Navijin

SNMP Management Switches Operation Manual

Manual Version: 2023-08-23-1.08

Directory

1 Product Overview 4
1.1 Overview 4
1.2 Network Design 4
1.3 MAN Access Solution 4
1.4 Education Network Solution 4
1.5 Multi-Service Carrier VLAN Solution 4
2 Using the Command-Line Interface 5
2.1 Command Modes 5
2.2 Getting Help 5
2.3 Specifying Ports in Interface Configuration Mode 5
2.4 Abbreviating Commands 6
2.5 Using no Forms of Commands 6
2.6 Conventions 6
2.7 Accessing the CLI from a Browser 6
3 Logging Swith 7
3.1 Logging into an Ethernet Switch 7
3.2 Logging in through the Console Port 7
4 System operation command 9
4.1 Command to configure multiple ports 9
4.2 Configure permission level 10
4.3 Save parameters 10
4.4 Switch restart 11
4.5 Restore default parameters 11
4.6 View system information 12
4.7 View the cpu usage of the switch 12
4.8 View memory usage 12
4.9 View all configuration information of the switch 13
5 Configuring IEEE802.1Q VLANs 13
5.1 Introduction to VLAN 13
5.2 Advantages of VLANs 14
5.2.1 Configuring an Access mode VLAN 14
5.2.2 Configuring a Hybrid mode VLAN 15
5.2.3 Configuring a Trunk mode VLAN 16
6 IP Addressing Overview 18
6.1 Configuring IP Addresses 19
6.2 Displaying IP Addressing Configuration 21
7 MAC Address Table Management 22
7.1 MAC address Overview 22
7.2 MAC Address Table Management 23
8 Port Basic Configuration 25
8.1 Ethernet Port Configuration 25

8.2 Adding a Description for an Interface 27
8.3 Configuring Storm Control 27
8.4 Configuring Port Rate Limiting 29
8.5 Testing the Cable on an Ethernet Port 30
9 PoE 30
9.1 PoE Overview 30
9.1.1 Introduction to PoE 30
9.1.2 Protocol Specification 31
9.1.3 PoE watchdog 31
9.2 PoE Configuration Task List 31
10 Configuring EtherChannels 32
10.1 Understanding EtherChannels 32
10.2 Understanding Load Balancing and Forwarding Methods..... 33
10.2.1 Configuring Layer 2 EtherChannels 34
10.2.2 Configuring the LACP 35
11 Clock Configuration 36
11.1 Introduction to NTP 36
11.2 Managing the System Time and Date 37
11.3 Configuring NTP 37
11.4 Configuration daylight-saving time 38
11.5 Timezone configuration for system time 38
11.6 Manual Configuring Time and Date Manually 39
12 Configuring mirror 39
12.1 Understanding mirror 39
12.2 Configuration mirror 40
13 STP Configuration 41
13.1 STP Overview 41
13.2 MSTP Overview 44
13.2.1 Specifying the MST Region Configuration and Enabling MSTP 49
13.2.2 Configuring the Port Priority..... 49
13.2.3 Configuring the Path Cost..... 50
13.2.4 Configuring the Switch Priority..... 50
13.2.5 Configuring the Hello Time 51
13.2.6 Configuring the Forwarding-Delay Time 51
13.2.7 Configuring the Maximum-Aging Time 52
13.2.8 Configuring the Maximum-Hop Count 52
14 ERPS(G.8032)..... 52
14.1 Introduction to ERPS..... 53
14.2 Principles 54
14.2.1 Basic ERPS Concepts 54
14.3 ERPS Configuration example 57
14.3.1 Configuring an ERPS single-ring instance 57
14.3.2 Configuring the Port Role 59

1 Product Overview

1.1 Overview

The Switch Ethernet Switches are high-performance, high-density, easy-to-install, NMS-manageable intelligent Ethernet switches which support wire-speed Layer 2 switching.

1.2 Network Design

The Switch can be flexibly deployed in networks. They can be used in enterprise networks, or serve as broadband access points.

1.3 MAN Access Solution

In a metropolitan area network (MAN), the Switch can serve as access devices. In the downlink direction, they directly connect to users through 1000 Mbps interfaces; and in the uplink direction, they connect to an aggregation layer (Layer 3) switches or service gateways, which further connect to the core of the MAN through routers. This provides you a comprehensive gigabit-to-backbone 1000-Mbps-to-desktop MAN solution.

1.4 Education Network Solution

In a campus network, the Switch can serve as desktop switching devices at the access layer. They directly connect to users in education buildings through 1000 Mbps downlink interfaces; and connect to the core switch in the campus through a 1000 Mbps uplink interface; the core switch further connects to the education network through a router. This enables the users in the campus to exchange information and share resources in the scope of the education network.

1.5 Multi-Service Carrier VLAN Solution

With development of various application technologies, enterprise users are increasingly relying on network services. They hope the networks can offer secure, reliable leased lines, VOIP and video conference services, thus reducing their operating costs. Additionally, apart from simple Internet surfing, individual users expect more abundant services from the networks, e.g., IPTV, video chatting, real-time gaming, etc.

To carry such services with different QOS requirements, the broadband access network needs to have effective service identification and isolation capacity. VLAN is the best service identification and isolation technology at present, and is the basis for multi-service deployment. As broadband users increase explosively and services appear continuously, however, the traditional VLAN technology cannot meet the requirements of service deployments. In this situation, QinQ, VLAN mapping, etc become new choices.

2 Using the Command-Line Interface

2.1 Command Modes

A command line interface (CLI) is a user interface to interact with a switch. Through the CLI on a switch, a user can enter commands to configure the switch and check output information to verify the configuration. Each Switch Ethernet switch provides an easy-to-use CLI and a set of configuration commands for the convenience of the user to configure and manage the switch.

The CLI on Switch Ethernet switches provides the following features, and so has good manageability and operability.

The user interface is divided into many different modes. The commands available to you depend on which mode you are currently in. Enter a question mark **(?)** at the system prompt to obtain a list of commands available for each command mode.

When you start a session on the switch, you begin in user mode, often called user EXEC mode. Only a limited subset of the commands is available in user EXEC mode. For example, most of the user EXEC commands are one-time commands, such as **show** commands, which show the current configuration status, and **clear** commands, which clear counters or interfaces. The user EXEC commands are not saved when the switch reboots.

To have access to all commands, you must enter privileged EXEC mode. Normally, you must enter a password to enter privileged EXEC mode. From this mode, you can enter any privileged EXEC command or enter global configuration mode.

Using the configuration modes (global, interface, and line), you can make changes to the running configuration. If you save the configuration, these commands are stored and used when the switch reboots. To access the various configuration modes, you must start at global configuration mode. From global configuration mode, you can enter interface configuration mode and line configuration mode.

2.2 Getting Help

You can enter a question mark **(?)** at the system prompt to display a list of commands available for each command mode. You can also obtain a list of associated keywords and arguments for any command.

For example:
Switch> **show ?**

2.3 Specifying Ports in Interface Configuration Mode

To configure a port, you need to specify the interface type, slot, and port number by using the interface

configuration command.

For example, to configure port 6 on a switch, you enter:
Switch(config)# **interface gigabitethernet 6**

For example, to configure port1-port 6 on a switch, you enter:
Switch(config)# **interface range gigabitethernet 1-6**

- Interface type—Each switch platform supports different types of interfaces. To display a complete list of the interface types supported on your switch, enter the interface ? global configuration command.
- Port number—The number of the physical port on the switch.

2.4 Abbreviating Commands

You have to enter only enough characters for the switch to recognize the command as unique. This example shows how to enter the **show interface** privileged EXEC command:

For example:
Switch# **sho int**

2.5 Using no Forms of Commands

Almost every configuration command also has a **no** form. In general, use the **no** form to disable a feature or function or reverse the action of a command. For example, the **no shutdown** interface configuration command reverses the shutdown of an interface. Use the command without the keyword **no** to re-enable a disabled feature or to enable a feature that is disabled by default.

2.6 Conventions

This publication uses these conventions to convey instructions and information:
Command descriptions use these conventions:
- Commands and keywords are in **boldface** text.
- Arguments for which you supply values are in *italic*.
- Square brackets ([ ]) mean optional elements.
- Braces ({ }) group required choices, and vertical bars (|) separate the alternative elements.
- Braces and vertical bars within square brackets ([{ | }]) mean a required choice within an optional element.

Interactive examples use these conventions:
- Terminal sessions and system displays are in screen font.
- Information you enter is in **boldface screen** font.
- Nonprinting characters, such as passwords or tabs, are in angle brackets (< >).

2.7 Accessing the CLI from a Browser

This procedure assumes that you have met the software requirements, and have assigned IP information and a password to the switch.

Copies of the web pages that you display are saved in your browser memory cache until you exit the browser session. You can access the CLI by clicking **Web Console - HTML access to the command line interface** from a cached copy of the Systems Access page. To prevent unauthorized access to web and the CLI, exit your browser to end the browser session.

3. Logging Switch

3.1 Logging into an Ethernet Switch

You can log into the Switch Ethernet switch in one of the following ways:

- Logging in locally through the Console port
- Logging in locally or remotely through an Ethernet port by means of Telnet or SSH
- Logging into the Web-based network management system
- Logging in through NMS (network management station)

3.2 Logging in through the Console Port

To log in through the Console port is the most common way to log into a switch. It is also the prerequisite to configure other login methods. By default, you can locally log into the switch through its Console port.

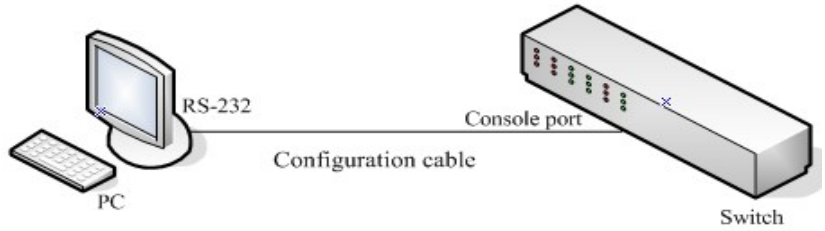
the default settings of a Console port.

Setting	**Default**
Baud rate	115,200 bps
Flow control	None
Check mode(Parity)	None
Stop bits	1
Data bits	8

To log into a switch through the Console port, make sure the settings of both the Console port and the user terminal are the same.

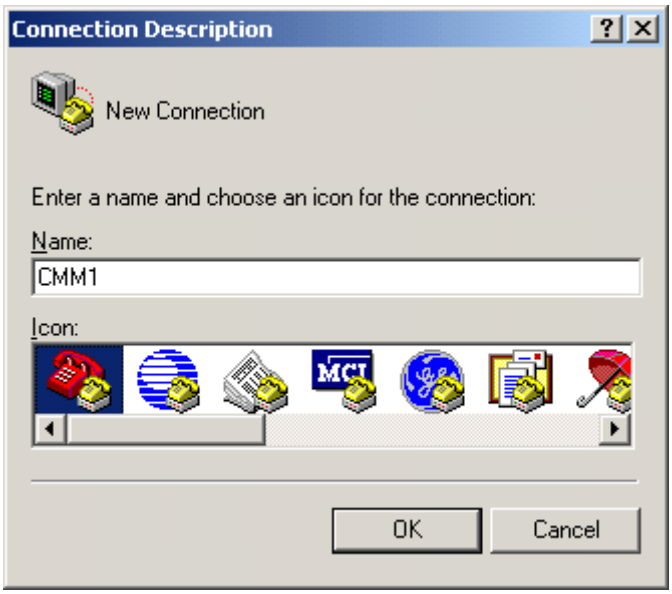
Following are the procedures to connect to a switch through the Console port.

1) Connect the serial port of your PC/terminal to the Console port of the switch as shown.



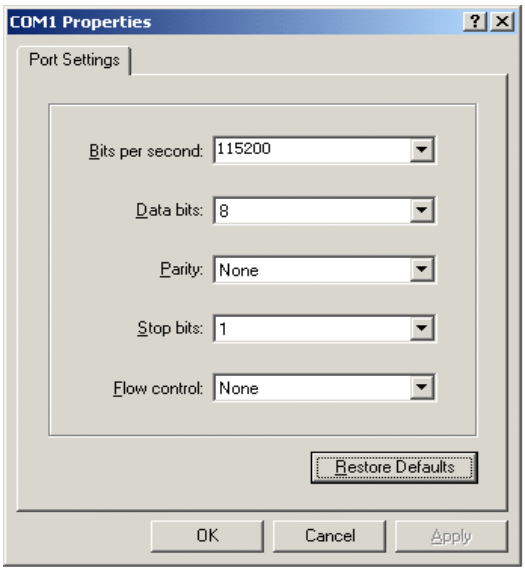
2) If you use a PC to connect to the Console port, launch a terminal emulation utility (such as Terminal in Windows 3.X or HyperTerminal in Windows 9X/Windows 200Windows XP. The following assumes that you are running Windows XP) and perform the configuration shown.

Create a connection



Specify the port used to establish the connection

Set port parameters



3) Turn on the switch. You will be prompted to press the Enter key if the switch successfully completes POST (power-on self test). The prompt (such as < Press RETURN to get started.>) appears after you press the Enter key.

4) You can then configure the switch or check the information about the switch by executing the corresponding commands. You can also acquire help by typing the ? character. Refer to related parts in this manual for information about the commands used for configuring the switch.

4 System operation command

4.1 Command to configure multiple ports

	Command	**Purpose**
Step 1	**configure**	Enter global configuration mode.
Step 2	**interface range gigabitethernet** *interface-id*	Configure port number range
Step 4	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

That is, if the user wants to configure some ports, he can use commands to enter the corresponding Ethernet port configuration mode.

E.g:
switch(config)# **interface range gigabitethernet 1-5**
switch(config)# **interface range gigabitethernet 1-5,7** (The configuration ports can be discontinuous, separated by ",")

4.2 Configure permission level

The Switch system provides two levels of access to configuration options: cli viewing, configuration permissions, and cli viewing permissions; viewing and controlling permissions for all functions of the web, and viewing permissions for a small number of functions of the web.
Supports privilege levels 0 to 15.

- Privilege levels 2 to 15 provide access to view and configure all the web functions of the switch system.
- Privilege levels 0 to 1 provide more viewing rights to some functions of the switch system's web.
- Privilege level 15 provides cli viewing and configuration permissions for the switch system.
- Privilege levels 0 to 14 provide cli viewing rights to the switch system.

The configuration contains admin and user permissions, and the levels correspond to level 15 and level 1.

	Command	**Purpose**
Step 1	**Configure**	Enter global configuration mode.
Step 2	**username** *username* **{nopassword | password | privilege | secret}**	Configure user name and privileged password level
Step 3	**username** *username* **nopassword**	Add username without password
Step 4	**username** *username* **password** *line*	Add username and password
Step 5	**username** *username* **privilege {<0-15> | admin | user}**	Configure user level
Step 6	**username** *username* **secret {password | encrypted}**	Configure whether the password of the username is encrypted or not
Step 7	**show username**	View the username information of the switch
Step 8	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Use the "**no username**" command to delete the username.

Example how to add the username aaa, and set the password aaa, the level is 15 and hide the password display:

Switch#
Switch# **configure**
Switch(config)# **username aaa privilege 15 secret aaa**
Switch# **show username**

4.3 Save parameters

	Command	**Purpose**

Step 1	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

The example shows how to save the parameters:

Switch# **copy running-config startup-config**
Success
Switch#

4.4 Switch restart

	Command	**Purpose**
Step 1	**reboot**	Switch restart

The example shows how to restart the switch:

Switch# **reboot**

4.5 Restore default parameters

	Command	**Purpose**
Step 1	**restore-defaults**	Restore the default parameters of the switch
Step 2	**restore-defaults interface {GigabitEthernet | LAG}** *interface-id*	Restore the default parameters of the switch port

When inputting the "**restore-defaults**" command, it displays "restore factory defaults. Do you want to reboot now? (y/n)", please press the "**y**" key. If you want to cancel this operation, press the "**n**" key.

The example shows how to restore the factory parameters:

Switch# **restore-defaults**
System: restore factory defaults. Do you want to reboot now? (y/n)*Jan 01 2000 08:35:05: %SYSTEM-5-RESTORE: System restore to default
y

The example shows how to restore the factory parameters of all ports:

Switch# **restore-defaults interfaces GigabitEthernet 1-28**

4.6 View system information

	Command	Purpose
Step 1	**show info**	View system information

Including viewing the system name, IP, MAC address, running time and so on.

The example shows how to view the current system information:

Switch# **show info**

4.7 View the CPU usage of the switch

	Command	Purpose
Step 1	**show cpu utilization**	View CPU usage

The example shows how to view the current CPU usage rate:

Switch# **show cpu utilization**

4.8 View memory usage

	Command	Purpose
Step 1	**show memory statistics**	View the memory usage of the switch

The example shows how to view the current memory usage:

Switch# **show memory statistics**

4.9 View all configuration information of the switch

	Command	Purpose
Step 1	**show running-config**	View all configuration information of the switch
Step 2	**show running-config interface {GigabitEthernet | LAG}** *interface-id*	View the configuration information of the switch port

The example shows how to view all the configuration information of the current system:

Switch# **show running-config**

The example shows how to view the port configuration information of the current system:

Switch# **show running-config interfaces GigabitEthernet 1-28**

5 Configuring IEEE802.1Q VLANs

5.1 Introduction to VLAN

The traditional Ethernet is a broadcast network, where all hosts are in the same broadcast domain and connected with each other through hubs or switches. Hubs and switches, which are the basic network connection devices, have limited forwarding functions.

- A hub is a physical layer device without the switching function, so it forwards the received packet to all ports except the inbound port of the packet.
- A switch is a link layer device which can forward a packet according to the MAC address of the packet. A switch builds a table of MAC addresses mapped to associated ports with that address and only sends a known MAC's traffic to one port. When the switch receives a broadcast packet or an unknown unicast packet whose MAC address is not included in the MAC address table of the switch, it will forward the packet to all the ports except the inbound port of the packet.

The above scenarios could result in the following network problems.

- Large quantity of broadcast packets or unknown unicast packets may exist in a network, wasting network resources.
- A host in the network receives a lot of packets whose destination is not the host itself, causing potential serious security problems.

- Related to the point above, someone on a network can monitor broadcast packets and unicast packets and learn of other activities on the network. Then they can attempt to access other resources on the network, whether or not they are authorized to do this.

Isolating broadcast domains is the solution for the above problems. The traditional way is to use routers, which forward packets according to the destination IP address and does not forward broadcast packets in the link layer. However, routers are expensive and provide few ports, so they cannot split the network efficiently. Therefore, using routers to isolate broadcast domains has many limitations.

The Virtual Local Area Network (VLAN) technology is developed for switches to control broadcasts in LANs.

A VLAN can span multiple physical spaces. This enables hosts in a VLAN to be located in different physical locations. By creating VLANs in a physical LAN, you can divide the LAN into multiple logical LANs, each of which has a broadcast domain of its own. Hosts in the same VLAN communicate in the traditional Ethernet way. However, hosts in different VLANs cannot communicate with each other directly but need the help of network layer devices, such as routers and Layer 3 switches.

5.2 Advantages of VLANs

Compared with traditional Ethernet technology, VLAN technology delivers the following benefits:

- Confining broadcast traffic within individual VLANs. This saves bandwidth and improves network performance.
- Improving LAN security. By assigning user groups to different VLANs, you can isolate them at Layer 2. To enable communication between VLANs, routers or Layer 3 switches are required.
- Flexible virtual workgroup creation. As users from the same workgroup can be assigned to the same VLAN regardless of their physical locations, network construction and maintenance is much easier and more flexible.

5.2.1 Configuring an Access mode VLAN

Configuration procedure

Follow these steps to perform basic VLAN interface configuration:

	Command	**Purpose**
Step 1	**configure**	Enter global configuration mode.
Step 2	**VLAN {***vlan-id* **| mac-vlan | protocol-vlan}**	Create VLAN
Step 3	**interface {GigabitEthernet | LAG | range}** *interface-id*	Enter the interface to be added to the VLAN.
Step 4	**switchport mode access**	Define the VLAN membership mode for the port (Layer 2 access port).

Step 5	**switchport access vlan** *vlan-id*	Assign the port to a VLAN. Valid VLAN IDs are 1 to 4094.
Step 6	**show interfaces switchport {gigabitEthernet | LAG}** *interface-id*	Verify your entries in the Administrative Mode and the Access Mode VLAN fields of the display.
Step 7	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To return an interface to its default configuration, use the **default interface** *interface-id* interface configuration command.
This example shows how to configure a port as an access port in VLAN 2:

Switch#
Switch# **configure**
Switch(config)# **vlan 2**
Switch(config-vlan)# **exit**
Switch(config)# **interface GigabitEthernet 2**
Switch(config-if)# **switchport mode access**
Switch(config-if)# **switchport access vlan 2**
Switch(config-if)# **exit**
Switch(config)# **exit**
Switch# **copy running-config startup-config**

5.2.2 Configuring a Hybrid mode VLAN

A Hybrid port may belong to multiple VLANs, and this configuration can only be performed in Ethernet port view.

Configuration procedure

	Command	**Purpose**
Step 1	**configure**	Enter global configuration mode.
Step 2	**interface {GigabitEthernet | LAG | range}** *interface-id*	Enter the interface to be added to the VLAN.
Step 3	**switchport mode** {**access | hybrid** | **trunk**}	Configure the interface as a Layer 2 trunk (required only if the interface is a Layer 2 access port or to specify the trunking mode). The link type of a port is Trunk by default.
Step 4	**switchport mode hybrid**	Define the VLAN membership mode for the port (Layer 2 hybrid port).
Step 5	**switchport hybrid allowed vlan** {**add** | **remove**} *vlan-list*	(Optional) Configure the list of untagged VLANs allowed on the hybrid. For explanations about using the **add**, and **remove** keywords, see the command reference for this release.

Step 6	**switchport hybrid allowed vlan add** *vlan-id* **untagged**	Configure PVID on the hybrid. Valid VLAN IDs are 1 to 4094. By default, all Access ports belong to VLAN 1.
Step 7	**switchport hybrid allowed vlan add** *vlan-id* **tagged**	(Optional) Configure the list of untagged VLANs allowed on the hybrid.. Valid VLAN IDs are 1 to 4094.
Step 8	**show interfaces switchport**	Verify your entries in the Administrative Mode and the Access Mode VLAN fields of the display.
Step 9	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

This example shows how to configure a port as an hybrid port in multiple VLAN.

Switch#
Switch# **configure**
Switch(config)# **vlan 3**
Switch(config-vlan)# **exit**
Switch(config)# **interface GigabitEthernet 3**
Switch(config-if)# **switchport mode hybrid**
Switch(config-if)# **switchport hybrid pvid 3**
Switch(config-if)# **switchport hybrid allowed vlan add 1 tag**
Switch(config-if)# **switchport hybrid allowed vlan add 2 untag**
Switch(config-if)# **exit**
Switch(config)# **exit**
Switch# **copy running-config startup-config**

This example shows how to remove VLAN 2 from the allowed VLAN list:

Switch# **configure**
Switch(config)# **interface gi 3**
Switch(config-if)# **switchport hybrid allowed vlan remove 2**
Switch(config-if)# **exit**
Switch(config)# **exit**
Switch#

5.2.3 Configuring a Trunk mode VLAN

A Trunk port may belong to multiple VLANs, and you can only perform this configuration in Ethernet port view.

Configuration procedure

	Command	Purpose
Step 1	**configure**	Enter global configuration mode.
Step 2	**interface {GigabitEthernet | LAG | range}** *interface-id*	Enter the interface to be added to the VLAN.
Step 3	**switchport mode** {**access | hybrid** | **qinq** | **trunk**}	Configure the interface as a Layer 2 trunk (required only if the interface is a Layer 2 access port or to specify the trunking mode). The link type of a port is Trunk by default.
Step 4	**switchport mode trunk**	Define the VLAN membership mode for the port (Layer 2 trunk port).
Step 5	**switchport trunk allowed vlan** {**add** | **remove**} *vlan-list*	(Optional) Configure the list of VLANs allowed on the trunk. For explanations about using the **add**, and **remove** keywords, see the command reference for this release.
Step 6	**switchport trunk allowed vlan add** *vlan-id*	Configure PVID on the trunk. Valid VLAN IDs are 1 to 4094.
Step 7	**show interfaces switchport**	Verify your entries in the Administrative Mode and the Access Mode VLAN fields of the display.
Step 8	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

This example shows how to configure a port as a trunk port and tag VLAN 1, 2, and 3:

Switch# **config**
Switch(config)# **vlan 4**
Switch(config-vlan)# **exit**
Switch(config)# **interface gi 4**
Switch(config-if)# **switchport mode trunk**
Switch(config-if)# **switchport trunk native vlan 4**
Switch(config-if)# **switchport trunk allowed vlan add 3**
Switch(config-if)# **switchport trunk allowed vlan add 2**
Switch(config-if)# **switchport trunk allowed vlan add 1**
Switch(config-if)# **exit**
Switch(config)# **exit**
Switch#

This example shows how to remove VLAN 1 from the allowed VLAN list:

Switch(config)# **interface gi 4**
Switch(config-if)# **switchport trunk allowed vlan remove 1**
Switch(config-if)# **exit**
Switch(config)# **exit**
Switch#

Displaying and Maintaining VLAN

	Command	Purpose
Step 1	**show vlan**	Verify your entries.
Step 2	**show interface switchport**	Verify your entries.
Step 3	**show vlan** [*vlan-id*]	Display characteristics for all interfaces or for the specified VLAN configured on the switch.
Step 4	**show interfaces switchport {Gigabitethernet | LAG}** *interface-id*	Display parameters for all VLANs or the specified VLAN on the switch.

If a packet has a VLAN ID that is the same as the outgoing port native VLAN ID, the packet is sent untagged; otherwise, the switch sends the packet with a tag.

6 IP Addressing Overview

IP Address Classes

IP addressing uses a 32-bit address to identify each host on a network. An example is 01010000100000001000000010000000 in binary. To make IP addresses in 32-bit form easier to read, they are written in dotted decimal notation, each being four octets in length, for example, 10.1.1.1 for the address just mentioned.
Each IP address breaks down into two parts:

- Net ID: The first several bits of the IP address defining a network, also known as class bits.
- Host ID: Identifies a host on a network.

Subnetting and Masking

Subnetting was developed to address the risk of IP address exhaustion resulting from fast expansion of the Internet. The idea is to break a network down into smaller networks called subnets by using some bits of the host ID to create a subnet ID. To identify the boundary between the host ID and the combination of net ID and subnet ID, masking is used.
Each subnet mask comprises 32 bits related to the corresponding bits in an IP address. In a subnet mask, the part containing consecutive ones identifies the combination of net ID and subnet ID whereas the part containing consecutive zeros identifies the host ID.

6.1 Configuring IP Addresses

The Switches support assigning IP addresses to VLAN interfaces. Besides directly assigning an IP address to a VLAN interface, you may configure a VLAN interface to obtain an IP address through DHCP client.

Configuration procedure

	Command	**Purpose**
Step 1	**configure**	Enter global configuration mode.
Step 2	**ip address** *ip-address subnet-mask*	Enter the static IP address and subnet mask.
Step 3	**ip dhcp**	Configure dhcp to dynamically get an IP address
Step 4	**exit**	Return to global configuration mode.
Step 5	**show ip**	Verify the configured IP address.
Step 6	**show dhcp**	Verify the IP configuration information of interface.
Step 7	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To change the IP address of the switch, use the **ip address** interface configuration command. If you want to delete the address through a Telnet session, the connection to the switch will be lost.

The switch default IP address is **192.168.1.1**.

This example shows how to configure an IP address:

Switch#
Switch# **configure**
Switch(config)# **ip address 192.168.1.2 mask 255.255.255.0**
Switch(config)# **ip default-gateway 192.168.1.253**
Switch(config)# **exit**
Switch# **sho ip**
IP Address: 192.168.1.2
Subnet Netmask: 255.255.255.0
Default Gateway: 192.168.1.253
Switch#

To configure the second ip address of the switch, use the **ip address** configuration command.

This example shows how to configure the second IP address of the switch:

Switch#
Switch# **configure**
Switch(config)# **ip address 192.168.2.1 mask 255.255.255.0 secondary**
Switch(config)# **exit**

Switch# **show running-config**
SYSTEM CONFIG FILE ::= BEGIN
! System Description: RTK GS8382-28 Switch
! System Version: v3.1.0
! System Name: Switch
! System Up Time: 0 days, 0 hours, 15 mins, 35 secs
!
!
!
ip address 192.168.2.1 mask 255.255.255.0 secondary
username "admin" secret encrypted MjEyMzJmMjk3YTU3YTVhNzQzODk0YTBlNGE4MDFmYzM=

This example shows how to configure DCHP to dynamically get an IP address:

Switch(config)# **ip dhcp**
Switch(config)# **exit**
Switch# **sho ip**
IP Address: 192.168.1.2
Subnet Netmask: 255.255.255.0
Default Gateway: 192.168.1.253
Switch#

To remove the gateway address of the switch, use the **no ip default-gateway** interface configuration command.

Switch(config)# **no ip default-gateway**
Switch(config)# **exit**
Switch# **show ip**
IP Address: 192.168.1.2
Subnet Netmask: 255.255.255.0
Default Gateway: 0.0.0.0
Switch#

6.2 Displaying IP Addressing Configuration

After the above configuration, you can execute the show command in any view to display the operating status and configuration on the interface to verify your configuration.

This is an example of output from the **show ip** privileged EXEC command for the interface:

Switch#
Switch# **show ip**
IP Address: 192.168.1.2
Subnet Netmask: 255.255.255.0
Default Gateway: 0.0.0.0

Switch# **show ip dhcp**
DHCP Status : disabled
Switch#

7 MAC Address Table Management

7.1 MAC address Overview

Introduction to MAC Address Table

An Ethernet switch is mainly used to forward packets at the data link layer, that is, transmit the packets to the corresponding ports according to the destination MAC address of the packets. To forward packets quickly, a switch maintains a MAC address table, which is a Layer 2 address table recording the MAC address-to-forwarding port association. Each entry in a MAC address table contains the following fields:

- Destination MAC address
- ID of the VLAN which a port belongs to
- Forwarding egress port number on the local switch

When forwarding a packet, an Ethernet switch adopts one of the two forwarding methods based upon the MAC address table entries.

- Unicast forwarding: If the destination MAC address carried in the packet is included in a MAC address table entry, the switch forwards the packet through the forwarding egress port in the entry.
- Broadcast forwarding: If the destination MAC address carried in the packet is not included in the MAC address table, tthe switch broadcasts the packet to all ports except the one that originally received the packet.

Introduction to MAC Address Learning

MAC address table entries can be updated and maintained through the following two ways:

- Manual configuration
- MAC address learning

Generally, the majority of MAC address entries are created and maintained through MAC address learning.

Managing MAC Address Table

Aging of MAC address table

To fully utilize a MAC address table, which has a limited capacity, the switch uses an aging mechanism for updating the table. That is, the switch starts an aging timer for an entry when dynamically creating the entry. The switch removes the MAC address entry if no more packets with the MAC address recorded in the entry are received within the aging time.

Entries in a MAC address table

Entries in a MAC address table fall into the following categories according to their characteristics and configuration methods:

- Static MAC address entry: Also known as permanent MAC address entry. This type of MAC address entries are added/removed manually by the network operator and cannot age out by themselves. Using static MAC address entries can greatly reduce broadcast packets and are

suitable for networks where network devices seldom change.

- Dynamic MAC address entry: This type of MAC address entries age out after the configured aging time. They are generated by the MAC address learning mechanism or configured manually.
- Blackhole MAC address entry: This type of MAC address entries are configured manually. A switch discards the packets destined for or originated from the MAC addresses contained in blackhole MAC address entries. Blackhole entries are configured for filtering out frames with specific source or destination MAC addresses.

7.2 MAC Address Table Management

MAC Address Table Management Configuration Task List

Configuring a MAC Address Entry

You can add, modify, or remove a MAC address entry, remove all MAC address entries concerning a specific port, or remove specific type of MAC address entries (dynamic or static MAC address entries). You can add a MAC address entry in either system view or Ethernet port view.

Adding a MAC address entry in system view

Steps to add a MAC address entry in system view:

	Command	**Purpose**
Step 1	**configure**	Enter global configuration mode.
Step 3	**mac address-table** {**aging-time** | **static** }	Configuring the MAC address entry.

Adding a MAC address entry in system view

Steps to add a MAC address entry in system view:

	Command	**Purpose**
Step 1	**configure**	Enter global configuration mode.
Step 2	**mac-address-table static** *mac-address* **vlan** *vlan-id* **interface** *interface-id*	Adding MAC address entry in VLAN and port.
Step 3	**show mac-address-table static**	Verify your entries.
Step 4	**show mac-address-table**	Verify your entries.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Follow these steps to configure static mac-address of port 1.

Switch#
Switch# **configure**
Switch(config)# **mac ad sta 00:00:00:00:00:dd vlan 1 int gi 1**
Switch(config)# **exit**
Switch# **show mac address-table**
Switch# **show mac-address-table static**

Configure a blackhole MAC address entry in system view

Steps to add a MAC address entry in system view:

	Command	Purpose
Step 1	**configure**	Enter global configuration mode.
Step 2	**mac-address-table static** *mac-address* **vlan** *vlan-id* **[interface** *interface-id***] drop**	Configure blackhole MAC address entry in VLAN and port.
Step 3	**show mac-address-table filter**	Verify your entries.
Step 4	**show mac-address-table**	Verify your entries.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Follow these steps to configure static mac-address of vlan 1.

Switch#
Switch# **configure**
Switch(config)# **mac address-table static 22:22:22:33:33:33 vlan 1 drop**
Switch(config)# **exit**
Switch# **show mac-address-table**
Switch# **show mac-address-table static**

Setting the MAC Address Aging Timer

Setting an appropriate MAC address aging timer is important for the switch to run efficiently.

- If the aging timer is set too long, excessive invalid MAC address entries maintained by the switch may fill up the MAC address table. This prevents the MAC address table from being updated with network changes in time.
- If the aging timer is set too short, the switch may remove valid MAC address entries. This decreases the forwarding performance of the switch.

Configure aging time of MAC address entries:

	Command	Purpose
Step 1	**configure**	Enter global configuration mode.
Step 2	**mac-address-table aging-time** *time-number*	Configuring the aging time of MAC address.
Step 3	**show mac-address-table aging**	Verify your entries.
Step 4	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Follow these steps to configure mac address aging time of system.

Switch#
Switch# **configure**
Switch(config)# **mac-address-table aging-time 60**
Switch(config)# **exit**
Switch# **show mac address-table aging-time**

Displaying MAC Address Table Information

Switch# **sho mac address-table** ?

```
  <cr>
  A:B:C:D:E:F    MAC address xx:xx:xx:xx:xx:xx
  aging-time      aging time of the address table
  counters        total entries
  dynamic         Dynamic entries
  interfaces      Interface status and configuration
  static          Static entries
  vlan            VLAN configuration
```

Command	Purpose
show mac address-table	Verify the MAC address table entries.
show mac address-table *MAC-address*	Verify the detailed MAC address table entries.
show mac address-table aging-time	Verify aging time of the dynamic MAC address entries in the MAC address table.
show mac address-table counters	Verify the MAC address table entries.
show mac address-table dynamic {interface | vlan}	Verify your entries.
show mac address-table interface {GigabitEthernet | LAG} *interface-id*	Verify the MAC address table entries.
show mac address-table static {interface | vlan}	Verify the blackhole MAC address entry.
show mac address-table vlan *vlan-id*	Verify the MAC address table entries in interface.

8 Port Basic Configuration

8.1 Ethernet Port Configuration

Initially Configuring a Port

	Command	Purpose
Step 1	**configure**	Enter global configuration mode.
Step 2	**interface {GigabitEthernet | LAG | range}** *interface-id*	Enter interface configuration mode and the physical interface to be configured.
Step 3	**speed** {**10 | 100 | 1000 | auto**}	Enter the appropriate speed parameter for the interface, or enter **auto**. If you use the **10**, **100**, or **1000** keywords

		with the **auto** keyword, the port only auto negotiates at the specified speeds.
Step 4	**duplex** {**auto | full | half**}	Enter the duplex parameter for the interface. For configuration guidelines, **Note** The **duplex** keyword is not available on Giga ports.
Step 5	**show interfaces {GigabitEthernet | LAG}** *interface-id* **status**	Display the interface speed and duplex mode configuration.
Step 6	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

This example shows how to set the interface speed to 10 Mbps and the duplex mode to half on a port:

Switch#
Switch# **configure**
Switch(config)# **interface gi 3**
Switch(config-if)# **speed 10**
Switch(config-if)# **duplex half**
Switch(config-if)# **exit**
Switch(config)# **exit**
Switch# **show interface gi 1-28 status**

Enabling Flow Control on a Port

Flow control is enabled on both the local and peer switches. If congestion occurs on the local switch:

- The local switch sends a message to notify the peer switch of stopping sending packets to itself or reducing the sending rate temporarily.
- The peer switch will stop sending packets to the local switch or reduce the sending rate temporarily when it receives the message; and vice versa. By this way, packet loss is avoided and the network service operates normally.

	Command	**Purpose**
Step 1	**configure**	Enter global configuration mode.
Step 2	**interface {GigabitEthernet | LAG | range}** *interface-id*	Enter interface configuration mode and the physical interface to be configured.
Step 3	**flowcontrol {}**	Enable the flow control of port
Step 4	**show interfaces {GigabitEthernet | LAG}** *interface-id* **status**	Display the interface speed and duplex mode configuration.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Use the **no flowcontrol** interface configuration command to disable the flow control.

This example shows how to turn on flow control on a port:

Switch#

Switch# **configure**
Switch(config)# **interface gi 3**
Switch(config-if)# **flowcontrol on**
Switch(config-if)# **exit**
Switch(config)# **exit**
Switch# **show interface gi 1-28 status**

8.2 Adding a Description for an Interface

You can add a description about an interface to help you remember its function. The description appears in the output of these commands: **show running-config**, and **show interfaces**.
Beginning in privileged EXEC mode, follow these steps to add a description for an interface:

	Command	**Purpose**
Step 1	**configure**	Enter global configuration mode.
Step 2	**Interface {GigabitEthernet | LAG | range}** *interface-id*	Enter interface configuration mode, and enter the interface for which you are adding a description.
Step 3	**description** *string*	Add a description for an interface.
Step 4	**show port-description**	Verify your entry.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Use the **no description** interface configuration command to delete the description.

This example shows how to add a description on a port and to verify the description:

Switch#
Switch# **configure**
Switch(config)# **interface gi 3**
Switch(config-if)# **description room3**
Switch(config-if)# **exit**
Switch(config)# **exit**
Switch# **show interface gi 1-28 status**

8.3 Configuring Storm Control

Understanding Storm Control
Storm control prevents traffic on a LAN from being disrupted by a broadcast, multicast, or unicast storm on a port. A LAN storm occurs when packets flood the LAN, creating excessive traffic and degrading network performance. Errors in the protocol-stack implementation, mistakes in network configuration, or users issuing a denial-of-service attack can cause a storm.

Storm control is configured for the switch as a whole but operates on a per-port basis. By default, storm control is disabled.

Storm control uses rising and falling thresholds to block and then restore the forwarding of broadcast, unicast, or multicast packets. You can also set the switch to shut down the port when the rising threshold is reached.

The thresholds can either be expressed as a percentage of the total available bandwidth that can be used by the broadcast, multicast, or unicast traffic, or as the rate at which the interface receives multicast, broadcast, or unicast traffic.

When a switch uses the bandwidth-based method, the rising threshold is the percentage of total available bandwidth associated with multicast, broadcast, or unicast traffic before forwarding is blocked. The falling threshold is the percentage of total available bandwidth below which the switch resumes normal forwarding. In general, the higher the level, the less effective the protection against broadcast storms. uses traffic rates as the threshold values, the rising and falling thresholds are in packets per second. The rising threshold is the rate at which multicast, broadcast, and unicast traffic is received before forwarding is blocked. \

The falling threshold is the rate below which the switch resumes normal forwarding. In general, the higher the rate, the less effective the protection against broadcast storms.

Configuring Storm Control and Threshold Levels
Beginning in privileged EXEC mode, follow these steps to configure storm control and threshold levels:

	Command	**Purpose**
Step 1	**configure**	Enter global configuration mode.
Step 2	**Storm-control {ifg {exclude | include} | unit {bps | pps}}**	Configure whether to include 8-byte preamble and 12-byte idle frame. Configure unit is pps or bps.
Step 3	**Interface {GigabitEthernet | LAG | range}** *interface-id*	Enter interface configuration mode, and enter the interface for which you are adding a description.
Step 4	**storm-control** {**action** | **broadcast** | **unknown-multicast** | **unknown-unicast**}	Configure broadcast, unknown-multicast, or unknown-unicast storm control.
Step 5	**show storm-control** [**interface**]	Verify your entries.
Step 6	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Use the **no storm-control broadcast/unknown-multicast/unknown-unicast** configuration command to delete these function of the port.

This example shows how to turn on storm control broadcast/unknown-multicast/unknown-unicast on a port to display the results:

Switch# **configure**
Switch(config)# **interface gigabitethernet 1**
Switch(config-if)# **storm-control**

Switch(config-if)# **storm-control broadcast**
Switch(config-if)# **storm-control broadcast level 100**
Switch(config-if)# **storm-control unknown-multicast**
Switch(config-if)# **storm-control unknown-multicast level 100**
Switch(config-if)# **storm-control unknown-unicast**
Switch(config-if)# **storm-control unknown-unicast level 100**
Switch(config-if)# **exit**
Switch(config)# **exit**
Switch# **show storm-control**

8.4 Configuring Port Rate Limiting

Port rate limiting refers to limiting the total rate of inbound or outbound packets on a port.

Port rate limiting can be implemented through token buckets. That is, if you perform port rate limiting configuration for a port, the token bucket determines the way to process the packets to be sent by this port or packets reaching the port. Packets can be sent or received if there are enough tokens in the token bucket; otherwise, they will be dropped.

Compared to traffic policing, port rate limiting applies to all the packets passing a port. It is a simpler solution if you want to limit the rate of all the packets passing a port.

	Command	**Purpose**
Step 1	**configure**	Enter global configuration mode.
Step 2	**qos**	Enter qos mode
Step 3	**Interface {GigabitEthernet | LAG | range}** *interface-id*	Enter interface configuration mode, and enter the interface for which you are adding a description.
Step 4	**rate-limit** {**egress** | **ingress**}	Configure rate limit of a port.
Step 5	**show interface rate-limit**	Verify your entries.
Step 6	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

This example shows how to turn on rate limit on a port to display the results:

Switch# **configure**
Switch(config)# **qos**
Switch(config)# **interface gigabitethernet 1**
Switch(config-if)# **rate-limit ingress 1000**
Switch(config-if)# **rate-limit egress 5000**
Switch(config-if)# **exit**
Switch(config)# **exit**
Switch# **show running-config interfaces GigabitEthernet 1**

8.5 Testing the Cable on an Ethernet Port

Through the following configuration tasks, the user can detect the current status of the cable connected to the Layer 2 Ethernet port on the device, and the system will return the detection result within 5 seconds. The detection content includes the receiving direction of the cable, the sending direction and whether there is a short circuit/open circuit phenomenon, at the same time, the length of the faulty cable can be detected.

	Command	**Purpose**
Step 1	**show cable-diag interface GigabitEthernet** *interface-id*	Verify your entries.

This example shows how to enable the cable test on the port and display the result:

Switch# **show cable-diag interfaces gi 1-24**

9 PoE

9.1 PoE Overview

9.1.1 Introduction to PoE

Power over Ethernet (PoE) means that power sourcing equipment (PSE) supplies power to powered devices (PD) such as IP telephony, wireless LAN access point, and web camera from Ethernet interfaces through twisted pair cables.

I. Advantages

- Reliable: Power is supplied in a centralized way so that it is very convenient to provide a backup power supply.
- Easy to connect: A network terminal requires only one Ethernet cable, but no external power supply.
- Standard: In compliance with IEEE 802.3af and 802.3at, and a globally uniform power interface is adopted.
- Promising: It can be applied to IP telephones, wireless LAN access points, portable chargers, card readers, web cameras, and data collectors.

II. Composition

A PoE system consists of PoE power, PSE, and PD.

- PoE power

The whole PoE system is powered by the PoE power, which includes external PoE power and internal PoE power.

- PSE

PSE is a card or subcard. PSE manages its own PoE interfaces independently. PSE examines the Ethernet cables connected to PoE interfaces, searches for the devices, classifies them, and supplies power to them. When detecting that a PD is unplugged, the PSE stops supplying power to the PD. An Ethernet interface with the PoE capability is called PoE interface. Currently, a PoE interface can be an FE or GE interface.

◯ PD

A PD is a device accepting power from the PSE. There are standard PDs and nonstandard PDs. A standard PD refers to the one that complies with IEEE 802.3af and 802.3at. The PD that is being powered by the PSE can be connected to other power supply units for redundancy backup.

9.1.2 Protocol Specification

The protocol specification related to PoE is IEEE 802.3af and IEEE 802.3at..

9.1.3 PoE watchdog

If the watchdog function of the port PoE is enabled, the port will detect the status of the port in real time. When the port is powered, but the port is in the linkdown state, or the ingress traffic of this port is 0, the PoE of this port will be powered off again and then powered. The detection interval is 3 minutes.

9.2 PoE Configuration Task List

Complete these tasks to configure PoE:

	Command	**Purpose**
Step 1	**configure**	Enter global configuration mode.
Step 2	**interface {GigabitEthernet | LAG | range}** *interface-id*	Specify the port to configure, and enter interface configuration mode.
Step 3	**poe {status | watchdog}**	Configure PoE enable and disable
Step 4	**show poe interface GigabitEthernet** *interface-id*	Verify your entries.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Configure the poe of port 3 to be closed, by default, all port poes are open.
Configure the poe's watchdog of port 3 to be open, by default, all port poe's watchdog are close.

Switch#
Switch# **configure**
Switch(config)# **interface gi 3**
Switch(config-if)# **no poe**
Switch(config-if)# **poe watchdog**

Switch(config-if)# **exit**
Switch(config)# **exit**
Switch# **show poe status**

10 Configuring EtherChannels

10.1 Understanding EtherChannels

EtherChannel provides fault-tolerant high-speed links between switches, routers, and servers. You can use it to increase the bandwidth among the wiring closets and the data center, and you can deploy it anywhere in the network where bottlenecks are likely to occur. EtherChannel provides automatic recovery for the loss of a link by redistributing the load across the remaining links. If a link fails, EtherChannel redirects traffic from the failed link to the remaining links in the channel without intervention.

Each EtherChannel can consist of up to eight compatibly configured Ethernet interfaces. All interfaces in each EtherChannel must be the same speed, and all must be configured as Layer 2 interfaces.

Introduction to Link Aggregation
Link aggregation can aggregate multiple Ethernet ports together to form a logical aggregation group. To upper layer entities, all the physical links in an aggregation group are a single logical link.

Link aggregation is designed to increase bandwidth by implementing outgoing/incoming load sharing among the member ports in an aggregation group. Link aggregation group also allows for port redundancy, which improves connection reliability.

Introduction to LACP
Link aggregation control protocol (LACP) is designed to implement dynamic link aggregation and disaggregation. This protocol is based on IEEE802.3ad and uses link aggregation control protocol data units (LACPDUs) to interact with its peer.

With LACP enabled on a port, LACP notifies the following information of the port to its peer by sending LACPDUs: priority and MAC address of this system, priority, number and operation key of the port.

Upon receiving the information, the peer compares the information with the information of other ports on the peer device to determine the ports that can be aggregated. In this way, the two parties can reach an agreement in adding/removing the port to/from a dynamic aggregation group.

Operation key is generated by the system. It is determined by port settings such as port speed, duplex mode, and basic configurations.

- Selected ports in a manual aggregation group or a static aggregation group have the same operation key.
- Member ports in a dynamic aggregation group have the same operation key.

Exchanging LACP Packets

Both the **active** and **passive** LACP modes allow interfaces to negotiate with partner interfaces to determine if they can form an EtherChannel based on criteria such as interface speed and, for Layer 2 EtherChannels, trunking state, and VLAN numbers.

Interfaces can form an EtherChannel when they are in different LACP modes as long as the modes are compatible. For example:

- An interface in the **active** mode can form an EtherChannel with another interface that is in the **active** mode.
- An interface in the **active** mode can form an EtherChannel with another interface in the **passive** mode.

An interface in the **passive** mode cannot form an EtherChannel with another interface that is also in the **passive** mode because neither interface starts LACP negotiation.

An interface in the **on** mode that is added to a port channel is forced to have the same characteristics as the already existing **on** mode interfaces in the channel.

10.2 Understanding Load Balancing and Forwarding Methods

EtherChannel balances the traffic load across the links in a channel by randomly associating a newly learned MAC address with one of the links in the channel.

With source-MAC address forwarding, packets forwarded to an EtherChannel are distributed across the ports in the channel based on the source-MAC address of the incoming packet. Therefore, to provide load balancing, packets from different hosts use different ports in the channel, but packets from the same host use the same port in the channel. The MAC address learned by the switch does not change).

With destination-MAC address forwarding, packets forwarded to an EtherChannel are distributed across the ports in the channel based on the destination host MAC address of the incoming packet. Therefore, packets to the same destination are forwarded over the same port, and packets to a different destination might be sent on a different port in the channel.

Multiple workstations are connected to a switch, and an EtherChannel connects the switch to the router. Source-based load balancing is used on the switch end of the EtherChannel to ensure that the switch efficiently uses the bandwidth of the router by distributing traffic from the workstation across the physical links. Since the router is a single MAC address device, it uses destination-based load balancing to efficiently spread the traffic to the workstations across the physical links in the EtherChannel.

10.2.1 Configuring Layer 2 EtherChannels

	Command	Purpose
Step 1	**configure**	Enter global configuration mode.
Step 2	**lag load-balance {src-dst-mac | src-dst-mac-ip}**	Configure the calculation mode of load balancing
Step 3	**interface {GigabitEthernet | LAG | range}** *interface-id*	Specify a physical interface to configure, and enter interface configuration mode. Valid interfaces include physical interfaces. Up to eight interfaces of the same type and speed can be configured for the same group.
Step 4	**lag** *lag-number* **mode** {**active** | **passive | static**}	Assign the port to a channel group, and specify the static mode, and active mode of LACP. For *channel-group-number*, the range is 1 to 14. Each EtherChannel can have up to eight compatibly configured Ethernet interfaces.
Step 5	**show lag**	Verify your entries.
Step 6	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Use the **no channel-group** configuration command to delete aggregation function of the port.

This example shows how to assign **gigabitethernet 1** and **gigabitethernet 2** interfaces to static **channel-group 1** and display the results:

Switch# **configure terminal**
Enter configuration commands, one per line.
Switch(config)# **interface gigabitethernet 1**
Switch(config-if)# **channel-group 1 mode on**
Switch(config-if)# **exit**
Switch(config)# **interface gigabitethernet 2**
Switch(config-if)# **channel-group 1 mode on**
Switch(config-if)# **exit**
Switch(config)# **exit**
Switch# **show etherchannel**

This example shows how to configure the load balancing calculation mode of the aggregation port.

Switch#
Switch# **configure**
Switch(config)# **lag load-balance src-dst-mac-ip**
Switch(config)# **exit**
Switch# **show lag**

10.2.2 Configuring the LACP

When enabled, LACP tries to configure the maximum number of LACP-compatible ports in a channel, up to a maximum of 8 ports. Only eight LACP links can be active at one time. Any additional links are put in a hot standby state. If one of the active links becomes inactive, a link that is in hot standby mode becomes active in its place.

If eight links are configured for an EtherChannel group, the software determines which of the hot standby ports to make active based on:

LACP port-priority

Port ID

All ports default to the same port priority. You can change the port priority of LACP EtherChannel ports to specify which hot standby links become active first by using the lacp port-priority interface configuration command to set the port priority to a value lower than the default of 32768.

The hot standby ports that have lower port numbers become active in the channel first unless the port priority is configured to be a lower number than the default value of 32768.

	Command	**Purpose**
Step 1	**configure**	Enter global configuration mode.
Step 2	**lacp system-priority** *priority-value*	Select the LACP port priority value. The priority value ranges from 1 to 65535. By default. Interfaces close to the lower range will be used for LACP transmission.
Step 3	**interface {GigabitEthernet | LAG | range}** *interface-id*	Specify a physical interface to configure, and enter interface configuration mode.
Step 4	**lacp {port-priority | timeout}**	Configure the lacp parameters of the port
Step 5	**lacp port-priority** *value*	Configure the priority of lacp
Step 6	**lacp timeout {long | short}**	Configure the timeout mechanism of lacp
Step 7	**lag** *lag-number* **mode** {**active** | **passive | static**}	Assign ports to aggregation groups, and specify static mode, and LACP active or passive mode. The aggregation group number ranges from 1 to 8. Each aggregation group can have up to 8 properly configured Ethernet interfaces.
Step 8	**show lacp {lag-number | counters | internal | neighbor | sys-id}**	Verify your entries.
Step 9	**show lag**	Verify your entries.
Step 10	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Use the **no channel-protocol** configuration command to delete lacp function.

This example shows how to assign **gigabitethernet 5** and **gigabitethernet 6** interfaces to **LACP channel-group 1** and display the results:

Switch#
Switch# **configure**
Switch(config)# **interface gi 5**
Switch(config-if)# **lacp port-priority 1**
Switch(config-if)# **lacp timeout long**
Switch(config-if)# **lag 2 mode active**
Switch(config-if)# **exit**
Switch(config)# **interface gi 6**
Switch(config-if)# **lacp port-priority 1**
Switch(config-if)# **lacp timeout long**
Switch(config-if)# **lag 2 mode active**
Switch(config)# **exit**
Switch# **sho lag**
Switch# **sho lacp counters**
Switch# **sho lacp internal**
Switch# **sho lacp neighbor**
Switch# **sho lacp sys-id**

11 Clock Configuration

11.1 Introduction to NTP

Network time protocol (NTP) is a time synchronization protocol defined in RFC 1305. It is used for time synchronization between a set of distributed time servers and clients. Carried over UDP, NTP transmits packets through UDP port 123.

NTP is intended for time synchronization between all devices that have clocks in a network so that the clocks of all devices can keep consistent. Thus, the devices can provide multiple unified-time-based applications.

A local system running NTP can not only be synchronized by other clock sources, but also serve as a clock source to synchronize other clocks. Besides, it can synchronize, or be synchronized by other systems by exchanging NTP messages.

Applications of NTP
As setting the system time manually in a network with many devices leads to a lot of workload and cannot ensure accuracy, it is unfeasible for an administrator to perform the operation. However, an

administrator can synchronize the clocks of devices in a network with required accuracy by performing NTP configuration.

11.2 Managing the System Time and Date

You can manage the system time and date on your switch using automatic configuration, such as the Network Time Protocol (NTP), or manual configuration methods.

Understanding the System Clock

The heart of the time service is the system clock. This clock runs from the moment the system starts up and keeps track of the date and time.

The system clock can then be set from these sources:

- ○ Network Time Protocol
- ○ Manual configuration

The system clock keeps track of time internally based on Universal Time Coordinated (UTC), also known as Greenwich Mean Time (GMT). You can configure information about the local time zone so that the time appears correctly for the local time zone.

Understanding Network Time Protocol

The NTP is designed to time-synchronize a network of devices. NTP runs over User Datagram Protocol (UDP), which runs over IP. NTP is documented in RFC 1305.

An NTP network usually gets its time from an authoritative time source, such as a radio clock or an atomic clock attached to a time server. NTP then distributes this time across the network. NTP is extremely efficient; no more than one packet per minute is necessary to synchronize two devices to within a millisecond of one another.

11.3 Configuring NTP

	Command	**Purpose**
Step 1	**configure**	Enter global configuration mode.
Step 2	**clock source {local | sntp}**	Enable NTP function.
Step 3	**sntp host** *host-ip* **[port** *port-id***]**	Configure the switch system clock to be synchronized by a time server
Step 4	**show sntp**	Verify your entries.
Step 5	**show clock**	Verify your entries.
Step 6	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Use the “**no ntp”** configuration command to disable NTP function of the switch.

This example shows how to configure the switch to synchronize its system clock.

Switch#
Switch# **configure**
Switch(config)# **clock source sntp**
Switch(config)# **sntp host 192.168.1.100**
Switch(config)# **exit**
Switch# **show sntp**
Switch# **show clock**

11.4 Configuration daylight-saving time

	Command	**Purpose**
Step 1	**configure**	Enter global configuration mode.
Step 2	**clock summer-time** *char* **{date {***date***} | recurring {eu | first | last | usa}}**	Configure the daylight-saving time of the switch system clock.
Step 3	**show clock detail**	Verify your entries.
Step 4	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

This example shows how to configure time ranges for daylight-saving time and how to verify your configuration.

Switch# **configure**
Switch(config)# **clock summer-time a date jun 1 2021 00:00 dec 31 2030 23:59**
Switch# **exit**
Switch# **show clock detail**

11.5 Timezone configuration for system time

Timezone - Your local time-zone, and it ranges from UTC-12 to UTC+13. The system default configuration is UTC +8

	Command	**Purpose**
Step 1	**configure**	Enter global configuration mode.
Step 2	**clock timezone** *char number*	Configure the timezone of the switch system clock.
Step 3	**show clock detail**	Verify your entries.
Step 4	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Switch# **configure**

Switch(config)# **clock timezone 1 +6**
Switch# **exit**
Switch# **show clock**

11.6 Manual Configuring Time and Date Manually

If no other source of time is available, you can manually configure the time and date after the system is restarted. The time remains accurate until the next system restart. We recommend that you use manual configuration only as a last resort. If you have an outside source to which the switch can synchronize, you do not need to manually set the system clock.

Setting the System Clock
If you have an outside source on the network that provides time services, such as an NTP server, you do not need to manually set the system clock.

	Command	**Purpose**
Step 1	**clock set** *hh*:*mm*:*ss day month year*	Configure the switch system clock.
Step 2	**Show clock**	Verify your entries.

This example shows how to manually set the system clock to 23:05:00 on January 22, 2021:

Switch# **clock set 23:05:00 jan 22 2021**
Switch# **show clock**

12 Configuring mirror

This chapter describes how to configure Switched Port Analyzer (mirror) on the switch.

12.1 Understanding mirror

You can analyze network traffic passing through ports by using mirror to send a copy of the traffic to another port on the switch that has been connected to a switch probe device or security device. mirrors received or transmitted (or both) traffic on a source port and received traffic on one or more source ports, to a destination port for analysis.

Mirror Session
A local mirror session is an association of a destination port with source ports. You can monitor incoming or outgoing traffic on a series or range of ports.

mirror sessions do not interfere with the normal operation of the switch. However, an oversubscribed mirror destination, for example, a 10-Mbps port monitoring a 100-Mbps port, results in dropped or lost packets.

You can configure mirror sessions on disabled ports; however, a mirror session does not become active unless you enable the destination port and at least one source port for that session. The **show monitor session** *session_number* privileged EXEC command displays the operational status of a mirror session.

A mirror session remains inactive after system power-on until the destination port is operational.

Source Port

A source port (also called a monitored port) is a switched port that you monitor for network traffic analysis. In a single local mirror session source session, you can monitor source port traffic such as received (Rx), transmitted (Tx), or bidirectional (both). The switch supports any number of source ports (up to the maximum number of available ports on the switch).

A source port has these characteristics:

- It can be any port type (for example, EtherChannel, Fast Ethernet, Gigabit Ethernet, and so on).
- It cannot be a destination port.
- Each source port can be configured with a direction (ingress, egress, or both) to monitor. For EtherChannel sources, the monitored direction would apply to all the physical ports in the group.
- Source ports can be in the same or different VLANs.
  You can configure a trunk port as a source port. All VLANs active on the trunk are monitored.

Destination Port

Each local mirror session destination session must have a destination port (also called a *monitoring port*) that receives a copy of traffic from the source port.

The destination port has these characteristics:

- It must reside on the same switch as the source port.
- It can be any Ethernet physical port.
- It cannot be a source port or a reflector port.
- It cannot be an EtherChannel group or a VLAN.
- It can be a physical port that is assigned to an EtherChannel group, even if the EtherChannel group has been specified as a mirror source. The port is removed from the group while it is configured as a mirror destination port.
- A destination port receives copies of sent and received traffic for all monitored source ports. If a destination port is oversubscribed, it could become congested. This could affect traffic forwarding on one or more of the source ports.

12.2 Configuration mirror

Beginning in privileged EXEC mode, follow these steps to create a mirror session and specify the source

(monitored) and destination (monitoring) ports:

	Command	Purpose
Step 1	**configure**	Enter global configuration mode.
Step 2	**mirror session** *session-id* **source** {**interface** *interface-id* [**both** | **rx** | **tx**]}	Specify the mirror session and the source port (monitored port).
Step 3	**mirror session** *session-id* **destination interface** *interface-id* **allow-ingress**	Specify the mirror session and the destination port (monitoring port).
Step 4	**show mirror**	Verify your entries.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Use the **no mirror session** configuration command to disable the mirror.
Use the **no mirror session source** configuration command to delete the source port of mirror.
Use the **no mirror session destination** configuration command to delete the destination port of mirror.

This example shows how to set up a mirror session, for monitoring source port traffic to a destination port. Bidirectional traffic is mirrored from source port 2-3 to destination port 1.

Switch#
Switch# **configure**
Switch(config)# **mirror session 1 destination interface gi 1 allow-ingress**
Switch(config)#
Switch(config)# **mirror session 1 source interfaces gi 2-3 both**
Switch(config)# **exit**
Switch# **show mirror**

13 STP Configuration

13.1 STP Overview

Functions of STP

Spanning tree protocol (STP) is a protocol conforming to IEEE 802.1d. It aims to eliminate loops on data link layer in a local area network (LAN). Devices running this protocol detect loops in the network by exchanging packets with one another and eliminate the loops detected by blocking specific ports until the network is pruned into one with tree topology. As a network with tree topology is loop-free, it prevents packets in it from being duplicated and forwarded endlessly and prevents device performance degradation.

Currently, in addition to the protocol conforming to IEEE 802.1d, STP also refers to the protocols based

on IEEE 802.1d, such as RSTP, and MSTP.

Protocol packets of STP

STP uses bridge protocol data units (BPDUs), also known as configuration messages, as its protocol packets.

STP identifies the network topology by transmitting BPDUs between STP compliant network devices. BPDUs contain sufficient information for the network devices to complete the spanning tree calculation. In STP, BPDUs come in two types:

- Configuration BPDUs, used to calculate spanning trees and maintain the spanning tree topology.
- Topology change notification (TCN) BPDUs, used to notify concerned devices of network topology changes, if any.

Basic concepts in STP

1) Root bridge

A tree network must have a root; hence the concept of “root bridge” has been introduced in STP. There is one and only one root bridge in the entire network, and the root bridge can change alone with changes of the network topology. Therefore, the root bridge is not fixed.

Upon network convergence, the root bridge generates and sends out configuration BPDUs periodically. Other devices just forward the configuration BPDUs received. This mechanism ensures the topological stability.

2) Root port

On a non-root bridge device, the root port is the port with the lowest path cost to the root bridge. The root port is used for communicating with the root bridge. A non-root-bridge device has one and only one root port. The root bridge has no root port.

3) Designated bridge and designated port

designated bridge: A designated bridge is a device that is directly connected to a switch and is responsible for forwarding BPDUs to this switch.

designated port: The port through which the designated bridge forwards BPDUs to this device

4) Path cost

Path cost is a value used for measuring link capacity. By comparing the path costs of different links, STP selects the most robust links and blocks the other links to prune the network into a tree.

How STP works

STP identifies the network topology by transmitting configuration BPDUs between network devices. Configuration BPDUs contain sufficient information for network devices to complete the spanning tree calculation. Important fields in a configuration BPDU include:

- Root bridge ID, consisting of root bridge priority and MAC address.

- Root path cost, the cost of the shortest path to the root bridge.
- Designated bridge ID, designated bridge priority plus MAC address.
- Designated port ID, designated port priority plus port name.
- Message age: lifetime for the configuration BPDUs to be propagated within the network.
- Max age, lifetime for the configuration BPDUs to be kept in a switch.
- Hello time, configuration BPDU interval.
- Forward delay, forward delay of the port.

5) Detailed calculation process of the STP algorithm

- Initial state
  Upon initialization of a device, each device generates a BPDU with itself as the root bridge, in which the root path cost is 0, designated bridge ID is the device ID, and the designated port is the local port.
- Selection of the optimum configuration BPDU
  Each device sends out its configuration BPDU and receives configuration BPDUs from other devices.
- Selection of the root bridge
  At network initialization, each STP-compliant device on the network assumes itself to be the root bridge, with the root bridge ID being its own bridge ID. By exchanging configuration BPDUs, the devices compare one another's root bridge ID. The device with the smallest root bridge ID is elected as the root bridge.
- Selection of the root port and designated ports
  A non-root-bridge device takes the port on which the optimum configuration BPDU was received as the root port.

Once the root bridge, the root port on each non-root bridge and designated ports have been successfully elected, the entire tree-shaped topology has been constructed.

6) The BPDU forwarding mechanism in STP

- Upon network initiation, every switch regards itself as the root bridge, generates configuration BPDUs with itself as the root, and sends the configuration BPDUs at a regular interval of hello time.
- If it is the root port that received the configuration BPDU and the received configuration BPDU is superior to the configuration BPDU of the port, the device will increase message age carried in the configuration BPDU by a certain rule and start a timer to time the configuration BPDU while it sends out this configuration BPDU through the designated port.
- If the configuration BPDU received on the designated port has a lower priority than the configuration BPDU of the local port, the port will immediately sends out its better configuration BPDU in response.
- If a path becomes faulty, the root port on this path will no longer receive new configuration BPDUs and the old configuration BPDUs will be discarded due to timeout. In this case, the device generates configuration BPDUs with itself as the root bridge and sends configuration BPDUs and TCN BPDUs. This triggers a new spanning tree calculation so that a new path is established to restore the network connectivity.

However, the newly calculated configuration BPDU will not be propagated throughout the network

immediately, so the old root ports and designated ports that have not detected the topology change continue forwarding data through the old path. If the new root port and designated port begin to forward data as soon as they are elected, a temporary loop may occur.

7) STP timers
The following three-time parameters are important for STP calculation:

◯ Forward delay, the period a device waits before state transition.
A link failure triggers a new round of spanning tree calculation and results in changes of the spanning tree. However, as new configuration BPDUs cannot be propagated throughout the network immediately, if the new root port and designated port begin to forward data as soon as they are elected, loops may temporarily occur.

For this reason, the protocol uses a state transition mechanism. Namely, a newly elected root port and the designated ports must go through a period, which is twice the forward delay time, before they transit to the forwarding state. The period allows the new configuration BPDUs to be propagated throughout the entire network.

◯ Hello time, the interval for sending hello packets. Hello packets are used to check link state.
A switch sends hello packets to its neighboring devices at a regular interval (the hello time) to check whether the links are faulty.

◯ Max time, lifetime of the configuration BPDUs stored in a switch. A configuration BPDU that has “expired” is discarded by the switch.

13.2 MSTP Overview

Background of MSTP
Disadvantages of STP and RSTP
STP does not support rapid state transition of ports. A newly elected root port or designated port must wait twice the forward delay time before transiting to the forwarding state, even if it is a port on a point-to-point link or it is an edge port (an edge port refers to a port that directly connects to a user terminal rather than to another device or a shared LAN segment.)

The rapid spanning tree protocol (RSTP) is an optimized version of STP. RSTP allows a newly elected root port or designated port to enter the forwarding state much quicker under certain conditions than in STP. As a result, it takes a shorter time for the network to reach the final topology stability.

RSTP supports rapid convergence. Like STP, it is of the following disadvantages: all bridges in a LAN are on the same spanning tree; redundant links cannot be blocked by VLAN; the packets of all VLANs are forwarded along the same spanning tree.

Features of MSTP

The multiple spanning tree protocol (MSTP) overcomes the shortcomings of STP and RSTP. In addition to support for rapid network convergence, it also allows data flows of different VLANs to be forwarded along their own paths, thus providing a better load sharing mechanism for redundant links.

MSTP features the following:

- MSTP supports mapping VLANs to MST instances by means of a VLAN-to-instance mapping table. MSTP introduces “instance” (integrates multiple VLANs into a set) and can bind multiple VLANs to an instance, thus saving communication overhead and improving resource utilization.
- MSTP divides a switched network into multiple regions, each containing multiple spanning trees that are independent of one another.
- MSTP prunes a ring network into a network with tree topology, preventing packets from being duplicated and forwarded in a network endlessly. Furthermore, it offers multiple redundant paths for forwarding data, and thus achieves load balancing for forwarding VLAN data.
- MSTP is compatible with STP and RSTP.

Basic MSTP Terminologies

MST region

A multiple spanning tree region (MST region) comprises multiple physically-interconnected MSTP-enabled switches and the corresponding network segments connected to these switches. These switches have the same region name, the same VLAN-to-MSTI mapping configuration and the same MSTP revision level.

A switched network can contain multiple MST regions. You can group multiple switches into one MST region by using the corresponding MSTP configuration commands.

MSTI

A multiple spanning tree instance (MSTI) refers to a spanning tree in an MST region.
Multiple spanning trees can be established in one MST region. These spanning trees are independent of each other.

VLAN mapping table

A VLAN mapping table is a property of an MST region. It contains information about how VLANs are mapped to MSTIs.

IST

An internal spanning tree (IST) is a spanning tree in an MST region.
ISTs together with the common spanning tree (CST) form the common and internal spanning tree (CIST) of the entire switched network. An IST is a special MSTI; it is a branch of CIST in the MST region.

CST

A CST is a single spanning tree in a switched network that connects all MST regions in the network. If

you regard each MST region in the network as a switch, then the CST is the spanning tree generated by STP or RSTP running on the "switches".

CIST

A CIST is the spanning tree in a switched network that connects all switches in the network. It comprises the ISTs and the CST.

Region root

A region root is the root of the IST or an MSTI in an MST region. Different spanning trees in an MST region may have different topologies and thus have different region roots.

Common root bridge

The common root bridge is the root of the CIST.

Port role

During MSTP calculation, the following port roles exist: root port, designated port, master port, region boundary port, alternate port, and backup port.

- A root port is used to forward packets to the root.
- A designated port is used to forward packets to a downstream network segment or switch.
- A master port connects an MST region to the common root. The path from the master port to the common root is the shortest path between the MST region and the common root. In the CST, the master port is the root port of the region, which is considered as a node. The master port is a special boundary port. It is a root port in the IST/CIST while a master port in the other MSTIs.
- A region boundary port is located on the boundary of an MST region and is used to connect one MST region to another MST region, an STP-enabled region or an RSTP-enabled region
- An alternate port is a secondary port of a root port or master port and is used for rapid transition. With the root port or master port being blocked, the alternate port becomes the new root port or master port.
- A backup port is the secondary port of a designated port and is used for rapid transition. With the designated port being blocked, the backup port becomes the new designated port fast and begins to forward data seamlessly. When two ports of an MSTP-enabled switch are interconnected, the switch blocks one of the two ports to eliminate the loop that occurs. The blocked port is the backup port.

Port state

In MSTP, a port can be in one of the following three states:

- Forwarding state. Ports in this state can forward user packets and receive/send BPDU packets.
- Learning state. Ports in this state can receive/send BPDU packets.
- Discarding state. Ports in this state can only receive BPDU packets.

Principle of MSTP

MSTP divides a Layer 2 network into multiple MST regions. The CSTs are generated between these MST regions, and multiple spanning trees (also called MSTIs) can be generated in each MST region. As well as RSTP, MSTP uses configuration BPDUs for spanning tree calculation. The only difference is that

the configuration BPDUs for MSTP carry the MSTP configuration information on the switches.

Calculate the CIST

Through comparing configuration BPDUs, the switch of the highest priority in the network is selected as the root of the CIST. In each MST region, an IST is calculated by MSTP. At the same time, MSTP regards each MST region as a switch to calculate the CSTs of the network. The CSTs, together with the ISTs, form the CIST of the network.

Calculate an MSTI

In an MST region, different MSTIs are generated for different VLANs based on the VLAN-to-MSTI mappings. Each spanning tree is calculated independently, in the same way as how STP/RSTP is calculated.

Implement STP algorithm

In the beginning, each switch regards itself as the root, and generates a configuration BPDU for each port on it as a root, with the root path cost being 0, the ID of the designated bridge being that of the switch, and the designated port being itself.

1) Each switch sends out its configuration BPDUs and operates in the following way when receiving a configuration BPDU on one of its ports from another switch:

◯ If the priority of the configuration BPDU is lower than that of the configuration BPDU of the port itself, the switch discards the BPDU and does not change the configuration BPDU of the port.

◯ If the priority of the configuration BPDU is higher than that of the configuration BPDU of the port itself, the switch replaces the configuration BPDU of the port with the received one and compares it with those of other ports on the switch to obtain the one with the highest priority.

2) Configuration BPDUs are compared as follows:

For MSTP, CIST configuration information is generally expressed as follows:

(Root bridge ID, External path cost, Master bridge ID, Internal path cost, Designated bridge ID, ID of sending port, ID of receiving port), so the compared as follows

◯ The smaller the Root bridge ID of the configuration BPDU is, the higher the priority of the configuration BPDU is.

◯ For configuration BPDUs with the same Root bridge IDs, the External path costs are compared.

◯ For configuration BPDUs with both the same Root bridge ID and the same External path costs, Master bridge ID, Internal path cost, Designated bridge ID, ID of sending port, ID of receiving port are compared in turn.

For MSTP, MSTI configuration information is generally expressed as follows:

(Instance bridge ID, Internal path costs, Designated bridge ID, ID of sending port, ID of receiving port), so the compared as follows

◯ The smaller the Instance bridge ID of the configuration BPDU is, the higher the priority of the configuration BPDU is.

- For configuration BPDUs with the same Instance bridge IDs, Internal path costs are compared.
- For configuration BPDUs with both the same Instance bridge ID and the same Internal path costs, Designated bridge ID, ID of sending port, ID of receiving port are compared in turn.

3) A spanning tree is calculated as follows:
- Determining the root bridge

Root bridges are selected by configuration BPDU comparing. The switch with the smallest root ID is chosen as the root bridge.
- Determining the root port

For each switch in a network, the port on which the configuration BPDU with the highest priority is received is chosen as the root port of the switch.
- Determining the designated port

First, the switch calculates a designated port configuration BPDU for each of its ports using the root port configuration BPDU and the root port path cost, with the root ID being replaced with that of the root port configuration BPDU, root path cost being replaced with the sum of the root path cost of the root port configuration BPDU and the path cost of the root port, the ID of the designated bridge being replaced with that of the switch, and the ID of the designated port being replaced with that of the port.

The switch then compares the calculated configuration BPDU with the original configuration BPDU received from the corresponding port on another switch. If the latter takes precedence over the former, the switch blocks the local port and keeps the port's configuration BPDU unchanged, so that the port can only receive configuration messages and cannot forward packets. Otherwise, the switch sets the local port to the designated port, replaces the original configuration BPDU of the port with the calculated one and advertises it regularly.

MSTP Implementation on Switches

MSTP is compatible with both STP and RSTP. That is, MSTP-enabled switches can recognize the protocol packets of STP and RSTP and use them for spanning tree calculation. In addition to the basic MSTP functions, the switches also provide the following functions for users to manage their switches.
- Root bridge hold
- Root bridge backup
- Root guard
- BPDU guard
- Loop guard
- TC-BPDU attack guard
- BPDU packet drop

STP-related Standards

STP-related standards include the following.
- IEEE 802.1D: spanning tree protocol
- IEEE 802.1w: rapid spanning tree protocol
- IEEE 802.1s: multiple spanning tree protocol

13.2.1 Specifying the MST Region Configuration and Enabling MSTP

For two or more switches to be in the same MST region, they must have the same VLAN-to-instance mapping, the same configuration revision number, and the same name.

A region can have one member or multiple members with the same MST configuration; each member must be capable of processing RSTP BPDUs. There is no limit to the number of MST regions in a network, but each region can only support up to 16 spanning-tree instances. You can assign a VLAN to only one spanning-tree instance at a time.

Beginning in privileged EXEC mode, follow these steps to specify the MST region configuration and enable MSTP. This procedure is required.

	Command	**Purpose**
Step 1	**config**	Enter global configuration mode.
Step 2	**spanning-tree**	Enable spanning-tree
Step 3	**spanning-tree mode** {**mstp** | **rstp | stp**}	Configure Spanning tree operating mode. Spanning tree protocol(STP) Rapid spanning tree protocol(RSTP) Multiple spanning tree protocol(MSTP)
Step 4	**show spanning-tree**	Verify your entries.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To return to the default MST region configuration, use the **no spanning-tree** global configuration command.

This example shows how to enable spanning tree on switch.

Switch#
Switch# **configure**
Switch(config)# **spanning-tree**
Switch(config)# **spanning-tree mode rstp**
Switch(config)# **exit**
Switch# **show spanning-tree**

13.2.2 Configuring the Port Priority

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

Beginning in privileged EXEC mode, follow these steps to configure the MSTP port priority of an interface. This procedure is optional.

	Command	Purpose
Step 1	**config**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Specify an interface to configure, and enter interface configuration mode.
Step 3	**spanning-tree mst** *instance-id* **port-priority** *priority*	Configure the port priority for an MST instance.
Step 4	**show spanning-tree interface** *interface-id* **priority**	Verify your entries.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To return the interface to its default setting, use the **no spanning-tree priority** interface configuration command.

13.2.3 Configuring the Path Cost

The MSTP path cost default value is derived from the media speed of an interface. If a loop occurs, the MSTP uses cost when selecting an interface to put in the forwarding state. You can assign lower cost values to interfaces that you want selected first and higher cost values that you want selected last. If all interfaces have the same cost value, the MSTP puts the interface with the lowest interface number in the forwarding state and blocks the other interfaces.

Beginning in privileged EXEC mode, follow these steps to configure the MSTP cost of an interface. This procedure is optional.

	Command	Purpose
Step 1	**config**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Specify an interface to configure, and enter interface configuration mode.
Step 3	**spanning-tree mst** *instance-id* **cost** *cost*	Configure the cost for an MST instance.
Step 4	**show spanning-tree interface** *interface-id*	Verify your entries.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To return the interface to its default setting, use the **no spanning-tree cost** interface configuration command.

13.2.4 Configuring the Switch Priority

You can configure the switch priority and make it more likely that the switch will be chosen as the root switch.

Beginning in privileged EXEC mode, follow these steps to configure the switch priority. This procedure is optional.

	Command	Purpose
Step 1	**config**	Enter global configuration mode.
Step 2	**spanning-tree mst** *instance-id* **priority** *priority*	Configure the switch priority for an MST instance.
Step 3	**show spanning-tree** or **show spanning-tree mst** *mst-id*	Verify your entries.
Step 4	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To return the switch to its default setting, use the **no spanning-tree priority** global configuration command.

13.2.5 Configuring the Hello Time

You can configure the interval between the generation of configuration messages by the root switch by changing the hello time.

Beginning in privileged EXEC mode, follow these steps to configure the hello time for all MST instances. This procedure is optional.

	Command	Purpose
Step 1	**config**	Enter global configuration mode.
Step 2	**spanning-tree mst hello-time** *seconds*	Configure the hello time for all MST instances.
Step 3	**show spanning-tree mst** *mst-id*	Verify your entries.
Step 4	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To return the switch to its default setting, use the **no spanning-tree hello-time** global configuration command.

13.2.6 Configuring the Forwarding-Delay Time

Beginning in privileged EXEC mode, follow these steps to configure the forwarding-delay time for all MST instances. This procedure is optional.

	Command	Purpose
Step 1	**config**	Enter global configuration mode.
Step 2	**spanning-tree mst forward-time** *seconds*	Configure the forward time for all MST instances.

Step 3	**show spanning-tree mst** *mst-id*	Verify your entries.
Step 4	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To return the switch to its default setting, use the **no spanning-tree forward-time** global configuration command.

13.2.7 Configuring the Maximum-Aging Time

Beginning in privileged EXEC mode, follow these steps to configure the maximum-aging time for all MST instances. This procedure is optional.

	Command	**Purpose**
Step 1	**config**	Enter global configuration mode.
Step 2	**spanning-tree maximum-age** *seconds*	Configure the maximum-aging time for all MST instances.
Step 3	**show spanning-tree mst** *mst-id*	Verify your entries.
Step 4	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To return the switch to its default setting, use the **no spanning-tree max-age** global configuration command.

13.2.8 Configuring the Maximum-Hop Count

Beginning in privileged EXEC mode, follow these steps to configure the maximum-hop count for all MST instances. This procedure is optional.

	Command	**Purpose**
Step 1	**configure**	Enter global configuration mode.
Step 2	**spanning-tree max-hops** *hop-count*	Specify the number of hops in a region before the BPDU is discarded, and the information held for a port is aged.
Step 3	**show spanning-tree mst** *mst-id*	Verify your entries.
Step 4	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To return the switch to its default setting, use the **no spanning-tree max-hops** global configuration command.

14 ERPS(G.8032)

Ethernet Ring Protection Switching (ERPS) is a protocol defined by the International Telecommunication Union - Telecommunication Standardization Sector (ITU-T) to eliminate loops at Layer 2. It implements convergence of carrier-class reliability standards, and allows all ERPS-capable devices on a ring network to communicate.

14.1 Introduction to ERPS

This section describes the concepts and functions of ERPS.

Definition

Ethernet Ring Protection Switching (ERPS) is a protocol defined by the International Telecommunication Union - Telecommunication Standardization Sector (ITU-T) to eliminate loops at Layer 2. Because the standard number is ITU-T G.8032/Y1344, ERPS is also called G.8032. ERPS defines Ring Auto Protection Switching (RAPS) Protocol Data Units (PDUs) and protection switching mechanisms.

ERPS has two versions: ERPSv1 released by ITU-T in June 2008 and ERPSv2 released in August 2010. EPRSv2, fully compatible with ERPSv1, provides the following enhanced functions:

- Multi-ring topologies, such as intersecting rings
- RAPS PDU transmission on virtual channels (VCs) and non-virtual-channels (NVCs) in sub-rings
- Forced Switch (FS) and Manual Switch (MS)
- Revertive and non-revertive switching

Purpose

Generally, redundant links are used on an Ethernet switching network such as a ring network to provide link backup and enhance network reliability. The use of redundant links, however, may produce loops, causing broadcast storms and rendering the MAC address table unstable. As a result, communication quality deteriorates, and communication services may even be interrupted. Table 19-1 describes ring network protocols supported by devices.

Table 19-1 Ring network protocols supported by devices

Ring Network Protocol	Advantage	Disadvantage
STP/RSTP/MSTP	• Applies to all Layer 2 networks. • Is a standard IEEE protocol that allows Huawei devices to communicate with non-Huawei devices.	Provides low convergence on a large network, which cannot meet the carrier-class reliability requirement.

Ring Network Protocol	Advantage	Disadvantage
ERPS	• Provides fast convergence and carrier-class reliability. • Is a standard ITU-T protocol that allows Huawei devices to communicate with non-Huawei devices. • Supports single-ring and multi-ring topologies in ERPSv2.	Requires the network topology to be planned in advance. The configuration is complex.

Ethernet networks demand faster protection switching. STP does not meet the requirement for fast convergence. RRPP and SEP are Huawei proprietary ring protocols, which cannot be used for communication between Huawei and non-Huawei devices on a ring network.

ERPS, a standard ITU-T protocol, prevent loops on ring networks. It optimizes detection and performs fast convergence. ERPS allows all ERPS-capable devices on a ring network to communicate.

Benefits

- Prevents broadcast storms and implements fast traffic switchover on a network where there are loops.
- Provides fast convergence and carrier-class reliability.
- Allows all ERPS-capable devices on a ring network to communicate.
-

14.2 Principles

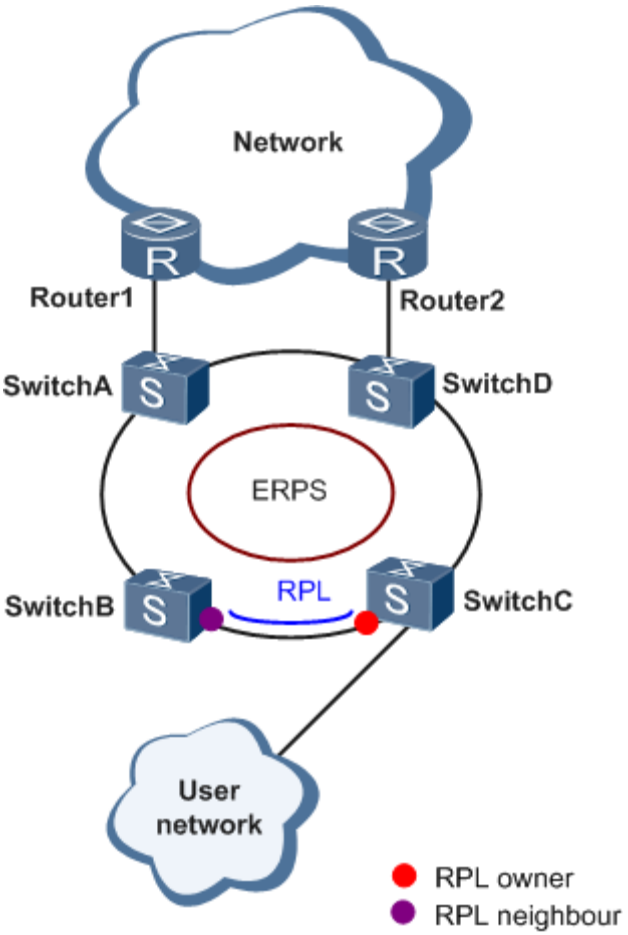
This section describes the implementation of ERPS.

14.2.1 Basic ERPS Concepts

ERPS eliminates loops at the link layer of an Ethernet network. ERPS works for ERPS rings. There are several nodes in an ERPS ring. ERPS blocks the RPL owner port and controls common ports to switch the port status between Forwarding and Discarding and eliminate loops. ERPS uses the control VLAN, data VLAN, and Ethernet Ring Protection (ERP) instance.

On the network shown in Figure 14-1, SwitchA through SwitchD constitute a ring and are dual-homed to the upstream network. This access mode will cause a loop on the entire network. To eliminate redundant links and ensure link connectivity, ERPS is used to prevent loops.

Figure 14-1 ERPS single-ring networking



ERPS can be deployed on the network shown in Figure 14-1.

Port Role

ERPS defines three port roles: RPL owner port, RPL neighbor port (only in ERPSv2), and common port.

- RPL owner port

  An RPL owner port is responsible for blocking traffic over the Ring Protection Link (RPL) to prevent loops. An ERPS ring has only one RPL owner port.

  When the node on which the RPL owner port resides receives an RAPS PDU indicating a link or node fault in an ERPS ring, the node unblocks the RPL owner port. Then the RPL owner port can send and receive traffic to ensure nonstop traffic forwarding.

  The link where the RPL owner port resides is the RPL.

- RPL neighbor port

  An RPL neighbor port is directly connected to an RPL owner port.

  Both the RPL owner port and RPL neighbor ports are blocked in normal situations to prevent loops.

  If an ERPS ring fails, both the RPL owner and neighbor ports are unblocked.

The RPL neighbor port helps reduce the number of FDB entry updates on the device where the RPL neighbor port resides.

- Common port

  Common ports are ring ports other than the RPL owner and neighbor ports.

  A common port monitors the status of the directly connected ERPS link and sends RAPS PDUs to notify the other ports of its link status changes.

Port Status

On an ERPS ring, an ERPS-enabled port has two statuses:

- Forwarding: forwards user traffic and sends and receives RAPS PDUs.
- Discarding: only sends and receives RAPS PDUs.

Control VLAN

A control VLAN is configured in an ERPS ring to transmit RAPS PDUs.

Each ERPS ring must be configured with a control VLAN. After a port is added to an ERPS ring configured with a control VLAN, the port is added to the control VLAN automatically.

Different ERPS rings must use different control VLANs.

Data VLAN

Unlike control VLANs, data VLANs are used to transmit data packets.

ERP Instance

On a Layer 2 device running ERPS, the VLAN in which RAPS PDUs and data packets are transmitted must be mapped to an Ethernet Ring Protection (ERPS) instance so that ERPS forwards or blocks the packets based on configured rules. If the mapping is not configured, the preceding packets may cause broadcast storms on the ring network. As a result, the network becomes unavailable.

Timer

ERPS defines four timers: Guard timer, WTR timer, Holdoff timer, and WTB timer (only in ERPSv2).

- Guard timer

  After a faulty link or node recovers or a clear operation is executed, the device sends RAPS No Request (NR) messages to inform the other nodes of the link or node recovery and starts the Guard timer. Before the Guard timer expires, the device does not process any RAPS (NR) messages to avoid receiving out-of-date RAPS (NR) messages. After the Guard timer expires, if the device still receives an RAPS (NR) message, the local port enters the Forwarding state.

- WTR timer

  If an RPL owner port is unblocked due to a link or node fault, the involved port may not go Up immediately after the link or node recovers. Blocking the RPL owner port may cause network flapping. To prevent this problem, the node where the RPL owner port resides starts the wait to restore (WTR) timer after receiving an RAPS (NR) message. If the node receives an RAPS Signal Fail (SF) message before the timer expires, it terminates the WTR timer. If the node does not receive any RAPS (SF) message before the timer expires, it blocks the RPL owner port when the timer expires and sends an RAPS (no request, root blocked) message. After receiving this RAPS (NR, RB) message, the nodes set their recovered ports on the ring to the Forwarding state.

- Holdoff timer

  On Layer 2 networks running EPRS, there may be different requirements for protection switching. For example, on a network where multi-layer services are provided, after a server fails, users may require a period of time to rectify the server fault so that clients do not detect the fault. You can set the Holdoff timer. If the fault occurs, the fault is not immediately sent to ERPS until the Holdoff timer expires.

14.3 ERPS Configuration example

Configuration Examples The typical application scenarios of ERPS are exemplified based on networking requirements, configuration roadmaps, and data preparation.

14.3.1 Configuring an ERPS single-ring instance

Taking the ERPS single-ring network as an example, this article focuses on how to configure ERPS functions and helps you configure basic ERPS functions.

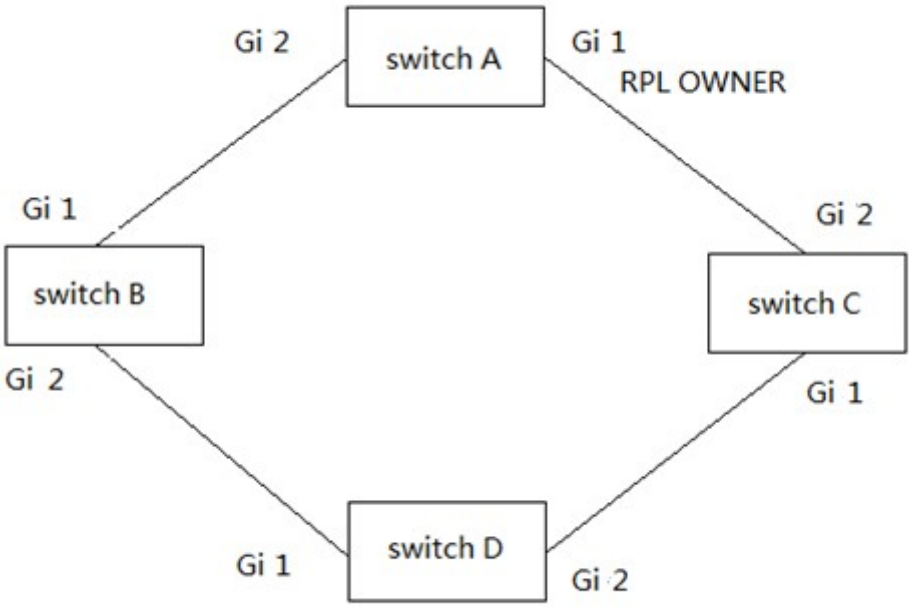
Networking requirements
In order to perform link backup and improve network reliability in an Ethernet switching network, redundant links are usually used. However, the use of redundant links will cause loops on the switching network, resulting in broadcast storms and unstable MAC address tables, and other faults, resulting in poor user communication quality and even communication interruption.

In order to solve the loop problem caused by the use of redundant links, the ERPS protocol can be deployed on the devices forming the ring network. The ERPS protocol is a layer-2 loop-breaking protocol standard defined by ITU-T, and the convergence speed is fast, which can meet the convergence requirements. The speed meets carrier-class reliability requirements.

As shown in Figure 14-2, taking the deployment of a single ERPS ring as an example, SwitchA to SwitchD form a ring network to complete Layer 2 service processing. The switch ring runs the ERPS protocol, providing the ring's

Layer 2 redundancy protection function. Configure ERPS instances on SwitchA to SwitchD. The ERPS ring blocks the Gi 1 port of SwitchA to implement load balancing and provide link backup.

Figure 14-2 ERPS Single Ring Example



Configuration ideas

Use the following ideas to configure an ERPS ring:

1. Configure all ports to be added to the ERPS ring as trunks.
2. Create an ERPS ring, and configure a control VLAN and a protection instance.
3. Add the Layer 2 port to the ERPS ring and configure the port role.
4. Configure the Guard Timer and WTR Timer of the ERPS ring.
5. Configure Layer 2 forwarding on SwitchA to SwitchD.

Configuration procedure

Follow these steps to perform basic ERPS configuration:

	Command	Purpose
Step 1	**configure**	Enter global configuration mode.
Step 2	**erps**	Enable erps
Step 3	**erps control-vlan** *vlan-id*	Configuration control vlan in erps
Step 4	**show erps**	Verify your entries.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

use the **no erps** global configuration command.

14.3.2 Configuring the Port Role

After ERPS is configured, add Layer 2 ports to an ERPS ring and configure port roles so that ERPS can work properly.

You can add a Layer 2 port to an ERPS ring in either of the following ways:

- In the ERPS ring view, add a specified port to the ERPS ring and configure the port role.
- In the interface view, add the current port to the ERPS ring and configure the port role.

Please follow these steps to configure the ERPS port role for the interface

	Command	**Purpose**
Step 1	**configure**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Enter interface configuration mode and the physical interface to be configured.
Step 3	**spanning-tree erps {rpl owner | ring}**	Configure ERP port roles
Step 4	**show erps**	Verify your entries.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Close the ERPS role of the port using the command **no erps rpl owner, no erps ring**

Configure ERPS according to the single-ring example diagram in 14-2.

switch A：

Switch# config

Switch(config)# vlan 200

Switch(config)# interface range GigabitEthernet 1,2

Switch(config-if-range)# switchport mode trunk

Switch(config-if-range)# switchport trunk allowed vlan add 200

Switch(config-if-range)# exit

Switch(config)# erps

Switch(config)# erps control-vlan 200

Switch(config)# interface GigabitEthernet 1

Switch(config-if)# erps rpl owner

Switch(config-if)# exit

Switch(config)# interface GigabitEthernet 2

Switch(config-if)# erps ring

switch B 和 C 和 D：

Switch# config

Switch(config)# vlan 200

Switch(config)# interface range GigabitEthernet 1,2

Switch(config-if-range)# switchport mode trunk

Switch(config-if-range)# switchport trunk allowed vlan add 200

Switch(config-if-range)# exit

Switch(config)# erps

Switch(config)# erps control-vlan 200

Switch(config)# interface GigabitEthernet 1

Switch(config-if)# erps ring

Switch(config-if)# exit

Switch(config)# interface GigabitEthernet 2

Switch(config-if)# erps ring

View configuration parameters for the switch A\B\C\D devices.

switch A：

Switch# sho erps

Status : Enable

Control Vlan : 200

WTR Timer(min) : 5

Guard Timer(ms) : 1000

Holdoff Timer(ms) : 0

RAPS_MEL : 7

Port Port Role Port Status Signal Status

GigabitEthernet1 RPL Owner Discarding Non-failed

GigabitEthernet2 Common Forwarding Non-failed

switch B 和 C 和 D：

Switch# sho erps

Status : Enable

Control Vlan : 200

WTR Timer(min) : 5

Guard Timer(ms) : 1000

Holdoff Timer(ms) : 0

RAPS_MEL : 7

Port	Port Role	Port Status	Signal Status
GigabitEthernet1	Common	Forwarding	Non-failed
GigabitEthernet2	Common	Forwarding	Non-failed