SuperStack® 4 Switch 5500G-EI Family
Configuration Guide

http://www.3com.com/
Part number: DUA1725-0BAA02
Published: August 2005

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

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

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

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

UNITED STATES GOVERNMENT LEGEND

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

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

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

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

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.

ABOUT THIS GUIDE

This guide provides information about configuring your network using the commands supported on the 3Com® SuperStack® 4 Switch 5500G-EI.

Organization of the Manual

The Switch 5500G-EI Configuration Guide consists of the following chapters:

- **Getting Started** — Details the main features and configurations of the Switch 5500G-EI.
- **Port Operation** — Details how to configure Ethernet port and link aggregation.
- **VLAN Operation** — Details how to configure VLANs.
- **Power over Ethernet (PoE) Configuration** — Details how to configure PoE.
- **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.
- **XRN Fabric** — Details how to configure an XRN fabric.
- **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 manual is intended for the following readers:

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

Conventions

This manual uses the following conventions:

Table 1 Icons

Icon	Notice Type	Description
ℹ	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 *Return* or *Enter* 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 *Return* or *Enter* 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 I y I ... }	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 Manuals

The *3Com SuperStack 4 Switch 5500G-EI Getting Started Guide* provides information about installation.

The *3Com SuperStack 4 Switch 5500G-EI 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
- XRN Overview
- Product Features
- Logging in to the Switch
- Command Line Interface
- User Interface Configuration

Product Overview

The Switch 5500G-EI Family are wire speed Layer 3 switching products supporting expandable resilient networking (XRN). Besides saving user cost otherwise invested on module rack-type switches, the Switch 5500G-EI family with XRN also offer excellent network availability, upgrade ability, performance, and power network control capacity.

The Switch 5500G-EI family includes the following Switches:

- Switch 5500G-EI 24 Port — the Switch has an AC/DC dual input 130W power PSU. The rear panel has two fixed fabric ports and one expansion module slot that is compatible with the following modules:
  - 8 Port 1000 Mbps SFP Module
  - 1 Port 10 Gbps XENPAK Module

  The front panel has 24 x 10/100/1000Base-T auto-negotiation ethernet ports with RJ-45 connectors and 4 SFP combo ports. Each combo port corresponds to an ethernet port, so there are 4 port pairs. Only 1 port in a pair can be used at the same time. For details of the relationship between combo and ethernet ports please refer to Table 3.
- Switch 5500G-EI 24 Port PWR — the Switch has a PoE power PSU. The rear panel has two fixed fabric ports and one expansion module slot that is compatible with the following modules:
  - 8 Port 1000 Mbps SFP Module
  - 1 Port 10 Gbps XENPAK Module

  The front panel has 24 x 10/100/1000Base-T auto-negotiation ethernet ports with RJ-45 connectors and 4 SFP combo ports. Each combo port corresponds to an ethernet port, so there are 4 port pairs. Only 1 port in a pair can be used at the same time.
- Switch 5500G-EI 48 Port — the Switch has an AC/DC 180W power PSU. The rear panel has two fixed fabric ports and one expansion module slot that is compatible with the following modules:

  - 8 Port 1000 Mbps SFP Module
  - 1 Port 10 Gbps XENPAK Module

  The front panel has 48 x 10/100/1000Base-T auto-negotiation ethernet ports with RJ-45 connectors and 4 SFP combo ports. Each combo port corresponds to an ethernet port, so there are 4 port pairs. Only 1 port in a pair can be used at the same time.

- Switch 5500G-EI 48 Port PWR — the Switch has a PoE power PSU. The rear panel has two fixed fabric ports and one expansion module slot that is compatible with the following modules:
  - 8 Port 1000 Mbps SFP Module
  - 1 Port 10 Gbps XENPAK Module

  The front panel has 48 x 10/100/1000Base-T auto-negotiation ethernet ports with RJ-45 connectors and 4 SFP combo ports. Each combo port corresponds to an ethernet port, so there are 4 port pairs. Only 1 port in a pair can be used at the same time.

- Switch 5500G-EI SFP 24 Port — the Switch has an AC/DC dual input 130W power PSU. The rear panel has two fixed fabric ports and one expansion module slot that is compatible with the following modules:
  - 8 Port 1000 Mbps SFP Module
  - 1 Port 10 Gbps XENPAK Module

  The front panel has 24 x 1000Base-X SFP ports and 4 10/100/1000Base-T auto-negotiation ethernet ports with RJ-45 connectors.

Table 3 Combo Ports

Switch Model	Combo Port	Corresponding Port
Switch 5500G-EI 24 Port/ Switch 5500G-EI 24 Port PWR	25	22
	26	24
	27	21
	28	23
Switch 5500G-EI 48 Port/ Switch 5500G-Ei 48 Port PWR	49	46
	50	48
	51	45
	52	47

The Switch 5500G-EI 24 Port PWR and Switch 5500G-EI 48 Port PWR are capable of supplying -48 VDC power to remote power devices. These switches use a power over ethernet module to provide DC power to powered devices. When delivering the AC input, the module can supply up to 300W. If more power is needed, you can use the DC input or both AC and DC inputs to ensure that all connected devices can operate.

The Switch 5500G-EI 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.

XRN Overview

Brief Introduction

With the XRN (eXpandable Resilient Networking) feature, you can connect several devices into a combined device and manage them as a single unit. The combined device is called the Fabric, while the member devices are units. With XRN you can:

- Manage multiple devices in centralized manner, with low management cost.
- Extend the number of ports and switching capacity just by adding devices. You can decide which equipment to purchase as needed, and better protect your existing investment while upgrading the network.
- Provide backup between multiple devices to improve reliability and to eliminate single points of failure.

Major Technologies

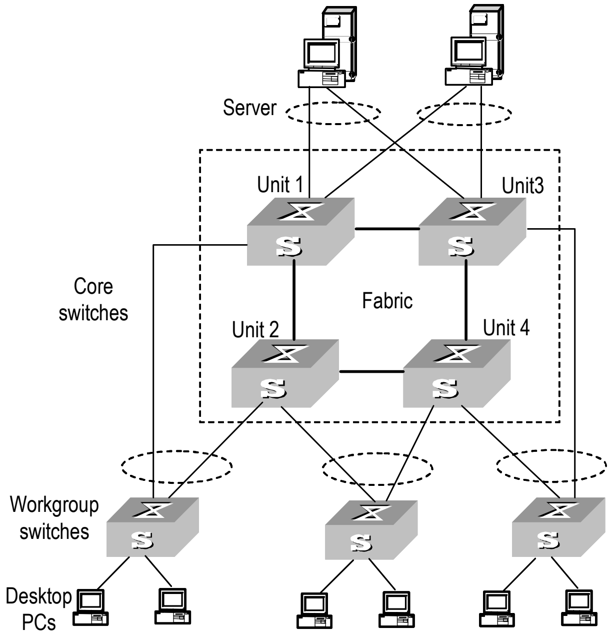
XRN includes three technologies: distributed device management (DDM), distributed link aggregation (DLA), and distributed resilient route (DRR).

- DDM: Users can treat the Fabric as a single device. They can manage the Fabric through any port or IP address connected into the Fabric, and from any unit in the fabric.
- DRR: The multiple units of a Fabric route and forward packets as a single unit, and provide uniform VLAN interfaces, routing table and L3 forwarding table, so the Fabric is regarded as a single Layer 3 switch. Failure of one of the units will not affect routing protocol and data forwarding.
- DLA: Users can aggregate multiple ports of several different units in a Fabric into a group, for centralized management within the Fabric. Trans-unit link aggregation can bring convenient aggregation setting and effectively reduce single points of failure.

Typical Networking Topology

Typical XRN networking topology is as shown in Figure 1. Switches of the same type (that is, units) form a Fabric. As a core switch, the Fabric can be downlinked to workgroup switches through several aggregation links, and uplinked to the server group also through several aggregation links.

Figure 1 Networking Topology with XRN



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
	Voice 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
	Internet Group Management Protocol (IGMP)
	Protocol-Independent Multicast-Dense Mode (PIM-DM) Protocol-Independent Multicast-Sparse Mode (PIM-SM)
IP routing	Static route
	RIP V1/v2
	OSPF
	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

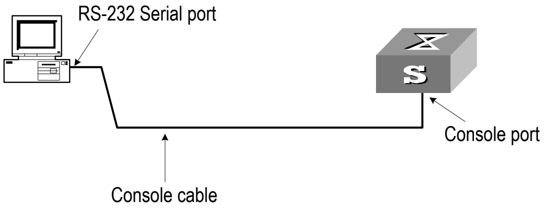
Features	Description
Security features	Multi-level user management and password protect
	802.1X authentication
	Packet filtering
Quality of Service (QoS)	Traffic classification
	Bandwidth control
	Priority
	Queues of different priority on the port
	Queue scheduling: supports Strict Priority Queuing (SP), Weighted Round Robin (WRR), WFQ, SP+WFQ, and SP+WRR
	QoS profile management manner
Management and Maintenance	Command line interface configuration
	Configuration through console port
	Remote configuration through Telnet or SSH
	Configuration through dialing the Modem
	SNMP
	System log
	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).

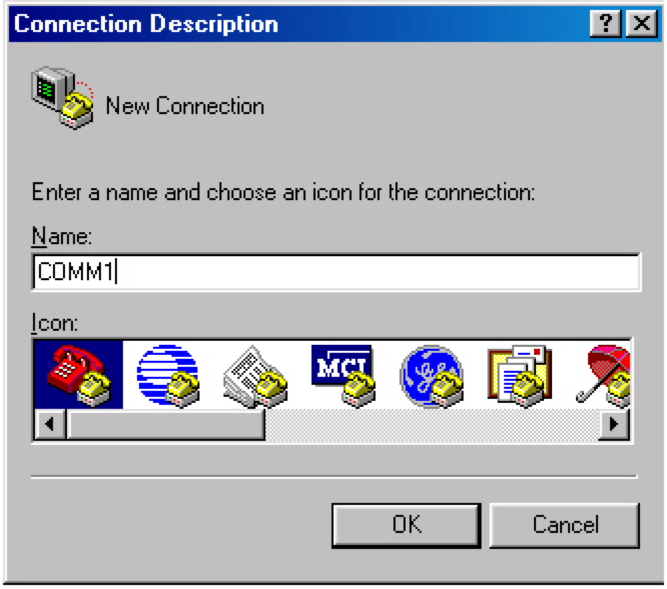
Figure 2 Setting up the Local Configuration Environment through the Console Port



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 = 9600
- Databit = 8
- Parity check = none
- Stopbit = 1
- Flow control = none
- Terminal type = VT100

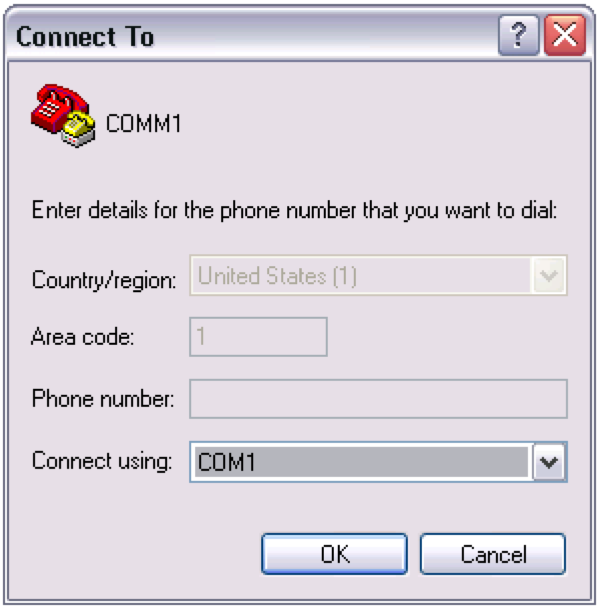
Figure 3 Setting up a New Connection



Enter a name and choose an icon for the connection:

Name: COMM1

Figure 4 Configuring the Port for Connection



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

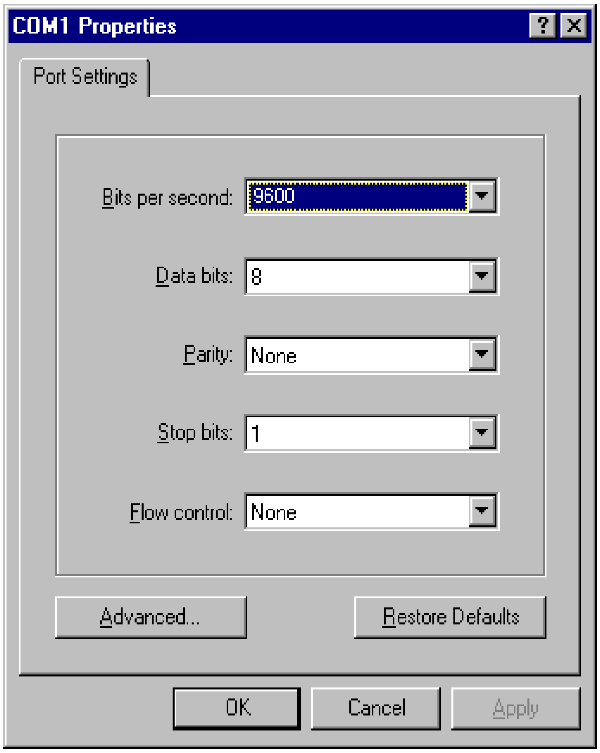
Country/region: United States (1)

Area code: 1

Phone number:

Connect using: COM1

Figure 5 Setting Communication Parameters



Bits per second: 9600
Data bits: 8
Parity: None
Stop bits: 1
Flow control: None

3 The Switch is powered on and it displays self-test information. Press < Enter> to show the command line prompt such as `<SW5500>`.

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.

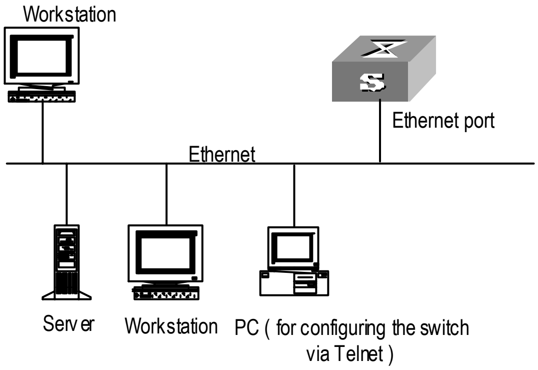
1 Authenticate the Telnet user through the console port before the user logs in by Telnet.

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!`.

```
<SW5500>system-view
[SW5500]user-interface vty 0
[SW5500-ui-vty0]set authentication password simple xxxx (xxxx is the
preset login password of the Telnet user)
```

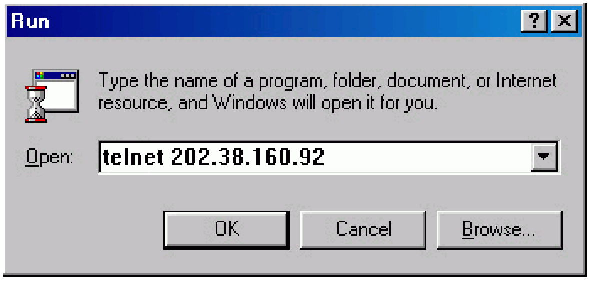
2 To set up the configuration environment, connect the network port of the PC to a port on the Switch through the LAN.

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


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

Open: telnet 202.38.160.92

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 `<SW5500>`). 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 SW5500 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.

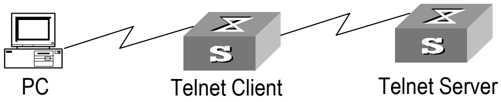
By default, when a Telnet user passes the password authentication to log on to the Switch, the access level for commands will be Level 0.

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 .

```
<SW5500> system-view
[SW5500] user-interface vty 0
[SW5500-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 "Connecting a PC to the Switch through Telnet" on page 26.
3. Perform the following on the Telnet Client:

```
<SW5500> 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 `<SW5500>`. 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 it 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 the prompt `Login password has not been set!.`

```
<SW5500>system-view
[SW5500]user-interface aux 0
```

`[SW5500-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
```

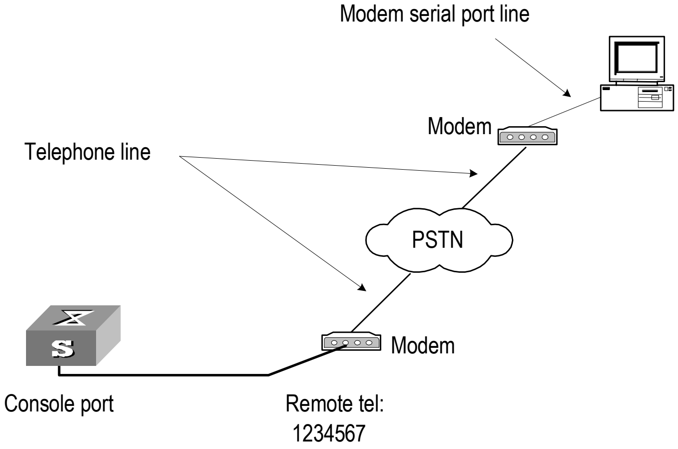
After the configuration, enter **`AT&V`** to verify the Modem settings.

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

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

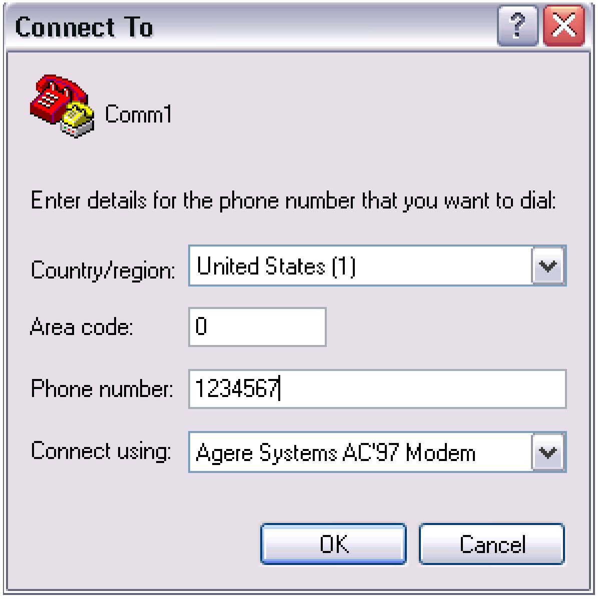
3 To set up the remote configuration environment, connect the Modems to a PC (or a terminal) serial port and the Switch console port respectively (see Figure 9).

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



Connect To

Comm1

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

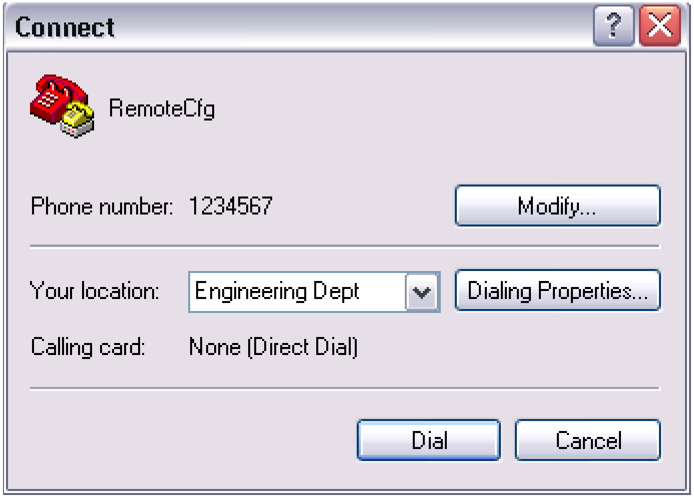
Country/region: United States (1)

Area code: 0

Phone number: 1234567

Connect using: Agere Systems AC'97 Modem

Figure 11 Dialing on the Remote PC



Connect

RemoteCfg

Phone number: 1234567

Your location: Engineering Dept

Calling card: None (Direct Dial)

5 Enter the preset login password on the remote terminal emulator and wait for the prompt `<SW5500>`. 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

Command Line Interface

The Switch 5500G-EI family provide 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 5500G-EI 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 5500G-EI 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
- PIM View
- RIP View
- OSPF View
- OSPF Area 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	<SW5500>	This is the view you are in after connecting to the Switch	**quit** disconnects to the Switch
System View	Configure system parameters	[SW5500]	Enter **system-view** in User View	**quit** or **return** returns to User View
Ethernet Port View	Configure Ethernet port parameters	[SW5500-Ethernet1/0/1]	100M Ethernet Port View: Enter **interface ethernet 1/0/1** in System View	**quit** returns to System View **return** returns to User View
		[SW5500-GigabitEthernet1/0/24]	GigabitEthernet Port View: Enter **interface gigabitethernet 1/0/24** in System View	
VLAN View	Configure VLAN parameters	[SW5500-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	[SW5500-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	[SW5500-luser-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	[SW5500-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	[SW5500-ftp]	Enter **ftp** in User View	**quit** returns to System View
RSA Public Key View	Configure RSA public key of SSH user	[SW5500-rsa-public-key]	Enter **rsa peer-public-key SW5500003** in System View	**peer-public-key end** returns to System View
RSA Key Code View	Edit RSA public key of SSH user	[SW5500-rsa-key-code]	Enter **public-key-code begin** in RSA Public Key View	**public-key-code end** returns to RSA Public Key View
PIM View	Configure PIM parameters	[SW5500-PIM]	Enter **pim** 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
RIP View	Configure RIP parameters	`[SW5500-rip]`	Enter **rip** in System View	**quit** returns to System View **return** returns to User View
OSPF View	Configure OSPF parameters	`[SW5500-ospf]`	Enter **ospf** in System View	**quit** returns to System View **return** returns to User View
OSPF Area View	Configure OSPF area parameters	`[SW5500-ospf-0.0.0.1]`	Enter **area 1** in OSPF View	**quit** returns to OSPF View **return** returns to User View
Route Policy View	Configure route policy parameters	`[SW5500-route-policy]`	Enter **route-policy policy1 permit node 10** in System View	**quit** returns to System View **return** returns to User View
Basic ACL View	Define the rule of basic ACL	`[SW5500-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	`[SW5500-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	`[SW5500-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	`[SW5500-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	`[SW5500-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	`[SW5500-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	`[SW5500-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.

```
[5500]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.

```
<SW5500>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.

```
<SW5500>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 <Ctrl+C> 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 <Enter> 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 and 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`	■ 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 5500 Family supports 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 SW5500 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	**user-interface** [type] first-number [last-number]

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	**protocol inbound** { **all** | **ssh** | **telnet** }

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	**speed** *speed_value*
Restore the default transmission speed on the AUX (console) port	**undo speed**

By default, the transmission speed on the AUX (console) port is 9600bps.

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	**flow-control { hardware** | **none** | **software }**
Restore the default flow control mode on the AUX (console) port	**undo flow-control**

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	**parity** { **even** | **mark** | **none** | **odd** | **space** }
Restore the default parity mode	**undo parity**

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	**stopbits** { **1** | **1.5** | **2** }
Restore the default stop bit of the AUX (console) port	**undo stopbits**

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	**databits** { **7** | **8** }
Restore the default data bit of the AUX (console) port	**undo databits**

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`** *`minutes`* `[` *`seconds`* `]`
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`** *`screen_length`*
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`** *`value`*
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.

```
[SW5500]user-interface vty 0
[SW5500-ui-vty0]authentication-mode password
[SW5500-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.

```
[SW5500-ui-vty0]authentication-mode scheme
[SW5500-ui-vty0]quit
[SW5500]local-user zbr
[SW5500-luser-zbr]password simple 3Com
[SW5500-luser-zbr]service-type telnet
```

3 No authentication

```
[SW5500-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	**undo service-type** { **ftp** [**ftp-directory**] **lan-access** | { **ssh** | **telnet** | **terminal** }* }

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	**user privilege level** *level*
Restore the default command level used after a user logs in from a user interface	**undo user privilege level**

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.	**command-privilege level** *level* **view** *view command*
Restore the default command level in a specified view.	**command-privilege view** *view command*

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** | *number* | *type number* }

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** *text*
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.

```
[SW5500-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** [*type*] *number*

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**]

2 PORT OPERATION

This chapter covers the following topics:

- Ethernet Port Configuration
- Link Aggregation Configuration

Ethernet Port Configuration

Ethernet Port Overview

The Switch 5500G-EI 24 Port provides 24 fixed 10/100/1000Base-T Ethernet ports, 4 combo SFP ports, 2 fixed stack ports and one expansion slot. The expansion slot can accomodate the 8 port SFP module, 1 port 10G module or 2 port 10G module.

The Switch 5500G-EI 48 Port provides 48 fixed 10/100/1000Base-T Ethernet ports, 4 combo SFP ports, 2 fixed stack ports and one expansion slot. The expansion slot can accomodate the 8 port SFP module, 1 port 10G module or 2 port 10G module.

The Switch 5500G-EI SFP 24 Port provides 24 1000BASE-X SFP ports and 4 10/100/1000Base-T auto-negotiation ethernet ports with RJ-45 connectors, 2 fixed stack ports and one expansion slot. The expansion slot can accomodate the 8 port SFP module, 1 port 10G module or 2 port 10G module.

The following features are found in the Ethernet ports of the Switch 5500G-EI

- 10/100/1000BASE-T Ethernet ports support MDI/MDI-X auto-sensing. They can operate in 1000Mbps full-duplex, 100Mbps half-duplex/full-duplex and 10Mbps half-duplex/full-duplex.
- 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).
- 10Gigabit Ethernet port operates in 10000Mbps full-duplex mode. The duplex mode can be set to **full** (full-duplex) and **auto** (auto-negotiation) and its speed can be set to **10000** (10000Mbps) 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
- Permitting/Forbidding Jumbo Frames to Pass through an 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** { *interface_type interface_num* | *interface_name* }

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** *text*

Table 32 Setting the Description Character String for the Ethernet Port

Operation	Command
Delete the description character string of Ethernet.	**`undo description`**

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

The cascade ports do not support the **`undo description`** command.

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 the 10/100/1000BASE-T port can operate in full duplex, half duplex or auto-negotiation mode. When the port operates at 1000Mbps, the duplex mode can be set to **full** (full duplex) or **auto** (auto-negotiation). The Gigabit ports and 10G port support full duplex mode 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`** | **10000** | **`auto`** }
Restore the default speed for the Ethernet port	**`undo speed`**

Note that the 10/100/1000BASE-T ports, excluding the combo ports, can operate at 10Mbps, 100Mbps or 1000Mbps as per different requirements. However, in half duplex mode, the port cannot operate at 1000Mbps. The Gigabit Ethernet port supports 1000Mbps and can be configured to operate at **1000** (1000Mbps) and **auto** (auto-negotiation).

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.

Permitting/Forbidding Jumbo Frames to Pass through an Ethernet Port

An Ethernet port may encounter jumbo frames exceeding the standard frame length, when switching large throughput data like transmitting files. This command can forbid or permit jumbo frames to pass through an Ethernet port.

Perform the following configuration in Ethernet Port View.

Table 37 Permitting/Forbidding Jumbo Frame to Pass through the Ethernet Port

Operation	Command
Permit jumbo frame to pass through the Ethernet port	**jumboframe enable**
Forbid jumbo frame to pass through the Ethernet port	**undo jumboframe enable**

By default, jumbo frames with lengths between 1518 bytes and 9216 bytes inclusive are permitted to pass through an Ethernet port.

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 38 Setting the Ethernet Port Suppression Ratio

Operation	Command
Set Ethernet port broadcast suppression ratio	**broadcast-suppression** { *ratio* | **pps** }
Restore the default Ethernet port broadcast suppression ratio	**undo broadcast-suppression**
Set Ethernet port multicast suppression ratio	**multicast-suppression** { *ratio* | **pps** }
Restore the default Ethernet port multicast suppression ratio	**undo multicast-suppression**
Set Ethernet port unicast suppression ratio	**unicast-suppression** { *ratio* | **pps** }
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 three different link types: access, hybrid, and trunk . 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 39 Setting the Link Type for the Ethernet Port

Operation	Command
Configure the port as an access port	**port link-type access**
Configure the port as a hybrid port	**port link-type hybrid**
Configure the port as a trunk port	**port link-type trunk**
Restore the default link type, that is, access port	**undo port link-type**

By default, the port is access port.

Note that:

- You can configure three types of ports concurrently on the same Switch, but you cannot switch port type between trunk port and hybrid 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.

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 40 Adding the Ethernet Port to Specified VLANs

Operation	Command
Add the current access port to a specified VLAN	**port access vlan** *vlan_id*
Add the current hybrid port to specified VLANs	**port hybrid vlan** *vlan_id_list* { **tagged** | **untagged** }
Add the current trunk port to specified VLANs	**port trunk permit vlan** { *vlan_id_list* | **all** }
Remove the current access port from to a specified VLAN.	**undo port access vlan**
Remove the current hybrid port from to specified VLANs.	**undo port hybrid vlan** *vlan_id_list*
Remove the current trunk port from specified VLANs.	**undo port trunk permit vlan** { *vlan_id_list* | **all** }

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 have 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 41 Setting the Default VLAN ID for an Ethernet Port

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

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 42 Setting Loopback Detection for the Ethernet Port

Operation	Command
Enable loopback detection on the port (System View/Ethernet Port View)	**`loopback-detection enable`**
Disable loopback detection on the port (System View/Ethernet Port View)	**`undo loopback-detection enable`**
Enable the loopback controlled function of the trunk and hybrid ports (Ethernet Port View)	**`loopback-detection control enable`**
Disable the loopback controlled function of the trunk and hybrid ports (Ethernet Port View)	**`undo loopback-detection control enable`**
Set the external loopback detection interval of the port (System View)	**`loopback-detection interval-time`** *`time`*
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, 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 43 Copying Port Configuration to Other Ports

Operation	Command
Copy port configuration to other ports	**copy configuration source** { *interface_type interface_number* | *interface_name* | **aggregation_group** *agg_id* } **destination** { *interface_list* [**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 44 Displaying and Debugging Ethernet Port

Operation	Command
Perform loopback test on the Ethernet port.	**loopback** { **external** | **internal** }
Display all port information	**display interface** { *interface_type* | *interface_type interface_num* | *interface_nam* }
Display port information of a specific unit	**display unit** *unit_id* **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** [*interface_type* | *interface_type interface_num* | *interface_name*]

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

S
S
Switch A
Switch B

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.

```
[SW5500]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.

```
[SW5500-Ethernet1/0/1]port link-type trunk
[SW5500-Ethernet1/0/1]port trunk permit vlan 2 6 to 50 100
```

3 Create the VLAN 100.

```
[SW5500]vlan 100
```

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

```
[SW5500-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, traffic statistics. The VLAN setting includes permitted VLAN types, and default VLAN ID. The port setting includes port link type.

The Switch 5500G-EI can support up to 32 aggregation groups. Each group can have eight Gigabit Ethernet ports or four 10G ports at most.

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 (LACPADU). 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. 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 unselected ports. Both selected and unselected ports can transceive LACP protocol, but unselected 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 unselected ports. If not, all member ports are selected ports. Both selected and unselected ports can transceive LACP protocol, but unselected 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 unselected state is determined by the port priority of the system. You can decide whether the port is selected or unselected 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 unselected 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 45 Enabling/Disabling LACP

Operation	**Command**
Enable LACP at the port	*`lacp enable`*
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 46 Creating/Deleting an Aggregation Group

Operation	Command
Create an aggregation group	**link-aggregation group** *agg-id* **mode** { **manual** | **static** }
Delete an aggregation group	**undo link-aggregation group** *agg-id*

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 occured.

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

Operation	Command
Add an Ethernet port into the aggregation group	**port link-aggregation group** *agg_id*
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 48 Setting/Deleting the Aggregation Group Descriptor

Operation	Command
Set aggregation group descriptor	**link-aggregation group** *agg_id* **description** *alname*
Delete aggregation group descriptor	**undo link-aggregation group** *agg_id* **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 unselected 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 unselected state.

Perform the following configuration in System View.

Table 49 Configuring System Priority

Operation	Command
Configure system priority	**lacp system-priority** *system_priority_value*
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 unselected 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 50 Configuring Port Priority

Operation	Command
Configure port priority	**lacp port-priority** *port_priority_value*
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 51 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** [*agg_id*]
Display local system ID	**display lacp system-id**
Display detailed link aggregation information at the port	**display link-aggregation interface** { *interface_type interface_number* | *interface_name* } [**to** { *interface_type interface_num* | *interface_name* }]
Clear LACP statistics at the port	**reset lacp statistics** [**interface** { *interface_type interface_number* | *interface_name* } [**to** { *interface_type interface_num* | *interface_name* }]]
Disable/enable debugging LACP state machine	[**undo**] **debugging lacp state** [**interface** { *interface_type interface_number* | *interface_name* } [**to** { *interface_type interface_num* | *interface_name* }]] { { **actor-churn** | **mux** | **partner-churn** | **ptx** | **rx** }* | **all** }
Disable/enable debugging LACP packets	[**undo**] **debugging lacp packet** [**interface** { *interface_type interface_number* | *interface_name* } [**to** { *interface_type interface_num* | *interface_name* }]]
Disable/enable debugging link aggregation errors	[**undo**] **debugging link-aggregation error**
Disable/enable debugging link aggregation events	[**undo**] **debugging link-aggregation event**

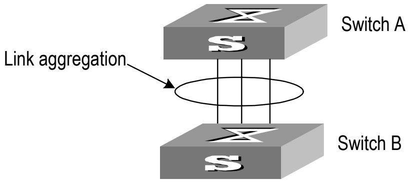
Link Aggregation Configuration Example

Networking Requirement

Switch A connects Switch B with three aggregation ports, numbered as GigabitEthernet1/0/1 to GigabitEthernet1/0/3, 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.

```
[SW5500]link-aggregation group 1 mode manual
```

b Add Ethernet ports GigabitEthernet1/0/1 to GigabitEthernet1/0/3 into aggregation group 1.

```
[SW5500]interface ethernet1/0/1
[SW5500-GigabitEthernet1/0/1]port link-aggregation group 1
[SW5500-GigabitEthernet1/0/1]interface gigabitethernet1/0/2
[SW5500-GigabitEthernet1/0/2]port link-aggregation group 1
[SW5500-GigabitEthernet1/0/2]interface gigabitethernet1/0/3
[SW5500-GigabitEthernet1/0/3]port link-aggregation group 1
```

2 Static LACP aggregation

a Create static LACP aggregation group 1.

```
[SW5500]link-aggregation group 1 mode static
```

b Add Ethernet ports GigabitEthernet1/0/1 to GigabitEthernet1/0/3 into aggregation group 1.

```
[SW5500]interface gigabitethernet1/0/1
[SW5500-GigabitEthernet1/0/1]port link-aggregation group 1
[SW5500-GigabitEthernet1/0/1]interface gigabitethernet1/0/2
[SW5500-GigabitEthernet1/0/2]port link-aggregation group 1
[SW5500-GigabitEthernet1/0/2]interface gigabitethernet1/0/3
[SW5500-GigabitEthernet1/0/3]port link-aggregation group 1
```

3 Dynamic LACP aggregation

a Enable LACP at Ethernet ports GigabitEthernet1/0/1 to GigabitEthernet1/0/3.

```
[SW5500]interface gigabitethernet1/0/1
[SW5500-GigabitEthernet1/0/1]lacp enable
[SW5500-GigabitEthernet1/0/1]interface gigabitethernet1/0/2
[SW5500-GigabitEthernet1/0/2]lacp enable
[SW5500-GigabitEthernet1/0/2]interface gigabitethernet1/0/3
[SW5500-GigabitEthernet1/0/3]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.

VLAN Configuartion

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 52 Creating/Deleting a VLAN

Operation	Command
Create a VLAN and enter the VLAN View	**vlan** *vlan_id*

Table 52 Creating/Deleting a VLAN

Operation	Command
Delete the specified VLAN	**undo vlan** { *vlan_id* [**to** *vlan_id*] | **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 53 Adding Ethernet Ports to a VLAN

Operation	Command
Add Ethernet ports to a VLAN	**port** *interface_list*
Remove Ethernet ports from a VLAN	**undo port** *interface_list*

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 54 Setting/Deleting a Vlan or Vlan Interface Description Character String

Operation	Command
Set the description character string for a VLAN or VLAN interface	**description** *string*
Restore the default description of current VLAN or VLAN interface	**undo description**

By default, there is no VLAN description character string. VLAN interface description character string of VLAN interface is the interface name, e.g. `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 55 Specifying/Removing the VLAN Interface

Operation	Command
Create a new VLAN interface and enter VLAN Interface View	**interface vlan-interface** *vlan_id*

Table 55 Specifying/Removing the VLAN Interface

Operation	Command
Remove the specified VLAN interface	**undo interface vlan-interface** *vlan_id*

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 56 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 it, 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 57 Displaying and Debugging a VLAN

Operation	Command
Display information about the VLAN interface	**display interface Vlan-interface** [*vlan_id*]
Display information about the VLAN	**display vlan** [*vlan_id* | **all** | **static** | **dynamic**]

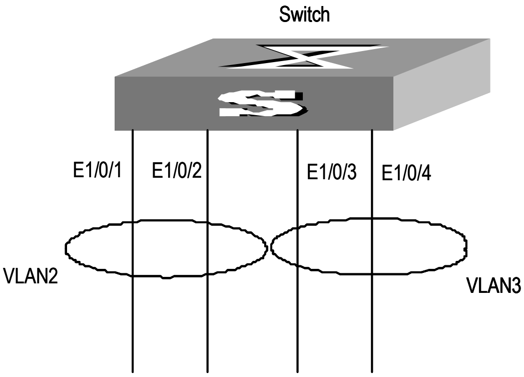
VLAN Configuration Example One

Networking Requirements

Create VLAN2 and VLAN3. Add GigabitEthernet1/0/1 and GigabitEthernet1/0/2 to VLAN2 and add GigabitEthernet1/0/3 and GigabitEthernet1/0/4 to VLAN3.

Networking Diagram

Figure 14 VLAN Configuration Example 1



Configuration Procedure

1 Create VLAN 2 and enter its view.

```
[SW5500]vlan 2
```

2 Add GigabitEthernet1/0/1 and GigabitEthernet1/0/2 to VLAN2.

```
[SW5500-vlan2]port gigabitethernet1/0/1 to gigabitethernet1/0/2
```

3 Create VLAN 3 and enter its view.

```
[SW5500-vlan2]vlan 3
```

4 Add GigabitEthernet1/0/3 and GigabitEthernet1/0/4 to VLAN3.

```
[SW5500-vlan3]port gigabitethernet1/0/3 to gigabitethernet1/0/4
```

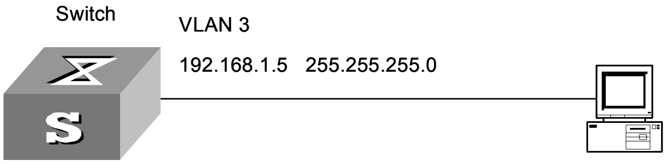
VLAN Configuration Example Two

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.

```
[SW5500]vlan 3
[SW5500-vlan3]quit
```

2 Enter the VLAN interface view:

```
[SW5500]interface vlan-interface 3
```

3 Provide the IP address and subnet mask:

```
[SW5500-Vlan-interface3]ip address 192.168.1.5 255.255.255
[SW5500-Vlan-interface3]quit
```

Voice VLAN Configuration

Voice VLAN Overview

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 58:

Table 58 The corresondance between Port Mode and IP Phone

Voice VLAN Mode	Type of IP Phone	Port Mode
Auto 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.
		Hybrid: Suppored, but the default VLAN of the connected port must exist and it is in the tagged VLAN list which is allowed to pass the connected port.
	Untagged IP Phone	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 Untag IP Phone Untagged 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
		Hybrid: Supported, but the default VLAN of the connected port must exist and it is in the tagged VLAN list which is allowed to pass the connected port.
		Access: Supported, but the default VLAN of the connected port must be the Voice VLAN.

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 59 Configuring Voice VLAN Features

Operation	Command
Enable Voice VLAN features	**voice vlan** *vlan_id* **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 60 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. Perform the following configuration in System View.

Table 61 Configuring the OUI address Learned by Voice VLAN

Operation	command
Set the OUI address learned by Voice VLAN	**voice vlan mac-address** *oui* **mask** *oui_mask* [**description** *string*]
Remove the OUI address learned by Voice VLAN	**undo voice vlan mac-address** *oui*

There are four default OUI addresses after the system starts.

Table 62 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 63 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 64 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 65 Configuring the Aging Time of Voice VLAN

Operation	command
Set the aging time of Voice VLAN	**voice vlan aging** *minutes*
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 66 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**

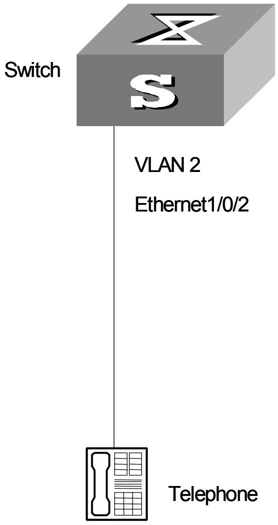
Voice VLAN Configuration Example

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 GigabitEthernet1/0/2 as the IP Phone access port. The type of IP Phone is untagged.

Network Diagram

Figure 16 Voice VLAN Configuration



Configuration Steps

```
[SW5500]vlan 2
[SW5500-vlan2]port gigabitethernet1/0/2
[SW5500-vlan2]interface gigabitethernet1/0/2
[SW5500-GigabitEthernet1/0/2]voice vlan enable
```

```
[SW5500-GigabitEthernet1/0/2]quit
[SW5500]undo voice vlan mode auto
[SW5500]voice vlan mac_address 0011-2200-0000 mask ffff-ff00-0000
description private
[SW5500]voice vlan 2 enable
[SW5500]voice vlan aging 100
```

4 POWER OVER ETHERNET (POE) CONFIGURATION

This chapter covers the following topics:

PoE Overview

The Switch 5500G-EI 24 Port PWR and Switch 5500G-EI 48 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 24/48 Ethernet electrical ports, the PWR switches can supply power to up to 24/48 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 24/48 ports.
- The PSE processing software on the PWR switches can be upgraded online.
- The PWR switches provides 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 ^{0}C; and restores the power feeding to all the PDs connected with the ports when the temperature drops below 60 ^{0}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 67 PoE Configuration

Device	Configuration	Default	Description
Switch 5500G-EI 24 Port PWR / Switch 5500G-EI 48 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 5500G-EI supports **`signal`** mode only
	Setting the compatibility detect function on a port	Close	
	Upgrading the PSE processing software online		Online downloading of upgrade file is needed
PD	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 68 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 S5624P-PWR/S5648P-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 69 Setting the Maximum power on a port

Operation	Command
Set the maximum power supplied by a port	**`poe max-power`** ***`max-power`***
Restore the default maximum power on the port	**`undo poe max-power`**

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 70 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 71 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 72 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 5500G-EI 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 73 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 74 Upgrading PSE Processing Software Online

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

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 (e.g. 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 75 PoE Information Display

Operation	Command
Display the PoE status of a specific port or all ports on the Switch	**display poe interface [** ***interface-name*** **|** ***interface-type*** **|** ***interaface-num*** **]**
Display the PoE power information of a specific port or all ports on the Switch	**display poe interface power [** ***interface-name*** **|** ***interface-type*** **|** ***interaface-num*** **]**
Display the PSE parameters	**`display poe powersupply`**

Refer to the Command Reference Manual for furhter details on parameters.

Configuration Example

Networking Requirements

The GigabitEthernet1/0/1 and GigabitEthernet1/0/2 ports of the Switch 5500 PWR are connected with a PD and an access point (AP) respectively.

The GigabitEthernet1/0/24 port is intended to be connected with an AP. The PSE processing software of the Switch 5500 PWR should be first upgraded online. The remotely accessed PDs should be powered by the Switch 5500 PWR. The power consumption of the AP that has already been connected with GigabitEthernet1/0/2 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 GigabitEthernet1/0/24 even when the Switch 5500 PWR is in full load.

Network Diagram

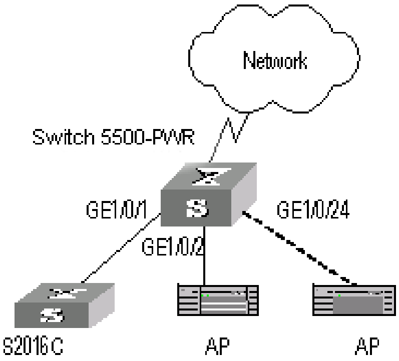


Figure 17 PoE Remote Power Supply

Configuration Procedure

Update the PSE processing software online.

```
[SW5500]poe update refresh 0290_021.s19
```

Enable the PoE feature on the GigabitEthernet1/0/1, GigabitEthernet1/0/2, and GigabitEthernet1/0/24 ports (the feature is enabled by default, so this step can be ignored).

```
[SW5500-GigabitEthernet1/0/1]poe enable
[SW5500-GigabitEthernet1/0/2]poe enable
[SW5500-GigabitEthernet1/0/24]poe enable
```

Set the maximum power output of GigabitEthernet1/0/1 and GigabitEthernet1/0/2 to 12000 and 3000 mW respectively.

```
[SW5500-GigabitEthernet1/0/1]poe max-power 12000
[SW5500-GigabitEthernet1/0/2]poe max-power 3000
```

Set the priority of GigabitEthernet1/0/24 to `critical` to guarantee the power feeding to the AP to which this port connects.

```
[SW5500-GigabitEthernet1/0/24]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).

```
[SW5500]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.

```
[SW5500]poe legacy enable
```

5 NETWORK PROTOCOL OPERATION

This chapter covers the following topics:

- IP Address Configuration
- ARP Configuration
- Resilient ARP Configuration
- BOOTP Client Configuration
- DHCP Configuration
- Access Management Configuration
- UDP Helper Configuration
- IP Performance Configuration

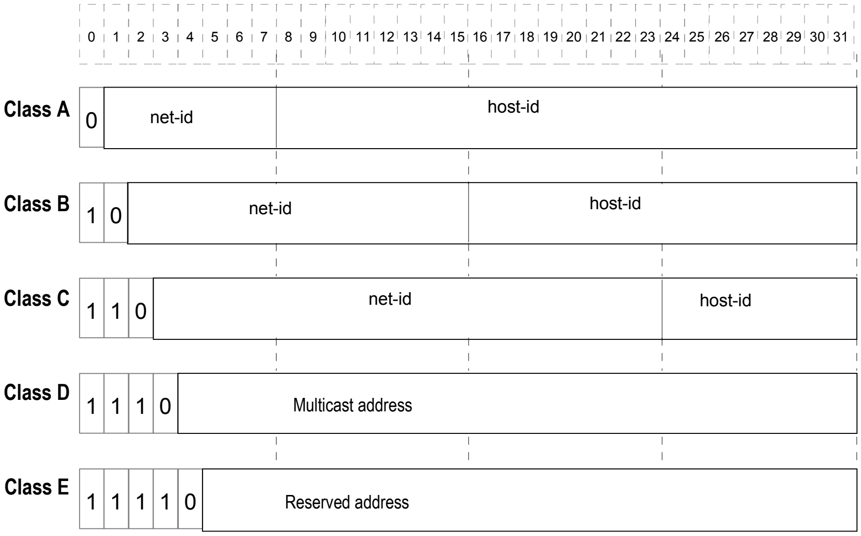
IP Address Configuration

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 18.

Figure 18 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 76.

Table 76 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	Host ID with all the digits being 0 indicates that the IP address is the network address, and is used for network routing. Host ID with all the digits being 1 indicates the broadcast address, that is, broadcast to all hosts on the network. IP address 0.0.0.0 is used for the host that is not put into use after starting up. 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. 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.
B	128.0.0.0 to 191.255.255.255	128.0.0.0 to 191.254.0.0	Host ID with all the digits being 0 indicates that the IP address is the network address, and is used for network routing. Host ID with all the digits being 1 indicates the broadcast address, that is, broadcast to all hosts on the network.
C	192.0.0.0 to 223.255.255.255	192.0.0.0 to 223.255.254.0	Host ID with all the digits being 0 indicates that the IP address is the network address, and is used for network routing. Host ID with all the digits being 1 indicates the broadcast address, that is, broadcast to all hosts on the network.
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.

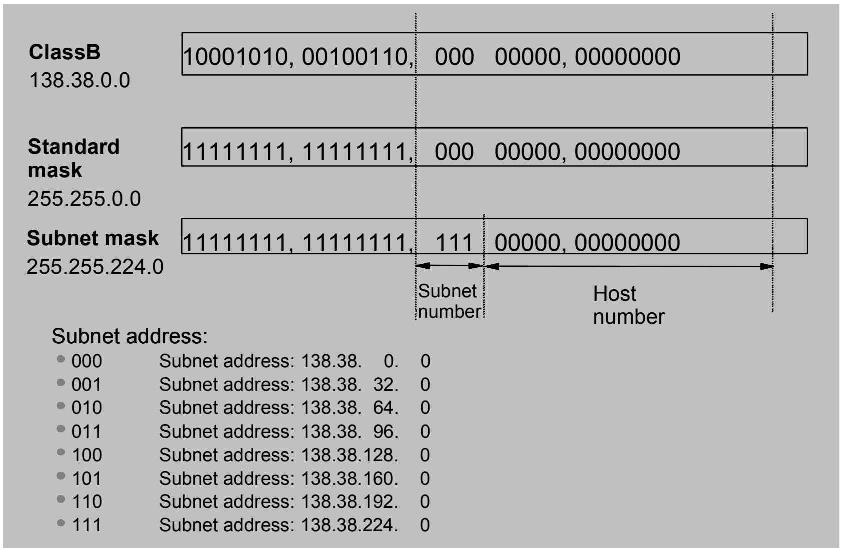
Subnet and Mask

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, 202.38.32.0, 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 19). Each subnet can contain more than 8000 hosts.

Figure 19 Subnet Division of IP Address


ClassB
138.38.0.0
10001010, 00100110, 000 00000, 00000000
Standard mask
255.255.0.0
11111111, 11111111, 000 00000, 00000000
Subnet mask
255.255.224.0
11111111, 11111111, 111 00000, 00000000
Subnet number
Host number
Subnet address:
000 Subnet address: 138.38. 0. 0
001 Subnet address: 138.38. 32. 0
010 Subnet address: 138.38. 64. 0
011 Subnet address: 138.38. 96. 0
100 Subnet address: 138.38.128. 0
101 Subnet address: 138.38.160. 0
110 Subnet address: 138.38.192. 0
111 Subnet address: 138.38.224. 0

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

Perform the following configuration in System View.

Table 77 Configuring the Host Name and the Corresponding IP Address

Operation	Command
Configure the hostname and the corresponding IP address	**ip host** *hostname ip_address*
Delete the hostname and the corresponding IP address	**undo ip host** *hostname* [*ip_address*]

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 Ethernet Switch. Generally, it is enough to configure one IP address for an interface. You can also configure up to five IP addresses for an interface, so that it can be connected to several subnets. Among these IP addresses, one is the primary IP address and all others are secondary.

Perform the following configuration in VLAN Interface View.

Table 78 Configuring the IP Address for a VLAN Interface

Operation	Command
Configure IP address for a VLAN interface	**ip address** *ip_address* { *mask* | *mask_length* } [**sub**]
Delete the IP address of a VLAN interface	**undo ip address** *ip-address* { *mask* | *mask_length* } [**sub**]

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

Note that the VLAN interface cannot be configured with the secondary IP address if its IP address is set to be allocated by BOOTP or DHCP.

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 79 Displaying and Debugging IP Address

Operation	Command
Display all hosts on the network and the corresponding IP addresses	**display ip host**
Display the configurations of each interface	**display ip interface** ***interface-type*** *interface-number*

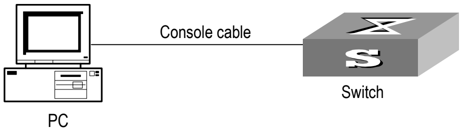
IP Address Configuration Example

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 Ethernet Switch.

Networking Diagram

Figure 20 IP Address Configuration Networking



Configuration Procedure

1 Enter VLAN interface 1.

```
[SW5500]interface vlan-interface 1
```

2 Configure the IP address for VLAN interface 1.

```
[SW5500-vlan-interface1]ip address 129.2.2.1 255.255.255.0
```

Troubleshooting IP Address Configuration

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

Troubleshooting can be performed as follows:

- Check the configuration of the Ethernet 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 80 Manually Adding/Deleting Static ARP Mapping Entries

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

Table 80 Manually Adding/Deleting Static ARP Mapping Entries

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

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 Ethernet 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 81 Configuring the Dynamic ARP Aging Timer

Operation	Command
Configure the dynamic ARP aging timer	**arp timer aging** *aging_time*
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 82 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 83 Displaying and Debugging ARP

Operation	Command
Display the ARP mapping table	**display arp** [*ip_address* | [**dynamic** | **static**] [| { **begin** | **include** | **exclude** } *text*]]
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** { *interface_type interface_num* | *interface_name* }]
Enable ARP information debugging	**debugging arp packet**
Disable ARP information debugging	**undo debugging arp packet**

Resilient ARP Configuration

Overview of Resilient ARP

To support resilient networking in XRN applications, redundant links are required between the XRN fabric and other devices. But if intra-fabric connections are broken and the original fabric is split, these redundant links may cause a situation where the network connects to two or more layer 3 devices of the same configuration and they run the same routing function. To eliminate this situation, you can resort to resilient ARP mechanism, which can immediately detect if there are layer 3 devices of the same configuration existing in the network. If yes, it will keep only one as a Layer 3 device and turn the others in to Layer 2 devices.

A resilient ARP state machine may be in one of six states: Initialize, LisentForL3Master, L3Master, L3Slave, L2Master and L2Slave. An L3Master state machine regularly sends resilient ARP messages to notify other XRN fabrics that its home fabric is in Layer 3 state.

The resilient ARP mechanism can implement state transition by sending/receiving resilient ARP messages regularly, so as to determine if a device serves as a Layer 3 or Layer 2 device.

Resilient ARP Configuration

Resilient ARP configuration is described in the following sections:

- Enabling/Disabling Resilient ARP Function
- Configuring Resilient ARP Packet-sending VLAN Interface

Enabling/Disabling Resilient ARP Function

After resilient ARP is enabled, the system can ensure there is only one Layer 3 device, and that others are Layer 2 devices.

Perform the following configuration in System View.

Table 84 Enabling/Disabling Resilient ARP Function

Operation	Command
Enable resilient ARP function	**`resilient-arp enable`**
Disable resilient ARP function	**`undo resilient-arp enable`**

By default, resilient ARP function is enabled.

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

Configuring Resilient ARP Packet-sending VLAN Interface

You must configure the VLAN interface corresponding to the redundant links which connect the XRN fabric with other devices, to make resilient ARP operate normally. Then if intra-fabric connections are broken, resilient ARP packets can be sent through these VLAN interfaces corresponding to the redundant links, to determine if the system works as a layer 3 or layer 2 device.

You can use the following command to configure through which VLAN interface resilient ARP packet is sent. The system provides a default VLAN interface to send resilient ARP packets.

Perform the following configuration in System View.

Table 85 Configuring/Deleting Resilient ARP Packet-sending VLAN Interface

Operation	Command
Configure resilient ARP packet-sending VLAN interface	**`resilient-arp interface vlan-interface`** *`vlan_id`*
Delete resilient ARP packet-sending VLAN interface	**`undo resilient-arp interface vlan-interface`** *`vlan_id`*

By default, the system sends resilient ARP packets through VLAN interface 1.

Note that you only specify resilient ARP packet-sending VLAN interfaces, and any VLAN interface can receive resilient ARP packets.

Displaying and Debugging Resilient ARP Configuration

After the above configurations are completed, you can enter the **`display`** command in any view to view the running of resilient ARP function and to further check configuration results.

You can also enter the **debugging** command in User View to debug the resilient ARP function.

Table 86 Displaying and Debugging Resilient ARP Configuration

Operation	Command
Display resilient ARP state information	**display resilient-arp** [**unit** *unit_id*]
Enable resilient ARP debugging	**debugging resilient-arp** { **packet** | **state** | **error** | **all** }
Disable resilient ARP debugging	**undo debugging resilient-arp** { **packet** | **state** | **error** | **all** }

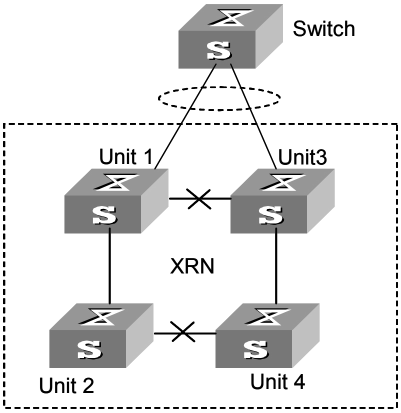
Resilient ARP Configuration Example

Networking Requirement

There are four units, numbered respectively Unit 1 through Unit 4, in the XRN network. Unit 1 and Unit 3 are connected to the Switch in link aggregation mode. Resilient ARP runs on the XRN fabric to avoid packet forwarding problems between the Switch and fabric when the network has two Layer 3 units, if the links between unit 1 and unit 3, between unit 2 and unit 4 are disconnected. MD5 authentication is enabled for the sake of security. The ports of Unit 1 and Unit 3, connecting the Switch, belong to VLAN 2.

Networking Diagram

Figure 21 Networking for Resilient ARP Configuration



Configuration Procedure

1 Enable resilient ARP function.

```
[SW5500]resilient-arp enable
```

2 Set VLAN interface 2 to send resilient ARP packets.

```
[SW5500]resilient-arp interface vlan-interface 2
```

BOOTP Client Configuration

Overview of BOOTP Client

A BOOTP client can request the server to allocate an IP address to it using BOOTP (bootstrap protocol). These two major processes are included on the BOOTP client:

- Sending BOOTP Request message to the server
- Processing BOOTP Response message returned from the server

In obtaining an IP address using BOOTP, the BOOTP client sends the server the BOOTP Request message. Upon receiving the request message, the server returns the BOOTP Response message. The BOOTP client can then obtain the allocated IP address from the received response message.

The BOOTP message is based on UDP, so a retransmission mechanism in the event of timeout is used to guarantee its reliable transmission. The BOOTP client also starts a retransmission timer when it sends the request message to the server. If the timer expires before the return of the response message from the server, the request message will be retransmitted. The retransmission occurs every five seconds and the maximum number of retransmissions is three, that is, the message shall not be retransmitted after the third time.

BOOTP Client Configuration

BOOTP client is described in the following section.

Configuring a VLAN Interface to Obtain the IP Address Using BOOTP

Perform the following configuration in VLAN Interface View.

Table 87 Configuring a VLAN Interface to Obtain the IP Address Using BOOTP

Operation	Command
Configure VLAN interface to obtain an IP address using BOOTP	**`ip address bootp-alloc`**
Remove the configuration	**`undo ip address bootp-alloc`**

By default, the VLAN interface cannot use BOOTP to get an IP address.

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

Displaying and Debugging BOOTP Client

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

Enter the **`debugging`** command in User View to debug BOOTP client.

Table 88 Displaying and Debugging BOOTP Client

Operation	Command
Disable/enable hot backup debugging of BOOTP client	[**`undo`**] **`debugging dhcp xrn xha`**

DHCP Configuration

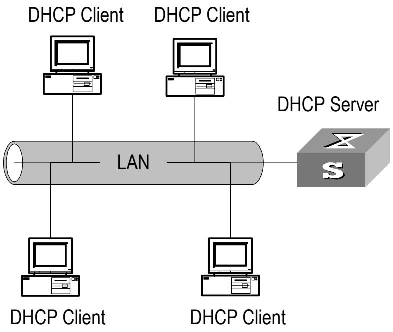
Overview of DHCP

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 22

Figure 22 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.

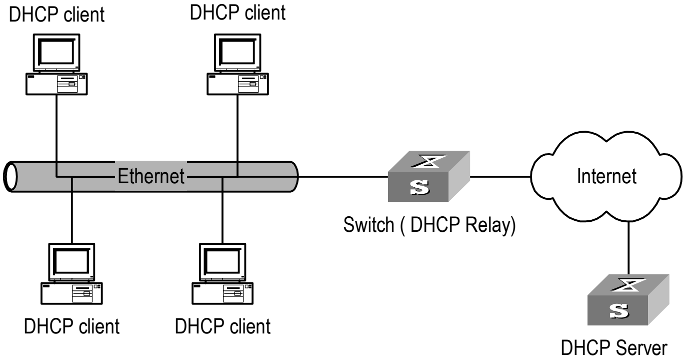
  In practice, the DHCP client, by default, shall originate the DHCP_Request message to the DHCP server right in the middle of the IP lease period, to update the IP lease. If the IP address is still available, the DHCP server responds with the DHCP_ACK message, notifying the client that it has got the 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 23.

Figure 23 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 89 Configuring a VLAN Interface to Obtain an IP Address Using DHCP

Operation	Command
Configure VLAN interface to obtain IP address using DHCP	`ip address dhcp-alloc`
Remove the configuration	`undo ip address dhcp-alloc`

By default, the VLAN interface does not obtain an IP address using DHCP.

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 followng sections:

- Configuring the IP address for the DHCP server
- Configuring the DHCP Server Group for the VLAN Interfaces
- Configuring the User Address Entry for the DHCP Server Group
- Enabling/Disabling the DHCP Security Feature on the VLAN interface

Note:

- After you have configured DHCP Relay, the Switch automatically configure UDP-Helper whether the Switch is a single unit or in a fabric. The UDP-Helper configuration remains when you remove the DHCP Relay configuration.
- If you remove UDP-Helper configuration when the DHCP Relay configuration still remains, the Switch will display the following prompt `This may result in DHCP Relay errors`, and you will need to confirm if you really want to remove the UDP-Helper configuration.

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 90 Configuring the IP Address for the DHCP Server

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

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 91 Configuring the DHCP Server Group Corresponding to VLAN Interfaces

Operation	Command
Configure DHCP server group corresponding to VLAN interfaces	**dhcp-server** *groupNo*
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.

Configuring the User Address Entry for the DHCP Server Group

To ensure that a valid user with a fixed IP address in a VLAN configured with DHCP Relay passes the address validity check of the DHCP security feature, you must add a static address entry which indicates the correspondence between an IP address and a MAC address.

If an illegal user configures a static IP address which is in conflict with the fixed IP address of a valid user, the Switch with DHCP Relay function enabled can identify the valid user and reject the illegal user's request to bind the IP address with the MAC address.

Perform the following configuration in System View..

Table 92 Configuring the User Address Entry for the DHCP Server Group

Operation	Command
Configure user address entry for DHCP server group	**dhcp-security static** *ip_address mac_address*
Delete the user address entry in the DHCP server group	**undo dhcp-security** { *ip_address* | **all** | **dynamic** | **static** }

Enabling/Disabling the DHCP Security Feature on the VLAN interface

Enabling DHCP security features will start the address validity check on the VLAN interface; disabling DHCP security features will cancel the address validity check.

Perform the following configuration in VLAN Interface View.

Table 93 Enabling/Disabling DHCP Security Feature on the VLAN Interface

Operation	Command
Enable DHCP security feature on VLAN interface	**address-check enable**
Disable DHCP security feature on VLAN interface	**address-check disable**

By default, the DHCP security feature is disabled on the VLAN interface.

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 94 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** *vlan_id*
Display all address information of the valid user address table for the DHCP server group	**display dhcp-security [** *ip_address* | **dynamic** | **static] [unit** *unit_id* **]**
Display address allocation information of DHCP client	**display dhcp client [verbose]**
Enable/disable DHCP client debugging	**[undo] debugging dhcp client { all** | **error** | **event** | **packet }**

Table 94 Displaying and Debugging DHCP Configuration

Operation	Command
Enable/disable DHCP Client hot backup debugging	**[undo] debugging dhcp xrn xha**
Enable/disable DHCP relay debugging	**[undo] debugging dhcp-relay**

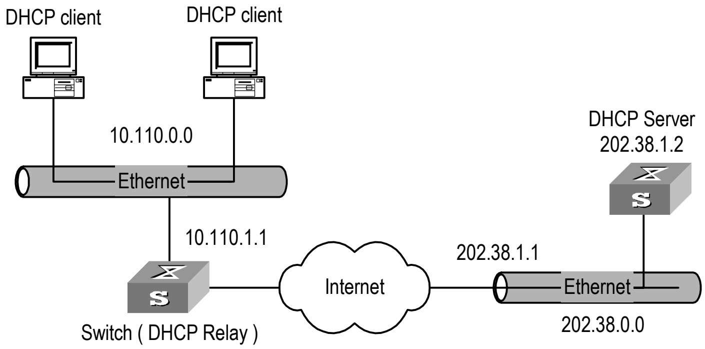
DHCP Relay Configuration Example One

Networking Requirements

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

Networking Diagram

Figure 24 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).

```
[SW5500]dhcp-server 0 ip 192.168.1.1 192.168.2.1
```

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

```
[SW5500]interface vlan-interface 1
[SW5500-Vlan-interface1]dhcp-server 0
[SW5500-Vlan-interface1]quit
[SW5500]interface vlan-interface 10
[SW5500-Vlan-interface10]dhcp-server 0
[SW5500-Vlan-interface10]quit
```

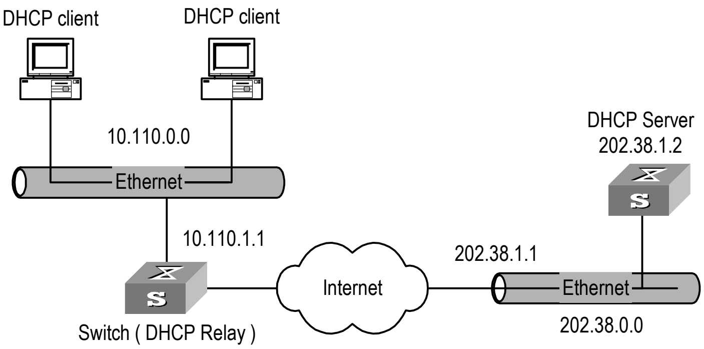
DHCP Relay Configuration Example Two

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 25 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.

```
[SW5500]dhcp-server 1 ip 202.38.1.2
```

2 Associate the VLAN interface 2 with DHCP Server group 1.

```
[SW5500]interface vlan 2
[SW5500-Vlan-interface2]dhcp-server 1
```

3 Configure the IP address of the VLAN interface 2, which must be in the same segment as DCHP Client.

```
[SW5500-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 Ethernet 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 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 95 Enabling/Disabling the Access Management Function

Operation	Command
Enable access management function	**`am enable`**
Disable access management function	**`undo am enable`**

By default, the system disables the access management function.

Configuring the Access 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 96 Configuring the AccessIP Address Pool Based on the Port

Operation	Command
Configure the access management IP address pool based on the port	**`am ip-pool`** *`address_list`*
Cancel part or all of the IP addresses in the access management IP address pool of the port	**`undo am ip-pool`** { **`all`** | *`address_list`* }

By default, the IP address pools for access control 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 97 Configuring Layer 2 Isolation Between Ports

Operation	Command
Add a port to the isolation group	`port isolate`
Remove a port from the isolation group	`undo port isolate`

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 98 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 99 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**

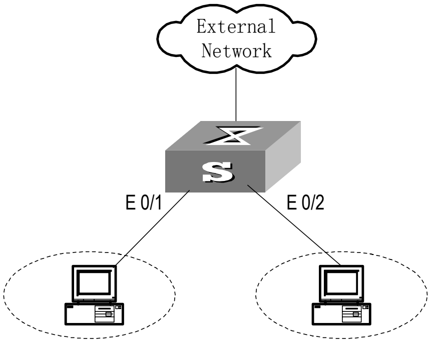
Access Management Configuration Example

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 26 Networking Diagram for Port Isolation Configuration



Configuration Procedure

1 Enable access management globally.

```
[SW5500]am enable
```

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

```
[SW5500]interface gigabitethernet1/0/1
[SW5500-GigabitEthernet1/0/1]am ip-pool 202.10.20.1 20
```

3 Add port 1 into isolation group.

```
[SW5500-GigabitEthernet1/0/1]port isolate
```

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

```
[SW5500-GigabitEthernet1/0/1]interface gigabitethernt1/0/2
[SW5500-GigabitEthernet1/0/2]am ip-pool 202.10.20.21 30
```

5 Add port 2 into isolation group.

```
[SW5500-GigabitEthernet1/0/2]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:

```
<SW5500>system-view
[SW5500]acl number 2500
[SW5500-acl-basic-2500]rule 0 permit source 10.10.10.1 0.0.0.255
```

To delete this feature, enter:

```
<SW5500>system-view
[SW5500]acl number 2500
[SW5500-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

Note:

- After you have configured DHCP Relay, the Switch automatically configure UDP-Helper whether the Switch is a single unit or in a fabric. The UDP-Helper configuration remains when you remove the DHCP Relay configuration.
- If you remove UDP-Helper configuration when the DHCP Relay configuration still remains, the Switch will display the following prompt `This may result in DHCP Relay errors`, and you will need to confirm if you really want to remove the UDP-Helper configuration.

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 100 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 101. You can configure up to 256 UDP ports with the relay function.

Table 101 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 102 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 103 Configuring the Relay Destination Server for Broadcast Packet

Operation	Command
Configure relay destination server for broadcast packet	**udp-helper server** *ip_address*
Delete relay destination server for broadcast packet	**undo udp-helper server** [*ip_address*]

Note that:

- The **undo udp-helper server** command (without any parameter) deletes all desitnation 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 104 Displaying and Debugging UDP Helper Configuration

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

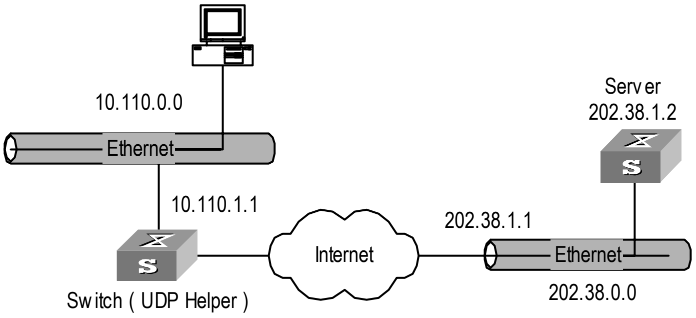
UDP Helper Configuration Example

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 27 Networking for UDP Helper Configuration



Configuration Procedure

1 Enable UDP Helper function.

```
[SW5500]udp-helper enable
```

2 Set to relay-forward the broadcast packets with destination UDP port 55.

```
[SW5500]udp-helper port 55
```

3 Set the IP address of the destination server corresponding to VLAN interface 2 as 202.38.1.2.

```
[SW5500]interface vlan 2
[SW5500-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 105 Configuring TCP Attributes

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

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 106 Displaying and Debugging IP Performance

Operation	Command
Display TCP connection state	**display tcp status**
Display TCP connection statistics data	**display tcp statistics**
Display UDP statistics information	**display udp statistics**
Display IP statistics information	**display ip statistics**
Display ICMP statistics information	**display icmp statistics**
Display socket interface information of current system	**display ip socket** [**socktype** *sock_type*] [*task_id socket_id*]
Display the summary of the Forwarding Information Base	**display fib**
Display the FIB entries matching the destination IP address (range)	**display fib** *ip_address1* [{ *mask1* | *mask_length1* } [*ip_address2* { *mask2* | *mask_length2* } | **longer**] | **longer**]
Display the FIB entries matching a specific ACL	**display fib acl** *number*
Display the FIB entries which are output from the buffer according to regular expression and related to the specific character string	**display fib** | { { **begin** | **include** | **exclude** } *text* }
Display the FIB entries matching the specific prefix list	**display fib ip-prefix** *listname*
Display the total number of FIB entries	**display fib statistics** [{**begin**|**include** |**exclude**} *text*]
Reset IP statistics information	**reset ip statistics**
Reset TCP statistics information	**reset tcp statistics**
Reset UDP statistics information	**reset udp statistics**

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:

```
[SW5500]terminal debugging
```

```
<SW5500>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

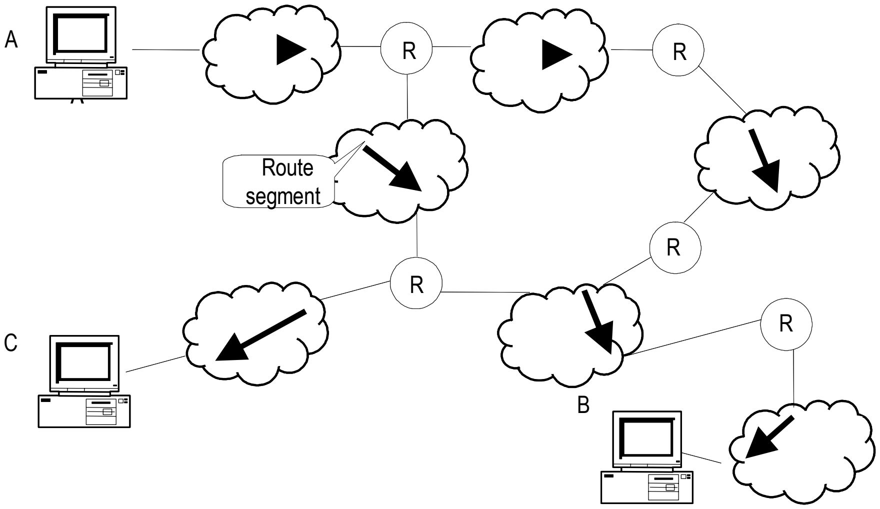
IP Routing Protocol Overview

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.

In a network, the router regards a path for sending a packet as a logical route unit, and calls it a hop. For example, in Figure 28, 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 across a network, there is a hop 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. A router can be connected to any physical link that constitutes a route segment for routing packets through the network.

When the Switch 5500G-EI 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 5500G-EI running routing protocols.

Figure 28 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.

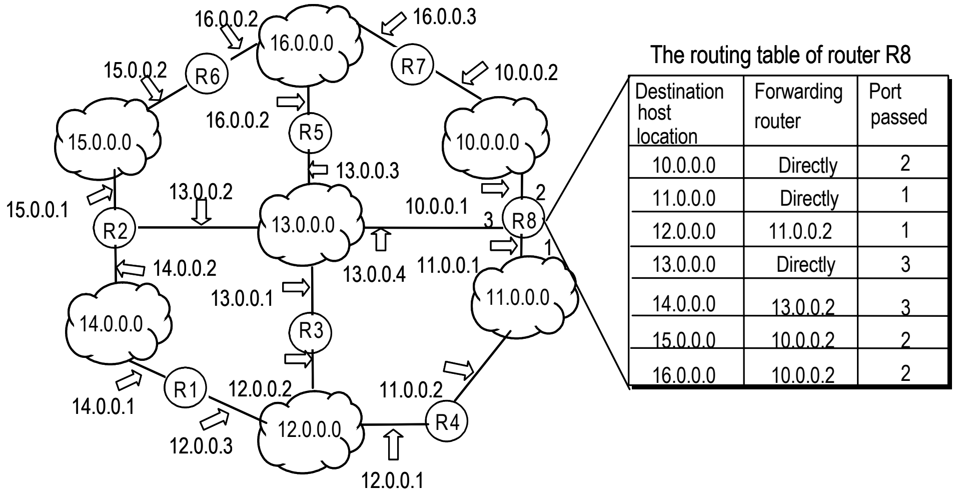
In addition, depending on whether the network of the destination host is directly connected to the router, there are the following types of routes:

- 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 29, 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 29 The routing table



The routing table of router R8

Destination host location	Forwarding router	Port passed
10.0.0.0	Directly	2
11.0.0.0	Directly	1
12.0.0.0	11.0.0.2	1
13.0.0.0	Directly	3
14.0.0.0	13.0.0.2	3
15.0.0.0	10.0.0.2	2
16.0.0.0	10.0.0.2	2

Routing Management Policy

The Switch 5500G-EI supports the configuration of a series of dynamic routing protocols such as RIP and OSPF, as well as static routes. The static routes configured by the user are managed together with the dynamic routes as detected by the routing protocol. The static routes and the routes learned or configured by routing protocols can be shared with each other.

Routing Protocols and Route Preferences

Routing protocols (including static configurations) 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 configurations) 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 107. The smaller the value, the higher the preference).

Table 107 Routing Protocols and the Default Preferences for Routes

Routing protocol or route type	The preference of the corresponding route
DIRECT	0
OSPF	10
ISIS	15
STATIC	60
RIP	100
OSPF ASE	150
OSPF NSSA	150

Table 107 Routing Protocols and the Default Preferences for Routes

Routing protocol or route type	The preference of the corresponding route
IBGP	256
EBGP	256
UNKNOWN	255

In Table 107, 0 indicates a direct route, and 255 indicates any route from an unreliable source.

Except for direct routing and BGP (IBGP and EBGP), 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

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 5500G-EI supports three routes to implement load sharing.

II. Route backup

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 5500G-EI can import the information of another routing protocol. Each protocol has its own route redistribution mechanism. For details, refer to "Enabling RIP to

Import Routes of Other Protocols" on page 125, "Configuring OSPF to Import the Default Route" on page 146 and "Importing Routing Information Discovered by Other Routing Protocols" on page 158.

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.

Static Routes configuration is described in the following sections:

- Configuring Static Routes
- Troubleshooting Static Routes

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 108 Configuring a static route

Operation	Command
Add a static route	**ip route-static** *ip_address* { *mask* | *mask_length* } { *interface_type interface_number* | *gateway_address* } [**preference** *value*] [**reject** | **blackhole**]
Delete a static route	**undo ip route-static** *ip_address* { *mask* | *mask_length* } [*interface_type interface_number* | *gateway_address*] [**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 an 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 109 Configuring a default route

Operation	Command
Configure a default route	**ip route-static** 0.0.0.0 { 0.0.0.0 | 0 } { *interface_type interface_number* | *gateway_address* } [**preference** *value*] [**reject** | **blackhole**]
Delete a default route	**undo ip route-static** 0.0.0.0 { 0.0.0.0 | 0 } [*interface_type interface_number* | *gateway_address*] [**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 5500G-EI 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 110 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 111 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**

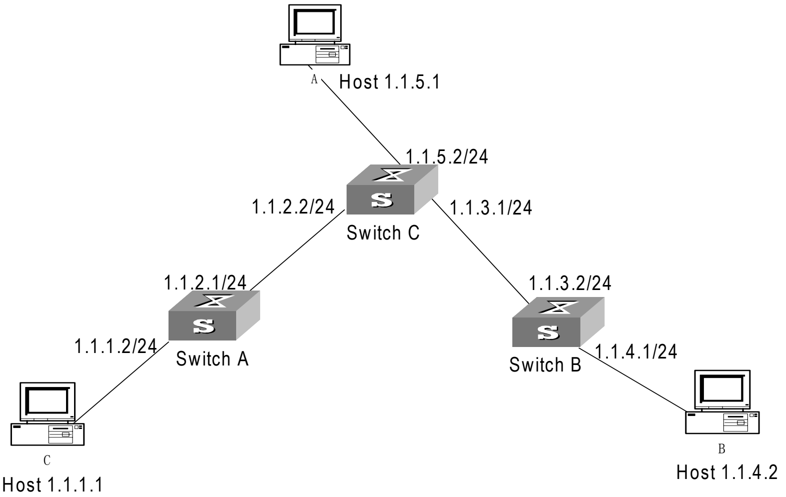
Example: Typical Static Route Configuration

Networking Requirements

The masks of all the IP addresses shown in Figure 30 are 255.255.255.0. All the hosts or switches must be interconnected in pairs by configuring static routes.

Networking Diagram

Figure 30 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 1.1.5.2

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 1.1.1.2

Using this procedure, all the hosts or switches in Figure 30 can be interconnected in pairs.

Troubleshooting Static Routes

The Switch 5500G-EI 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.
- Output 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.
- Route tag — The indication whether the route is generated by an interior routing protocol or by an exterior routing protocol.

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.
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
- Enabling 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
- Configuring Traffic Sharing Across RIP Interfaces

Enabling RIP and Entering the RIP View

Perform the following configurations in System View

Table 112 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 113 Enabling RIP Interface

Operation	Command
Enable RIP on the specified network	**`network`** *`network_address`*
Disable RIP on the specified network	**`undo network`** *`network_address`*

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. To exchange routing information with a non-broadcast network, unicast transmission mode must be used.

Perform the following configuration in the RIP View.

Table 114 Configuring unicast RIP messages

Operation	Command
Configure unicast RIP message	**`peer`** *`ip_address`*
Cancel unicast RIP message	**`undo peer`** *`ip_address`*

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 115 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 RFC1058, 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 116 Configuring RIP timers

Operation	Command
Configure RIP timers	**timers** { **update** *update_timer_length* | **timeout** *timeout_timer_length* } *
Restore the default settings of RIP	**undo timers** { **update** | **timeout** } *

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 RFC1058, 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 117 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 118 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 119 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 120 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 121 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 122 Configuring Split Horizon

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

By default, split horizon is enabled.

Enabling 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 routes from protocols including direct, static and OSPF.

Perform the following configurations in RIP View.

Table 123 Enabling RIP to Import Routes of Other Protocols

Operation	Command
Enable RIP to import routes of other protocols	**import-route** *protocol* [**cost** *value*] [**route-policy** *route_policy_name*]
Disable route imports from other protocols	**undo import-route** *protocol*

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

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 124 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 125 Setting the RIP Preference

Operation	Command
Set the RIP Preference	**preference** *value*
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 126 Setting Additional Routing Metrics

Operation	Command
Set the additional routing metric of the route when the interface receives an RIP packet	**rip metricin** *value*
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** *value*
Disable the additional routing metric of the route when the interface sends an RIP packet	**undo rip 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 127 Configuring RIP to Filter the Received Routes

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

Configuring RIP to Filter the Distributed Routes

Table 128 Configuring RIP to Filter the Distributed Routes

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

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.*

Configuring Traffic Sharing Across RIP Interfaces

Equivalent routes indicates that there is one destination address and multiple next-hop routes in the routing table. If RIP traffic sharing among the interfaces is enabled, then traffic can be distributed equally among interfaces by employing equivalent routes.

Table 129 Configuring RIP to Filter the Distributed Routes

Configuration Item	Command	Description
Enter System view	**system-view**	
Enter RIP view	**rip**	
Enter RIP traffic sharing among interfaces	**traffic-share-across -interface**	Required by default, RIP traffic sharing among interfaces is disabled

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 130 Displaying and Debugging RIP

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

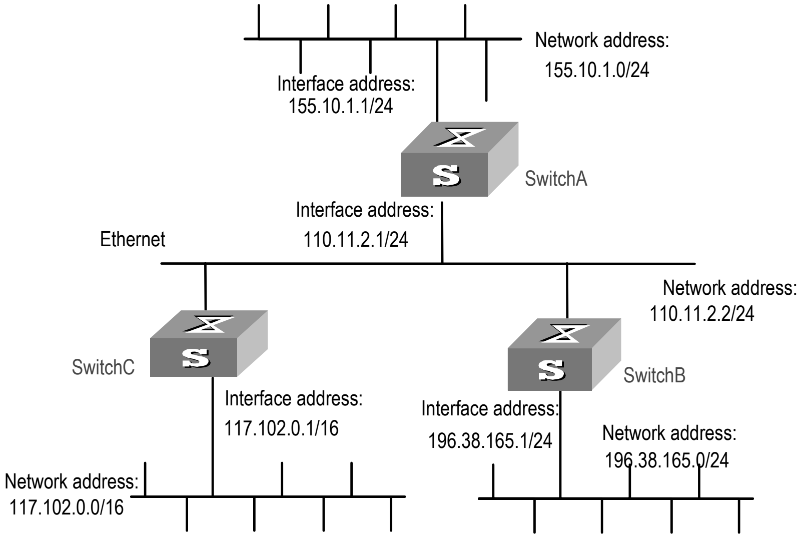
Example: Typical RIP Configuration

Networking Requirements

As shown in Figure 31, 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 31 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.

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 5500G-EI 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.

OSPF Configuration

Open Shortest Path First (OSPF) is an Interior Gateway Protocol based on the link state developed by IETF.

The Switch 5500G-EI uses OSPF version 2 (RFC2328), which has the following features:

- Scope — Supports networks of various sizes and can support several hundred routers.
- Fast convergence — Transmits the update packets instantly after the network topology changes so that the change is synchronized in the AS.
- Loop-free — Calculates routes with the shortest path tree algorithm, according to the collected link states, so that no loop routes are generated from the algorithm itself.
- Area partition — Allows the network of AS to be divided into different areas for management convenience, so that the routing information that is transmitted between the areas is further abstracted to reduce network bandwidth consumption.
- Equal-cost multi-route — Supports multiple equal-cost routes to a destination.
- Routing hierarchy — Supports a four-level routing hierarchy that prioritizes the routes into intra-area, inter-area, external type-1, and external type-2 routes.
- Authentication — Supports interface-based packet authentication to guarantee the security of the route calculation.
- Multicast transmission — Uses multicast address to receive and send packets.

Calculating OSPF Routes

The OSPF protocol calculates routes as follows:

- Each OSPF-capable router maintains a Link State Database (LSDB), which describes the topology of the entire AS. Depending on the surrounding network topology, each router generates a Link State Advertisement (LSA). The routers on the network transmit the LSAs among themselves by transmitting the protocol packets to each other. In this way, each router receives the LSAs of other routers and all these LSAs constitute its LSDB.
- LSA describes the network topology around a router, so the LSDB describes the network topology of the entire network. Routers can easily transform the LSDB to a weighted directed graph, which actually reflects the topology of the whole network. All routers have the same graph.
- A router uses the SPF algorithm to calculate the shortest path tree which shows the routes to the nodes in the autonomous system. The external routing information is a leaf node. A router that advertises the routes, also tags them and records the additional information of the autonomous system. Therefore, the routing tables obtained from different routers are different.

OSPF supports interface-based packet authentication to guarantee the security of route calculation. OSPF also transmits and receives packets by IP multicast.

OSPF Packets

OSPF uses five types of packets:

- Hello Packet.

The Hello Packet is the most common packet sent by the OSPF protocol. A router periodically sends it to its neighbor. It contains the values of some timers, DR, BDR and the known neighbor.

- Database Description (DD) Packet.

  When two routers synchronize their databases, they use DD packets to describe their own LSDBs, including the digest of each LSA. The digest refers to the HEAD of an LSA, which can be used to uniquely identify the LSA. Synchronizing databases with DD packets reduces the traffic size transmitted between the routers, since the HEAD of a LSA only occupies a small portion of the overall LSA traffic. With the HEAD, the peer router can judge whether it already has had the LSA.

- Link State Request (LSR) Packet.

  After exchanging the DD packets, the two routers know which LSAs of the peer routers are missing from the local LSDBs. In this case, they send LSR packets to the peers, requesting the missing LSAs. The packets contain the digests of the missing LSAs.

- Link State Update (LSU) Packet.

  The LSU packet is used to transmit the needed LSAs to the peer router. It contains a collection of multiple LSAs (complete contents).

- Link State Acknowledgment (LSAck) Packet.

  The packet is used for acknowledging the received LSU packets. It contains the HEAD(s) of LSA(s) requiring acknowledgement.

Basic Concepts Related to OSPF

- Router ID

  To run OSPF, a router must have a router ID. If no ID is configured, the system automatically selects an IP address from the IP addresses of the current interface as the Router ID. How a router ID is chosen: if the LoopBack interface address exists, the system chooses the LoopBack address with the greatest IP address value as the router ID; if no LoopBack interface configured, then the address of the physical interface with the greatest IP address value will be the router ID.

- Designated Router (DR)

  In multi-access networks, if any two routers establish adjacencies, the same LSA will be transmitted repeatedly, wasting bandwidth resources. To solve this problem, the OSPF protocol regulates that a DR must be elected in a multi-access network and only the DR (and the BDR) can establish adjacencies with other routers in this network. Two non-DR routers or non-BDR routers cannot establish adjacencies and exchange routing information.

  When the DR is not manually specified, the DR is elected by all the routers in the segment. See "Setting the Interface Priority for DR Election" on page 136.

- Backup Designated Router (BDR)

  If the DR fails, a new DR must be elected and synchronized with the other routers on the segment. This process will take a relatively long time, during which the route calculation is incorrect. To shorten the process, OSPF creates a BDR as backup for the DR. A new DR and BDR are elected in the meantime. The adjacencies are also established between the BDR and all the routers on the segment, and routing information is also exchanged between them. After the existing DR fails, the BDR will immediately becomes a DR.

- Area

  If all routers on a large network are running OSPF, the large number of routers results in an enormous LSD, which consumes storage space, complicates the SPF algorithm, and adds CPU load. Furthermore, as a network grows larger, the topology becomes more likely to change. Hence, the network is always in "turbulence", and a large number of OSPF packets are generated and transmitted in the network. This shrinks network bandwidth. In addition, each change causes all the routers on the network to recalculate the routes.

  OSPF solves this problem by dividing an AS into different areas. Areas logically group the routers, which form the borders of each area. Thus, some routers may belong to different areas. A router that connects the backbone area and a non-backbone area is called an area border router (ABR). An ABR can connect to the backbone area physically or logically.

- Backbone Area

  After the area division of OSPF, one area is different from all the other areas. Its area-id is 0 and it is usually called the backbone area.

- Virtual link

  As all the areas should be connected to the backbone area, virtual link is adopted so that the physically separated areas can still maintain logical connectivity to the backbone area.

- Route Summary

  An AS is divided into different areas that are interconnected via OSPF ABRs. The routing information between areas can be reduced by use of a route summary. Thus, the size of routing table can be reduced and the calculation speed of the router can be improved. After calculating an intra-area route of an area, the ABR summarizes multiple OSPF routes into an LSA and sends it outside the area according to the configuration of the summary.

Configuring OSPF

You must first enable OSPF then specify the interface and area ID before configuring other functions. However, the configuration of functions that are related to the interface does not depend on whether OSPF is enabled. If OSPF is disabled, the OSPF-related interface parameters become invalid.

OSPF configuration includes tasks that are described in the following sections:

- Enabling OSPF and Entering OSPF View
- Entering OSPF Area View
- Specifying the Interface
- Configuring a Router ID
- Configuring the Network Type on the OSPF Interface
- Configuring the Cost for Sending Packets on an Interface
- Setting the Interface Priority for DR Election
- Setting the Peer
- Setting the Interval of Hello Packet Transmission

- Setting a Dead Timer for the Neighboring Routers
- Configuring an Interval Required for Sending LSU Packets
- Setting an Interval for LSA Retransmission between Neighboring Routers
- Setting a Shortest Path First (SPF) Calculation Interval for OSPF
- Configuring STUB Area of OSPF
- Configuring the NSSA of OSPF
- Configuring the Route Summarization of OSPF Area
- Configuring Summarization of Imported Routes by OSPF
- Configuring OSPF Virtual Link
- Configuring the OSPF Area to Support Packet Authentication
- Configuring OSPF Packet Authentication
- Configuring OSPF to Import Routes of Other Protocols
- Configuring Parameters for OSPF to Import External routes
- Configuring OSPF to Import the Default Route
- Setting OSPF Route Preference
- Configuring OSPF Route Filtering
- Configuring the Filling of the MTU Field When an Interface Transmits DD Packets
- Disabling the Interface to Send OSPF Packets
- Configuring OSPF and Network Management System (NMS)
- Resetting the OSPF Process

Enabling OSPF and Entering OSPF View

Perform the following configurations in System View.

Table 131 Enabling the OSPF process

Operation	Command
Enable the OSPF process	**ospf** [*process_id* [**router-id** *router_id*]]
Disable the OSPF process	**undo ospf** [*process_id*]

By default, OSPF is not enabled.

When enabling OSPF, note the following:

- By default, the OSPF process ID is 1.
- If a router is running multiple OSPF processes, 3Com recommends that you to use **router-id** in the command to specify different Router IDs for different processes.

Entering OSPF Area View

Perform the following configurations in OSPF View.

Table 132 Entering OSPF Area View

Operation	Command
Enter an OSPF Area View	**area** *area_id*
Delete a designated OSPF area	**undo area** *area_id*

area_id is the ID of the OSPF area, which can be a decimal integer or in IP address format.

Specifying the Interface

OSPF divides the AS into different areas. You must configure each OSPF interface to belong to a particular area, identified by an area ID. The areas transfer routing information between them through the ABRs.

In addition, parameters of all the routers in the same area should be identical. Therefore, when configuring the routers in the same area, please note that most configurations should be based on the area. An incorrect configuration can disable the neighboring routers from transmitting information, and lead to congestion or self-loop of the routing information.

Perform the following configuration in OSPF Area View.

Table 133 Specifying interface

Operation	Command
Specify an interface to run OSPF	**network** *ip_address ip_mask*
Disable OSPF on the interface	**undo network** *ip_address ip_mask*

You must specify the segment to which the OSPF will be applied after enabling OSPF.

ip-mask can be IP address mask or IP address wildcard shielded text (similar to the complement of the IP address mask).

Configuring a Router ID

A Router ID is a 32-bit unsigned integer that uniquely identifies a router within an AS. A Router ID can be configured manually. If a Router ID is not configured, the system selects the IP address of an interface automatically. When you set a Router ID manually, you must guarantee that the IDs of any two routers in the AS are unique. It is usual to set the router ID to be the IP address of an interface on the router.

Perform the following configurations in System View.

Table 134 Configuring a router ID

Operation	Command
Configure a Router ID	**router id** *router_id*
Remove the router ID	**undo router id**

To ensure the stability of OSPF, you must determine the division of router IDs and manually configure them when implementing network planning.

Configuring the Network Type on the OSPF Interface

The route calculation of OSPF is based upon the topology of the adjacent network of the local router. Each router describes the topology of its adjacent network and transmits it to all the other routers.

OSPF divides networks into four types by link layer protocol:

- Broadcast — If Ethernet or FDDI is adopted, OSPF defaults the network type to broadcast.
- Non-Broadcast Multi-access (NBMA) — If Frame Relay, ATM, HDLC or X.25 is adopted, OSPF defaults the network type to NBMA.
- Point-to-Multipoint (P2MP) — OSPF will not default the network type of any link layer protocol to P2MP. The usual policy is to change a partially connected NBMA network to a P2MP network, if the NBMA network is not fully connected.
- Point-to-point (P2P) — If PPP, LAPB or POS is adopted, OSPF defaults the network type to P2P.

As you configure the network type, consider the following points:

- NBMA means that a network is non-broadcast and multi-accessible. ATM is a typical example. You can configure the polling interval for hello packets before the adjacency of the neighboring routers is formed.
- Configure the interface type to nonbroadcast on a broadcast network without multi-access capability.
- Configure the interface type to P2MP if not all the routers are directly accessible on an NBMA network.
- Change the interface type to P2P if the router has only one peer on the NBMA network.

The differences between NBMA and P2MP are listed below:

- In OSPF, NBMA refers to the networks that are fully connected, non-broadcast and multi-accessible. However, a P2MP network is not required to be fully connected.
- DR and BDR are required on a NBMA network but not on a P2MP network.
- NBMA is the default network type. For example, if ATM is adopted as the link layer protocol, OSPF defaults the network type on the interface to NBMA, regardless of whether the network is fully connected. P2MP is not the default network type. No link layer protocols will be regarded as P2MP. You must change the network type to P2MP manually. The most common method is to change a partially connected NBMA network to a P2MP network.
- NBMA forwards packets by unicast and requires neighbors to be configured manually. P2MP forwards packets by multicast.

Perform the following configuration in Interface View:

Table 135 Configuring a Network Type on the Interface That Starts OSPF

Operation	Command
Configure network type on the interface	**ospf network-type** { **broadcast** | **nbma** | **p2mp** | **p2p** }

After the interface has been configured with a new network type, the original network type of the interface is removed automatically.

Configuring the Cost for Sending Packets on an Interface

You can control network traffic by configuring different message sending costs for different interfaces. Otherwise, OSPF automatically calculates the cost according to the baud rate on the current interface.

Perform the following configuration in Interface View:

Table 136 Configuring the cost for sending packets on the Interface

Operation	Command
Configure the cost for sending packets on Interface	**ospf cost** *value*
Restore the default cost for packet transmission on the Interface	**undo ospf cost**

For the Switch 5500G-EI the default cost for running OSPF protocol on the VLAN interface is 10.

Setting the Interface Priority for DR Election

The priority of the router interface determines the qualification of the interface for DR election. A router of higher priority will be considered first if there is a collision in the election.

DR is not designated manually; instead, it is elected by all the routers on the segment. Routers with the priorities greater than 0 in the network are eligible candidates. Among all the routers self-declared to be the DR, the one with the highest priority is elected. If two routers have the same priority, the one with the highest router ID will be elected as the DR. Each router writes the expected DR in the packet and sends it to all the other routers on the segment. If two routers attached to the same segment concurrently declare themselves to be the DR, the one with higher priority is elected DR. If the priorities are the same, the router with the higher router ID is elected DR. If the priority of a router is 0, it will not be elected as DR or BDR.

If DR fails, the routers on the network must elect a new DR and synchronize with the new DR. The process takes a relatively long time, during which route calculation can be incorrect. To speed up this DR replacement process, OSPF implements the BDR as backup for DR. The DR and BDR are elected at the same time. The adjacencies are also established between the BDR and all the routers on the segment, and routing information is exchanged between them. When the DR fails, the BDR becomes the DR. Since no re-election is needed and the adjacencies have already been established, the process is very quick. But in this case, a new BDR should be elected. Although it also takes a long time, it does not influence route calculation.

Note that:

- The DR on the network is not necessarily the router with the highest priority. Likewise, the BDR is not necessarily the router with the second highest priority. If a new router is added after DR and BDR election, it is impossible for the router to become the DR even if it has the highest priority.
- The DR is based on the router interface in a certain segment. A router can be a DR on one interface, and a BDR or DROther on another interface.
- DR election is only required for the broadcast or NBMA interfaces. For P2P or P2MP interfaces, DR election is not required.

Perform the following configuration in Interface View:

Table 137 Setting the Interface Priority for DR Election

Operation	Command
Configure the interface with a priority for DR election	**`ospf dr-priority`** *`priority_num`*
Restore the default interface priority	**`undo ospf dr-priority`**

By default, the priority of the Interface is 1 in the DR election. The value can be taken from 0 to 255.

Setting the Peer

In an NBMA network, some special configurations are required. Since an NBMA interface on the network cannot discover the adjacent router through broadcasting Hello packets, you must manually specify an IP address for the adjacent router for the interface, and whether the adjacent router is eligible for election. This can be done by configuring the **`peer`** *`ip_address`* command.

Perform the following configuration in OSPF View.

Table 138 Configuring the peer

Operation	Command
Configure a peer for the NBMA interface	**`peer`** *`ip_address`* `[` **`dr-priority`** *`dr_priority_number`* `]`
Remove the configured peer for the NBMA interface	**`undo peer`** *`ip_address`*

By default, the preference for the neighbor of NBMA interface is 1.

Setting the Interval of Hello Packet Transmission

Hello packets are the most frequently sent packets. They are periodically sent to the adjacent router for discovering and maintaining adjacency, and for electing a DR and BDR. The user can set the hello timer.

According to RFC2328, the consistency of hello intervals between network neighbors should be kept. The hello interval value is in inverse proportion to the route convergence rate and network load.

Perform the following configuration in Interface View

Table 139 Setting Hello Timer and Poll Interval

Operation	Command
Set the hello interval of the interface	**`ospf timer hello`** *`seconds`*
Restore the default hello of the interface	**`undo ospf timer hello`**
Set the poll interval on the NBMA interface	**`ospf timer poll`** *`seconds`*
Restore the default poll interval	**`undo ospf timer poll`**

By default, P2P and broadcast interfaces send Hello packets every 10 seconds, and P2MP and NBMA interfaces send Hello packets every 30 seconds.

Setting a Dead Timer for the Neighboring Routers

If hello packets are not received from a neighboring router, that router is considered dead. The dead timer of neighboring routers refers to the interval after which a router considers a neighboring router dead. You can set a dead timer for the neighboring routers.

Perform the following configuration in Interface View:

Table 140 Setting a Dead Timer for the Neighboring Routers

Operation	Command
Configure a dead timer for the neighboring routers	**`ospf timer dead`** *`seconds`*
Restore the default dead interval of the neighboring routers	**`undo ospf timer dead`**

By default, the dead interval for the neighboring routers of P2P or broadcast interfaces is 40 seconds, and for the neighboring routers of P2MP or NBMA interfaces is 120 seconds.

Both hello and dead timers restore to the default values if you modify the network type.

Configuring an Interval Required for Sending LSU Packets

Trans-delay seconds should be added to the aging time of the LSA in an LSU packet. This parameter affects the time duration that the interface requires to transmit the packet.

You can configure the interval for sending LSU messages. This is more important on low speed networks.

Perform the following configuration in Interface View

Table 141 Configuring an Interval for LSU packets

Operation	Command
Configure an interval for sending LSU packets	**`ospf trans-delay`** *`seconds`*
Restore the default interval of sending LSU packets	**`undo ospf trans-delay`**

By default, the LSU packets are transmitted every second.

Setting an Interval for LSA Retransmission between Neighboring Routers

If a router transmits an LSA (Link State Advertisements) to the peer, it requires an acknowledgement packet from the peer. If it does not receive the acknowledgement packet within the retransmit time, it retransmits this LSA to the neighbor. You can configure the value of the retransmission interval.

Perform the following configuration in Interface View

Table 142 Setting an Interval for LSA Retransmission between Neighboring Routers

Operation	Command
Configure the interval of LSA retransmission for the neighboring routers	**`ospf timer retransmit`** *`interval`*
Restore the default LSA retransmission interval for the neighboring routers	**`undo ospf timer retransmit`**

By default, the interval for neighboring routers to retransmit LSAs is five seconds.

The value of *`interval`* should be bigger than the interval in which a packet can be transmitted and returned between two routers.

An LSA retransmission interval that is too small will cause unecessary retransmission.

Setting a Shortest Path First (SPF) Calculation Interval for OSPF

Whenever the OSPF LSDB changes, the shortest path requires recalculation. Calculating the shortest path after the change consumes enormous resources and affects the operating efficiency of the router. Adjusting the SPF calculation interval, however, can restrain the resource consumption due to frequent network changes.

Perform the following configuration in OSPF View.

Table 143 Setting the SPF calculation interval

Operation	Command
Set the SPF calculation interval	**`spf-schedule-interval`** *`seconds`*
Restore the SPF calculation interval	**`undo spf-schedule-interval`** *`seconds`*

By default, the interval for SPF recalculation is 5 seconds.

Configuring STUB Area of OSPF

STUB areas are special LSA areas in which the ABRs do not propagate the learned external routes of the AS. In these areas, the routing table sizes of routers and the routing traffic are significantly reduced.

The STUB area is an optional configuration attribute, but not every area conforms to the configuration condition. Generally, STUB areas, located at the AS boundaries, are those non-backbone areas with only one ABR. Even if this area has multiple ABRs, no virtual links are established between these ABRs.

To ensure that the routes to destinations outside the AS are still reachable, the ABR in this area will generate a default route (0.0.0.0) and advertise it to the non-ABR routers in the area.

Note the following items when you configure a STUB area:

- The backbone area cannot be configured as a STUB area, and virtual links cannot pass through the STUB area.
- If you want to configure an area as a STUB area, all the routers in this area should be configured with the **stub** command.
- No ASBR can exist in a STUB area, and the external routes of the AS cannot be propagated in the STUB area.

Perform the following configuration in OSPF Area View.

Table 144 Configuring and OSPF STUB area

Operation	Command
Configure an area to be the STUB area	**stub** [**no-summary**]
Remove the configured STUB area	**undo stub**
Configure the cost of the default route transmitted by OSPF to the STUB area	**default-cost** *value*
Remove the cost of the default route to the STUB area	**undo default-cost**

By default, the STUB area is not configured, and the cost of the default route to the STUB area is 1.

Configuring the NSSA of OSPF

To keep the advantages of stub areas and simultaneously improve the networking flexibility, RFC1587 (OSPF NSSA Option) defines a new type of area, namely NSSA, which has the capability of importing external routes in a limited way.

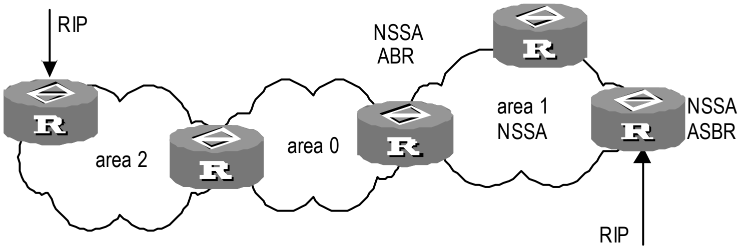
An NSSA is similar to a Stub area. Neither of them generates or imports AS-External-LSA (namely Type-5 LSA), and both of them can generate and import Type-7 LSAs. Type-7 LSAs are generated by the ASBR of the NSSA area, which can only advertise in the NSSA area. When a Type-7 LSA reaches the ABR of the NSSA, the ABR decides whether to transform the Type-7 LSA into an AS-External-LSA so as to advertise it to other areas.

For example, in Figure 32, the AS running OSPF comprises three areas: Area 1, Area 2 and Area 0. Area 0 is the backbone area. There are another two ASs running RIP. Area 1 is defined as an NSSA. After the RIP routes of the Area 1 are propagated to the NSSA, ASBR generates type-7 LSAs which are propagated in Area 1. When a type-7 LSA reaches the NSSA ABR, the NSSA ABR transforms it into a type-5 LSA, which is propagated to Area 0 and Area 2.

RIP routes of the AS running RIP are translated into type-5 LSAs that are propagated in the OSPF AS. However, type-5 LSAs do not reach Area 1 because Area 1 is an NSSA. NSSA and STUB areas use the same policy in this respect.

The NSSA cannot be configured with virtual links.

Figure 32 NSSA area



Perform the following configuration in OSPF Area View.

Table 145 Configuring the NSSA of OSPF

Operation	Command
Configure an area to be the NSSA area	**nssa** [**default-route-advertise** | **no-import-route** | **no-summary**]*
Cancel the configured NSSA	**undo nssa**
Configure the default cost value of the route to the NSSA	**default-cost** *cost*
Restore the default cost value of the route to the NSSA area	**undo default-cost**

All the routers connected to the NSSA should use the **nssa** command to configure the area with the NSSA attributes.

The **default-route-advertise** parameter is used to generate the default type-7 LSAs. When **default-route-advertise** is configured, the default type-7 LSA route is generated on the ABR, even though the default route 0.0.0.0 is not in the routing table. On an ASBR, however, the default type-7 LSA route can be generated only if the default route 0.0.0.0 is in the routing table.

Executing the **no-import-route** command on the ASBR prevents the external routes that OSPF imported through the **import-route** command from advertising to the NSSA. Generally, if an NSSA router is both ASBR and ABR, this argument is used.

The **default-cost** command is used on the ABR attached to the NSSA. Using this command, you can configure the default route cost on the ABR to NSSA.

By default, the NSSA is not configured, and the cost of the default route to the NSSA is 1.

Configuring the Route Summarization of OSPF Area

Route summary means that ABR can aggregate information of routes of the same prefix and advertise only one route to other areas. An area can be configured with multiple aggregate segments allowing OSPF can summarize them. When the ABR transmits routing information to other areas, it will generate Sum_net_Lsa (type-3 LSA) per network. If continuous networks exist in this area, you can use the **abr-summary** command to summarize these segments into one segment. Thus, the ABR only needs to send an aggregate LSA, and all the LSAs in the range of the aggregate segment specified by the command are not transmitted separately.

Once the aggregate segment of a certain network is added to the area, all the internal routes of the IP addresses in the range of the aggregate segment will no longer be separately advertised to other areas. Only the route summary of the whole aggregate network will be advertised. But if the range of the segment is restricted by the parameter **`not-advertise`**, the route summary of this segment is not advertised. This segment is represented by IP address and mask.

Route summarization can take effect only when it is configured on ABRs.

Perform the following configuration in OSPF Area View.

Table 146 Configuring the route summarization of OSPF area

Operation	Command
Configure the Route Summarization of OSPF Area	**`abr-summary`** *`ip_address mask`* `[` **`advertise`** `|` **`not-advertise`** `]`
Cancel the route summarization of OSPF Area	**`undo abr-summary`** *`ip_address mask`*

By default, the inter-area routes will not be summarized.

Configuring Summarization of Imported Routes by OSPF

Perform the following configurations in OSPF View.

Table 147 Configuring summarization of imported routes by OSPF

Operation	Command
Configure summarization of imported routes by OSPF	**`asbr-summary`** *`ip_address mask`* `[` **`not-advertise`** `|` **`tag`** *`value`* `]`
Remove summarization of routes imported into OSPF	**`undo asbr-summary`** *`ip_address mask`*

By default, summarization of imported routes is disabled.

After the summarization of imported routes is configured, if the local router is an autonomous system border router (ASBR), this command summarizes the imported Type-5 LSAs in the summary address range. When NSSA is configured, this command will also summarize the imported Type-7 LSA in the summary address range.

If the local router works as an area border router (ABR) and a router in the NSSA, this command summarizes Type-5 LSAs translated from Type-7 LSAs. If the router is not the router in the NSSA, this summarization is disabled.

Configuring OSPF Virtual Link

According to RFC2328, after the area division of OSPF, the backbone is established with an area-id of 0.0.0.0. The OSPF routes between non-backbone areas are updated with the help of the backbone area. OSPF stipulates that all the non-backbone areas should maintain the connectivity with the backbone area, and at least one interface on the ABR should fall into the area 0.0.0.0. If an area does not have a direct physical link with the backbone area 0.0.0.0, a virtual link must be created.

If physical connectivity cannot be ensured due to the network topology restrictions, a virtual link can be used to meet the requirements of RFC2328. The virtual link refers to a logic channel set up through the area of a non-backbone internal route between two ABRs. Both ends of the logic channel should be ABRs and the connection can take effect only when both ends are configured. The virtual link is identified by the ID of the remote router. The area, which provides the ends of the virtual link with a non-backbone area internal route, is called the transit area. The ID of the transit area should be specified during configuration.

The virtual link is activated after the route passing through the transit area is calculated, which is equivalent to a P2P connection between two ends. Therefore, similar to the physical interfaces, you can also configure various interface parameters on this link, such as an hello timer.

The "logic channel" means that the multiple routers running OSPF between two ABRs only take the role of packet forwarding (the destination addresses of the protocol packets are not these routers, so these packets are transparent to them and the routers forward them as common IP packets). The routing information is directly transmitted between the two ABRs. The routing information refers to the type-3 LSAs generated by the ABRs, for which the synchronization mode of the routers in the area will not be changed.

Perform the following configuration in OSPF Area View.

Table 148 Configuring OSPF Virtual Link

Operation	Command
Create and configure a virtual link	**vlink-peer** *router_id* [**hello** *seconds* | **retransmit** *seconds* | **trans-delay** *seconds* | **dead** *seconds* | **simple** *password* | **md5** *keyid key*]*
Remove the created virtual link	**undo vlink-peer** *router_id*

The *area_id* and *router_id* have no default value.

By default, hello timer is 10 seconds, retransmit 5 seconds, trans-delay 1 second, and the dead timer is 40 seconds.

Configuring the OSPF Area to Support Packet Authentication

All the routers in an area must use the same authentication mode. In addition, all routers on the same segment must use the same authentication key password. Use the **authentication-mode simple** command to configure a simple authentication password for the area, and the **authentication-mode md5** command to configure the MD5 authentication password.

Perform the following configuration in OSPF Area View.

Table 149 Configuring the OSPF Area to Support Packet Authentication

Operation	Command
Configure the area to support authentication type	**authentication-mode** { **simple** | **md5** }
Cancel the authentication attribute of this area	**undo authentication-mode**

By default, the area does not support packet authentication.

Configuring OSPF Packet Authentication

OSPF supports simple authentication or MD5 authentication between neighboring routers.

Perform the following configuration in Interface View:

Table 150 Configuring OSPF Packet Authentication

Operation	Command
Specify a password for OSPF simple text authentication	**`ospf authentication-mode simple`** *`password`*
Cancel simple authentication on the interface	**`undo ospf authentication-mode simple`**
Specify the key-id and key for OSPF MD5 authentication	**`ospf authentication-mode md5`** *`key_id key`*
Disable the interface to use MD5 authentication	**`undo ospf authentication-mode md5`**

By default, the interface is not configured with either simple authentication or MD5 authentication.

Configuring OSPF to Import Routes of Other Protocols

The dynamic routing protocols on the router can share routing information. As far as OSPF is concerned, the routes discovered by other routing protocols are always processed as the external routes of AS. In the **`import-route`** commands, you can specify the route cost type, cost value and tag to overwrite the default route receipt parameters (refer to "Configuring Parameters for OSPF to Import External routes" on page 145).

The OSPF uses the following four types of routes (in priority):

- Intra-area route
- Inter-area route
- External route type 1
- External route type 2

Intra-area and inter-area routes describe the internal AS topology whereas the external routes describes how to select the route to the destinations beyond the AS.

The external type-1 routes refer to imported IGP routes (such as static route and RIP). Since these routes are more reliable, the calculated cost of the external routes is the same as the cost of routes within the AS. Also, this route cost and the route cost of the OSPF itself are comparable. That is, the cost to reach the external route type 1 equals the cost to reach the corresponding ASBR from the local router plus the cost to reach the destination address of the route from the ASBR

The external routes type-2 refer to the imported EGP routes. Since these routes typically have higher cost, OSPF assumes that the cost from the ASBR to reach the destinations beyond the AS is higher than the cost from within the AS to ASBR. So in route cost calculation, the cost from the ASBR to the destination is considered and the cost between the router and the ASBR is ignored. If the cost from the router to the ASBR and the cost from the ASBR to the destination are of the same size, then the cost of the router to the ASBR will also be included.

Perform the following configuration in OSPF View.

Table 151 Configuring OSPF to Import Routes of Other Protocols

Operation	Command
Configure OSPF to import routes of other protocols	**import-route** *protocol* [**cost** *value* | **type** *value* | **tag** *value* | **route-policy** *route_policy_name*]*
Cancel importing routing information of other protocols	**undo import-route** *protocol*

By default, OSPF does not import the routing information of other protocols. The default type of the imported route is 2, cost is 1 and the tag is 1.

The *protocol* variable specifies a source routing protocol that can be imported. This can be Direct, Static and RIP.

3Com recommends that you configure the route **type**, **cost** *and* **tag** *together in one command. If you do not, note that a new configuration overwrites the previous configuration.*

Configuring Parameters for OSPF to Import External routes

When the OSPF imports the routing information discovered by other routing protocols in the autonomous system, some additional parameters need to be configured, such as default route cost and default tag of route distribution, etc. Route ID can be used to identify the protocol-related information.

Perform the following configuration in OSPF View.

Table 152 Configuring Parameters for OSPF to Import External routes

Operation	Command
Configure the minimum interval for OSPF to import the external routes	**default interval** *seconds*
Restore the default value of the minimum interval for OSPF to import the external routes	**undo default interval**
Configure the upper limit to the routes that OSPF import each time	**default limit** *routes*
Restore the default upper limit to the external routes that can be imported at a time	**undo default limit**
Configure the default cost for the OSPF to import external routes	**default cost** *value*
Restore the default cost for the OSPF to import external routes	**undo default cost**
Configure the default tag for the OSPF to import external routes	**default tag** *tag*

Table 152 Configuring Parameters for OSPF to Import External routes

Operation	Command
Restore the default tag for the OSPF to import external routes	**undo default tag**
Configure the default type of external routes that OSPF will import	**default type** { **1** | **2** }
Restore the default type of the external routes imported by OSPF	**undo default type**

By default, when importing external routes, the type of imported route is type-2, the cost is 1 and the tag is 1. The interval of importing the external route is 1 second. The upper limit to the external routes imported is 1000 per second.

Configuring OSPF to Import the Default Route

The **import-route** command cannot be used to import the default route. Using the **default-route-advertise** command, you can import the default route into the routing table.

Perform the following configuration in OSPF View.

Table 153 Configuring OSPF to Import the Default Route

Operation	Command
Import the default route to OSPF	**default-route-advertise** [**always** | **cost** *value* | **type** *type_value* | **route-policy** *route_policy_name*]*
Remove the imported default route	**undo default-route-advertise** [**always** | **cost** | **type** | **route-policy**]*

By default, OSPF does not import the default route.

Setting OSPF Route Preference

Since it is possible for multiple dynamic routing protocols to run concurrently on one router, problems of route sharing and selection between various routing protocols can occur. The system sets a priority for each routing protocol, which will be used in tie-breaking in the case that different protocols discover the same route.

Perform the following configuration in OSPF View.

Table 154 Setting OSPF Route Preference

Operation	Command
Configure a priority for OSPF for comparing with the other routing protocols	**preference** [**ase**] *preference*
Restore the default protocol priority	**undo preference** [**ase**]

By default, the OSPF preference is 10, and the imported external routing protocol is 150.

Configuring OSPF Route Filtering

Perform the following configuration in OSPF View.

Configuring OSPF to Filter the Received Routes

Table 155 Enabling OSPF to filter the received routes

Operation	Command
Disable to filter the received global routing information	**filter-policy** { *acl_number* | **ip-prefix** *ip_prefix_name* | **gateway** *ip_prefix_name* } **import**
Cancel to filter the received global routing information	**undo filter-policy** { *acl_number* | **ip-prefix** *ip_prefix_name* | **gateway** *ip_prefix_name* } **import**

Configuring OSPF to filter the distributed routes

Table 156 Enabling OSPF to filter the distributed routes

Operation	Command
Enable OSPF to filter the distributed routes	**filter-policy** { *acl_number* | **ip-prefix** *ip_prefix_name* } **export** [*routing_process*]
Disable OSPF to filter the distributed routes	**undo filter-policy** { *acl_number* | **ip-prefix** *ip_prefix_name* } **export** [*routing_process*]

By default, OSPF will not filter the imported and distributed routing information.

- *The* **filter-policy import** *command only filters the OSPF routes of this process received from the neighbors, and routes that cannot pass the filter will not be added to the routing table. This command only takes effect on ABR.*
- *The* **filter-policy export** *command only takes effect to the routes imported by the* **import-route** *command. If you configure the Switch with only the* **filter-policy export** *command, but without configuring the* **import-route** *command to import other external routes (including OSPF routes of different process), then the* **filter-policy export** *command does not take effect.*

Configuring the Filling of the MTU Field When an Interface Transmits DD Packets

OSPF-running routers use the DD (Database Description) packets to describe their own LSDBs when synchronizing the databases.

You can manually specify an interface to fill in the MTU field in a DD packet when it transmits the packet. The MTU should be set to the real MTU on the interface.

Perform the following configuration in Interface View:

Table 157 Configuring the Filling of the MTU Field when an Interface Transmits DD Packets

Operation	Command
Enable an interface to fill in the MTU field when transmitting DD packets	**ospf mtu-enable**
Disable the interface to fill MTU when transmitting DD packets	**undo ospf mtu-enable**

By default, the interface does not fill in the MTU field when transmitting DD packets, and the MTU in the DD packets is 0.

Disabling the Interface to Send OSPF Packets

Use the **`silent-interface`** command to prevent the interface from transmitting OSPF packets.

Perform the following configuration in OSPF View.

Table 158 Disabling the interface to send OSPF packets

Operation	Command
Prevent the interface from sending OSPF packets	**`silent-interface`** *`silent_interface_type silent_interface_number`*
Allow the interface to send OSPF packets	**`undo silent-interface`** *`silent_interface_type silent_interface_number`*

By default, all the interfaces are allowed to transmit and receive OSPF packets.

After an OSPF interface is set to silent status, the interface can still advertise its direct route. However, the OSPF hello packets of the interface are blocked, and no neighboring relationship can be established on the interface. This enhances the ability of OSPF to adapt to the network, which can reduce the consumption of system resources. On a Switch, this command can disable/enable the specified VLAN interface to send OSPF packets.

Configuring OSPF and Network Management System (NMS)

Configuring OSPF MIB binding After multiple OSPF processes are enabled, you can configure to which OSPF process MIB is bound.

Perform the following configuration in System View.

Table 159 Configure OSPF MIB binding

Operation	Command
Configure OSPF MIB binding	**`ospf mib-binding`** *`process_id`*
Restore the default OSPF MIB binding	**`undo ospf mib-binding`**

By default, MIB is bound to the first enabled OSPF process.

Configuring OSPF TRAP You can configure the switch to send multiple types of SNMP TRAP packets in case of OSPF anomalies. In addition, you can configure the switch to send SNMP TRAP packets when a specific process is abnormal by specifying the process ID.

Perform the following configuration in System View.

Table 160 Enabling/disabling OSPF TRAP function

Operation	Command
Enable OSPF TRAP function	**snmp-agent trap enable ospf** [*process_id*] [**ifstatechange** | **virifstatechange** | **nbrstatechange** | **virnbrstatechange** | **ifcfgerror** | **virifcfgerror** | **ifauthfail** | **virifauthfail** | **ifrxbadpkt** | **virifrxbadpkt** | **txretransmit** | **viriftxretransmit** | **originatelsa** | **maxagelsa** | **lsdboverflow** | **lsdbapproachoverflow**]
Disable OSPF TRAP function	**undo snmp-agent trap enable ospf** [*process_id*] [**ifstatechange** | **virifstatechange** | **nbrstatechange** | **virnbrstatechange** | **ifcfgerror** | **virifcfgerror** | **ifauthfail** | **virifauthfail** | **ifrxbadpkt** | **virifrxbadpkt** | **txretransmit** | **viriftxretransmit** | **originatelsa** | **maxagelsa** | **lsdboverflow** | **lsdbapproachoverflow**]

By default, OSPF TRAP function is disabled, so the switch does not send TRAP packets when any OSPF process is abnormal. The configuration is valid to all OSPF processes if you do not specify a process ID.

For detailed configuration of SNMP TRAP, refer to “System Management" on .

Resetting the OSPF Process

If the **undo ospf** command is executed on a router and then the **ospf** command is used to restart the OSPF process, the previous OSPF configuration is lost. With the **reset ospf** command, you can restart the OSPF process without losing the previous OSPF configuration.

Perform the following configuration in User View.

Table 161 Resetting the OSPF process

Operation	Command
Reset the OSPF process	**reset ospf** [statistics] { all | *process_id* }

Resetting the OSPF process can immediately clear the invalid LSAs, make the modified Router ID effective or re-elect the DR and BDR.

Displaying and Debugging OSPF

After the above configuration, execute **display** command in any view to display the operation of the OSPF configuration, and to verify the effect of the configuration. Execute the **debugging** command in User View to debug the OSPF module.

Table 162 Displaying and debugging OSPF

Operation	Command
Display the brief information of the OSPF routing process	**display ospf** [*process_id*] **brief**
Display OSPF statistics	**display ospf** [*process_id*] **cumulative**
Display LSDB information of OSPF	**display ospf** [*process_id*] [*area_id*] **lsdb** [**brief** | [**asbr** | **ase** | **network** | **nssa** | **router** | **summary**] [*ip_address*] [**originate-router** *ip_address* | **self-originate**]]
Display OSPF peer information	**display ospf** [*process_id*] **peer** [**brief**]
Display OSPF next hop information	**display ospf** [*process_id*] **nexthop**
Display OSPF routing table	**display ospf** [*process_id*] **routing**
Display OSPF virtual links	**display ospf** [*process_id*] **vlink**
Display OSPF request list	**display ospf** [*process_id*] **request-queue**
Display OSPF retransmission list	**display ospf** [*process_id*] **retrans-queue**
Display the information of OSPF ABR and ASBR	**display ospf** [*process_id*] **abr-asbr**
Display the summary information of OSPF imported route	**display ospf** [*process_id*] **asbr-summary** [*ip_address mask*]
Display OSPF interface information	**display ospf** [*process_id*] **interface**
Display OSPF errors	**display ospf** [*process_id*] **error**

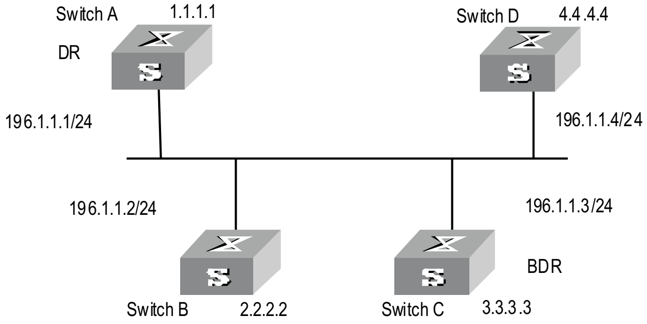
Example: Configuring DR Election Based on OSPF Priority

Networking Requirements

In this example, four Switch 5500G-EIs, Switch A, Switch B, Switch C and Switch D, which can perform the router functions and run OSPF, are located on the same segment, as shown Figure 33

Networking Diagram

Figure 33 Networking for configuring DR election based on OSPF priority



The commands listed in the following examples enable Switch A and Switch C to be DR and BDR, respectively. The priority of Switch A is 100, which is the highest on the network, so it is elected as the DR. Switch C has the second highest priority, so it is elected as the BDR. The priority of Switch B is 0, which means that it cannot be elected as the DR, and Switch D does not have a priority, and therefore takes priority 1 by default.

Configuration Procedure

1 Configure Switch A:

```
[Switch A]interface Vlan-interface 1
[Switch A-Vlan-interface1]ip address 196.1.1.1 255.255.255.0
[Switch A-Vlan-interface1]ospf dr-priority 100
[Switch A]router id 1.1.1.1
[Switch A]ospf
[Switch A-ospf-1]area 0
[Switch A-ospf-1-area-0.0.0.0]network 196.1.1.0 0.0.0.255
```

2 Configure Switch B:

```
[Switch B]interface Vlan-interface 1
[Switch B-Vlan-interface1]ip address 196.1.1.2 255.255.255.0
[Switch B-Vlan-interface1]ospf dr-priority 0
[Switch B]router id 2.2.2.2
[Switch B]ospf
[Switch B-ospf-1]area 0
[Switch B-ospf-1-area-0.0.0.0]network 196.1.1.0 0.0.0.255
```

3 Configure Switch C:

```
[Switch C]interface Vlan-interface 1
[Switch C-Vlan-interface1]ip address 196.1.1.3 255.255.255.0
[Switch C-Vlan-interface1]ospf dr-priority 2
[Switch C]router id 3.3.3.3
[Switch C]ospf
[Switch C-ospf-1]area 0
[Switch C-ospf-1-area-0.0.0.0]network 196.1.1.0 0.0.0.255
```

4 Configure Switch D:

```
[Switch D]interface Vlan-interface 1
[Switch D-Vlan-interface1]ip address 196.1.1.4 255.255.255.0
[Switch D]router id 4.4.4.4
[Switch D]ospf
```

```
[Switch D-ospf-1]area 0
[Switch D-ospf-1-area-0.0.0.0]network 196.1.1.0 0.0.0.255
```

On Switch A, run the **`display ospf peer`** command to show the Switch's OSPF neighbors. Note that Switch A has three neighbors.

The status of each neighbor is full, which means that adjacency is set up between Switch A and each neighbor. Switch A and Switch C should be set up with adjacencies to all the routers on the network so that they can serve as the DR and BDR on the network. Switch A is DR, while Switch C is BDR on the network. All the other neighbors are DROthers (which means that they are neither DRs nor BDRs).

5 Modify the priority of Switch B to 200:

```
[Switch B-Vlan-interface2000]ospf dr-priority 200
```

Execute the **`display ospf peer`** command on Switch A to show its OSPF neighbors. Please note the priority of Switch B has been modified to 200, but it is still not the DR.

Only when the current DR is offline does the DR change. Shut down Switch A, and run **`display ospf peer`** command on Switch D to display its neighbors. Note that the original BDR (Switch C) becomes the DR, and Switch B is the new BDR.

If all Ethernet Switches on the network are removed and added again, Switch B is elected as the DR (with a priority of 200), and Switch A becomes the BDR (with a priority of 100). Switching off and restarting all the switches initiates a new round of DR and BDR selection.

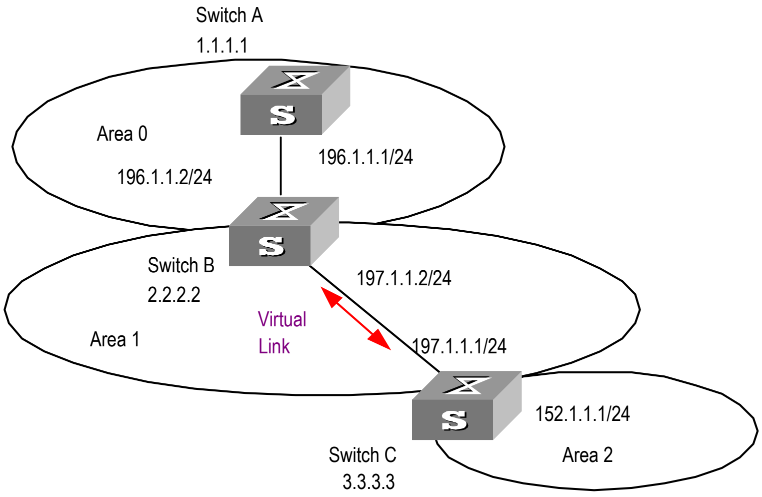
Example: Configuring OSPF Virtual Link

Networking requirements

In Figure 34, Area 2 and Area 0 are not directly connected. Area 1 is used as the transit area for connecting Area 2 and Area 0.

Networking diagram

Figure 34 OSPF virtual link configuration networking



The following commands configure a virtual link between Switch B and Switch C in Area 1.

Configuration procedure

1 Configure Switch A:

```
[Switch A]interface Vlan-interface 1
[Switch A-Vlan-interface1]ip address 196.1.1.1 255.255.255.0
[Switch A]router id 1.1.1.1
[Switch A]ospf
[Switch A-ospf-1]area 0
[Switch A-ospf-1-area-0.0.0.0]network 196.1.1.0 0.0.0.255
```

2 Configure Switch B:

```
[Switch B]interface vlan-interface 7
[Switch B-Vlan-interface7]ip address 196.1.1.2 255.255.255.0
[Switch B]interface vlan-interface 8
[Switch B-Vlan-interface8]ip address 197.1.1.2 255.255.255.0
[Switch B]router id 2.2.2.2
[Switch B]ospf
[Switch B-ospf-1]area 0
[Switch B-ospf-1-area-0.0.0.0]network 196.1.1.0 0.0.0.255
[Switch B-ospf-1-area-0.0.0.0]quit
[Switch B-ospf-1]area 1
[Switch B-ospf-1-area-0.0.0.1]network 197.1.1.0 0.0.0.255
[Switch B-ospf-1-area-0.0.0.1]vlink-peer 3.3.3.3
```

3 Configure Switch C:

```
[Switch C]interface Vlan-interface 1
[Switch C-Vlan-interface1]ip address 152.1.1.1 255.255.255.0
[Switch C]interface Vlan-interface 2
[Switch C-Vlan-interface2]ip address 197.1.1.1 255.255.255.0
[Switch C]router id 3.3.3.3
[Switch C]ospf
[Switch C-ospf-1]area 1
```

```
[Switch C-ospf-1-area-0.0.0.1]network 197.1.1.0 0.0.0.255
[Switch C-ospf-1-area-0.0.0.1]vlink-peer 2.2.2.2
[Switch C-ospf-1-area-0.0.0.1]quit
[Switch C-ospf-1]area 2
[Switch C-ospf-1-area-0.0.0.2]network 152.1.1.0 0.0.0.255
```

Troubleshooting OSPF

OSPF has been configured in accordance with the above-mentioned steps, but OSPF does not run normally on the router

Troubleshooting locally: Check whether the protocol between two directly connected routers is operating normally. The normal sign is the peer state machine between the two routers reaching the FULL state.

On a broadcast or NBMA network, if the interfaces for two routers are in DROther state, the peer state machine for the two routers are in 2-way state, instead of FULL state. The peer state machine between DR/BDR and all the other routers is in FULL state.

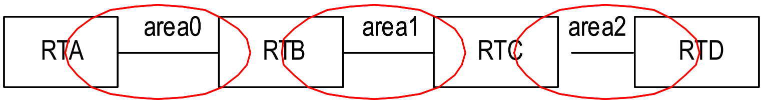
- Execute the **display ospf peer** command to view neighbors.
- Execute the **display ospf interface** command to view OSPF information in the interface.
- Use the **ping** command to check whether the physical link and the lower level protocol are normal. If the local router cannot ping the peer router, this indicates that faults have occurred on the physical link and the lower level protocol.
- If the physical link and the lower level protocol are normal, please check the OSPF parameters configured on the interface. The parameters should be the same parameters configured on the router adjacent to the interface. The same area ID should be used, and the networks and the masks should also be consistent. (The P2P or virtually linked segment can have different segments and masks.)
- Ensure that the dead timer on the same interface is at least four times the value of the hello timer.
- If the network type is NBMA, the peer must be manually specified, using the **peer ip-address** command.
- If the network type is broadcast or NBMA, there must be at least one interface with a priority greater than zero.
- If an area is set as the STUB area to which the routers are connected, the area on these routers must be also set as the STUB area.
- The same interface type must be adopted for neighboring routers.
- If more than two areas are configured, at least one area should be configured as the backbone area with an ID of 0.
- Ensure the backbone area connects with all other areas.
- The virtual links cannot pass through the STUB area.

Troubleshooting globally: If OSPF cannot discover the remote routes and you have checked all troubleshooting items listed above, check the following configurations:

- If more than two areas are configured on a router, at least one area should be configured as the backbone area.

  As shown in Figure 35, RTA and RTD are each configured to belong to only one area, whereas RTB and RTC are both configured to belong to two areas. RTB belongs to area0, which is compliant with the requirement. However, RTC does not belong to area0. Therefore, a virtual link must be set up between RTC and RTB to ensure that area2 and area0 (the backbone area) are connected.

Figure 35 OSPF areas



- The backbone area (area 0) cannot be configured as a STUB area and the virtual link cannot pass through the STUB area. So if a virtual link has been set up between RTB and RTC, neither area1 nor area0 can be configured as a STUB area. In Figure 35, only area 2 can be configured as stub area.
- Routers in the STUB area cannot redistribute the external routes.
- The backbone area must guarantee the connectivity of all nodes.

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 5500G-EI 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
- Configuring the Filtering of Received Routes
- Configuring the Filtering of Distributed Routes

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 163 Defining a route-policy

Operation	Command
Enter Route Policy View	**route-policy** *route_policy_name* { **permit** | **deny** } **node** { *node_number* }
Remove the specified route-policy	**undo route-policy** *route_policy_name* [**permit** | **deny** | **node** *node_number*]

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 164 Defining if-match Conditions

Operation	Command
Match the destination address of the routing information	**if-match** { **acl** *acl_number* | **ip-prefix** *ip_prefix_name* }
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**{ *interface_type_ interface_number* }
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** *acl_number* | **ip-prefix** *ip_prefix_name* **}**
Cancel the matched next-hop of the routing information set by ACL	**undo if-match ip next-hop**

Table 164 Defining if-match Conditions

Operation	Command
Cancel the matched next-hop of the routing information set by the address prefix list	**undo if-match ip next-hop ip-prefix**
Match the routing cost of the routing information	**if-match cost** *cost*
Cancel the matched routing cost of the routing information	**undo if-match cost**
Match the tag domain of the OSPF routing information	**if-match tag** *value*
Cancel the tag domain of the matched OSPF routing information	**undo if-match tag**

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 165 Defining Apply Clauses

Operation	Command
Set the routing cost of the routing information	**apply cost** *value*
Cancel the routing cost of the routing information	**undo apply cost**
Set the tag domain of the OSPF routing information	**apply tag** *value*
Cancel the tag domain of the OSPF routing information	**undo apply tag**

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.

Perform the following configuration in Routing Protocol View.

Table 166 Configuring to import the routes of other protocols

Operation	Command
Import routes of other protocols	**import-route** *protocol* [**cost** *cost*] [**tag** *value*] **type** { **1** | **2** } [**route-policy** *route_policy_name*]
Do not import routes of other protocols	**undo import-route** *protocol*

By default, the routes discovered by other protocols will not be distributed.

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 167 Defining Prefix-list

Operation	Command
Define a Prefix-list	**ip ip-prefix** *ip_prefix_name* [**index** *index_number*] { **permit** | **deny** } *network len* [**greater-equal** *greater_equal*] [**less-equal** *less_equal*]
Remove a Prefix-list	**undo ip ip-prefix** *ip_prefix_name* [**index** *index_number* | **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.

Configuring the Filtering of Received Routes

Perform the following configuration in Routing Protocol View.

Define a policy that filters the routing information that does not satisfy the conditions and receives routes with the help of an ACL or address prefix-list. The

filter-policy gateway command specifies that only the update packets from a specific neighboring router will be received.

Table 168 Configuring the Filtering of Received Routes

Operation	Command
Configure to filter the received routing information distributed by the specified address	**filter-policy gateway** *ip_prefix_name* **import**
Cancel the filtering of the received routing information distributed by the specified address	**undo filter-policy gateway** *ip_prefix_name* **import**
Configure to filter the received global routing information	**filter-policy** { *acl_number* | **ip-prefix** *ip_prefix_name* } [**gateway**] **import**
Cancel the filtering of the received global routing information	**undo filter-policy** { *acl_number* | **ip-prefix** *ip_prefix_name* } [**gateway**] **import**

By default, the filtering of received routes is not performed.

Configuring the Filtering of Distributed Routes

Define a policy concerning route distribution that filters the routing information that does not satisfy the conditions, and distributes routes with the help of an ACL or address ip-prefix.

Perform the following configuration in Routing Protocol View.

Table 169 Configuring to filter the distributed routes

Operation	Command
Configure to filter the routes distributed by the protocol	**filter-policy** { *acl_number* | **ip-prefix** *ip_prefix_name* } **export** [*routing_process*
Cancel the filtering of the routes distributed by the protocol	**undo filter-policy** { *acl_number* | **ip-prefix** *ip_prefix_name* } **export** [*routing_process*]

The route policy supports importing the routes discovered by the following protocols into the routing table:

- Direct — The hop (or host) to which the local interface is directly connected.
- Static — Static Route Configuration
- RIP — Route discovered by RIP
- OSPF — Route discovered by OSPF
- OSPF-ASE — External route discovered by OSPF
- OSPF-NSSA — NSSA route discovered by OSPF

By default, the filtering of distributed routes is not performed.

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 170 Displaying and Debugging the Routing Policy

Operation	Command
Display the routing policy	**display route-policy** [*route_policy_name*]
Display the address prefix list information	**display ip ip-prefix** [*ip_prefix_name*]

Typical IP Routing Policy Configuration Example

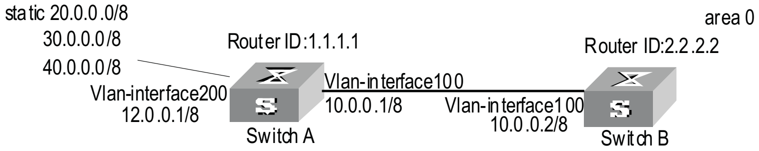
Configuring the Filtering of the Received Routing Information

Networking Requirements

- Switch A communicates with Switch B, running OSPF protocol.
- Import three static routes by enabling the OSPF 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 36 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 OSPF protocol and specifies the number of the area to which the interface belongs.

```
[Switch A]router id 1.1.1.1
[Switch A]ospf
[Switch A-ospf-1]area 0
[Switch A-ospf-1-area-0.0.0.0]network 10.0.0.0 0.255.255.255
```

d Import the static routes

```
[Switch A-ospf-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 OSPF protocol and specifies the number of the area to which the interface belongs.

```
[Switch B]router id 2.2.2.2
[Switch B]ospf
[Switch B-ospf-1]area 0
[Switch B-ospf-1-area-0.0.0.0]network 10.0.0.0 0.255.255.255
```

d Configure OSPF to filter the external routes received.

```
[Switch B-ospf-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).

Route Capacity Configuration

In practical networking applications, there is always a large number of routes in the routing table, especially OSPF routes. The routing information is usually stored in the memory of the Ethernet switch. When the size of the routing table increases, it can consume a significant amount of the switch memory.

To solve this problem, the Switch 5500G-EI provides a mechanism to control the size of the routing table. This monitors the free memory in the system to determine whether to add new routes to the routing table and whether or not to keep connection with a routing protocol.

The default value normally meets the network requirements. You must be careful when modifying the configuration to avoid reducing the stability of the network.

Limiting Route Capacity

The size of the routing table is determined by OSPF routes. Therefore, the route capacity limitation of the Switch 5500G-EI is only effective for these two types of routes and has no impact on static routes and other dynamic routing protocols.

When the free memory of the Switch 5500G-EI reduces to the lower limit value, the system will disconnect OSPF and remove the routes from the routing table to release memory. The system checks the free memory periodically. When enough free memory is detected the OSPF connection is restored.

Route Capacity Configuration

Route capacity configuration includes tasks described in the following sections:

- Setting the Lower Limit and the Safety Value of the Switch Memory
- Enabling and Disabling Automatic Recovery of Disconnected Routing Protocols

Setting the Lower Limit and the Safety Value of the Switch Memory

When the Switch memory is equal to or lower than the lower limit, OSPF is disconnected and OSPF routes are removed from the routing table.

Perform the following configuration in the System View.

Table 171 Setting the Lower Limit and the Safety Value of the Switch Memory

Operation	Command
Set the lower limit and the safety value of the Switch	**memory** { **safety** *safety_value* / **limit** *limit_value* }*
Restore the lower limit and the safety value of the Switch to the default value	**undo memory** [**safety** | **limit**]

The lower limit value set for the memory must be smaller than the safety value.

Enabling and Disabling Automatic Recovery of Disconnected Routing Protocols

If the Automatic Recovery function of the Switch 5500G-EI is disabled, connection to routing protocols is not restored even if the free memory returns to the safety value. Therefore, disabling automatic recovery must be performed cautiously.

Perform the following configurations in System View.

Table 172 Enabling/Disablingthe Switch to Recover the Disconnected Routing Protocol Automatically

Operation	Command
Enable memory automatic restoration function	**memory auto-establish enable**
Disable memory automatic restoration function of a Ethernet switch	**memory auto-establish disable**

By default, automatic recovery of disconnected routing protocols is enabled.

Displaying and Debugging Route Capacity

Enter the **`display`** command in any view to display the operation of the Route Capacity configuration.

Table 173 Displaying and debugging route capacity

Operation	**Command**
Display the route capacity memory information	**`display memory`** `[` **`unit`** *`unit_id`* `]`
Display the route capacity memory setting and state information	**`display memory limit`**

7 MULTICAST PROTOCOL

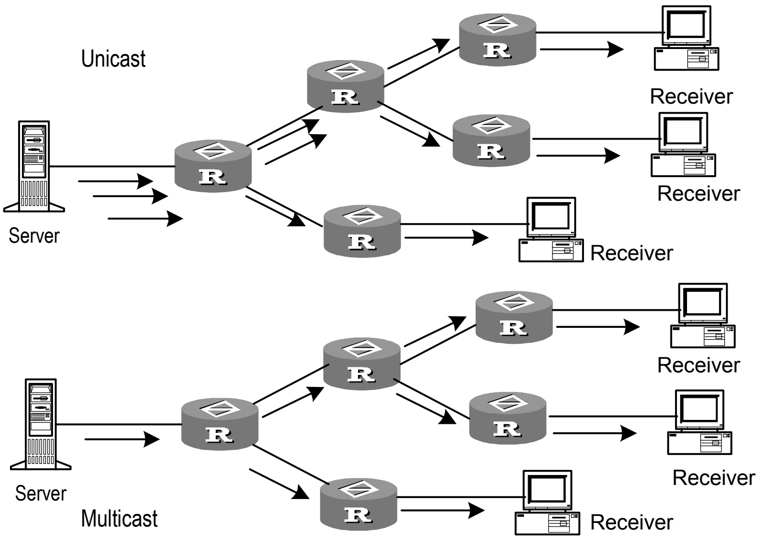
This chapter includes information on the following:

IP Multicast Overview

Many transmission methods can be used when the destination (including data, voice and video) is the secondary use of the network. If the multicast method is used you should establish an independent data transmission path for each user. The broadcast mode can be used if you intend to send the information to all users on the network. In either case, the end users will receive the information. For example, if the same information is required by 200 users on the network, the traditional solution is to send the information 200 times in unicast mode. In the broadcast mode, the data is broadcast over the entire network. However, both of the methods waste bandwidth resources. In addition, the broadcast mode cannot ensure information security.

IP multicast technology solves this problem. The multicast source sends the information only once. Multicast routing protocols establish tree-type routing for multicast packets. The information being sent will be replicated and distributed as far as possible (see Figure 37). Therefore, the information can be correctly sent, with high efficiency, to each user.

Figure 37 Comparison between the unicast and multicast transmission



A multicast source does not necessarily belong to a multicast group. It only sends data to the multicast group and it is not necessarily a receiver. Multiple sources can send packets to a multicast group simultaneously.

A router that does not support multicast may exist on the network. A multicast router can encapsulate multicast packets in unicast IP packets by tunneling and sending them on to the neighboring multicast router. The neighboring multicast router removes the unicast IP header and continues the multicast transmission.

Multicast advantages:

- Enhanced efficiency by reducing network traffic and relieving server and CPU loads.
- Optimized performance decreases traffic redundancy.
- Distributed applications make multipoint applications possible.

Multicast Addresses

The destination addresses of multicast packets use Class D IP addresses ranging from 224.0.0.0 to 239.255.255.255. Class D addresses cannot appear in the source IP address fields of IP packets.

During unicast data transmission, a packet is transmitted from the source address to the destination address with the “hop-by-hop” principle of the IP network. A packet has more than one destination address in a multi-cast environment, i.e., a group of addresses. All the information receivers join a group. Once a receiver joins the group, data flowing to the group is sent to the receiver immediately. All members in the group can receive the packets. Membership of a multicast group is dynamic, that is, hosts can join and leave groups at any time.

A multicast group can be either permanent or temporary. Part of addresses in the multicast group are reserved by the IANA and are known as the permanent multicast group. IP addresses of a permanent group are unchanged, but the members in the group can change. The number of members in a permanent multicast group can be random or even 0. Those IP multicast addresses that are not reserved for permanent multicast groups can be used by temporary groups.

Ranges and meanings of Class D addresses are shown in Table 174

Table 174 Ranges and meaning of Class D addresses

Class D address range	Meaning
224.0.0.0~224.0.0.255	Reserved multicast addresses (addresses of permanent groups). Address 224.0.0.0 is reserved. The other addresses can be used by routing protocols.
224.0.1.0~238.255.255.255	Multicast addresses available for users (addresses of temporary groups). They are valid in the entire network.
239.0.0.0~239.255.255.255	Multicast addresses for local management. They are valid only in the specified local range.

Reserved multicast addresses that are commonly used are shown in Table 175.

Table 175 Reserved multicast address list

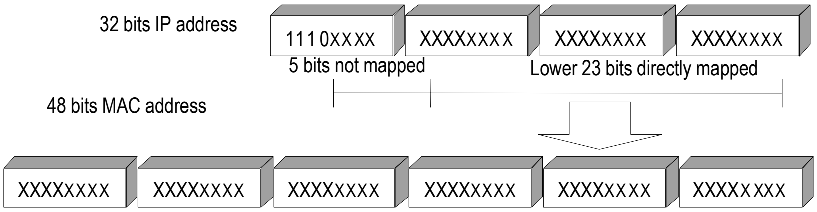
Class D address	Meaning
224.0.0.0	Base Address (Reserved)
224.0.0.1	Addresses of all hosts
224.0.0.2	Addresses of all multicast routers
224.0.0.3	Unassigned
224.0.0.4	DVMRP routers
224.0.0.5	OSPF routers
224.0.0.6	OSPF DR (designated router)
224.0.0.7	ST routers
224.0.0.8	ST hosts
224.0.0.9	RIP-2 routers
224.0.0.10	IGRP routers
224.0.0.11	Mobile agents
224.0.0.12	DHCP server/Relay agent
224.0.0.13	All PIM routers
224.0.0.14	RSVP encapsulation
224.0.0.15	All CBT routers
224.0.0.16	Designated SBM
224.0.0.17	All SBMS
224.0.0.18	VRRP
....	....

Ethernet Multicast MAC Addresses

When unicast IP packets are transmitted in Ethernet, the destination MAC address is the MAC address of the receiver. However, when multicast packets are transmitted, the destination is no longer a specific receiver but a group with unspecific members. Therefore, the multicast MAC address should be used. Multicast MAC addresses correspond to multicast IP addresses. IANA (Internet

Assigned Number Authority) stipulates that the higher 24 bits of the multicast MAC address is 0x01005e and the lower 23 bits of the MAC address is the lower 23 bits of the multicast IP address.

Figure 38 Mapping between the multicast IP address and the Ethernet MAC address



Only 23 bits of the last 28 bits in the IP multicast address are mapped to the MAC address. Therefore, the 32 IP multicast addresses are mapped to the same MAC address.

IP Multicast Protocols

Multicast uses the multicast group management protocol, and the multicast routing protocol. The multicast group management protocol uses Internet Group Management Protocol (IGMP) as the IP multicast basic signaling protocol. It is used between hosts and routers and enables routers to determine if members of the multicast group are on the network segment. The multicast routing protocol is used between multicast routers to create and maintain multicast routes, enabling highly-efficient multicast packet forwarding. Multicast routing protocols supported by the Switch 5500G-EI include PIM-SM and PIM-DM.

Internet Group Management Protocol (IGMP)

Internet Group Management Protocol (IGMP) is the only protocol that hosts can use. It defines the membership establishment and maintenance mechanism between hosts and routers, and is the basis of the entire IP multicast. Hosts report the group membership to a router through IGMP and inform the router of the conditions of other members in the group through the directly connected host.

If a user on the network joins a multicast group through IGMP declaration, the multicast router on the network will transmit the information sent to the multicast group through the multicast routing protocol. Finally, the network will be added to the multicast tree as a branch. When the host, as a member of a multicast group, begins receiving the information, the router will query the group periodically to check whether members in the group are involved. As long as one host is involved, the router receives data. When all users on the network quit the multicast group, the related branches are removed from the multicast tree.

Multicast Routing Protocol

A multicast group address has a virtual address. Unicast allows packets to be routed from the data source to the specified destination address. This is not possible for multicast. The multicast application sends the packets to a group of receivers (as with multicast addresses) who are ready to receive the data but not only to one receiver (as with unicast address).

The multicast routing creates a loop-free data transmission path from one data source to multiple receivers. The task of the multicast routing protocol is to create a distribution tree architecture. A multicast router can use multiple methods to build up a path for data transmission, i.e., the distribution tree.

PIM-DM (Protocol-Independent Multicast Dense Mode, PIM-DM) PIM dense mode is suitable for small networks. It assumes that each subnet in the network contains at least one receiver interested in the multicast source. As a result, multicast packets are flooded to all points of the network, consuming network bandwidth and increasing router processing. To reduce network resource consumption, branches that do not have members send Prune messages toward the source to reduce the unwanted/unnecessary traffic. To enable the receivers to receive multicast data streams, the pruned branches can be restored periodically to a forwarding state. To reduce latency time, the PIM dense mode uses the prune mechanism to actively restore multicast packet forwarding. Periodic flood and prune are characteristics of PIM dense mode. Generally, the forwarding path in dense mode is a “source tree” rooted at the source with multicast members as the branches. Since the source tree uses the shortest path from the multicast source to the receiver, it is also called the shortest path tree (SPT).

PIM-SM (Protocol-Independent Multicast Sparse Mode, PIM-SM) Dense mode uses the flood-prune technology, which is not applicable for WAN. In WAN, multicast receivers are sparse and therefore the sparse mode is used. In sparse mode, hosts need not receive multicast packets unless, by default, there is an explicit request for the packets. A multicast router must send a join message to the RP (Rendezvous Point, which needs to be built into the network and is a virtual place for data exchange) corresponding to the group for receiving the multicast data traffic from the specified group. The join message passes routers and finally reaches the root, i.e., the RP. The join message becomes a branch of the shared tree. In PIM sparse mode, multicast packets are sent to the RP first, and then are forwarded along the shared tree rooted at the RP and with members as the branches. To prevent the branches of the shared tree from being deleted, PIM sparse mode sends join messages to branches periodically to maintain the multicast distribution tree.

To send data to the specified address, senders register with the RP first before forwarding data to the RP. When the data reaches the RP, the multicast packets are replicated and sent to receivers along the path of the distribution tree. Replication only happens at the branches of the distribution tree. This process can be repeated automatically until the packets reach the destination.

Forwarding IP Multicast Packets

In the multicast model, the source host sends information to the host group represented by the multicast group address within the destination address fields of the IP packets. The multicast model must forward the multicast packets to multiple external interfaces so that the packets can be sent to all receivers.

RPF (Reverse Path Forwarding)

To ensure that a multicast packet reaches the router along the shortest path, the multicast must depend on the unicast routing table or a unicast routing table independently provided for multicast to check the receiving interface of multicast packets. This check mechanism is the basis for most multicast routing protocols performing multicast forwarding, which is known as RPF (Reverse Path Forwarding) check. A multicast router uses the source address from the multicast packet to query the unicast routing table, or the independent multicast routing table, to determine that the incoming interface on which the packet arrives is the shortest path from the receiver to the source address. If a source tree is used, the source address is the address of the source host sending the multicast packet. If a shared tree is used, the source address is the address of the root of the shared tree. When a multicast packet arrives at the router, if RPF check succeeds, the packet will be forwarded according to the multicast forwarding entry. Otherwise, the packet will be dropped.

Applying Multicast

IP multicast technology effectively solves the problem of packet forwarding from single-point to multi-point. It implements highly-efficient data transmission from single-point to multi-point in IP networks and can save a large amount of network bandwidth and reduce network loads. New value-added services that use multicast can be delivered, including direct broadcasting, Web TV, distance learning, distance medicine, net broadcasting station and real-time audio/video conferencing.

- Multimedia and streaming media applications
- Communications at training and corporate sites
- Data repository and finance (stock) applications
- Any "point-to-multipoint" data distribution

With the increase of multimedia services on IP networks, multicast has huge market potential.

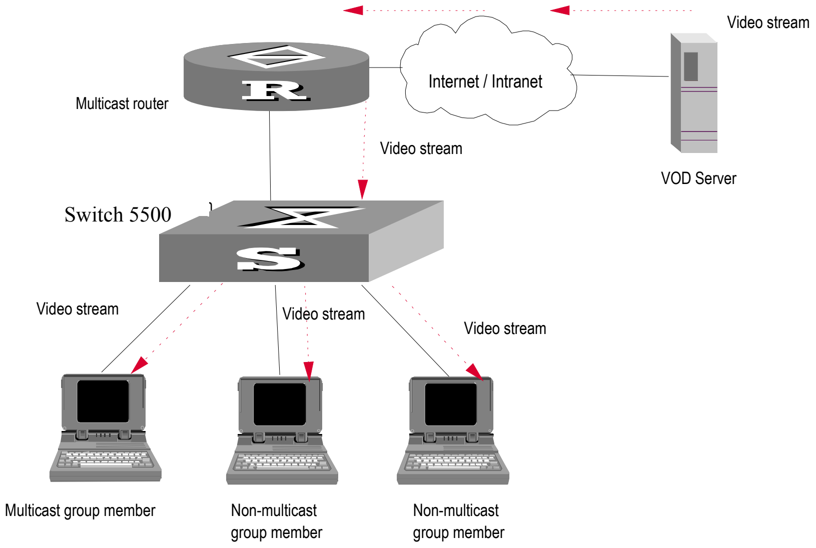
IGMP Snooping

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 5500G-EI 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.

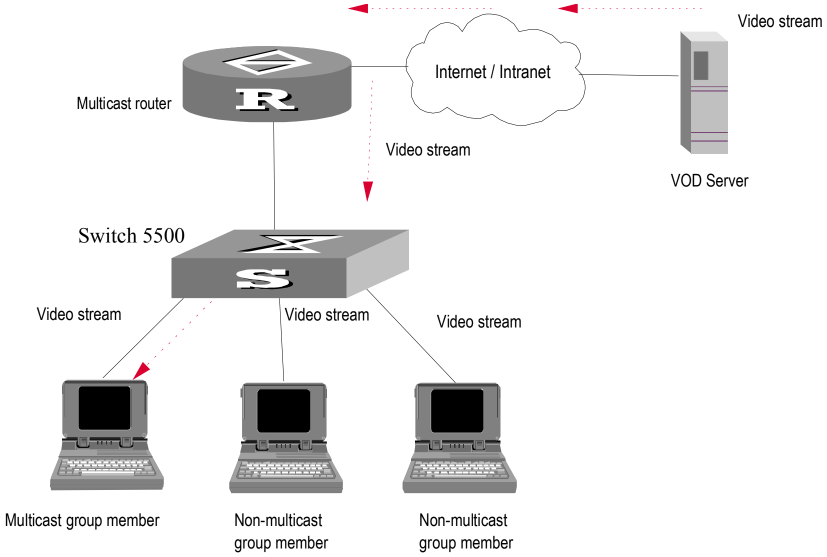
When IGMP Snooping is disabled, the packets are multicast to all ports, see Figure 39.

Figure 39 Multicast packet transmission without IGMP Snooping



When IGMP Snooping operates, packets are not forwarded to all ports, see Figure 40.

Figure 40 Multicast packet transmission when IGMP Snooping runs



IGMP Snooping Terminology

Table 176 explains switching terminology relevant to IGMP Snooping.

Table 176 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 5500G-EI.

Table 176 Switching Terminology relevant to IGMP Snooping

Term	Meaning
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 5500G-EI 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 5500G-EI 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 41.

Figure 41 Implementing IGMP Snooping

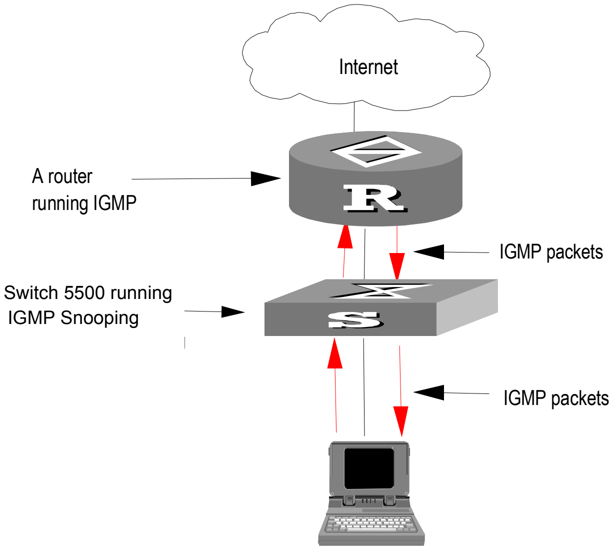


Table 177 explains IGMP Snooping terminology.

Table 177 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 5500G-EI will reset the aging timer of the port. When a port other than a router port receives the IGMP general query message, the Switch 5500G-EI will notify the multicast router that a port is ready to join a multicast group and starts the aging timer for the port.
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 5500G-EI 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 178 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 178 Enabling/Disabling IGMP Snooping

Operation	Command
Enable/disable IGMP Snooping	**igmp-snooping { enable | disable }**

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 179 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 179 Configuring router port aging time

Operation	Command
Configure router port aging time	**igmp-snooping router-aging-time** *seconds*
Restore the default aging time	**undo igmp-snooping router-aging-time**

By default, the port aging time is 105 seconds.

Configuring Maximum Response Time

Use the commands in Table 180 to manually configure the maximum response time. If the Switch 5500G-EI 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 180 Configuring the maximum response time

Operation	Command
Configure the maximum response time	**igmp-snooping max-response-time** *seconds*
Restore the default setting	**undo igmp-snooping max-response-time**

By default, the maximum response time is 10 seconds.

Configuring Aging Time of Multicast Group Member_

Use the commands in Table 181 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 181 Configuring aging time of the multicast member

Operation	Command
Configure aging time of the multicast member	**igmp-snooping host-aging-time** *seconds*
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 182 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** *vlanid* **]**
Reset the IGMP Snooping statistic information	**reset igmp-snooping statistics**

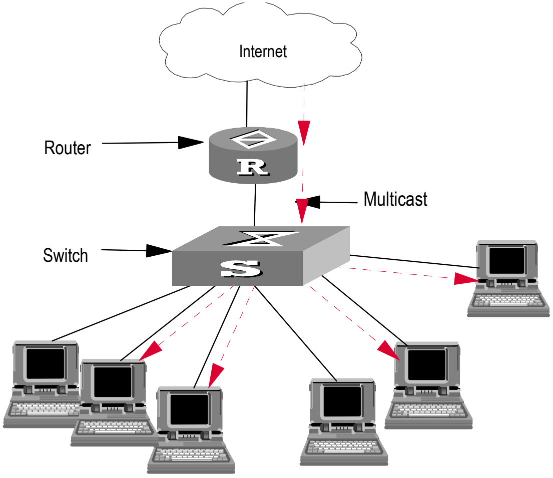
Configuration Example — Enable IGMP Snooping

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 42 IGMP Snooping configuration network



Configuration Procedure

Enable IGMP Snooping globally.

```
[SW5500]igmp-snooping enable
```

Enable IGMP Snooping on VLAN 10.

```
[SW5500]vlan 10
[SW5500-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.

Common Multicast Configuration

A common multicast configuration covers both the multicast group management protocol and the multicast routing protocol. The configuration includes enabling multicast, configuring the multicast forwarding boundary, and displaying the multicast routing table and multicast forwarding table.

Common multicast configuration includes:

- Enabling multicast
- Configuring the multicast route limit
- Clearing MFC forwarding entries or statistics information
- Clearing route entries from the core multicast routing table

Enabling Multicast

Enable multicast first before enabling IGMP and the multicast routing protocol.

Perform the following configuration in system view.

Table 183 Enabling multicast

Operation	Command
Enable multicast	**`multicast routing-enable`**
Disable multicast	**`undo multicast routing-enable`**

By default, multicast is disabled.

Other multicast configurations can only become effective when multicast is enabled.

Configuring Multicast Route Limit

If the existing route entries exceed the capacity value you configured using this command, the system will not delete the existing entries. The following prompt is shown; `Existing route entries exceed the configured capacity value.`

Perform the following configuration in System view:

Table 184 Configuring Multiast Route Limit

Operation	Command
Configure number limit of multicast routing entries	**`multicast route-limit`** *`limit`*
Restore the default number limit	**`undo multicast route-limit`**

Clearing MFC Forwarding Entries or Statistics Information

Use the command in Table 185 to clear the multicast forwarding cache (MFC) forward entries or statistics information.

Perform the following configuration in User View.

Table 185 Clearing MFC forwarding entries or its statistic information

Operation	Command
Clear MFC forwarding entries or its statistic information	**reset multicast forwarding-table** [**statistics**] { **all** | { *group_address* [**mask** { *group_mask* | *group_mask_length* }] | *source_address* [**mask** { *source_mask* | *source_mask_length* }] | **incoming-interface** *interface_type* *interface_number* } * }

Clearing Route Entries From The Core Multicast Routing Table

Use the command in Table 186 to clear route entries from the core multicast routing table, as well as MFC forwarding entries.

Perform the following configuration in User View.

Table 186 Clearing routing entries from multicast routing table

Operation	Command
Clear routing entries from multicast routing table	**reset multicast routing-table** { **all** | { *group_address* [**mask** { *group_mask* | *group_mask_length* }] | *source_address* [**mask** { *source_mask* | *source_mask_length* }] | { **incoming-interface** *interface_type* *interface_number* } } * }

The forwarding entries in MFC are deleted along with the routing entries in the multicast kernel routing table.

Displaying and Debugging Common Multicast Configuration

Execute **display** command in any view to display the running of the multicast configuration, and to verify the effect of the configuration.

Execute **debugging** command in User View to debug multicast.

Table 187 Displaying and debugging Common Multicast Configuration

Operation	Command
Display the multicast routing table	**display multicast routing-table** [*group-address* [**mask** { *mask* | *mask_length* }] | *source_address* [**mask** { *mask* | *mask_length* }] | **incoming-interface** { *interface-type* *interface_number* / **register** }]*
Display the multicast forwarding table	**display multicast forwarding-table** [*group_address* [**mask** { *mask* | *mask_length* }] | *source_address* [**mask** { *mask* | *mask_length* }] | **incoming-interface register**]*
Enable multicast packet forwarding debugging	**debugging multicast forwarding**
Disable multicast packet forwarding debugging	**undo debugging multicast forwarding**

Table 187 Displaying and debugging Common Multicast Configuration

Operation	Command
Enable multicast forwarding status debugging	**`debugging multicast status-forwarding`**
Disable multicast forwarding status debugging	**`undo debugging multicast status-forwarding`**
Enable multicast kernel routing debugging	**`debugging multicast kernel-routing`**
Disable multicast kernel routing debugging	**`undo debugging multicast kernel-routing`**

There are three types of multicast routing tables: individual multicast routing tables of each multicast routing protocol; a multicast kernel routing table integrating the routing information of those individual routing tables; and a multicast forwarding table in conformity with the kernel routing table and in charge of the multicast packet forwarding.

Multicast forwarding table is mainly used in debugging. Generally, users can obtain required information by viewing the multicast kernel routing table.

Tracing the Network Path of Multicast Data

You can use the **`mtracert`** command in any view to trace the network path multicast data taken from multicast source to destination receiver any locate any faults.

Table 188 Tracing the Network Path of Multicast Data

Operation	Command
Trace the network path multicast data taken from multicast source to destination receiver	**`mtracert { `*`source-address`*` } [ `*`last-hop-address`*` ] [ `*`group-address`*` ]`**

- If the multicast source address only is specified, the last hop address defaults to the address of a physical interface of the local router and the group address defaults to 0.0.0.0. In this instance, trace reversely hop by hop from the local router to the first hop router that connects directly to multicast source, following RPF rule.
- If the multicast source address and the last hop address are specified, the group address defaults to 0.0.0.0. In this instance, trace reversely hop by hop from the local router to the first hop router that connects directly to multicast source, following RPF rule.
- If the source address and group address only are specified, the last hop address defaults to that of a physical interface of the local router. In this instance, trace reversely from the local router to the first hop router which is directly connected with multicast source, following the associated entry (S, G) in the multicast kernel routing table of each router on the path.
- If the multicast source address, destination address and group address are all specified, trace reversely from the last hop router to the first hop router which directly connected with multicast source following the corresponding entry (S, G) in the multicast kernel routing table or each router on the path.

The trace mode is called weak trace if the group address is 0.0.0.0.

Internet Group Management Protocol (IGMP)

IGMP is a protocol in the TCP/IP suite, responsible for management of IP multicast members. It is used to establish and maintain multicast membership among IP hosts and their directly connected neighboring routers. IGMP excludes transmitting and maintenance of membership information among multicast routers, which are completed by multicast routing protocols. All hosts participating in multicast must implement IGMP.

Hosts participating in IP multicast can join and leave a multicast group at any time. The number of members of a multicast group can be any integer and their location can be anywhere. A multicast router does not need and cannot keep the membership of all hosts. It only uses IGMP to learn whether receivers (i.e., group members) of a multicast group are present on the subnet connected to each interface. A host only needs to keep the multicast groups it has joined.

IGMP is not symmetric on hosts and routers. Hosts need to respond to IGMP query messages from the multicast router, i.e., report the group membership to the router. The router needs to send membership query messages periodically to discover whether hosts join the specified group on its subnets according to the received response messages. When the router receives the report that hosts leave the group, the router will send a group-specific query (IGMP Version 2) to discover whether there are no members in the group.

Up to now, IGMP has three versions, namely, IGMP Version 1 (defined by RFC1112), IGMP Version 2 (defined by RFC2236) and IGMP Version 3. IGMP Version 2 is currently the most widely used version.

IGMP Version 2 benefits from the following improvements over IGMP Version 1:

- Election mechanism of multicast routers on the shared network segment
- Leaving group mechanism
- Specific group query
- Max response time

Election Mechanism of Multicast Routers on the Shared Network Segment

A shared network segment means that there are multiple multicast routers on a network segment. In this case, all routers running IGMP on the network segment can receive the membership report from hosts. Therefore, only one router is necessary to send membership query messages. In this case, the router election mechanism is required to specify a router as the querier.

In IGMP Version 1, selection of the querier is determined by the multicast routing protocol. While IGMP Version 2 specifies that the multicast router with the lowest IP address is elected as the querier when there are multiple multicast routers on the same network segment.

Leaving Group Mechanism

In IGMP Version 1, hosts leave the multicast group quietly without informing the multicast router. The multicast router can only depend on the timeout of the response time of the multicast group to confirm that hosts leave the group. In Version 2, when a host leaves a multicast group, it will send a leave group message.

Specific Group Query

In IGMP Version 1, a query of multicast routers is targeted at all the multicast groups on the network segment. This is known as General Query.

In addition to General Query, IGMP Version 2 also supports Group-Specific Query. The destination IP address of the query packet is the IP address of the multicast group. The group address domain in the packet is also the IP address of the multicast group. This prevents the hosts of members of other multicast groups from sending response messages.

Max Response Time

The Max Response Time is added in IGMP Version 2. It is used to dynamically adjust the allowed maximum time for a host to respond to the membership query message.

Configuring IGMP

Basic IGMP configuration includes:

- Enabling Multicast
- Enabling IGMP on an Interface

Advanced IGMP configuration includes:

- Configuring the IGMP Version
- Configuring the Interval and the Number of IGMP Query Packets
- Configuring Maximum Response Time for IGMP Query Message
- Configuring Maximum Response Time for IGMP Query Message
- Configuring the Limit of IGMP Groups on an Interface
- Configuring a Router to Join Specified Multicast Group
- Limiting Multicast Groups An Interface Can Access
- Configuring the Interval to Send IGMP Query Message
- Deleting IGMP Groups Joined on an Interface

Enabling Multicast

Refer to "Common Multicast Configuration" on page 177.

Enabling IGMP on an Interface

You must enable multicast before you can execute the `igmp enable` command. After this, you can initiate IGMP feature configuration.

Perform the following configuration in Interface View.

Table 189 Enabling/Disabling IGMP on an interface

Operation	Command
Enable IGMP on an interface	`igmp enable`
Disable IGMP on an interface	`undo igmp enable`

By default, IGMP is not enabled.

Configuring the IGMP Version

Perform the following configuration in Interface View.

Table 190 Selecting the IGMP version

Operation	Command
Select the IGMP version that the router uses	**igmp version { 1 | 2 }**
Restore the default setting	**undo igmp version**

By default, IGMP Version 2 is used.

All routers on a subnet must support the same version of IGMP. After detecting the presence of IGMP Version 1 system, a router cannot automatically switch to Version 1.

Configuring the Interval for Querying IGMP Packets

The router finds out which multicast groups on its connected network segment have members by sending IGMP query messages periodically. Upon the reception of a response message, the router refreshes the membership information of the corresponding multicast group.

Perform the following configurations in Interface View.l

Table 191 Configuring query interval

Operation	Command
Configure query interval	**igmp timer query** *seconds*
Restore the default query interval	**undo igmp timer query**

When there are multiple multicast routers on a network segment, the querier is responsible for sending IGMP query messages to all the hosts on the LAN.

By default, the interval is 60 seconds.

Configuring the Interval and the Number of IGMP Query Packets

On a shared network, the query router (querier) maintains IGMP membership on the interface. When an IGMP querier receives an IGMP Leave Group message from a host, the last member query interval can be specified for Group-Specific Queries.

1 The host sends the IGMP Leave message.

2 Upon receiving the message, the IGMP querier sends the designated group IGMP query message for the specified number of times (defined by the *robust_value* in **igmp robust-count**, with the default value as 1 second) and at a time interval (defined by the *seconds* in **igmp lastmember-queryinterval**, with the default value as 2).

3 When other hosts receive the message from the IGMP querier and are interested in this group, they return the IGMP Membership Report message within the defined maximum response time.

4 If the IGMP querier receives the report messges from other hosts within the period equal to *robust-value* × *seconds*, it continues membership maintenance for this group.

5 If the IGMP querier does not receive a report message from any other host within this period, then it takes it as timeout and ends membership maintenance for this group.

This command can be used only when the querier runs IGMP version 2, since a host running IGMP Version 1 does not send an IGMP Leave Group message when it leaves a group.

Perform the following configuration in Interface View.

- Configure interval for querying IGMP packets, see Table 192. By default, the interval is 1 second.
- Configuring the number of last member querying, see Table 193. By default, an IGMP group-specific query message is sent for twice

Table 192 Configuring interval for querying IGMP packets

Operation	Command
Configure interval for querying IGMP packets	**igmp lastmember-queryinterval** *seconds*
Restore the default query interval	**undo igmp lastmember-queryinterval**

Table 193 Configure the number of last member querying

Operation	Command
Configure number of last member querying	**igmp robust-count** *robust-value*
Restore the default number of querying	**undo igmp robust-count**

Configuring the Present Time of IGMP Querier

The IGMP querier present timer defines the period of time before the router takes over as the querier sending query messages, after the previous querier has stopped doing so.

Perform the following configuration in Interface view.

Table 194 Configuring the present time of IGMP querier

Operation	Command
Change the present time of IGMP querier	**igmp timer other-querier-present** *seconds*
Restore the default value	**undo igmp timer other-querier-present**

By default, the value is 120 seconds. If the router has received no query message within twice the interval specified by the **igmp timer query** command, it will regard the previous querier invalid.

Configuring Maximum Response Time for IGMP Query Message

When a router receives a query message, the host will set a timer for each multicast group it belongs to. The value of the timer is randomly selected between 0 and the maximum response time. When any timer becomes 0, the host will send the membership report message of the multicast group.

Setting the maximum response time reasonably can enable the host to respond to query messages quickly. In this case, the router can fast master the existing status of the members of the multicast group.

Perform the following configuration in Interface view.

Table 195 Configuring the maximum response time for IGMP query message

Operation	Command
Configure the maximum response time for IGMP query message	**igmp max-response-time** *seconds*
Restore the maximum query response time to the default value	**undo igmp max-response-time**

The smaller the maximum query response time value, the faster the router prunes groups. The actual response time is a random value in the range from 1 to 25 seconds. By default, the maximum query response time is 10 seconds.

Configuring the Limit of IGMP Groups on an Interface

If there is no limit to the number of IGMP groups added on a router interface or a router, the router memory may be exhausted, which may cause router failure.

You can set number limit for the IGMP groups added on the interface, but not the number limit for the IGMP groups added in the router, which is defined by the system.

Perform the following configuration in Interface view.

Table 196 Configuring the limit of IGMP groups on an interface

Operation	Command
Configure the limit of IGMP groups on an interface	**igmp group-limit** *limit*
Restore the limit of IGMP groups on an interface to the default value	**undo igmp group-limit**

By default, the maximum number of IGMP groups on an interface is 1024.

If the number of IGMP groups on an interface has exceeded the specified value during configuration, no IGMP group will be deleted.

Configuring a Router to Join Specified Multicast Group

Usually, the host operating IGMP will respond to IGMP query packet of the multicast router. In case of response failure, the multicast router will consider that there is no multicast member on this network segment and will cancel the corresponding path. Configuring one interface of the router as multicast member can avoid such problem. When the interface receives IGMP query packet, the router will respond, thus ensuring that the network segment where the interface is connected can normally receive multicast packets.

For a Switch 5500G-EI, you can configure a port in a VLAN interface to join a multicast group.

Perform the following configuration in the corresponding view.

Table 197 Configuring a router to join specified multicast group

Operation	Command
Configure a router to join specified multicast group (VLAN Interface View)	**igmp host-join** *group_address* **port** { *interface_type interface_ num* | *interface_name* } [**to** { *interface_type interface_ num* | *interface_name* }]
Quit from specified multicast group (VLAN Interface View)	**undo igmp host-join** *group-address* **port** { *interface_type interface_ num* | *interface_name* } [**to** { *interface_type interface_ num* | *interface_name* }]
Configure a router to join specified multicast group (Ethernet Port View)	**igmp host-join** *group-address* **vlan** *vlanid*
Quit from specified multicast group (Ethernet Port View)	**undo igmp host-join** *group-address* **vlan** *vlanid*

By default, a router joins no multicast group.

Limiting Multicast Groups An Interface Can Access

A multicast router learns whether there are members of a multicast group on the network via the received IGMP membership message. A filter can be set on an interface so as to limit the range of allowed multicast groups.

Perform the following configuration in Interface view.

Table 198 Limiting multicast groups an interface can access

Operation	Command
Limit the range of allowed multicast groups on current interface (Interface View)	**igmp group-policy** *acl_number* [**1** | **2** | **port** { *interface_type interface_ num* / *interface_name* } [**to** { *interface_type interface_ num* / *interface_name* }]]
Remove the filter set on the interface (Interface View)	**undo igmp group-policy** [**port** { *interface_type interface_ num* / *interface_name* } [**to** { *interface_type interface_ num* / *interface_name* }]]
Limit the range of allowed multicast groups on current interface (Ethernet port view)	**igmp group-policy** ***acl-number*** **vlan** ***vlanid***
Remove the filter set on the interface (Ethernet port view)	**undo igmp group-policy vlan** ***vlanid***

By default, no filter is configured, that is, all multicast groups are allowed on the interface.

Configuring the Interval to Send IGMP Query Message

Multicast routers send IGMP query messages to discover which multicast groups are present on attached networks. Multicast routers send query messages periodically to refresh their knowledge of members present on their networks.

Perform the following configuration in Interface view.

Table 199 Configuring the interval to send IGMP query message

Operation	Command
Configure the interval to send IGMP query message	**igmp timer query** *seconds*
Restore the default value	**undo igmp timer query**

When there are multiple multicast routers on a network segment, the querier is responsible for sending IGMP query messages to all hosts on the LAN.

By default, the interval is 60 seconds.

Deleting IGMP Groups Joined on an Interface

You can delete an existing IGMP group from the interface using the following command.

Perform the following configuration in Interface view.

Table 200 Deleting IGMP groups joined on an interface

Operation	Command
Delete IGMP groups joined on an interface	**reset igmp group** { **all** | **interface** *interface_type interface_number* { **all** | *group_address* [*group_mask*] } }

Displaying and debugging IGMP

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

Execute **debugging** command in user view for the debugging of IGMP.

Table 201 Displaying and debugging IGMP

Operation	Command
Display the information about members of IGMP multicast groups	**display igmp group [** *group_address* | **interface** *interface_type interface_number* **]**
Display the IGMP configuration and running information about the interface	**display igmp interface [** *interface_type interface_number* **]**
Enable the IGMP information debugging	**debugging igmp { all** | **event** | **host** | **packet** | **timer }**
Disable the IGMP information debugging	**undo debugging igmp { all** | **event** | **host** | **packet** | **timer }**

PIM-DM Overview

PIM-DM (Protocol Independent Multicast, Dense Mode) belongs to dense mode multicast routing protocols. PIM-DM is suitable for small networks. Members of multicast groups are relatively dense in such network environments.

The working procedures of PIM-DM include neighbor discovery, flood & prune and graft.

Neighbor discovery

The PIM-DM router uses Hello messages to perform neighbor discovery when it is started. All network nodes running PIM-DM stay in touch with one another by periodically sending Hello messages.

Flood&Prune

PIM-DM assumes that all hosts on the network are ready to receive multicast data. When a multicast source "S" begins to send data to a multicast group "G", after the router receives the multicast packets, the router will perform RPF check according to the unicast routing table first. If the RPF check is passed, the router will create an (S, G) entry and then flood the data to all downstream PIM-DM nodes. If the RPF check is not passed, that is, multicast packets enter from an error interface, the packets will be discarded. After this process, an (S, G) entry will be created in the PIM-DM multicast domain.

If the downstream node has no multicast group members, it will send a Prune message to the upstream nodes to inform the upstream node not to forward data to the downstream node. Receiving the prune message, the upstream node will remove the corresponding interface from the outgoing interface list corresponding to the multicast forwarding entry (S, G). In this way, a SPT (Shortest Path Tree) rooted at Source S is built. The pruning process is initiated by leaf routers first.

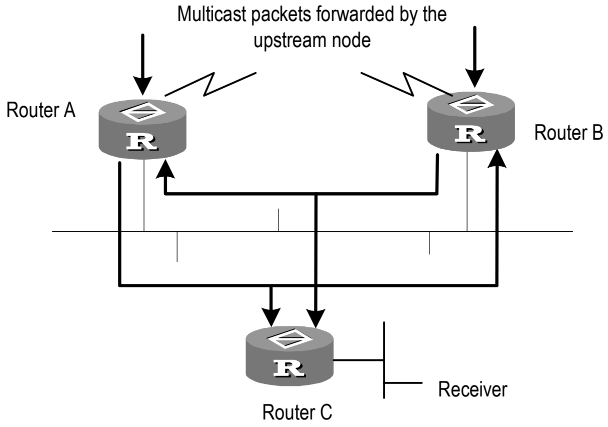
This process is called “flood & prune” process. In addition, nodes that are pruned provide timeout mechanism. Each router re-starts the “flood & prune” process upon pruning timeout. The consistent “flood & prune” process of PIM-DM is performed periodically.

During this process, PIM-DM uses the RPF check and the existing unicast routing table to build a multicast forwarding tree rooted at the data source. When a packet arrives, the router will first judge the correctness of the path. If the interface that the packet arrives is the one indicated by the unicast routing to the multicast source, the packet is regarded to be from the correct path. Otherwise, the packet will be discarded as a redundancy packet without the multicast forwarding. The unicast routing information as path judgment can come from any unicast routing protocol independent of any specified unicast routing protocol such as the routing information learned by RIP and OSPF

Assert Mechanism

As shown in the Figure 43, both routers A and B on the LAN have their own receiving paths to multicast source S. In this case, when they receive a multicast packet sent from multicast source S, they will both forward the packet to the LAN. Multicast Router C at the downstream node will receive two copies of the same multicast packet.

Figure 43 Assert mechanism diagram



When they detect such a case, routers need to select a unique sender by using the assert mechanism. Routers will send Assert packets to select the best path. If two or more than two paths have the same priority and metric, the path with a higher IP address will be the upstream neighbor of the (S, G) entry, which is responsible for forwarding the (S, G) multicast packet.

Graft

When the pruned downstream node needs to be restored to the forwarding state, the node will send a graft packet to inform the upstream node.

Configuring PIM-DM

PIM-DM basic configuration includes:

- Enabling Multicast
- Enabling PIM-DM

PIM-DM advanced configuration includes:

- Entering the PIM View
- Configuring Sending Interval for the Hello Packets
- Configuring the Filtering of Multicast Source/Group
- Configuring the Filtering of PIM Neighbor
- Configuring the Maximum Number of PIM Neighbor on an Interface
- Clearing Multicast Route Entries from PIM Routing Table
- Clearing PIM Neighbors

When the router is run in the PIM-DM domain, 3Com recommends that you enable PIM-DM on all interfaces of the non-border router.

Enabling Multicast

Refer to "Common Multicast Configuration" on page 177.

Enabling PIM-DM

PIM-DM needs to be enabled in the configuration of all interfaces.

After PIM-DM is enabled on an interface, it will send PIM Hello messages periodically and process protocol packets sent by PIM neighbors.

Perform the following configuration in Interface view.

Table 202 Enabling PIM-DM

Operation	Command
Enable PIM-DM on an interface	`pim dm`
Disable PIM-DM on an interface	`undo pim dm`

3Com recommends that you configure PIM-DM on all interfaces in non-special cases. This configuration is effective only after the multicast routing is enabled in System View.

Once PIM-DM is enabled on an interface, PIM-SM cannot be enabled on the same interface and vice versa.

Entering the PIM View

Global parameters of PIM should be configured in PIM View.

Perform the following configuration in System View.

Table 203 Entering PIM view

Operation	Command
Enter PIM view	`pim`
Back to system view	`undo pim`

Using `undo pim` command, you can clear the configuration in PIM view, and back to system view.

Configuring Sending Interval for the Hello Packets

After PIM is enabled on an interface, it will send Hello messages periodically on the interface. The interval at which Hello messages are sent can be modified according to the bandwidth and type of the network connected to the interface.

Perform the following configuration in Interface view.

Table 204 Configuring hello message interval on an interface

Operation	Command
Configure the hello message interval on an interface	**`pim timer hello`** *`seconds`*
Restore the interval to the default value	`undo pim timer hello`

The default interval is 30 seconds. You can configure the value according to different network environments. Generally, this parameter does not need to be modified.

This configuration can be performed only after PIM (PIM-DM or PIM-SM) is enabled in Interface View.

Configuring the Filtering of Multicast Source/Group

You can set to filter the source (and group) address of multicast data packets via this command. When this feature is configured, the router filters not only multicast data, but the multicast data encapsulated in the registration packets.

Perform the following configuration in the PIM view.

Table 205 Configuring the filtering of multicast source/group

Operation	Command
Configure the filtering of multicast source/group	**source-policy** *acl_number*
Remove the configuration of filtering	**undo source-policy**

If resource address filtering is configured, as well as basic ACLs, then the router filters the resource addresses of all multicast data packets received. Those not matched will be discarded.

If resource address filtering is configured, as well as advanced ACLs, then the router filters the resource and group addresses of all multicast data packets received. Those not matched will be discarded.

Configuring the Filtering of PIM Neighbor

You can set to filter the PIM neighbors on the current interface via the following configuration.

Perform the following configuration in the PIM View.

Table 206 Configuring the filtering of PIM neighbor

Operation	Command
Configure filtering of PIM neighbor	**pim neighbor-policy** *acl_number*
Remove the configuration of filtering	**undo pim neighbor-policy**

By default, no filtering rules are set.

Only the routers that match the filtering rule in the ACL can serve as a PIM neighbor of the current interface.

Configuring the Maximum Number of PIM Neighbor on an Interface

The maximum number of PIM neighbors of a router interface can be configured to avoid exhausting the memory of the router or router faults. The maximum number of PIM neighbors of a router is defined by the system, and is not open for modification.

Perform the following configuration in the PIM view.

Table 207 Configuring the maximum number of PIM neighbor on an interface

Operation	Command
Configure the maximum number of PIM neighbor on an interface	**pim neighbor-limit** *limit*
Restore the limit of PIN neighbor to the default value	**pim neighbor-limit**

By default, the PIM neighbors on the interface are limited to 128.

If the number of PIM neighbors of an interface has exceeded the configured value by the time of configuration, the existing PIM neighbors will not be deleted.

Clearing Multicast Route Entries from PIM Routing Table

Perform the following configuration in User View.

Table 208 Clearing multicast route entries from PIM routing table

Operation	Command
Clear multicast route entries from PIM routing table	**reset pim routing-table** { **all** | { *group_address* [**mask** { *group_mask* | *group_mask_length* }] | *source_address* [**mask** { *source_mask* | *source_mask_length* }] | { **incoming-interface** { *interface_type interface_number* | **null** } } } * }

If in this command, the *group-address* is 224.0.0.0/24 and *source-address* is the RP address (where group address can have a mask, but the resulted IP address must be 224.0.0.0, and source address has no mask), then it means only the (*, *, RP) item will be cleared.

If in this command, the *group-address* is any a group address, and *source-address* is 0 (where group address can have a mask, and source address has no mask), then only the (*, G) item will be cleared.

Note that this command clears not only multicast route entries from PIM routing table, but also the corresponding route entries and forward entries in the multicast core routing table and MFC.

Clearing PIM Neighbors

Perform the following configuration in User View.

Table 209 Resetting PIM neighbor

Operation	Command
Clear PIM neighbors	**reset pim neighbor** { **all** | { *neighbor_address* | **interface** *interface_type interface_number* } * }

Displaying and Debugging PIM-DM

After the above configuration, execute the **display** command in any view to display the running of PIM-DM configuration, and to verify the effect of the configuration.

Execute the **debugging** command in user view for the debugging of PIM-DM.

Table 210 Displaying and debugging PIM-DM

Operation	Command
Display the PIM multicast routing table	display pim routing-table [{ { *g [group_address [mask { mask_length | mask }]] | **rp [rp_address [mask { mask_length | mask }]] } | { group_address [mask { mask_length | mask }] | source_address [mask { mask_length | mask }] } * } | incoming-interface { interface-type interface_number | interface name | null } | { dense-mode | sparse-mode }] *
Display the PIM interface information	display pim interface [interface-type interface_number]
Display the information about PIM neighboring routers	display pim neighbor [interface-type interface_number]
Enable the PIM debugging	debugging pim common { all | event | packet | timer }
Disable the PIM debugging	undo debugging pim common { all | event | packet | timer }
Enable the PIM-DM debugging	debugging pim dm { alert | all | mbr | mrt | timer | warning | { recv | send } { all | assert | graft | graft-ack | join | prune } }
Disable the PIM-DM debugging	undo debugging pim dm { alert | all | mbr | mrt | timer | warning | { recv | send } { all | assert | graft | graft-ack | join | prune } }

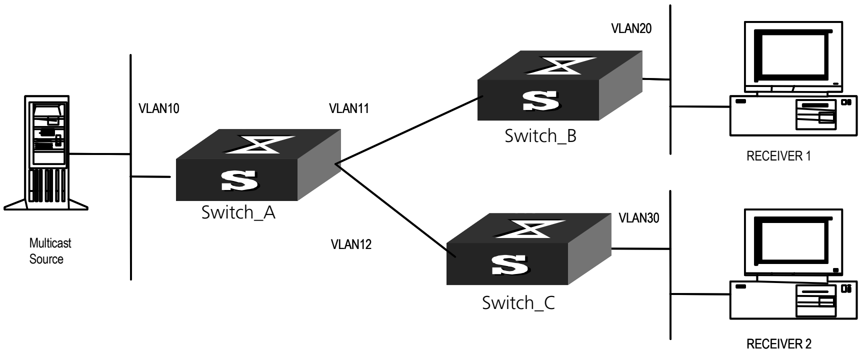
PIM-DM Configuration Example

Networking Requirements

Switch_A has a port carrying Vlan 10 to connect the Multicast Source, a port carrying Vlan11 to connect Switch_B and a port carrying Vlan12 to connect to Switch_C. Configure to implement multicast between Multicast Source and Receiver 1 and Receiver 2.

Networking Diagram

Figure 44 PIM-DM configuration networking



Configuration Procedure

This section only describes the configuration procedure for Switch_A. Follow a similar configuration procedure for Switch_B and Switch_C.

1 Enable the multicast routing protocol.

```
[SW5500]multicast routing-enable
```

2 Enable IGMP and PIM-DM.

```
[SW5500]vlan 10
[SW5500-vlan10]port gigabitethernet 1/0/2 to gigabitethernet 1/0/3
[SW5500-vlan10]quit
[SW5500]vlan 11
[SW5500-vlan11]port gigabitethernet 1/0/4 to gigabitethernet 1/0/5
[SW5500-vlan11]quit
[SW5500]vlan 12
[SW5500-vlan12]port gigabitethernet 1/0/6 to gigabitethernet 1/0/7
[SW5500-vlan12]quit
[SW5500]interface vlan-interface 10
[SW5500-vlan-interface10]ip address 1.1.1.1 255.255.0.0
[SW5500-vlan-interface10]igmp enable
[SW5500-vlan-interface10]pim dm
[SW5500-vlan-interface10]quit
[SW5500]interface vlan-interface 11
[SW5500-vlan-interface11]ip address 2.2.2.2 255.255.0.0
[SW5500-vlan-interface11]igmp enable
[SW5500-vlan-interface11]pim dm
[SW5500-vlan-interface11]quit
[SW5500]interface vlan-interface 12
[SW5500-vlan-interface12]ip address 3.3.3.3 255.255.0.0
[SW5500-vlan-interface12]igmp enable
[SW5500-vlan-interface12]pim dm
```

PIM-SM Overview

PIM-SM (Protocol Independent Multicast, Sparse Mode) is a multicast routing protocol, appropriate for large-scale networks (for example a WAN) where multicast group members are relatively sparse.

PIM-SM assumes that all hosts do not need to receive multicast packets, unless there is an explicit request for the packets. PIM-SM uses the RP (Rendezvous Point) and the BSR (Bootstrap Router) to advertise multicast information to all PIM-SM routers, and uses the join/prune information of the router to build the RP-rooted shared tree (RPT). This reduces the bandwidth occupied by data packets and control packets, and reduces the processing overhead on the router.

Multicast data flows along the shared tree to the network segments that have multicast group members. When the data traffic is sufficient, the multicast data flow can switch over to the SPT (Shortest Path Tree) rooted on the source to reduce network delay. PIM-SM does not depend on the specified unicast routing protocol but uses the present unicast routing table to perform the RPF check.

When running PIM-SM the user needs to configure candidate RPs and BSRs. The BSR is responsible for collecting the information from the candidate RP and advertising the information.

PIM-SM Operating Principle

The working procedures for PIM-SM include: neighbor discovery, building the RP-rooted shared tree (RPT), multicast source registration and switch over to the SPT.

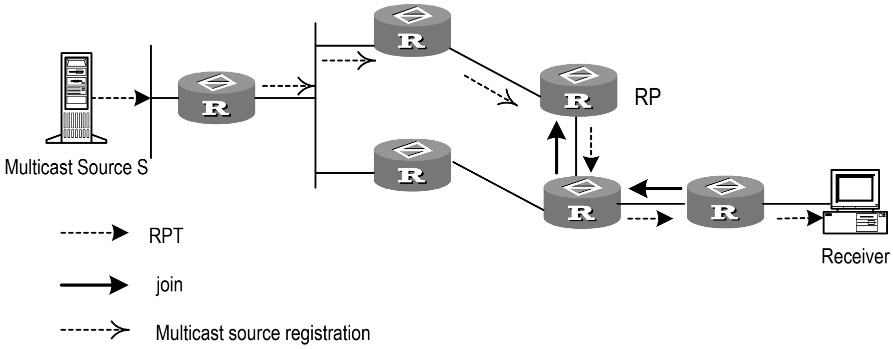
Neighbor Discovery

The PIM-SM router uses Hello messages to perform neighbor discovery when it is started. All network nodes running PIM-SM stay in touch with one another by periodically sending Hello messages.

Build the RP Shared Tree (RPT)

When hosts join a multicast group G, the leaf routers that directly connect with the hosts send IGMP messages to learn the receivers of multicast group G. In this way, the leaf routers calculate the corresponding rendezvous point (RP) for multicast group G and then send join messages to the node of a higher level toward the rendezvous point (RP). Each router along the path between the leaf routers and the RP will generate (*, G) entries in the forwarding table, indicating that all packets sent to multicast group G are applicable to the entries no matter from which source they are sent. When the RP receives the packets sent to multicast group G, the packets will be sent to leaf routers along the path built and then reach the hosts. In this way, an RP-rooted tree (RPT) is built as shown in Figure 45.

Figure 45 RPT schematic diagram



Multicast Source Registration

When multicast source S sends a multicast packet to the multicast group G, the PIM-SM multicast router directly connected to S will encapsulate the received packet into a registration packet and send it to the corresponding RP in unicast form. If there are multiple PIM-SM multicast routers on a network segment, the Designated Router (DR) will be responsible for sending the multicast packet.

Preparations before Configuring PIM-SM

Configuring Candidate RPs

In a PIM-SM network, multiple RPs (candidate-RPs) can be configured. Each Candidate-RP (C-RP) is responsible for forwarding multicast packets with the destination addresses in a certain range. Configuring multiple C-RPs is to implement load balancing of the RP. These C-RPs are equal. All multicast routers calculate the RPs corresponding to multicast groups according to the same algorithm after receiving the C-RP messages that the BSR advertises.

It should be noted that one RP can serve multiple multicast groups or all multicast groups. Each multicast group can only be uniquely correspondent to one RP at a time rather than multiple RPs.

Configuring BSRs

The BSR is the management core in a PIM-SM network. Candidate-RPs send announcement to the BSR, which is responsible for collecting and advertising the information about all candidate-RPs.

It should be noted that there can be only one BSR in a network but you can configure multiple candidate-BSRs. In this case, once a BSR fails, you can switch over to another BSR. A BSR is elected among the C-BSRs automatically. The C-BSR with the highest priority is elected as the BSR. If the priority is the same, the C-BSR with the largest IP address is elected as the BSR.

Configuring Static RP

The router that serves as the RP is the core router of multicast routes. If the dynamic RP elected by BSR mechanism is invalid for some reason, the static RP can be configured to specify RP. As the backup of dynamic RP, static RP improves network resilience and enhances the operation and management capability of multicast network.

Configuring PIM-SM

PIM-SM basic configuration includes:

- Enabling Multicast
- Enabling PIM-SM
- Configuring the PIM-SM Domain Border
- Entering the PIM View
- Configuring Candidate-BSRs
- Configuring Candidate-RPs
- Configuring Static RP

PIM-SM advanced configuration includes:

- Configuring the Sending Interval for the Hello Packets of the Interface
- Configuring the Filtering of Multicast Source/Group
- Configuring the Filtering of PIM Neighbor
- Configuring the Maximum Number of PIM Neighbor on an Interface
- Configuring RP to Filter the Register Messages Sent by DR
- Limiting the Range of Legal BSR
- Limiting the Range of Legal C-RP
- Clearing Multicast Route Entries from PIM Routing Table
- Clearing PIM Neighbors

It should be noted that at least one router in an entire PIM-SM domain should be configured with Candidate-RPs and Candidate-BSRs.

Enabling Multicast

Refer to "Common Multicast Configuration" on page 177.

Enabling PIM-SM

This configuration can be effective only after multicast is enabled.

Perform the following configuration in Interface view.

Table 211 Enabling PIM-SM

Operation	Command
Enable PIM-SM on an interface	**`pim sm`**
Disable PIM-SM on an interface	**`undo pim sm`**

Repeat this configuration to enable PIM-SM on other interfaces. Only one multicast routing protocol can be enabled on an interface at a time.

Once enabled PIM-SM on an interface, PIM-DM cannot be enabled on the same interface and vice versa.

Configuring the PIM-SM Domain Border

After the PIM-SM domain border is configured, bootstrap messages cannot cross the border in any direction. In this way, the PIM-SM domain can be split.

Perform the following configuration in Interface view.

Table 212 Configuring the PIM-SM domain border

Operation	Command
Set the PIM-SM domain border	`pim bsr-boundary`
Remove the PIM-SM domain border configured	`undo pim bsr-boundary`

By default, no domain border is set. After this configuration is performed, a bootstrap message cannot cross the border but other PIM packets can. This configuration can effectively divide a network into domains using different BSRs.

Entering the PIM View

Global parameters of PIM should be configured in PIM view.

Perform the following configuration in system view.

Table 213 Entering the PIM view

Operation	Command
Enter the PIM view	`pim`
Back to system view	`undo`

Using `undo pim` command, you can clear the configuration in PIM view, and back to system view.

Configuring Candidate-BSRs

In a PIM domain, one or more candidate BSRs should be configured. A BSR (Bootstrap Router) is elected among candidate BSRs. The BSR takes charge of collecting and advertising RP information.

The automatic election among candidate BSRs operates as follows:

- One interface which has started PIM-SM must be specified when configuring the router as the candidate BSR.
- At first, each candidate BSR considers itself as the BSR of the PIM-SM domain, and sends a Bootstrap message by taking the IP address of the interface as the BSR address.
- When receiving Bootstrap messages from other routers, the candidate BSR will compare the BSR address of the newly received Bootstrap message with that of itself. Comparison standards include priority and IP address. The bigger IP

address is considered better when the priority is the same. If the new BSR address is better, the candidate BSR will replace its BSR address and stop regarding itself as the BSR. Otherwise, the candidate BSR will keep its BSR address and continue to regard itself as the BSR.

Perform the following configuration in PIM view.

Table 214 Configuring candidate-BSRs

Operation	Command
Configure a candidate-BSR	**c-bsr** *interface-type interface_number hash_mask_len* [*priority*]
Remove the candidate-BSR configured	**undo c-bsr**

Candidate-BSRs should be configured on the routers in the network backbone. By default, no BSR is set. The default priority is 0.

One Switch can only be configured with one candidate-BSR. When a candidate-BSR is configured on another interface, it will replace the previous configuration.

Configuring Candidate-RPs

In PIM-SM, the shared tree built by the multicast routing data is rooted at the RP. There is a mapping from a multicast group to an RP. A multicast group can be mapped to an RP. Different groups can be mapped to one RP.

Perform the following configuration in PIM view.

Table 215 Configuring candidate-RPs

Operation	Command
Configure a candidate-RP	**c-rp** *interface_type interface_number* [**group-policy** *acl_number* | **priority** *priority_value*]*
Remove the candidate-RP configured	**undo c-rp** { *interface_type interface_number* | **all** }

When configuring RP, if the range of the served multicast group is not specified, the RP will serve all multicast groups. Otherwise, the range of the served multicast group is the multicast group in the specified range. 3Com recommends that you configure Candidate RP on the backbone router.

Configuring Static RP

Static RP serves as the backup of dynamic RP, so as to improve network robusticity.

Perform the following configuration in PIM view.

Table 216 Configuring Static RP

Operation	Command
Configure static RP	**static-rp** *rp_address* [*acl_number*]
Remove the configured static RP	**undo static-rp** *rp_address*

Basic ACL can control the range of multicast group served by static RP.

If static RP is in use, all routers in the PIM domain must adopt the same configuration. If the configured static RP address is the interface address of the local router whose state is UP, the router will function as the static RP. It is unnecessary to enable PIM on the interface that functions as static RP.

When the RP elected from BSR mechanism is valid, static RP does not work.

Configuring the Sending Interval for the Hello Packets of the Interface

Generally, PIM-SM advertises Hello messages periodically on the interface enabled with it to detect PIM neighbors and discover which router is the Designated Router (DR).

Perform the following configuration in Interface view.

Table 217 Configuring the sending interval for the Hello packets of the interface

Operation	Command
Configure the sending interval for the Hello packets of the interface	**pim timer hello** *seconds*
Restore the interval to the default value	**undo pim timer hello**

By default, the hello message interval is 30 seconds. Users can configure the value according to different network environments.

This configuration can be performed only after the PIM (PIM-DM or PIM-SM) is enabled in Interface view.

Configuring the Filtering of Multicast Source/Group

Refer to "PIM-DM Overview" on page 186.

Configuring the Filtering of PIM Neighbor

Refer to "PIM-DM Overview" on page 186.

Configuring the Maximum Number of PIM Neighbor on an Interface

Refer to "PIM-DM Overview" on page 186.

Configuring RP to Filter the Register Messages Sent by DR

In the PIM-SM network, the register message filtering mechanism can control which sources to send messages to which groups on the RP, i.e., RP can filter the register messages sent by DR to accept specified messages only.

Perform the following configuration in PIM view.

Table 218 Configuring RP to filter the register messages sent by DR

Operation	Command
Configure RP to filter the register messages sent by DR	**register-policy** *acl_number*
Cancel the configured filter of messages	**undo register-policy**

If an entry of a source group is denied by the ACL, or the ACL does not define operation to it, or there is no ACL defined, the RP will send RegisterStop messages to the DR to prevent the register process of the multicast data stream.

Only the register messages matching the ACL `permit` *clause can be accepted by the RP. Specifying an undefined ACL will make the RP to deny all register messages.*

Limiting the Range of Legal BSR

In the PIM SM network using BSR (bootstrap router) mechanism, every router can set itself as C-BSR (candidate BSR) and take the authority to advertise RP information in the network once it wins in the contention. To prevent malicious BSR proofing in the network, the following two measures need to be taken:

- Prevent the router from being spoofed by hosts though faking legal BSR messages to modify RP mapping. BSR messages are of multicast type and their TTL is 1, so this type of attacks often hit edge routers. Fortunately, BSRs are inside the network, while assaulting hosts are outside, therefore neighbor and RPF checks can be used to stop this type of attack.
- If a router in the network is manipulated by an attacker, or an illegal router is accessed into the network, the attacker may set itself as C-BSR and try to win the contention and gain authority to advertise RP information among the network. Since the router configured as C-BSR shall propagate BSR messages, which are multicast messages sent hop by hop with TTL as 1, among the network, then the network cannot be affected as long as the peer routers do not receive these BSR messages. One way is to configure **`bsr-policy`** on each router to limit legal BSR range, for example, only 1.1.1.1/32 and 1.1.1.2/32 can be BSR, thus the routers cannot receive or forward BSR messages other than these two. Even legal BSRs cannot contest with them.

Perform the following configuration in PIM View.

Table 219 Limiting the range of legal BSR

Operation	Command
Set the legal BSR range limit	**`bsr-policy`** *`acl_number`*
Restore to the default setting	**`undo bsr-policy`**

For detailed information of **`bsr-policy`**, please refer to the command manual.

Limiting the Range of Legal C-RP

In the PIM-SM network using BSR mechanism, every router can set itself as C-RP (candidate rendezvous point) servicing particular groups. If elected, a C-RP becomes the RP servicing the current group.

In BSR mechanism, a C-RP router unicasts C-RP messages to the BSR, which then propagates the C-RP messages among the network by BSR message. To prevent C-RP spoofing, you need to configure **`crp-policy`** on the BSR to limit legal C-RP range and their service group range. Since each C-BSR has the chance to become BSR, you must configure the same filtering policy on each C-BSR router.

Perform the following configuration in PIM view.

Table 220 Limiting the range of legal C-RP

Operation	Command
Set the legal C-RP range limit	**crp-policy** *acl-number*
Restore to the default setting	**undo crp-policy**

For detailed information of **crp-policy**, please refer to the command manual.

Clearing Multicast Route Entries from PIM Routing Table

Refer to "PIM-DM Overview" on page 186.

Clearing PIM Neighbors

Refer to "PIM-DM Overview" on page 186.

Displaying and Debugging PIM-SM

After the above configuration, execute display command in any view to display the running of PIM-SM configuration, and to verify the effect of the configuration.

Execute **debugging** command in user view for the debugging of PIM-SM.

Table 221 Displaying and debugging PIM-SM

Operation	Command
Display the BSR information	**display pim bsr-info**
Display the RP information	**display pim rp-info** [*group-address*]
Enable the PIM-SM debugging	**debugging pim sm** { **all** | **verbose** | **mrt** | **warning** | **mbr** { **alert** | **fresh** } | **timer** { **assert** | **bsr** | **crpadv** | **jp** | **jpdelay** | **mrt** | **probe** | **spt** } | { **recv** | **send** } { **assert** | **bootstrap** | **crpadv** | **reg** | **regstop** | **jp** } }
Disable the PIM-SM debugging	**undo debugging pim sm** { **all** | **verbose** | **mrt** | **warning** | **mbr** { **alert** | **fresh** } | **timer** { **assert** | **bsr** | **crpadv** | **jp** | **jpdelay** | **mrt** | **probe** | **spt** } | { **recv** | **send** } { **assert** | **bootstrap** | **crpadv** | **reg** | **regstop** | **jp** } }

PIM-SM Configuration Example

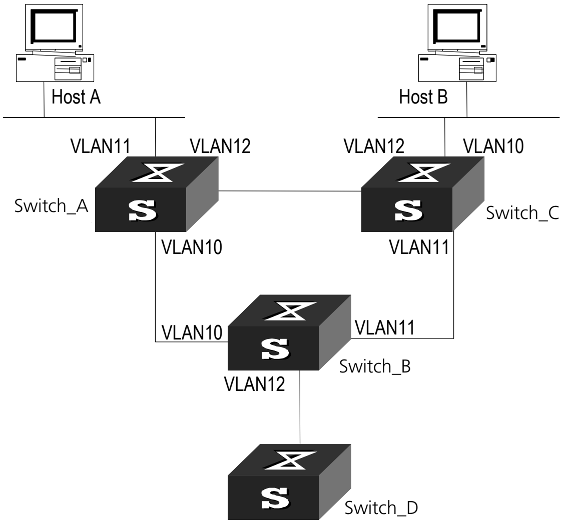
Networking Requirements

In actual network, we assume that the switches can intercommunicate.

Suppose that Host A is the receiver of the multicast group at 225.0.0.1. Host B begins transmitting data destined to 225.0.0.1. Switch_A receives the multicast data from Host B via Switch_B.

Networking Diagram

Figure 46 PIM-SM configuration networking



Configuration Procedure

1 On Switch_A:

a Enable PIM-SM.

```
[SW5500]multicast routing-enable
[SW5500]vlan 10
[SW5500-vlan10]port gigabitethernet 1/0/2 to gigabitethernet 1/0/3
[SW5500-vlan10]quit
[SW5500]interface vlan-interface 10
[SW5500-vlan-interface10]igmp enable
[SW5500-vlan-interface10]pim sm
[SW5500-vlan-interface10]quit
[SW5500]vlan 11
[SW5500-vlan11]port gigabitethernet 1/0/4 to gigabitethernet 1/0/5
[SW5500-vlan11]quit
[SW5500]interface vlan-interface 11
[SW5500-vlan-interface11]igmp enable
[SW5500-vlan-interface11]pim sm
[SW5500-vlan-interface11]quit
[SW5500]vlan 12
[SW5500-vlan12]port gigabitethernet 1/0/6 to gigabitethernet 1/0/7
[SW5500-vlan12]quit
[SW5500]interface vlan-interface 12
[SW5500-vlan-interface12]igmp enable
[SW5500-vlan-interface12]pim sm
[SW5500-vlan-interface12]quit
```

2 On Switch_B:

a Enable PIM-SM.

```
[SW5500]multicast routing-enable
[SW5500]vlan 10
[SW5500-vlan10]port gigabitethernet 1/0/2 to giagbitethernet 1/0/3
[SW5500-vlan10]quit
[SW5500]interface vlan-interface 10
```

```
[SW5500-vlan-interface10]igmp enable
[SW5500-vlan-interface10]pim sm
[SW5500-vlan-interface10]quit
[SW5500]vlan 11
[SW5500-vlan11]port gigabitethernet 1/0/4 to gigabitethernet 1/0/5
[SW5500-vlan11]quit
[SW5500]interface vlan-interface 11
[SW5500-vlan-interface11]igmp enable
[SW5500-vlan-interface11]pim sm
[SW5500-vlan-interface11]quit
[SW5500]vlan 12
[SW5500-vlan12]port gigabitethernet 1/0/6 to gigabitethernet 1/0/7
[SW5500-vlan12]quit
[SW5500]interface vlan-interface 12
[SW5500-vlan-interface12]igmp enable
[SW5500-vlan-interface12]pim sm
[SW5500-vlan-interface12]quit
```

b Configure the C-BSR.

```
[SW5500]pim
[SW5500-pim]c-bsr vlan-interface 10 30 2
```

c Configure the C-RP.

```
[SW5500]acl number 2000
[SW5500-acl-basic-2000]rule permit source 225.0.0.0 0.255.255.255
[SW5500]pim
[SW5500-pim]c-rp vlan-interface 10 group-policy 2000
```

d Configure PIM domain border.

```
[SW5500]interface vlan-interface 12
[SW5500-vlan-interface12]pim bsr-boundary
```

After VLAN-interface 12 is configured as the domain border, Switch_D will be excluded from the local PIM domain and will no longer receive the BSR information transmitted from Switch_B.

3 On Switch_C:

a Enable PIM-SM.

```
[SW5500]multicast routing-enable
[SW5500]vlan 10
[SW5500-vlan10]port gigabitethernet 1/0/2 to gigabitethernet 1/0/3
[SW5500-vlan10]quit
[SW5500]interface vlan-interface 10
[SW5500-vlan-interface10]igmp enable
[SW5500-vlan-interface10]pim sm
[SW5500-vlan-interface10]quit
[SW5500]vlan 11
[SW5500-vlan11]port gigabitethernet 1/0/4 to gigabitethernet 1/0/5
[SW5500-vlan11]quit
[SW5500]interface vlan-interface 11
[SW5500-vlan-interface11]igmp enable
[SW5500-vlan-interface11]pim sm
[SW5500-vlan-interface11]quit
[SW5500]vlan 12
[SW5500-vlan12]port gigabitethernet 1/0/6 to gigabitethernet 1/0/7
[SW5500-vlan12]quit
[SW5500]interface vlan-interface 12
```

```
[SW5500-vlan-interface12]igmp enable
[SW5500-vlan-interface12]pim sm
[SW5500-vlan-interface12]quit
```

8 ACL CONFIGURATION

This chapter covers the following topics:

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.

The case of filter or classify the 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.

Table 222 Hardware Match Order of ACL's sub-rule

Switch	Harware match order of ACL's sub-rule
Switch 5500G-EI	An ACL is configured with multiple sub-rules. The latest sub-rule will be matched first.

The case includes: ACL cited by QoS function, ACL used for filter the packet transmitted by the hardware and so on.

The case of filter or classify the 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, i.e. 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 223 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:

- Configuring Time-Range
- Defining ACL
- Activating ACL

The above three steps must be done in sequence. Configure the time range first and then define the ACL (using the defined time range in the definition), then activate the ACL to validate it.

Configuring Time-Range

The process of configuring a time-range includes: configuring the hour-minute range, date ranges and period range. The hour-minute range is expressed in units of minute, hour. Date range is expressed in units of minute, hour, date, month and year. The periodic time range is expressed as the day of the week.

You can use the following command to set the time range by performing the following configuration in the System View.

Table 224 Set the Absolute Time Range

Operation	Command
Set the time range	**time-range** *time-name* **{** *start_time* **to** *end_time days_of_the_week* **[from** *start_time start_date* **] [to** *end_time end_date* **] | from** *start_time start_date* **[to** *end_time end_date* **] | to** *end_time end_date* **}**
Delete the time range	**undo time-range** *time-name* **[** *start_time* **to** *end_time days_of_the_week* **[from** *start_time start_date* **] [to** *end_time end_date* **] | from** *start_time start_date* **[to** *end_time end_date* **] | to** *end_time end_date* **]**

When the start-time and end-time are not configured, it will be all the time for one day. The end time shall be later than the start time.

When *end-time end-date* is not configured, it will be all the time from now to the date which can be displayed by the system. The end time shall be later than the start time.

Defining ACL

The Switch 5500G-EI 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, i.e. 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 225 Define Basic ACL

Operation	Command
Enter basic ACL view (from System View)	**acl number** *acl_number* **[match-order { config | auto }]**
add a sub-item to the ACL (from Basic ACL View)	**rule [** *rule_id* **] { permit | deny } [source {** *source_addr wildcard* **| any } | fragment | logging | time-range** *name* **]***
delete a sub-item from the ACL (from Basic ACL View)	**undo rule** *rule_id* **[source | fragment | logging | time-range]***
Delete one ACL or all the ACL (from System View)	**undo acl { number** *acl_number* **| all }**

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 226 Define Advanced ACL

Operation	Command
Enter advanced ACL view (from System View)	**acl number** *acl_number* **[match-order { config | auto }]**
Add a sub-item to the ACL (from Advanced ACL View)	**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 | logging | time-range** *name* **]***
Delete a sub-item from the ACL (from Advanced ACL View)	**undo rule** *rule_id* **[source | destination | source-port | destination-port | icmp-type | precedence | tos | dscp | fragment | logging | time-range | vpn-instance]***
Delete one ACL or all the ACL (from System View)	**undo acl { number** *acl_number* **| 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 227 Define Layer-2 ACL

Operation	Command
Enter Layer-2 ACL view (from System View)	**acl number** *acl_number* **[match-order { config | auto }**
Add a sub-item to the ACL (from Layer-2 ACL View)	**rule [** *rule_id* **] { permit | deny } [[type** *protocol_type type_mask* | **lsap** *lsap_type type_mask* **]** | *format_type* | **cos** *cos* | **source {** *source_vlan_id* | *source_mac_addr source_mac_wildcard* **}*** | **dest {** *dest_mac_addr dest_mac_wildcard* **}** | **time-range** *name* **]***
Delete a sub-item from the ACL (from Layer-2 ACL View)	**undo rule** *rule_id*
Delete one ACL or all the ACL (from System View)	**undo acl { number** *acl_number* | **all }**

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 228 Activate ACL

Operation	Command
Activate an ACL	**packet-filter inbound ip-group** *acl_number* **[rule** *rule* **[link-group** *acl_number* **rule** *rule* **]]** | **link-group** *acl_number* **[rule** *rule* **] }**
Deactivate an ACL	**undo packet-filter ip-group** *acl_number* **[rule** *rule* **[link-group** *acl_number* **[rule** *rule* **] }**

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 229 Display and Debug ACL

Operation	Command
Display the status of the time range	**display time-range { all** | *name* **}**
Display the detail information about the ACL	**display acl { all** | *acl_number* **}**
Display the information about the ACL running state	**display packet-filter { interface {** *interface_name* | *interface_type interface_num* **}** | **unitid** *unit_id* **}**
Clear ACL counters	**reset acl counter { all** | *acl_number* **}**

The matched information of **display acl** command specifies the rules treated by the software.

For syntax description, refer to the Command Reference Manual.

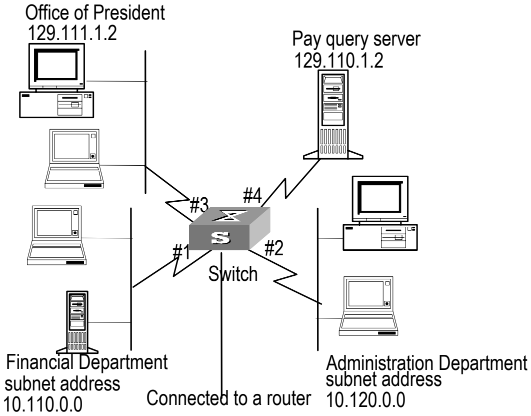
Advanced ACL Configuration Example

Networking Requirements

The interconnection between different departments on a company network is implemented through the 1000 Mbps ports of the Switch. The IP address of the payment query server of the Financial Dept. is 129.110.1.2. Financial Dept is accessed via GigabitEthernet1/0/1. 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 47 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.

```
[SW5500]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.

```
[SW5500]acl number 3000 match-order config
```

b Define the rules for other department to access the payment server.

```
[SW5500-acl-adv-3000]rule 1 deny ip source any destination
129.110.1.2 0.0.0.0 time-range 3Com
```

c Define the rules for the President's Office to access the payment server.

```
[SW5500-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.

```
[SW5500-GigabitEthernet1/0/1]packet-filter inbound ip-group 3000
```

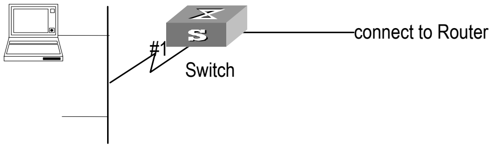
Basic ACL Configuration Example

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 GigabitEthernet1/0/1 of the Switch.

Networking Diagram

Figure 48 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.

```
[SW5500]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.

```
[SW5500]acl number 2000
```

b Define the rules for packet which source IP is 10.1.1.1.

```
[SW5500-acl-basic-2000]rule 1 deny source 10.1.1.1 0 time-range 3Com
```

3 Activate ACL.

Activate the ACL 2000.

```
[SW5500-GigabitEthernet1/0/1]packet-filter inbound ip-group 2000
```

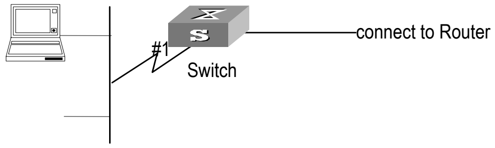
Link ACL Configuration Example

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 GigabitEthernet1/0/1.

Networking Diagram

Figure 49 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.

```
[SW5500]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.

```
[SW5500]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.

```
[SW5500-acl-ethernetframe-4000]rule 1 deny source 00e0-fc01-0101
ffff-ffff-ffff source 00e0-fc01-0303 ffff-ffff-ffff time-range 3Com
```

3 Activate ACL.

Activate the ACL 4000 .

```
[SW5500-GigabitEthernet1/0/1]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 Switche enables the filtering of various information carried in Layer 2 traffic to discard the useless, unreliable or doubtful traffic, thereby enhancing the 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, i.e. 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.

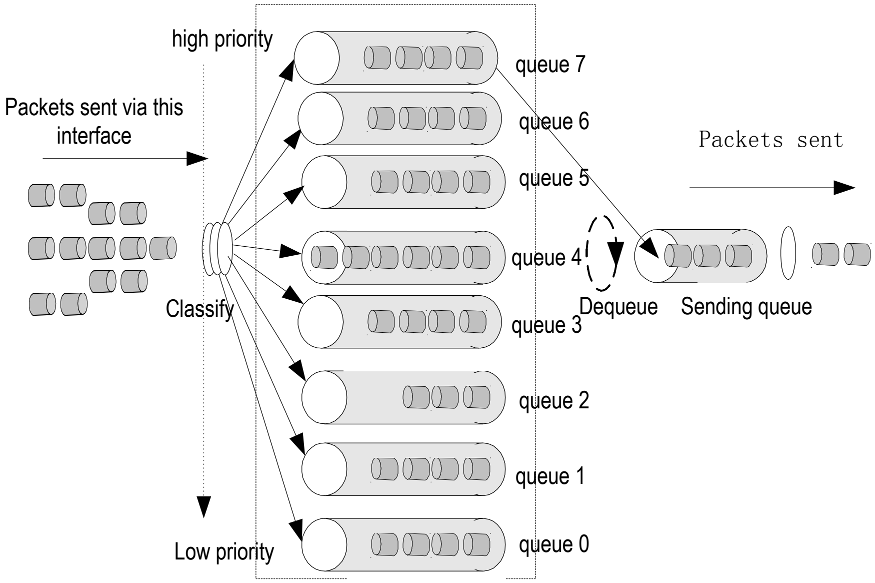
Traffic Priority

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 algorithms are used to overcome the problem. Here Strict-Priority Queue (SP) queue scheduling algorithm is introduced.

Figure 50 SP



The SP is designed for the key service application. A significant feature of the key service is the need for priority to enjoy the service to reduce the responding delay when congestion occurs. Take 8 egress queues for each port as an example, SP divides the queue of the port into up to 8 kinds, from high-priority queue to low-priority queue (which are shown as the Queue 7, 6, 5, 4, 3, 2, 1 and 0 in turn) with sequentially reduced priority.

During the progress of queue dispatching, strictly following the priority order from high to low, the SP gives preference to and sends the packets in the higher-priority queue first. When the higher-priority queue is empty it will send the packets in the lower-priority group. In this way, put the packets of higher priority service in the higher-priority queue and put the packets of lower priority, like e-mail, in the lower-priority queue, can guarantee the key service packets of higher priority are transmitted first, while the packets of lower service priority are transmitted during the idling gap between transmitting the packets of higher service priorities.

Note that SP has the drawback that when congestion occurs, if there are many packets queuing in the higher-priority queue, it will require a long time to transmit these packets of higher service priority while the messages in the lower-priority queue are continuously set aside without service.

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 QoS based traffic:

1. Identify the traffic by ACL
2. Perform the QoS operation to the traffic.

The configuration steps of QoS based traffic:

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 configue 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 230 Setting Port Priority

Operation	Command
Set the port priority	**`priority`** *`priority_level`*
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 port priority is 0 and 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 231 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 multi mirroring port. If several Switches form a Fabric, 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 232 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 233 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 234 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 235 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 236 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 237 Configuring Traffic Mirroring

Operation	Command
Configure traffic mirroring	**mirrored-to inbound ip-group** *acl_number* **[rule** *rule* **[link-group** *acl_number* **rule** *rule* **]]** | **link-group** *acl_number* **[rule** *rule* **] } { cpu** | **monitor-interface }**

Delete Traffic Mirroring

1 Delete traffic mirroring

Perform the following configuration in the Ethernet Port View.

Table 238 Delete Traffic Mirroring

Operation	Command
Cancel the configuration of traffic mirroring	**undo mirrored-to inbound {ip-group {** *acl_number* | *acl_name* **} [rule** *rule* **]** | **link-group {** *acl_number* | *acl_name* **} [rule** *rule* **] }**

2 Delete monitor port.

Perform the following configuration in the Ethernet Port View.

Table 239 Delete Monitor Port

Operation	Command
Delete monitor port	**undo monitor**

For details about the command, refer to the *Command Manual*.

Setting Queue Scheduling

Queue scheduling is commonly used to resolve the problem that multiple messages compete for resource when the network congestion happens. The queue scheduling function puts the packet to the output queue of the port according to the 802.1p priority of the packet. The mapping relationship between 802.1p priority and output queue of the port is as shown in Table 240.

Table 240 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 the Ethernet Port View.

Table 241 Configure the Queue Scheduling Algorithm

Operation	Command
Configure the queue scheduling algorithm	**queue-scheduler { wrr** *queue1_weight queue2_weight queue3_weight queue4_weight queue5_weight queue6_weight queue7_weight queue8_weight* **}**
Restore the default queue scheduling algorithm	**undo queue-scheduler**

By default, the Switch uses the WRR algorithm.

For details about the command, refer to the Command Reference Manual.

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 242 Setting Traffic Limit

Operation	Command
Set traffic limit	**traffic-limit inbound { ip-group** *acl_number* **[rule** *rule* **[link-group** *acl_number* **rule** *rule* **]] | link-group** *acl_number* **[rule** *rule* **] }** *target_rate* **[exceed** *action* **]**
Remove traffic limit	**undo traffic-limit inbound { ip-group** *acl-number* **[rule** *rule* **[link-group** *acl_number* **rule** *rule* **]] | link-group** *acl_number* **[rule** *rule* **] }**

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 automaticaly 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 243 Setting Line Rate

Operation	Command
Set line limit	**line-rate outbound** *target_rate*
Remove line limit	**undo line-rate outbound**

Relabeling Priority Level

This configuration re-labels priority level for the packets that match ACL. The new priority label can be put in the priority domain in the header.

Perform the following configurations in the Ethernet Port View.

Table 244 Relabeling Priority Level

Operation	Command
Relabel traffic priority	traffic-priority inbound |ip-group acl_number [rule rule [link-group acl_number rule rule]] | link-group acl_number [rule rule] } { { dscp dscp_value | ip-precedence { pre_value | from-cos } } | cos { pre_value | from-ipprec } | local-precedence pre_value }*
Remove the setting	undo traffic-priority inbound ip-group acl-number [rule rule [link-group acl_number rule rule]] | link-group acl_number [rule rule] }

Configuring Packet Redirection

Packet redirection is to redirect the packets to be forwarded to CPU or other output port.

You can use the following command in Ethernet Port View to configure the packet redirection.

Table 245 Configuring Redirection

Operation	Command
Relabel traffic priority	traffic-redirect inbound { ip-group acl_number [rule rule [link-group acl_number rule rule]] | link-group acl_number [rule rule] } { cpu | interface { interface-name | interface-type interface-num } }
Remove the setting	undo traffic-redirect inbound { ip-group acl_number [rule rule [link-group acl_number rule rule]] | link-group acl_number [rule rule] } { cpu | interface { interface-name | interface-type interface-num } }

For futher details about the `traffic-redirect` command, please refer to the Command Reference Guide.

Configuring Traffic Statistics

The traffic statistics function is used for counting the data packets of the specified traffic, that is, this function counts the transmitted data which matches the ACL rules. After the traffic statistics function is configured, the user can use **display qos-interface traffic-statistic** command to display the statistics information.

You can use the following command to configure traffic statistics.

Perform the following configuration in the Ethernet Port View.

Table 246 Configuring Traffic Statistics

Operation	Command
Configure traffic statistics	traffic-statistic inbound ip-group acl_number [rule rule [link-group acl_number rule rule]] | link-group acl_number [rule rule] }

Operation	Command
Cancel the configuration of traffic statistics	**undo traffic-statistic inbound ip-group** *acl_number* **[rule** *rule* **[link-group** *acl_number* **rule** *rule* **]] | link-group** *acl_number* **[rule** *rule* **] }**
Display the statistics information	**display qos-interface {** *interface_name* | *interface_type interface_num* | *unit_id* **} traffic-statistic**

For details about the command, refer to the Command Reference Manual.

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 247 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 {** *interface_name* | *interface_type interface_num* | *unit_id* **} line-rate**
Display port QoS configuration	**display qos-interface {** *interface_name* | *interface_type interface_num* | *unit_id* **} all**
Display traffic limit	**display qos-interface {** *interface_name* | *interface_type interface_num* | *unit_id* **} traffic-limit**
Display priority label	**display qos-interface {** *interface_name* | *interface_type interface_num* | *unit_id* **} traffic-priority**
Display the settings of the traffic mirror	**display qos-interface {** *interface_name* | *interface_type interface_num* | *unit_id* **} mirrored-to**
Display the setting of the redirection parameters	**display qos-interface {** *interface_name* | *interface_type interface_num* | *unit_id* **} traffic-redirect**
Display the traffic statistics information	**display qos-interface {** *interface_name* | *interface_type interface_num* | *unit_id* **} traffic-statistic**

QoS Configuration Example

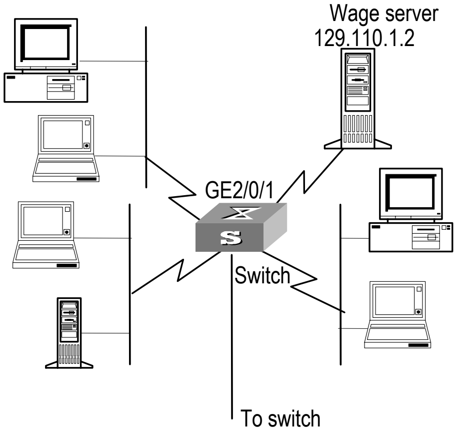
Traffic Limit and Line Rate Configuration Example

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 51 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.

```
[SW5500]acl number 3000
```

b Define the traffic-of-payserver rule in the advanced ACL 3000.

```
[SW5500-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.

```
[SW5500-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.

```
[SW5500-Ethernet1/0/1]line-rate outbound 128
```

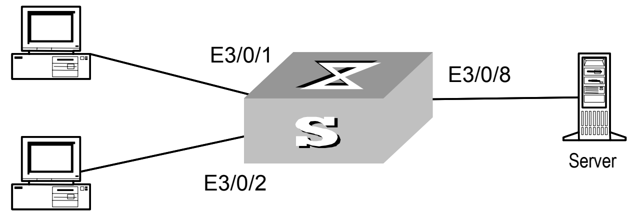
Port Mirroring Configuration Example

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 52 QoS Configuration Example



Configuration Procedure

Define port mirroring, with monitoring port being Ethernet3/0/8.

```
[SW5500-Ethernet3/0/8]monitor-port
[SW5500-Ethernet3/0/1]mirroring-port both
```

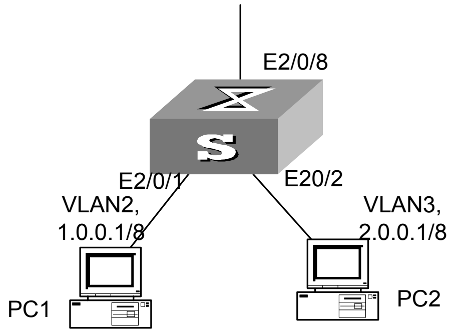
Priority Relabeling Configuration Example

Networking Requirement

In this example, ef labels are appended on packets sent between 8:00 and 18:00 each day from PC1 (IP 1.0.0.2), as priority labeling reference for the upper-layer device.

Networking Diagram

Figure 53 QoS Configuration Example



Configuration Procedure

1 Define the time range.

Define the time range 8:00~18:00.

```
[SW5500]time-range 3Com 8:00 to 18:00 daily
```

2 Define traffic rules for PC packets.

a Enter the number-based basic ACL and select the ACL 2000.

```
[SW5500]acl number 2000
```

b Define traffic classification rules for PC1 packets.

```
[SW5500-acl-basic-2000]rule 0 permit source 1.0.0.2 0 time-range
3Com
```

3 Relabel ef priority for PC1 packets.

```
[SW5500-Ethernet1/0/1]traffic-priority inbound ip-group 2000 dscp ef
```

QoS Profile Configuration

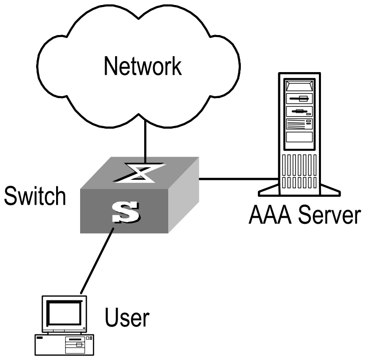
When used together with the 802.1x authentication function, the QoS profile function can offer preconfigured QoS settings for a qualified user in authentication (or a group of users).

When the user passes the 802.1x authentication, the Switch delivers the right profile dynamically to the port from which the user is accessed after referring to the mapping between user names and profiles stored on the AAA server.

The QoS profile function can offer packet filtering, traffic policing and preference replacing functions together.

QoS Profile Configuration

Figure 54 QoS Profile Configuration Environment



QoS profile configuration details:

Table 248 QoS Profile Configuration

Device	Configuration	Default	Description
AAA server	Configure user authentication information	—	—
	Configure mapping between user names and QoS profile	—	Multiple users can correspond to the same QoS profile.
Switch	Enable 802.1x authentication function	—	Refer to the Security part of this manual for detailed configuration.
	Define application mode on the port of QoS profile	Port-based mode	You can change it to user-based mode
	Configure QoS profile, including packet filtering, traffic policing and preference replacing	—	First define an ACL and then configure the QoS function. Refer to the ACL chapter of the QoS/ACL module for defining ACL
	Apply QoS profile to the port	—	You can apply the QoS profile actions to the current port with the right commands.

Configuring QoS Profile

You must first define ACLs for the traffic actions before adding the actions to the QoS profile.

Entering QoS Profile View

To configure the QoS profile, you must first enter QoS profile view.

Perform the following configuration in System View.

Table 249 Entering QoS Profile View

Operation	Command
Enter QoS profile view	**qos-profile** *profile-name*
Delete the QoS profile	**undo qos-profile** *profile-name*

You cannot delete the specific QoS profile which has been applied to the port.

Adding/Removing Traffic Action to a QoS Profile

From the QoS Profile View, you can configure the QoS actions for current QoS profile. The maximum action numbers in one QoS profile is 32.

Perform the following configuration in QoS Profile View.

Table 250 Adding/Removing Traffic Action to QoS Profile

Operation	Command
Add packet filtering action	packet-filter inbound ip-group acl_number [rule rule [link-group acl_number rule rule]] | link-group acl_number [rule rule] }
Add traffic policing action	traffic-limit inbound ip-group acl_number [rule rule [link-group acl_number rule rule]] | link-group acl_number [rule rule] } target_rate [exceed action]
Add preference replacing action	traffic-priority inbound { ip-group acl_number [rule rule [link-group acl_number rule rule]] | link-group acl-number [rule rule] } { { dscp dscp_value | ip-precedence { pre_value | from-cos } } | { pre_value | from-ipprec } | local-precedence pre_value }*
Remove packet filtering action	undo packet-filter inbound { ip-group acl_number [rule rule [link-group acl_number rule rule]] | link-group acl_number [rule rule] }
Remove traffic policing action	undo traffic-limit inbound { ip-group acl_number [rule rule [link-group acl_number rule rule]] | link-group acl_number [rule rule] }
Remove preference replacing action	undo traffic-priority inbound { ip-group acl_number [rule rule [link-group acl_number rule rule]] | link-group acl_number [rule rule] }

You cannot remove the packet filtering, traffic policing or preference replacing action from the QoS profile which has been applied to the port.

Configuring Profile Application Mode

After you configure the QoS profiles and the user passes the authentication, the Switch will deliver the right profile dynamically to the port from which the user is accessed. The QoS profile can be delivered to the port in these different modes:

- User-based mode: If the source station information (source MAC address, source IP address or source MAC address + IP address) has been defined in the ACL which is referenced in the traffic actions, the Switch cannot deliver the QoS profile; if no source station information is available, the Switch generates a new ACL by adding the source MAC address and source IP address into the existing ACL, and then delivers all traffic actions in the QoS profile to the user port.
- Port-based mode: The Switch delivers the traffic actions in the QoS profile directly to the user port.

Perform the following configuration in Ethernet Port View.

Table 251 Configuring Profile Application Mode

Operation	Command
Configure the user-based mode on the port	**`qos-profile user-based`**
Restore the default (port-based) mode on the port	**`undo qos-profile user- based`**

By default, port-based mode is enabled on the port.

Applying QoS Profile to the Port

With this configuration, you can apply all traffic actions in the QoS profile to the current port.

In System View

In System View, you can apply the QoS profile to one or more consecutive ports.

Table 252 Applying QoS Profile to the Port in System View

Operation	Command
Apply the QoS profile to the port	**apply qos-profile** *profile_name* **interface {** *interface_name* | *interface_type interface_num* **} [to interface {** *interface_name* | *interface_type interface_num* **}]**
Remove the configuration	**undo apply qos-profile** *profile_name* **interface {** *interface_name* | *interface_type interface_num* **} [to interface {** *interface_name* | *interface_type interface_num* **}]**

In Ethernet Port View

In Ethernet Port View, you can only apply the QoS profile to the current port.

Table 253 Applying QoS Profile to the Port in Ethernet Port View

Operation	Command
Apply the QoS profile to the port	**apply qos-profile** *profile_name*
Remove the configuration	**undo apply qos-profile** *profile_name*

You cannot delete the specific QoS profile once you apply it to the port.

Displaying and Debugging QoS Profile Configuration

Use the **`display`** command in any view to check the configuration result of the QoS profile.

Table 254 Displaying QoS Profile Configuration

Operation	Command
Display QoS profile configuration	**display qos-profile { all** | **name** *profile_name* | **interface {** *interface_name* | *interface_type interface_num* **}** | **user** *user_name* **}**

QoS Profile Configuration Example

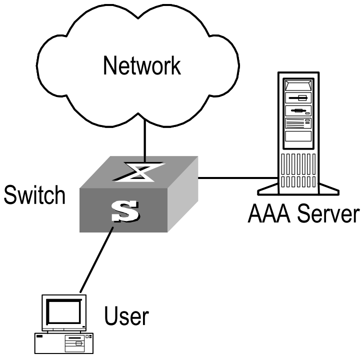
Networking Requirement

The Switch implements the QoS profile function for the accessed user.

The user (with user name **someone** and authentication password **hello**) is accessed from the GigabitEthernet1/0/1 port into the Switch. The user is assigned into the 3com163.net domain. The QoS profile example references the ACL with bandwidth limited to 128 kbps and new DSCP preference value 46.

Network Diagram

Figure 55 Network Diagram for QoS Configuration



Configuration Procedure

1 Configuration on the AAA server

Configure on the AAA server the mapping between QoS profiles and user names/authentication information. The configuration details are omitted here.

2 Configuration on the Switch

a Enable 802.1x

```
[SW5500]dot1x
[SW5500]dot1x interface ethernet 1/0/1
```

b Configure IP address for the RADIUS server

```
[SW5500]radius scheme radius1
[SW5500-radius-radius1]primary authentication 10.11.1.1
[SW5500-radius-radius1]primary accounting 10.11.1.2
[SW5500-radius-radius1]secondary authentication 10.11.1.2
[SW5500-radius-radius1]secondary accounting 10.11.1.1
```

c Configure authentication password on the RADIUS server for the Switch

```
[SW5500-radius-radius1]key authentication name
[SW5500-radius-radius1]key accounting money
```

d Configure the Switch to remove the user domain name from the user name and then to transfer it to the RADIUS server

```
[SW5500-radius-radius1]user-name-format without-domain
```

```
[SW5500-radius-radius1]quit
```

e Create the user domain 3com163.net and specify radius1 as the RADIUS server group for the user.

```
[SW5500]domain 3com163.net
[SW5500-isp-3com163.net]radius-scheme radius1
[SW5500-isp-3com163.net]quit
```

f Define the ACL

```
[SW5500]acl number 3000
[SW5500-acl-adv-3000]rule 1 permit ip destination any
[SW5500-acl-adv-3000]quit
```

g Configure the QoS profile

```
[SW5500]qos-profile example
[SW5500-qos-profile-example]traffic-limit inbound ip-group 3000 128
exceed drop
[SW5500-qos-profile-example]traffic-priority inbound ip-group 3000
dscp 46
[SW5500-qos-profile-example]quit
```

h Set user based mode on the Ethernet1/0/1 port

```
[SW5500]interface gigabitethernet1/0/1
[SW5500-GigabitEthernet1/0/1]qos-profile user-based
```

P

ACL Control Configuration

The Switch supports three major access modes: SNMP (Simple Network Management Protocol) access, Telnet access and HTTP (Hypertext Transfer Protocol) access. Security control is achieved at two levels: Connection request control is achieved at the first level and appropriate ACL configuration ensures that only legal users can be connected to the Switch. Password authentication is achieved at the second level and only those connected, with correct passwords, can log successfully onto the Switch.

In this section only the first level security control, ACL configuration, is detailed. See the "Getting Started" chapter on page 19 for the second level control.

Configuring ACL for Telnet Users

This configuration can filter out malicious or illegal connection request before password authentication.

Two steps are included in this configuration:

1. Define an ACL
2. Import the ACL to control Telnet users

Defining ACL

Currently only number-based ACLs can be imported, with the number ranging from 2000 to 3999.

Perform the following configuration in System View.

Table 255 Defining Basic ACL

Operation	Command
Enter basic ACL (System View)	**acl number** *acl_number* **match-order { config** | **auto }**
Define a sub-rule (Basic ACL View)	**rule [** *rule-id* **] { permit** | **deny } [source {** *source_addr wildcard* | **any }** | **fragment** | **logging** | **time-range** *name* **]***
Delete a sub-rule (Basic ACL View)	**undo rule** *rule_id* **[source** | **fragment** | **logging** | **time-range]***
Delete an ACL or all ACLs (System View)	**undo acl { number** *acl_number* | **all }**

You can define multiple rules for an ACL by using the **rule** command several times.

Importing ACL

You can import a defined ACL in User Interface View to achieve ACL control.

Perform the following configurations respectively in System View and User Interface View.

Table 256 Importing ACL

Operation	Command
Enter user interface view (System View)	**user-interface [** *type* **]** *first_number* **[** *last_number*]
Import the ACL (User Interface View)	**acl** *acl_number* **{ inbound** | **outbound }**

See the Command Reference Manual for details about these commands.

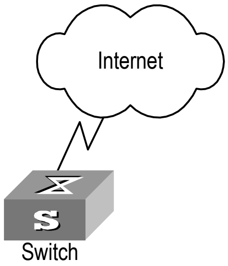
Configuration Example

Networking Requirement

Only the Telnet users from 10.110.100.52 and 10.110.100.46 can access the Switch.

Networking Diagram

Figure 56 ACL configuration for Telnet users



Configuration Procedure

1 Define a basic ACL.

```
[SW5500]acl number 2000 match-order config
[SW5500-acl-basic-2000]rule 1 permit source 10.110.100.52 0
[SW5500-acl-basic-2000]rule 2 permit source 10.110.100.46 0
[SW5500-acl-basic-2000]quit
```

2 Import the ACL.

```
[SW5500]user-interface vty 0 4
[SW5500-ui-vty0-4]acl 2000 inbound
```

Configuring ACL for SNMP Users

The Switch 5500G-EI Family supports remote network management (NM) and the user can use SNMP to access them. Proper ACL configuration can prevent illegal users from logging onto the Switches.

Two steps are included in this configuration:

1 Define an ACL

2 Import the ACL to control SNMP users

Defining ACL

Currently only number-based ACLs can be imported, with the number ranging from 2000 to 2999. See "Defining ACL " on page 207 for detailed configuration.

Importing ACL

Import the defined ACL into the commands with SNMP community, username and group name configured, to achieve ACL control over SNMP users.

Perform the following configurations in System View.

Table 257 Importing ACL

Operation	Command
Import the defined ACL into the commands with SNMP community configured	**snmp-agent community { read | write }** *community_name* **[[mib-view** *view_name* **] | [acl** *acl_number* **]]***
Import the defined ACL into the commands with SNMP group name configured	**snmp-agent group { v1 | v2c }** *group_name* **[read-view** *read_view* **] [write-view** *write_view* **] [notify-view** *notify_view* **] [acl acl-number]** **snmp-agent group v3** *group_name* **[authentication | privacy] [read-view** *read_view* **] [write-view** *write_view* **] [notify-view** *notify_view* **] [acl** *acl_number* **]**
Import the defined ACL into the commands with SNMP username configured	**snmp-agent usm-user { v1 | v2c }** *user_name group_name* **[acl** *acl_number* **]** **snmp-agent usm-user v3** *user_name group_name* **[authentication-mode { md5 | sha }** *auth_password* **] [privacy-mode des56** *priv_password* **] [acl** *acl_number* **]**

SNMP community is one of the features of SNMP v1 and SNMP v2, so you import the ACL into the commands with SNMP community configured, for the SNMP V1 and SNMP V2.

SNMP username or group name is one of the features of SNMP V2 and above, therefore you import the ACL into the commands with SNMP username or group name configured, for the SNMP V2 and above. If you import the ACL into both features, the Switch will filter both features for the users.

You can import different ACLs in the three commands listed above.

See the Command Manual for details about these commands.

Uou can import only the basic ACLs with digit IDs.

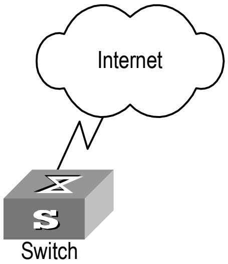
Configuration Example

Networking Requirement

Only SNMP users from 10.110.100.52 and 10.110.100.46 can access the Switch.

Networking Diagram

Figure 57 ACL Configuration for SNMP Users



Configuration Procedure

1 Define a basic ACL.

```
[SW5500]acl number 2000 match-order config
[SW5500-acl-baisc-2000]rule 1 permit source 10.110.100.52 0
[SW5500-acl-baisc-2000]rule 2 permit source 10.110.100.46 0
[SW5500-acl-baisc-2000]quit
```

2 Import the ACL.

```
[SW5500]snmp-agent community read 3Com acl 2000
[SW5500]snmp-agent group v2c 3Comgroup acl 2000
[SW5500]snmp-agent usm-user v2c 3Comuser 3Comgroup acl 2000
```

Configuring ACL Control over the HTTP Users

The Switch 5500G-EI 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 258 Calling ACL to Control HTTP Users

Operation	Command
Call an ACL to control the WEB NM users.	**ip http acl** *acl_number*
Cancel the ACL control function.	**undo ip http acl**

For more about the commands, refer to the Command Reference Manual.

Only the numbered basic ACL can be called for WEB NM user control.

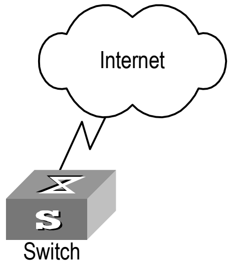
Configuration Example

Networking Requirements

Only permit Web NM user from 10.110.100.46 access Switch.

Networking Diagram

Figure 58 Controlling Web NM users with ACL



Configuration Procedure

1 Define the basic ACL.

```
[SW5500]acl number 2030 match-order config
[SW5500-acl-basic-2030]rule 1 permit source 10.110.100.46 0
[SW5500-acl-basic-2030]quit
```

2 Call the basic ACL.

```
[SW5500]ip http acl 2030
```

9 XRN FABRIC

This chapter covers the following topics:

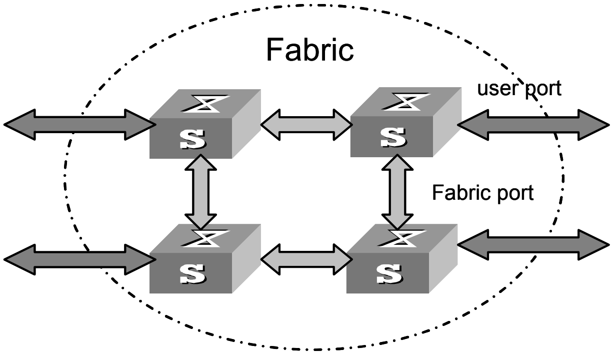
- Introduction to XRN
- Configuring an XRN Fabric
- Fabric Configuration Example

Introduction to XRN

Several XRN Switches of the same model can be interconnected to create a "Fabric", in which each Switch is a unit. The ports used to interconnect all the units are called Fabric ports, while the other ports that are used to connect the Fabric to users are called user ports. In this way, you can increase ports and switching capability by adding devices to the Fabric. In addition, reliability of the system will be improved because the devices within the Fabric can backup each other. This feature brings you many advantages:

- Realizes unified management of multiple devices. Only one connection and one IP address are required to manage the entire Fabric. Therefore, management cost is reduced.
- Enables you to purchase devices on demand and expand network capacity smoothly. Protects your investment to the full extent during network upgrade.
- Ensures high reliability by N+1 redundancy, avoids single point failure, and lessens service interruption.

Figure 59 Fabric Example



Fabric Topology Mapper (FTM) function can manage and maintain Fabric topology. FTM on each unit exchanges information with other units, including unit ID, Fabric name, and the authentication mode between units, by using a special kind of protocol packets. It manages and maintains Fabric topology according to the acquired information. For example, when a new device is connected to a Fabric, FTM will determine whether it should establish a new Fabric with the device according to the information.

Configuring an XRN Fabric

FTM provides user interfaces. You can configure VLAN unit IDs, Fabric name, and the authentication mode between units by using the command.

Table 259 Configuring FTM

Device	Configuration	Default Settings	Comment
Switch	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 Fabric can operate normally after all the Switches are interconnected.
	Set a name for the Fabric where the Switches belong	The Fabric name of the Switches is 5500	Interconnected the Switches with the same Fabric name to form a Fabric.

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 Fabric. On the Switches that support auto numbering, FTM will automatically number the Switches to constitute a Fabric, so that each Switch has a unique unit ID in the Fabric.

Perform the following configuration in System View.

Table 260 Setting unit IDs for Switches

Operation	Command
Set unit IDs for Switches	**change unit-id 1 to {1 | auto-numbering }**

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.

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 261 Setting Unit Names for Switches

Operation	Command
Set unit names for Switches	**set unit** *unit-id* **name unit-name**

Setting a Fabric Name for Switches

Only the Switches with the same Fabric name and XRN authentication mode can constitute a Fabric.

You can use the commands in the following table to set a Fabric name for the Switches.

Perform the following configuration in System View.

Table 262 Setting a Fabric Name for Switches

Operation	Command
Set a Fabric name for Switches	**sysname** *sysname*
Restore the default Fabric name	**undo sysname**

By default, the Fabric name is “5500G-EI”.

Displaying and Debugging a Fabric

Following completion of the above configuration, you can execute the **display** command in any view to view device management and verify the settings.

Table 263 Displaying and Debugging FTM

Operation	Command
Display the information of the entire Fabric	**display xrn-fabric [port]**
Display the topology information of Fabric	**display ftm{ information | route | topology-database }**

Fabric Configuration Example

Networking Requirements

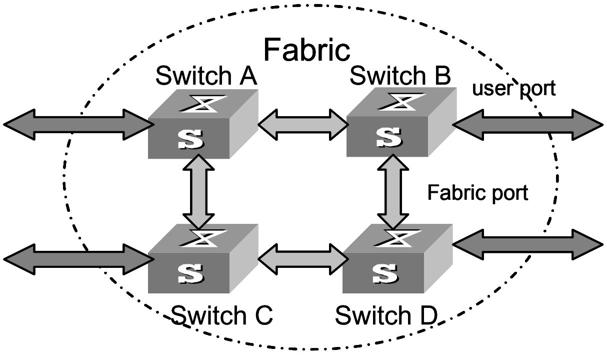
Configure unit ID, unit name, Fabric name, and authentication mode for four Switches, and interconnect them to form a Fabric.

The configuration details are as follows:

- Unit IDs: 1, 2, 3, 4
- Unit names: unit 1, unit 2, unit 3, unit 4
- Fabric name: hello
- Authentication mode: simple password
- Password: welcome

Networking Diagram

Figure 60 Networking Diagram of a Fabric



Configuration Procedure

Configure Switch A:

```
[SW5500]change unit-id 1 to 1
[SW5500]set unit 1 name unit1
[SW5500]sysname hello
```

Configure Switch B:

```
[SW5500]change unit-id 1 to auto-numbering
[SW5500}set unit 1 name unit2
[SW5500]sysname hello
```

Configure Switch C:

```
[SW5500]change unit-id 1 to auto-numbering
```

```
[SW5500}set unit 1 name unit3
[SW5500]sysname hello
```

Configure Switch D:

```
[SW5500]change unit-id 1 to auto-numbering
[SW5500}set unit 1 name unit
[[SW5500]sysname hello
```

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

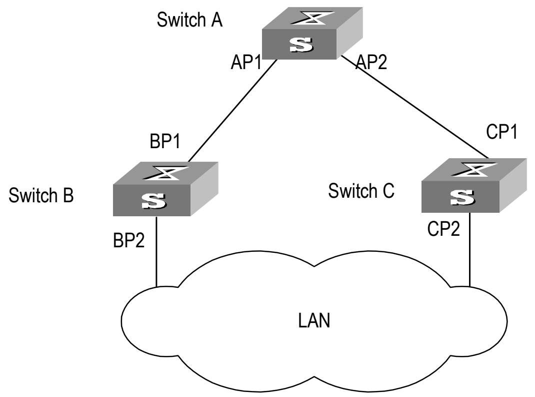
The fundamental of STP is that the Switches exchange a special type of protocol packet (which is called configuration Bridge Protocol Data Units, or BPDU, in IEEE 802.1D) to decide the topology of the network. The configuration BPDU contains the information enough to ensure the Switches to compute the 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 61 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 61, 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.

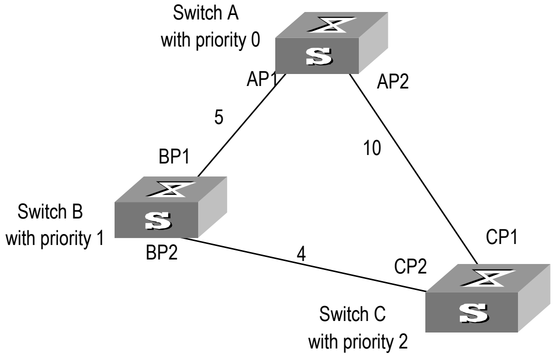
AP1, AP2, BP1, BP2, CP1 and CP2 respectively delegate the ports of Switch A, Switch B and Switch C.

The Specific Calculation Process of STP Algorithm

The following example illustrates the calculation process of STP.

Figure 62 illustrates the network.

Figure 62 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.

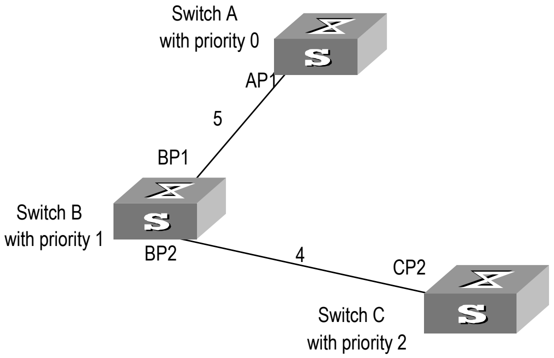
CP2 will receive the updated configuration BPDU, {0, 5, 1, BP2}, from Switch B. Since this configuration BPDU is better then the old one, the old BPDU will be updated to {0, 5, 1, BP2}.

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 63.

Figure 63 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.

In a Switch equipped with the XRN feature, RSTP has the following characteristics:

1) Processing the whole Fabric as a node;

2) Participation of all ports except those used as Fabric ports in role selection;

3) A single root port and bridge id for the whole Fabric;

4) Distributed saving of RSTP port information

RSTP Configuration

The configuration of RSTP changes with the position of the Switch in the network, as discussed below.

Figure 64 Configuring STP

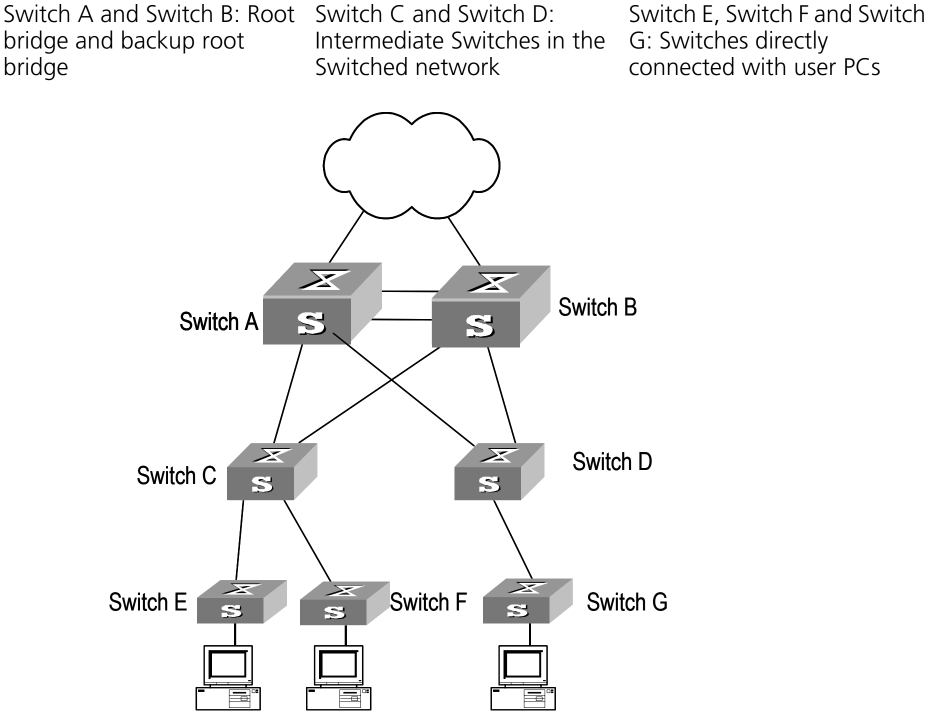

Switch A and Switch B: Root bridge and backup root bridge
Switch C and Switch D: Intermediate Switches in the Switched network
Switch E, Switch F and Switch G: Switches directly connected with user PCs
Switch A
Switch B
Switch C
Switch D
Switch E
Switch F
Switch G

Table 264 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	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 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.
	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.

Device	Configuration	Default Value	Note
	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	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 Root protection function on the root bridge.
Switch C & Switch D	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.
	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.
	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.

Device	Configuration	Default Value	Note
	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.
	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 pot 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.

Device	Configuration	Default Value	Note
	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 265 Enable/Disable RSTP on a Device

Operation	Command
Enable/Disable RSTP on a device	**`stp { enable | disable }`**
Restore RSTP to the default value	**`undo stp`**

Only after the RSTP is enabled on the Switch can other configurations take effect.

Some network resource will be occupied after RSTP is enabled.

By default, RSTP is disabled.

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 266 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 267 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 268 Configuring the STP-Ignore Attribute of VLANs on a Switch

Operation	Command
Specify an STP-Ignored VLAN	**stp ignored vlan** *vlan_list*

Operation	Command
Cancel the configuration of the STP-Ignored VLAN	**undo stp ignored vlan** *vlan_list*

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 269 Set Priority of a Specified Bridge

Operation	Command
Set priority of a specified bridge	**stp priority** *bridge_priority*
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 270 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**
Disqualify the current Switch as the primary or secondary root.	**undo stp root**

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, you are recommended to designate one primary root and more than one 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 271 Set Forward Delay of a Specified Bridge

Operation	Command
Set Forward Delay of a specified bridge	**`stp timer forward-delay`** *`centiseconds`*
Restore the default Forward Delay of specified bridge	**`undo stp timer forward-delay`**

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 272 Set Hello Time of the Specified Bridge

Operation	Command
Set Hello Time of the specified bridge	**`stp timer hello`** *`centiseconds`*
Restore the default Hello Time of the specified bridge	**`undo stp timer hello`**

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 273 Set Max Age of the Specified Bridge

Operation	Command
Set Max Age of the specified bridge	**`stp timer max-age`** *`centiseconds`*
Restore the default Max Age of the specified bridge	**`undo stp timer max-age`**

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 occurences 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 274 Set Timeout Factor of the Bridge

Operation	Command
Set the multiple value of hello time of a specified bridge	**`stp timeout-factor`** *`number`*
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 275 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`** *`packetnum`*
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 276 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 277 Specifying the Path Cost on a Port

Operation	Command
Specify the Path Cost on a port	**`stp cost`** *`cost`*
Restore the default Path Cost on the port	**`undo stp cost`**

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 278 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	**`stp pathcost-standard { dot1d-1998	dot1t }`**
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 279 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 280 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 281 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 it's 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 282 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 Manual*.

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 283 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

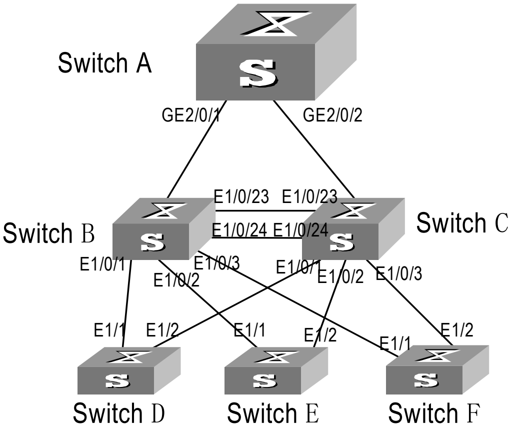
In the following scenario, Switch C serves as a standby of Switch B and forwards data when a fault occurs on Switch B. They are connected to each other with two links, so that, in case one of the links fails, the other one can still work normally. Switch D through Switch F are directly connected with 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 65 RSTP Configuration Example



Configuration Procedure

1 Configure Switch A

a Enable RSTP globally.

```
[SW5500]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 1/0/4 as an example.)

```
[SW5500]interface gigabitethernet 2/0/4
[SW5500-GigabitEthernet2/0/4]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

```
[SW5500]stp priority 0
```

d Designate Switch A as the root, using the following command.

```
[SW5500]stp root primary
```

e Enable the Root protection function on every designated port.

```
[SW5500]interface gigabitethernet 2/0/1
[SW5500-GigabitEthernet2/0/1]stp root-protection
[SW5500]interface gigabitethernet 2/0/2
[SW5500-GigabitEthernet2/0/2]stp root-protection
```

2 Configure Switch B

a Enable RSTP globally.

```
[SW5500]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 GigabitEthernet 1/0/4 as an example.)

```
[SW5500]interface gigabitethernet 1/0/4
[SW5500-GigabitEthernet1/0/4]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.

```
[SW5500]stp priority 4096
```

d Enable the Root protection function on every designated port.

```
[SW5500]interface gigabitethernet 1/0/1
[SW5500-GigabitEthernet1/0/1]stp root-protection
[SW5500]interface gigabitethernet 1/0/2
[SW5500-GigabitEthernet1/0/2]stp root-protection
[SW5500]interface gigabitethernet 1/0/3
[SW5500-GigabitEthernet1/0/3]stp root-protection
```

RSTP operating mode, time parameters, and port parameters take default values.

3 Configure Switch C

a Enable RSTP globally.

```
[SW5500]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 GigabitEthernet 1/0/4 as an example.)

```
[SW5500]interface gigabitethernet 1/0/4
[SW5500-GigabitEthernet1/0/4]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.

```
[SW5500]stp priority 8192
```

d Enable the Root protection function on every designated port.

```
[SW5500]interface gigabitethernet 1/0/1
[SW5500-GigabitEthernet1/0/1]stp root-protection
[SW5500]interface gigabitethernet 1/0/2
[SW5500-GigabitEthernet1/0/2]stp root-protection
[SW5500]interface gigabitethernet 1/0/3
[SW5500-GigabitEthernet1/0/3]stp root-protection
```

RSTP operating mode, time parameters, and port parameters take default values.

4 Configure Switch D

a Enable RSTP globally.

```
[SW5500]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 GigabitEthernet 1/3 as an example.)

```
[SW5500]interface gigabitethernet 1/3
[SW5500-GigabitEthernet1/3]stp disable
```

c Configure the ports (GigabitEthernet 0/1 through GigabitEthernet 0/24) directly connected to users as edge ports and enables BPDU PROTECTION function. (Take GigabitEthernet 0/1 as an example.)

```
[SW5500]interface gigabitethernet 1/3
[SW5500-GigabitEthernet1/3]stp edged-port enable
[SW5500-GigabitEthernet1/3]quit
[SW5500]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
- Centralized MAC Address Authentication Configuration
- 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 5500G-EI 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

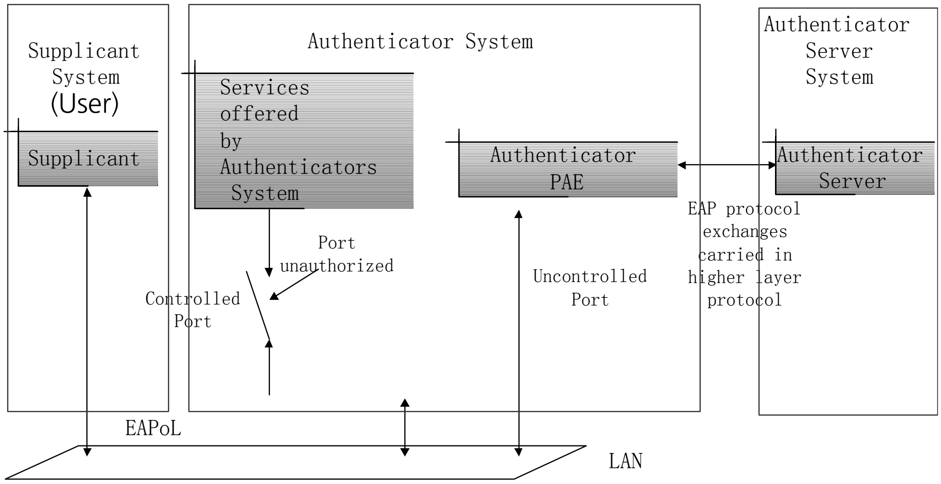
The system using the 802.1x is the typical C/S (Client/Server) system architecture. It contains three entities, which are illustrated in the following figure: Supplicant System (User), Authenticator System and Authentication Server System.

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 66 802.1x 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 5500G-EI 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 284 Enabling/Disabling 802.1x

Operation	Command
Enable the 802.1x	**dot1x [interface** *interface_list* **]**
Disable the 802.1x	**undo dot1x [interface** *interface_list* **]**

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 285 Setting the Port Access Control Mode.

Operation	Command
Set the port access control mode.	**dot1x port-control { authorized-force | unauthorized-force | auto } [interface** *interface_list* **]**
Restore the default access control mode of the port.	**undo dot1x port-control [interface** *interface_list* **]**

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 286 Setting the Port Access Control Method

Operation	Command
Set port access control method	**dot1x port-method { macbased | portbased } [interface** *interface_list* **]**

Operation	Command
Restore the default port access control method	**undo dot1x port-method [interface** *interface_list* **]**

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 287 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** *interface_list* **]**
Cancel the check for access users via proxy	**undo dot1x supp-proxy-check { logoff | trap } [interface** *interface_list* **]**

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 288 Setting the Maximum Number of Users via a Specified Port

Operation	Command
Set maximum number of users via specified port	**dot1x max-user** *user_number* **[interface** *interface_list* **]**
Restore the maximum number of users on the port to the default value	**undo dot1x max-user [interface** *interface_list* **]**

By default, 802.1x allows up to 256 users on each port for Series 5500 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 289 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**

Operation	Command
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).

Perform the following configurations in System View.

Table 290 Configuring the Authentication Method for 802.1x User

Operation	Command
Configure authentication method for 802.1x user	**dot1x authentication-method { chap** | **pap** | **eap md5-challenge}**
Restore the default authentication method for 802.1x user	**undo dot1x authentication-method**

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 291 Setting the Maximum Times of the Authentication Request Message Retransmission

Operation	Command
Set the maximum times of the authentication request message retransmission	**dot1x retry** *max_retry_value*
Restore the default maximum retransmission times	**undo dot1x retry**

By default, the *max-retry-value* is 2. That is, the Switch can retransmit the authentication request message to a user for a maximum of 2 times.

Configuring Timers

The following commands are used for configuring the 802.1x timers.

Perform the following configurations in System View.

Table 292 Configuring Timers

Operation	Command
Configure timers	**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* **}**

Operation	Command
Restore default settings of the timers	**undo dot1x timer { handshake-period | quiet-period | tx-period | supp-timeout | server-timeout }**

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 5 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 5500G-EI). 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 293 Enabling/Disabling a Quiet-Period Timer

Operation	Command
Enable a quiet-period timer	**`dot1x quiet-period`**
Disable a quiet-period timer	**`undo dot1x quiet-period`**

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 294 Displaying and Debugging 802.1x

Operation	Command
Display the configuration, running and statistics information of 802.1x	**display dot1x [sessions | statistics] [interface** *interface_list* **]**
Reset the 802.1x statistics information	**reset dot1x statistics [interface** *interface_list* **]**
Enable the error/event/packet/all debugging of 802.1x	**debugging dot1x { error | event | packet | all }**
Disable the error/event/packet/all debugging of 802.1x.	**undo debugging dot1x { error | event | packet | all }**

Auto QoS

Auto QoS uses the Filter-ID standard RADIUS attribute.

Table 295 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

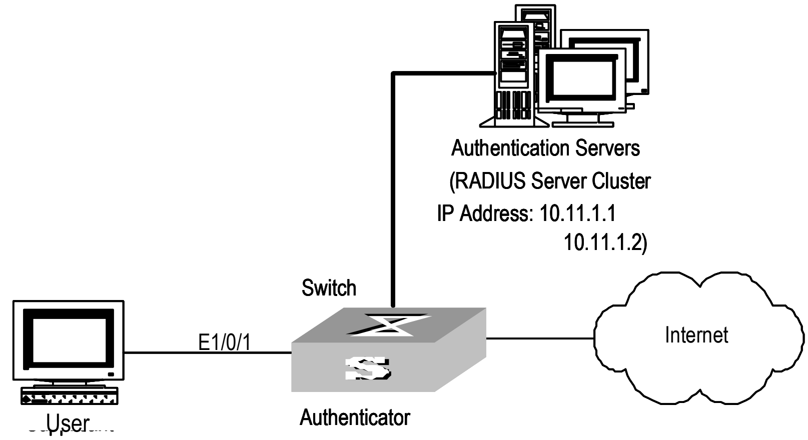
All the users belong to the default domain `3com163.net`, which can contain up to 30 users. RADIUS authentication is performed first. If there is no response from the RADIUS server, local authentication will be performed. For accounting, if the RADIUS server fails to account, the user will be disconnected. 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 67 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.

```
[SW5500]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.)

```
[SW5500]dot1x port-method macbased interface Ethernet 1/0/1
```

3 Create the RADIUS scheme radius1 and enters its view.

```
[SW5500]radius scheme radius1
```

4 Set IP address of the primary authentication/accounting RADIUS servers.

```
[SW5500-radius-radius1]primary authentication 10.11.1.1
[SW5500-radius-radius1]primary accounting 10.11.1.2
```

5 Set the IP address of the secondary authentication/accounting RADIUS servers.

```
[SW5500-radius-radius1]secondary authentication 10.11.1.2
[SW5500-radius-radius1]secondary accounting 10.11.1.1
```

6 Set the encryption key when the system exchanges packets with the authentication RADIUS server.

```
[SW5500-radius-radius1]key authentication name
```

7 Set the encryption key when the system exchanges packets with the accounting RADIUS server.

```
[SW5500-radius-radius1]key accounting money
```

8 Set the timeouts and times for the system to retransmit packets to the RADIUS server.

```
[SW5500-radius-radius1]timer 5
[SW5500-radius-radius1]retry 5
```

9 Set the interval for the system to transmit real-time accounting packets to the RADIUS server.

```
[SW5500-radius-radius1]timer realtime-accounting 15
```

10 Configure the system to transmit the user name to the RADIUS server after removing the domain name.

```
[SW5500-radius-radius1]user-name-format without-domain
[SW5500-radius-radius1]quit
```

11 Create the user domain 3com163.net and enters isp configuration mode.

```
[SW5500]domain 3com163.net
```

12 Specify radius1 as the RADIUS scheme for the users in the domain 3com163.net.

```
[SW5500-isp-3com163.net]scheme radius-scheme radius1 local
```

13 Set a limit of 30 users to the domain 3com163.net.

```
[SW5500-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.

```
[SW5500-isp-3com163.net]idle-cut enable 20 2000
```

15 Add a local user and sets its parameter.

```
[SW5500]local-user localuser
[SW5500-luser-localuser]service-type lan-access
[SW5500-luser-localuser]password simple localpass
```

16 Enable the 802.1x globally.

```
[SW5500]dot1x
```

Centralized MAC Address Authentication Configuration

Centralized MAC Address Authentication Overview

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 5500G-EI 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 296 Enabling/Disabling Centralized MAC Address Authentication

Operation	Command
Enable centralized MAC address authentication	**mac-authentication [interface** *interface_list* **]**
Disable centralized MAC address authentication	**undo mac-authentication [interface** *interface_list* **]**

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.

CAUTION: *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 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 297 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	**mac-authentication domain** *isp_name*
Return to the defaults	**undo mac-authentication domain**

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 298 Configuring Centralized MAC Address Authentication Timers

Operation	Command
Configure centralized MAC address authentication timers	**mac-authentication timer { offline-detect** *offline_detect_value* | **quiet** *quiet_value* | **server-timeout** *server_timeout_value* **}**
Return to the defaults	**undo mac-authentication timer { offline-detect** | **quiet** | **server-timeout }**

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 299 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 300 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 5500G-EI, you need to execute the following command on the Switch 5500G-EI to use standard private-group-ID:

```
[5500-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.

```
[SW5500]mac-authentication interface Ethernet 1/0/2
```

2 Add local access user.

a Set the user name and password.

```
[SW5500]local-user 00e0fc010101
[SW5500-luser-00e0fc010101]password simple 00e0fc010101
```

b Set the service type of the user to lan-access.

```
[SW5500-luser-00e0fc010101]service-type lan-access
```

3 Enable the MAC address authentication globally.

```
[SW5500]mac-authentication
```

4 Configure the ISP domain used by the user.

```
[SW5500]mac-authentication domain 3com163.net
```

For the configuration of the domain 3com163.net, see "802.1x Configuration Example" on page 266.

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.

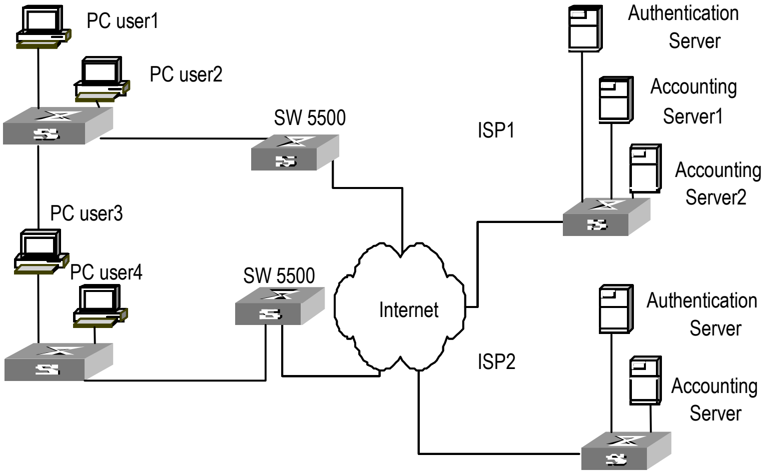
RADIUS Operation

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 5500G-EI 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 5500G-EI. The figure below illustrates the RADIUS authentication network including 5500G-EI Switches.

Figure 68 Networking when Switch 5500G-EI 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 (i.e. 3com163.net) following the @ is the ISP domain name. When the Switch 5500G-EI 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 5500G-EI 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 5500G-EI, 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 301 Creating/Deleting an ISP Domain

Operation	Command
Create ISP domain or enter the view of a specified domain.	**domain** *isp_name*
Remove a specified ISP domain	**undo domain** *isp_name*
Enable the default ISP domain specified by *isp-name*	**domain default enable** *isp_name*
Restore the default ISP domain to "system"	**domain default disable**

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 302 Configuring AAA Scheme Adopted by the ISP Domain

Operation	Command
Configure an AAA scheme for the domain.	**scheme { radius-scheme** *radius_scheme_name* | **local** | **none** }
Configure a RADIUS scheme	**radius-scheme** *radius_scheme_name*
Restore the default AAA scheme.	**undo scheme { radius-scheme** *radius_scheme_name* | **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.

When using **`scheme radius-scheme`** ***`radius-scheme-name`*** **`local`** in the configuraton command, the local refers to the alternative authentication scheme if the RADIUS server does not respond normally. Therefore, when RADIUS server operates normally, the local scheme is not used. Otherwise, the local scheme is used. When using **`scheme radius-scheme`** ***`radius-scheme-name`*** (without **`local`**), the local scheme does not work when there is no normal response.

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 303 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 304 Setting Access Limit

Operation	Command
Set a limit to the amount of users	**`access-limit { disable | enable`** *`max_user_number`* **`}`**
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 305 Enabling/Disabling the Idle-cut Function

Operation	Command
Set the idle	**`idle-cut enable`** *`minute flow`*
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 306 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 307 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 308 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** *url-string*
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 309 Creating/Deleting a Local User and Relevant Properties

Operation	Command
Add local users	**local-user** *user_name*
Delete all the local users	**undo local-user all**
Delete a local user by specifying its type	**undo local-user** { *user_name* | **all** [**service-type** { **lan_access** | **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 310 Setting the Password Display Mode of Local Users

Operation	Command
Set the password display mode of local users	**local-user password-display-mode** { **cipher-force** | **auto** }
Cancel the configuration of password display mode	**undo local-user password-display-mode**

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 311 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 311 Setting/Removing the Attributes Concerned with a Specified User

Operation	Command
Set a password for a specified user	**password { simple | cipher }** *password*
Remove the password set for the specified user	**undo password**
Set the state of the specified user	**state { active | block }**
Set a priority level for the user	**level** *level*
Restore the default priority level	**undo level**
Set a service type for the specified user	**service-type { ftp [ftp-directory** *directory* **] | lan-access | { ssh | telnet | terminal }* }**
Cancel the service type of the specified user	**undo service-type { ftp [ftp-directory] | lan-access | { ssh | telnet | terminal }* [level** *level* **] }**
Configure the attributes of lan-access users	**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* **} }***
Remove the attributes defined for the lan-access users	**undo attribute { ip | mac | idle-cut | access-limit | vlan | location }***

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 bothTelnet 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-priviledge level to be entered as an optional extra parameter. For example Telnet, Terminal & SSH.

  However, the user-priviledge 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:

  ```
  [5500-luser-adminpwd]service-type telnet level 1
  [5500-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 312 Disconnecting a User by Force

Operation	Command
Disconnect a user by force	**cut connection { all** | **access-type { dot1x** | **gcm** | **mac-authentication }** | **domain** *domain_name* | **interface** *interface_type interface_number* | **ip** *ip_address* | **mac** *mac_address* | **radius-scheme** *radius_scheme_name* | **vlan** *vlanid* | **ucibindex** *ucib_index* | **user-name** *user_name* **}**

By default, no online user will be disconnected by force.

Configuring the RADIUS Protocol

For the Switch 5500G-EI, 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 313 Creating/Deleting a RADIUS Server Group

Operation	Command
Create a RADIUS scheme and enter its view	**radius scheme** *radius_scheme_name*
Delete a RADIUS scheme	**undo radius scheme** *radius_scheme_name*

By default, the system has a RADIUS scheme named as `default system` whose attributes are all default values. The default attribute values will be introduced in the following text.

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 **default system**.

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 314 Configuring RADIUS Authentication/Authorization Servers

Operation	Command
Set IP address and port number of primary RADIUS authentication/authorization server.	**primary authentication** *ip_address* **[** *port_number* **]**
Restore IP address and port number of primary RADIUS authentication/authorization server to the default values.	**undo primary authentication**
Set IP address and port number of secondary RADIUS authentication/authorization server.	**secondary authentication** *ip_address* **[** *port_number* **]**
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 5500G-EI 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 315 Configuring RADIUS Accounting Servers

Operation	Command
Set IP address and port number of primary RADIUS accounting server.	**primary accounting** *ip_address* [*port_number*]
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** *ip_address* [*port_number*]
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 5500G-EI 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 316 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`** *`retry_times`*
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 317 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 318 Setting the Maximum Retransmitting Times of Stopping Accounting Request

Operation	Command
Set the maximum retransmitting times of stopping accounting request	**retry stop-accounting** *retry_times*
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 319 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 320 Setting the RADIUS Packet Encryption Key

Operation	Command
Set RADIUS authentication/authorization packet encryption key	**key authentication** *string*
Restore the default RADIUS authentication/authorization packet encryption key.	**undo key authentication**
Set RADIUS accounting packet key	**key accounting** *string*
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 321 Setting Retransmission Times of RADIUS Request Packet

Operation	Command
Set retransmission times of RADIUS request packet	**retry** *retry_times*
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 5500G-EI 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 322 Setting the Supported Type of the RADIUS Server

Operation	Command
Setting the Supported Type of RADIUS Server	**server-type { 3com** | **standard }**
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 323 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 324 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 325 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 326 Creating/Deleting the Local RADIUS Authentication Server

Operation	Command
Create the local RADIUS authentication server	**local-server nas-ip** *ip_address* **key** *password*
Delete the local RADIUSauthentication server	**undo local-server nas-ip** *ip_address*

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 authentication 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 327 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`** *`ip_address`*
Cancel the configured source address to be carried in the RADIUS packets sent by the NAS(RADIUS sheme view).	**`undo nas-ip`**
Configure the source address to be carried in the RADIUS packets sent by the NAS(System view).	**`radius nas-ip`** *`ip_address`*
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 328 Setting the Response Timeout Timer of the RADIUS Server

Operation	Command
Set response timeout timer of RADIUS server	**`timer`** *`second`*
Restore the response timeout timer of RADIUS server to default value	**`undo timer`**

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 329 Setting a Real-time Accounting Interval

Operation	Command
Set a real-time accounting interval	**`timer realtime-accounting`** *`minute`*
Restore the default value of the interval	**`undo timer realtime-accounting`**

`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 330 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 331 Configure the RADIUS Server Response Timer

Operation	Command
Configure the RADIUS server response timer	**`timer response-timeout`** *`seconds`*
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 332 Displaying and Debugging AAA and RADIUS Protocol

Operation	Command
Display the configuration information of the specified or all the ISP domains.	**display domain [** *isp_name* **]**
Display related information of user's connection	**display connection [access-type { dot1x | mac-authentication } | domain** *domain_name* **| interface** *interface_type interface_number* **| ip** *ip_address* **| mac** *mac_address* **| radius-scheme** *radius_scheme_name* **| vlan** *vlanid* **| ucibindex** *ucib_index* **| user-name** *user_name* **]**
Display related information of the local user	**display local-user [domain** *isp_name* **| idle-cut { disable | enable } | service-type { telnet | ftp | lan-access | ssh | terminal } | state { active | block } | user-name** *user_name* **| vlan** *vlan_id* **]**
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 [** *radius_scheme_name* **]**
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** *radius_scheme_name* **| session-id** *session_id* **| time-range** *start_time stop_time* **| user-name** *user_name* **}**
Delete the stopping accounting requests saved in buffer without response (from System View)	**reset stop-accounting-buffer { radius-scheme** *radius_scheme_name* **| session-id** *session_id* **| time-range** *start_time stop_time* **| user-name** *user_name* **}**
Clear stop-accounting packets from the buffer.	**reset stop-accounting-buffer { radius-scheme** *radius_scheme_name* **| session-id** *session_id* **| time-range** *start_time stop_time* **| user-name** *user_name* **}**
Reset the statistics of RADIUS server.	**reset radius statistics**
Enable RADIUS packet debugging	**debugging radius packet**
Disable RADIUS packet debugging	**undo debugging radius packet**
Enable debugging of localRADIUS scheme	**debugging local-server { all | error | event | packet }**
Disable debugging of localRADIUS scheme	**undo debugging local-server { all | error | event | packet }**

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 266.

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.

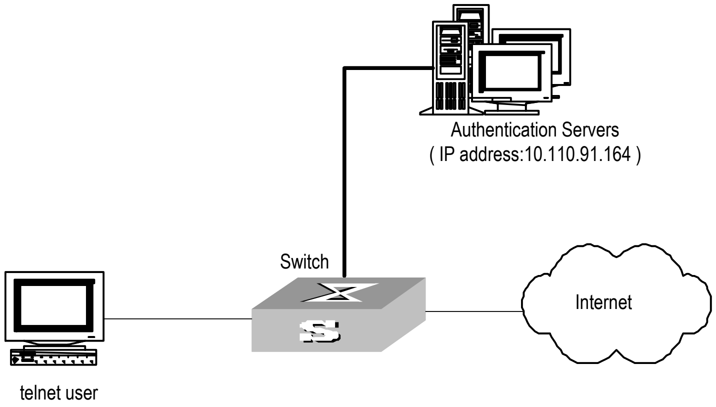
Networking Requirements

In Figure 69, 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 69 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.

```
[SW5500-ui-vty0-4]authentication-mode scheme
```

3 Configure domain.

```
[SW5500]domain cams
[SW5500-isp-cams]quit
```

4 Configure RADIUS scheme.

```
[SW5500]radius scheme cams
[SW5500-radius-cams]primary authentication 10.110.91.146 1812
[SW5500-radius-cams]key authentication expert
[SW5500-radius-cams]server-type 3com
[SW5500-radius-cams]user-name-format without-domain
```

5 Configuration association between domain and RADIUS.

```
[SW5500-radius-cams]quit
[SW5500]domain cams
[SW5500-isp-cams]scheme radius-scheme cams
```

Configuring the FTP/Telnet User Local Authentication

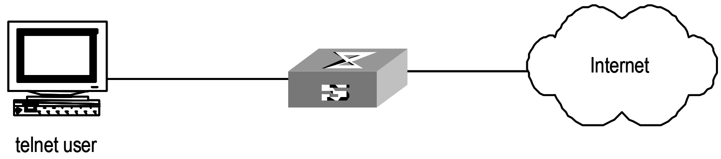
Configuring local authentication for FTP users is similar to that for Telnet users. The following example is based on Telnet users.

Networking Requirements

Configure the router to authenticate the login Telnet users locally (see Figure 70).

Networking Diagram

Figure 70 Local Authentication for Telnet Users



Configuration Procedure

1 Method 1: Using Local scheme.

a Apply AAA authentication to Telnet users.

```
<SW5500>system-view
[SW5500]user-interface vty 0 4
[SW5500-ui-vty0-4]authentication-mode scheme
[SW5500-ui-vty0-4]quit
```

b Create a local user telnet.

```
[SW5500]local-user telnet
[SW5500-luser-telnet]service-type telnet
[SW5500-luser-telnet]password simple 3com
[SW5500-luser-telnet]attribute idle-cut 300 access-limit 5
[SW5500-luser-telnet]quit
[SW5500]domain cams
[SW5500-isp-cams]scheme local
```

Telnet users use usernames in the “*userid*@cams” format to log onto the network and are to be authenticated as users of the cams 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 5500G-EI

General RADIUS setup

The Switch 5500G-EI supports multiple RADIUS schemes, which can be assigned to a domain.

This guide covers the recommended steps to setup the Switch 5500G-EI for login.

Domain and RADIUS scheme creation

The Switch 5500G-EI can have 1 or more domains created on it. A domain on the Switch 5500G-EI 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:

```
<SW5500>display domain
0  Domain = default system
   State = Active
   Scheme = LOCAL Access-limit = Disable
   Domain User Template:
   Idle-cut = Disable
   Self-service = Disable
   Messenger Time = Disable

Default Domain Name: default system
Total 1 domain(s).1 listed.
```

This default system domain uses the LOCAL scheme.

It is not recommended that you change the default 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:

```
[SW5500]radius scheme NewSchemeName
New Radius scheme
[SW5500-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.

```
[SW5500-radius-NewSchemeName]key authentication mysharedsecret
[SW5500-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".

```
[SW5500-radius-NewSchemeName]accounting optional
```

4 Next, create a new domain as follows:

```
[SW5500]domain Demo
New Domain added.
[SW5500-isp-Demo]
```

5 Change the domain to use the new RADIUS scheme that you have configured:

```
[SW5500-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:

```
[5500-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:

  ```
  [5500-xx]interface ethernet 1/0/7
  [5500-xx-Ethernet1/0/7]dot1x
  802.1x is enabled on port Ethernet1/0/7
  [5500-xx-Ethernet1/0/7]
  ```

- To enable dot1x on more than 1 port, enter the global dot1x command as follows:

  ```
  [5500-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
  [5500-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 ìuser@domainî where ìdomainî 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:

```
[5500-xx-radius-NewSchemeName]user-name-format without-domain
```

Switch Login

The Switch 5500G-EI 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, eg 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:

```
[SW5500-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 5500G-EI provides debugging of RADIUS. Terminal debugging can be enabled with the command:

```
<5500>terminal debugging
```

Once enabled, different debug traces can be enabled to the terminal. For example, to turn on RADIUS debugging, enter the command:

- `<5500> 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

This chapter covers the following topics:

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 path must start with “unit[No.]>flash:/:”, the [No.] is the unit ID. For example, suppose unit ID is 1, and the path 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 333 Directory Operation

Operation	Command
Create a directory	**mkdir** *directory*
Delete a directory	**rmdir** *directory*
Display the current working directory	**pwd**
Display the information about directories or files	**dir [/ all] [** *file-url* **]**
Change the current directory	**cd** *directory*

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 separatly 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 334 File Operation

Operation	Command
Delete a file	**delete [/unreserved]** *file-url*
Undelete a file	**undelete** *file-url*
Delete a file from the recycle bin permanently	**reset recycle-bin [** *file-url* **] [/ force]**
View contents of a file	**more** *file-url*
Rename a file	**rename** *fileurl-source fileurl-dest*
Copy a file	**copy** *fileurl-source fileurl-dest*
Move a file	**move** *fileurl-source fileurl-dest*
Display the information about directories or files	**dir [/ all] [** *file-url* *

Perform the following configuration in System View.

Table 335 Execute the Specified Batch File

Operation	Command
Execute the specified batch file	**execute** *filename*

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 336 Storage Device Operation

Operation	Command
Format the storage device	**format** *filesystem*

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 337 File System Operation

Operation	Command
Set the file system prompt mode.	**file prompt { alert** | **quiet }**

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 any view.

Table 338 Display the Configurations of the Switch

Operation	Command
Display the saved-configuration information of the Switch	**display saved-configuration [unit *unit-id*]**
Display the current-configuration information of the Switch	**display current-configuration [controller | interface** *interface-type* **[** *interface-number* **] | configuration [** *configuration* **]] [| { begin | exclude | include }** *regular-expression* **]**
Display the running configuration of the current view	**display this**

The configuration files are displayed in their corresponding saving formats.

Saving the Current-configuration

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 339 Save the Current-Configuration

Operation	Command
Save the current-configuration	**save** [*file-name* | **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 sw5500cfg.cfg for Series 5500G-EI 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 340 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 341 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 [unit *unitid*]** *cfgfile*

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 any view to display the running of the configuration files, and to verify the effect of the configuration.

Table 342 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 71 FTP Configuration

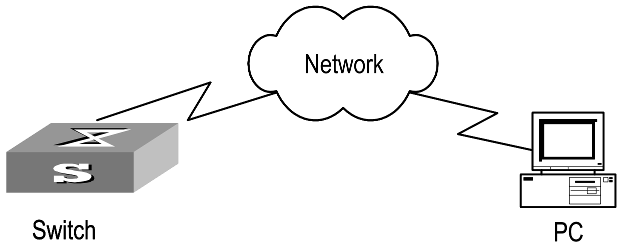


Table 343 Configuration of the Switch as FTP Client

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 344 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 **`display 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.
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 345 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 346 Configure the FTP Server Authentication and Authorization

Operation	Command
Create new local user and enter local User View (System View)	**`local-user`** *`username`*
Delete local user (System View)	**`undo local-user [`** *`username`* | **`all [ service-type ftp ] ]`**

Operation	Command
Configure password for local user (Local User View)	**password [cipher | simple]** *password*
Configure service type for local user (Local User View)	**service-type ftp ftp-directory** *directory*
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 347 Configure FTP Server Connection Timeout

Operation	Command
Configure FTP server connection timeouts	**ftp timeout** *minute*
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 348 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

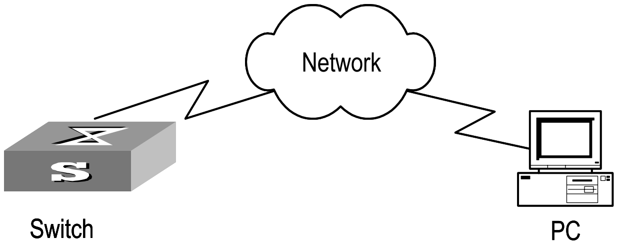
Networking Requirement

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 72 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).

```
<SW5500>
```

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.

```
<SW5500> 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
<SW5500>
```

7 Use the **boot boot-loader** command to specify the downloaded program as the application at the next login and reboot the Switch.

```
<SW5500> boot boot-loader switch.app
<SW5500> reboot
```

FTP Server Configuration Example

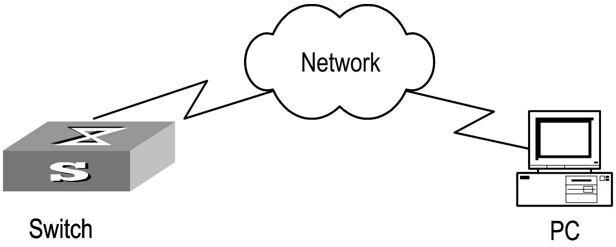
Networking Requirement

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 73 Networking for FTP Configuration



1 Configure the Switch

Log into the Switch (locally through the Console port or remotely using Telnet).

```
<SW5500>
```

2 Start FTP function and set username, password and file directory.

```
[SW5500]ftp server enable
[SW5500]local-user switch
[SW5500-luser-switch]service-type ftp ftp-directory flash:
[SW5500-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.

```
<SW5500>
```

Use the **boot boot-loader** command to specify the downloaded program as the application at the next login and reboot the Switch.

```
<SW5500> boot boot-loader switch.app
<SW5500> 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 74 TFTP Configuration

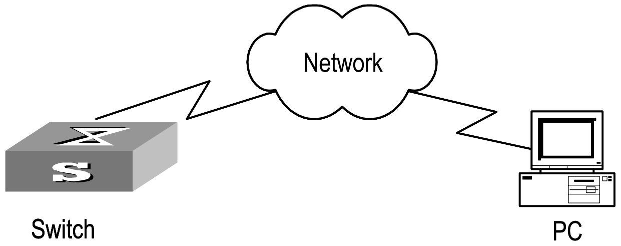


Table 349 Configuration of the Switch as TFTP Client

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 VLAN interface on the Switch and the TFTP server are reachable.
	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 350 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 351 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

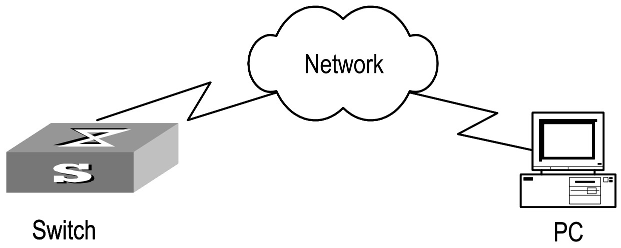
Networking Requirement

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 75 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).

```
<SW5500>
```

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.

```
<SW5500> system-view
```

```
[SW5500]
```

4 Configure IP address 1.1.1.1 for the VLAN interface, ensure the port connecting the PC is also in this VALN (VLAN 1 in this example).

```
[SW5500]interface vlan 1
[SW5500-vlan-interface1]ip address 1.1.1.1 255.255.255.0
[SW5500-vlan-interface1]quit
```

5 Upload the *config.cfg* to the TFTP server.

```
<SW5500> tftp 1.1.1.2 put config.cfg config.cfg
```

6 Download the *switch.app* from the TFTP server.

```
<SW5500> 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.

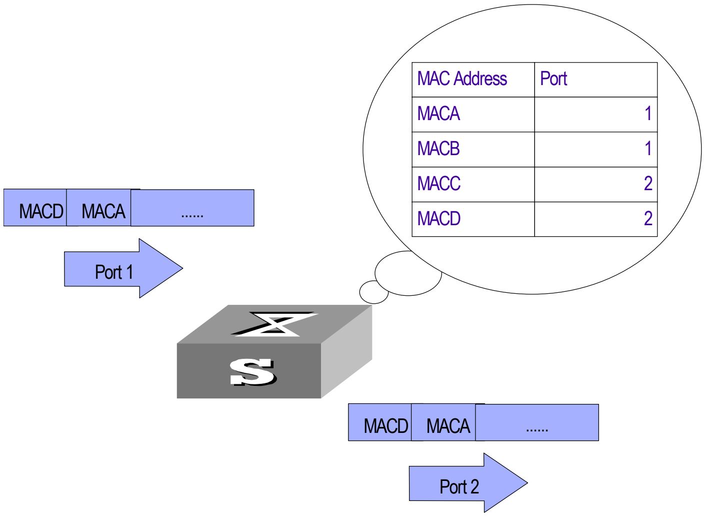
```
<SW5500> boot boot-loader switch.app
<SW5500> reboot
```

MAC Address Table Management

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 76 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 352 Set MAC Address Table Entries

Operation	Command
Add/Modify an address entry	**mac-address { static | dynamic | blackhole }** *mac-address* **interface {** *interface-name* | *interface-type interface-num* **} vlan** *vlan-id*
Delete an address entry	**undo mac-address [{ static | dynamic | blackhole }** *mac-address* **interface {** *interface-name* | *interface-type interface-num* **} vlan** *vlan-id* **]**

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 353 Set the MAC Address Aging Time for the System

Operation	Command
Set the dynamic MAC address aging time	**mac-address timer { aging** *age* | **no-aging }**
Restore the default MAC address aging time	**undo mac-address timer aging**

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 its received 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 354 Set the Max Count of MAC Address Learned by a Port

Operation	Command
Set the Max Count of MAC Address Learned by a Port	**mac-address max-mac-count** *count*
Restore the default Max Count of MAC Address Learned by a Port	**undo mac-address max-mac-count**

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 355 Display and Debug MAC Address Table

Operation	Command
Display the information in the address table	**display mac-address [** *mac-addr* **[vlan** *vlan-id***]** | **[static** | **dynamic** | **blackhole] [interface {** *interface-name* | *interface-type interface-num* **}] [vlan** *vlan-id* **] [count]]**
Display the aging time of dynamic address table entries	**display mac-address aging-time**

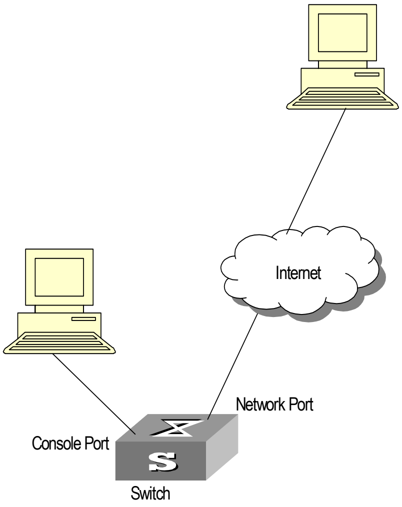
MAC Address Table Management Display Example

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 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 77 Display MAC address table



Configuration procedure

The **`display`** command shows a stack wide view of the MAC address table.

```
[SW5500]display mac-address
MAC ADDR        VLAN ID STATE      PORT INDEX          AGING TIME(s)
00e0-fc00-3943     1    Learned    GigabitEthernet1/0/11         300
0000-0000-5100     1    Learned    GigabitEthernet2/0/22         300
0020-9c08-e774     1    Learned    GigabitEthernet2/0/7          288
0000-0000-5000     1    Learned    GigabitEthernet2/0/3          143
  ---  4 mac address(es) found  ---
```

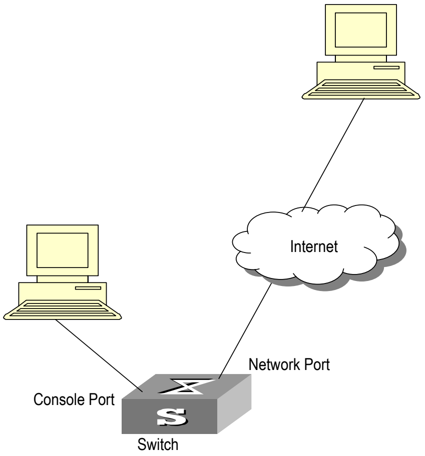
MAC Address Table Management Configuration Example

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 GigabitEthernet1/0/2 in vlan1.

Networking Diagram

Figure 78 Typical Configuration of Address Table Management



Configuration Procedure

1 Enter the System View of the Switch.

```
<SW5500> system-view
System View: return to User View with Ctrl+Z
```

2 Add a MAC address (specify the native VLAN, port and state).

```
[SW5500]mac-address static 00e0-fc35-dc71 interface
gigabitethernet1/0/2 vlan 1
```

3 Set the address aging time to 500s.

```
[SW5500]mac-address timer 500
```

4 Display the MAC address configurations in all views.

```
[SW5500]display mac-address interface gigabitethernet1/0/2
MAC ADDR           VLAN ID    STATE      PORT INDEX    AGING TIME(s)
00-e0-fc-35-dc-71     1       Static     GigabitEthernet1/0/2NOAGED
00-e0-fc-17-a7-d6     1       Learned    GigabitEthernet1/0/2500
00-e0-fc-5e-b1-fb     1       Learned    GigabitEthernet1/0/2500
00-e0-fc-55-f1-16     1       Learned    GigabitEthernet1/0/2500
---  4 mac address(es) found on port GigabitEthernet1/0/2---
```

Device Management

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 356 Reboot the Switch

Operation	Command
Reboot the Switch	**reboot [unit** *unit-id* **]**

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 357 Reboot the Switch

Operation	Command
Enable the timing reboot function of the Switch, and set specified time and date	**schedule reboot at** *hh:mm* **[** *yyyy/mm/dd* **]**
Enable the timing reboot function of the Switch, and set waiting time	**schedule reboot delay {** *hhh:mm* | *mmm* **}**
Cancel the parameter configuration of timing reboot function of the Switch	**undo schedule reboot**
Check the parameter configuration of the reboot terminal service of the current Switch	**display schedule reboot**

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 358 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** *file-url*

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 359 Upgrade BootROM

Operation	Command
Upgrade BootROM	**boot bootrom** *file-url*

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 360 Display and Debug Device Management

Operation	Command
Display the module types and running states of each card.	**display device [unit** *unit-id* **]**
Display the running state of the built-in fans.	**display fan [unit** *unit-id* **]**
Display the Used status of Switch memory	**display memory [unit** *unit-id* **]**
Display the state of the power.	**display power [unit** *unit-id* **] [** *power-ID* **]**
Display the APP to be applied when rebooting the Switch.	**display boot-loader [unit** *unit-id* **]**
Display the busy status of CPU	**display cpu [unit** *unit-id* **]**

Device Management Configuration Example

Networking Requirement

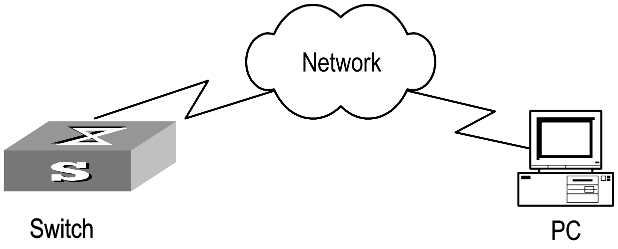
The user logs into the Switch using Telnet, downloads the application from the FTP server to the flash memory of the Switch, and implements remote upgrade using the right commands.

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 79 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.

```
<SW5500>
```

***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.

```
<SW5500> 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
<SW5500>
```

7 Upgrade BootROM.

```
<SW5500> boot bootrom boot.btm
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.

```
<SW5500> boot boot-loader switch.app
<SW5500>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
<SW5500> reboot
```

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 361 Set the Name for the Switch

Operation	Command
Set the Switch system name	**sysname** *sysname*
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 362 Set the System Clock

Operation	Command
Set the system clock	**clock datetime** *time date*

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 363 Setting the Time Zone

Operation	Command
Set the local time	**clock timezone** *zone_name* { **add** | **minus** } *HH:MM:SS*
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 364 Setting the Summer Time

Operation	Command
Set the name and range of the summer time which is effective for one year	**clock summer-time** *zone_name* **one-off** *start-time start-date end-time end-date offset-time*
Set the name and range of the summer time whic is effective for every year	**clock summer-time** ***zone name*** **repeating** ***{ start-time start-date end-time end-date | start-time start-year start-month start-week start-day end-time end-year end-month end-week end-day } offset-time***
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 365 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** *interface-type* **[** *interface-number* **]** | **configuration [** *configuration* **]] [** | **{ begin** | **exclude** | **include }** *regular-expression* **]**
Display the state of the debugging	**display debugging [interface {** *interface-name* | *interface-type interface-number* **}] [** *module-name* **]**
Display statistics of the configuration agent	**display config-agent unit-id** *unit-id*

System Debugging

Enable/Disable the Terminal Debugging

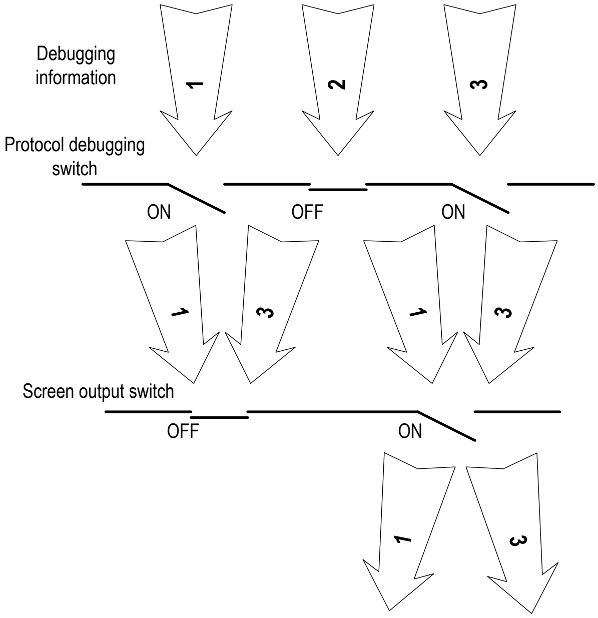
The Switch provides various ways for debugging most of the supported protocols and functions, which can help you diagnose and address the errors.

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 80 illustrates the relationship between two Switches.

Figure 80 Debug Output



You can use the following commands to control the above-mentioned debugging.

Perform the following operations in User View.

Table 366 Enable/Disable the Debugging

Operation	Command
Enable the protocol debugging	**debugging** *module-name* **[** *debugging-option* **]**
Disable the protocol debugging	**undo debugging { all | {** *protocol-name* | *function-name* **} [** *debugging-option* **] }**
Enable the terminal debugging	**terminal debugging**
Disable the terminal debugging	**undo terminal debugging**

For more about the usage and format of the debugging commands, refer to the relevant chapters.

Since the debugging output will affect the system operating efficiency, do not enable the debugging without necessity. 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 367 Display Diagnostic Information

Operation	Command
display diagnostic information	**`display diagnostic-information`**

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 368 The ping Command

Operation	Command
Support IP ping	**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*

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 369 Test Periodically if the IP address is Reachable

Operation	Command
Configure the IP address requiring periodical testing	**end-station polling ip-address** *ip-address*
Delete the IP address requiring periodical testing	**undo end-station polling ip-address** *ip-address*

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 81 The tracert Command

Operation	Command
Trace route	**tracert [-a** *source-IP* **] [-f** *first-TTL* **] [-m** *max-TTL* **] [-p** *port* **] [-q** *nqueries* **] [-w** *timeout* **]** *string*

HWPing

Introduction to HWPing

HWPing is a tool used for testing performance of the protocols operating on a network. It is an enhancement to the ping function, which only allows you to test the roundtrip delay (time for a packet to travel from the local end to a specified destination and return).

You can set parameters of HWPing operations by making use of the network management software and enable HWPing to view the results of the operations. Alternatively, you can execute the **display hwping result** command to view statistics about the HWPing operations.

HWPing Configurations

To configure HWPing Client, perform the following tasks:

- Enable HWPing Client
- Create a Test Group

- Configure the Test Parameter

Enable HWPing Client

By enabling HWPing client, various types of tests can be set and carried out.

Perform the following configurations in System View.

Table 370 Enable HWPing Client

Operation	Command
Enable HWPing client	**hwping-agent enable**
Disable HWPing client	**undo hwping-agent enabled**

By default, HWPing Client is disabled.

Creating a Test Group

HWPing test group is a set of HWPing test items. Each test group includes several test items and is uniquely identified by an administrator name plus an operation tag.

You may perform HWPing test after creating a test group and configuring all the parameters.

Perform the following configurations in System View.

Table 371 Create a Test Group

Operation	Command
Create a test group	**hwping** *administrator-name operation-tag*
Remove the test group	**undo hwping** *administrator-name operation-tag*

By default, no test group is configured.

Configure the Test Parameter

The following parameters are included in an HWPing test group:

- Destination address
- Test type
- Number of packets sent for a test
- Packet transmission interval
- Test timeout time

Configuring a Destination Address

The Destination address is equal to the destination address in a **ping** command.

Perform the following configurations in HWPing Test Group View.

Table 372 Configuring a Destination Address

Operation	Command
Configure a destination address	**destination-ip** *ip-address*
Delete the destination address	**undo destination-ip**

By default, no destination address is configured.

Configuring a Test Type

You can test various connections by using the HWPing function. You can only configure one test type at a time.

Currently, the system only supports ICMP test.

Perform the following configuration in HWPing Test Group View.

Table 373 Configure a Test Type

Operation	Command
Configure a test type	**`test-type`** *`type`*

By default, test type is set to ICMP.

Configure the Number of Messages Sent for a Test

If the number of messages sent for a test is set to greater than 1, the system sends the second message (after the first message has been sent) upon acknowledgement of the first message or upon the expiration of the test timer if no acknowledgement is received. This continues until all the test messages have been sent as configured. The parameter discussed in this subsection is equal to the parameter `-n` in a **`ping`** command.

Perform the following configurations in HWPing Test Group View.

Table 374 Configure the Number of Messages sent for a Test

Operation	Command
Configure the number of messages sent for a test	**`count`** *`times`*
Restore the default number of message sent for a test	**`undo count`** *`times`*

By default, one message is sent for a test.

Configuring Auto-Test Interval

Configured with the auto-test feature, the system will automatically test the connection of a specified type at regular intervals.

Perform the following configurations in HWPing Test Group View.

Table 375 Configure Auto-Test Interval

Operation	Command
Configure an auto-test interval	**`frequency`** *`interval`*
Disable auto-test	**`undo frequency`**

By default, auto-test interval is set to 0, i.e. only one test is performed.

Configuring Test Timeout Time

Test timeout time refers to the period that the system waits for ECHO-RESPONSE after sending an ECHO-REQUEST message. If the message expires, the system will regard the destination unreachable. The parameter discussed in this subsection is equal to the parameter `-t` in a **`ping`** command, except in a different time unit.

Perform the following configurations in HWPing Test Group View.

Table 376 Configure a Test Timeout Time

Operation	Command
Configure a test timeout time	**`timeout`** *`time`*
Restore the default setting of test timeout time	**`undo timeout`**

By default, test timeout time is set to three seconds.

Executing Test

After creating a test group and configuring the required test parameters, you can perform an HWPing test in the test group by executing the **`test-enable`** command.

Perform the following configuration in HWPing Test Group View.

Table 377 Test

Operation	Command
Execute test	*`test-enable`*

After you execute the **`test-enable`** *command, the system does not display the test result. You may view the test result information by executing the* **`display hwping`** *command.*

Displaying Test Information

You may view the test history and the last test information respectively by executing **`display hwping history`** and **`display hwping result`** commands.

Perform the following operations in any view.

Table 378 Display the Test Information

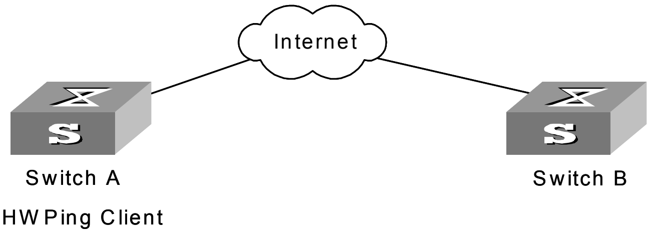
Operation	Command
Display the test information	**`display hwping`** `{` **`history`** `|` **`result`** `}` `[` *`administer-name operation-tag`* `]`

Typical HWPing Configuration Example

Like ping test, ICMP test in HWPing determines the roundtrip delay of a packet by making use of ICMP.

Network Diagram

Figure 82 HWPing



Configuration Procedure

Steps 1 to 3 and 6 are required for an ICMP test and the remaining three steps are optional.

Enable HWPing Client.

```
[SW5500]hwping-agent enable
```

1 Create an HWPing test group, given an administrator name “administrator” and a test operations is “icmp”.

```
[SW5500]hwping administrator icmp
```

2 Set the test type to ICMP.

```
[SW5500-hwping-administrator-icmp]test-type icmp
```

3 Configure a destination IP address 169.254.10.2.

```
[SW5500-hwping-administrator-icmp]destination-ip 169.254.10.2
```

4 Configure the number of test messages

```
[SW5500-hwping-administrator-icmp]count 10
```

5 Configure the timeout time.

```
[SW5500-hwping-administrator-icmp]timeout 3
```

6 Enable a test.

```
[SW5500-hwping-administrator-icmp]test-enable
```

7 View the test result.

```
[SW5500-hwping-administrator-icmp]display hwping result
administrator icmp
[SW5500-hwping-administrator-icmp]display hwping 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 SW5500 IFNET/6/UPDOWN:Line protocol on
interface GigabitEthernet1/0/2, 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 SW5500 IFNET/6/UPDOWN:Line protocol on
interface GigabitEthernet1/0/2, 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 SW5500 IFNET/6/UPDOWN:Line protocol on interface
Ethernet1/0/2, changed state to UP
```

It means that 166970ms (0*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 "SW5500".

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 379 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
FTPS	FTP server module
HA	High availability module
HTTPD	HTTP server module

Module name	Description
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	LANswitch ACL module
LQOS	LANswitch 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 380 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 six output directions of information.

The system assigns a channel in each output direction by default. See the table below.

Table 381 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
Trap buffer	3	trapbuffer
Logging buffer	4	logbuffer
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 six directions, that is, Console, monitor to Telnet terminal, logbuffer, loghost, trapbuffer, and SNMP.
- The log is divided into 8 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 loghost.

Table 382 Sending the Information to Loghost

Device	Configuration	Default Value	Configuration Description
Switch	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 loghost	-	The configuration about the loghost on the Switch and that on loghost must be the same; otherwise the information cannot be sent to the loghost correctly.
	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.
Loghost	Refer to configuration cases for related log host configuration	-	-

2 Sending the information to the control terminal.

Table 383 Sending the Information to the Control Terminal.

Device	Configuration	Default Value	Configuration Description
Switch	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	-	-
	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

3 Sending the Information to monitor terminal

Table 384 Sending the Information to Monitor Terminal

Device	Configuration	Default Value	Configuration Description
Switch	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	-	-
	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.

4 Sending the Information to log buffer.

Table 385 Sending the Information to Log Buffer

Device	Configuration	Default Value	Configuration Description
Switch	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.
	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 trap buffer.

Table 386 Sending the Information to Trap Buffer

Device	Configuration	Default Value	Configuration Description
Switch	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.
	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.

6 Sending the Information to SNMP

Table 387 Sending the Information to SNMP

Device	Configuration	Default value	Configuration description
Switch	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	-	-
	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	-	-

7 Turn on/off the information synchronization Switch in Fabric

Figure 83 Turn on/off the Information Synchronization Switch in Fabric

Device	Configuration	Default Value	Configuration Description
Switch	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	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 the loghost, follow the steps below:

1 Enabling info-center

Perform the following operation in System View.

Table 388 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.

Table 389 Configuring to Output Information to Loghost

Operation	Command
Output information to loghost	**info-center loghost** *host-ip-addr* **[channel {** *Channel-number* | *channel-name* **}** | **facility** *local-number* | **language { chinese** | **english }]**
Cancel the configuration of outputting information to loghost	**undo info-center loghost** *host-ip-addr*

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 the information source on the Switch

With this command, you can define the information that is sent to the control terminal, such as: generated by which modules, information type, information level, and so on.

Perform the following operation in System View.

Figure 84 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 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 390 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	**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 latter part of this chapter.

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 391 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 392 Configuring the Output Information to Control Terminal

Operation	Command
Output information to Console	**info-center console channel{** *channel-number* | *channel-name* **}**
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 393 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 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 394 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 395 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 396 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 397 Configuring to Output Information to Telnet Terminal or Dumb Terminal

Operation	Command
Output information to Telnet terminal or dumb terminal	**info-center monitor channel {** *channel-number* | *channel-name* **}**
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 398 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 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 399 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 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 400 Enabling Terminal Display Function

Operation	Command
Enable terminal display function of log, debugging and trap information	**terminal monitor**
Disable terminal display function of the above information	**undo terminal monitor**
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 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 401 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 log buffer

Perform the following operation in System View.

Table 402 Configuring the Output Information to Log Buffer

Operation	Command
Output information to log buffer	**info-center logbuffer [channel {** *channel-number* | *channel-name* **}** | **size** *buffersize* **]**
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 403 Defining the 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 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 404 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 405 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 406 Configuring the 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 407 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 408 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 409 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 410 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 411 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 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 412 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 413 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 414 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 {** *unit-id* | **master** | **all } [debugging** | **logging** | **trapping]***
Turn off the information synchronization Switch of the specified Switch	**undo info-center switch-on {** *unit-id* | *master* | **all } [debugging** | **logging** | **trapping]***

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 85 Displaying and Debugging Info-center

Operation	Command
Display the content of information channel	**display channel [** *channel-number* | *channel-name* **]**
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 Log to Unix Loghost

Networking Requirement

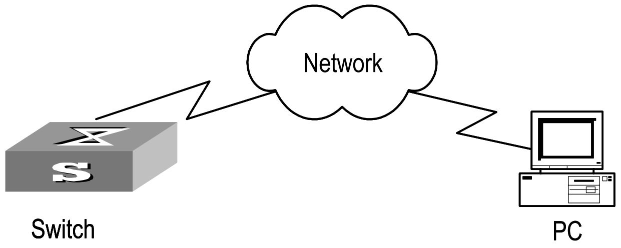
The networking requirements are as follows:

- 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 86 Schematic Diagram of Configuration



Configuration Procedure

1 Configuration on the Switch

a Enabling info-center

```
[SW5500]info-center enable
```

b 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.

```
[SW5500]info-center loghost 202.38.1.10 facility local4 language
english
[SW5500]info-center source arp channel loghost log level
informational
[SW5500]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/SW5500
# touch /var/log/SW5500/information
```

b Edit file /etc/syslog.conf as the super user (root), add the following selector/actor pairs.

```
# SW5500 configuration messages
local4.info /var/log/SW5500/information
```

Note the following points when editing /etc/syslog.conf:

(1) The note must occupy a line and start with the character #.

(2) There must be a tab other than a space as the separator in selector/actor pairs.

(3) No redundant space after file name.

(4) 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 for Sending Log to Linux Loghost

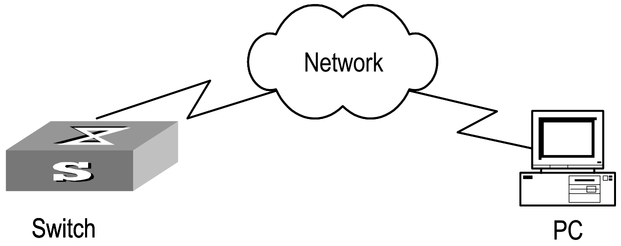
Networking Requirement

The networking requirements 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 87 Schematic Diagram of Configuration



Configuration Procedure

1 Enabling info-center

```
[SW5500]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.

```
[SW5500]info-center loghost 202.38.1.10 facility local7 language
english
[SW5500]info-center source default channel loghost log level
informational
```

2 Configuration on the loghost

This configuration is performed on the loghost.

a Perform the following command as the super user (root).

```
# mkdir /var/log/SW5500
# touch /var/log/SW5500/information
```

b Edit file `/etc/syslog.conf` as the super user (root), add the following selector/actor pairs.

```
# SW5500 configuration messages
local7.info /var/log/SW5500/information
```

Note the following points when editing /etc/syslog.conf:

(1) The note must occupy a line and start with the character #.

(2) There must be a tab other than a space as the separator in selector/actor pairs.

(3) No redundant space after file name.

(4) 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

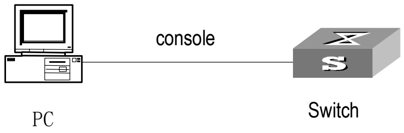
The networking requirements are as follows:

- 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 88 Schematic Diagram of Configuration



Configuration Procedure

1 Configuration on the Switch

Enabling info-center

```
[SW5500]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.

```
[SW5500]info-center console channel console
[SW5500]info-center source arp channel console log level
informational
[SW5500]info-center source ip channel console log level
informational
```

3 Enabling terminal display function

```
<SW5500> terminal logging
```

SNMP Configuration

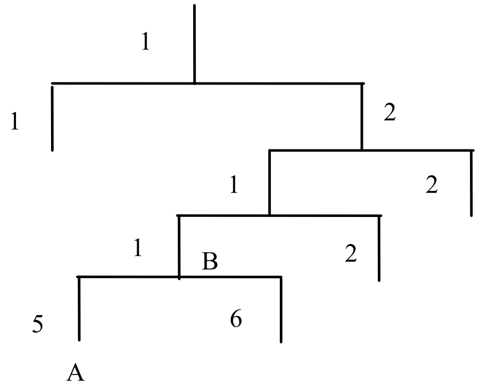
The Simple Network Management Protocol (SNMP) has gained the most extensive application in the computer networks. SNMP has been put into use and widely accepted as an industry standard in practice. It is used for ensuring the transmission of the management information between any two nodes. In this way, 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 89 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 415 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	

Configure 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 416 Set Community Name

Operation	Command
Set the community name and the access authority	**snmp-agent community { read | write }** *community-name* **[mib-view** *view-name* **] [acl** *acl-list* **]**
Remove the community name and the access authority	**undo snmp-agent community** *community-name*

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 417 Enable/Disable SNMP Agent to Send Trap

Operation	Command
Enable to send trap	**snmp-agent trap enable [configuration | flash | ospf [** *process-id* **] [** *ospf-trap-list* **] | standard [authentication | coldstart | linkdown | linkup | warmstart]* | system]**
Disable to send trap	**undo snmp-agent trap enable [bgp [backwardtransition] [established] | configuration | flash | ospf [** *process-id* **] [** *ospf-trap-list* **] | standard [authentication | coldstart | linkdown | linkup | warmstart]* | system]**

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 418 Set the Destination Address of Trap

Operation	Command
Set the destination address of trap	**snmp-agent target-host trap address udp-domain** *host-addr* **[udp-port** *udp-port-number* **] params securityname** *community-string* **[v1 | v2c | v3 [authentication | privacy]]**
Delete the destination address of trap	**undo snmp-agent target-host** *host-addr* **securityname** *community-string*

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 419 Set the Lifetime of Trap Message

Operation	Command
Set lifetime of Trap message	**snmp-agent trap life** *seconds*
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 420 Set SNMP System Information

Operation	Command
Set SNMP System Information	**snmp-agent sys-info { contact** *sysContact* **| location** *syslocation* **| version { { v1 | v2c | v3 } * | all } }**

Operation	Command
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 421 Set the Engine ID of a Local or Remote Device

Operation	Command
Set the engine ID of the device	**snmp-agent local-engineid** *engineid*
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 422 Set/Delete an SNMP Group

Operation	Command
Setting an SNMP group	**snmp-agent group { v1 | v2c }** *group-name* **[read-view** *read-view* **] [write-view** *write-view* **] [notify-view** *notify-view* **] [acl** *acl-list* **]** **snmp-agent group v3** *group-name* **[authentication | privacy] [read-view** *read-view* **] [write-view** *write-view* **] [notify-view** *notify-view* **] [acl** *acl-list* **]**
Deleting an SNMP group	**undo snmp-agent group { v1 | v2c }** *group-name* **undo snmp-agent group v3** *group-name* **[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 423 Set the Source Address of Trap

Operation	Command
Set the source address of trap	**snmp-agent trap source** *interface-name interface-num*
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 424 Add/Delete a user to/from an SNMP Group

Operation	Command
Add a user to an SNMP group.	**snmp-agent usm-user { v1 | v2c }** *username groupname* **[acl** *acl-list* **] snmp-agent usm-user v3** *username groupname* **[authentication-mode { md5 | sha }** *authpassstring* **[privacy-mode { des56** *privpassstring* **}]] [acl** *acl-list* **]**
Delete a user from an SNMP group.	**undo snmp-agent usm-user { v1 | v2c }** *username groupname* **undo snmp-agent usm-user v3** *username groupname* **{ local | engineid** *engine-id* **}**

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 425 Create/Update View Information or Deleting a View

Operation	Command
Create/Update view information	**snmp-agent mib-view { included | excluded }** *view-name oid-tree*
Delete a view	**undo snmp-agent mib-view** *view-name*

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 426 Set the Size of SNMP Packet sent/received by an Agent

Operation	Command
Set the size of SNMP packet sent/received by an agent	**snmp-agent packet max-size** *byte-count*
Restore the default size of SNMP packet sent/received by an agent	**undo snmp-agent packet max-size**

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 427 Enable/Disable a Port Transmitting Trap Information SNMP Agent

Operation	Command
enable current port to transmit the trap information	**enable snmp trap updown**
disable current port to transmit the trap information	**undo enable snmp trap updown**

Disabling SNMP Agent

To disable SNMP Agent, perform the following configuration in System View.

Table 428 Disable SNMP Agent

Operation	Command
Disable snmp agent	**undo snmp-agent**

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.

Table 429 Display and Debug SNMP

Operation	Command
Display the statistics information about SNMP packets	**display snmp-agent statistics**
Display the engine ID of the active device	**display snmp-agent { local-engineid | remote-engineid }**
Display the group name, the security mode, the states for all types of views, and the storage mode of each group of the Switch.	**display snmp-agent group [** *group-name* **]**
Display the names of all users in the group user table	**display snmp-agent usm-user [engineid** *engineid* **] [group** *groupname* **] [username** *username* **]**
Display the current community name	**display snmp-agent community [read | write]**
Display the current MIB view	**display snmp-agent mib-view [exclude | include | viewname** *mib-view* **]**
Display the contact character string of the system	**display snmp-agent sys-info contact**
Display the location character string of the system	**display snmp-agent sys-info location**
Display the version character string of the system	**display snmp-agent sys-info version**

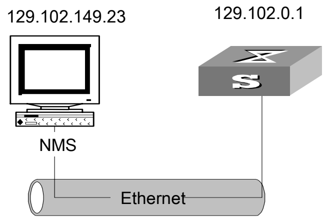
SNMP Configuration Example

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 90 SNMP Configuration Example



Configuration Procedure

1 Enter the System View.

```
<SW5500> system-view
```

2 Set the community name , group name and user.

```
[SW5500]snmp-agent sys-info version all
[SW5500]snmp-agent community write public
[SW5500]snmp-agent mib include internet 1.3.6.1
[SW5500]snmp-agent group v3 managev3group write internet
[SW5500]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.

```
[SW5500]vlan 2
[SW5500-vlan2]port ethernet 1/0/3
[SW5500-vlan2]interface vlan 2
[SW5500-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.

```
[SW5500]snmp-agent sys-info contact Mr.Wang-Tel:3306
[SW5500]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.

```
[SW5500]snmp-agent trap enable standard authentication
[SW5500]snmp-agent trap enable standard coldstart
[SW5500]snmp-agent trap enable standard linkup
[SW5500]snmp-agent trap enable standard linkdown
[SW5500]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 Usmusr Table Configuration Example

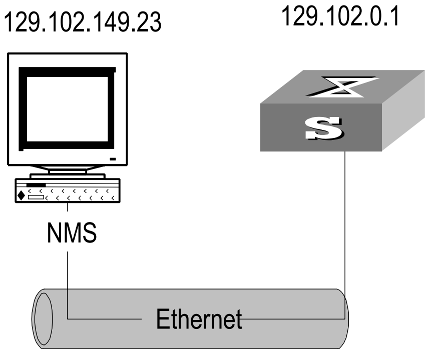
Networking requirements

ViewDefault view should be reconfigured if you use SNMP V3 to read the usmusr table.

The snmpVacmMIB and snmpUsmMIB should be included in ViewDefault view.

Networking diagram

Figure 91 SNMP configuration example



Configuration procedure

```
[SW5500]snmp-agent community read public
[SW5500]snmp-agent community write private
[SW5500]snmp-agent sys-info version all
[SW5500]snmp-agent group v3 sdsdsd
[SW5500]snmp-agent usm-user v3 paul sdsdsd authentication-mode md5
hello
[SW5500]snmp-agent mib-view included ViewDefault snmpUsmMIB
[SW5500]snmp-agent mib-view included ViewDefault snmpVacmMIB
[SW5500]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
```

RMON Configuration

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 430 Add/Delete an Entry to/from the Alarm Table

Operation	Command
Add an entry to the alarm table.	**rmon alarm** *entry-number alarm-variable sampling-time* **{ delta | absolute } rising-threshold** *threshold-value1 event-entry1* **falling-threshold** *threshold-value2 event-entry2* **[owner** *text* **]**
Delete an entry from the alarm table.	**undo rmon alarm** *entry-number*

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 431 Add/Delete an Entry to/from the Event Table

Operation	Command
Add an entry to the event table.	**rmon event** *event-entry* **[description** *string*] **{ log | trap** *trap-community* | **log-trap** *log-trapcommunity* | **none } [owner** *rmon-station* **]**
Delete an entry from the event table.	**undo rmon event** *event-entry*

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 432 Add/Delete an Entry to/from the History Control Terminal

Operation	Command
Add an entry to the history control terminal.	**rmon history** *entry-number* **buckets** *number* **interval** *sampling-interval* **[owner** *text-string* **]**
Delete an entry from the history control terminal.	**undo rmon history** *entry-number*

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 433 Add/Delete an Entry to/from the Extended RMON Alarm Table

Operation	Command
Add an entry to the extended RMON alarm table.	**rmon prialarm** *entry-number alarm-var* **[** *alarm-des* **]** *sampling-timer* **{ delta | absolute | changeratio } rising-threshold** *threshold-value1 event-entry1* **falling-threshold** *threshold-value2 event-entry2* **entrytype { forever | cycle** *cycle-period* **} [owner text]**
Delete an entry from the extended RMON alarm table.	**undo rmon prialarm** *entry-number*

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 434 Add/Delete an Entry to/from the Statistics Table

Operation	Command
Add an entry to the statistics table	**rmon statistics** *entry-number* **[owner** *text-string* **]**
Delete an entry from the statistics table	**undo rmon statistics** *entry-number*

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 435 Display and Debug RMON

Operation	Command
Display the RMON statistics	**display rmon statistics [** *port-num* **]**
Display the history information of RMON	**display rmon history [** *port-num* **]**

Operation	Command
Display the alarm information of RMON	**display rmon alarm [** *alarm-table-entry* **]**
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* **]**

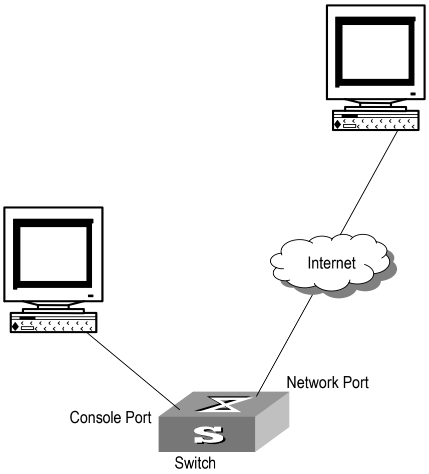
RMON Configuration Example

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 92 RMON Configuration Networking



Configuration Procedure

1 Configure RMON.

```
[SW5500-GigabitEthernet1/0/1]rmon statistics 1 owner 3com-rmon
```

2 View the configurations in User View.

```
<SW5500> display rmon statistics Ethernet 1/0/1
Statistics entry 1 owned by 3com-rmon is VALID.
  Gathers statistics of interface GigabitEthernet1/0/1. 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
```

NTP Overview

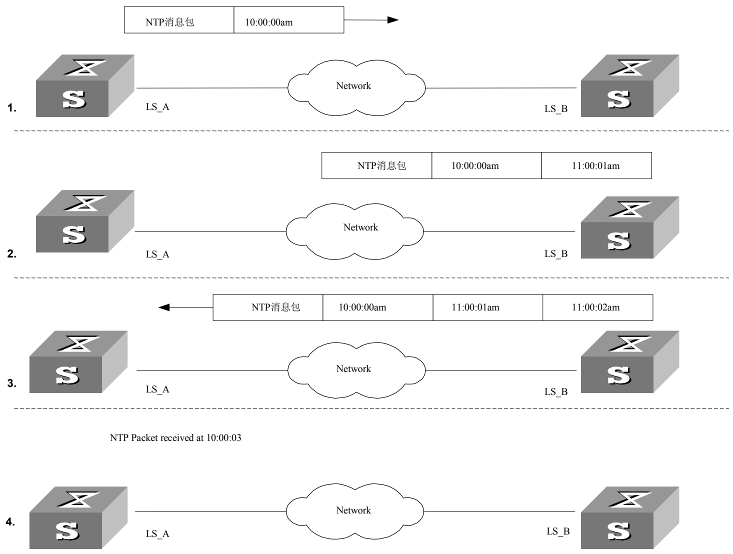
As the network topology gets more and more complex, it becomes important to synchronize the clocks of the equipment on the whole network. Network Time Protocol (NTP) is the TCP/IP that advertises the accurate time throughout the network.

NTP ensures the consistency of the following applications:

- For the increment backup between the backup server and client, NTP ensures the clock synchronization between the two systems.
- For multiple systems that coordinate to process a complex event, NTP ensures them to reference the same clock and guarantee the right order of the event.
- Guarantee the normal operation of the inter-system (Remote Procedure Call).
- Record for an application when a user logs in to a system, a file is modified, or Basic Operating Principle of NTP

The following figure illustrates the basic operating principle of NTP:

Figure 93 Basic Operating Principle of NTP



In the figure above, Switch A and Switch B are connected via the Ethernet port. They have independent system clocks. Before implementing automatic clock synchronization on both Switches, it is assume that:

- The clock on Switch A is set to 10:00:00am, and that on B is set to 11:00:00am.
- Switch B serves as an NTP time server. That is, Switch A synchronizes the local clock with the clock of B.
- It takes 1 second to transmit a data packet from either A or B to the opposite end.

The system clocks are synchronized as follows:

- Switch A sends an NTP packet to Switch B. The packet carries the timestamp 10:00:00am (T_1) that tells when it left Switch A.
- When the NTP packet arrives at Switch B, Switch B adds a local timestamp 11:00:01am (T_2) to it.
- When the NTP packet leaves Switch B, Switch B adds another local timestamp 11:00:02am (T_3) to it.
- When Switch A receives the acknowledgement packet, it adds a new timestamp 10:00:03am (T_4) to it.

Now Switch A collects enough information to calculate the following two important parameters:

- The delay for a round trip of an NTP packet traveling between the Switch A and B: Delay= (T_4-T_1) - (T_3-T_2).
- Offset of Switch A clock relative to Switch B clock: offset= ((T_2-T_1) + (T_4-T_3)) /2.

In this way, Switch A uses the above information to set the local clock and synchronize it with the clock on Switch B.

The operating principle of NTP is briefly introduced above. For more information, refer to RFC1305.

NTP Configuration

NTP is used for time synchronization throughout a network. NTP configuration tasks include:

- Configure NTP operating mode
- Configure NTP ID authentication
- Set NTP authentication key
- Set the specified key to be reliable
- Set a local interface for transmitting NTP packets
- Set an external reference clock or the local clock as the master NTP clock
- Enable/Disable an interface to receive NTP packets
- Set control authority to access the local Switch service
- Set maximum local sessions

Configuring NTP Operating Mode

You can set the NTP operating mode of a Switch according to its location in the network and the network structure. For example, you can set a remote server as the time server of the local equipment. In this case the local Switch works as an NTP client. If you set a remote server as a peer of the local Switch, the local equipment operates in symmetric active mode. If you configure an interface on the local Switch to transmit NTP broadcast packets, the local Switch will operate in broadcast mode. If you configure an interface on the local Switch to receive NTP broadcast packets, the local Switch will operate in broadcast client mode. If you configure an interface on the local Switch to transmit NTP multicast packets, the local Switch will operate in multicast mode. Or you may also configure an interface on the local Switch to receive NTP multicast packets, the local Switch will operate in multicast client mode.

- Configure NTP server mode
- Configure NTP peer mode
- Configure NTP broadcast server mode
- Configure NTP broadcast client mode
- Configure NTP multicast server mode
- Configure NTP multicast client mode

Configuring NTP Server Mode

Set a remote server whose ip address is *ip-address* as the local time server. *ip-address* specifies a host address other than a broadcast, multicast or reference clock IP address. In this case, the local Switch operates in client mode. In this mode, only the local client synchronizes its clock with the clock of the remote server, while the reverse synchronization will not happen.

Perform the following configurations in System View.

Table 436 Configure NTP Time Server

Operation	Command
Configure NTP time server	**ntp-service unicast-server** *ip-address* **[version** *number* **] [authentication-keyid** *keyid* **] [source-interface {** *interface-name* | *interface-type interface-number* **}] [priority]**
Cancel NTP server mode	**undo ntp-service unicast-server** *ip-address*

NTP version number *number* ranges from 1 to 3 and defaults to 3; the authentication key ID *keyid* ranges from 0 to 4294967295; *interface-name* or *interface-type interface-number* specifies the IP address of an interface, from which the source IP address of the NTP packets sent from the local Switch to the time server will be taken; **priority** indicates the time server will be the first choice.

Configuring NTP Peer Mode

Set a remote server whose ip address is *ip-address* as the peer of the local equipment. In this case, the local equipment operates in symmetric active mode. *ip-address* specifies a host address other than a broadcast, multicast or reference clock IP address. In this mode, both the local Switch and the remote server can synchronize their clocks with the clock at the opposite end.

Perform the following configurations in System View.

Table 437 Configure NTP Peer Mode

Operation	Command
Configure NTP peer mode	**ntp-service unicast-peer** *ip-address* **[version** *number* **] [authentication-key** *keyid* **] [source-interface {** *interface-name* | *interface-type interface-number* **}] [priority]**
Cancel NTP peer mode	**undo ntp-service unicast-peer** *ip-address*

NTP version number *number* ranges from 1 to 3 and defaults to 3; the authentication key ID *keyid* ranges from 0 to 4294967295; *interface-name* or *interface-type interface-number* specifies the IP address of an interface, from which the source IP address of the NTP packets sent from the local Switch to the peer will be taken; **priority** indicates the peer will be the first choice for the time server.

Configuring NTP Broadcast Server Mode

Designate an interface on the local Switch to transmit NTP broadcast packets. In this case, the local equipment operates in broadcast mode and serves as a broadcast server to broadcast messages to its clients regularly.

Perform the following configurations in the VLAN interface view.

Table 438 Configure NTP Broadcast Server Mode

Operation	Command
Configure NTP broadcast server mode	**ntp-service broadcast-server [authentication-keyid** *keyid* **version** *number* **]**
Cancel NTP broadcast server mode	**undo ntp-service broadcast-server**

NTP version number *number* ranges from 1 to 3 and defaults to 3; the authentication key ID *keyid* ranges from 0 to 4294967295. This command can only be configured on the interface where the NTP broadcast packets will be transmitted.

Configuring NTP Broadcast Client Mode

Designate an interface on the local Switch to receive NTP broadcast messages and operate in broadcast client mode. The local Switch listens to the broadcast from the server. When it receives the first broadcast packets, it starts a brief client/server mode to Switch messages with a remote server for estimating the network delay. Thereafter, the local Switch enters broadcast client mode and continues listening to the broadcast and synchronizes the local clock according to the arrived broadcast message.

Perform the following configurations in the VLAN Interface View.

Table 439 Configure NTP Broadcast Client Mode

Operation	Command
Configure NTP broadcast client mode	**ntp-service broadcast-client**
Disable NTP broadcast client mode	**undo ntp-service broadcast-client**

This command can only be configured on the interface where the NTP broadcast packets will be received.

Configuring NTP Multicast Server Mode

Designate an interface on the local Switch to transmit NTP multicast packets. In this case, the local equipment operates in multicast mode and serves as a multicast server to multicast messages to its clients regularly.

Perform the following configurations in the VLAN Interface View.

Table 440 Configure NTP Multicast Server Mode

Operation	Command
Configure NTP multicast server mode	**ntp-service multicast-server [** *ip-address* **] [authentication-keyid** *keyid* **] [ttl** *ttl-number* **] [version** *number* **]**
Cancel NTP multicast server mode	**undo ntp-service multicast-server**

NTP version number *number* ranges from 1 to 3 and defaults to 3; the authentication key ID *keyid* ranges from 0 to 4294967295; *ttl-number* of the multicast packets ranges from 1 to 255; and the multicast IP address defaults to 224.0.1.1.

This command can only be configured on the interface where the NTP multicast packet will be transmitted.

Configuring NTP Multicast Client Mode

Designate an interface on the local Switch to receive NTP multicast messages and operate in multicast client mode. The local Switch listens to the multicast from the server. When it receives the first multicast packets, it starts a brief client/server mode to Switch messages with a remote server for estimating the network delay. Thereafter, the local Switch enters multicast client mode and continues listening to the multicast and synchronizes the local clock by the arrived multicast message.

Perform the following configurations in VLAN interface view.

Table 441 Configure NTP multicast client mode

Operation	Command
Configure NTP multicast client mode	**ntp-service multicast-client [** *ip-address* **]**
Cancel NTP multicast client mode	**undo ntp-service multicast-client**

Multicast IP address *ip-address* defaults to 224.0.1.1. This command can only be configured on the interface where the NTP multicast packets will be received.

Configuring NTP ID Authentication

Enable NTP authentication, set MD5 authentication key, and specify the reliable key. A client will synchronize itself by a server only if the server can provide a reliable key.

Perform the following configurations in System View.

Table 442 Configure NTP Authentication

Operation	Command
Enable NTP authentication	**ntp-service authentication enable**
Disable NTP authentication	**undo ntp-service authentication enable**

Setting NTP Authentication Key

This configuration task is to set NTP authentication key.

Perform the following configurations in System View.

Table 443 Configure NTP Authentication Key

Operation	Command
Configure NTP authentication key	**ntp-service authentication-keyid** *number* **authentication-mode md5** *value*
Remove NTP authentication key	**undo ntp-service authentication-keyid** *number*

Key number *number* ranges from 1 to 4294967295; the key *value* contains 1 to 32 ASCII characters.

Setting Specified Key as Reliable

This configuration task is to set the specified key as reliable.

Perform the following configurations in System View.

Table 444 Set the Specified Key as Reliable

Operation	Command
Set the specified key as reliable	**ntp-service reliable authentication-keyid** *key-number*
Cancel the specified reliable key.	**undo ntp-service reliable authentication-keyid** *key-number*

Key number *key-number* ranges from 1 to 4294967295.

Designating an Interface to Transmit NTP Message

If the local equipment is configured to transmit all the NTP messages, these packets will have the same source IP address, which is taken from the IP address of the designated interface.

Perform the following configurations in System View.

Table 445 Designate an Interface to Transmit NTP Message

Operation	Command
Designate an interface to transmit NTP message	**ntp-service source-interface {** *interface-name* | *interface-type interface-number* **}**
Cancel the interface to transmit NTP message	**undo ntp-service source-interface**

An interface is specified by *interface-name* or *interface-type interface-number*. The source address of the packets will be taken from the IP address of the interface. If the **ntp-service unicast-server** or **ntp-service unicast-peer** command also designates a transmitting interface, use the one designated by them.

Enabling/Disabling an Interface to Receive NTP Message

This configuration task is to enable/disable an interface to receive NTP message.

Perform the following configurations in VLAN interface view.

Table 446 Enable/Disable an Interface to Receive NTP Message

Operation	Command
Disable an interface to receive NTP message	**ntp-service in-interface disable**
Enable an interface to receive NTP message	**undo ntp-service in-interface disable**

This configuration task must be performed on the interface to be disabled to receive NTP message.

Setting Authority to Access a Local Switch

Set authority to access the NTP services on a local Switch. This is a basic and brief security measure, compared to authentication. An access request will be matched with **peer**, **serve**, **serve only**, and **query only** in an ascending order of the limitation. The first matched authority will be given.

Perform the following configurations in System View.

Table 447 Set Authority to Access a Local Switch

Operation	Command
Set authority to access a local Switch	**ntp-service access { query | synchronization | server | peer }** *acl-number*
Cancel settings of the authority to access a local Switch	**undo ntp-service access { query | synchronization | server | peer }**

IP address ACL number is specified through the *acl-number* parameter and ranges from 2000 to 2999. The meanings of other authority levels are as follows:

query: Allow control query for the local NTP service only.

synchronization: Allow request for local NTP time service only.

serve: Allow local NTP time service request and control query. However, the local clock will not be synchronized by a remote server.

peer: Allow local NTP time service request and control query. The local clock will also be synchronized by a remote server.

Setting Maximum Local Sessions

This configuration task is to set the maximum local sessions.

Perform the following configurations in System View.

Table 448 Set the Maximum Local Sessions

Operation	Command
Set the maximum local sessions	**ntp-service max-dynamic-sessions** *number*
Resume the maximum number of local sessions	**undo ntp-service max-dynamic-sessions**

number specifies the maximum number of local sessions, ranges from 0 to 100, and defaults to 100.

Displaying and Debugging NTP

After completing the above configurations, you can use the **display** command to show how NTP runs and verify the configurations according to the outputs.

In User View, you can use the **debugging** command to debug NTP.

Table 449 NTP Display and Debugging

Operation	Command
Display the status of NTP service	**display ntp-service status**
Display the status of sessions maintained by NTP service	**display ntp-service sessions [verbose]**
Display the brief information about every NTP time server on the way from the local equipment to the reference clock source.	**display ntp-service trace**
Enable NTP debugging	**debugging ntp-service**

Typical NTP Configuration Examples

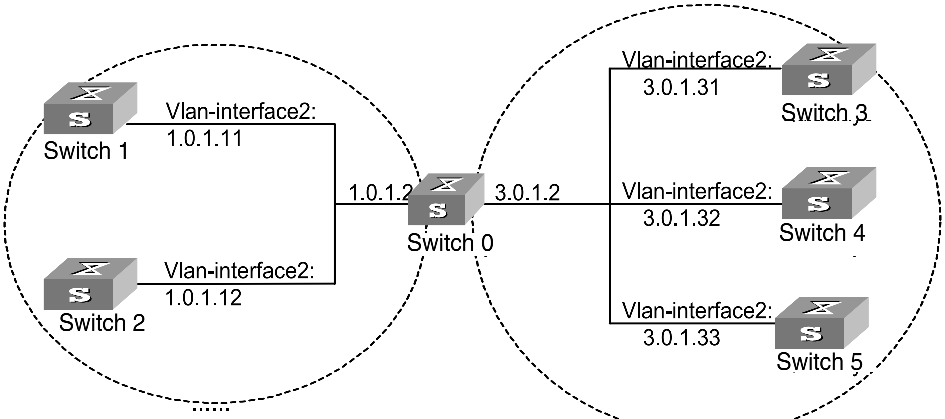
Configure NTP Server

Network Requirements

On Switch1, set the local clock as the NTP master clock at stratum 2. On Switch 2, configure Switch 1 as the time server in server mode and set the local equipment as in client mode.

Networking Diagram

Figure 94 Typical NTP Configuration Networking Diagram



Configuration Procedure

Configure Switch 1:

1 Enter System View.

```
<switch1> system-view
```

2 Set the local clock as the NTP master clock at stratum 2.

```
[switch1]ntp-service refclock-master 2
```

Configure Switch 2:

1 Enter System View.

```
<switch2> system-view
```

2 Set SW5500 1 as the NTP server.

```
[switch2]ntp-service unicast-server 1.0.1.11
```

The above examples synchronized Switch 2 by Switch 1. Before the synchronization, the Switch 2 is shown in the following status:

```
[switch2]display ntp-service status
clock status: unsynchronized
 clock stratum: 16
 reference clock ID: none
 nominal frequency: 100.0000 Hz
 actual frequency: 100.0000 Hz
 clock precision: 2^17
 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)
```

After the synchronization, Switch 2 turns into the following status:

```
[switch2]display ntp-service status
clock status: synchronized
 clock stratum: 3
 reference clock ID: 1.0.1.11
 nominal frequency: 60.0002 Hz
 actual frequency: 60.0002 Hz
 clock precision: 2^17
 clock offset: -9.8258 ms
 root delay: 27.10 ms
 root dispersion: 48.29 ms
 peer dispersion: 10.94 ms
 reference time: 19:21:32.287 UTC Oct 24 2004(C5267F3C.49A61EOC)
```

By this time, Switch 2 has been synchronized by Switch 1 and is at stratum 3, higher than Switch 1 by 1.

Display the sessions of Switch 2 and you will see Switch 2 has been connected with Switch 1.

```
[switch2]display ntp-service sessions
source          reference    stra reach poll now offset delay disper
```

```
*******************************************************************
[12345]1.0.1.11 LOCAL(0)      3     377   64    16 -0.4      0.0 0.9
note: 1 source(master),2 source(peer),3 selected,4 candidate,5
configured
```

NTP peer Configuration

Network Requirements

On Switch 3, set local clock as the NTP master clock at stratum 2. On Switch 2, configure SW5500G-EI 1 as the time server in server mode and set the local equipment as in client mode. At the same time, Switch 5 sets Switch 4 as its peer.

Networking Diagram

See Figure 94.

Configuration Procedure

Configure Switch 3:

1 Enter System View.

```
<switch3> system-view
```

2 Set the local clock as the NTP master clock at stratum 2.

```
[switch3]ntp-service refclock-master 2
```

Configure Switch 4:

1 Enter System View.

```
<switch4> system-view
```

2 Set Switch 1 as the NTP server at stratum 3 after synchronization.

```
[switch4]ntp-service unicast-server 3.0.1.31
```

Configure Switch 5: (Switch 4 has been synchronized by Switch 3)

1 Enter System View.

```
<switch5> system-view
```

Set the local clock as the NTP master clock at stratum 1

```
[switch5] ntp-service unicast-peer 3.0.1.32
```

2 After performing local synchronization, set Switch 4 as a peer.

```
[switch5]ntp-service unicast-peer 3.0.1.32
```

The above examples configure Switch 4 and Switch 5 as peers and configures Switch 5 in active peer mode and Switch 4 in passive peer mode. Since Switch 5 is at stratum 1 and Switch 4 is at stratum 3, synchronize Switch 4 by Switch 5.

After synchronization, Switch 4 status is shown as follows:

```
[switch4]display ntp-service status
clock status: synchronized
 clock stratum: 2
 reference clock ID: 3.0.1.31
 nominal frequency: 60.0002 Hz
 actual frequency: 60.0002 Hz
 clock precision: 2^17
 clock offset: -9.8258 ms
 root delay: 27.10 ms
 root dispersion: 49.29 ms
 peer dispersion: 10.92 ms
reference time: 19:21:32.287 UTC Oct 24 2004(C5267F3C.49A61E0C)
```

By this time, Switch 4 has been synchronized by Switch 5 and it is at stratum 2, or higher than Switch 5 by 1.

Display the sessions of Switch 4 and you will see Switch 4 has been connected with Switch 5.

```
[switch4]display ntp-service sessions
source          reference stra reach poll  now offset  delay disper
*******************************************************************
[12345]3.0.1.33 LOCAL(0) 2   377   64      16   0.0     0.0 0.9
note: 1 source(master),2 source(peer),3 selected,4 candidate,5
configured
```

Configure NTP Broadcast Mode

Network Requirements

On Switch 3, set local clock as the NTP master clock at stratum 2 and configure to broadcast packets from Vlan-interface2. Configure Switch 4 and Switch 1 to listen to the broadcast from their Vlan-interface2 respectively. **Networking Diagram**

See Figure 94.

Configuration Procedure

Configure Switch 3:

1 Enter System View.

```
<switch3> system-view
```

2 Set the local clock as the NTP master clock at stratum 2.

```
[switch3]ntp-service refclock-master 2
```

3 Enter Vlan-interface2 view.

```
[switch3]interface vlan-interface 2
```

4 Set it as broadcast server.

```
[switch3-Vlan-Interface2]ntp-service broadcast-server
```

Configure Switch 4:

1 Enter System View.

```
<switch4> system-view
```

2 Enter Vlan-interface2 view.

```
[switch4]interface vlan-interface 2
[switch4-Vlan-Interface2]ntp-service broadcast-client
```

Configure Switch 1:

1 Enter System View.

```
<switch1> system-view
```

2 Enter Vlan-interface2 view.

```
[switch1]interface vlan-interface 2
[switch1-Vlan-Interface2]ntp-service broadcast-client
```

In the above examples Switch 4 and Switch 1 are configured to listen to the broadcast via Vlan-interface2, Switch 3 to broadcast packets from Vlan-interface2. As Switch 1 and Switch 3 are not located on the same segment, they cannot receive any broadcast packets from Switch 3, while Switch 4 is synchronized by Switch 3 after receiving its broadcast packet.

3 After the synchronization, you can find the state of Switch 4 as follows:

```
[switch4]display ntp-service status
clock status: synchronized
 clock stratum: 3
 reference clock ID: LOCAL(0)
 nominal frequency: 100.0000 Hz
 actual frequency: 100.0000 Hz
 clock precision: 2^17
 clock offset: 0.0000 ms
 root delay: 0.00 ms
 root dispersion: 10.94 ms
 peer dispersion: 10.00 ms
 reference time: 20:54:25.156 UTC Mar 7 2002(C0325201.2811A112)
```

By this time, Switch 4 has been synchronized by Switch 3 and it is at stratum 3, higher than Switch 3 by 1.

Display the status of Switch 4 sessions and you will see Switch 4 has been connected to Switch 3.

```
[switch2]display ntp-service sessions
source       reference stra reach poll  now offset  delay disper
********************************************************************
[12345]127.127.1.0 LOCAL(0) 7 377  64   57    0.0    0.0    1.0
[5]1.0.1.11        0.0.0.0 3  0    64    -    0.0    0.0    0.0
[5]128.108.22.44   0.0.0.0 16 0    64    -    0.0    0.0    0.0
note: 1 source(master),2 source(peer),3 selected,4 candidate,5
configured
```

Configure NTP Multicast Mode

Network Requirements

Switch 3 sets the local clock as the master clock at stratum 2 and multicast packets from Vlan-interface2. Set Switch 4 and Switch 1 to receive multicast messages from their respective Vlan-interface2. **Networking Diagram**

See Figure 94.

Configuration Procedure

Configure Switch 3:

1 Enter System View.

```
<switch3> system-view
```

2 Set the local clock as a master NTP clock at stratum 2.

```
[switch3]ntp-service refclock-master 2
```

3 Enter Vlan-interface2 view.

```
[switch3]interface vlan-interface 2
```

4 Set it as a multicast server.

```
[switch3-Vlan-Interface2]ntp-service multicast-server
```

Configure Switch 4:

1 Enter System View.

```
<switch4> system-view
```

2 Enter Vlan-interface2 view.

```
[switch4]interface vlan-interface 2
```

3 Enable multicast client mode.

```
[switch4-Vlan-Interface2]ntp-service multicast-client
```

Configure Switch 1:

1 Enter System View.

```
<switch1> system-view
```

2 Enter Vlan-interface2 view.

```
[switch1]interface vlan-interface 2
```

3 Enable multicast client mode.

```
[switch1-Vlan-Interface2]ntp-service multicast-client
```

The above examples configure Switch 4 and Switch 1 to receive multicast messages from Vlan-interface2, Switch 3 multicast messages from Vlan-interface2. Since Switch 1 and Switch 3 are not located on the same segments, Switch 1 cannot receive the multicast packets from Switch 3, while Switch 4 is synchronized by Switch 3 after receiving the multicast packet.

Configure Authentication-enabled NTP Server Mode

Network Requirements

Switch 1 sets the local clock as the NTP master clock at stratum 2. Switch 2 sets Switch 1 as its time server in server mode and itself in client mode and enables authentication. **Networking Diagram**

See Figure 94.

Configuration Procedure

Configure Switch 1:

1 Enter System View.

```
<switch1> system-view
```

2 Set the local clock as the master NTP clock at stratum 2.

```
[switch1]ntp-service refclock-master 2
```

Configure Switch 2:

1 Enter System View.

```
<switch2> system-view
```

2 Set Switch 1 as time server.

```
[switch2]ntp-service unicast-server 1.0.1.11
```

3 Enable authentication.

```
[switch2]ntp-service authentication enable
```

4 Set the key.

```
[switch2]ntp-service authentication-keyid 42 authentication-mode md5
aNiceKey
```

Set the key as reliable.

5
```
[switch2]ntp-service reliable authentication-keyid 42
[switch2]ntp-service unicast-server 1.0.1.11 authentication-keyid 42
```

The above examples synchronized Switch 2 by Switch 1. Since Switch 1 has not been enabled authentication, it cannot synchronize Switch 2. And now let us do the following additional configurations on Switch 1:

1 Enable authentication.

```
[switch1]ntp-service authentication enable
```

2 Set the key.

```
[switch1]ntp-service authentication-keyid 42 authentication-mode md5
aNiceKey
```

3 Configure the key as reliable.

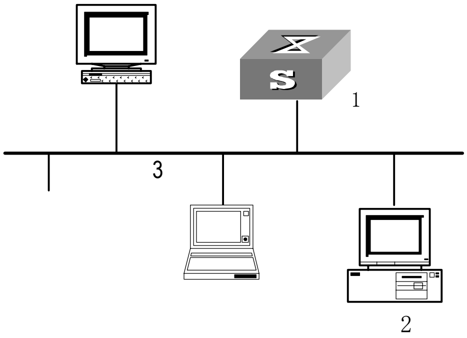
```
[switch1]ntp-service reliable authentication-keyid 42
```

SSH Terminal Services

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 from an insecure network environment. A Switch can connect to multiple SSH clients. SSH Client functions to enable SSH connections between users and the Switch or UNIX host that support SSH Server. You can set up SSH channels for local connection. See Figure 95.

Currently the Switch that runs SSH server supports SSH version 1.5.

Figure 95 Setting up SSH channels in LAN



1: Switch running SSH server
2: PC running SSH client
3: Ethernet LAN

In the above figure, the VLAN for the Ethernet port must have been configured with VLAN interfaces and IP address.

The communication process between the server and client include these five stages: version negotiation stage, key negotiation stage, authentication stage, session request stage, interactive session stage.

- Version negotiation stage: The client sends TCP connection requirement to the server. When TCP connection is established, both ends begin to negotiate the SSH version. If they can work together in harmony, they enter the key algorithm negotiation stage. Otherwise the server clears the TCP connection.
- Key negotiation stage: Both ends negotiate key algorithm and compute session key. The server randomly generates its RSA key and sends the public key to the client. The client figures out session key based on the public key from the server and the random number generated locally. The client encrypts the random number with the public key from the server and sends the result back to the server. The server then decrypts the received data with the server private key to get the client random number. It then uses the same algorithm to work out the session key based on server public key and the returned random number. Then both ends get the same key without data transfer over the network, while the key is used at both ends for encryption and description.
- Authentication stage: The server authenticates the user at the client after obtaining a session key. The client sends its username to the server: If the username has been created and configured as no authentication, authentication stage is skipped for this user. Otherwise, the authentication process continues. SSH supports two authentication types: password authentication and RSA authentication. In the first type, the server compares the username and password received with those configured locally. The user is allowed to log on to the Switch if the usernames and passwords match exactly. RSA authentication works in this way: The RSA public key of the client user is configured at the server. The client first sends the member modules of its RSA public key to the server, which checks its validity. If it is valid, the server generates a random number, which is sent to the client after being encrypted with RSA public key. Both ends calculate authentication data based on the random number and session ID. The client sends the authentication data calculated back to the server, which compares it with its attention data obtained locally. If they match exactly, the user is allowed to access the Switch. Otherwise, authentication process fails.
- Session request stage: The client sends session request messages to the server which processes the request messages.
- Interactive session stage: Both ends exchange data till the session ends.

  Session packets are encrypted in transfer and the session key is generated randomly. Encryption is used in exchanging session key and RSA authentication achieves key exchange without transfer over the network. SSH can protect server-client data security. The authentication will also start even if the username received is not configured at the server, so malicious intruders cannot judge whether a username they key in exists or not. This is also a way to protect a username.

Configuring SSH Server

Basic configuration tasks refer to those required for successful connection from SSH client to SSH server, which advanced configuration tasks are those modifying SSH parameters.

Configuration tasks on the SSH server include:

- Setting system protocol and link maximum
- Configuring and deleting local RSA key pair
- Configuring authentication type
- Defining update interval of server key
- Defining SSH authentication timeout value
- Defining SSH authentication retry value
- Entering public key view and editing public key
- Associating public key with SSH user

Setting System Protocol

You must specify SSH protocol for the system before enabling SSH.

Perform the following configuration in User Inteface View.

Table 450 Setting System Protocols and Link Maximum

Operation	Command
Set system protocol and link maximum	**protocol inbound { all | ssh | telnet }**

By default, the system supports Telnet and SSH protocols.

CAUTION: *If SSH protocol is specified, to ensure a successful login, you must configure the AAA authentication 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 and Canceling Local RSA Key Pair

In executing this command, if you have configured RSA host key pair, the system gives an alarm after using this command and prompts that the existing one will be replaced. The server key pair is created dynamically by the SSH server. The maximum bit range of both key pairs is 2048 bits and the minimum is 512.

Please perform the following configurations in System View.

Table 451 Configuring and Canceling Local RSA Key Pair

Operation	Command
Configure local RSA key pair	**rsa local-key-pair create**
Cancel local RSA key pair	**rsa local-key-pair destroy**

CAUTION: *For a successful SSH login, you must configure and generate the local RSA key pairs. To generate local key pairs, you just need to execute the command once, with no further action required even after the system is rebooted.*

Configuring Authentication Type

For a new user, you must specify authentication type. Otherwise, they cannot access the Switch.

Perform the following configurations in System View.

Table 452 Configuring Authentication Type

Operation	Command
Configure authentication type	**ssh user** *username* **authentication-type { password | rsa | all }**
Remove authentication type setting	**undo ssh user** *username* **authentication-type**

If the configuration is RSA authentication type, then the RSA public key of the client user must be configured on the Switch, that is to perform the 7 and 8 serial number marked configuration.

By default, no authentication type is specified for a new user, so they cannot access the Switch.

Defining Update Interval of Server Key

Perform the following configurations in System View.

Table 453 Defining Update Interval of Server Key

Operation	Command
Define update interval of server key	**ssh server rekey-interval** *hours*
Restore the default update interval	**undo ssh server rekey-interval**

By default, the system does not update server key.

Defining SSH Authentication Timeout Value

Perform the following configurations in System View.

Table 454 Defining SSH Authentication Timeout Value

Operation	Command
Define SSH authentication timeout value	**ssh server timeout** *seconds*
Restore the default timeout value	**undo ssh server timeout**

By default, the timeout value for SSH authentication is 60 seconds.

Defining SSH Authentication Retry Value

Setting SSH authentication retry value can effectively prevent malicious registration attempt.

Perform the following configurations in System View.

Table 455 Defining SSH Authentication Retry Value

Operation	Command
Define SSH authentication retry value	**ssh server authentication-retries** *times*
Restore the default retry value	**undo ssh server authentication-retries**

By default, the retry value is 3.

Entering Public Key Edit View and Editing Public Key

You can enter the public key edit view and edit the client public key.

This operation is only available for the SSH users using RSA authentication. At the Switch, you configure the RSA public key of the client, while at the client, you specify the RSA private key which corresponds to the RSA public key.

This operation will fail if you configure password authentication for the SSH user.

Perform the following configurations in System View.

Table 456 Configuring Public Key

Operation	Command
Enter public key view	**`rsa peer-public-key`** *`key-name`*
Delete a designated public key	**`undo rsa peer-public-key`** *`key-name`*

When entering the public key edit view with the **`rsa peer-public-key`** command, you can begin editing the public key with the **`public-key-code begin`** command. You can key in a blank space between characters, since the system can remove the blank space automatically. But the public key should be composed of hexadecimal characters. Terminate public key editing and save the result with the **`public-key-code end`** command. Validity check comes before saving: the public key editing fails if the key contains invalid characters.

Perform the following configurations in the Public Key View.

Figure 96 Starting/Terminating Public Key Editing

Operation	Command
Enter public key edit view	**`public-key-code begin`**
Terminate public key edit view	**`public-key-code end`**
Quit public key view	**`peer-public-key end`**

Associating Public Key with SSH User

Please perform the following configurations in System View.

Figure 97 Associating Public Key with SSH User

Operation	Command
Associate existing public with an SSH user	**`ssh user`** *`username`* **`assign rsa-key`** *`keyname`*
Remove the association	**`undo ssh user`** *`username`* **`assign rsa-key`**

Configuring SSH Client

There are several types of SSH client software, such as PuTTY and FreeBSD. You should first configure the client's connection with the server. The basic configuration tasks on the client include:

- Specifying server IP address.
- Selecting SSH protocol. The client supports the remote connection protocols link Telnet, Rlogin and SSH. To set up SSH connection, you must select SSH protocol.
- Choosing SSH version. The Switch currently supports SSH Server 1.5, so you have to choose 1.5 or an earlier version.

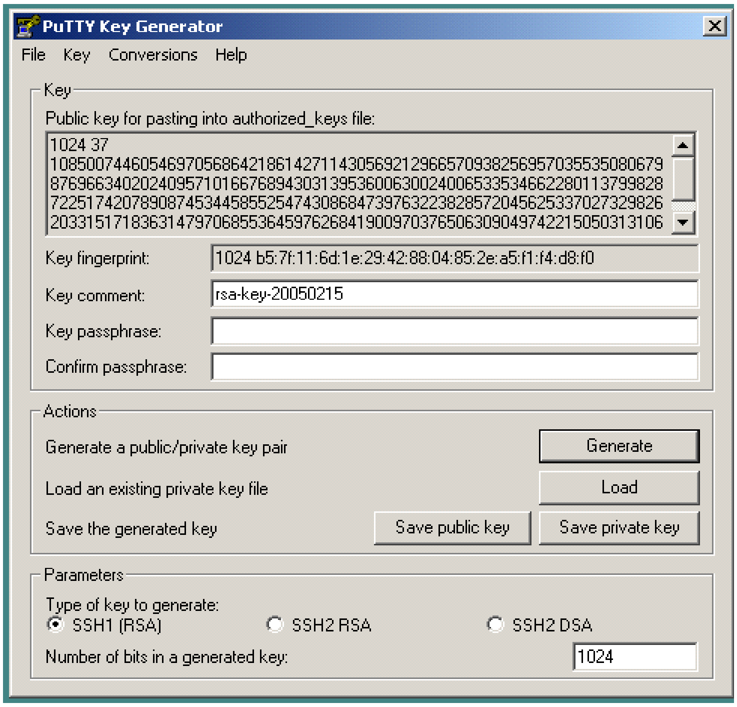
- Specifying RSA private key file. If you specify RSA authentication for the SSH user, you must specify RSA private key file. The RSA key, which includes the public key and private key, are generated by the client software. The former is configured in the server (Switch) and the latter is in the client.

The following description takes the PuTTY as an example.

Generating the Key

Start the Puttygen program, choose SSH1(RSA), then click on the Generate button and follow the instructions

Figure 98 PuTTy key generator



PuTTY Key Generator

Public key for pasting into authorized_keys file:

```
1024 37
10850074460546970568642186142711430569212966570938256957035535080679
87696634020240957101667689430313953600630024006533534662280113799828
72251742078908745344585525474308684739763223828572045625337027329826
20331517183631479706855364597626841900970376506309049742215050313106
```

Key fingerprint: 1024 b5:7f:11:6d:1e:29:42:88:04:85:2e:a5:f1:f4:d8:f0

Key comment: rsa-key-20050215

Key passphrase:

Confirm passphrase:

Type of key to generate: ● SSH1 (RSA) ○ SSH2 RSA ○ SSH2 DSA

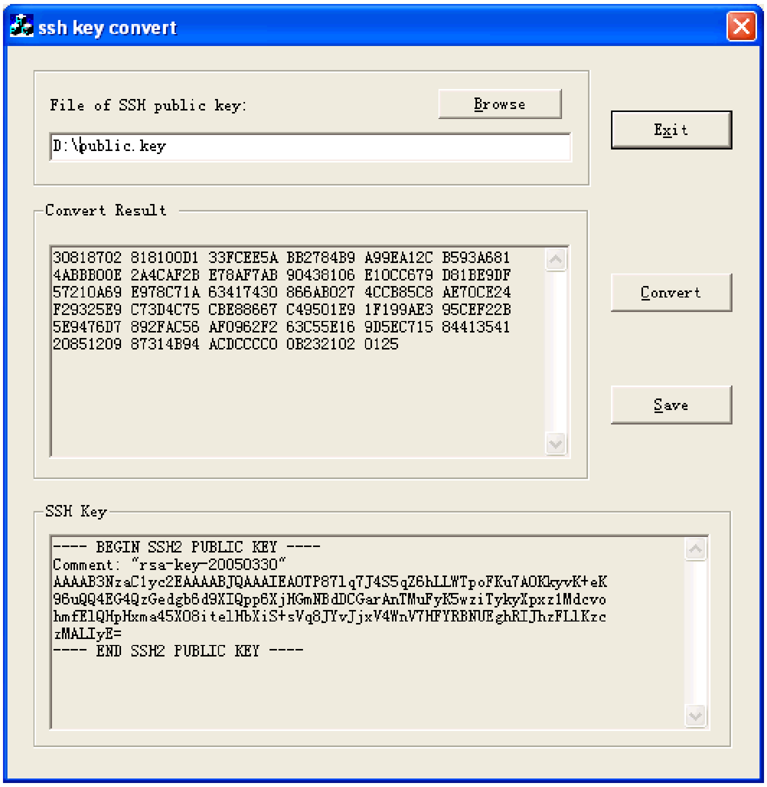
Number of bits in a generated key: 1024

When the generation process has finished, save the generated public and private keys to files using the Save buttons.

Run the sshkey program. This converts SSH public key to the format required by the switch.

Open the public key file generated by puttygen, then click the Convert button

Figure 99 SSH key convert.



File of SSH public key:
D:\public.key

Convert Result

```
30818702 818100D1 33FCEE5A BB2784B9 A99EA12C B593A681
4ABBB00E 2A4CAF2B E78AF7AB 90438106 E10CC679 D81BE9DF
57210A69 E978C71A 63417430 866AB027 4CCB85C8 AE70CE24
F29325E9 C73D4C75 CBE88667 C49501E9 1F199AE3 95CEF22B
5E9476D7 892FAC56 AF0962F2 63C55E16 9D5EC715 84413541
20851209 87314B94 ACDCCCC0 0B232102 0125
```

SSH Key

```
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "rsa-key-20050330"
AAAAB3NzaC1yc2EAAAABJQAAAIEAOTP87lq7J4S5qZ6hLLWTpoFKu7AOKkyvK+eK
96uQQ4EG4QzGedgb6d9XIQpp6XjHGmNBdDCGarAnTMuFyK5wziTykyXpxz1Mdcvo
hmfElQHpHxma45XO8itelHbXiS+sVq8JYvJjxV4WnV7HFYRBNUEghRIJhzFL1Krc
zMALIyE=
---- END SSH2 PUBLIC KEY ----
```

Use the save button to save this converted key to a file.

Open the public key file in notepad and the following lines of text before the existing text:

`rsa peer-public-key` *`mykey`*
`public-key-code begin`

where *`myKey`* is a name used to identify the key within the switch, you may choose any name for this.

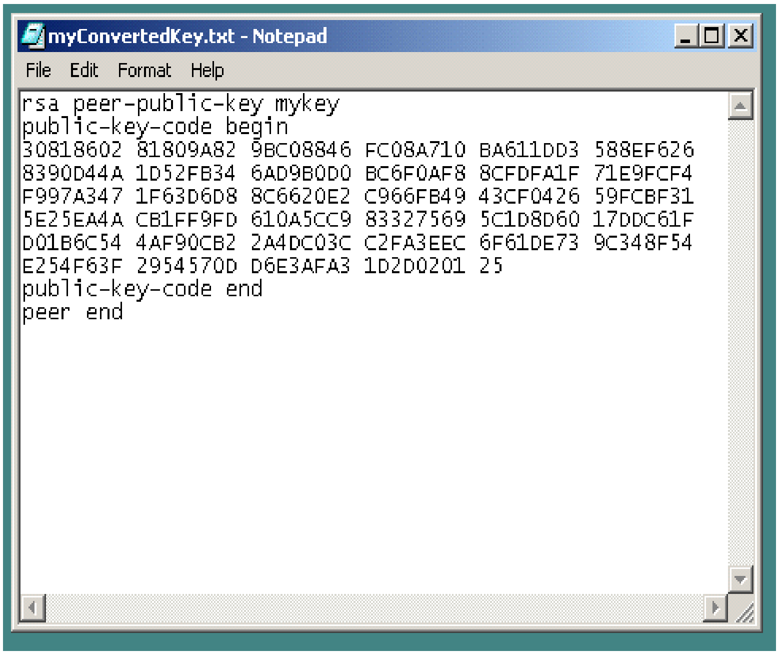
Then add the following after the existing text:

```
public-key-code end
peer end
```

Also remove any blank lines from the file.

The file should look like this:

Figure 100 Text file of myKey



```
rsa peer-public-key mykey
public-key-code begin
30818602 81809A82 9BC08846 FC08A710 BA611DD3 588EF626
8390D44A 1D52FB34 6AD9B0D0 BC6F0AF8 8CFDFA1F 71E9FCF4
F997A347 1F63D6D8 8C6620E2 C966FB49 43CF0426 59FCBF31
5E25EA4A CB1FF9FD 610A5CC9 83327569 5C1D8D60 17DDC61F
D01B6C54 4AF90CB2 2A4DC03C C2FA3EEC 6F61DE73 9C348F54
E254F63F 2954570D D6E3AFA3 1D2D0201 25
public-key-code end
peer end
```

Save this to a file ending with a ".bat" extension e.g "keys.bat".

This file can be transferred to the switch using FTP or TFTP.

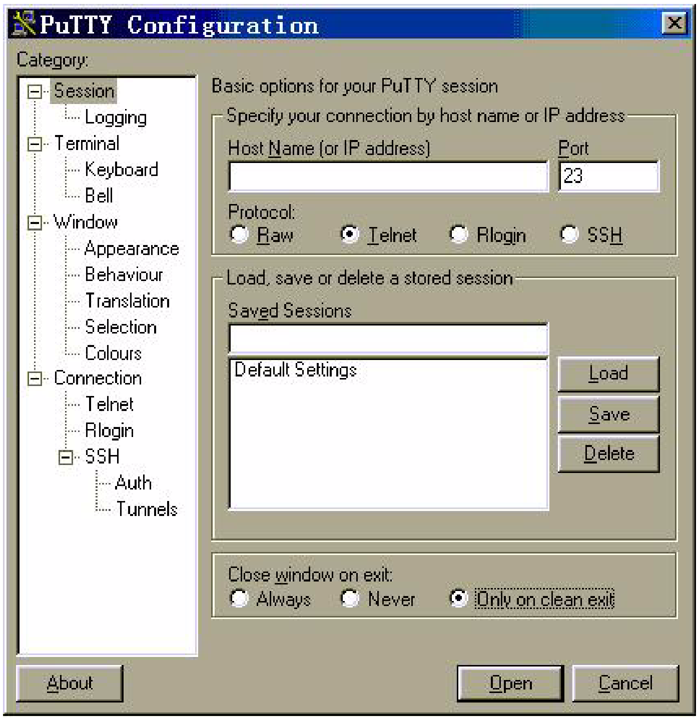
The key is installed using the execute command in the System view

```
[SW5500]execute keys.bat
```

Specifying Server IP Address

Start PuTTY program and the client configuration interface pops up.

Figure 101 SSH Client Configuration Interface (1)



PuTTY Configuration

Basic options for your PuTTY session

Specify your connection by host name or IP address

Host Name (or IP address)

Port: 23

Protocol: ○ Raw ● Telnet ○ Rlogin ○ SSH

Load, save or delete a stored session

Saved Sessions

Default Settings

Close window on exit: ○ Always ○ Never ● Only on clean exit

In the Host Name (or IP address) text box key in the IP address of the Switch, for example, 10.110.28.10. You can also input the IP address of an interface in UP state, but its route to SSH client PC must be reachable.

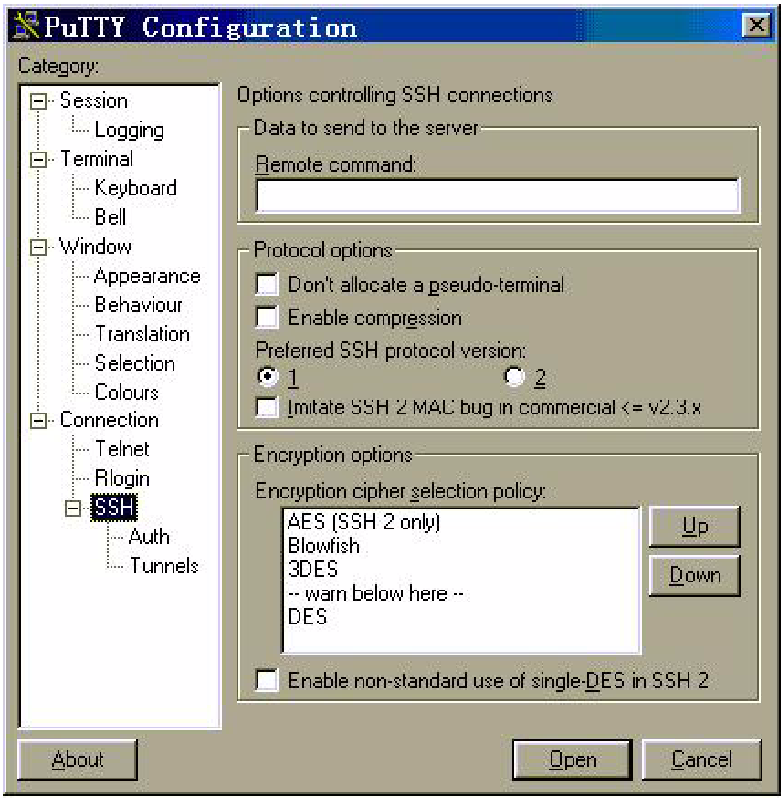
Selecting SSH Protocol

Select SSH for the Protocol item.

Choosing SSH Version

Click the left menu *[Category/Connection/SSH]* to enter the interface shown in following figure:

Figure 102 SSH Client Configuration Interface (2)



PuTTY Configuration

Category:

- Session
  - Logging
- Terminal
  - Keyboard
  - Bell
- Window
  - Appearance
  - Behaviour
  - Translation
  - Selection
  - Colours
- Connection
  - Telnet
  - Rlogin
  - SSH
    - Auth
    - Tunnels

Options controlling SSH connections

Data to send to the server

Remote command:

Protocol options

□ Don't allocate a pseudo-terminal

□ Enable compression

Preferred SSH protocol version:

● 1 ○ 2

□ Imitate SSH 2 MAC bug in commercial <= v2.3.x

Encryption options

Encryption cipher selection policy:

AES (SSH 2 only)
Blowfish
3DES
-- warn below here --
DES

□ Enable non-standard use of single-DES in SSH 2

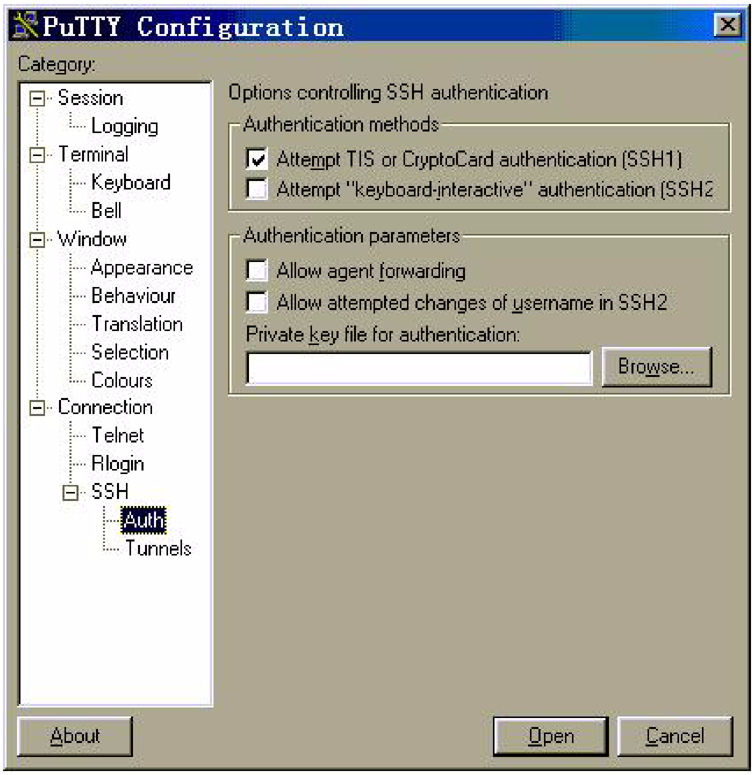
You can select 1, as shown in the above figure.

Specifying RSA Private Key File

If you want to enable RSA authentication, you must specify RSA private key file, which is not required for password authentication.

Click *[SSH/Auth]* to enter the interface as shown in the following figure:

Figure 103 SSH client configuration interface (3)



Options controlling SSH authentication

Authentication methods

☑ Attempt TIS or CryptoCard authentication (SSH1)

□ Attempt "keyboard-interactive" authentication (SSH2

Authentication parameters

□ Allow agent forwarding

□ Allow attempted changes of username in SSH2

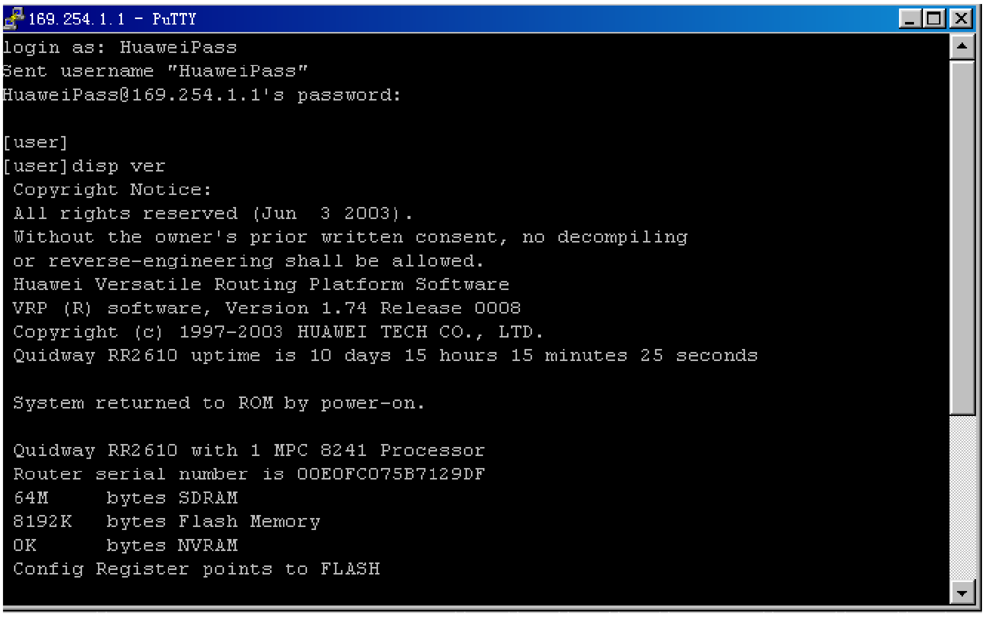
Private key file for authentication:

Click *Browse* to enter the File Select interface. Choose a desired file and click *OK*.

Opening SSH Connection

Click *Open* to enter SSH client interface. If it runs normally, you are prompted to enter username and password. See the following figure.

Figure 104 SSH client interface



```
login as: HuaweiPass
Sent username "HuaweiPass"
HuaweiPass@169.254.1.1's password:

[user]
[user]disp ver
 Copyright Notice:
 All rights reserved (Jun  3 2003).
 Without the owner's prior written consent, no decompiling
 or reverse-engineering shall be allowed.
 Huawei Versatile Routing Platform Software
 VRP (R) software, Version 1.74 Release 0008
 Copyright (c) 1997-2003 HUAWEI TECH CO., LTD.
 Quidway RR2610 uptime is 10 days 15 hours 15 minutes 25 seconds

 System returned to ROM by power-on.

 Quidway RR2610 with 1 MPC 8241 Processor
 Router serial number is 00E0FC075B7129DF
 64M     bytes SDRAM
 8192K   bytes Flash Memory
 0K      bytes NVRAM
 Config Register points to FLASH
```

Key in the correct username and password and log into SSH connection.

Log out of SSH connection with the **logout** command.

Displaying and Debugging SSH

Run the **display** command in any view to view the running of SSH and further to check configuration result.

Run the **debugging** command to debug the SSH.

Perform the following configurations in any view.

Table 457 Display SSH Information

Operation	Command
Display host and server public keys	**display rsa local-key-pair public**
Display client RSA public key	**display rsa peer-public-key [brief | name** *keyname* **]**
Display SSH state information and session	**display ssh server { status | session }**
Display SSH user information	**display ssh user-information [** *username* **]**
Enable SSH debugging	**debugging ssh server { VTY** *index* | **all }**
Disable SSH debugging	**undo debugging ssh server { VTY** *index* | **all }**

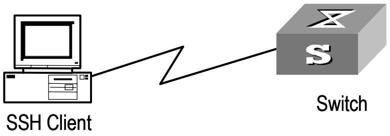
SSH Configuration Example

Networking Requirements

As shown in Figure 105, configure a local connection from the SSH Client to the Switch. The client uses SSH protocol to access the Switch.

Networking Diagram

Figure 105 Networking for SSH Local Configuration



Configuration Procedure

1 You should run this command before any other configuration:

```
[SW5500]rsa local-key-pair create
```

If you have configured local key pair in advance, this operation is unnecessary.

2 For password authentication mode

```
[SW5500]user-interface vty 0 4
[SW5500-ui-vty0-4]authentication-mode scheme
[SW5500-ui-vty0-4]protocol inbound ssh
[SW5500]local-user client001
[SW5500-luser-client001]password simple 3com
[SW5500-luser-client001]service-type ssh
[SW5500]ssh user client001 authentication-type password
```

Select the default values for SSH authentication timeout value, retry value and update interval of server key. Then run SSH1.5 client program on the PC which is connected to the Switch and access the Switch using username “client001” and password “3com”.

3 For RSA authentication mode:

Create local user client002

```
[SW5500]local-user client002
[SW5500-luser-client002]service-type ssh
```

4 Specify AAA authentication on the user interface.

```
[SW5500]user-interface vty 0 4
[SW5500-ui-vty0-4]authentication-mode scheme
```

5 Select SSH protocol on the Switch.

```
[SW5500-ui-vty0-4]protocol inbound ssh
```

6 Specify RSA authentication on the Switch.

```
[SW5500]ssh user client002 authentication-type RSA
```

7 Configure RSA key pair on the Switch.

If you followed the procedure for generating and executing a ".bat" file containing keys then you need not perfom this step.

```
[SW5500]rsa peer-public-key switch002
[SW5500-rsa-public]public-key-code begin
[SW5500-key-code]308186028180739A291ABDA704F5D93DC8FDF84C427463
[SW5500-key-code]1991C164B0DF178C55FA833591C7D47D5381D09CE82913
[SW5500-key-code]D7EDF9C08511D83CA4ED2B30B809808EB0D1F52D045DE4
[SW5500-key-code]0861B74A0E135523CCD74CAC61F8E58C452B2F3F2DA0DC
[SW5500-key-code]C48E3306367FE187BDD944018B3B69F3CBB0A573202C16
[SW5500-key-code]BB2FC1ACF3EC8F828D55A36F1CDDC4BB45504F020125
[SW5500-key-code]public-key-code end
[SW5500-rsa-public]peer-public-key end
[SW5500]ssh user client002 assign rsa-key key002
```

You need to specify RSA private key which corresponds to the public key for the SSH user client002.

Run SSH1.5 client program on the PC that has been configured with private RSA private key and you can set up SSH connection.

A PASSWORD RECOVERY PROCESS

Introduction

The Switch 5500G-EI has two separate password systems:

- Passwords which are used by the Web User Inteface and the CLI and are stored in the 3comoscfg.cfg file.

  For more information on this, refer to the Getting Started Guide which 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:

```
<5500>undo startup bootrom-access enable
```

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 inactivel

The following commands enable and display the current bootrom access settings respectively:

```
<5500>startup bootrom-access enable
<5500>display startup
```

Bootrom Interface

During the intitial 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 458 displays the configuration files:

Table 458 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 5500G-EI.

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 5500G-EI deployed.

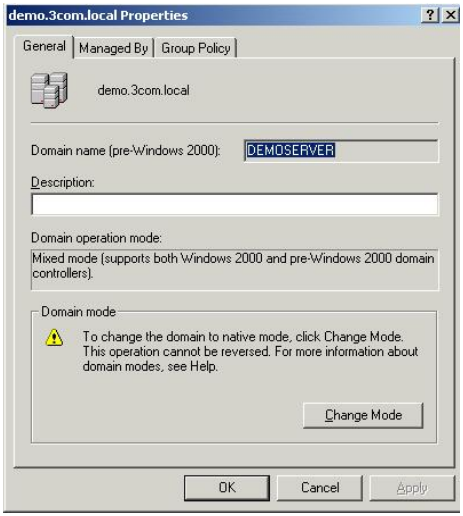
The following steps are required to setup a RADIUS server using the Microsoft IAS RADIUS application. You will need to use the Install CD for Microsoft Windows 2000 Server to complete the process.

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*.



demo.3com.local Properties

demo.3com.local

Domain name (pre-Windows 2000): DEMOSERVER

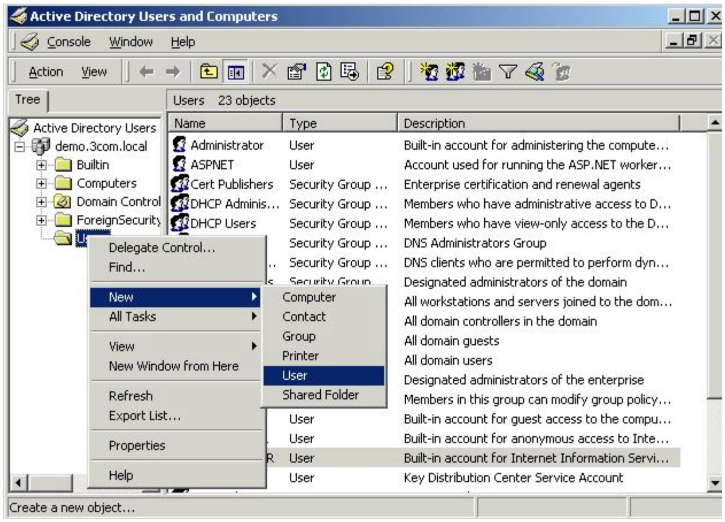
Description:

Domain operation mode:
Mixed mode (supports both Windows 2000 and pre-Windows 2000 domain controllers).

Domain mode

To change the domain to native mode, click Change Mode. This operation cannot be reversed. For more information about domain modes, see Help.

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.



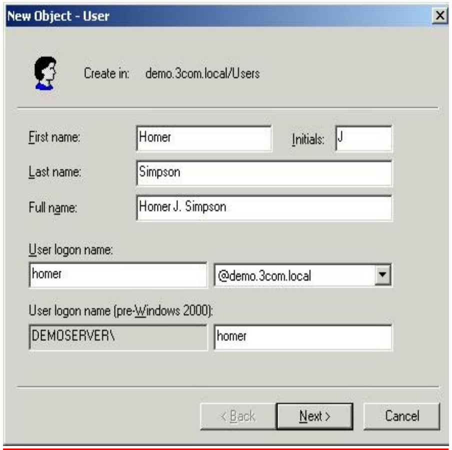
Active Directory Users and Computers

Users 23 objects

Name	Type	Description
Administrator	User	Built-in account for administering the compute…
ASPNET	User	Account used for running the ASP.NET worker…
Cert Publishers	Security Group …	Enterprise certification and renewal agents
DHCP Adminis…	Security Group …	Members who have administrative access to D…
DHCP Users	Security Group …	Members who have view-only access to the D…
	Security Group …	DNS Administrators Group
..	Security Group …	DNS clients who are permitted to perform dyn…
s	Security Group	Designated administrators of the domain
		All workstations and servers joined to the dom…
		All domain controllers in the domain
		All domain guests
		All domain users
		Designated administrators of the enterprise
		Members in this group can modify group policy…
	User	Built-in account for guest access to the compu…
	User	Built-in account for anonymous access to Inte…
R	User	Built-in account for Internet Information Servi…
	User	Key Distribution Center Service Account

Create a new object…

d Follow the wizard to create a user, enter the required information at each stage



New Object - User

Create in: demo.3com.local/Users

First name: Homer Initials: J

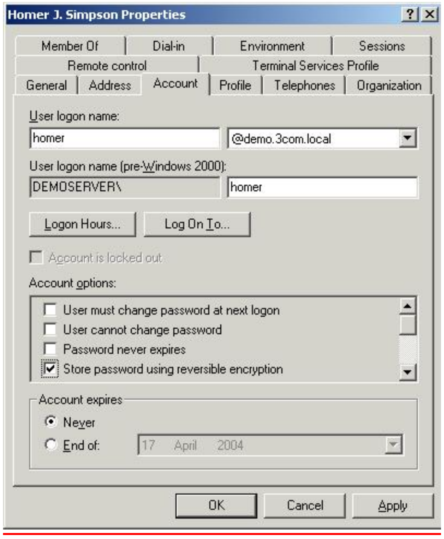
Last name: Simpson

Full name: Homer J. Simpson

User logon name: homer @demo.3com.local

User logon name (pre-Windows 2000): DEMOSERVER\ homer

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 labelled *Store password using reversible encryption*.



User logon name: homer @demo.3com.local

User logon name (pre-Windows 2000): DEMOSERVER\ homer

□ Account is locked out

Account options:

- □ User must change password at next logon
- □ User cannot change password
- □ Password never expires
- ☑ Store password using reversible encryption

Account expires

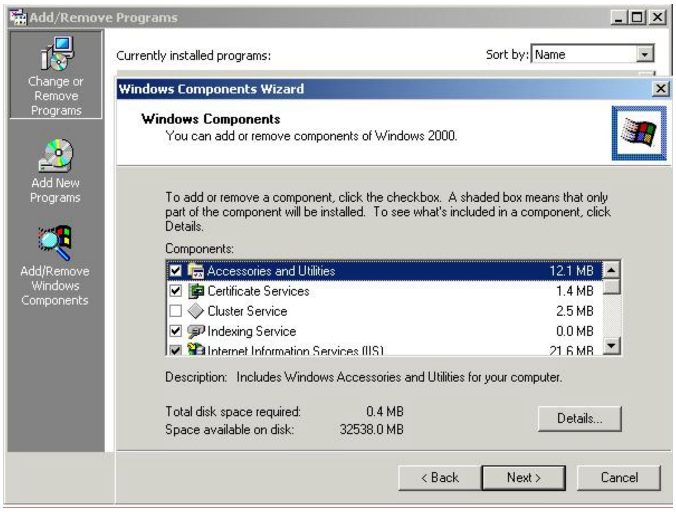
- ● Never
- ○ End of: 17 April 2004

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.


Add/Remove Programs
Change or Remove Programs
Add New Programs
Add/Remove Windows Components
Currently installed programs:
Sort by: Name
Windows Components Wizard
Details...
< Back
Next >
Cancel

Windows Components
You can add or remove components of Windows 2000.

To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Components:

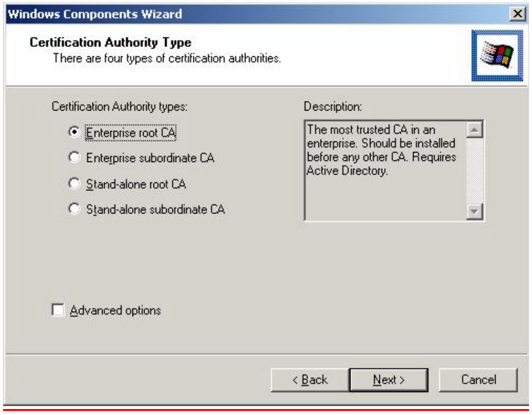
☑	Accessories and Utilities	12.1 MB
☑	Certificate Services	1.4 MB
□	Cluster Service	2.5 MB
☑	Indexing Service	0.0 MB
☑	Internet Information Services (IIS)	21.6 MB

Description: Includes Windows Accessories and Utilities for your computer.

Total disk space required: 0.4 MB
Space available on disk: 32538.0 MB

b Select *Next* and continue through the wizard.

In the *Certificate Authority Type* window select *Enterprise root CA*



Windows Components Wizard

Certification Authority Type
There are four types of certification authorities.

Certification Authority types:

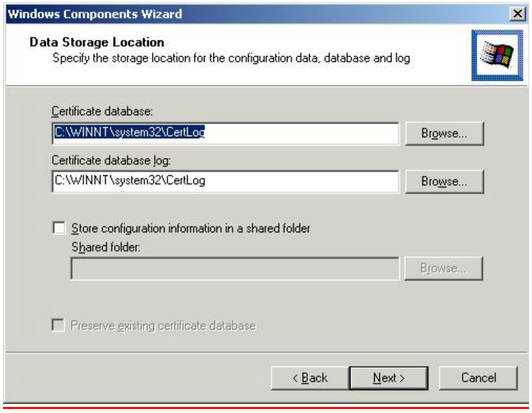
- ● Enterprise root CA
- ○ Enterprise subordinate CA
- ○ Stand-alone root CA
- ○ Stand-alone subordinate CA

Description:
The most trusted CA in an enterprise. Should be installed before any other CA. Requires Active Directory.

□ Advanced options

Enter information to identify the Certificate Authority on the *CA Identifying Information* window.

Enter the storage location on the *Data Storage Location* window.



Windows Components Wizard

Data Storage Location
Specify the storage location for the configuration data, database and log

Certificate database:
C:\WINNT\system32\CertLog

Certificate database log:
C:\WINNT\system32\CertLog

□ Store configuration information in a shared folder

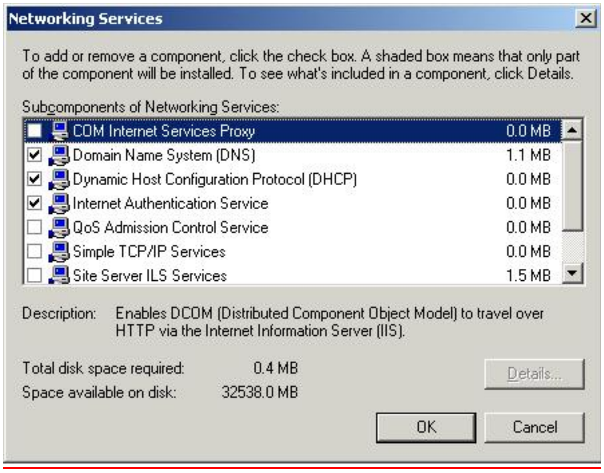
Shared folder:

□ Preserve existing certificate database

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.



Networking Services

To add or remove a component, click the check box. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Subcomponents of Networking Services:

□	COM Internet Services Proxy	0.0 MB
☑	Domain Name System (DNS)	1.1 MB
☑	Dynamic Host Configuration Protocol (DHCP)	0.0 MB
☑	Internet Authentication Service	0.0 MB
□	QoS Admission Control Service	0.0 MB
□	Simple TCP/IP Services	0.0 MB
□	Site Server ILS Services	1.5 MB

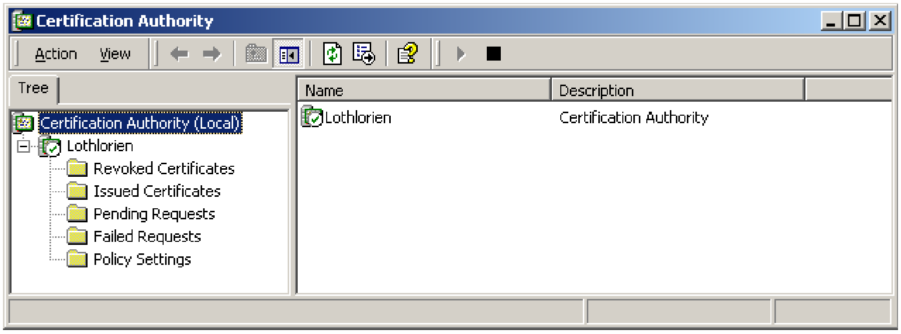
Description: Enables DCOM (Distributed Component Object Model) to travel over HTTP via the Internet Information Server (IIS).

Total disk space required: 0.4 MB
Space available on disk: 32538.0 MB

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.

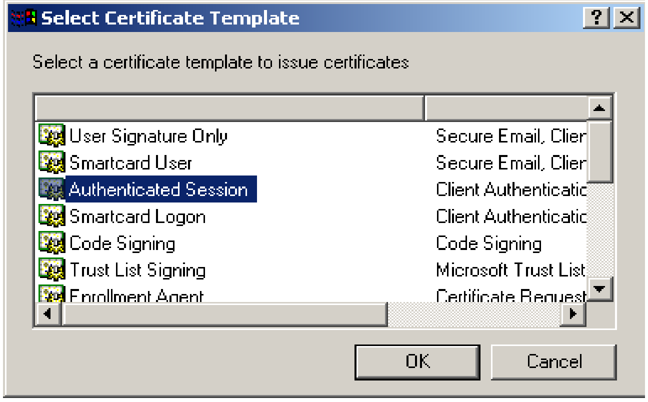


Certification Authority (Local)
Lothlorien
Revoked Certificates
Issued Certificates
Pending Requests
Failed Requests
Policy Settings

Name	Description
Lothlorien	Certification Authority

b Select *New > Certificate to Issue*

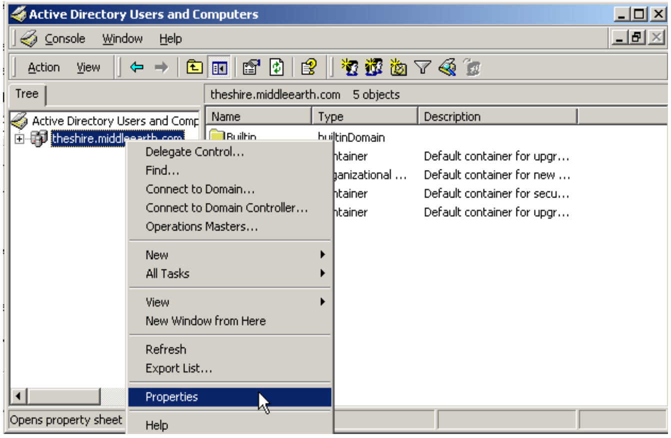
c Select *Authenticated Session* and select *OK*.



Select a certificate template to issue certificates

User Signature Only	Secure Email, Clier
Smartcard User	Secure Email, Clier
Authenticated Session	Client Authenticatic
Smartcard Logon	Client Authenticatic
Code Signing	Code Signing
Trust List Signing	Microsoft Trust List
Enrollment Agent	Certificate Request

d Go to *Programs > Administrative Tools > Active Directory Users and Computers* and right-click your active directory domain. Select *Properties*



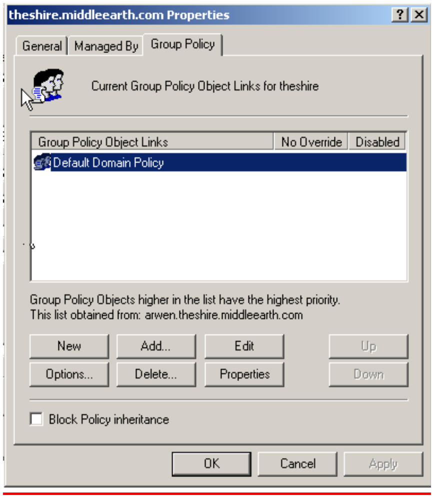
Active Directory Users and Comp
theshire.middleearth.com

theshire.middleearth.com 5 objects

Name	Type	Description
Builtin	builtinDomain	
	ntainer	Default container for upgr...
	ganizational ...	Default container for new ...
	ntainer	Default container for secu...
	ntainer	Default container for upgr...

Opens property sheet

e Select the *Group Policy* tab, and ensure that the *Default Domain Policy* is highlighted. Click *Edit* to launch the Group Policy editor.



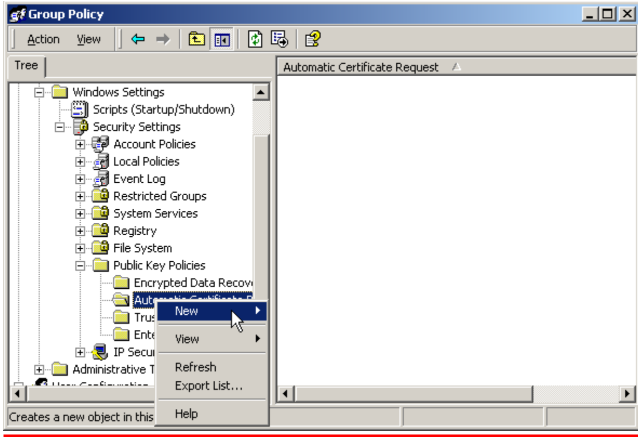
Current Group Policy Object Links for theshire

Group Policy Object Links	No Override	Disabled
Default Domain Policy		

Group Policy Objects higher in the list have the highest priority.
This list obtained from: arwen.theshire.middleearth.com

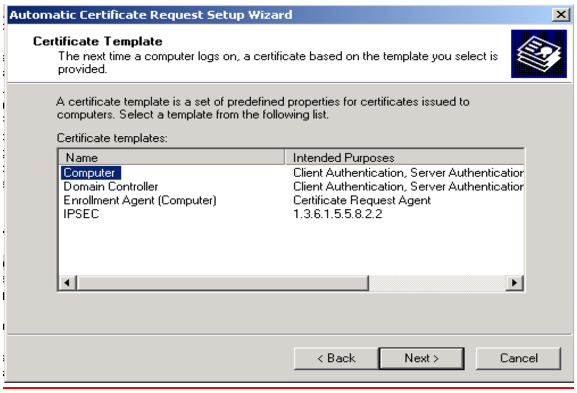
☐ Block Policy inheritance

f Go to *Computer Configuration* > *Windows Settings* > *Security Settings* > *Public Key Policies,* and right-click *Automatic Certificate Request Settings*. Select *New* > *Automatic Certificate Request.*



Creates a new object in this

g The Certificate Request Wizard will start. Select *Next* > *Computer certificate template* and click *Next*.



Certificate Template

The next time a computer logs on, a certificate based on the template you select is provided.

A certificate template is a set of predefined properties for certificates issued to computers. Select a template from the following list.

Certificate templates:

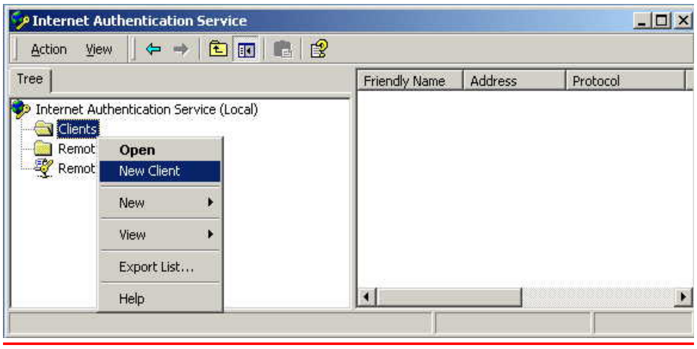
Name	Intended Purposes
Computer	Client Authentication, Server Authenticatior
Domain Controller	Client Authentication, Server Authenticatior
Enrollment Agent (Computer)	Certificate Request Agent
IPSEC	1.3.6.1.5.5.8.2.2

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

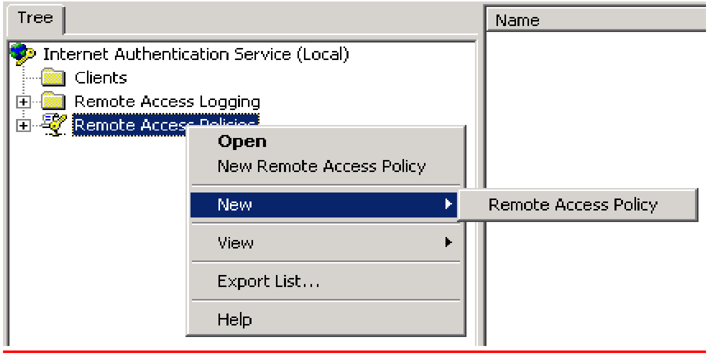
a Go to *Programs* > *Administrative Tools* > *Internet Authentication Service*, right-click *Clients*, and *Select New Client*.



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.*

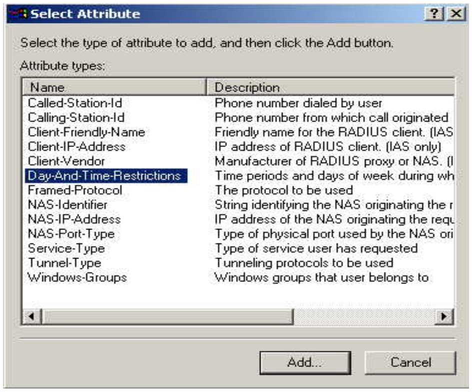


e Give the policy a name, for example EAP-TLS, and select *Next*.

f Click *Add...*

g Set the conditions for using the policy to access the network.

Select *Day-And-Time-Restrictions,* and click *Add...*



Select the type of attribute to add, and then click the Add button.

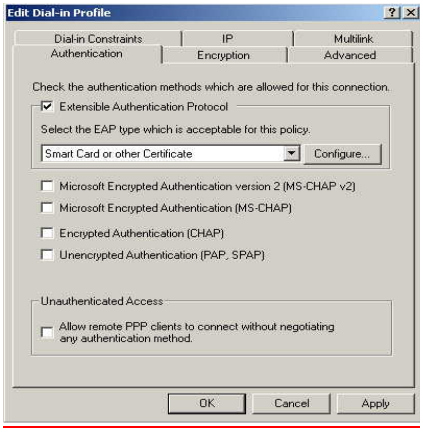
Attribute types:

Name	Description
Called-Station-Id	Phone number dialed by user
Calling-Station-Id	Phone number from which call originated
Client-Friendly-Name	Friendly name for the RADIUS client. (IAS
Client-IP-Address	IP address of RADIUS client. (IAS only)
Client-Vendor	Manufacturer of RADIUS proxy or NAS. (I
Day-And-Time-Restrictions	Time periods and days of week during wh
Framed-Protocol	The protocol to be used
NAS-Identifier	String identifying the NAS originating the r
NAS-IP-Address	IP address of the NAS originating the requ
NAS-Port-Type	Type of physical port used by the NAS ori
Service-Type	Type of service user has requested
Tunnel-Type	Tunneling protocols to be used
Windows-Groups	Windows groups that user belongs to

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*.


Edit Dial-in Profile

Check the authentication methods which are allowed for this connection.

☑ Extensible Authentication Protocol

Select the EAP type which is acceptable for this policy.

Smart Card or other Certificate

☐ Microsoft Encrypted Authentication version 2 (MS-CHAP v2)

☐ Microsoft Encrypted Authentication (MS-CHAP)

☐ Encrypted Authentication (CHAP)

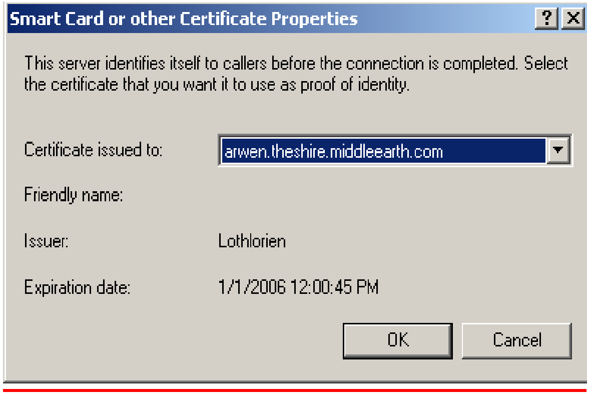
☐ Unencrypted Authentication (PAP, SPAP)

Unauthenticated Access

☐ Allow remote PPP clients to connect without negotiating any authentication method.

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.


Smart Card or other Certificate Properties

This server identifies itself to callers before the connection is completed. Select the certificate that you want it to use as proof of identity.

Certificate issued to: arwen.theshire.middleearth.com

Friendly name:

Issuer: Lothlorien

Expiration date: 1/1/2006 12:00:45 PM

Windows may ask if you wish to view the Help topic for EAP. Select No if you want to continue with the installation.

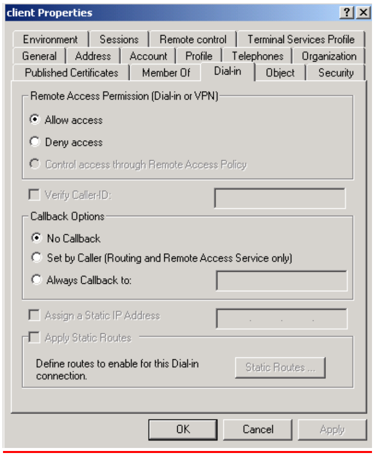
l Click *Finish*.

IFor 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*.



client Properties

? ✕
Environment | Sessions | Remote control | Terminal Services Profile
General | Address | Account | Profile | Telephones | Organization
Published Certificates | Member Of | Dial-in | Object | Security

Remote Access Permission (Dial-in or VPN)

● Allow access

○ Deny access

○ Control access through Remote Access Policy

□ Verify Caller-ID:

Callback Options

● No Callback

○ Set by Caller (Routing and Remote Access Service only)

○ Always Callback to:

□ Assign a Static IP Address

□ Apply Static Routes

Define routes to enable for this Dial-in connection.

Static Routes ...
OK
Cancel
Apply

c Click *OK* to confirm.

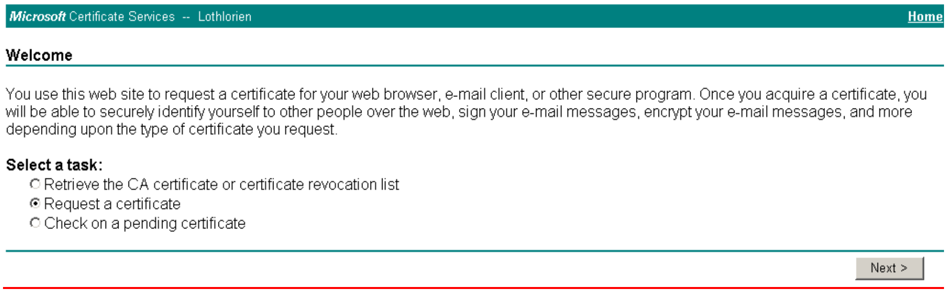
8 Configure the Switch 5500G-EI for RADUIS access and client authentication see Chapter 11 "802.1x Configuration".

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.

a On the RADIUS server, open *Internet Explorer* and enter the URL `http://localhost/certsrv`

b When you are prompted for a login, enter the user account name and password that you will be using for the certificate.

c Select *Request a certificate* and click *Next >*



Microsoft Certificate Services -- Lothlorien

Welcome

You use this web site to request a certificate for your web browser, e-mail client, or other secure program. Once you acquire a certificate, you will be able to securely identify yourself to other people over the web, sign your e-mail messages, encrypt your e-mail messages, and more depending upon the type of certificate you request.

Select a task:

○ Retrieve the CA certificate or certificate revocation list

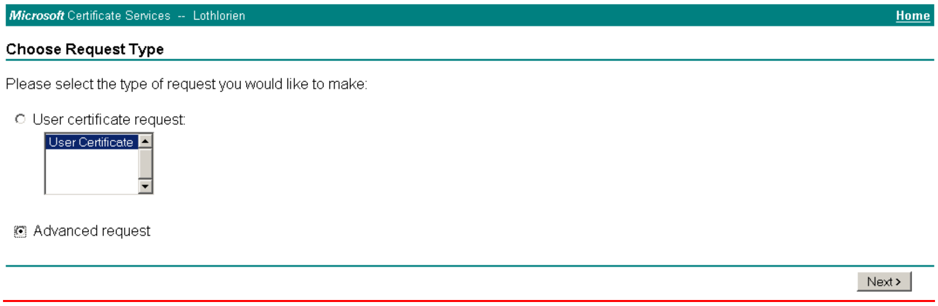
● Request a certificate

○ Check on a pending certificate

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 >*



Choose Request Type

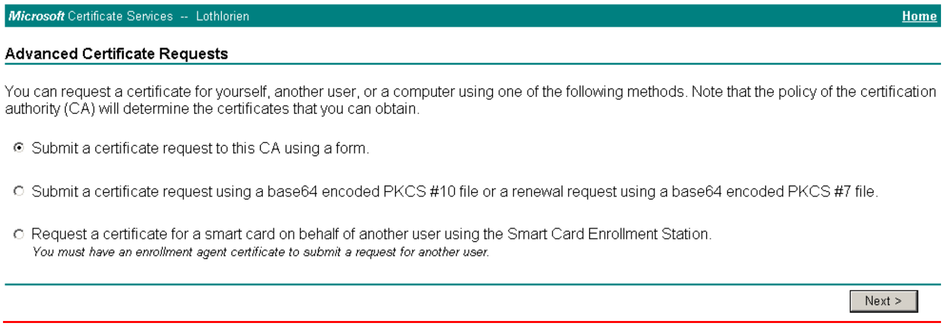
Please select the type of request you would like to make:

○ User certificate request:

User Certificate

● Advanced request

e Select the first option and click *Next >*



Advanced Certificate Requests

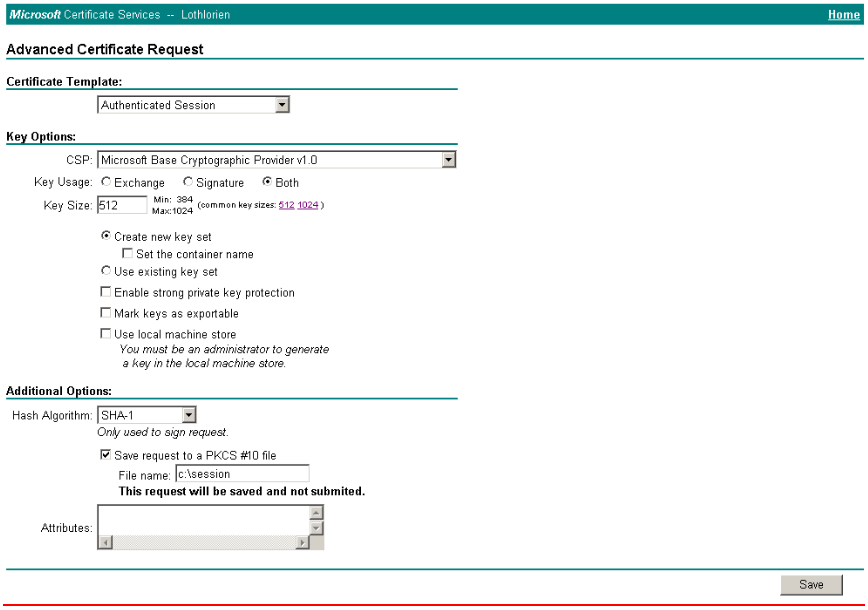
You can request a certificate for yourself, another user, or a computer using one of the following methods. Note that the policy of the certification authority (CA) will determine the certificates that you can obtain.

● Submit a certificate request to this CA using a form.

○ Submit a certificate request using a base64 encoded PKCS #10 file or a renewal request using a base64 encoded PKCS #7 file.

○ Request a certificate for a smart card on behalf of another user using the Smart Card Enrollment Station.
You must have an enrollment agent certificate to submit a request for another user.

f Either copy the settings from the screenshot below or choose different key options. Click *Save* to save the PKCS #10 file.



Advanced Certificate Request

Certificate Template:

Authenticated Session

Key Options:

CSP: Microsoft Base Cryptographic Provider v1.0

Key Usage: ○ Exchange ○ Signature ● Both

Key Size: 512 Min: 384 Max:1024 (common key sizes: 512 1024)

● Create new key set

□ Set the container name

○ Use existing key set

□ Enable strong private key protection

□ Mark keys as exportable

□ Use local machine store
You must be an administrator to generate a key in the local machine store.

Additional Options:

Hash Algorithm: SHA-1
Only used to sign request.

☑ Save request to a PKCS #10 file

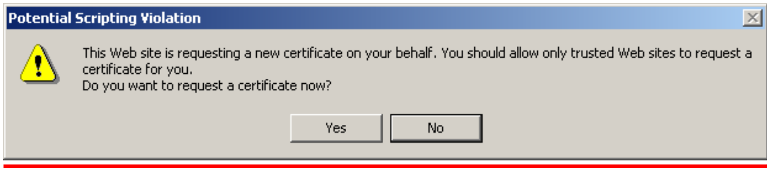
File name: c:\session

This request will be saved and not submited.

Attributes:

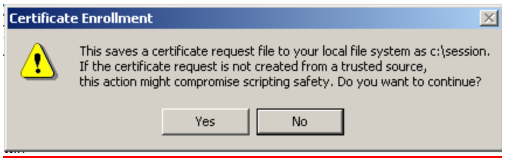
The PKCS #10 file is used to generate a certificate.

g You will receive this warning messages, select *Yes*



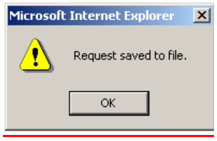
This Web site is requesting a new certificate on your behalf. You should allow only trusted Web sites to request a certificate for you.
Do you want to request a certificate now?

followed by this warning message, select *Yes*



This saves a certificate request file to your local file system as c:\session.
If the certificate request is not created from a trusted source,
this action might compromise scripting safety. Do you want to continue?

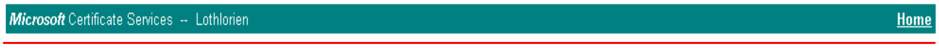
and then *OK*



Request saved to file.

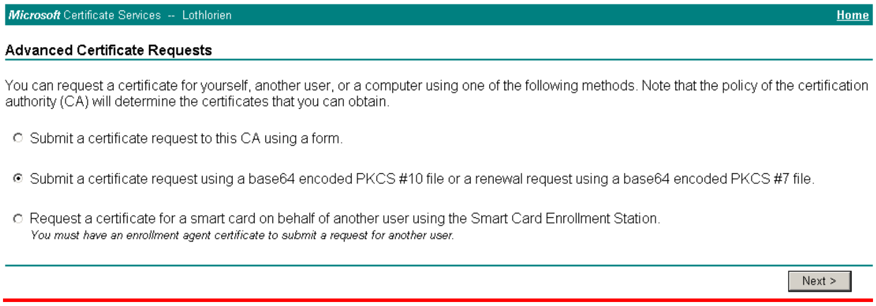
The PKCS #10 file is now saved to the local drive.

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* >



Advanced Certificate Requests

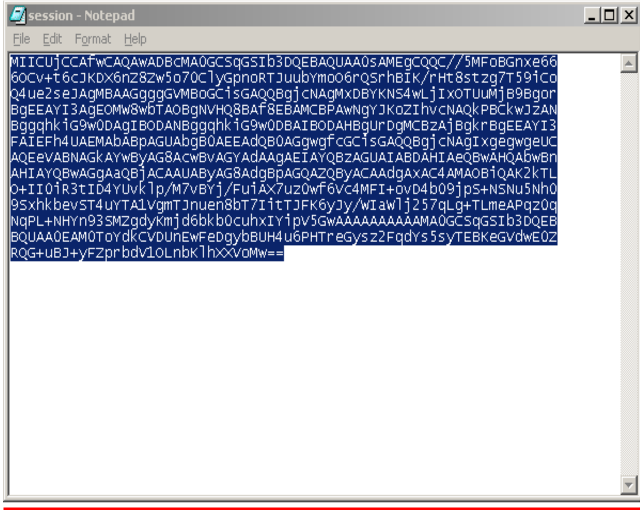
You can request a certificate for yourself, another user, or a computer using one of the following methods. Note that the policy of the certification authority (CA) will determine the certificates that you can obtain.

○ Submit a certificate request to this CA using a form.

● Submit a certificate request using a base64 encoded PKCS #10 file or a renewal request using a base64 encoded PKCS #7 file.

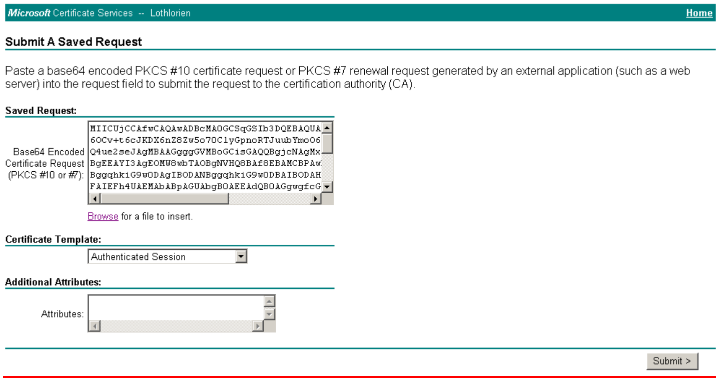
○ Request a certificate for a smart card on behalf of another user using the Smart Card Enrollment Station.
You must have an enrollment agent certificate to submit a request for another user.

k Open the previously saved PKCS #10 certificate file in Notepad, select all (Control + a) and copy (Control + c), as shown below



```
MIICUjCCAfwCAQAwADBcMA0GCSqGSIb3DQEBAQUAA0sAMEgCQQC//5MFoBGnxe66
6OCv+t6cJKDX6nZ8Zw5o70ClyGpnoRTJuubYmoO6rQSrhBIK/rHt8stzg7T59iCo
Q4ue2seJAgMBAAGgggGVMBoGCisGAQQBgjcNAgMxDBYKNS4wLjIxOTUuMjB9Bgor
BgEEAYI3AgEOMW8wbTAOBgNVHQ8BAf8EBAMCBPAwNgYJKoZIhvcNAQkPBCkwJzAN
BggqhkiG9w0DAgIBODANBggqhkiG9w0DBAIBODAHBgUrDgMCBzAjBgkrBgEEAYI3
FAIEFh4UAEMAbABpAGUAbgB0AEEAdQB0AGgwgfcGCisGAQQBgjcNAgIxgegwgeUC
AQEeVABNAGkAYwByAG8AcwBvAGYAdAAgAEIAYQBzAGUAIABDAHIAeQBwAHQAbwBn
AHIAYQBwAGgAaQBjACAAUAByAG8AdgBpAGQAZQByACAAdgAxAC4AMAOBiQAK2kTL
O+II0iR3tID4YUvklp/M7vBYj/FuiAX7uz0wf6Vc4MFI+ovD4b09jpS+NSNu5Nh0
9SxhkbevST4uYTA1VgmTJnuen8bT7IitTJFK6yJy/WIaWlj257qLg+TLmeAPqz0q
NqPL+NHYn93SMZgdyKmjd6bkb0cuhxIYipV5GwAAAAAAAAAAMA0GCSqGSIb3DQEB
BQUAA0EAM0ToYdkCVDUnEwFeDgybBUH4u6PHTreGysz2FqdYs5syTEBKeGVdwE0Z
RQG+uBJ+yFZprbdV1oLnbKlhXXVoMw==
```

l Paste the copied information into the *Saved Request* field as shown below. Select *Authenticated Session* from the *Certificate Template* selector and click *Submit >*



Microsoft Certificate Services -- Lothlorien **Home**

Submit A Saved Request

Paste a base64 encoded PKCS #10 certificate request or PKCS #7 renewal request generated by an external application (such as a web server) into the request field to submit the request to the certification authority (CA).

Saved Request:

Base64 Encoded Certificate Request (PKCS #10 or #7):

```
MIICUjCCAfwCAQAwADBcMA0GCSqGSIb3DQEBAQUA
6OCv+t6cJKDX6nZ8Zw5o7OClyGpnoRTJuubYmoO6
Q4ue2seJAgMBAAGgggGVMBoGCisGAQQBgjcNAgMx
BgEEAYI3AgEOMW8wbTAOBgNVHQ8BAf8EBAMCBPAw
BggqhkiG9w0DAgIBODANBggqhkiG9w0DBAIBODAH
FAIEFh4UAEMAbABpAGUAbgB0AEEAdQB0AGgwgfcG
```

Browse for a file to insert.

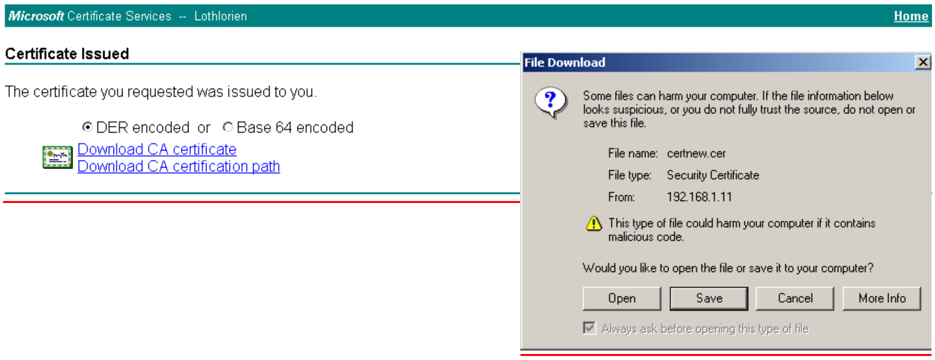
Certificate Template:

Authenticated Session

Additional Attributes:

Attributes:

m Download the certificate and certification path. Click on the *Download CA Certificate* hyperlink to save the certificate. Save the file as DER encoded..



Microsoft Certificate Services -- Lothlorien **Home**

Certificate Issued

The certificate you requested was issued to you.

● DER encoded or ○ Base 64 encoded

Download CA certificate

Download CA certification path

File Download

Some files can harm your computer. If the file information below looks suspicious, or you do not fully trust the source, do not open or save this file.

File name: certnew.cer

File type: Security Certificate

From: 192.168.1.11

This type of file could harm your computer if it contains malicious code.

Would you like to open the file or save it to your computer?

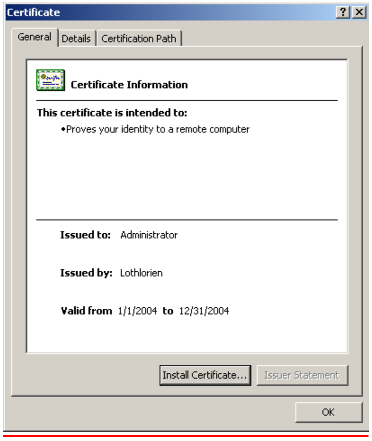
☑ Always ask before opening this type of file

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)



Certificate

Certificate Information

This certificate is intended to:

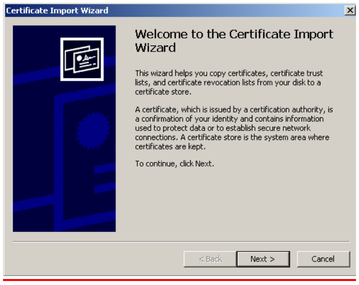
- Proves your identity to a remote computer

Issued to: Administrator

Issued by: Lothlorien

Valid from 1/1/2004 **to** 12/31/2004

o Click *Install Certificate* to launch the certificate import wizard



Certificate Import Wizard

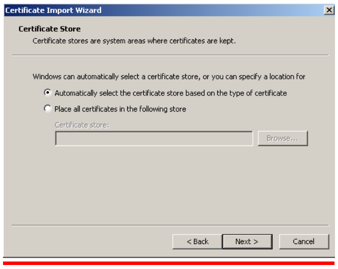
Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

p Leave the settings on the next screen as is, click *Next >* followed by *Finish* and *OK*. This will install the certificate,



Certificate Import Wizard

Certificate Store

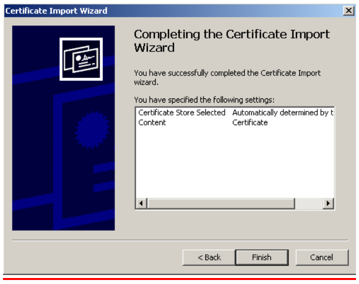
Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for

● Automatically select the certificate store based on the type of certificate

○ Place all certificates in the following store

Certificate store:



Certificate Import Wizard

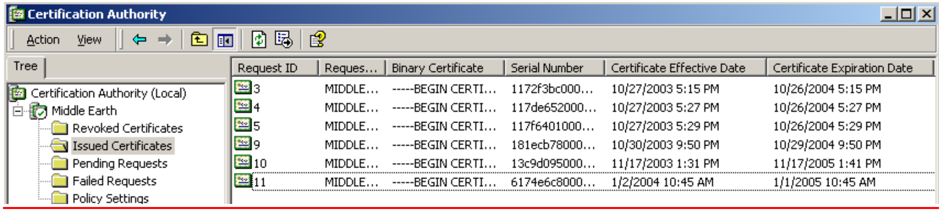
Completing the Certificate Import Wizard

You have successfully completed the Certificate Import wizard.

You have specified the following settings:

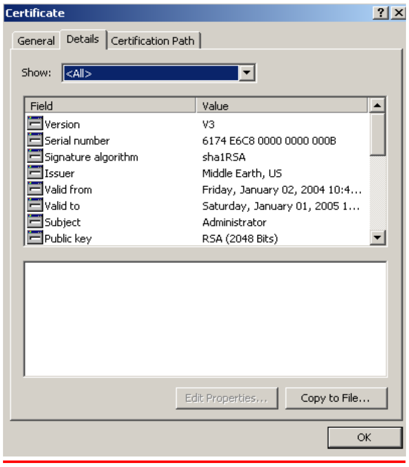
```
Certificate Store Selected   Automatically determined by t
Content                      Certificate
```

q Launch the *Certification Authority* management tool on the server and expand the *Issued Certificates* folder. You should see the newly created certificate.



Request ID	Reques...	Binary Certificate	Serial Number	Certificate Effective Date	Certificate Expiration Date
3	MIDDLE...	-----BEGIN CERTI...	1172f3bc000...	10/27/2003 5:15 PM	10/26/2004 5:15 PM
4	MIDDLE...	-----BEGIN CERTI...	117de652000...	10/27/2003 5:27 PM	10/26/2004 5:27 PM
5	MIDDLE...	-----BEGIN CERTI...	117f6401000...	10/27/2003 5:29 PM	10/26/2004 5:29 PM
9	MIDDLE...	-----BEGIN CERTI...	181ecb78000...	10/30/2003 9:50 PM	10/29/2004 9:50 PM
10	MIDDLE...	-----BEGIN CERTI...	13c9d095000...	11/17/2003 1:31 PM	11/17/2005 1:41 PM
11	MIDDLE...	-----BEGIN CERTI...	6174e6c8000...	1/2/2004 10:45 AM	1/1/2005 10:45 AM

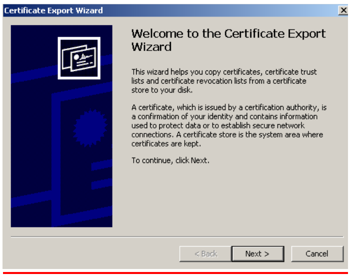
r Double-click the certificate that was generated by the client and select the *Details* tab



Show: <All>

Field	Value
Version	V3
Serial number	6174 E6C8 0000 0000 000B
Signature algorithm	sha1RSA
Issuer	Middle Earth, US
Valid from	Friday, January 02, 2004 10:4...
Valid to	Saturday, January 01, 2005 1...
Subject	Administrator
Public key	RSA (2048 Bits)

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.



Certificate Export Wizard

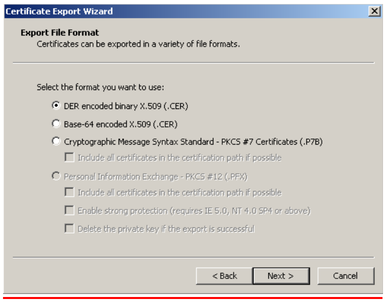
Welcome to the Certificate Export Wizard

This wizard helps you copy certificates, certificate trust lists and certificate revocation lists from a certificate store to your disk.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

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.

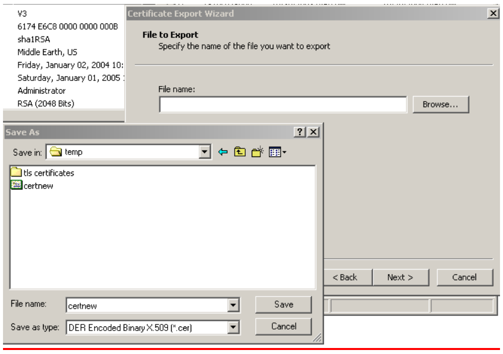


Certificate Export Wizard

Export File Format
Certificates can be exported in a variety of file formats.

Select the format you want to use:

- ● DER encoded binary X.509 (.CER)
- ○ Base-64 encoded X.509 (.CER)
- ○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
  - □ Include all certificates in the certification path if possible
- ○ Personal Information Exchange - PKCS #12 (.PFX)
  - □ Include all certificates in the certification path if possible
  - □ Enable strong protection (requires IE 5.0, NT 4.0 SP4 or above)
  - □ Delete the private key if the export is successful



V3
6174 E6C8 0000 0000 000B
sha1RSA
Middle Earth, US
Friday, January 02, 2004 10:
Saturday, January 01, 2005
Administrator
RSA (2048 Bits)

Certificate Export Wizard

File to Export
Specify the name of the file you want to export

File name:

Save As

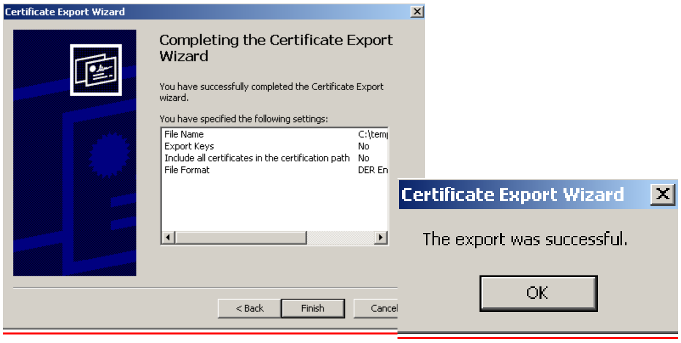
Save in: temp

tls certificates
certnew

File name: certnew

Save as type: DER Encoded Binary X.509 (*.cer)

Click *Finish* and followed by *OK*.



Certificate Export Wizard

Completing the Certificate Export Wizard

You have successfully completed the Certificate Export wizard.

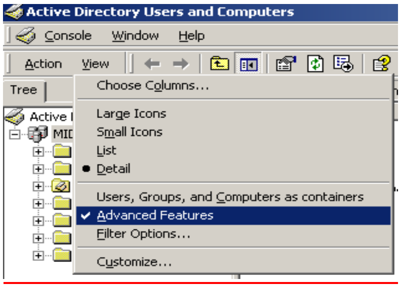
You have specified the following settings:

File Name	C:\tem
Export Keys	No
Include all certificates in the certification path	No
File Format	DER En

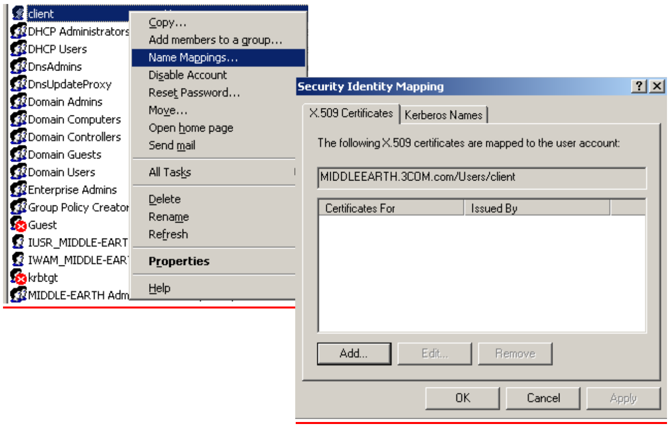
Certificate Export Wizard

The export was successful.

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.



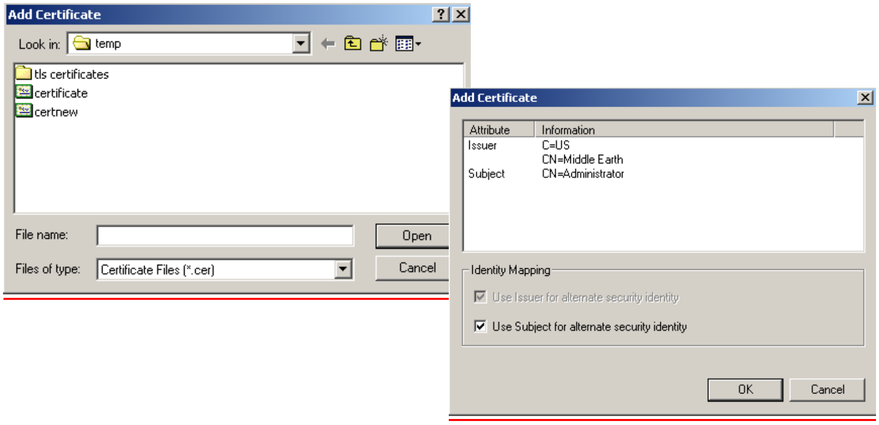
u Select the user that becomes the IEEE 802.1x client. Right-click on the user and select *Name mappings*. Select *Add*



The following X.509 certificates are mapped to the user account:

MIDDLEEARTH.3COM.com/Users/client

v Select the certificate that you have just exported and click *Open*. Click *OK*



Attribute	Information

Issuer	C=US
	CN=Middle Earth

Subject	CN=Administrator

☑ Use Issuer for alternate security identity

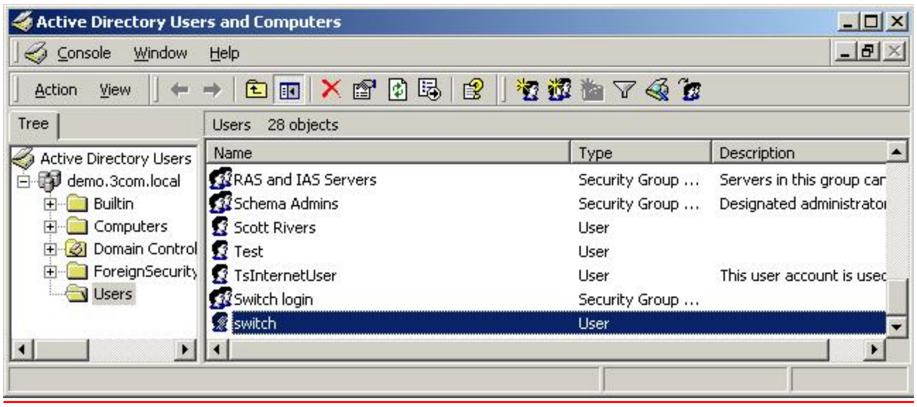
☑ Use Subject for alternate security identity

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.

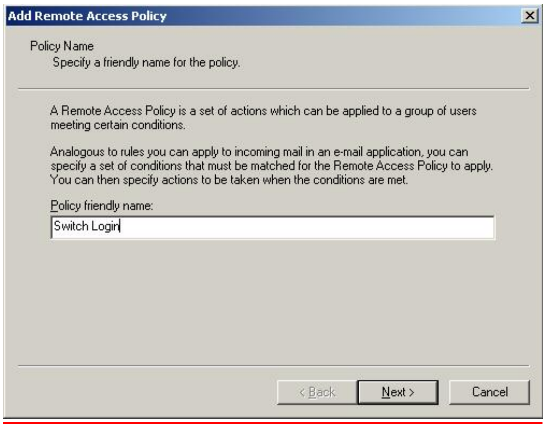
10 Configure Microsoft IAS RADIUS Server for Switch Login.

a Create a Windows Group that contains the users that are allowed access to the Switch 5500G-EI. Add an additional user as a member of this windows group:



Name	Type	Description
RAS and IAS Servers	Security Group ...	Servers in this group car
Schema Admins	Security Group ...	Designated administrator
Scott Rivers	User	
Test	User	
TsInternetUser	User	This user account is usec
Switch login	Security Group ...	
switch	User	

b Create a new remote access policy under IAS and name it *Switch Login. S*elect *Next>.*.



Add Remote Access Policy

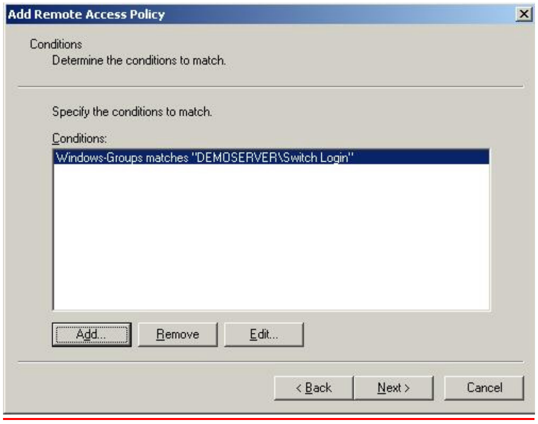
Policy Name
Specify a friendly name for the policy.

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.

Policy friendly name:
Switch Login

c Specify *Switch Login* to match the users in the switch access group, select *Next >*



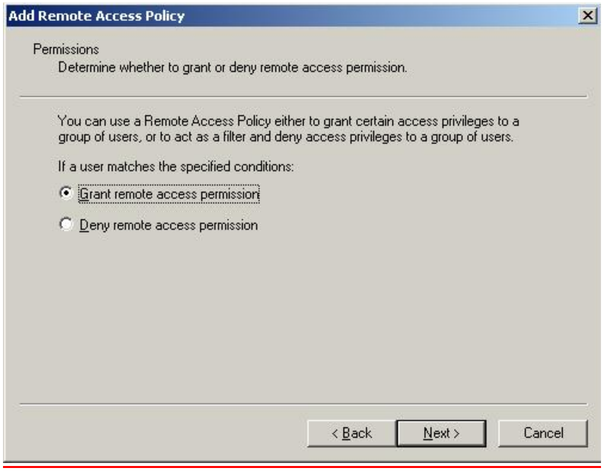
Add Remote Access Policy

Conditions
Determine the conditions to match.

Specify the conditions to match.

Conditions:
Windows-Groups matches "DEMOSERVER\Switch Login"

d Allow *Switch Login* to grant access to these users, select *Next >*



Add Remote Access Policy

Permissions
Determine whether to grant or deny remote access permission.

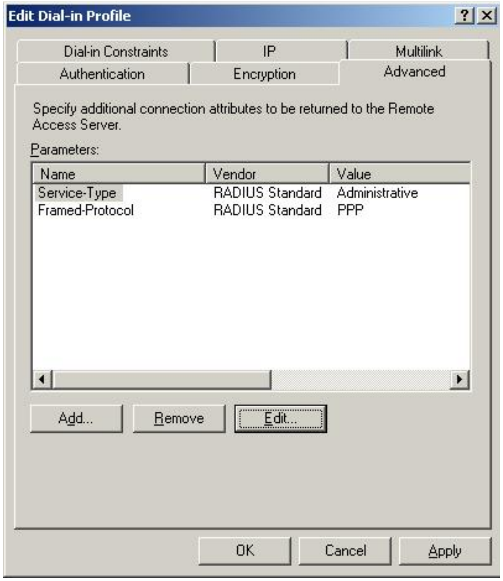
You can use a Remote Access Policy either to grant certain access privileges to a group of users, or to act as a filter and deny access privileges to a group of users.

If a user matches the specified conditions:

● Grant remote access permission

○ Deny remote access permission

e Use the *Edit* button to change the *Service-Type* to *Administrative.*

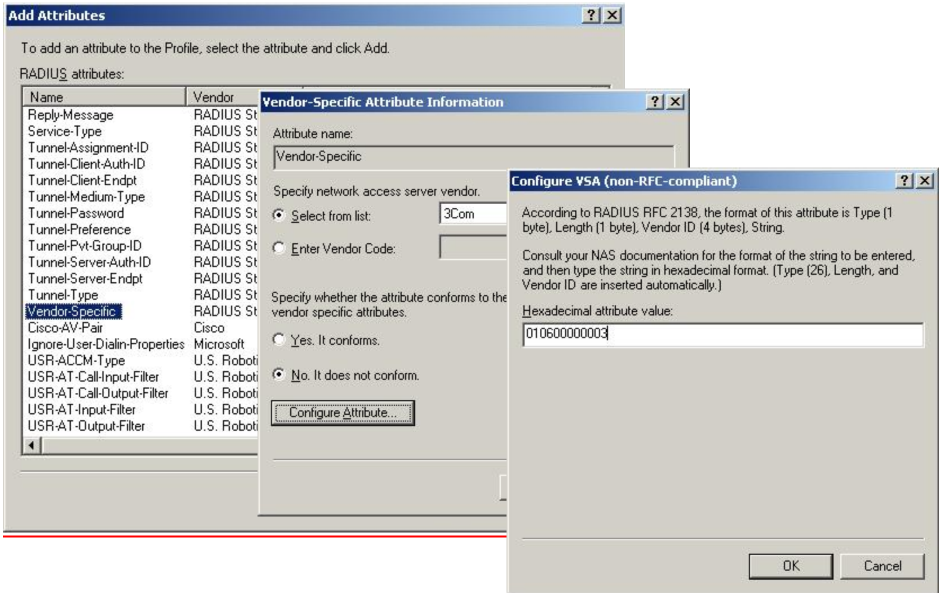


Specify additional connection attributes to be returned to the Remote Access Server.

Parameters:

Name	Vendor	Value
Service-Type	RADIUS Standard	Administrative
Framed-Protocol	RADIUS Standard	PPP

f Add a Vendor specific attribute to indicate the access level that should be provided:


Add Attributes
Vendor-Specific Attribute Information
Configure VSA (non-RFC-compliant)
Configure Attribute...
OK
Cancel

To add an attribute to the Profile, select the attribute and click Add.

RADIUS attributes:

Name	Vendor
Reply-Message	RADIUS St
Service-Type	RADIUS St
Tunnel-Assignment-ID	RADIUS St
Tunnel-Client-Auth-ID	RADIUS St
Tunnel-Client-Endpt	RADIUS St
Tunnel-Medium-Type	RADIUS St
Tunnel-Password	RADIUS St
Tunnel-Preference	RADIUS St
Tunnel-Pvt-Group-ID	RADIUS St
Tunnel-Server-Auth-ID	RADIUS St
Tunnel-Server-Endpt	RADIUS St
Tunnel-Type	RADIUS St
Vendor-Specific	RADIUS St
Cisco-AV-Pair	Cisco
Ignore-User-Dialin-Properties	Microsoft
USR-ACCM-Type	U.S. Roboti
USR-AT-Call-Input-Filter	U.S. Roboti
USR-AT-Call-Output-Filter	U.S. Roboti
USR-AT-Input-Filter	U.S. Roboti
USR-AT-Output-Filter	U.S. Roboti

Attribute name: Vendor-Specific

Specify network access server vendor.

● Select from list: 3Com

○ Enter Vendor Code:

Specify whether the attribute conforms to the
vendor specific attributes.

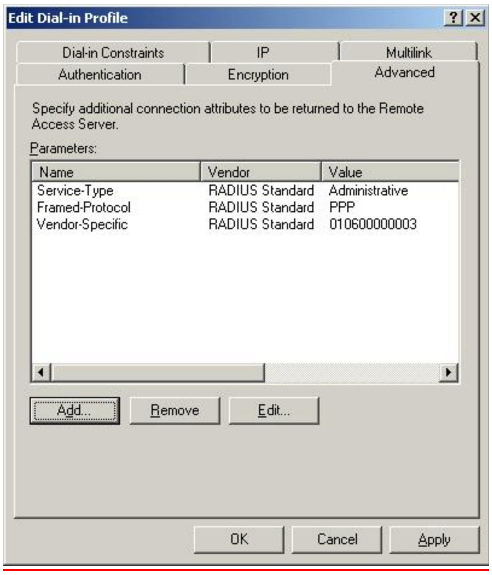
○ Yes. It conforms.

● No. It does not conform.

According to RADIUS RFC 2138, the format of this attribute is Type (1 byte), Length (1 byte), Vendor ID (4 bytes), String.

Consult your NAS documentation for the format of the string to be entered, and then type the string in hexadecimal format. (Type (26), Length, and Vendor ID are inserted automatically.)

Hexadecimal attribute value: 010600000003



Specify additional connection attributes to be returned to the Remote Access Server.

Parameters:

Name	Vendor	Value
Service-Type	RADIUS Standard	Administrative
Framed-Protocol	RADIUS Standard	PPP
Vendor-Specific	RADIUS Standard	010600000003

The Value 010600000003 indicates admin privileges for the switch. 01 at the end indicates monitor and 02 indicates manager access. On the Switch 5500G-EI, 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.

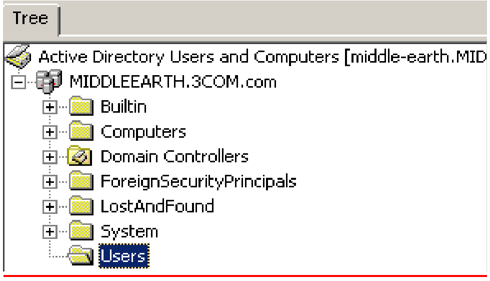
Configuring auto VLAN and QoS membership for Microsoft IAS

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 5500G-EI. The VLAN Groups must be created as Global/Security groups

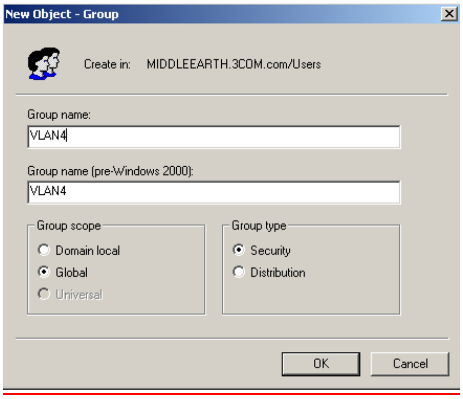
Follow these steps to set up auto VLAN and QoS for use by Microsoft IAS:

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 Groupn, for example *VLAN4.* Check *Global* in the *Group Scope* box and *Security* in the *Group Type* box, click *OK*..



New Object - Group

Create in: MIDDLEEARTH.3COM.com/Users

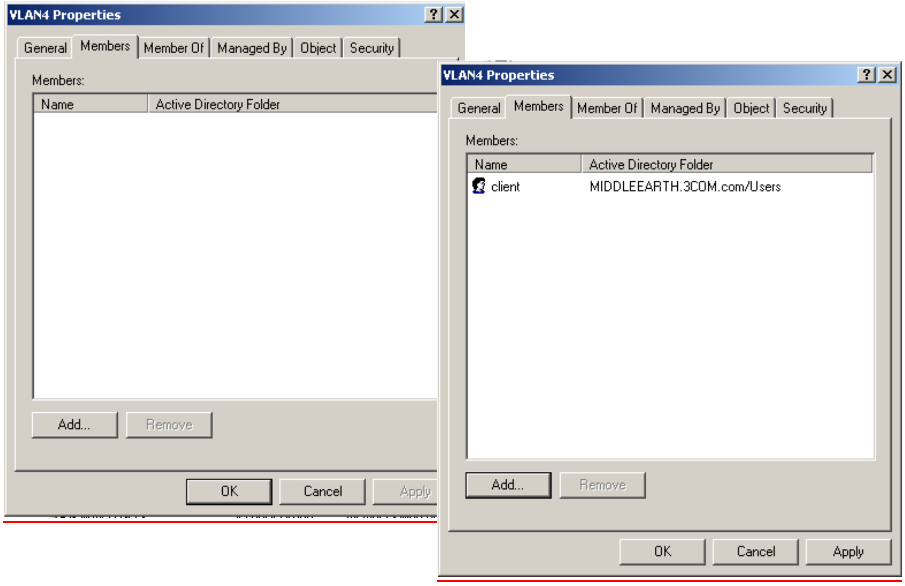
Group name: VLAN4

Group name (pre-Windows 2000): VLAN4

Group scope: ○ Domain local ● Global ○ Universal

Group type: ● Security ○ Distribution

   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.



VLAN4 Properties

Members:

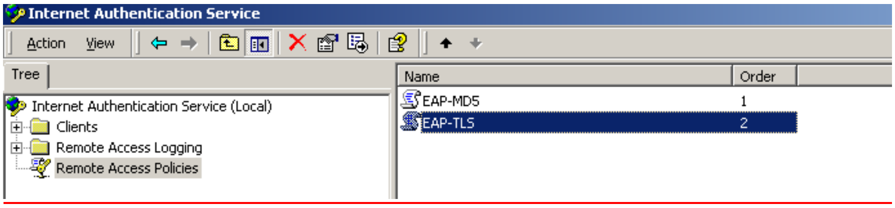
Name	Active Directory Folder

VLAN4 Properties

Members:

Name	Active Directory Folder
client	MIDDLEEARTH.3COM.com/Users

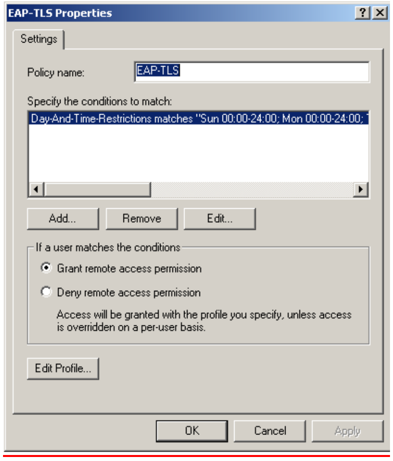
d Go to *Programs* > *Administrative Tools* > *Internet Authentication Service*. and select *Remote Access Policies*. Select the policy that you configured earlier, right-click and select *Properties*.



Internet Authentication Service (Local)
- Clients
- Remote Access Logging
- Remote Access Policies

Name	Order
EAP-MD5	1
EAP-TLS	2

e Click *Add* to add policy membership.

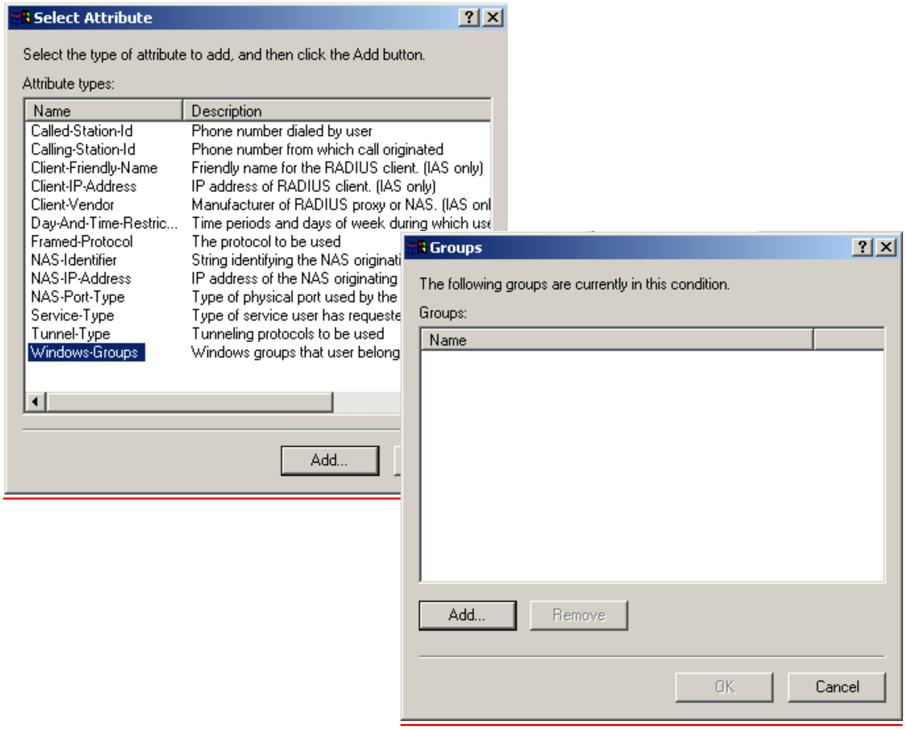


Policy name: EAP-TLS

Specify the conditions to match:
Day-And-Time-Restrictions matches "Sun 00:00-24:00; Mon 00:00-24:00;

If a user matches the conditions
● Grant remote access permission
○ Deny remote access permission
Access will be granted with the profile you specify, unless access is overridden on a per-user basis.

f Select the *Windows-Groups* attribute type, and select *Add* and *Add* again



Select the type of attribute to add, and then click the Add button.

Attribute types:

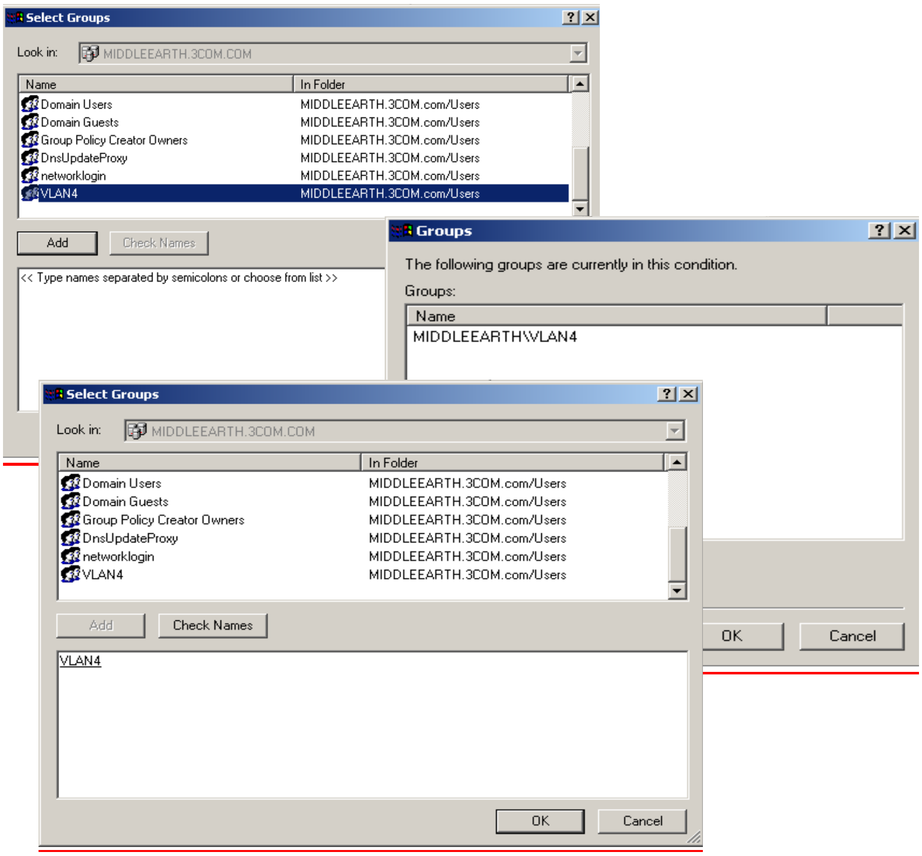
Name	Description
Called-Station-Id	Phone number dialed by user
Calling-Station-Id	Phone number from which call originated
Client-Friendly-Name	Friendly name for the RADIUS client. (IAS only)
Client-IP-Address	IP address of RADIUS client. (IAS only)
Client-Vendor	Manufacturer of RADIUS proxy or NAS. (IAS onl
Day-And-Time-Restric...	Time periods and days of week during which use
Framed-Protocol	The protocol to be used
NAS-Identifier	String identifying the NAS originati
NAS-IP-Address	IP address of the NAS originating
NAS-Port-Type	Type of physical port used by the
Service-Type	Type of service user has requeste
Tunnel-Type	Tunneling protocols to be used
Windows-Groups	Windows groups that user belong

The following groups are currently in this condition.

Groups:

Name

g Select the VLAN group that you have just created and click *Add* and then *OK* to confirm.


Select Groups
Look in: MIDDLEEARTH.3COM.COM
Add
Check Names
<< Type names separated by semicolons or choose from list >>

Name	In Folder
Domain Users	MIDDLEEARTH.3COM.com/Users
Domain Guests	MIDDLEEARTH.3COM.com/Users
Group Policy Creator Owners	MIDDLEEARTH.3COM.com/Users
DnsUpdateProxy	MIDDLEEARTH.3COM.com/Users
networklogin	MIDDLEEARTH.3COM.com/Users
VLAN4	MIDDLEEARTH.3COM.com/Users

The following groups are currently in this condition.

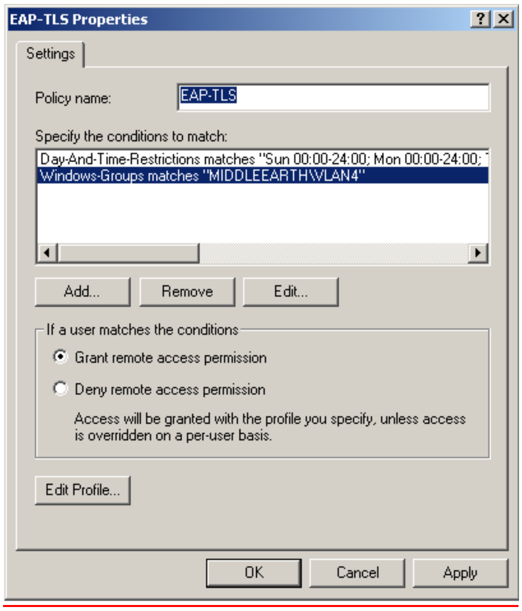
Groups:

Name
MIDDLEEARTH\VLAN4

OK
Cancel
Select Groups
Look in: MIDDLEEARTH.3COM.COM
Add
Check Names
OK
Cancel

VLAN4

h Click *OK* again to return you to the *Security Policy* properties.



Policy name: EAP-TLS

Specify the conditions to match:

Day-And-Time-Restrictions matches "Sun 00:00-24:00; Mon 00:00-24:00;

Windows-Groups matches "MIDDLEEARTH\VLAN4"

If a user matches the conditions

● Grant remote access permission

○ Deny remote access permission

Access will be granted with the profile you specify, unless access is overridden on a per-user basis.

i Click *Edit Profile...* and select the *Advanced* tab. Click *Add*. Refer to Table 459 and Table 460 for the RADIUS attributes to add to the profile.

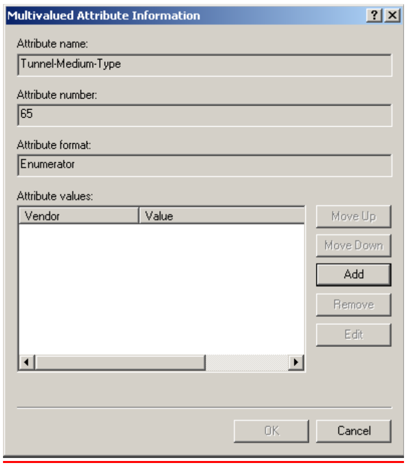
Table 459 Summary of auto VLAN attributes

For Auto VLAN	Return String	Comment
Tunnel-Medium-type	802	
Tunnel-Private-Group-ID	2	VLAN value
Tunnel-Type	VLAN	

Table 460 Summary of QoS attributes

For Auto QoS	Return String	Comment
Filter-id	profile=student	QoS Profile name

j Select *Tunnel-Medium-Type* and click *Add*.



Multivalued Attribute Information

Attribute name: Tunnel-Medium-Type

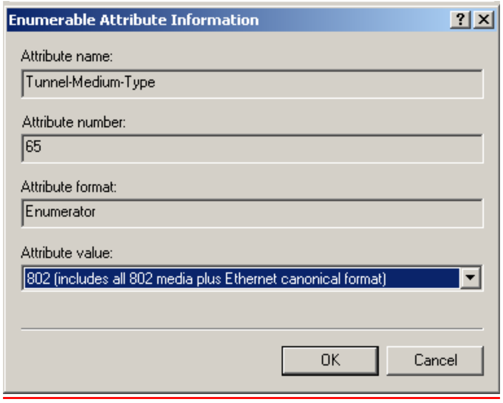
Attribute number: 65

Attribute format: Enumerator

Attribute values:

Vendor	Value

k Ensure that the Attribute value is set to 802 and click *OK*.



Enumerable Attribute Information

Attribute name: Tunnel-Medium-Type

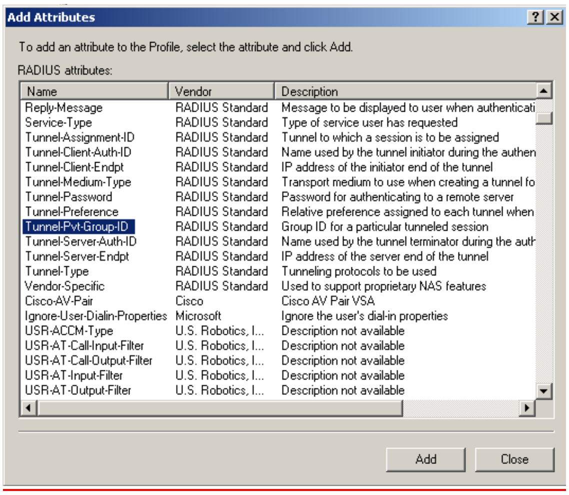
Attribute number: 65

Attribute format: Enumerator

Attribute value: 802 (includes all 802 media plus Ethernet canonical format)

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*.

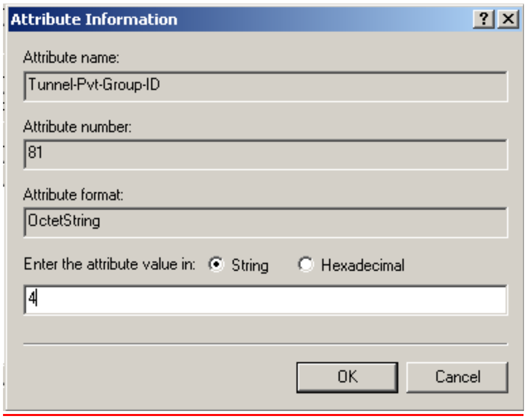


To add an attribute to the Profile, select the attribute and click Add.

RADIUS attributes:

Name	Vendor	Description
Reply-Message	RADIUS Standard	Message to be displayed to user when authenticati
Service-Type	RADIUS Standard	Type of service user has requested
Tunnel-Assignment-ID	RADIUS Standard	Tunnel to which a session is to be assigned
Tunnel-Client-Auth-ID	RADIUS Standard	Name used by the tunnel initiator during the authen
Tunnel-Client-Endpt	RADIUS Standard	IP address of the initiator end of the tunnel
Tunnel-Medium-Type	RADIUS Standard	Transport medium to use when creating a tunnel fo
Tunnel-Password	RADIUS Standard	Password for authenticating to a remote server
Tunnel-Preference	RADIUS Standard	Relative preference assigned to each tunnel when
Tunnel-Pvt-Group-ID	RADIUS Standard	Group ID for a particular tunneled session
Tunnel-Server-Auth-ID	RADIUS Standard	Name used by the tunnel terminator during the auth
Tunnel-Server-Endpt	RADIUS Standard	IP address of the server end of the tunnel
Tunnel-Type	RADIUS Standard	Tunneling protocols to be used
Vendor-Specific	RADIUS Standard	Used to support proprietary NAS features
Cisco-AV-Pair	Cisco	Cisco AV Pair VSA
Ignore-User-Dialin-Properties	Microsoft	Ignore the user's dial-in properties
USR-ACCM-Type	U.S. Robotics, I...	Description not available
USR-AT-Call-Input-Filter	U.S. Robotics, I...	Description not available
USR-AT-Call-Output-Filter	U.S. Robotics, I...	Description not available
USR-AT-Input-Filter	U.S. Robotics, I...	Description not available
USR-AT-Output-Filter	U.S. Robotics, I...	Description not available

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.



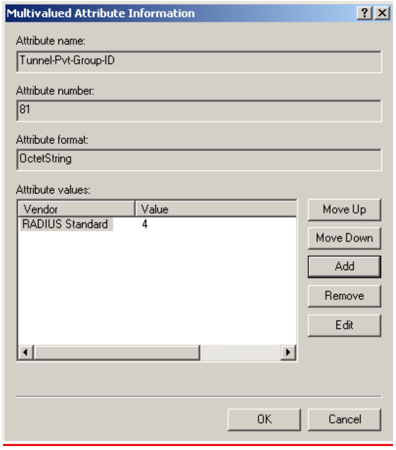
Attribute name: Tunnel-Pvt-Group-ID

Attribute number: 81

Attribute format: OctetString

Enter the attribute value in: ● String ○ Hexadecimal

4



Attribute name: Tunnel-Pvt-Group-ID

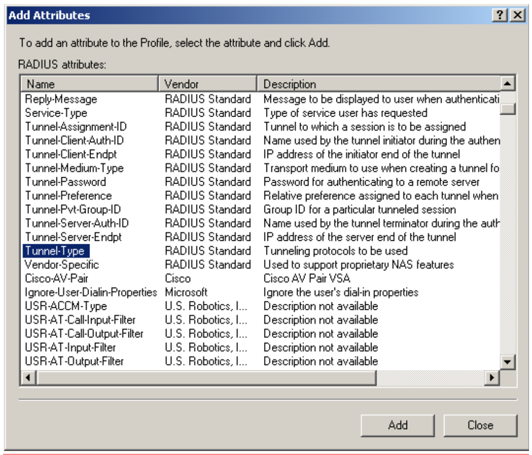
Attribute number: 81

Attribute format: OctetString

Attribute values:

Vendor	Value
RADIUS Standard	4

o Click *OK* again on the *Multivalued Attribute Information* screen to return to the the *Add Attributes* screen. Select the *Tunnel-Type* entry and click *Add*.

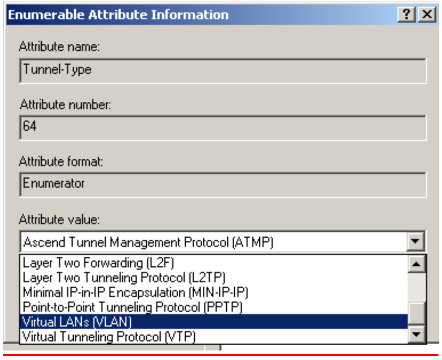


To add an attribute to the Profile, select the attribute and click Add.

RADIUS attributes:

Name	Vendor	Description
Reply-Message	RADIUS Standard	Message to be displayed to user when authenticati
Service-Type	RADIUS Standard	Type of service user has requested
Tunnel-Assignment-ID	RADIUS Standard	Tunnel to which a session is to be assigned
Tunnel-Client-Auth-ID	RADIUS Standard	Name used by the tunnel initiator during the authen
Tunnel-Client-Endpt	RADIUS Standard	IP address of the initiator end of the tunnel
Tunnel-Medium-Type	RADIUS Standard	Transport medium to use when creating a tunnel fo
Tunnel-Password	RADIUS Standard	Password for authenticating to a remote server
Tunnel-Preference	RADIUS Standard	Relative preference assigned to each tunnel when
Tunnel-Pvt-Group-ID	RADIUS Standard	Group ID for a particular tunneled session
Tunnel-Server-Auth-ID	RADIUS Standard	Name used by the tunnel terminator during the auth
Tunnel-Server-Endpt	RADIUS Standard	IP address of the server end of the tunnel
Tunnel-Type	RADIUS Standard	Tunneling protocols to be used
Vendor-Specific	RADIUS Standard	Used to support proprietary NAS features
Cisco-AV-Pair	Cisco	Cisco AV Pair VSA
Ignore-User-Dialin-Properties	Microsoft	Ignore the user's dial-in properties
USR-ACCM-Type	U.S. Robotics, I...	Description not available
USR-AT-Call-Input-Filter	U.S. Robotics, I...	Description not available
USR-AT-Call-Output-Filter	U.S. Robotics, I...	Description not available
USR-AT-Input-Filter	U.S. Robotics, I...	Description not available
USR-AT-Output-Filter	U.S. Robotics, I...	Description not available

p Click *Add* again. In the pull down menu, select *Virtual LANs* and click *OK*.



Enumerable Attribute Information

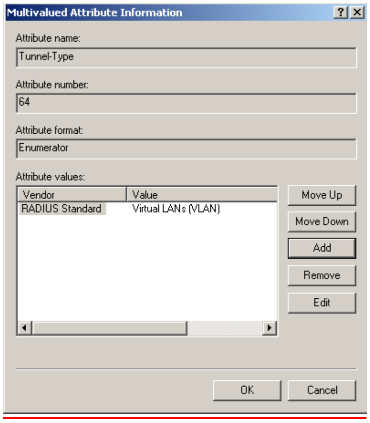
Attribute name: Tunnel-Type

Attribute number: 64

Attribute format: Enumerator

Attribute value: Ascend Tunnel Management Protocol (ATMP)

- Layer Two Forwarding (L2F)
- Layer Two Tunneling Protocol (L2TP)
- Minimal IP-in-IP Encapsulation (MIN-IP-IP)
- Point-to-Point Tunneling Protocol (PPTP)
- Virtual LANs (VLAN)
- Virtual Tunneling Protocol (VTP)



Multivalued Attribute Information

Attribute name: Tunnel-Type

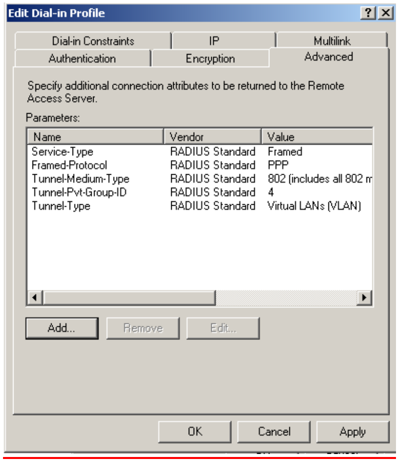
Attribute number: 64

Attribute format: Enumerator

Attribute values:

Vendor	Value
RADIUS Standard	Virtual LANs (VLAN)

q Click *OK* again and to return to the *Add Attributes* screen. Click *Close*. You will now see the added attributes



Edit Dial-in Profile

Specify additional connection attributes to be returned to the Remote Access Server.

Parameters:

Name	Vendor	Value
Service-Type	RADIUS Standard	Framed
Framed-Protocol	RADIUS Standard	PPP
Tunnel-Medium-Type	RADIUS Standard	802 (includes all 802 m
Tunnel-Pvt-Group-ID	RADIUS Standard	4
Tunnel-Type	RADIUS Standard	Virtual LANs (VLAN)

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 5500G-EI (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.

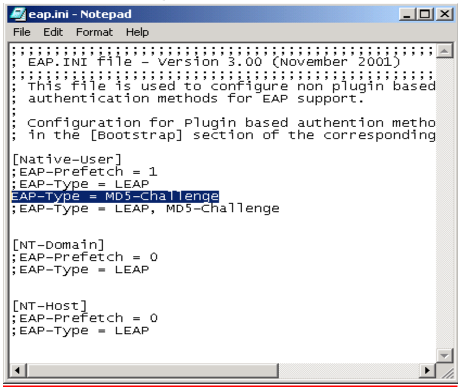
Configuring Funk RADIUS

3Com has successfully installed and tested Funk RADIUS running on a Windows server in a network with Switch 5500G-EI 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.

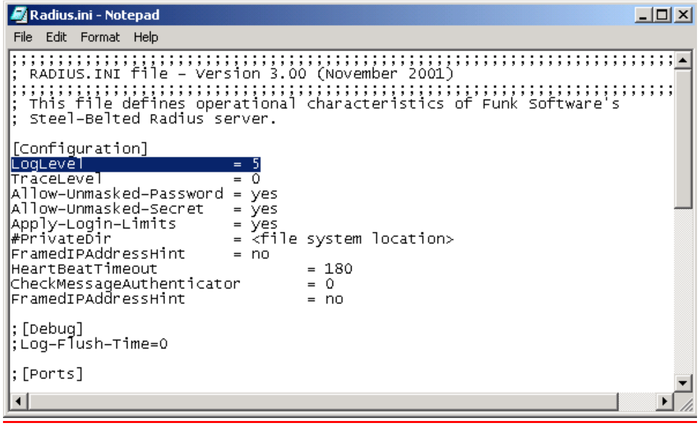
To configure Funk RADIUS as a RADIUS server for networks with the Switch 5500G-EI, follow these steps:

1 Open file `eap.ini` in `\radius\service` and remove the ";" before the MD5-Challenge Line. This enables the MD5-challenge



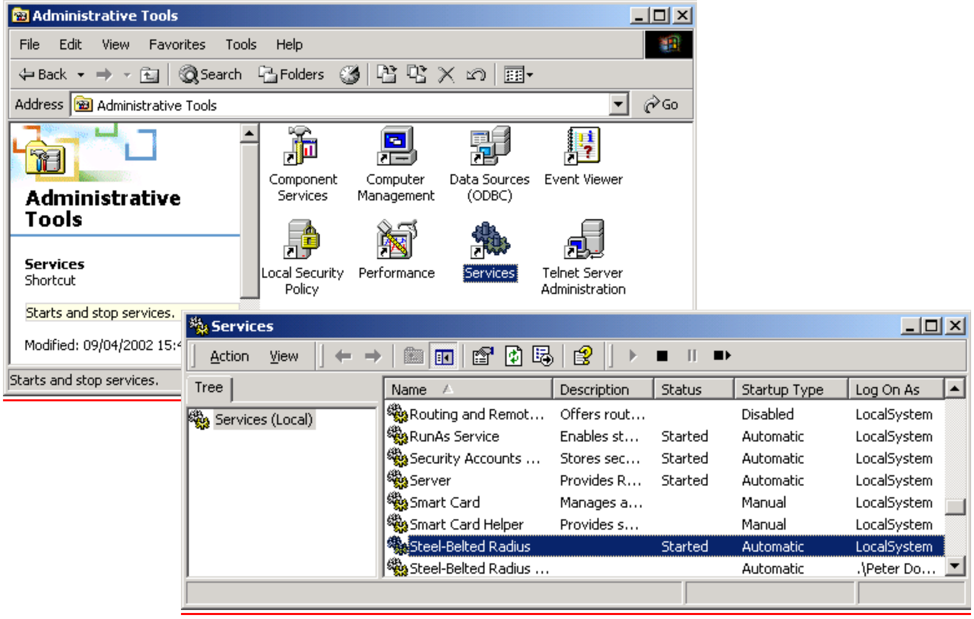
```
;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;
;  EAP.INI file - Version 3.00 (November 2001)
;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;
;  This file is used to configure non plugin based
;  authentication methods for EAP support.
;
;  Configuration for Plugin based authention metho
;  in the [Bootstrap] section of the corresponding

[Native-User]
;EAP-Prefetch = 1
;EAP-Type = LEAP
EAP-Type = MD5-Challenge
;EAP-Type = LEAP, MD5-Challenge


[NT-Domain]
;EAP-Prefetch = 0
;EAP-Type = LEAP


[NT-Host]
;EAP-Prefetch = 0
;EAP-Type = LEAP
```

2 Open file `radius.ini` in `\radius\service` and change the log level to 5.



```
;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;
;  RADIUS.INI file - Version 3.00 (November 2001)
;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;
;  This file defines operational characteristics of Funk Software's
;  Steel-Belted Radius server.

[Configuration]
LogLevel                = 5
TraceLevel              = 0
Allow-Unmasked-Password = yes
Allow-Unmasked-Secret   = yes
Apply-Login-Limits      = yes
#PrivateDir             = <file system location>
FramedIPAddressHint     = no
HeartBeatTimeout                = 180
CheckMessageAuthenticator       = 0
FramedIPAddressHint             = no

;[Debug]
;Log-Flush-Time=0

;[Ports]
```

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.

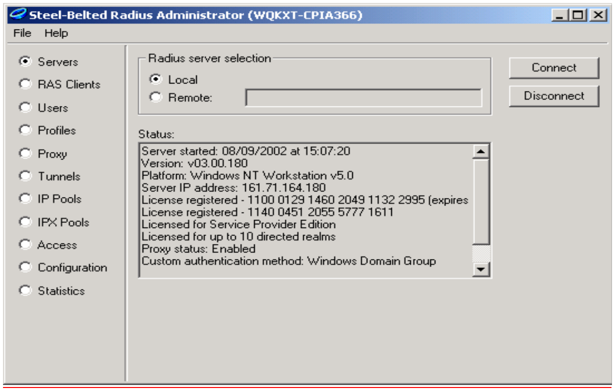


Name	Description	Status	Startup Type	Log On As
Routing and Remot...	Offers rout...		Disabled	LocalSystem
RunAs Service	Enables st...	Started	Automatic	LocalSystem
Security Accounts ...	Stores sec...	Started	Automatic	LocalSystem
Server	Provides R...	Started	Automatic	LocalSystem
Smart Card	Manages a...		Manual	LocalSystem
Smart Card Helper	Provides s...		Manual	LocalSystem
Steel-Belted Radius		Started	Automatic	LocalSystem
Steel-Belted Radius ...			Automatic	.\Peter Do...

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 5500G-EI and follow the instructions in Configuring auto VLAN and QoS for Funk RADIUS.

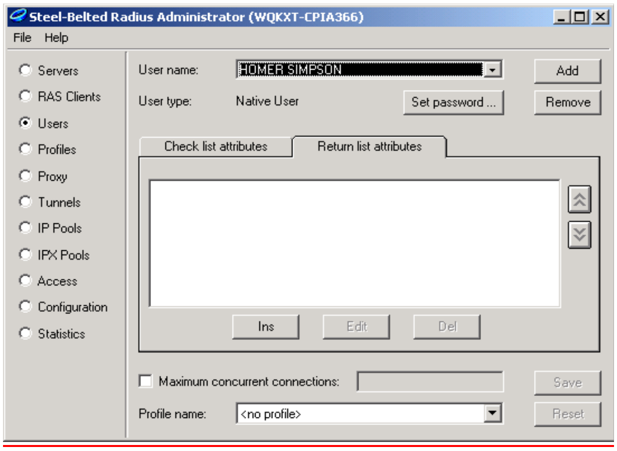
4 Start the Funk RADIUS program, select *Servers* from the left hand list and select *Local* Radius server. Select *Connect* to start listening for clients.



```
Server started: 08/09/2002 at 15:07:20
Version: v03.00.180
Platform: Windows NT Workstation v5.0
Server IP address: 161.71.164.180
License registered - 1100 0129 1460 2049 1132 2995 (expires
License registered - 1140 0451 2055 5777 1611
Licensed for Service Provider Edition
Licensed for up to 10 directed realms
Proxy status: Enabled
Custom authentication method: Windows Domain Group
```

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.



Steel-Belted Radius Administrator (WQKXT-CPIA366)

○ Servers
○ RAS Clients
● Users
○ Profiles
○ Proxy
○ Tunnels
○ IP Pools
○ IPX Pools
○ Access
○ Configuration
○ Statistics

User name: HOMER SIMPSON

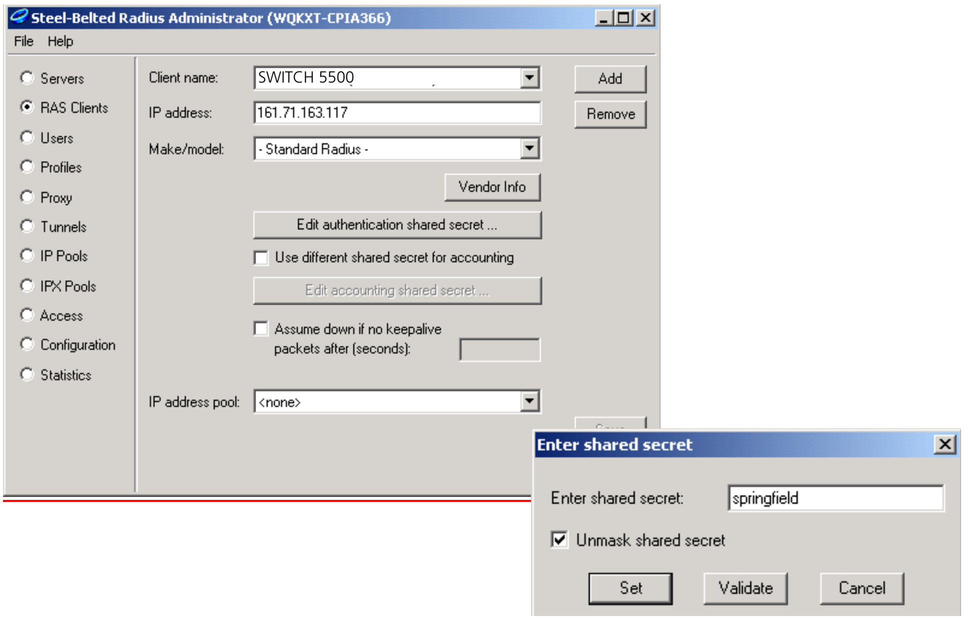
User type: Native User

□ Maximum concurrent connections:

Profile name: <no profile>

6 Enter the shared secret to encrypt the authentication data. The shared secret must be identical on the Switch 5500G-EI and the RADIUS Server

a Select *RAS Clients* from the left hand list, enter a *Client name* , the *IP address* and the *Shared secret*.



Steel-Belted Radius Administrator (WQKXT-CPIA366)

○ Servers
● RAS Clients
○ Users
○ Profiles
○ Proxy
○ Tunnels
○ IP Pools
○ IPX Pools
○ Access
○ Configuration
○ Statistics

Client name: SWITCH 5500

IP address: 161.71.163.117

Make/model: - Standard Radius -

□ Use different shared secret for accounting

□ Assume down if no keepalive packets after (seconds):

IP address pool: <none>

Enter shared secret

Enter shared secret: springfield

☑ Unmask shared secret

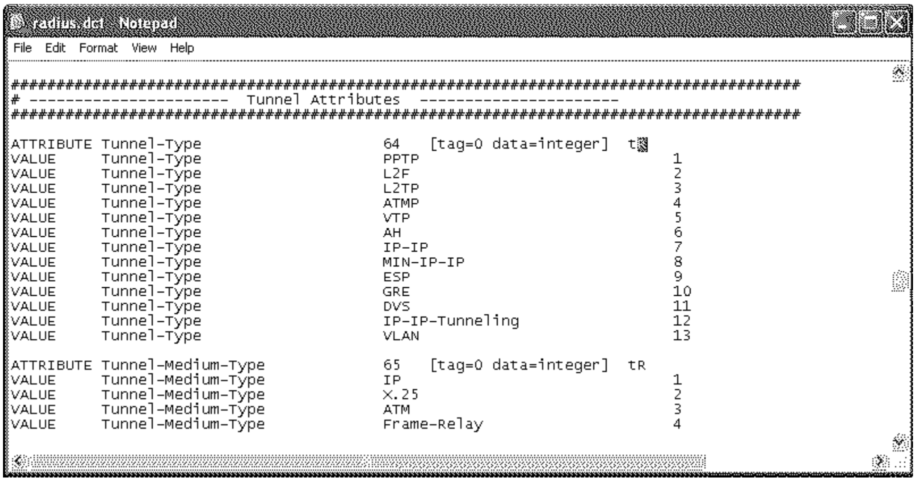
File
Help
Add
Remove
Vendor Info
Edit authentication shared secret ...
Edit accounting shared secret ...
Set
Validate
Cancel

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 5500G-EI. 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.



```
########################################################################################
# ----------------------  Tunnel Attributes  ----------------------
########################################################################################

ATTRIBUTE Tunnel-Type                   64    [tag=0 data=integer]  tR
VALUE     Tunnel-Type                   PPTP                            1
VALUE     Tunnel-Type                   L2F                             2
VALUE     Tunnel-Type                   L2TP                            3
VALUE     Tunnel-Type                   ATMP                            4
VALUE     Tunnel-Type                   VTP                             5
VALUE     Tunnel-Type                   AH                              6
VALUE     Tunnel-Type                   IP-IP                           7
VALUE     Tunnel-Type                   MIN-IP-IP                       8
VALUE     Tunnel-Type                   ESP                             9
VALUE     Tunnel-Type                   GRE                             10
VALUE     Tunnel-Type                   DVS                             11
VALUE     Tunnel-Type                   IP-IP-Tunneling                 12
VALUE     Tunnel-Type                   VLAN                            13

ATTRIBUTE Tunnel-Medium-Type            65    [tag=0 data=integer]  tR
VALUE     Tunnel-Medium-Type            IP                              1
VALUE     Tunnel-Medium-Type            X.25                            2
VALUE     Tunnel-Medium-Type            ATM                             3
VALUE     Tunnel-Medium-Type            Frame-Relay                     4
```

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 461 .and Table 462

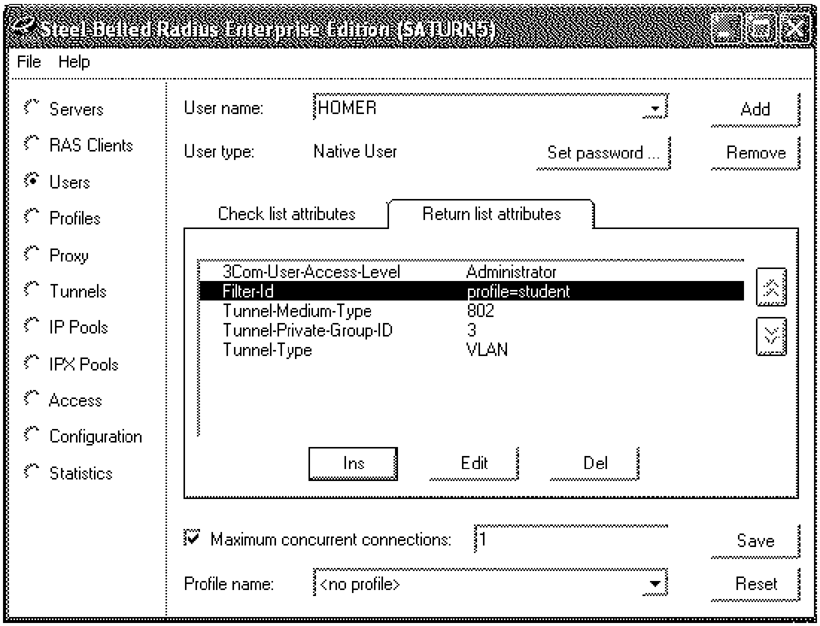
Table 461 Summary of auto VLAN attributes

For Auto VLAN	Return String	Comment
Tunnel-Medium-type	802	
Tunnel-Private-Group-ID	2	VLAN value
Tunnel-Type	VLAN	

Table 462 Summary of QoS attributes

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,



User name: HOMER

User type: Native User

```
3Com-User-Access-Level    Administrator
Filter-Id                 profile=student
Tunnel-Medium-Type        802
Tunnel-Private-Group-ID   3
Tunnel-Type               VLAN
```

☑ Maximum concurrent connections: 1

Profile name: <no profile>

The VLANs and QoS profiles must also be created on the 3Com Switch 5500G-EI.

Configuring FreeRADIUS

3Com has successfully installed and tested FreeRADIUS running on Solaris 2.6 and RedHat Linux servers in networks with the Switch 5500G-EI 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 5500G-EI, follow these steps:

1 Add each Switch 5500G-EI 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 5500G-EI 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 5500G-EI.

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 5500G-EI:

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 -sfxxyz -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:

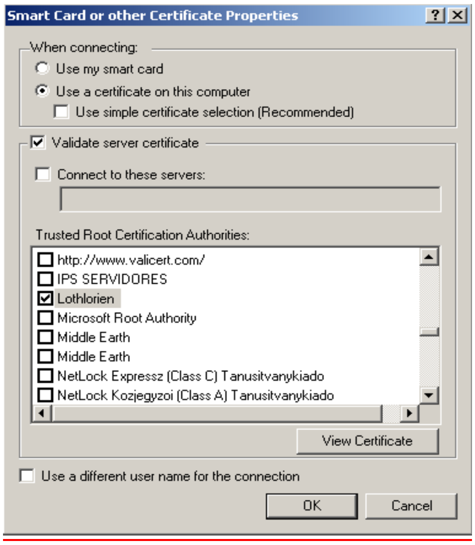
`http://www.microsoft.com/Downloads/details.aspx?displaylang=en&FamilyID=6B78EDBE-D3CA-4880-929F-453C695B9637`

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.



Smart Card or other Certificate Properties

When connecting:

○ Use my smart card

● Use a certificate on this computer

□ Use simple certificate selection (Recommended)

☑ Validate server certificate

□ Connect to these servers:

Trusted Root Certification Authorities:

□ http://www.valicert.com/
□ IPS SERVIDORES
☑ Lothlorien
□ Microsoft Root Authority
□ Middle Earth
□ Middle Earth
□ NetLock Expressz (Class C) Tanusitvanykiado
□ NetLock Kozjegyzoi (Class A) Tanusitvanykiado

□ Use a different user name for the connection

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 authorised 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 authorised. 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

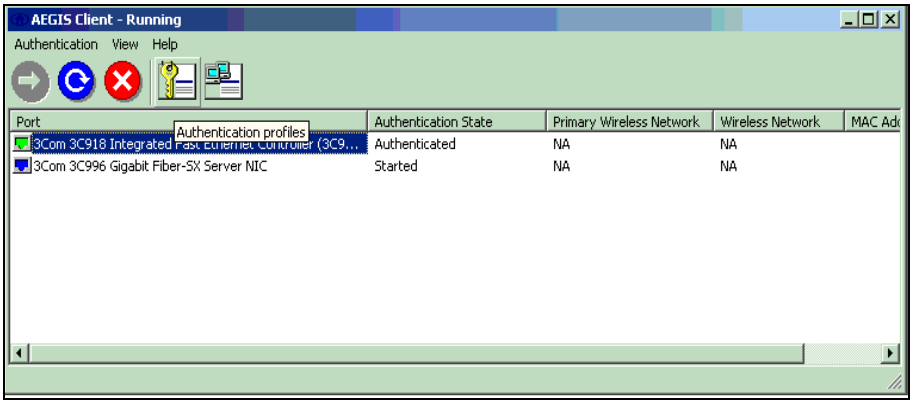
c Copy the License ID indicated at the bottom of the dialog box into the *License ID* field.

d Copy the License Key provided in the email from Meetinghouse into the *License Key* field.

e Press *OK*

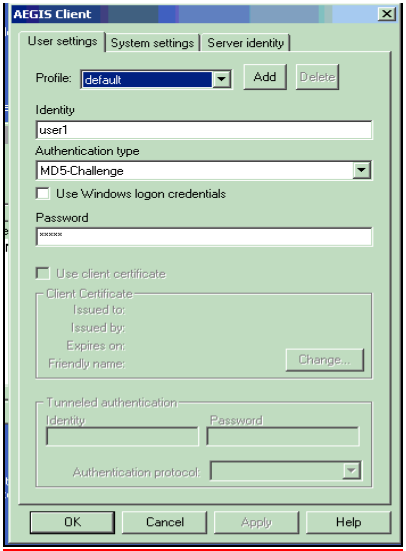
2 Configuring the Aegis Client

a Click the *Key* icon.



Port	Authentication State	Primary Wireless Network	Wireless Network	MAC Ad
3Com 3C918 Integrated Fast Ethernet Controller (3C9...	Authenticated	NA	NA	
3Com 3C996 Gigabit Fiber-SX Server NIC	Started	NA	NA	

b This screen will appear:



Profile: default

Identity
user1

Authentication type
MD5-Challenge

☐ Use Windows logon credentials

Password
*****

☐ Use client certificate

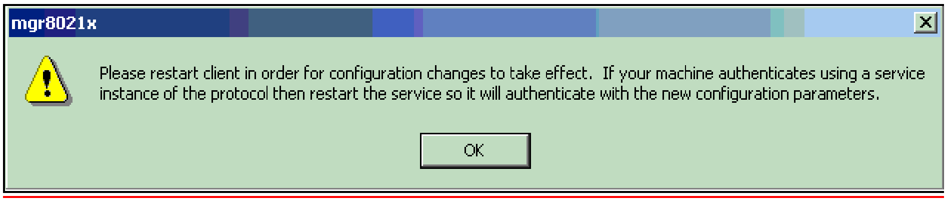
Client Certificate
Issued to:
Issued by:
Expires on:
Friendly name:

Tunneled authentication
Identity
Password
Authentication protocol:

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.



mgr8021x

Please restart client in order for configuration changes to take effect. If your machine authenticates using a service instance of the protocol then restart the service so it will authenticate with the new configuration parameters.

f Click the *OK* button, then return tothe 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 5500G-EI WITH CISCO SECURE ACS

This appendix covers the following topics:

- Cisco Secure ACS (TACACS+) and the 3Com Switch 5500G-EI
- Setting Up the Cisco Secure ACS (TACACS+) server

Cisco Secure ACS (TACACS+) and the 3Com Switch 5500G-EI

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 centralised control over network and management access, can also deploy the 3Com Switch 5500G-EI 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 authorised using the TACACS+ or RADIUS server, an optional VLAN and QoS profile can be applied to the user. Network administrators can also be authorised using the built in RADIUS server, providing centralised 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 5500G-EI on your network and allow any additional users to login to the nework:

- Adding a 3Com Switch 5500G-EI as a RADIUS client
- Adding a User for Network Login

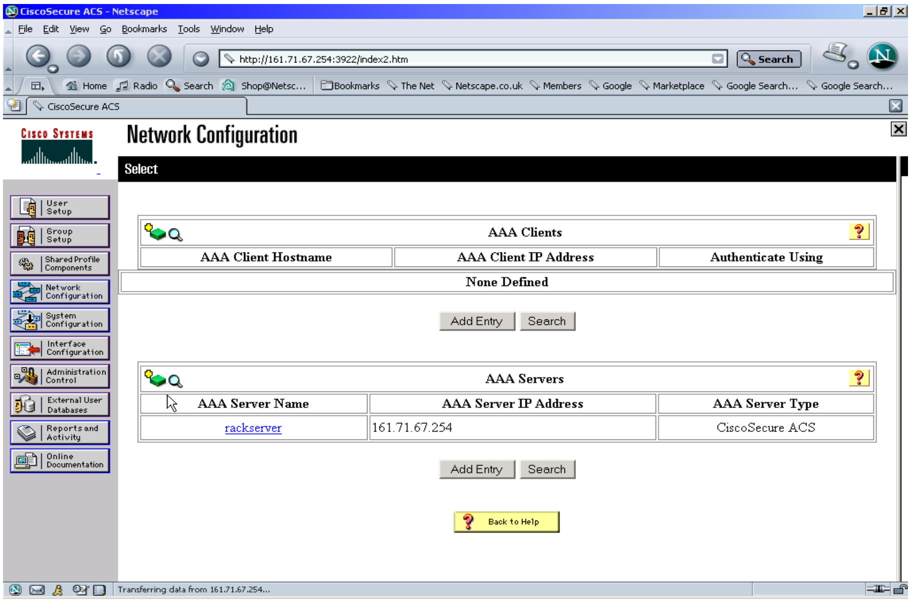
The final section details how to add a User (Network Administrator) for Switch Login to enable centralised management of the switch through the Cisco Secure ACS server.

- Adding a User for Switch Login

Adding a 3Com Switch 5500G-EI as a RADIUS client

Once logged into the Cisco Secure ACS interface, follow these steps:

1 Select *Network Configuration* from the left hand side


CiscoSecure ACS - Netscape
File Edit View Go Bookmarks Tools Window Help
http://161.71.67.254:3922/index2.htm
Search
Home Radio Search Shop@Netsc... Bookmarks The Net Netscape.co.uk Members Google Marketplace Google Search... Google Search...
CiscoSecure ACS
CISCO SYSTEMS
User Setup
Group Setup
Shared Profile Components
Network Configuration
System Configuration
Interface Configuration
Administration Control
External User Databases
Reports and Activity
Online Documentation
Transferring data from 161.71.67.254...

Network Configuration

Select

AAA Clients

AAA Client Hostname	AAA Client IP Address	Authenticate Using
None Defined		

Add Entry Search

AAA Servers

AAA Server Name	AAA Server IP Address	AAA Server Type
rackserver	161.71.67.254	CiscoSecure ACS

Add Entry Search

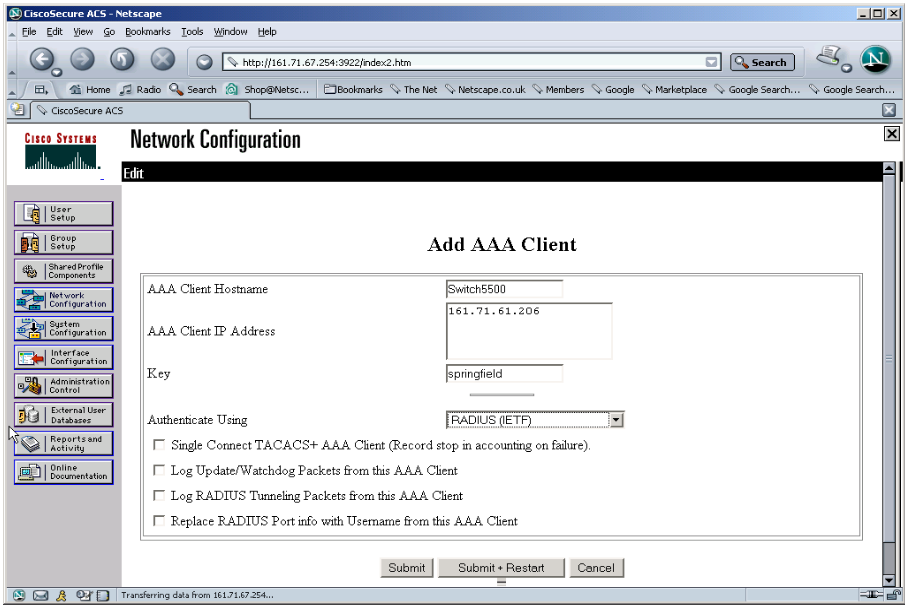
Back to Help

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


CiscoSecure ACS - Netscape
File Edit View Go Bookmarks Tools Window Help
http://161.71.67.254:3922/index2.htm
Search
Home Radio Search Shop@Netsc... Bookmarks The Net Netscape.co.uk Members Google Marketplace Google Search... Google Search...
CiscoSecure ACS
CISCO SYSTEMS
User Setup
Group Setup
Shared Profile Components
Network Configuration
System Configuration
Interface Configuration
Administration Control
External User Databases
Reports and Activity
Online Documentation
Transferring data from 161.71.67.254...

Network Configuration

Edit

Add AAA Client

AAA Client Hostname	Switch5500
AAA Client IP Address	161.71.61.206
Key	springfield
Authenticate Using	RADIUS (IETF)

□ Single Connect TACACS+ AAA Client (Record stop in accounting on failure).

□ Log Update/Watchdog Packets from this AAA Client

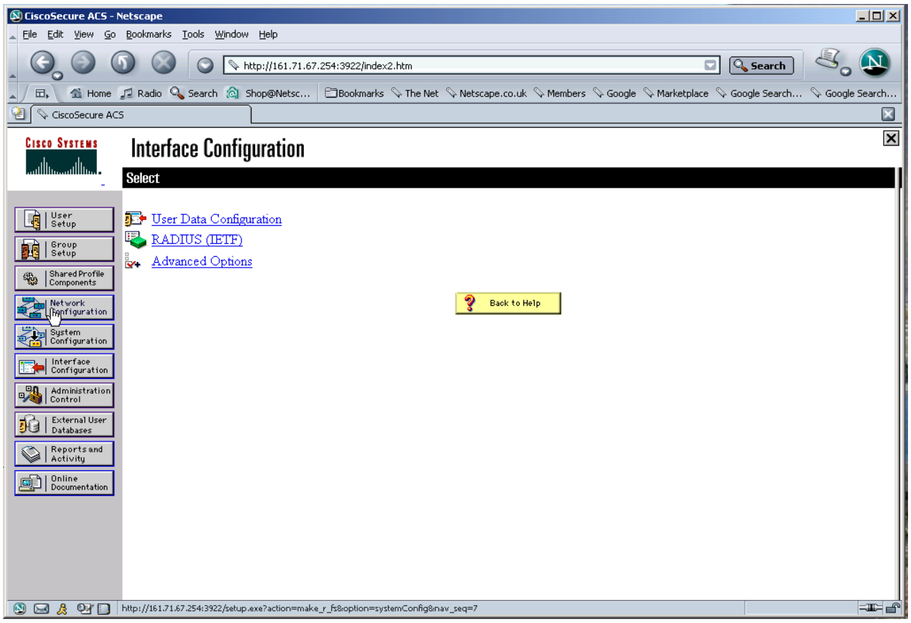
□ Log RADIUS Tunneling Packets from this AAA Client

□ Replace RADIUS Port info with Username from this AAA Client

Submit Submit + Restart Cancel

4 Select *Submit*. Do not restart the ACS server at this stage

5 Select *Interface Configuration* from the left hand side.

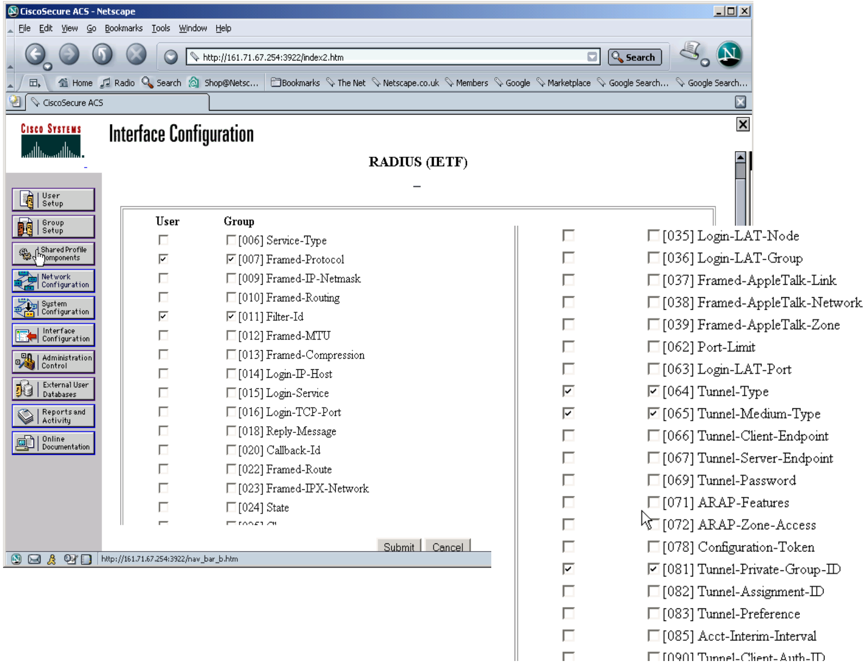

CiscoSecure ACS - Netscape
File Edit View Go Bookmarks Tools Window Help
http://161.71.67.254:3922/index2.htm
Search
Home Radio Search Shop@Netsc... Bookmarks The Net Netscape.co.uk Members Google Marketplace Google Search... Google Search...
CiscoSecure ACS
Cisco Systems
Interface Configuration
Select
User Data Configuration
RADIUS (IETF)
Advanced Options
Back to Help
User Setup
Group Setup
Shared Profile Components
Network Configuration
System Configuration
Interface Configuration
Administration Control
External User Databases
Reports and Activity
Online Documentation
http://161.71.67.254:3922/setup.exe?action=make_r_fs&option=systemConfig&nav_seq=7

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-I


CiscoSecure ACS - Netscape
File Edit View Go Bookmarks Tools Window Help
http://161.71.67.254:3922/index2.htm
Search
Home Radio Search Shop@Netsc... Bookmarks The Net Netscape.co.uk Members Google Marketplace Google Search... Google Search...
CiscoSecure ACS
Cisco Systems
Interface Configuration
User Setup
Group Setup
Shared Profile Components
Network Configuration
System Configuration
Interface Configuration
Administration Control
External User Databases
Reports and Activity
Online Documentation
Submit
Cancel
http://161.71.67.254:3922/nav_bar_b.htm

RADIUS (IETF)

User	Group
□	□ [006] Service-Type
☑	☑ [007] Framed-Protocol
□	□ [009] Framed-IP-Netmask
□	□ [010] Framed-Routing
☑	☑ [011] Filter-Id
□	□ [012] Framed-MTU
□	□ [013] Framed-Compression
□	□ [014] Login-IP-Host
□	□ [015] Login-Service
□	□ [016] Login-TCP-Port
□	□ [018] Reply-Message
□	□ [020] Callback-Id
□	□ [022] Framed-Route
□	□ [023] Framed-IPX-Network
□	□ [024] State

□	□ [035] Login-LAT-Node
□	□ [036] Login-LAT-Group
□	□ [037] Framed-AppleTalk-Link
□	□ [038] Framed-AppleTalk-Network
□	□ [039] Framed-AppleTalk-Zone
□	□ [062] Port-Limit
□	□ [063] Login-LAT-Port
☑	☑ [064] Tunnel-Type
☑	☑ [065] Tunnel-Medium-Type
□	□ [066] Tunnel-Client-Endpoint
□	□ [067] Tunnel-Server-Endpoint
□	□ [069] Tunnel-Password
□	□ [071] ARAP-Features
□	□ [072] ARAP-Zone-Access
□	□ [078] Configuration-Token
☑	☑ [081] Tunnel-Private-Group-ID
□	□ [082] Tunnel-Assignment-ID
□	□ [083] Tunnel-Preference
□	□ [085] Acct-Interim-Interval
□	□ [090] Tunnel-Client-Auth-ID

8 Select *Submit*.

9 Repeat steps 1 to 8 for each Switch 5500G-EI on your network. When all of the Switch 5500G-EIs 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

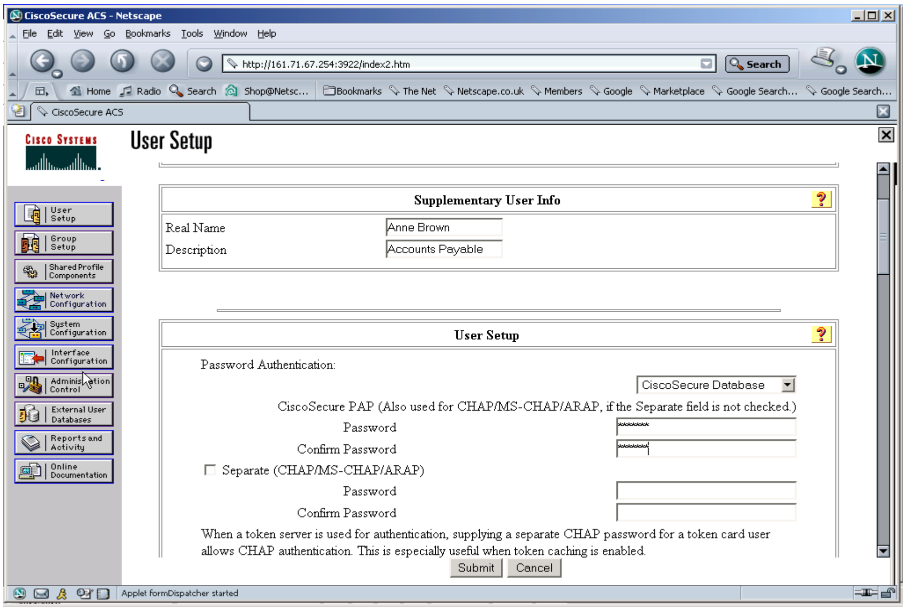
Existing users on a network with a Secure ACS server can be authorised using the TACACS+ or RADIUS server. New users connected through a Switch 5500G-EI to the network need to be authorised via the RADIUS server. An optional VLAN and QoS profile can be applied to the user.

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.


CiscoSecure ACS - Netscape
File Edit View Go Bookmarks Tools Window Help
http://161.71.67.254:3922/index2.htm
Search
Home Radio Search Shop@Netsc... Bookmarks The Net Netscape.co.uk Members Google Marketplace Google Search... Google Search...
CiscoSecure ACS
CISCO SYSTEMS
User Setup
Group Setup
Shared Profile Components
Network Configuration
System Configuration
Interface Configuration
Administration Control
External User Databases
Reports and Activity
Online Documentation
Applet formDispatcher started

User Setup

Supplementary User Info

Real Name Anne Brown

Description Accounts Payable

User Setup

Password Authentication:

CiscoSecure Database

CiscoSecure PAP (Also used for CHAP/MS-CHAP/ARAP, if the Separate field is not checked.)

Password *******

Confirm Password *******

□ Separate (CHAP/MS-CHAP/ARAP)

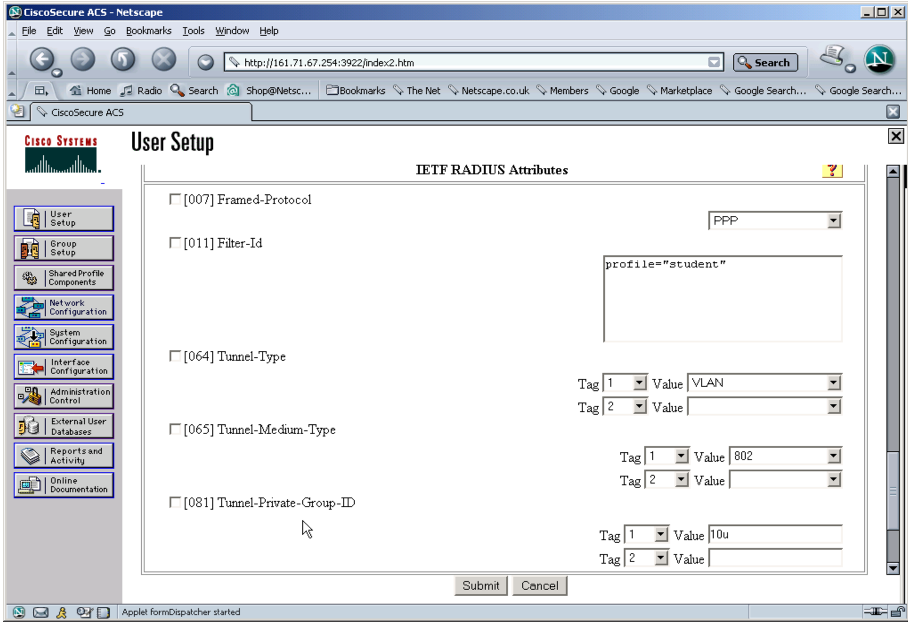
Password

Confirm Password

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.


CiscoSecure ACS - Netscape
File Edit View Go Bookmarks Tools Window Help
http://161.71.67.254:3922/index2.htm
Search
Home Radio Search Shop@Netsc... Bookmarks The Net Netscape.co.uk Members Google Marketplace Google Search... Google Search...
CiscoSecure ACS
Cisco Systems
User Setup
Group Setup
Shared Profile Components
Network Configuration
System Configuration
Interface Configuration
Administration Control
External User Databases
Reports and Activity
Online Documentation
Submit
Cancel
Applet formDispatcher started

User Setup

IETF RADIUS Attributes

□ [007] Framed-Protocol — PPP

□ [011] Filter-Id — profile="student"

□ [064] Tunnel-Type — Tag 1 Value VLAN; Tag 2 Value

□ [065] Tunnel-Medium-Type — Tag 1 Value 802; Tag 2 Value

□ [081] Tunnel-Private-Group-ID — Tag 1 Value 10u; Tag 2 Value

The RADIUS attributes need to have already been selected, see step 7 in Adding a 3Com Switch 5500G-EI 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 5500G-EI. These RADIUS attributes define the access level of the the user to the management interface.

Follow these steps:

1 Add the required RADIUS attributes to the Cisco Secure ACS server, by editing a .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
```

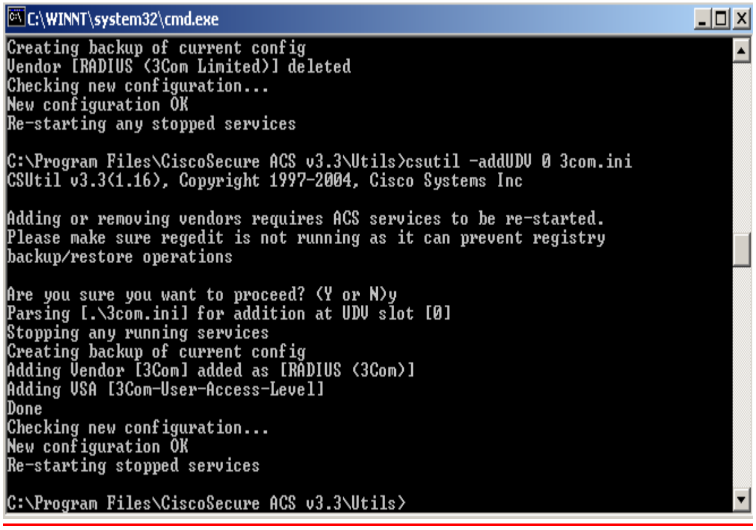
```
3=Administrator
```

b Locate the application **`csutil.exe`**. in the utils directory of the install path (eg. C:\program files\Cisco Secure ACS\utils\).

c Copy the 3Com.ini file into the utils directory

d At the command prompt enter

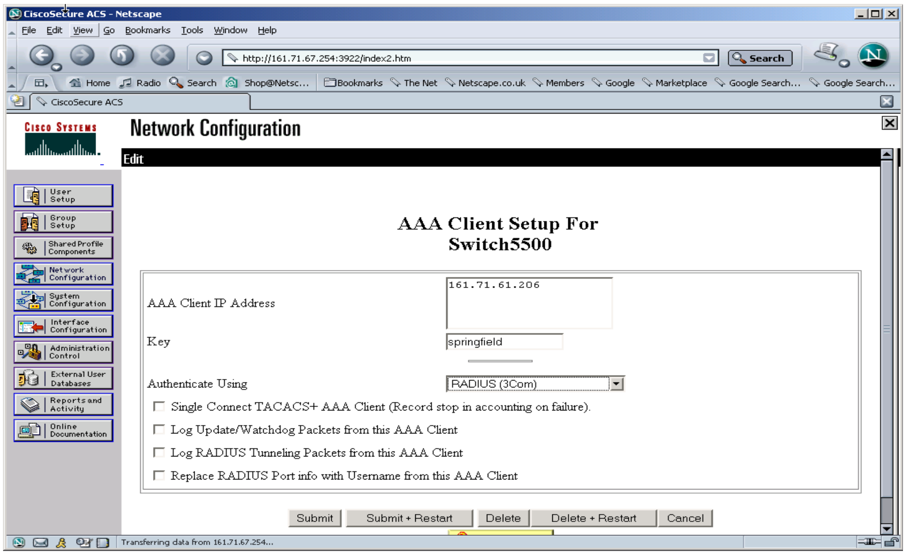
```
csutil -addUDV 0 3Com.ini
```



```
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 [.\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 VSA [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. .


CiscoSecure ACS - Netscape
File Edit View Go Bookmarks Tools Window Help
http://161.71.67.254:3922/index2.htm
Search
Home Radio Search Shop@Netsc... Bookmarks The Net Netscape.co.uk Members Google Marketplace Google Search... Google Search...
CiscoSecure ACS
CISCO SYSTEMS
Network Configuration
Edit
User Setup
Group Setup
Shared Profile Components
Network Configuration
System Configuration
Interface Configuration
Administration Control
External User Databases
Reports and Activity
Online Documentation
Submit
Submit + Restart
Delete
Delete + Restart
Cancel
Transferring data from 161.71.67.254...

AAA Client Setup For
Switch5500

AAA Client IP Address: 161.71.61.206

Key: springfield

Authenticate Using: RADIUS (3Com)

□ Single Connect TACACS+ AAA Client (Record stop in accounting on failure).

□ Log Update/Watchdog Packets from this AAA Client

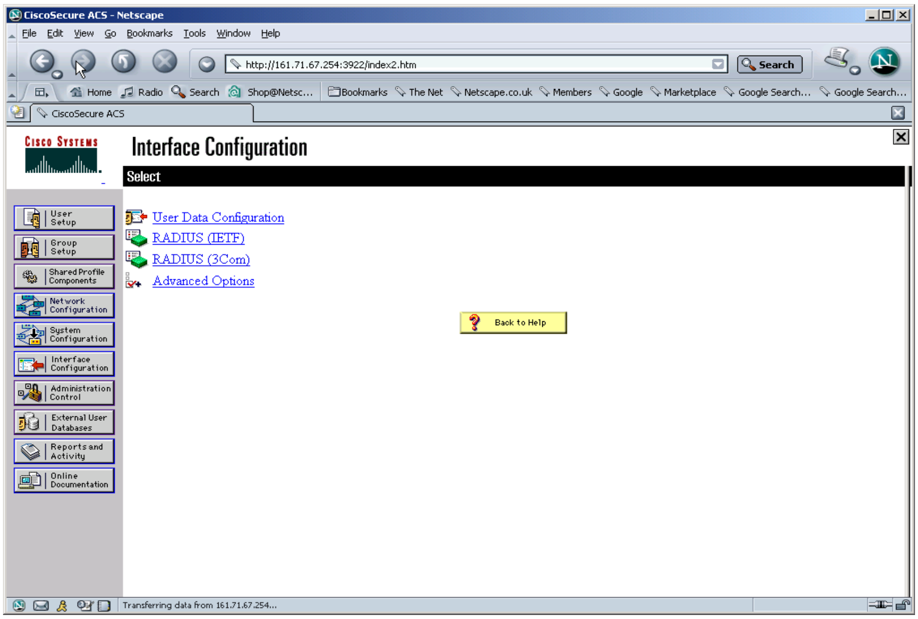
□ Log RADIUS Tunneling Packets from this AAA Client

□ Replace RADIUS Port info with Username from this AAA Client

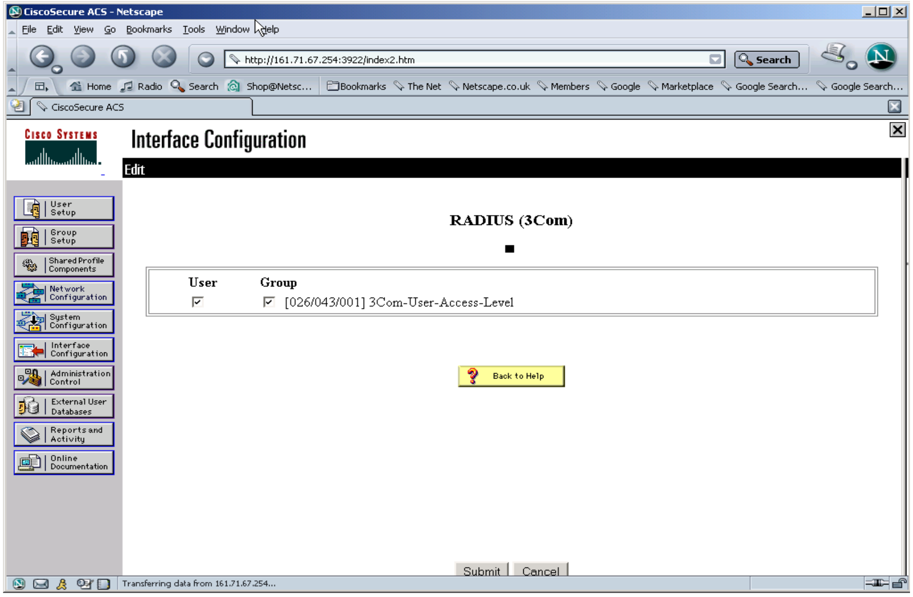
3 Select *Submit+Restart*

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)*



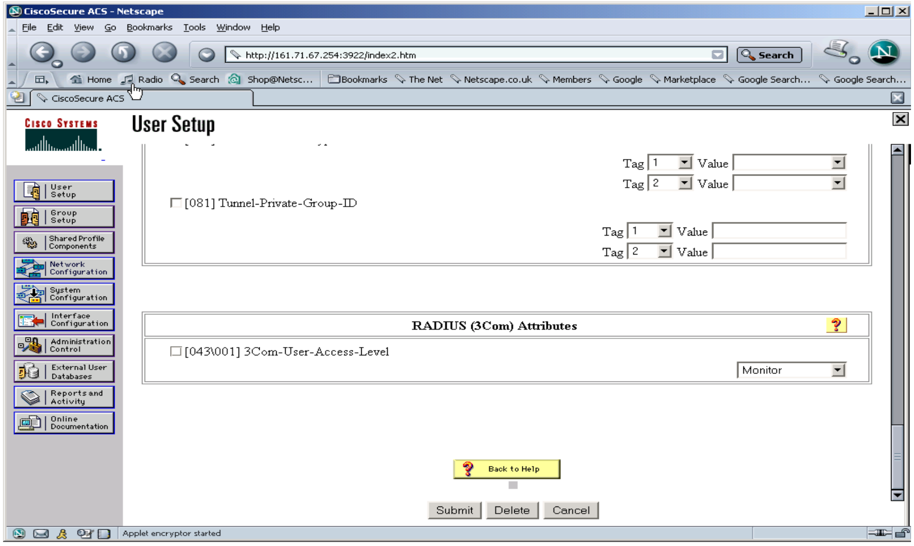
a Ensure that the *3Com-User-Access-Level* option is selected for both *User* and *Group* setup, as shown below


CiscoSecure ACS - Netscape
File Edit View Go Bookmarks Tools Window Help
http://161.71.67.254:3922/index2.htm
Search
Home Radio Search Shop@Netsc... Bookmarks The Net Netscape.co.uk Members Google Marketplace Google Search... Google Search...
CiscoSecure ACS
Cisco Systems
Interface Configuration
Edit
User Setup
Group Setup
Shared Profile Components
Network Configuration
System Configuration
Interface Configuration
Administration Control
External User Databases
Reports and Activity
Online Documentation
Back to Help
Submit
Cancel
Transferring data from 161.71.67.254...

RADIUS (3Com)

User	Group
☑	☑ [026/043/001] 3Com-User-Access-Level

5 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 5500G-EI by scrolling to the bottom of the user profile where there should be the option for configuring the access level as shown below:

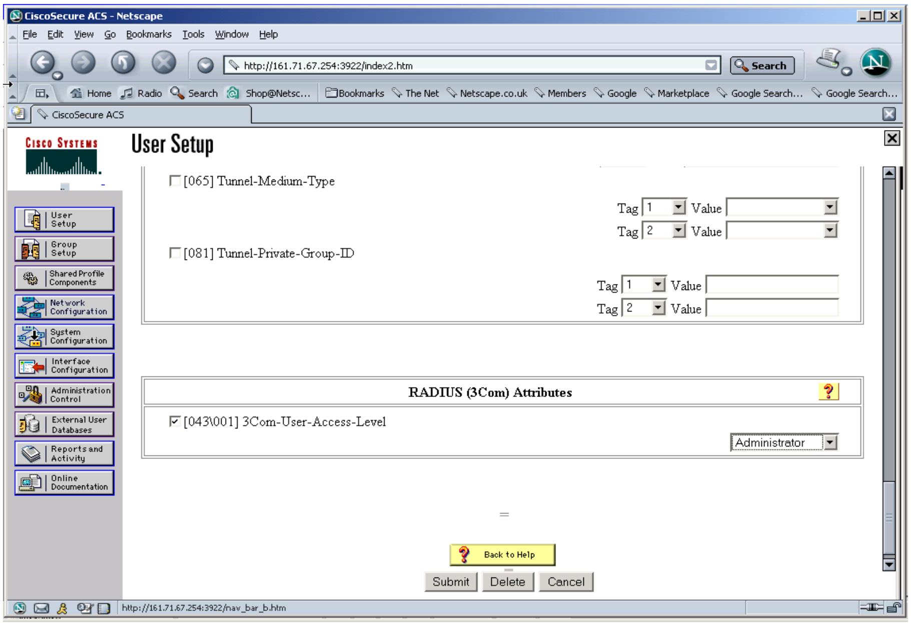


Tag 1 Value
Tag 2 Value
□ [081] Tunnel-Private-Group-ID
Tag 1 Value
Tag 2 Value

RADIUS (3Com) Attributes

□ [043\001] 3Com-User-Access-Level
Monitor

6 In the *RADIUS (3Com) Attribute* box , check *3Com-User-Access-Level* and select *Administrator* from the pull down list, see below:


CiscoSecure ACS - Netscape
File Edit View Go Bookmarks Tools Window Help
http://161.71.67.254:3922/index2.htm
Search
Home Radio Search Shop@Netsc... Bookmarks The Net Netscape.co.uk Members Google Marketplace Google Search... Google Search...
CiscoSecure ACS
CISCO SYSTEMS
User Setup
User Setup
Group Setup
Shared Profile Components
Network Configuration
System Configuration
Interface Configuration
Administration Control
External User Databases
Reports and Activity
Online Documentation
Back to Help
Submit
Delete
Cancel
http://161.71.67.254:3922/nav_bar_b.htm

□ [065] Tunnel-Medium-Type
Tag 1 Value
Tag 2 Value
□ [081] Tunnel-Private-Group-ID
Tag 1 Value
Tag 2 Value

RADIUS (3Com) Attributes

☑ [043\001] 3Com-User-Access-Level
Administrator

7 Select *Submit*.

The Switch 5500G-EI can now be managed by the Network Administrator through the CISCO Secure ACS server.

D 3Com XRN

This section explains what 3Com XRN™ (eXpandable Resilient Networking) is and how you can use it to benefit your network. It also explains how to implement XRN on your network.

This chapter contains the following sections:

The sections below provide supplementary information that are not essential reading, but may be of interest to advanced users.

For detailed descriptions of the web interface operations and the command line interface (CLI) commands that you require to manage the Switch please refer to the Command Reference Guide supplied in PDF format on the CD-ROM that accompanies your Switch or on the 3Com Web site.

What is XRN?

XRN (eXpandable Resilient Network) is a 3Com LAN technology built into the software and hardware of your Switch that offers high availability, scalability, and connectivity.

Supported Switches

XRN is supported by the 3Com Operating System on the following Switches installed with Version 1.0 software or later:

Table 463 SuperStack 4 Switch 5500G-EI Support for XRN Distributed Fabric

SuperStack 4 Switch	XRN support
Switch 5500G-EI 24-Port (3CR17254-91) (no PSU)	Full XRN functionality
Switch 5500G-EI 48-Port (3CR17255-91) (no PSU)	Full XRN functionality
Switch 5500G-EI 24 Port (3CR17259-910 (no PSU)	Full XRN functionality

XRN is standards based. The 3Com only proprietary technology operates across the Fabric Interconnect ports.

XRN Terminology

This section contains a glossary of the common XRN terminology.

eXpandable Resilient Network (XRN) XRN is developed by 3Com that allows you to implement fault tolerant, high performance and scalable multilayer networks.

Fabric Interconnect Fabric Interconnect is the interconnection between XRN Switches that form the Distributed Fabric.

XRN Distributed Fabric (Distributed Fabric) XRN Distributed Fabric is the term used to describe interconnected devices supporting XRN.

Distributed Device Management (DDM) DDM allows Switches in the XRN Distributed Fabric to behave as a single managed entity, irrespective of the form factor or Switch deployed. For further information see page 431.

Distributed Link Aggregation (DLA) DLA is the configuration of Aggregated Links across interconnected devices in the Distributed Fabric. 3Com and non-3Com devices can connect to the XRN Distributed Fabric using DLA. For further information see page 432.

Distributed Resilient Routing (DRR) DRR provides distributed routing and router resiliency across an XRN Distributed Fabric. For further information see page 431.

Benefits of XRN

The benefits of XRN include:

- Increased environmental resilience provided by:
  - Hardware and Software redundancy per unit or across the Distributed Fabric.
  - Distributed management across the Distributed Fabric.
  - Distributed Link Aggregation across the Distributed Fabric.
  - Distributed Resilient Routing across the Distributed Fabric.
- Increased network performance provided by:

  - Switching capacity that increases as you add a Switch to the Fabric. So network performance and resilience expand as the Fabric grows.
  - Link Aggregation supported across the Distributed Fabric.
- Flexibility provided by:
  - Support across any of the Switches within an individual SuperStack 4 Switch 5500G-EI family to create an XRN Distributed Fabric.

XRN Features

This section describes the key features of XRN.

Distributed Device Management (DDM)

DDM provides single IP address management across the interconnected Switches that form the Distributed Fabric. This allows the entire Distributed Fabric to be managed and configured as a single managed entity. In the event of failure in one of the Switches in the Distributed Fabric, management access to the remaining Switch is retained on the same IP address.

DDM allows you to manage the Distributed Fabric via the command line interface (CLI), Web interface, or SNMP.

DDM provides you with the ability to carry out the following:

- Single step Switch software upgrades across the Distributed Fabric (provided the Switches are of the same family).
- Distributed Fabric-wide configuration of all software features.
- Configuration of port-specific software features across the Distributed Fabric via a single management interface.

Distributed Resilient Routing (DRR)

DRR allows the Switches in the Distributed Fabric to act as a single logical router which provides router resiliency in the event of failure in one of the interconnected Switches. With DRR, Switches in the Distributed Fabric are routing, which significantly increases the overall Layer 3 capacity of the core of the network.

DRR can intelligently distribute the routing load across both Switches in the Distributed Fabric, which maximizes routing performance and makes full use of bandwidth capacity.

Switches in the Distributed Fabric provide Layer 3 local forwarding for directly connected hosts and devices.

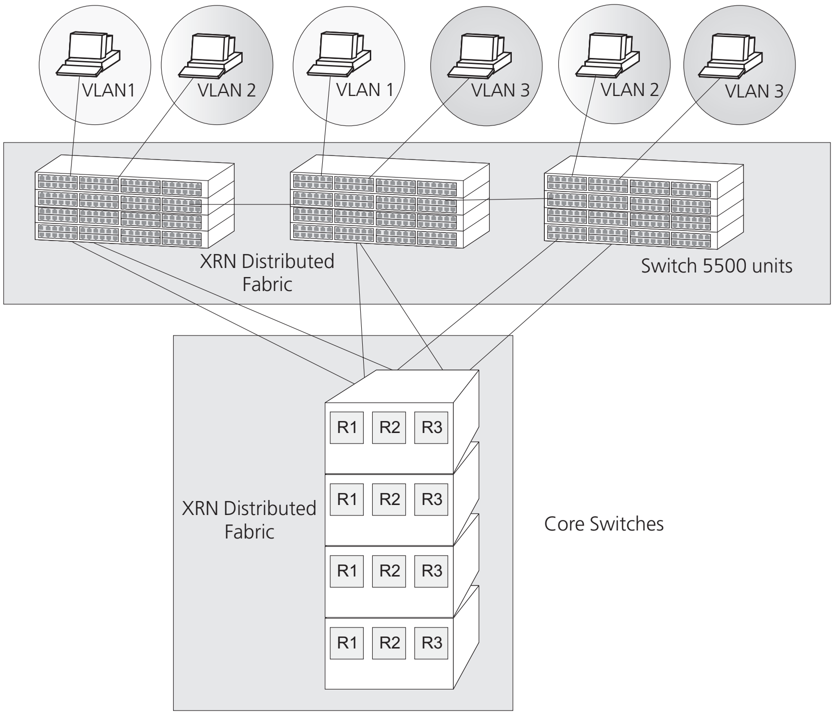
Switch units within the Distributed Fabric provide the same router interfaces and mirror each other’s routing tables. This allows each unit to keep the routing local to the unit for locally connected hosts and devices.

In the example shown in Figure 106, there is a single logical router across the XRN Distributed Fabric with router interfaces (R1, R2, and R3) shared by both units.

If there is a loss of a unit in an XRN Distributed Fabric it does not affect routing provided you are using Distributed Link Aggregation or the devices in the wiring closet are multihomed.

DRR is an XRN-specific implementation that only operates on XRN within the Distributed Fabric. However it will interoperate with other routers outside of the XRN Distributed Fabric.

Figure 106 Network Example illustrating Distributed Resilient Routing



Distributed Link Aggregation (DLA)

DLA ensures that all member ports of an aggregated link distribute the traffic flow across the Distributed Fabric. This provides resilience and enhanced performance. Failure in one of the member links in the Aggregated Link will not affect communication to the Distributed Fabric as traffic will be forwarded via the remaining member links. **Distributed Link Aggregation Example**

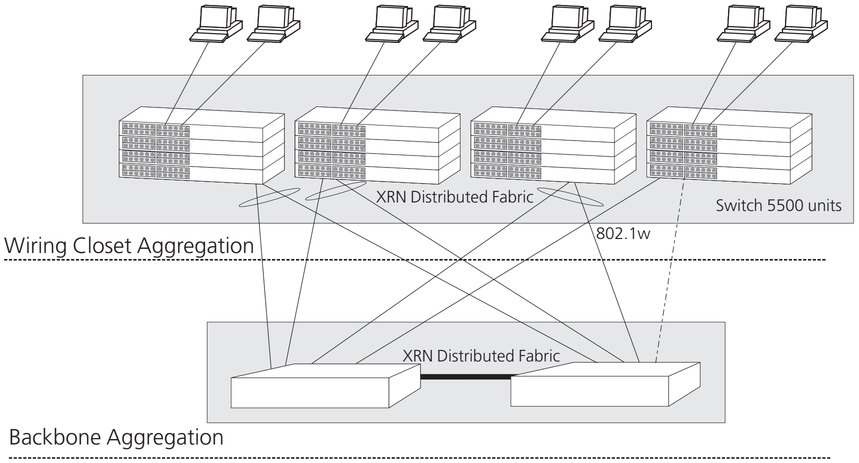
You can also use DLA to create highly resilient network backbones, supporting multihomed links to the wiring closets as shown in Figure 107.

Intelligent local forwarding ensures that each Switch in the XRN Distributed Fabric forwards traffic to local Link Aggregation ports rather than across the Fabric Interconnect, thereby reducing network traffic.

You can also use resilient links or STP/RSTP for resilience, however, this does not provide the bandwidth advantage of link aggregation.

For more information about STP/RSTP refer to Chapter 5 "Network Protocol Operation".

Figure 107 Distributed Link Aggregation at the Network Backbone



How to Implement XRN — Overview

This section provides an overview on how to implement XRN in your network. Following the steps below will ensure that your XRN network operates correctly.

1 Design your network using XRN Distributed Fabrics, taking into account all the important considerations and recommendations (see "Important Considerations and Recommendations" on page 434).

2 Ensure that the Switches you plan to interconnect to create an XRN Distributed Fabric are of the same Family and are running the same version of software.

3 Create the XRN Distributed Fabric as follows:

- **Switch 5500G-EI Family** — via the built-in dedicated Fabric ports connected using a stacking cable as described in the "Creating an XRN Distributed Fabric" Chapter in the Getting Started Guide that accompanies your Switch.

Once the Switches are interconnected to create an XRN Distributed Fabric, they behave as if they were one Switch and can be managed via a single IP address.

4 Set up the IP information so you can begin managing and configuring the Switches in the Distributed Fabric.

For more information on setting up IP information for your Switch so it is ready for management, refer to the Getting Started Guide that accompanies your Switch.

5 If VLANs are required (for example, if the network is in a Layer 3 environment), create the VLANs and assign VLAN membership to all ports.

6 Configure the Aggregated Links either manually or automatically via LACP, ensuring they are tagged members of all VLANs.

7 Configure the router IP interfaces.

For detailed descriptions of the web interface operations and the command line interface (CLI) commands that you require to manage the Switch please refer to *the Command Guide supplied in PDF format on the CD-ROM that accompanies your Switch or on the 3Com Web site.*

Important Considerations and Recommendations

This section contains important points and recommendations that you need to consider or be aware of when designing a network using XRN .

- Bandwidth across the XRN Interconnect is detailed in Table 464. Intelligent Local Forwarding and DRR ensures efficient use of bandwidth across the Fabric Interconnect.

Table 464 Bandwidth across the XRN Interconnect

Switch Model	Bandwidth across the XRN Interconnect
Switch 5500G-EI	48 Gbps, 96 Gbps (full duplex)

- When you create a Distributed Fabric the relevant port-based tables do not double in size, they remain as they were.
- When Switch 5500G-EI units are in an XRN Distributed Fabric their unit IDs are user configurable.
- The maximum number of Switch units that can be interconnected is shown in Table 465.

Table 465 Number of Switch units that can create an XRN Distributed Fabric

Switch Model	Max number of units	Method
Switch 5500G-EI	8	Loop

- It is not possible to create an XRN Distributed Fabric with Switches from different SuperStack 4 5500 families, for example, a Switch 5500-EI with a 5500G-EI. You can only use Switches within an individual SuperStack 4 5500 family to create an XRN Distributed Fabric, for example, a Switch 5500G-EI 52-Port with a Switch 5500G-EI 28-Port.
- 3Com strongly recommends that you upgrade all Switches to be interconnected to the latest software agent.
- 3Com recommends that you initialize a Switch unit that has previously been used elsewhere in your network before you interconnect to an existing unit. If you do not initialize the unit, problems may be caused by conflicting Switch configurations.
- When a port is operating in XRN mode it will no longer be configurable in the normal way, that is, you cannot control port features such as auto-negotiation, VLANs, static addresses, STP, Aggregated Links, Resilient Links, and so on.

Recommendations for Achieving Maximum Resilience

To achieve maximum network-level resilience 3Com recommends that:

- Servers and wiring closets are multihomed. That is, each server or wiring closet is connected to both units within the Distributed Fabric.
- On all multi-homed links you use link aggregation (preferably configured automatically via LACP rather than configured manually) across an XRN Distributed Fabric, and you have STP/RSTP enabled across your network. (See “Legacy Aggregated Links” on page 439 for more information.)

If you are unable to use link aggregation on multihomed links, then STP/RSTP should be used as the second option, and the last option would be to use resilient links.

This implementation increases the level of fault tolerance as it also protects against loss of the physical interfaces at the core.

- If you use the Switch 5500 in a Distributed Fabric further resilience can be achieved by utilising a redundant power source.
- You always have STP/RSTP enabled on your network to prevent the risk of loops occuring if you have links that are multihomed, particularly if you are using link aggregation.
- All multihomed links and alternate paths must carry *all* VLANs, and packets must be tagged.
- The Distributed Fabric is the STP root bridge.
- Individual port members of each aggregated link must have VLAN membership manually configured before the aggregated link is set up. You must not rely on port members inheriting VLAN membership configuration from the aggregated link. (See “VLANs” on page 438 for more information.)
- If you are using resilient links, these must be configured on the remote unit, not on the units within the Distributed Fabric.

If you follow the 3Com recommendations, should there be a unit or interconnect failure within the Distributed Fabric, traffic flow will be maintained at all times. If you want to know more detail about how the Distributed Fabric behaves in certain failure scenarios, see “How a Failure affects the Distributed Fabric” *on* page 441.

Unit ID Numbering Mechanism

This section outlines the mechanisms that the Switch 5500G-EI Family uses to determine the unit IDs for management purposes.

When a Fabric is created using the Switch 5500G-EI the unit numbering can be determined in two ways.

- You can manually assign unit IDs 1 to 8 to specific units using the `Change[self-unit, unit-id] to [1-8, auto-numbering]` command from the System View. If you manually assign unit IDs to a Switch via the `change` command the IDs will be retained after a power cycle.

  If you add a unit to a Fabric that has previously been manually configured with a unit ID and this conflicts with an ID already within the Fabric, then the Switch with the lowest MAC address assumes the ID in question and the other unit will automatically renumber.

3Com recommends that you manually assign the unit IDs within the Fabric if you wish to have predictability of knowing which units have which IDs at all times.

- Fabric topology is ‘discovered’ and the units auto-number their IDs.

Adding and removing units from the Fabric does not cause any renumbering to occur and the Fabric will continue to work normally. Renumbering only occurs when the Fabric is next power cycled if the units are configured to auto-number.

The unit LEDs will display the unit number in the Fabric, from 1 to 8.

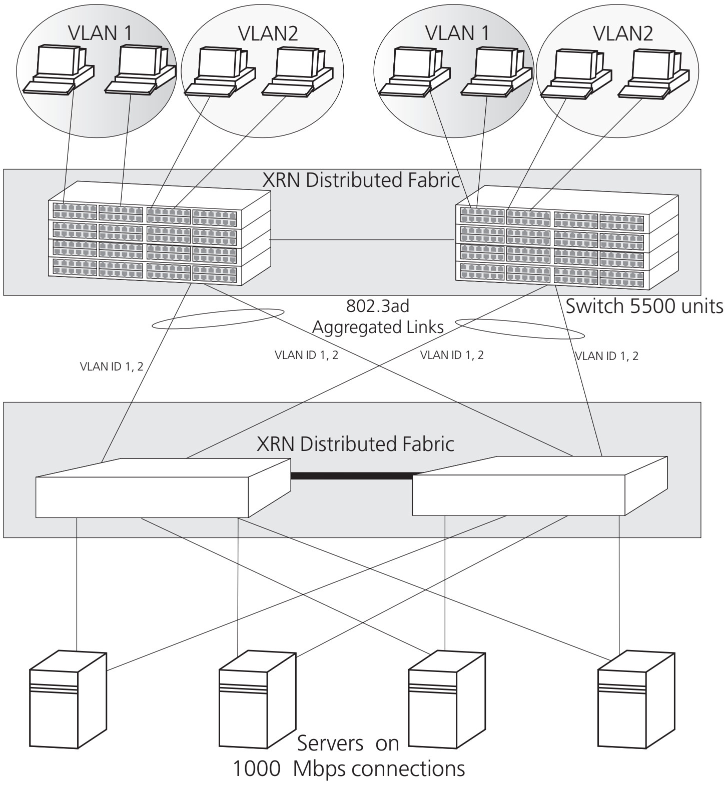
Network Example using XRN

The following example explains how to set up XRN in a network to gain maximum resilence using two Distributed Fabrics. The same process scales for larger networks if you are using multiple XRN Distributed Fabrics.

XRN Distributed Fabric Network

The example in Figure 108 shows a network with two Switches interconnected to create a single XRN Distributed Fabric in the Server Distribution section of the network, this Fabric in turn is connected to a Fabric within the Core of the network. The servers are multi-homed as are the Switch 5500G-EI Fabrics to create a highly resilient network.

Figure 108 A Dual XRN Distributed Fabric Network



How to Set up this Network

This section provides information on how to configure an XRN network as shown in Figure 108. It assumes you have carried out steps 1 to 4 as detailed in "How to Implement XRN — Overview" on page 433.

1 Enable LACP on the required ports, ensuring you have not connected your devices to the Distributed Fabric yet as you must configure your VLANs before the aggregated links are configured. Individual port members of each aggregated link must have VLAN membership explicitly set, that is, manually configured, before the aggregated link is set up. You must not rely on port members inheriting VLAN membership configuration from the aggregated link.

2 Create the VLANs and assign VLAN membership to all ports.

3. Connect up your ports. As LACP was enabled in step 1 the aggregated links will now automatically configure themselves.
4. Configure the router IP interfaces.
5. Ensure that RSTP is enabled across the network.

Legacy aggregated links are not resilient to an interconnect failure. Hence the 3Com recommendation to use IEEE 802.3ad aggregated links (LACP) for maximum resilience.

If an automatic aggregated link (created by LACP) contains ports with different VLAN membership, the aggregated link will inherit the VLAN memberhip of the first port that comes up in the aggregated link. It will override any pre-defined VLAN membership for the aggregated link.

Recovering your XRN Network

In the event of a failure within your XRN network, 3Com recommends that you follow the recommendations below.

Unit Failure

The steps below outline the procedure to recover your XRN network in the event of a unit failure within your Distributed Fabric.

1. Obtain a Switch and ensure it is installed with the same software version as the failed Switch.
2. Initialise the new Switch so it is operating with its factory default settings.
3. Connect the new Switch to the operational Switch to form the Distributed Fabric.
4. IP interfaces and VLANs will be converged between the Switches, that is, IP interfaces and the creation of the VLANs is done automatically on the new Switch. However, any port-based configuration must be done manually.
5. If any Switch features, for example, IGMP snooping or passwords are not set to default state then these should be reset after the new Distributed Fabric has been formed.

Interconnect Failure

The steps below outline the procedure to recover your XRN network in the event of an interconnect failure within your Distributed Fabric.

1. Obtain a new cable.
2. Install the new cable.

How XRN Interacts with other 3Com Switches

This section provides guidelines on connecting legacy and new 3Com Switches (including non-XRN enabled Switches) to an XRN Distributed Fabric. Table 466 lists the features supported by the Switches that can be used when connecting to a Distributed Fabric.

For detailed information on how the Switch features interact with XRN , refer to the following section "How XRN Interacts with other Features" on page 438.

Table 466 Features supported by 3Com Switches connecting to an XRN Distributed Fabric

3Com Switch	Resilient Links	STP/ RSTP	MSTP	Manual Link Aggregations	LACP Link Aggregations
SuperStack II Switch 1100 Family	Yes	Yes	No	Yes	No

3Com Switch	Resilient Links	STP/ RSTP	MSTP	Manual Link Aggregations	LACP Link Aggregations
SuperStack 3 Switch 3300 Family	Yes	Yes	No	Yes	No
SuperStack 3 Switch 4200 Family	Yes	Yes	No	Yes	Yes
SuperStack 3 Switch 4400 Family	Yes	Yes	No	Yes	Yes
SuperStack II Switch 3800	No	Yes	No	Yes	Yes
SuperStack 3 Switch 4900 Family	Yes	Yes	No	Yes	Yes
3Com Switch 40x0 Family	Yes	Yes	No	Yes	Yes
3Com Switch 4005	No	Yes	No	Yes	Yes
3Com Switch 4007	No	Yes	No	Yes	No
3Com Switch 5500 Family	No	Yes	No	Yes	**Yes**
3Com Switch 5500G Family	No	Yes	No	Yes	**Yes**
3Com Switch 7700	No	Yes	Yes	Yes	No
3Com Switch 8800	No	Yes	Yes	Yes	No

How XRN Interacts with other Features

This section provides supplementary information on how XRN interacts with other software features supported by your Switch.

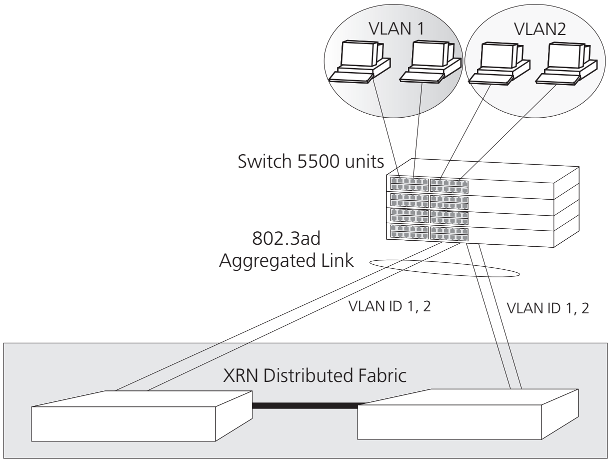
VLANs

Figure 109 shows a single aggregated link, created automatically via LACP, connecting the Switch 5500G-EI stack to the Distributed Fabric. The Distributed Fabric will take its VLAN membership from a port within the Switch 5500G-EI stack .

If the Fabric Interconnect fails the aggregated link will split, creating two separate aggregated links (as shown in Figure 110). If the ports within the Switch 5500G-EI stack each have different VLAN membership, this will mean the two newly formed aggregated links will also have different VLAN membership. This will result in the different VLANs not being able to communicate.

3Com recommends that you set individual ports that are to be members of an aggregated link to the same VLAN membership. This ensures communication between all VLANs at all times.

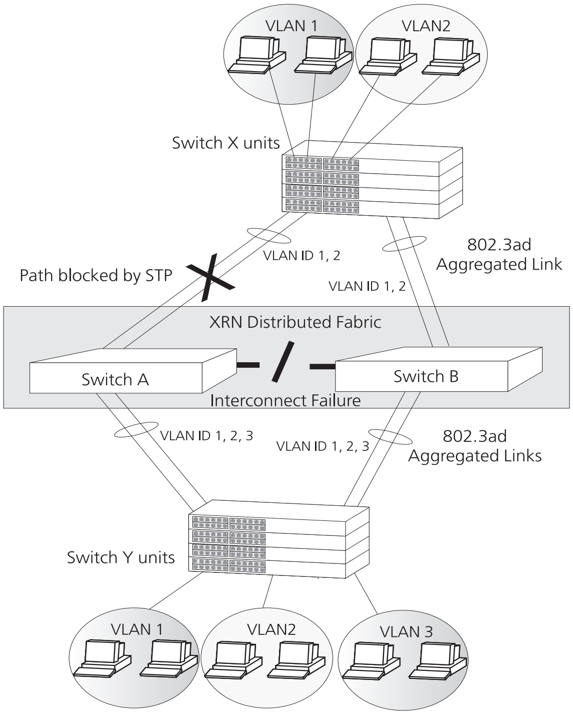
Figure 109 How XRN interacts with VLANs — Example 1



The Distributed Resilient Routing (DRR) feature also requires that all units can communicate with each other on all VLANs. This ensures that on an interconnect failure all units can communicate with each other.

For example in Figure 110 the interconnect has failed and only one of the units in the Distributed Fabric will act as the router. STP will detect a potential loop and block a path of its choosing, in this example it has blocked the path between Switch X units and Switch A. If ports have different VLAN membership as shown here there will be loss of communication between VLANs 1 and 2.

Figure 110 How XRN interacts with VLANs — Example 2



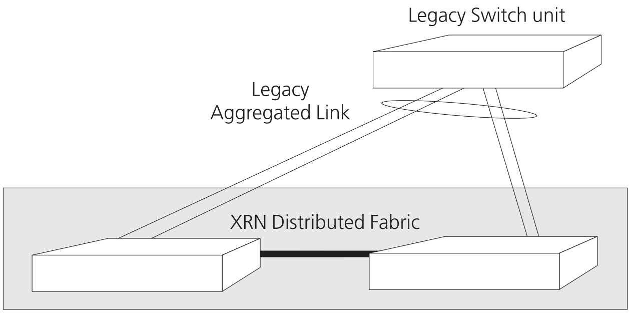
Legacy Aggregated Links

Legacy aggregated links, will react in the normal way if a unit within the Distributed Fabric fails, that is, all traffic will be redirected down the link(s) to the unit that is still operating.

However, in Figure 111, if the interconnect fails, the aggregation is still a single logical entity at the legacy Switch end, but it is now split over both units within the Distributed Fabric. The legacy Switch is not aware that the aggregation has split and will continue to send traffic over both links, resulting in data loss.

Hence the recommendation to use IEEE 802.3ad aggregated links, if possible, as legacy aggregated links are not resilient to an Fabric Interconnect failure.

Figure 111 How XRN interacts with legacy aggregated links

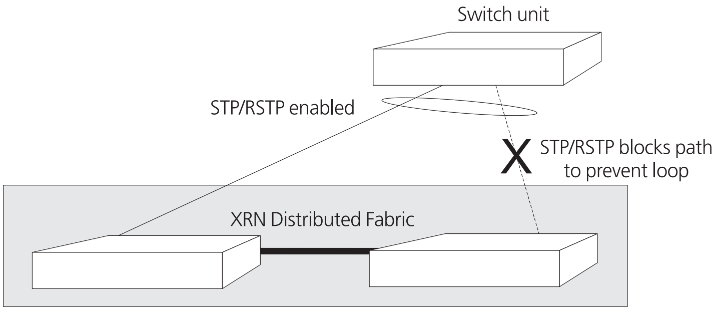


STP/RSTP

STP/RSTP should be used for multihomed links if you are not able to use aggregated links. Figure 112 shows how STP will prevent a loop occuring on a multihomed link.

STP/RSTP should always be enabled if your multihomed links are aggregated links. Figure 110 shows how, on interconnect failure, STP/RSTP will detect the potential loop caused by the aggregated links splitting and block a path to prevent the loop occuring.

Figure 112 How XRN interacts with STP/RSTP



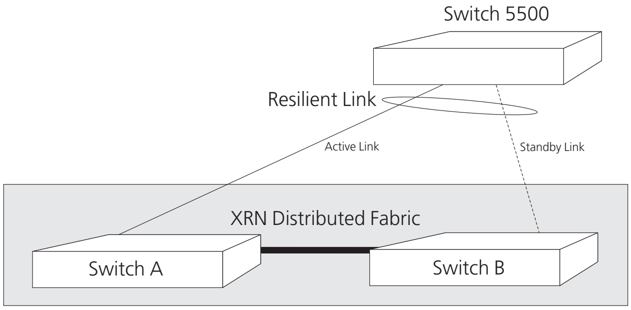
Resilient Links

In Figure 113, if Switch A within the Distributed Fabric fails, the Switch 3300 will detect that a link has gone down and will make the standby link to Switch B active and pass all traffic down the link to Switch B.

When using resilient links in a Distributed Fabric network the resilient links must be configured at the remote end rather than at the Distributed Fabric. In a unit failure scenario as described above it would not matter if the resilient links were configured at the Distributed Fabric end. However, on an interconnect failure it would matter.

For example, if the resilient links were configured on Switches A and B, if the interconnect fails, both Switches will detect a failed link to Switch 3300 and both A and B will activate their links to Switch 3300. So both links in the resilient link will be passing traffic, potentially causing a loop in the network.

Figure 113 How XRN interacts with Resilient Links



How a Failure affects the Distributed Fabric

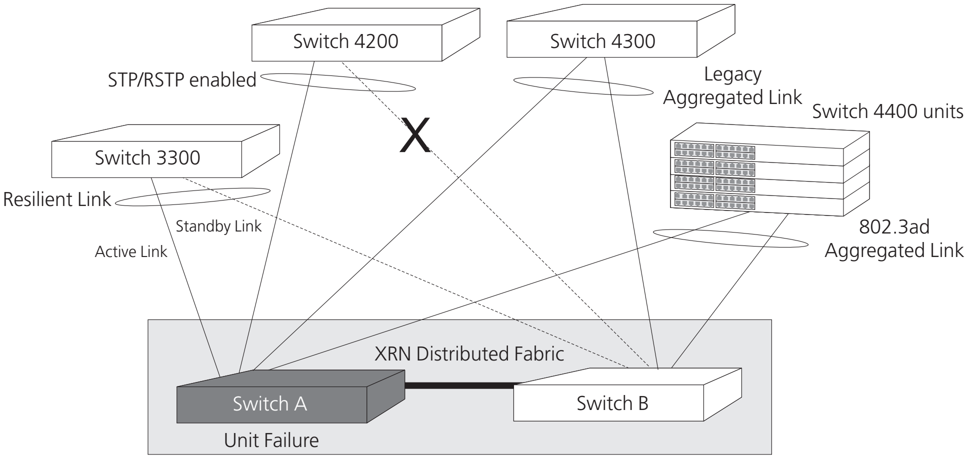
This section provides supplementary information on how the Distributed Fabric and traffic flow is affected by failure of an Fabric Interconnect and of a unit in the Distributed Fabric.

Loss of a Switch within the XRN Distributed Fabric

When a Switch unit in the Distributed Fabric fails, assuming you have followed the recommendations in "Important Considerations and Recommendations" on page 434, your traffic flow should continue through your network.

The way the network reacts depends upon which features are configured on which links. For example, Figure 114 shows an XRN network where all the edge devices are connected to the Distributed Fabric using a range of supported features, some of which are legacy features.

Figure 114 XRN Network reaction on Distributed Fabric unit failure



Should Switch A fail, the network will react in the following way:

LACP (IEEE 802.3ad) and Legacy Aggregated Links

The Switch 4400 and Switch 4300 Aggregated Links will reroute all traffic down the link connected to Switch B.

Legacy STP (IEEE802.1D) and RSTP (IEEE 802.1w)

The Switch 4200 is using legacy STP. STP will reconfigure the network to open the previously blocked link to Switch B. The STP reconfiguration will cause all Switch forwarding databases (MAC address tables) to be fast aged (if using RSTP, they will be flushed).

Resilient Links

The Switch 3300 is using resilient links, which should be set up at the 3300 end of the link. The Switch 3300 will detect the unit failure and activate the link to Switch B

VLANs

Any VLANs will not be affected by unit failure.

Router

Switch B will continue to do all the routing. As it was routing prior to Switch A's failure there will be no change of the router identity, that is, the router interface IP addresses will not change. The router interface MAC addresses may change but this will have no visible impact on your network. Any MAC address change is propogated to your network by the issuing of gratuitous ARP messages.

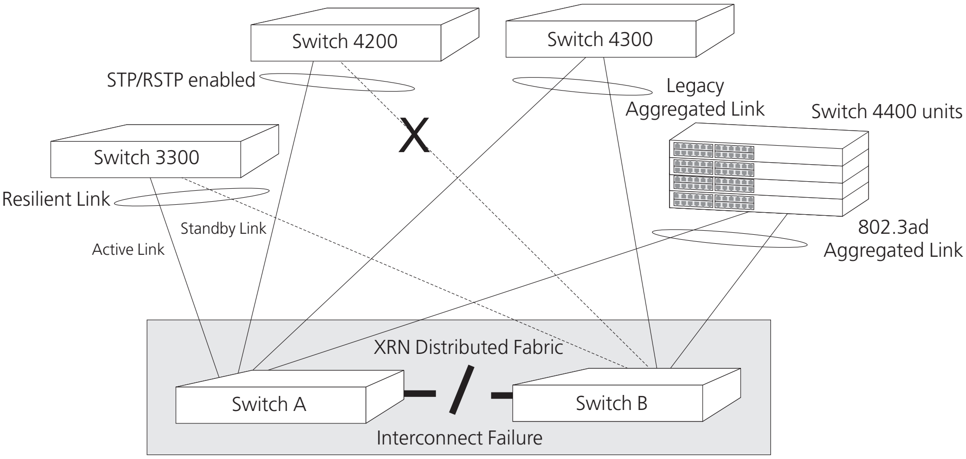
Switch A Recovery

When Switch A recovers and starts to operate again, all links will reconfigure themselves as they were before the failure, according to the protocols used. The routing task will once again be shared between Switches A and B, using the same IP address.

Loss of the Fabric Interconnect

When an interconnect fails between two Switches in the Distributed Fabric, assuming you have STP/RSTP and LACP enabled as recommended in "Important Considerations and Recommendations" on page 434, your traffic flow should continue through your network.

Figure 115 XRN Network reaction on Fabric Interconnect failure



In Figure 115, if the interconnect fails, the network will react in the following way:

LACP (IEEE 802.3ad) and Legacy Aggregated Links

The Switch 4400 automatically configured aggregated link (LACP) will reconfigure itself to create two separate aggregated links.

The Switch 4300 legacy aggregated link will be split between the two Switches in the Distributed Fabric and will no longer operate and will cause network disruption.

Legacy aggregated links are not resilient to an interconnect failure. Hence the 3Com recommendation to use IEEE 802.3ad aggregated links (LACP) for maximum resilience.

IEEE802.1D (Legacy STP) and RSTP

The Switch 4200 is using legacy STP. STP (and RSTP) will reconfigure the network to open the previously blocked link to Switch B. The STP reconfiguration will cause all Switch forwarding databases (MAC address tables) to be fast aged (if using RSTP, they will be flushed). If STP is enabled throughout the network, it will reconfigure the network to ensure that no loops occur due to split aggregated links.

If the Distributed Fabric has been configured to be the root bridge in the network then this will encourage STP to maintain the traffic flow through the shortest paths in the event of an Fabric Interconnect failure.

Resilient Links

The Switch 3300 will continue to send traffic down the active link to Switch A and keep the link to Switch B in standby mode.

VLANs

As all VLANs will have been configured on all links, the traffic will still reach its destination via the paths that remain open.

Router

Initially both Switches continue to route. Simultaneously the Switches attempt to contact each other and carry out a process that determines which Switch will become the Layer 3 router and which Switch will become the Layer 2 bridge. This avoids the scenario of two different and independent routers operating with the same identity.

Interconnect Recovery

When the interconnect recovers and starts to operate again, all links will reconfigure themselves as they were before the failure, according to the protocols used. The routing task will once again be shared between Switches A and B, using the same IP address.