 DNS, refer to "IPv6 Mangement Configuration" on page 525.

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 memorable 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, when acting as a DNS client, the Switch 4210 supports 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.

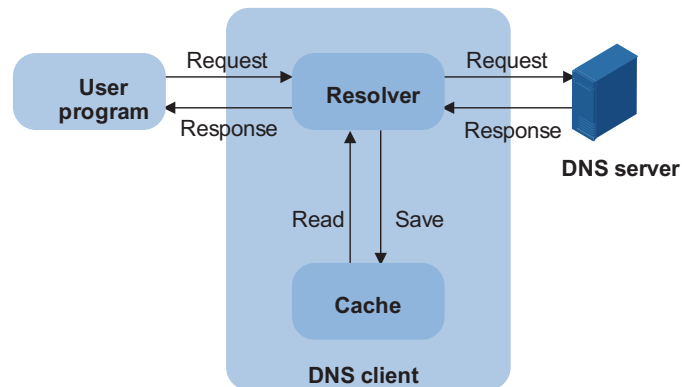
Figure 197 Dynamic domain name resolution

Figure 197 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 or aabbcc., it indicates that no DNS suffix needs to be added and the resolver will consider this as a host name and add a DNS suffix before processing. The original name such as aabbcc is used if all DNS lookups fail.
- If there is a dot in the domain name, such as www.aabbcc, the resolver will use this domain name to do DNS lookup first. If the lookup fails, the resolver adds a DNS suffix for another lookup.

Configuring Domain Name Resolution

Configuring Static Domain Name Resolution

Table 405 Configure static domain name resolution

Operation	Command	Remarks
Enter system view	system-view	-
Configure a mapping between a host name and an IP address	ip host <i>hostname ip-address</i>	Required No IP address is assigned to a host name by default.



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

Table 406 Configure dynamic domain name resolution

Operation	Command	Remarks
Enter the system view	system-view	-
Enable dynamic domain name resolution	dns resolve	Required Disabled by default
Configure an IP address for the DNS server	dns server <i>ip-address</i>	Required No IP address is configured for the DNS server by default.
Configure DNS suffixes	dns domain <i>domain-name</i>	Optional No DNS suffix is configured by default



You may configure up to six DNS servers and ten DNS suffixes.

Displaying and Maintaining DNS

After the above configuration, you can execute the display command and the nslookup type command in any view to display the DNS configuration information and the DNS resolution result to verify the configuration effect. You can execute the reset command in user view to clear the information stored in the dynamic domain name resolution cache.

Table 407 Display and maintain DNS

Operation	Command...	Remarks
Display static DNS database	display ip host	Available in any view

Table 407 Display and maintain DNS

Operation	Command...	Remarks
Display the DNS server information	display dns server [dynamic]	
Display the DNS suffixes	display dns domain [dynamic]	
Display the information in the dynamic domain name cache	display dns dynamic-host	
Display the DNS resolution result	nslookup type { ptr ip-address a domain-name }	Available in any view
Clear the information in the dynamic domain name cache	reset dns dynamic-host	Available in user view

DNS Configuration Example

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 198 Network diagram for static DNS configuration



Configuration procedure

Configure a mapping between host name host.com and IP address 10.1.1.2.

```
<4210> system-view
[4210] 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.

```
[4210] 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
```

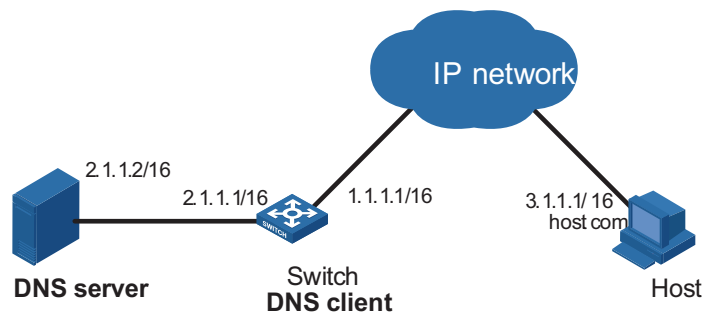
Dynamic Domain Name Resolution Configuration Example

Network requirements

As shown in Figure 199, 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 199 Network diagram for dynamic DNS configuration



Configuration procedure



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.

```
<4210> system-view
[4210] dns resolve
```

Configure the IP address 2.1.1.2 for the DNS server.

```
[4210] dns server 2.1.1.2
```

Configure com as the DNS suffix

```
[4210] 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.

```
[4210] 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=255 time=3 ms
```

```
Reply from 3.1.1.1: bytes=56 Sequence=2 ttl=255 time=1 ms
Reply from 3.1.1.1: bytes=56 Sequence=3 ttl=255 time=1 ms
Reply from 3.1.1.1: bytes=56 Sequence=4 ttl=255 time=1 ms
Reply from 3.1.1.1: bytes=56 Sequence=5 ttl=255 time=1 ms

--- 3.1.1.1 ping statistics ---
 5 packet(s) transmitted
 5 packet(s) received
 0.00% packet loss
 round-trip min/avg/max = 1/1/3 ms
--- host.com ping statistics ---
 5 packet(s) transmitted
 0 packet(s) received
100.00% packet loss
```

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.

PASSWORD CONTROL CONFIGURATION OPERATIONS

Introduction to Password Control Configuration

The password control feature is designed to manage the following passwords:

- Telnet passwords: passwords for logging into the switch through Telnet.
- SSH passwords: passwords for logging into the switch through SSH.
- FTP passwords: passwords for logging into the switch through FTP.
- Super passwords: passwords used by the users who have logged into the switch and are changing from a lower privilege level to a higher privilege level.

Password control provides the following functions:

Table 408 Functions provided by password control

Function	Description	Application
Password aging	Password aging time setting: Users can set the aging time for their PASSWORDS. If a password ages out, its user must change it, otherwise the user cannot log into the device.	All passwords
	Password change: After a password ages out, the user can change it when logging into the device.	Telnet SSH and Super passwords
	Alert before password expiration: Users can set their respective alert time. If a user logs into the system when the password is about to age out (that is, the remaining usable time of the password is no more than the set alert time), the switch will alert the user to the forthcoming expiration and prompts the user to change the password as soon as possible.	
Limitation of minimum password	This function is used to limit the minimum length of the passwords. A user can successfully configure a password only when the password is not shorter than its minimum length.	All passwords
History password function	History password recording function: The password configured and once used by a user is called a history (old) password. The switch is able to record the user history password. Users cannot successfully replace their passwords with history passwords.	All passwords
	History password protection function: History passwords are saved in a readable file in the Flash memory, so they will not be lost when the switch reboots.	
Password protection and encryption	Encrypted display: The switch protects the displayed password. The password is always displayed as a string containing only asterisks (*) in the configuration file or on user terminal.	All passwords
	Saving passwords in ciphertext: The switch encrypts and saves the configured passwords in ciphertext in the configuration file.	

Table 408 Functions provided by password control

Function	Description	Application
Login attempt limitation and failure processing.	<p>Login attempt limitation: You can use this function to enable the switch to limit the number of login attempts allowed for each user.</p> <p>If the number of login attempts exceeds the configured maximum number, the user fails to log in. In this case, the switch provides three failure processing modes.</p> <p>By default, the switch adopts the first mode, but you can actually specify the processing mode as needed.</p>	Telnet and SSH passwords
	<p>Inhibit the user from re-logging in within a certain time period. After the period, the user is allowed to log into the switch again.</p> <p>Inhibit the user from re-logging in forever. The user is allowed to log into the switch again only after the administrator manually removes the user from the user blacklist.</p> <p>Allow the user to log in again without any inhibition.</p>	
User blacklist	<p>If the maximum number of attempts is exceeded, the user cannot log into the switch and is added to the blacklist by the switch. All users in the blacklist are not allowed to log into the switch.</p> <ul style="list-style-type: none"> ■ For the user inhibited from logging in for a certain time period, the switch will remove the user from the blacklist when the time period expires. ■ For the user inhibited from logging in forever, the switch provides a command which allows the administrator to manually remove the user from the blacklist. ■ The blacklist is saved in the RAM of the switch, so it will be lost when the switch reboots. 	-
System log function	<p>The switch automatically records the following events in logs:</p> <ul style="list-style-type: none"> ■ Successful user login. The switch records the user name, user IP address, and VTY ID. ■ Inhibition of a user due to ACL rule. The switch records the user IP address. ■ User authentication failure. The switch records the user name, user IP address, VTY ID, and failure reason. 	No configuration is needed for this function.

Password Control Configuration

Configuration Prerequisites

A user PC is connected to the switch to be configured; both devices are operating normally.

Configuration Tasks

The following sections describe the configuration tasks for password control:

- “Configuring Password Aging”
- “Configuring the Limitation of Minimum Password Length”

- “Configuring History Password Recording”
- “Configuring a User Login Password in Interactive Mode”
- “Configuring Login Attempt Times Limitation and Failure Processing Mode”
- “Configuring the Password Authentication Timeout Time”
- “Configuring Password Composition Policies”

After the above configuration, you can execute the **display password-control** command in any view to check the information about the password control for all users, including the enabled/disabled state of password aging, the aging time, enabled/disabled state of password composition policy, minimum number of types that a password should contain, minimum number of characters of each type, the enabled/disabled state of history password recording, the maximum number of history password records, the alert time before password expiration, the timeout time for password authentication, the maximum number of attempts, and the processing mode for login attempt failures.

If the password attempts of a user fail for several times, the system adds the user to the blacklist. You can execute the **display password-control blacklist** command in any view to check the names and the IP addresses of such users.

Configuring Password Aging

Table 409 Configure password aging

Operation	Command	Description
Enter system view	system-view	-
Enable password aging	password-control aging enable	Optional By default, password aging is enabled.
Configure a password aging time globally	password-control aging <i>aging-time</i>	Optional By default, the aging time is 90 days.
Configure a password aging time for a super password	password-control super aging <i>aging-time</i>	Optional By default, the aging time is 90 days.
Enable the system to alert users to change their passwords when their passwords will soon expire, and specify how many days ahead of the expiration the system alerts the users.	password-control alert-before-expire <i>alert-time</i>	Optional By default, users are alerted seven days ahead of the password expiration.
Create a local user or enter local user view	local-user <i>user-name</i>	-
Configure a password aging time for the local user	password-control aging <i>aging-time</i>	Optional By default, the aging time is 90 days.



In this section, you must note the effective range of the same commands when executed in different views or to different types of passwords:

- Global settings in system view apply to all local user passwords and super passwords.

- Settings in the local user view apply to the local user password only.
- Settings on the parameters of the super passwords apply to super passwords only.

The priority of these settings is as follows:

- For local user passwords, the settings in local user view override those in system view unless the former are not provided.
- For super passwords, the separate settings for super password override those in system view unless the former are not provided.

After password aging is enabled, the device will decide whether the user password ages out when a user logging into the system is undergoing the password authentication. This has three cases:

- 1 The password has not expired. The user logs in before the configured alert time. In this case, the user logs in successfully.
- 2 The password has not expired. The user logs in after the configured alert time. In this case, the system alerts the user to the remaining time (in days) for the password to expire and prompts the user to change the password.
 - If the user chooses to change the password and changes it successfully, the system records the new password, restarts the password aging, and allows the user to log in at the same time.
 - If the user chooses not to change the password, the system allows the user to log in. If the user chooses to change the password but fails in modification, the system logs out the user after the maximum number of attempts is reached.
- 3 The password has already expired. In this case, the system alerts the user to the expiration, requires the user to change the password, and requires the user to change the password again if the user inputs an inappropriate password or the two input passwords are inconsistent.



CAUTION:

- You can configure the password aging time when password aging is not yet enabled, but these configured parameters will not take effect.
- After the user changes the password successfully, the switch saves the old password in a readable file in the flash memory.
- The switch does not provide the alert function for FTP passwords. And when an FTP user logs in with a wrong password, the system just informs the user of the password error, and it does not allow the user to change the password.

Configuring the Limitation of Minimum Password Length

This function is used to enable the switch to check the password length when a password is configured. If the switch finds the length of the input password does not meet the limitation, it informs the user of this case and requires the user to input a new password.

Table 410 Configure the limitation of the minimum password length

Operation	Command	Description
Enter system view	system-view	-

Table 410 Configure the limitation of the minimum password length

Operation	Command	Description
Enable the limitation of minimum password length	password-control length enable	Optional By default, the limitation of minimum password length is enabled.
Configure the minimum password length globally	password-control length <i>length</i>	Optional By default, the minimum length is 10 characters.
Configure the minimum password length for a super password	password-control super length <i>min-length</i>	Optional By default, the minimum length is 10 characters.
Create a local user or enter local user view	local-user <i>user-name</i>	-
Configure the minimum password length for the local user	password-control length <i>length</i>	Optional By default, the minimum length is 10 characters.



In this section, you must note the effective range of the same commands when executed in different views or to different types of passwords:

- Global settings in system view apply to all local user passwords and super passwords.
- Settings in the local user view apply to the local user password only.
- Settings on the parameters of the super passwords apply to super passwords only.

The priority of these settings is as follows:

- For local user passwords, the settings in local user view override those in system view unless the former are not provided.
- For super passwords, the separate settings for super password override those in system view unless the former are not provided.

Configuring History Password Recording

With this function enabled, when a login password expires, the system requires the user to input a new password and save the old password automatically. You can configure the maximum number of history records allowed for each user. The purpose is to inhibit the users from using one single password or using an old password for a long time to enhance the security.

Table 411 Configure history password recording

Operation	Command	Description
Enter system view	system-view	-
Enable history password recording	password-control history enable	Optional By default, history password recording is enabled.
Configure the maximum number of the history password records	password-control history <i>max-record-number</i>	Optional By default, the maximum number is 4.

**CAUTION:**

- When the system adds a new record but the number of the recorded history passwords has reached the configured maximum number, the system replaces the oldest record with the new one.
- When you configure the maximum number of history password records for a user, the excessive old records will be lost if the number of the history password records exceeds the configured number.
- When changing a password, do not use the recorded history password; otherwise, the system will prompt you to reset a password.

The system administrator can perform the following operations to manually remove history password records.

Table 412 Manually remove history password records

Operation	Command	Description
Remove history password records of one or all users	reset password-control history-record [user-name <i>user-name</i>]	Executing this command without the user-name <i>user-name</i> option removes the history password records of all users. Executing this command with the user-name <i>user-name</i> option removes the history password records of the specified user.
Remove history records of one or all super passwords	reset password-control history-record super [level <i>level-value</i>]	Executing this command without the level <i>level-value</i> option removes the history records of all super passwords. Executing this command with the level <i>level-value</i> option removes the history records of the super password for the users at the specified level.

Configuring a User Login Password in Interactive Mode

A password can be a combination of characters from the following four types: letters A to Z, a to z, numbers 0 to 9, and 32 special characters (including the space and ~ ' ! @ # \$ % ^ & * () _ + - = { } | [] : " ; ' < > , . /).

The password must conform to the related configuration of password control when you set the local user password in interactive mode.

Table 413 Configure a user login password in interactive mode

Operation	Command	Description
Enter system view	system-view	-
Enter the specified user view	local-user <i>user-name</i>	-

Table 413 Configure a user login password in interactive mode

Operation	Command	Description
Configure a user login password in interactive mode	password	Optional Input a password according to the system prompt and ensure the two input passwords are consistent.

Configuring Login Attempt Times Limitation and Failure Processing Mode

Table 414 Configure the login attempts limitation and the failure processing mode

Operation	Command	Description
Enter system view	system-view	-
Enable the login attempts limitation, configure the maximum number of attempts and configure the processing mode used when the maximum number of attempts is exceeded.	password-control login-attempt <i>login-times</i> [exceed { lock unlock lock-time <i>time</i> }]	Optional By default, the maximum number of attempts is three, and the switch operates in the lock-time processing mode when the maximum number of attempts is exceeded.

When the maximum number of attempts is exceeded, the system operates in one of the following processing mode:

- **lock-time:** In this mode, the system inhibits the user from re-logging in within a certain time period. After the period, the user is allowed to log into the switch again. By default, this time is 120 minutes.
- **lock:** In this mode, the system inhibits the user from re-logging in forever. The user is allowed to log into the switch again only after the administrator removes the user from the user blacklist.
- **unlock:** In this mode, the system allows the user to log in again.



CAUTION:

- Login attempt times limitation and failure processing are not supported for FTP and Super passwords.
- The number of retries allowed to enter an SSH password is determined by the configuration of the SSH server instead of that configured by using the **password-control login-attempt** command. You can use the **password-control login-attempt** command to configure the actions to be taken when the number of retries to enter the SSH password exceeds the configured value. Refer to “SSH Configuration” on page 387 for information about SSH server.
- If a user in the blacklist changes his/her IP address, the blacklist will not affect the user anymore when the user logs into the switch.

The system administrator can perform the following operations to manually remove one or all user entries in the blacklist.

Table 415 Manually remove one or all user entries in the blacklist

Operation	Command	Description
Delete one specific or all user entries in the blacklist	reset password-control blacklist [user-name <i>user-name</i>]	Executing this command without the user-name <i>user-name</i> option removes all the user entries in the blacklist. Executing this command with the user-name <i>user-name</i> option removes the specified user entry in the blacklist.

Configuring the Password Authentication Timeout Time

When the local/remote server receives the user name, the authentication starts; when the user authentication is completed, the authentication ends. Whether the user is authenticated on the local server or on a remote server is determined by the related AAA configuration.

If a password authentication is not completed before the authentication timeout expires, the authentication fails, and the system terminates the connection and makes some logging.

If a password authentication is completed within the authentication timeout time, the user will log into the switch normally.

Table 416 Configure the timeout time for users to be authenticated

Operation	Command	Description
Enter system view	system-view	-
Configure the timeout time for users to be authenticated	password-control authentication-timeout <i>authentication-timeout</i>	Optional By default, it is 60 seconds.

Configuring Password Composition Policies

A password can be combination of characters from the following four categories: letters A to Z, a to z, number 0 to 9, and 32 special characters of space and ~'!@#\$%^&*()_+=~{}|[]: ";' <> , /.

Depending on the system security requirements, the administrator can set the minimum number of categories a password should contain and the minimum number of characters in each category.

Password combination falls into four levels: 1, 2, 3, and 4, each representing the number of categories that a password should at least contain. Level 1 means that a password must contain characters of one category, level 2 at least two categories, level 3 three categories, and level 4 four categories.

When you set or modify a password, the system will check if the password satisfies the component requirement. If not, an error message will occur.

Table 417 Configure password composition policy

Operation	Command	Description
Enter system view	system-view	-

Table 417 Configure password composition policy

Operation	Command	Description
Enable the password composition check function	password-control composition enable	Optional By default, the password composition check function is enabled.
Configure the password composition policy, globally	password-control composition type-number <i>policy-type</i> [type-length <i>type-length</i>]	Optional By default, the minimum number of types a password should contain is 1 and the minimum number of characters of each type is 1.
Configure the password composition policy for a super password	password-control super composition type-number <i>policy-type</i> [type-length <i>type-length</i>]	Optional By default, the minimum number of types a password should contain is 1 and the minimum number of characters of each type is 1. If the <i>type-length</i> is not specified, the global <i>type-length</i> is used.
Create a local user or enter local user view	local-user <i>user-name</i>	-
Configure the password composition policy for the local user	password-control composition type-number <i>policy-type</i> [type-length <i>type-length</i>]	Optional By default, the minimum number of types a password should contain is 1 and the minimum number of characters of each type is 1. If the <i>type-length</i> is not specified, the global <i>type-length</i> is used.



In this section, you must note the effective range of the same commands when executed in different views or to different types of passwords:

- Global settings in system view apply to all local user passwords and super passwords.
- Settings in the local user view apply to the local user password only.
- Settings on the parameters of the super passwords apply to super passwords only.

The priority of these settings is as follows:

- For local user passwords, the settings in local user view override those in system view unless the former are not provided.
- For super passwords, the separate settings for super password override those in system view unless the former are not provided.

Displaying Password Control

After completing the above configuration, you can execute the **display** command in any view to display the operation of the password control and verify your configuration.

Table 418 Displaying password control

Operation	Command
Display the information about the password control for all users	display password-control
Display the information about the super password control	display password-control super
Display the information about one or all users who have been added to the blacklist because of password attempt failure	display password-control blacklist [user-name <i>user-name</i> ip <i>ip-address</i>]

Password Control Configuration Example

Network requirements

The following password control functions should be implemented:

- Globally, the password aging time is 30 days.
- For the super password, the minimum number of password composition types is 3 and the minimum number of characters in each composition type is 3.
- For a local user named test, the minimum password length is 6 characters, the minimum number of password composition types is 2, the minimum number of characters in each password composition type is 3, and the password aging time is 20 days.

Configuration procedure

Enter system view.

```
<4210> system-view
```

Set the global password aging time to 30 days.

```
[4210] password-control aging 30
```

Set the minimum number of composition types for the super password to 3 and the minimum number of characters in each composition type to 3.

```
[4210] password-control super composition type-number 3 type-length 3
```

Configure a super password.

```
[4210] super password level 3 simple 11111AAAAAaaaaa
```

Create a local user named test.

```
[4210] local-user test
```

Set the minimum password length for the local user to 6.

```
[4210-luser-test] password-control length 6
```

Set the minimum number of composition types for the local user password to 2 and the minimum number of characters in each password composition type to 3.

```
[4210-luser-test] password-control composition type-number 2 type-length 3
```

Set the aging time for the local user password to 20 days.

```
[4210-luser-test] password-control aging 20
```

Configure the password of local user.

```
[4210-luser-test] password simple 11111#####
```