



3Com® Switch 4500 Family

Configuration Guide

Version 03.02.00

Switch 4500 26-Port
Switch 4500 50-Port
Switch 4500 PWR 26-Port
Switch 4500 PWR 50-Port

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

Copyright © 2009, 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.

Environmental Statement about the Documentation

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

CONTENTS

ABOUT THIS GUIDE

How This Guide is Organized	11
Intended Readership	11
Conventions	12
Related Documentation	13

1 GETTING STARTED

Product Overview	15
Stacking Overview	16
Brief Introduction	16
Typical Networking Topology	16
Product Features	16
Logging In to the Switch	17
Setting up Configuration Environment Through the Console Port	17
Setting up Configuration Environment Through Telnet	19
Setting up Configuration Environment Through a Dial-up Modem	21
Command Line Interface	24
Command Line View	24
Features and Functions of Command Line	28
User Interface Configuration	30
User Interface Overview	30
User Interface Configuration	31
Displaying and Debugging User Interface	37
Default Configuration File Description	38

2 PORT OPERATION

Ethernet Port Configuration	39
Ethernet Port Overview	39
Ethernet Port Configuration	39
Displaying and Debugging Ethernet Port	45
Ethernet Port Configuration Example	46
Ethernet Port Troubleshooting	47
Link Aggregation Configuration	47
Overview	47
Link Aggregation Configuration	51
Displaying and Debugging Link Aggregation	54
Link Aggregation Configuration Example	54

3 VLAN OPERATION

VLAN Configuration	57
VLAN Overview	57
Configuring a VLAN	57
Displaying and Debugging VLAN	59
VLAN Configuration Example One	59
VLAN Configuration Example Two	60
Voice VLAN Configuration	61
Introduction to Voice VLAN	61
Voice VLAN Configuration	61
Displaying and Debugging of Voice VLAN	64
Voice VLAN Configuration Example	64
Configuring Voice VLAN with a PC Downstream from Phone	65
Key Details for Proper Setup	65
Step By Step Description	66
Voice VLAN in Auto Mode	67
Voice VLAN in Manual Mode	71

4 POWER OVER ETHERNET CONFIGURATION

PoE Overview	73
PoE Configuration	74
Enabling/Disabling the PoE Feature on a Port	74
Setting the Maximum Power Output on a Port	75
Setting Power Supply Management Mode in Overload and Port Priority	75
Setting the PoE Mode on a Port	76
Enabling/Disabling PD Compatibility Detect	76
Upgrading the PSE Processing Software Online	77
Displaying PoE Information	77
Configuration Example	77

5 NETWORK PROTOCOL OPERATION

IP Address Configuration	79
IP Address Overview	79
Configuring IP Address	81
Displaying and Debugging IP Address	82
IP Address Configuration Example	83
Troubleshooting IP Address Configuration	83
ARP Configuration	83
Introduction to ARP	83
Configuring ARP	84
Displaying and Debugging ARP	86
DHCP Configuration	86
Overview of DHCP	86
DHCP Client Configuration	89
DHCP Relay Configuration	89
Displaying and Debugging DHCP Configuration	90

DHCP Relay Configuration Example One	90
DHCP Relay Configuration Example Two	91
Troubleshooting DHCP Relay Configuration	92
Access Management Configuration	93
Access Management Overview	93
Configuring Access Management	93
Displaying and Debugging Access Management	95
Access Management Configuration Example	95
Access Management via the Web	96
UDP Helper Configuration	96
Overview of UDP Helper	96
UDP Helper Configuration	97
Displaying and Debugging UDP Helper Configuration	98
UDP Helper Configuration Example	98
IP Performance Configuration	99
IP Performance Configuration	99
Displaying and Debugging IP Performance	100
Troubleshooting IP Performance	100

6 IP ROUTING PROTOCOL OPERATION

IP Routing Protocol Overview	103
Selecting Routes Through the Routing Table	104
Routing Management Policy	105
Static Routes	106
Configuring Static Routes	107
Example: Typical Static Route Configuration	109
Troubleshooting Static Routes	110
RIP	110
Configuring RIP	111
Displaying and Debugging RIP	119
Example: Typical RIP Configuration	120
Troubleshooting RIP	121
IP Routing Policy	121
Configuring an IP Routing Policy	122
Displaying and Debugging the Routing Policy	125
Typical IP Routing Policy Configuration Example	125
Troubleshooting Routing Protocols	127

7 ACL CONFIGURATION

Brief Introduction to ACL	129
ACL Supported by the Switch	130
Configuring ACL	130
Defining ACL	130
Activating ACL	133
Displaying and Debugging ACL	133
Advanced ACL Configuration Example	134

Basic ACL Configuration Example	135
Link ACL Configuration Example	135
QoS Configuration	136
QoS Configuration	138
Setting Port Priority	138
Configuring Trust Packet Priority	138
Setting Port Mirroring	139
Configuring Traffic Mirroring	139
Setting Traffic Limit	141
Setting Line Limit	141
Configuring WRED Operation	141
Displaying and Debugging QoS Configuration	142
QoS Configuration Example	142
Port Mirroring Configuration Example	143
ACL Control Configuration	144
TELNET/SSH User ACL Configuration	144
ACL Control Over Users Accessing Switches by SNMP	148
Configuring ACL Control for HTTP Users	150

8 IGMP SNOOPING

IGMP Snooping Overview	153
Configuring IGMP Snooping	156
Enabling/Disabling IGMP Snooping	156
Configuring Router Port Aging Time	157
Configuring Maximum Response Time	157
Configuring Aging Time of Multicast Group Member	157
Displaying and Debugging IGMP Snooping	158
Configuration Example — Enable IGMP Snooping	158
IGMP Snooping Fault Diagnosis and Troubleshooting	159

9 STACKING

Introduction to Stacking	161
Establishment of an XRN Fabric	161
Configuring a Stack	161
Specifying the Stacking VLAN of the Switch	162
Setting Unit IDs for Switches	162
Saving the Unit ID of Each Unit in the Stack	163
Specifying the Fabric Port of the Switch	163
Setting Unit Names for Switches	163
Setting a Stack Name for Switches	163
Setting an XRN Authentication Mode for Switches	164
Displaying and Debugging a Stack	164
Stack Configuration Example	165

10 RSTP CONFIGURATION

STP Overview	167
Implement STP	167

Configuration BPDU Forwarding Mechanism in STP	171
Implement RSTP on the Switch	172
RSTP Configuration	173
Enable/Disable RSTP on a Switch	176
Enable/Disable RSTP on a Port	177
Configure RSTP Operating Mode	177
Configure the STP-Ignore attribute of VLANs on a Switch	177
Set Priority of a Specified Bridge	178
Specify the Switch as Primary or Secondary Root Bridge	178
Set Forward Delay of a Specified Bridge	179
Set Hello Time of the Specified Bridge	180
Set Max Age of the Specified Bridge	180
Set Timeout Factor of the Bridge	180
Specifying the Maximum Transmission Rate of STP Packets on a Port	181
Set Specified Port to be an EdgePort	181
Specifying the Path Cost on a Port	182
Set the Priority of a Specified Port	183
Configure a Specified Port to be Connected to Point-to-Point Link	183
Set mCheck of the Specified Port	184
Configure the Switch Security Function	184
Display and Debug RSTP	185
RSTP Configuration Example	186

11 802.1X CONFIGURATION

IEEE 802.1X Overview	189
802.1X System Architecture	189
802.1X Authentication Process	190
Implementing 802.1X on the Switch	191
Configuring 802.1X	191
Enabling/Disabling 802.1X	191
Setting the Port Access Control Mode	192
Setting the Port Access Control Method	192
Checking the Users that Log on the Switch via Proxy	193
Setting the User Number on a Port	193
Setting the Authentication in DHCP Environment	193
Configuring the Authentication Method for 802.1X User	194
Setting the Maximum Times of Authentication Request Message Retransmission	194
Configuring Timers	194
Enabling/Disabling a Quiet-Period Timer	195
Displaying and Debugging 802.1X	196
Auto QoS	196
802.1X Configuration Example	196
Centralized MAC Address Authentication	198
Centralized MAC Address Authentication Configuration	199
Enabling MAC Address Authentication Both Globally and On the Port	199
Configuring Centralized MAC Address Authentication Mode	199

Configuring the User Name and Password for Fixed Mode	200
Configuring Domain Name Used by the MAC Address Authentication User	200
Configuring Centralized MAC Address Authentication Timers	200
Displaying and Debugging Centralized MAC Address Authentication	201
Auto VLAN	201
Configuration Example of Centralized MAC Address Authentication	201
AAA and RADIUS Protocol Configuration	202
RADIUS Protocol Overview	202
Implementing AAA/RADIUS on the Ethernet Switch	203
Configuring AAA	203
Creating/Deleting an ISP Domain	204
Configuring Relevant Attributes of the ISP Domain	204
Enabling/Disabling the Messenger Alert	206
Configuring Self-Service Server URL	207
Creating a Local User	207
Setting Attributes of the Local User	207
Disconnecting a User by Force	209
Configuring the RADIUS Protocol	209
Creating/Deleting a RADIUS Scheme	210
Configuring RADIUS Authentication/Authorization Servers	210
Configuring RADIUS Accounting Servers and the Related Attributes	211
Setting the RADIUS Packet Encryption Key	213
Setting Retransmission Times of RADIUS Request Packet	214
Setting the Supported Type of the RADIUS Server	214
Setting the RADIUS Server State	214
Setting the Username Format Transmitted to the RADIUS Server	215
Setting the Unit of Data Flow that Transmitted to the RADIUS Server	215
Configuring the Local RADIUS Authentication Server	216
Configuring Source Address for RADIUS Packets Sent by NAS	216
Setting the Timers of the RADIUS Server	216
Displaying and Debugging AAA and RADIUS Protocol	218
AAA and RADIUS Protocol Configuration Example	219
Configuring the Switch 4500	220
AAA and RADIUS Protocol Fault Diagnosis and Troubleshooting	224
Problem Diagnosis	225
3Com-User-Access-Level	225

12 FILE SYSTEM MANAGEMENT

File System Overview	227
Directory Operation	227
File Operation	227
Storage Device Operation	228
Setting the Prompt Mode of the File System	228
Configuring File Management	229
Displaying the Current-configuration and Saved-configuration of the Switch	229
Saving the Current-configuration	230

Erasing Configuration Files from Flash Memory	230
Configuring the Name of the Configuration File Used for the Next Startup.	230
FTP Overview	231
Enabling/Disabling FTP Server	232
Configuring the FTP Server Authentication and Authorization	232
Configuring the Running Parameters of FTP Server	232
Displaying and Debugging FTP Server	233
Introduction to FTP Client	233
FTP Server Configuration Example	235
TFTP Overview	235
Downloading Files by means of TFTP	236
Uploading Files by means of TFTP	236
TFTP Client Configuration Example	237

13 MAC Address Table Management

Overview	239
MAC Address Table Configuration	240
Setting MAC Address Table Entries	240
Setting MAC Address Aging Time	240
Setting the Max Count of MAC Addresses Learned by a Port	241
Displaying MAC Address Table	241
MAC Address Table Management Display Example	242
Networking Requirements	242
MAC Address Table Management Configuration Example	243

14 DEVICE MANAGEMENT

Overview	244
Device Management Configuration	244
Rebooting the Switch	244
Enabling the Timing Reboot Function	244
Designating the APP Adopted when Booting the Switch Next Time	244
Upgrading BootROM	245
Displaying and Debugging Device Management	245
Device Management Configuration Example	245

15 SYSTEM MAINTENANCE AND DEBUGGING

Basic System Configuration	249
Setting the System Name for the Switch	249
Setting the System Clock	249
Setting the Time Zone	249
Setting the Summer Time	249
Displaying the State and Information of the System	250
System Debugging	250
Enable/Disable the Terminal Debugging	250
Display Diagnostic Information	252
Testing Tools for Network Connection	252

ping	252
Introduction to Remote-ping	254
Remote-ping Configuration	255
Introduction to Remote-ping Configuration	255
Configuring Remote-ping	255
Configuration Example	256
Logging Function	257
Introduction to Info-center	257
Info-Center Configuration	260
Sending the Information to Loghost	263
Sending the Information to Control Terminal	264
Sending the Information to Telnet Terminal or Dumb Terminal	266
Sending the Information to the Log Buffer	268
Sending the Information to the Trap Buffer	270
Sending the Information to SNMP Network Management	271
Configuration examples of sending logs to Unix loghost	273
Configuration examples of sending log to Linux loghost	275
Configuration Examples of Sending Log to Control Terminal	276

16 SNMP CONFIGURATION

Overview	279
SNMP Versions and Supported MIB	279
Configuring SNMP	280
Setting Community Name	281
Enabling/Disabling SNMP Agent to Send Trap	281
Setting the Destination Address of Trap	282
Setting Lifetime of Trap Message	282
Setting SNMP System Information	282
Setting the Engine ID of a Local or Remote Device	282
Setting/Deleting an SNMP Group	283
Setting the Source Address of Trap	283
Adding/Deleting a User to/from an SNMP Group	283
Creating/Updating View Information or Deleting a View	284
Setting the Size of SNMP Packet Sent/Received by an Agent	284
Enabling/Disabling a Port Transmitting Trap Information SNMP Agent	284
Disabling SNMP Agent	284
Displaying and Debugging SNMP	284
SNMP Configuration Example	285
Reading Usmsr Table Configuration Example	287

17 RMON CONFIGURATION

Overview	289
Configuring RMON	289
Adding/Deleting an Entry to/from the Alarm Table	290
Adding/Deleting an Entry to/from the Event Table	290
Adding/Deleting an Entry to/from the History Control Terminal	290

Adding/Deleting an Entry to/from the Extended RMON Alarm Table	291
Adding/Deleting an Entry to/from the Statistics Table	291
Displaying and Debugging RMON	291
RMON Configuration Example	292

18 NTP CONFIGURATION

Overview	293
Applications of NTP	293
Implementation Principle of NTP	294
NTP Implementation Modes	295
Configuring NTP Implementation Modes	297
Configuration Prerequisites	297
Configuration Procedure	297
Configuring Access Control Right	299
Configuring NTP Authentication	299
Configuration Prerequisites	299
Configuration Procedure	300
Configuring Optional NTP Parameters	301
Displaying and Debugging NTP	302
Configuration Examples	302
Configuring NTP Server Mode	302
Configuring NTP Peer Mode	303
Configuring NTP Broadcast Mode	305
Configuring NTP Multicast Mode	306
Configuring NTP Server Mode with Authentication	308

19 SSH TERMINAL SERVICES

SSH Terminal Service	311
SSH Server Configuration	314
SSH Client Configuration	318
Configuring the Device as an SSH Client	326
Displaying and Debugging SSH	327
SSH Server Configuration Example	328
SSH Client Configuration Example	329
SFTP Service	331
SFTP Overview	331
SFTP Server Configuration	331
SFTP Client Configuration	332
SFTP Configuration Example	335

20 PASSWORD CONTROL CONFIGURATION OPERATIONS

Introduction to Password Control Configuration	339
Password Control Configuration	341
Configuration Prerequisites	341
Configuration Tasks	341
Configuring Password Aging	342

Configuring the Minimum Password Length	343
Configuring History Password Recording	343
Configuring User Login Password in Encryption Mode	344
Configuring Login Attempts Limitation and Failure Procession Mode	344
Configuring the Timeout for User Password Authentication	345
Displaying Password Control	346
Password Control Configuration Example	346
Network Requirements	346
Configuration Procedure	347

A PASSWORD RECOVERY PROCESS

Introduction	349
CLI Commands Controlling Bootrom Access	349
Bootrom Interface	350
Displaying all Files in Flash	350
Skipping the Current Configuration File	351
Bootrom Passwords	351
Bootrom Password Recovery	352

B RADIUS SERVER AND RADIUS CLIENT SETUP

Setting Up a RADIUS Server	353
Configuring Microsoft IAS RADIUS	353
Configuring Funk RADIUS	376
Configuring FreeRADIUS	381
Setting Up the RADIUS Client	382
Windows 2000 Built-in Client	383
Windows XP Built-in Client	383
Aegis Client Installation	383

C AUTHENTICATING THE SWITCH 4500 WITH CISCO SECURE ACS

Cisco Secure ACS (TACACS+) and the 3Com Switch 4500	387
Setting Up the Cisco Secure ACS (TACACS+) Server	387
Adding a 3Com Switch 4500 as a RADIUS Client	388
Adding a User for Network Login	390
Adding a User for Switch Login	391

ABOUT THIS GUIDE

This guide provides information about configuring your network using the commands supported on the 3Com® Switch 4500.

How This Guide is Organized

The Switch 4500 Configuration Guide consists of the following chapters:

- **Getting Started** — Details the main features and configurations of the Switch 4500.
- **Port Operation** — Details how to configure Ethernet port and link aggregation.
- **VLAN Operation** — Details how to configure VLANs.
- **PoE Operation** — Details on Power over Ethernet configuration.
- **Network Protocol Operation** — Details how to configure network protocols.
- **IP Routing Protocol Operation** — Details how to configure routing protocols.
- **Multicast Protocol** — Details how to configure multicast protocols.
- **ACL Configuration**— Details how to configure QoS/ACL.
- **Stacking Configuration**— Details how to configure stacking.
- **RSTP Configuration** — Details how to configure RSTP.
- **802.1X Configuration** — Details how to configure 802.1X.
- **File System Management** — Details how to configure file system management.

Intended Readership

The guide is intended for the following readers:

- Network administrators
- Network engineers
- Users who are familiar with the basics of networking

Conventions

This guide uses the following conventions:

Table 1 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 Text conventions

Convention	Description
Screen displays	This typeface represents text 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.”
Fixed command text	This typeface indicates the fixed part of a command text. You must type the command, or this part of the command, exactly as shown, and press <i>Return</i> or <i>Enter</i> when you are ready to enter the command. Example: The command display history-command must be entered exactly as shown.
Variable command text	This typeface indicates the variable part of a command text. You must type a value here, and press <i>Return</i> or <i>Enter</i> when you are ready to enter the command. Example: in the command super level , a value in the range 0 to 3 must be entered in the position indicated by level
{ x y ... }	Alternative items, one of which must be entered, are grouped in braces and separated by vertical bars. You must select and enter one of the items. Example: in the command flow-control {hardware none software} , the braces and the vertical bars combined indicate that you must enter one of the parameters. Enter either hardware , or none , or software .
[]	Items shown in square brackets [] are optional. Example 1: in the command display users [all] , the square brackets indicate that the parameter all is optional. You can enter the command with or without this parameter. Example 2: in the command user-interface [type] first-number [last-number] the square brackets indicate that the parameters [type] and [last-number] are both optional. You can enter a value in place of one, both or neither of these parameters. Alternative items, one of which can optionally be entered, are grouped in square brackets and separated by vertical bars. Example 3: in the command header [shell incoming login] text , the square brackets indicate that the parameters shell , incoming and login are all optional. The vertical bars indicate that only one of the parameters is allowed.

**Related
Documentation**

The *3Com Switch 4500 Getting Started Guide* provides information about installation.

The *3Com Switch 4500 Command Reference Guide* provides all the information you need to use the configuration commands.

1

GETTING STARTED

This chapter covers the following topics:

- [Product Overview](#)
- [Stacking Overview](#)
- [Product Features](#)
- [Logging In to the Switch](#)
- [Command Line Interface](#)
- [User Interface Configuration](#)
- [Default Configuration File Description](#)

Product Overview

[Table 3](#) lists the models in the Switch 4500 family:

Table 3 Models in the Switch 4500 family

Model	Power Supply Unit (PSU)	Number of Service Ports	Number of 10/100 Mbps Ports	Number of 10/100/1000 Mbps Ports*	Number of 1000 Mbps SFP Ports	Console Port
SW4500-26	AC- input	26	24	2	2	
SW4500-50	AC-input	50	48		2	1
SW4500-26 PWR	AC-input, DC-input	26	24		2	1
SW4500-50 PWR	AC-input, DC-input	50	48		2	1

* Combo SFP and 10/100/1000 Ports

The Switch 4500 family supports the following services:

- Internet broadband access
- MAN (metropolitan area network), enterprise/campus networking
- Multicast service, multicast routing, and audio and video multicast service.

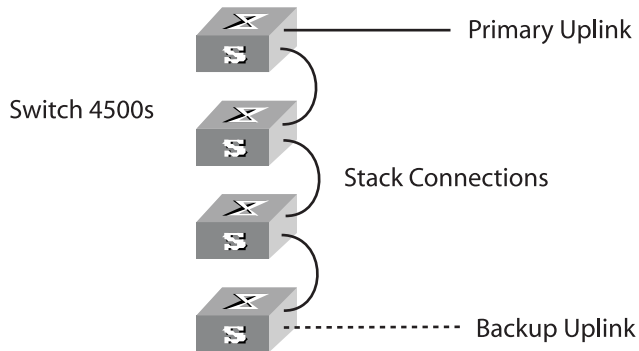
Stacking Overview

Brief Introduction With the 3Com Switch 4500, up to eight units can be operated together as a single larger logical unit to simplify administration. This is called stacking.

Stacking allows you to add ports in a site or location incrementally, without adding complexity to the management of the switch. Only a single IP address is required for a stack. Also, a single interface is presented for configuring a stack using telnet, CLI, web management, or SNMP.

Typical Networking Topology Typical stacking networking topology is as shown in [Figure 1](#). Switches of the same type (that is, units) form a the stack. The Switch 4500 stacking makes use of existing Gigabit connections for interconnecting the members of the stack.

Figure 1 Stacking Networking Topology



Product Features

[Table 4](#) lists the function features:

Table 4 Function Features

Features	Description
VLAN	VLAN compliant with IEEE 802.1Q Standard Port-based VLAN
STP protocol	Spanning Tree Protocol (STP) / Rapid Spanning Tree Protocol (RSTP), compliant with IEEE 802.1D/IEEE802.1w Standard
Flow control	IEEE 802.3 flow control (full-duplex) Back-pressure based flow control (half-duplex)
Broadcast Suppression	Broadcast Suppression
Multicast	Internet Group Management Protocol (IGMP) Snooping
IP routing	Static route RIP V1/v2 IP routing policy
DHCP	Dynamic Host Configuration Protocol (DHCP) Relay DHCP Client
Link aggregation	Link aggregation
Mirror	Mirror based on the traffic classification Port-based mirror

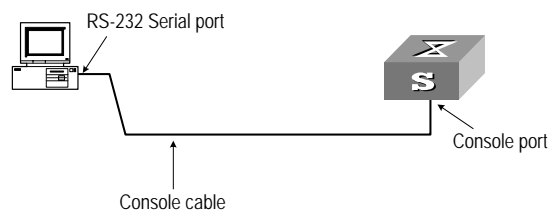
Table 4 Function Features

Features	Description
Security features	Multi-level user management and password protect 802.1X authentication Packet filtering
Quality of Service (QoS)	Traffic classification Bandwidth control Priority Queues of different priority on the port
Management and Maintenance	Command line interface configuration Configuration through console port Remote configuration through Telnet or SSH Configuration through dialing the Modem SNMP Level alarms Output of debugging information Ping and Tracert Remote maintenance with Telnet, Modem and SSH
Loading and updates	Loading and upgrading of software through the XModem protocol Loading and upgrading of software through File Transfer Protocol (FTP) and Trivial File Transfer Protocol (TFTP)

Logging In to the Switch

Setting up Configuration Environment Through the Console Port

- 1 To set up the local configuration environment, connect the serial port of a PC (or a terminal) to the console port of the Switch with the console cable (see [Figure 2](#)).

Figure 2 Setting up the Local Configuration Environment through the Console Port

- 2 Run terminal emulator (such as Terminal on Windows 3X or the Hyper Terminal on Windows 9X) on the PC. Set the terminal communication parameters as follows:
 - Baud rate = 19200

- Databit = 8
- Parity check = none
- Stopbit = 1
- Flow control = none
- Terminal type = VT100

Figure 3 Setting up a New Connection

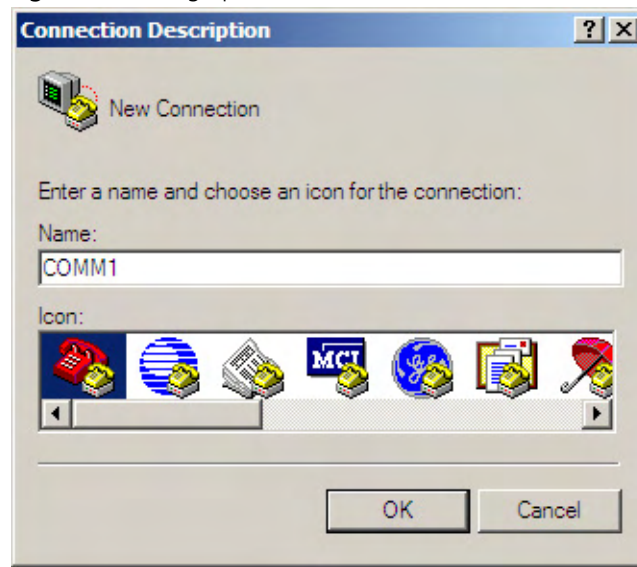


Figure 4 Configuring the Port for Connection

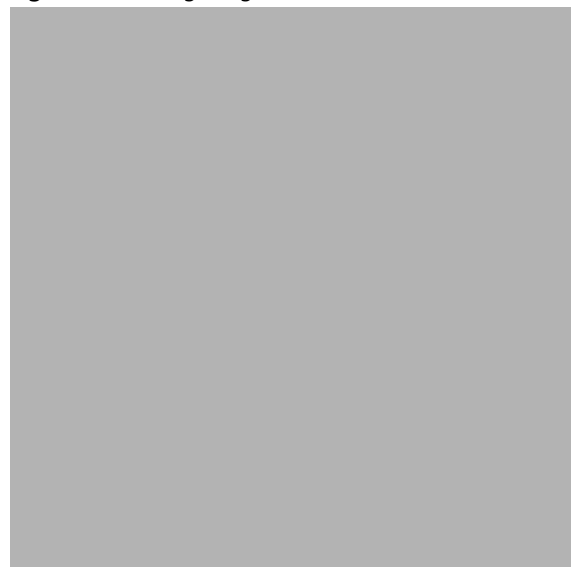
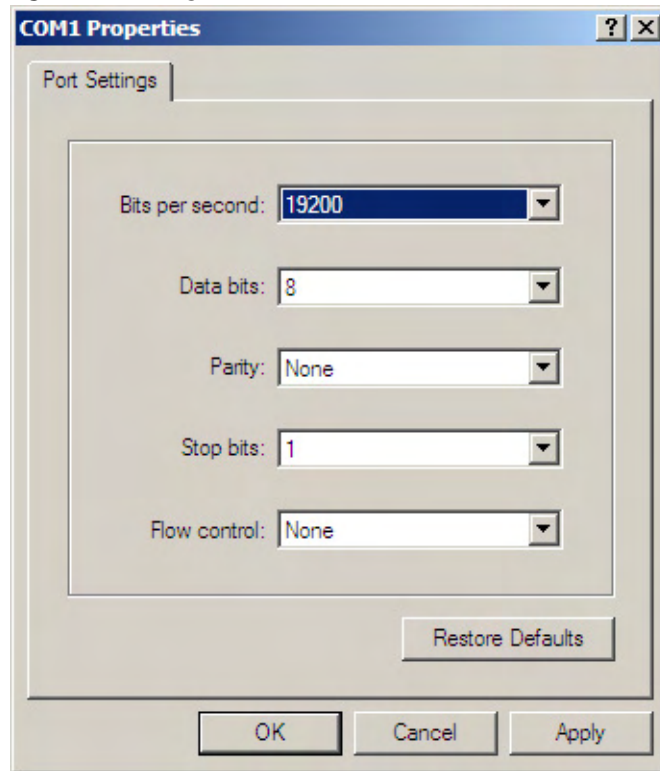


Figure 5 Setting Communication Parameters

- 3 The Switch is powered on and it displays self-test information. Press < Enter> to show the command line prompt such as <4500>.
- 4 Enter a command to configure the Switch or view the operation state. Enter a ? to view online help. For details of specific commands, refer to the following sections.

Setting up Configuration Environment Through Telnet

Connecting a PC to the Switch Through Telnet

After you have correctly configured the IP address of a VLAN interface for the Switch through the console port (using the **ip address** command in VLAN Interface View), and added the port (that connects to a terminal) to this VLAN (using the **port** command in VLAN View), you can Telnet this Switch and configure it.

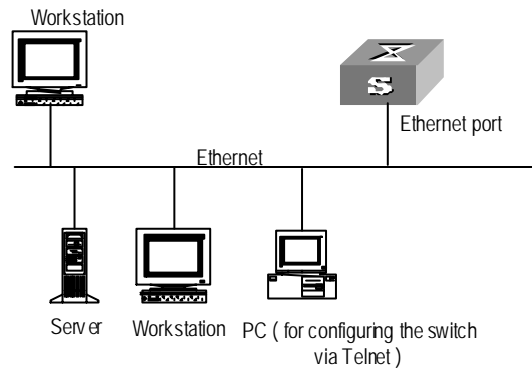
- 1 Authenticate the Telnet user through the console port before the user logs in by Telnet.



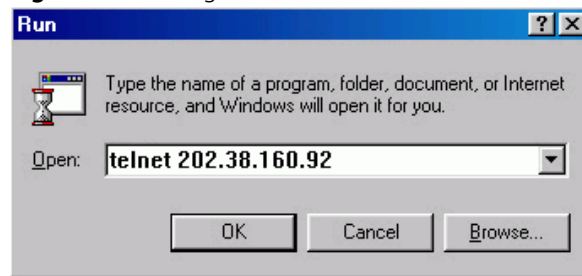
By default, the password is required for authenticating the Telnet user to log in to the Switch. If a user logs in through the Telnet without password, he will see the prompt Login password has not been set!.

```
<4500>system-view
[4500]user-interface vty 0
[4500-ui-vty0]set authentication password simple xxxx (xxxx is the
preset login password of the Telnet user)
```

- 2 To set up the configuration environment, connect the network port of the PC to a port on the Switch through the LAN.

Figure 6 Setting up the Configuration Environment through Telnet

- 3 Run Telnet on the PC and enter the IP address of the VLAN connected to the network port on the PC.

Figure 7 Running Telnet

- 4 The terminal displays Login authentication and prompts the user to enter the logon password. After you enter the correct password, it displays the command line prompt (such as <4500>). If the prompt All user interfaces are used, please try later! appears, too many users are connected to the Switch through Telnet. At most five Telnet users are allowed to log on to the SW4500 Switch simultaneously.
- 5 Use the corresponding commands to configure the Switch or to monitor the running state. Enter ? to view online help. For details of specific commands, refer to the following chapters.



When configuring the Switch through Telnet, do not modify the IP address of the Switch unnecessarily, for the modification might end the Telnet connection.



By default, when a Telnet user passes the password authentication to log on to the Switch, the access level for commands will be Level 0.

Telneting a Switch Through Another Switch

After a user has logged into a Switch, it is possible to configure another Switch through the Switch through Telnet. The local Switch serves as Telnet client and the peer Switch serves as the Telnet server. If the ports connecting these two Switches are in the same local network, their IP addresses must be configured in the same network segment. Otherwise, the two Switches must establish a route to communicate with each other.

As shown in [Figure 8](#), after you Telnet to a Switch, you can run the `telnet` command to log in to, and configure, another Switch.

Figure 8 Providing Telnet Client Service

- 1 Authenticate the Telnet user through the console port on the Telnet Server (a Switch) before login.



By default, the password is required to authenticate Telnet users and to enable them to log on to the Switch. If a user logs in through Telnet without the password, the unit displays an error prompt .

```
<4500> system-view
[4500] user-interface vty 0
[4500-ui-vty0] set authentication password simple xxxx
```

(where xxxx is the preset login password of Telnet user)

- 2 The user logs in to the Telnet Client (Switch). For the login process, refer to the section [?<paratext>?](#) on [page 19](#).
- 3 Perform the following on the Telnet Client:


```
<4500> telnet xxxx
```

(xxxx can be the hostname or IP address of the Telnet Server. If it is the hostname, use the `ip host` command to specify.)
- 4 Enter the preset login password and you will see the prompt such <4500>. If the prompt `All user interfaces are used, please try later!` appears, it indicates that too many users are connected to the Switch through Telnet. In this case, connect later.
- 5 Use the corresponding commands to configure the Switch or view its running state. Enter `?` to view online help. For details of specific commands, refer to the following chapters.

Setting up Configuration Environment Through a Dial-up Modem

- 1 Authenticate the modem user through the console port of the Switch before the user logs in to the Switch through a dial-up modem.



By default, the password is required for authenticating the Modem user to log in to the Switch. If a user logs in through the Modem without the password, the user will see an error prompt.

```
<4500>system-view
[4500]user-interface aux 0
```

```
[4500-ui-aux0]set authentication password simple xxxx (xxxx is the preset login password of the Modem user.)
```

- 2 Perform the following configurations on the Modem that is directly connected to the Switch. (You are not required to configure the Modem connected to the terminal.)

```
AT&F -----Reset Modem factory settings
```

```
ATS0=1-----Set auto response (ring once)
```

```
AT&D -----Ignore DTR signal
```

```
AT&K0-----Disable flow control
```

```
AT&R1 -----Ignore RTS signal
```

```
AT&S0-----Force DSR to be high-level
```

```
ATEQ1&W----- Bar the modem to send command response or execution result and save the configurations
```

After the configuration, enter **AT&V** to verify the Modem settings.



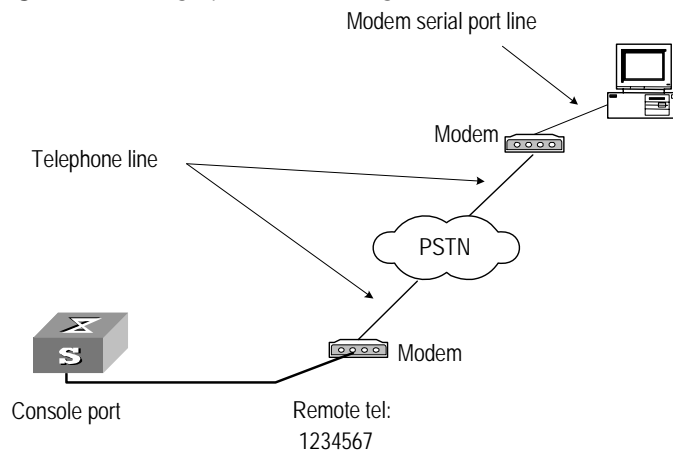
The Modem configuration commands and outputs may be different according to different Modems. For details, refer to the User Guide of the Modem.



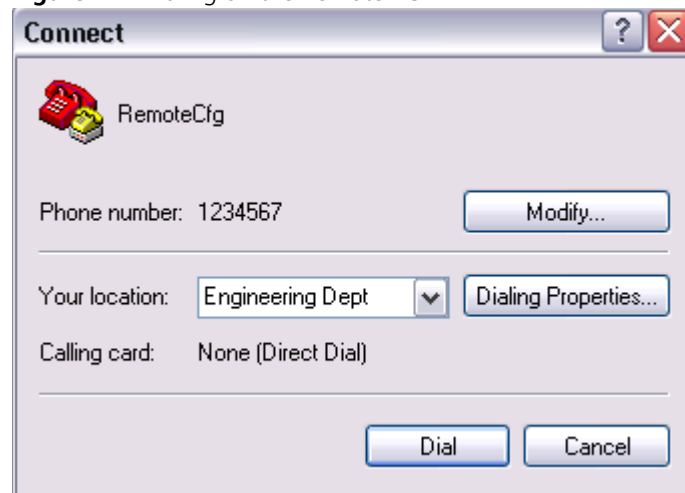
3Com recommends that the transmission rate on the console port must lower than that of Modem, otherwise packets may be lost.

- 3 To set up the remote configuration environment, connect the Modems to a PC (or a terminal) serial port and the Switch console port respectively (see [Figure 9](#)).

Figure 9 Setting up Remote Configuration Environment



- 4 Dial for connection to the Switch, using the terminal emulator and Modem on the remote end. The number you dial is the telephone number of the Modem connected to the Switch. See [Figure 10](#) and [Figure 11](#).

Figure 10 Setting the Dialed Number**Figure 11** Dialing on the Remote PC

- 5 Enter the preset login password on the remote terminal emulator and wait for the prompt <4500>. Then you can configure and manage the Switch. Enter ? to view online help. For details of specific commands, refer to the following chapters.



By default, after login, a modem user can access the commands at Level 0.

Command Line Interface

The Switch 4500 Family provides a series of configuration commands and command line interfaces for configuring and managing the Switch. The command line interface has the following characteristics:

- Local configuration through the console port.
- Local or remote configuration through Telnet or SSH.
- Remote configuration through a dial-up Modem to log in to the Switch.
- Hierarchy command protection to avoid the unauthorized users accessing the Switch.
- Access to online Help by entering ?.
- Network test commands, such as Tracert and Ping, to troubleshoot the network.
- Detailed debugging information to help with network troubleshooting.
- Ability to log in and manage other Switch 4500 units directly, using the Telnet command.
- FTP service for users to upload and download files.
- Ability to view previously executed commands.
- The command line interpreter that searches for a target not fully matching the keywords. You can enter the whole keyword or part of it, as long as it is unique and unambiguous.

Command Line View

The Switch 4500 Family provides hierarchy protection for command lines to avoid unauthorized users accessing it illegally.

Commands are classified into four levels, namely visit level, monitoring level, system level and management level:

- Visit level: Commands in this level include network diagnosis tools (such as **ping** and **tracert**), commands for the different language environments of the user interface (**language-mode**) and the **telnet** command etc. The saving of the configuration file is not allowed at this command level.
- Monitoring level: Commands in this level include the **display** command and the **debugging** command, and are used for system maintenance, service fault diagnosis, etc. The saving of the configuration file is not allowed at this command level.
- System level: Commands in this level include service configuration commands, including routing commands and commands for each network layer, and are used to provide direct network service to the user.
- Management level: Commands in this level include those that influence basic operation of the system and system support module, which plays a support role for services. Commands in this level include file system commands, FTP commands, TFTP commands, XModem downloading commands, user management commands, and level setting commands.

Login users are also classified into four levels that correspond to the four command levels respectively. After users of different levels log in, they can only use commands at the levels that are equal to or lower than their own level.

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

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

The command line provides the following views:

- User View
- System View
- Ethernet Port View
- VLAN View
- VLAN Interface View
- Local-User View
- User Interface View
- FTP Client View
- RSA Public Key View
- RSA Key Code View
- RIP View
- Route Policy View
- Basic ACL View
- Advanced ACL View
- Layer-2 ACL View
- User-Defined ACL View
- QoS Profile View
- RADIUS Server Group View
- ISP Domain View

[Table 5](#) describes the features of different views and the ways to enter or quit.

Table 5 Features of Command Views

Command view	Function	Prompt	Command to enter	Command to exit
User View	Show the basic information about operation and statistics	<4500>	This is the view you are in after connecting to the Switch	quit disconnects to the Switch
System View	Configure system parameters	[4500]	Enter system-view in User View	quit or return returns to User View
Ethernet Port View	Configure Ethernet port parameters	[4500-Ethernet1/0/1] [4500-GigabitEthernet1/0/24]	100M Ethernet Port View: Enter interface ethernet 1/0/1 in System View GigabitEthernet Port View: Enter interface gigabitethernet 1/0/24 in System View	quit returns to System View return returns to User View
VLAN View	Configure VLAN parameters	[4500-Vlan1]	Enter vlan 1 in System View	quit returns to System View return returns to User View
VLAN Interface View	Configure IP interface parameters for a VLAN or a VLAN aggregation	[4500-Vlan-interface1]	Enter interface vlan-interface 1 in System View	quit returns to System View return returns to User View
Local-User View	Configure local user parameters	[4500-user-user1]	Enter local-user user1 in System View	quit returns to System View return returns to User View
User Interface View	Configure user interface parameters	[4500-ui0]	Enter user-interface 0 in System View	quit returns to System View return returns to User View
FTP Client View	Configure FTP Client parameters	[4500-ftp]	Enter ftp in User View	quit returns to System View
RSA Public Key View	Configure RSA public key of SSH user	[4500-rsa-public-key]	Enter rsa peer-public-key 4500003 in System View	peer-public-key end returns to System View
RSA Key Code View	Edit RSA public key of SSH user	[4500-rsa-key-code]	Enter public-key-code begin in RSA Public Key View	public-key-code end returns to RSA Public Key View
RIP View	Configure RIP parameters	[4500-rip]	Enter rip in System View	quit returns to System View return returns to User View
Route Policy View	Configure route policy parameters	[4500-route-policy]	Enter route-policy policy1 permit node 10 in System View	quit returns to System View return returns to User View

Table 5 Features of Command Views

Command view	Function	Prompt	Command to enter	Command to exit
Basic ACL View	Define the rule of basic ACL	[4500-acl- basic-2000]	Enter acl number 2000 in System View	quit returns to System View return returns to User View
Advanced ACL View	Define the rule of advanced ACL	[4500-acl-adv-3000]	Enter acl number 3000 in System View	quit returns to System View return returns to User View
Layer-2 ACL View	Define the rule of layer-2 ACL	[4500-acl-ethernetframe-4000]	Enter acl number 4000 in System View	quit returns to System View return returns to User View
User-defined ACL View	Define the rule of user-defined ACL	[4500-acl-user-5000]	Enter acl number 5000 in System View	quit returns to System View return returns to User View
QoS profile View	Define QoS profile	[4500-qos-profile-h3c]	Enter qos-profile h3c in System View	quit returns to System View return returns to User View
RADIUS Server Group View	Configure radius parameters	[4500-radius-1]	Enter radius scheme 1 in System View	quit returns to System View return returns to User View
ISP Domain View	Configure ISP domain parameters	[4500-isp-3Com.net]	Enter domain 3Com.net in System View	quit returns to System View return returns to User View

Features and Functions of Command Line

Command Line Help

The command line interface provides full and partial online help.

You can get help information through the online help commands, which are described below:

- 1 Enter `?` in any view to get all the commands in that view.
- 2 Enter a command with a `?` separated by a space. If this position is for parameters, all the parameters and the corresponding brief descriptions will be listed.

```
[4500-EI]interface ?
```

```
Aux                Aux interface
Ethernet           Ethernet interface
GigabitEthernet    GigabitEthernet interface
Loopback           LoopBack interface
NULL              NULL interface
Vlan-interface     VLAN interface
```

- 3 Enter a character string followed by a `?`, then all the commands with this character string as their initials will be listed.

```
<4500>p?
```

```
ping
```

- 4 Enter a command with a character string and `?`, then all the keywords with this character string as their initials in the command will be listed.

```
<4500>display ver?
```

```
version
```

- 5 Enter the first letters of a keyword of a command and press `<Tab>`. If no other keywords begin with these letters, then this unique keyword will be displayed automatically.
- 6 To switch to the Chinese display for the above information, perform the `language-mode` command.

Displaying Characteristics of the Command Line

The command line interface provides a pausing function. If the information to be displayed exceeds one screen, users have three choices, as shown in [Table 6](#).

Table 6 Functions of Displaying

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

History Command

The command line interface provides a function similar to that of the DosKey. Commands entered by users are automatically saved by the command line interface and you can invoke and execute them at any time later. The history

command buffer is defaulted as 10. That is, the command line interface stores 10 history commands for each user. The operations are shown in [Table 7](#).

Table 7 Retrieving History Command

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



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

Common Command Line Error Messages

Incorrectly entered commands will cause error messages to be reported to users. The common error messages are listed in [Table 8](#).

Table 8 Common Command Line Error Messages

Error messages	Causes
Unrecognized command	<ul style="list-style-type: none"> ■ Cannot find the command ■ Cannot find the keyword ■ Wrong parameter type ■ The value of the parameter exceeds the range
Incomplete command	The command is incomplete.
Too many parameters	Too many parameters have been entered.
Ambiguous command	The parameters entered are not specific.

Editing Characteristics of Command Line

The command line interface provides basic command editing and supports the editing of multiple lines. A command cannot be longer than 256 characters. See [Table 9](#).

Table 9 Editing Functions

Key	Function
Common keys	Insert from the cursor position and the cursor moves to the right, if the edition buffer still has free space.
Backspace	Delete the character preceding the cursor and the cursor moves backward.
Leftwards cursor key <> or <Ctrl+B>	Move the cursor a character backward
Rightwards cursor key <> or <Ctrl+F>	Move the cursor a character forward
Up cursor key <> or <Ctrl+P>	Retrieve the history command.
Down cursor key <> or <Ctrl+N>	

Table 9 Editing Functions

Key	Function
<Tab>	Press <Tab> after typing an incomplete keyword and the system will display partial help: If the keyword matching the one entered is unique, the system will replace it with the complete keyword and display it in a new line; if there is no matched keyword or the matched keyword is not unique, the system will do no modification but display the originally typed word in a new line.

User Interface Configuration

User Interface Overview User interface configuration is another way provided by the Switch to configure and manage the port data.

Switch 4500 family Switches support the following configuration methods:

- Local configuration through the console port
- Local and remote configuration through Telnet or SSH through an Ethernet port
- Remote configuration through a dial-up modem through the console port.

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

- AUX user interface

AUX user interface is used to log in to the Switch through the console port. A fabric can have up to eight AUX user interfaces.

- VTY user interface

VTY user interface is used to Telnet to the Switch. A Switch can have up to five VTY user interfaces.



For SW4500 family Switches, AUX port, and console port are the same port. There is only the one type of AUX user interface.

The user interface is numbered by absolute number or relative number.

To number the user interface by absolute number:

- The AUX user interface is the first interface — user interface 0. The number ranges from 0 to 7.
- The VTY is numbered after the AUX user interface. The absolute number of the first VTY is the AUX user interface number plus 1. The number ranges from 8 to 12.

To number the user interface by relative number, represented by *interface + number* assigned to each type of user interface:

- AUX user interface = AUX 0.
- The first VTY interface = VTY 0, the second one = VTY 1, and so on.

User Interface Configuration

Tasks for configuring the user interface are described in the following sections:

- [Entering User Interface View](#)
- [Configuring the User Interface-Supported Protocol](#)
- [Configuring the Attributes of AUX \(Console\) Port](#)
- [Configuring the Terminal Attributes](#)
- [Managing Users](#)
- [Configuring Redirection](#)

Entering User Interface View

Use the `user-interface` command to enter a User Interface View. You can enter a single User Interface View or multi User Interface View to configure one or more user interfaces respectively.

Perform the following configuration in System View.

Table 10 Entering User Interface View

Operation	Command
Enter a single User Interface View or multi User Interface Views	<code>user-interface [type] first-number [last-number]</code>

Configuring the User Interface-Supported Protocol

The following command is used for setting the supported protocol by the current user interface. You can log in to the Switch only through the supported protocol. The configuration becomes effective when you log in again.

Perform the following configurations in User Interface (VTY user interface only) View.

Table 11 Configuring the User Interface-supported Protocol

Operation	Command
Configure the user interface-supported protocol	<code>protocol inbound { all ssh telnet }</code>

By default, the user interface supports Telnet and SSH protocols.



If the Telnet protocol is specified, to ensure a successful login through Telnet, you must configure the password by default.



If SSH protocol is specified, to ensure a successful login, you must configure the local or remote authentication of username and password using the `authentication-mode scheme` command. The `protocol inbound ssh` configuration fails if you configure `authentication-mode password` and `authentication-mode none`. When you configure SSH protocol successfully for the user interface, then you cannot configure `authentication-mode password` and `authentication-mode none` any more.

Configuring the Attributes of AUX (Console) Port

Use the `speed`, `flow control`, `parity`, `stop bit`, and `data bit` commands to configure these attributes of the AUX (console) port.

Perform the following configurations in User Interface (AUX user interface only) View.

Configuring the Transmission Speed on the AUX (Console) Port

Table 12 Configuring the Transmission Speed on the AUX (Console) Port

Operation	Command
Configure the transmission speed on the AUX (console) port	<code>speed speed_value</code>
Restore the default transmission speed on the AUX (console) port	<code>undo speed</code>

By default, the transmission speed on the AUX (console) port is 19200bps.

Configuring the Flow Control on the AUX (Console) Port

Table 13 Configuring the Flow Control on the AUX (Console) Port

Operation	Command
Configure the flow control on the AUX (console) port	<code>flow-control { hardware none software }</code>
Restore the default flow control mode on the AUX (console) port	<code>undo flow-control</code>

By default, the flow control on the AUX (console) port is none, that is, no flow control will be performed.

Configuring Parity on the AUX (Console) Port

Table 14 Configuring Parity on the AUX (Console) Port

Operation	Command
Configure parity mode on the AUX (console) port	<code>parity { even mark none odd space }</code>
Restore the default parity mode	<code>undo parity</code>

By default, the parity on the AUX (console) port is none, that is, no parity bit.

Configuring the Stop Bit of AUX (Console) Port

Table 15 Configuring the Stop Bit of AUX (Console) Port

Operation	Command
Configure the stop bit of the AUX (console) port	<code>stopbits { 1 1.5 2 }</code>
Restore the default stop bit of the AUX (console) port	<code>undo stopbits</code>

By default, the AUX (console) port supports 1 stop bit.

Configuring the Data Bit of the AUX (Console) Port

Table 16 Configuring the Data Bit of the AUX (Console) Port

Operation	Command
Configure the data bit of the AUX (console) port	<code>databits { 7 8 }</code>
Restore the default data bit of the AUX (console) port	<code>undo databits</code>

By default, the AUX (console) port supports 8 data bits.

Configuring the Terminal Attributes

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

Perform the following configuration in User Interface View. Perform the **lock** command in User View.

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

Table 17 Enabling/Disabling Terminal Service

Operation	Command
Enable terminal service	shell
Disable terminal service	undo shell

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

Note the following points:

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

Configuring Idle-timeout

Table 18 Configuring Idle-timeout

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

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

idle-timeout 0 Disables idle-timeout.

Locking the User Interface This configuration locks the current user interface and prompts the user to enter the password. This makes it impossible for others to operate in the interface after the user leaves.

Table 19 Locking the User Interface

Operation	Command
Lock user interface	lock

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

Table 20 Setting the Screen Length

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

By default, the terminal screen length is 24 lines.

screen-length 0 Disables screen display separation function.

Setting the History Command Buffer Size

Table 21 Setting the History Command Buffer Size

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

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

Managing Users

The management of users includes the setting of user login authentication method, level of command which a user can use after logging in, level of command which a user can use after logging in from a specific user interface, and command level.

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

Perform the following configuration in User Interface View.

Table 22 Configuring the Authentication Method

Operation	Command
Configure the authentication method	authentication-mode { password scheme }
Configure no authentication	authentication-mode none

By default, terminal authentication is not required for users logged in through the console port, whereas the password is required for authenticating the Modem and Telnet users when they log in.

1 Perform local password authentication to the user interface

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

Perform the following configuration in User Interface View.

Table 23 Configuring the local authentication password

Operation	Command
Configure the local authentication password	set authentication password { cipher simple }password
Remove the local authentication password	undo set authentication password

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

```
[4500]user-interface vty 0
[4500-ui-vty0]authentication-mode password
[4500-ui-vty0]set authentication password simple 3Com
```

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

Using the **authentication-mode scheme** command, you can perform local or remote authentication of username and password. The type of the authentication depends on your configuration.

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

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

```
[4500-ui-vty0]authentication-mode scheme
[4500-ui-vty0]quit
[4500]local-user zbr
[4500-luser-zbr]password simple 3Com
[4500-luser-zbr]service-type telnet
```

- 3 No authentication

```
[4500-ui-vty0]authentication-mode none
```



By default, the password is required for authenticating Modem and Telnet users when they log in. If the password has not been set, when a user logs in, he will see the prompt Login password has not been set!



*If the **authentication-mode none** command is used, the Modem and Telnet users will not be required to enter a password.*

Setting the command level used after a user has logged on The following command is used for setting the command level used after a user logs in.

Perform the following configuration in Local-User View.

Table 24 Setting the Command Level used after a User Logs In

Operation	Command
Set command level used after a user logs in	service-type { ftp [ftp-directory directory lan-access { ssh telnet terminal }* [level level] }

Table 24 Setting the Command Level used after a User Logs In

Operation	Command
Restore the default command level used after a user logs in	<code>undo service-type { ftp [ftp-directory] lan-access { ssh telnet terminal }* }</code>

By default, the specified logged-in user can access the commands at Level 1.

Setting the Command Level used after a User Logs In from a User Interface

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

Perform the following configuration in User Interface View.

Table 25 Setting the Command Level used after a User Logs In from a User Interface

Operation	Command
Set command level used after a user logs in from a user interface	<code>user privilege level level</code>
Restore the default command level used after a user logs in from a user interface	<code>undo user privilege level</code>

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



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

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

Perform the following configuration in System View.

Table 26 Setting the Command Priority

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



Do not change the command level unnecessarily for it may cause inconvenience with maintenance and operation.

Configuring Redirection

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

Perform the following configuration in User View.

Table 27 Configuring to Send Messages Between Different User Interfaces

Operation	Command
Configuring to send messages between different user interfaces.	send { all <i>number</i> <i>type number</i> }

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

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

Perform the following configuration in User Interface View.

Table 28 Configuring to Automatically Run the Command

Operation	Command
Configure to automatically run the command	auto-execute command <i>text</i>
Configure not to automatically run the command	undo auto-execute command

Note the following points:

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

Telnet 10.110.100.1 after the user logs in through VTY0 automatically.

```
[4500-ui-vty0]auto-execute command telnet 10.110.100.1
```

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

Displaying and Debugging User Interface

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

Use the **free** command in User View to clear a specified user interface.

Table 29 Displaying and Debugging User Interface

Operation	Command
Clear a specified user interface	free user-interface [<i>type</i>] <i>number</i>

Table 29 Displaying and Debugging User Interface

Operation	Command
Display the user application information of the user interface	display users [all]
Display the physical attributes and some configurations of the user interface	display user-interface [type number number] [summary]

Default Configuration File Description

To facilitate management, 3Com Switch 4500 provides a default configuration file named "3ComOScfg.def". This file contains local users configuration for login to the device and SNMP parameters configuration for NMS management. In addition, it provides configurations for basic services, for example, it provides basic flow control settings to avoid impact on the access network due to excessive traffic.

Switch 4500 loads the default configuration file during first startup. You can use a username and password predefined in the file to log into the device and use a NMS to manage the device remotely.



Configurations for some features in the default configuration file differ from the default settings of such features described in the corresponding chapters of this manual.

- *If the device starts up by using the default configuration file, configurations for those features in the default configuration file are used as their default settings.*
- *If not, those features use the default settings described in the corresponding chapters of this manual.*

The following introduces the device management configuration and service configuration contained in the default configuration file.

Device Management Configuration

Local Users Configuration

The default configuration file of Switch 4500 predefines three local users. You can use one of them to login to the device as needed.

Table 30 Users predefined in the default configuration file

User name	Password	Level	Available login modes	Description
admin	Not set	3	<ul style="list-style-type: none"> ■ ssh ■ telnet ■ terminal 	The admin user has the highest authority. You are recommended to modify its password after first login to ensure device security.
manager	manager	2	<ul style="list-style-type: none"> ■ ssh ■ telnet ■ terminal 	The manager user can execute all configuration commands except for management-level commands.

Table 30 Users predefined in the default configuration file

User name	Password	Level	Available login modes	Description
monitor	monitor	1	<ul style="list-style-type: none"> ■ ssh ■ telnet ■ terminal 	The monitor user can execute commands for system maintenance and troubleshooting.

VLAN Interface and IP Address Configuration

After startup by using the default configuration file, Switch 4500 automatically creates VLAN-interface 1, and obtains an IP address for the interface through DHCP (A DHCP server must exist on the network and has assignable IP addresses.).

You can use the `display ip interface brief` command to view the IP address of VLAN-interface 1 after logging into the device through the Console port, and use that IP address to telnet to the device or to manage the device through NMS remotely.

SNMP Configuration

After startup by using the default configuration file, Switch 4500 enables the SNMP agent, which has the following settings:

- Name of the community with read access right: public
- Name of the community with write access right: private
- SNMP versions supported: all (that is, v1, v2c, and v3)

Services Configuration



The following port-related configurations are effective for 100 Mbps ports only. The default configuration file contains no configurations for 1000 Mbps ports.

STP

By default, STP is enabled on all the ports of Switch 4500. If you connect a PC to a port of the device, the port needs 30 seconds to enter the forwarding state. To reduce the wait time, the default configuration file configures all the ports as STP edge ports. In this way, a port immediately enters the forwarding state after a device is connected to it.

Broadcast Storm Suppression

To avoid broadcast storms, the default configuration file of Switch 4500 enables the broadcast storm suppression function on all ports and sets the threshold as 3000 pps.

Illegal Packet Filtering

Packets with a destination IP address of all-zero are illegal. To stop propagation of such packets, the default configuration file of Switch 4500 creates an ACL numbered 4999 to match such packets, and enables the packet-filter function on all ports. In this way, a port will discard packets matching ACL 4999.

Priority Trust Modes on Ports

The default configuration file of Switch 4500 sets the priority trust mode of all ports as trusting the 802.1p priority of packets. That is, the device puts packets into different queues according to their 802.1p priorities.

IGMP-Snooping

To avoid security problems caused by flooding multicast traffic, the default configuration file of Switch 4500 enables global IGMP Snooping and IGMP Snooping on VLAN 1. In this way, the device will automatically maintain multicast entries and send multicast traffic through specified ports only.

2

PORT OPERATION

This chapter covers the following topics:

- [Ethernet Port Configuration](#)
- [Link Aggregation Configuration](#)

Ethernet Port Configuration

Ethernet Port Overview

The following features are found in the Ethernet ports of the Switch 4500

- 10/100BASE-T Ethernet ports support MDI/MDI-X auto-sensing. They can operate in half-duplex, full-duplex and auto-negotiation modes. They can negotiate with other network devices to determine the operating mode and speed. Thus the appropriate operating mode and speed is automatically configured and the system configuration and management is greatly streamlined.
- Gigabit SFP ports operate in 1000Mbps full duplex mode. The duplex mode can be set to **full** (full-duplex) and **auto** (auto-negotiation) and its speed can be set to **1000** (1000Mbps) and **auto** (auto-negotiation).

The configuration of these Ethernet ports is fundamentally the same and is described in the following sections.

Ethernet Port Configuration

Ethernet port configuration is described in the following sections:

- [Entering Ethernet Port View](#)
- [Enabling/Disabling an Ethernet Port](#)
- [Setting the Description Character String for the Ethernet Port](#)
- [Setting the Duplex Attribute of the Ethernet Port](#)
- [Setting Speed on the Ethernet Port](#)
- [Setting the Cable Type for the Ethernet Port](#)
- [Enabling/Disabling Flow Control for the Ethernet Port](#)
- [Setting the Ethernet Port Suppression Ratio](#)
- [Setting the Link Type for an Ethernet Port](#)
- [Adding an Ethernet Port to Specified VLANs](#)
- [Setting the Default VLAN ID for the Ethernet Port](#)
- [Setting Loopback Detection for an Ethernet Port](#)
- [Copying Port Configuration to Other Ports](#)



Entering Ethernet Port View

Before configuring an Ethernet port, enter Ethernet Port View.

Perform the following configuration in System View.

Table 30 Entering Ethernet Port View

Operation	Command
Enter Ethernet Port View	interface { <i>interface_type</i> <i>interface_num</i> <i>interface_name</i> }

Enabling/Disabling an Ethernet Port

Use the following command to disable or enable the port. After configuring the related parameters and protocol of the port, you can use the following command to enable the port. If you do not want a port to forward data, use the command to disable it.

Perform the following configuration in Ethernet Port View.

Table 31 Enabling/Disabling an Ethernet Port

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

By default, the port is enabled.

Setting the Description Character String for the Ethernet Port

To distinguish the Ethernet ports, use the following command to assign a description to each port.

Perform the following configuration in Ethernet Port View.

Table 32 Setting the Description Character String for the Ethernet Port

Operation	Command
Set description character string for Ethernet port.	description <i>text</i>
Delete the description character string of Ethernet.	undo description

By default, the port description is a null character string.

Setting the Duplex Attribute of the Ethernet Port

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

Perform the following configuration in Ethernet Port View.

Table 33 Setting the Duplex Attribute for the Ethernet Port

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

Note that 10/100BASE-T Ethernet ports support full duplex, half duplex and auto-negotiation, which can be set as required. Gigabit Ethernet ports support full duplex and can be configured to operate in **full** (full duplex) or **auto** (auto-negotiation) mode.

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

Setting Speed on the Ethernet Port

Use the following command to set the speed of the Ethernet port. If the speed is set to auto-negotiation mode, the local and peer ports will automatically negotiate the port speed.

Perform the following configuration in Ethernet Port View.

Table 34 Setting Speed on the Ethernet Port

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

Note that 10/100BASE-T Ethernet ports support 10Mbps, 100Mbps and auto-negotiation, which can be set as required. Gigabit Ethernet ports support 1000Mbps and can be configured to operate at **1000** (1000Mbps) or **auto** (auto-negotiation) speed.

By default, the speed of the port set to **auto** mode.

Setting the Cable Type for the Ethernet Port

Ethernet ports support straight-through and cross-over network cables. Use the following command to configure the cable type.

Perform the following configuration in Ethernet Port View.

Table 35 Setting the Type of the Cable Connected to an Ethernet Port

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

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

Enabling/Disabling Flow Control for the Ethernet Port

After flow control is enabled in both the local and the peer Switch, if congestion occurs in the local Switch, the Switch will inform its peer to pause packet sending. In this way, packet loss is reduced. The flow control function of the Ethernet port can be enabled or disabled using the following command.

Perform the following configuration in Ethernet Port View.

Table 36 Enabling/Disabling Flow Control for an Ethernet Port

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

By default, Ethernet port flow control is disabled.

Setting the Ethernet Port Suppression Ratio

Use the following commands to restrict broadcast/multicast/unicast traffic. Once traffic exceeds the value set by the user, the system will maintain an appropriate packet ratio by discarding the overflow traffic, so as to suppress storm, avoid congestion and ensure the normal service.

Perform the following configuration in Ethernet Port View.

Table 37 Setting the Ethernet Port Suppression Ratio

Operation	Command
Set Ethernet port broadcast suppression ratio	broadcast-suppression { <i>ratio</i> pps bandwidth }
Restore the default Ethernet port broadcast suppression ratio	undo broadcast-suppression
Set Ethernet port multicast suppression ratio	multicast-suppression { <i>ratio</i> pps bandwidth }
Restore the default Ethernet port multicast suppression ratio	undo multicast-suppression
Set Ethernet port unicast suppression ratio	unicast-suppression { <i>ratio</i> pps bandwidth }
Restore the default Ethernet port unicast suppression ratio	undo unicast-suppression

By default, all traffic is allowed to pass through, that is, no suppression is performed.

Setting the Link Type for an Ethernet Port

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

Perform the following configuration in Ethernet Port View.

Table 38 Setting the Link Type for the Ethernet Port

Operation	Command
Configure the port as an access port	port link-type access

Table 38 Setting the Link Type for the Ethernet Port

Operation	Command
Configure the port as a hybrid port	<code>port link-type hybrid</code>
Configure the port as a trunk port	<code>port link-type trunk</code>
Configure the port as a stack port	<code>port link-type xrn-fabric</code>
Restore the default link type, that is, access port	<code>undo port link-type</code>

By default, the port is access port.

Note that:

- You can configure four types of ports concurrently on the same Switch, but you cannot switch port type between trunk port, hybrid port and stack port. You must return it first into access port and then set it as the other type. For example, you cannot configure a trunk port directly as a hybrid port, but first set it as an access port and then as a hybrid port.
- For the Switch 4500 26-Port and Switch 4500 26-Port PWR, GigabitEthernet1/0/25 and GigabitEthernet1/0/26 ports can be configured as a stack port; For the Switch 4500 50-Port and Switch 4500 50-Port PWR, GigabitEthernet1/0/49 and GigabitEthernet1/0/50 ports can be configured as a stack port.

Adding an Ethernet Port to Specified VLANs

Use the following commands to add an Ethernet port to a specified VLAN. An access port can only be added to one VLAN, while hybrid and trunk ports can be added to multiple VLANs.

Perform the following configuration in Ethernet Port View.

Table 39 Adding the Ethernet Port to Specified VLANs

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

Note that the access port shall be added to an existing VLAN other than VLAN 1. The VLAN to which a hybrid port is added must already exist. The one to which a trunk port is added cannot be VLAN 1.

After adding an Ethernet port to specified VLANs, the local port can forward packets of these VLANs. Hybrid and trunk ports can be added to multiple VLANs, thereby implementing the VLAN intercommunication between peers. For a hybrid

port, you can configure to tag some VLAN packets, based on which the packets can be processed differently.

Setting the Default VLAN ID for the Ethernet Port

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

Perform the following configuration in Ethernet Port View.

Table 40 Setting the Default VLAN ID for an Ethernet Port

Operation	Command
Set the default VLAN ID for a hybrid port.	<code>port hybrid pvid vlan vlan_id</code>
Set the default VLAN ID for a trunk port	<code>port trunk pvid vlan vlan_id</code>
Restore the default VLAN ID of a hybrid port to the default value	<code>undo port hybrid pvid</code>
Restore the default VLAN ID of a trunk port to the default value	<code>undo port trunk pvid</code>

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

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

Setting Loopback Detection for an Ethernet Port

Use the following command to enable port loopback detection and set the detection interval for the external loopback condition of each port. If there is a loopback port found, the Switch will put it under control.

Other correlative configurations function only when port loopback detection is enabled in System View.

Perform the following configuration in the view listed in [Table 42](#).

Table 41 Setting Loopback Detection for the Ethernet Port

Operation	Command
Enable loopback detection on the port (System View/Ethernet Port View)	<code>loopback-detection enable</code>
Disable loopback detection on the port (System View/Ethernet Port View)	<code>undo loopback-detection enable</code>
Enable the loopback controlled function of the trunk and hybrid ports (Ethernet Port View)	<code>loopback-detection control enable</code>
Disable the loopback controlled function of the trunk and hybrid ports (Ethernet Port View)	<code>undo loopback-detection control enable</code>

Table 41 Setting Loopback Detection for the Ethernet Port

Operation	Command
Set the external loopback detection interval of the port (System View)	loopback-detection interval-time <i>time</i>
Restore the default external loopback detection interval of the port (System View)	undo loopback-detection interval-time
Configure that the system performs loopback detection to all VLANs on Trunk and Hybrid ports (Ethernet Port View)	loopback-detection per-vlan enable
Configure that the system only performs loopback detection to the default VLANs on the port (Ethernet Port View)	undo loopback-detection per-vlan enable

By default, port loopback detection and the loopback detection control function on trunk and hybrid ports are disabled. The detection interval is 30 seconds, and the system detects the default VLAN on the trunk and hybrid ports.

Copying Port Configuration to Other Ports

To keep the configuration of other ports consistent with a specified port, you can copy the configuration of that specified port to other ports. The configuration may include: STP setting, QoS setting, VLAN setting, port setting, and LACP setting. The STP setting includes STP enabling/disabling, link attribute (point-to-point or not), STP priority, path cost, max transmission speed, loop protection, root protection, edge port or not. The QoS setting includes traffic limiting, priority marking, default 802.1p priority, bandwidth assurance, congestion avoidance, traffic redirection, and traffic statistics. The VLAN setting includes permitted VLAN types, and default VLAN ID. The port setting includes port link type, port speed, and duplex mode. LACP setting includes LACP enabling/disabling.

Perform the following configuration in System View.

Table 42 Copying Port Configuration to Other Ports

Operation	Command
Copy port configuration to other ports	copy configuration source { <i>interface_type interface_number</i> <i>interface_name</i> aggregation_group agg_id } destination { <i>interface_list</i> [aggregation_group agg_id] aggregation_group agg_id }

Note that if the copy source is an aggregation group, take the port with minimum ID as the source; if the copy destination is an aggregation group, make the configurations of all group member ports identical with that of the source.

Displaying and Debugging Ethernet Port

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

Enter the **reset** command in User View to clear the statistics information of the port.

Enter the **loopback** command in Ethernet Port View to check whether the Ethernet port works normally. In the process of the loopback test, the port cannot forward any packets. The loop test will finish automatically after a short time.

Table 43 Displaying and Debugging Ethernet Port

Operation	Command
Perform loopback test on the Ethernet port.	loopback { external internal }
Display all port information	display interface { <i>interface_type</i> <i>interface_type interface_num</i> <i>interface_name</i> }
Display port information of a specific unit	display unit <i>unit_id</i> interface
Display hybrid port or trunk port	display port { hybrid trunk }
Display the state of loopback detection on the port.	display loopback-detection
Clear statistics information of the port	reset counters interface [<i>interface_type</i> <i>interface_type interface_num</i> <i>interface_name</i>]

Note that:

- The loopback test cannot be performed on a port disabled by the **shutdown** command. During the loopback test, the system will disable **speed**, **duplex**, **mdi** and **shutdown** operation on the port. Some ports do not support the loopback test. If performing this command in these ports, you will see the system prompt.
- After 802.1X is enabled, the port information cannot be reset.

Ethernet Port Configuration Example

Networking Requirements

Switch A is connected to Switch B through Trunk port Ethernet1/0/1. Configure the trunk port with a default VLAN ID, so that:

- When receiving packets without a VLAN Tag, the port can forward them to the member ports belonging to the default VLAN
- When it is sending the packets with VLAN Tag and the packet VLAN ID is the default VLAN ID, the trunk port will remove the packet VLAN Tag and forward the packet.

Networking Diagram

Figure 12 Configuring the Default VLAN for a Trunk Port



Configuration Procedure

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

- 1 Enter the Ethernet Port View of Ethernet1/0/1.

```
[4500]interface ethernet1/0/1
```
- 2 Set the Ethernet1/0/1 as a trunk port and allow VLAN 2, 6 through 50, and 100 to pass through.

```
[4500-Ethernet1/0/1]port link-type trunk
[4500-Ethernet1/0/1]port trunk permit vlan 2 6 to 50 100
```
- 3 Create the VLAN 100.

```
[4500]vlan 100
```
- 4 Configure the default VLAN ID of Ethernet1/0/1 as 100.

```
[4500-Ethernet1/0/1]port trunk pvid vlan 100
```

Ethernet Port Troubleshooting

Fault: Default VLAN ID configuration failed.

Troubleshooting: Take the following steps.

- 1 Use the **display interface** or **display port** command to check if the port is a trunk port or a hybrid port. If it is neither, configure it as a trunk port or a hybrid port.
- 2 Configure the default VLAN ID.

Link Aggregation Configuration

Overview Brief Introduction to Link Aggregation

Link aggregation means aggregating several ports together to implement the outgoing/incoming payload balance among the member ports and enhance the connection reliability. Link aggregation includes manual aggregation, dynamic LACP aggregation, and static LACP aggregation. In terms of load sharing, link aggregation may be load sharing aggregation and non-load sharing aggregation.

For the member ports in an aggregation group, their basic configurations must be the same. That is, if one is a trunk port, the others must also be; when it turns into access port, then others must change to access port.

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

The Switch 4500 26-Port can support up to 14 aggregation groups, the Switch 4500 50-Port can support up to 26 aggregation groups. Each group can have a maximum of eight 100 Mbps Ethernet ports or four Gigabit SFP ports. For the Switch 4500 series, the ports in an aggregation group must physically belong to the same unit.

Brief Introduction to LACP

IEEE802.3ad-based Link Aggregation control protocol (LACP) implements dynamic link aggregation and disaggregation and exchanges information with the peer through LACP data unit (LACPDU). When LACP is enabled on it, the port notifies, through sending LACPDU, the peer of its system priority, system MAC, port priority, port number and operation key. On receiving this information, the peer compares the received information with that stored at other ports to determine which ports can be aggregated, so that the two parties can agree on adding/deleting which port into/from a certain dynamic aggregation group.

The operation key is a configuration set generated by LACP based on port setting (speed, duplex mode, basic configuration and management key). When LACP is enabled, the management key of a dynamic aggregation port is 0 by default, but the management key of a static aggregation port consists with the aggregation group ID. For a dynamic aggregation group, all member ports must have the same operation key, while for a manual or static aggregation group, only the active member ports must have the same operation key.

Types of Link Aggregation

The types of link aggregation are described in the following sections:

- [Manual Aggregation and Static LACP Aggregation](#)
- [Dynamic LACP Aggregation](#)

Manual Aggregation and Static LACP Aggregation Both manual aggregation and static LACP aggregation require manual configuration of aggregation groups and prohibit automatic adding or deleting of member ports by the system. A manual or static LACP aggregation group must contain at least one member port, and you must delete the aggregation group, instead of the port, if the group contains only one port. At a manual aggregation port, LACP is disabled and you are not allowed to enable it. LACP is enabled at a static aggregation port. When a static aggregation group is deleted, its member ports form one or several dynamic LACP aggregation groups and LACP remains enabled on them. You are not allowed to disable LACP protocol at a static aggregation group.

In a manual or static LACP aggregation group, its ports may be in active or inactive state and only the active ports can transceive user service packets. The active port

with the minimum port number serves as the master port, while others as sub-ports.

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

- The system sets the port with the highest priority to active state, and others to inactive state based on the following descending order of priority levels:
 - full duplex/high speed
 - full duplex/low speed
 - half duplex/high speed
 - half duplex/low speed
- The system sets to inactive state the ports which cannot aggregate with the active port with minimum port number, due to hardware limit, for example, trans-board aggregation unavailable.
- The system sets to inactive state the ports with basic configurations different from that of the active port with minimum port number.

In a static LACP aggregation group, the system sets the ports to active or inactive state by using these rules:

- The system sets the port with the highest priority to active state, and others to inactive state based on the following descending order of priority levels:
 - full duplex/high speed
 - full duplex/low speed
 - half duplex/high speed
 - half duplex/low speed
- The system sets to inactive state the ports which connect to different peer devices from one that the active port with minimum port number connects to, or the ports in different aggregation groups though they are connected to the same peer device.
- The system sets to inactive state the ports which cannot aggregate with the active port with minimum port number, due to hardware limit, for example, trans-board aggregation unavailable.
- The system sets to inactive state the ports with basic configurations different from that of the active port with minimum port number.

Because only a defined number of ports can be supported in an aggregation group, if the active ports in an aggregation group exceed the port quantity threshold for that group, the system shall set some ports with smaller port numbers (in ascending order) as selected ports and others as standby ports. Both selected and standby ports can transceive LACP protocol, but standby ports cannot forward user service packets.

Dynamic LACP Aggregation

The LACP uses peer exchanges across the links to determine, on an ongoing basis, the aggregation capability of the various links, and continuously provides the maximum level of aggregation capability achievable between a given pair of

systems as well as under manual control through direct manipulation of the state variables of Link Aggregation (for example, keys) by a network manager.

Dynamic LACP aggregation can be established even for a single port, as is called single port aggregation. LACP is enabled at dynamic aggregation ports. Only the ports with the same speed, duplex mode and basic configuration and connected to the same device can be aggregated dynamically.

Because only a defined number of ports can be supported in an aggregation group, if the ports in an aggregation group exceed the port quantity threshold for that group, the system shall set some ports with smaller system IDs (system priority + system MAC address) and port IDs (port priority + port number) as selected ports and others as standby ports. If not, all member ports are selected ports. Both selected and standby ports can transceive LACP protocol, but standby ports cannot forward user service packets. Among the selected ports of an aggregation group, the one with minimum port number serves as the master port for that group and the others are sub-ports.

In comparing system IDs, the system first compares system priority values; if they are equal, then it compares system MAC addresses. The smaller system ID is given priority. Comparing port IDs follows the same process: the system first compares port priority values and then port numbers and the smaller port ID is given priority. If system ID changes from non-priority to priority, then the selected or standby state is determined by the port priority of the system. You can decide whether the port is selected or standby by setting system priority and port priority.

Load Sharing

In terms of load balancing, link aggregation may be load balancing aggregation and non-load balancing aggregation. In general, the system only provides limited load balancing aggregation resources, so the system needs to rationally allocate these resources among manual aggregation groups, static LACP aggregation groups, dynamic LACP aggregation groups, and the aggregation groups including special ports which require hardware aggregation resources. The system will always allocate hardware aggregation resources to the aggregation groups with higher priority levels. When the load sharing aggregation resources are used up for existing aggregation groups, newly-created aggregation groups will be non-load sharing ones. The priority levels (in descending order) for allocating load sharing aggregation resources are as follows:

- Aggregation groups including special ports which require hardware aggregation resources
- Manual and static LACP aggregation groups
- Aggregation groups that probably reach the maximum rate after the resources are allocated to them
- Aggregation groups with the minimum master port numbers if they reach the equal rate with other groups after the resources are allocated to them

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

A load sharing aggregation group may contain several selected ports, but a non-load sharing aggregation group can only have one selected port, while others are standby ports. Selection criteria of selected ports vary for different types of aggregation groups.

Link Aggregation Configuration

Link aggregation configuration is described in the following sections:

- [Enabling/Disabling LACP](#)
- [Creating/Deleting an Aggregation Group](#)
- [Adding/Deleting an Ethernet Port into/from an Aggregation Group](#)
- [Setting/Deleting the Aggregation Group Descriptor](#)
- [Configuring System Priority](#)
- [Configuring Port Priority](#)

Enabling/Disabling LACP

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

Perform the following configuration in Ethernet Port View.

Table 44 Enabling/Disabling LACP

Operation	Command
Enable LACP at the port	<i>lacp enable</i>
Disable LACP at the port	undo lacp enable

By default, LACP is disabled at the port.

Note that:

- You cannot enable LACP at a
 - stack port
 - mirrored port
 - port with a static MAC address configured
 - port with static ARP configured
 - port with 802.1X enabled
 - port in a manual aggregation group
- You can add a port with LACP enabled into a manual aggregation group, but then the LACP will be disabled on it automatically. Or you can add a port with LACP disabled into a static LACP aggregation group, and then the LACP will be enabled automatically.
- The Switch selects the port with the minimum port number as the master port of the aggregation group. This rule applies to all aggregation groups.

Creating/Deleting an Aggregation Group

Use the following command to create a manual aggregation group or static LACP aggregation group, but the dynamic LACP aggregation group is established by the system when LACP is enabled on the ports. You can also delete an existing

aggregation group: when you delete a manual aggregation group, all its member ports are disaggregated; when you delete a static or dynamic LACP aggregation group, its member ports form one or several dynamic LACP aggregation groups.

Perform the following configuration in System View.

Table 45 Creating/Deleting an Aggregation Group

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

The Switch selects the port with the minimum port number as the master port of the aggregation group. This rule applies to all aggregation groups.

A manual or static aggregation group can have up to eight ports. To change an existing dynamic aggregation group into a manual or static group enter:

```
link-aggregation group agg-id mode
```

If the port number in a group exceeds eight, you will be prompted that a configuration failure has occurred.

If the aggregation group you create already exists but contains no member port, you can overwrite the existing group; if it already exists in the system and contains member ports, then you can only change a dynamic or static LACP aggregation group to a manual one, or a dynamic LACP aggregation group to a static one. In the former case, LACP shall be disabled at the member ports automatically, while in the latter case, LACP shall remain enabled.

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

You can add/delete ports into/from a manual or static LACP aggregation group, but member port adding or deleting for a dynamic LACP aggregation group is implemented by the system.

Perform the following configuration in Ethernet Port View.

Table 46 Adding/Deleting an Ethernet Port into/from an Aggregation Group

Operation	Command
Add an Ethernet port into the aggregation group	port link-aggregation group <i>agg_id</i>
Delete an Ethernet port from the aggregation port	undo port link-aggregation group

Note that:

- You cannot enable LACP for a
 - stack port
 - mirrored port
 - port with static MAC address configured
 - port with static ARP configured

- port with 802.1X enabled.
- You must delete the aggregation group, instead of the port, if the manual or static LACP aggregation group contains only one port.

Setting/Deleting the Aggregation Group Descriptor

Perform the following configuration in System View.

Table 47 Setting/Deleting the Aggregation Group Descriptor

Operation	Command
Set aggregation group descriptor	link-aggregation group <i>agg_id</i> description <i>aname</i>
Delete aggregation group descriptor	undo link-aggregation group <i>agg_id</i> description

By default, an aggregation group has no descriptor.



*If you have saved the current configuration with the **save** command, the configured manual aggregation groups, static LACP aggregation groups and corresponding descriptors exist when the system reboots. But the dynamic LACP aggregation groups do not exist, and even the descriptors configured for them will not be restored.*

Configuring System Priority

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

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

Perform the following configuration in System View.

Table 48 Configuring System Priority

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

By default, system priority is 32768.

Configuring Port Priority

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

Perform the following configuration in Ethernet Port View.

Table 49 Configuring Port Priority

Operation	Command
Configure port priority	lacp port-priority <i>port_priority_value</i>
Restore the default port priority	undo lacp port-priority

By default, port priority is 32768.

Displaying and Debugging Link Aggregation

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

You can also enter, in User View, the **reset** command to clear LACP statistics of the port and **debugging** commands to debug LACP.

Table 50 Displaying And Debugging Link Aggregation

Operation	Command
Display summary information of all aggregation groups	display link-aggregation summary
Display detailed information of a specific aggregation group	display link-aggregation verbose [<i>agg_id</i>]
Display local system ID	display lacp system-id
Display detailed link aggregation information at the port	display link-aggregation interface { <i>interface_type interface_number interface_name</i> } [to { <i>interface_type interface_num interface_name</i> }]
Clear LACP statistics at the port	reset lacp statistics [interface { <i>interface_type interface_number interface_name</i> } [to { <i>interface_type interface_num interface_name</i> }]]
Disable/enable debugging LACP state machine	[undo] debugging lacp state [interface { <i>interface_type interface_number interface_name</i> } [to { <i>interface_type interface_num interface_name</i> }]] [{ actor-churn mux partner-churn ptx rx } * all]
Disable/enable debugging LACP packets	[undo] debugging lacp packet [interface { <i>interface_type interface_number interface_name</i> } [to { <i>interface_type interface_num interface_name</i> }]]
Disable/enable debugging link aggregation errors	[undo] debugging link-aggregation error
Disable/enable debugging link aggregation events	[undo] debugging link-aggregation event

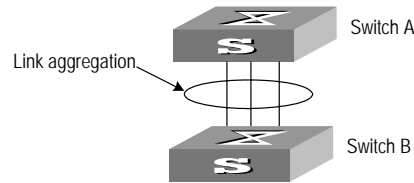
Link Aggregation Configuration Example

Networking Requirement

Switch A connects Switch B with three aggregation ports, numbered as Ethernet1/0/1 to Ethernet1/0/3, so that incoming/outgoing load can be balanced among the member ports.

Networking Diagram

Figure 13 Networking for Link Aggregation



Configuration Procedure

The following only lists the configuration for Switch A; configure Switch B similarly.

1 Manual link aggregation

- a** Create manual aggregation group 1.

```
[4500]link-aggregation group 1 mode manual
```

- b** Add Ethernet ports Ethernet1/0/1 to Ethernet1/0/3 into aggregation group 1.

```
[4500]interface ethernet1/0/1
[4500-Ethernet1/0/1]port link-aggregation group 1
[4500-Ethernet1/0/1]interface ethernet1/0/2
[4500-Ethernet1/0/2]port link-aggregation group 1
[4500-Ethernet1/0/2]interface ethernet1/0/3
[4500-Ethernet1/0/3]port link-aggregation group 1
```

2 Static LACP aggregation

- a** Create static LACP aggregation group 1.

```
[4500]link-aggregation group 1 mode static
```

- b** Add Ethernet ports Ethernet1/0/1 to Ethernet1/0/3 into aggregation group 1.

```
[4500]interface ethernet1/0/1
[4500-Ethernet1/0/1]port link-aggregation group 1
[4500-Ethernet1/0/1]interface ethernet1/0/2
[4500-Ethernet1/0/2]port link-aggregation group 1
[4500-Ethernet1/0/2]interface ethernet1/0/3
[4500-Ethernet1/0/3]port link-aggregation group 1
```

3 Dynamic LACP aggregation

- a** Enable LACP at Ethernet ports Ethernet1/0/1 to Ethernet1/0/3.

```
[4500]interface ethernet1/0/1
[4500-Ethernet1/0/1]lacp enable
[4500-Ethernet1/0/1]interface ethernet1/0/2
[4500-Ethernet1/0/2]lacp enable
[4500-Ethernet1/0/2]interface ethernet1/0/3
[4500-Ethernet1/0/3]lacp enable
```

Only when the three ports are configured with identical basic configuration, rate and duplex mode, can they be added into a same dynamic aggregation group after LACP is enabled on them, for load sharing.

3

VLAN OPERATION

This chapter covers the following topics:

- [VLAN Configuration](#)
- [Voice VLAN Configuration](#)

VLAN Configuration

VLAN Overview A virtual local area network (VLAN) creates logical groups of LAN devices into segments to implement virtual workgroups. IEEE issued the IEEE 802.1Q in 1999, which was intended to standardize VLAN implementation solutions.

Using VLAN technology, you can logically divide the physical LAN into different broadcast domains. Every VLAN contains a group of workstations with the same demands. However, the workstations of a VLAN do not have to belong to the same physical LAN segment.

Within a VLAN, broadcast and unicast traffic is not forwarded to other VLANs. Therefore, VLAN configurations are very helpful in controlling network traffic, saving device investment, simplifying network management and improving security.

Configuring a VLAN VLAN configuration is described in the following sections:

- [Creating/Deleting a VLAN](#)
- [Adding Ethernet Ports to a VLAN](#)
- [Setting/Deleting a VLAN or VLAN Interface Description Character String](#)
- [Specifying/Removing the VLAN Interface](#)
- [Shutting Down/Enabling the VLAN Interface](#)

To configure a VLAN, first create a VLAN according to network requirements.

Creating/Deleting a VLAN

Use the following command to create/delete a VLAN. If the VLAN to be created exists, enter the VLAN View directly. Otherwise, create the VLAN first, and then enter the VLAN View.

Perform the following configurations in System View.

Table 51 Creating/Deleting a VLAN

Operation	Command
Create a VLAN and enter the VLAN View	<code>vlan vlan_id</code>

Table 51 Creating/Deleting a VLAN

Operation	Command
Delete the specified VLAN	undo vlan { <i>vlan_id</i> [to <i>vlan_id</i>] all }

Note that the default VLAN, namely VLAN 1, cannot be deleted.

Adding Ethernet Ports to a VLAN

Use the following command to add Ethernet ports to a VLAN.

Perform the following configuration in VLAN View.

Table 52 Adding Ethernet Ports to a VLAN

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

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

Note that you can add/delete a trunk port or a hybrid port to/from VLAN by using the **port** and **undo port** commands in Ethernet Port View, but not in VLAN View.

Setting/Deleting a VLAN or VLAN Interface Description Character String

Use the following command to set/delete a VLAN or VLAN interface description character string.

Perform the following configuration in VLAN or VLAN Interface View.

Table 53 Setting/Deleting a Vlan or Vlan Interface Description Character String

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

By default, a VLAN description character string is `No description!`. VLAN interface description character string of VLAN interface is the interface name, for example, `vlan-interface1 Interface`.

Specifying/Removing the VLAN Interface

Use the following command to specify/remove the VLAN interface. To implement the network layer function on a VLAN interface, the VLAN interface must be configured with an IP address and a subnet mask.

Perform the following configurations in System View.

Table 54 Specifying/Removing the VLAN Interface

Operation	Command
Create a new VLAN interface and enter VLAN Interface View	interface <i>vlan-interface</i> <i>vlan_id</i>

Table 54 Specifying/Removing the VLAN Interface

Operation	Command
Remove the specified VLAN interface	undo interface vlan-interface <i>vlan_id</i>

Create a VLAN first before creating an interface for it.

For this configuration task, *vlan_id* takes the VLAN ID.

Shutting Down/Enabling the VLAN Interface

Use the following command to shut down/enable a VLAN interface.

Perform the following configuration in VLAN Interface View.

Table 55 Shutting Down/Enabling the VLAN Interface

Operation	Command
Shut down the VLAN interface	shutdown
Enabling the VLAN interface	undo shutdown

The operation of shutting down or enabling the VLAN interface has no effect on the UP/DOWN status of the Ethernet ports on the local VLAN.

By default, when all the Ethernet ports belonging to a VLAN are in DOWN status, this VLAN interface is also DOWN, that is, this VLAN interface is shut down. When there is one or more Ethernet ports in UP status, this VLAN interface is also UP, that is, this VLAN interface is enabled.

Displaying and Debugging VLAN

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

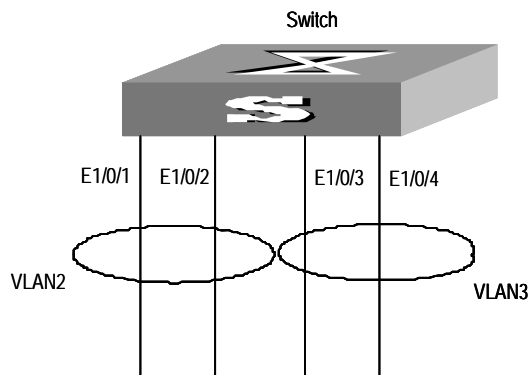
Table 56 Displaying and Debugging a VLAN

Operation	Command
Display information about the VLAN interface	display interface vlan-interface [<i>vlan_id</i>]
Display information about the VLAN	display vlan [<i>vlan_id</i> all static dynamic]

VLAN Configuration Example One

Networking Requirements

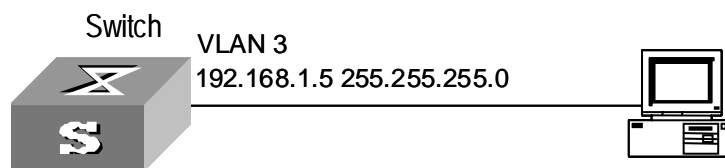
Create VLAN2 and VLAN3. Add Ethernet1/0/1 and Ethernet1/0/2 to VLAN2 and add Ethernet1/0/3 and Ethernet1/0/4 to VLAN3.

Networking Diagram**Figure 14** VLAN Configuration Example 1**Configuration Procedure**

- 1 Create VLAN 2 and enter its view.
[4500]vlan 2
- 2 Add Ethernet1/0/1 and Ethernet1/0/2 to VLAN2.
[4500-vlan2]port ethernet1/0/1 to ethernet1/0/2
- 3 Create VLAN 3 and enter its view.
[4500-vlan2]vlan 3
- 4 Add Ethernet1/0/3 and Ethernet1/0/4 to VLAN3.
[4500-vlan3]port ethernet1/0/3 to ethernet1/0/4

VLAN Configuration Example Two**Networking Requirements**

Configure an IP address on a VLAN interface.

Networking Diagram**Figure 15** VLAN Configuration Example 2**Configuration Procedure**

- 1 If the VLAN does not currently exist, then create it. This example uses VLAN ID 3.
[4500]vlan 3
[4500-vlan3]quit
- 2 Enter the VLAN interface view:
[4500]interface vlan-interface 3
- 3 Provide the IP address and subnet mask:
[4500-vlan-interface3]ip address 192.168.1.5 255.255.255
[4500-vlan-interface3]quit

Voice VLAN Configuration

Introduction to Voice VLAN

Voice VLAN is specially designed for users' voice flow, and it distributes different port precedence in different cases.

The system uses the source MAC of the traffic traveling through the port to identify the IP Phone data flow. You can either preset an OUI address or adopt the default OUI address as the standard. Here the OUI address refers to that of a vendor.

Voice VLAN can be configured either manually or automatically. In auto mode, the system learns the source MAC address and automatically adds the ports to a Voice VLAN using the untagged packets sent out when IP Phone is powered on; in manual mode, however, you need to add ports to a Voice VLAN manually. Both of the modes forward the tagged packets sent by IP Phone without learning the address.

Since there are multiple types of IP Phones, you must ensure that the mode on a port matches the IP Phone. See [Table 57](#):

Table 57 Correspondence Between Port Mode and IP Phone

	Type of IP Phone	Port Mode
Auto mode	Tagged IP Phone	Access: Not supported
		Access, Trunk, and Hybrid: Not supported, because the default VLAN of the connected port must be the Voice VLAN, and the connected port belongs to the Voice VLAN, that is, user add the port to the Voice VLAN manually.
Manual Mode	Tagged IP Phone	Access: Not supported
		Trunk: Supported, but the default VLAN of the connected port must exist and cannot be the voice VLAN. The default VLAN is allowed to pass the connected port

Voice VLAN Configuration

The configuration of Voice VLAN is described in the following sections:

- [Enabling/Disabling Voice VLAN Features](#)
- [Enabling/Disabling Voice VLAN Features on a Port](#)

- [Setting/Removing the OUI Address Learned by Voice VLAN](#)
- [Enabling/Disabling Voice VLAN Security Mode](#)
- [Enabling/Disabling Voice VLAN Auto Mode](#)
- [Setting the Aging Time of Voice VLAN](#)

If you change the status of Voice VLAN security mode, you must first enable Voice VLAN features globally.

Enabling/Disabling Voice VLAN Features

Enable/disable the Voice VLAN in System View.

Table 58 Configuring Voice VLAN Features

Operation	Command
Enable Voice VLAN features	voice vlan <i>vlan_id</i> enable
Disable Voice VLAN features	undo voice vlan enable

The VLAN must already exist before you can enable Voice VLAN features. You cannot delete a specified VLAN that has enabled Voice VLAN features and only one VLAN can enable Voice VLAN at one time.

Enabling/Disabling Voice VLAN Features on a Port

Perform the following configuration in Ethernet Port View.

Table 59 Configuring Voice VLAN Features on a Port

Operation	Command
Enable the Voice VLAN features on a port	voice vlan enable
Disable the Voice VLAN features on a port	undo voice vlan enable

Only when the Voice VLAN features in System View and Port View are all enabled can the Voice VLAN function on the port run normally.

Setting/Removing the OUI Address Learned by Voice VLAN

Configure OUI addresses which can be learned by Voice VLAN using the following command; otherwise the system uses the default OUI addresses as the standard of IP Phone traffic.

The OUI address system can learn 16 MAC addresses at most. Adding the OUI addresses, you need only input the first three-byte values of the MAC address.

Perform the following configuration in System View.

Table 60 Configuring the OUI address Learned by Voice VLAN

Operation	command
Set the OUI address learned by Voice VLAN	voice vlan mac_address <i>oui</i> mask <i>oui_mask</i> [<i>description string</i>]
Remove the OUI address learned by Voice VLAN	undo voice vlan mac_address <i>oui</i>

There are four default OUI addresses after the system starts.

Table 61 Default OUI Addresses

No.	OUI	Description
1	00:E0:BB	3Com phone
2	00:03:6B	Cisco phone
3	00:E0:75	Polycom phone
4	00:D0:1E	Pingtel phone

Enabling/Disabling Voice VLAN Security Mode

In security mode, the system can filter out the traffic whose source MAC is not OUI within the Voice VLAN, while the other VLANs are not influenced. If security mode is disabled, the system cannot filter anything.

Perform the following configuration in System View.

Table 62 Configuring the Voice VLAN Security Mode

Operation	Command
Enable Voice VLAN security mode	voice vlan security enable
Disable Voice VLAN security mode	undo voice vlan security enable

By default, the Voice VLAN security mode is enabled.

Enabling/Disabling Voice VLAN Auto Mode

In auto mode, if you enable Voice VLAN features on a port and there is IP Phone traffic through the port, the system automatically adds the port to the Voice VLAN. But in manual mode, you have to perform the above operation manually.

Perform the following configuration in System View.

Table 63 Configuring Voice VLAN Auto Mode

Operation	Command
Enable Voice VLAN auto mode	voice vlan mode auto
Disable Voice VLAN auto mode (that is, to enable manual mode)	undo voice vlan mode auto

By default, Voice VLAN auto mode is enabled.

Setting the Aging Time of Voice VLAN

In auto mode, using the follow command, you can set the aging time of Voice VLAN. After the OUI address, the MAC address of IP Phone, is aged on the port, this port enters the aging phase of Voice VLAN. If OUI address is not learned by a port within the aging time, the port is automatically deleted from Voice VLAN. This command does not operate in manual mode.

Perform the following configuration in System View.

Table 64 Configuring the Aging Time of Voice VLAN

Operation	command
Set the aging time of Voice VLAN	voice vlan aging <i>minutes</i>
Restore the default aging time	undo voice vlan aging

The default aging time is 1440 minutes.

Displaying and Debugging of Voice VLAN

After completing the above configuration, enter the **display** command in any view to view the configuration and running state of Voice VLAN.

Table 65 Displaying Voice VLAN

Operation	Command
Display the status of Voice VLAN	display voice vlan status
Display the OUI address supported by the current system	display voice vlan oui

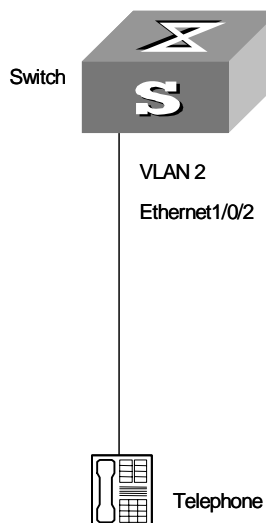
Voice VLAN Configuration Example

Networking Requirements

Create VLAN 2 as the Voice VLAN in manual mode and enable its security mode. It is required to set the aging time to 100 minutes, the OUI address to 0011-2200-0000, and configure the port Ethernet1/0/2 as the IP Phone access port. The type of IP Phone is untagged.

Network Diagram

Figure 16 Voice VLAN Configuration



Configuration Steps

```

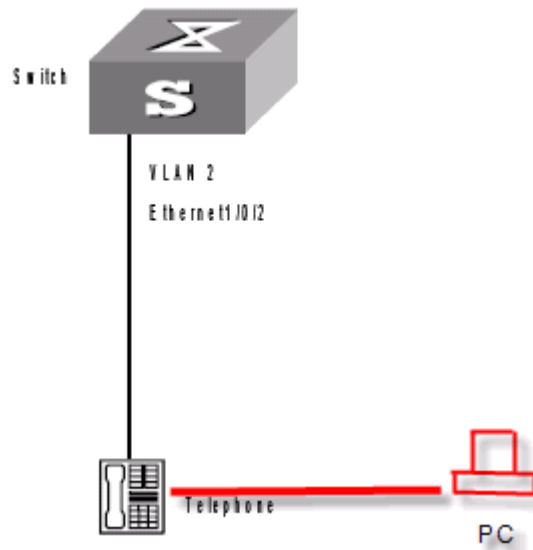
[4500]vlan 2
[4500-vlan2]port ethernet1/0/2
[4500-vlan2]interface ethernet1/0/2
[4500-Ethernet1/0/2]voice vlan enable
  
```

```
[4500 -Ethernet1/0/2]quit
[4500]undo voice vlan mode auto
[4500]voice vlan mac_address 0011-2200-0000 mask ffff-ff00-0000
description private
[4500]voice vlan 2 enable
[4500]voice vlan aging 100
```

Configuring Voice VLAN with a PC Downstream from Phone

A common configuration for voice enabled networks is to place a PC downstream from a VoIP phone. In this configuration, the phone is usually with tagged traffic residing on a Voice VLAN, and the PC is untagged on the default VLAN for the switch port.

Figure 17 Voice VLAN/PC Configuration

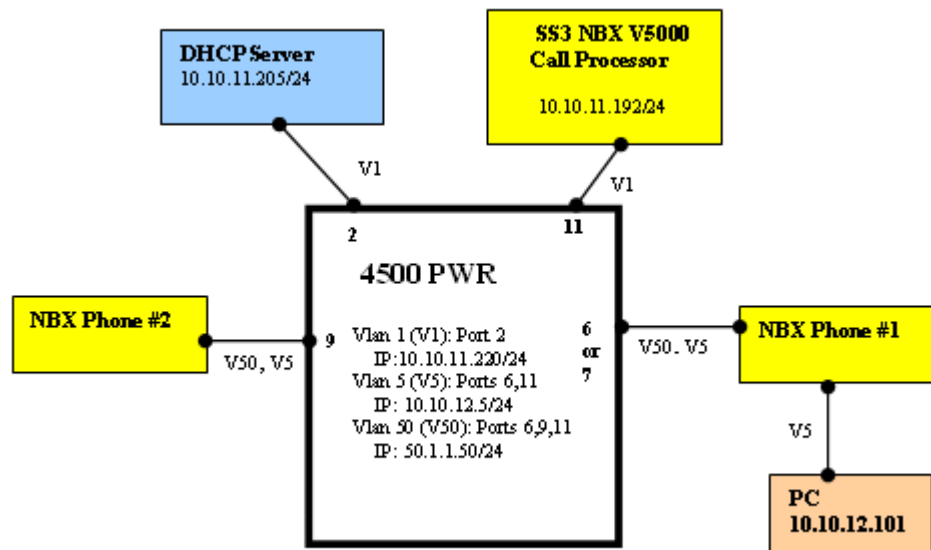


Key Details for Proper Setup

- The Voice VLAN must be set and enabled, both globally for the switch and at the system view level.
- Each port where a VoIP phone may be connected must have Voice VLAN enabled locally
- Each port where Voice VLAN is enabled must be configured as trunk or hybrid, not access type
- The default VLAN PVID for all ports is 1. This is where the PC data traffic will go by default. This can be changed if necessary.
- For the phone to be automatically configured with the VLAN for voice traffic, there must be a DHCP server that is capable of supporting Option 184 available for both the phone and the PC. This can either be via two DHCP servers, one on the Voice VLAN and one on the data VLAN, or by enabling DHCP Relay across both VLANs.
- If no DHCP server is used, then the phones must be manually configured to use the voice VLAN

- Be sure that the OUI of the phone is included in the OUI table. This will certainly be the case by default for 3Com NBX phones but should be checked for non-3Com phones
- If a PWR unit is being used to power the VoIP phone, you must enable PoE on the required ports
- If Cisco phones are used that are not IEEE 802.3af PoE compliant, but they support pre-standard PoE signaling, you may need to enable the legacy PoE feature
- Ensure phones are not pre-configured with a static IP address
- If used in a 3Com NBX network, be sure NBX Call processor is set to "Standard IP." Likewise, ensure the NBX Call Processor default Gateway is set to the VLAN interface IP address. Note that any IP related configuration changes to the NBX Call processor will require a reboot to take affect.

Figure 18 VoIP Sample Configuration with 3Com NBX

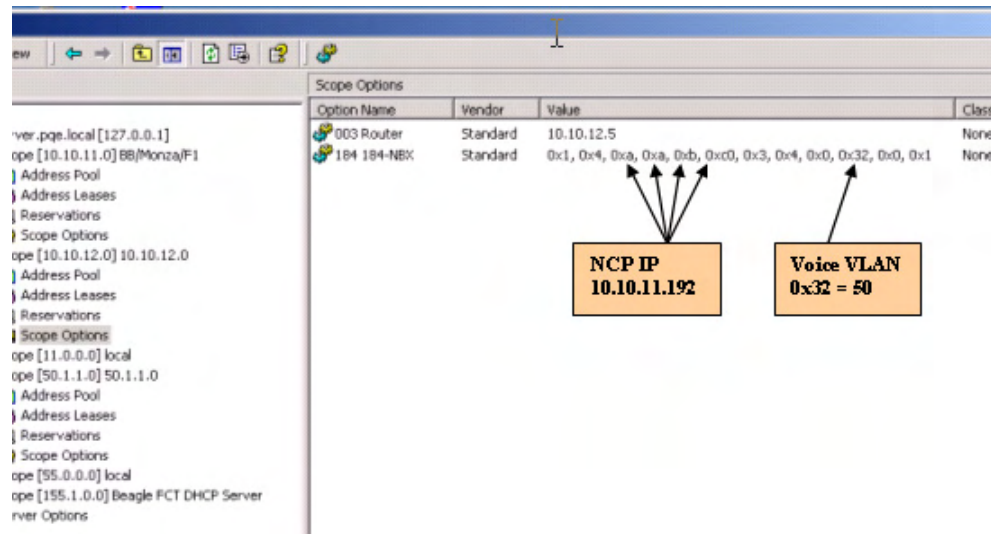


Step By Step Description

- 1 The DHCP Server (IP address is 10.10.11.205/24) connected to Port 2 of the switch (Switch 4500-PWR) has three scopes:
 - 10.10.11.0 (Address pool:10.10.11.211-250) for Data Vlan 1
 - 10.10.12.0 (Address pool: 10.10.12.100-130) for Data Vlan 5
 - 50.1.1.0 for Voice Vlan 50.

This server needs to have Option 184 configured. [Figure 19](#) displays the DHCP scopes.

Figure 19 DHCP Scopes



- 2 Connect the NBX call processor (IP address is 10.10.11.192/24), 3Com NBX phones (2102PE) 1 and 2 to Port 11, 6 or 7, and 9 on the Switch, respectively. Attach a PC (TPC4) to Phone 1.
- 3 Port 6 is a hybrid port while Port 7 is a trunk port. In order to attach Layer 3 phones to DUT, enable the routing capability.
- 4 After implementing the setup described above, data vlan 5 and Voice vlan 50 are established. The phones and attached PC can obtain their IP address from the DHCP server. Phone #1 can call Phone #2 and the PC can ping all networks (10.10.11.0, 10.10.12.0 and 50.1.1.0).

Voice VLAN in Auto Mode

This section provides a detailed listing of a Switch configuration file. The lines in red are important for voice vlan configuration.

```
<4500>display current-configuration
#
 private-group-id mode standard
#
 local-server nas-ip 127.0.0.1 key 3com
#
 domain default enable system
#
 dhcp-server 1 ip 10.10.11.205 <----- Define the IP address of DHCP server
#
 igmp-snooping enable
#
 undo password-control aging enable
 undo password-control length enable
 password-control login-attempt 3 exceed lock-time 120
#
 radius scheme system
#
 domain system
#
 local-user admin
 service-type ssh telnet terminal
 level 3
 local-user manager
 service-type ssh telnet terminal
```

```

level 2
local-user monitor
service-type ssh telnet terminal
level 1
#
acl number 4999
rule 0 deny dest 0000-0000-0000 ffff-ffff-ffff
#
vlan 1
igmp-snooping enable
#
vlan 5      <----- Create Data Vlan 5
#
vlan 50     <----- Create voice Vlan 50
#
interface Vlan-interface1
ip address dhcp-alloc
rip version 2 multicast
#
interface Vlan-interface5
ip address 10.10.12.5 255.255.255.0
dhcp-server 1<----- Enable dhcp-relay by pointing to DHCP Server 1
rip version 2 multicast
#
interface Vlan-interface50
ip address 50.1.1.50 255.255.255.0
dhcp-server 1<----- Enable dhcp-relay by pointing to DHCP Server 1
rip version 2 multicast
#
interface Aux1/0/0
#
interface Ethernet1/0/1
poe enable
stp edged-port enable
broadcast-suppression PPS 3000
priority trust
packet-filter inbound link-group 4999 rule 0
#
interface Ethernet1/0/2
poe enable
stp edged-port enable
broadcast-suppression PPS 3000
priority trust
packet-filter inbound link-group 4999 rule 0
#
interface Ethernet1/0/3
poe enable
stp edged-port enable
broadcast-suppression PPS 3000
priority trust
packet-filter inbound link-group 4999 rule 0
#
interface Ethernet1/0/4
poe enable
stp edged-port enable
broadcast-suppression PPS 3000
priority trust
packet-filter inbound link-group 4999 rule 0
#
interface Ethernet1/0/5
poe enable
stp edged-port enable
broadcast-suppression PPS 3000
priority trust
packet-filter inbound link-group 4999 rule 0
#

```



```

interface Ethernet1/0/6
 poe enable
 stp edged-port enable
 port link-type hybrid<----- Setup for Hybrid ports
 port hybrid vlan 5 untagged
 undo port hybrid vlan 1
 port hybrid pvid vlan 5
 broadcast-suppression PPS 3000
 priority trust
 voice vlan enable
 packet-filter inbound link-group 4999 rule 0
#
interface Ethernet1/0/7
 poe enable
 stp edged-port enable
 port link-type trunk<----- Setup for Trunk ports
 undo port trunk permit vlan 1
 port trunk permit vlan 5
 port trunk pvid vlan 5
 broadcast-suppression PPS 3000
 priority trust
 voice vlan enable
 packet-filter inbound link-group 4999 rule 0
#
interface Ethernet1/0/8
 poe enable
 stp edged-port enable
 broadcast-suppression PPS 3000
 priority trust
 packet-filter inbound link-group 4999 rule 0
#
interface Ethernet1/0/9
 poe enable
 stp edged-port enable
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 5
 port trunk pvid vlan 5
 broadcast-suppression PPS 3000
 priority trust
 voice vlan enable
 packet-filter inbound link-group 4999 rule 0
#
interface Ethernet1/0/10
 poe enable
 stp edged-port enable
 broadcast-suppression PPS 3000
 priority trust
 packet-filter inbound link-group 4999 rule 0
#
interface Ethernet1/0/11
 poe enable
 stp edged-port enable
 broadcast-suppression PPS 3000
 priority trust
 packet-filter inbound link-group 4999 rule 0
#
interface Ethernet1/0/12
 poe enable
 stp edged-port enable
 broadcast-suppression PPS 3000
 priority trust
 packet-filter inbound link-group 4999 rule 0
#
interface Ethernet1/0/13
 poe enable

```

```
    stp edged-port enable
    broadcast-suppression PPS 3000
    priority trust
    packet-filter inbound link-group 4999 rule 0
#
interface Ethernet1/0/14
    poe enable
    stp edged-port enable
    broadcast-suppression PPS 3000
    priority trust
    packet-filter inbound link-group 4999 rule 0
#
interface Ethernet1/0/15
    poe enable
    stp edged-port enable
    broadcast-suppression PPS 3000
    priority trust
    packet-filter inbound link-group 4999 rule 0
#
interface Ethernet1/0/16
    poe enable
    stp edged-port enable
    broadcast-suppression PPS 3000
    priority trust
    packet-filter inbound link-group 4999 rule 0
#
interface Ethernet1/0/17
    poe enable
    stp edged-port enable
    broadcast-suppression PPS 3000
    priority trust
    packet-filter inbound link-group 4999 rule 0
#
interface Ethernet1/0/18
    poe enable
    stp edged-port enable
    broadcast-suppression PPS 3000
    priority trust
    packet-filter inbound link-group 4999 rule 0
#
interface Ethernet1/0/19
    poe enable
    stp edged-port enable
    broadcast-suppression PPS 3000
    priority trust
    packet-filter inbound link-group 4999 rule 0
#
interface Ethernet1/0/20
    poe enable
    stp edged-port enable
    broadcast-suppression PPS 3000
    priority trust
    packet-filter inbound link-group 4999 rule 0
#
interface Ethernet1/0/21
    poe enable
    stp edged-port enable
    broadcast-suppression PPS 3000
    priority trust
    packet-filter inbound link-group 4999 rule 0
#
interface Ethernet1/0/22
    poe enable
    stp edged-port enable
    broadcast-suppression PPS 3000
    priority trust
```

```

packet-filter inbound link-group 4999 rule 0
#
interface Ethernet1/0/23
  poe enable
  stp edged-port enable
  broadcast-suppression PPS 3000
  priority trust
  packet-filter inbound link-group 4999 rule 0
#
interface Ethernet1/0/24
  poe enable
  stp edged-port enable
  broadcast-suppression PPS 3000
  priority trust
  packet-filter inbound link-group 4999 rule 0
#
interface GigabitEthernet1/0/25
#
interface GigabitEthernet1/0/26
#
interface GigabitEthernet1/0/27
  shutdown
#
interface GigabitEthernet1/0/28
  shutdown
#
sysname 4500
undo xrn-fabric authentication-mode
#
interface NULL0
#
rip      <----- Dynamic Routing setup (only required if deploying L3 network)
undo summary
network 10.0.0.0
network 50.0.0.0
#
voice vlan 50 enable<----- Set Vlan 50 as the Voice Vlan
#
snmp-agent
snmp-agent local-engineid 8000002B0012A99298C06877
snmp-agent community read public
snmp-agent community write private
snmp-agent sys-info version all
#
user-interface aux 0 7
  authentication-mode scheme
user-interface vty 0 4
  authentication-mode scheme
#
return

```

Voice VLAN in Manual Mode

This section provides a configuring Voice VLAN in manual mode. The lines in red are important for voice vlan configuration.

```

Undo voice vlan mode auto
#
interface Ethernet1/0/6
  poe enable
  stp edged-port enable
  port link-type hybrid<----- Setup for Hybrid ports
  port hybrid vlan 50 tagged
  port hybrid vlan 5 untagged

```

```

undo port hybrid vlan 1
port hybrid pvid vlan 5
broadcast-suppression PPS 3000
priority trust
voice vlan enable
packet-filter inbound link-group 4999 rule 0
#
interface Ethernet1/0/7
po e enable
stp edged-port enable
port link-type trunk<----- Setup for Trunk ports
undo port trunk permit vlan 1
port trunk permit vlan 5 50
port trunk pvid vlan 5
broadcast-suppression PPS 3000
priority trust
voice vlan enable
packet-filter inbound link-group 4999 rule 0
#
interface Ethernet1/0/8
po e enable
stp edged-port enable
broadcast-suppression PPS 3000
priority trust
packet-filter inbound link-group 4999 rule 0
#
interface Ethernet1/0/9
po e enable
stp edged-port enable
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 5 50
port trunk pvid vlan 5
broadcast-suppression PPS 3000
priority trust
voice vlan enable
packet-filter inbound link-group 4999 rule 0
#
Undo voice vlan mode auto
#

```

4

POWER OVER ETHERNET CONFIGURATION

This chapter covers the following topics:

- [PoE Overview](#)
- [PoE Configuration](#)

PoE Overview

The Switch 4500 26 Port PWR and Switch 4500 50 Port PWR support Power over Ethernet (PoE). This feature uses twisted pairs to provide -44 through -62 VDC power to remote powered devices (PDs), such as IP Phones, WLAN APs, Network Cameras, and so on. The PWR switches provide the following capabilities:

- Power sourcing equipment (PSE), the PWR switches support the IEEE802.3af standard and can also supply power to part of the PDs non-compliant with the standard.
- The PWR switches can deliver data and current in the mean time through data wires (1, 3, 2, and 6) of the category-3/5 twisted pairs.
- Through its 26/50 Ethernet electrical ports, the PWR switches can supply power to up to 26/50 remote Ethernet switches with the maximum distance of 100 m (328 feet).
- Each Ethernet port can supply at most 15400 mW of power to a PD.
- When AC power input is adopted for the switch: the maximum total power that can be provided by the PWR switches is 300 W. These switches can determine whether to supply power to the next remote PD it detected depending on the total power.
- When DC power input is adopted for the switch: the PWR switches are capable of supplying full power to all of the 26/60 ports.
- The PSE processing software on the PWR switches can be upgraded online.
- The PWR switches provide statistics about power supplying on each port and the whole equipment, which you can query through the **display** command.
- The PWR switches provide two modes (**auto** and **manual**) to manage the power feeding to ports in the case of PSE power overload.
- The PWR switches provide overheat protection mechanism. This stops the power feeding to any PD connected with a port when the ambient temperature reaches 65 °C; and restores the power feeding to all the PDs connected with the ports when the temperature drops below 60 °C.

- When using the PWR switches to supply power to remote PDs, the PDs need not have any external power supply.
- If a remote PD has an external power supply, the PWR switches and the external power supply will be redundant with each other for the PD.
- Only the electrical ports of the PWR switches support the PoE feature.

PoE Configuration

The PWR switches can automatically detect any device that needs remote power supply through the port to which it connects and feeds power to this device.

You can use the command line to enable/disable the PoE feature of a port, set the power supply priority, maximum output power, and compatibility detect function of a port.

PoE configuration tasks are listed in the following table.

Table 66 PoE Configuration

Device	Configuration	Default	Description
Switch 4500 26 Port PWR / Switch 4500 50 Port PWR	Enabling/Disabling PoE on a port	Disable	
	Setting the maximum output power on a port	15400 mW	
	Setting the PoE management mode on a port used in the case of power overloading	Auto	
	Setting the port priority	Low	
	Setting the PoE mode on a port	Signal line	Switch 4500 supports signal mode only
	Setting the compatibility detect function on a port	Close	
PD	Upgrading the PSE processing software online		Online downloading of upgrade file is needed
	Correctly connecting a PD with an electrical port on the PWR switches		

Enabling/Disabling the PoE Feature on a Port

You can use the following command to enable/disable the PoE feature on a port in accordance with the network requirement.

Perform the following configuration in Ethernet Port View.

Table 67 Enabling/disabling PoE feature on a port

Operation	Command
Enable the PoE feature on a port	poe enable
Disable the PoE feature on a port	undo poe enable

By default, the PoE feature of each port is enabled.

Setting the Maximum Power Output on a Port

The maximum power that can be supplied by an Ethernet port of the Switch 4500 26-Port PWR and Switch 4500 50-Port PWR to its PD is 15400 mW. In practice, you can set the maximum power on a port depending on the actual power of the PD, with a range from 1000 to 15400 mW and in the increment of 100 mW.

Perform the following configuration in Ethernet Port View to set the maximum power supplied by a port..

Table 68 Setting the Maximum power on a port

Operation	Command
Set the maximum power supplied by a port	<code>poe max-power max-power</code>
Restore the default maximum power on the port	<code>undo poe max-power</code>

By default, the maximum power on a port is 15400 mW.

Setting Power Supply Management Mode in Overload and Port Priority

The power supply management mode and the port priority settings will work together to control the power feeding of the switch when the switch is reaching its full power load in supplying power.

When AC power input is adopted for the switch, The maximum main total power that can be supplied by the PWR switches is 300 W. By default, when the Switch reaches its full load in supplying power, it will manage the power supply to its ports in **auto** mode.

- **auto** mode — when the switch is reaching 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 is reaching 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 low priority and turn to supply power to this new PD. IF more than one port has the same lowest priority, the Switch will power down the PD connected to the port with larger logical port number.

- **manual** mode — when the switch is reaching its full load in supplying power, it will neither take the priority into account nor make change to its original power supply status. For example:

Port A has the priority critical. When the Switch is reaching 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.

Setting the Power Supply Management Mode on the Switch

Perform the following configuration in System View.

Table 69 Setting the Power Supply Management Mode on the Switch

Operation	Command
Set the power supply management mode on the Switch to auto	poe power-management auto
Set the power supply management mode on the Switch to manual	poe power-management manual
Restore the default power supply management mode on the Switch	undo poe power-management

By default, the power supply management mode on the Switch is **auto**.

Setting the Port Priority

Set the priority of the current port in Ethernet Port View.

Table 70 Setting the Port Priority

Operation	Command
Set the port priority	poe priority { critical high low }
Restore the port priority	undo poe priority

By default, the port priority is low.

Setting the PoE Mode on a Port

Set the PoE mode on the current port in Ethernet port view.

Table 71 Setting the PoE Mode on a Port

Operation	Command
Set the PoE mode on a port	poe mode { signal spare }
Restore the default PoE mode on the port	undo poe mode

By default, the power supply mode on port is by signal lines.

Currently, the Switch 4500 does not support the **spare** mode. If a PD only supports the **spare** mode, a conversion will be needed.

Enabling/Disabling PD Compatibility Detect

The PD compatibility detect function allows the switch to detect PDs noncompliant with the 802.3af standard and then supply power to them. You can use the following commands to enable/disable the PD compatibility detect function.

Perform the following configuration in System View.

Table 72 Enabling/Disabling the PD Compatibility Detect

Operation	Command
Enable the PD compatibility detect	poe legacy enable
Restore the default PD compatibility default setting	undo poe legacy enable

By default, the PD compatibility detect function is disabled.

Upgrading the PSE Processing Software Online

The online upgrading of PSE processing software can update the processing software or repair the software if it is damaged. After upgrading files are downloaded, you can use the following command to perform online upgrading on the PSE processing software.

Perform the following configuration in system view.

Table 73 Upgrading PSE Processing Software Online

Operation	Command
Update PSE Processing Software	<code>poe update full</code>
Refresh PSE Processing Software	<code>poe update refresh</code>

Upgrading in Refresh Mode

Normally, the online upgrading of PSE processing software should be done in **refresh** mode.

Upgrading in Full Mode

- When the upgrading procedure in **refresh** mode is interrupted for some unexpected reason (for example, power-off) or some error occur, you can use the **full** mode to re-upgrade.
- When the PSE processing software is damaged (that is, all the PoE commands cannot be successfully executed), you can use the **full** mode to upgrade and restore the software.

Displaying PoE Information

After the above configuration, execute the **display** command in any view to see the operation of the PoE feature on the switch and verify the effect of the configuration.

Table 74 PoE Information Display

Operation	Command
Display the PoE status of a specific port or all ports on the Switch	<code>display poe interface [interface-name interface-type interface-num]</code>
Display the PoE power information of a specific port or all ports on the Switch	<code>display poe interface power [interface-name interface-type interface-num]</code>
Display the PSE parameters	<code>display poe powersupply</code>

For more information on the parameters, refer to the Command Reference Guide.

Configuration Example

Networking Requirements

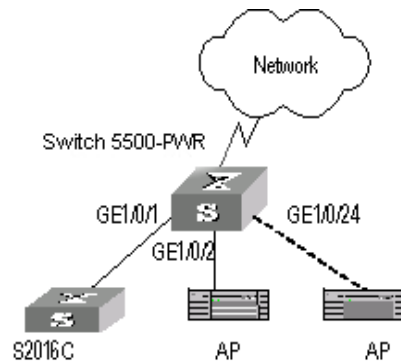
The Ethernet1/0/1 and Ethernet1/0/2 ports of the Switch 4500 PWR are connected with a PD and an access point (AP) respectively.

The Ethernet1/0/24 port is intended to be connected with an AP. The PSE processing software of the Switch 4500 PWR should be first upgraded online. The remotely accessed PDs should be powered by the Switch 4500 PWR. The power consumption of the AP that has already been connected with Ethernet1/0/2 is 2500 mW, and the power consumption of the PSU is 12000 mW. This is required

to guarantee the power feeding to the PD that will be connected to the Ethernet1/0/24 even when the Switch 4500 PWR is in full load.

Network Diagram

Figure 20 PoE Remote Power Supply



Configuration Procedure

Update the PSE processing software online.

```
[4500]poe update refresh 0290_021.s19
```

Enable the PoE feature on the Ethernet1/0/1, Ethernet1/0/2, and Ethernet1/0/24 ports (the feature is enabled by default, so this step can be ignored).

```
[4500-Ethernet1/0/1]poe enable
[4500-Ethernet1/0/2]poe enable
[4500-Ethernet1/0/24]poe enable
```

Set the maximum power output of Ethernet1/0/1 and Ethernet1/0/2 to 12000 and 3000 mW respectively.

```
[4500-Ethernet1/0/1]poe max-power 12000
[4500-Ethernet1/0/2]poe max-power 3000
```

Set the priority of Ethernet1/0/24 to **critical** to guarantee the power feeding to the AP to which this port connects.

```
[4500-Ethernet1/0/24]poe priority critical
```

Set the power supply management mode on the switch to **auto** (it is the default mode, so this step can be ignored).

```
[4500]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.

```
[4500]poe legacy enable
```

5

NETWORK PROTOCOL OPERATION

This chapter covers the following topics:

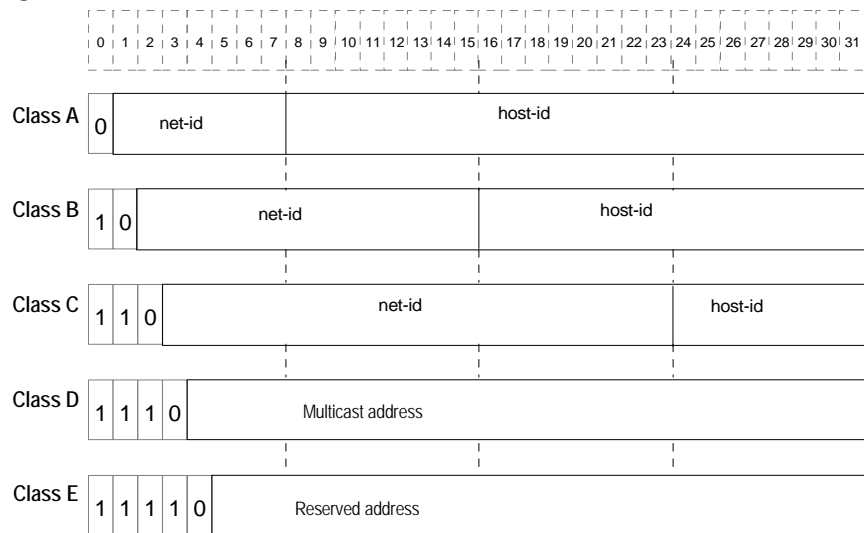
- [IP Address Configuration](#)
- [ARP Configuration](#)
- [DHCP Configuration](#)
- [Access Management Configuration](#)
- [UDP Helper Configuration](#)
- [IP Performance Configuration](#)

IP Address Configuration

IP Address Overview IP Address Classification and Indications

An IP address is a 32-bit address allocated to the devices which access the Internet. It consists of two fields: net-id field and host-id field. There are five types of IP address. See [Figure 21](#).

Figure 21 Five Classes of IP Address



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

The IP address is in dotted decimal format. Each IP address contains 4 integers in dotted decimal notation. Each integer corresponds to one byte, for example, 10.110.50.101.

When using IP addresses, note that some of them are reserved for special uses, and are seldom used. The IP addresses you can use are listed in [Table 75](#).

Table 75 IP Address Classes and Ranges

Network class	Address range	IP network range	Note
A	0.0.0.0 to 127.255.255.255	1.0.0.0 to 126.0.0.0	<p>Host ID with all the digits being 0 indicates that the IP address is the network address, and is used for network routing.</p> <p>Host ID with all the digits being 1 indicates the broadcast address, that is, broadcast to all hosts on the network.</p> <p>IP address 0.0.0.0 is used for the host that is not put into use after starting up.</p> <p>The IP address with network number as 0 indicates the current network and its network can be cited by the router without knowing its network number.</p> <p>Network ID with the format of 127.X.Y.Z is reserved for self-loop test and the packets sent to this address will not be output to the line. The packets are processed internally and regarded as input packets.</p>
B	128.0.0.0 to 191.255.255.255	128.0.0.0 to 191.254.0.0	<p>Host ID with all the digits being 0 indicates that the IP address is the network address, and is used for network routing.</p> <p>Host ID with all the digits being 1 indicates the broadcast address, that is, broadcast to all hosts on the network.</p>
C	192.0.0.0 to 223.255.255.255	192.0.0.0 to 223.255.254.0	<p>Host ID with all the digits being 0 indicates that the IP address is the network address, and is used for network routing.</p> <p>Host ID with all the digits being 1 indicates the broadcast address, that is, broadcast to all hosts on the network.</p>
D	224.0.0.0 to 239.255.255.255	None	Addresses of class D are multicast addresses.
E	240.0.0.0 to 255.255.255.254	None	The addresses are reserved for future use.
Other addresses	255.255.255.255	255.255.255.255	255.255.255.255 is used as LAN broadcast address.

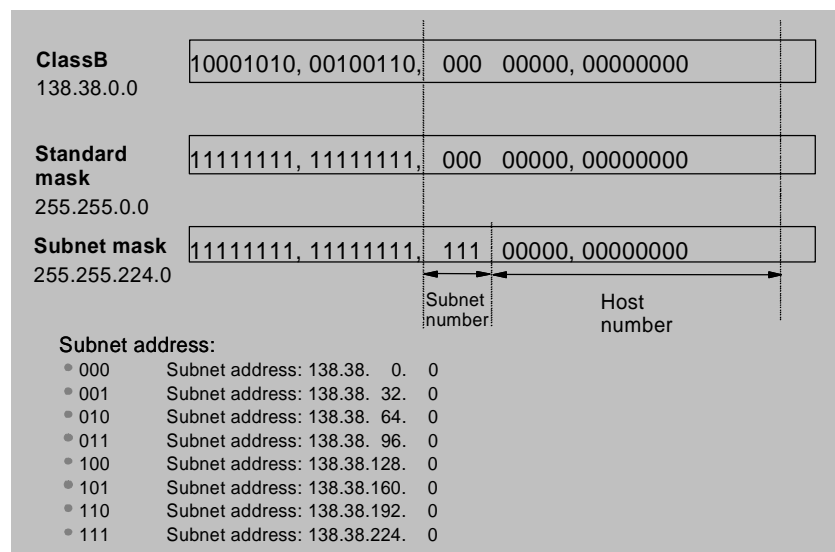
Subnet and Mask

With the rapid development of the Internet, available IP addresses are depleting very fast. The traditional IP address allocation method wastes IP addresses. In order to make full use of the available IP addresses, the mask and subnet are used.

A mask is a 32-bit number corresponding to an IP address. The number consists of 1s and 0s. Principally, these 1s and 0s can be combined randomly. However, the first consecutive bits are set to 1s when designing the mask. The mask divides the IP address into two parts: subnet address and host address. The bits 1s in the address and the mask indicate the subnet address and the other bits indicate the host address. If there is no subnet division, then its subnet mask is the default value and the length of "1" indicates the net-id length. Therefore, for IP addresses of classes A, B and C, the default values of corresponding subnet mask are 255.0.0.0, 255.255.0.0 and 255.255.255.0 respectively.

The mask can be used to divide a Class A network containing more than 16,000,000 hosts or a Class B network containing more than 60,000 hosts into multiple small networks. Each small network is called a subnet. For example, for the Class B network address 138.38.0.0, the mask 255.255.224.0 can be used to divide the network into 8 subnets: 138.38.0.0, 138.38.32.0, 138.38.64.0, 138.38.96.0, 138.38.128.0, 138.38.160.0, 138.38.192.0 and 138.38.224.0 (Refer to the [Figure 22](#)). Each subnet can contain more than 8000 hosts.

Figure 22 Subnet Division of IP Address



Configuring IP Address Configure an IP address for a VLAN interface in one of three ways:

- Using the IP address configuration command
- Allocated by BOOTP server
- Allocated by DHCP server

These three methods are mutually exclusive and a new configuration will replace the current IP address. For example, if you apply for an IP address using the `ip address bootp-alloc` command, the address allocated by BOOTP shall replace the currently-configured IP address.

This section introduces how to configure an IP address with the IP address configuration command. The other two methods are described in subsequent chapters.

The IP address configuration is described in the following sections:

- [Configuring the Hostname and Host IP Address](#)
- [Configuring the IP Address of the VLAN Interface](#)

Configuring the Hostname and Host IP Address

The host name is corresponded to the IP address by using this command. When you use applications like Telnet, you can use the host name without having to memorize the IP address since the system translates it to the IP address automatically.

Perform the following configuration in System View.

Table 76 Configuring the Host Name and the Corresponding IP Address

Operation	Command
Configure the hostname and the corresponding IP address	<code>ip host hostname ip_address</code>
Delete the hostname and the corresponding IP address	<code>undo ip host hostname [ip_address]</code>

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



For further information on IP Address configuration, please refer to the Getting Started Guide that accompanies your Switch.

Configuring the IP Address of the VLAN Interface

You can configure an IP address for every VLAN interface of the Switch.

Perform the following configuration in VLAN Interface View.

Table 77 Configuring the IP Address for a VLAN Interface

Operation	Command
Configure IP address for a VLAN interface	<code>ip address ip_address { mask mask_length }</code>
Delete the IP address of a VLAN interface	<code>undo ip address ip-address { mask mask_length }</code>

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

Displaying and Debugging IP Address

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

Table 78 Displaying and Debugging IP Address

Operation	Command
Display all hosts on the network and the corresponding IP addresses	<code>display ip host</code>
Display the configurations of each interface	<code>display ip interface interface_type interface_num</code>

IP Address Configuration Example

Networking Requirements

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

Networking Diagram

Figure 23 IP Address Configuration Networking



Configuration Procedure

- 1 Enter VLAN interface 1.


```
[4500]interface vlan-interface 1
```
- 2 Configure the IP address for VLAN interface 1.


```
[4500-vlan-interface1]ip address 129.2.2.1 255.255.255.0
```

Troubleshooting IP Address Configuration

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

Troubleshooting can be performed as follows:

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

ARP Configuration

Introduction to ARP Necessity of ARP

An IP address cannot be directly used for communication between network devices because network devices can only identify MAC addresses. An IP address is an address of a host in the network layer. To send the data packets transmitted through the network layer to the destination host, the physical address of the host is required. So the IP address must be resolved into a physical address.

ARP Implementation Procedure

When two hosts on the network communicate, they must know the MAC addresses of each other. Every host will maintain the IP-MAC address translation table, which is known as ARP mapping table. A series of maps between IP addresses and MAC addresses of other hosts which were recently used to communicate with the local host are stored in the ARP mapping table. When a

dynamic ARP mapping entry is not in use for a specified period of time, the host will remove it from the ARP mapping table so as to save the memory space and shorten the interval for Switch to search ARP mapping table.

Suppose there are two hosts on the same network segment: Host A and Host B. The IP address of Host A is IP_A and the IP address of Host B is IP_B. Host A will transmit messages to Host B. Host A checks its own ARP mapping table first to make sure whether there are corresponding ARP entries of IP_B in the table. If the corresponding MAC address is detected, Host A will use the MAC address in the ARP mapping table to encapsulate the IP packet in frame and send it to Host B. If the corresponding MAC address is not detected, Host A will store the IP packet in the queue waiting for transmission, and broadcast it throughout the Ethernet. The ARP request packet contains the IP address of Host B and IP address and MAC address of Host A. Because the ARP request packet is broadcast, all hosts on the network segment can receive the request. However, only the requested host (that is, Host B) needs to process the request. Host B will first store the IP address and the MAC address of the request sender (Host A) in the ARP request packet in its own ARP mapping table. Then Host B will generate an ARP reply packet, into which it will add MAC address of Host B, and then send it to Host A. The reply packet will be directly sent to Host A in stead of being broadcast. Receiving the reply packet, Host A will extract the IP address and the corresponding MAC address of Host B and add them to its own ARP mapping table. Then Host A will send Host B all the packets standing in the queue.

Normally, dynamic ARP automatically executes and searches for the resolution from the IP address to the Ethernet MAC address without the administrator.

Configuring ARP

The ARP mapping table can be maintained dynamically or manually. Usually, the manually configured mapping from the IP addresses to the MAC addresses is known as static ARP. The user can display, add, or delete entries in the ARP mapping table through relevant manual maintenance commands.

Static ARP configuration is described in the following sections:

- [Manually Adding/Deleting Static ARP Mapping Entries](#)
- [Configuring the Dynamic ARP Aging Timer](#)
- [Configuring the Creation of ARP Entries for Multicast Packets](#)

Manually Adding/Deleting Static ARP Mapping Entries

You can configure static ARP mapping items either in System View or Ethernet Port View. In System View, you can configure global static ARP mapping entries, or configure static ARP mapping entries for the designated egress port; while in Ethernet Port View, you may set the current port as the egress port of static ARP.

Perform the following configuration in System View or Ethernet Port View.

Table 79 Manually Adding/Deleting Static ARP Mapping Entries

Operation	Command
Manually add a static ARP mapping entry (System View)	<code>arp static ip_address mac_address [vlan_id { interface_type interface_num interface_name }]</code>

Table 79 Manually Adding/Deleting Static ARP Mapping Entries

Operation	Command
Manually add a static ARP mapping entry (Ethernet Port View)	arp static <i>ip_address mac_address vlan_id</i>
Manually delete a static ARP mapping entry (System View or Ethernet Port View)	undo arp <i>ip_address</i>

By default, the ARP mapping table is empty and the address mapping is obtained through dynamic ARP.

Note that:

- Static ARP map entry will be always valid as long as the Switch works normally. But if the VLAN corresponding to the ARP mapping entry is deleted, the ARP mapping entry will be also deleted. The valid period of dynamic ARP map entries will last only 20 minutes by default.
- The parameter *vlan-id* must be the ID of a VLAN that has been created by the user, and the Ethernet port specified behind this parameter must belong to the VLAN.
- The aggregation port or port with LACP enabled cannot be set as the egress port of static ARP.

Configuring the Dynamic ARP Aging Timer

For purpose of flexible configuration, the system provides the following commands to assign dynamic ARP aging period. When the system learns a dynamic ARP entry, its aging period is based on the current value configured.

Perform the following configuration in System View.

Table 80 Configuring the Dynamic ARP Aging Timer

Operation	Command
Configure the dynamic ARP aging timer	arp timer aging <i>aging_time</i>
Restore the default dynamic ARP aging time	undo arp timer aging

By default, the aging time of the dynamic ARP aging timer is 20 minutes.

Configuring the Creation of ARP Entries for Multicast Packets

Use the following command to specify whether the Switch should create ARP table entries for multicast MAC addresses. Address resolution, for multicast packets, is not required because the IANA (Internet Assigned Numbers Authority) have reserved a block of Ethernet addresses that map on to the Class D multicast addresses.

Perform the following configuration in System View.

Table 81 Configuring the Creation of ARP Entries for Multicast Packets

Operation	Command
Configure the Switch NOT to create ARP entries	arp check enable
Configure the Switch to create ARP entries	undo arp check enable

By default, this feature is enabled.

Displaying and Debugging ARP

After the above configuration, enter the **display** command in any view to display the running of the ARP configuration, and to verify the effect of the configuration. Enter the **debugging** command in User View to debug ARP configuration. Enter the **reset** command in User View to clear ARP mapping table.

Table 82 Displaying and Debugging ARP

Operation	Command
Display the ARP mapping table	display arp [<i>ip_address</i> [dynamic static] [{ begin include exclude } <i>text</i>]]
Display the current setting of the dynamic ARP map aging timer	display arp timer aging
Reset the ARP mapping table	reset arp [dynamic static interface { <i>interface_type interface_num</i> <i>interface_name</i> }]
Enable ARP information debugging	debugging arp packet
Disable ARP information debugging	undo debugging arp packet

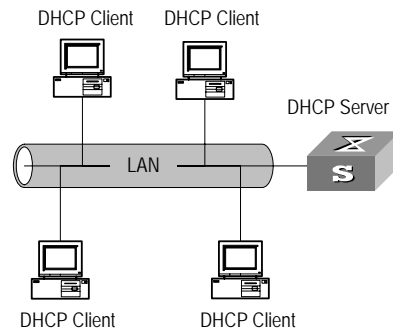
DHCP Configuration

Overview of DHCP

Dynamic Host Configuration Protocol (DHCP) offers dynamic IP address assignment. DHCP works in Client-Server mode. With this protocol, the DHCP Client can dynamically request configuration information and the DHCP server can configure the information for the Client.

The DHCP relay serves as conduit between the DHCP Client and the server located on different subnets. The DHCP packets can be relayed to the destination DHCP server (or Client) across network segments. The DHCP clients on different networks can use the same DHCP server. This is economical and convenient for centralized management.

A typical DHCP application often contains a DHCP server and several clients (desktop and laptop PCs). See [Figure 24](#)

Figure 24 Typical DHCP Application.

To obtain valid dynamic IP addresses, the DHCP client exchanges different types of information with the server at different stages. One of the following three situations may occur:

- A DHCP client logs into the network for the first time

When a DHCP client logs into the network for the first time, its communication with the DHCP server includes these four stages:

- Discovery stage, the stage when the DHCP client looks for the DHCP server. The client broadcasts the DHCP_Discover message and only the DHCP server can respond.
- Offer stage, the stage when the DHCP server allocates the IP address. After receiving the DHCP_Discover message from the client, the DHCP server chooses an IP address still available in the IP address pool for the client, and sends to the client the DHCP_Offer message containing the leased IP address and other settings.
- Select stage, the stage when the client selects the IP address. If several DHCP servers send DHCP_Offer messages to the client, the client only accepts the first received one and then broadcasts DHCP_Request messages respectively to those DHCP servers. The message contains the information of the IP address request from the selected DHCP server.
- Acknowledge stage, the stage when the DHCP server acknowledges the IP address. When receiving the DHCP_Request message from the client, the DHCP server sends the DHCP_ACK message containing the allocated IP address and other settings back to the client. Then the DHCP client binds its TCP/IP components to the NIC (network interface card).

Other DHCP servers not selected still can allocate their IP addresses to other clients later.

- A DHCP client logs into the network for a second time

When DHCP client logs into the network for a second time, its communication with the DHCP server includes these stages:

- The client broadcasts the DHCP_Request message containing the IP address obtained last time, other than the DHCP_Discover message.
- After the reception of the DHCP_Request message, the DHCP server returns the DHCP_ACK message if the requested IP address is still not allocated, to indicate the client to continue use of the IP address.

- If the requested IP address becomes unavailable (for example, having been allocated to another client), the DHCP server returns the DHCP_NAK message. After receiving the DHCP_NAK message, the client sends the DHCP_Discover message to request another new IP address.
- A DHCP client extends its IP lease period

There is a time limit for the IP addresses leased to DHCP clients. The DHCP server shall withdraw the IP addresses when their lease period expires. If the DHCP client wants to continue use of the old IP address, it has to extend the IP lease.

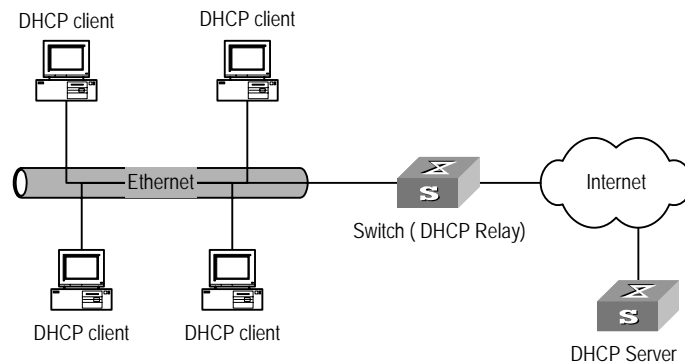
In practice, the DHCP client, by default, shall originate the DHCP_Request message to the DHCP server right in the middle of the IP lease period, to update the IP lease. If the IP address is still available, the DHCP server responds with the DHCP_ACK message, notifying the client that it has got the new IP lease.

The DHCP client implemented on the Switch supports automatic IP lease update.

DHCP Relay

The DHCP described above applies only when DHCP clients and server(s) are in the same subnet, and it does not support trans-segment networking. To achieve dynamic address configuration, you would have to configure a DHCP server for each subnet, which is not a practical solution. Introduction of DHCP relay has solved this problem: the clients in a LAN can communicate with DHCP servers in another subnet through DHCP relay, to get valid IP addresses. Then DHCP clients of multiple different networks can share a DHCP server, which saves networking cost, as well as facilitating centralized management. A typical DHCP relay application is shown in [Figure 25](#).

Figure 25 Typical DHCP Relay Application



DHCP Relay works on the following principle:

- When the DHCP client starts and initializes DHCP, it broadcasts the request message to the local network.
- If there is a DHCP server on the local network, it can begin DHCP configuration without requiring a DHCP relay function. If not, the local network device configured for DHCP relay, upon receiving the broadcast message, will forward the message to the DHCP server on the specified network.

- The DHCP server determines a correct configuration based on the information from the client and returns the configuration information back to the client through DHCP relay.

In fact, several such interactions may be needed to complete a DHCP relay configuration.

DHCP Client Configuration

DHCP client configuration is described in the following section.

Configuring a VLAN Interface to Obtain an IP Address Using DHCP

Perform the following configuration in VLAN Interface View.

Table 83 Configuring a VLAN Interface to Obtain an IP Address Using DHCP

Operation	Command
Configure VLAN interface to obtain IP address using DHCP	<code>ip address dhcp-alloc</code>
Remove the configuration	<code>undo ip address dhcp-alloc</code>

By default, the Switch attempts to obtain an IP address by DHCP on VLAN 1.

If you are attempting to stop the Switch from transmitting packets, you need to disable all features which may generate packets. By default these are:

- DHCP
- Resilient ARP
- Spanning Tree

DHCP Relay Configuration

DHCP relay configuration is described in the following sections:

- [Configuring the IP address for the DHCP server](#)
- [Configuring the DHCP Server Group for the VLAN Interfaces](#)

Configuring the IP address for the DHCP server

You can configure a master and a backup DHCP server, which are in the same DHCP server group, in the same network segment to ensure reliability.

Perform the following configuration in System View.

Table 84 Configuring the IP Address for the DHCP Server

Operation	Command
Configure IP address for DHCP server	<code>dhcp-server groupNo ip ipaddress1 [ipaddress2]</code>
Delete all DHCP server IP addresses (set the IP addresses of master and backup DHCP servers to 0)	<code>undo dhcp-server groupNo</code>

By default, no IP address is configured for the DHCP server.

Note that you must configure an IP address for the backup DHCP server together with that of the master server.

Configuring the DHCP Server Group for the VLAN Interfaces

Perform the following configuration in VLAN Interface View.

Table 85 Configuring the DHCP Server Group Corresponding to VLAN Interfaces

Operation	Command
Configure DHCP server group corresponding to VLAN interfaces	dhcp-server <i>groupNo</i>
Delete DHCP server group	undo dhcp-server

By default, no DHCP server corresponds to VLAN interfaces.

When associating a VLAN interface to a new DHCP server group, you can configure the association without disassociating it from the previous group.

Displaying and Debugging DHCP Configuration

After the above configuration, enter the **display** command in any view to display the running of the DHCP configuration, and to verify the effect of the configuration. Enter the **debugging** command in User View to debug DHCP configuration.

Table 86 Displaying and Debugging DHCP Configuration

Operation	Command
Display configuration information of DHCP server group	display dhcp-server groupNo
Display configuration information about the DHCP Server group corresponding to the VLAN interface	display dhcp-server interface vlan-interface <i>vlan_id</i>
Display all address information of the valid user address table for the DHCP server group	display dhcp-security [<i>ip_address</i> dynamic static] [unit <i>unit_id</i>]
Display address allocation information of DHCP client	display dhcp client [verbose]
Enable/disable DHCP client debugging	[undo] debugging dhcp client { all error event packet }
Enable/disable DHCP Client hot backup debugging	[undo] debugging dhcp xrn xha
Enable/disable DHCP relay debugging	[undo] debugging dhcp-relay

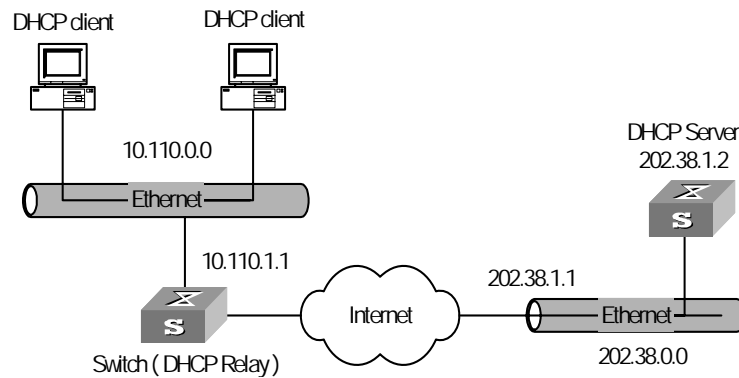
DHCP Relay Configuration Example One

Networking Requirements

There are two VLANs (1 and 10) and they both need to use the same DHCP server.

Networking Diagram

Figure 26 Configuring DHCP Relay



Configuration Procedure

- 1 Create a DHCP server group that will use two DHCP servers (a master and an optional backup) and assign it the IP addresses of the two DHCP servers (the first IP address is the master).

```
[4500]dhcp-server 0 ip 192.168.1.1 192.168.2.1
```

- 2 Configure the Switch so all clients use DHCP server group '0'.

```
[4500]interface vlan-interface 1
[4500-Vlan-interface1]dhcp-server 0
[4500-Vlan-interface1]quit
[4500]interface vlan-interface 10
[4500-Vlan-interface10]dhcp-server 0
[4500-Vlan-interface10]quit
```

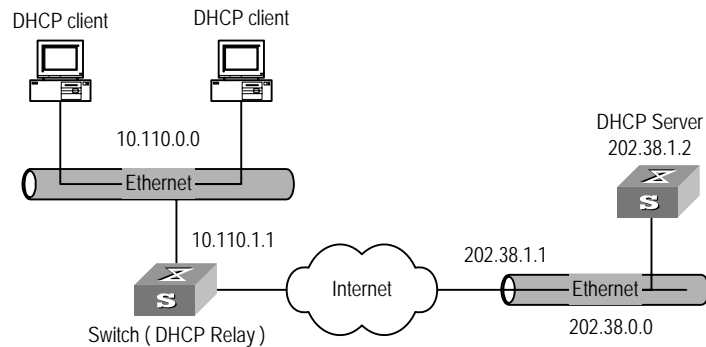
DHCP Relay Configuration Example Two

Networking Requirements

The segment address for the DHCP Client is 10.110.0.0, which is connected to a port in VLAN2 on the Switch. The IP address of the DHCP Server is 202.38.1.2. The DHCP packets should be forwarded via the Switch with DHCP Relay enabled. A DHCP Client can get its IP address and other configuration information from the DHCP Server.

Networking Diagram

Figure 27 Networking Diagram of Configuration DHCP Relay



Configuration Procedure

- 1 Configure the group number of DHCP Server as 1 and the IP address as 202.38.1.2.

```
[4500]dhcp-server 1 ip 202.38.1.2
```
- 2 Associate the VLAN interface 2 with DHCP Server group 1.

```
[4500]interface vlan 2
[4500-Vlan-interface2]dhcp-server 1
```
- 3 Configure the IP address of the VLAN interface 2, which must be in the same segment as DHCP Client.

```
[4500-Vlan-interface2]ip address 10.110.1.1 255.255.0.0
```

To allocate an IP address successfully for the DHCP Client, you need to make the necessary configuration on the DHCP Server, which varies, depending on device type.

Troubleshooting DHCP Relay Configuration

Perform the following procedure if a user cannot apply for an IP address dynamically:

- 1 Use the **display dhcp-server groupNo** command to check if the IP address of the corresponding DHCP Server has been configured.
- 2 Use the **display vlan** and **display ip interface vlan-interface** commands to check if the VLAN and the corresponding interface IP address have been configured.
- 3 Ping the configured DHCP Server to ensure that the link is connected.
- 4 Ping the IP address of the VLAN interface of the Switch to which the DHCP user is connected from the DHCP Server to make sure that the DHCP Server can correctly find the route of the network segment the user is on. If the ping execution fails, check if the default gateway of the DHCP Server has been configured as the address of the VLAN interface that it locates on.

If there is no problem found in the last two steps, use the **display dhcp-server groupNo** command to view which packet has been received. If you only see the Discover packet and there is no response packet, the DHCP Server has not sent the message to the Switch. In this case, check if the DHCP Server has been configured properly. If the numbers of request and response packets are normal, enable the

`debugging dhcp-relay` in User View and then use the `terminal debugging` command to output the debugging information to the console. In this way, you can view the detailed information of all DHCP packets on the console as they apply for the IP address, and so locate the problem.

Access Management Configuration

Access Management Overview

In networking, the ports in a Switch which access different users belong to the same VLAN and they cannot communicate with each other, for the purposes of security, simplicity, and saving VLAN resources. Different ports have different IP addresses and only the users with an IP address which is allowed to pass the port can access the external network through the port. You can achieve this configuration using the functions binding Switch port with IP address and port layer-2 isolating.

Configuring Access Management

Access management configuration includes:

- [Enabling/Disabling Access Management](#)
- [Configuring the Access Management IP Address Pool Based on the Port](#)
- [Configuring Layer 2 Isolation Between Ports](#)
- [Enabling/Disabling Access Management Trap](#)

Enabling/Disabling Access Management

You can use the following command to enable the access management function. Only after the access management function is enabled will the access management features (IP and port binding and Layer 2 port isolation) take effect.

Perform the following configuration in System View.

Table 87 Enabling/Disabling the Access Management Function

Operation	Command
Enable access management function	<code>am enable</code>
Disable access management function	<code>undo am enable</code>

By default, the system disables the access management function.

Configuring the Access Management IP Address Pool Based on the Port

You can use the following command to set the IP address pool for access management on a port. The packet whose source IP address is in the specified pool is allowed to be forwarded on Layer 3 via the port of the Switch.

Perform the following configuration in Ethernet Port View.

Table 88 Configuring the Access Management IP Address Pool Based on the Port

Operation	Command
Configure the access management IP address pool based on the port	<code>am ip-pool address_list</code>

Table 88 Configuring the Access Management IP Address Pool Based on the Port

Operation	Command
Cancel part or all of the IP addresses in the access management IP address pool of the port	<code>undo am ip-pool { all address_list }</code>

By default, the IP address pools for access management on the port are null and all the packets are permitted.

Note that if the IP address pool to be configured contains the IP addresses configured in the static ARP at other ports, then the system prompts you to delete the static ARP to make the later binding effective.

Configuring Layer 2 Isolation Between Ports

You can add a port to an isolation group using the following commands, and achieve port-to-port isolation between this port and other ports of this group, that is, Layer 2 forwarding between the isolated ports is not available.

Perform the following configuration in Ethernet Port View.

Table 89 Configuring Layer 2 Isolation Between Ports

Operation	Command
Add a port to the isolation group	<code>port isolate</code>
Remove a port from the isolation group	<code>undo port isolate</code>

By default, a port is not in an isolation group, that is Layer 2 forwarding is achievable between this port and other ports.

Note that:

- One unit only supports one isolation group. That is, a port in an isolation group on a unit is isolated only from ports within this group, and not isolated from ports in isolation groups on other units.
- The port isolation feature is synchronous on the same unit within an aggregation group. Note the following:
 - When a port in an aggregation group is added to, or removed from, an isolation group, then all the other ports of this aggregation group on the same unit are automatically added in or removed from this isolation group.
 - In the same aggregation group, the port isolation feature on one unit is consistent.
 - If a port is removed from an aggregation group, its port isolation configuration will not change.
 - If a port of an aggregation group is isolated on unit 1, then you can achieve port-to-port isolation between this aggregation group and all the ports of the isolation group on unit 1.
 - If all the ports on unit 1 of this aggregation group are removed from this aggregation group, then the isolation feature of this aggregation group is disabled, that is, the port-to-port isolation mentioned above is unavailable.

Enabling/Disabling Access Management Trap

You can enable the access management trap function using the following commands. When this function is enabled, the trap information of access management is delivered to the console for the purpose of monitoring.

Perform the following configuration in System View.

Table 90 Enabling/Disabling Access Management Trap

Operation	Command
Enable access management trap	am trap enable
Disable access management trap	undo am trap enable

By default, the access management trap is disabled.

Displaying and Debugging Access Management

After the above configuration, enter the **display** command in any view to display the current configurations of access management and port isolation information, and to verify the effect of the configuration.

Table 91 Displaying Current Configuration of Access Management

Operation	Command
Display the status of access management function and configuration of IP address pool	display am [interface_list]
Display port isolation information	display isolate port

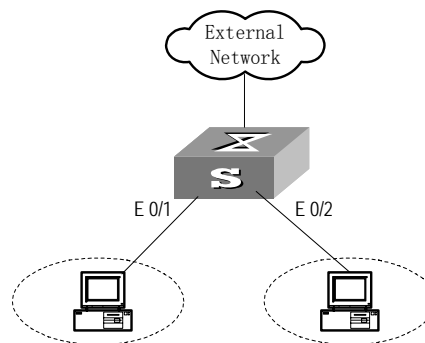
Access Management Configuration Example

Networking Requirements

Organization 1 is connected to port 1 of the Switch, and organization 2 to port 2. Ports 1 and 2 belong to the same VLAN. The IP addresses range 202.10.20.1 to 202.10.20.20 can be accessed from port 1 and the range 202.10.20.21 to 202.10.20.50 from the port 2. Organization 1 and organization 2 cannot communicate with each other.

Networking Diagram

Figure 28 Networking Diagram for Port Isolation Configuration



Configuration Procedure

- 1 Enable access management globally.

```
[ 4500 ] am enable
```

- 2 Configure the IP address pool for access management on port 1.

```
[4500]interface ethernet1/0/1
[4500-Ethernet1/0/1]am ip-pool 202.10.20.1 20
```

- 3 Add port 1 into isolation group.

```
[4500-Ethernet1/0/1]port isolate
```

- 4 Configure the IP address pool for access management on port 2

```
[4500-Ethernet1/0/1]interface ethernt1/0/2
[4500-Ethernet1/0/2]am ip-pool 202.10.20.21 30
```

- 5 Add port 2 into isolation group.

```
[4500-Ethernet1/0/2]port isolate
```

Access Management via the Web

The Security/Authorized IP menu option on the Web interface allows the user to specify a range of IP addresses that will permit Web, Telnet and SSH access.

Network Requirements

Enter an IP address and a 'wildcard' value. For example, an authorized IP address of 10.10.10.1 with a wildcard of 0.0.0.255 will authorize all addresses from 10.10.10.0 to 10.10.10.254.

Configuration Procedure

To configure this feature using the CLI, the following commands should be entered from System View:

```
<4500>system-view
[4500]acl number 2500
[4500-acl-basic-2500]rule 0 permit source 10.10.10.1 0.0.0.255
```

To delete this feature, enter:

```
<4500>system-view
[4500]acl number 2500
[4500-acl-basic-2500]undo rule 0
```

UDP Helper Configuration

Overview of UDP Helper

The major function of the UDP Helper is to relay-forward UDP broadcast packets, that is, it can convert UDP broadcast packets into unicast packets and send them to the designated server, as a relay.

When UDP Helper starts, the Switch can judge whether to forward the UDP broadcast packets received at the port based on UDP port ID. If yes, the Switch then modifies the IP address in the IP packet header and sends the packet to the designated destination server. Otherwise, it sends the packet to the upper layer module for further processing. For the BOOTP/DHCP broadcast packet, if the client specifies in the request message that the response message needs to be received as broadcast packet, then the Switch broadcasts the response message to the client. Otherwise, it unicasts the response message.

UDP Helper Configuration

UDP Helper configuration includes:

- [Enabling/Disabling UDP Helper Function](#)
- [Configuring UDP Port with Replay Function](#)
- [Configuring the Relay Destination Server for Broadcast Packet](#)

Enabling/Disabling UDP Helper Function

When the UDP Helper function is enabled, you can configure the UDP ports where UDP function is required and the relay function is enabled at UDP ports 69, 53, 37, 137, 138, and 49. When the function is disabled, the relay function configured at all UDP ports, including the default six ports, is disabled.

Perform the following configuration in System View.

Table 92 Enabling/Disabling UDP Helper function

Operation	Command
Enable UDP Helper function	udp-helper enable
Disable UDP Helper function	undo udp-helper enable

By default, the UDP Helper function is disabled.

Configuring UDP Port with Replay Function

When the UDP relay function is enabled, by default the system forwards the broadcast packets on the UDP ports listed in [Table 93](#). You can configure up to 256 UDP ports with the relay function.

Table 93 Default UDP Ports List

Protocol	UDP port ID
Trivial File Transfer Protocol (TFTP)	69
Domain Name System (DNS)	53
Time service	37
NetBIOS Name Service (NetBIOS-NS)	137
NetBIOS Datagram Service (NetBIOS-DS)	138
Terminal Access Controller Access Control System (TACACS)	49

Perform the following configuration in System View.

Table 94 Configuring UDP Port with Replay Function

Operation	Command
Configure UDP port with replay function	udp-helper port {port dns netbios-ds netbios-ns tacacs tftp time}
Remove the configuration	undo udp-helper port {port dns netbios-ds netbios-ns tacacs tftp time}

Note that:

- You must first enable the UDP Helper function and then configure the UDP port with the relay function. Otherwise, error information will appear.
- The parameters **dns**, **netbios-ds**, **netbios-ns**, **tacacs**, **tftp** and **time** respectively refer to the six default ports. You can configure the default UDP port in two ways: specifying port IDs and specifying the correct parameters.

For example, the `udp-helper port 53` command is equivalent to the `udp-helper port dns` command in function.

- The default UDP ports are not displayed when using the `display current-configuration` command. But its ID is displayed after its relay function is disabled.

Configuring the Relay Destination Server for Broadcast Packet

You can configure up to 20 relay destination servers for a VLAN interface. If a VLAN interface is configured with relay destination servers and UDP Helper function is enabled on the VLAN interface, then the broadcast packets of a designated UDP port received at the VLAN interface will be unicasted to the destination server.

Perform the following configuration in VLAN Interface View.

Table 95 Configuring the Relay Destination Server for Broadcast Packet

Operation	Command
Configure relay destination server for broadcast packet	<code>udp-helper server ip_address</code>
Delete relay destination server for broadcast packet	<code>undo udp-helper server [ip_address]</code>

Note that:

- The `undo udp-helper server` command (without any parameter) deletes all destination servers configured on the interface.
- By default, no relay destination server for UDP broadcast packets is configured.

Displaying and Debugging UDP Helper Configuration

After the above configuration, enter the `display` command in any view to display the running of the UDP Helper destination server, and to verify the effect of the configuration. Enter the `debugging` command in User View to debug UDP Helper configuration.

Table 96 Displaying and Debugging UDP Helper Configuration

Operation	Command
Display the destination server corresponding to VLAN interface	<code>display udp-helper server [interface vlan-interface vlan_id]</code>
Enable UDP Helper debugging	<code>debugging udp-helper { event packet [receive send] }</code>
Disable UDP Helper debugging	<code>undo debugging udp-helper { event packet [receive send] }</code>

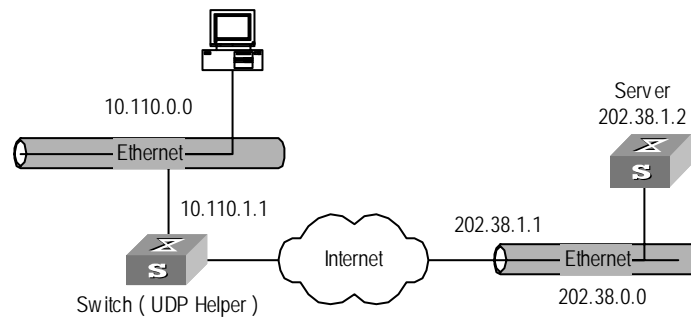
UDP Helper Configuration Example

Networking Requirement

The IP address of VLAN interface 2 on the Switch is 10.110.1.1, which is connected with network segment 10.110.0.0. Set to relay-forward the broadcast packets with destination IP of all 1s and destination UDP port 55 in the network segment 10.110.0.0 to the destination server 202.38.1.2.

Networking Diagram

Figure 29 Networking for UDP Helper Configuration



Configuration Procedure

- 1 Enable UDP Helper function.

```
[ 4500]udp-helper enable
```
- 2 Set to relay-forward the broadcast packets with destination UDP port 55.

```
[ 4500]udp-helper port 55
```
- 3 Set the IP address of the destination server corresponding to VLAN interface 2 as 202.38.1.2.

```
[ 4500]interface vlan 2
[ 4500-Vlan-interface2]udp-helper server 202.38.1.2
```

IP Performance Configuration

IP Performance Configuration

IP performance is described in the following section

Configuring TCP Attributes

TCP attributes that can be configured include:

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

Perform the following configuration in System View.

Table 97 Configuring TCP Attributes

Operation	Command
Configure synwait timer in TCP	<code>tcp timer syn-timeout <i>time_value</i></code>

Table 97 Configuring TCP Attributes

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

By default, the TCP finwait timer is 675 seconds, the synwait timer is 75 seconds, and the receiving/sending buffer size of connection-oriented Socket is 8K bytes.

Displaying and Debugging IP Performance

After the above configuration, enter the `display` command in any view to display the running of the IP Performance configuration, and to verify the effect of the configuration. Enter the `reset` command in User View to clear IP, TCP, and UDP statistics information.

Table 98 Displaying and Debugging IP Performance

Operation	Command
Display TCP connection state	<code>display tcp status</code>
Display TCP connection statistics data	<code>display tcp statistics</code>
Display UDP statistics information	<code>display udp statistics</code>
Display IP statistics information	<code>display ip statistics</code>
Display ICMP statistics information	<code>display icmp statistics</code>
Display socket interface information of current system	<code>display ip socket [socktype <i>sock_type</i>] [task_id <i>socket_id</i>]</code>
Display the summary of the Forwarding Information Base	<code>display fib</code>
Display the FIB entries matching the destination IP address (range)	<code>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]</code>
Display the FIB entries matching a specific ACL	<code>display fib acl <i>number</i></code>
Display the FIB entries which are output from the buffer according to regular expression and related to the specific character string	<code>display fib { { begin include exclude } <i>text</i> }</code>
Display the FIB entries matching the specific prefix list	<code>display fib ip-prefix <i>listname</i></code>
Display the total number of FIB entries	<code>display fib statistics [{ begin include exclude } <i>text</i>]</code>
Reset IP statistics information	<code>reset ip statistics</code>
Reset TCP statistics information	<code>reset tcp statistics</code>
Reset UDP statistics information	<code>reset udp statistics</code>

Troubleshooting IP Performance

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

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

- Use the **terminal debugging** command to output the debugging information to the console.
- Use the command **debugging udp packet** to enable the UDP debugging to trace the UDP packet.

The following are the UDP packet formats:

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

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

Operations include:

```
[4500]terminal debugging  
<4500>debugging tcp packet
```

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

```
TCP output packet:  
Source IP address:202.38.160.1  
Source port:1024  
Destination IP Address 202.38.160.1  
Destination port: 4296  
Sequence number :4185089  
Ack number: 0  
Flag :SYN  
Packet length :60  
Data offset: 10
```


6

IP ROUTING PROTOCOL OPERATION

IP Routing Protocol Overview

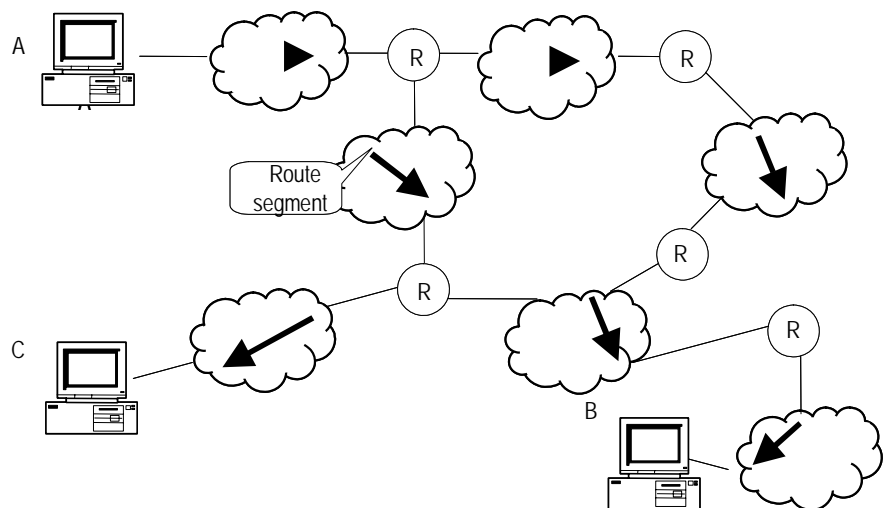
Routers select an appropriate path through a network for an IP packet according to the destination address of the packet. Each router on the path receives the packet and forwards it to the next router. The last router in the path submits the packet to the destination host.

For example, in [Figure 30](#), a packet sent from Host A to Host C goes through 3 networks and 2 routers and the packet is transmitted through two hops (represented by the bold arrows) and route segments. Therefore, when a node is connected to another node through a network, there is a route segment between these two nodes and these two nodes are considered adjacent in the Internet. Adjacent routers are two routers connected to the same network. The number of route segments between a router and hosts in the same network is zero.



When the Switch 4500 runs a routing protocol, it can perform router functions. In this guide, a router and its icon represent either a generic router or a Switch 4500 running routing protocols.

Figure 30 About hops



Networks can be different sizes, so the segment lengths between two different pairs of routers can also be different.

If a router in a network is regarded as a node and a route segment in the Internet is regarded as a link, message routing in the Internet works in a similar way as the message routing in a conventional network. The shortest route may not always be

the optimal route. For example, routing through three LAN route segments may be much faster than routing through two WAN route segments.

Configuring the IP Routing Protocol is described in the following sections:

- [Selecting Routes Through the Routing Table](#)
- [Routing Management Policy](#)

Selecting Routes Through the Routing Table

For a router, the routing table is the key to forwarding packets. Each router saves a routing table in its memory, and each entry in this table specifies the physical port of the router through which a packet is sent to a subnet or a host. The packet can reach the next router over a particular path or reach a destination host through a directly connected network.

A routing table has the following key entries:

- A destination address — Identifies the destination IP address or the destination network of the IP packet, which is 32 bits in length.
- A network mask — Made up of several consecutive 1s, which can be expressed either in the dotted decimal format, or by the number of the consecutive 1s in the mask. Combined with the destination address, the network mask identifies the network address of the destination host or router. With the destination address and the network mask, you have the address of the network segment where the destination host or router is located. For example, if the destination address is 129.102.8.10, the address of the network where the host or the router with the mask 255.255.0.0 is located is 129.102.0.0.
- The output interface — Indicates an interface through which an IP packet should be forwarded.
- The next hop address — Indicates the next router that an IP packet will pass through.
- The priority added to the IP routing table for a route — Indicates the type of route that is selected. There may be multiple routes with different next hops to the same destination. These routes can be discovered by different routing protocols, or they can be the static routes that are configured manually. The route with the highest priority (the smallest numerical value) is selected as the current optimal route.

Routes are divided into the following types: subnet routes, in which the destination is a subnet, or host routes, in which the destination is a host.

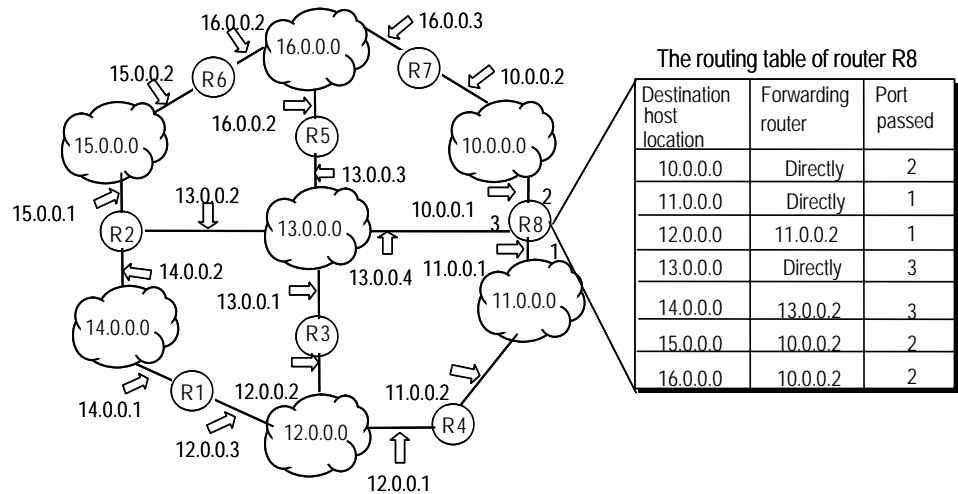
In addition, depending on whether the network of the destination host is directly connected to the router, there are the following types of routes:

- Direct route — The router is directly connected to the network where the destination is located.
- Indirect route — The router is not directly connected to the network where the destination is located.

To limit the size of the routing table, an option is available to set a default route. All the packets that fail to find a suitable table entry are forwarded through this default route.

In a complicated Internet configuration, as shown in [Figure 31](#), the number in each network is the network address. The router R8 is connected to three networks, so it has three IP addresses and three physical ports. Its routing table is shown in Figure 2.

Figure 31 The routing table



The Switch 4500 can automatically obtain some direct routes according to the interface state and user configuration.

Routing Management Policy

You can manually configure a static route to a certain destination or configure the interaction between dynamic routing protocol and other routers in your network and find a route via routing algorithm. The static routes configured by the user are managed together with the dynamic routes discovered by the routing protocol in the router. The static routes and the routes learned or configured by different routing protocols can also be shared among routing protocols.

Routing Protocols and Route Preferences

Routing protocols (including static routes) can generate different routes to the same destination, but not all these routes are optimal. In fact, at a certain moment, only one routing protocol can determine a current route to a single destination. Thus, each routing protocol (including static routes) has a set preference, and when there are multiple routing information sources, the route with the highest preference becomes the current route. Routing protocols and the default preferences of the routes that they learn are shown in [Table 99](#). The smaller the value, the higher the preference).

Table 99 Routing Protocols and the Default Preferences for Routes

Routing protocol or route type	The preference of the corresponding route
DIRECT	0
STATIC	60
UNKNOWN	255

Except for direct routing, the preferences of various dynamic routing protocols can be manually configured to meet the user requirements. The preferences for individual static routes can be different.

Supporting Load Sharing and Route Backup

I. Load sharing

The Switch 4500 supports multi-route mode, allowing the user to configure multiple routes that reach the same destination and use the same precedence. The same destination can be reached via multiple different paths, whose precedences are equal. When there is no route that can reach the same destination with a higher precedence, the multiple routes will be adopted by IP, which will forward the packets to the destination via these paths so as to implement load sharing.

For the same destination, a specified routing protocol may find multiple different routes. If the routing protocol has the highest precedence among all active routing protocols, these multiple routes will be regarded as currently valid routes. Thus, load sharing of IP traffic is ensured in terms of routing protocols.

The Switch 4500 supports three routes to implement load sharing.

II. Route backup

The Switch 4500 supports route backup. If the main route is in failure, the unit will automatically switch to a backup route to improve the network reliability.

To achieve route backup, the user can configure multiple routes to the same destination according to actual situation. One of the routes has the highest precedence and is called the main route. The other routes have descending precedences and are called backup routes. Normally, the router sends data via the main route. When the line fails, the main route will hide itself and the router will choose from one of the remaining routes as a backup route whose precedence is higher than the others to send data. This process is the switchover from the main route to the backup route. When the main route recovers, the router will restore it by re-selecting the main route. As the main route has the highest precedence, the router will select the main route again to send data. This process is the automatic switchover from the backup route to the main route.

Routes Shared between Routing Protocols

As the algorithms of various routing protocols are different, different protocols can generate different routes. This situation creates the problem of how to resolve the different routes being generated by different routing protocols. The Switch 4500 can import the information of another routing protocol. Each protocol has its own route redistribution mechanism. For more information, see [“Configuring RIP to Import Routes of Other Protocols”](#) on [page 117](#).

Static Routes

A static route is a route that is manually configured by the network administrator. You can set up an interconnected network using static routes. However, if a fault occurs in the network, the static route cannot change automatically to steer packets away from the fault without the help of the administrator.

In a relatively simple network, you only need to configure static routes to make the router work normally. Proper configuration and usage of the static route can improve network performance and ensure bandwidth for important applications.

The following routes are static routes:

- Reachable route — The IP packet is sent to the next hop towards the destination. This is a common type of static route.
- Unreachable route — When a static route to a destination has the *reject* attribute, all the IP packets to this destination are discarded, and the originating host is informed that the destination is unreachable.
- Blackhole route — If a static route to a destination has the *blackhole* attribute, all the IP packets to this destination are discarded, and the originating host is not informed.

The attributes *reject* and *blackhole* are usually used to control the range of reachable destinations for the router, and to help troubleshoot the network.

Default Route

The default route is also a static route. The default route is used only when no suitable routing table entry is found. In a routing table, the default route is in the form of the route to the network 0.0.0.0 (with the mask 0.0.0.0). You can determine whether a default route has been set by viewing the output of the **display ip routing-table** command. If the destination address of a packet fails to match any entry of the routing table, the router selects the default route to forward this packet. If there is no default route and the destination address of the packet fails to match any entry in the routing table, the packet is discarded, and an Internet Control Message Protocol (ICMP) packet is sent to the originating host to indicate that the destination host or network is unreachable.

In a typical network that consists of hundreds of routers, if you used multiple dynamic routing protocols without configuring a default route then significant bandwidth is consumed. Using the default route can provide appropriate bandwidth for communications between large numbers of users.

Configuring Static Routes

Static route configuration tasks are described in the following sections:

- [Configuring a Static Route](#)
- [Configuring a Default Route](#)
- [Deleting All The Static Routes](#)
- [Displaying and Debugging Static Routes](#)

Configuring a Static Route

Perform the following configurations in System View.

Table 100 Configuring a static route

Operation	Command
Add a static route	ip route-static <i>ip_address</i> { <i>mask</i> <i>mask_length</i> } { <i>interface_type interface_number</i> <i>gateway_address</i> } [preference value] [reject blackhole]
Delete a static route	undo ip route-static <i>ip_address</i> { <i>mask</i> <i>mask_length</i> } [<i>interface_type interface_number</i> <i>gateway_address</i>] [preference value] [reject blackhole]

The parameters are explained as follows:

- IP address and mask

The IP address and mask use a decimal format. Because the 1s in the 32-bit mask must be consecutive, the dotted decimal mask can also be replaced by the mask-length which refers to the digits of the consecutive 1s in the mask.

- Next hop address and NULL interface

When configuring a static route, you can specify the *gateway_address* to decide the next hop address, depending on the actual conditions.

For all the routing items, the next hop address must be specified. When the IP layer transmits a packet, it first searches the matching route in the routing table, depending on the destination address of the packet. Only when the next hop address of the route is specified can the link layer find the corresponding link layer address, and then forward the packet.

The packets sent to the NULL interface, which is a virtual interface, are discarded at once. This can decrease system load.

You cannot specify an interface address of the local Switch as the next hop address of a static route.

- Preference

For different configurations of *preference_value*, you can flexibly apply the routing management policy.

- Other parameters

The attributes **reject** and **blackhole** indicate the unreachable route and the blackhole route, respectively.

Configuring a Default Route

Perform the following configurations in System View.

Table 101 Configuring a default route

Operation	Command
Configure a default route	ip route-static 0.0.0.0 { 0.0.0.0 0 } { <i>interface_type interface_number gateway_address</i> } [preference value] [reject blackhole]
Delete a default route	undo ip route-static 0.0.0.0 { 0.0.0.0 0 } [<i>interface_type interface_number gateway_address</i>] [preference value] [reject blackhole]

The parameters for the default route are the same as those for the static route.

Deleting All The Static Routes

You can use the **undo ip route-static** command to delete a static route. The Switch 4500 also provides the **delete static-routes all** command for you to delete all static routes at one time, including the default routes.

Perform the following configuration in System View.

Table 102 Deleting all static routes

Operation	Command
Delete all static routes	delete static-routes all

Displaying and Debugging Static Routes

After you configure static and default routes, execute the **display** command in any view to display the static route configuration, and to verify the effect of the configuration.

Table 103 Displaying and debugging the routing table

Operation	Command
View routing table summary	display ip routing-table
View routing table details	display ip routing-table verbose
View the detailed information of a specific route	display ip routing-table ip_address [mask] [longer-match] [verbose]
View the route information in the specified address range	display ip routing-table ip_address1 mask1 ip_address2 mask2 [verbose]
View the route filtered through specified basic access control list (ACL)	display ip routing-table acl acl_number [verbose]
View the route information that through specified ip prefix list	display ip routing-table ip-prefix ip_prefix_name [verbose]
View the routing information found by the specified protocol	display ip routing-table protocol protocol [inactive verbose]
View the tree routing table	display ip routing-table radix
View the statistics of the routing table	display ip routing-table statistics

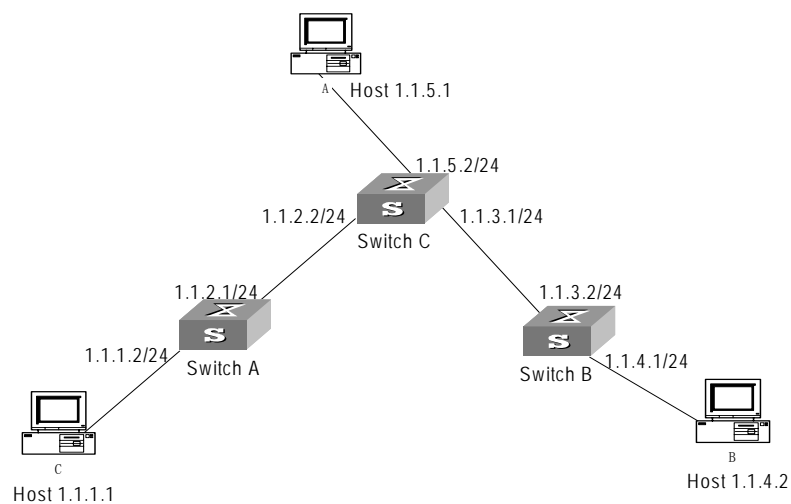
Example: Typical Static Route Configuration

Networking Requirements

The masks of all the IP addresses shown in [Figure 32](#) are 255.255.255.0. All the hosts or switches must be interconnected in pairs by configuring static routes.

Networking Diagram

Figure 32 Networking diagram of the static route configuration example



Configuration procedure

- 1 Configure the static route for Ethernet Switch A

```
[Switch A]ip route-static 1.1.3.0 255.255.255.0 1.1.2.2
[Switch A]ip route-static 1.1.4.0 255.255.255.0 1.1.2.2
```

```
[Switch A]ip route-static 1.1.5.0 255.255.255.0 1.1.2.2
```

2 Configure the static route for Ethernet Switch B

```
[Switch B]ip route-static 1.1.2.0 255.255.255.0 1.1.3.1
```

```
[Switch B]ip route-static 1.1.5.0 255.255.255.0 1.1.3.1
```

```
[Switch B]ip route-static 1.1.1.0 255.255.255.0 1.1.3.1
```

3 Configure the static route for Ethernet Switch C

```
[Switch C]ip route-static 1.1.1.0 255.255.255.0 1.1.2.1
```

```
[Switch C]ip route-static 1.1.4.0 255.255.255.0 1.1.3.2
```

4 Configure the default gateway of the Host A to be 1.1.5.1

5 Configure the default gateway of the Host B to be 1.1.4.1

6 Configure the default gateway of the Host C to be 1.1.1.1

Using this procedure, all the hosts or switches in [Figure 32](#) can be interconnected in pairs.

Troubleshooting Static Routes

The Switch 4500 is not configured with the dynamic routing protocol enabled. Both the physical status and the link layer protocol status of the interface are enabled, but the IP packets cannot be forwarded normally.

Troubleshooting:

- Use the **display ip routing-table protocol static** command to view whether the corresponding static route is correctly configured.
- Use the **display ip routing-table** command to view whether the corresponding route is valid.

RIP

Routing Information Protocol (RIP) is a simple dynamic routing protocol, that is Distance-Vector (D-V) algorithm based. It uses hop counts to measure the distance to the destination host. This is called the routing cost. In RIP, the hop count from a router to its directly connected network is 0; the hop count to a network which can be reached through another router is 1; and so on. To restrict the time to converge, RIP prescribes that the cost value is an integer ranging from 0 and 15. A hop count equal to or exceeding 16 is defined as infinite, which indicates that the destination network or the host is unreachable.

RIP sends a routing refresh message every 30 seconds. If no routing refresh message is received from a network neighbor in 180 seconds, RIP tags all routes of the network neighbor as unreachable. If no routing refresh message is received from a network neighbor in 300 seconds, RIP removes the routes of the network neighbor from the routing table.

To improve network performances and avoid routing loops, RIP supports split horizon, poison reverse, and allows importing of routes discovered by other routing protocols.

Each router that is running RIP manages a route database, which contains routing entries to all the reachable destinations in the network. These routing entries contain the following information:

- Destination address — The IP address of a host or network.

- Next hop address — The address of the next router that an IP packet will pass through for reaching the destination.
- Interface — The interface through which the IP packet should be forwarded.
- Cost — The cost for the router to reach the destination, which should be an integer in the range of 0 to 16.
- Timer — The length of time from the last time that the routing entry was modified until now. The timer is reset to 0 whenever a routing entry is modified.

RIP is controlled by three timers as follows:

- Period update — Triggered periodically to send all RIP routes to all neighbors.
- Timeout — If a RIP route has not been updated when the timer times out (i.e. the Switch has not received update packets from the neighbors) the route will be considered unreachable.
- Garbage-collection — If Garbage-collection times out before the unreachable route is updated by the packets from the neighbors, then the route will be deleted from the routing table.

The process of RIP startup and operation is as follows:

- 1 If RIP is enabled on a router for the first time, the router broadcasts or multicasts a request packet to the adjacent routers. When they receive the request packet, adjacent routers (on which RIP is also enabled) respond to the request by returning response packets containing information about their local routing tables.
- 2 After receiving the response packets, the router that sent the request modifies its own routing table and sends a modification triggering packet to the neighbor router. The neighbor router sends this packet to all its neighbor routers. After a series of modification triggering processes, each router can get and keep the updated routing information.
- 3 RIP broadcasts its routing table to the adjacent routers every 30 seconds. The adjacent routers maintain their own routing table after receiving the packets and elect an optimal route. They then advertise the modification information to their adjacent network to make the updated route globally available. RIP uses the timeout mechanism to handle timed out routes to ensure the timeliness and validity of the routes. With these mechanisms, RIP, an interior routing protocol, enables the router to learn the routing information of the entire network.

RIP has become one of the most popular standards of transmitting router and host routes. It can be used in most campus networks and regional networks that are simple yet extensive. RIP is not recommended for larger and more complicated networks.

RIP configuration is described in the following sections:

- [Configuring RIP](#)
- [Troubleshooting RIP](#)

Configuring RIP

Only after RIP is enabled can other functional features be configured. But the configuration of the interface-related functional features is not dependent on whether RIP has been enabled.



After RIP is disabled, the interface-related features also become invalid.

The RIP configuration tasks are described in the following sections:

- [Enabling RIP and Entering the RIP View](#)
- [Enabling RIP on a Specified Network](#)
- [Configuring Unicast RIP Messages](#)
- [Specifying the RIP Version](#)
- [Configuring RIP Timers](#)
- [Configuring RIP-1 Zero Field Check of the Interface Packet](#)
- [Specifying the Operating State of the Interface](#)
- [Disabling Host Route](#)
- [Enabling RIP-2 Route Aggregation](#)
- [Setting RIP-2 Packet Authentication](#)
- [Configuring Split Horizon](#)
- [Configuring RIP to Import Routes of Other Protocols](#)
- [Configuring the Default Cost for the Imported Route](#)
- [Setting the RIP Preference](#)
- [Setting Additional Routing Metrics](#)
- [Configuring Route Filtering](#)

Enabling RIP and Entering the RIP View

Perform the following configurations in System View

Table 104 Enabling RIP and Entering the RIP View

Operation	Command
Enable RIP and enter RIP view	rip
Disable RIP	undo rip

By default, RIP is not enabled.

Enabling RIP on a Specified Network

For flexible control of RIP operation, you can specify the interface and configure the network on which the interface is located to the RIP network, so that these interfaces can send and receive RIP packets.

Perform the following configurations in RIP View.

Table 105 Enabling RIP Interface

Operation	Command
Enable RIP on the specified network	network <i>network_address</i>
Disable RIP on the specified network	undo network <i>network_address</i>



After the RIP interface is enabled, you should also specify its operating network segment, because RIP only operates on the interface when the network segment

has been specified. RIP does not receive or send routes for an interface that is not on the specified network, and does not forward its interface route.

When the **network** command is used for an address, the effect is to enable the interface of the network with this address. For example, for network 129.102.1.1, you can see network 129.102.0.0 either using the **display current-configuration** command, or using the **display rip** command.

By default, RIP is disabled on all interfaces.

Configuring Unicast RIP Messages

RIP is a broadcast protocol which uses broadcast or multicast addresses to send packets. To exchange routing information with a non-broadcast network, unicast transmission mode must be used.

Perform the following configuration in the RIP View.

Table 106 Configuring unicast RIP messages

Operation	Command
Configure unicast RIP message	peer <i>ip_address</i>
Cancel unicast RIP message	undo peer <i>ip_address</i>

By default, RIP does not send messages to unicast addresses.

3Com does not recommend the use of this command, because the destination address does not need to receive two copies of the same message at the same time. Note that **peer** should be restricted using the following commands: **rip work**, **rip output**, **rip input** and **network**.

Specifying the RIP Version

RIP has two versions, RIP-1 and RIP-2. You can specify the version of the RIP packet used by the interface.

RIP-1 broadcasts the packets. RIP-2 can transmit packets by both broadcast and multicast. By default, multicast is adopted for transmitting packets. In RIP-2, the default multicast address is 224.0.0.9. The advantage of transmitting packets in multicast mode is that the hosts in the same network that do not run RIP, do not receive RIP broadcast packets. In addition, this mode prevents the hosts that are running RIP-1 from incorrectly receiving and processing the routes with subnet masks in RIP-2. When an interface is running RIP-2, it can also receive RIP-1 packets.

Perform the following configuration in Interface View.

Table 107 Specifying RIP Version of the Interface

Operation	Command
Specify the interface version as RIP-1	rip version 1
Specify the interface version as RIP-2	rip version 2 [broadcast multicast]
Restore the default RIP version running on the interface	undo rip version

By default, the interface receives and sends the RIP-1 packets. It transmits packets in multicast mode when the interface RIP version is set to RIP-2.

Configuring RIP Timers

As stipulated in RFC 1058, RIP is controlled by three timers: period update, timeout, and garbage-collection:

- Period update is triggered periodically to send all RIP routes to all neighbors.
- If an RIP route has not been updated when the timeout timer expires, the route is considered unreachable.
- If the garbage-collection timer expires before the unreachable route is updated by the update packets from the neighbors, the route will be deleted completely from the routing table.

Modification of these timers can affect the convergence speed of RIP.

Perform the following configuration in RIP View.

Table 108 Configuring RIP timers

Operation	Command
Configure RIP timers	<code>timers { update update_timer_length timeout timeout_timer_length } *</code>
Restore the default settings of RIP	<code>undo timers { update timeout } *</code>

The modification of RIP timers is validated immediately.

By default, the values of the period update and timeout timers are 30 seconds and 180 seconds respectively. The value of the garbage-collection timer is four times of that of Period Update timer: 120 seconds.

In fact, you may find that the timeout time of the garbage-collection timer is not fixed. If the period update timer is set to 30 seconds, the garbage-collection timer might range from 90 to 120 seconds.

Before RIP completely deletes an unreachable route from the routing table, it advertises the route by sending four update packets with a route metric of 16, to let all the neighbors know that the route is unreachable. Routes do not always become unreachable when a new period starts so the actual value of the garbage-collection timer is 3 to 4 times of that of the period update timer.



You must consider network performance when adjusting RIP timers, and configure all the routes that are running RIP, so as to avoid unnecessary traffic or network oscillation.

Configuring RIP-1 Zero Field Check of the Interface Packet

According to the RFC 1058, some fields in the RIP-1 packet must be 0. When an interface version is set to RIP-1, the zero field check must be performed on the packet. If the value in the zero field is not zero, processing is refused. There are no zero fields in RIP-2 packets so configuring a zero field check is invalid for RIP-2.

Perform the following configurations in RIP View.

Table 109 Configuring Zero Field Check of the Interface Packets

Operation	Command
Configure zero field check on the RIP-1 packet	checkzero
Disable zero field check on the RIP-1 packet	undo checkzero

Specifying the Operating State of the Interface

In the Interface View, you can specify whether RIP update packets are sent and received on the interface. In addition, you can specify whether an interface sends or receives RIP update packets.

Perform the following configuration in Interface View:

Table 110 Specifying the Operating State of the Interface

Operation	Command
Enable the interface to run RIP	rip work
Disable the interface from running RIP	undo rip work
Enable the interface to receive RIP update packets	rip input
Disable the interface from receiving RIP update packets	undo rip input
Enable the interface to send RIP update packets	rip output
Disable the interface from sending RIP update packets	undo rip output

The **undo rip work** command and the **undo network** command have similar but not the same functions. The **undo rip work** command allows other interfaces to forward the route of the interface applying this command. The **undo network** command prevents other interfaces from forwarding the route of the interface applying this command, and it appears that this interface has been removed.

In addition, the **rip work** command is functionally equivalent to both the **rip input** and **rip output** commands.

By default, all interfaces except loopback interfaces both receive and transmit RIP update packets.

Disabling Host Route

In some cases, the router can receive many host routes from the same segment, and these routes are of little help in route addressing but consume a lot of network resources. Routers can be configured to reject host routes by using the **undo host-route** command.

Perform the following configurations in RIP View.

Table 111 Disabling Host Route

Operation	Command
Enable receiving host route	host-route
Disable receiving host route	undo host-route

By default, the router receives the host route.

Enabling RIP-2 Route Aggregation

Route aggregation means that different subnet routes in the same natural network can be aggregated into one natural mask route for transmission when they are sent to other networks. Route aggregation can be performed to reduce the routing traffic on the network as well as to reduce the size of the routing table.

RIP-1 only sends the routes with natural mask, that is, it always sends routes in the route aggregation form.

RIP-2 supports subnet mask and classless inter-domain routing. To advertise all the subnet routes, the route aggregation function of RIP-2 can be disabled.

Perform the following configurations in RIP View.

Table 112 Enabling Route Aggregation

Operation	Command
Activate the automatic aggregation function of RIP-2	summary
Disable the automatic aggregation function of RIP-2	undo summary

By default, RIP-2 uses the route aggregation function.

Setting RIP-2 Packet Authentication

RIP-1 does not support packet authentication. However, you can configure packet authentication on RIP-2 interfaces.

RIP-2 supports two authentication modes:

- Simple authentication — This mode does not ensure security. The key is not encrypted and can be seen in a network trace, so simple authentication should not be applied when there are high security requirements.
- MD5 authentication — This mode uses two packet formats. One format follows RFC1723, and the other follows RFC2082.

Perform the following configuration in Interface View:

Table 113 Setting RIP-2 Packet Authentication

Operation	Command
Configure RIP-2 simple authentication key	rip authentication-mode simple password_string
Configure RIP-2 MD5 authentication with packet type following RFC 1723	rip authentication-mode md5 usual key_string
Configure RIP-2 MD5 authentication with packet type following RFC 2082	rip authentication-mode md5 nonstandard key_string key_id
Cancel authentication of RIP-2 packet	undo rip authentication-mode

The **usual** packet format follows RFC1723 and **nonstandard** follows RFC2082.

Configuring Split Horizon

Split horizon means that the route received through an interface will not be sent through this interface again. The split horizon algorithm can reduce the

generation of routing loops, but in some special cases, split horizon must be disabled to obtain correct advertising at the cost of efficiency. Disabling split horizon has no effect on P2P connected links but is applicable on the Ethernet.

Perform the following configuration in Interface View:

Table 114 Configuring Split Horizon

Operation	Command
Enable split horizon	rip split-horizon
Disable split horizon	undo rip split-horizon

By default, split horizon is enabled.

Configuring RIP to Import Routes of Other Protocols

RIP allows users to import the route information of other protocols into the routing table.

RIP can import the routes of Direct and Static.

Perform the following configurations in RIP View.

Table 115 Configure RIP to Import Routes of Other Protocols

Operation	Command
Configure RIP to import routes of other protocols	import-route <i>protocol</i> [cost value] [route-policy <i>route_policy_name</i>]
Disable the imported routing information of other protocols	undo import-route <i>protocol</i>
Configure the default cost for the imported route	default cost value
Restore the default cost of the imported route	undo default cost

By default, RIP does not import the route information of other protocols.

If you do not specify the cost of the imported route, RIP will set it to the default cost. By default, the cost *value* for the RIP imported route is 1.

Configuring the Default Cost for the Imported Route

When you use the **import-route** command to import the routes of other protocols, you can specify their cost. If you do not specify the cost of the imported route, RIP will set the cost to the default cost, specified by the **default cost** parameter.

Perform the following configurations in RIP View.

Table 116 Configuring the Default Cost for the Imported Route

Operation	Command
Configure default cost for the imported route	default cost value
Restore the default cost of the imported route	undo default cost

By default, the cost *value* for the RIP imported route is 1.

Setting the RIP Preference

Each routing protocol has its own preference by which the routing policy selects the optimal route from the routes of different protocols. The greater the preference value, the lower the preference. The preference of RIP can be set manually.

Perform the following configurations in RIP View.

Table 117 Setting the RIP Preference

Operation	Command
Set the RIP Preference	preference <i>value</i>
Restore the default value of RIP preference	undo preference

By default, the preference of RIP is 100.

Setting Additional Routing Metrics

The additional routing metric is the input or output routing metric added to an RIP route. It does not change the metric value of the route in the routing table, but adds a specified metric value when the interface receives or sends a route.

Perform the following configuration in Interface View:

Table 118 Setting Additional Routing Metrics

Operation	Command
Set the additional routing metric of the route when the interface receives an RIP packet	rip metricin <i>value</i>
Disable the additional routing metric of the route when the interface receives an RIP packet	undo rip metricin
Set the additional routing metric of the route when the interface sends an RIP packet	ip metricout <i>value</i>
Disable the additional routing metric of the route when the interface sends an RIP packet	undo ip metricout

By default, the additional routing metric added to the route when RIP sends the packet is 1. The additional routing metric when RIP receives the packet is 0.



The metricout configuration takes effect only on the RIP routes learnt by the router and RIP routes generated by the router itself, which means that it has no effect on the routes imported to RIP by other routing protocols.

Configuring Route Filtering

The Router provides a route filtering function. You can configure the filter policy rules by specifying the ACL and ip-prefix for route redistribution and distribution. To import a route, the RIP packet of a specific router can also be received by designating a neighbor router.

Perform the following configurations in RIP View.

Configuring RIP to Filter the Received Routes

Table 119 Configuring RIP to Filter the Received Routes

Operation	Command
Filter the received routing information distributed by the specified address	filter-policy gateway <i>ip_prefix_name</i> import
Cancel filtering of the received routing information distributed by the specified address	undo filter-policy gateway <i>ip_prefix_name</i> [gateway <i>ip-prefix-name</i>] route-policy <i>route-policy-name</i> } import
Filter the received global routing information	filter-policy { <i>acl_number</i> ip-prefix <i>ip_prefix_name</i> [gateway <i>ip-prefix-name</i>] route-policy <i>route-policy-name</i> } import
Cancel filtering of the received global routing information	undo filter-policy { <i>acl_number</i> ip-prefix <i>ip_prefix_name</i> } import

Configuring RIP to Filter the Distributed Routes

Table 120 Configuring RIP to Filter the Distributed Routes

Operation	Command
Configure RIP to filter the distributed routing information	filter-policy { <i>acl_number</i> ip-prefix <i>ip_prefix_name</i> route-policy <i>route_policy_name</i> } export [<i>routing_protocol</i>]
Cancel the filtering of the routing information	undo filter-policy { <i>acl_number</i> ip-prefix <i>ip_prefix-name</i> route-policy <i>route_policy_name</i> } export [<i>routing_protocol</i>]

By default, RIP will not filter the received and distributed routing information.



- *The **filter-policy import** command filters the RIP routes received from its neighbors, and the routes that cannot pass the filter will not be added to the routing table, and will not be advertised to the neighbors.*
- *The **filter-policy export** command filters all the advertised routes, including routes imported by using the **import-route** command, and RIP routes learned from the neighbors.*
- *If the **filter-policy export** command does not specify which route is to be filtered, then all the routes imported by the **import-route** command and the transmitted RIP routes will be filtered.*

Displaying and Debugging RIP

After configuring RIP, enter the **display** command in any view to display the RIP configuration, and to verify the effect of the configuration. Enter the **debugging** command in User View to debug the RIP module. Enter the **reset** command in RIP View to reset the system configuration parameters of RIP.

Table 121 Displaying and Debugging RIP

Operation	Command
Display the current RIP running state and configuration information	display rip
Enable the RIP debugging information	debugging rip packet
Disable the RIP debugging information	undo debugging rip packet

Table 121 Displaying and Debugging RIP

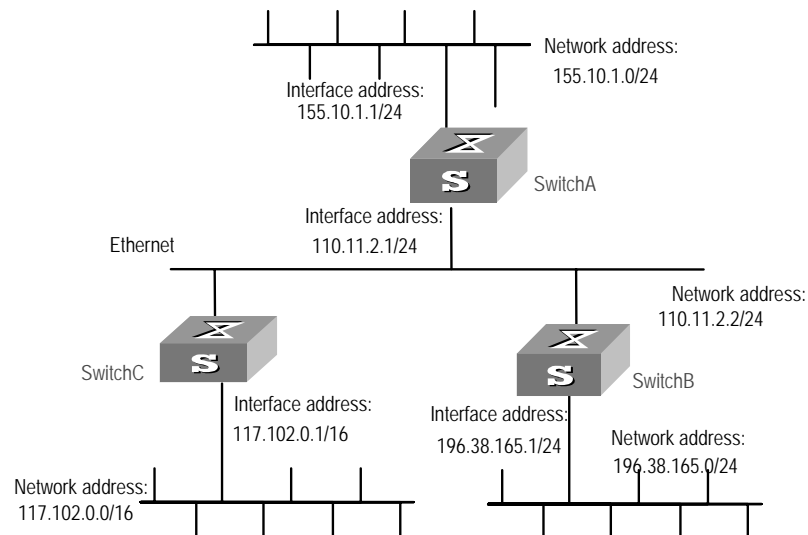
Operation	Command
Enable the debugging of RIP receiving packet	debugging rip receive
Disable the debugging of RIP receiving packet	undo debugging rip receive
Enable the debugging of RIP sending packet	debugging rip send
Disable the debugging of RIP sending packet	undo debugging rip send
Reset the system configuration parameters of RIP	reset

Example: Typical RIP Configuration

Networking Requirements

As shown in [Figure 33](#), Switch C connects to the subnet 117.102.0.0 through the Ethernet port. The Ethernet ports of Switch A and Switch B are connected to the networks 155.10.1.0 and 196.38.165.0 respectively. Switch C, Switch A and Switch B are connected via Ethernet 110.11.2.0. Correctly configure RIP to ensure that Switch C, Switch A and Switch B can interconnect.

Networking Diagram

Figure 33 RIP configuration networking

Configuration Procedure



The following configuration only shows the operations related to RIP. Before performing the following configuration, please make sure the Ethernet link layer can work normally and the IP addresses for the VLAN interfaces are configured.

1 Configure RIP on Switch A

```
[Switch A]rip
[Switch A-rip]network 110.11.2.0
[Switch A-rip]network 155.10.1.0
```

2 Configure RIP on Switch B

```
[Switch B]rip
[Switch B-rip]network 196.38.165.0
[Switch B-rip]network 110.11.2.0
```

3 Configure RIP on Switch C

```
[Switch C]rip
[Switch C-rip]network 117.102.0.0
[Switch C-rip]network 110.11.2.0
```

Troubleshooting RIP The Switch 4500 cannot receive the update packets when the physical connection to the peer routing device is normal.

- RIP does not operate on the corresponding interface (for example, the **undo rip work** command is executed) or this interface is not enabled through the **network** command.
- The peer routing device is configured to be in the multicast mode (for example, the **rip version 2 multicast** command is executed) but the multicast mode has not been configured on the corresponding interface of the local Ethernet Switch.

IP Routing Policy

When a router distributes or receives routing information, it must implement policies to filter the routing information so that it can receive or distribute only the routing information that meets specified conditions. A routing protocol, such as RIP, may need to import routing information discovered by other protocols to enrich its routing knowledge. While importing the routing information, it must import only the information that meets its conditions.

To implement a routing policy, you must define a set of rules by specifying the characteristics of the routing information to be filtered. You can set the rules based on such attributes as the destination address and source address of the information. The rules can be set in advance and then used in the routing policy to advertise, receive and import the route information.

The Switch 4500 supports three kinds of filters. The following sections introduce these filters:

- Route Policy
- ACL
- IP Prefix

Route Policy

A route policy is used to match some attributes with given routing information and the attributes of the information will be set if the conditions are satisfied.

A route policy can comprise multiple nodes. Each node is a unit for match testing, and the nodes will be matched in a sequence-number-based order. Each node comprises a set of **if-match** and **apply** clauses. The **if-match** clauses define the matching rules and the matching objects are attributes of routing information. The relationship of **if-match** clauses for a node uses a series of Boolean "AND" statements. As a result, a match is found unless all the matching conditions specified by the **if-match** clauses are satisfied. The **apply** clause specifies the actions that are performed after the node match test concerning the attribute settings of the route information.

The comparisons of different nodes in a route policy uses a Boolean "OR" statement. The system examines the nodes in the route policy in sequence. Once

the route is permitted by a single node in the route-policy, the route passes the matching test of the route policy without attempting the test of the next node.

ACL

The access control list (ACL) used by the route policy can be divided into three types: advanced ACL, basic ACL and interface ACL.

A basic ACL is usually used for routing information filtering. When the user defines the ACL, the user must define the range of an IP address or subnet for the destination network segment address, or the next-hop address of the routing information. If an advanced ACL is used, perform the matching operation by the specified source address range.

For details of ACL configuration, refer to Chapter 7, Using QoS/ACL Commands.

IP Prefix

The function of the IP Prefix is similar to that of the ACL, but it is more flexible and easier for users to understand. When the IP Prefix is applied to routing information filtering, its matching objects are the destination address information and the domain of the routing information. In addition, in the IP Prefix, you can specify the **gateway** options and require it to receive only the routing information distributed by some certain routers.

An IP Prefix is identified by the ip-prefix name. Each IP Prefix can include multiple list items, and each list item can specify the match range of the network prefix forms, and is identified with an index-number. The index-number designates the matching check sequence in the IP Prefix.

During the matching, the router checks list items identified by the sequence-number in ascending order. Once a single list item meets the condition, it means that it has passed the ip-prefix filtering and does not enter the testing of the next list item.

Configuring an IP Routing Policy

Configuring a routing policy includes tasks described in the following sections:

- [Defining a Route Policy](#)
- [Defining If-match Clauses for a Route-policy](#)
- [Defining Apply Clauses for a Route Policy](#)
- [Importing Routing Information Discovered by Other Routing Protocols](#)
- [Defining IP Prefix](#)

Defining a Route Policy

A route policy can include multiple nodes. Each node is a unit for the matching operation. The nodes are tested against the *node_number*.

Perform the following configurations in System View.

Table 122 Defining a route-policy

Operation	Command
Enter Route Policy View	route-policy <i>route_policy_name</i> { permit deny } node { <i>node_number</i> }
Remove the specified route-policy	undo route-policy <i>route_policy_name</i> [permit deny node <i>node_number</i>]

The **permit** parameter specifies that if a route satisfies all the **if-match** clauses of a node, the route passes the filtering of the node, and the **apply** clauses for the node are executed without taking the test of the next node. If a route does not satisfy all the **if-match** clauses of a node, however, the route takes the test of the next node.

The **deny** parameter specifies that the **apply** clauses are not executed. If a route satisfies all the **if-match** clauses of the node, the node denies the route and the route does not take the test of the next node. If a route does not satisfy all the **if-match** clauses of the node, however, the route takes the test of the next node.

The router tests the route against the nodes in the route policy in sequence, once a node is matched, the route policy filtering will be passed.

By default, the route policy is not defined.



If multiple nodes are defined in a route-policy, at least one of them should be in permit mode. Apply the route policy to filter routing information. If the routing information does not match any node, the routing policy denies the routing information. If all the nodes in the route policy are in deny mode, all routing information is denied by the route policy.

Defining If-match Clauses for a Route-policy

The **if-match** clauses define the matching rules that the routing information must satisfy to pass the route policy. The matching objects are attributes of the routing information.

Perform the following configurations in Route Policy View.

Table 123 Defining if-match Conditions

Operation	Command
Match the destination address of the routing information	if-match { acl <i>acl_number</i> ip-prefix <i>ip_prefix_name</i> }
Cancel the matched destination address of the routing information	undo if-match { acl ip-prefix }
Match the next-hop interface of the routing information	if-match interface { <i>interface_type_</i> <i>interface_number</i> }
Cancel the matched next-hop interface of the routing information	undo if-match interface
Match the next-hop of the routing information	if-match ip next-hop { acl <i>acl_number</i> ip-prefix <i>ip_prefix_name</i> }
Cancel the matched next-hop of the routing information set by ACL	undo if-match ip next-hop

Table 123 Defining if-match Conditions

Operation	Command
Cancel the matched next-hop of the routing information set by the address prefix list	<code>undo if-match ip next-hop ip-prefix</code>
Match the routing cost of the routing information	<code>if-match cost cost</code>
Cancel the matched routing cost of the routing information	<code>undo if-match cost</code>

By default, no matching is performed.



The `if-match` clauses for a node in the route policy require that the route satisfy all the clauses to match the node before the actions specified by the `apply` clauses can be executed.



If no `if-match` clauses are specified, all the routes will pass the filtering on the node.

Defining Apply Clauses for a Route Policy

The `apply` clauses specify actions, which are the configuration commands executed after a route satisfies the filtering conditions that are specified in the `if-match` clauses. In this way, some attributes of the route can be modified.

Perform the following configurations in Route Policy View.

Table 124 Defining Apply Clauses

Operation	Command
Set the routing cost of the routing information	<code>apply cost value</code>
Cancel the routing cost of the routing information	<code>undo apply cost</code>

By default, no apply clauses are defined.

Importing Routing Information Discovered by Other Routing Protocols

A routing protocol can import the routes that are discovered by other routing protocols to enrich its route information. The route policy can filter route information to implement the redistribution. If the destination routing protocol that imports the routes cannot directly reference the route costs of the source routing protocol, you should satisfy the requirement of the destination protocol by specifying a route cost for the imported route.



In different routing protocol views, the parameter options are different. For details, refer to the description of the `import-route` command for each protocol.

Defining IP Prefix

A prefix list is identified by the IP Prefix name. Each IP Prefix can include multiple items, and each item can specify the matching range of the network prefix forms. The `index_number` specifies the matching sequence in the prefix list.

Perform the following configurations in System View.

Table 125 Defining Prefix-list

Operation	Command
Define a Prefix-list	ip ip-prefix <i>ip_prefix_name</i> [index <i>index_number</i>] { permit deny } <i>network len</i> [greater-equal <i>greater_equal</i>] [less-equal <i>less_equal</i>]
Remove a Prefix-list	undo ip ip-prefix <i>ip_prefix_name</i> [index <i>index_number</i> permit deny]

During the matching, the router checks list items identified by the *index_number* in ascending order. If only one list item meets the condition, it means that it has passed the **ip-prefix** filtering (and does not enter the testing of the next list item).

If more than one IP prefix item is defined, then the match mode of at least one list item should be the **permit** mode. The list items of the **deny** mode can be defined to rapidly filter the routing information not satisfying the requirement, but if all the items are in the **deny** mode, no route will pass the **ip-prefix** filtering. You can define an item of **permit** 0.0.0.0/0 **greater-equal** 0 **less-equal** 32 after the multiple list items in the **deny** mode to let all the other routes pass.

Displaying and Debugging the Routing Policy

Enter the **display** command in any view to display the operation of the routing policy configuration, and to verify the effect of the configuration.

Table 126 Displaying and Debugging the Routing Policy

Operation	Command
Display the routing policy	display route-policy [<i>route_policy_name</i>]
Display the address prefix list information	display ip ip-prefix [<i>ip_prefix_name</i>]

Typical IP Routing Policy Configuration Example

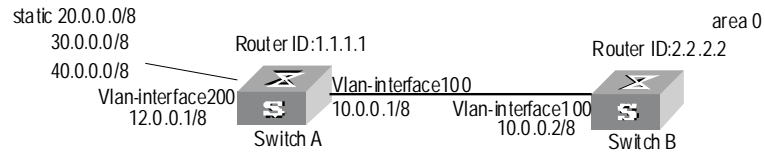
Configuring the Filtering of the Received Routing Information

Networking Requirements

- Switch A communicates with Switch B, running RIP protocol.
- Import three static routes by enabling the RIP protocol on Switch A.
- The route filtering rules can be configured on Switch B to make the received three static routes partially visible and partially shielded. This means that routes in the network segments 20.0.0.0 and 40.0.0.0 are visible while those in the network segment 30.0.0.0 are shielded.

Networking diagram

Figure 34 Filtering the received routing information



Configuration procedure

1 Configure Switch A:

- a** Configure the IP address of VLAN interface.

```
[Switch A]interface vlan-interface 100
[Switch A-Vlan-interface100]ip address 10.0.0.1 255.0.0.0
[Switch A]interface vlan-interface 200
[Switch A-Vlan-interface200]ip address 12.0.0.1 255.0.0.0
```

- b** Configure three static routes.

```
[Switch A]ip route-static 20.0.0.1 255.0.0.0 12.0.0.2
[Switch A]ip route-static 30.0.0.1 255.0.0.0 12.0.0.2
[Switch A]ip route-static 40.0.0.1 255.0.0.0 12.0.0.2
```

- c** Enable RIP protocol and specifies the number of the area to which the interface belongs.

```
[Switch A]router id 1.1.1.1
[Switch A]rip
[Switch A-rip-1]area 0
[Switch A-rip-1-area-0.0.0.0]network 10.0.0.0 0.255.255.255
```

- d** Import the static routes

```
[Switch A-rip-1]import-route static
```

2 Configure Switch B:

- a** Configure the IP address of VLAN interface.

```
[Switch B]interface vlan-interface 100
[Switch B-Vlan-interface100]ip address 10.0.0.2 255.0.0.0
```

- b** Configure the access control list.

```
[Switch B]acl number 2000
[Switch B-acl-basic-2000]rule deny source 30.0.0.0 0.255.255.255
[Switch B-acl-basic-2000]rule permit source any
```

- c** Enable RIP protocol and specifies the number of the area to which the interface belongs.

```
[Switch B]router id 2.2.2.2
[Switch B]rip
[Switch B-rip-1]area 0
[Switch B-rip-1-area-0.0.0.0]network 10.0.0.0 0.255.255.255
```

- d** Configure RIP to filter the external routes received.

```
[Switch B-rip-1]filter-policy 2000 import
```

Troubleshooting Routing Protocols

Routing information filtering cannot be implemented in normal operation of the routing protocol

Check for the following faults:

- The if-match mode of at least one node of the Route Policy should be the **permit** mode. When a Route Policy is used for the routing information filtering, if a piece of routing information does not pass the filtering of any node, then it means that the route information does not pass the filtering of the Route Policy. When all the nodes of the Route Policy are in the **deny** mode, then all the routing information cannot pass the filtering of the Route Policy.
- The if-match mode of at least one list item of the ip-prefix should be the **permit** mode. The list items of the **deny** mode can be firstly defined to rapidly filter the routing information not satisfying the requirement, but if all the items are in the deny mode, no routes will not pass the **ip-prefix** filtering. You can define an item of **permit 0.0.0.0/0 less-equal 32** after the multiple list items in the **deny** mode so as to let all the other routes pass the filtering (If **less-equal 32** is not specified, only the default route will be matched).

7

ACL CONFIGURATION

This chapter covers the following topics:

- [Brief Introduction to ACL](#)
- [QoS Configuration](#)
- [ACL Control Configuration](#)

Brief Introduction to ACL

A series of matching rules are required for the network devices to identify the packets to be filtered. After identifying the packets, the Switch can permit or deny them to pass through according to the defined policy. Access Control List (ACL) is used to implement such functions.

ACL classifies the data packets with a series of matching rules, including source address, destination address and port number, and so on. The Switch verifies the data packets with the rules in ACL and determines to forward or discard them.

The data packet matching rules defined by ACL can also be called in some other cases requiring traffic classification, such as defining traffic classification for QoS.

An access control rule includes several statements. Different statements specify different ranges of packets. When matching a data packet with the access control rule, the issue of match order arises.

Filtering or Classifying Data Transmitted by the Hardware

ACL can be used to filter or classify the data transmitted by the hardware of the Switch. In this case, the match order of the ACL's sub-rules is determined by the Switch hardware. The match order defined by the user will not be effective.

The case includes: ACL cited by QoS function, ACL used for filter the packet transmitted by the hardware and so on.

Filtering or Classifying Data Transmitted by the Software

ACL can be used to filter or classify the data treated by the software of the Switch. In this case, the match order of ACL's sub-rules can be determined by the user. There are two match-orders: **config** (by following the user-defined configuration order when matching the rule) and **auto** (according to the system sorting automatically when matching the rule, that is, in depth-first order). Once the user specifies the match-order of an access control rule, it cannot be modified later, unless all the content is deleted and the match-order specified again.

The case includes: ACL cited by route policy function, ACL used for control logon user, and so on.



The depth-first principle is to put the statement specifying the smallest range of packets on the top of the list. This can be implemented through comparing the wildcards of the addresses. The smaller the wildcard is, the less hosts it can specify. For example, 129.102.1.1 0.0.0.0 specifies a host, while 129.102.1.1 0.0.255.255 specifies a network segment, 129.102.0.1 through 129.102.255.255. Obviously, the former one is listed ahead in the access control list.

The specific standard is as follows.

For basic access control list statements, compare the source address wildcards directly. If the wildcards are the same, follow the configuration sequence.

For the advanced access control list, compare the source address wildcards first. If they are the same, then compare the destination address wildcards. For the same destination address wildcards, compare the ranges of port numbers, the one with the smaller range is listed ahead. If the port numbers are in the same range, follow the configuration sequence.

ACL Supported by the Switch

The table below lists the limits to the numbers of different types of ACL on a Switch.

Table 127 Quantitative Limitation to the ACL

Item	Value range
Numbered basic ACL.	2000 to 2999
Numbered advanced ACL.	3000 to 3999
Numbered Layer-2 ACL.	4000 to 4999
Numbered user-defined ACL.	5000 to 5999
The sub items of an ACL	0 to 65534

Configuring ACL

ACL configuration includes:

- [Defining ACL](#)
- [Activating ACL](#)

The above steps must be done in sequence. Define the ACL (using the defined time range in the definition), then activate the ACL to validate it.

Defining ACL

The Switch 4500 supports several types of ACL. This section introduces how to define these ACLs.

Defining ACL by following the steps below:

- 1 Enter the corresponding ACL view.
- 2 Add a rule to the ACL.

You can add multiple rules to one ACL.



- If a specific time range is not defined, the ACL will always function after activated.
- During the process of defining the ACL, you can use the rule command several times to define multiple rules for an ACL.

- If ACL is used to filter or classify the data transmitted by the hardware of the Switch, the match order defined in the `acl` command will not be effective. If ACL is used to filter or classify the data treated by the software of the Switch, the match order of ACL's sub-rules will be effective. Once the user specifies the match-order of an ACL rule, he cannot modify it later.
- The default matching-order of ACL is `config`, that is, following the order as that configured by the user.

Define Basic ACL

The rules of the basic ACL are defined on the basis of the Layer-3 source IP address to analyze the data packets.

You can use the following command to define basic ACL.

Perform the following configuration in the corresponding view.

Table 128 Define Basic ACL

Operation	Command
Enter basic ACL view (from System View)	<code>acl number acl_number [match-order { config auto }]</code>
add a sub-item to the ACL (from Basic ACL View)	<code>rule [rule_id] { permit deny } [source { source_addr wildcard any } fragment]*</code>
delete a sub-item from the ACL (from Basic ACL View)	<code>undo rule rule_id [source fragment]*</code>
Delete one ACL or all the ACL (from System View)	<code>undo acl { number acl_number all }</code>

Define Advanced ACL

The rules of the classification for advanced ACL are defined on the basis of the attributes such as source and destination IP address, the TCP or UDP port number in use and packet priority to process the data packets. The advanced ACL supports the analysis of three types of packet priorities, ToS (Type of Service), IP and DSCP priorities.

You can use the following command to define advanced ACL.

Perform the following configuration in the corresponding view.

Table 129 Define Advanced ACL

Operation	Command
Enter advanced ACL view (from System View)	<code>acl number acl_number [match-order { config auto }]</code>
Add a sub-item to the ACL (from Advanced ACL View)	<code>rule [rule_id] { permit deny } protocol [source { source_addr wildcard any }] [destination { dest_addr wildcard any }] [source-port operator port1 [port2]] [destination-port operator port1 [port2]] [icmp-type type code] [established] [[{ precedence precedence tos tos dscp dscp vpn-instance instance }] fragment]*</code>

Operation	Command
Delete a sub-item from the ACL (from Advanced ACL View)	undo rule <i>rule_id</i> [source destination source-port destination-port icmp-type precedence tos dscp fragment vpn-instance]*
Delete one ACL or all the ACL (from System View)	undo acl { number <i>acl_number</i> all }

Note that, the *port1* and *port2* in the above command specify the TCP or UDP ports used by various high-layer applications. For some common port numbers, you can use the mnemonic symbols as a shortcut. For example, “bgp” can represent the TCP number 179 used by BGP.

Define Layer-2 ACL

The rules of Layer-2 ACL are defined on the basis of the Layer-2 information such as source MAC address, source VLAN ID, Layer-2 protocol type, Layer-2 packet format and destination MAC address.

You can use the following command to define the numbered Layer-2 ACL.

Perform the following configuration in corresponding view.

Table 130 Define Layer-2 ACL

Operation	Command
Enter Layer-2 ACL view (from System View)	acl number <i>acl_number</i> [match-order { config auto }
Add a sub-item to the ACL (from Layer-2 ACL View)	rule [<i>rule_id</i>] { permit deny } [[type <i>protocol_type</i> <i>type_mask</i> lsap <i>lsap_type</i> <i>type_mask</i>] format_type cos <i>cos</i> source { <i>source_vlan_id</i> <i>source_mac_addr</i> <i>source_mac_wildcard</i> }* dest { <i>dest_mac_addr</i> <i>dest_mac_wildcard</i> }]*
Delete a sub-item from the ACL (from Layer-2 ACL View)	undo rule <i>rule_id</i>
Delete one ACL or all the ACL (from System View)	undo acl { number <i>acl_number</i> all }

Defining the User-defined ACL

The user-defined ACL matches any bytes in the first 80 bytes of the Layer-2 data frame with the character string defined by the user and then processes them accordingly. To correctly use the user-defined ACL, you are required to understand the Layer-2 data frame structure.



Any packet ending up at the FFP (Fast Filter Processor), that performs ACL functionality, will contain a VLAN tag. Even packets that ingress the Switch untagged will be tagged at the FFP.

You can use the following ACL commands to define user-defined ACL.

Perform the following configuration in corresponding view.

Table 131 Defining the User-defined ACL

Operation	Command
Enter user-defined ACL view (from System View)	acl number <i>acl_number</i> [match-order { config auto }]
Add a sub-item to the ACL (from User-defined ACL View)	rule [<i>rule_id</i>] { permit deny } { <i>rule_string</i> <i>rule_mask</i> <i>offset</i> }<1-8>]
Delete a sub-item from the ACL (from User-defined ACL View)	undo rule <i>rule_id</i>
Delete one ACL or all the ACL (from System View)	undo acl { number <i>acl_number</i> all }

rule-string is a character string defined by a user. It is made up of a hexadecimal character string with even digits of characters. *rule-mask offset* is used to extract the packet information. Here, *rule-mask* is rule mask, used for logical AND operation with bytes from the data packets and corresponding bytes from the rule-mask and offset determines the start location of the rule-mask in the packet. *rule-mask offset* extracts a character string from the packet and compares it with the user-defined rule-string to identify and process the matched packets.

Activating ACL

The defined ACL can be active after being activated globally on the Switch. This function is used to activate the ACL filtering or classify the data transmitted by the hardware of the Switch.

You can use the following command to activate the defined ACL.

Perform the following configuration in Ethernet Port View.

Table 132 Activate ACL

Operation	Command
Activate an ACL	packet-filter { inbound outbound } { user-group <i>acl_number</i> [rule <i>rule</i>] ip-group <i>acl_number</i> [rule <i>rule</i> [link-group <i>acl_number</i> rule <i>rule</i>]] link-group <i>acl_number</i> [rule <i>rule</i>] }
Deactivate an ACL	undo packet-filter { inbound outbound } { user-group <i>acl_number</i> [rule <i>rule</i>] ip-group <i>acl_number</i> [rule <i>rule</i> [link-group <i>acl_number</i> rule <i>rule</i>]] link-group <i>acl_number</i> [rule <i>rule</i>] }

Displaying and Debugging ACL

After the above configuration, execute **display** command in all views to display the running of the ACL configuration, and to verify the effect of the configuration. Execute **reset** command in User View to clear the statistics of the ACL module.

Table 133 Display and Debug ACL

Operation	Command
Display the detail information about the ACL	display acl { all <i>acl_number</i> }
Display the information about the ACL running state	display packet-filter { interface { <i>interface_name</i> <i>interface_type</i> <i>interface_num</i> } unitid <i>unit_id</i> }
Clear ACL counters	reset acl counter { all <i>acl_number</i> }

The matched information of `display acl` command specifies the rules treated by the Switch's CPU.

For syntax description, refer to the *Command Reference Guide*.

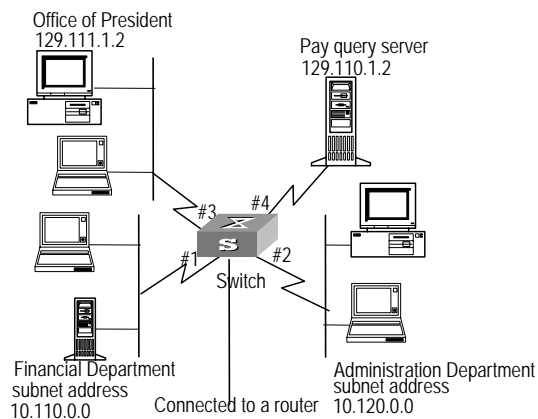
Advanced ACL Configuration Example

Networking Requirements

The interconnection between different departments on a company network is implemented through the 1000 Mbps ports of the Switch. The Subnet IP address of the Financial Dept. is 129.110.0.0, the IP address of the pay query server is 129.112.1.2. The Financial Dept is accessed via GigabitEthernet1/0/50. It is required to properly configure the ACL and limit Financial Dept access to the payment query server between 8:00 and 18:00.

Networking Diagram

Figure 35 Access Control Configuration Example



Configuration Procedure



In the following configurations, only the commands related to ACL configurations are listed.

1 Define the work time range

Define time range from 8:00 to 18:00.

```
[4500]time-range 3Com 8:00 to 18:00 working-day
```

2 Define the ACL to access the payment server.

a Enter the numbered advanced ACL, number as 3000.

```
[4500]acl number 3000 match-order config
```

b Define the rules for other department to access the payment server.

```
[4500-acl-adv-3000]rule 1 deny ip source 129.110.1.2 0.0.255.255
destination 129.112.1.2 time-range 3Com
```

c Define the rules for the President's Office to access the payment server.

```
[4500-acl-adv-3000]rule 2 permit ip source 129.111.1.2 0.0.0.0
destination 129.110.1.2 0.0.0.0
```

3 Activate ACL.

Activate the ACL 3000.

```
[4500-GigabitEthernet1/0/50]packet-filter inbound ip-group 3000 rule 1
```

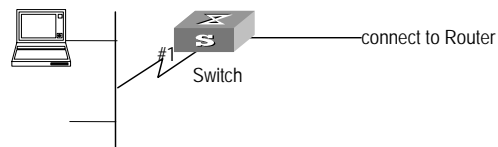
Basic ACL Configuration Example

Networking Requirements

Using basic ACL, filter the packet whose source IP address is 10.1.1.1 during the time range 8:00 ~ 18:00 every day. The host connects port GigabitEthernet1/0/50 of the Switch.

Networking Diagram

Figure 36 Access Control Configuration Example



Configuration Procedure



In the following configurations, only the commands related to ACL configurations are listed.

1 Define the time range

Define time range from 8:00 to 18:00.

```
[4500]time-range 3Com 8:00 to 18:00 daily
```

2 Define the ACL for packet which source IP is 10.1.1.1.

a Enter the number basic ACL, number as 2000.

```
[4500]acl number 2000
```

b Define the rules for packet which source IP is 10.1.1.1.

```
[4500-acl-basic-2000]rule 1 deny source 10.1.1.1 0 time-range 3Com
```

3 Activate ACL.

Activate the ACL 2000.

```
[4500-GigabitEthernet1/0/50]packet-filter inbound ip-group 2000
```

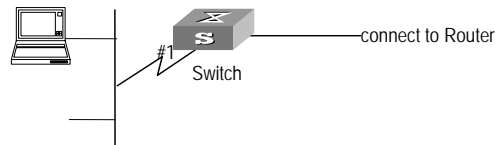
Link ACL Configuration Example

Networking Requirements

Using Link ACL, filter the packet whose source MAC address is 00e0-fc01-0101 and destination MAC address is 00e0-fc01-0303 during the time range 8:00 ~ 18:00 every day. The ACL is activated on GigabitEthernet1/0/50.

Networking Diagram

Figure 37 Access Control Configuration Example



Configuration Procedure



In the following configurations, only the commands related to ACL configurations are listed.

1 Define the time range

Define time range from 8:00 to 18:00.

```
[4500]time-range 3Com 8:00 to 18:00 daily
```

2 Define the ACL for the packet whose source MAC address is 00e0-fc01-0101 and destination MAC address is 00e0-fc01-0303.

a Enter the numbered link ACL, number as 4000.

```
[4500]acl number 4000
```

b Define the rules for the packet whose source MAC address is 00e0-fc01-0101 and destination MAC address is 00e0-fc01-0303.

```
[4500-acl-ethernetframe-4000]rule 1 deny source 00e0-fc01-0101
ffff-ffff-ffff 00e0-fc01-0303 ffff-ffff-ffff time-range 3Com
```

3 Activate ACL.

Activate the ACL 4000 .

```
[4500-GigabitEthernet1/0/50]packet-filter inbound link-group 4000
```

QoS Configuration

Traffic

Traffic refers to all packets passing through a Switch.

Traffic Classification

Traffic classification means identifying the packets with certain characteristics, using the matching rule called classification rule, set by the configuration administrator based on the actual requirements. The rule can be very simple. For example, the traffic with different priorities can be identified according to the ToS field in IP packet header. There are also some complex rules. For example, the information over the integrated link layer (Layer-2), network layer (Layer-3) and transport layer (Layer-4), such as MAC address, IP protocol, source IP address, destination IP address and the port number of application etc can be used for traffic classification. Generally the classification standards are encapsulated in the header of the packets. The packet content is seldom used as the classification standard.

Packet Filter

Packet filter is used to filter traffic. For example, the operation “deny” discards the traffic that is matched with a traffic classification rule, while allowing other traffic to pass through. With the complex traffic classification rules, the Switch enables the filtering of various information carried in Layer 2 traffic to discard the useless, unreliable or doubtful traffic, thereby enhancing network security.

The two key steps of realizing the frame filtering are as follows.

- 1 Classify the ingress traffic according to the classification rule;
- 2 Filter the classified traffic, that is, the “deny” operation, the default ACL operation.

Traffic Policing

To deliver better service with the limited network resources, QoS monitors the traffic of the specific user on the ingress, so that it can make a better use of the assigned resource.

Port Traffic Limit

The port traffic limit is the port-based traffic limit used for limiting the general speed of packet output on the port.

Traffic Priority

The Ethernet Switch can deliver priority tag service for some special packets. The tags include TOS, DSCP and 802.1p, etc., which can be used and defined in different QoS modules.

Queue Scheduling

When congestion occurs, several packets will compete for the resources. The queue scheduling algorithm is used to overcome the problem.

Weighted Round Robin (WRR)

Round scheduling ensures every queue is given some service time on the Switch port. Take 4 egress queues for each port as an example, WRR gives each queue a weight (w_3 , w_2 , w_1 , and w_0 respectively) for obtain resource. For example, you can configure the weight value of the WRR algorithm for 100M port as 50, 30, 10, 10 (corresponding to the w_3 , w_2 , w_1 and w_0 respectively). Therefore, the low-priority queue can be guaranteed to get the minimum bandwidth of 10Mbps, avoiding the case in SP scheduling that the messages in the lower-priority queues may not get any service for some time. Another advantage of the WRR queue is that the service time is assigned to each queue flexibly, although it is the round multiple queue scheduling. When a queue is empty, it will switch to the next queue immediately, thereby making good use of the bandwidth resource.

Traffic Mirroring

The traffic mirroring function is carried out by copying the specified data packets to the monitoring port for network diagnosis and troubleshooting.

Traffic Counting

With the flow-based traffic counting, you can request a traffic count to count and analyze the packets.

QoS Configuration The process of traffic based QoS:

- 1 Identify the traffic by ACL
- 2 Perform the QoS operation to the traffic.

The configuration steps of traffic based QoS:

- 1 Define the ACL
- 2 Configure the QoS operation

If QoS is not based on traffic, you need not define ACL first.

See [“Configuring ACL”](#) for information on how to define ACL. This section mainly describes how to configure QoS operation.

Setting Port Priority You can use the following command to set the port priority. The Switch will replace the 802.1p priority carried by a packet with the port priority by default.

Perform the following configuration in Ethernet Port View.

Table 134 Setting Port Priority

Operation	Command
Set the port priority	priority <i>priority_level</i>
Restore the default port priority	undo priority

The Switch port supports 8 priority levels. You can configure the port priority to your requirements.

priority-level ranges from 0 to 7.

By default, the Switch replaces the priority carried by a packet with the port priority.

Configuring Trust Packet Priority The system replaces the 802.1p priority carried by a packet with the port priority by default. The user can configure system trusting the packet 802.1p priority and not replacing the 802.1p priorities carried by the packets with the port priority.

Perform the following configuration in Ethernet Port View.

Table 135 Configuring Port Priority Replacement

Operation	Command
Configure trust packet 802.1p priority	priority trust
Configure not trust packet 802.1p priority	undo priority

Before configuring trust packet 802.1p priority, the Switch puts the packets into different queues according to the priorities of the received port. After configuring trust packet 802.1p priority, the Switch will trust the packet 802.1p priority and put the packet into different queues accordingly, when forwarding the packets.

By default, the system replaces the 802.1p priority carried by a packet with the port priority.

Setting Port Mirroring Port mirroring means duplicating data on the monitored port to the designated mirror port, for purpose of data analysis and supervision.

The Switch supports one monitor port and multiple mirroring ports. If several Switches form a Fabric, multiple mirroring ports and only one monitor port and one mirroring port can be configured in the Fabric.

Configure Port Mirroring

1 Configure monitor port

Perform the following configuration in the Ethernet Port View.

Table 136 Configure Monitor Port

Operation	Command
Configure a monitor port	monitor-port

Only one monitor port can be configured on one Switch. If a group of Switches form a fabric, only one monitor port can be configured on one fabric.

2 Configure the mirroring port.

Perform the following configuration in the Ethernet Port View.

Table 137 Configure Mirroring Port

Operation	Command
Configure mirroring port	mirroring-port { inbound outbound both }

Delete Port Mirroring

1 Delete mirroring port

Perform the following configuration in the Ethernet Port View.

Table 138 Delete Mirroring Port

Operation	Command
Delete a mirroring port	undo mirroring-port { inbound outbound both }

2 Delete monitor port.

Perform the following configuration in the Ethernet Port View.

Table 139 Delete Monitor Port

Operation	Command
Delete monitor port	undo monitor

Configuring Traffic Mirroring

The function of traffic mirroring is to copy the traffic matching an ACL rule to the designated observing port to analyze and monitor the packets.

Configure Traffic Mirroring

1 Configure monitor port

Perform the following configuration in the Ethernet Port View.

Table 140 Configure Monitor Port

Operation	Command
Configure a monitor port.	monitor-port

Only one monitor port can be configured on one Switch. If a group of Switches form a Fabric, only one monitor port can be configured on one Fabric.

2 Configure traffic mirroring

Perform the following configuration in the Ethernet Port View.

Table 141 Configuring Traffic Mirroring

Operation	Command
Configure traffic mirroring	<code>mirrored-to { inbound outbound } { user-group acl_number [rule rule] ip-group acl_number [rule rule [link-group acl_number rule rule]] link-group acl_number [rule rule] } { cpu monitor-interface }</code>

Delete Traffic Mirroring

1 Delete traffic mirroring

Perform the following configuration in the Ethernet Port View.

Table 142 Delete Traffic Mirroring

Operation	Command
Cancel the configuration of traffic mirroring	<code>undo mirrored-to { inbound outbound } { user-group acl_number [rule rule] ip-group acl_number acl_name } [rule rule] link-group acl_number rule rule] }</code>

2 Delete monitor port.

Perform the following configuration in the Ethernet Port View.

Table 143 Delete Monitor Port

Operation	Command
Delete monitor port	<code>undo monitor</code>

For details about the command, refer to the *Command Reference Guide*.

Configuring the Mapping Relationship Between COS and Local Precedence

The default mapping relationship between 802.1p priority and output queue of the port is as follows:

Table 144 Mapping between 802.1p Priority Levels and Outbound Queues

802.1p priority level	Queues
0	2
1	0
2	1
3	3
4	4
5	5
6	6
7	7

Perform the following configuration in System View.

Table 145 Map Configuration

Operation	Command
Configure "COS ->Local-precedence" map	qos cos-local-precedence-map <i>cos0_map_local_prec</i> <i>cos1_map_local_prec</i> <i>cos2_map_local_prec</i> <i>cos3_map_local_prec</i> <i>cos4_map_local_prec</i> <i>cos5_map_local_prec</i> <i>cos6_map_local_prec</i> <i>cos7_map_local_prec</i>
Restore its default value	undo qos cos-local-precedence-map

By default, the Switch uses the default mapping relationship.

Setting Traffic Limit

Traffic limit refers to rate limit based on traffic. If the traffic threshold is exceeded, corresponding measures will be taken, for example, dropping the excessive packets or re-defining their priority levels.

Perform the following configurations in the Ethernet Port View.

Table 146 Setting Traffic Limit

Operation	Command
Set traffic limit	traffic-limit inbound { user-group <i>acl_number</i> [rule <i>rule</i>] ip-group <i>acl_number</i> [rule <i>rule</i> [link-group <i>acl_number</i> rule <i>rule</i>]] link-group <i>acl_number</i> [rule <i>rule</i>] } target_rate [exceed <i>action</i>]
Remove traffic limit	undo traffic-limit inbound { user-group <i>acl_number</i> [rule <i>rule</i>] ip-group <i>acl_number</i> [rule <i>rule</i> [link-group <i>acl_number</i> rule <i>rule</i>]] link-group <i>acl_number</i> [rule <i>rule</i>] }

You should first define an ACL before this configuration task.

The granularity of traffic limit is 64kbps. If the *target-rate* user input is in (N*64, (N+1)*64], in which N is a natural number, Switch automatically sets (N+1)*64 as the parameter value.

This configuration achieves rate control for those packets that match the ACL. If the traffic rate threshold is exceeded, corresponding measures will be taken, for example, dropping excessive packets.

Setting Line Limit

Line limit refers to rate limit based on the port, that is, limiting the total rate at the port. The granularity of line rate is 64 kbps.

Perform the following configurations in the Ethernet Port View.

Table 147 Setting Line Rate

Operation	Command
Set line limit	line-rate { inbound outbound } <i>target_rate</i>
Remove line limit	undo line-rate { inbound outbound }

Configuring WRED Operation

The function of WRED Operation is to avoid congestion in advance.

Perform the following configuration in the Ethernet Port View.

Table 148 Configuring WRED Operation

Operation	Command
Configure WRED Operation	wred <i>queue_index</i> <i>qstart</i> <i>probability</i>
Cancel the configuration of WRED Operation	undo wred <i>queue_index</i>

For details about the command, refer to the *Command Reference Guide*.

Displaying and Debugging QoS Configuration

You can use the **display** command in any view to see the QoS operation and to check the status of the configuration. You can also clear the statistic information using the **reset** command in the Ethernet Interface View.

Table 149 Displaying and Debugging QoS Configuration

Operation	Command
Display mirroring configuration	display mirror
Display queue scheduling mode	display queue-scheduler
Display line rate for outbound packets	display qos-interface { <i>interface_name</i> <i>interface_type</i> <i>interface_num</i> <i>unit_id</i> } line-rate
Display port QoS configuration	display qos-interface { <i>interface_name</i> <i>interface_type</i> <i>interface_num</i> <i>unit_id</i> } all
Display traffic limit	display qos-interface { <i>interface_name</i> <i>interface_type</i> <i>interface_num</i> <i>unit_id</i> } traffic-limit
Display the settings of the traffic mirror	display qos-interface { <i>interface_name</i> <i>interface_type</i> <i>interface_num</i> <i>unit_id</i> } mirrored-to

QoS Configuration Example

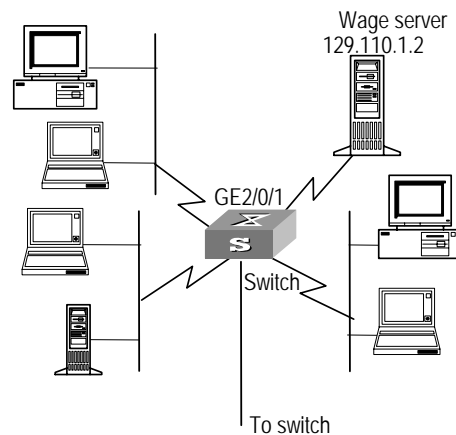
Traffic Limit and Line Rate Configuration Example

Networking Requirement

The intranet is connected through 1000 Mbps ports between departments and the wage server is connected through the port Ethernet1/0/1 (subnet address 129.110.1.2). For the wage server, the inbound traffic is limited at 128 kbps and the inbound port rate at 128 kbps. Those packets exceeding the threshold will be labeled with dscp priority level 4.

Networking Diagram

Figure 38 QoS Configuration Example



Configuration Procedure



Only the commands concerning QoS/ACL configuration are listed here.

- 1 Define outbound traffic for the wage server.
 - a Enter numbered advanced ACL view.


```
[4500]acl number 3000
```
 - b Define the traffic-of-pay server rule in the advanced ACL 3000.


```
[4500-acl-adv-3000]rule 1 permit ip source 129.110.1.2 0.0.0.0
destination any
```
- 2 Set traffic limit for the wage server.
 - a Limit average traffic from the wage server at 128 Kbps and label over-threshold packets with priority level 4.


```
[4500-Ethernet1/0/1]traffic-limit inbound ip-group 3000 128 exceed
remark-dscp 4
```
 - b Limit traffic to the wage server from the port Ethernet1/0/1 at 128 Kbps.


```
[4500-Ethernet1/0/1]line-rate outbound 128
```

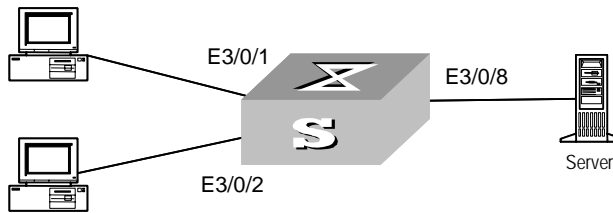
Port Mirroring Configuration Example

Networking Requirement

Use one server to monitor the packets of two PCs. One PC is accessed from the port E1/0/1 and the other from the port E1/0/2. The server is connected to the port E3/0/8. Require monitor the traffic of E3/0/1.

Networking Diagram

Figure 39 QoS Configuration Example



Configuration Procedure

Define port mirroring, with monitoring port being Ethernet3/0/8.

```
[ 4500-Ethernet3/0/8 ]monitor-port
[ 4500-Ethernet3/0/1 ]mirroring-port both
```

ACL Control Configuration

The Switch provides three modes for users to access devices remotely:

- TELNET access
- Security shell (SSH) access
- Simple network management protocol (SNMP) access

The Switch provides security control features and controls the three access modes, consequently preventing illegal users from logging into and accessing switches. Security control can be divided into the following two levels:

- Level 1 – User connection control. Configured access control list (ACL) filters login users so that only legal users can be connected to the switch.
- Level 2: User password authentication. Before logging into the switch, the users connected to the switch must pass the password authentication.

This chapter describes how to configure level 1 security control, that is how to configure ACLs for login users. For the level 2 security configuration, refer to [“User Interface Configuration”](#).

TELNET/SSH User ACL Configuration

Before login users perform password authentication, the ACLs configured for TELNET or SSH users filter some malicious or illegal connection request, consequently assuring device security.

Configuration Prerequisites

You have correctly configured to log into switches in the TELNET or SSH mode.

Configuration Tasks

[Table 150](#) lists the commands that you can execute to configure TELNET or SSH user ACL.

Table 150 Commands for Configuring TELNET/SSH User ACL

To	In This View	Type This Command	Description
Enter system view		system-view	
Define ACLs and enter ACL view		acl number acl-number [match-order { config auto }]	Required. You can only define number-based ACLs here.
Define rules	Basic ACL view	rule [rule-id] { permit deny } [source { source-addr wildcard any } fragment {source [source-addr wildcard any]}]	When TELNET and SSH users use basic and advanced ACLs, only the source IP and the corresponding mask, the destination IP and the corresponding mask, and the time-range keyword in the rule parameters take effect.
Define rules	Advanced ACL view	r rule rule-id { permit deny } protocol [source { source-addr wildcard any }] [destination { dest-addr wildcard any }] [icmp-type type code] [precedence precedence] [tos tos] [dscp dscp] [fragment]	When TELNET and SSH users use basic and advanced ACLs, only the source IP and the corresponding mask, the destination IP and the corresponding mask, and the time-range keyword in the rule parameters take effect.
Quit ACL view		quit	
Enter user interface view		user-interface [type] first-number	
Use ACLs, and restrict incoming/outgoing calls for TELNET or SSH users	Basic or advanced ACLs	acl acl-number1 { inbound outbound }	The acl-number1 parameter indicates basic or advanced ACL number, in the range of 2,000 to 3,999.
	Use L2 ACLs	acl acl-number2 inbound	The acl-number2 parameter indicates the L2 ACL number, in the range of 4,000 to 4,999.

By default, the incoming/outgoing calls are not restricted on the user interface.



- You can only use number-based ACLs for TELNET or SSH user ACL control.
- When TELNET or SSH users use basic or advanced ACLs, the incoming/outgoing calls are restricted on the basis of the source or destination IP address. As a result, when you use the rules for basic and advanced ACLs, only the source IP and the corresponding mask, the destination IP and the corresponding mask, and the time-range keyword take effect. When TELNET and SSH users use L2

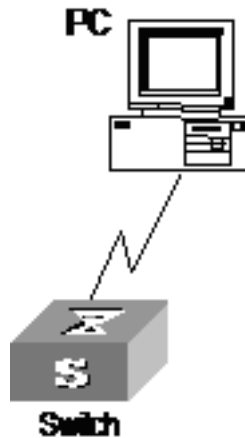
ACLs, the incoming/outgoing calls are restricted on the basis of source MAC addresses. As a result, when you use the rules for L2 ACLs, only the source MAC and the corresponding mask, and the time-range keyword take effect.

- When you control telnet and SSH users on the basis of L2 ACLs, only the incoming calls are restricted.
- If a user is refused to log in due to ACL restriction, the system will record the log information about an access failure. The log information includes the user IP address, login mode, index value for a login user interface and reason for login failure.

L2 ACL Configuration Example

Configuration Prerequisites Only the TELNET users with 00e0-fc01-0101 and 00e0-fc01-0303 source MAC addresses are allowed to access switches.

Figure 40 Source MAC Control Over TELNET User Accessing Switch



Configuration Steps

Define L2 ACLs.

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500] acl number 4000 match-order config
```

Define rules.

```
[4500-acl-link-4000] rule 1 permit ingress 00e0-fc01-0101
0000-0000-0000 [4500-acl-link-4000] rule 2 permit ingress
00e0-fc01-0303 0000-0000-0000
```

```
[4500-acl-link-4000] rule 3 deny ingress any
```

```
[4500-acl-link-4000] quit
```

Enter the user interface view.

```
[4500] user-interface vty 0 4
```

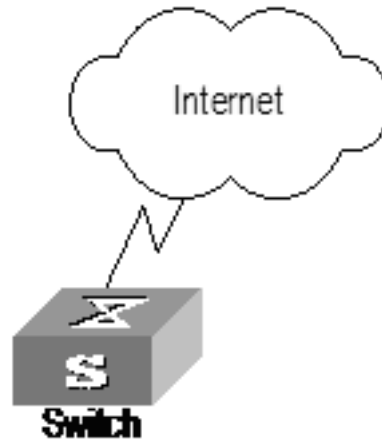
Use L2 ACLs, and restrict incoming calls of the user interface.

```
[4500-user-interface-vty0-4] acl 4000 inbound
```

Basic ACL Configuration Example

Configuration Prerequisites Only the TELNET users, whose IP addresses are 10.110.100.52 and 10.110.100.46, are allowed to access switches.

Figure 41 Source IP Control Over TELNET User Accessing Switch



Configuration Steps

Define basic ACLs.

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500] acl number 2000 match-order config
```

Define rules.

```
[4500-acl-basic-2000] rule 1 permit source 10.110.100.52 0
[4500-acl-basic-2000] rule 2 permit source 10.110.100.46 0
[4500-acl-basic-2000] rule 3 deny source any
[4500-acl-basic-2000] quit
```

Enter the user interface view.

```
[4500] user-interface vty 0 4
```

Use ACLs.

```
[4500-user-interface-vty0-4] acl 2000 inbound
```

ACL Control Over Users Accessing Switches by SNMP

The Switch supports remote management through network management software. Network management users can access switches by simple network management protocol (SNMP). The ACL control over these users can filter illegal network management users so that the illegal users cannot log into this Switch.

Configuration Prerequisites

Users have correctly configured to log into switches by SNMP.

Configuration Tasks

[Table 151](#) lists the commands that you can execute to configure SNMP user ACL.

Table 151 Commands for Controlling ACL Access via SNMP

To	Type This Command	Description
Enter system view	<code>system-view</code>	
Define ACLs and enter ACL view	<code>acl number acl-number [match-order { config auto }]</code>	Required. You can only define number-based ACLs here. The acl-number parameter ranges from 2,000 to 2,999.
Define rules for basic ACLs	<code>rule [rule-id] {permit deny } [source { source-addr wildcard any } fragment [source { source-addr wildcard any }]]</code>	Required
Quit ACL view	<code>quit</code>	

Table 151 Commands for Controlling ACL Access via SNMP

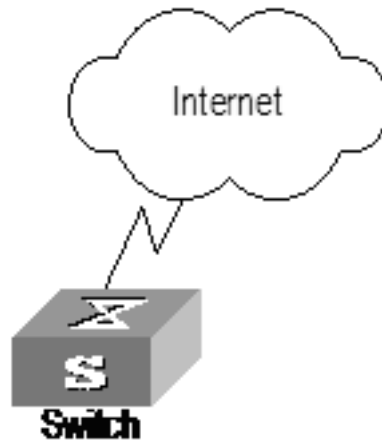
To	Type	This Command	Description
Use ACLs, and control users accessing switches by SNMP	Use ACLs when configuring the SNMP community name commands	<code>snmp-agent community { read write } community-name [[mib-view view-name] [acl acl-number]]</code>	SNMP community name is a feature of SNMP V1 and SNMP V2 versions. Using ACLs can filter network management system of SNMP V1 and SNMP V2 versions when you configure the SNMP community name command.
	Use ACLs when you configure the SNMP group name command	<code>snmp-agent group { v1 v2c } group-name [read-view read-view] [write-view write-view] [notify-view notify-view] [acl acl-number]</code> <code>snmp-agent group v3 group-name [authentication privacy] [read-view read-view] [write-view write-view] [notify-view notify-view] [acl acl-number]</code> <code>snmp-agent usm-user { v1 v2c } user-name group-name [acl acl-number]</code> <code>snmp-agent usm-user v3 user-name group-name [authentication-mode { md5 sha } auth-password] [privacy-mode des56 priv-password] [acl acl-number]</code>	The SNMP group and user names are a feature of SNMP V2 version or later. Using ACLs can filter the network management system of SNMP V2 version or later when you configure the commands for the SNMP group and user names. If you simultaneously configure ACL control function for the two commands, the switch will filter the two attributes for the network management user.



- *The `snmp-agent community`, `snmp-agent group` and `snmp-agent usm-use` commands can use different ACLs.*
- *You can only use number-based basic ACLs for ACL control over network management users.*

Configuration Example

Network Requirements Only the SNMP users with the IP address 10.110.100.52 and 10.110.100.46 are allowed to access switches.

Figure 42 ACL Control Over SNMP Users of the Switch**Configuration Steps**

Define basic ACLs and rules.

```
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500] acl number 2000 match-order config
[4500-acl-basic-2000] rule 1 permit source 10.110.100.52 0
[4500-acl-basic-2000] rule 2 permit source 10.110.100.46 0
[4500-acl-basic-2000] rule 3 deny source any
[4500-acl-basic-2000] quit
```

Use ACLs.

```
[4500] snmp-agent community read huawei acl 2000
[4500] snmp-agent group v3 huaweigroup acl 2000
[4500] snmp-agent usm-user v3 huaweiuser huaweigroup acl 2000
```

Configuring ACL Control for HTTP Users

The Switch 4500 Family supports the remote management through the Web interface. The users can access the Switch through HTTP. Controlling such users with ACL can help filter the illegal users and prevent them from accessing the local Switch. After configuring ACL control over these users, the Switch allows only one Web user to access the Ethernet Switch at one time.

Take the following steps to control the HTTP users with ACL.

- 1 Defining ACL
- 2 Calling ACL to control HTTP users

The follow section introduces the configuration procedures.

Defining ACL

You can only call the numbered basic ACL, ranging from 2000 to 2999, to implement ACL control function. Use the same configuration commands introduced in the last section.

Calling ACL to Control HTTP Users

To control the Web network management users with ACL, call the defined ACL.

You can use the following commands to call an ACL.

Perform the following configuration in System View.

Table 152 Calling ACL to Control HTTP Users

Operation	Command
Call an ACL to control the WEB NM users.	<code>ip http acl acl_number</code>
Cancel the ACL control function.	<code>undo ip http acl</code>

For more information about the commands, refer to the *Command Reference Guide*.



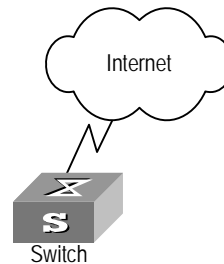
Only the numbered basic ACL can be called for WEB NM user control.

Configuration Example

Networking Requirements Only permit Web NM user from 10.110.100.46 access Switch.

Networking Diagram

Figure 43 Controlling Web NM users with ACL



Configuration Procedure

- 1 Define the basic ACL.

```
[4500]acl number 2030 match-order config
[4500-acl-basic-2030]rule 1 permit source 10.110.100.46 0
[4500-acl-basic-2030]rule 2 deny source any
[4500-acl-basic-2030]quit
```

- 2 Call the basic ACL.

```
[4500]ip http acl 2030
```


8

IGMP SNOOPING

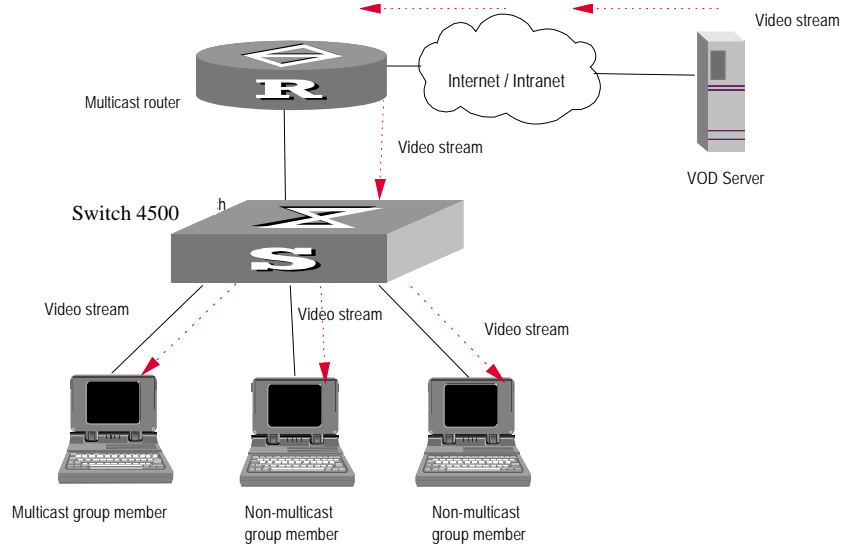
IGMP Snooping Overview

IGMP Snooping (Internet Group Management Protocol Snooping) is a multicast control mechanism running on Layer 2 (the link layer) of the switch. It is used for multicast group management and control.

When receiving IGMP messages transmitted between the host and router, the Switch 4500 uses IGMP Snooping to analyze the information carried in the IGMP messages. If the switch hears an IGMP host report message from an IGMP host, it will add the host to the corresponding multicast table. If the switch hears an IGMP leave message from an IGMP host, it will remove the host from the corresponding multicast table. The switch continuously listens to the IGMP messages to create and maintain MAC multicast address table on Layer 2. And then it can forward the multicast packets transmitted from the upstream router according to the MAC multicast address table.

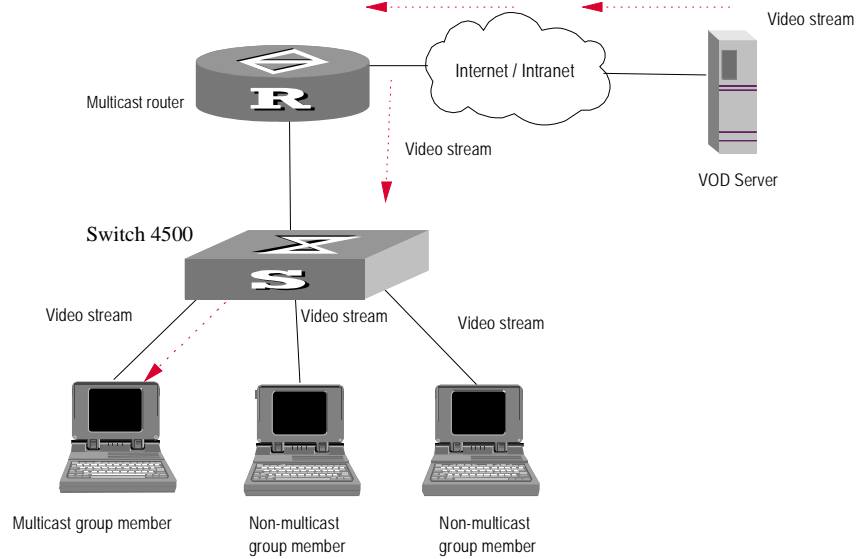
When IGMP Snooping is disabled, the packets are multicast to all ports, see [Figure 44](#).

Figure 44 Multicast packet transmission without IGMP Snooping



When IGMP Snooping operates, packets are not forwarded to all ports, see [Figure 45](#).

Figure 45 Multicast packet transmission when IGMP Snooping runs



IGMP Snooping Terminology

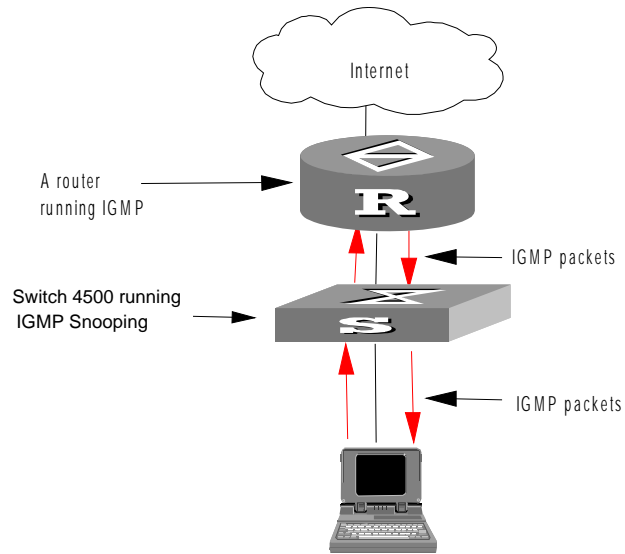
[Table 153](#) explains switching terminology relevant to IGMP Snooping.

Table 153 Switching Terminology relevant to IGMP Snooping

Term	Meaning
Router Port	The port of the switch, directly connected to the multicast router.
Multicast member port	The port connected to the multicast member. The multicast member refers to a host that joined a multicast group.
MAC multicast group	The multicast group is identified with MAC multicast address and maintained by the Switch 4500.
Router port aging time	Time set on the router port aging timer. If the switch has not received any IGMP general query messages before the timer times out, it is no longer considered a router port.
Multicast group member port aging time	When a port joins an IP multicast group, the aging timer of the port will begin timing. If the switch has not received any IGMP report messages before the timer times out, it transmits IGMP specific query message to the port.
Maximum response time	When the switch transmits IGMP specific query message to the multicast member port, the Switch 4500 starts a response timer, which times before the response to the query. If the switch has not received any IGMP report message before the timer times out, it will remove the port from the multicast member ports

The Switch 4500 runs IGMP Snooping to listen to the IGMP messages and map the host and its ports to the corresponding multicast group address. To implement IGMP Snooping, the switch processes different IGMP messages as shown in [Figure 46](#).

Figure 46 Implementing IGMP Snooping



[Table 154](#) explains IGMP Snooping terminology.

Table 154 IGMP Snooping Terminology

Term	Meaning
IGMP general query message	Transmitted by the multicast router to query which multicast group contains member. When a router port receives an IGMP general query message, the Switch 4500 will reset the aging timer of the port. When a port other than a router port receives the IGMP general query message, the Switch 4500 will notify the multicast router that a port is ready to join a multicast group and starts the aging timer for the port.

Table 154 IGMP Snooping Terminology

Term	Meaning
IGMP specific query message	Transmitted from the multicast router to the multicast members and used for querying if a specific group contains any member. When received IGMP specific query message, the switch only transmits the specific query message to the IP multicast group which is queried.
IGMP report message	Transmitted from the host to the multicast router and used for applying to a multicast group or responding to the IGMP query message. When received, the switch checks if the MAC multicast group is ready to join. If the corresponding MAC multicast group does not exist, the switch notifies the router that a member is ready to join a multicast group, creates a new MAC multicast group, adds the port that received the message to the group, starts the port aging timer, and then adds all the router ports in the native VLAN of the port into the MAC multicast forwarding table. Meanwhile, it creates an IP multicast group and adds the port received to it. If the corresponding MAC multicast group exists but does not contain the port that received the report message, the switch adds the port into the multicast group and starts the port aging timer. Then, the switch checks if the corresponding IP multicast group exists. If it does not exist, the switch creates a new IP multicast group and adds the port that received the report message to it. If it does exist, the switch adds the port. If the corresponding MAC multicast group exists and contains the port, the switch will only reset the aging timer of the port.
IGMP leave message	Transmitted from the multicast group member to the multicast router, to notify that a host has left the multicast group. The Switch 4500 transmits the specific query message, concerning the group, to the port that received the message in an effort to check if the host still has other members of this group, and then starts a maximum response timer. If the switch has not received any report message from the multicast group, the port will be removed from the corresponding MAC multicast group. If the MAC multicast group does not have any member, the switch will notify the multicast router to remove it from the multicast tree.

Configuring IGMP Snooping

IGMP Snooping configuration includes:

- [Enabling/Disabling IGMP Snooping](#)
- [Configuring Router Port Aging Time](#)
- [Configuring Maximum Response Time](#)
- [Configuring Aging Time of Multicast Group Member](#)

Of the above configuration tasks, enabling IGMP Snooping is required, while others are optional.

Enabling/Disabling IGMP Snooping

Use the commands in [Table 155](#) to enable/disable IGMP Snooping on Layer 2. First enable IGMP Snooping globally in System View, and then enable IGMP Snooping of the corresponding VLAN in VLAN View.

Perform the following configuration in System View and VLAN View.

Table 155 Enabling/Disabling IGMP Snooping

Operation	Command
Enable/disable IGMP Snooping	<code>igmp-snooping { enable disable }</code>



Although layer 2 and layer 3 multicast protocols can run together, they cannot run on the same VLAN or its corresponding VLAN interface at the same time. For example, if the layer 2 multicast protocol is enabled on a VLAN, then the layer 3 multicast protocol cannot operate on this VLAN, and vice versa.



IGMP Snooping functions only when it is enabled both in System View and in VLAN View.

By default, IGMP Snooping is disabled.

Configuring Router Port Aging Time

Use the commands in [Table 156](#) to manually configure the router port aging time. If the switch has not received a general query message from the router before the router port is aged, the switch will remove the port from the MAC multicast group.

Perform the following configuration in system view.

Table 156 Configuring router port aging time

Operation	Command
Configure router port aging time	<code>igmp-snooping router-aging-time seconds</code>
Restore the default aging time	<code>undo igmp-snooping router-aging-time</code>

By default, the port aging time is 105 seconds.

Configuring Maximum Response Time

Use the commands in [Table 157](#) to manually configure the maximum response time. If the Switch 4500 receives no report message from a port within the maximum response time, the switch will remove the port from the multicast group.

Perform the following configuration in System View.

Table 157 Configuring the maximum response time

Operation	Command
Configure the maximum response time	<code>igmp-snooping max-response-time seconds</code>
Restore the default setting	<code>undo igmp-snooping max-response-time</code>

By default, the maximum response time is 10 seconds.

Configuring Aging Time of Multicast Group Member

Use the commands in [Table 158](#) to manually set the aging time of the multicast group member port. If the switch receives no multicast group report message during the member port aging time, it will transmit the specific query message to that port and start a maximum response timer.

Perform the following configuration in system view.

Table 158 Configuring aging time of the multicast member

Operation	Command
Configure aging time of the multicast member	igmp-snooping host-aging-time <i>seconds</i>
Restore the default setting	undo igmp-snooping host-aging-time

By default, the aging time of the multicast member is 260 seconds.

Displaying and Debugging IGMP Snooping

Execute **display** command in any view to display the running of the IGMP Snooping configuration, and to verify the effect of the configuration. Execute **reset** command in user view to reset the IGMP Snooping statistic information. Execute **debugging** command in user view to debug IGMP Snooping configuration.

Table 159 Displaying and debugging IGMP Snooping

Operation	Command
Display the information about current IGMP Snooping configuration	display igmp-snooping configuration
Display IGMP Snooping statistics of received and sent messages	display igmp-snooping statistics
Display IP/MAC multicast group information in the VLAN	display igmp-snooping group [vlan <i>vlanid</i>]
Reset the IGMP Snooping statistic information	reset igmp-snooping statistics

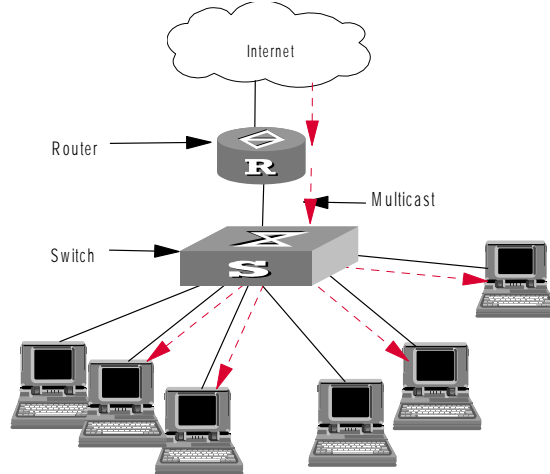
Configuration Example — Enable IGMP Snooping

Networking Requirements

To implement IGMP Snooping on the switch, first enable it. The switch is connected to the router via the router port, and with user PCs through the non-router ports on vlan 10.

Networking Diagram

Figure 47 IGMP Snooping configuration network



Configuration Procedure

Enable IGMP Snooping globally.

```
[ 4500 ]igmp-snooping enable
```

Enable IGMP Snooping on VLAN 10.

```
[ 4500 ]vlan 10
```

```
[ 4500-vlan10 ]igmp-snooping enable
```

IGMP Snooping Fault Diagnosis and Troubleshooting

Fault: Multicast function cannot be implemented on the switch.

Troubleshooting:

Diagnosis 1: IGMP Snooping is disabled.

- 1 Input the **display current-configuration** command to display the status of IGMP Snooping.
- 2 If the switch disabled IGMP Snooping, check whether the IGMP Snooping is enabled globally and also enabled on the VLAN. If IGMP Snooping is not enabled globally, first input the **igmp-snooping enable** command in System View and then input the **igmp-snooping enable** command in VLAN view. If IGMP Snooping is not enabled on the VLAN, input the **igmp-snooping enable** command in VLAN view.

Diagnosis 2: Multicast forwarding table set up by IGMP Snooping is wrong.

- 1 Input the **display igmp-snooping group** command to display if the multicast group is the expected one.
- 2 If the multicast group created by IGMP Snooping is not correct, refer to Technical Support for assistance.
- 3 Continue with diagnosis 3 if the second step is completed.

Diagnosis 3: Multicast forwarding table set up on the bottom layer is wrong.

- 1 Enable IGMP Snooping group in user view and then input the command **display igmp-snooping group** to check if MAC multicast forwarding table in the bottom layer and that created by IGMP Snooping is consistent. You may also input the **display mac vlan** command in any view to check if MAC multicast forwarding table under vlanid in the bottom layer and that created by IGMP Snooping is consistent.
- 2 If they are not consistent, refer to Technical Support for assistance.

9

STACKING

This chapter covers the following topics:

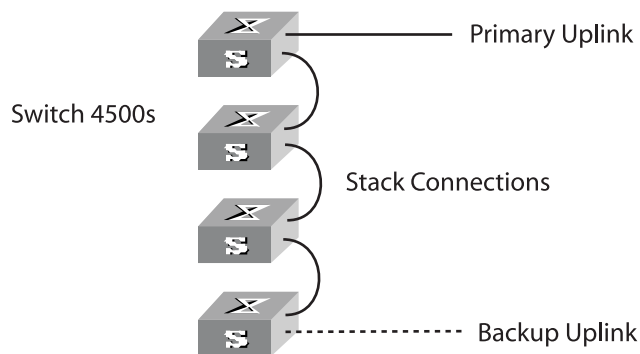
- [Introduction to Stacking](#)
- [Establishment of an XRN Fabric](#)
- [Configuring a Stack](#)
- [Stack Configuration Example](#)

Introduction to Stacking

Several Switch 4500 units can be interconnected to create a “stack”, in which each Switch is a unit. The ports used to interconnect all the units are called stacking ports, while the other ports that are used to connect the stack to users are called user ports. In this way, you can increase ports and switching capability by adding devices to the stack. In addition, reliability of the system will be improved because the devices within the stack can backup each other. This feature brings you many advantages:

- Realizes unified management of multiple devices. Only one connection and one IP address are required to manage the entire stack. Therefore, management cost is reduced.
- Enables you to purchase devices on demand and expand network capacity smoothly. Protects your investment to the full extent during network upgrade.

Figure 48 Stack Example



Establishment of an XRN Fabric

Topology and connections of an XRN fabric

An XRN fabric typically has a ring topology structure. Each switch has two ports connected with two other switches in the fabric. These two ports are called fabric ports in general, a left port and a right port respectively; the other ports, which are

available for connections with users or devices outside the fabric, are called user ports.

A correctly built XRN fabric features the following:

- Multiple Switch 4500 series switches are interconnected through their fabric ports.
- Given a switch, its left port is connected to the right port of another switch, and its right port is connected to the left port of a third one.

XRN fabric also supports bus topology, which has the same requirements as the ring topology. The difference is that in a bus topology structure, the units at both ends of the bus have only one fabric port connected.

Fabric ports

On an Switch 4500 series Ethernet switch, only four GigabitEthernet ports can be configured as fabric ports. If not used for fabric connection, these four ports can be used as general data ports. The four ports fall into two groups according to their port numbers:

- GigabitEthernet 1/0/25 and GigabitEthernet 1/0/26 form the first group.
- GigabitEthernet 1/0/27 and GigabitEthernet 1/0/28 form the second group.

Only one group of ports can be configured as fabric ports at a time. Given a group, either GigabitEthernet 1/0/25 or GigabitEthernet 1/0/27 can be configured as the left fabric port, and either GigabitEthernet 1/0/26 or GigabitEthernet 1/0/28 can be configured as the right fabric port.

Once you configure a port as a fabric port, the group that comprises this fabric port becomes the fabric port group, and you cannot configure a port in the other group as a fabric port. For example, once you configure GigabitEthernet 1/0/25 as a fabric port, this port automatically becomes the left port and the first group becomes the fabric port group.



The system does not require a consistency in the fabric port groups between different switches. That is, the left fabric port in the first group of a switch can be connected to the right fabric port in the second group of the peer switch.

Configuring a Stack

You can configure VLAN unit IDs, stack name, and the authentication mode between units by using the command.

Table 160 Configuring a Stack

Device	Configuration	Default Settings	Comment
Switch	Specify the stacking VLAN of the Switch	The stacking VLAN is VLAN 4093	You should specify the stacking VLAN before the stack is established.
	Set unit IDs for the Switches	The unit ID of a Switch is set to 1	Make sure that you have set different unit IDs to different Switches, so that the stack can operate normally after all the Switches are interconnected.
	Specify the stack port of the Switch	-	Only the Gigabit combo ports can be used to interconnect the Switch units to form a stack.

Device	Configuration	Default Settings	Comment
	Set unit names for the Switches	-	-
	Set a name for the stack where the Switches belong	The stack name of the Switches is 4500	Interconnected the Switches with the same stack name to form a stack.
	Set the authentication mode for the stack	No authentication mode is set on the Switches	Set the same authentication mode on all the devices within the stack.

Specifying the Stacking VLAN of the Switch

You can use the command in the following table to specify the stacking VLAN of the Switch.

Perform the following configuration in System View.

Table 161 Specifying the Stacking VLAN of the Switch

	Command
Specifying the stacking VLAN of the Switch	ftm stacking-vlan <i>vlan-id</i>
Setting the stacking VLAN of the Switch to Default Value	undo ftm stacking-vlan

By default, the stacking VLAN is VLAN 4093.

You should specify the stacking VLAN before the stack is established.

Setting Unit IDs for Switches

You can use the command in the following table to set unit IDs for Switches. Make sure to set different unit IDs for different Switches in a stack. On the Switches that support auto numbering, its stacking logic will automatically number the Switches to constitute a stack, so that each Switch has a unique unit ID in the stack.

Perform the following configuration in System View.

Table 162 Setting unit IDs for Switches

	Command
Set unit IDs for Switches	change unit-id <1-8> to {<1-8> auto-numbering }

- If the modified unit ID does not exist in the stack, the Switch sets its priority to 5 and saves it in the unit Flash memory.
- If the modified unit ID is an existing one, the Switch prompts you to confirm if you really want to change the unit ID. If you choose to change, the existing unit ID is replaced and the priority is set to 5. Then you can use the **fabric save-unit-id** command to save the modified unit ID into the unit Flash memory and clear the information about the existing one.
- If **auto-numbering** is selected, the system sets the unit ID priority to 10. You can use the **fabric save-unit-id** command to save the modified unit ID into the unit Flash memory and clear the information about the existing one.



The unit IDs in a stack are not necessarily numbered consecutively or in ascending order.

By default, the unit ID of a Switch is set to 1. A unit ID can be set to a value in the range from 1 to the maximum number of devices supported in XRN.

Saving the Unit ID of Each Unit in the Stack

You can use the commands in the following table to save the unit ID of each unit in the stack to the unit Flash memory.

Perform the following configuration in User View.

Table 163 Save the unit ID of each unit in the stack

	Command
Save the unit ID of each unit in the stack	fabric save-unit-id
Restore the unit ID of each unit in the stack	undo fabric save-unit-id

Specifying the Fabric Port of the Switch

Perform the following configuration in System View.

Table 164 Specifying the Fabric Port of the Switch

	Command
Specifying the stacking port of the Switch	fabric-port { <i>interface-name</i> <i>interface-type interface-num</i> } enable
Cancel the stacking port of the Switch	undo fabric-port { <i>interface-name</i> <i>interface-type interface-num</i> } enable

Only the Gigabit combo ports can be used to interconnect the Switch units to form a stack.



In the 3Com switch operating system, the term "fabric" is used as a general expression for stack.

Setting Unit Names for Switches

You can use the command in the following table to set a unit name for each Switch.

Perform the following configuration in System View.

Table 165 Setting Unit Names for Switches

	Command
Set unit names for Switches	set unit <i>unit-id</i> name <i>unit-name</i>

Setting a Stack Name for Switches

Only the Switches with the same stack name and XRN authentication mode can constitute a stack.

You can use the commands in the following table to set a stack name for the Switches.

Perform the following configuration in System View.

Table 166 Setting a Stack Name for Switches

	Command
Set a stack name for Switches	sysname <i>sysname</i>
Restore the default stack name	undo sysname

By default, the stack name is "4500".

Setting an XRN Authentication Mode for Switches



Only the Switches with the same stack name and XRN authentication mode can constitute a stack.

Note: "XRN" is a proprietary 3Com technology for enterprise-level stacking on our Switch 5500-EI switches. Because the Switch 4500 shares its operating system with the Switch 5500 family, the XRN terminology is referred to when setting authentication mode.

You can use the commands in the following table to set an authentication mode for the Switches.

Perform the following configuration in System View.

Table 167 Setting an XRN Authentication Mode for Switches

	Command
Set an XRN authentication mode for Switches	<code>xrn-fabric authentication-mode { simple password md5 key }</code>
Restore the default XRN authentication mode	<code>undo xrn-fabric authentication-mode</code>

By default, no authentication mode is set on the Switches.

Displaying and Debugging a Stack

Following completion of the above configuration, you can execute the `display` command in any view to view device management and verify the settings.

Table 168 Displaying and Debugging FTM

	Command
Display the information of the entire stack	<code>display xrn-fabric [port]</code>
Display the topology information of stack	<code>display ftm{ information route topology-database }</code>

Stack Configuration Example

Networking Requirements

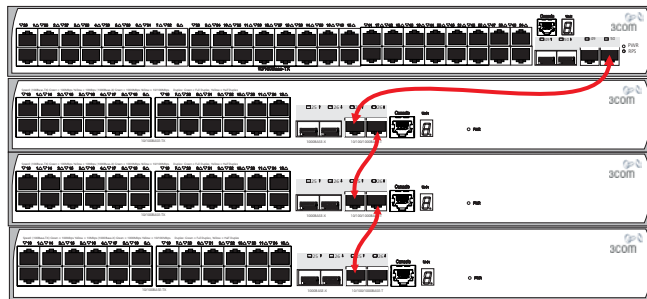
Configure unit ID, unit name, stack name, and authentication mode for four switches, and interconnect them to form a stack.

The configuration details are as follows:

- Unit IDs: 1, 2, 3, 4
- Unit names: unit 1, unit 2, unit 3, unit 4
- Stack name: hello
- Authentication mode: simple password
- Password: welcome

Networking Diagram

Figure 49 Networking Diagram of a stack



Configuration Procedure

Configure Switch A:

```
[4500]change unit-id 1 to 1
[4500]fabric-port gigabitethernet1/0/51 enable
[4500]fabric-port gigabitethernet1/0/52 enable
[4500]sysname hello
[hello]xrn-fabric authentication-mode simple welcome
```

Configure Switch B:

```
[4500]change unit-id 1 to auto-numbering
[4500]fabric-port gigabitethernet2/0/27 enable
[4500]fabric-port gigabitethernet2/0/28 enable
[4500]sysname hello
[hello]xrn-fabric authentication-mode simple welcome
```

Configure Switch C:

```
[4500]change unit-id 1 to auto-numbering
[4500]fabric-port gigabitethernet3/0/27 enable
[4500]fabric-port gigabitethernet3/0/28 enable
[4500]sysname hello
[hello]xrn-fabric authentication-mode simple welcome
```

Configure Switch D:

```
[4500]change unit-id 1 to auto-numbering
[4500]fabric-port gigabitethernet4/0/27 enable
[4500]fabric-port gigabitethernet4/0/28 enable
[4500]sysname hello
[hello]xrn-fabric authentication-mode simple welcome
```



- *In the example, it is assumed that the system will automatically change the unit IDs of Switch B, Switch C and Switch D to 2, 3 and 4 after you choose auto-numbering for unit-id.*

10

RSTP CONFIGURATION

This chapter covers the following topics:

- [STP Overview](#)
- [RSTP Configuration](#)
- [RSTP Configuration Example](#)

STP Overview

Spanning Tree Protocol (STP) is applied in loop networks to block some undesirable redundant paths with certain algorithms and prune the network into a loop-free tree, thereby avoiding the proliferation and infinite cycling of the packet in the loop network.

Implement STP

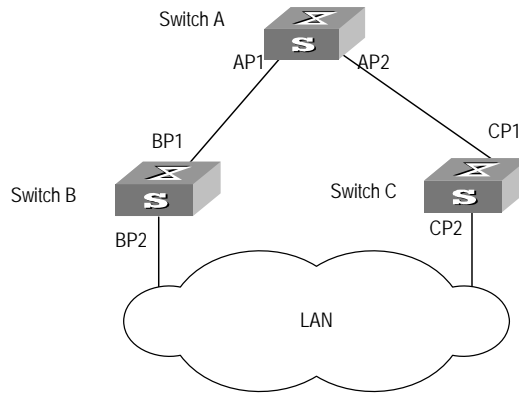
The fundamental of STP is that the Switches exchange a special type of protocol packet (which is called configuration Bridge Protocol Data Units, or BPDU, in IEEE 802.1D) to decide the topology of the network. The configuration BPDU contains the information enough to ensure the Switches to compute the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

The configuration BPDU mainly contains the following information:

- 1 The root ID consisting of root priority and MAC address
- 2 The cost of the shortest path to the root
- 3 Designated bridge ID consisting of designated bridge priority and MAC address
- 4 Designated port ID consisting of port priority and port number
- 5 The age of the configuration BPDU: MessageAge
- 6 The maximum age of the configuration BPDU: MaxAge
- 7 Configuration BPDU interval: HelloTime
- 8 Forward delay of the port: ForwardDelay.

What are the Designated Bridge and Designated Port?

Figure 50 Designated Bridge and Designated Port



For a Switch, the designated bridge is a Switch in charge of forwarding BPDU to the local Switch via a port called the designated port. For a LAN, the designated bridge is a Switch that is in charge of forwarding BPDU to the network segment via a port called the designated port. As illustrated in [Figure 50](#), Switch A forwards data to Switch B via the port AP1. So to Switch B, the designated bridge is Switch A and the designated port is AP1. Also in the figure above, Switch B and Switch C are connected to the LAN and Switch B forwards BPDU to LAN. So the designated bridge of LAN is Switch B and the designated port is BP2.



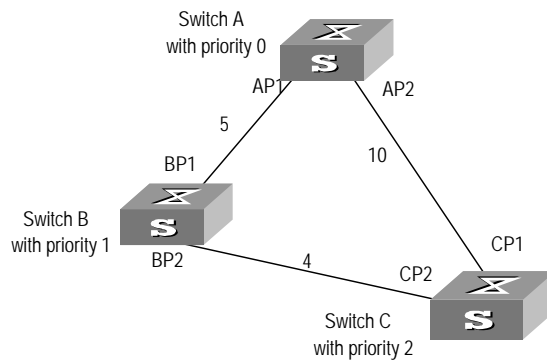
AP1, AP2, BP1, BP2, CP1 and CP2 respectively delegate the ports of Switch A, Switch B and Switch C.

The Specific Calculation Process of STP Algorithm

The following example illustrates the calculation process of STP.

[Figure 51](#) illustrates the network.

Figure 51 Switch Networking.



To facilitate the descriptions, only the first four parts of the configuration BPDU are described in the example. They are root ID (expressed as Ethernet Switch priority), path cost to the root, designated bridge ID (expressed as Ethernet Switch priority) and the designated port ID (expressed as the port number). As illustrated

in the figure above, the priorities of Switch A, B and C are 0, 1 and 2 and the path costs of their links are 5, 10 and 4 respectively.

1 Initial state

When initialized, each port of the Switches will generate the configuration BPDU taking itself as the root with a root path cost as 0, designated bridge IDs as their own Switch IDs and the designated ports as their ports.

- Switch A:
 - Configuration BPDU of AP1: {0, 0, 0, AP1}
 - Configuration BPDU of AP2: {0, 0, 0, AP2}
- Switch B:
 - Configuration BPDU of BP1: {1, 0, 1, BP1}
 - Configuration BPDU of BP2: {1, 0, 1, BP2}
- Switch C:
 - Configuration BPDU of CP2: {2, 0, 2, CP2}
 - Configuration BPDU of CP1: {2, 0, 2, CP1}

2 Select the optimum configuration BPDU

Every Switch transmits its configuration BPDU to others. When a port receives a configuration BPDU with a lower priority than that of its own, it will discard the message and keep the local BPDU unchanged. When a higher-priority configuration BPDU is received, the local BPDU is updated. And the optimum configuration BPDU will be elected through comparing the configuration BPDUs of all the ports.

The comparison rules are:

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

3 Specify the root port and designated port, block the redundancy link and update the configuration BPDU of the designated port.

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

The Switch compares the calculated BPDU with the BPDU of the corresponding port. If the BPDU of the corresponding port is better, the BPDU of the port remains the same. If the calculated BPDU is better, the port will be the designated port, and the port BPDU will be modified by the calculated BPDU.

The comparison process of each Switch is as follows.

- Switch A:

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

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

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

- Switch B:

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

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

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

Switch B compares the configuration BPDUs of the ports and selects the BP1 BPDU as the optimum one. Thus BP1 is elected as the root port and the configuration BPDUs of Switch B ports are updated as follows.

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

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

- Switch C:

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

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

By comparison, CP1 configuration BPDU is elected as the optimum one. The CP1 is thus specified as the root port with no modifications made on its configuration BPDU. However, CP2 will be blocked and its BPDU also remains the same, but it will not receive the data (excluding the STP packet) forwarded from Switch B until spanning tree calculation is launched again by some new events. For example, the link from Switch B to C is down or the port receives a better configuration BPDU.

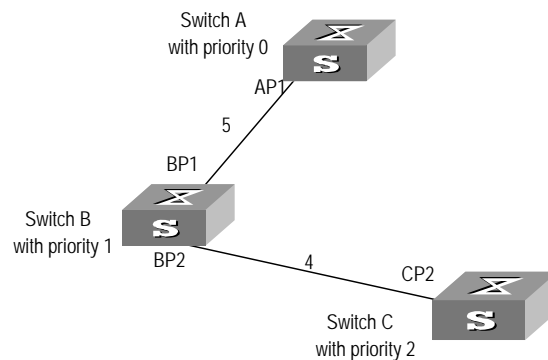
CP2 will receive the updated configuration BPDU, {0, 5, 1, BP2}, from Switch B. Since this configuration BPDU is better than the old one, the old BPDU will be updated to {0, 5, 1, BP2}.

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

By comparison, {0, 5, 1, BP2}, the configuration BPDU of CP2, is elected as the optimum one, CP2 is elected as the root port, whose BPDU will not change, while CP1 will be blocked and retain its BPDU, but it will not receive the data forwarded from Switch A until spanning tree calculation is triggered again by some changes. For example, the link from Switch B to C as down.

Thus the spanning tree is stabilized. The tree with the root bridge A is illustrated in [Figure 52](#).

Figure 52 The Final Stabilized Spanning Tree



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

Configuration BPDU Forwarding Mechanism in STP

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

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

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

Implement RSTP on the Switch

The Switch implements the Rapid Spanning Tree Protocol (RSTP), an enhanced form of STP. The Forward Delay for the root ports and designated ports to enter forwarding state is greatly reduced in certain conditions, thereby shortening the time period for stabilizing the network topology.

To achieve the rapid transition of the root port state, the following requirement should be met: The old root port on this Switch has stopped data forwarding and the designated port in the upstream has begun forwarding data.

The conditions for rapid state transition of the designated port are:

- The port is an edge port that does not connect with any Switch directly or indirectly. If the designated port is an edge port, it can Switch to forwarding state directly without immediately forwarding data.
- The port is connected with the point-to-point link, that is, it is the master port in aggregation ports or full duplex port. It is feasible to configure a point-to-point connection. However, errors may occur and therefore this configuration is not recommended. If the designated port is connected with the point-to-point link, it can enter the forwarding state right after handshaking with the downstream Switch and receiving the response.

The Switch that uses RSTP is compatible with the one using STP. Both protocol packets can be identified by the Switch running RSTP and used in spanning tree calculation.

RSTP Configuration

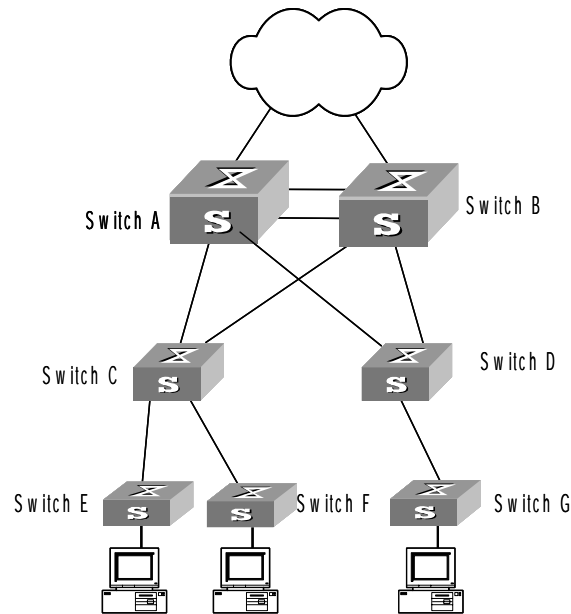
The configuration of RSTP changes with the position of the Switch in the network, as discussed below.

Figure 53 Configuring STP

Switch A and Switch B: Root bridge and backup root bridge

Switch C and Switch D: Intermediate Switches in the Switched network

Switch E, Switch F and Switch G: Switches directly connected with user PCs



In [Figure 53](#) the Switch 4500 is typically Switch E, F and G. Additionally it could be Switch C and D. For completeness, configuration of all devices is presented here.

Table 169 RSTP Configuration

Device	Configuration	Default Value	Note
Switch A & Switch B	Enable the STP feature on the Switch Enable the STP feature on the port Configure RSTP operational mode	The STP feature is disabled from the Switch, but will be enabled on all ports once being enabled on the Switch. The Switch works in RSTP mode.	The configuration of STP feature status on the port will not take effect if the STP feature is disabled from the Switch. If there are Switches respectively running STP and RSTP on the network, it is recommended to set the Switch in STP-compatible mode.
	Configure the STP-Ignore attribute of VLANs on a Switch	No VLAN on a STP-enabled Switch is STP-Ignored.	Once a VLAN is specified to be STP-Ignored, the packets of this VLAN will be forwarded on any Switch port, with no restriction from the calculated STP path.
	Specify a Switch as the root or backup root bridge	The role of the current Switch as the root or backup root bridge depends on the STP calculation.	A Switch can be made the root bridge by specifying its Bridge preference to 0.

Device	Configuration	Default Value	Note
	Configure the Bridge preference of a Switch	The Bridge preference of a Switch is 32768.	A Switch can be made the root bridge by specifying its Bridge preference to 0.
	Specify Forward Delay, Hello Time, and Max Age	Forward Delay fixes on 15 seconds, Hello Times on 2 seconds, and Max Age on 20 seconds.	The other Switches copies the configuration on the root bridge with respect to these time parameters. You can therefore only configure them on the root bridge. The default values are highly recommended.
	Specify the maximum transmission rate of STP packets on a port	No Ethernet port can send more than 3 STP packets within one Hello Time.	The more STP packets a port sends within one Hello Time, the more resources are consumed. It is therefore recommended to limit the transmission rate of STP packets on a port, preferably to the default value.
	Configure whether to connect a port with a peer-to-peer link	RSTP can detect automatically whether the current Ethernet port is connect to a peer-to-peer link.	The two ports connected with a peer-to-peer link can rapidly transit to the forwarding status by sending synchronous packets, eliminating unnecessary forwarding delay.
	Specify the Path Cost on a port Specify the standard to follow in Path Cost calculation	The Switch gets the path cost of a port from the link rate under the IEEE 802.1t standard.	The path cost of a port is closely related to the transmission rate of the link the port connected with. The larger the link rate is, the smaller the path cost shall be. It is recommended to use the default configuration.
	Specify mCheck for a port	-	You can change the operational mode of a port from STP-compatible to RSTP.
	Configure the protection functions on a Switch	No protection function is enabled on a Switch.	It is recommended to enable the Root protection function on the root bridge.
Switch C & Switch D	Enable the STP feature on the Switch Enable the STP feature on the port	The STP feature is disabled from the Switch, but will be enabled on all ports once being enabled on the Switch.	The configuration of STP feature status on the port will not take effect if the STP feature is disabled from the Switch.
	Configure RSTP operational mode	The Switch works in RSTP mode.	If there are Switches respectively running STP and RSTP on the network, it is recommended to set the Switch in STP-compatible mode.
	Configure the Bridge preference of a Switch	The Bridge preference of a Switch is 32768.	A Switch can be made the designated bridge of the downstream Switches by specifying an appropriate Bridge preference in the STP calculation.

Device	Configuration	Default Value	Note
	Configure the timeout time factor of a Switch	The Switch, if has not received any Hello packet from the upstream Switch for thrice the Hello Time, will consider the upstream Switch failed and recalculate the spanning tree.	In a stable network, it is recommended to set the timeout time factor to 5, 6, or 7. Then the Switch will not consider the upstream Switch failed unless it has not received any Hello packet from it for 5, 6, or 7 times the Hello Time.
	Specify the maximum transmission rate of STP packets on a port	No Ethernet port can send more than 3 STP packets within one Hello Time.	The more STP packets a port sends within one Hello Time, the more resources are consumed. It is therefore recommended to limit the transmission rate of STP packets on a port, preferably to the default value.
	Specify the preference of a port	All Ethernet ports are at the preference 128.	The port preference plays an important role in root port selection. You can make a port to be root port by giving it a smallest preference value.
	Configure whether to connect a port with a peer-to-peer link	RSTP can detect automatically whether the current Ethernet port is connect to a peer-to-peer link.	The two ports connected with a peer-to-peer link can rapidly transit to the forwarding status by sending synchronous packets, eliminating unnecessary forwarding delay.
	Specify the Path Cost on a port	The Switch gets the path cost of a port from the link rate under the IEEE 802.1t standard.	The path cost of a port is closely related to the transmission rate of the link the port connected with. The larger the link rate is, the smaller the path cost shall be. It is recommended to use the default configuration.
	Specify the standard to follow in Path Cost calculation		
	Specify mCheck for a port	-	You can change the operational mode of a port from STP-compatible to RSTP.
	Configure the protection functions on a Switch	No protection function is enabled on a Switch.	It is recommended to enable the loop protection function on the intermediate Switches.
Switch E, Switch F & Switch G	Enable the STP feature on the Switch	The STP feature is disabled from the Switch, but will be enabled on all ports once being enabled on the Switch.	The configuration of STP feature status on the port will not take effect if the STP feature is disabled from the Switch.
	Enable the STP feature on the port		
	Configure RSTP operational mode	The Switch works in RSTP mode.	If there are Switches respectively running STP and RSTP on the network, it is recommended to set the Switch in STP-compatible mode.

Device	Configuration	Default Value	Note
	Configure the timeout time factor of a Switch	The Switch, if has not received any Hello packet from the upstream Switch for thrice the Hello Time, will consider the upstream Switch failed and recalculate the spanning tree.	In a stable network, it is recommended to set the timeout time factor to 5, 6, or 7. Then the Switch will not consider the upstream Switch failed unless it has not received any Hello packet from it for 5, 6, or 7 times the Hello Time.
	Specify the maximum transmission rate of STP packets on a port	No Ethernet port can send more than 3 STP packets within one Hello Time.	The more STP packets a port sends within one Hello Time, the more resources are consumed. It is therefore recommended to limit the transmission rate of STP packets on a port, preferably to the default value.
	Specify the preference of a port	All Ethernet ports are at the preference 128.	The port preference plays an important role in root port selection. You can make a port to be root port by giving it a smallest preference value.
	Configure whether to connect a port with a peer-to-peer link	RSTP can detect automatically whether the current Ethernet port is connect to a peer-to-peer link.	The two ports connected with a peer-to-peer link can rapidly transit to the forwarding status by sending synchronous packets, eliminating unnecessary forwarding delay.
	Specify the Path Cost on a port	The Switch gets the path cost of a port from the link rate under the IEEE 802.1t standard.	The path cost of a port is closely related to the transmission rate of the link the port connected with. The larger the link rate is, the smaller the path cost shall be. It is recommended to use the default configuration.
	Specify the standard to follow in Path Cost calculation		
	Configure whether a port can be an Edge Port	All Ethernet ports are configured as non-edge ports.	For ports directly connected with terminals, please configure them as edge ports, and enable the BPDU protection function on them.
	Specify mCheck for a port	-	You can change the operational mode of a port from STP-compatible to RSTP.
	Configure the protection functions on a Switch	No protection function is enabled on a Switch.	It is recommended to enable the BPDU protection function on the Switches directly connected with user PCs.



After the STP protocol is enabled, the modification of any parameter will result in the re-calculation of the spanning tree on the Switch. It is therefore recommended to configure all the RSTP parameters before enabling the STP feature on the Switch and the port.

Enable/Disable RSTP on a Switch

You can use the following command to enable RSTP on the Switch.

Perform the following configurations in System View.

Table 170 Enable/Disable RSTP on a Device

Operation	Command
Enable/Disable RSTP on a device	<code>stp { enable disable }</code>

Operation	Command
Restore RSTP to the default value	undo stp

Only after the RSTP is enabled on the Switch can other configurations take effect.

By default, RSTP is enabled.

Enable/Disable RSTP on a Port

You can use the following command to enable/disable the RSTP on the designated port. To flexibly control the RSTP operations, after RSTP is enabled on the Ethernet ports of the Switch, it can be disabled again to prevent the ports from participating in the spanning tree calculation.

Perform the following configurations in Ethernet Port View.

Table 171 Enable/Disable RSTP on a Port

Operation	Command
Enable RSTP on a specified port	stp enable
Disable RSTP on a specified port	stp disable

Note that the redundancy route may be generated after RSTP is disabled on the Ethernet port.

By default, RSTP on all the ports will be enabled after it is enabled on the Switch.

Configure RSTP Operating Mode

RSTP is executable in RSTP mode or STP-compatible mode. RSTP mode is applied when all the network devices provided for executing RSTP, while the STP-compatible mode is applied when both STP and RSTP are executable on the network.

You can use the following command to set the RSTP operating mode.

Perform the following configurations in System View.

Table 172 Set RSTP Operating Mode

Operation	Command
Configure to run RSTP in STP-compatible/RSTP mode	stp mode { stp rstp }
Restore the default RSTP mode	undo stp mode

Normally, if there is a bridge provided to execute STP in the Switching network, the port (in the Switch running RSTP), which connects to another port (in the Switch for executing STP), can automatically Switch to STP compatible mode from RSTP mode.

By default, RSTP runs in RSTP mode.

Configure the STP-Ignore attribute of VLANs on a Switch

RSTP is a single spanning tree protocol, under which only one spanning tree will be generated on one Switched network. To ensure the successful communication between VLANs on a network, all of them must be distributed consecutively along the STP path; otherwise, some VLANs will be isolated due to the blocking of intra-links, causing the failure in cross-VLAN communication. Once there are VLANs specially required to be located away from the STP path, you can solve the

consequent blocking by configuring the STP-Ignore attribute on the appropriate Switch.

Once an STP-Ignored VLAN is configured, the packets of this VLAN will be forwarded on any Switch port, with no restriction from the calculated STP path.

You can configure the STP-Ignore attribute on a Switch by using the following commands.

Perform the following configuration in System View.

Table 173 Configuring the STP-Ignore Attribute of VLANs on a Switch

Operation	Command
Specify an STP-Ignored VLAN	stp ignored vlan <i>vlan_list</i>
Cancel the configuration of the STP-Ignored VLAN	undo stp ignored vlan <i>vlan_list</i>

By default, no VLAN is STP-Ignored if STP is enabled on the Switch.

Set Priority of a Specified Bridge

Whether a bridge can be selected as the “root” of the spanning tree depends on its priority. By assigning a lower priority, a bridge can be artificially specified as the root of the spanning tree.

You can use the following command to configure the priority of a specified bridge. Perform the following configurations in System View.

Table 174 Set Priority of a Specified Bridge

Operation	Command
Set priority of a specified bridge	stp priority <i>bridge_priority</i>
Restore the default priority of specified bridge	undo stp priority

Note that if the priorities of all the bridges in the Switching network are the same, the bridge with the smallest MAC address will be selected as the “root”. When RSTP is enabled, an assignment of a priority to the bridge will lead to recalculation of the spanning tree.

By default, the priority of the bridge is 32768.

Specify the Switch as Primary or Secondary Root Bridge

RSTP can determine the spanning tree root through calculation. You can also specify the current Switch as the root using this command.

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

Perform the following configuration in System View.

Table 175 Specify the Switch as Primary or Secondary Root Bridge

Operation	Command
Specify the current Switch as the primary root bridge of the spanning tree.	stp root primary
Specify the current Switch as the secondary root bridge of the spanning tree.	stp root secondary

Operation	Command
Disqualify the current Switch as the primary or secondary root.	<code>undo stp root</code>

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

A Switch can either be a primary or secondary root bridge, but not both of them.

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



To configure a Switch as the root of the spanning tree instance, you can specify its priority as 0 or simply set it as the root, using the command.

It is not necessary to specify two or more roots for an STI — do not specify the root for an STI on two or more Switches.

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

Generally, 3Com recommends designating one primary root and two or more secondary roots for a spanning tree.

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

Set Forward Delay of a Specified Bridge

Link failure will cause recalculation of the spanning tree and change its structure. However, the newly calculated configuration BPDU cannot be propagated throughout the network immediately. If the newly selected root port and designated port begin to forward data frames right away, this can cause an occasional loop. Accordingly, the protocol adopts a state transition mechanism, that is, the root port and the designated port must undergo a transition state for a period of Forward Delay before they transition to the forwarding state and resume data frame forwarding. This delay ensures that the new configuration BPDU has been propagated throughout the network before the data frame forwarding is resumed.

You can use the following command to set the Forward Delay for a specified bridge.

Perform the following configurations in System View.

Table 176 Set Forward Delay of a Specified Bridge

Operation	Command
Set Forward Delay of a specified bridge	<code>stp timer forward-delay centiseconds</code>
Restore the default Forward Delay of specified bridge	<code>undo stp timer forward-delay</code>

Forward Delay of the bridge is related to the diameter of the Switching network. As a rule, the larger the network diameter, the longer the Forward Delay. Note

that if the Forward Delay is configured too short, occasional path redundancy may occur. If the Forward Delay is configured too long, restoring the network connection may take a long time. It is recommended to use the default setting.

By default, the bridge Forward Delay is 15 seconds.

Set Hello Time of the Specified Bridge

A bridge transmits hello packet regularly to the adjacent bridges to check if there is link failure.

You can use the following command to set the Hello Time of a specified bridge.

Perform the following configurations in System View.

Table 177 Set Hello Time of the Specified Bridge

Operation	Command
Set Hello Time of the specified bridge	<code>stp timer hello centiseconds</code>
Restore the default Hello Time of the specified bridge	<code>undo stp timer hello</code>

An appropriate Hello Time can ensure that the bridge can detect certain link failures in the network in a timely manner. It is strongly recommended that default value of 2 seconds is retained.

By default, the Hello Time of the bridge is 2 seconds.

Set Max Age of the Specified Bridge

Max Age is a parameter to judge whether the configuration BPDU is "timeout". Users can configure it according to the actual network situation.

You can use the following command to set Max Age of a specified bridge.

Perform the following configuration in System View.

Table 178 Set Max Age of the Specified Bridge

Operation	Command
Set Max Age of the specified bridge	<code>stp timer max-age centiseconds</code>
Restore the default Max Age of the specified bridge	<code>undo stp timer max-age</code>

If the Max Age is too short, it will result in frequent calculation of spanning tree or misjudge the network congestion as a link fault. On the other hand, too long Max Age may make the bridge unable to find link failure in time and weaken the network auto-sensing ability. It is recommended to use the default setting.

By default, the bridge Max Age is 20 seconds.

Set Timeout Factor of the Bridge

A bridge transmits hello packet regularly to the adjacent bridges to check if there is link failure. Generally, if the Switch does not receive the RSTP packets from the upstream Switch for 3 occurrences of hello time, the Switch will decide the upstream Switch is dead and will recalculate the topology of the network. Then in a steady network, the recalculation may be caused when the upstream Switch is busy. In this case, you can redefine the timeout interval to a longer time by defining the multiple value of hello time.

You can use the following command to set the multiple value of hello time of a specified bridge.

Perform the following configurations in System View.

Table 179 Set Timeout Factor of the Bridge

Operation	Command
Set the multiple value of hello time of a specified bridge	stp timeout-factor <i>number</i>
Restore the default multiple value of hello time	undo stp timeout-factor

It is recommended to set 5, 6 or 7 as the value of multiple in the steady network.

By default, the multiple value of hello time of the bridge is 3.

Specifying the Maximum Transmission Rate of STP Packets on a Port

The maximum transmission rate of STP packets on an Ethernet port is dependent on the physical status of the port and the network architecture. You can specify it as needed.

You can specify the maximum transmission rate on a port by using the following commands.

Perform the following configuration in Ethernet Interface View.

Table 180 Specifying the Maximum Transmission Rate of STP Packets on a Port

Operation	Command
Specify the maximum transmission rate of STP packets on a port	stp transmit-limit <i>packetnum</i>
Restore the default transmission rate of STP packets on a port	undo stp transmit-limit

Notably, though a higher transmission rate is introduced at larger *Packetnum*, more Switch resources are consequently occupied. It is therefore recommended to use the default value.

By default, an Ethernet port can transmit at most 3 STP packets within one Hello Time.

Set Specified Port to be an EdgePort

EdgePort is not connected to any Switch directly or indirectly via the connected network.

You can use the following command to set a specified port as an EdgePort.

Perform the following configurations in Ethernet Port View.

Table 181 Set Specified Port as the EdgePort

Operation	Command
Set a specified port as an EdgePort or a non-EdgePort	stp edged-port { enable disable }
Set the specified port as the non-EdgePort, as defaulted	undo stp edged-port

In the process of recalculating the spanning tree, the EdgePort can transfer to the forwarding state directly and reduce unnecessary transition time. If the current

Ethernet port is not connected with any Ethernet port of other bridges, this port should be set as an EdgePort. If a specified port connected to a port of any other bridge is configured as an edge port, RSTP will automatically detect and reconfigure it as a non-EdgePort.

After the network topology changed, if a configured non-EdgePort changes to an EdgePort and is not connected to any other port, it is recommended to configure it as an EdgePort manually because RSTP cannot configure a non-EdgePort as an EdgePort automatically.

Configure the port directly connected to the terminal as an EdgePort, so that the port can transfer immediately to the forwarding state.

By default, all the Ethernet ports are configured as non-EdgePort.

Specifying the Path Cost on a Port

Path Cost is a parameter related with the link rate.

Specify the Path Cost on a Port

You can specify the Path Cost on a port by using the following commands.

Perform the following configuration in Ethernet Interface View.

Table 182 Specifying the Path Cost on a Port

Operation	Command
Specify the Path Cost on a port	<code>stp cost cost</code>
Restore the default Path Cost on the port	<code>undo stp cost</code>

The path cost on an Ethernet port is related to the transmission rate of the link the port connects to. The larger the link rate is, the smaller the path cost shall be. RSTP can automatically detect the link rate and calculate the path cost for the current Ethernet port. The configuration of path cost brings about the re-calculation of the spanning tree. It is recommended to adopt the default value, with which RSTP will automatically calculate the path cost of the current port.

By default, the Switch calculates the path cost directly from the link rate.

Specify the Standard to be Followed in Path Cost Calculation

The following two standards are currently available on the Switch:

- **dot1d-1998:** The Switch calculates the default Path Cost of a port by the IEEE 802.1D-1998 standard.
- **dot1t:** The Switch calculates the default Path Cost of a port by the IEEE 802.1t standard.

You can specify the intended standard by using the following commands.

Perform the following configuration in System View.

Table 183 Specifying the Standard to be Followed in Path Cost Calculation

Operation	Command
Specify the standard to be adopted when the Switch calculates the default Path Cost for the connected link	<code>stp pathcost-standard { dot1d-1998 dot1t }</code>

Operation	Command
Restore the default standard to be used	undo stp pathcost-standard

By default, the Switch calculates the default Path Cost of a port by the IEEE 802.1t standard.

Set the Priority of a Specified Port

The port priority is an important basis to decide if the port can be a root port. In the calculation of the spanning tree, the port with the highest priority will be selected as the root assuming all other conditions are the same.

You can use the following command to set the priority of a specified port.

Perform the following configurations in the Ethernet Port View.

Table 184 Set the Priority of a Specified Port

Operation	Command
Set the priority of a specified port	stp port priority port_priority
Restore the default priority of the specified port	undo stp port priority

By setting the priority of an Ethernet port, you can put a specified Ethernet port into the final spanning tree. Generally, the lower the value is set, the higher priority the port has and the more likely it is for this Ethernet port to be included in the spanning tree. If all the Ethernet ports of the bridge adopt the same priority parameter value, then the priority of these ports depends on the Ethernet port index number. Note that changing the priority of Ethernet port will cause recalculation of the spanning tree. You can set the port priority at the time when setting up the networking requirements.

By default, priorities of all the Ethernet ports are 128.

Configure a Specified Port to be Connected to Point-to-Point Link

Generally, a point-to-point link connects the Switches.

You can use the following command to configure a specified port to be connected to a point-to-point link.

Perform the following configurations in the Ethernet Port View.

Table 185 Configure a Specified Port to be Connected to a Point-to-Point Link

Operation	Command
Configure a specified port to be connected to a point-to-point link	stp point-to-point force-true
Configure a specified port not to be connected to a point-to-point link	stp point-to-point force-false
Configure RSTP to automatically detect if the port is connected to a point-to-point link.	stp point-to-point auto
Configure the port to be automatically detected if it is connected to a point-to-point link, as defaulted	undo stp point-to-point

The two ports connected via the Point-to-Point link can enter the forwarding state rapidly by transmitting synchronous packets, so that the unnecessary forwarding delay can be reduced. If this parameter is configured to be **auto** mode, RSTP can automatically detect if the current Ethernet port is connected to a Point-to-Point

link. Note that, for an aggregated port, only the master port can be configured to connect with the point-to-point link. After auto-negotiation, the port working in full duplex can also be configured to connect with such a link.

You can manually configure the active Ethernet port to connect with the point-to-point link. However, if the link is not a point-to-point link, the command may cause a system problem, and therefore it is recommended to set it as **auto** mode.

By default, this parameter is configured to **auto**, namely in auto mode.

Set mCheck of the Specified Port

RSTP is STP-compatible, so on a Switching network it does not matter if some Switches are running STP and other Switches are running RSTP. In a relatively stable network though the bridge running STP has been removed, the port of the Switch running RSTP is still working in STP-compatible mode. You can use the following command to manually configure the port to work in RSTP mode. This command can only be issued if the bridge runs RSTP in RSTP mode and has no effect in the STP-compatible mode.

You can use the following command to configure mCheck of a specified port.

Perform the following configuration in Ethernet Port View or System View.

Table 186 Set mCheck of the Specified Port

Operation	Command
Set mCheck of the specified port	stp mcheck

This command can be used when the bridge runs RSTP in RSTP mode, but it cannot be used when the bridge runs RSTP in STP-compatible mode.

Configure the Switch Security Function

An RSTP Switch provides BPDU protection and root protection functions.

It looks like 'flapping' refers to Spanning Tree reconfiguring its topology, which may cause links to switch state.

For an access device, the access port is generally directly connected to the user terminal, for example, a PC or a file server, and the access port is set to EdgePort to implement fast transition. When such a port receives a BPDU packet, the system will automatically set it as a non-edge port and recalculate the spanning tree, which causes the network topology to reconfigure and may cause links to switch state. In normal cases, these ports will not receive STP BPDU. If someone forges a BPDU to attack the Switch, the network topology to reconfigure. BPDU protection function is used against such network attack.

In case of configuration error or malicious attack, the primary root may receive the BPDU with a higher priority and then lose its place, which causes network topology change errors. Due to the erroneous change, the traffic supposed to travel over the high-speed link may be pulled to the low-speed link and congestion will occur on the network. Root protection function is used against such problem.

The root port and other blocked ports maintain their state according to the BPDUs sent by the uplink Switch. Once the link is blocked or encountering a faulty condition, the ports cannot receive BPDUs and the Switch will select the root port

again. In this case, the former root port will turn into a BPDU specified port and the former blocked ports will enter into a forwarding state, as a result, a link loop will be generated.

The security functions can control the generation of loops. After it is enabled, the root port cannot be changed, the blocked port will remain in "Discarding" state and will not forward packets, thus avoiding link loops.

You can use the following command to configure the security functions of the Switch.

Perform the following configuration in corresponding views.

Table 187 Configure the Switch Security Function

Operation	Command
Configure Switch BPDU protection (from System View)	stp bpdu-protection
Restore the disabled BPDU protection state, as defaulted, (from System View).	undo stp bpdu-protection
Configure Switch Root protection (from Ethernet Port View)	stp root-protection
Restore the disabled Root protection state, as defaulted, (from Ethernet Port View)	undo stp root-protection
Configure Switch loop protection function (from Ethernet Port View)	stp loop-protection
Restore the disabled loop protection state, as defaulted (from Ethernet Port View)	undo stp loop-protection

After being configured with BPDU protection, the Switch will disable the edge port through RSTP, which receives a BPDU, and notify the network manager at the same time. Only the network manager can resume these ports.

The port configured with Root protection only plays a role of a designated port. Whenever such a port receives a higher-priority BPDU when it is about to turn into a non-designated port, it will be set to a listening state and not forward packets any more (as if the link to the port is disconnected). If the port has not received any higher-priority BPDU for a certain period of time thereafter, it will resume to the normal state.

When you configure a port, only one configuration at a time can be effective among loop protection, root protection, and edge port configuration.

By default, the Switch does not enable loop protection, BPDU protection or Root protection.

For detailed information about the configuration commands, refer to the *Command Reference Guide*.

Display and Debug RSTP

After the above configuration, execute **display** command in all views to display the running of the RSTP configuration, and to verify the effect of the configuration. Execute **reset** command in User View to clear the statistics of RSTP module. Execute **debugging** command in User View to debug the RSTP module.

Table 188 Display and Debug RSTP

Operation	Command
Display RSTP configuration information about the local Switch and the specified ports	display stp [interface interface_list]
Display the list of STP-Ignored VLANs	display stp ignored-vlan
Clear RSTP statistics information	reset stp [interface interface_list]
Enable RSTP (error/event/packet) debugging	debugging stp { error event packet }
Disable RSTP debugging	undo debugging stp { error event packet }

RSTP Configuration Example

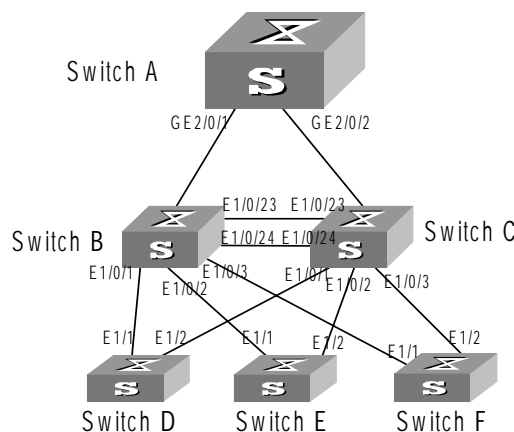
Networking Requirements

In the following scenario, Switch C serves as a standby of Switch B and forwards data when a fault occurs on Switch B. They are connected to each other with two links, so that, in case one of the links fails, the other one can still work normally. Switch D through Switch F are directly connected with the downstream user computers and they are connected to Switch C and Switch B with uplink ports.

You can configure RSTP on the Switch B through Switch F to meet these requirements.

Only the configurations related to RSTP are listed in the following procedure. Switch A serves as the root. Switch D through Switch F are configured in same way basically, so only the RSTP configuration on Switch D will be introduced.

Networking Diagram

Figure 54 RSTP Configuration Example

Configuration Procedure

- 1 Configure Switch A
 - a Enable RSTP globally.


```
[4500]stp enable
```
 - b The port RSTP defaults are enabled after global RSTP is enabled. You can disable RSTP on those ports that are not involved in the RSTP calculation,

however, be careful and do not disable those involved. (The following configuration takes GigabitEthernet 1/0/25 as an example.)

```
[4500]interface gigabitEthernet 1/0/25
[4500-GigabitEthernet1/0/25]stp disable
```

- c To configure Switch A as a root, you can either configure the Bridge priority of it as 0 or simply use the command to specify it as the root.

Set the Bridge priority of Switch A to 0

```
[4500]stp priority 0
```

- d Designate Switch A as the root, using the following command.

```
[4500]stp root primary
```

- e Enable the Root protection function on every designated port.

```
[4500]interface GigabitEthernet 2/0/1
[4500-GigabitEthernet2/0/1]stp root-protection
[4500]interface GigabitEthernet 2/0/2
[4500-GigabitEthernet2/0/2]stp root-protection
```

2 Configure Switch B

- a Enable RSTP globally.

```
[4500]stp enable
```

- b The port RSTP defaults are enabled after global RSTP is enabled. You can disable RSTP on those ports that are not involved in RSTP calculation, however, be careful and do not disable those involved. (The following configuration takes Ethernet 1/0/4 as an example.)

```
[4500]interface Ethernet 1/0/4
[4500-Ethernet1/0/4]stp disable
```

- c Configure Switch C and Switch B to serve as standby of each other and sets the Bridge priority of Switch B to 4096.

```
[4500]stp priority 4096
```

- d Enable the Root protection function on every designated port.

```
[4500]interface Ethernet 1/0/1
[4500-Ethernet1/0/1]stp root-protection
[4500]interface Ethernet 1/0/2
[4500-Ethernet1/0/2]stp root-protection
[4500]interface Ethernet 1/0/3
[4500-Ethernet1/0/3]stp root-protection
```

RSTP operating mode, time parameters, and port parameters take default values.

3 Configure Switch C

- a Enable RSTP globally.

```
[4500]stp enable
```

- b The port RSTP defaults are enabled after global RSTP is enabled. You can disable RSTP on those ports that are not involved in RSTP calculation, however, be careful and do not disable those involved. (The following configuration takes Ethernet 1/0/4 as an example.)

```
[4500]interface Ethernet 1/0/4
[4500-Ethernet1/0/4]stp disable
```

- c Configure Switch C and Switch B to serve as standby of each other and sets the Bridge priority of Switch C to 8192.

```
[4500]stp priority 8192
```

- d Enable the Root protection function on every designated port.

```
[4500]interface Ethernet 1/0/1
[4500-Ethernet1/0/1]stp root-protection
[4500]interface Ethernet 1/0/2
[4500-Ethernet1/0/2]stp root-protection
[4500]interface Ethernet 1/0/3
[4500-Ethernet1/0/3]stp root-protection
```

RSTP operating mode, time parameters, and port parameters take default values.

4 Configure Switch D

- a Enable RSTP globally.

```
[4500]stp enable
```

- b The port RSTP defaults are enabled after global RSTP is enabled. You can disable RSTP on those ports that are not involved in RSTP calculation, however, be careful and do not disable those involved. (The following configuration takes Ethernet 1/3 as an example.)

```
[4500]interface Ethernet 1/3
[4500-Ethernet1/3]stp disable
```

- c Configure the ports (Ethernet 0/1 through Ethernet 0/24) directly connected to users as edge ports and enables BPDU PROTECTION function. (Take Ethernet 0/1 as an example.)

```
[4500]interface Ethernet 1/3
[4500-Ethernet1/3]stp edged-port enable
[4500-Ethernet1/3]quit
[4500]stp bpdu-protection
```

RSTP operating mode, time parameters, and port parameters take default values.

11

802.1X CONFIGURATION

This chapter covers the following topics:

- [IEEE 802.1X Overview](#)
- [Configuring 802.1X](#)
- [AAA and RADIUS Protocol Configuration](#)

For information on setting up a RADIUS server and RADIUS client refer to [Appendix B](#).

For details on how to authenticate the Switch 4500 with a Cisco Secure ACS server with TACACS+, refer to [Appendix C](#).

IEEE 802.1X Overview

IEEE 802.1X (hereinafter simplified as 802.1X) is a port-based network access control protocol that is used as the standard for LAN user access authentication.

In the LANs complying with the IEEE 802 standards, the user can access the devices and share the resources in the LAN through connecting the LAN access control device like the LAN Switch. However, in telecom access, commercial LAN (a typical example is the LAN in the office building) and mobile office and so on, the LAN providers generally hope to control the user's access. In these cases, the requirement on the above-mentioned "Port Based Network Access Control" originates.

As the name implies, "Port Based Network Access Control" means to authenticate and control all the accessed devices on the port of LAN access control device. If the user's device connected to the port can pass the authentication, the user can access the resources in the LAN. Otherwise, the user cannot access the resources in the LAN. It equals that the user is physically disconnected.

802.1X defines port based network access control protocol and only defines the point-to-point connection between the access device and the access port. The port can be either physical or logical. The typical application environment is as follows: Each physical port of the LAN Switch only connects to one user workstation (based on the physical port) and the wireless LAN access environment defined by the IEEE 802.11 standard (based on the logical port), etc.

802.1X System Architecture

The system using the 802.1X is the typical C/S (Client/Server) system architecture. It contains three entities, which are illustrated in the following figure: Supplicant System (User), Authenticator System and Authentication Server System.

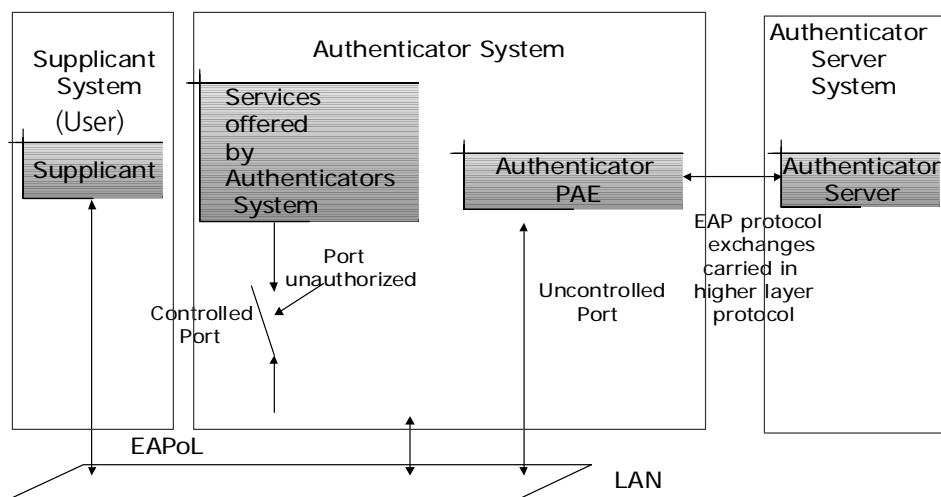
The LAN access control device needs to provide the Authenticator System of 802.1X. The devices at the user side such as the computers need to be installed with the 802.1X client Supplicant (User) software, for example, the 802.1X client

provided by 3Com (or by Microsoft Windows XP). The 802.1X Authentication Server system normally stays in the carrier's AAA center.

Authenticator and Authentication Server exchange information through EAP (Extensible Authentication Protocol) frames. The user and the Authenticator exchange information through the EAPoL (Extensible Authentication Protocol over LANs) frame defined by IEEE 802.1X. Authentication data are encapsulated in the EAP frame, which is to be encapsulated in the packets of other AAA upper layer protocols (for example, RADIUS) so as to go through the complicated network to reach the Authentication Server. Such procedure is called EAP Relay.

There are two types of ports for the Authenticator. One is the Uncontrolled Port, and the other is the Controlled Port. The Uncontrolled Port is always in bi-directional connection state. The user can access and share the network resources any time through the ports. The Controlled Port will be in connecting state only after the user passes the authentication. Then the user is allowed to access the network resources.

Figure 55 802.1X System Architecture



802.1X Authentication Process

802.1X configures EAP frame to carry the authentication information. The Standard defines the following types of EAP frames:

- EAP-Packet: Authentication information frame, used to carry the authentication information.
- EAPoL-Start: Authentication originating frame, actively originated by the user.
- EAPoL-Logoff: Logoff request frame, actively terminating the authenticated state.
- EAPoL-Key: Key information frame, supporting to encrypt the EAP packets.
- EAPoL-Encapsulated-ASF-Alert: Supports the Alerting message of Alert Standard Forum (ASF).

The EAPoL-Start, EAPoL-Logoff and EAPoL-Key only exist between the user and the Authenticator. The EAP-Packet information is re-encapsulated by the Authenticator System and then transmitted to the Authentication Server System.

The EAPoL-Encapsulated-ASF-Alert is related to the network management information and terminated by the Authenticator.

Although 802.1X provides user ID authentication, 802.1X itself is not enough to implement the scheme. The administrator of the access device should configure the AAA scheme by selecting RADIUS or local authentication to assist 802.1X to implement the user ID authentication. For detailed description of AAA, refer to the corresponding AAA configuration.

Implementing 802.1X on the Switch

The Switch 4500 Family not only supports the port access authentication method regulated by 802.1X, but also extends and optimizes it in the following way:

- Support to connect several End Stations in the downstream via a physical port.
- The access control (or the user authentication method) can be based on port or MAC address.
- In this way, the system becomes much securer and easier to manage.

Configuring 802.1X

The configuration tasks of 802.1X itself can be fulfilled in System View of the Ethernet switch. When the global 802.1X is not enabled, you can configure the 802.1X state of the port. The configured items will take effect after the global 802.1X is enabled.



When 802.1X is enabled on a port, the maximum number of MAC address learning which is configured by the command `mac-address max-mac-count` cannot be configured on the port, and vice versa.

The main 802.1X configuration includes:

- Enabling/disabling 802.1X
- Setting the port access control mode
- Setting the port access control method
- Checking the users that log on the Switch via proxy
- Setting the maximum number of users via each port
- Setting the Authentication in DHCP Environment
- Configuring the authentication method for 802.1X user
- Setting the maximum times of authentication request message retransmission
- Configuring timers
- Enabling/disabling a quiet-period timer

Among the above tasks, the first one is compulsory, otherwise 802.1X will not take any effect. The other tasks are optional. You can perform the configurations at requirements.

Enabling/Disabling 802.1X

The following command can be used to enable/disable the 802.1X on the specified port or globally. When it is used in System View, if the parameter `interface-list` is not specified, 802.1X will be globally enabled. If the parameter `interface-list` is specified, 802.1X will be enabled on the specified port. When

this command is used in Ethernet port view, the parameter *interface-list* cannot be input and 802.1X can only be enabled on the current port..

Perform the following configurations in System View or Ethernet Port View.

Table 189 Enabling/Disabling 802.1X

Operation	Command
Enable the 802.1X	dot1x [interface <i>interface_list</i>]
Disable the 802.1X	undo dot1x [interface <i>interface_list</i>]

You can configure 802.1X on an individual port before it is enabled globally. The configuration will take effect after 802.1X is enabled globally.

By default, 802.1X authentication has not been enabled globally and on any port.

Setting the Port Access Control Mode

The following commands can be used for setting 802.1X access control mode on the specified port. When no port is specified, the access control mode of all ports is configured.

Perform the following configurations in System View or Ethernet Port View.

Table 190 Setting the Port Access Control Mode.

Operation	Command
Set the port access control mode.	dot1x port-control { authorized-force unauthorized-force auto } [interface <i>interface_list</i>]
Restore the default access control mode of the port.	undo dot1x port-control [interface <i>interface_list</i>]

By default, the mode of 802.1X performing access control on the port is **auto** (automatic identification mode, which is also called protocol control mode). That is, the initial state of the port is unauthorized. It only permits EAPoL packets receiving/transmitting and does not permit the user to access the network resources. If the authentication flow is passed, the port will be switched to the authorized state and permit the user to access the network resources. This is the most common case.

Setting the Port Access Control Method

The following commands are used for setting 802.1X access control method on the specified port. When no port is specified in System View, the access control method of the port is configured globally.

Perform the following configurations in System View or Ethernet Port View.

Table 191 Setting the Port Access Control Method

Operation	Command
Set port access control method	dot1x port-method { macbased portbased } [interface <i>interface_list</i>]
Restore the default port access control method	undo dot1x port-method [interface <i>interface_list</i>]

By default, 802.1X authentication method on the port is **macbased**. That is, authentication is performed based on MAC addresses.

Checking the Users that Log on the Switch via Proxy

The following commands are used for checking the users that log on the Switch via proxy.

Perform the following configurations in System View or Ethernet Port View.

Table 192 Checking the Users that Log on the Switch via Proxy

Operation	Command
Enable the check for access users via proxy	dot1x supp-proxy-check { logoff trap } [interface <i>interface_list</i>]
Cancel the check for access users via proxy	undo dot1x supp-proxy-check { logoff trap } [interface <i>interface_list</i>]

These commands can be used to check on the specified interface when executed in system view. The parameter *interface-list* cannot be input when the command is executed in Ethernet Port view and it has effect only on the current interface. After globally enabling proxy user detection and control in system view, only if you enable this feature on a specific port can this configuration take effect on the port.

Setting the User Number on a Port

The following commands are used for setting the number of users allowed by 802.1X on a specified port. When no port is specified, all the ports accept the same number of users.

Perform the following configurations in System View or Ethernet Port View.

Table 193 Setting the Maximum Number of Users via a Specified Port

Operation	Command
Set maximum number of users via specified port	dot1x max-user <i>user_number</i> [interface <i>interface_list</i>]
Restore the maximum number of users on the port to the default value	undo dot1x max-user [interface <i>interface_list</i>]

By default, 802.1X allows up to 256 users on each port for Series 4500 Switches.

Setting the Authentication in DHCP Environment

If in a DHCP environment the users configure static IP addresses, you can set 802.1X to disable the Switch to trigger the user ID authentication over them with the following command.

Perform the following configurations in System View.

Table 194 Setting the Authentication in DHCP Environment

Operation	Command
Disable the switch to trigger the user ID authentication over the users who configure static IP addresses in DHCP environment	dot1x dhcp-launch
Enable the switch to trigger the authentication over them	undo dot1x dhcp-launch

By default, the Switch can trigger the user ID authentication over the users who configure static IP addresses in DHCP environment.

Configuring the Authentication Method for 802.1X User

The following commands can be used to configure the authentication method for 802.1X user. Three methods are available: PAP authentication (the RADIUS server must support PAP authentication), CHAP authentication (the RADIUS server must support CHAP authentication), EAP relay authentication (the Switch sends authentication information to the RADIUS server in the form of EAP packets directly and the RADIUS server must support EAP authentication). You can use EAP authentication in one of the four sub-methods: PEAP, EAP-TLS, EAP-TTLS and EAP-MD5.

Perform the following configurations in System View.

Table 195 Configuring the Authentication Method for 802.1X User

Operation	Command
Configure authentication method for 802.1X user	<code>dot1x authentication-method { chap pap eap }</code>
Restore the default authentication method for 802.1X user	<code>undo dot1x authentication-method</code>

By default, CHAP authentication is used for 802.1X user authentication.

Setting the Maximum Times of Authentication Request Message Retransmission

The following commands are used for setting the maximum retransmission times of the authentication request message that the Switch sends to the user.

Perform the following configurations in System View.

Table 196 Setting the Maximum Times of the Authentication Request Message Retransmission

Operation	Command
Set the maximum times of the authentication request message retransmission	<code>dot1x retry max_retry_value</code>
Restore the default maximum retransmission times	<code>undo dot1x retry</code>

By default, the *max-retry-value* is 3. That is, the Switch can retransmit the authentication request message to a user for a maximum of 3 times.

Configuring Timers

The following commands are used for configuring the 802.1X timers.

Perform the following configurations in System View.

Table 197 Configuring Timers

Operation	Command
Configure timers	<code>dot1x timer { { handshake-period handshake-period-value quiet-period quiet-period-value tx-period tx_period_value supp-timeout supp_timeout_value server-timeout server_timeout_value }</code>
Restore default settings of the timers	<code>undo dot1x timer { handshake-period quiet-period tx-period supp-timeout server-timeout }</code>

handshake-period: This timer begins after the user has passed the authentication. After setting handshake-period, system will send the handshake packet by the period. Suppose the dot1x retry time is configured as N, the system

will consider the user having logged off and set the user as logoff state if system doesn't receive the response from user for consecutive N times.

handshake-period-value: Handshake period. The value ranges from 1 to 1024 in units of second and defaults to 15.

quiet-period: Specify the quiet timer. If an 802.1X user has not passed the authentication, the Authenticator will keep quiet for a while (which is specified by **quiet-period** timer) before launching the authentication again. During the quiet period, the Authenticator does not do anything related to 802.1X authentication.

quiet-period-value: Specify how long the quiet period is. The value ranges from 10 to 120 in units of second and defaults to 60.

server-timeout: Specify the timeout timer of an Authentication Server. If an Authentication Server has not responded before the specified period expires, the Authenticator will resend the authentication request.

server-timeout-value: Specify how long the duration of a timeout timer of an Authentication Server is. The value ranges from 100 to 300 in units of second and defaults to 100.

supp-timeout: Specify the authentication timeout timer of a user. After the Authenticator sends a Request/Challenge request packet to request the MD5 encrypted text, the supp-timeout timer of the Authenticator begins to run. If the user does not respond back successfully within the time range set by this timer, the Authenticator will resend the above packet.

supp-timeout-value: Specify how long the duration of an authentication timeout timer of a user is. The value ranges from 10 to 120 in units of second, and defaults to 30.

tx-period: Specify the transmission timeout timer. After the Authenticator sends a Request/Identity request packet which requests the user name, or the user name and password together the tx-period timer of the Authenticator begins to run. If the user does not respond back successfully with an authentication reply packet, then the Authenticator will resend the authentication request packet.

tx-period-value: Specify how long the duration of the transmission timeout timer is. The value ranges from 10 to 120 in units of second, and defaults to 30.

Enabling/Disabling a Quiet-Period Timer

You can use the following commands to enable/disable a quiet-period timer of an Authenticator (which can be a Switch 4500). If an 802.1X user has not passed the authentication, the Authenticator will keep quiet for a while (which is specified by **dot1x timer quiet-period** command) before launching the authentication again. During the quiet period, the Authenticator does not do anything related to 802.1X authentication.

Perform the following configuration in System View.

Table 198 Enabling/Disabling a Quiet-Period Timer

Operation	Command
Enable a quiet-period timer	dot1x quiet-period

Operation	Command
Disable a quiet-period timer	<code>undo dot1x quiet-period</code>

By default, the quiet-period timer is disabled.

Displaying and Debugging 802.1X

After the above configuration, execute `display` command in any view to display the running of the VLAN configuration, and to verify the effect of the configuration. Execute `reset` command in User View to reset 802.1X statistics. Execute `debugging` command in User View to debug 802.1X.

Table 199 Displaying and Debugging 802.1X

Operation	Command
Display the configuration, running and statistics information of 802.1X	<code>display dot1x [sessions statistics] [interface interface_list]</code>
Reset the 802.1X statistics information	<code>reset dot1x statistics [interface interface_list]</code>
Enable the error/event/packet/all debugging of 802.1X	<code>debugging dot1x { error event packet all }</code>
Disable the error/event/packet/all debugging of 802.1X.	<code>undo debugging dot1x { error event packet all }</code>

Auto QoS

Auto QoS uses the Filter-ID standard RADIUS attribute.

Table 200 Auto QoS

Auto QoS	Return String	Comment
Filter-id	student	QoS profile name

802.1X Configuration Example

Networking Requirements

As shown in the following figure, the workstation of a user is connected to the port Ethernet 1/0/1 of the Switch.

The switch administrator will enable 802.1X on all the ports to authenticate the users so as to control their access to the Internet. The access control mode is configured as based on the MAC address

All the users belong to the default domain `3com163.net`, which can contain up to 30 users. RADIUS authentication is performed first. If there is no response from the RADIUS server, local authentication will be performed. For accounting, if the RADIUS server fails to account, the user will be disconnected. In addition, when the user is accessed, the domain name does not follow the user name. Normally, if the user's traffic is less than 2 kbps consistently over 20 minutes, they will be disconnected.

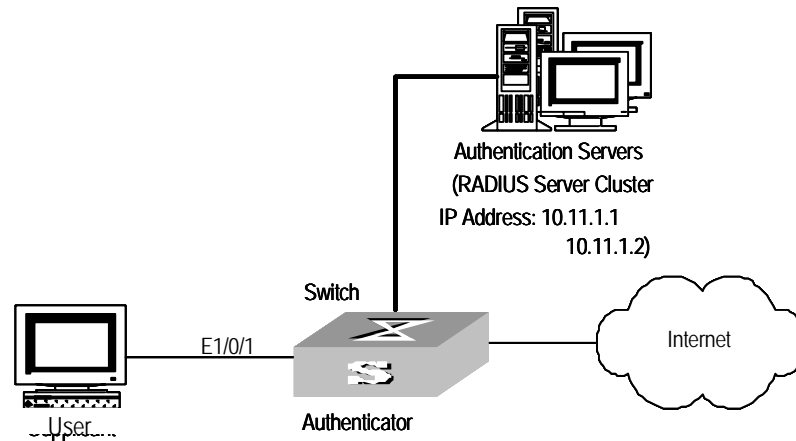
A server group, consisting of two RADIUS servers at 10.11.1.1 and 10.11.1.2 respectively, is connected to the switch. The former one acts as the primary-authentication/second-accounting server. The latter one acts as the secondary-authentication/primary-accounting server. Set the encryption key as "name" when the system exchanges packets with the authentication RADIUS server and "money" when the system exchanges packets with the accounting RADIUS server. Configure the system to retransmit packets to the RADIUS server if no response is received within 5 seconds. Retransmit the packet no more than 5 times in all. Configure the system to transmit a real-time accounting packet to the

RADIUS server every 15 minutes. The system is instructed to transmit the user name to the RADIUS server after removing the user domain name.

The user name of the local 802.1X access user is *localuser* and the password is *localpass* (input in plain text). The idle cut function is enabled.

Networking Diagram

Figure 56 Enabling 802.1X and RADIUS to Perform AAA on the User



Configuration Procedure



The following examples concern most of the AAA/RADIUS configuration commands. For details, refer to the chapter AAA and RADIUS Protocol Configuration.

The configurations of accessing user workstation and the RADIUS server are omitted.

- 1 Enable the 802.1X performance on the specified port Ethernet 1/0/1.


```
[4500]dot1x interface Ethernet 1/0/1
```
- 2 Set the access control mode. (This command could not be configured, when it is configured as MAC-based by default.)


```
[4500]dot1x port-method macbased interface Ethernet 1/0/1
```
- 3 Create the RADIUS scheme radius1 and enters its view.


```
[4500]radius scheme radius1
```
- 4 Set IP address of the primary authentication/accounting RADIUS servers.


```
[4500-radius-radius1]primary authentication 10.11.1.1
[4500-radius-radius1]primary accounting 10.11.1.2
```
- 5 Set the IP address of the second authentication/accounting RADIUS servers.


```
[4500-radius-radius1]secondary authentication 10.11.1.2
[4500-radius-radius1]secondary accounting 10.11.1.1
```
- 6 Set the encryption key when the system exchanges packets with the authentication RADIUS server.


```
[4500-radius-radius1]key authentication name
```

- 7 Set the encryption key when the system exchanges packets with the accounting RADIUS server.

```
[4500-radius-radius1]key accounting money
```
- 8 Set the timeouts and times for the system to retransmit packets to the RADIUS server.

```
[4500-radius-radius1]timer 5
[4500-radius-radius1]retry 5
```
- 9 Set the interval for the system to transmit real-time accounting packets to the RADIUS server.

```
[4500-radius-radius1]timer realtime-accounting 15
```
- 10 Configure the system to transmit the user name to the RADIUS server after removing the domain name.

```
[4500-radius-radius1]user-name-format without-domain
[4500-radius-radius1]quit
```
- 11 Create the user domain 3com163.net and enters isp configuration mode.

```
[4500]domain 3com163.net
```
- 12 Specify radius1 as the RADIUS scheme for the users in the domain 3com163.net.

```
[4500-isp-3com163.net]scheme radius-scheme radius1 local
```
- 13 Set a limit of 30 users to the domain 3com163.net.

```
[4500-isp-3com163.net]access-limit enable 30
```
- 14 Enable idle cut function for the user and set the idle cut parameter in the domain 3com163.net.

```
[4500-isp-3com163.net]idle-cut enable 20 2000
```
- 15 Add a local user and sets its parameter.

```
[4500]local-user localuser
[4500-luser-localuser]service-type lan-access
[4500-luser-localuser]password simple localpass
```
- 16 Enable the 802.1X globally.

```
[4500]dot1x
```

Centralized MAC Address Authentication

Centralized MAC address authentication is a type of authentication method that controls the user network access rights using the port and MAC address. It requires no client software for the user and uses the user's MAC address as the user name and password. The authentication to the user initiates after the Switch detects the user's MAC address for the first time.

The Switch 4500 supports local and RADIUS MAC address authentication. When it functions as the RADIUS client and works with the RADIUS server to finish the MAC address authentication, it sends the detected user MAC address used as the user name and password to the RADIUS server and the rest processing is the same to 802.1x. After passing the authentication conducted by the RADIUS server, the user then can access the network.

Centralized MAC Address Authentication Configuration

Centralized MAC address authentication configuration includes:

- Enabling MAC address authentication both globally and on the port
- Configuring domain name used by the MAC address authentication user
- Configuring centralized MAC address authentication timers



CAUTION: Note the following two items in local authentication:

- The MAC address which is used as local user name and password must be in the "HHH" format and exclude hyphens.
- The service type of local user must be set to lan-access.

Enabling MAC Address Authentication Both Globally and On the Port

You can use the following commands to enable/disable the centralized MAC address authentication on the specified port; if you do not specify the port, the feature is enabled globally.

Perform the following configuration in System View or Ethernet Port View.

Table 201 Enabling/Disabling Centralized MAC Address Authentication

Operation	Command
Enable centralized MAC address authentication	mac-authentication [interface <i>interface_list</i>]
Disable centralized MAC address authentication	undo mac-authentication [interface <i>interface_list</i>]

You can configure the centralized MAC address authentication status on the ports first. However, the configuration does not function on each port until the feature has been enabled globally.



Centralized MAC address authentication and 802.1x cannot be used on the same port together.

By default, the centralized MAC address authentication feature is disabled both on each port and globally.

Configuring Centralized MAC Address Authentication Mode

[Table 202](#) lists the operations to configure centralized MAC address authentication mode.

Table 202 Configure centralized MAC address authentication mode

Operation	Command	Description
Enter system view	system-view	
Configure centralized MAC address authentication mode	mac-authentication authmode { usernameasmacaddress usernamefixed }	Optional By default, the authentication mode is MAC address mode.

Configuring the User Name and Password for Fixed Mode

If you configure the centralized MAC address authentication mode to be fixed mode, you need to configure the user name and password for fixed mode.

Table 203 Configure the user name and password for fixed mode

Operation	Command	Description
Enter system view	<code>system-view</code>	—
Configure a user name for fixed mode	<code>mac-authentication authusername <i>username</i></code>	Optional By default, the user name is mac and the password is not required.
Configure the password for fixed mode	<code>mac-authentication authpassword <i>password</i></code>	Required

Configuring Domain Name Used by the MAC Address Authentication User

You can use the following commands to configure the ISP domain used by the centralized MAC address authentication user.

Perform the following configuration in System View.

Table 204 Configuring the ISP Domain used by the Centralized MAC Address Authentication User

Operation	Command
Configure the ISP domain used by the centralized MAC address authentication user	<code>mac-authentication domain <i>isp_name</i></code>
Return to the defaults	<code>undo mac-authentication domain</code>

By default, the domain used by the centralized MAC address authentication user is null, that is, not configured.

Configuring Centralized MAC Address Authentication Timers

Centralized MAC address authentication timers include:

Offline-detect: Sets the time interval for the Switch to detect whether the user is offline. When the Switch detects that the user is offline, it notifies the RADIUS server immediately, and the server stops charging the user from that address.

Quiet: If the authentication to the user fails, the Switch needs a period of quiet time (set by the quiet timer) before it re-authenticates. The Switch does not authenticate during the quiet time.

Server-timeout: During the authentication to the user, if the connection between the Switch and the RADIUS server times out, the Switch denies the user's access to the network on corresponding ports.

Perform the following configuration in System View.

Table 205 Configuring Centralized MAC Address Authentication Timers

Operation	Command
Configure centralized MAC address authentication timers	<code>mac-authentication timer { offline-detect <i>offline_detect_value</i> quiet <i>quiet_value</i> server-timeout <i>server_timeout_value</i> }</code>
Return to the defaults	<code>undo mac-authentication timer { offline-detect quiet server-timeout }</code>

By default, the offline-detect time is 300 seconds; quiet time is 60 seconds; and the server-timeout time is 100 seconds.

Displaying and Debugging Centralized MAC Address Authentication

After the above configuration, perform the **display** command in any view, you can view the centralized MAC address authentication running state and check the configuration result. Perform the **debugging** command in User View, you can debug the centralized MAC address authentication.

Table 206 Displaying and Debugging Centralized MAC Address Authentication

Operation	Command
Display the global information of the centralized MAC address authentication	display mac-authentication [interface interface_list]
Enable the centralized MAC address authentication debugging switch	debugging mac-authentication event
Disable the centralized MAC address authentication debugging switch	undo debugging mac-authentication event

Auto VLAN

Auto VLAN uses three return list attributes to dynamically assign VLAN(s) to a port as the user logs in.

Table 207 Auto VLAN

Auto VLAN	Return String	Comment
Tunnel-Medium-type	802	
Tunnel-Private-Group-ID	2	VLAN value
Tunnel-Type	VLAN	



Before the VLAN is correctly received by the Switch 4500, you need to execute the following command on the Switch 4500 to use standard private-group-ID:

```
[ 4500-xx ]private-group-id mode standard
```

Configuration Example of Centralized MAC Address Authentication

How to enable centralized MAC address authentication both on a port and globally, and how to configure a local user are shown as follows. For other configurations, see ["802.1X Configuration Example"](#).



The configurations of centralized MAC address authentication is similar to 802.1x, their differences are:

- 1) *Enabling centralized MAC address authentication both globally and on a port.*
- 2) *User name and password of the local authentication must be configured to the MAC address of the user.*
- 3) *User name and password on the RADIUS server must be configured to the MAC address of the user.*

The following example shows how to enabling centralized MAC address authentication both on a port and globally, and the way of configuring local user are shown as follows. For other configurations, see

- 1 Enable centralized MAC address authentication on port Ethernet 1/0/2.

```
[ SW4500 ]mac-authentication interface Ethernet 1/0/2
```

2 Add local access user.**a** Set the user name and password.

```
[SW4500]local-user 00e0fc010101
[SW4500-luser-00e0fc010101]password simple 00e0fc010101
```

b Set the service type of the user to lan-access.

```
[SW4500-luser-00e0fc010101]service-type lan-access
```

3 Enable the MAC address authentication globally.

```
[SW4500]mac-authentication
```

4 Configure the ISP domain used by the user.

```
[SW4500]mac-authentication domain 3com163.net
```

For the configuration of the domain 3com163.net, see [“802.1X Configuration Example”](#) on [page 196](#).

AAA and RADIUS Protocol Configuration

Authentication, Authorization and Accounting (AAA) provide a uniform framework used for configuring these three security functions to implement the network security management.

The network security mentioned here refers to access control and it includes:

- Which user can access the network server?
- Which service can the authorized user enjoy?
- How to keep accounts for the user who is using the network resource?

Accordingly, AAA provides the following services:

- Authentication: authenticates if the user can access the network server.
- Authorization: authorizes the user with specified services.
- Accounting: traces network resources consumed by the user.

RADIUS Protocol Overview

As mentioned above, AAA is a management framework, so it can be implemented by some protocols. RADIUS is such a protocol that is frequently used.

What is RADIUS?

Remote Authentication Dial-In User Service, RADIUS for short, is a type of distributed information switching protocol in Client/Server architecture. RADIUS can prevent the network from interruption of unauthorized access and it is often used in the network environments requiring both high security and remote user access. For example, it is often used for managing a large number of scattering dial-in users who use serial ports and modems. RADIUS system is the important auxiliary part of Network Access Server (NAS).

After RADIUS system is started, if the user wants to have the right to access other networks or consume some network resources through connection to NAS (dial-in access server in PSTN environment or a Switch with the access function in an Ethernet environment), NAS, namely RADIUS client end, will transmit user AAA request to the RADIUS server. A RADIUS server has a user database recording all the information of user authentication and network service access. When

receiving a user's request from NAS, the RADIUS server performs AAA through user database query and update and returns the configuration information and accounting data to NAS. Here, NAS controls users and corresponding connections, while the RADIUS protocol regulates how to transmit configuration and accounting information between NAS and RADIUS.

NAS and RADIUS exchange the information with UDP packets. During the interaction, both sides encrypt the packets with keys before uploading user configuration information (for example, password) to avoid being intercepted or stolen.

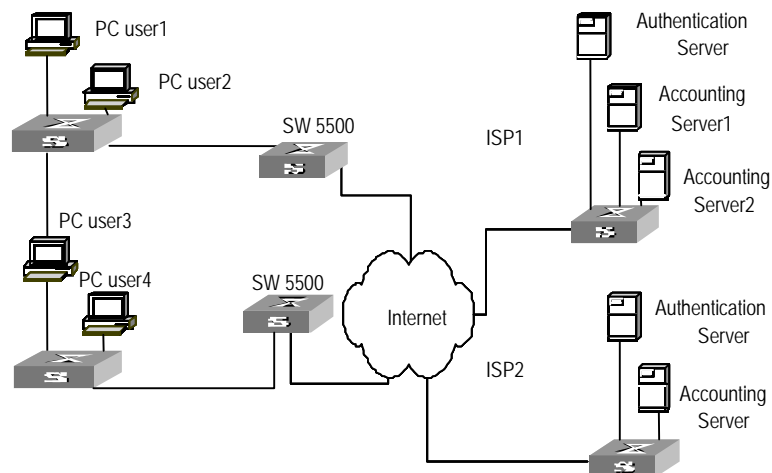
RADIUS Operation

A RADIUS server generally uses proxy function of the devices such as an access server to perform user authentication. The operation process is as follows: First, the user sends a request message (the client username and encrypted password is included in the message) to the RADIUS server. Second, the user will receive from the RADIUS server various kinds of response messages in which the ACCEPT message indicates that the user has passed the authentication, and the REJECT message indicates that the user has not passed the authentication and needs to input their username and password again, otherwise they will be rejected access.

Implementing AAA/RADIUS on the Ethernet Switch

In the above-mentioned AAA/RADIUS framework, the Switch 4500 Family, serving as the user access device or NAS, is the client end of RADIUS. In other words, the AAA/RADIUS concerning the client-end is implemented on the Switch 4500. The figure below illustrates the RADIUS authentication network including 4500 Switches.

Figure 57 Networking when Switch 4500 Units are Applying RADIUS Authentication



Configuring AAA

AAA configuration includes:

- Creating/deleting an ISP domain
- Configuring relevant attributes of the ISP domain
- Creating a local user
- Setting attributes of the local user

- Disconnecting a user by force

Among the above configuration tasks, creating ISP domain is compulsory, otherwise the user attributes cannot be distinguished. The other tasks are optional. You can configure them at requirements.

Creating/Deleting an ISP Domain

What is Internet Service Provider (ISP) domain? To make it simple, ISP domain is a group of users belonging to the same ISP. Generally, for a username in the `userid@isp-name` format, taking `gw20010608@3com163.net` as an example, the `isp-name` (that is, `3com163.net`) following the `@` is the ISP domain name. When the Switch 4500 controls user access, as for an ISP user whose username is in `userid@isp-name` format, the system will take `userid` part as username for identification and take `isp-name` part as domain name.

The purpose of introducing ISP domain settings is to support the multi-ISP application environment. In such an environment, one access device might access users of different ISP. Because the attributes of ISP users, such as username and password formats, and so on, may be different, it is necessary to differentiate them through setting ISP domain. In the Switch 4500 units, ISP domain view, you can configure a complete set of exclusive ISP domain attributes on a per-ISP domain basis, which includes AAA policy (RADIUS scheme applied etc.)

For the Switch 4500, each user belongs to an ISP domain. Up to 16 domains can be configured in the system. If a user has not reported their ISP domain name, the system will put them into the default domain.

Perform the following configurations in System View.

Table 208 Creating/Deleting an ISP Domain

Operation	Command
Create ISP domain or enter the view of a specified domain.	<code>domain isp_name</code>
Remove a specified ISP domain	<code>undo domain isp_name</code>
Enable the default ISP domain specified by <i>isp-name</i>	<code>domain default enable isp_name</code>
Restore the default ISP domain to "system"	<code>domain default disable</code>

By default, a domain named "system" has been created in the system. Its attributes are all default values.

Configuring Relevant Attributes of the ISP Domain

The relevant attributes of ISP domain include the AAA scheme, domain state, maximum number of users, the idle-cut function, the accounting optional option, the messenger alert and self-service server URL.

Perform the following configurations in ISP Domain View.

Configuring AAA Scheme

The AAA schemes includes:

- RADIUS scheme — you can implement authentication, authorization, and accounting by referencing the RADIUS server group. The adopted RADIUS scheme is the one used by all the users in the ISP domain. For detailed

information of the commands of setting RADIUS scheme, refer to the following Configuring RADIUS section of this chapter.

- Local authentication — if you use the local scheme, you can only implement authentication and authorization at local without RADIUS server.
- None — no authentication and accounting.

Table 209 Configuring AAA Scheme Adopted by the ISP Domain

Operation	Command
Configure an AAA scheme for the domain.	scheme { radius-scheme <i>radius_scheme_name</i> local none }
Configure a RADIUS scheme	radius-scheme <i>radius_scheme_name</i>
Restore the default AAA scheme.	undo scheme { radius-scheme <i>radius_scheme_name</i> none }

By default, after an ISP domain is created, the default AAA scheme is **local**. You cannot use a RADIUS scheme together with the **local** or **none** scheme.



*You can use either **scheme** or **radius-scheme** command to specify the RADIUS scheme for an ISP domain. If both of these two commands are used, the latest configuration will take effect.*

Configuring ISP Domain State

Every ISP has active/block states. If an ISP domain is in active state, the users in it can request for network service, while in block state, its users cannot request for any network service, which will not affect the users already online.

Table 210 Configuring ISP Domain State

Operation	Command
Specify the ISP domain state to be active	state active
Specify the ISP domain state to be block	state block

By default, after an ISP domain is created, the state of the domain is **active**.

Setting Access Limit

Maximum number of users specifies how many users can be contained in the ISP. For any ISP domain, there is no limit to the number of users by default.

Table 211 Setting Access Limit

Operation	Command
Set a limit to the amount of users	access-limit { disable enable <i>max_user_number</i> }
Restore the limit to the default setting	undo access-limit

By default, there is no limit to the amount of users.

Enabling/Disabling the Idle-Cut Function

The idle cut function means if the traffic from a certain connection is lower than the defined traffic, this connection is cut off.

Table 212 Enabling/Disabling the Idle-cut Function

Operation	Command
Set the idle	idle-cut enable <i>minute flow</i>

Operation	Command
Disable the idle-cut function	idle-cut disable

By default, the idle-cut function is disabled.

Enabling the Selection of the RADIUS Accounting Option

If no RADIUS server is available or if the RADIUS accounting server fails when the **accounting optional** is configured, the user can still use the network resource, otherwise, the user will be disconnected. The user configured with the **accounting optional** command in RADIUS scheme will no longer send real-time accounting update packets or offline accounting packets.

Perform the following configurations in ISP Domain View.

Table 213 Enabling the Selection of the RADIUS Accounting Option

Operation	Command
Enable the selection of RADIUS accounting option	accounting optional
Disable the selection of RADIUS accounting option	undo accounting optional

By default, the selection of RADIUS accounting option is disabled.

The **accounting optional** command can also be configured in the RADIUS scheme view which is only effective on the accounting that uses this RADIUS scheme. If this command is configured both on an ISP domain and the RADIUS scheme it uses, the latest configuration will take effect.

Enabling/Disabling the Messenger Alert

Messenger alert function allows the clients to inform the online users about their remaining online time through the message alert dialog box.

The implementation of this function is as follows:

- On the switch, use the following command to enable this function and to configure the remaining-online-time threshold (the *limit* argument) and the alert message interval.
- If the threshold is reached, the switch sends messages containing the user's remaining online time to the client at the interval you configured.
- The client keeps the user informed of the updated remaining online time through a dialog box.

Perform the following configuration in ISP domain view.

Table 214 Enabling/disabling message alert

Operation	Command
Enable messenger alert and configure the remaining-online-time threshold and the interval at which the alert message is sent	messenger time enable limit interval
Disable messenger alert	messenger time disable
Restore the messenger alert as the default setting	undo messenger time

By default, messenger alert is disabled on the switch.

Configuring Self-Service Server URL

The `self-service-url enable` command can be used to configure self-service server uniform resource locator (URL). This command must be incorporated with a RADIUS server (such as a CAMS) that supports self-service. Self-service means that users can manage their accounts and card numbers by themselves. And a server with the self-service software is called a self-service server.

Once this function is enabled on the switch, users can locate the self-service server and perform self-management through the following operations:

- Select Change user password on the 802.1X client.
- After the client opens the default explorer (IE or Netscape), locate the specified URL page used to change the user password on the self-service server.
- Change user password on this page.

Perform the following configuration in ISP domain view.

Table 215 Configuring the self-service server URL

Operation	Command
Configure self-service server URL and configure the URL address used to change the user password on the self-service server	self-service-url enable <i>url-string</i>
Remove the configuration of self-service server URL	self-service-url disable

By default, the self-service server URL is not configured on the switch.

Note that, if "?" is contained in the URL, you must replace it with "|" when inputting the URL in the command line.

The "Change user password" option is available only when the user passes the authentication; otherwise, this option is in grey and unavailable.

Creating a Local User

A local user is a group of users set on NAS. The user name is the unique identifier of a user. A user requesting network service may use local authentication only if its corresponding local user has been added onto NAS.

Perform the following configurations in System View

Table 216 Creating/Deleting a Local User and Relevant Properties

Operation	Command
Add local users	local-user <i>user_name</i>
Delete all the local users	undo local-user all
Delete a local user by specifying its type	undo local-user { <i>user_name</i> all [service-type { <i>lan_access</i> ftp telnet ssh terminal }] }

By default, there is no local user in the system.

Setting Attributes of the Local User

The attributes of a local user include its password display mode, state, service type and some other settings.

Setting the Password Display Mode

Perform the following configurations in System View.

Table 217 Setting the Password Display Mode of Local Users

Operation	Command
Set the password display mode of local users	<code>local-user password-display-mode { cipher-force auto }</code>
Cancel the configuration of password display mode	<code>undo local-user password-display-mode</code>

auto means that the password display mode will be the one specified by the user at the time of configuring the password (see the **password** command in [Table 218](#) for reference), and **cipher-force** means that the password display mode of all the accessing users must be in cipher text.

Setting the Attributes of Local Users

Perform the following configurations in Local User View.

Table 218 Setting/Removing the Attributes Concerned with a Specified User

Operation	Command
Set a password for a specified user	<code>password { simple cipher } password</code>
Remove the password set for the specified user	<code>undo password</code>
Set the state of the specified user	<code>state { active block }</code>
Set a priority level for the user	<code>level level</code>
Restore the default priority level	<code>undo level</code>
Set a service type for the specified user	<code>service-type { ftp [ftp-directory directory] lan-access { ssh telnet terminal }* }</code>
Cancel the service type of the specified user	<code>undo service-type { ftp [ftp-directory] lan-access { ssh telnet terminal }* [level level] }</code>
Configure the attributes of lan-access users	<code>attribute { ip ip_address mac mac_address idle-cut second access-limit max_user_number vlan vlanid location { nas-ip ip_address port portnum port portnum } }*</code>
Remove the attributes defined for the lan-access users	<code>undo attribute { ip mac idle-cut access-limit vlan location }*</code>

Note the following two items when you configure these service types: SSH, Telnet or Terminal.

- When you configure a new service type for a user, the system adds the requested service-type to any existing configuration. For example, if the user previously had just Telnet access, and SSH was added, the user would now have access to both Telnet and SSH.
- You can set user level when you configure a service type. If you set multiple service types and specify the user levels, then only the last configured user level is valid. Some of the service types allow a user-privilege level to be entered as an optional extra parameter. For example Telnet, Terminal & SSH.

However, the user-privilege level is a global value for all service types. Entering the following two commands will result in the user having a level of 3 for all service types. In this case both telnet and SSH:

```
[4500-SI-luser-adminpwd]service-type telnet level 1
```

```
[4500-SI-luser-adminpwd]service-type ssh level 3
```



You can use either **level** or **service-type** command to specify the level for a local user. If both of these two commands are used, the latest configuration will take effect.

Disconnecting a User by Force

Sometimes it is necessary to disconnect a user or a category of users by force. The system provides the following command to serve this purpose.

Perform the following configurations in System View.

Table 219 Disconnecting a User by Force

Operation	Command
Disconnect a user by force	cut connection { all access-type { dot1x gcm mac-authentication } domain <i>domain_name</i> interface <i>interface_type interface_number</i> ip ip_address mac <i>mac_address</i> radius-scheme <i>radius_scheme_name</i> vlan <i>vlanid</i> ucibindex <i>ucib_index</i> user-name <i>user_name</i> }

By default, no online user will be disconnected by force.

Configuring the RADIUS Protocol

For the Switch 4500, the RADIUS protocol is configured on the per RADIUS scheme basis. In a real networking environment, a RADIUS scheme can be an independent RADIUS server or a set of primary/secondary RADIUS servers with the same configuration but two different IP addresses. Accordingly, attributes of every RADIUS scheme include IP addresses of primary and secondary servers, shared key and RADIUS server type, etc.

RADIUS protocol configuration only defines some necessary parameters used for information interaction between NAS and RADIUS Server. To make these parameters effective, it is necessary to configure, in the view, an ISP domain to use the RADIUS scheme and specify it to use RADIUS AAA schemes. For more information about the configuration commands, refer to the AAA Configuration section above.

RADIUS protocol configuration includes:

- [Creating/Deleting a RADIUS Scheme](#)
- [Configuring RADIUS Authentication/ Authorization Servers](#)
- [Configuring RADIUS Accounting Servers and the Related Attributes](#)
- [Setting the RADIUS Packet Encryption Key](#)
- [Setting Retransmission Times of RADIUS Request Packet](#)
- [Setting the Supported Type of the RADIUS Server](#)
- [Setting the RADIUS Server State](#)
- [Setting the Username Format Transmitted to the RADIUS Server](#)

- [Configuring the Local RADIUS Authentication Server](#)
- [Configuring Source Address for RADIUS Packets Sent by NAS](#)
- [Setting the Timers of the RADIUS Server](#)

Among the above tasks, creating the RADIUS scheme and setting the IP address of the RADIUS server are required, while other tasks are optional and can be performed as per your requirements.

Creating/Deleting a RADIUS Scheme

As mentioned above, RADIUS protocol configurations are performed on the per RADIUS scheme basis. Therefore, before performing other RADIUS protocol configurations, it is essential to create the RADIUS scheme and enter its view to set its IP address.

You can use the following commands to create/delete a RADIUS scheme.

Perform the following configurations in System View.

Table 220 Creating/Deleting a RADIUS Server Group

Operation	Command
Create a RADIUS scheme and enter its view	radius scheme <i>radius_scheme_name</i>
Delete a RADIUS scheme	undo radius scheme <i>radius_scheme_name</i>

Several ISP domains can use a RADIUS scheme at the same time. You can configure up to 16 RADIUS schemes, including the default scheme named as **system**.

By default, the system has a RADIUS scheme named as `system` whose attributes are all default values. The default attribute values will be introduced in the following text.

Configuring RADIUS Authentication/Authorization Servers

After creating a RADIUS scheme, you have to set IP addresses and UDP port numbers for the RADIUS servers, including primary/secondary authentication/authorization servers and accounting servers. You can configure up to four groups of IP addresses and UDP port numbers. However, as a minimum, you have to set one group of IP address and UDP port number for each pair of primary/secondary servers to ensure the normal AAA operation.

You can use the following commands to configure the IP address and port number for RADIUS servers.

Perform the following configurations in RADIUS Scheme View.

Table 221 Configuring RADIUS Authentication/Authorization Servers

Operation	Command
Set IP address and port number of primary RADIUS authentication/authorization server.	primary authentication <i>ip_address [port_number]</i>
Restore IP address and port number of primary RADIUS authentication/authorization server to the default values.	undo primary authentication

Operation	Command
Set IP address and port number of secondary RADIUS authentication/authorization server.	secondary authentication <i>ip_address [port_number]</i>
Restore IP address and port number of second RADIUS authentication/authorization server to the default values.	undo secondary authentication

By default, as for the newly created RADIUS scheme, the IP address of the primary authentication server is 0.0.0.0, and the UDP port number of this server is 1812; as for the "system" RADIUS scheme created by the system, the IP address of the primary authentication server is 127.0.0.1, and the UDP port number is 1645.

The authorization information from the RADIUS server is sent to RADIUS clients in authentication response packets, so you do not need to specify a separate authorization server.

In real networking environments, you may specify two RADIUS servers as primary and secondary authentication/authorization servers respectively, or specify one server to function as both.

The RADIUS service port settings on the Switch 4500 should be consistent with the port settings on the RADIUS server. Normally, the authentication/authorization service port is 1812.

Configuring RADIUS Accounting Servers and the Related Attributes

Configuring RADIUS Accounting Servers

You can use the following commands to configure the IP address and port number for RADIUS accounting servers.

Perform the following configurations in RADIUS Scheme View.

Table 222 Configuring RADIUS Accounting Servers

Operation	Command
Set IP address and port number of primary RADIUS accounting server.	primary accounting <i>ip_address [port_number]</i>
Restore IP address and port number of primary RADIUS accounting server to the default values.	undo primary accounting
Set IP address and port number of second RADIUS accounting server.	secondary accounting <i>ip_address [port_number]</i>
Restore IP address and port number of second RADIUS accounting server to the default values.	undo secondary accounting

By default, as for the newly created RADIUS scheme, the IP address of the primary accounting server is 0.0.0.0, and the UDP port number of this server is 1813; as for the "system" RADIUS scheme created by the system, the IP address of the primary accounting server is 127.0.0.1, and the UDP port number is 1646.

In real networking environments, you can specify two RADIUS servers as the primary and the secondary accounting servers respectively; or specify one server to function as both.

To guarantee the normal interaction between NAS and RADIUS server, you are supposed to guarantee the normal routes between RADIUS server and NAS before setting the IP address and UDP port of the RADIUS server. In addition, because

RADIUS protocol uses different UDP ports to receive/transmit authentication/authorization and accounting packets, you need to set two different ports accordingly. Suggested by RFC2138/2139, authentication/authorization port number is 1812 and accounting port number is 1813. However, you may use values other than the suggested ones. (Especially for some earlier RADIUS Servers, authentication/authorization port number is often set to 1645 and accounting port number is 1646.)

The RADIUS service port settings on the Switch 4500 units are supposed to be consistent with the port settings on RADIUS server. Normally, RADIUS accounting service port is 1813.

Setting the Maximum Times of Real-time Accounting Request Failing to be Responded to

A RADIUS server usually checks if a user is online with a timeout timer. If the RADIUS server has not received the real-time accounting packet from NAS for a while, it will consider that there is device failure and stop accounting. It is necessary to disconnect the user at the NAS end and on the RADIUS server synchronously when some unpredictable failure occurs. The Switch allows you to set the maximum number of times of a real-time accounting request failing to be responded to. NAS will disconnect the user if it has not received a real-time accounting response from the RADIUS server for the specified number of times.

You can use the following command to set the maximum number of times of a real-time accounting request failing to be responded to.

Perform the following configurations in RADIUS Scheme View.

Table 223 Setting the Maximum Times of Real-time Accounting Request Failing to be Responded

Operation	Command
Set maximum times of real-time accounting request failing to be responded	retry realtime-accounting <i>retry_times</i>
Restore the maximum times to the default value	undo retry realtime-accounting

How to calculate the value of *retry-times*? Suppose that RADIUS server connection will timeout in T and the real-time accounting interval of NAS is t, then the integer part of the result from dividing T by t is the value of *count*. Therefore, when applied, it is suggested that T should be a number that can be divided exactly by t.

By default, the real-time accounting request can fail to be responded to no more than 5 times.

Enabling/Disabling the Stopping Accounting Request Buffer

Because the stopping accounting request concerns the account balance and will affect the amount of charge, which is very important for both the subscribers and the ISP, NAS shall make its best effort to send the message to the RADIUS accounting server. If the message from the Switch to the RADIUS accounting server has not been responded to, the Switch will save it in the local buffer and retransmit it until the server responds or discards the messages after transmitting for the specified number of times. The following command can be used for setting to save the message or not.

Perform the following configurations in RADIUS Scheme View.

Table 224 Enabling/Disabling the Stopping Accounting Request Buffer

Operation	Command
Enable stopping accounting request buffer	stop-accounting-buffer enable
Disable stopping accounting request buffer	undo stop-accounting-buffer enable

By default, the stopping accounting request will be saved in the buffer.

Setting the Maximum Retransmitting Times of Stopping Accounting Request

Use this command to set the maximum number of retransmission times that the Switch will attempt to retransmit the saved message from its local buffer.

Perform the following configurations in RADIUS Scheme View.

Table 225 Setting the Maximum Retransmitting Times of Stopping Accounting Request

Operation	Command
Set the maximum retransmitting times of stopping accounting request	retry stop-accounting <i>retry_times</i>
Restore the maximum retransmitting times of stopping accounting request to the default value	undo retry stop-accounting

By default, the stopping accounting request can be retransmitted up to 500 times.

Enabling the Selection of the Radius Accounting Option

Perform the following configurations in RADIUS Scheme View.

Table 226 Enabling the Selection of RADIUS Accounting Option

Operation	Command
Enable the selection of RADIUS accounting option	accounting optional
Disable the selection of RADIUS accounting option	undo accounting optional

This command can also be configured in ISP Domain View. For details, refer to Configuring Relevant Attributes of the ISP Domain.

Setting the RADIUS Packet Encryption Key

The RADIUS client (Switch system) and the RADIUS server use MD5 algorithm to encrypt the exchanged packets. The two ends verify the packet through setting the encryption key. Only when the keys are identical can both ends accept the packets from each other and give responses.

You can use the following commands to set the encryption key for RADIUS packets.

Perform the following configurations in RADIUS Scheme View.

Table 227 Setting the RADIUS Packet Encryption Key

Operation	Command
Set RADIUS authentication/authorization packet encryption key	key authentication <i>string</i>
Restore the default RADIUS authentication/authorization packet encryption key.	undo key authentication

Operation	Command
Set RADIUS accounting packet key	key accounting <i>string</i>
Restore the default RADIUS accounting packet key	undo key accounting

By default, the keys of RADIUS authentication/authorization and accounting packets are all "3com".

Setting Retransmission Times of RADIUS Request Packet

Since RADIUS protocol uses UDP packets to carry the data, the communication process is not reliable. If the RADIUS server has not responded to NAS before timeout, NAS has to retransmit the RADIUS request packet. If it transmits more than the specified *retry-times*, NAS considers the communication with the primary and secondary RADIUS servers has been disconnected.

You can use the following command to set the retransmission times of the RADIUS request packet.

Perform the following configurations in RADIUS Scheme View.

Table 228 Setting Retransmission Times of RADIUS Request Packet

Operation	Command
Set retransmission times of RADIUS request packet	retry <i>retry-times</i>
Restore the default value of retransmission times	undo retry

By default, RADIUS request packet will be retransmitted up to three times.

Setting the Supported Type of the RADIUS Server

The Switch 4500 supports the standard RADIUS protocol and the extended RADIUS service platforms.

You can use the following command to set the supported types of RADIUS servers. Perform the following configurations in RADIUS Scheme View.

Table 229 Setting the Supported Type of the RADIUS Server

Operation	Command
Setting the Supported Type of RADIUS Server	server-type { <i>3com</i> <i>standard</i> }
Restore the RADIUS server type to the default setting	undo server_type

By default, the newly created RADIUS scheme supports the server type **standard**, while the "system" RADIUS scheme created by the system supports the server type **3com**.

Setting the RADIUS Server State

For the primary and secondary servers (no matter if they are an authentication/authorization server or accounting server), if the primary server is disconnected from the NAS for some fault, the NAS will automatically turn to exchange packets with the secondary server. However, after the primary server recovers, the NAS will not resume the communication with it at once, instead, it continues communicating with the secondary server. When the secondary server fails to communicate, the NAS will turn to the primary server again. The following commands can be used to set the primary server to be **active** manually, in order that NAS can communicate with it immediately after a fault has been resolved.

When the primary and secondary servers are both **active** or **block**, NAS will send the packets to the primary server only.

Perform the following configurations in RADIUS Scheme View.

Table 230 Setting the RADIUS Server State

Operation	Command
Set the state of primary RADIUS server	state primary { accounting authentication } { block active }
Set the state of second RADIUS server	state secondary { accounting authentication } { block active }

By default, for the newly created RADIUS scheme, the primary and secondary accounting/authentication servers are in the state of **block**; for the "system" RADIUS scheme created by the system, the primary accounting/authentication servers are in the state of **active**, and the secondary accounting/authentication servers are in the state of **block**.

Setting the Username Format Transmitted to the RADIUS Server

As mentioned above, the users are generally named in `userid@isp-name` format. The part following "@" is the ISP domain name. The Switch will put the users into different ISP domains according to the domain names. However, some earlier RADIUS servers reject the username including ISP domain name. In this case, you have to remove the domain name before sending the username to the RADIUS server. The following command of switch decides whether the username to be sent to RADIUS server carries ISP domain name or not.

Perform the following configurations in RADIUS Scheme View.

Table 231 Setting the Username Format Transmitted to the RADIUS Server

Operation	Command
Set Username Format Transmitted to RADIUS Server	user-name-format { with-domain without-domain }



If a RADIUS scheme is configured not to allow usernames including ISP domain names, the RADIUS scheme shall not be simultaneously used in more than one ISP domain. Otherwise, the RADIUS server will regard two users in different ISP domains as the same user by mistake, if they have the same username (excluding their respective domain names.)

By default, the RADIUS scheme acknowledges that the username sent to it includes the ISP domain name.

Setting the Unit of Data Flow that Transmitted to the RADIUS Server

The following command defines the unit of the data flow sent to RADIUS server.

Perform the following configurations in RADIUS Scheme View

Table 232 Setting the Unit of Data Flow Transmitted to the RADIUS Server

Operation	Command
Set the unit of data flow transmitted to RADIUS server	data-flow-format data { byte giga-byte kilo-byte mega-byte } packet { giga-byte kilo-byte mega-byte one-packet }
Restore the unit to the default setting	undo data-flow-format

By default, the default data unit is byte and the default data packet unit is one packet.

Configuring the Local RADIUS Authentication Server

RADIUS service adopts authentication/authorization/accounting servers to manage users. Local authentication/authorization/accounting service is also used in these products and it is called local RADIUS authentication server function.

Perform the following commands in System View to create/delete local RADIUS authentication server.

Table 233 Creating/Deleting the Local RADIUS Authentication Server

Operation	Command
Create the local RADIUS authentication server	local-server nas-ip <i>ip_address</i> key <i>password</i>
Delete the local RADIUS authentication server	undo local-server nas-ip <i>ip_address</i>

By default, the IP address of the local RADIUS authentication server is 127.0.0.1 and the password is 3com.



1) When using local RADIUS server function of 3com, remember the number of the UDP port used for authentication is 1645 and that for accounting is 1646.

2) The password configured by this command must be the same as that of the RADIUS authentication/authorization packet configured by the command **key authentication** in RADIUS Scheme View.

Configuring Source Address for RADIUS Packets Sent by NAS

Perform the following configurations in the corresponding view.

Table 234 Configuring Source Address for the RADIUS Packets sent by the NAS

Operation	Command
Configure the source address to be carried in the RADIUS packets sent by the NAS(RADIUS scheme view).	nas-ip <i>ip_address</i>
Cancel the configured source address to be carried in the RADIUS packets sent by the NAS(RADIUS scheme view).	undo nas-ip
Configure the source address to be carried in the RADIUS packets sent by the NAS(System view).	radius nas-ip <i>ip_address</i>
Cancel the configured source address to be carried in the RADIUS packets sent by the NAS(System view).	undo radius nas-ip

You can use either command to bind a source address with the NAS.

By default, no source address is specified and the source address of a packet is the address of the interface to where it is sent.

Setting the Timers of the RADIUS Server

Setting the Response Timeout Timer of the RADIUS Server

After RADIUS (authentication/authorization or accounting) request packet has been transmitted for a period of time, if NAS has not received the response from the RADIUS server, it has to retransmit the request to guarantee RADIUS service for the user.

You can use the following command to set response timeout timer of RADIUS server.

Perform the following configurations in RADIUS Scheme View.

Table 235 Setting the Response Timeout Timer of the RADIUS Server

Operation	Command
Set response timeout timer of RADIUS server	<code>timer second</code>
Restore the response timeout timer of RADIUS server to default value	<code>undo timer</code>

By default, timeout timer of RADIUS server is 3 seconds.

Setting a Real-time Accounting Interval

To implement real-time accounting, it is necessary to set a real-time accounting interval. After the attribute is set, NAS will transmit the accounting information of online users to the RADIUS server regularly.

You can use the following command to set a real-time accounting interval.

Perform the following configurations in RADIUS Scheme View.

Table 236 Setting a Real-time Accounting Interval

Operation	Command
Set a real-time accounting interval	<code>timer realtime-accounting minute</code>
Restore the default value of the interval	<code>undo timer realtime-accounting</code>

minute specifies the real-time accounting interval in minutes. The value should be a multiple of 3.

The value of *minute* is related to the performance of NAS and RADIUS server. The smaller the value, the higher the performances of NAS and RADIUS that are required. When there are a large amount of users (more than 1000, inclusive), 3Com suggests a larger value. The following table recommends the ratio of *minute* value to the number of users.

Table 237 Recommended Ratio of Minute to Number of Users

Number of users	Real-time accounting interval (minute)
1 to 99	3
100 to 499	6
500 to 999	12
1000	15

By default, *minute* is set to 12 minutes.

Configure the RADIUS Server Response Timer

If the NAS receives no response from the RADIUS server after sending a RADIUS request (authentication/authorization or accounting request) for a period of time, the NAS resends the request, thus ensuring the user can obtain the RADIUS service. You can specify this period by setting the RADIUS server response timeout timer, taking into consideration the network condition and the desired system performance.

Perform the following configurations in RADIUS Scheme View.

Table 238 Configure the RADIUS Server Response Timer

Operation	Command
Configure the RADIUS server response timer	timer response-timeout <i>seconds</i>
Restore the default value of the interval	undo timer response-timeout

By default, the response timeout timer for the RADIUS server is set to three seconds.

Displaying and Debugging AAA and RADIUS Protocol

After the above configuration, execute the **display** command in any view to display the running of the AAA and RADIUS configuration, and to verify the effect of the configuration. Execute the **reset** command in User View to reset AAA and RADIUS statistics. Execute the **debugging** command in User View to debug AAA and RADIUS.

Table 239 Displaying and Debugging AAA and RADIUS Protocol

Operation	Command
Display the configuration information of the specified or all the ISP domains.	display domain [<i>isp_name</i>]
Display related information of user's connection	display connection [access-type { dot1x mac-authentication } domain <i>domain_name</i> interface <i>interface_type interface_number</i> ip <i>ip_address</i> mac <i>mac_address</i> radius-scheme <i>radius_scheme_name</i> vlan <i>vlanid</i> ucibindex <i>ucib_index</i> user-name <i>user_name</i>]
Display related information of the local user	display local-user [domain <i>isp_name</i> idle-cut { disable enable } service-type { telnet ftp lan-access ssh terminal } state { active block } user-name <i>user_name</i> vlan <i>vlan_id</i>]
Display the statistics of local RADIUS authentication server	display local-server statistics
Display the configuration information of all the RADIUS schemes or a specified one	display radius [<i>radius_scheme_name</i>]
Display the statistics of RADIUS packets	display radius statistics
Display the stopping accounting requests saved in buffer without response (from System View)	display stop-accounting-buffer { radius-scheme <i>radius_scheme_name</i> session-id <i>session_id</i> time-range <i>start_time stop_time</i> user-name <i>user_name</i> }
Delete the stopping accounting requests saved in buffer without response (from System View)	reset stop-accounting-buffer { radius-scheme <i>radius_scheme_name</i> session-id <i>session_id</i> time-range <i>start_time stop_time</i> user-name <i>user_name</i> }
Clear stop-accounting packets from the buffer	reset stop-accounting-buffer { radius-scheme <i>radius_scheme_name</i> session-id <i>session_id</i> time-range <i>start_time stop_time</i> user-name <i>user_name</i> }
Reset the statistics of RADIUS server	reset radius statistics
Enable RADIUS packet debugging	debugging radius packet
Disable RADIUS packet debugging	undo debugging radius packet

Operation	Command
Enable debugging of local RADIUS scheme	<code>debugging local-server { all error event packet }</code>
Disable debugging of local RADIUS scheme	<code>undo debugging local-server { all error event packet }</code>

AAA and RADIUS Protocol Configuration Example

For the hybrid configuration example of AAA/RADIUS protocol and 802.1X protocol, refer to [“802.1X Configuration Example”](#) on [page 196](#).

Configuring the FTP/Telnet User Authentication at a Remote RADIUS Server



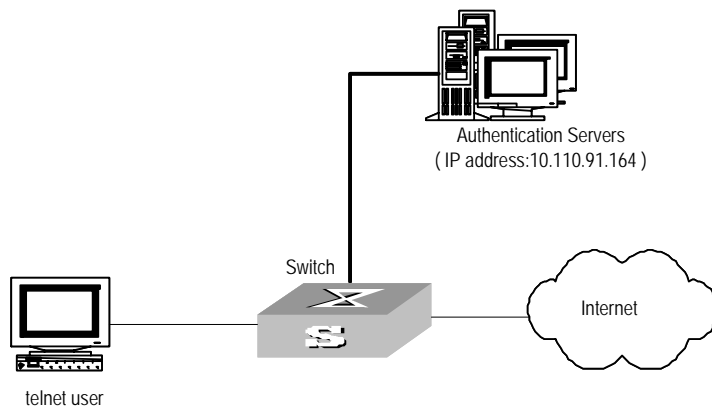
Configuring Telnet user authentication at the remote server is similar to configuring FTP users. The following description is based on Telnet users.

Networking Requirements In [Figure 58](#), it is required to configure the remote RADIUS authentication of Telnet users.

One RADIUS server (as authentication server) is connected to the Switch and the server IP address is 10.110.91.146. The password for exchanging messages between the Switch and the authentication server is "expert". The Switch cuts off the domain name from username and sends the remaining part to the RADIUS server.

Networking Topology

Figure 58 Configuring the Remote RADIUS Authentication for Telnet Users



Configuration Procedure

- 1 Add a Telnet user.



For details about configuring FTP and Telnet users, refer to *User Interface Configuration in the Getting Started* chapter.

- 2 Configure remote authentication mode for the Telnet user, that is, scheme mode.

```
[ 4500-ui-vty0-4 ] authentication-mode scheme
```

- 3 Configure domain.

```
[ 4500 ] domain cams
[ 4500-isp-cams ] quit
```

4 Configure RADIUS scheme.

```
[4500]radius scheme cams
[4500-radius-cams]primary authentication 10.110.91.146 1812
[4500-radius-cams]key authentication expert
[4500-radius-cams]server-type 3com
[4500-radius-cams]user-name-format without-domain
```

5 Configuration association between domain and RADIUS.

```
[4500-radius-cams]quit
[4500]domain cams
[4500-isp-cams]scheme radius-scheme cams
```

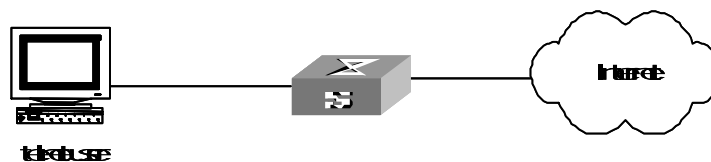
Configuring the FTP/Telnet User Local Authentication

Configuring local authentication for FTP users is similar to that for Telnet users. The following example is based on Telnet users.

Networking Requirements Configure the router to authenticate the login Telnet users locally (see [Figure 59](#)).

Networking Diagram

Figure 59 Local Authentication for Telnet Users

**Configuration Procedure****1** Method 1: Using Local scheme.

a Apply AAA authentication to Telnet users.

```
[4500-ui-vty0-4]authentication-mode scheme
```

b Create a local user telnet.

```
[4500]local-user telnet
[4500-luser-telnet]service-type telnet
[4500-luser-telnet]password simple 3com
[4500-luser-telnet]attribute idle-cut 300 access-limit 5
[4500]domain system
[4500-isp-system]scheme local
```

Telnet users use usernames in the "userid@system" format to log onto the network and are to be authenticated as users of the system domain.

2 Method 2: Using Local RADIUS authentication server.

Local server method is similar to remote RADIUS authentication. But you should modify the server IP address to 127.0.0.1, authentication password to 3com, the UDP port number of the authentication server to 1645.

Configuring the Switch 4500**General RADIUS Setup**

The Switch 4500 supports multiple RADIUS schemes, which can be assigned to a domain.

This guide covers the recommended steps to setup the Switch4500 for login.

Domain and RADIUS Scheme Creation

The Switch 4500 can have 1 or more domains created on it. A domain on the Switch 4500 is similar to a windows domain. By default, there is one domain created called "system". This uses the local scheme to validate users. The information about the local domain can be seen by typing "display domain". For example:

```
<4500>display domain
0 Domain = system
  State = Active
  Scheme = LOCAL
  Access-limit = Disable
  Domain User Template:
  Idle-cut = Disable
  Self-service = Disable
  Messenger Time = Disable
```

This system domain uses the local scheme.

It is not recommended that you change the system domain, as it could result in locking all users out of the switch. This could happen if you change the default local scheme to use an external RADIUS server, which is unavailable.

- 1 A new RADIUS scheme should be created as follows:

```
[4500]radius scheme NewSchemeName
New Radius scheme
[4500-radius-NewSchemeName]
```

- 2 Next, we need to add the attributes of the RADIUS scheme. This involves configuring the RADIUS server IP address and shared secret.

```
[4500-radius-NewSchemeName]key authentication mysharedsecret
[4500-radius-NewSchemeName]primary authentication 161.71.67.250
```

- 3 The RADIUS scheme will not become active unless an accounting server is also defined. If you don't have an accounting server, then the RADIUS scheme needs to have accounting set to "optional".

```
[4500-radius-NewSchemeName]accounting optional
```

- 4 Next, create a new domain as follows:

```
[4500]domain Demo
New Domain added.
[4500-isp-Demo]
```

- 5 Change the domain to use the new RADIUS scheme that you have configured:

```
[4500-isp-demo]radius-scheme NewSchemeName
```

And that completes the configuration of the new radius server and associating it with a domain.

Network Login

Network login must first be enabled globally by issuing the command dot1x:

```
[4500-xx]dot1x
802.1X is enabled globally
```

(where xx is either EI or SI)

Once enabled globally, the network login needs to be enabled on a per port basis. This can be done in one of two ways:

- To enable dot1x on one port, enter the interface of the port and enable dot1x on the port. For example:

```
[4500-xx]interface ethernet 1/0/7
[4500-xx-Ethernet1/0/7]dot1x
802.1X is enabled on port Ethernet1/0/7
[4500-xx-Ethernet1/0/7]
```

- To enable dot1x on more than 1 port, enter the global dot1x command as follows:

```
[4500-xx]dot1x interface Ethernet 1/0/7 to Ethernet 1/0/12
Ethernet 1/0/14 to Ethernet 1/0/20
802.1X is enabled on port Ethernet1/0/7 already
802.1X is enabled on port Ethernet1/0/8
802.1X is enabled on port Ethernet1/0/9
802.1X is enabled on port Ethernet1/0/10
802.1X is enabled on port Ethernet1/0/11
802.1X is enabled on port Ethernet1/0/12
802.1X is enabled on port Ethernet1/0/14
802.1X is enabled on port Ethernet1/0/15
802.1X is enabled on port Ethernet1/0/16
802.1X is enabled on port Ethernet1/0/17
802.1X is enabled on port Ethernet1/0/18
802.1X is enabled on port Ethernet1/0/19
802.1X is enabled on port Ethernet1/0/20
[4500-xx]
```

802.1X login is now enabled on the port. When a device with an 802.1X client connects to the port, the user will be challenged for a username and password. The username should be in the form "user@domain" where "domain" is the name of the domain that was created on the Switch. This will tell the Switch which domain, and subsequently which RADIUS server the user is associated with.

By default, the username sent to the RADIUS server for verification will be in the form user@domain.

You can send the username without the domain extension to the RADIUS server. This can be changed under the RADIUS scheme as follows:

```
[4500-xx-radius-NewSchemeName]user-name-format without-domain
```

Switch Login

The Switch 4500 supports Switch login, to allow multiple users access to the management interface of the switch.

Once the RADIUS scheme and domain have been set up, see [Domain and RADIUS Scheme Creation](#), then switch login is enabled.

By default, when you use the username admin to login, you are actually logging in as "admin@local". If no domain is given, the "@local" is automatically added at

the end of the username. This states the user is a member of the local domain, and as a result uses the local RADIUS server.

Based on the steps in section [Domain and RADIUS Scheme Creation](#) to login using the external RADIUS server defined, you need to login as user@domain, for example, joe@demo. This will try to log you into the demo domain, which uses the external, rather than the internal RADIUS server.

By default, the username sent to the RADIUS server for verification will be in the form user@domain. To just send the username without the domain extension to the RADIUS server. This is changed under the RADIUS scheme as follows:

```
[ 4500-radius-NewSchemeName ]user-name-format without-domain
```

AAA and RADIUS Protocol Fault Diagnosis and Troubleshooting

The RADIUS protocol of the TCP/IP protocol suite is located on the application layer. It mainly specifies how to exchange user information between NAS and RADIUS server of ISP. So it is likely to be invalid.

Fault One: User Authentication/Authorization Always Fails

Troubleshooting:

- The username may not be in the *userid@isp-name* format or NAS has not been configured with a default ISP domain. Use the username in proper format and configure the default ISP domain on NAS.
- The user may have not been configured in the RADIUS server database. Check the database and make sure that the configuration information of the user does exist in the database.
- The user may have input a wrong password. So make sure that the user inputs the correct password.
- The encryption keys of RADIUS server and NAS may be different. Check carefully and make sure that they are identical.
- There might be some communication fault between NAS and RADIUS server, which can be discovered through pinging RADIUS from NAS. So ensure there is normal communication between NAS and RADIUS.

Fault Two: RADIUS Packet Cannot be Transmitted to RADIUS Server

Troubleshooting:

- The communication lines (on physical layer or link layer) connecting NAS and the RADIUS server may not work well. So ensure the lines work well.
- The IP address of the corresponding RADIUS server may not have been set on NAS. Set a proper IP address for RADIUS server.
- UDP ports of authentication/authorization and accounting services may not be set properly. So make sure they are consistent with the ports provided by RADIUS server.

Fault Three: After Being Authenticated and Authorized, the User Cannot Send Charging Bill to the RADIUS Server

Troubleshooting:

- The accounting port number may be set improperly. Please set a proper number.
- The accounting service and authentication/authorization service are provided on different servers, but NAS requires the services to be provided on one server (by specifying the same IP address). So make sure the settings of the servers are consistent with the actual conditions.

Problem Diagnosis The Switch 4500 provides debugging of RADIUS. Terminal debugging can be enabled with the command:

```
<4500-xx>terminal debugging
```

Once enabled, different debug traces can be enabled to the terminal. For example, to turn on RADIUS debugging, enter the command:

```
■ <4500-xx> debugging radius packet
```

3Com-User-Access-Level This determines the Access level a user will have with Switch login. This can be administrator, manager , monitor or visitor.

You may need to add the return list attributes to a dictionary file using the following information:

VENDOR	3Com	43	
ATTRIBUTE	3Com-User-Access-Level	1	Integer 3Com
VALUE	3Com-User-Access-Level	Visit	0
VALUE	3Com-User-Access-Level	Monitor	1
VALUE	3Com-User-Access-Level	Manager	2
VALUE	3Com-User-Access-Level	Administrator	3

12

FILE SYSTEM MANAGEMENT

File System Overview

The Switch provides a flash file system for efficient management of the storage devices such as flash memory. The file system offers file access and directory management, including creating the file system, creating, deleting, modifying and renaming a file or a directory, and opening a file.

By default, the file system requires that the user confirm before executing commands. This prevents unwanted data loss.



In the Switches supporting XRN, the file URL must start with "unit[No.]>flash:/:", the [No.] is the unit ID. For example, suppose unit ID is 1, and the URL of the "text.txt" file under the root directory must be "unit1>flash:/text.txt".

Based on the operated objects, the file system can be divided as follows:

- Directory operation
- File operation
- Storage device operation
- Set the prompt mode of the file system

Directory Operation

You can use the file system to create or delete a directory, display the current working directory, and display the information about the files or directories under a specified directory. You can use the following commands to perform directory operations.

Perform the following configuration in User View.

Table 240 Directory Operation

Operation	Command
Create a directory	mkdir <i>directory</i>
Delete a directory	rmdir <i>directory</i>
Display the current working directory	pwd
Display the information about directories or files	dir [/ all] [<i>file-url</i>]
Change the current directory	cd <i>directory</i>

File Operation

The file system can be used to delete or undelete a file and permanently delete a file. Also, it can be used to display file contents, rename, copy and move a file and display the information about a specified file.

Using the **delete file-url** command to delete a file, leaves the contents of the file on the flash file system and does not free flash space. The file can be recovered using the **undelete** command. To delete a file and free space on the flash file

system use the `delete /unreserved file-url` command. Using this command will ensure that space is made available on the flash file system for additional information. To ensure that all deleted files have been removed from the system use the `reset recycle-bin` command, this will prompt for removal of all files in the file system.



When operating in a stack of switches to clear space the user has to change to the flash of each switch in the stack separately and then clear space in the file system of each switch in turn. Use the `cd directory` command for changing focus to a different switches file system or the `unit2>flash: device name parameter` for the command "reset recycle".

You can use the following commands to perform file operations.

Perform the following configuration in User View.

Table 241 File Operation

Operation	Command
Delete a file	<code>delete [/unreserved] file-url</code>
Undelete a file	<code>undelete file-url</code>
Delete a file from the recycle bin permanently	<code>reset recycle-bin file-url</code>
View contents of a file	<code>more file-url</code>
Rename a file	<code>rename fileurl-source fileurl-dest</code>
Copy a file	<code>copy fileurl-source fileurl-dest</code>
Move a file	<code>move fileurl-source fileurl-dest</code>
Display the information about directories or files	<code>dir [/ all] [file-url *</code>

Perform the following configuration in System View.

Table 242 Execute the Specified Batch File

Operation	Command
Execute the specified batch file	<code>execute filename</code>

Storage Device Operation

The file system can be used to format a specified memory device. You can use the following commands to format a specified memory device.

Perform the following configuration in User View.

Table 243 Storage Device Operation

Operation	Command
Format the storage device	<code>format filesystem</code>

Setting the Prompt Mode of the File System

The following command can be used for setting the prompt mode of the current file system.

Perform the following configuration in System View.

Table 244 File System Operation

Operation	Command
Set the file system prompt mode.	<code>file prompt { alert quiet }</code>

Configuring File Management

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

The format of the configuration file includes:

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

The management over the configuration files includes:

- Display the current-configuration and saved-configuration of the Switch
- Save the current-configuration
- Erase configuration files from Flash Memory

Displaying the Current-configuration and Saved-configuration of the Switch

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

Perform the following configuration in all views.

Table 245 Display the Configurations of the Switch

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



Saving the Current-configuration

The configuration files are displayed in their corresponding saving formats.

Use the **save** command to save the current-configuration in the Flash Memory, and the configurations will become the saved-configuration when the system is powered on for the next time.

Perform the following configuration in any view.

Table 246 Save the Current-Configuration

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

After a Fabric is formed, if you execute the **save** command, every switch in the Fabric saves the current configuration to its individual configuration file. If you do not enter the *file-name* parameter in this command, for the Switches that have specified the configuration file for booting, the current configurations will be stored to the specified configuration file; and for the Switches that have not specified the configuration file for booting, the current configurations will be stored to the default configuration file, which is sw4500cfg.cfg for Series 4500 Switches.

Erasing Configuration Files from Flash Memory

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

Perform the following configuration in User View.

Table 247 Erase Configuration Files from Flash Memory

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

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

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

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

Perform the following configuration in User View.

Table 248 Configure the Name of the Configuration File used for the Next Startup

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

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

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

Table 249 Display the Information of the File used at Startup

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

FTP Overview

FTP is a common way to transmit files on the Internet and IP network. Before the World Wide Web (WWW), files were transmitted in the command line mode and FTP was the most popular application. Even now, FTP is still used widely, while most users transmit files via email and Web.

FTP, a TCP/IP protocol on the application layer, is used for transmitting files between a remote server and a local host.

The Switch provides the following FTP services:

- FTP server: You can run FTP client program to log in the server and access the files on it.
- FTP client: After connected to the server through running the terminal emulator or Telnet on a PC, you can access the files on it, using FTP command.

Figure 60 FTP Configuration

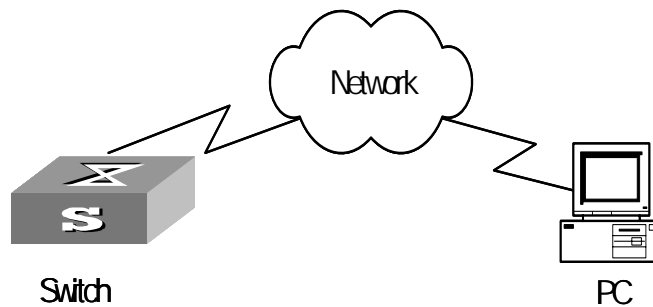


Table 250 Configuration of the Switch as FTP Client

Device	Configuration
Default	Description
Switch	Log into the remote FTP server directly with the ftp command.
--	You need first get FTP user command and password, and then log into the remote FTP server. Then you can get the directory and file authority.
PC	Start FTP server and make such settings as username, password, authority.
--	--

Table 251 Configuration of the Switch as FTP Server

Device	Configuration	Default	Description
Switch	Start FTP server.	FTP server is disabled.	You can view the configuration information of FTP server with the ftp-server command.
	Configure authentication and authorization for FTP server.	-	Configure username, password and authorized directory for FTP users.
	Configure running parameters for FTP server.	-	Configure timeout time value for FTP server.

Device	Configuration	Default	Description
PC	Log into the Switch from FTP client.	-	-



The prerequisite for normal FTP function is that the Switch and PC are reachable.

Enabling/Disabling FTP Server

You can use the following commands to enable/disable the FTP server on the Switch. Perform the following configuration in System View.

Table 252 Enable/Disable FTP Server

Operation	Command
Enable the FTP server	ftp server enable
Disable the FTP server	undo ftp server

FTP server supports multiple users to access at the same time. A remote FTP client sends request to the FTP server. Then, the FTP server will carry out the corresponding operation and return the result to the client.

By default, FTP server is disabled.

Configuring the FTP Server Authentication and Authorization

You can use the following commands to configure FTP server authentication and authorization. The authorization information of FTP server includes the top working directory provided for FTP clients.

Perform the following configuration in the corresponding view.

Table 253 Configure the FTP Server Authentication and Authorization

Operation	Command
Create new local user and enter local User View (System View)	local-user <i>username</i>
Delete local user (System View)	undo local-user [<i>username</i> all [service-type ftp]]
Configure password for local user (Local User View)	password [cipher simple] <i>password</i>
Configure service type for local user (Local User View)	service-type ftp ftp-directory <i>directory</i>
Cancel password for local user (Local User View)	undo password
Cancel service type for local user (Local User View)	undo service-type ftp [ftp-directory]

Only the clients who have passed the authentication and authorization successfully can access the FTP server.

Configuring the Running Parameters of FTP Server

You can use the following commands to configure the connection timeout of the FTP server. If the FTP server receives no service request from the FTP client for a period of time, it will cut the connection to it, thereby avoiding the illegal access from the unauthorized users. The period of time is FTP connection timeout.

Perform the following configuration in System View.

Table 254 Configure FTP Server Connection Timeout

Operation	Command
Configure FTP server connection timeouts	ftp timeout <i>minute</i>
Restoring the default FTP server connection timeouts	undo ftp timeout

By default, the FTP server connection timeout is 30 minutes.

Displaying and Debugging FTP Server

After the above configuration, execute *display* command in all views to display the running of the FTP Server configuration, and to verify the effect of the configuration.

Table 255 Display and Debug FTP Server

Operation	Command
Display FTP server	display ftp-server
Display the connected FTP users.	display ftp-user

The **display ftp-server** command can be used for displaying the configuration information about the current FTP server, including the maximum amount of users supported by the FTP server and the FTP connection timeout. The **display ftp-user** command can be used for displaying the detailed information about the connected FTP users.

Introduction to FTP Client

As an additional function provided by the Switch, FTP client is an application module and has no configuration functions. The Switch connects the FTP clients and the remote server and inputs the command from the clients for corresponding operations (such as creating or deleting a directory).

FTP Client Configuration Example

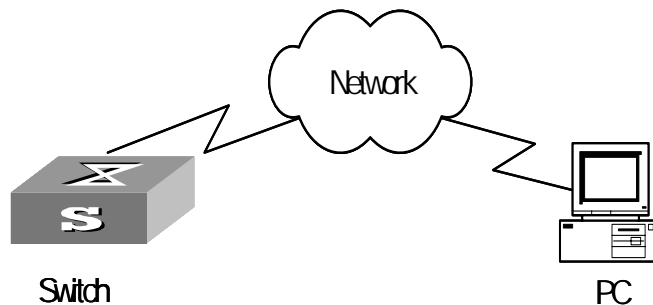
Networking Requirement

The Switch serves as the FTP client and the remote PC as the FTP server. The configuration on the FTP server: Configure a FTP user named as Switch, with the password hello and with read and write authority over the Switch root directory on the PC. The IP address of a VLAN interface on the Switch is 1.1.1.1, and that of the PC is 2.2.2.2. The Switch and PC are reachable.

The Switch application *switch.app* is stored on the PC. Using FTP, the Switch can download the **switch.app** from the remote FTP server and upload the *config.cfg* to the FTP server under the Switch directory for backup purpose.

Networking Diagram

Figure 61 Networking for FTP Configuration



Configuration Procedure

- 1 Configure the FTP server parameters on the PC: a user named as Switch, password hello, read and write authority over the Switch directory on the PC.

- 2 Configure the Switch

Log into the Switch (locally through the Console port or remotely using Telnet).

```
<4500>
```



CAUTION: If the flash memory of the Switch is not enough, you need to first delete the existing programs in the flash memory and then upload the new ones.

Type in the right command in User View to establish FTP connection, then correct username and password to log into the FTP server.

```
<4500> 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]
```

- 3 Type in the authorized directory of the FTP server.

```
[ftp]cd switch
```

- 4 Use the **put** command to upload the config.cfg to the FTP server.

```
[ftp]put config.cfg
```

- 5 Use the **get** command to download the switch.app from the FTP server to the flash directory on the FTP server.

```
[ftp]get switch.app
```

- 6 Use the **quit** command to release FTP connection and return to User View.

```
[ftp]quit
```

```
<4500>
```

- 7 Use the **boot boot-loader** command to specify the downloaded program as the application at the next login and reboot the Switch.

```
<4500> boot boot-loader switch.app
```

```
<4500> reboot
```


FTP Server Configuration Example

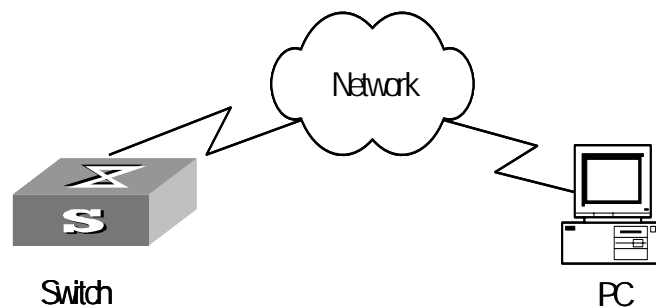
Networking Requirement

The Switch serves as FTP server and the remote PC as FTP client. The configuration on FTP server: Configure a FTP user named as Switch, with password hello and with read and write authority over the flash root directory on the PC. The IP address of a VLAN interface on the Switch is 1.1.1.1, and that of the PC is 2.2.2.2. The Switch and PC are reachable.

The Switch application *switch.app* is stored on the PC. Using FTP, the PC can upload the *switch.app* from the remote FTP server and download the *config.cfg* from the FTP server for backup purpose.

Networking Diagram

Figure 62 Networking for FTP Configuration



1 Configure the Switch

Log into the Switch (locally through the Console port or remotely using Telnet).

```
<4500>
```

2 Start FTP function and set username, password and file directory.

```
[4500]ftp server enable
[4500]local-user switch
[4500-luser-switch]service-type ftp ftp-directory flash:
[4500-luser-switch]password simple hello
```

3 Run FTP client on the PC and establish FTP connection. Upload the *switch.app* to the Switch under the Flash directory and download the *config.cfg* from the Switch. FTP client is not shipped with the Switch, so you need to buy it separately.



CAUTION: If the flash memory of the Switch is not enough, you need to first delete the existing programs in the flash memory and then upload the new ones.

4 When the uploading is completed, initiate the file upgrade on the Switch.

```
<4500>
```

Use the **boot boot-loader** command to specify the downloaded program as the application at the next login and reboot the Switch.

```
<4500> boot boot-loader switch.app
<4500> reboot
```

TFTP Overview

Trivial File Transfer Protocol (TFTP) is a simple protocol for file transmission. Compared with FTP, another file transmission protocol, TFTP has no complicated interactive access interface or authentication control, and therefore it can be used

when there is no complicated interaction between the clients and server. TFTP is implemented on the basis of UDP.

TFTP transmission is originated from the client end. To download a file, the client sends a request to the TFTP server and then receives data from it and sends an acknowledgement to it. To upload a file, the client sends a request to the TFTP server and then transmits data to it and receives the acknowledgement from it. TFTP transmits files in two modes: binary mode for program files and ASCII mode for text files.

Figure 63 TFTP Configuration

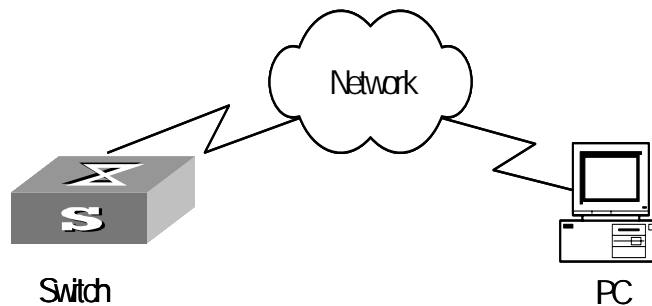


Table 256 Configuration of the Switch as TFTP Client

Device	Configuration	Default	Description
Switch	Configure IP address for the VLAN interface of the Switch, in the same network segment as that of TFTP server.	-	TFTP is right for the case where no complicated interactions are required between the client and server. Make sure that the IP address of the VLAN interface on the Switch is in the same network segment as that of the TFTP server.
	Use the tftp command to log into the remote TFTP server for file uploading and downloading.	-	-
PC	Start TFTP server and set authorized TFTP directory.	-	-

Downloading Files by means of TFTP

To download a file, the client sends a request to the TFTP server and then receives data from it and sends acknowledgement to it. You can use the following commands to download files by means of TFTP.

Perform the following configuration in User View.

Table 257 Download Files by means of TFTP

Operation	Command
Download files by means of TFTP	tftp tftp-server get source-file [dest-file]

Uploading Files by means of TFTP

To upload a file, the client sends a request to the TFTP server and then transmits data to it and receives the acknowledgement from it. You can use the following commands to upload files.

Perform the following configuration in User View.

Table 258 Upload Files by means of TFTP

Operation	Command
Upload files by means of TFTP	tftp tftp-server put source-file [dest-file]

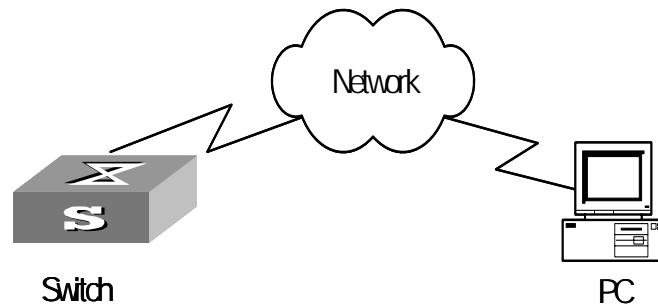
TFTP Client Configuration Example

Networking Requirement

The Switch serves as TFTP client and the remote PC as TFTP server. Authorized TFTP directory is set on the TFTP server. The IP address of a VLAN interface on the Switch is 1.1.1.1, and that of the PC is 2.2.2.2. The interface on the Switch connecting the PC belong to the same VLAN.

The Switch application *switch.app* is stored on the PC. Using TFTP, the Switch can download the *switch.app* from the remote TFTP server and upload the *config.cfg* to the TFTP server under the Switch directory for backup purpose.

Networking Diagram

Figure 64 Networking for TFTP Configuration

Configuration Procedure

- 1 Start TFTP server on the PC and set authorized TFTP directory.
- 2 Configure the Switch

Log into the Switch (locally through the Console port or remotely using Telnet).

```
<4500>
```



CAUTION: If the flash memory of the Switch is not enough, you need to first delete the existing programs in the flash memory and then upload the new ones.

- 3 Enter System View and download the *switch.app* from the TFTP server to the flash memory of the Switch.

```
<4500> system-view
[4500]
```

- 4 Configure IP address 1.1.1.1 for the VLAN interface, ensure the port connecting the PC is also in this VLAN (VLAN 1 in this example).

```
[4500]interface vlan 1
[4500-vlan-interface1]ip address 1.1.1.1 255.255.255.0
[4500-vlan-interface1]quit
```

- 5 Upload the *config.cfg* to the TFTP server.

```
<4500> tftp 1.1.1.2 put config.cfg config.cfg
```

- 6 Download the *switch.app* from the TFTP server.

```
<4500> tftp 1.1.1.2 get switch.app switch.app
```

- 7 Use the `boot boot-loader` command to specify the downloaded program as the application at the next login and reboot the Switch.

```
<4500> boot boot-loader switch.app  
<4500> reboot
```

13

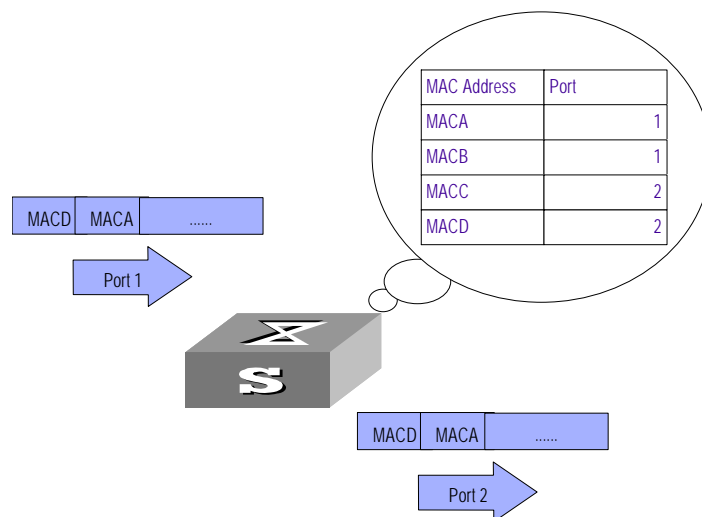
MAC Address Table Management

Overview

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

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

Figure 65 The Switch Forwards Packets with MAC Address Table



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

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

MAC Address Table Configuration

MAC address table management includes:

- Set MAC Address Table Entries
- Set MAC Address Aging Time
- Set the maximum count of MAC addresses learned by a port

Setting MAC Address Table Entries

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

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

Perform the following configuration in System View.

Table 259 Set MAC Address Table Entries

Operation	Command
Add/Modify an address entry	<code>mac-address { static dynamic blackhole } mac-address interface { interface-name interface-type interface-num } vlan vlan-id</code>
Delete an address entry	<code>undo mac-address [{ static dynamic blackhole } mac-address interface { interface-name interface-type interface-num } vlan vlan-id]</code>

When deleting the dynamic address table entries, the learned entries will be deleted simultaneously.

Setting MAC Address Aging Time

Setting an appropriate aging time implements MAC address aging. Too long or too short an aging time set by subscribers will cause the Ethernet switch to flood a large amount of data packets. This affects the Switch operation performance.

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

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

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

Perform the following configuration in System View.

Table 260 Set the MAC Address Aging Time for the System

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

In addition, this command takes effect on all the ports. However the address aging only functions on the dynamic addresses (manual entries added to the Switch are not aged).

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

Setting the Max Count of MAC Addresses Learned by a Port

With the address learning function, a Switch can learn new MAC addresses. After it receives a packet destined for an already learned MAC address, the Switch will forward it directly with the hardware, instead of broadcasting it. However, too many MAC address items learned by a port will affect the Switch operation performance.

You can control the MAC address items learned by a port through setting the max count of MAC addresses learned by a port. If a user sets the max count value of a port as *count*, the port will not learn new MAC address items when the count of MAC address items reaches the *count* value.

You can use the following commands to set the max count of MAC addresses learned by a port.

Perform the following configuration in Ethernet Port View.

Table 261 Set the Max Count of MAC Address Learned by a Port

Operation	Command
Set the Max Count of MAC Address Learned by a Port	<code>mac-address max-mac-count count</code>
Restore the default Max Count of MAC Address Learned by a Port	<code>undo mac-address max-mac-count</code>

By default, there is no limit to the MAC addresses learned via the Ethernet port.

Displaying MAC Address Table

After the above configuration, execute the `display` command in all views to display the running of the MAC address table configuration, and to verify the effect of the configuration.

Execute the `debugging` command in User View to debug MAC address table configuration.

Table 262 Display and Debug MAC Address Table

Operation	Command
Display the information in the address table	<code>display mac-address [mac-addr [vlan vlan-id] [static dynamic blackhole] [interface { interface-name interface-type interface-num }] [vlan vlan-id] [count]]</code>

Operation	Command
Display the aging time of dynamic address table entries	<code>display mac-address aging-time</code>

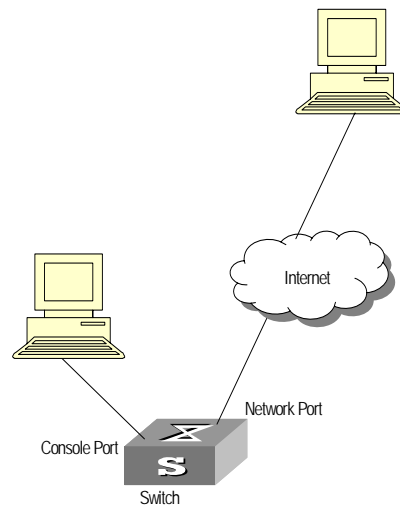
MAC Address Table Management Display Example

Networking Requirements

The user logs into the Switch via the Console port to display the MAC address table. Switch display the entire MAC address table of the Switch. If this Switch is a member of a stack then the entire database of all the switches will be shown here.

Networking Diagram

Figure 66 Display MAC address table



Configuration procedure

The `display` command shows a stack wide view of the MAC address table.

```
[4500]display mac-address
MAC ADDR          VLAN ID STATE      PORT INDEX      AGING TIME(s)
00e0-fc00-3943    1    Learned  Ethernet1/0/11    300
0000-0000-5100    1    Learned  Ethernet2/0/22    300
0020-9c08-e774    1    Learned  Ethernet2/0/7     288
0000-0000-5000    1    Learned  Ethernet2/0/3     143
--- 4 mac address(es) found ---
```

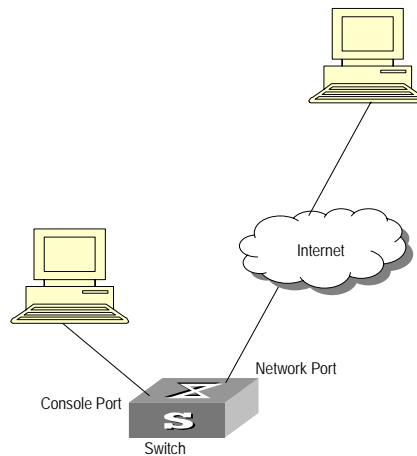

MAC Address Table Management Configuration Example

Networking Requirements

The user logs into the Switch via the Console port to configure the address table management. It is required to set the address aging time to 500s and add a static address 00e0-fc35-dc71 to Ethernet1/0/2 in vlan1.

Networking Diagram

Figure 67 Typical Configuration of Address Table Management



Configuration Procedure

- 1 Enter the System View of the Switch.

```
<4500> system-view
```

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

```
[4500]mac-address static 00e0-fc35-dc71 interface ethernet1/0/2 vlan 1
```

- 3 Set the address aging time to 500s.

```
[4500]mac-address timer 500
```

- 4 Display the MAC address configurations in all views.

```
[4500]display mac-address interface ethernet1/0/2
```

MAC ADDR	VLAN ID	STATE	PORT INDEX	AGING TIME(s)
00-e0-fc-35-dc-71	1	Static	Ethernet1/0/2	NOAGED
00-e0-fc-17-a7-d6	1	Learned	Ethernet1/0/2	500
00-e0-fc-5e-b1-fb	1	Learned	Ethernet1/0/2	500
00-e0-fc-55-f1-16	1	Learned	Ethernet1/0/2	500

--- 4 mac address(es) found ---

14

DEVICE MANAGEMENT

Overview

With the device management function, the Switch can display the current running state and event debugging information about the unit, thereby implementing the maintenance and management of the state and communication of the physical devices. In addition, there is a command available for rebooting the system, when some function failure occurs.

The device management configuration task is simple. As far as a user is concerned, it is mainly to display and debug the device management.

Device Management Configuration

Rebooting the Switch

It is necessary to reboot the Switch when failure occurs.

Perform the following configuration in User View.

Table 263 Reboot the Switch

Operation	Command
Reboot the Switch	<code>reboot [unit unit-id]</code>

Enabling the Timing Reboot Function

After enabling the timing reboot function on the Switch, the Switch will be rebooted at the specified time.

Perform the following configuration in User View, and the `display schedule reboot` command can be performed in any view.

Table 264 Reboot the Switch

Operation	Command
Enable the timing reboot function of the Switch, and set specified time and date	<code>schedule reboot at hh:mm [yyyy/mm/dd]</code>
Enable the timing reboot function of the Switch, and set waiting time	<code>schedule reboot delay { hhh:mm mmm }</code>
Cancel the parameter configuration of timing reboot function of the Switch	<code>undo schedule reboot</code>
Check the parameter configuration of the reboot terminal service of the current Switch	<code>display schedule reboot</code>

Designating the APP Adopted when Booting the Switch Next Time

In the case that there are several APPs in the Flash Memory, you can use this command to designate the APP adopted when booting the Switch next time.

Perform the following configuration in User View.

Table 265 Designate the APP Adopted when Booting the Switch Next Time

Operation	Command
Designate the APP adopted when booting the Switch next time	boot boot-loader <i>file-url</i>

Upgrading BootROM

You can use this command to upgrade the BootROM with the BootROM program in the Flash Memory. This configuration task facilitates the remote upgrade. You can upload the BootROM program file from a remote end to the Switch via FTP and then use this command to upgrade the BootROM.

Perform the following configuration in User View.

Table 266 Upgrade BootROM

Operation	Command
Upgrade BootROM	boot bootrom <i>file-url</i>

Displaying and Debugging Device Management

After the above configuration, execute **display** command in all views to display the running of the device management configuration, and to verify the effect of the configuration.

Table 267 Display and Debug Device Management

Operation	Command
Display the module types and running states of each card.	display device [unit <i>unit-id</i>]
Display the running state of the built-in fans.	display fan [unit <i>unit-id</i>]
Display the Used status of Switch memory	display memory [unit <i>unit-id</i>]
Display the state of the power.	display power [unit <i>unit-id</i>] [<i>power-ID</i>]
Display the APP to be applied when rebooting the Switch.	display boot-loader [unit <i>unit-id</i>]
Display the busy status of CPU	display cpu [unit <i>unit-id</i>]

Device Management Configuration Example

Networking Requirement

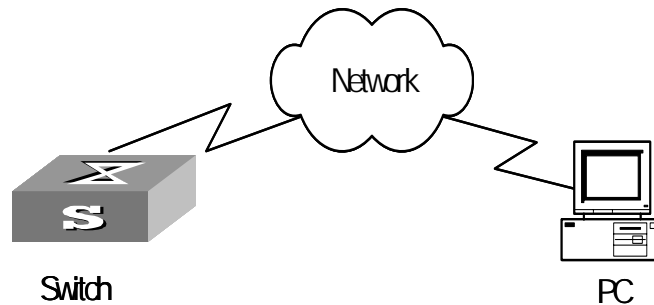
The user logs into the Switch using Telnet, downloads the application from the FTP server to the flash memory of the Switch, and implements remote upgrade using the right commands.

The Switch serves as FTP client and the remote PC as FTP server. The configuration on the FTP server: Configure an FTP user named as Switch, with password hello and with read and write authority over the Switch root directory on the PC. The IP address of a VLAN interface on the Switch is 1.1.1.1, and that of the PC is 2.2.2.2. The Switch and PC are reachable.

The Switch applications *switch.app* and *boot.app* are stored on the PC. Using FTP, the Switch can download the *switch.app* and *boot.app* from the remote FTP server.

Networking Diagram

Figure 68 Networking for FTP Configuration



Configuration Procedure

- 1 Configure FTP server parameters on the PC. Define a user named as *switch*, password *hello*, read and write authority over the Switch directory on the PC.
- 2 Configure the Switch

The Switch has been configured with a Telnet user named as *user*, as 3-level user, with password *hello*, requiring username and password authentication.

Use the **telnet** command to log into the Switch.

```
<4500>
```



CAUTION: *If the flash memory of the Switch is not enough, you need to first delete the existing programs in the flash memory and then upload the new ones.*

- 3 Type in the correct command in User View to establish FTP connection, then enter the correct username and password to log into the FTP server.

```
<4500> 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]
```

- 4 Enter the authorized directory of the FTP server.

```
[ftp]cd switch
```

- 5 Use the **get** command to download the *switch.app* from the FTP server to the flash directory on the FTP server.

```
[ftp]get switch.app
[ftp]get boot.app
```

- 6 Use the **quit** command to release the FTP connection and return to User View.

```
[ftp]quit
<4500>
```

- 7 Upgrade BootROM.

```
<4500> boot bootrom boot.app
This will update BootRom file on unit 1. Continue? [Y/N]y
```

```
Upgrading BOOTROM, please wait...  
Upgrade BOOTROM succeeded!
```

- 8 Use the **boot boot-loader** command to specify the downloaded program as the application at the next login and reboot the Switch.

```
<4500> boot boot-loader switch.app  
<4500>display boot-loader  
The app to boot at the next time is: flash:/Switch.app  
The app to boot of board 0 at this time is: flash:/PLAT.APP  
<4500> reboot
```


15

SYSTEM MAINTENANCE AND DEBUGGING

Basic System Configuration

Setting the System Name for the Switch

Perform the operation of **sysname** command in the System View.

Table 268 Set the Name for the Switch

Operation	Command
Set the Switch system name	sysname <i>sysname</i>
Restore Switch system name to default value	undo sysname

Setting the System Clock

Perform the operation of **clock datetime** command in the User View.

Table 269 Set the System Clock

Operation	Command
Set the system clock	clock datetime <i>time date</i>

Setting the Time Zone

You can configure the name of the local time zone and the time difference between the local time and the standard Universal Time Coordinated (UTC).

Perform the following operations in the User View.

Table 270 Setting the Time Zone

Operation	Command
Set the local time	clock timezone <i>zone_name</i> { add minus } <i>HH:MM:SS</i>
Restore to the default UTC time zone	undo clock timezone

By default, the UTC time zone is adopted.

Setting the Summer Time

You can set the name, start and end time of the summer time.

Perform the following operations in the User View.

Table 271 Setting the Summer Time

Operation	Command
Set the name and range of the summer time	clock summer-time <i>zone_name</i> { one-off repeating } <i>start-time start-date end-time end-date offset-time</i>
Remove the setting of the summer time	undo clock summer-time

By default, the summer time is not set.

Displaying the State and Information of the System

The **display** commands can be classified as follows according to their functions.

- Commands for displaying the system configuration information
- Commands for displaying the system running state
- Commands for displaying the system statistics information

For the **display** commands related to each protocol and different ports, refer to the relevant chapters. The following **display** commands are used for displaying the system state and the statistics information.

Configuration agent is one of the XRN features. You can log into one Switch of the Fabric to configure and manage the Fabric. The functions of the configuration agent include:

- Distributing configuration commands to the right destination Switches or processing modules based on the resolution result of the commands input.
- Sending output information of the commands from the Switch you have logged into to your terminal.
- Supporting simultaneous configuration of multiple users.

You cannot configure the configuration agent, but can view the statistics of the configuration agent.

Perform the following operations in all views.

Table 272 The Display Commands of the System

Operation	Command
Display the system clock	display clock
Display the system version	display version
Display the saved-configuration	display saved-configuration
Display the current-configuration	display current-configuration [controller interface <i>interface-type</i> [<i>interface-number</i>] configuration [<i>configuration</i>]] [{ begin exclude include } <i>regular-expression</i>]
Display the state of the debugging	display debugging [interface { <i>interface-name</i> <i>interface-type</i> <i>interface-number</i> }] [<i>module-name</i>]
Display statistics of the configuration agent	display config-agent unit-id <i>unit-id</i>

System Debugging

Enable/Disable the Terminal Debugging

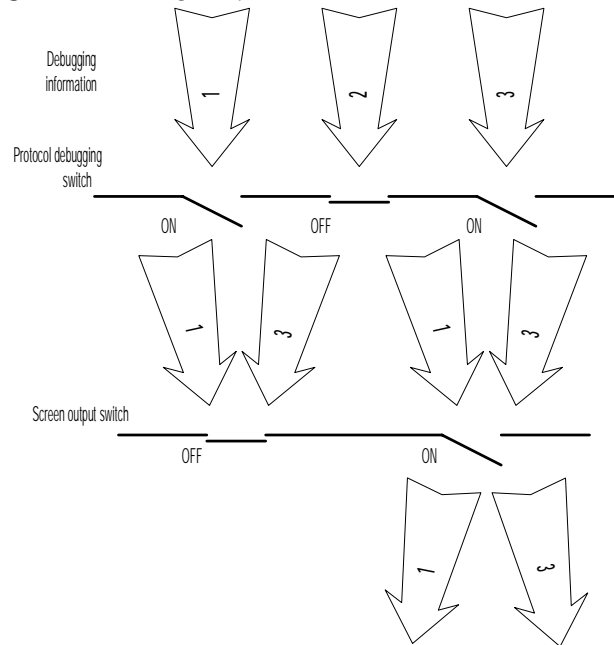
The Switch provides various ways for debugging most of the supported protocols and functions, which can help you diagnose and address the errors.

The following Switches can control the outputs of the debugging information:

- Protocol debugging Switch controls the debugging output of a protocol.
- Terminal debugging Switch controls the debugging output on a specified user screen.

Figure 69 illustrates the relationship between two Switches.

Figure 69 Debug Output



You can use the following commands to control the above-mentioned debugging.

Perform the following operations in User View.

Table 273 Enable/Disable the Debugging

Operation	Command
Enable the protocol debugging	<code>debugging { all [timeout interval] module-name [debugging-option] }</code>
Disable the protocol debugging	<code>undo debugging { all { protocol-name function-name } [debugging-option] }</code>
Enable the terminal debugging	<code>terminal debugging</code>
Disable the terminal debugging	<code>undo terminal debugging</code>

For more about the usage and format of the debugging commands, refer to the relevant chapters.



CAUTION: Since the debugging output will affect the system operating efficiency, do not enable the debugging without necessity, especially use the `debugging all` command with caution. When the debugging is over, disable all the debugging.

By default, if multiple devices form a fabric, the debugging information of the master is broadcasted within the fabric and the debugging information of the slave is only displayed on the slave device. You can view the debugging information including that of the master and the device in which the login port resides.

You can enable the logging, debugging and trap information switches within the fabric by executing the `info-center switch-on all` command. Synchronization is a process that each switch sends its own information to the other switches in the fabric, and meantime receives information from others to update local

information, ensuring the consistency of logging, debugging and trap information in a fabric.



After the synchronization of the whole fabric, a great deal of terminal display is generated. You are recommended not to enable the information synchronization switch of the whole fabric. If you enabled the information synchronization switch, after the synchronization information statistics and detection, you must execute the `undo info-center switch-on` command to disable the Switch in time.

Display Diagnostic Information

You can collect information about the Switch to locate the source of a fault. However, each module has its corresponding `display` command, which makes it difficult to collate all the information needed. In this case, you can use `display diagnostic-information` command.

You can perform the following operations in all views.

Table 274 Display Diagnostic Information

Operation	Command
display diagnostic information	<code>display diagnostic-information</code>

Testing Tools for Network Connection

ping The `ping` command can be used to check the network connection and if the host is reachable.

Perform the following operation in all views.

Table 275 The ping Command

Operation	Command
Support IP ping	<code>ping [-a ip-address] [-c count] [-d] [-h ttl] [-i { interface-type interface-num interface-name }] [ip] [-n] [-p pattern] [-q] [-r] [-s packetsize] [-t timeout] [-tos tos] [-v] host</code>

The output of the command includes:

- The response to each ping message. If no response packet is received when time is out, "Request time out" information appears. Otherwise, the data bytes, the packet sequence number, TTL, and the round-trip time of the response packet will be displayed.
- The final statistics, including the number of the packets the Switch sent out and received, the packet loss ratio, the round-trip time in its minimum value, mean value and maximum value.

Test Periodically if the IP Address is Reachable

You can use the `end-station polling ip-address` command in System View to configure the IP address requiring periodical testing.

Perform the following configuration in System View.

Table 276 Test Periodically if the IP address is Reachable

Operation	Command
Configure the IP address requiring periodical testing	end-station polling ip-address <i>ip-address</i>
Delete the IP address requiring periodical testing	undo end-station polling ip-address <i>ip-address</i>

The Switch can ping an IP address every one minute to test if it is reachable. Three PING packets can be sent at most for every IP address in every testing with a time interval of five seconds. If the Switch cannot successfully ping the IP address after the three PING packets, it assumes that the IP address is unreachable.

You can configure up to 50 IP addresses by using the command repeatedly.

tracert

The **tracert** is used for testing the gateways passed by the packets from the source host to the destination one. It is mainly used for checking if the network is connected and analyzing where the fault occurs in the network.

The execution process of **tracert** is described as follows: Send a packet with TTL value as 1 and the first hop sends back an ICMP error message indicating that the packet cannot be sent, for the TTL is timeout. Re-send the packet with TTL value as 2 and the second hop returns the TTL timeout message. The process is carried over and over until the packet reaches the destination. The purpose to carry out the process is to record the source address of each ICMP TTL timeout message, so as to provide the route of an IP packet to the destination.

Perform the following operation in all views.

Figure 70 The tracert Command

Operation	Command
Trace route	tracert [<i>-a source-IP</i>] [<i>-f first-TTL</i>] [<i>-m max-TTL</i>] [<i>-p port</i>] [<i>-q nqueries</i>] [<i>-w timeout</i>] <i>string</i>

Introduction to Remote-ping

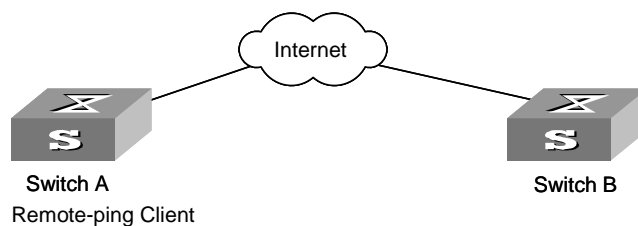
Remote-ping is a network diagnostic tool used to test the performance of protocols (only ICMP by far) operating on network. It is an enhanced alternative to the ping command.

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 plus a test tag.

You can perform an remote-ping test after creating a test group and configuring the test parameters.

Being different from the ping command, remote-ping does not display the round trip time (RTT) and timeout status of each packet on the console terminal in real time. You need to execute the display remote-ping command to view the statistic results of your remote-ping test operation. remote-ping allows administrators to set the parameters of remote-ping test groups and start remote-ping test operations.

Figure 71 Illustration for Remote-ping



Remote-ping Configuration

This section contains information on remote-ping.

Introduction to Remote-ping Configuration

The configuration tasks for remote-ping include:

- Enabling remote-ping Client
- Creating test group
- Configuring test parameters

The test parameters that you can configure include:

- Destination IP address

It is equivalent to the destination IP address in the ping command.

Test type. Currently, remote-ping supports only one test type: ICMP.

- Number of test packets sent in a test

If this parameter is set to a number greater than one, the system sends the second test packet once it receives a response to the first one, or when the test timer times out if it receives no response after sending the first one, and so forth until the last test packet is sent out. This parameter is equivalent to the -n parameter in the ping command.

Automatic test interval. This parameter is used to allow the system to automatically perform the same test at regular intervals.

- Test timeout time

Test timeout time is the time the system waits for an ECHO-RESPONSE packet after it sends out an ECHO-REQUEST packet. If no ECHO-RESPONSE packet is received within this time, this test is considered a failure. This parameter is similar to the -t parameter in the ping command, but has a different unit (the -t parameter in the ping command is in ms, while the timeout time in the remote-ping command is in seconds).

Configuring Remote-ping

Refer to [Table 277](#) for remote-ping configuration information.

Table 277 Configure Remote-ping

Operation	Command	Description
Enter system view	system-view	-
Enable remote-ping Client	Remote-ping-agent enable	Required By default, remote-ping Client is disabled.
Create an remote-ping test group	Remote-ping administrator-name test-tag	Required By default, no remote-ping test group is configured.

Table 277 Configure Remote-ping (continued)

Operation	Command	Description
Configure the test parameters	destination-ip ip-address	Required By default, no destination IP address is configured.
	test-type type	Optional By default, the test type is ICMP.
	count times	Optional By default, the packet sending times in each test is 1.
	frequency interval	Optional By default, the automatic test interval is zero, which indicating the test will be performed only once.
	timeout time	Optional By default, the timeout time is 3 seconds.
Execute the test	test-enable	Required
Display test results	display remote-ping { history results } [administrator-name test-tag]	Required You can execute the command in any view.



The remote-ping test does not display test results. You can use the display remote-ping command to view the test results.



You can use the display remote-ping command to check the test history as well as the latest test results.

Configuration Example Network Requirement

Perform an remote-ping ICMP test between two switches. Like a ping test, this test uses ICMP to test the RTTs of data packets between the source and the destination.

Configuration procedure

- 1 Enable remote-ping Client.

```
[S5500] remote-ping-agent enable
```

- 2 Create an remote-ping test group administrator icmp.

```
[S5500] remote-ping administrator icmp
```

- 3 Configure the test parameters.

```
[S5500-remote-ping-administrator-icmp] test-type icmp
```

```
[S5500-remote-ping-administrator-icmp] destination-ip 10.10.10.10
```

```
[S5500-remote-ping-administrator-icmp] count 10
```

```
[S5500-remote-ping-administrator-icmp] timeout 3
```

- 4 Enable the test operation.

```
[S5500-remote-ping-administrator-icmp] test-enable
```

5 Display the test results.

```
[S5500-remote-ping-administrator-icmp] display remote-ping results
administrator icmp
[S5500-remote-ping-administrator-icmp] display remote-ping history
administrator icmp
```

Logging Function

Introduction to Info-center

The Info-center serves as an information center of the system software modules. The logging system is responsible for most of the information outputs, and it also makes detailed classification to filter the information efficiently. Coupled with the debugging program, the info-center provides powerful support for network administrators and support personnel to monitor the operating state of networks and diagnose network failures.

When the log information is output to terminal or log buffer, the following parts will be included:

```
%Timestamp Sysname Module name/Severity/Digest: Content
```

For example:

```
%Jun 7 05:22:03 2003 4500 IFNET/6/UPDOWN:Line protocol on interface
Ethernet1/0/2, changed state to UP
```

When the log information is output to the info-center, the first part will be "<Priority>".

For example:

```
<187>Jun 7 05:22:03 2003 4500 IFNET/6/UPDOWN:Line protocol on
interface Ethernet1/0/2, changed state to UP
```

The description of the components of log information is as follows:

1 Priority

The priority is computed according to following formula: facility*8+severity-1. The default value for the facility is 23. The range of severity is 1~8, and the severity will be introduced in a separate section.

The value of the facility can be set by command **info-center loghost**, .local1 to local7 corresponding to 16 to 23 respectively, for detailed information, refer to RFC3164 (The BSD syslog Protocol).



Priority is only effective when information is send to loghost. There is no character between priority and timestamp.

2 Timestamp

If the logging information is sent to the log host, the default format of the timestamp is the date, and it can be changed to **boot** format or **none** format through the command:

```
info-center timestamp log { date | boot | none }
```

The date format of timestamp is "*mm dd hh:mm:ss yyyy*".

"*mm*" is the month field, such as: Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, Dec.

"*dd*" is the day field, if the day is less than the 10th, one blank should be added, such as " 7".

"*hh:mm:ss*" is the time field, "*hh*" is from 00 to 23, "*mm*" and "*ss*" are from 00 to 59.

"*yyyy*" is the year field.

If changed to boot format, it represents the milliseconds from system booting. Generally, the data are so large that two 32 bits integers are used, and separated with a dot '.'.

For example:

```
<189>0.166970 4500 IFNET/6/UPDOWN:Line protocol on interface
Ethernet1/0/2, changed state to UP
```

It means that 166970ms ($0 \times 2^{32} + 166970$) has passed from system booting.

If changed to **none** format, the timestamp field is not present in logging information.



There is a blank between timestamp and sysname. If the timestamp is none format, there is a blank between priority and sysname.

3 Sysname

The sysname is the host name, the default value is 4500.

You can change the host name through **sysname** command.



There is a blank between sysname and module name.

4 Module name

The module name is the name of module which created this logging information, the following sheet lists some examples:

Table 278 Module Names in Logging Information

Module name	Description
8021X	802.1X module
ACL	Access control list module
AM	Access management module
ARP	Address resolution protocol module
CFAX	Configuration proxy module
CFG	Configuration management platform module
CFM	Configuration file management module
CMD	Command line module
COMMONSY	Common system MIB module
DEV	Device management module
DHCC	DHCP Client module
DHCP	Dynamic host configuration protocol module
DRV	Driver module
DRV_MNT	Driver maintenance module
ESP	End-station polling module
ETH	Ethernet module
FIB	Forwarding module
FTM	Fabric topology management module
FTMCMD	Fabric topology management command line module

Module name	Description
FTPS	FTP server module
HA	High availability module
HTTPD	HTTP server module
IFNET	Interface management module
IGSP	IGMP snooping module
IP	IP module
IPC	Inter-process communication module
IPMC	IP multicast module
L2INF	Interface management module
LACL	LAN switch ACL module
LQOS	LAN switch QoS module
LS	Local server module
MPM	Multicast port management module
NTP	Network time protocol module
PPRDT	Protocol packet redirection module
PTVL	Driver port, VLAN (Port & VLAN) module
QACL	QoS/ACL module
QOSF	QoS profile module
RDS	Radius module
RM	Routing management
RMON	Remote monitor module
RSA	Revest, shamir and adleman encryption system
RTPRO	Routing protocol
SHELL	User interface
SNMP	Simple network management protocol
SOCKET	Socket
SSH	Secure shell module
STP	Spanning tree protocol module
SYSMIB	System MIB module
TELNET	Telnet module
UDPH	UDP helper module
VFS	Virtual file system module
VTY	Virtual type terminal module
WCN	Web management module
XM	XModem module

Note that there is a slash ('/') between module name and severity.

5 Severity

Switch information falls into three categories: log information, debugging information and trap information. The info-center classifies every kind of information into 8 severity or urgent levels. The log filtering rule is that the system prohibits outputting the information whose severity level is greater than the set threshold. The more urgent the logging packet is, the smaller its severity level. The

level represented by “emergencies” is 1, and that represented by “debugging” is 8. Therefore, when the threshold of the severity level is “debugging”, the system will output all the information.

Definition of severity in logging information is as follows.

Table 279 Info-Center-Defined Severity

Severity	Description
emergencies	Extremely emergent errors
alerts	Errors that need to be corrected immediately
critical	Critical errors
errors	Errors that need to be addressed but are not critical
warnings	Warning, there may be some types of errors
notifications	Information that should be noted
informational	Common prompting information
debugging	Debugging information

Note that there is a slash between severity and digest.

6 Digest

The digest is abbreviation, it represent the abstract of contents.

Note that there is a colon between digest and content.

7 Content

It is the contents of logging information.

Info-Center Configuration

The Switch supports five output directions of information.

The system assigns a channel in each output direction by default. See the table below.

Table 280 Numbers and Names of the Channels for Log Output

Output direction	Channel number	Default channel name
Console	0	console
Monitor	1	monitor
Info-center loghost	2	loghost (not supported)
Trap buffer	3	trapbuf
Logging buffer	4	logbuf
snmp	5	snmpagent



The settings in the six directions are independent from each other. The settings will take effect only after enabling the information center.

The Switch info-center has the following features:

- Support to output log in five directions, that is, console, monitor to Telnet terminal, logbuffer, trapbuffer, and SNMP.
- The log is divided into eight levels according to the significance and it can be filtered based on the levels.

- The information can be classified in terms of the source modules and the information can be filtered in accordance with the modules.
- The output language can be selected between Chinese and English.

1 Sending the information to the control terminal.

Table 281 Sending the Information to the Control Terminal.

Device	Configuration	Default Value	Configuration Description
	Enable info-center	By default, info-center is enabled.	Other configurations are valid only if the info-center is enabled.
	Set the information output direction to Console	-	-
Switch	Set information source	-	You can define which modules and information to be sent out and the time-stamp format of information, and so on. You must turn on the Switch of the corresponding module before defining output debugging information.
	Enable terminal display function	-	You can view debugging information after enabling terminal display function

2 Sending the Information to monitor terminal

Table 282 Sending the Information to Monitor Terminal

Device	Configuration	Default Value	Configuration Description
	Enable info-center	By default, info-center is enabled.	Other configurations are valid only if the info-center is enabled.
	Set the information output direction to monitor	-	-
Switch	Set information source	-	You can define which modules and information to be sent out and the time-stamp format of information, and so on. You must turn on the Switch of the corresponding module before defining output debugging information.
	Enable the terminal display function and this function for the corresponding information	-	For Telnet terminal and dumb terminal, to view the information, you must enable the current terminal display function using the terminal monitor command.

3 Sending the Information to log buffer.

Table 283 Sending the Information to Log Buffer

Device	Configuration	Default Value	Configuration Description
	Enable info-center	By default, info-center is enabled.	Other configurations are valid only if the info-center is enabled.
	Set the information output direction to logbuffer	-	You can configure the size of the log buffer at the same time.
Switch	Set information source	-	You can define which modules and information to be sent out and the time-stamp format of information, and so on. You must turn on the Switch of the corresponding module before defining output debugging information.

4 Sending the Information to trap buffer.

Table 284 Sending the Information to Trap Buffer

Device	Configuration	Default Value	Configuration Description
	Enable info-center	By default, info-center is enabled.	Other configurations are valid only if the info-center is enabled.
	Set the information output direction to trapbuffer	-	You can configure the size of the trap buffer at the same time.
Switch	Set information source	-	You can define which modules and information to be sent out and the time-stamp format of information, and so on. You must turn on the Switch of the corresponding module before defining output debugging information.

5 Sending the Information to SNMP

Table 285 Sending the Information to SNMP

Device	Configuration	Default value	Configuration description
	Enable info-center	By default, info-center is enabled.	Other configurations are valid only if the info-center is enabled.
	Set the information output direction to SNMP	-	-
Switch	Set information source	-	You can define which modules and information to be sent out and the time-stamp format of information, and so on. You must turn on the Switch of the corresponding module before defining output debugging information.
	Configuring SNMP features	-	See SNMP Configuration
Network management workstation	The same as the SNMP configuration of the Switch	-	-

6 Turn on/off the information synchronization Switch in Fabric

Figure 72 Turn on/off the Information Synchronization Switch in Fabric

Device	Configuration	Default Value	Configuration Description
	Enable info-center	By default, info-center is enabled.	Other configurations are valid only if the info-center is enabled.
Switch	Set the information output direction to SNMP	By default, Switches of master log in Fabric, debugging and trap information synchronization are turned on, so as log and strap information synchronization Switches in other Switches.	This configuration can keep log information, debugging information and trap information in Fabric in every Switch synchronized.

Sending the Information to Loghost

To send information to loghost, follow the steps below:

- 1 Perform the following operation in System View.

Table 286 Enable/disable info-center

Operation	Command
Enable info-center	info-center enable
Disable info-center	undo info-center enable



Info-center is enabled by default. After info-center is enabled, system performances are affected when the system processes much information because of information classification and outputting.

- 2 Configuring to output information to loghost

Perform the following operation in system view.

Figure 73 Configuring to output information to loghost

Operation	Command
Output information to loghost	info-center loghost <i>host-ip-addr</i> [channel { <i>channel-number</i> <i>channel-name</i> }] [facility <i>local-number</i>] [language { chinese english }]
Cancel the configuration of outputting information to loghost	undo info-center loghost <i>host-ip-addr</i>



Ensure to enter the correct IP address using the info-center loghost command to configure loghost IP address. If you enter a loopback address, the system prompts of invalid address appears.

- 3 Configuring information source on the switch

By this configuration, you can define the information that sent to loghost is generated by which modules, information type, information level, and so on. Perform the following operation in system view.

Table 287 Defining information source

Operation	Command
Define information source	info-center source { <i>modu-name</i> default } channel { <i>channel-number</i> <i>channel-name</i> } [{ log trap debug }* { level severity state state }*]
Cancel the configuration of information source	undo info-center source { <i>modu-name</i> default } channel { <i>channel-number</i> <i>channel-name</i> }

modu-name specifies the module name; default represents all the modules; level refers to the severity levels; severity specifies the severity level of information. The information with the level below it will not be output. *channel-number* specifies the channel number and *channel-name* specifies the channel name.

When defining the information sent to the loghost, *channel-number* or *channel-name* must be set to the channel that corresponds to loghost direction.

Every channel has been set with a default record, whose module name is default and the module number is 0xffff0000. However, for different channels, the default record may have different default settings of log, trap and debugging. When there is no specific configuration record for a module in the channel, use the default one.



If you want to view the debugging information of some modules on the switch, you must select debugging as the information type when configuring information source, meantime using the debugging command to turn on the debugging switch of those modules.

You can use the following commands to configure log information, debugging information and the time-stamp output format of trap information.

Perform the following operation in system view:

Table 288 Configuring the output format of time-stamp

Operation	Command
Configure the output format of the time-stamp	info-center timestamp { log trap debugging } { boot date none }
Output time-stamp is disabled	undo info-center timestamp { log trap debugging }

4 Configuring loghost

The configuration on the loghost must be the same with that on the switch. For related configuration, see the configuration examples in the later part.

Sending the Information to Control Terminal

To send information to the control terminal, follow the steps below:

1 Enabling info-center

Perform the following operation in System View.

Table 289 Enable/disable info-center

Operation	Command
Enable info-center	info-center enable
Disable info-center	undo info-center enable



Info-center is enabled by default. After info-center is enabled, system performances are affected when the system processes much information because of information classification and outputting.

2 Configuring to output information to the control terminal.

Perform the following operation in System View.

Table 290 Configuring to Output Information to Control Terminal

Operation	Command
Output information to Console	info-center console channel { <i>channel-number</i> <i>channel-name</i> }
Cancel the configuration of outputting information to Console	undo info-center console channel

3 Configuring the information source on the Switch.

With this configuration, you can define the information sent to the control terminal that is generated by which modules, information type, information level, and so on.

Perform the following operation in System View:

Table 291 Defining Information Source

Operation	Command
Define information source	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> }*]
Cancel the configuration of information source	undo info-center source { <i>modu-name</i> default } channel { <i>channel-number</i> <i>channel-name</i> }

modu-name specifies the module name; **default** represents all the modules; **level** refers to the severity levels; *severity* specifies the severity level of information. The information with the level below it will not be output. *channel-number* specifies the channel number and *channel-name* specifies the channel name.

When defining the information sent to the control terminal, *channel-number* or *channel-name* must be set to the channel that corresponds to the Console direction.

Every channel has been set with a default record, whose module name is **default** and the module number is 0xffff0000. However, for different channels, the default record may have different default settings of log, trap and debugging. When there is no specific configuration record for a module in the channel, use the default one.



*If you want to view the debugging information of some modules on the Switch, you must select **debugging** as the information type when configuring information source, meantime using the **debugging** command to turn on the debugging Switch of those modules.*

You can use the following commands to configure log information, debugging information and the time-stamp output format of trap information.

Perform the following operation in System View:

Table 292 Configuring the Output Format of Time-stamp

Operation	Command
Configure the output format of the time-stamp	info-center timestamp { log trap debugging } { boot date none }
Output time-stamp is disabled	undo info-center timestamp { log trap debugging }

4 Enable terminal display function

To view the output information at the control terminal, you must first enable the corresponding log, debugging and trap information functions at the Switch.

For example, if you have set the log information as the information sent to the control terminal, now you need to use the **terminal logging** command to enable the terminal display function of log information on the Switch, then you can view the information at the control terminal.

Perform the following operation in User View:

Table 293 Enabling Terminal Display Function

Operation	Command
Enable terminal display function of debugging information	terminal debugging
Disable terminal display function of debugging information	undo terminal debugging
Enable terminal display function of log information	terminal logging
Disable terminal display function of log information	undo terminal logging
Enable terminal display function of trap information	terminal trapping
Disable terminal display function of trap information	undo terminal trapping

Sending the Information to Telnet Terminal or Dumb Terminal

To send information to a Telnet terminal or dumb terminal, follow the steps below:

1 Enabling info-center

Perform the following operation in System View.

Table 294 Enable/Disable Info-Center

Operation	Command
Enable info-center	info-center enable
Disable info-center	undo info-center enable



Info-center is enabled by default. After info-center is enabled, system performances are affected when the system processes much information because of information classification and outputting.

2 Configuring to output information to Telnet terminal or dumb terminal

Perform the following operation in System View.

Table 295 Configuring to Output Information to Telnet Terminal or Dumb Terminal

Operation	Command
Output information to Telnet terminal or dumb terminal	info-center monitor channel { <i>channel-number</i> <i>channel-name</i> }
Cancel the configuration of outputting information to Telnet terminal or dumb terminal	undo info-center monitor channel

3 Configuring information source on the Switch

With this configuration, you can define the information that is sent to the Telnet terminal or dumb terminal that is generated by which modules, information type, information level, and so on.

Perform the following operation in System View:

Table 296 Defining Information Source

Operation	Command
Define information source	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> }*]
Cancel the configuration of information source	undo info-center source { <i>modu-name</i> default } channel { <i>channel-number</i> <i>channel-name</i> }

modu-name specifies the module name; **default** represents all the modules; **level** refers to the severity levels; *severity* specifies the severity level of information. The information with the level below it will not be output. *channel-number* specifies the channel number and *channel-name* specifies the channel name.

When defining the information sent to Telnet terminal or dumb terminal, *channel-number* or *channel-name* must be set to the channel that corresponds to the Console direction.

Every channel has been set with a default record, whose module name is **default** and the module number is 0xffff0000. However, for different channels, the default record may have different default settings of log, trap and debugging. When there is no specific configuration record for a module in the channel, use the default one.



When there are more than one Telnet users or monitor users at the same time, some configuration parameters should be shared among the users, such as module-based filtering settings and severity threshold. When a user modifies these settings, it will be reflected on other clients.



*If you want to view the debugging information of some modules on the Switch, you must select **debugging** as the information type when configuring information source, meantime using the **debugging** command to turn on the debugging Switch of those modules.*

You can use the following commands to configure log information, debugging information and the time-stamp output format of trap information.

Perform the following operation in System View.

Table 297 Configuring the Output Format of Time-stamp

Operation	Command
Configure the output format of the time-stamp	info-center timestamp { log trap debugging } { boot date none }

Operation	Command
Output time-stamp is disabled	<code>undo info-center timestamp { log trap debugging }</code>

4 Enabling terminal display function

To view the output information at the Telnet terminal or dumb terminal, you must first enable the corresponding log, debugging and trap information functions at the Switch.

For example, if you have set the log information as the information sent to the Telnet terminal or dumb terminal, you need to use the `terminal logging` command to enable the terminal display function of log information on the Switch, then you can view the information at the Telnet terminal or dumb terminal.

Perform the following operation in User View.

Table 298 Enabling Terminal Display Function

Operation	Command
Enable terminal display function of log, debugging and trap information	<code>terminal monitor</code>
Disable terminal display function of the above information	<code>undo terminal monitor</code>
Enable terminal display function of debugging information	<code>terminal debugging</code>
Disable terminal display function of debugging information	<code>undo terminal debugging</code>
Enable terminal display function of log information	<code>terminal logging</code>
Disable terminal display function of log information	<code>undo terminal logging</code>
Enable terminal display function of trap information	<code>terminal trapping</code>
Disable terminal display function of trap information	<code>undo terminal trapping</code>

Sending the Information to the Log Buffer

To send information to the log buffer, follow the steps below:

1 Enabling info-center

Perform the following operation in System View.

Table 299 Enabling/Disabling Info-center

Operation	Command
Enable info-center	<code>info-center enable</code>
Disable info-center	<code>undo info-center enable</code>



Info-center is enabled by default. After info-center is enabled, system performances are affected when the system processes much information because of information classification and outputting.

2 Configuring to output information to the log buffer

Perform the following operation in System View.

Table 300 Configuring to Output Information to Log Buffer

Operation	Command
Output information to log buffer	info-center logbuffer [channel { <i>channel-number</i> <i>channel-name</i> }] [size <i>buffersize</i>]
Cancel the configuration of outputting information to log buffer	undo info-center logbuffer [channel size]

3 Configuring the information source on the Switch

With this configuration, you can define the information that is sent to the log buffer: generated by which modules, information type, information level, and so on.

Perform the following operation in System View:

Table 301 Defining the Information Source

Operation	Command
Define information source	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> }*]
Cancel the configuration of information source	undo info-center source { <i>modu-name</i> default } channel { <i>channel-number</i> <i>channel-name</i> }

modu-name specifies the module name; **default** represents all the modules; **level** refers to the severity levels; *severity* specifies the severity level of information. The information with the level below it will not be output. *channel-number* specifies the channel number and *channel-name* specifies the channel name.

When defining the information sent to the log buffer, *channel-number* or *channel-name* must be set to the channel that corresponds to the Console direction.

Every channel has been set with a default record, whose module name is **default** and the module number is 0xffff0000. However, for different channels, the default record may have different default settings of log, trap and debugging. When there is no specific configuration record for a module in the channel, use the default one.



*If you want to view the debugging information of some modules on the Switch, you must select **debugging** as the information type when configuring the information source, meantime using the **debugging** command to turn on the debugging Switch of those modules.*

You can use the following commands to configure log information, debugging information and the time-stamp output format of trap information.

Perform the following operation in System View.

Table 302 Configuring the Output Format of Time-stamp

Operation	Command
Configure the output format of the time-stamp	info-center timestamp { log trap debugging } { boot date none }
Output time-stamp is disabled	undo info-center timestamp { log trap debugging }

Sending the Information to the Trap Buffer

To send information to the trap buffer, follow the steps below:

1 Enabling info-center

Perform the following operation in System View.

Table 303 Enabling/Disabling Info-center

Operation	Command
Enable info-center	info-center enable
Disable info-center	undo info-center enable



Info-center is enabled by default. After info-center is enabled, system performances are affected when the system processes much information because of information classification and outputting.

2 Configuring to output information to the trap buffer.

Perform the following operation in System View.

Table 304 Configuring to Output Information to Trap Buffer

Operation	Command
Output information to trap buffer	info-center trapbuffer [size buffersize] [channel { channel-number channel-name }]
Cancel the configuration of outputting information to trap buffer	undo info-center trapbuffer [channel size]

3 Configuring the information source on the Switch.

With this configuration, you can define the information that is sent to the trap buffer: generated by which modules, information type, information level, and so on.

Perform the following operation in System View.

Table 305 Defining Information Source

Operation	Command
Define information source	info-center source { modu-name default } channel { channel-number channel-name } [{ log trap debug }* { level severity state state }*]
Cancel the configuration of information source	undo info-center source { modu-name default } channel { channel-number channel-name }

modu-name specifies the module name; **default** represents all the modules; **level** refers to the severity levels; *severity* specifies the severity level of information. The information with the level below it will not be output. *channel-number* specifies the channel number and *channel-name* specifies the channel name.

When defining the information sent to the trap buffer, *channel-number* or *channel-name* must be set to the channel that corresponds to the Console direction.

Every channel has been set with a default record, whose module name is **default** and the module number is 0xffff0000. However, for different channels, the default record may have different default settings of log, trap and debugging. When there

is no specific configuration record for a module in the channel, use the default one.



*If you want to view the debugging information of some modules on the Switch, you must select **debugging** as the information type when configuring information source, meantime using the **debugging** command to turn on the debugging Switch of those modules.*

You can use the following commands to configure log information, debugging information and the time-stamp output format of trap information.

Perform the following operation in System View.

Table 306 Configuring the Output Format of Time-stamp

Operation	Command
Configure the output format of the time-stamp	info-center timestamp { log trap debugging } { boot date none }
Output time-stamp is disabled	undo info-center timestamp { log trap debugging }

Sending the Information to SNMP Network Management

To send information to SNMP NM, follow the steps below:

1 Enabling info-center

Perform the following operation in System View.

Table 307 Enabling/Disabling Info-center

Operation	Command
Enable info-center	info-center enable
Disable info-center	undo info-center enable



Info-center is enabled by default. After info-center is enabled, system performances are affected when the system processes much information because of information classification and outputting.

2 Configuring to output information to SNMP NM

Perform the following operation in System View.

Table 308 Configuring to Output Information to SNMP NM

Operation	Command
Output information to SNMP NM	info-center snmp channel { channel-number channel-name }
Cancel the configuration of outputting information to SNMP NM	undo info-center snmp channel

3 Configuring the information source on the Switch.

With this configuration, you can define the information that is sent to SNMP NM: generated by which modules, information type, information level, and so on.

Perform the following operation in System View.

Table 309 Defining Information Source

Operation	Command
Define information source	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> }*]
Cancel the configuration of information source	undo info-center source { <i>modu-name</i> default } channel { <i>channel-number</i> <i>channel-name</i> }

modu-name specifies the module name; **default** represents all the modules; **level** refers to the severity levels; *severity* specifies the severity level of information. The information with the level below it will not be output. *channel-number* specifies the channel number and *channel-name* specifies the channel name.

When defining the information sent to SNMP NM, *channel-number* or *channel-name* must be set to the channel that corresponds to Console direction.

Every channel has been set with a default record, whose module name is **default** and the module number is 0xffff0000. However, for different channels, the default record may have different default settings of log, trap and debugging. When there is no specific configuration record for a module in the channel, use the default one.



*If you want to view the debugging information of some modules on the Switch, you must select **debugging** as the information type when configuring information source, meantime using the **debugging** command to turn on the debugging Switch of those modules.*

You can use the following commands to configure log information, debugging information and the time-stamp output format of trap information.

Perform the following operation in System View:

Table 310 Configuring the Output Format of Time-stamp

Operation	Command
Configure the output format of the time-stamp	info-center timestamp { log trap debugging } { boot date none }
Output time-stamp is disabled	undo info-center timestamp { log trap debugging }

4 Configuring SNMP and a network management workstation on the Switch

You have to configure SNMP on the Switch and the remote workstation to ensure that the information is correctly sent to the SNMP NM. Then you can get correct information from the network management workstation.

Turning On/Off the Information Synchronization Switch in Fabric

After the forming of a Fabric by Switches which support XRN; the log, debugging and trap information among the Switches is synchronous. The synchronization process is as follows: each Switch sends its own information to other Switches in the Fabric and meantime receives the information from others, and then the Switch updates the local information to ensure the information synchronizes within the Fabric.

The Switch provides a command to turn on/off the synchronization Switch in every Switch. If the synchronization Switch of a Switch is turned off, it does not send information to other Switches but still receives information from others.

1 Enable info-center

Perform the following operation in System View.

Table 311 Enable/Disable Info-center

Operation	Command
Enable info-center	info-center enable
Disable info-center	undo info-center enable

2 Turn on the information synchronization Switch

Perform the following operation in System View.

Table 312 Turn on/off the Information Synchronization Switch of every Switch

Operation	Command
Turn on the information synchronization Switch of the specified Switch	info-center switch-on { <i>unit-id</i> <i>master</i> <i>all</i> } [<i>debugging</i> <i>logging</i> <i>trapping</i>]*
Turn off the information synchronization Switch of the specified Switch	undo info-center switch-on { <i>unit-id</i> <i>master</i> <i>all</i> } [<i>debugging</i> <i>logging</i> <i>trapping</i>]*

You can turn on/off the synchronization Switch of the specified information on the specified Switch as needed.

Displaying and Debugging Info-Center

After the above configuration, performing the **display** command in any view, you can view the running state of the info-center. You can also authenticate the effect of the configuration by viewing displayed information. By performing the **reset** command in User View, you can clear the statistics of info-center.

Perform the following operation in User View. The **display** command still can be performed in any view.

Figure 74 Displaying and Debugging Info-center

Operation	Command
Display the content of information channel	display channel [<i>channel-number</i> <i>channel-name</i>]
Display configuration of system log and memory buffer	display info-center
Clear information in memory buffer	reset logbuffer
Clear information in trap buffer	reset trapbuffer

Configuration examples of sending logs to Unix loghost

Networking Requirement

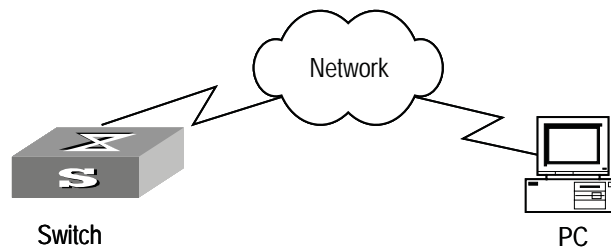
The networking requirement are as follows:

- Sending the log information of the switch to Unix loghost
- The IP address of the loghost is 202.38.1.10

- The information with the severity level above informational will be sent to the loghost
- The output language is English
- The modules that allowed to output information are ARP and IP

Networking diagram

Table 313 Schematic diagram of configuration



Configuration steps

1 Configuration on the switch

```
Enabling info-center
[3com] info-center enable
# Set the host with the IP address of 202.38.1.10 as the loghost; set
the severity level threshold value as informational, set the output
language to English; set that the modules which are allowed to output
information are ARP and IP.
[3com] info-center loghost 202.38.1.10 facility local4 language
english
[3com] info-center source arp channel loghost log level
informational
[3com] info-center source ip channel loghost log level informational
```

2 Configuration on the loghost

This configuration is performed on the loghost. The following example is performed on SunOS 4.0 and the operation on Unix operation system produced by other manufactures is generally the same to the operation on SunOS 4.0.

a Perform the following command as the super user (root).

```
# mkdir /var/log/3com
# touch /var/log/3com/information
```

b Edit file `/etc/syslog.conf` as the super user (root), add the following selector/actor pairs.

```
# 3com configuration messages
local4.info    /var/log/3Com/information
```



Note the following points when editing `/etc/syslog.conf`:

- The note must occupy a line and start with the character #.
- There must be a tab other than a space as the separator in selector/actor pairs.
- No redundant space after file name.

- The device name and the

acceptant log information level specified in `/etc/syslog.conf` must be consistent with `info-center loghost` and `info-center loghost a.b.c.d` facility configured on the switch. Otherwise, the log information probably cannot be output to the loghost correctly.

- c After the establishment of information (log file) and the revision of `/etc/syslog.conf`, you should send a HUP signal to `syslogd` (system daemon),

through the following command, to make `syslogd` reread its configuration file `/etc/syslog.conf`.

```
# ps -ae | grep syslogd
147
# kill -HUP 147
```

After the above operation, the switch system can record information in related log files.



To configure facility, severity, filter and the file `syslog.conf` synthetically, you can get classification in great detail and filter the information.

Configuration examples of sending log to Linux loghost

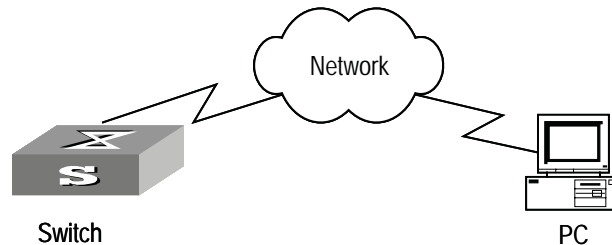
Networking Requirement

The networking requirement are as follows:

- Sending the log information of the switch to Linux loghost
- The IP address of the loghost is 202.38.1.10
- The information with the severity level above informational will be sent to the loghost
- The output language is English
- All modules are allowed to output information

Networking diagram

Figure 75 Schematic diagram of configuration



Configuration steps

```
# Enabling info-center
[3com] info-center enable
# Set the host with the IP address of 202.38.1.10 as the loghost; set
the severity level threshold value as informational, set the output
```

```
language to English; set all the modules are allowed output
information.
[3com] info-center loghost 202.38.1.10 facility local7 language
english
[3com] info-center source default channel loghost log level
informational
```

Configuration on the loghost

This configuration is performed on the loghost.

- a** Perform the following command as the super user (root).

```
# mkdir /var/log/3com
# touch /var/log/3com/information
```

- b** Edit file `/etc/syslog.conf` as the super user (root), add the following selector/actor pairs.

```
# 3com configuration messages
local7.info /var/log/3com/information
```



Note the following points when editing `/etc/syslog.conf`:

- *The note must occupy a line and start with the character #.*
 - *There must be a tab other than a space as the separator in selector/actor pairs.*
 - *No redundant space after file name.*
 - *The device name and the acceptant log information level specified in `/etc/syslog.conf` must be consistent with `info-center loghost` and `info-center loghost a.b.c.d facility` configured on the switch. Otherwise, the log information probably cannot be output to the loghost correctly.*
- c** After the establishment of information (log file) and the revision of `/etc/syslog.conf`, you should view the number of `syslogd` (system daemon) through the following command, kill `syslogd` daemon and **reuse -r** option the start `syslogd` in daemon.

```
# ps -ae | grep syslogd
147
# kill -9 147
# syslogd -r &
```



For Linux loghost, you must ensure that `syslogd` daemon is started by `-r` option.

After the above operation, the switch system can record information in related log files.



To configure facility, severity, filter and the file `syslog.conf` synthetically, you can get classification in great detail and filter the information.

Configuration Examples of Sending Log to Control Terminal

Networking Requirement

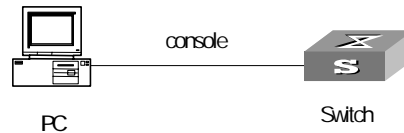
The networking requirements are as follows:

- Sending the log information of the Switch to Unix loghost
- The IP address of the loghost is 202.38.1.10

- The information with the severity level above informational will be sent to the loghost
- The output language is English
- The modules that allowed to output information are ARP and IP

Networking Diagram

Figure 76 Schematic Diagram of Configuration



Configuration Procedure

1 Configuration on the Switch

Enabling info-center

```
[4500]info-center enable
```

2 Configure control terminal log output; allow modules ARP and IP to output information; the severity level is restricted within the range of emergencies to informational.

```
[4500]info-center console channel console
```

```
[4500]info-center source arp channel console log level informational
```

```
[4500]info-center source ip channel console log level informational
```

3 Enabling terminal display function

```
<4500> terminal logging
```


16

SNMP CONFIGURATION

Overview

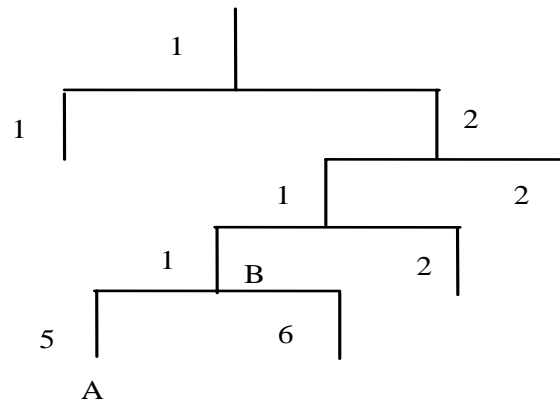
The Simple Network Management Protocol (SNMP) has gained the most extensive application in the computer networks. SNMP has been put into use and widely accepted as an industry standard in practice. It is used for ensuring the transmission of the management information between any two nodes. In this way, network administrators can easily search and modify the information on any node on the network. In the meantime, they can locate faults promptly and implement the fault diagnosis, capacity planning and report generating. SNMP adopts the polling mechanism and provides the most basic function set. It is most applicable to the small-sized, fast-speed and low-cost environment. It only requires the unverified transport layer protocol UDP; and is thus widely supported by many other products.

In terms of structure, SNMP can be divided into two parts, namely, Network Management Station and Agent. Network Management Station is the workstation for running the client program. At present, the commonly used NM platforms include Sun NetManager and IBM NetView. Agent is the server software operated on network devices. Network Management Station can send GetRequest, GetNextRequest and SetRequest messages to the Agent. Upon receiving the requests from the Network Management Station, Agent will perform Read or Write operation according to the message types, generate and return the Response message to Network Management Station. On the other hand, Agent will send Trap message on its own initiative to the Network Management Station to report the events whenever the device encounters any abnormalities such as new device found and restart.

SNMP Versions and Supported MIB

To uniquely identify the management variables of a device in SNMP messages, SNMP adopts the hierarchical naming scheme to identify the managed objects. It is like a tree. A tree node represents a managed object, as shown in the figure below. Thus the object can be identified with the unique path starting from the root.

Figure 77 Architecture of the MIB Tree



The MIB (Management Information Base) is used to describe the hierarchical architecture of the tree and it is the set defined by the standard variables of the monitored network device. In the above figure, the managed object B can be uniquely specified by a string of numbers {1.2.1.1}. The number string is the Object Identifier of the managed object.

The current SNMP Agent of the Switch supports SNMP V1, V2C and V3. The MIBs supported are listed in the following table.

Table 314 MIBs Supported by the Switch

MIB attribute	MIB content	References
Public MIB	MIB II based on TCP/IP network device	RFC1213
	BRIDGE MIB	RFC1493 RFC2675
	RIP MIB	RFC1724
	RMON MIB	RFC2819
	Ethernet MIB	RFC2665
	OSPF MIB	RFC1253
	IF MIB	RFC1573
Private MIB	DHCP MIB	
	QACL MIB	
	ADBM MIB	
	RSTP MIB	
	VLAN MIB	
	Device management	
	Interface management	

Configuring SNMP

The main configuration of SNMP includes:

- Set community name
- Set the Method of Identifying and Contacting the Administrator
- Enable/Disable snmp Agent to Send Trap
- Set the Destination Address of Trap

- Set SNMP System Information
- Set the Engine ID of a Local or Remote Device
- Set/Delete an SNMP Group
- Set the Source Address of Trap
- Add/Delete a User to/from an SNMP Group
- Create/Update View Information or Deleting a View
- Set the Size of SNMP Packet Sent/Received by an Agent
- Enable/Disable a Port Transmitting Trap Information SNMP Agent
- Disable SNMP Agent

Setting Community Name

SNMP V1 and SNMPV2C adopt the community name authentication scheme. The SNMP message incompliant with the community name accepted by the device will be discarded. SNMP Community is named with a character string, which is called Community Name. The various communities can have read-only or read-write access mode. The community with read-only authority can only query the device information, whereas the community with read-write authority can also configure the device.

You can use the following commands to set the community name.

Perform the following configuration in System View.

Table 315 Set Community Name

Operation	Command
Set the community name and the access authority	<code>snmp-agent community { read write } community-name [mib-view view-name] [acl acl-list]</code>
Remove the community name and the access authority	<code>undo snmp-agent community community-name</code>

Enabling/Disabling SNMP Agent to Send Trap

The managed device transmits a trap without request to the Network Management Station to report some critical and urgent events (such as restart).

You can use the following commands to enable or disable the managed device to transmit trap messages.

Perform the following configuration in System View.

Table 316 Enable/Disable SNMP Agent to Send Trap

Operation	Command
Enable to send trap	<code>snmp-agent trap enable [configuration flash ospf [process-id] [ospf-trap-list] standard [authentication coldstart linkdown linkup warmstart]* system]</code>
Disable to send trap	<code>undo snmp-agent trap enable [bgp [backwardtransition] [established] configuration flash ospf [process-id] [ospf-trap-list] standard [authentication coldstart linkdown linkup warmstart]* system]</code>

Setting the Destination Address of Trap

You can use the following commands to set or delete the destination address of the trap.

Perform the following configuration in System View.

Table 317 Set the Destination Address of Trap

Operation	Command
Set the destination address of trap	snmp-agent target-host trap address udp-domain <i>host-addr</i> [udp-port <i>udp-port-number</i>] params securityname <i>community-string</i> [v1 v2c v3 [authentication privacy]]
Delete the destination address of trap	undo snmp-agent target-host <i>host-addr securityname community-string</i>

Setting Lifetime of Trap Message

You can use the following command to set the lifetime of a Trap message. A trap message that exists longer than the set lifetime will be dropped.

Perform the following configuration in System View.

Table 318 Set the Lifetime of Trap Message

Operation	Command
Set lifetime of Trap message	snmp-agent trap life <i>seconds</i>
Restore lifetime of Trap message	undo snmp-agent trap life

By default, the lifetime of Trap message is 120 seconds.

Setting SNMP System Information

The SNMP system information includes the character string *sysContact* (system contact), the character string describing the system location, the version information about the SNMP operating in the system.

You can use the following commands to set the system information.

Perform the following configuration in System View.

Table 319 Set SNMP System Information

Operation	Command
Set SNMP System Information	snmp-agent sys-info { contact <i>sysContact</i> location <i>syslocation</i> version { { v1 v2c v3 } * all } }
Restore the default SNMP System Information of the Switch	undo snmp-agent sys-info [{ contact location }* version { { v1 v2c v3 }* all }]

By default, the *sysLocation* is specified as a blank string, that is, "".

Setting the Engine ID of a Local or Remote Device

You can use the following commands to set the engine ID of a local or remote device.

Perform the following configuration in System View.

Table 320 Set the Engine ID of a Local or Remote Device

Operation	Command
Set the engine ID of the device	snmp-agent local-engineid <i>engineid</i>
Restore the default engine ID of the device.	undo snmp-agent local-engineid

By default, the engine ID is expressed as enterprise No. + device information. The device information can be IP address, MAC address, or user-defined text.

Setting/Deleting an SNMP Group

You can use the following commands to set or delete an SNMP group.

Perform the following configuration in System View.

Table 321 Set/Delete an SNMP Group

Operation	Command
Setting an SNMP group	snmp-agent group { v1 v2c } <i>group-name</i> [read-view <i>read-view</i>] [write-view <i>write-view</i>] [notify-view <i>notify-view</i>] [acl <i>acl-list</i>] snmp-agent group v3 <i>group-name</i> [authentication privacy] [read-view <i>read-view</i>] [write-view <i>write-view</i>] [notify-view <i>notify-view</i>] [acl <i>acl-list</i>]
Deleting an SNMP group	undo snmp-agent group { v1 v2c } <i>group-name</i> undo snmp-agent group v3 <i>group-name</i> [authentication privacy]

Setting the Source Address of Trap

You can use the following commands to set or remove the source address of the trap.

Perform the following configuration in System View.

Table 322 Set the Source Address of Trap

Operation	Command
Set the source address of trap	snmp-agent trap source <i>interface-name</i> <i>interface-num</i>
Remove the source address of trap	undo snmp-agent trap source

Adding/Deleting a User to/from an SNMP Group

You can use the following commands to add or delete a user to/from an SNMP group.

Perform the following configuration in System View.

Table 323 Add/Delete a user to/from an SNMP Group

Operation	Command
Add a user to an SNMP group.	snmp-agent usm-user { v1 v2c } <i>username</i> <i>groupname</i> [acl <i>acl-list</i>] snmp-agent usm-user v3 <i>username</i> <i>groupname</i> [authentication-mode { md5 sha } <i>authpassstring</i> [privacy-mode { des56 privpassstring }]] [acl <i>acl-list</i>]
Delete a user from an SNMP group.	undo snmp-agent usm-user { v1 v2c } <i>username</i> <i>groupname</i> undo snmp-agent usm-user v3 <i>username</i> <i>groupname</i> { local engineid <i>engine-id</i> }

Creating/Updating View Information or Deleting a View

You can use the following commands to create, update the information of views or delete a view.

Perform the following configuration in System View.

Table 324 Create/Update View Information or Deleting a View

Operation	Command
Create/Update view information	<code>snmp-agent mib-view { included excluded } view-name oid-tree</code>
Delete a view	<code>undo snmp-agent mib-view view-name</code>

Setting the Size of SNMP Packet Sent/Received by an Agent

You can use the following commands to set the size of SNMP packet sent/received by an agent.

Perform the following configuration in System View.

Table 325 Set the Size of SNMP Packet sent/received by an Agent

Operation	Command
Set the size of SNMP packet sent/received by an agent	<code>snmp-agent packet max-size byte-count</code>
Restore the default size of SNMP packet sent/received by an agent	<code>undo snmp-agent packet max-size</code>

The agent can receive/send the SNMP packets of the sizes ranging from 484 to 17940, measured in bytes. By default, the size of SNMP packet is 1500 bytes.

Enabling/Disabling a Port Transmitting Trap Information SNMP Agent

To enable/disable a port transmitting trap information SNMP Agent. Perform the following configuration in Ethernet Port View.

Table 326 Enable/Disable a Port Transmitting Trap Information SNMP Agent

Operation	Command
enable current port to transmit the trap information	<code>enable snmp trap updown</code>
disable current port to transmit the trap information	<code>undo enable snmp trap updown</code>

Disabling SNMP Agent

To disable SNMP Agent perform the following configuration in System View.

Table 327 Disable SNMP Agent

Operation	Command
Disable snmp agent	<code>undo snmp-agent</code>

If user disable NMP Agent, it will be enabled whatever `snmp-agent` command is configured thereafter.

Displaying and Debugging SNMP

After the above configuration, execute the `display` command in all views to display the running of the SNMP configuration, and to verify the effect of the configuration. Execute the `debugging` command in User View to debug SNMP configuration.

Operation	Command
Display the statistics information about SNMP packets	<code>display snmp-agent statistics</code>
Display the engine ID of the active device	<code>display snmp-agent { local-engineid remote-engineid }</code>

Operation	Command
Display the group name, the security mode, the states for all types of views, and the storage mode of each group of the Switch.	<code>display snmp-agent group [group-name]</code>
Display the names of all users in the group user table	<code>display snmp-agent usm-user [engineid engineid] [group groupname] [username username]</code>
Display the current community name	<code>display snmp-agent community [read write]</code>
Display the current MIB view	<code>display snmp-agent mib-view [exclude include viewname mib-view]</code>
Display the contact character string of the system	<code>display snmp-agent sys-info contact</code>
Display the location character string of the system	<code>display snmp-agent sys-info location</code>
Display the version character string of the system	<code>display snmp-agent sys-info version</code>

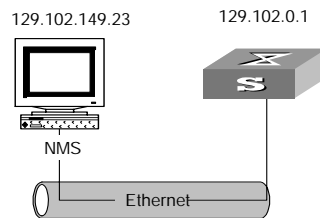
SNMP Configuration Example

Networking Requirements

Network Management Station and the Switch are connected via the Ethernet. The IP address of Network Management Station is 129.102.149.23 and that of the VLAN interface on the Switch is 129.102.0.1. Perform the following configurations on the Switch: set the community name and access authority, administrator ID, contact and Switch location, and enable the Switch to send trap packet.

Networking Diagram

Figure 78 SNMP Configuration Example



Configuration Procedure

- 1 Enter the System View.

```
<4500> system-view
```

- 2 Set the community name, group name and user.

```
[4500]snmp-agent sys-info version all
[4500]snmp-agent community write public
[4500]snmp-agent mib include internet 1.3.6.1
[4500]snmp-agent group v3 managev3group write internet
[4500]snmp-agent usm v3 managev3user managev3group
```

- 3 Set the VLAN interface 2 as the interface used by network management. Add port Ethernet 1/0/3 to the VLAN 2. This port will be used for network management.. set the IP address of VLAN interface 2 as 129.102.0.1.

```
[4500]vlan 2
[4500-vlan2]port ethernet 1/0/3
[4500-vlan2]interface vlan 2
[4500-Vlan-interface2]ip address 129.102.0.1 255.255.255.0
```

- 4 Set the administrator ID, contact and the physical location of the Switch.

```
[4500]snmp-agent sys-info contact Mr.Wang-Tel:3306
[4500]snmp-agent sys-info location telephone-closet,3rd-floor
```

- 5 Enable SNMP agent to send the trap to Network Management Station whose ip address is 129.102.149.23. The SNMP community is public.

```
[4500]snmp-agent trap enable standard authentication
[4500]snmp-agent trap enable standard coldstart
[4500]snmp-agent trap enable standard linkup
[4500]snmp-agent trap enable standard linkdown
[4500]snmp-agent target-host trap address udp-domain 129.102.149.23
udp-port 5000 params securityname public
```

Configure Network Management System

The Switch supports 3Com Network Director. Users can query and configure the Switch through the network management system. For more information, refer to the network management user documentation.

Reading Usmsr Table Configuration Example

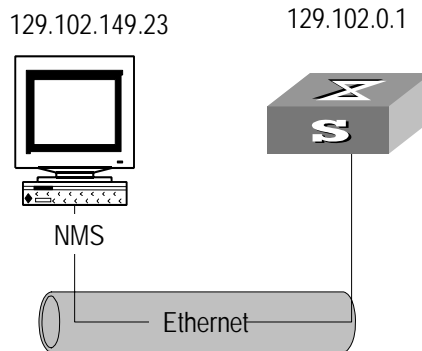
Networking Requirements

ViewDefault view should be reconfigured if you use SNMP V3 to read the usmsr table.

The snmpVacmMIB and snmpUsmMIB should be included in ViewDefault view.

Networking Diagram

Figure 79 SNMP configuration example



Configuration procedure

```
[4500]snmp-agent community read public
[4500]snmp-agent community write private
[4500]snmp-agent sys-info version all
[4500]snmp-agent group v3 sdsdsd
[4500]snmp-agent usm-user v3 paul sdsdsd authentication-mode md5
hello
[4500]snmp-agent mib-view included ViewDefault snmpUsmMIB
[4500]snmp-agent mib-view included ViewDefault snmpVacmMIB
[4500]display snmp-agent mib-view
View name:ViewDefault
  MIB Subtree:iso
  Subtree mask:
  Storage-type: nonVolatile
  View Type:included
  View status:active

View name:ViewDefault
  MIB Subtree:snmpUsmMIB
  Subtree mask:
  Storage-type: nonVolatile
  View Type:excluded
  View status:active

View name:ViewDefault
  MIB Subtree:snmpVacmMIB
  Subtree mask:
  Storage-type: nonVolatile
  View Type:excluded
  View status:active
```

```
View name:ViewDefault
  MIB Subtree:snmpModules.18
  Subtree mask:
  Storage-type: nonVolatile
  View Type:excluded
  View status:active
```

17

RMON CONFIGURATION

Overview

Remote Network Monitoring (RMON) is a type of IETF-defined MIB. It is the most important enhancement to the MIB II standard. It is mainly used for monitoring the data traffic on a segment and even on a whole network. It is one of the most widely used Network Management standards.

RMON is implemented fully based on the SNMP architecture (which is one of its outstanding advantages) and compatible with the existing SNMP framework, and therefore it is unnecessary to adjust the protocol. RMON includes NMS and the Agent running on the network devices. On the network monitor or detector, RMON Agent tracks and accounts different traffic information on the segment connected to its port, such as the total number of packets on a segment in a certain period of time or that of the correct packets sent to a host. RMON helps SNMP monitor the remote network device more actively and effectively, which provides a highly efficient means for the monitoring of the subnet operations. RMON can reduce the communication traffic between the NMS and the agent, thus facilitating effective management over large interconnected networks.

RMON allows multiple monitors. It can collect data in two ways.

- One is to collect data with a special RMON probe. NMS directly obtains the management information from the RMON probe and controls the network resource. In this way, it can obtain all the information of the RMON MIB.
- Another way is to implant the RMON Agent directly into the network devices (such as a Switch, Hub, etc.), so that the devices become network facilities with RMON probe function. RMON NMS uses the basic SNMP commands to exchange data information with SNMP Agent and collect NM information. However, limited by the device resources, normally, not all the data of the RMON MIB can be obtained with this method. In most cases, only four groups of information can be collected. The four groups include trap information, event information, history information and statistics information.

The Switch implements RMON as described in the second bullet point above. With the RMON-supported SNMP Agent running on the network monitor, NMS can obtain such information as the overall traffic of the segment connected to the managed network device port, the error statistics and performance statistics, thereby implementing the management (generally remote management) over the network.

Configuring RMON

RMON configuration includes:

- Add/Delete an Entry to/from the Alarm table
- Add/Delete an Entry to/from the Event table

- Add/Delete an Entry to/from the History Control terminal
- Add/Delete an Entry to/from the extended RMON alarm table
- Add/Delete an Entry to/from the Statistics table

Adding/Deleting an Entry to/from the Alarm Table

RMON alarm management can monitor the specified alarm variables such as the statistics on a port. When a value of the monitored data exceeds the defined threshold, an alarm event will be generated. Generally, the event will be recorded in the device log table and a trap message will be sent to the NMS. The events are defined in the event management. The alarm management includes browsing, adding and deleting the alarm entries.

You can use the following commands to add/delete an entry to/from the alarm table.

Perform the following configuration in System View.

Table 329 Add/Delete an Entry to/from the Alarm Table

Operation	Command
Add an entry to the alarm table.	rmon alarm <i>entry-number</i> <i>alarm-variable</i> <i>sampling-time</i> { delta absolute } rising-threshold <i>threshold-value1</i> <i>event-entry1</i> falling-threshold <i>threshold-value2</i> <i>event-entry2</i> [owner <i>text</i>]
Delete an entry from the alarm table.	undo rmon alarm <i>entry-number</i>

Adding/Deleting an Entry to/from the Event Table

RMON event management defines the event ID and the handling of the event by keeping logs, sending trap messages to NMS or performing both at the same time.

You can use the following commands to add/delete an entry to/from the event table.

Perform the following configuration in System View.

Table 330 Add/Delete an Entry to/from the Event Table

Operation	Command
Add an entry to the event table.	rmon event <i>event-entry</i> [description <i>string</i>] { log trap <i>trap-community</i> log-trap <i>log-trapcommunity</i> none } [owner <i>rmon-station</i>]
Delete an entry from the event table.	undo rmon event <i>event-entry</i>

Adding/Deleting an Entry to/from the History Control Terminal

The history data management helps you set the history data collection, periodical data collection and storage of the specified ports. The sampling information includes the utilization ratio, error counts and total number of packets.

You can use the following commands to add/delete an entry to/from the history control terminal.

Perform the following configuration in Ethernet Port View.

Table 331 Add/Delete an Entry to/from the History Control Terminal

Operation	Command
Add an entry to the history control terminal.	rmon history <i>entry-number</i> buckets <i>number</i> interval <i>sampling-interval</i> [owner <i>text-string</i>]
Delete an entry from the history control terminal.	undo rmon history <i>entry-number</i>

Adding/Deleting an Entry to/from the Extended RMON Alarm Table

You can use the command to add/delete an entry to/from the extended RMON alarm table.

Perform the following configuration in System View.

Table 332 Add/Delete an Entry to/from the Extended RMON Alarm Table

Operation	Command
Add an entry to the extended RMON alarm table.	rmon prialarm <i>entry-number</i> <i>alarm-var</i> [<i>alarm-des</i>] sampling-timer { 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 } [owner <i>text</i>]
Delete an entry from the extended RMON alarm table.	undo rmon prialarm <i>entry-number</i>

Adding/Deleting an Entry to/from the Statistics Table

The RMON statistics management concerns the port usage monitoring and error statistics when using the ports. The statistics include collision, CRC and queuing, undersize packets or oversize packets, timeout transmission, fragments, broadcast, multicast and unicast messages and the usage ratio of bandwidth.

You can use the following commands to add/delete an entry to/from the statistics table.

Perform the following configuration in Ethernet Port View.

Table 333 Add/Delete an Entry to/from the Statistics Table

Operation	Command
Add an entry to the statistics table	rmon statistics <i>entry-number</i> [owner <i>text-string</i>]
Delete an entry from the statistics table	undo rmon statistics <i>entry-number</i>

Displaying and Debugging RMON

After the above configuration, execute the **display** command in all views to display the running of the RMON configuration, and to verify the effect of the configuration.

Table 334 Display and Debug RMON

Operation	Command
Display the RMON statistics	display rmon statistics [<i>port-num</i>]
Display the history information of RMON	display rmon history [<i>port-num</i>]
Display the alarm information of RMON	display rmon alarm [<i>alarm-table-entry</i>]

Operation	Command
Display the extended alarm information of RMON	display rmon prialarm [prialarm-table-entry]
Display the RMON event	display rmon event [event-table-entry]
Display the event log of RMON	display rmon eventlog [event-number]

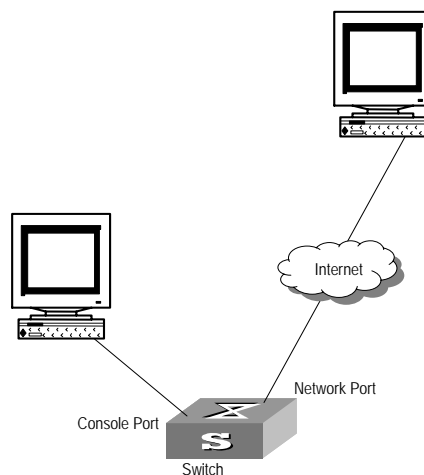
RMON Configuration Example

Networking Requirements

Set an entry in RMON Ethernet statistics table for the Ethernet port performance, which is convenient for network administrators' query.

Networking Diagram

Figure 80 RMON Configuration Networking



Configuration Procedure

- 1 Configure RMON.

```
[4500-Ethernet1/0/1]rmon statistics 1 owner 3com-rmon
```

- 2 View the configurations in User View.

```
<4500> display rmon statistics Ethernet 1/0/1
Statistics entry 1 owned by 3com-rmon is VALID.
Gathers statistics of interface Ethernet1/0/1. Received:
octets          : 270149,packets          : 1954
broadcast packets :1570 ,multicast packets:365
undersized packets :0 ,oversized packets:0
fragments packets :0 ,jabbers packets :0
CRC alignment errors:0 ,collisions :0
Dropped packet events (due to lack of resources):0
Packets received according to length (in octets):
64 :644 , 65-127 :518 , 128-255 :688
256-511:101 , 512-1023:3 , 1024-1518:0
```

18

NTP CONFIGURATION

Overview

Network time protocol (NTP) is a time synchronization protocol defined in RFC1305. It is used for time synchronization between a set of distributed time servers and clients. NTP transmits packets through UDP port 123.

NTP is intended for time synchronization between all devices that have clocks in a network so that the clocks of all devices can keep consistent. Thus, the devices can provide multiple unified-time-based applications.

A local system running NTP can not only be synchronized by other clock sources, but also serve as a clock source to synchronize other clocks. Besides, it can synchronize, or be synchronized by other systems by exchanging NTP packets.

Applications of NTP

NTP is mainly applied to synchronizing the clocks of all devices in a network. For example:

- In network management, the analysis of the log information and debugging information collected from different devices is meaningful and valid only when network devices that generate the information adopts the same time.
- The billing system requires that the clocks of all network devices be consistent.
- Some functions, such as restarting all network devices in a network simultaneously require that they adopt the same time.
- When multiple systems cooperate to handle a rather complex transaction, they must adopt the same time to ensure a correct execution order.
- To perform incremental backup operations between a backup server and a host, you must make sure they adopt the same time.

As setting the system time manually in a network with many devices leads to a lot of workload and cannot ensure the accuracy, it is unfeasible for an administrator to perform the operation. However, an administrator can synchronize the clocks of devices in a network with required accuracy by performing NTP configuration.

NTP has the following advantages:

- Defining the accuracy of clocks by stratum to synchronize the clocks of all devices in a network quickly
- Supporting access control and MD5 authentication
- Sending protocol packets in unicast, multicast, or broadcast mode



- *The clock stratum determines the accuracy, which ranges from 1 to 16. The stratum of a reference clock ranges from 1 to 15. The clock accuracy decreases as the stratum number increases. A stratum 16 clock is in the unsynchronized state and cannot serve as a reference clock.*

- The local clock of an Switch 4500 cannot operate as a reference clock. It can serve as a NTP server only after synchronized.

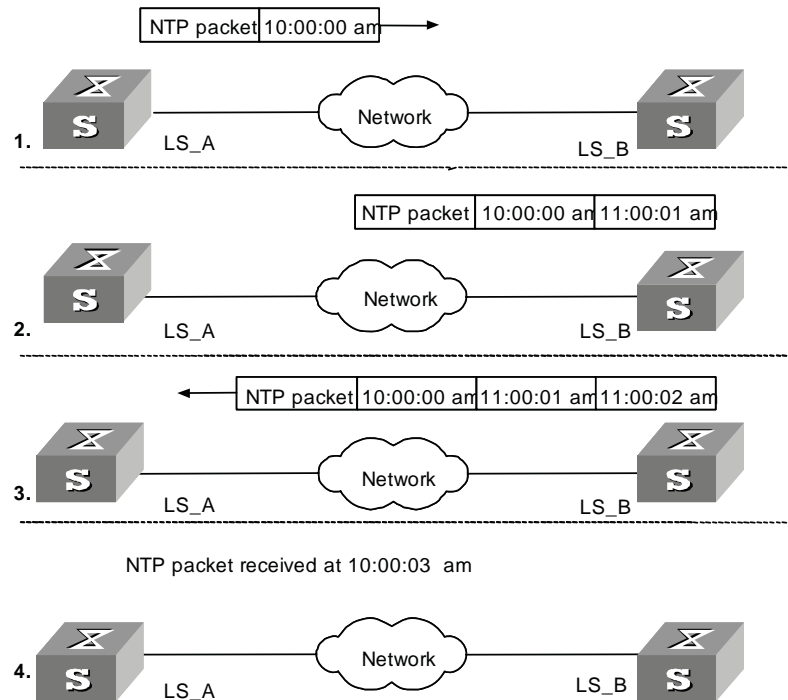
Implementation Principle of NTP

Figure 81 shows the implementation principle of NTP.

Ethernet switch A (LS_A) is connected to Ethernet switch B (LS_B) through Ethernet ports. Both have their own system clocks, and they need to synchronize the clocks of each other through NTP. To help you to understand the implementation principle, we suppose that:

- Before the system clocks of LS_A and LS_B are synchronized, the clock of LS_A is set to 10:00:00 am, and the clock of LS_B is set to 11:00:00 am.
- LS_B serves as the NTP server, that is, the clock of LS_A will be synchronized to that of LS_B.
- It takes one second to transfer an NTP packet from LS_A to LS_B or from LS_A to LS_B.

Figure 81 Implementation principle of NTP



The procedure of synchronizing the system clock is as follows:

- LS_A sends an NTP packet to LS_B, with a timestamp 10:00:00 am (T_1) identifying when it is sent.
- When the packet arrives at LS_B, LS_B inserts its own timestamp 11:00:01 am (T_2) into the packet.
- When the NTP packet leaves LS_B, LS_B inserts its own timestamp 11:00:02 am (T_3) into the packet.

- When receiving a response packet, LS_A inserts a new timestamp 10:00:03 am (T_4) into it.

At this time, LS_A has enough information to calculate the following two parameters:

- Delay for an NTP packet to make a round trip between LS_A and LS_B:
 $Delay = (T_4 - T_1) - (T_3 - T_2)$.
- Time offset of LS_A relative to LS_B:
 $Offset = ((T_2 - T_1) + (T_3 - T_4))/2$.

LS_A can then set its own clock according to the above information to synchronize its clock to that of LS_B.

For detailed information, refer to RFC1305.

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.

Figure 82 Client/sever mode

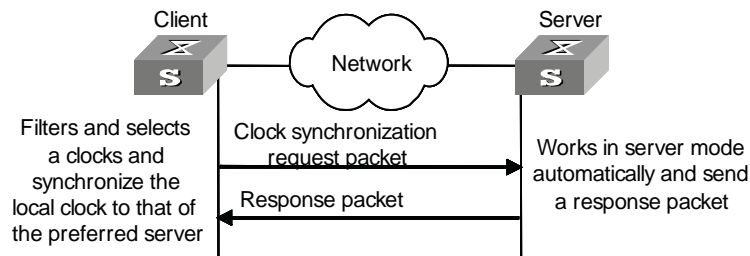
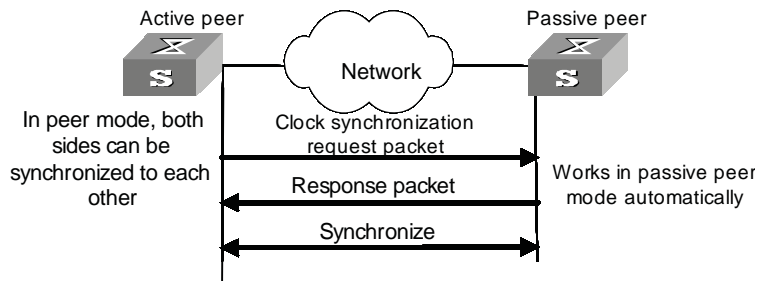


Figure 83 Peer mode



In the peer mode, the local Switch 4500 Ethernet switch serves as the active peer and sends clock synchronization request packets first, while the remote server serves as the passive peer automatically.

If both of the peers have reference clocks, the one with a smaller stratum number is adopted.

Figure 84 Broadcast Mode

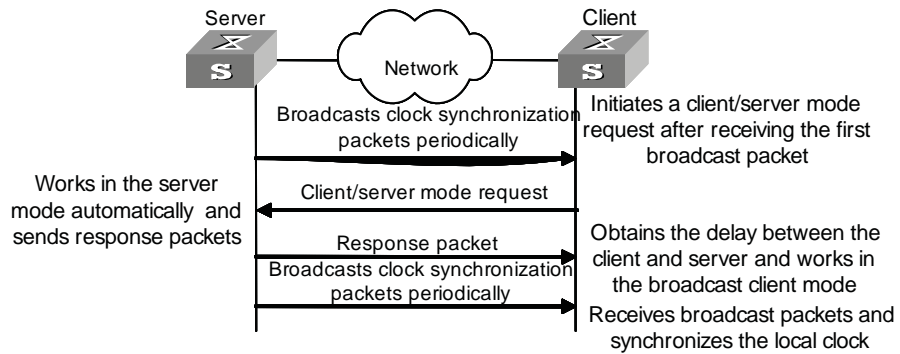
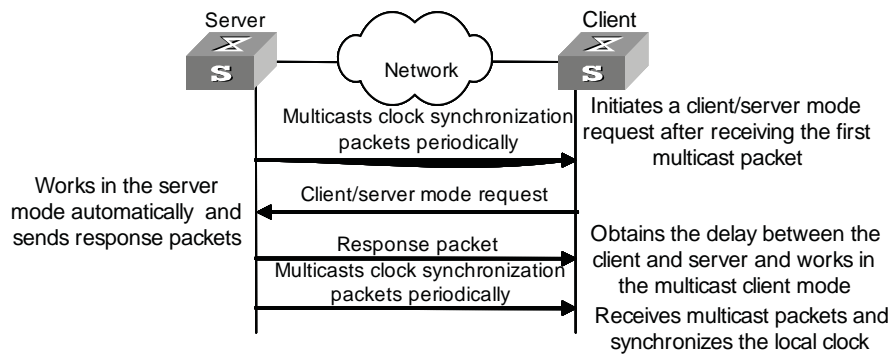


Figure 85 Multicast mode



[Table 335](#) describes how the above mentioned NTP modes are implemented on the Switch 4500.

Table 335 NTP implementation modes on the Switch 4500 Family

NTP implementation mode	Configuration on the Switch 4500 Family
Client/server mode	Configure the local Switch 4500 to operate in the NTP server mode. In this mode, the remote server serves as the local time server, while the local switch serves as the client.
Peer mode	Configure the local Switch 4500 to operate in NTP peer mode. In this mode, the remote server serves as the peer of the Switch 4500, and the local switch serves as the active peer.
Broadcast mode	<ul style="list-style-type: none"> Configure the local Switch 4500 to operate in NTP broadcast server mode. In this mode, the local switch broadcasts NTP packets through the VLAN interface configured on the switch. Configure the Switch 4500 to operate in NTP broadcast client mode. In this mode, the local Switch 4500 receives broadcast NTP packets through the VLAN interface configured on the switch.

NTP implementation mode	Configuration on the Switch 4500 Family
Multicast mode	<ul style="list-style-type: none"> ■ Configure the local Switch 4500 Ethernet switch to operate in NTP multicast server mode. In this mode, the local switch sends multicast NTP packets through the VLAN interface configured on the switch. ■ Configure the local Switch 4500 Ethernet switch to operate in NTP multicast client mode. In this mode, the local switch receives multicast NTP packets through the VLAN interface configured on the switch.



CAUTION: An Switch 4500 can operate in the NTP peer, NTP broadcast server, or NTP multicast server mode only after its clock is synchronized.

Configuring NTP Implementation Modes

A Switch 4500 can operate in one of the following NTP modes:

- NTP client mode
- NTP server mode
- NTP peer mode
- NTP broadcast server mode
- NTP broadcast client mode
- NTP multicast server mode
- NTP multicast client mode

Configuration Prerequisites

You need to perform configurations only on the client (or the active peer) when you want a Switch 4500 to operate in NTP server mode (or NTP peer mode). However, you need to perform configurations on both the server and client when you want the switch to operate in NTP broadcast mode or NTP multicast mode.

Configuration Procedure

[Table 336](#) describes how to configure the Switch 4500 NTP modes.

Table 336 Configure NTP implementation modes

Operation	Command	Description
Enter system view	system-view	
Configure the switch to operate in NTP client mode	ntp-service unicast-server { <i>remote-ip</i> <i>server-name</i> } [authentication-keyid <i>key-id</i> priority source-interface Vlan-interface <i>vlan-id</i> version <i>number</i>]*	Optional By default, no Ethernet switch operates in NTP client mode.
Configure the switch to operate in NTP peer mode	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>]*	Optional By default, no Ethernet switch operates in NTP peer mode.
Enter VLAN interface view	interface Vlan-interface <i>vlan-id</i>	

Operation	Command	Description
Configure the switch to operate in the NTP broadcast client mode	ntp-service broadcast-client	Optional By default, no Ethernet switch operates in NTP broadcast client mode.
Configure the switch to operate in NTP broadcast server mode	ntp-service broadcast-server [authentication-keyid key-id version number]*	Optional By default, no Ethernet switch operates in NTP broadcast server mode.
Configure the switch to operate in NTP multicast client mode	ntp-service multicast-client [ip-address]	Optional By default, no Ethernet switch operates in NTP multicast client mode.
Configure the switch to operate in NTP multicast server mode	ntp-service multicast-server [ip-address] [authentication-keyid keyid ttl ttl-number version number]*	Optional By default, no Ethernet switch operates in NTP multicast server mode.



To reduce the risk of being attacked by malicious users against opened socket and enhance switch security, the Switch 4500 Ethernet switches provides the following functions, so that a socket is opened only when it is needed:

- *Opening UDP port 123 (used for NTP) when NTP is enabled;*
- *Close UDP port 123 when NTP is disabled.*

The preceding functions are implemented as follows:

- When you enable NTP by using the `ntp-service unicast-server`, `ntp-service unicast-peer`, `ntp-service broadcast-client`, `ntp-service broadcast-server`, `ntp-service multicast-client`, or `ntp-service multicast-server` command, UDP port 123 is opened at the same time.
- When you disable NTP from operating in any modes by using the undo forms of the preceding six commands, UDP port 123 is closed at the same time.

NTP client mode

The remote server specified by the `remote-ip` or `server-name` argument serves as the NTP server. The local Switch 4500 serves as the client. The clock of the client is synchronized to the NTP server, while the clock of the NTP server is not synchronized to the client. The IP address specified by the `remote-ip` argument cannot be a broadcast address, a multicast address, or the IP address used by the local reference clock.

NTP peer mode

The remote server specified by the `remote-ip` or `peer-name` argument serves as the peer of the local Ethernet switch, and the local Ethernet switch operates in the active peer mode. The clock of the local switch can be synchronized to the remote server or used to synchronize the clock of the remote server. The IP address specified by the `remote-ip` argument cannot be a broadcast address, a multicast address, or the IP address used by the local reference clock.

NTP broadcast server mode

When a Switch 4500 operates in NTP broadcast server mode, it broadcasts clock synchronization packets periodically. The devices in NTP broadcast client mode will respond to these packets and start the clock synchronization process.

NTP multicast server mode

When a Switch 4500 operates in NTP multicast server mode, it multicasts clock synchronization packets periodically. The devices in the NTP multicast client mode will respond to these packets and start the clock synchronization process. The switch operating in this mode can support up to 1,024 multicast clients.



- *The total number of the servers and peers configured for a switch is up to 128.*
- *After the configuration, a Switch 4500 does not establish connections with peers if it operates in NTP server mode. Whereas if it operates in any of the other modes, it establishes connections with peers.*
- *If a Switch 4500 operates in passive peer mode, NTP broadcast client mode, or NTP multicast client mode, it establishes connections with peers dynamically. If it operates in any of the other modes, it establishes connections with peers statically.*

Configuring Access Control Right

The access control right to the NTP server only provides a minimal degree of security measure. A more secure way is to perform identity authentication.

The right of an access request received by the NTP server is matched from the highest to the lowest in order of peer, server, synchronization, and query.

Table 337 Configure the access control right to the local NTP server

Operation	Command	Description
Enter system view	system-view	
Configure the access control right to the local NTP server	ntp-service access { peer server synchronization query } acl-number	Optional By default, the access control right to the local NTP server is peer.

Configuring NTP Authentication

In networks with higher security requirements, the NTP authentication function must be enabled to run NTP. Through password authentication on the client and the server, the client is synchronized only to the server that passes the authentication. This improves network security.

Configuration Prerequisites

NTP authentication configuration involves:

- Configuring NTP authentication on the client
- Configuring NTP authentication on the server

Observe the following principles when configuring NTP authentication:

- If the NTP authentication function is not enabled on the client, the client can be synchronized to a server no matter whether the NTP authentication function is

enabled on the server (assuming that other related configurations are performed).

- You need to couple the NTP authentication with a trusted key.
- Configurations on the server and the client must be consistent.
- The client with the NTP authentication function enabled is only synchronized to the server that provides a trusted key.

Configuration Procedure

Table 338 Configuring the NTP authentication on the client

Operation	Command	Description
Enter system view	system-view	
Enable the NTP authentication function globally	ntp-service authentication enable	Required By default, the NTP authentication function is disabled.
Configure the NTP authentication key	ntp-service authentication-keyid <i>key-id</i> authentication-model md5 <i>value</i>	Required By default, no NTP authentication key is configured.
Configure the specified key to be 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	NTP client mode: ntp-service unicast-server { <i>remote-ip</i> <i>server-name</i> } authentication-keyid <i>key-id</i> Peer mode: ntp-service unicast-peer { <i>remote-ip</i> <i>peer-name</i> } authentication-keyid <i>key-id</i>	In NTP client mode and NTP peer mode, you need to associate the specified key with the corresponding NTP server on the client. You can associate the NTP server with the authentication key while configuring NTP mode. You can also use this command to associate them after configuring NTP mode.

NTP authentication requires that the authentication keys configured for the server and the client are the same. Besides, the authentication keys must be trusted keys. Otherwise, the client cannot be synchronized with the server.

In NTP server mode and NTP peer mode, you need to associate the specified key with the corresponding NTP server (active peer) on the client (passive peer). In these two modes, multiple servers (active peers) may be configured for a client/passive peer, and therefore, the authentication key is required to determine which server the client is synchronized to.

Table 339 Configuring NTP authentication on the server

Operation	Command	Description
Enter system view	system-view	
Enable NTP authentication	ntp-service authentication enable	Required By default, the NTP authentication function is disabled.

Operation	Command	Description
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 to be a trusted key	ntp-service reliable authentication-keyid <i>key-id</i>	Required By default, no trusted authentication key is configured.
Enter VLAN interface view	interface Vlan-interface <i>vlan-id</i>	
Associate the specified key with the corresponding NTP server	Broadcast server mode: ntp-service broadcast-server authentication-keyid <i>key-id</i> Multicast server mode: ntp-service multicast-server authentication-keyid <i>key-id</i>	In NTP broadcast server mode and NTP multicast server mode, you need to associate the specified key with the corresponding NTP server on the server You can associate an NTP server with an authentication key while configuring NTP mode. You can also use this command to associate them after configuring the NTP mode.

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

Optional NTP parameters are:

- Local VLAN interface that sends NTP packets
- Number of dynamic sessions that can be established locally
- VLAN interface disabled from receiving NTP packets

Table 340 Configure optional NTP parameters

Operation	Command	Description
Enter system view	system-view	
Configure a local interface that sends NTP packets	ntp-service source-interface Vlan-interface <i>vlan-id</i>	Optional
Configure the number of sessions that can be established locally	ntp-service max-dynamic-sessions <i>number</i>	Optional By default, up to 100 dynamic sessions can be established locally.
Enter VLAN interface view	interface Vlan-interface <i>vlan-id</i>	
Disable an interface from receiving NTP packets	ntp-service in-interface disable	Optional By default, a VLAN interface receives NTP packets.



CAUTION:

If a sending interface is specified in the `ntp-service unicast-server` command or the `ntp-service unicast-peer` command, the source IP address of an NTP packet is the address of this interface.

Dynamic connections can be established when a switch operates in passive peer mode, NTP broadcast client mode, or NTP multicast client mode. In other modes, the connections established are static.

Displaying and Debugging NTP

After the performing the above configurations, you can execute display commands in any view to display the switch's running status and verify the effect of the configuration.

Table 341 Display and debug NTP

Operation	Command	Description
Display the status of NTP services	display ntp-service status	The display commands can be executed in any view
Display the information about the sessions maintained by NTP	display ntp-service sessions [verbose]	
Display the brief information about NTP servers along the path from the local device to the reference clock source	display ntp-service trace	

Configuration Examples

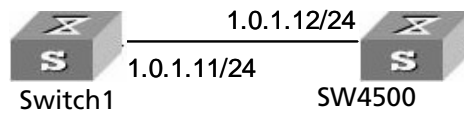
Configuring NTP Server Mode

Network requirements

The local clock of the is set to the NTP master clock, with a stratum level of 2. The Switch1 is a 4500 switch that allows the local clock to serve as the NTP master clock. The SW4500 considers that Switch1 is the NTP server and operates in client mode, while SW4500 operates in server mode automatically.

Network Diagram

Table 342 Network diagram for the NTP server mode configuration



Configuration procedure

Configure the following on Switch 4500.

```

# View the NTP status of the Swich 4500 before synchronization.
<4500> display ntp-service status
Clock status: unsynchronized
Clock stratum: 16
Reference clock ID: none
Nominal frequency: 99.8562 Hz
Actual frequency: 99.8562 Hz
  
```

```

Clock precision: 2^7
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 Switch1 to the NTP server of the Switch 4500.
<4500> system-view
[4500] ntp-service unicast-server 1.0.1.11

# (After the above configurations, the Switch 4500 is synchronized to
Switch1.) View the NTP status of the Switch 4500.

[4500] display ntp-service status
Clock status: synchronized
Clock stratum: 3
Reference clock ID: 1.0.1.11
Nominal frequency: 250.0000 Hz
Actual frequency: 249.9992 Hz
Clock precision: 2^19
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 Sep 6 2001 (BF422AE4.05AEA86C)

```

The above output information indicates that Switch4500 is synchronized with Switch1, and the stratum level of its clock is 3, one level lower than that of Switch1.

View the information about NTP sessions of the Switch 4500. (You can see that Switch2 establishes a connection with Switch1.)

```

[4500] 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

```

Configuring NTP Peer Mode

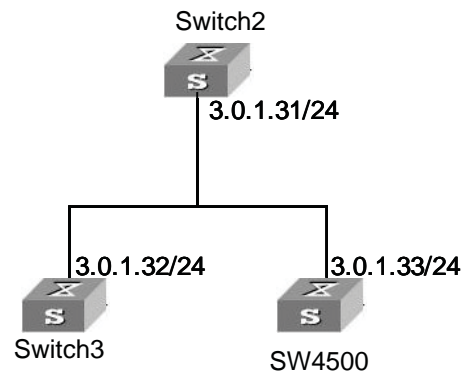
Network requirements

The local clock of Switch2 is set to the NTP master clock, with the clock stratum level of 2.

A Switch 4500 considers Switch2 as the NTP server and serves as the client, while Switch2 operates in server mode automatically. In addition, Switch3 considers the Switch 4500 as its peer.

This example assumes that:

- Switch2 is a switch that allows its local clock to be the master clock.
- Switch3 is a switch that allows its local clock to be the master clock and the stratum level of its clock is 1.

Figure 86 Network diagram for NTP peer mode configuration**Configuration procedure**

- 1 Configure the Switch 4500.

```

# Set Switch2 to the NTP server.
<SW4500> system-view
[SW4500] ntp-service unicast-server 3.0.1.31
  
```

- 2 Configure Switch3 (after the SW4500 Ethernet switch is synchronized to Switch2).

```

# Enter system view.
<Switch3> system-view
[Switch3]
# Set the SW4500 Ethernet switch to the peer of Switch3.
[Switch3] ntp-service unicast-peer 3.0.1.33
  
```

The SW4500 Ethernet switch and Switch3 are a pair of peers. Switch3 operates in active peer mode, while the SW4500 Ethernet switch operates in passive peer mode. Because the stratum level of the local clock of Switch3 is 1, and that of the SW4500 Ethernet switch is 3, the SW4500 Ethernet switch is synchronized to Switch3.

View the status of the SW4500 Ethernet switch after synchronization.

```

[Sw4500] display ntp-service status
Clock status: synchronized
Clock stratum: 2
Reference clock ID: 3.0.1.32
Nominal frequency: 250.0000 Hz
Actual frequency: 249.9992 Hz
Clock precision: 2^19
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 Sep 6 2001 (BF422AE4.05AEA86C)
  
```

The output information indicates that the SW4500 Ethernet switch is synchronized to Switch3 and the stratum level of its local clock is 2, one level lower than that Switch3.

```
# View the information about the NTP sessions of the SW4500 Ethernet
switch (you can see that a connection is established between the
SW4500 Ethernet switch and Switch3).
[SW4500] display ntp-service sessions
      source      reference      strata reach poll now offset delay disper
*****
[2]3.0.1.32      127.127.1.0      1      1      64      1      350.1      15.1      0.0
note: 1 source(master),2 source(peer),3 selected,4 candidate,5 configured
```

Configuring NTP Broadcast Mode

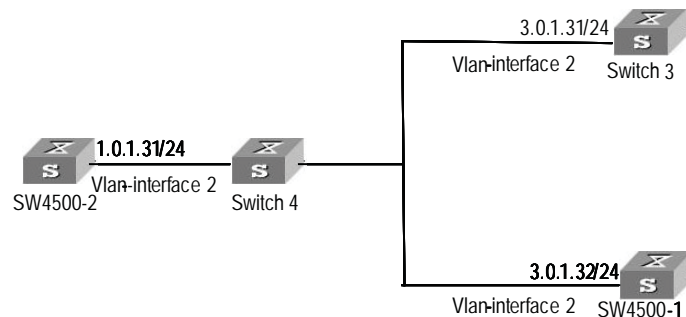
Network requirements

The local clock of Switch3 is set to the NTP master clock, with a stratum level of 2. NTP packets are broadcast through Vlan-interface2. Configure SW4500-1 and SW4500-2 to listen to broadcast packets through their own Vlan-interface2.

This example assumes that Switch3 is a switch that supports the local clock being the master clock.

Network diagram

Figure 87 Network diagram for the NTP broadcast mode configuration



Configuration procedure

1 Configure Switch3.

```
# Enter system view.
<Switch3> system-view
[Switch3]
# Enter Vlan-interface2 view.
[Switch3] interface Vlan-interface 2
[Switch3-Vlan-interface2]
# Set switch3 to the broadcast server, which sends broadcast packets
through Vlan-interface2.
[Switch3-Vlan-interface2] ntp-service broadcast-server
```

2 Configure SW4500-1.

```
# Enter system view.
<SW4500-1> system-view
[SW4500-1]
# Enter Vlan-interface2 view.
[SW4500-1] interface Vlan-interface 2
[SW4500-1-Vlan-interface2]
# Set SW4500-1 to a broadcast client.
[SW4500-1-Vlan-interface2] ntp-service broadcast-client
```

3 Configure SW4500-2

```

# Enter system view.
<SW4500-2> system-view
[SW4500-2]
# Enter Vlan-interface2 view.
[SW4500-2] interface Vlan-interface 2
[SW4500-2-Vlan-interface2]
# Set SW4500-2 to a broadcast client.
[SW4500-2-Vlan-interface2] ntp-service broadcast-client

```

After the above configurations, SW4500-1 and SW4500-2 will listen to broadcast packets through their own Vlan-interface2, and Switch3 will send broadcast packets through Vlan-interface2. Because SW4500-2 and Switch3 do not share the same network segment, SW4500-2 cannot receive broadcast packets from Switch3, while SW4500-1 is synchronized to Switch3 after receiving broadcast packets from Switch3.

View the status of SW4500-1 after synchronization.

```

[SW4500-1] display ntp-service status
Clock status: synchronized
Clock stratum: 3
Reference clock ID: 3.0.1.31
Nominal frequency: 250.0000 Hz
Actual frequency: 249.9992 Hz
Clock precision: 2^19
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 Sep 6 2001 (BF422AE4.05AEA86C)

```

The output information indicates that SW4500-1 is synchronized to Switch3, with the clock stratum level of 3, one level lower than that of Switch3.

```

# View the information about the NTP sessions of SW4500-1 and you can
see that a connection is established between SW4500-1 and Switch3.
[SW4500-1] display ntp-service sessions
      source           reference           stra reach poll  now offset  delay disper
*****
[1]3.0.1.31           127.127.1.0        2    1    64  377   26.1  199.53  9.7
note: 1 source(master),2 source(peer),3 selected,4 candidate,5 configured

```

Configuring NTP Multicast Mode

Network requirements

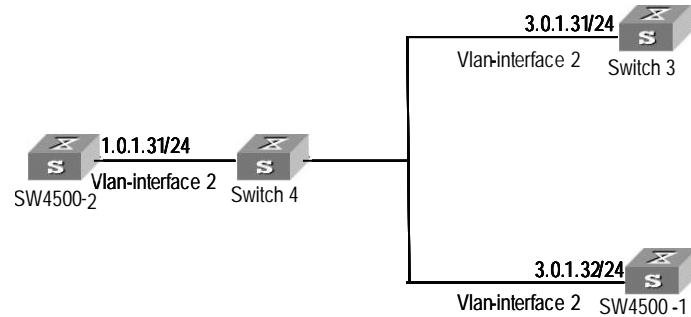
The local clock of Switch3 is set to the NTP master clock, with a clock stratum level of 2. Switch3 advertises multicast packets through Vlan-interface2.

SW4500-1 and SW4500-2 respectively listen to multicast packets through their own Vlan-interface2.

This example assumes that Switch3 is a switch that supports the local clock being the master clock.

Network diagram

Figure 88 Network diagram for NTP multicast mode configuration



Configuration procedure

1 Configure Switch3.

```
# Enter system view.
<Switch3> system-view
[Switch3]
# Enter Vlan-interface2 view.
[Switch3] interface Vlan-interface 2
# Set Switch3 to a multicast server.
[Switch3-Vlan-interface2] ntp-service multicast-server
```

2 Configure SW4500-1.

```
# Enter system view.
<SW4500-1> system-view
[SW4500-1]
# Enter Vlan-interface2 view.
[SW4500-1] interface Vlan-interface 2
# Set SW4500-1 to a multicast client.
[SW4500-1-Vlan-interface2] ntp-service multicast-client
```

3 Configure SW4500-2.

```
# Enter system view.
<SW4500-2> system-view
[SW4500-2]
# Enter Vlan-interface2 view.
[SW4500-2] interface Vlan-interface 2
# Set SW4500-2 to a multicast client.
[SW4500-2-Vlan-interface2] ntp-service multicast-client
```

After the above configurations, SW4500-1 and SW4500-2 respectively listen to multicast packets through their own Vlan-interface2, and Switch3 advertises multicast packets through Vlan-interface2. Because SW4500-2 and SW4500-3 do not share the same network segment, SW4500-2 cannot receive multicast packets

from Switch3, while SW4500-1 is synchronized to Switch3 after receiving multicast packets from Switch3.

View the status of SW4500-1 after synchronization.

```
[SW4500-1] display ntp-service status
Clock status: synchronized
Clock stratum: 3
Reference clock ID: 3.0.1.31
Nominal frequency: 250.0000 Hz
Actual frequency: 249.9992 Hz
Clock precision: 2^19
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 Sep 6 2001 (BF422AE4.05AEA86C)
```

The output information indicates that SW4500-1 is synchronized to Switch3, with a clock stratum level of 3, one stratum level lower than that Switch3.

View the information about the NTP sessions of SW4500-1 (You can see that a connection is established between SW4500-1 and Switch3).

```
[SW4500-1] display ntp-service sessions
source          reference      stra reach poll  now offset  delay disper
*****
[1]3.0.1.31     127.127.1.0   2    1    64   377 26.1  199.53  9.7
note: 1 source(master),2 source(peer),3 selected,4 candidate,5 configured
```

Configuring NTP Server Mode with Authentication

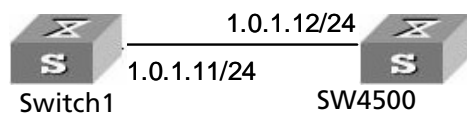
Network requirements

The local clock of Switch1 is set to the NTP master clock, with a clock stratum level of 2. The Switch 4500 considers Switch1 as the NTP server and operates in client mode, while Switch1 operates in server mode automatically. In addition, the NTP authentication function is enabled on both sides.

This example assumes that Switch1 is a switch that supports the local clock being the NTP master clock.

Network diagram

Figure 89 Network diagram for NTP server mode with authentication configuration



Configuration procedure

- 1 Configure the SW4500 Ethernet switch.

```
# Enter system view.
<SW4500> system-view
[SW4500]
# Set Switch1 to the NTP server.
[SW4500] ntp-service unicast-server 1.0.1.11
```

```

# Enable the NTP authentication function.
[SW4500] ntp-service authentication enable
# Configure an MD5 authentication key, with the key ID being 42 and
the key being aNiceKey.
[SW4500] ntp-service authentication-keyid 42 authentication-mode md5
aNiceKey
# Specify the key as a trusted key.
[SW4500] ntp-service reliable authentication-keyid 42
[SW4500] ntp-service unicast-server 1.0.1.11 authentication-keyid 42

```

After the above configurations, SW4500 is ready to synchronize with Switch1. Because the NTP authentication function is not enabled on Switch1, SW4500 will fail to be synchronized to Switch1.

To synchronize the SW4500 Ethernet switch, you need to perform the following configurations on Switch1.

```

# Enable the NTP authentication function on Switch1.
[Switch1] system-view
[Switch1] ntp-service authentication enable
# Configure an MD5 authentication key, with the key ID being 42 and
the key being aNiceKey.
[Switch1] ntp-service authentication-keyid 42 authentication-mode
md5 aNiceKey
# Specify the key as a trusted key.
[Switch1] ntp-service reliable authentication-keyid 42

```

(After the above configurations, the SW4500 Ethernet switch can be synchronized to Switch1.) View the status of SW4500 after synchronization.

```

[SW4500] display ntp-service status
Clock status: synchronized
Clock stratum: 3
Reference clock ID: 1.0.1.11
Nominal frequency: 250.0000 Hz
Actual frequency: 249.9992 Hz
Clock precision: 2^19
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 Sep 6 2001 (BF422AE4.05AEA86C)

```

The output information indicates that SW4500 is synchronized to Switch1, with a clock stratum level of 3, one stratum level lower than that Switch1.

```

# View the information about NTP sessions of SW4500 (You can see that
a connection is established between SW4500 and Switch1).
<SW4500> display ntp-service sessions
      source           reference           stra reach poll  now offset  delay disper
*****
[5]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

```


19

SSH TERMINAL SERVICES

This section contains information for SSH Terminal Services.

SSH Terminal Service

Secure Shell (SSH) can provide information security and powerful authentication to prevent such assaults as IP address spoofing, plain-text password interception when users log on to the Switch remotely using an insecure network environment.

- A Switch can connect to multiple SSH clients. SSH 2.0 and SSH1.x are currently available.
- SSH client functions to enable SSH connections between users and the Switch or UNIX host that support SSH server.

[Figure 90](#) and [Figure 91](#) show respectively SSH connection establishment for client and server.

- SSH connections through a LAN
- SSH connections through a WAN

Figure 90 Establish SSH channels through LAN

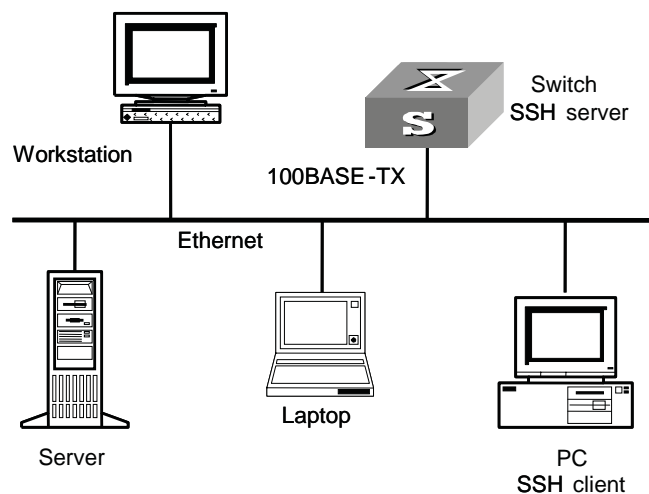
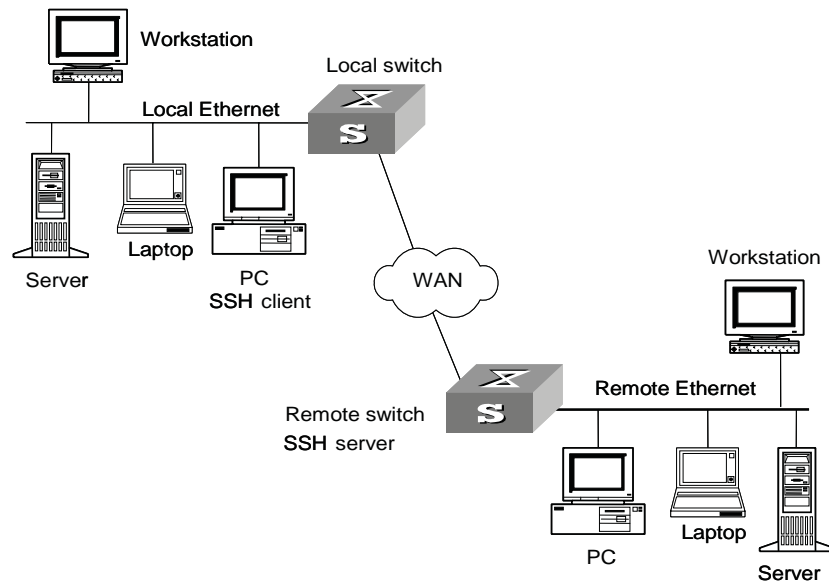


Figure 91 Establish an SSH channel through a WAN

To establish an SSH authentication secure connection, the server and the client must go through the following five phases:

- 1 Version number negotiation:
 - The client sends a TCP connection request.
 - After the TCP connection is established, the server and the client negotiate the version number.
 - If the negotiation succeeds, the key algorithm negotiation phase starts; otherwise, the server tears down the TCP connection.
- 2 Key algorithm negotiation:
 - The server generates an RSA key pair and a 8-byte number randomly, and sends the public key to the client.
 - Both the server and the client use the public key module of the server and the 8-byte number as parameters, and calculate a 16-byte session ID via the same algorithm.
 - The client uses the public key from the server and the random number generated locally as parameters to calculate the session key.
 - Using the public key from the server, the client encrypts the random number for calculating the session key and sends the result to the server.
 - Using the local private key, the server decrypts the data sent by the client and obtains the random number used by the client.
 - Using the local public key and the random number sent by the client as parameters, the server calculates the session key via the same algorithm as the one employed by the client.

On completion of the above steps, the server and the client obtains the same session key. During the session, both ends use the same session key to perform encryption and decryption, thereby guaranteeing the security of data transfer.

3 Authentication mode negotiation:

- The client sends its username information to the server.
- The server initiates a procedure to authenticate the user. If the server is configured not to authenticate the user, the process proceeds to session request phase directly.
- The client employs an authentication mode to authenticate the server till the authentication succeeds or the server tears down the connection because of timeout.

SSH provides two authentication modes: password authentication and RSA authentication.

- Password authentication procedure:

- The client sends the username and password to the server;
- The server compares the username and password sent from the client with the local configuration. If it finds an exact match, the authentication succeeds.

- RSA authentication procedure:

- The server configures an RSA public key for the client;
- The client sends its RSA public key member module to the server;
- The server performs validity authentication on the member module. If the authentication succeeds, the server generates a random number, encrypts it using the RSA public key from the client, and sends the encrypted information back to the client;
- Both the server and the client uses the random number and the session ID as parameters to calculate the authentication data;
- The client sends the authentication data it generates to the server;
- The server compares the authentication data from the client with that locally calculated. If they match, the authentication succeeds.

4 Session request: If the authentication succeeds, the client sends a session request to the server. When the server has successfully processed the request, SSH enters the interactive session phase.

5 Interactive session: The client and the server exchange data till the session is over.

SSH Server Configuration

SSH server configuration tasks are described in the following sections:

Table 343 SSH server configuration

No	Configuration Item	Command	View	Description
1	Configure the protocol the current user interface supports	protocol inbound	VTY user interface view	Optional
2	Generate an RSA key pair	rsa local-key-pair create	System view	Required
	Destroy an RSA key pair	sa local-key-pair destroy	System view	Optional
3	Configure the SSH user authentication mode	ssh user username authentication-type	System view	Required
4	Set the SSH authentication timeout	ssh server timeout	System view	Optional
5	Set the number of SSH authentication retries	ssh server authentication-retries	System view	Optional
6	Set the update interval of server key	ssh server rekey-interval hours	System view	Optional
7	Enter the public key view	rsa peer-public-key	System view	Optional
8	Enter the public key edit view and edit the public key	public-key-code begin	Public key view	Optional
9	Exit the public key edit view	public-key-code end	Public key view	Optional
10	Specify the public key for an SSH user	ssh user username assign rsa-key keyname	System view	Required
11	Set the SSH compatibility mode	ssh server compatible_ssh1 x enable	System view	Optional

1 Configuring the supported protocol

Use this configuration task to specify the protocol the current user interface supports.

Perform the following configuration in VTY user interface view.

Table 344 Configure the protocol the current user interface supports

Operation	Command
Configure the supported protocol	protocol inbound { all ssh telnet }

By default, the system supports all protocols.



CAUTION: If the supported protocol configured in the user interface is SSH, make sure to configure the authentication mode for logging into the user interface to **authentication-mode scheme** (using AAA authentication mode).

If the authentication mode is configured as **authentication-mode password** or **authentication-mode none**, the configuration of **protocol inbound ssh** will fail, and vice versa.

2 Generating an RSA key pair

Use this configuration task to generate or destroy an RSA key pair (including the host key and server key) of the server. The naming conventions for the keys are switchname + _host and switchname + _server respectively.

After this command is entered, the system prompts you to input the number of the key pair bits. Pay attention to the following:

- The host key and the server key must have a difference of at least 128 bits in length.
- The minimum and maximum lengths for the host key and the server key are 512 bits and 2048 bits respectively.

Perform the following configuration in system view.

Table 345 Generate an RSA key pair

Operation	Command
Generate an RSA key pair	rsa local-key-pair create
Destroy an RSA key pair	rsa local-key-pair destroy



CAUTION:

- *Generating the RSA key pair of the server is the first step to perform after SSH login.*
- *This command needs to be performed only once; you need not re-perform it after rebooting the switch.*
- *If a key pair exists before the configuration, a prompt will appear asking if you want to replace it.*

3 Configuring the user authentication mode

Use this configuration task to specify the authentication mode for an SSH user. You must specify an authentication mode for a new user; otherwise, the new user will not be able to log in.

Perform the following configuration in system view.

Table 346 Configure the authentication mode for an SSH user

Operation	Command
Configure the authentication mode for an SSH user	ssh user username authentication-type { password rsa password-publickey all }
Restore the default unable-to-login mode	undo ssh user username authentication-type

By default, no login authentication mode is specified, that is, SSH users are unable to log in.

4 Configuring the authentication timeout

Use this configuration task to set the authentication timeout of SSH connections.

Perform the following configuration in system view.

Table 347 Set the SSH authentication timeout

Operation	Command
Set the SSH authentication timeout	ssh server timeout <i>seconds</i>
Restore the default SSH authentication timeout	undo ssh server timeout

By default, the authentication timeout is 60 seconds.

5 Set the update interval of server key

Please perform the following configurations in system view.

Table 348 Set the update interval of server key

Operation	Command
Set the update interval of server key	ssh server rekey-interval <i>hours</i>
Restore the default update interval	undo ssh server rekey-interval

By default, the system does not update server key.

The command is only available for the client version SSH1.5.

6 Configuring the number of authentication retries

Use this configuration task to set the number of authentication retries an SSH user can request for a connection, thereby preventing illegal behaviors such as malicious guessing.

Perform the following configuration in system view.

Table 349 Configure the number of SSH authentication retries

Operation	Command
Configure the number of SSH authentication retries	ssh server authentication-retries <i>times</i>
Restore the default number of SSH authentication retries	undo ssh server authentication-retries

By default, the number of authentication retries is 3.

7 Entering the public key view

Use this configuration command to enter the public key view and specify the name of the public key.

Perform the first configuration in the following table in system view.

Table 350 Public key configuration

Operation	Command
Enter the public key view	rsa peer-public-key <i>key-name</i>
Exit the public view and return to the system view	peer-public-key end

The configuration commands are applicable to the environments where the server employs RSA authentication on SSH users. If the server adopts password authentication on SSH users, these configurations are not necessary.

8 Entering the public key edit view

After entering the public key view by the `rsa peer-public-key` command, you can use the `public-key-code begin` command to enter the public key edit view and input the public key of the client.

When inputting the public key, you may type spaces between the characters (the system will delete the spaces automatically), or press <Enter> and then continue to input the key. Note that the public key must be a hexadecimal string coded in the public key format.

Perform the following configuration in public key view.

Table 351 Enter the public key edit view

Operation	Command
Enter the public key edit view	public-key-code begin

9 Exiting the public key edit view

Use this configuration task to return from the public key edit view to the public key view and save the input public key. Before saving the input public key, the system will check the validity of the key:

- If the public key string contains any illegal character, the configured key is invalid;
- If the configured key is valid, it will be saved to the public key list.

Perform the following configuration in public key edit view.

Table 352 Exit the public key edit view

Operation	Command
Exit the public key edit view	public-key-code end

10 Specifying the public key for an SSH user

Use this configuration task to specify an existing public key for an SSH user.

Perform the following configuration in system view.

Table 353 Specify the public key for an SSH user

Operation	Command
Specify the public key for an SSH user	ssh user <i>username</i> assign rsa-key <i>keyname</i>

Operation	Command
Cancel the corresponding relationship between the user and the public key	<code>undo ssh user <i>username</i> assign rsa-key</code>

11 Configuring the server compatibility mode

Use this configuration task to set whether the server should be compatible with the SSH 1.x client.

Perform the following configuration in system view.

Table 354 Configure the compatibility mode

Operation	Command
Set the server to be compatible with the SSH 1.x client	<code>ssh server compatible_ssh1x enable</code>
Set the server to be incompatible with the SSH 1.x client	<code>undo ssh server compatible_ssh1x</code>

By default, the server is compatible with the SSH 1.x client.

SSH Client Configuration

A variety of SSH client software are available, such as PuTTY. For an SSH client to establish a connection with an SSH server, you must complete these configuration tasks:

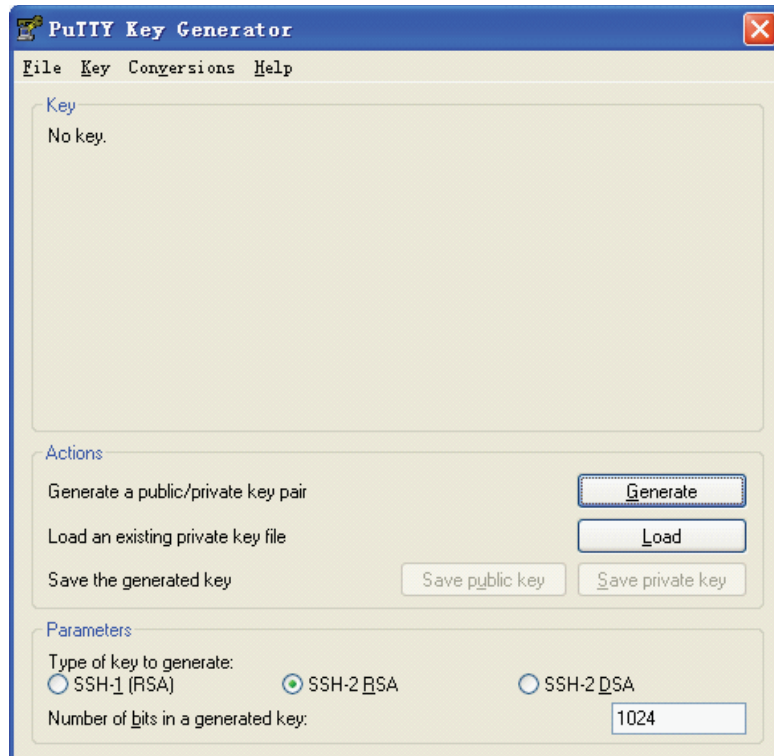
- Specifying the IP address of the server.
- Selecting the protocol for remote connection. Usually, a client can use a variety of remote connection protocols, such as Telnet, Rlogin, SSH. To establish an SSH connection, you must select SSH.
- Selecting the SSH version. Since the device supports SSH Server 2.0 now, select 2.0 for the client.
- Specifying the RSA private key file. On the server, if RSA authentication is enabled for an SSH user and a public key is set for the user, the private key file corresponding to the public key must be specified on the client. RSA key pairs are generated by a tool of the client software.

The following takes the client software of PuTTY, PuTTYGen and SSHKEY as examples to illustrate how to configure the SSH client:

Currently, the S3200 Series Ethernet Switches support using PuTTY (Version 0.58) as an SSH client

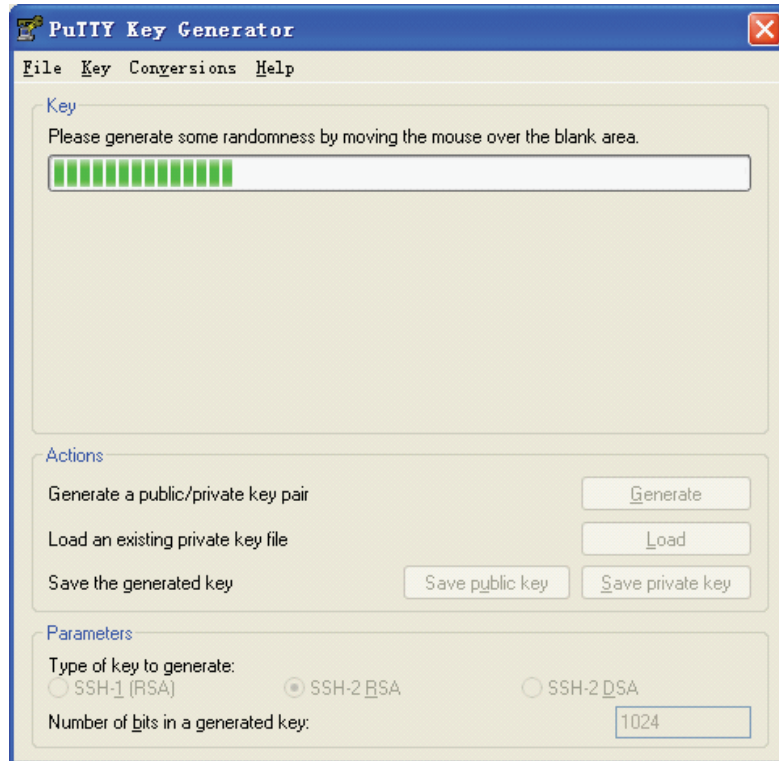
Generating the Client Key

To generate the client key pair, run PuTTYGen.exe, choose "SSH2(RSA)" in the parameter field and click "Generate".

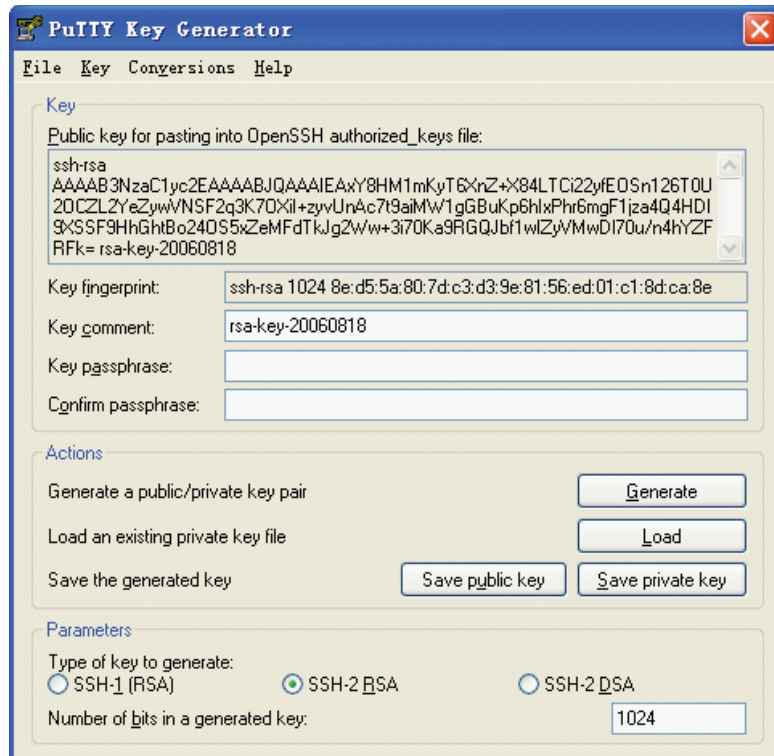
Figure 92 Generating the client key (1)

While generating the key pair, you must move the mouse continuously. The mouse should be restricted off the green process bar in the blue box of [Figure 93](#). Otherwise, the process bar does not move and the key pair cannot be generated.

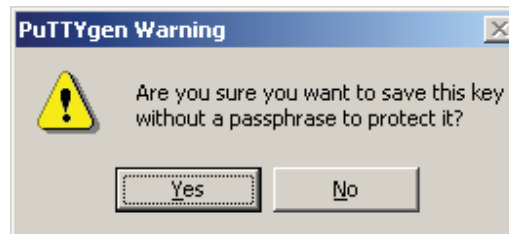
Figure 93 Generating the client key (2)



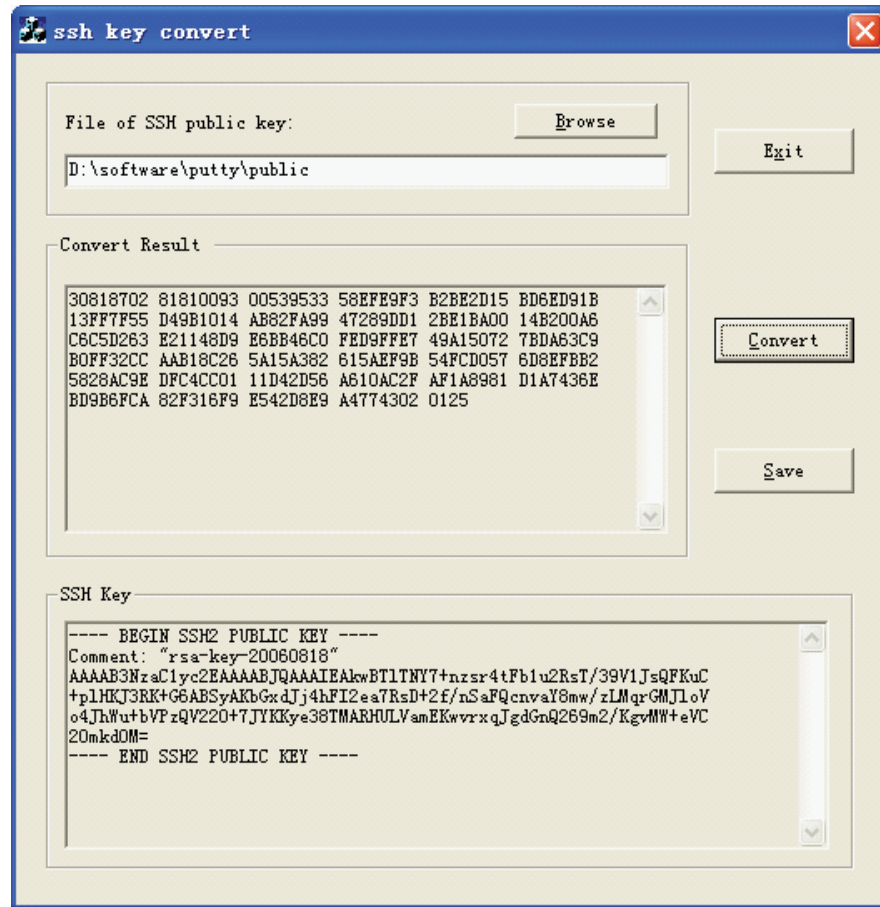
After the key pair is generated, click "Save public key" and enter the file name (public for here) to save the key pair.

Figure 94 Generating the client key (3)

Likewise, to save a private key, click "Save private key" and a warning window pops up to prompt you whether to save a private key without any precautions. Click "Yes" and enter a name (private for here) to save the private key.

Figure 95 Generating the client key (4)

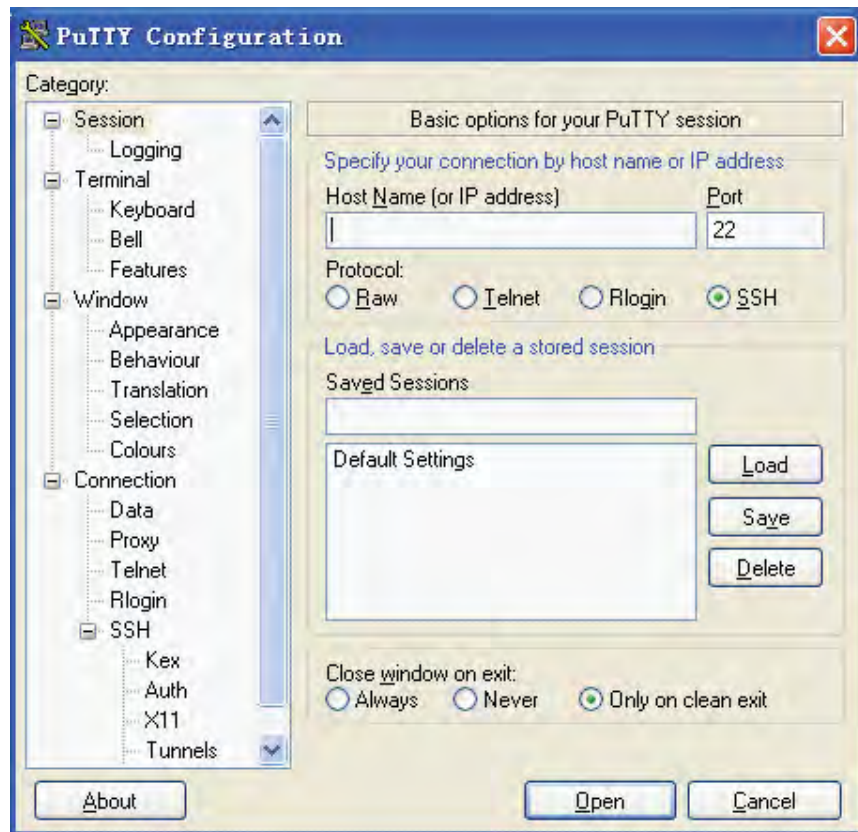
To generate RSA public key in PKCS format, run SSHKEY.exe, click "Browse" and select the public key file, and then click "Convert".

Figure 96 Generating the client key (5)

Specifying the IP address of the server

Launch PuTTY.exe and the following window appears.

Figure 97 FiSSH client interface 1



In the [Host Name (or IP address)] text box, enter the IP address of the server, for example, 10.110.28.10. Note that the IP address can be the IP address of any interface on the server that has SSH in the state of up and a route to the client.

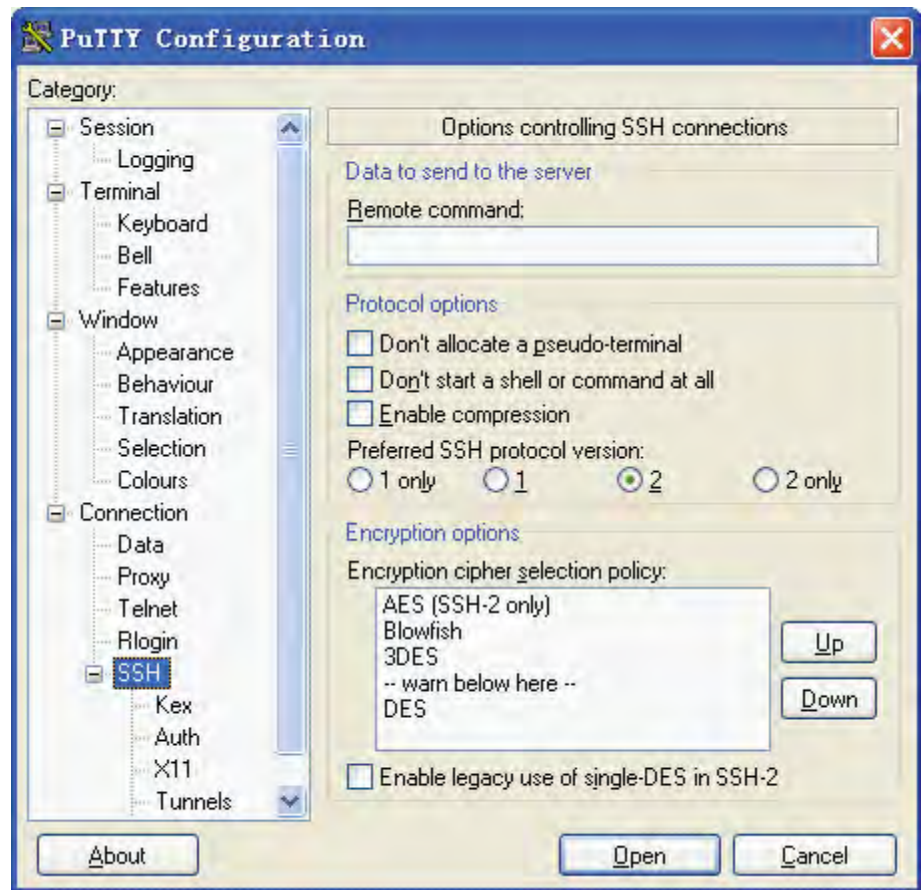
Selecting the protocol for remote connection

As shown in [Figure 97](#), select the [SSH] option from the [Protocol] section.

Selecting the SSH version

From the category on the left of the window, click [Connection/SSH]. The window as shown in [Figure 98](#) appears.

Figure 98 SSH client interface 2

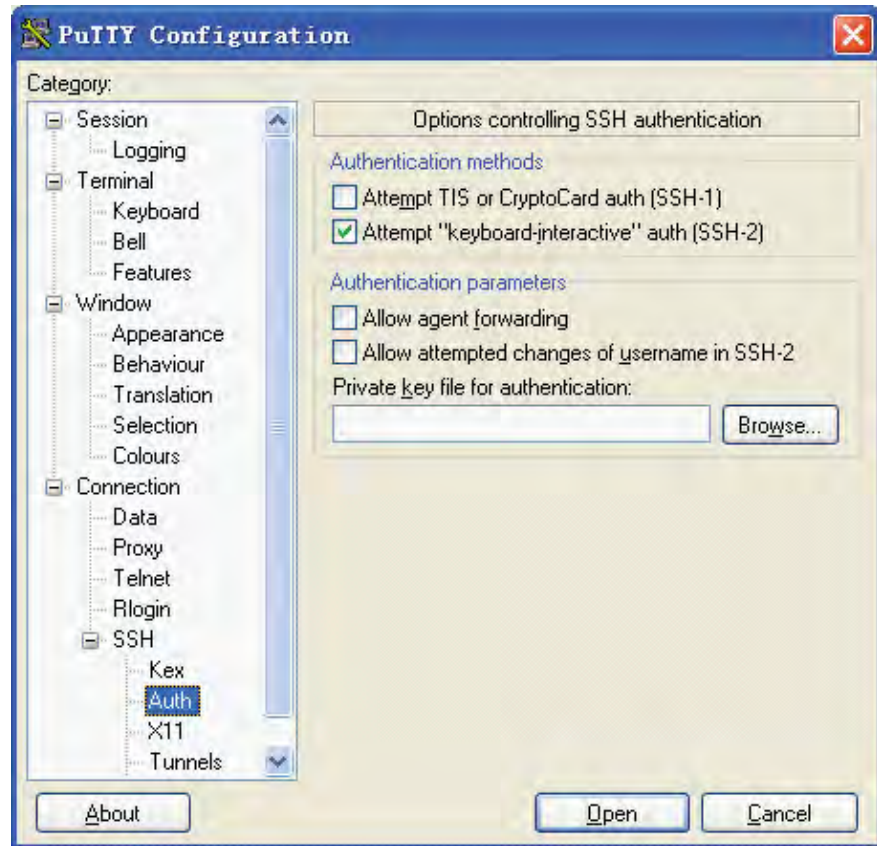


In the [Protocol options] field, select [2] from the [Preferred SSH protocol version] section.

Open an SSH Connection with RSA

If the client needs to use RSA authentication, you must specify the RSA private key file. If the client needs to use password authentication, this is not required.

From the category on the left of the window, click [Connection/SSH/Auth]. The following window appears.

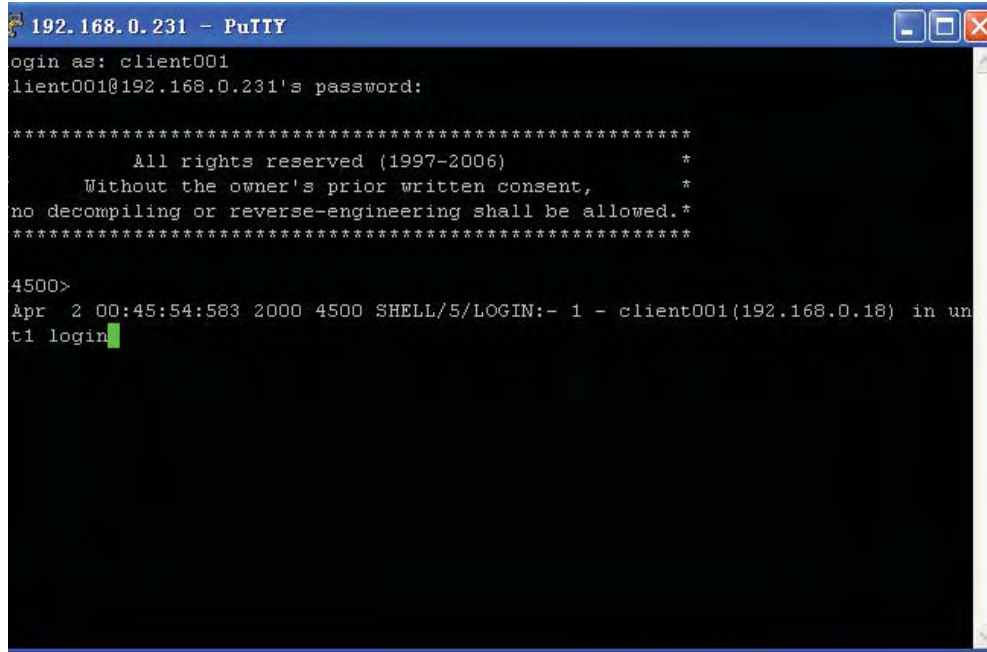
Figure 99 Figure 8-10 SSH client interface 3

Click <Browse...> to bring up the file selection window, navigate to the private key file and click <OK>.

Open an SSH Connection with Password

- 1 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 100](#).

Figure 100 SSH client interface



- 2 Enter the username and password to create an SSH connection.
- 3 To log out, enter the quit command.

Configuring the Device as an SSH Client

[Table 355](#) describes the tasks required to configure an SSH client.

Table 355 SSH client configuration

No	Configuration Item	Command	View	Description
1	Set to perform the first-time authentication on the SSH server to be accessed	ssh client first-time enable	System view	Optional
2	Specify the public key of the server	ssh client <i>server-ip assign</i> rsa-key <i>keyname</i>	System view	Required
3	Start the SSH client	ssh2	System view	Required

- 1 Starting the SSH client

Use this configuration task to enable the connection with the SSH client and the server, and specify the preferred key exchange algorithm, encryption algorithm and HMAC algorithm of the client and the server. Perform the following configuration in system view.

Table 356 Start the SSH client

Operation	Command
Start the SSH client	<code>ssh2 { host-ip host-name } [port-num] [prefer_kex { dh_group1 dh_exchange_group }] [prefer_ctos_cipher { des 3des aes128 }] [prefer_stoc_cipher { des 3des aes128 }] [prefer_ctos_hmac { sha1 sha1_96 md5 md5_96 }] [prefer_stoc_hmac { sha1 sha1_96 md5 md5_96 }]</code>

2 Specifying the public key of the server

Use this configuration task to specify the public key of the server to be connected to the client, so that the client authenticates if the connected server is trustworthy. Perform the following configuration in system view.

Table 357 Specify the public key of the server

Operation	Command
Specify the public key of the server	<code>ssh client server-ip assign rsa-key keyname</code>
Cancel the corresponding relationship between the server and the public key	<code>undo ssh client server-ip assign rsa-key</code>

3 Configuring the first-time authentication of the server

Use this configuration task to configure or cancel the first-time authentication of the server performed by the SSH client.

The first-time authentication means that when the SSH client accesses the server for the first time in the case that there is no local copy of the server's public key, the user can choose to proceed to access the server and save a local copy of the server's public key; when the client accesses the server next time, it uses the saved public key to authenticate the server.

If the first-time authentication is not supported, when there is no local copy of the public key of the connected server, the client assumes that the server is illegal and will refuse to access the server.

Perform the following configuration in system view.

Table 358 Configure the first-time authentication of the server

Operation	Command
Configure the first-time authentication of the server	<code>ssh client first-time enable</code>
Cancel the first-time authentication of the server	<code>undo ssh client first-time</code>

By default, the client perform the first-time authentication.

Displaying and Debugging SSH

On completion of the above configurations, you can use the display command in any view to view the operation of the configured SSH and further verify the result

of the configurations. You can also debug SSH by performing the debugging command in user view.

Table 359 Display information relevant to SSH

Operation	Command
Display the public key of the host key pair and the server key pair of the server	<code>display rsa local-key-pair public</code>
Display the public key of the specified RSA key pair of the client	<code>display rsa peer-public-key [brief name keyname]</code>
Display the SSH status information and session information	<code>display ssh server { status session }</code>
Display information about the SSH user	<code>display ssh user-information [username]</code>
Enable SSH debugging	<code>debugging ssh server { vty vty-num all }</code>
Disable SSH debugging	<code>undo debugging ssh server { vty vty-num all }</code>

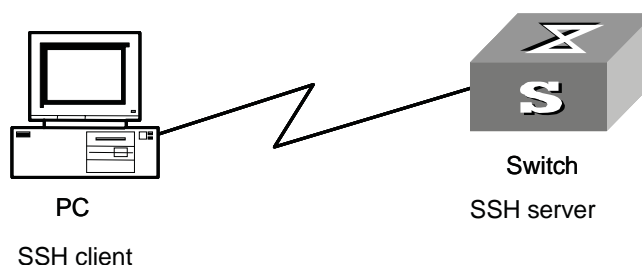
SSH Server Configuration Example

Network requirements

As shown in [Figure 101](#), a PC (SSH client) running SSH 2.0-enabled client software establishes a local connection with the switch (SSH server) to better guarantee the security of exchanged information.

Network diagram

Figure 101 Network diagram for SSH server



Configuration procedure

- 1 Generate the RSA key.
[3Com] `rsa local-key-pair create`



Note: If the configuration for generating the local key has already been completed, skip this step.

- 2 Set the user login authentication mode.

The following shows the configuration methods for both password authentication and RSA public key authentication.

Password authentication.

```
# Set the authentication mode of the user interface to AAA.
```

```
[3Com] user-interface vty 0 4
[3Com-ui-vty0-4] authentication-mode scheme
# Specify the login protocol for user client001 as SSH, the
authentication mode as password.
[3Com-ui-vty0-4] protocol inbound ssh
[3Com] local-user client001
[3Com-luser-client001] password simple 3com
[3Com] ssh user client001 authentication-type password
```



Note: You can use the default values for SSH authentication timeout and retries. After completing the above configurations, you can run the SSH 2.0-enabled client software on any other terminal connected with the switch and access the switch with the username client001 and password huawei.

RSA public key authentication.

```
# Set the authentication mode of the user interface to AAA.
[3Com] user-interface vty 0 4
[3Com-ui-vty0-4] authentication-mode scheme
# Specify the login protocol for user client002 as SSH, the
authentication mode as RSA.
[3Com-ui-vty0-4] protocol inbound ssh
[3Com] ssh user client002 authentication-type rsa
```

- 3 Using the SSH 2.0-enabled client software, randomly generate an RSA key pair and send the public key to the server.
- 4 Configure the public key of the client, and specify the name of the public key as 3com002.

```
[3Com] rsa peer-public-key 3Com002
[3Com-rsa-public-key] public-key-code begin
[3Com-rsa-key-code] 308186028180739A291ABDA704F5D93DC8FDF84C427463
[3Com-rsa-key-code] 1991C164B0DF178C55FA833591C7D47D5381D09CE82913
[3Com-rsa-key-code] D7EDF9C08511D83CA4ED2B30B809808EB0D1F52D045DE4
[3Com-rsa-key-code] 0861B74A0E135523CCD74CAC61F8E58C452B2F3F2DA0DC
[3Com-rsa-key-code] C48E3306367FE187BDD944018B3B69F3CBB0A573202C16
[3Com-rsa-key-code] BB2FC1ACF3EC8F828D55A36F1CDDC4BB45504F020125
[3Com-rsa-key-code] public-key-code end
[3Com-rsa-public-key] peer-public-key end
[3Com] ssh user client002 assign rsa-key 3com002
```

- 5 Start the SSH client software on the terminal preserving the RSA private key, and perform the corresponding configurations to establish the SSH connection.

SSH Client Configuration Example

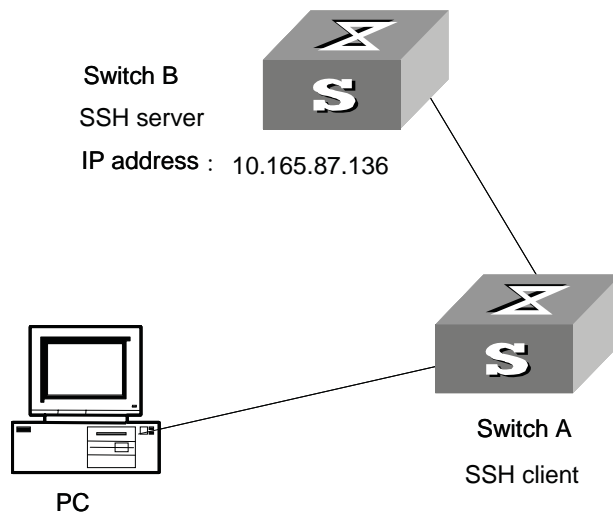
Network requirements

As shown in [Figure 102](#):

- Switch A is used as an SSH client, and the username is client003.
- Switch B is used as the SSH server, and the IP address is 10.165.87.136.

Network diagram

Figure 102 Network diagram for SSH client



Configuration procedure

- 1 Configure the client to perform the first-time authentication of the server.

```
[3Com] ssh client first-time enable
```

- 2 Specify the public key of the server on the client.

```
[3Com] rsa peer-public-key hello
[3Com-rsa-public-key] public-key-code begin
[3Com-rsa-key-code] 308186028180739A291ABDA704F5D93DC8FDF84C427463
[3Com-rsa-key-code] 1991C164B0DF178C55FA833591C7D47D5381D09CE82913
[3Com-rsa-key-code] D7EDF9C08511D83CA4ED2B30B809808EB0D1F52D045DE4
[3Com-rsa-key-code] 0861B74A0E13523CCD74CAC61F8E58C452B2F3F2DA0DC
[3Com-rsa-key-code] C48E3306367FE187BDD944018B3B69F3CBB0A573202C16
[3Com-rsa-key-code] BB2FC1ACF3EC8F828D55A36F1CDDC4BB45504F020125
[3Com-rsa-key-code] public-key-code end
[3Com-rsa-public-key] peer-public-key end
[3Com] ssh client 10.165.87.136 assign rsa-key hello
```



CAUTION: Before logging into the SSH server, the SSH client (except for the software Putty and Openssh) must configure the public key of the server.

- 3 Start the SSH client.

The following shows the configuration methods for both password authentication and RSA public key authentication.

Employ password authentication mode, and start using the default encryption algorithm

```
[3Com] ssh2 10.165.87.136
Please input the username: client003
Trying 10.165.87.136
Press CTRL+K to abort
Connected to 10.165.87.136...
The Server is not autherncated.Do you continue access it?(Y/N):y
Do you want to save the server's public key?(Y/N):y
```



```

Enter password:
*****
*           All rights reserved (1997-2004)           *
*   Without the owner's prior written consent,       *
*no decompiling or reverse-engineering shall be allowed.*
*****

<3Com>

Employ RSA public key authentication mode, and start using the
corresponding encryption algorithm configured.

[3Com] ssh2 10.165.87.136 22 perfer_kex dh_group1 perfer_ctos_cipher
des perfer_stoc_cipher 3des perfer_ctos_hmac md5 perfer_stoc_hmac
md5
Please input the username: client003
Trying 10.165.87.136...
Press CTRL+K to abort
Connected to 10.165.87.136...
The Server is not autherncated.Do you continue access it?(Y/N):y
Do you want to save the server's public key?(Y/N):y
*****
*           All rights reserved (1997-2004)           *
*   Without the owner's prior written consent,       *
*no decompiling or reverse-engineering shall be allowed.*
*****

<3Com>

```

SFTP Service

SFTP Overview Secure FTP (SFTP) is a new feature introduced in SSH 2.0.

SFTP is established on SSH connections, which makes remote users able to securely log in to the switch and perform file management and transfer operations such as system upgrade, and thereby providing higher security for data transfer. At the same time, since the switch can be used as a client, users can log in to remote devices to transfer files securely.

SFTP Server Configuration SFTP server configuration tasks are described in this section:

SFTP server configuration

No	Configuration Item	Command	View	Description
1	Configure the service type to be used	ssh user service-type	System view	Optional
2	Start the SFTP server	sftp server enable	System view	Required

1 Configuring the service type to be used

Use this configuration task to set the SSH service type to be used. Perform the following configuration in system view.

Table 360 Configure the service type to be used

Operation	Command
Configure the service type to be used	ssh user <i>username</i> service-type { stelnet sftp all }
Restore the default service type	undo ssh user <i>username</i> service-type

By default, the service type is stelnet.

2 Starting the SFTP server

Perform the following configuration in system view.

Table 361 Start the SFTP server

Operation	Command
Start the SFTP server	sftp server enable
Shut down the SFTP server	undo sftp server

By default, the SFTP server is shut down.

SFTP Client Configuration

SFTP client configuration tasks are described in this section:

Table 362 SFTP client configuration

No	Configuration Item	Command	View	Description
1	Start the SFTP client	sftp	System view	Required
2	Shut down the SFTP client	bye exit quit	SFTP client view	Optional
3	SFTP directory operations	Change the current directory cd Return to the upper directory cdup Display the current directory pwd Display the list of files in the specified directory dir ls Create a new directory mkdir Delete a directory rmdir	SFTP client view	Optional
4	SFTP file operations	Change the name of the specified file on the server rename Download a file from the remote server get Upload a local file to the remote server put Display the list of files in the specified directory dir ls Delete a file from the server delete remove	SFTP client view	Optional
5	help information for client commands	help	SFTP client view	Optional

1 Starting the SFTP client

Use this configuration task to start the SFTP client program, establish a connection with the remote SFTP server, and enter the SFTP client view. Perform the following configuration in system view.

Table 363 Start the SFTP client

Operation	Command
Start the SFTP client	<code>sftp { host-ip host-name } [port-num] [prefer_kex { dh_group1 dh_exchange_group }] [prefer_ctos_cipher { des 3des aes128 }] [prefer_stoc_cipher { des 3des aes128 }] [prefer_ctos_hmac { sha1 sha1_96 md5 md5_96 }] [prefer_stoc_hmac { sha1 sha1_96 md5 md5_96 }]</code>

2 Shutting down the SFTP client

Use this configuration task to shut down the SFTP client program. Perform the following configuration in SFTP client view.

Table 364 Shut down the SFTP client

Operation	Command
Shut down the SFTP client	<code>bye</code> <code>exit</code> <code>quit</code>

The three commands, `bye`, `exit`, and `quit`, have the same functionality.

3 SFTP directory operations

As shown in [Table 365](#), available SFTP directory operations include: change or display the current directory, create or delete a directory, display the specified file or directory.

Perform the following configuration in SFTP client view.

Table 365 SFTP directory operations

Operation	Command
Change the current directory	<code>cd remote-path</code>
Return to the upper directory	<code>cdup</code>
Display the current directory	<code>pwd</code>
Display the list of files in the specified directory	<code>dir [remote-path]</code> <code>ls [remote-path]</code>
Create a new directory on the server	<code>mkdir remote-path</code>
Delete a directory from the server	<code>rmdir remote-path</code>

The `dir` command and the `ls` command have the same functionality.

4 SFTP file operations

As shown in [Table 366](#), available SFTP file operations include: change the name of a file, download a file, upload a file, display the list of files, and delete a file. Perform the following configuration in SFTP user view.

Table 366 SFTP file operations

Operation	Command
Change the name of the specified file on the server	rename old-name new-name
Download a file from the remote server	get remote-file [local-file]
Upload a local file to the remote server	put local-file [remote-file]
Display the list of files in the specified directory	dir [remote-path] ls [remote-path]
Delete a file from the server	delete remote-file remove remote-file

The **dir** command and the **ls** command have the same functionality. The **delete** command and the **remove** command have the same functionality.

5 Displaying help information

Use this command to display command-relevant help information such as the format of the command, parameter configurations, and so on. Perform the following configuration in SFTP client view.

Table 367 Display help information for client commands

Operation	Command
Display help information for client commands	help [command-name]

SFTP Configuration Example

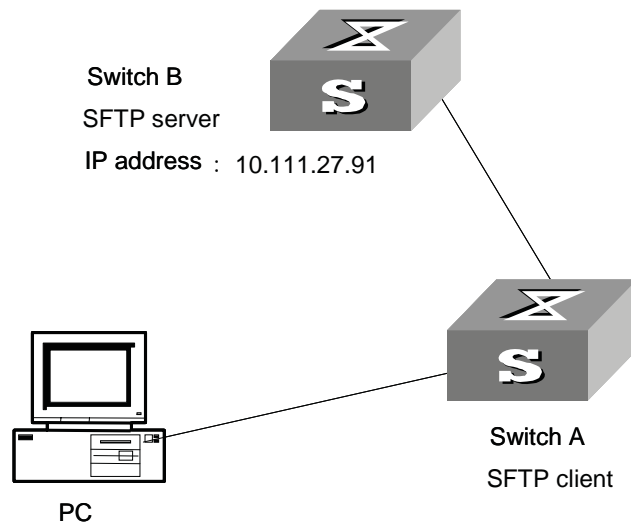
Network requirements

As shown in [Figure 103](#):

- A secure SSH connection has been established between Switch A and Switch B;
- Switch A is used as the SFTP server, and its IP address is 10.111.27.91;
- Switch B is used as the SFTP client;
- An SFTP user is configured with the username 8040 and password 3com.

Network diagram

Figure 103 Network diagram for SFTP



Configuration procedure

1 Configure Switch B as the server.

```
# Start the SFTP server.
[3Com] sftp-server enable
# Specify the service type as SFTP.
[3Com] ssh user 8040 service-type sftp
```

2 Configure Switch A as the client.

```
# Establish a connection with the remote SFTP server and enter the
SFTP client view.
[3Com] sftp 10.111.27.91
# Display the current directory of the server, delete file z, and
check if the directory has been deleted successfully.
sftp-client> dir
-rwxrwxrwx  1 noone  nogroup  1759 Aug 23 06:52 vrpcfg.cfg
-rwxrwxrwx  1 noone  nogroup   225 Aug 24 08:01 pubkey2
-rwxrwxrwx  1 noone  nogroup   283 Aug 24 07:39 pubkey1
drwxrwxrwx  1 noone  nogroup    0 Sep 01 06:22 new
-rwxrwxrwx  1 noone  nogroup   225 Sep 01 06:55 pub
-rwxrwxrwx  1 noone  nogroup    0 Sep 01 08:00 z
sftp-client> delete z
Remove this File?(Y/N)
flash:/zy
File successfully Removed
sftp-client> dir
-rwxrwxrwx  1 noone  nogroup  1759 Aug 23 06:52 vrpcfg.cfg
-rwxrwxrwx  1 noone  nogroup   225 Aug 24 08:01 pubkey2
-rwxrwxrwx  1 noone  nogroup   283 Aug 24 07:39 pubkey1
drwxrwxrwx  1 noone  nogroup    0 Sep 01 06:22 new
-rwxrwxrwx  1 noone  nogroup   225 Sep 01 06:55 pub
# Create a new directory new1, and check if the new directory has
been created successfully.
sftp-client> mkdir new1
New path created
```

```

sftp-client> dir
-rwxrwxrwx 1 noone nogroup 1759 Aug 23 06:52 vrpcfg.cfg
-rwxrwxrwx 1 noone nogroup 225 Aug 24 08:01 pubkey2
-rwxrwxrwx 1 noone nogroup 283 Aug 24 07:39 pubkey1
drwxrwxrwx 1 noone nogroup 0 Sep 01 06:22 new
-rwxrwxrwx 1 noone nogroup 225 Sep 01 06:55 pub
drwxrwxrwx 1 noone nogroup 0 Sep 02 06:30 new1
# Change the directory name new1 to new2, and check if the directory
name has been changed successfully.
sftp-client> rename new1 new2
sftp-client> dir
-rwxrwxrwx 1 noone nogroup 1759 Aug 23 06:52 vrpcfg.cfg
-rwxrwxrwx 1 noone nogroup 225 Aug 24 08:01 pubkey2
-rwxrwxrwx 1 noone nogroup 283 Aug 24 07:39 pubkey1
drwxrwxrwx 1 noone nogroup 0 Sep 01 06:22 new
-rwxrwxrwx 1 noone nogroup 225 Sep 01 06:55 pub
drwxrwxrwx 1 noone nogroup 0 Sep 02 06:33 new2
# Download file pubkey2 from the server to a local device, and change
the file name to public.
sftp-client> get pubkey2 public
Downloading file successfully ended
# Upload local file pu to the server, change the file name to puk,
and check if the operations are successful.
sftp-client> put pu puk
Uploading file successfully ended
sftp-client> dir
-rwxrwxrwx 1 noone nogroup 1759 Aug 23 06:52 vrpcfg.cfg
-rwxrwxrwx 1 noone nogroup 225 Aug 24 08:01 pubkey2
-rwxrwxrwx 1 noone nogroup 283 Aug 24 07:39 pubkey1
drwxrwxrwx 1 noone nogroup 0 Sep 01 06:22 new
drwxrwxrwx 1 noone nogroup 0 Sep 02 06:33 new2
-rwxrwxrwx 1 noone nogroup 283 Sep 02 06:35 pub
-rwxrwxrwx 1 noone nogroup 283 Sep 02 06:36 puk
sftp-client>
# Exit SFTP.
sftp-client> quit
Bye
<3Com>

```


20

PASSWORD CONTROL CONFIGURATION OPERATIONS

Introduction to Password Control Configuration

The password control feature is designed to manage the following passwords:

- Telnet passwords: passwords used by the users who log in the switch through Telnet.
- SSH passwords: passwords used by the users who log in the switch through SSH.
- FTP passwords: passwords used by the users who log in the switch through FTP.
- Super passwords: passwords used by the users who have logged in the switch and are changing from a lower privilege level to a higher privilege level.

[Table 368](#) lists the functions provided by password control.

Table 368 Functions Provided by Password Control

Function	Description	Application
Password aging	<p>The password aging function has the following sub-functions:</p> <ul style="list-style-type: none">■ Password aging time setting: users can set the aging time for their passwords. If a password ages out, its user must update it, otherwise the user cannot log in the switch.■ Password update: after a password ages out, the user can update it when logging in the switch.■ Alert before password expiration: users can set their respective alert times. When a user logs in the system and 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 alerts the user to the forthcoming expiration and prompt the user to update the password as soon as possible.	<p>Telnet and SSH passwords: all password aging sub-functions are applicable.</p> <p>Super passwords: only the password aging time setting and the password update sub-functions are applicable.</p> <p>FTP passwords: only the password aging time setting sub-function is applicable.</p>
Limitation of minimum password length	<p>This function is used to limit the minimum length of the passwords. A user can successfully configure a password only when the length of the password is not shorter than its minimum length.</p>	<p>Telnet, SSH, super, and FTP passwords.</p>

Table 368 Functions Provided by Password Control

Function	Description	Application
History password recording	<p>The password configured and once used by a user is called a history (old) password. The switch is able to record the user history passwords. User cannot successfully update their passwords if they use a history password.</p> <p>The history passwords are saved in a readable file in the flash memory so they will not be lost when the switch reboots.</p> <p>The system hot-backs up the history passwords such that they keep synchronized between the primary and secondary SRP cards (that is, the main control cards) of the switch.</p>	Telnet, SSH, super, and FTP passwords.
Password protection and encryption	<p>The switch takes protection measure on the password displaying. No matter where a password is displayed (in the configuration file or on the command line), it is always displayed as a string containing only the asterisk (*) characters.</p> <p>The switch encrypts the configured passwords and save the passwords in ciphertext mode in the configuration file.</p>	Telnet, SSH, super, and FTP passwords.
Login attempts limitation and failure procession	<p>You can use this function to enable the switch to limit the times of login attempts allowed for each user.</p> <p>If the login attempt times of a user exceeds the configured maximum times, the user fails the login. In this case, the switch operates in one of the following procession mode:</p> <ol style="list-style-type: none"> 1 Inhibit the user from re-login within a certain time period. After that period of time, the user is allowed to log in the switch again. 2 Inhibit the user from re-login forever. The user is allowed to log in the switch again only after the administrator manually removes the user from the user blacklist. 3 Allows the user to log in again. <p>By default, the switch adopts the first mode. In actual, you can configure the procession mode.</p>	<p>Telnet, SSH, and FTP passwords: the limitation and all the three modes of procession are applicable.</p> <p>Super passwords: the limitation and the first mode of procession are applicable.</p>

Table 368 Functions Provided by Password Control

Function	Description	Application
User blacklist	<p>If the maximum attempt times is exceeded, the user cannot log in the switch and is added to the blacklist by the switch. All users in the blacklist are not allowed to log in the switch.</p> <p>For the user inhibited from login for a certain time period, the switch will remove the user from the blacklist when the time period is used out.</p> <p>For the user inhibited from login forever, the switch provides a command which allows the administrator to manually remove the user from the blacklist.</p> <p>The blacklist is saved in the RAM of the switch, so it will be lost when the switch reboots.</p>	
System logging	<p>The switch automatically logs the following events:</p> <ul style="list-style-type: none"> ■ Successful user login: The switch logs the user name, user IP address, and VTY ID. ■ Inhibition of a user due to ACL rule: The switch logs the user IP address. ■ User authentication failure. The switch logs 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 4500 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 Minimum Password Length](#)
- [Configuring History Password Recording](#)
- [Configuring User Login Password in Encryption Mode](#)
- [Configuring Login Attempts Limitation and Failure Procession Mode](#)
- [Configuring the Timeout for User Password Authentication](#)

After the above configuration, you can execute the `display password-control` command in any view to check the information about the global password control for all users, including the enable/disable state of password aging, the aging time, the enable/disable state of the shortest-password limitation, the configured

minimum password length (if available), the enable/disable state of history password recording, the procession mode for login attempt failures, and the time when the password history was last cleared.

If all the password attempts of a user fail, 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 369 Configure Password Aging

Operation	Command	Description
Enter system view	system-view	
Enable password aging	password-control aging enable	By default, password aging is enabled.
Set an aging time for super passwords	password-control super aging aging-time	By default, it 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 does the system alert the users.	password-control alert-before-expire alert-time	By default, users are alerted seven days ahead of the password expiration.

To cancel the above configurations, you can use the corresponding undo commands.



CAUTION: You can configure the password aging parameters when password aging is not yet enabled, but these parameters will not take effect.

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:

- The password has not expired and its remaining usable time is greater than the configured alert time. In this case, the user log in successfully.
- The password has not expired but its remaining usable time is no more than the configured alert time. In this case, the system alerts the user to the remaining time (in days) before the password expires and prompt the user to change the password.
 - If the user chooses to change the password and change it successfully, the system saves the new password, restarts the password aging procedure, and at the same time allows the user to log in.
 - If the user chooses to change the password but fails to do so, or the user chooses not to change the password, the system just allows the user to log in.
- 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 re-change the password if the user input an inappropriate password or the two inputs are inconsistent.



CAUTION: After the user updates the password successfully, the switch saves the old password in a readable file in the flash memory.



CAUTION: The switch does not provide the alert function for super passwords.



CAUTION: The switch does not provide the alert function for FTP passwords. And when a FTP user logs in with a wrong password, the system just inform the user of the password error, it does not allow the user to change the password.

Configuring the 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 input password has a length that does not meet the limitation condition, it informs the user of this case and requires the user to input a new password.

Table 370 Configure the Minimum Password Length

Operation	Command	Description
Enter system view	system-view	
Enable the limitation of minimum password length	password-control length enable	By default, the limitation of minimum password length is enabled.
Configure a minimum length for super passwords	password-control super length min-length	By default, it is 10 characters.
Configure a minimum length for all user passwords	password-control length length	By default, it is 10 characters.

Configuring History Password Recording

After History password recording is 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 of this is to inhibit the users from using one single password for a long time or using an old password that was once used to enhance the security.

Table 371 Configure History Password Recording

Operation	Command	Description
Enter system view	system-view	
Enable history password recording	password-control history enable	By default, history password recording is enabled.
Configure the maximum number of the history password records	password-control history max-record-num	By default, the maximum number is four.



CAUTION: When adding a new record but the number of the recorded history passwords exceeds the configured maximum number, the system replaces the oldest record of the user with the new one.



CAUTION: When you configure the maximum number of history password records, if the number of the history password records of a user succeeds your configuration value, the excessive old records will be lost.



CAUTION: When updating a password, do not reuse one of the recorded history passwords, or else, the system will give a prompt to reset a password.

The system administrator can perform the following operations to manually remove history password records.

Table 372 Remove History Password Records Manually

Operation	Command	Description
Enter system view	<code>system-view</code>	
Remove history password records of one or all users	<code>reset password-control history-record [username username]</code>	Executing this command without the <code>username username</code> option will remove the history password records of all users. Executing this command with the <code>username username</code> option will remove the history password records of the specified user.
Remove history records of one or all super passwords	<code>reset password-control history-record super [level level-value]</code>	Executing this command without the <code>level level-value</code> option will remove the history records of all super passwords. Executing this command with the <code>level level-value</code> option will remove the history records of the super password for the users at the specified level.

Configuring User Login Password in Encryption Mode

Table 373 Configure User Login Password in Encryption Mode

Operation	Command	Description
Enter system view	<code>system-view</code>	
Enter the specified user view	<code>local-user username</code>	
Configure a user login password in encryption mode	<code>password</code>	Input a password at the prompt of the system and ensure the two inputs are consistent.

Configuring Login Attempts Limitation and Failure Procession Mode

Table 374 Configure Login Attempts Limitation and Failure Procession Mode

Operation	Command	Description
Enter system view	<code>system-view</code>	
Enable the login attempts limitation, configure the maximum login attempt times and configure the procession mode used when the maximum attempt times is exceeded.	<code>password-control login-attempt login-times [exceed { lock unlock locktime time }]</code>	By default, the maximum attempt times is three, and the switch operates in the locktime procession mode for the users that exceed the maximum times.

Table 374 Configure Login Attempts Limitation and Failure Procession Mode

Operation	Command	Description
Display the information about one or all users added in the blacklist	display password-control blacklist [username username ipaddress ip-address]	You can execute the display command in any view

When the maximum attempt times is exceeded, the system operates in one of the following procession mode:

- **locktime:** in this mode, the system inhibit the user from re-login within a certain time period. After that period of time, the user is allowed to log in the switch again. By default, this time is 120 minutes.
- **lock:** in this mode, the system inhibit the user from re-login forever. The user is allowed to log in 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: No inhibition operation is performed for the users who execute the super command but fail the password attempts.



CAUTION: If a user in the blacklist changes his/her IP address, the blacklist will not affect the user anymore when the user logs in the switch.

The system administrator can perform the following operations to manually remove one or all user entries in the blacklist.

Table 375 Remove User Entries in Blacklist

Operation	Command	Description
Enter system view	system-view	
Delete one specific or all user entries in the blacklist	reset password-control blacklist [username username]	Executing this command without the username username option will remove all the user entries in the blacklist. Executing this command with the username username option will remove the specified user entry in the blacklist.

Configuring the Timeout for User Password Authentication

The authentication procedure starts from the time the local/remote server of the switch receives the user name and ends at the time the user authentication is completed. Whether the user is authenticated on the local server or on a remote server is determined by the related AAA configuration. For more details, see the secure module of this guide.

If a password authentication is not completed within the configured authentication timeout time, the authentication fails, and the system terminates the connection of the user and makes some logging.

If a password authentication is completed without timing out, the user will log in the switch normally.

Table 376 Configuring the Timeout for User Password Authentication

Operation	Command	Description
Enter system view	<code>system-view</code>	
Configure the timeout time of user password authentication	<code>password-control authentication-time out authentication-time out</code>	By default, it is 60 seconds.

Displaying Password Control

After the above configurations, you can execute the display command in any view to display the operation of the password control and verify your configurations.

Table 377 Displaying Password Control

Operation	Command
Display the information about the global password control for all users	<code>display password-control</code>
Display the information about the password control for super passwords	<code>display password-control super</code>
Display the information about one or all users who have been added to the blacklist because of password attempt failure	<code>display password-control blacklist [username username ipaddress ip-address]</code>

Password Control Configuration Example

Network Requirements A PC is connected to a Switch 4500. You can configure the password control parameters as required.

Figure 104




```

Configuration Procedure # Configure the system login password.
<4500>system-view
System View: return to User View with Ctrl+Z.
[4500]local-user test
New local user added.
[4500-luser-test]password
Password:*****
confirm:*****

# Change the system login password to 0123456789.

[4500-luser-test]password
Password:*****
Confirm :*****
Updating the password file ,please wait ...

# Enable password aging.

[4500]password-control aging enable
Password aging enabled for all users. Default: 90 days.

# Enable the limitation of the minimum password length.

[4500]password-control length enable
Password minimum length enabled for all users. Default: 10
characters.

# Enable history password recording.

[4500]password-control history enable
Password history enabled for all users.

# Configure the aging time of super passwords to 10 days.

[4500]password-control super aging 10
The super password aging time is 10 days.

# Display the information about the global password control for all users.

[4500] display password-control
Global password settings for all users:
  Password Aging:      Enabled (90 days)
  Password Length:    Enabled (10 Characters)
  Password History:    Enabled (Max history-record num : 6)
  Password alert-before-expire: 7 days
  Password Authentication-timeout : 60 seconds
Password Attemp-failed action : Disable
Password History was last reset 38 days ago.

# Display the names and corresponding IP addresses of all the users that have
been added to the blacklist because of password attempt failure.

[4500] display password-control blacklist
USERNAME                IP
Jack                    10.1.1.2
The number of users in blacklist is :1

# Remove the history password records of all users.

<4500> reset password-control history-record
Are you sure to delete all the history record?[Y/N]

If you input "Y", the system removes the history records of all users and gives the
following prompt:

All historical passwords have been cleared for all users.

```


A

PASSWORD RECOVERY PROCESS

Introduction

The Switch 4500 has two separate password systems:

- Passwords which are used by the Web user interface and the CLI and are stored in the 3comoscfg.cfg file.

For more information on this, refer to the Getting Started Guide that accompanies your Switch.

- A password system which protects the bootrom and is stored in the bootrom.

If the password protecting the bootrom is forgotten or lost, a fixed (unit unique) password can be provided by 3Com Technical Support to bypass the lost password.

This fixed password recovery mechanism can be disabled within the bootrom menu. However, if the password recovery mechanism is disabled and the user configurable bootrom password is lost, there is no recovery mechanism available. In this instance, the Switch will need to be returned to 3Com for repair.

The following commands are all executed from the Bootrom directly via the console.

CLI Commands Controlling Bootrom Access

Access to the bootrom is enabled by default on your Switch. To disable access enter the following command:

```
<4500-XX>undo startup bootrom-access enable
```

(where **xx** is either SI or EI)

If the bootrom is disabled, *Ctrl-B* is still available during the initial boot phase. The only password that will be accepted at the prompt is the unit unique password. any user configured bootrom password will be inactive.

The following commands enable and display the current bootrom access settings respectively:

```
<4500-xx>startup bootrom-access enable  
<4500-xx>display startup
```

Bootrom Interface

During the initial boot phase of the Switch (when directly connected via the console), various messages are displayed and the following prompt is shown with a five second countdown timer:

```
Press Ctrl-B to enter Boot Menu... 4
```

Before the countdown reaches 0 enter <CTRL>B.

The timer is followed by a password prompt. The default is no password.

Press *Enter* to display the following 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):
```

Enter the boot menu number to display that menu option.

Displaying all Files in Flash

Enter boot menu option 3 to display the following:

```
Boot menu choice: 3
File Number   File Size(bytes) File Name
=====
1              714784          s4h01_04.zip
2              164             private-data.txt
3              11043           3ComOScfg.def
4              4               snmpboots
5*            4529259         s4b03_01_04s56.app
6              11343           3ComOScfg.cfg
```

```
Free Space: 10460160 bytes
The current application file is s4b03_01_04s56.app.
```

[Table 378](#) displays the configuration files:

Table 378 Configuration Files

Filename	Description
3comoscfg.def	This file contains the factory default configurations. It is only used if there is no other configuration file present. This file should not be modified.
3comoscfg.cfg	This file contains the live configurations and is always used to load the active configuration into the Switch unless the bootrom skip current configuration file is specified.

Skipping the Current Configuration File

Enter boot menu option 7 to enable the Switch to boot from the factory default configuration file `3comoscfg.def`.

When the Switch has booted from the factory default it can be configured with an IP address and default gateway if needed.

The live configuration file (`3comoscfg.cfg`) can be added to a TFTP server and edited.

Search through the file with a text editor until the following section is found:

```
#
local-user admin
  password cipher ZG6-:\Y>MQGQ=^Q`MAF4<1!!
  service-type telnet terminal
  level 3
local-user manager
  password simple manager
  service-type telnet terminal
  level 2
local-user monitor
  password simple monitor
  service-type telnet terminal
  level 1
#
```

In the `local-user admin` section there is an entry called `password` which is followed by either of the following entries:

- **Simple** - this enables you to read and/or change a password and send the configuration file via TFTP back into the Switch.
- **Cipher** - change this word to **simple** and replace the encrypted password with a plain text password and send the configuration file via TFTP back into the Switch.

The `manager` and `monitor` passwords can be modified in the same way.

Bootrom Passwords

The bootrom can be configured with a user defined password. Select Option 5 to display the following:

```
Boot menu choice: 5

Old password:
New password:xxxx
Confirm password:xxxx
Current password has been changed successfully!
```

If the user configured bootrom password is lost, a fixed, unit unique password can be provided by 3Com Technical Support to bypass the lost password.



Please ensure that the Switch is registered with 3Com promptly as the unit unique password will only be supplied to the registered owner of the Switch.

This final password recovery safeguard can be disabled.

Bootrom Password Recovery

Select option 8 to set the bootrom password discovery. The following is displayed:

```
Warning: if disable the bootrom password recovery, the super password  
based on switch mac address is invalid!  
The current mode is enable bootrom password recovery.
```

```
Are you sure to disable bootrom password recovery? Yes or No(Y/N)
```

This option allows the user to disable the fixed, unit unique password recovery mechanism. If this is disabled and the bootrom password recovery is lost then a recovery will not be possible. In this instance, the Switch will need to be returned to 3Com for repair.

B

RADIUS SERVER AND RADIUS CLIENT SETUP

This appendix covers the following topics:

- [Setting Up a RADIUS Server](#)
- [Setting Up the RADIUS Client](#)

Setting Up a RADIUS Server

There are many third party applications available to configure a RADIUS server. 3Com has successfully installed and tested the following applications on networks with the Switch 4500.

For Windows servers:

- Microsoft IAS RADIUS (creates a standard RADIUS server)
- Funk RADIUS (creates an enhanced RADIUS server)

For Solaris and Linux servers:

- FreeRADIUS

The remainder of this section describes how to setup a RADIUS server using these products.



Microsoft IAS RADIUS, Funk RADIUS and FreeRADIUS are not 3Com products and are not supported by 3Com.

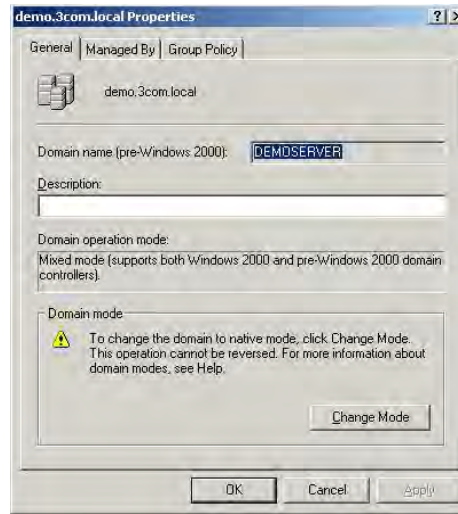
Configuring Microsoft IAS RADIUS

3Com has successfully installed and tested Microsoft IAS RADIUS running on a Windows server in a network with Switch 4500 deployed.

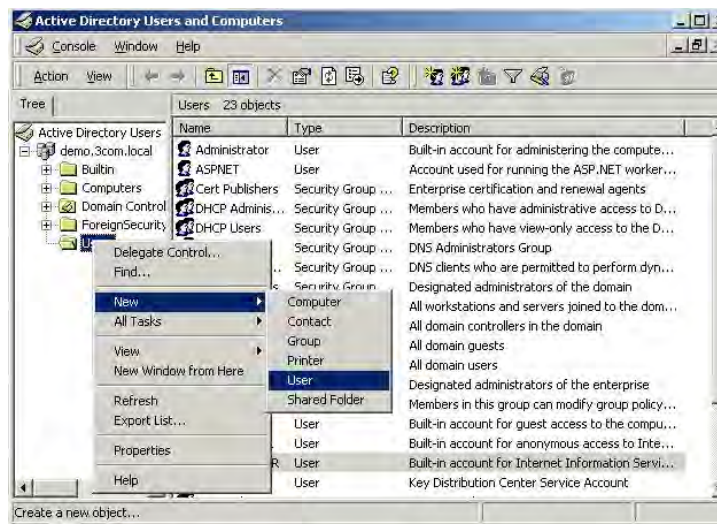
The following steps are required to setup a RADIUS server using the Microsoft IAS RADIUS application. You will need to use the Install CD for Microsoft Windows 2000 Server to complete the process.

- 1 Install Windows 2000 Server (Vanilla Install) on a Windows PC, with the latest available patches from <http://windowsupdate.microsoft.com>.
- 2 Configure the server as a Domain Name Server (DNS) by running `dcpromo`
 - a For example, create the domain `demo.3com.local` and enable it as a DNS server for the network.
 - b The server will need to run in Native mode in order to support EAP-TLS which is not available in Mixed mode. To change mode go to the *Active Directory Users*

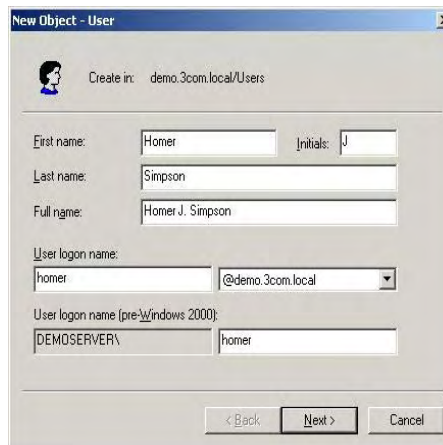
and *Computers* window, right-click *Domain* and choose *Properties*, select *Change Mode*.



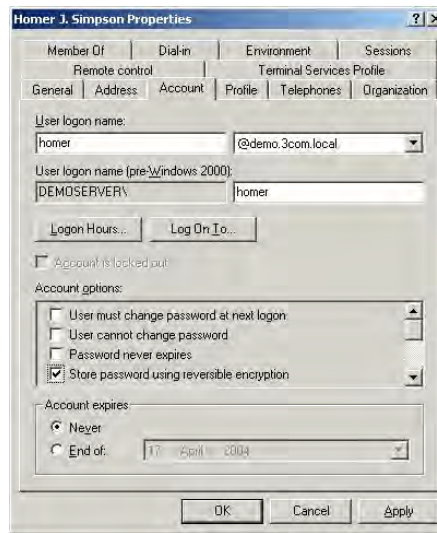
- c Add a user that is allowed to use the network. Go to *Active Directory Users and Computers*, from the left hand window right-click the *Users* folder and choose *New > User*, as shown below.



- d Follow the wizard to create a user, enter the required information at each stage



- e The password for the user must be set to be stored in reversible encryption. Right-click the user account and select *Properties*. Select the *Account* tab, check the box labeled *Store password using reversible encryption*.

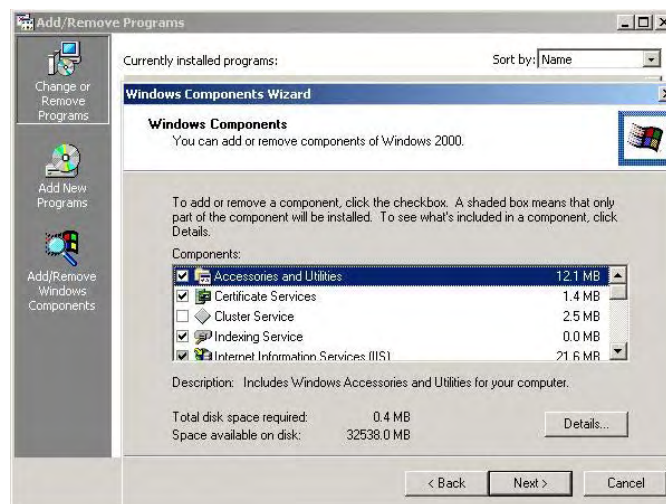


- f Now re-enter the password for the account, right-click the user account and select *Reset Password...*
- 3 Enable the server as a certificate server. To use EAP-TLS certificate based authentication, you need to enable the Certificate services in windows.



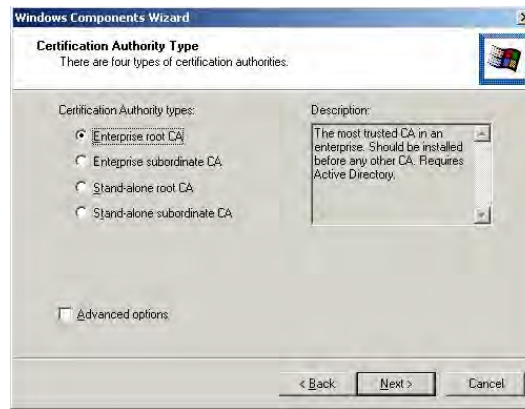
Make sure you have completed step 2 and created the DNS server, before enabling Certificate services. You will not be able to create the DNS server after certification has been enabled.

- a Go to *Control Panel > Add/Remove Programs > Add/Remove Windows Components*. The *Certificate Services* component should be checked.



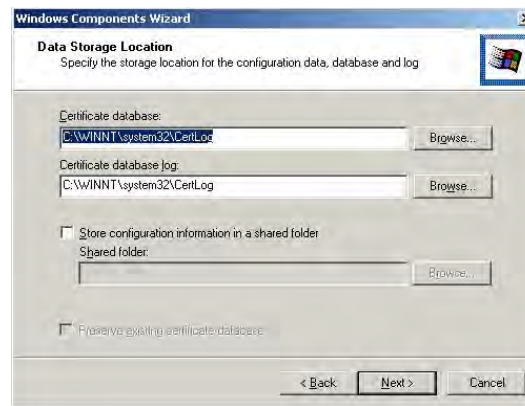
- b Select *Next* and continue through the wizard.

In the *Certificate Authority Type* window select *Enterprise root CA*



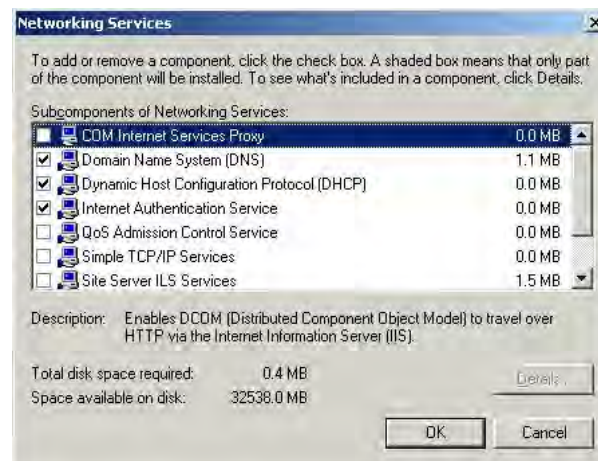
Enter information to identify the Certificate Authority on the *CA Identifying Information* window.

Enter the storage location on the *Data Storage Location* window.



To complete the installation and set up of the certificates server, the wizard will require the Install CD for Microsoft Windows 2000 Server.

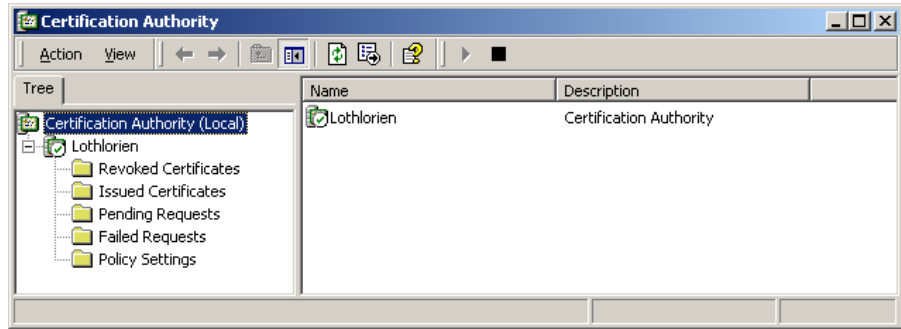
- 4 Install the Internet Authentication Service (IAS) program.
 - a Go to *Control Panel > Add/Remove Programs > Add/Remove Windows Components*. Enable *Networking Services* and ensure *Internet Authentication Service* component is checked.



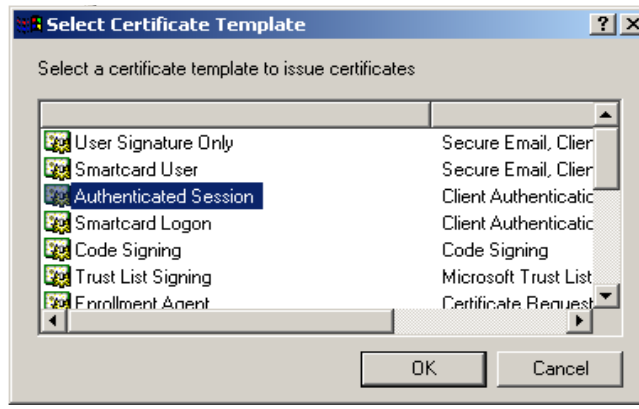
- b Select *OK* to end the wizard.

5 Configure a Certificate Authority

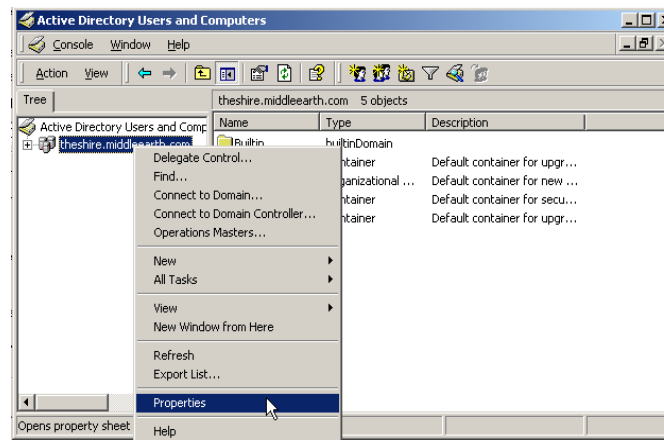
- a Go to *Programs > Administrative Tools > Certification Authority* and right-click *Policy Settings* under your Certificate Authority server.



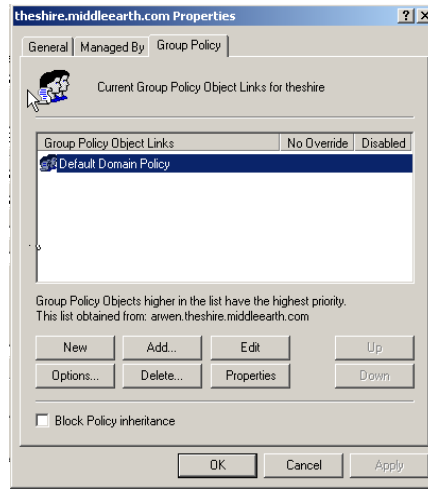
- b Select *New > Certificate to Issue*
- c Select *Authenticated Session* and select *OK*.



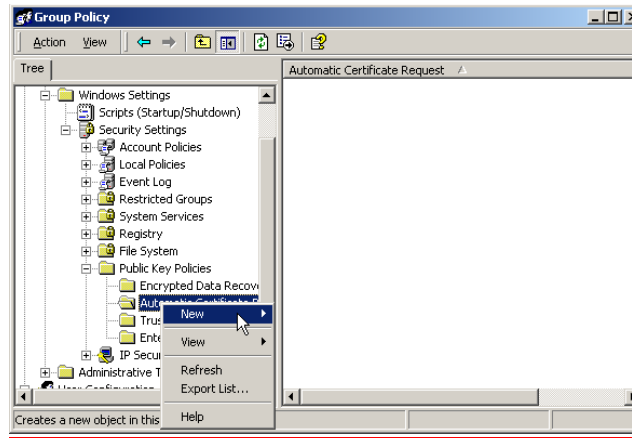
- d Go to *Programs > Administrative Tools > Active Directory Users and Computers* and right-click your active directory domain. Select *Properties*



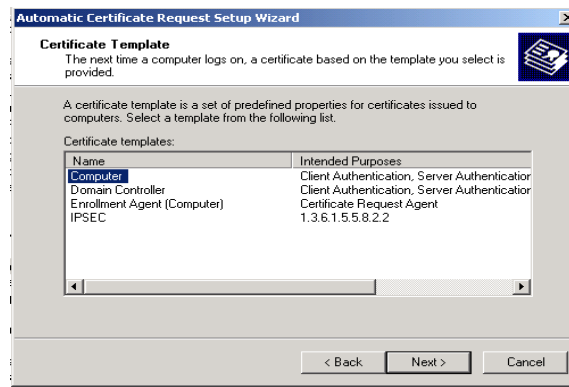
- e Select the *Group Policy* tab, and ensure that the *Default Domain Policy* is highlighted. Click *Edit* to launch the Group Policy editor.



- f Go to *Computer Configuration > Windows Settings > Security Settings > Public Key Policies*, and right-click *Automatic Certificate Request Settings*. Select *New > Automatic Certificate Request*.

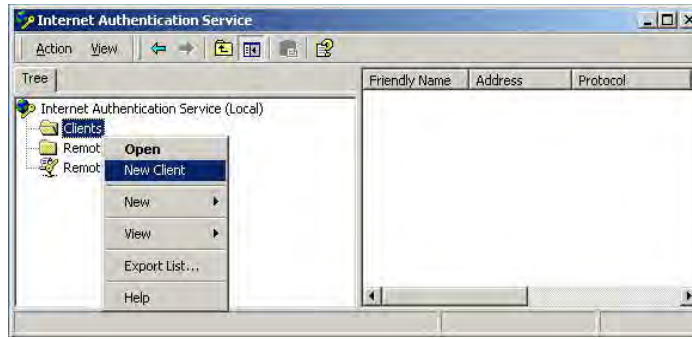


- g The Certificate Request Wizard will start. Select *Next > Computer certificate template* and click *Next*.

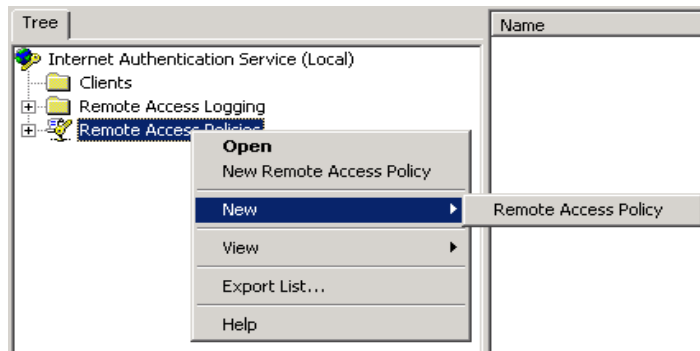


- h Ensure that your *Certificate Authority* is checked, then click *Next*. Review the *Policy Change Information* and click *Finish*.

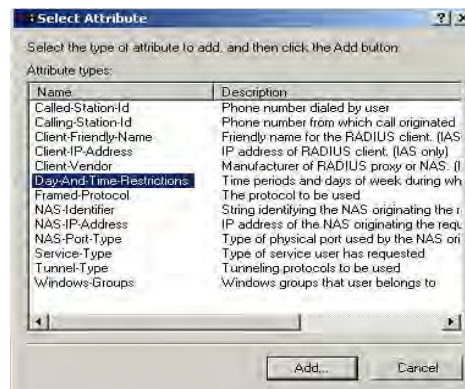
- i Open up a command prompt (*Start > Run*, enter `cmd`). Enter `secedit /refreshpolicy machine_policy`. The command may take a few minutes to take effect.
- 6 Setup the Internet Authentication Service (IAS) RADIUS Server
- a Go to *Programs > Administrative Tools > Internet Authentication Service*, right-click *Clients*, and *Select New Client*.



- b Enter a name for your device that supports IEEE 802.1X. Click *Next*.
- c Enter the IP address of your device that supports IEEE 802.1X, and set a shared secret. Select *Finish*. Leave all the other settings as default.
- d Right-click *Remote Access Policies*, and select *New Remote Access Policy*.

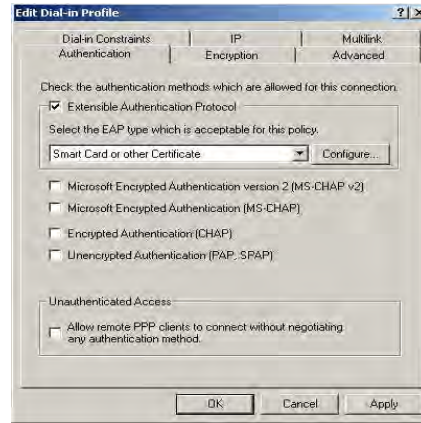


- e Give the policy a name, for example EAP-TLS, and select *Next*.
- f Click *Add...*
- g Set the conditions for using the policy to access the network. Select *Day-And-Time-Restrictions*, and click *Add...*

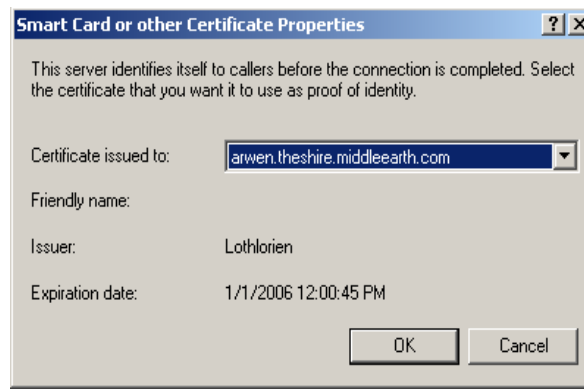


Click *Permitted*, then *OK*. Select *Next*.

- h Select *Grant remote access permission*, and select *Next*
- i Click on *Edit Profile...* and select the *Authentication* tab. Ensure *Extensible Authentication Protocol* is selected, and *Smart Card or other Certificate* is set. Deselect any other authentication methods listed. Click *OK*.



- j Click the *Configure* button next to the *EAP type selector*.
- k Select the appropriate certificate and click *OK*. There should be at least one certificate. This is the certificate that has been created during the installation of the Certification Authority Service.



Windows may ask if you wish to view the Help topic for EAP. Select *No* if you want to continue with the installation.

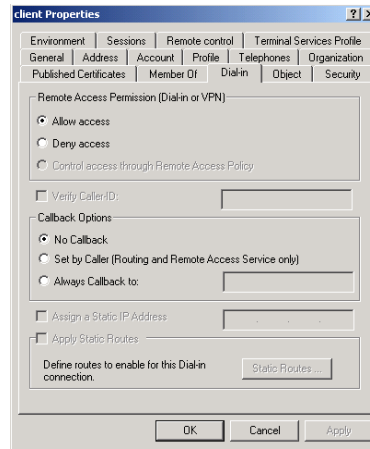
- l Click *Finish*.



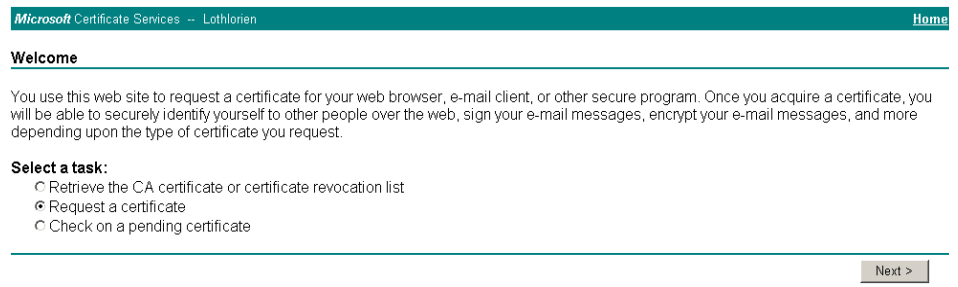
For EAP-TLS to work correctly, it is important that there is only one policy configured in IAS.

- 7 Enable Remote Access Login for Users.
 - a Select *Programs > Administrative Tools > Active Directory Users and Computers*. Double-click the user account for which you want to enable authentication.

- b Select the *Dial-in* tab from the client *Properties* window. Select *Allow access*. Click *OK*.



- c Click *OK* to confirm.
- 8 Configure the Switch 4500 for RADIUS access and client authentication see [Chapter 11 “802.1X Configuration”](#).
- 9 Generate a certificate by requesting a certificate from the Certification Authority. The certificate is used to authorize the RADIUS client with the RADIUS Server.
- On the RADIUS server, open *Internet Explorer* and enter the URL **http://localhost/certsrv**
 - When you are prompted for a login, enter the user account name and password that you will be using for the certificate.
 - Select *Request a certificate* and click *Next >*



There are two ways to request a certificate: the Advanced Request or the Standard Request. The following steps show an Advanced Request.



The Standard Request differs in the way the certificate is stored on the local computer, it allows you to install the certificate on your computer directly after it is generated and does not require the complex configuration of the Advanced Request. You will, however, still need to map the certificate to the username in the Active Directory Services for the Standard Request, see [step u](#).

d Select *Advanced request* and click *Next >*

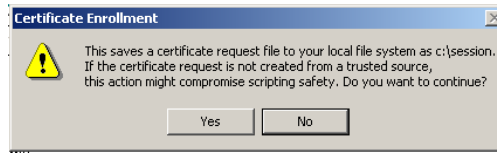
e Select the first option and click *Next >*

f Either copy the settings from the screenshot below or choose different key options. Click *Save* to save the PKCS #10 file.

The PKCS #10 file is used to generate a certificate.

g You will receive this warning message, select *Yes*

followed by this warning message, select Yes



and then OK

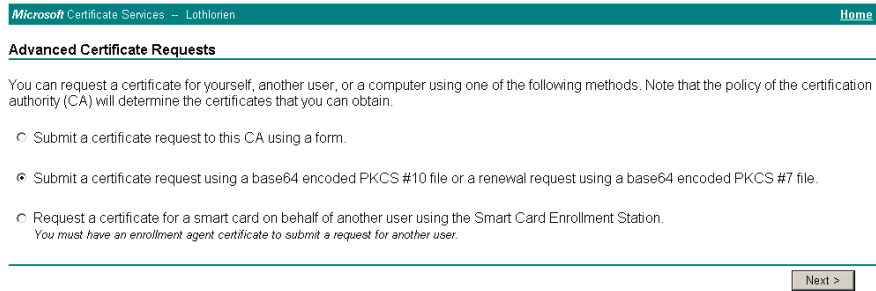


The PKCS #10 file is now saved to the local drive.

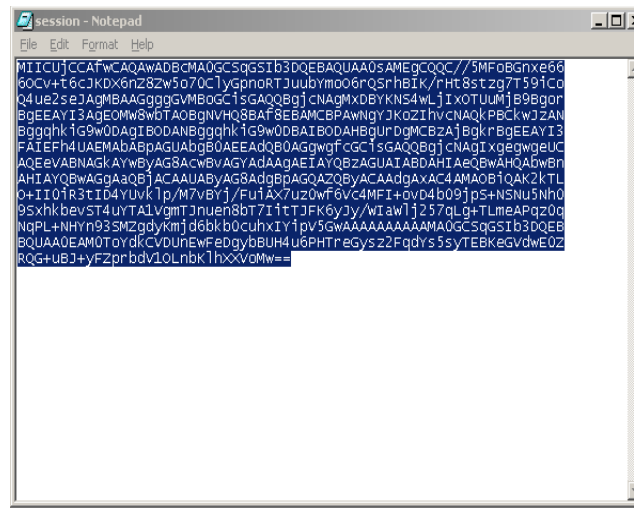
- h** To generate a portable certificate using PKCS #10, click the *Home* hyperlink at the top right of the CA Webpage.



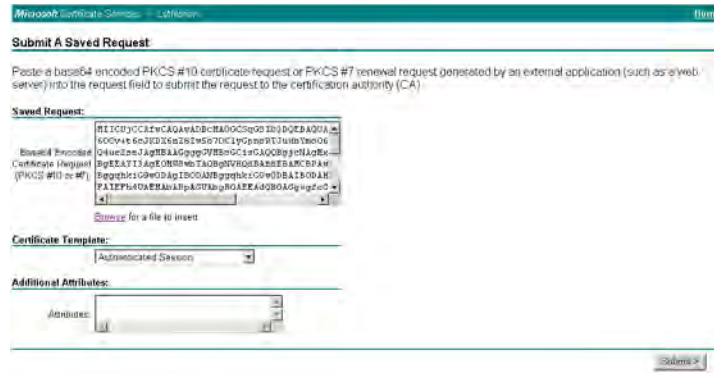
- i** Select *Request a certificate > Next > Advanced request > Next*
- j** Select the second option as shown in the screenshot below, and click *Next >*



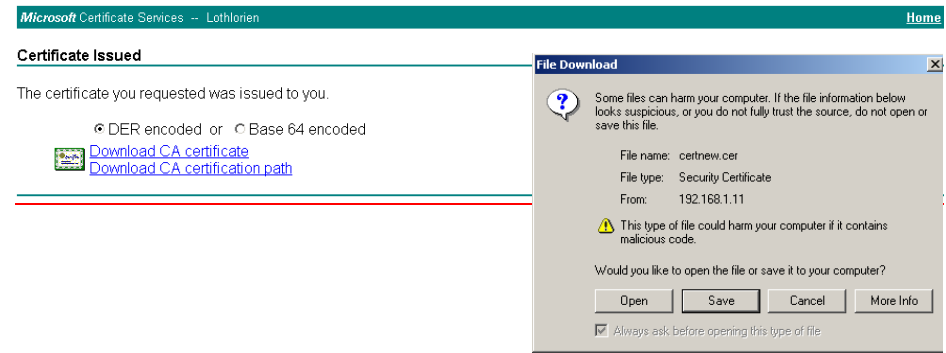
- k** Open the previously saved PKCS #10 certificate file in Notepad, select all (Control + a) and copy (Control + c), as shown below



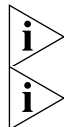
- l Paste the copied information into the *Saved Request* field as shown below. Select *Authenticated Session* from the *Certificate Template* selector and click *Submit* >



- m Download the certificate and certification path. Click on the *Download CA Certificate* hyperlink to save the certificate. Save the file as DER encoded..



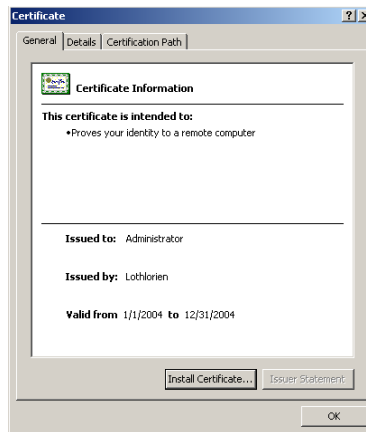
Click on the *Download CA certification path* hyperlink to save the PKCS #7, and select *Save*



The certificate is also installed on the Certification Authority. You can verify this in the CA Administration tool under Issued Certificates

The PKCS #7 file is not actually required for IEEE 802.1X functionality.

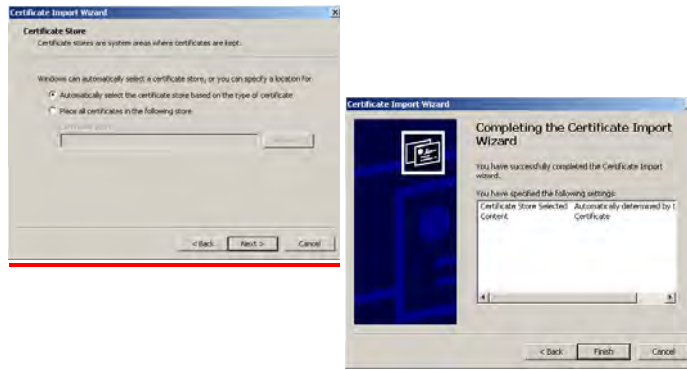
- n Install both PKCS #10 and PKCS #7 files on the workstation that requires IEEE 802.1X Network Login. On the workstation, double-click the certificate file (extension is .cer)



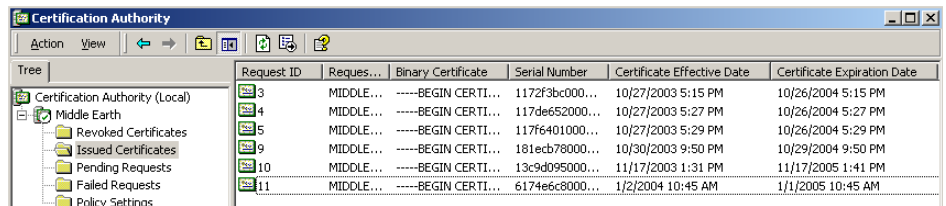
- o Click *Install Certificate* to launch the certificate import wizard



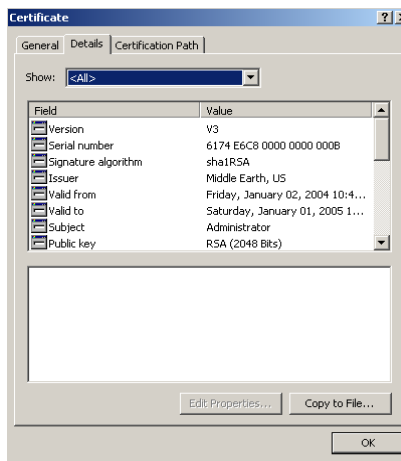
- p Leave the settings on the next screen as is, click *Next >* followed by *Finish* and *OK*. This will install the certificate,



- q Launch the *Certification Authority* management tool on the server and expand the *Issued Certificates* folder. You should see the newly created certificate.



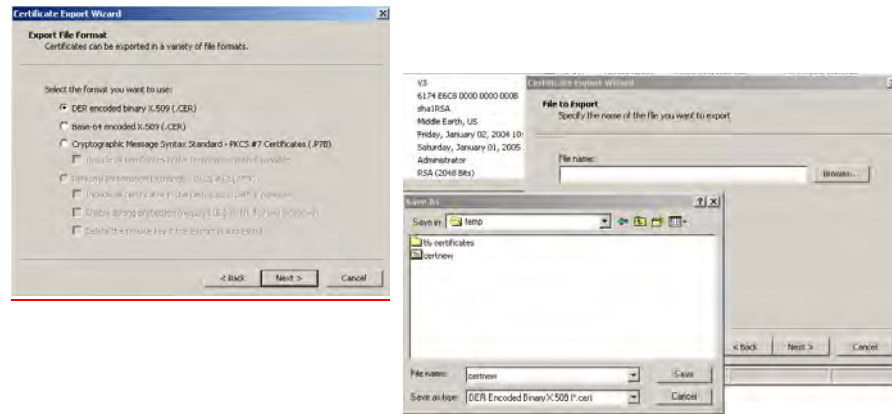
- r Double-click the certificate that was generated by the client and select the *Details* tab



- s Click *Copy to File* to save the certificate. This action is actually already performed with the Advanced Request, but this is an alternative way to save the certificate. Click *Next* when the wizard is launched.



Save the certificate using DER x.509 encoding, select *DER encoded binary* followed by *Next*. Provide a name for the certificate and save it to a specified location.



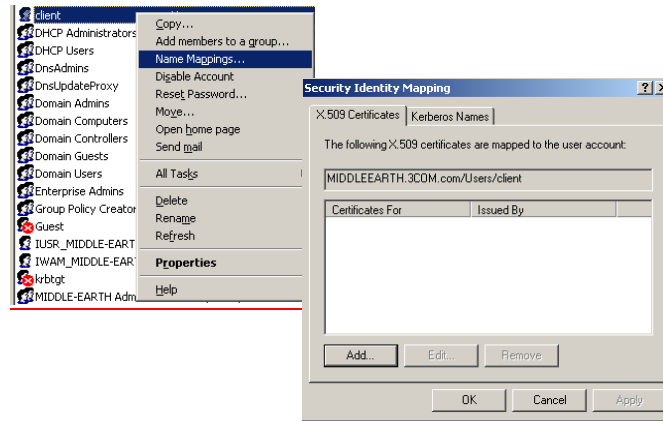
Click *Finish* and followed by *OK*.



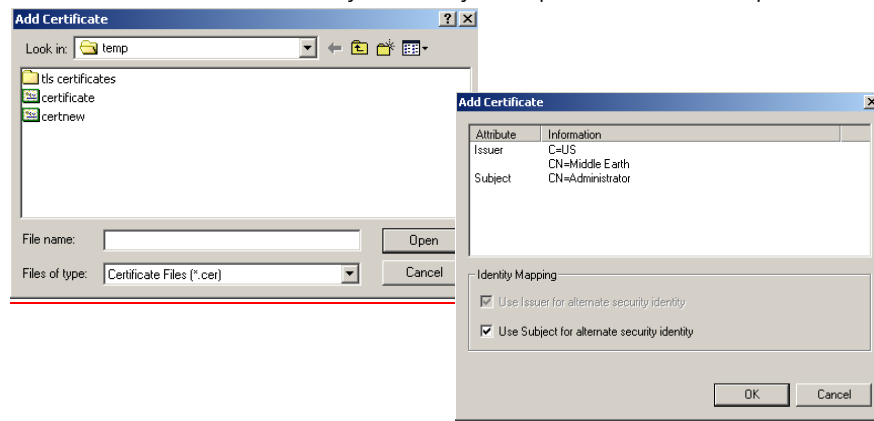
- t Exit the *Certification Authority* management tool and launch the *Active Directory Users and Computers* management tool. Ensure that the *Advanced Features* are enabled in the *Action* menu, as shown below.



- u Select the user that becomes the IEEE 802.1X client. Right-click on the user and select *Name mappings*. Select *Add*



- v Select the certificate that you have just exported and click *Open*. Click *OK*



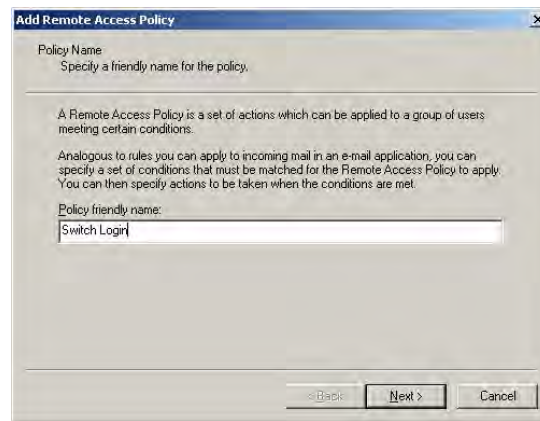
- w In the *Security Identity Mapping* screen, click *OK* to close it.
- x Close the *Active Directory Users and Domains* management tool. This completes the configuration of the RADIUS server.

10 Configure Microsoft IAS RADIUS Server for Switch Login.

- a Create a Windows Group that contains the users that are allowed access to the Switch 4500. Add an additional user as a member of this windows group:

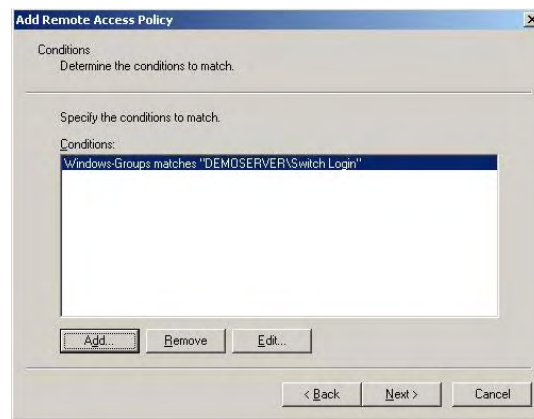


- b Create a new remote access policy under IAS and name it *Switch Login*. Select *Next>..*



The screenshot shows the 'Add Remote Access Policy' dialog box with the 'Policy Name' tab selected. The text reads: 'Specify a friendly name for the policy.' Below this is a text box containing 'Switch Login'. There is also explanatory text: 'A Remote Access Policy is a set of actions which can be applied to a group of users meeting certain conditions. Analogous to rules you can apply to incoming mail in an e-mail application, you can specify a set of conditions that must be matched for the Remote Access Policy to apply. You can then specify actions to be taken when the conditions are met.' At the bottom are buttons for '< Back', 'Next >', and 'Cancel'.

- c Specify *Switch Login* to match the users in the switch access group, select *Next >*



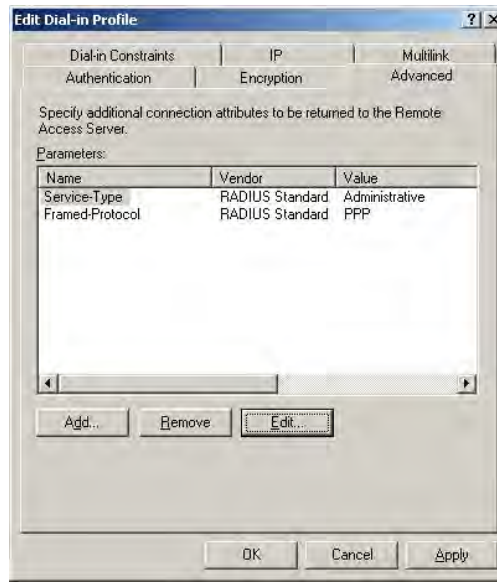
The screenshot shows the 'Add Remote Access Policy' dialog box with the 'Conditions' tab selected. The text reads: 'Determine the conditions to match.' Below this is a list box containing one condition: 'Windows Groups matches "DEMO SERVER\Switch Login"'. There are buttons for 'Add...', 'Remove', and 'Edit...'. At the bottom are buttons for '< Back', 'Next >', and 'Cancel'.

- d Allow *Switch Login* to grant access to these users, select *Next >*

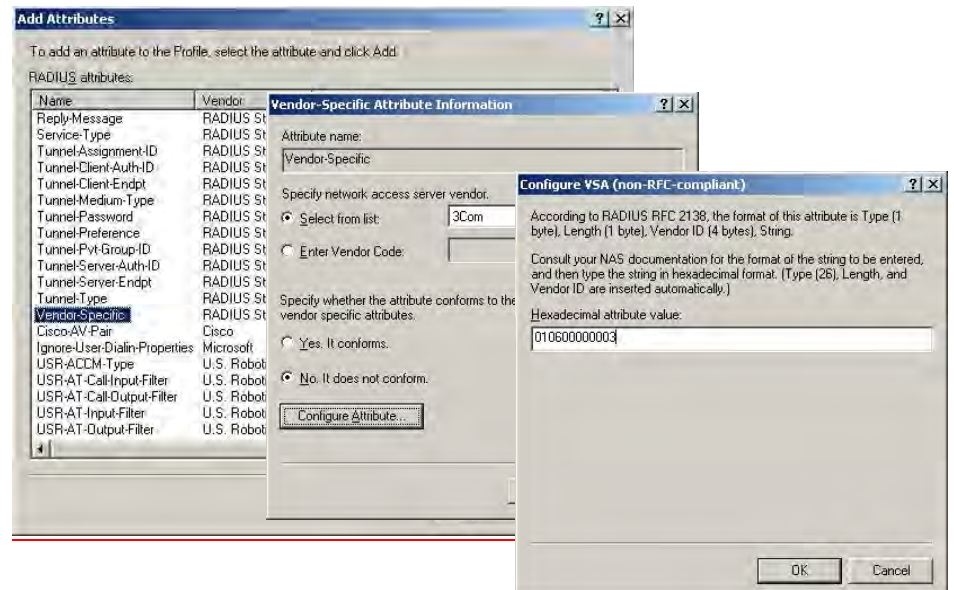


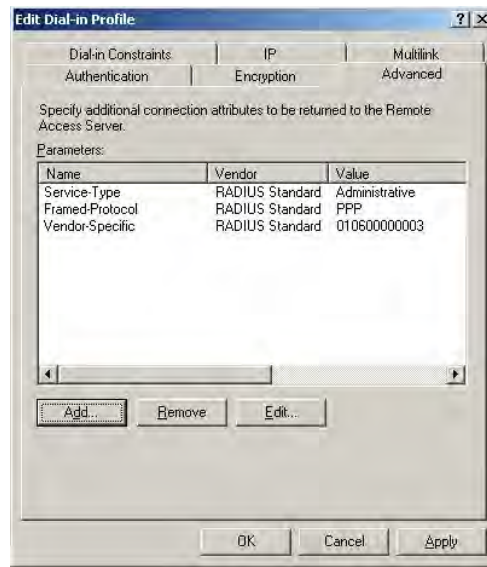
The screenshot shows the 'Add Remote Access Policy' dialog box with the 'Permissions' tab selected. The text reads: 'Determine whether to grant or deny remote access permission.' Below this is explanatory text: 'You can use a Remote Access Policy either to grant certain access privileges to a group of users, or to act as a filter and deny access privileges to a group of users. If a user matches the specified conditions:'. There are two radio buttons: 'Grant remote access permission' (which is selected) and 'Deny remote access permission'. At the bottom are buttons for '< Back', 'Next >', and 'Cancel'.

- e Use the *Edit* button to change the *Service-Type* to *Administrative*.



- f Add a Vendor specific attribute to indicate the access level that should be provided:





The Value 010600000003 indicates admin privileges for the Switch. 01 at the end indicates monitor and 02 indicates manager access. On the Switch 4500, 00 indicates visitor level.

- 11 Configure the RADIUS client. Refer to section [Setting Up the RADIUS Client](#) for information on setting up the client.
- 12 Establish an IEEE 802.1X session, using Microsoft's Internet Authentication Service. When you are prompted to select a certificate (it could be that there are additional active certificates on your client computer), select the certificate that you have installed for this specific Certification Authority server.

If you encounter problems, check the *Event Viewer* and the *System Log* on the server to determine what is what is happening, and possible causes for the problems.

Configuring Auto VLAN and QoS Membership for Microsoft IAS

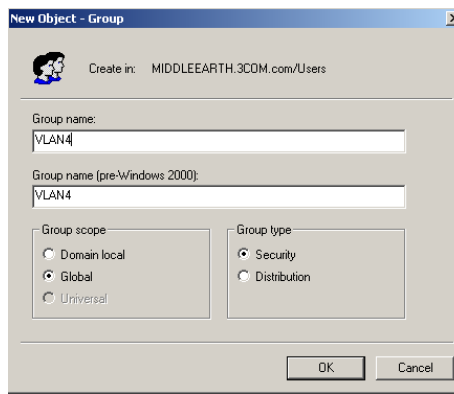
VLAN Groups are used by IAS to assign the correct VLAN ID to each user account. One VLAN Group must be created for each VLAN defined on the Switch 4500. The VLAN Groups must be created as Global/Security groups

Follow these steps to set up auto VLAN and QoS for use by Microsoft IAS:

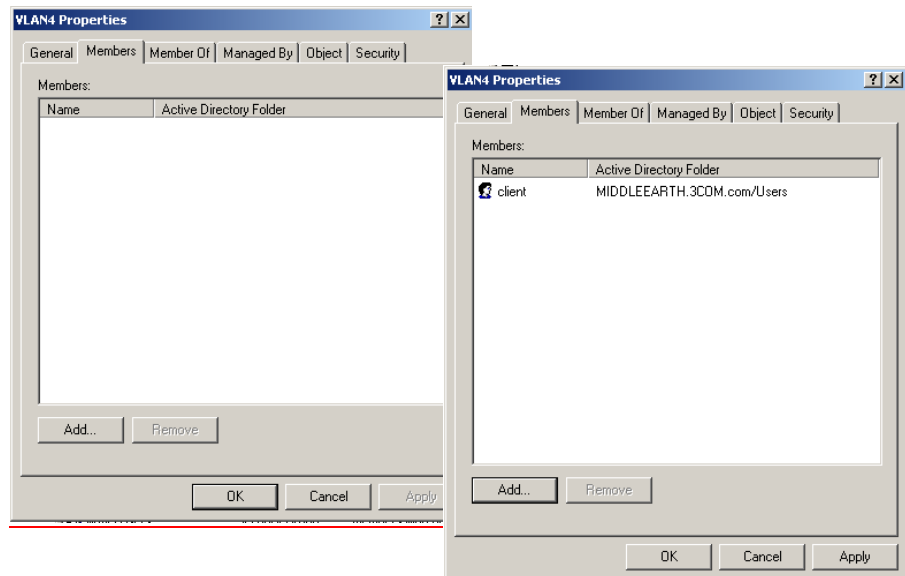
- 1 Define the VLAN Groups on the Active Directory server and assign the user accounts to each VLAN Group. Go to *Programs > Administrative Tools > Active Directory Users and Computers*
 - a For example, to create one group that will represent VLAN 4 select the *Users* folder from the domain (see below),



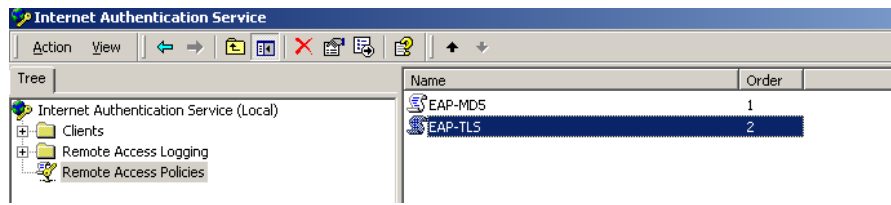
- b Name the VLAN Group with a descriptive name that describes the function of the VLAN Group, for example *VLAN4*. Check *Global* in the *Group Scope* box and *Security* in the *Group Type* box, click *OK*.



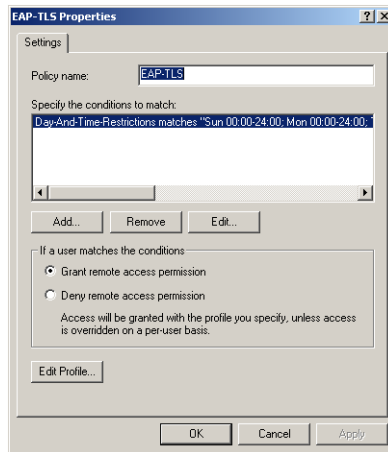
- c Select the group, right click and select *Properties*. Select the *Members* tab, add the users that have received the certificate and will use the VLAN functionality.



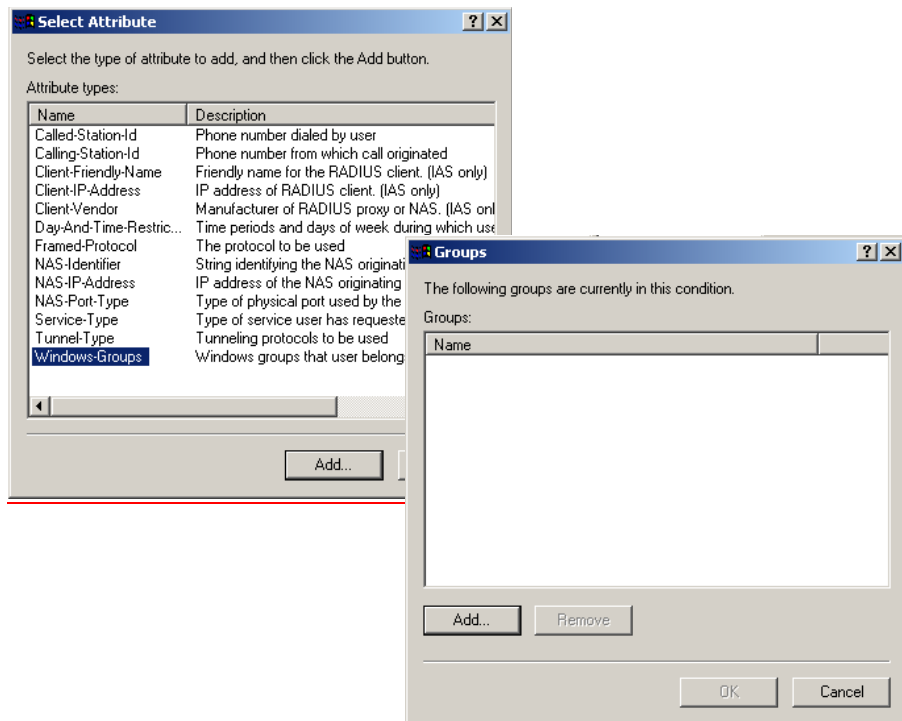
- d Go to *Programs > Administrative Tools > Internet Authentication Service*, and select *Remote Access Policies*. Select the policy that you configured earlier, right-click and select *Properties*.



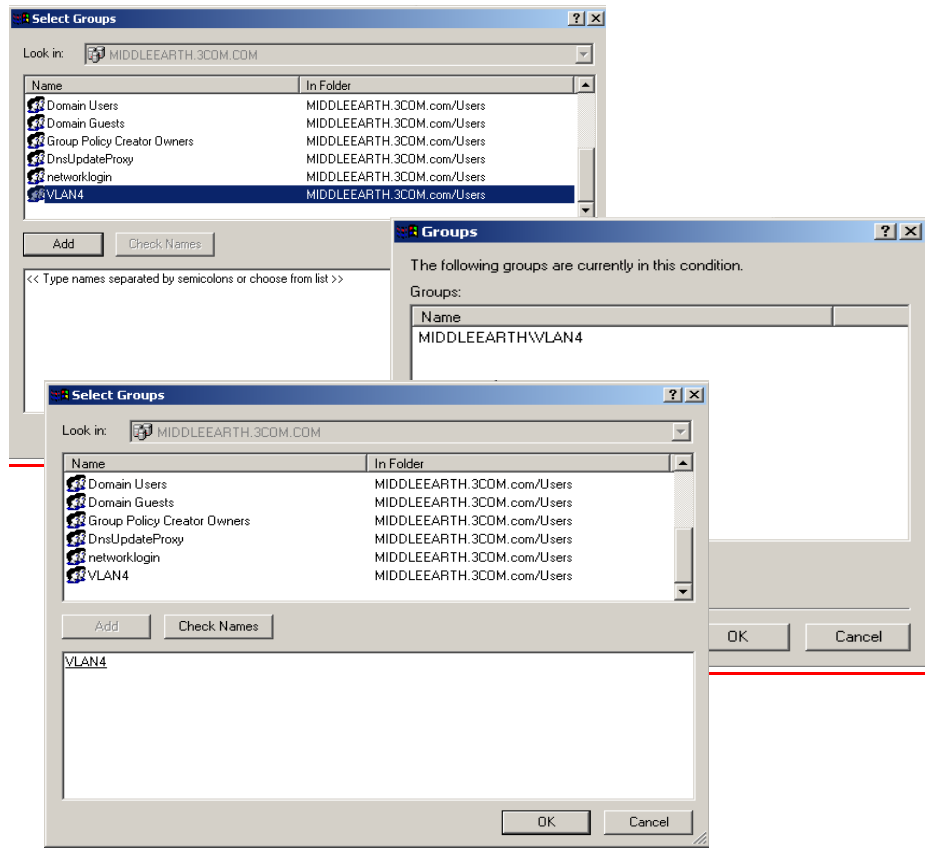
- e Click *Add* to add policy membership.



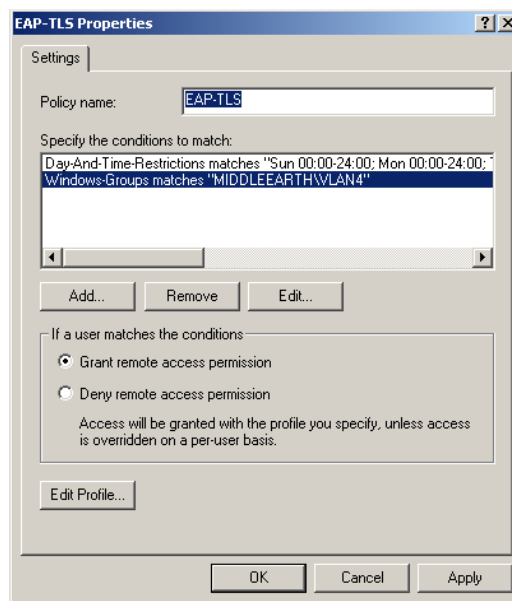
- f Select the *Windows-Groups* attribute type, and select *Add* and *Add* again



- g Select the VLAN group that you have just created and click *Add* and then *OK* to confirm.



- h Click *OK* again to return you to the *Security Policy* properties.



- i Click *Edit Profile...* and select the *Advanced* tab. Click *Add*. Refer to [Table 379](#) and [Table 381](#) for the RADIUS attributes to add to the profile.

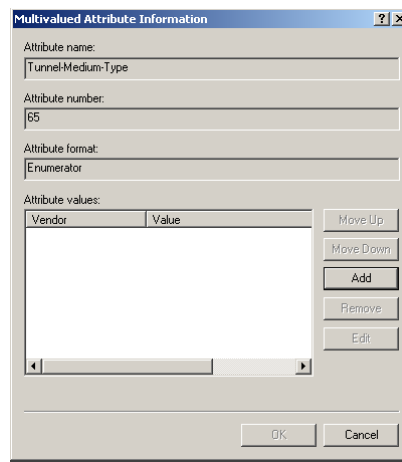
Table 379 Summary of auto VLAN attributes
Table 380

For Auto VLAN	Return String	Comment
Tunnel-Medium-type	802	
Tunnel-Private-Group-ID	2	VLAN value
Tunnel-Type	VLAN	

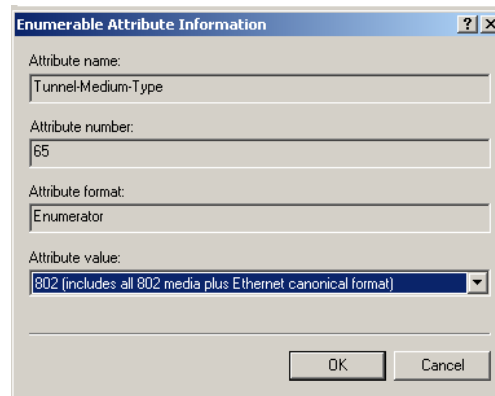
Table 381 Summary of QoS attributes
Table 382

For Auto QoS	Return String	Comment
Filter-id	profile=student	QoS Profile name

j Select *Tunnel-Medium-Type* and click *Add*.

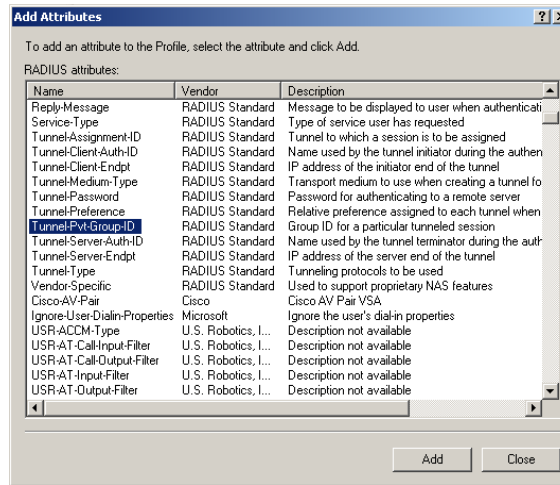


k Ensure that the Attribute value is set to 802 and click *OK*.

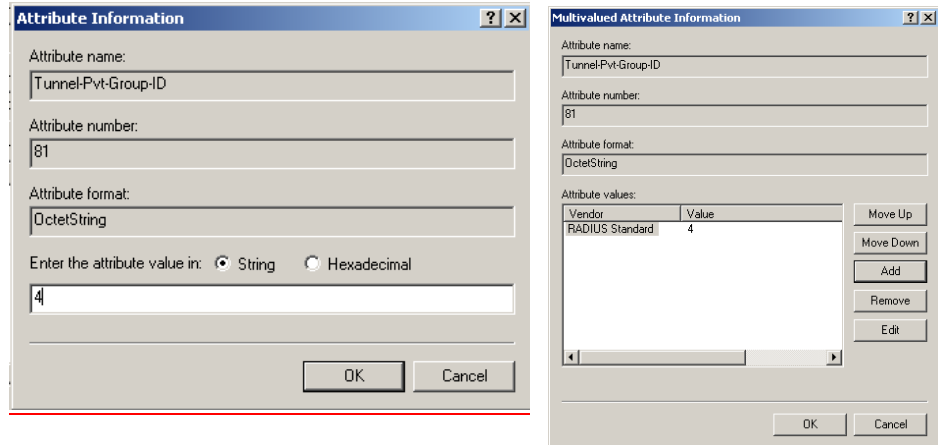


l Click *OK* again on the *Multivalued Attribute Information* screen to return to the *Add Attributes* screen.

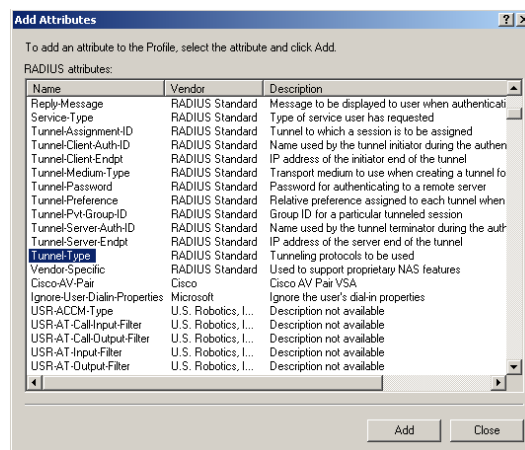
- m Select the *Tunnel-Pvt-Group-ID* entry and click *Add*.



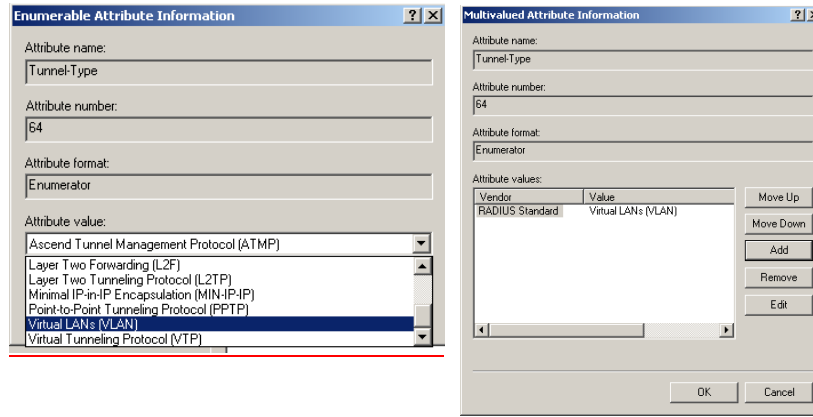
- n Click *Add*, ensure that the Attribute value is set to 4 (Attribute value in string format), and click *OK*. This value represents the VLAN ID.



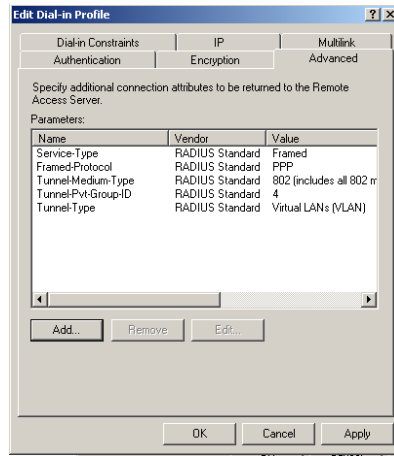
- o Click *OK* again on the *Multivalued Attribute Information* screen to return to the *Add Attributes* screen. Select the *Tunnel-Type* entry and click *Add*.



- p Click *Add* again. In the pull down menu, select *Virtual LANs* and click *OK*.



- q Click *OK* again and to return to the *Add Attributes* screen. Click *Close*. You will now see the added attributes



- r Click *OK* to close the *Profile* screen and *OK* again to close the *Policy* screen. This completes the configuration of the Internet Authentication Service.
- 2 To test the configuration, connect the workstation to a port on the Switch 4500 (the port does not have to be a member of VLAN 4). Ensure that there is a DHCP server connected to the Switch that resides on a switch port that is an untagged member of VLAN 4. The RADIUS server should reside in the same VLAN as the workstation.

Once authenticated the Switch will receive VLAN information from the RADIUS server and will place the switch port in the associated VLAN.

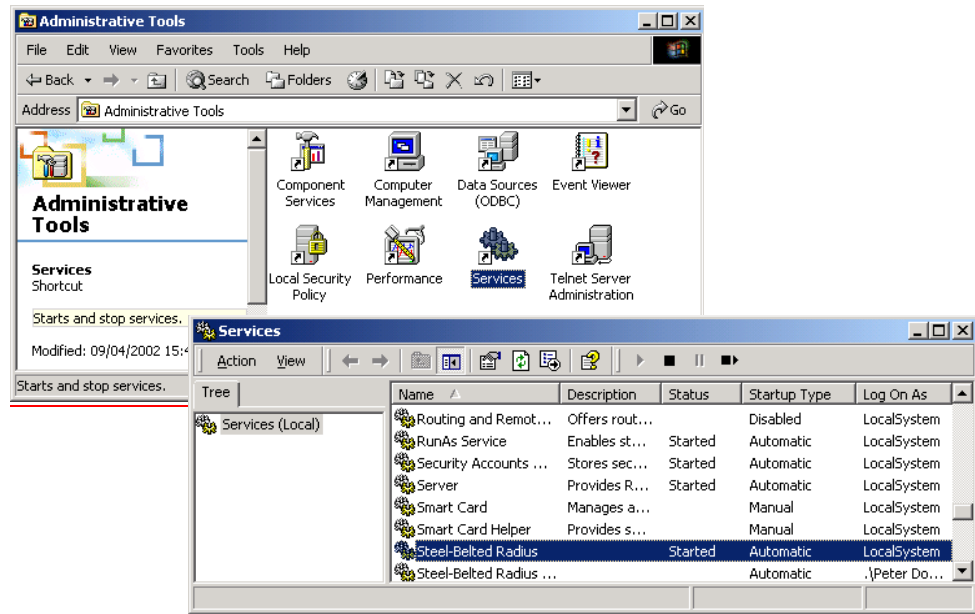
For troubleshooting, you can use the Event Viewer on both the workstation and the RADIUS server.

Configuring Funk RADIUS

3Com has successfully installed and tested Funk RADIUS running on a Windows server in a network with Switch 4500 deployed.

Download the Funk Steel-Belted RADIUS Server application from www.funk.com and install the application. Once installed you have a 30 day license to use it.

- 3 Either re-boot the server or stop then restart the RADIUS service. To stop and restart the Steel-Belted RADIUS service, go to *Control Panel > Administrative tools > Services*. Scroll down to the Steel-Belted service, stop and restart it.

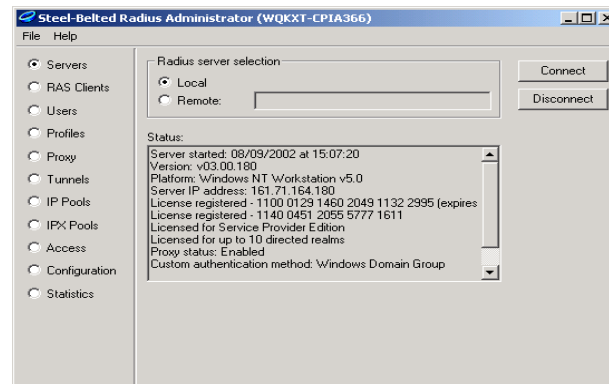


Funk RADIUS is now ready to run.



If you intend to use auto VLAN and QoS, you will need to create VLAN and QoS profiles on the 3Com Switch 4500 and follow the instructions in [Configuring Auto VLAN and QoS for Funk RADIUS](#).

- 4 Start the Funk RADIUS program, select *Servers* from the left hand list and select *Local Radius* server. Select *Connect* to start listening for clients.



- 5 To add a user, select *Users* from the left hand list, enter the *User name*, Set password and select *Add*.



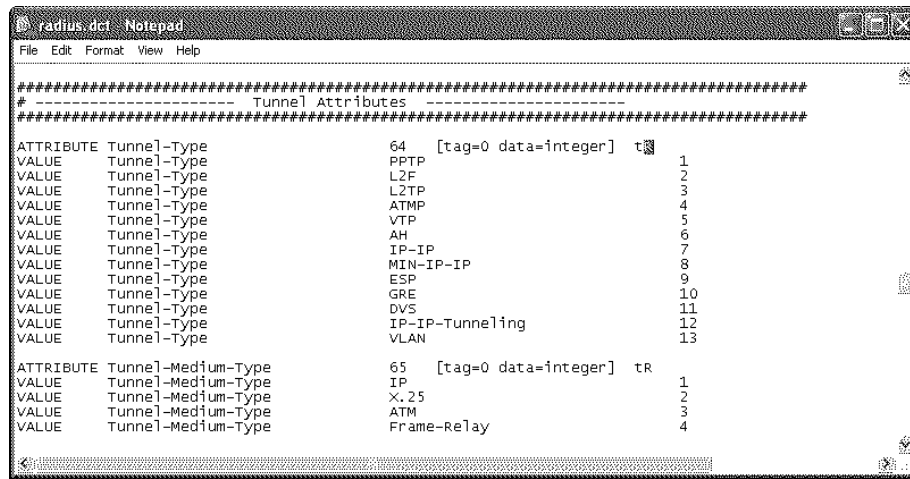
Passwords are case sensitive.

- 6 Enter the shared secret to encrypt the authentication data. The shared secret must be identical on the Switch 4500 and the RADIUS Server
 - a Select *RAS Clients* from the left hand list, enter a *Client name*, the *IP address* and the *Shared secret*.

Configuring Auto VLAN and QoS for Funk RADIUS

To set up auto VLAN and QoS using Funk RADIUS, follow these steps:

- 1 Edit the dictionary file `radius.dct` so that Return list attributes from the Funk RADIUS server are returned to the Switch 4500. The changes to make are:
 - a Add an **R** at the end of the correct attributes in the file, see example below. The attributes will now appear as potential Return list attributes for every user.



- 2 After saving the edited `radius.dct` file, stop and restart the Funk RADIUS service.
- 3 To use these return list attributes, they need to be assigned to a user or group. Create a new user and add the return list attributes shown in [Table 383](#) and [Table 385](#)

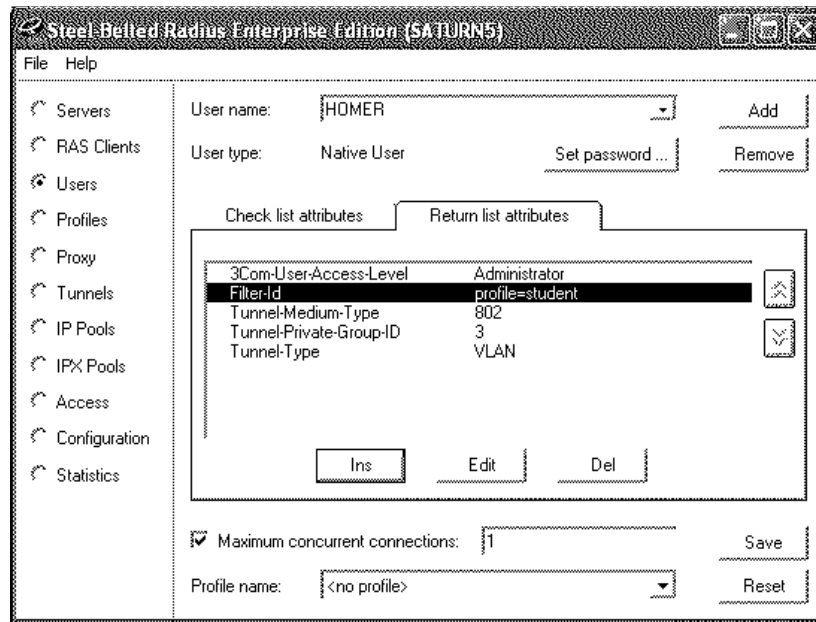
Table 383 Summary of auto VLAN attributes
Table 384

For Auto VLAN	Return String	Comment
Tunnel-Medium-type	802	
Tunnel-Private-Group-ID	2	VLAN value
Tunnel-Type	VLAN	

Table 385 Summary of QoS attributes
Table 386

For Auto QoS	Return String	Comment
Filter-id	profile=student	QoS Profile name

The following example shows the User name HOMER with the correct Return list Attributes inserted,



The VLANs and QoS profiles must also be created on the 3Com Switch 4500.

Configuring FreeRADIUS

3Com has successfully installed and tested FreeRADIUS running on Solaris 2.6 and RedHat Linux servers in networks with the Switch 4500 deployed.

Download FreeRADIUS source files from <http://www.freeradius.org> and install the application following the instructions from the website. The following instructions assume that you have installed a standard version of FreeRADIUS.

To configure FreeRADIUS as a RADIUS server for networks with the Switch 4500, follow these steps:

- 1 Add each Switch 4500 as a RADIUS client to the FreeRADIUS server
 - a Locate the existing file `clients.conf` in `/usr/local/etc/raddb`
 - b Add an entry in `clients.conf` for the Switch 4500 you wish to administer. For example:

```
client xxx.xxx.xxx.xxx {
    secret    = a-shared-secret
    shortname = a-short-name
}
```

Where `xxx.xxx.xxx.xxx` is the IP address of the 3Com Switch 4500.

- 2 Update the dictionary for Switch login
 - a In `/usr/local/etc/raddb` create a new file called `dictionary.3Com` containing the following information:

```
VENDOR      3Com                43
ATTRIBUTE   3Com-User-Access-Level 1          Integer 3Com
VALUE       3Com-User-Access-Level Monitor      1
VALUE       3Com-User-Access-Level Manager      2
VALUE       3Com-User-Access-Level Administrator 3
```

- b** Edit the existing file `dictionary` in `/usr/local/etc/raddb` to add the following line:

```
$INCLUDE dictionary.3Com
```

The new file `dictionary.3Com` will be used in configuring the FreeRADIUS server

- 3** Locate the existing file `users` in `/usr/local/etc/raddb` and for each user authorized to administer the Switch 4500:

- a** Add an entry for Switch Login. For example

```
user-name Auth-Type = System, 3Com-User-Access-Level = Administrator
```

This indicates that the server should return the 3Com vendor specific attribute `3Com-User-Access-Level` in the Access-Accept message for that user.

- b** Add an entry for Network Login. For example

```
user-name Auth-Type := Local, User-Password == "password"
```

- 4** Run the FreeRADIUS server with `radiusd`, to turn on debugging. so you can see any problems that may occur with the authentication:

```
cd /usr/local/sbin
./radiusd -sfxyz -l stdout
```

Setting Up Auto VLAN and QOS using FreeRADIUS

It is slightly more complex to set up auto VLAN and QoS using FreeRADIUS, as the dictionary file needs to be specially updated.

- 1** Update the `dictionary.tunnel` file with the following lines:

```
ATTRIBUTE Tunnel-Type          64 integerhas_tag
ATTRIBUTE Tunnel-Medium-Type   65 integerhas_tag
ATTRIBUTE Tunnel-Private-Group-Id 81 stringhas_tag
VALUE Tunnel-Type VLAN 13
VALUE Tunnel-Medium-Type TMT802 6
```

- 2** Locate the file `users` in `/usr/local/etc/raddb` and add the return list attributes to the user. For example:

```
bob Auth-Type := Local, User-Password == "bob"
    Tunnel-Medium-Type = TMT802,
    Tunnel-Private-Group-Id = 2,
    Tunnel-Type = VLAN,
    Filter-Id = "profile=student"
```



In the example above, Tunnel-Medium-Type has been set to TMT802, to force FreeRADIUS to treat 802 as a string requiring to be looked up in the dictionary and return integer 6, rather than return integer 802 which would be the case if Tunnel-Medium-Type was set to 802.

Setting Up the RADIUS Client

This section covers the following RADIUS clients:

- [Windows 2000 Built-in Client](#)
- [Windows XP Built-in Client](#)
- [Aegis Client Installation](#)

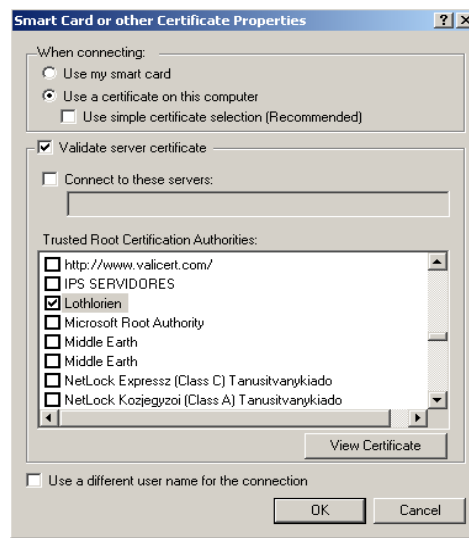
Windows 2000 Built-in Client

Windows 2000 requires Service Pack 3 and the IEEE 802.1X client patch for Windows 2000.

- 1 Downloaded the patches if required from:

<http://www.microsoft.com/Downloads/details.aspx?displaylang=en&FamilyID=6B78EDBE-D3CA-4880-929F-453C695B9637>

- 2 After the updates have been installed, start the *Wireless Authentication Service* in *Component Services* on the Windows 2000 workstation (set the service to startup type *Automatic*).
- 3 Open the *Network and Dial up* connections folder, right-click the desired Network Interface and select *Properties*.
- 4 Select the *Authentication* tab and check *Enable Network Access Control using IEEE 802.1X*
- 5 Set *Smart Card or Certificate* as *EAP type* and select the previously imported certificate as shown below.

**Windows XP Built-in Client**

The RADIUS client shipped with Windows XP has a security issue which affects the port authentication operation. If the RADIUS client is configured to use EAP-MD5, after a user logs-off, then the next user to log-on will remain authorized with the original user's credentials. This occurs because the Microsoft client does not generate an EAPOL-Logoff message when the user logs-off, which leaves the port authorized. To reduce the impact of this issue, decrease the "session-timeout" return list attribute to force re-authentication of the port more often. Alternatively, use a RADIUS client without this security flaw, for example the Aegis client



A patch for the Windows XP RADIUS client may be available from Microsoft since publishing this guide.

Aegis Client Installation

The Aegis Client is a standards-based implementation of IEEE 802.1X and supports many different encrypted algorithms such as MD5. It works on different Windows and Linux operating systems, such as Win XP, 2000, NT, 98, ME, Mac OSX. Details of the Aegis client can be found at <http://www.mtghouse.com/>

Follow these steps to install the Aegis client:

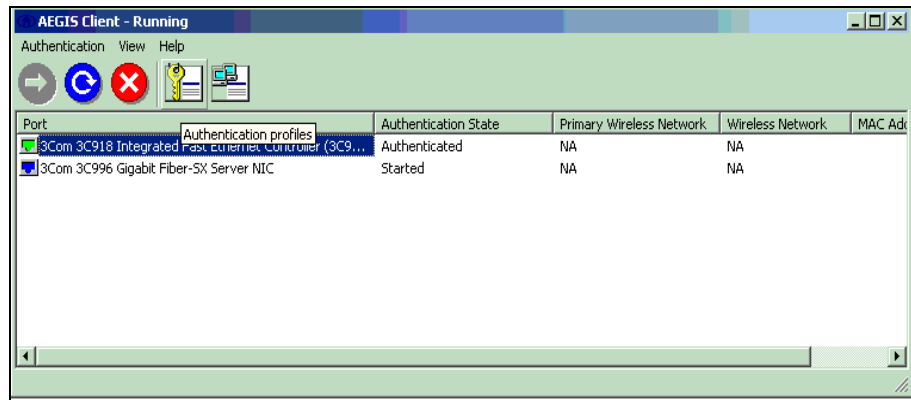
1 Registering the Aegis Client.

When using the Aegis client for the first time, a license key will be requested. To obtain a valid license key, complete an online form on the Meetinghouse website giving the System ID. A license key will then be sent via e-mail. The System ID can be found when running the Aegis Client application for the first time. To apply the license key:

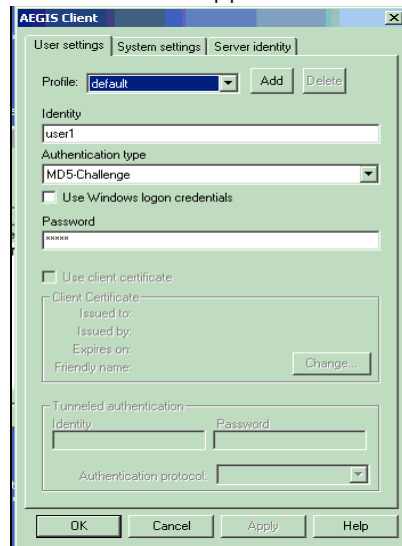
- a Run the Aegis Client software.
- b Go to *Aegis Client* > *Register* and select *Help* on the menu
- c Copy the License ID indicated at the bottom of the dialog box into the *License ID* field.
- d Copy the License Key provided in the email from Meetinghouse into the *License Key* field.
- e Press *OK*

2 Configuring the Aegis Client

- a Click the Key icon.

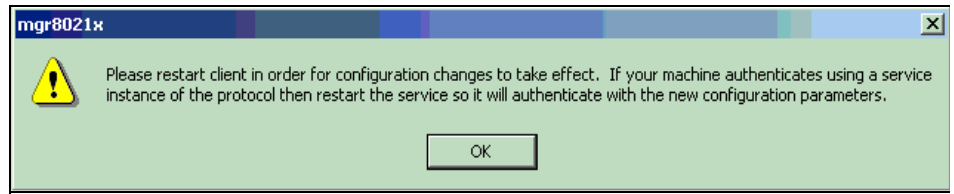


- b This screen will appear:



- c Leave the *Profile* as *default*. The *Identity* is an account created on the RADIUS Server with the *Password*.

- d Click *OK* to finish the configuration.
- e Restart the client either by rebooting, or stopping and re-starting the service.



- f Click the *OK* button, then return to the Aegis Client main interface. To restart the client, press the button with the red-cross. If authentication is successful, the icon will turn green.

C

AUTHENTICATING THE SWITCH 4500 WITH CISCO SECURE ACS

This appendix covers the following topics:

- [Cisco Secure ACS \(TACACS+\) and the 3Com Switch 4500](#)
- [Setting Up the Cisco Secure ACS \(TACACS+\) Server](#)

Cisco Secure ACS (TACACS+) and the 3Com Switch 4500

Cisco Secure ACS and TACACS+ are proprietary protocols and software created by Cisco, they provide similar functionality to a RADIUS server. Enterprises which contain a Cisco Secure ACS server with TACACS+ to provide centralized control over network and management access, can also deploy the 3Com Switch 4500 on their network.

Although 3Com does not directly support the proprietary TACACS+ protocol, 3Com Switches can still be authenticated in networks which use TACACS+ and Cisco Secure ACS. The windows based Cisco Secure ACS server contains a built-in RADIUS server. This RADIUS server integrates seamlessly with the TACACS database allowing 3Com Switches to authenticate correctly using the RADIUS protocol. Users that already exist on the TACACS+ server can be authorized using the TACACS+ or RADIUS server, an optional VLAN and QoS profile can be applied to the user. Network administrators can also be authorized using the built in RADIUS server, providing centralized access to 3Com Switches.

The remainder of this appendix describes how to setup Cisco Secure ACS (v3.3) to operate using RADIUS with a 3Com Switch.

Setting Up the Cisco Secure ACS (TACACS+) Server

Configure the Cisco Secure ACS server through the web interface. Log into the web interface from any PC or localhost of the server, using port 2002 . For example:

`http://TACACS-server:2002`

The following sections detail the steps required to configure the Cisco Secure ACS (TACACS+) server to authenticate a Switch 4500 on your network and allow any additional users to login to the network:

- [Adding a 3Com Switch 4500 as a RADIUS Client](#)
- [Adding a User for Network Login](#)

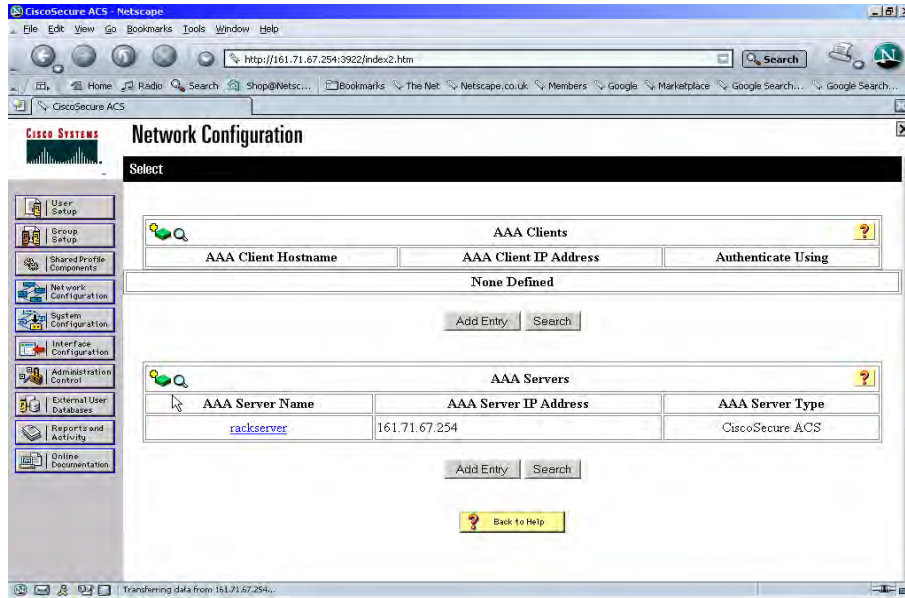
The final section details how to add a User (Network Administrator) for Switch Login to enable centralized management of the Switch through the Cisco Secure ACS server.

- [Adding a User for Switch Login](#)

Adding a 3Com Switch 4500 as a RADIUS Client

Once logged into the Cisco Secure ACS interface, follow these steps:

- 1 Select *Network Configuration* from the left hand side

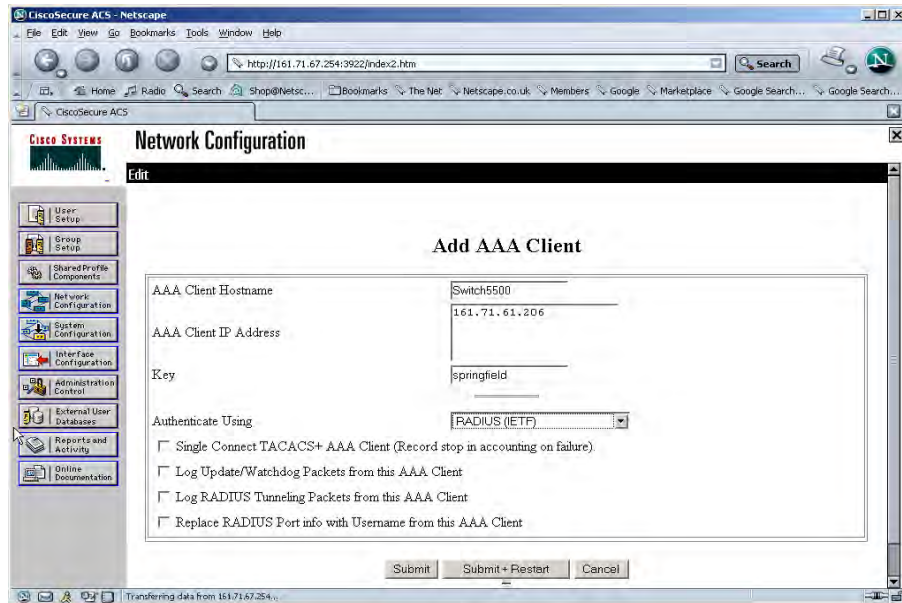


- 2 Select *Add Entry* from under AAA Clients.
- 3 Enter the details of the 3Com Switch.



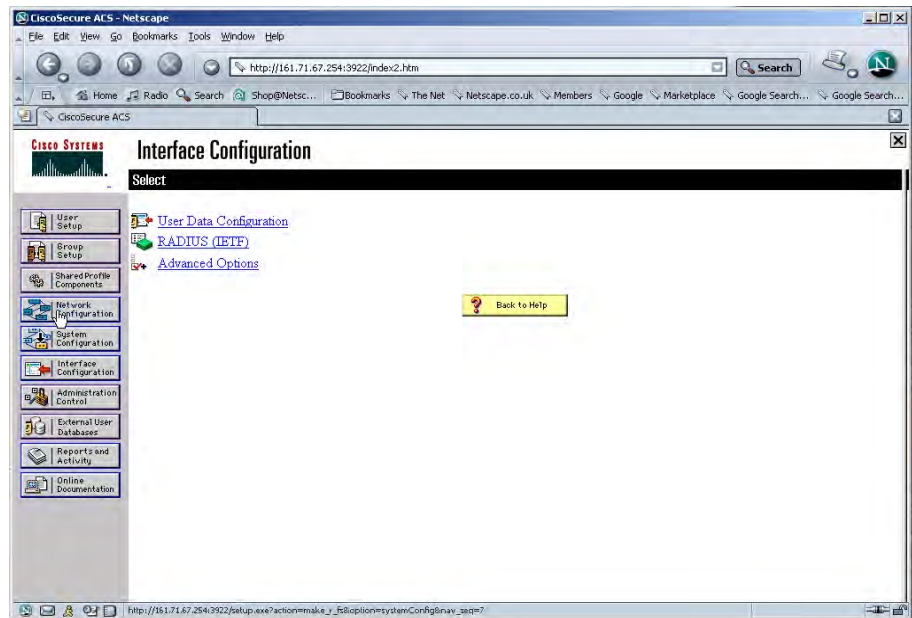
Spaces are not permitted in the AAA Client Host name.

An example is shown below



- 4 Select *Submit*. Do not restart the ACS server at this stage

5 Select *Interface Configuration* from the left hand side.

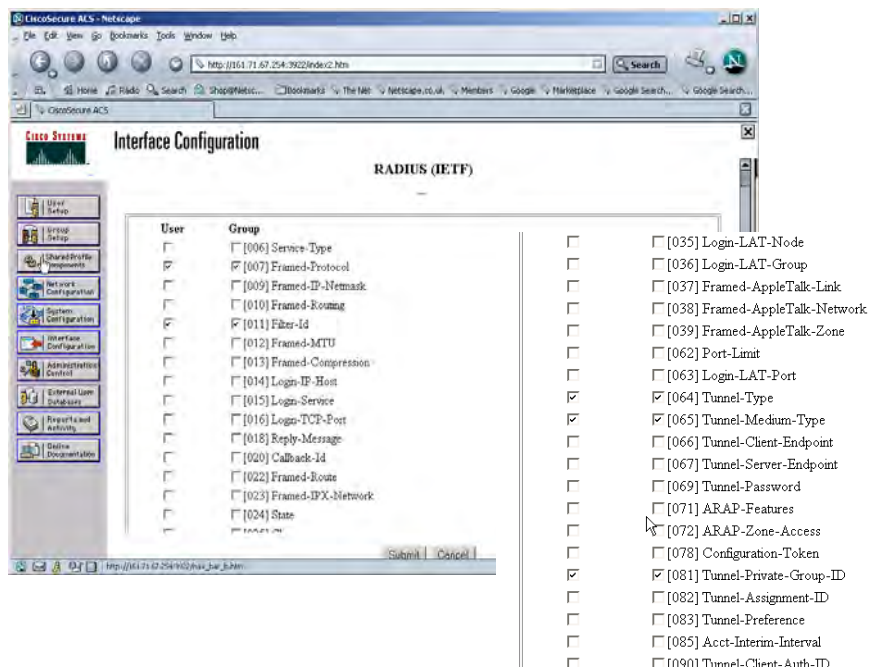


6 Select *RADIUS (IETF)* from the list under *Interface Configuration*.

7 Check the RADIUS attributes that you wish to install.

If you want to use auto VLAN and QoS, ensure that you have the following options selected for both the User and Group:

- Filter-ID
- Tunnel-Type
- Tunnel-Medium-Type
- Tunnel-Private-Group-ID



- 8 Select *Submit*.
- 9 Repeat steps 1 to 8 for each Switch 4500 on your network. When all of the Switch 4500s have been added as clients to the Cisco Secure ACS server, restart the Secure ACS server by selecting *System Configuration* from the left hand side, then select *Service Control* and click *Restart*.

Adding a User for Network Login

Existing users on a network with a Secure ACS server can be authorized using the TACACS+ or RADIUS server. New users connected through a Switch 4500 to the network need to be authorized via the RADIUS server. An optional VLAN and QoS profile can be applied to the user.

Follow these steps to add a user for Network Login.

- 1 Select *User Setup* from the left hand side
- 2 Enter the username, and select *Add/edit*
- 3 Enter the user information, scroll down to complete the user profile, including specific RADIUS attributes if required.

The screenshot shows the Cisco Secure ACS web interface in a Netscape browser window. The browser title is "CiscoSecure ACS - Netscape" and the address bar shows "http://161.71.67.254:3922/index2.htm". The page title is "User Setup". On the left side, there is a navigation menu with the following items: User Setup (selected), Group Setup, Shared Profile Components, Network Configuration, System Configuration, Interface Configuration, Administration Control, External User Databases, Reports and Activity, and Online Documentation. The main content area is divided into two sections: "Supplementary User Info" and "User Setup".

Supplementary User Info

Real Name	Anne Brown
Description	Accounts Payable

User Setup

Password Authentication:

CiscoSecure Database (selected)

CiscoSecure PAP (Also used for CHAP/MS-CHAP/ARAP, if the Separate field is not checked.)

Password: [text input]

Confirm Password: [text input]

Separate (CHAP/MS-CHAP/ARAP)

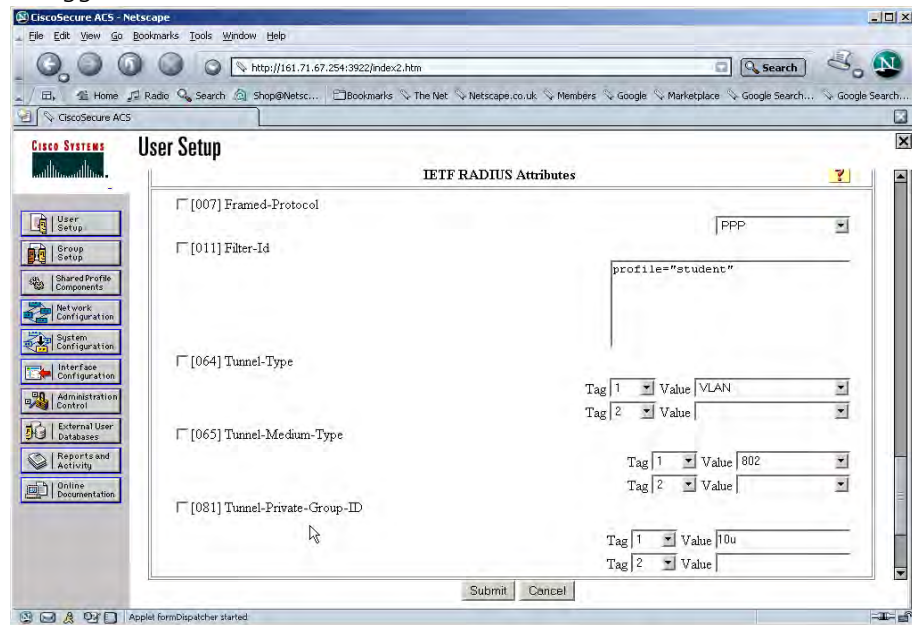
Password: [text input]

Confirm Password: [text input]

When a token server is used for authentication, supplying a separate CHAP password for a token card user allows CHAP authentication. This is especially useful when token caching is enabled.

Submit Cancel

The screen below shows specific RADIUS attributes having been selected for the user. The user has the student profile selected and is assigned to VLAN 10 untagged.



The RADIUS attributes need to have already been selected, see [step 7 in Adding a 3Com Switch 4500 as a RADIUS Client](#).

The User can now access the network through Network Login.

Adding a User for Switch Login

Adding a user for switch login is slightly more complex, as 3Com specific RADIUS attributes need to be returned to the 3Com Switch 4500. These RADIUS attributes define the access level of the user to the management interface.

Follow these steps:

- 1 Add the required RADIUS attributes to the Cisco Secure ACS server, by editing an .ini file and compiling it into the Secure ACS RADIUS server using an application called `csutil.exe`.

For example:

- a Create 3Com.ini file with the following contents:

```
[User Defined Vendor]
Name=3Com
IETF Code=43
VSA 1=3Com-User-Access-Level

[ 3Com-User-Access-Level ]
Type=INTEGER
Profile=OUT
Enums=3Com-User-Access-Level-Values

[ 3Com-User-Access-Level-Values ]
1=Monitor
2=Manager
```

3=Administrator

- b** Locate the application `csutil.exe` in the utils directory of the install path (for example, `C:\program files\Cisco Secure ACS\utils\`).
- c** Copy the `3Com.ini` file into the utils directory
- d** At the command prompt enter

```
csutil -addUDV 0 3Com.ini
```

```

C:\WINNT\system32\cmd.exe
Creating backup of current config
Vendor [RADIUS (3Com Limited)] deleted
Checking new configuration...
New configuration OK
Re-starting any stopped services

C:\Program Files\CiscoSecure ACS v3.3\Utils>csutil -addUDV 0 3com.ini
CSUtil v3.3(1.16), Copyright 1997-2004, Cisco Systems Inc

Adding or removing vendors requires ACS services to be re-started.
Please make sure regedit is not running as it can prevent registry
backup/restore operations

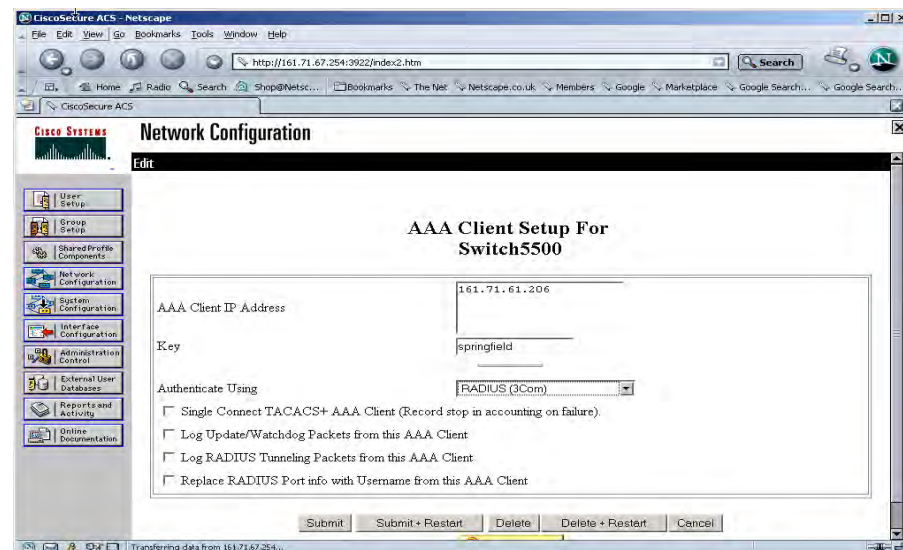
Are you sure you want to proceed? (Y or N)y
Parsing [L.3com.ini] for addition at UDV slot [0]
Stopping any running services
Creating backup of current config
Adding Vendor [3Com] added as [RADIUS (3Com)]
Adding USA [3Com-User-Access-Level]
Done
Checking new configuration...
New configuration OK
Re-starting stopped services

C:\Program Files\CiscoSecure ACS v3.3\Utils>

```

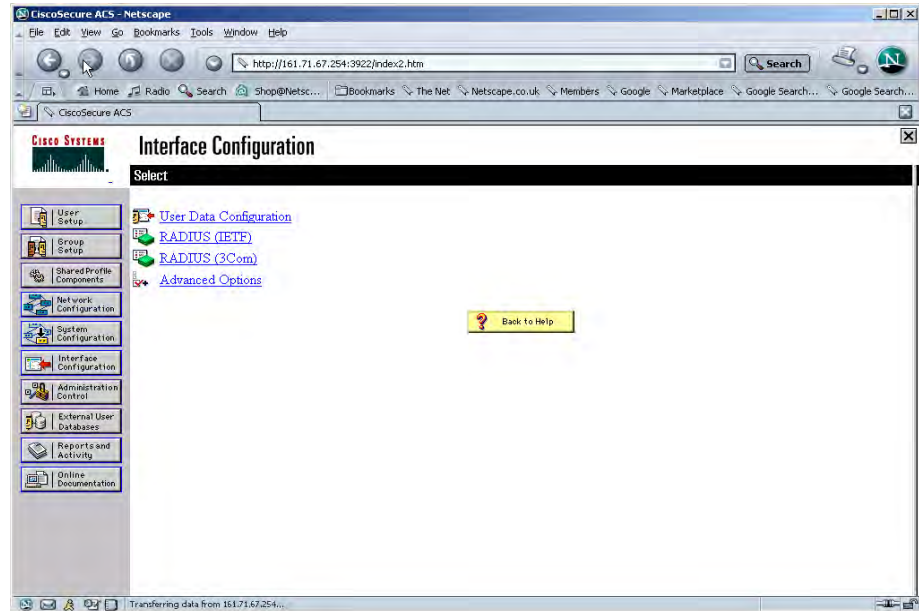
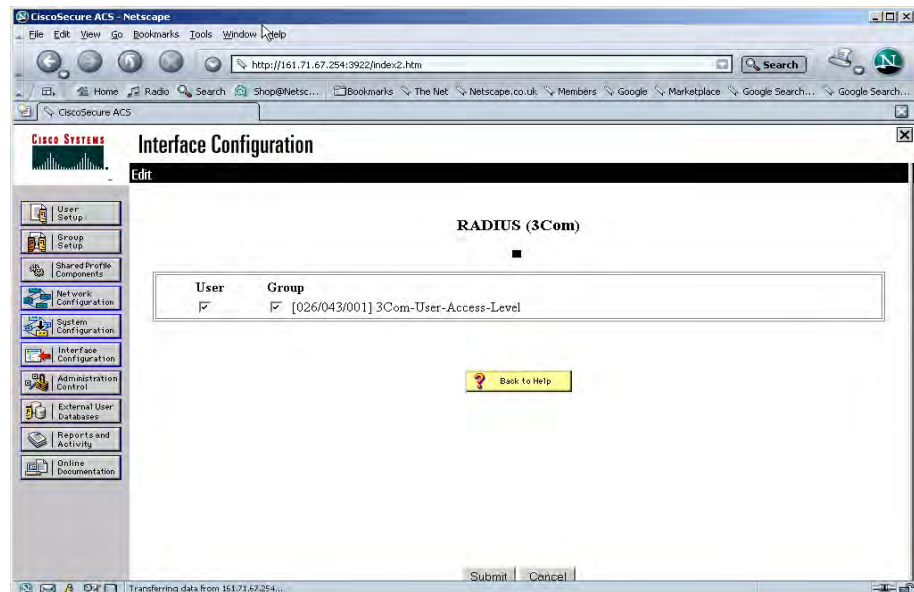
This will stop the Cisco Secure ACS server, add the RADIUS information (by adding the contents of `3Com.ini` to UDV (User Defined Vendor) slot 0), and then restart the server. Once complete, log into the Secure ACS server again and complete steps 2 and 3.

- 2** To use the new RADIUS attributes, a client needs to be a user of RADIUS (3Com) attributes. Select *Network Configuration* from the left hand side and select an existing device or add a new device. In the *AAA Client Setup* window select *RADIUS (3COM)* from the *Authenticate Using* pull down list. .

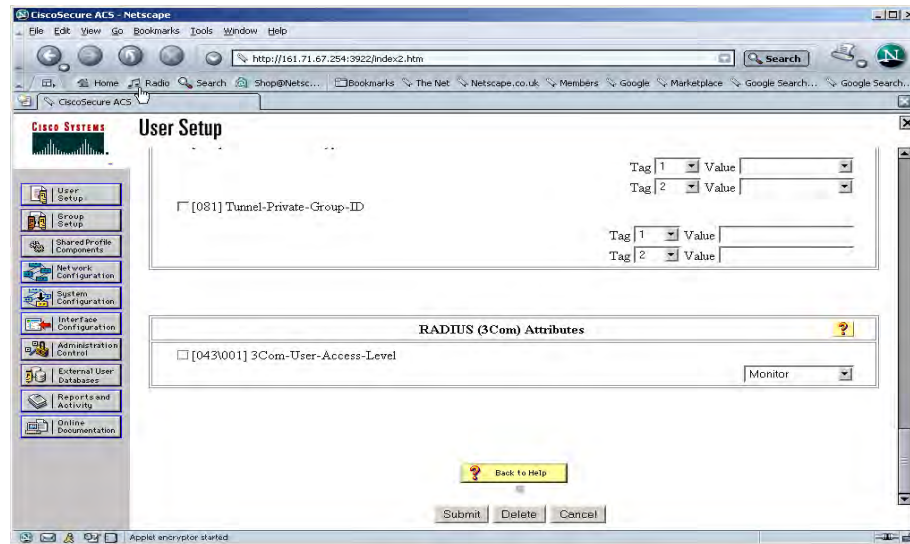


3 Select *Submit+Restart*

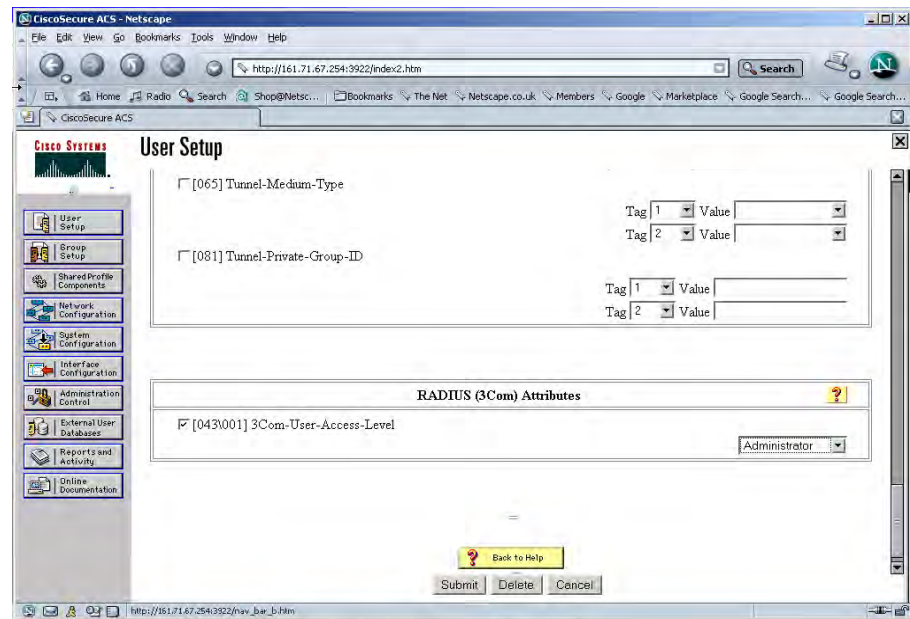
The IETF attributes will still be available to the device, the 3Com attributes are simply appended to them.

4 Select *Interface Configuration*, followed by *RADIUS (3Com)*a Ensure that the *3Com-User-Access-Level* option is selected for both *User* and *Group* setup, as shown below5 Select *User Setup* and either modify the attributes of an existing user (select *Find* to display the User List in the right hand window) or *Add* a new user (see [Adding a User for Network Login](#)). Set the user's access level to the 3Com Switch 4500 by

scrolling to the bottom of the user profile where there should be the option for configuring the access level as shown below:



- 6 In the *RADIUS (3Com) Attribute* box, check *3Com-User-Access-Level* and select *Administrator* from the pull down list, see below:



- 7 Select *Submit*.

The Switch 4500 can now be managed by the Network Administrator through the CISCO Secure ACS server.