DXS-F3500 Series
Configuration Guide

DXS-F3500-32S | DXS-F3500-64S





Product photo for illustration only. Actual appearance may vary by hardware version and regional release.

October 2026

Notice

Specifications are subject to change without notice. D-Link is a registered trademark of D-Link Corporation and its overseas subsidiaries. All other trademarks belong to their respective owners.

Support: qr.dlink-me.com/support/

Contents

01 Configuration Preparation 4
02 Basic Configuration 9
03 Network Management Configuration 21
04 Security Configuration 24
05 Web Configuration 54
06 Interface Configuration 123
07 Interface Range Configuration 135
08 Port Physical Characteristic Configuration 138
09 Port Additional Characteristics Configuration 147
10 Port Mirroring Configuration 153
11 MAC Address Table Configuration 158
12 MAC Access List Configuration 162
13 802.1x Configuration 166
14 VLAN Configuration 177
15 GVRP Configuration 193
16 Private VLAN Settings 198
17 STP Configuration 206
18 STP Optional Characteristic Configuration 240
19 Link Aggregation Configuration 254
20 PDP Configuration 260
21 LLDP Configuration 265
22 EAPS Configuration 290
23 IGMP-Snooping Configuration 302
24 IGMP-proxy Configuration 316
25 DHCP-Snooping Configuration 322
26 Layer 2 Tunnel Protocol Configuration 334
27 QoS Configuration 338
28 DoS Attack Prevention Configuration 353
29 Attack Prevention Configuration 358
30 Network Protocol Configuration 366
31 IP ACL Application Configuration 398
32 Routing Protocol Configuration 401
33 IP Hardware Subnet Routing Configuration 479
34 IP-PBR Configuration 483
35 Multi-VRF CE Configuration 489
36 Reliability Configuration 504
37 Multicast Configuration 512
38 IPv6 Configuration 542
39 ND Configuration 558
40 OSPFv3 Configuration 564
41 NTP Configuration 580
42 IPv6 ACL Configuration 585
43 Time Range Configuration 590
44 uRPF Configuration 597

Configuration Preparation

Table of Contents

Chapter 1 Configuration Preparation....1
1.1 Port Number of the Switch....1
1.2 Preparation Before Switch Startup....1
1.3 Acquiring Help....2
1.4 Command Modes....2
1.5 Canceling a Command....3
1.6 Saving Configuration....3

Chapter 1 Configuration Preparation

The chapter mainly describes the following preparatory works before you configure the switch at the first time:

- Port number of the switch
- Preparation before switch startup
- How to get help
- Command mode
- Cancelling a command
- Saving configuration

1.1 Port Number of the Switch

The physical port of the switch is numbered in the **<type><slot>/<port>** form. The type-to-name table is shown as follows:

Interface Type	Name	Simplified Name
10M Ethernet	Ethernet	e
100M fast Ethernet	FastEthernet	f
1000M Ethernet	GigaEthernet	g

The expansion slot number to mark and set ports must be the number **0**. Other expansion slots are numbered from left to right, starting from **1**.

The ports in the same expansion slot are numbered according to the order from top to bottom and the order from left to right, starting from **1**. If only one port exists, the port number is **1**.

Note:

Ports in each kind of modulars must be numbered sequently from top to bottom and from left to right.

1.2 Preparation Before Switch Startup

Do the following preparatory works before the switch is configured:

(1) Set the switch's hardware according to the requirements of the manual.

(2) Configure a PC terminal simulation program.

(3) Determine the IP address layout for the IP network protocols.

1.3 Acquiring Help

Use the question mark (?) and the direction mark to help you enter commands:

- Enter a question mark. The currently available command list is displayed.

  Switch> ?

- Enter several familiar characters and press the space key. The available command list starting with the entered familiar characters is displayed.

  Switch> s?

- Enter a command, press the space key and enter the question mark. The command parameter list is displayed.

  Switch> show ?

- Press the “up” key and the commands entered before can be displayed. Continue to press the “up” key and more commands are to be displayed. After that, press the “down” key and the next command to be entered is displayed under the current command.

1.4 Command Modes

The command line interfaces for the switch can be classified into several modes. Each command mode enables you to configure different groupware. The command that can be used currently is up to the command mode where you are. You can enter the question mark in different command modes to obtain the available command list. Common command modes are listed in the following table:

Command Mode	Login Mode	Prompt	Exit Mode
System monitoring mode	Enter **Ctrl-p** after the power is on.	monitor#	Run **quit**.
User mode	Log in.	Switch>	Run **exit** or **quit**.
Management mode	Enter **enter** or **enable** in user mode.	Switch#	Run **exit** or **quit**.
Office configuration mode	Enter **config** in management mode.	Switch_config#	Run **exit** or **quit** or **Ctrl-z** to directly back to the management mode.
Port configuration mode	Enter the **interface** command in office configuration mode, such as **interface f0/1**.	Switch_config_f0/1#	Run **exit** or **quit** or **Ctrl-z** to directly back to the management mode.

Each command mode is unsuitable to subsets of some commands. If problem occurs when you enter commands, check the prompt and enter the question mark to obtain the available command list. Problem may occur when you run in incorrect command mode or you misspelled the command.

Pay attention to the changes of the interface prompt and the relative command mode in the following case:

```
Switch> enter
Password: <enter password>
Switch# config
Switch_config# interface f0/1
Switch_config_f0/1# quit
Switch_config# quit
Switch#
```

1.5 Canceling a Command

To cancel a command or resume its default properties, add the keyword “no” before most commands. An example is given as follows:

no ip routing

1.6 Saving Configuration

You need to save configuration in case the system is restarted or the power is suddenly off. Saving configuration can quickly recover the original configuration. You can run write to save configuration in management mode or office configuration mode.

Basic Configuration

Table of Contents

Basic Configuration 1

Table of Contents I

Chapter 1 System Management Configuration 1

1.1 File Management Configuration 1

1.1.1 Managing the file system 1

1.1.2 Commands for the file system 1

1.1.3 Starting up from a file manually 1

1.1.4 Updating software 2

1.1.5 Updating configuration 3

1.1.6 Using ftp to perform the update of software and configuration 3

1.2 Basic System Management Configuration 4

1.2.1 Configuring Ethernet IP Address 4

1.2.2 Setting the Default Route 5

1.2.3 Using Ping to Test Network Connection State 5

Chapter 2 Terminal Configuration 6

2.1 VTY Configuration Overview 6

2.2 Configuration Tasks 6

2.2.1 Relationship between Line and Interface 6

2.3 Monitor and Maintenance 7

2.4 Browsing Logs 7

2.5 VTY Configuration Example 7

Chapter 3 SSH Configuration Commands 8

3.1 Ssh Overview 8

3.1.1 SSH Server 8

3.1.2 SSH Client 8

3.1.3 Attribute Realization 8

3.2 Configuration Tasks 8

3.2.1 Configuring the Authentication Method List 8

3.2.2 Configuring Access List 8

3.2.3 Configuring the Authentication Timeout Time 9

3.2.4 Configuring the Authentication Retry Times 9

3.2.5 Configuring the Login Silence Period 9

3.2.6 Enabling Encryption Key Saving Function 9

3.2.7 Enabling SFTP Function 10

3.2.8 Enabling SSH Server 10

3.3 Configuration Example of SSH Server 10

3.3.1 ACL 10

3.3.2 Global Configuration 10

Chapter 1 System Management Configuration

1.1 File Management Configuration

1.1.1 Managing the file system

The filename in flash is no more than 20 characters and filenames are case insensitive.

startup-config is the system configuration file.

1.1.2 Commands for the file system

The boldfaces in all commands are keywords. Others are parameters. The content in the square brakcet "[ ]" is optional.

Command	Purpose
format	Formats the file system and delete all data.
dir [filename]	Displays files and directory names. The file name in the symbol "[]" means to display files starting with several letters. The file is displayed in the following format: Index number file name <FILE> length established time
delete filename	Deletes a file. The system will prompt if the file does not exist.
md dirname	Creates a directory.
rd dirname	Deletes a directory. The system will prompt if the directory is not existed.
more filename	Displays the content of a file. If the file content cannot be displayed by one page, it will be displayed by pages.
cd	Changes the path of the current file system.
pwd	Displays the current path.

1.1.3 Starting up from a file manually

monitor#boot flash <*local_filename*>

The command starts switch software in flash, which may contain multiple software images.

Description

Parameters	Description
local_filename	file name in the flash, the user must enter the file name

Example

monitor#boot flash switch.bin

1.1.4 Updating software

User can use this command to download switch system software locally or remotely to obtain version update or the custom-made function version.

There are two ways of software update in monitor mode.

1. Through TFTP protocol

monitor#copy tftp flash [ip_addr]

The command is to copy file from the tftp server to the flash in the system. After you enter the command, the system will prompt you to enter the remote server name and the remote filename.

Description

Parameters	Description
ip_addr	Means the IP address of the TFTP server. If this parameter is not designated, you are prompted to enter the IP address after the copy command is run.

Example

The following example shows a main.bin file is read from the server, written into the switch and changed into the name switch. Bin.

monitor#copy tftp flash

Prompt: Source file name[]?main.bin

Prompt: Remote-server ip address[]?192.168.20.1

Prompt: Destination file name[main.bin]?switch.bin

please wait ...
##
##
##
##
##
##

TFTP:successfully receive 3377 blocks ,1728902 bytes
monitor#

1.1.5 Updating configuration

The switch configuration is saved as a file, the filename is startup-config. You can use commands similar to software update to update the configuration.

1. Through TFTP protocol

monitor#copy tftp flash startup-config

1.1.6 Using ftp to perform the update of software and configuration

switch #copy ftp flash [ip_addr]

Use ftp to perform the update of software and configuration in formal program management. Use copy to download a file from an FTP server to the switch, or to upload a file from the switch to an FTP server. After you enter the command, the system will prompt you to enter the remote server name and remote filename.

copy{**ftp**:[[[//login-name:[login-password]@]location]/directory]/filename}|**flash**:filenam e>}{**flash**<:filename>|**ftp**:[[[//login-name:[login-password]@]location]/directory]/filenam e}<blksize><mode><type>

Description

Parameters	Description
login-nam	Username of the ftp server If this parameter is not designated, you are prompted to enter the IP address after the copy command is run.
login-password	Password of the ftp server If this parameter is not designated, you are prompted to enter the IP address after the copy command is run.
ip_addr	IP address of the ftp server If this parameter is not designated, you are prompted to enter the IP address after the copy command is run.
active	Means to connect the ftp server in active mode.
passive	Means to connect the ftp server in passive mode.
type	Set the data transmission mode (ascii or binary)

Example

The following example shows a main.bin file is read from the server, written into the switch and changed into the name switch.bin.

switch#copy ftp flash

Prompt:ftp user name[anonymous]? login-nam

Prompt:ftp user password[anonymous]? login-password

Prompt:Source file name[]?main.bin

Prompt:Remote-server ip address[]?192.168.20.1

Prompt:Destination file name[main.bin]?switch.bin

Or

switch#copy ftp://login-nam:login-password@192.168.20.1/main.bin flash:switch.bin
##
##
FTP:successfully receive 3377 blocks ,1728902 bytes
switch#

Note:

1) When the ftp server is out of service, the wait time is long. If this problem is caused by the tcp timeout time (the default value is 75s), you can configure the global command ip tcp synwait-time to modify the tcp connection time. However, it is not recommended to use it.

2) When you use ftp in some networking conditions, the rate of data transmission might be relatively slow. You can properly adjust the size of the transmission block to obtain the best effect. The default size is 512 characters, which guarantee a relatively high operation rate in most of the networks.

1.2 Basic System Management Configuration

1.2.1 Configuring Ethernet IP Address

monitor#ip address <*ip_addr*> <*net_mask*>

This command is to configure the IPaddress of the Ethernet.,The default IP address is 192.168.0. 1,and the network mask is255.255.255.0.

Description

Parameters	Description
ip_addr	IP address of the Ethernet
net_mask	Mask of the Ethernet

Example

monitor#ip address 192.168.1.1 255.255.255.0

1.2.2 Setting the Default Route

monitor#ip route default <*ip_addr*>

This command is used to configure the default route. You can configure only one default route.

Description

Parameters	Description
ip_addr	IP address of the gateway

Example

monitor#ip route default 192.168.1.1

1.2.3 Using Ping to Test Network Connection State

monitor#ping <*ip_address*>

This command is to test network connection state.

Description

Parameters	Description
ip_address	Stands for the destination IP address

Example

monitor#ping 192.168.20.100
PING 192.168.20.100: 56 data bytes
64 bytes from 192.168.20.100: icmp_seq=0. time=0. ms
64 bytes from 192.168.20.100: icmp_seq=1. time=0. ms
64 bytes from 192.168.20.100: icmp_seq=2. time=0. ms
64 bytes from 192.168.20.100: icmp_seq=3. time=0. ms
----192.168.20.100 PING Statistics----
4 packets transmitted, 4 packets received, 0% packet loss
round-trip (ms) min/avg/max = 0/0/0

Chapter 2 Terminal Configuration

2.1 VTY Configuration Overview

The system uses the line command to configure terminal parameters. Through the command, you can configure the width and height that the terminal displays.

2.2 Configuration Tasks

The system provides console and virtual terminal lines for management access.

Line Type	Interface	Description	Numbering
CON(CTY)	Console	To log in to the system for configuration.	0
VTY	Virtual	Remote management access over Ethernet	32 numbers starting from 1

2.2.1 Relationship between Line and Interface

1. Relationship between Synchronous Interface and VTY Line

The virtual terminal line provides a synchronous interface to access to the system. When you connect to the system through VTY line, you actually connects to a virtual port on an interface. For each synchronous interface, there can be many virtual ports.

For example, several Telnet sessions can connect through an Ethernet interface.

Steps for configuring VTY:

(1) Log in to the line configuration mode.

(2) Configure the terminal parameters.

Note: The console and Telnet sessions may log out if they remain idle for a configured period. The timeout can be configured.

For VTY configuration, refer to the section “VTY configuration example”.

2.3 Monitor and Maintenance

Runshow line to checkthe VTYconfiguration.

2.4 Browsing Logs

By default, the system will export the logs to the console port.

After the terminal monitor command is set on the telnet line, the logs will be exported to this line.

By default the logs will not be exported to the cache and cannot be browsed after you run show log. After you run logging buffer *size* to set the log cache, you can run show log to browse the log information.

2.5 VTY Configuration Example

It shows how to cancel the limit of the line number per screen for all VTYs without more prompt:

config#line vty 0 32

config_line#length 0

32 vty configuration timeout time

Switch_config#line vty 0 31

Switch_config_line#exec-timeout 10

Switch_config_line#exit

Switch_config#

Chapter 3 SSH Configuration Commands

3.1 Ssh Overview

3.1.1 SSH Server

SSH client can provide a secure and encrypted communication link through SSH server and other devices. This connection has the same functions as those of Telnet. SSH server supports the following encryption algorithms: des, 3des and blowfish.

3.1.2 SSH Client

SSH client runs on the basis of the SSH protocol, providing authentication and encryption. Due to the application of authentication and encryption, SSH client ssh client allows to establish secure communication in unsecure network environment between our's communication devices or between other devices that support ssh server. SSH client supports the following encryption algorithms: des, 3des and blowfish.

3.1.3 Attribute Realization

SSH server and SSH client support SSH 1.5. Both of them supports the shell application.

3.2 Configuration Tasks

3.2.1 Configuring the Authentication Method List

SSH server adopts the login authentication mode. SSH server uses the default authentication method list by default.

In global configuration mode, the following command can be used to configure the authentication method list.

Command	Purpose
ip sshd auth-method STRING	Configure the authentication method list. The length of the authentication method's name is no more than 20 characters.

3.2.2 Configuring Access List

In order to control SSH server to access other devices, you can configure ACL for SSH server.

In global configuration mode, the following command can be used to configure the timeout time.

Command	Purpose
ip sshd access-class STRING	Configures ACL. The length of the access list's name is no more than 19 characters.

3.2.3 Configuring the Authentication Timeout Time

After SSH client connects SSH server successfully, the SSH server will close the connection if the authentication cannot be passed during the configured time.

In global configuration mode, the following command can be used to configure the authentication timeout.

Command	Purpose
ip sshd timeout <60-65535>	Configure the authentication timeout time.

3.2.4 Configuring the Authentication Retry Times

If the times for failed authentications exceed the maximum times, SSH server will not allow you to retry authentication and the system enters the silent period. The maximum times for retrying authentication is 6 by default.

In global configuration mode, the following command can be used to configure the authentication retry times.

Command	Purpose
ip sshd auth-retries <0-65535>	Configures the authentication retry times.

3.2.5 Configuring the Login Silence Period

The system enters in the silent period when the authentication retry times exceed the threshold. The silence period is 60s by default.

In global configuration mode, the following command can be used to configure the silence period.

Command	Purpose
ip sshd silence-period <0-3600>	Configures the login silence period

3.2.6 Enabling Encryption Key Saving Function

Enable ssh server and the initial encryption key needs to be calculated. The process may take one to two minutes. When enabling the encryption key saving function, the initial encryption key is saved in the flash. When enabling ssh server in a second time, the encryption key will be read first.

sftp function is disabled by default. Use the following command to enable sftp function in global configuration mode:

Command	Purpose
ip sshd save	Enable encryption key saving function.

3.2.7 Enabling SFTP Function

The SFTP function refers to the secure file transmission system based on SSH, of which the authentication procedure and data transmission are encrypted. Though it has low transmission efficiency, network security is highly improved.

SFTP function is disabled by default. Run following command to enable SFTP function in global configuration mode.

Command	Purpose
ip sshd sftp	Enable sftp function.

3.2.8 Enabling SSH Server

Ssh server is disabled by default. WHEN SSH server is enabled, a RSA key pair will be generated and then listens the connection request from SSH client. The whole process probably requires one or two minutes.

The following command can be used in global configuration mode to enable SSH server:

Command	Purpose
ip sshd enable	Enable SSH server. The digit of the password is 1024.

3.3 Configuration Example of SSH Server

The following configuration allows the host whose IP is 192.168.20.40 to access SSH server, while the local user database will be used to authenticate the user.

3.3.1 ACL

```
ip access-list standard ssh-acl
permit 192.168.20.40
```

3.3.2 Global Configuration

```
aaa authentication login ssh-auth local
ip sshd auth-method ssh-auth
ip sshd access-class ssh-acl
ip sshd enable
```

Network Management Configuration

Table of Contents

Chapter 1 Network Management Configuration 1
1.1 SNMP Configuration 1
1.1.1 Overview 1

Chapter 1 Network Management Configuration

1.1 SNMP Configuration

1.1.1 Overview

The SNMP system includes the following 3 parts:

- SNMP management server (NMS)
- SNMP agent (agent)
- MIB

SNMP is a protocol for the application layer.It provides the format for the packets which are transmitted between NMS and agent.

SNMP management server is a part of the network management system, such as a network management system.

SNMP agent includes the MIB variable and the SNMP management server can be used to browse or change these variables' values.The management server can get the values from the agent or save these variables in the agent.The agent collects data from MIB.MIB is the database of equipment parameters and network data.

1. SNMP Notification

When a special event occurs, the system will send an inform to the SNMP management server.For example, when the agent system runs into a incorrect condition, it will send a message to the management server.

The SNMP notification can be sent as a trap or a inform request.Because the receiver receives a trap and does not send any response, the transmitter hence cannot confirm whether the trap is received. In this way, the trap is unreliable.Comparatively, the SNMP management server uses SNMP to respond PDU, which is acted as a response of this message.If the management server does not receive the inform request, it will not transmit a response.If the transmitter does not receives the response, it will transmit the inform request again.In this way, the inform has more chance to arrive the planned destination.

Security Configuration

Table of Contents

Chapter 1 AAA Configuration....1
1.1 AAA Overview....1
1.1.1 AAA Security Service....1
1.1.2 Benefits of Using AAA....2
1.1.3 AAA Principles....2
1.1.4 AAA Method List....2
1.1.5 AAA Configuration Process....3
1.2 Authentication Configuration....4
1.2.1 AAA Authentication Configuration Task List....4
1.2.2 AAA Authentication Configuration Task....4
1.2.3 AAA Authentication Configuration Example....8
1.3 Authorization Configuration....9
1.3.1 AAA Authorization Configuration Task List....9
1.3.2 AAA Authorization Configuration Task....9
1.3.3 AAA Authorization Examples....10
1.4 AAA Accounting Configuration....11
1.4.1 AAA Accounting Configuration Task List....11
1.4.2 AAA Accounting Configuration Task....11
1.5 Local Account Policy Configuration....14
1.5.1 Local Account Policy Configuration Task List....14
1.5.2 Local Account Policy Configuration Task....14
1.5.3 Local Account Policy Example....16
Chapter 2 Configuring RADIUS....17
....17
2.1 Overview....17
2.1.1 RADIUS Overview....17
2.1.2 RADIUS Operation....18
2.2 RADIUS Configuration Steps....18
2.3 RADIUS Configuration Task List....19
2.4 RADIUS Configuration Task....19
2.4.1 Configuring Switch to RADIUS Server Communication....19
2.4.2 Configuring Switch to Use Vendor-Specific RADIUS Attributes....20
2.4.3 Specifying RADIUS Authentication....20
2.4.4 Specifying RADIUS Authorization....20
2.4.5 Specifying RADIUS Accounting....20
2.5 RADIUS Configuration Examples....21
2.5.1 RADIUS Authentication Example....21
2.5.2 RADIUS Application in AAA....21

Chapter 3 TACACS+ Configuration 22
..... 22
3.1 TACACS+ Overview 22
3.1.1 The Operation of TACACS+ Protocol 22
3.2 TACACS+ Configuration Process 23
3.3 TACACS+ Configuration Task List 24
3.4 TACACS+ Configuration Task 24
3.4.1 Assigning TACACS+ Server 24
3.4.2 Setting up TACACS+ Encrypted Secret Key 25
3.4.3 Assigning to Use TACACS+ for Authentication 25
3.4.4 Assigning to Use TACACS+ for Authorization 25
3.4.5 Assigning to Use TACACS+ for Accounting 25
3.5 TACACS+ Configuration Example 25
3.5.1 TACACS+ Authentication Examples 25
3.5.2 TACACS+ Authorization Examples 26
3.5.3 TACACS+ Accounting Examples 26

Chapter 1 AAA Configuration

1.1 AAA Overview

Access control is used to control the users to access switch or NAS and to limit their service types. Authentication, authorization, and accounting (AAA) network security services provide the primary framework through which you set up access control on your switch or access server.

1.1.1 AAA Security Service

AAA is an architectural framework for configuring a set of three independent security functions in a consistent manner. AAA provides a modular way of performing the following services:

- Authentication: It is a method of identifying users, including username/password inquiry and encryption according to the chosen security protocol.

  Authentication is a method to distinguish the user's identity before users access the network and enjoy network services. AAA authentication can be configured through the definition of an authentication method list and then application of this method list on all interfaces. This method list defines the authentication type and the execution order; any defined authentication method list must be applied on a specific interface before it is executed. The only exception is the default authentication method list (which is named default). If there are no other authentication method lists, the default one will be applied on all interfaces automatically. If anyone is defined, it will replace the default one. For how to configure all authentications, see "Authentication Configuration".

- Authorization: it is a remote access control method to limit user's permissions.

  AAA authorization takes effect through a group of features in which a user is authorized with some permissions. Firstly, the features in this group will be compared with the information about a specific user in the database, then the comparison result will be returned to AAA to confirm the actual permissions of this user. This database can be at the accessed local server or switch, or remote Radius/TACACS+ server. The Radius or TACACS+ server conducts user authorization through a user-related attribute-value peer. The attribute value (AV) defines the allowably authorized permissions. All authorization methods are defined through AAA. Like authentication, an authorization method list will be first defined and then this list will be applied on all kinds of interfaces. For how to carry on the authorization configuration, see "Authorization Configuration".

- Accounting: it is a method to collect user's information and send the information to the security server. The collected information can be used to open an account sheet, make auditing and form report lists, such as the user ID, start/end time, execution commands, and the number of packets or bytes.

  The accounting function can track the services that users access, and at the same time track the service-consumed network resource number. When AAA accounting is activated, the access server can report user's activities to the TACACS+ or Radius server in way of accounting. Each account contains an AV

peer, which is stored on the security server. The data can be used for network management, client's accounting analysis or audit. Like authentication and authorization, an accounting method list must be first defined and then applied on different interfaces. For how to carry on the accounting configuration, see “Accounting Configuration”.

1.1.2 Benefits of Using AAA

AAA provides the following benefits:

- Increased flexibility and control of access configuration
- Scalability
- Standardized authentication methods, such as RADIUS, TACACS+, and Kerberos
- Multiple backup systems

1.1.3 AAA Principles

AAA is designed to enable you to dynamically configure the type of authentication and authorization you want on a per-line (per-user) or per-service (for example, IP, IPX, or VPDN) basis. You define the type of authentication and authorization you want by creating method lists, then applying those method lists to specific services or interfaces.

1.1.4 AAA Method List

To configure AAA, define a named method list first and then apply it to the concrete service or interface. This method list defines the running AAA type and their running sequence. Any defined method list must be applied to a concrete interface or service before running. The only exception is the default method list. The default method list is automatically applied to all interfaces or services. Unless the interface applies other method list explicitly, the method list will replace the default method list.

A method list is a sequential list that defines the authentication methods used to authenticate a user. In AAA method list you can specify one or more security protocols. Thus, it provides with a backup authentication system, in case the initial method is failed. Our switch software uses the first method listed to authenticate users; if that method does not respond, the software selects the next authentication method in the method list. This process continues until there is successful communication with a listed authentication method or the authentication method list is exhausted, in which case authentication fails.

It is important to notice that the switch software attempts authentication with the next listed authentication method only when there is no response from the previous method. If authentication fails at any point in this cycle—meaning that the security server or local user name database responds by denying the user access—the authentication process stops and no other authentication methods are attempted.

The following figures shows a typical AAA network configuration that includes four security servers: R1 and R2 are RADIUS servers, and T1 and T2 are TACACS+ servers. Take the authentication as an example to demonstrate the relation between AAA service and AAA method list.

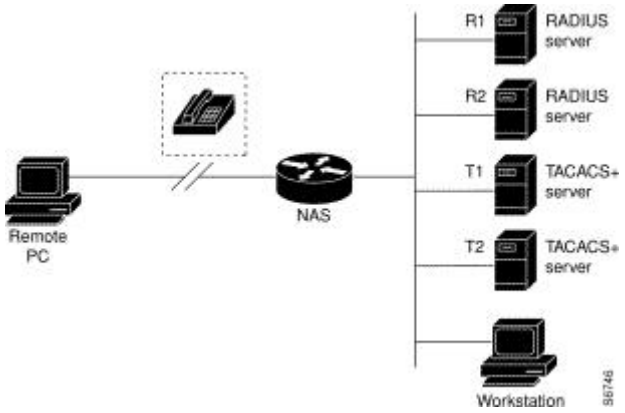


Figure 1- 1 Typical AAA Network Configuration

In this example, default is the name of the method list, including the protocol in the method list and the request sequence of the method list follows the name. The default method list is automatically applied to all interfaces.

When a remote user attempts to dial in to the network, the network access server first queries R1 for authentication information. If R1 authenticates the user, it issues a PASS response to the network access server and the user is allowed to access the network. If R1 returns a FAIL response, the user is denied access and the session is terminated. If R1 does not respond, then the network access server processes that as an ERROR and queries R2 for authentication information. This pattern continues through the remaining designated methods until the user is either authenticated or rejected, or until the session is terminated.

A FAIL response is significantly different from an ERROR. A FAIL means that the user has not met the criteria contained in the applicable authentication database to be successfully authenticated. Authentication ends with a FAIL response. An ERROR means that the security server has not responded to an authentication query. Only when an ERROR is detected will AAA select the next authentication method defined in the authentication method list.

Suppose the system administrator wants to apply the method list to a certain or a specific port. In such case, the system administrator should create a non-default method list and then apply the list of this name to an appropriate port.

1.1.5 AAA Configuration Process

You must first decide what kind of security solution you want to implement. You need to assess the security risks in your particular network and decide on the appropriate means to prevent unauthorized entry and attack. Before you configure AAA, you need know the basic configuration procedure. To do AAA security configuration on switch or access servers, perform the following steps:

- If you decide to use a security server, configure security protocol parameters first, such as RADIUS, TACACS+, or Kerberos.
- Define the method lists for authentication by using an AAA authentication command.
- Apply the method lists to a particular interface or line, if required.

- (Optional) Configure authorization using the aaa authorization command.
- (Optional) Configure accounting using the aaa accounting command.

1.2 Authentication Configuration

1.2.1 AAA Authentication Configuration Task List

- Configuring Login Authentication Using AAA
- Enabling Password Protection at the Privileged Level
- Configuring Message Banners for AAA Authentication
- Modifying the Notification Character String for Username Input
- Modifying AAA authentication password-prompt
- Creating local user name authentication database
- Creating the Authentication Database with the Local Privilege

1.2.2 AAA Authentication Configuration Task

General configuration process of AAA authentication

To configure AAA authentication, perform the following configuration processes:

(1) If you decide to use a separate security server, configure security protocol parameters, such as RADIUS, or TACACS+. Refer to the relevant section for the concrete configuration methods.

(2) Configuring Authentication Method List Using aaa authentication

(3) If necessary, apply the accounting method list to a specific interface or line.

1.2.2.1 Configuring Login Authentication Using AAA

The AAA security services facilitate a variety of login authentication methods. Use the aaa authentication login command to enable AAA authentication no matter which of the supported login authentication methods you decide to use. With the aaa authentication login command, you create one or more lists of authentication methods that are tried at login. These lists are applied using the login authentication line configuration command. After the authentication method lists are configured, you can apply these lists by running login authentication. You can run the following command in global configuration mode to start the configuration:

Command	Purpose
aaa authentication login {**default** |	Enables AAA globally.

list-name}*method1* [*method2...*]	
line { **console** | **vty** } *line-number* [*ending-line-number*]	Enter the configuration mode of a line.
login authentication {**default** | *list-name*}	Applies the authentication list to a line or set of lines. (In the line configuration mode)

The list-name is a character string used to name the list you are creating. The key word method specifies the actual method of the authentication method. The additional methods of authentication are used only if the previous method returns an error, not if it fails. To specify that the authentication should succeed even if all methods return an error, specify none as the final method in the command line.

The default parameter can create a default authentication list, which will be automatically applied to all interfaces. For example, to specify that authentication should succeed even if (in this example) the TACACS+ server returns an error, enter the following command:

aaa authentication login default group radius

Note:

Because the none keyword enables any user logging in to successfully authenticate, it should be used only as a backup method of authentication.

If you cannot find the authentication method list, you can only login through the console port. Any other way of login is in accessible.

The following table lists the supported login authentication methods:

Keyword	Notes:
enable	Uses the enable password for authentication.
group *name*	Uses named server group for authentication.
group radius	Uses RADIUS for authentication.
group tacacs+	Uses group tacacs+ for authentication.
line	Uses the line password for authentication.
local	Uses the local username database for authentication.
localgroup	Uses the local strategy group username database for authentication.
local-case	Uses case-sensitive local user name authentication.
none	Passes the authentication unconditionally.

(1) Using the enable password to carry on the login authentication:

To specify the enable password as the user authentication method, run the following command:

aaa authentication login default enable

(2) Using the line password to login

Use the aaa authentication login command with the line method keyword to specify the line password as the login authentication method. For example, to specify the line password as the method of user authentication at login when no other method list has been defined, enter the following command:

aaa authentication login default line

Before you can use a line password as the login authentication method, you need to define a line password.

(3) Using the local password to carry on the login authentication:

When you run aaa authentication login, you can use the keyword “local” to designate the local database as the login authentication method. For example, if you want to specify the local username database as the user authentication method and not define any other method, run the following command:

aaa authentication login default local

For information about adding users into the local username database, refer to the section "Establishing Username Authentication" in this chapter.

(4) Login Authentication Using RADIUS

Use the aaa authentication login command with the group radius method to specify RADIUS as the login authentication method. For example, to specify RADIUS as the method of user authentication at login when no other method list has been defined, enter the following command:

aaa authentication login default group radius

Before you can use RADIUS as the login authentication method, you need to enable communication with the RADIUS security server. For more information about establishing communication with a RADIUS server, refer to the chapter "Configuring RADIUS."

1.2.2.2 Enabling Password Protection at the Privileged Level

Use the aaa authentication enable default command to create a series of authentication methods that are used to determine whether a user can access the privileged EXEC command level. You can specify up to four authentication methods. The additional methods of authentication are used only if the previous method returns an error, not if it fails. To specify that the authentication should succeed even if all methods return an error, specify none as the final method in the command line. Use the following command in global configuration mode:

Command	Purpose
aaa authentication enable default *method1* [*method2...*]	Enables user ID and password checking for users requesting privileged EXEC level.

The method argument refers to the actual list of methods the authentication algorithm tries, in the sequence entered.

The following table lists the supported enable authentication methods:

Keyword	Notes
enable	Uses the enable password for authentication.
group *group-name*	Uses named server group for authentication.
group radius	Uses RADIUS authentication.
group tacacs+	Uses tacacs+ for authentication.
line	Uses the line password for authentication.
none	Passes the authentication unconditionally.

When configuring enable authentication method as the remote authentication, use RADIUS for authentication. Do as follows:

(1) Uses RADIUS for enable authentication:

The user name for authentication is $ENABLE*level*$; level is the privileged level the user enters, that is, the number of the privileged level after enable command. For instance, if the user wants to enter the privileged level 7, enter command enable 7; if configuring RADIUS for authentication, the user name presenting to Radius-server host is $ENABLE7$; the privileged level of enable is 15 by default, that is, the user name presenting to Radius-server host in using RADIUS for authentication is $ENABLE15$. The user name and the password need to configured on Radius-server host in advance. The point is that in user database of Radius-server host, the Service-Type of the user specifying the privileged authentication is 6, that is, Admin-User.

1.2.2.3 Configuring Message Banners for AAA Authentication

The banner of configurable, personal logon or failed logon is supported. When AAA authentication fails during system login, the configured message banner will be displayed no matter what the reason of the failed authentication is.

Configuring the registration banner

Run the following command in global configuration mode.

Command	Purpose
aaa authentication banner *delimiter text-string delimiter*	Configures a personal logon registration banner.

Configuring the banner of failed logon

Run the following command in global configuration mode.

Command	Purpose
aaa authentication fail-message *delimiter text-string delimiter*	Configures a personal banner about failed logon.

Usage Guidelines

When creating a banner, you need to configure a delimiter and then to configure the text string itself. The delimiter is to notify that the following text string will be displayed as the banner. The delimiter appears repeatedly at the end of the text character string, indicating that the banner is ended.

1.2.2.4 Modifying the Notification Character String for Username Input

To modify the default text of the username input prompt, run aaa authentication username-prompt. You can run no aaa authentication username-prompt to resume the password input prompt.

username:

The aaa authentication username-prompt command does not change any prompt information provided by the remote TACACS+ server or the RADIUS server. Run the following command in global configuration mode:

Command	Purpose
aaa authentication username-prompt *text-string*	Modifies the default text of the username input prompt.

1.2.2.5 Modifying AAA authentication password-prompt

To change the text displayed when users are prompted for a password, use the aaa authentication password-prompt command. To return to the default password prompt text, use the no form of this command. You can run no aaa authentication username-prompt to resume the password input prompt.

password:

The aaa authentication password-prompt command does not change any prompt information provided by the remote TACACS+ server or the RADIUS server. Run the following command in global configuration mode:

Command	Purpose
aaa authentication password-prompt *text-string*	String of text that will be displayed when the user is prompted to enter a password.

1.2.2.6 Creating the Authentication Database with the Local Privilege

To create the enable password database with the local privilege level, run enable password { [encryption-type] encrypted-password} [level level] in global configuration mode. To cancel the enable password database, run no enable password [level level].

enable password { [*encryption-type*] *encrypted-password*} [**level** *level*]

no enable password [**level** *level*]

1.2.3 AAA Authentication Configuration Example

1.2.3.1 RADIUS Authentication Example

The following example shows how to configure the switch to authenticate and authorize using RADIUS:

```
aaa authentication login radius-login group radius local
aaa authorization network radius-network group radius
line vty 3
login authentication radius-login
```

The meaning of each command line is shown below:

- The aaa authentication login radius-login group radius local command configures the switch to use RADIUS at the login prompt. If RADIUS returns an error, the user is authenticated using the local database.
- The aaa authorization network radius-network group radius command queries RADIUS for network authorization, address assignment, and other access lists.
- The login authentication radius-login command enables the radius-login method list for line 3.

1.3 Authorization Configuration

1.3.1 AAA Authorization Configuration Task List

- Configuring EXEC authorization through AAA

1.3.2 AAA Authorization Configuration Task

General configuration process of AAA authorization

To configure AAA authorization, perform the following configuration processes:

(1) If you decide to use a separate security server, configure security protocol parameters, such as RADIUS, or TACACS+. Refer to the relevant section for the concrete configuration methods.

(2) Run aaa authorization to define the authorization method list. The authorization service is not provided by default.

(3) If necessary, apply the accounting method list to a specific interface or line.

1.3.2.1 Configuring EXEC authorization through AAA

To enable AAA authorization, run aaa authorization. The aaa authorization exec command can create one or several authorization method lists and enable the EXEC authorization to decide whether the EXEC hull program is run by the users or not, or decide whether the users are authorized with the privilege when entering the EXEC hull program. After the authorization method lists are configured, you can apply these lists by running login authorization. You can run the following command in global configuration mode to start the configuration:

Command	Purpose
aaa authorization exec {**default** | *list-name*}*method1* [*method2...*]	Creates the global authorization list.
line [**console** | **vty**] *line-number* [*ending-line-number*]	Enter the configuration mode of a line.
login authorization {**default** | *list-name*}	Applies the authorization list to a line or set of lines. (In the line configuration mode)

The list-name is a character string used to name the list you are creating. The method keyword is used to designate the real method for the authorization process. Only when the previously-used method returns the authorization error can other authorization methods be used. If the authorization fails because of the previous method, other authorization methods will not be used. If you requires the EXEC shell to be entered even when all authorization methods returns the authorization errors, designate none as the last authorization method in the command line.

The default parameter can create a default authentication list, which will be automatically applied to all interfaces. For example, you can run the following command to designate RADIUS as the default authorization method of EXEC:

aaa authorization exec default group radius

Note:

If the authorization method list cannot be found during authorization, the authorization will be directly passed without the authorization service conducted.

The following table lists currently-supported EXEC authorization methods:

Keyword	Notes:
group *WORD*	Uses the named server group to conduct authorization.
group radius	Uses RADIUS authorization.
group tacacs+	Uses tacacs+ authorization.
local	Uses the local database to perform authorization.
if-authenticated	Automatically authorizes the authencated user with all required functions.
none	Passes the authorization unconditionally.

1.3.3 AAA Authorization Examples

1.3.3.1 Example of Local EXEC Authorization

The following example shows how to perform the local authorization and local authorization by configuring the switch:

```
aaa authentication login default local
aaa authorization exec default local
!
localauthor a1
  exec privilege default 15
!
local author-group a1
username exec1 password 0 abc
username exec2 password 0 abc author-group a1
username exec3 password 0 abc maxlinks 10
username exec4 password 0 abc autocommand telnet 172.16.20.1
!
```

The following shows the meaning of each command line:

- The aaa authentication login default local command is used to define the default login-authentication method list, which will be automatically applied to all login authentication services.
- The command is used to define the default EXEC authorization method list, which will be automatically applied to all users requiring to enter the EXEC shell.
- Command localauthor al defines a local authority policy named al. Command exec privilege default 15 means the privileged level of exec login user is 15 by default.
- Command local author-group a1 means apply the local authorization policy a1 to global configuration (the default local policy group).
- Command username exec1 password 0 abc defines an account exec1 with password abc in the global configuration mode.
- Command username exec2 password 0 abc author-group a1 defines an account exec 2 with password abc in the global configuration mode. The account is applied to the local authorization policy a1.
- Command username exec3 password 0 abc maxlinks 10 defines an account exec 3 with password abc in the global configuration mode. The account makes 10 users available simultaneously.
- Command username exec4 password 0 abc autocommand telnet 172.16.20.1 defines an account exec4 with password abc. telnet 172.16.20.1 is automatically run when the user login the account.

1.4 AAA Accounting Configuration

1.4.1 AAA Accounting Configuration Task List

- Configuring Connection Accounting using AAA

1.4.2 AAA Accounting Configuration Task

General configuration process of AAA accounting

To configure AAA accounting, perform the following configuration processes:

(1) If you decide to use a separate security server, configure security protocol parameters, such as RADIUS, or TACACS+. Refer to the relevant section for the concrete configuration methods.

(2) Apply the method lists to a particular interface or line, if required. The accounting service is not provided by default.

(3) If necessary, apply the accounting method list to a specific interface or line.

1.4.2.1 Configuring Connection Accounting Using AAA

To enable AAA accounting, run command aaa accounting. To create a or multiple method list(s) to provide accounting information about all outbound connections made from the switch, use aaa accounting connection. The outbound connections include Telnet, H323 and rlogin. Only H323 is supported currently. You can run the following command in global configuration mode to start the configuration:

Command	Purpose
aaa accounting connection {**default** | *list-name*} {{{**start-stop** | **stop-only**} **group** *groupname}* | **none**}	Establishes the global accounting list.

The list-name is a character string used to name the list you are creating. The method keyword is used to designate the real method for the accounting process.

The following table lists currently-supported connection accounting methods:

Keyword	Notes:
group *WORD*	Uses the named server group to conduct accounting.
group radius	Uses the RADIUS for accounting.
group tacacs+	Uses the TACACS+ for accounting.
none	Disables accounting services for the specified line or interface.
stop-only	Sends a "stop" record accounting notice at the end of the requested user process.
start-stop	RADIUS or TACACS+ sends a "start" accounting notice at the beginning of the requested process and a "stop" accounting notice at the end of the process.

1.4.2.2 Configuring Accounting Update through AAA

To activate the AAA accounting update function for AAA to send the temporary accounting record to all users in the system, run the following command: You can run the following command in global configuration mode to start the configuration:

Command	Purpose
aaa accounting update [**newinfo**] [**periodic** *number*]	Enables AAA accounting update.

If the newinfo keyword is used, a temporary accounting record is sent to the accounting server when new accounting information is available.

When the periodic keyword is used, the temporary accounting record will be sent periodically. The period is defined by the number parameter. The temporary accounting record includes all accounting information occurred before the accounting record is sent.

The two keywords are contradictable, that is, the previously-configured parameter will replace the latter-configured one. For example, if aaa accounting update periodic and then aaa accounting update new info are configured, all currently-registered users will generate temporary accounting records periodically. All new users have accounting records generated according to the new info algorithm.

1.4.2.3 Limiting User Accounting Without Username

To prevent the AAA system from sending the accounting record to the users whose username character string is null, run the following command in global configuration mode:

- **aaa accounting suppress null-username**

1.5 Local Account Policy Configuration

1.5.1 Local Account Policy Configuration Task List

- Local authentication policy configuration
- Local authorization policy configuration
- Local password policy configuration
- Local policy group configuration

1.5.2 Local Account Policy Configuration Task

1.5.2.1 Local authentication policy configuration

To enter local authentication configuration, run command localauthen WORD in global configuration mode.

(1) The max login tries within a certain time

login max-tries *<1-9>* **try-duration** *1d2h3m4s*

The configured local authentication policy can be applied to a local policy group or directly applied to a local account. It gives priority to some local account directly.

1.5.2.2 Local authorization policy configuration

To enter local authorization configuration, run command localauthor *WORD* in global configuration mode.

(1) To authorize priority for login users.

exec privilege {**default | console | ssh | telnet}** *<1-15>*

The configured local authorization policy can be applied to a local policy group or directly applied to a local account. It gives priority to some local account directly.

1.5.2.3 Local password policy configuration

To enter local authorization configuration, run command localpass *WORD* in global configuration mode.

(1) The password cannot be the same with the user name

non-user

(2) The history password check (The new password cannot be the same with the history password. The history password record is 20.)

non-history

(3) Specify the components of the password (complicate the password)

element *[number] [lower-letter] [upper-letter] [special-character]*

(4) Specify the components of the password (complicate the password)

min-length *<1-127>*

(5) password validity period (the validity of the password)

validity 1d2h3m4s

The configured local authorization policy can be applied to a local policy group or directly applied to a local account. It gives priority to some local account directly.

1.5.2.4 Local policy group configuration

To configure local policy group, run localgroup *WORD* in global configuration mode:

(1) local authentication configuration: apply the configured local authentication policy to the policy group

local authen-group *WORD*

(2) local authorization configuration: apply the configured local authorization policy to the policy group

local author-group *WORD*

(3) local password configuration: apply the configured local password policy to the policy group

local pass-group *WORD*

(4) local account configuration: set the maxlinks and freeze for the policy group

local user {{maxlinks *<1-255>***} | { freeze** *WORD* **}}**

(5) account configuration: set the account for the policy group and establish the local database

username *username* [[[**password** *password* | **encryption-type** *encrypted-password*] | **maxlinks** *number* | **authen-group** *WORD* | **author-group** *WORD* | **pass-group** *WORD* | **bind-ip** *A.B.C.D* | **bind-mac** *H:H:H:H:H:H* | **bind-pool** *WORD* | **bind-port** *port* | **callback-dialstring** *string* | **callback-line** *line* | **callback-rotary** *rotary* | **nocallback-verify** | **nohangup** | **noescape**]* | **autocommand** *command* [*line*]&<0-n>

The configured local policy group can be used in local authentication and authorization. Local method is applicable to the default policy group and

localgroup word is to a local policy group.

1.5.3 Local Account Policy Example

This section provides one sample configuration using local account policy. The following example shows how to configure the local authentication and local authorization.

```
aaa authentication login default local
aaa authorization exec default local
!
localpass a3
 non-user
 non-history
 element number lower-letter upper-letter special-character
 min-length 10
 validity 2d
!
localauthen a1
 login max-tries 4 try-duration 2m
!
localauthor a2
 exec privilege default 15
!
local pass-group a3
local authen-group a1
local author-group a2
!
```

The meaning of each command line is shown below:

- The aaa authentication login default local command is used to define the default login-authentication method list, which will be automatically applied to all login authentication services.
- The command is used to define the default EXEC authorization method list, which will be automatically applied to all users requiring to enter the EXEC shell.
- The command localpass a3 defines the password policy named a3.
- The command localauthen a1 defines the authentication policy named a1.
- The command localauthor a2 defines the authorization policy named a2.
- The command local pass-group a3 applies the password policy named a3 to the default policy group.
- The command localauthen a1 applies the authentication policy named a1 to the default policy group.
- The command localauthor a2 applies the authorization policy named a2 to the default policy group.

Chapter 2 Configuring RADIUS

This chapter describes the Remote Authentication Dial-In User Service (RADIUS) security system, defines its operation, and identifies appropriate and inappropriate network environments for using RADIUS technology. The "RADIUS Configuration Task List" section describes how to configure RADIUS with the authentication, authorization, and accounting (AAA) command set. The last section in this chapter-RADIUS Configuration Examples- provides with two examples. Refer to RADIUS Configuration Commands for more details of RADIUS command.

2.1 Overview

2.1.1 RADIUS Overview

RADIUS is a distributed client/server system that secures networks against unauthorized access. In the implementation, RADIUS clients run on switches and send authentication requests to a central RADIUS server that contains all user authentication and network service access information. RADIUS has been implemented in a variety of network environments that require high levels of security while maintaining network access for remote users.

Use RADIUS in the following network environments that require access security:

- Networks with multiple-vendor access servers, each supporting RADIUS. For example, access servers from several vendors use a single RADIUS server-based security database. In an IP-based network with multiple vendors' access servers, dial-in users are authenticated through a RADIUS server.

- Networks that require resource accounting. You can use RADIUS accounting independent of RADIUS authentication or authorization. The RADIUS accounting functions allow data to be sent at the start and end of services, indicating the amount of resources (such as time, packets, bytes, and so on) used during the session.

- Conditions of the switch. RADIUS does not provide two-way authentication. On the switch only incoming call authentication is available when running RADIUS. The outbound call is impossible.

- Networks using a variety of services. RADIUS generally binds a user to one service model.

2.1.2 RADIUS Operation

When a user attempts to log in and authenticate to an access server using RADIUS, the following steps occur:

(1) The user is prompted for and enters a username and password.

(2) The username and encrypted password are sent over the network to the RADIUS server.

(3) The user receives one of the following responses from the RADIUS server:

ACCEPT—The user is authenticated.

REJECT—The user is not authenticated and is prompted to reenter the username and password, or access is denied.

CHALLENGE—A challenge is issued by the RADIUS server. The challenge collects additional data from the user.

The ACCEPT or REJECT response is bundled with additional data that is used for EXEC or network authorization. You must first complete RADIUS authentication before using RADIUS authorization. The additional data included with the ACCEPT or REJECT packets consists of the following:

Services that the user can access, including Telnet or rlogin.

Connection parameters, including the host or client IP address, access list, and user timeouts.

2.2 RADIUS Configuration Steps

To configure RADIUS on your switch or access server, you must perform the following tasks:

- Use the aaa authentication global configuration command to define method lists for RADIUS authentication. For more information about using the aaa authentication command, refer to the "Configuring Authentication" chapter.

- Use line and interface commands to enable the defined method lists to be used. For more information, refer to the "Configuring Authentication" chapter.

The following configuration tasks are optional:

- If necessary, run aaa authorization in global configuration mode to authorize the user’s service request. For more information about using the aaa authorization command, refer to the "Configuring Autorization" chapter.

- If necessary, run aaa accounting in global configuration mode to record the whole service procedure. For more information about running aaa accounting, see Record Configuration.

2.3 RADIUS Configuration Task List

- Configuring switch to RADIUS Server Communication
- Configuring switch to Use Vendor-Specific RADIUS Attributes
- Specifying RADIUS Authentication
- Specifying RADIUS Authorization
- Specifying RADIUS Accounting

2.4 RADIUS Configuration Task

2.4.1 Configuring Switch to RADIUS Server Communication

The RADIUS host is normally a multiuser system running RADIUS server software from a software provider.

A RADIUS server and the switch use a shared secret text string to encrypt passwords and exchange responses.

To configure RADIUS to use the AAA security commands, you must specify the host running the RADIUS server daemon and a secret text (key) string that it shares with the router.

To configure per-server RADIUS server communication, use the following command in global configuration mode:

command	purpose
radius-server host *ip-address* [**auth-port** *port-number*][**acct-port** *portnumber*]	Specifies the IP address or host name of the remote RADIUS server host and assign authentication and accounting destination port numbers.
radius-server key *string*	Specifies the shared secret text string used between the router and a RADIUS server.

To configure global communication settings between the router and a RADIUS server, use the following radius-server commands in global configuration mode:

command	purpose
radius-server retransmit *retries*	Specifies how many times the switch transmits each RADIUS request to the server before giving up (the default is 2).
radius-server timeout *seconds*	Specifies for how many seconds a switch waits for a reply to a RADIUS request before retransmitting the request.
radius-server deadtime *minutes*	Specifies for how many minutes a RADIUS server that is not responding to authentication requests is passed over by requests for RADIUS authentication.

2.4.2 Configuring Switch to Use Vendor-Specific RADIUS Attributes

The Internet Engineering Task Force (IETF) draft standard specifies a method for communicating vendor-specific information between the network access server and the RADIUS server by using the vendor-specific attribute (attribute 26).

Vendor-specific attributes (VSAs) allow vendors to support their own extended attributes not suitable for general use.

For more information about vendor-IDs and VSAs, refer to RFC 2138, Remote Authentication Dial-In User Service (RADIUS). To configure the network access server to recognize and use VSAs, use the following command in global configuration mode:

command	purpose
radius-server vsa send [authentication]	Enables the network access server to recognize and use VSAs as defined by RADIUS IETF attribute 26.

2.4.3 Specifying RADIUS Authentication

After you have identified the RADIUS server and defined the RADIUS authentication key, you must define method lists for RADIUS authentication. Because RADIUS authentication is facilitated through AAA, you must enter the aaa authentication command, specifying RADIUS as the authentication method. For more information, refer to the chapter "Configuring Authentication."

2.4.4 Specifying RADIUS Authorization

AAA authorization lets you set parameters that restrict a user's access to the network. Authorization using RADIUS provides one method for remote access control, including one-time authorization or authorization for each service, per-user account list and profile, user group support, and support of IP, IPX, ARA, and Telnet. Because RADIUS authorization is facilitated through AAA, you must issue the aaa authorization command, specifying RADIUS as the authorization method. For more information, refer to the chapter "Configuring Authorization."

2.4.5 Specifying RADIUS Accounting

The AAA accounting feature enables you to track the services users are accessing as well as the amount of network resources they are consuming. Because RADIUS accounting is facilitated through AAA, you must issue the aaa accounting command, specifying RADIUS as the accounting method. For more information, refer to the chapter "Configuring Accounting."

2.5 RADIUS Configuration Examples

2.5.1 RADIUS Authentication Example

The following example shows how to configure the switch to authenticate and authorize using RADIUS:

aaa authentication login use-radius group radius local

The lines in this sample RADIUS authentication and authorization configuration are defined as follows:

aaa authentication login use-radius radius local configures the switch to use RADIUS for authentication at the login prompt. If RADIUS returns an error, the user is authenticated using the local database. In this example, use-radius is the name of the method list, which specifies RADIUS and then local authentication.

2.5.2 RADIUS Application in AAA

The following example shows a general configuration using RADIUS with the AAA command set:

radius-server host 1.2.3.4

radius-server key myRaDiUSpassWoRd

username root password AlongPassword

aaa authentication login admins group radius local

line vty 1 16

login authentication admins

The meaning of each command line is shown below:

radius-server host is used to define the IP address of the RADIUS server.

radius-server key is used to define the shared key between network access server and RADIUS server.

aaa authentication login admins group radius local command defines the authentication method list "admins," which specifies that RADIUS authentication and then (if the RADIUS server does not respond) local authentication will be used for login.

login authentication admins is used to designate to apply the admins method list during login.

Chapter 3 TACACS+ Configuration

3.1 TACACS+ Overview

As an access security control protocol, TACACS+ provides the centralized verification of acquiring the network access server's access right for users. . The communication's safety is guaranteed because the information exchange between network access server and TACACS+ service program is encrypted

Before using TACACS+ configured on network access server, TACACS+'s server has to be accessed and configured. TACACS+ provides independent modularized authentication, authorization and accounting.

Authentication—supporting multiple authentication ways (ASCII, PAP, CHAP and etc), provides the ability of processing any conversation with users (for example, bringing forward probing questions like family address, service type, ID number and etc. after providing login username and password). Moreover, TACACS+ authentication service supports sending information to user's screen, like sending information to notify user that their password has to be changed because of the company's password aging policy.

Authorization—detailed controlling of user's service limitation during service time, including setting up automatic commands, access control, dialog continuing time and etc. It can also limit the command enforcement which user might execute.

Accounting—collecting and sending the information of creating bills, auditing, or counting the usage status of network resources. Network manager can use accounting ability to track user's activities for security auditing or provide information for user's bills. The accounting function keeps track of user authentication, beginning and starting time, executed commands, packets' quantity and bytes' quantities, and etc.

3.1.1 The Operation of TACACS+ Protocol

3.1.1.1 Authentication in ASCII Form

When user logs in network access server which uses TACACS+, and asking for simple authentication in ASCII form, the following process might happen under typical circumstances:

When the connection is built up, network access server communicates with TACACS+ service program to acquire username prompt, and then gives it to user. User enters username, and network access server communicates with TACACS+ service program again to acquire password prompt. It shows password prompt to user. User enters password and then the password is sent to TACACS+ service program.

Note:

TACACS+ allows any dialogues between server's program and user until it collects enough information to identify user. Normally it is accomplished by the combination of

prompting username and password, but it can also include other items, like ID number. All of these are under the control of TACACS+ server's program.

Network access server finally gets one of the following responses from TACACS+ server:

ACCEPT	User passes authentication, and service begins. If network access server is configured as requiring service authorization, authorization begins at this moment.
REJECT	User does not pass authentication. User might be rejected for further access or prompted to access again. It depends on the treatment of TACACS+ server.
ERROR	Error happens during authentication, and the cause might be at server. It also might happen at the network connection between server and network access server. If ERROR response is received, normally network access tries another way to identify user.
CONTINUE	It prompts user to enter additional authentication information.

3.1.1.2 Authentication in PAP and CHAP Ways

PAP login is similar with ASCII login, but the difference is that username and password of network access server is in PAP message not entered by user, thus it would not prompt user to enter relative information. CHAP login is similar in the main parts. After authentication, user need to enter authorization stage if network access server asks for the authorization for user. But before TACACS+ authorization is handled, TACACS+ authentication has to be finished.

If TACACS+ authorization needs to be processed, it needs to contact with TACACS+ server program again and go back to the authorization response of ACCEPT or REJECT. If back to ACCEPT, AV (attribute-value) for data, which is used for specifying the user's EXEC or NETWORK dialogue and confirming services which user can access, might be included.

3.2 TACACS+ Configuration Process

In order to configure as supporting TACACS+, the following tasks must be processed:

Using command tacacs-server to assign one or multiple IP addresses of TACACS+ server. Using command tacacs key to assign encrypted secret key for all the exchanged information between network access server and TACACS+ server. The same secret key has to be configured in TACACS+ server program.

Use the global configuration command aaa authentication to define the method table which uses TACACS+ to do authentication. More information about command aaa authentication, please refer to "Authentication Configuration".

Use commands line and interface to apply the defined method table on interfaces or lines. More relative information, please refer to "Authentication Configuration".

3.3 TACACS+ Configuration Task List

- Assigning TACACS+ server
- Setting up TACACS+ encrypted secret key
- Assigning to use TACACS+ for authentication
- Assigning to use TACACS+ for authorization
- Assigning to use TACACS+ for accounting

3.4 TACACS+ Configuration Task

3.4.1 Assigning TACACS+ Server

Command Tacacs-server could help to assign the IP address of TACACSC+ server. Because TACACS+ searching host in the configured order, this characteristic is useful for servers which configured with different priorities. In order to assign TACACS+ host, use the following commands under global configuration mode:

Command	Purpose
tacacs-server host *ip-address* [**single-connection**| **multi-connection**] [**port** *integer*] [**timeout** *integer*] [**key** *string*]	To assign the IP address of TACACS+ server and relative features.

Use command tacacs-server to configure the following as well:

- Use single-connection key word to assign the adoption of single connection. This would allow server program to deal with more TACACS+ operations and be more efficient. multi-connection means the adoption of multiple TCP connection.
- Use parameter port to assign TCP interface number which is used by TACACS+ server program. The default interface number is 49.
- Use parameter timeout to assign the time's upper limit (taken second as the unit) for switch·s waiting response from server.
- Use parameter key to assign the encrypted and decrypted secret keys for messages.

Note:

Connect host after using tacacs-server, and connect the timeout value defined by command timeout to cover the global timeout value configured by command tacacs-server timeout. Use the encrypted secret key assigned by tacacs-server to cover the default secret key configured by global configuration command tacacs-server key. Therefore, this command could be used to configure the unique TACACS+ connection to enhance the network security.

3.4.2 Setting up TACACS+ Encrypted Secret Key

In order to set up the encrypted secret key of TACACS+ message, use the following command under the global configuration mode:

Command	Purpose
tacacs-server key *keystring*	To set up the encrypted secret key matched with the encrypted secret key used by TACACS+ server.

Note:

In order to encrypt successfully, the same secret key should also be configured for TACACS+ server program.

3.4.3 Assigning to Use TACACS+ for Authentication

After having marked the TACACS+ server and defined its related encrypted secret key, method table need to be defined for TACACS+ authentication. Because TACACS+ authentication is by AAA, command aaa authentication should be assigned as TACACS+'s authentication way. More information, please refer to "Authentication Configuration".

3.4.4 Assigning to Use TACACS+ for Authorization

AAA authorization could help to set up parameter to confine user's network access limitation. TACACS+ authorization could be applied to services like command, network connection, EXEC dialogue and etc. Because TACACS+ authorization is by AAA, command aaa authorization should be assigned as TACACS+'s authentication way. More information, please refer to "Authorization Configuration".

3.4.5 Assigning to Use TACACS+ for Accounting

AAA accounting is able to track user's current service and their consumed network resources' quantity. Because TACACS+ authorization is by AAA, command aaa accounting should be assigned as TACACS+'s accounting way. More information, please refer to "Accounting Configuration".

3.5 TACACS+ Configuration Example

This chapter includes the following TACACS+ configuration example.

3.5.1 TACACS+ Authentication Examples

The following configuring login authentication is accomplished by TACACS+:

aaa authentication login test group tacacs+ local

tacacs -server host 1.2.3.4

tacacs-server key testkey

```
line vty 0
login authentication test
```

In this example:

Command aaa authentication defines the authentication method table test used on vty0. Key word tacacs+ means the authentication is processed by TACACS+, and if TACACS+ does not respond during authentication, key word local indicates to use the local database on the network access server to do authentication.

Command tacacs-server host marks TACACS+ server's IP address as 1.2.3.4. command tacacs-server key defines the shared encrypted secret key as testkey.

The following example is the security protocol used when configuring TACACS+ as login authentication, with the usage of method table default not test:

```
aaa authentication login default group tacacs+ local
tacacs-server host 1.2.3.4
tacacs-server key goaway
```

In this example:

Command aaa authentication defines the default authentication method table default during login authentication. If authentication required, keyword tacacs+ means authentication is by TACACS+. If TACACS+ does not respond, keyword local indicates to use the local database on the network access server for authentication.

Command tacacs-server host marks TACACS+ server program's IP address as 1.2.3.4. Command tacacs-server key defines the shared encrypted secret key as goaway.

3.5.2 TACACS+ Authorization Examples

```
aaa authentication login default group tacacs+ local
aaa authorization exec default group tacacs+
tacacs-server host 10.1.2.3
tacacs-server key goaway
```

In this example:

Command aaa authentication defines the default authentication method table default during login authentication. If authentication required, keyword tacacs+ means authentication is by TACACS+. If TACACS+ does not respond, keyword local indicates to use the local database on the network access server for authentication.

Command aaa authorization does network service authorization by TACACS+.

Command tacacs-server host marks TACACS+ server's IP as 10.1.2.3. Command tacacs-server key defines the shared encrypted secret key as goaway.

3.5.3 TACACS+ Accounting Examples

The following configuration of login authentication's method table uses TACACS+ as one of the methods to configure the accounting by TACACS+:

```
aaa authentication login default group tacacs+ local
```

```
aaa accounting exec default start-stop group tacacs+
tacacs-server host 10.1.2.3
tacacs-server key goaway
```

In this example:

Command aaa authentication defines the default authentication method table default during login authentication. If authentication required, keyword tacacs+ means authentication is by TACACS+. If TACACS+ does not respond, keyword local indicates to use the local database on the network access server for authentication.

Command aaa accounting does accounting of network service by TACACS+. In this example, the relative information of starting and beginning time is accounted and sent to TACACS+ server.

Command tacacs-server host marks TACACS+ server's IP address as 10.1.2.3. command Command tacacs-server key defines the shared encrypted secret key as goaway.

Web Configuration

Table of Contents

Chapter 1 HTTP Switch Configuration 1
1.1 HTTP Configuration 1
1.1.1 Choosing the Prompt Language 1
1.1.2 Setting the HTTP Port 1
1.1.3 Enabling the HTTP Service 1
1.1.4 Setting the HTTP Access Mode 1
1.1.5 Setting the Maximum Number of VLAN Entries on Web 2
1.1.6 Setting the Maximum Number of Multicast Entries Displayed on Web 2
1.2 HTTPS Configuration 2
1.2.1 Setting the HTTP Access Mode 2
1.2.2 It is used to set the HTTPS port. 2
Chapter 2 Configuration Preparation 4
2.1 Accessing the Switch Through HTTP 4
2.1.1 Initially Accessing the Switch 4
2.1.2 Upgrading to the Web-Supported Version 5
2.2 Accessing a Switch Through Secure Links 5
2.3 Introduction of Web Interface 5
2.3.1 Top Control Bar 6
2.3.2 Navigation Bar 7
2.3.3 Configuration Area 7
2.3.4 Bottom Control Bar 8
2.3.5 Configuration Area 8
Chapter 3 Basic Configuration 9
3.1 Hostname Configuration 9
3.2 Time Management 10
Chapter 4 Configuration of the Physical Interface 11
4.1 Configuring Port Description 11
4.2 Configuring the Attributes of the Port 12
4.3 Rate control 12
4.4 Port mirroring 12
4.5 Loopback Detection 13
4.6 Port security 13
4.6.1 IP Binding Configuration 13
4.6.2 MAC Binding Configuration 14
4.6.3 Setting the Static MAC Filtration Mode 14
4.6.4 Static MAC Filtration Entries 14
4.6.5 Setting the Dynamic MAC Filtration Mode 15
4.7 Storm control 15
4.7.1 Broadcast Storm Control 15
4.7.2 Multicast Storm Control 16
4.7.3 Unknown Unicast Storm Control 17
4.8 Port Protect Group Configuration 17
4.8.1 Port Protect Group List 17
4.8.2 Port Protect Group Interface Configuration 18
Chapter 5 Layer-2 Configuration 19
5.1 VLAN Settings 20
5.1.1 VLAN List 20
5.1.2 VLAN Settings 20
5.2 GVRP Configuration 21

Table of Contents

5.2.1 GVRP Global Attribute Configuration 21
5.2.2 Global Interface Attribute Configuration 22
5.3 STP Configuration 21
5.3.1 STP Status Information 21
5.3.2 Configuring the Attributes of the STP Port 22
5.4 IGMP-Snooping Configuration 23
5.4.1 IGMP-Snooping Configuration 23
5.4.2 IGMP-Snooping VLAN List 23
5.4.3 Static Multicast Address 24
5.4.4 Multicast List 25
5.5 Setting Static ARP 25
5.6 Static MAC Address Configuration 26
5.7 LLDP Configuration 27
5.7.1 Configuring the Global Attributes of LLDP 27
5.7.2 LLDP Port Attribute Configuration 28
5.8 DDM Configuration 28
5.9 Link Aggregation Configuration 28
5.9.1 Port Aggregation Configuration 28
5.9.2 Configuring Load Balance of Port Aggregation Group 29
5.10 EAPS Ring Protection Configuration 29
5.10.1 EAPS Ring List 29
5.10.2 EAPS Ring Configuration 30
5.11 MEAPS Configuration 30
5.11.1 MEAPS Ring Configuration 30
5.11.2 MEAPS Ring Configuration 31
5.12 Backup Link Protocol Configuration 32
5.12.1 Backup Link Protocol Global Configuration 32
5.12.2 Backup Link Protocol Interface Configuration 32
5.13 DHCP Snooping Configuration 33
5.13.1 DHCP Snooping Global Attribute Configuration 33
5.13.2 DHCP Snooping VLAN Attribute Configuration 33
5.13.3 DHCP Snooping Interface Attribute Configuration 34
5.13.4 DHCP Snooping Manual Binding Configuration 35
5.14 MTU Configuration 35
5.15 PDP Configuration 36
5.15.1 Configuring the Global Attributes of PDP 36
5.15.2 Configuring the Attributes of the PDP Port 36
5.16 STP Configuration 36
5.16.1 STP Status Information 36
5.16.2 Configuring the Attributes of the STP Port 37
5.17 IGMP-Snooping Configuration 38
5.17.1 IGMP-Snooping Configuration 38
5.17.2 IGMP-Snooping VLAN List 38
5.17.3 Static Multicast Address 39
5.17.4 Multicast List 40
5.18 Setting Static ARP 40
5.19 Ring Protection Configuration 41
5.19.1 EAPS Ring List 41
5.19.2 EAPS Ring Configuration 41

Table of Contents

5.20 EVC Configuration 42
5.20.1 Global QinQ Configuration 42
5.20.2 Configuring the QinQ Port 43
5.21 DDM Configuration 43
Chapter 6 Layer-3 Configuration 44
6.1 Configuring the VLAN Interface 44
6.2 Setting the Static Route 45
6.3 IGMP Agent 46
6.3.1 Enabling the IGMP Agent 46
6.3.2 Setting the IGMP Agent 46
Chapter 7 Advanced Configuration 47
7.1 QoS Configuration 47
7.1.1 Configuring QoS Port 47
7.1.2 Global QoS Configuration 48
7.2 MAC Access Control List 48
7.2.1 Setting the Name of the MAC Access Control List 48
7.2.2 Setting the Rules of the MAC Access Control List 49
7.2.3 Applying the MAC Access Control List 49
7.3 IP Access Control List 50
7.3.1 Setting the Name of the IP Access Control List 50
7.3.2 Setting the Rules of the IP Access Control List 50
7.3.3 Applying the IP Access Control List 52
Chapter 8 Network Management Configuration 53
8.1 SNMP Configuration 53
8.1.1 SNMP Community Management 53
8.1.2 SNMP Host Management 54
8.2 RMON 54
8.2.1 RMON Statistic Information Configuration 54
8.2.2 RMON History Information Configuration 55
8.2.3 RMON Alarm Information Configuration 56
8.2.4 RMON Event Configuration 56
Chapter 9 Diagnosis Tools 58
9.1 Ping 58
9.1.1 Ping 58
Chapter 10 System Management 60
10.1 User Management 60
10.1.1 User List 60
10.1.2 Establishing a New User 61
10.2 Log Management 61
10.3 Managing the Configuration Files 62
10.3.1 Exporting the Configuration Information 62
10.3.2 Importing the Configuration Information 63
10.4 Software Management 63
10.4.1 Backing up the firmware Software 63
10.4.2 Upgrading the firmware Software 64
10.5 Resuming Initial Configuration 64
10.6 Rebooting the Device 65

Chapter 1 HTTP Switch Configuration

1.1 HTTP Configuration

Switch configuration can be conducted not only through command lines and SNMP but also through Web browser. The switches support the HTTP configuration, the abnormal packet timeout configuration, and so on.

1.1.1 Choosing the Prompt Language

Up to now, switches support two languages, that is, English and Chinese, and the two languages can be switched over through the following command.

Command	Purpose
ip http language {chinese | english}	Sets the prompt language of Web configuration to **Chinese** or **English**.

1.1.2 Setting the HTTP Port

Generally, the HTTP port is port 80 by default, and users can access a switch by entering the IP address directly; however, switches also support users to change the service port and after the service port is changed you have to use the IP address and the changed port to access switches. For example, if you set the IP address and the service port to **192.168.1.3** and **1234** respectively, the HTTP access address should be changed to **http:// 192.168.1.3:1234**. You'd better not use other common protocols' ports so that access collision should not happen. Because the ports used by a lot of protocols are hard to remember, you'd better use port IDs following port 1024.

Command	Purpose
ip http port { *portNumber* }	Sets the HTTP port.

1.1.3 Enabling the HTTP Service

Switches support to control the HTTP access. Only when the HTTP service is enabled can HTTP exchange happen between switch and PC and, when the HTTP service is closed, HTTP exchange stops.

Command	Purpose
ip http server	Enables the HTTP service.
ip http {*timeout*}	Configures the timeout time of HTTP abnormal packets.

1.1.4 Setting the HTTP Access Mode

You can access a switch through two access modes: HTTP access and HTTPS access, and you can use the following command to set the access mode to **HTTP**.

Command	Purpose
ip http http-access enable	Sets the HTTP access mode.

1.1.5 Setting the Maximum Number of VLAN Entries on Web Page

A switch supports at most 4094 VLANs and in most cases Web only displays parts of VLANs, that is, those VLANs users want to see. You can use the following command to set the maximum number of VLANs. The default maximum number of VLANs is 100.

Command	Purpose
ip http web max-vlan { *max-vlan* }	Sets the maximum number of VLAN entries displayed in a web page.

1.1.6 Setting the Maximum Number of Multicast Entries Displayed on a Web Page

A switch supports at most 100 multicast entries. You can run the following command to set the maximum number of multicast entries and Web then shows these multicast entries. The default maximum number of multicast entries is 15.

Command	Purpose
ip http web igmp-groups { *igmp-groups* }	Sets the maximum number of multicast entries displayed in a web page.

1.2 HTTPS Configuration

In order to improve the security of communications, switches support not only the HTTP protocol but also the HTTPS protocol. HTTPS is a security-purposed HTTP channel and it is added to the SSL layer under HTTP.

1.2.1 Setting the HTTP Access Mode

You can run the following command to set the access mode to **HTTPS**.

Command	Purpose
ip http ssl-access enable	Sets the HTTPS access mode.

1.2.2 It is used to set the HTTPS port.

As the HTTP port, HTTPS has its default service port, port 443, and you also can run the following command to change its service port. It is recommended to use those ports following port 1024 so as to avoid collision with other protocols' ports.

Parameter	Remarks
ip http secure-port	Sets the HTTPS port.

{*portNumber*}	

Chapter 2 Configuration Preparation

2.1 Accessing the Switch Through HTTP

When accessing the switch through Web, please make sure that the applied browser complies with the following requirements:

- HTML of version 4.0
- HTTP of version 1.1
- JavaScript™ of version 1.5

What's more, please ensure that the main program file, running on a switch, supports Web access and your computer has already connected the network in which the switch is located.

2.1.1 Initially Accessing the Switch

When the switch is initially used, you can use the Web access without any extra settings:

1. Modify the IP address of the network adapter and subnet mask of your computer to **192.168.0.1** and **255.255.255.0** respectively.

2. Open the Web browser and enter **192.168.0.1** in the address bar. It is noted that **192.168.0.1** is the default management address of the switch.

3,If the web browser is used, you can see the dialog box in figure 1. Both
the original username and the password are “admin”, which is capital sensitive.



Figure 1: ID checkup of WEB login

4. After successful authentication, the systematic information about the switch will appear on the web browser.

2.1.2 Upgrading to the Web-Supported Version

If your switch is upgraded to the Web-supported version during its operation and the switch has already stored its configuration files, the Web visit cannot be directly applied on the switch. Perform the following steps one by one to enable the Web visit on the switch:

1. Connect the console port of the switch with the accessory cable, or telnet to the management address of the switch through the computer.

2. Enter the global configuration mode of the switch through the command line, the DOS prompt of which is similar to “Switch_config#”.

3. If the management address of the switch is not configured, please create the VLAN interface and configure the IP address.

4. Enter the **ip http server** command in global configuration mode and start the Web service.

5. Run **username** to set the username and password of the switch. For how to use this command, refer to the “Security Configuration” section in the user manual.

After the above-mentioned steps are performed, you can enter the address of the switch in the Web browser to access the switch.

6. Enter **write** to store the current configuration to the configuration file.

2.2 Accessing a Switch Through Secure Links

The data between the WEB browser and the switch will not be encrypted if you access a switch through common HTTP. To encrypt these data, you can use the secure links, which are based on the secure sockets layer, to access the switch.

To do this, you should follow the following steps:

1. Connect the console port of the switch with the accessory cable, or telnet to the management address of the switch through the computer.

2. Enter the global configuration mode of the switch through the command line, the DOS prompt of which is similar to “Switch_config#”.

3. If the management address of the switch is not configured, please create the VLAN interface and configure the IP address.

4. Enter the **ip http server** command in global configuration mode and start the Web service.

5. Run **username** to set the username and password of the switch. For how to use this command, refer to the “Security Configuration” section in the user manual.

6. Run ip http ssl-access enable to enable secure access.

7. Run **no ip http http-access enable** to forbid to access the switch through insecure links.

8. Enter **write** to store the current configuration to the configuration file.

9. Open the WEB browser on the PC that the switch connects, enter **https://192.168.0.1** on the address bar (**192.168.0.1** stands for the management IP address of the switch) and then press the **Enter** key. Then the switch can be accessed through the secure links.

2.3 Introduction of Web Interface

The Web homepage appears after login, as shown in figure 2:

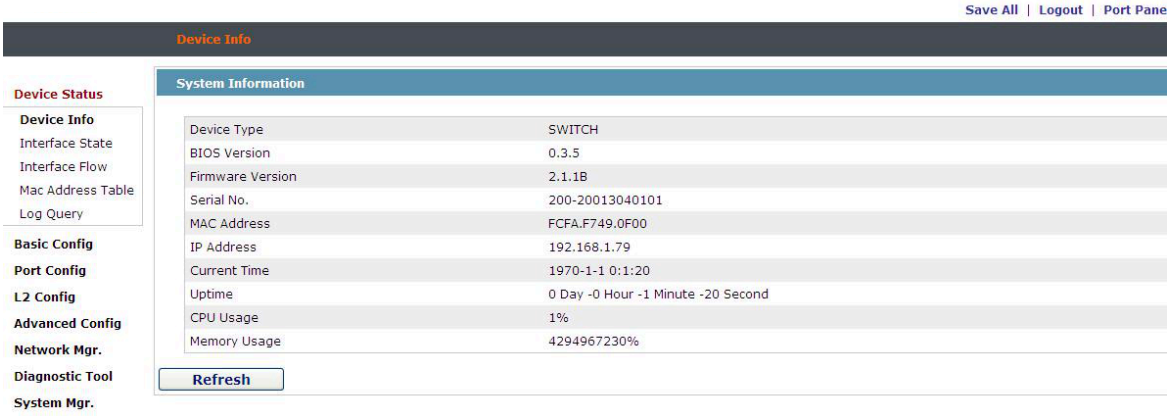


Figure 2: Web homepage

The whole homepage consists of the top control bar, the navigation bar, the configuration area and the bottom control bar.

2.3.1 Top Control Bar



Figure 3: Top control bar

Save All	Write the current settings to the configuration file of the device. It is equivalent to the execution of the **write** command. The configuration that is made through Web will not be promptly written to the configuration file after validation. If you click “Save All”, the unsaved configuration will be lost after rebooting.
English	The interface will turn into the English version.
Chinese	The interface will turn into the Chinese version.
Logout	Exit from the current login state. After you click "logout", you have to enter the username and the password again if you want to continue the Web function.

After you configure the device, the result of the previous step will appear on the left side of the top control bar. If error occurs, please check your configuration and retry it later.

2.3.2 Navigation Bar



Figure 4 Navigation bar

The contents in the navigation bar are shown in a form of list and are classified according to types. By default, the list is located at “Runtime Info”. If a certain item need be configured, please click the group name and then the sub-item. For example, to browse the flux of the current port, you have to click “Interface State" and then “Interface Flow”.

Note:
The limited user can only browse the state of the device and cannot modify the configuration of the device. If you log on to the Web with limited user’s permissions, only “Interface State” will appear.

2.3.3 Configuration Area

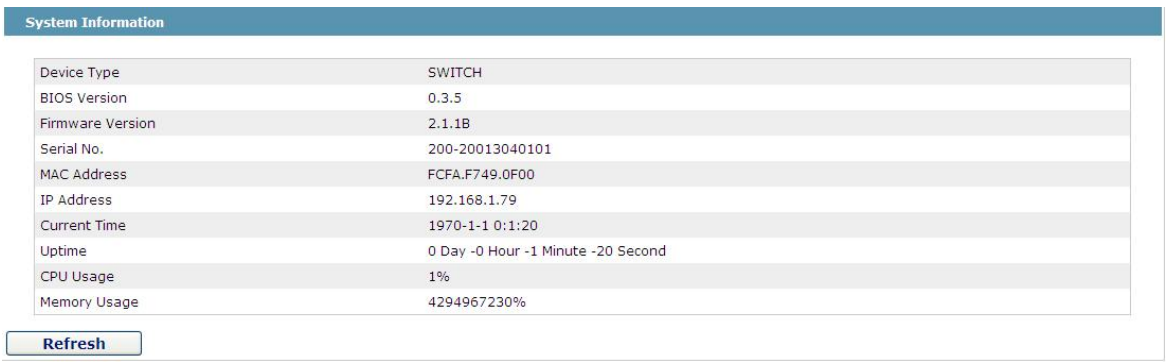


Figure 5 Configuration Area

The configuration display area shows the state and configuration of the device. The contents of this area can be modified by the clicking of the items in the navigation bar.

2.3.4 Bottom Control Bar



Figure 6: Bottom control bar

If you click the **About** button on the top control bar, the bottom control bar appears. The main function of the bottom control bar is to realize the automatic refreshing of the configuration display area. For example, if you click “Interface Flow” in the navigation bar and then click “Refresh”, the flow of the interface can be continuously monitored.

After you click “Refresh”, the countdown of the next-time refresh will appear on the left side. You can modify the countdown settings by clicking the dropdown list.

Note:
The smaller the countdown value is set, that is, the higher the frequency is, the higher the CPU usage is.

2.3.5 Configuration Area

The configuration area is to show the content that is selected in the navigation area. The configuration area always contains one or more buttons, and their functions are listed in the following table:

Refresh	Refresh the content shown in the current configuration area.
Apply	Apply the modified configuration to the device. The application of the configuration does not mean that the configuration is saved in the configuration file. To save the configuration, you have to click “Save All” on the top control bar.
Reset	Means discarding the modification of the sheet. The content of the sheet will be reset.
New	Creates a list item. For example, you can create a VLAN item or a new user.
Delete	Deletes an item in the list.
Back	Go back to the previous-level configuration page.

Chapter 3 Basic Configuration



Figure 1 A list of basic configuration

3.1 Hostname Configuration

If you click **Basic Config -> Hostname Config** in the navigation bar, the **Hostname Configuration** page appears, as shown in figure 3.

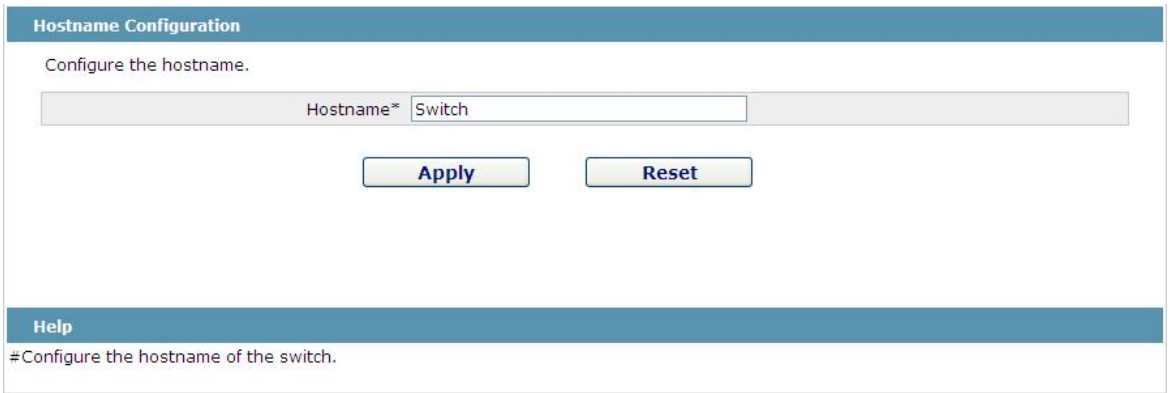


Figure 3 Hostname configuration

The hostname will be displayed in the login dialog box.

The default name of the device is “Switch”. You can enter the new hostname in the text box shown in figure 3 and then click “Apply”.

3.2 Time Management

If you click **System Manage -> Time Manage**, the **Time Setting** page appears.

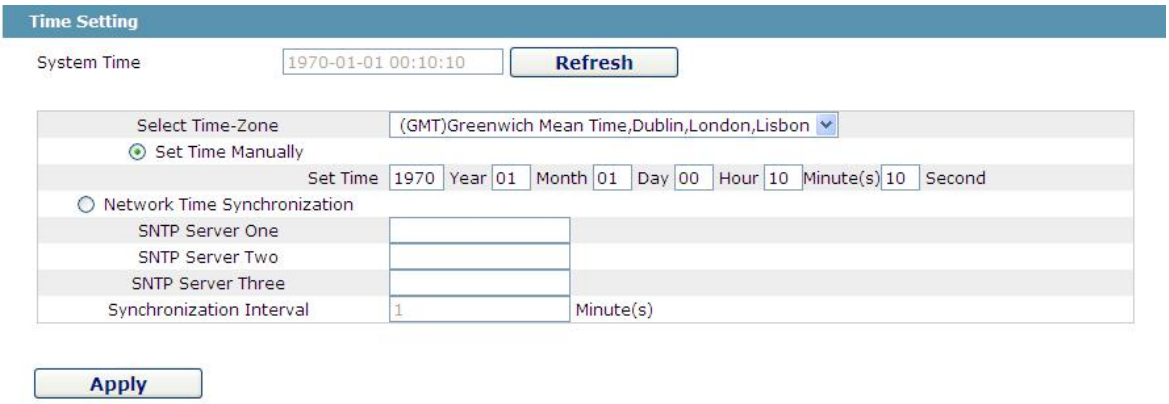


Figure 4 Clock management

To refresh the clock of the displayed device, click “Refresh”.

In the “Select Time-Zone” dropdown box select the time zone where the device is located. When you select “Set Time Manually”, you can set the time of the device manually. When you select “Network Time Synchronization”, you can designate 3 SNTP servers for the device and set the interval of time synchronization.

Chapter 4 Configuration of the Physical Interface



Figure 1: Physical port configuration list

4.1 Configuring Port Description

If you click **Physical port config -> Port description Config** in the navigation bar, the **Port description Configuration** page appears, as shown in figure 2.

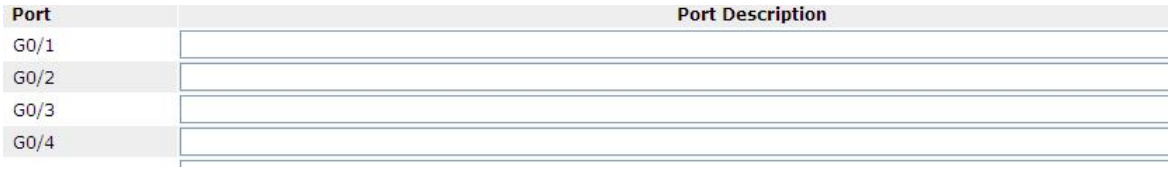
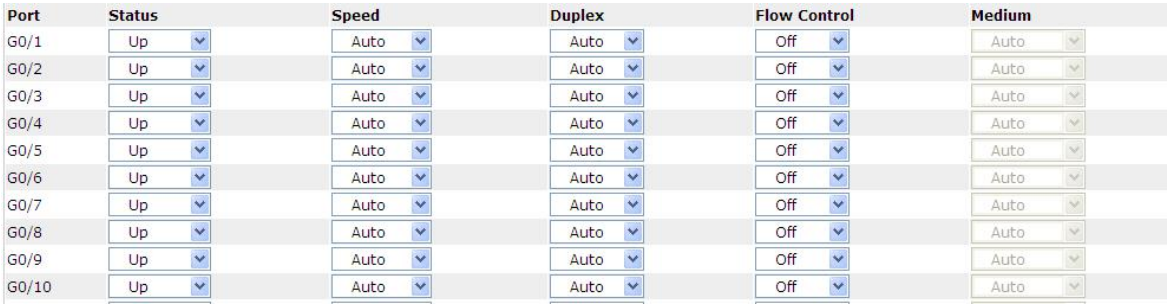


Figure 2: Port description configuration

You can modify the port description on this page and enter up to 120 characters. The description of the VLAN port cannot be set at present.

4.2 Configuring the Attributes of the Port

If you click **Physical port config -> Port attribute Config** in the navigation bar, the **Port Attribute Configuration** page appears, as shown in figure 3.



Port	Status	Speed	Duplex	Flow Control	Medium
G0/1	Up	Auto	Auto	Off	Auto
G0/2	Up	Auto	Auto	Off	Auto
G0/3	Up	Auto	Auto	Off	Auto
G0/4	Up	Auto	Auto	Off	Auto
G0/5	Up	Auto	Auto	Off	Auto
G0/6	Up	Auto	Auto	Off	Auto
G0/7	Up	Auto	Auto	Off	Auto
G0/8	Up	Auto	Auto	Off	Auto
G0/9	Up	Auto	Auto	Off	Auto
G0/10	Up	Auto	Auto	Off	Auto

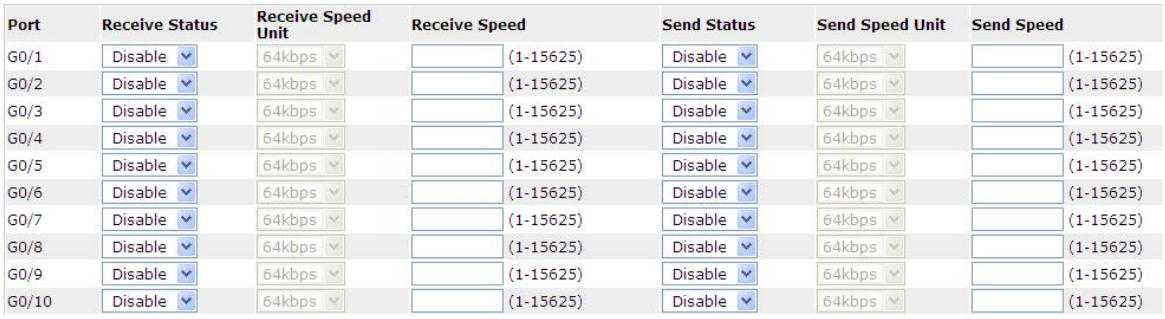
Figure 3 Configuring the port attributes

On this page you can modify the on/off status, rate, duplex mode, flow control status and medium type of a port.

Note:
1. The Web page does not support the speed and duplex mode of the fast-Ethernet port.
2. After the speed or duplex mode of a port is modified, the link state of the port may be switched over and the network communication may be impaired.

4.3 Rate control

If you click **Physical port Config -> Port rate-limit Config** in the navigation bar, the **Port rate limit** page appears, as shown in figure 4.



Port	Receive Status	Receive Speed Unit	Receive Speed	Send Status	Send Speed Unit	Send Speed
G0/1	Disable	64kbps	(1-15625)	Disable	64kbps	(1-15625)
G0/2	Disable	64kbps	(1-15625)	Disable	64kbps	(1-15625)
G0/3	Disable	64kbps	(1-15625)	Disable	64kbps	(1-15625)
G0/4	Disable	64kbps	(1-15625)	Disable	64kbps	(1-15625)
G0/5	Disable	64kbps	(1-15625)	Disable	64kbps	(1-15625)
G0/6	Disable	64kbps	(1-15625)	Disable	64kbps	(1-15625)
G0/7	Disable	64kbps	(1-15625)	Disable	64kbps	(1-15625)
G0/8	Disable	64kbps	(1-15625)	Disable	64kbps	(1-15625)
G0/9	Disable	64kbps	(1-15625)	Disable	64kbps	(1-15625)
G0/10	Disable	64kbps	(1-15625)	Disable	64kbps	(1-15625)

Figure 4: Port's rate limit

On this page you can set the reception speed and transmission speed of a port. By default, all ports have no speed limited.

4.4 Port mirroring

If you click **Physical port Config -> Port Mirror** in the navigation bar, the **Port Mirror Config** page appears, as shown in figure 4-5.



Figure 4-5 Port mirror configuration

Click the dropdown list on the right side of "Mirror Port" and select a port to be the destination port of mirror.

Click a checkbox and select a source port of mirror, that is, a mirrored port.

RX	The received packets will be mirrored to the destination port.
TX	The transmitted packets will be mirrored to a destination port.
RX & TX	The received and transmitted packets will be mirrored simultaneously.

4.5 Loopback Detection

If you click **Physical port Config -> Port loopback detection** in the navigation bar, the **Setting the port loopback detection** page appears, as shown in figure 4-6.



Figure 4-6: Port loopback detection

You can set the loopback detection cycle on the **Loopback Detection** page.

4.6 Port security

4.6.1 IP Binding Configuration

If you click **Physical port Config -> Port Security -> IP bind** in the navigation bar, the **Configure the IP-Binding Info** page appears, as shown in figure 4-7.

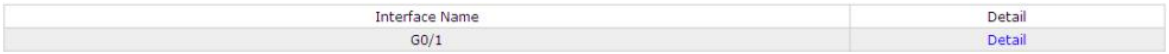


Figure 4-7 IP binding configuration

Click “Detail” and then you can conduct the binding of the source IP address for each physical port. In this way, the IP address that is allowed to visit the port will be limited.



Figure 4-8 Setting the binding of the source IP address

4.6.2 MAC Binding Configuration

If you click **Physical port Config -> Port Security -> MAC bind** in the navigation bar, the **Configure the MAC-Binding Info** page appears, as shown in figure 4-10.



Figure 4-9 MAC binding configuration

Click “Detail” and then you can conduct the binding of the source MAC address for each physical port. In this way, the MAC address that is allowed to visit the port will be limited.



Figure 4-10 Setting the binding of the source MAC address

4.6.3 Setting the Static MAC Filtration Mode

If you click **Physical port Config -> Port Security -> Static MAC filtration mode** in the navigation bar, the **Configure the static MAC filtration mode** page appears, as shown in figure 4-11.



Figure 4-11: Setting the static MAC filtration mode

On this page you can set the static MAC filtration mode. By default, the static MAC filter is disabled. Also, the static MAC filter mode cannot be set on ports in trunk mode.

4.6.4 Static MAC Filtration Entries

If you click **Physical port Config -> Port security -> Static MAC filtration entries** in the navigation bar, the **Setting the static MAC filtration entries** page appears.



Figure 4-12: Static MAC filtration entry list

If you click “Detail”, you can conduct the binding of the source MAC address for each physical port. According to the configured static MAC filtration mode, the MAC address of a port can be limited, allowed or forbidden to visit.



Figure 4-13: Setting static MAC filtration entries

4.6.5 Setting the Dynamic MAC Filtration Mode

If you click **Physical port Config -> Port Security -> Dynamic MAC filtration mode** in the navigation bar, the **Configure the dynamic MAC filtration mode** page appears, as shown in figure 4-14.



Figure 4-14: Setting the dynamic MAC filtration mode

You can set the dynamic MAC filtration mode and the allowable maximum number of addresses on this page. By default, the dynamic MAC filtration mode is disabled and the maximum number of addresses is 1.

4.7 Storm control

In the navigation bar, click **Physical port Config -> Storm control**. The system then enters the page, on which the broadcast/multicast/unknown unicast storm control can be set.

4.7.1 Broadcast Storm Control

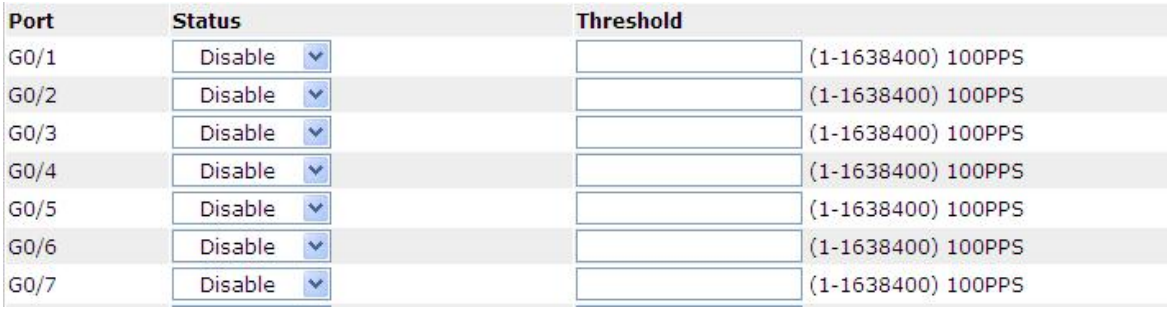


Figure 5 Broadcast storm control

Through the dropdown boxes in the **Status** column, you can decide whether to enable broadcast storm control on a port. In the **Threshold** column you can enter the threshold of the broadcast packets. The legal threshold range for each port is given behind the threshold.

4.7.2 Multicast Storm Control

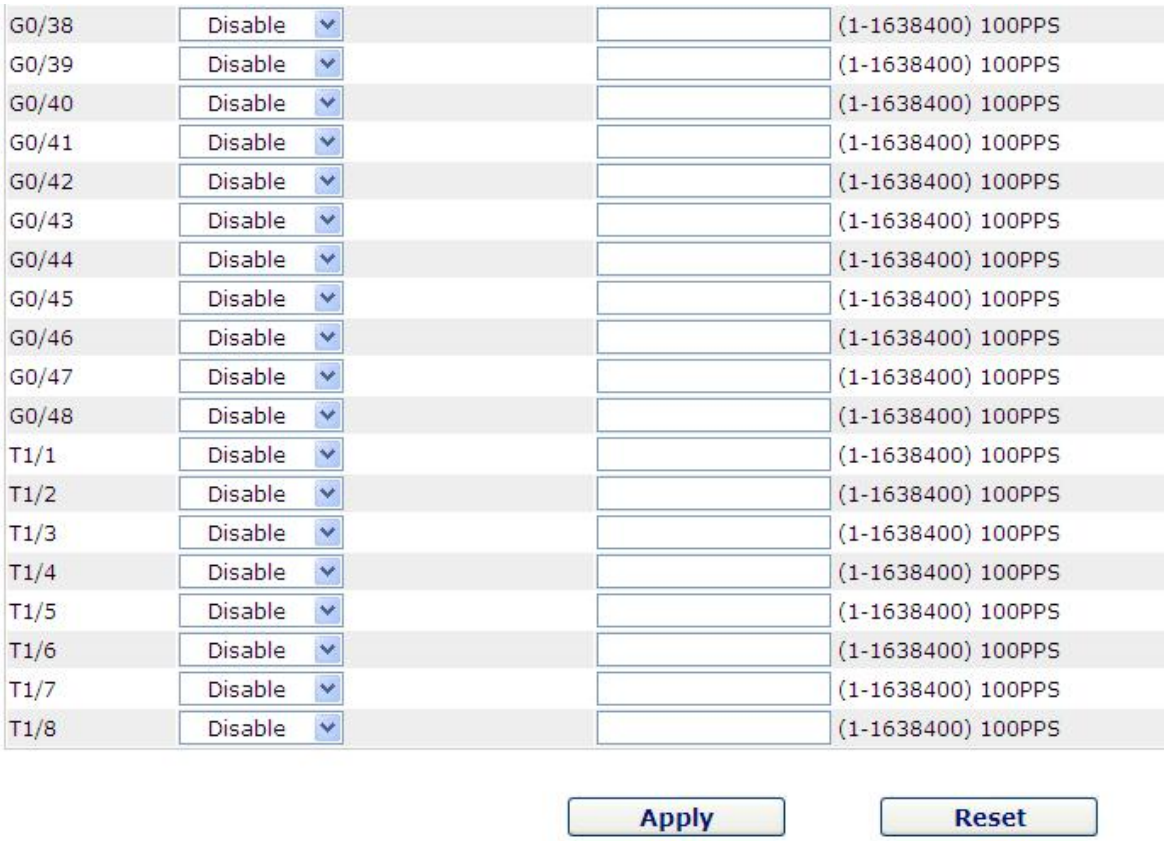


Figure 6 Setting the broadcast storm control

Through the dropdown boxes in the **Status** column, you can decide whether to enable multicast storm control on a port. In the **Threshold** column you can enter the threshold of the multicast packets. The legal threshold range for each port is given behind the threshold.

4.7.3 Unknown Unicast Storm Control



Figure 7 Unknown unicast storm control

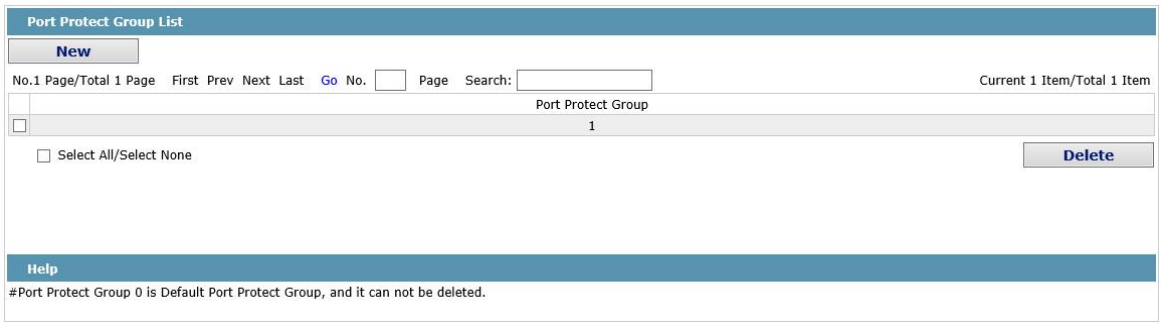
In the **Threshold** column you can enter the threshold of the broadcast packets. The legal threshold range for each port is given behind the threshold.

4.8 Port Protect Group Configuration

Click "Port Config" -> “Port Protect Group Config” in the navigation bar, and enter the configuration page of Port Protect Group List and Port Protect Group Interface Config.

4.8.1 Port Protect Group List

Click "Port Config" -> “Port Protect Group Config” -> “Port Protect Group List” in the navigation bar, and enter the configuration page of “Port Protect Group List”.



Click “New” to create a new port protect group, as shown in the above figure.

Tick one port protect group and delete it. The port protect group is 0 by default, which cannot be deleted.



4.8.2 Port Protect Group Interface Configuration

Click "Port Config" -> “Port Protect Group Config” -> “Port Protect Group Interface Config” in the navigation bar, and enter the configuration page of “Port Protect Group Interface Config”.



The port protect group must be a created group. If one port has configured the default protect group, other ports can only be configured with the default protect group.

Chapter 5 Layer-2 Configuration



Figure 1: Layer-2 configuration list

5.1 VLAN Settings

5.1.1 VLAN List

If you click **Layer-2 Config -> VLAN Config** in the navigation bar, the **VLAN Config** page appears, as shown in figure 2.



Figure 2 VLAN configuration

The VLAN list will display VLAN items that exist in the current device according to the ascending order. In case of lots of items, you can look for the to-be-configured VLAN through the buttons like “Prev”, “Next” and “Search”.

You can click “New” to create a new VLAN.

You can also click “Edit” at the end of a VLAN item to modify the VLAN name and the port’s attributes in the VLAN.

If you select the checkbox before a VLAN and then click “Delete”, the selected VLAN will be deleted.

Note:
By default, a VLAN list can display up to 100 VLAN items. If you want to configure more VLANs through Web, please log on to the switch through the Console port or Telnet, enter the global configuration mode and then run the “**ip http web max-vlan**” command to modify the maximum number of VLANs that will be displayed.

5.1.2 VLAN Settings

If you click "New" or “Edit” in the VLAN list, the VLAN configuration page appears, on which new VLANs can be created or the attributes of an existent VLAN can be modified.

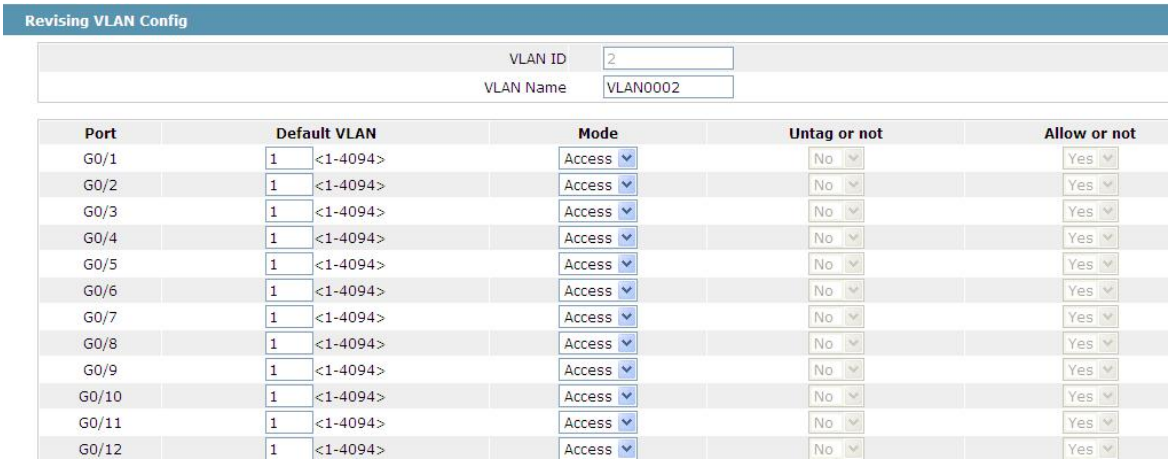


Figure 3 Revising VLAN configuration

If you want to create a new VLAN, enter a VLAN ID and a VLAN name; the VLAN name can be null.

Through the port list, you can set for each port the default VLAN , the VLAN mode (Trunk or Access), whether to allow the entrance of current VLAN packets and whether to execute the untagging of the current VLAN when the port works as the egress port.

Note:
When a port in Trunk mode serves as an egress port, it will untag the default VLAN by default.

5.2 GVRP Configuration

5.2.1 GVRP Global Attribute Configuration

If you click **Layer-2 Config -> GVRP Config -> GVRP Global Config** in the navigation bar, the **GVRP Global Config** page appears, as shown the following Figure.



Figure 9 GVRP Global Configuration

You can enable or disable the global GVRP protocol and sets whether the dynamic vlan is only effective on the registration interface.

5.2.2 Global Interface Attribute Configuration

If you click **Layer-2 Config -> GVRP Config -> GVRP Interface Config** in the navigation bar, the **GVRP Interface Config** page appears, as shown the following Figure.



Figure 10 Global Interface Attribute Configuration

To enable or disable GVRP protocol on the GVRP interface configuration.

5.3 STP Configuration

5.3.1 STP Status Information

If you click **Layer-2 Config -> STP Config** in the navigation bar, the **STP Config** page appears, as shown in figure 10.



Figure 10 Configuring the global attributes of STP

The root STP configuration information and the STP port's status are only-read.

On the local STP configuration page, you can modify the running STP mode by clicking the Protocol type dropdown box. The STP modes include STP, RSTP and disabled STP.

The priority and the time need be configured for different modes.

Note:
The change of the STP mode may lead to the interruption of the network.

5.3.2 Configuring the Attributes of the STP Port

If you click the "Configure RSTP Port" option, the "Configure RSTP Port" page appears.

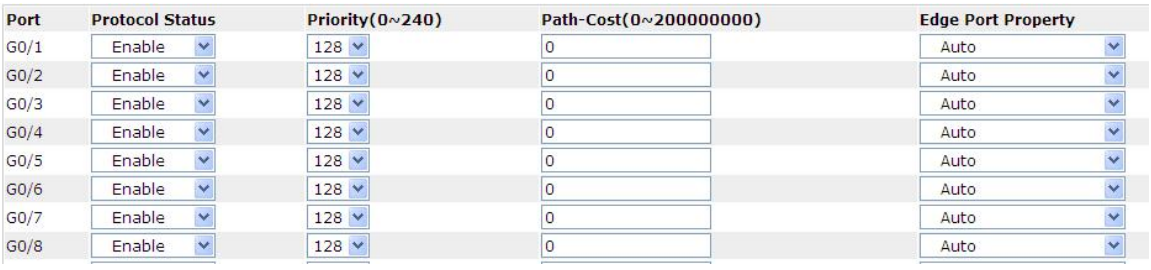


Figure 11 Configuring the attributes of RSTP

The configuration of the attributes of the port is irrelative of the global STP mode. For example, if the protocol status is set to "Disable" and the STP mode is also changed, the port will not run the protocol in the new mode.

The default value of the path cost of the port is 0, meaning the path cost is automatically calculated according to the speed of the port. If you want to change the path cost, please enter another value.

5.4 IGMP-Snooping Configuration

5.4.1 IGMP-Snooping Configuration

If you click **Layer-2 Config -> IGMP snooping**, the IGMP-Snooping configuration page appears.



Figure 12 IGMP-snooping configuration

On this page you can set whether to make a switch to forward unknown multicasts, whether to enable IGMP snooping, and whether to configure the switch as the querier of IGMP.

5.4.2 IGMP-Snooping VLAN List

If you click **Layer-2 Config -> IGMP snooping vlan list**, the **IGMP-Snooping VLAN list** page appears.



	VLAN ID	Status of the IGMP Snooping Vlan	Immediate-leave	Multicast Router's Port	Operate
☐	1	Running	Disable	SWITCH(querier);	Edit

Figure 13: IGMP-snooping VLAN list

If you click **New**, IGMP-snooping VLAN configuration can be done. Through Web up to 8 physical ports can be set on each IGMP snooping VLAN. If you click **Cancel**, a selected IGMP-Snooping VLAN can be deleted; if you click **Edit**, you can modify the member port, running status and immediate-leave of IGMP-Snooping VLAN.

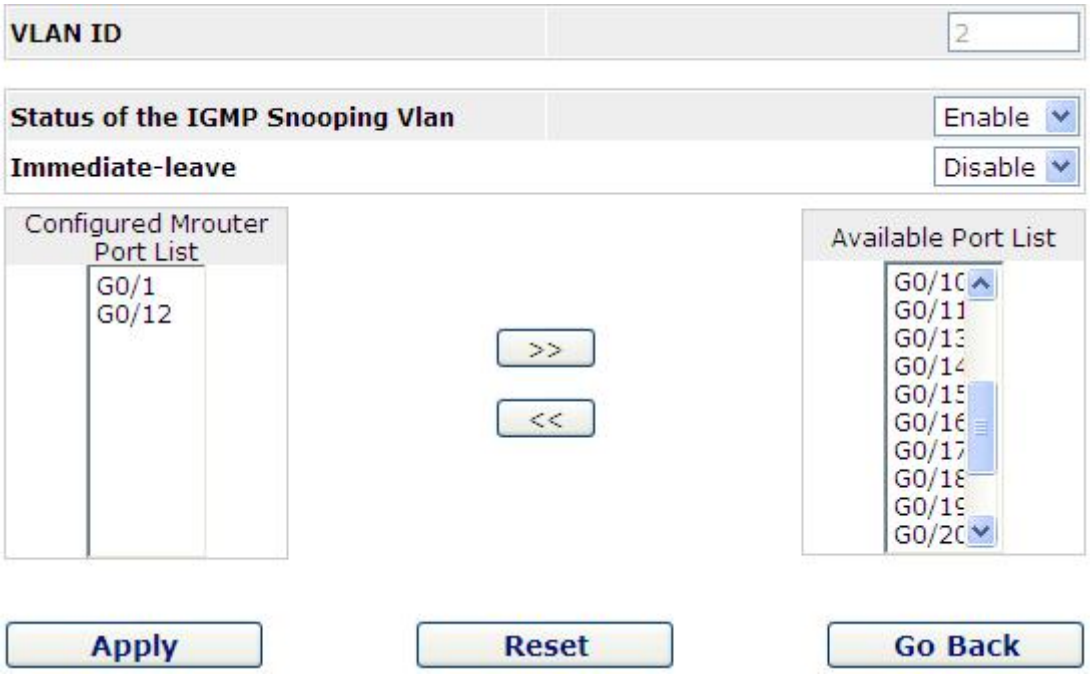


Figure 14: Static routing port of IGMP VLAN

When an IGMP-Snooping VLAN is created, its VLAN ID can be modified; but when the IGMP-Snooping VLAN is modified, its VLAN ID cannot be modified.

You can click "**>>**" and "**<<**" to delete and add a routing port.

5.4.3 Static Multicast Address

If you click **Static multicast address**, the **Setting the static multicast address** page appears.

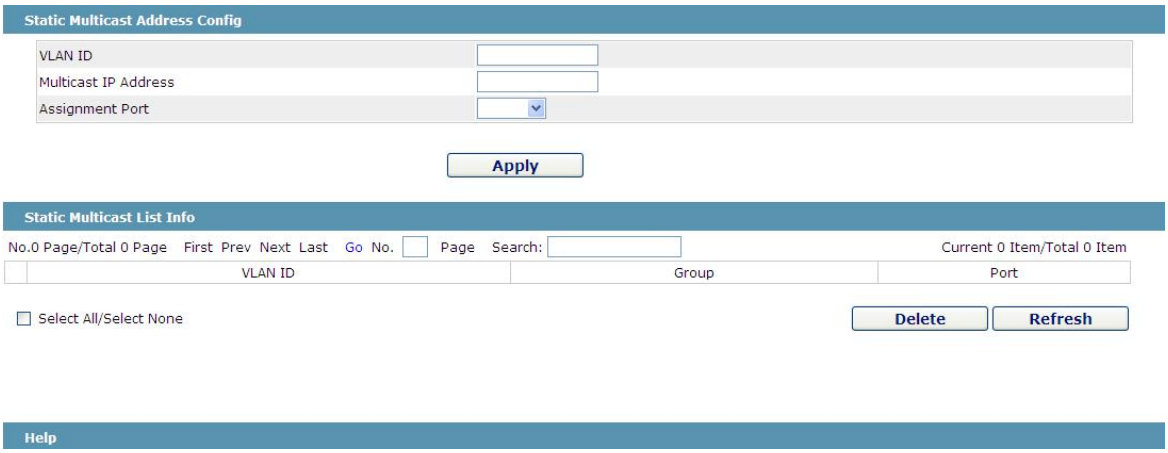


Figure 15 Multicast List

On this page, the currently existing static multicast groups and port groups in each static multicast group are shown.

Click "Refresh" to refresh the contents in the list.

5.4.4 Multicast List

Click the **Multicast List Info** option on the top of the page and the **Multicast List Info** page appears.

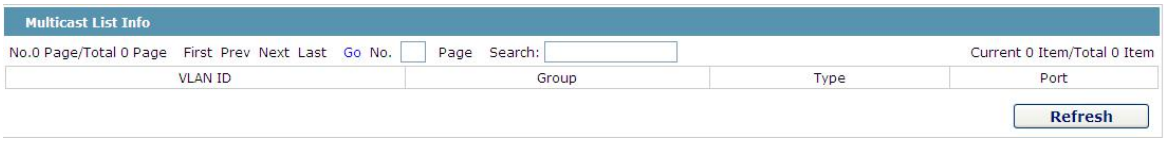


Figure 16 Multicast List

On this page the multicat groups, which are existent in the current network and are in the statistics of IGMP snooping, as well as port sets which members in each group belong to are dislayed.

Click “Refresh” to refresh the contents in the list.

Note:
By default, a multicast list can display up to 15 VLAN items. You can modify the number of multicast items by running **ip http web igmp-groups** after you log on to the device through the Console port or Telnet.

5.5 Setting Static ARP

If you click **Layer-2 Config -> Static ARP Config**, the static ARP configuration page appears.

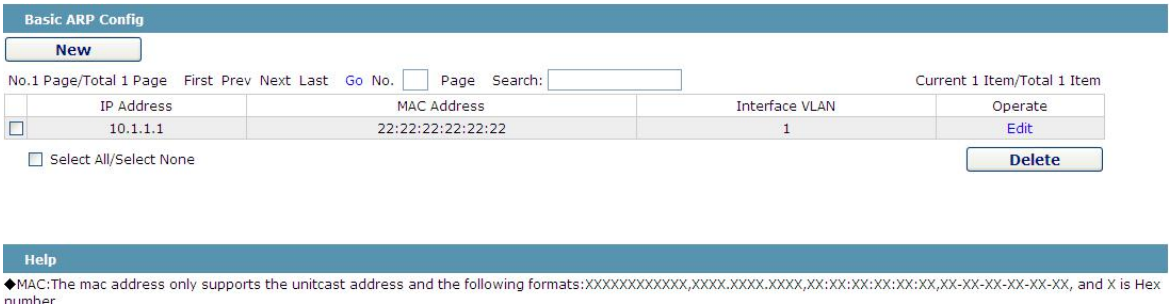


Figure 17 Displaying static ARP

You can click **New** to add an ARP entry. If the **Alias** column is selected, it means to answer the ARP request of the designated IP address.

If you click Edit, you can modify the current ARP entry.

If you click Cancel, you can cancel the chosen ARP entry.

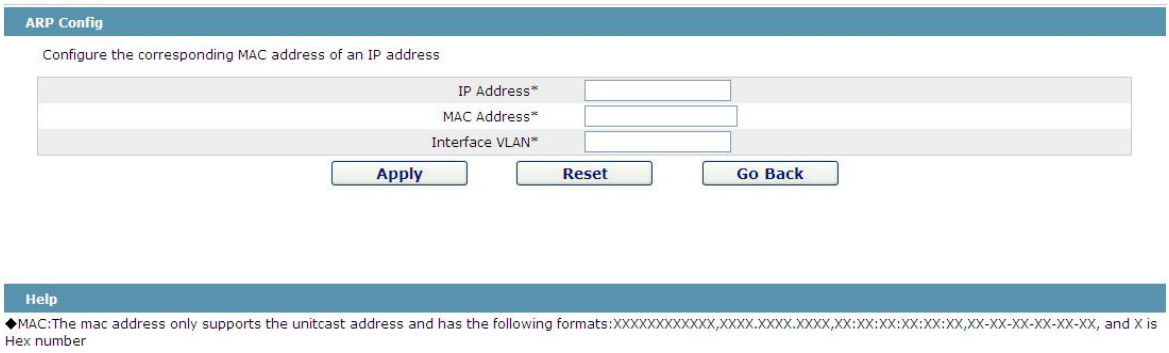


Figure 18 Setting static ARP

5.6 Static MAC Address Configuration

If you click **Layer-2 Config -> Static MAC Config -> Static MAC List**, the **Static MAC Address List Info** page appears.

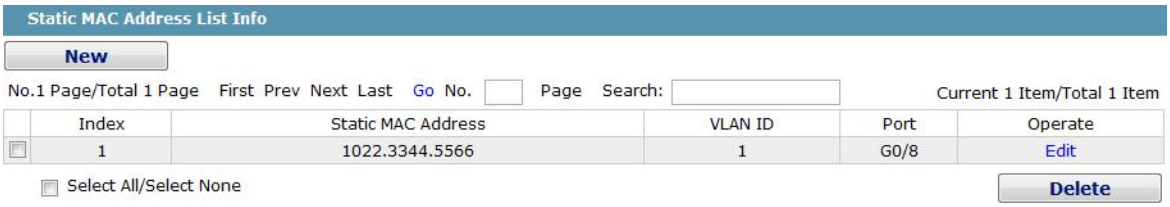


Figure 22 Setting Static MAC Address List Info

Click **New** to designate static MAC address and VLAN. The unicast MAC address can only configure one interface. Multiple MAC addresses can configure multiple interfaces.

Click **Edit** to modify the static MAC address.

Click **Delete** to delete the selected MAC address table.

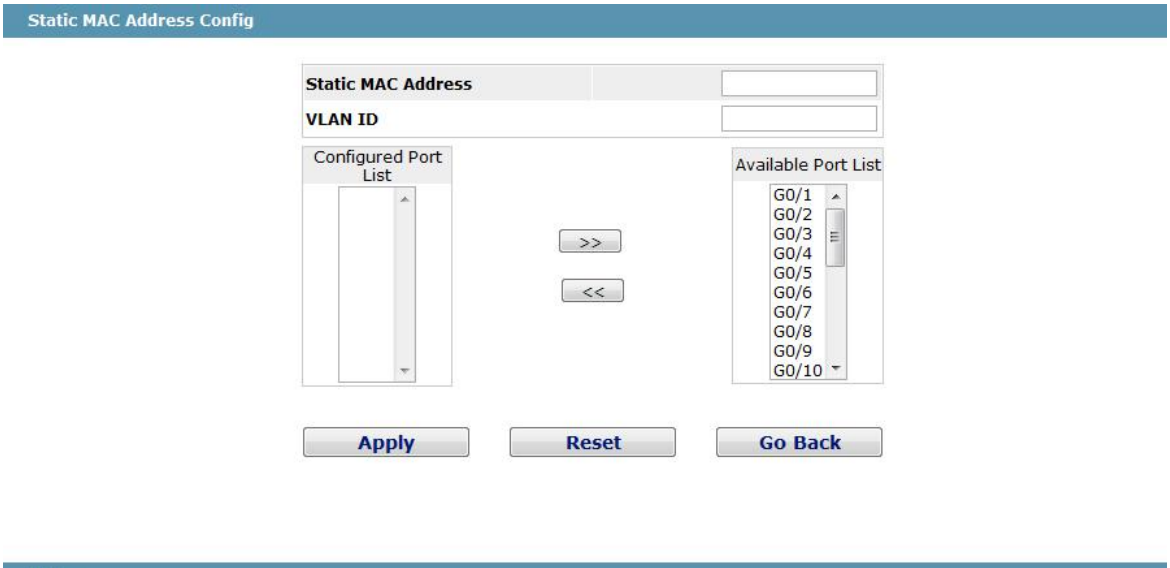


Figure 19 Static MAC Address Config

5.7 LLDP Configuration

5.7.1 Configuring the Global Attributes of LLDP

If you click **Layer-2 Config -> LLDP Config -> LLDP Global Config** in the navigation bar, the **Basic Config of LLDP Protocol** page appears, as shown in the following Figure.

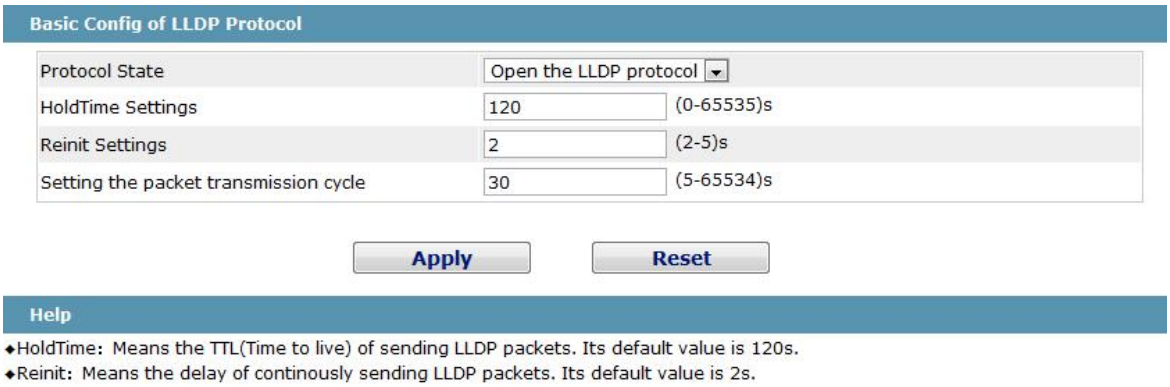


Figure11 Configuring the Global Attributes of LLDP

You can choose to enable LLDP or disable it. When you choose to disable LLDP, you cannot configure LLDP.

The “HoldTime” parameter means the ttl value of the packet that is transmitted by LLDP. Its default value is 120s.

The “Reinit” parameter means the delay of successive packet transmission of LLDP. Its default value is 2s.

5.7.2 LLDP Port Attribute Configuration

If you click **Layer-2 Config -> LLDP Config -> LLDP Interface Config** in the navigation bar, the **LLDP Port Config** page appears.

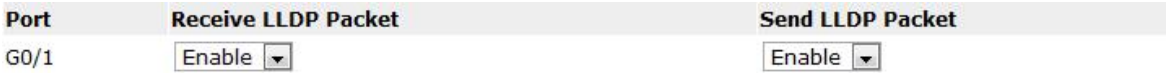


Figure 12 Configuring the LLDP port

After the LLDP port is configured, you can enable or disable LLDP on this port.

5.8 DDM Configuration

If you click **L2 Config -> DDM Config** in the navigation bar, the **DDM configuration** page appears, as shown in figure 5-21.

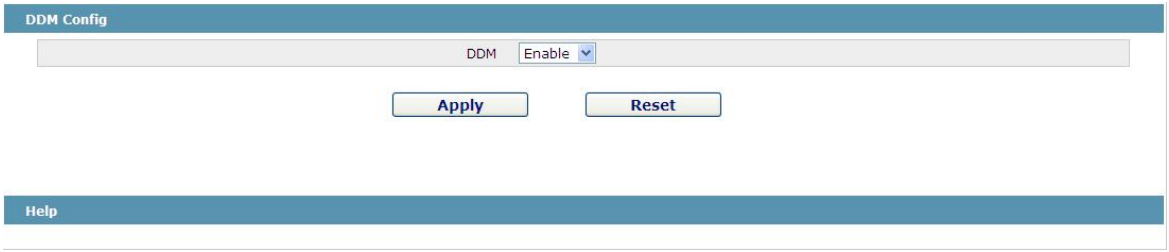
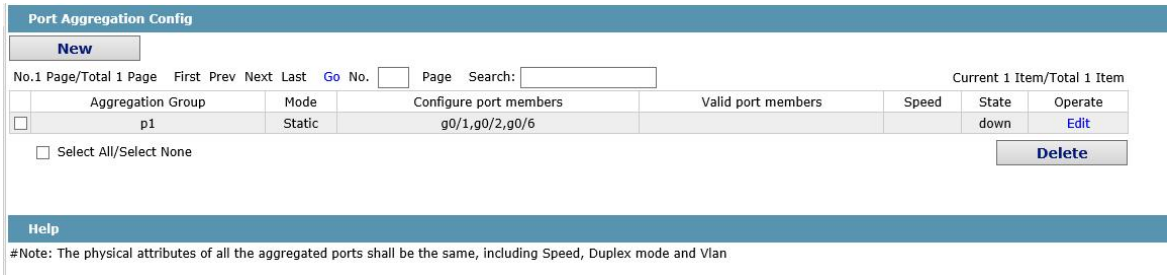


Figure 5-21: DDM configuration

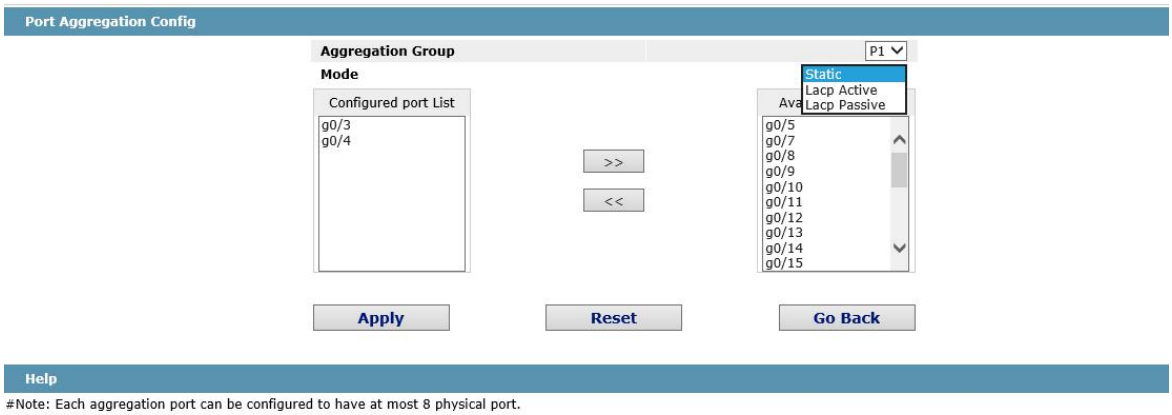
5.9 Link Aggregation Configuration

5.9.1 Port Aggregation Configuration

If you click Advanced Config -> Link aggregation Config in the navigation bar, the Link aggregation Config page appears, as shown in figure 22.



If you click New, an aggregation group can be created. Up to 32 aggregation groups can be configured through Web and up to 8 physical ports in each group can be aggregated. If you click Cancel, you can delete a selected aggregation group; if you click Modify, you can modify the member port and the aggregation mode.



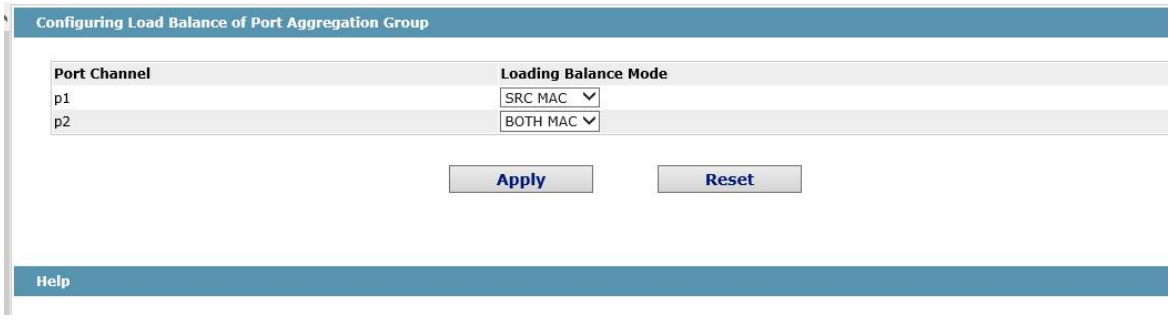
An aggregation group is selectable when it is created but is not selectable when it is modified.

When a member port exists on the aggregation port, you can choose the aggregation mode to be Static, LACP Active or LACP Passive.

You can click >> and << to delete and add a member port in the aggregation group.

5.9.2 Configuring Load Balance of Port Aggregation Group

Some models support aggregation group based load balance mode configuration and some not but can be configured in the global configuration mode.

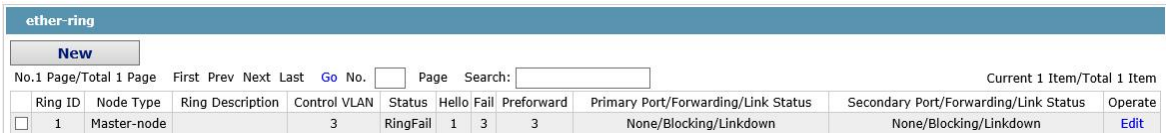


The user can adopt varied aggregation modes for different aggregation groups.

5.10 EAPS Ring Protection Configuration

5.10.1 EAPS Ring List

If you click Layer-2 Config -> Ring Protection ->EAPS Config, the EAPS Ring Config page appears.



In the list shows the currently configured EAPS ring, including the status of the ring, the forwarding status of the port and the status of the link.

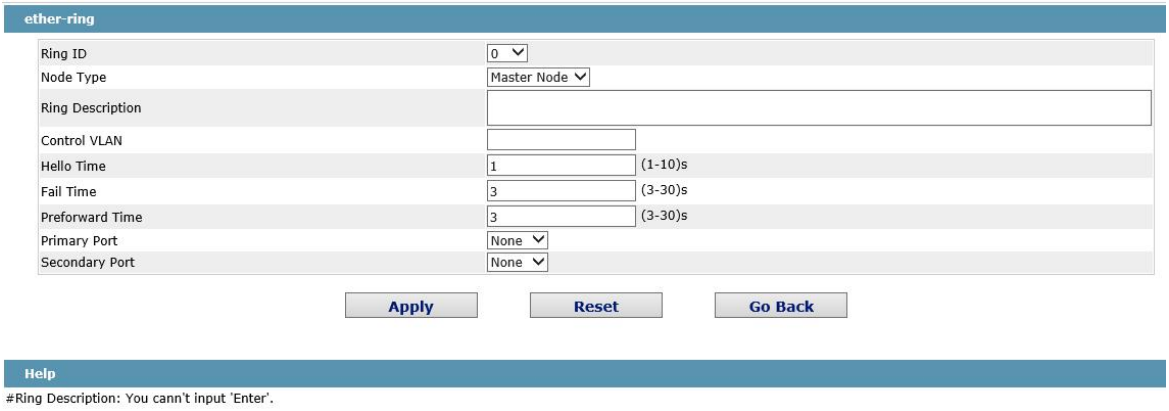
Click “New” to create a new EAPS ring.

Click the “Operate” option to configure the “Time” parameter of the ring.

Note:
1. The system can support 8 EAPS rings.
2. After a ring is configured, its port, node type and control Vlan cannot be modified. If the port of the ring, the node type or the control Vlan need be adjusted, please delete the ring and then establish a new one.

5.10.2 EAPS Ring Configuration

If you click “New” on the EAPS ring list, or “Operate” on the right side of a ring item, the “Configure EAPS” page appears.



Note:
If you want to modify a ring, on this page the node type, the control VLAN, the primary port and the secondary port cannot be modified.

In the dropdown box on the right of “Ring ID”, select an ID as a ring ID. The ring IDs of all devices on the same ring must be the same.

The dropdown box on the right of “Node Type” is used to select the type of the node. Please note that only one master node can be configured on a ring.

Enter a value between 1 and 4094 in the text box on the right of “Control VLAN” as the control VLAN ID. When a ring is established, the control VLAN will be automatically established too. Please note that if the designated control VLAN is 1 and the VLAN of the control device is also 1 the control device cannot access the control VLAN. Additionally, please do not enter a control VLAN ID that is same as that of another ring.

In the text boxes of “Primary Port” and “Secondary Port”, select a port as the ring port respectively. If "Node Type" is selected as “Transit-Node”, the two ports will be automatically set to transit ports.

Click “Apply” to finish EAPS ring configuration, click “Reset” to resume the initial values of the configuration, or click “Return” to go back to the EAPS list page.

5.11 MEAPS Configuration

5.11.1 MEAPS Ring Configuration

If you click Layer-2 Config -> Multiple Ring Protection -> Multiple Ring Protection on the navigation bar, the Multiple Ring Protection Configuration page appears.



The list shows the current configured MEAPS ring, including Domain ID, Ring ID, Ring type, Node type, Control Vlan, Hello Time, Failed Time, Pre Forward Time, primary port and secondary port.

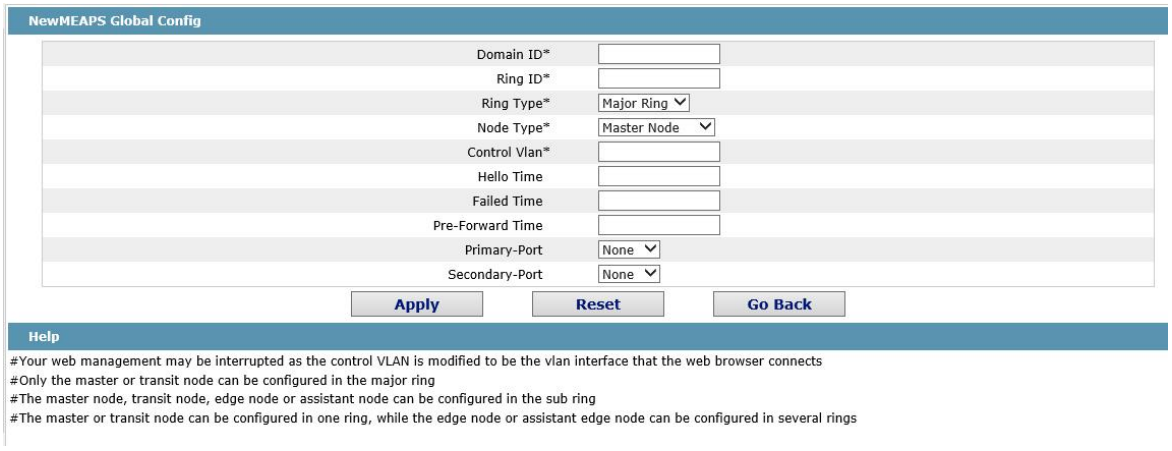
Click New to create a MEAPS ring.

Click Edit on the right and configure the time parameter and the primary and secondary port of the ring.

Note:
1. The system supports 4 MEAPS (0-3).
2. One domain supports 8 rings (0-7).
3. Once one MEAPS is configured, its Domain ID, ring ID, ring type, node type and control Vlan cannot be modified. If adjustment is needed, please delete the Ethernet ring and reset it.

5.11.2 MEAPS Ring Configuration

If you click New on the Multiple Ring Protection page or click Edit on the right, the New MEAPS Global Config page appears.



Note:
In an existed MEAPS ring, its domain ID, ring ID, ring type, node type and control Vlan cannot be modified.

The primary ring can only be configured with the main node and the Transit node.

The secondary ring can be configured with the main node, the transit node, the edge node and the assistant edge node.

The primary node and the transit node can only be existed in one ring. The edge node and the assistant edge node can be existed in multiple rings simultaneously.

On the right drop box of “Primary-Port” and “Secondary-Port”, select one port respectively as the ring port or select None

5.12 Backup Link Protocol Configuration

5.12.1 Backup Link Protocol Global Configuration

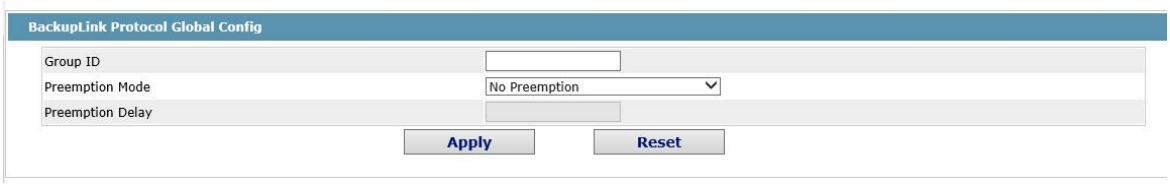
If you click Layer-2 Config ->Backup Link Config ->Backup Link Protocol Global Config on the navigation bar, the Backup Link Protocol Global Config page appears.



On the page, the current configured backup link groups are shown, including Preemption Mode and Preemption Delay.

Click New to create a new link backup group.

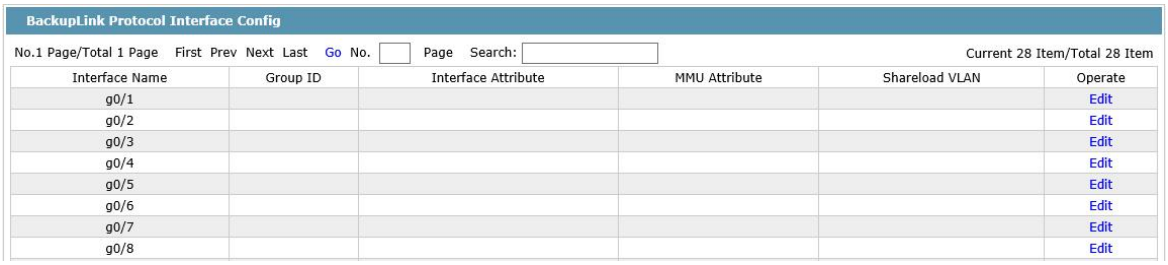
Click Edit on the right to configure Preemption Mode and Preemption Delay.



Note:
1. The system supports 8 link backup groups.
2. The Preemption mode determines the policy the primary port and the backup port forward packets.

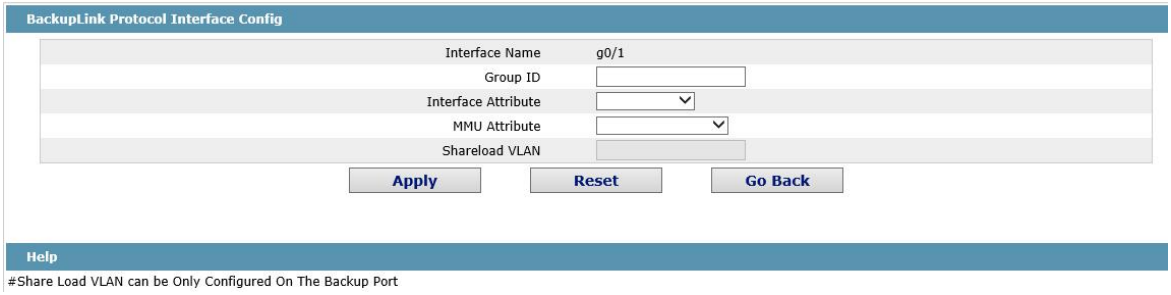
5.12.2 Backup Link Protocol Interface Configuration

If you click Layer-2 Config -> Backup Link Protocol Config -> Backup Link Protocol Interface Config on the navigation bar, the Backup Link Protocol Global Config page appears.



This page shows the backup link group's member ports, Interface Attribute, MMU Attribute, Shareload Vlan, etc.

Click Edit on the right to configure the Backup Link Protocol.



The backup link group which has configured the primary port cannot take other ports as its primary port. Likewise, the backup link group which has configured the backup port cannot take other ports as its backup port.

5.13 DHCP Snooping Configuration

5.13.1 DHCP Snooping Global Attribute Configuration

If you click Layer-2 Config -> DHCP Snooping Config -> DHCP Snooping Global Config on the navigation bar, the DHCP Snooping Global Config page appears.



Enable global DHCP Snooping protocol, the switch is to monitor all DHCP packets and form the corresponding binding relationship. If the client obtains the address of a switch before the global DHCP Snooping protocol is enabled, the switch cannot add the corresponding binding relationship.

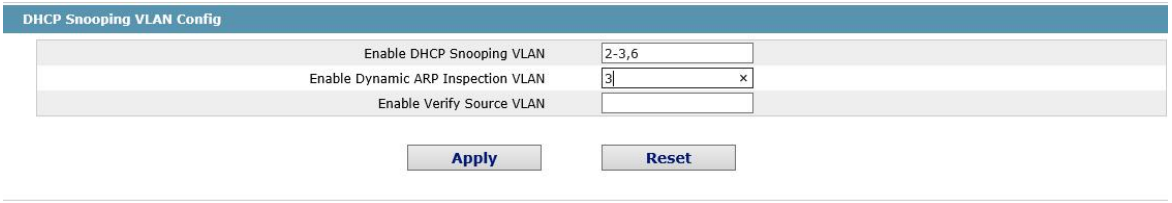
After the switch configuration is rebooted, the previously-configured interface binding will be lost. In this case, there is no binding relationship on this interface. After source IP address monitoring is enabled, the switch rejected forwarding all IP packets. After the TFTP server is configured for interface binding backup, the binding relationship will be backed up to the server through the TFTP protocol. After the switch is restarted, the switch automatically downloads the binding list from the TFTP server, securing the normal running of the network.

When backing up the interface binding relationship, the corresponding file name will be saved on the TFTP server. In this way, different switches can back up their own interface binding relationships to the same TFTP server.

The MAC-to-IP binding relationship on an interface changes dynamically. Hence, you need check whether the binding relationship updates after a certain interval. If the binding relationship updates, it need be backed up again. The default time interval is 30mins.

5.13.2 DHCP Snooping VLAN Attribute Configuration

If you click Layer-2 Config -> DHCP Snooping Config -> DHCP Snooping VLAN Config on the navigation bar, the DHCP Snooping VLAN Config page appears.



If DHCP snooping is enabled in a VLAN, the DHCP packets which are received from all distrusted physical ports in a VLAN will be legally checked. The DHCP response packets which are received from distrusted physical ports in a VLAN will then be dropped, preventing the faked or mis-configured DHCP server from providing address distribution services. For the DHCP request packet from distrusted ports, if the hardware address field in the DHCP request packet does not match the MAC address of this packet, the DHCP request packet is then thought as a fake packet which is used as the attack packet for DHCP DOS and then the switch will drop it.

When dynamic ARP monitoring is conducted in all physical ports of a VLAN, a received ARP packet will be rejected if the source MAC address and the source IP address of this packet do not match up with the configured MAC-IP binding relationship. The binding relationship on an interface can be dynamically bound by DHCP or configured manually. If no MAC addresses are bound to IP addresses on a physical interface, the switch rejects forwarding all ARP packets.

After source IP address monitoring is enabled in a VLAN, IP packets received from all physical ports in the VLAN will be rejected if their source MAC addresses and source IP addresses do not match up with the configured MAC-to-IP binding relationship. The binding relationship on an interface can be dynamically bound by DHCP or configured manually. If no MAC addresses are bound to IP addresses on a physical interface, the switch rejects forwarding all IP packets received from the physical interface.

5.13.3 DHCP Snooping Interface Attribute Configuration

If you click Layer-2 Config -> DHCP Snooping Config -> DHCP Snooping Interface Config on the navigation bar, the DHCP Snooping Interface Config page appears.



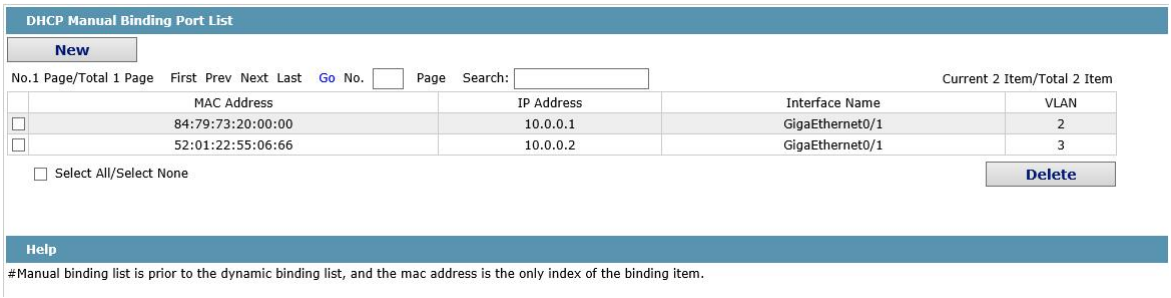
If an interface is set to be a DHCP-trusting interface, the DHCP packets received from this interface will not be checked.

ARP monitoring is not enabled on those trusted interfaces. The interfaces are distrusted ones by default.

The source address detection function will not be enabled for the IP source address trust interface.

5.13.4 DHCP Snooping Manual Binding Configuration

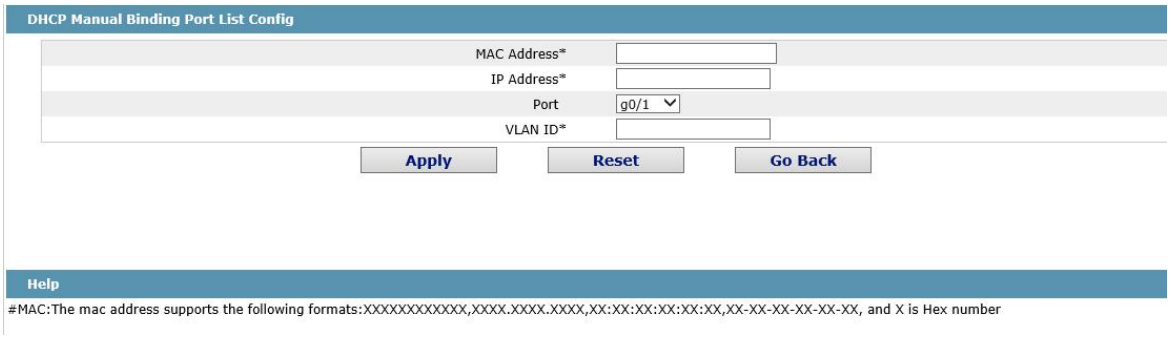
If you click Layer-2 Config -> DHCP Snooping Config -> DHCP Interface Binding List Manual Config on the navigation bar, the DHCP Manual Port List page appears.



If a host does not obtain the address through DHCP, you can add the binding item on an interface of a switch to enable the host to access the network. You can run no ip source binding MAC IP to delete items from the corresponding binding list.

Note that the manually-configured binding items have higher priority than the dynamically-configured binding items. If the manually-configured binding item and the dynamically-configured binding item have the same MAC address, the manually-configured one updates the dynamically-configured one. The interface binding item takes the MAC address as the unique index. The interface binding item takes the MAC address as the unique index.

Click New to create DHCP Snooping manual Binding Port Item.



5.14 MTU Configuration

If you click Layer-2 Config -> MTU Config on the navigation bar, the MTU Config page appears.

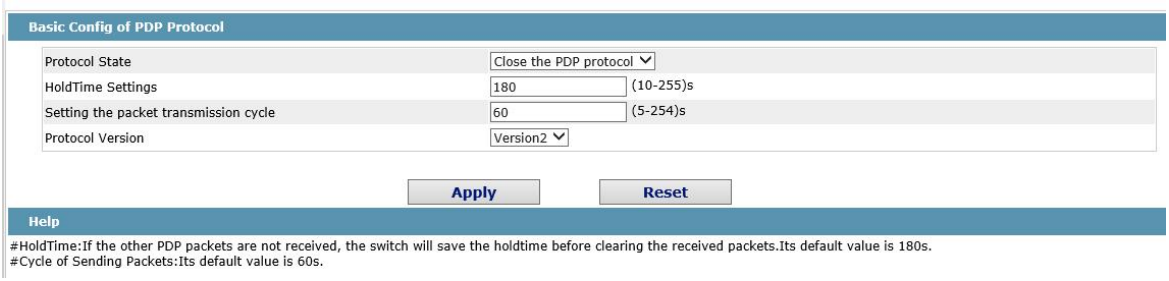


You can set the size of the maximum transmission unit (MTU).

5.15 PDP Configuration

5.15.1 Configuring the Global Attributes of PDP

If you click Layer-2 Config -> PDP Config in the navigation bar, the Global PDP Config page appears, as shown in figure 4.



You can choose to enable PDP or disable it. When you choose to disable PDP, you cannot configure PDP.

The “HoldTime” parameter means the time to be saved before the router discards the received information if other PDP packets are not received.

5.15.2 Configuring the Attributes of the PDP Port

If you click Layer-2 Config -> PDP Config-> PDP port Config in the navigation bar, the Setting the attributes of the PDP port page appears, as shown in figure 5.



After the PDP port is configured, you can enable or disable PDP on this port.

5.16 STP Configuration

5.16.1 STP Status Information

If you click **Layer-2 Config -> STP Config** in the navigation bar, the **STP Config** page appears, as shown in figure 10.



Figure 10 Configuring the global attributes of STP

The root STP configuration information and the STP port's status are only-read.

On the local STP configuration page, you can modify the running STP mode by clicking the Protocol type dropdown box. The STP modes include STP, RSTP and disabled STP.

The priority and the time need be configured for different modes.

Note:
The change of the STP mode may lead to the interruption of the network.

5.16.2 Configuring the Attributes of the STP Port

If you click the "Configure RSTP Port" option, the "Configure RSTP Port" page appears.

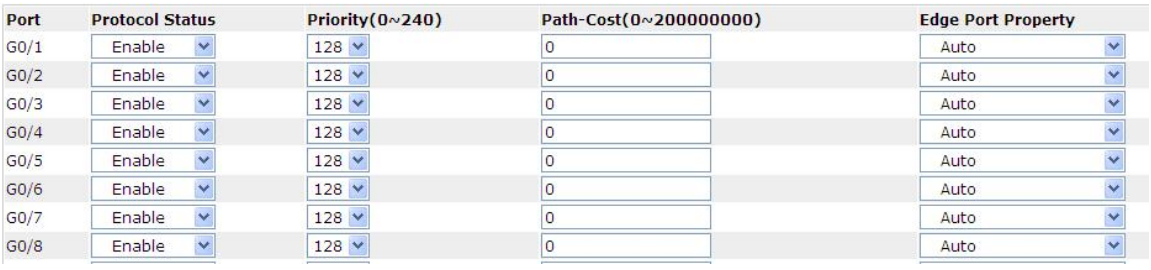


Figure 11 Configuring the attributes of RSTP

The configuration of the attributes of the port is irrelative of the global STP mode. For example, if the protocol status is set to "Disable" and the STP mode is also changed, the port will not run the protocol in the new mode.

The default value of the path cost of the port is 0, meaning the path cost is automatically calculated according to the speed of the port. If you want to change the path cost, please enter another value.

5.17 IGMP-Snooping Configuration

5.17.1 IGMP-Snooping Configuration

If you click **Layer-2 Config -> IGMP snooping**, the IGMP-Snooping configuration page appears.

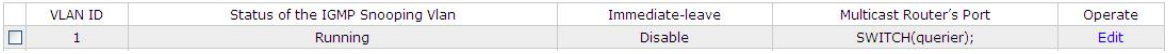


Figure 12 IGMP-snooping configuration

On this page you can set whether to make a switch to forward unknown multicasts, whether to enable IGMP snooping, and whether to configure the switch as the querier of IGMP.

5.17.2 IGMP-Snooping VLAN List

If you click **Layer-2 Config -> IGMP snooping vlan list**, the **IGMP-Snooping VLAN list** page appears.



	VLAN ID	Status of the IGMP Snooping Vlan	Immediate-leave	Multicast Router's Port	Operate
☐	1	Running	Disable	SWITCH(querier);	Edit

Figure 13: IGMP-snooping VLAN list

If you click **New**, IGMP-snooping VLAN configuration can be done. Through Web up to 8 physical ports can be set on each IGMP snooping VLAN. If you click **Cancel**, a selected IGMP-Snooping VLAN can be deleted; if you click **Edit**, you can modify the member port, running status and immediate-leave of IGMP-Snooping VLAN.

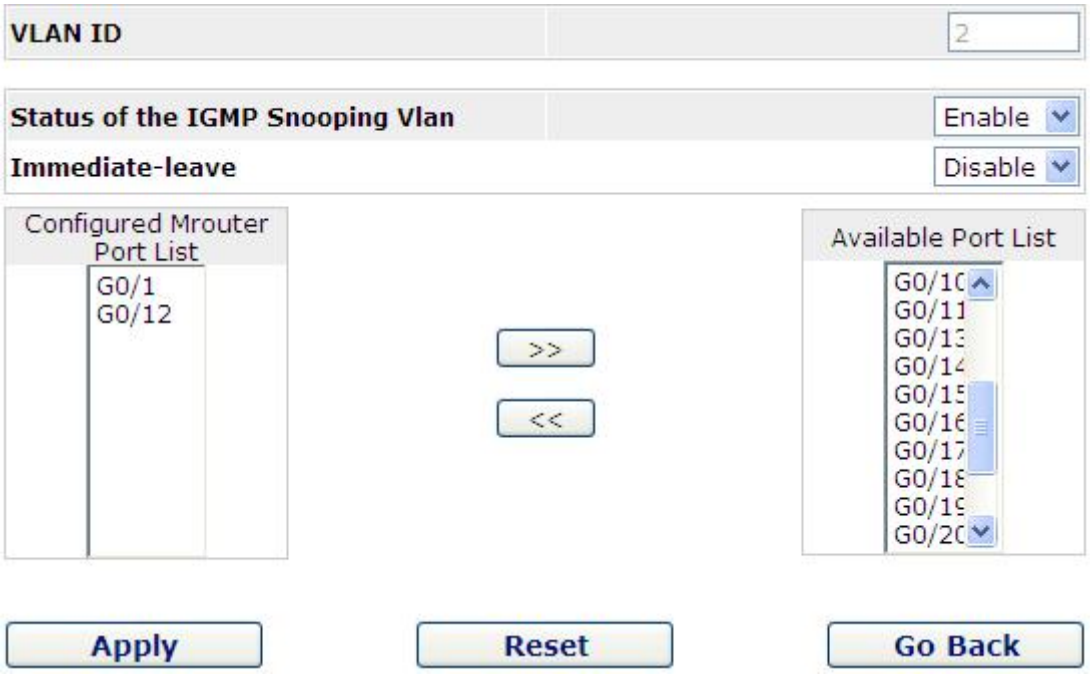


Figure 14: Static routing port of IGMP VLAN

When an IGMP-Snooping VLAN is created, its VLAN ID can be modified; but when the IGMP-Snooping VLAN is modified, its VLAN ID cannot be modified.

You can click "**>>**" and "**<<**" to delete and add a routing port.

5.17.3 Static Multicast Address

If you click **Static multicast address**, the **Setting the static multicast address** page appears.

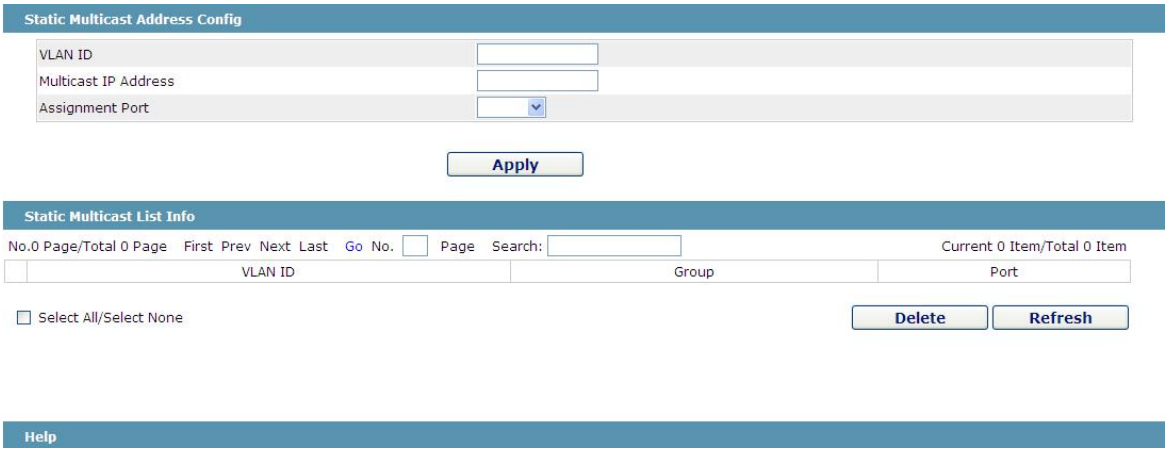


Figure 15 Multicast List

On this page, the currently existing static multicast groups and port groups in each static multicast group are shown.

Click "Refresh" to refresh the contents in the list.

5.17.4 Multicast List

Click the **Multicast List Info** option on the top of the page and the **Multicast List Info** page appears.

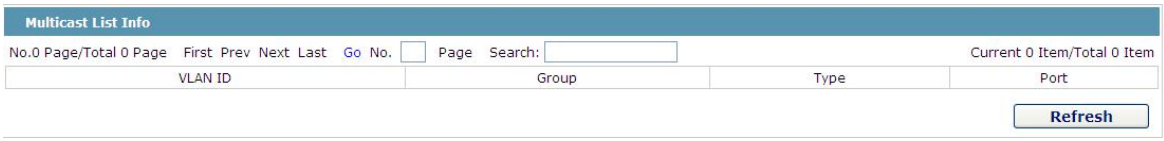


Figure 16 Multicast List

On this page the multicat groups, which are existent in the current network and are in the statistics of IGMP snooping, as well as port sets which members in each group belong to are dislayed.

Click “Refresh” to refresh the contents in the list.

Note:
By default, a multicast list can display up to 15 VLAN items. You can modify the number of multicast items by running **ip http web igmp-groups** after you log on to the device through the Console port or Telnet.

5.18 Setting Static ARP

If you click **Layer-2 Config -> Static ARP Config**, the static ARP configuration page appears.

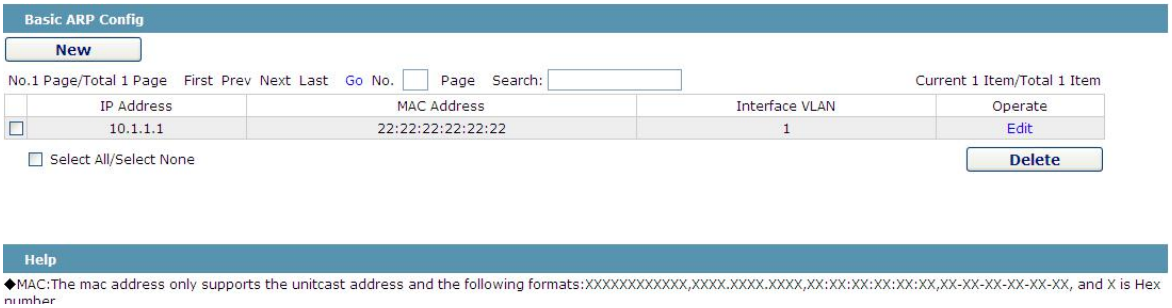


Figure 17 Displaying static ARP

You can click **New** to add an ARP entry. If the **Alias** column is selected, it means to answer the ARP request of the designated IP address.

If you click Edit, you can modify the current ARP entry.

If you click Cancel, you can cancel the chosen ARP entry.

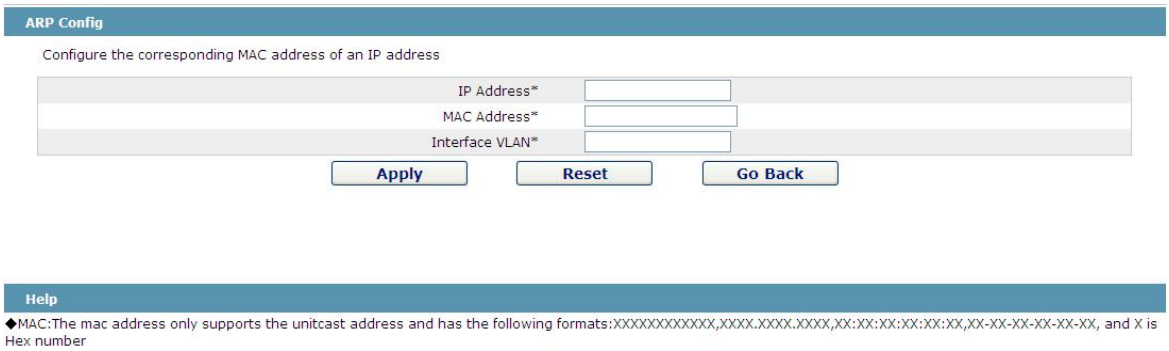


Figure 18 Setting static ARP

5.19 Ring Protection Configuration

5.19.1 EAPS Ring List

If you click **Layer-2 Config -> Ring protection Config**, the **EAPS ring list** page appears.

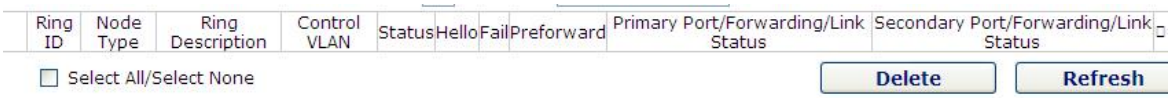


Figure 19 EAPS Ring List

In the list shows the currently configured EAPS ring, including the status of the ring, the forwarding status of the port and the status of the link.

Click “New” to create a new EAPS ring.

Click the “Operate” option to configure the “Time” parameter of the ring.

Note:
1. The system can support 8 EAPS rings.
2. After a ring is configured, its port, node type and control Vlan cannot be modified. If the port of the ring, the node type or the control Vlan need be adjusted, please delete the ring and then establish a new one.

5.19.2 EAPS Ring Configuration

If you click “New” on the EAPS ring list, or “Operate” on the right side of a ring item, the “Configure EAPS” page appears.

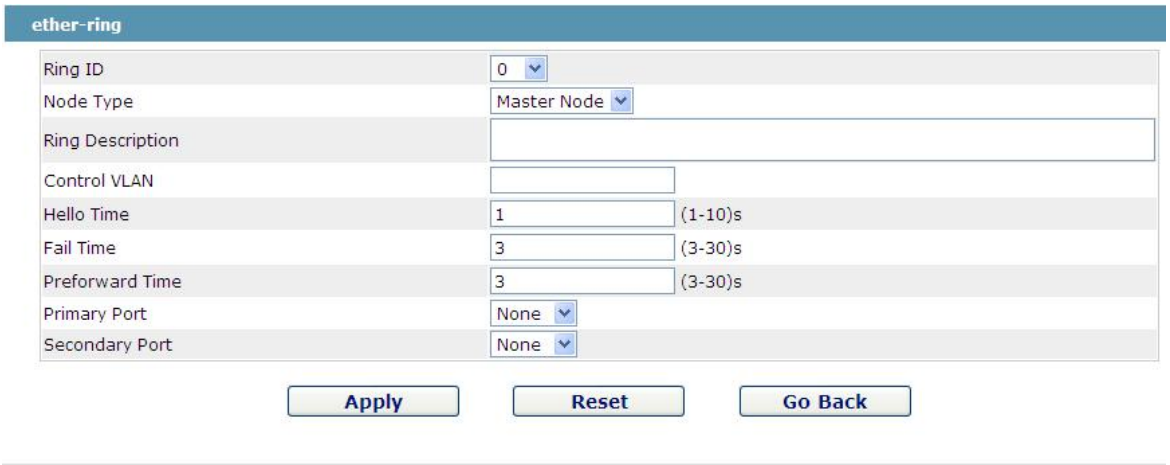


Figure 20 EAPS ring configuration

Note:
If you want to modify a ring, on this page the node type, the control VLAN, the primary port and the secondary port cannot be modified.

In the dropdown box on the right of “Ring ID”, select an ID as a ring ID. The ring IDs of all devices on the same ring must be the same.

The dropdown box on the right of “Node Type” is used to select the type of the node. Please note that only one master node can be configured on a ring.

Enter a value between 1 and 4094 in the text box on the right of “Control VLAN” as the control VLAN ID. When a ring is established, the control VLAN will be automatically established too. Please note that if the designated control VLAN is 1 and the VLAN of the control device is also 1 the control device cannot access the control VLAN. Additionally, please do not enter a control VLAN ID that is same as that of another ring.

In the text boxes of “Primary Port” and “Secondary Port”, select a port as the ring port respectively. If "Node Type" is selected as “Transit-Node”, the two ports will be automatically set to transit ports.

Click “Apply” to finish EAPS ring configuration, click “Reset” to resume the initial values of the configuration, or click “Return” to go back to the EAPS list page.

5.20 EVC Configuration

5.20.1 Global QinQ Configuration

If you click **Layer-2 Config -> EVC Config**, the **Global QinQ configuration** page appears.



Figure 21: Global EVC configuration

In global EVC configuration mode, you can enable or disable the global dot1q.

5.20.2 Configuring the QinQ Port

If you click **Layer-2 Config -> EVC Config -> QinQ port Config**, the **Configuring the QinQ port** page appears.



Figure 22: Configuring the PTP port

The QinQ related configuration of all ports can be displayed and modified on the **Configuring the QinQ port** page.

5.21 DDM Configuration

If you click **L2 Config -> DDM Config** in the navigation bar, the **DDM configuration** page appears, as shown in figure 5-21.

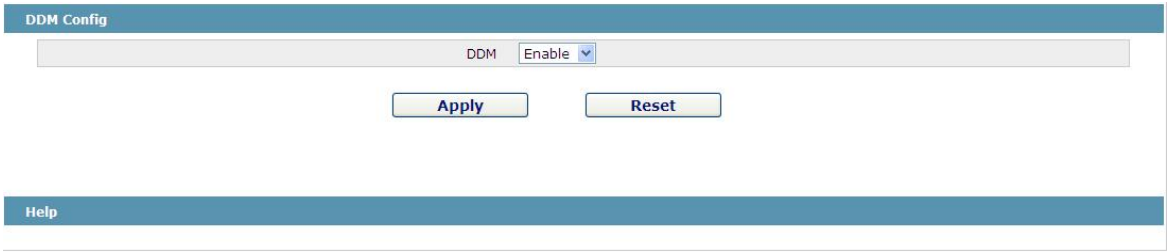


Figure 5-21: DDM configuration

Chapter 6 Layer-3 Configuration



Figure 1: Layer-3 configuration list

Note:
Only layer-3 switches have the layer-3 configuration.

6.1 Configuring the VLAN Interface

If you click **Layer-3 Config -> VLAN interface Config**, the **Configuring the VLAN interface** page appears.

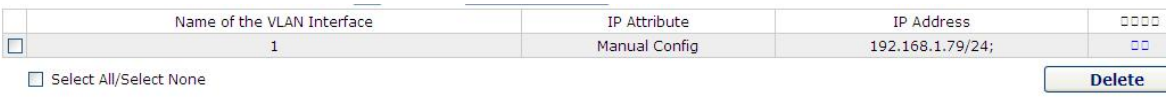


Figure 2: Configuring the VLAN interface

Click **New** to add a new VLAN interface. Click **Cancel** to delete a VLAN interface. Click **Modify** to modify the settings of a corresponding VLAN interface.

When you click **New**, the name of the corresponding VLAN interface can be modified; but if you click **Modify**, the name of the corresponding VLAN interface cannot be modified.

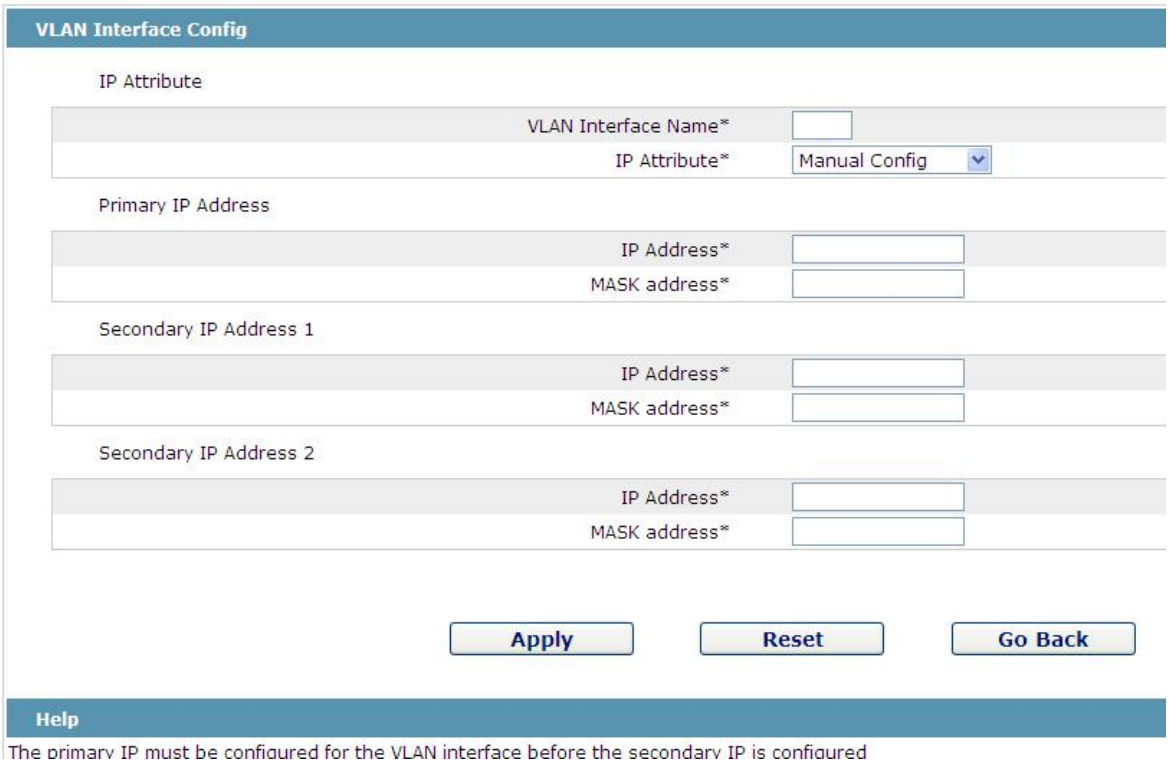


Figure 3: VLAN interface configuration

Note:
Before the accessory IP of a VLAN interface is set, you have to set the main IP.

6.2 Setting the Static Route

If you click **Layer-3 Config -> Static route Config**, the **Static route configuration** page appears.



Figure 4 Displaying the static route

Click **Create** to add a static route.

If you click **Edit**, you can modify the current static route.

If you click **Cancel**, you can cancel the chosen static route.

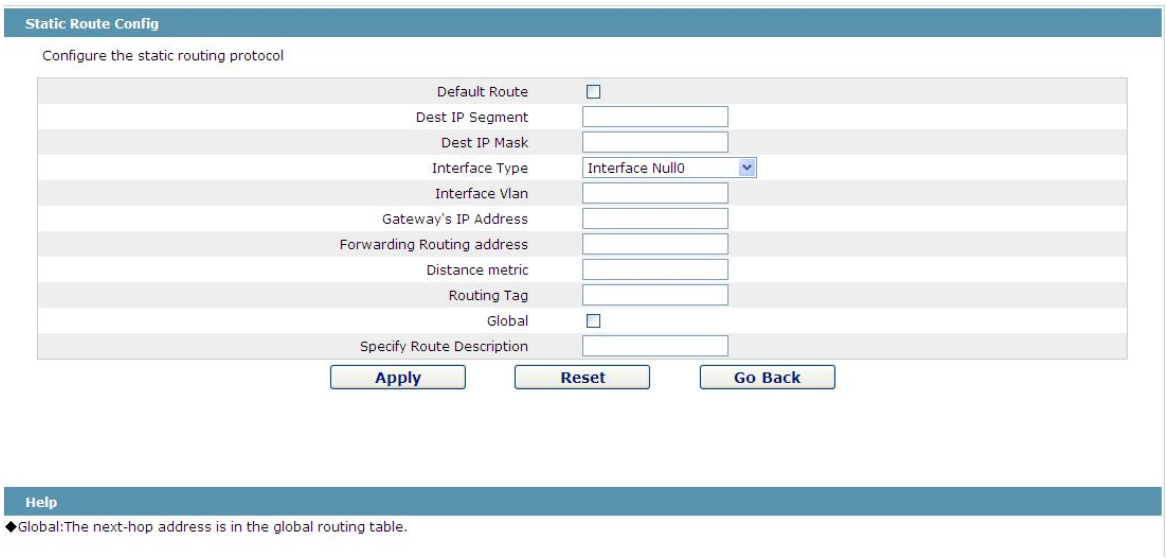


Figure 5: Setting the static route

6.3 IGMP Agent

6.3.1 Enabling the IGMP Agent

If you click **Layer-3 Config -> IGMP agent**, the **IGMP agent** page appears.

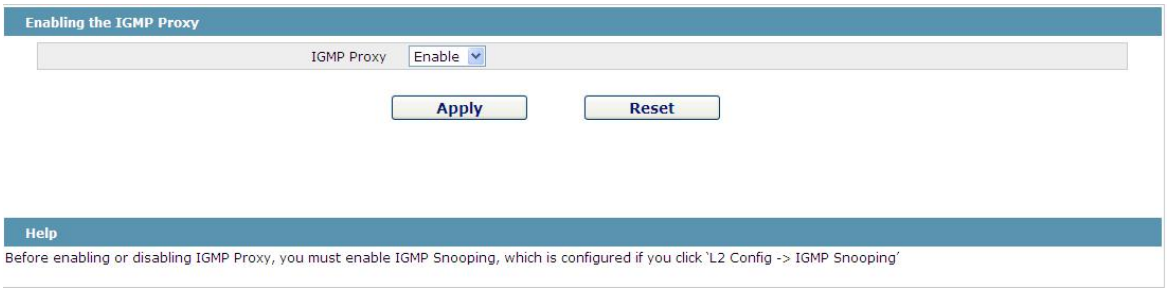


Figure 6: Enabling the IGMP agent

On this page you can enable or disable the IGMP agent. It is noted that the IGMP agent can be enabled or disabled on a switch only after the IP IGMP-snooping function is enabled on the switch.

6.3.2 Setting the IGMP Agent

If you click **Layer-3 Config -> IGMP agent -> IGMP agent Config**, the **IGMP agent configuration** page appears. Click **New** to create a new IGMP agent.

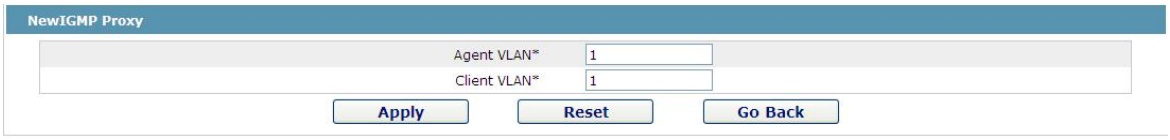


Figure 7: Setting the IGMP agent

Chapter 7 Advanced Configuration



Figure 1 A list of advanced configuration

7.1 QoS Configuration

7.1.1 Configuring QoS Port

If you click **Advanced Config -> QoS -> Configure QoS Port,** the **Port Priority Config** page appears.



Figure 2 Configuring the QoS Port

You can set the CoS value by clicking the dropdown box on the right of each port and selecting a value. The default CoS value of a port is 0, meaning the lowest priority. If the CoS value is 7, it means that the priority is the highest.

7.1.2 Global QoS Configuration

If you click **Advanced Config -> QoS Config -> Global QoS Config**, the **Port's QoS parameter configuration** page appears.

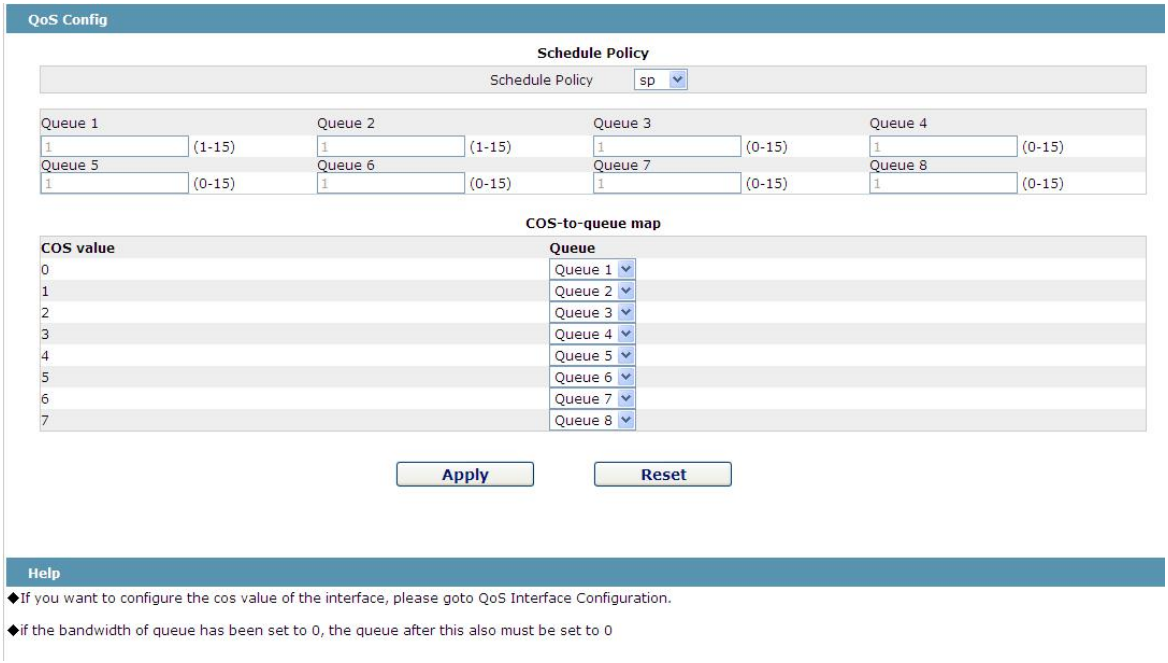


Figure 3 Configuring global QoS attributes

In WRR schedule mode, you can set the weights of the QoS queues. There are 4 queues, among which queue 1 has the lowest priority and queue 4 has the highest priority.

7.2 MAC Access Control List

7.2.1 Setting the Name of the MAC Access Control List

If you click **Advanced Config -> MAC access control list -> MAC access control list Config**, the MAC ACL configuration page appears.

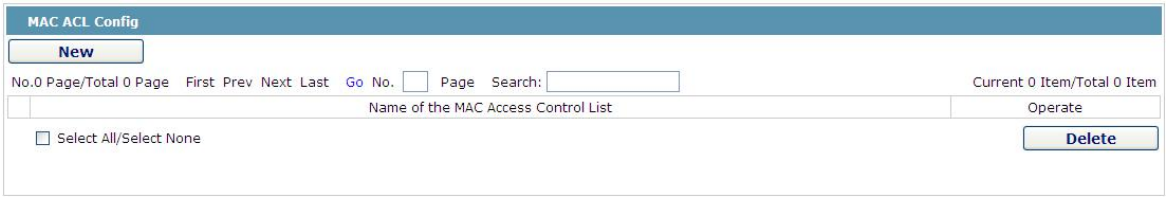


Figure 4: MAC access control list configuration

Click **New** to add a name of the MAC access control list. Click **Cancel** to delete a MAC access control list.



Figure 5: Setting the name of MAC access control list

7.2.2 Setting the Rules of the MAC Access Control List

If you click **Modify**, the corresponding MAC access control list appears and you can set the corresponding rules for the MAC access control list.



Figure 6: Specific MAC access control list configuration

Click **New** to add a rule of the MAC access control list. Click **Cancel** to delete a rule of the MAC access control list.

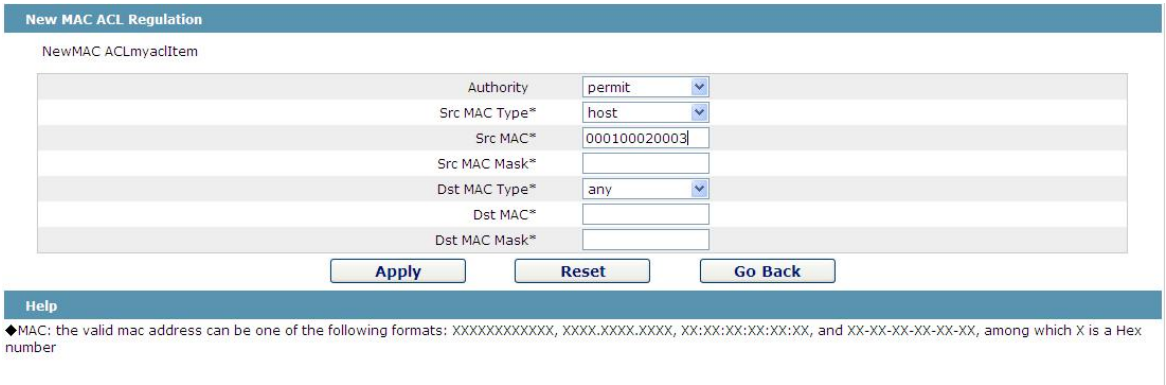


Figure 7: Setting the Rules of the MAC Access Control List

7.2.3 Applying the MAC Access Control List

If you click **Advanced Config -> MAC access control list -> Applying the MAC access control list**, the **Applying the MAC access control list** page appears.

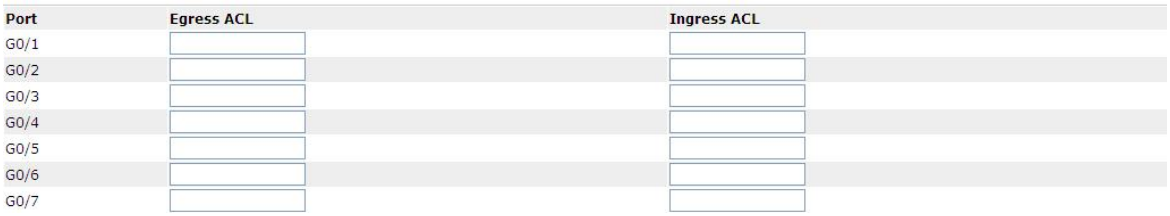


Figure 8: Applying the MAC access control list

7.3 IP Access Control List

7.3.1 Setting the Name of the IP Access Control List

If you click **Advanced Config -> IP access control list -> IP access control list Config**, the IP ACL configuration page appears.



Figure 9: IP access control list configuration

Click **New** to add a name of the IP access control list. Click **Cancel** to delete an IP access control list.



Figure 10: Creating a name of the IP access control list

If you click **Modify**, the corresponding IP access control list appears and you can set the corresponding rules for the IP access control list.

7.3.2 Setting the Rules of the IP Access Control List

- Standard IP access control list

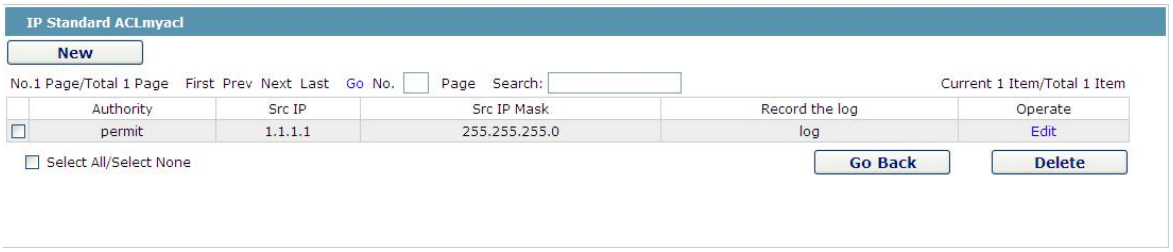


Figure 11: Standard IP access control list

Click **New** to add a rule of the IP access control list. Click **Cancel** to delete a rule of the IP access control list. If you click **Modify**, the corresponding IP access control list appears and you can set the corresponding rules for the IP access control list.



Figure 12: Setting the Rules of the standard IP access control list

- Extended IP access control list

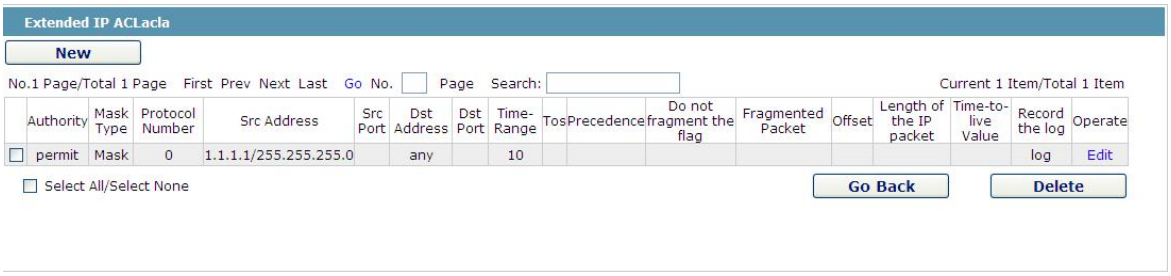


Figure 13: Extended IP access control list

Click **New** to add a rule of the IPaccess control list. Click **Cancel** to delete a rule of the IP access control list. If you click **Modify**, the corresponding IP access control list appears and you can set the corresponding rules for the IP access control list.

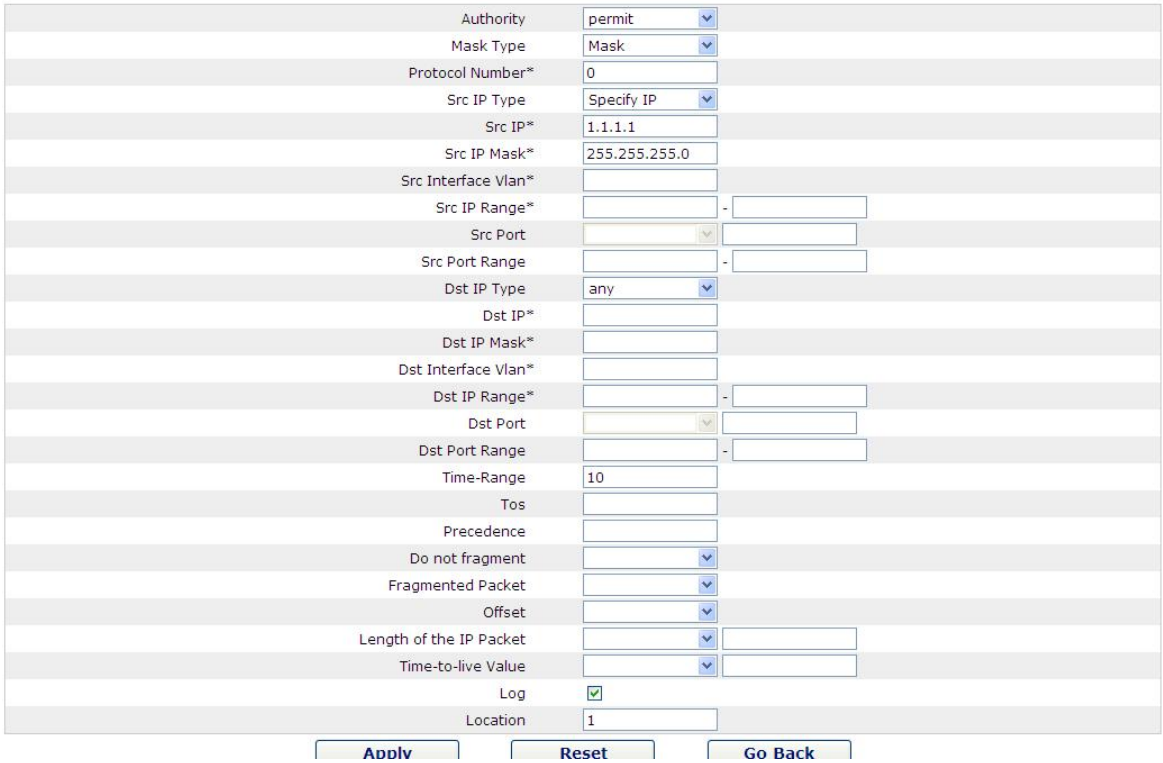


Figure 14: Setting the Rules of the extended IP access control list

7.3.3 Applying the IP Access Control List

If you click **Advanced Config -> IP access control list -> Applying the IP access control list**, the **Applying the IP access control list** page appears.

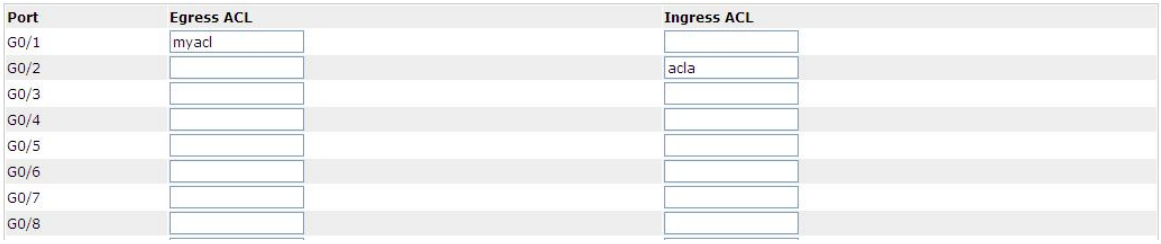


Figure 15: Applying the IP access control list

Chapter 8 Network Management Configuration



Figure 1: Network management configuration list

8.1 SNMP Configuration

If you click **Network management Config -> SNMP management** in the navigation bar, the **SNMP management** page appears, as shown in figure 2.

8.1.1 SNMP Community Management

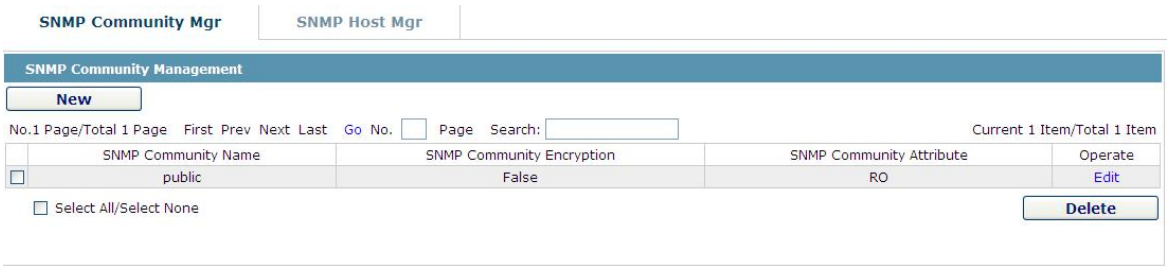


Figure 2 SNMP community management

On the SNMP community management page, you can know the related configuration information about SNMP community.

You can create, modify or cancel the SNMP community information, and if you click **New or Edit, you ca switch to the configuration page of SNMP community.**

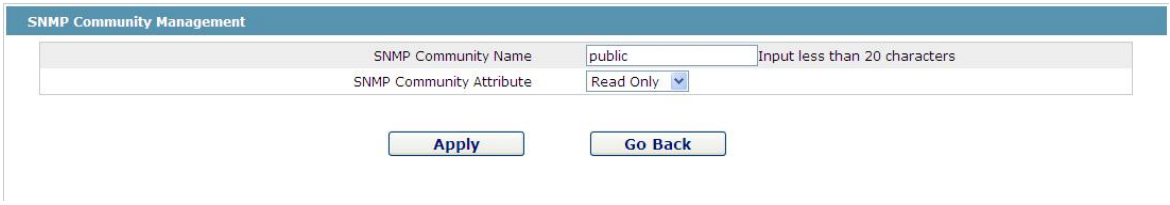


Figure 4.2 SNMP community management settings

On the SNMP community management page you can enter the SNMP community name, select the attributes of SNMP community, which include Read only and Read-Write.

8.1.2 SNMP Host Management

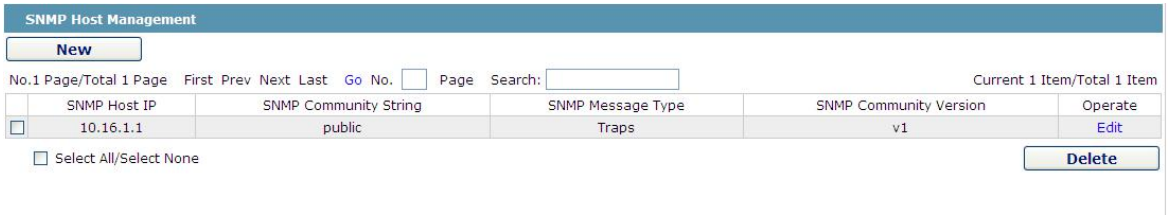


Figure 4 SNMP host management

On the SNMP community host page, you can know the related configuration information about SNMP host.

You can create, modify or cancel the SNMP host information, and if you click **New** or **Edit**, you ca switch to the configuration page of SNMP host.

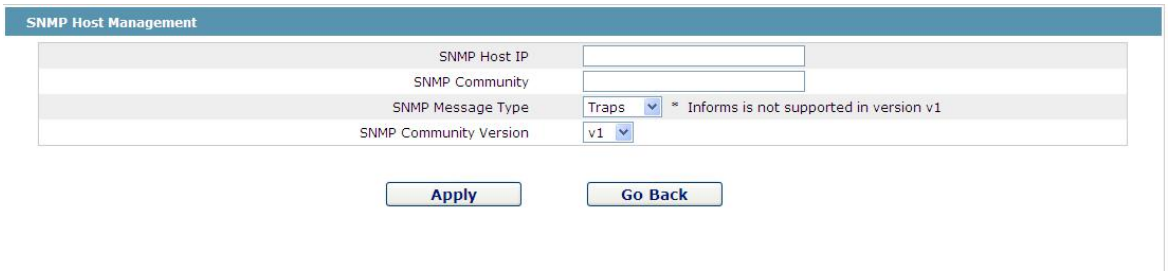


Figure 5 SNMP host management settings

On the SNMP host configuration page, you can enter **SNMP Host IP**, **SNMP Community**, **SNMP Message Type** and **SNMP Community Version**. **SNMP Message Type** includes **Traps** and **Informs**, and as to version 1, **SNMP Message Type** does not support **Informs**.

8.2 RMON

8.2.1 RMON Statistic Information Configuration

If you click **Network Management Config -> RMON -> RMON Statistics -> New**, the **RMON Statistics** page appears.



Figure 6 Configuring the RMON statistic information

You need to set a physical port to be the reception terminal of the monitor data.

The index is used to identify a specific interface; if the index is same to that of the previous application interface, it will replace that of the previous application interface.

At present, the monitor statistic information can be obtained through the command line “show rmon statistics”, but the Web does not support this function.

8.2.2 RMON History Information Configuration

If you click **Network Management Config -> RMON -> RMON history -> New**, the **RMON history** page appears.

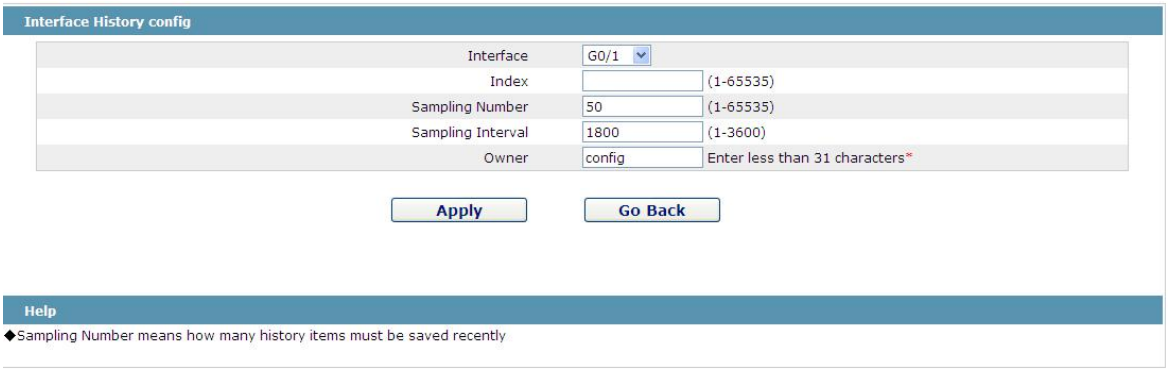


Figure 7 Configuring the RMON history information

You need to set a physical port to be the reception terminal of the monitor data.

The index is used to identify a specific interface; if the index is same to that of the previous application interface, it will replace that of the previous application interface.

The sampling number means the items that need be reserved, whose default value is 50.

The sampling interval means the time between two data collection, whose default value is 1800s.

At present, the monitor statistic information can be obtained through the command line “show rmon history”, but the Web does not support this function.

8.2.3 RMON Alarm Information Configuration

If you click **Network Management Config -> RMON -> RMON Alarm -> New**, the **RMON Alarm** page appears.

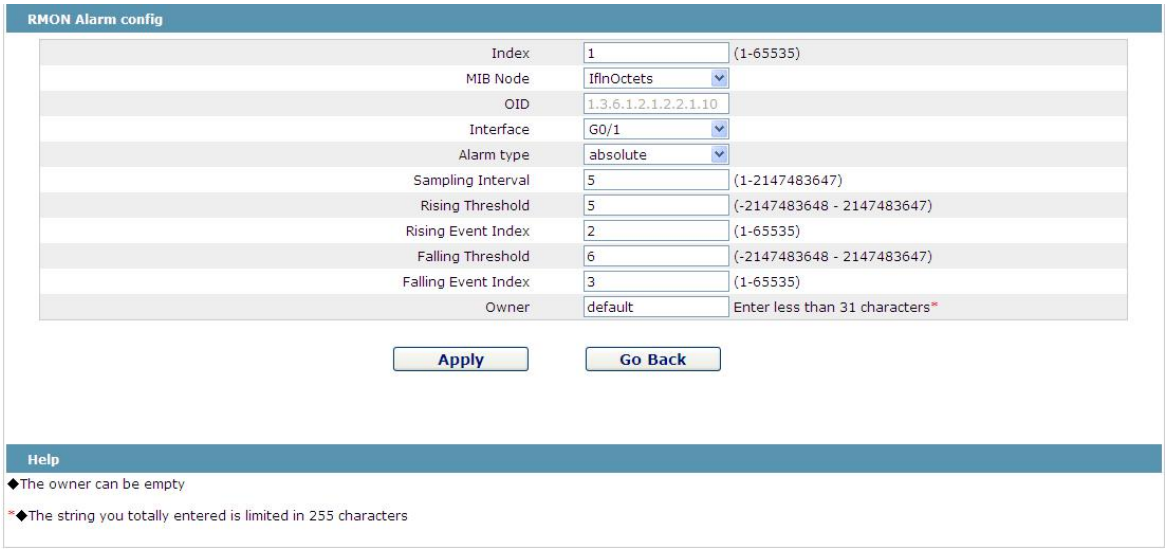


Figure 8 Configuring the RMON alarm information

The index is used to identify a specific alarm information; if the index is same to the previously applied index, it will replace the previous one.

The MIB node corresponds to OID.

If the alarm type is **absolute**, the value of the MIB object will be directly minitored; if the alarm type is **delta**, the change of the value of the MIB object in two sampling will be monitored.

When the monitored MIB object reaches or exceeds the rising threshold, the event corresponding to the index of the rising event will be triggered.

When the monitored MIB object reaches or exceeds the falling threshold, the event corresponding to the index of the falling event will be triggered.

8.2.4 RMON Event Configuration

If you click **Network Management Config -> RMON -> RMON Event -> New**, the **RMON event** page appears.

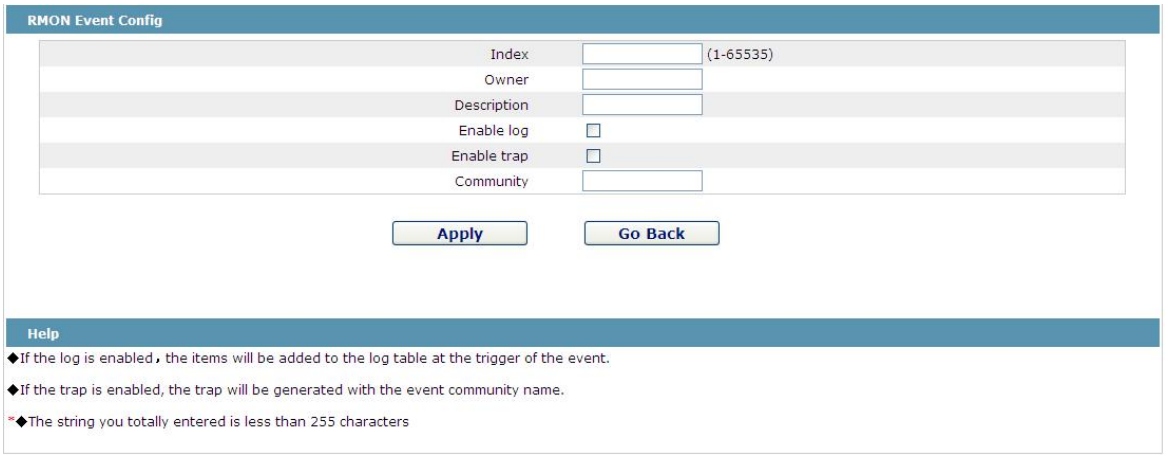


Figure 9 RMON event configuration

The index corresponds to the rising event index and the falling event index that have already been configured on the **RMON alarm config** page.

The owner is used to describe the descriptive information of an event.

"Enable log" means to add an item of information in the log table when the event is triggered.

“Enable trap” means a trap will be generated if the event is triggered.

Chapter 9 Diagnosis Tools



Figure 1: Diagnosis tool list

9.1 Ping

9.1.1 Ping

If you click **Diagnosis Tools -> Ping**, the **Ping** page appears.

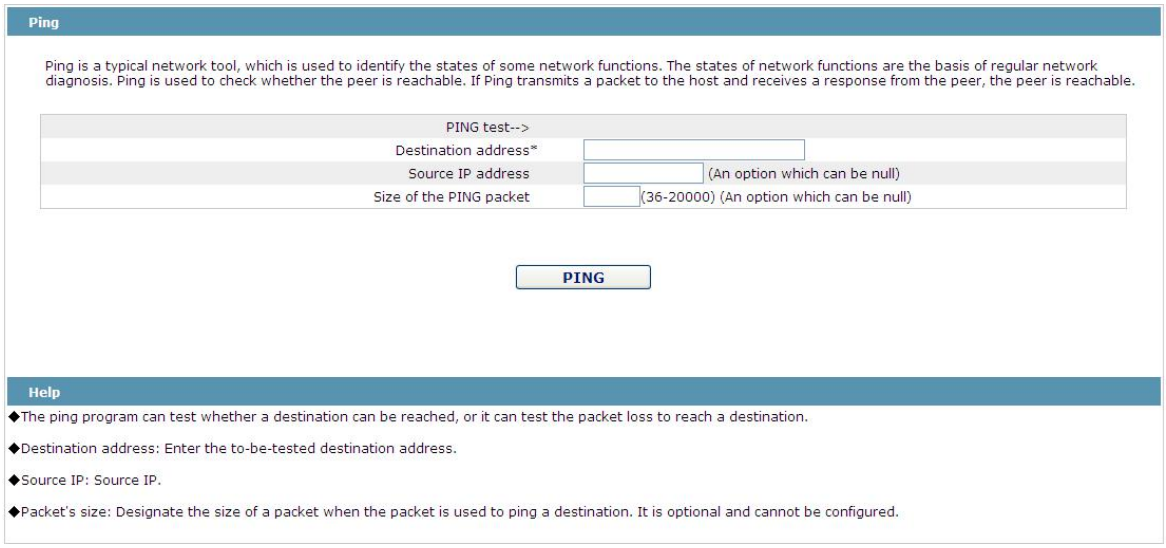


Figure 2 Ping

Ping is used to test whether the switch connects other devices.

If a Ping test need be conducted, please enter an IP address in the “Destination address” textbox, such as the IP address of your PC, and then click the “PING” button. If the switch connects your entered address, the device can promptly return a test result to you; if not, the device will take a little more time to return the test result.

“Source IP address” is used to set the source IP address which is carried in the Ping packet.

“Size of the PING packet” is used to set the length of the Ping packet which is transmitted by the device.

Chapter 10 System Management



Figure 1 Navigation list of system management

10.1 User Management

10.1.1 User List

If you click **System Manage -> User Manage**, the **User Management** page appears.



Figure 2 User list

You can click “New” to create a new user.

To modify the permission or the login password, click “Edit” on the right of the user list.

Note:
1. Please make sure that at least one system administrator exists in the system, so that you can manage the devices through Web.
2. The limited user can only browse the status of the device.

10.1.2 Establishing a New User

If you click “New” on the **User Management** page, the **Creating User** page appears.

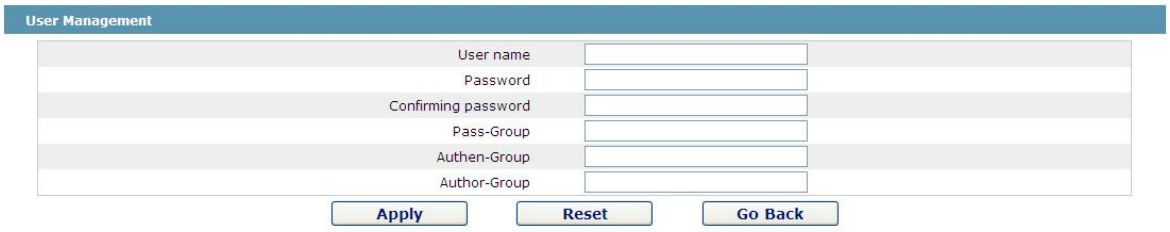


Figure 3 Creating new users

In the “User name” text box, enter a name, which contains letters, numbers and symbols except "?", "\", "&", "#" and spaces.

In the “Password” textbox enter a login password, and in the “Confirming password” textbox enter this login password again.

In the “User permission” dropdown box set the user's permission. The “System administrator” user can browse the status of the device and conduct relevant settings, while the limited user can only browse the status of the device.

10.2 Log Management

If you click **System Manage -> Log Manage**, the **Log Management** page appears.

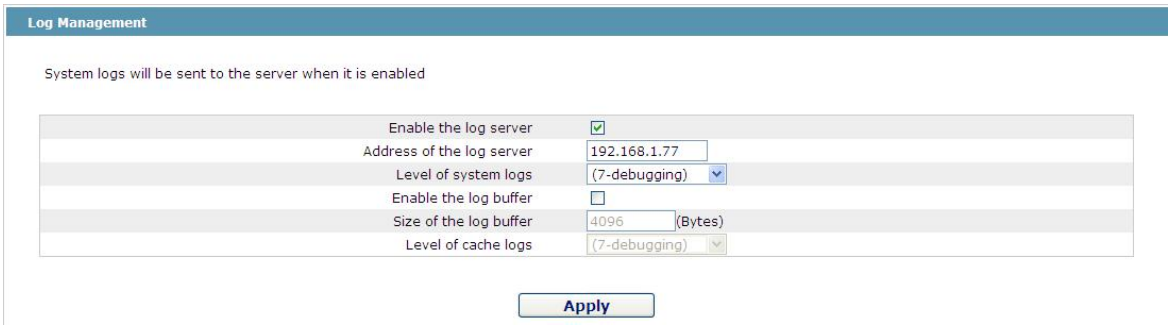


Figure 4 Log management

If “Enabling the log server” is selected, the device will transmit the log information to the designated server. In this case, you need enter the address of the server in the “Address of the system log server” textbox and select the log's grade in the “Grade of the system log information” dropdown box.

If “Enabling the log buffer” is selected, the device will record the log information to the memory. By logging on to the device through the Console port or Telnet, you can run the command “show log” to browse the logs which are saved on the device. The log information which is saved in the memory will be lost after rebooting. Please enter the size of the buffer area in the “Size of the system log buffer” textbox and select the grade of the cached log in the “Grade of the cache log information” dropdown box.

10.3 Managing the Configuration Files

If you click **System Manage -> Configuration file**, the **Configuration file** page appears.

10.3.1 Exporting the Configuration Information



Figure 5 Exporting the configuration file

The current configuration file can be exported, saved in the disk of PC or in the mobile storage device as the backup file.

To export the configuration file, please click the “Export” button and then select the “Save” option in the pop-up download dialog box.

The default name of the configuration file is “startup-config”, but you are suggested to set it to an easily memorable name.

10.3.2 Importing the Configuration Information

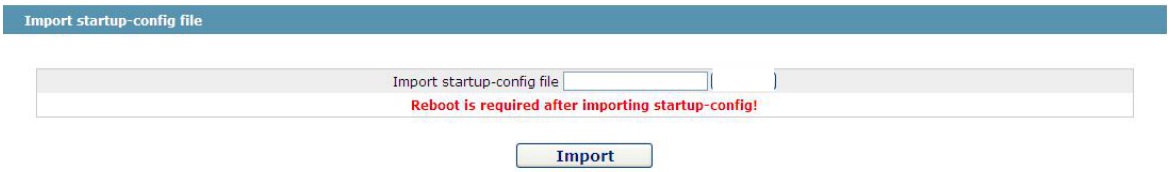


Figure 6 Importing the configuration files

You can import the configuration files from PC to the device and replace the configuration file that is currently being used. For example, by importing the backup configuration files, you can resume the device to its configuration of a previous moment.

Note:
1. Please make sure that the imported configuration file has the legal format for the configuration file with illegal format cannot lead to the normal startup of the device.
2. If error occurs during the process of importation, please try it later again, or click the “Save All” button to make the device re-establish the configuration file with the current configuration, avoiding the incomplete file and the abnormality of the device.
3. After the configuration file is imported, if you want to use the imported configuration file immediately, do not click “Save All”, but reboot the device directly.

10.4 Software Management

If you click **System Manage -> Software Upgrade**, the software management page appears.

10.4.1 Backing up the firmware Software

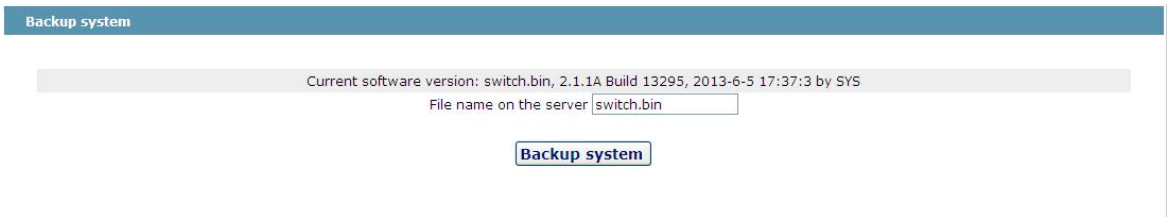


Figure 7 Backing up firmware

On this page the currently running software version is displayed. If you want to backup firmware, click "Backup system". The browser file download dialog box appears; click "Save" to store the firmware file on the PC, a mobile device or other network location.

Note:
The default filename is "Switch.bin". Use a clear backup name.

10.4.2 Upgrading the firmware Software

Note:
1. Please make sure that your upgraded firmware matches the device type, because the matchable firmware will not lead to the normal startup of the device.
2. The upgrade of firmware probably takes one to two minutes; when the ·updating· button is clicked, the firmware files will be uploaded to the device.
3. If errors occur during upgrade, please do not restart the device or cut off the power of the device, or the device cannot be started. Please try the upgrade again.
4. After the upgrade please save the configuration and then restart the device to run the new firmware.

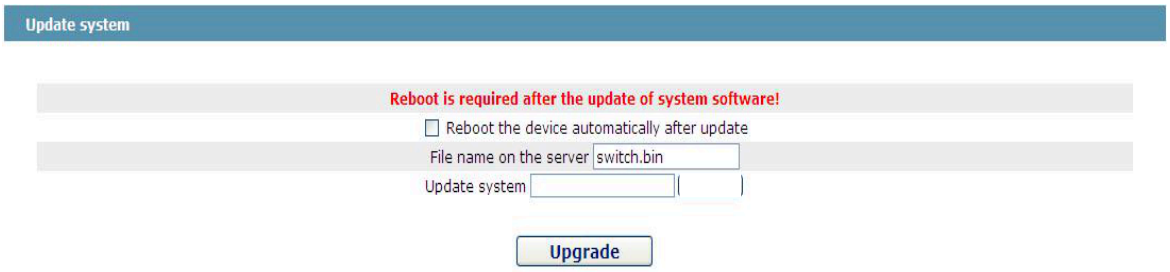


Figure 8 Upgrading the firmware software

Upgraded firmware resolves known problems or improves a specific function. If you device run normally, do not upgrade your firmware software frequently.

To upgrade, first enter the full path of the new firmware file in the textbox beside "Update system", or click the Browse button and select the new firmware files on your computer, and then click ·Updating·.

10.5 Resuming Initial Configuration

If you click **System Manage -> Resume Config**, the **Resuming the original configuration** page appears.

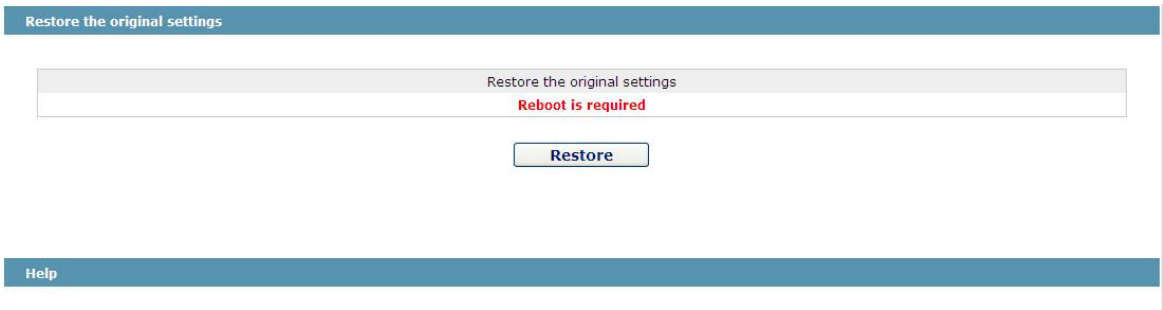


Figure 9 Resuming the original configuration

Note:
1. If you click the “Resume” button, the current configuration will be replaced by the original configuration, which will take effect after rebooting.

2. Before rebooting the device still works under the current configuration, and if you click “Save All” at the moment, the current configuration will replace the original configuration. The original configuration, therefore, cannot take effect after rebooting.
3. After the rebooting is done and the original configuration takes effect, the Web access of the device will be automatically started. The address of Vlan 1 is 192.168.0.1/255.255.255.0, and the username and password are both “admin”.

To resume the original configuration, click “Resume” and then reboot the device.

10.6 Rebooting the Device

If you click **System Manage -> Reboot Device**, the **Rebooting** page appears.



Figure 10 Rebooting the device

If the device need be rebooted, please first make sure that the modified configuration of the device has already been saved, and then click the “Reboot” button.

Interface Configuration

Table of Contents

Chapter 1 Overview 1
1.1 Supported Interface Types 1
1.2 Interface Configuration Introduction 2
Chapter 2 Interface Configuration 4
2.1 Configuring Interface Common Attribute 4
2.1.1 Adding Description 4
2.1.2 Configuring Bandwidth 4
2.1.3 Configuring Time Delay 4
2.2 Monitoring and Maintaining the Port 5
2.2.1 Browsing the State of an Interface 5
2.2.2 Initializing and Deleting the Port 5
2.2.3 Closing and Restarting the Port 5
2.3 Setting the Ethernet Interface 6
2.3.1 Choosing an Ethernet Interface 6
2.3.2 Setting the Rate 6
2.3.3 Setting the Duplex Mode of an Interface 7
2.3.4 Setting Flow Control on an Interface 7
2.4 Configuring Logical Interface 7
2.4.1 Configuring Null Interface 7
2.4.2 Configuring Loopback Interface 8
2.4.3 Configuring Aggregation Interface 8
2.4.4 Configuring VLAN Interface 8
2.4.5 Configuring SuperVLAN Interface 9
Chapter 3 Interface Configuration Example 10
3.1 Configuring Public Attribute of Interface 10
3.1.1 Example for Interface Description 10
3.1.2 Example of Interface Shutdown 10

Chapter 1 Overview

This section helps user to learn various kinds of interface that our switch supports and consult configuration information about different interface types.

For detailed description of all interface commands used in this section, refer to Interface configuration command. For files of other commands appeared in this section, refer to other parts of the manual.

The introduction includes communication information that can be applied to all interface types.

1.1 Supported Interface Types

For information about interface types, please refer to the following table.

Interface type	Task	Reference
Ethernet interface	Configures fast Ethernet interface. Configures gigabit Ethernet interface. Configures 10GE Ethernet interface.	Setting the Ethernet Interface
Logical interface	Loopback interface Null interface Aggregation interface VLANinterface SuperVlan interface	Conifugring Logical Interface

The two supported kinds of interface: Ethernet interface and logical interface. The Ethernet interface type depends on one device depends on the standard communication interfaces provided by the
switch. The logical interface is the interface without the corresponding physical device, which is established by user manually.

The supported Ethernet interfaces of our switch include:

- Fast Ethernet
- Gigabit Ethernet interface
- 10GE Ethernet interface

The supported logical interface of our switch include:

- Loopback interface
- Null interface

- Aggregation interface
- VLANinterface
- SuperVlan interface

1.2 Interface Configuration Introduction

The following description applies to the configuration process of all interfaces. Take the following steps to perform interface configuration in global configuration mode.

(1) At this time, the switch prompt becomes ‘config_’ plus the shortened form of the interface to be configured. Use these interfaces in terms of their numbers. Interface numbers are assigned at the factory.
Run the show interface command to display these
interfaces. Each interface that the device supports provides its own state as follows:

```
Switch_config#show interface g0/2
GigaEthernet0/2 is administratively down, line protocol is down
  Hardware is Giga-Combo-FX, address is 00e0.0f8d.e0e1 (bia 00e0.0f8d.e0e1)
  MTU 1500 bytes, BW 10000 kbit, DLY 10 usec
  Encapsulation ARPA
  port info 1 0 2 1
  Auto-duplex,    Auto-speed
  flow-control off
    Received 0 packets, 0 bytes
    0 broadcasts, 0 multicasts
    0 discard, 0 error, 0 PAUSE
    0 align, 0 FCS, 0 symbol
    0 jabber, 0 oversize, 0 undersize
    0 carriersense, 0 collision, 0 fragment
    0 L3 packets, 0 discards, 0 Header errors
    Transmited 0 packets, 0 bytes
    0 broadcasts, 0 multicasts
    0 discard, 0 error, 0 PAUSE
    0 sqettest, 0 deferred
    0 single, 0 multiple, 0 excessive, 0 late
    0 L3 forwards
```

Note:

There is no need to add blank between interface type and interface number. For example, in the above line, g 0/2 or g 0/2 is both available.

(2) You can configure the interface configuration commands in interface configuration mode. Various commands define protocols and application programs to be executed on the interface. These commands will stay until user exits the interface configuration mode or switches to another interface.

(3) Once the interface configuration has been completed, use the show command in the following chapter ‘Monitoring and Maintaining Interface’ to test the interface state.

Chapter 2 Interface Configuration

2.1 Configuring Interface Common Attribute

The following content describes the command that can be executed on an interface of any type and configures common attributes of interface. The common attributes of interface that can be configured include: interface description, bandwidth and delay and so on.

2.1.1 Adding Description

Adding description about the related interface helps to memorize content attached to the interface. This description only serves as the interface note to help identify uses of the interface and has no effect on any feature of the interface. This description will appear in the output of the following commands: show running-config and show interface. Use the following command in interface configuration mode if user wants to add a description to any interface.

Command	Purpose
description *string*	Adds description to the currently-configured interface.

For examples relevant to adding interface description, please refer to the following section 'Interface Description Example'.

2.1.2 Configuring Bandwidth

The upper protocol uses bandwidth information to perform operation decision. Use the following command to configure bandwidth for the interface:

Command	Purpose
bandwidth *kilobps*	Configures bandwidth for the currently configured interface.

The bandwidth is just a routing parameter, which doesn't influence the communication rate of the actual physical interface.

2.1.3 Configuring Time Delay

The upper protocol uses time delay information to perform operation decision. Use the following command to configure time delay for the interface in the interface configuration mode.

Command	Purpose
delay *tensofmicroseconds*	Configures time delay for the currently configured interface.

The configuration of time delay is just an information parameter. Use this command cannot adjust the actual time delay of an interface.

2.2 Monitoring and Maintaining the Port

To maintain and monitor the interface, perform the following tasks:

- To browse the state of an interface, run the above-mentioned command.
- Initializing and deleting the port
- Closing and restarting the port

2.2.1 Browsing the State of an Interface

Our switches support those commands to display interface information, including the version ID of hardware and software, and the interface state. The following table presents you some port monitor commands: For more details, please refer to the "Interface Configuration Command".

Run the following commands:

Command	Purpose
show interface [**type** [slot|port]]	Displays the state of a port.
show running-config	Displays the current settings.
show version	Displays the memory configuration, the software version and the startup mirror.

2.2.2 Initializing and Deleting the Port

The logic interface can be dynamically created and deleted. So it is with the sub-interface and the channelized interface. The physical interface which cannot be deleted dynamically can return to the default setting of the interface. In global configuration mode, run the following command to initialize and delete an interface:

Command	Purpose
no interface [**type** [slot|port]]	Initializes a physical interface or deletes a virtual interface.

2.2.3 Closing and Restarting the Port

You can disable the interface, so that all functions on this interface can be disabled, and then all monitor commands will label this interface as unavailable. This information can be transmitted to other devices through the dynamic routing protocol. The modification on any route will not affect this port.

Run the following commands in interface configuration mode to shut down an interface and then restart it.

Command	Purpose

shutdown	Disable the interface.
no shutdown	Restarting the interface

To check whether an interface is shut down, you can run show interface and show running-config. After the show interface command is run, a disabled interface will be presented as “administratively down”. For more examples, please refer to "Interface Shutdown Example".

2.3 Setting the Ethernet Interface

In this section the procedure of setting the Enthernet interface will be described. The detailed configuration includes the following steps, among which step 1 is obligatory while other steps are optional.

2.3.1 Choosing an Ethernet Interface

Run the following command in global configuration mode to enter the Ethernet interface configuration mode:

Command	Function
interface fastethernet [*slot*|*port*]	Enters the fast-Ethernet interface configuration mode.
interface gigaethernet [*slot*|*port*]	Enters the gigabit-Ethernet interface configuration mode.
interface tgigaEthernet [*slot*|*port*]	Enters the 10GE-Ethernet interface configuration mode.

The show interface fastethernet command can be used to show the state of the Ethernet interface, while the show interface gigaethernet command can be used to show the state of the gigabit-Ethernet interface.

2.3.2 Setting the Rate

The Ethernet rate can be realized not only through auto-negotiation but also through interface configuration.

Command	Function
Speed {**10**|**100**|**1000**|**10000**|**auto**}	Sets the rate of fast Ethernet to 10M, 100M, 1000M or auto-negotiation.
No speed	Resumes the default settings. The rate is auto-negotiation.

Note:

The speed of the optical interface is fixed. For example, the speeds of GBIC and GE-FX are 1000M, while the speed of FE-FX is 100M. If the speed command for an optical interface has the auto parameter, the optical interface has the automatic negotiation function, or the optical interface is mandatory and cannot be negotiated.

2.3.3 Setting the Duplex Mode of an Interface

By default, the Ethernet interface can be auto, half duplex or full duplex. The duplex mode for the gigbit interface is always auto.

Command	Function
duplex {**full**|**half**|**auto**}	Sets the duplex mode of an Ethernet interface.
No duplex	Resumes the default settings. The duplex mode is auto-negotiation.

2.3.4 Setting Flow Control on an Interface

When an interface is in full duplex mode, flow control is realized through the 802.3X-defined PAUSE frame; when an interface is in half duplex mode, flow control is realized through backpressure.

Command	Usage Guidelines
flow-control on/off /atuo	Enables or disables flow control on an interface.
no flow-control	Resumes the default settings, that is, there is no flow control on an interface.

2.4 Configuring Logical Interface

This section describes how to configure a logical interface. The contents are as follows:

- Configuring null interface
- Configuring loopback interface.
- Configuring aggregation interface
- Configuring VLAN interface
- Configuring SuperVLAN interface

2.4.1 Configuring Null Interface

The whole system supports only one null interface. Its functions are similar to those of applied null devices on most operating systems. The null interface is always available, but it never sends or receives communication information. The null interface provides an optional method to filtrate communication. That is, the unwanted network communication can be routed to the null interface; the null interface can function as the access control list.

You can run the following command in global configuration mode to specify the null interface:

Command	Usage Guidelines
interface null *0*	Enters the null interface configuration state.

The null interface can be applied in any command that takes the interface type as its parameter.

The following example shows how to configure a null interface for the routing of IP 192.168.20.0.

ip route 192.168.20.0 255.255.255.0 null 0

2.4.2 Configuring Loopback Interface

The loopback interface is a logical interface. It always functions and continues BGP session even in the case that the outward interface is shut down. The loopback interface can be used as the terminal address for BGP session. If other switches try to reach the loopback interface, a dynamic routing protocol should be configured to broadcast the routes with loopback interface address. Messages that are routed to the loopback interface can be re-routed to the switch and be handled locally. For messages that are routed to the loopback interface but whose destination is not the IP address of the loopback interface, they will be dropped. This means that the loopback interface functions as the null interface.

Run the following command in global configuration mode to specify a loopback interface and enter the interface configuration state:

Command	Usage Guidelines
interface loopback *number*	Enter the loopback interface configuration state.

2.4.3 Configuring Aggregation Interface

The aggregator interface is introduced in the background that the bandwidth of a single Ethernet interface is insufficient. It can bind together multiple full-duplex interfaces of the same rate to multiply the bandwidth.

Run the following command to define the aggregation interface:

Command	Function
Interface port-aggregator *number*	Configuring aggregation interface

2.4.4 Configuring VLAN Interface

VLAN interface is the routing interface in switch. TheVLANcommand in global configuration mode only adds layer 2 VLAN to system without defining how to deal with the IP packet whose destination address is itself in the VLAN. If there is no VLAN interface, this kind of packets will be dropped.

Run the following command to define VLAN interface:

Command	Function
Interface vlan *number*	Configuring VLAN interface

2.4.5 Configuring SuperVLAN Interface

The Super VLAN technology provides a mechanism: hosts in different VLANs of the same switch can be allocated in the same Ipv4 subnet and use the same default gateway; lots of IP addresses are, therefore, saved. The Super VLAN technology puts different VLANs into a group where VLANs use the same management interface and hosts use the same IPv4 network section and gateway. VLAN belonging to Super VLAN is called as SubVLAN. No SubVLAN can possess the management interface by configuring IP address.

Run the following command to define Super VLAN interface:

Command	Function
Interface superVLAN *number*	Configuring the superVLAN interface

Chapter 3 Interface Configuration Example

3.1 Configuring Public Attribute of Interface

3.1.1 Example for Interface Description

The following example shows how to add a description for an interface.

```
interface vlan 1
ip address 192.168.1.23 255.255.255.0
```

3.1.2 Example of Interface Shutdown

The following example shows how to disable GigaEthernet interface 0/1.

```
interface GigaEthernet0/1
shutdown
```

The following example shows how to restart the interface.

```
interface GigaEthernet0/1
no shutdown
```

Interface Range Configuration

Table of Contents

Chapter 1 Interface Range Configuration 1
1.1 Interface Range Configuration Task 1
1.1.1 Understanding Interface Range 1
1.1.2 Entering Interface Range Mode 1
1.1.3 Configuration Example 1

Chapter 1 Interface Range Configuration

1.1 Interface Range Configuration Task

1.1.1 Understanding Interface Range

In the process of configuring interface tasks, there are cases when you have to configure the same attribute on ports of the same type. In order to avoid repeated configuration on each port, we provide the **interface range** configuration mode. You can configure ports of the same type and slot number with the same configuration parameters. This reduces the workload.

Note:

when entering the **interface range** mode, all interfaces included in this mode must have been established.

1.1.2 Entering Interface Range Mode

Run the following command to enter the **interface range** mode.

Step	Command	Description
1	**interface range** *type slot*/<*port1* - *port2* | port3>[, <port1 - port2|port3>]	Enters the range mode. All ports included in this mode accord to the following conditions: (1) The slot number is set to **slot**. (2) The port numbers before/after the hyphen must range between port1 and port2, or equal to port3. (3) Port 2 must be less than port 1 (4) There must be space before/after the hyphen or the comma.

1.1.3 Configuration Example

Enter the interface configuration mode via the following commands, including slot 0 and fast Ethernet 1,2,3,6,8,10,11,12:

switch_config#interface range 1 - 3 , 6 , 8 , 10 - 12

switch_config_if_range#

Port Additional Characteristics Configuration

Table of Contents

Chapter 1 Port Additional Characteristics Configuration....1
1.1 Storm Block....1
1.2 Port Isolation....1
1.3 Storm Control....2
1.4 Rate Limit....2
1.5 Loopback Detection....3
1.6 MAC Address Learning....3
1.7 Port Security....4
1.8 Port Binding....4
1.9 VLAN MAC Address Learning....5
1.10 VLAN MAC Address Learning Number....5
1.11 Port FEC....6
1.12 Configuring Link scan....6
1.12.1 Overview....6
1.12.2 Link Scan Configuration Task....6
1.12.3 Configuration Example....7
1.13 Configuring system mtu....7
1.13.1 Overview....7
1.13.2 Configuration Task....7
1.13.3 Configuration Example....7

Chapter 1 Port Additional Characteristics Configuration

1.1 Storm Block

In actual application, the Ethernet interface may receive the unknown packets (DLF packets) and the switch then broadcasts by default this kind of packets to all interfaces in a VLAN. This will increase the network load and influence the network capacity. To avoid the DLF packets from being broadcasted, you can set on the egress to drop the DLF packets, which is called storm limit.

Command	Purpose
config	Enters the global configuration mode.
interface g0/1	Enters the to-be-configured port.
[no] **switchport block {unicast|multicast|broadcast}**	Configures the port storm block. **Unicast** means that storm block is conducted to the unknown unicast packets. **Multicast** means that storm block is conducted to the multicast packets. **Broadcast** means that storm block is conducted to the broadcast packets.
exit	Backs to the global configuration mode.
exit	Backs to the EXEC mode.

1.2 Port Isolation

Generally, the packets between different ports of a switch can be freely forwarded. In some cases, the data flows between ports need be forbidden and port isolation is then required. Data communication cannot go on between isolated ports, but can do between normal ports or between normal port and isolated port. Data communication cannot go on between the isolated ports within one group, but can do between the isolated port and any arbitrary port outside the group. It is noted that port isolation plays a role in the layer-2 packets. This switch series does not support group-based isolation.

Isolation not based on the group:

Command	Purpose
config	Enters the global configuration mode.
interface g0/1	Enters the to-be-configured port.

exit	Backs to the global configuration mode.
exit	Backs to the EXEC mode.

1.3 Storm Control

The port of a switch may bear continuous and abnormal impact from unicast (MAC address fails to be found), multicast or broadcast packets, and therefore gets paralyzed even to the extent that the whole switch breaks down. That's why a mechanism must be provided to limit this phenomena. The storm control enables the switch to set on the ingress the rates of different kinds of packets.

Command	Purpose
config	Enters the global configuration mode.
interface g0/1	Enters the to-be-configured port.
[no] **storm-control** {**broadcast** | **multicast** | **unicast**} **threshold** *count*	Configures the port storm block. **Unicast** means that storm control is conducted to the unknown unicast packets. **Multicast** means that storm control is conducted to the multicast packets. **Broadcast** means that storm control is conducted to the broadcast packets. Count means to-be-configured threshold.
exit	Backs to the global configuration mode.
exit	Backs to the EXEC mode.

1.4 Rate Limit

Rate limit is used to limit the rate of a flow that runs through a port. Run the following command in the EXEC mode to configure the rate limit.

Command	Purpose
config	Enters the global configuration mode.
interface g0/1	Enters the to-be-configured port.
[no] **switchport rate-limit {***band* **| Bandwidth** *percent }* { **ingress** | **egress**}	Configures the rate limit for a port. *Band* is the limited rate. *Percent* is the limited ratio.

	ingress means to exert an influence on the ingress. **egress** means to exert an influence on the egress.
exit	Backs to the global configuration mode.
exit	Backs to the EXEC mode.

1.5 Loopback Detection

Loopback detection is used to check whether loopback exists on an interface. You can configure the interval for a port to transmit the loop check packets. Run the following command in EXEC mode to forward the time interval of the loopback detection packets.

Command	Purpose
config	Enters the global configuration mode.
Interface g0/1	Enters the to-be-configured port.
[no] **keepalive** [*second*]	To configure the interval for a port to transmit the loop check packets, run keepalive second. *second* means the interval of transmitting the packets.
exit	Backs to the global configuration mode.
exit	Backs to the EXEC mode.

1.6 MAC Address Learning

To enable or disable MAC learning on a port, run the following commands.

Command	Purpose
config	Enters the global configuration mode.
interface g0/1	Enters the to-be-configured port.
[no] **switchport disable-learning**	Configures MAC Learning on a Port. Enable/disable port MAC address learning.
exit	Backs to the global configuration mode.
exit	Backs to the EXEC mode.

Port security supports security control on an interface. Port security has three modes: dynamic security mode, static reception mode and static rejection mode. In dynamic security mode, you can set the threshold of MAC addresses that can be learned by a port. If the learned MAC addresses on a port have reached the threshold in number, the switch will not learn the MAC addresses any more and at the same time drop all DLF packets. In static security mode, you can set the static security MAC address on a port and then you should consider two cases: if it is in static reception mode, only the packets whose destination MACs are security MACs can be allowed to enter this port and other packets will be dropped; if it is in static rejection mode, the packets whose destination MACs are security MACs will be all dropped and other packets will be allowed to pass through this port.

Command	Purpose
config	Enters the global configuration mode.
interface g0/1	Enters the to-be-configured port.
[no] **switchport port-security mode** {**dynamic | static** *accept|reject* }	Configures the port security mode. Dynamic means the dynamic security mode. *static accept* means the static reception mode. *static reject* means the static rejection mode.
[no] **switchport port-security dynamic maximum** *num*	Sets the threshold of learning MAC addresses.
[**no**] **switchport port-security static mac-address** *H.H.H*	Sets static security address
exit	Backs to the global configuration mode.
exit	Backs to the EXEC mode.

1.8 Port Binding

This type of switches can bind the IP address and the MAC address to a port at the same time, and of course you can bind either one to the port.

Run the following commands to enter the EXEC mode:

Command	Purpose
config	Enters the global configuration mode.
interface g0/1	Enters the to-be-configured port.
[no] **switchport port-security**	Configures the port binding function.

A.B.C.D **| mac** *H.H.H* }	bind means that only the packets that comply with the binding requirements can pass while other packets will be dropped; block means that only the packets that comply with the binding requirements will be rejected and other packets will pass. Ip means only the ip packets that comply with the binding requirements can pass. Arp means only the arp packets that comply with the binding requirements can pass. both-arp-ip means that ip and arp packets that comply with the binding requirements can pass.
exit	Backs to the global configuration mode.
exit	Backs to the EXEC mode.

1.9 VLAN MAC Address Learning

To enable or disable Vlan MAC learning on a port, run the following commands.

Command	Purpose
config	Enters the global configuration mode.
[no] vlan disable-learning < add | remove word | word>	Disable/enable vlan mac address learning Enable/disable vlan mac address learning.
exit	Backs to the EXEC configuration mode.

1.10 VLAN MAC Address Learning Number

To configure VLAN MAC Address Learning Number, run the following command:

Command	Purpose
config	Enters the global configuration mode
[no] **vlan dynamic vlan** *word* **maximum** *num*	Cancels/configures the learnable max number of vlan mac address Word needs to configure vlan of learning address num learnable max mac address num
exit	Exit to management configuration mode

To reduce error rate of 100G port using dual-mode optical module, enable FEC. The function runs with enabled ports on both sides. Disable this function when using the single-mode optical module.

To enter the configuration mode, run the following mode:

Command	Purpose
config	Enters the global configuration mode.
interface cg0/1	Enters the port to be configured.
[no] **fec-enable**	Configures port FEC.
exit	Exit from the global configuration mode.
exit	Exit from the management configuration mode.

1.12 Configuring Link scan

1.12.1 Overview

The command is used to scan the time interval on the port. You can fast scan the up/down state on the port.

1.12.2 Link Scan Configuration Task

- Configure the time interval on the port.

1. Set the time interval of port scan

To set the scan interval of an interface, run the following command in the global configuration mode:

Command	Purpose
[no] Link scan {**mode highspeed | normal** *interval* **| fast** *interval* }	Mode: optical port scan mode Normal: standard link scan mode Fast link scan mode. Fast mode is mainly used for service protocol requirement, such as rstp. *interval*: Set the time interval of port scan.
Command	Purpose

link scan normal time	Sets the time interval of port scan.

1.12.3 Configuration Example

The following example shows how to set the scan interval to 20ms.

link scan normal 20

1.13 Configuring system mtu

1.13.1 Overview

This is used to configure system mtu.

1.13.2 Configuration Task

- Set system mtu.

1. Set system mtu

Run the following command in the global configuration mode:

Command	Purpose
[no] system mtu *mtu*	Set the mtu value of the system.

1.13.3 Configuration Example

The following example shows how to set mtu to 1536 bytes.

Switch_config#system mtu 1536

Port Additional Characteristics Configuration

Table of Contents

Chapter 1 Interface Configuration 1
1.1 Configuring the Ethernet Interface 1
1.1.1 Configuring Flow Control for the Port 1
1.1.2 Comfiguring the Rate Unit for the Port 1
1.1.3 Configuring the Storm Control on the Port 2
Chapter 2 Secure Port Configuration 3
2.1 Overview 3
2.2 Configuration Task of the Secure Port 3
2.3 Configuring the Secure Port 3
2.3.1 Configuring the Secure Port Mode 3
2.3.2 Configuring the Static MAC Address of the Secure Port 4

Chapter 1 Interface Configuration

1.1 Configuring the Ethernet Interface

The switch supports the 10Mbps/100Mbps Ethernet interfaces. See the following content for detailed configuration. Among the configuration, the first step is mandatory while others are optional.

1.1.1 Configuring Flow Control for the Port

You can control the flow rate on the incoming and outgoing ports through configuration.
Run the following commands in previliged mode to limit the flow rate of the port.
Each band is defaulted as 128 kbps.

Command	Purpose
configure	Enters the global configuration mode.
interface f1/0	Enters the to-be-configured port.
[no] switchport rate-limit *band* { ingress|egress}	Configures the flow rate limits for the port. The parameter **band** represents the to-be-limited flow rate. The parameter **ingress** means the function works at the incoming port. The parameter **egress** means the function works at the outgoing port.
exit	Exits the global configuration mode.
exit	Returns the EXEC mode.

1.1.2 Comfiguring the Rate Unit for the Port

Run the following commands to modify the rate unit of the flow on a port. The rate unit can be one of these values: 16K, 64K, 128K, 1M, 10M and 40M.

Command	Purpose
Configure	Enters the global configuration mode.
[**no**] **rate-unit count**	Configures the rate unit for a port.
exit	Returns the EXEC mode.

1.1.3 Configuring the Storm Control on the Port

The ports of the switch may receives the attack by the continuous abnormal unicast (MAC address lookup failing), multicast or broadcast message. In this case, the attacked ports or the whole switch may break down. The storm control mechanism of the port is therefore generated.

Command	Purpose
storm-control {**broadcast** | **multicast** | **unicast**} **threshold count**	Performs the storm control to the broadcast/multicast/unicast message.
no storm-control {**broadcast** | **multicast** | **unicast**} **threshold**	Cancels the storm control.

Chapter 2 Secure Port Configuration

2.1 Overview

You can control the access function of the secure port, enabling the port to run in a certain range according to your configuration. If you enable the security function of a port through configuring the number of secure MAC addresses for the port. If the number of secure MAC addresses exceeds the upper limitation and MAC addresses are insecure, secure port violation occurs. You should take actions according to different violation modes.

The secure port has the following functions:

- Configuring the number of secure MAC addresses
- Configuring static secure MAC addresses
  If the secure port has no static secure MAC address or the number of static secure MAC addresses is smaller than that of secure MAC addresses, the port will learn dynamic MAC addresses.
- Dropping violated packets when secure port violation occurs

The section describes how to configure the secure port for the switch.

2.2 Configuration Task of the Secure Port

- Configuring Secure Port Mode
- Configuring the Static MAC Address of the Secure Port

2.3 Configuring the Secure Port

2.3.1 Configuring the Secure Port Mode

There are two static secure port modes: accept and reject. If it is the **accept** mode, only the flow whose source address is same to the local MAC address can be received by the port for communication. If it is the **reject** mode, only the flow whose source address is different to the local MAC address can be received by the port.

Run the following commands in EXEC mode to enable or disable the secure port function:

Command	Purpose
configure	Enters the global configuration mode.
interface g0/1	Enters the to-be-configured port.

[no] switchport port-security mode static {accept | reject}	Configures the secure port mode.
exit	Goes back to the global configuration mode.
exit	Goes back to the EXEC mode.
write	Saves the configuration.

2.3.2 Configuring the Static MAC Address of the Secure Port

After you configure the static MAC address of the secure port, In **accept** mode, the flow whose source address is same to the local MAC address can be received by the port for communication. In **reject** mode, the flow whose source address is different to the local MAC address can be received by the port.

Run the following commands in EXEC modeto configure the static MAC address of the secure port:

Command	Purpose
configure	Enters the global configuration mode.
interface g0/1	Enters the to-be-configured port.
[no] switchport port-security static mac-address *mac-addr*	Adds or deletes the static MAC address of the secure port. • ***mac-addr*** is the configured MAC address.
exit	Goes back to the global configuration mode.
exit	Goes back to the EXEC mode.
write	Saves the configuration.

Port Mirroring Configuration

Table of Contents

Chapter 1 Configuring Port Mirroring.....1
1.1 Configuring Port Mirroring Task List..... 1
1.2 Configuring Port Mirroring Task..... 1
1.2.1 Configuring Port Mirroring.....1
1.2.2 Displaying Port Mirroring Information..... 1

Chapter 1 Configuring Port Mirroring

1.1 Configuring Port Mirroring Task List

- Configuring port mirroring
- Displaying port mirroring information

1.2 Configuring Port Mirroring Task

1.2.1 Configuring Port Mirroring

Through configuring port mirroring, you can use one port of a switch to observe the traffic on a group of ports.

Enter the privilege mode and perform the following steps to configure port mirroring:

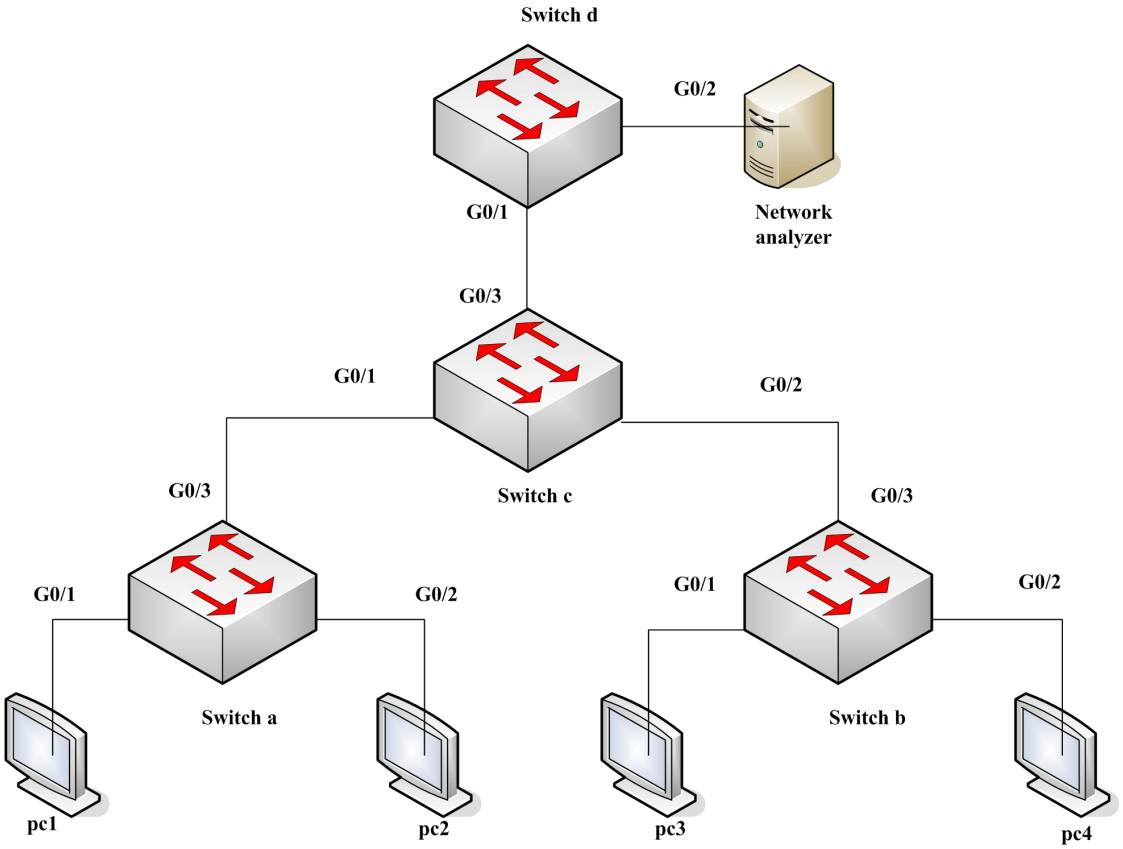
Command	Description
configure	Enters the global configuration mode.
mirror session *session_number* {**destination** {**interface** *interface-id*} | **source** {**interface** *interface-id* [, | -]rx] }	Configures port mirroring. **session-number** is the number of the port mirroring. **destination** is the destination port of the mirroring. **source** is the source port of mirroring. **rx** means the input data of mirroring.
exit	Enters the management mode again.
write	Saves the configuration.

1.2.2 Displaying Port Mirroring Information

Run show to display the configuration information of port mirroring.

Command	Description
show mirror [session *session_number]*	Displays the configuration information about port mirroring. **session-number** is the number of the port mirroring.

The network topology is shown in the following figure:



You need to monitor the traffic of interface g0/1 on switch a and interface g0/1 on switch b by the network analysis meter.

Configure as follows by the remote mirroring:

switch a:

mirror session 1 destination interface g0/3 rspan 100 0x8100

mirror session 1 source interface g0/1 both

switch b:

mirror session 1 destination interface g0/3 rspan 1000 0x8100

mirror session 1 source interface g0/1 both

switch c:

vlan disable-learning 100,1000

```
interface GigaEthernet0/1
 switchport mode trunk
!
interface GigaEthernet0/2
 switchport mode trunk
!
interface GigaEthernet0/3
 switchport mode trunk
!
!
vlan 1,100,1000
!
```

switch d:

```
mirror session 1 destination interface g0/2
mirror session 1 source interface g0/1 both
```

MAC Address Table Attribute Configuration

Table of Contents

Chapter 1 Configuring MAC Address Attribute..... 1
1.1 MAC Address Configuration Task List.....1
1.2 MAC address Configuration Task.....1
1.2.1 Configuring Static Mac Address.....1
1.2.2 Configuring MAC Address Aging Time.....1
1.2.3 Displaying MAC Address Table.....2
1.2.4 Clearing Dynamic MAC Address.....2

Chapter 1 Configuring MAC Address Attribute

1.1 MAC Address Configuration Task List

- Configuring Static Mac Address
- Configuring Mac Address Aging Time
- Configring VLAN-shared MAC Address
- Displaying Mac Address Table
- Clearing Dynamic Mac Address

1.2 MAC address Configuration Task

1.2.1 Configuring Static Mac Address

Static MAC address entries are MAC address entries that do not age by the switch and can only be deleted manually. According to the actual requirements during the operation process, you can add and delete a static MAC address. Use the following command in privileged level to add and delete a static MAC address.

Command	Purpose
configure	Enters the global configuration mode.
[no] mac address-table static *mac-addr* **vlan** *vlan-id* **interface** *interface-id*	Adds/deletes a static MAC address entry. Mac-addr indicates the MAC address. Vlan-id indicates the VLAN number. Valid value is from 1~4094. Interface-id indicates the interface name.
exit	Returns to EXEC mode.
write	Saves configuration.

1.2.2 Configuring MAC Address Aging Time

When a dynamic MAC address is not used during the specified aging time, the switch will delete this MAC address from the MAC address table. The aging time of the switch MAC address can be configured in terms of needs. The default aging time is 300 seconds.

Configure the aging time of MAC address in the privileged mode as follows:

Command	Purpose
configure	Enters the global configuration mode

mac address-table aging-time [**0 | 10-1000000**]	Configures the aging time of MAC address. 0 indicates no-age of the MAC address. Valid value is from 10 to 1000000 in seconds.
exit	Returns to the management mode.
write	Saves configuration.

1.2.3 Displaying MAC Address Table

Since debugging and management are required in operation process, we want to know content of the switch MAC address table. Use the show command to display content of the switch MAC address table.

Command	Purpose
show mac address-table {**dynamic** [**interface** interface-id **| vlan** vlan-id] **| static**}	Displays content of the MAC address table. Dynamic indicates the MAC address that acquires dynamically. Vlan-id indicates the VLAN number. Valid value is from 1 to 4094. Interface-id indicates the interface name. Static indicates the static MAC address table.

1.2.4 Clearing Dynamic MAC Address

The acquired MAC addresses need to be cleared in some circumstances.

Use the following command to delete a dynamic MAC address in privileged mode:

Command	Purpose
clear mac address-table dynamic [address *mac-addr* | **interface** *interface-id* **| vlan** *vlan-id*]	Deletes a dynamic MAC address entry. Dynamic indicates the MAC address that dynamically acquires. Mac-addr is the MAC address. Interface-id indicates the interface name. Vlan-id indicates the VLAN number. Valid value is from 1 to 4094.

MAC Access List Configuration

Table of Contents

Chapter 1 Configuring MAC List 1
1.1 MAC List Configuration Task 1
1.1.1 Creating MAC List 1
1.1.2 Configuring Items of MAC List 1
1.1.3 Applying MAC List 2

Chapter 1 Configuring MAC List

1.1 MAC List Configuration Task

1.1.1 Creating MAC List

To apply the MAC list on the port, you must first create the MAC list. After the MAC list is successfully created, you log in to the MAC list configuration mode and then you can configure items of the MAC access list.

Perform the following operations to add and delete a MAC list in privilege mode:

Run…	To…
configure	Log in to the global configuration mode.
[**no**] **mac access-list** *name*	Add or delete a MAC list. **name** means the name of the MAC list.

1.1.2 Configuring Items of MAC List

You can use the **permit** or **deny** command to configure the **permit** or **deny** items of the MAC list. Multiple **permit** or **deny** items can be configured on a MAC list.

The mask of multiple items configured in a MAC list must be the same. Otherwise, the configuration may be out of effect (see the following example). The same item can only be configured once in the same MAC address.

Perform the following operations in MAC list configuration mode to configure the items of the MAC list:

Run…	To…
[no] {deny | permit} {**any** | **host** *src-mac-addr*} {**any** | **host** *dst-mac-addr*}**[**ethertype**]**	Add/Delete an item of the MAC list. You can rerun the command to add or delete multiple items of the MAC list. **any** means any MAC address can be compatible; **src-mac-addr** means the source MAC address; **dst-mac-addr** means the destination MAC address. **ethertype** means the type of matched Ethernet packet.
exit	Log out from the MAC list configuration mode and enter the global configuration mode again.
exit	Enter the management mode again.
write	Save configuration.

MAC list configuration example

Switch_config#mac acce 1

Switch-config-macl#permit host 1.1.1 any
Switch-config-macl#permit host 2.2.2 any

The above configuration is to compare the source MAC address, so the mask is the same. The configuration is successful.

Switch_config#mac acce 1
Switch-config-macl#permit host 1.1.1 any
Switch-config-macl#permit any host 1.1.2
Switch-config-macl#2003-11-19 18:54:25 rule conflict,all the rule in the acl should match!

The first line on the above configuration is to compare source MAC addresses, while the second line is to compare destination MAC addresses. Therefore, the mask is different. The configuration fails.

1.1.3 Applying MAC List

The created MAC list can be applied on any physical port. Only one MAC list can be applied to a port. The same MAC list can be applied to multiple ports.

Enter the privilege mode and perform the following operation to configure the MAC list.

Run…	To…
configure	Enter the global configuration mode.
interface f0/1	Log in to the port that is to be configured.
[**no**] **mac access-group** *name*	Apply the created MAC list to the port or delete the applied MAC list from the port. **name** means the name of the MAC list.
exit	Enter the global configuration mode again.
exit	Enter the management mode again.
write	Save configuration.

802.1x Configuration

Chapter 1 802.1x Configuration 1
1.1 802.1x Configuration Task List 1
1.2 802.1x Configuration Tasks 1
1.2.1 Configuring 802.1x Authentication on the Port 1
1.2.2 Configuring 802.1x on Multiple Ports Authentication 2
1.2.3 Configuring 802.1x Re-Authentication 3
1.2.4 Configuring 802.1x Authentication Retry Times 3
1.2.5 Configuring 802.1x Transmission Frequency 3
1.2.6 Configuring Refresh Time of Hybrid MAB Authentication 3
1.2.7 Configuring Aging time of MAB Authentication 4
1.2.8 Configuring 802.1x User Binding 4
1.2.9 Configuring 802.1x Mac Address Binding 4
1.2.10 Configuring the Authentication Method on the 802.1x Port 4
1.2.11 Selecting the Authentication type for the 802.1x Port 5
1.2.12 Configuring MAB Authentication on the Port 5
1.2.13 Configuring 802.1x Accounting 6
1.2.14 Configuring 802.1x guest-vlan 6
1.2.15 Forbidding the Multi-NIC Supplicant 7
1.2.16 Resuming the Default Settings of 802.1x 7
1.2.17 Monitoring the 802.1x Authentication Configuration and State 7
1.3 802.1x Configuration Example 7

Chapter 1 802.1x Configuration

1.1 802.1x Configuration Task List

- Configuring 802.1x Authentication on the Port
- Configuring 802.1x on Multiple Ports of the Host
- Configuring 802.1x Re-Authentication
- Configuring 802.1x Authentication Retry Times
- Configuring 802.1x transmission frequency
- Configuring 802.1x User Binding
- Configuring the Authentication Method on the 802.1x Port
- Selecting the Authentication Mode for the 802.1x Port
- Configuring MAB Authentication on the Port
- Configuring 802.1x Accounting
- Configuring 802.1x guest-vlan
- Forbidding the Multi-NIC Supplicant
- Resuming the Default Settings of 802.1x
- Monitoring the 802.1x Authentication Configuration and State

1.2 802.1x Configuration Tasks

1.2.1 Configuring 802.1x Authentication on the Port

802.1x has three modes to control the port: force-authorized, force-unauthorized and enable.

Force-authorized means that the port has been authenticated and thus no authentication process is needed. In this mode, all users can conduct the data access control through the port. This mode is the default mode of the port. Force-unauthorized means that port authentication is not passed no matter what kind of authentication method you apply. In this mode, all users cannot conduct the data access control through the port.

Enable means that the 802.1x authentication protocol will be run on the port and the users who access the port will be authenticated by 802.1x. The successfully-authenticated users can conduct the data access control through the port. After enabling 802.1x authentication, you have to configure AAA authentication method.

the following commands:

Command	Purpose
dot1x enable	Enables the 802.1x function.

Run the following commands to enable the 802.1x authentication:

Command	Purpose
dot1x port-control auto	Sets the port to the 802.1x control mode.
aaa authentication dot1x {*default* **|** *word* } *method1* [*method2...*]	Configures 802.1x AAA authentication.

Run one of the following commands in interface configuration mode to select the 802.1x control mode:

Command	Purpose
dot1x port-control auto	Sets the port to the 802.1x control mode.
dot1x port-control force-authorized	The port authentication is authorized mandatorily.
dot1x port-control force-unauthorized	The port authentication is unauthorized mandatorily.

1.2.2 Configuring 802.1x on Multiple Ports Authentication

The 802.1x authentication is mainly for the single host user. At this time, the switch allows only one user to conduct the authentication and the access control. However, sometimes the port may connect multiple hosts through device without 802.1x support, such as an unmanaged switch. In order to make these hosts' users access successfully, you can enable the multi-host port access function. Actually, the authentication port may connect with multiple users. To ensure all users can be authenticated adn visited, enable multiuser authentication function.

There are two kinds of multi-host authentication: one is the multiple-hosts mode and the other is multiple-auth mode. The multiple-hosts mode is that when one of the hosts passes through the authentication the port will be up and the other hosts (including the previous ones and the following ones) will not need authentication; the multiple-auth mode is that the switch authenticates each host respectively and these authentications do not interfere with each other. When only one user passes its authentication, the interface will be up; only when all users fail in their authentication, in another word, only when no successfully authenticated user exist on the interface, the interface will be down. This mechanism gives guarantee to respective authentication for each user and if a user fails in its authentication, other users still have the normal access rights.

Note: The multi-auth mode cannot coexist with guest vlan or mab. If an interface is in multi-auth mode, all users on the interface will be authenticated again.

Run the following command in interface configuration mode to activate the 802.1x multi-host port authentication:

Command	Purpose
dot1x authentication multiple-hosts	Sets 802.1x multiple-hosts interface access mode. As long as one user passes the

dot1x authentication multiple-auth	Sets 802.1x multiple-hosts interface authentication mode. The authentication for each user is in parallel.

1.2.3 Configuring 802.1x Re-Authentication

After the authentication is passed, the authentication to the client will still be conducted every interval to ensure the legality of the client's authentication.

In this case, you need to enable the re-authentication function. After the re-authentication is started, the authentication request will be periodically sent to the host.

Run the following commands to configure the re-authentication function.

Command	Purpose
dot1x re-authentication	Enables the re-authentication function.
dot1x timeout re-authperiod *time*	Configures the period of the re-authentication function.

1.2.4 Configuring 802.1x Authentication Retry Times

After the authentication is failed, the switch will continue forward request/ID packet to resume the authentication. If the device has no response when the authentication exceeds the max retry times, the authentication will be suspended.

Run the following commands to configure the max re-authentication times:

Command	Purpose
dot1x reauth-max *count*	Configures the retry times after the re-authentication function fails.

1.2.5 Configuring 802.1x Transmission Frequency

During 802.1x authentication, the packets will be transmitted to the client's host. You can adjust the data transmission to ensure the response of the client's host by controlling the 802.1x transmission frequency.

Run the following command to configure the transmission frequency.

Command	Purpose
dot1x timeout tx-period *time*	Sets the transmission frequency of the 802.1x packet.

1.2.6 Configuring Refresh Time of Hybrid MAB Authentication

The command is used to configure the refresh time of hybrid MAB authentication and read dynamic mac address of the port in each refresh event.

The following command is used to configure the refresh time.

Command	Purpose
dot1x timeout misc-mab-refresh *time*	Sets hybrid refresh time of MAB authentication

1.2.7 Configuring Aging time of MAB Authentication

The command is used to configure the aging time of hybrid MAB authentication. Re-read dynamic mac address of the port in each refresh event. If the mac address has an corresponding auth, refresh the aging time of auth; if it does not exist, the mac address ages.

The following command is used to configure the aging time:

Command	Purpose
dot1x timeout misc-mab-aging *time*	Sets aging time of hybrid MAB authentication

1.2.8 Configuring 802.1x User Binding

You can bind the user to a certain port during 802.1x authentication to ensure the security of the interface access. To enable the 802.1x user binding, run the following command in interface configuration mode:

Command	Purpose
dot1x user-permit *xxxz*	Configures the user which is bound to the interface.

1.2.9 Configuring 802.1x Mac Address Binding

802.1x authentication can bind a MAC address to a port for secure access.
To enable MAC binding, use this command in interface configuration mode:

Command	Purpose
dot1x macr-permit *h:h:h:h:h:h*	Sets the port bound MAC address.

1.2.10 Configuring the Authentication Method on the 802.1x Port

Different ports will be applied with different authentication methods during 802.1x authentication. By default, the 802.1x authentication adopts the default method.

To configure the 802.1x authentication method, run the following command in interface configuration mode:

Command	Purpose
dot1x authentication method *yyy*	Configures the 802.1x authentication method.

The authentication mode can be selected during the 802.1x authentication. The authentication class decides whether AAA uses the CHAP authentication or the EAP authentication. If the CHAP authentication is used, the challenge required by MD5 is locally generated; if the EAP authentication is used, the challenge is generated on the authentication server. Only one authentication mode can be applied to one interface. By default, the authentication mode is applied in global mode. When an authentication mode is configured for an interface, the authentication mode will be always used on the interface unless the negative form of the command is run to resume the default settings.

EAP-TLS adopts the electronic certificate as the evidence of authentication and follows the handshake regulations in TLS so that it is more secure.

Run the following command in global configuration mode to configure an authentication mode:

Command	Purpose
dot1x authen-type {**chap**|**eap**}	Selects CHAP or EAP.

To configure the authentication mode, you also can run the following command in interface configuration mode:

Command	Purpose
dot1x authentication type {**chap**|**eap**}	Selects CHAP or EAP, or just uses the configuration class in global mode.

1.2.12 Configuring MAB Authentication on the Port

When a peer device cannot run the 802.1x client software, the switch will adopt the MAB authentication mode and then the MAC address of the peer device will be sent as both the username and password to the radius server for authentication.

Note: You can run the dot1x mabformat command on a switch to specify the accounting ID and the password's format so that you make it sure that they are same with those on the radius server.

When the MAB authentication is enabled and the peer device, however, neither sends the eapol_start packet nor responds to the request_identity packet and exceeds the timeout threshold, the switch regards this case as the evidence of not support the 802.1x authentication client on the peer device and then turns to the MAB authentication. When the switch sends the gained MAC address as the username and password to the Radius server for authentication, the authentication will still not succeed until the switch has authorized this MAC address.

Note: The MAB authentication mode cannot coexist with the multi-auth mode.

To enable the MAB authentication, you also can run the following command in interface configuration mode:

Command	Purpose
dot1x mab	Enables the MAB authentication on a port.

To set the format of the MAC address, you can run the following command in global configuration mode:

Command	Purpose
dot1x mabformat{1|2|3|4|5|6}	Chooses one MAC address' format from format 1 to format 6. The default format is 1.

1.2.13 Configuring 802.1x Accounting

The time the dot1x authentication is adopted you can conduct accounting. The actual accounting mechanism is that after dot1x authentication a judgment will be made as of whether the accounting is enabled on an authentication interface; if it is yes, the AAA interface will send the accounting request, and after receiving the request response information from the AAA module the authentication interface can allow the packets to pass through.

For the detailed accounting methods, refer to the relevant contents in the document AAA Settings.

For the correctness of the accounting data, the dot1x, after the accounting starts, will periodically use the AAA interface to send the update data to the server, while the AAA module, according to different AAA settings, decides whether to really send the accounting data.

Meanwhile, the dot1x re-authentication shall be enabled so that the switch will know a trouble as soon as it occurs on the supplicant.

To enable dot1x accounting and then set the accounting method, run the following commands in interface configuration mode:

Command	Purpose
dot1x accounting enable	Opens 802.1x accounting.
dot1x accounting method {*method name***}**	Sets the accounting method.

1.2.14 Configuring 802.1x guest-vlan

Guest-vlan is to attribute the corresponding port with a limited access permission when the client does not respond. Guest-VLAN can be any configured VLAN in a system; when the configured guest –VLAN cannot reach the requirements, the port cannot enter the guest VLAN.

Note: If the authentication fails, the port will obtain no access permission.

To enable the guest vlan in global mode, run the following command:

Command	Purpose
dot1x guest-vlan	Opens the guest-VLAN on all ports.

At the initial time when the guest-vlan ID of each port is 0, the guest-vlan takes no effect even if it is enabled in global mode; only when the guest vlan ID is set in port configuration mode can the guest VLAN work.

Run the following command to set guest-vlan ID in port configuration mode:

Command	Purpose
dot1x guest-vlan {id(1-4094)}	Sets the VLAN ID of the guest VLAN on a port.

This command can be used to forbid the supplicant terminal with multiple network adapters, preventing an agent from being occurred. Run the following command in port configuration mode:

Command	Purpose
dot1x forbid multi-network-adapter	Forbids the supplicant with multiple NICs.

1.2.16 Resuming the Default Settings of 802.1x

This command is used to resume all global configurations to the default settings. To configure the authentication mode, you also can run the following command in interface configuration mode:

Command	Purpose
dot1x default	This command is used to resume all global configurations to the default settings.

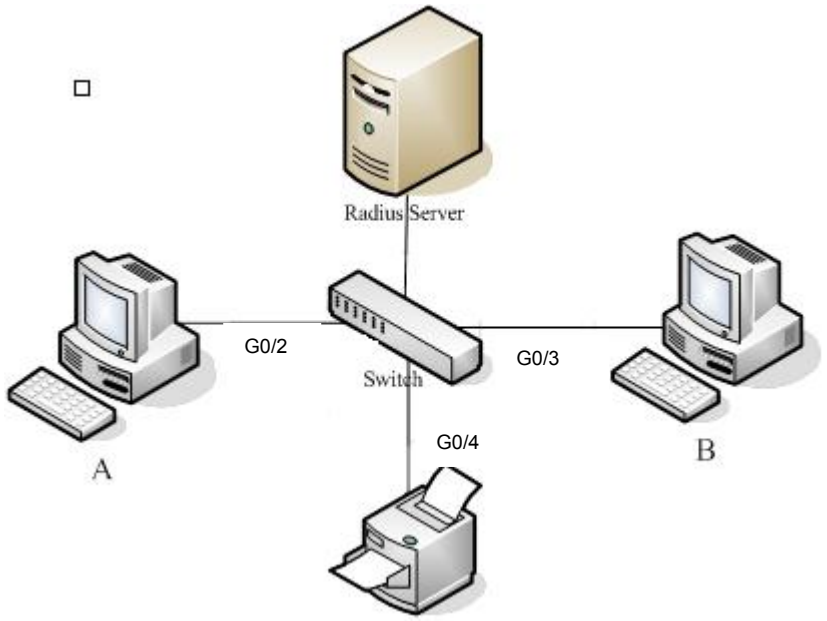
1.2.17 Monitoring the 802.1x Authentication Configuration and State

To monitor the 802.1x authentication configuration and state, run the following commands in EXEC mode:

Command	Purpose
show dot1x { *interface*|*statistics* }	Displays the 802.1x authentication configuration and state.

1.3 802.1x Configuration Example

See the following figure:



C the G0/4 interface; the radius-server host's IP is 192.168.20.2 and its key is TST; on the G0/2 interface the remote radius authentication, user-bind, accounting and re-authentication will be enabled altogether, on the G0/3 interface the local authentication, eap, multi-hosts and guest-vlan are enabled altogether, and on the G0/4 interface the MAB authentication is used and its MAC address' format is AA:BB:CC:DD:EE:FF.

Global configuration

```
username switch password 0 TST
username TST password 0 TST
aaa authentication dot1x TST-G0/2 group radius
aaa authentication dot1x TST-G0/3 local
aaa authentication dot1x TST-G0/4 group radius
aaa accounting network dot1x_acc start-stop group radius
dot1x enable
dot1x re-authentication
dot1x timeout re-authperiod 10
dot1x mabformat 2
dot1x guest-vlan
interface VLAN1
ip address 192.168.20.24 255.255.255.0
!
vlan 1-2
radius-server host 192.168.20.2 auth-port 1812 acct-port 1813
radius-server key TST
```

Configuration of interface f0/2

```
interface GigaEthernet 0/2
 dot1x port-control auto
 dot1x authentication method TST-G0/2
 dot1x user-permit radius-TST
 dot1x accounting enable
 dot1x accounting method dot1x_acc
```

Configuration of interface f0/3

```
Interface GigaEthernet 0/3
 dot1x authentication multiple-hosts
 dot1x port-control auto
 dot1x authentication method TST-G0/3
 dot1x guest-vlan 2
```

Configuration of interface f0/4

```
interface GigaEthernet 0/4
 dot1x mab
 dot1x authentication method TST-G0/4
```

VLAN Configuration

1.1 VLAN Introduction....1
1.2 Dot1Q Tunnel Overview....1
1.2.1 Preface....1
1.2.2 Dot1Q Tunnel Realization Mode....2
1.2.3 Modifying Attributes Through TPID Value....2
1.3 VLANConfiguration Task List....3
1.4 VLAN Configuration Task....3
1.4.1 Adding/Deleting VLAN....3
1.4.2 Configuring the Port of the Switch....3
1.4.3 Creating/deleting the VLAN interface....4
1.4.4 Configuring the Super VLAN Interface....5
1.4.5 Monitoring the VLAN Configuration and VLAN State....5
1.4.6 Enabling or disabling Dot1 Q Tunnel globally and configuring TPID globally....6
1.4.7 enable/disable globalflat-translation....6
1.4.8 Configuring VLAN translation mode and items on a port....6
1.4.9 Setting MAC-Based VLAN....7
1.4.10 Setting IP Subnet-Based VLAN....7
1.4.11 Setting Protocol-Based VLAN....8
1.5 Configuration Example....9
1.5.1 SuperVLAN Configuration Example....9
1.5.2 Dot1Q Tunnel Configuration Examples....9
Appendix A Abbreviations....14

1.1 VLAN Introduction

The virtual local area network (VLAN) is an exchange network which logically groups the devices in LAN. IEEE issued the IEEE 802.1Q standard in 1999 for realizing the VLAN standard. The VLAN technology can divide a physical LAN logic address into different broadcast domains. Each VLAN has a group of devices which have the same demands but the same attributes with those on the physical LAN. Because it is a logical group, the devices in a same VLAN can be in different physical spaces. The broadcast/unicast flow within a VLAN cannot be forwarded to other VLANs. Such advantages as flow control, low device investment, easy network management and high network security, hence, are obtained.

- Support port-based VLAN
- Support 802.1Q relay mode
- Support the access port

  The port-based VLAN is to classify the port into a subset of VLAN supported by the switch. If the VLAN subnet includes only one VLAN, the port is the access port; if the VLAN subnet has multiple VLANs, the port is a trunk port; there is a default VLAN among these VLANs, which is the native VLAN of the port and whose ID is PVID.
- Support VLAN range control

  The vlan-allowed parameter is used to control theVLANrange; the vlan-untagged parameter is used to control the transmission of the untaggedVLANpacket from the port to the correspondingVLAN.

VLAN planning modes are various such as based on MAC, IP subnet, protocol, or port. As to these VLAN planning modes, VLAN matchup is conducted by default according to the following order: MAC VLAN, IP-subnet VLAN, protocol VLAN and at last, port VLAN.

1.2 Dot1Q Tunnel Overview

1.2.1 Preface

Dot1Q Tunnel is a lively name of the tunnel protocol based on 802.1Q encapsulation, which is defined in IEEE 802.1ad. Its core idea is to encapsulate the VLAN tag of the private network to that of the public network, and the packets with two layers of tags traverse the backbone network of ISP and finally a relatively simple L2 VPN tunnel is provided to users. The Dot1Q Tunnel protocol is a simple and manageable protocol, which is realized through static configuration without signaling support and widely applied to enterprise networks consisting of L3 switches or small-scale MAN.

The Dot1Q Tunnel attribute of switches just meets this requirement. As a cheap and compact L2 VPN solution, it is increasingly popular among more and more small-scale users when VPN network is required. At the inside of carrier's network, P device need not support the Dot1Q Tunnel function. That is, traditional L3 switches can meet the requirements fully and protect the investment of the carrier greatly.

- Enables Dot1Q Tunnel globally.
- Supports the inter-translation between customer VLAN and SPVLAN on the downlink port, including translation in Flat mode and in QinQ mode.
- Supports the configuration of the uplink port.
- Supports changeable TPID.

There are two modes to realize Dot1Q Tunnel: port-based Dot1Q Tunnel and Dot1Q Tunnel based on inner CVLAN tag classification.

1) Port-based Dot1Q Tunnel:

When a port of this device receives packets, no matter whether packets have the VLAN tag, the switch will add the VLAN tag of the default VLAN on this port to these packets. Thus, if a received packet has a VLAN tag, the packet become a packet with double tags; if a received packet is untagged, this packet will be added a default VLAN tag of this port.

The packet with a single VLAN tag has the following structure, as shown in table 1:

DA (6B)	SA (6B)	ETYPE(8100) (2B)	VLAN TAG (2B)	ETYPE (2B)	DATA (0~1500B)	FCS (4B)

Table 1 Packet with a single VLAN tag

The packet with double VLAN tags has the following structure, as shown in table 2:

DA (6B)	SA (6B)	**ETYPE(8100) (2B)**	**SPVLAN Tag (2B)**	ETYPE (8100) (2B)	CVLAN Tag (2B)	ETYPE (2B)	DATA (0~1500B)	FCS (4B)

Table 2 Packet with double VLAN tags

2) Dot1Q Tunnel based on the inner CVLAN Tag:

The service is distributed according to the CVLAN ID zone of the inner CVLAN tag of Dot1Q Tunnel. The CVLAN zone can be translated into SPVLAN ID and there are two translation modes: Flat VLAN translation and QinQ VLAN translation. In QinQ VLAN translation mode, when a same user uses different services by using different CVLAN IDs, the services can be distributed according to CVLAN ID. For example, the CVLAN ID of bandwidth service ranges between 101 and 200; the CVLAN ID of VOIP service ranges between 201~300; and the CVLAN ID of IPTV service ranges between 301~400. When PE device receives the user data, set SPVLAN Tag with ID as 1000 for the bandwidth service; set SPVLAN Tag with ID as 2000 for the VOIP service; set SPVLAN Tag with ID as 3000 for IPTV. The difference of the Flat VLAN translation mode and the QinQ VLAN translation mode is that in the flat VLAN translation mode the SPVLAN tag is not on the out-layer of the CVLAN tag, but replaces the CVLAN tag directly.

1.2.3 Modifying Attributes Through TPID Value

The structure of the Tag packet of Ethernet frame that is defined by the IEEE 802.1Q protocol is shown below:

TPID	User Priority	CFI	VLAN ID
2 byte	3 bit	1 bit	12 bit

Figure 3 Structure of the VLAN Tag of Ethernet frame

TPID is a field in VLAN Tag and the value of this field regulated by IEEE 802.1Q is 0x8100.switches adopt the default TPID value, that is, 0x8100. Some manufacturers do not set the TPID of the outside tag of the Dot1Q Tunnel packets in their devices to 0x8100. In order to be compatible with these devices, most switches provide the function to modify the TPID value of the Dot1Q Tunnel packets. The TPID value of the PE device can be configured by users. After the ports of these devices receive packets, the TPID value of the outside VLAN tag of these packets will be replaced with user-defined value and then these packets will be

other manufacturer after they are forwarded into the public network.

1.3 VLANConfiguration Task List

- Adding/Deleting VLAN
- Configuring the Port of the Switch
- Creating/deleting the VLAN interface
- Configuring the superVLAN interface
- Monitoring the VLAN Configuration and VLAN State
- Configuring the VLAN-based access control model
- Enabling or Disabling Dot1Q Tunnel Globally
- Configuring VLAN translation mode and items on a port
- Setting MAC-Based VLAN
- Setting IP Subnet-Based VLAN
- Setting Protocol-Based VLAN

1.4 VLAN Configuration Task

1.4.1 Adding/Deleting VLAN

VLAN is grouped according to different functions, project groups or different applications, not based on the physical locations of these users. VLAN has the similar attributes as the physical LAN, but can group terminals in different physical LANs into a same VLAN. One VLAN can have multiple ports, while all unicast/broadcast/multicast packets can be forwarded or diffused to the terminals through a same VLAN. Each VLAN is a logical network; to forward one packet to another VLAN, the routes or bridge must be used to forward it.

Run the following commands to configure VLAN:

Command	Purpose
vlan *vlan-id*	Enters theVLANconfiguration mode.
name *str*	Name in theVLANconfiguration mode
Exit	Exits theVLANconfiguration mode and creates theVLAN.
vlan *vlan-range*	Creates multiple VLANs simultaneously.
no vlan *vlan-id* | *vlan-range*	Deletes one or multiple VLANs.

You can use the GVRP protocol to dynamically add or delete the VLAN.

1.4.2 Configuring the Port of the Switch

The switch's port supports the following modes: the access mode, the relay mode, the VLAN tunnel mode, the VLAN translating tunnel mode and the VLAN tunnel uplink mode.

- The access mode indicates that the port belongs to just one VLAN; only the untagged Ethernet frame can be transmitted and received.

Ethernet frame can be transmitted and received.

- The VLAN translating tunnel mode is a sub mode based on the relay mode. The port looks up the VLAN translation table according to the VLAN tag of received packets to obtain corresponding SPVLAN, and then the switching chip replaces the original tag with SPVLAN or adds the SPVLAN tag to the outside layer of the original tag. When the packets is forwarded out of the port, the SPVLAN will be replaced by the original tag or the SPVLAN tag will be removed mandatorily. Hence, the switch omits different VLAN partitions that access the network, and then passes them without change to the other subnet that connects the other port of the same client, realizing transparent transmission.
- The VLAN tunnel uplink mode is a sub mode based on the relay mode. The SPVLAN should be set when packets are forwarded out of the port. When the packets are received by the port, their TPIDs will be checked. If difference occurs or they are untagged packets, the SPVLAN tag which contains their own TPID will be added to them as their outer-layer tag.When the packets are received by the port, their TPIDs will be checked. If difference occurs or they are untagged packets, the SPVLAN tag which contains their own TPID will be added to them as their outer-layer tag.

Each port has a default VLAN and PVID; all VLAN-untagged data received on the port belongs to the packets of the VLAN.

The relay mode can group the port to multiple VLANs; at the same time, you can configure the type of to-be-forwarded packets and the quantity of the corresponding VLANs.

Run the following commands to configure the switch's port:

Command	Purpose
switchport pvid *vlan-id*	Configures PVID of the switch's interface.
switchport mode {access | trunk | dot1q-translating-tunnel | dot1q-tunnel-uplink *tpid* **}**	Configures the interface mode of the switch.
switchport trunk vlan-allowed …	Configures the VLAN range of the switch's interface.
switchport trunk vlan-untagged …	Configures the untagged VLAN ranges of the switch's port.
swithport flat-translation	To enable flat mode N:1 flat translation function.

1.4.3 Creating/deleting the VLAN interface

To realize network management or layer-3 routing, you need create a VLAN interface which can be used for designating the IP address and mask of the interface. Run the following command to configure the VLAN interface.

Command	Purpose
[no] interface vlan *vlan-id*	Creates or deletes a VLAN interface.

The Super Vlan technology provides the following mechanism: hosts that are in different VLANs but connect the same switch can be distributed to the same IPv4 subnet to use the same default gateway, and therefore lots of IP addresses are saved. The SuperVLAN technology classifies many different VLANs into a group, in which these VLANs use a same management interface and the hosts use a same IPv4 network segment and a same gateway. The VLANs belonging to a SuperVLAN are called SubVLANs, any of which cannot possess a management interface through IP configuration.

A SuperVLAN interface can be configured through the command line; the SuperVLAN interface is configured as follows:

Command	Usage Guidelines
[no] interface supervlan *index*	Enters the configuration mode of the SuperVLAN interface. If the designated SuperVLAN interface does not exist, the system will create the SuperVLAN interface. The “index” parameter means the index of the SuperVLAN interface, whose valid value ranges from 1 to 32. The “no” parameter means to delete the SuperVLAN interface.
[**no**] **subvlan** [*setstr*] [**add** *addstr*] [**remove** *remstr*] **[none]**	Configures the SubVlan of the SuperVLAN. The added SubVLAN does not possess a management interface or belong to other SuperVLAN. In initial state SuperVLAN does not contain any SubVLAN. Each time only one subcommand can be used. The “setstr” parameter means to set the SubVLAN list. For example, list 2, 4-6 means VLAN2, VLAN4, VLAN5 and VLAN6. The “add” parameter means to add VLAN lists in the previous SubVLAN; the “addstr” parameter means the list string, whose format is the same above. The “remove” parameter means to delete VLAN lists from the previous SubVLAN list; the “remstr” parameter means the list string, whose format is the same above. The “no” parameter means to delete all SubVLANs of a SuperVLAN. The “no” subcommand cannot be used together with other subcommands.

After a SuperVLAN interface is configured, you can configure an IP address for the SuperVLAN interface; the SuperVLAN interface is also a routing port and any configuration for a port can be configured on this routing port.

1.4.5 Monitoring the VLAN Configuration and VLAN State

To monitor the configuration and state of VLAN and Dot1Q tunnel, run the following commands in EXEC mode:

Command	Purpose
show vlan [id *x* **| interface** *intf* **| dot1q-tunnel [interface** *intf***] | mac-vlan | subnet | protocol-vlan]**	Displays the configuration and state of VLAN or Dot1Q tunnel.

show interface {vlan | supervlan} *x*	Displays the state of the VLAN interface or that of the SuperVLAN interface.

1.4.6 Enabling or disabling Dot1 Q Tunnel globally and configuring TPID globally

After Qot1Q Tunnel is globally enabled, all ports serve as the downlink ports of Qot1Q Tunnel by default and put the SPVLAN tag on the incoming packets.

The command to enable dot1q-tunnel globally:

Command	Purpose
dot1q-tunnel	The command is used to configure dot1q-tunnel globally.

1.4.7 enable/disable globalflat-translation

To enable flat-translation globally, the command is

Command	Purpose
[no] flat-translation-global	To enable or disable global flat mode N:1 flat translation function, run previous commands.

1.4.8 Configuring VLAN translation mode and items on a port

Both the VLAN translating mode and the VLAN translating items validate in dot1q-translating-tunnel mode after they are configured. The translation modes fall into two kinds: the Flat mode and the QinQ mode. In Flat mode, the CLAN tag of packets which are received by the dot1q-translating-tunnel downlink port will be used as an index to look up the VLAN translating list. The CVLAN will be replaced by detected SPVLANs; when the packets are forwarded out of the port, the SPVLAN will then be replaced by CVLAN. In QinQ mode, the CLAN tag of packets which are received by the dot1q-translating-tunnel downlink port will be used as an index to look up the VLAN translating list and then the detected SPVLANs will form into SPVLAN tag to be added to the outside of CVLAN tag; when the packets are forwarded out of the port, the SPVLAN tag will then be removed.

When the VLAN translating items are configured on a port, the mapping between CVLAN and multiple SPVLANs can be configured in QinQ mode. To configure the mapping between CVLAN and multiple SPVLANs in flat mode, you have to configure QoS and then the correct transformation from SPVLAN to CVLAN can be conducted when packets are transmitted out from this port.

The command to configure the VLAN translation mode and translation items is shown in the following table:

Command	Purpose
switchport dot1q-translating-tunnel mode {flat | qinq} translate {*oldvlanid* **|** *oldvlanlist***}** *newvlan* **[***priority***]**	Configures the VLAN translation mode and translation item.

The MAC-based VLAN is a VLAN planning mode based on the source MAC address of the packet. When a port of a device receives an untagged packet, the device will take the source MAC address of the packet as the matchup keyword and know the home VLAN by looking for the MAC VLAN entry.

The settings of the MAC-based VLAN includes adding/deleting MAC VLAN entry and enabling/disabling the MAC VLAN function on the port.

In global configuration mode run the following commands to add or delete the MAC VLAN entry.

Command	Purpose
mac-vlan mac-address *mac-addr* **vlan** *vlan-id priority*	Adds a MAC VLAN entry.
no mac-vlan mac-address *mac-addr*	Deletes a MAC VLAN entry.

The MAC-based VLAN function takes effect only on a port on which this function is enabled. In port configuration mode, run the following commands respectively to enable or disable the MAC VLAN function on a port.

Command	Purpose
[no] switchport mac-vlan	To enable or disable the MAC-based VLAN function, run the above-mentioned commands respectively.

Note: In port access mode, an incoming packet will be dropped if its VLAN, which is obtained through the matchup of MAC VLAN entry, is not the PVID of the port. Hence, if not necessary, do not set the port mode, which is to enable MAC VLAN, to access.

1.4.10 Setting IP Subnet-Based VLAN

IP subnet-based VLAN is a VLAN planning mode based on the source IP address and configured subnet mask of a packet. When a device receives an untagged packet on one of its ports, the device will locate the VLAN of this packet according to the source IP address of the packet and the configured subnet mask.

The settings of the IP-subnet VLAN includes adding/deleting the subnet VLAN entry and enabling/disabling the subnet VLAN function on the port.

In global configuration mode run the following commands to add or delete the subnet VLAN entry.

Command	Purpose
[no] subnet { any | *ip-addr mask* **}**	Adds or deletes a subnet VLAN entry.

The IP-subnet VLAN function takes effect only on a port on which this function is enabled. In port configuration mode, run the following commands respectively to enable or disable the MAC VLAN function on a port.

Command	Purpose
[no] switchport vlan-subnet enable	To enable or disable the IP-subnet VLAN function on the ports, run the above-mentioned commands respectively.

Note: In port access mode, an incoming packet will be dropped if its VLAN, which is obtained through the matchup of MAC VLAN entry, is not the PVID of the port. Hence, if not necessary, do not set the port mode, which is to enable subnet VLAN, to access.

1.4.11 Setting Protocol-Based VLAN

The protocol-based VLAN is a VLAN planning mode which is based on the protocol to which the received packet belongs. When a switch receives an untagged packet on one of its ports, the switch will determine the VLAN of the packet according to the protocol of this packet.

The way the switch determines the type of the protocol that the packet belongs to is based on the encapsulation type and the value of the special field.

Adding/deleting a protocol template globally and adding/deleting the association of a protocol template on a port

- Adding/deleting a protocol template globally and adding/deleting the association of a protocol template on a port

In global configuration mode, run the following commands to add or delete a protocol template.

Command	Purpose
protocol-vlan *protocol_index* **frame-type { ETHERII | SNAP | LLC } ether-type** *etype-id*	Adds a protocol template.
no protocol-vlan *protocol_index*	Deletes a protocol template.

Note: When the frame-type parameter is LLC, the high and low bytes in the Ether-Type field correspond to DSAP and SSAP in a packet respectively.

A protocol template only takes effect on a port where the protocol template is applied. The same protocol template can correspond to different VLANs on different ports. In port configuration mode, run the following commands to add or delete the association of a protocol template.

Command	Purpose
switchport protocol-vlan *protocol_index* **vlan** *vlan-id*	Adds the association of a protocol template.
no switchport protocol-vlan *protocol_index*	Deletes the association of a protocol template.

1.5.1 SuperVLAN Configuration Example

The network topology is shown in the following figure:

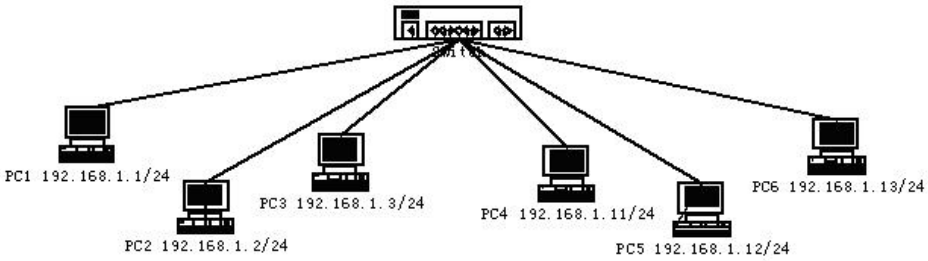


Figure 9 SuperVLAN

Six PC users from PC1 to PC6 connect six ports of a switch respectively. The IP addresses of these PCs belong to the 192.168.1.0/24 network segment. These PCs can ping each other successfully and the switch can be controlled through the IP address, 192.168.1.100, but group PC1-PC3 and group PC4-PC6 are in different layer-2 broadcast domains respectively. In this case, ports 1, 2 and 3 can be configured to be in VLAN1 and ports 4, 5 and 6 to be in VLAN2, and then vlan1 and vlan2 can be added as a SubVLAN of a same SuperVLAN. To do these, you need do the following configurations:

```
interface fastethernet 0/4
switchport pvid 2
!
interface fastethernet 0/5
switchport pvid 2
!
interface fastethernet 0/6
switchport pvid 2
!
interface supervlan 1
subvlan 1,2
ip address 192.168.1.100 255.255.255.0
ip proxy-arp subvlan
!
```

1.5.2 Dot1Q Tunnel Configuration Examples

The following typical solutions show how to apply Dot1Q tunnel.

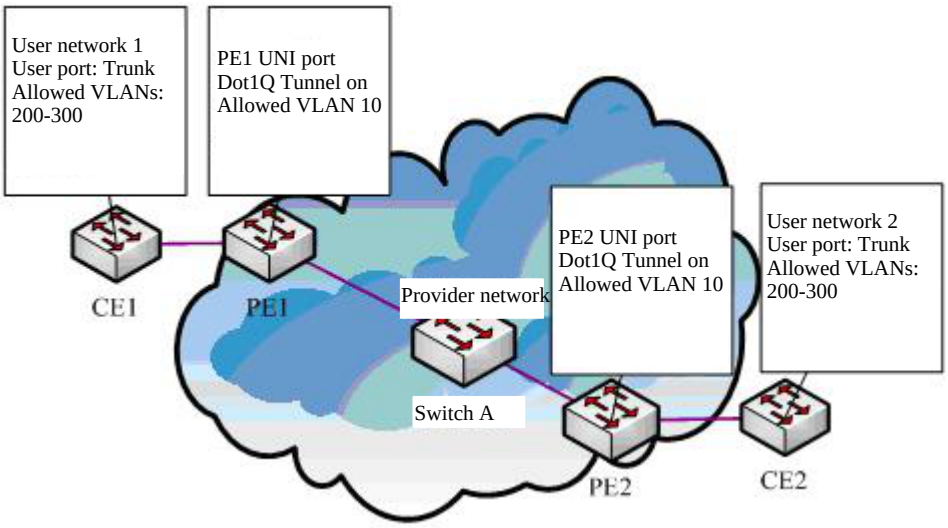


Figure 4 Typical configuration of Dot1Q tunnel

As shown in the figure above, port F0/1 of CE1 connects port F0/1 (or port G0/1) of PE1, PE1 connects Switch A on port F0/2 (or port G0/2), PE2 connects Switch A on port F0/2 (or port G0/2), and port F0/1 (or port G0/1) of PE2 connects port F0/1 of CE1.

Port G0/1 of PE is set to be the access port of VLAN 10 and on them Dot1Q Tunnel is enabled. However, the ports of CE still need Trunk VLAN 200-300, enabling the link between CE and PE to be an asymmetrical link. In this case, the public network only needs to distribute users a VLAN ID, 10. No matter how many VLAN IDs of private network are planned in the user's network, the newly distributed VLAN ID of the public network will be mandatorily inserted into the tagged packets when these packets enter the backbone network of ISP. These packets then pass through the backbone network through the VLAN ID of the public network, reach the other side of the backbone network, that is, the PE devices, get rid of the VLAN tag of the public network, resume the user's packets and at last are transmitted to the CE devices of the users. Therefore, the packets that are forwarded in the backbone network have two layers of 802.1Q tag headers, one being the tag of the public network and the other being the tag of the private network. The detailed flow of packet forwarding is shown as follows:

1) Because the egress port of CE1 is a Trunk port, all the packets that are transmitted by users to PE1 have carried the VLAN tag of the private network (ranging from 200 to 300). One of these packets is shown in figure 5.

DA (6B)	SA (6B)	ETYPE(8100) (2B)	VLAN TAG (2B)	ETYPE (2B)	DATA (0~1500B)	FCS (4B)

Figure 5 Structure of a packet from CE1

2) After the packets enter PE1, PE1, for the ingress port is the access port of Dot1Q tunnel, ignores the VLAN tag of the private network but inserts the default VLAN 10's tag into these packets, as shown in figure 6.

DA (6B)	SA (6B)	ETYPE(8100) (2B)	SPVLAN Tag (2B)	ETYPE (8100) (2B)	CVLAN Tag (2B)	ETYPE (2B)	DATA (0~1500B)	FCS (4B)

Figure 6 Structure of a packet going into PE1

The tag of the private network is kept in transparent state until these packets reach PE2.

4) PE2 discovers that the port where it connects CE2 is the access port of VLAN 10, removes the tag header of VLAN 10 according to 802.1Q, resumes the initial packets of users, and transmit the initial packets to CE2, as shown in figure 7.

DA (6B)	SA (6B)	ETYPE(8100) (2B)	VLAN TAG (2B)	ETYPE (2B)	DATA (0~1500B)	FCS (4B)

Figure 7 Structure of a packet from PE2

Seen from the forwarding flow, Dot1Q Tunnel is very concise for the signaling is not required to maintain the establishment of the tunnel, which can be realized through static configuration.

As to the typical configuration figure of Dot1Q Tunnel, products of different models are configured as follows when they run as PE (PE1 configuration is same to PE2).

1) Dot1Q Tunnel Configuration of the switch

Switch_config#dot1q-tunnel

Switch_config_g0/1#switchport pvid 10

Switch_config_g0/2#switchport mode trunk

Switch_config_g0/2#switchport trunk vlan-untagged 1-9,11-4094

2. Example 2

If different services of a same user are dealt with and the access terminal of a user connects the UNI port of PE, the Dot1Q tunnel VLAN translation must be used to differentiate different services and carry different QoS standards.

As shown in figure 8, the carrier distributes three VLANs for each user and each VLAN corresponds to a kind of service. For example, user 1 is distributed with 3 VLANs, that is, VLAN 1001, VLAN 2001 and VLAN 3001, among which VLAN 1001 is for broadband services, VLAN 2001 is for VoIP services and VLAN 3001 is for IPTV services. When a service reaches the UNI port of the PE switch, an out-layer label will be added to the service according to its VLAN ID (different services are added with different outer-layer labels). If the out-layer label of the user data is 1001, the user data will be added with label 1001 directly on its outer layer. As to user 2, different services can be distributed with different VLAN tags. The outer-layer tag of user 2 is different from that of user 1 mainly for differentiating the location of CE and also locating users.

Device	Service	Inner-layer CVLAN tag	Outer-layer SPVLAN tag	Flow classification principle
CE1	broadband	101-200	1001	CVLAN domain
	VOIP	201-300	2001	
	IPTV	301-400	3001	
CE2	broadband	101-200	1002	
	VOIP	201-300	2002	

	IPTV	301-400	3002	

In this networking solution, the two layers of tags differentiate services very well and locate users. The outer-layer tag identifies the location of CE and a service, while the inner-layer tag identifies the location of a user.

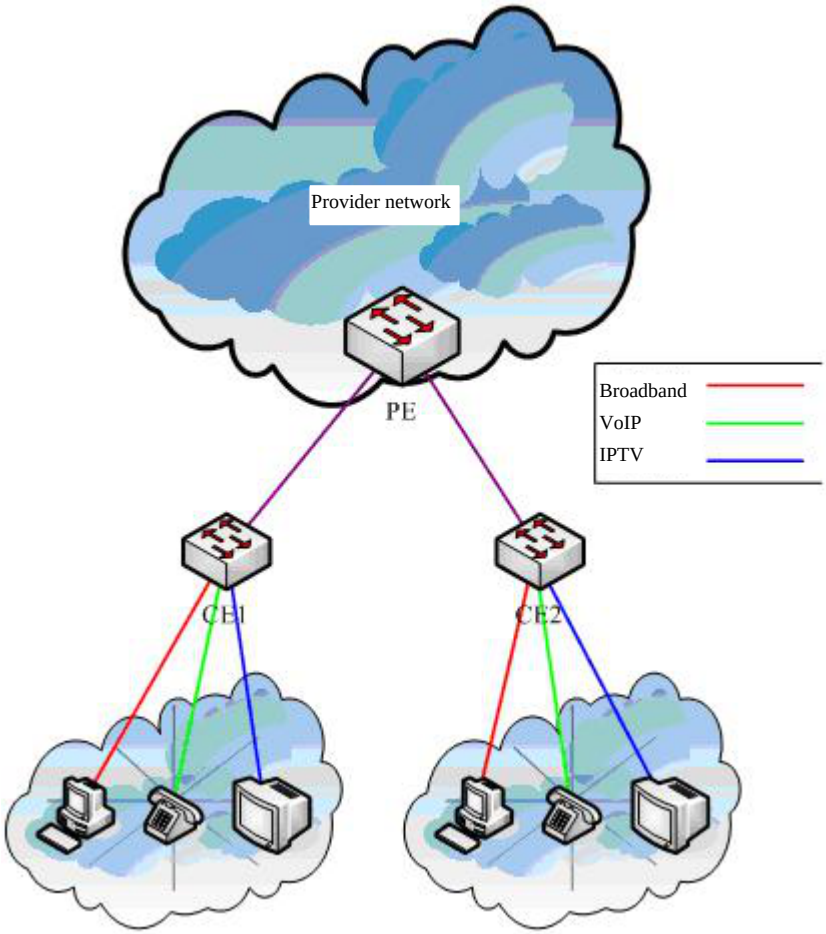


Figure 8 Typical configuration of Dot1Q tunnel (3)

In figure 9, CE1 connects port G0/1 of PE1, CE2 connects port G0/2 of PE1 and the Dot1Q Tunnel NNI port of PE is port G0/3. Configuring the command as follows:

1) Dot1Q Tunnel Configuration of the switch

Switch_config#dot1q-tunnel

Switch_config#vlan 1-4094

Switch_config_g0/1#interface g0/1

Switch_config_g0/1#switchport mode dot1q-translating-tunnel

Switch_config_g0/1#switchport dot1q-translating-tunnel mode QinQ translate 101-200 1001

Switch_config_g0/1#switchport dot1q-translating-tunnel mode QinQ translate 201-300 2001

Switch_config_g0/1#switchport dot1q-translating-tunnel mode QinQ translate 301-400 3001

Switch_config_g0/1#interface g0/2

Switch_config_g0/2#switchport mode dot1q-translating-tunnel

1002

Switch_config_g0/2#switchport dot1q-translating-tunnel mode QinQ translate 201-300 2002

Switch_config_g0/2#switchport dot1q-translating-tunnel mode QinQ translate 301-400 3002

Switch_config_g0/1#interface g0/3

Switch_config_g0/3#switchport mode dot1q-tunnel-uplink

Appendix A Abbreviations

Abbrev.	Full Name	Chinese Name
VPN	Virtual Private Network	Virtual Private Network
TPID	Tag Protocol Identifier	Tag Protocol Identifier
QoS	Quality of Service	QoS
P	provider bridged network core	provider bridged network core
PE	provider bridged network edge	provider bridged network edge
CE	customer network edge	customer network edge
UNI	user-network interface	user-network interface
NNI	network-network interface	network-network interface
CVLAN	Customer VLAN	Customer VLAN
SPVLAN	Service provider VLAN	Service provider VLAN

GVRP Configuration

Table of Contents

Chapter 1 Configuring GVRP 1
1.1 Introduction 1
1.2 Configuring Task List 1
1.2.1 GVRP Configuration Task List 1
1.3 GVRP Configuration Task 1
1.3.1 Enabling/Disabling GVRP Globally 1
1.3.2 Dynamic VLAN to Validate only on a Registered Port 1
1.3.3 Enabling/Disabling GVRP on the Interface 2
1.3.4 Monitoring and Maintenance of GVRP 2
1.4 Configuration Example 2

Chapter 1 Configuring GVRP

1.1 Introduction

GVRP (GARP VLAN Registration Protocol GARP VLAN) is a GARP (GARP VLAN Registration Protocol GARP VLAN) application that provides IEEE 802.1Q-compliant VLAN pruning and dynamic VLAN creation on 802.1Q trunk ports.

With GVRP, the switch can exchange the VLAN configuration information with the other GVRP switches, prune the unnecessary broadcast and unknown unicast traffic, and dynamically create and manage the VLANs on the switches that are connected through the 802.1Q trunk ports.

1.2 Configuring Task List

1.2.1 GVRP Configuration Task List

- Enabling/Disabling GVRP Globally
- Enabling/Disabling GVRP on the Interface
- Monitoring and Maintenance of GVRP

1.3 GVRP Configuration Task

1.3.1 Enabling/Disabling GVRP Globally

Perform the following configuration in global configuration mode.

Command	Description
[no] gvrp	Enables/disables GVRP globally.

It is disabled by default.

1.3.2 Dynamic VLAN to Validate only on a Registered Port

Run the following commands in global configuration mode:

Command	Description
[no] gvrp dynamic-vlan-pruning	Enable/disable VLAN to validate only on a registered port.

After this function is enabled, dynamic VLAN takes effect only on the ports on which this dynamic VLAN is registered. After this command is enabled and if a port has not registered a dynamic VLAN, this port will not belong to the dynamic VLAN

through.

The function is disabled by default.

1.3.3 Enabling/Disabling GVRP on the Interface

Perform the following configuration in interface configuration mode:

Command	Description
[no] gvrp	Enables/disables interface GVRP.

In order for the port to become an active GVRP participant, you must enable GVRP globally first and the port must be an 802.1Q trunk port,

It is enabled by default.

1.3.4 Monitoring and Maintenance of GVRP

Perform the following operations in EXEC mode:

Command	Description
show gvrp statistics [**interface** port_list]	Displays GVRP statistics.
show gvrp status	Displays GVRP global state information.
[**no**] **debug gvrp** [**packet** | **event**]	Enables/disables GVRP data packet and event debug switches. All debug switches will be enabled/disabled if not specified the concrete switch.

Display GVRP statistics:

switch#show gvrp statistics interface Tthernet0/1

GVRP statistics on port Ethernet0/1

GVRP Status: Enabled

GVRP Failed Registrations: 0

GVRP Last Pdu Origin: 0000.0000.0000

GVRP Registration Type: Normal

Display GVRP global state information:

Switch#show gvrp status

GVRP is enabled

1.4 Configuration Example

The network connection is as follows. In order to make the VLAN configuration information of Switch A and Switch B identical, you can enable GVRP on Switch A and Switch B. The configuration is as follows:



1) Configure the interface 1 that Switch A connects to Switch B to trunk:

Switch_config_g0/1# switchport mode trunk

2) Enable global GVRP of switch A:

Switch_config#gvrp

3) Enable GVRP of interface 1 of Switch A:

Switch_config_g0/1#gvrp

4) Configure VLAN 10, Vlan 20 and Vlan30 on Switch A

Switch_config#vlan 10,20,30

5) Configure the interface 2 that Switch A connects to Switch B to trunk:

Switch_config_g0/2# switchport mode trunk

6) Enable global GVRP of switch B:

Switch_config#gvrp

7) Enable GVRP of interface 2 of Switch B

Switch_config_g0/2#gvrp

8) Configure VLAN 40, Vlan 50 and Vlan60 on Switch B

Switch_config#vlan 40,50,60

After completing the configuration, the VLAN configuration information will be displayed respectively on Switch A and Switch B, that is, VLAN10, VLAN20,VLAN30, VLAN40, VLAN50 and VLAN60 on both switches.

Private VLAN Settings

Table of Contents

Chapter 1 Private VLAN Settings 1
1.1 Overview of Private VLAN 1
1.2 Private VLAN Type and Port Type in Private VLAN 1
1.2.1 Having One Primary VLAN Type 1
1.2.2 Having Two Secondary VLAN Types 1
1.2.3 Port Types Under the Private VLAN Port 1
1.2.4 Modifying the Fields in VLAN TAG 2
1.3 Private VLAN Configuration Task List 2
1.4 Private VLAN Configuration Tasks 2
1.4.1 Configuring Private VLAN 2
1.4.2 Configuring the Association of Private VLAN Domains 2
1.4.3 Configuring the L2 Port of Private VLAN to Be the Host Port 3
1.4.4 Configuring the L2 Port of Private VLAN to Be the Promiscuous Port 3
1.4.5 Modifying Related Fields of Egress Packets in Private VLAN 3
1.4.6 Displaying the Configuration Information of Private VLAN 4
1.5 Configuration Example 4

Chapter 1 Private VLAN Settings

1.1 Overview of Private VLAN

Private VLAN has settled the VLAN application problems facing ISPs: If ISP provides each user with a VLAN, the support by each device of 4094 VLANs will restrict the total of ISP-supported users.

1.2 Private VLAN Type and Port Type in Private VLAN

Private VLAN subdivides the L2 broadcast domain of a VLAN into multiple sub-domains, each of which consists of a private VLAN pair: a primary VLAN and a secondary VLAN. One private VLAN domain may have multiple private VLAN pairs and each private VLAN pair stands for a sub-domain. There is only one primary VLAN in a private VLAN domain and all private VLAN pairs share the same primary VLAN. The IDs of secondary VLANs in each sub-domain differ with each other.

1.2.1 Having One Primary VLAN Type

- Primary VLAN: It is relevant to a promiscuous port and only one primary VLAN exists in the private VLAN. Each port in the primary VLAN is a member in the primary VLAN.

1.2.2 Having Two Secondary VLAN Types

- Isolated VLAN: No layer-2 communication can be conducted between two ports in the same isolated VLAN. Also, there is only one isolated VLAN in a private VLAN. The isolated VLAN must be related with the primary VLAN.
- Community VLAN: Layer-2 communication can be conducted between two ports in the same VLAN, but they have no communication with the ports in another community VLAN. One private VLAN may contain multiple community VLANs. The community VLAN must be related with the primary VLAN.

1.2.3 Port Types Under the Private VLAN Port

- Promiscuous port: it belongs to the primary VLAN. It can communicate with all other ports, including the isolated port and community port of a secondary VLAN in the same private VLAN.
- Isolated port: It is the host port in the isolated VLAN. In the same private VLAN, the isolated port is totally L2 isolated from other ports except the promiscuous port, so the flows received from the isolated port can only be forwarded to the promiscuous port.

the community ports of the same community VLAN can conduct L2 communication each other or with the promiscuous port, but not with the community ports of other VLANs and the isolated ports in the isolated VLANs.

1.2.4 Modifying the Fields in VLAN TAG

This functionality supports to modify the VLAN ID and priority in VLAN tag and decides whether the egress packets of private VLAN carry the tag or not.

1.3 Private VLAN Configuration Task List

- Configuring Private VLAN
- Configuring the association of private VLAN domains
- Configuring the L2 port of private VLAN to be the host port
- Configuring the L2 port of private VLAN to be the promiscuous port
- Modifying related fields of egress packets in private VLAN
- Displaying the configuration information of private VLAN

1.4 Private VLAN Configuration Tasks

The conditions for a private VLAN peer to take effect are listed below:
1. Having the primary VLAN
2. Having the secondary VLAN
3. Having the association between primary VLAN and secondary VLAN
4. Having the promiscuous port in primary VLAN

1.4.1 Configuring Private VLAN

Use the following commands to set VLAN to be a private VLAN.

Command	Purpose
vlan *vlan-id*	Enters the VLAN mode.
private-vlan {primary|community|isolated}	Configures the features of private VLAN.
no private-vlan {primary|community|isolated}	Deletes the features of private VLAN.
show vlan private-vlan	Displays the configuration of private VLAN.
exit	Exits from Vlan configuration mode.

1.4.2 Configuring the Association of Private VLAN Domains

Run the following commands to associate the primary VLAN and the secondary VLAN.

Command	Purpose

	Enters the primary VLAN configuration mode.
private-vlan association {*svlist* | **add** *svlist* | **remove** *svlist*}	Sets the to-be-associated secondary VLAN.
no private-vlan association	Clears all associations between the current primary VLAN and all secondary VLANs.
exit	Exits the VLAN configuration mode.

1.4.3 Configuring the L2 Port of Private VLAN to Be the Host Port

Run the following commands to set the L2 port of private VLAN to be the host port:

Command	Purpose
Interface *interface*	Enters the interface configuration mode.
switchport mode private-vlan host	Sets the layer-2 port to be in host's port mode.
no switchport mode	Deletes the private VLAN mode configuration of L2 port.
switchport private-vlan host-association *p_vid s_vid*	Associates the L2 host port with private VLAN.
no switchport private-vlan host-association	Deletes the association between L2 host port and private VLAN.
exit	Exits from the interface configuration mode.

1.4.4 Configuring the L2 Port of Private VLAN to Be the Promiscuous Port

Run the following commands to set the L2 port of private VLAN to be the promiscuous port:

Command	Purpose
Interface *interface*	Enters the interface configuration mode.
switchport mode private-vlan promiscuous	Sets the layer-2 port to be in promiscuous port mode.
no switchport mode	Deletes the private VLAN mode configuration of L2 port.
switchport private-vlan mapping *p_vid{svlist | add svlist | **remove** svlist}*	Associates the L2 promiscuous port with private VLAN.
no switchport private-vlan mapping	Deletes the association between L2 promiscuous port and private VLAN.
exit	Exits from the interface configuration mode.

1.4.5 Modifying Related Fields of Egress Packets in Private VLAN

Run the following commands to modify related fields of the egress packets in private VLAN:

Command	Purpose
Interface *interface*	Enters the interface configuration mode.
switchport private-vlan tag-pvid *vlan-id*	Sets the VLAN ID field in the tag of egress packet.
switchport private-vlan tag-pri *pri*	Sets the priority field in the tag of egress packet.
[no] switchport private-vlan untagged	Sets whether the egress packets have the tag or not.
exit	Exits from interface configuration mode.

1.4.6 Displaying the Configuration Information of Private VLAN

Run the following commands in global, interface or VLAN configuration mode to display the private VLAN configuration information of private VLAN and L2 port:

Command	Purpose
show vlan private-vlan	Displays the configuration of private VLAN.
show vlan private-vlan interface *interface*	Displays the configuration of the L2 port in the private VLAN.

1.5 Configuration Example

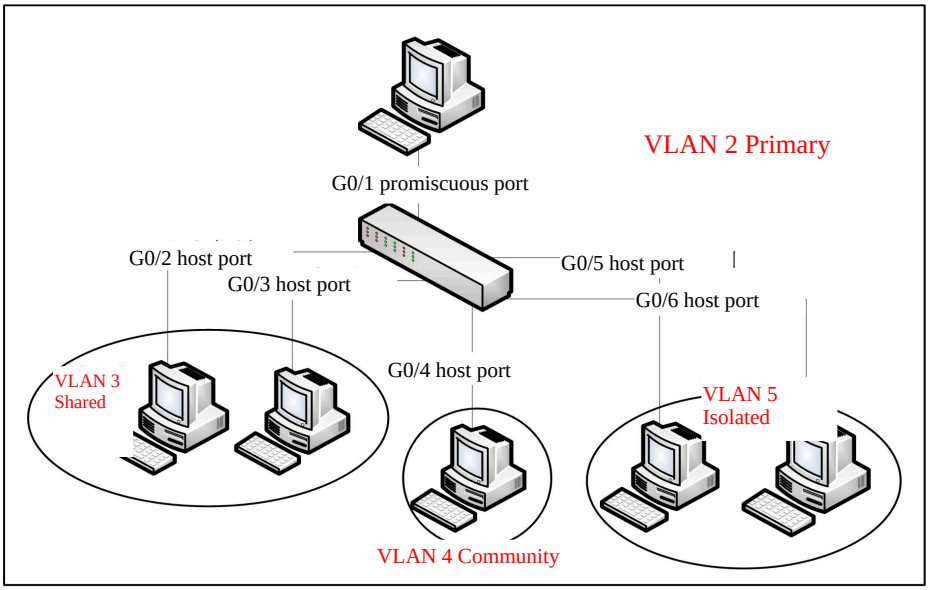


Figure 1: Typical Configuration of Private VLAN

As shown in figure 1, port G0/1 is the promiscuous port in primary VLAN 2 and ports G0/2-G0/6 are host ports, among which ports G0/2 and G0/3 are host ports (public ports) of Community VLAN 3, port G0/4 is that of Community VLAN 4, and ports G0/5 and G0/6 are host ports of Isolated VLAN 5.

promiscuous port G0/1 and host ports of all sub-VLAN domains, so it is between host ports G0/2 and G0/3 of community VLAN 3, but they cannot conduct L2 communication with other host ports of secondary VLANs. L2 communication cannot go on between ports G0/5 and G0/6 in Isolated VLAN 5, but the two ports can conduct L2 communication with promiscuous port G0/1.

The commands requiring to be entered in a switch are shown below:

```
Switch_config#interface GigaEthernet0/1
Switch_config_g0/1#switchport mode private-vlan promiscuous
Switch_config_g0/1#switchport private-vlan mapping 2 3-5
Switch_config_g0/1#switchport pvid 2

 Switch_config#interface GigaEthernet0/2
 Switch_config_g0/2#switchport mode private-vlan host
 Switch_config_g0/2#switchport private-vlan host-association 2 3
 Switch_config_g0/2#switchport pvid 3

 Switch_config#interface GigaEthernet0/3
 Switch_config_g0/3#switchport mode private-vlan host
 Switch_config_g0/3#switchport private-vlan host-association 2 3
 Switch_config_g0/3#switchport pvid 3

 Switch_config#interface GigaEthernet0/4
 Switch_config_g0/4#switchport mode private-vlan host
 Switch_config_g0/4#switchport private-vlan host-association 2 4
 Switch_config_g0/4# switchport pvid 4

 Switch_config#interface GigaEthernet0/5
 Switch_config_g0/5#switchport mode private-vlan host
 Switch_config_g0/5#switchport private-vlan host-association 2 5
 Switch_config_g0/5#switchport pvid 5

 Switch_config#interface GigaEthernet0/6
 Switch_config_g0/5#switchport mode private-vlan host
 Switch_config_g0/5#switchport private-vlan host-association 2 5
 Switch_config_g0/5#switchport pvid 5

 Switch_config#vlan 2
 Switch_config_vlan2#private-vlan primary
 Switch_config_vlan2#private-vlan association 3-5
```

```
Switch_config#vlan 3
Switch_config_vlan3#private-vlan community

Switch_config#vlan 4
Switch_config_vlan4#private-vlan community

Switch_config#vlan 5
Switch_config_vlan5#private-vlan isolated
```

```
Switch_config#show vlan private-vlan
Primary  Secondary  Type              Ports
-------  ---------  ----------------- ------------------------------------------
2        3          community         g0/1, g0/2, g0/3
2        4          community         g0/1, g0/4
2        5          isolated          g0/1, g0/5, g0/6
```

STP Configuration

Table of Contents

Chapter 1 Configuring STP....1
1.1 STP Introduction....1
1.2 SSTPConfiguration Task List....2
1.3 SSTP Configuration Tasks....2
1.3.1 Choosingthe STP Mode....2
1.3.2 Disabling/Enabling STP....2
1.3.3 Disabling/Enabling STP on a Port....3
1.3.4 Settingthe Bridge Priority....3
1.3.5 Setting the Hello Time....4
1.3.6 Setting the Max Age....4
1.3.7 Setting the Forward Delay....4
1.3.8 Setting the PortPriority....4
1.3.9 Value of the path cost of a port....5
1.3.10 Monitoring the STP state....5
1.3.11 Setting the SNMP Trap....5
1.4 Setting the Spanning Tree of VLAN....6
1.4.1 Overview....6
1.4.2 VLAN STP Configuration Tasks....6
Chapter 2 Configuring RSTP....8
2.1 RSTP Configuration Task List....8
2.2 RSTP Configuration Tasks....8
2.2.1 Enabling/disabling RSTP of the Switch....8
2.2.2 Settingthe Bridge Priority....8
2.2.3 Setting the Forward Time....9
2.2.4 Setting the Hello Time....9
2.2.5 Setting the Max Age....10
2.2.6 Value of the path cost of a port....10
2.2.7 Setting the Port Priority....10
2.2.8 Setting the Edge Port....11
2.2.9 Setting the Port Connection Type....11
2.2.10 Restarting the protocol conversion check....12
Chapter 3 Configuring MSTP....13
3.1 MSTP Introduction....13
3.1.1 Overview....13
3.1.2 MST Region....13
3.1.3 IST, CST, CIST and MSTI....13
3.1.4 Port Role....15
3.1.5 MSTP BPDU....18
3.1.6 Stable State....19
3.1.7 Hop Count....20
3.1.8 STP Compatibility....20
3.2 MSTP Configuration Task List....20
3.3 MSTP Configuration Tasks....21
3.3.1 Default MSTP Configuration....21

3.3.2 Enabling and disabling MSTP..... 22
3.3.3 Configuring MSTP region..... 22
3.3.4 Configuring network root..... 23
3.3.5 Configuring secondary root..... 24
3.3.6 Configuring Bridge Priority..... 25
3.3.7 Configuring time parameters of STP..... 25
3.3.8 Configuring network diameter..... 26
3.3.9 Configuring maximum hop count..... 27
3.3.10 Setting the Port Priority..... 27
3.3.11 Value of the path cost of a port..... 28
3.3.12 Setting the Edge Port..... 28
3.3.13 Setting the Port Connection Type..... 28
3.3.14 Activating MST-compatible mode..... 29
3.3.15 Restarting the protocol conversion check..... 30
3.3.16 Configuring role restriction of the port..... 30
3.3.17 Configuring TCN restriction of the port..... 30
3.3.18 Check MSTP information..... 31

Chapter 1 Configuring STP

1.1 STP Introduction

The standard Spanning Tree Protocol (STP) is based on the IEEE 802.1D standard. An switch stack appears as a single spanning-tree node to the rest of the network, and all stack members use the same bridge ID.

The spanning-tree algorithm and the spanning-tree protocol can set any bridge LAN to be a simply connected mobile topology. In the mobile topology, some bridge ports can forward frames, while other ports are blocked and cannot forward data. A port in blocked state can also be contained in the mobile topology. When some network device is out of effect, added or removed, the port in blocked state will enter the forwarding state.

In the spanning-tree topology, a bridge is regarded as a root or a root bridge. Each LAN segment has a bridge port to take in charge of data forwarding from this network segment to the root. This bridge port is regarded as the designated port of this LAN segment, while the bridge where the bridge port locates is regarded as the designated bridge of LAN The root is the designated bridge of each LAN segment that connects this root. In each bridge port, the port that is nearest to the root bridge is the root port of this bridge and only the root port and the designated port are in forwarding state; another kind of ports are open, but they are not root ports or designated ports but standby ports.

The following parameters decide the structure of the stabile mobile topology:

(1) Each unique bridge identifier

(2) path cost of each port

(3) ID of each bridge port

The bridge with the highest priority (the identifier value is the smallest) will be chosen as the root bridge. The ports of each bridge in the network all have root path cost, that is, the root path cost is the smallest value of the path cost sum of all ports between the root bridge and the bridge. The designated port of each LAN segment means the port that connect this LAN segment and has the smallest root path cost; if several ports have the same root path cost, their bridge identifiers will first be compared and then their port identifiers. According to this method, each LAN segment has only one designated port and each bridge has only one root port.

The spanning tree topology makes the loop inexistent in a network, guaranteeing the stability and fault recovery of the network. With the wide spread of Ethernet switch, STP plays a more and more important role. Therefore, STP is provided as a basic function of switches.

Rapid Spanning-Tree Protocol (RSTP) is an important update of 802.1D STP. When faults occur in the bridge, bridge port or LAN segment in a network, RSTP will realize the rapid convergence of the network topology. In this case, the new root port on the bridge will enter the forwarding state promptly, and at the same time the direct

acceptance between bridges can make a designated port to forward data immediately. Please refer to Chapter 2 for RSTP protocolConfiguring RSTP.

This chapter describes how to configure the standard STP of the switch.

Note:
802.1D STP and 802.1D RSTP mentioned in this text are simplified as SSTP and RSTP respectively. SSTP here is short for Single Spanning-Tree Protocol.

1.2 SSTPConfiguration Task List

- Choosing the STP Mode
- Disabling/Enabling STP
- Disabling/Enabling STP on a Port
- Setting the Bridge Priority
- Setting the Hello Time
- Setting the Max Age
- Setting the Forward Delay
- Setting the Port Priority
- Value of the path cost of a port
- Monitoring the STP state
- Setting the SNMP Trap

1.3 SSTP Configuration Tasks

1.3.1 Choosingthe STP Mode

Run the following command to set the STP mode:

Command	Purpose
spanning-tree mode {sstp | pvst | rstp | mstp}	Selects the STP mode.

1.3.2 Disabling/Enabling STP

By default, when STP is started, the running mode is RSTP; if STP is not required, you can stop it from running.

Run the following command to disable STP:

Command	Purpose

no spanning-tree	Disables STP.

Run the following commands to enable STP:

Command	Purpose
spanning-tree	Enables STP that runs in default mode—RSTP.
spanning-tree mode {**sstp** | **pvst** | **rstp** | **mstp**}	Selects a mode for the enabled STP.

1.3.3 Disabling/Enabling STP on a Port

By default, STP is running on all switch ports (physical ports and aggregation ports); if you want to disable STP, you can run the following command in port configuration mode.

Command	Purpose
no spanning-tree	Disables STP to run on the ports.

After STP is forbidden to run on a port, this port maintains a designated port and its forwarding state and stops to transmit BPDU again. However, each STP mode still has such operations as type checkup, numbering, edge information update and topology information update towards BPDU that a port receives.

Note:
When no spanning-tree is set and a port has served as a root port, alternate port, master port or backup port, the protocol information that this port receives in RSTP/MSTP mode will age immediately and transfer to be a designated port, while the protocol information that this port receives in SSTP/PVST mode will remain the original role for a certain period and then age after the timer times out.

Note:
Every STP mode supports the BPDU Guard function on the port on which no spanning-tree is set.

1.3.4 Settingthe Bridge Priority

You can choose the spanning-tree root of the network topology by changing the bridge priority of a switch.

Run the following commands to set the bridge priority of SSTP:

Command	Purpose
spanning-tree sstp priority *value*	Modifies the bridge priority of the SSTP mode.
no spanning-tree sstp priority	Resumes the SSTP bridge priority to the default value, 32768.

1.3.5 Setting the Hello Time

You can configure the hello time of the SSTP to decide the packet transmission's interval when the switch works as the root.

Run the following commands to set the SSTP hello time.

Command	Purpose
spanning-tree sstp hello-time *value*	Modifies the hello time in SSTP mode.
no spanning-tree sstp hello-time	Resumes the SSTP hello time to the default value, 2 seconds.

1.3.6 Setting the Max Age

You can configure the SSTP max age to decide the maximum lifespan of the packet when the switch works as the root.

Run the following commands to configure the SSTP max age.

Command	Purpose
spanning-tree sstp max-age *value*	Modifies the Max Age of the SSTP mode.
no spanning-tree sstp max-age	Resumes the max age to the default value, 20 seconds.

1.3.7 Setting the Forward Delay

You can configure the forward delay time of the SSTP to decide the state change interval of all switches when these switches works as the root.

Run the following commands to configure the SSTP forward delay.

Command	Purpose
spanning-tree sstp forward-time *value*	Modifies the forward time of the SSTP mode.
no spanning-tree sstp forward-time	Resumes the default forward time, 15 seconds.

1.3.8 Setting the PortPriority

When a loop generates, STP will change the states of some ports to the blocking state to cut off the loop. You can control whether to block a port by setting the port priority and the port path cost.

Run the following commands to set the port priority of SSTP:

Command	Purpose
spanning-tree port-priority *value*	Sets the port priority in all modes.
spanning-tree sstp port-priority *value*	Modifies the port priority of the SSTP mode.
no spanning-tree sstp port-priority	Resumes the port priority to the default value,

	128.

1.3.9 Value of the path cost of a port

Run the following commands to set the port path cost of SSTP.

Command	Purpose
spanning-tree cost *value*	Sets the port priority in all modes.
spanning-tree sstp cost *value*	Modifies the port path cost in SSTP mode.
no spanning-tree sstp cost	Resumes the port path cost to the default value.

1.3.10 Monitoring the STP state

To monitor STP configuration and STP's state, run the following commands in EXEC mode:

Command	Purpose
show spanning-tree	Displays the state of STP in current mode.
show spanning-tree detail	Displays the detailed information about STP in current mode.
show spanning-tree interface	Displays the information about a port in STP in current mode.

1.3.11 Setting the SNMP Trap

You can monitor the change of STP in a switch remotely from the network management software of the host by configuring the trap function of STP.

STP protocols support two types of traps: newRoot and topologyChange. When a switch changes from a non-root to a root, the newRoot Trap message will be transmitted; when the topology change is detected, such as a non-edge port is changed from the non-forwarding state to the forwarding state, the topologyChange Trap message will be transmitted.

Note:
The STP trap can be received only when the network management software supports trap reception. The network management need be imported into the bridge MIB and OID is 1.3.6.1.2.1.17.

Run the following commands in global configuration mode to enable the STP trap:

Command	Purpose
spanning-tree management trap **[newroot | topologychange]**	Enables the STP trap. If the trap type is not designated, two kinds of traps will be enabled at the same time.
no spanning-tree management trap	Disables the STP trap.

1.4 Setting the Spanning Tree of VLAN

1.4.1 Overview

In SSTP mode, the whole network only has one spanning-tree instance, and the state of a port in the spanning tree decides its state in all VLANs. When multiple VLANs exist in a network, the isolation between SSTP and VLAN topology may lead to the communication block of some network parts.

The switch supports that independent SSTP runs on a certain number of VLANs and guarantees that a port has different states in different VLANs. At the same time the flow balance can be realized between VLANs.

It should be noted that the VLAN number which can independently running STP protocol depends on the actual version. Othter VLAN topology exceeding the number limit will not affected by STP.

1.4.2 VLAN STP Configuration Tasks

Run the following commands to set the features of SSTP in VLAN:

Command	Purpose
spanning-tree mode pvst	Enables STP distribution according to VLAN.
spanning-tree vlan *vlan-list*	Distributes the STP instance for a designated VLAN. vlan-list means the VLAN list (similarly hereinafter).
no spanning-tree vlan *vlan-list*	Deletes the spanning-tree instance in a designated VLAN
spanning-tree vlan *vlan-list* **priority** *value*	Sets the spanning-tree priority in a designated VLAN.
no spanning-tree *vlan-list* **priority**	Resumes the spanning-tree priority in a VLAN to the default value.
spanning-tree vlan *vlan-list* **forward-time** *value*	Sets the Forward Delay of a designated VLAN.
no spanning-tree vlan *vlan-list* **forward-time**	Resumes the Forward Delay of a designated VLAN.
spanning-tree vlan *vlan-list* **max-age** *value*	Sets the max age of a designated VLAN.
no spanning-tree vlan *vlan-list* **max-age**	Resumes the Max-Age of a designated VLAN to the default value.
spanning-tree vlan *vlan-list* **hello-time** *value*	Sets the Hello-time of a designated VLAN.
no spanning-tree vlan *vlan-list* **hello-time**	Resumes the hello-time of a designated VLAN to the default value.

Run the following commands to set the port's features in switch port configuration mode:

Command	Purpose
spanning-tree vlan *vlan-list* **cost**	Sets the path cost of a port in a designated VLAN.
no spanning-tree vlan *vlan-list* **cost**	Resumes the path cost of a port in VLAN to the default value.
spanning-tree vlan *vlan-list* **port-priority**	Sets the port priority in VLAN.
no spanning-tree vlan *vlan-list* **port-priority**	Resumes the priority of a port in VLAN to the default value.

In monitor or configuration mode, run the following commands to browse the state of the spanning tree in a designated VLAN:

Command	Purpose
show spanning-tree vlan *vlan-list*	Browses the state of the spanning tree in a VLAN.
show spanning-tree pvst instance-list	To check the corresponding relation between PVST instances and VLAN, run this command.

Chapter 2 Configuring RSTP

2.1 RSTP Configuration Task List

- Enabling/disabling RSTP of the Switch
- Setting the Bridge Priority
- Setting the Forward Time
- Setting the Hello Time
- Setting the Max Age
- Value of the path cost of a port
- Setting the Port Priority
- Setting the Edge Port
- Setting the Port Connection Type
- Restarting the protocol conversion check

2.2 RSTP Configuration Tasks

2.2.1 Enabling/disabling RSTP of the Switch

Run the following commands in global configuration mode.

Command	Purpose
spanning-tree mode rstp	Enables RSTP.
no spanning-tree mode	`Disables stp funciton.`

2.2.2 Settingthe Bridge Priority

The bridge priority decides whether this bridge can be chosen as the root bridge of the whole spanning tree. Setting a comparatively low priority can make a bridge to be the root bridge of the spanning tree.

Run the following commands in global configuration mode.

Command	Purpose
spanning-tree rstp priority *value*	Sets the priority of a bridge.
no spanning-tree rstp priority	Resumes the bridge priority to be the default

	value.

Note that if the priorities of all bridges in a switched network have the same value the bridge with the smallest MAC address will be chosen as the root bridge. In case that RSTP is enabled, if the bridge priority is changed the spanning tree will be calculated again.

In the default settings, the bridge priority is set to 32768.

2.2.3 Setting the Forward Time

Link fault will trigger the recalculation of the spanning-tree structure, but the new configuration information, which is obtained through recalculation, cannot be sent to the whole network immediately; if the newly chosen root port and designated port starts data forwarding immediately, temporary loop may be caused. To solve this problem, RSTP adopts a state removal mechanism. Before the root port and the designated port begin to forward data, an intermediate state must be experienced. The intermediate state changes into the forwarding state after the forward delay that guarantees the new configuration information has spread all over the whole network. The Forward Delay of a bridge depends on the diameter of the switch network. Generally speaking, the longer the network diameter is, the longer the forward delay should be set to be.

Run the following commands in global configuration mode.

Command	Purpose
spanning-tree rstp forward-time *value*	Sets the Forward Delay.
no spanning-tree rstp forward-time	Resumes the default forward delay, 15 seconds.

It is especially noted that if Forward Delay is set too small the temporary redundant path may occur in the network, but if Forward Delay is set too big the network may be disconnected for a long time. That's why users are recommended to take the default value.

In the default settings, the forward delay of a bridge is 15 seconds.

2.2.4 Setting the Hello Time

A suitable hello time not only guarantees that a bridge can detect a link fault in a network promptly but also occupies a few network resources.

Run the following commands in global configuration mode.

Command	Purpose
spanning-tree rstp hello-time *value*	Sets the Hello Time.
no spanning-tree rstp hello-time	Resumes the hello time to the default value.

It takes attention that if a long hello time is set, packet loss in the links may cause a bridge not to receive the hello packets for a long time and the bridge then regards the occurrence of link faults and starts spanning-tree recalculation, but if a too short hello time is set the bridge will frequently send the configuration information and then the network bandwidth will be heavily occupied and the network/CPU load will be increased. That's why users are recommended to take the default value.

In the default settings, the hello time of a bridge is 2 seconds.

2.2.5 Setting the Max Age

The max age is used to judge whether the configuration information expires. Users can set the max age according actual conditions.

Run the following commands in global configuration mode.

Command	Purpose
spanning-tree rstp max-age *value*	Setting the Max Age
no spanning-tree rstp max-age	Resumes the max age to the default value, 20 seconds.

Link fault, reduces the network auto-adaptivity. We recommend user to use the default value. Note: if you configure the Max Age to a relatively small value, then the calculation of the spanning tree will be relatively frequent, and the system may regard the network block as link failure. If you configurethe Max Age to a relatively big value, then the link status will go unnoticed in time.

The Max Age of bridge is 20 seconds by default.

2.2.6 Value of the path cost of a port

The path cost is related with the link rate of the port. If the link rate is required to be high, the path cost should be set to a small value; when the path cost is set to its default value, RSTP can automatically check the link rate of the current Ethernet port and calculate the corresponding path cost.

Run the following commands in interface configuration mode.

Command	Purpose
spanning-tree rstp cost *value*	Sets the path cost of a port.
no spanning-tree rstp cost	Resumes the path cost of a port to the default value.

It is especially noted that the settings of the path cost will lead to the recalculation of the spanning tree, so users are recommended to take the default value and wait RSTP to calculate the path cost of the current Ethernet port automatically.

By default, the path costs of all Ethernet ports of a bridge are all set to 2000,000 at the 10Mbps port rate, or set to 200,000 at the 100Mbps port rate.

2.2.7 Setting the Port Priority

Port priority settings can be used to designate a specific Ethernet port to be contained in the spanning tree. In general, the smaller the value is, the higher the port priority is, and the Ethernet port has more possibility to be contained in the spanning tree. If all Ethernet ports of a bridge adopt the same priority value, the index number of an Ethernet port decides whether the Ethernet port has a high priority or not.

Run the following commands in interface configuration mode.

Command	Purpose
spanning-tree rstp port-priority *value*	Sets the port priority.
no spanning-tree rstp port-priority	Resumes the port priority to the default value.

It should be noted that the change of the priority of an Ethernet port can lead to the recalculation of the spanning tree.

The priority of all Ethernet ports of a bridge is 128 by default.

2.2.8 Setting the Edge Port

The edge port means this port connects terminal devices of a network. A mandatory edge port will enter the forwarding state after link-up. In port configuration mode, run the following command to set the edge port of RSTP:

Command	Purpose
spanning-tree rstp edge	Sets the edge port.

In auto mode, if a port has not received BPDU in a certain time this port is viewed as the edge port.

2.2.9 Setting the Port Connection Type

If switches, on which RSTP is run, are in the point-to-point connection, these switches can establish a topology rapidly through the handshake mechanism. When the port connection type is set, the connection of a port can be set point-to-point.

By default, RSTP will judge whether a port is in the point-to-point connection according to the duplex mode of this port. If this port works in full duplex mode, RSTP regards this port is in a point-to-point connection; if this port works in half duplex mode, RSTP regards this port's connection is shared.

If it is confirmed that RSTP or MSTP is running on the switches connected by a port, you should set this port's connection type to point-to-point so that fast handshake should be conducted.

In the port configuration mode, run the following command to set the connection type of a port.

Command	Purpose
spanning-tree rstp point-to-point [**force-true** | **force-false** | **auto**]	Sets the point to point interface. force-true: Mandatorily sets the connection to point-to-point. force-false: Mandatorily sets the connection to non-point-to-point. auto: Automatically checks the port type.

2.2.10 Restarting the protocol conversion check

RSTP makes a switch to work together with a traditional 802.1D STP switch through a protocol transfer mechanism. If one port of the switch receives the STP configuration message, the port then only transmits the STP message.

After a port enters the STP-compatible state, even if this port does not receive 802.1D STP BPDU again, this port will not resume the RSTP state. In this case, you can run spanning-tree rstp migration-check to enable the protocol transfer checkup process and resume this port to the RSTP mode.

In global mode run the following command to restart RSTP transfer checkup:

Command	Purpose
spanning-tree rstp migration-check	Restarts RSTP transfer checkup on all ports.

In switch port configuration mode, run the following command to conduct protocol transfer checkup on this port:

Command	Purpose
spanning-tree rstp migration-check	Restarts RSTP transfer checkup on the current port.

Chapter 3 Configuring MSTP

3.1 MSTP Introduction

3.1.1 Overview

Multiple Spanning Tree Protocol (MSTP) is used to establish a simple and complete topology in the bridge LAN. MSTP is compatible with STP (Spanning Tree Protocol) and RSTP (Rapid Spanning Tree Protocol).

Both STP and RSTP only construct a single spanning tree topology in a network and the packets of all VLANs are forwarded along with this unique topology. STP converges too slowly, while RSTP guarantees the a rapid and stable network topology through handshake.

MSTP keeps the fast handshake of RSTP to guarantee fast topology establishment, and at the same time MSTP allows different VLANs to be classified into different spanning trees to establish multiple tree topologies in the network. In a MSTP-constructing network, frames that belong to different VLANs can be forwarded on different paths to realize the load balance of VLAN data.

Different from PVST (per-VLAN Spanning Tree), MSTP permits multiple VLANs to be classified into the same spanning tree topology, effectively reducing spanning trees that are used to support VLANs.

3.1.2 MST Region

In MSTP, the relationship of VLAN and spanning tree is described through a MSTP. The MST configuration table, along with a configuration name and a configuration edit number, makes up of a MST configuration identifier.

In a network, the bridges that interconnect with others and possess the same MST configuration identifier are regarded that they are in the same MST region. The bridges in the same MST region generally have the same VLAN settings so that the frames of these VLANs can only be running at the inside of this MST region.

3.1.3 IST, CST, CIST and MSTI

Figure 2.1 shows an MSTP network, which consists of 3 MST regions and a switch running 802.1D STP protocol.

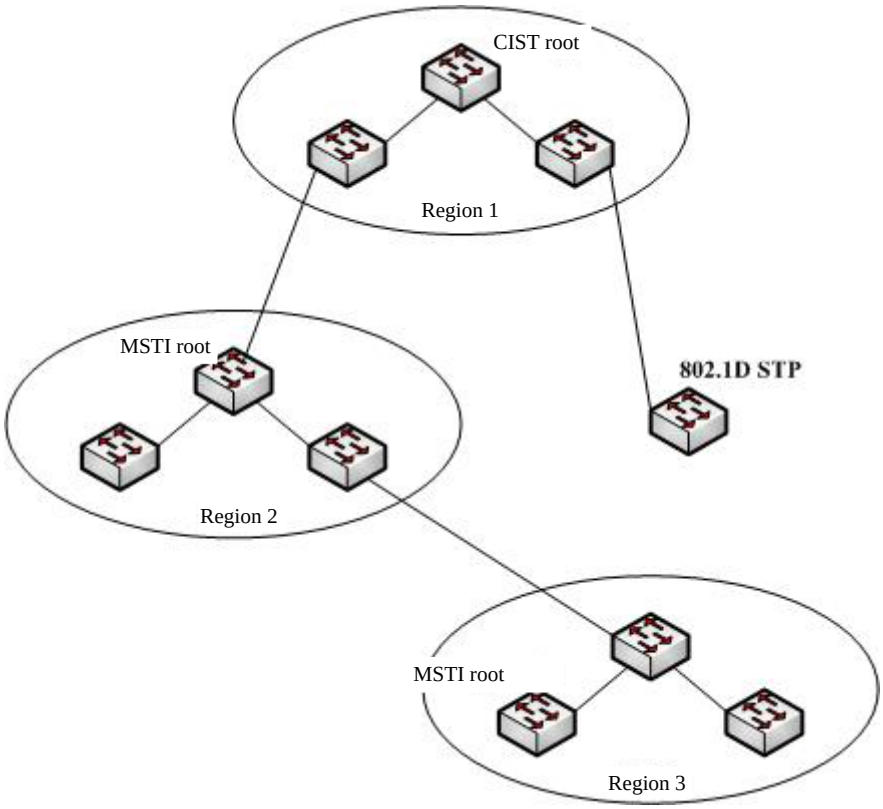


Figure 2.1 MSTP topology

1. CIST

CIST stands for Common and Internal Spanning Tree. Common and Internal Spanning Tree (CIST) means the spanning tree comprised by allsingle switches and interconnected LAN. These switches may belong to different MSTregions. They may be switches running traditional STP or RSTP. Switches running STP or RSTP in the MST regions are considered to be in their own regions.

After the network topology is stable, the whole CIST chooses a CIST root bridge. An internal CIST root bridge will be selected in each region, which is the shortest path from the heart of the region to CIST root.

2. CST

CST stands for Common Spanning Tree. If each MST region is viewed as a single switch, CST is then the spanning tree that connects these “single switches”. As shown in figure 2.1, regions 1-3 and the STP switch constitute a CST of this network.

3. IST

IST stands for Internal Spanning Tree. IST means a CIST part in a MST region, or be considered that IST and CST constitute CIST.

4. MSTI

MSTI stands for Multiple Spanning Tree Instance. MSTP permits different VLANs to be classified into different spanning trees to establish multiple MSTIs. In general, MSTI 0 means CIST, which can be expanded to the whole network, while other MSTIs are each in a region. Each MSTI can be distributed to multiple VLANs. Originally, all VLANs are distributed in CIST.

All MSTIs in the MST region are independent and they can choose different switches to be their roots. For example, in region 3 of figure 2.1, the root of MSTI01 may be the switch at the left bottom corner, while the root of MSTI00 (CIST) may be the switch in the middle.

3.1.4 Port Role

MSTP, like RSTP, has the similar function to conduct port role distribution.

1. Root Port

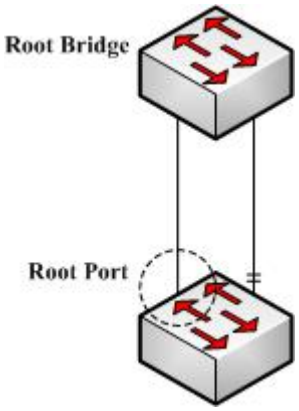


Figure 2.2 Root port

The root port means the path between the current switch to the root bridge. This path has the minimum root path cost.

2. Alternate Port

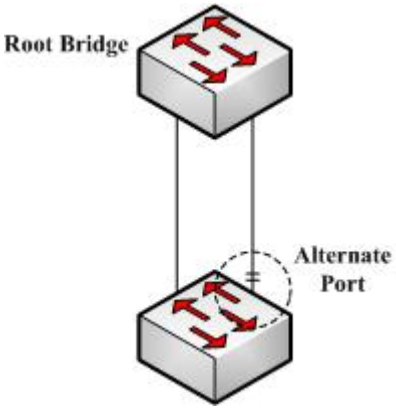


Figure 2.3 Alternate Port

The alternate port serves as path backup between the current switch and the root bridge. When the root port fails to connect, the alternate port can be immediately transferred to be a new root port and start work.

3. Designated Port

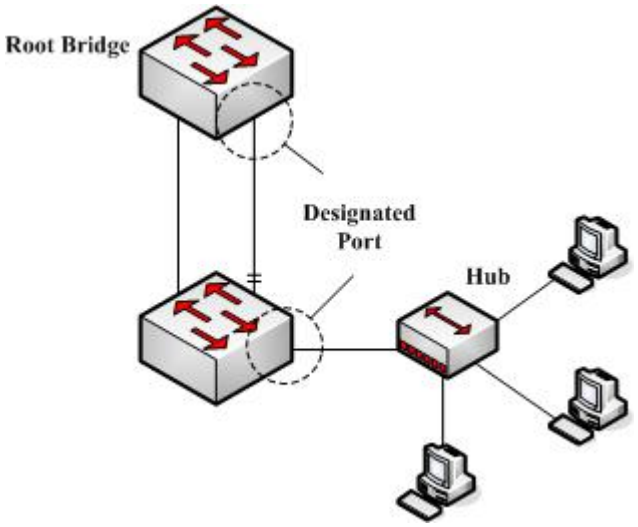


Figure 2.4 Designated port

The designated port can be used to connect the downstream switch or the downstream LAN and then runs as the path between LAN and thr root bridge.

4. Backup Port

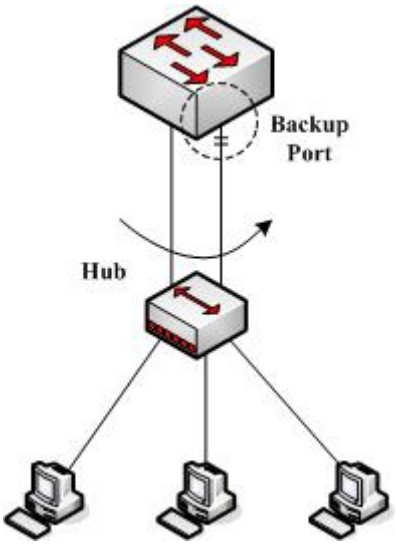


Figure 2.5 Backup port

When two ports of a switch connect directly or connect the same LAN, the port with relatively low priority will run as the backup port and the other port will run as the designated port. If the designated port invalidates, the backup port will serve as the designated port.

5. Master port

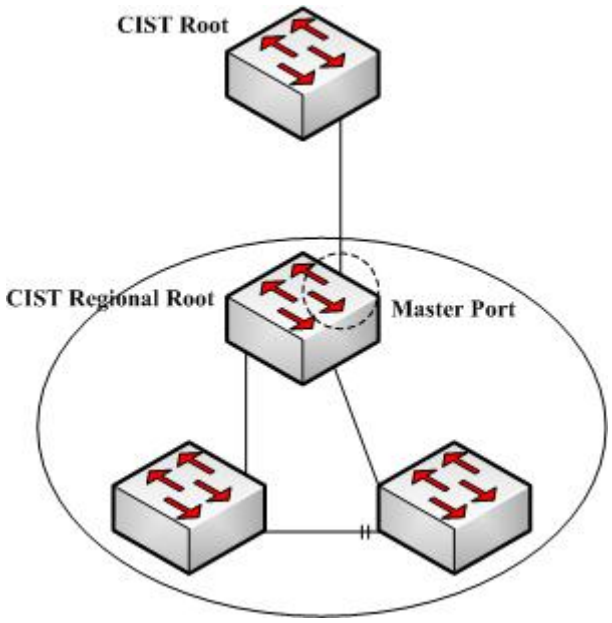


Figure 2.6 Master port

The master port is used as the shortest path between MST region and CIST root bridge. The master port is also the root port of the root bridge in CIST region.

6. Boundary Port

The concept of the boundary port is different from in CIST and in MSTI. In CIST, the boundary port means a port connecting another MST region; while in MSTI, the boundary port means that this spanning tree instance is not extended outside of this port.

7. Edge Port

In RSTP and MSTP, the edge port means a port directly connecting the host, and is capable of entering the forwarding state directly without waiting and loop.

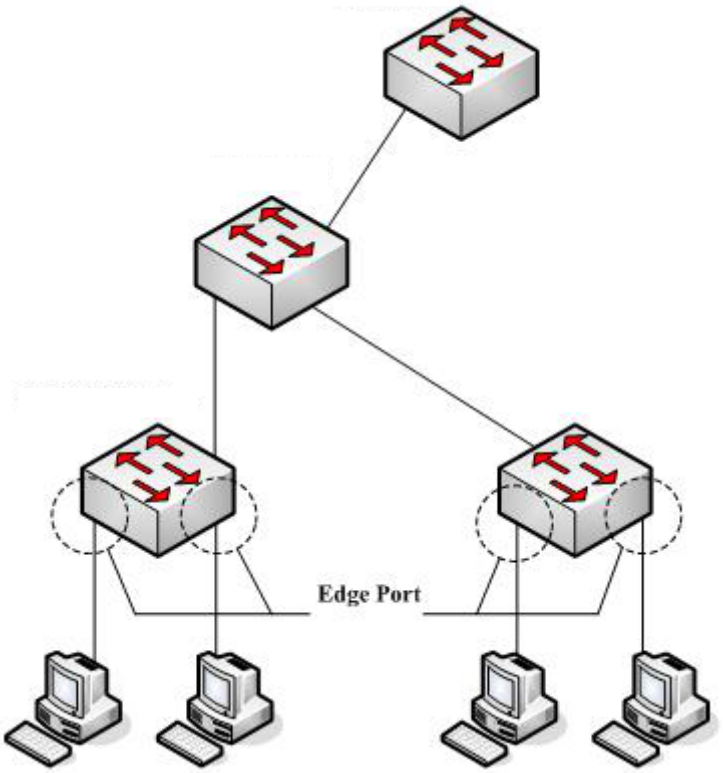


Figure 2.7 Edge port

Originally, MSTP, including RSTP, regards all ports are edge ports and therefore the network topology can be established swiftly. If a port in this case receives BPDU from another switch, the port will resume its edge state from its normal state; if it receives 802.1D STP BPDU, it has to wait for double forward delays and then enters its forwarding state.

3.1.5 MSTP BPDU

Similar to STP and RSTP, switches running MSTP can communicate with each otherthrough Bridge Protocol Data Unit (BPDU). All configuration information about the CIST and MSTI can be carried by BPDU. Table 2.1 and Table 2.2 list the structure ofBPDU used by the MSTP.

Table 2.1 MSTP BPDU

Field Name	Byte Number
Protocol Identifier	1 – 2
Protocol Version Identifier	3
BPDU Type	4
CIST Flags	5
CIST Root Identifier	6 – 13

CIST External Root Path Cost	14 – 17
CIST Regional Root Identifier	18 – 25
CIST Port Identifier	26 – 27
Message Age	28 – 29
Max Age	30 – 31
Hello Time	32 – 33
Forward Delay	34 – 35
Version 1 Length	36
Version 3 Length	37 – 38
Format Selector	39
Configuration Name	40 – 71
Revision	72 – 73
Configuration Digest	74 – 89
CIST Internal Root Path Cost	90 – 93
CIST Bridge Identifier	94 – 101
CIST Remaining Hops	102
MSTI Configuration Messages	103 ~

Table 2.2 MST configuration information

Field Name	Byte Number
MSTI FLAGS	1
MSTI Regional Root Identifier	2 – 9
MSTI Internal Root Path Cost	10 – 13
MSTI Bridge Priority	14
MSTI Port Priority	15
MSTI Remaining Hops	16

3.1.6 Stable State

The MSTP switch performs calculation and compares operations according to thereceived BPDU, and finally ensures that:

(1) One switch is selected as the CIST root of the whole network.

(2) Each switch and LAN segment can decide the minimum cost path to the CIST root, ensuring a complete connection and prevent loops.

(3) Each region has a switch as the CIST regional root. The switch has the minimumcost path to the CIST root.

(4) Each MSTI can independently choose a switch as the MSTI regional root.

(5) Each switch in the region and the LAN segment can decide the minimum costpath to the MSTI root.

(6) The root port of CIST provides the minimum-cost path between the CISTregional root and the CIST root.

(7) The designated port of the CIST provided its LAN with the minimum-cost path tothe CIST root.

(8) The Alternate port and the Backup port provides connection when the switch,port or the LAN does not work or is removed.

(9) The MSTI root port provides the minimum cost path to the MSTI regional root.

(10) The designated port of MSTI provides the minimum cost path to the MSTIregional root.

(11) A master port provides the connection between the region and the CIST root. In the region, the CIST root port of the CIST regional root functions as the masterport of all MSTI in the region.

3.1.7 Hop Count

Different from STP and RSTP, the MSTP protocol does not use Message Age and Max Age in the BPDU configuration message to calculate the network topology. MSTP usesHop Count to calculate the network topology.

To prevent information from looping, MSTP relates the transmitted information to theattribute of hop count in each spanning tree. The attribute of hop count for BPDU is designated by the CIST regional root or the MSTI regional root and reduced in eachreceiving port. If the hop count becomes 0 in the port, the information will be dropped and then the port turns to be a designated port.

3.1.8 STP Compatibility

MSTP allows the switch to work with the traditional STP switch through protocolconversion mechanism. If one port of the switch receives the STP configuration message, the port then only transmits the STP message. At the same time, the portthat receives the STP information is then considered as a boundary port.

Note:
When a port is in the STP-compatible state, the port will not automatically resume to the MSTP state even if the port does not receive the STP message any more. In this case, you can run spanning-tree mstpmigration-check to clear the STP message that the port learned, and make the port to return to the MSTPstate.

The switch that runs the RSTP protocol can identify and handle the MSTP message. Therefore, the MSTP switch does not require protocol conversion when it works with the RSTP switch.

3.2 MSTP Configuration Task List

- Default MSTP Configuration

- Enabling and disabling MSTP
- Configuring MSTP region
- Configuring network root
- Configuring secondary root
- Configuring bridge priority
- Configuring time parameters of STP
- Configuring network diameter
- Configuring maximum hop count
- Configuring port priority
- Configuring path cost for port
- Configuring the edge port
- Configuring port connection type
- Activating MST-compatible mode
- Restarting the protocol conversion check
- Configuring role restriction of the port
- Configuring TCN restriction of the port
- CheckMSTPinformation

3.3 MSTP Configuration Tasks

3.3.1 Default MSTP Configuration

Attributes	Default Settings
STP mode	RSTP (PVST, SSTP and MSTP is not enabled)
Area name	Its default value is the MAC address of a switch.
Area edit level	0
MST configuration list	All VLANs are mapped to CIST (MST00).
Spanning-tree port priority (CIST and all MSTI)	32768
Spanning-tree port priority (CIST and all MSTI)	128
Path cost of the spanning-tree port (CIST and allMSTI)	1000 Mbps:20000

	100 Mbps:200000 10 Mbps:2000000
Hello Time	2 seconds
Forward Delay	15 seconds
Maximum-aging Time	20 seconds
Maximum hop count	20

3.3.2 Enabling and disabling MSTP

The STP protocol can be started in RSTP mode by default. You can stop it running when the spanning-tree is not required.

Run the following command to set the STP to the MSTP mode:

Command	Purpose
spanning-tree	Enables STP in default mode.
spanning-tree mode mstp	Enables MSTP.

Run the following command to disable STP:

Command	Purpose
no spanning-tree	Disable the STP.

3.3.3 Configuring MSTP region

The MST area where the switch resides is decided by three attributes: configurationname, edit number, the mapping relation between VLAN and MSTI. You can configure them through area configuration commands. Note that the change of any of the three attributes will cause the change of the area where the switch resides.

In original state, the MST configuration name is the character string of the MACaddress of the switch. The edit number is 0 and all VLANs are mapped in the CIST (MST00). Because different switch has different MAC address, switches that run MSTP are in different areas in original state. You can run spanning-tree mstp instance instance-id vlan vlan-list to create a new MSTI and map the esignated VLAN to it. If the MSTI is deleted, all these VLANs are mapped to the CIST again.

Run the following command to set the MST area information:

Command	Purpose
spanning-tree mstp name *string*	Configures the MST configuration name. string means the character string of the configurationname. It contains up to 32 characters, capital sensitive. The default value is the character string of the MAC address.
no spanning-tree mstp name	Sets the MST configuration name to the default value.
spanning-tree mstp revision *value*	Sets the MST edit number.

	value represents the edit number, ranging from 0 to 65535. The default value is 0.
no spanning-tree mstp revision	Sets the MST edit number to the default value.
spanning-tree mstp instance *instance-id* **vlan** *vlan-list*	Maps VLAN to MSTI. Instance ID of the spanning-tree, which stands for an MSTI Value range: 1-15 vlan-list: means the VLAN list that is mapped to thespanning tree. It ranges from 1 to 4094. Instance ID is an independent value which stands for an STP instance. vlan-list can represent a group of VLANs, suchas ”1,2,3”, ”1-5” and “1,2,5-10”. "1,2: 5 -10"...
no spanning-tree mstp instance *instance-id*	Cancels the VLAN mapping of MSTI and disables thespanning tree instance. instance-id: Instance ID of the spanning-tree, which stands for a MSTI. Value range: 1-15

Run the following command to check the configuration of the MSTP area:

Command	Purpose
show spanning-tree mstp region	Displays the configuration of the MSTP area.

3.3.4 Configuring network root

In MSTP, each spanning tree instance has a Bridge ID, containing the priority value and MAC address of the switch. During the establishment of spanning tree topology, the switch with comparatively small bridge ID is selected as the network root.

MSTP can set the switch to the network root through configuration. You can run the command Spanning-tree mstp instance-id root to modifythe priority value of the switch in a spanning tree instance from the default value (32768) to a sufficiently small value, ensuring the switch turns to be the root in the spanning tree instance.

In general, after the command to set the primary root is executed, the protocol automatically check the bridge ID of the current network’s root and then sets the priority of the bridge ID to 24576, which guarantees that the current switch serves as the root of the STP instance.

If the priority value of the network root is less than 24576, the protocol will automatically set the STP priority of the current bridge to a value which is 4096 smaller than the priority of the root. It deserves attention that 4096 is the step of the priority value of the bridge.

When setting the root, you can run the diameter subcommand to the network diameter of the spanning tree network. The keyword is effective only when the spanning tree instance ID is 0. After the network diameter is set, MSTP automatically calculates proper STP time parameters to ensure the stability of network convergence. Time

parameters include Forward Delay and Maximum Age. The subcommandHello-time can be used to set a new hello time to replace the default settings.

Run the following command to set the switch to the network root:

Command	Purpose
spanning-tree mstp *instance-id* **root primary** [**diameter** *net-diameter* [**hello-time** *seconds*]]	Sets the switch to the root in the designated spanning treeinstance. instance-id represents the number of the spanning treeinstance, ranging from 0 to 15. net-diameter represents the network diameter, which is anoptional parameter. It is effective when instance-id is 0. It ranges from 2 to 7. seconds represents the unit of the hello time, ranging from1 to 10.
no spanning-tree mstp *instance-id* **root**	Cancels the root configuration of the switch in the spanning tree. instance-id represents the number of the spanning treeinstance, ranging from 0 to 15.

Run the following command to check the MSTP message:

Command	Purpose
show spanning-tree mstp [**instance** *instance-id*]	Checks the MSTP message.

3.3.5 Configuring secondary root

After the network root is configured, you can run spanning-tree mstp instance-id root secondary to set one or multiple switches to the secondary roots or the backuproots. If the root does not function for certain reasons, the secondary roots will become the network root.

Different from primary root configuration, after the command to set the secondary root is executed, the protocol directly set the STP priority of the switch to 28672. In case that the priority value of other switches in the network is 32768 by default, the current switch serves as the secondary root.

When configuring the secondary root, you can run the subcommands diameter and hello-time to update the STP time parameters. When the secondary root becomes the primary root and starts working, all these parameters starts functioning.

Run the following command to set the switch to the secondary root of the network:

Command	Purpose
spanning-tree mstp *instance-id* **root secondary** [**diameter** *net-diameter* [**hello-time** *seconds*]]	Sets the switch to the secondary root in the designated spanning tree instance. instance-id represents the number of the spanning treeinstance, ranging from 0 to 15.

	net-diameter represents the network diameter, which is anoptional parameter. It is effective when instance-id is 0. It ranges from 2 to 7. seconds represents the unit of the hello time, ranging from1 to 10.
no spanning-tree mstp *instance-id* **root**	Cancels the root configuration of the switch in the spanning tree. instance-id represents the number of the spanning treeinstance, ranging from 0 to 15.

Run the following command to check the MSTP message:

Command	Purpose
show spanning-tree mstp [**instance** *instance-id*]	Checks the MSTP message.

3.3.6 Configuring Bridge Priority

In some cases, you can directly set the switch to the network root by configuring the bridge priority. It means that you can set the switch to the network root without running the subcommand root. The priority value of the switch is independent in eachspanning tree instance. Therefore, the priority of the switch can be set independently.

Run the following command to configure the priority of the spanning tree:

Command	Purpose
spanning-tree mstp *instance-id* **priority** *value*	Sets the priority of the switch. instance-id represents the number of the spanning treeinstance, ranging from 0 to 15. value represents the priority of the bridge. It can be one ofthe following values: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672,32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440.
no spanning-tree mstp *instance-id* **priority**	Resumes the bridge priority of the switch to the defaultvalue. instance-id represents the number of the spanning treeinstance, ranging from 0 to 15.

3.3.7 Configuring time parameters of STP

The following are STP time parameters:

- **Hello Time:**

  The interval to send the configuration message to the designated port when theswitch functions as the network root.

- **Forward Delay:**

  Time that the port needs when it changes from the Blocking state to theLearning state and to the Forwarding state in STP mode.

- **Max Age:**

  The maximum live period of the configuration information about the spanningtree.

To reduce the shock of the network topology, the following requirements for the time parameters must be satisfied:

- 2 x (fwd_delay - 1.0) >= max_age
- max_age >= (hello_time + 1) x 2

Running the following command to set the time parameter of MSTP:

Command	Purpose
spanning-tree mstp hello-time *seconds*	Resumes Hello Time to the default value. seconds: value range: 1-10 seconds, Default value: 2 seconds
no spanning-tree mstp hello-time	Resumes the hello time to the default value.
spanning-tree mstp forward-time *seconds*	Sets the parameter Forward Delay. seconds: value range from 4 to 30 seconds, the default value is 15 seconds.
no spanning-tree mstp forward-time	Resumes Forward Delay to the default value.
spanning-tree mstp max-age *seconds*	Sets the parameter Max Age. seconds: value range from 6 to 40 seconds, the default value is 20 seconds.
no spanning-tree mstp max-age	Resumes the Max Age to the default value.

It is recommended to modify the time parameter of STP through setting the root or network diameter, ensuring the rationality of the time parameter.

The newly-set time parameters are valid even if they do not comply with the previous formula's requirements. Pay attention to the notification on the console when you perform configuration.

3.3.8 Configuring network diameter

Network diameter stands for the maximum number of switches between two hosts in the network, representing the scale of the network.

You can set the MSTP network diameter by running the command spanning-treemstp diameter net-diameter. The parameter net-diameter is valid only to CIST. Afterconfiguration, three STP time parameters is automatically updated to comparativelybetter values.

Run the following command to configure net-diameter:

Command	Purpose
spanning-tree mstp diameter *net-diameter*	Configure net-diameter. net-diameter: value range: 2-7; default value: 7
no spanning-tree mstp diameter	Resumes net-diameter to the default value.

The net-diameter parameter is not saved as an independent configuration in the switch. Only the time parameter which is modified through network diameter configuration can be saved.

3.3.9 Configuring maximum hop count

Use the following command to configure the max hop-count.

Command	Purpose
spanning-tree mstp max-hops *hop-count*	Set the maximum hops. hop-count: value range: 6-40 Default value: 20
no spanning-tree mstp max-hops	Resume the maximum hop count to the default value.

3.3.10 Setting the Port Priority

If a loop occurs between two ports of the switch, the port with higher priority will enterthe forwarding state and the port with lower priority is blocked. If all ports have thesame priority, the port with smaller port number will first enter the forwarding state.

In port configuration mode, run the following command to set the priority of the STPport:

Command	Purpose
spanning-tree mstp *instance-id* **port-priority** *priority*	Sets the priority of the STP port. instance-id represents the number of the spanning treeinstance, ranging from 0 to 15. priority stands for the port priority. It can be one of thefollowing values: 0, 16, 32, 48, 64, 80, 96, 112 128, 144, 160, 176, 192, 208, 224, 240,
spanning-tree port-priority *value*	Sets the port priority in all spanning tree instances. value: value of the port priority, which can be one of the following values. 0, 16, 32, 48, 64, 80, 96, 112 128, 144, 160, 176, 192, 208, 224, 240,
no spanning-tree mstp *instance-id* **port-priority**	Resumes the port priority to the default value.
no spanning-tree port-priority	Resumes the port priority to the default value in all spanning tree instances.

3.3.11 Value of the path cost of a port

In MSTP, the default value of the port's path cost is based on the connection rate. If a loop occurs between two switches, the port with less path cost will enter the forwarding state. The less the path cost is, the higher rate the port is. If all ports have the samepath cost, the port with smaller port number will first enter the forwarding state.

In port configuration mode, run the following command to set the path cost of the port:

Command	Purpose
spanning-tree mstp *instance-id* **cost** *cost*	Sets the path cost of the port. instance-id represents the number of the spanning treeinstance, ranging from 0 to 15. cost stands for the path cost of the port, which ranges from 1 to 200000000.
spanning-tree cost *value*	Sets the path cost of the port in all spanning tree instances. value: Path cost of a port, which ranges between 1 and 200,000,000
no spanning-tree mstp *instance-id* **cost**	Resumes the port path cost to the default value.
no spanning-tree cost	Resumes the path cost of the port to the default value.

3.3.12 Setting the Edge Port

The edge port means this port connects terminal devices of a network. A mandatory edge port will enter the forwarding state after link-up. In port configuration mode, run following command to set the edge port of MSTP:

Command	Purpose
spanning-tree mstp edge	Sets the edge port.
no spanning-tree mstp edge	Resume the default setting.

3.3.13 Setting the Port Connection Type

If switches, on which RSTP is run, are in the point-to-point connection, these switches can establish a topology rapidly through the handshake mechanism. When the port connection type is set, the connection of a port can be set point-to-point.

By default, RSTP will judge whether a port is in the point-to-point connection according to the duplex mode of this port. If this port works in full duplex mode, RSTP regards this port is in a point-to-point connection; if this port works in half duplex mode, RSTP regards this port's connection is shared.

If it is confirmed that RSTP or MSTP is running on the switches connected by a port, you should set this port's connection type to point-to-point so that fast handshake should be conducted.

In the port configuration mode, run the following command to set the connection type of a port.

Command	Purpose
spanning-tree mstp point-to-point force-true	Sets the port connection mode to point-to-point.
spanning-tree mstp point-to-point force-false	Sets the port connection mode to non-point-to-point.
spanning-tree mstp point-to-point auto	Sets the port connection mode to auto-check (the default mode).
no spanning-tree mstp point-to-point	Resumes the port connection type to the default settings.

3.3.14 Activating MST-compatible mode

The MSTP protocol that our switches support is based on IEEE 802.1Q. In order to be compatible with other vendors' MSTP implementations, the
MSTP protocol can work in MST-compatible mode. Switches running in MSTP-compatible mode can identify the message structure of other MSTPs, check the contained MST regional identifier and establish the MST region.

The MST-compatible mode and the STP-compatible mode are based on MSTPprotocol conversion mechanism. If one port of the switch receives BPDU in compatible mode, the port automatically changes to the mode and sends BPDU in compatible mode. To resume the port to standard MST mode, you can run spanning-tree mstpmigration-check.

In global configuration mode, run the following commands to enable or disable theMST-compatible mode:

Command	Purpose
spanning-tree mstp mst-compatible	Enable the MST-compatible mode of the switch.
no spanning-tree mstp mst-compatible	Disable the MST-compatible mode of the switch.

Note:

The main function of the compatible mode is to create the MST area for switches and other MSTP-runningswitches. In actual networking, make sure that the switch has the same configuration name and the same edit number. It is recommended to configure switches running other MSTP protocols to the CIST root, ensuring that the switch enters the compatible mode by receiving message.

If the MST-compatible mode is not activated, the switch will not resolve the whole BPDU-compatiblecontent and take the content as the common RSTP BPDU. In this way, the switch cannot be in the samearea with the MST-compatible switch that it connects.

A port in compatible mode cannot automatically resumes to send standard MST BPDU even if thecompatible mode is shut down in global configuration mode. In this case, run migration-check.

3.3.15 Restarting the protocol conversion check

MSTP allows the switch to work with the traditional STP switch through protocolconversion mechanism. If one port of the switch receives the STP configuration message, the port then only transmits the STP message. At the same time, the port that receives the STP information is then considered as a boundary port. Likewise, in MST compatible mode, if one interface receives the compatible BPDU, the interface will also forward compatible BPDU.

Note:
When a port is in the STP-compatible state, the port will not automatically resume to the MSTP state even if the port does not receive the STP message any more. In this case, you can run spanning-tree mstpmigration-check to clear the STP message that the port learned, and make the port to return to the MSTPstate.

The switch that runs the RSTP protocol can identify and handle the MSTP message. Therefore, the MSTP switch does not require protocol conversion when it works with the RSTP switch.

In global configuration mode, run the following command to clear all STP informationthat is detected by all ports of the switch:

Command	Purpose
spanning-tree mstp migration-check	Clears all STP information that is detected by all ports of the switch.

In port configuration mode, run the following command to clear STP informationdetected by the port.

Command	Purpose
spanning-tree mstp migration-check	Clears STP information detected by the port.

3.3.16 Configuring role restriction of the port

The port will not be selected as the root port if the role restriction of the port is enabled.

In the port configuration mode, run the following command to set the role restriction of a port.

Command	Purpose
spanning-tree mstp restricted-role	Sets the port not to be the root port

3.3.17 Configuring TCN restriction of the port

The topology change will not be transferred to other port if TCN restriction of the port is enabled.

In the port configuration mode, run the following command to set the TCN restriction of a port.

Command	Purpose
spanning-tree mstp restricted-tcn	Enable the topology changes on one port cannot

	be transmissed to other ports.

3.3.18 Check MSTP information

In monitoring mode, global configuration mode or port configuration mode,run the following command to check all information about MSTP.

Command	Purpose
show spanning-tree	Checks MSTP information. (Information about SSTP, PVST, RSTP and MSTP can be checked)
show spanning-tree detail	Checks MSTP information. (Information about SSTP, PVST, RSTP and MSTP can be checked)
show spanning-tree interface *interface-id*	Checks the STP interface information. (Information about SSTP, PVST, RSTP and MSTP can be checked)
show spanning-tree mstp	Checks all MST instances.
show spanning-tree mstp region	Checks the MST area configuration.
show spanning-tree mstp instance *instance-id*	Checks information about a MST instance.
show spanning-tree mstp detail	Checks detailed MST information.
show spanning-tree mstp interface *interface-id*	Checks MST port configuration.
show spanning-tree mstp protocol-migration	Checks the protocol conversion state of the port.

STP Optional Characteristic Configuration

Chapter 1 Configuring STP Optional Characteristic..... 1
1.1 STP Optional Characteristic Introduction.....1
1.1.1 Port Fast.....1
1.1.2 BPDU Guard.....2
1.1.3 BPDU Filter.....2
1.1.4 Uplink Fast.....3
1.1.5 Backbone Fast.....4
1.1.6 Root Guard.....6
1.1.7 Loop Guard.....6
1.2 Configuring STP Optional Characteristic.....7
1.2.1 STP Optional Characteristic Configuration Task.....7
1.2.2 Configuring Port Fast.....7
1.2.3 Configuring BPDU Guard.....7
1.2.4 Configuring BPDU Filter.....8
1.2.5 Configuring Uplink Fast.....9
1.2.6 Configuring Backbone Fast.....9
1.2.7 Configuring Root Guard.....9
1.2.8 Configuring Loop Guard.....9
1.2.9 Configuring Loop Fast.....10
1.2.10 Configuring Address Table Aging Protection.....11
1.2.11 Configuring FDB-Flush.....11
1.2.12 Configuring BPDU Terminal.....12

Chapter 1 Configuring STP Optional Characteristic

1.1 STP Optional Characteristic Introduction

The spanning tree protocol module of the switch supports seven additional characteristics (the so-called optional characteristics). These characteristics are not configured by default. The supported condition of various spanning tree protocol modes towards the optional characteristics are as follows:

Optional Characteristic	Single STP	PVST	RSTP	MSTP
Port Fast	Yes	Yes	No	No
BPDU Guard	Yes	Yes	Yes	Yes
BPDU Filter	Yes	Yes	No	No
Uplink Fast	Yes	Yes	No	No
Backbone Fast	Yes	Yes	No	No
Root Guard	Yes	Yes	Yes	Yes
Loop Guard	Yes	Yes	Yes	Yes

1.1.1 Port Fast

Port Fast immediately brings an interface to the forwarding state, bypassing the listening and learning states. In SSTP and PVST mode, you can use Port Fast on interfaces connected to the host or server, to allow those devices to immediately connect to the network.

Port Fast is applicable for connecting ports of the host. As these ports will not receive BPDU and will not affect the network topology, they can enter the forward state without waiting. If the Port Fast function is configured on the interface connecting to the switch, there may cause a loop.

Port Fast Characteristics can be configured in global configuration mode or interface configuration mode. When in global configuration mode, all interfaces will be taken as Port Fast interfaces and fast enter Forwarding state. Thus, it is more likely to cause loop. For avoiding the network loop resulting from Port Fast function, use BPDU Guard or BPDU Filter to protect the interface.

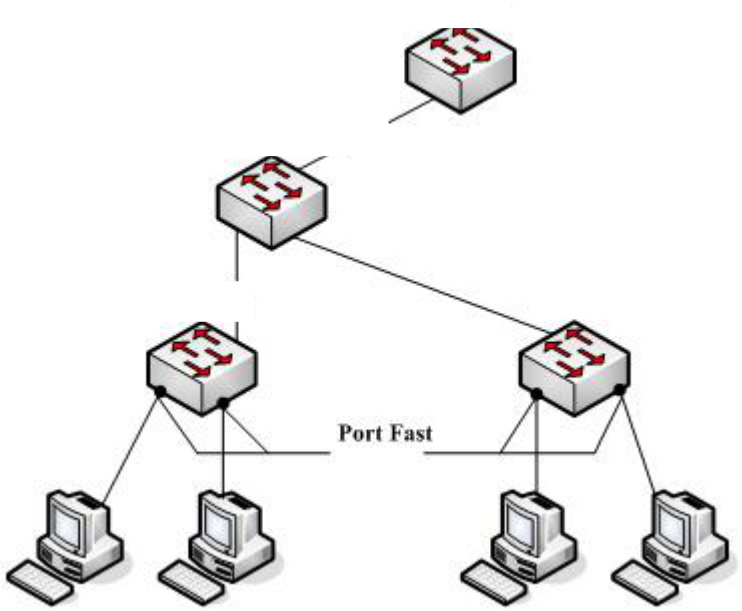


Figure 1.1 Port Fast

Note:

The rapid convergent spanning tree protocol, RSTP and MSTP can immediately bring an interface to the forwarding state, and therefore there is no need to use Port Fast feature.

1.1.2 BPDU Guard

If one Port Fast receives BPDU, it may because of the false network configuration. When one Port Fast receives BPDU, BPDU Guard will protect it passively.

In different STP modes, BPDU Guard acts differently. In SSTP/PVST mode, if a port that has the BPDU Guard function and the Portfast function configured receives BPDU, this port will be manadatorily shut down. You have to configure the port manually to resume this port. In RSTP/MSTP mode, if a BPDU-Guard-configured port receives BPDU, the port will be set to the Blocking state in a period of time.

BPDU Guard characteristics can be configured independent of Port Fast. In all STP modes, the interfaces configured with BPDU Guard will not send BPDU. But the interface can receive BPDU and process it. In RSTP/MSTP mode, you can configure BPDU Guard on the port to ensure the device connected to the switch will not receive BPDU.

BPDU Guard characteristics can be configured in global or interface mode. In global configuration mode, run command spanning-tree portfast bpduguard to block all interfaces sending BPDU. Note that inappropriate use of BPDU Guard will cause loop in complicated network.

1.1.3 BPDU Filter

With the BPDU filtering characteristic, the switch will block BPDU to send out in SSTP/PVST mode, and also from a protection of the Port Fast.

characteristic BPDU Filter and Port Fast at the port will be automatically disabled, resuming the port as a normal port. Before entering the Forwarding state, the port must be in the Listening state and Learning state.

The same with BPDU Guard, BPDU Filter characteristic can be configured in global configuration mode or in port configuration mode. In global configuration mode, run the command spanning-tree portfast bpdufilter to block all ports to send BPDU out. The port, however, can still receive and process BPDU.

1.1.4 Uplink Fast

The characteristic Uplink Fast enables new root ports to rapidly enter the Forwarding state when the connection between the switch and the root bridge is disconnected.

A complex network always contains multiple layers of devices, as shown in figure 1.2. Both aggregation layer and the access layer of the switch have redundancy connections with the upper layer. These redundancy connections are normally blocked by the STP to avoid loops.

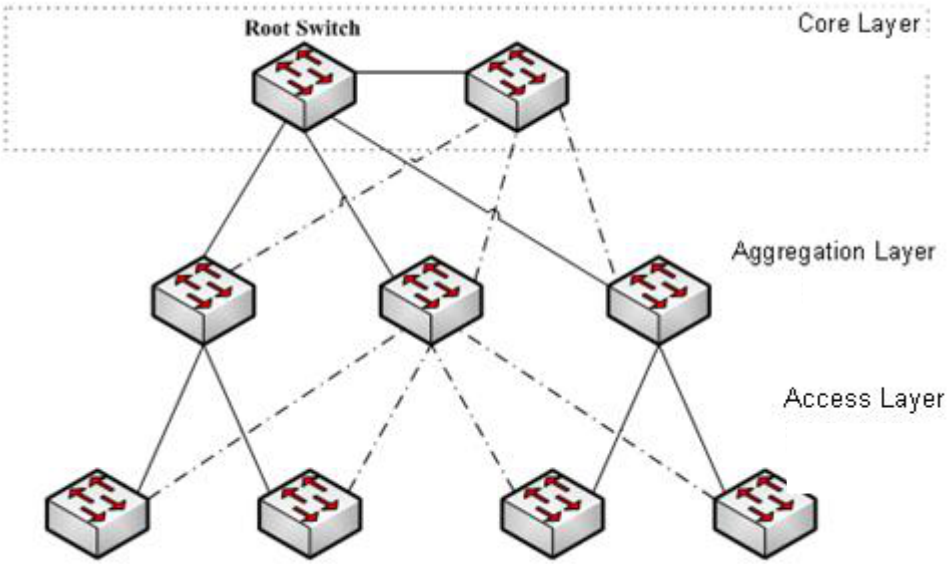


Figure 1.2 Switching network topology

Suppose the connection between a switch and the upper layer is disconnected (called as Direct Link Failure), the STP chooses the Alternate port on the redundancy line as the root port. Before entering the Forwarding state, the Alternate port must be in the Listening state and Learning state. If the Uplink Fast feature is configured by running the command spanning-tree uplinkfast in global configuration mode, new root port can directly enter the forwarding state, resuming the connection between the switch and the upper layer.

Figure 1.3 shows the working principle of the Uplink Fast feature. The port for device C to connect device B is the standby port when the port is in the original state. When the connection between device C and root device A is disconnected, the previous Alternate port is selected as new root port and immediately starts forwarding.

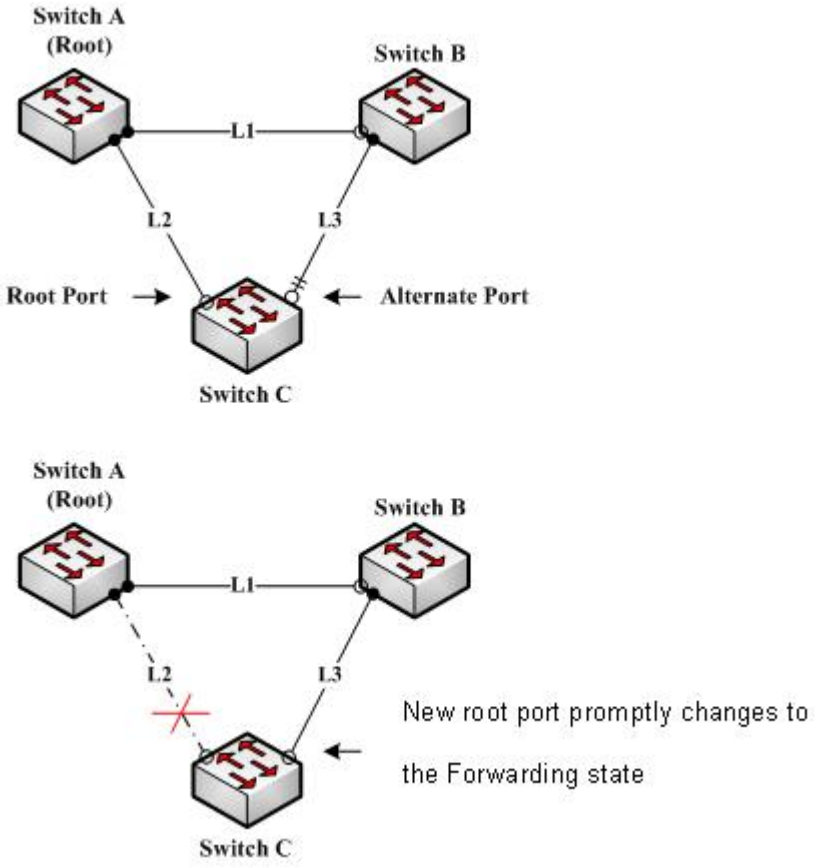


Figure 1.3 Uplink Fast

Note:

The Uplink Fast characteristic adjusts to the slowly convergent SSTP and PVST. In RSTP and MSTP mode, new root port can rapidly enter the Forwarding state without the Uplink Fast function.

1.1.5 Backbone Fast

The Backbone Fast characteristic is a supplement of the Uplink Fast technology. The Uplink Fast technology makes the redundancy line rapidly work in case the direct connection to the designated switch is disconnected, while the Backbone Fast technology detects the indirect-link network blackout in the upper-layer network and boosts the change of the port state.

In figure 1.3, Connection L2 between switch C and switch A is called as the direct link between switch C and root switch A. If the connection is disconnected, the Uplink Fast function can solve the problem. Connection L1 between devices A and B is called as the indirect link of device C. The disconnected indirect link is called as indirect failure, which is handled by the Backbone Fast function.

The working principle of the Backbone Fast function is shown in Figure 1.4.

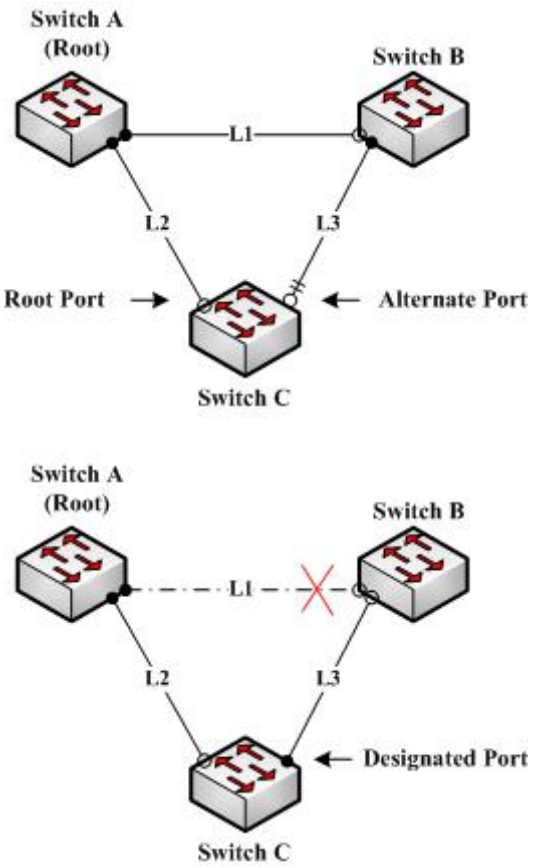


Figure 1.4 Backbone Fast

Suppose the bridge priority of switch C is higher than that of switch B. When L1 is disconnected, device B is selected to send BPDU to device C because the bridge priority is used as root priority. To device C, the information contained by BPDU is not prior to information contained by its own. When Backbone Fast is not enabled, the port between device C and device B ages when awaiting the bridge information and then turns to be the designated port. The aging normally takes a few seconds. After the function is configured in global configuration mode by running the command spanning-tree backbonefast, when the Alternate port of device C receives a BPDU with lower priority, device C thinks that an indirect-link and root-device-reachable connection on the port is disconnected. Device C then promptly update the port as the designated port without waiting the aging information.

After the Backbone Fast function is enabled, if BPDU with low priority is received at different ports, the switch will perform different actions. If the Alternate port receives the message, the port is updated to the designated port. If the root port receives the low-priority message and there is no other standby port, the switch turns to be the root switch.

Note that the Backbone Fast feature just omits the time of information aging. New designated port still needs to follow the state change order: the listening state, then the learning state and finally the forwarding state.

Note:

Similar to Uplink Fast, the Backbone Fast characteristic is effective in SSTP and

1.1.6 Root Guard

The Root Guard attribute can prevent a port from serving as a root port after it receives a higher-priority BPDU.

In a complicated layer-2 network, the administrator may hope a switch in the core layer as the root of the network, but it cannot manage all switches in the access layer (That's because the switch in the access layer may belong to other clients.) Thus, the inappropriate configuration of other switches may cause the core switch cannot become the root.

To avoid the root role is occupied by switches outside the management area, you can configure Root Guard function on the boundary switch. If an interface configured Root Guard receives information that a higher BPDU is chosen as Port Port, Root Guard will automatically set the port as the blocking state and resumes it as the designated port.

In PVST and MSTP mode, Root Guard can work independently in each STP. In MSTP mode, if a boundary interface in CIST is blocked because of Root Guard, the interface will be blocked in all MSTI. The boundary interfaces are those connected to the LAN host, STP switch, RSTP switch or MSTP switch outside the region.

In interface configuration mode, run command **spanning-tree guard root** to enable Root Guard characteristic.

> Note:
>
> Root Guard characteristic acts differently somehow in SSTP/PVST and RSTP/MSTP. In SSTP/PVST mode, Root port is always blocked by Root Guard. In RSTP/MSTP mode, Root port won't be blocked until receiving higher level BPDU. A port which formerly plays the Root role will not be blocked.

1.1.7 Loop Guard

The Loop Guard attribute can protect a port after it changes from a root port or an alternate port to a designated port. This function can prevent a port from generating a loop when the port cannot receive BPDU continuously.

You can enable this feature by using the spanning-tree loopguard default global configuration command. After enabled the command, a Root port or Alternate port wil change to designated port and set as the block state. If the port receives high priority BODU in a while, it will resumes from Loop Guard automatically.

In PVST and MSTP mode, Loop Guard can work independently in each STP. In MSTP mode, if a boundary interface in CIST is blocked because of Root Guard, the interface will be blocked in all MSTI.

Note:

Root Guard characteristic acts differently somehow in SSTP/PVST and RSTP/MSTP. In SSTP/PVST mode, designated port is always blocked by Loop Guard. In RSTP/MSTP mode, the port will be blocked when it changes to designated port if it cannot receive BPDU. An interface receiving low priority BPDU and is of the designated role will not be blocked by

1.2 Configuring STP Optional Characteristic

1.2.1 STP Optional Characteristic Configuration Task

- Configuring Port Fast
- Configuring BPDU Guard
- Configuring BPDU Filter
- Configuring Uplink Fast
- Configuring Backbone Fast
- Configuring Root Guard
- Configuring Loop Guard
- Configuring Loop Fast
- Configuring Address Table Aging Protection
- Configuring FDB-Flush
- Configuring BPDU Terminal

1.2.2 Configuring Port Fast

In SSTP/PVST mode, Port Fast immediately brings an interface to the forwarding state, bypassing the listening and learning states. The function is invalid in other STP mode.

Use the following command to configure the port fast feature in the global configuration mode:

Command	Purpose
spanning-tree portfast default	Globally enables port fast feature. It is valid to all interfaces.
no spanning-tree portfast default	Globally disables port fast feature. It has no effect on the interface configuration.

Note:

The port fast feature only applies to the interface that connects to the host. The BPDU Guard or BPDU Filter must be configured at the same time when the port fast feature is configured globally.

Use the following command to configure the port fast feature in the interface configuration mode:

Command	Purpose
spanning-tree portfast	Disables port fast feature on the interface. It has no effect on the global configuration.
no spanning-tree portfast	Globally disables port fast feature. It has no effect on the interface configuration.

1.2.3 Configuring BPDU Guard

BPDU Guard feature acts when receiving BPDU. The interface configured BPDU Guard feature will not send BPDU.

In different STP modes, BPDU Guard acts differently. In SSTP/PVST mode, if a configured

be shut down mandatorily. You have to configure the port manually to resume this port. In RSTP/MSTP mode, if a BPDU-Guard-configured port receives BPDU, the port will be set to the Blocking state in a period of time.

In global configuration mode, run command BPDU Guard:

Command	Purpose
spanning-tree portfast bpduguard	Globally enables BPDU Guard feature. It is valid to all interfaces.
no spanning-tree portfast bpduguard	Globally disables bpdu guard feature.

Note:

Globally enabling port fast feature may result in broadcast storm. The BPDU Guard or BPDU Filter should be configured for protection sake.

Use the following command to configure the BPDU Guard feature in the interface configuration mode:

Command	Purpose
spanning-tree bpduguard enable	Enables bpdu guard feature on the interface.
spanning-tree bpduguard disable	Disables bpdu guard feature on the interface. It has no effect on the global configuration.
no spanning-tree bpduguard	Disables bpdu guard feature on the interface. It has no effect on the global configuration.

1.2.4 Configuring BPDU Filter

With the BPDU filtering characteristic, the switch will block BPDU to send out in SSTP/PVST mode, and also from a protection of the Port Fast.

In global configuration mode, run command BPDU Filter:

Command	Purpose
spanning-tree portfast bpdufilter	Globally enables BPDU Filter feature. It is valid to all interfaces.
no spanning-tree portfast bpdufilter	Globally disables BPDU Filter feature.

Note:

Globally enabling port fast feature may result in broadcast storm. The BPDU Guard or BPDU Filter should be configured for protection sake.

Use the following command to configure the BPDU Filter feature in the interface configuration mode:

Command	Purpose
spanning-tree bpdufilter enable	Enables BPDU Filter feature on the interface.
spanning-tree bpdufilter disable	Disables BPDU Filter feature on the interface. It has no effect on the global configuration.

	has no effect on the global configuration.

1.2.5 Configuring Uplink Fast

The characteristic Uplink Fast enables new root ports to rapidly enter the Forwarding state when the connection between the switch and the root bridge is disconnected.

The Uplink Fast function validates only in SSTP/PVST mode.

In global configuration mode, run command Uplink Fast characteristic:

Command	Purpose
spanning-tree uplinkfast	Enables uplink fast feature.
no spanning-tree uplinkfast	Disables Uplink Fast feature.

1.2.6 Configuring Backbone Fast

The Backbone Fast characteristic is a supplement of the Uplink Fast technology. The Uplink Fast technology makes the redundancy line rapidly work in case the direct connection to the designated switch is disconnected, while the Backbone Fast technology detects the indirect-link network blackout in the upper-layer network and boosts the change of the port state.

The backbonefast function validates only in SSTP/PVST mode.

In global configuration mode, run command Backbone Fast characteristic:

Command	Purpose
spanning-tree backbonefast	Enables backbone fast feature.
no spanning-tree backbonefast	Disables backbone fast feature.

1.2.7 Configuring Root Guard

The Root Guard attribute can prevent a port from serving as a root port after it receives a higher-priority BPDU.

Root Guard characteristic acts differently somehow in SSTP/PVST and RSTP/MSTP. In SSTP/PVST mode, Root port is always blocked by Root Guard. In RSTP/MSTP mode, Root port won't be blocked until receiving higher level BPDU. A port which formerly plays the Root role will not be blocked.

Use the following command to configure the Root Guard feature in the interface configuration mode:

Command	Purpose
spanning-tree guard root	Enables Root Guard feature on the interface.
no spanning-tree guard	Disables root guard and loop guard features on the interface.
spanning-tree guard none	Disables root guard and loop guard features on the interface.

1.2.8 Configuring Loop Guard

The Loop Guard attribute can protect a port after it changes from a root port or an alternate port to a designated port. This function can prevent a port from generating a loop when the

Root Guard characteristic acts differently somehow in SSTP/PVST and RSTP/MSTP. In SSTP/PVST mode, designated port is always blocked by Loop Guard. In RSTP/MSTP mode, the port will be blocked when it changes to designated port if it cannot receive BPDU. An interface receiving low priority BPDU and is of the designated role will not be blocked by Loopt Guard.

In global configuration mode, run command Loop Guard:

Command	Purpose
spanning-tree loopguard default	Globally enables loop guard feature. It is valid to all interfaces.
no spanning-tree loopguard default	Globally disables loop guard.

Use the following command to configure the Loop Guard feature in the interface configuration mode:

Command	Purpose
spanning-tree guard loop	Enables loop guard feature on the interface.
no spanning-tree guard	Disables root guard and loop guard features on the interface.
spanning-tree guard none	Disables root guard and loop guard features on the interface.

1.2.9 Configuring Loop Fast

Note:

Please configure this command under the guide of technical engineers.

Loop Fast feature is applied to improve the network convergence in a limited range in special network environment. For instance, enable Loop Fast feature for all interfaces in the ring network with a dozen of switches.

Run following commands in global mode to configure Loop Fast feature:

Command	Purpose
spanning-tree loopfast	Globally enables Loop Fast feature. It is valid to all interfaces.
no spanning-tree loopfast	Globally disables Loop Fast.

Use the following command in interface configuration mode to enable Loop Fast:

Command	Purpose
spanning-tree loopfast	Enables loop fast feature on the interface.
no spanning-tree loopfast	Disables Loop Fast feature on the interface. If the global loop fast is configured, the feature on the interface remains effective.
spanning-tree loopfast disable	Disables Loop Fast on the interface.

1.2.10 Configuring Address Table Aging Protection

Under the circumstance of changeable network topology, the configuration of address table aging protection will not affect communication as a result of STP frequently changing the MAC address table.

STPs, such as RSTP and MSTP, will clear the MAC address table of the switch when detecting the STP topology change (delete the old MAC address and update the MAC address), so that the communication can be recovered rapidly. By default, clear action is finished through MAC address table fast aging. Most switches can finish MAC address table fast aging within 1 minute and has little effect on the performance of CPU.

After enabling the address table aging protection function, STP enables protection timer after running the first aging. Before the timeout, another aging will not run. The timer is 15 seconds by default. If the network topology changes within 15 seconds, STP will run a second aging automatically after the timeout.

Note:

The command **no spanning-tree fast-aging** can disable STP running address table aging. Before running the configuration, please ensure the network does not exist loop. Otherwise, the terminal device may need5 mins or even longer time to resume the communication after the network topology changes

In global configuration mode, run following command to configure the address table aging protection function.

Command	Purpose
spanning-tree fast-aging	Enable/disable address table aging function.
spanning-tree fast-aging protection	Enable/disable address table aging protection function.
spanning-tree fast-aging protection time	Sets the time of address table aging protection. Before the time, STP can only run address table aging once. The default value is 15 second.

Use the no form of this command to resume the default setting

1.2.11 Configuring FDB-Flush

Note:

Please configure this command under the guide of technical engineers.

By default, RSTP and MSTP of the switch clear the old MAC address by way of address table fast aging, rather than FDB-Flush.

In global configuration mode, run the following command to configure FDB-Flush:

Command	Purpose
spanning-tree fast-aging flush-fdb	Enable FDB-Flush.

Note that FDB-Flush is independent of fast aging. FDB-Flush can be configured while no spanning-tree fast-aging is configured. But fast aging protection function has no effect on FDB-Flush.

1.2.12 Configuring BPDU Terminal

By default, the device will forward the received BPDU when there is no STP running. BPDU terminal function can forbid forwarding BPDU when there is no STP running.

In global configuration mode, run the following command to configure BPDU Terminal:

Command	Purpose
spanning-tree bpdu-terminal	Enables BPDU Terminal.
no spanning-tree bpdu-terminal	Disables BPDU Terminal.

Layer-2 Link Aggregation Configuration

Table of Contents

Chapter 1 Configuring Port Aggregation....1
1.1 Overview....1
1.2 Port Aggregation Configuration Task....1
1.3 Port Aggregation Configuration Task....1
1.3.1 Configuring Logical Channel Used to Aggregation....1
1.3.2 Aggregation of Physical Port....2
1.3.3 Selecting Load Balance Method After Port Aggregation....2
1.3.4 Monitoring the Concrete Conditions of Port Aggregation....4

Chapter 1 Configuring Port Aggregation

1.1 Overview

Link aggregation, also called trunking, is an optional feature available on the Ethernet switch and is used with Layer 2 Bridging. Link aggregation allows logical merge of multiple ports in a single link. Because the full bandwidth of each physical link is available, inefficient routing of traffic does not waste bandwidth. As a result, the entire cluster is utilized more efficiently. Link aggregation offers higher aggregate bandwidth to traffic-heavy servers and reroute capability in case of a single port or cable failure.

Supported Features:

- Static aggregation control is supported

  Bind a physical port to a logical port, regardless whether they can actually bind to a logical port.

  Aggregation control of LACP dynamic negotiation is supported

  Only a physical port that passes the LACP protocol negotiation can bind to a logical port. Other ports won't bind to the logical port.
- Aggregation control of LACP dynamic negotiation is supported

  When a physical port is configured to bind to a logical port, the physical port with LACP negotiation can be bound to a logical port. Other ports cannot be bound to the logical port.
- Flow balance of port aggregation is supported.

  After port aggregation, the data flow of the aggregation port will be distributed to each aggregated physical port.

1.2 Port Aggregation Configuration Task

- Configuring logical channel used for aggregation
- Aggregation of physical port
- Selecting load balance mode after port aggregation
- Monitoring the concrete condition of port aggregation

1.3 Port Aggregation Configuration Task

1.3.1 Configuring Logical Channel Used to Aggregation

You should establish a logical port before binding all the physical ports together. The logical port is used to control the channel formed by these binding physical ports.

Command	Description
interface port-aggregator id	Configures aggregated logical channel.

1.3.2 Aggregation of Physical Port

To aggregate multiple physical ports into a logical channel, you can use static aggregation or LACP protocol for negotiation.

In the case when the static aggregation is used, it is required that the link of the physical port should be up, and the VLAN attribute of aggregation port and physical port should be identical, and then this port will be aggregated to the logical channel, regardless of whether the current port accords with the conditions of port aggregation and whether the port that connects with the physical port accords with the aggregation conditions.

Prerequisites for ports to be aggregated:

- The link of the port must be up and the port should be negotiated to full-duplex mode.
- The speed of all physical ports should be same during aggregation process, that is, if there is one physical port that has been aggregated successfully, then the speed of the second physical port must be the same as the first configured one. Also the vlan attributes of all physical ports must be identical to the aggregated port.

LACP packets are exchanged between ports in these modes:

- Active—Places a port into an active negotiating state, in which the port initiates negotiations with remote ports by sending LACP packets.
- Passive—Places a port into a passive negotiating state, in which the port responds to LACP packets it receives but does not initiate LACP negotiation. In this mode, the port channel group attaches the interface to the bundle.

If both ports use Passive method, then the aggregation fails. This is because both sides will wait for the other side to launch aggregation negotiation process.

VALN attributes: PVID, Trunk attribute, vlan-allowed range and vlan-untagged range.

Use the following command to perform aggregation on the physical ports:

Command	Description
aggregator-group *agg-id* **mode** { **lacp** | **static** }	Configures aggregation option of the physical port.

1.3.3 Selecting Load Balance Method After Port Aggregation

You can select the load share method to ensure that all ports can share the data traffic after the aggregation of all physical ports. The switch can provides up to six load balance strategy:

- src-mac

message with same MAC address attributes is to get through a physical port.

- dst-mac

  It is to share the data traffic according to the destination MAC address, that is, the message with same MAC address attributes is to get through a physical port.

- both-mac

  It is to share the data traffic according to source and destination MAC addresses, that is, the message with same MAC address attributes is to get through a physical port.

- src-ip

  It is to share the data traffic according to the source IP address, that is, the message with same IP address attributes is to get through a physical port.

- dst-ip

  It is to share the data traffic according to the destination IP address, that is, the message with same IP address attributes is to get through a physical port.

- both-ip

  It is to share the data traffic according to the destination and source IP addresses, that is, the message with same IP address attributes is to get through a physical port.

Use the following command to configure load balance method:

Command	Description
aggregator-group load-balance	Configures load balance method.

Note:

The command is unavailable at the switch that does not support load balance methods or supports only one method. The switch using the command only selects the load balance strategies supported by itself.

1.3.4 Monitoring the Concrete Conditions of Port Aggregation

Use the following command to monitor port aggregation state in EXEC mode:

Command	Description
show aggregator-group	Displays port aggregation state.

PDP Configuration

Table of Contents

Chapter 1 PDP Overview....1
1.1 Overview....1
1.2 PDP Configuration Tasks....1
1.2.1 Default PDP Configuration....1
1.2.2 Setting the PDP Clock and Information Storage....1
1.2.3 Setting the PDP Version....2
1.2.4 Starting PDP on a Switch....2
1.2.5 Starting PDP on a Port....2
1.2.6 PDP Monitoring and Management....2
1.3 PDP Configuration Example....2

Chapter 1 PDP Overview

1.1 Overview

PDP is specially used to discover network equipment, that is, it is used to find all neighbors of a known device. Through PDP, the network management program can use SNMP to query neighboring devices to acquire network topology.

Our company's switches can discover the neighboring devices but they do not accept SNMP queries. Therefore, switches only run at the edge of network, or they cannot acquire a complete network topology.

PDP can be set on all SNAPs (e.g. Ethernet).

1.2 PDP Configuration Tasks

- Default PDP Configuration
- Setting the PDP Clock and Information Storage
- Setting the PDP Version
- Starting PDP on a Switch
- Starting PDP on a Port
- PDP Monitoring and Management

1.2.1 Default PDP Configuration

Function	Default Settings
Global configuration mode	This function is not enabled by default.
Interface configuration mode	Starts up.
PDP clock (packet transmission frequency)	60 seconds
PDP information storage	180 seconds
PDP version	2

1.2.2 Setting the PDP Clock and Information Storage

To set the PDP packet transmission frequency and the PDP information storage time, you can run the following commands in global configuration mode.

Command	Purpose

pdp timer seconds	Sets the transmission frequency of the PDP packets.
pdp holdtime seconds	Sets the PDP information storage time.

1.2.3 Setting the PDP Version

To set the PDP version, you can run the following command in global configuration mode.

Command	Purpose
pdp version {1|2}	Setts the PDP version.

1.2.4 Starting PDP on a Switch

To enable PDP, you can run the following commands in global configuration mode.

Command	Purpose
pdp run	Starts PDP on a switch.

1.2.5 Starting PDP on a Port

To enable PDP on a port by default, you can run the following command in port configuration mode.

Command	Purpose
pdp enable	Starts PDP on a port of a switch.

1.2.6 PDP Monitoring and Management

To monitor the PDP, run the following commands in EXEC mode:

Command	Purpose
show pdp traffic	Displays the counts of received and transmitted PDP packets.
show pdp neighbor [detail]	Displays neighbors that PDP discovers.

1.3 PDP Configuration Example

Example 1: Starting PDP

Switch_config# pdp run
Switch_config# int f0/1
Switch_config_f0/1#pdp enable

Example 2: Setting the PDP clock and information storage

Switch_config#pdp timer 30

Switch_config#pdp holdtime 90

Example 3: Setting the PDP version

Switch_config#pdp version 1

Example 4: Monitoring PDP

Switch_config#show pdp neighbor

Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge

S - Switch, H - Host, I - IGMP, r - Repeater

Device-ID	Local-Intf	Hldtme	Port-ID	Platform	Capability
Switch	Fas0/1	169	Gig0/1	COMPANY, RISC	R S

LLDP Configuration

Table of Contents

Chapter 1 Link Layer-2 Discovery Protocol (LLDP) 1
1.1 LLDP Overview 1
1.1.1 Initializing the Protocol 1
1.1.2 Initializing LLDP Transmit Mode 1
1.1.3 Initializing LLDP Reception Mode 2
1.1.4 LLDP PDU Packet Structure Description 2
1.2 LLDP Configuration Task List 3
1.3 LLDP Configuration Tasks 4
1.3.1 Disabling/enablingLLDP 4
1.3.2 Configuringholdtime 4
1.3.3 Configuring Timer 5
1.3.4 Configuring Reinit 5
1.3.5 Configuring the To-Be-SentTLV 6
1.3.6 Specifying the Port's Configuration and Selecting the To-Be-Sent Expanded TLV 7
1.3.7 Configuring the Transmission or Reception Mode 9
1.3.8 Specifying the Management IP Address of a Port 10
1.3.9 Sending Trap Notification to mib Database 10
1.3.10 Configuring the Location Information 11
1.3.11 Specifying a Port to Set the Location Information 13
1.3.12 Configuring Show-Relative Commands 14
1.3.13 Configuring the Deletion Commands 14
1.4 Configuration Example 14
1.4.1 Network Environment Requirements 14
1.4.2 Network Topology 15
1.4.3 Configuration Procedure 15

Chapter 1 Link Layer-2 Discovery Protocol (LLDP)

1.1 LLDP Overview

802.1ABThe link layer discovery protocol (LLDP) at 802.1AB helps to detect network troubles easily and maintain the network topology. It enables the neighboring device to sending out notice of its own state information to other devices and each port of all devices stores information of defining themselves. If necessary, they can also sending update information to the neighboring devices and the neighboring devices will store the information in standard SNMP MIBs. The network management system can inquire the connection of current layer-2 from MIB. LLDPcan neither configure nor control the network element or traffic. It only reports configuration of layer-2.

Simply, LLDP is a neighbor discovery protocol. It sets a standard method for the Ethernet network device, such as switches, routers and WAPs. It enables the Ethernet device notify its existence to other nodes and save the discovery information of neighboring devices. For instance, all information including the device configuration and the device identification can be notified through the protocol. Specifically, LLDP defines a universal notification information set, a transmission notification protocol and a method of storing all notification information. The device need to notify the notification information can transmit many notifications in a LAN data packet. The transmission type is TLV.

TLV has three compulsory types: Chassis ID TLV, Port ID TLV and Time To Live TLV; five optional types: Port Description, System Name, System Description, System Capabilities and Management Address; and three extension TLVs: DOT1 (Port Vlan ID, Protocol Vlan ID, Vlan Name, Protocol Identity); DOT3 (MAC/PHY Configuration/Status, Power Via MDI, Link Aggregation, Max Frame Size); MED (MED Capability, Network Policy, Location Identification, Extended Power-via-MDI, Inventory (Hardware Revision, Firmware Revision, Software Revision, Serial Number, Manufacturer Name, Model Name, Asset ID).

LLDP is a unidirectional protocol. One LLDP agent transmits its state information and functions through its connected MSAP, or receives the current state information or function information about the neighbor. However, the LLDP agent cannot request any information from the peer through the protocol. During message exchange, message transmission and reception do not affect each other. You can configure only message transmission or reception or both.

1.1.1 Initializing the Protocol

LLDP can work under three modes: transmit-only, receive-only and transmit-and-receive. The default mode is transmit-and-receive.

1.1.2 Initializing LLDP Transmit Mode

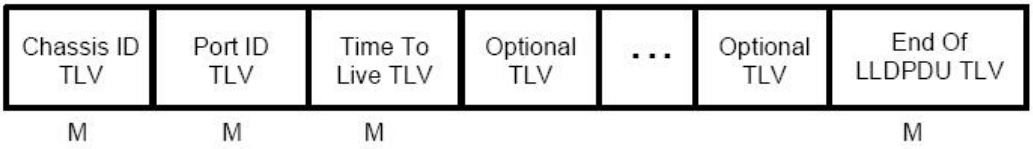
Set LLDP to transmit-only in the interface mode. In transmit-only mode, the interface transmits LLDP packets when the state or value of one or more information elements (management object) of the local system change or the transmission timer is timeout. The interface will not transmit LLDP packets when disabling the function.

1.1.3 Initializing LLDP Reception Mode

Set LLDP to receive-only in the interface mode. In receive-only mode, the interface can receive LLDP packets from the neighbors and save tlv into the remote MIB. The interface will drop LLDP packets when disabling the function.

1.1.4 LLDP PDU Packet Structure Description

In accordance with the order, LLDP PDU includes three compulsory TLVs in the front, one or more optional TLV in the middle and LLDPUD TLV in the end. As shown in figure 1:



M must include TLV.

Figure 1 LLDP PDU Format

(1) Three compulsory TLVs should be listed in sequence at the beginning of LLDP PDU:

1. Chassis ID TLV
2. Port ID TLV
3. Time To Live TLV

(2) Optional TLV selected by the network management can be listed randomly.

4. Port Description
5. System Name
6. System Description
7. System Capabilities
8. Management Address

Three extensions (including DOT1):

9. Port Vlan ID
10. Protocol Vlan ID
11. Vlan Name
12. Protocol Identity

DOT3:

13. MAC/PHY Configuration/Status
14. Power Via MDI
15. Link Aggregation
16. Max Frame Size

MED (TLV of MED is not transmitted by default. LLDP packets with MED TLV will be transmitted only when LLDP packets with MED TLV are received.)

17. MED Capability (TLV is compulsory if MED TLV is added.)
18. Network Policy
19. Location Identification
20. Extended Power-via-MDI

Inventory (including Hardware Revision, Firmware Revision, Software Revision, Serial Number,Manufacturer Name,Model Name,Asset ID)

(3) The end TLV should be the last one in LLDP PDU.

1.2 LLDP Configuration Task List

- Disabling/enabling LLDP
- Configuring holdtime
- Configuring Timer
- Configuring Reinit
- Configuring the To-Be-Sent TLV
- Configuring the Transmission or Reception Mode
- Specifying the Management IP Address of a Port
- Sending Trap Notification to mib Database
- Configuring Show-Relative Commands
- Configuring the Deletion Commands

1.3 LLDP Configuration Tasks

1.3.1 Disabling/enablingLLDP

LLDP is disabled by default. You need start up LLDP before it runs. After enabling LLDP, the local port regularly forwards lldp frame to notify the information of the opposite local port.

Run the following command in global configuration mode to enable LLDP:

Procedure	Command	Purpose
Step1	config	Enters the global configuration mode.
Step2	lldp run	Runs LLDP.

Run the following command to disable LLDP:

Procedure	Command	Purpose
Step1	config	Enters the global configuration mode.
Step2	no lldp run	Disables LLDP.

Caution: Only lldp function is enabled can the system process lldp packets. Otherwise, lldp frame will be directly forwarded.

1.3.2 Configuringholdtime

In normal condition, the remote information stored in MIB will update before aging. But the frame may loss in sending and causes the information ages. For avoiding this, you need to set the value of TTL and ensure the update LLDP frame is forwarded time after time. You can control the timeout time of transmitting the LLDP message through modifying holdtime:

Run the following command in global configuration mode to configure holdtime of LLDP:

Procedure	Command	Purpose
Step1	config	Enters the global configuration mode.
Step2	lldp holdtime time	Configures the timeout time of LLDP. The value range from 0 to 65535. The default value is 120s.

Resumes the timeout time to the default value:

Procedure	Command	Purpose
Step1	config	Enters the global configuration mode.
Step2	no lldp holdtime	Resumes the timeout time to the default value, 120 seconds.

Caution: To ensure the former neighbor information is not lost owing to aging when receiving next LLDP frame, the timeout time should be longer than the LLDP packet transmit interval.

1.3.3 Configuring Timer

You can control the interval of the switch to transmit message by configuring the timer of LLDP.

Run the following command in global configuration mode to configure timer of LLDP:

Procedure	Command	Purpose
Step1	config	Enters the global configuration mode.
Step2	lldp timer time	Configures the interval of message transmission of LLDP. The value ranges from 5 to 65534. The default time is 30 seconds.

Resumes the default interval, that is, 30 seconds.

Procedure	Command	Purpose
Step1	config	Enters the global configuration mode.
Step2	no lldp timer	Resumes the default interval, that is, 30 seconds.

1.3.4 Configuring Reinit

LLDP information will be forwarded automatically in two conditions: first, the status or value of one or more information elements (management objects) change; second, the sending timer timeouts. A single information change cause the LLDP packet is forwarded and a series of information change may cause many LLDP frames forwarded, but a frame can only report one change. For avoiding this, the web management defines the interval of two continuous LLDP frames. You can control the interval of the switch to continuously transmit two messages by configuring reinit of LLDP.

Run the following command in global configuration mode to configure reinit of LLDP:

Procedure	Command	Purpose
Step1	config	Enters the global configuration mode.
Step2	lldp reinit time	Configures the interval of LLDP to continuously transmit message. The value ranges from 2 to 5. The default time is 2 seconds.

Resumes the default value of reinit.

Procedure	Command	Purpose

Step1	config	Enters the global configuration mode.
Step2	no lldp reinit	Resumes the default interval of continuously transmitting message; the default interval value is two seconds.

1.3.5 Configuring the To-Be-SentTLV

You can choose TLV which requires to be sent by configuring tlv-select of LLDP. By default, all TLVs are transmitted.

Run the following commands in global configuration mode to add or delete tlv of LLDP:

Procedure	Command	Purpose
Step1	config	Enters the global configuration mode.
Step2	lldp tlv-select management-address	This step is optional. Transmits the management address tlv. The management address is usually layer-3 IP address which should be easy to use.
Step3	lldp tlv-select port-description	This step is optional. Transmits the port description tlv. The port description uses number or letters for description.
Step4	lldp tlv-select system-capabilities	This step is optional. Transmits the system performance tlv. The system performance refers to the system of transmitting packets such as the switch or router.
Step5	lldp tlv-select system-description	This step is optional. Transmits system description tlv. The system description is consist of texts including numbers and letters. The system description should include the full name of the system, the hardware version, the software system and the network software.
Step6	lldp tlv-select system-name	This step is optional. Transmits system name tlv. The system name domain is a specified name consisted of numbers and letters. The name of the system should be the name of the system manager. That is the name of the switch.

Run the following commands in global configuration mode to delete to-be-sent TLV:

Procedure	Command	Purpose
Step1	config	Enters the global configuration mode.
Step2	no lldp tlv-select management-address	This step is optional. Transmits the management address tlv. The management

		address is usually layer-3 IP address which should be easy to use.
Step3	no lldp tlv-select port-description	This step is optional. Transmits the port description tlv. The port description uses number or letters for description.
Step4	no lldp tlv-select system-capabilities	This step is optional. Transmits the system performance tlv. The system performance refers to the system of transmitting packets such as the switch or router.
Step5	no lldp tlv-select system-description	This step is optional. Transmits system description tlv. The system description is consist of texts including numbers and letters. The system description should include the full name of the system, the hardware version, the software system and the network software.
Step6	no lldp tlv-select system-name	This step is optional. Transmits system name tlv. The system name domain is a specified name consisted of numbers and letters. The name of the system should be the name of the system manager. That is the name of the switch.

1.3.6 Specifying the Port's Configuration and Selecting the To-Be-Sent Expanded TLV

Through the configuration of dot1-tlv-select/ dot3-tlv-select/ med-tlv-select of LLDP on a port, you can select expanded TLV to be sent. By default, TLV of both DOT1 and DOT3 will be transmitted while TLV of MED will not be transmitted.

Run the following commands in port configuration mode to add the to-be-sent TLV:

Procedure	Command	Purpose
Step1	config	Enters the global configuration mode.
Step2	interface intf-type intf-id	Enters the interface configuration mode.
Step3	lldp dot1-tlv-select port-vlan-id	(Optional) Sends the 802.1-defined TLV and notifies the PVID of a port.
Step4	lldp dot1-tlv-select protocol-vlan-id	(Optional) Sends the 802.1-defined TLV and notifies the PPVID of a port.
Step5	lldp dot1-tlv-select vlan-name	(Optional) Sends the 802.1-defined TLV and notifies the VLAN name of a port.
Step6	lldp dot3-tlv-select macphy-confg	(Optional) Sends the 802.3-defined TLV. The following contents are contained: a) The bit rate and the communication mode (duplex) on the physical layer;

		b) Current duplex and the set bit rate; c) Showing whether the setting is the results of auto-negotiation in the initial connection phase or is a compulsory manual behavior;
Step7	lldp dot3-tlv-select power	(Optional) Sends the 802.3-defined TLV and shows the interface allows the power supply connecting to the non-power system through the link.
Step8	lldp dot3-tlv-select link-aggregation	(Optional) Sends the 802.3-defined TLV and specifies a port to identify the aggregation if the link can be aggregated.
Step9	lldp dot3-tlv-select max-frame-size	(Optional) Sends the 802.3-defined TLV and specifies the size of the maximum frame on a port(byte) .
Step10	lldp med-tlv-select network-policy	(Optional) Sends the MED-defined TLV and the interface can effectively discover and diagnose VLAN configured error-matching flow and the attribute of layer-2 and layer-3
Step11	lldp med-tlv-select location	(Optional) Sends the MED-defined TLV and specifies the address. a) coordinate-based LCI, which is defined in IETF 3825[6]; b) city's address LCI, which is defined in IETF (refer to Annex B); c) ELIN code of the urgency call service;
Step12	lldp med-tlv-select power-management	(Optional) Sends the MED-defined TLV and shows the information of power supply.
Step13	lldp med-tlv-select inventory	(Optional) Sends the MED-defined TLV and shows the attribute of detailed inventory.

Run the following commands in global configuration mode to delete to-be-sent TLV:

Procedure	Command	Purpose
Step1	config	Enters the global configuration mode.
Step2	interface intf-type intf-id	Enters the interface configuration mode.
Step3	no lldp dot1-tlv-select port-vlan-id	(Optional) Sends the 802.1-defined TLV and notifies the PVID of a port.
Step4	no lldp dot1-tlv-select protocol-vlan-id	(Optional) Sends the 802.1-defined TLV and notifies the PPVID of a port.
Step5	no lldp dot1-tlv-select vlan-name	(Optional) Sends the 802.1-defined TLV and notifies the VLAN name of a port.
Step6	no lldp dot3-tlv-select macphy-confg	(Optional) Sends the 802.3-defined TLV. The following contents are contained:

		a) The bit rate and the communication mode (duplex) on the physical layer; b) Current duplex and the set bit rate; c) Showing whether the setting is the results of auto-negotiation in the initial connection phase or is a compulsory manual behavior;
Step7	no lldp dot3-tlv-select power	(Optional) Sends the 802.3-defined TLV and shows the interface allows the power supply connecting to the non-power system through the link.
Step8	no lldp dot3-tlv-select link-aggregation	(Optional) Sends the 802.3-defined TLV and specifies a port to identify the aggregation if the link can be aggregated.
Step9	no lldp dot3-tlv-select max-frame-size	(Optional) Sends the 802.3-defined TLV and specifies the size of the maximum frame on a port(byte) .
Step10	no lldp med-tlv-select network-policy	(Optional) Sends the MED-defined TLV and the interface can effectively discover and diagnose VLAN configured error-matching flow and the attribute of layer-2 and layer-3.
Step11	no lldp med-tlv-select location	(Optional) Sends the MED-defined TLV and specifies the address. a) coordinate-based LCI, which is defined in IETF 3825[6]; b) city's address LCI, which is defined in IETF (refer to Annex B); c) ELIN code of the urgency call service;
Step12	no lldp med-tlv-select power-management	(Optional) Sends the MED-defined TLV and shows the information of power supply.
Step13	no lldp med-tlv-select inventory	(Optional) Sends the MED-defined TLV and shows the attribute of detailed inventory.

1.3.7 Configuring the Transmission or Reception Mode

LLDP can work under three modes: transmit-only, receive-only and transmit-and-receive. By default, LLDP works under the transmit-and-receive mode. You can modify the working mode of LLDP through the following commands.

Run the following commands in the interface configuration mode and set lldp to the transmit-and-receive mode.

Procedure	Command	Purpose
Step1	config	Enters the global configuration mode.

Step2	interface intf-type intf-id	Enters the interface configuration mode.
Step3	no lldp transmit	Disables the transmit-only mode of the port.
Step4	no lldp receive	Disables the receive-only mode of the port.

Run the following commands in the interface configuration mode and set lldp to the transmit-and-receive mode.

Procedure	Command	Purpose
Step1	config	Enters the global configuration mode.
Step2	interface intf-type intf-id	Enters the interface configuration mode.
Step3	lldp transmit	Enables the transmit mode of the port.
Step4	lldp receive	Enables the receive mode of the port.

Note: Except the above mode, the interface can also be configured to the transmit-only mode or the receive-only mode.

1.3.8 Specifying the Management IP Address of a Port

In port configuration state, you can randomly configure the management address of the port, from which the LLDP packets are transmitted. This management address should be an IP address related with this port, and only in this way the normal communication of this port can be guaranteed.

Run the following commands in port configuration mode to set the management IP address:

Procedure	Command	Purpose
Step1	config	Enters the global configuration mode.
Step2	interface intf-type intf-id	Enters the interface configuration mode.
Step3	lldp management-ip A.B.C.D	Sets the management IP address of a port.

Note: Both the no lldp command and the management-ip command can be used to resume the default management address of the port and the default management address is the IP address of the VLAN interface that corresponds to the PVID port. When the corresponding VLAN interface does not exist, the management address is 0.0.0.0.

1.3.9 Sending Trap Notification to mib Database

Sending Trap Notification to lldp mib databaseor ptopomib database.

Run the following commands in the global configuration mode to sending trap notification to lldp mib database or ptopo mib database.

Procedure	Command	Purpose
Step1	config	Enters the global configuration mode.
Step2	lldp trap-send lldp-mib	Sends trap notification to lldp mib database.

Step3	lldp trap-send ptopo-mib	Sends trap notification to ptopo mib database.

Note: Both the no lldp command and the management-ip command can be used to resume the default management address of the port and the default management address is the IP address of the VLAN interface that corresponds to the PVID port. When the corresponding VLAN interface does not exist, the management address is 0.0.0.0.

1.3.10 Configuring the Location Information

The location configuration is used to determine the address of the local machine.

Run the following commands in global configuration mode to configure the location information:

Procedure	Command	Purpose
Step1	config	Enters the global configuration mode.
Step2	location elin identifier id WORD	Sets the location elin information, in which id is the elin identifier number and WORD stands for the elin information, which ranges from 10 to 25 bytes.
Step3	location civic identifier id	Enters the location configuration mode.
Step4	language WORD	Sets the language.
Step5	state WORD	Sets the state's (provincial) name, such as SiteB.
Step6	county WORD	Sets the name of a county.
Step7	city WORD	Sets the name of a city.
Step8	division WORD	Sets the name of a division.
Step9	neighborhood WORD	Sets the name of neighborhood.
Step10	street WORD	Sets the name of a street.
Step11	leading-street-dir WORD	Sets the direction of a main street, such as N (north).
Step12	trailing-street-suffix WORD	Sets the suffix of a small street, such as SW.
Step13	street-suffix WORD	Sets the suffix of a street, such as platz.
Step14	number WORD	Sets the street number, such as number 123.
Step15	street-number-suffix WORD	Sets the suffix of the street number, such as number 1/2 of A road.
Step16	landmark WORD	Sets the landmark, such as Colombia University.
Step17	additional-location WORD	Sets the additional location.
Step18	name WORD	Sets the information about a resident, such as Joe's haircut shop.

Step19	postal-code WORD	Sets the postal code.
Step20	building WORD	Sets the information about a building.
Step21	unit WORD	Sets the information about a unit.
Step22	floor WORD	Sets the information about a floor.
Step23	room WORD	Sets the information about a room.
Step24	type-of-place WORD	Sets the type of a place, such as office.
Step25	postal-community WORD	Sets the name of a postal office.
Step26	post-office-box WORD	Sets the name of a postal box, such as 12345.
Step27	additional-code WORD	Sets the additional code.
Step28	country WORD	Sets the name of a country.
Step29	script WORD	Sets the script.

Run the following commands in global configuration mode to delete the location information:

Procedure	Command	Purpose
Step1	config	Enters the global configuration mode.
Step2	no location elin identifier id	Deletes the location enlin information of elin identifier.
Step3	no location civic identifier id	Deletes the location enlin information of id, which is the number of civic identifier.
Step4	location civic identifier id	Enters the location configuration mode.
Step5	no language	Deletes the language.
Step6	no state	Deletes the state's (provincial) name, such as SiteB.
Step7	no county	Deletes the name of a county.
Step8	no city	Deletes the name of a city.
Step9	no division	Deletes the name of a division.
Step10	no neighborhood	Deletes the name of neighborhood.
Step11	no street	Deletes the name of a street.
Step12	no leading-street-dir	Deletes the direction of a main street, such as N (north).
Step13	no trailing-street-suffix	Deletes the suffix of a small street, such as SW.
Step14	no street-suffix	Deletes the suffix of a street, such as platz.
Step15	no number	Deletes the street number, such as number 123.

Step16	no street-number-suffix	Deletes the suffix of the street number, such as number 1/2 of A road.
Step17	no landmark	Deletes the landmark, such as Colombia University.
Step18	no additional-location	Deletes the additional location.
Step19	no name	Deletes the information about a resident, such as Joe's haircut shop.
Step20	no postal-code	Deletes the name of a postal office.
Step21	no building	Deletes the information about a building.
Step22	no unit	Deletes the information about a unit.
Step23	no floor	Deletes the information about a floor.
Step24	no room	Deletes the information about a room.
Step25	no type-of-place	Deletes the type of a place, such as office.
Step26	no postal-community	Deletes the name of a postal office.
Step27	no post-office-box	Deletes the name of a postal box, such as 12345.
Step28	no additional-code	Deletes the additional code.
Step29	no country	Deletes the name of a country.
Step30	no script	Deletes the script.

1.3.11 Specifying a Port to Set the Location Information

The following commands can be used to set the location information for a port and bear the location information in TLV.

Run the following commands in port configuration mode to set the location information:

Procedure	Command	Purpose
Step1	config	Enters the global configuration mode.
Step2	interface intf-type intf-id	Enters the interface configuration mode.
Step3	location civic id	Sets the location information of civic id.
Step4	location elin id	Sets the location information of elin id.

Run the following commands in port configuration mode to delete the location information:

Procedure	Command	Purpose
Step1	config	Enters the global configuration mode.
Step2	interface intf-type intf-id	Enters the interface configuration mode.

Step3	no location civic	Deletes the location information of civic id.
Step4	no location elin	Deletes the location information of elin id.

1.3.12 Configuring Show-Relative Commands

You can observe the information about the neighbor, statistics or port state received by the LLDP module by running show-relative commands..

Run the following commands in EXEC or global configuration mode:

Command	Purpose
Show lldp errors	Displays the error information about the LLDP module.
Show lldp interface interface-name	Displays the information about port state, that is, the transmission mode and the reception mode.
Show lldp neighbors	Displays the abstract information about the neighbor.
Show lldp neighbors detail	Displays the detailed information about the neighbor.
Show lldp traffic	Displays all received and transmitted statistics information.
Show location elin	Displays the information of location elin.
Show location civic	Displays the information of location civic.

1.3.13 Configuring the Deletion Commands

You can delete the received neighbor lists and all statistics information by running the following command.

Run the following commands in EXEC mode:

Command	Purpose
clear lldp counters	Deletes all statistics data.
clear lldp table	Deletes all received neighbor information.

1.4 Configuration Example

1.4.1 Network Environment Requirements

Configure LLDP protocol on the port connecting two switches.

1.4.2 Network Topology

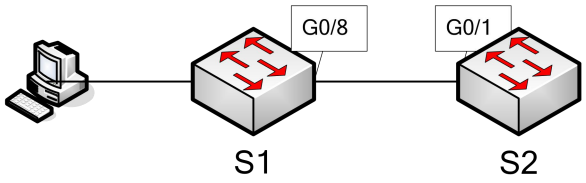


Figure 2 Network Topology

1.4.3 Configuration Procedure

1. Basic Settings

Configuring switch S1:

Switch_config#lldp run

Switch_config#

Configuring switch S2:

Switch_config#lldp run

Switch_config#

The information of Neighbor B will be displayed on Switch A about 1 minute later. MED-TLV information is not sent by default.

S1:

Switch_config#show lldp neighbors

Capability Codes:

(R)Router,(B)Bridge,(C)DOCSIS Cable Device,(T)Telephone

(W)WLAN Access Point, (P)Repeater,(S)Station,(O)Other

Device-ID	Local-Intf	Hldtme	Port-ID	Capability
Switch	Gig0/8	99	Gig0/1	B

Total entries displayed: 1

Switch_config#show lldp neighbors detail

chassis id: 00e0.0fac.32ff

port id: Gig0/1

port description: GigaEthernet0/1

system name: Switch

system description: SWITCH Software, Version 4.1.0B

Serial: S24090103

Compiled: 2011-9-21 9:24:8

Time remaining: 96

system capabilities: R B

enabled capabilities: B

Management Address:

IP: 90.0.0.21

Port VLAN ID: 1

PPVID: 1

VLAN 1 name: Default

Auto Negotiation: supported,enabled

Physical media capabilities:

1000baseX(FD)

1000baseX(HD)

100baseTX(FD)

100baseTX(HD)

Operational MAU type: 2 pair category 5 UTP, full duplex mode(16)

Power Via MDI:

MDI power support --

PSE MDI power support: support

Port class: PSE

PSE MDI power state: enabled

PSE pairs selection control ability: can not be controlled

PSE power pair: signal

Power Classification: Class 0

Link Aggregation:

Aggregation capability: capable of being aggregated

Aggregation status: not currently in aggregation

Maximum frame size: 1500

Total entries displayed: 1

2. TLV Configuration

Configuring switch S1:

Switch_config#lldp run

Switch_config#

Configuring switch S2:

Switch_config#lldp run

Switch_config# no lldp tlv-select system-name

Switch_config#int g0/8

Switch_config_g0/8#no lldp dot1-tlv-select port-vlan-id

Switch_config_g0/8#no lldp dot3-tlv-select max-frame-size

Switch_config_g0/8#

The information of Neighbor B will be displayed on Switch A about 1 minute later, which is highlighted in red. To differentiate, the information displayed in the basic configuration of 1.4.3.1 is highlighted in blue.

S1:

Switch_config#show lldp neighbors

Capability Codes:

(R)Router,(B)Bridge,(C)DOCSIS Cable Device,(T)Telephone

(W)WLAN Access Point, (P)Repeater,(S)Station,(O)Other

Device-ID	Local-Intf	Hldtme	Port-ID	Capability
Switch	Gas0/8	92	Gig0/1	R B

Total entries displayed: 1

Switch_config#show lldp neighbors detail

chassis id: 00e0.0fac.32ff

port id: Gig0/1

port description: GigaEthernet0/1

system name: -- not advertised

system description: SWITCH Software, Version 4.1.0B

Serial: S24090103

Compiled: 2011-9-21 9:24:8

Time remaining: 95

system capabilities: R B

enabled capabilities: B

Management Address:

IP: 90.0.0.21

Port VLAN ID -- not advertised

PPVID: 1

VLAN 1 name: Default

Auto Negotiation: supported,enabled

Physical media capabilities:

1000baseX(FD)

1000baseX(HD)

100baseTX(FD)

100baseTX(HD)

Operational MAU type: 2 pair category 5 UTP, full duplex mode(16)

Power Via MDI:

MDI power support --

PSE MDI power support: support

Port class: PSE

PSE MDI power state: enabled

PSE pairs selection control ability: can not be controlled

PSE power pair: signal

Power Classification: Class 0

Link Aggregation:

Aggregation capability: capable of being aggregated

Aggregation status: not currently in aggregation

Total entries displayed: 1

3. Location Configuration

Configuring switch S1:

Switch_config#lldp run

Switch_config#

Configuring switch S2:

Switch_config#lldp run

Switch_config#location elin identifier 1 1234567890 //Configuring elin information

Switch_config#location civic identifier 1 //Entering location configuration mode

Switch_config_civic#language English

Switch_config_civic#city SiteB

Switch_config_civic#street Curie

Switch_config_civic#script EN //The above configured is civic information

Switch_config_civic#quit

Switch_config#int g0/8

Switch_config_g0/8#location elin 1 //Set elin id for the interface

Switch_config_g0/8#location elin 1 //Set civic id for the interface

Switch_config_g0/8#show location elin //Display elin configuration information

elin information:

elin 1: 1234567890

total: 1

Switch_config_g0/8#show location elin //Display civic configuration information

civic address information:

identifier: 1

City: SiteB

Language: English

Script: EN

Street: Curie

---

total: 1

Switch_config_g0/8#

The information of Neighbor B will be displayed on Switch A about 1 minute later.

S1:

Switch_config#show lldp neighbors

Capability Codes:

(R)Router,(B)Bridge,(C)DOCSIS Cable Device,(T)Telephone

(W)WLAN Access Point, (P)Repeater,(S)Station,(O)Other

Device-ID	Local-Intf	Hldtme	Port-ID	Capability
Switch	Gig0/8	115	Gig0/1	B

Total entries displayed: 1

Switch_config#show lldp neighbors detail

chassis id: 00e0.0fac.32ff

port id: Gig0/1

port description: GigaEthernet0/1

system name: Switch

system description: SWITCH Software, Version 4.1.0B

Serial: S24090103

Compiled: 2011-9-21 9:24:8

Time remaining: 109

system capabilities: R B

enabled capabilities: B

Management Address:

IP: 90.0.0.21

Port VLAN ID: 1

Auto Negotiation: supported,enabled

Physical media capabilities:

1000baseX(FD)

1000baseX(HD)

100baseTX(FD)

100baseTX(HD)

Operational MAU type: 2 pair category 5 UTP, full duplex mode(16)

Power Via MDI:

MDI power support --

PSE MDI power support: support

Port class: PSE

PSE MDI power state: enabled

PSE pairs selection control ability: can not be controlled

PSE power pair: signal

Power Classification: Class 0

MED Information:

MED Codes:

(CA)Capabilities, (NP)Network Policy, (LI)Location Identification

(PS)Power via MDI ¨CPSE, (PD)Power via MDI ¨CPD, (IN)Inventory

Hardware Revision: 0.4.0

Software Revision: 4.1.0B

Serial Number: S24090103

Manufacturer Name:

Model Name: SWITCH

Asset ID: S24090103

Capabilities: CA,NP,LI,PS,IN

Device type: Network Connectivity

Network Policy: Voice

Policy: Unknown

Power requirements:

Type: PSE Device

Source: Unknown

Priority: Low

Value: 150(0.1 Watts)

Civic address location:

Language: English

City: SiteB

Street: Curie

Script: EN

ELIN location:

ELIN: 1234567890

Total entries displayed: 1

Switch_config#

EAPS Configuration

Table of Contents

Chapter 1 Introduction of Fast Ethernet Ring Protection 1
1.1 Overview 1
1.2 Related Concepts of Fast Ether-Ring Protection 1
1.2.1 Roles of Ring's Nodes 2
1.2.2 Role of the Ring's Port 2
1.2.3 Control VLAN and Data VLAN 2
1.2.4 Aging of the MAC Address Table 3
1.2.5 Symbol of a Complete Ring Network 3
1.3 Types of EAPS Packets 3
1.4 Fast Ethernet Ring Protection Mechanism 4
1.4.1 Ring Detection and Control of Master Node 4
1.4.2 Notification of Invalid Link of Transit Node 4
1.4.3 Resuming the Link of the Transit Node 4
Chapter 2 Fast Ethernet Ring Protection Configuration 6
2.1 Default EAPS Settings 6
2.2 Requisites Before Configuration 6
2.3 MEAPS Configuration Tasks 7
2.4 Fast Ethernet Ring Protection Configuration 7
2.4.1 Configuring the Master Node 7
2.4.2 Configuring the Transit Node 8
2.4.3 Configuring the Ring Port 8
2.4.4 Browsing the State of the Ring Protection Protocol 9
2.5 MEAPS configuration 9
2.5.1 Configuration Example 9

Chapter 1 Introduction of Fast Ethernet Ring Protection

1.1 Overview

D-Link Ethernet ring protection protocol is a special type of link-layer protocol specially designed for constructing the ring Ethernet topology. The Ethernet protection protocol can shut down one link in a complete ring topology, preventing the data loop from forming the broadcast storm. If a link is broken, the protocol immediately resumes the link that is previously shut down. In this way, the nodes among the ring network can communicate with each other.

The ring protection protocol and STP are both used for topology control on the link layer. STP is suitable for all kinds of complicated networks, which transmits the change of network topology hop by hop. The ring protection protocol is used for ring topology and adopts the pervasion mechanism to transmit the change of network topology. Therefore, the convergence of the ring protection protocol in the ring network is better than STP. In a sound network, the ring protection protocol can resume network communication within less than 50ms.

Remark:
EAPS supports to set a switch to be a node of multiple physical ring to construct complicated topology.

1.2 Related Concepts of Fast Ether-Ring Protection

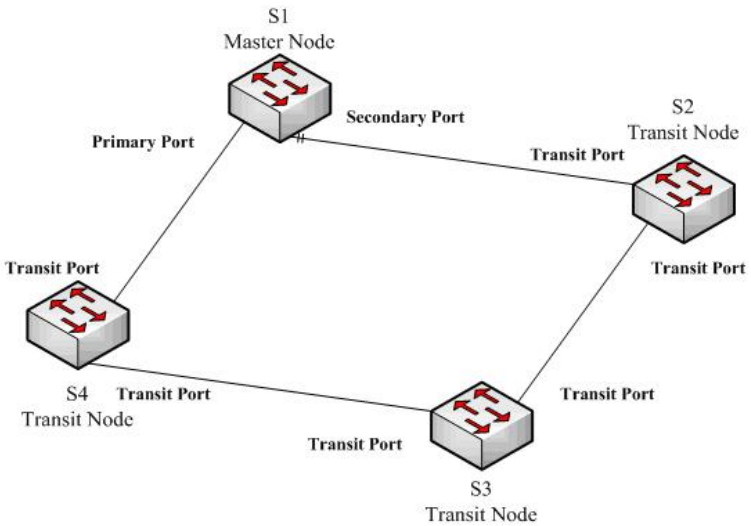


Figure 1.1 EAPS Ethernet ring

1.2.1 Roles of Ring's Nodes

Each switch on an Ethernet ring is a ring node. The ring nodes are classified into master nodes and transit nodes. Only one switch on the Ethernet ring can serve as a mere master node and other switches are worked as transit nodes.

Master node: It positively knows whether the ring's topology is complete, removes loopback, control other switches to update topology information.

Transit node: It only checks the state of the local port of the ring, and notifies the master node of the invalid link.

The role of each node can be specified by user through configuration. The thing is that each switch in the same ring can be set to only one kind of node. In figure 1.1, switch S1 is the master node of ring network, while switches S2, S3 and S4 are transit nodes.

1.2.2 Role of the Ring's Port

EAPS demands each switch has two ports to connect the ring network. Each port of the ring network also needs to be specified through configuration and the protocol supports the following kinds of port roles:

Primary port: the primary port can be configured only on the master node. The master node transmits the ring detection packets through the primary port.

Secondary port: the secondary port can be configured only on the master node. The master node receives the ring detection packets from the secondary port and judges whether the topology of the ring network is complete. In complete topology, the master node blocks the data packets on the secondary port, and prevents loopback from occurring; after a link on the ring network is interrupted, the master node will open the secondary port to forwarding the data packets.

Transit port: the transmit port can only be configured on the transit node. Both ports through which the transit node connects the ring network are all transit ports.

Each port of the ring network can be configured as only one port role after the node's role of the switch and the control VLAN are configured. As shown in figure 1.1, the port through which master node S1 connects transit node S4 is a primary port, the port through which S1 connects S2 is a secondary port, and the ports through which other switches connect the ring network are all transit ports.

Remark:
To configure a same switch to belong to multiple rings, the switch must connect different rings through different physical ports.

1.2.3 Control VLAN and Data VLAN

A private control VLAN is used between master node and transit node to transmit protocol packets. This control VLAN is specified by user through configuration and ring's ports are added also by user to the control VLAN, which guarantees that the protocol packets can be normally forwarded. In general, each port of the ring network is in the forwarding state in the control VLAN and the ports which do not belong to the ring network cannot forward the packets of control VLAN.

Note:
You can specify different control VLAN for each ring on a switch. The control VLAN is only used to forward the control packets of the ring network, not for L2/L3 communication. For example, if the VLAN port that corresponds to the control VLAN is established, the IP address of the VLAN port cannot be pinged through other devices.

The VLANs except the control VLAN are all data VLANs, which are used to transmit the packets of normal services or the management packets.

Note:
The data VLAN can be used for normal L2/L3 communication. For example, you can establish a VLAN port corresponding to data VLAN and configure dynamic routing protocols.

1.2.4 Aging of the MAC Address Table

The Ethernet ring protection protocol can transmit data packets to the correct link by controlling the aging of the switch's MAC address table when the topology changes. In general, the time for a MAC address to age in the MAC address table is 300 seconds. The ring protection protocol can control the aging of the MAC address table in a short time.

1.2.5 Symbol of a Complete Ring Network

Both the master node and the transit node can show whether the current ring network is complete through the state symbol "COMPLETE". On the master node, only when all links of the ring network are normal, the primary port is in forwarding state and the secondary port is in blocking state can the "COMPLETE" symbol be real; on the transit node, only when its two transit ports are in forwarding state can the "COMPLETE" symbol be true.

The state symbol of the ring network helps user to judge the topology state of the current network.

1.3 Types of EAPS Packets

The EAPS packets can be classified into the following types, as shown in table 1.1.

Table 1.1 Types of EAPS packets

Type of the packet	**Remarks**
Loopback detection (HEALTH)	It is transmitted by the master node to detect whether the topology of the ring network is complete.
LINK-DOWN	Indicates that link interruption happens in the ring. This kinds of packets are transmitted by the transit node.
RING-DOWN-FLUSH-FDB	It is transmitted by the master node after interruption of the ring network is detected and the packets show the MAC address aging table of the transit node.

RING-UP-FLUSH-FDB	It is transmitted by the master node after interruption of the ring network is resumed and the packets show the MAC address aging table of the transit node.

1.4 Fast Ethernet Ring Protection Mechanism

1.4.1 Ring Detection and Control of Master Node

The master node transmits the HEALTH packets to the control VLAN through the primary port in a configurable period. In normal case, the HEALTH packets will pass through all other nodes of the ring network and finally arrive at the secondary port of the master node.

The secondary port blocks all data VLANs in primitive condition. When receiving the HEALTH packets continuously, the secondary port keeps blocking data VLANs and blocking the loop. If the secondary port does not receive the HEALTH packets from the primary port in a certain time (which can be configured), it will regard the ring network is out of effect. Then the master node removes the blocking of data VLANs on the secondary port, ages the local MAC address table, and transmits the RING-DOWN-FLUSH-FDB packets to notify other nodes.

If the master node receives the HEALTH packets at the secondary port that is open to data VLANs, the ring network is resumed. In this case, the master node immediately blocks data VLANs on the secondary port, updates the local topology information and reports other nodes to age the MAC address table through RING-UP-FLUSH-FDB packets.

You can configure related commands on the Hello-time node and the Fail-time node to modify the interval for the primary port to transmit the HEALTH packets and the time limit for the secondary port to wait for the HEALTH packets.

1.4.2 Notification of Invalid Link of Transit Node

After the transit port of the transit node is out of effect, the LINK-DOWN packet will be immediately transmitted by the other transit port to notify other nodes. In normal case, the packet passes through other transit nodes and finally arrives at one port of the master node.

After the master node receives the LINK-DOWN packet, it thinks that the ring network is invalid. In this case, the master node removes the blocking of data VLANs on its secondary port, ages the local MAC address table, transmits the RING-DOWN-FLUSH-FDB packet and notifies other nodes.

1.4.3 Resuming the Link of the Transit Node

After the transit port is resumed, it does not immediately transmit the packets of data VLANs, but enters the Pre-Forwarding state. A transit port in pre-forwarding state only transmits and receives the control packets from the control VLAN.

If there is only one transit port invalid in the ring network and when the port enters the pre-forwarding state, the secondary port of the master node can receive the HEALTH packet from the primary port again. In this case, the master node blocks data VLANs on

the secondary port again and transmits the notification of ageing address table outside. After the node with a transit port in pre-forwarding state receives the notification of aging address table, the node will first modify the pre-forwarding port to the forwarding port and then ages the local MAC address table.

If a transit mode does not receives the notification of aging address table from the master node, it thinks that the link to the master node is already out of effect, the transit node will automatically set the pre-forwarding port to be a forwarding one.

You can configure the related commands through the pre-forward-time node to modify the time for the transit port to keep the pre-forwarding state.

Chapter 2 Fast Ethernet Ring Protection Configuration

2.1 Default EAPS Settings

Note:
The fast Ethernet protection protocol cannot be set together with STP.
After STP is disabled, you are recommended to run **spanning-tree bpdu-terminal** to keep the ring node from forwarding BPDU, which leads to the storm.

See the following table:

Table 2.1 Default settings of the Ethernet ring protection protocol and STP.

Spanning tree protocol	**spanning-tree mode rstp**
Fast Ethernet Ring Protection	There is no configuration.

2.2 Requisites Before Configuration

Before configuring MEAPS, please read the following items carefully:

- One of important functions of the ring protection protocol is to stop the broadcast storm, so please make sure that before the ring link is reconnected all ring nodes are configured.If the ring network is connected in the case that the configuration is not finished, the broadcast storm may easily occur.
- EAPS is well compatible with STP, but the port under the control of EAPS is not subject to STP.
- The ring protection protocol supports a switch to configure multiple ring networks.
- Configuring ring control VLAN will lead to the automatic establishment of corresponding system VLAN.
- The port of each ring can forward the packets from the control VLAN of the ring, while other ports, even in the Trunk mode, cannot forward the packets from the control VLAN.
- By default, Fail-time of the master node is triple longer than Hello-time, so that packet delay is avoided from shocking the ring protection protocol. After Hello-time is modified, Fail-time need be modified accordingly.
- By default, Pre-Forward-Time of the transit node is triple longer than Hello-time of the master node so that it is ensured that the master node can detect the recovery of the ring network before the transit port enters the pre-forwarding state. If Hello-time configured on the master node is longer than Fre-Forward-Time of the transit node, loopback is easily generated and broadcast storm is then triggered.

- The physical interface, the fast-Ethernet interface, the gigabit-Ethernet interface and the aggregation interface can all be set to be the ring's interfaces. If link aggregation, 802.1X or port security has been already configured on a physical interface, the physical interface cannot be set to be a ring's interface any more. Note: The versions of D-Linkswitch software prior to version 2.0.1L and the versions of hi-end switch software prior to version 4.0.0M do not support the configuration of the converged port.

2.3 MEAPS Configuration Tasks

- Configuring the Master Node
- Configuring the Transit Node
- Configuring the Ring Port
- Browsing the State of the Ring Protection Protocol

2.4 Fast Ethernet Ring Protection Configuration

2.4.1 Configuring the Master Node

Configure a switch to be the master node of a ring network according to the following steps:

Command	**Purpose**
Switch**#config**	Enters the switch configuration mode.
Switch_config**#ether-ring** *id*	Sets a node and enters the node configuration mode. id: Instance ID
Switch_config_ring**#control-vlan** *vlan-id*	Configures the control VLAN. Vlan-id: ID of the control VLAN
Switch_config_ring**#master-node**	Configures the node type to be a master node.
Switch_config_ring**#hello-time** *value*	This step is optional. Configures the cycle for the master node to transmit the HEALTH packets. Value: It is a time value ranging from 1 to 10 seconds and the default value is 1 second.
Switch_config_ring**#fail-time** *value*	This step is optional. Configures the time for the secondary port to wait for the HEALTH packets. Value: It is a time value ranging from 3 to 30 seconds and the default value is 3 second.
Switch_config_ring**#exit**	Saves the current settings and exits the node configuration mode.

Remark:

The **no ether-ring *id*** command is used to delete the node settings and port settings of the Ethernet ring.

2.4.2 Configuring the Transit Node

Configure a switch to be the transit node of a ring network according to the following steps:

Command	Purpose
Switch**#config**	Enters the switch configuration mode.
Switch_config**#ether-ring** *id*	Sets a node and enters the node configuration mode. id: Instance ID
Switch_config_ring**#control-vlan** *vlan-id*	Configures the control VLAN. Vlan-id: ID of the control VLAN
Switch_config_ring**#transit-node**	Configures the node type to be a transit node.
Switch_config_ring**#pre-forward-time** *value*	This step is optional. Configures the time of maintaining the pre-forward state on the transit port. Value: It is a time value ranging from 3 to 30 seconds and the default value is 3 second.
Switch_config_ring**#exit**	Saves the current settings and exits the node configuration mode.

2.4.3 Configuring the Ring Port

Configure a port of a switch to be the port of Ethernet ring according to the following steps:

Command	Purpose
Switch**#config**	Enters the switch configuration mode.
Switch_config**#interface** *intf-name*	Enters the interface configuration mode. intf-name: Stands for the name of an interface.
Switch_config_intf**#ether-ring** *id* **{primary-port | secondary-port | transit-port }**	Configures the type of the port of Ethernet ring. ID of the node of Ethernet ring
Switch_config_intf**#exit**	Exits from interface configuration mode.

Remark:

The **no ether-ring *id* primary-port** { **secondary-port** | **transit-port** } command can be used to cancel the port settings of Ethernet ring.

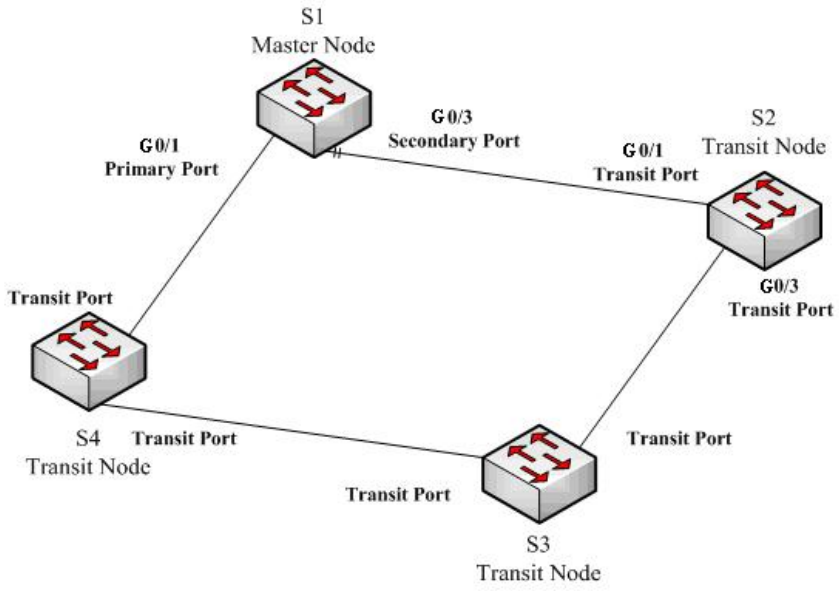
2.4.4 Browsing the State of the Ring Protection Protocol

Run the following command to browse the state of the ring protection protocol:

Command	Purpose
show ether-ring *id*	Browses the summary information about the ring protection protocol and the port of Ethernet ring. id: ID of Ethernet ring
show ether-ring *id* **detail**	Browses the detailed information about the ring protection protocol and the port of Ethernet ring.
show ether-ring *id* **interface** *intf-name*	Browses the state of the Ether-ring port or that of the common port.

2.5 MEAPS configuration

2.5.1 Configuration Example



MEAPS configuration

As shown in figure 2.1, master node S1 and transit node S2 are configured as follows. As to the settings of other nodes, they are same to S2's settings.

Configuring switch S1:

Shuts down STP and configures the Ether-ring node:

S1_config#no spanning-tree

S1_config#ether-ring 1

S1_config_ring1#control-vlan 2

```
S1_config_ring1#master-node
```

The following commands are used to set the time related parameters:

```
S1_config_ring1#hello-time 2
S1_config_ring1#fail-time 6
```

Exits from the node configuration mode:

```
S1_config_ring1#exit
```

Configures the primary port and the secondary port:

```
S1_config#interface gigaEthernet 0/1
S1_config_g0/1#ether-ring 1 primary-port
S1_config_g0/1#exit
S1_config#interface gigaEthernet 0/3
S1_config_g0/3#ether-ring 1 secondary-port
S1_config_g0/3#exit
```

Establishes the control VLAN:

```
S1_config#vlan 2
S1_config_vlan2#exit
S1_config#interface range g0/1 , 3
S1_config_if_range#switchport mode trunk
S1_config_if_range#exit
```

Configuring switch S2:

```
S1_config#no spanning-tree
S1_config#ether-ring 1
S1_config_ring1#control-vlan 2
S1_config_ring1#transit-node
S1_config_ring1#pre-forward-time 8
S1_config_ring1#exit
S1_config#interface gigaEthernet 0/1
S1_config_g0/1#ether-ring 1 transit-port
S1_config_g0/1#exit
S1_config#interface gigaEthernet 0/3
S1_config_g0/3#ether-ring 1 transit-port
S1_config_g0/3#exit
S1_config#vlan 2
S1_config_vlan2#exit
S1_config#interface range gigaEthernet 0/1 , 3
S1_config_if_range#switchport mode trunk
S1_config_if_range#exit
```

IGMP-SNOOPING Configuration

Table of Contents

Chapter 1 IGMP-snooping Configuration....1
1.1 IGMP-snooping Configuration Task....1
1.1.1 Enabling/Disabling IGMP-Snooping of VLAN....1
1.1.2 Adding/Deleting Static Multicast Address of VLAN....2
1.1.3 Configuring immediate-leave of VLAN....2
1.1.4 Configuring Static Routing Interface of VLAN....3
1.1.5 Configuring IPACL of Generating Multicast Forward Table....3
1.1.6 Configuring the Function to Filter Multicast Message Without Registered Destination Addresss....3
1.1.7 Configuring Router Age Timer of IGMP-snooping....4
1.1.8 Configuring Response Time Timer of IGMP-Snooping....4
1.1.9 Configuring Querier of IGMP-Snooping....4
1.1.10 Configuring IGMP-snooping's Querier Time Timer....5
1.1.11 Configuring filter of IGMP-snooping....5
1.1.12 Configuring clear-group of IGMP-snooping....6
1.1.13 Configuring quick-query of IGMP-snooping....6
1.1.14 Configuring decrease-query-report-for-mvc of IGMP-snooping....6
1.1.15 Configuring no-send-special-query of IGMP-snooping....7
1.1.16 Configuring Forward-L3-to-Mrouter of IGMP-Snooping to Forward the Data Packets to the Routing Port....7
1.1.17 Configuring sensitive mode and value for IGMP-snooping....8
1.1.18 Configuring IGMP-snooping's v3-leave-check function....8
1.1.19 Configuring IGMP-snooping's forward-wrongiif-within-vlan function....9
1.1.20 Configuring IGMP-snooping's IPACL function at port....9
1.1.21 Configuring maximum multicast IP address quantity function at IGMP-snooping's port....9
1.1.22 Monitoring and Maintaining IGMP-Snooping....10
1.1.23 IGMP-Snooping Configuration Example....12

Chapter 1 IGMP-snooping Configuration

1.1 IGMP-snooping Configuration Task

The task of IGMP-snooping is to maintain the relationships between VLAN and group address and to update simultaneously with the multicast changes, enabling layer-2 switches to forward data according to the topology structure of the multicast group.

The main functions of IGMP-snooping are shown as follows:

(1) Listening IGMP message;

(2) Maintaining the relationship table between VLAN and group address;

(3) Keeping the IGMP entity of host and the IGMP entity of router in the same state to prevent flooding from occurring.

Note:

Because igmp-snooping realizes the above functions by listening the **query** message and **report** message of igmp, igmp-snooping can function properly only when it works on the multicast router, that is, the switch must periodically receive the igmp **query** information from the router. The **router age** timer of igmp-snooping must be set to a time value that is bigger than the group query period of the multicast router connecting igmp-snooping. You can check the multicast router information in each VLAN by running **show ip igmp-snooping**.

- Enabling/Disabling IGMP-snooping of VLAN
- Adding/Deleting static multicast address of VLAN
- Configuring immediate-leave of VLAN
- Configuring the function to filter multicast message without registered destination address
- Configuring the **Router Age** timer of IGMP-snooping
- Configuring the **Response Time** timer of IGMP-snooping
- Configuring IGMP Querier of IGMP-snooping
- Monitoring and maintaining IGMP-snooping
- IGMP-snooping configuration example

1.1.1 Enabling/Disabling IGMP-Snooping of VLAN

Perform the following configuration in global configuration mode:

Command	Description

ip igmp-snooping [**vlan** *vlan_id*]	Enables IGMP-snooping of VLAN.
no ip igmp-snooping [**vlan** *vlan_id*]	Resumes the default configuration.

If vlan is not specified, all vlans in the system, including vlans created later, can be enabled or disabled.

In the default configuration, IGMP-snooping of all VLANs is enabled, just as the **ip igmp-snooping** command is configured.

Note: IGMP-snooping can run on up to 16 VLANs.

To enable IGMP-snooping on VLAN3, you must first run **no ip IGMP-snooping** to disable IGMP-snooping of all VLANs, then configure **ip IGMP-snooping VLAN 3** and save configuration.

1.1.2 Adding/Deleting Static Multicast Address of VLAN

Hosts that do not support IGMP can receive corresponding multicast message by configuring the static multicast address.

Perform the following configuration in global configuration mode:

Command	Description
ip igmp-snooping vlan *vlan_id* **static** *A.B.C.D* **interface** *intf*	Adds static multicast address of VLAN.
no ip igmp-snooping vlan *vlan_id* **static** *A.B.C.D* **interface** *intf*	Deletes static multicast address of VLAN.

1.1.3 Configuring immediate-leave of VLAN

When the characteristic immediate-leave is configured, the switch can delete the port from the port list of the multicast group after the switch receives the **leave** message. The switch, therefore, does not need to enable the timer to wait for other hosts to join the multicast. If other hosts in the same port belongs to the same group and their users do not want to leave the group, the multicast communication of these users may be affected. In this case, the **immediate-leave** function should not be enabled.

Perform the following configuration in global configuration mode:

Command	Description
ip igmp-snooping vlan *vlan_id* **immediate-leave**	Configures the **immediate-leave** function of the VLAN.
no ip igmp-snooping vlan *vlan_id* **immediate-leave**	Sets immediate-leave of VLAN to its default value.

The **immediate-leave** characteristic of VLAN is disabled by default.

Configure the static routing interface and send the multicast packet to the routing port. The switch will send the multicast report packets to all routing ports in vlan.

Run following commands in the global configuration mode:

Command	Purpose
ip igmp-snooping vlan *vlan_id* **mrouter interface** *intf*	Add the static routing port of VLAN.
no ip igmp-snooping vlan *vlan_id* **mrouter interface** *intf*	Delete the static routing port of VLAN.

1.1.5 Configuring IPACL of Generating Multicast Forward Table

Run following commands to configure IPACl. Thus, The rules and limitations of generating the multicast forwarding table after receiving packets of igmp report can be set.

Command	Purpose
ip igmp-snooping policy *word*	Adds IPACL in generating multicast forwarding table.
no ip igmp-snooping policy	Deletes IPACL in generating multicast forwarding table.

1.1.6 Configuring the Function to Filter Multicast Message Without Registered Destination Addresss

When multicast message target fails to be found (DLF, the destination address is not registered in the switch chip through igmp-snooping), the default process method is to send message on all ports of VLAN.Through configuration, you can change the process method and all multicast messages whose destination addresses are not registered to any port will be dropped.

Command	Description
ip igmp-snooping dlf-drop	Drops multicast message whose destination fails to be found.
no ip igmp-snooping dlf-drop	Resumes the fault configuration (forward).

Note:

(1) The attribute is configured for all VLANs.

1) The default method for the switch to handle this type of message is forward (message of this type will be broadcasted within VLAN).

The **Router Age** timer is used to monitor whether the IGMP inquirer exists. IGMP inquirers maintains multicast addresses by sending **query** message. IGMP-snooping works through communication between IGMP inquier and host.

Perform the following configuration in global configuration mode:

Command	Description
ip igmp-snooping timer router-age *timer_value*	Configures the value of Router Age of IGMP-snooping.
no ip igmp-snooping timer router-age	Resumes the default value of Router Age of IGMP-snooping.

Note:

For how to configure the timer, refer to the query period setup of IGMP inquirer. The timer cannot be set to be smaller than query period. It is recommended that the timer is set to three times of the query period.

The default value of Router Age of IGMP-snooping is 260 seconds.

1.1.8 Configuring Response Time Timer of IGMP-Snooping.

The **response time** timer is the upper limit time that the host reports the multicast after IGMP inquirer sends the **query** message. If the **report** message is not received after the timer ages, the switch will delete the multicast address.

Perform the following configuration in global configuration mode:

Command	Description
ip igmp-snooping timer response-time *timer_value*	Configures the value of Response Time of IGMP-snooping.
no ip igmp-snooping timer response-time	Resumes the default value of Response Time of IGMP-snooping.

Note:

The timer value cannot be too small. Otherwise, the multicast communication will be unstable.

The value of Response Time of IGMP-snooping is set to 15 seconds.

1.1.9 Configuring Querier of IGMP-Snooping

If the multicast router does not exist in VLAN where IGMP-snooping is activated, the **querier** function of IGMP-snooping can be used to imitate the multicast router to regularly send IGMP **query** message. (The function is global, that is, it can be enabled or disabled in VLAN where IGMP-snooping is globally enabled)

routing, the automatic query function of the switch can be activated through IGMP snooping, enabling IGMP snooping to work properly.

Perform the following configuration in global configuration mode:

Command	Description
[**no**] **ip igmp-snooping querier [address** *[ip_addr*]	Configures the querier of IGMP-snooping. The optional parameter **address** is the source IP address of **query** message.

The **IGMP-snooping querier** function is disabled by default. The source IP address of fake **query** message is 10.0.0.200 by default.

Note:

If the **querier** function is enabled, the function is disabled when the multicast router exists in VLAN; the function can be automatically activated when the multicast router times out.

1.1.10 Configuring IGMP-snooping's Querier Time Timer

Querier Time Timer is the time interval when switch as local IGMP querier sends messages. Timer broadcasts query message within VLAN after aging.

Configure as following under global configuration mode:

Command	Operation
ip igmp-snooping querier querier-timer *timer_value*	Configures the value of IGMP-snooping's Querier Time
no ip igmp-snooping querier querier-timer	Recovers IGMP-snooping's Querier Time as default

By default IGMP-snooping querier is shut down. The default time interval of Query messages is 200 seconds.

Notice:

If Querier function is initiated, querier-timer should not be set as too long. In subnet if there are other switches with querier initiated, long querier-timer (longer than other switch's router-age) would lead to the instablization of querier selection in subnet.

1.1.11 Configuring filter of IGMP-snooping

The command is used to enable IGMP-snooping filter, the switch only enables the configured multicast group in the filter to add group.

Configure as following under port configuration mode:

Command	Purpose
[no] ip igmp-snooping filter	Configures filter of IGMP-snooping, the optional parameter: address is the multicast group

By default the function “IGMP-snooping filter” is disabled. All multicast addresses can add groups.

Note:

Only an arbitrary address is configured can the filter function takes effect. Delete all addresses and the filter function is disabled.

1.1.12 Configuring clear-group of IGMP-snooping

The command is used to delete all multicast groups recorded by igmp-snooping in the switch.

Configure as following under global configuration mode:

Command	Purpose
ip igmp-snooping clear-group	Delete all multicast groups manually

Note:

The command is used to delete all multicast groups in non-service condition.

1.1.13 Configuring quick-query of IGMP-snooping

If enable quick of IGMP-snooping, there is port up, send igmp query packets to the port directly.

Configure as following under global configuration mode:

Command	Purpose
[no] ip igmp-snooping quick-query	Enables the command and if there is port up, send igmp query packets to port up.

Note:

If quick-query is enabled, send query to the new port when there is up of the port. The function is applicable to the downstream host of not actively sending join packets.

1.1.14 Configuring decrease-query-report-for-mvc of IGMP-snooping

If to enable descrease-query-report of IGMP-snooping, the command works after enabling mvc. The command is used to decrease igmp-snooping forwarding or protocol packets of the broadcast in mvc mode.

Configure as following under global configuration mode:

Command	Purpose
[no] ip igmp-snooping decrease-query-report-for-mvc	Configures decrease-query-report-for-mvc of IGMP-snooping. Decrease the number of protocol packet in the mode of mvc after the command is enabled.

By default, igmp-snooping and mvc will collaboratively send igmp protocol packets, which will increase the number of packets.

Note: If the function is enabled, it is not applicable to the condition of igmp-snooping and mvc working collaboratively.

1.1.15 Configuring no-send-special-query of IGMP-snooping

If no-send-special-query of IGMP-snooping is enabled and querier is disabled, special query will not be forwarded after receiving leave packets.

Configure as following under global configuration mode:

Command	Purpose
[**no**] **ip igmp-snooping no-send-special-query**	Configure no-send-special-query of IGMP-snooping

By default, special-query packets will be forwarded only leave packets are received.

Note:

If Querier is enabled, the command will not take effect.

1.1.16 Configuring Forward-L3-to-Mrouter of IGMP-Snooping to Forward the Data Packets to the Routing Port

If L3 multicast feature is initiated and igmp-snooping does not join messages to downstream port, only downstream vlan port can be learnt by multicast route. If forward-l3-to-mrouter function is intiated, all the downstream router ports can be learned. Data messages could be sent to multicast router pot registered by PIM-SM message not broadcasting messages to all downstream physical port. The command is mainly used under the following conditions.

When L3 multicast is enabled in multiple switch cascading, the upstream devices can only learn the downstream vlan ports through the multicast routing protocol and there is no IGMP packet exchange between the upstream and downstream devices. Hence the snooping of the upstream devices cannot learn the specific physical ports that the downstream devices connect and the upstream devices will send the multicast packets to all physical ports in the local vlan. After this command is enabled, the upstream devices can forward the multicast packets to

packets to be broadcast in the downstream vlan.

Run the following commands in global configuration mode.

Command	Purpose
[**no**] **ip igmp-snooping forward-l3-to-mrouter**	Sets the forward-l3-to-mrouter function of IGMP-snooping.

By default, the IGMP-snooping forward-l3-to-mrouter is disabled.

Note:

This command can be used to send the data packets to the multicast routing port, but the switchchip can limit the source-data-port, so the data packets will not be sent to the port of source data, but to the downstream multicast routing port that is registered on PIM-SM.

1.1.17 Configuring sensitive mode and value for IGMP-snooping

If IGMP-snooping's sensitive mode is enabled, when port at trunk mode is shut down, set router-age time of mrouter at active status as sensitive value, and send out query message quickly.

Configure as following under global configuration mode:

Command	Purpose
[**no**] **ip igmp-snooping sensitive** [value [3-30]]	Configuring IGMP-snooping's sensitive and value could be router-age time of currently active mrouter.

By default IGMP-snooping sensitive is disabled.

Notice:

When it is sensitive mode, sensitive value is used to update router-age aiming at current one time period. Next time, route-age is recovered as configured time router-age time.

1.1.18 Configuring IGMP-snooping's v3-leave-check function

If IGMP-snooping's v3-leave-check feature is enabled, send special query message after receiving v3's leave message. Otherwise, no operation is processed.

Configure as following under global configuration mode:

Command	Purpose
[**no**] **ip igmp-snooping**	Configuring IGMP-snooping's v3-leave-check. Send special query message after receiving v3 leave message.

1.1.19 Configuring IGMP-snooping's forward-wrongiif-within-vlan function

If IGMP-snooping's forward-wrongiif-within-vlan function is enabled, do L2 forwarding of the multicast data message received from wrong vlan interface port within source vlan. Forward messages to the group member ports in the vlan. Otherwise, drop messages.

Configure as following under global configuration mode:

Command	Purpose
[**no**] **ip igmp-snooping forward-wrongiif-within-vlan**	Configuring IGMP-snooping's forward-wrongiif-within-vlan and forwarding relative group member ports within the vlan

By default IGMP-snooping forward-wrongiif-within-vlan is enabled.

Notice:

Command ip igmp-snooping forward-wrongiif-within-vlan is only meaningful when L3 multicast is enabled.

1.1.20 Configuring IGMP-snooping's IPACL function at port

If IGMP-snooping's IPACL function at port is enabled, use IPACL at port to assign whether messages of some multicast IP address need to be dealt with or ignored.

Configure as following under physical port configuration mode:

Command	Purpose
ip igmp-snooping policy *word*	Adding multicast message's IPACL which need to be dealt with port.
no ip igmp-snooping policy	Deleteding multicast message's IPACL which need to be dealt with port.

1.1.21 Configuring maximum multicast IP address quantity function at IGMP-snooping's port

If configuring the maximum multicast IP address quantity at IGMP-snooping port, the quantity of applied groups at the port would be judged whether it is beyond the configured maximum quantity when IGMP-snooping generates forwarding entry. If it is beyond the maximum quantity, the port's entry would not be generated.

Configure as following under physical port configuration mode:

Command	Purpose

	[**no**] **ip igmp-snooping limit** [value [1-2048]]	configuring the maximum multicast IP address quantity at IGMP-snooping port

By default the maximum quantity is 2048 at IGMP-snooping.

1.1.22 Monitoring and Maintaining IGMP-Snooping

Perform the following operations in management mode:

Command	Purpose
show ip igmp-snooping	Displays IGMP-snooping configuration information.
show ip igmp-snooping timer	Displays the clock information of IGMP-snooping.
show ip igmp-snooping groups	Displays information about the multicast group of IGMP-snooping.
show ip igmp-snooping statistics	Displays statistics information about IGMP-snooping.
[**no**] **debug ip igmp-snooping** [**packet** | **timer** | **event** | **error**]	Enables and disables packet/clock debug/event/mistake print switch of IGMP-snooping. If the debug switch is not specified, all debug switches will be enabled or disabled.

Display VLAN information about IGMP-snooping running:

```
switch # show ip igmp-snooping
Global IGMP snooping configuration:
----------------------------------
Globally enable          : Enabled
VLAN nodes               : 1,50,100,200,400,500
Dlf-frames filtering : Disabled
Sensitive                : Disabled
Querier                  : Enabled
Querier address          : 10.0.0.200
Querier interval         : 140 s
Router age               : 260 s
Response time            : 15 s

   vlan_id     Immediate-leave     Ports     Router Ports
-------------------------------------------------------------
       1            Disabled          5-10       SWITCH(querier);
      50            Disabled          1-4        SWITCH(querier);
     100            Disabled          NULL       SWITCH(querier);G0/1(static);
     200            Disabled          NULL       SWITCH(querier);
     400            Disabled          NULL       SWITCH(querier);
     500            Disabled          NULL       SWITCH(querier);
```

```
switch# show ip igmp-snooping groups
          The total number of groups          2

 Vlan Group          Type Port(s)
---- --------------- ---- -----------------------------------------------------
 1 226.1.1.1         IGMP G0/1                    G0/3
 1 225.1.1.16        IGMP G0/1                    G0/3
```

Display IGMP-snooping timer:

```
switch#show ip igmp-snooping timers
vlan 1 router age : 251 Indicating the timeout time of the router age timer
vlan 1 multicast address 0100.5e00.0809 response time : 1    Indicating the period from when the
  last multicast group query message is received to the current time; if no host on the port respond
  when the timer times out, the port will be deleted..
```

Display IGMP-snooping statistics:

```
switch#show ip igmp-snooping statistics
vlan 1
------------
      v1_packets:0          IGMP v1    packet number
      v2_packets:6          IGMP v2    packet number
      v3_packets:0          IGMP v3    packet number
      general_query_packets:5       General query of the packet number
      special_query_packets:0       Special query of the packet number
      join_packets:6        Number of report packets
      leave_packets:0       Number of Leave packets
      send_query_packets:0        Rserved statistics option
      err_packets:0         Number of incorrect packets
```

Debug the message timer of IGMP-snooping:

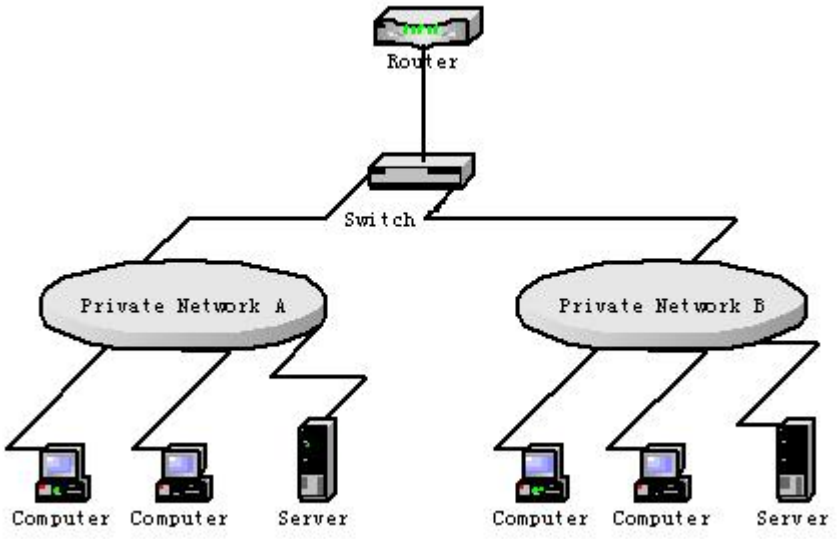
```
switch#debug ip igmp-snooping packet
Jan   1 02:22:28 IGMP-snooping: Receive IGMPv3 report from F0/1, vlan 1:
Jan   1 02:22:28 IGMP-snooping: Flood packet from F0/1 to vlan 1 rc = 0.
Jan   1 02:22:29 IGMP-snooping: Receive IGMPv3 report from F0/1, vlan 1:
Jan   1 02:22:29 IGMP-snooping: Flood packet from F0/1 to vlan 1 rc = 0.
Jan   1 02:22:38 IGMP-snooping: Receive IGMPv3 report from F0/1, vlan 1:
Jan   1 02:22:38 IGMP-snooping: Flood packet from F0/1 to vlan 1 rc = 0.
Jan   1 02:22:39 IGMP-snooping: Receive IGMPv3 report from F0/1, vlan 1:
Jan   1 02:22:39 IGMP-snooping: Flood packet from F0/1 to vlan 1 rc = 0.
Jan   1 02:23:11 IGMP-snooping: Receive IGMPv3 report from F0/1, vlan 1:
Jan   1 02:23:11 IGMP-snooping: Flood packet from F0/1 to vlan 1 rc = 0.
Jan   1 02:23:12 IGMP-snooping: Receive IGMPv3 report from F0/1, vlan 1:
Jan   1 02:23:12 IGMP-snooping: Flood packet from F0/1 to vlan 1 rc = 0.
```

Debug the message timer of IGMP-snooping:

Jan 1 02:30:36 IGMP-snooping: Vlan 1 router on interface (null) expiry.
Jan 1 02:30:36 IGMP-snooping: Vlan 100 router on interface (null) expiry.
Jan 1 02:30:36 IGMP-snooping: Vlan 200 router on interface (null) expiry.
Jan 1 02:30:36 IGMP-snooping: Vlan 400 router on interface (null) expiry.
Jan 1 02:30:36 IGMP-snooping: Vlan 500 router on interface (null) expiry. Inquerying the response timer expiry

1.1.23 IGMP-Snooping Configuration Example

Figure 1 shows network connection of the example.



Configuring Switch

(1) Enable IGMP-snooping of VLAN 1 connecting Private Network A.

Switch_config#ip igmp-snooping vlan 1

(2) Enable IGMP-snooping of VLAN 2 connecting Private Network B.

Switch_config#ip igmp-snooping vlan 2

IGMP-PROXY Configuration

Table of Contents

Chapter 1 IGMP-Proxy Configuration....1
1.1 IGMP-proxy Configuration Tasks.... 1
1.1.1 Enabling/Disabling IGMP-Proxy....1
1.1.2 Adding/Deleting VLAN Agent Relationship.... 2
1.1.3 Adding/Deleting Static Multicast Source Entries.... 2
1.1.4 Monitoring and Maintaining IGMP-Proxy.... 2
1.1.5 IGMP-Proxy Configuration Example....3

Chapter 1 IGMP-Proxy Configuration

1.1 IGMP-proxy Configuration Tasks

The IGMP Proxy allows the VLAN where the multicast user is located to receive the multicast source from other VLANs. The IGMP Proxy runs on layer 2 independently without other multicast routing protocols. IGMP proxy will be transmitted by the IGMP packets of the proxied VLAN to the proxying VLAN and maintain the hardware forward table of the multicast user of the agent VLAN according to these IGMP packets. IGMP proxy divides different VLANs into two kinds: proxied VLANs and proxying VLANs. The downstream multicast VLANs can be set to the proxied VLANs, while the upstream multicast VLANs can be set to the proxying VLANs.

Although IGMP proxy is based on IGMP snooping, two are independent in application; IGMP Snooping will not be affected when IGMP proxy is enabled or disabled, while IGMP proxy can run only when IGMP Snooping is enabled.

IGMP proxy cannot be used unless the following conditions are met:

1. L3 switch
2. Avoiding to enable IP multicast routing at the same time
3. Preventing a vlan to act as downstream vlan and also upstream vlan

- Enabling/Disabling IGMP-Proxy
- Adding/deleting VLAN agent relationship
- Adding/deleting static multicast source entries
- Monitoring and Maintaining IGMP-Proxy
- Setting the Example of IGMP Proxy

1.1.1 Enabling/Disabling IGMP-Proxy

Run the following commands in global configuration mode.

Command	Purpose
ip igmp-proxy enable	Enables IGMP proxy.
no ip igmp-proxy enable	Resumes the default settings.

Note: IGMP-proxy cannot be enabled after IP multicast-routing is enabled. The previously enabled IGMP proxy is automatically shut down if IP multicast routing is enabled. The shutdown of ip multicast-routing will not lead to the automatic enablement of IGMP proxy.

1.1.2 Adding/Deleting VLAN Agent Relationship

Run the following commands in global configuration mode.

Command	Purpose
ip igmp-proxy agent-vlan a*vlan_map* **client-vlan map** c*vlan_map*	Adds the agent VLAN (avlan_map) to manage the represented vlan (cvlan_map).
no ip igmp-proxy agent-vlan a*vlan_map* **client-vlan map** c*vlan_map*	Deletes the agent relationship.

Note:

1. The represented VLAN cannot be configured before vlan is designated by avlan_map; also, the agent VLAN cannot be configured before cvlan_map.

2. The represented and agent VLANs must accept the control of IGMP-Snooping.

1.1.3 Adding/Deleting Static Multicast Source Entries

Run the following commands in global configuration mode.

Command	Purpose
ip igmp-proxy source multi_ip src_ip **svlan** vlan_id **sport** intf_name	Adds entries of the static source multicast.
no ip igmp-proxy source multi_ip src_ip **svlan** vlan_id **sport** intf_name	Deletes entries of the static source multicast.

Note: The SVLAN mentioned here is the multicast source VLAN and the vlan ID of SVLAN cannot be that of represented VLAN.

1.1.4 Monitoring and Maintaining IGMP-Proxy

Run the following commands in EXEC mode:

Command	Operation
show ip igmp-proxy	Displays the information about IGMP proxy.
show ip igmp-proxy mcache *[delete* | *nonsync* | *sync*| *static]*	Displays the forwarding cache of IGMP proxy. delete: display those entries of which hardware caches are deleted but software caches do not time out. nonsync: display those entries that have been processed but not yet synchronized to the hardware

	Sync: display those entries already in the hardware cache. All entries are to be displayed if no filtration conditions are specified. static: only display the entries of static multicast cache.
[**no**] **debug ip igmp-proxy** *[error | event | packet]*	Enables or disables the IGMP-proxy debug switch.

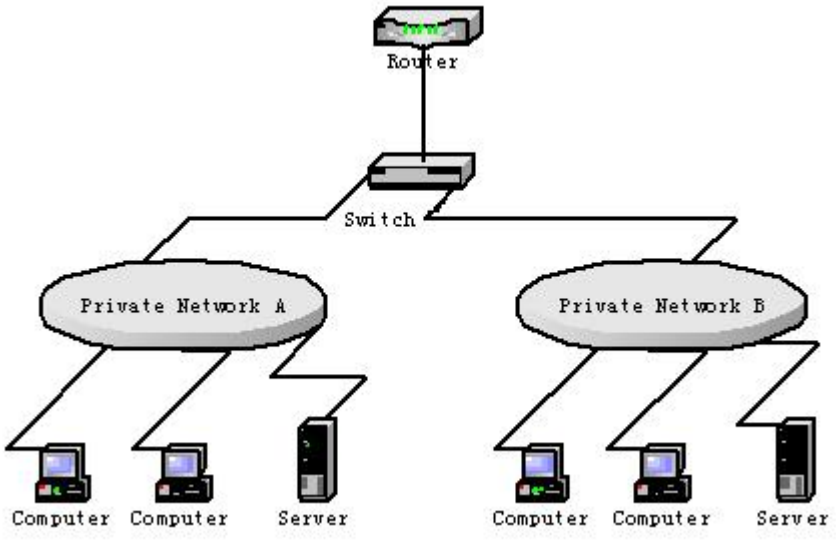
The following example shows how to display the forwarding caches of IGMP proxy:

```
Switch# show ip igmp-proxy mcache
Codes: '+' synchronization, '-' deleted, 'S' static
          '^' unsynchronization

Item 1: Group 225.1.1.2
     +(192.168.213.163, 2, G3/24)
      VLAN 3,4
```

1.1.5 IGMP-Proxy Configuration Example

The network topology is shown in figure 1.



Switch configuration:

(1) Enable IGMP snooping and IGMP proxy.

Switch_config#ip igmp-snooping

Switch_config#ip igmp-proxy enable

(2) Add VLAN 2 as the agent VLAN of the represented VLAN 3.

Switch_config#ip igmp-proxy agent-vlan 2 client-vlan map 3

DHCP-Snooping Configuration

Table of Contents

Chapter 1 DHCP-Snooping Configuration 1
1.1 IGMP-Snooping Configuration Tasks 1
1.1.1 Enabling/Disabling DHCP-Snooping 1
1.1.2 Enabling DHCP-Snooping in a VLAN 1
1.1.3 Enabling DHCP anti-attack in a VLAN 2
1.1.4 Setting an Interface to a DHCP-Trusting Interface 2
1.1.5 Enabling/Disabling binding table fast update function 2
1.1.6 Enabling DAI in a VLAN 3
1.1.7 Setting an Interface to an ARP-Trusting Interface 3
1.1.8 Enabling Source IP Address Monitoring in a VLAN 3
1.1.9 Setting an Interface to the One Which is Trusted by IP Source Address Monitoring 3
1.1.10 Setting DHCP-Snooping Option 82 4
1.1.11 Setting the Policy of DHCP-Snooping Option82 Packets 5
1.1.12 Setting the TFTP Server for Backing up Interface Binding 6
1.1.13 Setting a File Name for Interface Binding Backup 6
1.1.14 Setting the Interval for Checking Interface Binding Backup 6
1.1.15 Setting Interface Binding Manually 7
1.1.16 Monitoring and Maintaining DHCP-Snooping 7
1.1.17 Example of DHCP-Snooping Configuration 8

Chapter 1 DHCP-Snooping Configuration

1.1 IGMP-Snooping Configuration Tasks

DHCP-Snooping is to prevent the fake DHCP server from providing the DHCP service by judging the DHCP packets, maintaining the binding relationship between MAC address and IP address. The L2 switch can conduct the DAI function and the IP source guard function according to the binding relationship between MAC address and IP address. The DHCP-snooping is mainly to monitor the DHCP packets and dynamically maintain the MAC-IP binding list. The L2 switch filters the packets, which do not meet the MAC-IP binding relationship, to prevent the network attack from illegal users.

- Enabling/Disabling DHCP-Snooping
- Enabling DHCP-Snooping in a VLAN
- Enabling DHCP anti-attack in a VLAN.
- Setting an Interface to a DHCP-Trusting Interface
- Enabling/Disabling binding table fast update function
- Enabling DAI in a VLAN
- Setting an Interface to an ARP-Trusting Interface
- Enabling Source IP Address Monitoring in a VLAN
- Setting anInterface to the One Which is Trusted by IP Source Address Monitoring
- Setting DHCP-Snooping Option 82
- Setting the Policy of DHCP-Snooping Option82 Packets
- Setting the TFTP Server for Backing up Interface Binding
- Setting a File Name for Interface Binding Backup
- Setting the Interval for Checking Interface Binding Backup
- Setting Interface Binding Manually
- Monitoring and Maintaining DHCP-Snooping
- Example of DHCP-Snooping Configuration

1.1.1 Enabling/Disabling DHCP-Snooping

Run the following commands in global configuration mode.

Command	Purpose
ip dhcp-relay snooping	Enables DHCP-snooping.
no ip dhcp-relay snooping	Resumes the default settings.

This command is used to enable DHCP snooping in global configuration mode. After this command is run, the switch is to monitor all DHCP packets and form the corresponding binding relationship.

Note: If the client obtains the address of a switch before this command is run, the switch cannot add the corresponding binding relationship.

1.1.2 Enabling DHCP-Snooping in a VLAN

If DHCP snooping is enabled in a VLAN, the DHCP packets which are received from all distrusted physical ports in a VLAN will be legally checked. The DHCP response packets which are received from distrusted physical ports in a VLAN will then be dropped, preventing

DHCP request packet from distrusted ports, if the hardware address field in the DHCP request packet does not match the MAC address of this packet, the DHCP request packet is then thought as a fake packet which is used as the attack packet for DHCP DOS and then the switch will drop it.

Run the following commands in global configuration mode.

Command	Purpose
ip dhcp-relay snooping vlan *vlan_id*	Enables DHCP-snooping in a VLAN.
no ip dhcp-relay snooping vlan *vlan_id*	Disables DHCP-snooping in a VLAN.

1.1.3 Enabling DHCP anti-attack in a VLAN.

To enable attack prevention in a VLAN, you need to configure the allowable maximum DHCP clients in a specific VLAN and conduct the principle of “first come and first serve”. When the number of users in the specific VLAN reaches the maximum number, new clients are not allowed to be distributed.

Run the following commands in global configuration mode.

Command	Purpose
ip dhcp-relay snooping vlan *vlan_id* **max-client** *number*	Enabling DHCP anti-attack in a VLAN.
no ip dhcp-relay snooping vlan *vlan_id* **max-client**	Disables DHCP anti-attack in a VLAN.

1.1.4 Setting an Interface to a DHCP-Trusting Interface

If an interface is set to be a DHCP-trusting interface, the DHCP packets received from this interface will not be checked.

Run the following commands in physical interface configuration mode.

Command	Operation
dhcp snooping trust	Setting an Interface to a DHCP-Trusting Interface
no dhcp snooping trust	Resumes an interface to a DHCP-distrusted interface.

The interface is a distrusted interface by default.

1.1.5 Enabling/Disabling binding table fast update function

This function is disabled by default. When this function is disabled and a port has been bound to client A, the DHCP request of the same MAC address on other ports will be regarded as a fake MAC attack even if client A is off line.

When this function is enabled, the above-mentioned case will not occur.

It is recommended to use this function in case that a client frequently changes its port and address lease, distributed by DHCP server, cannot be modified to a short period of time.

Command	Operation
ip dhcp-relay snooping rapid-refresh-bind	Enables the fast update function of the binding table.

no ip dhcp-relay snooping rapid-refresh-bind	Disables the fast update function of the binding table.

1.1.6 Enabling DAI in a VLAN

When dynamic ARP monitoring is conducted in all physical ports of a VLAN, a received ARP packet will be rejected if the source MAC address and the source IP address of this packet do not match up with the configured MAC-IP binding relationship. The binding relationship on an interface can be dynamically bound by DHCP or configured manually. If no MAC addresses are bound to IP addresses on a physical interface, the switch rejects forwarding all ARP packets.

Command	Operation
ip arp inspection vlan *vlanid*	Enables dynamic ARP monitoring on all distrusted ports in a VLAN.
no ip arp inspection vlan *vlanid*	Disables dynamic ARP monitoring on all distrusted ports in a VLAN.

1.1.7 Setting an Interface to an ARP-Trusting Interface

ARP monitoring is not enabled on those trusted interfaces. The interfaces are distrusted ones by default.

Run the following commands in interface configuration mode.

Command	Operation
arp inspection trust	Setting an Interface to an ARP-Trusting Interface
no arp inspection trust	Resumes an interface to an ARP-distrusting interface.

1.1.8 Enabling Source IP Address Monitoring in a VLAN

After source IP address monitoring is enabled in a VLAN, IP packets received from all physical ports in the VLAN will be rejected if their source MAC addresses and source IP addresses do not match up with the configured MAC-to-IP binding relationship. The binding relationship on an interface can be dynamically bound by DHCP or configured manually. If no MAC addresses are bound to IP addresses on a physical interface, the switch rejects forwarding all IP packets received from the physical interface.

Run the following commands in global configuration mode.

Command	Operation
ip verify source vlan *vlanid*	Enables source IP address checkup on all distrusted interfaces in a VLAN.
no ip verify source vlan *vlanid*	Disables source IP address checkup on all interfaces in a VLAN.

Note: If the DHCP packet (also the IP packet) is received, it will be forwarded because global snooping is configured.

1.1.9 Setting an Interface to the One Which is Trusted by IP Source Address Monitoring

interface.

Run the following commands in interface configuration mode.

Command	Operation
ip-source trust	Sets an interface to the one with a trusted source IP address.
no ip-source trust	Resumes an interface to the one with a distrusted source IP address.

1.1.10 Setting DHCP-Snooping Option 82

Option 82 brings the local information to a server and helps the server to distribute addresses to clients.

Run the following commands in global configuration mode.

Command	Operation
ip dhcp-relay snooping information option	Sets that option82, which is in the default format, is carried when DHCP-snooping forwards the DHCP packets.
no ip dhcp-relay snooping information option	Sets that option82 is not carried when DHCP-snooping forwards the DHCP packets.

To specify the format of option82, conduct the following settings in global mode.

Command	Operation
ip dhcp-relay snooping information option format {snmp-ifindex/manual/hn-type / cm-type/ [host]}	Sets the format of option82 that the DHCP packets carry when they are forwarded by DHCP-Snooping.
no ip dhcp-relay snooping information option format {snmp-ifindex/manual/hn-type /cm-type/[[host]}	Sets that option82 is not carried when DHCP-snooping forwards the DHCP packets.

If a manual mode is set to enter in option82, conduct the following configurations in interface mode to set the circuit-id:

Command	Operation
dhcp snooping information circuit-id string [STRING]	If option82 is set to be in the manual format, you need to set DHCP-snooping to forward DHCP packets with bearing of option82, whose content is the character string written by STRING. This command is set on the port that connects the client.
dhcp snooping information circuit-id **hex [***xx-xx-xx-xx-xx-xx***]**	If option82 is set to be in the manual format, you need to set DHCP-snooping to forward DHCP packets with bearing of option82, whose content is the Hex system..

	This command is set on the port that connects the client.
no dhcp snooping information circuit-id	Deletes the manually configured option82 circuit-id.

If a manual mode is set to enter in option82, conduct the following configurations in interface mode to set the remote-id:

Command	Operation
dhcp snooping information remote-id string [STRING]	If option82 is set to be in the manual format, you need to set DHCP-snooping to forward DHCP packets with bearing of option82, whose content is the character string written by STRING. This command is set on the port that connects the client.
dhcp snooping information remote-id **hex [***xx-xx-xx-xx-xx-xx***]**	If option82 is set to be in the manual format, you need to set DHCP-snooping to forward DHCP packets with bearing of option82, whose content is the Hex system.. This command is set on the port that connects the client.
no dhcp snooping information remote-id	Deletes the manually configured option82 remote-id.

If a manual mode is set to enter in option82, conduct the following configurations in interface mode to set the vendor-specific:

Command	Operation
dhcp snooping information vendor-specific string STRING	If option82 is set to be in the manual format, you need to set DHCP-snooping to forward DHCP packets with bearing of option82, whose content is the character string written by STRING. This command is set on the port that connects the client.
dhcp snooping information vendor-specific hex [*xx-xx-xx-xx-xx-xx***]**	If option82 is set to be in the manual format, you need to set DHCP-snooping to forward DHCP packets with bearing of option82, whose content is the Hex system.. This command is set on the port that connects the client.
no **dhcp snooping information vendor-specific**	Deletes the manually configured option82 vendor-specific.

1.1.11 Setting the Policy of DHCP-Snooping Option82 Packets

You can set the policy for the DHCP request packets, which carry with option82, after these packets are received. The policies include the following ones:

“Drop” policy: Run the following command in port mode to drop the request packets with option82.

Command	Operation
dhcp snooping information drop	Drops the request packets that contain option82.

option82.

Command	Operation
dhcp snooping information append	Enables the function to add option82 on a port.
dhcp snooping information append first-subop9-param { hex *xx-xx-xx-xx-xx-xx* **| vlanip | hostname }**	Stands for the first parameter carried by option82 vendor-specific (suboption9).
dhcp snooping information append second-subop9-param { hex *xx-xx-xx-xx-xx-xx* **| vlanip | hostname }**	Stands for the second parameter carried by option82 vendor-specific (suboption9).

1.1.12 Setting the TFTP Server for Backing up Interface Binding

After the switch configuration is rebooted, the previously-configured interface binding will be lost. In this case, there is no binding relationship on this interface. After source IPaddress monitoring is enabled, the switch rejected forwarding all IP packets. After the TFTP server is configured for interface binding backup, the binding relationship will be backed up to the server through the TFTP protocol. After the switch is restarted, the switch automatically downloads the binding list from the TFTP server, securing the normal running of the network.

Run the following commands in global configuration mode.

Command	Operation
ip dhcp-relay snooping database-agent *ip-address*	Configures the IP address of the TFTP server which is to back up interface binding.
no ip dhcp-relay snooping database-agent *ip-address*	Cancels the TFTP Server for backing up interface binding.

1.1.13 Setting a File Name for Interface Binding Backup

When backing up the interface binding relationship, the corresponding file name will be saved on the TFTP server. In this way, different switches can back up their own interface binding relationships to the same TFTP server.

Run the following commands in global configuration mode.

Command	Operation
ip dhcp-relay snooping db-file *name* [timestamp]	Configures a file name for interface binding backup.
no ip dhcp-relay snooping db-file	Cancels a file name for interface binding backup.

1.1.14 Setting the Interval for Checking Interface Binding Backup

check whether the binding relationship updates after a certain interval. If the binding relationship updates, it need be backed up again. The default time interval is 30mins.

Run the following commands in global configuration mode.

Command	Operation
ip dhcp-relay snooping write-immediately	Configures DHCP Snooping immediate backup when the binding information changes. no ip dhcp-relay snooping {write-time | write-immediately} Resumes the interval of checking interface binding backup to the default settings.
ip dhcp-relay snooping write-time *num*	Configures the interval for checking interface binding backup. The unit is min.
no ip dhcp-relay snooping write-time	Resumes the interval of checking interface binding backup to the default settings.

1.1.15 Setting Interface Binding Manually

If a host does not obtain the address through DHCP, you can add the binding item on an interface of a switch to enable the host to access the network. You can run no ip source binding MAC IP to delete items from the corresponding binding list.

Note that the manually-configured binding items have higher priority than the dynamically-configured binding items. If the manually-configured binding item and the dynamically-configured binding item have the same MAC address, the manually-configured one updates the dynamically-configured one. The interface binding item takes the MAC address as the unique index.

Run the following commands in global configuration mode.

Command	Operation
ip source binding *MAC IP* interface *name* [vlan *vlan-id*]	Configures Interface Binding Manually
no ip source binding *MAC IP* vlan *vlan-id*	Cancels an interface binding item.

1.1.16 Monitoring and Maintaining DHCP-Snooping

Run the following commands in EXEC mode:

Command	Operation
show ip dhcp-relay snooping	Displays the information about DHCP-snooping configuration.
show ip dhcp-relay snooping binding	Displays the effective address binding items on an interface.
show ip dhcp-relay snooping binding all	Displays all binding items which are generated by DHCP snooping.
[**no**] **debug ip dhcp-relay** [snooping |	Enables or disables the switch of DHCP

binding | event | all]	relay snooping binding or event.

The following shows the information about the DHCP snooping configuration.

```
switch#show ip dhcp-relay snooping
 ip dhcp-relay snooping vlan 3
ip arp inspection vlan 3
DHCP Snooping trust interface:
   GigaEthernet0/1
ARP Inspect interface:
   GigaEthernet0/11
```

The following shows the binding information about dhcp-relay snooping:

```
switch#show ip dhcp-relay snooping binding
Hardware Address      IP Address      remainder time Type          VLAN      interface

00-e0-0f-26-23-89      192.2.2.101          86400          DHCP_SN                3
GigaEthernet0/3
```

The following shows the binding information about dhcp-relay snooping:

```
switch#show ip dhcp-relay snooping binding all
Hardware Address      IP Address      remainder time Type          VLAN      interface

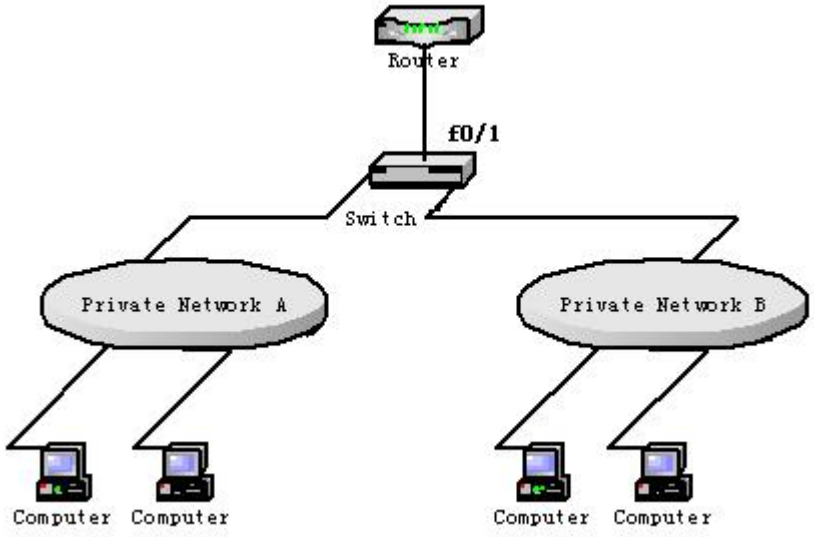
00-e0-0f-32-1c-59      192.2.2.1            infinite       MANUAL                 1
GigaEthernet0/2
00-e0-0f-26-23-89      192.2.2.101          86400          DHCP_SN                3
GigaEthernet0/3
```

The following shows the information about dhcp-relay snooping.

```
switch#debug ip dhcp-relay all
DHCPR: receive l2 packet from vlan 3, dilD: 3
DHCPR: DHCP packet len 277
DHCPR: add binding on interface GigaEthernet0/3
DHCPR: send packet continue
DHCPR: receive l2 packet from vlan 3, dilD: 1
DHCPR: DHCP packet len 300
DHCPR: send packet continue
DHCPR: receive l2 packet from vlan 3, dilD: 3
DHCPR: DHCP packet len 289
DHCPR: send packet continue
DHCPR: receive l2 packet from vlan 3, dilD: 1
DHCPR: DHCP packet len 300
DHCPR: update binding on interface GigaEthernet0/3
DHCPR:    IP address: 192.2.2.101, lease time 86400 seconds
DHCPR: send packet continue
```

1.1.17 Example of DHCP-Snooping Configuration

The network topology is shown in figure 1.



Configuring Switch

Enable DHCP snooping in VLAN 1 which connects private network A.

Switch_config#ip dhcp-relay snooping

Switch_config#ip dhcp-relay snooping vlan 1

Enable DHCP snooping in VLAN 2 which connects private network B.

Switch_config#ip dhcp-relay snooping

Switch_config#ip dhcp-relay snooping vlan 2

Sets the interface which connects the DHCP server to a DHCP-trusting interface.

Switch_config_g0/1#dhcp snooping trust

Configure option82 instance manually

```
interface GigaEthernet0/1
  dhcp snooping information circuit-id hex 00-01-00-05
  dhcp snooping information remote-id hex 00-e0-0f-13-1a-50
  dhcp snooping information vendor-specific hex
00-00-0c-f8-0d-01-0b-78-69-61-6f-6d-69-6e-37-31-31-34
  dhcp snooping information append
  dhcp snooping information append first-subop9-param hex
61-62-63-61-62-63
!
interface GigaEthernet0/2
  dhcp snooping trust
  arp inspection trust
  ip-source trust
!
!
!
ip dhcp-relay snooping
ip dhcp-relay snooping vlan  1-100
ip arp inspection vlan  1
ip verify source vlan  1
```

Layer 2 Tunnel Protocol Configuration

Table of Contents

Chapter 1 Configuring Layer-2 Protocol Tunnel..... 1
1.1 Introduction..... 1
1.2 Configuring Layer-2 Protocol Tunnel..... 1
1.3 Configuration Example of Layer 2 Protocol Tunnel..... 1

Chapter 1 Configuring Layer-2 Protocol Tunnel

1.1 Introduction

Layer-2 protocol tunnel allows users between two sides of the switch to transmit the specified layer 2 protocol on their own network without being influenced by the relevant layer 2 software module of the switch. The switch is a transparent media for users.

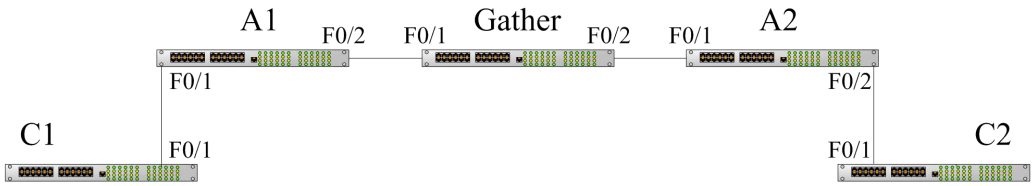
1.2 Configuring Layer-2 Protocol Tunnel

Use the command line on the interface of the switch to configure tunnel function of the layer 2 protocol. The configuration steps are as follows:

Command	Description
configure	Enters global configuration mode.
interface <*intf_name*>	Enters interface configuration mode of the switch. Only the switch port supports layer 2 protocol tunnel (including physical port and aggregation port).
[**no**] **l2protocol-tunnel** *[stp]*	Enables layer 2 protocol of the tunnel function. Currently we only support tunnel function of stp protocol.
[CTRL] + Z	Returns to EXEC mode.
write	Saves configuration.

1.3 Configuration Example of Layer 2 Protocol Tunnel

Network environment is as follows:



A1/A2/Gather belong to core network, C1/C2 are switches distributed in two places. Customer wants to combine two of its network to one , that is, the core network is a transparent transmission channel for the customer. If user wants to realize the

configured on each switch:

(1) The f0/2 of Switch A1, f0/1 and f0/2 of Gather, f0/1 of A2 should be configured to trunk mode.

(2) The f0/1 of switch A1, f0/2 of A2 should be configured to Access, and enables tunnel function of the STP protocol.

QoS Configuration

Table of Contents

Chapter 1 QoS Configuration 1
1.1 QoS Overview 1
1.1.1 QoS Concept 1
1.1.2 Terminal-To-Terminal QoS Model 1
1.1.3 Queue Algorithm of QoS 2
1.1.4 Weighted Random Early Detection 3
1.2 QoS Configuration Task List 4
1.3 QoS Configuration Tasks 4
1.3.1 Setting the Global CoS Priority Queue 4
1.3.2 Setting Global Cos to Local Priority Mapping 5
1.3.3 Setting the Bandwidth of the CoS Priority Queue 5
1.3.4 Setting the Schedule Policy of the CoS Priority Queue 6
1.3.5 Configuring the Minimum and Maximum Bandwidths of CoS Priority Queue 7
1.3.6 Setting the Default CoS Value of a Port 7
1.3.7 Setting the CoS Priority Queue of a Port 8
1.3.8 Setting Cos Priority Queue Based on dscp 8
1.3.9 Setting QoS Policy Mapping 8
1.3.10 Setting the Description of the QoS Policy Mapping 9
1.3.11 Setting the Matchup Data Flow of the QoS Policy Mapping 9
1.3.12 Setting the Actions of the Match-up Data Flow of the QoS Policy Mapping 10
1.3.13 Applying the QoS Policy on a Port 12
1.3.14 Configuring the Trust Mode 12
1.3.15 Displaying the QoS Policy Mapping Table 13
1.4 QoS Configuration Example 13
1.4.1 Example for Applying the QoS Policy on a Port 13

Chapter 1 QoS Configuration

If you care to use your bandwidth and your network resources efficiently, you must pay attention to QoS configuration.

1.1 QoS Overview

1.1.1 QoS Concept

In general, the switch works in best-effort served mode in which the switch treats all flows equally and tries its best to deliver all flows. Thus if congestion occurs all flows have the same chance to be discarded. However in a real network different flows have different significances, and the QoS function of the switch can provide different services to different flows based on their own significances, in which the important flows will receive a better service.

As to classify the importance of flows, there are two main ways on the current network:

- The tag in the 802.1Q frame header has two bytes and 3 bits are used to present the priority of the packet. There are 8 priorities, among which 0 means the lowest priority and 7 means the highest priority.
- The DSCP field in IP header of the IP packet uses the bottom 6 bits in the TOS domain of the IP header.

In real network application the edge switch distributes different priorities to different flows based on their significance and then different services will be provided to different flows based on their priorities, which is the way to realize the terminal-to-terminal QoS.

Additionally, you can also configure a switch in a network, enabling the switch to process those packets with specific attributes (according to the MAC layer or the L3 information of packets) specially. This kind of behaviors are called as the one-leap behaviors.

The QoS function of the switch optimizes the usage of limited network bandwidth so that the entire performance of the network is greatly improved.

1.1.2 Terminal-To-Terminal QoS Model

The service model describes a group of terminal-to-terminal QoS abilities, that is, the abilities for a network to transmit specific network communication services from one terminal to another terminal. The QoS software supports two kinds of service models: Best-Effort service and Differentiated service.

1. Best-effort service

The best-effort service is a singular service model. In this service model, an application can send any amount of data at any necessary time without application of permits or

network notification. As to the best-effort service, if allowed, the network can transmit data without any guarantee of reliability, delay or throughput. The QoS of the switch on which the best-effort service is realized is in nature this kind of service, that is, first come and first served (FCFS).

2. Differentiated service

As to the differentiated service, if a special service is to be transmitted in a network, each packet should be specified with a corresponding QoS tag. The switch uses this QoS rule to conduct classification and complete the intelligent queuing. The QoS of the switch provides Strict Priority (SP), Weighted Round Robin (WRR), Deficit Round Robin (DRR) and First-Come-First-Served (FCFS).

1.1.3 Queue Algorithm of QoS

Each queue algorithm is the important basis to realize QoS. The QoS of the switch provides the following algorithms: Strict Priority (SP), Weighted Round Robin (WRR), Deficit Round Robin (DRR) and First-Come-First-Served (FCFS).

1. Strict priority

This algorithm means to first provide service to the flow with the highest priority and after the highest-priority flow comes the service for the next-to-highest flow. This algorithm provides a comparatively good service to those flows with relatively high priority, but its shortage is also explicit that the flows with low priority cannot get service and wait to die.

2. Weighted round robin

Weighted Round Robin (WRR) is an effective solution to the defect of Strict Priority (SP), in which the low-priority queues always die out. WRR is an algorithm that brings each priority queue a certain bandwidth and provides service to each priority queue according to the order from high priority to low priority. After the queue with highest priority has used up all its bandwidth, the system automatically provides service to those queues with next highest priority.

3. Weighted Fair Queuing

Weighted Round Robin (WRR) is an effective solution to the defect of Strict Priority (SP), in which the low-priority queues always die out. WRR is an algorithm that brings each priority queue a certain bandwidth and provides service to each priority queue according to the order from high priority to low priority. After the queue with highest priority has used up all its bandwidth, the system automatically provides service to those queues with next highest priority.

4. First come first served

The First-Come-First-Served queue algorithm, which is shortened as FCFS, provides service to those packets according to their sequence of arriving at a switch, and the packet that first arrives at the switch will be served first.

1.1.4 Weighted Random Early Detection

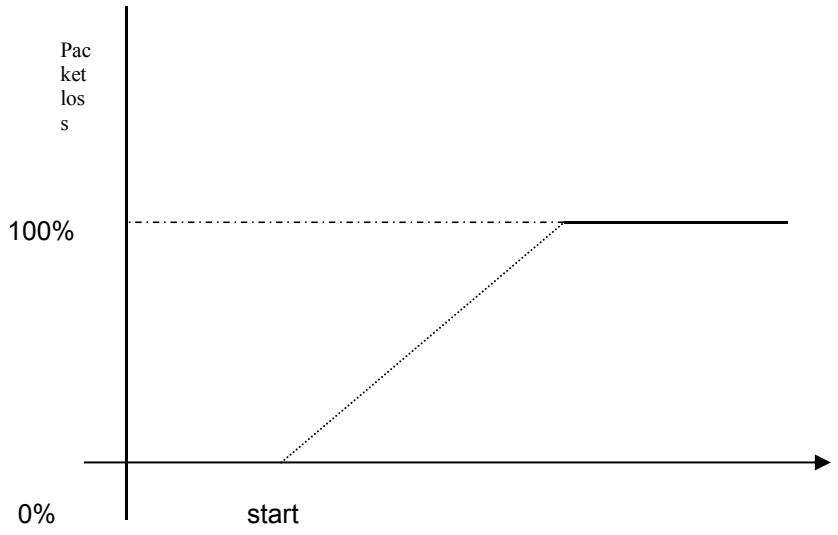
Congestion avoidance and traditional packet loss mechanism

Excessive congestion may inflict damage on network resources, so network congestion should be resolved through some measures. Congestion avoidance is a sort of flow control method of positively dropping packets and regulating network flows to solve network overload via network resource monitoring. The traditional way of resolving network congestion is to drop all incoming packets when the queue length reaches its threshold. But for TCP packets, heavy packet loss may cause TCP timeout and lead to slow TCP startup and congestion avoidance, which is called as TCP global synchronization.

WRED

The WRED algorithm is adopted to prevent TCP global synchronization. WRED helps users to set the queue threshold. When the queue length is less than the configured threshold, the packets will not be dropped; otherwise, the packets will be dropped randomly. Because WRED drops packets randomly, it is avoided for multiple TCP connections to slow down the transmission speed at the same time, which is the reason why TCP global synchronization is avoided. WRED enables other TCP connections to maintain a relatively high transmission speed when the packets of a certain TCP connection begin to be dropped and their transmission speed is slowed down. No matter what time it is, there are always some TCP connections to transmit packets with a high speed, which ensures effective bandwidth usability.

WRED cooperation is conducted when packets enter the outgoing queue and are checked for their size and packets in different ranges get different treatments. The key parameters include **Start**, **Slop** and **Drop priority**.



When the queue length is less than **start**, packets will not be dropped.

When the queue length is bigger than **start**, the incoming packets begin to be dropped

randomly.The longer the queue is, the higher the dropping rate is.

The rate for packet loss rises along with the increase of the queue length.

1.2 QoS Configuration Task List

In general, switch will try its best to deliver each packet and when congestion occurs all packets have the same chance to be discarded. However, in reality different packets have different importance and the comparatively important packets should get the comparatively good service. QoS is a mechanism to provide different priority services to packets with different importance, in which the network can have its better performance and be used efficiently.

This chapter presents how to set QoS on switch.

The following are QoS configuration tasks:

- Setting the Global CoS Priority Queue
- Setting Global Cos to Local Priority Mapping
- Setting the Bandwidth of the CoS Priority Queue
- Setting the Schedule Policy of the CoS Priority Queue
- Setting the Default CoS Value of a Port
- Setting the CoS Priority Queue of a Port
- Setting the CoS Priority Queue of a Port
- Establishing the QoS Policy Mapping
- Setting the Description of the QoS Policy Mapping
- Setting the Matchup Data Flow of the QoS Policy Mapping
- Setting the Actions of the Matchup Data Flow of the QoS Policy Mapping
- Applying the QoS Policy on a Port
- Configuring the Trust Mode
- Displaying the QoS Policy Mapping Table

1.3 QoS Configuration Tasks

1.3.1 Setting the Global CoS Priority Queue

The task to set the QoS priority queue is to map 8 CoS values, which are defined by IEEE802.1p, to the priority queues in a switch. This series of switch has 8 priority

queues. According to different queues, the switch will take different schedule policies to realize QoS.

If a CoS priority queue is set in global mode, the mapping of CoS priority queue on all ports will be affected. When priority queues are set on a L2 port, the priority queues can only work on this L2 port.

Enter the following privileged mode and run the following commands one by one to set DSCP mapping.

Command	Purpose
config	Enters the global configuration mode.
[**no**] **cos map** *quid cos1..cosn*	Sets the CoS priority queue. **quid** stands for the ID of a CoS priority queue. **cos1…cosn** stands for the IEEE802.1p-defined CoS value.
exit	Goes back to the EXEC mode.
write	Saves the settings.

1.3.2 Setting Global Cos to Local Priority Mapping

The command is used to set map inner CoS priority to the congestion bit.

Enter the following privileged mode and configure global CoS to local priority mapping.

Command	Purpose
config	Enters the global configuration mode.
[**no**] **cos map-local-priority** *cos-value1* {**cos** *cos-value2* | **cng** *cng-bit* }	Sets the local priority mapping of cos. *cos-value1* is cos value defined IEEE802.1p, 0-7. *cos-value2* is remapping inner priority cos, 0-7. *cng-bit* is congestion bit of cos mapping.
exit	Exit from management configuration mode.
write	Saving the configuration.

1.3.3 Setting the Bandwidth of the CoS Priority Queue

The bandwidth of priority queue means the bandwidth distribution ratio of each priority queue, which is set when the schedule policy of the CoS priority queue is set to WRR/DRR. This series of switches has 8 priority queues in total.

If this command is run, the bandwidth of all priority queues on all interfaces are affected. This command validates only when the queue schedule policy is set to WRR or DRR. This command decides the bandwidth weight of the CoS priority queue when the WRR/DRR schedule policy is used.

Run the following commands one by one to set the bandwidth of the CoS priority queue.

Command	Purpose
config	Enters the global configuration mode.
[**no**] **scheduler weight bandwidth** *weight1...weightn*	Sets the bandwidth of the CoS priority queue.. **weight1…weightn** stand for the weights of 8 CoS priority queues of WRR/DRR.
exit	Goes back to the EXEC mode.
write	Saves the settings.

1.3.4 Setting the Schedule Policy of the CoS Priority Queue

A switch has many output queues on each of its port. This series of switches has 8 priority queues. The output queues can adopt the following three schedule modes:

- SP (Sheer Priority): In this algorithm, only when the high-priority queue is null can the packets in the low-priority queue be forwarded, and if there are packets in the high-priority queue these packets will be unconditionally forwarded.
- In this mode, the bandwidth of each queue is distributed with a certain weight and then bandwidth distribution is conducted according to the weight of each queue. The bandwidth in this mode takes byte as its unit.
- The First-Come-First-Served queue algorithm, which is shortened as FCFS, provides service to those packets according to their sequence of arriving at a switch, and the packet that first arrives at the switch will be served first.

Enter the following configuration mode and set the schedule policy of CoS priority queue.

Command	Purpose
config	Enters the global configuration mode.
[**no**] **scheduler policy** { **sp** | **wrr|wfq|fcfs** }	Sets the schedule policy of the CoS priority queue. **sp** means to use the SP schedule policy. **Wrr** means to use the WRR schedule policy. **Fcfs** to use the FCFS schedule policy. **drr** means to use the DRR schedule policy.
exit	Goes back to the EXEC mode.
write	Saves the settings.

,

1.3.5 Configuring the Minimum and Maximum Bandwidths of CoS Priority Queue

The minimum and maximum bandwidths of CoS priority queue can be modified through configuration. All the flows with a bandwidth less than the configured minimum bandwidth shall not be dropped, but the flows with a bandwidth bigger than the configured maximum bandwidth shall all be dropped.

Enter the privileged mode.

Command	Purpose
config	Enters the global configuration mode.
interface g0/1	Enters the to-be-configured port.
[**no**] **cos bandwidth** *quid min-bandwidth max-bandwidth*	**quid** stands for the priority queue. **min-bandwidth** means the minimum bandwidth. **max-bandwidth** means the maximum bandwidth.
exit	Goes back to the global configuration mode.
exit	Goes back to the EXEC mode.
write	Saves the settings.

1.3.6 Setting the Default CoS Value of a Port

If the port of a switch receives a data frame without tag, the switch will add a default CoS priority to it. Setting the default CoS value of a port is to set the untagged default CoS value, which is received by the port, to a designated value.

Enter the privilege mode and run the following commands to set the default CoS value of a port:

Command	Purpose
config	Enters the global configuration mode.
interface g0/1	Enters the to-be-configured port.
[**no**] **cos default** *cos*	Sets the CoS value of the received untagged frames. **cos** stands for the corresponding CoS value.
exit	Goes back to the global configuration mode.
exit	Goes back to the EXEC mode.
write	Saves the settings.

1.3.7 Setting the CoS Priority Queue of a Port

When a priority queue is set on a L2 port, the priority queue will be used by the L2 port; otherwise, you should conduct the configuration of a global CoS priority queue.

Enter the privilege mode and run the following commands to set the default CoS value of a port:

Command	Purpose
config	Enters the global configuration mode.
interface g0/1	Enters the to-be-configured port.
[**no**] **cos map** *quid cos1..cosn*	Sets the CoS priority queue. **quid** stands for the ID of a CoS priority queue. **cos1…cosn** stands for the IEEE802.1p-defined CoS value.
exit	Goes back to the global configuration mode.
exit	Goes back to the EXEC mode.

1.3.8 Setting Cos Priority Queue Based on dscp

The command is used to remap cos queue based on dscp value, modify dscp and the congestion bit.

Enters the privileged mode and configures CoS of the port.

Command	Purpose
config	Enters the global configuration mode.
[**no**]**dscp map** *word* {**dscp** dscp-value | **cos** *cos-value* | **cng** *cng-bit* }	Word configures dscp range table. Dscp-value Configures re-mapped dscp value. Cos-value Configures priority cos of mapping. Cog-bit Configures congestion bit of mapping.
exit	Exit from the global configuration mode.
exit	Exit from the management configuration mode.

1.3.9 Setting QoS Policy Mapping

QoS policy mapping refers to use a certain rule (based on MAC layer or IP header information) to identify packets with certain characteristics and adopt a certain action.

Do as follows to set a QoS policy.

Enters the privileged mode and configures CoS policy mapping.

Command	Purpose
config	Enters the global configuration mode.
[no]policy-map *name*	Enters QoS policy table configuration mode. name The name of policy
exit	Exit from the global configuration mode.
exit	Exit from the management mode.

1.3.10 Setting the Description of the QoS Policy Mapping

Enter the privileged mode and run the following commands to set the description of a QoS policy mapping. This settings will replace the previous settings.

Command	Purpose
config	Enters the global configuration mode.
[**no**]**policy-map** *name*	Enters the configuration mode of the QoS policy map. **name** stands for the name of the policy.
description description-text	Sets the description of the QoS policy. **description-text** stands for the text to describe the policy.
exit	Goes back to the global configuration mode.
exit	Goes back to the EXEC mode.

1.3.11 Setting the Matchup Data Flow of the QoS Policy Mapping

The classification rule of the QoS data flow means the filtration rule configured by the administrator according to management requirements. It can be simple, for example, flows with different priorities can be identified by the ToS field of the IP packet's header, or complicated, for example, the packets can be classified according to the related information about the comprehensive link layer, the network layer and the transmission layer, such as the MAC address, the source address of IP, the destination address or the port ID of the application. In general, the classification standard is limited in the header of an encapsulated packet. It is rare to use the content of a packet as the classification standard.

Enter the policy configuration mode, set the match-up data flow of policy and replace the previous settings with this data flow according to the following steps:

Command	Purpose
config	Enters the global configuration mode.
[no]policy-map name	Enters the configuration mode of the QoS

	policy map. **name** stands for the name of the policy.
description description-text	Sets the description of the QoS policy. **description-text** stands for the text to describe the policy.
classify {**any** | **cos** *cos* | **icos** *icos* | **vlan** *vlanid* | **ivlan** *ivlanid* | **ethernet-type** *ethernet-type* | **precedence** *precedence-value* | **dscp** *dscp-value* | **tos** *tos-value* | **diffserv** *diffserv-value* | **ip** *ip-access-list* | **ipv6** *ipv6-access-list* | **mac** *mac-access-list* } **no classify** { **cos** | **icos** | **vlan** | **ivlan** | **ethernet-type** | **precedence** | **dscp** | **tos** | **diffserv** | **ip** | **ipv6** | **mac** }	Matches up with any packet. Configures the matched COS value which ranges between 0 and 7. **icos** stands for the matched inner COS value which ranges between 0 and 7. **vlanid** stands for the matched VLAN, which ranges from 1 to 4094. **ivlanid** stands for the matched inner VLAN, which ranges from 1 to 4094. **ethernet-type** stands for the matched packet type, which is between 0x0600 and 0xFFFF. **precedence-value** stands for the priority field in tos of IP packet, which ranges from 0 to 7. **dscp-value** stands for the dscp field in tos of IP packet, which ranges from 0 to 63. **tos-value** stands for latency, throughput, reliability and cost fields in tos of IP packet, which ranges from 0 to 15. **diffserv-value** stands for the entire tos field. **Ip-access-list** stands for the name of the matched IP access list. The name has 1 to 20 characters. **Ipv6-access-list** stands for the name of the matched IPv6 access list. The name has 1 to 20 characters. Configures the name of the matched MAC access list. The name has 1 to -20 characters.
exit	Goes back to the global configuration mode.
exit	Goes back to the EXEC mode.

1.3.12 Setting the Actions of the Match-up Data Flow of the QoS Policy Mapping

The actions to define the data flow mean to take corresponding actions to a data flow with compliance of the filtration rule, which include bandwidth limit, drop, update, etc.

Enter the privileged mode and run the following commands to set the action of a policy, matching up the data flow. The action will replace the previous settings.

Command	Purpose
config	Enters the global configuration mode.
[**no**]**policy-map** *name*	Enters the configuration mode of the QoS policy map. **name** stands for the name of the policy.
action{**bandwidth** *max-band* **|** {**cir** *commit-band* {**bc** *commit-burst-size* {**be** *peak-burst-size* | **pir** *pir-band* } } | **[conform** {**forward | dscp** *dscp-value*} **| exceed** {**forward | drop | dscp** *dscp-value* **| discardable** {**green | yellow | red**}} **| violate** {**forward | drop | dscp** *dscp-value* **| discardable** {**green | yellow | red**}}]} **| cos** *cos* **| drop | dscp** *dscp-value* **| precedence** *precedence-value* **| forward | icos** *icos* **| ivlan** {**add** *ivlanid* **| del** *ivlanid* **|** *ivlanid*} **| cpicos | mac** *mac-addr* **| monitor** *session-value* **| queue** *queue-value* **| redirect** *interface-id* **| stat-packet | stat-byte | vlanID** { **add** *vlanid* | *vlanid* }} **no action** {**bandwidth | cir | cos | drop | dscp | precedence | forward | icos | ivlan | cpicos | mac | monitor | queue | redirect | stat-packet | stat-byte | vlanID**}	**max-band** stands for the occupied maximum bandwidth. Sets the policing: **cir commit-band** stands for the certified bandwidth. **bc commit-burst-size** stands for the size of burst packet, which ranges from 4 to 4096Kb. **be peak-burst-size** stands for the size of peak burst, which ranges from 4 to 4096Kb. **pir pir-band** stands for the peak bandwidth, which ranges from 1 to 163840. **conform {forward | dscp dscp-value}** stands for a bandwidth guarantee action, among which **forward** means not to conduct any action and **dscp** means to change the dscp value. **drop** means to drop the matched packets. Sets the matched DSCP field to ***dscp-value*** **0~63**. **precedence-value** stands for the priority field of tos in ip packet.0-7. Conducts no operations to the matched packets. Sets the matched COS field to cos-value 0-7. **ivlanid** is used to replace, add or delete the inner VLAN ID. **cpicos** means to replace the outer cos with inner cos. **mac-addr** is used to set the destination MAC address. **session-value** is used to set mirroring, which ranges from 1 to 4. **queue-value** is used to set the mapping

	queue, which ranges from 1 to 8. Redirects the egress port of the matched flow. **stat-packet** stands for the number of packets under statistics. **stat-byte** means the number of bytes under statistics. **vlanID** is used to replace or add the outer vlan ID, which ranges from 1 to 4094.
exit	Goes back to the global configuration mode.
exit	Goes back to the EXEC mode.

1.3.13 Applying the QoS Policy on a Port

The QoS policy can be applied to a port; multiple QoS policies can be applied to the same port and the same QoS policy can also be applied to multiple ports. On the same port, the priorities of the policies which are earlier applied than those of the policies which are later applied. If a packet is set to have two policies and the actions are contradicted, the actions of the firstly matched policies. After a QoS policy is applied on a port, the switch adds a policy to this port by default to block other data flows, which are not allowed to pass through. When all policies on a port are deleted, the switch will automatically remove the default blockage policy from a port.

Enter the following privileged mode and run the following commands to apply the QoS policy.

Command	Purpose
config	Enters the global configuration mode.
interface g0/1	Enters the to-be-configured port.
[**no**] **qos policy** *name* { **ingress**|**egress**}	Applies the QoS policy on a port. **name** stands for the name of QoS policy mapping. ***ingress*** means to exert an influence on the ingress. *egress* means to exert an influence on the egress.
exit	Goes back to the global configuration mode.
exit	Goes back to the EXEC mode.

1.3.14 Configuring the Trust Mode

In the global configuration mode, trust of cos, dscp or untrust can be configured. When the data maps to the queue, the trusted mode chosen by the global will be mapped to the queue. If the configured trust mode is untrust, the default priority of the packet will be mapped to the queue.

Enters the management mode and do as the following steps:

Command	Purpose
config	Enters the global configuration mode.
[**no**] **qos trust** { cos | dscp | untrust }	Configures the trust mode in the global configuration mode. untrust refers to untrust of any mode.
exit	Exit to the management configuration mode.

1.3.15 Displaying the QoS Policy Mapping Table

You can run the **show** command to display all or some designated QoS policy maps.

Run the following command in privileged mode to display the QoS policy mapping table.

Command	Purpose
show policy-map [*policy-map-name*]	Displays all or some designated QoS policy maps. **policy-map-name** stands for the name of QoS mapping table.

1.4 QoS Configuration Example

1.4.1 Example for Applying the QoS Policy on a Port

The following example shows how to set packet's cos to 2 on port g0/2:

```
ip access-list extended ipacl
permit ip 192.168.20.2 255.255.255.255 192.168.20.210 255.255.255.255
!
policy-map pmap
classify ip ipacl
action cos 2
!
interface g0/2
qos policy pmap ingress
!
```

DoS Attack Prevention Configuration

Table of Contents

Chapter 1 DoS Attack Prevention Configuration....1
1.1 DoS Attack Overview....1
1.1.1 Concept of DoS Attack....1
1.1.2 DoS Attack Type....1
1.2 DoS Attack Prevention Configuration Task List....2
1.3 DoS Attack Prevention Configuration Tasks....2
1.3.1 Configuring Global DoS Attack Prevention....2
1.3.2 Displaying All DoS Attack Prevention Configurations....3
1.4 DoS Attack Prevention Configuration Example....3

Chapter 1 DoS Attack Prevention Configuration

1.1 DoS Attack Overview

1.1.1 Concept of DoS Attack

The DoS attack is also called the service rejection attack. Common DoS attacks include network bandwidth attacks and connectivity attacks. DoS attack is a frequent network attack mode triggered by hackers. Its ultimate purpose is to break down networks to stop providing legal users with normal network services.

DoS attack prevention requires a switch to provide many attack prevention methods to stop such attacks as Pingflood, SYNflood, Landattack, Teardrop, and illegal-flags-contained TCP. When a switch is under attack, it needs to judge which attack type it is and handles these attack packets specially, for example, sending them to CPU and drop them.

1.1.2 DoS Attack Type

Hackers will make different types of DoS attack packets to attack the servers. The following are common DoS attack packets:

1. Ping of Death

Ping of Death is the abnormal Ping packet, which claims its size exceeds the ICMP threshold and causes the breakdown of the TCP/IP stack and finally the breakdown of the receiving host.

2. TearDrop

TearDrop uses the information, which is contained in the packet header in the trusted IP fragment in the TCP/IP stack, to realize the attack. IP fragment contains the information that indicates which part of the original packet is contained, and some TCP/IP stacks will break down when they receive the fake fragment that contains the overlapping offset.

3. SYN Flood

A standard TCP connection needs to experience three hand-shake processes. A client sends the SYN message to a server, the server returns the SYN-ACK message, and the client sends the ACK message to the server after receiving the SYN-ACK message. In this way, a TCP connection is established. SYN flood triggers the DoS attack when the TCP protocol stack initializes the hand-shake procedure between two hosts.

4. Land Attack

The attacker makes a special SYN message (the source address and the destination address are the same service address). The SYN message causes the server to send the SYN-ACK message to the sever itself, hence this address also sends the ACK message and creates a null link. Each of this kinds of links will keep until the timeout time, so the server will break down. Landattack can be classified into IPland and MACland.

1.2 DoS Attack Prevention Configuration Task List

As to global DoS attack prevention configuration, you configure related sub-functions and then the switch drops corresponding DoS attack packets. Hence, the bandwidth of the switch is guaranteed not to be used up.

DoS attack prevention configuration tasks are shown below:

Configuring Global DoS Attack Prevention

Displaying All DoS Attack Prevention Configuration

1.3 DoS Attack Prevention Configuration Tasks

1.3.1 Configuring Global DoS Attack Prevention

Configuring global DoS attack prevention means configuring DoS attack prevention sub-functions in global mode and each sub-function can prevent a different type of DoS attack packets. The DoS IP sub-function can prevent the LAND attacks, while the DoS ICMP sub-function can prevent Ping of Death. You can set the corresponding sub-function according to actual requirements.

Configure the DoS attack prevention function in EXEC mode.

Command	Purpose
config	Enters the global configuration mode.
[**no**] **dos enable {all | icmp** ***icmp-value*** **| ip | ipv4firstfrag | l4port | mac | tcpflags | tcpfrag** ***tcpfrag-value*****}**	Configures **all** to prevent all types of DoS attack packets. Configures **icmp** to prevent the ICMP packets, among which the **icmp-value** means the maximum length of the ICMP packet. Configures **ip** to prevent those IP packets whose source IPs are the same as the destination IPs. Configures **ipv4firstfrag** to check the first fragment of the IP packet. Configures **l4port** to prevent those TCP/UDP packets whose source port IDs are destination

	port IDs. Configures **mac** to prevent those packets whose source MACs are destination MACs. Configures **tcpflags** to prevent those TCP packets containing illegal TCP flags. Configures **tcpfrag** to prevent those TCP packets whose minimum TCP header is **tcpfrag-value**.
exit	Goes back to the EXEC mode.
write	Saves the settings.

1.3.2 Displaying All DoS Attack Prevention Configurations

You can display the Dos attack prevention configurations through the **show** command.

Run the following command in EXEC mode to display the configured DoS attack prevention functions.

Command	Purpose
show dos	Displays Dos attack prevention configuration.

1.4 DoS Attack Prevention Configuration Example

The following example shows how to configure to prevent the attacks of TCP packets, which have illegal flags, and then displays user's configuration.

config

dos enable tcpflags

show dos

The following example shows how to prevent the attacks of IP packets whose source IPs are destination IPs in global mode.

config

dos enable ip

The following example shows how to prevent in global mode the attacks of ICMP packets whose maximum length is more than 255.

config

dos enable icmp 255

Attack Prevention Configuration

Table of Contents

Chapter 1 Attack Prevention Introduction....1
1.1 Overview of Filter....1
1.2 The Mode of Filter....1
Chapter 2 Attack Prevention Configuration....2
2.1 Attack Prevention Configuration Tasks....2
2.2 Attack Prevention Configuration....2
2.2.1 Configuring the Attack Filter Parameters....2
2.2.2 Configuring the Attack Prevention Type....2
2.2.3 Enabling the Attack Prevention Function....3
2.2.4 Checking the State of Attack Prevention....3
Chapter 3 Attack Prevention Configuration Example....5
3.1 Using Filter ARP to Protect the LAN....5
3.2 Using Filter IP to Protect Layer-3 Network....5

Chapter 1 Attack Prevention Introduction

1.1 Overview of Filter

To guarantee the reasonable usage of network bandwidth, this switch series provides the function to prevent vicious traffic from occupying lots of network bandwidth.

Filter can identify the packets received by the interface of the switch and calculate them according to the packet type. In light of current attack modes, Filter can calculate the number of ARP, IGMP or IP message that a host sends in a time. Once the number exceeds the threshold, the switch will not provide any service to these hosts.

Filter limits the packet from a certain host by blocking the source address. For ARP attack, Filter blocks source MAC address; for IP attacks, such as Ping scan and TCP/UDP scan, Filter blocks source IP address.

1.2 The Mode of Filter

The mode of Filter determines how the switch specifies the attack source. There are two modes of Filter.

Source Address Block Time (Raw)

In Raw mode, the switch will drop packets from the attack source in scheduled block-time since the attack source is determined. After block-time, the restriction on the attack source will be removed and a new calculation will be enabled.

In Raw mode, all the packets from the source address will be blocked. For instance, when the MAC address of the attack source is blocked, all packets whose source MAC address are the same with that of the attack source will be dropped, no matter it is ARP, ICMP, DHCP or other types.

Source Address Block Polling (Hybrid)

After blocking the attack source, the switch will continue calculate the packets from the attack source and detect whether the packet number exceeds the threshold before the end of Polling Interval. If the packet number exceeds the threshold, the blocking state keeps. Otherwise, the blocking will be removed. In Hybrid Mode, the packet number when initially determining the attack source and the threshold of the packet number in Polling can be configured independently.

To realize continually calculate the packet, in the hybrid mode the packet type will be matched while the source address is blocked. For instance, if the MAC address of a host is blocked as it triggers ARP attack, IP packets from the host will be sent by the switch continually, unless the host is also identified with the existence of IP attack.

Please select the mode of Filter according to your application environment. If you want to set a strict limit on the attack source and reduce the burden of switch CPU, please use Raw mode; if you want to control the attack source flexibly and resume communication of the host as soon as possible after the end of the attack, please use Hybrid mode. Note that the Filter number a switch can support in Hybrid mode is limited. In condition of inadequate Filter number, Raw mode will be adopted automatically.

Chapter 2 Attack Prevention Configuration

2.1 Attack Prevention Configuration Tasks

When the number of IGMP, ARP or IP message that is sent by a host in a designated interval exceeds the threshold, we think that the host attack the network.

You can select the type of attack prevention (ARP, IGMP or IP), the attack prevention port and the attack detection parameter. You have the following configuration tasks:

- Configuring the attack filter parameters
- Configuring the attack prevention type
- Enables the attack prevention function.
- Checking the State of Attack Prevention

2.2 Attack Prevention Configuration

2.2.1 Configuring the Attack Filter Parameters

In global configuration mode, run the following command to configure the parameters of Filter.

Command	Purpose
Switch# config	Enters the global configuration mode.
Switch_config# **filter period** *time*	Sets the attack filter period to time. Its unit is second.
Switch_config# **filter threshold [arp | bpdu | dhcp | igmp | ip | icmp]** *value*	Sets the attack filter threshold to value.
Switch_config# **filter block-time** *time*	Sets the out-of-service time (block-time) for the attack source when the attack source is detected. Its unit is second.
Switch_config# filter polling period time	Sets the filter polling period in Hybrid mode. Its unit is second.
Switch_config# filter polling threshold [arp | bpdu | dhcp | igmp | ip | icmp | icmpv6] value	Sets the filter polling threshold in Hybrid mode.
Switch_config# filter polling auto-fit	Sets the corresponding parameters of period and threshold of polling filter which adapts to the attack source filter. The command is efficient by default. The polling period equals with the attack filter period and the polling packet threshold equals to 3/4 of the attack filter packet threshold
Switch_config# filter shutdown-action	Sets shutdown of the port when detecting the attack source in raw mode.

2.2.2 Configuring the Attack Prevention Type

In global and interface configuration mode, use the following command to configure the type of attack filter.

Command	Purpose
Switch# config	Enters the global configuration mode.

Switch_config# filter dhcp	Enables DHCP packet attack filter in the global configuration mode.
Switch_config# filter icmp	Enables ICMP packet attack filter.
Switch_config# **filter icmpv6**	Enables ICMPv6 packet attack detection.
Switch_config# **filter igmp**	Enables IGMP packet attack filter.
Switch_config# **filter ip source-ip**	Enables IP attack filter in the global configuration mode.
Switch_config# **interface intf-name**	Enters the interface configuration mode.
Switch_config_intf# **filter arp**	Enables ARP packet attack filter on the interface.
Switch_config_intf# filter bpdu	Enables BPDU packet attack filter on the interface.
Switch_config_intf# filter dhcp	Enables DHCP packet attack filter on the interface.
Switch_config_intf# filter icmp	Enables ICMP packet attack filter on the interface.
Switch_config_intf# **filter icmpv6**	Enables ICMPv6 packet attack detection on the interface.
Switch_config_intf# filter ip source-ip	Enables IP packet attack filter on the interface.

Note:

ARP attack takes the combination "the host mac address + the source port" as an attack source. That is to say, packets with the same MAC address but coming from different ports, the count will not be accumulated. Both the IGMP attack and IP attack take the host's IP address and source port as the attack source.

Note:

1, The IGMP attack prevention and the IP attack prevention cannot be started up together.

2. IP, ICMP, ICMPv6 and DHCP filter take effect only in global and interface configuration mode.

2.2.3 Enabling the Attack Prevention Function

After all parameters for attack prevention are set, you can start up the attack prevention function. Note that small parts of processor source will be occupied when the attack prevention function is started.

Command	Purpose
Switch_config# **filter enable**	Enables the attack prevention function.
Switch_config# filter mode [raw | hybrid]	Sets the mode of Filter: Raw or Hybrid.

Use the no filter enable command to disable the attack prevention function and remove the block to all attack sources.

2.2.4 Checking the State of Attack Prevention

After attack prevention is started, you can run the following command to check the state of attack prevention:

Command	Purpose
show filter	After attack prevention is started, you

	can run the following command to check the state of attack prevention:
show filter summary	Checks the parameter configuration and summary information of Filter.

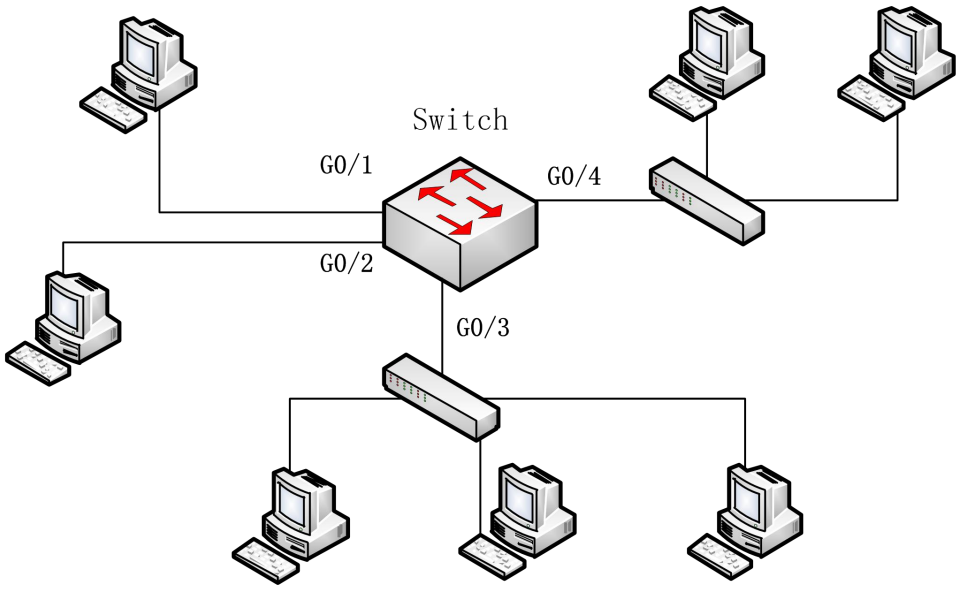
Chapter 3 Attack Prevention Configuration Example

Note:

The examples shown in this chapter is only a reference for Filter configuration. Please configure according to your actual network condition.

3.1 Using Filter ARP to Protect the LAN

As shown in the following figure, configure ARP attack Filter on Switch.



Sets the parameter of Filter. A host sending more than 100 ARP messages in 10s will be taken as an attack source.

Switch# config

Switch_config# filter period 10

Switch_config# filter threshold arp 100

Sets APR attack filter with 4 ports:

Switch_config# interface range g0/1 – 4

Switch_config_intf# filter arp

Sets Raw mode and enable Filter:

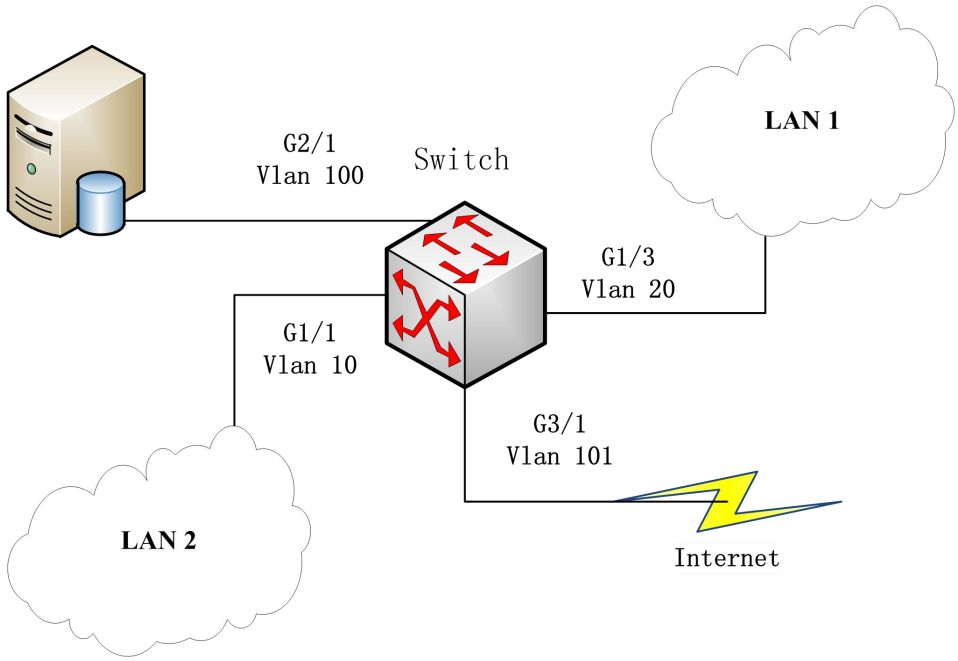
Switch_config_intf# exit

Switch_config# filter mode raw

Switch_config# filter enable

3.2 Using Filter IP to Protect Layer-3 Network

As shown in the following figure, Switch is connected to multiple LANs, servers and the internet. IP packet attack prevention can block IP scan of cross-subnet and large network connections triggered by BitTorrent in a short time.



Sets the parameter of Filter. A host sending more than 300 ARP messages in 1 minute will be taken as an attack source.

Switch# config

Switch_config# filter period 60

Switch_config# filter threshold ip 300

Enable IP packet filter in the global configuration mode and the interface mode. Note that the interface connecting the server and the external network is no need to configure:

Switch_config# filter ip source-ip

Switch_config# interface g1/1

Switch_config_g1/1# filter ip source-ip

Switch_config_g1/1# interface g1/3

Switch_config_g1/3# filter ip source-ip

Switch_config_g1/3# exit

Switch_config#

Enables Filter:

Switch_config# filter enable

Network Protocol Configuration

Table of Contents

Chapter 1 Configuring IP Addressing....1
1.1 IP Introduction....1
1.1.1 IP....1
1.1.2 IP Routing Protocol....1
1.2 Configuring IP Address Task List....2
1.3 Configuring IP Address....2
1.3.1 Configuring IP Address at the Network Interface....2
1.3.2 Configuring Multiple IP Addresses at the Network Interface....3
1.3.3 Configuring Address Resolution....4
1.3.4 Configuring Routing Process....7
1.3.5 Configuring Broadcast Packet Process....7
1.3.6 Detecting and Maintaining IP Address....8
1.4 IP Addressing Example....8
Chapter 2 Configuring DHCP....10
2.1 Overview....10
2.1.1 DHCP Application....10
2.1.2 Advantages of DHCP....10
2.1.3 DHCP Terms....10
2.2 Configuring DHCP Client....11
2.2.1 Configuration Task List of DHCP Client....11
2.2.2 DHCP Client Configuration Tasks....11
2.2.3 DHCP Client Configuration Example....12
2.3 Configuring DHCP Server....12
2.3.1 DHCP Server Configuration Tasks....12
2.3.2 Setting the Address Pool of DHCP Server....12
2.3.3 DHCP Server Configuration Example....18
2.4 Configuring DHCP Relay....19
2.4.1 Configuration Task List of DHCP Relay....19
2.4.2 DHCP Relay Configuration Tasks....19
2.4.3 DHCP Relay Configuration Example....19
Chapter 3 IP Service Configuration....20
3.1 Configuring IP Service....20
3.1.1 Managing IP Connection....20
3.1.2 Configuring Performance Parameters....24
3.1.3 Detecting and Maintaining IP Network....24
3.2 Configuring Access List....26
3.2.1 Filtering IP Packet....26
3.2.2 Creating Standard and Extensible IP Access List....26
3.2.3 Applying the Access List to the Routing Interface....27
3.2.4 Applying the Access List to the Global Mode....28

3.2.5 Applying the Access List to the Physical Interface.....28
3.2.6 Extensible Access List Example.....29

Chapter 1 Configuring IP Addressing

1.1 IP Introduction

1.1.1 IP

Internet Protocol (IP) is a protocol in the network to exchange data in the text form. IP has the functions such as addressing, fragmenting, regrouping and multiplexing. Other IP protocols (IP protocol cluster) are based on IP. As a protocol working on the network layer, IP contains addressing information and control information which are used for routing.

Transmission Control Protocol (TCP) is also based on IP. TCP is a connection-oriented protocol which regulates the format of the data and information in data transmission. TCP also gives the method to acknowledge data is successfully reached. TCP allows multiple applications in a system to communicate simultaneously because it can send received data to each of the applications respectively.

The IP addressing, such as Address Resolution Protocol, are to be described in section "Configuring IP Addressing." IP services such as ICMP, HSRP, IP statistics and performance parameters are to be described in "Configuring IP Services."

1.1.2 IP Routing Protocol

Our routing switch supports multiple IP routing dynamic protocols, which will be described in the introduction of each protocol.

IP routing protocols are divided into two groups: Interior Gateway Routing Protocol (IGRP) and Exterior Gateway Routing Protocol (EGRP). The switch supports RIP and OSPF. You can configure RIP and OSPF respectively according to your requirements. Our switch also supports the simultaneous configuration of multiple routing protocols: OSPF processes (if memory is available), a BGP process and a RIP process. You can run the redistribute command to redistribute routes from other routing protocols to the database of the current routing process, connecting the routes of multiple protocol processes.

To configure IP dynamic routing protocols, you must first configure relevant processes, make relevant network ports interact with dynamic routing processes, and then designate routing processes to be started up on the ports. To do this, you may check configuration steps in configuration command documents.

(1) Choosing Routing Protocol

It is a complex procedure to choose routing protocol. When you choose the routing protocol, consider the following items:

- Size and complexity of the network
- Whether the length-various network need be supported
- Network traffic
- Safety requirements
- Reliability requirements

- Strategy
- Others

Details of the above items are not described in the section. We just want to remind you that your network requirements must be satisfied when you choose the routing protocols.

(2) IGRP

Interior Gateway Routing Protocol (IGRP) is used for network targets in an autonomous system. All IP IGRPs must be connected with networks when they are started up. Each routing process monitors the update message from other routing devices in the network and broadcasts its routing message in the network at the same time. The switch supports following internal routable protocols:

RIP

OSPF

(3) EGRP

Exterior Gateway Routing Protocol (EGRP) is used to exchange routing information between different autonomous systems. Neighbors to exchange routes, reachable network and local autonomous system number generally need to be configured. The switch supports BGP.

1.2 Configuring IP Address Task List

An essential and mandatory requirement for IP configuration is to configure the IP address on the network interface of the routing switch. Only in this case can the network interface be activated, and the IP address can communicate with other systems. At the same time, you need to confirm the IP network mask.

To configure the IP addressing, you need to finish the following tasks, among which the first task is mandatory and others are optional.

For creating IP addressing in the network, refer to section “IP Addressing Example.”

IP address configuration task list:

- Configuring IP address at the network interface
- Configuring multiple IP addresses at the network interface
- Configuring Address Resolution
- Configuring broadcast packet processing
- Detecting and maintaining IP addressing

1.3 Configuring IP Address

1.3.1 Configuring IP Address at the Network Interface

The IP address determines the destination where the IP message is sent to. Some IP special addresses are reserved and they cannot be used as the host IP address or network address. Table 1 lists the range of IP addresses, reserved IP addresses and available IP addresses.

Type	Address or Range	Status
A	0.0.0.0 1.0.0.0 to 126.0.0.0	Reserved Available

	127.0.0.0	Reserved
B	128.0.0.0 to 191.254.0.0 191.255.0.0	Available Reserved
C	192.0.0.0 192.0.1.0 to 223.255.254 223.255.255.0	Reserved Available Reserved
D	224.0.0.0 to 239.255.255.255	Multicast address
E	240.0.0.0 to 255.255.255.254 255.255.255.255	Reserved Broadcast

The official description of the IP address is in RFC 1166 “Internet Digit”. You can contact the Internet service provider.

An interface has only one primary IP address. Run the following command in interface configuration mode to configure the primary IP address and network mask of the network interface:

Command	Purpose
ip address *ip-address mask*	Configure the main IP address of the interface.

The mask is a part of the IP address, representing the network.

Note:

Our switch only supports masks which are continuously set from the highest byte according to the network character order.

1.3.2 Configuring Multiple IP Addresses at the Network Interface

Each interface can possess multiple IP addresses, including a primary IP address and multiple subordinate IP addresses. You need to configure the subordinate IP addresses in the following two cases:

If IP addresses in a network segment are insufficient. For example, there are only 254 available IP addresses in a certain logical subnet, however, 300 hosts are needed to connect the physical network. In this case, you can configure the subordinate IP address on the switch or the server, enabling two logical subnets to use the same physical subnet.

Most of early-stage networks which are based on the layer-2 bridge are not divided into multiple subnets. You can divide the early-stage network into multiple route-based subnets by correctly using the subordinate IP addresses. Through the configured subordinate IP addresses, the routing switch in the network can know multiple subnets that connect the same physical network.

If two subnets in one network are physically separated by another network In this case, you can take the address of the network as the subordinate IP address. Therefore, two subnets in a logical network that are physically separated, therefore, are logically connected together.

Note:

If you configure a subordinate IP address for a routing switch in a network segment, you need to do

this for other routing switch in the same network segment.
Run the following command in interface configuration mode to configure multiple IP addresses on the network interface.

Command	Purpose
ip address *ip-address mask* **secondary**	Configures multiple IP addresses on the network interface.

Note:
When the IP routing protocol is used to send the route update information, subordinate IP addresses may be treated in different ways.
1.3.3 Configuring Address Resolution
IP can realize functions such as IP address resolution control. The following sections show how to configure address resolution:

(1) Creating Address Resolution

An IP device may have two addresses: local address (local network segment or device uniquely identified by LAN) and network address (representing the network where the device is located). The local address is the address of the link layer because the local address is contained in the message header at the link layer, and is read and used by devices at the link layer. The professionals always call it as the MAC address. This is because the MAC sub layer in the link layer is used to process addresses.
For example, if you want your host to communicate with a device on Ethernet, you must know the 48-bit MAC address of the device or the local address of the link layer. The process on how to obtain the local address of the link layer from the IP address is called as Address Resolution Protocol (ARP). The process on how to obtain the IP address from the local address of the link layer is called as Reverse Address Resolution (RARP).
Our system adopts address resolution in two types: ARP and proxy ARP. The ARP and proxy ARP are defined in RFC 860 and 1027 respectively.
ARP is used to map IP addresses to media or MAC address. When the IP address is known, ARP will find the corresponding MAC address. When the MAC address is known, the mapping relationship between IP address and MAC address is saved in ARP cache for rapid access. The IP message is then packaged in the message at the link layer and at last is sent to the network.
Defining a static ARP cache
ARP and other address resolution protocols provide a dynamic mapping between IP address and MAC address. The static ARP cache item is generally not required because most hosts support dynamic address resolution. You can define it in global configuration mode if necessary. The system utilizes the static ARP cache item to translate the 32-bit IP address into a 48-bit MAC address. Additionally, you can specify the routing switch to respond to the ARP request for other hosts.
You can set the active period for the ARP entries if you do not want the ARP entry to exist permanently. The following two types show how to configure the mapping between the static IP address and the MAC address.

Run one of the following commands in global configuration mode:

Command	Purpose
arp ip-address hardware-address **vlan** vlan-id	Globally maps an IP address to a MAC address in the ARP cache.
arp ip-address hardware-address **vlan** vlan-id **alias**	Makes the switch respond to the ARP request of the designated IP address through the MAC address of the routing switch.

Run the following command in VLAN interface configuration mode:

Command	Purpose
arp timeout *seconds*	Sets the timeout time of the ARP cache item in the ARP cache.
arp dynamic	Enables arp dynamic learning in the interface

Run show interfaces to display the ARP timeout time of the designated interface. Run the show arp to check the content of the ARP cache. Run clear arp-cache to delete all entries in the ARP cache.

Activating proxy ARP

The system uses the proxy ARP (defined by RFC 1027) to obtain the host's MAC address on other networks for the hosts without corresponding routes. For example, when the routing switch receives an ARP request and finds that the source host and the destination host are not connected to the same interface and all the routes that the routing switch reaches the destination host are not through the interface that receives the ARP request, it will send a proxy ARP response that contains its address of the link layer. The source host then sends the message to the routing switch and the switch forwards it to the destination host. The proxy ARP is activates by default.

To activate the proxy ARP, run the following command in interface configuration mode:

Command	Purpose
ip proxy-arp	Activates the proxy ARP on the interface.

Configuring free ARP function

The switch can know whether the IP addresses of other devices collide with its IP address by sending free ARP message. The source IP address and the destination IP address contained by free ARP message are both the local address of the switch. The source MAC address of the message is the local MAC address.

The switch processes free ARP message by default. When the switch receives free ARP message from a device and finds that the IP address contained in the message collide with its own IP address, it will return an ARP answer to the device, informing the device that the IP addresses

collide with each other. At the same time, the switch will inform users by logs that IP addresses collide.

The switch·s function to send free ARP message is disabled by default. Run the following commands to configure the free ARP function on the port of the switch:

Command	Purpose
arp send-gratuitous	Starts up free ARP message transmission on the interface.
arp send-gratuitous interval *value*	Sets the interval for sending free ARP message on the interface. The default value is 120 seconds.

To set the waiting time of ARP cache resolution, run the following command.

The switch will create incomplete ARP entry when first resolve arp. The incomplete entry will create complete ARP entry when the opposite end responses correct arp reply packet. At this point, the ARP resolution is finished.

Run following command to set the time to live of the incomplete entry.

Command	Purpose
arp pending-time *seconds*	Sets the waiting time of ARP cache resolution, run the following command: The default value is 15 seconds.

Set the maximum number of incomplete ARP entries.

Command	Purpose
arp max-incomplete *number*	Sets the maximum number of incomplete ARP entries. The default is 0.

To set the maximum retransmissions of the Re-Detect packets, run the following command.

The ARP entries (to be tagged with G), which the routing entry gateway depends on, require being re-detected at their aging so that the promptness and correctness of the hardware subnet routing can be guaranteed. The greater the retransmission times, the more likely to re-detect.

Command	Purpose
arp max-gw-retries *number*	Sets the maximum retransmissions of the Re-Detect packets. The default is 3.

Set re-detection when ARP entry is aging.

By default only ARP depends on routing entry has re-detection when aging. After enable this command, all ARP entries will adopt aging re-detection mechanism.

Command	Purpose
arp retry-allarp	Sets re-detection when the ARP entry is aging.

(2) Mapping Host Name to IP Address

Any IP address can correspond to a host name. The system has saved a mapping (host name to address) cache which can be telneted or pinged.

To designate a mapping from host name to address, run the following commands in global mode:

Command	Purpose
ip host *name address*	Statically maps the host name to the IP address.

1.3.4 Configuring Routing Process

You can configure one or multiple routing protocols according to your actual network requirements. The routing protocol provides information about the network topology. The details about configuring IP routing protocols such as BGP, RIP and OSPF are shown in the following sections.

1.3.5 Configuring Broadcast Packet Process

The destination addresses of the broadcast message are all the hosts on a physical network. The host can identify the broadcast message through special address. Some protocols, including some important Internet protocols, frequently use the broadcast message. One primary task of the IP network administrator is to control the broadcast message. The system supports the directed broadcast, that is, the broadcast of designated network. The system does not support the broadcast of all subnets in a network.

Some early-stage IP's do not adopt the current broadcast address standard. The broadcast address adopted by these IPs is represented completely by the number "0", not "1" completely. The system can simultaneously identify and receive message of the two types.

(1) Allowing Translating from Directed Broadcast to Physical Broadcast

By default, the IP directional broadcast packets will be dropped, rather than being forwarded. Dropping the IP directional broadcast packet is conducive to prevent the routing switch from attacks of "refusal service".

You can activate the function of forwarding directed IP broadcast on the interface where the directed broadcast is transformed to the physical message. If the forwarding function is activated, all the directed broadcast message of the network that connects the interface will be forwarded to the interface. The message then will be sent as the physical broadcast message.

You can designate an access table to control the forwarding of broadcast message. After the access table is specified, only IP message that the access table allows can be transformed from the directed broadcast to the physical broadcast.

Run the following command in interface configuration mode to activate the forwarding of the directed broadcast.

Command	Purpose
ip directed-broadcast [*access-list-name*]	Allows the translation from the directed broadcast to the physical broadcast on the interface.

(2) Forwarding UDP Broadcast Message

Sometimes, the host uses the UDP broadcast message to determine information about the

address, configuration and name, and so on. If the network where the host is located has no corresponding server to forward the UDP message, the host cannot receive any of the UDP message. To solve the problem, you can do some configuration on the corresponding interface to forward some types of broadcast message to an assistant address. You can configure multiple assistant addresses for an interface.

You can designate a UDP destination port to decide which UDP message is to be forwarded. Currently, the default forwarding destination port of the system is UDP packet of NetBIOS name service (port 137).

Run the following command in interface configuration mode to allow message forwarding and to specify the destination address:

Command	Purpose
ip helper-address *address*	Allows to forward the UDP broadcast message and to specify the destination address.

Run the following command in global configuration mode to specify protocols to be forwarded:

Command	Purpose
ip forward-protocol udp [*port*]	Specifies which interfaces' UDP protocols will be forwarded.

1.3.6 Detecting and Maintaining IP Address

To detect and maintain the network, run the following command:

(1) Clearing Cache, List and Database

Clearing cache, list and database You can clear all content in a cache, list or the database. When you think some content is ineffective, you can clear it.

Run the following command in management mode to clear the cache, list and database:

Command	Purpose
clear arp-cache	Clears the IP ARP cache.

(2) Displaying Statistics Data about System and Network

The system can display designated statistics data, such as IP routing table, cache and database. All such information helps you know the usage of the systematic resources and solve network problems. The system also can display the reachability of the port and the routes that the message takes when the message runs in the network.

All relative operations are listed in the following table. For how to use these commands, refer to Chapter "IP Addressing Commands". Run the following commands in management mode:

Command	Purpose
show arp	Displays content in the ARP table.
show hosts	Displays the cache table about hostname-to-IP mapping.
show ip interface [*type number*]	Displays the state of a port.
ping {**host	address**}	Tests the reachability of the network node.

1.4 IP Addressing Example

The following case shows how to configure the IP address on interfaceVLAN11.

```
interface vlan 11
ip address 202.96.2.3 255.255.255.0
```

Chapter 2 Configuring DHCP

2.1 Overview

Dynamic Host Configuration Protocol (DHCP) is used to provide some network configuration parameters for the hosts on the Internet, which is described in details in RFC 2131. One of the major functions of DHCP is to distribute IPs on an interface. DHCP supports the following three IP distribution mechanism:

Automatic distribution

The DHCP server automatically distributes a permanent IP address to a client.

Dynamic distribution

The DHCP server distributes an IP address for a client to use for a certain period of time or until the client does not use it.

Manual distribution

The administrator of the DHCP server manually specifies an IP address and through the DHCP protocol sends it to the client.

2.1.1 DHCP Application

DHCP can be applied at the following cases: You can distribute IP address, network segment and related sources (such as relevant gateway) to an Ethernet interface by configuring the DHCP client.

When a DHCP-capable switch connects multiple hosts, it can obtain an IP address
from the DHCP server through the DHCP relay and then distribute the address to the hosts.

2.1.2 Advantages of DHCP

In current software version, the DHCP client or the DHCP client on the Ethernet interface is supported. DHCP has the following strong points:

Fastening the settings;

Reducing configuration errors;

Controlling IP addresses of some device ports through the DHCP server

2.1.3 DHCP Terms

DHCP is based on the server/client mode. So the DHCP server and the DHCP client must exist at the same time:

DHCP-Server

It is a device to distribute and recycle the DHCP-related sources such as IP addresses and lease time.

DHCP-Client

It is a device to obtain information from the DHCP server for devices of the local system to use, such as IP address information.

In a word, there exists lease time during the process of dynamic DHCP distribution:

Lease time – it means the effective period of an IP, which starts from the distribution. After the lease time, the DHCP server withdraws the IP. To continue to use this IP, the DHCP client needs to apply it again.

2.2 Configuring DHCP Client

2.2.1 Configuration Task List of DHCP Client

- Obtaining an IP address
- Specifying an address for DHCP server
- Configuring DHCP parameters
- Monitoring DHCP

2.2.2 DHCP Client Configuration Tasks

(1) Obtaining an IP address

Run the following command on the VLAN interface to obtain an IP address through the DHCP protocol for an interface.

Command	Purpose
ip address dhcp	Sets the IP address of an Ethernet interface through DHCP.

(2) Specifying an Address for DHCP Server

If knowing the addresses of some DHCP servers, you can specify these servers' addresses on switch so as to reduce the time of protocol processing. You can run the following command in global mode:

Command	Purpose
ip dhcp-server *ip-address*	Specifies the IP address of the DHCP server.

The command is optional when you perform operations to "obtain an IP address".

(3) Configuring DHCP Parameters

To adjust the parameters of DHCP communication according to actual requirements, run the following commands in global mode:

Command	Purpose
ip dhcp client minlease *seconds*	Specifies the acceptable minimum lease time.
ip dhcp client retransmit *count*	Specifies the retransmission times for DHCP packet.
ip dhcp client select *seconds*	Specifies the interval for SELECT.
ip dhcp client class_identifier *WORD*	Specifies the classification code of the provider.
ip dhcp client client_identifier hrd_ether	Specifies the client ID as the Ethernet type
ip dhcp client timeout_shut	Specifies client timeout shutdown of the interface
ip dhcp client retry_interval *<1-1440>*	Sets the re-transmission time.
ip dhcp client bootfileaddmac	Enables DHCP file name to add MAC address

	of the client
ip dhcp client tftpdownload	Enables TFTP download function

The command is optional when you perform operations to "obtain an IP address".

(4) Monitoring DHCP

To browse related information of the DHCP server, which is discovered by switch currently, run the following command in EXEC mode:

Command	Purpose
show dhcp server	Displays related information about the DHCP server, which is known by switch.

To browse which IP address is currently used by switch, run the following command in EXEC mode:

Command	Purpose
show dhcp lease	Displays IP resources, which are currently used by the switch, and related information.

Additionally, if you use DHCP to distribute an IP for an Ethernet interface, you can also run show interface to browse whether the IP address required by the Ethernet interface is successfully acquired.

2.2.3 DHCP Client Configuration Example

DHCP Client configuration example is shown below:

(1) Obtaining an IP Address

The following example shows interface vlan11 obtains an IP address through DHCP.

!

interface vlan 11

ip address dhcp

2.3 Configuring DHCP Server

2.3.1 DHCP Server Configuration Tasks

- Enabling DHCP server
- Disabling DHCP server
- Configuring ICMP detection parameter
- Configuring database storage parameter
- Configuring the address pool of DHCP server
- Configuring the parameter for the address pool of DHCP server
- Monitoring DHCP server
- Clearing information about DHCP server

2.3.2 Setting the Address Pool of DHCP Server

(1) Enabling DHCP Server

To enable the DHCP server and distribute IP addresses for DHCP client, run the following commands in global mode (thereupon, the DHCP server also supports the relay operation; As to those IPs that the DHCP server cannot distribute, the interface on which IP helper-address is

configured will forward the DHCP request)

Command	Purpose
ip dhcpd enable	Enables DHCP server

(2) Disabling DHCP Server Service

To disable DHCP server and stop distributing parameters such as IP address parameter for the DHCP client, run the following command in global configuration mode:

Command	Purpose
no ip dhcpd enable	Disables DHCP server

(3) Configuring ICMP Detection Parameter

You can adjust the parameters of ICMP packet transmission according to actual requirements when the DHCP server is checking addresses.

To set the number of ICMP packets to be sent, run the following command in global mode:

Command	Purpose
ip dhcpd ping packets *pkgs*	Sets how many ICMP packets to be sent during address checkup.

To set the timeout time of ICMP response, run the following command in global mode:

Command	Purpose
ip dhcpd ping timeout *timeout*	Sets the timeout time of ICMP response.

(4) Setting a Parameter to Clear the “Abandoned” Mark

To set the interval of clearing the “Abandoned” mark, run the following command in global mode:

Command	Purpose
ip dhcpd abandon-time *time*	Sets the interval of clearing the “Abandoned” mark.

(5) Configuring Database Storage Parameter

To set the interval of storing the address distribution information to the agent database, run the following command in global mode:

Command	Purpose
ip dhcpd write-time *time*	Sets the interval for storing the address distribution information to the agent database.

(6) Configuring DHCP File Domain

Run the following command in the global configuration mode:

Command	Purpose

ip dhcpd bootfile-name *word*	The command is used to configure DHCP file domain.

(7) Configuring DHCP Enabling File Name Option

Run the following command in the global configuration mode:

Command	Purpose
ip dhcpd bootfile-option	The following command is used to configure DHCP enabling file name option.

(8) Configuring DHCP Supporting BOOTP Client

Run the following command in the global configuration mode:

Command	Purpose
ip dhcpd bootp [auto-bind]	The command is used to configure DHCP supporting BOOTP client. auto-bind means to allow BOOTP client distributing auto binding address.

(9) Configuring DHCP Database Server Address

Run the following command in the global configuration mode:

Command	Purpose
ip dhcpd database-agent *ip-address*	Configures DHCP database server address, run the following command. If this address is not set, the address distribution information will be saved to the flash. Note: Before the address distribution information is saved, PC should enable the TFTP server and also PC and the DHCP server should connect correctly.

(10) Configuring DHCP Database File Name

Run the following command in the global configuration mode:

Command	Purpose
ip dhcpd database-file *word* [**time-stamp**]	Configures the DHCP database file name, run the following command. Word means database file name

	Time-stamp means file name addition time stamp

(11) Saving the Change of Cache Entry in Time to the Data Base File

Run the following command in the global configuration mode:

Command	Purpose
ip dhcpd database-realtime	Saves the change of cache entry in time to the data base file, run the following command.

(12) Configuring DHCP Optional Server Host Name

Run the following command in the global configuration mode:

Command	Purpose
ip dhcpd server-name *name*	Configures DHCP optional server host name.

(13) Enabling DHCP TFTP Server Name Option

Run the following command in the global configuration mode:

Command	Purpose
ip dhcpd sname-option	Enables DHCP TFTP server name option.

(14) Configuring Relevant Parameters of DHCP Snooping

The command can be used to enable the ARP map protection. When this command is set, the DHCP server will establish an ARP map between the MAC address and distributed IP address of the DHCP client, and then protect this ARP map. Run the following command in the global configuration mode:

Command	Purpose
ip dhcpd snooping arp	Configures the parameters of DHCP snooping.

(15) Forwarding STB DHCP Data Packet

Run the following command in the global configuration mode:

Command	Purpose
ip dhcpd relay-STB	Enables STB DHCP data packet.

(16) Compulsorily Enabling DHCP TFTP Server Name Option and DHCP Enabling File Name Option

To compulsorily enable DHCP TFTP server name option (option:66) and DHCP enabling file name option (option: 67). Run the following command in the global configuration mode:

Command	Purpose
ip dhcpd sname-bootfile-option-force	Compulsorily enables DHCP TFTP server name option (option:66) and DHCP enabling file name option (option: 67).

(17) Configuring Address Pool of DHCP Server

To add the address pool of DHCP server, run the following command in global mode:

Command	Purpose
ip dhcpd pool *name*	Adds the address pool of DHCP server and enters the configuration mode of the DHCP address pool.

(18) Configuring Relevant Parameters for the Address Pool of DHCP Server

In the configuration mode of DHCP address pool, you can run the following commands to set related parameters.

To set the network address of the address pool of automatic distribution, run the following command:

Command	Purpose
network *ip-addr netsubnet*	Sets the network address of the address pool of automatic distribution.

To set the address range of automatic distribution, run the following command:

Command	Purpose
range *low-addr high-addr*	Sets the address range of automatic distribution.

To set the default route, which is distributed by the client, run the following command:

Command	Purpose
default-router *ip-addr …*	Sets the default route that is distributed to the client.

To set the address of DNS server, which is distributed to the client, run the following command:

Command	Purpose
dns-server *ip-addr …*	Sets the address of DNS server, which is distributed to the client.

To set a domain name, which is distributed to the client, run the following command:

Command	Purpose
domain-name *name*	Sets a domain name, which is distributed to the client.

To set the time limitation of the address, which is distributed to the client, run the following command:

Command	Purpose
lease {*days* [*hours*][*minutes*] | *infinite* }	Sets the time limitation of the address, which is distributed to the client.

To set the address of the netbios name server, which is distributed to the client, run the following command:

Command	Purpose
netbios-name-server *ip-addr…*	Sets the address of the netbios name server, which is distributed to the client.

You can run the following command to reject to distribute the IP address to the host whose MAC address is hardware-address.

Command	Purpose
hw-access deny hardware-address	Reject to distribute IP addresses to the host whose MAC address is hardware-address.

(19) Monitoring DHCP Server

To browse the current address distribution information of DHCP server, run the following command in EXEC mode:

Command	Purpose
show ip dhcpd binding	Displays the current address distribution information of DHCP server.

To browse the current packet statistics of DHCP server, run the following command in EXEC mode:

Command	Purpose
show ip dhcpd statistic	Displays the current packet statistics of DHCP server.

To browse the current database server address of DHCP server, run the following command in EXEC mode:

Command	Purpose
show ip dhcpd database-agent	Displays the current address distribution information of DHCP server.

To check the current address pool information of DHCP Server, run the following command in EXEC mode.

Command	Purpose
show ip dhcpd pool	Displays the current address pool information of DHCP server.

(20) Clearing Information about DHCP Server

To delete the current address distribution information of DHCP server, run the following command in EXEC mode:

Command	Purpose
clear ip dhcpd binding {[*ip-addr*]&<0-10>|*}	Deletes the specified address distribution information.

To delete the current packet statistics of DHCP server, run the following command in EXEC mode:

Command	Purpose
clear ip dhcpd statistic	Deletes the current packet statistics of DHCP server.

To delete the current address which has abandoned or disabled by DHCP Server address pool, run the following command in EXEC mode.

Command	Purpose
clear ip dhcpd abandoned	Deletes the current address which has abandoned or disabled by DHCP Server address pool.

2.3.3 DHCP Server Configuration Example

In the following example, the timeout time of the ICMP detection packet is set to 200ms; Address pool 1 is configured and the DHCP server is enabled.

```
ip dhcpd ping timeout 2
ip dhcpd pool 1
 network 192.168.20.0 255.255.255.0
 range 192.168.20.211 192.168.20.215
 domain-name my315
 default-router 192.168.20.1
 dns-server 192.168.1.3 61.2.2.10
```

```
 netbios-name-server 192.168.20.1
 lease 1 12 0
!
ip dhcpd enable
```

2.4 Configuring DHCP Relay

2.4.1 Configuration Task List of DHCP Relay

Enabling DHCP relay

Disabling DHCP relay

Setting the parameters of DHCP relay

2.4.2 DHCP Relay Configuration Tasks

(1) Enabling DHCP Relay

If you want to enable DHCP Relay on switch, please enable DHCP server first. For details, please refer to section “Enabling the DHCP Server.”

(2) Disabling DHCP Relay

If you want to disable DHCP Relay on switch, please disable the DHCP server first. For details, please refer to section “Disabling the DHCP Server.”

(3) Setting the Parameters of DHCP Relay

You can modify the destination address of DHCP relay according to requirements. The relay function of the DHCP packet is same in the mechanism of “Forwarding the UDP broadcast packet”. You can refer to the command, ip forward-protocol udp.

2.4.3 DHCP Relay Configuration Example

In the following example, the DHCP relay is enabled, the DHCP-request packet that is received from vlan 1 will be relayed to 10.1.1.1 and at the same time the DHCP-relay packet that arrives 192.168.20.1 will be retransmitted out from VLAN1.

```
interface vlan 1
  ip address 192.168.20.1 255.255.255.0
  ip help-address 10.1.1.1
!
ip dhcpd enable
```

Chapter 3 IP Service Configuration

The section is to describe how to configure optional IP service. For the details of the IP service commands, refer to section “IP Service Commands”.

3.1 Configuring IP Service

Optional IP service configuration tasks are listed as follows:

- Managing IP connection
- Configuring performance parameters
- Configuring default gateway
- Detecting and Maintaining IP Network

The above operations are not mandatory. You can perform the operations according to your requirements.

3.1.1 Managing IP Connection

The IP protocol provides a series of services to control and manage IP connections. Most of these services are provided by ICMP. The ICMP message is sent to the host or other routing switch when the routing switch or the access server detects faults in the IP message header. ICMP is mainly defined in RFC 792.

Perform the following different operations according to different IP connection conditions:

(1) Sending ICMP Unreachable Message

If the system receives a message and cannot send it to the destination, such as no routes, the system will send an ICMP-unreachable message to the source host. The function of the system is enabled by default.

If the function is disabled, you can run the following command in VLAN interface configuration mode to enable the function.

Command	Purpose
ip unreachables	Enable the function to send an ICMP-unreachable message.

(2) Sending ICMP Redirection Message

Sometimes the host selects an unfavorable route. After a routing switch on the route receives a message from the host, it is to check the routing table and then forward the message through the message-receiving interface to another switch that is in the same network segment as the host. In this case, the switch notifies the source host of directly sending the message with the destination to another switch without winding itself. The redirection message requires the source host to discard the original route and take more direct route suggested in the message. Many host’s operating system adds a host route to its routing table. However, the routing switch is more willing to trust information obtained through the routing protocol. Therefore, the switch will not add the host route according to the information.

The function is enabled by default. However, if a hot standby switch protocol is configured on an interface, IPv6 redirection is automatically closed. If the hot standby switch protocol is canceled, this

function will not automatically opened.

To enable the function, run the following command in VLAN interface configuration mode to forward ICMP re-directional packets:

Command	Purpose
ip redirects	Permit sending the ICMP redirection message.

(3) Sending ICMP Mask Response Message

Sometimes the host must know the network mask. To get the information, the host can send the ICMP mask request message. If the routing switch can confirm the mask of the host, it will respond with the ICMP mask response message. By default, the routing switch can send the ICMP mask response message.

To send the ICMP mask request message, run the following command in VLAN interface configuration mode:

Command	Purpose
ip mask-reply	Send the ICMP mask reply message.

(4) Supporting Route MTU Detection

The system supports the IP route MTU detection mechanism defined by RFC 1191. The IP route MTU detection mechanism enables the host to dynamically find and adjust to the maximum transmission unit (MTU) of different routes. Sometimes the routing switch detects that the received IP message length is larger than the MTU set on the message forwarding interface. The IP message needs to be segmented, but the “unsegmented” bit of the IP message is reset. The message, therefore, cannot be segmented. The message has to be dropped. In this case, the routing switch sends the ICMP message to notify the source host of the reason of failed forwarding, and the MTU on the forwarding interface. The source host then reduces the length of the message sent to the destination to adjust to the minimum MTU of the route.

If a link in the route is disconnected, the message is to take other routes. Its minimum MTU may be different from the original route. The routing switch then notifies the source host of the MTU of the new route. The IP message should be packaged with the minimum MTU of the route as much as possible. In this way, the segmentation is avoided and fewer message is sent, improving the communication efficiency.

Relevant hosts must support the IP route MTU detection. They then can adjust the length of IP message according to the MTU value notified by the routing switch, preventing segmentation during the forwarding process.

(5) Setting IP Maximum Transmission Unit (MTU)

All interfaces have a default IP maximum transmission unit (MTU), that is, the transmissible maximum IP message length. If the IP message length exceeds MTU, the routing switch segments the message.

Changing the MTU value of the interface is to affect the IP MTU value. If IP MTU equals to MTU, IP MTU will automatically adjust itself to be the same as new MTU as MTU changes. The change of IP MTU, however, does not affect MTU. IP MTU cannot be bigger than MTU configured on the current interface. Only when all devices connecting the same physical media must have the same

MTU protocol can normal communication be created.

To set IP MTU on special interface, run the following command in interface configuration mode:

Command	Purpose
ip mtu *bytes*	Sets IP MTU of the interface.

(6) Authorizing IP Source Route

The switch checks the IP header of every message. It supports the IP header options defined by RFC 791: strict source route, relax source route, record route and time stamp. If the switch detects that an option is incorrectly selected, it will send message about the ICMP parameter problem to the source host and drop the message. If problems occur in the source route, the routing switch will send ICMP unreachable message (source route fails) to the source host.

IP permits the source host to specify the route of the IP network for the message. The specified route is called as the source route. You can specify it by selecting the source route in the IP header option. The routing switch has to forward the IP message according to the option, or drop the message according to security requirements. The routing switch then sends ICMP unreachable message to the source host. switch supports the source route by default.

If the IP source route is disabled, run the following command in global configuration mode to authorize the IP source route:

Command	Purpose
ip source-route	Authorizes IP source route.

(7) Allowing IP Fast Exchange

IP fast exchange uses the route cache to forward the IP message. Before the switch forwards message to a certain destination, its system will check the routing table and then forward the message according to a route. The selected route will be stored in the routing cache of the system software. If latter message will be sent to the same host, the switch will forward latter message according to the route stored in the routing cache. Each time message is forwarded, the value of hit times of the corresponding route item is increasing by 1. When the hit times is equal to the set value, the software routing cache will be stored in the hardware routing cache. The following message to the same host will be forwarded directly by the hardware. If the cache is not used for a period of time, it will be deleted. If the software/hardware cache items reach the upper limitation, new destination hosts are not stored in the cache any more.

To configure the hit times required when the software cache items are stored to the hardware cache, run the following command in global configuration.

Command	Purpose
ip route-cache hit-numbers *hitnumber*	When the hit times of the routing item in the software cache reaches the value of the parameter hitnumber, the

	routing item in the software cache will be stored as a routing item in the hardware cache.

The command can be enabled in global configuration mode. In case the next hop of the route of the indirectly connected host is same as that of a subnet route, the command will be used to decide whether to delete the hardware route of a host.

Command	Purpose
ip route-cache age-exf	Deletes the indirectly connected hardware route of a host whose next hop is the same with the hardware subnet route next hop.
no ip route-cache age-exf	Saves the indirectly connected hardware route of a host whose next hop is the same with the hardware subnet route next hop.

To set the delay of the route cache, which is caused by ARP change, run the following command in global mode:

Command	Purpose
ip route-cache age-delay *age-delay*	When arp changes, delete all hardware route cache in a delay (related to age-delay).

To set the lifetime of the entries in the software cache, run the following command in global mode:

Command	Purpose
ip route-cache softcache-alive-time *milliseconds*	Deletes the software route cache after milliseconds.

To set the operation time index of the software cache, run the following command in global mode:

Command	Purpose
ip route-cache software-index *ticks*	The bigger the ticks, the faster the switch can age the invalid software route cache.

To set the operation time index of the hardware route cache, run the following command in global mode:

Command	Purpose
ip route-cache hardware-index *ticks*	The bigger the ticks, the faster the switch can add the hardware route cache.

To set the lifetime of the hardware route cache, run the following command in global mode:

Command	Purpose
ip route-cache-aging-time *seconds*	Sets the lifetime of the switch hardware route cache.

To enable the route cache add to the hardware table, run the following command in the global configuration mode:

Command	Purpose
ip route-cache cache-pbr	Adds the route cache which searches the route by the route policy to the hardware table.

(8) Supporting IP Fast Exchange on the Same Interface

You can enable the switch to support IP fast exchange by making the receiving interface the same as the transmitting interface. Generally, it is recommended not to enable the function because it conflicts with the redirection function of the router.

Run the following command in the VLAN interface configuration mode to allow IP routing cache in the same interface:

Command	Purpose
ip route-cache *same-interface*	Allows IP message with the same receiving/transmitting interfaces to be stored in the routing cache.

3.1.2 Configuring Performance Parameters

Run the following command to adjust IP performance.

(1) Setting the Wait Time for TCP Connection

When the switch triggers the TCP connection and if the TCP connection is not established in the designated wait time, the switch views that the connection fails and then sends the result to the upper-layer program. The default value of the system is 75 seconds. The previous configuration has no impact on TCP connections that the switch forwards. It only affects TCP connections that are created by the switch itself.

Run the following command in global configuration mode to set the wait time for TCP connections:

Command	Purpose
ip tcp synwait-time *seconds*	Sets the wait time for TCP connection.

(2) Setting the Size of TCP Windows

The default size of TCP windows is 2000 byte. Run the following command in global configuration mode to change the default window size:

Command	Purpose
ip tcp window-size *bytes*	Sets the size of TCP windows.

3.1.3 Detecting and Maintaining IP Network

To detect and maintain the network, run the following command:

(1) Clearing Cache, List and Database

You can clear all content in a cache, list or database. All incorrect data in a cache, list or database need be cleared.

Run the following command to clear incorrect data:

Command	Purpose
clear tcp statistics	Clears the statistics data about TCP

(2) Clearing TCP Connection

To disconnect a TCP connection, run the following command:

Command	Purpose
clear tcp {**local** *host-name port* **remote** *host-name port* | **tcb** *address*}	Clears the designated TCP connection. TCB refers to TCP control block.

(3) Displaying Statistics Data about System and Network

The system can display the content in the cache, list and database. These statistics data can help you know the usage of systematic sources and solve network problems.

The command can be used in other modes except the user mode. For details, refer to “IP Service Command”.

Command	Purpose
show ip access-lists *name*	Displays the content of one or all access lists.
show ip cache [*prefix mask* | **software** | **hardware | vlan** *number* | **summary**]	Displays the routing cache that is used for fast IP message exchange.
show ip sockets	Displays all socket information of switch.
show ip traffic	Displays IP protocol statistics data
show tcp	Displays all TCP connection status information
show tcp brief	Briefly displays information about TCP connection states.
show tcp statistics	Displays the statistics data about TCP
show tcp tcb *address*	Displays information about the designated TCP connection state.

(4) Displaying Debug Information

When problem occurs on the network, you can run debug to display the debugging information. Run the following command in EXEC mode. For details, refer to “IP Service Command”.

Command	Purpose
debug arp	Displays the interaction information about ARP.
debug ip icmp	Displays the interaction information about ICMP.
debug ip raw	Displays the information about received/transmitted

	Internet IP message.
debug ip packet	Displays the interaction information about IP.
debug ip tcp packet	Displays the interaction information about TCP.
debug ip tcp transactions	Displays the interaction information about TCP.
debug ip udp	Displays the interaction information about UDP.

3.2 Configuring Access List

3.2.1 Filtering IP Packet

Filtering message helps control the movement of packet in the network. The control can limit network transmission and network usage through a certain user or device. To make packets valid or invalid through the crossly designated interface, our routing switch provides the access list. The access list can be used in the following modes:

- Controlling packet transmission on the interface
- Controlling virtual terminal line access
- Limiting route update content

The section describes how to create IP access lists and how to use them.

The IP access list is an orderly set of the permit/forbid conditions for applying IP addresses. The ROS software of our switch tests the addresses one by one in ACL. The first match determines whether the ROS accepts or declines the address. After the first match, the ROS software terminates the match regulations. The order of the conditions is, therefore, important. If no regulations match, the address is declined.

Use the access list by following steps:

(1) Create the access list by designating the access list name and conditions.

(2) Apply the access list to the interface.

3.2.2 Creating Standard and Extensible IP Access List

Use a character string to create an IP access list.

Note:

The standard access list and the extensible access list cannot have the same name.

Run the following command in global configuration mode to create a standard access list:

Command	Purpose
ip access-list standard *name*	Use a name to define a standard access list.
deny [reverse-mask] {*source [source-mask]* | **any**}[**log**][**location**] or **permit [reverse-mask]** {*source [source-mask]* | **any**}[**log**][**location**]	Designate one or multiple permit/deny conditions in standard access list configuration mode. The previous setting decides whether the packet is approved or disapproved.
Exit	Log out from the access list configuration mode.

Run the following command in global configuration mode to create an extensible access list.

Command	Purpose
ip access-list extended *name*	Use a name to define an extensible IP access list.
{deny|permit} [reverse-mask] protocol source source-mask destination destination-mask **[precedence** precedence**] [tos** tos**] [log] [offset-zero] [offset-not-zero] [time-range** rangename**] [totallen {eq | gt | lt}** totallen**] [ttl {eq | gt | lt}** ttl**] [donotfragment-set] [donotfragment-notset] [is-fragment] [not-fragment] [location][dest-portrange][established]**	Designate one or multiple permit/deny conditions in extensible access list configuration mode. The previous setting decides whether the packet is approved or disapproved. precedence means the priority of the IP packet; TOS means Type of Service; offset-zero / offset-not-zero means whether IP packet Fragment offset is 0; is-fragment / not-fragment means whether IP packet is fragmented; donotfragement-notset / donotfragement-set means whether IP packet non-allowed is set; totallen means the total length of the packet; timer-rage means the time range of conditions being effective; ttl means IP packet Time To Live; dest-portrange means the range of destination port; established means established connection
Exit	Log out from the access list configuration mode.

After the access list is originally created, any part that is added later can be put at the end of the list. That is to say, you cannot add the command line to the designated access list. However, you can run no permit and no deny to delete items from the access list.

Note:

When you create the access list, the end of the access list includes the implicit deny sentence by default. If the mask is omitted in the relative IP host address access list, 255.255.255.255 is supposed to be the mask.

When ip acl is applied on the switch interface, the device does not support configuration of larger, smaller and not equal to L4 port. In other words, L4 port can only be a fixed value.

After the access list is created, the access list must be applied on the route or interface. For details, refer to the following section “Applying the Access List to the Interface”.

3.2.3 Applying the Access List to the Routing Interface

After the access list is created, you can apply it to the routing interface including ingress and egress.

Run the following command in VLAN interface configuration mode.

Command	Purpose
{ip|ipv6} access-group *name* {**in | out**}	Applies the access list to the interface.

The access control list can be used on the incoming or outgoing interface. After a packet is received, the source address of the packet will be checked according to the standard egress interface access control list. For the expanded access control list, the switch also checks the objective address. If the access control list permits the destination address, the system will continue handling the packet. However, if the access control list forbids the destination address, the system will drop the packet and then returns an ICMP unreachable packet.

For the standard access list of the out interfaces, after a packet is received or routed to the control interface, the software checks the source address of the packet according to the access list. For the expanded access control list, the switch will also check the access control list at the receiver terminal. If the access list permits the address, the software will send the packet. If the access list does not permit the address, the software drops the packet and returns an ICMP unreachable message.

If the designated access control list does not exist, all packets are allowed to pass through.

3.2.4 Applying the Access List to the Global Mode

After the access list is created, you can apply it to the routing interface in the global configuration mode including ingress and egress.

Run the following command in global mode:

Command	Purpose
[no] {ip|ipv6} access-group *name* **[egress | vlan {**word **| add** word **| remove** word**]**	Applies the established ip access list to an interface or cancels it on the interface in the global configuration mode. name Name of the IP access control list egress The access list is applied in egress. Vlan The access list is applied in ingress. Word vlan range table Add add vlan range table Remove delete vlan range table

If the designated access control list does not exist, all packets are allowed to pass through.

3.2.5 Applying the Access List to the Physical Interface

After the access list is created, you can apply it to the routing interface including ingress and egress.

Run the following command in physical interface configuration mode.

Command	Purpose
[no] {ip|ipv6} access-group *name* **[egress]**	Applies the established ip access list to an interface or cancels it on the interface in the global configuration mode, run the following command: name Name of the IP access control list egress Applies access list on the egress direction. The default is the ingress direction.

If the designated access control list does not exist, all packets are allowed to pass through.

3.2.6 Extensible Access List Example

In the following example, the first line allows any new TCP to connect the destination port after port 1023. The second line allows any new TCP to connect the SMTP port of host 130.2.1.2.

```
ip access-list extended aaa
permit tcp any 130.2.0.0 255.255.0.0 gt 1023
permit tcp any 130.2.1.2 255.255.255.255 eq 25
interface vlan 10
ip access-group aaa in
```

Another example to apply the extensible access list is given. Suppose a network connects the Internet, you expect any host in the Ethernet can create TCP connection with the host in the Internet. However, you expect the host in the Internet cannot create TCP connection with the host in the Ethernet unless it connects the SMTP port of the mail host.

SMTP connects with TCP port in one end and the arbitrary port number in the other end. During the connection period, the same two port numbers are used. The mail packet from the Internet has a destination port, that is, port 25. The outgoing packet has a contrary port number. In fact, the security system behind the routing switch always receives mails from port 25. That is the exact reason why the incoming service and the outgoing service can be uniquely controlled. The access list can be configured as the outgoing service or the incoming service.

In the following example, the Ethernet is a B-type network with the address 130.20.0.0. The address of the mail host is 130.20.1.2. The keyword established is only used for the TCP protocol, meaning a connection is created. If TCP data has the ACK or RST digit to be set, the match occurs, meaning that the packet belongs to an existing connection.

```
ip access-list aaa
permit tcp any 130.20.0.0 255.255.0.0 established
permit tcp any 130.20.1.2 255.255.255.255 eq 25
interface vlan 10
ip access-group aaa in
```

IP ACL Application Configuration

Table of Contents

Chapter 1 Application of IP Access Control List..... 1
1.1 Applying the IP Access Control List..... 1
1.1.1 Applying ACL on Ports..... 1

Chapter 1 Application of IP Access Control List

1.1 Applying the IP Access Control List

1.1.1 Applying ACL on Ports

After an ACL is established, it can be applied on one or many slots or globally.

Run the following command in global or port configuration mode:

Command	Purpose
config	Enters the global configuration mode.
interface g0/1	Enters the to-be-configured port.
[**no**] **{ip | ipv6} access-group** *name* **[egress | vlan {***word* **| add** *word* **remove** *word***|]**	Applies the established IP/IPv6 access list to an interface or cancels it on the interface. **Egress** means that the ACL is applied in an outbound direction. **Vlan** means that the ACL is applied in an inbound VLAN. **Word** stands for the VLAN range table. **Add** means to add the VLAN range table. **Remove** means to delete the VLAN range table.
exit	Goes back to the global configuration mode.
exit	Goes back to the EXEC mode.
write	Saves the settings.

Routing Protocol Configuration

Table of Contents

Chapter 1 Routing Protocol Overview 1
1.1 IP Routing Protocol 1
1.2 Choosing Routing Protocol 1
1.2.1 Interior Gateway Router Protocol 1
1.2.2 Exterior Gateway Routing Protocol 2
Chapter 2 Configuring VRF 3
2.1 Overview 3
2.2 VRF Configuration Task List 3
2.3 Configuration Task 3
2.3.1 Creating VRF Table 3
2.3.2 Relating the interface to VRF 4
2.3.3 Configuring the Target VPN Expansion Attribute of VRF 4
2.3.4 Configuring Description of VRF 4
2.3.5 Configuring Static Route of VRF 5
2.3.6 Monitoring VRF 5
2.3.7 Maintaining VRF 5
2.4 Example of the VRF Configuration 6
Chapter 3 Static routing Configuration 9
3.1 Overview 9
3.2Static Routing Configuration Task List 10
3.3Static Routing Configuration Task 11
3.3.1 Configure the Static Routing 11
3.4 Example of the Static Routing Configuration 11
Chapter 4 Configuring RIP 12
4.1 Overview 12
4.2 RIP Configuration Task List 12
4.3 RIP Configuration Task 13
4.3.1 Starting the RIP 13
4.3.2 Allowing the mono-broadcasting updated and grouped by RIP Router 13
4.3.2 Allowing the mono-broadcasting updated and grouped by RIP Router 13
4.3.3 Using the Offsets on the Route metric 13
4.3.4 Regulating the Timer 14
4.3.5 Appointing the RIP Version Number 14
4.3.6 Enabling the RIP Authentication 15
4.3.7 Activating the ·Passive· and ·Deaf· of the Interface 15
4.3.8 Activating RIP Authentication 16
4.3.9 Prohibiting the Route summary 17
4.3.10 Prohibiting the Authentication of Source IP Address 17
4.3.11 Maximum Number of Routes 17

Table of Contents

4.3.12 Activating or Prohibit the Horizontal Split 17
4.3.13 Monitoring and Maintenance of RIP 18
4.4 Example of the RIP Configuration 19
Chapter 5 Configuring OSPF 20
5.1 Overview 20
5.2 OSPF Configuration Tast List 20
5.3 OSPF Configuration Tast 21
5.3.1 Starting OSPF 21
5.3.2 Configuring the Interface Parameter of OSPF 21
5.3.3 Configuring OSPF Network Type 22
5.3.4 Configuring One-to-Multiple Broadcast Network 23
5.3.5 Configuring Non-Broadcasting Network 23
5.3.6 Configure OSPF domain 24
5.3.7 Configuring the NSSAArea of OSPF 25
5.3.8 Configuring Route Summary Within OSPF Domain 25
5.3.9 Configuring the Gathering of a Forwarding Router 26
5.3.10 Creating Default Route 26
5.3.11 Selecting Router ID Through Loopback Interface 26
5.3.12 Configuring the Management Distance of OSPF 27
5.3.13 Configuring the Route Calculation Timer 27
5.3.14 Monitoring and Maintaining OSPF 28
5.4 Examples of OSPF Configuration 29
5.4.1 Examples of the configuration of OSPF route and route distribution 29
Chapter 6 Configure BGP 37
6.1 Overview 37
6.1.1 The BGP implementation of the router 37
6.1.2 How does BGP select the path 38
6.2 BGP Configuration Task List 38

Table of Contents

6.2.1 Basic configuration task list of BGP 38
6.2.2 Advanced BGP configuration tasks list 39
6.3 Configure basic BGP features tast 39
6.3.1 Configuring Basic BGP Features 39
6.3.2 Configuring advanced BGP features 44
6.4 Monitoring and Maintaining BGP 49
6.4.1 Deleting the BGP Routing Table and the BGP Database 49
6.4.2 Displaying the Routing Table and the System Statistics Information 50
6.4.3 Tracking the BGP Information 50
6.5 Examples of BGP configuration 51
6.5.1 Example of BGP route-map 51
6.5.2 Example of neighbour configuration 52
6.5.3 Example of BGP route filtration based on the neighbor 52
6.5.4 Examples of BGP route filtration based on the interface 52
6.5.5 Examples of using prefix list to configure route filtration 53
6.5.6 Example of BGP route aggregation 54
6.5.7 Example of BGP route reflector 54
6.5.8 Example of BGP confederation 56
6.5.9 Example of route map with BGP group attribute 58
Chapter 7 Configure RSVP 61
7.1 Overview 61
7.2 RSVP Configuration Task List 61
7.3 RSVP Configuration Task 61
7.3.1 Enable a RSVP on a Router 61
7.3.2 Start RSVP in a IP Phone Module Configuration 62
7.3.3 Use RSVP to configure Command 62
7.3.4 Configure TOS and Precedence for RSVP flow 63
7.3.5 Use access-list in RSVP module 63
Chapter 8 Configuring PBR 64
8.1 Overview 64
8.2 PBR Configuration Task List 64
8.3 PBR Configuration Task 64
8.3.1 Create standard access-list 64
8.3.2 Create route-map 65
8.3.3 Apply route-map on interface 65
8.3.4 Debug PBR 65
8.4 PBR configution example 65
Chapter 9 Configuring DNS 67
9.1 Overview 67
9.1.1 DNS Application 67
9.1.2 DNS Term 67
9.2 DNS Configuration Task List 68
9.3 DNS Configuration Task 69
9.3.1 Enable DNS-based host name-to-address translation 69
9.3.2 Specify the IP address of a domain name server 69

Table of Contents

9.3.3 Set a default domain name 69
9.3.4 Define a list of domains 70
9.3.5 Define static host name-to-address mapping 70
9.3.6 Specify times to retry a DNS query 71
9.3.7 Specify timeout waiting for response to a DNS query 71
9.3.8 Delete the mapping of a host name to IP address in cache 71
9.3.9 Specify the IP address of a primary server 71
9.3.10 Enable update function of dynamic DNS 71
9.3.11 Set the period of DNS update 72
9.3.12 Bind the domain name to a IP address or IP address of interface 72
9.3.13 The function of information showing or debug showing 73

Chapter 1 Routing Protocol Overview

1.1 IP Routing Protocol

The router of the Company implements multiple IP dynamic routing protocol. They will be introduced in the description of each potocol in this Chapter.

IP routing protocols are classified into two categories: interior gateway router protocol (IGP) and exterior gateway router protocol (EGP). The routers of our Company support RIP, OSPF and BGP. RIP, OSPF and BGP can be configured separately
on real needs. The router of our company supports simultaneous configuration of multiple routing protocol, including unlimited OSPF (if memory is sufficient) processes, a BGP process and a RIP process. Command "redistribute" can
be used to inject other router protocols into the database of current routing protocol so that the multiple routing protocols can be associated.

In order to configure IP dynamic routing protocol, the corresponding process shall be started and the corresponding network interfaces and the specific dynamic routing process should be associated, to indicate on which interfaces where the routing process run. To this end, the relevant steps for configuration shall be referred to in the corresponding document of configuration commands.

1.2 Choosing Routing Protocol

The choice of routing protocol is a complicated process. When choosing a routing protocol, the following factors shall be taken into account:

- The size and complexity of the network
- Whether the support for VLSM is needed
- Network traffic
- Security requirement
- Reliability requirement
- Policy
- Others

The subject will not be detailed here. It is noted that the chosen routing protocol shall meet the real condition of network and comply with your requirements.

1.2.1 Interior Gateway Router Protocol

Interior Gateway Routing Protocol is used for the network in a single autonomous system. All the IP interior gateway routing protocol shall be associated with some specific networks (such as configuring: *network*) when it is launched. Each routing process listens to update messages from other routers on the network and broadcasts its own routing information on

the network at the same time. The inside gateway router protocol supported by the router of the Company includes:

- RIP
- OSPF

1.2.2 Exterior Gateway Routing Protocol

Exterior gateway routing protocol is used for exchange routing information between different autonomous systems. It is usually required to configure the corresponding neighbors for exchanging routes, the reachable networks and local autonomous system number. The exterior gateway routing protocol supported by the router of our company is BGP.

Chapter 2 Configuring VRF

2.1 Overview

One of the key of VPN is to keep safe and isolate data; it must be able to prevent communication of stations which belongs not to a same VPN. In order to differentiate VPN user route sent by which local interface on PE device, create virtual routes on PE device. Every virtual route has its own routing table and forwarding table. These routing tables and forwarding tables are called VRF(VPN Routing and Forwarding instances). One VRF includes the same station related routing table, interface (sub-interface), routing instances and routing policies. On PE, the physical port or the logic port with the same VPN corresponds to one VRF.

2.2 VRF Configuration Task List

If you would like to configure the VRF, the following tasks are necessary.

- Creating VRF Table
- Relating the interface to VRF
- Configuring the Target VPN Expansion Attribute of VRF
- Configuring Description of VRF
- Configuring Static Route of VRF
- Monitoring VRF
- Maintaining VRF
- Example of the VRF Configuration

2.3 Configuration Task

2.3.1 Creating VRF Table

To create VPN routing and forwarding table, do as follows in the global configuration mode:

Command	Purpose
PE_config#**ip vrf** ce	Enters VRF configuration mode, define VRF table.
PE_config_vrf_ce#**rd** *ASN:nn or IP-address:nn*	Designate the routing tag of VRF, create VRF routing and forwarding table
PE_config_vrf_ce#**route-target** [**export** | **import** | **both**] *ASN:nn or IP-address:nn*	Create input of VRF and output target VPN expansion attribute

2.3.2 Relating the interface to VRF

Relate the interface to VRF, do as follows:

Command	Purpose
PE_config#**interface vlan** 1	Enters the interface configuration mode
PE_config_v1#**ip vrf forwarding** *vrf-name*	Relate the interface to VRF
PE_config_v1#**ip address** *ip-address subnet-mask*	Configures the IP address of the interface.

2.3.3 Configuring the Target VPN Expansion Attribute of VRF

To configure the target VPN expansion attribute of VRF, do as follows:

Command	Purpose
PE_config#**ip vrf** ce	Enters the configuration mode of VRF
PE_config_vrf_ce#**rd** *ASN:nn or IP-address:nn*	Configures VRF routing tag and creates VRF table.
PE_config_vrf_ce#**route-target** [**export** | **import** | **both**]*ASN:nn or IP-address:nn*	Configures input of VRF and output target expansion attribute.
PE_config_vrf_ce#**import map** *WORD*	Configures route-map filter of the route adding to VRF routing table.
PE_config_vrf_ce#**export map** *WORD*	Add target VPN expansion attribute complying with route-map condition to the output target VPN expansion attribute of VRF.

Before publish the local route to other PE routing device, the entrance PE will add a route target attribute to every route learned from the direct station. The target value affiliated to the route is based on the VRF value configured in the output target expansion attribute.

Before installing the remote route published by other PE on the local VRF, every VRF on the entrance PE route device will be configured with one input target expansion attribute. The PE routing device can only be installed on a certain VRF until the routing target attribute borne by VPN-IPv4 matching with the VRF input target.

2.3.4 Configuring Description of VRF

To configure the description of VRF, do as follows:

Command	Purpose

PE_config#**ip vrf** ce	Enters VRF configuration mode.
PE_config_vrf_ce#**rd** *ASN:nn or IP-address:nn*	Configures VRF routing tag, and creates VRF table.
PE_config_vrf_ce# **description** LINE	Configures description of VRF.

2.3.5 Configuring Static Route of VRF

To configure the static route of VRF, do as follows:

Command	Purpose
PE_config#**ip vrf** ce	Enters VRF configuration mode.
PE_config_vrf_ce#**rd** *ASN:nn or IP-address:nn*	Configures VRF routing tag and creates VRF table.
PE_config_vrf_ce#**exit**	Exits from VRF configuration mode.
PE_config#**ip route** [**vrf** vrf-name] dest mask { type num | nexthop } [distance]	Configures VRF static route.

2.3.6 Monitoring VRF

To monitor VRF, show the statistics of VRF. To monitor, do as follows:

Command	Purpose
PE#**show ip vrf**	Shows VRF and its associated port information.
PE#**show ip vrf** [{**brief** | **detail** | **interfaces**}] *vrf-name*	Shows VRF configuration and its associated port information.
PE# show ip route vrf vrf-name [A.B.C.D | all | bgp | ospf | rip | connect | static | summary]	Shows the routing information in VRF routing table.

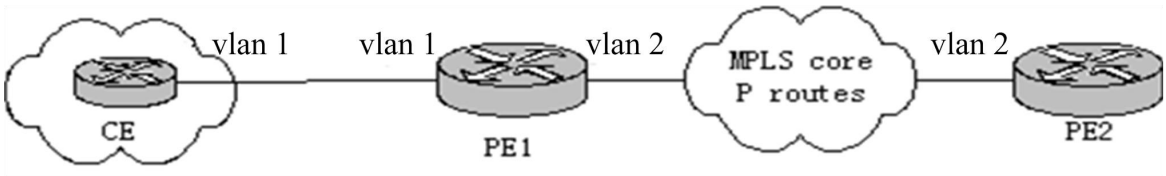
2.3.7 Maintaining VRF

Maintain VRF, track the main routing table and change of VRF routing table and VRF configuration information in the management mode and do as follows:

Command	Purpose
PE#**debug ip routing**	Track the addition, deletion and change of the route in the main routing table
PE **#debug ip routing message**	Track information VRF received and sent
PE **#debug ip routing vrf** *vrf-name*	Track the change of designated VRF routing table including adding, deleting and

	changing.

2.4 Example of the VRF Configuration



The configuration of the routing device is as follows:

Routing device CE:

```
interface loopback 0
   ip address 22.1.1.1 255.255.255.0
!
interface vlan 1
   ip address 170.168.20.152 255.255.255.0
!
router ospf 1
   network 170.168.20.0 255.255.255.0 area 0
   network 22.1.1.0 255.255.255.0 area 0
!
```

Routing device PE1:

```
ip vrf pe1
       rd 1:1
       route-target 1:1
!
interface vlan 1
   ip vrf forwarding pe1
   ip address 170.168.20.153 255.255.255.0
!
```

```
interface vlan 2
   ip address 176.168.20.152 255.255.255.0
!
router ospf 1 vrf pe1
   network 170.168.20.0 255.255.255.0 area 0
!
router bgp 1
        neighbor 176.168.20.154 remote-as 2

        address-family vpnv4
        neighbor 176.168.20.154 activate
        exit-address-family

        address-family ipv4 vrf pe1
        no synchronization
        redistribute ospf 1
        exit-address-family
```

Routing device PE2:

```
ip vrf pe2
        rd 1:1
        route-target 1:1
!
interface loopback 0
   ip vrf forwarding pe2
   ip address 44.1.1.1 255.255.255.0
!
```

```
interface vlan 2
   ip address 176.168.20.154 255.255.255.0
!
router bgp 2
      neighbor 176.168.20.153 remote-as 1

      address-family vpnv4
      neighbor 176.168.20.153 activate
      exit-address-family

      address-family ipv4 vrf pe2
      no synchronization
      redistribute connected
      exit-address-family
```

Chapter 3 Static routing Configuration

3.1 Overview

The chapter illustrates how to configure the Satatic routing. If you would like to have the detailed description on the Satatic routing commands in this section, you can refer to the Chapter of " Satatic routing " in the "Reference for the Network Protocol Commands". If you would like to search the document with other commands, you can use the master index for commands and conduct inline search.

Static routing is a special routing configuration ,and is configured by an administrator. In the network structure is relatively simple network, you only need to configure static routes on network interoperability. Properly setting up and using static routes can improve network performance and be guaranteed bandwidth for important network applications.

The shortcomings of the static route is: It can not automatically adapt to changes in network topology. When network failure or topology change may be the route is unreachable, resulting in network outages, then you must manually by the network administrator to modify the configuration of static routes.

Default route in the router can not find a matching routing table entry when routing:

- If the packet's destination address can not be any entries in the routing table to match, the packet will select the default routing;

- If no default route and destination of the packet is not in the routing table, the packet will be discarded.

Network 0.0.0.0/0.0.0.0 in the form of default route through the static routing configuration, in order to appear in the routing table.

3.2 Static Routing Configuration Task List

If you would like to configure the static routing, the following tasks are necessary.

- configure the relevant physical parameters of the interface
- configure the link layer attributes of the related interface
- configure the IP address of the relevant interface

3.3 Static Routing Configuration Task

3.3.1 Configure the Static Routing

To activate the static routing, the following steps shall be carried out under the global configuration mode:

Command	Purpose
ip route *A.B.C.C mask* {next-hop | interface} [distance] [tag tag] [global] [description]	Configure the Static Routing

3.4 Example of the Static Routing Configuration

Assigned to the network segment 10.0.0.0/8 packets port is interface GigaEthernet3/0,the configuration is as follows:

ip route 10.0.0.0 255.0.0.0 gigaEthernet 3/0

Chapter 4 Configuring RIP

4.1 Overview

The chapter illustrates how to configure the RIP. If you would like to have the detailed description on the RIP commands in this section, you can refer to the Chapter of "RIP Commands" in the "Reference for the Network Protocol Commands". If you would like to search the document with other commands, you can use the master index for commands and conduct inline search.

The Route Information Protocol (RIP) is a relatively old but still commonly used Interior Gateway Protocol (IGP), which is mainly used in the small-sized network of the same kind.. And RIP is a traditional Distance Vector Routing Protocol, which occurs in the RFC 1058.

RIP exchanges Routing Information through broadcasting UDP Packets. In the Router, the update Route Information will be sent every 30 seconds. In case that no update information from the neighbor router has been received within 180 seconds, the Routes from that neighboring router in the Routing Table will then be labeled as "Unusable". And if there is still no updated information received in the next 120 seconds, these Routes will be deleted from the Routing Table.

The Hop Count is taken by the RIP as a metric to measure different routes. And the Hop Count refers to the number of the passed routers of packets from the Source to the destination. The metric of the Route that is directly connected to the Network is "0", the metric of the Route whose network is not able to reach is "16". As the Route metric used by the RIP is in a relatively small range, it is not applicable to large-scale network. .

If a router has a default route, RIP then will advertises the route to the false Network of 0.0.0.0. In fact, the 0.0.0.0 network does not exist, which is only used for realizing the function of default route in RIP.. If the RIP has learned a default route, or the default gateway is configured in router and configured with default metric, the router will then announce the default network.

The RIP will send the updates to the interface of the appointed network. If the network of the very interface is not appointed, the network then will not be announced in any RIP updating. .

The RIP-2 of our company's router supports Plaintext and MD5 Authentication, Route Summary, CIDR and VLSM.

4.2 RIP Configuration Task List

If you would like to configure the RIP, the following tasks are necessary. While you have to first activate the RIP, the other tasks are optional.

- Starting the RIP
- Enabling Unicasting of RIP route update messages.

- Applying the offset on the route metric
- Regulating the Timer
- Designating the RIP Version Number
- Activating the RIP Authentication
- Prohibiting Route summary
- Prohibiting the Authentication on Source IP Address
- Activating or Prohibit the split-horizon

4.3 RIP Configuration Task

4.3.1 Starting the RIP

To activate the RIP, the following steps shall be carried out under the global configuration mode:

Command	Purpose
router rip	Activate the RIP Routing Process and enter the router configuration mode.
network *network-number <network-mask>*	Appoint the Network Number relevant to the RIP Routing Process

4.3.2 Allowing the mono-broadcasting updated and grouped by RIP Router

The RIP is a broadcasting-Type Protocol. If you would like the updating of routes to to access to the non-broadcasting type network, the router shall be configured so as to enable information exchange. To this end , the following commands shall be used under router configuration mode:

Command	Purpose
neighbor *ip-address*	Define a neighbor router to exchange with it the Routing Information.

In addition, if you would like to control which interface(s) that can be used to exchange routing information, the command "ip rip passive" can be used to designate an interface or some interfaces prohibiting the sending of the update of routes. If necessary, please refer to the relevant discussion on the route filtration in the "Filtrating the Routing Information" in the Chapter of " Protocol-Independent Commands in Configuring IP Router".

4.3.3 Using the Offsets on the Route metric

Offset List is taken to increase an offset on the Input and Output Routes, which have been learned with the RIP. On the other hand, you can use the Access List or the interface to limit the Offset List. In order to increase the Route metric, the following commands should be executed in the router configuration mode:

Command	Purpose
offset-list {[interface-type number]|* } {**in**|**out**} *access-list-name* **offset**	Increase an offset on the route metric.

4.3.4 Regulating the Timer

Routing protocols use several timers to determine the frequency for sending the updating of routes, how long the router will become invalid and other parameters. You can regulate these timers so as to make the performance of the Routing Protocols more suitable to the requirements of the network.

It is also possible to regulate the Route Protocol to accelerate the Convergence Time of all kinds of the IP Routing computation, to quickly backup to the redundant router so as to minimize the time of quick recovery. To regulate the Timer, the following commands should be used under router configuration model.

Command	Purpose
timers holddown *value*	Regulating the time (Unit: Second) it take to delete certain route from the Routing Table
timers expire *value*	Regulating the time (Unit: Second) that the router is announced to be invalid.
timers update *value*	Regulating the frequency for sending the updating of the Router (the time interval between sedning of the updating of routing, (unit: Second)

4.3.5 Appointing the RIP Version Number

The RIP-2 of our company's router supports Authentication, Password Management, Route summary, CIDR and VLSM.

Under the default circumstance, the router can receive the updates of RIPv1 and RIPv2, while it can only send the updates of RIP-1. By configuration, the router can be set to receive and send the updates of RIPv1 only, or receive and send the updates of RIPv2 only. For this purpose, the following commands should be taken in the router configuration mode:

Command	Purpose
version {1 | 2}	Configure the router to send and receive the updates of RIPv1 or RIPv2 only.

The above tasks are controlling the default behavior of the RIP. And you can also configure a certain interface to change this default behavior. In order to control the interface to send the RIP-1 updates or the RIP-2 updates, the following commands shall be used under interface configuration mode.

Command	Purpose
ip rip send version 1	Configure the interface to send the updates of RIP-1 only.
ip rip send version 2	Configure the interface to send the updates of RIP-2 only.
ip rip send version compatibility	Send by broadcasting t the Updating of RIP-2.message.

At the same time, to control the interface to receive the updates of RIP-1 and RIP-2, the following commands shall be used under the interface configuration mode:

Command	Purpose
ip rip receive version 1	Configure the interface to receive the updates of RIP-1 only.
ip rip receive version 2	Configure the interface to receive the updates of RIP-2 only.
ip rip receive version 1 2	Configure the interface to receive the updates of RIP-1 and RIP-2 only.

4.3.6 Enabling the RIP Authentication

RIP-1 does not support Authentication. If you would like to send and receive the updates of RIP-2, you can activate the function of RIP Authentication on the interface.

On the activated interface of RIP, we support 2 kinds of Authentication Modes: Plaintext Authentication and MD5 Authentication. the Plaintext authentication is used in each subgroups of BIP-2 under default status.

Notes:

Regarding the safety, please don't use Plaintext Authentication in the groups of RIP, because the unencrypted authentication key would be sent to each update of the RIP-2. If the safety is not a big question, (in case that it is guaranteed that the wrongly configured host can not take part in the route) the Plaintext Authentication can be used.

To configure the RIP Plaintext Authentication, the following steps should be taken under interface configuration mode:

Command	Purpose
ip rip authentication simple	Activate the RIP Authentication.
ip rip password [*string*]	Configure the Plaintext Authentication key for the interface.

In order to configure the MD5 Authentication, the steps below should be taken under interface configuration mode:

Command	Purpose
ip rip authentication *message-digest*	Activate the RIP MD5 Authentication
ip rip message-digest-key [*key-ID*] **md5** [*key*]	Configure the MD5 Authentication key for the interface

4.3.7 Activating the 'Passive' and 'Deaf' of the Interface

By default the interface covered by RIP can forward and receive the routing update by flexibly applying the RIP protocol.

To configure the passive and deaf status of the interface in the interface configuration mode:

Command	Purpose
Ip rip passive	The interface will not forward the rip protocol grouping.

ip rip deaf	The interface does not receive rip protocol grouping.

4.3.8 Activating RIP Authentication

RIP-1 does not support authentication. If the grouping of RIP-2 is forwarding and receiving, the RIP authentication can be activated on the interface.

Multiple authentication modes are supported on RIP activated interface: plaintext authentication, MD5 authentication, dynamic authentication (md5 and sha1). Each RIP-2 grouping uses plaintext authentication by default.

Note:

If considering safety, do not use the plaintext authentication in RIP grouping, this is because the authentication key without encryption is forwarded to each RIP-2 grouping. If safety is not considered (for instance, the host with error configuration cannot participate in the route), the plaintext authentication is available.

To configure RIP plaintext authentication, do as follows in the interface configuration mode:

Command	Purpose
ip rip authentication simple	Configures the interface with the plaintext authentication.
ip rip password *string*	Configures the plaintext authentication key.

To configure MD5 authentication of RIP, do as follows in the interface configuration mode:

Command	Purpose
ip rip authentication md5	Configures the interface with MD5 authentication.
ip rip md5-key *key-ID* **md5** *key*	Configures MD5 authentication key and authentication ID.

To configure the dynamic authentication of RIP, do as follows in the interface configuration mode:

Command	Purpose
ip rip authentication dynamic	Configures the interface with dynamic authentication (md5 and sha1).
ip rip dynamic-key *key-ID* { **md5 | sha1** } *key xxxx-xx-xx-xx:xx xx:xx*	Configures dynamic authentication key and authentication ID.

After configuring the RIP authentication configuration, do as follows in the interface configuration mode:

Command	Purpose
ip rip authentication commit	If the authentication cannot pass, age the opposite end peer and the route learned from the opposite end.

4.3.9 Prohibiting the Route summary

Under the default circumstance, the RIP-2 supports the automatic route summary, summarizing the RIP-2 Routes when crossing the boundary of the classified network. And the RIP-1 Automatic Route Gathering Function is always activated.

If there is a separated Sub-net, it is necessary to prohibit the Route summary to declare this Sub-net. If the Route Gathering is prohibited, when crossing the boundary of the classified network, the router will then send the route information of the sub-net and the host. Under the router configuration mode, the following command should be taken to prohibit the automatic gathering.

Command	Purpose
no auto-summary	Prohibit the Automatic summary

4.3.10 Prohibiting the Authentication of Source IP Address

Under the default circumstance, the router will authenticate the Authenticable Source IP Address of the received route update. If this address is illegal, the router update will then be rejected.

If you have a router in hope to receive the updating from it, but you have not configured the corresponding "network" or "neighbor" on the receiver, the function should be therefore prohibited. However in the common practice, this command is not recommended to use. Under router configuration mode, the following commands will prohibit the default function of authenticating the source IP address in incoming route updates.

Command	Purpose
no validate-update-source	Prohibit to authenticate the Source IP Address of the incoming RIP Router Updating.

4.3.11 Maximum Number of Routes

By default, the local RIP routing table can contain up to 1024 routes. When the number of routes in the routing table exceeds the maximum number, the route will not be added to the routing table any more. Meanwhile, the user will be notified that the number of routes in the routing table has reached the maximum number. Run the commands in the following table to configure the maximum number of the routes in the local RIP routing table in router configuration mode.

Command	Purpose
maximum-count *number*	Configures the maximum number of routes for the local RIP routing table.
no maximum-count	Resumes the default maximum number of the routes in the local RIP routing table.

4.3.12 Activating or Prohibit the Horizontal Split

Normally, the router, which is connected with IP Network and using the Distance Vector Routing Protocol, takes split-horizon to lower the possibility of route loops. The Split-Horizon prevents the announcements of route information to the receiving

interface of this route information. In this way, communication within several routers (especially when the loop breaks) will be optimized.

If an interface has been configured with a supplementary IP Address and he Horizontal Split has been activated, the update-Source IP Address of the route update may not include every secondary IP address. The source IP address of one route update includes only one Network Number (unless the split-horizon is Prohibited).

In order to activate or prohibit the Horizontal Split, the following commands should be taken under interface configuration mode:

Command	Purpose
ip rip split-horizon	Activate the Split- Horizon
no ip rip split-horizon	Prohibit the Split- Horizon

Under the default circumstance, for the point to Point Interface, the Split-Horizon is activated; For Point-to multiple point Interface, the Split-Horizon is prohibited.

Please refer to the specific example of using Split-Horizon in the "Examples of Split-Horizon" in Section of this Chapter.

Notes:

Commonly, it is suggested that the default state remain unchanged unless you are sure that your application cannot advertise the route correctly until you change its state.

4.3.13 Monitoring and Maintenance of RIP

With the RIP monitored and maintained, the Network Statistics can be displayed, such as: RIP protocol Parameter Configuration, Network utilization, Real-time Tracing of Network Communication and so on. Such information can help you judge the use of Network Resource and further solve the network problems and know the reachability of network nodes .

The following commands can be used to display the statistics information of all kinds of routes under management statistics:

Command	Purpose
show ip rip	Display the present Status of RIP
show ip rip *database*	Display all routes of RIP
Show ip rip protocol	Display all the relevant information of RIP Protocol

Under the management mode, the following commands shall be used to trace route protocol information.

Command	Purpose
Debug ip rip database	Trace the procedure information of RIP Routing such as Insertion into the Routing Table, Deletion from the Routing Table, Changes of Routes and so on.

Debug ip rip protocol	Trace the RIP protocol messages.

4.4 Example of the RIP Configuration

Examples of the RIP Configuration is included in this section:

RouterA

```
interface ethernet 1/1
ip address 192.168.20.81 255.255.255.0
!
interface loopback 0
ip address 10.1.1.1 255.0.0.0
!
router rip
  network 192.168.20.0
  network 10.0.0.0
!
```

RouterB

```
interface ethernet 1/1
ip address 192.168.20.82 255.255.255.0
interface loopback 0
ip address 20.1.1.1 255.0.0.0
!
router rip
network 192.168.20.0
network 20.0.0.0
!
```

Chapter 5 Configuring OSPF

5.1 Overview

The OSPF Configuration will be introduced in this chapter. For more specific detailed information about all the OSPF commands, please refer to the relevant sections about OSPF Commanders in the Reference for Network Protocol Configuration.

OSPF is an IGP Route protocol developed by the OSPF Working Group of IETF. The OSPF, which is designed for the IP Network, supports the IP Sub-network and the External Route Information Label and at the same time allows the authentication of message and supports the IP Multicast.

The Implementation of OSPF of our company complies with the OSPF V2 specification (Refers to RFC2328). Some key feathers in the implementation are listed in the following:

- Stub Area--Supporting the Stub Area
- Route redistribution--Any route, formed by and learned a routing protocol, can always be redistributed to the other route protocol Domain. Within the autonomous System, it means that OSPF can input the route learned by the RIP. And the routes learned by OSPF can also be redistributed to the RIP. Between autonomous Systems, OSPF can input the routes learned by BGP; and OSPF routes can also be injected to BGP.
- Authentication--The Plaintext and MD5 Authentications are supported between the neighboring routers within a area.
- Router Interface Parameters--The configurable Parameters include: Outgoing Cost, Retransmission Interval, Interface Transmission Delay, router Priority, Judgement on the router Switching-off Interval, the Interval of Hello Message and the Authentication Password.
- Virtue Link--Supporting the Virtue Link
- NSSA area--Refer to RFC 1587
- OSPF---RFC 1793 on the virtual circuit.

5.2 OSPF Configuration Tast List

OSPF requires to exchange routing data among all routers, ABR and ASBR in a area. In order to simplify the configuration, you may let them all work under default parameters without authentication, etc… but if you want to alter some parameters, you should guarantee the identity of the parameters on all routers.

In order to configure OSPF complete the following tasks. Besides the necessity of activating OSPF, other configurations are all optional.

- Start OSPF
- Configure the interface parameter of OSPF
- OSPF configuration on different physical networks
- Configure route summary within OSPF domain
- Configure the gathering of a forward router
- Create default route
- Select router ID through LOOPBACK interface
- Configure the management distance of OSPF
- Configure the route calculating timer
- The supervision and maintenance of OSPF

In addition to that, about configuring route redistribution, please refer to the related content about “Route Redistribution” of “Protocol-independent Feather Configurations of IP routing Protocol”.

5.3 OSPF Configuration Tast

5.3.1 Starting OSPF

Like other routing protocols, activating OSPF demands creating OSPF routing process, allocation of an IP address range related to the executing process, allocation of an area ID related to IP address range. Under the global configuration mode, use the following commands:

Command	Purpose
router ospf *process-id*	This command activates OSPF routing protocol, and enters router configuration mode.
network *address mask* **area** *area-id*	This command configures the interface(s) running OSPF and the area ID of the interface

5.3.2 Configuring the Interface Parameter of OSPF

During the implementation of OSPF, it is permitted to change the OSPF parameters related to interface according to the requirement. There is no need to change any parameter, but you should guarantee the identity of certain parameters on all routers on connected network.

Under interface configuration mode, use the following commands to configure interface parameters:

Command	Purpose
ip ospf cost *cost*	Configure the metric of OSPF interface to forward packets.
ip ospf retransmit-interval *seconds*	The seconds taken to retransmit LSA between the neighbors belonging to the same OSPF interface.
ip ospf transmit-delay *seconds*	Configure the estimated time to transmit LSA on an OSPF interface (second as the unit).
ip ospf priority *number*	Configure the priority of router to become the DR router
ip ospf hello-interval *seconds*	Configure the time interval to send hello packet on OSPF interface.
ip ospf dead-interval *seconds*	If the router does not receive “hello” packet from the neighbor within the time interval defined, it considers the neighbor router to be turned off.
ip ospf authentication-key *key*	It is an authentication password of the adjacent router in an address, which uses simple password authentication of OSPF.
ip ospf message-digest-key *keyid* **md5** *key*	Demand OSPF to use MD5 authentication.
ip ospf passive	Do not send “hello” message on the interface.

5.3.3 Configuring OSPF Network Type

The OSPF network type can be configured as broadcast, non-broadcast multi-access, point-to-point or point-to-multipoint to match the logical topology.

Configure non-broadcasting, multi-access network to be broadcasting network or non-broadcasting network, that is, to suppose there exists virtual links from every router to other routers, or suppose they consist of a full-mesh network. Because of the restriction of expenses, it is usually not practical; or a partially full-mesh network. Under this situation, you can configure a point-to-multiple point network. Routers not adjacent to each other can exchange routing information through virtual links.

OSPF point-to-multiple point interface can be defined as several point-to-point network interfaces, which creates multiple host routes. OSPF point-to-multiple point network has the following advantages over non-broadcasting, multi-access network and point-to-point network:

Point-to-multiple point network is easy to configure, it does not demand neighbor configuration command, it only uses one IP and will not produce DR.

Because it does not need to full-mesh network topology, it costs less.

It is more reliable. Even when virtual links fail, it can still maintain the connection.

Under interface configuration mode, configure OSPF network type with the following command:

Command	Purpose
ip ospf network {**broadcast** | **non-broadcast** | {**point-to-multipoint** [**non-broadcast**] }}	This command configures the network type of OSPF.

5.3.4 Configuring One-to-Multiple Broadcast Network

You do not need to describe the neighbor relations in point-to-multiple point network and broadcasting network. But you can use command “neighbor” to describe the priority of a certain neighbor.

Before using this command, some OSPF point-to-multiple point protocol traffic is multicast traffic. So for point-to-multiple point interface, command “neighbor” is not needed. Packet “hello”, update packet and confirmation packet are all transmitted through broadcasting form, especially, multicast “hello” packet can dynamically discover all neighbors.

In point-to-multiple point network, the router supposes that all neighbors have the same metric. This value can be configured through command “ip ospf cost”. In fact, the bandwidth of every neighbor is different, so the value should be different. This feature only applies to point-to-multiple point interface.

Using the following command to configure the interface to be point-to-multipoint interface and allocate a metric for each neighbor:

Command	Purpose
ip ospf network point-to-multipoint	On broadcasting media, configure the interface to be a point-to-multiple point network
Exit	Return to global configuration mode
router ospf *process-id*	Configure an OSPF router process and enter into router configuration mode.
neighbor *ip-address* cost *number*	Designate a neighbor and allocate a metric for it

For each neighbor wishing to designate its metric, repeat step 4. Otherwise use the value designated by command “ip ospf cost”.

5.3.5 Configuring Non-Broadcasting Network

Because there are many routers in the OSPF network, so there must be one DR elected for the network. If the broadcasting ability is not configured, it is requested to perform parameter configuration for the selection process.

These parameters only carry out configuration on the routers that are eligible to become DR or BDR.

Under router configuration mode, use the following command to configure routers of non-broadcasting network which are mutually related:

Command	Purpose
neighbor *ip-address* [**priority** *number*] [**poll-interval** *seconds*]	Configure the router connected to the non-broadcasting network

You can designate the following parameters for a neighbor router:

- The precedence of neighbor router.
- Non-broadcasting poll interval.
- Interface accessible to the neighbor

In point to multiple point, non-broadcasting network, you can use command “neighbor” to designate neighbor relation. Allocate an optional priority.

In the previous software versions, some users configure point to multipoint connections on non-broadcasting media (IP over ATM), so the router cannot dynamically discover its neighbor router. This feature permits the usage of command “neighbor” on point to multipoint interface.

In a point to multipoint network, the router supposes all neighbors have the same metric. This value can be configured through the command “ip ospf cost”. In fact, as the bandwidth of each neighbor is different, the value should also be different. This feature only applies to point to multiple point interfaces.

Under interface configuration mode, use the following command to configure point to multiple point interfaces on media that do not support broadcasting.

Command	Purpose
ip ospf network point-to-multipoint non-broadcast	Configure point to multiple point interface on non-broadcasting media
exit	Enter into global configuration mode.
router ospf *process-id*	Create a OSPF routing process and enter into router configuration mode
neighbor *ip-address* [**cost** *number*]	Designate an OSPF neighbor and allocate a metric for it

Repeat step 4 for each neighbor.

5.3.6 Configure OSPF domain

Configurable area parameters include: authentication, designating Stub area, designating metric for default summary route. Authentication adopts protection based on passwords.

Stub areas are those that don’t distribute external routes in them. Instead, ABR generates a default external route to enter the stub area, enable it to enter the external

network of the autonomous system. in order to utilize the features OSPF Stub support, you should use default route in the Stub area. In order to additionally reduce LSA number sent into the Stub area, you can prohibit gathering ABR to reduce the sending of summary LSA (type3) entered into the Stub area.

Under router configuration mode, use the following command to define the area parameter:

Command	Purpose
area *area-id* **authentication simple**	Activates OSPF area authentication
area *area-id* **authentication message-digest**	Enables OSPF to use MD5 for authentication
area *area-id* **stub** [**no-summary**]	Defines a Stub area
area *area-id* **default-cost** *cost*	Sets metric for default route in Stub area.

5.3.7 Configuring the NSSA Area of OSPF

The NSSA area is similar to the STUB area. However, the NSSA area allows external routes to be entered. The route summary and packet filtration are also supported during transmission. If ISP requires to use the remote network with different routing protocols, the NSSA can simplify management.

The enterprise-core boundary router cannot run in the STUB area of OSPF if NSSA is not applied. That's because the routes of the remote network cannot be forwarded to the STUB area. The simple routing protocols such as RIP can be advertised, but two kinds of routing protocols need be maintained. NSSA can put the center router and the remote router in the same NSSA area and OSPF thus be applied to the remote network.

When the NSSA area is used, note that the route generated by the ABR router can enter the NSSA area once NSSA is configured. Each router in the same area must admit that they are in the NSSA area, or different routers cannot communicate with each other. The displayed release must be used on ABR to avoid packet transmission confusement of the router.

Run the following command in router configuration mode to set the NSSA area of OSPF:

Command	Purpose
Area area-id nssa [**no-redistribution**][**no-summary**][**default-information -originate**]	Configures the OSPF NSSA area.

5.3.8 Configuring Route Summary Within OSPF Domain

This feature enables ABR to broadcast a summary route to other areas. In OSPF, ABR will broadcast every network to other areas. If the network number can be allocated according to a certain method, and be continuous, you can configure ABR to broadcast a summary route to other areas. A summary route can cover all networks within a certain range.

Under router configuration mode, use the following commands to define the address ranges:

Command	Purpose
area *area-id* **range** *address mask*	Define the address range for route summary.

5.3.9 Configuring the Gathering of a Forwarding Router

When distributing routes from other router areas to OSPF router area, each performs independent broadcasting in the form of external LSA. But you can configure the router to broadcast a route, which covers a certain address range. This method can reduce the size of OSPF link status database.

Under the router configuration mode, use the following command to configure gathering the router:

Command	Purpose
summary-address *prefix mask* [**not advertise**]	Describe the address and mask that cover the distribution route, only one gathering route is broadcasted.

5.3.10 Creating Default Route

You can demand ASBR to create a default route to enter into the OSPF route area. Whenever you configure a router distribute route to enter into OSPF domain, this router automatically changes into ASBR. But, ASBR does not create default route entering into OSPF route area by default.

Under router configuration mode, use the following command to force ASBR to create a default route:

Command	Purpose
default-information originate [**always**] [**route-map** *map-name*]	Force ASBR to create a default route entering into OSPF route area.

5.3.11 Selecting Router ID Through Loopback Interface

OSPF uses the biggest IP address configured on the interface as its router ID. If the interface connected to this IP address changes into DOWN state, or this IP address is deleted, OSPF process will restart to calculate new router ID and resend routing information from all interfaces.

If one loopback interface is configured with IP address, then the router uses that IP address as its router ID, since loopback interface will never become Down, and all these make the routing table more stable.

The router preferably uses LOOPBACK interface as the router ID, meanwhile selects the biggest IP address among all loopback interfaces as the router ID. If there is no loopback interface, then uses the biggest IP address of the router. You cannot designate OSPF to use any special interface.

Under global mode, use the following command, to configure IP Loopback interface.

Command	Purpose
interface loopback 0	Create a loopback interface and enter into

	interface configuration mode.
ip address *ip-address mask*	Allocate an IP address for the interface.

5.3.12 Configuring the Management Distance of OSPF

Management distance is defined as the reliability level of routing information source, such as a router or a group of routers. Generally speaking, management distance is an integer between 0-255, the higher the value is, the lower the reliability level it is. If the management distance is 255, then the route information source will not be trusted and should be neglected.

OSPF uses 3 different types of management distances: inter-domain, inner-domain and exterior. The route within an area is inner-domain; the route to other areas is inter-domain; the route distributed from other route protocol domains is exterior. The default value of every kind of route is 110.

Under router configuration mode, use the following command to configure the distance value of OSPF:

Command	Purpose
distance ospf [**intra-area** *dist1*] [**inter-area** *dist2*] [**external** *dist3*]	Change the management distance value of OSPF inner-domain, inter-domain and exterior route.

5.3.13 Configuring the Route Calculation Timer

You can configure the time delay between the time when OSPF receives topologic change information and when it starts to calculate SPF. You can also configure the interval between two consecutive calculations of SPF. Under router configuration mode, use the following command to configure:

Command	Purpose
timers delay *delaytime*	Set the time delay in the route calculation in a area.
timers hold *holdtime*	Set the minimum time interval of route calculation in a area.

5.3.14 Monitoring and Maintaining OSPF

It can display the statistic information of the network, such as: the statistics about the content of IP routing Table, cache and database and etc… This information can help you to judge the utilization of the network resource, and solve the network problem. You can understand the availability of the network nodes, discover the route the network data packet goes through the network.

Use the following commands to display various routing statistics:

Command	Purpose
show ip ospf [*process-id*]	Display the general information about OSPF routing process.
show ip ospf *process-id* [**database** [**router**|**network**|**summary**|**asbr-summary**|**external**| **database-summary**]][*link-state-id*][**self-originate**]	Display the related information about OSPF database.
show ip ospf border-routers	Display the internal routing table entry of ABR and ASBR.
show ip ospf interface	Display the information about OSPF interface.
show ip ospf neighbor	Display the OSPF neighbor information according to the interface.
debug ip ospf adj	Supervise the adjacency establishment of OSPF.
debug ip ospf events	Supervise the interface and neighbour events of OSPF.
debug ip ospf flood	Supervise the flooding process of OSPF database.
debug ip ospf lsa-generation	Supervise the LSA generation of OSPF.
debug ip ospf packet	Supervise the message of OSPF.
debug ip ospf retransmission	Supervise the message retransmission process of OSPF.
debug ip ospf spf [**intra**| **external**]	Supervise the SPF calculation route of OSPF.

5.4 Examples of OSPF Configuration

5.4.1 Examples of the configuration of OSPF route and route distribution

OSPF requires exchanging information among many internal routers, ABRs and ASBRs. Under minimum configuration, the routers based on OSPF can work under default parameters and have no requirement of authentication.

Here are three examples of configuration:

The first example practices the basic OSPF command.

The second example configures the configuration of internal router, ABR and ASBR in a single OSPF autonomous system.

The third example illustrates a more complex example of configuration with various OSPF tools.

1. An example of basic OSPF configuration

The following example illustrates a simple OSPF configuration. Activate routing process 90 , then connect the Ethernet interface 0 to area 0.0.0.0. Meanwhile, redistribute RIP to OSPF, OSPF to RIP.

```
interface ethernet 1/0
  ip address 130.130.1.1 255.255.255.0
  ip ospf cost 1
!
interface ethernet 1/0
  ip address 130.130.1.1 255.255.255.0
!
router ospf 90
  network 130.130.0.0 255.255.0.0 area 0
  redistribute rip
!
router rip
  network 130.130.0.0
  redistribute ospf 90
```

2. An example of the basic configuration of inner router, ABR and ASBR

The following example allocates 4 areas ID for 4 IP address range. Firstly, routing process 109 is activated, the 4 areas are: 10.9.5.0, 2, 3, 0. The masks of area 10.9.50.0,2,3 designate the address range, but area 0 includes all the networks.

```
router ospf 109
  network 131.108.20.0 255.255.255.0 area 10.9.50.0
  network 131.108.0.0 255.255.0.0 area 2
  network 131.109.10.0 255.255.255.0 area 3
  network 0.0.0.0 0.0.0.0 area 0
!
! Interface Ethernet1/0 is in area 10.9.50.0:
interface ethernet 1/0
  ip address 131.108.20.5 255.255.255.0
!
```

```
! Interface Ethernet1/1 is in area 2:
interface ethernet 1/1
  ip address 131.108.1.5 255.255.255.0
!
! Interface Ethernet1/2 is in area 2:
interface ethernet 1/2
  ip address 131.108.2.5 255.255.255.0
!
! Interface Ethernet1/3 is in area 3:
interface ethernet 1/3
  ip address 131.109.10.5 255.255.255.0
!
! Interface Ethernet1/4 is in area 0:
interface ethernet 1/4
  ip address 131.109.1.1 255.255.255.0
!
! Interface FastEthernet0/0 is in area 0:
interface FastEthernet0/0
  ip address 10.1.0.1 255.255.0.0
```

The functions of network area configuration command are ordinal, so the order of the commands is important. The router matches the address/mask pair of each interface in order. For detailed information, please refer to the related content in the reference of related network protocol command in “OSPF command”.

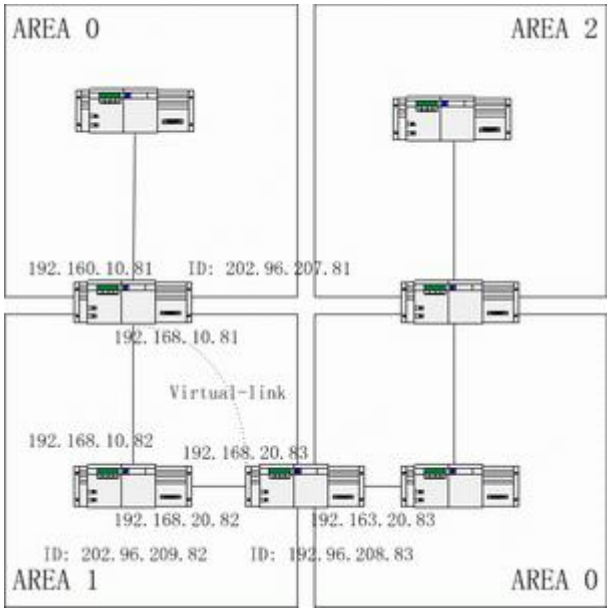
Let’s return to the first network area in the above example. The area ID 10.9.50.0 is configured with an interface sub-network mask as 131.108.20.0. So Ethernet interface 0 matches. So Ethernet interface 0 only exists in area 10.0.50.0.

Then come to the second area. Except interface 0, apply the same process on other interfaces, then Ethernet interface 1 matches. So interface 1 connects to area2.

Continue the matching of other network areas. NOTICE that the last network area command is a special case, which means that the rest interfaces are all connected to network area 0.

An example of the complex configuration of interior router, ABR and ASBR.

The following example illustrates the configuration of several routers in a single OSPF autonomous system. Figure 24 is the network topology of the example:



1. Configure the router according to the above Figure:

RouterA:

```
interface loopback 0/0
ip address 202.96.207.81 255.255.255.0
!
interface Ethernet 1/0
ip address 192.168.10.81 255.255.255.0
!
interface ethernet 1/0
ip address 192.160.10.81 255.255.255.0
!
router ospf 192
network 192.168.10.0 255.255.255.0 area 1
network 192.160.10.0 255.255.255.0 area 0
!
```

RouterB:

```
interface loopback 0/0
ip address 202.96.209.82 255.255.255.252
!
interface Ethernet 1/0
ip address 192.168.10.82 255.255.255.0
!
interface ethernet 1/1
ip address 192.160.20.82 255.255.255.0
!
router ospf 192
network 192.168.20.0 255.255.255.0 area 1
```

```
network 192.168.10.0 255.255.255.0 area 1
!
```

routerC:

```
interface loopback 0/0
ip address 202.96.208.83 255.255.255.252
!
interface Ethernet 1/0
ip address 192.163.20.83 255.255.255.0
!
interface ethernet 1/1
ip address 192.160.20.83 255.255.255.0
!
router ospf 192
network 192.168.20.0 255.255.255.0 area 1
network 192.163.20.0 255.255.255.0 area 0
!
```

3. Configuration examples for complicated internal router, ABR and ASBR

The following example shows how to configure multiple routers in a single OSPF autonomous system. Figure 4-2 shows the network topology of the configuration example:

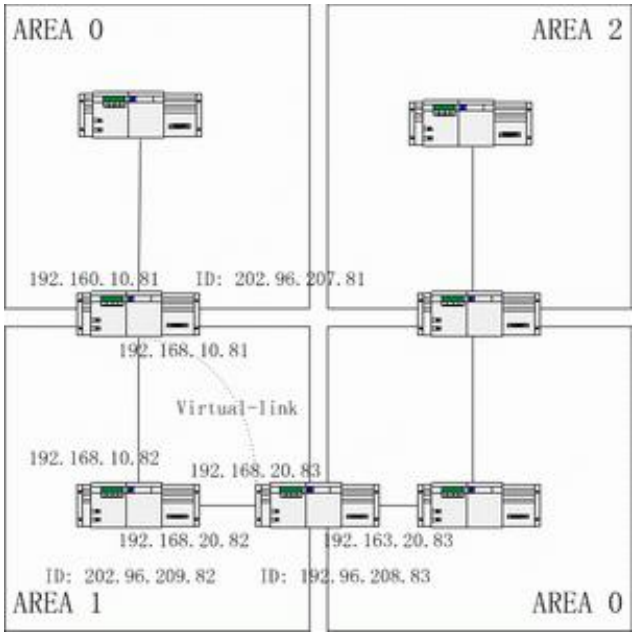


Figure 4-2 Network topology of the configuration example

Configure the router according to Figure 4-2:

Router A:

```
interface loopback 0/0
ip address 202.96.207.81 255.255.255.0
!
interface Ethernet 1/0
ip address 192.168.10.81 255.255.255.0
!
interface ethernet 1/0
ip address 192.160.10.81 255.255.255.0
!
router ospf 192
network 192.168.10.0 255.255.255.0 area 1
network 192.160.10.0 255.255.255.0 area 0
!
```

Router B:

```
interface loopback 0/0
ip address 202.96.209.82 255.255.255.252
!
interface Ethernet 1/0
ip address 192.168.10.82 255.255.255.0
!
interface ethernet 1/1
ip address 192.160.20.82 255.255.255.0
!
router ospf 192
network 192.168.20.0 255.255.255.0 area 1
network 192.168.10.0 255.255.255.0 area 1
!
```

Router C:

```
interface loopback 0/0
ip address 202.96.208.83 255.255.255.252
!
interface Ethernet 1/0
ip address 192.163.20.83 255.255.255.0
!
interface ethernet 1/1
ip address 192.160.20.83 255.255.255.0
!
router ospf 192
network 192.168.20.0 255.255.255.0 area 1
network 192.163.20.0 255.255.255.0 area 0
!
```

4. an example of complex OSPF on ABR router configuration

Here is an example of OSPF configuration:

```
interface ethernet 1/0
ip address 192.168.20.81 255.255.255.0
ip ospf password GHGHGHG
ip ospf cost 10
!
interface ethernet 1/1
ip address 192.168.30.81 255.255.255.0
ip ospf password ijklmnop
ip ospf cost 20
ip ospf retransmit-interval 10
ip ospf transmit-delay 2
ip ospf priority 4
!
interface ethernet 1/2
ip address 192.168.40.81 255.255.255.0
ip ospf password abcdefgh
ip ospf cost 10
!
interface ethernet 1/3
ip address 192.168.0.81 255.255.255.0
ip ospf password ijklmnop
ip ospf cost 20
ip ospf dead-interval 80
!
router ospf 192
network 192.168.0.0 255.255.255.0 area 0
network 192.168.20.0 255.255.255.0 area 192.168.20.0
network 192.168.30.0 255.255.255.0 area 192.168.30.0
network 192.168.40.0 255.255.255.0 area 192.168.40.0
area 0 authentication simple
area 192.168.20.0 stub
area 192.168.20.0 authentication simple
area 192.168.20.0 default-cost 20
area 192.168.20.0 authentication simple
area 192.168.20.0 range 36.0.0.0 255.0.0.0
area 192.168.30.0 range 192.42.110.0 255.255.255.0
area 0 range 130.0.0.0 255.0.0.0
area 0 range 141.0.0.0 255.0.0.0
redistribute rip
RIP on network 192.168.30.0
router rip
network 192.168.30.0
redistribute ospf 192
```

!

Chapter 6 Configure BGP

6.1 Overview

This chapter describes how to configure border gateway protocol (BGP). For complete description about BGP commands in this chapter, please refer to other sections related to “BGP command”. BGP is an Exterior Gateway Protocol (EGP) defined in RFC1163, 1267 and 1771. It permits to establish a route selection mechanism among different autonomous systems, this mechanism can automatically guarantee the loop-free routing information exchange between the autonomous systems.

6.1.1 The BGP implementation of the router

In BGP, each route includes a network number, the autonomous system list this route has tranverse (called As-path) and other attribute lists. Our router software supports BGP v4 defined in RFC1771. The basic function of BGP is to exchange network reachability information with other BGP systems, including information about AS-path information. This information can be used to construct the AS connection graph which can eliminate route loop, and it can implement AS level routing policy with AS connection graph. BGP v4 supports classless inter-domain router (CIDR), CIDR can reduce the size of the routing table through creating summary routes and thus creates a super network. CIDR removes the concept of network level in BGP, and supports IP prefix broadcasting. CIDR route can be transferred through OSPF, Enhanced IGRP, ISIS-IP and RIP2.

An important difference between exterior gateway routing and interior gateway router is the former has better controllability. In order to control the route, the implementation of BGP provides several optional methods:

- In order to filter routes, it can be based on access-list based on neighbour, aspath-list, prefix-list and also use the access-list based on interface, prefix-list to filter routes or the Nexthop attribute of the routes.
- In order to change the attribute of the routes, you can use the route-map to mend the attributes of BGP routes including MED, Local preference, route value and etc…
- In order to interact with the interior gateway dynamic routing protocol (OSPF, RIP, etc…), you can redistribute route, so as to automatically generate BGP routing information. You can also generate BGP routes through manual configuration of network, aggregation. While generating BGP routes, you can use route-map to configure the attributes of the routes.
- In order to control the precedence of BGP routes in the system, you can use command “distance” to configure the management distance of BGP routes.

6.1.2 How does BGP select the path

The decision process of BGP is established on the basis of comparing route attribute value. When the same network has several routes, BGP selects the best route to the destination. The following process summarizes how BGP selects the best route:

- If it cannot arrive at the next hop, it will not be considered.
- If the path is internal and the synchronization is activated, and if the route is not in IGP, the route will not be considered.
- Select preferable path with the maximum precedence.
- If each route has the same value, preferably select the route with the maximum local precedence.
- If each route has the same local precedence, select preferably the route generated by local router. For example, route may be generated by local router through the using of command “network, aggregate” or by redistributing IGP route.
- If the local precedences are the same, or if there is no route generated by local router, then select preferably the route with the shortest AS path.
- If the AS path lengths are the same, then select preferably the route with the lowest attribute value of “origin” (IGP<EGP<IMCOMPLETE)
- If the attribute values of “Origin” are the same, then select preferable route with the lowest MED value. Unless “bgp always-compare-med” is activated, this comparable can only be carried out between the routes from the same neighbour AS.
- If each route has the same MED, select preferable external path (EBGP) rather than internal path (IBGP). All paths inside the autonomous system confederation are considered to be internal paths, but select preferably EBGP confederation not IBGP confederation.
- If each route has the same connection attribute, select preferable route with a smaller router-id.

6.2 BGP Configuration Task List

6.2.1 Basic configuration task list of BGP

The configuration tasks of BGP can be divided into basic tasks and advanced tasks. The first two entries of basic tasks are necessary to configure BGP, other entries in basic tasks and all advanced tasks are optional.

The basic configuration tasks of BGP include:

- Activate the route selection of BGP.
- Configure BGP neighbor.

- Configure BGP soft reconfiguration
- Reset BGP connection.
- Configure the synchronization between BGP and IGPs
- Configure BGP route value
- Configure BGP route filter based on the neighbour
- Configure BGP route filtration based on the interface
- Disable the nexthop treatment of BGP update

6.2.2 Advanced BGP configuration tasks list

Advanced, optional BGP configuration tasks are listed as the following:

- Use route-map to filter and modify route update
- Configure aggregate address
- Configure BGP community attribute
- Configure autonomous system confederation
- Configure route reflector
- Shut down peer entity
- Configure multihop external peer body
- Configure the management distance of BGP routes
- Adjust BGP timer.
- Compare MED of routes from different AS.

For more related information about the configuration of the attributes of several IP route selection protocols, please refer to“The configuration of attributes of IP routing which are independent from the protocol”.

6.3 Configure basic BGP features tast

6.3.1 Configuring Basic BGP Features

1. Activate the route selection of BGP

In order to activate BGP route selection, use the following commands under global configuration mode to activate BGP route selection:

Command	Purpose

router bgp autonomous-system	Under router configuration mode, activate BGP route selection process.
network *network-number*/*masklen* [**route-map** *route-map-name*]	Tag the network as local autonomous system and add it to the BGP list.

Notes:

For exterior gateway routing protocol, the using of configuration command “network ” to configure an IP network canand to only control which networks will be informed. This is opposite to interior gateway protocol (IGP), such as RIP, it is using command “network” to decide where to send the update.

Command “network” is used to import IGP routes to BGP routing table. Router resource, such as configured RAM, decides the upper limit of the usable command “network”. As a choice, you can use command “redistribute” to achieve the same effect.

2. Configure BGP neighbour

To configure BGP neighbour is to establish the peer to exchange routing information. BGP neighbour ought to be configured in order to exchange routing information with the outer world.

BGP supports two kinds of neighbours: internal neighbour (IBGP) and external neighbour (EBGP). Internal neighbours are in the same AS; external neighbours are in different ASs. Normally, external neighbours are adjacent to each other and share the same sub-network. But internal neighbours can be at any place in the same AS.

Use configuration command “Neighbor” to configure BGP neighbour:

Command	Purpose
neighbor {*ip-address* | *peer-group-name*} **remote-as** *number*	Designate a BGP neighbour.

For example about the configuration of the BGP neighbor, please refer to the section in the bottom of this chapter “an example of the configuration of the BGP neighbor”.

3. Configure BGP soft reconfiguration

Generally speaking, BGP neighbors only exchange all routes when the connections are established, after that, they only exchange update routes. So if the configured routing policy gently changes, in order to apply it on the received routes, it is necessary to clear BGP session. The clearing of BGP session will cause the invalidation of cache and will exert great influence on the operation of the network. Soft reconfiguration function enables the configuration and activation of policy without clearing BGP session. So, we recommend you to use soft reconfiguration, currently, we enable the soft reconfiguration based on each neighbour. When the soft reconfiguration is used on the incoming update produced by the neighbor, it is called incoming soft reconfiguration; When the soft reconfiguration is used on the outcoming update to the neighbor, it is called outcoming soft reconfiguration. Applying incoming soft reconfiguration can make the new input policy effective, Applying outcoming soft reconfiguration makes new local output policy effective without the reset of BGP session.

In order to generate new incoming update without resetting of BGP session, local BGP speaker should save the received incoming update without any modification, regardless whether it would be accepted or denied under current incoming policy. This will be very memory consuming and should be avoided. On the other hand, outcoming reconfiguration does not have any extra memory consumption, so it is always effective.

You can trigger outcoming soft reconfiguration on the other side of BGP session to make the new local incoming policy effective.

In order to permit incoming soft reconfiguration, you should configure the BGP to save all accepted routing update. Outcoming reconfiguration need not be pre-configured.

Use the following router configuration command to configure BGP soft reconfiguration:

Command	Purpose
Neighbor {*ip-address* | *peer-group-name*} **soft-reconfiguration** [**inbound**]	Configure BGP soft reconfiguration

If you use parameter **"peer-community-name"** to designate BGP peer community, all peer community members in it will inherit the feature of this command.

4. Reset BGP connection

Once two routers are defined as BGP neighbours, they create a BGP connection, and exchange routing information. If the BGP routing policy has been changed, or other configurations have been changed, then you should reset the BGP connection in order to make the change of configuration effective. Use one of the following two management mode commands to reset BGP connection:

Command	Purpose
clear ip bgp {***** | *address}*	Reset all BGP connections. Recreate a special BGP connection.

5. Configure the synchronization between BGP and IGPs

If you permit another AS to transfer data to the third AS through your AS, then the synchronization between your AS internal routing state and the routing information it broadcasted to another ASs is very important. For example, if your BGP wants to broadcast routes before all routers in your AS get to know the routes through IGP, then your AS may receive some information that some routers cannot route. In order to prevent these situations, BGP should wait until all IGP routers inside AS get to know that routing information, this is the synchronization between BGP and IGP, and the synchronization is activated by default.

Under certain situations, it is not necessary to synchronize. If you do not permit other ASs to transfer data through your AS, or if all routers in your AS will run BGP, your can cancel the Synchronization function. Cancelling that feature will enable you to put fewer routes in your IGP, and enable quicker convergence of BGP. Use the following router configuration command to cancel synchronization:

Command	Purpose
no synchronization	Cancel the synchronization between BGP and IGP.

While canceling synchronization, you should use command "clear ip bgp" to clear BGP dialogue.

For an example about BGP synchronization, please refer to the section in the bottom of this chapter "an example of BGP path filtration by the neighbors".

Normally, you do not expect to redistribute all routes to your IGP. A common design is to redistribute one or two routes, and make them the external routes in IGRP, or force the BGP session to generate an AS default route. When BGP redistribute routes to IGP,

only the routes acquired through EBGP will be redistributed. Under most situations, you do not want to allocate your IGP to BGP, just use configuration command “network ” to list the network in AS, then your network will be broadcasted. The networks listed in this form are called local network, and enables BGP to have attribute “Origin” of IGP. They must appear in the main IP routing table, and are effective; for example, they are direct-connected routes, static routes or routes known through IGP. BGP routing process periodically scans the main IP routing table to check the existence of a local network, and accordingly updates BGP routing table if you really want BGP to execute redistribution, you must be very careful, because these may be the routes in IGP that are injected by other routers through BGP, this may bring force a kind of situation that BGP potentially injects the information into IGP, and then send back the information to BGP. Vice versa.

6. Configure BGP route value

BGP route value is a number set to BGP route in order to control the route selection process, value is local for the router. The value ranges from 0 to 65535. BGP route generated locally has a default value of 32768, the route got from the neighbour values 0. The administrator can implement routing policy through the change of route value.

Use the following router configuration command to configure BGP route weight:

Command	Purpose
neighbor {*ip-address* | *peer-group-name*} **weight** *weight*	Designate a value to each route from one neighbour.

Besides, you can change the route weight through route-map.

7. Configure BGP route filter based on the neighbour

There are 4 methods in BGP implementation of router software to filter BGP routes of the designated neighbours:

Use Aspath list filter together with global configuration command **“ip aspath-list”** and command “**neighbour filter-list**”.

Command	Purpose
ip aspath-list aspaths-list-name {**permit | deny**} as-regular-expression	Define an accessing list relative to BGP.
router bgp autonomous-system	Enter into router configuration mode.
neighbor {ip-address | peer-group-name} **filter-list** aspath-list-name {**in | out** }	Establish a BGP filter.

Use access list together with global configuration command “ip access-list” and command “neighbour distribute-list”.

Command	Purpose
ip access-list standard *access-list-name*	Define an access list.
router bgp *autonomous-system*	Enter into router configuration mode.
neighbor {*ip-address* | *peer-group-name*} **distribute-list** *access-list-name* {**in** | **out** }	Establish a BGP filter.

Use prefix list together with global configuration command “ip prefix-list” and command “neighbour prefix-list”.

Command	Purpose
ip prefix-list prefixs-list-name {permit |deny} A.B.C.D/n **ge** x **le** y	Define a prefix list.
router bgp *autonomous-system*	Enter into router configuration mode.
neighbor {*ip-address* | *peer-group-name*} **prefix-list** *prefix-list-name* {**in | out** }	Establish a BGP filter.

Use route-map together with global configuration command “route-map” and command “neighbour route-map”.

Using route-map can not only filter routes, but also changes routes attribute, the usage will be described in the following chapters.

For example based on neighbour filter route, please refer to “example of BGP route filtration based on the neighbor”.

8. Configure BGP route filtration based on the interface

Configuring BGP route filtration based on the interface can be achieved through using access list and prefix list. Network number and the gateway address of the routes can be filtered. It can designate “access-list” option to use access list for filtration of network number of the routes, designate “prefix-list” option to use prefix list for filtration of network number of the routes, designate “gateway” option to use access list for filtration of “nexthop” attribute of the routes. It can even filter the network number and “nexthop” attribute of routes at the same time, but “access-list” option cannot be used together with “prefix-list” option. Designate “*” can filter the routes on all interfaces.

To order to configure the filtration of BGP routes based on the interface, you should carry out the following configurations under BGP configuration mode:

Command	Purpose
filter interface { in | out }[access-list *access-list-name][prefix-list prefix-list-name]* [gateway access-list-name]	Filter BGP routes based on the interface.

For examples of route filtration based on the interface, please refer to “examples of BGP route filtration based on the interface”.

9. Disable the nexthop treatment of BGP update

A BGP neighbor may not directly access every other neighbor in its IP subnet. You can change next-hop handling in three ways:

1. Use the local IP address of this BGP connection to replace the nexthop address of the outcoming route;

2. Use route-map to designate the nexthop address of incoming or outcoming routes. (Please refer to other chapters)

3. Use the following router configuration command to disable nexthop treatment and use the local IP address of this BGP connection to replace the nexthop address of the outcoming routes.

Command	Purpose
neighbor {*ip-address* | *peer-group-name*} **next-hop-self**	Disable the nexthop treatment while carrying out BGP neighbour update.

Using this command to configure will enable the current router to inform itself to be the nexthop of the route. So, other BGP neighbours will forward packets to this network to the current router. This is very useful in non-broadcasting network environment, because there exists a path from the current router to the designated neighbor. But it is not the case in broadcasting network environment, because this will induce unnecessary extra hops.

6.3.2 Configuring advanced BGP features

1. Use route-map to filter and modify route update

You can use route-map to filter route update and modify parameter attribute based on each neighbour. Route-map can be applied both on incoming update and outcoming update. Only the routes passing route-map can be processed while sending or accepting route update.

Route-map supports incoming and outcoming update to match with AS path, community and network number. AS matching demands the using of command “aspath-list”; the matching based on community demands the using of command “community-list”, the matching based on the network demands the use of command “ip access-list”.

Use the following BGP configuration command to configure route-map for filtration and modification of route update:

Command	Purpose
neighbor {*ip-address* | *peer-group-name*} **route-map** *route-map-name* **{in | out}**	Apply route-map on incoming or outcoming routes.

For examples of using route-map to filter and modify the route update, please refer to “Examples of BGP route-map”.

2. Configure aggregate address

Classless inter-domain routing can create aggregate routing (and super network) to minimize the routing table. You can configure aggregate routing in BGP through redistributing aggregate routes to BGP or through using conditional aggregate attributes described in the following task list. If there is at least one more detailed record in BGP routing table, add the aggregate address to the BGP routing table.

Use one or more router configuration commands in the following to create an aggregate address in the routing table:

Command	Purpose
aggregate *network/len*	Create aggregate address in BGP routing table.
aggregate *network/len* **summary-only**	Broadcast summary address only.
aggregate *network/len* **route-map** *map-name*	Generate aggregate address according to conditions designated by route-map.

For examples regarding the using of BGP route aggregation, please refer to the section in the bottom of this chapter “examples of BGP route aggregation”.

3. Configure BGP community attribute

The routing policy that BGP supports is mainly based on one of the 3 values in BGP routing information:

- Network number of routes:
- as_path attribute value of routes:
- The “community” attribute value of routes

Dividing the routes into communities through “community” attribute, and applying the routing policy based on the community, thereby simplifies the configuration of control of routing information.

Community is a group of routes with the common attributes; each route may belong to several communities. AS administrators can define a certain route belongs to a certain community.

Community attribute is an optional and transferable global attribute ranging from 1 to 4,294,967,200. The famous communities pre-defined in the Internet communities include:

- No-export--- Do not advertise this route to EBGP peer (Including the EBGP peers inside the autonomous system confederation).
- No-advertise---Do not advertise this route to any peer .
- local-as---Do not advertise this route to the exterior of autonomous system (ca send this route to the other sub-AS peers in the autonomous system confederation.)

When generating, accepting or sending routes, BGP speakers can configure, add or modify the route community attribute. when aggregating routes, the generated aggregation includes the “community” attributes from complete communities of all original routes.

By default, “Community” attributes are not sent to the neighbor. Use the following BGP configuration command to designate sending “community” attribute to the neighbour:

Command	Purpose
neighbor {*ip-address* | *peer-group-name*} **send-community**	Designate to send attribute “community” to the neighbor.

You need to do the following jobs to configure community attribute for the router:

Command	Purpose
route-map *map-name sequence-number* **{deny | permit}**	Configure route-map.
set community *community-value*	Configure rule of setting.

router bgp *autonomous-system*	Enter into router configuration mode.
neighbor {*ip-address* | *peer-group-name*} **route-map** *access-list-name* {**in | out** }	Apply route-map.

To filter routing information based on community attributes, you need to do the following jobs:

Command	Purpose
ip community-list *community-list-name* {**permit | deny**} **communtiy-expression**	Define community list.
route-map *map-name* s*equence-number* **{deny | permit}**	Configure route-map.
match *community-list-name*	Configure rules of matching.
router bgp autonomous-system	Enter into router configuration mode
neighbor {*ip-address* | *peer-group-name*} **route-map** *route-map-name* {**in | out** }	Apply route-map.

For examples of using community attributes, please refer to “Examples of route-map using BGP community attribute”.

4. Configure autonomous system confederation

The way to reduce the number of IBGP connections is to divide an AS into several sub-AS, then form them into an autonomous system confederation. From the external perspective, the confederation looks like an AS. In the confederation, each sub-AS is full-mesh inside, and has connections with other sub-ASs in the same confederation. Even if there are EBGP sessions between peers of different sub-ASs, they may still exchange routing selection information like IBGP peers. Concretely speaking, it is saving the nexthop, MED and local precedence information.

To configure a BGP autonomous system confederation, you should designate the confederation identifier. The confederation identifier is an AS number, from an external perspective, the confederation is just like a single AS with AS number being the confederation identifier.

Use the following BGP configuration command to configure confederation identifier of the autonomous system:

Command	Purpose
bgp confederation0 identifier *autonomous-system*	Configure the confederation identifier of the autonomous system.

In order to designate the autonomous system number belonging to autonomous system confederation, use the following BGP configuration command:

Command	Purpose
bgp confederation peers autonomous-system [**autonomous-system ...**]	Designate the AS belongs to the confederation of autonomous system.

For examples of autonomous system confederation, please refer to “examples of BGP autonomous system confederation”.

5. Configure route reflector

Another method to reduce the number of IBGP connections instead of configuring autonomous system confederation is to configure route reflector.

The internal peers of the route reflector are divided into two groups: client peers and all other routers (non-client peers). The route reflector reflects the routes between the two groups; the route reflector and its client peers form a cluster. Non-client peers must be full-mesh connected, but client peers need not. The clients in the cluster do not communicate with IBGP speakers outside the cluster.

When route reflector receives routing information, it completes the following tasks:

- Broadcast the routes from external BGP speaker to all clents and non-client peers.
- Broadcast the routes from non-client to all clents.
- Broadcast the routes from the clients to all clients and non-client peers. So, the client peers need not be full-mesh-conneted.

Use the following router configuration command to configure the local router as the reflector and designate neighbors as the router reflector client:

Command	Purpose
neighbor *ip-address* **route-reflector-client**	Configure the local router as route reflector and designate neighbors as the client.

An AS may have several route reflectors, the way route reflector to process other route reflectors is the same as the processing of IBGP speakers.Normally, a cluster of clients have only one route reflector, and then the cluster is identified by the route reflector ‘s router ID. In order to increase the redundancy and avoid the failure of single node, a cluster may have more than one route reflectors. In this case, all the route reflectors in the cluster should be configured with 4-bit cluster ID, so that the route reflector can identify the update information of the route reflector in the same cluster. All the route reflectors belonging to the same cluster should be full-mesh-connected, and they should have the same client and non-client peer set.

If there is more than one route reflector in the cluster, you can use the following BGP configuration command to configure cluster ID:

Command	Purpose
bgp *cluster-id cluster-id*	Configure cluster-ID.

For examples of the configuration of route reflector, please refer to “examples of the configuration of BGP route reflector”.

6. Shut down peer entity

Use the following BGP configuration command to shut down BGP neighbour:

Command	Purpose
neighbor {*ip-address* | *peer-group-name*} **shutdown**	Shut down BGP neighbour.

Use the following BGP configuration command to activate the neighbour shut down previously:

Command	Purpose

no neighbor {*ip-address* | *peer-group-name*} **shutdown**	Activate BGP neighbour.

7. Configure multihop external peer body

By default, external peers should be on a directly connected network, in order to configure multihop external peer, you need to carry out the following task:

Command	Purpose
neighbor {*ip-address* | *peer-group-name*} **ebgp-multihop** ttl	Configure BGP neighbor as multihop external peer.

8. Configure the management distance of BGP routes

Management distance is a kind of measurement of the preference of different routing protocol. BGP uses 3 different management distances: external distance, internal distance and local distance. The routes obtained from external BGP will be assigned with the external distiance; the routes obtained from internal BGP will have a distance as internel distance, local routes will be given the local distance. Use the following BGP configuration command to configure BGP route management distance:

Command	Purpose
distance bgp {**external-distance| internal-distance| local-distance**}	Configure BGP route management distances.

The change of management distances of BGP route is dangerous, and normally it is not recommended. The external distance should be shorter than the distance of any other dynamic routing protocol and the internal distance should be longer than the distance of any other dynamic routing protocol.

9. Adjust BGP timer

Use the following BGP configuration command to adjust the BGP “keepalive” and “holdtime” timers of detailed neighbour:

Command	Purpose
neighbor *[ip-address | peer group-name]* **timers** *keepalive holdtime*	Set “keepalive” and “holdtime” timer interval (count with unit ‘second’) for designated peer or peer community

Use command “no neighbour timers” to reset the timer interval of BGP neighbor or peer community to the default value.

10. Compare MED of routes from different AS

MED is a parameter to be considered when selecting the best route from several paths. The path with lower MED value will be preferably considered than the route with higher MED value.

Under default situation, during the process of selecting the best route, MED’s comparison only takes place in the routes from the same AS. You can permit the MEDs’ comparison to take place in routing selection, regardless of which AS the routes come from.

Use the following BGP configuration command to realize the above objective:

Command	Purpose

bgp always-compare-med	Permit to make MEDs comparison among routes from different AS.

11. Configure the MD5 authentication for BGP neighbor

To make sure of the secure routing information forwarding between ASs, perform the password authentication on the BGP connection through the MD5 option provided by TCP.

Run the following command to achieve the previous purpose:

Command	Purpose
Neighbor A.B.C.D password LINE	Enables the MD5 authentication of the BGP neighbor and set the password.

You can run **no neighbor A.B.C.D password** to cancel the MD5 authentication for the BGP neighbor.

6.4 Monitoring and Maintaining BGP

The administrator can display or delete the BGP routing table or the content of other databases. Of course the detailed statistics information can also be displayed. The following are relative tasks:

- Deleting the BGP routing table and the database
- Displaying the routing table and the system statistics information
- Tracking the BGP information

6.4.1 Deleting the BGP Routing Table and the BGP Database.

The following table lists the tasks relative with high-speed cache deletion, table deletion or BGP database deletion. The commands listed in the following table are all run in EXEC mode.

Command	Purpose
clear ip bgp *	Resets all BGP connections.
clear ip bgp *as-number*	Resets the BGP connections of the designated autonomous system.
clear ip bgp *address*	Resets the BGP connections of the designated neighbor.
clear ip bgp address soft {in|out}	Deletes the incoming database or the outgoing database of the designated neighbor.
clear ip bgp *aggregates*	Deletes the routes generated in route aggregation.
clear ip bgp *networks*	Deletes the routes generated during forwarding process.
clear ip bgp *redistribute*	Deleting the routes generated by the

	network command.

6.4.2 Displaying the Routing Table and the System Statistics Information

The detailed statistics information about the BGP routing table or the database will be displayed. The provided information can decide resource utilization and help resolving network problems. The information about the node reachability can also be displayed.

You can run the following commands to display all kinds of routing statistics information:

Command	Purpose
show ip bgp	Displays the BGP routing table in the system.
show ip bgp prefix	Displays the routes which match the designated prefix list.
show ip bgp community	Displays the statistics information about the group attribute.
show ip bgp regexp *regular-expression*	Displays the routes which match the designated regular expression.
show ip bgp *network*	Displays the designated BGP route.
show ip bgp neighbors *address*	Displays the information about the TCP and the BGP connections of the designated neighbor.
show ip bgp neighbors *[address]* [**received-routes** | **routes** | **advertised-routes**]	Displays the routes learned from the special BGP neighbor.
show ip bgp paths	Displays the information about all BGP paths in the database.
show ip bgp summary	Displays the states of all BGP connections.

6.4.3 Tracking the BGP Information

You can observe BGP connection establishment and route transmission/reception by tracking the BGP information, which helps to locate the troubles and resolve the problems. The commands to track the BGP information are shown in the following table:

Command	Purpose
debug ip bgp *	Tracks the general BGP information.
debug ip bgp all	Tracks all BGP information.
debug ip bgp fsm	Tracks the BGP state machine.
debug ip bgp keepalive	Tracks the KeepAlive packets of BGP.
debug ip bgp *open*	Tracks the OPEN packets of BGP.
debug ip bgp *update*	Tracks the UPDATE packets of BGP.

6.5 Examples of BGP configuration

The following sections provide the examples of BGP configuration:

6.5.1 Example of BGP route-map

The following example illustrates how to use route-map to change the incoming route attribute from the neighbor. Set the metric of all routes that come from neighbour 140.222.1.1 and meet the requirement of ASPATH accessing list “aaa” to 200, local precedence value to 250, and they are accepted, all other routes will be denied.

```
router bgp 100
!
neighbor 140.222.1.1 route-map fix-weight in
neighbor 140.222.1.1 remote-as 1
!
route-map fix-weight permit 10
match as-path aaa
set local-preference 250
set weight 200
!
ip aspath-list aaa permit ^690$
ip aspath-list aaa permit ^1800
```

In the following example, the first entry of route-map “freddy” will set the MED attributes of all routes origining from autonomous system 690 to 127. The second entry allows the routes that don’t meet the above conditions to be transferred to neighbor 1.1.1.1.

```
router bgp 100
neighbor 1.1.1.1 route-map freddy out
!
ip aspath-list abc permit ^690_
ip aspath-list xyz permit .*
!
route-map freddy permit 10
match as-path abc
set metric 127
!
route-map freddy permit 20
match as-path xyz
```

The following example illustrates how to use route-map to change the routes from route redistribution:

```
router bgp 100
redistribute rip route-map rip2bgp
!
route-map rip2bgp
match ip address rip
set local-preference 25
```

```
set metric 127
set weight 30000
set next-hop 192.92.68.24
set origin igp
!
ip access-list standard rip
permit 131.108.0.0 255.255.0.0
permit 160.89.0.0 255.255.0.0
permit 198.112.0.0 255.255.128.0
```

6.5.2 Example of neighbour configuration

In the following example, BGP router belongs to AS109, and creates two networks. This router has 3 neighbors: the first neighbor is an external one (in different AS); the second is internal one (with the same AS number). The third is also an external one.

```
router bgp 109
network 131.108.0.0
network 192.31.7.0
neighbor 131.108.200.1 remote-as 167
neighbor 131.108.234.2 remote-as 109
neighbor 150.136.64.19 remote-as 99
```

6.5.3 Example of BGP route filtration based on the neighbor

Here is an example of BGP path filtration based on the neighbor. The routes passing through as-path access list “test1” will receive a metric value as 100. Only routes passing through as-path access list “test2” will be sent to 193.1.12.10, similarly, only those routes passing access list “test3” will be accepted by 193.1.12.10:

```
router bgp 200
neighbor 193.1.12.10 remote-as 100
neighbor 193.1.12.10 filter-list test1 weight 100
neighbor 193.1.12.10 filter-list test2 out
neighbor 193.1.12.10 filter-list test3 in
ip aspath-list test1 permit _109_
ip aspath-list test2 permit _200$
ip aspath-list test2 permit ^100$
ip aspath-list test3 deny _690$
ip aspath-list test3 permit .*
```

6.5.4 Examples of BGP route filtration based on the interface

The following is the example of the configuration of route filtration based on the interface. It filters the routes from interface e1/0 through access list “ac1”:

```
router bgp 122
filter e1/0 in access-list acl
```

The following example uses access list “filter-network” to filter the network numbers of the routes, and meanwhile, uses access list “filter-gateway” to filter gateway address of the routes from interface s1/0.

```
router bgp 100
filter s1/0 in access-list filter-network gateway filter-gateway
```

The following example: uses prefix list “filter-prefix” to filter the network numbers of the routes, and meanwhile, use accessing list “filter-gateway” to filter gateway address of routes from all interfaces.

```
router bgp 100
filter * in prefix-list filter-prefix gateway filter-gateway
```

6.5.5 Examples of using prefix list to configure route filtration

In the following example default route 0.0.0.0/0 is denied.

```
ip prefix-list abc deny 0.0.0.0/0
```

The following example: permits routes matching prefix 35.0.0.0/8:

```
ip prefix-list abc permit 35.0.0.0/8
```

In the following example, BGP process only accepts prefix with length ranges from /8 to /24:

```
router bgp
network 101.20.20.0
filter * in prefix max24
!
ip prefix-list max24 seq 5 permit 0.0.0.0/0 ge 8 le 24
!
```

In the following configuration, the router filters routes from all interfaces, it only accepts routes with prefix from 8 to 24:

```
router bgp 12
filter * in prefix-list max24
!
ip prefix-list max24 seq 5 permit 0.0.0.0/0 ge 8 le 24
```

Here are some other examples of configuration of prefix lists

The following example: permits routes with prefix length no more than 24 in network 192/8:

```
ip prefix-list abc permit 192.0.0.0/8 le 24
```

The following example: denies routes with prefix length of more than 25 in network 192/8:

```
ip prefix-list abc deny 192.0.0.0/8 ge 25
```

The following example: permits routes with prefix length of more than 8 yet less than 24 in all address space:

ip prefix-list abc permit 0.0.0.0/0 ge 8 le 24

The following example: denies all routes with prefix length of more than 25 in all address space:

ip prefix-list abc deny 0.0.0.0/0 ge 25

This example: denies routes from network 10/8, because if the mask on class A network 10.0.0.0/8 is smaller or equal to 32 bit, all routes from that network will be denied:

ip prefix -list abc deny 10.0.0.0/8 le 32

The following example: denies routes with mask length of more than 25 in network 204.70.1.24:

ip prefix-list abc deny 204.70.1.0/24 ge 25

The following example: permits all routes:

ip prefix-list abc permit any

6.5.6 Example of BGP route aggregation

The following example illusrates how to create aggregation routes in BGP.It may be created by route redistribution or the using of conditional route aggregation function.

In the following example, command “redistribute static” is used to redistribute aggregation route 193.*.*.*:

ip route 193.0.0.0 255.0.0.0 null 0

!

router bgp 100

redistribute static

When there is at least one route in the routing table within the designated range, the following configuration will create an aggregation route in BGP routing table. The aggregation route will be considered to be from your AS, and has the “atomic” attribution, to indicate the possibilities of the loss of information.

router bgp 100

aggregate 193.0.0.0/8

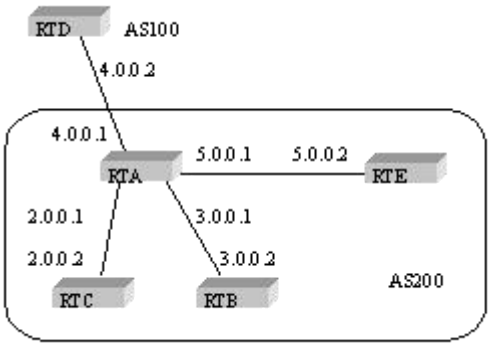
The following example not only creates an aggregation route 193.*.*.*, but also prohibit it to broadcast the more concrete routes to all the neighbours:

router bgp 100

aggregate 193.0.0.0/8 summary-only

6.5.7 Example of BGP route reflector

The following is an example of route reflector configuration. RTA, RTB, RTC, RTE all belong to the same autonomous system AS200, RTA serves as route reflector, RTB and RTC are route reflector clients, and RTE is normal IBGP neighbor. RTD belongs to AS100, and creates EBGP connection with RTA, the configuration is illustrated as the following:



RTA configuration:

```
interface s1/0
ip address 2.0.0.1 255.0.0.0
!
interface s1/1
ip address 3.0.0.1 255.0.0.0
!
interface s1/2
ip address 4.0.0.1 255.0.0.0
!
interface s1/3
ip address 5.0.0.1 255.0.0.0
!
router bgp 200
neighbor 2.0.0.1 remote-as 200     /*RTC IBGP*/
neighbor 2.0.0.1 route-reflector-client
neighbor 3.0.0.1 remote-as 200     /*RTB IBGP*/
neighbor 3.0.0.1 route-reflector-client
neighbor 5.0.0.1 remote-as 200     /*RTE IBGP*/
neighbor 4.0.0.2 remote-as 100     /*RTD EBGP*/
network 11.0.0.0/8
!
ip route 11.0.0.0 255.0.0.0 2.0.0.12
```

RTB configuration:

```
interface s1/0
ip address 3.0.0.2 255.0.0.0
!
router bgp 200
neighbor 3.0.0.1 remote-as 200     /*RTA IBGP*/
network 13.0.0.0/8
!
ip route 13.0.0.0 255.0.0.0 3.0.0.12
```

RTC configuration:

```
interface s1/0
ip address 2.0.0.2 255.0.0.0
!
router bgp 200
neighbor 2.0.0.1 remote-as 200     /*RTA IBGP*/
network 12.0.0.0/8
!
ip route 12.0.0.0 255.0.0.0 2.0.0.12
```

RTD configuration:

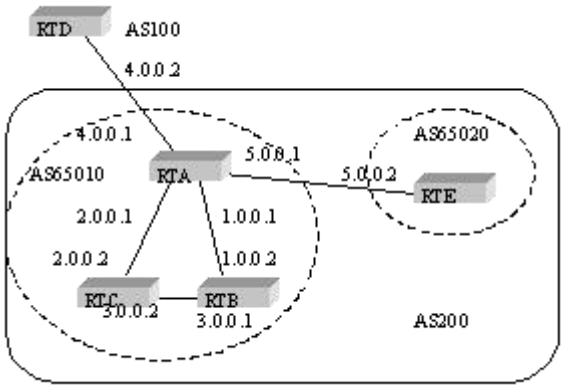
```
interface s1/0
ip address 4.0.0.2 255.0.0.0
!
router bgp 100
neighbor 4.0.0.1 remote-as 200     /*RTA EBGP*/
network 14.0.0.0/8
!
ip route 14.0.0.0 255.0.0.0 4.0.0.12
```

RTE configuration:

```
interface s1/0
ip address 5.0.0.2 255.0.0.0
!
router bgp 200
neighbor 5.0.0.1 remote-as 200     /*RTA IBGP*/
network 15.0.0.0/8
!
ip route 15.0.0.0 255.0.0.0 5.0.0.12
```

6.5.8 Example of BGP confederation

The following is the configuration of confederation. RTA, RTB, RTC create IBGP connections, and it belongs to a private autonomous system 65010; RTE belongs to another private autonomous system 65020; RTE and RTA establish internal EBGP connection of confederation; AS65010 AS65020 comprise the confederation, whose identifier is AS200; RTD belongs to autonomous system AS100, RTD establishes EBGP connection with autonomous system 200 through RTA.



RTA configuration:

```
interface s1/0
ip address 1.0.0.1 255.0.0.0
!
interface s1/1
ip address 2.0.0.1 255.0.0.0
!
interface s1/2
ip address 4.0.0.1 255.0.0.0
!
interface s1/3
ip address 5.0.0.1 255.0.0.0
!
router bgp 65010
bgp confederation identifier 200
bgp confederation peers 65020
neighbor 1.0.0.2 remote-as 65010   /*RTB IBGP*/
neighbor 2.0.0.2 remote-as 65010   /*RTC IBGP*/
neighbor 5.0.0.2 remote-as 65020   /*RTE EBGP*/
neighbor 4.0.0.2 remote-as 100     /*RTD EBGP*/
```

RTB configuration:

```
interface s1/0
ip address 1.0.0.2 255.0.0.0
!
interface s1/1
ip address 3.0.0.1 255.0.0.0
!
router bgp 65010
bgp confederation identifier 200
bgp confederation peers 65020
```

```
neighbor 1.0.0.1 remote-as 65010   /*RTA IBGP*/
neighbor 3.0.0.2 remote-as 65010   /*RTC IBGP*/
```

RTC configuration:

```
interface s1/0
ip address 2.0.0.2 255.0.0.0
!
interface s1/1
ip address 3.0.0.2 255.0.0.0
!
router bgp 65010
bgp confederation identifier 200
bgp confederation peers 65020
neighbor 2.0.0.1 remote-as 65010   /*RTA IBGP*/
neighbor 3.0.0.1 remote-as 65010   /*RTB IBGP*/
```

RTD configuration:

```
interface s1/0
ip address 4.0.0.2 255.0.0.0
!
router bgp 100
neighbor 4.0.0.1 remote-as 200   /*RTA EBGP*/
```

RTE configuration:

```
interface s1/0
ip address 5.0.0.2 255.0.0.0
!
router bgp 65020
bgp confederation identifier 200
bgp confederation peers 65010
neighbor 5.0.0.1 remote-as 65010   /*RTA EBGP*/
```

6.5.9 Example of route map with BGP group attribute

This section includes three examples of using route map with BGP community attribute.

In the first example, “route map set-community” is applied on the outcoming update of neighbor 171.69.232.50. Set the special community attribute with value “no-export” for the routes passing access list aaa, while other routes are broadcasted normally. This special community attribute will automatically prevent BGP speakers in AS200 from advertising the route outside of the autonomous system.

```
router bgp 100
 neighbor 171.69.232.50 remote-as 200
 neighbor 171.69.232.50 send-community
 neighbor 171.69.232.50 route-map set-community out
!
```

```
 route-map set-community 10 permit
 match ip address aaa
 set community no-export
!
 route-map set-community 20 permit
```

In the second example, “route map set-community” is used for the outcoming update of neighbour 171.69.232.90. All routes orgining from AS70 will insert value 200 into the community attribute 200, all other routes will just be advertised normally.

```
route-map bgp 200
 neighbor 171.69.232.90 remote-as 100
 neighbor 171.69.232.90 send-community
 neighbor 171.69.232.90 route-map set-community out
!
route-map set-community 10 permit
 match as-path test1
 set community-additive 200 200
!
route-map set-community 20 permit
 match as-path test2
!
ip aspath-list test1 permit 70$
ip aspath-list test2 permit .*
```

In the third example, selectively set the MED and local preference value of routes from neighbor 171.69.232.55 according to the commumity attribute value of the routes. All routers matching with community list com1will be set with MED as 8000, this may include routes with community value “100 200 300” or “900 901”. These routes may have other attribute values.

All routes transmitting community list com2 will be set with the local preference value as 500.

All other routes will be set with the local priority value as 50. So, all the rest of the routes of neighbor 171.69.232.55 have the preference of 50.

```
router bgp 200
neighbor 171.69.232.55 remote-as 100
neighbor 171.69.232.55 route-map filter-on-community in
!
route-map filter-on-community 10 permit
match community com1
set metric 8000
!
route-map filter-on-community 20 permit
match community com2
set local-preference 500
!
route-map filter-on-community 30 permit
set local-preference 50
!
```

```
ip community-list com1 permit 100 200 300
ip community-list com1 permit 900 901
!
ip community-list com2 permit 88
ip community-list com2 permit 90
!
```

Chapter 7 Configure RSVP

7.1 Overview

This chapter explains how to configure RSVP. For details about RSVP Command, see “RSVP Command” in the “Network Protocol Command Reference”. For other document about Command, use index or type in Command in online help.

Try to understand RSVP before configuring it, which would be helpful for users. RSVP protocol can be used by a host to request a certain quality of business to an application data process. Routers can use RSVP protocol to transfer quality of service request and carry out reservation. RSVP request is going to be reserved on each node of data channels.

RSVP resource request is for single task data process. Logically, RSVP separates data sender and receiver, despite sender and receiver are in the same application process. RSVP is above IP protocol. Although RSVP does not transfer data, it belongs to Internet protocol (just like ICMP, IGMP or routing protocol). RSVP implementation is like routing protocol and managing protocol.

RSVP is not a routing protocol; however RSVP is able to assist a current and future routing protocol. A routing protocol decides how to transfer a data package, while RSVP deals with the Quality of Service (QoS) of the transferred data packages.

RSVP and WFQ (weighted fair queuing) or RED (random early detection) coordinate and function together. This kind of coordination contains two major concepts: use the RSVP flow between two ends, and use WFQ dialog between two routers.

7.2 RSVP Configuration Task List

- Enable a RSVP on a Router
- Start RSVP in a IP Phone Module Configuration
- Use RSVP to configure Command
- Configure TOS and Precedence for RSVP flow
- Use access-list in RSVP module

7.3 RSVP Configuration Task

7.3.1 Enable a RSVP on a Router

To enable RSVP on a router, users must configure the interface for starting RSVP, which can be realized by configure Command with interface on the RSVP. When the above configuration is done, RSVP protocol is able to work on these interfaces.

Configure Network interface with RSVP and use the following Commands in interface configurations:

Command	Function
ip rsvp bandwidth [*interface-kbps*] [*single-flow-kbps*]	Configure Network interface with RSVP

Notes:

When using ip rsvp bandwidthCommand, under default configuration (interface-kbps and single-flow-kbp), the max resource reservation for the whole port and resource reservation for single data process will be limited to just 75% of the port total resource.

7.3.2 Start RSVP in a IP Phone Module Configuration

Before configuring our IP Phone and IP Phone module of the router to use Voice over IP, users have to enable RSVP to use RSVP to reserve resource.

RSVP Command has to be configured on ports that requires RSVP. That is because RSVP is disable by default. (See the last chapter)

IP phone disables QoS (default), therefore, users must configure dial-peer voipCommand with enabling QoSCommand.

To enable RSVP on interface f0/0, use the following commands in dail - peer Configuration mode of none IVR type:

Command	Function
req-qos { **best-effort** | **controlled-load** | **guaranteed-delay** }	Used Qos policy in dialpeer.

7.3.3 Use RSVP to configure Command

In this RSVP, users may use Command provided by the module to adjust RSVP. Adjustments including establishing RSVP conversation, RSVP path, path tear, resv, resv tear message transmission. This is going to be useful for users to test RSVP.

Users may use the following Commands in global configuration mode:

Command	Function
ip rsvp local session session-ip-address session-dport {tcp | udp}	By setting this Command, users may configure a new RSVP dialog, which can be used by other Commands.
ip rsvp local sender session-id sender-ip-address sender-sport [bandwidth] [burst-size]	Users may send path message with this Command, whose no form may send path tear message.
ip rsvp local reservation session-id sender-ip-address sender-sport [**guarantee** | **load**] [bandwidth] [burst-size]	Users may send resv message with this Command, whose no form may send resv tear message.

7.3.4 Configure TOS and Precedence for RSVP flow

To obtain better reservation results, users may use Commands offered by RSVP module to configure TOS and Precedence for RSVP. When RSVP flow is over the reserved range, the Command configures a higher TOS. When RSVP flow is within the reserved range, the command configures a lower TOS. So does Precedence.

Users may use the following Command in interface configuration mode:

Command	Function
ip rsvp tos {**conform**|**exceed**} *tos-value*	This Command can be used to configure the reserved TOS options.
ip rsvp precedence {**conform**|**exceed**} *precedence-value*	This Command can be used to configure the reserved precedence options.

7.3.5 Use access-list in RSVP module

When users are configuring RSVP on a router, they are able to use access-list to accept or reject communication with certain hosts or routers.

Command	Function
ip rsvp neighbor *access-list-name*	With this function, users may configure the following Commands under interface configuration mode.

Chapter 8Configuring PBR

8.1 Overview

This section describes how to configure PBR. PBR is the abbreviation of Policy Based Routing. PBR make the user have the ability to route ip packet according some policy other than dynamic routing protocol. We currently support the following policy: based on the length of ip packet, source ip address. You can set gateway or outgoing interface for packets matching the policy. PBR can support load balance.

The rule for PBR selecting nexthop is following :

- If set ip next-hop is configured,and the gateway is reachable,the gateway will be used. If multiple gateway is configured, use the first reachable gateway , if load-balance key word is used , the load balance is used between these gateways.
- If set interface is configured, and the outgoing interface is routable(interface protocol up,and ip address is configured),use the outgoing interface.If multiple outgoing interfaces are configured, first routable interface will be used. If load-balance key word is used , the load balance is used between these interface . If both set ip next-hop and set interface configured, , use set ip next-hop first.
- 3.set ip default next-hop or set default interface won't be used until routing lookup failed.

8.2 PBR Configuration Task List

If you want to use PBR,the following configuration is needed:

- Create standard access-list(optional)
- Creat route-map
- Apply route-map on interface

8.3 PBR Configuration Task

8.3.1 Create standard access-list

To create access-list, following the step below:

Command	Function
ip access-list stand *net1*	Enter access-list configurtion mode.

8.3.2 Create route-map

To create route-map,following the step below:

Command	Function
route-map pbr	Enter route-map configuration.
match ip address *access-list*	Configure matching policy.
match length *min_length max_length*	Configure matching policy.
set ip [**default**] **next-hop** *A.B.C.D*	Set gateway.
set [**default**] **interface** *interface_name*	Set outgoing interface.

8.3.3 Apply route-map on interface

To enable PBR on interface,following the step below:

Command	Function
interface *interface_name*	Enter interface configurtion mode.
ip policy route-map *route-map_name*	Apply PBR on interface.

8.3.4 Debug PBR

To debug PBR,following the step below:

Command	Function
debug ip policy	To debug PBR.

8.4 PBR configution example

router configure

```
!
interface FastEthernet0/0
ip address 10.1.1.3 255.255.255.0
no ip directed-broadcast
ip policy route-map pbr
!
interface FastEthernet0/0.13
ip address 13.1.1.3 255.255.255.0
no ip directed-broadcast
encapsulation dot1Q 13
bandwidth 100000
delay 1
!
interface FastEthernet0/0.14
ip address 14.1.1.3 255.255.255.0
no ip directed-broadcast
```

```
encapsulation dot1Q 14
!




ip access-list standard net1
permit 10.1.1.2 255.255.255.255
!
ip access-list standard net2
permit 10.1.1.4 255.255.255.255
!
ip access-list standard net3
permit 10.1.1.21 255.255.255.255
!
route-map pbr 10 permit
match ip address net1
set ip next-hop 13.1.1.99
!
route-map pbr 20 permit
match ip address net2
set ip next-hop 14.1.1.99
!
route-map pbr 30 permit
match ip address net3
set ip next-hop 13.1.1.99 14.1.1.99 load-balance
!
route-map pbr 40 permit
set ip default next-hop 13.1.1.99
```

configure explanation

Policy routing is enabled on interface f0/0. For packets origined from 10.1.1.2, the gateway is 13.1.1.99 if 13.1.1.99 is reachable, if 13.1.1.99 isn't reachable, destination base routing is used. For packes from 10.1.1.21, route-map pbr 30 is used, for load-balance key word is used, both 13.1.1.99 and 14.1.1.99 will be used as the gateway.

Chapter 9 Configuring DNS

9.1 Overview

DNS is Domain Name System for short , DNS is a distributing database using in TCP/IP application.. It can provide the translation of host name and IP address, some information about email and hosts.

The name DNS is used in the TCP/IP network, such as Internet,and it orientates hosts and service according to friendly name. When the DNS name is input, the system can translate it into relative information such as IP address.

In DNS system, DNS Resolver equals to a client of DNS Server. The application can get relative information by accessing DNS Server. The base of this information is: getting the IP address according to a host name or getting the host name according to a IP address.

Dynamic DNS Resolver is used in the condition of dynamic IP addresses. Dynamic DNS Resolver can register Host/address information to DNS Server automatically, when the IP address changes, it can send updating message to DNS Server and the DNS Server will update its database.

9.1.1 DNS Application

DNS has abroad application:

- Provide translating host name to IP address for ping,telnet and traceroute.
- Provide translating IP address to host name for telnet. When traceroute gets each IP address, it can get the name of the address.
- When IP address of client changes, it can update the address in primary server.

9.1.2 DNS Term

- DNS Resource Record(RR):

Information, which may be empty. The set of resource information associated with a particular name is composed of separate resource records (RRs). The order of RRs in a set is not significant, and need not be preserved by name servers, resolvers, or other parts of the DNS.

- Starting Organism of Authorization (SOA)

A record is used to designated the starting point of the area. The record contains the domain name, e-mail address of the domain administrator and the settings about how to enable the DNS server to update the domain data files.

- Comman types of resource records:

Parameter	Description
A	A host address.
CNAME	Identifies the canonical name of analias.
HINFO	Identifies the CPU and OS used by a host.
MX	Identifies a mail exchange for the domain. See [RFC-974 for details.
NS	The authoritative name server for the domain.
PTR	A pointer to another part of the domain name space.
SOA	Identifies the start of a zone of authority.

- DNS Zone:

In general, the DNS database can dispart into different resource records and each record is called zone. A zone can include the resource record of all the zones or parts of a zone.A zone is divide into several child zone is to simplify the management. After using this distrabuting frame, the administrator can manage every child zone effectivly when the domain name extends.

- Authoritative name server:

The DNS Server which manages the RR is named authoritative name server.Every server can be an authoritative name server or many.

- Primary server and slave server:

In order to ensure the high trustiness, DNS requests using many name server to support every zone. The RR of every zone updates to a primary server manuly or antoly.The primay server can be an authoritative name server having one or more zone. The other servers(named master DNS server) are standby server servicing for the same zone,and this can avoiding some instance when the primary server is abnormity.Master servers make their database are update to date by communicating to primary server. Copying the zone files to many name servers is named zone exchange.

9.2 DNS Configuration Task List

This modual realize the DNS Resolver only and the DNS Server is not range of this modual.

- Enables DNS-based host name-to-address translation
- Specify the IP address of a domain name server
- Set a default domain name
- Defines a list of domains
- Defines static host name-to-address mapping
- Specify times to retry a DNS query
- Specify timeout waiting for response to a DNS query

- Delete the mapping of a host name to IP address in cache
- Specify the IP address of a primary server
- Enable update function of dynamic DNS
- Set the period of DNS update
- Bind the domain name to a IP address or IP address of interface
- The function of information showing or debug showing

9.3 DNS Configuration Task

9.3.1 Enable DNS-based host name-to-address translation

That is,make it query the hosts by name or address. This modual enable DNS lookup by default.

In configuration mode use the following command:

Command	Function
ip domain lookup	Eable DNS lookup.
no ip domain lookup	Disable DNS lookup.

9.3.2 Specify the IP address of a domain name server

It may assign several name servers,but can only appoint six at most.The name server assigned before will be queried earlier. When we use the no format without any parameter,it express for delete all the name servers.

In configuration mode use the following command:

Command	Function
ip domain name-server *ip-address*	Set a domain name server
no ip domain name-server *ip-address*	Delete domain name server

Note:

no ip domain name-server ip-address	Express delete a domain name server which IP address is ip-address.
no ip domain name-server	Express delete all the domain name servers.

9.3.3 Set a default domain name

We can complete the host name by a default domain name.But the default domain name is useful only when there is no domain list.

In configuration mode use the following command:

Command	Function
ip domain name *name*	Specify a default domain name.
no ip domain *name*	Delete the default domain name.

9.3.4 Define a list of domains

The DNS Resolver completes a host name by the domain list, it can try the domain list in turn until it find the host or all the domain lists are tried. The domain name will not be used if a domain list exists. We can set six domain lists at most.

In configuration mode use the following command:

Command	Function
ip domain list *name*	Define a domain list.
no ip domain list *name*	Delete a domain list.

Notes:

no ip domain list name	Express delete a domain name named name.
no ip domain list	Express delete all the domain names.

9.3.5 Define static host name-to-address mapping

Any IP address can correspond to a name, and the same name can correspond to many IP addresses. By doing this, the command such as telnet,ping can use the names directly.

In configuration mode use the following command:

Command	Function
ip host name address1[address2,·]	Map a name to some IP address.
no ip host name [address1,·]	Delete a map.

Example:the following express mapping a name to several IP addresses

router_config# ip host djh 172.16.20.209
router_config# ip host djh 172.16.20.210

or:

router_config**#** ip host djh 172.16.20.209 172.16.20.210

If you want to delete, you can delete a IP address or delete many addresses or delete the host.

router_config# no ip host djh 172.16.20.209 /*delete a IP address mapping to a host name djh*/
router_config# no ip host djh 172.16.20.209 172.16.20.210
/**delete 2 IP address mapping to a host name djh*/
router_config# no ip host djh /*delete the host named djh*/

9.3.6 Specify times to retry a DNS query

When sending failing or not receiving the correspond, it can send again. By default , the retry times is 3 (times). You can modify the retry times when neeing.

In configuration mode use the following command:

Command	Function
ip domain retry *count*	Set retry times
no ip domain retry	Restore to the default

9.3.7 Specify timeout waiting for response to a DNS query

When sending failing or not receiving the correspond, it can send again.This time is the interval time between two sending.By default , the timeout value is 2 (seconds). You can modify the retry times when neeing.

In configuration mode use the following command:

Command	Function
ip domain timeout *seconds*	Set timout value.
no ip domain timeout	Restore to the default.

9.3.8 Delete the mapping of a host name to IP address in cache

The host having been queried will be set in cache. We can delete one or all of the hosts in cache. The command can't delete the static mapping of host and IP address.

In manager use the following command:

Command	Function
clear ip host *name*	Delete a host in cache.
clear ip host *	Delte all the hosts in cache.

9.3.9 Specify the IP address of a primary server

You can only specify one primary server, if you specify another,it will replace the one earlier.

In configuration mode use the following command:

Command	Function
ip domain primary-server *address*	Set a primary server.
no ip domain primary-server	Delete the primary server.

9.3.10 Enable update function of dynamic DNS

The router having static IP address doesn't need the function, so you can use the no format to disable domain dynamic. By default, the function is disable.

In configuration mode use the following command:

Command	Function
ip domain dynamic enable	Enable domain dynamic.
no ip domain dynamic enable	Disable domain dynamic.

9.3.11 Set the period of DNS update

In configuration mode use the following command:

Command	Function
ip domain dynamic period *seconds*	Set time of updating period.
no ip domain dynamic period	Restore to the default.

9.3.12 Bind the domain name to a IP address or IP address of interface

This command doesn't support binding the second IP address to a domain name.

After the command is using, the changing of the IP address of interface will update the mapping in the primary server, that is, dynamic domain updating.

In general, it needs to update in the following cases:

- When the router reboots, it should register to the primay server at once.
- By clock
- If the binding command is used, it will add or delete a mapping in primary server.
- When the IP address of a interface changes
- When the interface having been binded is shut up or is deleted

In configuration mode use the following command:

Command	Function
ip domain bind *name* **interface** *number*	Bind the domain name to the primary IP address of interface (Note:an interface can only correspond to one domain name, when you use another,the later will replace for the earlier.)
ip domain bind *name* **interface** *number singly*	Bind the domain name to the primary IP address of interface, and delete all the hosts named *name* in primary server
no ip domain bind *name* **interface** *number*	Delete the mapping of the domain name to the primary IP address of interface
ip domain bind *name ip_addr*	Bind the domain name to a IP address. (Note:the same domain name can correspond to several IP addresses.)

ip domain bind *name ip_addr singly*	Bind the domain name to a IP address, and delete all the hosts named *name* in primary server
no ip domain bind *name ip_addr*	Delete the mapping of the domain name to the IP address
no ip domain bind *name*	Delete all the hosts named *name* in the primary server

Notes:

If the command **ip domain dynamic enable** or **ip domain primary-server** is not been configurated , then command **ip domain bind** and **no ip domain bind** will not be successful,and will not be in flash memory or be deleted from flash memory.

To the command of domain dynamic,the router will register to the primary server autoly,but if the interface shut down, the communication to primary server will fail,that is,it can't register successly. In order that the register goes along after the interface shut up, the modual set a much bigger timeout and retry,so the configuring of retry and timeout go into effect after 30 seconds when the router reboots.

On the side, If we bind a domain name with an interface,when the ip address of the interface changed and makes the communication to the primary server fail,but after a while,it can restore, at this instance, we can enhance the times of retry and the seconds of timeout so that it can update successfully.

9.3.13 The function of information showing or debug showing

The system can show some information such as the default domain name,domain list,the host in the cache and so on.What's more, it can show information when running. This information can help us to resolve some problems.

In manager use the following command

Command	Function
show ip hosts	Show the default domain name,domain list,the host in the cache and so on.
show ip hosts detail	It show some information of the applications using the DNS Resolver unblocking such as the queue ID(or address of a callback) an time before ttl.
debug ip domain	Show the debug information of this modual.

IP Hardware Subnet Routing Configuration

Table of Contents

Chapter 1 IP Hardware Subnet Routing Configuration.....1
1.1 IP Hardware Subnet Configuration Task.....1
1.1.1 Overview.....1
1.1.2 Configuring IP Hardware Subnet Routing.....1
1.2 Configuration Example.....2

Chapter 1 IP Hardware Subnet Routing Configuration

1.1 IP Hardware Subnet Configuration Task

1.1.1 Overview

IP hardware subnet routing is similar to IP fast exchange.

When the IP hardware subnet routing is not enabled, before forwarding message containing the IP address A at the next hop, the switch first checks whether the item of destination A exists in the IP cache of hardware. If the item exists, the message will be forwarded through hardware. If the item does not exist, the message is sent to CPU and then processed through software. IP hardware subnet routing items include the destination subnet, mask, IP address of the next hop, interface and so on. When the IP hardware subnet routing is enabled, after the IP cache fails to be matched, the system is to check the IP hardware subnet routing items. If the matched item is found, the message will be directly forwarded through the next-hop IP address and the interface designated in the matched item. If the IP hardware subnet routing item is not found, the message will be sent to CPU for processing.

The IP hardware subnet routing has two modes: automatic and manual. In manual mode, you need to manually configure all routing items required by the IP hardware subnet routing. Note that routing items having longer mask of destination subnet should be configured earlier. In automatic mode, the system automatically adds the known routes to the hardware subnet routing. All the procedure is automatic after the hardware subnet routing is started.

1.1.2 Configuring IP Hardware Subnet Routing

Perform the following steps to configure the IP hardware subnet routing:

Step	Command	Description
1	[**no**] **ip exf** {**default** | *destination mask*} {**cpu** | *nexthop* vlan *vlanid*}	Add or delete a hardware subnet route. Deleting a hardware subnet route requires to specify the destination network and mask. Replace **destination** and **mask** in the command line with **default** when you delete a route. In this case, The next hop is not CPU. The command is effective only in manual configuration mode.
2	[**no**] **ip exf**	Enable or disable the IP hardware subnet routing.

Pay attention to the following content when you configure the routing items:

- As to the direct-connecting routing, the next hop is CPU. If the next hop is a routing interface not an IP address, do as in the direct-connecting routing.
- When the number of the routing items in the system is bigger than that of the IP hardware subnet routing items, the default routing cannot be the IP hardware subnet routing. Two or several routes, which are prefix to each other, must be used together when IP hardware subnet routing is adopted. For other items, advise to add heavy-traffic items to the hardware subnet routing table.
- The ARP of the next-hop IP address does not exist, the system will send an ARP request and temporarily designate the next-hop routing item as CPU. After the system receives the ARP response, the system then update the next hop to the user-designating address. If the VLAN interface where the next hop resides is found different from the configured interface during the ARP response, the next hop of the route is designated as CPU. Users then need to correct the configuration.
- If the next-hop interface or the interface protocol does not exist, the item will not be added to the hardware subnet routing table.

Suppose a switch has the following routing items:

(1) 192.168.0.0/16 next hop 192.168.26.3/vlan1

(2) 192.168.20.0/24 next hop 192.168.26.1/vlan1

(3) 192.168.1.0/24 direct-connecting routing

(4) 192.168.26.0/24 direct-connecting routing

(5) 10.0.0.0/8 next hop 192.168.1.4/vlan2

(6) 0.0.0.0/0 next hop 192.168.1.6/vlan2

The destination subnet of route item 1 is the prefix of subnet 2, 3 and 4. Therefore,these items should be added to the hardware subnet routing table together. Item 3 and 4 are direct-connecting routing and the next hop is CPU.

The relative configuration is as follows:

ip exf 192.168.20.0 255.255.255.0 nexthop 192.168.26.1 vlan 1

ip exf 192.168.1.0 255.255.255.0 cpu

ip exf 192.168.26.0 255.255.255.0 cpu

ip exf 192.168.0.0 255.255.0.0 nexthop 192.168.26.3 vlan 1

ip exf 10.0.0.0 255.0.0.0 nexthop 192.168.1.4 vlan 2

ip exf 0.0.0.0 0.0.0.0 nexthop 192.168.1.6 vlan 2

IP-PBR Configuration

Table of Contents

IP-PBR Configuration..... 1
IP-PBR Configuration..... 1
1.1.1 Enabling or Disabling IP-PBR Globally..... 1
1.1.2 ISIS Configuration Task List..... 2
1.1.3 Monitoring and Maintaining MVC..... 2
1.1.4 IP-PBR Configuration Example..... 4

IP-PBR Configuration

IP-PBR Configuration

IP-PBR realizes software PBR functions through the hardware of switch chip.

PBR stands for Policy Based Routing. PBR enables users to rely on a certain policy not on routing protocol for routing. Software based PBR supports multiple policies and rules and also load balance. You can designate the next hop's IP address or port for those packets that are in line with policy. PBR supports load balance and applies multiple next-hop IP addresses or ports on those policy-supported packets.

Only when the next-hop egress ARP designated by route map is already learned can IP-PBR regard that this egress is valid and then the corresponding rule is effective. When a packet satisfies IP-PBR policy, the hardware directly forwards this packet to the next-hop egress that the rule specifies. This process is finished by the hardware without the operation of CPU. The packets forwarded by IP-PBR have the highest priority and only those packets unmatched with IP-PBR rule are forwarded to CPU.

The current IP-PBR supports the IP ACL policy and the next-hop IP address policy. When multiple next hops are configured, the first effect next hop is chosen. IP-PBR also supports equivalent routing that is realized by the switch chip. Hardware equivalent routing needs no extra configuration.

IP-PBR supports the following policy routing commands:

route-map *WORD*

match ip address *WORD*

set ip next-hop *X.X.X.X* [**load-balance**]

ip policy route-map *WORD*

IP-PBR is a little different from router's policy routing. IP-PBR chooses an effective next hop as the egress and drops packets if no valid next hop available, while router's policy routing selects an effective next hop but packet loss happens if this next hop has not learned ARP. Once multiple sequences are set, one difference between IP-PBR and software policy routing must be noted. Software policy routing always chooses high-priority sequence routes no matter whether IP address matched by high-priority sequences overlaps with that matched by low-priority sequences and whether these routes are effective, while IP-PBR chooses low-priority sequence routes when high-priority sequence routes invalidate.

1.1.1 Enabling or Disabling IP-PBR Globally

Run the following commands in global configuration mode.

Command	Purpose

ip pbr	The IP-PBR function is disabled by default.
no ip pbr	Resumes the default settings.

IP-PBR is disabled by default.

1.1.2 ISIS Configuration Task List

To configure IP-PBR, do as follows:

Create ACL;

Create a route map;

Apply the route map on a port;

To create an ACL, run the following command globally:

Command	Remarks
ip access-list standard *net1*	Enters the ACL configuration mode and defines ACL.

To create a route map, run the following commands globally:

Command	Remarks
route-map *pbr*	Enters the route map configuration mode.
match ip address *access-list*	Configures the match-up policy.
set ip next-hop *A.B.C.D*	Configures the next-hop address of IP packet.

To apply policy routing on an IP-receiving port, run the following commands:

Command	Remarks
interface *interface_name*	Enters the interface configuration mode.
ip policy route-map *route-map_name*	Applies policy routing on the port.

1.1.3 Monitoring and Maintaining MVC

Run the following commands in EXEC mode:

Command	Operation
show ip pbr	It is used to display the information about RIP

show ip policy	Shows the port on which IP-PBR is applied.
show ip pbr policy	It is used to display the information about IP-PBR equivalent routing.
debug ip pbr	It is used to enable or disable the debugging switch of IP-PBR.

The information that IP-PBR is not running is shown:

```
switch#show ip pbr

IP policy based route state: disabled


No pbr apply item

No equiv exf apply item
```

All data related about IP-PBR running are shown below:

```
switch#show ip pbr
IP policy based route state: enabled

No equiv exf apply item

VLAN3 use route-map ddd, and has 1 entry active.
------------------
Entry sequence 10, permit
  Match ip access-list:
    ac1
  Set Outgoing nexthop
    90.0.0.3
```

The IP-PBR policy routing information is shown below:

```
switch#show ip pbr policy
IP policy based route state: enabled

VLAN3 use route-map ddd, and has 1 entry active.
------------------
Entry sequence 10, permit
  Match ip access-list:
    ac1
  Set Outgoing nexthop
    90.0.0.3
```

The equivalent routing information is shown below:

```
switch#show ip pbr exf
IP policy based route state: enabled
```

```
------------------
Entry sequence 1, handle c1f95b0
   Dest ip: 1.1.0.0/16
      90.0.0.3
      192.168.213.161
```

1.1.4 IP-PBR Configuration Example

Switch configuration:

```
!
ip pbr
!
interface vlan1
ip address 10.1.1.3 255.255.255.0
no ip directed-broadcast
ip policy route-map pbr
!
ip access-list standard ac1
permit 10.1.1.21 255.255.255.255
!
ip access-list standard ac2
permit 10.1.1.2 255.255.255.255
!
route-map pbr 10 permit
match ip address ac1
set ip next-hop 13.1.1.99
!
route-map pbr 20 permit
match ip address ac2
set ip next-hop 13.1.1.99 14.1.1.99 load-balance
!
```

Configuration Description

The switch is to apply policy routing on the packets that are received from VLAN1.As to the packets whose source IPs are 10.1.1.21, their next hop is 13.1.1.99.As to the packets whose source IPs are 10.1.1.2, they are applied on **route-map pbr 20**; because **set ip next-hop** has the **load-balance** parameter, the switch chip will automatically choose 13.1.1.99 or 14.1.1.99 as the egress according to destination IP address.

Multi-VRF CE Configuration

Table of Contents

Chapter 1 Multi-VRF CE Intro....1
1.1 Overview....1
1.1.1 Establishing Routes with CE....1
1.1.2 Establishing Routes with PE....2
Chapter 2 Multi-VRF CE Configuration....3
2.1 Default VRF Configuration....3
2.2 MCE Configuration Tasks....3
2.3 MCE Configuration....3
2.3.1 Configuring VRF....3
2.3.2 Configuring VPN Route....4
2.3.3 Configuring the BGP Route Between PE and CE....5
2.3.4 Testifying the VRF Connectivity Between PE and CE....5
Chapter 3 MCE Configuration Example....6
3.1 Configuring S11....6
3.2 Configuring MCE-S1....7
3.3 Configuring PE....9
3.4 Configuring MCE-S2....10
3.5 Setting S22....12
3.6 TestifyingVRF Connectivity....13

Chapter 1 Multi-VRF CE Intro

1.1 Overview

The Virtual Private Network (VPN) provides a secure method for multiple client networks to share the ISP-supplied bandwidth. In general, one VPN comprises a team of client networks that share a public routing table on the ISP's routers. Each client network is connected to the interface of the network devices of ISP, while ISP's device will relate each interface to a VPN routing table. One VPN routing table is also called as a VRF (VPN Routing /Forwarding table).

VRF is usually deployed on a Provider Edge (PE) device, such as MPLS VRF VPN. A PE supports multiple VPNs, and each VPN has its independent IP address space among which IP addresses can be overlapped. The VPN of a different client connects a different interface of PE, while PE differentiates the to-be-checked routing tables according to the incoming port of the packet.

Multi-VRF CE is to remove the task of connecting multiple client networks from PE to CE, which only requires a physical link to connect CE and PE. In this way, the port resource of PE is saved. CE also maintains the VRF routing table for each VPN. The packets from the client network are first forwarded on CE and then transmitted to PE after the packets pass through the ISP network.

The switch which serves as MCE connects different client networks through different ports and then relates these ports to a VPN routing table. D-Link switches only support VRF settings on the VLAN port.

The MCE function is usually deployed at the edge of the large-scale MPLS-VRF VPN network. The three functions, Multi-VRF CE, MPLS label switching and the function of MPLS control layer, are independent. Figure 1.1 shows an MPLS-VRF VPN network.

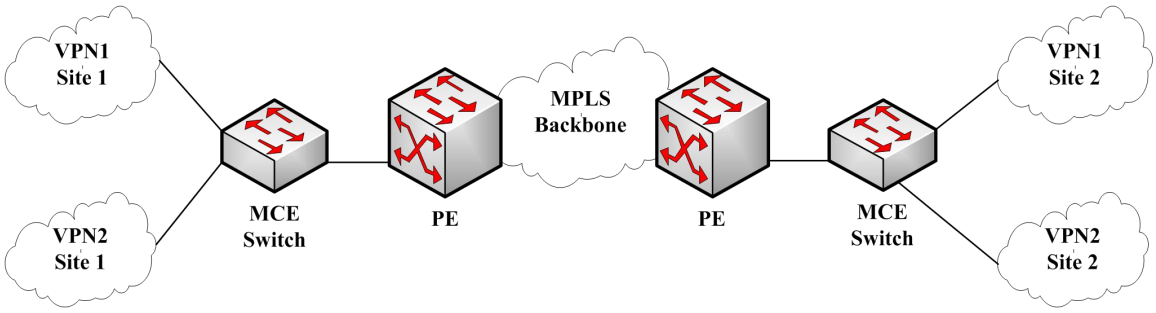


Figure 1.1 MCE in the MPLS-VRF VPN network

1.1.1 Establishing Routes with CE

The Multi-VRF CE switch can establish routes with CE through multiple dynamic routing protocols. CE can be routers or the Ethernet switches. The routing protocols which are supported include OSPF and RIP. The MCE switch also supports static routing configuration.

The MCE switch generally needs different VLAN ports to connect CEs that belong to different VPNs. The VLAN ports that are used to connect the VPNs require to be related to a VRF. CE does not need to support VRF.

1.1.2 Establishing Routes with PE

The MCE switch (MCE) can connect one or multiple PEs, but both MCE and the connected PEs have to get VRF configured. MCE will provide PE the routes which MCE learns from CE and learns the routes of remote client networks from PE.

The VRF route can be established between MCE and PE through dynamic routing protocols such as BGP, OSPF and RIP. The VRF route can also be established statically.

In general, MCE and PE belong to different autonomous systems. Hence, the method to establish the VRF route between MCE and PE by using EBGP is the key point in this document.

Chapter 2 Multi-VRF CE Configuration

2.1 Default VRF Configuration

Function	Default Configuration
VRF	There is no configuration. All routes are added to the default routing table.
VPN expansibility of VRF	There is no Routing Distinguisher (RD). There is no input/output Routing Target (RT).
Maximum number of VRF routes	10240
VRF port	N/A. None of VLAN ports is related with VRF, and the routes of ports are added to the default routing table.
IP Express Forwarding	The hardware IP routing is not enabled.

2.2 MCE Configuration Tasks

- Configuring VRF
- Configuring a VPN Route
- Configuring BGP Route Between PE and CE
- Testifying the VRF Connectivity between PE and CE

2.3 MCE Configuration

2.3.1 Configuring VRF

Refer to the following steps to configure one or multiple VRFs.

Command	Purpose
Switch# **config**	Enters the switch configuration mode.
Switch_config# **ip vrf** *vrf-name*	Creates VRF and enters the VRF configuration mode. vrf-name: VRF name with up to 31 characters
Switch_config_vrf# **rd** *route-distinguisher*	Sets the route distinguisher of VRF. route-distinguisher: Stands for the distinguisher of the route. It consists of autonomous domain ID and random numbers, or IP and random numbers.

Switch_config_vrf# **route-target** **{ export | import | both }** *route-target-extened-community*	Creates the expanded VPN attributes of input/output VRF objects. route-target-extended-community: It consists of autonomous domain ID and random numbers, or IP and random numbers.
Switch_config_vrf# **interface** *intf-name*	Enters the interface configuration mode. intf-name: Stands for the name of an interface.
Switch_config_intf# **ip vrf forwarding** *vrf-name*	Relates the L3 interface with VRF. vfi-name: Means the name of VRF.
Switch_config_intf# **exit**	Exits from interface configuration mode.
Switch_config# **ip exf**	Enables ip hardware routing .
Switch_config# **show ip vrf** **[brief | detail | interface] [** *vrf-name* **]**	Browses the VRF information.
Switch_config**#no ip vrf** *vrf-name*	Deletes the configured VRF and the relation between VRF and the L3 interface. vfi-name: Means the name of VRF.
Switch_config_intf# **no ip vrf forwarding** **[** *vrf-name* **]**	Deletes the relation between the L3 interface and VRF.

2.3.2 Configuring VPN Route

The route can be established between MCE and customer device through the configuration of BGP, OSPF, RIP or static routes. The following takes OSPF configuration as an example, which is similar to other routes' configurations.

Note:
When a route is configured on MCE to connect the client network, the VRF attributes of the routing protocol need be specified. VRF need not be configured on the customer device.

Command	**Purpose**
Switch# **config**	Enters the switch configuration mode.
Switch_config# **router ospf** *process-id* **vrf** *vrf-name*	Starts the OSPF-VRF route and enters the configuration mode.
Switch_config_ospf# **network** *network-number* *network-mask* **area** *area-id*	Defines the OSPF network, mask and area ID.
Switch_config_ospf# **redistribute bgp** *ASN*	Forwards the designated BGP network to the OSPF network.
Switch_config_ospf# **exit**	Exits from the OSPF configuration mode.

Switch_config# **show ip ospf**	Browses the information about the OSPF protocol.
Switch_config# **no router ospf** *process-id*	Deletes the OSPF-VRF routing configuration.

2.3.3 Configuring the BGP Route Between PE and CE

Refer to the following configuration commands:

Command	**Purpose**
Switch# **config**	Enters the switch configuration mode.
Switch_config# **router bgp** *autonomous-system-number*	Starts the BGP protocol by designating autonomous system number and enters the BGP configuration mode.
Switch_config_bgp# **bgp log-neighbor-changes**	Starts the record about BGP neighbor change.
Switch_config_bgp# **address-family ipv4 vrf** *vrf-name*	Enters the configuration mode of VRF address-family.
Switch_config_bgp_af# **redistribute ospf** *ospf-process-id*	Forwards the OSPF routing information to the BGP network.
Switch_config_bgp_af# **network** *network-number/prefix-length*	Configures the network number and the mask's length that are distributed by BGP.
Switch_config_bgp_af# **neighbor** *address* **remote-as** *ASN*	Configures the BGP neighbor and the autonomous system number of a neighbor.
Switch_config_bgp_af# **exit-address-family**	Exits from the configuration mode of address-family.
Switch_config_bgp# **exit**	Exits from the BGP configuration mode.
Switch_config# **show ip bgp vpnv4 [all | rd | vrf]**	Browses the BGP-VRF routing information.
Switch_config# **no router bgp** *ASN*	Deletes the BGP routing configuration.

2.3.4 Testifying the VRF Connectivity Between PE and CE

Use the PING command with the VRF option to testify the VRF connectivity of PE and CE.

Command	**Purpose**
Switch# **ping** –**vrf** *vrf-name ip-address*	Conducts the PING operation to the addresses in VRF.

Chapter 3 MCE Configuration Example

Figure 2.1 shows a simple VRF network. Both S1 and S2 are the Multi-VRF CE switches. S11, S12 and S13 belong to VPN1, S21 and S22 belong to VPN2, and all of them are customer devices. The OSPF route should be configured between CE and customer device, while the BGP route is configured between CE and PE.

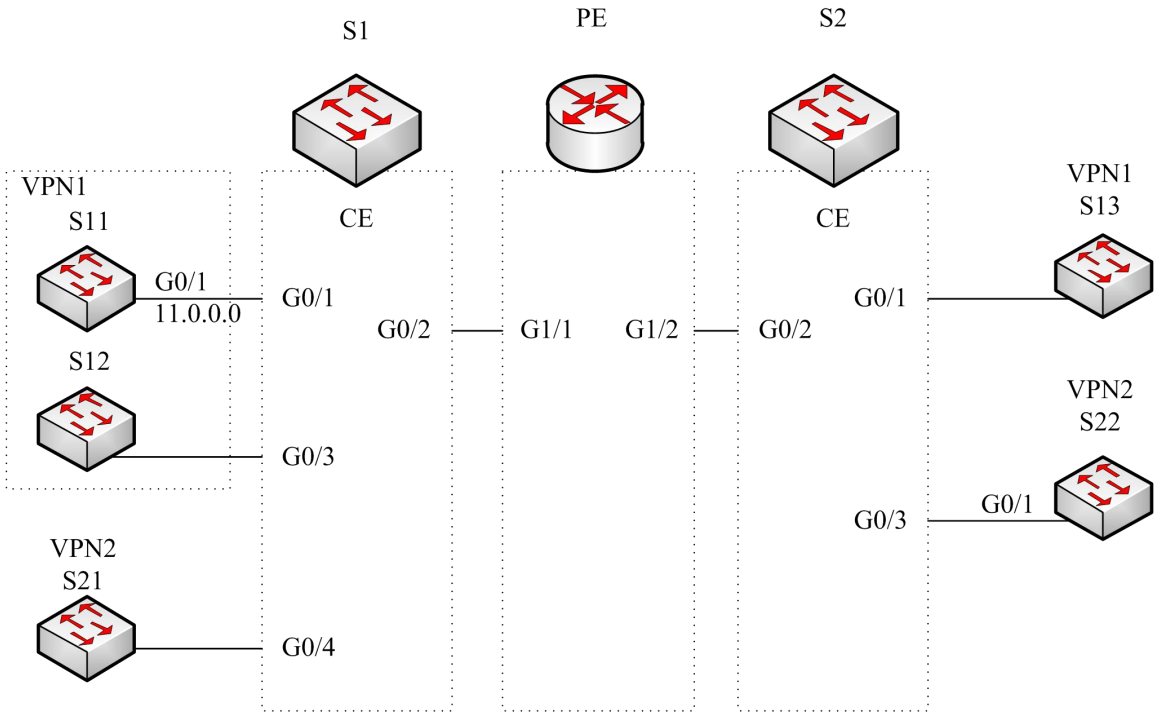


Figure 2.1 MCE configuration example

3.1 Configuring S11

Set the VLAN attributes of the physical interface that connects CE:

Switch_config# interface gigaEthernet 0/1
Switch_config_g0/1# switchport pvid 11
Switch_config_g0/1# exit

Sets the IP address and the VLAN interface.

Switch_config# interface VLAN11
Switch_config_v11# ip address 11.0.0.2 255.0.0.0
Switch_config_v11# exit

Set the routing protocol between CE and customer's device:

```
Switch_config# router ospf 101
Switch_config_ospf_101# network 11.0.0.0 255.0.0.0 area 0
Switch_config_ospf_101# exit
```

3.2 Configuring MCE-S1

Configures VRF on the Multi-VRF CE device.

```
Switch#config
Switch_config# ip vrf vpn1
Switch_config_vrf_vpn1# rd 100:1
Switch_config_vrf_vpn1# route-target export 100:1
Switch_config_vrf_vpn1# route-target import 100:1
Switch_config_vrf_vpn1# exit

Switch_config# ip vrf vpn2
Switch_config_vrf_vpn2# rd 100:2
Switch_config_vrf_vpn2# route-target export 100:2
Switch_config_vrf_vpn2# route-target import 100:2
Switch_config_vrf_vpn2# exit
```

Configure the loopback port and the physical port, and use the address of the loopback port as the router ID of the BGP protocol.

```
Switch_config# interface loopback 0
Switch_config_l0# ip address 101.0.0.1 255.255.255.255
Switch_config_l0# exit
```

S1 connects S11 through the F0/1 port, S21 through the G0/4 port and PE through the G0/2 port.

```
Switch_config# interface gigaEthernet 0/1
Switch_config_g0/1# switchport pvid 11
Switch_config_g0/1# exit

Switch_config# interface gigaEthernet 0/4
Switch_config_g0/4# switchport pvid 15
Switch_config_g0/4# exit

Switch_config# interface gigaEthernet 0/2
Switch_config_g0/2# switchport mode trunk
Switch_config_g0/2# exit
```

Set the L3 VLAN port of a switch, bind the VRF to the VLAN port and set the IP address. S1 connects PE through two logical ports, VLAN21 and VLAN22. The two ports, VLAN11 and VLAN15, connect VPN1 and VPN2 respectively.

```
Switch_config# interface VLAN11
Switch_config_v11# ip vrf forwarding vpn1
```

```
Switch_config_v11# ip address 11.0.0.1 255.0.0.0
Switch_config_v11# exit

Switch_config# interface VLAN15
Switch_config_v15# ip vrf forwarding vpn2
Switch_config_v15# ip address 15.0.0.1 255.0.0.0
Switch_config_v15# exit

Switch_config# interface VLAN21
Switch_config_v21# ip vrf forwarding vpn1
Switch_config_v21# ip address 21.0.0.2 255.0.0.0
Switch_config_v21# exit

Switch_config# interface VLAN22
Switch_config_v22# ip vrf forwarding vpn2
Switch_config_v22# ip address 22.0.0.2 255.0.0.0
Switch_config_v22# exit
```

Configure the OSPF route between CE and customer device.

```
Switch_config# router ospf 1 vrf vpn1
Switch_config_ospf_1# network 11.0.0.0 255.0.0.0 area 0
Switch_config_ospf_1# redistribute bgp 100
Switch_config_ospf_1#exit

Switch_config# router ospf 2 vrf vpn2
Switch_config_ospf_2# network 15.0.0.0 255.0.0.0 area 0
Switch_config_ospf_2# redistribute bgp 100
Switch_config_ospf_2#exit
```

Configure the EBGP route between PE and CE.

```
Switch_config# router bgp 100
Switch_config_bgp# bgp log-neighbor-changes

Switch_config_bgp# address-family ipv4 vrf vpn1
Switch_config_bgp_vpn1# no synchronization
Switch_config_bgp_vpn1# redistribute ospf 1
Switch_config_bgp_vpn1# neighbor 21.0.0.1 remote-as 200
Switch_config_bgp_vpn1# exit-address-family

Switch_config_bgp# address-family ipv4 vrf vpn2
Switch_config_bgp_vpn2# no synchronization
Switch_config_bgp_vpn2# redistribute ospf 2
Switch_config_bgp_vpn2# neighbor 22.0.0.1 remote-as 200
Switch_config_bgp_vpn2# exit-address-family
Switch_config_bgp# exit
```

Create VLAN.

```
Switch_config# vlan 1,11-12,21-22
```

Enables the forwarding of subnet route of the switch.

```
Switch_config# ip exf
```

3.3 Configuring PE

Set VRF on PE:

```
Switch#config
Switch_config# ip vrf vpn1
Switch_config_vrf_vpn1# rd 200:1
Switch_config_vrf_vpn1# route-target export 200:1
Switch_config_vrf_vpn1# route-target import 200:1
Switch_config_vrf_vpn1# exit

Switch_config# ip vrf vpn2
Switch_config_vrf_vpn2# rd 200:2
Switch_config_vrf_vpn2# route-target export 200:2
Switch_config_vrf_vpn2# route-target import 200:2
Switch_config_vrf_vpn2# exit
```

Set the loopback interface as the router identifier:

```
Switch_config# interface loopback 0
Switch_config_l0# ip address 102.0.0.1 255.255.255.255
Switch_config_l0# exit
```

Set the physical interface which connects PE and CE: G1/1 and G1/2 connect S1 and S2 respectively:

```
Switch_config# interface gigaEthernet 1/1
Switch_config_g1/1# switchport mode trunk
Switch_config_g1/1# interface gigaEthernet 1/2
Switch_config_g1/2# switchport mode trunk
Switch_config_g1/2# exit
```

Set the L3 VLAN interface of PE, which connects S1:

```
Switch_config# interface VLAN21
Switch_config_v21# ip vrf forwarding vpn1
Switch_config_v21# ip address 21.0.0.1 255.0.0.0
Switch_config_v21# exit

Switch_config# interface VLAN22
```

```
Switch_config_v22# ip vrf forwarding vpn2
Switch_config_v22# ip address 22.0.0.1 255.0.0.0
Switch_config_v22# exit
```

Set the L3 VLAN interface of PE, which connects S2:

```
Switch_config# interface VLAN31
Switch_config_v31# ip vrf forwarding vpn1
Switch_config_v31# ip address 31.0.0.1 255.0.0.0
Switch_config_v31# exit

Switch_config# interface VLAN32
Switch_config_v32# ip vrf forwarding vpn2
Switch_config_v32# ip address 32.0.0.1 255.0.0.0
Switch_config_v32# exit
```

Set the EBGP of PE:

```
Switch_config# router bgp 200
Switch_config_bgp# bgp log-neighbor-changes
Switch_config_bgp# address-family ipv4 vrf vpn1
Switch_config_bgp_vpn1# no synchronization
Switch_config_bgp_vpn1# neighbor 21.0.0.2 remote-as 100
Switch_config_bgp_vpn1# neighbor 31.0.0.2 remote-as 300
Switch_config_bgp_vpn1# exit-address-family

Switch_config_bgp# address-family ipv4 vrf vpn2
Switch_config_bgp_vpn2# no synchronization
Switch_config_bgp_vpn2# neighbor 22.0.0.2 remote-as 100
Switch_config_bgp_vpn2# neighbor 32.0.0.2 remote-as 300
Switch_config_bgp_vpn2# exit-address-family
Switch_config_bgp# exit
```

Set VLAN and enable the subnet routing forwarding.

```
Switch_config# vlan 1,21-22,31-32
Switch_config# ip exf
```

3.4 Configuring MCE-S2

Configures VRF:

```
Switch#config
Switch_config# ip vrf vpn1
Switch_config_vrf_vpn1# rd 300:1
Switch_config_vrf_vpn1# route-target export 300:1
Switch_config_vrf_vpn1# route-target import 300:1
Switch_config_vrf_vpn1# exit
```

```
Switch_config# ip vrf vpn2
Switch_config_vrf_vpn2# rd 300:2
Switch_config_vrf_vpn2# route-target export 300:2
Switch_config_vrf_vpn2# route-target import 300:2
Switch_config_vrf_vpn2# exit
```

Configure the loopback port and the physical port, and use the address of the loopback port as the router ID of the BGP protocol.

```
Switch_config# interface loopback 0
Switch_config_l0# ip address 103.0.0.1 255.255.255.255
Switch_config_l0# exit
```

S2 connects S13 through the F0/1 port, S22 through the G0/3 port and PE through the G0/2 port.

```
Switch_config# interface gigaEthernet 0/1
Switch_config_g0/1# switchport pvid 41
Switch_config_g0/1# exit

Switch_config# interface gigaEthernet 0/3
Switch_config_g0/3# switchport pvid 46
Switch_config_g0/3# exit

Switch_config# interface gigaEthernet 0/2
Switch_config_g0/2# switchport mode trunk
Switch_config_g0/2# exit
```

Set the L3 VLAN port of a switch, bind the VRF to the VLAN port and set the IP address. S2 connects PE through two logical ports, VLAN31 and VLAN32. The two ports, VLAN41 and VLAN46, connect VPN1 and VPN2 respectively.

```
Switch_config# interface VLAN41
Switch_config_v41# ip vrf forwarding vpn1
Switch_config_v41# ip address 41.0.0.1 255.0.0.0
Switch_config_v41# exit

Switch_config# interface VLAN46
Switch_config_v46# ip vrf forwarding vpn2
Switch_config_v46# ip address 46.0.0.1 255.0.0.0
Switch_config_v46# exit

Switch_config# interface VLAN31
Switch_config_v31# ip vrf forwarding vpn1
Switch_config_v31# ip address 31.0.0.2 255.0.0.0
Switch_config_v31# exit
```

```
Switch_config# interface VLAN32
Switch_config_v32# ip vrf forwarding vpn2
Switch_config_v32# ip address 32.0.0.2 255.0.0.0
Switch_config_v32# exit
```

Configure the OSPF route between CE and customer device.

```
Switch_config# router ospf 1 vrf vpn1
Switch_config_ospf_1# network 41.0.0.0 255.0.0.0 area 0
Switch_config_ospf_1# redistribute bgp 300
Switch_config_ospf_1#exit

Switch_config# router ospf 2 vrf vpn2
Switch_config_ospf_2# network 46.0.0.0 255.0.0.0 area 0
Switch_config_ospf_2# redistribute bgp 300
Switch_config_ospf_2# exit
```

Configure the EBGP route between PE and CE.

```
Switch_config# router bgp 300
Switch_config_bgp# bgp log-neighbor-changes

Switch_config_bgp# address-family ipv4 vrf vpn1
Switch_config_bgp_vpn1# no synchronization
Switch_config_bgp_vpn1# redistribute ospf 1
Switch_config_bgp_vpn1# neighbor 31.0.0.1 remote-as 200
Switch_config_bgp_vpn1# exit-address-family

Switch_config_bgp# address-family ipv4 vrf vpn2
Switch_config_bgp_vpn2# no synchronization
Switch_config_bgp_vpn2# redistribute ospf 2
Switch_config_bgp_vpn2# neighbor 32.0.0.1 remote-as 200
Switch_config_bgp_vpn2# exit-address-family
Switch_config_bgp# exit
```

Create VLAN.

```
Switch_config# vlan 1,31-32,41,46
```

Enables the forwarding of subnet route of the switch.

```
Switch_config# ip exf
```

3.5 Setting S22

Set the VLAN attributes of the physical interface of CE, and connect S22 and S2 through interface f0/1:

```
Switch_config# interface gigaEthernet 0/1
```

```
Switch_config_g0/1# switchport pvid 46
Switch_config_g0/1# exit
```

Sets the IP address and the VLAN interface.

```
Switch_config# interface VLAN46
Switch_config_v46# ip address 46.0.0.2 255.0.0.0
Switch_config_v46# exit
```

Set the routing protocol between CE and customer's device:

```
Switch_config# router ospf 103
Switch_config_ospf_103# network 46.0.0.0 255.0.0.0 area 0
Switch_config_ospf_103# exit
```

3.6 TestifyingVRF Connectivity

Run the PING command on S1 to testify the connectivity of VPN1 between S1 and S11:

```
Switch# ping -vrf vpn1 11.0.0.2
!!!!!
--- 11.0.0.2 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0/0/0 ms
```

Testify the connectivity between S1 and PE:

```
Switch# ping -vrf vpn1 21.0.0.1
!!!!!
--- 21.0.0.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0/0/0 ms
```

Reliability Configuration

Table of Contents

Chapter 1 VRRP Configuration 3
1.1 Overview 3
1.2 VRRP Configuration Task List 3
1.3 VRRP Configuration Task 3
1.3.1 Configuring VRRP Virtual IP Address 3
1.3.2 Configuring VRRP Authentication Mode 4
1.3.3 Configuring VRRP Description 4
1.3.4 Configuring VRRP Priority Preemption 4
1.3.5 Configuring VRRP Protocol Packet MAC Address 4
1.3.6 Configuring VRRP Priority 5
1.3.7 Configuring VRRP Clock Value 5
1.3.8 Configuring VRRP Monitoring Object 5
1.3.9 Monitoring and Maintaining VRRP 6
1.3.10 VRRP Configuration Example 6

Chapter 1 VRRP Configuration

1.1 Overview

The Virtual Router Redundancy Protocol (VRRP) ensures the successful single-node service in the default static routing condition. VRRP avoids the defects of a statically designated gateway. A group of switches can work together as a virtual switch through VRRP. The virtual switch has a virtual IP address and a virtual MAC address for the outside. VRRP chooses one switch from the switch group as the master switch, responsible for forwarding packet. When the master switch has problems, the standby switch will promptly take over the tasks of the master switch without changing the default gateway address. The whole takeover process is transparent to the terminal system. This mechanism can provide fast and effective resolution when trouble occurs.

1.2 VRRP Configuration Task List

- Enabling/Disabling VRRP on the Interface
- Configuring VRRP authentication mode
- Configuring VRRP priority preemption
- Configuring VRRP priority
- Configuring VRRP clock value
- Monitoring and maintaining VRRP

1.3 VRRP Configuration Task

1.3.1 Configuring VRRP Virtual IP Address

Run the following commands in vlan interface configuration mode.

Command	Purpose
vrrp *vrid* **associate** *virtual-address address-mask*	Configures VRRP Virtual IP address on the interface
no vrrp *vrid* **associate [***virtual-address address-mask***]**	Deletes VRRP Virtual IP address on the interface

The virtual switch is enabled after the virtual address of VRRP is configured. The virtual address and the primary IP address of the port must be in the same network segment. Otherwise, the virtual switch remains in the Init state. When the virtual IP address and the IP address of the port are consistent, the system automatically promote the precedence of the routing switch to 255.

Run the following commands in vlan interface configuration mode.

Command	Purpose
vrrp *vrid* **authentication** *WORD*	Configures VRRP authentication mode to simple-text.
no vrrp *vrid* **authentication**	Resumes the VRRP authentication mode to the default setting.

In simple-text authentication mode, the authentication character string is in the message as clear code and is forwarded out. The receiver checks the authentication character string in the message to see whether it matches the locally configured authentication character string. The authentication character string has eight characters at most.

By default, the authentication mode of VRRP is no-authen.

1.3.3 Configuring VRRP Description

Run the following commands in vlan interface configuration mode.

Command	Purpose
vrrp *vrid* **description** *WORD*	Configures VRRP description information
no vrrp *vrid* **description**	Deletes VRRP description information

VRRP description information, which is used for stating the usage of local VRRP.

By default, VRRP has no description information.

1.3.4 Configuring VRRP Priority Preemption

Run the following commands in vlan interface configuration mode.

Command	Purpose
vrrp *vrid* **preempt [delay** *second***]**	Configures VRRP priority preemption
no vrrp *vrid* **preempt [delay]**	Resumes the default VRRP priority preemption mode.

The priority preemption is effective only to the backup switch. After the backup switch receives the announce message from the master switch, it will examine the priority of the master switch. If the priority level of the master switch is lower than the locally configured priority level and the backup switch is configured with priority preemption, the backup switch will leap from the backup state to the master state and send the announce message to the outside. Otherwise, the backup switch remains in the backup state.

In default state, the authentication mode of VRRP is no-authen.

1.3.5 Configuring VRRP Protocol Packet MAC Address

Run the following commands in vlan interface configuration mode.

Command	Purpose
vrrp *vrid* **source-mac-use-system**	Configures VRRP group to forward packets with system mac address
no vrrp*vrid* **source-mac-use-system**	Configures VRRP group to forward packets with protocol mac address

By default, VRRP protocol packet forward source address with protocol mac address; after the command is configured, VRRP protocol packet forwards the system mac address as the source address.

1.3.6 Configuring VRRP Priority

Run the following commands in vlan interface configuration mode.

Command	Purpose
vrrp *vrid* **priority** *value* **(1~254)**	Configures VRRP priority
no vrrp *vrid* **priority**	Resumes the default VRRP priority mode.

When the virtual address and the port address are same, VRRP will automatically increase its priority value to 255. After the virtual address or the port address changes, the priority value automatically resumes to the original value.

The default value is 100.

1.3.7 Configuring VRRP Clock Value

Run the following commands in vlan interface configuration mode.

Command	Purpose
vrrp*vrid* **timer advertise {** *value* **| dsec** *value* **| csec** *value* **}**	Configures VRRP clock value
no vrrp *vrid* **timer advertise**	Resumes the VRRP clock value to the default value.
no vrrp *vrid* **timer learn**	Configures VRRP clock as the learning mode

The clock value means the shortest time for the virtual routing switch to recover from a trouble. When the master switch is down, the backup switch will serve as the master routing switch after the 3*advertisement + skew_time interval. It is clear that the trouble cannot be removed immediately if the advertisement clock value is too big. Hence, the default value of the advertisement clock is recommended.

The default value is 1 second.

1.3.8 Configuring VRRP Monitoring Object

Run the following commands in vlan interface configuration mode.

Command	Purpose
vrrp *vrid* **track interface** *intf-id value*	Configures VRRP monitoring local interface state
no vrrp *vrid* **track interface** *intf-id*	Resumes to the default setting
vrrp *vrid* **track ip** *ip-address value*	Configures VRRP monitoring to the static routing state to the designated address
no vrrp *vrid* **track ip** *ip-address*	Resumes to the default setting.

With the monitoring function, VRRP group can adjust the priority appropriately according to the change of the link state. It provides an opportunity of switching master line state to the backup line state. The change of the link state refers to whether the destination link bypass the VRRP routing switch is reachable, rather than the VRRP switch itself is reachable.

VRRP supports two monitoring objects: First, monitoring the interface status. When the monitored port link state is down, lower the priority of itself proactively. Second, monitoring the static route state of designated node. When the monitored route is unreachable, lower the priority of itself proactively. Monitoring the static route state of designated node needs to apply the function of BFD detecting static route.

1.3.9 Monitoring and Maintaining VRRP

Run the following commands in EXEC configuration mode.

Command	Purpose
show vrrp { brief | [interface *vlan_intf***] [detail]}**	Displays the VRRP information.
debug vrrp [interface *intf-id vrid***] {errors | events | packets | all}**	Enables the debugging on-off for VRRP packets and events.
no debug vrrp	Disables the debugging on-off for VRRP packets and events.

Displaying the VRRP information:

Switch_config# **show vrrp interface vlan** *1* **detail**
VLAN1 - Group 1
VRRP State is Master
Virtual IP address : 192.168.20.110/24
Virtual Mac address : 0000.5e00.0101
Current Priority : 100 (Config 100)
VRRP timer : Advertise 1.0 s (default) master_down 3.6 s
VRRP current timer : Advertise 1.0 s master_down 0.0 s preempt after 0.0 s
Authentication string is not set
Preempt is set (delay : 0 s)
Learn Advertise Interval is not set
Master Router IP : 192.168.20.118, priority : 100, advertisment : 1.0 s

1.3.10 VRRP Configuration Example

The network topology is shown in figure 1.

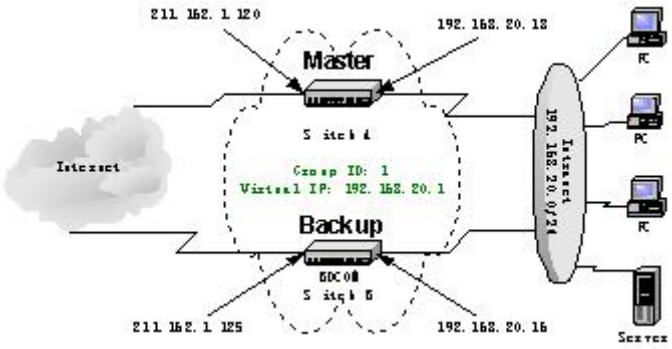


Figure1 1-1 Network topology

1. 1. Configuring Switch A

(1) Fault 1: Configure the address for the interface of the private network.

Switch_config_v1# **ip address** *192.168.20.18 255.255.255.0*

(2) Fault 2: Configure the address for the interface of the public network.

Switch_config_v2# **ip address** *211.162.1.120 255.255.255.0*

(3) Fault 3: Configure virtual switch group 1 on the interface of the private network. The virtual address is 192.168.20.1. The priority value is 120.

Switch_config_v1# **vrrp** 1 **associate** *192.168.20.1 255.255.255.0*

Switch_config_v1# **vrrp** 1 **priority** *120*

(4) Fault 4: Display information about the virtual switch.

Switch_config**#show vrrp detail**

VLAN1 - Group 1

VRRP State is Master

Virtual IP address : 192.168.20.1/24

Virtual Mac address : 0000.5e00.0101

Current Priority : 120 (Config 120)

VRRP timer : Advertise 1.0 s (default) master_down 3.6 s

VRRP current timer : Advertise 1.0 s master_down 0.0 s preempt after 0.0 s

Authentication string is not set

Preempt is set (delay : 0 s)

Learn Advertise Interval is not set

Master Router IP : 192.168.20.18, priority : 100, advertisment : 1.0 s

2. Configuring Switch B

(1) Configure the address for the interface of the private network.

Switch_config_v1# **ip address** *192.168.20.16 255.255.255.0*

(2) Configure the address for the interface of the public network.

Configure virtual switch group 1 on the interface of the private network. The virtual address is 192.168.20.1. The priority value is 120.

Switch_config_v1# **vrrp** 1 **associate** *192.168.20.1 255.255.255.0*

Display information about the virtual switch.

Switch_config**#show vrrp detail**

Switch_config**#show vrrp interface vlan** *1* **detail**

VLAN1 - Group 1

VRRP State is Backup

Virtual IP address : 192.168.20.1/24

Virtual Mac address : 0000.5e00.0101

Current Priority : 100 (Config 100)

VRRP timer : Advertise 1.0 s (default) master_down 3.6 s

VRRP current timer : Advertise 0.0 s master_down 3.0 s preempt after 0.0 s

Authentication string is not set

Preempt is set (delay : 0 s)

Learn Advertise Interval is not set

Master Router IP : 192.168.20.18, priority : 120, advertisement : 1.0 s

3. Configuring PC and Server of the Private Network

Configure the default gateway for each PC and server in the private network to 192.168.20.1.

Multicast Configuration

Table of Contents

Chapter 1 Multicast Overview 1
1.1 Multicast Routing Realization 1
1.2 Multicast Routing Configuration Task List 2
1.2.1 Basic Multicast Configuration Task List 2
1.2.2 IGMP Configuration Task List 2
1.2.3 PIM-DM Configuration Task List 3
1.2.4 PIM-SM Configuration Task List 3
Chapter 2 Basic Multicast Routing Configuration 4
2.1 Starting up Multicast Routing 4
2.2 Starting up the Multicast Function on the Port 4
2.2.1 Starting up PIM-DM 4
2.2.2 Starting up PIM-SM 4
2.3 Configuring TTL Threshold 5
2.4 Configuring IP Multicast Boundary 5
2.5 Configuring IP Multicast Helper 5
2.6 Configuring Stub Multicast Route 7
2.7 Monitoring and Maintaining Multicast Route 7
Chapter 3 IGMP Configuration 9
3.1 Overview 9
3.2 IGMP Configuration 9
3.2.1 Changing Current IGMP Version 9
3.2.2 Configuring IGMP Query Interval 10
3.2.3 Configuring IGMP Querier Interval 10
3.2.4 Configuring Maximum IGMP Response Time 11
3.2.5 Configuring IGMP Query Interval for the Last Group Member 11
3.2.6 Static IGMP Configuration 11
3.2.7 Configuring the IGMP Immediate-leave List 12
3.3 IGMP Characteristic Configuration Example 13
Chapter 4 PIM-DM Configuration 16
4.1 PIM-DM Introduction 16
4.2 Configuring PIM-DM 17
4.2.1 Modifying Timer 17
4.2.2 Designating the Version Number 17
4.2.3 Configuring State-Refresh 17
4.2.4 Configuring Filtration List 18
4.2.5 Setting DR Priority 18
4.2.6 Clearing Item (S,G) 18
4.3 PIM-DM State-Refresh Configuration Example 19
Chapter 5 Configuring PIM-SM 20

Table of Contents

5.1 PIM-SM Introduction 20
5.2 Configuring PIM-SM 21
5.2.1 Enabling Global Multicast 21
5.2.2 Starting up PIM-SM 21
5.2.3 Configuring Neighbor Filter List 21
5.2.4 DR Election 23
5.2.5 Configuring Candidate RP 23
5.2.6 Configuring Candidate BSR 23
5.2.7 Configuring SPT-threshhold 24
5.2.8 Configuring SSM 24
5.2.9 Configuring Management Domain sz 25
5.2.10 Configuring Source Address of Registered Packets 26
5.2.11 Configuring anycast-rp 26
5.2.12 Displaying PIM-SM Multicast Route 26
5.2.13 Clearing Multicast Routes Learned by PIM-SM 27

Chapter 1 Multicast Overview

The chapter describes how to cofigure the multicast routing protocol. For the details of the multicast routing commands, refer to the part “Multicast Routing Commands”.

The traditional IP transmission allows only one host to communicate with a single host (unicast communication) or to communicate with all hosts (broadcast communication). The multicast technology allows one host to send message to some hosts. These hosts are called as group members.

The destination address of the message sent to the group member is a D-class address (224.0.0.0~239.255.255.255). The multicast message is transmitted like UDP. It does not provide reliable transmission and error control as TCP does.

The sender and the receiver make up of a multicast application. The sender can send the multicast message without joining in a group. However, the receiver has to join in a group before it receives the message from the group.

The relationship between group members is dynamic. The host can join in or leave a group at any time. There is no limitation to the location and number of the group member. If necessary, a host can be a member of multiple groups. Therefore, the state of the group and the number of group members varies with the time.

The router can maintain the routing table for forwarding multicast message by executing the multicast routing protocol such as PIM-DM and PIM-SM. The router learns the state of the group members in the directly-connected network segment through IGMP. The host can join in a designated IGMP group by sending the **IGMP Report** message.

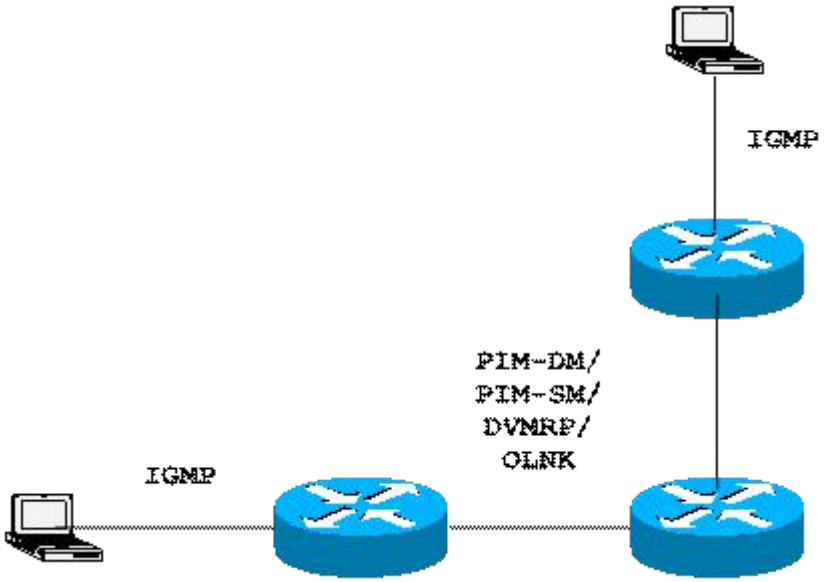
The IP multicast technology is suitable for the one-to-multiple multimedia application.

1.1 Multicast Routing Realization

In the router software of our router, the multicast routing includes the following regulations:

- IGMP runs between the router and the host in the LAN, which is used to track the group member relationship.
- OLNK is a static multicast technology, which is used in the simple topology. It realizes the multicast forwarding and effectively saves CPU and bandwidth.
- PIM-DM, PIM-SM and DVMRP is dynamic multicast routing protocols. They run between routeres and realizes the multicast forwarding by creating the multicast routing table.

The following figure shows the multicast protocols used in the IP multicast applications:



1.2 Multicast Routing Configuration Task List

1.2.1 Basic Multicast Configuration Task List

- Starting up the multicast routing (mandatory)
- Configuring TTL threshold (optional)
- Canceling rapid multicast forwarding (optional)
- Configuring static multicast route (optional)
- Configuring multicast boundary (optional)
- Configuring multicast helper (optional)
- Configuring Stub multicast route (optional)
- Monitoring and maintaining multicast route (optional)

1.2.2 IGMP Configuration Task List

- Modifying the current version of IGMP
- Configuring the IGMP query interval
- Configuring IGMP Querier interval
- Configuring the maximum response time of IGMP
- Configuring the query interval of the last IGMP group member
- Static IGMP configuration

- Configuring the IGMP **Immediate-leave** list

1.2.3 PIM-DM Configuration Task List

- Regulating the timer
- Designate the PIM-DM version
- Configuring the state refreshment
- Configuring the filtration list
- Setting the DR priority
- Clearing (S,G) information

1.2.4 PIM-SM Configuration Task List

- Configuring static RP
- Configuring standby BSR
- Configuring standby RP
- Displaying PIM-SM multicast routing
- Clearing multicast routes learned by PIM-SM

Chapter 2 Basic Multicast Routing Configuration

2.1 Starting up Multicast Routing

To allow the router software to forward the multicast message, you must start up the multicast routing. Run the following command in global configuration mode to start up the multicast message forwarding:

Command	Purpose
ip multicast-routing	Starts up the multicast routing.

2.2 Starting up the Multicast Function on the Port

When the multicast routing protocol runs on a port, the IGMP is activated on the port. The multicast routing protocols include OLNK, PIM-DM, PIM-SM and DVMRP. Only one multicast routing protocol is allowed to run on the same port. When the router connects multiple multicast domains, different multicast protocols can be run on different ports.

Although the router software can function as the multicast boundary router (MBR). If possible, do not simultaneously run multiple multicast routing protocols on the same router for some multicast routing protocols may be badly affected. For example, when PIM-DM and BIDIR PIM-SM simultaneously run, confusion is to occur.

2.2.1 Starting up PIM-DM

Run the following command to run PIM-DM on a port and then activate the multicast dense mode function:

Command	Purpose
ip pim-dm	Enters the port where PIM-DM is running and then activates PIM-DM multicast routing process in port configuration mode.

2.2.2 Starting up PIM-SM

To run PIM-DM on a port and activate the PIM-DM multicast, perform the following operation:

Command	Purpose
ip pim-sm	Enters a port where PIM-SM needs to run and then activates the PIM-SM multicast routing process in port configuration mode.

2.3 Configuring TTL Threshold

Run the command **ip multicast ttl-threshold** to configure the TTL threshold of the multicast message that is allowed to pass the port. Run the command **no ip multicast ttl-threshold** to use the default threshold value **1**.

Command	Purpose
ip multicast ttl-threshold *ttl-value*	Configures the TTL threshold on the port.

Example

The following example shows how the administrator configures the TTL threshold on a port:

interface ethernet 1/0

ip multicast ttl-threshold 200

2.4 Configuring IP Multicast Boundary

Run the command **ip multicast boundary** to configure the multicast boundary for the port. Run the command **no ip multicast boundary** to cancel the configured boundary. The commands used in the second configuration will replace the commands used in the first configuration.

Command	Purpose
ip multicast boundary *access-list*	Configures the multicast boundary for the port.

Example

The following example shows how to configure the management boundary for a port:

interface ethernet 0/0

ip multicast boundary acl

ip access-list standard acl

permit 192.168.20.97 255.255.255.0

2.5 Configuring IP Multicast Helper

Run the command **ip multicast helper-map** to use the multicast route to connect two broadcast networks in the multicast network. Run the command **no ip multicast helper-map** to cancel the command.

Command	Purpose
interface *type number*	Enters the interface configuration mode.
ip multicast helper-map broadcast *group-address access-list*	Configures the command **ip multicast helper** to convert the broadcast message to the multicast message.
ip directed-broadcast	Allows the directional broadcast.

ip forward-protocol [*port*]	Configures the port number allowing to forward the message.

On the last-hop router connecting the destination broadcast network, perform the following operations:

Command	Purpose
interface *type number*	Enters the interface configuration mode.
ip directed-broadcast	Allows the directional broadcast.
ip multicast helper-map *group-address broadcast-address access-list*	Configures the command **ip multicast helper** to convert the multicast message to the broadcast message.
ip forward-protocol [port]	Configures the port number allowing to forward the message.

Example

The following example shows how to configure the command **ip multicast helper**.

The configuration of the router is shown in the following figure. Configure the command **ip directed-broadcast** on the e0 port of the first-hop router to handle the directional message. Configure **ip multicast helper-map broadcast 230.0.0.1 testacl1**, allowing to convert the UDP broadcast message with port number 4000 that is sent from the source address 192.168.20.97/24 to the multicast message with the destination address 230.0.0.1.

Configure the command **ip directed-broadcast** on the e1 port of the last-hop router to handle the directional message. Configure **ip multicast helper-map 230.0.0.1 172.10.255.255 testacl2**, allowing to convert the multicast message with port number 4000 and the destination address 230.0.0.1 that is sent from the source address 192.168.20.97/24 to the broadcast message with the destination address 172.10.255.255.

In the first-hop router connecting the source broadcast network, perform the following operations: (the router is configured on the VLAN port)

```
interface ethernet 0
ip directed-broadcast
ip multicast helper-map broadcast 230.0.0.1 testacl
ip pim-dm
!
ip access-list extended testacl    permit udp 192.168.20.97 255.255.255.0 any
ip forward-protocol udp 4000
```

In the last-hop router connecting the destination broadcast network, perform the following operations:

```
interface ethernet 1
ip directed-broadcast
ip multicast helper-map 230.0.0.1 172.10.255.255 testacl2
ip pim-dm
!
ip access-list extended testacl2    permit udp 192.168.20.97 255.255.255.0 any
```

ip forward-protocol udp 4000

2.6 Configuring Stub Multicast Route

Run the commands **ip igmp helper-address** and **ip pim-dm neighbor-filter** to configure the Stub multicast route.

On the port where the stub router and the host are connected, perform the following operations:

Command	Purpose
interface *type number*	Enters the interface configuration mode.
ip igmp helper-address *destination-address*	Configures the command **ip igmp helper-address** to forward the multicast message to the central router.

On the port where the central router and the stub router are connected, perform the following operations:

Command	Purpose
interface *type number*	Enters the interface configuration mode.
ip pim neighbor-filter *access-list*	Filters all **pim** messages on the stub router.

Example

The configuration of router A and B is shown as follows:

Stub Router A Configuration

ip multicast-routing

ip pim-dm

ip igmp helper-address 10.0.0.2

Central Router B Configuration

ip multicast-routing

ip pim-dm

ip pim-dm neighbor-filter stubfilter

ip access-list stubfilter

deny 10.0.0.1

2.7 Monitoring and Maintaining Multicast Route

a. Clearing the multicast cache and the routing table

If special caches or the routing table is invalid, you need to clear its content. Run the following commands in management mode:

Command	Purpose
clear ip igmp group [*type number*] [*group-address* | <*cr*>]	Clears the items in the IGMP cache.

clear ip mroute *[* | group-address | source-address]*	Clears the items in the multicast routing table.

b. Displaying the multicast routing table and system statistics information

The detailed information about the IP multicast routing table, cache or database helps to judge how the resources are used and to resolve network problems.

Run the following commands in management mode to display the statistics information about the multicast route:

Command	Purpose
show ip igmp groups [*type number* | *group-address*] [detail]	Displays the information about the multicast group in the IGMP cache.
show ip igmp interface [*type number*]	Displays the IGMP configuration information on the interface.
show ip mroute mfc	Displays the multicast forwarding cache.
show ip rpf [**ucast | mstatic | pim-dm** | **pim-sm** | **dvmrp**] *source-address*	Displays the RPF information.

Chapter 3 IGMP Configuration

3.1 Overview

a. IGMP

Internet Group Management Protocol (IGMP) is a protocol used to manage multicast group members. IGMP is an asymmetric protocol, containing the host side and the switch side. At the host side, the IGMP protocol regulates how the host, the multicast group member, reports the multicast group it belongs to and how the host responds to the query message from the switch. At the switch side, the IGMP protocol regulates how the IGMP-supported switch learns the multicast group member ID of the hosts in the local network and how to modify the stored multicast group member information according to the report message from the host.

Since our switches support the IGMP Router protocol, the multicast routing protocol can be provided with the information about the multicast group members in the current network and the switch decides whether to forward the multicast message. In a word, to enable the switch support the multicast process of the IP message, the switch need be configured to support the multicast routing protocol and the IGMP Router protocol. Currently, D-Link' switches support the IGMP Router protocol and version 3
IGMP, the latest version.

There is no independent startup commands for IGMP. The function of the IGMP-Router protocol is started up through the multicast routing protocol.

3.2 IGMP Configuration

The commands to configure the attributes of the IGMP-Router mainly are the commands to adjust the IGMP parameters. The following is to describe these commands. For details about these commands, refer to explanation documents relative to the IGMP commands.

3.2.1 Changing Current IGMP Version

Up to now, the IGMP protocol has three formal versions. The corresponding RFCs are RFC1112, RFC2236 and RFC3376. IGMP V1 supports only the function to record the multicast group members. IGMP V2 can query the designated multicast group member, generates the leave message when an IGMP host leaves a multicast group, and shortens the change delay of the group member. IGMP V3 has additional functions to update and maintain the multicast group member IDs which correspond to the source host addresses. The IGMP Router protocol of IGMP V3 is fully compatible with the host side of IGMP V1 and IGMP V2. D-Link·s switch software supports the IGMP
Router protocols of the three IGMP versions.

You can configure the IGMP-Router function at different interfaces (the multicast routing protocol configured on different interfaces can start up the IGMP-Router function) and different versions of IGMP can be run on different interfaces.

Note that a multicast switch can start up the IGMP-Router function on only one of the ports that connect the same network.

Run the following command in interface configuration mode to change the version of the IGMP-Router protocol on a port:

Command	Purpose
ip igmp version *version_number*	Changes the IGMP version running on the current port.

3.2.2 Configuring IGMP Query Interval

No matter what version number of the current IGMP-Router protocol is, the multicast switch can send the IGMP General Query message every a certain time on the port where the IGMP-Router function is started. The transmission address is 224.0.0.1. The purpose of the multicast switch is to get the report message from the IGMP host and therefore know which multicast group each IGMP host in the network belongs to. The interval to send the General Query message is called as IGMP Query Interval. If the parameter IGMP Query Interval is set to a big value, the switch cannot immediately receive the information about which multicast group the current IGMP host belongs to. If the parameter IGMP Query Interval is set to a small value, the flow of the IGMP message is to increase in the current network.

Run the following command in interface configuration mode to modify the IGMP query interval on a port:

Command	Purpose
ip igmp query-interval *time*	Modifies the IGMP query interval on the current interface (unit: second).

3.2.3 Configuring IGMP Querier Interval

As to version 2 and version 3 of the IGMP-Router protocol, if another switch that runs the IGMP-Router protocol exists in the same network, you need to choose a querier. Querier stands for a switch that can send the query message (In fact, it is a port of the switch where the IGMP-Router protocol is enabled). Normally, one network has only one querier, that is, only one switch sends the IGMP Query message. There is no querier choice for IGMP-Router V1 because the multicast routing protocol decides which switch to send the IGMP Query message in IGMP-Router V1.

IGMP-Router V2 and IGMP-Router V3 have the same querier choice mechanism, that is, the switch with the minimum IP address is the querier in the network. The switch that is not the querier needs to save a clock to record the existence of the querier. If the clock times out, the non-querier switch turns to be the querier until it receives the IGMP Query message from the switch with a smaller IP address.

For IGMP-Router V2, you can configure other querier intervals using the following command:

Command	Purpose
ip igmp querier-timeout *time*	Configures the interval for other queriers (unit: second).

For IGMP-Router V1, the interval of other queriers is useless. For IGMP-Router V3, the interval cannot be configured because it is decided by the protocol itself.

3.2.4 Configuring Maximum IGMP Response Time

For IGMP-Router V2 and IGMP-Router V3, special data field in the transmitted IGMP General Query message regulates the maximum response time of the IGMP host. That is, the IGMP host has to send the response message before the regulated maximum response time expires, indicating that the General Query message is received. If the maximum response time is set to a big value, the change of multicast group members delays. If the maximum response time is set to a small value, the flow of the IGMP message will be increased in the current network.

Note:

The maximum IGMP response time must be shorter than the IGMP query interval. If the value of the maximum response time is bigger than the query interval, the system will automatically set the maximum response time to **query-interval – 1**.

For IGMP-Router V2 and IGMP-Router V3, run the following command in interface configuration mode to set the maximum IGMP response time:

Command	Purpose
ip igmp query-max-response-time *time*	Configures the maximum IGMP response time (unit: second).

For IGMP-Router V1, the maximum IGMP response time is decided by the protocol itself. Therefore, the previous command is useless to IGMP-Router V1.

3.2.5 Configuring IGMP Query Interval for the Last Group Member

For IGMP-Router V2 and IGMP-Router V3, When the Group Specific Query message for a specific multicast group is sent, the query interval of the last group member will be used as the maximum response time of the host. That is, the IGMP host has to send the response message before the maximum response time of the last group member expires, indicating that the Group Specific Query message is received. If the IGMP host finds that it need not respond to the query message, it will not respond to the message after the interval. In this case, the multicast switch is to update the saved multicast group member information. If the query interval of the last group member is set to a big value, the change of the multicast group member delays. If the query interval of the last group member is set to a small value, the flow of the IGMP message is to increase in the current network.

For IGMP-Router V2 and IGMP-Router V3, run the following command in interface configuration mode to configure the IGMP query interval of the last group member:

Command	Purpose
ip igmp last-member-query-interval *time*	Configures the IGMP query interval of the last group member (unit: ms).

The previous command is useless for IGMP-Router V1.

3.2.6 Static IGMP Configuration

Besides the functions regulated by the IGMP-Router protocol, BODCOM's switches support the static multicast group configuration on the port. For the IGMP host, its multicast group member relationship may vary. Suppose the IGMP host only belongs to

the multicast group **group1**, it receives the multicast message from and sends the multicast message to the multicast group **group1**. After a period of time, it may belong to the multicast group **group2**, and receives the multicast message from and sends the multicast message to the multicast group **group2**. After another period of time, the IGMP host may not belong to any multicast group. Therefore, the multicast group assignment information varies.

Different the above “dynamic multicast group”, if a port is configured to belong to a static multicast group, the multicast routing protocol then takes the port as one that always receives and sends the multicast message of the multicast group. To be better compatible with IGMP-Router V3, the static multicast group can be configured to receive the multicast message from the designated source address, that is, the source-filter function is added when the multicast message is received.

Run the following command in interface configuration mode to configure the static multicast group for a port:

Command	Purpose
ip igmp static-group { * | *group-address*} {**include** *source-address* | <*cr*> }	Configures the static multicast group attribute for a port.

3.2.7 Configuring the IGMP Immediate-leave List

If IGMP V2 is started up on a port of the switch and the network that the port connects has only one IGMP host, you can realize the Immediate Leave function of the IGMP host by configuring the **IGMP Immediate-leave** list. According to the regulations of IGMP V2, when a host leaves a specific multicast group, the host will send the Leave message to all multicast switches. After receiving the Leave message, the multicast switches send the Group Specific message to confirm whether any multicast message to be received from or sent to the multicast group by the host exists on the port. If the Immediate Leave function is configured, no message need be interacted between the IGMP host and the multicast switch, the change of the multicast group member IDs will not be delayed.

Note:

The command can be configured both in global configuration mode and in interface configuration mode. The priority of the command configured in global configuration mode is higher than that configured in interface configuration mode. If the command is first configured in global configuration mode, the command configured in interface configuration mode will be omitted. If the command is first configured in interface configuration mode, the command configured in global configuration mode will delete the command configured in interface configuration mode.

For IGMP-Router V2, run the following command in interface configuration mode to configure the IGMP **Immediate-leave** list:

Command	Purpose
ip igmp immediate-leave group-list *list-name*	Configures the access list that realizes the function to immediately leave the multicast group for the IGMP host.
ip access-list standard *list-name*	Creates a standard IP access list named **list-name**.
permit *source-address*	Configures the IP address for the IGMP host that will realize the immediate-leave

	function in standard access-list configuration mode.

The previous command is invalid to IGMP-Router V1 and IGMP-Router V3.

3.3 IGMP Characteristic Configuration Example

All configurations about the IGMP characteristics are performed in VLAN port.

a. Example for changing the IGMP version

The IGMP-Router protocol of latter version is compatible with the IGMP host of low version, but cannot be compatible with the IGMP-Router protocol of the earlier version. Therefore, if, there are switches running the IGMP-Router protocol of the earlier version in the current network, you need to change the IGMP-Router protocol of latter version to the IGMP-Router protocol of earliest version in the same network segment.

Suppose the administrator knows that switches running IGMP-Router V1 and IGMP-Router V2 exist in a network that the local switch connects, the administrator needs to change the version of the IGMP-Router protocol from version 2 to version 1 on a port of the switch that runs IGMP-Router V2.

```
interface ethernet 1/0
ip igmp version 1
```

b. IGMP query interval configuration example

The following example shows how to modify the IGMP query interval to 50 seconds on the interface **ethernet 1/0**:

```
interface ethernet 1/0
ip igmp query-interval 50
```

c. IGMP Querier interval configuration example

The following example shows how to modify the IGMP Querier interval to 100 seconds on the interface **ethernet 1/0**:

```
interface ethernet 1/0
ip igmp querier-timeout 100
```

d. Maximum IGMP response time example

The following example shows how to modify the maximum IGMP response time to 15 seconds on the interface **ethernet 1/0**:

```
interface ethernet 1/0
ip igmp query-max-response-time 15
```

e. Example for configuring IGMP query interval for the last group member

The following example shows how to modify the IGMP query interval of the last group member to 2000 ms on the interface ethernet 1/0:

interface ethernet 1/0

ip igmp last-member-query-interval 2000

f. Static IGMP configuration example

The configuration command of the static multicast group can define different classes of static multicast groups by adopting different parameters. The following examples shows the results of running different command parameter.

interface ethernet 1/0

ip igmp static-group *

The previous configuration command configures all static multicast groups on the interface ethernet 1/0. The multicast routing protocol is to forward all IP multicast messages to the interface ethernet 1/0.

interface ethernet 1/0

ip igmp static-group 224.1.1.7

The previous configuration command configures the static multicast group 224.1.1.7 on the interface ethernet 1/0, that is, the interface belongs to the multicast group 224.1.1.7. The multicast routing protocol is to forward all IP multicast messages that are finally sent to the multicast group 224.1.1.7 to the interface ethernet 1/0.

interface ethernet 1/0

ip igmp static-group 224.1.1.7 include 192.168.20.168

The previous configuration command configures the static multicast group 224.1.1.7 on the interface ethernet 0/0, and defines source-filter of the multicast group as 192.168.20.168. That is, the interface belongs to the multicast group 224.1.1.7, but it only receives the IP multicast messages from 192.168.20.168. The multicast routing protocol is to forward IP multicast messages that are received from 192.168.20.168 and finally sent to the multicast group 224.1.1.7 to the interface ethernet 0/0.

Run the following command in interface configuration mode to receive the IP multicast message that is from 192.168.20.169 and finally sent to the multicast group 224.1.1.7:

ip igmp static-group 224.1.1.7 include 192.168.20.169

The previous command can be executed for many times to define different source addresses.

Note:

In a multicast group, the multicast group information cannot be simultaneously configured both for a specific source address and for all source addresses. The command used in the later configuration will be omitted. For example, If you run the command **ip igmp static-group 224.1.1.7 include 192.168.20.168** after the command **ip igmp static-group 224.1.1.7** is executed, the command **ip igmp static-group 224.1.1.7 include 192.168.20.168** will be omitted.

g. IGMP Immediate-leave list configuration example

The following example shows how to set the access list to **imme-leave** on the interface ethernet 1/0 with the **immediate-leave** function and to add the IP address 192.168.20.168 of the IGMP host to the access list. The configuration ensures that the IGMP host with IP address 192.168.20.168 realizes the **immediate-leave** function.

```
interface ethernet 1/0
ip igmp immediate-leave imme-leave
exit
ip access-list standard imme-leave
permit 192.168.20.168
```

Chapter 4 PIM-DM Configuration

4.1 PIM-DM Introduction

Protocol Independent Multicast Dense Mode (PIM-DM) is a multicast routing protocol in dense mode. By default, when the multicast source starts to send the multicast data, all network nodes in the domain receive the data. Therefore, PIM-DM forwards the multicast packets in broadcast-pruning mode. When the multicast source starts to send data, the switches alongside forward the multicast packets to all PIM-activated interfaces except the RPF interface. In this way, all network nodes in the PIM-DM domain can receive these multicast packets. To finish the multicast forwarding, the switches alongside need create the corresponding multicast routing item (S,G) for group G and its source S. The routing item (S,G) includes the multicast source address, multicast group address, incoming interface, outgoing interface list, timer and logo.

If there is no multicast group member in a certain network segment, PIM-DM will send the pruning information, prune the forwarding interface connecting the network segment and then establish the pruning state. The pruning state corresponds to the timeout timer. When the timer times out, the pruning state turns to be the forwarding state again and the multicast data can be forwarded along these branches. Additionally, the pruning state contains information about the multicast source and the multicast group. When the multicast group member appears in the pruning area, PIM-DM actively sends the graft message to the upper field without waiting for the pruning state of the upper field to time out, turning the pruning state to the forwarding state.

As long as source S still sends information to group G, the first-hop switch will periodically send the refreshing information of the routing item (S,G) to the nether original broadcast tree to finish refreshing. The state refreshing mechanism of PIM-DM can refresh the state of the downstream, ensuring that the pruning of the broadcast tree does not time out.

In the multi-access network, besides the DR selection, PIM-DM also introduces the following mechanisms:

- Use the assertion mechanism to select the unique forwarder to prevent the multicast packet from being repeatedly forwarded.
- Use the add/prune restraint mechanism to reduce redundant add/prune information.
- Use the pruning deny mechanism to deny improper pruning actions.

In the PIM-DM domain, the switches that run PIM-DM periodically send the Hello information to achieve the following purposes:

- Discover neighboring PIM switches.
- Judge leaf networks and leaf switches.
- Select the designated router (DR) in the multi-access network.

To be compatible with IGMP v1, PIM-DM is in charge of the DR choice. When all PIM neighboring routers on the interface support DR Priority, the neighboring router with higher priority is selected as the DR. If the priority is the same, the neighboring router with the maximum interface IP value is selected as the DR. If the priority is not shown in the Hello message of multiple routers, the router whose interface has the biggest IP value is selected as the DR.

The PIM-DM v2 of DBCOM's switches supports the neighbor filtration list, CIDR, VLSM and IGMP v1-v3.

4.2 Configuring PIM-DM

4.2.1 Modifying Timer

The routing protocol adopts several timers to judge the transmission frequency of Hello message and state-refresh control message. The interval to transmit the Hello message affects whether the neighbor relationship can correctly created.

Run the following commands in switch configuration mode to regulate the timer:

Command	Purpose
ip pim-dm hello-interval	Sets the interval (unit: second) to send the Hello message from the interface and the neighbor.
ip pim-dm state-refresh origination-interval	For the first-hop switch directly connecting the source, the interval to send the state-refresh message is only valid to the configurations at the upstream ports. For the following switches, the interval is the period to receive and handle the state-refresh message.

4.2.2 Designating the Version Number

PIM-DM of the router only supports PIM v2.

As PIM v1 is out of date, we supports PIM v2 by default. The command here only aims to be compatible with the former in style.

Command	Purpose
ip pim-dm version *version*	Configures PIM-DM version on the switch logical port.

4.2.3 Configuring State-Refresh

The state-refresh control information of the PIM-DM is forwarded in management mode by default. The configuration commands in interface configuration mode are effective only to the configurations at the upstream ports when the first-hop switch directly connecting the source sends the state-refresh message periodically. For the following switches, the interval is the period to receive and handle the state-refresh message.

Command	Purpose

no ip pim-dm state-refresh disable	Allows to send and receive the state-refresh message on the port.
ip pim-dm state-refresh origination-interval	Configures the interval to send and receive the state-refresh message on the port.

4.2.4 Configuring Filtration List

PIM-DM does not set the filtration list by default. The referred filtration list includes the neighbor filtration list and the multicast boundary filtration list. The filtration list requires to be configured in interface configuration mode.

To forbid a switch or switches at a network segment to join in the PIM-DM negotiation, the neighbor filtration list need be configured. To forbid or permit some groups to pass the local region, the multicast boundary filtration list need be configured.

Command	Purpose
ip pim-dm neighor-filter	Configures the neighbor filtration list.
ip multicast boundary	Configures the multicast boundary filtration list.

4.2.5 Setting DR Priority

To be compatible with IGMP v1, the DR choice is required. By default, the priority of the DR is set to **1**. When all PIM neighboring routers on the interface support DR Priority, the neighboring router with higher priority is selected as the DR. If the priority is the same, the neighboring router with the maximum interface IP value is selected as the DR. If the priority is not shown in the Hello message of multiple routers, the router whose interface has the biggest IP value is selected as the DR.

Run the following command in interface configuration mode:

Command	Purpose
ip pim-dm dr-priority	Configures the priority for the local DR on the designated port.

4.2.6 Clearing Item (S,G)

Normally, item (S,G) in the local MRT or the statistics value of the multicast message number forwarded through item (S,G) need be cleared. Run the following commands in management mode.

Command	Purpose
clear ip mroute pim-dm {***** | *group* [*source*]}	Clears the item (S,G) in the local MRT. The operation is to delete all or part items of the local multicast routing table. Multicast message forwarding may be affected. The command is used to delete only the (S,G) items created by the PIM-DM multicast routing protocol on the upstream ports.
clear ip pim-dm interface	Resets the statistics value of multicast message forwarded by (S,G) on the PIM-DM port. The command is used to reset only the

	(S,G) items created by the PIM-DM multicast routing protocol on the upstream ports.

4.3 PIM-DM State-Refresh Configuration Example

Refer to section 4.2.2 “Configuring State-Refresh”.

Chapter 5 Configuring PIM-SM

5.1 PIM-SM Introduction

Protocol Independent Multicast Spare Mode (PIM-SM) is a multicast routing protocol in sparse mode. In the PIM-SM domain, the switches that run PIM-SM periodically send the Hello information to achieve the following purposes:

- Discover neighboring PIM-SM switches.
- Select the designated router (DR) in the multi-access network.

The DR sends the join/prune message to the directly-connected group members at the direction of multicast distribution tree, or sends the data of the directly-connected multicast source to the multicast distribution tree.

PIM-SM forwards the multicast packet by creating the multicast distribution tree. The multicast distribution tree can be classified into two groups: Shared Tree and Shortest Path Tree. Shared Tree takes the RP of group G as the root, while Shortest Path Tree takes the multicast source as the root. PIM-SM creates and maintains the multicast distribution tree through the displayed join/prune mode. As shown in Figure 5-1, when the DR receives a Join message from the receiving side, it will multicast a (*, G)-join message at each hop towards the RP of group G to join in the shared tree. When the source host sends the multicast message to the group, the packet of the source host is packaged in the registration message and unicast to the RP by the DR; The RP then sends the unpackaged packet of the source host to each group member along the shared tree; The RP sends the (S,G)-join message to the first-hop switch towards the source's direction to join in the shortest path tree of the source; In this way, the packet of the source will be sent to the RP along the shortest path tree without being packaged; When the first multicast data arrives, the RP sends the registration-stop message to the DR of the source and the DR stops the registration-packaged process. Afterwards, the multicast data of the source is not packaged any more, but it will be sent to the RP along the shortest path three of the source and then sent to each group member by the RP along the shared tree. When the multicast data is not needed, the DR multicasts the Prune message hop by hop towards the RP of group G to prune the shared tree.

PIM-SM also deals with the RP choice mechanism. One or multiple candidate BSRs are configured in the PIM-SM domain. You can select a BSR among candidate BSRs according to certain regulations. Candidate RPs are also configured in the PIM-SM domain. These candidate RPs unicast the packets containing RP's address and multicast groups to the BSR. The BSR regularly generates the Bootstrap message containing a series of candidate RPs and corresponding group addresses. The Bootstrap message is sent hop by hop in the whole domain. The switch receives and stores the Bootstrap message. After the DR receives a report about a group member's relationship from the directly-connected host, if the DR has no the routing item of the group, the DR will map the group address to a candidate RP through the Hash algorithm. The DR then multicasts the Join/prune message hop by hop towards the RP. Finally, the DR packages the multicast data in the registration message and unicasts it to the RP.

5.2 Configuring PIM-SM

5.2.1 Enabling Global Multicast

Command:

ip multicast-routing

no ip multicast-routing

If you want to use the protocol pim-sm, run the command in the configuration mode:

switch_config#ip multicast-routing

Show running as follows:

!

ip multicast-routing

!

If you don't want to use the protocol pim-sm, run the command in the configuration mode:

switch_config #no ip multicast-routing

5.2.2 Starting up PIM-SM

Run the following command to run PIM-SM on the interface to activate the multicast function in sparse mode:

Command	Purpose
ip pim-sm	Enters the interface where PIM-SM needs to be run and activates the PIM-SM multicast routing process in interface configuration mode.

5.2.3 Configuring Neighbor Filter List

pim-sm needs to maintain neighbor relation in work. pim-sm finishes negotiation of the detection and related parameters through Hello information. Pim-sm forwards pim-sm hello packet by multicast periodically to all pim routers (224.0.0.13) and set up the neighbor relation by receiving hello information and agreed parameters. If one router receives Hello information before forwarding Hello information, the router will deem existence of the neighbor, otherwise, it will deem no existence of the neighbor.

Configure the neighbor filter list on the corresponding interface and check and filter the neighbor for the hello packet. If the neighbor filter list is deleted or the forbidden neighbor is relived just now, the neighbor information can only be acquired when the next hello period is appeared.

Steps for configuring neighbor access list:

1. Configure main ip address on the interface;
2. Port protocol up
3. Configure pim-sm on the interface;
4. Configure pim-sm standard access list on the interface and filter the neighbor.

Configuration instances:

switch_config#interface v9

switch_config_v9#ip address 172.20.21.172 255.255.255.0

switch_config_v9#ip pim-sm

switch_config_v9#ip pim-sm nbr-filter nbr_permit

switch_config_v9#exit

switch_config#ip access-list standard nbr_permit

switch_config_std_nacl#permit 172.20.21.174 255.255.255.0

Configuration result: enable hello packets from segment 172.20.21.0/24 and set up neighbor relation.

R172_config_std_nacl#show ip pim-s nei

PIM-SMv2 Neighbor Table

Neighbor Interface Uptime/Expires DR

Address Prior

172.20.21.173 v9 00:15:24/00:01:30 1(DR)

Change the configuration as follows and the interface v9 only enables hello packets from 172.20.21.174.

SwitchA_config_std_nacl#permit 172.20.21.174 255.255.255.255

The debug information is as follows:

2004-1-1 00:16:26 PIM-SM: rcvd hello from 172.20.21.173, filter by acl

The former established neighbor will be aged gradually until timeout:

SwitchA#show ip pim-s nei

PIM-SMv2 Neighbor Table

Neighbor Interface Uptime/Expires DR

Address Prior

172.20.21.173 v9 00:17:21/00:00:03 1(DR)

5.2.4 DR Election

DR election is to select DR for the router segment by comparing the priority and IP address in the Hello packets of each router.

The role of DR plays:

1. For response on the host IGMP(v1) information, if the host connects two or more PIM-SM routers directly by the Ethernet, only DR informs these information and forwards packets (*,g) join. If DR and assert winner on the receiver end confronts, the former prevails.
2. DR on the multicast source generates original registration packets and register to RP.

If a new neighbor is found, DR is responsible for forwarding the local memorized BSM packets.

If the locak tries to become DR, enhance the local DR priority and IP address value in condition of the same DR priority.

Steps for configuring DR priority:

1. Configures main ip address on the interface;
2. Port protocol up;
3. Configure pim-sm on the interface;
4. Configure ip pim-sm dr-pri ** on the interface;

5.2.5 Configuring Candidate RP

Configure the candidate RP to enable it to be sent to the BSR periodically and then be diffused to all PIM-SM routers in the domain, ensuring the RP mapping is unique.

Run the following command in global configuration mode:

Command	Purpose
ip pim-sm rp-candidate [**type** *number*] [**interval**|*group-list acl-name*] **no ip pim-sm rp-candidate** [**type** *number*]	Configures the local switch as the candidate RP. After the candidate RP is configured, it will be sent to the BSR periodically. The BSR then broadcasts all PIM-SM routers in the PIM-SM domain.

5.2.6 Configuring Candidate BSR

The configuration of the candidate RP can generate the unique global BSR in the PIM-SM domain. The global BSR collects and distributes the RP in the domain, ensuring the RP mapping is unique.

Run the following command in global configuration mode:

Command	Purpose
ip pim-sm bsr-candidate *type number*	Configures the local switch as the candidate

[*hash-mask-length*] [**priority**] **no ip pim-sm bsr-candidate** *type number*	BSR, and competes the global BSR by learning the BSM message.

5.2.7 Configuring SPT-threshhold

When the data is forwarded on the switch, it needs to judge whether shift RPT to SPT. The evidence for this judge is spt-threshold. By default SPT switches if the receiver receives the first data packet. We can set the threshold of RPT switching to SPT; unit: KB/s. In general if RPT switches to SPT, there is no return.

switch_config#router pim-sm

switch_config_ps#spt-threshold 1000

5.2.8 Configuring SSM

SSM model needs support of IGMPv3 and enables IGMPv3 on the PIM-SM device of the receiver. SSM model can be realized by the subset function of pim-sm and the system enables functions of PIM-SM and SSM. When deploying pim-sm, it is recommend to enable pim-sm on all non-boundary interfaces.

During the process of transmitting the information of multicast source to the receiver, whether pim-ssm or pim-sm is determined by whether the multicast group of the receiver prescribed channel (S, G) exists within the multicast group of pim-ssm. Interfaces which enables pim-sm will deem the multicast group within the range adopting the model “pim-ssm”.

Before configuring the basic functions of pim-ssm, the unicast route needs to be configured first, which ensures the interaction of the inner network layer and available route.

Steps for configuring pim-ssm:

1. Enable pim-sm on the interface;
2. Enter pim-sm configuration mode and address range of SSM group address;
3. Configure other functions of pim-sm (optional).

Configuration instances:

switch_config#interface v8

switch_config_v8#ip addr 1.1.1.1 255.255.255.0

switch_config_v8#ip pim-sm

switch_config_v8#exit

switch_config#router pim-sm

switch_config_ps#ssm rang grp_range

switch_config_ps#exit

switch_config#ip access-list standard grp-range

switch_config_std_nacl#permit 233.1.0.0 255.255.0.0

switch_config_std_nacl#

The following configuration does not take the default 232.0.0.0/8 as the group range of SSM, but 233.1.0.0/8. If SSM is canceled, disable ssm related configuration with “no” in the configuration mode of pim-sm.

5.2.9 Configuring Management Domain sz

In the mechanism of non-management domain, one pim-sm domain only has an exclusive BSR. The whole network is controlled by the BSR. For better management, the whole pim-sm domain can be divided into many management domains: each management domain maintains one BSR respectively and serves the multicast group within a certain range; global domain also maintains one BSR, which serves all left multicast groups.

In the mechanism of management domain, the boundary of each management domain is consisted of ZBR and each management domain maintains one BSR, which serves the multicast group of a certain range. The packets(such as assert message and BSR BootStrap message) of multicast protocol belonging to this range cannot pass the boundary of the management domain.

In the network which applies the management domain mechanism, select BSR for different multicast groups from C-BSR. C-RP within the network only forward inform packets to the corresponding BSR and BSR summarizes these packets on RP-SET and inform all devices within the service management domain.

For a group, if you want to find its rp, find sz corresponding to this group based on the longest prefix and sub-mask prevails; and find the corresponding RP-SET in sz according to the prefix and sub-mask of the group, and then calculate rp.

Steps for configuring management domain:

1. On management boundary device ZBR, configuring the range of local management domain group.
2. In the management domain, enter the configuration of pim-sm:
   i. Configure the group range of standby BSR and keep consistent with the management domain boundary.
   ii. Configure standby BSR and designate standby BSR port.

Configuration instances:

1. Configure the management domain range on ZBR

Sa_config_v9#ip pim-sm admin-scope 225.1.1.0 255.255.255.0

3. Configure the group range and port of standby BSR on domain pim-sm device

Sb_config#interface loopback1

Sb_config_l1#ip addr 1.1.1.1 255.255.255.0

Sb_config_l1#ip pim-sm

Sb_config#router pim-sm

Sb_config_ps#c-bsr admin-scope 225.1.1.0 255.255.255.0 30 200

Sb_config_ps#c-bsr loopback1 32 250

30,32 means the sub-mask length of hash, and 200, 250 means standby BSR priority. When there is inconsistency, the designated value when configuring standby BSR is superior to that of configuring management domain.

5.2.10 Configuring Source Address of Registered Packets

By default, when DR on the data source forwarding register packets, the address with DR will be taken as the source address of the registered packets. We can designate any active pim-sm interface on the DR device as the source address of the registered packets.

Configuration instances:

Sb_config#interface loopback1

Sb_config_l1#ip addr 1.1.1.1 255.255.255.0

Sb_config_l1#ip pim-sm

Sb_config#router pim-sm

Sb_config_ps# reg-src loopback 1

Designate the main address of loopback1 as the source address of the registered packets.

5.2.11 Configuring anycast-rp

An individual RP has a great load in the domain of pim-sm. To lower such burden, we can designate many same rp. The multicast source and the receiver will forward registered packets and join requests based on the latest rp.

If there is no MSDP module introduced, the neighbor of anycast-rp must be clearly specified when configuring anycast-rp and the neighbor address and the port address acting as rp cannot be the same.

Refer to *Pim-sm Command Manual* for configuration instances.

5.2.12 Displaying PIM-SM Multicast Route

Run the following command to check the multicast route information learned by PIM-SM:

Command	Purpose
show ip mroute pim-sm [*group-address*] [*source-address*] [**type** *number*] [**summary**] [**count**] [**active** *kbps*]	Displays the PIM-SM multicast route information.

5.2.13 Clearing Multicast Routes Learned by PIM-SM

Run the following command to clear multicast routes learned by PIM-SM:

Command	Purpose
clear ip mroute pim-sm [* | group-address] [source-address]	Clears information about the PIM-SM multicast routes.

IPv6 Configuration

Table of Contents

Chapter 1 IPv6 Protocol's Configuration....1
1.1 IPv6 Protocol's Configuration....1
1.2 Enabling IPv6....1
1.2.1 Setting the IPv6 Address....1
Chapter 2 Setting the IPv6 Services....3
2.1 Setting the IPv6 Services....3
2.1.1 Managing the IPv6 Link....3
Chapter 3 Configuring the Routing Management Modules....6
3.1 Overview....6
3.2 Configuration Task List of Routing Management Module....7
3.3 Routing Management Module's Configuration Tasks....8
3.3.1 Setting the Static Route....8
3.3.2 Setting the Threshold of Routes in a Routing Table....8
3.3.3 Monitoring and Maintaining the State of the Routing Table....9
3.4 Static Route's Configuration Example....11

Chapter 1 IPv6 Protocol's Configuration

1.1 IPv6 Protocol's Configuration

The configuration of the IPv6 address of the router only takes effect on the VLAN interface, not on the physical interface.

The IPv6 protocol is disabled in default state. If the IPv6 protocol need be used on a VLAN interface, this protocol should be first enabled in VLAN interface configuration mode. To enable the IPv6 protocol, users have to set the IPv6 address. If on a VLAN interface at least one IPv6 address is set, the VLAN interface can handle the IPv6 packets and communicates with other IPv6 devices.

To enable the IPv6 protocol, users should finish the following task:

- Setting at least one IPv6 address in VLAN interface configuration mode

1.2 Enabling IPv6

1.2.1 Setting the IPv6 Address

The IPv6 address is used to determine the destination address to which the IPv6 packets can be sent. There are three kinds of IPv6 addresses.

Kind	Referred Format	Remarks
Unicast address	2001:0:0:0:0DB8:800:200C:417A/64	**2001:0:0:0:0DB8:800:200C:417A** stands for a unicast address, while **64** stands for the length of the prefix of this address.
Multicast address	FF01:0:0:0:0:0:0:101	All multicast addresses begin with FF.
Any address	2002:0:0:0:0DB8:800:200C:417A/64	The format of this address is the same as that of the unicast address. Different VLAN interfaces can be set to have the same address, no matter it is a unicast/broadcast/multicast address.

For the further details of the IPv6 address, see RFC 4291.

In order to enable IPv6, users must set a unicast address in VLAN interface configuration mode. The set unicast address must be one or multiple addresses of the following type:

- Global IPv6 address

To set an IPv6 link-local address in VLAN interface configuration mode, run the following commands.

Command	Purpose
ipv6 enable	Sets a link-local address automatically.
ipv6 address fe80::x link-local	Sets a link-local address manually.

Note:

- The link-local address must begin with fe80. The default length of the prefix is 64 bit. At manual settings only the values at the last 64 bits can be designated.
- On a VLAN interface can only one link-local address be set.
- After IPv6 is enabled through the configuration of the link-local address, IPv6 only takes effect on the local link.

To set a global IPv6 address in VLAN interface configuration mode, run the following commands.

Command	Purpose
ipv6 address autoconfig	Sets a global address automatically.
ipv6 address [ipv6-address/prefix-length | prefix-name sub-bits/prefix-length] | [eui-64]	Sets a global address.
ipv6 address X:X:X:X::X/<0-128> anycast	Sets an address of unicast/broadcast/multicast.

Note:

- When IPv6 is enabled through the configuration of a global address, all interconnected IPv6 device can be handled by IPv6.
- If a link-local address has not been set before the configuration of the global address, the system will set a link-local address automatically.

Chapter 2 Setting the IPv6 Services

2.1 Setting the IPv6 Services

After IPv6 is enabled, all services provided by IPv6 can be set. The configurable IPv6 service is shown below:

(1) Managing the IPv6 Link

2.1.1 Managing the IPv6 Link

IPv6 provides a series of services to control and manage the IPv6 link. This series of services includes:

(1) Setting the transmission frequency of the ICMPv6 packet

(2) Setting the source IPv6 route

(3) Setting the MTU of IPv6

(4) Setting IPv6 redirection

(5) Setting IPv6 destination unreachablity

(6) Setting IPv6 ACL

(7) Setting IPv6 Hop-Limit

1. Setting the transmission frequency of the ICMPv6 packet

If you want to limit the transmission frequency of the ICMPv6 packet, run the command in the following table. If the ICMPv6 transmission frequency is larger than the set value, the transmission frequency will be limited.

The default transmission frequency is 1000us. If you want to modify the transmission frequency, run the following command in global mode:

Command	Purpose
ipv6 icmp6-ratelimit *ratelimit*	Sets the transmission frequency of the ICMPv6 packet.

2. Setting the source IPv6 route

IPv6 allows a host to designate the route of an IPv6 network, that is, the source route. The host can realize the source route through using the routing header in the IPv6 packets. The router can

security.

The router supports the source route by default. If the source route is closed, users can run the following command in global configuration mode to open the source route.

Command	Purpose
ipv6 source-route	Allows the source IPv6 route.

3. Setting the MTU of IPv6

All interfaces have a default IPv6 MTU. If the length of an IPv6 packet exceeds MTU, the router will fragment this IPv6 packet.

To set IPv6 MTU on a specific interface, run the following command in interface configuration mode:

Command	Purpose
ipv6 mtu *bytes*	Sets IPv6 MTU on an interface.

4. Setting IPv6 redirection

Sometimes, the route selected by the host is not the best one. In this case, when a switch receives a packet from this route, the switch will transmit, according to the routing table, the packet from the interface where the packet is received, and forward it to another router which belongs to the same network segment with the host. Under this condition, the switch will notify the source host of sending the packets with the same destination address to another router directly, not by way of the switch itself. The redirection packet demands the source host to replace the original route with the more direct route contained in the redirection packet. The operating system of many hosts will add a host route to the routing table. However, the switch more trusts the information getting from the routing protocol and so the host route will not be added according to this information.

IPv6 redirection is opened by default. However, if a hot standby router protocol is configured on an interface, IPv6 redirection is automatically closed. If the hot standby router protocol is canceled, this function will not automatically opened.

To open IPv6 redirection, run the following command:

Command	Purpose
ipv6 redirects	Allows IPv6 to transmit the redirection packets.

5. Setting IPv6 destination unreachablity

In many cases, the system will automatically transmit the destination-unreachable packets. Users can close this function. If this function is closed, the system will not transmit the ICMP unreachable packets.

To enable this function, run the following command:

	Purpose
ipv6 unreachables	Allows IPv6 to transmit the destination unreachable packets.

6. Setting IPv6 ACL

Users can use ACL to control the reception and transmission of packets on a VLAN interface. If you introduce ACL on a VLAN interface in global configuration mode and designate the filtration's direction, the IPv6 packets will be filtered on this VLAN interface.

To filter the IPv6 packets, run the following command in interface configuration mode.

Command	Purpose
ipv6 traffic-filter *WORD* { in | out }	Filters the IPv6 packets in the reception or transmission direction (in: receive; out: transmit) on a VLAN interface.

7. Setting IPv6 Hop-Limit

Users can designate a router to transmit the value of the hop-limit field in the packets (except those forwarded packets). All those packets that this router transmits out, if the upper-level application does not apparently designate a hop-limit value, use the set value of hop-limit. At the same time, the value of the hop-limit field is added to the RA packets that this router transmits.

The default hop-limit value is 64. If you want to change this value, you can run the following command in interface configuration mode.

Command	Purpose
ipv6 cur-hoplimit *value*	Designates a router to transmit the hop-limit field of the packets.

Chapter 3 Configuring the Routing Management Modules

3.1 Overview

The static route is a special route and configured by the administrator manually; after a static route is set the packets with a designated destination will be forwarded along the path that is designated by the administrator.

In those networks with simple networking structures, only the configuration of the static routes can realize network interconnection. Properly setting and using static routes can improve the performance of networks and guarantee the bandwidth for important network application.

The shortage of the static route is that it cannot automatically adapt to the change of the network topology. When the network has trouble or the topology changes, the static routes are unreachable and the network then interrupts. In this case, the network administrator has to change the settings of static routes manually.

If the data packets that reach a designated network cannot find the corresponding items in the routing table in a device, the device will then discard these data packets.

After a default route is configured on the current device, those data packets that have no corresponding items in the routing table will not be discarded by the current device but forwarded to another device, which will forward these data packets.

The default route is used only when a device has not found a matching entry in the routing table.

If the destination address of a packet does not match up any entry in the routing table, this packet will select the default route.

If there is no default route and the destination of the packet is not in the routing table, this packet will be discarded and an ICMPv6 packet will be sent back to the source terminal, reporting that the destination address and the network are unreachable.

The default routes can be generated in two ways:

an incoming data packet, if the current device cannot find the corresponding routing item in the routing table, it will forward this packet to the designated next-hop port that is set in the static route.

The second way is that the default route is generated by the dynamic routing protocols. A device with strong routing ability forwards the default route to other devices, and the other devices generate in their own routing tables the default route that is oriented to the device with strong routing ability.

3.2 Configuration Task List of Routing Management Module

The routing management module has the following configuration tasks:

- Setting the static route
- Setting the threshold of routes in a routing table
- Checking whether the next hop of the static route is reachable

3.3 Routing Management Module's Configuration Tasks

3.3.1 Setting the Static Route

To set the static route, run the following command in global configuration mode:

Command	Purpose
Ipv6 route *prefix / prefixlen* {*ipv6-address* | *interface-type interface-number* [*ipv6-address*]} [*distance*]	Sets the static route.

When setting the static route, you can designate the type and number of the outgoing interfaces, and also the address of the next hop. It depends on actual requirements whether to designate an outgoing interface or the next-hop address. The next-hop address cannot be the IPv6 address of the local address, or the static route is invalid.

When you run **IPv6 route** to set the static route, if the destination address and the mask are set to 0::0/0, the configured route is a default one. The **prefixlen** parameter in the configured prefix should be less than or equal to 64, or be equal to 128 (host's route).

Different management distances can be set for different static routes and therefore these static routes can be flexibly applied on the routing management modules.

The next hop of the configured static route must be activated, otherwise the static route cannot be activated. When the next hop is an interface or an interface VLAN, the interface must be a v6 one; when the next hop is a gateway, this gateway must be in the directly-connected network segment.

3.3.2 Setting the Threshold of Routes in a Routing Table

To a maximum number of routes in a routing table, that is, to set a threshold for routes in a routing table, run the following command in global configuration mode:

Command	Purpose

	systematic resources reasonably and provides a set speed.

3.3.3 Monitoring and Maintaining the State of the Routing Table

To display all kinds of statistics information about routes, run the following commands in EXEC mode:

Command	Purpose
show ipv6 route	Displays the information in the main routing table.
show ipv6 route [*protocol*]	Displays the routing information of the corresponding routing protocol in the routing table.

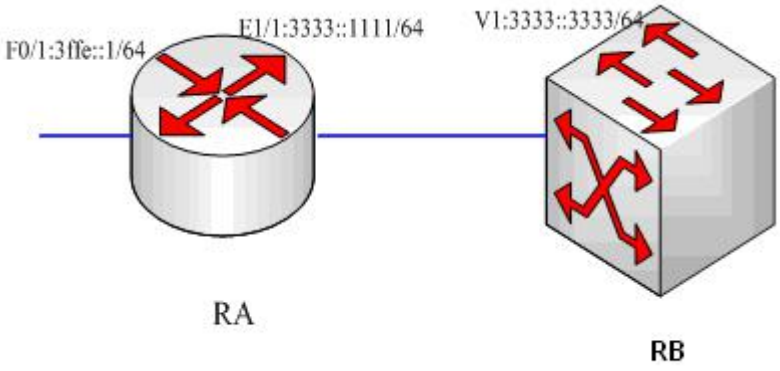
show ipv6 route summary	Displays the statistics information about the main routing table.
show ipv6 fib route	Displays the items in the main forwarding table, FIB.
show ipv6 fib summary	Displays the statistics information about the forwarding table.

To trace all related events and information on the route management module, run the following commands in EXEC mode.

Command	Purpose
debug ipv6 routing message	Traces the reception and transmission of the IPv6 information.
debug ipv6 routing search	Traces routing search.
debug ipv6 routing timer	Traces the IPv6 clock.
Debug ipv6 routing redis	Traces the IPv6-redistribute information.
debug ipv6 fib cache	Traces the IPv6-cache information.
Debug ipv6 fib message	Traces the information in the IPv6 forwarding table.

3.4 Static Route's Configuration Example

As shown in the following figure, RA directly connects router RB.



1) RA configuration:

```
interface    FastEthernet0/1
 no ip address
 no   ip   directed-broadcast
 ipv6 address 3FFE::1/64
!
interface    Ethernet1/1
 no ip address
 no  ip  directed-broadcast
 duplex half
 ipv6 address 3333::1111/64
!
```

2) RB configuration:

```
interface    VLAN1
 no ip address
 no   ip   directed-broadcast
 ipv6 address 3333::3333/64
!
```

3) Browsing the address of the local link of RA:

```
RA_config#show ipv6 route
Codes: C - Connected, L - Local, S - Static, R - Ripng, B - BGP
       ON1 - OSPF NSSA external type 1, ON2 - OSPF NSSA external type 2 OE1
       - OSPF external type 1, OE2 - OSPF external type 2
       DHCP - DHCP type

VRF ID: 0

C       3333::/64[1]
         is directly connected, C,Ethernet1/1
C       3333::1111/128[1]
         is directly connected, L,Ethernet1/1
C       3ffe::/64[1]
         is directly connected, C,FastEthernet0/1
```

```
C       3ffe::1/128[1]
         is directly connected, L,FastEthernet0/1
C       fe80::/10[1]
         is directly connected, L,Null0
C       fe80::/64[1]
         is directly connected, C,FastEthernet0/1
C       fe80::a00:3eff:fed5:effc/128[1]
         is directly connected, L,FastEthernet0/1
C       fe80::/64[1]
         is directly connected, C,Ethernet1/1
C       fe80::a00:3eff:fed5:effd/128[1]
         is directly connected, L,Ethernet1/1
C       ff00::/8[1]
         is directly connected, L,Null0
!
```

Setting a static route, which leads to subnet **3ffe::/64** on RB:

```
!

ipv6 route 3ffe::/64 3333::1111

!
```

Or:

```
!

ipv6 route 3ffe::/64 VLAN1 fe80::a00:3eff:fed5:effd

!
```

ND Configuration

Table of Contents

Chapter 1 ND Configuration 1
1.1 ND Overview 1
1.1.1 Address Resolution 1
1.1.2 ND Configuration 2

Chapter 1 ND Configuration

1.1 ND Overview

A node (host and router) uses ND (Neighbor Discovery protocol) to determine the link-layer addresses of the connected neighbors and to delete invalid cache rapidly. The host also uses the neighbor to discover the packet-forwarding neighboring routers. Additionally, the node uses the ND mechanism to positively trace which neighbors are reachable or unreachable and to test the changed link-layer address. When a router or the path to a router has trouble, the host positively looks for another working router or another path.

IPv6 ND corresponds to IPv4 ARP, ICMP router discovery and ICMP redirect.

ND supports the following link types: P2P, multicast, NBMA, shared media, changeable MTU and asymmetric reachability. The ND mechanism has the following functions:

(1) To discover routers: how the host to locate the routers on the connected links.

(2) To discover prefixes: how the host to find a group of address prefixes, defining which destinations are on-link on the connected links.

(3) To discover parameters: how the node to know the link-related or network-related parameters of the transmission interface.

(4) To automatically set addresses: how the node to set the address of an interface automatically.

(5) Address solution: When the IP of a destination is given, how a node determines the link-layer address of the on-link destination.

(6) To determine the next hop: it is an algorithm to map the IP address of a destination to the neighboring IP. The next hop can be a router or destination.

(7) To test unreachable neighbors: how a node to determine unreachable neighbors; if neighbor is a router, the default router can be used.

(8) To test repeated address: how a node to determine whether a to-be-used address is not used by another node.

(9) Redirect: how a router to notify the host of the best next hop.

1.1.1 Address Resolution

Address resolution is a procedure of resolving the link-layer address through node's IP. Packet exchange is realized through ND request and ND notification.

- Configuring a static ND cache

In most cases, dynamic address resolution is used and static ND cache configuration is not needed. If necessary, you can set static ND cache in global

following table shows how to set a static-IP-to-link-layer-address mapping.

Run the following relative command in global mode:

Command	Purpose
ipv6 neighbor ipv6address **vlan** vlanid hardware-address	Sets a static ND cache and translates IPv6 address into a link-layer address.

1.1.2 ND Configuration

The ND protocol is used not only for address resolution but for other functions such as neighbor solicitation, neighbor advertisement, router solicitation, router advertisement and redirect.

The following commands are all run in port configuration mode:

- Setting the number of transmitted NSs when ND performs DAD on a local port

Before the IPv6 port is started, it should send the NS information to the local machine to find if there is any duplicate IPv6 address existing on links through DAD.

Command	Purpose
ipv6 nd dad attempts num	Sets the number of transmitted NSs when the local port performs DAD.

- Setting the M flag in the RA message transmitted by the local port

The M flag indicates that the RA message host should obtain addresses through on-status automatic configuration. To set the M flag in the RA message transmitted by the local port to 1, run the following command.

Command	Purpose
ipv6 nd managed-flag	Sets the M flag in the RA message transmitted by the local port.

- Setting the NS transmission interval of the local port and the **retrans-timer** field in the RA message

This command can be used to set the NS transmission interval of the local switch on the local port and at the same time the **retrans-timer** field in the RA message on the local port.

The host sets its **retrans-timer** variable according to the retrans-timer field in RA.

Command	Purpose
ipv6 nd ns-interval milliseconds	Means the NS retransmission interval in the local port and the retrans-timer field in the RA message.Its default value is 1000ms.

- Setting the O flag in the RA message transmitted by the local port

The O flag indicates that the RA message host should obtain other information through on-status automatic configuration. To set the O flag in the RA message transmitted by the local port to 1, run the following command:

Command	Purpose
ipv6 nd other-flag	Sets the O flag in the RA message transmitted by the local port.

- Setting the prefix of the RA message

The router releases address prefixes to the network host via RA message. The address prefix plus the host address is the entire unicast address. The prefix option is carried by the RA message, and the host obtains the IPv6 address prefix and related parameter from this option.

Command	Purpose
ipv6 nd prefix {ipv6-prefix/prefix-length | **default**} [**no-advertise** | [valid-lifetime preferred-lifetime [**off-link** | **no-autoconfig**]]]	Means that the local port transmits the prefix option's content in the RA message.

- Setting the RA transmission interval

The following command is used to set the range of RA transmission interval. The RA transmission interval is in general an indefinite value but a random value in a fixed range, which can avoid abrupt flow surge in the network.

Command	Purpose
ipv6 nd ra-interval-range max min	Sets the range of RA transmission interval. The maximum RA transmission interval is 600s and the minimum RA transmission interval is 200s.

The interval for the local port to transmit the first three messages cannot be more than 16 seconds, while that to transmit the following messages varies between the maximum interval (600 seconds) and the minimum interval (200 seconds).

- Setting a specific RA transmission interval

RA packets are transmitted in an interval configured by **ra-interval-range**, but if users want to use a specific transmission interval, they can set this value through the following command:

Command	Purpose
ipv6 nd ra-interval interval	Sets a specific RA transmission interval, which is not set by default.

- Setting the router-lifetime field in the RA message transmitted by the local port

The **router-lifetime** field in the RA message is the triple of the maximum value of **ipv6 nd ra-interval-range**.

Command	Purpose
ipv6 nd ra-lifetime seconds	Sets the router-lifetime field in the RA message transmitted by the local port.

- Setting the reachable-time field of the RA message

reachable-time means the time to reach a neighbor, which is 0 by default.

Command	Purpose
ipv6 nd reachable-time milliseconds	Sets the **reachable-time** field in the RA message transmitted by the local port. Its default value is 0ms.

- Setting the value of the router preference in the RA message

router-preference means the router's priority, which accounts for two bits in the **flags** domain in the RA message.The router's priority can be high, medium and low. The medium priority is the default settings.

Command	Purpose
ipv6 nd router-preference preference	Sets the **router-preference** field in the RA message transmitted by the local port.It is medium by default.

- Stopping a port to be the notification port of a switch

Only the notification port can transmit RA packets. The notification port supports multicast and is set to have at least one unicast IP address. Its AdvSendAdvertisment flag is TRUE in value.

The configuration of **ipv6 nd suppress-ra** in the VLAN port means shutdown the notification port. This command is not set by default.

Command	Purpose
ipv6 nd suppress-ra	Means the value of the AdvSendAdvertisment flag on the local port. 0

OSPFv3 Configuration

Table of Contents

Chapter 1 OSPFv3 Configuration 1
1.1 Overview 1
1.2 OSPFv3 Configuration Task List 2
1.3 OSPFv3 Configuration Tasks 2
1.3.1 Enabling OSPFv3 2
1.3.2 Setting the Parameters of the OSPFv3 Interface 3
1.3.3 Setting the OSPF Network Type 3
1.3.4 Setting the Parameters of the OSPFv3 Domain 4
1.3.5 Setting the Route Summary in the OSPFv3 Domain 5
1.3.6 Setting the Summary of the Forwarded Routes 5
1.3.7 Generating a Default Route 5
1.3.8 Choosing the Route ID on the Loopback Interface 5
1.3.9 Setting the Management Distance of OSPFv3 6
1.3.10 Setting the Timer of Routing Algorithm 6
1.3.11 Monitoring and Maintaining OSPFv3 6
1.4 OSPFv3 Configuration Example 7
1.4.1 Example for OSPFv3 Route Learning Settings 7

Chapter 1 OSPFv3 Configuration

1.1 Overview

OSPFv3 is an IGP routing protocol developed by the OSPF working group of IETF for the IPv6 network. OSPFv3 supports the IPv6 subnet, the mark of the external routing information and the packet's authentication.

OSPFv3 and OSPFv2 have a lot in common:

- Both router ID and area ID are 32 bit.
- The following are the same type of packets: Hello packets, DD packets, LSR packets, LSU packets and LSAck packets.
- Having the same neighbor discovery mechanism and the same neighborhood generation mechanism
- Having the same LSA expansion mechanism and the same LSA aging mechanism

The main differences of both OSPFv3 and OSPFv2 are shown below:

- OSPFv3 is running on the basis of link, while OSPFv2 is running on the basis of network segment.
- OSPFv3can run multiple instances on the same link.
- OSPFv3 labels its neighbor through router ID, while OSPFv2 labels its neighbor through IP.
- OSPFv3 defines 7 classes of LSAs.

The following table shows some key functions in the realization of the OSPFv3 functions.

Key attributes	Description
Stub domain	Supports the stub domain.
Route forwarding	Means that routes that are learned or generated by any routing protocol can be forwarded to the domains of other routing protocols.In the autonomous domain, it means that OSPFv3 can input the RIPng learned routes. The routes learned by OSPFv3 can also be exported to RIPng.Between the autonomous domains, OSPFv3 can import the BGP-learned routes; OSPFv3 routes can also be exported to the BGPs.
Parameters of a routing interface	The following are configurable interface parameters: output cost, retransmission interval, interface's transmission delay, router's priority, interval for judging the shutdown of a router, hello interval, and authentication key.
Virtual link	Supports the virtual link.

1.2 OSPFv3 Configuration Task List

OSPFv3 demands the switchover of routing data between in-domain router, ABR and ASBR. In order to simplify the settings, you can make related configuration to enable them to work under the default parameters without any authentication; if you want to change some parameters, you must guarantee that the parameters on all routers are identical.

To set OSPFv3, you must perform the following tasks. Except that the task of activating OSPFv3 is mandatory, other settings are optional.

- Enabling OSPFv3
- Setting the parameters of the OSPFv3 interface
- Setting the parameters of the OSPFv3 domain
- Configuring the NSSA Domain of OSPFv3
- Setting the Route Summary in the OSPFv3 Domain
- Setting the Summary of the Forwarded Routes
- Generating a Default Route
- Choosing the route ID on the loopback interface
- Setting the management distance of OSPFv3
- Setting the Timer of Routing Algorithm
- Monitoring and Maintaining OSPFv3

1.3 OSPFv3 Configuration Tasks

1.3.1 Enabling OSPFv3

Before OSPFv3 is enabled, the function to forward the IPv6 packets must be enabled.

Run the following commands in global configuration mode:

Command	Purpose
router ospfv3 *process-id*	Activates OSPFv3 and enters the router configuration mode.
router-id *router-id*	Sets the router ID of a router on which OSPFv3 is running.

Run the following command in interface configuration mode:

Command	Purpose

ipv6 ospf *process-id* **area** *area-id* **[instance** *instance-id***]**	Enables OSPFv3 on an interface.

Note: If the OSPFv3 process is still not created before OSPFv3 is enabled on an interface, the OSPFv3 process will be automatically created.

1.3.2 Setting the Parameters of the OSPFv3 Interface

During OSPFv3 realization, related OSPFv3 parameters on an interface are allowed to be modified according to actual requirements. Of cause you have no need to change every parameter, but you have to make sure that some parameters are consistent on all routers in the connected networks.

Run the following commands in interface configuration mode to do relevant configurations:

Command	Purpose
ipv6 ospf cost *cost*	Sets the cost of the packet that is transmitted from the OSPFv3 interface.
ipv6 ospf retransmit-interval *seconds*	Sets the LSA retransmission interval between neighbors.
ipv6 ospf transmit-delay *seconds*	Sets the delay time for transmitting LSA on an OSPFv3 interface.
ipv6 ospf priority *number*	Sets a router to be the priority of the OSPFv3 DR router.
ipv6 ospf hello-interval *seconds*	Sets the interval for the OSPFv3 interface to transmit the Hello packets.
ipv6 ospf dead-interval *seconds*	Means that in a regulated interval if the OSPFv3 packets are not received from a neighboring router, this neighboring router is viewed to be shut down.

1.3.3 Setting the OSPF Network Type

The Ethernet network can use the broadcast network type. The OSPF network type can also be configured to meet the logical topology.

To set an un-broadcast and multi-access network is to suppose that every two routers have a virtual link or suppose a full-mesh network. It is unrealistic due to unbearable cost. But you set this network to be a point-to-multipoint one. Between those routers which are not adjacent the routing information can be switched through the virtual link.

The OSPFv3 point-to-multipoint interface can be set to be multipoint-to-point interface, through which multiple routes of a host can be established. The OSPFv3 point-to-multipoint network, comparing with the non-broadcast and multi-access network or the point-to-point network, has the following advantages:

- The point-to-multipoint network is easy to be set without generating DR.
- This kind of network do not require the full-mesh topology, so the construction cost is relatively low.
- This kind of networks are more reliable. Even if its virtual link fails, the connection can be maintained.

The network type of the routers is the broadcast type.

1.3.4 Setting the Parameters of the OSPFv3 Domain

The configurable domain parameters include: authentication, designating a stub area and specifying a weight for a default summary route. Its authentication is based on password protection.

The stub area means that external routes cannot be distributed to this area. Instead, ABR generates a default external route that enters the stub area, enabling the stub area to communicate with external networks of an autonomous area. In order to make use of the attributes supported by the OSPF stub, the default route must be used in the stub area. To further reduce LSAs that are forwarded to the stub area, you can forbid the summary function on ABR.

Run the following command in router configuration mode to set the domain's parameters:

Command	Purpose
area *area-id* **stub** [no-summary]	Defines a stub area.
area *area-id* **default-cost** *cost*	Sets the weight of the default route of the stub area.

As to those areas that are not backbone areas and do not connect the backbone areas directly or as to those discontinuous areas, the OSPFv3 virtual link can be used to establish a logic connectivity. In order to create a virtual link, you have to perform configuration at the two terminals of the virtual link. If only one terminal is configured, the virtual link cannot work.

Run the following command in router configuration mode to set the domain's parameters:

Command	Purpose
area *area-id* **virtual-link** *neighbor-ID* [**dead-interval** *dead-value*][**hello-interval** *hello-value*][**retransmit-interval**	Establishes the virtual link.

retrans-value][**transmit-delay** *dly-value*]	

1.3.5 Setting the Route Summary in the OSPFv3 Domain

With this function ABR can broadcast a summary route to other areas. In OSPFv3 ABR will broadcast each network to other areas. If network IDs are distributed to be continuous, you can set ABR to broadcast a summary route to other areas. The summary route can cover all networks in a certain range.

Run the following command in router configuration mode to set the address' range:

Command	Purpose
area *area-id* **range** *ipv6-prefix /prefix-length*	Sets the address' range of the summary route.

1.3.6 Setting the Summary of the Forwarded Routes

When routes are distributed from other routing areas to the OSPFv3 routing area, each route is singularly broadcasted as an external LSA. However, you can set a route on a router to make this route cover an address range. In this way, the size of the OSPFv3 link-state database can be reduced.

Run the following command in router configuration mode to set a summary route:

Command	Purpose
summary-prefix *ipv6-prefix /prefix-length*	Broadcasts only one summary route.

1.3.7 Generating a Default Route

ASBR should generate a default route to enter the OSPFv3 routing area. Whenever it is, you make configuration to enable a router to distribute a route to the OSPFv3 routing area and this route becomes ASBR automatically. However, ASBR does not generate a default route by default to enter the OSPFv3 routing area.

1.3.8 Choosing the Route ID on the Loopback Interface

OSPFv3 uses the maximum IPv4 address as its router ID. If the interface that connects the IPv4 address is down or the IPv4 address is deleted, the OSPF process will recalculate the ID of this new router and retransmit the routing information from all interfaces.

If an IPv4 address is configured on a loopback interface, the router will first use the IPv4 address of loopback as its ID. Because the loopback interface will never be down, the routing table is greatly stable.

The router can first select the loopback interface as its ID or select the maximum IPv4 address in all loopback interfaces as its ID. If there is no loopback interface, the IPv4 address of a router will be used as the router ID. You cannot specify OSPFv3 to use any specific interface.

Run the following commands in global configuration mode to set the IP loopback interface:

Command	Purpose
interface loopback ***num***	Creates a loopback interface and enters the interface configuration mode.
ip address *ip-address mask*	Distributes an IPv4 address for an interface.

1.3.9 Setting the Management Distance of OSPFv3

The management distance means the trust level of the routing information source. Generally speaking, the management distance is an integer between 0 and 255. The bigger its value is, the lower the trust level is. If the management distance is 255, the routing information source will be distrusted and omitted.

OSPFv3 uses three different kinds of management distances: inter-domain, inner-domain and exterior. The routes in a domain are called inner-domain routes; the routes to other domains are called inter-domain routes; the routes transmitted from other routing protocols are called the exterior routes. The default value of each kind of routes is 110.

1.3.10 Setting the Timer of Routing Algorithm

You can set the delay between receiving the topology change information and calculating SPF. You can also set the interval between two continuous SFP algorithm. Run the following command in router configuration mode:

Command	Purpose
timers delay *delaytime*	Set a delay for routing algorithm in an area.
timers hold *holdtime*	Sets a minimum interval for routing algorithm in an area.

1.3.11 Monitoring and Maintaining OSPFv3

The network statistics information which can be displayed includes the content of the IP routing table, caching and database. This kind of information can help users to judge the usage of network resources and solve network problems.

You can run the following commands to display all kinds of routing statistics information:

Command	Purpose
show ipv6 ospf [*process-id*]	Displays the general information about the OSPFv3 routing process.
show ipv6 ospf [*process-id*] **database** **show ipv6 ospf** [*process-id*] **database [router] [adv-router** *router-id***]** **show ipv6 ospf** [*process-id*] **database [network] [adv-router** *router-id***]** **show ipv6 ospf** [*process-id*] **database [inter-prefix] [adv-router** *router-id***]**	Displays the information about the OSPFv3 database.

show ipv6 ospf [*process-id*] **database [inter-router] [adv-router** *router-id***]** **show ipv6 ospf** [*process-id*] **database [external] [adv-router** *router-id***]** **show ipv6 ospf** [*process-id*] **database [link] [adv-router** *router-id***]** **show ipv6 ospf** [*process-id*] **database [intra-prefix] [adv-router** *router-id***]**	
show ipv6 ospf interface	Displays the information about the OSPFv3 interface.
show ipv6 ospf neighbor	Displays the information about OSPFv3 neighbors.
show ipv6 ospf route	Displays the routing information about OSPFv3.
show ipv6 ospf topology	Displays the OSPFv3 topology.
show ipv6 ospf virtual-links	Displays the virtual links of OSPFv3.
debug ipv6 ospf	Monitors all OSPFv3 behaviors.
debug ipv6 ospf events	Monitors the OSPFv3 events.
debug ipv6 ospf ifsm	Monitors the state machine of the OSPFv3 interface.
debug ipv6 ospf lsa	Monitors related behaviors about OSPFv3 LSA.
debug ipv6 ospf nfsm	Monitors the state machine of the OSPFv3 neighbors.
debug ipv6 ospf nsm	Monitors the information of which the management module notifies OSPFv3.
debug ipv6 ospf packet	Monitors the OSPFv3 packets.
debug ipv6 ospf route	Monitors the routing information about OSPFv3.

1.4 OSPFv3 Configuration Example

1.4.1 Example for OSPFv3 Route Learning Settings

OSPFv3 requires switching information among many internal routers, ABR and ASBR. In the minimum settings, the OSPFv3-based router works under the case that all its parameters take their default values and there is no authentication.

The following are three configuration examples:

The first example shows the commands for basic OSPFv3 settings.

The second example shows multiple OSPFv3 processes can be set on a router.

The third example shows how to use OSPFv3 to learn routes.

The fourth example shows how to set the OSPFv3 virtual link.

1. Basic OSPFv3 Configuration Example

The following example shows a simple OSPFv3 settings. In this example, you have to activate process 90, connect Ethernet interface 0 to area 0.0.0.0, distribute RIPng to OSPFv3 and OSPFv3 to RIPng.

```
ipv6 unicast-routing
!
interface vlan 10
ipv6 address 2001::1/64
ipv6 enable
ipv6 rip aaa enable
ipv6 rip aaa split-horizon

ipv6 ospf 90 area 0
ipv6 ospf cost 1
!
router ospfv3 90
router-id 1.1.1.1
redistribute rip
!
router ripng aaa
redistribute ospf 90
```

2. Configuring multiple OSPFv3 processes

The following example shows that two OSPFv3 processes are created.

```
ipv6 unicast-routing
!
!
interface vlan 10
  ipv6 address 2001::1/64
   ipv6 enable

   ipv6 ospf 109 area 0 instance 1
   ipv6 ospf 110 area 0 instance 2
!
!
interface vlan 11
  ip address 2002::1/64
   ipv6 enable

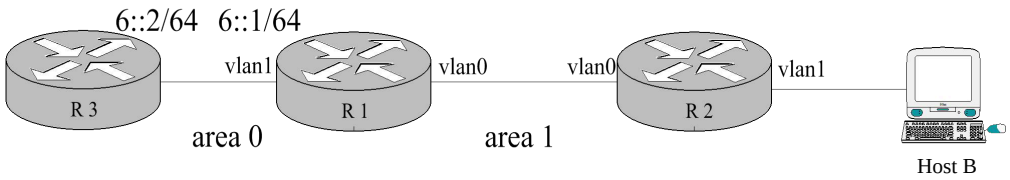
 ipv6 ospf 109 area 1 instance 1
 ipv6 ospf 110 area 1 instance 2
```

```
!
!
router ospfv3 109
  router-id 1.1.1.1
   redistribute static
!
router ospfv3 110
  router-id 2.2.2.2
!
```

Each interface can belong to many OSPFv3 processes, but if an interface belongs to multiple OSPFv3 processes each OSPFv3 process must correspond to different instances.

3. Complicated configuration example

The following example shows how to configure multiple routers in a single OSPFv3 autonomous system. The following figure shows the network topology of the configuration example:



Configure the router according to the above-mentioned figure:

R1:

```
interface vlan 0
     ipv6 enable

    ipv6 ospf 1 area 1
!
interface vlan 1
     ipv6 enable

    ipv6 ospf 1 area 0
!
ipv6 route 2001::/64 6::2
!
router ospfv3 1
   router-id 1.1.1.1
    redistribute static
!
```

```
R2:
interface vlan 0
     ipv6 enable

    ipv6 ospf 1 area 1
!
!
router ospfv3 1
   router-id 2.2.2.2
!
```

Browsing the routing table of R2:

```
R2#show ipv6 route
O          6::/64[1]
            [110,20] via fe80:4::2e0:fff:fe26:2d98(on VLAN0)
O 2001::/64[1] (forwarding route)
            [110,150] via fe80:4::2e0:fff:fe26:2d98(on VLAN0)
C          fe80::/10[1]
            is directly connected, L,Null0
C          fe80::/64[1]
            is directly connected, C, VLAN0
C          fe80::2e0:fff:fe26:a8/128[1]
            is directly connected, L, VLAN0
C          ff00::/8[1]
            is directly connected, L,Null0
```

From the command sentences above, we can see that R2 has learned route forwarding.

Setting area 1 to be the stub area:

```
R1:
interface vlan 0
     ipv6 enable

    ipv6 ospf 1 area 1
!
interface vlan 1
     ipv6 enable

    ipv6 ospf 1 area 0
!
ipv6 route 2001::/64 6::2
!
router ospfv3 1
   router-id 1.1.1.1
   area 1 stub
    redistribute static
!
```

```
R2:
interface vlan 0
     ipv6 enable

    ipv6 ospf 1 area 1
!
!
router ospfv3 1
   router-id 2.2.2.2
   area 1 stub
!
```

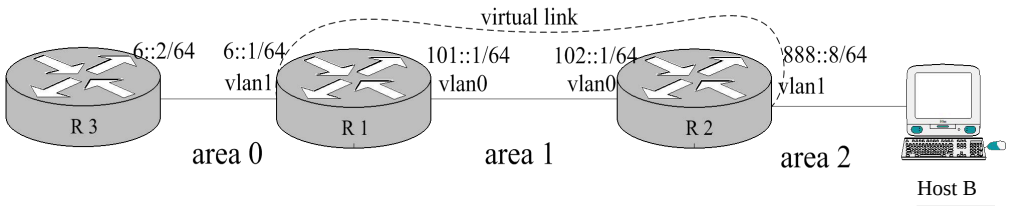
Browsing the routing table of R2:

```
R2#show ipv6 route
O       ::/0[1]
         [110,11] via fe80:4::2e0:fff:fe26:2d98(on VLAN0)
O       6::/64[1]
         [110,20] via fe80:4::2e0:fff:fe26:2d98(on VLAN0)
C       fe80::/10[1]
         is directly connected, L,Null0
C       fe80::/64[1]
         is directly connected, C, VLAN0
C       fe80::2e0:fff:fe26:a8/128[1]
         is directly connected, L, VLAN0
C       ff00::/8[1]
         is directly connected, L,Null0
```

It can be judged that ABR in the stub area can generate a default route normally and notify other routers in this area without importing ASE LSA into the stub area.

4. Configuring the virtual link

The following example shows how to configure a virtual link in a single autonomous OSPFv3 system. The following figure shows the network topology of the configuration example:



Configure the router according to the above-mentioned figure:

```
R1:
interface vlan 0
    ipv6 address 101::1/64
    ipv6 enable

    ipv6 ospf 1 area 1
!
interface vlan 1
    ipv6 address 6::1/64
    ipv6 enable

    ipv6 ospf 1 area 0
!
ipv6 route 2001::/64 6::2
!
router ospfv3 1
  router-id 200.200.200.1
  area 1 virtual-link 200.200.200.2
  redistribute static
!

R2:
interface vlan 0
    ipv6 address 101::2/64
    ipv6 enable

    ipv6 ospf 1 area 1
!
interface vlan 1
    ipv6 address 888::8/64
    ipv6 enable

    ipv6 ospf 1 area 2
!
!
router ospfv3 1
 router-id 200.200.200.2
 area 1 virtual-link 200.200.200.1
!
```

Browsing the state of the OSPFv3 neighbor:

```
R1#show ipv6 ospf neighbor
OSPFv3 Process (1)
Neighbor ID      Pri    State           Dead Time    Interface    Instance ID
200.200.200.2      1    Full/DR         00:00:35     VLAN0          0
200.200.200.2      1    Full/ -         00:00:36     VLINK1         0
```

```
R2#show ipv6 ospf neighbor
OSPFv3 Process (1)
OSPFv3 Process (1)
Neighbor ID     Pri   State           Dead Time   Interface   Instance ID
200.200.200.1     1   Full/Backup      00:00:36    VLAN0       0
200.200.200.1     1   Full/ -          00:00:37    VLINK1      0
```

Browsing the information in the routing table:

```
R1#show ipv6 route
C       6::/64[1]
         is directly connected, C,VLAN1
C       6::1/128[1]
         is directly connected, L, VLAN1
C       101::/64[2]
         is directly connected, C, VLAN0
C       101::1/128[2]
         is directly connected, L, VLAN0
O       101::2/128[2]
         [110,10] via fe80:4::2e0:fff:fe26:a8(on VLAN0)
O       888::/64[2]
         [110,20] via fe80:4::2e0:fff:fe26:a8(on VLAN0)
S       2001::/64[1]
         [1,0] via 6::2(on VLAN1)
C       fe80::/10[2]
         is directly connected, L,Null0
C       fe80::/64[2]
         is directly connected, C, VLAN0
C       fe80::2e0:fff:fe26:2d98/128[2]
         is directly connected, L, VLAN0
C       fe80::/64[1]
         is directly connected, C, VLAN1
C       fe80::2e0:fff:fe26:2d99/128[1]
         is directly connected, L, VLAN1
C       ff00::/8[2]
         is directly connected, L,Null0

R2#show ipv6 route
O       6::/64[1]
         [110,20] via fe80:4::2e0:fff:fe26:2d98(on VLAN0)
C       101::/64[1]
         is directly connected, C, VLAN0
O       101::1/128[1]
         [110,10] via fe80:4::2e0:fff:fe26:2d98(on VLAN0)
C       101::2/128[1]
         is directly connected, L, VLAN0
C       888::/64[1]
```

```
          is directly connected, C, VLAN1
C         888::8/128[1]
          is directly connected, L, VLAN1
O         2001::/64[1]
          [110,150] via fe80:4::2e0:fff:fe26:2d98(on VLAN0)
C         fe80::/10[1]
          is directly connected, L,Null0
C         fe80::/64[1]
          is directly connected, C, VLAN0
C         fe80::2e0:fff:fe26:a8/128[1]
          is directly connected, L, VLAN0
C         fe80::/64[1]
          is directly connected, C, VLAN1
C         fe80::2e0:fff:fe26:a9/128[1]
          is directly connected, L, VLAN1
C         ff00::/8[1]
          is directly connected, L,Null0
```

NTP Configuration

Table of Contents

Chapter 1 Overview 1
1.1 Stipulation 1
1.1.1Format Stipulation in the Command Line 1
Chapter 2 NTP Configuration 2
2.1 Overview 2
1.2 NTP Configuration 2
2.2.1 Configuring the Equipment As an NTP Server 2
2.2.2 Configuring NTP Authentication Function 2
2.2.3 Configuring NTP Association 3

Chapter 1 Overview

1.1 Stipulation

1.1.1Format Stipulation in the Command Line

Syntax	Meaning
Bold	Stands for the keyword in the command line, which stays unchanged and must be entered without any modification. It is presented as a bold in the command line.
{italic}	Stands for the parameter in the command line, which must be replaced by the actual value. It must be presented by the italic in the brace.
<*italic*>	Stands for the parameter in the command line, which must be replaced by the actual value. It must be presented by the italic in the point bracket.
[ ]	Stands for the optional parameter, which is in the square bracket.
{ x | y | ... }	Means that you can choose one option from two or more options.
[x | y | ...]	Means that you can choose one option or none from two or more options.
{ x | y | ... } *	Means that you has to choose at least one option from two or more options, or even choose all options.
[x | y | ...] *	Means that you can choose multiple options or none from two or more options.
&<1-n> Means that the parameter before the ·&· symbol can be entered 1~n times.	
#	Means that the line starting with the “#” symbol is an explanation line.

Chapter 2 NTP Configuration

2.1 Overview

Network Time Protocol (NTP) is a type of computer time synchronization protocol which can be used for time synchronization between distributed time servers and clients. It has highly accurate time correction function and can prevent malicious protocol attacks through encrypted authentication. Clients and servers communicate through the User Datagram Protocol (UDP), and the port number is 123.

1.2 NTP Configuration

2.2.1 Configuring the Equipment As an NTP Server

Configuration mode: Global

Command	Purpose
ntp master primary	In the event that the equipment does not have an upper-level NTP server, configure the equipment as the original NTP server (stratum = 1).
ntp master secondary	In the event that the equipment has an upper-level NTP server, configure the equipment as the secondary NTP server. (In other words, the equipment cannot provide time synchronization service for NTP clients unless the "ntp server" command is configured and time synchronization is achieved in designated servers.)

2.2.2 Configuring NTP Authentication Function

Configuration mode: Global

Command	Purpose
ntp authentication enable	Enable the authentication function (disabled by default).
ntp authentication key *keyid* **md5** *password*	Configure NTP md5 authentication keyid and corresponding keys.
ntp authentication trusted-key *keyid*	Configure the keyid corresponding key as the trusted key.

2.2.3 Configuring NTP Association

Configuration mode: Global

Command	Purpose
ntp server *ip-address* [**version** *number* | **key** *keyed* | **vrf** *vrf-name*]*	Configure the IP address of NTP server; the version number, key number, and vrf instance can be designated.
ntp peer *ip-address* [**version** *number* | **key** *keyid* | **vrf** *vrf-name*]*	Configure the IP address of equipment NTP peer; the version number, key number, and vrf instance can be designated.

Usage Guidelines:

1. Equipment can provide time services for NTP clients provided that the equipment has achieved time synchronization; otherwise the client device that employs the equipment as its server cannot achieve time synchronization.

2. To conduct NTP authentication, both parties must open the NTP authentication function simultaneously, configure the same keyid and key, and designate the keyid as trusted; otherwise time synchronization would fail.

IPv6 ACL Configuration

Table of Contents

Chapter 1 IPv6 ACL Configuration....1
1.1 IPv6 ACL Configuration....1
1.1.1 Filtering IPv6 Packets....1
1.1.2 Setting up IPv6 ACL....1
1.1.3 Applying ACL to the Ports....2
1.1.4 Examples of IPv6 ACL....2

Chapter 1 IPv6 ACL Configuration

1.1 IPv6 ACL Configuration

1.1.1 Filtering IPv6 Packets

Filtering IPv6 packets helps the control packet run in the network. Such control can limit network transmission and network running by a certain user or device. For enabling or disabling packets from the cross designated port, we provide with ACL. You can use IPv6 ACL as follows:

- Limit of packet transmission on the port
- Limit of virtual terminal line access
- Limit of the route update

This chapter summarizes how to set up IPv6 ACL and how to apply them.

IPv6 ACL is a well-organized set which applies enable/disable of IPv6 address. ROS of the switch will test addresses in ACL accordingly. The first match determines whether the software accept or refuse the address. Because after the first match, the software will stop the match rule, the sequence of the condition is important. If there is no rule to match, the address will be refused.

Steps for using ACL:

(1) Set up ACL by designating ACL name and ACL conditions.

(2) Apply ACL to the port.

1.1.2 Setting up IPv6 ACL

Use a character string to set up IPv6 ACL.

Note:

The standard ACL and the expanded ACL cannot be the same.

In order to set up IPv6 ACL, run the following command in the global configuration mode.

Command	Purpose
IPv6 access-list *name*	Use the name to define an IPv6 ACL.
{**deny** | **permit**} *protocol* {*source-ipv6-prefix*|*prefix-length* | **any** | **host** *source-ipv6-address*} [*operator* [*port-number*]]	In the configuration mode of IPv6 ACL, designate one or multiple enable/disable conditions. This determines whether to pass

{*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address*} [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**routing**] [**sequence** *value*] [**time-range** *name*]	the packet or not. (dscp is used for matching IPv6 grouping header Traffic Class domain, flow-label is used for matching Flow Label tag domain of IPv6 grouping header, fragments is used for matching fragment grouping when the grouping expansion header includes none-0 offset; log means whether to record log, routing is used for the source grouping of the route expansion header of IPv6 grouping header, time-range is used for limit the time range of ACL.)
Exit	Exit from the configuration mode of ACL.

After setting up ACL, any additional parts will be affiliated to the end of the ACL if no sequence is added to the rule deny or permit. In other words, add [**sequence** value] in the front or back of the rule deny/permit, you can add ACL commands in any position of the designated ACL.

Likewise, you can use “no permit” and “no deny” to delete an item in ACL or “no sequence” to delete the rule in a certain position directly.

Note:

When setting up ACL, please remember the end sentence of ACL by default covers the sentence of **deny ipv6 any any.**

The ACL must be applied to the line or port after being set up. Refer to the description of “Apply the ACL to the port”.

1.1.3 Applying ACL to the Ports

ACL can be applied to one or multiple ports or the ingress.

Run this command in the configuration mode.

Command	Purpose
IPv6 access-group *name*	Apply ACL to the port.

For the standard ingress ACL, check the source address of the packet after receiving it. For the expanded ACL, the routing switch also checks the objective address. If the ACL enables the address, the software continues to handle the packet. If ACL does not allow the address, the software will drop the packet and returns one ICMP host unreachable packets.

If there is no designated ACL, all packets will be allowed to pass.

1.1.4 Examples of IPv6 ACL

In the following example, please first enable to connect with the individual destination host of the host A:B:C:D::E and disable the new TCP to connect with SMTP port whose host IPv6 source prefix 255:255:255::/48. The next rule sequence of the final ACL comes before the former rule.

```
Switch_config#ipv6 access-list xxcom
Switch_config_ipv6acl#permit any host A:B:C:D::E sequence 20
Switch_config_ipv6acl#deny tcp any 255:255:255::/48 eq 25 sequence 10
Switch_config_ipv6acl#ex
Switch_config#show ipv6 access-lists xxcom
ipv6 access-list xxcom
    deny tcp any 255:255:255::/48 eq smtp sequence 10
    permit ipv6 any host A:B:C:D::E sequence 20
```

Time Range Configuration

Table of Contents

Chapter 1 Configuring Time Range....1
1.1 Time Range Introduction....1
1.1.1 Overview....1
1.1.2 Absolute Time Range....1
1.1.3 Periodic Time Range....1
1.1.4 Isolating Time Range....1
1.1.5 From-to Time Range....1
1.1.6 Activating Time Range....2
1.2 Time Range Configuration Task List....2
1.3 Time Range Configuration Task....2
1.3.1 Adding/Deleting Time Range....2
1.3.2 Adding/Deleting Absolute Time Range....3
1.3.2 Adding/Deleting Periodic Time Range....3
1.3.4 Applying Time Range....4
1.3.5 Monitoring the configuration and state of Time Range....4
1.4 Configuration Example....5

Chapter 1 Configuring Time Range

1.1 Time Range Introduction

1.1.1 Overview

Time Range is a time module controlling the effective time and the failure time of a function (For instance, expansion IP access control list).

Time Range can play its role only when cooperating with other modules which support the Time Range function.

Time Range is consisted of separate time ranges. These time ranges have two kinds: one is absolute and the other is periodic. Of these, periodic is classified into two kinds further: isolate and from-to.

The whole system has many Time Ranges. Each Time Range is differentiated according to their names(case sensitive). Each Time Range has at most only one absolute time range but many periodic time ranges.

1.1.2 Absolute Time Range

Absolute Time Range is a time range starting and ending with concrete date and time (The Absolute Time Range without concrete starting date and time is taken as the current time; the absolute time range without concrete ending time is taken as effective forever.). For example, 08:08 8 8 2008 - 10:10 10 10 2010 is an absolute time range.

1.1.3 Periodic Time Range

Periodic Time Range is a back-and-forth time range. It has no concrete starting time and ending time, but it has concrete starting week and moment and ending date and moment. For example, a periodic time range starts from 20:00~21:00 on every Tuesday, Thursday and Sunday; or starts from 09:00 on every Tuesday to 18:00 on every Thursday. More examples such as 09:00~10:00 in every weekend; 23:00~07:00 everyday; and 09:00~18:00 on weekdays.

1.1.4 Isolating Time Range

Isolate Time Range is one type of Periodic Time Range. It is periodical. And its starting time and ending time will not span 24 hours. For example,19:00~19:30 on every Monday is an isolate time range; 20:00~21:00 on every Tuesday, Thursday and Sunday is an isolate time range; but time from 09:00 on Tuesday to 18:00 on every Thursday is not an isolate time range, but "from-to time range" described below.

1.1.5 From-to Time Range

From-to Time Range is also a type of Periodic Time Range. It is periodical. Moreover, its starting time and ending time must span at least 24 hours. For example, time from 09:00 on Tuesday to 18:00 on every Thursday is a from-to time range.

1.1.6 Activating Time Range

A Time Range can have the absolute time range and periodic time range simultaneously. The state of Time Range can be divided into 4 situations according to whether the absolute time range/periodic time range is configured.

Situation 1

If a Time Range neither configure absolute time range nor periodic time range, it is called EMPTY. The Time Range does not exist activating time range.

Situation 2

If a Time Range doesn't have the absolute time but has periodic time range, the activating time range of the Time Range is the total time ranges of the periodic time range.

Situation 3

If a Time Range doesn't have the periodic time but has absolute time range, the activating time range of the Time Range is the total time ranges of the absolute time range.

Situation 4

If a Time Range neither have the periodic time nor the absolute time range, the activating time range of the Time Range is set intersection of the set union of the absolute time range and all periodic time range.

The complementary set of the activating time range of a Time Range is considered as non-activating time range.

If the system time is in an activating time range of a Time Range, the Time Range is active; if a Time Range has the activating time range but the system time does not in the activating range, the time range is inactive; if a Time Range does not have the activating time range, the Time Range is empty.

When a Time Range changes among inactive, active and empty, the Time Range is changed. Otherwise, the Time Range is unchanged.

1.2 Time Range Configuration Task List

- Adding/ing Time Range
- Adding/Deleting Absolute Time Range
- Adding/ing Periodic Time Range
- Applying Time Range
- Monitoring the configuration and state of Time Range

1.3 Time Range Configuration Task

1.3.1 Adding/Deleting Time Range

The whole system has many Time Ranges. Each Time Range is differentiated according to their names (case sensitive).

Run the following commands to configure Time Range:

Command	Purpose
time-range *name*	Add a Time Range named name and enter the configuration mode of Time Range
exit	Exit the configuration mode of Time Range
no time-range *name*	Delete Time Range named name

Note:

1. If the system has Time Range named name, *run command* time-range name to enter the **TimeRange** *configuration mode,* but not create the new TimeRange.

1.3.2 Adding/Deleting Absolute Time Range

Each TimeRange has only at most only one absolute time range. Absolute Time Range can have the starting time and the ending time simultaneously or it has the ending time but not the starting time, or it has the starting time but not the ending time. When the absolute time has no starting time, the current time is the starting time; when the absolute time has no ending time, the absolute time is effective forever.

To configure the absolute time range, run the following command:

Command	Purpose
absolute { **start** *hour:minute day month year* **end** *hour:minute day month year* **| start** *hour:minute day month year* **| end** *hour:minute day month year* **}**	Adds an absolute time range
no absolute	Deletes the absolute time range

Note:

1. If a Time Range has the absolute time range, the absolute command modifies the absolute time range.

1.3.2 Adding/Deleting Periodic Time Range

A Time Range can has many periodic time ranges. Each periodic time range is not all the same, but the time range can overlap.

To configure the periodic time, run the following command:

Command	Purpose
periodic { **daily** *hour:minute* **to** *hour:minute* **| weekdays** *hour:minute* **to** *hour:minute* **| weekend** *hour:minute* **to** *hour:minute* **| {Friday | Monday | Saturday | Sunday | Thursday |Tuesday|Wednesday}** *hour:minute* **to** *hour:minute*	Adds a periodic time range

| {Friday | Monday | Saturday | Sunday | Thursday | Tuesday | Wednesday} *hour:minute* **to {Friday | Monday | Saturday | Sunday | Thursday | Tuesday | Wednesday}** *hour:minute* **}**	
no periodic [**daily** *hour:minute* **to** *hour:minute* **| weekdays** *hour:minute* **to** *hour:minute* **| weekend** *hour:minute* **to** *hour:minute* **| {Friday | Monday | Saturday | Sunday | Thursday |Tuesday|Wednesday}** *hour:minute* **to** *hour:minute* **| {Friday | Monday | Saturday | Sunday | Thursday | Tuesday | Wednesday}** *hour:minute* **to {Friday | Monday | Saturday | Sunday | Thursday | Tuesday | Wednesday}** *hour:minute* **]**	Deletes a periodic time range

1.3.4 Applying Time Range

A created Time Range can be applied to one or more function modules. At present the Time Range can only be applied to IP ACL function module.

In order to apply Time Range to IP ACL, you must enter the name of Time Range to the end of the sub-command of time-range.

Note:

1. Time Range can only be applied to extensible ACL, but not to the standard ACL.

1.3.5 Monitoring the configuration and state of Time Range

To monitor Time Range Configuration, run the following command:

Command	Purpose
show time-range	Shows the configuration of all Time Range in the system
show time-range *name*	Shows the configuration *of* Time Range named name.

Attach: The result analysis of the command

Take the result of the typical configuration as an example:

```
Switch_config#show time-range

Now: Date: 2016.3.4        Time: 13:16        Day: Tuesday

time-range entry: x (inactive)
        absolute start 12:00 1 January 2008 end 13:00 2 January 2016
        periodic weekdays    09:00 to 18:00
time-range entry: y (empty)
time-range entry: z (active)
        periodic daily        12:00 to 13:00
        periodic Monday       Thursday    Friday       08:00 to 09:00
        periodic Saturday     15:00 to Sunday       20:00
        periodic daily        9:00 AM to 6:00 PM

Switch_config#
```

In the first line shows “Now: Date: 2016.3.4 Time: 13:16 Day: Tuesday”, which means the date is 4th March, 2016; the time is 13:16; the day is Tuesday.

Subsequently the screen shows the configuration and status of Time Ranges which named x, y and z respectively. Time Range x has two items: absolute time and period, and it is in the inactive state; Time Range y has no item and it is in the empty state; Time Range z has 4 periods and it is in active state.

1.4 Configuration Example

The following example shows how to apply a Time Range named sample to a rule of extensible IP ACL ex.

Switch_config# **time-range** *sample*
Switch_config_tr# **periodic monday** *12:00* **to** *13:00*
Switch_config_tr# **exit**
Switch_config# **ip access-list extended** *ex*
Switch_config_ext#
Switch_config_ext# **permit ip** *192.168.213.180 255.255.255.255* **any time-range** *sample*
Switch_config_extl# **exit**

uRPF Configuration

Table of Contents

Chapter 1 uRPF Configuration 1
1.1 Overview of uRPF 1
1.1.1 uRPF(Unicast Reverse Path Forwarding) 1
1.2 uRPF Configuration 1
1.2.1 Enabling uRPF in the Global Configuration Mode 1
1.2.2 Configuring uRPF Check Mode on the VLAN Interface 1

Chapter 1 uRPF Configuration

1.1 Overview of uRPF

1.1.1 uRPF(Unicast Reverse Path Forwarding)

uRPF (Unicast reverse path forwarding) is a mechanism for allowing devices to check if the source address is in the local routing table before forwarding it. This is useful to check for source address spoofing and protecting against DOS attacks.

There are two modes of uRPF strict and loose mode. Strict mode checks that the source address has a routing table entry and that the egress interface for the route is the same as the interface the packet was received on. Loose mode only checks that a route is in the table before forwarding the packet.

1.2 uRPF Configuration

1.2.1 Enabling uRPF in the Global Configuration Mode

To use uRPF,enable uRPF in the global configuration mode:

Command	Purpose
[no] urpf check	Enable/disable uRPF check in the global configuration mode

1.2.2 Configuring uRPF Check Mode on the VLAN Interface

Configure uRPF check mode on the VLAN interface (strict mode or loose mode). In the strict mode, the source address of the packet will be used not only to check whether FIB table is reachable, but also to check whether the ingress port of the packet is consistent with the next hop interface. In the loose mode, the source address of the packet will only be used to check whether it is reachable in FIB table.

After configuring uRPF,the filter of the route is also supported. When the default route is configured and uRPF check the source address based on FIB table, all source addresses can find the matched item.By default, if the finding of uRPF check FIB is the default route, it will be taken as no entry found and the packets will be dropped.

Note:

Enable urpf check in the global configuration mode and uRPF takes effect.

Configure uRPF mode in the VLAN interface and run the command in the interface configuration mode:

Command	Purpose

[no] urpf check *strict/loose [uncheck-default-route]*	Configure uRPF check mode in the VLAN interface. uncheck-default-route is disabled by default.

Note:

Enable **uncheck-default-route**. If the packet source address can check the matched item in the FIB table, the matched item whether it is the default route or not will be taken as pass and the packet will not be dropped. By default (uncheck-default-route is disabled), the packet source address finds the matched item in FIB table and if the matched item is taken as the default route, thus uRPF is failed and the packet will be dropped.