DIGITUS®

GIGABIT MANAGED POE SWITCH

DN-95351 **DN-95352**

User Manual

Directory

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 100 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 100-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 100 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.

When the LAN is connected to dense Home Gateways (HG). Generally, the ex-factory setting of an HG is simple as it uses a fixed VLAN tag to identify the attached service type (data service, IPTV, etc). Thus, precise division and management for users and services can be implemented. And VLAN mapping is then implemented on the access the Switch device. In this way, respective service VLANs are “translated” into the VLANs that comply with the carrier’s deployment. In addition, QinQ is used on the upstream device to identify the campus position. Such uniform configuration implements carriers’ precise PUPSPV (respective users and respective services use their own VLANs) management.

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 are 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 fastethernet 0/6
```

For example, to configure port1-port 6 on a switch, you enter:

```
Switch(config)# interface range fastethernet 0/1-6
```

- 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.

- Slot number — The slot number on the switch. On the modular switches, the slot number is 0.
- Port number — The number of the physical port on the switch. Refer to your switch for the port numbers.

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 Swith

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)

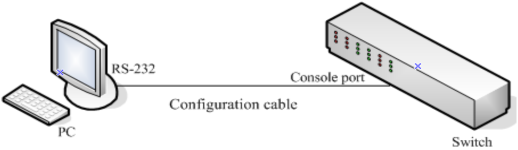
3.2 Logging in through the Console Port

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

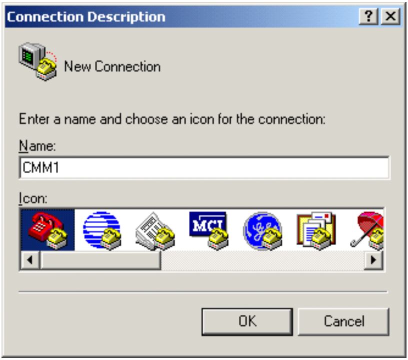
To log into a switch through the Console port, make sure the settings of both the Console port and the user terminal are the same.
Following are the procedures to connect to a switch through the Console port.

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 2000/Windows XP. The following assumes that you are running Windows XP) and perform the configuration shown.

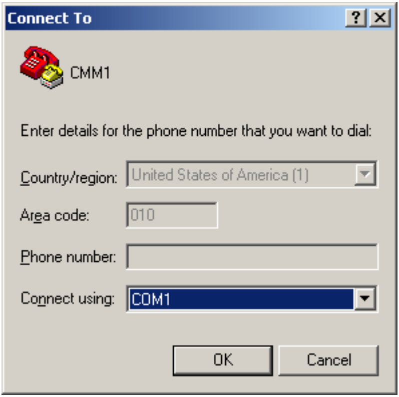
Create a connection



Enter a name and choose an icon for the connection:

Name: CMM1

Specify the port used to establish the connection



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

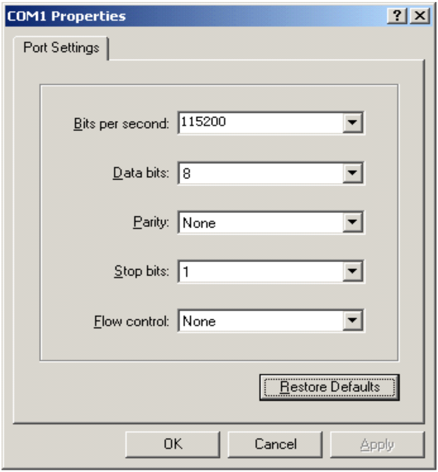
Country/region: United States of America (1)

Area code: 010

Phone number:

Connect using: COM1

Set port parameters



COM1 Properties

Port Settings

Bits per second: 115200

Data bits: 8

Parity: None

Stop bits: 1

Flow control: None

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 Configuring IEEE802.1Q VLANs

4.1 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.

4.2 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.

4.2.1 Configuring an Access mode VLAN

Configuration procedure

Follow these steps to perform basic VLAN interface configuration:

	Command	**Purpose**
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface *interface-id*	Enter the interface to be added to the VLAN.
Step 3	Switchport mode access	Define the VLAN membership mode for the port (Layer 2 access port).
Step 4	switchport access vlan *vlan-id*	Assign the port to a VLAN. Valid VLAN IDs are 1 to 4094.
Step 5	show interfaces	Verify your entries in the

	switchport	Administrative Mode and the Access Mode VLAN fields of the display.
Step 6	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# configure terminal
Enter configuration commands, one per line.
Switch(config)# interface fastethernet 0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 2
Switch(config-if)# exit
Switch(config) # exit
Switch#
```

4.2.2 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 terminal	Enter global configuration mode.
Step 2	interface *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 Access by default.
Step 4	switchport mode hybrid	Define the VLAN membership mode for the port (Layer 2

		hybrid port).
Step 5	switchport hybrid {add | remove} {vlan-untagged|vlan} *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 access vlan *vlan-id*	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 {add | remove} {vlan-tagged|vlan} *vlan-list*	(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# configure terminal
Enter configuration commands, one per line.
Switch(config)# interface fastethernet 0/1
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan add 2
Switch(config-if)# exit
Switch(config) # exit
Switch#
```

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

```
Switch(config)# interface fastethernet 0/1
Switch(config-if)# switchport trunk allowed vlan remove 2
Switch(config-if)# exit
Switch(config) # exit
Switch#
```

4.2.3 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 terminal	Enter global configuration mode.
Step 2	interface *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 Access 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 native-vlan *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 an access port in VLAN 2:

```
Switch# configure terminal
Enter configuration commands, one per line.
```

```
Switch(config)# interface fastethernet 0/1
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan add 2
Switch(config-if)# exit
Switch(config) # exit
Switch#
```

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

```
Switch(config)# interface fastethernet 0/1
Switch(config-if)# switchport trunk allowed vlan remove 2
Switch(config-if)# exit
Switch(config) # exit
Switch#
```

Displaying and Maintaining VLAN

	Command	**Purpose**
Step 1	show vlan	Verify your entries.
Step 2	Show trunk	Verify your entries.
Step 3	show interfaces [vlan *vlan-id*]	Display characteristics for all interfaces or for the specified VLAN configured on the switch.
Step 4	show vlan [id *vlan-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.

5 Protocol-Based VLAN Configuration

5.1 Introduction to Protocol-Based VLAN

In this approach, inbound packets are assigned with different VLAN IDs based on their protocol type and encapsulation format. The protocols that can be used to categorize VLANs include: IP, IPX, and AppleTalk (AT). The encapsulation formats Ethernet II.

A protocol-based VLAN can be defined by a protocol template, which is determined by encapsulation format and protocol type. A port can be associated to multiple protocol templates. An untagged packet (that is, packet carrying no VLAN tag) reaching a port associated with a protocol-based VLAN will be processed as follows.

- If the packet matches a protocol template, the packet will be tagged with the VLAN ID of the protocol-based VLAN defined by the protocol template.
- If the packet matches no protocol template, the packet will be tagged with the default VLAN ID of the port.
- The port processes a tagged packet (that is, a packet carrying a VLAN tag) in the same way as it processes packets of a port-based VLAN.
- If the port is configured to permit the VLAN identified by this VLAN tag, the port forwards the packet.
- If the port is configured to deny the VLAN identified by this VLAN tag, the port discards the packet.

This feature is mainly used to bind the service type with VLAN for ease of management and maintenance.

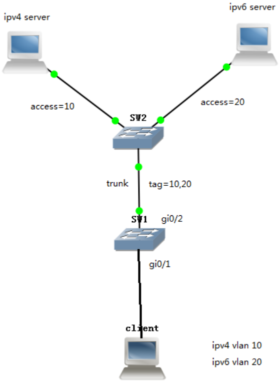
5.2 Configuring a Protocol-Based VLAN

Follow these steps to configure a protocol-based VLAN:

	Command	**Purpose**
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface *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 Access 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	Vlan *vlan-id* protocol-vlan *index-id* {at | etherII | ipv4 | ipv6}	Configure the protocol-VLAN type
Step 7	switchport trunk allowed vlan add *vlan-id*	Assign the port to a VLAN. 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 to join the protocol-VLAN:



When client sends ipv4 protocol packets, the switch will add tag VLAN 10,

When client sends ipv6 protocol packets, the switch will add tag VLAN 20

Configure on the switch of SW1

Step 1 Set gi 0/2 of SW1 to trunk, support vlan 10,20

```
Switch# configure terminal
Enter configuration commands, one per line.
Switch(config)# interface gigabitethernet 0/2
Switch(config-if-gi 0/2)# switchport mode trunk
Switch(config-if-gi 0/2)# switchport trunk allowed vlan add 10
Switch(config-if-gi 0/2)# switchport trunk allowed vlan add 20
```

Step 2 On SW1,set ipv4 to vlan 10,ipv6 to vlan 20

```
Switch(config)# vlan 10 protocol-vlan ipv4
Switch(config)# vlan 10 protocol-vlan ipv6
```

Step 3 On SW1, apply protocol-vlan on incoming port gi0/1

```
Switch(config)# interface gigabitethernet 0/1
Switch(config-if-gi 0/1)# protocol-vlan vlan 10 1
Switch(config-if-gi 0/1)# protocol-vlan vlan 20 1
```

Step 4 Set gi 0/1 of SW1 support vlan 10,20 untagged

```
Switch(config)# interface gigabitethernet 0/1
Switch(config-if-gi 0/1)# switchport mode hybrid
Switch(config-if-gi 0/1)# switchport hybrid add vlan-untagged 10
Switch(config-if-gi 0/1)# switchport hybrid add vlan-untagged 20
Switch(config-if)# exit
Switch(config) # exit
Switch#
```

6 Voice VLAN Configuration

6.1 Introduction to Voice VLAN

A voice VLAN is configured specially for voice traffic. By adding the ports that connect voice devices to the voice VLAN, you can configure quality of service (QOS for short) attributes for the voice traffic, improving transmission priority and ensuring voice quality. A device determines whether a received packet is a voice packet by checking its source MAC address. Packets containing source MAC addresses that comply with the voice device Organizationally Unique Identifier (OUI for short) addresses are regarded as voice traffic, and are forwarded to the voice VLAN.

You can configure the OUI addresses in advance or use the default OUI addresses, which are listed as follows.

Table 6-1 The default OUI addresses of different vendors:

Number	OUI address	Vendors
1	0001-e300-0000	Siemens phone
2	0003-6b00-0000	Cisco phone
3	0004-0d00-0000	Avaya phone
4	0060-b900-0000	Philips/NEC phone
5	00d0-1e00-0000	Pingtel phone
6	00e0-7500-0000	Polycom phone
7	00e0-bb00-0000	3Com phone

6.1.1 Voice VLAN Modes on a Port

There are two voice VLAN modes on a port: automatic and manual (the mode here refers to the way of adding a port to a voice VLAN).

- In automatic mode, the system identifies the source MAC address contained in the protocol packets (untagged packets) sent when the IP phone is powered on and matches it against the OUI addresses. If a match is found, the system will automatically add the port into the Voice VLAN and apply ACL rules and configure the packet precedence. An aging time can be configured for the voice VLAN. The system will remove a port from the voice VLAN if no voice packet is received from it after the aging time. The adding and removing of ports are automatically realized by the system.
- In manual mode, administrators add the IP phone access port to the voice VLAN manually. It then identifies the source MAC

address contained in the packet, matches it against the OUI addresses. If a match is found, the system issues ACL rules and configures the precedence for the packets. In this mode, the operation of adding ports to and removing ports from the voice VLAN are carried out by the administrators.
- Both modes forward tagged packets according to their tags.

6.1.2 Security Mode and Normal Mode for the Voice VLAN

Ports that have the voice VLAN feature enabled can be divided into two modes based on their filtering mechanisms applied to inbound packets.

- Security mode: only voice packets with source OUI MAC addresses can pass through the inbound port (with the voice VLAN feature enabled), other non-voice packets will be discarded, including authentication packets, such as 802.1x authentication packet.
- Normal mode: both voice packets and non-voice packets are allowed to pass through an inbound port (with the voice VLAN feature enabled), the former will abide by the voice VLAN forwarding mechanism whereas the latter normal VLAN forwarding mechanism.

It is recommended that you do not mix voice packets with other types of data in a voice VLAN. If necessary, please ensure that the security mode is disabled.

How an IP Phone Works

IP phones can convert analog voice signals into digital signals to enable them to be transmitted in IP-based networks. Used in conjunction with other voice devices, IP phones can offer large-capacity and low-cost voice communication solutions. As network devices, IP phones need IP addresses to operate properly in a network.

To set an IP address and a voice VLAN for an IP phone manually, just make sure that the voice VLAN ID to be set is consistent with that of the switch and the NCP is reachable to the IP address to be set.

The switches Identify Voice Traffic

The switches determine whether a received packet is a voice packet by checking its source MAC address against an organizationally unique identifier (OUI) list. If a match is found, the packet is considered as a voice packet. Ports receiving packets of this type will be added to the voice VLAN automatically for transmitting voice data.You can configure OUI addresses for voice packets or specify to use the default OUI addresses.

Setting the Voice Traffic Transmission Priority

In order to improve transmission quality of voice traffic, the switch by default re-marks the priority of the traffic in the voice VLAN as follows:

- Set the CoS (802.1p) priority to 6.
- Set the DSCP value to 46.

Configuring Voice VLAN Assignment Mode of a Port

A port can work in automatic voice VLAN assignment mode or manual voice VLAN assignment mode.
You can configure the voice VLAN assignment mode for a port according to data traffic passing through the port.

Processing mode of untagged packets sent by IP voice devices

- Automatic voice VLAN assignment mode. Switch automatically adds a port connecting an IP voice device to the voice VLAN by learning the source MAC address in the untagged packet sent by the IP voice device when it is powered on. The voice VLAN uses the aging mechanism to maintain the number of ports in the voice VLAN. When the aging timer expires, the ports whose OUI addresses are not updated (that is, no voice traffic passes) will be removed from the voice VLAN. In voice VLAN assignment automatic mode, ports can not be added to or removed from a voice VLAN manually.
- Manual voice VLAN assignment mode: In this mode, you need to add a port to a voice VLAN or remove a port from a voice VLAN manually.

Processing mode of tagged packets sent by IP voice devices

Tagged packets from IP voice devices are forwarded based on their tagged VLAN IDs, whether the automatic or manual voice VLAN assignment mode is used.

Support for Voice VLAN on Various Ports

Voice VLAN packets can be forwarded by access ports, trunk ports, and hybrid ports. You can enable a trunk or hybrid port belonging to other VLANs to forward voice and service packets simultaneously by enabling the voice VLAN.
IP phones acquiring IP address and voice VLAN through manual configuration can forward only tagged traffic, so the matching relationship is relatively simple.

6.2 Configuring Voice VLAN

6.2.1 Configuration Prerequisites

- Create the corresponding VLAN before configuring the voice VLAN;
- As a default VLAN, VLAN 1 does not need to be created. However, it cannot be enabled with the voice VLAN feature.

	Command	**Purpose**
Step 1	configure terminal	Enter global configuration mode.
Step 2	voice-vlan	Enable Voice VLAN.
Step 3	voice-vlan {age *age-time* | id *vlan-id* | oui *oui-value* prefix *mask-value* | remark { cos | dscp } }	Configure Voice VLAN parameter.
Step 4	interface *interface-id*	Specify the port to configure, and enter interface configuration mode.
Step 5	voice-vlan	Enable Voice VLAN on interface.
Step 6	voice-vlan { age-dev-manual | mode {auto | munual } | security }	Configure Voice VLAN parameter of interface.
Step 7	end	Return to privileged EXEC mode.

Step 8	show voice-vlan	Verify your entries.
Step 9	show voice-vlan { dev | mode | oui | state }	Verify your entries.
Step 10	copy running-config startup-config	(Optional) Save your entries in the configuration file.

This example shows how to configure automatic voice VLAN on port:

```
Switch# configure terminal
Enter configuration commands, one per line.
Switch(config)# voice-vlan
Switch(config)# voice-vlan id 100
Switch(config)# interface fastethernet 0/2
Switch(config-if-fa 0/2)# switch mode trunk
Switch(config-if fa 0/2)# voice-vlan mode auto
Switch(config-if fa 0/2)# voice-vlan
Switch(config-if-fa 0/2)# exit
Switch(config)# voice-vlan oui 0001.e300.0000 prefix ffff.ff00.0000
Switch(config) # exit
Switch# show voice-vlan
Switch# show voice-vlan state
```

7 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.

7.1 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 terminal	Enter global configuration mode.
Step 2	interface vlan *vlan-id*	Enter interface configuration mode, and enter the VLAN to which the IP information is assigned. The range is 1 to 4094.
Step 3	ip address *ip-address subnet-mask*	Enter the IP address and subnet mask.
Step 4	exit	Return to global configuration mode.
Step 5	show interfaces vlan *vlan-id*	Verify the configured IP address.
Step 6	show ip interface brief	Verify the IP configuration information of interface.
Step 7	copy running-config startup-config	(Optional) Save your entries in the configuration file.

The switch vlan 1 interface default IP address is **192.168.2.11.**

This example shows how to configure an interface as a VLAN interface port and to assign it an IP address:

```
Switch# configure terminal
Enter configuration commands, one per line.
Switch(config)# interface vlan 2
Switch(config-if)# ip address 192.20.135.21/24
Switch(config-if)# no shutdown
Switch(config-if)# exit
Switch(config) # exit
Switch#
```

To remove the switch IP address, use the no ip address interface configuration command. If you are removing the address through a Telnet session, your connection to the switch will be lost.

7.2 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 interface vlan privileged EXEC command for the interface:

```
Switch# show interface vlan 1
Interface vlan1
  Hardware is Ethernet, address is 0810.0a3b.2be9
  index 3 metric 1 mtu 1500    <UP,BROADCAST,RUNNING,MULTICAST>
  VRF Binding: Not bound
  inet 192.168.2.11/24 broadcast 192.168.2.255
    input packets 3901932, bytes 183463870, dropped 0, multicast packets 0
    input errors 0, length 0, overrun 0, CRC 0, frame 0, fifo 0, missed 0
    output packets 180800, bytes 10925379, dropped 0
    output errors 0, aborted 0, carrier 0, fifo 0, heartbeat 0, window 0
    collisions 0
```

8 DoS Defend

8.1 Introduction to DoS

DoS (Denial of Service) Attack is to occupy the network bandwidth maliciously by the network attackers or the evil programs sending a lot of service requests to the Host, which incurs an abnormal service or even breakdown of the network.

With DoS Defend function enabled, the switch can analyze the specific fields of the IP packets and distinguish the malicious DoS attack packets. Upon detecting the packets, the switch will discard the illegal packets directly and limit the transmission rate of the legal packets if the over legal packets may incur a breakdown of the network. The switch can defend several types of DoS attack listed in the following table.

DoS Attack Type	**Description**
Land Attack	The attacker sends a specific fake SYN packet to the destination Host. Since both the source IP address and the destination IP address of the SYN packet are set to be the IP address of the Host, the Host will be trapped in an endless circle for building the initial connection. The performance of the network will be reduced extremely.
Scan SYNFIN	The attacker sends the packet with its SYN field and the FIN field set to 1. The SYN field is used to request initial connection whereas the FIN field is used to request disconnection. Therefore, the packet of this type is illegal. The switch can defend this type of illegal packet.
Xmascan	The attacker sends the illegal packet with its TCP index, FIN, URG and PSH field set to 1.
NULL Scan Attack	The attacker sends the illegal packet with its TCP index and all the control fields set to 0. During the TCP connection and data transmission, the packets with all the control fields set to 0 are considered as the illegal packets.
SYN sPort less	The attacker sends the illegal packet with its TCP SYN field

1024	set to 1 and source port less than 1024.
Smurf Attack	By pretending to be a Host, the attacker broadcasts request packets for ICMP response in the LAN. When receiving the request packet, all the Hosts in the LAN will respond and send the reply packets to the actual Host, which will causes this Host to be attacked.
Blat Attack	The attacker sends the illegal packet with its source port and destination port on Layer 4 the same and its URG field set to 1. Similar to the Land Attack, the system performance of the attacked Host is reduced since the Host circularly attempts to build a connection with the attacker.
Ping Flooding	The attacker floods the destination system with Ping broadcast storm packets to forbid the system to respond to the legal communication.
SYN/SYN-ACK Flooding	The attacker uses a fake IP address to send TCP request packets to the Server. Upon receiving the request packets, the Server responds with SYN-ACK packets. Since the IP address is fake, no response will be returned. The Server will keep on sending SYN-ACK packets. If the attacker sends overflowing fake request packets, the network resource will be occupied maliciously and the requests of the legal clients will be denied.
winNuke Attack	Since the Operation System with bugs cannot correctly process the URG (Urgent Pointer) of TCP packets, the attacker sends this type of packets to the TCP port139 (NetBIOS) of the Host with the Operation System bugs, which will cause the Host with a blue screen.
Ping Of Death	ICMP ECHO Request Packet whose sum of "Fragment Offset" and "Total Length" fields in the IP header is greater than 65535 may cause Ping of Death attack. As the

	maximum packet length of an IPv4 packet including the IP header is 65,535 bytes, many computer systems could not properly handle this malformed or malicious ICMP ECHO Request Packet. Thus, the hosts may break down or reboot automatically when receive this kind of packet.

8.2 DoS Defend Configuration

The ip dos-prevent command is used to enable the DoS defend function globally. To disable the DoS defend function, please use no ip dos-prevent command.

DoS attack-prevent

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	dos attack-prevent	Enable DoS-defend
Step 3	dos attack-prevent {daeqsa-deny | icmp-frag-pkts-deny | icmpv4-ping-max-check | land-deny | nullscan-deny | pod-deny | smurf-deny | syn-sportl1024-deny | synfin-deny | synrst-deny | tcp-frag-off-min-check | tcpblat-deny | tcphdr-min-check | udpblat-deny | xma-deny | -deny }	Enter the DoS-attack type
Step 4	interface *interface-id*	Specify the port to configure, and enter interface configuration mode.
Step 5	dos	Enable DoS-defend function on interface.
Step 6	end	Return to privileged EXEC mode.
Step 7	show dos	Verify the configured DoS-defend
Step 8	show dos interface	Verify the DoS-defend information of interface.
Step 9	copy running-config startup-config	(Optional) Save your entries in the configuration file.

This example shows how to configure daeqsa-deny type of DoS attack-prevent:

```
Switch# configure terminal
Enter configuration commands, one per line.
Switch(config)# dos attack-prevent daeqsa-deny
Switch(config)# interface fastethernet 0/2
Switch(config-if)# dos
Switch(config-if) # end
Switch# show dos
Switch# show dos interface
```

9 GVRP Configuration

9.1 Introduction to GVRP

GARP VLAN registration protocol (GVRP) is an implementation of generic attribute registration protocol(GARP). GARP is introduced as follows.

GARP

The generic attribute registration protocol (GARP), provides a mechanism that allows participants in a GARP application to distribute, propagate, and register with other participants in a bridged LAN the attributes specific to the GARP application, such as the VLAN or multicast attribute.
GARP itself does not exist on a device as an entity. GARP-compliant application entities are called GARP applications. One example is GVRP. When a GARP application entity is present on a port on your device, this port is regarded a GARP application entity.

Operating mechanism of GARP

Through the mechanism of GARP, the configuration information on a GARP member will be propagated within the whole LAN. A GARP member can be a terminal workstation or a bridge; it instructs other GARP members to register/deregister its attribute information by declaration/recant, and register/deregister other GARP member's attribute information according to other member's

declaration/recant. When a port receives an attribute declaration, the port will register this attribute. When a port receives an attribute recant, the port will deregister this attribute.
The protocol packets of GARP entities use specific multicast MAC addresses as their destination MAC addresses. When receiving these packets, the switch distinguishes them by their destination MAC addresses and delivers them to different GARP application (for example, GVRP) for further processing.

GVRP

As an implementation of GARP, GARP VLAN registration protocol (GVRP) maintains dynamic VLAN registration information and propagates the information to the other switches through GARP. With GVRP enabled on a device, the VLAN registration information received by the device from other devices is used to dynamically update the local VLAN registration information, including the information about the VLAN members, the ports through which the VLAN members can be reached, and so on. The device also propagates the local VLAN registration information to other devices so that all the devices in the same LAN can have the same VLAN information. VLAN registration information propagated by GVRP includes static VLAN registration information, which is manually configured locally on each device, and dynamic VLAN registration information, which is received from other devices.

Protocol Specifications

GVRP is defined in IEEE 802.1Q standard.

9.2 GVRP Configuration

Configuration Prerequisite

The port on which GVRP will be enabled must be set to a trunk port.

	Command	**Purpose**
Step 1	configure terminal	Enter global configuration mode.

Step 2	interface *interface-id*	Specify the port to configure, and enter interface configuration mode.
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 Access by default.
Step 4	switchport mode trunk	Define the VLAN membership mode for the port (Layer 2 trunk port).
Step 5	gvrp application	Enable gvrp application on port.
Step 6	gvrp registration {fixed | forbidden | qinq | normal }	Configure gvrp registration mode.
Step 7	show gvrp	Verify your entries.
Step 8	Show vlan detail	Verify your entries.
Step 9	copy running-config startup-config	(Optional) Save your entries in the configuration file.

This example shows how to configure gvrp application on port:
Switch# configure terminal
Enter configuration commands, one per line.

```
Switch# configure terminal
Enter configuration commands, one per line.
Switch(config)# dos attack-prevent daeqsa-deny
Switch(config)# interface fastethernet 0/2
Switch(config-if)# dos
Switch(config-if) # end
Switch# show dos
Switch# show dos interface
```

10 MAC Address Table Management

10.1 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, the 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.

10.2 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 terminal	Enter global configuration mode.
Step 2	interface *interface-id*	Specify the port to configure, and enter interface configuration mode.
Step 3	mac-address-table {aging-time | filter | 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 terminal	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 5.

```
Switch# configure terminal
Enter configuration commands, one per line.
Switch(config)# mac-address-table static 0000.2222.3333 vlan 1 interface fastethernet 0/5
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 terminal	Enter global configuration mode.

Step 2	mac-address-table filter {*mac-address* | destination *mac-address*} vlan *vlan-id* interface *interface-id*	Configure balckhole 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 port 1.

```
Switch# configure terminal
Enter configuration commands, one per line.
Switch(config)# mac-address-table filter 0000.2222.1111 vlan 1 interface fastethernet 0/1
Switch(config)# exit
Switch# show mac-address-table
Switch# show mac-address-table filter
```

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 terminal	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# configure terminal
Enter configuration commands, one per line.
Switch(config)# mac-address-table aging-time 60
Switch(config)# exit
Switch# show mac-address-table aging-time
```

Setting the Maximum Number of MAC Addresses a Port Can Learn

The MAC address learning mechanism enables an Ethernet switch to acquire the MAC addresses of the network devices on the segment connected to the ports of the switch. By searching the MAC address table, the switch directly forwards the packets destined for these MAC addresses through the hardware, improving the forwarding efficiency. A MAC address table too big in size may prolong the time for searching MAC address entries, thus decreasing the forwarding performance of the switch.

By setting the maximum number of MAC addresses that can be learned from individual ports, the administrator can control the number of the MAC address entries the MAC address table can dynamically maintain. When the number of the MAC address entries learnt from a port reaches the set value, the port stops learning MAC addresses.

Set the maximum number of MAC addresses a port can learn:

	Command	**Purpose**
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface *interface-id*	Specify the port to configure, and enter interface configuration mode.
Step 3	mac dynamic-mac limit *number*	Configuring the MAC learn number.
Step 4	show mac-address-table dynamic limit	Verify your entries.
Step 5	copy running-config startup-config	(Optional) Save your entries in the configuration file.

Follow these steps to configure the maximum number of mac address learn of port 1.

```
Switch# configure terminal
Enter configuration commands, one per line.
Switch(config)# interface fastethernet 0/1
Switch(config-if)# mac dynamic-mac limit 50
Switch(config-if)# exit
Switch(config)# exit
Switch# show mac-address-table dynamic limit
```

Disabling MAC Address learning for port

You can disable a switch from learning MAC addresses in specific ports to improve stability and security for the users belong to these ports and prevent unauthorized accesses.

Disable MAC address learning for a port

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface *interface-id*	Specify the port to configure, and enter interface configuration mode.
Step 3	switchport port-security	Configuring MAC address learning is disable.
Step 4	show port-security	Verify your entries.
Step 5	copy running-config startup-config	(Optional) Save your entries in the configuration file.

Follow these steps to disable the mac address learn of port 1.

```
Switch# configure terminal
Enter configuration commands, one per line.
Switch(config)# interface fastethernet 0/1
Switch(config-if)# switchport port-security
Switch(config-if)# exit
Switch(config)# exit
Switch# show port-security
```

Assigning MAC Addresses for system

You are allowed to assign MAC addresses to the switch system.

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 3	system mac *MAC-address*	Configuring system MAC address
Step 4	show system mac	Verify your entries.
Step 5	copy running-config startup-config	(Optional) Save your entries in the configuration file.

Follow these steps to configure the system MAC address:

```
Switch# configure terminal
Enter configuration commands, one per line.
Switch(config)# system mac 0000.2222.3333
Switch(config)# exit
Switch# show system mac
```

Displaying MAC Address Table Information

switch#show mac-address-table ?

address	Address keyword
aging-time	Set MAC address table entry maximum age
automatic-learning	automatic learning status
count	Count keyword
dynamic	Dynamic entry type
filter	Create MAC filter entry
interface	Interface keyword
static	Static entry type
vlan	VLAN keyword

Command	Purpose
show mac-address-table	Verify the MAC address table entries.
show mac-address-table address *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 automatic-learning	Verify the MAC address table entries.
show mac-address-table count	Verify your entries.
show mac-address-table dynamic { address | interface | limit | vlan }	Verify the MAC address table entries.
show mac-address-table filter	Verify the blackhole MAC address entry.
show mac-address-table interface {fastethernet | gigabitethernet | port-channel }	Verify the MAC address table entries in interface.
show mac-address-table static {address | interface | vlan }	Verify your entries.
show mac-address-table vlan *vlan-id*	Verify the MAC address table entries in VLAN.

11 Port Basic Configuration

11.1 Ethernet Port Configuration

Initially Configuring a Port

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface *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 autonegotiates 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 *interface-id*	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# configure terminal
Enter configuration commands, one per line.
Switch(config)# interface fastethernet 0/3
Switch(config-if)# speed 10
Switch(config-if)# duplex half
Switch(config-if)# exit
Switch(config)# exit
Switch# show interface
```

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 terminal	Enter global configuration mode.
Step 2	interface *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 *interface-id*	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# configure terminal
Enter configuration commands, one per line.
Switch(config)# interface gigabitethernet 0/1
Switch(config-if)# flowcontrol
Switch(config-if)# exit
Switch(config)# exit
Switch# show interface
```

11.2 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 terminal	Enter global configuration mode.
Step 2	interface *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# configure terminal
Enter configuration commands, one per line.
Switch(config)# interface fastethernet 0/4
Switch(config-if)# description Marketing
Switch(config-if)# exit
Switch(config)# exit
Switch# show port-description
```

11.3 Loopback Detection

Configuring Loopback Detection for an Ethernet Port

Loopback detection is used to monitor if a port of a switch is looped back. After you enable loopback detection on Ethernet ports, the switch can monitor if an external loopback occurs on them. If there is a loopback port found, the switch will deal with the loopback port according to your configuration.

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	loop-detection	Enable loopback detection globally
Step 3	Loop-detection { block-threshold | hellotime}	Set the interval for performing port loopback detection
Step 4	show port-detection	Verify your entry.
Step 5	copy running-config startup-config	(Optional) Save your entries in the configuration file.

Configuring Loopback Detection for Ethernet Port(s)

To enable loopback detection on a specific port, you must use the loop-detection command in both system view and the specific port view. After you use the no loop-detection command in system view, loopback detection will be disabled on all ports.

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface *interface-id*	Enter interface configuration mode and the physical interface to be configured.

Step 3	Loop-detection { always | close | interval}	Enable the loopback port shutdown function mode.
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 loop-detection configuration command to disable loop-detection function.

This example shows how to turn on loop-detection on a port to display the results:

```
Switch# configure terminal
Enter configuration commands, one per line.
Switch(config)# loop-detection
Switch(config)# interface gigabitethernet 0/1
Switch(config-if)# loop-detection interval
Switch(config-if)# exit
Switch(config)# exit
Switch# show loop-detection
```

11.4 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 terminal	Enter global configuration mode.
Step 2	interface *interface-id*	Specify the port to configure, and enter interface configuration mode.
Step 3	storm-control {broadcast | multicast | unicast | level }	Configure broadcast, multicast, or unicast storm control.
Step 4	show storm-control [interface] [{broadcast | multicast | unicast}]	Verify your entries.
Step 5	copy running-config startup-config	(Optional) Save your entries in the configuration file.

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

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

Switch# configure terminal

Enter configuration commands, one per line.

```
Switch# configure terminal
Enter configuration commands, one per line.
Switch(config)# interface gigabitethernet 0/1
Switch(config-if)# storm-control level 100
Switch(config-if)# storm-control broadcast
Switch(config-if)# storm-control multicast
Switch(config-if)# storm-control unicast
Switch(config-if)# exit
Switch(config)# exit
Switch# show storm-control
```

11.5 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 terminal	Enter global configuration mode.
Step 2	interface *interface-id*	Specify the port to configure, and enter interface configuration mode.
Step 3	rate-limit { egress | ingress }	Configure rate limit of a port.
Step 4	show interface rate-limit	Verify your entries.
Step 5	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 terminal
Enter configuration commands, one per line.
Switch(config)# interface gigabitethernet 0/1
Switch(config-if)# rate-limit ingress 1000
Switch(config-if)# rate-limit egress 64
Switch(config-if)# exit
Switch(config)# exit
Switch# show interface rate-limit
```

12 Configuring EtherChannels

12.1 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 de-aggregation. 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.

12.2 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.

12.2.1 Configuring Layer 2 EtherChannels

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface *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 3	channel-group *channel-group-number* mode { on | active }	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 4	Show etherchannel { detail | lacp | port | port-channel | summary}	Verify your entries.
Step 5	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 0/1 and gigabitethernet 0/2 interfaces to static channel-group 1 and display the results:

```
Switch# configure terminal
Enter configuration commands, one per line.
Switch(config)# interface gigabitethernet 0/1
Switch(config-if)# channel-group 1 mode on
Switch(config-if)# exit
Switch(config)# interface gigabitethernet 0/2
Switch(config-if)# channel-group 1 mode on
Switch(config-if)# exit
Switch(config)# exit
Switch# show etherchannel
```

12.2.2 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 terminal	Enter global configuration mode.
Step 2	channel-protocol lacp	Enable LACP protocol.
Step 3	lacp system-priority *priority-value*	Select the LACP port priority value. For priority-value, the range is 1 to 65535. By default, the priority value is 32768. The lower the range, the more likely that the interface will be used for LACP transmission.
Step 4	interface *interface-id*	Specify the interface for transmission, and enter interface configuration mode.
Step 5	channel-group *channel-group-number* mode { on | active }	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 6	show etherchannel { detail | lacp | port | port-channel | summary}	Verify your entries.
Step 7	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 0/1 and gigabitethernet 0/2 interfaces to LACP channel-group 1 and display the results:

```
Switch# configure terminal
Enter configuration commands, one per line.
Switch(config)# channel-protocol lacp
Switch(config)# interface gigabitethernet 0/1
Switch(config-if)# channel-group 1 mode active
Switch(config-if)# exit
Switch(config)# interface gigabitethernet 0/2
Switch(config-if)# channel-group 1 mode active
Switch(config-if)# exit
Switch(config)# exit
Switch# show etherchannel
Switch# show etherchannel detail
Switch# show etherchannel lacp
Switch# show etherchannel port
Switch# show etherchannel port-channel
Switch# show etherchannel summary
```

13 Port Isolation

13.1 Port Isolation Overview

Through the port isolation feature, you can add the ports to be controlled into an isolation group to isolate the Layer 2 and Layer 3 data between each port in the isolation group. Thus, you can construct your network in a more flexible way and improve your network security.Currently, you can create 10 isolation group on the switch. The number of Ethernet ports in an isolation group is not limited.

13.2 Port Isolation Configuration

You can perform the following operations to add an Ethernet ports to an isolation group, thus isolating Layer 2 and Layer 3 data among the ports in the isolation group.

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	port-isolation { group {*group-number*} { *group-name* } }	Enable port isolation function and create isolation group.
Step 3	interface *interface-id*	Specify the port to configure, and enter interface configuration mode.
Step 4	port-isolation allowed *group-number*	Add the Ethernet port to the isolation group
Step 5	show port-isolation { group }	Verify your entries.
Step 6	copy running-config startup-config	(Optional) Save your entries in the configuration file.

Use the no port-isolation allowed configuration command to delete isolation function of the port.

This example shows how to turn on port isolation function on fastethernet 0/1 and fastethernet 0/2 interface to display the results:

```
Switch# configure terminal
Enter configuration commands, one per line.
Switch(config)# port-isolation
Switch(config)# port-isolation group 1 name market
Switch(config)# interface fastethernet 0/1
Switch(config-if)# port-isolation allowed 1
Switch(config-if)# exit
Switch(config)# interface fastethernet 0/2
Switch(config-if)# port-isolation allowed 1
Switch(config-if)# exit
Switch(config)# exit
Switch# show port-isolation
Switch# show port-isolation group
```

14 UDLD Configuration

This chapter describes how to configure the UniDirectional Link Detection (UDLD) protocol on your switch.

14.1 Understanding UDLD

UDLD is a Layer 2 protocol that enables devices connected through fiber-optic or twisted-pair Ethernet cables to monitor the physical configuration of the cables and detect when a unidirectional link exists.

All connected devices must support UDLD for the protocol to successfully identify and disable unidirectional links. When UDLD detects a unidirectional link, it administratively shuts down the affected port and alerts you. Unidirectional links can cause a variety of problems, including spanning-tree topology loops.

14.2 Modes of Operation

UDLD supports two modes of operation: normal (the default) and aggressive. In normal mode, UDLD can detect unidirectional links due to misconnected interfaces on fiber-optic connections. In aggressive mode, UDLD can also detect unidirectional links due to one-way traffic on fiber-optic and twisted-pair links and to misconnected interfaces on fiber-optic links.

In normal and aggressive modes, UDLD works with the Layer 1 mechanisms to determine the physical status of a link. At Layer 1, autonegotiation takes care of physical signaling and fault detection. UDLD performs tasks that autonegotiation cannot perform, such as detecting the identities of neighbors and shutting down misconnected interfaces. When you enable both autonegotiation and UDLD, the Layer 1 and Layer 2 detections work together to prevent physical and logical unidirectional connections and the malfunctioning of other protocols.

A unidirectional link occurs whenever traffic sent by a local device is received by its neighbor but traffic from the neighbor is not received by the local device.

In normal mode, UDLD detects a unidirectional link when fiber strands in a fiber-optic interface are misconnected and the Layer 1 mechanisms do not detect this misconnection. If the interfaces are connected correctly but the traffic is one way, UDLD does not detect the unidirectional link because the Layer 1 mechanism, which is supposed to detect this condition, does not do so. In case, the logical link is considered undetermined, and UDLD does not disable the interface.

When UDLD is in normal mode, if one of the fiber strands in a pair is disconnected and autonegotiation is active, the link does not stay up because the Layer 1 mechanisms did not detect a physical problem with the link. In this case, UDLD does not take any action, and the logical link is considered undetermined.

In aggressive mode, UDLD detects a unidirectional link by using the previous detection methods. UDLD
in aggressive mode can also detect a unidirectional link on a point-to-point link on which no failure
between the two devices is allowed. It can also detect a unidirectional link when one of these problems
exists:

- On fiber-optic or twisted-pair links, one of the interfaces cannot send or receive traffic.
- On fiber-optic or twisted-pair links, one of the interfaces is down while the other is up.
- One of the fiber strands in the cable is disconnected.

In these cases, UDLD shuts down the affected interface.

In a point-to-point link, UDLD hello packets can be considered as a heart beat whose presence guarantees the health of the link. Conversely, the loss of the heart beat means that the link must be shut down if it is not possible to re-establish a bidirectional link.

If both fiber strands in a cable are working normally from a Layer 1 perspective, UDLD in aggressive mode determines whether those fiber strands are connected correctly and whether traffic is flowing bidirectionally between the correct neighbors. This check cannot be performed by autonegotiation because autonegotiation operates at Layer 1.

14.3 UDLD Configuration

Performing Basic UDLD Configuration

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	udld { message { *number* } | interval-time { *number* } }	Set the interval of sending UDLD packets and the aging timer.
Step 3	interface *interface-id*	Specify the port to configure, and enter interface configuration mode.
Step 4	udld port [aggressive]	Enable UDLD function.
Step 5	show udld *interface-id*	Verify your entries.
Step 6	copy running-config startup-config	(Optional) Save your entries in the configuration file.

Use the no udld port configuration command to disable udld function of the port.

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

```
Switch# configure terminal
Enter configuration commands, one per line.
Switch(config)# interface gigabitethernet 0/1
Switch(config-if)# udld port
Switch(config-if)# exit
Switch(config)# exit
Switch# show udld
```

15 Configuring SPAN and RSPAN

This chapter describes how to configure Switched Port Analyzer (SPAN) and Remote SPAN (RSPAN) on the switch.

15.1 Understanding SPAN

You can analyze network traffic passing through ports by using SPAN to send a copy of the traffic to another port on the switch that has been connected to a SwitchProbe device or other Remote Monitoring (RMON) probe or security device. SPAN 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.

SPAN Session

A local SPAN 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.

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

You can configure SPAN sessions on disabled ports; however, a SPAN 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 SPAN session.

A SPAN 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 SPAN session or RSPAN 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 ort
Each local SPAN 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 SPAN source. The port is removed from the group while it is configured as a SPAN 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.

Reflector Port
The reflector port is the mechanism that copies packets onto an RSPAN VLAN. The reflector port forwards only the traffic from the RSPAN source session with which it is affiliated. Any device connected to a port set as a reflector port loses connectivity until the RSPAN source session is disabled.
The reflector port has these characteristics:

- It is a port set to loopback.
- It cannot be an EtherChannel group, it does not trunk, and it cannot do protocol filtering.
- It can be a physical port that is assigned to an EtherChannel group, even if the EtherChannel group is specified as a SPAN source. The port is removed from the group while it is configured as a reflector port.
- A port used as a reflector port cannot be a SPAN source or destination port, nor can a port be a reflector port for more than one session at a time.
- It is invisible to all VLANs.
- The native VLAN for looped-back traffic on a reflector port is the

RSPAN VLAN.

- The reflector port loops back untagged traffic to the switch. The traffic is then placed on the RSPAN VLAN and flooded to any trunk ports that carry the RSPAN VLAN.
- Spanning tree is automatically disabled on a reflector port.

If the bandwidth of the reflector port is not sufficient for the traffic volume from the corresponding source ports and VLANs, the excess packets are dropped. A 10/100 port reflects at 100 Mbps. A Gigabit port reflects at 1 Gbps.

15.2 Configuration SPAN and RSPAN

15.2.2 Configuring SPAN

Beginning in privileged EXEC mode, follow these steps to create a SPAN session and specify the source (monitored) and destination (monitoring) ports:

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

Use the no monitor session configuration command to disable the SPAN.

Use the no monitor session source configuration command to delete the source port of SPAN.

Use the no monitor session destination configuration command to delete the destination port of SPAN.

This example shows how to set up a SPAN session, for monitoring source port traffic to a destination port. Bidirectional traffic is mirrored from source port 1 to destination port 8.

```
Switch# configure terminal
Enter configuration commands, one per line.
Switch(config)# interface gigabitethernet 0/1
Switch(config-if)# udld port
Switch(config-if)# exit
Switch(config)# exit
Switch# show udl
```

15.2.2 Configuring RSPAN

First create an RSPAN VLAN that does not exist for the RSPAN session in any of the switches that will participate in RSPAN. With VTP enabled in the network, you can create the RSPAN VLAN in one switch, and VTP propagates it to the other switches in the VTP domain for VLAN-IDs that are lower than 4094.

After creating the RSPAN VLAN, begin in privileged EXEC mode, and follow these steps to start an RSPAN source session and to specify the source (monitored) ports and the destination RSPAN VLAN.

	Command	**Purpose**
Step 1	configure terminal	Enter global configuration mode.
Step 2	monitor session source { interface *interface-id* [| both | rx | tx] | remote *vlan-id}*	Specify the RSPAN session and the source port (monitored port) and remote VLAN.
Step 3	monitor session destination { interface *interface-id* | remote *vlan-id* }	Specify the RSPAN session the destination port (monitoring port) and remote VLAN.
Step 4	monitor session reflector-port *interface-id*	Specify the RSPAN session the reflector port.
Step 5	show monitor	Verify your entries.
Step 6	copy running-config startup-config	(Optional) Save your entries in the configuration file.

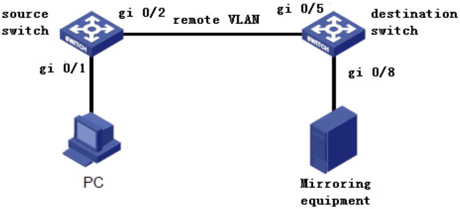
This example shows how to clear any existing RSPAN configuration for session, configure RSPAN session to monitor multiple source interfaces, and configure the destination RSPAN VLAN and the reflector-port.

```
Switch# configure terminal
```

```
Enter configuration commands, one per line.
Switch(config)# interface gigabitethernet 0/1
Switch(config-if)# udld port
Switch(config-if)# exit
Switch(config)# exit
Switch# show udld
```

15.2.3 Example for Configuring RSPAN

This example shows how to configure RSPAN session to monitor traffic received on port 1, and send traffic to destination remote VLAN 902 with port 2 as the reflector port.



Source switch:

```
Switch# configure terminal
Enter configuration commands, one per line.
Switch(config)#monitor session source interface gigabitethernet 0/1 rx
Switch(config)#monitor session destination remote vlan 902
Switch(config)#monitor session reflector-port gigabitethernet 0/2
Switch(config)# exit
Switch# show monitor
```

Destination switch:

```
Switch# configure terminal
Enter configuration commands, one per line.
Switch(config)#monitor session source remote vlan 902
Switch(config)#monitor session destination interface gigabitethernet 0/8
Switch(config)# exit
Switch# show monitor
```

16 Configuring Time Range

16.1 Creating a Time Range

A time range-based configuration takes effect only in specified time ranges. Only after a time range is configured and the system time is within the time range, can an configuration rule take effect.

Two types of time ranges are available:

- Periodic time range, which recurs periodically on the day or days of the week.
- Absolute time range, which takes effect only in a period of time and does not recur.

16.2 Configuration Procedure

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	time-range *time-range-name*	Assign a meaningful name (for example, *workhours*) to the time range to be created, and enter time-range configuration mode. The name cannot contain a space or quotation mark and must begin with a letter.
Step 3	absolute [start *time date*] [end *time date*] or periodic *day-of-the-week hh:mm to* [*day-of-the-week*] *hh:mm* or periodic {weekday	Specify when the function it will be applied to is operational. • You can use only one absolute statement in the time range. If you configure more than one absolute statement, only the one configured last is executed • You can enter multiple periodic statements. For example, you could configure different hours for weekdays and weekends. Refer to the example configurations.
Step 4	show time-range	Verify the time-range configuration.
Step 5	copy running-config startup-config	(Optional) Save your entries in the configuration file.

To remove a configured time-range limitation, use the no time-range time-range-name global configuration command.

Repeat the steps if you have multiple items that you want operational at different times.

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

```
Switch# configure terminal
Enter configuration commands, one per line.
Switch(config)# time-range summer
Switch(config-time-range)# absolute start 00:00 1 4 2018 end 23:59 30 9 2018
Switch(config)# exit
Switch# show time-range
```

This example shows how to configure time ranges for workhours and for company holidays and how to verify your configuration.

```
Switch(config)# time-range workhours
Switch(config-time-range)# periodic weekdays 9:00 to 12:00
Switch(config-time-range)# periodic weekdays 13:00 to 18:00
Switch(config-time-range)# exit
Switch(config)# time-range new_year_day_2018
Switch(config-time-range)# absolute start 00:00 1 1 2018 end 23:59 1 1 2018
Switch(config-time-range)# exit
Switch(config)# time-range spring-festival _2018
Switch(config-time-range)# absolute start 00:00 16 2 2018 end 23:59 23 2 2018
Switch(config-time-range)# exit
Switch# show time-range
```

17 Clock Configuration

17.1 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.

17.2 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.

17.3 Configuring NTP

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	ntp	Enable ntp function.
Step 3	ntp { gmt time [*gmt-number*] | stratum [*number*] | unicast-server [*server-ip*] }	Configure the switch system clock to be synchronized by a time server
Step 4	Show ntp	Verify your entries.
Step 5	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# configure terminal
Enter configuration commands, one per line.
Switch(config)# ntp
Switch(config)# ntp gmt time gmt+8
Switch(config)# exit
Switch# show ntp
```

17.4 Configuration time-range be applied to clock

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

```
Switch# configure terminal
Enter configuration commands, one per line.
Switch(config)# time-range summer
Switch(config-time-range)# absolute start 00:00 1 4 2018 end 23:59 30 9 2018
Switch(config)# exit
Switch(config)# clock daylight-saving-time summer gmt 1
Switch# show time-range
Switch# show clock
```

17.5 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	configure terminal	Enter global configuration mode.
Step 2	clock set *hh*:*mm*:*ss* *day month year*	Manually set the system clock using one of these formats.
Step 3	Show clock	Verify your entries.
Step 4	copy running-config startup-config	(Optional) Save your entries in the configuration file.

This example shows how to manually set the system clock to 23:05:00 on February 23, 2015:

```
Switch# configure terminal
Enter configuration commands, one per line.
Switch(config)# clock set 23:05:00 23 2 2015
Switch(config)# exit
Switch# show clock
```

18 ACL Configuration

18.1 ACL Overview

As the network scale and network traffic are increasingly growing, security control and bandwidth assignment play a more and more important role in network management. Filtering data packets can prevent a network from being accessed by unauthorized users efficiently while controlling network traffic and saving network resources. Access control lists (ACL) are often used to filter packets with configured matching rules.

Upon receiving a packet, the switch compares the packet with the rules of the ACL applied on the current port to permit or discard the packet.

The rules of an ACL can be referenced by other functions that need traffic classification, such as QoS.

ACLs classify packets using a series of conditions known as rules. The conditions can be based on source addresses, destination addresses and port numbers carried in the packets.

According to their application purposes, ACLs fall into the following four types.

- Basic ACL. Rules are created based on source IP addresses only.
- Advanced ACL. Rules are created based on the Layer 3 and Layer 4 information such as the source and destination IP addresses, type of the protocols carried by IP, protocol-specific features, and so on.
- Layer 2 ACL. Rules are created based on the Layer 2 information such as source and destination
- MAC addresses, VLAN priorities, type of Layer 2 protocol, and so on.
- User-defined ACL. An ACL of this type matches packets by comparing the strings retrieved from the packets with specified strings. It defines the byte it begins to perform “and” operation with the mask on the basis of packet headers.

18.2 Understanding Access Control Parameters

Before configuring ACLs on the switches, you must have a thorough understanding of the access control parameters (ACPs). ACPs are referred to as masks in the switch CLI commands output.

Each ACE has a mask and a rule. The Classification Field or mask is the field of interest on which you want to perform an action. The specific values associated with a given mask are called rules.

Packets can be classified on these Layer 2, Layer 3, and Layer 4 fields:

- Layer 2 fields:
- Source MAC address (Specify all 48 bits.)
- Destination MAC address (Specify all 48 bits.)
- Ethertype (16-bit ethertype field)

- You can use any combination or all of these fields simultaneously to define a flow.
- Layer 3 fields:
- IP source address (Specify all 32 IP source address bits to define the flow, or specify a user defined subnet. There are no restrictions on the IP subnet to be specified.)
- IP destination address (Specify all 32 IP destination address bits to define the flow, or specify a user-defined subnet. There are no restrictions on the IP subnet to be specified.)
- You can use any combination or all of these fields simultaneously to define a flow.
- Layer 4 fields:
- TCP (You can specify a TCP source, destination port number, or both at the same time.)
- UDP (You can specify a UDP source, destination port number, or both at the same time.)

18.3 Configuring ACLs

18.3.1 Creating Standard and Extended IP ACLs

This section describes how to create switch IP ACLs. The first match determines whether the switch accepts or rejects the packet. Because the switch stops testing conditions after the first match, the order of the conditions is critical. If no conditions match, the switch denies the packet.

ACL Numbers

The number you use to denote your ACL shows the type of access list that you are creating. Lists the access list number and corresponding type and shows whether or not they are supported by the switch. The switch supports IP standard and IP extended access lists, numbers 1 to 99 and 100 to 199. and supports standard MAC and extended MAC access lists, numbers 700 to 799 and 1100 to1199. Beginning in privileged EXEC mode, follow these steps to create a numbered standard IP ACL:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.

Step 2	access-list *access-list-number* {deny | permit} {*source source-wildcard* | host *source* | any}	Define a standard IP ACL by using a source address and wildcard.
Step 3	commit	Commit all the ACL Config to be valid
Step 4	show access-list	Verify your entries.
Step 5	show access-list { [*acl-number*] | type [extended-ip] | [extended-mac] | [standard-ip] | [standard-mac] | [type-code]}	Verify your entries.
Step 6	copy running-config startup-config	(Optional) Save your entries in the configuration file.

Use the no access-list access-list-number global configuration command to delete the entire ACL. You cannot delete individual ACEs from numbered access lists.

This example shows how to create a standard ACL to deny access to IP host 192.168.2.23, permit access to any others, and display the results.

```
Switch# configure terminal
Enter configuration commands, one per line.
Switch (config)# access-list 1 deny host 192.168.2.23
Switch (config)# access-list 2 permit any
Switch(config)# commit
Switch# show access-lists
```

18.3.2 Creating a Numbered Extended ACL

Although standard ACLs use only source addresses for matching, you can use an extended ACL source and destination addresses for matching operations and optional protocol type information for finer granularity of control. Some protocols also have specific parameters and keywords that apply to that protocol.

These IP protocols are supported on physical interfaces (protocol keywords are in parentheses in bold):

Internet Protocol (ip), Transmission Control Protocol (tcp), or User Datagram Protocol (udp).

Beginning in privileged EXEC mode, follow these steps to create an extended ACL:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	access-list *access-list-number* {deny | permit } *protocol* {*source source-wildcard* | host *source* | any} [*operator port*] {*destination destination-wildcard* | host *destination* | any} [*operator port*] [dscp *dscp-value*]	Define an extended IP access list and the access conditions. The *access-list-number* is a decimal number from 100 to 199. Enter deny or permit to specify whether to deny or permit the packet if conditions are matched. For *protocol*, enter the name or number of an IP protocol: IP, TCP, or UDP. To match any Internet protocol (including TCP and UDP), use the keyword ip.
Step 3	commit	Commit all the ACL Config to be valid
Step 4	show access	Verify your entries.
Step 5	show access { [*acl-number*] | type [extended-ip] | [extended-mac] | [standard-ip] | [standard-mac] | [type-code]}	Verify your entries.
Step 6	copy running-config startup-config	(Optional) Save your entries in the configuration file.

Use the no access-list access-list-number global configuration command to delete the entire access list.
You cannot delete individual ACEs from numbered access lists.
This example shows how to create and display an extended access list to deny Telnet access from any host in network 192.168.2.23 to any host in network 192.168.2.0 and permit any others. (The eq keyword after the destination address means to test for the TCP

destination port number equaling Telnet.)

```
Switch# configure terminal
Enter configuration commands, one per line.
Switch(config)# access-list 100 deny tcp 192.168.2.23 255.255.255.0 192.168.2.0
255.255.255.0 eq 23
Switch(config)# access-list 101 permit tcp any any
Switch(config)# exit
Switch# show access-lists
```

18.3.3 Configuration time-range be applied to ACL

For a time range to be applied, you must enter the time-range name in an extended ACL that can implement time ranges. This example shows how to create and verify extended access list 189 that denies TCP traffic from any source to any destination during the defined any time ranges and permits all TCP traffic during work hours.

```
Switch(config)# time-range workhours
Switch(config-time-range)# periodic weekdays 9:00 to 12:00
Switch(config-time-range)# periodic weekdays 13:00 to 18:00
Switch(config-time-range)# exit
Switch(config)# access-list 188 deny tcp any any
Switch(config)# access-list 189 permit tcp any any time-range workhours
Switch(config)# exit
Switch# show time-range
Switch# show access-lists
```

19 QoS Configuration

19.1 Overview

Introduction to QoS

Quality of Service (QoS) is a concept concerning service demand and supply. It reflects the ability to meet customer needs. Generally, QoS does not focus on grading services precisely, but on improving services under certain conditions.

In an internet, QoS refers to the ability of the network to forward packets. The evaluation on QoS of a network can be based on different aspects because the network may provide various services. Generally, QoS refers to the ability to provide improved service by addressing the essential issues such as delay, jitter, and packet loss ratio in the packet forwarding process.

Traditional Packet Forwarding Service

In traditional IP networks, packets are treated equally. That is, the FIFO (first in first out) policy is adopted for packet processing. Network resources required for packet forwarding is determined by the order in which packets arrive. All the packets share the resources of the network. Network resources available to the packets completely depend on the time they arrive. This service policy is known as Best-effort, which delivers the packets to their destination with the best effort, with no assurance and guarantee for delivery delay, jitter, packet loss ratio, reliability, and so on.

The traditional Best-Effort service policy is only suitable for applications insensitive to bandwidth and delay, such as WWW, file transfer and E-mail.

New Applications and New Requirements

With the expansion of computer network, more and more networks become part of the Internet. The Internet gains rapid development in terms of scale, coverage and user quantities. More and more users use the Internet as a platform for their services and for data transmission.

Besides the traditional applications such as WWW, E-mail, and FTP, new services are developed on the Internet, such as tele-education, telemedicine, video telephone, videoconference and Video-on-Demand (VoD). Enterprise users expect to connect their regional branches together using VPN techniques for coping with daily business, for instance, accessing databases or manage remote equipments through Telnet.

All these new applications have one thing in common, that is, they have special requirements for bandwidth, delay, and jitter. For instance, bandwidth, delay, and jitter are critical for videoconference and VoD. As for other applications, such as transaction processing and Telnet, although bandwidth is not as critical, a too long delay may cause unexpected results. That is, they need to get serviced in

time even if congestion occurs.
Newly emerging applications demand higher service performance from IP networks. In addition to simply delivering packets to their destinations, better network services are demanded, such as allocating dedicated bandwidth, reducing packet loss ratio, avoiding congestion, regulating network traffic, and setting priority of the packets. To meet those requirements, the network should be provided with better service capability.

Traffic classification is the basis of all the above-mentioned traffic management technologies. It identifies packets using certain rules and makes differentiated services possible. Traffic policing, traffic shaping, congestion management, and congestion avoidance are methods for implementing network traffic control and network resource management. They are occurrences of differentiated services.

Introduction to QoS Features

Traffic Classification

Traffic here refers to service traffic; that is, all the packets passing the switch.
Traffic classification means identifying packets that conform to certain characteristics according to certain rules. It is the foundation for providing differentiated services.
In traffic classification, the priority bit in the type of service (ToS) field in IP packet header can be used to identify packets of different priorities. The network administrator can also define traffic classification policies to identify packets by the combination of source address, destination address, MAC address, IP protocol or the port number of an application. Normally, traffic classification is done by checking the information carried in packet header. Packet payload is rarely adopted for traffic classification. The identifying rule is unlimited in range. It can be a quintuplet consisting of source address, source port number, protocol number, destination address, and destination port number. It can also be simply a network segment.

Priority Trust Mode

Precedence types

1) IP precedence, ToS precedence, and DSCP precedence
The ToS field in an IP header contains eight bits numbered 0 through 7, among which,

- The first three bits indicate IP precedence in the range 0 to 7.
- Bit 3 to bit 6 indicate ToS precedence in the range of 0 to 15.
- In RFC2474, the ToS field in IP packet header is also known as DS field. The first six bits (bit 0 through bit 5) of the DS field indicate differentiated service codepoint (DSCP) in the range of 0 to 63, and the last two bits (bit 6 and bit 7) are reserved.

2) 802.1p priority
802.1p priority lies in Layer 2 packet headers and is applicable to occasions where the Layer 3 packet
header does not need analysis but QoS must be assured at Layer 2.

3) Local precedence
Local precedence is a locally significant precedence that the device assigns to a packet. A local precedence value corresponds to one of the eight hardware output queues. Packets with the highest local precedence are processed preferentially. As local precedence is used only for internal queuing, a packet does not carry it after leaving the queue.

19.1.1 Configuring Priority trust mode

After a packet enters a switch, the switch sets the 802.1p priority and local precedence for the packet according to its own capability and the corresponding rules.
1) For a packet carrying no 802.1q tag
When a packet carrying no 802.1q tag reaches a port, the switch uses the port priority as the 802.1p precedence value of the received packet, searches for the local precedence corresponding to the port priority of the receiving port in the 802.1p-to-local precedence mapping table, and assigns the local precedence to the packet.

2) For an 802.1q tagged packet

For incoming 802.1q tagged packets, you can configure the switch to trust packet priority with the priority trust command or to trust port priority with the undo priority trust command. By default, the switches trust port priority.

- Trusting port priority

In this mode, the switch replaces the 802.1p priority of the received packet with the port priority, searches for the local precedence corresponding to the port priority of the receiving port in the 802.1p-to-local precedence mapping table, and assigns the local precedence to the packet.

- Trusting packet priority

After configuring to trust packet priority, you can specify the trusted priority type, which can be 802.1p priority, DSCP precedence, or IP precedence. With trusting packet priority enabled, the switch trusts the 802.1p priority of received packets.

The switches provide 802.1p-to-local-precedence, DSCP-to-local-precedence, and IP-to-local-precedence mapping tables for priority mapping.

	Command	**Purpose**
Step 1	configure terminal	Enter global configuration mode.
Step 2	mls qos	Enable global qos
Step 3	mls qos trust { layer2 | layer2+3 | layer3 |port}	Configure trust mode of QoS. By default, is trusted port. Layer2- classify by packet 802.1p Layer2+3- classify by packet first by layer3, else by layer2 Layer3- classify by packet DSCP Port- classify by packet port priority
Step 4	show mls qos global	Verify your entries.
Step 5	copy running-config startup-config	(Optional) Save your entries in the configuration file.

To return to the default setting, use the no mls qos trust interface configuration command.

This example shows how to configure trust mode :

```
Switch# configure terminal
Enter configuration commands, one per line.
```

```
Switch(config)# mls qos
Switch(config)# mls qos trust layer2+3
Switch(config)# exit
Switch# show mls qos global
```

Priority Marking

The priority marking function is to reassign priority for the traffic matching an ACL referenced for traffic classification.

- If 802.1p priority marking is configured, the traffic will be mapped to the local precedence corresponding to the re-marked 802.1p priority and assigned to the output queue corresponding to the local precedence.
- If local precedence marking is configured, the traffic will be assigned to the output queue corresponding to the re-marked local precedence.
- If IP precedence or DSCP marking is configured, the traffic will be marked with new IP precedence or DSCP precedence.

Traffic Policing and Traffic Shaping

The network will be made more congested by plenty of continuous burst packets if the traffic of each user is not limited. The traffic of each user must be limited in order to make better use of the limited network resources and provide better service for more users. For example, a traffic flow can be limited to get only its committed resources during a time period to avoid network congestion caused by excessive bursts.

Traffic policing and traffic shaping is each a kind of traffic control policy used to limit the traffic and the resource occupied by supervising the traffic. The regulation policy is implemented according to the evaluation result on the premise of knowing whether the traffic exceeds the specification when traffic policing or traffic shaping is performed. Normally, token bucket is used for traffic evaluation.

Token bucket

The token bucket can be considered as a container with a certain capacity to hold tokens. The system puts tokens into the bucket at the set rate. When the token bucket is full, the extra tokens will overflow and the number of tokens in the bucket stops increasing.

Evaluating the traffic with the token bucket

When token bucket is used for traffic evaluation, the number of the tokens in the token bucket determines the amount of the packets that can be forwarded. If the number of tokens in the bucket is enough to forward the packets, the traffic is conforming to the specification; otherwise, the traffic is nonconforming or excess. Parameters concerning token bucket include:

- Average rate: The rate at which tokens are put into the bucket, namely, the permitted average rate of the traffic. It is generally set to committed information rate (CIR).
- Burst size: The capacity of the token bucket, namely, the maximum traffic size that is permitted in each burst. It is generally set to committed burst size (CBS). The set burst size must be greater than the maximum packet length.

One evaluation is performed on each arriving packet. In each evaluation, if the number of tokens in the bucket is enough, the traffic is conforming to the specification and you must take away some tokens whose number is corresponding to the packet forwarding authority; if the number of tokens in the bucket is not enough, it means that too many tokens have been used and the traffic is excess.

Traffic policing

The typical application of traffic policing is to supervise specific traffic into the network and limit it to a reasonable range, or to "discipline" the extra traffic. In this way, the network resources and the interests of the operators are protected.

Traffic policing is widely used in policing the traffic into the network of internet service providers (ISPs).

Traffic policing can identify the policed traffic and perform pre-defined policing actions based on different evaluation results. These actions include:

- Discarding the nonconforming packets.
- Forwarding the conforming packets or nonconforming packets.

- Marking the conforming packets with 802.1p precedence and then forwarding the packets.
- Marking the conforming packets or nonconforming packets with DSCP precedence and forwarding the packets.

Traffic shaping

Traffic shaping is a measure to regulate the output rate of traffic actively. Its typical application is to control local traffic output based on the traffic policing indexes of downstream network nodes.
The major difference between traffic shaping and traffic policing is that the packets to be dropped in traffic policing are cached in traffic shaping——usually in buffers or queues,

When there are enough tokens in the token bucket, the cached packets are sent out evenly. Another difference between traffic policing and traffic shaping is that traffic shaping may increase the delay while traffic policing hardly increases the delay.

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 thi 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.

19.1.2 Configuring Queue Scheduling

When the network is congested, the problem that many packets compete for resources must be solved, usually through queue scheduling.
In the following section, strict priority (SP) queues, weighted round robin (WRR), and SP+WRR (High
Queue-WRR) queues are introduced.

1) SP queuing

SP queue-scheduling algorithm is specially designed for critical service applications. An important feature of critical services is that they demand preferential service in congestion in order to reduce the response delay. Assume that there are four output queues on the port and the preferential queue classifies the four output queues on the port into four classes, which are queue 3, queue 2, queue 1, and queue 0. Their priorities decrease in order.

In queue scheduling, SP sends packets in the queue with higher priority strictly following the priority order from high to low. When the queue with higher priority is empty, packets in the queue with lower priority are sent. You can put critical service packets into the queues with higher priority and put non-critical service (such as e-mail) packets into the queues with lower priority. In this case, critical service packets are sent preferentially and non-critical service packets are sent when critical service groups are not sent.

The disadvantage of SP queue is that: if there are packets in the queues with higher priority for a long time in congestion, the packets in the queues with lower priority will be “starved” because they are not served.

2) WRR queuing

WRR queue-scheduling algorithm schedules all the queues in turn and every queue can be assured of a certain service time. Assume there are four output queues on a port. WRR configures a weight value for each queue, which is w3, w2, w1, and w0 for queue 3 through queue 0. The weight value indicates the proportion of obtaining resources. On a 100 M port, configure the weight value of WRR queue-scheduling algorithm to 5, 3, 1, and 1 (corresponding to w3, w2, w1, and w0 in order). In this way, the queue with the lowest priority can get 10 Mbps bandwidth (100-Mbps × 1/ (5 + 3 + 1 + 1)) at least, and the disadvantage of SP queue-scheduling that the packets in queues with lower priority may not get service for a long time is avoided. Another advantage of WRR queue is that: though the queues are scheduled in order, the service time for each queue is not fixed; that is to say, if a queue is empty, the next queue will be scheduled. In this way, the bandwidth resources are made full use.

3) SP+WRR queuing

SP+WRR is an improvement over WRR. Assume there are four priority queues on a port and queue 3 allocated with the highest priority, the switch will ensure that this queue get served first and will perform round-robin scheduling to the other three queues when the traffic has exceeded the bandwidth capacity of a port.

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	mls qos	Enable global qos
Step 3	mls qos map queue *number(0-8)* {wrr|strict} [weight] *number(1-8)*	Configure queue type. By default, the type is strict.
Step 4	show mls qos queue	Verify your entries.
Step 5	copy running-config startup-config	(Optional) Save your entries in the configuration file.

This example shows how to configure cos value of a port :

```
Switch# configure terminal
Enter configuration commands, one per line.
Switch(config)# mls qos
Switch(config)# mls qos queue type sp+wrr
Switch(config)# exit
Switch# show mls qos queue
```

19.1.3 Configuring the Trust State on Ports within the QoS Domain

Packets entering a QoS domain are classified at the edge of the QoS domain. When the packets are classified at the edge, the switch port within the QoS domain can be configured to one of the trusted states because there is no need to classify the packets at every switch within the QoS domain.

Beginning in privileged EXEC mode, follow these steps to configure the port to trust the classification of the traffic that it receives:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface *interface-id*	Specify the interface to be trusted, and enter interface configuration mode.

		Valid interfaces include physical interfaces.
Step 3	mls qos default-Priority *value(0-7)*	Configure the port default-Priority. By default, the port default-Priority is 0.
Step 4	show mls qos interface [*interface-id*]	Verify your entries.
Step 5	copy running-config startup-config	(Optional) Save your entries in the configuration file.

To return to the default setting, use the no mls qos default-Priority interface configuration command.

This example shows how to configure cos value of a port :

```
Switch# configure terminal
Enter configuration commands, one per line.
Switch(config)# interface fastethernet 0/1
Switch(config-if)# mls qos default-Priority    7
Switch(config-if)# exit
Switch(config)# exit
Switch# show mls qos interface fastethernet 0/1
Switch# show mls qos interface
```

19.1.4 Configuring the 802.1P-to-CoS Map

You use the 802.1P-to-CoS map to map 802.1P values in incoming packets to a cos value that QoS uses internally to represent the priority of the traffic.

If default values are not appropriate for your network, you need to modify them.

Beginning in privileged EXEC mode, follow these steps to modify the 802.1P-to-CoS map:

	Command	**Purpose**
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**mls qos rewrite 802-1p**	Configure qos rewrite 802-1p.
Step 3	**mls qos map l2map 1p-to-queue** *1p-value(0-7) queue(1-8)*	Modify the 1p-to-queue map
Step 4	**mls qos map rewrite l2map 802-1p-to-cos** *1p-value(0-7) cos(0-7)*	Modify the 802-1p-to-cos map
Step 5	**show mls qos map** {**1p-to-queue | 802-1p-to-cos** }	Verify your entries.

Step 6	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

This example shows how the 802.1p values 4 and 5 are mapped to CoS value 7.

```
Switch# configure terminal
Enter configuration commands, one per line.
Switch(config)# mls qos rewrite 802-1p
Switch(config)# mls qos map rewrite l2map 802-1p-to-cos 4 7
Switch(config)# mls qos map rewrite l2map 802-1p-to-cos 5 7
Switch(config)# exit
Switch# show mls qos map 802-1p-to-cos
Switch# show mls qos map 1p-to-queue
```

19.1.5 Configuring the DSCP-to-DSCPMap

You use the DSCP-to-DSCPmap to map DSCP values in incoming packets to a DSCPMap value, which is used to select one of the four egress queues.

If default values are not appropriate for your network, you need to modify them.

Beginning in privileged EXEC mode, follow these steps to modify the DSCP-to-DSCPmap:

	Command	**Purpose**
Step 1	configure terminal	Enter global configuration mode.
Step 2	mls qos rewrite dscp	Configure qos rewrite dscp.
Step 3	mls qos map l3map dscpmap-to-queue *dscp queue*	Modify the dscpmap-to-queue map.
Step 4	mls qos map rewrite l3map dscp-to-dscpmap *dscp dscp*	Modify the dscp-to-dscpmap map.
Step 5	show mls qos map { dscp-to-dscpmap | dscp-to-queue }	Verify your entries.
Step 6	copy running-config startup-config	(Optional) Save your entries in the configuration file.

To return to the default map, use the no mls qos map global configuration command.

This example shows how the DSCP values 26 and 48 are mapped to

CoS value 7. For the remaining DSCP values, the DSCP-to-CoS mapping is the default.

```
Switch# configure terminal
Enter configuration commands, one per line.
Switch(config)# mls qos rewrite dscp
Switch(config)# mls qos map rewrite l3map dscp-to-dscpmap 26 63
Switch(config)# mls qos map rewrite l3map dscp-to-dscpmap 48 63
Switch(config)# exit
Switch# show mls qos map dscp-to-dscpmap
Switch# show mls qos map dscp-to-queue
```

19.1.6 Configuring QoS based on ACL

Flow-Based Traffic Accounting

The function of traffic-based traffic accounting is to use ACL rules in traffic classification and perform traffic accounting on the packets matching the ACL rules. You can get the statistics of the packets you are interested in through this function.

Traffic Mirroring

Traffic mirroring uses ACL for traffic classification and duplicates the matched packets of all ports, the specified VLAN, the specified port group, or the specified port to the destination port. For information about port mirroring, refer to the Mirroring module of this manual.

Traffic Redirecting

Traffic redirecting identifies traffic using ACLs and redirects the matched packets to specific ports. By traffic redirecting, you can change the way in which a packet is forwarded to achieve specific purposes.

After a traffic class has been defined with the ACL, you can attach a policy to it. A policy might contain multiple classes with actions specified for each one of them. A policy might include commands to classify the class as a particular aggregate (for example, assign a DSCP) or rate-limit the class. This policy is then attached to a particular port on which it becomes effective.

You implement IP ACLs to classify IP traffic by using the access-list global configuration command; you implement Layer 2 MAC ACLs to classify Layer 2 traffic by using the mac access-list extended global configuration command.

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	access-list *access-list-number* {deny | permit } {*source source-wildcard* | host *source* | any}	Define a standard IP ACL by using a source address and wildcard.
Step 3	commit	Commit all the ACL Config to be valid
Step 4	Policy-map access-group *access-list* *-number*	Define a policer for the classified traffic.
Step 5	counter *name*	Statistical packets of a policer.
Step 6	dscp *number*	Rewrite dscp value of policer.
Step 7	Monitor	Monitor data packets of policer.
Step 8	up *number*	Rewrite up value of policer.
Step 9	show plicy-map	Verify your entries.
Step 10	copy running-config startup-config	(Optional) Save your entries in the configuration file.

This example shows how to create a policy map and attach it to an ingress interface. In the configuration, the IP standard ACL permits traffic from network 10.1.0.0. For traffic matching this classification, the DSCP value in the incoming packet is trusted. DSCP is marked to a value of 10 and sent.

```
Switch# configure terminal
Enter configuration commands, one per line.
Switch(config)# access-list 1 permit 10.1.0.0 255.255.255.0
Switch(config)# commit
Switch(config)# policy-map access-group 1
Switch(config-pmap)# counter market
Switch(config-pmap)# dscp 10
Switch(config-pmap)# monitor
Switch(config-pmap)# exit
Switch(config)# exit
Switch# show policy-map
```

20 DHCP Overview

20.1 Introduction to DHCP

With networks getting larger in size and more complicated in structure, lack of available IP addresses becomes the common situation the network administrators have to face, and network configuration becomes a tough task for the network administrators. With the emerging of wireless networks and the using of laptops, the position change of hosts and frequent change of IP addresses also require new technology. Dynamic host configuration protocol (DHCP) is developed to solve these issues.

DHCP adopts a client/server model, where the DHCP clients send requests to DHCP servers for configuration parameters; and the DHCP servers return the corresponding configuration information such as IP addresses to implement dynamic allocation of network resources.

DHCP IP Address Assignment

IP Address Assignment Policy

Currently, DHCP provides the following three IP address assignment policies to meet the requirements
of different clients:

- Manual assignment. The administrator configures static IP-to-MAC bindings for some special clients, such as a WWW server. Then the DHCP server assigns these fixed IP addresses to the clients.
- Automatic assignment. The DHCP server assigns IP addresses to DHCP clients. The IP addresses will be occupied by the DHCP clients permanently.
- Dynamic assignment. The DHCP server assigns IP addresses to DHCP clients for predetermined period of time. In this case, a DHCP client must apply for an IP address again at the expiration of the period. This policy applies to most clients.

Obtaining IP Addresses Dynamically

A DHCP client undergoes the following four phases to dynamically obtain an IP address from a DHCP server:

1) Discover: In this phase, the DHCP client tries to find a DHCP server by broadcasting a DHCP-DISCOVER packet.

2) Offer: In this phase, the DHCP server offers an IP address. After the DHCP server receives the DHCP-DISCOVER packet from the DHCP client, it chooses an unassigned IP address from the address pool according to the priority order of IP address assignment and then sends the IP address and other configuration information together in a DHCP-OFFER packet to the DHCP client.The sending mode is decided by the flag filed in the DHCP-DISCOVER packet.

3) Select: In this phase, the DHCP client selects an IP address. If more than one DHCP server sends DHCP-OFFER packets to the DHCP client, the DHCP client only accepts the DHCP-OFFER packet that first arrives, and then broadcasts a DHCP-REQUEST packet containing the assigned IP address carried in the DHCP-OFFER packet.

4) Acknowledge: In this phase, the DHCP servers acknowledge the IP address. Upon receiving the DHCP-REQUEST packet, only the selected DHCP server returns a DHCP-ACK packet to the DHCP client to confirm the assignment of the IP address to the client, or returns a DHCP-NAK packet to refuse the assignment of the IP address to the client. When the client receives the DHCP-ACK packet, it broadcasts an ARP packet with the assigned IP address as the destination address to detect the assigned IP address, and uses the IP address only if it does not receive any response within a specified period.

Updating IP Address Lease

After a DHCP server dynamically assigns an IP address to a DHCP client, the IP address keeps valid only within a specified lease time and will be reclaimed by the DHCP server when the lease expires. If the DHCP client wants to use the IP address for a longer time, it must update the IP lease.

By default, a DHCP client updates its IP address lease automatically by unicasting a DHCP-REQUEST packet to the DHCP server when half of the lease time elapses. The DHCP server responds with a

DHCP-ACK packet to notify the DHCP client of a new IP lease if the server can assign the same IP address to the client. Otherwise, the DHCP server responds with a DHCP-NAK packet to notify the DHCP client that the IP address will be reclaimed when the lease time expires.

If the DHCP client fails to update its IP address lease when half of the lease time elapses, it will update its IP address lease by broadcasting a DHCP-REQUEST packet to the DHCP servers again when seven-eighths of the lease time elapses. The DHCP server performs the same operations as those described above.

DHCP Packet Format

DHCP has eight types of packets. They have the same format, but the values of some fields in the packets are different. The DHCP packet format is based on that of the BOOTP packets.

Protocol Specification

Protocol specifications related to DHCP include:

- RFC2131: Dynamic Host Configuration Protocol
- RFC2132: DHCP Options and BOOTP Vendor Extensions
- RFC1542: Clarifications and Extensions for the Bootstrap Protocol
- RFC3046: DHCP Relay Agent Information option

20.2 DHCP Snooping Configuration

Introduction to DHCP Snooping

For the sake of security, the IP addresses used by online DHCP clients need to be tracked for the administrator to verify the corresponding relationship between the IP addresses the DHCP clients obtained from DHCP servers and the MAC addresses of the DHCP clients.

Layer 2 switches can track DHCP client IP addresses through the DHCP snooping function, which listens DHCP broadcast packets.

Introduction to DHCP Snooping Trusted/Untrusted Ports

When an unauthorized DHCP server exists in the network, a DHCP client may obtains an illegal IP address. To ensure that the DHCP clients obtain IP addresses from valid DHCP servers, the switches can specify a port to be a trusted port or an untrusted port by the DHCP snooping function.

- Trusted: A trusted port is connected to an authorized DHCP server directly or indirectly. It forwards DHCP messages to guarantee that DHCP clients can obtain valid IP addresses.
- Untrusted: An untrusted port is connected to an unauthorized DHCP server. The DHCP-ACK or DHCP-OFFER packets received from the port are discarded, preventing DHCP clients from receiving invalid IP addresses.

Overview of DHCP-Snooping Option 82

Introduction to Option 82

Option 82 is the relay agent information option in the DHCP message. It records the location information of the DHCP client. When a DHCP relay agent (or a device enabled with DHCP snooping) receives a client's request, it adds the Option 82 to the request message and sends it to the server.

The administrator can locate the DHCP client to further implement security control and accounting. The

Option 82 supporting server can also use such information to define individual assignment policies of IP address and other parameters for the clients.

Option 82 involves at most 255 sub-options. If Option 82 is defined, at least one sub-option must be defined. Currently the DHCP relay agent supports two sub-options: sub-option 1 (circuit ID sub-option) and sub-option 2 (remote ID sub-option).

Padding content and frame format of Option 82

There is no specification for what should be padded in Option 82. Manufacturers can pad it as required.

By default, the sub-options of Option 82 for the Switches (enabled with DHCP snooping) are padded as follows:

- sub-option 1 (circuit ID sub-option): Padded with the port index (smaller than the physical port number by 1) and VLAN ID of the port that received the client's request.
- sub-option 2 (remote ID sub-option): Padded with the bridge MAC address of the DHCP snooping device that received the client's request.

Overview of IP Filtering

A denial-of-service (DoS) attack means an attempt of an attacker sending a large number of forged address requests with different source IP addresses to the server so that the network cannot work normally. The specific effects are as follows:

- The resources on the server are exhausted, so the server does not respond to other requests.
- After receiving such type of packets, a switch needs to send them to the CPU for processing. Too many request packets cause high CPU usage rate. As a result, the CPU cannot work normally.
- The switch can filter invalid IP packets through the DHCP-snooping table and IP static binding table.

DHCP-snooping table

After DHCP snooping is enabled on a switch, a DHCP-snooping table is generated. It is used to record IP addresses obtained from the DHCP server, MAC addresses, the number of the port through which a client is connected to the DHCP-snooping-enabled device, and the number of the VLAN to which the port belongs to. These records are saved as entries in the DHCP-snooping table.

IP static binding table

The DHCP-snooping table only records information about clients that obtains IP address dynamically through DHCP. If a fixed IP address is configured for a client, the IP address and MAC address of the client cannot be recorded in the DHCP-snooping table. Consequently, this client cannot pass the IP filtering of the DHCP-snooping table, thus it cannot access external networks.

To solve this problem, the switch supports the configuration of static binding table entries that is the binding relationship between IP address, MAC address, and the port connecting to the client, so that packets of the client can be correctly forwarded.

IP filtering

The switch can filter IP packets in the following two modes:

- Filtering the source IP address in a packet. If the source IP address and the number of the port that receives the packet are consistent with entries in the DHCP-snooping table or static binding table, the switch regards the packet as a valid packet and forwards it;

otherwise, the switch drops it directly.

- Filtering the source IP address and the source MAC address in a packet. If the source IP address and source MAC address in the packet, and the number of the port that receives the packet are consistent with entries in the DHCP-snooping table or static binding table, the switch regards the packet as a valid packet and forwards it; otherwise, the switch drops it directly.

20.2.1 Enabling DHCP Snooping and Option 82

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	ip dhcp snooping	Enable DHCP snooping.
Step 3	interface *interface-id*	Specify the port to configure, and enter interface configuration mode.
Step 4	ip dhcp option {circuit-id | policy | remote-id }	Configure dhcp option value.
Step 5	show ip dhcp relay helper-address	Verify your entries.
Step 6	Show ip dhcp relay option	Verify your entries.
Step 7	copy running-config startup-config	(Optional) Save your entries in the configuration file.

This example shows how to configure dhcp snooping and option 82 :

```
Switch# configure terminal
Enter configuration commands, one per line.
Switch(config)# ip dhcp snooping
Switch(config)# interface fastethernet 0/1
Switch(config-if)# ip dhcp snooping information trust
Switch(config-if)# exit
Switch(config)# interface fastethernet 0/2
Switch(config-if)# ip dhcp option circuit-id index 1 vlan-id 2 vlan 2
Switch(config-if)# exit
Switch(config)# ip dhcp remote-id 2222.2222.2222
Switch(config)# exit
Switch# show ip dhcp option fastethernet 0/2 circuit-id
Switch# show ip dhcp server trust
```

```
Switch# show ip dhcp information
Switch# show arp
```

20.2.2 Configuring DHCP Snooping Trusted/Untrusted Ports

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	ip dhcp snooping	Enable DHCP snooping globally.
Step 2	interface *interface-id*	Specify the port to configure, and enter interface configuration mode.
Step 3	ip dhcp snooping information trust	Configure dhcp snooping trust port.
Step 4	show ip dhcp server trust	Verify your entries.
Step 5	copy running-config startup-config	(Optional) Save your entries in the configuration file.

This example shows how to configure dhcp trust port:

```
Switch# configure terminal
Enter configuration commands, one per line.
Switch(config)# interface fastethernet 0/18
Switch(config-if)# ip dhcp snooping information trust
Switch(config-if)# exit
Switch(config)# exit
Switch# show ip dhcp server trust
```

20.2.3 Configuring DHCP Relay and Option 82

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	ip dhcp relay	Enable DHCP relay.
Step 3	ip dhcp relay helper-address *ip-address*	Configure dhcp relay helper address.
Step 4	interface *interface-id*	Specify the port to configure, and enter interface configuration mode.
Step 5	ip dhcp option {circuit-id	Configure dhcp option value.

	| policy | remote-id }	
Step 6	show ip dhcp relay helper-address	Verify your entries.
Step 7	Show ip dhcp relay option	Verify your entries.
Step 8	copy running-config startup-config	(Optional) Save your entries in the configuration file.

This example shows how to configure dhcp relay and option 82 :

```
Switch# configure terminal
Enter configuration commands, one per line.
Switch(config)# ip dhcp option
Switch(config)# interface fastethernet 0/18
Switch(config-if)# ip dhcp snooping information trust
Switch(config-if)# exit
Switch(config)# ip dhcp relay
Switch(config)# ip dhcp relay helper-address 192.168.1.1
Switch(config)# interface gigabitethernet 0/3
Switch(config-if)# switchport access vlan 2
Switch(config-if)# ip dhcp option circuit-id index 1 vlan-id 2 vlan 2
Switch(config-if)# exit
Switch(config)# ip dhcp remote-id 2222.2222.2222
Switch(config)# exit
Switch# show ip dhcp relay helper-address
Switch# show ip dhcp option gigabitethernet 0/3 circcuit-id
Switch# show ip dhcp server trust
Switch# show arp
```

Introduction to DHCP Packet Rate Limit

To prevent ARP attacks and attacks from unauthorized DHCP servers, ARP packets and DHCP packets will be processed by the switch CPU for validity checking. But, if attackers generate a large number of ARP packets or DHCP packets, the switch CPU will be under extremely heavy load. As a result, the switch cannot work normally and even goes down.

After DHCP packet rate limit is enabled on an Ethernet port, the switch counts the number of DHCP packets received on this port per

second. If the number of DHCP packets received per second exceeds the specified value, packets are passing the port at an over-high rate, which implies an attack to the port.
In this case, the switch shuts down this port so that it cannot receive any packet, thus protect the switch from attacks.

21 ARP Configuration

21.1 Introduction to ARP

ARP Function

Address Resolution Protocol (ARP) is used to resolve an IP address into a data link layer address.
An IP address is the address of a host at the network layer. To send a network layer packet to a destination host, the device must know the data link layer address (MAC address, for example) of the destination host or the next hop. To this end, the IP address must be resolved into the corresponding data link layer address.

ARP Message Format

ARP messages are classified as ARP request messages and ARP reply messages. Illustrates the format of these two types of ARP messages.
As for an ARP request, all the fields except the hardware address of the receiver field are set. The hardware address of the receiver is what the sender requests for.
As for an ARP reply, all the fields are set.

ARP Table

In an Ethernet, the MAC addresses of two hosts must be available for the two hosts to communicate with each other. Each host in an Ethernet maintains an ARP table, where the latest used IP address-to-MAC address mapping entries are stored. The switches provide the show arp command to display the information about ARP mapping entries.
ARP entries in the switch can either be static entries or dynamic entries, as described in.

Introduction to ARP Source MAC Address Consistency Check

An attacker may use the IP or MAC address of another host as the sender IP or MAC address of ARP packets. These ARP packets can cause other network devices to update the corresponding ARP entries incorrectly, thus interrupting network traffic.
To prevent such attacks, you can configure ARP source MAC address consistency check on the switches (operating as gateways). With this function, the device can verify whether an ARP packet is valid by checking the sender MAC address of the ARP packet against the source MAC address in the Ethernet header.

Introduction to ARP Attack Detection

Man-in-the-middle attack

According to the ARP design, after receiving an ARP response, a host adds the IP-to-MAC mapping of the sender into its ARP mapping table even if the MAC address is not the real one. This can reduce the ARP traffic in the network, but it also makes ARP spoofing possible.

ARP attack detection

To guard against the man-in-the-middle attacks launched by hackers or attackers, the switches support the ARP attack detection function. All ARP (both request and response) packets passing through the switch are redirected to the CPU, which checks the validity of all the ARP packets by using the DHCP snooping table or the manually configured IP binding table. For description of DHCP snooping table and the manually configured IP binding table, refer to the DHCP snooping section in the part discussing DHCP in this manual.
After you enable the ARP attack detection function, the switch will check the following items of an ARP packet: the source MAC address, source IP address, port number of the port receiving the ARP packet, and the ID of the VLAN the port resides. If these items match the entries of the DHCP snooping table or the manual configured IP binding table, the switch will forward the ARP packet; if not, the switch discards the ARP packet.

Introduction to ARP Packet Rate Limit

To prevent the man-in-the-middle attack, a switch enabled with the ARP attack detection function delivers ARP packets to the CPU to check the validity of the packets. However, this causes a new problem: If an attacker sends a large number of ARP packets to a port of a switch, the CPU will get overloaded, causing other functions to fail, and even the whole device to break down. To guard against such attacks, the switches support the ARP packets rate limit function, which will shut down the attacked port, thus preventing serious impact on the CPU.

With this function enabled on a port, the switch will count the ARP packets received on the port within each second. If the number of ARP packets received on the port per second exceeds the preconfigured value, the switch considers that the port is attacked by ARP packets. In this case, the switch will shut down the port. As the port does not receive any packet, the switch is protected from the ARP packet attack.

At the same time, the switch supports automatic recovery of port state. If a port is shut down by the switch due to high packet rate, the port will revert to the Up state after a configured period of time.

21.1.1 Configuring ARP Packet Rate Limit

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface *interface-id*	Specify the port to configure, and enter interface configuration mode.
Step 3	arp-rate-limit *value*	Configure dhcp pakcket rate-limit.
Step 4	show arp-rate-limit	Verify your entries.
Step 5	copy running-config startup-config	(Optional) Save your entries in the configuration file.

This example shows how to configure arp packet rate-limit on a port :

```
Switch# configure terminal
Enter configuration commands, one per line.
Switch(config)# interface fastethernet 0/1
Switch(config-if)# arp-rate-limit 5
Switch(config-if)# exit
Switch(config)# exit
Switch# show arp-rate-limit
```

21.1.2 Configuring ARP Filtering

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	Interface *interface-id*	Specify the port to configure, and enter interface configuration mode.
Step 3	arp filter	Configure arp filter on port.
Step 4	show arp filter	Verify your entries.
Step 5	copy running-config startup-config	(Optional) Save your entries in the configuration file.

This example shows how to configure arp filter on a port :

```
Switch# configure terminal
Enter configuration commands, one per line.
Switch(config)# interface fastethernet 0/1
Switch(config-if)# arp filter
Switch(config-if)# exit
Switch(config)# exit
Switch# show arp filter
```

21.1.3 Configuring IP Filtering

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface *interface-id*	Specify the port to configure, and enter interface configuration mode.
Step 3	ip filter	Configure ip filter on port.
Step 4	show ip filter	Verify your entries.
Step 5	copy running-config startup-config	(Optional) Save your entries in the configuration file.

This example shows how to configure ip filter on a port :

```
Switch# configure terminal
Enter configuration commands, one per line.
Switch(config)# interface fastethernet 0/1
Switch(config-if)# ip filter
Switch(config-if)# exit
Switch(config)# exit
Switch# show ip filter
```

22 802.1x Overview

22.1 Introduction to 802.1x

The 802.1x protocol (802.1x for short) was developed by IEEE802 LAN/WAN committee to address security issues of wireless LANs. It was then used in Ethernet as a common access control mechanism for LAN ports to address mainly authentication and security problems.

802.1x is a port-based network access control protocol. It authenticates and controls devices requesting for access in terms of the ports of LAN access devices. With the 802.1x protocol employed, a user-side device can access the LAN only when it passes the authentication. Those fail to pass the authentication are denied when accessing the LAN.

Architecture of 802.1x Authentication

As shown in Figure 1-1, 802.1x adopts a client/server architecture with three entities: a supplicant system, an authenticator system, and an authentication server system.

- The supplicant system is an entity residing at one end of a LAN segment and is authenticated by the authenticator system at the other end of the LAN segment. The supplicant system is usually a user terminal device. An 802.1x authentication is triggered when a user launches client program on the supplicant system. Note that the client program must support the extensible authentication protocol over LAN (EAPoL).
- The authenticator system is another entity residing at one end of a LAN segment. It authenticates the connected supplicant systems. The authenticator system is usually an 802.1x-supported network device. It provides the port (physical or logical) for the supplicant system to access the LAN.
- The authentication server system is an entity that provides authentication service to the authenticator system. Normally in the form of a RADIUS server, the authentication server system serves to perform AAA (authentication, authorization, and accounting) services to users. It also stores user information, such as user name, password, the VLAN a user belongs to, priority, and

the ACLs (access control list) applied.

- The four basic concepts related to the above three entities are PAE, controlled port and uncontrolled port, the valid direction of a controlled port and the way a port is controlled.

PAE

A PAE (port access entity) is responsible for implementing algorithms and performing protocol-related operations in the authentication mechanism.

- The authenticator system PAE authenticates the supplicant systems when they log into the LAN and controls the status (authorized/unauthorized) of the controlled ports according to the authentication result.
- The supplicant system PAE responds to the authentication requests received from the authenticator system and submits user authentication information to the authenticator system. It also sends authentication requests and disconnection requests to the authenticator system PAE.

Controlled port and uncontrolled port

The Authenticator system provides ports for supplicant systems to access a LAN. Logically, a port of this kind is divided into a controlled port and an uncontrolled port.

- The uncontrolled port can always send and receive packets. It mainly serves to forward EAPoL packets to ensure that a supplicant system can send and receive authentication requests.
- The controlled port can be used to pass service packets when it is in authorized state. It is blocked when not in authorized state. In this case, no packets can pass through it.
- Controlled port and uncontrolled port are two properties of a port. Packets reaching a port are visible to both the controlled port and uncontrolled port of the port.

The valid direction of a controlled port

When a controlled port is in unauthorized state, you can configure it to be a unidirectional port, which sends packets to supplicant systems only.

By default, a controlled port is a unidirectional port.

The way a port is controlled

A port of the switch can be controlled in the following two ways.

- Port-based authentication. When a port is controlled in this way, all the supplicant systems connected to the port can access the network without being authenticated after one supplicant system among them passes the authentication. And when the authenticated supplicant system goes offline, the others are denied as well.
- MAC address-based authentication. All supplicant systems connected to a port have to be authenticated individually in order to access the network. And when a supplicant system goes offline, the others are not affected.

The Mechanism of an 802.1x Authentication System

IEEE 802.1x authentication system uses the extensible authentication protocol (EAP) to exchange information between supplicant systems and the authentication servers.

- EAP protocol packets transmitted between the supplicant system PAE and the authenticator system PAE are encapsulated as EAPoL packets.
- EAP protocol packets transmitted between the authenticator system PAE and the RADIUS server can either be encapsulated as EAP over RADIUS (EAPoR) packets or be terminated at system PAEs. The system PAEs then communicate with RADIUS servers through password authentication protocol (PAP) or challenge-handshake authentication protocol (CHAP) packets.
- When a supplicant system passes the authentication, the authentication server passes the information about the supplicant system to the authenticator system. The authenticator system in turn determines the state (authorizedor unauthorized) of the controlled port according to the instructions (accept or reject) received from the RADIUS server.

22.1.1 Configuring IEEE 802.1x Authentication base on local

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	dot1x system-auth-control	Enable 802.1x authentication.
Step 3	dot1x auth-mode { local | radius }	Configure 802.1x authentication mode.
Step 4	dot1x local-userInfo *user-name password*	Configure 802.1x user-name and password of local authentication.
Step 5	show dot1x	Verify your entries.
Step 6	copy running-config startup-config	(Optional) Save your entries in the configuration file.

This example shows how to configure 802.1x authentication base on local :

```
Switch# configure terminal
Enter configuration commands, one per line.
Switch(config)# dot1x system-auth-control
Switch(config)# dot1x auth-mode local
Switch(config)# dot1x local-userInfo public public
Switch(config)# exit
Switch# show dot1x
Switch# show dot1x local-user
Switch# show statistics
```

22.1.2 Configuring IEEE 802.1x Authentication base on radius

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	dot1x system-auth-control	Enable 802.1x authentication.
Step 3	dot1x auth-mode { local | radius }	Configure 802.1x authentication mode.
Step 4	Radius-server { host [*ip-address* { acct-port *port-number* | auth-port *port-number* }] | key *key-vaule*}	Configure 802.1x user-name and password of radius authentication.
Step 5	interface *interface-id*	Specify the port to configure, and enter interface configuration mode.

Step 6	dot1x port-control force-authorized	Configure a port is force-authorized port.
Step 7	show dot1x	Verify your entries.
Step 8	copy running-config startup-config	(Optional) Save your entries in the configuration file.

This example shows how to configure 802.1x authentication base on radius :

```
Switch# configure terminal
Enter configuration commands, one per line.
Switch(config)# dot1x system-auth-control
Switch(config)# dot1x auth-mode radius
Switch(config)# radius-server host 192.168.2.12 acct-port 1813
Switch(config)# radius-server host 192.168.2.12 auth-port 1812
Switch(config)# radius-server key 12345678
Switch(config)# interface gigabitethernet 0/1
Switch(config-if)# dot      1x port-control force-authorized
Switch(config-if)# exit
Switch(config)# exit
Switch# show dot1x
Switch# show radius information
Switch# show statistics
```

23 STP Configuration

23.1 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.

23.2 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 toan 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

23.2.1 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	configure terminal	Enter global configuration mode.
Step 2	spanning-tree	Enable spanning-tree
Step 3	spanning-tree force-version { 0 | 1 | 2 }	Configure Spanning tree operating mode. 0: Spanning tree protolol(STP) 1: Rapid spanning tree protocol(RSTP) 2: 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# configure terminal
Enter configuration commands, one per line.
Switch(config)# spanning-tree
Switch(config)# spanning-tree force-version 2
Switch(config)# exit
Switch# show spanning-tree
```

23.2.2 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	configure terminal	Enter global configuration mode.
Step 2	interface *interface-id*	Specify an interface to configure, and enter interfaceconfiguration 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 mst instance-id priority interface configuration command.

23.2.3 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	configure terminal	Enter global configuration mode.
Step 2	interface *interface-id*	Specify an interface to configure, and enter interface configuration mode.
Step 3	spanning-tree mst	Configure the cost for an MST instance.

	instance-id cost *cost*	
Step 4	show spanning-tree interface *interface-id* cost	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 mst instance-id cost interface configuration command.

23.2.4 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	configure terminal	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	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 mst instance-id priority global configuration command.

23.2.5 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	configure terminal	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	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 mst hello-time global configuration command.

23.2.6 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	configure terminal	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	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 mst forward-time global configuration command.

23.2.7 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	configure terminal	Enter global configuration mode.
Step 2	spanning-tree mst max-age *seconds*	Configure the maximum-aging time for all MST instances.
Step 3	show spanning-tree mst	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 mst max-age global configuration command.

23.2.8 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 terminal	Enter global configuration mode.
Step 2	spanning-tree mst 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	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 mst max-hops global configuration Command

24 Configuring SNMP

24.1 Understanding SNMP

SNMP is an application-layer protocol that provides a message format for communication between managers and agents. The SNMP system consists of an SNMP manager, an SNMP agent, and a MIB. The SNMP manager can be part of a network management system (NMS) such as CiscoWorks. The agent and MIB reside on the switch. To configure SNMP on the switch, you define the relationship between the manager and the agent.

The SNMP agent contains MIB variables whose values the SNMP manager can request or change. A manager can get a value from an agent or store a value into the agent. The agent gathers data from the MIB, the repository for information about device parameters and

network data. The agent can also respond to a manager's requests to get or set data.
An agent can send unsolicited traps to the manager. Traps are messages alerting the SNMP manager to a condition on the network. Traps can mean improper user authentication, restarts, link status (up or down), MAC address tracking, closing of a TCP connection, loss of connection to a neighbor, or other significant events.

SNMP Versions

This software release supports these SNMP versions:

- SNMPv1—The Simple Network Management Protocol, a Full Internet Standard, defined in RFC 1157.
- SNMPv2C replaces the Party-based Administrative and Security Framework of SNMPv2Classic with the community-string-based Administrative Framework of SNMPv2C while retaining the bulk retrieval and improved error handling of SNMPv2Classic. It has these features:
- – SNMPv2—Version 2 of the Simple Network Management Protocol, a Draft Internet Standard, defined in RFCs 1902 through 1907.
- – SNMPv2C—The community-string-based Administrative Framework for SNMPv2, an
- Experimental Internet Protocol defined in RFC 1901.
- SNMPv3—Version 3 of the SNMP is an interoperable standards-based protocol defined in RFCs 2273 to 2275. SNMPv3 provides secure access to devices by authenticating and encrypting packets over the network and includes these security features:
- – Message integrity—ensuring that a packet was not tampered with in transit
- – Authentication—determining that the message is from a valid source
- – Encryption—mixing the contents of a package to prevent it from being read by an unauthorized source.

Both SNMPv1 and SNMPv2C use a community-based form of security. The community of managers able to access the agent's MIB is defined by an IP address access control list and password. SNMPv2C includes a bulk retrieval mechanism and more detailed error message reporting to management stations. The bulk retrieval

mechanism retrieves tables and large quantities of information, minimizing the number of round-trips required. The SNMPv2C improved error-handling includes expanded error codes that distinguish different kinds of error conditions; these conditions are reported through a single error code in SNMPv1. Error return codes in SNMPv2C report the error type.
SNMPv3 provides for both security models and security levels. A security model is an authentication strategy set up for a user and the group within which the user resides. A security level is the permitted level of security within a security model. A combination of the security level and the security model determine which security mechanism is used when handling an SNMP packet. Available security models are SNMPv1, SNMPv2C, and SNMPv3.

SNMP Security Models and Levels as follow:

Model	Level	Authentication	Result
SNMPv1	noAuthNoPriv	Community	Uses a community string match for authentication.
SNMPv2C	noAuthNoPriv	Community	Uses a community string match for authentication.
SNMPv3	noAuthNoPriv	Username	Uses a username match for authentication.
SNMPv3	authNoPriv	MD5	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms.
SNMPv3 authPriv	authPriv (requires the cryptographic software image)	MD5 or SHA	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms. Provides DES 56-bit encryption in addition to authentication based on the CBC-DES (DES-56) standard.

You must configure the SNMP agent to use the SNMP version supported by the management station.
Because an agent can communicate with multiple managers, you can configure the software to support communications using SNMPv1,

SNMPv2C, or SNMPv3.

SNMP Community Strings

SNMP community strings authenticate access to MIB objects and function as embedded passwords. In order for the NMS to access the switch, the community string definitions on the NMS must match at least one of the three community string definitions on the switch.
A community string can have one of these attributes:

- Read-only (RO)—Gives read access to authorized management stations to all objects in the MIB except the community strings, but does not allow write access
- Read-write (RW)—Gives read and write access to authorized management stations to all objects in the
- MIB, but does not allow access to the community strings

SNMP Notifications

SNMP allows the switch to send notifications to SNMP managers when particular events occur. SNMP notifications can be sent as traps or inform requests. In command syntax, unless there is an option in the command to select either traps or informs, the keyword traps refers to either traps or informs, or both.
Use the snmp-server host command to specify whether to send SNMP notifications as traps or informs.
Traps are unreliable because the receiver does not send an acknowledgment when it receives a trap, and the sender cannot determine if the trap was received. When an SNMP manager receives an inform request, it acknowledges the message with an SNMP response protocol data unit (PDU). If the sender does not receive a response, the inform request can be sent again. Because they can be re-sent, informs are more likely than traps to reach their intended destination.
The characteristics that make informs more reliable than traps also consume more resources in the switch and in the network. Unlike a trap, which is discarded as soon as it is sent, an inform request is held in memory until a response is received or the request times out. Traps are sent only once, but an inform might be re-sent or retried several times. The retries increase traffic and contribute to a higher overhead on the network. Therefore, traps and informs require a

trade-off between reliability and resources. If it is important that the SNMP manager receive every notification, use inform requests. If traffic on the network or memory in the switch is a concern and notification is not required, use traps.

24.1.1 Configuring Community Strings

You use the SNMP community string to define the relationship between the SNMP manager and the agent. The community string acts like a password to permit access to the agent on the switch.

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	Snmp-server	Enable the SNMP agent operation.
Step 3	snmp-server community {v1|v2c}*string* {ro | rw} {A.B.C.D *ip-address|* default|subnet} *oid-number*	Configure the community string.
Step 4	show snmp	Verify your entries.
Step 5	copy running-config startup-config	(Optional) Save your entries in the configuration file.

To remove a specific community string, use the no snmp-server community global configuration command.

This example shows how to assign the string private to SNMP, to allow read-write access.

```
Switch# configure terminal
Enter configuration commands, one per line.
Switch(config)# snmp-server
Switch(config)# snmp-server community rw private default 1.3.6
Switch(config)# exit
Switch# show snmp
```

24.1.2 Configuring SNMP Groups and Users

You can specify an identification name (engineID) for the local or remote SNMP server engine on the switch. You can configure an SNMP server group that maps SNMP users to SNMP views, and you can add new users to the SNMP group.

Beginning in privileged EXEC mode, follow these steps to configure SNMP on the switch:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	Snmp-server	Enable the SNMP agent operation.
Step 3	snmp-server view *view-name OID* [included | exclude]	Configure the view of snmp.
Step 4	snmp-server group *group-name* v3 [auth | noauth | priv] {read | write } *view-name*	Configure the snmp group on the device.
Step 5	snmp-server user *user-name group-name* v3 { auth [md5 | sha]}	Configure the snmp user on the device.
Step 6	show snmp-server group	Verify your entries.
Step 7	show snmp-server user	Verify your entries.
Step 8	show snmp-server security	Verify your entries.
Step 9	show snmp-server view	Verify your entries.
Step 10	copy running-config startup-config	(Optional) Save your entries in the configuration file.

To remove a specific community string, use the no snmp-server group string and no snmp-server user string global configuration command.

This example shows how to associate a user with a remote host and to send priv (authPriv) authentication-level informs when the user enters global configuration mode:

```
Switch# configure terminal
Enter configuration commands, one per line.
Switch(config)# snmp-server
Switch(config)# snmp-server view kkk 1.3.6 included
Switch(config)# snmp-server group qwerty v3 priv read kkk write kkk
Switch(config)# snmp-server user abc qwerty v3 auth md5
Switch(config)# exit
Switch# show snmp group
```

```
Switch# show snmp user
Switch# show snmp security
Switch# show snmp view
```

24.1.3 Setting the and Agent Contact and Location Information

Beginning in privileged EXEC mode, follow these steps to set the system contact and location of the SNMP agent so that these descriptions can be accessed through the configuration file:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	Snmp-server	Enable the SNMP agent operation.
Step 3	snmp-server contact *test*	Set the system contact string.
Step 4	snmp-server location *test*	Set the system location string.
Step 5	snmp-server system-name *test*	Set the system name string.
Step 6	show snmp	Verify your entries.
Step 7	copy running-config startup-config	(Optional) Save your entries in the configuration file.

This example shows how to assign the string to SNMP contact, location and system-name.

```
Switch# configure terminal
Enter configuration commands, one per line.
Switch(config)# snmp-server
Switch(config)# snmp-server contact Kevin
Switch(config)# snmp-server location Shenzhen-China
Switch(config)# snmp-server system-name switch1
Switch(config)# exit
Switch# show snmp
```

25 Configuring IGMP Snooping and MVR

This chapter describes how to configure Internet Group Management Protocol (IGMP) snooping, including an application of local IGMP snooping, Multicast VLAN Registration (MVR). It also includes procedures for controlling multicast group membership by using IGMP filtering and procedures for configuring the IGMP throttling action.

25.1 Understanding IGMP Snooping

Layer 2 switches can use IGMP snooping to constrain the flooding of multicast traffic by dynamically configuring Layer 2 interfaces so that multicast traffic is forwarded to only those interfaces associated with IP multicast devices. As the name implies, IGMP snooping requires the LAN switch to snoop on the IGMP transmissions between the host and the router and to keep track of multicast groups and member ports. When the switch receives an IGMP report from a host for a particular multicast group, the switch adds the host port number to the forwarding table entry; when it receives an IGMP Leave Group message from a host, it removes the host port from the table entry. It also periodically deletes entries if it does not receive IGMP membership reports from the multicast clients.

The multicast router sends out periodic IGMP general queries to all VLANs. When IGMP snooping is enabled, the switch responds to the router queries with only one join request per MAC multicast group, and the switch creates one entry per VLAN in the Layer 2 forwarding table for each MAC group from which it receives an IGMP join request. All hosts interested in this multicast traffic send join requests and are added to the forwarding table entry.

Layer 2 multicast groups learned through IGMP snooping are dynamic. However, you can statically configure MAC multicast groups by using the ip igmp snooping vlan static global configuration command. If you specify group membership for a multicast group address statically, your setting supersedes any automatic manipulation by IGMP snooping. Multicast group membership lists can consist of both user-defined and IGMP snooping-learned settings.

IGMP Versions

The switch supports IGMP version 1, IGMP version 2, and IGMP version 3. These versions are interoperable on the switch. For example, if IGMP snooping is enabled on an IGMPv2 switch and the switch receives an IGMPv3 report from a host, the switch can forward the IGMPv3 report to the multicast router.

Joining a Multicast Group

When a host connected to the switch wants to join an IP multicast group, it sends an unsolicited IGMP join message, specifying the IP multicast group to join. Alternatively, when the switch receives a general query from the router, it forwards the query to all ports in the VLAN. Hosts wanting to join the multicast group respond by sending a join message to the switch. The switch CPU creates a multicast forwarding-table entry for the group if it is not already present. The CPU also adds the interface where the join message was received to the forwarding-table entry. The host associated with that interface receives multicast traffic for that multicast group.

Leaving a Multicast Group

The router sends periodic multicast general queries and the switch forwards these queries through all ports in the VLAN. Interested hosts respond to the queries. If at least one host in the VLAN wishes to receive multicast traffic, the router continues forwarding the multicast traffic to the VLAN. The switch forwards multicast group traffic to only those hosts listed in the forwarding table for that Layer 2 multicast group.

When hosts want to leave a multicast group, they can either silently leave, or they can send a leave message. When the switch receives a leave message from a host, it sends out a MAC-based general query to determine if any other devices connected to that interface are interested in traffic for the specific multicast group. The switch then updates the forwarding table for that MAC group so that only those hosts interested in receiving multicast traffic for the group are listed in the forwarding table. If the router receives no reports from a VLAN, it removes the group for the VLAN from its IGMP cache.

Immediate-Leave Processing

Immediate Leave is only supported with IGMP version 2 hosts.

The switch uses IGMP snooping Immediate-Leave processing to remove from the forwarding table an interface that sends a leave message without the switch sending MAC-based general queries to the interface. The VLAN interface is pruned from the multicast tree for the multicast group specified in the original leave message. Immediate-Leave processing ensures optimal bandwidth management for all hosts on a switched network, even when multiple multicast groups are simultaneously in use.

IGMP Report Suppression

The switch uses IGMP report suppression to forward only one IGMP report per multicast router query to multicast devices. When IGMP router suppression is enabled (the default), the switch sends the first IGMP report from all hosts for a group to all the multicast routers. The switch does not send the remaining IGMP reports for the group to the multicast routers. This feature prevents duplicate reports from being sent to the multicast devices.

If the multicast router query includes requests only for IGMPv1 and IGMPv2 reports, the switch forwards only the first IGMPv1 or IGMPv2 report from all hosts for a group to all the multicast routers. If the multicast router query also includes requests for IGMPv3 reports, the switch forwards all IGMPv1,

IGMPv2, and IGMPv3 reports for a group to the multicast devices.

If you disable IGMP report suppression, all IGMP reports are forwarded to the multicast routers.

25.2 Configuring IGMP Snooping

IGMP snooping allows switches to examine IGMP packets and make forwarding decisions based on their content.

Enabling or Disabling IGMP Snooping

By default, IGMP snooping is globally enabled on the switch.

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	ip igmp snooping vlan *vlan-id*	Enable IGMP snooping based on vlan.
Step 3	copy running-config startup-config	(Optional) Save your entries in the configuration file.

Configuring a Multicast Router Port

To add a multicast router port (add a static connection to a multicast router), use the ip igmp snooping vlan mrouter global configuration command on the switch.

Beginning in privileged EXEC mode, follow these steps to enable a static connection to a multicast router:

	Command	**Purpose**
Step 1	configure terminal	Enter global configuration mode.
Step 2	ip igmp snooping mrouter interface *interface-id* vlan *vlan-id*	Specify the multicast router VLAN ID and specify the interface to the multicast router. The VLAN ID range is 1 to 4094.
Step 3	show ip igmp snooping mrouter	Verify that IGMP snooping is enabled on the VLAN interface.
Step 4	copy running-config startup-config	(Optional) Save your entries in the configuration file.

To remove a multicast router port from the VLAN, use the no ip igmp snooping mrouter interface interface-id vlan vlan-id global configuration command.

This example shows how to enable a static connection to a multicast router and verify the configuration:

```
Switch# configure terminal
Enter configuration commands, one per line.
Switch(config)# ip igmp snooping mrouter interface gigabitethernet0/1 vlan 200
Switch(config)# exit
Switch# show ip igmp snooping mrouter
```

Enabling IGMP Immediate-Leave Processing

When you enable IGMP Immediate-Leave processing, the switch immediately removes a port when it detects an IGMP version 2 leave message on that port. You should use the Immediate-Leave feature only when there is a single receiver present on every port in the VLAN.

Immediate Leave is supported with only IGMP version 2 hosts.

Beginning in privileged EXEC mode, follow these steps to enable IGMP Immediate-Leave processing:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	ip igmp snooping immediate-leave	Enable IGMP immediate-leave on the switch.
Step 3	show ip igmp snooping	Verify your entries.
Step 4	copy running-config startup-config	(Optional) Save your entries in the configuration file.

25.3 Understanding Multicast VLAN Registration

Multicast VLAN Registration (MVR) is designed for applications using wide-scale deployment of multicast traffic across an Ethernet ring-based service provider network (for example, the broadcast of multiple television channels over a service-provider network). MVR allows a subscriber on a port to subscribe and unsubscribe to a multicast stream on the network-wide multicast VLAN. It allows the single multicast VLAN to be shared in the network while subscribers remain in separate VLANs. MVR provides the ability to continuously send multicast streams in the multicast VLAN, but to isolate the streams from the subscriber VLANs for bandwidth and security reasons.

MVR assumes that subscriber ports subscribe and unsubscribe (join and leave) these multicast streams by sending out IGMP join and leave messages. These messages can originate from an IGMP version-2-compatible host with an Ethernet connection. Although MVR operates on the underlying mechanism of IGMP snooping, the two features operate independently of each other. One can be enabled or disabled without affecting the behavior of the other feature. However, if IGMP snooping and MVR are both enabled, MVR reacts only to join and leave messages from multicast groups configured under MVR. Join and leave messages from all other multicast groups are managed by IGMP snooping.

The switch CPU identifies the MVR IP multicast streams and their associated MAC addresses in the switch forwarding table, intercepts the IGMP messages, and modifies the forwarding table to include or remove the subscriber as a receiver of the multicast stream, even though the receivers might be in a different VLAN from the source.

This forwarding behavior selectively allows traffic to cross between different VLANs.

25.4 Configuring MVR

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	ip igmp snooping vlan *vlan-id*	Enable IGMP snooping based on vlan.
Step 3	ip igmp snooping mrouter interface *interface-id* vlan *vlan-id*	Specify the multicast router VLAN ID and specify the interface to the multicast router. The VLAN ID range is 1 to 4094.
Step 4	ip igmp snooping cross-vlan *vlanid*	Configure IGMP MVR.
Step 5	show ip igmp snooping	Verify your entries.
Step 6	copy running-config startup-config	(Optional) Save your entries in the configuration file.

This example shows how to enable MVR, specify the MVR multicast VLAN as VLAN 2, and verify the results:

```
Switch# configure terminal
Enter configuration commands, one per line.
Switch(config)# interface fastethernet 0/1
Switch(config-if)# switchport access vlan 2
Switch(config-if)# exit
Switch(config)# interface fastethernet 0/2
Switch(config-if)# switchport access vlan 4
Switch(config-if)# exit
Switch(config)# exit
Switch# show vlan

VID    VLAN_Name             Tagged_Ports                          Untagged_Ports
--------------------------------------------------------------------------------
 1      default vlan                                              Fa 0/3    Fa 0/4    Fa 0/5
                                                                     Fa 0/6    Fa 0/7    Fa 0/8
                                                                     Fa 0/9    Fa 0/10 Fa 0/11
                                                                     Fa 0/12 Fa 0/13 Fa 0/14
```

```
                                                              Fa 0/15 Fa 0/16 Fa 0/17
                                                              Fa 0/18 Fa 0/19 Fa 0/20
                                                              Fa 0/21 Fa 0/22 Fa 0/23
                                                              Fa 0/24 Gi 0/1    Gi 0/2
 2      Vlan2                                                Fa 0/1
 4      Vlan4                                                Fa 0/2
```

```
Switch# configure terminal
Enter configuration commands, one per line.
Switch(config)# ip igmp snooping
Switch(config)# ip igmp snooping cross-vlan 2
Switch(config)# ip igmp snooping mrouter interface fastethernet 0/1 cross-vlan untaged
Switch(config)# exit
Switch# show ip igmp snooping mrouter

Interface          Vid          VlanName          Type          State          EgressRule
-----------------------------------------------------------------
Fa 0/1               2               cross-vlan        Static      inactive      untagged

Switch# show ip igmp snooping
IGMP snooping
---------------
IGMP snooping is globally Enable
IGMP snooping immediate-leave is Enable
IGMP snooping forward-all-leave is Disable
IGMP snooping forward-unknown-multicast is Enable
IGMP snooping send general query timer is 10 seconds
IGMP snooping member aged timer is 260 seconds
IGMP snooping dynamic router port aged timer is 260 seconds
IGMP snooping cross vlan is 2
IGMP snooping received packet is 11
NO      Multicast group Interface Vid Version Filter-Mode Source-Hosts Source Expiry-Time
---------------------------------------------------------------------------------------
1       226.1.1.1       Fa 0/1                2         3           Include               N/A
N/A
1       226.1.1.1       Fa 0/2                2         3           Include             192.168.2.66
182
```

26 QinQ Configuration

26.1 Selective QinQ Overview

Selective QinQ is an enhanced application of the VLAN-VPN feature. With the selective QinQ feature, you can configure inner-to-outer VLAN tag mapping, according to which you can add different outer VLAN tags to the packets with different inner VLAN tags.

The selective QinQ feature makes the service provider network structure more flexible. You can classify the terminal users on the port connecting to the access layer device according to their VLAN tags, and add different outer VLAN tags to these users. In the public network, you can configure QoS policies based on outer VLAN tags to assign different priorities to different packets, thus providing differentiated services.

In this way, you can configure different forwarding policies for data of different type of users, thus improving the flexibility of network management. On the other hand, network resources are well utilized, and users of the same type are also isolated by their inner VLAN tags. This helps to improve network security.

26.2 Configuring QinQ

	Command	**Purpose**
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface *interface-id*	Specify the port to configure, and enter interface configuration mode.
Step 3	qinq {enable| flexible-qinq|tx}	Enable is Enable basic qinq for ingress port, flexible-qinq is enable selective qinq for ingress port, tx is enable qinq for egress port
Step 4	qinq outbound *vlan-id* inbound *vlan-id*	Configure the interface selective qinq entries for egress port.
Step 5	show qinq	Verify your entries.
Step 6	copy running-config startup-config	(Optional) Save your entries in the configuration file.

```
Switch# configure terminal
Enter configuration commands, one per line.
Switch(config)# interface fastethernet 0/1
Switch(config-if)#    qinq enable
Switch(config-if)# exit
Switch(config) # exit
Switch# show    qinq
```

27 PoE

27.1 PoE Overview

Introduction to PoE

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

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, 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.

27.2 Configuring PoE

Configuring the PoE Interface

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface *interface-id*	Specify the port to configure, and enter interface configuration mode.
Step 3	poe status auto	Enable PoE function of ports.

Step 4	poe status never	Disable PoE function of ports.
Step 5	show interface poe	Verify your entries.
Step 6	show poe status	Verify your entries.
Step 7	copy running-config startup-config	(Optional) Save your entries in the configuration file.

Follow these steps to configure a PoE interface through the command line:

```
Switch# configure terminal
Enter configuration commands, one per line.
Switch(config)# interface fastethernet 0/1 – 0/24
Switch(config-if-Range)# poe status never
Switch(config-if-Range)# poe status auto
Switch(config-if-Range)# exit
Switch(config)# exit
Switch# show interface poe
Switch# show poe status
```

Configuring the PoE Priority

The PoE priority of a equipment depends on the priority of the PoE interface. The priority levels of PoE interfaces include critical, high and low in descending order. Power supply to a equipment is subject to equipment priority management policies, all power-sourcing-equipment implement the same equipment priority management policies. When the power-sourcing-equipment supplies power to a equipment.

- By default, no power will be supplied to a new equipment if the power-sourcing-equipment power is overloaded.
- Under the control of a priority policy, the equipment with a lower priority is first powered off to guarantee the power supply to the new equipment with a higher priority when the power-sourcing-equipment power is overloaded.

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface *interface-id*	Specify the port to configure, and enter interface configuration mode.

Step 3	poe priority {critical | high | low}	Configuring the PoE priority of interface.
Step 4	show interface poe	Verify your entries.
Step 5	copy running-config startup-config	(Optional) Save your entries in the configuration file.

Follow these steps to configure PoE priority of port 1.

```
Switch# configure terminal
Enter configuration commands, one per line.
Switch(config)# interface fastethernet 0/1
Switch(config-if)# poe priority critical
Switch(config-if)# exit
Switch(config)# exit
Switch# show interface poe
```

Configuring the PoE Classification

	Command	**Purpose**
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface *interface-id*	Specify the port to configure, and enter interface configuration mode.
Step 3	poe classification {auto | disable}	Configuring the PoE classification of interface.
Step 4	show interface poe	Verify your entries.
Step 5	copy running-config startup-config	(Optional) Save your entries in the configuration file.

Follow these steps to configure power classification of port 1.

```
Switch# configure terminal
Enter configuration commands, one per line.
Switch(config)# interface fastethernet 0/1
Switch(config-if)# poe priority critical
Switch(config-if)# exit
Switch(config)# exit
Switch# show interface poe
```

Configuring the PoE Port-force

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface *interface-id*	Specify the port to configure, and enter interface configuration mode.
Step 3	poe portforceon	Configuring the PoE port-force function.
Step 4	show poe portforceon	Verify your entries.
Step 5	show interface poe	Verify your entries.
Step 6	copy running-config startup-config	(Optional) Save your entries in the configuration file.

Follow these steps to configure PoE port-force of port 1.

```
Switch# configure terminal
Enter configuration commands, one per line.
Switch(config)# interface fastethernet 0/1
Switch(config-if)# poe poe portforceon
Switch(config-if)# exit
Switch(config)# exit
Switch# show poe portforceon
Switch# show interface poe
```

28 RRPP

28.1 RRPP Overview

Rapid Ring Protection Protocol (RRPP) is an Ethernet ring-specific link layer protocol. Itcan not only prevent data loop from causing broadcast storm efficiently when the Ethernet ring is complete, but also restore communication channels among nodes on the Ethernet ring rapidly when a link is torn down.

Compared with Spanning Tree Protocol (STP), RRPP features：

- Expedited topology convergence
- Independent of the number of nodes on the Ethernet ring

Basic Concepts in RRPP

Primary port and secondary port

Each master node or transit node has two ports accessing an RRPP ring, in which one serves as the primary port and the other serves as the secondary port. You can determine the role of a port.

1) In terms of functionality, the difference between the primary port and the secondary port of a master node is:

- The primary port and the secondary port are designed to play the role of sending and receiving loop-detect packets respectively.
- When an RRPP ring is in health state, the secondary port of the master node will logically deny data VLANs and permit only the packets of the control VLANs.
- When an RRPP ring is in disconnect state, the secondary port of the master node will permit data VLANs, that is, forward packets of data VLANs.

2) In terms of functionality, there is no difference between the primary port and the secondary port of the transit node. Both are designed for the transfer of protocol packets and data packets over an RRPP ring.

Timers

The master node uses two timers to send and receive RRPP packets: the Hello timer and the Fail timer.

- The Hello timer is used for the primary port to send Health packets.
- The Fail timer is used for the secondary port to receive Health packets from the master node.

If the secondary port receives the Health packets before the Fail timer expires, the overall ring is in health state. Otherwise, the ring transits into disconnect state until the secondary port receives the Health packet again.

28.2 How RRPP Works

Polling mechanism

The primary port of the master node sends Health packets across the control VLAN periodically.

- If the ring works properly, the secondary port of the master node will receive Health packets and the master node will maintain it in block state.
- If the ring is torn down, the secondary port of the master node will not receive Health packets after the timeout timer expires. The master node will release the secondary port from blocking data VLAN while sending Common-Flush-FDB packets to notify all transit nodes to update their own MAC entries and ARP entries.

Link down alarm mechanism

The transit node, the edge node or the assistant edge node sends Link-Down packets to the master node immediately when they find any port belonging to an RRPP domain is down. Upon the receipt of a Link-Down packet, the master node releases the secondary port from blocking data VLAN while sending Common-Flush-FDB packet to notify all the transit nodes, the edge nodes and the assistant nodes to update their own MAC entries and ARP entries.

Ring recovery

The master node may find the ring is restored after a period of time after the ports belonging to the RRPP domain on the transit node, the edge node or the assistant edge node are up again. A temporary loop may arise in the data VLAN in this period. As a result, broadcast storm occurs.

To prevent temporary loops, non-master nodes block them immediately (and permits only the packets of the control VLAN) when they find their ports accessing the ring are up again. The blocked ports are activated only when the nodes ensure that no loop will be brought forth by these ports.

28.3 Configuring Master Node

Follow these steps to configure master node:

	Command	***Purpose***
Step 1	configure terminal	Enter global configuration mode.
Step 2	rrpp domain *number*	Create an RRPP domain and enter its view.
Step 3	ring *ring-id* node-role master primary-port interface *interface-id* secondary-port *interface-id* control-vlan *vlan-id*	Specify the current device as the master node of the ring, and specify the primary port and the secondary port. Specify control VLAN for the RRPP domain.
Step 4	rrpp	Enable the RRPP ring
Step 5	show rrpp	Verify your entries.
Step 6	copy running-config startup-config	(Optional) Save your entries in the configuration file.

Follow these steps to configure rrpp.

```
Switch# configure terminal
Enter configuration commands, one per line.
Switch(config)# rrpp domain 1
Rrpp domain 1
Switch(rrpp-domain)# ring 1 node-role master   primary-port   in gigabitethernet   0/1
secondary-port   gigabitethernet 0/2 control-vlan 2
switch(rrpp-domain)# rrpp
switch(rrpp-domain)# exit
switch(config)# exit
switch# show rrpp

Rrpp status: Enable
Ring status: Active
Domain id: 1
Ring id: 1
Hello timer:   1
Fail timer:   3
Control_vlan id: 2
Node role: MASTER
```

```
Primary port:     Gi 0/1          status: Link Down
Primary port:     Gi 0/2          status: Link Down
```

29 SSH

29.1 SSH Overview

SSH is a protocol that provides a secure, remote connection to a device. SSH provides more security for remote connections than Telnet does by providing strong encryption when a device is authenticated. This software release supports SSH version 1 (SSHv1) and SSH version 2 (SSHv2).

The SSH feature has an SSH server, which are applications that run on the switch. You can use an SSH client to connect to a switch running the SSH server. The SSH server works with the SSH client supported in this release. The SSH client also works with the SSH server supported in this release.

The switch supports an SSHv1 or an SSHv2 server.

SSH supports the Data Encryption Standard (DES) encryption algorithm, the Triple DES (3DES) encryption algorithm, and password-based user authentication.

29.2 Configuring SSH

Follow these steps to set up your switch to run SSH when configuring the switch as an SSH server:

- An RSA key pair generated by a SSHv1 server can be used by an SSHv2 server, and the reverse.
- Generate an RSA key pair for the switch, which automatically enables SSH. Follow this procedure only if you are configuring the switch as an SSH server.
- Configure user authentication for local or remote access. This step is required.

Beginning in privileged EXEC mode, follow these steps to configure to generate an RSA key pair. This procedure is required if you are configuring the switch as an SSH server.

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	ssh	Enable ssh
Step 3	ssh tftp-publickey *username filename* {dsa | rsa} *A.B.C.D*	Upload an DSA or RSA key pair has been generated.
Step 4	show ssh config	Verify your entries.
Step 5	show ssh status	Verify your entries.
Step 6	show ssh user	Verify your entries.
Step 7	copy running-config startup-config	(Optional) Save your entries in the configuration file.

Follow these steps to configure ssh:

```
Switch# configure terminal
Enter configuration commands, one per line.
Switch(config)# ssh
Switch(config)# username aaa password 123
Switch(config)# ssh tftp-publickey aaa Identity rsa 192.168.2.23
Switch# show ssh config
Switch# show ssh status
Switch# show ssh user
```

30 TACACS+

30.1 Controlling Switch Access with TACACS+

This section describes how to enable and configure Terminal Access Controller Access Control System Plus (TACACS+), which provides detailed accounting information and flexible administrative control over authentication and authorization processes.

TACACS+ Overview

TACACS+ is a security application that provides centralized validation of users attempting to gain access to your switch. TACACS+ services are maintained in a database on a TACACS+ daemon typically running on a UNIX or Windows NT workstation. You should have access to and should configure a TACACS+ server before the configuring TACACS+ features on your switch.

TACACS+ provides for separate and modular authentication, authorization, and accounting facilities. TACACS+ allows for a single access control server (the TACACS+ daemon) to provide each service—authentication, authorization, and accounting—independently. Each service can be tied into its own database to take advantage of other services available on that server or on the network, depending on the capabilities of the daemon.
The goal of TACACS+ is to provide a method for managing multiple network access points from a single management service. Your switch can be a network access server along with other routers and access servers.

30.2 Configuring TACACS+

This section describes how to configure your switch to support TACACS+. At a minimum, you must identify the host or hosts maintaining the TACACS+ daemon and define the method lists for TACACS+ authentication. You can optionally define method lists for TACACS+ authorization and accounting. A method list defines the sequence and methods to be used to authenticate, to authorize, or to keep accounts on a user. You can use method lists to designate one or more security protocols to be used, thus ensuring a backup system if the initial method fails. The software uses the first method listed to authenticate, to authorize, or to keep accounts on users; if that method does not respond, the software selects the next method in the list. This process continues until there is successful communication with a listed method or the method list is exhausted.
Beginning in privileged EXEC mode, follow these steps to identify the IP host or host maintaining TACACS+ server and optionally set the encryption key:

	Command	**Purpose**
Step 1	configure terminal	Enter global configuration mode.
Step 2	tacacs+	Enable tacacs+.
Step 4	tacacs+ server {ip | key}	Configuring tacacs+.
Step 5	show tacacs+	Verify your entries.
Step 6	copy running-config startup-config	(Optional) Save your entries in the configuration file.

Follow these steps to configure tacacs+:

```
Switch# configure terminal
Enter configuration commands, one per line.
Switch(config)# tacacs+
Switch(config)# tacacs+ server ip 192.168.2.23
Switch(config)# tacacs+ server key 123
Switch# show tacacs+
tacacs+ is enable.
tacacs+ server ip is : 192.168.2.23
tacacs+ server key is : 123
```

31 Smart Link & Monitor Link

Abstract: Smart Link is a feature developed to provide effective, reliable link redundancy, load sharing, and fast convergence for dual-uplink networks. Monitor Link is a feature developed to complement the link backup mechanism of Smart Link. By monitoring the uplink, and synchronizing the downlink with the uplink, Monitor Link triggers the switchover between the primary and backup links in a smart link group. This document mainly describes the basic concepts, mechanisms, and typical application scenarios of Smart Link and Monitor Link.

31.1 Smart Link overview

Smart Link is a feature developed to address the slow convergence issue with the Spanning Tree Protocol (STP).

Smart Link is dedicated to dual-uplink networks to provide link redundancy with subsecond convergence. It allows the backup link to take over quickly when the primary link fails. In addition to fast convergence, Smart Link is easy to configure.

Smart link group

A smart link group consists of only two member ports: the master and the slave. At a time, only one port is active for forwarding, and the other port is blocked, that is, in the standby state. When link failure occurs on the active port due to physical fault, or presence of unidirectional link for example, the standby port becomes active to take over while the original active port transits to the blocked state.

Master port

Master port is a port role in a smart link group. When the link states of both ports in a smart link group are normal, the master port preferentially transits to the forwarding state. Once the master port fails, the slave port takes over to forward traffic. In this case, if the smart link group is not configured with role preemption, the master port stays in standby state until next link switchover even if it has recovered.

Slave port

Slave port is the other port role in a smart link group. When the two ports in a smart link group are both in the standby state, the master port takes the precedence to enter the active state. When the master fails, the slave port takes over with the state changing from standby to active.

Flush message

Link switchover in a smart link group can outdate the current forwarding entries. To adapt to the new topology, network-wide MAC address and ARP table update must be done. A smart link group achieves this by sending flush messages to notify other devices to update the address table.

31.2 Smart Link Configuration

Configuring Smart Link Devices

You are recommended to disable the two ports to be added to a smart link group to prevent possible loops (which may result in broadcast storms) during the configuration.

Follow these steps to configure a smart link device:

	Command	**Purpose**
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface *interface-id*	Specify the port to configure, and enter interface configuration mode.
Step 3	smart-link {master | slave}	Configure a port as the master or slave port of the smart link

Step 4	smart-link flush-control	Configure the control VLAN for sending flush messages
Step 5	show smart-link	Verify your entries.
Step 6	copy running-config startup-config	(Optional) Save your entries in the configuration file.

Follow these steps to configure smart link.

```
Switch# configure terminal
Enter configuration commands, one per line.
Switch(config)# interface fastethernet 0/1
Switch(config-if)# smart-link master
Switch(config)# interface fastethernet 0/2
Switch(config-if)# smart-link slave
Switch(config-if)# exit
Switch(config)# smart-link flush-control
Switch(config)# exit
Switch# show smart-link
```

31.3 Monitor Link overview

Monitor link is a port collaboration solution introduced to complement smart link. It is used to monitor uplinks.
Monitor link is implemented through monitor link groups.
A monitor link group consists of an uplink port and multiple downlink ports.
Members of a monitor group can be single ports, static aggregation groups, manual aggregation groups, or smart link groups. Note that a smart link group in a monitor group can only serve as the uplink.

Operating Mechanism of Monitor Link

When the uplink of a monitor link group fails, the downlink ports in the monitor link group are shut down forcibly. When the uplink recovers, all the downlink ports in the group go up again.

31.4 Monitor Link Configuration

Follow these steps to configure a monitor link device:

	Command	**Purpose**
Step 1	configure terminal	Enter global configuration mode.

Step 2	interface *interface-id*	Specify the port to configure, and enter interface configuration mode.
Step 3	monitor-link {downlink | uplink}	Configure a port as the master or slave port of the smart link
Step 4	show monitor-link	Verify your entries.
Step 5	copy running-config startup-config	(Optional) Save your entries in the configuration file.

Follow these steps to configure monitor link.

```
Switch# configure terminal
Enter configuration commands, one per line.
Switch(config)# interface fastethernet 0/3
Switch(config-if)# monitor-link uplink
Switch(config)# interface fastethernet 0/4
Switch(config-if)# monitor-link downlink
Switch(config-if)# exit
Switch(config)# exit
Switch# show monitor-link
```

32 LLDP and LLDP-MED

Link Layer Discovery Protocol (LLDP), standardized by the IEEE as part of 802.1ab, enables standardized discovery of nodes, which in turn facilitates future applications of standard management tools such as Simple Network Management Protocol (SNMP) in multivendor networks. Using standard management tools makes physical topology information available and helps network administrators detect and correct network malfunctions and inconsistencies in configuration.

Media Endpoint Discovery (MED) is an LLDP enhancement that was formalized by the Telecommunications Industry Association (TIA) for voice over IP (VoIP) applications.

The implementation of LLDP is based on the IEEE 802.1ab standard. This document describes LLDP and LLDP-MED and how they are supported in software.

32.1 Finding Feature Information

Prerequisites for Using Link Layer Discovery Protocol in Multivendor Networks

- Type-Length-Value (TLV) types 0 through 127
- To support LLDP-MED, the following organizationally specific TLVs must be implemented:

– Extended Power-via-Media Dependent Interface (MDI)
– Inventory
– LLDP-MED Capabilities
– MAC/PHY Configuration Status
– Network Policy
– Port VLAN ID

32.2 Understanding LLDP and LLDP-MED

IEEE 802.1ab LLDP

IEEE 802.1ab LLDP is an optional link layer protocol for network topology discovery in multivendor networks. Discovery information includes device identifiers, port identifiers, versions, and other details. As a protocol that aids network management, LLDP provides accurate network mapping, inventory data, and network troubleshooting information.

LLDP is unidirectional, operating only in an advertising mode. LLDP does not solicit information or monitor state changes between LLDP nodes. LLDP periodically sends advertisements to a constrained multicast address. Devices supporting LLDP can send information about themselves while they receive and record information about their neighbors. Additionally, devices can choose to turn off the send or receive functions independently. Advertisements are sent out and received on every active and enabled interface, allowing any device in a network to learn about all devices to which it is connected.

Applications that use this information include network topology discovery, inventory management, emergency services, VLAN assignment, and inline power supply.

LLDP-MED

LLDP-MED operates between several classes of network equipment such as IP phones, conference bridges, and network connectivity devices such as routers and switches. By default, a network connectivity device sends out only LLDP packets until it receives LLDP-MED packets from an endpoint device. The network device then sends out LLDP-MED packets until the remote device to which it is connected ceases to be LLDP-MED capable.

Types of Discovery Supported

LLDP-MED provides support to discover the following types of information, which are crucial to efficient operation and management of endpoint devices and the network devices supporting them:

- Capabilities—Endpoints determine the types of capabilities that a connected device supports and which ones are enabled.
- Inventory—LLDP-MED support exchange of hardware, software, and firmware versions, among other inventory details.
- LAN speed and duplex—Devices discover mismatches in speed and duplex settings.
- Location identification—An endpoint, particularly a telephone, learns its location from a network device. This location information may be used for location-based applications on the telephone and is important when emergency calls are placed.
- Network policy—Network connectivity devices notify telephones about the VLANs they should use.
- Power—Network connectivity devices and endpoints exchange power information. LLDP-MED provides information about how much power a device needs and how a device is powered. LLDP-MED also determines the priority of the device for receiving power.

32.3 LLDP and LLDP-MED Configuration

Follow these steps to configure a LLDP and LLDP-MED device:

	Command	**Purpose**
Step 1	configure terminal	Enter global configuration mode.

Step 2	lldp {fast-count | hold-multiplier | timer }	Set the interval of sending UDLD packets and the aging timer.
Step 3	interface *interface-id*	Specify the port to configure, and enter interface configuration mode.
Step 4	lldp {med-tlv-select | mode }	Enables an LLDP-MED TLV or LLDP packet transmission on a supported interface.
Step 5	show lldp { interface [ethernet number] | neighbors [ethernet number | information] }	Verify your entries.
Step 6	copy running-config startup-config	(Optional) Save your entries in the configuration file.

The following example shows LLDP configurations for two routers in a network. Hold time, a timer value, and TLVs are configured for each router. In each case an assumption is made that the Ethernet interfaces being configured are in the UP state.

Configure LLDP on Switch with TLV options.

```
Switch> enable
Switch# configure terminal
Enter configuration commands, one per line.
Switch(config)# lldp
switch(config)#interface fastethernet 0/1
switch(config-if-fa 0/1)#lldp med-tlv-select all
switch(config-if-fa 0/1)#exit
switch(config)#exit
Switch#show lldp
Switch#show lldp interface information
Switch#show running-config
```

33 DDM

33.1 Introduction of Digital Diagnostic Monitoring（DDM）

The communication system capacity, transfer rate, and service level requirements continue to increase, communication networks become increasingly large, increasingly complex communication link management. People are eager to use intelligent performance detection technology in communication system to solve this growing problem. The digital diagnostic monitoring of optical transceiver module provides such low cost performance test means.

Definition:

DDM means Digital Diagnostic Monitoring.

The features of Digital Diagnostic Monitoring:

- Monitoring module operating temperature
- Monitoring module operating voltage
- Monitoring module operating current
- Display module factory version.

Through real-time monitoring the module internal operating voltage and temperature, allowing the system administrators to find out some potential problems:

- If Vcc voltage is too high, it will breakdown CMOS device; If Vcc voltage is too low, the laser does not work.
- If received power is too high, it will damage the receiver module.
- If working temperature is too high, it will accelerate the aging of the device.

What’s more, it can monitor the circuit and the performance of the remote transmitters by monitoring the received optical power meter.

Digital diagnostic monitoring applications:

The DDM function provides a performance monitoring tool for the system that can help the system management to predict the life of the module, isolate the system fault, verify compatibility of the module during the installation.

The appearance of the module with DDM and without DDM is same, but the internal circuit is different. If a module doesn’t with DDM function, once the products appear problems, it will not provide prompt alarm.

33.2 View DDM information

Follow these steps to view DDM information.

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	show transceiver interfaces { fastEthernet *interface-id* | gigabitethernet *interface-id*}	Verify your entries.

The following example shows DDM information of SFP module.

```
Switch> enable
Switch# show transceiver interfaces
******************************
Gi 0/1    Common Information
Transcevier Type                       :SFP/SFP+
Connector Type                          :LC
Compliance                                :1000Base-SX I SN M5/M5E M6 100MB/s
200MB/s
Length(50 um)OM2                         :300 (m)
Length(62.5 um)OM1                       :150 (m)
Laser wavelength                       :850(nm)
Digital Diagnostic Monitoring    :Yes
Vendor Name                                 :FINISAR CORP.
Vendor PN                                   :FTLF8519P2BNL
Vendor SN                                   :PF918XW
Date                                         :2/25/2009
Temperture(Celsius)                    :28.39
Voltage(V)                                :3.34
Bias Current(mA)                        :8.49
Bias High Threshold(mA)               :17.00
Bias Low    Threshold(mA)              :1.00
Rx Power(dBM)                             :-4.65
RX Power High Threshold(dBM)         :1.00
RX Power Low    Threshold(dBM)         :-20.00
Tx Power(dBM)                             :-4.44
TX Power High Threshold(dBM)         :-2.00
TX Power Low    Threshold(dBM)        :-11.74
switch#
```

34 IPStack Overview

34.1 Introduction to IPStack

With networks getting larger in size and more complicated in structure, network configuration becomes a tough task for the network administrators. IPStack is developed to solve these issues. IPStack adopts a MASTER/SLAVE model, and virtual ip of SLAVE send by master.

IPStack setup

IPStack group

IPStack group mean witch switch can set though IPStack, set IPStack group of some switches as same， then you can option these switches can though IPStack, you cannot option switches though IPStack if they are not the same group.

IPStack name

IPStack name distinguish switches in the same group, so you can select them in topology.

IPStack priority

IPStack adopts a MASTER/SLAVE model. When some switches interaction though IPStack, first they elect MASTER which has the lowest priority number， IPStack priority includes: ID and priority, when priority are same, who has the lowest switch ID is MASTER

IPStack role

You can set role of switch static, the role of switch is set by administrator.

34.2 IPStack configuration

Enable IPStack

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	lldp	Enable lldp.
Step 3	IPStack	Enable IPStack.
Step 4	show ip IPStack	Verify your entries.
Step 5	copy running-config startup-config	(Optional) Save your entries in the configuration file.

This example shows how to configure IPStack :

```
Switch# configure terminal
Enter configuration commands, one per line.
Switch(config)# lldp
Switch(config)# IPStack
Switch(config)# exit
Switch# show IPStack
Switch# copy running-config startup-config
```

Configure IPStack Group

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	IPStack group *name*	Configure IPStack group name.
Step 3	show IPStack	Verify your entries.
Step 4	copy running-config startup-config	(Optional) Save your entries in the configuration file.

This example shows how to configure IPStack group:

```
Switch# configure terminal
Enter configuration commands, one per line.
Switch(config)# IPStack group test
Switch(config)# exit
Switch# show IPStack
```

Configure IPStack Name

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	ipstack name *name*	Configure IPStack name.
Step 3	show ipstack	Verify your entries.
Step 4	copy running-config startup-config	(Optional) Save your entries in the configuration file.

This example shows how to configure IPStack name:

```
Switch# configure terminal
Enter configuration commands, one per line.
Switch(config)# ipstack name test
Switch(config)# exit
Switch# show ipstack
```

Configure IPStack priority

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	IPStack priority *priority*	Configure IPStack priority.
Step 3	show IPStack	Verify your entries.
Step 4	copy running-config startup-config	(Optional) Save your entries in the configuration file.

This example shows how to configure IPStack priority:

```
Switch# configure terminal
Enter configuration commands, one per line.
Switch(config)# ipstack priority 100
Switch(config)# exit
Switch# show ipstack
```

Configure IPStack role

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	IPStack role ability [m|ms]	Enable IPStack role.

Step 3	show IPStack	Verify your entries.
Step 4	copy running-config startup-config	(Optional) Save your entries in the configuration file.

This example shows how to configure IPStack role:

```
Switch# configure terminal
Enter configuration commands, one per line.
Switch(config)# ipstack role ability s
Switch(config)# exit
Switch# show ipstack
```

35 Configuring System Message Logging

35.1 Understanding System Message Logging

By default, a switch sends the output from system messages and debug privileged EXEC commands to a logging process. The logging process controls the distribution of logging messages to various destinations, such as the logging buffer, terminal lines, or a syslog server, depending on your configuration. The process also sends messages to the console.

When the logging process is disabled, messages are sent only to the console. The messages are sent as they are generated, so message and debug output are interspersed with prompts or output from other commands. Messages appear on the console after the process that generated them has finished.

You can set the severity level of the messages to control the type of messages displayed on the console and each of the destinations. You can time stamp log messages or set the syslog source address to enhance real-time debugging and management. For information on possible messages, refer to the system message guide for this release.

You can access logged system messages by using the switch command-line interface (CLI) or by saving them to a properly configured syslog server. The switch software saves syslog messages in an internal buffer. You can remotely monitor system messages by accessing the switch through Telnet, through the console port, or by viewing the logs on a syslog server.

35.2 Configuring Message Logging

Enabling Message Logging of local

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	logging type {dai | interface | loop-check | overload | pause | web}	Enable logging message of local.
Step 3	show running-config or show logging	Verify your entries.
Step 4	copy running-config startup-config	(Optional) Save your entries in the configuration file.

Follow these steps to configure login web message of local.

```
Switch# configure terminal
Enter configuration commands, one per line.
Switch(config)# logging type web
Switch(config)# exit
Switch# show logging
Switch# show running-config
```

Setting the Message Display Destination Device

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**logging {degree | server | server-ip}**	Configuring the logging message of destination device.
Step 4	**show running-config** **or** **show logging**	Verify your entries.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Follow these steps to configure login web message of destination device.

```
Switch# configure terminal
Enter configuration commands, one per line.
Switch(config)# logging server
Switch(config)# logging servers-ip 192.168.2.5
Switch# show logging
Switch# show running-config
```

36 Configuring Tcpdump

36.1 Understanding Tcpdump

Tcpdump prints out a description of the contents of packets on a network interface that match the boolean expression. Which causes it to read from a saved packet file rather than to read packets from a network interface. In all cases, only packets that match expression will be processed by tcpdump.

When tcpdump finishes capturing packets, it will report counts of:

packets ``captured'' (this is the number of packets that tcpdump has received and processed);

packets ``received by filter'' (the meaning of this depends on the OS on which you're running tcpdump, and possibly on the way the OS was configured - if a filter was specified on the command line, on some OSes it counts packets regardless of whether they were matched by the filter expression and, even if they were matched by the filter expression, regardless of whether tcpdump has read and processed them yet, on other OSes it counts only packets that were matched by the filter expression regardless of whether tcpdump has read and processed them yet, and on other OSes it counts only packets that were matched by the filter expression and were processed by tcpdump);

packets ``dropped by kernel'' (this is the number of packets that were dropped, due to a lack of buffer space, by the packet capture mechanism in the OS on which tcpdump is running, if the OS reports that information to applications; if not, it will be reported as 0).

Common uses

Tcpdump prints the contents of network packets. It can read packets from a network interface card or from a previously created saved packet file. Tcpdump can write packets to standard output or a file.

It is also possible to use tcpdump for the specific purpose of intercepting and displaying the communications of another user or computer. A user with the necessary privileges on a system acting as a router or gateway through which unencrypted traffic such as Telnet or HTTP passes can use tcpdump to view login IDs, passwords, the URLs and content of websites being viewed, or any other unencrypted information.

The user may optionally apply a BPF-based filter to limit the number of packets seen by tcpdump; this renders the output more usable on networks with a high volume of traffic.

36.2 Disabling and Enabling the tcpdump

	Command	Purpose
Step 1	tcpdump [aarp | arp | icmp | ip | ipv6 | rarp | tcp | udp]	Enable tcpdump all types of packets. Or enable tcpdump specifies the packet type.
Step 2	tcpdump param	Set specifies the detailed parameters of tcpdump.

1). Follow these steps to configure tcpdump, print out the arp packet information.

```
Switch# tcpdump arp
```

2). Follow these steps to configure tcpdump, shut down tcpdump.

```
Switch# no tcpdump
```

3). Follow these steps to configure tcpdump, print out the all packet information.

```
Switch# tcpdump
```

37 IPv6 Overview

Internet Protocol Version 6 (IPv6), also called IP next generation (IPng), was designed by the Internet Engineering Task Force (IETF) as the successor to Internet Protocol Version 4 (IPv4). The significant difference between IPv6 and IPv4 is that IPv6 increases the IP address size from 32 bits to 128 bits.

37.1 IPv6 Features

Header format simplification

IPv6 cuts down some IPv4 header fields or move them to the IPv6 extension headers to reduce the length of the basic IPv6 header. IPv6 uses the basic header with a fixed length, thus making IPv6 packet handling simple and improving the forwarding efficiency. Although the IPv6 address size is four times that of IPv4 addresses, the size of basic IPv6 headers is 40 bytes and is only twice that of IPv4 headers (excluding the Options field).

Adequate address space

The source and destination IPv6 addresses are both 128 bits (16 bytes) long. IPv6 can provide 3.4 x 1038 addresses to completely meet the requirements of hierarchical address division as well as allocation of public and private addresses.

Hierarchical address structure

IPv6 adopts the hierarchical address structure to quicken route search and reduce the system source occupied by the IPv6 routing table by means of route aggregation.

Automatic address configuration

To simplify the host configuration, IPv6 supports stateful and stateless address configuration.

- Stateful address configuration means that a host acquires an IPv6 address and related information from a server (for example, DHCP server).
- Stateless address configuration means that a host automatically configures an IPv6 address and related information on basis of its

own link-layer address and the prefix information advertised by a router.

In addition, a host can generate a link-local address on basis of its own link-layer address and the default prefix FE80::/64) to communicate with other hosts on the link.

Built-in security
IPv6 uses IPSec as its standard extension header to provide end-to-end security. This feature provides a standard for network security solutions and improves the interoperability between different IPv6 applications.

QoS support
The Flow Label field in the IPv6 header allows the device to label packets in a flow and provide special handling for these packets.

Enhanced neighbor discovery mechanism
The IPv6 neighbor discovery protocol is implemented through a group of Internet Control Message Protocol Version 6 (ICMPv6) messages that manages the information exchange between neighbor nodes on the same link. The group of ICMPv6 messages takes the place of Address Resolution Protocol (ARP) message, Internet Control Message Protocol version 4 (ICMPv4) router discovery message, and ICMPv4 redirection message to provide a series of other functions.

Flexible extension headers
IPv6 cancels the Options field in IPv4 packets but introduces multiple extension headers. In this way, IPv6 enhances the flexibility greatly to provide scalability for IP while improving the handling efficiency. The Options field in IPv4 packets contains 40 bytes at most, while the size of IPv6 extension headers is restricted by that of IPv6 packets.

37.2 Introduction to IPv6 Address

IPv6 address format
An IPv6 address is represented as a series of 16-bit hexadecimals, separated by colons. An IPv6 address is divided into eight groups, and the 16 bits of each group are represented by four hexadecimal

numbers which are separated by colons, for example: **2001:0000:130F:0000:0000:09C0:876A:130B.**

To simplify the representation of IPv6 addresses, zeros in IPv6 addresses can be handled as follows:

- Leading zeros in each group can be removed. For example, the above-mentioned address can be represented in shorter format as **2001:0:130F:0:0:9C0:876A:130B.**
- If an IPv6 address contains two or more consecutive groups of zeros, they can be replaced by the double-colon :: option. For example, the above-mentioned address can be represented in the shortest format as **2001:0:130F::9C0:876A:130B.**

An IPv6 address consists of two parts: address prefix and interface ID. The address prefix and the interface ID are respectively equivalent to the network ID and the host ID in an IPv4 address.

An IPv6 address prefix is written in IPv6-address/prefix-length notation, where IPv6-address is an IPv6 address in any of the notations and prefix-length is a decimal number indicating how many bits from the utmost left of an IPv6 address are the address prefix.

IPv6 address classification

IPv6 addresses fall into three types: unicast address, multicast address, and anycast address.

- Unicast address: An identifier for a single interface, similar to an IPv4 unicast address. A packet sent to a unicast address is delivered to the interface identified by that address.
- Multicast address: An identifier for a set of interfaces (typically belonging to different nodes), similar to an IPv4 multicast address. A packet sent to a multicast address is delivered to all interfaces identified by that address.
- Anycast address: An identifier for a set of interfaces (typically belonging to different nodes). A packet sent to an anycast address is delivered to one of the interfaces identified by that address (the nearest one, according to the routing protocols’ measure of distance).

Unicast address

There are several forms of unicast address assignment in IPv6, including aggregatable global unicast address, link-local address, and site-local address.

- The aggregatable global unicast address, equivalent to an IPv4 public address, is provided for network service providers. The type of address allows efficient route prefix aggregation to restrict the number of global routing entries.
- The link-local address is used for communication between link-local nodes in neighbor discovery and stateless autoconfiguration. Routers must not forward any packets with link-local source or destination addresses to other links.
- IPv6 unicast site-local addresses are similar to private IPv4 addresses. Routers must not forward any packets with site-local source or destination addresses outside of the site (equivalent to a private network).
- Loopback address: The unicast address 0:0:0:0:0:0:0:1 (represented in the shortest format as ::1) is called the loopback address and may never be assigned to any physical interface. Like the loopback address in IPv4, it may be used by a node to send an IPv6 packet to itself.
- Unassigned address: The unicast address "::” is called the unassigned address and may not be assigned to any node. Before acquiring a valid IPv6 address, a node may fill this address in the source address field of an IPv6 packet, but may not use it as a destination IPv6 address.

Multicast address

Besides, there is another type of multicast address: solicited-node address. A solicited-node multicast address is used to acquire the link-layer addresses of neighbor nodes on the same link and is also used for duplicate address detection (DAD). Each IPv6 unicast or anycast address has one corresponding solicited-node address. The format of a solicited-node multicast address is as follows:

FF02:0:0:0:0:1:FFXX:XXXX

Where, FF02:0:0:0:0:1 FF is permanent and consists of 104 bits, and XX:XXXX is the last 24 bits of an IPv6 unicast or anycast address.

Interface identifier in IEEE EUI-64 format
Interface identifiers in IPv6 unicast addresses are used to identify interfaces on a link and they are required to be unique on that link. Interface identifiers in IPv6 unicast addresses are currently required to be 64 bits long. An interface identifier in IEEE EUI-64 format is derived from the link-layer address of that interface. Interface identifiers in IPv6 addresses are 64 bits long, while MAC addresses are 48 bits long. Therefore, the hexadecimal number FFFE needs to be inserted in the middle of MAC addresses (behind the 24 high-order bits). To ensure the interface identifier obtained from a MAC address is unique, it is necessary to set the universal/local (U/L) bit (the seventh high-order bit) to “1”. Thus, an interface identifier in IEEE EUI-64 format is obtained.

37.3 Introduction to IPv6 Neighbor Discovery Protocol

IPv6 Neighbor Discovery Protocol (NDP) uses five types of ICMPv6 messages to implement the following functions:

- Address resolution
- Neighbor reachability detection
- Duplicate address detection
- Router/prefix discovery and address autoconfiguration
- Redirection

The NDP mainly provides the following functions:

Address resolution
Similar to the ARP function in IPv4, a node acquires the link-layer addresses of neighbor nodes on the same link through NS and NA messages. Figure 1-1 shows how node A acquires the link-layer address of node B.

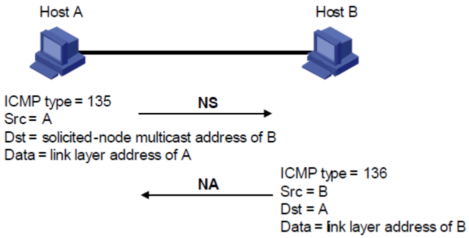

Host A
Host B
ICMP type = 135
Src = A
Dst = solicited-node multicast address of B
Data = link layer address of A
NS
NA
ICMP type = 136
Src = B
Dst = A
Data = link layer address of B

Figure 1-1 Address resolution

The address resolution procedure is as follows:

1) Node A multicasts an NS message. The source address of the NS message is the IPv6 address of an interface of node A and the destination address is the solicited-node multicast address of node B. The NS message contains the link-layer address of node A.
2) After receiving the NS message, node B judges whether the destination address of the packet corresponds to the solicited-node multicast address. If yes, node B can learn the link-layer address of node A, and unicasts an NA message containing its link-layer address.
3) Node A acquires the link-layer address of node B from the NA message.

Neighbor reachability detection

After node A acquires the link-layer address of its neighbor node B, node A can verify whether node B is reachable according to NS and NA messages.
1) Node A sends an NS message whose destination address is the IPv6 address of node B.
2) If node A receives an NA message from node B, node A considers that node B is reachable. Otherwise, node B is unreachable.

Duplicate address detection

After node A acquires an IPv6 address, it will perform duplicate address detection (DAD) to determine whether the address is being used by other nodes (similar to the gratuitous ARP function of IPv4). DAD is accomplished through NS and NA messages. **Figure 1-2** shows the DAD procedure.

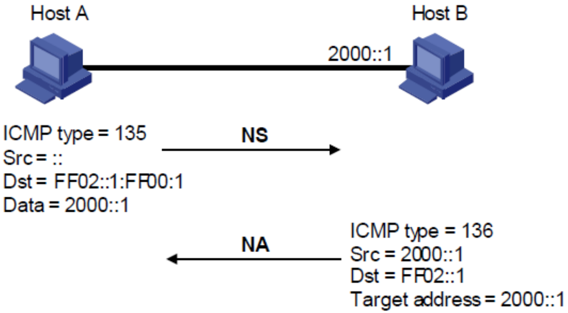


Figure 1-2 Duplicate address detection

The DAD procedure is as follows:

1) Node A sends an NS message whose source address is the unassigned address: and destination address is the corresponding solicited-node multicast address of the IPv6 address to be detected. The NS message contains the IPv6 address.
2) If node B uses this IPv6 address, node B returns an NA message. The NA message contains the IPv6 address of node B.
3) Node A learns that the IPv6 address is being used by node B after receiving the NA message from node B. Otherwise, node B is not using the IPv6 address and node A can use it.

Router/prefix discovery and address autoconfiguration

Router/prefix discovery means that a node locates the neighboring routers, and learns the prefix of the network where the host is located, and other configuration parameters from the received RA message.

Stateless address autoconfiguration means that a node automatically

configures an IPv6 address according to the information obtained through router/prefix discovery.
The router/prefix discovery is implemented through RS and RA messages. The router/prefix discovery procedure is as follows:

1) After started, a node sends an RS message to request the router for the address prefix and other configuration information for the purpose of autoconfiguration.
2) The router returns an RA message containing information such as prefix information option. (The router also regularly sends an RA message.)
3) The node automatically configures an IPv6 address and other information for its interface according to the address prefix and other configuration parameters in the RA message.

Redirection
When a host is started, its routing table may contain only the default route to the gateway. When certain conditions are satisfied, the gateway sends an ICMPv6 redirect message to the source host so that the host can select a better next hop to forward packets (similar to the ICMP redirection function in IPv4).

The gateway will send an IPv6 ICMP redirect message when the following conditions are satisfied:

- The receiving interface is the forwarding interface.
- The selected route itself is not created or modified by an IPv6 ICMP redirect message.
- The selected route is not the default route.
- The forwarded IPv6 packet does not contain any routing header.

37.4 Configuring Basic IPv6 Functions

37.4.1 Configuring the IPv6 address

The Switches support assigning IPv6 Global Unicast Addres addresses to VLAN interfaces. Besides directly assigning an IPv6 Global Unicast Addres address to a VLAN interface, it also has Link Local Address.

Configuration procedure

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface vlan *vlan-id*	Enter interface configuration mode, and enter the VLAN to which the IPv6 information is assigned. The range is 1 to 4094.
Step 3	ipv6 address *ipv6-address subnet-mask*	Enter the IPv6 address and subnet mask.
Step 4	exit	Return to global configuration mode.
Step 5	show interfaces vlan *vlan-id*	Verify the configured IPv6 address.
Step 6	show ipv6 interface brief	Verify the IPv6 configuration information of interface.
Step 7	copy running-config startup-config	(Optional) Save your entries in the configuration file.

This example shows how to configure an interface as a VLAN interface port and to assign it an IPv6 address:

```
Switch# configure terminal
Enter configuration commands, one per line.
Switch(config)# interface vlan 2
Switch(config-if)# ipv6 address 2001::1/64
Switch(config-if)# no shutdown
Switch(config-if)# exit
Switch(config) # exit
Switch#
```

To remove the switch IPv6 address, use the **no ipv6 address** ipv6-address subnet-mask interface configuration command. If you are removing the address through a Telnet session, your connection to the switch will be lost.

37.4.2 Configuring the IPv6 default-gateway

	Command	Purpose

Step 1	configure terminal	Enter global configuration mode.
Step 2	ipv6 route default *X:X::X:X*	Configure ipv6 default-gateway.
Step 3	copy running-config startup-config	(Optional) Save your entries in the configuration file.

This example shows how to configure dhcp trust port: and enable option

```
Switch# configure terminal
Enter configuration commands, one per line.
Switch(config)# ipv6 route default 2000::1
Switch(config)# exit
```

37.4.3 Ping or Traceroute with IPv6

	Command	Purpose
Step 1	ipv6 ping x:x::x:x	Ping with IPv6
Step 2	ipv6 tracertoute x:x::x:x	Traceroute with IPv6

This example shows how to ping or traceroute with IPv6

```
Switch# ipv6 ping 2001::2
PING 2001::2 : 56 data bytes,press CTRL_C to break
64 bytes from 2001::2: seq=1 ttl=128 time=100
64 bytes from 2001::2: seq=2 ttl=128 time=1
64 bytes from 2001::2: seq=3 ttl=128 time=1

--- 2001::2 ping statistics ---
   3 packets transmitted
   3 packets received
   0% packet loss
   round-trip min/avg/max = 1/34/100 ms
switch# ipv6 traceroute 2001::2 ttl 3
traceroute to traceroute (2001::2)
  1nprobes: 3
   2001::2 (2001::2)    0.000 msnprobes: 3
   *nprobes: 3
   0.000 ms
```

37.4.4 Configuring the IPv6 DHCP Snooping agent

The **Dynamic Host Configuration Protocol version 6 (DHCPv6)** is a network protocol for configuring Internet Protocol version 6 (IPv6) hosts with IP addresses, IP prefixes and other configuration data required to operate in an IPv6 network. It is the IPv6 equivalent of the Dynamic Host Configuration Protocol for IPv4.

To make DHCPv6 Server to obtain accurate physical location information of DHCPv6 users, the Option37 or Option38 fields can be added to the DHCPv6 message.

	Command	**Purpose**
Step 1	configure terminal	Enter global configuration mode.
Step 2	ipv6 dhcp snooping remote-id option	Enable DHCP snooping agent remote-id globally.
Step 3	ipv6 dhcp snooping subscriber-id option	Enable DHCP snooping agent subscriber-id globally.
Step 4	interface *interface-id*	Specify the port to configure, and enter interface configuration mode.
Step 5	ipv6 dhcp snooping trust	Configure dhcpv6 snooping trust port.
Step 6	copy running-config startup-config	(Optional) Save your entries in the configuration file.

This example shows how to configure dhcp trust port: and enable option

```
Switch# configure terminal
Enter configuration commands, one per line.
Switch(config)# ipv6 dhcp snooping remote-id option
Switch(config)# ipv6 dhcp snooping subscriber-id option
Switch(config)# interface fastethernet 0/18
Switch(config-if)# ipv6 dhcp snooping trust
Switch(config-if)# exit
Switch(config)# exit
```

37.4.5 Configuring DHCPv6 Option string

Specifies the string value for the remote-ID and subscriber-id.

Specify an option value:

- pv—port + BD-VLAN

Specify the delimiter between port/BD-VLAN.
Values for delimiterinclude: #|,|.|;|/|space.|

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	ipv6 dhcp snooping subscriber-id select pv delimiter	Configuring the delimiter for DHCPv6 snooping agent subscriber-id
Step 3	interface *interface-id*	Specify the client port to configure remote-id and subscriber-id
Step 4	show running-config	Verify your entries.
Step 5	ipv6 dhcp snooping remote-id *string*	configure remote-id
Step 6	ipv6 dhcp snooping subscriber-id *string*	configure subscriber-id
Step 7	copy running-config startup-config	(Optional) Save your entries in the configuration file.

Follow these steps to configure the delimiter for PPPoE+

```
Switch# configure terminal
Enter configuration commands, one per line.
Switch(config)# ipv6 dhcp snooping subscriber-id select pv delimiter #
Switch(config)# interface gigabitethernet 0/1
switch(config-if-gi 0/1)# ipv6 dhcp snooping remote-id switch
switch(config-if-gi 0/1)# ipv6 dhcp snooping subscriber-id switch
switch(config-if-gi 0/1)# exit
Switch(config)# exit
Switch# show running-config
```

37.4.6 Configuring the SNMP over IPv6

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	Snmp-server	Enable the SNMP agent operation.
Step 3	Snmp-server ipv6 *udp-port-number*	Enable SNMP ipv6 and configure the UDP port number
Step 4	snmp-server communityv6	Configure the communityv6 string.

	[v1 | v2c] [ro | rw] *string* [X:X::X:X *ipv6-address|* default] *oid-number*	
Step 5	show snmp	Verify your entries.
Step 6	copy running-config startup-config	(Optional) Save your entries in the configuration file.

To remove a specific community string, use the **no snmp-server communityv6 [v1 | v2c] [ro | rw] string [X:X::X:X ipv6-address| default]** oid-number global configuration command.

This example shows how to assign the string private to SNMP, to allow read-write access.

```
Switch# configure terminal
Enter configuration commands, one per line.
Switch(config)# snmp-server
Switch(config)# snmp-server
switch(config)# snmp-server ipv6 200
Switch(config)# snmp-server communityv6 v2c rw public default 1.3.6.1
Switch(config)# exit
Switch# show snmp
```

38 PPPoE+ Overview

This section describes the principle of PPPoE+.

Currently, PPPoE provides authentication and security, but still has certain disadvantages, for example, account embezzlement.

In common PPPoE dialup mode, when users dial up through PPPoE from different interfaces of devices, they can access the network as long as their accounts are authenticated successfully on the same RADIUS server. After PPPoE+ is enabled, you need to enter the user name and password in authentication and the authentication packet carries information including the interface. If the port number identified by the RADIUS server is different from the configured one, the authentication fails. In this manner, unauthorized users cannot embezzle the accounts of authorized users (mainly the company) to access the Internet.

38.1 PPPoE+ Features

The switch can add the device type and interface number to the received PPPoE packets. In this manner, the PPPoE server can perform policy control flexibly for the client according to the information in the received PPPoE packets, for example, IP address allocation control and flexible accounting.

To prevent the access of unauthorized users during PPPoE authentication, configure PPPoE+ on the switch. In this case, interface information is added to the PPPoE packets. This ensures network security.

38.2 Configuring PPPoE+

38.2.1 Enabling PPPoE+ Globally

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	PPPoE intermediate-agent information enable	PPPoE+ is enabled globally.
Step 3	show running-config	Verify your entries.
Step 4	copy running-config startup-config	(Optional) Save your entries in the configuration file.

Follow these steps to configure PPPoE+ is enabled on all the interfaces.

```
Switch# configure terminal
Enter configuration commands, one per line.
Switch(config)# pppoe intermediate-agent information enable
Switch(config)# exit
Switch# show running-config
```

38.2.2 Configuring the Information Field Content to Be Added To PPPoE Packets

After PPPoE+ is enabled globally, user-side interfaces on the switch add circuit-id and remoteid in common format to the received PPPoE packets. You can modify the format of the field to be added to PPPoE packets.

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	PPPoE intermediate-agent format { circuit-id | remote-id } { ascii | hex }	Add fields in specified format to the received PPPoE packets.
Step 4	show running-config	Verify your entries.
Step 5	copy running-config startup-config	(Optional) Save your entries in the configuration file.

The format and contents of fields to be added to PPPoE packets are set.

After the **pppoe intermediate-agent information format** command is run in the system view.

Follow these steps to configure to add fields in specified format to the received PPPoE packets.

```
Switch# configure terminal
Enter configuration commands, one per line.
Switch(config)# pppoe intermediate-agent information format circuit-id ascii
Switch(config)# pppoe intermediate-agent information format remote-id ascii
Switch(config)# exit
Switch# show running-config
```

38.2.3 Configuring the Delimiter for PPPoE IA

Specifies the ASCII string value for the circuit-ID.

Specify an optionvalue:

- pv—port + BD-VLAN

Specify the delimiter between port/BD-VLAN.

Values for delimiterinclude: #|,|.|;|/|space.|

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	PPPoE intermediate-agent delimiter {# | . | , | ; | : | / | space }	Configuring the delimiter for PPPoE+
Step 3	show running-config	Verify your entries.
Step 4	copy running-config startup-config	(Optional) Save your entries in the configuration file.

Follow these steps to configure the delimiter for PPPoE+

```
Switch# configure terminal
Enter configuration commands, one per line.
Switch(config)# pppoe intermediate-agent delimiter #
Switch(config)# exit
Switch# show running-config
```

38.2.4 Configuring PPPoE IA on an Interface

This setting applies to all frames passing through this interface, regardless of the EFP to which they belong. By default the PPPoE IA feature is disabled on all interfaces. You need to run this command on every interface that requires this feature.

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface *interface-id*	Enter interface configuration mode, and enter the interface for which you are adding a description.
Step 3	pppoe intermediate-agent information { circuit-id | remote-id | strip | trusted }	Configuring PPPoE IA on an interface.
Step 4	show pppoe intermediate-agent info	Verify your entry.
Step 5	copy running-config startup-config	(Optional) Save your entries in the configuration file.

Enables PPPoE IA on the interface

Enabling PPPoE IA on an interface does not ensure that incoming packets are tagged. For this to happen PPPoE IA must be enabled globally, and at least one interface that connects the device to PPPoE server has a trusted PPPoE IA setting.

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface *interface-id*	Enter interface configuration mode, and enter the interface for which you are adding a description.
Step 3	pppoe intermediate-	Enable PPPoE IA on an interface.

	agent information	
Step 4	show pppoe intermediate-agent info	Verify your entry.
Step 5	copy running-config startup-config	(Optional) Save your entries in the configuration file.

Follow these steps to enables PPPoE IA on interface gi 0/1.

```
Switch# configure terminal
Enter configuration commands, one per line.
Switch(config)# interface gigabitethernet 0/1
Switch(config-if-gi 0/1)# pppoe intermediate-agent information
Switch(config-if-gi 0/1)# end
Switch# show running-config
```

Configuring PPPoE IA Circuit-ID on an Interface

You can configure the circuit-ID on a physical interface. The PADI, PADR, and PADT packets (belonging to PPPoE discovery stage) that are received on this physical interface are tagged with either one of these IDs. These packets are tagged regardless of their VLAN if PPPoE is not enabled for that VLAN.

Set the circuit-ID on an interface to override the automatic generation of the circuit-ID by the switch.

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface *interface-id*	Enter interface configuration mode, and enter the interface for which you are adding a description.
Step 3	pppoe intermediate-agent information circuit-id *string*	Configuring PPPoE IA Circuit-id for an interface.
Step 4	show pppoe intermediate-agent info	Verify your entry.
Step 5	copy running-config startup-config	(Optional) Save your entries in the configuration file.

Follow these steps to configuring PPPoE IA Circuit-id on interface gi 0/1.

```
Switch# configure terminal
Enter configuration commands, one per line.
Switch(config)# interface gigabitethernet 0/1
Switch(config-if-gi 0/1)# pppoe intermediate-agent information circuit-id root
Switch(config-if-gi 0/1)# end
Switch# show running-config
```

Configuring PPPoE IA Remote-ID on an Interface

You can configure the remote-ID on a physical interface. The PADI, PADR, and PADT packets (belonging to PPPoE discovery stage) that are received on this physical interface are tagged with either one of these IDs. These packets are tagged regardless of their VLAN if PPPoE is not enabled for that VLAN.

Set the remote-ID for subscriber link identification. Configure the remote-ID on every interface in which you enabled PPPoE IA. Otherwise, the default value for remote-ID is the switch MAC address.

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface *interface-id*	Enter interface configuration mode, and enter the interface for which you are adding a description.
Step 3	pppoe intermediate-agent information remote-id *string*	Configuring PPPoE IA Remote-id for an interface.
Step 4	show pppoe intermediate-agent info	Verify your entry.
Step 5	copy running-config startup-config	(Optional) Save your entries in the configuration file.

Follow these steps to configuring PPPoE IA remote-id on interface gi 0/1.

```
Switch# configure terminal
Enter configuration commands, one per line.
Switch(config)# interface gigabitethernet 0/1
Switch(config-if-gi 0/1)# pppoe intermediate-agent information circuit-id granite
Switch(config-if-gi 0/1)# end
Switch# show running-config
```

Configuring the PPPoE IA Trust Setting on an Interface

Interfaces that connect the device to the PPPoE server are configured as trusted. Interfaces that connect the device to users (PPPoE clients) are untrusted.

This setting is disabled by default.

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface *interface-id*	Enter interface configuration mode, and enter the interface for which you are adding a description.
Step 3	pppoe intermediate-agent information trusted	Configuring PPPoE IA trusted interface.
Step 4	show pppoe intermediate-agent info	Verify your entry.
Step 5	copy running-config startup-config	(Optional) Save your entries in the configuration file.

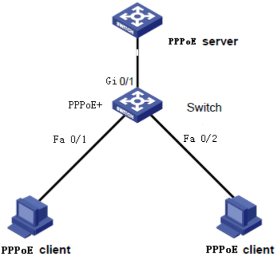
To prevent bogus PPPoE servers and the security risk caused by PPPoE packets forwarded to non-PPPoE service interfaces, you can configure the interface connecting the switch and the PPPoE server as the trusted interface. After the trusted interface is configured, PPPoE packets sent from the PPPoE client to the PPPoE server are forwarded through the trusted interface only. In addition, only the PPPoE packets received from the trusted interface are forwarded to the PPPoE client. The trusted interface only controls protocol packets in PPPoE discovery period, and does not control service packets in PPPoE session period.

Follow these steps to configure the PPPoE trusted interface.

```
Switch# configure terminal
Enter configuration commands, one per line.
Switch(config)# interface gigabitethernet 0/1
Switch(config-if-gi 0/1)# pppoe intermediate-agent information trusted
Switch(config-if-gi 0/1)# end
Switch# show running-config
```

38.2.5 Example for Configuring PPPoE+

As shown in Figure 37-1, the Switch is connected to the upstream device BRAS and the downstream device PC; the PPPoE server is configured on the BRAS device. PPPoE+ is enabled on the Switch to control and monitor dialup users.



Step 1 Enable PPPoE+.

```
Switch# configure terminal
Enter configuration commands, one per line.
Switch(config)# pppoe intermediate-agent information enable
```

Step 2 Configure the trusted interface.

```
Switch(config)# interface gigabitethernet 0/1
Switch(config-if-gi 0/1)# pppoe intermediate-agent information trusted
```

Step 3 Enable pppoe+ on client port.

```
Switch(config)# interface fastethernet 0/1
Switch(config-if-fa 0/1)# pppoe intermediate-agent information
Switch(config-if-fa 0/1)# exit
Switch(config)# interface fastethernet 0/2
Switch(config-if-fa 0/2)# pppoe intermediate-agent information
Switch(config-if-fa 0/1)# end
Switch#
```

The following are specific commands for PPPoE+

1.set circuit-id delimiter,you can choose # or . or , or ; or : or space

```
switch(config)#pppoe intermediate-agent delimiter #
switch(config)#pppoe intermediate-agent delimiter ,
```

2.set format of circuit-id and remote-id ,ascii or hex.

```
switch(config)#pppoe intermediate-agent format circuit-id ascii
switch(config)#pppoe intermediate-agent format circuit-id hex
switch(config)#pppoe intermediate-agent format remote-id ascii
switch(config)#pppoe intermediate-agent format remote-id hex
```

3.set cirecuit-id globally,access-node-id or identifier-string ,and value

```
switch(config)#pppoe intermediate-agent type tr-101 circuit-id access-node-id test
switch(config)#pppoe intermediate-agent type tr-101 circuit-id identifier-string test option pv delimiter /
```

4.set circuit-id and remote-id value for one port

```
switch(config-if-gi 0/1)#pppoe intermediate-agent information circuit-id aaa
switch(config-if-gi 0/1)#pppoe intermediate-agent information remote-id bbb
```

5.enable strip vendor tag,it is used for server port.

```
switch(config-if-gi 0/1)#pppoe intermediate-agent information strip
```

39 Configuring Privilege Levels

Switch's system provides two levels of access to the configuration options: read-write access and read-only access.
Privilege levels 1 to 15 are supported.

- Privilege level 15 provides read-write access to system of switch. This is the default.
- Privilege level 15 provides read-write access to web of switch, level 1 only provides read access to web of switch.
- Privilege levels 1 to 14 provide read-only access to system of switch.

If you do not specify a privilege level when you access system of switch, the switch verifies whether you have privilege level 15. If you do not, you are denied access to system of switch. If you do have privilege level 15, you are granted read-write access. Therefore, you do not need to include the privilege level if it is 15.

Configuring the username and privilege levels

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	username *username* privilege [1-15] password *line*	Configuring the username and privilege levels.
Step 3	show running-config	Verify your entries.
Step 4	copy running-config startup-config	(Optional) Save your entries in the configuration file.

Follow these steps to configure username is admin, privilege levels is 15.

```
Switch# configure terminal
Enter configuration commands, one per line.
Switch(config)# username admin privilege 15 admin password admin
Switch(config)# exit
Switch# show running-config
Current configuration:
!
interface vlan 1
  ip address 192.168.2.11/24
  ipv6 address fe80::4644:44ff:fe44:4445/64
no shutdown
!
ip route default 192.168.2.1
!
!
!
username guest privilege 15 password guest
username admin privilege 15 password admin

logging buffered 10000
logging type interface
logging type DAI
!
```

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	service password-encryption	(Optional) Encrypt the password when the password is defined or when the configuration is written. Encryption prevents the password from being readable in the configuration file.
Step 3	show running-config	Verify your entries.
Step 4	copy running-config startup-config	(Optional) Save your entries in the configuration file.

Follow these steps to configure username is admin, privilege levels is 15.

```
switch(config)#service password-encryption

switch(config)#

Switch# show running-config



Current configuration:

!

interface vlan 1

  ip address 192.168.2.11/24

  ipv6 address fe80::4644:44ff:fe44:4445/64

no shutdown

!

ip route default 192.168.2.1
```

```
!

!

!

username guest privilege 15 password 8 bJd4N6cxAnGnc

username admin privilege 15 password 8 4DZYhHHTxfhm.



logging buffered 10000

logging type interface

logging type DAI

!

!

!

service password-encryption

!
```

40 Reboot the switch

	Command	Purpose
Step 1	reload	Reload the switch
Step 2	Save?[y/n]	Type yes or no to save parameters or not
Step 3	[confirm]enter	Confirm reboot

When input “reload” command, display “save?[y/n]”,please type “y” or “n” if you want to save parameters or no ,then display “Proceed with reload? [confirm]”, please press the Enter keyboard.

If you want to cancel this operation, please press any key, Then press the Enter key to return to privileged mode(switch#).

This example shows how to reboot the switch:

```
switch#reload
System configuration has been modified. Save?
[y/n]:y
Proceed with reload? [confirm]

Save parameter may take half a minute, please wait......
Restarting system.
System restart.
```

41 Recovery factory parameters

	Command	Purpose
Step 1	erase startup-config	Erase all config from startup-config
Step 2	[confirm]enter	Confirm this operation.

When input “erase startup-config” command, display “Continue? [confirm]”, please press the Enter keyboard.

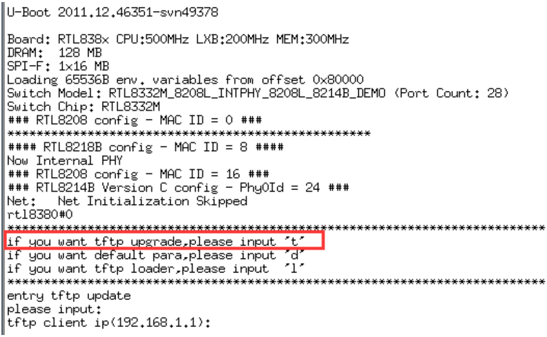
If you want to cancel this operation, please press any key, Then press the Enter key to return to privileged mode(switch#).

This example shows how to recovery factory parameters:

```
switch#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
switch#
switch#reload
System configuration has been modified. Save?
[y/n]:n
Proceed with reload? [confirm]
Restarting system.
System restart.
```

42 Upgrade the switch system by TFTP

When the switch is powered on, check the CLI.
When it shows:



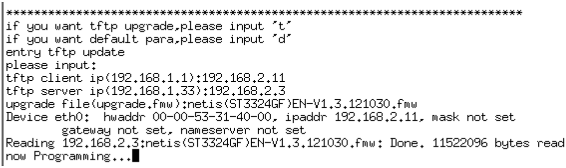
```
U-Boot 2011.12.46351-svn49378

Board: RTL838x CPU:500MHz LXB:200MHz MEM:300MHz
DRAM:  128 MB
SPI-F: 1x16 MB
Loading 65536B env. variables from offset 0x80000
Switch Model: RTL8332M_8208L_INTPHY_8208L_8214B_DEMO (Port Count: 28)
Switch Chip: RTL8332M
### RTL8208 config - MAC ID = 0 ###
**************************************************
#### RTL8218B config - MAC ID = 8 ####
Now Internal PHY
### RTL8208 config - MAC ID = 16 ###
### RTL8214B Version C config - Phy0Id = 24 ###
Net:   Net Initialization Skipped
rtl8380#0
**************************************************************************
if you want tftp upgrade,please input 't'
if you want default para,please input 'd'
if you want tftp loader,please input  'l'
**************************************************************************
entry tftp update
please input:
tftp client ip(192.168.1.1):
```

Step 1 If you want tftp upgrade, please input’t’. Then press “t” to get into TFTP upgrade mode.

Step 2 Run TFTP server， put the upgrade file into the TFTP folder.

Step 3 Input the IP address of switch, e.g. 192.168.2.11

Input the IP address of PC, e.g. 192.168.2.3
Input the file name, e.g. EN-V1.3.171030.fmw
Then press “Enter” to wait upload and upgrade.



```
**************************************************************************
if you want tftp upgrade,please input 't'
if you want default para,please input 'd'
entry tftp update
please input:
tftp client ip(192.168.1.1):192.168.2.11
tftp server ip(192.168.1.33):192.168.2.3
upgrade file(upgrade.fmw):netis(ST3324GF)EN-V1.3.121030.fmw
Device eth0:  hwaddr 00-00-53-31-40-00, ipaddr 192.168.2.11, mask not set
        gateway not set, nameserver not set
Reading 192.168.2.3:netis(ST3324GF)EN-V1.3.121030.fmw: Done. 11522096 bytes read
now Programming...█
```

Step 4 when the upgrade finished, the switch will automatic restart.

Hereby Assmann Electronic GmbH, declares that the Declaration of Conformity is part of the shipping content. If the Declaration of Conformity is missing, you can request it by post under the below mentioned manufacturer address.

www.assmann.com
Assmann Electronic GmbH
Auf dem Schüffel 3
58513 Lüdenscheid
Germany