

S3700 Switch Software

Configuration Guide

CONTENTS

1.	Switch Basic Management and Maintenance Commands.....	1
1.1	Login Method.....	1
1.1.1	Console Interface Settings.....	1
1.1.2	Telnet Login Settings.....	2
1.1.3	WEB Management Configuration.....	3
1.2	Introduction to Command Modes.....	5
1.3	System Maintenance and Debugging.....	8
1.3.1	Configuring the Host Name of the System.....	8
1.3.2	Configure the System Clock.....	9
1.3.3	Configuring the Terminal Timeout Property.....	10
1.3.4	View System Information.....	10
1.3.5	Network Connectivity Debugging.....	11
1.3.6	Traceroute Debugging.....	12
1.3.7	Telnet Client.....	12
1.4	Profile Management.....	13
1.4.1	View the Configuration Information.....	13
1.4.2	Saving the Configuration.....	13
1.4.3	Delete the Configuration File.....	14
1.4.4	Configure the File Loading.....	14
1.4.5	Upgrade the Software Version.....	15
2.	Layer Port Settings.....	17
2.1	Open and Close the Port.....	17
2.2	Duplex Mode Configuration.....	17
2.3	Display the Port Information.....	19
2.4	Port Rate-limiting.....	19
3.	Port Monitor.....	22
3.1	Introduction.....	22
3.2	Configure Port Monitor.....	22
4.	LACP Configuration.....	24
4.1	About the LACP Protocol.....	24
4.2	Port Status.....	24
4.3	Aggregation Types.....	24
4.4	Configure Static Aggregation Ports.....	25
4.5	Configure Dynamic Aggregation Ports.....	26
4.6	Mode and Timeout.....	27
4.7	Configure the System Priority.....	28
4.8	Configure the Port Priority.....	29
4.9	Load Balancing.....	29
4.10	Clear LACP Statistics Information.....	30
4.11	Display Aggregation Port Information.....	31

5.	Broadcast Storm Suppression.....	33
5.1	Overview.....	33
5.2	Configure the Ethernet Interface Broadcast Storm Suppression.....	33
5.3	Display Configuration.....	34
6.	MAC.....	35
6.1	Configure the MAC Forwarding and Filtering.....	35
6.2	Configure the Learning Ability of the Port MAC.....	36
6.3	Configure Dynamic MAC Aging Time.....	36
6.3.1	Configure Aging Time.....	36
6.3.2	View the Configuration.....	37
6.4	Configure MAC Binding.....	37
6.4.1	Overview.....	37
6.4.2	Configure MAC Binding.....	37
6.4.3	View the Configuration.....	38
6.5	Delete MAC.....	38
7.	VLAN Configuration.....	39
7.1	Establish a VLAN.....	40
7.2	Delete a VLAN.....	42
7.3	Display a VLAN.....	43
7.4	Ingress Filtering.....	44
7.5	The Configuration of the Message Type Received by the Port.....	46
7.6	Configure the Port with VLAN Mode.....	47
7.7	The VLAN Configuration of Access Mode.....	48
7.8	The VLAN Configuration of Trunk Mode.....	49
7.9	The VLAN Configuration of Hybrid Mode.....	50
7.10	View the VLAN Information.....	51
7.11	Configure the VLAN Based on the MAC Protocol and IP Protocol.....	52
8.	QinQ Configuration.....	54
8.1	QinQ Overview.....	54
8.2	Introduction to the Port Types and the Abbreviations.....	54
8.3	Configure the Basic Functions of QinQ.....	55
9.	MSTP Configuration.....	58
9.1	STP Protocol.....	58
9.1.1	Overview.....	58
9.1.2	Basic Concept.....	58
9.1.3	Port Status.....	59
9.1.4	Message Format.....	60
9.2	MSTP Protocol.....	60
9.2.1	Overview.....	60
9.2.2	Basic Concept.....	61
9.2.3	Port Status and Port Role.....	62

9.3	MSTP Module Implementation.....	62
9.3.1	MSTP Domain.....	62
9.3.2	MSTP Instance.....	63
9.3.3	Protocol Protection Mechanism.....	63
9.4	Configure the Basic Functions of MSTP.....	63
9.4.1	Open MSTP and Configure the running MSTP of the Switch.....	64
9.4.2	Configure the Mapping Relationship between Instances and vlan.....	64
9.4.3	Configure the Priority of Instance 0.....	65
9.4.4	Configure the Priority of the Instances non-zero.....	66
9.4.5	Configure MSTP Domain Name.....	66
9.4.6	Configure MSTP Revision Level.....	67
9.4.7	Configure MSTP Forwarding Delaying Time.....	68
9.4.8	Configure hello time of the MSTP.....	68
9.4.9	Configure MSTP the Configuration Information Timeout Time.....	69
9.4.10	Configure the Largest Diameter of the MSTP.....	70
9.4.11	Configure the Port the Priority in Instance 0.....	70
9.4.12	Configure the Port the Path Cost in Instance 0.....	71
9.4.13	Configure the Port the Priority in any Instance.....	72
9.4.14	Configure the Port the Path Cost in any Instance.....	72
9.4.15	Configure the Port as the Edge Port.....	73
9.4.16	Configure the Port as the Automatic Edge Port.....	74
9.4.17	Display Every Parameters of Instance 0 in the Port.....	74
9.4.18	Display the Detailed Information of MSTP.....	75
9.4.19	Display the Details of the Port in MSTP.....	75
9.4.20	Display the Parameters of the Port in the Instance of Non-zero.....	76
9.4.21	Display the Relevant Information in MSTP Domain.....	76
9.4.22	Display the Instance Information.....	76
9.4.23	Display the MSTP Protocol Running State.....	77
9.5	Configure MSTP Features.....	77
9.5.1	Configure the MSTP bpdu Guard Global Switch.....	78
9.5.2	Configure the Port bpdu-guard Features.....	79
9.5.3	Configure the Global Switch of the MSTP bpdu Filter Function.....	80
9.5.4	Configure the Port bpdu filter Function.....	81
9.5.5	Configure MSTP with the errdisable-timeout Function.....	81
9.5.6	Configure the MSTP errdisable-timeout Interval.....	82
9.5.7	Configure the Port Link Type.....	82
9.5.8	Configure the Port with root guard Function.....	83
9.5.9	Configure the MSTP Version of the Port.....	84
9.5.10	Configure the MSTP Cisco Compatibility.....	84
10.	EAPS.....	86
10.1	Brief Introduction.....	86
10.2	Restrictions.....	86
10.3	Command Introduction.....	86

11.	ACL Configuration.....	89
11.1	The Role of ACL.....	90
11.2	The Classification of ACL.....	90
11.3	ACL Sorted Automatically.....	90
11.4	ACL Matching Order.....	91
11.5	The Appliance of ACL in Switches.....	92
11.6	Input/Output the Matching Fields of ACL and ACE.....	93
11.7	Configure the ACL Announcements.....	93
11.8	The Command IP Access the Control List.....	94
11.9	Configure IP Access Control Lists.....	95
11.10	Display IP Access Control Lists.....	96
11.11	Configure the MAC Extended Access Control List.....	96
12.	ARP Configuration.....	98
12.1	Overview.....	98
12.2	Configure the ARP Timeout.....	98
12.3	Configure the Static ARP.....	99
12.4	Delete the Static ARP.....	100
12.5	Clear the Dynamic ARP.....	100
13.	Static Route.....	101
13.1	Overview.....	101
13.2	Networking Scene.....	101
13.3	Configuration Instances.....	101
13.3.1	Add a Route.....	102
13.3.2	Delete a Route.....	103
13.4	3-Layer Sub-interface Configuration.....	103
13.4.1	Overview.....	103
13.4.2	Networking Scene.....	104
13.4.3	VLAN Sub-interface Configuration.....	104
14.	QoS Configuration.....	107
14.1	Overview.....	107
14.2	QoS Processes.....	107
14.2.1	Classifying.....	107
14.2.2	Policing.....	107
14.2.3	Marking.....	108
14.2.4	Queueing.....	108
14.2.5	Scheduling.....	108
14.3	Configure the QoS.....	109
14.3.1	Default QoS Settings.....	109
14.3.2	Enable the QoS Configuration.....	109
14.3.3	Configure the Interface with the QoS Trust Model.....	110
14.3.4	Configure the Interface with the Default CoS Value.....	110
14.3.5	Configure the Dscp-CoS Map.....	111

14.3.6	Configure Class-map.....	112
14.3.7	Configure Policy-map.....	112
14.3.8	Configure the Interface to Apply with Policy-map.....	113
14.3.9	Configure CoS-Map.....	114
14.3.10	Configure the Output Queue Scheduling Algorithm.....	115
14.4	Show the Configuration.....	115
	Syslog Messages.....	117

1. Switch Basic Management and Maintenance Commands

1.1 Login Method

There are three ways to log in such as serial, Telnet and web.

No authentication mode, the host password authentication mode, and user name password authentication mode are three authentication modes in login.

1. No authentication mode is to log in directly without any verification.
2. The host password authentication mode requires the host password to log in.
3. User name password authentication mode requires user name and password to log in.



Attention: The device default is no authentication which means that you can log in directly without a user name or password.

If the user table is empty, the serial connection will switch to the password authentication mode, and the telnet will be failed to connect; if the password authentication mode and the host password are blank, Telnet cannot log in.

1.1.1 Console Interface Settings

Switch can log in the command line configuration interface to make a simple configuration on the device through the Console line. The specific configuration steps are as follows (in Windows XP operating system, for example):

- 1) Open **【START】 -- 【PROCEDURE】 -- 【ACCESSORY】 -- 【COMMUNICATION】 -- 【HYPERTERMINAL】** (the other way is to open **【START】 -- 【OPERATION】 -- 【type into“hypertrm.exe”】**) in turn ;
- 2) Enter a name in the new connection pop-up and select an icon for the connection. When the configuration is complete, click the button **<OK>** so that configuration is to take effect.

- 3) Select the COM port ;
- 4) Set the bits per second 115200; data bits 8; parity for nothing; stop bit 1; data flow control to none, click the button<OK> to put it into effect ;
- 5) No user name and password is used by default after logging into the Console interface successfully.

1.1.2Telnet Login Settings

Switches needs to configure the management address and login user name password to log in the equipment via telnet. Telnet login configuration steps are as follows:

OPERATION	COMMAND	ILLUSTRATION
Enter into ENABLE mode	enable	-
Enter into CONFIG mode	configure terminal	
Enter into line mode	line vty	-
Log on locally	login local	-
Log out line mode	exit	
Establish one user named aaa, and the password being bbb	username admin password admin	User name length is to 16 characters and password length to 16 characters.
Enter into interface mode	interface vlan1.1	
Configuration management address	ip address 192.168.1.100/24	
Turn on the interface	no shut	
Check current connecting users	Who	

Typed in telnet 192.168.1.100 by cmd

```
C:\Users\luna>telnet 192.168.1.100
```

“Enter” to jump to the following interface:

```
User Access Verification
Username: _
```

Enter a user name admin and password admin. Then log in after going through verification. As shown below:

```
User Access Verification
Username:aaa
Password:
switch>
```

“who” command is available to view the current connection, as shown below:

```
C:\ Telnet 192.168.1.100

User Access Verification
Username:aaa
Password:
switch>en
switch#who
 vty[0] connected from console
 vty[63] connected from console
 vty[78] connected from 192.168.1.25
switch#
```



Attention: Multiple users can simultaneously telnet log in one device, but only one device can be configured to enter the configuration terminal mode.

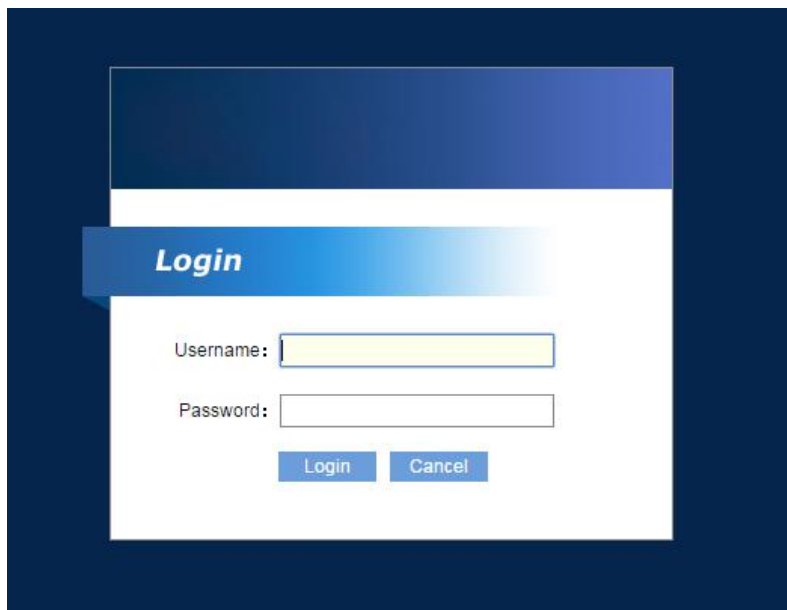
1.1.3WEB Management Configuration

A serial line is used to connect with the switch, and the Hyper Terminal is connected to the switch. After that, enter into the cli command configuration mode and open the web under the global configuration mode, as follows:

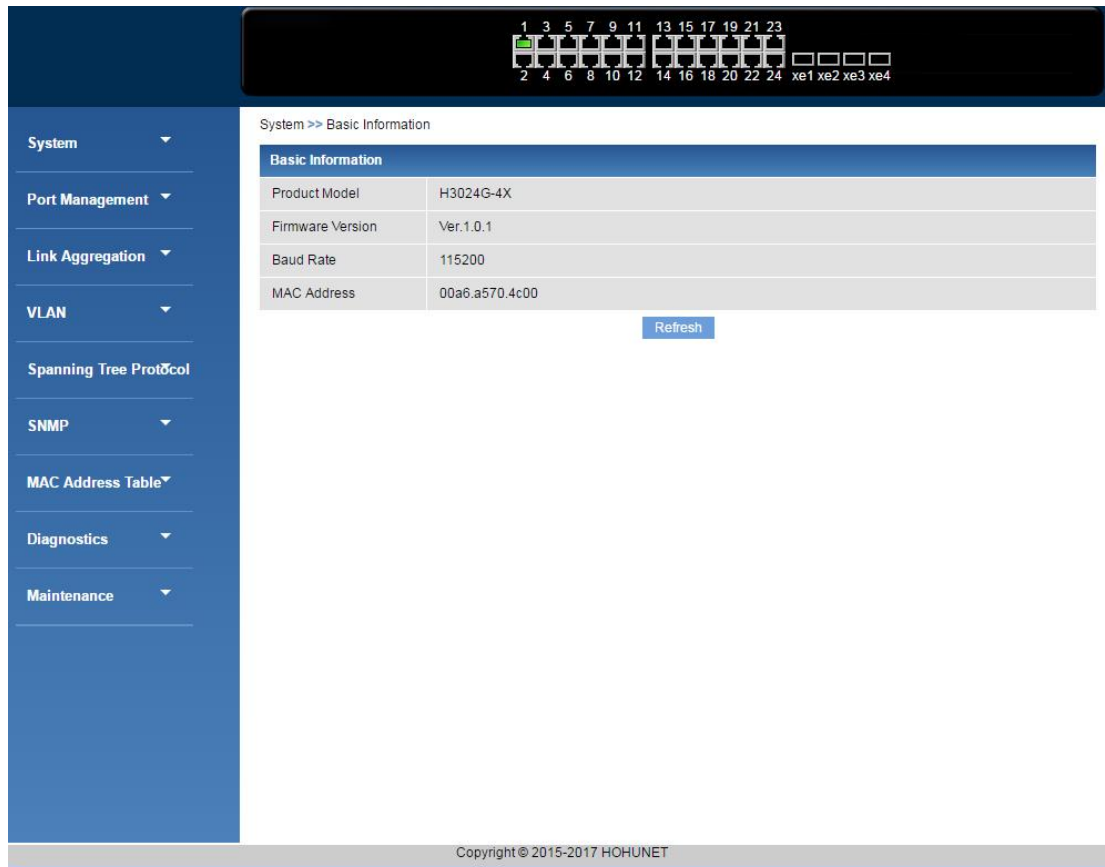
OPERATION	COMMAND	ILLUSTRATION
Enter into ENABLE mode	enable	-
Enter into CONFIG mode	configure terminal	
Open web management	web enable	
Establish a user named aaa, and password being bbb	username admin password admin	Configure the user name and password if the web is

OPERATION	COMMAND	ILLUSTRATION
		to be used
Enter into interface mode	interface vlan1.1	
Configure the management address	ip address 192.168.1.100/24	
Turn on the interface	no shut	

Open a browser and enter in the address bar : 192.168.1.100 to access the switch:



When the user name admin and password admin just configured are entered to log in, the configuration of the switch can begin:



Attention : In order to prevent the web configuration conflicting with the command line, the command line interface must be in enable mode. Otherwise, it will lead to unsuccessful web configuration.

Please note that this device does not have default management IP. To log in the web page must configure management ip first. After that, please note that the copy command is used to save the configuration to avoid the failed login for the loss of configuration caused by the restart

1.2 Introduction to Command Modes

The command line mode can be divided into four main categories, normal mode, privileged mode, global configuration mode and configuration sub-mode which is made by a number of command line modes.

Console and Telnet terminals go into the normal mode first, and then enter the enable command in normal mode and the successful authentication password to enter the privileged mode. For Telnet terminal, the general user can only stay in the normal mode not the privileged mode. In the privileged mode, command line mode transforms to global configuration mode with entering the configure terminal. Under the global configuration,

relevant commands are entered to go into the configuration sub-mode. Each mode corresponding to the prompts is in the following table:

MODE	DESCRIPTION	PROMPT	COMMANDS TO LOG IN THE MODE	COMMANDS TO LOG OUT THE MODE
NORMAL MODE	Providing a display command to view the switch status information.	switch>	The mode the terminal entered first.	Exit or quit in the Console terminal can be used to return to the user login mode. Exit or quit in the Telnet terminal can be used to logout to the Telnet terminal.
PRIVILEGED MODE	Providing a command to debug, upgrade and configure maintenance apart from the display command to view switch status information.	switch #	Enter the command enable in the normal mode.	The command of disables returns to the normal mode. exit or quit in the Console terminal can be used to return to the user login mode. exit or quit in the Telnet terminal can be used to logout to the Telnet terminal.
GLOBAL CONFIGURATION MODE	Providing a common command which cannot be realized in configuration	switch (config)#	Enter the command of configure	Commands of exit, quit and end can return to the

	sub-mode such as configuration a static route command.		terminal in the privileged mode.	privileged mode.
INTERFACE CONFIGURATION MODE	Providing the commands to configure the ports and VLAN interfaces. The ports can be divided into Fast, Gigabit and 10 Gigabit ports.	Fast port : switch(config-fe 1)# Gigabit port : switch(config-ge 1)# 10 Gigabit port : switch(config-xe 1)# VLAN port : switch(config-vlan1.1)#		Commands of exit and quit are used to logout to the global configuration mode, the command end to the privileged mode.
VLAN CONFIGURATION MODE	Providing the command to configure the VLAN. Such as creating and deleting the VLAN command.	switch(config-vlan)#	Enter the vlan database command in the global configuration mode.	Commands of exit and quit are used to logout to the global configuration mode, and the command end to the privileged mode.
MSTP CONFIGURATION MODE	Providing the command to configure the MSTP. Such as creating and deleting the MSTP example command.	switch(config-mst)#	Enter the spanning-tree mst configuration command in the global configuration	Commands of exit and quit are used to logout to the global configuration mode, and the command of end to the privileged mode.

			mode.	
TERMINAL CONFIGURATION MODE	Providing the command to configure Console and Telnet terminal. Such as to configure the terminal overtime command.	switch(config-line)#	Enter the line vty command in the global configuration mode.	Commands of exit and quit are used to logout to the global configuration mode, and the command of end to the privileged mode.

enable --rising the priority to the highest

disable --decreasing the priority to a minimum

exit --typing“exit”in any mode will return to the previous mode

quit --returning to the previous mode

end --returning to user mode from the non-user mode

1.3 System Maintenance and Debugging

The basic system maintenance and debugging features include the followings:

- Configuring the host name of the system
- Configuring the system clock
- Configuring the terminal timeout property
- System reset
- Viewing system information

1.3.1 Configuring the Host Name of the System

The system's host name is used to identify switches, facilitate the user to distinguish between different switches. At the same time, it is still a part of the CLI prompt. The system's host name default is switch.

System hostname's relevent commands are in the following table:

COMMAND	DESCRIPTION	COMMAND LINE
---------	-------------	--------------

		MODE
hostname <name>	Set the system's hostname, and the maximum length of the host name is 256 characters.	GLOBAL CONFIGURATION MODE
no hostname	Clear the system's name which means the host name returns to the default value of Switch.	GLOBAL CONFIGURATION MODE
show running-config	View the current system configuration such as the configuration of the system's host name.	PRIVILEGED MODE

1.3.2 Configure the System Clock

The switches provide real-time clock function which can be set or viewed the current clock via the command. An internal power supply ensures the clock's continuous operation when the system is powered down. Do not need to reset the clock after the system startup.

The clock of the switch is factory-set which users do not need to set again. If the user finds the time wrong, the user can reset the clock.

System clock commands as follows:

COMMAND	DESCRIPTION	COMMAND LINE MODE
systime <date> <time> Date format:2010-01-01 Time format:23:59:59	Set the system clock, the year, month, day, hour, minutes and seconds parameters.	PRIVILEGED MODE
show systime	Display the system clock.	NORMAL MODE, PRIVILEGED MODE

1.3.3 Configuring the Terminal Timeout Property

When there is no entering over a certain time, the terminal will do exit the processing for its security. If the configuration in the terminal mode exceeds time, Console Terminal and Telnet Terminal both come into force simultaneously. The logout of them are different. To Console terminal, command line mode returns to the user login mode if the terminal exceeds the time. But to Telnet terminal, the connection drops and the Telnet terminal logs out.

Terminal timeout default is 10 minutes, and the user can also set the terminal as never timeout.

Terminal timeout's relevant command in the following table:

COMMAND	DESCRIPTION	COMMAND LINE MODE
exec-timeout <minutes> <sec. >	Set the terminal timeout, the unit in minutes and seconds, minutes of the set value of <0-35791 >, seconds to set a value of <0-2147483 >. The minutes and seconds parameters are set to 0:00 which means that the terminal will never exceed the time.	TERMINAL CONFIGURATION MODE
no exec-timeout	Set the terminal timeout back to the default, 10 minutes.	TERMINAL CONFIGURATION MODE
show running-config	View the system configuration such as the configuration of the terminal timeout.	PRIVILEGED MODE

1.3.4 View System Information

The system provides rich display commands to view the operation of the system state and system information. Only several common system maintenance commands are listed in the following table:

COMMAND	DESCRIPTION	COMMAND LINE MODE
---------	-------------	-------------------

show version	Display the version number of the system and the connection time executing the file compiling.	NORMAL MODE, PRIVILEGED MODE
show history	Display a list of the entered commands recently in the CLI command line.	NORMAL MODE, PRIVILEGED MODE

The system information is as follows:

switch#show version

OS : Version 1.0.1 (build 6444)

Created : Jul 13 2012, 17:13:09

Product Name:

MAC Address : 0002.0a0b.0d0e

DRAM SIZE : 65536K bytes

FLASH SIZE : 8192K bytes

Running Time: DAY:0 HOUR:0 MIN:6 SEC:59

View the commands entered in the history as follows:

switch#show history

configure terminal

line vty

ex

exec-timeout 0

ex

end

show running-config

show running-config

1.3.5 Network Connectivity Debugging

For debugging the network connectivity of the switches with other devices, the ping command on the switch needs realizing to ping each other's IP address. If the switch receives the ping response from the other party, it means that the ends are connected. Otherwise, it means that both ends cannot communicate with together.

The switch not only achieves a ping command, but also supports many options with the ping command. Users can do much more accurate and complex debugging with these options.

Ping commands are as follows:

COMMAND	DESCRIPTION	COMMAND LINE MODE
ping <ip-address> [-n <count> -l <size> -r <count> -s <count> -j <count> <ip-address>* -k <count> <ip-address>* -w <timeout>]*	No options, one or more options are all available in using. If none, it is the simple ping command. Ctrl+c can be typed to break off the command's execution.	PRIVILEGED MODE

1.3.6 Traceroute Debugging

In order to debug which devices the network goes through during the switches communicating with the other device in the network, all they need to do is to realize the trace-route command in the switch. When the trace-route command is operated in a switch, the command execution process will display all the paths with the specific IP.

Switches not only achieve the trace-route command, but also support many options with the trace-route command. Users can do much more accurate and complex debugging with these options.

Trace-route commands are as follows:

COMMAND	DESCRIPTION	COMMAND LINE MODE
trace-route <ip-address> [-h <maximum-hops> -j <count> <ip-address>* -w <timeout>]*	No options, one or more options are all available in using. If none, it is the simple trace-route command. Ctrl+c can be typed to break off the command's execution.	PRIVILEGED MODE

1.3.7 Telnet Client

The switch provides Telnet client functionality, and users can remote the access to other devices through the Telnet client.

COMMAND	DESCRIPTION	COMMAND LINE MODE
telnet <ip-address>	The parameter is the IP address of the target device.	PRIVILEGED MODE

1.4 Profile Management

1.4.1 View the Configuration Information

Viewing configuration information includes the current configuration of the system and the initial configuration. The initial configuration is actually the configuration file in FLASH. If there are no configuration files in FLASH, the system is started up with the default configuration. If you look at the initial configuration of the system this time, it will prompt the configuration file not existing.

Configuration information of the command in the following table:

COMMAND	DESCRIPTION	COMMAND LINE MODE
show running-config	View the current configuration of the system.	PRIVILEGED MODE
show startup-config	View the initial configuration of the system.	PRIVILEGED MODE

1.4.2 Saving the Configuration

When users modifies the current configuration of the system, these configurations need to be saved in the configuration file. In this way, they still exist when you open it up next time. Otherwise, the configuration information will be lost after its reset. Saving the configuration is to save the current configuration to the initial configuration.

Configuration saving command is as follows:

COMMAND	DESCRIPTION	COMMAND LINE
---------	-------------	--------------

		MODE
write	Keep the current configuration reserved.	PRIVILEGED MODE



Attention: After users' configuration on switches, the configuration should be reserved with this command. Otherwise, the configuration will be lost after the system's restart.

1.4.3 Delete the Configuration File

When users want the initial configuration to return to the default configuration, the configuration file can be deleted which has no influence on current configuration. If the current configuration needs being the default configuration, please reboot the switch. Deleting the configuration must be careful. Otherwise, the configuration will be lost. The commands to delete the configuration file are as follows:

COMMAND	DESCRIPTION	COMMAND LINE MODE
erase startup-config	Remove the configuration files of the system.	PRIVILEGED MODE
erase private-config	Remove the personal configuration files.	PRIVILEGED MODE

1.4.4 Configure the File Loading

The user can use the command to the configuration file upload to a PC to do a backup for the security of the configuration file. When the system's configuration loses abnormally or the modified configuration needs returning to the original configuration, the original configuration file can be downloaded from the PC to the switch which has no influence on the current configuration. The configuration comes into effect once the switch reboots. The commands to load the configuration file are as follows:

COMMAND	DESCRIPTION	COMMAND
---------	-------------	---------

		LINE MODE
copy tftp startup-config <ip-address> <file-name>	The configuration file will be uploaded in the host flash via tftp. The first parameter is the IP address of the host and the second parameter is the name of the uploaded file.	PRIVILEGED MODE
copy startup-config tftp <ip-address> <file-name>	The configuration file will be downloaded to the local device. The first parameter is the tftp address, and the second parameter is the download file name.	PRIVILEGED MODE

The TFTP protocol is used to configure files loading, run the TFTP client software and the TFTP service on a PC. The steps to load the configuration files are as follows:

Step 1: Building a network environment and the connection of the switch with the PC are configured in a connected state in the same segment.

Step 2: Start the TFTP server software on a PC and set the contents which the configuration file stored.

Step 3: Save the configuration in the switch.

Step 4: Downloading configuration files commands are implemented in the switch to make a configuration file backup to a PC.

Step 5: when the switch needs the configuration file of the PC, configuration file uploading command is implemented in the switch to transform the files from the PC to the switch.

Step 6: To make the configuration effective, and the switch must restart..

1.4.5 Upgrade the Software Version

TFTP is used to the upgrading of the software version. The upgrading commands in privileged mode are as follows:

COMMAND	DESCRIPTION	COMMAND LINE MODE
copy image tftp <ip-address> <file-name>	The configuration file will be uploaded to the host flash via tftp. The first parameter is the IP address of the host, and the second parameter is the name of the software upgrade.	PRIVILEGED MODE

The software upgrading procedure is as follows:

1、 Connecting a PC to the switch, and the device management IP is configured to 192.168.1.100/24. The PC's IP address configuration and switch are kept in the same network segment to ensure the connectivity between the PC and the switch.

```
switch(config)#interface vlan1.1
```

```
switch(config-vlan1.1)#ip address 192.168.1.100/24
```

2、 Selecting the software upgrading path stored in the tftp software as well as the tftp server address (i.e. the local address of the PC).

3、 Using the copy tftp image command in the switch to upgrade the software version.

```
switch#copy tftp image 192.168.1.101 host.jj
```

```
Download(TFTP) ...
```

```
Write flash ...6291456 bytes.
```

```
Download [OK]!
```

4、 After a successful upgrading, the reboot command is used to restart the device in privileged mode to ensure that the software is in effect.



Attention: Please ensure the correctness of the software upgrading, as incorrect software upgrading may lead to the device's crash or software's failed upgrading.

2. Layer Port Settings

2.1 Open and Close the Port

COMMAND	DESCRIPTION	ILLUSTRATION
interface <IFNAME>(e.g. fe, ge, xe, sa, po, vlan)	Enter into the port mode, and the interface is followed by the port type and port number.	Fe stands for Fast port, ge for the Gigabit port, xe Gigabit port, sa for static aggregation port, po for dynamic aggregation port, and vlan for vlan interface.

Switch ports default is to open. If an administrator does not want the user under the port to access the network, this port can be closed.

The commands below are to open the controlled state under the port configuration mode:

no shutdown

Such as opening port 1 administrative states:

Switch(config-ge1)#no shutdown

The following command is to close the administrative state of the port in the port configuration mode:

Shutdown

Such as close the administrative states of port 1.

Switch(config-ge1)#shutdown

2.2 Duplex Mode Configuration

All ports of the system default are auto mode. All the duplex modes of the port are in the following table:

STEP	COMMAND	DESCRIPTION
------	---------	-------------

1	switch# configure terminal	Enter into terminal mode
2	switch(config)# interface IFNAME e.g., switch(config)#interface ge10	Enter into the physical port configuration mode.
3	switch(config-fe10)# speed ? 10-full Force 10 Mbps full operation 10-half Force 10 Mbps half operation 100-full Force 100 Mbps full operation 100-half Force 100 Mbps half operation 1000-full Force 1000 Mbps full operation auto Enable AUTO speed configuration e.g., switch(config-fe10)# speed 100-full	Configuration port duplex mode: 10M full-duplex, 10M half-duplex, 100M full-duplex, 100M half-duplex, 1000M full-duplex and adaptive.
4	end	Exit
5	switch# show interface ge10 Interface ge10 Hardware is Ethernet, address is 0011.2233.44a8 (bia 0011.2233.44a8) Description: This is the test desc. index 5014 metric 1 mtu 1500 duplex-full arp ageing timeout 0 <UP,BROADCAST,MULTICAST> VRF Binding: Not bound Bandwidth 100m input packets 00, bytes 00, dropped 00, multicast packets 00 output packets 00, bytes 00, multicast packets 00 broadcast packets 00	Display the port information, and verify the results.

2.3 Display the Port Information

The command below displays the information of one or one more ports in normal mode or privileged mode:

```
show interface [if-name]
```

For example, display the information of port 1:

```
switch#show interface ge1
```

Interface ge1

Hardware is Ethernet, address is 0011.2233.4457 (bia 0011.2233.4457)

index 5001 metric 1 jumbo-frame 1500 duplex-half

<UP,BROADCAST,MULTICAST>

VRF Binding: Not bound

input packets 00, bytes 00, dropped 00, multicast packets 00

output packets 00, bytes 00, multicast packets 00 broadcast packets 00

2.4 Port Rate-limiting

Switch supports the rate-limiting of the port on the entry/exit direction. The system default is not rate-limiting, and the smallest unit of the port limited rate in kbps can be set as a value of 64k.

The methods of duplexing rate-limiting to configure the port 10 are as follows:

STEP	COMMAND	DESCRIPTION
1.	switch# configure terminal	Enter into terminal mode
2.	switch(config)# interface IFNAME e.g., switch(config)#interface ge10	Enter into the physical port configuration mode.
3.	switch(config-fe10)# line-rate ?	Configuring the port limited

	egress Egress rate ingress Ingress rate	speed: egress is the speed limit for the outbound direction; ingress is the speed limit for the inbound direction.
4.	switch(config-fe10)# line-rate ingress ? LINERATE Limit rate <64-1024000 kbps> (usable units : k, m, g , must be a multiple of 64k) e.g., switch(config-fe10)# line-rate ingress 64k	The port limited rate of the ingress direction (the smallest basic unit is k. The rate must be an integer multiple of 64, and the minimum is 64.) can be configured in units of k, m, and g.
5.	switch(config-fe10)# line-rate egress ? LINERATE Limit rate <64-1024000 kbps> (usable units : k, m, g , must be a multiple of 64k) e.g., switch(config-fe10)# line-rate egress 64k	The port limited rate of the egress direction (the smallest basic unit is k. The rate must be an integer multiple of 64, and the minimum is 64.) can be configured in units of k, m, and g.
6.	end	Exit
7.	switch#show interface ge10 Interface ge10 Hardware is Ethernet, address is 0011.2233.44a8 (bia 0011.2233.44a8) index 5014 metric 1 jumbo-frame 1500 duplex-half <UP,BROADCAST,MULTICAST> VRF Binding: Not bound Bandwidth 10m Ingress Rate 64k burst 64k Egress Rate 128k burst 64k	Display the port information, and verify the results.

	<div>input packets 00, bytes 00, dropped 00, multicast packets 00</div> <div>output packets 00, bytes 00, multicast packets 00</div> <div>broadcast packets 00</div>	
--	--	--

3. Port Monitor

3.1 Introduction

The Port Monitor can monitor the flow of package one or more ports received and send, that is a very useful feature. In addition, it can monitor the package as well. supports Port Monitor which can monitor the incoming data and outgoing data of another port. A monitor port can monitor multiple ports.

3.2 Configure Port Monitor

The configuration steps of configuring the duplexing data of port 2 to port 1 are as follows:

STEP	COMMAND	DESCRIPTION
1.	switch#configure terminal	Enter into terminal mode
2.	switch(config)#interface IFNAME e.g., switch(config)# interface ge1	Enter into the physical port configuration mode.
3.	switch(config-fe1)#mirror ? interface Interface to use	Configuring port mirroring.
4.	switch(config-fe1)#mirror interface ge2 ? direction Mirroring direction	Specify the port to be mirrored (such as: Port ge2)
5.	switch(config-fe1)#mirror interface ge2 direction ? both Mirror traffic in both directions receive Mirror received traffic transmit Mirror transmit traffic e.g., switch(config-fe1)#mirror interface fe2 direction both	Specify direction: both for two-way traffic receive for the port to receive traffic, transmit for the port to send traffic.

6.	end	Exit
7.	switch#show mirror Mirror Test Port Name: ge1 Mirror option: Enabled Mirror direction: both Monitored Port Name: ge2	Display the port information, and verify the results.



Attention: A port can be set to a monitor port and a monitored port at the same time. Monitor port is only one, but the monitored ports can be more than one.

4. LACP Configuration

4.1 About the LACP Protocol

Link Aggregation, sometimes known as port aggregation, is used as a single port through binding the ports with the same properties of the Ethernet switch. Link Aggregation allows customers to enhance the bandwidth of the connection between devices and provide a link backup and load sharing without the hardware upgrading. LACP protocol provides a dynamic link aggregation management.

The LACP protocol sends the LACP configuration information of the local interface to the remote receiver through sending LACPDU message, and it receives the LACPDU message the remote receiver sent at the same time. Then the interface is determined to be added to the aggregation according to the result of calculating the LACP configuration information of the local side and remote side. The port to start LACP has two modes: active mode and passive mode. The passive mode will not take the initiative to do the LACP protocol interaction. Only it receives the LACP message the remote receiver send do it start the interaction of the LACP protocol. Therefore, if both ends of the docking are passive mode, the LACP protocol interaction is not available.

4.2 Port Status

Selected: The state says the port has been elected into an aggregation group, as a member of the aggregation port.

Unselected: The state says the port has not been selected into any aggregation.

Standby: The state says the port has been identified to be added to the aggregation. However, it cannot join the aggregation as the number limiting of the ports in the aggregation.

4.3 Aggregation Types

LACP module realizes the port aggregation of two types, static aggregation and dynamic aggregation. Static aggregation is equivalent to the traditional switch es'Trunk features, and its members of the port group specified by the user. Dynamic aggregation is made up by the protocol running parameters of each port the users set, the aggregation each ports belonged by the protocol calculation and their own ports.

The system provides 8 dynamic and static aggregation groups, named for No. 1-8 individually, eight members in each group. The LACP priority attribute can be set for each interface. The port is added into the priority of the group which is determined by the port number and the properties of the interface. When multiple interfaces can be added into an aggregation that has only one interface margin, the LACP priority and port number decide which interface to join the aggregation.

4.4 Configure Static Aggregation Ports

Create or delete a static aggregation port:

OPERATION	COMMAND	ILLUSTRATION
Enter into ENABLE mode	enable	-
Enter into CONFIG mode	configure terminal	-
Create static LAG group	static-channel-group <1-8>	Create a static LAG group with no members. If adding a member port, it needs to enter into the LAG mode. The maximum LAG group number of the global supporting is 8.
Delete the static aggregation port	no static-channel-group <1-8>	-

Add or remove the member port for the static aggregation port:

OPERATION	COMMAND	ILLUSTRATION
Enter into ENABLE mode	enable	-
Enter into CONFIG mode	configure terminal	-
Create a static aggregation port	static-channel-group <1-8>	Required
Enter into port mode	interface IFNAME	enter into the static aggregation interface mode

		(only in the aggregation interface mode to add and delete ports)
Add member port	static-channel-group member add interface IFNAME	Add a member port in the port mode, and the maximum of each group in the static aggregation is 8 ports.
Delete member port	static-channel-group member remove interface IFNAME	Remove the member ports in the port mode.



Attention: no configuration is best for the added member port. Keep it consistent with the port type. A 100 M port can only be aggregated with the Fast port, and the electrical port with the electrical port. The aggregation port must be in VLAN1.

4.5 Configure Dynamic Aggregation Ports

Configure the dynamic aggregation ports and each dynamic aggregation port can only be added up to 8 member ports.

Configure the dynamic aggregation ports:

OPERATION	COMMAND	ILLUSTRATION
Enter into ENABLE mode	enable	-
Enter into CONFIG mode	configure terminal	-
Enter into port mode	interface IFNAME	Required
Create a dynamic aggregation port	channel-group <1-8> mode <i>(active passive)</i>	Create dynamic aggregation port in the port mode, and add the interface to its member ports

Add a member port	channel-group <1-8> mode (<i>active passive</i>)	Add member ports for the created dynamic aggregation port in the port mode.
Delete a member port	no channel-group	Delete a member port in the physical port mode. When all the member ports of the dynamic aggregation port are deleted, the aggregation port itself will be deleted automatically.
Delete the dynamic aggregation port	no channel-group	When all member ports of the aggregation port are removed, the aggregation port will automatically be deleted.

Illustration: There are active and passive modes in dynamic mode. Active is to initiate the consultation, and a passive is to response the LACP received. The configuration is as follows:

```

Active-----Active      OK
Active-----Passive      OK
Passive-----Passive     NOK

```

OK indicates that the aggregation is established, and NOK is on the contrary.

4.6 Mode and Timeout

Every port can be configured with LACP mode which includes active mode and passive mode. In passive mode, the port will not take the initiative to send LACPDU message to do the protocol interaction. Only the port receives the LACPDU message from the other does it run the LACP protocol, send the LACPDU message and do the protocol calculation.

Each port running LACP protocol sends LACPDU message to the opposite end to inform the LACP property periodically. The period is determined by the timeout mode of the port. Port timeout mode is in two ways: short time mode and long cycle mode. In short time mode, the port sends LACPDU message every 1 second to the opposite end, and it is timeout if the opposite end does not receive it in 3 seconds. In long cycle mode, the port sends the LACPDU message every 30 seconds to the opposite end, and the timeout of the end is 90 seconds.

OPERATION	COMMAND	ILLUSTRATION
Enter into ENABLE mode	enable	-
Enter into CONFIG mode	configure terminal	-
Enter into port mode	interface IFNAME	Enter into the port mode and the port is as the member port for the aggregation port.
Configuring timeout mode	lacp timeout (short long)	The time for short timeout mode is 1 second, and the long cycle mode is 30 seconds.

4.7 Configure the System Priority

Configure the priority of the system which is used to calculate the LACP attribute of the port for the opposite end. A system has only one priority and the default value is 32768.

OPERATION	COMMAND	ILLUSTRATION
Enter into ENABLE mode	enable	-
Enter into CONFIG mode	configure terminal	-
Configuring system priority	lacp system-priority <1-65535>	Configure the system priority, the range of which is 0~65535 , and the default

		value is 32768.
Reset system priority	no lacp system-priority	Restore the default priority 32768.

4.8 Configure the Port Priority

OPERATION	COMMAND	ILLUSTRATION
Enter into ENABLE mode	enable	-
Enter into CONFIG mode	configure terminal	-
Enter into port mode	interface IFNAME	Enter into the port mode, and the port is the member port of the dynamic aggregation port.
Configuring system priority	lacp port-priority <1-65535>	Configure the port priority, the range of which is 1~65535 , and the default value is 32768.
Reset system priority	no lacp port-priority	Restore the default priority 32768.

4.9 Load Balancing

Load balancing algorithm means that some specific physical port transmits the message entering the aggregation port according to some certain algorithm to avoid some ports blocking and some ports free. The system supports the aggregation load balancing. There are some load balancing algorithms in the following:

dst-mac|src-mac|src-dst-mac|dst-ip|src-ip|src-dst-ip|dst-port|src-port|src-dst-port.

dst-mac : The load balancing algorithm of destination MAC address

src-mac : The source MAC address load balancing algorithm

src-dst-mac : Source/destination MAC address load balancing algorithm

dst-ip : The load balancing algorithm of destination IP address

src-ip : The load balancing algorithm of the source IP address

src-dst-ip : The load balancing algorithm of the source/destination IP address

dst-port : The load balancing algorithm of destination port whose port number is TCP/UDP

src-port : Source port load balancing algorithm

src-dst-port : Source/destination port load balancing algorithm

OPERATION	COMMAND	ILLUSTRATION
Enter into ENABLE mode	enable	-
Enter into CONFIG mode	configure terminal	-
Enter into port mode	interface IFNAME	Enter into the port mode, and the port is the dynamic aggregation port.
Configure the load balancing algorithm	port-channel load-balance (<i>dst-mac src-mac src-dst-mac dst-ip src-ip src-dst-ip dst-port src-port src-dst-port</i>)	-
Reset the load balancing algorithm	no port-channel load-balance	Restore the default. The default load balancing algorithm is based on source destination MAC.

4.10 Clear LACP Statistics Information

OPERATION	COMMAND	ILLUSTRATION
-----------	---------	--------------

Enter into ENABLE mode	enable	-
Clear all the LACP statistics information of the aggregation port	clear lacp counters	-
Clear all the LACP statistics information of the specified aggregation port.	clear lacp <1-8> counters	-

4.11 Display Aggregation Port Information

The information on the static and dynamic port aggregation:

OPERATION	COMMAND	ILLUSTRATION
Enter into ENABLE mode	enable	-
Display the static aggregation port	show static-channel-group	-
Display the dynamic aggregation port	show lacp etherchannel	-
Display the summary information of the dynamic aggregation port.	show lacp etherchannel summary	-
Display the detailed information of the dynamic aggregation port.	show lacp etherchannel detail	-
Display the LACP information of the port	show lacp port etherchannel IFNAME	-

Display the device ID of the local system	show lacp sys-id	Display the device ID of the client system, including the system priority and the system MAC address.
Display the load balancing algorithm of the aggregation port.	show lacp etherchannel load-balance	-
Display the transceiver package of the dynamic aggregation port.	show lacp counter	

5. Broadcast Storm Suppression

5.1 Overview

Users can do the configuration under the port through limiting the flow of the broadcast / multicast / unknown unicast the Ethernet allowed.

When the flow of the broadcast / multicast / unknown unicast in the port exceeds the value set by the user, the system will discard the exceeding part to reduce to a limited range in order to ensure the normal operation of the network business.

In order to limit the storm of the looped network in a real environment, the default value of broadcast is 10%, the multicast 100% and dlf 10%.

5.2 Configure the Ethernet Interface Broadcast Storm Suppression

OPERATION	COMMAND	ILLUSTRATION
Enter into ENABLE mode	enable	-
Enter into CONFIG mode	configure terminal	-
Enter into port mode	interface ifname	
Configure the Ethernet interface of the broadcast storm suppression ratio	storm-control broadcast level level	Level: storm suppression percentage (0.0 to 100.0) By default, the default value is of 10%.
Configure the Ethernet interface of the multicast storm suppression ratio	storm-control multicast level level	Level: storm suppression percentage (0.0 to 100.0) By default, the interface does not suppress multicast traffic.
Configure the Ethernet interface of the unicast storm suppression ratio	storm-control dlf level level	Level: storm suppression percentage (0.0 to 100.0) By default, the default value is of 10%.



Illustration :

The “no” command is used to revert to the default value.

Level is calculated according to the physical rate of the port, and fe port is fixed to 100M, ge port fixed to 1000M.

5.3 Display Configuration

OPERATION	COMMAND	ILLUSTRATION
Enter into ENABLE mode	enable	-
Display the broadcast storm suppression configuration of all the ports	show storm-control	Display the broadcast storm suppression configuration of all the ports
Display the unicast storm suppression configuration of all the ports	show storm-control <i>interface-id</i>	Display the broadcast storm suppression configuration of the interface-id port

6. MAC

6.1 Configure the MAC Forwarding and Filtering

MAC address forwarding and filtering functions configured with the message of the MAC address are transmitted to the specified port of vlan, or the specified vlan cannot receive any message taking the MAC address as the source and purpose.

OPERATION	COMMAND	ILLUSTRATION
Enter into ENABLE mode	enable	-
Enter into CONFIG mode	configure terminal	-
Configure the MAC forwarding/ filtering	mac-address-table static <i>mac-address</i> vlan <i>vlan-id</i> {drop interface <i>interface-name</i> }	<i>mac-address</i> : specify the table body corresponding to the destination MAC address <i>vlan-id</i> : specify the VLAN the address belonged <i>interface-id</i> : interface name When the device receives the message taking the mac-address as the destination on the VLAN vlan specified, the message is forwarded in this port; when the configuration is drop, the device should discard the entire message taking mac-address as source or destination in the ports of vlan-id.
Delete the configuration of the MAC forwarding/filtering	no mac-address-table static <i>mac-address</i> vlan <i>vlan-id</i> {drop interface <i>interface-name</i> }	Delete the MAC forwarding entries or filter table bodies, and the parameters should correspond with the adding

OPERATION	COMMAND	ILLUSTRATION
		command
View the MAC forwarding/filtering	show mac-address-table	View the MAC forwarding/filtering table

6.2 Configure the Learning Ability of the Port MAC

Open or close the learning ability of the configuring port for MAC address:

OPERATION	COMMAND	ILLUSTRATION
Enter into ENABLE mode	enable	-
Enter into CONFIG mode	configure terminal	-
Enter into port mode	interface <i>interface-id</i>	
Configure MAC learning	mac-address-learning enable	Open the MAC learning function(default)
Close MAC learning	no mac-address-learning	Close the port MAC learning function which means the port cannot learn new MAC address.



Illustration: If the MAC binding function in the port is open, the MAC learning function is not available.

6.3 Configure Dynamic MAC Aging Time

6.3.1 Configure Aging Time

After configured the MAC address aging function, the device will delete all dynamically learned MAC address entries once it reaches to its aging time. Then, the device begins to relearning. If the MAC address aging is turned off, the dynamic MAC address table will be updated no longer.

OPERATION	COMMAND	ILLUSTRATION
Enter into ENABLE mode	enable	-
Enter into CONFIG mode	configure terminal	-
Configure dynamic address	mac-address-table	Set the time length kept in the dynamic

OPERATION	COMMAND	ILLUSTRATION
aging time	agint-time {<0-0> <10-1000000>}	address table after being learned in second. The range is 10-1000000 seconds, and the default is 300 seconds. Configuration 0 means to turn off the aging of the mac address.
Cancel configuring mac aging time	no mac-address-table agint-time	Restore mac address aging time for the default value(300s)



Attention:

Dynamic MAC address aging is finished in the second cycle it configured by its own.

6.3.2View the Configuration

View the MAC address aging configuration information:

OPERATION	COMMAND	ILLUSTRATION
Enter into ENABLE mode	enable	-
View the dynamic address aging time	show mac-address-table aging-time	View the aging configuration information of all addresses

6.4 Configure MAC Binding

6.4.1Overview

The port is only allowed to receive the bound MAC message as the receiving source and forward the bound MAC message as the destination.

6.4.2Configure MAC Binding

OPERATION	COMMAND	ILLUSTRATION
Enter into ENABLE mode	enable	-
Enter into CONFIG mode	configure terminal	-
Enter into port mode	interface <i>interface-id</i>	-
Configure MAC binding	switchport port-security	Port <i>interface-id</i> only allows the message

OPERATION	COMMAND	ILLUSTRATION
	mac-address <i>mac-address</i> vlan <i>vlan-id</i>	taking mac-address as address in <i>vlan-id</i> to go through.
Delete MAC binding	no switchport port-security mac-address <i>mac-address</i> vlan <i>vlan-id</i>	Delete MAC binding, and the parameter correspond with that added before.



Illustration:

- One port can be bound to multiple MAC addresses which need multiple configurations.
- One time is to delete one bound MAC. When the last bound MAC is deleted, the port MAC binding is lifted.
- After opening the port MAC binding, the port dynamic MAC learning function will be closed and cannot be re-open.
- After opening the port MAC binding, the static MAC configured and the dynamic MAC addresses learnt in the port will be deleted.
- Do not configure MAC forwarding and filtering with the port once the MAC binding function opens.
- Do not delete the static address of the port after opening the MAC binding function.
- After opening the port MAC binding, the command of deleting the MAC address cannot delete the bound MAC, and the system is silent.

6.4.3 View the Configuration

OPERATION	COMMAND	ILLUSTRATION
Enter into ENABLE mode	enable	-
View the dynamic address aging time	show port-security	View all MAC binding information.

6.5 Delete MAC

OPERATION	COMMAND	ILLUSTRATION
Enter into ENABLE mode	enable	-
Delete the dynamic MAC	clear mac address-table dynamic	Delete all dynamic addresses on the

OPERATION	COMMAND	ILLUSTRATION
address		device.
	clear mac address-table dynamic address <i>mac-address</i>	Delete the specified dynamic address <i>mac-address</i> : specify the MAC address to be deleted
	clear mac-address-table dynamic vlan <i>vlan-id</i>	Delete all dynamic addresses on a specific VLAN <i>vlan-id</i> : specify the VLAN the dynamic addresses to be deleted belonged
	clear mac-address-table dynamic interface <i>interface-id</i>	Delete all dynamic addresses on a specific physical interface. <i>interface-id</i> : specific physical interface.
	no mac-address-table static MAC vlan <1-4094> interface IFNAME	Press vlan+port to delete the mac

7. VLAN Configuration

VLAN (Virtual Local Area Network) is a network segment divided from a LAN logically by a LAN device in order to achieve the emerging data exchanging technology of the virtual work.

The advantages of VLANs:

- Broadcast storm prevention
- Security
- Reduced costs
- Performance enhancing
- Facilitating the application and management
- Flexibility

Ethernet ports have three linking types: Access, Hybrid and Trunk.

The ports of Access type only belong to one VLAN, and it is generally used to connect the computer port;

Allowing multiple vlan go through, the ports of Trunk types can receive and transmit multiple vlan messages and they are generally used for the connection between the ports of switches;

Allowing multiple vlan go through, the ports of Hybrid types can receive and transmit multiple vlan messages and they are generally used for the connection between the ports of switches as well as users' computers.

The dealing method of receiving data for Hybrid ports and Trunk ports is the same, and the only difference is located in sending data: Hybrid ports allow to send multiple vlan messages without tags and Trunk ports only allow to send the default message without tags.

7.1 Establish a VLAN

STEP	COMMAND	DESCRIPTION
1.	switch# configure terminal	Enter into terminal mode
2.	switch(config)# vlan database	Enter into VLAN configuration mode
3.	switch(config-vlan)# vlan ? <2-4094> VLAN id VLAN_ID The List of the VLAN IDs that will be added, range <2-4094>, format:2,4,6 or 3-10 e.g., 1. Establish a sigle VLAN switch(config-vlan)#vlan 10 switch(config-vlan)#vlan 11 switch(config-vlan)#vlan 12 2. Establish specified VLAN range in bulk, and the maximum of each bulk will be 100 vlans every time switch(config-vlan)#vlan 10,11,12 or switch(config-vlan)#vlan 10-12 3. Establish a VLAN and specify the VLAN another	Parameters: VLAN ID can be configured as 2-4094, and multiple VLANs configured can be separated by a comma or a specified range in bulk. The maximum length VLAN described is 16 characters. Two ways to establish VLAN: 1. Establish single VLAN 2. Establish in bulk in the specified VLAN range

	name switch(config-vlan)#vlan 10 name aaa 4. Establish a VLAN and specify the VLAN state at the same time. switch(config-vlan)#vlan 11 state disable	
4.	end	Exit
5.	switch# show vlan VLAN ID Name State Instance L3 Interface Member ports (u)-Untagged, (t)-Tagged ===== ===== ===== ===== ===== ===== 1 default ACTIVE 0 vlan1.1 ge1(u) ge2(u) ge3(u) ge4(u) ge5(u) ge6(u) ge7(u) ge8(u) ge9(u) ge10(u) ge11(u) ge12(u) ge13(u) ge14(u) ge15(u) ge16(u) ge17(u) ge18(u) ge19(u) ge20(u) ge21(u) ge22(u) ge23(u) ge24(u) ge25(u) ge26(u) ge27(u) ge28(u) ge29(u) ge30(u) ge31(u) ge32(u) ge33(u) ge34(u) ge35(u) ge36(u) ge37(u) ge38(u) ge39(u) ge40(u) ge41(u) ge42(u) ge43(u) ge44(u) ge45(u) ge46(u) ge47(u) ge48(u) 10 aaa ACTIVE 0	Display VLAN and verify the results.

11	VLAN0011	SUSPEND 0
12	VLAN0012	ACTIVE 0

7.2 Delete a VLAN

STEP	COMMAND	DESCRIPTION
1.	switch# configure terminal	Enter into terminal mode
2.	switch(config)# vlan database	Enter into VLAN configuration mode
3.	switch(config-vlan)# no vlan ? <2-4094> VLAN id VLAN_ID The List of the VLAN IDs that will be added, range <2-4094>, format:2,4,6 or 3-10 e.g., 5. Delete a single VLAN switch(config-vlan)#no vlan 10 switch(config-vlan)#no vlan 11 switch(config-vlan)#no vlan 12 6. Delete the specified VLAN range in bulk switch(config-vlan)#no vlan 10,11,12 或 switch(config-vlan)#no vlan 10-12	Deleting VLAN supports a single deletion and bulk deletion.
4.	end	Exit
5.	switch# show vlan VLAN ID Name State Instance L3 Interface Member ports (u)-Untagged, (t)-Tagged =====	Display VLAN and verify the results.

	<pre> ===== ===== 1 default ACTIVE 0 vlan1.1 ge1(u) ge2(u) ge3(u) ge4(u) ge5(u) ge6(u) ge7(u) ge8(u) ge9(u) ge10(u) ge11(u) ge12(u) ge13(u) ge14(u) ge15(u) ge16(u) ge17(u) ge18(u) ge19(u) ge20(u) ge21(u) ge22(u) ge23(u) ge24(u) ge25(u) ge26(u) ge27(u) ge28(u) ge29(u) ge30(u) ge31(u) ge32(u) ge33(u) ge34(u) ge35(u) ge36(u) ge37(u) ge38(u) ge39(u) ge40(u) ge41(u) ge42(u) ge43(u) ge44(u) ge45(u) ge46(u) ge47(u) ge48(u) </pre>	
--	--	--

7.3 Display a VLAN

STEP	COMMAND	DESCRIPTION
1.	<pre> switch#show vlan VLAN ID Name State Instance L3 Interface Member ports (u)-Untagged, (t)-Tagged ===== ===== 1 default ACTIVE 0 vlan1.1 vlan1.1 ge1(u) ge2(u) ge3(u) ge4(u) ge5(u) ge6(u) ge7(u) ge8(u) ge9(u) ge10(u) ge11(u) ge12(u) </pre>	Display all the VLAN

	<pre> ge13(u) ge14(u) ge15(u) ge16(u) ge17(u) ge18(u)ge19(u) ge20(u) ge21(u)ge22(u)ge23(u) ge24(u) ge25(u) ge26(u) ge27(u)ge28(u) ge29(u) ge30(u)ge31(u) ge32(u) ge33(u)ge34(u) ge35(u) ge36(u) ge37(u) ge38(u) ge39(u)ge40(u) ge41(u) ge42(u)ge43(u) ge44(u) ge45(u) ge46(u) ge47(u) ge48(u) 10 VLAN0010 ACTIVE 0 </pre>	
2.	<pre> switch#show vlan 10 VLAN ID Name State Instance L3 Interface Member ports (u)-Untagged, (t)-Tagged ===== ===== ===== ===== ===== 10 VLAN0010 ACTIVE 0 </pre>	Display the specified VLAN

7.4 Ingress Filtering

Ingress filtering is to discard those packets in different VLANs at the inlet which can save bandwidth and reduce the workload of the port to process the packets in the follow-up as far as possible.

STEP	COMMAND	DESCRIPTION
1.	switch# configure terminal	Enter into terminal mode
2.	switch(config)# interface ge2	Enter into the port configuration mode
3.	switch(config-ge2)# switchport mode access ? ingress-filter Set the ingress filtering of the frames received	Choose one type of the three ports: access, hybrid, and trunk

	<cr>	
4.	switch(config-ge2)# switchport mode access ingress-filter ? disable Disable ingress filtering enable Enable ingress filtering e.g., switch(config-ge2)#switchport mode access ingress-filter enable	Open/close the ingress filtering
5.	end	Exit
6.	switch#show interface switchport Interface name : ge1 Switchport mode : access Ingress filter : disable Acceptable frame types : all Default Vlan : 1 Configured Vans : 1 Interface name : ge2 Switchport mode : trunk Ingress filter : enable Acceptable frame types : vlan-tagged only Default Vlan : 1 Configured Vans : 1 100 200 Interface name : ge3 Switchport mode : access Ingress filter : disable Acceptable frame types : all Default Vlan : 1 Configured Vans : 1 Interface name : ge4 Switchport mode : access Ingress filter : disable	Display interface and verify the results.

Acceptable frame types	: all	
Default Vlan	: 1	
--More--		

7.5 The Configuration of the Message Type Received by the Port

A port can be configured to receive the frame type. And access, trunk and hybrid three modes of the port all can be set to receive the type of message.

STEP	COMMAND	DESCRIPTION
1.	switch# configure terminal	Enter into terminal mode
2.	switch(config)# interface ge1	Enter into the port configuration mode
3.	switch(config-ge1)# switchport mode hybrid	Parameters : access, trunk, and hybrid The port is configured as a hybrid mode.
4.	switch(config-ge1)#switchport mode hybrid acceptable-frame-type ? all Set all frames can be received vlan-tagged Set vlan-tagged frames can only be received	Configure frame types the ports can receive, all for all frames, tagged or untagged, and vlan-tagged just for tagged frame.
5.	end	Exit
6.	switch#show interface switchport Interface name : ge1 Switchport mode : hybrid Ingress filter : disable Acceptable frame types : vlan-tagged only	Display interface information and verify the results.

Default Vlan	: 1
Configured Vlans	: 1
Interface name	: ge2
Switchport mode	: trunk
Ingress filter	: disable
Acceptable frame types	: vlan-tagged only
Default Vlan	: 1
Configured Vlans	: 1 100 200
Interface name	: ge3
Switchport mode	: access
Ingress filter	: disable
Acceptable frame types	: all
Default Vlan	: 1
Configured Vlans	: 1
Interface name	: ge4
Switchport mode	: access
Ingress filter	: disable
Acceptable frame types	: all
Default Vlan	: 1
--More--	

7.6 Configure the Port with VLAN Mode

Before configuring the port VLAN, the VLAN mode needs to specify. The port VLAN mode by default is the ACCESS mode. The VLAN mode commands of the specified port are as follows:

COMMAND	DESCRIPTION	CONFIGURATION MODE
switchport mode access	The VLAN mode of the specified port is ACCESS mode. The port running the command is the untagged member of	Interface configuration mode

	VLAN1, and the default VLAN is 1.	
switchport mode trunk	The VLAN mode of the specified port is TRUNK mode. The port running the command is the untagged member of VLAN1, and the default VLAN is 1.	Interface configuration mode
no switchport trunk	The VLAN of the port is no longer TRUNK mode, and it returns to the default situation, the ACCESS mode.	Interface configuration mode
switchport mode hybrid	The VLAN mode of the specified port is hybrid mode. The port running the command is the untagged member of VLAN1, and the default VLAN is 1.	Interface configuration mode
no switchport hybrid	The VLAN of the port is no longer HYBRID mode, and it returns to the default situation, the ACCESS mode.	Interface configuration mode

7.7 The VLAN Configuration of Access Mode

Before the port VLAN configuration, the VLAN mode of the port is specified to be ACCESS mode. To this VLAN mode, the port by default is an untagged member of VLAN1, and the VLAN default of the port is 1. The VLAN configuration commands for the ACCESS mode are in the following:

COMMAND	DESCRIPTION	CONFIGURATION MODE
switchport access vlan <vlan-id>	The configuration port is an untagged member of the specified VLAN. The port's default VLAN is specified VLAN. Parameter range is 2-4094.	Interface configuration mode

no switchport access vlan	The VLAN configuration of the port returns to the default which means the port is an untagged member of VLAN1, and the default of the port is 1.	Interface configuration mode
---------------------------	--	------------------------------

7.8 The VLAN Configuration of Trunk Mode

Before the VLAN configuration of the port, the VLAN mode of the port is specified to be TRUNK mode. To this VLAN mode, the port by default is a tagged member of VLAN1, and the VLAN default of the port is 1. The VLAN configuration commands for the TRUNK mode are in the following:

COMMAND	DESCRIPTION	CONFIGURATION MODE
switchport trunk allowed vlan except <vlan-list>	The configuration port takes all the tagged members of VLAN in except some VLAN.	Interface configuration mode
switchport trunk allowed vlan none	Apart from VLAN1, the port is no longer the tagged member of VLAN for all the other VLAN	Interface configuration mode
switchport trunk allowed vlan add <vlan-list>	Configuration port can be a tagged member of specified one or multiple VLAN. Parameter <vlan-list> can be a VLAN, a VLAN RANGE or multiple VLANs. For example, the parameter can be "1", "2-4" or "1, 3, 5".	Interface configuration mode
switchport trunk allowed vlan remove <vlan-list>	The port is cleared from the specified one or more VLANs	Interface configuration mode

	and it is no longer the tagged member of the VLAN. Parameter <vlan-list> can be a VLAN, a VLAN RANGE or multiple VLANs. For example, the parameter can be "1", "2-4" or "1, 3, 5".	
--	--	--

7.9 The VLAN Configuration of Hybrid Mode

Before the port VLAN configuration, the VLAN mode of the port is specified to be HYBRID mode. To this VLAN mode, the port by default is an untagged member of VLAN1, and the VLAN default of the port is 1. The VLAN configuration commands for the HYBRID mode are in the following:

COMMAND	DESCRIPTION	CONFIGURATION MODE
switchport hybrid vlan <vlan-id>	The configuration port is an untagged member of the specified VLAN, and the port default VLAN is the specified VLAN. The parameter range is 2-4094.	Interface configuration mode
no switchport hybrid vlan	The port is cleared from the default VLAN and the default VLAN tagged or untagged member no longer. The default of the port returns to 1.	Interface configuration mode
switchport hybrid allowed vlan none	Apart from the VLAN1, the port is no longer any tagged or untagged member of all the other VLAN. The default VLAN of the port returns to 1.	Interface configuration mode
switchport hybrid allowed vlan add <vlan-list> egress-tagged enable	The port is configured to be a specified tagged member of one or more	Interface configuration

	VLANs. Parameter <vlan-list> can be a VLAN, a VLAN range and multiple VLANs. For example, the parameter can be "1", "2-4" and "1, 3, 5".	mode
switchport hybrid allowed vlan add <vlan-list> egress-tagged disable	The port is configured to be a specified untagged member of one or more VLANs. Parameter <vlan-list> can be a VLAN, a VLAN range and multiple VLANs. For example, the parameter can be "1", "2-4" and "1, 3, 5".	Interface configuration mode
switchport hybrid allowed vlan remove <vlan-list>	The port is cleared from the specified one or more VLANs and no longer the tagged or untagged member of these VLANs. If the default VLAN of the port belongs to the specified VLAN, the default VLAN returns to 1.	Interface configuration mode

7.10 View the VLAN Information

The commands to view the VLAN information are in the following:

COMMAND	DESCRIPTION	CONFIGURATION MODE
show vlan [vlan-id]	All the VLAN information will be displayed without inputting any parameters, and the specified VLAN information will be displayed with parameters entered. The parameter ranges from 1 to 4094.	Normal mode, privileged mode
show interface switchport	Display all the VLAN relevant information of the ports in the system, such as the VLAN mode, the default VLAN and so on.	Normal mode, privileged mode

show running-config	View the system configuration which is detailed to the VLAN configuration.	Privileged mode
---------------------	--	-----------------

7.11 Configure the VLAN Based on the MAC Protocol and IP Protocol

If the message is an empty VLAN ID message (UNTAG or Priority message), the VLAN ID the message adding TAG will be elected from the corresponding VLAN ID group of the VLAN classification in the input port with the device supporting the configuration VLAN classification. The device supports the following methods to divide the VLAN (ordered): the method based on MAC, the method based on IP subnet, and the method based on protocol. The VLAN configuration of all the above methods are configured in global mode and the opening is under the interface mode. Then, all the rules come into force.

COMMAND	DESCRIPTION	CONFIGURATION MODE
vlan classifier rule <1-999> mac <mac-address> vlan <vlan-id>	Configure the VLAN rule which is based on MAC The range of the Rule ID : 1-999	Global configuration mode
vlan classifier rule <1000-1999> ipv4 <ip-address> vlan <vlan-id>	Configure the VLAN rule which is based on IP. The range of the Rule ID : 1000-1999	Global configuration mode
vlan classifier rule <2000-2099> proto <proto-type> encap {ethv2 nosnapllc snapllc} vlan <vlan-id>	Configure the VLAN rule which is based on protocol. The range of the Rule ID : 2000-2099. <proto-type> is taken as the protocol type.	Global configuration mode

vlan classifier activate mac-vlan	Use the vlan based on MAC	Interface mode
vlan classifier activate ip-subnet-vlan	Use the vlan based on IP	Interface mode
vlan classifier activate protocol-vlan rule < 2000-2099>	Use the vlan based on protocol	Interface mode
no vlan classifier activate {mac-vlan ip-subnet-vlan protocol-vlan rule < 2000-2099>}	Delete the vlan based on MAC/subnet/protocol	Interface mode
show vlan classifier rule <1-999 1000-1999 2000-2999>	Display the VLAN classification rules	Normal mode, privileged mode
show vlan classifier interface <interface-id>	Display the VLAN classification information configured in the port.	Normal mode, privileged mode



Illustration: The number of the protocol-based VLAN configured on the interface can be one more.

8. QinQ Configuration

8.1 QinQ Overview

QinQ is the expansion of the 802.1Q. Its core idea is to encapsulate the user private network VLAN tag to the public network VLAN tag to provide the user with a simpler two layer VPN tunnel as the message goes through the service provider's backbone network with two layers of tag. It is characterized by simple and easy management, supporting without signals, realizing through static configuration and small-type enterprise or small-scale MAN suited whose backbone is three-layer switches.

8.2 Introduction to the Port Types and the Abbreviations

There are three Ethernet port link types that the device supports:

Access Type : Only belonging to one VLAN, the port is generally used for the connection between the switch and end-users;

Trunk Type : Belonging to multiple VLANs, the port receives and sends the messages of multiple VLANs and is generally used for the connection between the switches;

Hybrid Type : Belonging to multiple VLANs, the port can receive and send messages of multiple VLANs and is used for the connection between switches and the connection between users' computers.



Illustration: Hybrid port allows sending multiple VLAN message without labels, and Trunk port only allows sending the default VLAN message with no labels

The ports of three types can exist in one device.

Abbreviation for comment :

NNI:Network-Network Interface

UNI:User-Network Interface

8.3 Configure the Basic Functions of QinQ

Configure VLAN:

OPERATION	COMMAND	ILLUSTRATION
Enter into ENABLE mode	enable	-
Enter into CONFIG mode	configure terminal	-
Enter into VLAN mode	vlan database	Optional By default, all the ports are in vlan1.
Create a VLAN	vlan VLANID1 , VLANID2	Optional By default, only vlan1 exists, and the qinq function based on vlan translation cannot be used.

The working status of the configuration interface:

OPERATION	COMMAND	ILLUSTRATION
Enter into ENABLE mode	enable	-
Enter into CONFIG mode	configure terminal	-
Enter into interface mode	Interface IFNAME	-
Configure the interface working mode	switchport mode trunk	-
Configure the vlan	switchport trunk allowed vlan add	Configure UNI, VLANID=VLANID1;

the interface belongs to	VLANID	configure NNI, VLANID=VLANID2
Configure the interface mode	switchport vlan-stacking {customer-edge-port provider-port } (ethertype ETHERTYPE)	Required Use the qinq at this port and set the mode. Optional Configure the tpid value, using the default value 0x8100 if no configuring.



Illustration: At this point, the port-based qinq is to complete. After that one port is configured as customer mode, all the ports will be configured as customer mode. When one port is configured as provider mode and the present port is configured as provider mode, all the other ports will be configured as customer mode.

Configure the qinq based on vlan translation:

OPERATION	COMMAND	ILLUSTRATION
Enter into ENABLE mode	enable	-
Enter into CONFIG mode	configure terminal	-
Enter into interface mode	Interface IFNAME	-
Configure the vlan the port belongs to	switchport trunk allowed vlan add VLANID	When the port is a UNI port, VLANID=VLANID1; when the port is an NNI port, VLANID=VLANID2.
Configure the vlan translation entry of the UNI interface	switchport vlan mapping VLANID1 VLANID2	When vlan id!=VLANID1 of the tag on the outermost of the package, the vlan translation does not work.



Illustration: When the vlan translation table does not work, the port-based qinq function will come into use.

Delete an entry in the vlan translation table:

OPERATION	COMMAND	ILLUSTRATION
Enter into ENABLE mode	enable	-
Enter into CONFIG mode	configure terminal	-
Enter into interface mode	Interface IFNAME	-
Delete one entry in the vlan translation table	no switchport vlan mapping VLAN-ID	VLAN-ID is the VLAN-ID1 for establishing the vlan translation table

Delete all the entries on the vlan translation table:

OPERATION	COMMAND	ILLUSTRATION
Enter into ENABLE mode	enable	-
Enter into CONFIG mode	configure terminal	-
Delete all the entries on the vlan translation table	no switchport vlan mapping all	Delete the vlan translation entries of all the ports

Close the qinq function:

OPERATION	COMMAND	ILLUSTRATION
Enter into ENABLE mode	enable	-
Enter into CONFIG mode	configure terminal	-
Enter into interface mode	Interface IFNAME	-
Close the qinq function	no switchport vlan-stacking	-

9. MSTP Configuration

9.1 STP Protocol

9.1.1 Overview

STP protocol is a single spanning tree protocol which is to put all the bridge devices into a single spanning tree topology in the network to ensure the full connectivity and loop-free link of the network connection.

At first, STP protocol selects one root for the spanning tree, and then according to the distance of each bridge device to the root bridge, the root path will be determined. In this way, the root, bridge devices and the path between them make up a spanning tree with a full communication and no cycles. The STP protocol makes the interaction of the protocol data through BPDU (bridge protocol data unit). The STP BPDU is a message with two layers, and its MAC is multicast address of 01-80-C2-00-00-00. All the net bridges supporting STP protocol will receive and deal with the received BPDU message which will not be forwarded.

9.1.2 Basic Concept

Bridge identifier: Each bridge has an identifier, and the BID is composed of two parts. The first two bytes mean the priority and the default of 32768 can range in 0-65535. The last 6 bytes is made up by the MAC address of the bridge. Make sure the BID of each bridge in the network is unique.

Root Bridge : The bridge is taken as the root of a spanning tree in the network, and it has the smallest BID.

Root identifier (RID) : the identifier in the root bridge

Path cost : It is the path cost the package transmission required in the network. The cost is to determine the path cost of the packet in the network according to the LAN type (bandwidth and duplex mode). The cost is the key parameter used to determine the most excellent spanning tree.

Port identifier(PID) : Each port of each bridge has a PID which consists of two parts for 16 bits. (The first 6 bits take for the priority, and the last 10 bits stand for the port name without official instructions.)

Root path cost : The overhead the package needs to arrive at the root bridge.

Root port : The port of the smallest cost the non-root bridge needs to reach the root bridge.

Designated port: One of the ports connecting to a LAN has the minimum root path. The port is called as the designated port of the LAN.

Designated bridge : The bridge the specified port of the LAN located in is called as the designated port of the LAN.

Alternate port : Backup ports

9.1.3Port Status

Blocking: The port is in permitting status. However, according to the calculation results of STP algorithm, the port does not belong to the effective ports of the spanning tree. (There are other paths to generate a spanning tree structure and the paths have a better structure than the port.) The port in blocking only receives the STP BPDU message with no forwarding, and does not receive or forward the message of other business.

Listening : In permitting status, the port is elected as an effective port to make up the spanning tree. However, in order to prevent the spanning tree's instability caused by the turmoil and changes of the network topology, the listening status is added up between the blocking status and forwarding status. The listening status monitors BPDU packets in the network to judge whether there is a better path or not, and the port begins to delete the relevant entries in the FDB table. The state receives and forwards STP BPDU message not the ordinary business message.

Learning : In permitting status, the port is elected as an effective port to make up the spanning tree. However, in order to prevent the spanning tree's instability caused by the turmoil and changes of the network topology, the learning status is added up between the blocking status and forwarding status. When the port keeps the listening status for a certain time (forwarder timer), if there is no better path, the port will turn to learning status. The status monitors BPDU message in the network to judge whether there is a better path. At the same time, the port receives and forwards STP BPDU message receives the ordinary business message without forwarding and learns the MAC address of the message.

Forwarding : In permitting status, the port is elected as an effective port to make up the spanning tree. When the port keeps the listening status for a certain time (forwarder timer), if there is no better path, the port will turn to forwarding status from learning status. The status receives and forwards STP BPDU message as well as ordinary business

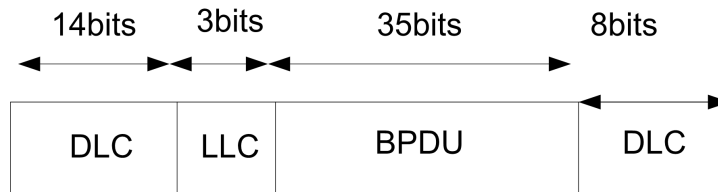
message.

Disable : The state is considered as the port without connection physically.

Port State	Address Learning Ability	Forwarding/receiving Message Ability	Receive BPDU Message	Forward BPDU Message
Disabled	NO	NO	NO	NO
Blocking	NO	NO	YES	NO
Listening	NO	NO	YES	YES
Learning	YES	NO	YES	YES
Forwarding	YES	YES	YES	YES

9.1.4 Message Format

STP protocol uses BPDU message to carry the interaction information the protocol needs. There are two kinds of STP protocol message: configuration BPDU and topology change notification BPDU. BPDU message format is shown in the following:



BPDU takes 01-80-c2-00-00-00 destination multicast address as the destination address.

9.2 MSTP Protocol

9.2.1 Overview

MSTP protocol is a Multi Spanning Tree protocol which introduces the concept of instances and domains compared with RSTP. The domain is the unified configuration implemented in the network segment and can do the spanning tree constructing in the region independently in order to divide the net segment with different configuration in the network. A single spanning tree will connect the entire domain between domains to ensure the connectivity and no cycles. (The spanning tree is known as CST, public spanning tree.) More than one spanning tree instances can be constructed in the domain, and the different VLANs can be mapped to the different spanning tree instances at the same time. Each domain inside has an instance ID of 0, and the instance and CST make up the CIST (Common Internal Spanning Tree) together. The spanning tree connects the domains, the

bridge devices of their own and the net segments into a full-link tree without cycles. Domain is made up by multiple devices in the switched network and the segments between them. These devices are characterized by MSTP opening, the same domain name, the same instance mapping configuration from the VLAN to the spanning tree, the same MSTP revised configuration, and the link between the devices are connected physically.

In the initial phase of the LAN configuration, MTSP will elect one root switch according to every switch's ID (its priority + MAC address). The lower the priority is, the more likely the switch can be elected to be a root switch.

9.2.2 Basic Concept

MST Domain: MST Domain is made up by one or one more Configuration identifiers with the same MST to realize the same MSTI instances.

MST Configuration identifier : It is used to mark an MST configuration content of a bridge to make sure whether the bridges can be in the same domain. The content includes: Configuration Identifier Format Selector , Configuration Name , Revision Level and Configuration Digest.

CIST Root identifier : Bridge ID of the CIST root bridge.

CIST External root port cost : CIST external root path cost is the path cost from the domain the bridge located in to the domain the root bridge located in. All CIST External root port cost of the bridges in a domain is the same. During the calculation, CIST means to calculate the path cost the root port of the domain root bridge locating in LAN.

Regional Root Identifier : The bridge ID of the domain root bridge and the domain root bridge are not the smallest one in all the domain bridges but the lowest path cost from the domain inside to the root path of the CIST root bridge.

Internal Root Port Cost : Internal path cost is the path cost from the internal bridge device to the root path of the root bridge with the domain being considered as a separate local area network.

Master Port : Master port refers to a domain root bride of the root port. The path from the port to the root bridge is the least.

VLAN Mapping Table : VLAN mapping table means that the VLAN is mapped to a specified MSTI, and the VLAN mapping table of all the bridge devices in a domain must be consistent. The default is that all the VLANs are mapped to instance 0.

CST : Common spanning tree is used to connect different domains and non-MSTP

bridge devices to construct a spanning tree.

9.2.3 Port Status and Port Role

There are four various port states and six port roles in RSTP.

Port State: Discarding, Learning, and Forwarding

Port Role: Root port, Backup port, designated port, backup port, Disabled port, and master port

The relationship between port status and port role is as follows :

STP Port State	Administrative port state	RSTP Port State	MSTP Port State	Active Topology (Port Role)
DISABLED	Disabled	Discarding	Discarding	Excluded
BLOCKING	Enabled	Discarding	Discarding	Excluded(Alternate, backup)
LISTENING	Enabled	Discarding	Discarding	Included(Root, Designated, master port)
LEARNING	Enabled	Learning	Learning	Included(Root, Designated, master port)
Forwarding	Enabled	Forwarding	Forwarding	Included(Root, Designated, master port)

9.3 MSTP Module Implementation

9.3.1 MSTP Domain

MSTP protocol provides the concept of domain which is more convenient for users to manage and configure. The switches in the domain are considered as the same set of switches with the same configuration. Placing different switches in a domain needs the same domain name, the same VLAN to MSTI mapping configuration, the same MSTP revision level, and the link connectivity between these devices physically with opening MSTP protocol. Only STP or RSTP protocol switch alone can be as a domain. The system can be configured as a domain name in 32 characters. Configuring the domain characteristics of the configuration switches needs to configure the switch domain name (bridge_region_cmd) and the revision level (bridge_revision_cmd) to ensure that the VLAN instance mapping and the domain is exactly the same.

9.3.2 MSTP Instance

MSTP protocol the system realized can create 15 instances of 1-15 and any VLAN mapping can be mapped in any instance. By default, all the VLANs are mapped to instance 0. (Note: A VLAN can only be mapped to an instance of MSTP or EAPS.) After a VLAN mapped to instance, the system will automatically add all the VLAN ports to the instance.

9.3.3 Protocol Protection Mechanism

- BPDUGUARD

The port configured as edge port cannot receive BPDU message normally, and if it received, it is considered as an unusual of aggressive behavior. Once the BPDUGUARD function starts, the edge port will shut down and wait for the manager's operation (open err disable-timeout function) or restore the up state automatically after receiving the BPDU message.

- BPDUFILTER

The edge port is generally connected to the user terminal port directly, and therefore, the port does not need forwarding the BPDU message. Once configured the BPDUFILTER function, the port will not forward any BPDU message.

- ROOTGUARD

The port is configured as discarding status when the ROOTGUARD function discards the better BPDU message the port received. Enable the forward delay timers. After two delays, it becomes into forwarding status. To ROOTGUARD port, no better BPDU message can exist at the port. Otherwise, it is considered as an attack.

9.4 Configure the Basic Functions of MSTP

The following tasks need completing before configuring the basic functions of mstp: Switches or physical ports should have the MAC address to link the adjacent switches physically.

9.4.1 Open MSTP and Configure the running MSTP of the Switch

Open the MSTP function of the switch

OPERATION	COMMAND	ILLUSTRATION
Enter into ENABLE mode	enable	-
Enter into CONFIG mode	configure terminal	-
Open MSTP protocol	multiple-spanning-tree enable	Required By default , MSTP is open.
Close MSTP protocol	no multiple-spanning-tree enable	-



Illustration: Without MSTP configuration, the port default belongs to instance 0 once opening MSTP.

9.4.2 Configure the Mapping Relationship between Instances and vlan

Configure the mapping relationship between instances and vlan

OPERATION	COMMAND	ILLUSTRATION
Enter into ENABLE mode	enable	-
Enter into CONFIG mode	configure terminal	
Enter into MSTP mode	spanning-tree mst configuration	-
Configure the relationship of the instances mapping the	instance <1-15>vlan<1-4094>	Optional By default, MSTP is permitting and

OPERATION	COMMAND	ILLUSTRATION
vlan		the interface default belongs to instance 0.
Return to CONFIG mode	exit	-



Illustration: The command is to map the VLAN to some non-zero instance. If the instance exists, the VLAN should be mapped to the instance directly. Otherwise, create an instance at first and then map the VLAN to the instance.

9.4.3 Configure the Priority of Instance 0

Configure the priority of instance 0

OPERATION	COMMAND	ILLUSTRATION
Enter into ENABLE mode	enable	-
Enter into CONFIG mode	configure terminal	
Enter into MSTP mode	spanning-tree mst configuration	-
Configure the priority of instance 0	priority <0-61440>	Optional By default, the priority of instance 0 is 32768.
Return to CONFIG mode	exit	-



Illustration: MSTP priority determines that the switch will become into a root switch in the LAN or not. If a switch of good performance is selected as the root switch, the priority of the switch is set to the lowest. Among them, the priority must be an integer multiple of 4096.

9.4.4 Configure the Priority of the Instances non-zero

Configure the priority of the instances non-zero

OPERATION	COMMAND	ILLUSTRATION
Enter into ENABLE mode	enable	-
Enter into CONFIG mode	configure terminal	
Enter into MSTP mode	spanning-tree mst configuration	-
Configure the priority of instance 0	instance <1-15>priority <0-61440>	Optional By default, the priority of instances is 32768.
Return to CONFIG mode	exit	-



Illustration: The MSTP priority determines the switch will become the root switch or not. If a switch of good performance is selected as the root switch, the priority of the switch is set to the lowest. Among them, the priority must be an integer multiple of 4096.

9.4.5 Configure MSTP Domain Name

Configure MSTP domain name

OPERATION	COMMAND	ILLUSTRATION
Enter into ENABLE mode	enable	-
Enter into CONFIG mode	configure terminal	
Enter into MSTP mode	spanning-tree mst configuration	-
Configure the priority of instance 0	region REGION_NAME	Optional By default, the domain name is

OPERATION	COMMAND	ILLUSTRATION
		empty.
Return to CONFIG mode	exit	-



Illustration: If multiple MSTP switches are placed in a domain, the switches need configuring the same domain name. The domain name can be configured to any string of 0-32 characters.

9.4.6 Configure MSTP Revision Level

Configure MSTP revision level

OPERATION	COMMAND	ILLUSTRATION
Enter into ENABLE mode	enable	-
Enter into CONFIG mode	configure terminal	
Enter into MSTP mode	spanning-tree mst configuration	-
Configure the priority of instance 0	revision REVISION_NUM	Optional By default, the revision level is 0.
Return to CONFIG mode	exit	-



Illustration: If multiple MSTP switches are placed in a domain, the switches need configuring the same revision level. The revision level range is 0-255.

9.4.7 Configure MSTP Forwarding Delaying Time

Configure MSTP forwarding delaying time

OPERATION	COMMAND	ILLUSTRATION
Enter into ENABLE mode	enable	-
Enter into CONFIG mode	configure terminal	
Enter into MSTP mode	spanning-tree mst configuration	-
Configure the priority of instance 0	forward-time <4-30>	Optional By default, the time is 15s.
Return to CONFIG mode	exit	-



Illustration: Forward time is a variable used by the switch during the topology changing, and it determines the converging time the network topology needs in STP protocol.

9.4.8 Configure hello time of the MSTP

Configure hello time of the MSTP

OPERATION	COMMAND	ILLUSTRATION
Enter into ENABLE mode	enable	-
Enter into CONFIG mode	configure terminal	
Enter into MSTP mode	spanning-tree mst configuration	-
Configure the priority of instance 0	hello-time <1-10>	Optional By default, the time is 2s.
Return to CONFIG mode	exit	-



Illustration: When the root bridge is elected, the root bridge device will broadcast a BPDU message carrying the MSTP protocol information in a time interval of every hello time, in order to maintain the stability of the network topology.

9.4.9 Configure MSTP the Configuration Information Timeout Time

Configure MSTP the configuration information timeout time

OPERATION	COMMAND	ILLUSTRATION
Enter into ENABLE mode	enable	-
Enter into CONFIG mode	configure terminal	
Enter into MSTP mode	spanning-tree mst configuration	-
Configure the priority of instance 0	max-age <6-40>	Optional By default, the time is 20s.
Return to CONFIG mode	exit	-



Illustration: The root bridge device sends BPDU message periodically once the network topology is stable. Every non-root bridge device can receive the BPDU message through its own root port. If it receiving no BPDU message in max age time, the bridge will consider that the network topology is changed and makes a new convergence of the network topology. This value must be greater than 2*hello time and less than 2*forward time.

9.4.10 Configure the Largest Diameter of the MSTP

Configure the largest diameter of the MSTP

OPERATION	COMMAND	ILLUSTRATION
Enter into ENABLE mode	enable	-
Enter into CONFIG mode	configure terminal	
Enter into MSTP mode	spanning-tree mst configuration	-
Configure the priority of instance 0	max-hops <1-40>	Optional By default, the time is 20s.
Return to CONFIG mode	exit	-



Illustration: When the network topology changes, it takes some time to carry out the convergence. Topology convergence time has a certain relationship to the size of the network. In order to limit the time, the size of the network is generally limited. The parameter limits up the most middle paths from the root bridge devices to a leaf device.

9.4.11 Configure the Port the Priority in Instance 0

Configure the port the priority in instance 0

OPERATION	COMMAND	ILLUSTRATION
Enter into ENABLE mode	enable	-
Enter into CONFIG mode	configure terminal	
Enter into interface mode	interface IFNAME	-

OPERATION	COMMAND	ILLUSTRATION
Configure the priority	priority <0-240>	Optional By default, the priority of the port is 128.



Illustration: When selecting the root port, the lower the port priority value is, the more likely it is to become the root port. The value must be an integer multiple of 16.

9.4.12 Configure the Port the Path Cost in Instance 0

Configure the port the path cost in instance 0

OPERATION	COMMAND	ILLUSTRATION
Enter into ENABLE mode	enable	-
Enter into CONFIG mode	configure terminal	
Enter into interface mode	interface IFNAME	-
Configure path overhead	path-cost <1-200000000>	Optional. The default will calculate it according to the features of the link.



Illustration: during the network topology calculation, MSTP determines the root of each bridge according to the path cost from the bridge devices to root bridge devices.

9.4.13 Configure the Port the Priority in any Instance

Configure the port the priority in any instance

OPERATION	COMMAND	ILLUSTRATION
Enter into ENABLE mode	enable	-
Enter into CONFIG mode	configure terminal	
Enter into interface mode	interface <i>IFNAME</i>	-
Configure the priority	instance <1-15> priority <0-240>	Optional



Illustration: When selecting the root port, the lower the port priority value is, the more likely it is to become the root port. The value must be an integer multiple of 16.

9.4.14 Configure the Port the Path Cost in any Instance

Configure the port the path cost in any instance

OPERATION	COMMAND	ILLUSTRATION
Enter into ENABLE mode	enable	-
Enter into CONFIG mode	configure terminal	
Enter into	interface <i>IFNAME</i>	-

OPERATION	COMMAND	ILLUSTRATION
interface mode		
Configure path cost	instance <1-15> path-cost <1-200000000>	Optional. The default will calculate it according to the features of the link.



Illustration: during the network topology calculation, MSTP determines the root of each bridge according to the path cost from the bridge devices to root bridge devices.

9.4.15 Configure the Port as the Edge Port

Configure the port as the edge port

OPERATION	COMMAND	ILLUSTRATION
Enter into ENABLE mode	enable	-
Enter into CONFIG mode	configure terminal	
Enter into interface mode	interface IFNAME	-
Configure to be edge port	spanning-tree (portfast edgeport)	Optional The default is unedging port.



Illustration: The edge port transforms to the forwarding state directly. Generally, the port which is connecting to the user terminal device directly is set to be the edge port.

9.4.16 Configure the Port as the Automatic Edge Port

Configure the port as the automatic edge port

OPERATION	COMMAND	ILLUSTRATION
Enter into ENABLE mode	enable	-
Enter into CONFIG mode	configure terminal	
Enter into interface mode	interface <i>IFNAME</i>	-
Configured as the automatic edge port	spanning-tree autoedge	Optional The default is not an automatic edge port.



Illustration: Set the function, and the port is up. If the port receives no BPDU message in err disable-timeout interval time, the device port is set to be the edge port and comes into the forwarding state directly.

9.4.17 Display Every Parameters of Instance 0 in the Port

Display every parameters of the instance0 in the port

OPERATION	COMMAND	ILLUSTRATION
Enter into ENABLE mode	enable	-
Display port information	show spanning-tree mst interface IFNAME	Required Display every running parameters of the

OPERATION	COMMAND	ILLUSTRATION
		instance0 in the port.

9.4.18 Display the Detailed Information of MSTP

Display the detailed information of MSTP

OPERATION	COMMAND	ILLUSTRATION
Enter into ENABLE mode	enable	-
Display MSTP information	show spanning-tree mst detail	Required Display every running parameters of MSTP.

9.4.19 Display the Details of the Port in MSTP

Display the detailed information of the port in MSTP

OPERATION	COMMAND	ILLUSTRATION
Enter into ENABLE mode	enable	-
Display port information	show spanning-tree mst detail interface IFNAME	Required Display the detailed information of the port in MSTP.

9.4.20 Display the Parameters of the Port in the Instance of Non-zero

Display the parameters of the port in the instance of non-zero

OPERATION	COMMAND	ILLUSTRATION
Enter into ENABLE mode	enable	-
Display the port information	show spanning-tree mst instance <1-15> interface IFNAME	Required Display the parameters of the port in the instance of non-zero

9.4.21 Display the Relevant Information in MSTP Domain

Display the relevant information in MSTP domain

OPERATION	COMMAND	ILLUSTRATION
Enter into ENABLE mode	enable	-
Display the domain information	show spanning-tree mstconfig	Required Display the domain information of the switch.

9.4.22 Display the Instance Information

Display the instance information

OPERATION	COMMAND	ILLUSTRATION
Enter into ENABLE	enable	-

OPERATION	COMMAND	ILLUSTRATION
mode		
Display the instance information	show spanning-tree mst instance <1-15>	Required Display the instance information

9.4.23 Display the MSTP Protocol Running State

Display the MSTP protocol running state

OPERATION	COMMAND	ILLUSTRATION
Enter into ENABLE mode	enable	-
Display the MSTP state	show spanning-tree mst	Required Display the MSTP protocol running state of the switch.

9.5 Configure MSTP Features

In practical applications, the network topology sometimes requires more precise control to satisfy the needs of the complex network environments. MSTP provides a number of features.

9.5.1 Configure the MSTP bpdu Guard Global Switch

Configure the global switch to the MSTP bpdu guard

OPERATION	COMMAND	ILLUSTRATION
Enter into ENABLE mode	enable	-
Enter into CONFIG mode	configure terminal	
Enter into MSTP mode	spanning-tree mst configuration	-
Configure the switch of the function	spanning-tree portfastbpdu-guard	Required By default, the switch of the function is closed.
Return to CONFIG mode	exit	-



Illustration: in order to reduce the topology convergence time of the MSTP protocol, MSTP protocol sets the device connected with the user terminal device directly as the edge port. Under the normal circumstances, the edge port receives no BPDU message. If the port receives the BPDU message, it is generally considered to be an attack. Therefore, the edge port is set to receive no BPDU message in order to protect the MSTP protocol from the attack like this. If the bpduguard function of the port is open, it will shut down after it receiving the BPDU message and wait for the manager's operation. The command also set the port of the default bpduguard function to be open.

9.5.2 Configure the Port bpdu-guard Features

Configure the port bpdu-guard features

OPERATION	COMMAND	ILLUSTRATION
Enter into ENABLE mode	enable	-
Enter into CONFIG mode	configure terminal	
Enter into interface mode	interface IFNAME	-
Configure bpdu guard features	spanning-tree portfastbpdu-guard (enable disable default)	Required Configure the port bpdu-guard features



Illustration: When the value is set to be default, the bpdu-guard of the port is configured by the system global setting.

9.5.3 Configure the Global Switch of the MSTP bpdu Filter Function

Configure the global switch of the MSTP bpdu filter function

OPERATION	COMMAND	ILLUSTRATION
Enter into ENABLE mode	enable	-
Enter into CONFIG mode	configure terminal	
Enter into MSTP mode	spanning-tree mst configuration	-
Configure the switch of the function	spanning-tree portfastbpdu-filter	Required By default, the switch of the function is closed.
Return to CONFIG mode	exit	-



Illustration: The command will set the port of default bpdufilter to be open at the same time.

9.5.4 Configure the Port bpdu filter Function

Configure the port bpdu filter function

OPERATION	COMMAND	ILLUSTRATION
Enter into ENABLE mode	enable	-
Enter into CONFIG mode	configure terminal	
Enter into interface mode	interface IFNAME	-
Configure the priority	spanning-tree portfastbpdu-filter (enable disable default)	Configure the port bpdu filter function



Illustration: The port configured with the bpdu filter function cannot receive or forward BPDU message. When it is set to be the default value, the port bpdu filter function is set by the system-wide settings.

9.5.5 Configure MSTP with the errdisable-timeout Function

Configure MSTP with the errdisable-timeout function

OPERATION	COMMAND	ILLUSTRATION
Enter into ENABLE mode	enable	-
Enter into CONFIG mode	configure terminal	
Enter into MSTP mode	spanning-tree mst configuration	-
Configure the function	spanning-tree errdisable-timeout enable	Optional By default, the switch of the

OPERATION	COMMAND	ILLUSTRATION
		function is closed.
Return to CONFIG mode	exit	-



Illustration: When the port shuts down because of the bpduguard function, the port will restore to up state automatically with receiving no new BPDU message in the timeout time if the errdisable-timeout function is open.

9.5.6 Configure the MSTP errdisable-timeout Interval

Configure the MSTP errdisable-timeout interval

OPERATION	COMMAND	ILLUSTRATION
Enter into ENABLE mode	enable	-
Enter into CONFIG mode	configure terminal	
Enter into MSTP mode	spanning-tree mst configuration	-
Configure the interval of the function	spanning-tree errdisable-timeout interval <10-1000000>	Optional By default, the interval is 300s.
Return to CONFIG mode	exit	-

9.5.7 Configure the Port Link Type

Configure the port link type

OPERATION	COMMAND	ILLUSTRATION
Enter into ENABLE mode	enable	-
Enter into	configure terminal	

OPERATION	COMMAND	ILLUSTRATION
CONFIG mode		
Enter into interface mode	interface <i>IFNAME</i>	-
Configure link type	spanning-tree link-type shared/ point-to-point	Optional By default, the link type is point-to-point.



Illustration: The switch ports are generally point-to-point connection. If some port is connected to a hub, the port is set to be shared mode.

9.5.8 Configure the Port with root guard Function

Configure the port with the root guard function

OPERATION	COMMAND	ILLUSTRATION
Enter into ENABLE mode	enable	-
Enter into CONFIG mode	configure terminal	
Enter into interface mode	interface <i>IFNAME</i>	-
Configure root guard function	spanning-tree guard root	Optional By default, the function is closed.



Illustration: When the root guard function is open, the port will discard the message once it receives better BPDU message and is set to be discarding status at the same time. Enable the forward delay timer, and it becomes forwarding status after two delays.

9.5.9 Configure the MSTP Version of the Port

Configure the MSTP version of the port

OPERATION	COMMAND	ILLUSTRATION
Enter into ENABLE mode	enable	-
Enter into CONFIG mode	configure terminal	
Enter into interface mode	interface <i>IFNAME</i>	-
Configure the MSTP version of the port	spanning-tree force-version <0-3>	Optional By default, the version is MSTP version.



Illustration: In order to be compatible with RSTP protocol and STP protocol, mstp can configure every port with the adaptive version number of the port, as 0 stands for STP, 2 for RSTP and 3 for MSTP. If there is no set, the port will select a compatible version automatically according to the BPDU message the opposite end forwarded.

9.5.10 Configure the MSTP Cisco Compatibility

Configure the MSTP Cisco compatibility

OPERATION	COMMAND	ILLUSTRATION
Enter into ENABLE mode	enable	-
Enter into CONFIG mode	configure terminal	
Enter into MSTP mode	spanning-tree mst configuration	-
Configure the compatibility	cisco-interoperability enable	Optional

OPERATION	COMMAND	ILLUSTRATION
with Cisco		By default, the function is closed.
Return to CONFIG mode	exit	-



Illustration: The function is open in order to be compatible with the MSTP of Cisco.

10. EAPS

10.1 Brief Introduction

The EAPS protocol is a loop protection protocol. An EAPS loop contains a control VLAN and a set of protected VLANs. The control VLAN is used to interact with protocol message and the protected VLANs for business data communications. EAPS protocol ensures the VLAN no loop by the control VLAN exchanging message. If there is a connection failure in the loop, EAPS restores the data communication by starting an alternative link.

10.2 Restrictions

- 1、 It cannot run with the MSTP simultaneously.
- 2、 The single VLAN runs either EAPS or VLLP protocol.
- 3、 To the control VLAN configured as EAPS protocol, control VLAN just contains two TRUNK member ports: the main port and the standby port. The 3-layer interface cannot be configured.
- 4、 To the protected VLAN configured as EAPS protocol, the protected VLAN just contains two TRUNK member ports: the main port and the standby port. There is no limit for other ports.
- 5、 One port just belongs to one EAPS protocol loop.
- 6、 Without considering the case of LACP at present.

10.3 Command Introduction

The system can be configured with 16 EAPS loops, each loop with only one control VLAN and a set of protected VLAN. The fail-time must be greater than the hello-time.

Configuration process: create a loop - > configure the necessary parameters of the loop

- > start a loop

Deletion process: close a loop - > delete a loop. The active loop cannot be deleted.

For an active loop, the control-vlan, primary-port, secondary-port and mode cannot be revised. The others causing the fail-time, hello-time and protected-vlan etc. are permitted to be modified.

Restrictions:

- 1、 It cannot run with the MSTP simultaneously.
- 2、 To the control VLAN configured as EAPS protocol, control VLAN just contains two TRUNK member ports: the main port and the standby port. The 3-layer interface cannot be configured.
- 3、 To the protected VLAN configured as EAPS protocol, the protected VLAN just contains two TRUNK member ports: the main port and the standby port. There is no limit for other ports.
- 4、 One port just belongs to one EAPS protocol loop.
- 5、 Without considering the case of LACP at present.

1、 eaps create <ring-id>

Create a ring

2、 eaps control-vlan <ring-id> <vlan-id>

Configure a control VLAN of a ring

3、 eaps mode <ring-id> <master | transit>

Configure node mode of a ring

4、 eaps primary-port <ring-id> <interface-name>

Configure the main port of the ring node

5、 eaps secondary-port <ring-id> <interface-name>

Configure the standby port of the ring node

6、 eaps protected-vlan <ring-id> <vlan-id>

Configure the included VLAN of the ring node

7、 eaps extrem-interoperability <ring-id> <enable | disable>

Configure a ring node with the eaps which is whether compatible with extreme or not

8、 eaps enable <ring-id>

Start EAPS protocol at a ring node

9、 eaps disable <ring-id>

Close EAPS protocol at a ring node

10、 eaps remove <ring-id>

Delete a ring

11、 eaps hello-time <ring-id> <1-65535>

Configure the hello-time of the ring node in seconds

12、 eaps fail-time <ring-id> <1-65535>

Configure the fail-time of the ring node in seconds

11. ACL Configuration

ACL Overview

With the expansion of the network size and the increasing of the traffic, the control of network security and the bandwidth allocation become into the main content of the network management. That the unauthorized users' access to the network can be prevented effectively by the packet filtering. It controls the traffic to save the network resources. ACL (Access Control List) is to realize the packet filtering through configuring the packet matching rules and processing operations.

The port of the switch makes an analysis of the message according to the applied ACL rules on the current port after the message receiving. Once the message is recognized as the identified message, it will be allowing or forbidding going through the corresponding packets based on the pre-set strategy.

The ACL consists of a series of tables of composition which is named as the access control list entries(Access Control Entry : ACE). Each access control list entries have been affirmed to meet the matching conditions of the entry and behavior.

The ACL makes the packet classification depending on a set of matching conditions which can be the packet's source address, destination address, and the port number and so on. The ACL can be divided into the following types according to the application purpose:

- The basic ACL: The rules should be made according to the packet's IP address.
- The advanced ACL: The rules should be made according to the packet's source IP, destination IP address, and the protocol types the IP carrying, the information on 3rd-layer and 4th-layer of the protocol features.

Two-layer ACL: The rules are made according to the two-layer information such as the packet's source MAC address, destination MAC address, 802.1p priority and two-layer protocol types and so on.

11.1 The Role of ACL

ACL can limit network traffic and improve network performance. For example, ACL can specify the priority of the packets according to the protocol of the packet.

ACL provides methods to control the communication traffic. For example, ACL limits or simplifies the routing to update the message length in order to limit the communication traffic through a segment of the router.

ACL is the basic means to provide network security access. For example, ACL allowsthe host A to access the Human Resource Network not the host B.

ACL decides the communication traffic of which type to be forwarded or blocked at the port of the router. For example, the user can allow the E-mail communication traffic to be routed and reject all the Telnet communication traffic.

11.2 The Classification of ACL

There are two main types of ACL: Standard ACL and Extended ACL.

Standard ACLs use a number of 1 to 99 and from 99 to 1999 as a table number, and Extended ACLs use a number of 100 to 199 and from 2000 to 2699 as the table number.

Standard ACL can block all the communication traffic from a network, allow the traffic from a particular network, and refuse all the communication traffic from a particular protocol stack (IP).

Extended ACL provides a broader range of control than a standard ACL. For example, if the network administrator wants to allow the communication traffic from the external Web to go through and refuse that of the external FTP and FTP, extended ACL can be used to achieve as the standard ACL cannot control precisely like it.

11.3 ACL Sorted Automatically

- 1) First, compare the scope of the protocols. The rule with the little number takes the

precedence;

- 2) If the protocols are the same, the source IP address ranges can be compared with. The rule with the little source IP address range (the number of "0" in anti-mask is large) takes the precedence;
- 3) If the scope of the protocols and source IP address both are the same, the rule with the little destination IP address range (the number of "0" in anti-mask is large) takes the precedence;
- 4) If the scope of the protocols, the source IP address range and destination IP address range are all the same, the 4th-layer port name (TCP/UDP) range should be compared with. The rule with the little the 4th-layer port name range takes the precedence. – current priority: eq (equal), range(range), lt(less than), and gt(greater than);
- 5) If the scope of the protocols, the source IP address range, destination IP address range and the port number of 4th-layer are all the same, the number of the parameters should be compared with. The rule with the large number takes the precedence.

11.4 ACL Matching Order

An ACL can contain multiple rules and each rule specifies a different range of the packet. Thus, there will be matching order problems in matching messages.

ACL supports automatic sorting: Rules are matched according to "depth first" order.

1、The judgment principles of the basic "depth first" order

First, compare the scope of the protocols. The rule with the little number takes the precedence ;

2、The judgment principles of the advanced "depth first" order

(1) First, compare the scope of the protocols. The rule with the little number takes the precedence;

(2) If the protocols are the same, the source IP address ranges can be compared with. The rule with the little source IP address range (the number of "0" in anti-mask is large)

takes the precedence;

(3) If the scope of the protocols and source IP address both are the same, the rule with the little destination IP address range (the number of "0" in anti-mask is large) takes the precedence;

(4) If the scope of the protocols, the source IP address range and destination IP address range are all the same, the 4th-layer port name (TCP/UDP) range should be compared with. The rule with the little the 4th-layer port name range takes the precedence.
– Current priority: eq (equal), range (range), lt (less than), and gt (greater than);

(5) If the scope of the protocols, the source IP address range, destination IP address range and the port number of 4th-layer are all the same, the number of the parameters should be compared with. The rule with the large number takes the precedence.

11.5 The Appliance of ACL in Switches

1、 The case of ACL is issued to the hardware directly

ACL can be directly issued to the switch hardware for the packet filtering and traffic classification in the data forwarding process. At this time, the matching order of multiple principles in one ACL is decided by the switch hardware. For the Ethernet switches of the FS series, the matching order is that match first for the first issued rules.

The conditions ACL sent to the hardware directly includes: filter or forward the data through ACL.

2、 The condition the ACL referred by the upper-layer

ACL can be used for the filtering and classification of the message the software dealt with, and the upper protocols only match the extended ACL source and destination addresses.

The conditions ACL referred by the upper software includes: the RIP/OSPF redistribution reference to the ACL, and the reference to an ACL routing policy.

11.6 Input/Output the Matching Fields of ACL and ACE

The input ACL checks whether the message received at the device port to match with the ACE string of the input ACL at the port or not; the output ACL checks whether the message received at the device port to match with the ACE string of the output ACL at the port or not.

ACE of ACL is to identify the Ethernet message according to some fields of the Ethernet message which contain:

Layer 2 Fields:

The source MAC address of 48

The destination MAC address of 48

The two-story type field of 16

Layer 3 Fields:

Source IP address field

Destination IP address field

The protocol type field

Layer 4 Fields:

Affirm one or a range of TCP source port, destination or the all

Affirm one or a range of UDP source port, destination or the all

Affirm a flag marking field of TCP

11.7 Configure the ACL Announcements

- 1) IP ACL only supports digital ACLs:

IP ACL number range

PROTOCOL	NUMBER RANGE
STANDARD IP	1-99,1300-1999

EXTENDED IP	100-199,2000-2699
-------------	-------------------

- 2) MAC ACL only supports character ACLs;
- 3) Supporting the automatic sorting of the “depth first”, and the sorting process is the inserting sort;
- 4) When a string of ACL is created, the deny ip any (any|) ACE is automatically added up. And the ACE can be displayed by the show command;
- 5) According to the sorting order, the deny ip any (any|) should be located on the last one in the ACL; the ACE cannot be deleted by no command but can be replaced by permit ip any (any|);
- 6) Supporting dynamically to add/remove an ACL or one ACE among them;
- 7) A string of IP supports 256 ACEs(including deny|permit ip any (any|)) at most; the whole device supports 1792 ACEs;
- 8) A string of MAC ACL supports 32 ACEs at most; the whole device supports 128 MAC ACEs;
- 9) ACL can only be used in the direction at the two-layer interface;
- 10) the ACL supporting 16 groups of ports;
- 11) IP ACL is in the form of the anti-mask; MAC ACL is in the form of the mask.

11.8 The Command IP Access the Control List

The configuration of IP accessing the control list includes the following two steps:

- ◆ the definition of accessing the control list
- ◆ apply the accessing the control list to interfaces

IP ACL configuration commands:

Basic ACL:

access-list (<1-99>|<1300-1999>) (**deny|permit**) ((*src-addr* *src-wildcard*)|(**any**)|(**host** *src-addr*))

Extended ACL:

access-list (<100-199>|<2000-2699>) (**deny|permit**) (*ip-protocol*) ((*src-addr*

```
src-wildcard)|(any)|(host src-addr)) ((src-addr src-wildcard)|(any)|(host src-addr))
```

Among them, *ip-protocol* is

```
(<0-255>|ahp|eigrp|esp|gre|ip|ipinip|ospf|pcp|pim|icmp)
```

4-Layer ACL:

```
access-list (<100-199>|<2000-2699>) (deny|permit) (tcp)
```

```
((src-addr src-wildcard)|(any)|(host src-addr))
```

```
((eq|lt|gt) (ftp|ftp-data|pop3|smtp|telnet|www|<1-65535>)))
```

```
((src-addr src-wildcard)|(any)|(host src-addr))
```

```
((eq|lt|gt) (ftp|ftp-data|pop3|smtp|telnet|www|<1-65535>)))
```

```
(fin|syn|rst|psh|ack|urg|)
```

```
access-list (<100-199>|<2000-2699>) (deny|permit) (tcp)
```

```
((src-addr src-wildcard)|(any)|(host src-addr))
```

```
(range) (ftp|ftp-data|pop3|smtp|telnet|www|<1-65535>)
```

```
(ftp|ftp-data|pop3|smtp|telnet|www|<1-65535>)
```

```
((src-addr src-wildcard)|(any)|(host src-addr))
```

```
(range) (ftp|ftp-data|pop3|smtp|telnet|www|<1-65535>)
```

```
(ftp|ftp-data|pop3|smtp|telnet|www|<1-65535>)
```

```
(fin|syn|rst|psh|ack|urg|)
```

Among them, **(eq|lt|gt)** and **(range)** can be used in groups.

UDP :

It corresponds with TCP configuration basically, and the difference is what the upper protocol the port carrying with.

```
(<1-65535>|rip|snmp|snmp-trap|tftp|))
```

11.9 Configure IP Access Control Lists

OPERATION	COMMAND	ILLUSTRATION
Enter into ENABLE mode	enable	-

OPERATION	COMMAND	ILLUSTRATION
Enter into CONFIG mode	configure terminal	-
Configure ACL rules	access-list id	Define ACL

11.10 Display IP Access Control Lists

OPERATION	COMMAND	ILLUSTRATION
Enter into ENABLE mode	enable	-
View ACL rules	show access-list [id]	View one or all the ACL rules

11.11 Configure the MAC Extended Access Control List

2-Layer ACL makes the rules according to the source MAC address, destination MAC address of the 2-Layer information and so on is to deal with the data correspondingly.

2-Layer takes in the naming forms.

OPERATION	COMMAND	ILLUSTRATION
Enter into CONFIG mode	configure terminal	-
Enter into MAC ACL mode	mac access-list extended name	
Configure MAC ACL rules	(deny permit) ((src-mac-addr src-mac-wildcard) (any) (host src-mac-addr)) ((src-mac-addr src-mac-wildcard) (any) (host src-mac-addr)) (ethernet-type)	Add entries for ACL

OPERATION	COMMAND	ILLUSTRATION
Exit MAC ACL mode and return to config mode	exit	

Display MAC ACL configuration

OPERATION	COMMAND	ILLUSTRATION
Enter into ENABLE mode	enable	-
	show mac access-list extended (name)	View one or all the ACL rules

12. ARP Configuration

12.1 Overview

In the LAN, when the host and other devices want to send data to another host or device, they must know the IP address of the opposite. However, only IP address is not enough as IP data message must be sent in encapsulated frame through the physical network which is a must for the sending station. Therefore, the mapping from an IP address to the physical address is necessary. ARP is the protocol to realize the function.

COMMAND	DESCRIPTION
arp-ageing-timeout	Configure the ARP timeout
arp A.B.C.D MAC	Configure the static ARP entry
no arp A.B.C.D	Delete the static ARP entry
clear arp-cache	Clear the dynamic ARP table entries

12.2 Configure the ARP Timeout

STEP	COMMAND	DESCRIPTION
1.	switch# configure terminal	Enter into terminal mode
2.	switch(config)# interface vlan1.10	Enter into interface mode
3.	switch(config-vlan1.10)# arp-ageing-timeout ? <60-1000> ARP Ageing timeout in sec e.g., switch(config-vlan1.10)#arp-ageing-timeout 100	Configure the ARP timeout in a unit of a second
4.	end	Exit
5.	switch# show interface vlan1.10 Interface vlan1.10 Hardware is VLAN, address is 00fd.6c1c.0002 (bia 00fd.6c1c.0002)	Display the interface information and view the ARP timeout

index 3 metric 1 mtu 0 duplex-half arp ageing timeout 100 <UP,BROADCAST,MULTICAST> VRF Binding: Not bound input packets 00, bytes 00, dropped 00, multicast packets 00 output packets 00, bytes 00, multicast packets 00 broadcast packets 00	
--	--

12.3 Configure the Static ARP

STEP	COMMAND	DESCRIPTION
1.	switch# configure terminal	Enter into terminal mode
2.	switch(config)# arp ? A.B.C.D IP address of the ARP entry switch(config)#arp 192.168.10.1 ? MAC Mac (hardware) address of the ARP entry in HHHH.HHHH.HHHH format e.g., switch(config)#arp 192.168.10.1 1122.3344.5566	Configure the static ARP
3.	end	Exit
4.	switch# show ip arp IP Address MAC Address Interface Type 192.168.5.2 d842.ac16.0767 vlan1.1 dynamic 192.168.10.1 1122.3344.5566 vlan1.10 static	Display the ARP information. An entry of 192.168.10.1 recorded is added up in the displaying ARP information, and it is static.

12.4 Delete the Static ARP

STEP	COMMAND	DESCRIPTION
1.	switch#configure terminal	Enter into terminal mode
2.	switch(config)#no arp ? A.B.C.D IP address of the ARP entry e.g., switch(config)#no arp 192.168.10.1	Delete the static ARP table entry
3.	end	Exit
4.	switch#show ip arp IP Address MAC Address Interface Type 192.168.5.2 d842.ac16.0767 vlan1.1 dynamic	Display ARP information. An ARP record of 192.168.10.1 has been deleted.

12.5 Clear the Dynamic ARP

STEP	COMMAND	DESCRIPTION
1.	switch#clear arp-cache	Enter into terminal mode
2.	switch#show ip arp IP Address MAC Address Interface Type	Display the ARP information, and all the dynamic ARP have been cleared,

13. Static Route

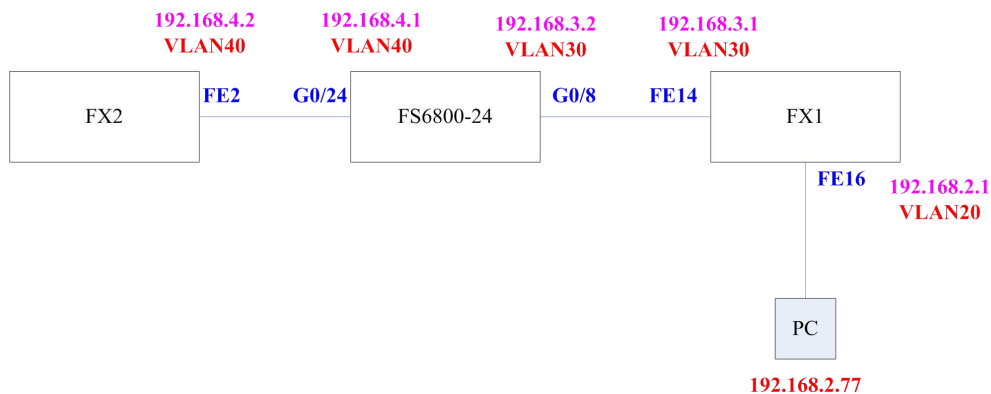
13.1 Overview

Static routing is configured by the administrator manually; when the static routing is configured, the data message going to the specified destination does the forwarding according to the administrator's specified path

In the network with a relative simple structure, all we need to do is to configure the static routing to realize the network connectivity. Properly configuration and using of the static routing can develop the performance of the network, and it guarantees the bandwidth for the important network applications.

The disadvantages of the static routing: It cannot adapt to the changes of the network topology automatically. When running into the network bug and the topology change, the routing may be unreachable which leads to the network outage. At this time, the configuration of the static routing must be modified by the administrator manually.

13.2 Networking Scene



13.3 Configuration Instances

COMMAND LINE	DESCRIPTION
ip route	Add routing
no ip route	Delete routing

13.3.1 Add a Route

As the above networking shown, a static route is added up to a network segment of 192.168.4.0 manually.

STEP	COMMAND	DESCRIPTION
1.	switch#configure terminal	Enter into terminal mode
2.	switch(config)# ip route ? A.B.C.D IP destination prefix A.B.C.D/M IP destination prefix (e.g. 10.0.0.0/8)	Specify the destination segment of 192.168.4.0
3.	switch(config)# ip route 192.168.4.0/24 ? A.B.C.D IP gateway address e.g., switch(config)#ip route 192.168.4.0/24 192.168.3.2 or switch(config)#ip route 192.168.4.0 255.255.255.0 192.168.3.2 Add the default routing: switch(config)#ip route 0.0.0.0 0.0.0.0 192.168.3.2	Specify the next hop.
4.	end	Exit
5.	switch# show ip route Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP O - OSPF, IA - OSPF inter area N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area * - candidate default C 127.0.0.0/8 is directly connected, lo0 C 192.168.2.0/24 is directly connected, vlan1.20 C 192.168.3.0/24 is directly connected, vlan1.30 S 192.168.4.0/24 [1/0] via 192.168.3.2, vlan1.30	Display the route information and the route is added up successfully. Attention: if the address of the configuration static route is unreachable, it cannot be shown in the route table.

13.3.2 Delete a Route

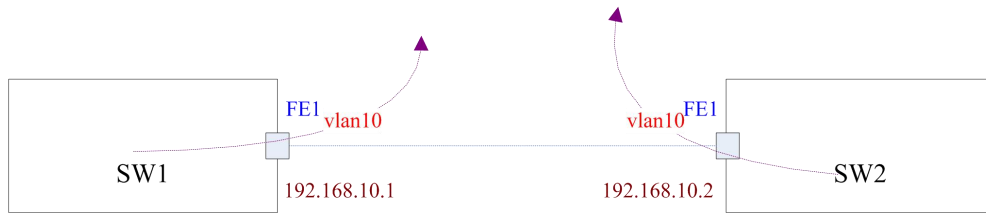
STEP	COMMAND	DESCRIPTION
1	switch#configure terminal	Enter into terminal mode
2	switch(config)#no ip route ? A.B.C.D IP destination prefix A.B.C.D/M IP destination prefix (e.g. 10.0.0.0/8) e.g., switch(config)#no ip route 192.168.4.0/24	Specify the destination network segment of 192.168.4.0
3	end	Exit
4	switch#show ip route Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP O - OSPF, IA - OSPF inter area N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area * - candidate default C 127.0.0.0/8 is directly connected, lo0 C 192.168.2.0/24 is directly connected, vlan1.20 C 192.168.3.0/24 is directly connected, vlan1.30	Display the route information, and the route is deleted.

13.4 3-Layer Sub-interface Configuration

13.4.1 Overview

3-Layer sub-interface is a virtual interface, the biggest feature of which is to configure the 3-storey property such as IP address. In this way, the interface can be accessed directly by the user through the IP address.

13.4.2 Networking Scene



13.4.3 VLAN Sub-interface Configuration

Establish VLAN sub-interface

OPERATION	COMMAND	ILLUSTRATION
Enter into ENABLE mode	enable	-
Enter into CONFIG mode	configure terminal	-
Create vlan sub-interface	ip interface vlan VLAN_ID	- VLAN ID is the vid which has been existed

Delete a VLAN sub-interface

OPERATION	COMMAND	ILLUSTRATION
Enter into ENABLE mode	enable	-
Enter into CONFIG mode	configure terminal	-
Delete a vlan sub-interface	no ip interface vlan VLAN_ID	- VLAN ID is the vid which has been existed

Display interface information

OPERATION	COMMAND	ILLUSTRATION
Enter into ENABLE mode	enable	-
Display all the interface	show ip interface brief	



OPERATION	COMMAND	ILLUSTRATION
information		
Display the information on the specified interface	show ip interface VLAN_ID brief	-eg : view the vlan10 interface information show ip interface vlan1.10 brief
Display the detailed information of the specified interface	show interface vlan VLAN_ID	-

Configure IP address

OPERATION	COMMAND	ILLUSTRATION
Enter into ENABLE mode	enable	-
Enter into CONFIG mode	configure terminal	-
Enter into vlan sub-interface	interface vlan VLAN_ID	-eg. Enter into vlan10sub-interface mode : Interface vlan1.10
Configure the vlan sub-interface with IP address	ip address A.B.C.D/M (secondary)	-

Configure MAC address

OPERATION	COMMAND	ILLUSTRATION
Enter into ENABLE mode	enable	-
Enter into CONFIG mode	configure terminal	-
Enter into vlan sub-interface	interface vlan VLAN_ID	-eg. Enter into vlan10sub-interface mode : Interface vlan1.10

OPERATION	COMMAND	ILLUSTRATION
Configure the vlan sub-interface with MAC address	mac -address HHHH.HHHH.HHHH	-eg. Configure vlan10 sub-interface with mac (config-vlan1.10)#mac-address aabb.ccde.eeff

14. QoS Configuration

14.1 Overview

QOS (Quality of Service) is used to assess the ability of the service side to meet the customers' needs. On the Internet, in order to improve the quality of the network, QOS mechanisms are introduced to assess the ability of the network to delivery and grouping. QOS, we usually refer to the assessment of the support service for the delay, jitter, and packet loss and other core needs in the process of the packet delivery.

14.2 QoS Processes

14.2.1 Classifying

Classifying is the classification process. The process is based on the trust policy or the content of every message to make sure that the messages should be classified into data flows depending on the CoS value. Classification occurred in the port receiving input message, and when some port associates with a representation of QoS policies' Policy-map, the classification takes effect on that port. Apart from this, it is effective for the entire input message from the port.

14.2.2 Policing

Policing is used to constrain the bandwidth occupied by the classification of data streams after the completion of the data stream classification. Policing actions check every message which is classified into the data streams. If the message is beyond the limit bandwidth allowed but the data flow, it will be dealt with in special treatment such as being discarded, or being given an additional DSCP value.

During the QoS handling processes, policing action is optional. Without Policing action, the DSCP value of the message classified into the data flow will not make any change, and the message will not be discarded before sending the Marking action.

14.2.3 Marking

After Classifying and Policing action processing, Marking is used to ensure the corresponding DSCP value with the classified message to deliver to the next hop device on the network. The QoS information is written in the message with the Marking action and changed by the usage of QoS ACLs. Of course, the QoS information in the message could be kept by the Trust method.

14.2.4 Queueing

Queueing is responsible for sending the message of the data stream into an output queue of the port. If the sending ports are different, the message in the output queue will have different transmission service strategies in different classes and qualities.

Each port has 4 output queues. The COS value is transformed into the queueing number through the Cos-to-QueueMap configured on the device, so that we can determine the queue number the message is sent.

14.2.5 Scheduling

Scheduling is the dispatch, the last link in the QoS process. When the message is sent to the different output queue of the port, the device will adapt WRR or any other algorithms to send the message of the four queues.

14.3 Configure the QoS

14.3.1 Default QoS Settings

During the QoS configuration, the user needs to acknowledge the following information which is as follows:

An interface is associated with a Policy-map at most.

One Policy-map can have one more Class-maps.

One Class-map is associated with one ACL at most, and all the ACEs of the ACL have the same filtering domain templates.

By default, QoS is closed that means the device for all the message is the same. The following the QOS default configuration:

The interface default trust cos

the default CoS value	0
queuing number	4
Queue rotation algorithm	SRR

The default mapping table of the value to the queue

CoS value	0	1	2	3	4	5	6	7
queue	1	1	2	2	3	3	4	4

14.3.2 Enable the QoS Configuration

OPERATION	COMMAND	ILLUSTRATION
Enter into ENABLE mode	enable	-
Enter into CONFIG mode	configure terminal	-

OPERATION	COMMAND	ILLUSTRATION
configuration is enabled globally	mls qos enable	The qos is enabled globally, and the default is to disable. All the QoS configuration commands need global QoS enablement.

14.3.3 Configure the Interface with the QoS Trust Model

By default, the QoS trust model of the interface is the trust CoS.

OPERATION	COMMAND	ILLUSTRATION
Enter into ENABLE mode	enable	-
Enter into CONFIG mode	configure terminal	-
Enter into interface mode	interface <i>interface-id</i>	
Configure the QOS trust mode	mls qos cos trust dscp	Configure the trust mode of the interface as the trust DSCP
the default QOS trust mode	no mls qos cos trust dscp	Restore the interface to the trust CoS

14.3.4 Configure the Interface with the Default CoS Value

OPERATION	COMMAND	ILLUSTRATION
Enter into ENABLE mode	enable	-
Enter into CONFIG mode	configure terminal	-
Enter into the interface mode	interface <i>interface-id</i>	

OPERATION	COMMAND	ILLUSTRATION
Configure the default CoS value	mls qos cos default-cos	Configure the interface with the default CoS value, and the default-cos is set as the default CoS value ranging from 0 to 7.
Default CoS value	no mls qos cos	Default CoS value.

14.3.5 Configure the Dscp-CoS Map

DSCP-to-CoS is used for the DSCP values of the message mapped to the CoS values in order to select the output queue for messages.

OPERATION	COMMAND	ILLUSTRATION
Enter into ENABLE mode	enable	-
Enter into CONFIG mode	configure terminal	-
Configure the dscp-cos mapping	mls qos map dscp-cos NAME dscp-list to cos	NAME : the name of dscp-cos dscp-list : The list is to set the DSCP values with spaces between the DSCP values to separate. The range is <0~63>. The range of the CoS value corresponding with DSCP values is 0 ~ 7.
Default dscp-cos mapping	no mls qos map dscp-cos NAME	Cancel the configuration
The dscp-cos mapping is used on the port	interface interface-id mls qos dscp-cos NAME	Enter into the interface mode ; NAME is the name of the configured dscp-cos
The dscp-cos mapping is cancelled on the port	interface interface-id no mls qos dscp-cos	Enter into the interface mode ; Cancel the configured dscp-cos mapping in the port



Illustration:

One interface can only be configured with one dscp-cos mapping.

Dscp-cos mapping cannot be applied to the interface with policy-map.

If the dscp-cos mapping needs a configuration, only configure the interface trust mode as the trust dscp does it take effect.

14.3.6 Configure Class-map

OPERATION	COMMAND	ILLUSTRATION
Enter into ENABLE mode	enable	-
Enter into CONFIG mode	configure terminal	-
Configure the class-map and enter into it	[no]class-map <i>class-map-name</i>	Create and enter into class map configuration mode. Class-map-name is the name of class map to be created. No option is to delete an existed class map.
Configure the match options	[no]match {access-group <i>access-name</i> ip-dscp <i>dscp-list</i> ip-precedence <i>pre-list</i> layer4 [source-port destination-port] <i>port</i> vlan <i>vid</i> vlan-range <i>start-vid to end-vid</i> }	<i>access-name</i> : the name of ip acl or mac acl <i>dscp-list</i> : the list of the dscp values <i>pre-list</i> : the list of the ip priority <i>port</i> : the port number of the tcp udp <i>vid</i> : vlan id no option: delete the matching one



Illustration: Match option except for the vlan has the exclusive with other items, and vlan must be used in conjunction with other options.

14.3.7 Configure Policy-map

OPERATION	COMMAND	ILLUSTRATION
Enter into ENABLE mode	enable	-

Enter into CONFIG mode	configure terminal	-
Configure the policy-map and enter into it	[no]policy-map <i>policy-map-name</i>	Create and enter into the policy map configuration mode , policy-map-name is the name of the policy map to be created. No option is to delete an existed policy map
Enter into class mode	[no] class <i>class-map-name</i>	Create and enter into the data classification configuration mode , class-map-name is the name of the created class map No option is to delete the data classification
Configure re-marking option	[no] set {cos <i>new-cos</i> ip-dscp <i>new-dscp</i> ip-precedence <i>new-pre</i> }	Reconfigure the cos, dscp and tos value of the message
Configure bandwidth limiting	police <i>rate-kbps burst-kbyte</i> exceed-action drop	Limit the bandwidth of the data stream and discarding of the bandwidth section. The limit of the rate-bps is the amount of (kbps) per second , and the burst traffic limit of the burst-byte is (Kbyte).

14.3.8 Configure the Interface to Apply with Policy-map

OPERATION	COMMAND	ILLUSTRATION
Enter into ENABLE mode	enable	-

Enter into CONFIG mode	configure terminal	-
Enter into interface mode	interface <i>interface-id</i>	enter into the interface configuration mode
Enter into class mode	[no] class <i>class-map-name</i>	Create and enter into the data classification configuration mode , class-map-name is the name of the created class map No option is to delete the data classification
Configure policy-map	[no] service-policy input <i>policy-map-name</i>	The created Policy Map is applied to the input direction on the port; policy-map-name is the name of the created Policy map.

14.3.9 Configure CoS-Map

Cos-Map is configured to select which the output queue the message is output in.

Cos-Map's default settings are to see the default QOS configuration.

OPERATION	COMMAND	ILLUSTRATION
Enter into ENABLE mode	enable	-
Enter into CONFIG mode	configure terminal	-
Configure the mapping the CoS values to the queue	mls qos cos-map <i>cos0-map-queueid</i> <i>cos1-map-queueid</i> <i>cos2-map-queueid</i> <i>cos3-map-queueid</i> <i>cos4-map-queueid</i> <i>cos5-map-queueid</i>	Configure the mapping the CoS values to the queue, and the range is 0 ~ 3. Parameters is the queue id of the cos 0-7 mapped in order.

	<i>cos6-map-queueid</i> <i>cos7-map-queueid</i>	
The mapping the default CoS values to the queue	no mls qos cos-map	The mapping the default CoS values to the queue

14.3.10 Configure the Output Queue Scheduling Algorithm

The output queue scheduling algorithm of the port: WRR, SP and SRR. By default, the output queue algorithm is SRR (simple polling).

OPERATION	COMMAND	ILLUSTRATION
Enter into ENABLE mode	enable	-
Enter into CONFIG mode	configure terminal	-
Configure the queue scheduling	mls qos scheduler {sp wrr queue0-weight queue1-weight queue2-weight queue2-weight}	Configure the queue scheduling ranging from 1 to 10. Parameters are queue0-3 of the queue weight.
The default queue scheduling	no mls qos scheduler	The queue scheduling is srr.

14.4 Show the Configuration

OPERATION	COMMAND	ILLUSTRATION
Enter into ENABLE mode	enable	-
Show the mapping the CoS values to queue	show mls qos cos-map	Show the mapping the CoS values to queue

Show the queue scheduling algorithm	show mls qos scheduler	Show the queue scheduling
Show the dscp-cos map	show mls qos maps dscp-cos [NAME]	Show single or all the dscp-cos maps
Show the class-map	show class-map [NAME]	Show single or all the class-maps
Show the policy-map	show policy-map [NAME]	Show single or all the policy-maps

Syslog Messages

OPERATION	COMMAND	ILLUSTRATION
Increase the log grade field in the log information	logging record-priority	Configuration within the configure mode
Configure to show the grade of the log	logging trap	There are seven levels for setting: emergencies, alerts, critical, errors, warnings, notifications, informational and debugging
Add a log server IP	logging host A.B.C.D	The server IP will be saved into syslogip.txt files
Open the log sending	logging syslog	Set the level, and at the same time, the log will be sent to the log server.
Open the log serial display	logging console	Set the level at the same time
Open the terminal log monitoring	logging monitor	Set the level at the same time (such as the telnet terminal)
Open the buffer log monitoring	logging buffer	Set the level at the same time (log information will be saved to a memory buffer)
	logging buffer <4096->	The largest memory buffer used for accessing the logs
Open the log information statics	logging count	
Close the log information statics	no logging count	
Cancel the level field in the log information	no logging record-priority	

Cancel all the terminal log level configuration	no logging trap	Restore the default
Cancel the log server sending	no logging syslog	
Delete the specified log server IP	no logging syslog host A.B.C.D	
Delete all the log server IP	no logging syslog host all	