



GIGABIT MANAGED POE SWITCH



DN-95351



DN-95352

User Manual

Manual Description

This user guide is provided for using this type of switch. The manual includes the switch performance and function. Please read this manual before managing the device:

Intended Audience

This guide is intended for network administrators familiar with IT concepts and network terminology.

SAFETY NOTICES

Do not use this product near water, for example, in a wet basement or near a swimming pool. Avoid using this product during an electrical storm. There may be a remote risk of electric shock from lightning.

Contents

Chapter1: Login the Device	6
1.1 Login the device	6
1.2 Functional Overview	7
Chapter 2: System	8
2.1 The Home page.....	8
2.2 System Information.....	8
2.3 Interface IP	9
2.4 HTTP Port	10
2.5 Console.....	11
2.6 System Time Config.....	11
2.7 System Update.....	12
2.8 Backup/Recovery	12
2.9 Load Default	13
2.10 Reboot.....	13
2.11 Show Cli Running.....	14
2.12 Password	14
Chapter 3: SNMP	15
3.1 Understanding SNMP	15
3.2 Basic Config	18
3.3 Community	19
3.4 Management Station.....	20
3.5 V3Engine ID	20
3.6 V3Group Config.....	21
3.7 V3User Config	22
3.8 V3View Config.....	23
Chapter 4: Port Management.....	24
4.1 Port Configuration.....	24

4.2 Port Statistics.....	25
4.3 Band Restricting.....	25
4.4 Port Description.....	26
4.5 Storm Control.....	26
4.6 POE.....	28
Chapter 5: Redundancy.....	29
5.1 Link Aggregation.....	32
5.2 LACP.....	33
5.3 Smart /Monitor Link.....	34
5.4 RRP.....	37
5.5 STP/RSTP/MSTP.....	42
Chapter 6: Security.....	57
6.1 ACL.....	57
6.2 VLAN.....	61
6.3 MAC Config.....	65
6.4 IEEE802.1x.....	68
6.5 DHCP.....	74
6.6 ARP.....	84
Chapter 7: QoS.....	86
7.1 Qos Information.....	91
7.2 DSCP Queue Mapping.....	92
7.3 802.1p-Queue Mapping.....	93
7.4 Port Default Priority.....	94
7.5 Queue Scheduling.....	95
Chapter 8: Multicast.....	95
8.1 IGMP Snooping.....	99
8.2 Cross VLAN.....	100
8.3 IGMP Route Port.....	100
8.4 IGMP Port Policy.....	101
8.5 IGMP Group Policy.....	102
Chapter 9: Network Analysis.....	103

9.1 Traffic Counter	103
9.2 Port Mirror	103
9.3 Ping	105
9.4 Log	105
Chapter10: Network Equipment.....	106
10.1 Loopback Detection	106
Chapter11: Advanced Setup.....	107
11.1 GVRP	107
11.2 SSH	110
11.3 Web Cli	112
Chapter 12: Save Parameters	113
Chapter 13: FAQ	113
13.1 Link status indicator don't shows normal (Link-Error)	113
13.2 Link status indicator show normal but can't communication.....	113
13.3 Can't login to manage switch	114
13.4 Switch start-up failure	114
13.5 Power failure	115

The Management switch is managed via WEB pages. The smart and friendly interfaces make the switch management an easy job. You can use the web browser-based configuration to manage switch. The switch to be configured through a web browser, at least a reasonable allocation of computer through an Ethernet connection to the switch.



Figure 1-1

Chapter 1: Login the Device

The machine-default IP address is **192.168.2.11**, subnet mask is **255.255.255.0**. So when you log on to the switch, make sure the IP address of the computer network card and the IP of the switch in the same network segment: 192.168.2.*** (1 <*** <255, *** is not equal to 11). Reference to the following steps to set up:

1.1 Login the device

1. Open IE browser, enter **http://192.168.2.11** in the address bar, then return.



Figure 1-1-1

2. In the pop-up window to enter **user name: guest, password: guest**, then press the OK button

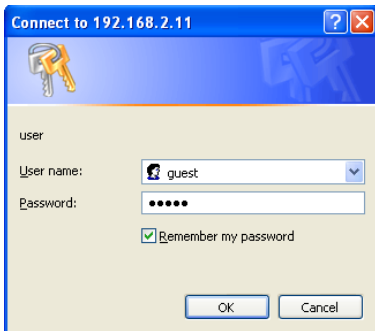


Figure 1-1-2

NOTES:

If you are successful login into the switch webpage, the page from time to time automatically refresh, allowing you to dynamically view the port status.

1.2 Functional Overview

The switch have rich feature ,including the functions of system management, SNMP management, Port Management, Redundancy management, Security management , QoS management, Multicast management, Network Analysis, Network Equipment , and Advanced Setup, next chapter will introduce you these functions.



Figure 1-2-1

Chapter 2: System

2.1 The Home page

After logging into the switch, the main page appears as the following. It contains three parts:



Figure 2-1-1

zone"1": The Port LED Indicator table lies at the top of the page. It provides a visual representation of the ports. The green icon indicates that the port is linked; the gray icon indicates that the port is not linked;

zone"2": On the left side of the page is the menu table. It contains 10 main menus. Each menu has some submenus. Click on a menu, it will open its submenus and the main window.

zone"3": The main part of the page is the main window to display the configuration page.

2.2 System Information

Click on the "System ", the switch manage page will show as figure below, The system submenu have basic information, including: system information, Interface IP, HTTP Port, Console, System Time

Config, System Update, Backup/Recovery, Load Default, Reboot, Show Cli Running, User Information;. The following picture is the detailed description.

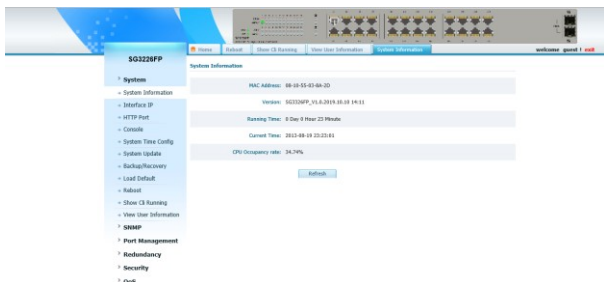


Figure 2-2-1

The System Information shows the system information of the switch, such as model, MAC address, , hardware and software version information, Running Time, Current Time, CPU Utilization Rate.

2.3 Interface IP



Figure 2-3-1

On this page you can manually set the IP address, subnet mask, gateway and other information; can also use your network, among

other DHCP SERVER switch automatically assigns an IP address. The switch default IP address is: 192.168.2.11 default subnet mask: 255.255.255.0 Default Gateway: no. When finished editing, click the "OK" to complete the IP address settings.

Notes:

- (1)When you select "DHCP Settings" is disabled, the switch will have to manually assign an IP address.
- (2)When DHCP client is enabled, the IP parameters are obtained automatically from the DHCP server.

2.4 HTTP Port

This page provides the configuring HTTP Port.

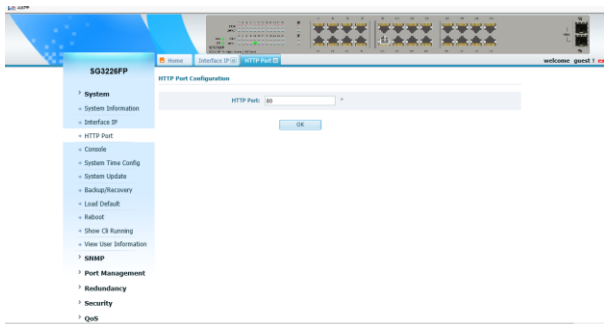


Figure 2-4-1

You are kindly suggested to type the HTTP Port, default is 80.

Caution:

Only numbers can be input into Port. The other characters are considered illegal. The initial port is 80.

Notes:

After modifying the HTTP Port, for example, if you change the port as 8080, then you need use ip of 192.168.2.11:8080 in the address bar, then return.

2.5 Console

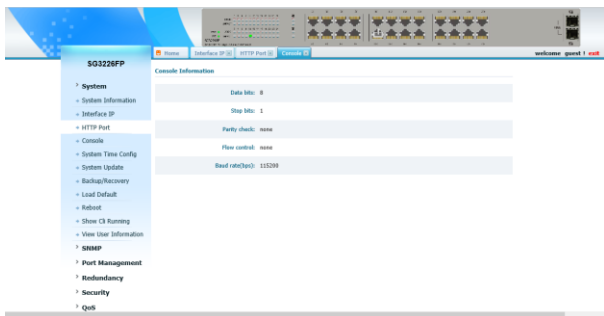


Figure 2-5-1

The figure shows the switch connected information for user to configure through the console.

2.6 System Time Config

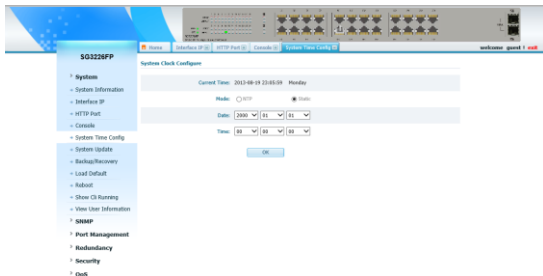


Figure 2-6-1

You can adjust the time to the local through the option. Click “OK” When you have corrected the time.

2.7 System Update



Figure 2-7-1

Browse the right file you need to complete the update, it will spent about 2 minutes to finish. Make sure the power is on and do not restart during the updating program. When it shows that is successful you can restart the switch.

2.8 Backup/Recovery

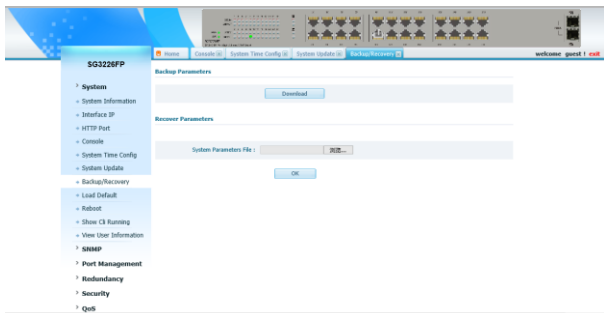


Figure 2-8-1

In this step you can recovery the system of the switch if you want to back to the old system. And you need to load the software you refresh just now.

2.9 Load Default

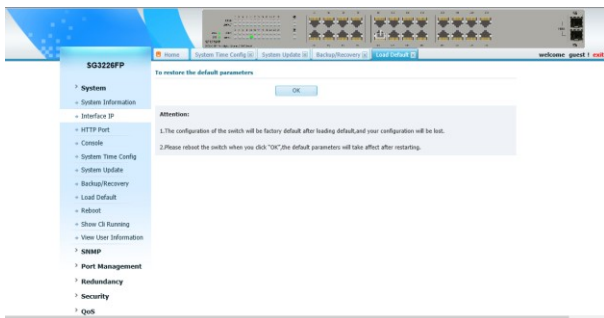


Figure 2-9-1

In this step you will restore the factory setting. The operation would delete the current configuration and irrecoverable! Are you sure to recover default configuration? Click 'Ok' to recover default configuration, and then reboot the switch to make it effect!

2.10 Reboot

On this page you can reboot the switch and return to the login page .Please save the current configuration before reboot or you will lose the configuration.



Figure 2-10-1

2.11 Show Cli Running

On this page you can get the running config of this switch.

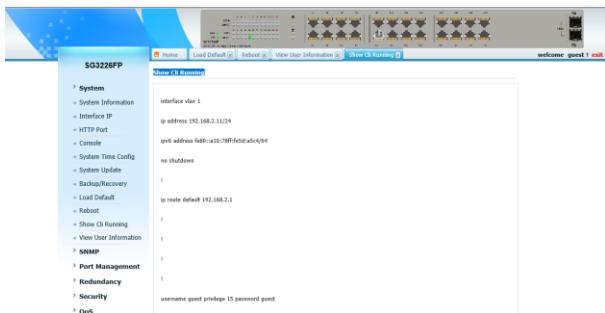


Figure 2-11-1

2.12 Password

This page provides the interface of configuring password.

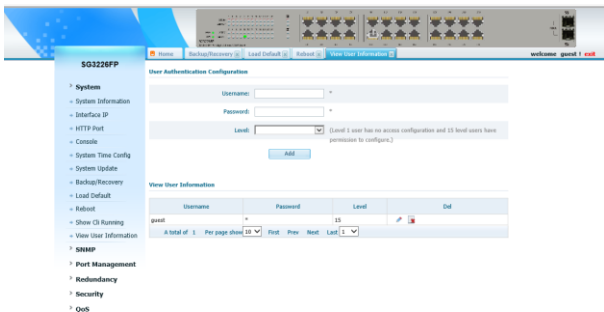


Figure 2-12-1

You are kindly suggested to retype the new password in "Confirm new password" box instead of copying in order to avoid typing mistakes.

Caution:

Only letters, numbers and punctuations can be input into username and password. The other characters are considered illegal. The length of password ranges from 1 to 16 characters. The initial password is guest

Notes:

After modifying the password with immediate effect, the parameters will not be lost though is powered off

Chapter 3: SNMP

3.1 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 Cisco Works. 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 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. 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.

3.2 Basic Config

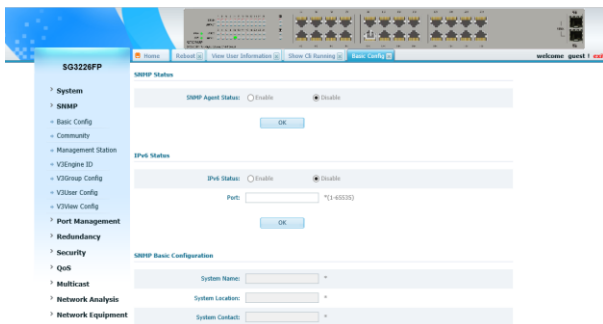


Figure 3-2-1

In this step you need to enable SNMP function first, and then you can set the System Name, Location and Contact

3.3 Community



Figure 3-3-1

On this page, you can configure SNMP Group to the network access by providing the users in various groups with different management rights (Read View and Write View).

Community: Name defined by administrator.

Manage IP: The IP who can manage the switch through the community.

SMMP View: The OID accessed by the community.

Popedom: Read Only or Read/Write.

Notes:

Every Group should contain a Read View .The default Read View is View fault.

3.4 Management Station

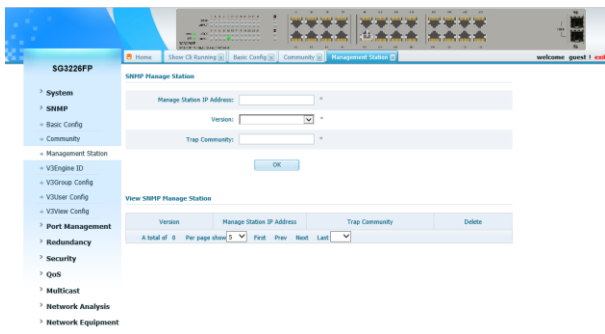


Figure 3-4-1

SNMP Management Station is the workstation for running the SNMP client program, trap agent send urgent log to the management station. You need set IP and community.

3.5 V3Engine ID



Figure 3-5-1

On this page, the default of the V3Engine ID is not configurable.

3.6 V3Group Config

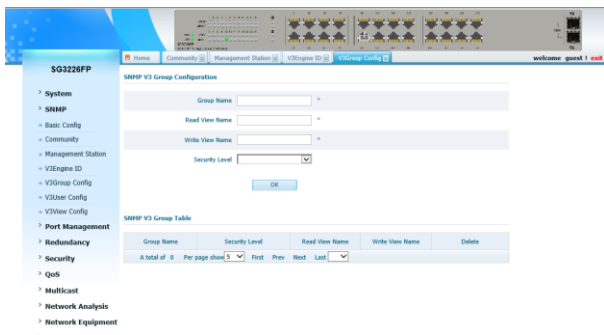


Figure 3-6-1

Group Name: The Group Name, security Model and Security Level compose the identifier of the SNMP Group.

Read View Name: The management access is restricted to read-only, and changes cannot be made to the assigned SNMP View. Configure it as the Figure 5-1-5.

Write View Name: The management access is writing only and changes can be made to the assigned SNMP View .The View defined both as the Read View and the write view can be read and modified. Configure it as the Figure 5-1-5.

Security Level:

NoAuthNoPriv: Not Certified and Not Encrypted.

AuthNoPriv: Certified and Not Encrypted.

AuthPriv: Certified and Encrypted.

3.7 V3User Config



Figure 3-7-1

On this page, it shows the V3User configuration.

User Name: The user name needs to be added.

User Group: The group that the user belongs to.

Validated and Encrypted: Whether needs to open the Validated and Encrypted.

Auth- Protocol: After opening the Validate/Encrypt, it should select MD5 or SHA and configure password unless than 8 digit.

Priv-Protocol: whether needs to open the function of Encrypted .It should select DES and configure password unless than 8 digit.

3.8 V3View Config

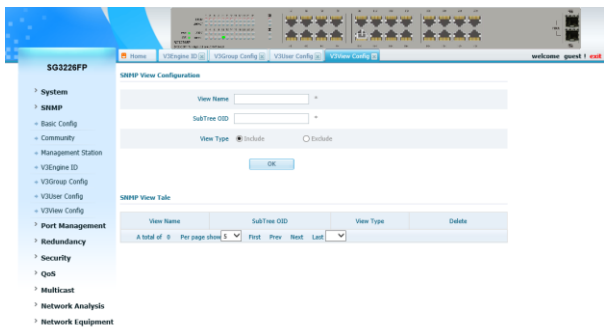


Figure 3-8-1

Configure the SNMP V3view as Figure 5-1-7.

View Name: The new View name.

SubTree OID: It means the View needs OID.

View type: Including means the SubTree displaying View. Exclude means the left of the SubTree displaying View.

Chapter 4: Port Management

4.1 Port Configuration

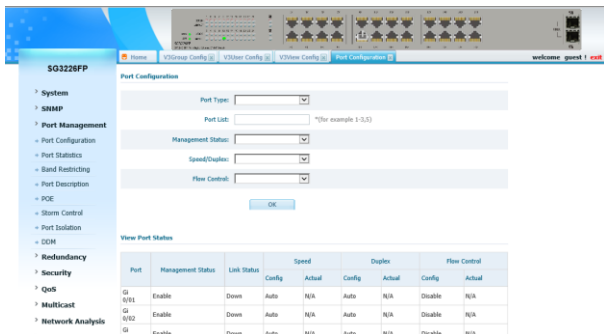


Figure 4-1-1

On this page ,you can configure the basic parameter for the ports .When the port is disabled ,the packets on the port will be discard .Shut down the port which is vacant for a long time can reduce the power consumption effectively .And you can enable the port when it is in need. The parameters will affect the working mode of the ports, please set the parameters appropriate.

Management Status: Allows you to Enable/Disable the port .When Enable is set, the port can forward the packets normally.

Speed and Duplex: Select the speed and Duplex mode for the port .The device connected to the switch should be in the same Speed and Duplex mode with the switch .When “Auto” is set, the Speed and Duplex mode will be determined by auto-negotiation. But the SFP port, this Switch does not support auto-negotiation.

Flow Control: Allows you to Enable /Disable the Flow Control feature .When Flow Control is enabled, the switch can synchronize the speed with its peer to avoid the congestion.

4.2 Port Statistics

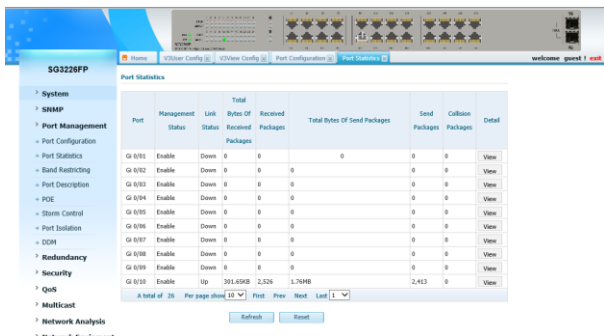


Figure 4-2-1

Port Statics: It includes Link Status, total bytes of received packages, received packages, total bytes of send packages, send packages, collision packages, and discarded packages.

4.3 Band Restricting

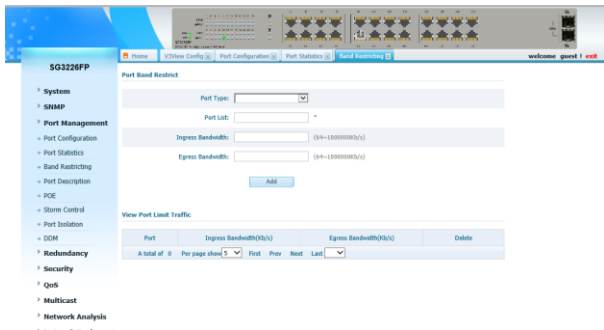


Figure 4-3-1

Bandwidth function, allowing you to control the traffic rate and

broadcast flow on each port, can be implemented on the Rate Limit and Storm Control pages.

4.4 Port Description

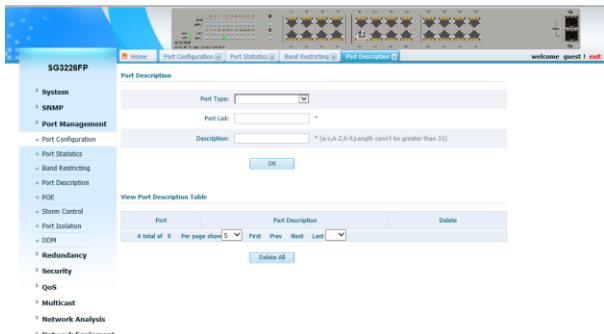


Figure 4-4-1

Port Description can make a sign to the port which is convenient for you to find any useful information quickly.

4.5 Storm Control

4.5.1 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.

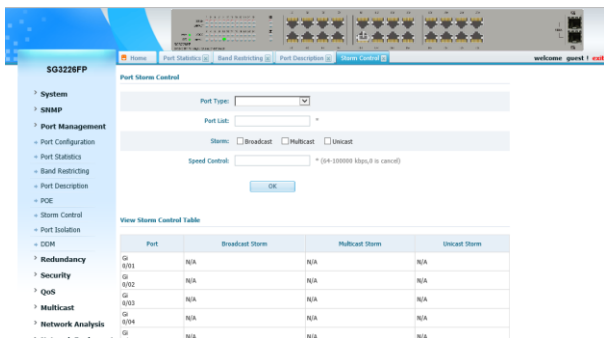


Figure 4-5-1

Set and view limit of broadcast, multicast, unknown unicast flood level on port.

4.6 POE

Introduction to PoE

This function is only in PE series switches.

Power over Ethernet (PoE) means that power sourcing equipment (PSE) supplies power to powered devices (PD) such as IP Phone, 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.

POE Status

Vmain: 54.47V

Pconsume: 1.70W

POE Configuration

Port Type:

Port List:

POE Management: Enable Disable

Figure 4-6-1

On POE page, you can check consume, and set if PoE is enabled on each port.

Input port number and set enable or disable, then press OK.

View POE Configuration Status

Port	POE Management	Operational Status	Classification	Power Supply PRI	Consumption
Fa 0/01	Auto	N/A	ClassHalt	Critical	0.00W
Fa 0/02	Auto	On	Class3	Critical	1.70W
Fa 0/03	Auto	N/A	ClassHalt	Critical	0.00W
Fa 0/04	Auto	N/A	ClassHalt	Critical	0.00W
Fa 0/05	Auto	N/A	ClassHalt	Critical	0.00W
Fa 0/06	Auto	N/A	ClassHalt	Critical	0.00W
Fa 0/07	Auto	N/A	ClassHalt	Critical	0.00W
Fa 0/08	Auto	N/A	ClassHalt	Critical	0.00W
Fa 0/09	Auto	N/A	ClassHalt	Critical	0.00W
Fa 0/10	Auto	N/A	ClassHalt	Critical	0.00W

A total of 24 Per page show 10 First Prev Next Last 1

Figure 4-6-2

On the below part of POE page, you can check management and consume of each port.

Chapter 5: Redundancy

Understanding Ether Channels

Ether Channel 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. Ether Channel provides automatic recovery for the loss of a link by redistributing the load across the remaining links. If a link fails, Ether Channel redirects traffic from the failed link to the remaining links in the channel without intervention.

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

Introduction to Link Aggregation

Link aggregation can aggregate multiple Ethernet ports together to form a logical aggregation group. To upper layer entities, all the physical links in an aggregation group are a single logical link. Link aggregation is designed to increase bandwidth by implementing

outgoing/incoming load sharing among the member ports in an aggregation group. Link aggregation group also allows for port redundancy, which improves connection reliability.

Introduction to LACP

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

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

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

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

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

Exchanging LACP Packets

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

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 Ether Channel 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 Ether Channel connects the switch to the router.

Source-based load balancing is used on the switch end of the Ether Channel 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 Ether Channel.

5.1 Link Aggregation

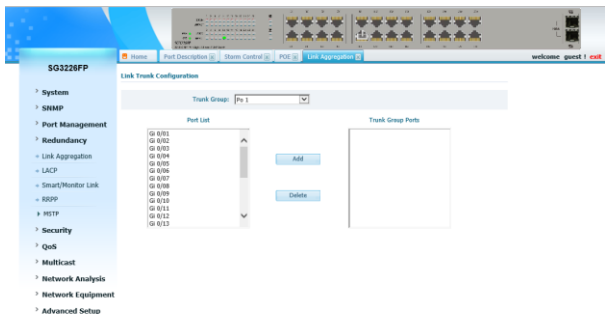


Figure 5-1-1

Select an aggregation group number, and then add port in the left form to the right form, that makes port join into aggregation group. The switch has max 8 groups, and one aggregation group can support max 8 member ports.

Attention:

100M port and 1000M port cannot join into a same aggregation group.

5.2 LACP

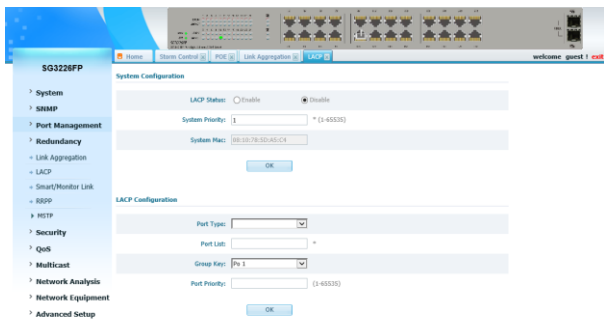


Figure 5-2-1

System Configuration:

LACP Status: you can disable or enable LACP function.

System Priority: set priority of switch

System Mac: show system default MAC, cannot modify.

LACP Configuration:

Port: input the port number which you want to set

Group key: select a group number which you want the port joins into

Mode: set the port LACP mode

Port priority: set the port LACP priority

View Port Information

Group	Port	Port Priority	Activity	Timeout	Aggregation	Synchronization	Collecting	Distributing	Defaulted	Expired	Delete
1	Fa 0/01	1	Active	Long	False	True	False	False	True	True	
1	Fa 0/02	1	Active	Long	False	True	False	False	True	True	

A total of 2 Per page show 10 First Prev Next Last 1

View Partner's information

Actor Port	Group	Port Priority	Activity	Timeout	Aggregation	Synchronization	Collecting	Distributing	Defaulted	Expired
Fa 0/01	0	0	Passive	Short	False	False	False	False	False	False
Fa 0/02	0	0	Passive	Short	False	False	False	False	False	False

A total of 2 Per page show 10 First Prev Next Last 1

View Standby Port

Group	Standby Port
A total of 0 Per page show 5 First Prev Next Last	

View Unselected Port

Group	Unselected Port
1	Fa 0/01 Fa 0/02

A total of 1 Per page show 10 First Prev Next Last 1

Figure 5-2-2

View information of port, partner, stand by port and unselected port.

5.3 Smart /Monitor Link

Basic Concepts in Smart Link

Smart Link Group

A smart link group consists of two member ports: the master port and the slave port. A port can belong to different smart link groups at the same time. Normally, at a time, only one port (master or slave) is active for forwarding, while the other port is blocked, that is, in the standby state.

Master Port

The master port of a smart link group is a port role specified using commands. It can be an Ethernet port (electrical or optical), or an aggregate interface.

Slave Port

The slave port of a smart link group is another port role specified using commands. It can be an Ethernet port (electrical or optical), or an aggregate interface. The link on which the slave port resides is called the backup link.

Basic Concepts in Monitor Link

Monitor Link Group

A monitor link group is a set of uplink and downlink ports. Downlink ports adapt to the state changes of uplink ports.

Uplink Port

An uplink port is a monitored port in a monitor link group. It is a port role specified using commands. It can be an Ethernet port (electrical or optical), or an aggregate interface.

Downlink Port

A downlink port is a monitoring port in a monitor link group. It is another port role specified using commands. It can be an Ethernet port (electrical or optical), or an aggregate interface.

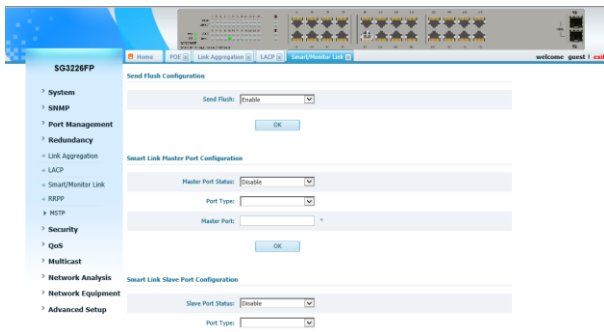


Figure 5-3-1

Send flush: you can disable or enable send flush status.

Master port status: set a port is master port or not.

Port: input port type and number which you want to set.

Slave port status: set a port is slave port or not.

Port: input port type and number which you want to set.

Monitor Up Link Configuration

Up link Port Status:

Port Type:

Up link Port:

Monitor Down Link Configuration

Down Link Port Status:

Port Type:

Port List:

Figure 5-3-2

Up link port status: set a port is up link port or not.

Port: input port type and number which you want to set.

Down link status: set a port is down link port or not.

Port: input port type and number which you want to set.

View Smart Link

Member	Role	Status
A total of 0		
Per page show	5	First Prev Next Last

View Monitor Link

Member	Role	Status
A total of 0		
Per page show	5	First Prev Next Last

Figure 5-3-3

View configuration of smart link and monitor link.

5.4 RRPP

Introduce RRPP

RRPP Domain

An RRPP domain identified by an integral ID defines a topology range calculated and controlled by the RRPP protocol. It consists of some interconnected devices with the same domain ID, control VLANs, and protected VLANs. A device can belong to multiple RRPP domains.

An RRPP domain consists of the following elements:

- RRPP rings
- RRPP control VLANs
- RRPP protected VLANs
- Master nodes
- Transit nodes
- Edge nodes
- Assistant-edge nodes

RRPP Ring

Each RRPP ring corresponds to a ring-shaped Ethernet topology and is identified by an integral ID. As described in the last section, an RRPP domain consists of a single RRPP ring or multiple connected RRPP rings. The topology calculation is actually based on RRPP rings. Typically, ring topologies fall into these three types: single ring, tangent rings, and intersecting rings. For each topology type, the RRPP domain configuration is different:

All devices on the single ring are configured to be in the same RRPP domain.

All devices on intersecting rings are also configured to be in the same RRPP domain.

For two tangent rings, the devices on each ring are configured to be in the same RRPP domain. That is, two tangent rings need two different RRPP domains, one for each ring.

In an RRPP domain with intersecting rings, to achieve independent topology calculation on each ring without affecting other rings and prevent loops, you need to configure one ring as the primary ring and the others as subrings. The primary ring as a whole serves as a logical node on the subrings, and protocol packets from the subrings

are transparently transmitted through the primary ring. In this way, topology calculation is performed on the intersecting rings as a whole.

Protocol packets of the primary ring are confined within the primary ring. The level of the primary ring is 0 and that of subrings is 1.

RRPP Control VLAN

As described earlier, RRPP separates data traffic from RRPPDUs (RRPP packets) by transmitting RRPPDUs in dedicated VLANs called control VLANs. An RRPP domain is configured with one primary control VLAN and one secondary control VLAN. After you specify a VLAN as the primary control VLAN, the VLAN whose ID is one plus the primary control VLAN ID is configured as the secondary control VLAN automatically. The primary control VLAN transmits the RRPPDUs of the primary ring and the EDGE-HELLO messages of the subrings. The secondary control VLAN transmits the RRPPDUs of the subrings except the EDGE-HELLO messages.

All the ports connecting devices to RRPP rings are assigned to control VLANs, and only such ports can be assigned to control VLANs.

RRPP Protected VLAN

A protected VLAN is a VLAN that transmits data packets. It can contain both RRPP ports and non-RRPP ports. A protected VLAN's forwarding status is controlled by its RRPP domain. Different RRPP domains on the same RRPP ring are configured with different protected VLANs, and each RRPP domain controls the forwarding status of ports in it independently.

Master Node

Each device on an RRPP ring is called an RRPP node. On an RRPP ring, you must configure only one as the master node. The master node initiates ring status detection with the polling mechanism and makes operation decisions upon ring topology changes.

A master node can be in one of the following states:

- Complete state

The master node is in the complete state if it can receive at its secondary port the Hello packets sent out its primary port. In this case, the master node blocks the secondary port to prevent traffic loops.

- Failed state

When a link in the ring fails, the master node is in the failed state. To avoid traffic interruption in the ring, the master node unblocks the secondary port to forward data traffic.

Note:

The state of the master node represents the state of the whole RRPP ring. That is, when the master node is in the complete (failed) state, the RRPP ring is also in the complete (failed) state.

Transit Node

All the nodes except the master node on a ring are transit nodes. A transit node can be in one of the following states depending on the states of its primary and secondary ports:

- Link-up state

When both the primary port and secondary port are up, the transit node is in the link-up state.

- Link-down state

When either the primary port or the secondary port is down, the transit node is in the link-down state.

- Pre-forwarding state

When either the primary port or the secondary port is blocked, the transit node is in the pre-forwarding state.

Edge Node and Assistant-Edge Node

In an RRPP domain, of the two nodes at which the primary ring and a subring intersect, one is the edge node and the other is the assistant-edge node. You can configure either of them as the edge or the assistant-edge but must ensure that the roles of the two nodes are different.

Edge nodes and assistant-edge nodes are special transit nodes. An edge or edge-assistant node can be in one of the following three states depending on the state of its edge port:

- Link-up state

When the edge port is up, the node is in the link-up state.

- Link-down state

When the edge port is down, the node is in the link-down state.

- Pre-forwarding state

When the edge port is blocked, the node is in the pre-forwarding state.

The state transition of an edge or edge-assistant node is the same as that of a transit node but it is triggered by the link state change of the edge port only.

Primary Port and Secondary Port

Of the ports that connect a node to an RRPP ring, one is the primary port and the other is the secondary port. You can configure them as needed.

The primary and secondary ports of master nodes are different in functions. A master node sends HELLO messages out its primary port. If it can receive these HELLO messages on its secondary port, the master node considers the RRPP ring as complete and thus blocks the secondary port to avoid loops. If the master node fails to receive these HELLO messages within the specified period, it considers the ring as having failed and unblocks the secondary port to ensure service continuity.

The primary and secondary ports of a transit node are the same in functions.

In an RRPP domain, the primary ring is a logical node of each subring and it transmits subring RRPPDUs (except the EDGE-HELLO messages) transparently as data traffic. Therefore, no data packet or subring RRPPDU (except the EDGE-HELLO messages) can pass through a blocked port on the primary ring.

Common Port and Edge Port

On an edge or assistant-edge node, the port connecting to the subring is called the edge port while the two ports connecting to the primary ring are called common ports. The link between the common port on the edge node and that on the assistant-edge node is called the common link.

As a primary ring is considered as a logical node on its siblings, the common link is considered as an internal link of the “primary ring” node. Thus, the common link state changes are reported only to the master node of the primary ring.



Figure 5-4-1

RRPP Configuration

Domain ID: input a Domain ID here.

Ring ID: input a Ring ID here

Node Role: set Node role is master or transit

Primary port: select and set primary port number

Secondary port: select and set secondary port number

Control VID: input control VLAN id.

RRPP State Configuration

RRPP State: config rrp function is enable or disable globally.

RRPP Timer Configuration

Hello-timer: * (1-100)

Fail-timer: * (1-100 and fail time >= 3*hello timer)

Delete Ring

Ring ID: * (1-66)

Figure 5-4-2

RRPP Timer Configuration

Hello timer: set interval time the switch sends rrrp hello,default is 1 second.

Fail-timer: set a time period,which can help slave port to know whether receive a hello or not.

Delete Ring

Ring ID: input ring id then press OK,this can delete the ring set before.

View RRPP Info

Ring status	Domain id	Ring id	Control VID	Node role	Primary port	Primary state	Secondary port	Secondary state
Active	1	1	2	MASTER	Fa 0/01	Link Down	Fa 0/02	Link Down
A total of 1		Per page show	10	First	Prev	Next	Last	1

Figure 5-4-3

View rrrp infomation

5.5 STP/RSTP/MSTP

5.5.1 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 along 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 send 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.

5.5.2 STP Configure

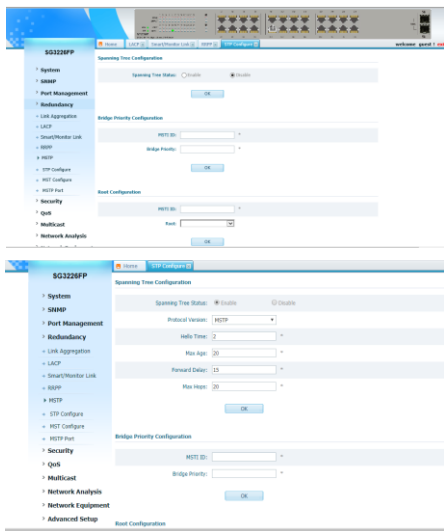


Figure 5-5-1

Rapid Spanning Configuration

Spanning Tree Status: Whether enable stp on switch.

Protocol Version: MSTP is recommended.

Hello Time: Set hello time, it's 2 by default.

Max Age: Set max-age, it's 20 by default.

Forward Delay: Set forward delay, it's 15 by default.

Max Hops: Set max hops, it's 20 by default.

Bridge Priority Configuration

MSTI ID: Choose one MSTI ID.

Bridge priority: Set bridge priority of the MSTI ID.

Root Configuration

MSTI ID: Choose one MSTI ID.

Root: Set the MSTI ID is primary root or secondary root.

View Spanning Tree Information

Instance	Root priority	mac	hello time	max age	forward delay	max hops	Bridge priority	Root
MST 0	32768	44-44-44-44-44-44	2	20	15	20	32768	CIST Root

A total of 1 Per page show 10 First Prev Next Last 1

Refresh

Figure 5-5-2

View information of spanning tree running

5.5.3 MSTP

5.5.3.1 MSTP Overview

Background of MSTP

Disadvantages of STP and RSTP

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

The rapid spanning tree protocol (RSTP) is an optimized version of STP. RSTP allows a newly elected root port or designated port to

enter the forwarding state much quicker under certain conditions than in STP. As a result, it takes a shorter time for the network to reach the final topology stability.

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

Features of MSTP

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

MSTP features the following:

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

Basic MSTP Terminologies

MST region

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

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

MSTI

A multiple spanning tree instance (MSTI) refers to a spanning tree in an MST region.

Multiple spanning trees can be established in one MST region. These spanning trees are independent of each other.

VLAN mapping table

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

IST

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

CST

A CST is a single spanning tree in a switched network that connects all MST regions in the network. If you regard each MST region in the network as a switch, then the CST is the spanning tree generated by STP or RSTP running on the "switches".

CIST

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

Region root

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

Common root bridge

The common root bridge is the root of the CIST.

Port role

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

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

Port state

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

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

Principle of MSTP

MSTP divides a Layer 2 network into multiple MST regions. The CSTs are generated between these MST regions, and multiple spanning

trees (also called MSTIs) can be generated in each MST region. As well as RSTP, MSTP uses configuration BPDUs for spanning tree calculation. The only difference is that the configuration BPDUs for MSTP carries 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

5.5.3.2 MST Configure

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.



Figure 5-5-3

MST Region Configuration

Name: MST region name

MSTI ID: Create MSTP instance number.

VID: Create VLAN map to instance.

Revision: Defined by yourself.

Bpdu Set

Digest Snooping Status: Whether enable digest snooping on global.

Bpdu Filter: Whether enable bpdu filter on global.

Protection state: Whether enable bpdu guard on global.

Bpdu Interval state: You can set bpdu interval here and input the

time.

View Instance

View instances running on the switch.

5.5.3.3 MSTP Port

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.

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.

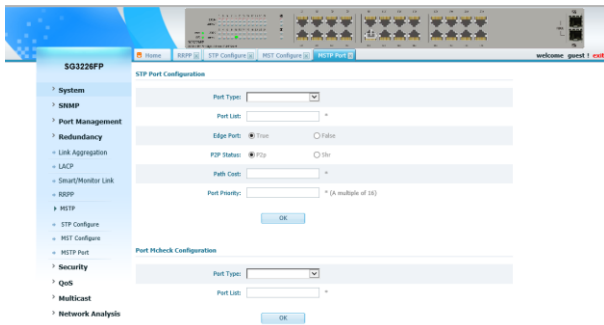


Figure 5-5-4

STP Port Configuration

Port type & List: Choose the port you want to set.

Edge Port: Set the port to be edge port or not.

P2P Status: Set the port to be P2P port or not.

Path Cost: Set the port cost on global.

Port Priority: Set the port priority on global.

Port Mcheck Configuration

Port MST Configuration

Port Type:

Port List:

Digest Snooping: Enable Disable

Bpdu Filtering/Guard Status: Enable Disable

MSTI:

Path Cost:

Port Priority: * (A multiple of 16)

View Port Status

Hub	Port	Port Role	Status	Port cost	Port priority	Digest Snooping	P2p port	Edge port	Protocol Mode
0	Fa 0/01	Disb	BLK	0	128	Disable	Shr	False	MSTP
0	Fa 0/02	Disb	BLK	0	128	Disable	Shr	False	MSTP
0	Fa 0/03	Disb	BLK	0	128	Disable	Shr	False	MSTP
0	Fa 0/04	Disb	BLK	0	128	Disable	Shr	False	MSTP
0	Fa 0/05	Disb	BLK	0	128	Disable	Shr	False	MSTP
0	Fa 0/06	Disb	BLK	0	128	Disable	Shr	False	MSTP
0	Fa 0/07	Disb	BLK	0	128	Disable	Shr	False	MSTP
0	Fa 0/08	Disb	BLK	0	128	Disable	Shr	False	MSTP
0	Fa 0/09	Disb	BLK	0	128	Disable	Shr	False	MSTP
0	Fa 0/10	Disb	BLK	0	128	Disable	Shr	False	MSTP

A total of 28 Per page show First Prev Next Last

Figure 5-5-5

Port MST Configuration

Port type & list: Choose the port you want to set.

Digest Snooping: Whether enable digest snooping on port.

Bpdu Filtering/Guard Status: Whether enable BPDU filter or Guard on port.

MSTI: Choose MSTI you want to set.

Path Cost: Input cost value in the MSTI

Port Priority: Input priority value in the MSTI.

View Ports Status

View port status in every instance of stp.

Chapter 6: Security

6.1 ACL

6.1.1 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.

6.1.2 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.)

6.1.3 ACL Config

The image displays two screenshots of the SG3226FP switch configuration interface. The top screenshot shows the 'ACL Configuration' page with the following settings:

- ACL Type: Standard MAC ACL
- Permit/Deny: PERMIT
- Source MAC Address Type: Any
- Source MAC Address: 00-00-00-00-00-00
- Source MAC Mask: 00-00-00-00-00-00
- Cos: (0-7)
- DSCP: (0-63)

The bottom screenshot shows the 'ACL Configuration' page with the following settings:

- ACL Type: Extended MAC ACL
- Permit/Deny: PERMIT
- Source MAC Address Type: Host
- Source MAC Address: 00-00-00-00-00-01
- Source MAC Mask: ff-ff-ff-ff-ff-ff
- Destination MAC Address Type: Host
- Destination MAC Address: 00-00-00-00-00-02
- Destination MAC Mask: ff-ff-ff-ff-ff-ff
- Cos: 7 (0-7)
- DSCP: 63 (0-63)

Figure 6-1-1

There are 5 types of ACL on the switch, as Standard MAC ACL, Extended MAC ACL, Standard IP ACL, Extended IP ACL and Protocol type-code. Here shows you the configuration of Standard MAC ACL for example.

ACL Type: Choose one type of ACL.

Permit/Deny: Set the switch permit packets matched ACL to go through or discard.

Source MAC Address Type: Set all MAC addresses (any) or specific MAC addresses (host)

Source Mac Address: Fill source MAC address you want to control.

Source MAC Mask: Fill source MAC mask you want to control

Destination MAC Address: Fill source MAC address you want to control.

Destination MAC Mask: Fill Destination MAC mask you want to control

Counter: Fill name, then will create a counter of packets match ACL.

Police: Speed restrict of flow matched ACL.

Capture Port: If input port number, the flow matched ACL will captured to the port.

Cos: If fill a cos, it means specify flow with this cos value is matched the ACL.

Dscp: If fill a dscp, it means specify flow with this dscp value is matched the ACL.

Cos rewrite: 1p priority will be rewrite to the new value if flow matched ACL.

DSCP rewrite: Dscp will be rewrite to the new value if flow matched ACL.

Time Bucket: First create a time-range what time you want ACL gets effect, then check it.

6.1.4 Time Range

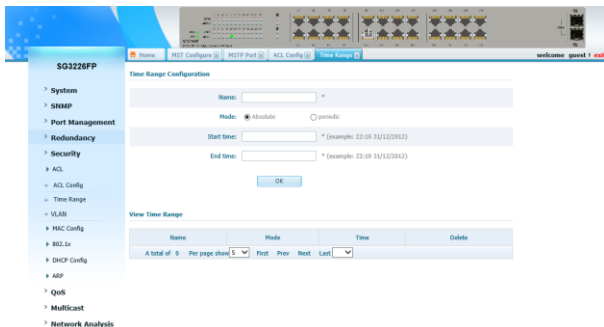


Figure 6-1-2

Name: Fill a time-range name so that you can choose and bind it into a ACL.

Mode: The time-range runs mode, absolute or periodic.

Start time: Fill time point which ACL get start.

End time: Fill time point which ACL get off effect.

6.2 VLAN

6.2.1 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.

6.2.2 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.

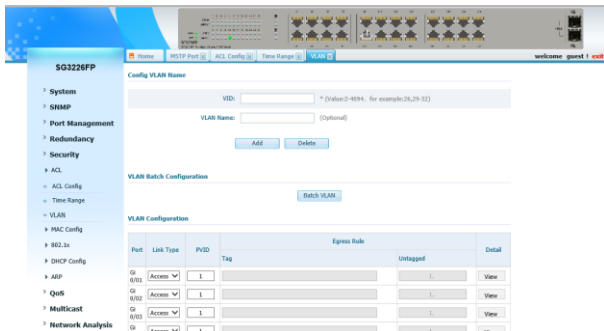


Figure 6-2-1

Config VLAN Name

VID: Input VID you want to create.

VLAN Name: Input the name of VLAN you want to create, then press Add to create.

VLAN Config

Link type: Choose Access, Trunk or Hybrid of the port you want to set.

PVID: Input PVID of the port.

Tag: Click the blank and input tag VIDs. Cannot input in access mode.

Untagged: Click the blank and input untagged VIDs. Only can input in Hybrid mode.

Batch VLAN



Figure 6-2-2

802.1Q VLAN Port Configuration

Port Type & List: You can input many ports number which you want to set, eg.1, 2, 3-5.

Link type: Access, Trunk or Hybrid.

PVID: Input PVID of these ports.

Configure VLAN Name

VID: Input VID you want to create.

VLAN Name: Input the name of VLAN you want to create, and then press Add to create.

View Vlan

VID	VLAN Name	Member
1	default vlan	Fa 0/01,Fa 0/02,Fa 0/03,Fa 0/04,Fa 0/05,Fa 0/06,Fa 0/07,Fa 0/08,Fa 0/09,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 0/01,Gi 0/02,Gi 0/03,Gi 0/04

A total of 1 Per page show 10 First Prev Next Last 1

Figure 6-2-3

View VLAN configuration on switch.

6.3 MAC Config

6.3.1 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 addresses 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.

6.3.2 Static MAC Address

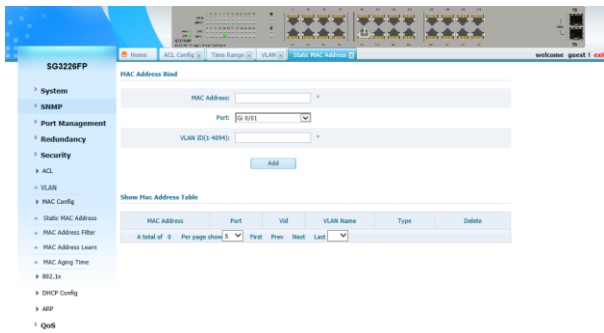


Figure 6-3-1

MAC Address: Input MAC address you want to bind.
Port: Choose the port you want the MAC address bind to.
VLAN ID (1-4094): Input the VLAN ID you want the MAC address bind to.

6.3.3 MAC Address Filter

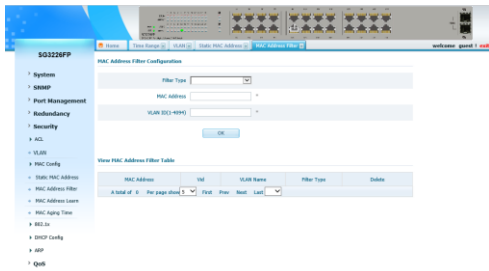


Figure 6-3-2

MAC Address: Input MAC address you want to deny.
VLAN ID (1-4094): Input the VLAN ID you want the MAC address denied in.

6.3.4 MAC Address Learn

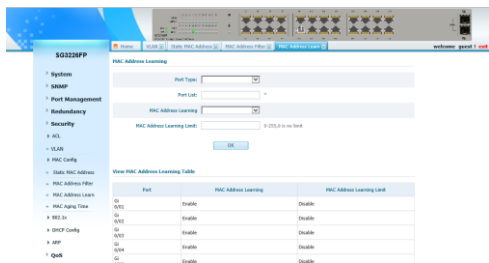


Figure 6-3-3

Port Type & List: Choose the port you want to set.

MAC Address learning limit: Input the number of MAC learning you want to limit on the port.

6.3.5 MAC Aging Time



Figure 6-3-4

Input aging time and press OK.

6.4 IEEE802.1x

6.4.1 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

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 (authorized or unauthorized) of the controlled port according to the instructions (accept or reject) received from the RADIUS server.

6.4.2 IEEE802.1x Config

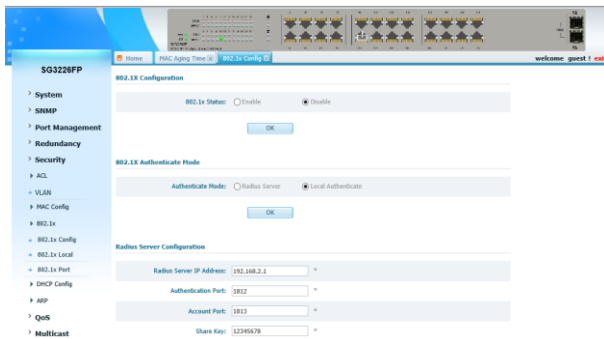


Figure 6-4-1

802.1X Mode: Whether enable 802.1X function.

Authenticate Mode: There two types of authenticate mode, radius server or local.

Radius Server IP Address: IP address of radius server.

Authentication Port: Port used for authentication, 1812 by default.

Account Port: Port used for account, 1813 by default.

Share Key: The share key is used for radius sever, 12345678 by default.

802.1X Authorized Work Mode

Authorized Work Mode: port mac

OK

Other Configuration

Re-Authentication: Enable Disable

Dot1x MaxReq: 8 (1-10)

Dot1x reAuthMax: * (1-10)

Supplicant Timeout: * (1-255)

Re-Authentication Period: * (10-65535)

Quiet Period: * (0-65535)

Server Timeout: * (1-255)

Tx Period: * (0-65535)

OK

Figure 6-4-2

Authorized Work Mode: Set authorized work is based on port or MAC.

Re-Authentication: Whether enable re-authentication.

Dot1x MaxReq: Times of 802.1x max request.

Dot1x reAuthMax: Times of max re-auth.

Supplicant Timeout: Set time of supplicant timeout, 60 by default.

Re-Authentication Period: Set time of re-authentication period, 300 by default.

Quiet Period: Set time of quiet period, 60 by default.

Server Timeout: Set time of server timeout, 45 by default.

Tx Period: Set time of tx period, 30 by default.

6.4.3 802.1x Local

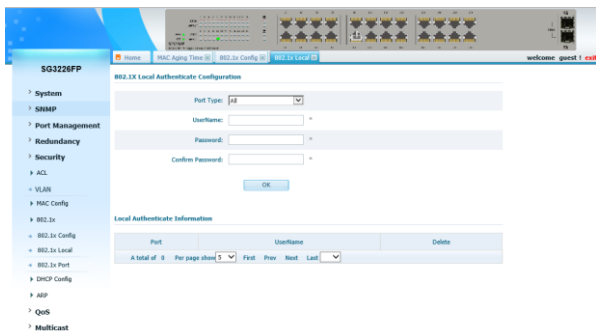


Figure 6-4-3

Port Type & List: Choose the port you want to set.

UserName: Input username for local authenticate.

Password: Input password.

Confirm Password: Confirm the password.

6.4.4 802.1x Port

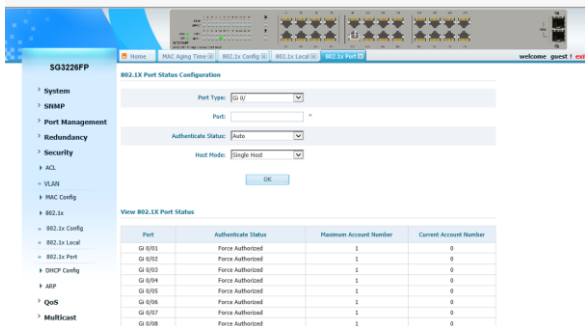


Figure 6-4-4

Port Type & List: Choose the port you want to set.

Authenticate Status: There are 3 modes, Auto, Force Authorized and Force Unauthorized. The default is automatic.

Host Mode: Choose one host or more than one host on the port.

6.5 DHCP

6.5.1 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.

6.5.2 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

6.5.3 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 obtain 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, which 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.

6.5.4 DHCP Configuration



Figure 6-5-1

DHCP Relay: Whether enable DHCP relay.

DHCP Snooping: Whether enable DHCP snooping.

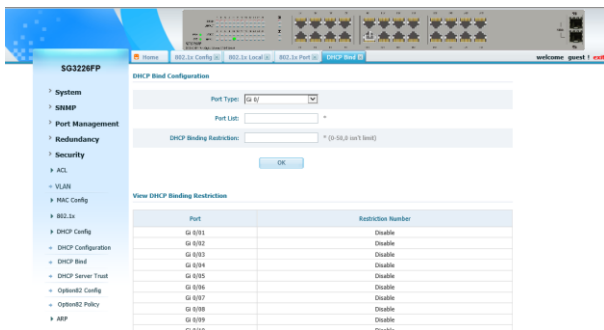
Rewrite DHCP lease Time: Whether need rewrite DHCP lease.

Lease Time: Input the new lease time.

Option 82: Whether enable option 82 of DHCP.

Global Remote ID: Input the remote ID of option 82.

6.5.5 DHCP Bind



The screenshot shows the DHCP Bind Configuration page. The configuration form includes:

- Port Type: G 0/1
- Port List: *
- DHCP Binding Restriction: * (0-50,0 isn't limit)

An OK button is located below the form. Below the form is a table titled "View DHCP Binding Restriction":

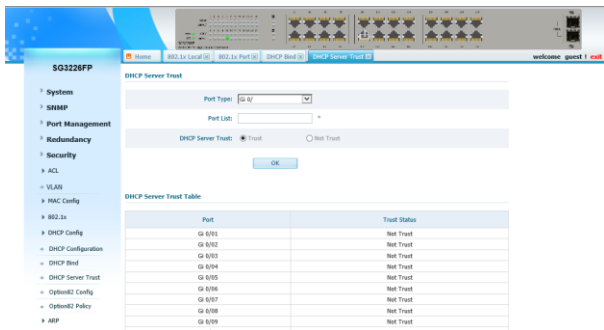
Port	Restriction Number
G 0/11	Disable
G 0/12	Disable
G 0/13	Disable
G 0/14	Disable
G 0/15	Disable
G 0/16	Disable
G 0/17	Disable
G 0/18	Disable
G 0/19	Disable
G 0/19A	Disable

Figure 6-5-2

Port Type & List: Choose the port you want to set.

DHCP Binding Restriction: Input the number of DHCP address you want to restrict on the port.

6.5.6 DHCP Server Trust



The screenshot shows the DHCP Server Trust configuration page. The configuration form includes:

- Port Type: G 0/1
- Port List: *
- DHCP Server Trust: Trust Not Trust

An OK button is located below the form. Below the form is a table titled "DHCP Server Trust Table":

Port	Trust Status
G 0/11	Not Trust
G 0/12	Not Trust
G 0/13	Not Trust
G 0/14	Not Trust
G 0/15	Not Trust
G 0/16	Not Trust
G 0/17	Not Trust
G 0/18	Not Trust
G 0/19	Not Trust
G 0/19A	Not Trust

Figure 6-5-3

Port Type & List: Choose the port which is connected to the DHCP

Server.

DHCP Server Trust: If the port connect to DHCP server, click Trust, otherwise click Not trust.

6.5.7 Option82 Config



Figure 6-5-4

Port Type & List: Choose the port you want to set.

(Circuit ID)Port Index: Input the index values in circuit ID, usually it's port number -1.

(Circuit ID)VLAN ID: Input VLAN ID of port in circuit.

(Remote ID)MAC: Input MAC in remote ID.

6.5.8 Option82 Policy

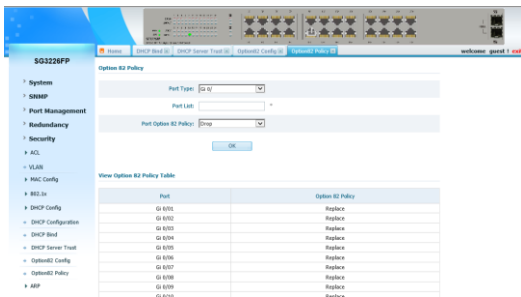


Figure 6-5-5

Port Type & List: Choose the port you want to set.

Port Option 82 Policy: There 3 modes of op 82 policy, Drop, Replace and Keep.

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.

It 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

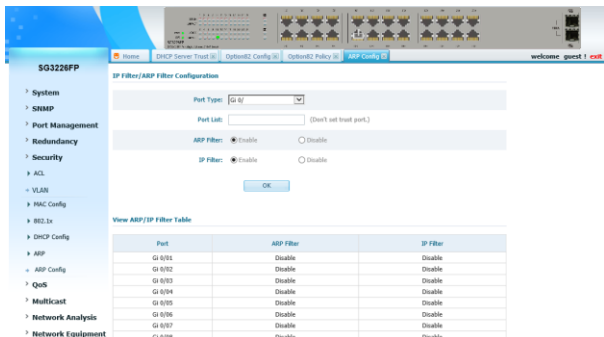
function, which will shut down the attacked port, thus preventing serious impact on the CPU.

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.

6.6 ARP

6.6.1 ARP Config



The screenshot shows the configuration page for ARP Filter on a switch. The interface includes a navigation menu on the left, a main configuration area, and a table at the bottom.

IP Filter/ARP Filter Configuration

Port Type:

Port List: (Don't set trust port.)

ARP Filter: Enable Disable

IP Filter: Enable Disable

View ARP/IP Filter Table

Port	ARP Filter	IP Filter
Gi 0/0/1	Disable	Disable
Gi 0/0/2	Disable	Disable
Gi 0/0/3	Disable	Disable
Gi 0/0/4	Disable	Disable
Gi 0/0/5	Disable	Disable
Gi 0/0/6	Disable	Disable
Gi 0/0/7	Disable	Disable
Gi 0/0/8	Disable	Disable

Figure 6-6-1

Port type & List: Choose the port you want to set.

ARP Filter: Whether enable ARP filter on the port.

IP Filter: Whether enable IP filter on the port.

ARP Binding

IP Address:

MAC Address:

VLAN ID: * (1-4094)

Port type:

Port List: (Don't set trust port.)

DHCP Security Check

Port type:

Port List: (Don't set trust port.)

Security Check Mode:

Figure 6-6-2

ARP Binding

IP Address: The IP address you want to bind.

MAC Address: The MAC address you want to bind.

VLAN ID: The VLAN ID you want the IP and MAC bind into.

Port type & List: Choose the port you want the IP and MAC bind on.

DHCP Security Check:

Port type & List: Choose the port you want to set.

Security Check Mode: There are 4 security check mode, DAI, IP source guard, DAI+IP source guard and none. If choose DAI, that only check ARP packets, and IP source guard only check IP packets, DAI+IP source guard will check both ARP and IP packets, and none will not check any packets, none by default.

View DHCP Security Check Table

Port	Status
Fa 0/01	FAIL
Fa 0/02	FAIL
Fa 0/03	FAIL
Fa 0/04	FAIL
Fa 0/05	FAIL
Fa 0/06	FAIL
Fa 0/07	FAIL
Fa 0/08	FAIL
Fa 0/09	FAIL
Fa 0/10	FAIL

A total of 20 Per page show First Prev Next Last

View DHCP Bind Table

IP Address	MAC Address	VLAN	Port	Type	Delete
------------	-------------	------	------	------	--------

A total of 0 Per page show First Prev Next Last

Figure 6-6-3

View DHCP security check configuration and DHCP static bind on the switch.

Chapter 7: QoS

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 equipment's 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 code point (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.

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 or to trust port priority. 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.

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.

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 w_3 , w_2 , w_1 , and w_0 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 w_3 , w_2 , w_1 , and w_0 in order). In this way, the queue with the lowest

priority can get 10 Mbps bandwidth ($100\text{-Mbps} \times 1 / (5 + 3 + 1 + 1)$) 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.

7.1 QoS Information



Figure 7-1-1

Trust mode: There are 4 trust modes, port-based, 1p, dscp and 1p+dscp.

Rewrite CoS: If you want to rewrite 1p-priority with packets, you must enable rewrite cos first.

Rewrite DSCP: If you want to rewrite DSCP with packets, you must enable rewrite DSCP first.

7.2 DSCP Queue Mapping

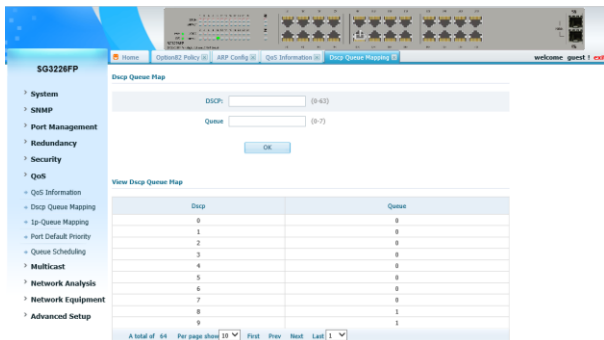


Figure 7-2-1

Internal priority: The initializing dscp values with packets.

Queue: The queue you want the dscp of packets map to.

View dscp queue map: View dscp values to queue mapped table.

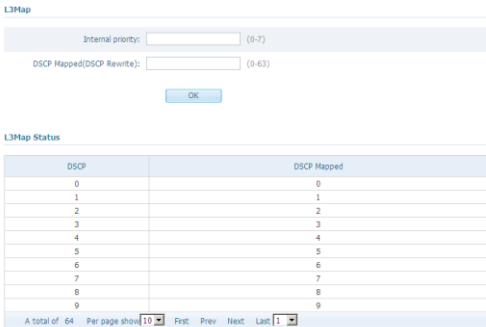


Figure 7-2-2

Internal priority: The initializing dscp values with packets.
DSCP Mapped (DSCP Rewrite): The new dscp values you want to rewrite.
L3Map Status: View DSCP rewrite mapped table.

7.3 802.1p-Queue Mapping

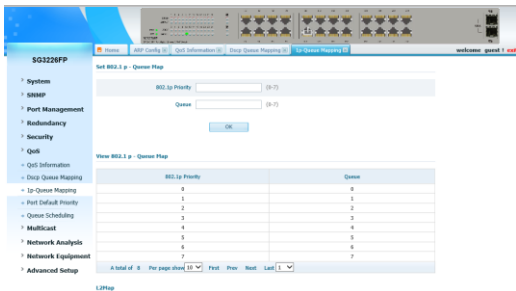


Figure 7-3-1

CosMapped (Cos Rewrite): The initializing 1p priority values with packets.

Queue: The queue you want the 1p of packets map to.

View 802.1p-queue map: View 1p to queue map table.

L2Map

802.1p:

CosMapped(Cos Rewrite):

OK

L2Map Status

802.1p	Cos Mapped(Cos Rewrite)
0	0
1	1
2	2
3	3
4	4
5	5
6	6
7	7

A total of 8 Per page show 10 First Prev Next Last 1

Figure 7-3-2

802.1p: The initializing 1p priority values with packets.

CosMapped (Cos Rewrite): The new 1p values you want to rewrite.

L2Map Status: View 1p rewrite mapped table.

7.4 Port Default Priority

SQ3226FP

Home QoS Information Deep Queue Mapping 1p Queue Mapping Port Default Priority welcome guest 1 exit

Set port the default priority

Port Type:

Port:

Priority:

OK

default priority view port

Port	Priority
Gi 0/1/1	0
Gi 0/1/2	0
Gi 0/1/3	0
Gi 0/1/4	0
Gi 0/1/5	0
Gi 0/1/6	0
Gi 0/1/7	0
Gi 0/1/8	0
Gi 0/1/9	0
Gi 0/1/10	0

Figure 7-4-1

Port Type & List: The port you want to set.

Priority: Priority values you want the packets through the port to be.

Default priority view port: View port to priority map table.

7.5 Queue Scheduling

Queue Scheduling

Queue: (0-7)

Type:

Weight: (1-8)

Check the Queue Table

Queue	Type	Weight
7	strict	strict
6	strict	strict
5	strict	strict
4	strict	strict
3	strict	strict
2	strict	strict
1	strict	strict
0	strict	strict

A total of 8 Per page show 10 First Prev Next Last 1

Figure 7-5-1

Strategy: choose mode of queue scheduling, there are 3 mode: WRR, Strict and SP+WRR.

Check the queue table: View scheduling of all the 8 queues, and weight of every queue.

Chapter 8: Multicast

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. 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.

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.

8.1 IGMP Snooping

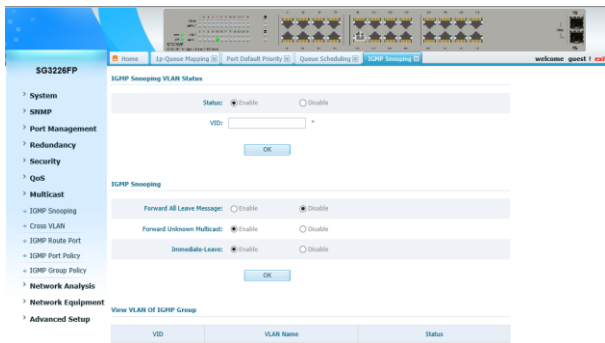


Figure 8-1-1

IGMP Snooping:

IGMP Snooping Status: set state of IGMP Snooping, enable or disable.

Forward All Leave Message: Whether forward all leave messages.

Forward Unknown Multicast: Whether forward unknown multicast packets.

Immediate-leave: Whether run immediate-leave.

View Multicast:

View Multicast Groups information here.

8.2 Cross VLAN

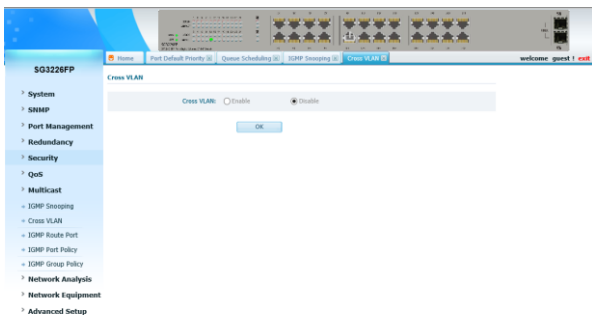


Figure 8-2-1

Cross VLAN: enable or disable.

VID: input vid, by which VLAN you want to implement cross-VLAN.

8.3 IGMP Route Port



Figure 8-3-1

Multicast Routing Port:

Port Type & List: Choose a port which you want to set it be routing port.

VLAN Type: This routing port belongs to normal VLAN or cross-VLAN. If choose cross-VLAN, you must choose egress rule is tagged or untagged.

VID: Input VLAN ID if it belongs to normal VLAN.

Aging Time Configuration:

Group member Aging Time: Input time in range 100-65535.

Dynamic route Aging Time: Input time in range 100-65535.

View Multicast Routing Port Configuration:

View routing port on switch.

8.4 IGMP Port Policy

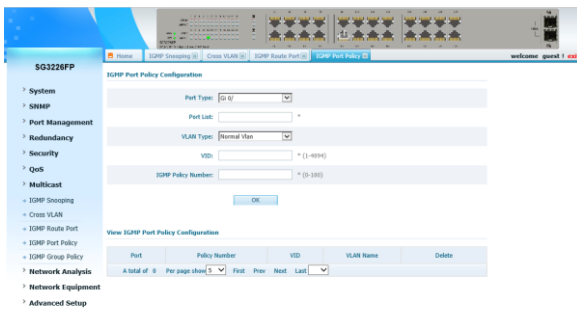


Figure 8-4-1

IGMP Port Policy Configuration:

Port Type & List: Input which port you want to set.

VLAN Type: This port belongs to normal VLAN or cross-VLAN.

VID: Which VLAN ID this port belongs to.

IGMP Policy Number: Input how many multicast groups you want to limit on this port.

View IGMP Port Policy Configuration:

View configuration of policy on ports.

8.5 IGMP Group Policy

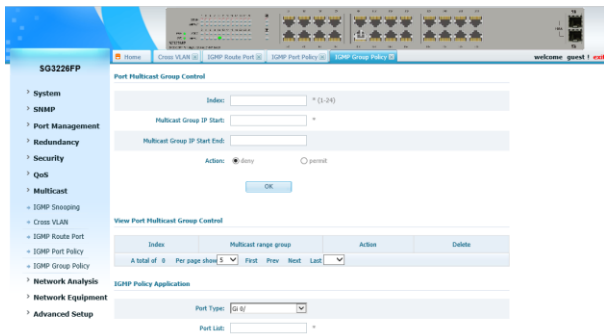


Figure 8-5-1

Port Multicast Group Control:

Index: Create a policy; first input any index in range 1-24

Multicast Group IP: Then input a multicast group IP which you want to deny.

View Port Multicast Group Control:

View how many and what policies set on switch.

IGMP Policy Application:

Port Type & List: Which port you want to set.

VLAN Type: This port belongs to normal or cross VLAN.

VID: If normal, please input the VLAN ID.

Index: Input index you created, which deny policy you want to set on this port.

View IGMP Application Policy:

View configuration of which port denied to join into which group

Chapter 9: Network Analysis

9.1 Traffic Counter

This part you can see the counter of packets.

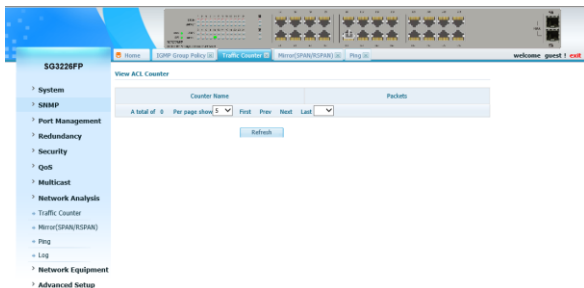


Figure 9-1-1

9.2 Port Mirror

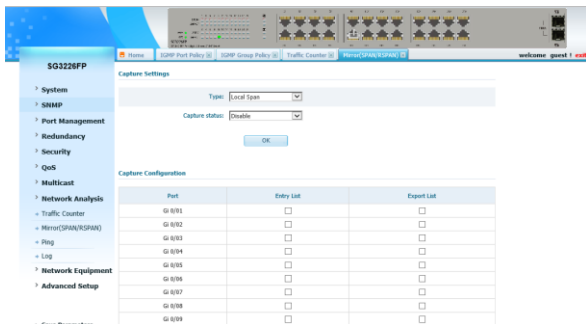


Figure 9-2-1

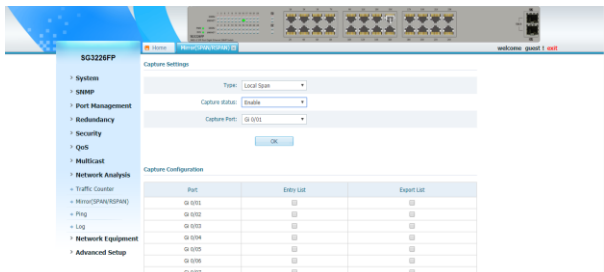


Figure 9-2-2

Capture Settings:

The part is the mirror port settings.

Type: Choose capture type, there are 3 mode: Local Span, Source RSpan and Destination RSpan.

Capture status: Set state of mirror function.

Capture port: Choose capture port, which port you want to capture mirror packets.

Capture Configuration:

The part is set by the mirror port. Check the port and direction you want to mirror.

Entry List: Mirror the data packets entered from this port.

Export List: Mirroring the data packets out of port.

9.3 Ping



Figure 9-3-1

Input IP address you want to ping, press OK then view the result below.

9.4 Log



Figure 9-4-1

You can set the log server and log degree.

Chapter10: Network Equipment

10.1 Loopback Detection

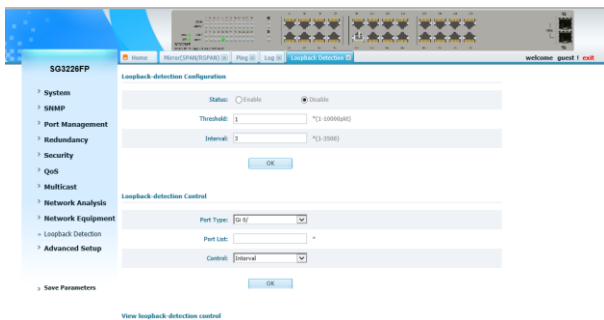


Figure 10-1-1

Loopback-detection Configuration:

State: Whether enable loopback-detection function on switch.

Threshold: Set the threshold of packets.

Interval: Set time interval to send packets.

Loopback-detection Control:

Port Type & List: Choose the port you want to set.

Control: Mode of port control. If there is loop occurs, how to deal with port state.

There are 3 modes: Interval means wait for an interval then the port still turn to forwarding state, but ports cannot turn to forwarding state in always and close mode.

View loopback-detection control:

View the port configuration of loopback-detection.

Chapter11: Advanced Setup

11.1 GVRP

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.

11.1.1 GVRP Config

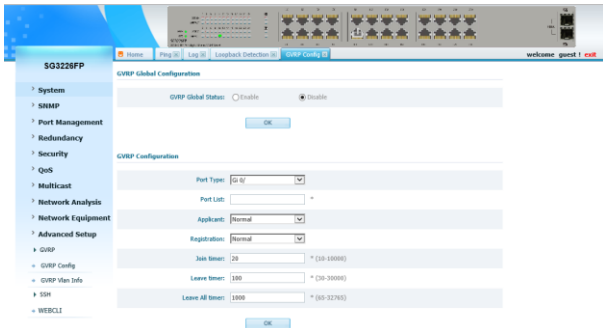


Figure 11-1-1

GVRP Global Setting: Enable or disable GVRP function on switch.

Port Type & List: Choose the port you want to set.

Applicant: Set applicant state, there 2 modes: Normal and non-applicant.

Registration: Set registration state, there 3 modes: Normal, Fixed and Forbidden.

Join timer: Input time number between 10-10000

Leave timer: Input time number between 30-30000

Leave all timer: Input time number between 65-32865

GVRP Status: View GVRP status on switch

11.1.2 GVRP VLAN Info

The screenshot displays the GVRP VLAN Group Information page on a switch. The page title is "GVRP VLAN Group Information". The table below shows the configuration for VLAN 1.

Field	VLAN Name	Static Ports	Dynamic Ports
1	default-vlan	Gi 0/12 Gi 0/13 Gi 0/14 Gi 0/15 Gi 0/16 Gi 0/17 Gi 0/18 Gi 0/19 Gi 0/20 Gi 0/21 Gi 0/22 Gi 0/23 Gi 0/24 Gi 0/25 Gi 0/26	

A total of 1 Per page show 10 First Prev Next Last 1

Figure 11-1-2

View VLAN group information on switch.

11.2 SSH

11.2.1 SSH Configuration



Figure 11-2-1

SSH Server Status: Whether enable SSH server. If enable, configure some parameters below.

MAX Session: Configure max SSH session.

Max Auth Fall Time: Configure max auth fall time.

Login Grace Time: Configure login grace time.

11.2.2 SSH User Auth Mode

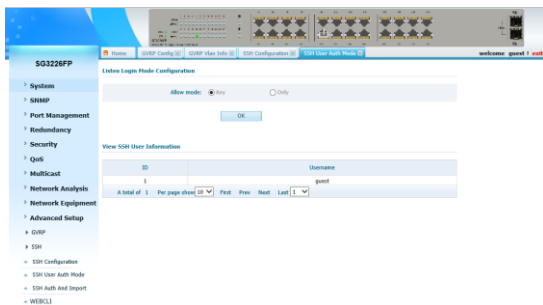


Figure 11-2-2

Listen Login Mode Configuration:

Allow mode: Choose allow mode, any or only.

View SSH User Information:

This is the system login user name.

The screenshot shows the web interface for SG3228FP. The left sidebar contains a navigation menu with categories like System, SNMP, Port Management, Redundancy, Security, QoS, Multicast, Network Analysis, Network Equipment, and Advanced Setup. The main content area is titled "Listen Login Mode Configuration" and includes a section for "Allow mode" with radio buttons for "Any" (selected) and "Only". Below this is an "OK" button. The "View SSH User Information" section contains a table with columns "ID" and "Username".

ID	Username
1	guest
2	admin

Below the table, it shows "A total of 2" and "Per page show 10" with navigation buttons for "First", "Prev", "Next", and "Last 1".

Figure 11-2-3

If you set the admin user name in the [System] - [View User Information] directory, it will also be displayed here. Then you can set any or only as needed. If you select only, you can enter guest or admin.

This screenshot shows the "View User Information" sub-page. The "Allow mode" section now has radio buttons for "Any" and "Only" (selected). Below it is a "Username:" label followed by a text input field containing "admin" and an "OK" button. The "View SSH User Information" section contains the same table as in Figure 11-2-3.

ID	Username
1	guest
2	admin

Figure 11-2-4

11.2.3 SSH Auth and Import



Figure 11-2-3

SSH Authentication Mode Settings: Authentication mode: password, public key, or both.

Username: Input username.

User Host IP: Input user host IP address.

Public Key Algorithm: Set algorithm of public key, RSA or DSA.

Key File: Choose a key file.

11.3 Web Cli

Selective QinQ Overview

In this way, you can configure the switch as console without console cable.



Figure 11-3-1

Chapter 12: Save Parameters

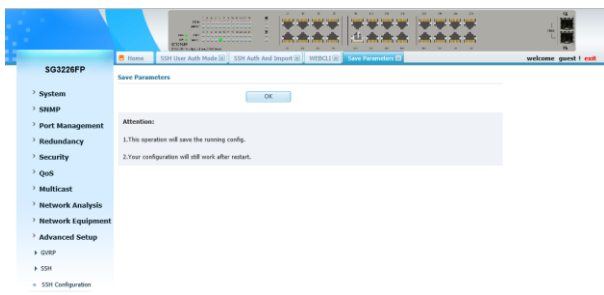


Figure 12-1-1

Press “OK”, this can make parameters saved, your configuration will still work after restart.

Chapter 13: FAQ

13.1 Link status indicator don't shows normal (Link-Error)

View the link end is connected to a PC card or other Ethernet interface;

Check that, the joint at ends of the cable is rust or damaged;

Use WEB to check this port's communication configuration (duplex, speed), to make sure configuration the same as another end of link's.

Caution: If both ends' duplex and speed are forced to be set, one link's configuration have to match with another's, otherwise it is unable to establish a connection.

13.2 Link status indicator show normal but can't communication

When this happens, please do as follows:

Use WEB form (Show in "Port state search") to check whether the port is stopped or not, if the port was stopped, use a WEB form (Show in "Port configuration") to open the port;
Use WEB form to check whether the port is in the isolated VLAN or not, compared with other ports; Ports' communication can only be accessed, when they are in the same VLAN.

13.3 Can't login to manage switch

Please do as follows to check the switch:

Check whether the switch is power on or not;

Check for link failures; Use "PING" to check switch's response; if no response, check whether the IP address configuration of switch and PC is correct or not; If that, you can determine the cause of the problem, according to the feedback information of HTTP connection.

Check the IP address setting

Please do as follows to check the switch:

- Check whether the PCs IP address, subnet mask and default gateway is your expectation setting or not: Please input "ipconfig" in Windows command to check the PC's IP address configurations.
- Check whether the switch IP address, subnet mask and default gateway is your expectation Setting or not;
- Check whether the switch IP address is occupied by another equipment or not.

Check the login account

When login via WEB form, if switch continuously request user to enter account and password, this maybe remind that the account don't exist or password invalid.

13.4 Switch start-up failure

If switch can't successfully start through CONSOLE connection, please do as follows:

- Check whether the serial port number is correct or not: usually COM1 and COM2;
- Make sure the software configuration as follows: 115200bPS, 8 data bits, 1 stop bits, and no odd and parity checking, no flow control;
- Check the Serial Port status in the device management of Windows, and connect the switch using the HyperTerminal of The Windows tools detecting the failure of the connection.
- Make sure no other program is in the use of the serial port: Any

serial port can't be used by program more than one at the same time in Windows operating systems.

13.5 Power failure

Check the power indicator light, if indicator light goes out, the power supply connection may be bad, please make sure the power supply is normal, and check whether the connection between switch and the power is stable and reliable or not.

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

