IES3100 Series Switches Command Line Interface Reference Guide

Models: IES3100-8TF;IES3100-8TF-P

CLI REFERENCE GUIDE

Contents

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
- Canceling 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 bottom to top and the order from left to right, starting from 1. If only one port exists, the port number is 1.

Note:

The ports of various modules are numbered in the order from bottom to top and the order 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 monitor mode	Enter **Ctrl-p** when open the power.	monitor#	Run **quit**.
User mode	Log in.	Switch>	Run **exit** or **quit**.
Configuration mode	Enter **enter** or **enable** command in User mode.	Switch#	Run **exit** or **quit**.
Global configuration mode	Enter **configure terminal** in global configuration mode.	Switch_config#	Run **exit** or **quit** or **Ctrl-z** to back to the configuration mode
Port configuration mode	Enter the **interface** command in global configuration mode, such as **interface f0/1**.	Switch_config_f0/1#	Run **exit** or **quit** or **Ctrl-z** to back to the configuration 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.

Following is the example.

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 below:

no ip routing

1.6 Saving a Command

If you need to save the configuration, you can use write command to save the configuration under the global configuration mode or the configuration mode. Then It can restore the configuration fast after the system reboot or power failure.

Chapter 2 Basic Configuration Commands

2.1 System Management Commands

2.1.1 Configuring File Management Commands

File System Management

File names in FLASH can only have 20 characters at most, and not case-sensitive.

File System Commands

All commands in boldface are keywords and the rest are parameters. The part of [] is optional.

Command	Purpose
format	Format the file system, and delete all data.
dir[filename]	Display filename and directory name. Filenames in [] indicate to display the file named begin with these letters. The file is displayed in the following format: Index filename <FILE> length of the file created time
delete filename	Delete a file. If the file is not exist, prompt that the file is not exist.
md dirname	Create a directory
rd dirname	Delete a directory. If the directory is not existed, prompt that the directory is not existed.
more filename	Display the content of a file.
cd	Change the current file system path.
pwd	Display the current path.

File System Commands

monitor#boot flash <local_filename>

This command is used to start the switch software in FLASH. There may be multiple switch software in FLASH.

Parameters

Parameter	Description

flash	The file is saved in FLASH.
local_filename	The filename saved in FLASH. The users must enter the filename.

Example

monitor#boot flash switch.bin

Software Update

The user can use this command to download the switch system software locally or remotely for a version upgrade or a special feature version (such as data encryption) that you have customized to the company.

There are two ways to update the software in monitoring state.

1）Use TFTP protocol

monitor#copy tftp flash [ip_addr]

This command is used to copy the file from the tftp server to the system's FLASH. After the user entering the command, the system will prompt the user to enter the remote server name and remote file name.

Parameters

Parameter	Description
Flash:	The file is saved in FLASH.
Ip_addr	IP address of the TFTP server. If it is not specified, it will prompt the user to enter after running copy command.

Example

Read the file named "main.bin" from the server, then write to the switch and named "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#

2.1.2 Basic System Management Configuration

Configuration Update

The configuration of the switch is saved as a file with the file name startup-config. The user can update the configuration using commands similar to software updates.

1）Use TFTP protocol

monitor#copy tftp flash startup-config

Use ftp to update the Software and Configuration

config #copy ftp flash [ip_addr|option]

In the formal program, it can also use ftp to update software and configuration under the management state. Use the copy command to download files from the ftp server to the switch, or you can upload a file from the switch file system to the ftp server. After the user entering the command, the system will prompt the user for the remote server name and the remote file name.

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

Parameters

Parameter	Description
login-name	The username of the file server. If it is not specified, it will prompt the user to enter after running copy command.
login-password	Password of the file server. If it is not specified, it will prompt the user to enter after running copy command.
nchecksize	Don't detect the size of the file on the server.
vrf	Provide vrf binding for MPLS–enabled device.
blksize	Data transfer block size (the default value is 512.)
Ip-addr	IP address of the ftp server. If it is not specified, it will prompt the user to enter after running copy command.
active	Specify to connect the ftp server using active method.

passive	Specify to connect the ftp server using passive method.
type	Set the type of the transmission data (ascii or Binary)

Example

Download the file "main.bin" from the server, then write it to the switch and named "switch.bin".

config#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 config#copy ftp://login-nam:login-password@192.168.20.1/main.bin flash:switch.bin

##
##

FTP:successfully receive 3377 blocks ,1728902 bytes

config#

Note:

1) When the ftp server cannot be access and the waiting time is too long due to the tcp time-out(the default value is 75s), the tcp connecting time can be changed by setting the global command ip tcp synwait-time. But it is not suggested.

2) When using ftp in some network condition which may exist the slow data transfer situation, please adjust the size of the transport block to get the best results. The default size of 512 bytes, it can achieve high operational efficiency in the most networks.

Configure Ethernet IP Address

monitor#ip address <ip_addr> <net_mask>

This command is used to configure Ethernet IP address. The default value is 192.168.1.1. and the Netmask is 255.255.255.0.

Parameters

Parameter	Description
ip_addr	Ethernet IP address.
net_mask	Ethernet Netmask.

Example

monitor#ip address 192.168.1.1 255.255.255.0

Configure Default Route

monitor#ip route default <*ip_addr*>

This command is used to configure the default route. And it can only configure 1 default route.

Parameters

Parameter	Description
ip_addr	IP address of the gateway.

Example

monitor#ip route default 192.168.1.1

Test the Network Connection by PING

monitor#ping <ip_address>

This command is used to test the condition of the network connection.

Parameters

Parameter	Description
ip_addr	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

2.1.3 HTTP Configuration

- Enable http service
- Change the port number of the http service
- Configure the password of the http service

- Specify the access control list for http service

1) Enable http service

By default, http service is disabled.

Use the following command to enable http service under the global configuration mode.

Command	Purpose
Ip http server	Enable http service

2) Change the port number of the http service

By default, the monitoring port number of http service is 80.

Use the following command to change the port number of the http service under the global configuration mode.

Command	Purpose
Ip http port number	Enable http service

3) Configure the password of the http service

http uses enable password as the access password. If you want to authenticate http access, you need to set the enable password. Use the following command to configure the enable password in the global configuration mode:

Command	Purpose
Enable password {0|7} line	Configure enable password.

4) Specify the access control list for http service

To control the host access http service, specify the access control list for http service. Use the following command to specify the access control list for http service.

Command	Purpose
ip http access-class STRING	specify the access control list for http service

HTTP Configuration Example

Following uses the default port(80) as http service port, and are only allowed to access from 192.168.20.0/24:

ip acl configuration:

ip access-list standard http-acl

permit 192.168.20.0 255.255.255.0

global configuration:

ip http access-class http-acl

ip http server

2.2 Configure the Terminal

2.2.1 VTY Configuration Description

Use **line** command to configure parameters of terminal simply and flexibly, and the configuration process is suitable for the using habit of customers. The displayed width and height of the terminal can be set by the **line** command.

2.2.2 Configuration Task

There are 4 types of lines: console, auxiliary, asynchronous and virtual terminal lines. Different systems have different numbers of these lines. Refer to the following software and hardware configuration guide for proper configuration of the device.

Line type	Interface	Description	Number rule
CON(CTY)	Console	Used to login the system to run configure service.	Number 0
VTY	Virtual asynchronous	Used to connect Telnet、X.25 PAD、HTTP and Rlogin of the sync port in the system[like Ethernet or Serial interface]	Number 1~32 from beginning

Relationships between the line and the interface

1) Relationship between Sync interface and VTY line

Virtual terminal lines provide access to the system through a synchronous interface. When a user connects to the system through a VTY line, the user is connecting to a virtual port on an interface. There can be multiple virtual ports for each synchronization interface.

For example, several Telnet connect to 1 interface [Ethernet or serial interface].

The VTY configuration needs to do the following:

1) Enter the row configuration mode.

2) Configure the terminal parameters.

Refer to the "VTY Configuration Example" section below for the configuration of VTY.

2.2.3 Monitoring and Maintenance

Use **show line** to check the configuration of VTY.

2.2.4 VTY Configuration Example

Following configurations will cancel the output line limit per screen of all VTY, and more tips will not be prompted:

config#line vty 0 32

config_line#length 0

2.3 Network Management Configuration

2.3.1 Configure SNMP

Overview

SNMP system includes the following 3 parts:

- SNMP management side (NMS)
- SNMP Agent (AGENT)
- Management Information Base (MIB)

SNMP is the application layer protocol. It provides a message format for communication between the SNMP management side and the agent.

The SNMP management side can be part of the network management system (NMS, such as CiscoWorks). Agents and MIBs reside on the system. To configure SNMP on the system, you need to define the relationship between the management and the agent.

The SNMP agent contains MIB variables that the SNMP management can query or change the value of these variables. The management side can get the value of the variable from the agent, or store the variable value at the agent. The agent collects data from the MIB. The MIB is a repository of device parameters and network data. Agents can also respond to requests from the management side to read or set data. The SNMP agent can actively send traps to the management side. A trap is a message that alerts the SNMP management side to a condition of the network. Traps can indicate incorrect user authentication, reboot, link status (start or shutdown), TCP connection shutdown, loss of connection to neighboring systems, or other important events.

1) SNMP Notice

When a special event occurs, the system can send an inform to the SNMP management side. For example, when the proxy system encounters an error condition, it may send a message to the management side.

SNMP notice can be sent as traps or inform requests. The receiver receives a trap without any response, and then the sender cannot determine whether the trap has been received, so the trap is unreliable. In contrast, the SNMP management side receiving the inform request uses the SNMP response PDU as the response of the message. If the management does not receive a inform request, it will not send the response. If the sender does not receive the reply, the inform request can be sent again. In this way, the notice is more likely to reach the destination.

Because the inform requests are more reliable, they consume more resources of the system and the network. Traps are discarded as soon as they are issued. In contrast to this, the inform request must remain in memory until a response is received or the request timed out. In

addition, the trap can only be sent once, and the inform request can be sent again multiple times. Resend the inform request will increase the network traffic and the load on the network. Thus, traps and inform requests provide a balance between reliability and resources. If the SNMP management need to receive each notice, the inform request can be used; traps can be used if you care about the network traffic or the system's memory and do not have to receive each notification.

Our company's system currently supports traps, and provides an extension of the notification request.

2) SNMP Version

Our company's system support the following SNMP version

- SNMPv1- Simple Network Management Protocol, a complete Internet Standard, defined in RFC1157.
- SNMPv2's community-based management framework, Internet Test Protocol, defined in RFC1901.

Our 3-layer switches also can support following SNMP:

- SNMPv3- Simple Network Management Protocol Version 3, defined in RFC1157.

SNMPv1 uses community-based security. The management group that can access the proxy MIB is defined with an IP address access control list and password.

SNMPv3 can provide authentication and encryption operation for SNMP packets to ensure the safe access to the device.

SNMPv3 provides the following security features:

- Integrity of the Message: Ensure that the message in the transmission process has not been tampered with.
- Authentication: To ensure the legitimacy of the source of the message
- Encryption: Encrypts the message, unauthenticated hosts cannot decrypt even if they got the message.

SNMPv3 provides security models and security levels. A security model is an authentication policy that is implemented by configuring the user name and the group of the user. The security level refers to the different authentication modes supported in the security model. SNMPv3 user-based security model supports three security levels, and in the order from high to low, respectively, is the authentication and encryption, authentication without encryption and not certified. Transfer the summary value of the authentication key which is calculated by MD5 or SHA hash algorithm in the network, and compare them in the SNMP engine to ensure that the password is not released. Use DES encryption algorithm to ensure that the device is not eavesdropped by a third party. The administrator can authenticate the device by configuring the user / password pair and the group where the user belongs to. The access to MIB for different operation of the user can be determined by configuring the group and the view. The group also limits the minimum number of users in the group Security Level.

The agent SNMP must be configured to the SNMP version supported by the management workstation. The agent can communicate with multiple management terminals.

3) Supported MIB

SNMP of the system supports all MIB II variables (described in RFC 1213) and SNMP traps (described in RFC 1215).

Our company supports the private MIB expansion for each system.

SNMP Configuration Task

SNMP configuration task:

- Configure SNMP View

- Create or modify access control for SNMP communities
- Set the system administrator's contact method and the system location
- Define the max length of the SNMP agent packet
- Monitor SNMP status
- Configure SNMP traps

1) Configure SNMP View

The SNMP view is used to specify access to the MIB: include and exclude. Use the following command to configure the SNMP view.

Line type	Description
snmp-server view name oid] [exclude | include]	Add the MIB leaf or table specified by oid to the SNMP view name and specify the access for the object identifier specified by oid in the SNMP view name, exclude to deny access, include to allow access

A subset that can be accessed in the SNMP view removes all objects that are denied access for all MIB objects that are configured to allow access; the object which is not configured cannot be accessed by default.

After you configure the SNMP view, you can apply the SNMP view to the SNMP community name configuration to limit the subset of accessible objects for that community name.

2) Create or modify access control for SNMP communities

Use the SNMP community string to define the relationship between the SNMP management and the agent. The community string is similar to the password which is used to allow the access to the system agent. Optionally, you can specify one or more of the following attributes associated with a community string:

Allow the use of community strings to obtain proxy access to the SNMP manager's IP address access list.

Define a MIB view of all MIB object subsets that have access to the specified community.

Specifies the community's read and write access to MIB objects with access.

In the global configuration mode, use the following command to configure the community string:

Command	Description
snmp-server community string [**view** view-name] [**ro** | **rw**] [word]	Define a community access string.

You can configure one or more community strings. Use no snmp-server community to remove a given community string.

For community strings configuration, please refer to the chapter "SNMP Commands".

3) Set the system administrator's contact method and the system location

sysContact and **sysLocation** are the administrative variables in the system group in MIB that define the contact ID and the actual location of the node (system) that is being managed. This information can be accessed through the configuration file. Use one or more of the following commands in global configuration mode:

Command	Description
snmp-server contact text	Define a community access string.
snmp-server location text	Set the node location string

4) Define the max length of the SNMP agent packet

When the SNMP agent receives a request or responds, it can set the maximum length of the packet. Use the following command in global configuration mode:

Command	Description
snmp-server packetsize *byte-count*	Sets the maximum length of the packet.

5) Monitor SNMP status

Use the following command in global configuration mode to monitor SNMP input and output statistics, including illegal community string entries, errors, and the number of requested variables.

Command	Description
show snmp	Monitor SNMP status

6) Configure SNMP traps

Use the following command to configure the system to send SNMP traps (the second task is optional):

- Configure the trap sent by system

In the global configuration mode, use the following command to configure the system to send traps to a host.

Command	Description
snmp-server host host community-string [trap-type]	Specifies the recipient of the trap message.
snmp-server host *host* [traps|informs]{version {v1 | v2c | v3 {auth | noauth | priv } }}*community-string [trap-type]*	Specify the recipient of the trap message, and the version number and user name of the trap information. **Note**: For SNMPv3 traps, you must configure the SNMP engine ID for the host before configuring the host that received the trap.

After the system is powered on, the SNMP agent starts automatically and all types of traps are activated. Use **snmp-server host** to specify the host and which type of trap the host will receive.

Some traps need to be controlled by other commands. For example, if you want to send an SNMP link trap when the interface is open or closed, you need to activate the link trap using **snmp trap link-status** in interface configuration mode. Use the interface configuration command **no snmp trap link-stat** to close these traps.

In order for the host to receive a trap, you must configure the snmp-server host command for that host.

- Change trap operating parameters

As an option, you can specify the source interface that generates the trap, and specify the length of the message (packet) queue length or retransmission interval for each host

In the global configuration mode, use the following optional command to change the trap run parameters:

Command	Description
snmp-server trap-source *interface*	Specifies the source interface that generates the trap message. The command also sets the source IP address for the message.
snmp-server queue-length *length*	Create a message queue length for each trap host. The default value is 10.
snmp-server trap-timeout *seconds*	Defines the frequency of retransmission trap messages in the retransmission queue. The default value is 30 seconds.

7) SNMP bind source address

In the global configuration mode, use the following command to set the source address of SNMP packets.

Command	Description
snmp source-addr *ipaddress*	Set the source address of SNMP packets

Example

snmp-server community public RO

snmp-server community private RW

snmp-server host 192.168.10.2 public

In this example, it configures the community string **public** which have access to read all MIB variables and private which have the access to write all MIB variables. The user can use the community string to read the MIB variables in the system, read the MIB variables in the system and write the MIB variables that can be written in the system. It also specifies that when the system needs to send a trap message, the community string public is used to send trap messages to 192.168.20.2. For example, when a port of the system is down, the system will send a linkdown trap message to 192.168.20.2.

2.3.2 Configure RMON

RMON Configuration Task

- Following are the RMON configuration task:
- Configure the rMon alarm function
- Configure the rMon event function
- Configure the rMon statistics function
- Configure the rMon history function
- Display the rMon configuration

1) Configure the rMon alarm function

You can configure the rMon alarm function through the command line or SNMP network management. If you need to configure the SNMP network through the SNMP network management, you need to configure the SNMP of the switch. After the alarm function is configured, the device can monitor some statistics in the system. To configure the rMon alarm function, follow these steps:

Command	Description
configure	Enter the global configuration mode.
rmon alarm index variable *interval* **{absolute | delta} rising-threshold** *value [eventnumber]* **falling-threshold** *value [eventnumber]* **[owner** *string]*	Add a rMon alarm index Index is the index for the entry, the valid range is 1~65535. Variable means that the object of the monitored MIB must be a valid MIB object in the system, and only objects of type INTEGER, Counter, Gauge or TimeTicks can be detected. Interval is the interval of the sampling time, in seconds, the effective range of 1 ~ 4294967295. Use absolute to directly monitor the value of the MIB object; use delta to monitor changes in MIB object values between two samples. Value is used to indicate the threshold at which the alarm is generated, and the corresponding eventnumber represents the index of the event that occurs when the threshold is reached; eventnumber is optional. The owner string can be used to describe some of the descriptive information about the alert.

exit	Back to the management mode
write	Save the configuration

After an alarm entry is complete, the device acquires the value of oid specified by variable every interval. It is compared with the previous value according to the alarm type (absolute or delta). If the statistics are larger than the previous value and exceed the rising-threshold, it will raise an event with an index of eventnumber (if eventnumber is zero or the event table does not have an event that is indexed as eventnumber), and if the oid specified by variable is not available, the item status is set to invalid. When you use the rmon alarm command to configure the alarm entries with the same index multiple times, only the last configured parameter is valid. Use no rmon alarm index to delete the alarm entry with the index.

2) Configure the rMon event function

Configure the rMon event as follows

Steps	Command	Description
1	**configure**	Enter the global configuration mode.
2	**rmon event index [description** *string***] [log] [owner** *string***] [trap** *community***]**	Add an rMon event entry. **Index** is the index of the entry. The valid range is 1 ~ 65535. **description** represents the description of the event. **log** indicates that the event is raised in the log table to add a message. **trap** indicates that a trap will be generated when the event was raised. community is the community name. **owner string** can be used to describe some descriptive information about the event.
3	**exit**	Back to the management mode
4	**write**	Save the configuration

After the rMon event is configured, the eventLastTimeSent field of the event entry is updated to the sysUpTime when the rMon alarm is triggered. If the event is configured with the log attribute, add one information list to the log table. If the trap attribute is configured, send a trap by community. When the rmon event command is used to configure the event entry with the same index multiple times, only the last configured parameter is valid. Use **no rmon event index** to delete the event entry whose index is index.

3) Configure the rMon statistics function

The rMon statistics group is used to monitor the statistics on each interface on the device. RMon statistics function configuration steps are as follows:

Steps	Command	Description
1	**configure**	Enter the global configuration mode.
2	**interface iftype ifid**	Enter the interface mode. Iftype is the type of the interface. Ifid is the id for the interface.
3	**rmon collection stat index [owner** *string*]	Enable the statistics function on the interface. **Index** is the index of the statistics entry. **owner string** can be used to describe some descriptive information about the statistics table.
4	**exit**	Back to the global configuration mode.
5	**exit**	Back to the management mode
6	**write**	Save the configuration

When you use **rmon collection stat** to configure the event table entry with the same index multiple times, only the last configured parameter is valid. Use **no rmon collection stats index** to delete the entry whose index is index.

4) Configure the rMon history function

The RMON history group collects statistics for different time periods on an interface on the device. Following are the rMon history function configuration:

Steps	Command	Description
1	**configure**	Enter the global configuration mode.
2	**interface iftype ifid**	Enter the interface mode. Iftype is the type of the interface. Ifid is the id for the interface.

3	**rmon collection history index [buckets bucket-number] [interval second] [owner owner-name]**	Enable the history function on the interface. Index is the index of the history entry. In all data collected by this history control entry, the latest bucket-number entry needs to be retained. Users can view the Ethernet history table to get these statistics. The default value is 50. **second** is the interval for obtaining statistics every two times. The default value is 1800 seconds (half an hour). **owner string** can be used to describe some descriptive information about the statistics table.
4	**exit**	Back to the global configuration mode.
5	**exit**	Back to the management mode
6	**write**	Save the configuration

After adding a history control entry, the device gets the statistics from the specified interface every second and adds the result as an entry to the Ethernet history table. When you use **rmon collection history index** to configure the history entry of the same index multiple times, only the last configured parameter is valid. Use **no rmon history index** to delete the index control entry whose index is index. Note that the bucket-number is too large and the interval second is too small will occupy too much system resources.

5) Display the rMon configuration

Use **show** command to display the rMon configuration.

Command	Description
show rmon [alarm] [event] [statistics] [history]	Display rmon configuration information **alarm** indicates the configuration for alarm entry. **event** indicates the configuration for event entry and also displays the entry caused by that the event is be raised. **statistics** indicates the configuration for statistic entry and also display the statistic collected on the interface. **history** indicates configuration for history entry and also display the latest statistics collected on the interface in specified intervals.

2.3.3 Configure PDP

Overview

The PDP protocol is the two-layer protocol used to discover the network device and help management program to discover all the neighbors of the known device. Use PDP to learn the device type and the SNMP agent address of the neighbor device. The neighbor device is discovered by PDP, and the network management program can query the neighbor device with SNMP to obtain the network topology.

PDP can discover the neighbor device, but cannot accept the SNMP to query neighbor device. Therefore, the switch can only be at the edge of the network. Otherwise, the complete network topology cannot be obtained.

PDP on the switch can be configured on all SANPs (such as Ethernet).

There are several switches that currently support PDP:

S2008/S2026B/S2116/S2224D/S2224M/S2226/S2448/S3224/S3224M/S3424/S3448/S3512/S3524

PDP Configuration Task

- Default PDP configuration
- Configure PDP clock and information save time
- Configure PDP version
- Enable PDP
- Enable PDP on port
- Monitor and manage PDP

1) Default PDP configuration

Function	Default
PDP global configuration	Disable
PDP port configuration	Disable
PDP clock（frequency of sending message）	60s
Save PDP information	180s
PDP version	2

2) Configure PDP clock and information save time

Command	Description
pdp timer *seconds*	Set the frequency for PDP sending message
pdp holdtime *seconds*	Set the time for saving PDP information

3) Configure PDP version

Use the following command to set PDP version in global configuration mode.

Command	Description
pdp version {1|2}	Set PDP version

4) Enable PDP

PDP is not enabled on the default configuration. You can use the following command to enable PDP.

Command	Description
pdp run	Enable the PDP on the switch

5) Enable PDP on port

PDP is not enabled in the default configuration. Use the following command in interface configuration mode to enable PDP on the port, after enabling PDP on the switch:

Command	Description
pdp enable	Enable PDP on the port

6) Monitor and manage PDP

Use the following command to monitor PDP.

Command	Description
show pdp traffic	Display the count of receiving and sending PDP packet by the switch
show pdp neighbor [detail]	Display the neighbors discovered by PDP

Example for PDP Configuration

Example 1: Enable PDP

config# pdp run

config# int f0/0

config_f0/0#pdp enable

Example 2: Configure PDP clock and information save time

config#**pdp timer** 30

config#**pdp holdtime** 90

Example 3: Configure PDP version

config#pdp version 1

Example 4: Monitor PDP information

config#show pdp neighbors

Capability Codes:R - Router, T - Trans Bridge, B - Source Route Bridge S - Switch, H - Host, I - IGMP, r - Repeater

Device ID Local IntrfceHoldtmeCapabilityPlatform Port ID

joeEth 0 133 4500 Eth 0

samEth 0 152 R AS5200 Eth 0

2.4 SSH Configuration

2.4.1 SSH Overview

SSH server

The SSH client connect the device safely and securely through the SSH server. This connection provides the function similar with telnet. SSH server supports encryption algorithms including des, 3des and blowfish.

SSH client

SSH client is running on the SSH protocol, and provide authentication and encryption. Because using authentication and encryption, the SSH client allows secure communication between the communication devices or between other devices that support the SSH server in an insecure network environment. SSH client supports encryption algorithms including des, 3des and blowfish.

Implement Features

ssh server and ssh client support ssh version 1.5. It only supports shell.

2.4.2 Configuration Task

Configure Authentication Methods List

SSH server use login authentication and the default name of authentication methods list is “default”.

Command	Description

Ip sshd auth_method STRING	Configure authentication methods list

Configure Access Control List

To control the access to ssh server of the device, you can configure access control list for ssh server. Use the following command to configure in global configuration mode.

Command	Description
Ip sshd access-class STRING	Configure access control list

Configure the timeout for authentication

After the client and server establish the connection, if the server cannot pass the authentication within the set time, the server will close the connection.

Use the following command to configure the access control list in global configuration mode.

Command	Description
Ip sshd timeout <60-65535>	Configure the timeout for authentication

Configure the number of authentication retries

When the user authentication fails and exceed the maximum of authentication times, the SSH server does not allow the user to continue again, unless the connection is restarted. It can retry 3 times by default.

Use the following command to configure the maximum number of retries in the global configuration mode:

Command	Description
Ip sshd auth-retries <0-65535>	Configure the maximum of

Enable SSH server

The SSH server is enabled by default. When enable the SSH server, the device generates an rsa key pair and then monitor the connection requests from the client. This process takes about one or two minutes.

Use the following command to enable SSH server in the global configuration mode:

Command	Description
Ip sshd enable	Enable ssh server. The bits number of the key is 1024.

Example for ssh server Configuration

The following configuration only allows hosts with IP 192.168.20.40 to access the ssh server and use the local user database to identify the user.

Access Control List

ip access-list standard ssh-acl

permit 192.168.20.40

Global Configuration

aaa authentication login ssh-auth local

ip sshd auth-method ssh-auth

ip sshd access-class ssh-acl

ip sshd enable

Chapter 3 Interface Configuration Commands

3.1 Overview

The information in the overview will help you learn about the various interface types supported by our switch and provide reference configuration information that is appropriate for different interface types.

For a detailed description of the interface commands, please refer to "Interface Configuration Commands". If you want to view the documentation for other commands that appear in this overview, please refer to other part.

The overview contains general information that can be applied to all interface types. Following are the information:

3.1.1 Interface Type

Following are the information about the interface type:

Type	Task	Reference
Ethernet interface	Configure the Ethernet interface Configure fast Ethernet Interface Configure gigabit Ethernet interface	"Configure Ethernet Interface"
Logical interface	Loopback interface empty interface VLAN interface SuperVlan Interface	"configure logical interface". Loopback interface and empty interface only can be configured on the three-layer switch. VLAN and SuperVlan interface only can be configured on the two-layer switch.
	Aggregate interface	"Configure aggregate interface"

Our switches support two types of interfaces: Ethernet interfaces and logical interfaces. The type of Ethernet interface on a device depends on the standard communication interface and the interface card or interface module installed on the switch. A logical interface is an interface without corresponding physical device and is created manually by the user.

The Ethernet interfaces supported by our switches include:

- Ethernet interface
- Fast Ethernet Interface
- Gigabit Ethernet interface

The logical interfaces supported by our switches include:

- Loopback interface
- empty interface
- Aggregate interface

- VLAN interface

3.1.2 Introduction for Interface Configuration

Following configuration is suitable for all interfaces. In the global configuration mode, follow the steps below to configure the interface:

- Use **interface** to enter the interface configuration mode, then you can configure the interface. These interfaces are used according to the interface number, which is assigned when the installation (factory) or interface card is added to the system. You can use **show interface** to display these interfaces. Each interface supported by the device provides its own status, as shown below:

```
Switch#show interface
FastEthernet0/1 is down, line protocol is down
    Hardware is Fast Ethernet, Address is 0009.7cf7.7dc1
MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Auto-duplex, Auto-speed
input flow-control is off, output flow-control is off
ARP type: ARPA, ARP Timeout 04:00:00
Last input never, output 17:52:52, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue :0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
  1 packets input, 64 bytes, 0 no buffer
  Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
  0 watchdog, 0 multicast, 0 pause input
  0 input packets with dribble condition detected
  1 packets output, 64 bytes, 0 underruns
  0 output errors, 0 collisions, 1 interface resets
  0 babbles, 0 late collision, 0 deferred
  0 lost carrier, 0 no carrier, 0 PAUSE output
  0 output buffer failures, 0 output buffers swapped out
```

Use the following command to configure Fast Gigabit Ethernet Interface g0/1

interface g 0/1

Note:

It is not necessary to add a blank between the interface type and the interface number. For example, g0 / 1 or g 0/1 can both be accepted by the switch.

1） You can configure the interface configuration command for the current interface in the interface configuration mode. The various commands define the protocols and applications that will be executed on the interface. These commands will remain until you exit the interface configuration state or switch to another interface.

2） Once the interface is configured, the interface status can be tested by using show command listed in the "Monitor and Maintain Interfaces" section.

3.2 Interface Configuration

3.2.1 Configure the common attributes for the Interface

Following describes the commands that can be executed on any type of interface to configure the common attributes of the interface. The common attributes that can be configured include: interface description, bandwidth and delay.

Add Description

Adding a description of the interface helps to remember the content attached to the interface. This description is only used as an interface annotation to help identify the purpose of the interface without affecting any function of the interface. This description will appear in the output of the following command: **show running-config** and **show interface**. If you want to add a description to any interface, use the following command in the interface configuration mode.

Command	Description
description *string*	Add description to currently configured interface.

Please refer to “Example for Interface Description”.

Set the Bandwidth

The upper layer protocol uses the bandwidth information to make operational decisions. In the interface configuration mode, use the following command to set the bandwidth for the interface:

Command	Description
bandwidth *kilobps*	Set the bandwidth for currently configured interface.

The bandwidth setting is only a routing parameter. It does not affect the actual physical interface communication rate

Set the Delay

The upper layer protocol uses delay information to make operational decisions. In the interface configuration mode, use the following command to set the delay for the interface:

Command	Description
delay *tensofmicroseconds*	Set the delay for current configured interface.

The delay setting only set the information parameters; this configuration command cannot adjust the actual delay of an interface.

3.2.2 Monitor and Maintain the Interface

Here are the tasks to monitor and maintain the interface:

- View interface status
- Initialize and delete interfaces
- Turn off and re-enable the interface

View Interface Status

Our switches can display a variety of commands related to the interface information, including the software and hardware version, interface status. Following are part of the interface monitoring commands. Refer to "Interface Configuration Commands". Following are the commands:

Command	Description
show interface [**type** [slot|port]]	Display interface status.
show running-config	Display current configuration.

Initialize and Delete Interfaces

For the logical interface, users can dynamically create and delete the interface. For sub-interfaces and channelized interfaces, it can also be dynamically deleted. Use the following command to initialize and delete the interface in global configuration mode:

Command	Description
no interface type [*slot*|*port*]	Initialize the and Delete Interfaces

Close and Restart the Interface

An interface can be disabled, and then all functions on the specified interface are enabled. And mark this interface as unavailable interface on all monitoring command displays. This information can be sent to other switches through dynamic routing protocol. Any routing modification will not affect this interface.

Use the following command in the interface configuration mode to close the interface and then restart it:

Command	Description
shutdown	Shutdown the interface.

no shutdown	Restart the interface.

You can use the command **show interface** and **show running-config** to check whether an interface is disabled. In the **show interface** command display, a disabled interface is displayed as "administratively down". Please refer to "Example for Interface Disable" for details.

3.2.3 Configure the Logical Interface

Following are the description of configuring logical interface:

- Configure aggregate interface
- Configure VLAN interface

Configure Aggregate Interface

The aggregate interface is generated for the bandwidth of a single Ethernet interface. It can be more than the same rate of the full-duplex interface bundled together, thus doubling the bandwidth.

Use the following command to define the aggregate interface.

Command	Description
Interface port-aggregator *number*	Define the aggregate interface.

S2224D can support aggregation interface. The maximum number of Ethernet interface supported by each aggregation interface is 4. Do not exceed the number.

Configure VLAN interface

The VLAN interface is the routing interface in the switch. The VLAN configuration in the global configuration mode is only used to add a Layer 2 VLAN to the system, and it is not defined if the switch receives the IP address in the VLAN. If there is no VLAN interface, such packets will be discarded.

Define the VLAN interface with the following command:

Command	Description
Interface vlan *number*	Configure VLAN interface.

3.2.4 Configure Ethernet Interface

Configure the Cable Detection Function

By default, this feature is enabled, and the gigabit port always turns off the feature

Command	Description
cable-diagnostic	Enable cable detection function
No cable-diagnostic	Disable cable detection function

Chapter 4 Interface Physical Characteristic Configuration

4.1 Configure the Ethernet Interface

This section describes the procedure for configuring an Ethernet interface. The switch supports 10Mbps Ethernet and 100Mbps Fast Ethernet interfaces. Following are the Specific configuration. The first step is necessary, and the other steps is optional.

4.1.1 Select the Ethernet interface

In the global configuration mode, use the following command to enter the Ethernet interface configuration mode.

Command	Description
interface fastethernet [slot|*port*]	Enter fast Ethernet configuration mode.
interface gigaethernet [slot|*port*]	Enter gigabit Ethernet configuration mode.

Show interface fastethernet command can display the status of the Fast Ethernet interface. **show interface gigaethernet** command can display the status of the Gigabit Ethernet interface.

4.1.2 Configure Rate

Ethernet rate can be achieved through the self-negotiation, and it also can be configured under the interface.

Command	Description
Speed {**10**|**100**|**1000**|**auto**}	Set the rate of fast Ethernet as 10M, 100M, 1000M or negotiation.
No speed	Restore the default setting. Rate is self-negotiated.

Note:

The speed of the optical interface is fixed, such as: the rate of GBIC and GE-FX is 1000M, and the rate of FE-FX is 100M. If the optical interface **speed** command is followed by **auto**, then the interface can open the auto-negotiation function. Otherwise, the interface is mandatory and cannot be negotiated.

By default, the Ethernet interface can be set to auto-negotiate either half or full duplex. On the gigabit port, this command is not exist. Gigabit port duplex mode can always be set to auto.

Command	Description
duplex {**full**|**half**|**auto**}	Set the duplex mode of the Ethernet.
No speed	Restore the default setting. Rate is self-negotiated.

4.1.3 Configure Interface Traffic Control

When the interface is full duplex mode, the traffic control is implemented through the PAUSE frame defined by 802.3X; when the interface is half duplex mode, it is implemented by back pressure.

Command	Description
flow-control [**on**|**off**]	Enable/disable interface traffic control.
no flow-control	Restore the default setting: no flow control on the interface.

Chapter 5 Interface Additional Characteristic Configuration

5.1 Interface Security

5.1.1 Configure the Number of Secure MAC Addresses for the Security Port

The number of secure port secure MAC addresses is the maximum number of MAC addresses that can be learned on the port where the security function is enabled. A packet with a source MAC address exceeding that number can cause a security port violation. The default value is 1.

Enter the management mode, and then follow the steps below to configure the number of secure port MAC addresses.

Command	Description
configure	Enter global configuration mode.
interface f0/1	Enter the interface configuration mode.
[no] switchport port-security maximum *value*	Specify/cancel the maximum MAC address number. ***Value*** is the maximum MAC address number.
exit	Back to the global configuration mode.
exit	Back to the configuration mode.
write	Save the configuration.

5.1.2 Configure the Static MAC Address of the Secure Port

After the static MAC address of the security port is configured, if the MAC address of the port is the configured static MAC address, the packet does not generate a security violation.

Enter the management mode, and then follow the steps below to configure the static MAC address of the security port.

Command	Description
configure	Enter global configuration mode.
interface f0/1	Enter the interface configuration mode.
[no] switchport port-security mac-address *mac-addr*	Add/cancel the maximum MAC address number. Mac-addr is the maximum MAC address number.
exit	Back to the global configuration mode.

exit	Back to the configuration mode.
write	Save the configuration.

5.2 Port Protection

Normally, the packet between the different ports of the switch can be free to forward. In some cases, the flow between ports needs to be forbid. Port isolation is to provide this control. The ports with port isolation function cannot transfer the packet with each other, but the other port can still transfer the packet with each other normally.

Command	Description
switchport protected	Set port isolation.
no switchport protected	Cancel port isolation.

5.3 Port Storm Control

The switch port may suffer from persistent, abnormal unicast (MAC address lookup failure), multicast or broadcast packet impact which result the paralysis of the port or even the entire switch. So a mechanism must be provided to suppress this phenomenon.

Command	Description
storm-control {**broadcast** | **multicast** | **unicast**} **threshold count**	Storm control of broadcast, multicast, or unicast packets.
no storm-control {**broadcast** | **multicast** | **unicast**} **threshold**	No storm control

5.4 Port Speed Limit

Limit the traffic rate of the port import and export by following configuration.

In privileged mode, use the following command to limit the traffic rate of the port.

Command	Description
configure	Enter global configuration mode.
interface f1/0	Enter the interface configuration mode.
[no] switchport rate-limit *band* { ingress|egress}	Configure the traffic rate limit for the port. **band** is the traffic rate to be limited.

	ingress indicates working on the entry; **egress** indicates working on the exit.
exit	Back to the global configuration mode.
exit	Back to the configuration mode.

Chapter 6 Interface Range Commands

6.1 Interface Range

6.1.1 Understand Interface Range

This is the often case that we need to configure the same attributes on a batch of the same type of port, when the port configuration task is in progress. To avoid dual configuration on each port, we provide the **interface range** configuration mode which allows you to configure the same command on multiple ports of the same type and slot number at once, reducing configuration effort. It should be noted that when entering the **interface range** mode, all the interfaces contained on this mode must have been already created.

6.1.2 Enter into Interface Range Mode

Use the following command to enter into interface range mode**.**

Step	Command	Description
1	**interface range** *type slot/<port1 - port2 | port3>[, <port1 - port2|port3>]*	Enter the range mode, which contains the following conditions: Slot number is **slot**; Port number is value between port1 and port2 or equal to port3; Port2 must be less than port1; There must be spaces before and after "-" and ",".

6.1.3 Example

Use the following command to enter into the port configuration mode, which contains 0 slots 1,2,3,6,8,10,11,12 Fast Ethernet port:

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

switch_config_if_range#

Chapter 7 Port Mirroring Configuration Commands

7.1 Port Mirroring Configuration Commands Task List

- Configure port mirroring
- Display the port mirroring information

7.1.1 Port Mirroring Configuration Commands Task

1) Configure port mirroring

In order to facilitate the management of the switch, you can configure the port mirroring, use a switch port to flow through a group of ports to observe the flow.

To enter privileged mode, follow these steps to configure port mirroring:

Command	Description
configure	Enter into global configuration mode.
mirror session *session_number* **{destination {interface** *interface-id***} | source {interface** *interface-id* **[, | -] [both | rx | tx] }**	Enter the interface configuration mode.
[no] switchport rate-limit *band* { ingress|egress}	Configure port mirroring. **session-number** is the port mirroring number. **destination** is the mirroring destination port. **source** is the mirroring source port **both | rx | tx** is the data stream to be mirrored. **rx** means only mirror the input data, **tx** means only mirror output data, **both** means input and output data.
exit	Back to management mode.
write	Save the configuration.

2) Display the port mirroring information

Chapter 8 Port Mirroring Configuration Commands

8.1 VLAN Configuration Commands

8.1.1 VLAN Overview

VLAN (Virtual Local Area Network), that is, a virtual local area network, is a network which divides the equipment of the LAN logically rather than physically. IEEE in 1999 promulgated a draft standard for IEEE 802.1Q protocol for standardized VLAN implementation. VLAN technology can logically divide a physical LAN to different broadcast domains (VLAN). Each VLAN contains a group of devices with the same requirements that have the same attributes as the physically formed LAN. But it is logically Rather than physically partitioning, so the devices in the same VLAN need not to be placed in the same physical space, that is, these devices may not belong to the same physical LAN segment, a VLAN internal broadcast and unicast traffic will not be forwarded to other VLANs, which helps to control traffic, reduce equipment investment, simplify network management, and improve network security.

- Support port-based VLAN
- The port supports 802.1Q relay mode
- Support access port

Port-based VLANs are assigned to a subset of VLANs supported by the switch. If the VLAN subset has only one VLAN, then the port is the access port; if there are multiple VLANs in the VLAN subset, the port is a trunk port. And it has a default VLAN which is native VLAN of the port. The VLAN ID is the Port VLAN ID (PVID).

- Support controlling the range of the port VLAN.

The vlan-allowed parameter is used to control the range of VLANs which the port belongs to. The vlan-untagged parameter is used to control the port to sent packets without VLAN tag to the corresponding VLAN.

VLANs are divided into a variety of ways, based on the MAC address, based on IP subnet, based on protocol, based on port to divide VLANs. And the VLAN is divided according to the sequence of the MAC VLAN, IP subnet VLAN, protocol VLAN, and port VLAN by default.

8.1.2 Dot1Q Tunnel Overview

Preface

The Dot1Q tunnel is a visualized call to the 802.1Q-based tunnel protocol and is defined in IEEE 802.1ad. The core concept is to encapsulate the user's private VLAN tag into the public network VLAN tag. The packet carries the two-layer tag through the backbone network of the service provider, so as to provide the user with a relatively simple Layer 2 VPN tunnel. Dot1Q Tunnel protocol is a simple and easy to manage. It does not require the support of the signaling, and it can be achieved only through the static configuration, especially for small, three-tier switch as the backbone of the enterprise network or small-scale MAN.

The Dot1Q tunnel feature meets the requirement of some user, providing a low-cost, simple two-tier VPN solution, and more and more small users tend to use the this function to build their own VPN network. In the operator's network, P devices do not need to support Dot1Q tunnel, that is, the traditional three-layer switch can meet the demand. It greatly protects the operator's investment.

- Support to enable the Dot1Q tunnel in global.
- Support for translation of Customer VLAN and SPVLAN, including translation of flat mode and translation of double-label (QinQ) mode.
- Support the configuration of the connection.

- Support for variable TPID.

Implementation of Dot1Q tunnel

One of the implementation of Dot1Q tunnel is based on port and the other is based on CVLAN Tag classification.

1) Dot1Q tunnel based on port

When the device receives the packet, the switch will tag the port with the VLAN tag of the default VLAN, regardless of whether the packet contains a VLAN tag. In this case, if the packet is received with a VLAN tag, the packet becomes the packet of the Double Tag. If receives untagged packets, the packet will be tagged with the default VLAN tag of the port.

The structure of the packet with single VLAN Tag as the figure 1 shows:

DA	SA	ETYPE(8100)	VLAN TAG	ETYPE	DATA	FCS
(6B)	(6B)	(2B)	(2B)	(2B)	(0~1500B)	(4B)

Figure 1 Packet with single VLAN Tag

The structure of the packet with double VLAN Tag as the figure 2 shows:

DA	SA	ETYPE(8100)	ETYPE	CVLAN Tag	ETYPE	ETYPE	DATA	FCS
(6B)	(6B)	(2B)	(8100)	(2B)	(2B)	(2B)	(0~1500B)	(4B)
			(2B)					

Figure 2 Packets with outer VLAN tags

2) Dot1Q tunnel based on CVLAN Tag classification.

The service shunts are implemented according to the CVLAN ID range of the inner CVLAN tag of the Dot1Q tunnel. You can translate the CVLAN interval into an SPVLAN ID, with flat VLAN translation mode and QinQ VLAN translation mode.In the QinQ VLAN translation mode, when different service of the same users use different CVLAN IDs, traffic can be divided according to the CVLAN ID range. For example, the CVLAN ID range of the broadband service is 101 to 200, the CVLAN ID range of the VOIP service is 201 to 300, the CVLAN ID range of the IPTV service is 301 to 400. After PE device receiving the user data, tag the broadband services with the SPVLAN Tag, SPVLAN ID of which is 1000; tag the VOIP with the SPVLAN Tag, SPVLAN ID of which is 2000; tag the IPTV with the SPVLAN Tag, SPVLAN ID of which is 3000.

The difference between the Flat VLAN translation mode and the QinQ VLAN translation mode is that the SPVLAN Tag in the Flat VLAN translation mode is not superimposed on the outer layer of the CVLAN tag, but instead replaces the CVLAN tag directly.

TPID Value can be modified

Following figure shows the structure of the Tag defined by IEEE802.1Q:

TPID	User Priority	CFI	VLAN ID
2 byte	3 bit	1 bit	12 bit

Figure 3 tag structure of the VLAN Tag

The TPID is a field in the VLAN tag. The value of field is 0x8100 specified by IEEE 802.1Q. The switch use the TPTD value (0x8100) specified by the protocol by default. Some vendors' devices does not set the TPID value of the outer tag on the Dot1Q tunnel packet to 0x8100. In order to be compatible with these devices, most switches can modify the TPID value of the Dot1Q tunnel packets. The TPID value of the PE device can be configured by the user. When the port of these devices receives the packet, the TPID value in the outer VLAN tag of the packet will be replaced with value set by the user and sent to the public network. Then these Dot1Q tunnel packets can be identified by other vendors' devices.

8.1.3 VLAN Configuration Task List

- Adding/Deleting VLAN
- Configuring switch port
- Creating/Deleting VLAN interface
- Monitoring configuration and state of VLAN
- Configuring VLAN-based access control list
- Enable/ disable global Dot1Q Tunnel
- Configuring VLAN transmit mode and entry on the interface mode
- Configuring MAC-based VLAN
- Configuring IP subnet-based VLAN
- Configuring protocol-based VLAN

8.1.4 VLAN Configuration Task

Adding/Deleting VLAN

A virtual LAN, commonly known as a VLAN, is a group of hosts with a common set of requirements that communicate as if they were attached to the same wire, regardless of their physical location. A VLAN has the same attributes as a physical LAN, but it allows for end device to be grouped together even if they are not located on the same LAN segment. A VLAN may have multiple ports and all unicast, multicast and broadcast packet can only be forwarded from the same VLAN to the terminal. Each VLAN is a logistical network. If the data wants to reach another VLAN, it must be forwarded by router or bridge.

Run the following command to configure VLAN.

Run	To
vlan vlan-id	Enter the VLAN configuration mode.
name str	Name in the VLAN configuration mode.
Exit	Exit vlan configuration mode, and establish vlan.
vlan vlan-range	Establish multiple VLANs at the same time.

no vlan vlan-id | vlan-range	Delete one or multiple VLANs.

It can also dynamically add/delete VLAN via VLAN management protocol GVRP.

Configuring Switch Port

The switch port supports the following modes: access mode, trunk mode, dot1q-tunnel mode and VLAN tunnel linkup port mode.

- The access mode indicates that this port is only subordinate to one VLAN and only sends and receives untagged Ethernet frame.
- The trunk mode indicates that this port is connected to other switches and can send and receive tagged Ethernet frame.
- The dot1q-tunnel mode takes is based on the trunk mode. This port search the SPVLAN on the VLAN translation table according to the received VLAN tag. The switch chip changes the original tag with SPVLAN tag or adds SPVLAN tag to the original tag. When the packet goes out from the port, it will change changes the original tag with SPVLAN tag or forcibly adds SPVLAN tag to the original tag. Therefore allowing switch to ignore the different VLAN partitions that connected to the network. Then the packet will be delivered to the other port in the other sub network of the same customer. The transparent transmission is realized in this way.
- VLAN tunnel linkup port mode is a sub mode based on trunk mode. When the packet goes out of the port, SPVLAN should be configured in the untagged range to ensure that all packets are intact. When a packet arrives from the port, the TPID of the packet will be checked. If the packet is found to be undeserved or untagged, the SPVLAN tag containing its own TPID is added as the outer label of the packet.

Each port has one default VLAN and PVID, and all the data without VLAN tag received on the port belong to the data packets of the VLAN.

Trunk mode can ascribe port to multiple VLAN and also can configure which kind of packet to forward and the number of VLAN that belongs, that is, the packet sent on the port is tagged or untagged, and the VLAN list that the port belongs.

Run the following command to configure the switch port:

Run	To
switchport pvid *vlan-id*	Configure PVID of switch port.
switchport mode access|trunk|dot1q-translation-tunnel| dot1q-tunnel-uplink *tpid*	Configure port mode of the switch.
switchport trunk vlan-allowed	Configure vlan-allowed range of switch port.
switchport trunk vlan-untagged	Configure vlan-untagged range of switch port.
switchport flat-translation	Enable flat N:1 VLAN reversal translation function of the port

Creating/Deleting VLAN Interface

The vlan interface can be used to specify ip address and mask. Run the following command to configure vlan interface:

Run	To
[no] interface vlan *vlan-id*	Create/Delete a VLAN interface.

Monitoring configuration and state of VLAN

Run the following command to monitor the configuration and state of VLAN and other Dot1Q Tunnel:

Run	To
show vlan [id *x* **| interface** *intf* **| dot1q-tunnel [interface** *intf***] | mac-vlan | subnet | protocol-vlan]**	Display the configuration and state of VLAN and other Dot1Q Tunnel
show interface vlan *x*	Display the state of vlan port/supervlan port.

Enable/ Disable Global Dot1Q Tunnel

Enable the dot1q-tunnel in global mode. All the ports will become Dot1Q Tunnel uplink port and the coming packet will be forced to be tagged with SPVLAN tag.

Run	To
dot1q-tunnel	Configure dot1q-tunnel in global.

Configuring flat N:1 VLAN Reversal Translation Function in Global

Enable flat N:1 VLAN reversal translation function in global.

Run	To
[no] flat-translation-global	Enable flat N:1 VLAN reversal translation function in global.

Configuring VLAN Translation Mode and Entry of Port

VLAN translation mode and VLAN translation entries are configured in port mode **dot1q-translating-tunnel**. There are two types of translation modes: Flat mode and QinQ mode. Flat mode will use the CVLAN tag which enter into dot1q-translating-tunnel linkup port as the index, search the VLAN translation table, replace the SPVLAN with the CVLAN, and the SPVLAN to CVLAN will be converted when the packet came out from the port. The QinQ mode will use the CVLAN tag which enter into dot1q-translating-tunnel linkup port as the index, search the VLAN translation table. Then the SPVLAN tag will be superimposed on the outer edge of the CVLAN tag. When the packet comes out of this port, the SPVLAN tag will be removed.

When configuring a VLAN translation entry on port configuration, QinQ mode can configure multiple-to-one mapping between CVLAN and SPVLAN. To configure a multi-to-one mapping between CVLAN and SPVLAN in flat mode, you must configure flat-translation, then SPVLAN and CVLAN will be correctly converted when the packet comes out of this port.

Following is the command to configure VLAN translation mode and entry.

Run	To
switchport dot1q-translating-tunnel mode {flat | qinq} translate {*oldvlanid* **|** *oldvlanlist***}** *newvlan* **[***priority***]**	Configure VLAN translation mode and entry.

Configuring MAC-Based VLAN

A MAC-Based VLAN is a way of dividing a VLAN by the source MAC address of a packet. When a port receives an untagged packet, the device obtains the source MAC address of the packet as the matching keyword to find the VLAN which the packet belongs to by searching the MAC VLAN entry.

The MAC-Based VLAN configuration includes adding / deleting MAC VLAN entries and enabling / disabling MAC VLAN on the port.

In the global configuration mode, use the following command to add / remove MAC address entries:

Run	To
mac-vlan mac-address *mac-addr* **vlan** *vlan-id* **[priority]**	Add a MAC VLAN entry.
no mac-vlan mac-address *mac-addr*	Delete a MAC VLAN entry.

MAC-Based VLAN only works on ports that enable the function. In the port configuration mode, use the following command to enable / disable the MAC VLAN on the port:

Run	To
[no] switchport mac-vlan	Enable/Disable MAC-Based VLAN on the port configuration.

Caution: When the port mode is access, if the incoming VLAN matched through MAC VLAN is not the PVID of the port, the packets will be discarded. Therefore, if not, do not configure the port mode for MAC VLAN enabled as access.

Configuring IP Subnet-Based VLAN

IP Subnet-Based VLAN is a way to divide VLANs based on the source IP address of packets and the subnet mask. When a port receives an untagged packet, the device will determine the VLAN to which the packet belongs based on the source IP address of the packet and the subnet mask.

IP subnet-based VLAN configuration includes adding / removing subnet VLAN entries and enable/disable the Subnet VLAN function on the port.

Use the following command to add / remove a Subnet VLAN entry in VLAN configuration mode:

Run	To
[no] subnet { any | *ip-addr mask* **}**	add / remove a Subnet VLAN entry

The IP subnet-based VLAN only works on ports that enable the function. In the port configuration mode, use the following command to enable / disable the Subnet VLAN function on the port:

Run	To
[no] switchport vlan-subnet enable	Enable/disable IP Subnet-based VLAN on port configuration mode.

Caution: When the port mode is access, if the incoming VLAN matched through Subnet VLAN is not the PVID of the port, the packets will be discarded. Therefore, if not, do not configure the port mode for Subnet VLAN enabled as access.

Configuring Protocol-Based VLAN

Protocol-Based VLAN divide the VLAN based on the protocol which the receiving message belongs to on the port. When the port receives an untagged packet, the device will divide the VLAN based on the protocol which the receiving message belongs to on the port.

The way to determine the protocol of the packet on the switch is to determine the protocol-based VLAN configuration according to the encapsulation format of the packet and the value of the special field: add / remove protocol templates in global mode and add / remove associations with protocol templates in port configuration mode.

- add / remove protocol templates in global mode and add / remove associations with protocol templates on the port configuration mode.

In the global configuration mode, use the following command to add / remove protocol templates.

Run	To
protocol-vlan *protocol_index* **frame-type { ETHERII | SNAP | LLC } ether-type** *etype-id*	add a protocol templates
no protocol-vlan *protocol_index*	remove a protocol templates

Note that when frame-type is LLC, the upper and lower bytes of ether-type correspond to DSAP and SSAP in the packet respectively.

The protocol template only works on the port of the template. The same protocol template can correspond to different VLANs on different ports. In port configuration mode, use the following command to add / remove association with the protocol template:

Run	To
switchport protocol-vlan *protocol_index* **vlan** *vlan-id*	add association with the protocol template
no switchport protocol-vlan *protocol_index*	remove association with the protocol template

8.1.5 Configuration Example

Example for Dot1Q Tunnel

Here are a few typical networking schemes to explain the application of the Dot1Q Tunnel.

- Example 1

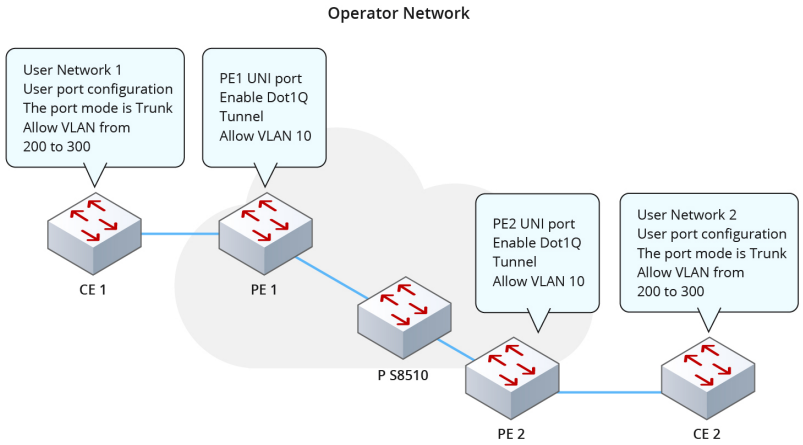


Figure 4 typical networking schemes for Dot1Q Tunnel

Assume that F0/1 of CE1 is connected to F0/1 (or G0/1) of PE1. PE1 and S8510 are connected to F0/2 (or G0/2). PE2 and S8510 are F0/2 (or G0/2). F0/1 (or G0/1) of PE2 is connected to F0/1 of CE1.

The port G0/1 of the PE is configured as the access port of VLAN 10 and enables Dot1Q tunnel. However, the trunk port still needs trunk VLAN 200-300, so that the connection between CE and PE becomes an Asymmetrical Link. So the public network only need to assign a VLAN number 10 to the user, regardless of how many private network VLAN ID within the user network. When the user message with the tag came into the service provider's backbone network, the newly assigned Public network is uniformly forced to be inserted. After the packet arrives at the PE device on the other side of the backbone network according to the VLAN number of the public network passes through the backbone network, the public network VLAN tag is stripped, the user packets are restored, and then transmitted to the user's CE device. Therefore, the packets transmitted in the backbone network have two 802.1Q tag headers. One is the public network tag, another is the private network tag. Following is the specific message forwarding process:

1) Because the out port of CE1 is a trunk port, the packets sent to PE1 carry the VLAN tag of the private network (range is 200-300). The message is shown in Figure 5.

DA	SA	ETYPE(8100)	VLAN TAG	ETYPE	DATA	FCS
(6B)	(6B)	(2B)	(2B)	(2B)	(0~1500B)	(4B)

Figure 5 The message structure from CE1

2) After entering PE1, because the ingress port is the access port of the Dot1Q tunnel, PE1 ignores the VLAN tag of the user's private network, but instead inserts the tag of the default VLAN 10 into the user's message, as shown in Figure 6.

DA	SA	ETYPE(8100)	SPVLAN Tag	ETYPEA(8100)	CVLAN Tag	ETYPE	DATA	FCS
(6B)	(6B)	(2B)	(2B)	(2B)	(2B)	(2B)	(0~1500B)	(4B)

Figure 6 The message structure from PE1

3) In the backbone network, the packets are propagated along the port of trunk port 10, and the tag of the user's private network remains transparent in the backbone network until it reaches the network edge device PE2.

4) PE2 discovers the access port VLAN 10 connected to CE2, and strips the tag of VLAN 10 according to the traditional 802.1Q protocol. Then send the original packet of the user to CE2, as shown in Figure 7.

DA	SA	ETYPE(8100)	VLAN TAG	ETYPE	DATA	FCS
(6B)	(6B)	(2B)	(2B)	(2B)	(0~1500B)	(4B)

Figure 7 The message structure from PE2

It can be seen that, the Dot1Q tunnel protocol is very simple. And it requires no signaling to maintain the tunnel establishment and can be configured by static configuration.

For the typical configuration of the Dot1Q Tunnel, the switch needs the following configuration (PE1 is the same as PE2):

Dot1Q Tunnel configuration for 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

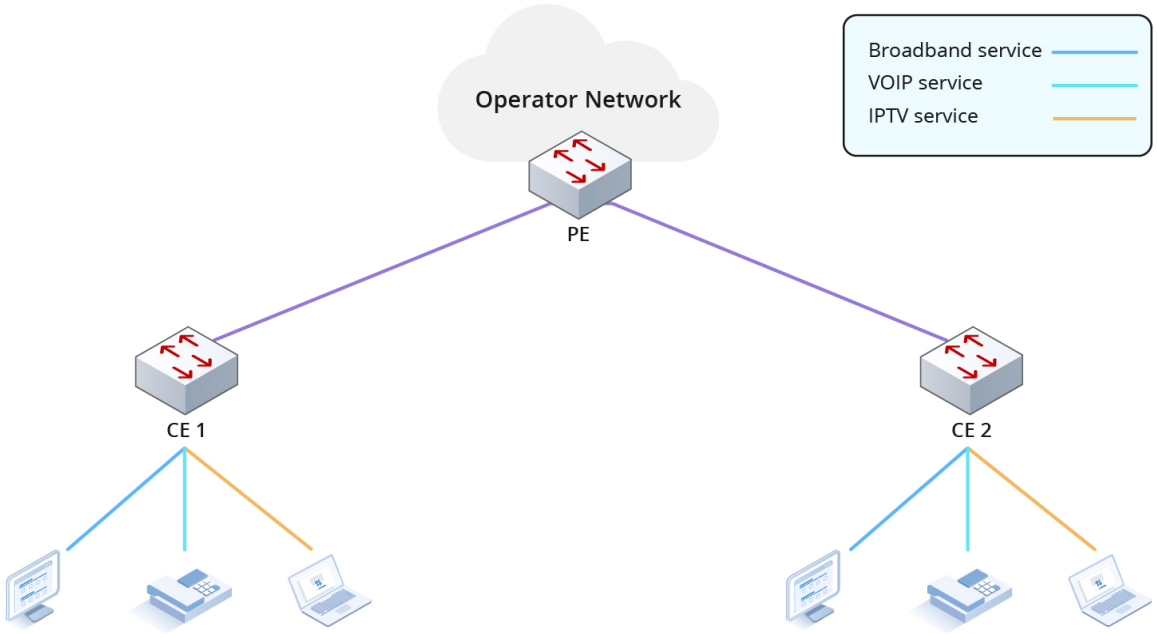
- Example 2

If different services of the same user are involved, the user access point is set on a UNI port of the PE. To distinguish between different services and implement different QOS standards, you must use Do1Q tunnel VLAN translation.

As shown in Figure 8, the operator assigns three VLANs to each user, one VLAN corresponding to one service. For example, for users 1, VLAN tag values are 1001, 2001, and 2001 respectively. VLAN1001 corresponds to broadband. VLAN 2001 corresponds to the VOIP. VLAN 3001 corresponds to the IPTV. After the service enters into the UNI port of the PE switch, it will be marked with a different outer tag according to the user VLAN ID. If the user data outer label is 1001, the label 1001 is added directly to the outer tag. For user 2, its different business can also be assigned different VLAN tags. The difference between the assignment of outer labels and users is mainly to distinguish the location of the CE, but also to find the final positioning of the user.

Device	Service	Inner CVLAN tag	Outer SPVLAN tag	Stream classification principle
CE1	Broadband	101-200	1001	VLAN Interval
	VOIP	201-300	2001	
	IPTV	301-400	3001	
CE2	Broadband	101-200	1002	
	VOIP	201-300	2002	
	IPTV	301-400	3002	

In this networking scheme, the inner and outer labels well distinguish the business and locate the user. The inner label + outer label can locate a user whose outer label identifies the location of the CE and also identifies the service, the inner label identifies the location of the user on the CE.



Assume that CE1 is connected to G0/1 port of PE1 and CE2 is connected to G0/2 port of PE1. The Dot1Q tunnel NNI port of PE is g0/3, which needs to be configured as follows:

Dot1Q Tunnel configuration for the switch:

Switch_config#dot1q-tunnel

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_g0/2#switchport mode dot1q-translating-tunnel

Switch_config_g0/2#switchport dot1q-translating-tunnel mode QinQ translate 101-200 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_g0/3#switchport mode dot1q-tunnel-uplink

Appendix A Abbreviations

Abbreviations	Full name

VPN	Virtual Private Network
TPID	Tag Protocol Identifier
QoS	Quality of Service
P	provider bridged network core
PE	provider bridged network edge
CE	customer network edge
UNI	user-network interface
NNI	network-network interface
CVLAN	Customer VLAN
SPVLAN	Service provider VLAN

Chapter 9 STP Configuration Commands

9.1 SSTP Configuration Commands

9.1.1 spanning-tree

The standard Spanning Tree Protocol (STP) is based on the IEEE 802.1D standard. It simplifies the LAN topology comprising several bridges to a sole spanning tree, preventing network loop from occurring and ensuring stable work of the network.

The algorithm of STP and its protocol configure the random bridging LAN to an active topology with simple connections. In the active topology, some bridging ports can forward frames; some ports are in the congestion state and cannot transmit frames. Ports in the congestion state may be concluded in the active topology. When the device is ineffective, added to or removed from the network, the ports may be changed to the transmitting state.

In the STP topology, a bridge can be viewed as root. For every LAN section, a bridging port will forward data from the network section to the root. The port is viewed as the designated port of the network section. The bridge where the port is located is viewed as the designated bridge of the LAN. The root is the designated bridge of all network sections that the root connects. In ports of each bridge, the port which is nearest to the root is the root port of the bridge. Only the root port and the designated port (if available) are in the transmitting state. Ports of another type are not shut down but they are not the root port or the designated port. We call these ports are standby ports.

The following parameters decide the structure of the stabilized active topology:

(1) Identifier of each bridge

(2) Path cost of each port

(3) Port identifier for each port of the bridge

The bridge with highest priority (the identifier value is the smallest) is selected as the root. Ports of each bridge have the attribute Root Path Cost, that is, the minimum of path cost summation of all ports from the root to the bridge. The designated port of each network segment refers to the port connecting to the network segment and having the minimum path cost. If several ports (connected to different bridges on the same LAN segment) have the same root path cost, they will first compare the identity of their bridge and then compare the port identification. In this way, each LAN segment has only one designated port (Designated Port), and each bridge also has only one Root Port.

Spanning tree topology dost not have loop in the network. It can also ensure the stability of the network and the ability to recover from failure. Nowadays the Ethernet switch is widely used, and STP is more and more important. So the spanning tree protocol is provided as a basic function of the switch.

Rapid Spanning-Tree Protocol (RSTP) is an important update to 802.1D STP. When the bridge, bridge port or LAN segment fails in the network, the RSTP realizes the fast convergence of the network topology. The new root port on the bridge can go into the forwarding state immediately, and the direct acknowledgment between the bridges allows the specified port to be forwarded immediately. For the configuration of the RSTP protocol, please refer to Chapter 2.

This chapter describes how to configure the standard spanning tree protocol that switch supports.

Note:

802.1D STP and 802.1D RSTP are abbreviated to SSTP and RSTP in this article. SSTP indicates Single Spanning-tree.

9.1.2 SSTP Configuration Task List

- Selecting STP Mode
- Selecting STP Mode
- Disabling/Enabling STP of Port
- Configuring the Switch Priority
- Configuring the Hello Time
- Configuring the Max-Age Time
- Configuring the Forward Delay Time
- Configuring Port Priority
- Configuring Path Cost
- Monitoring STP Status
- Configuring SNMP Trap

9.1.3 SSTP Configuration Task

Selecting STP Mode

Run the following command to configure the STP mode:

Run	To
spanning-tree mode {sstp | pvst | rstp | mstp }	Virtual Private Network

Disabling/Enabling STP

Spanning tree is enabled by default. Disable spanning tree if there is no need to run STP.

Follow these steps to disable spanning-tree:

Run	To
no spanning-tree	Disables STP.

Use the following command to enable spanning-tree:

Run	To
spanning-tree	Enables default mode STP (SSTP).
spanning-tree mode { **sstp | pvst | rstp | mstp** }	Enables a certain mode STP.

Disabling/Enabling STP of Port

Spanning tree is enabled on all switch port by default. Use following command to disable STP on the port configuration mode:

Run	To
no spanning-tree	Disables STP of port.

After the port is disabled, the port will maintain the assigned port role and forwarding status. And the BPDU will not be sent. But each STP mode will still check and count the BPDU received by the port and update the boundary information and topology information.

Note:

If the port already has "RootPort", "AlternatePort", "MasterPort" or "BackupPort" when configuring “no spanning-tree”, the protocol information received by the port will be aged and concerted to “DesignatedPort” on RSTP / MSTP mode. In SSTP / PVST mode, the port will remain in the original role for a period of time, waiting for the timer timeout, then the information will be aging.

Each STP mode supports the **BpduGuard** of the port with "no spanning-tree".

Configuring the Switch Priority

You can configure the switch priority to choose the STP for network topology.

Use the following command to configure the switch priority of SSTP：

command	purpose
spanning-tree sstp priority *value*	Modifies sstp priority value.
no spanning-tree sstp priority	Returns sstp priority to default value (32768).

Configuring the Hello Time

You can determine the interval for sending packets when the switch serves as the root bridge by configuring the Hello time of SSTP.

Use the following command to configure Hello Time of SSTP：

command	purpose
spanning-tree sstp hello-time *value*	Configures sstp Hello Time.
no spanning-tree sstp hello-time	Returns sstp Hello Time to default value (2s).

Configuring the Max-Age Time

Use the sstp max age to configure the max-age time for the STP message when the switch is work as the root bridge.

Use the following command to configure Max-age of SSTP：

command	purpose
spanning-tree sstp max-age *value*	Configures the sstp max-age time.
no spanning-tree sstp max-age	Restore the max-age time to default value (20s).

Configuring the Forward Delay Time

Configure SSTP Forward Delay to determine the interval for the transition of all the switches in the network when the switch is work as the root bridge.

Use the following command to configure SSTP Forward Delay Time：

command	purpose
spanning-tree sstp *forward-time*	Configures sstp Forward time.
no spanning-tree sstp forward-time	Returns forward time to default value (15s).

Configuring the Port Priority

If a loop occurs, STP will convert the state of some ports to Blocking to break the loop. You can control whether a port is blocked by configuring port priority and port path.

Use the following command to configure port priority of SSTP：

command	purpose
spanning-tree port-priority *value*	Configures the port priority for interfaces on all configuration modes.
spanning-tree sstp port-priority *value*	Modifies SSTP port priority.
no spanning-tree sstp port-priority	Return port priority to default value (128).

Configuring the Path Cost

Follow these steps to configure the cost of an interface：

command	purpose

spanning-tree cost *value*	Configures the cost for an interface on all configuration modes.
spanning-tree sstp cost *value*	Modifies SSTP path cost.
no spanning-tree sstp cost	Restore path cost to default value.

Monitoring STP State

To monitor the STP configuration and state, use the following command in management mode:

command	purpose
show spanning-tree	Displays spanning-tree information on current mode.
show spanning-tree detail	Displays a detailed summary of STP on current mode.
show spanning-tree interface	Displays interface information of STP on current mode.

Configuring SNMP Trap

By configuring the trap function of STP, you can monitor the changes of STP remotely from the host's network management software.

STP supports two types of Trap: newRoot and topologyChange. The switch sends a newRoot trap message when a non-root switch converts to a root switch. When the switch detects a change of topology, such as a non-edge port is changed from a non-forwarding state to a forwarding state, a topologyChange trap message will be sent.

Note:

You need to use the network management software that supports Trap to receive STP Trap. The network management software needs to import the Bridge-MIB set with the OID of 1.3.6.1.2.1.17.

Use the following command to configure STP Trap：

Run	To
spanning-tree management trap	Enable STP Trap.
[newroot | topologychange]	Enable two traps if no trap type is specified.
no spanning-tree management trap	Disable STP Trap.

9.1.4 Configuring VLAN STP

Overview

In SSTP mode, the whole network has only one STP entity. The state of the switch port in the STP decides its state in all VLANs. In the case that multiple VLANs exist in the network, the separation of the single STP and the network topology may cause communication congestion in some parts of network.

Our switches run independent SSTP on a certain number of VLANs, ensuring that the port has different state in different VLANs and that the load balance is realized between VLANs.

Note that the number of VLANs that can run STP independently depends on the actual version. Other VLAN topologies is not controlled by the STP.

VLAN STP Configuration Task

Use the following commands to configure SSTP attributes in VLAN in global configuration mode:

Command	Purpose
spanning-tree mode pvst	Starts the VLAN-based STP distribution mode.
spanning-tree vlan *vlan-list*	Distributes the STP case for the designated VLAN. vlan-list: the list of VLAN
no spanning-tree vlan *vlan-list*	Deletes the STP case in the designated VLA.
spanning-tree vlan *vlan-list* **priority** *value*	Configures the priority for the STP in the designated VLAN.
no spanning-tree *vlan-list* **priority**	Restore the STP priority in the VLAN to the default configuration.
spanning-tree vlan *vlan-list* **forward-time** *value*	Configure Forward Delay for the designated VLAN.
no spanning-tree vlan *vlan-list* **forward-time**	Restore Forward Delay of the designated VLAN to the default configuration.
spanning-tree vlan *vlan-list* **max-age** *value*	Configure Max-age for the designated VLAN.
no spanning-tree vlan *vlan-list* **max-age**	Restore Max-age of the designated VLAN to the default configuration.
spanning-tree vlan *vlan-list* **hello-time** *value*	Configure HELLO-TIME for the designated VLAN.
no spanning-tree vlan *vlan-list* **hello-time**	Restore HELLO-TIME of the designated VLAN to the default configuration.

In port configuration mode, run the following command to configure attributes of the port:

Command	Purpose
spanning-tree vlan *vlan-list* **cost**	Configure the path cost of the designated VLAN for the port.

no spanning-tree vlan *vlan-list* **cost**	Restore the default path cost of the designated VLAN for the port.
spanning-tree vlan *vlan-list* **port-priority**	Configure the port priority in the VLAN.
no spanning-tree vlan *vlan-list* **port-priority**	Restore the default port priority in the VLAN.

In monitor or configuration mode, run the following command to check the STP state in the specified VLAN:

Command	Purpose
show spanning-tree vlan *vlan-list*	Check the STP state in the VLAN.
show spanning-tree pvst instance-list	Check the corresponding relationship between PVST and VLAN

9.2 Configuring Rapid Spanning Tree Protocol(RSTP)

9.2.1 RSTP Configuration Task List

- Enabling/Disabling Switch RSTP
- Configuring the Switch Priority
- Configuring the Forward Time
- Configuring the Hello time
- Configuring the Max-Age
- Configuring the Path Cost
- Configuring the Port Priority
- Configuring Edge Port
- Configuring the Port Connection Type
- Enabling Protocol Conversation Check

9.2.2 RSTP Configuration Task

Enabling/Disabling Switch RSTP

Follow these configurations in the global configuration mode:

Run	To
spanning-tree mode rstp	Enables RSTP

no spanning-tree mode	Disable STP.

Configuring the Switch Priority

The size of the bridge determines whether the bridge can be selected as the root bridge of the entire spanning tree. By configuring a smaller priority, a bridge can be used as the root bridge of the spanning tree.

Use the following command to configure the priority in the global configuration mode:

Run	To
spanning-tree rstp priority *value*	Modifies rstp priority value.
no spanning-tree rstp priority	Returns rstp priority to default value.

Note: If the priority of all bridges in the whole switch network uses the same value, then the bridge with the least MAC address will be chosen as the root bridge. In the situation when the RSTP protocol is enabled, if the bridge priority value is modified, it will cause the recalculation of spanning tree.

The bridge priority is configured to 32768 by default.

Configuring the Forward Time

Link failures may cause network to recalculate the spanning tree structure. But the latest configuration message cannot be conveyed to the whole network. If the newly selected root port and the specified port immediately start forwarding data, this may cause temporary path loop. Therefore the protocol adopts a kind of state migration mechanism. There is an intermediate state before root port and the specified port starting data forwarding, after the intermediate state passing the Forward Delay Time, the forward state begins. This delay time ensures the newly configured message has been conveyed to the whole network. The Forward Delay characteristic of the bridge is related to the network diameter of the switch network. Generally, the grater the network diameter, the longer the Forward Delay Time should be configured.

Use the following command to configure forward delay time in the global configuration mode:

Command	purpose
spanning-tree rstp forward-time *value*	Configures Forward Delay
no spanning-tree rstp forward-time	Returns Forward Delay Time to default value (15s).

Note: If you configure the Forward Delay Time to a relatively small value, it may leads to a temporary verbose path. If you configure the Forward Delay Time to a relatively big value, the system may not resume connecting for a long time. We recommend user to use the default value.

The Forward Delay Time of the bridge is 15 seconds.

Configuring the Hello Time

The proper hello time value can ensure that the bridge detect link failures in the network without occupying too much network resources.

Use the following command to configure hello time in the global configuration mode:

Command	purpose
spanning-tree rstp hello-time *value*	Configures Hello Time
no spanning-tree rstp hello-time	Restore Hello Time to default value.

It is important to note that the Hello Time value will cause the bridge to receive hello packets for a long time because the link is lost. The bridge will consider that there is a link to fail, and then restart recalculating the spanning tree. If the Hello time is too short, it will cause the bridge to send configuration messages frequently and occupy the network bandwidth, increase the network burden and CPU burden. The default value is recommended.

The default Hello Time is 2 seconds.

Configuring the Max-Age

Max Age is the parameters used to determine whether the configuration message is outdated. The user can be based on the actual network to configure it.

Use the following command to configure the Max-Age in the global configuration mode:

Command	purpose
spanning-tree rstp max-age *value*	Configures the max-age value.
no spanning-tree rstp max-age	Restore the max-age time to default value (20s).

We recommend user to use the default value. 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 configure the 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.

Configuring the Path Cost

The path cost of the Ethernet port depends on the link rate of the port. The larger the link rate, the smaller the configuration of the parameter. When the parameter is configured as the default value, the RSTP protocol can automatically detect the Link rate of the current Ethernet port, and converted to the corresponding path cost.

Use the following command to configure the Path-Cost in the interface configuration mode:

Command	purpose
spanning-tree rstp cost *value*	Configures the path cost for an interface.
no spanning-tree rstp cost	Restore path cost to default value.

Note: Configuring the cost of the Ethernet port will cause the spanning tree to recalculate. The default value is recommended. And let the RSTP protocol to calculate the path cost of the current Ethernet port.

When the port speed is 10Mbps, the path cost of the Ethernet interface is 2000000.

When the port speed is 100Mbps, the path cost of the Ethernet interface is 200000.

Configuring the Port Priority

If a loop occurs, spanning tree uses the port priority when selecting an interface to put into the forwarding state. You can assign higher priority values (lower numerical values) to interfaces that you want selected first, and lower priority values (higher numerical values) that you want selected last. If all interfaces have the same priority value, spanning tree puts the interface with the lowest interface number in the forwarding state and blocks the other interfaces.

Follow these configurations in the interface configuration mode：

Command	purpose
spanning-tree rstp port-priority *value*	Configures the port priority for an interface.
no spanning-tree rstp port-priority	Returns the port priority to the default value.

Note: The modification of the priority of the Ethernet interface will arise the recalculation of the spanning tree.

The default Ethernet interface priority is 128.

Configuring the Edge Port

The edge port indicates that the port is connected to the terminal device on the network. A forced edge port will immediately enter the forwarding state after Link Up. In port configuration mode, use the following command to configure the RSTP edge port:

Command	purpose
Spanning-tree rstp edge	Configure the port to the edge port

In the protocol auto-detection mode, if the port does not receive BPDU for a certain period of time, the port is considered to be an edge port.

Configuring the Port Connection Type

If the switch between the RSTP-enabled switches is a point-to-point direct connection, they can quickly establish a topology through a handshake mechanism. Configuring the Port Connection Type feature allows to set the port to point-to-point connection.

By default, the protocol determines whether it is a point-to-point connection based on the duplex properties of the port. If the port is in full-duplex mode, the protocol considers it to be a point-to-point connection; if the port is in half-duplex mode, the protocol considers its connection to be shared.

If you can check that the switch connected to the port is running RSTP or MSTP, you can set the connection type of the port to point to point to ensure fast handshake

In the port configuration mode, use the following command to set the port connection type:

Command	purpose
Spanning-tree rstp point-to-point [force-true | force-false |auto]	Configure point-to-point port. force-true: forced to point-to-point type. force-false: forced to other type not point-to-point type. auto: The protocol automatically detects the port

Enabling Protocol Conversion Check

RSTP protocol allows switch to cooperate with traditional 802.1D STP switch via a kind of protocol conversion mechanism. If one interface of the switch receives configuration information of STP, then this interface will be converted to the one that only sends STP packet.

When an interface enters STP-compatible state, this interface won't returns to RSTP state even this interface no longer receives 802.1D STP BPDU. To return an interface to RSTP mode, user can use the spanning-tree rstp migration-check command to enable protocol conversion check process on an interface.

Only switches supporting IEEE 802.1D 2004 RSTP support the migration-check command.

In global configuration mode, run the following command to restart the RSTP conversion check:

Command	purpose
spanning-tree rstp migration-check	Restart the protocol conversion check on all ports.

In port configuration mode, run the following command to perform the protocol conversion check on the port:

Command	purpose
spanning-tree rstp migration-check	Restart the protocol conversion check on the current port.

9.3 Configuring MTSP

9.3.1 MSTP Overview

Introduction

Multiple Spanning Tree Protocol (MSTP) is used to create simple complete topology in the bridging LAN. MSTP can be compatible with the earlier Spanning Tree Protocol (STP) and Rapid Spanning Tree Protocol (RSTP).

Both STP and RSTP only can create sole STP topology. All VLAN messages are forwarded through the only STP. STP converges too slow, so RSTP ensures a rapid and stable network topology through the handshake mechanism.

MSTP inherits the rapid handshake mechanism of RSTP. At the same time, MST allows different VLAN to be distributed to different STPs, creating multiple topologies in the network. In networks created by MSTP, frames of different VLANs can be forwarded through different paths, realizing the load balance of the VLAN data.

Different from the mechanism that VLAN distributes STP, MSTP allows multiple VLANs to be distributed to one STP topology, effectively reducing STPs required to support lots of VLANs.

MST Domain

In MSTP, the relationship between VLAN and STP is described through the MSTP configuration table. MSTP configuration table, configuration name and configuration edit number makes up of the MST configuration identifier.

In the network, interconnected bridges with same MST configuration identifier are considered in the same MST region. Bridges in the same MST region always have the same VLAN configuration, ensuring VLAN frames are sent in the MST region.

IST, CST, CIST and MSTI

Figure 2.1 shows an MSTP network, including three MST regions and a switch running 802.1D STP.

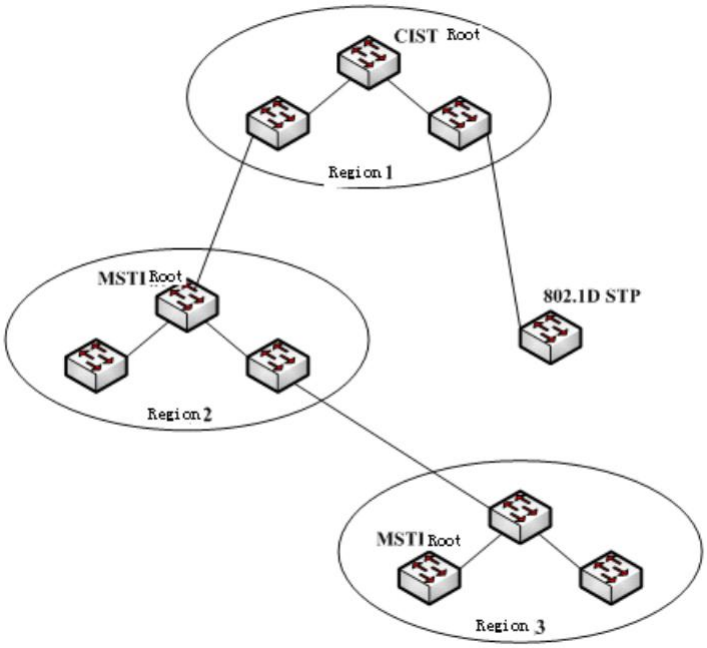


Figure3- 1 MSTP topology

CIST

Common and Internal Spanning Tree (CIST) means the spanning tree comprised by all single switches and interconnected LAN. These switches may belong to different MST regions. 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 choosed in each region, which is the shortest path from the heart of the region to CIST root.

CST

If each MST region is viewed as a single switch, Common Spanning Tree (CST) is the spanning tree connecting all “single switches”. As shown in Figure 2.1, region 1, 2 and 3 and STP switches make up of the network CST.

IST

Internal Spanning Tree (IST) refers to part of CIST that is in an MST region, that is, IST and CST make up of the CIST.

MSTI

The MSTP protocol allows different VLANs to be distributed to different spanning trees. Multiple spanning tree instances are then created. Normally, No.0 spanning tree instance refers to CIST, which can be expanded to the whole network. Every spanning tree instance starting from No.1 is in a certain region. Each spanning tree instance can be distributed with multiple VLANs. In original state, all VLANs are distributed in CIST.

MSTI in the MST region is independent. They can choose different switches as their own roots. For example, in area 3 of Figure 2.1, the root bridge of MSTI01 may be the switch in the lower left corner, and MSTI00, that is, the root bridge in the CIST area, may be the switch in the middle.

Port Role

Ports in MSTP can function as similar roles to ports in RSTP.

- Root port

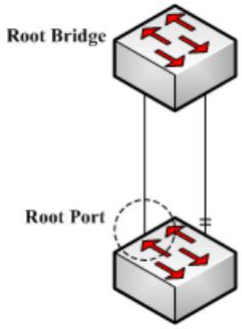


Figure3- 2 Root port

Root port stands for the path between the current switch and the root bridge, which has minimum root path cost.

- Alternate port

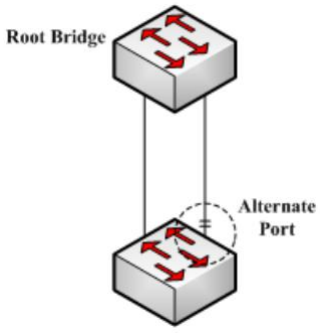


Figure3- 3 Alternate port

The alternate port is a backup path between the current switch and the root bridge. When the connection of root port is out of effect, the alternate port can promptly turn into a new root port without work interruption.

- Designated port

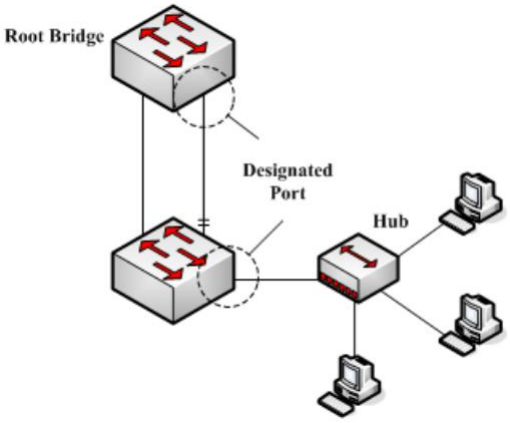


Figure3- 4 Designated port

The designated port can connect switches or LAN in the next region. It is the path between the current LAN and root bridge.

- Backup port

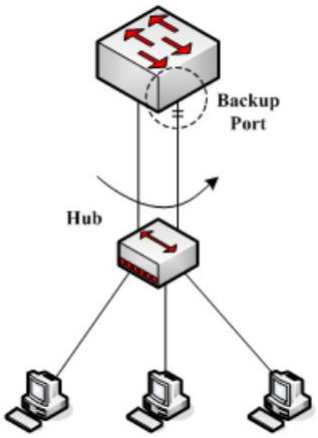


Figure3- 5 Backup port

When two switch ports directly connect or both connect to the same LAN, the port with lower priority is to be the backup port, the other port is to be the designated port. If the designated port breaks down, the backup port becomes the designated port to continue working.

- Master port

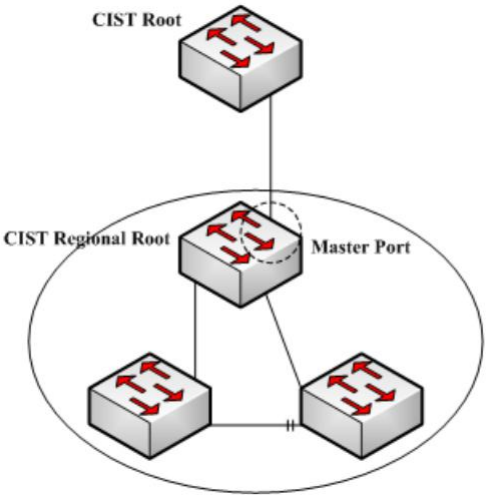


Figure3- 6 Master port

The Master port is the shortest path between MST region and CIST root bridge. Master port is the root port of the root bridge in the CIST region.

- Boundary port

The concept of boundary port in CIST is a little different from that in each MSTI. In CIST, the boundary port represents the port that connects to another MSTP port; in the MSTI, the role of the boundary port means that the spanning tree instance does not expand on the port.

- Edge port

In the RSTP protocol or MSTP protocol, edge port means the port directly connecting the network host. These ports can directly enter the forwarding state without causing any loop in the network.

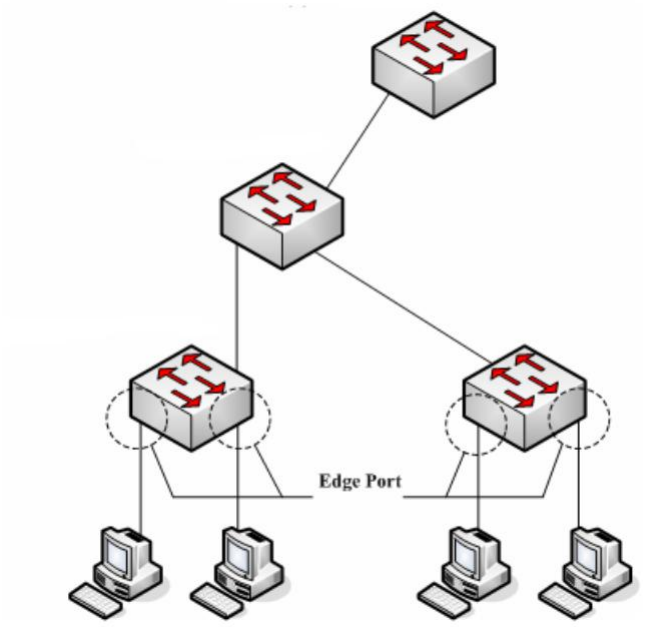


Figure3- 7 Edge port

In original state, MTSP and RSTP do not take all ports as edge ports, ensuring the network topology can be rapidly created. In this case, if a port receives BPDU from other switches, the port is resumed from the edge state to the normal state. If the port receives 802.1D STP BPDU, the port has to wait for double Forward Delay time and then enter the forwarding state.

MSTP BPDU

Similar to STP and RSTP, switches running MSTP can communicate with each other through Bridge Protocol Data Unit (BPDU). All configuration information about the CIST and MSTI can be carried by BPDU. Chart and Chart 9.3.2 list the structure of BPDU used by the MSTP.

Chart 9.3.1 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 ~

Chart 9.3.2 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

Stable State

The MSTP switch performs calculation and compares operations according to the received 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 minimum cost 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 cost path to the MSTI root.

6) The root port of CIST provides the minimum-cost path between the CIST regional root and the CIST root.

7) The designated port of the CIST provided its LAN with the minimum-cost path to the CIST root.

8) The Alternate port and the Backup port provide 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 MSTI regional 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 master port of all MSTI in the region.

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 uses Hop Count to calculate the network topology.

To prevent information from looping, MSTP relates the transmitted information to the attribute 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 each receiving 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.

STP Compatibility

MSTP allows the switch to work with the traditional STP switch through protocol conversion 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.

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 mstp migration-check** to clear the STP message that the port learned, and make the port to return to the MSTP state.

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.

9.3.2 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 edge port
- Configuring port connection type
- Activating MST-compatible mode
- Restarting protocol conversion check
- Configuring the role of the port restrictions
- Configuring the TCN restrictions for the port
- Checking MSTP information

9.3.3 MSTP Configuration Task

Default MSTP Configuration

Attribute	Default Settings
STP mode	RSTP (PVST, RSTP and MSTP is not started)
Area name	Character string of MAC address
Area edit level	0
MST configuration list	All VLANs are mapped in CIST (MST00).
Spanning-tree priority (CIST and all MSTI)	32768
Spanning-tree port priority (CIST and all MSTI)	128
Path cost of the spanning-tree port (CIST and all MSTI)	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

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
spanning-tree	Disable the STP.

Configuring MST Area

The MST area where the switch resides is decided by three attributes: configuration name, 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 MAC address 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 designated 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 configuration name. 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** represents the instance number of the spanning tree, meaning an MSTI. It ranges from 1 to 15. **vlan-list** means the VLAN list that is mapped to the spanning tree. It ranges from 1 to 4094. **instance-id** is an independent value representing a spanning tree instance. **vlan-list** can represent a group of VLANs, such as "1,2,3", "1-5" and "1,2,5-10".
no spanning-tree mstp instance *instance-id*	Cancels the VLAN mapping of MSTI and disables the spanning tree instance. instance-id represents the instance number of the spanning tree, meaning an MSTI. It ranges from 1 to 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.

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 switch through configuration. You can run the command **Spanning-tree mstp instance-id rootroot** to modify the 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 previous command is executed, the protocol automatically check the bridge ID of the current network root and then sets the priority field of the bridge ID to **24576** when the value **24576** ensures that the current switch becomes the root of the spanning tree.

If the network root's priority value is smaller than the value **24576**, MSTP automatically sets the spanning tree's priority of the current bridge to a value that is 4096 smaller than the priority value of the root. Note that the number **4096** is a step length of network priority value.

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 Hello Time, Forward Delay and Maximum Age. The subcommand Hello-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 tree instance. **instance-id** represents the number of the spanning tree instance, ranging from 0 to 15. **net-diameter** represents the network diameter, which is an optional parameter. It is effective when instance-id is 0. It ranges from 2 to 7. **seconds** represents the unit of the hello time, ranging from 1 to 10.
no spanning-tree mstp *instance-id* **root**	Cancels the root configuration of the switch in the spanning tree. **instance-id** means the number of the spanning tree instance, 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.

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 backup roots. If the root does not function for certain reasons, the secondary roots will become the network root.

Different from the primary root configuration, after the command to configure the primary root is run, MSTP sets the spanning tree priority of the switch to 28672. In the case that the priority value of other switches is the default value 32768, the current switch can be 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 tree instance, ranging from 0 to 15. **net-diameter** represents the network diameter, which is an optional parameter. It is effective when instance-id is 0. It ranges from 2 to 7. **seconds** represents the unit of the hello time, ranging from 1 to 10.
no spanning-tree mstp *instance-id* **root**	Cancels the root configuration of the switch in the spanning tree. **instance-id** means the number of the spanning tree instance, ranging from 0 to 15.

Run the following command to check the MSTP message:

Command	Purpose
show spanning-tree mstp **[instance** *instance-id* **]**	Check the message about the MST instance.

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 each spanning 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 tree instance, ranging from 0 to 15. value represents the priority of the bridge. It can be one of the 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 default value. **instance-id** means the number of the spanning tree

	instance, ranging from 0 to 15.

Configuring STP Time Parameters

The following are STP time parameters:

- **Hello Time**:

The interval is to send the configuration message to the designated port when the switch functions as the network root.

- **Forward Delay**:

Time that the port needs when it changes from the Blocking state to the learning state and to the forwarding state in STP mode.

- **Max Age**:

The maximum live period of the STP configuration information.

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

Command	Purpose
spanning-tree mstp hello-time *seconds*	Sets the parameter **Hello Time**. The parameter **seconds** is the unit of Hello Time, ranging from 1 to 10 seconds. Its default value is two seconds.
no spanning-tree mstp hello-time	Resumes **Hello Time** to the default value.
spanning-tree mstp forward-time *seconds*	Sets the parameter **Forward Delay**. The parameter **seconds** is the unit of **Forward Delay**, ranging from 4 to 30 seconds. Its 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**. The parameter **seconds** is the unit of **Max Age**, ranging from 6 to 40 seconds. Its default value is 20 seconds.
no spanning-tree mstp max-age	Resumes **Max Age** to the default value.

It is recommended to modify STP time parameters by setting root or network diameter, which ensures correct modification of time parameters.

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.

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-tree mstp diameter *net-diameter***. The parameter **net-diameter** is valid only to CIST. After configuration, three STP time parameters are automatically updated to comparatively better values.

Run the following command to configure **net-diameter**:

Command	Purpose
spanning-tree mstp diameter *net-diameter*	Configure **net-diameter**. The parameter **net-diameter** ranges from 2 to 7. The default value is 7.
no spanning-tree mstp diameter	Resumes **net-diameter** to the default value.

The parameter **net-diameter** is not saved as an independent setup in the switch. Only when modified by setting the network diameter can the time parameter be saved.

Configuring Maximum Hop Count

Run the following command to configure the maximum hop count.

Command	Purpose
spanning-tree mstp max-hops *hop-count*	Set the maximum hops. **hop-count** ranges from 1 to 40. Its default value is 20.
no spanning-tree mstp *hop-count*	Resume the maximum hop count to the default value.

Configuring Port Priority

If a loop occurs between two ports of the switch, the port with higher priority will enter the **forwarding** state and the port with lower priority is blocked. If all ports have the same 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 STP port:

Command	Purpose
spanning-tree mstp *instance-id* **port-priority** *priority*	Sets the priority of the STP port. **instance-id** stands for the number of the spanning tree instance, ranging from 0 to 15.

	priority stands for the port priority. It can be one of the following 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** stands for the port priority. It 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.

Configuring Path Cost of the 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 same path 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** stands for the number of the spanning tree instance, ranging from 0 to 15. **cost** stands for the path cost of the port, which ranges from 1 to 200000000.128, 144, 160, 176, 192, 208, 224, 240
spanning-tree cost *value*	Sets the path cost of the port in all spanning tree instances. **Value** stands for the path cost of the port, which ranges from 1 to 200000000.
no spanning-tree mstp *instance-id* **cost**	Resumes the path cost of the port to the default value.
no spanning-tree cost	Resumes the path cost of the port to the default value in all spanning tree instances.

Configuring Edge Port

The edge port indicates that the port is connected to the terminal device on the network. A forced edge port will immediately enter the forwarding state after Link Up. In port configuration mode, configure the MSTP edge port by using the following command:

Command	Purpose
Spanning-tree edge force-true	Configure the port to an edge port.
No spanning-tree mstp edge	Restore the default automatically detected edge ports.

Configuring Port Connection Type

If the connection between MSTP-supported switches is the point-to-point direct connection, the switches can rapidly establish connection through handshake mechanism. When you configure the port connection type, you can set the port connection to the point-to-point type.

The protocol decides whether to use the point-to-point connection or not according to the duplex attribute. If the port works in full-duplex mode, the protocol considers the connection is a point-to-point one. If the port works in the half-duplex mode, the protocol considers the connection is a shared one.

If the switch that connects the port runs the RSTP protocol or the MSTP protocol, you can set the port connection type to **point-to-point**, ensuring that a handshake is rapidly established.

In port configuration mode, run the following command to set the port connection type.

Command	Purpose
spanning-tree mstp point-to-point force-true	Sets the port connection type to **point-to-point**.
spanning-tree mstp point-to-point force-false	Sets the port connection type to **shared**.
spanning-tree mstp point-to-point auto	Automatically checks the port connection type (default).
no spanning-tree mstp point-to-point	Resumes the port connection type to the default settings.

Activating MST-Compatible Mode

The MSTP protocol that our switches support is based on IEEE 802.1Q. In order to be compatible with other MSTPs, especially MSTP that the Cisco switches support, 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 MSTP protocol 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 mstp migration-check**.

In global configuration mode, run the following commands to enable or disable the MSTP-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 MSTP area for switches and other MSTP-running switches. 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-compatible content and take the content as the common RSTP BPDU. In this way, the switch cannot be in the same area with the MST-compatible switch that it connects.

A port in compatible mode cannot automatically resumes to send standard MST BPDU even if the compatible mode is shut down in global configuration mode. In this case, run **migration-check**.

Restarting Protocol Conversion Check

MSTP allows the switch to work with the traditional STP switch through protocol conversion 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. Similarly, in MST-compatible mode, if a port receives a BPDU in compatible mode, the port will also transmit a BPDU in compatibility mode.

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 mstp migration-check** to clear the STP message that the port learned, and make the port to return to the MSTP state.

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 information that 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 information detected by the port.

Command	Purpose
spanning-tree mstp migration-check	Clears STP information detected by the port.

Configuring the Role of the Port Restrictions

Configure the port's role restrictions so that the port will not be selected as the root port.

In port configuration mode, use the following command to configure the port's role restrictions:

Command	Purpose
Spanning-tree mstp restricted-role	Make the port not to be selected as the root port.

Configuring the TCN Restrictions for the Port

Configuring the TCN restriction of a port can make the port not to spread the topology changes to other ports.

In port configuration mode, use the following command to configure the TCN restriction for the port:

Command	Purpose
Spanning-tree mstp restricted-tcn	Make the port not to spread the topology changes to other ports.

Check MSTP Information

In monitor command, global configuration command or port configuration command, 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 the details of 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.

Chapter 10 STP Optional Characteristics Configuration Commands

10.1 STP Optional Characteristic Introduction

The spanning tree protocol module of the switch supports seven additional features (the so-called optional features). These features are not configured by default. The supported condition of various spanning tree protocol modes towards the optional characteristics is as follows:

Optional Characteristic	Single STP	PVST	RSTP	MSTP
Port Fast	Yes	Yes	No	No
BPDU Guard	Yes	Yes	No	No
BPDU Filter	Yes	Yes	Yes	Yes
Uplink Fast	Yes	Yes	Yes	Yes
Backbone Fast	Yes	Yes	No	No
Root Guard	Yes	Yes	No	No
Loop Guard	Yes	Yes	No	No

10.1.1 Port Fast

Port Fast immediately brings an interface to the forwarding state from a blocking state, bypassing the listening and learning states. You can use Port Fast on interfaces connected to a single workstation or server, to allow those devices to immediately connect to the network.

The Port Fast feature is applicable to the ports of the directly connected hosts. These ports do not receive BPDUs and do not affect the network topology. Therefore, they can enter the forwarding state without waiting. If you enable Port Fast on an interface connecting to another switch, you risk creating a spanning-tree loop.

The Port Fast feature can be set in global or port configuration mode. If configured in global mode, all ports are considered to be Port Fast ports and enter the Forwarding state quickly. This is also more prone to loop. To prevent network loops due to the configuration of the Port Fast function, you can use the BPDU Guard or BPDU Filter feature to protect the ports.

Note：

For the rapid convergent STP, RSTP and MSTP, can immediately bring an interface to the forwarding state, and therefore there is no need to use Port Fast feature.

10.1.2 BPDU Guard

If a Port Fast port receives a BPDU, it can be thought of as a result of the wrong network configuration. The BPDU Guard feature is protected passively after receiving a BPDU on a Port Fast port.

The BPDU Guard is different in different STP modes. In SSTP / PVST mode, a Port Fast port with BPDU guard configured. If a BPDU is received, the port is forced to shutdown. After that, the user can only restore it by manually configuring it. In RSTP / MSTP mode, a port configured with BPDU Guard will receive the BPDU and the port will be set to Blocking for a period of time.

The BPDU Guard feature can be configured independently of Port Fast. In all STP modes, ports configured with BPDU guard do not send BPDU, but the port can receive BPDU and do with them. In RSTP / MSTP mode, BPDUs cannot be received on devices connected to the switch by configuring BPDU Guard on the ports connected to the host.

The BPDU Guard feature can be configured in global or port configuration mode. In the global configuration mode, the spanning-tree portfast bpduguard command prevents all ports from sending BPDU. It should be noted that in a more complex network, improper use of BPDU Guard function may lead to loop.

10.1.3 BPDU Filter

The BPDU filtering feature allows the switch's ports to send BPDU in SSTP / PVST mode, as well as another protection for Port Fast ports.

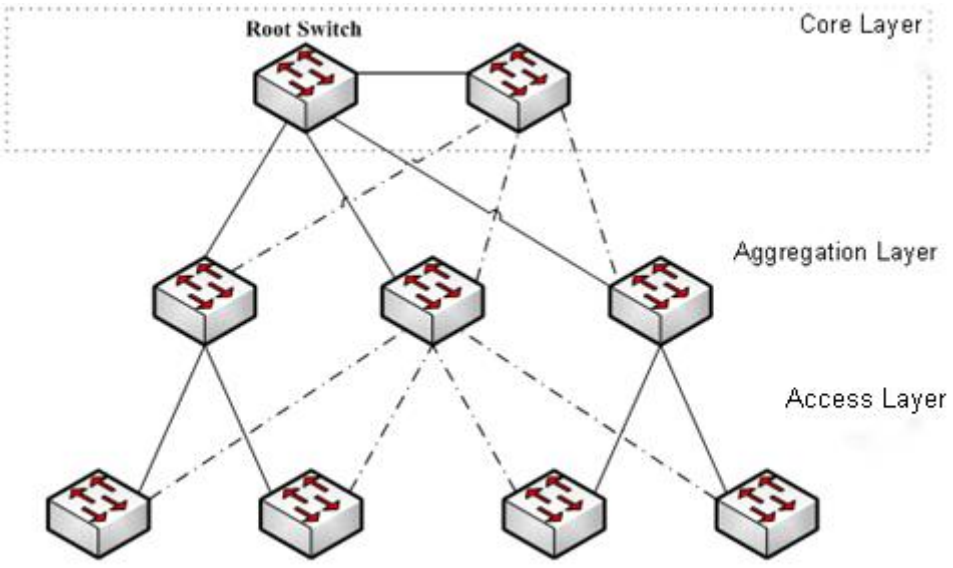
In SSTP/PVST mode,.if a **Port Fast** port with BPDU filter configured receives the BPDU, the features BPDU Filter and Port Fast at the port will be automatically disabled, resuming the port as a normal port. Before entering the **Forwarding** state, the port must be in the **Listening** state and **Learning** state.

The BPDU Filter feature can be configured in global configuration mode or in port configuration mode. In global configuratiom mode, run the command **spanning-tree portfast bpdufilter** to block all ports to send BPDU out. The port, howerver, can still receive and process BPDU.

10.1.4 Uplink Fast

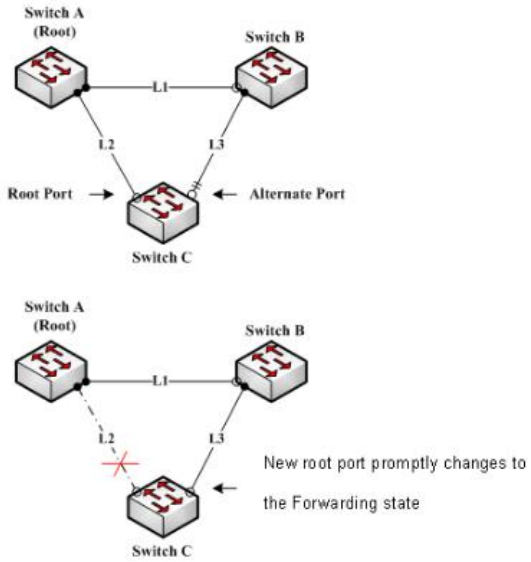
The feature **Uplink Fast** enables new root ports to rapidly enter the **Forwarding** state when the connection between the switch and the root bridge is disconnected.

A complex network always contains multilayers of devices, as shown below. 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.



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.

Below picture shows the working principle of the **Uplink Fast** feature. The port for switch C to connect switch B is the standby port when the port is in the original state. When the connection between switch C and root switch A is disconnected, the previous Alternate port is selected as new root port and immediately be forwarding.



Note:

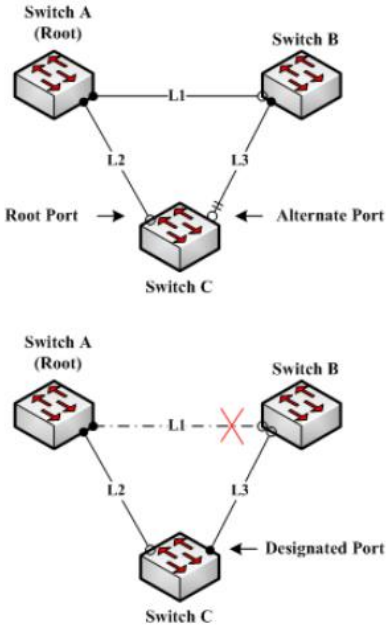
The **Uplink Fast** feature adjusts to the slowly convergent SSTP and PVST. In RSTP and MSTP mode, new root port can rapidly enter the Forwarding state without the **Uplink Fast** function.

10.1.5 Backbone Fast

The **Backbone Fast** feature 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 above picture, 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 switches A and B is called as the indirect link of switch 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 below picture.



Suppose the bridge priority of switch C is higher than that of switch B. When L1 is disconnected, switch B is selected to send BPDU to switch C because the bridge priority is used as root priority. To switch C, the information contained by BPDU is not prior to information contained by its own. When Backbone Fast is not enabled, the port between switch C and switch 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 switch C receives a BPDU with lower priority, switch C thinks that an indirect-link and root-switch-reachable connection on the port is disconnected. Switch 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 feature is effective in SSTP and PVST modes.

10.1.6 Root Guard

The Root Guard feature prevents a port from turning into a root port because of receiving high-priority BPDU.

In a more complex two-tier network, the administrator may want a core layer of the switch as the root bridge of the network, but he cannot manage all the switch of the access layer (probably because the access layer switches belong to other customers). In this way, improper configuration of other switches may cause the core switch to fail to become a root.

You can prevent the root bridge role from being exploited by a switch outside the managed area by configuring the root guard function on the edge switch. If a port configured with a root guard receives a higher-level BPDU as Root Port, Root Guard automatically sets the port to a blocked state and restores it to an assigned port.

In PVST and MSTP mode, Root Guard can work independently in each spanning tree instance. In MSTP mode, if a border port is blocked in the CIST because the Root Guard is blocked, the port is blocked in all other MSTIs. A border port is a port that connects to a LAN host, an STP switch, an RSTP switch, or an MSTP switch outside the zone.

You can enable this feature by using the **spanning-tree guard root** interface configuration command.

Note：

Root Guard feature 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.

10.1.7 Loop Guard

The Loop Guard feature protects a Root Port or Alternate Port into a Designated Port, which prevents loops due to the failure of the port to receive BPDUs continuously.

You can use the spanning-tree loopguard default global configuration command to enable the loopback function of the switch. After a boot, a Root port or alternate port will be set to a blocked state if it becomes a designated port. If the port re-receives the high priority BPDU after a period of time, it will automatically recover from the Loop Guard.

In PVST and MSTP mode, Loop Guard can work independently in each spanning tree instance. In MSTP mode, if a border port is blocked in the CIST because Loop Guard is blocked, the port is blocked in all other MSTIs.

Note：

Loop Guard feature acts differently somehow in SSTP/PVST and RSTP/MSTP. In SSTP/PVST mode, the designated port is always be blocked by Loop Guard. In RSTP/MSTP mode, the port will be blocked only when it changes into the designated port because of inaccessibility to receiving BPDU. Loop Guard will not block a port, which is provided with the designated role due to receiving the lower level BPDU.

10.2 Configuring STP Optional Characteristic

10.2.1 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

10.2.2 Configuring Port Fast

Port Fast feature in SSTP / PVST mode can make a port immediately into the Forwarding state without having to wait from Listening to Learning state. This function is invalid in other spanning tree 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	Enables port fast feature on the interface.
no spanning-tree portfast	Disables port fast feature on the interface. It has no effect on the global configuration.

10.2.3 Configuring BPDU Guard

The BPDU Guard feature performs a protection action when a port receives a BPDU. The port configured with the feature does not send BPDUs.

BPDU Guard is different in different spanning tree protocol modes. In SSTP / PVST mode, a port with BPDU Guard and Port Fast features is forced to shut down if a BPDU is received. After that, the user can only restore it by manually configuring it. In RSTP / MSTP mode, a port configured with BPDU Guard will receive the BPDU and the port will be set to Blocking for a period of time.

Follow these steps to globally enable the BPDU guard feature：

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.

Follow these steps to enable the BPDU guard feature in 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	Disable bpdu guard feature on the interface. It has no effect on the global configuration.

10.2.4 Configuring BPDU Filter

The BPDU Filter feature makes the switch's ports not to send BPDUs in the SSTP / PVST mode, as well as another means of protection for Port Fast ports.

Follow these steps to enable the BPDU filter feature in global configuration mode.：

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.

Follow these steps to enable 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. It has no effect on the global configuration.
no spanning-tree bpdufilter	Disables bpdu filter feature. It has no influence on the global configuration.

10.2.5 Configuring Uplink Fast

The Uplink Fast feature can make the new root port to enter the Forwarding state quickly when the connection between the switch and the network root bridge is interrupted.

Uplink Fast feature is only valid in SSTP/PVST mode.

Use the following command to enable UplinkFast in global configuration mode：

Command	Purpose
spanning-tree uplinkfast	Enables uplink fast feature.
no spanning-tree uplinkfast	Disables uplink fast feature.

10.2.6 Configuring Backbone Fast

The Backbone Fast feature is a complement to Uplink Fast technology. Uplink Fast makes the redundant lines work quickly when the direct connection to the assigned switch is interrupted. And Backbone Fast can detect the non-directly connected network outages in the upper layer and accelerate the status of the port.

Backbone fast feature is only valid in SSTP/PVST mode.

Use the following command to enable BackboneFast in global configuration mode：

Command	Purpose
spanning-tree backbonefast	Enables backbone fast feature.
no spanning-tree backbonefast	Disables backbone fast feature.

10.2.7 Configuring Root Guard

The Root Guard feature prevents a port from becoming a root port because it receives a high priority BPDU.

Root Guard feature 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 enable root guard on an interface in global 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.

10.2.8 Configuring Loop Guard

The Loop Guard feature protects a Root Port or Alternate Port into a Designated Port, which prevents loops due to the failure of the port to receive BPDUs continuously.

Loop Guard feature acts differently somehow in SSTP/PVST. In SSTP/PVST mode,, the designated port is always blocked by Loop Guard. In RSTP/MSTP, the designated port is always blocked by Loop Guard. In RSTP/MSTP mode, the port will be blocked only when it changes into the designated port because of inaccessibility to receiving BPDU. A port which is provided with the designated role due to receiving the lower level BPDU will not be blocked by Loop Guard.

Use the following command to enable loop guard in global configuration mode：

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 enable loop guard 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 feature on the interface.
spanning-tree guard none	Disables root guard and loop guard on the interface.

10.2.9 Configuring Loop Fast

Note:

Please use the configuration commands described in this section under the guidance of the technician.

The Loop Fast feature is used to increase the convergence of the network in a particular network environment. For example, in a ring composed of dozens of switches for each of the ring network to enable the characteristics of the port.

Use the following command to enable loop fast in global configuration mode：

Command	Purpose

spanning-tree loopfast	Enable loop fast globally which is valid for all ports.
no spanning-tree loopfast	Disable loop fast globally.

Use the following command to enable loop fast in interface configuration mode：

Command	Purpose
spanning-tree loopfast	Enable loop fast for port.
no spanning-tree loopfast	Cancel loop fast for port. If Loop Fast is configured globally, it is still valid on the port.
spanning-tree loopfast disable	Disable loop fast for port.

10.2.10 Configuring Address Table Aging Protection

In the case of frequent network topology changes, configuring the address table aging protection function can avoid STP affecting the communication due to frequent update of MAC address table.

Fast convergence of spanning tree protocols, such as RSTP and MSTP, will perform a cleanup on the MAC address table of the switch when the spanning tree topology changes, delete the old MAC address, and update the MAC address to ensure fast communication restore. By default, the switch performs the cleanup operation through the MAC address table. For most models of switches, the rapid aging of the address table can be completed within 1 second, and have almost no effect on the performance of the device CPU.

After the address table aging protection function is enabled, the STP protocol will start the protection timer after the first aging. The timer will not be aged before the timer expires (default is 15 seconds). If the network topology changes within 15 seconds, the protocol will automatically perform a second aging after the timer expires

Note:

By **no spanning-tree fast-aging**, the STP protocol can completely disable the aging of the address table. Before executing this configuration, make sure that there is no loop on the network. Otherwise, it may take 5 minutes or more for the terminal device to resume communication after the network topology changes.

Use the following command to configure the address table aging protection in global configuration mode：

Command	Purpose
Spanning-tree fast-aging	Enable/disable the address table aging.
Spanning-tree fast-aging protection	Enable/disable the address table aging protection.
Spanning-tree fast-aging protection time	Configure the address table for aging protection. Within

this time, the STP can only perform an address table aging.

The default value is 15s.

Add no before the command to cancel the corresponding configuration.

10.2.11 Configuring FDB-Flush

Note:

Please use the configuration commands described in this section under the guidance of the technician.

The Rapid Spanning Tree Protocol (RSTP and MSTP) of the switch clears the old MAC address, rather than FDB-Flush, using the address table for quick aging by default.

Use the following command to configure FDB-Flush in global configuration mode:

Command	Purpose
Spanning-tree fast-aging flush-fdb	Enable FDB-Flush.
No spanning-tree fast-aging flush-fdb	Disable FDB-Flush.

Note that FDB-Flush is independent of fast aging, and you can configure **FDB-Flush** while configuring **no spanning-tree fast-aging**. But the fast aging protection function is not valid for FDB-Flush.

Chapter 11 MAC Address Configuration Commands

11.1 MAC Address Configuration Task List

- Configuring Static Mac Address
- Configuring Mac Address Aging Time
- Displaying Mac Address Table
- Clearing Dynamic Mac Address

11.2 MAC Address Configuration Task

11.2.1 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 the management mode.
write	Saves configuration.

11.2.2 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.

11.2.3 Displaying MAC Address

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.

11.2.4 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 is dynamically acquired. 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.

Chapter 12 Link Aggregation Configuration Commands

This chapter is taking about how to configure port aggregation for a switch

12.1 Overview

Port aggregation, that is, several physical properties of the same physical port aggregation can be bound together to form a logical channel. The aggregation mode of a port can be static aggregation of several physical ports regardless of whether the ports connected to these physical ports meet the aggregation conditions. When aggregating with the LACP protocol, the aggregation of the ports must be negotiated with the peer end and the port, then the port will be aggregated into a logical channel.

Supported Features:

- Supporting static aggregation control

Bind a physical port to a logical port, regardless whether they can actually bind to a logical port.

- Supporting aggregation control of LACP dynamic negotiation

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.

- Supporting flow balance of port aggregation

After port aggregation, the data flow of the aggregation port will be distributed to each aggregated physical port.

12.2 Port Aggregation Configuration Task List

- Configuring logical channel used for aggregation
- Aggregation of physical port
- Selecting load balance mode after port aggregation
- Monitoring the concrete condition of port aggregation

12.3 Port Aggregation Configuration Task

12.3.1 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.

Use the following command to configure the logical channel:

Command	Purpose
interface port-aggregator id	Configures the logical channel of aggregation.

12.3.2 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.

When using the LACP protocol, the port aggregation must be negotiated with the peer and the port connected to the port. The primary condition that the port can be aggregated is that the port must be LinkUp and the port negotiates the full-duplex mode. During the aggregation process, the Speed of all the physical member ports must be consistent. That is, if a physical port has been successfully aggregated. At this point, the Speed of the second physical port must be the same as the Speed of the physical port that has been successfully aggregated; the VALN attribute of all physical ports and aggregation ports must also be consistent.

LACP provides two aggregation methods, one is Active, the other is Passive mode. In Active mode, the switch initiates the aggregation negotiation process, and in passive mode, it is passive to accept the aggregation negotiation process. When choosing LACP polymerization, 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	Purpose
aggregator-group *agg-id* **mode { lacp | static }**	Configures aggregation option of the physical port.

12.3.3 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

It is to share the data traffic according to the source MAC address, that is, the 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	Purpose
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.

12.3.4 Monitoring the Concrete Conditions of Port Aggregation

Use the following command to monitor port aggregation state in the management mode:

Command	Purpose
show aggregator-group	Displays port aggregation state.

Chapter 13 GVRP Configuration Commands

13.1 Introduction

GVRP (GARP VLAN Registration Protocol GARP VLAN) is a specific GARP (GARP VLAN Registration Protocol GARP VLAN) application. It uses the working mechanism of the GARP protocol to maintain the VLAN information in the switch. All the switches that support the GVRP feature can receive the VLAN registration information from other switches and dynamically update the local VLAN registration information, including the current VLAN members as well as which VLAN members can reach through which port and other information. At the same time, all the switches that support the GVRP feature can communicate the local VLAN registration information (including dynamic VLAN information and statically configured VLAN information) to other switches to match that the VLAN information of all the devices which support GVRP is the same in the same switching network.

13.2 Configuring Task List

13.2.1 GVRP Configuration Task List

- Enabling/Disabling GVRP Globally
- Enabling/Disabling GVRP on the Interface
- Monitoring and Maintenance of GVRP

13.3 GVRP Configuration Task

13.3.1 Enabling/Disabling GVRP Globally

Perform the following configuration in global configuration mode.

Command	Purpose
[no] gvrp	Enables/disables GVRP globally.

It is disabled by default.

13.3.2 Enabling/Disabling GVRP on the Interface

Perform the following configuration in interface configuration mode:

Command	Purpose
[no] gvrp	Enables/disables interface GVRP.

Before enabling port GVRP, please enable global GVRP first. Otherwise, GVRP on the interface does not work. And only the GVRP function can be configured on the trunk port. Otherwise, the port GVRP function will not work.

It is enabled by default.

13.3.3 Monitoring and Maintenance of GVRP

Perform the following operations in the management mode:

Command	Purpose
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.

13.4 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 8 that Switch A connects to Switch B to trunk:

Switch_config_g0/8# switchport mode trunk

(2) Enable global GVRP of switch A:

Switch_config#gvrp

(3) Enable GVRP of interface 8 of Switch A:

Switch_config_g0/8#gvrp

(4) Configure VLAN 10, Vlan 20 and Vlan30 on Switch A

Switch_config#vlan 10

Switch_config#vlan 20

Switch_config#vlan 30

(5) Configure the interface 9 that Switch A connects to Switch B to trunk:

Switch_config_g0/9# switchport mode trunk

(6) Enable global GVRP of switch B:

Switch_config#gvrp

(7) Enable GVRP of interface 9 of Switch B

Switch_config_g0/9#gvrp

(8) Configure VLAN 40, Vlan 50 and Vlan60 on Switch B

Switch_config#vlan 40

Switch_config#vlan 50

Switch_config#vlan 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.

Chapter 14 IGMP-SNOOPING Configuration Commands

14.1 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 includes Listening IGMP message; Maintaining the relationship table between VLAN and group address; 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

14.1.1 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.

By default, 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.

14.1.2 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.

14.1.3 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.

14.1.4 Configuring the Function to Filter Multicast Message without Registered Destination Address

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-frames *filter*	Drops multicast message whose destination fails to be found.
no ip igmp-snooping dlf-frames	Resumes the fault configuration (forward).

Note:

1) The attribute is configured for all VLANs.

2） The default method for the switch to handle this type of message is forward (message of this type will be broadcasted within VLAN).

14.1.5 Configuring Router Age Timer of IGMP-snooping

The Router Age timer is used to monitor whether the IGMP inquirer exists. IGMP inquirer maintains multicast addresses by sending query message. IGMP-snooping works through communication between IGMP inquirer 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, please 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.

14.1.6 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 default value of Response Time of IGMP-snooping is set to ten seconds.

14.1.7 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)

When the multicast router does not exist in LAN and multicast flow does not need 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.

14.1.8 Monitoring and Maintaining IGMP-Snooping

Perform the following operations in management mode:

Command	Description
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
igmp-snooping response time:10 s
vlan 1
------------
   running
   Router: 90.0.0.120(F0/2)
```

Display information about the multicast group of IGMP-snooping:

```
switch#show ip igmp-snooping groups
Vlan Source                Group                Type Port(s)
---- --------------- --------------- ---- ---------------------------------------
     1 0.0.0.0             234.5.6.6            IGMP F0/2
     1 0.0.0.0             239.255.255.250 IGMP F0/2
```

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:

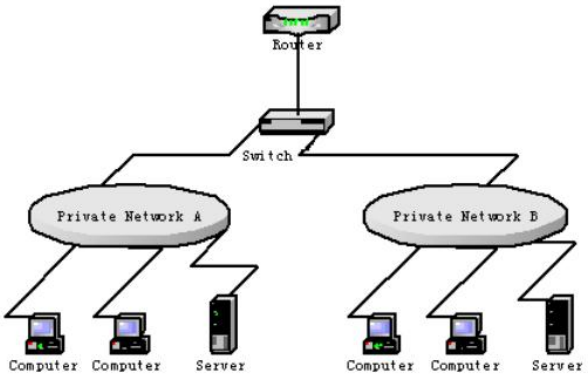
```
switch#debug ip igmp-snooping packet
rx: s_ip:90.0.0.3, d_ip:224.0.8.9    Source and destination IP addresses where packets are received
        type:16(V2-Report), max resp:00, group address:224.0.8.9    Type and content of packet
rx: s_ip:90.0.0.90, d_ip:224.0.0.1
        type:11(Query), max resp:64, group address:0.0.0.0
rx: s_ip:90.0.0.3, d_ip:224.0.8.9
        type:16(V2-Report), max resp:00, group address:224.0.8.9
rx: s_ip:90.0.0.3, d_ip:224.0.0.2
        type:17(V2-Leave), max resp:00, group address:224.0.8.9
rx: s_ip:90.0.0.90, d_ip:224.0.8.9
        type:11(Query), max resp:0a, group address:224.0.8.9
```

Debug the message timer of IGMP-snooping:

```
switch#debug ip igmp-snooping timer
tm: vlan 1 igmp router age expiry at port 2(F0/2)
tm: multicast item 0.0.0.0->224.0.8.9(0100.5e00.0809) response time expiry at port F0/4    Inquerying the response timer expiry
```

14.1.8 IGMP-Snooping Configuration Example

Below Figure shows network connection of the example.



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

Chapter 15 802.1x Configuration Commands

15.1 802.1x Configuration Task List

- Configuring 802.1x port authentication
- Configuring 802.1x multiple host authentication
- Configuring 802.1x re-authentication
- Configuring 802.1x transmission frequency
- Configuring 802.1x user binding
- Configuring authentication method for 802.1x port
- Selecting authentication type for 802.1x port
- Configuring mab port authentication
- Configuring 802.1x accounting
- Configuring guest-vlan
- Forbidding Supplicant with multiple network cards
- Resuming default 802.1x configuration
- Monitoring 802.1x authentication configuration and state

15.2 802.1x Configuration Task

15.2.1 Configuring 802.1x Port Authentication

802.1x defines three control methods for the port: mandatory authentication approval, mandatory authentication disapproval and 802.1x authentication startup.

Mandatory authentication approval means the port has already passed authentication. The port does not need any authentication any more, and all users can perform data access control through the port. The authentication method is defaulted by the port. Mandatory authentication disapproval means the port authentication does not get passed no matter what kind of method is applied. No user can perform the data access control through the port.

802.1x authentication startup means the port is to run 802.1x authentication protocol. 802.1x authentication will be applied to users who access the port. Only users who pass the authentication can perform data access control through the port. After the 802.1x authentication is started up, the AAA authentication method must be configured.

Run the following command to enable the 802.1x function before configuring 802.1x:

Run	To
dot1x enable	Enable the 802.1x function.

Run the following command to start up the 802.1x authentication:

Run	To
dot1x port-control auto	dot1x port-control auto
Configure the 802.1x protocol control method on the port.	Configure the 802.1x protocol control method on the port.

Run one of the following commands in port configuration mode to select 802.1x control method:

Run	To
dot1x port-control auto	Start up the 802.1x authentication method on the port.
dot1x port-control force-authorized	Approve the mandatory port authentication.
dot1x port-control force-unauthorized	Disapprove the mandatory port authentication.

15.2.2 Configuring 802.1x Multiple Host Authentication

802.1x authentication is for the authentication of single host user. In this case, the switch allows only one user to perform authentication and access control. Other users cannot be authenticated and access unless the previous user exits authentication and access. In the case the port connects multiple hosts through switch devices, such as 1108 switch, that do not support 802.1x, you can start up the multiple Host access function to make sure that all host users can access.

After a port is configured to multiple host authentication of 802.1x, the switch authenticates different host users. When authentication is approved, the host will be allowed to access through the switch (the MAC address of host is used for control). Theoretically, 802.1x cannot limit the number of host users. Because the switch controls the user authentication through the MAC address of user, the number of host users will be limited by the size of the MAC address table of the switch.

Multi-host authentication is divided into two types, one is the **multiple-hosts** mode: when the user host authentication, only one of the hosts through the certification, the port will be set to up state, and do not need to other users host authentication including the host before or after the request for authentication; the other is the **multiple-auth** mode: the switch will be authenticated for each host user, each user authentication does not affect each other, that this certification does not affect before or after Certification. Once there is a user authentication success, the port is on the up. And only when all users are certified failure, that is, authentication port does not exist the successful authentication users, the port is down. It ensures that each user is authenticated separately, and a user authentication failure does not affect the normal access rights of other users.

Note:

multi-auth mode and guest vlan function cannot be configured at the same time, and mab authentication cannot be configured at the same time. After modifying the multiuser authentication mode of the port, all users on the port are re-authenticated.

Run the following command in interface configuration mode to activate 802.1x multiple host authentication:

Run	To
dot1x authentication multiple-hosts	Set the 802.1x multiple port authentication. Once a user authentication success, the port is on the up
dot1x authentication multiple-auth	Set the 802.1x multiple port authentication. The port will be up only when all host pass the authentication.

15.2.3 Configuring 802.1x Re-authentication

After first authentication is approved, the client will be authenticated every a certain time to ensure the legality of the client. In this case, the re-authentication function needs to be enabled.

After the re-authentication function is enabled, 802.1x will periodically send the authentication request to the host.

You can run the following commands to configure the re-authentication function.

Run	To
dot1x re-authentication	Enable the re-authentication function.
dot1x timeout re-authperiod time	Configure the period of re-authentication.
dot1x reauth-max time	Configure the retry times after the re-authentication fails.

15.2.4 Configuring 802.1x Transmission Frequency

In the process of 802.1x authentication, data texts will be sent to the host. The data transmission can be adjusted by controlling 802.1x transmission frequency so that the host response is successful.

Run the following command to configure the transmission frequency:

Run	To
dot1x timeout tx-period *time*	Set the message transmission frequency of 802.1x.

15.2.5 Configuring 802.1x User Binding

When 802.1x authentication is performed, you can bind a user to a certain port to ensure the security of port access. Run the following command in interface configuration mode to start up 802.1x user binding.

Run	To
dot1x user-permit *xxx*	Configure a user that is bound to a port.

15.2.6 Configuring Authentication Method for 802.1x Port

The 802.1x authentication can be performed in different methods at different ports. In the default configuration, the 802.1x authentication adopts the **default** method.

Run the following command in interface configuration mode to configure the method of the 802.1x authentication:

Run	To
dot1x authentication method *yyy*	Configure the method of the 802.1x authentication.

15.2.7 Selecting Authentication Type for 802.1x Port

You can select the type for the 802.1x authentication. The 802.1x authentication type determines whether AAA uses Chap authentication or Eap authentication. Eap authentication supports the md5-challenge mode and the eap-tls mode. Challenge required by MD5 is generated locally when the Chap authentication is adopted, while challenge is generated at the authentication server when the eap authentication is adopted. Each port adopts only one authentication type. The authentication type of global configuration is adopted by default. Once a port is set to an authentication type, the port will use the authentication type unless you run the **No** command to resume the default value.

Eap-tls takes the electronic certificate as the authentication warrant and complies with the handshake rules in Translation Layer Security (tls). Therefore, high security is guaranteed.

Run the following command in global configuration mode to configure the authentication type:

Run	To
dot1x authen-type {**chap**|**eap**}	Select chap or eap.

Also run the following command in interface configuration mode:

Run	To
dot1x authentication type {**chap**|**eap**}	Select chap or eap or the configured authentication type in global mode.

15.2.8 Configuring Mab Port Authentication

When the opposite end cannot use the 802.1x client software, the switch uses the Mab (MAC Authentication Bypass) authentication method, and send the MAC address of the opposite end as a user name and password to the radius server to authenticate.

Note: The dot1x mabformat command can be used to specify the account and password format on the switch to ensure that it matches the settings on the radius server.

After the mab function is enabled, if the peer device does not send eapol_start packets or respond to the request_identity packet, the switch considers that the peer device does not support the 802.1x authentication client and goes to the mab authentication process after timeout. The switch sends the mac address of the acquired device as the user name and password to the radius server for authentication.

If the MAC address is authorized on the radius server, the authentication is succeeded. The switch allows the user to access the network through the port.

Note: When you enable mab authentication, you cannot configure the multi-auth multi-host authentication mode at the same time.

Run the following command in global configuration mode to enable mab authentication:

Run	To
dot1x mab	Enable mab authentication.

Also run the following command in interface configuration mode to configure the format of mac address:

Run	To
dot1x mabformat{1|2|3|4|5|6}	Select the format of mac address from 1 to 6. The default value is 1.

15.2.9 Configuring 802.1x Accounting

The 802.1x authentication and 802.1x accounting can be performed at the same time. It working mechanism is: after the dot1x authentication is approved, judge whether the accounting function is enabled on the authentication interface; if the accounting function is enabled, send the accounting request through the AAA interface; when the AAA module returns successful request response message, the AAA interface can forward texts.

The accounting can adopt various accounting methods configured in the AAA module. For details, refer to AAA configuration.

After the beginning of accounting, dot1x periodically sends **update** message to the server through the AAA interface for obtaining correct accounting information. According to different AAA configuration, the AAA module decides whether to send the **update** message.

At the same time, you are required to enable the dot1x re-authentication function so that the switch can know when supplicant is abnormal.

Run the following commands in interface configuration mode to enable the dot1x accounting and to configure the accounting method:

Run	To
dot1x accounting enable	Enable the dot1x accounting.
dot1x accounting method {*method name*}	Configure the accounting method. Its default value is **default**.

15.2.10 Configuring 802.1x guest-vlan

Guest-vlan gives relevant ports some access rights (such as downloading client software) when the client does not respond. Guest-vlan can be any configured vlan in the system. If the configured guest-vlan does not meet the conditions, ports cannot run in the guest-vlan.

Note:

There is no access right if the authentication fails.

Run the following command in the global mode to enable the guest-vlan:

Run	To
Dot1x guest-vlan	Enable the guest-vlan at all ports.

When the original value of **guest-vlan id** at each port is 0, guest-vlan cannot function even if guest-vlan is enabled in global mode. Only when **guest-vlan id** is configured in port configuration mode, guest-vlan can function.

Run the following command in port configuration mode to configure **guest-vlan id**:

Run	To
Dot1x guest-vlan {id(1-4094)}	Enable guest-vlan at all ports.

15.2.11 Forbidding Supplicant with Multiple Network Cards

Forbid the Supplicant with multiple network adapters to prevent agents. Run the following command in port configuration mode:

Run	To
dot1x forbid multi-network-adapter	Forbid the Supplicant with multiple network adapters.

15.2.12 Resuming Default 802.1x Configuration

Run the following command to resume all global configurations to the default configuration:

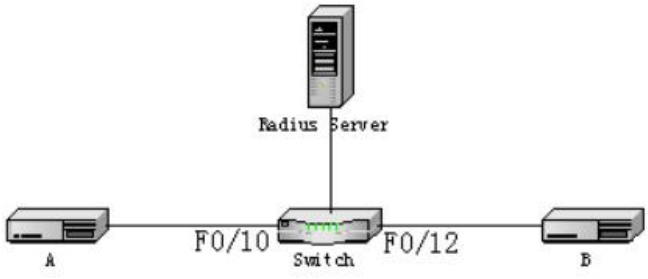
Run	To
dot1x default	Resume all global configurations to the default configuration.

15.2.13 Monitoring 802.1x Authentication Configuration and State

To monitor the configuration and state of 802.1x Authentication and decide which 802.1x parameter needs to be adjusted, run the following command in management mode:

Run	To
show dot1x {*interface …***}**	Monitor the configuration and state of 802.1x authentication.

15.3 802.1x Configuration Example



Host A connects port F0/10 of the switch. Host B connects port F0/12. The IP address of the radius-server host is 192.168.20.2. The key of radius is TST. Port F0/10 adopts remote radius authentication and user binding. Port F0/12 adopts local authentication of eap type, and Multi-hosts are enabled at Port F0/12.

Global configuration

username switch password 0 TST

username TST password 0 TST

aaa authentication dot1x TST-F0/10 radius

aaa authentication dot1x TST-F0/12 local

interface VLAN1

ip address 192.168.20.24 255.255.255.0

radius-server host 192.168.20.2 auth-port 1812 acct-port 1813

radius-server key TST

Configuring port F0/10

interface FastEthernet0/10

dot1x port-control auto

dot1x authentication method TST-F0/10

dot1x user-permit radius-TST

Configuring port F0/12

interface FastEthernet0/12

dot1x multiple-hosts

dot1x port-control auto

dot1x authentication method TST-F0/12

dot1x authentication type eap

Chapter 16 MAC Access List Configuration Commands

16.1 MAC Access List Configuration Task

16.1.1 Creating MAC Access List

To apply the MAC list on the port, you must first create the MAC list. After the MAC access list is successfully created, you log in to the MAC access 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.

16.1.2 Configuring Items of MAC Access 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 access 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 access 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.

16.1.3 Applying MAC Access List

The created MAC list can be applied on any physical port. One port can only be applied with one MAC access list. The same MAC list can be applied to multiple ports.

Enter the privilege mode and perform the following operation to configure the MAC access 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 access list.
exit	Enter the global configuration mode again.
exit	Enter the management mode again.
write	Save configuration.

Chapter 17 Physical Port IP Access List Configuration Commands

17.1 Physical Port IP Access List Configuration

17.1.1 Filtering IP Message

Filtering message helps control the running of packets in the network. This control can constrain network transmission or limit network usage through user or device. To enable or disable packets on the crossly specified port, our routing switches provide the access list. The access list can be used through the following methods:

- Controlling packet transmission on the port
- Controlling the access of virtual terminal line
- Limiting routing update content

The section describes how to create and use the IP access list.

The IP access list is an orderly set IP of applying the allowed and forbidden conditions of IP address. The ROS software of our routing switches is to test the addresses in the access list one by one. The first match decides whether the software to accept or reject the address. Because the ROS software stops the match rules after the first match, the order of conditions is very important. If rule match does not exist, the address is to be rejected.

You need to perform the following steps before using the access list:

- Create the IP access list by specifying the access list name and access conditions.
- Apply the IP access list to the port.

17.1.2 Creating Standard and Extensible IP Access List

Use a character string to create an IP access list.

Note:

The standard IP access list and the extensible IP access list cannot use the same name.

Run the following commands in global configuration mode to create a standard IP access list:

Run	To
ip access-list standard *name*	Use name to define a standard IP access list.
deny {*source [source-mask]* | **any**} or **permit** {*source [source-mask]* | any}	Specify one or multiple permit/reject conditions in standard IP access list configuration mode, which decides whether the packet is approved or disapproved.
Exit	Log out from the IP access list configuration mode.

Run the following commands in global configuration mode to create an extensible IP access list:

Run	To
ip access-list extended *name*	Use a name to define an extensible IP access list.
{deny | permit} *protocol source source-mask destination destination-mask* **[precedence** *precedence***] [tos** *tos***]** **{deny | permit}** *protocol* **any any**	Specify one or multiple **deny** or **permit** conditions in extensible access list configuration mode, which decides whether the IP packet is passed or not (**precedence** means the priority of the IP packet. **TOS** is the simplified form of Type of Service).
Exit	Log out of the access list configuration mode.

After the access list is originally created, any part added later (may be entered from the terminal) is put at the end of the list, that is, 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 name access list.

Note:

When you create the access list, remember that the end of the access list contains the invisible **deny** sentence. In another word, if the mask is not specified in relevant IP address access list, 255.255.255.255 is supposed to be the mask.

After the access list is created, it must be applied to the line or the port. Refer to section 1.3 "Applying the Access List to Port".

17.1.3 Applying the Access List to Port

After the access list is created, you can apply it to one or multiple ports or entries.

Run the following command in port configuration mode:

Run	To
ip access-group *name*	Apply the access list to the port.

For the standard entry access list, when the packet is received, the source address of the access list checking packet will be checked. For the extensible access list, the routing switch also checks the destination address. If the access list permits the destination address, the software continues to handle the packet. If the access list denies the destination address, the software drops the packet and returns a message that the ICMP host is unreachable.

If the designated access list does not exist, all packets are allowed to get through.

17.1.4 Extensible Access List Example

In the following example, the first line allows the new TCP to connect to the SMTP port of host 130.2.1.2.

ip access-list extended aaa

permit tcp any 130.2.1.2 255.255.255.255 eq 25

interface f0/10

ip access-group aaa

Chapter 18 QoS Configuration

If you care to use your bandwidth and network resources efficiently, you must pay attention to QoS configuration.

18.1 QoS Overview

18.1.1 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 is 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.

18.1.2 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 single service model. In this service model, an application can send any amount of data at any necessary time without application of permits or beforehand 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).

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).

18.1.3 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 until the highest-priority has no 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. 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.

18.2 QoS Configuration Task List

In general, the 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 the switch.
- The following are QoS configuration tasks:
- Setting the Global CoS Priority Queue
- Setting the Bandwidth of the CoS Priority Queue
- Setting the Schedule Policy of the CoS Priority Queue
- Setting the Schedule Standard for the CoS Priority Queue
- Setting the Default CoS Value 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
- Displaying the QoS Policy Mapping Table
- Setting the Rate Limit on a Port

18.3 QoS Configuration Tasks

18.3.1 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 a global CoS priority queue.

Command	Purpose
configure	configure Enters the global configuration mode.
[no] cos map *quid cos1..cosn* **(1~8)**	Sets a 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 management configuration mode.
write	Saves the settings.

18.3.2 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
configure	Enters the global configuration mode.
[no] scheduler weight bandwidth *weight1...weightn* **(1~8)**	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 management configuration mode.
write	Saves the settings.

18.3.3 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 four 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.
- FCFS: First come first served
- WRR (Weighted Round Robin): 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 packet as its unit.
- DRR(Deficit Round Robin): 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.

After this command is configured, the schedule mode of the interface is set to the designated value.

Enter the following configuration mode and set the schedule policy of CoS priority queue.

Command	Purpose
configure	Enters the global configuration mode.
[**no**] **scheduler policy** { **sp** | **fcfs** | **wrr** | **drr** }	Sets the schedule policy of the CoS priority queue. **sp** means to use the SP schedule policy. **fcfs** means to use the FCFS schedule policy. **wrr** means to use the WRR schedule policy. **drr** means to use the DRR schedule policy.
exit	Goes back to the management configuration mode.
write	Saves the settings.

18.3.4 Setting the Schedule Standard for the CoS Priority Queue

The schedule benchmark of priority queue is the scale standard of bandwidth distribution ratio of different priority queues when the schedule policy of the CoS priority queue is set to WRR/DRR. There are mainly two standards:

- packet-count: means that the occupied bandwidth is expressed by the number of packets.

- byte-count: means that the occupied bandwidth is expressed by the size of packet.
- latency: means that the occupied bandwidth is expressed by the transmitted time segment.

This switch series supports the **packet-count** and **byte-count** schedule standards. Wrr is based on packet-count, while drr is based on byte-count.

18.3.5 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 set the default CoS value fir a port according to the following steps:

Command	Purpose
configure	Enters the global configuration mode.
interface g0/1	Enters the to-be-configured port.
[no] cos default cos (0~7)	Configure the CoS value of untagged frames received by the port. Cos is the corresponding cos value.
exit	Goes back to the global configuration mode.
exit	Goes back to the management configuration mode.
write	Saves the settings.

18.3.6 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
configure	Enters the global configuration mode.
interface g0/1	Enters the to-be-configured port.
[no] cos map *quid cos1..cosn* **(1~8)**	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 management configuration mode.

18.3.7 Establishing the QoS Policy Mapping

Flow classification means to identify a class of packets with certain attributes by applying a certain regulation and take designated actions towards to these packets.

The IP access list and the MAC access list which are used to match up with the data flows can be configured only one regulation, or the configuration will fail. When the action in the regulation is **permit**, the regulation is used to differentiate the data flows; when the action in the regulation is **deny**, the regulation has no function. The port ID in the IP access list must be a certain value and cannot be a range.

You can establish a QoS policy according to the following procedure. During configuration, you can set all the parameters of the QoS policy, that is, **description**, **classify** and **action**, or one or two of them. In the following section you can also edit the policy.

Enter the privileged mode and then run the following commands to establish a new QoS policy mapping.

Command	Purpose
configure	Enters the global configuration mode.
[no]policy-map *name*	Enters the configuration mode of 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.
[no]classify {*ip access-list-name* **| dscp** *dscp-value* **| mac** *mac-access-name* **| vlan** *vlan-id* **| cos cos-value | any }**	Configures the data flow of the QoS policy map. **access-list-name** stands for the name of the IP access list. **dscp-value** means to designate the **diffserv** field in the IP packet. **mac-access-name** stands for the name of the MAC access list. **vlan-id** stands for the ID of the matched VLAN. cos stands for the matched CoS value. **any** means to match any data flow.
action{bandwidth *max-band* **| cos cos-value | dscp**	Configures the data flow policy of the QoS policy map.

dscp-value **| redirect** *interface-id* **| drop | stat | monitor }**	**max-band** stands for the highest bandwidth allowably occupied by a data flow. **cos-value** means to set the CoS field of the matchup flow to **cos-value**. **dscp-value** means to set the DSCP field of the matchup flow to **dscp-value**. **interface-id** means to redirect the egress port of the matched flow. **drop** means to discard the configured packets. **stat** means a switch collects the statistics of the corresponding matchup flows. **monitor** means to transmit a packet to the mirror port.
exit	Goes back to the global configuration mode.
exit	Goes back to the management configuration mode.

18.3.8 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 setting will replace the previous settings.

Command	Purpose
configure	Enters the global configuration mode.
[no]policy-map *name*	Enters the configuration mode of 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 management configuration mode.

18.3.9 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 matchup data flow of policy and replace the previous settings with this data flow according to the following steps:

Command	Purpose
configure	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.
[no]classify {ip *access-list-name* **| dscp** *dscp-value* **| mac** *mac-access-name* **| vlan** *vlan-id* **| cos cos-value | any }**	Configures the matchup data flow of the QoS policy map. **access-list-name** stands for the name of the IP access list. **dscp-value** stands for the diffserv field in the IP packet. **Mac-access-name** stands for the name of the MAC access list. **vlan-id** stands for the ID of the matched VLAN. **cos** stands for the matched CoS value. **any** means to match any data flow.
exit	Goes back to the global configuration mode.
exit	Goes back to the management configuration mode.

18.3.10 Setting the Actions of the Matchup 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
configure	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* **| cos cos-value | dscp dscp-value | vlanID vlanid-value | redirect**	Configures the matchup data flow of the QoS policy map.

interface-id | drop | stat | monitor }	**access-list-name** stands for the name of the IP access list. **dscp-value** stands for the diffserv field in the IP packet. **Mac-access-name** stands for the name of the MAC access list. **vlan-id** stands for the ID of the matched VLAN. **cos** stands for the matched CoS value. **any** means to match any data flow.
exit	Goes back to the global configuration mode.
exit	Goes back to the management configuration mode.

18.3.11 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 will be first applied. 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
configure	Enters the global configuration mode.
interface g0/1	Enters the configuration mode of the QoS policy map. **name** stands for the name of the policy.
[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 management configuration mode.

18.3.12 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.

18.3.13 Configuring Rate Limit on a Port

Through configuration the flow rates at the ingress and the egress can be limited.

Enter the privileged mode and run the following commands to limit the rate of a port.

Command	Purpose
configure	Enters the global configuration mode.
interface g0/1	Enters the to-be-configured port.
[no] switchport rate-limit *band* **(1~1000)** { ingress|egress}	Configures the rate limit for a port. *band* means to limit the flow rate. *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 management configuration mode.

18.4 QoS Configuration Example

18.4.1 Example for Applying the QoS Policy on a Port

After you have set on a port a policy that the CoS value of the packet is set to 2 and apply it, you have to set another policy to allow all data flows to pass through, or all data flows will be hindered. See the following example:

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 any

classify any

policy-map pmap

classify ip ipacl

action cos 2

interface GigaEthernet0/2

qos policy pmap ingress

qos policy any ingress (pay attention to the order of applying the two policies)

Chapter 19 Layer 2 Protocol Tunnel Configuration Commands

19.1 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.

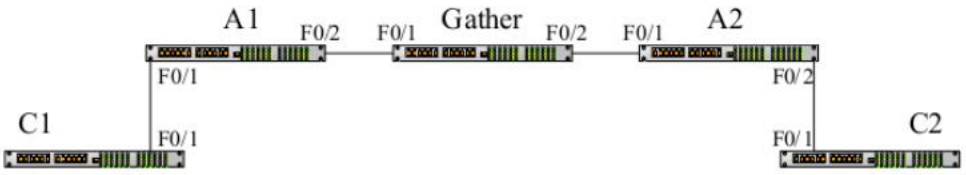
19.2 Configuring Layer 2 Protocol Tunnel

Use command line on the interface of the switch to configure tunnel function of the layer 2 protocol. The configuration steps are as follows:

Command	Purpose
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 management configuration mode.
write	Saves configuration.

19.3 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 transparent transmission of STP, then the following configurations should be configured on each switch:

The f0/2 of Switch A1, f0/1 and f0/2 of Gather, f0/1 of A2 should be configured to trunk mode.

The f0/1 of switch A1, f0/2 of A2 should be configured to Access, and enables tunnel function of the STP protocol.

Chapter 20 Security Configuration Commands

20.1 AAA Configuration Commands

20.1.1 AAA Overview

Access control is the way to control access to the switch and the network access service. Authentication, authorization, and accounting (AAA) network security services provide the primary framework to improve network security performance.

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—Provide the method of identifying users, including login and password dialog, and encryption depending on the security protocol you select.

Authentication is the way that a user is identified prior to being allowed access to the network and network services. You configure AAA authentication by defining a named list of authentication methods, and then applying that list to various interfaces. The method list defines the types of authentication to be performed and the sequence in which they will be performed; it must be applied to a specific interface before any of the defined authentication methods will be performed. The only exception is the default method list (which is named "default"). The default method list is automatically applied to all interfaces if no other method list is defined. A defined method list overrides the default method list. For more information, please refer to the chapter "Configuring Authentication."

Authorization—Provide the method for remote access to control the privilege of user's server.

AAA authorization works by assembling a set of attributes that describe what the user is authorized to perform. These attributes are compared to the information contained in a database for a given user and the result is returned to AAA to determine the user's actual capabilities and restrictions. The database can be located locally on the access server or router or it can be hosted remotely on a RADIUS or TACACS+ security server. Remote security servers, such as RADIUS and TACACS+, authorize users for specific rights by associating attribute-value (AV) pairs, which define those rights with the appropriate user. All authorization methods must be defined through AAA. For more information, please refer to the chapter "Configuring Authorization."

Accounting—Provides the method for collecting and sending security server information used for billing, auditing, and reporting, such as user identities, start and stop times, executed commands (such as PPP), number of packets, and number of bytes.

Accounting enables you to track the services users are accessing as well as the amount of network resources they are consuming. When AAA accounting is activated, the network access server reports user activity to the RADIUS or TACACS+ security server (depending on which security method you have implemented) in the form of accounting records. Each accounting record is comprised of accounting AV pairs and is stored on the security server. This data can be analyzed for network management, client billing, and/or auditing. All accounting methods must be defined through AAA. As with authentication and authorization, you configure AAA accounting by defining a named list of accounting methods, and then applying that list to various interfaces. For more information, please refer to the chapter "Configuring Accounting."

Benefits of Using AAA

AAA provides the following benefits:

Flexible and ease to control

Easy to upgrade

Standardized authentication methods, such as RADIUS, TACACS+

Multiple backup systems

AAA Principles

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

Method Lists

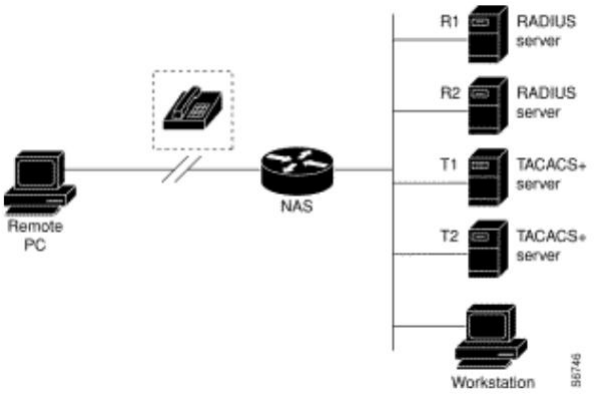
To configure an AAA, define a method list of name first and then apply the list to a specific service or interface. The list of methods defines all AAA types to be executed and the order in which they are to be executed; any method list defined must be applied to a specific interface or service before being executed. The only exception is the default method list (default). The default method list is automatically applied to all interfaces or services. Unless the interface explicitly refers to other method list, the method list will override the default method list.

A method list is a sequential list that defines the authentication methods used to authenticate a user. Method lists enable you to designate one or more security protocols to be used for authentication, thus ensuring a backup system for authentication in case the initial method fails. The software of our switches use the first method listed to authenticate users; if that method does not respond, 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.

Note:

The 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 username database responds by denying the user access—the authentication process stops and no other authentication methods are attempted.

The following figures show a typical AAA network configuration that includes four security servers: R1 and R2 are RADIUS servers, and T1 and T2 are TACACS+ servers.



Typical AAA Network Configuration

In this example, default is the name for method list, including listing the protocol in the method list and the order in which they are to be queried after the method list name. The default 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. If all of the authentication methods return errors, the network access server will process the session as a failure, and the session will be terminated.

Note:

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. Because of this, no authentication has been attempted. Only when an ERROR is detected, will AAA select the next authentication method defined in the authentication method list.

Suppose that the system administrator wants to apply the method list only to a particular port or a specific port. In this case, the system administrator should create a list of non-default methods and then apply the named list to the appropriate port.

20.1.2 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.

Overview of the AAA Configuration Process

Configuring AAA is relatively simple after you understand the basic process involved. To configure security on our switches or access server using AAA, follow this process:

- If you decide to use a security server, configure security protocol parameters, such as RADIUS, TACACS+.
- 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.

20.1.3 AAA Authentication Configuration Task List

- Configuring Login Authentication Using AAA
- Configuring PPP Authentication Using AAA
- Enabling Password Protection at the Privileged Level
- Configuring Message Banners for AAA Authentication
- AAA authentication username-prompt
- AAA authentication password-prompt
- Establishing Username Authentication
- Establishing Local Privilege Level Authentication Database

20.1.4 AAA Authentication Configuration Task

To configure AAA authentication, perform the following configuration processes：

(1) If you decide to use a security server, configure security protocol parameters, such as RADIUS, TACACS+.

(2) Define the method lists for authentication by using an AAA authentication command.

(3) Apply the method lists to a particular interface or line, if required.

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.

To configure login authentication by using AAA, use the following commands in global configuration mode:

Command	Purpose
aaa authentication login {default | *list-name*}*method1* [*method2*...]	Create global authentication list.
line [console | vty] *line-number* [*ending-line-number*]	Enters line configuration mode.
login authentication {default | *list-name*}	Applies the authentication list to a line or set of lines.

The list-name is a character string used to name the list you are creating. The method argument refers to the actual method the authentication algorithm tries. 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 **default** to create a default list, and the default list is automatically applied to all interfaces. For example, to specify RADIUS as the default authentication method for user login, use the following command:

aaa authentication login default group radius

Note:

Because the keyword none 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 when login in, in addition to the console port login, any other form of login will end with the fail certification.

The following table lists the supported login authentication methods.：

Keyword	Purpose
enable	Uses the enable password for authentication.

group *name*	Uses named server group for authentication.
group radius	Uses the list of all RADIUS servers for authentication.
line	Uses the line password for authentication.
local	Uses the local username database for authentication.
local-case	Uses case-sensitive local username authentication.
none	Uses no authentication.

(1) Login Authentication Using Enable Password

Use the aaa authentication login command with the enable method keyword to specify the enable password as the login authentication method. For example, to specify the enable 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 enable

(2) Login Authentication Using Line Password

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) Login Authentication Using Local Password

Use the aaa authentication login command with the local method keyword to specify that the Cisco router or access server will use the local username database for authentication. For example, to specify the local username database as the method of user authentication at login when no other method list has been defined, enter 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 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 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."

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	Purpose
enable	Uses the enable password for authentication.
group *group-name*	Uses the naming server group for authentication
group radius	Uses the list of all RADIUS hosts for authentication.
line	Uses the line password for authentication.
none	Uses no authentication.

When the enable authentication method is configured as remote authentication, RADIUS is used for authentication. Following is the description:

(1) Use RADIUS for enable authentication

The user name is $ENABLElevel$, and level is the privilege level that the user wants to enter. For example, if a user wants to enter a privilege level of level 7, enter the command enable 7. If RADIUS authentication is configured for authentication, the user name for the Radius-server host is $ENABLE7$. By default, the privilege level entered is 15, that is, when using RADIUS for authentication, the user name for Radius-server host is $ENABLE15$. It is necessary to configure the corresponding user name and password on the Radius-server host in advance. In particular, in the user database of the Radius-server host, specify the service type (Service-Type) of the user for privileged authentication is 6 which is Admin-User.

Configuring Message Banners for AAA Authentication

AAA supports the use of configurable, personalized login and failed-login banners. You can configure message banners that will be displayed when a user logs in to the system to be authenticated using AAA and when, for whatever reason, authentication fails.

(1) Configuring a Login Banner

Use the following commands in global configuration mode:

Keyword	Purpose
aaa authentication banner *delimiter text-string delimiter*	Creates a personalized login banner.

(2) Configuring a Failed-Login Banner

Use the following commands in global configuration mode:

Keyword	Purpose
aaa authentication fail-message *delimiter text-string delimiter*	Creates a message to be displayed when a user fails login.

(3) Instruction

To create a login banner, you need to configure a delimiting character, which notifies the system that the following text string is to be displayed as the banner, and then the text string itself. The delimiting character is repeated at the end of the text string to signify the end of the banner.

AAA authentication username-prompt

To change the text displayed when users are prompted to enter a username, use the aaa authentication username-prompt command in global configuration mode. To return to the default username prompt text, use the no form of this command:

Username:

The aaa authentication username-prompt command does not change any dialog that is supplied by a remote TACACS+ server or RADIUS server. Use the following command to configure in global configuration mode:

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

AAA authentication password-prompt

To change the text displayed when users are prompted for a password, use the aaa authentication password-prompt command in global configuration mode. To return to the default password prompt text, use the no form of this command:

password:

The aaa authentication password-prompt command does not change any dialog that is supplied by a remote TACACS+ server or RADIUS server. Use the following command to configure in global configuration mode:

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

Establishing Username Authentication

You can create a username-based authentication system, which is useful in the following situations:

Provide authentication method for users when it does not support AAA server (such as RADIUS).

To provide special-case logins: for example, access list verification, no password verification, autocommand execution at login, and "no escape" situations.

To establish username authentication, use the following commands in global configuration mode as needed for your system configuration. Use the no form of this command to delete a username.

username *name* **{nopassword | password** *password* **| password encryption-type** *encrypted-password***}**

username *name* **[autocommand** *command***]**

username *name* **[callback-dialstring** *telephone-number***]**

username *name* **[callback-rotary** *rotary-group-number***]**

username *name* **[callback-line [tty | aux]** *line-number* **[***ending-line-number]***]**

username *name* **[noescape] [nohangup]**

username *name* **[privilege** *level***]**

username *name* **[user-maxlinks** *number***]**

no username *name*

Establishing Local Privilege Level Authentication Database

To set a local password to control access to various privilege levels, use the enable password command in global configuration mode. To remove the password requirement, use the no form of this command.

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

no enable password [**level** level]

20.1.5 AAA Authentication Configuration Example

1. RADIUS Authentication Example

This section provides one sample configuration using RADIUS.

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 radius

line vty

login authentication radius-login

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

- The aaa authentication login radius-login radius local command configures the router to use RADIUS for authentication at the login prompt. If RADIUS returns an error, the user is authenticated using the local database.
- The aaa authentication ppp radius-ppp radius command configures the software to use PPP authentication using CHAP or PAP if the user has not already logged in. If the EXEC facility has authenticated the user, PPP authentication is not performed.
- The aaa authorization network radius-network radius command 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.

20.1.6 AAA Authorization Configuration Task List

- Configuring EXEC Authorization using AAA

20.1.7 AAA Authorization Configuration Task

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, TACACS+.

(2) Define the method lists for authorization by using an aaa authorization command. It does not provide authorization server, by default.

(3) Apply the method lists to a particular interface or line, if necessary.

Configuring EXEC Authorization using AAA

Use aaa authorization exec command to run authorization to determine if the user is allowed to run an EXEC shell. This facility might return user profile information such as autocommand information. Use line configuration command login authorization to apply these lists. Use the following command in global configuration mode:

command	Purpose
aaa authorization exec {**default** | *list-name*}*method1* [*method2*...]	Establishes global authorization list.
line [**console** | **vty**] *line-number* [*ending-line-number*]	Enters the line configuration mode for the lines to which you want to apply the authorization method list.
login authorization {**default** | *list-name*}	Applies the authorization list to a line or set of lines(in line configuration mode).

The keyword **list-name** is the character string used to name the list of authorization methods. The keyword **method** specifies the actual method during authorization process. Method lists enable you to designate one or more security protocols to be used for authorization, thus ensuring a backup system in case the initial method fails. The system uses the first method listed to authorize users for specific network services; if that method fails to respond, the system selects the next method listed in the method list. This process continues until there is successful communication with a listed authorization method, or all methods defined are exhausted. If all specified methods fail to respond, and you still want the system to enter the EXEC shell, you should specify none as the last authorization method in command line.

Use default parameter to establish a default list, and the default list will apply to all interfaces automatically. For example, use the following command to specify RADIUS as the default authorization method for exec:

aaa authorization exec default group radius

Note:

If no method list is defined, the local authorization service will be unavailable and the authorization is allowed to pass.

The following table lists the currently supported EXEC authorization mode:

keyword	Purpose
group *WORD*	Uses a named server group for authorization.
group radius	Uses radius authorization.
local	Uses the local database for authorization.
if-authenticated	Allows the user to access the requested function if the user is authenticated.
none	No authorization is performed.

20.1.8 AAA Authorization Example

1. EXEC local authorization example

This section provides a configuration example that uses local authorization to demonstrate how to configure the switch, and use LOCAL for authentication and authorization:

aaa authentication login default local

aaa authorization exec default local

!

username exec1 password 0 abc privilege 15

username exec2 password 0 abc privilege 10

username exec3 nopassword

username exec4 password 0 abc user-maxlinks 10

username exec5 password 0 abc autocommand telnet 172.16.20.1

!

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

- The aaa authentication login default local command defines the default method list of login authentication. This method list applies to all login authentication servers automatically.
- The aaa authorization exec default local command defines default method list of exec authorization. The method list automatically applies to all users that need to enter exec shell.

- Username is exec1, login password is abc, EXEC privileged level is 15(the highest level), that is, when user exec1 whose privileged level is 15 logs in exec shell, all commands can be checked and performed.
- Username is exec2, login password is abc, EXEC privileged level is 10, that is, when user exec2 whose privileged level is 10 logs in EXEC shell, commands with privileged level less than 10 can be checked and performed.
- Username is exec3, no password is needed for login.
- Username is exec4, login password is abc, the maximum links of the user is 10.
- Username is exec5, login password is abc, user performs telnet 172.16.20.1 immediately when logging in exec shell.

20.1.9 AAA Accounting Configuration Task List

- Configuring Connection Accounting using AAA
- Configuring Network Accounting using AAA

20.1.10 AAA Accounting Configuration Task

To configure AAA accounting, perform the following configuration processes：

(1) If you decide to use a security server, configure security protocol parameters, such as RADIUS, TACACS+.

(2) Define the method lists for accounting by using an aaa accounting command.

(3) Apply the method lists to a particular interface or line, if necessary.

Configuring Accounting Connection using AAA

Use the aaa accounting command to enable AAA accounting. To create a method list to provide accounting information about all outbound connections made from the network access server, use the aaa accounting connection command. The outbound connection contains: Telnet, PAD, H323 and rlogin, and we only support H323 now. Use the following command in global configuration mode.

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

The keyword **list-name** is used to name any character string of the establishing list. The keyword method specifies the actual method adopted during accounting process.

The following table lists currently supported connection accounting methods:

keyword	Description
group *WORD*	Enables named server group for accounting.
group radius	Enables radius 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.

Configuring Network Accounting using AAA

Use the aaa accounting command to enable AAA accounting. To create a method list to provide accounting information for PPP or SLIP sessions, use the aaa accounting network command in global configuration mode.

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

The keyword list-name is used to name any character string of the establishing list. The keyword method specifies the actual method adopted during accounting process.

The following table lists currently supported network accounting methods:

keyword	Description
group *WORD*	Enables named server group for accounting.
group radius	Enables radius 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.

AAA accounting update

To enable periodic interim accounting records to be sent to the accounting server, use the aaa accounting update command in global configuration mode. To disable interim accounting updates, use the no form of this command.

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

If the keyword **newinfo** is used, interim accounting records will be sent to the accounting server every time there is new accounting information to report. An example of this would be when IP Control Protocol (IPCP) completes IP address negotiation with the remote peer. The interim accounting record will include the negotiated IP address used by the remote peer.

When used with the keyword **periodic**, interim accounting records are sent periodically as defined by the argument number. The interim accounting record contains all of the accounting information recorded for that user up to the time the accounting record is sent.

When using both the keywords **newinfo** and **periodic**, interim accounting records are sent to the accounting server every time there is new accounting information to report, and accounting records are sent to the accounting server periodically as defined by the argument number. For example, if you configure the aaa accounting update newinfo periodic number command, all users currently logged in will continue to generate periodic interim accounting records while new users will generate accounting records based on the newinfo algorithm.

AAA accounting suppress null-username

To prevent the AAA system from sending accounting records for users whose username string is NULL, use the aaa accounting suppress null-username command in global configuration mode. To allow sending records for users with a NULL username, use the no form of this command.

aaa accounting suppress null-username

20.2 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.

20.2.1 Introduction

RADIUS Introduction

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 that has been customized to work with the Kerberos security system.
- Networks in which a user must only access a single service. Using RADIUS, you can control user access to a single host, to a single utility such as Telnet, or to a single protocol such as Point-to-Point Protocol (PPP). For example, when a user logs in, RADIUS identifies this user as having authorization to run PPP using IP address 10.2.3.4 and the defined access list is started.

- 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.

RADIUS is not suitable in the following network security situations:

- Multiprotocol access environments. RADIUS does not support the following protocols:

AppleTalk Remote Access (ARA)

NetBIOS Frame Control Protocol (NBFCP)

- NetWare Asynchronous Services Interface (NASI)
- X.25 PAD connections
- Switch-to-switch situations. RADIUS does not provide two-way authentication.
- Networks using a variety of services. RADIUS generally binds a user to one service model.

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:

a. Services that the user can access, including Telnet, rlogin, or local-area transport (LAT) connections, and PPP, Serial Line Internet Protocol (SLIP), or EXEC services.

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

20.2.2 RADIUS Configuration Task List

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

The following configuration tasks are optional:

- You may use the aaa authorization global command to authorize specific user functions. For more information about using the aaa authorization command, refer to the chapter "Configuring Authorization."
- You may use the aaa accounting command to enable accounting for RADIUS connections. For more information about using the aaa accounting command, refer to the chapter "Configuring Accounting."

20.2.3 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

20.2.4 RADIUS Configuration Task

Configuring Switch to RADIUS Server Communication

The RADIUS host is normally a multiuser system running RADIUS server software from Livingston, Merit, Microsoft, or another software provider. A RADIUS server and a 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 switch 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.

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.

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."

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."

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."

20.2.5 RADIUS Configuration Examples

RADIUS Authentication and Authorization Example

The following example shows how to configure the router 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 router 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.

RADIUS Authentication, Authorization, and Accounting Example

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 radius local

line vty 1 16

login authentication admins

The lines in this example RADIUS authentication, authorization, and accounting configuration are defined as follows:

radius-server host command defines the IP address of the RADIUS server host;

radius-server key command defines the shared secret text string between the network access server and the RADIUS server host.

aaa authentication login admins group radius local command defines the authentication method list "dialins," which specifies that RADIUS authentication and then (if the RADIUS server does not respond) local authentication will be used on serial lines using PPP;

login authentication admins command applies the "admins" method list for login authentication.

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

Chapter 21 DHCP-SNOOPING Configuration Commands

21.1 DHCP-snooping Configuration Tasks

The task of the DHCP-snooping is to judge the DHCP message, prevent the fake DHCP server from providing DHCP service and maintain the mapping between MAC address and IP address. According to the mapping between MAC address and IP address, the DAI function and the IP source guard function can be complete. DHCP-snooping functions contain DHCP message listening, dynamic maintenance of the mapping table of MAC address and IP address. The layer-2 switch filters the messages that do not satisfy the mapping relationship and prevents the network attack from illegal users.

- Enabling or disabling DHCP-Snooping
- Enabling DHCP-Snooping on VLAN
- Configuring the DHCP-Trusted Port
- Enabling the DAI Function on VLAN
- Configuring the ARP-Trusted Port
- Enabling Source IP Monitoring on VLAN
- Configuring Source-IP-Trusted Port
- Configuring the TFTP Server to Backup the Port-Binding Relationship
- Configuring the Filename of Port-Binding Relationship Backup
- Configuring the interval of Port-Binding Relationship Backup
- Configuring Port-Binding Manually
- Monitoring and Maintaining DHCP-Snooping
- DHCP-Snooping Configuration Example

21.1.1 Enabling or disabling DHCP-Snooping

Perform the following configuration globally:

Run	To
ip dhcp-relay snooping	Enable the DHCP-snooping function.
no ip dhcp-relay snooping	Resume the default settings.

The command is a globally control command to start up the DHCP snooping function. If the command is configured, the switch monitors all DHCP messages and relative binding relationship is formed.

Note:

Before the command is configured at the client, the switch cannot add the corresponding binding relationship when the switch obtains an address.

21.1.2 Enabling DHCP-Snooping on VLAN

If the DHCP snooping function is configured on VLAN, all DHCP messages received from illegal physical ports in the whole VLAN will be legally monitored. The DHCP response messages from all illegal physical ports in the whole VLAN will be dropped, preventing illegal users from forging addresses or the incorrectly configured DHCP server from allocating addresses. For the DHCP request messages from illegal ports, if the MAC address that the message is sent to does not match the hardware address field, the message will be considered as the DHCP DOS attack message that is forged by user, so the switch will drop the message.

Perform the following configuration globally:

Run	To
Ip dhcp-relay snooping vlan *vlan_id*	Enable DHCP-snooping on VLAN.
no ip DHCP-snooping vlan *vlan_id*	Disable DHCP-snooping on VLAN

21.1.3 Configuring the DHCP-Trusted Port

If a DHCP-trusted port is configured, the DHCP messages from the DHCP-trusted port will not be checked.

Perform the following operations in physical port configuration mode:

Run.	To
Dhcp snooping trust	Configure the DHCP-trusted port.
no Dhcp snooping trust	Resume the DHCP-trusted port to a distrusted port.

The ports are distrusted by default.

21.1.4 Enabling the DAI Function on VLAN

When the dynamic ARP monitoring is performed on all physical ports of a VLAN, if the source MAC address and the source IP address of the ARP message received by a port do not satisfy the binding relationship of MAC address and IP address, the ARP message will be rejected. The MAC-to-IP mapping relationship can be configured on the port manually or dynamically. If the MAC-to-IP mapping is not configured on the physical port, the switch declines to forward all ARP message.

Run	To
Ip arp inspection vlan *vlanid*	Enable the dynamic ARP monitoring on all illegal ports within a VLAN.
No Ip arp inspection vlan *vlanid*	Disable the dynamic ARP monitoring on all illegal ports within a VLAN.

21.1.5 Configuring the ARP-Trusted Port

The ARP monitoring is not enabled on the ARP-trusted port. The ports are distrusted ports by default.

Perform the following operations in port configuration mode:

Run	To
Arp inspection trust	Configure the ARP -trusted port.
no Arp inspection trust	Resume to the ARP-distrusted port.

21.1.6 Enabling Source IP Monitoring on VLAN

After source IP monitoring is enabled on a VLAN, if the source MAC address and the source IP address of the IP message received by a port do not satisfy the binding relationship of MAC address and IP address, the IP message will be rejected. The MAC-to-IP mapping relationship can be configured on the port manually or dynamically. If the MAC-to-IP mapping is not configured on the physical port, the switch declines to forward all IP message.

Perform the following configuration globally:

Run...	To...
ip verify source vlan *vlanid*	Enable source IP address monitoring on all distrusted ports in a VLAN.
No ip verify source vlan *vlanid*	Disable source IP address monitoring on all ports in a VLAN.

Note:

After the global snooping is configured, the received message may be the DHCP message and also the IP message.

21.1.7 Configuring Source-IP-Trusted Port

The source address checkup is not enabled on the source-IP-trusted ports.

Perform the following operations in port configuration mode:

Run...	To...
Ip-source trust	Configure the source-IP-trusted port.
No ip-source trust	Resume to a source-IP-distrusted port.

21.1.8 Configuring the TFTP Server to Backup the Port-Binding Relationship

After the switch configuration is saved and then the switch is restarted, the previously-configured port binding relationship does not exist again. In this case, if the source IP address monitoring function is enabled, the switch declines to forward the IP message. To resolve the

problem, the TFTP server is adopted to backup the port-binding relationship. After the TFTP server is configured, the port-binding relationship will be automatically downloaded to the TFTP server through the TFTP protocol. In this case, the switch automatically downloads the port-binding table from the TFTP server after the switch is restarted.

Perform the following configuration globally:

Run...	To...
Ip dhcp-relay snooping database-agent *ip-address*	Configure the IP address of the TFTP server which is used to backup the port-binding relationship.
No ip dhcp-relay snooping database-agent	Delete the TFTP server configuration.

21.1.9 Configuring the Filename of Port-Binding Relationship Backup

It is the filename saved on the TFTP server when the TFTP server backups the port-binding relationship. Therefore, different switches can backup their own port-binding relationship to a same TFTP server.

Perform the following configuration globally:

Run...	To...
Ip dhcp-relay snooping db-file *name*	Configure the filename of port-binding relationship backup.
No ip dhcp-relay snooping db-file	Delete the filename of port-binding relationship backup.

21.1.10 Configuring the Interval for Checking Port-Binding Relationship Backup

The MAC-to-IP binding table dynamically changes; therefore, it need be checked after a certain time. If the binding table is updated, it need be backed up again. The default value of the interval is 30 minutes.

Perform the following configuration globally:

Run...	To...
Ip dhcp-relay snooping write *num*	Configure the interval for checking port-binding relationship backup (unit: minute).
No Ip dhcp-relay snooping write	Resume the interval for checking port-binding relationship backup to the default value.

21.1.11 Configuring Port-Binding Manually

For hosts whose MAC addresses are not obtained from the DHCP server, the items in the port-binding table can be manually configured on the port of a switch to enable the hosts to access the network normally.

Note:

The items configured manually in the port-binding table have higher priority than the dynamically-configured items. If the manually-configured item has the same MAC address as the dynamically-configured item, the manually-configured item replaces the dynamically-configured item. The item in the port-binding table takes the MAC address as the unique index.

Perform the following configuration globally:

Run...	To...
ip source binding *MAC IP interface name*	Configure port binding manually.
No ip source binding *MAC IP*	Delete items in the port-binding table.

21.1.12 Monitoring and Maintaining DHCP-Snooping

Perform the following operations in management mode:

Run...	To...
show ip dhcp-relay snooping	Display the configuration information about DHCP-snooping.
show ip dhcp-relay snooping binding	Display the address-binding items that validate on the port.
show ip dhcp-relay snooping binding all	Display all address-binding items that are generated by DHCP snooping.
[**no**] **debug ip dhcp-relay** [snooping | binding | event]	Enable or disable the snooping, binding or event of the DHCP relay.

Display the configuration information about DHCP-snooping:

```
switch#show ip dhcp-relay snooping
  ip dhcp-relay snooping vlan 3
ip arp inspection vlan 3
DHCP Snooping trust interface:
    FastEthernet0/1
ARP Inspect interface:
    FastEthernet0/11
```

Display the information about dhcp-relay snooping binding:

```
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         FastEthernet0/3
```

Display all information about dhcp-relay snooping binding:

```
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         FastEthernet0/2
00-e0-0f-26-23-89     192.2.2.101     86400      DHCP_SN           3         FastEthernet0/3
```

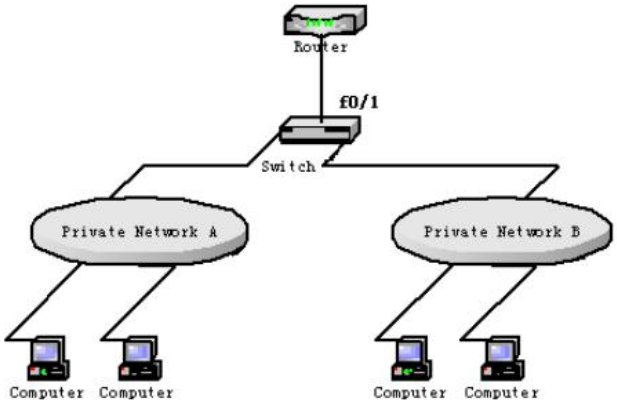
Debug the information about dhcp-relay snooping:

```
switch#debug ip DHCP-snooping packet
DHCPR: receive l2 packet from vlan 3, dilD: 3
DHCPR: DHCP packet len 277
DHCPR: add binding on interface FastEthernet0/3
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 FastEthernet0/3
DHCPR:    IP address: 192.2.2.101, lease time 86400 seconds
DHCPR: send packet continue
```

21.1.12 DHCP-Snooping Configuration Example

Below figure shows the networking of an example.



(1) Enable the DHCP-snooping of VLAN 1 that connects private network A.

Switch_config# ip dhcp-relay snooping

Switch_config#ip dhcp-relay snooping vlan 1

(2) Enable the DHCP-snooping of VLAN 2 that connects private network B.

Switch_config# ip dhcp-relay snooping

Switch_config# ip dhcp-relay snooping vlan 2

(3) Configure the DHCP-trusted port that the DHCP server connects.

Switch_config_f0/1# dhcp snooping trust

Chapter 22 LLDP Configuration Commands

22.1 LLDP Configuration Commands

The 802.1AB Link Layer Discovery Protocol makes it easier to troubleshoot enterprise network failures and enhances the ability of network management tools to discover and maintain accurate network topologies in a multi-vendor environment. It allows the neighboring device to send a notification of its status information to other devices, and each port of each device has stored the define information. If necessary, they can also directly connect with the neighboring devices and send updated information. The device stores the information in the standard SNMP MIBs. The network management system can query the current Layer 2 connection from the MIB. LLDP does not configure or control network elements or traffic. It only reports the configuration of the second layer.

In short, LLDP is a proximity discovery protocol. It defines a standard way for Ethernet network devices, such as switches, routers, and wireless LAN access points, to advertise their presence to other nodes in the network and to store discovery information for each neighboring device. Such as device configuration and device identification and other details can be announced by this agreement. Specifically, LLDP defines a general announcement information set, a protocol for transport announcements, and a method for storing the received announcement information. The device that advertises its own information can transmit multiple bulletin information within a LAN packet, in the form of a Type Length Value (TLV) field.

TLV contains three mandatory TLVs: Chassis ID TLV, Port ID TLV and Time To Live TLV, five optional TLVs: Port Description, System Name, System Description, System Capabilities, Management Address, and three extended 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, Mode Name, Assert ID)).

LLDP is a one-way protocol, an LLDP agent can be associated with the MSAP to send their own system status and their own functions, but also can receive the current system status and function of adjacent devices. However, the LLDP agent cannot request any information from this party through this protocol. LLDP agent does not affect its sending and receiving messages, and can only configure the transmission or receiving, or both.

22.1.1 Protocol Initialization

The local LLDP agent may be configured to receive- only frames, transmit- only frames, and receive-and-transmit frames. Therefore, receive-and-transmit frames need independent protocol initialization. In the case of receive- only frames or transmit- only frames without configuration instructions, LLDP proxy is considered to be receive-and-transmit frames mode by default.

22.1.2 LLDP Send Mode Initialization

In interface mode, configure whether the interface is a transmit frame mode. When the frame mode is configured to transmit the frame mode, LLDP information is automatically sent when the status or value of one or more information elements (management objects) in the local system changes and the transmission timer is timed out; when the frame is not transmittable, the interface does not send LLDP packets to its neighbors.

22.1.3 LLDP Receive Mode Initialization

Configure the interface as receive frame mode in interface mode. The LLDP packets sent by neighbors can be received when the configuration is receive frame mode and the contents of tlv are stored in the remote MIB. When the frame is not receivable, the interface discards the LLDP packets directly after receiving the LLDP packets sent by neighbors.

22.1.4 Description of LLDP PDU Message Structure

LLDP PDUs should contain three mandatory TLVs in sequence, followed by one or more optional TLVs, and finally is the end the TLV. As shown in Figure 21.1:

Chassis ID TLV	Port ID TLV	Time To Live TLV	Optional TLV	…	Optional TLV	End of LLDPDU TLV
M	M	M				M

M is the TLV which must be contained.

(1) Three mandatory TLVs should appear at the beginning of the LLDP PDU in the following order:

1. Chassis ID TLV
2. Port ID TLV
3. Time To Live TLV

(2) Select an optional TLV from the network management, in any order, including:

4. Port Description
5. System Name
6. System Description
7. System Capabilities
8. Management Address

Three extended TLVs, with 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 (By default, the TLV of the MED is not sent. When an LLDP packet with the MED TLV is received, the LLDP packet with the MED TLV will be sent.):

17. MED Capability (If the MED extension TLV is added, this TLV is required)
18. Network Policy
19. Location Identification
20. Extended Power-via-MDI
21. Inventory (including Hardware Revision、Firmware Revision、Software Revision、Serial Number、Manufacturer Name、Mode Name、Assert ID)

(3) The end of the TLV should be the last TLV in the LLDP PDU.

22.2 LLDP Configuration Task List

- Disabling/enabling LLDP
- Configuring holdtime
- Configuring the timer
- Configuring reinit
- Configuring the to-be-sent tlv
- Configuring the Transmission or Reception Mode
- Specifying the port management ip address
- Sending trap notification to mib library
- Configuring Show-Relative Commands
- Configuring the Deletion Commands

22.3 LLDP Configuration Task

22.3.1 Forbidding/enabling LLDP

LLDP is disabled by default. You need start up LLDP before it runs. After the LLDP function is enabled, the local port periodically sends the lldp frame to notify the local port information.

Run the following command in global configuration mode to enable LLDP:

Command	Purpose
Config	Enter the global configuration mode.
lldp run	Runs LLDP.

Run the following command to disable LLDP:

Command	Purpose
Config	Enter the global configuration mode.
no lldp run	Disables LLDP.

Note:

Only the lldp function can be used to process the received lldp packets, otherwise the lldp frame will be forwarded directly.

22.3.2 Configuring Holdtime

Normally, the remote information stored in the MIB will be updated before aging, but the information in the MIB will be degraded due to the possible loss of the frame. To prevent this, set the TTL value so that the updated LLDP frame is sent multiple times during the aging time. You can control the ttl timeout for sending lldp packets by changing the holdtime of the switch.

Run the following command in global configuration mode to configure holdtime of LLDP:

Command	Purpose
Config	Enter the global configuration mode.
lldp holdtime *time*	Configures the timeout time of LLDP. The range of the value is <0-65535>. The default value is 120s.

Resume the default timeout value.

Command	Purpose
Config	Enter the global configuration mode.
no lldp holdtime	Resumes the timeout time to the default value, 120 seconds.

Note:

The timeout should be longer than the interval of sending the lldp packet, so that the previous neighbor information is not lost when the next lldp frame is received.

22.3.3 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:

Command	Purpose

config	Enter the global configuration mode.
lldp reinit time	Configures the interval of message transmission of LLDP.

Resume the default interval.

Command	Purpose
config	Enter the global configuration mode.
no lldp timer	Resumes the default interval, that is, 30 seconds.

22.3.4 Configuring Reinit

In the local systems, it will automatic send LLDP information when one or more of the information elements (management objects) state or value changes or send timer timeout in both cases. Since a single information change is required to send LLDP frames, a series of consecutive information changes may trigger a number of LLDP frames to be sent, and only one change is reported in each frame. To avoid this, network management defines two consecutive LLDP frames waiting time. By configuring the reinit of lldp, you can control the interval between two consecutive lldp packets.

Run the following command in global configuration mode to configure **reinit** of LLDP:

Command	Purpose
config	Enter the global configuration mode.
lldp reinit time	Configures the interval of LLDP to continuously transmit message. The range is <2-5>. And the default value is 2s.

Resume the default value for reinit.

Command	Purpose
config	Enter the global configuration mode.
no lldp reinit	Resumes the default interval of continuously transmitting message; the default interval value is two seconds.

22.3.5 Configuring the To-Be-Sent TLV

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 the to-be-sent tlvs.

Command	Purpose

Config	Enter the global configuration mode.
lldp tlv-select management-address	Optional. Send management address tlv. And the management address should be easy to manage the use of the general three-tier IP address.
lldp tlv-select port-description	Optional. Send port description tlv. Port Description uses numbers or letters to describe the port.
lldp tlv-select system-capabilities	Optional. Send system performance tlv, system performance refers to the system to send the message is a switch / router or other.
lldp tlv-select system-description	Optional. Send the system description tlv, the system describes the textual description of the network entities consisting of alphanumeric characters. The system description should include the full name of the system, the version definition of the system hardware type, the software operating system, and the network software.
lldp tlv-select system-name	Optional. Send system name tlv. The system name field is the name specified by the system administrator of the alphanumeric alphabet. The system name should be the name of the system administrator. The name of the switch.

Run the following commands in global configuration mode to add or delete the to-be-sent tlvs.

Run the following commands in global configuration mode to add or delete **tlv** of LLDP:

Command	Purpose
Config	Enter the global configuration mode.
No lldp tlv-select management-address	Optional. Send management address tlv. And the management address should be easy to manage the use of the general three-tier IP address.
No lldp tlv-select port-description	Optional. Send port description tlv. Port Description uses numbers or letters to describe the port.
No lldp tlv-select system-capabilities	Optional. Send system performance tlv, system performance refers to the system to send the message is a

	switch / router or other.
No lldp tlv-select system-description	Optional. Send the system description tlv, the system describes the textual description of the network entities consisting of alphanumeric characters. The system description should include the full name of the system, the version definition of the system hardware type, the software operating system, and the network software.
No lldp tlv-select system-name	Optional. Send system name tlv. The system name field is the name specified by the system administrator of the alphanumeric alphabet. The system name should be the name of the system administrator. The name of the switch.

22.3.6 Specifying the Port Management Ip Address

Select the to-be-send extended TLV to send by configuring lldp dot1-tlv-select / dot3-tlv-select / med-tlv-select in the interface. By default, the TLVs of DOT1 and DOT3 are sent, and the TLV of MED is not sent.

In the interface configuration mode, use the following command to configure the tlv to be sent:

Command	Purpose
Config	Enter the global configuration mode.
Interface intf-type intf-id	Enter the interface configuration mode.
Lldp dot1-tlv-select port-vlan-id	Optional, send the 802.1- organization custom tlv, inform the PVID of the port.
Lldp dot1-tlv-select protocol-vlan-id	Optional, send the 802.1- organization custom tlv, inform the PVID of the port
Lldp dot1-tlv-select vlan-name	Optional, send the 802.1- organization custom tlv, inform the vlan name of the port.
No lldp tlv-select system-name	Optional. Send system name tlv. The system name field is the name specified by the system administrator of the alphanumeric alphabet. The system name should be the name of the system administrator. The name of the switch.
Lldp dot3-tlv-select macphy-config	Optional, send the 802.1- organization custom tlv, including: (a)the bit rate and the duplex of the physical layer;

	(b)the current duplex and set bit rate; (c)Indicates whether the setting is the result of the auto-negotiation of the connection initialization phase or the manual forced behavior.
Lldp dot3-tlv-select power	Optional, send 802.3 organization custom tlv, show the port can allow the power to be provided to connect the system without power through the link.
Lldp dot3-tlv-select link-aggregation	Optional, send 802.3 organization custom tlv, indicating whether the port link can be aggregated, if so, then indicate the port to identify the aggregation.
Lldp dot3-tlv-select max-frame-size	Optional, send 802.3 organization custom tlv, indicating the maximum size (bytes) of the frame supported by the port.
Lldp med-tlv-select network-policy	Optional, send MED custom tlv, display port can effectively find and diagnose VLAN configuration error matching flow, and the related 2 and 3 layers property.
Lldp med-tlv-select location	Optional, send MED custom tlv, specify the address, including: (a) coordinate-based LCI, defined in IETF RFC 3825 [6]; (b) city address LCI, defined in (c) (c) IETF (refer to ANNEX B); Emergency call service ELIN number;
Lldp med-tlv-select power-management	Optional, send MED custom tlv, display through the media dependent port of the extended power to find the media terminal and network connectivity device advertising detailed power information.
Lldp med-tlv-select inventory	Optional, send MED custom tlv, display found the related detailed inventory attributes with enable tracking and identify the terminal.

Use the following command to configure to delete the tlv to be sent in the global configuration mode:

Command	Purpose

Config	Enter the global configuration mode.
Interface intf-type intf-id	Enter the interface configuration mode.
No lldp dot1-tlv-select port-vlan-id	Optional, send the 802.1- organization custom tlv, inform the PVID of the port.
No lldp dot1-tlv-select protocol-vlan-id	Optional, send the 802.1- organization custom tlv, inform the PVID of the port
No lldp dot1-tlv-select vlan-name	Optional, send the 802.1- organization custom tlv, inform the vlan name of the port.
No lldp dot3-tlv-select macphy-config	Optional. Send system name tlv. The system name field is the name specified by the system administrator of the alphanumeric alphabet. The system name should be the name of the system administrator. The name of the switch.
No lldp dot3-tlv-select power	Optional, send the 802.1- organization custom tlv, including: (a)the bit rate and the duplex of the physical layer; (b)the current duplex and set bit rate; (c)Indicates whether the setting is the result of the auto-negotiation of the connection initialization phase or the manual forced behavior.
No lldp dot3-tlv-select link-aggregation	Optional, send 802.3 organization custom tlv, show the port can allow the power to be provided to connect the system without power through the link.
No lldp dot3-tlv-select max-frame-size	Optional, send 802.3 organization custom tlv, indicating whether the port link can be aggregated, if so, then indicate the port to identify the aggregation.
No lldp med-tlv-select network-policy	Optional, send 802.3 organization custom tlv, indicating the maximum size (bytes) of the frame supported by the port.
No lldp med-tlv-select location	Optional, send MED custom tlv, display port can effectively find and diagnose VLAN configuration error matching flow, and the related 2 and 3 layers property.

No lldp med-tlv-select power-management	Optional, send MED custom tlv, specify the address, including: (d) coordinate-based LCI, defined in IETF RFC 3825 [6]; (e) city address LCI, defined in (f) (c) IETF (refer to ANNEX B); Emergency call service ELIN number;
No lldp med-tlv-select inventory	Optional, send MED custom tlv, display through the media dependent port of the extended power to find the media terminal and network connectivity device advertising detailed power information.
No lldp dot1-tlv-select vlan-name	Optional, send MED custom tlv, display found the related detailed inventory attributes with enable tracking and identify the terminal.

22.3.7 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 command in interface configuration mode to disable the transmit-only mode of the port:

Command	Purpose
config	Enter the global configuration mode.
Interface intf-type intf-id	Enter the interface configuration mode.
No lldp transmit	Disable the transmit-only mode of the port.
No lldp receive	Disable the receive-only mode of the port.

Run the following command in interface configuration mode to enable the transmit-only mode of the port:

Command	Purpose
config	Enter the global configuration mode.
Interface intf-type intf-id	Enter the interface configuration mode.

lldp transmit	Enable the transmit-only mode of the port.
lldp receive	Enable the receive-only mode of the port.

Note:

In addition to the above mode, it can also be set to receive-only mode or transmit-only mode.

22.3.8 Specifying the port management ip address

In the port configuration mode, the user can configure the management address of the port sent by the lldp packet. The management address should be a port-related ip address, so that the normal communication of the management address can be ensured.

Use the following command to configure the management ip address in the interface configuration mode:

Command	Purpose
Config	Enter the global configuration mode.
Interface intf-type intf-id	Enter the interface configuration mode.
Lldp management-ip A.B.C.D	Configure the management ip address of the port.

Note:

You can use **no lldp management-ip** to restore the default management address of the port. The default management address is the ip address of the vlan interface corresponding to port pvid. When the corresponding vlan interface does not exist, the management address is 0.0.0.0.

22.3.9 Sending trap notification to mib library

Send a trap notification to the lldp mib library or the ptopo mib library.

In the global configuration mode, use the following command to send a trap notification to the lldp mib library or the ptopo mib library:

Command	Purpose
Config	Enter the global configuration mode.
Ldp trap-send lldp-mib	Send trap notification to lldp mib library.
Ldp trap-send ptopo-mib	Send trap notification to ptopo mib library.

Note:

You can use **no lldp management-ip** to restore the default management address of the port. The default management address is the ip address of the vlan interface corresponding to port pvid. When the corresponding vlan interface does not exist, the management address is 0.0.0.0.

22.3.10 Configuring Location Information

Check the address information by configuring the location information.

Use the following command to configure the location information on the global configuration mode.

command	Purpose
Config	Enter the global configuration mode.
Location elin identifier id WORD	Set location elin information. **Id** is the elin identifier number. **Word** is elin information, and the value ranges from 10 to 25bytes.
Location civic identifier id	Enter location configuration mode.
Language WORD	Set language.
State WORD	Set state (district, district, province, district) name, such as shanghai
County WORD	Set country name.
City WORD	Set city name.
Division WORD	Set division name.
Neighborhood WORD	Set neighborhood name.
Street WORD	Set street name.
Leading-street-dir WORD	Set the leading street direction, such as N (north).
Trailing-street-suffix WORD	Set the trailing street suffix, such as SW.
Street-suffix WORD	Set the street suffix, such as Platz Avenue.
Number WORD	Set the street number, such as NO.123.
Street-number-suffix WORD	Set the street number suffix, such A Road, No.1/2
Landmark WORD	Set up landmark information, such as Columbia University
Additional-location WORD	Set additional location information.
Name WORD	Set up resident information, such as Joe's barber shop

Postal-code WORD	Set postal-code.
Building WORD	Set building information.
Unit WORD	Set unit information.
Floor WORD	Set floor information.
Room WORD	Set room information.
Type-of-place WORD	Set the type of location, such as an office
Postal-community WORD	Set the postal community name
Post-office-box WORD	Set the mailbox name, such as 12345
Additional-code WORD	Set the additional code.
Country WORD	Set country name.
Script WORD	Set the script information.

Use the following command to delete the location information in global configuration mode.

command	Purpose
Config	Enter global configuration mode.
No location elin identifier id	Delete the location elin information which elin identifier number is id.
No location civic identifier id	Delete the location civic information which elin identifier number is id.
location civic identifier id	Enter location configuration mode.
No language	Delete language.
No state	Delete state (district, district, province, district) name, such as shanghai
No county	Delete country name.

No city	Delete city name.
No division	Delete division name.
No neighborhood	Delete neighborhood name.
No street	Delete street name.
No leading-street-dir	Delete the leading street direction, such as N (north).
No trailing-street-suffix	Delete the trailing street suffix, such as SW.
No street-suffix	Delete the street suffix, such as Platz Avenue.
No number	Delete the street number, such as NO.123.
No street-number-suffix	Delete the street number suffix, such A Road, No.1/2
No landmark	Delete landmark information, such as Columbia University
No additional-location	Delete additional location information.
No name	Delete resident information, such as Joe's barber shop
No postal-code	Delete postal-code.
No building	Delete building information.
No unit	Delete unit information.
No floor	Delete floor information.
No room	Delete room information.
No type-of-place	Delete the type of location, such as an office
No postal-community	Delete the postal community name
No post-office-box	Delete the mailbox name, such as 12345
No additional-code	Delete the additional code.
No country	Delete country name.
No script	Delete the script information.

22.3.11 Specify the Port Configuration Location Information

Configure the location information for the port and the location information in the TLV information.

Use the following command to configure location information in the interface configuration mode:

command	Purpose
Config	Enter the global configuration mode.
Interface intf-type intf-id	Enter the interface configuration mode.
Location civic id	Configure the location information which id is civic for the port.
Location elin id	Configure the location information which id is elin for the port.

Use the following command to delete location information in the interface configuration mode:

command	Purpose
Config	Enter the global configuration mode.
Interface intf-type intf-id	Enter the interface configuration mode.
No location civic	Delete the location information which id is civic for the port.
No location elin	Delete the location information which id is elin for the port.

22.3.12 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 management or global configuration mode:

command	Purpose
Show lldp errors	Display the error information about the LLDP module.
Show lldp interface interface-name	Display the information about port state, that is, the transmission mode and the reception mode.

Show lldp neighbors	Display the abstract information about the neighbor.
Show lldp neighbors detail	Display the detailed information about the neighbor.
Show lldp traffic	Display all received and transmitted statistics information.
Show location elin	Display location elin information.
Show location civic	Display location civic information.

22.3.13 Configuring the Deletion Commands

You can delete the received neighbor lists and all statistics information by running the following command in management configuration mode.

Run the following commands in management configuration mode:

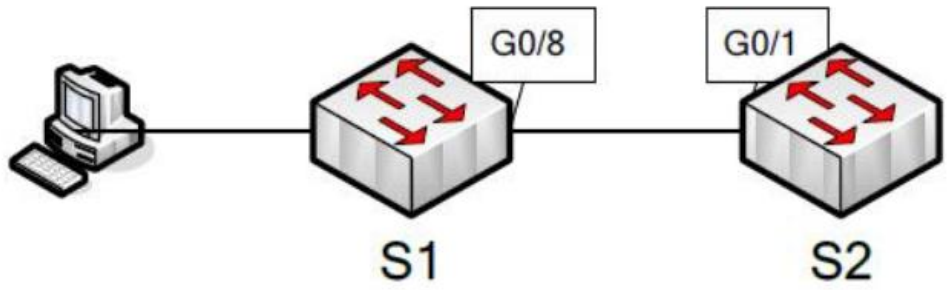
command	Purpose
Clear lldp counters	Deletes all statistics data.
Clear lldp table	Deletes all received neighbor information.

22.4 Configuration Example

22.4.1 Network Environment Requirements

Configure the LLDP protocol on the ports connected to the two switches.

22.4.2 Network topology



22.4.3 Configuration Steps

1. Basis configuration

Configure switch S1:

Switch_config#lldp run

Switch_config#

Configure switch S2:

Switch_config#lldp run

Switch_config#

Approximately one minute later, you can view the neighbor B information on Switch A. The 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: FSOS Switch 2.0.2G 132609 Software

Copyright by FS

Compiled: 2011-9-21 9:24:8 by WRL

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

Configure switch S1:

Switch_config#lldp run

Switch_config#

Configure 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#

Approximately one minute later, you can view the neighbor B information on Switch A, which is distinguished from the information displayed in the basic configuration of 1.4.3.1, in red and blue, respectively.

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: FSOS Switch 2.0.2G 132609 Software

Copyright by FS.

Compiled: 2011-9-21 9:24:8 by WRL

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

Configure Switch S1:

Switch_config#lldp run

Switch_config#

Configure Switch S2:

Switch_config#lldp run

Switch_config#location elin identifier 1 1234567890 //configure elin information

Switch_config#location civic identifier 1 //enter location configuration mode

Switch_config_civic#language English

Switch_config_civic#city Shanghai

Switch_config_civic#street Curie

Switch_config_civic#script EN //configure civic information

Switch_config_civic#quit

Switch_config#int g0/8

Switch_config_g0/8#location elin 1 // specify the elin id for the port

Switch_config_g0/8#location civic 1 // specify the civic id for the port

Switch_config_g0/8#show location elin //display elin configuration information

elin information:

elin 1: 1234567890

total: 1

Switch_config_g0/8#show location civic //display civic configuration information

civic address information:

identifier: 1

City: Shanghai

Language: English

Script: EN

Street: Curie

---

total: 1

Switch_config_g0/8#

Approximately one minute later, you can view the neighbor B information on Switch A,

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: FSOS Switch 2.0.2G 132609 Software

Copyright by FS.

Compiled: 2011-9-21 9:24:8 by WRL

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: cannot 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: FS

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: Shanghai

Street: Curie

Script: EN

ELIN location:

ELIN: 1234567890

Total entries displayed: 1

Switch_config#

Chapter 23 Fast Ethernet Ring Protection Configuration Command

23.1 Overview

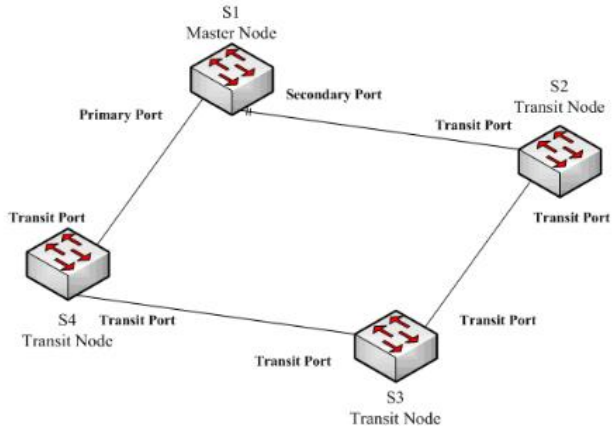
Ethernet ring protection protocol is a special type of link-layer protocol specially designed for constructing the ring Ethernet topology. The Ethernet protection protocol can shut down one link in a complete ring topology, preventing the data loop from forming the broadcast storm. If a link is broken, 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.

Note:

Ring protection protocol supports that one switch is set to the node of multiple physical ring network, so that the tangency ring can be formed.

23.2 Related Concepts of Fast Ethernet Ring Protection



23.2.1 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.

23.2.2 Roles of Ring's Port

Fast Ethernet Ring Protection 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 removes the blocking state of the secondary port.

Transit port: the transit 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.

Note:

To configure a same switch to belong to multiple rings, the switch must connect different rings through different physical ports.

23.2.3 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. It is the ring protection protocol that controls whether the port of the Ethernet ring can forward the packets of the data VLAN; the forwarding state of the non-ring port is controlled by STP.

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.

23.2.4 MAC Address Table Aging

The Fast Ethernet Ring Protection can ensure that the data packets can be sent to the correct link by controlling the aging of the MAC address table of the switch when the topology changes. In general, the aging time of the MAC address in the address table is 300 seconds. Fast Ethernet Ring Protection can control the aging of the switch MAC address table in a very short period of time.

23.2.5 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.

23.3 Type of Fast Ethernet Ring Protection

The Fast Ethernet Ring Protection packets can be classified into the following types, as shown in below chart.

Type of the packet	Description
HEALTH	It is transmitted by the master node to detect whether the topology of the ring network is complete.
LINK-DOWN	It is transmitted by the transit node to indicate that link interruption occurs in the ring network.
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.

23.4 Fast Ethernet Ring Protection Mechanism

23.4.1 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.

23.4.2 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.

23.4.3 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 24 Fast Ethernet Ring Protection Settings

24.1 Fast Ethernet Ring Protection Default Configuration

Note:

Fast Ethernet Ring Protection and STP can be configured at the same time.

After the STP is shut down, it is recommended to configure the spanning-tree bpdu-terminal function to prevent the ring nodes from forwarding BPDU.

The default configuration of Fast Ethernet Ring Protection and STP is shown in below chart

STP	Spanning-tree mode rstp
Fast Ethernet Ring Protection	none

24.2 Reading before Fast Ethernet Ring Protection Configuration

Before configuring Fast Ethernet Ring Protection, please read the following items carefully:

- Blocking broadcast storms is an important function of the ring protection protocol. Make sure that the ring network links are connected when all ring nodes are configured. For example, after configuring the master node and all the transport nodes, connect the network cable to the secondary port of the primary node. It will easily lead to broadcast storm when the connection of the ring network is done before all nodes are configured.
- The configuration of Fast Ethernet Ring Protection is now compatible with STP of the switch, but the ports controlled by Fast Ethernet Ring Protection are not controlled by STP.
- The Fast Ethernet Ring Protection supports the switch to configure multiple ring network instances.
- The configuration of the control VLAN of the ring network does not automatically establish the corresponding systematic VLAN.
- Only the ring ports of each ring can forward packets in the control VLAN of the ring. And other ports, if they are configured as Trunk mode, they cannot be forwarded in 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 Pre-Forward-Time of the transit node, it is easily to generate loopback and trigger the broadcast storm.
- Physical ports, Interface FastEthernet, Interface GigaEthernet, and aggregation ports can be configured as ring ports. If the link aggregation, 802.1X, or port security is configured on the physical port, the port cannot be configured as a ring port. Note: The version of the switch software 2.0.1L and the previous version of the high-end switch 4.0.0M do not support the configuration of the aggregation port.

24.3 Fast Ethernet Ring Protection Configuration Tasks

- Configuring the Master Node
- Configuring the Transit Node
- Configuring the Port of Ethernet Ring
- Browsing the State of the Ring Protection Protocol

24.4 Fast Ethernet Ring Protection Settings

24.4.1 Configuring the Master Node

Configure a switch to be the master node of a ring network according to the following steps:

Command	Purpose
Switch# **configure**	Enters the switch configuration mode.
Switch_config# **ether-ring** id	Configure the node instance and enter the node configuration mode. Id: instance number.
Switch_config# **control-vlan** vlan-id	Configure control VLAN. Vlan-id: control vlan number.
Switch_config# **master-node**	Configure the node type to the master node.
Switch_config_ring# **hello-time** value	Optional. Configure the period in which the master node sends probe packets. Value: Time value, 1 to 10 seconds, defaults value to 1 second.
Switch_config_ring# **fail-time** value	Optional. Configure the time limit for the secondary port to wait for probe packets. Value: Time value, 3 to 30 seconds, defaults value is 3 seconds.
Switch_config_ring# **exit**	Save the current configuration and back to the node configuration mode.

Note:

Use **no ether-ring id** command to delete the node settings and port settings of the Ethernet ring.

24.4.2 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**	Enter the switch configuration mode.
Switch_config# **ether-ring** id	Set a node and enters the node configuration mode. id：Instances number.
Switch_config_ring# **control-vlan** vlan-id	Configure the control VLAN. vlan-id：ID of the control VLAN
Switch_config_ring# **transit-node**	Configure the node type to be a transit node.
Switch_config_ring# **pre-forward-time** value	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**	Save the current settings and exits the node configuration mode.

24.4.3 Configuring the Port of Ethernet Ring

Configure a port of a switch to be the port of Ethernet ring according to the following steps:

Command	Purpose
Switch# **configure**	Enter the switch configuration mode.
Switch_config# **interface** intf-name	Enter 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** }	Configure the type of the port of Ethernet ring. id：ID of the node of Ethernet ring
Switch_config_intf# **exit**	Back to interface configuration mode.

Note:

Use no ether-ring id primary-port { secondary-port | transit-port } command to cancel the port settings of Ethernet ring.

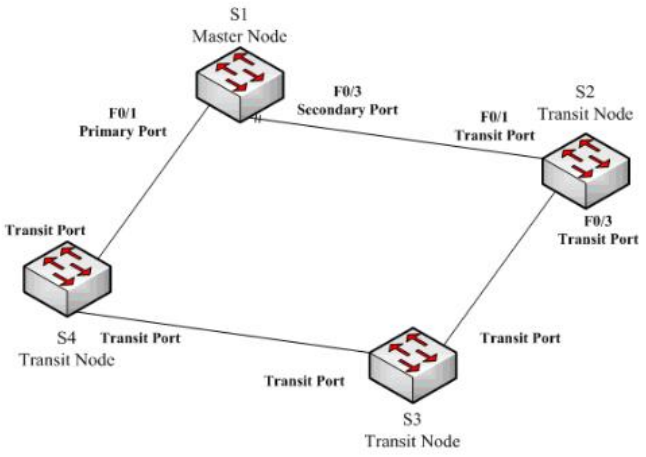
24.4.4 Browsing the State of the Ring Protection Protocol

Run the following command to browse the state of the ring protection protocol:

Command	Purpose
show ether-ring *id*	Browse the summary information about the ring protection protocol and the port of Ethernet ring. id：Instance number.
show ether-ring *id* **detail**	Browse the detailed information about the ring protection protocol and the port of Ethernet ring.
show ether-ring *id* **interface** *intf-name*	Browse the state of the Ether-ring port or the common port.

24.5 Fast Ethernet Ring Protection Configuration Example

24.5.1 Configuration Example



As shown in above figure, 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

Configures 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_f0/1# ether-ring 1 primary-port

S1_config_f0/1# exit

S1_config# interface gigaEthernet 0/3

S1_config_f0/3# ether-ring 1 secondary-port

S1_config_f0/3# exit

Establishes the control VLAN:

S1_config# vlan 2

S1_config_vlan2# exit

S1_config# interface range f0/1 , 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 fastEthernet 0/1

S1_config_f0/1# ether-ring 1 transit-port

S1_config_f0/1# exit

S1_config# interface fastEthernet 0/3

S1_config_f0/3# ether-ring 1 transit-port

S1_config_f0/3# 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

Chapter 25 Power Over Ethernet Configuration Commands

25.1 POE Configuration Commands

25.1.1 show poe system

Show POE related system information.

show poe system.

- Parameter

none

- Default

none

- Command mode

monitoring mode

- Instruction

POE DRIVER: the chip driver

POE CHIP: specific chip type

POE Port Num: number of maximum power ports

PSE PowerManagement: power management mode (including automatic, preemptive and non-preemptive)

PSE Total Power: total power

PSE Usage Threshold: power alarm (set by percentage)

PSE Alarm Power: power alarm threshold

PSE Lower-Port-Disable Power: threshold of higher-priority preemptive power, it is valid in non-automatic mode

PSE Lower-Port-NoConnect Power: prohibit the threshold of lower-priority or equal port power, it is valid in non-automatic mode

PSE Consumed Power: consumed power

PSE Peak Power: peak power, it is only valid while statistical power is enabled

PSE Mib Notification: MIB notification when power supply of the port is changed or the power alarm occurs

PSE Temperature PSE: chip temperature

- Example

Switch#show poe system

POE DRIVER:PETH PD69012 DRV

POE CHIP:PD69012

POE Port Num:24

PSE PowerManagement:Preemptive

PSE Total Power:80000 mW

PSE Usage Threshold:80%

PSE Alarm Power:64000 mW

PSE Lower-Port-Disable Power:62000 mW

PSE Lower-Port-NoConnect Power:44000 mW

PSE Consumed Power:47500 mW

PSE Peak Power:101300 mW

PSE Mib Notification:Disable

PSE Temperature:38 degree

- Related commands

none

25.1.2 show poe all

Show the description table of POE port information.

show poe all

- Parameter

none

- Default

none

- Command mode

monitoring mode

- Instruction

Port enabled/disabled: port POE enabled

Port detection: port power states, including disabled, searching, delivering-power, fault and so on.

delivering-power: represent normal power supply

Port pairs: line sequence of port power, signal represents signal line power supply, spare represents spare line power supply

Port priority: port priority, they are critical, high and low in descending order

- Example

Switch#show poe all

Port	Enable	Status	Pair	Priority
f0/3	enabled	disabled	signal	low
f0/4	enabled	disabled	signal	low

f0/2	enabled	disabled	signal	low
f0/1	enabled	disabled	signal	low
f0/5	enabled	disabled	signal	low
f0/6	enabled	disabled	signal	low
f0/7	enabled	disabled	signal	low
f0/8	enabled	disabled	signal	low
f0/9	enabled	searching	signal	high
f0/10	enabled	searching	signal	high
f0/11	enabled	searching	signal	high
f0/12	enabled	searching	signal	high
f0/13	enabled	delivering-power	signal	high
f0/14	enabled	searching	signal	high
f0/15	enabled	delivering-power	signal	high
f0/16	enabled	searching	signal	high
f0/17	enabled	disabled	signal	low
f0/18	enabled	disabled	signal	low
f0/19	enabled	disabled	signal	low
f0/20	enabled	disabled	signal	low
f0/21	enabled	disabled	signal	low
f0/22	enabled	delivering-power	signal	low
f0/23	enabled	delivering-power	signal	low
f0/24	enabled	delivering-power	signal	critical

- Related commands

none

25.1.3 show poe power

Show the power information of all ports.

show poe power

- Parameter

none

- Default

none

- Command mode

monitoring mode

- Instruction

Max: maximum power limit of the port

Current: current power of the port

Average: average power of the port, it is valid while power statistics is enabled.

Peak: peak power of the port, it is valid while power statistics is enabled.

Bottom: bottom power of the port, it is valid while power statistics is enabled.

- Example

Switch#show poe power

Port	Current	Max	Average	Peak	Bottom
f0/3	0 mW	30000 mW	0 mW	0 mW	0 mW
f0/4	0 mW	30000 mW	0 mW	0 mW	0 mW
f0/2	0 mW	30000 mW	0 mW	0 mW	0 mW
f0/1	0 mW	30000 mW	0 mW	0 mW	0 mW
f0/5	0 mW	30000 mW	0 mW	0 mW	0 mW
f0/6	0 mW	30000 mW	0 mW	0 mW	0 mW
f0/7	0 mW	30000 mW	0 mW	0 mW	0 mW
f0/8	0 mW	30000 mW	0 mW	0 mW	0 mW
f0/9	0 mW	30000 mW	0 mW	0 mW	0 mW
f0/10	0 mW	30000 mW	0 mW	0 mW	0 mW
f0/11	0 mW	30000 mW	0 mW	0 mW	0 mW
f0/12	0 mW	30000 mW	0 mW	0 mW	0 mW
f0/13	7600 mW	30000 mW	7620 mW	7800 mW	7600 mW
f0/14	0 mW	30000 mW	0 mW	0 mW	0 mW
f0/15	7600 mW	30000 mW	7600 mW	7800 mW	7600 mW
f0/16	0 mW	30000 mW	0 mW	0 mW	0 mW
f0/17	0 mW	30000 mW	0 mW	0 mW	0 mW
f0/18	0 mW	30000 mW	0 mW	0 mW	0 mW
f0/19	0 mW	30000 mW	0 mW	0 mW	0 mW
f0/20	0 mW	30000 mW	0 mW	0 mW	0 mW

f0/21	0 mW	30000 mW	0 mW	0 mW	0 mW
f0/22	15900 mW	30000 mW	15890 mW	16200 mW	14900 mW
f0/23	7700 mW	30000 mW	7780 mW	7800 mW	7700 mW
f0/24	8400 mW	30000 mW	9850 mW	22500 mW	6500 mW

- Related commands

none

25.1.4 show poe interface

Show detailed POE information of specified interface.

show poe interface *type slot/port*

- Parameter

Parameter	Description
type	Interface type.
slot	Slot or card number.
port	Slot or card port number.

- Default

none

- Command mode

monitoring mode

- Instruction

PSE Port Number: internal port number

Port Power Enabled: port power enabled

Port Force Power: forced power enabled, the priority is lower than port power enabled

Port Detection Status: port power status, including disabled, searching, delivering-power, fault and so on

Port Fault Status: port error information

Port Last Disconnection Reason: the reason of port last disconnection

Port pairs: line sequence of port power, signal represents signal line power supply, spare represents spare line power supply

Port IEEE Class: port device classification

Port priority: port priority, they are critical, high and low in descending order

Port Current: current of the port

Port Voltage: current voltage of the port, some chips do not display it

Port Current Power: current power of the port

Port Average Power: average power of the port, it is valid while power statistics is enabled.

Port Peak Power: peak power of the port, it is valid while power statistics is enabled.

Port Bottom Power: bottom power of the port, it is valid while power statistics is enabled.

Port Max Power: maximum power limit of the port

Port PD Discription: port description

- Example

Switch#show poe interface f0/24

PSE Port Number: 23

Port Power Enabled: enable

Port Force Power: disable

Port Detection Status: delivering-power

Port Fault Status :

Port Last Disconnection Reason: Port was disabled

Port Pairs: signal

Port IEEE Class: 0

Port Priority: critical

Port Current: 163 mA

Port Current Power: 8400 mW

Port Average Power: 8440 mW

Port Peak Power: 22500 mW

Port Bottom Power: 6500 mW

Port Max Power: 30000 mW

Port PD Description: AP

- Related commands

none

25.1.5 poe power-management

Configure the power management mode of the switch.

poe power-management {auto | preemptive | non-preemptive | lowDisable | lowNoConnect } *value*

- Parameter

Parameter	Description
auto	Configure the power management mode of the switch to auto mode.
preemptive	Configure the power management mode of the switch to preemptive mode.
non-preemptive	Configure the power management mode of the switch to non-preemptive mode.
lowDisable	When the total power exceeds lowDisable, the port cannot supply power any more, it can continue to power when lower than lowDisable. lowDisable= total power of the device – value.
lowNoConnect	When the total power exceeds lowNoConnect, the power enabling will be shut down if the port with lower or equal priority. lowNoConnect=lowDisable – value.

- Default

auto

- Command mode

global configuration mode

- Instruction

Auto mode: the maximum power limit of the port cannot be set, the default is the maximum port power can be supported by the chip; the port power priority cannot be set, the default priority is low.

Preemptive mode: enable the maximum power limit of the port, enable the power priority function of the port.

Non-preemptive mode: enable the maximum power limit of the port, enable the power priority function of the port.

Preemptive mode indicates the port with higher priority supply power normally for new access PD device in full load condition, the port with lower power priority is cut off power supply.

Non-peemptive mode indicates the port with higher priority generates prompt information while access to PD device in full load condition, it will prompt the PD device access for the high priority port.

- Example

The following example shows how to set the power management mode to preemptive mode:

Switch_config#poe power-management preemptive

Switch_config#poe power-management lowDisable 18000

Switch_config#poe power-management lowNoConnect 18000

- Related commands

poe max-power

poe priority

25.1.6 poe led-time

Configure LED mode to the POE's duration.

poe led-time time

no poe led-time

- Parameter

Parameter	Description
time	The unit is second.

- Default

30 seconds

- Command mode

global configuration mode

- Instruction

Use the no form of this command to return to the default value.

- Example

The following example shows how to set the duration to 10 seconds:

Switch_config#poe led-time 10

- Related commands

none

25.1.7 poe mib notification-stop

Trap notification is not set to the user if the port power changes or power alarm occurs.

poe mib notification-stop

no poe mib notification-stop

- Parameter

none

- Default

Trap notification is sent to the user if the port power changes or power alarm occurs.

- Command mode

global configuration mode

- Instruction

Use the no form of this command to return to the default value.

- Example

In the following example, trap notification is not set to the user if the port power changes or power alarm occurs.

Switch_config#poe mib notification-stop

- Related commands

none

25.1.8 poe pse-unprotect

Port power protection is to prevent the problem may cause by connecting with PSE device.

poe pse-unprotect

no poe pse-unprotect

- Parameter

none

- Default

enabled

- Command mode

global configuration mode

- Instruction

Use the no form of this command to return to the default value.

- Example

The following example shows how to disable the port protection:

Switch_config# poe pse-unprotect

- Related commands

none

25.1.9 poe counter value

Enable power counter function of global and interface.

poe counter value

no poe counter

- Parameter

Parameter	Description
value	Sampling interval, the unit is second.

- Default

disabled

- Command mode

global configuration mode

- Instruction

Use the no form of this command to return to the default value.

- Example

The following example shows how to set the sampling interval of power counter to 5 seconds:

Switch_config# poe counter 5

- Related commands

none

25.1.10 poe threshold

Configure the percentage of alarm power to the total power.

poe threshold *value*

no poe threshold

- Parameter

Parameter	Description
value	The percentage of alarm power to the total power.

- Default

100%

- Command mode

global configuration mode

- Instruction

Use the no form of this command to return to the default value.

- Example

The following example shows how to set the percentage of alarm power to the total power to 50%.

Switch_config#poe threshold 50

- Related commands

poe power-management

25.1.11 poe standard

Configure PSE standard.

poe standard {AF| AT| MAX}

- Parameter

Parameter	Description
AF	Select AF standard, maximum power output of the port: 15.4W.
AT	Select AT standard, maximum power output of the port: 30W.
MAX	Select MAX to take the newest standard of the switch, if the device supports both AF and AT, then take AT standard, if the device support AF but not AT, then take AF standard.

- Default

MAX

- Command mode

global configuration mode

- Instruction

Select AF standard, maximum power output of the port: 15.4W.

Select AT standard, maximum power output of the port: 30W.

Select MAX to take the newest standard of the switch, if the device supports both AF and AT, then take AT standard, if the device support AF but not AT, then take AF standard.

- Example

The following example shows how to set the PSE standard to AF:

Switch_config#poe standard AF

- Related commands

none

25.1.12 poe disable

Configure POE enabling.

poe disable { time-range name | <cr>}

no poe disable {time-range | <cr>}

- Parameter

Parameter	Description
time-range *name*	*name* indicates the name in no power period.
<cr>	Enter, that is, simply input poe disable, shut down the port.

- Default

The POE is enabled by default, no time limit of the power.

- Command mode

interface configuration mode

- Instruction

poe disable: disable POE function

no poe disable: enable POE function

poe disable time-range name: indicate the time range control that disables the POE function of the port during the time of adding a period named name.

no poe disable time-range: remove the time range control for disabling the port POE function within a time range

- Example

The following example shows how to disable the POE function on interface f0/1:

Switch_config_f0/1#poe disable

In the following example, the POE device disables the POE function during the time range named Sunday_free:

Switch_config_f0/1poe disable time-range Sunday_free

- Related commands

time-range

25.1.13 poe max-power

Configure the maximum power of the port.

poe max-power value

no poe max-power

- Parameter

Parameter	Description

value	The maximum power of the port, the unit is mW.

- Default

30000mW

- Command mode

interface configuration mode

- Instruction

Use the no form of this command to return to the default value; this command is in non-auto mode.

- Example

The following example shows how to set the maximum power of interface f0/1 to 15000mW.

Switch_config_f0/1#poe max-power 15000

- Related commands

poe power-management

25.1.14 poe priority

Configure POE priority of the port.

poe priority {critical | high | low }

- Parameter

Parameter	Description
critical	The highest priority.
high	The secondary priority.
low	The lowest priority.

- Default

low

- Command mode

interface configuration mode

- Instruction

This command is in non-auto mode.

- Example

The following example shows how to set the power priority of interface f0/1 to critical:

Switch_config_f0/1#poe priority critical

- Related commands

agement

25.1.15 poe PD-discription

Configure port description, usually describe the PD device.

poe PD-discription string

no poe PD-discription

- Parameter

Parameter	Description
string	Port description string.

- Default

null

- Command mode

interface configuration mode

- Instruction

Use the no form of this command to clear the description string.

- Example

The following example shows how to set the POE description of interface f0/1 to "AP-1":

Switch_config_f0/1#poe PD-discription AP-1

- Related commands

none

25.1.16 poe force-power

Configure the forced power function of the port.

poe force-power

no poe force-power

- Parameter

none

- Default

disabled

- Command mode

interface configuration mode

- Instruction

Use the no form of this command to disable the forced power function.

- Example

The following example shows how to set the POE configuration of interface f0/1 to forced power:

Switch_config_f0/1#poe force-power

- Related commands

poe power-management

25.1.17 poe extern-power

Configure the power value of external power supply.

poe extern-power value

no poe extern-power

- Parameter

Parameter	Description
value	Actual power value of external power supply, the unit is W.

- Default

0W

- Command mode

global configuration mode

- Instruction

Use the no form of this command to set the power value of external power supply to the default value (0W). POE power total power=built-in power supply value+ external power supply value. The power configuration value of external power supply is the actual power value.

- Example

When the external power value is 400W, use the following command to configure the external power to 400W.

Switch_config#poe extern-power 400

- Related commands

none