

# **Web-Managed Series Managed PoE Switch**

## **User Manual**

# Content

---

<b>Chapter 1 Switch Login</b>	P1
<b>Chapter 2 System Management</b>	P1
2.1 System Information	P1
2.2 IP Setting	P2
2.3 Account Setting	P2
2.4 Port Management	P3
<b>Chapter 3 System Configuration</b>	P3
3.1 IGMP Snooping	P3
3.2 Aggregation Management	P4
3.3 Loopback Protection	P5
3.4 Port Mirroring	P5
3.5 Port Rate Limiting	P6
3.6 Jumbo frame setting	P6
3.7 EEE Setting	P7
3.8 PoE Setting	P7
3.9 Simple Network Management	P8
3.10 Spanning Tree	P8
3.11 Cloud Network Connection	P9
3.12 LLDP Configuration	P9
3.13 LLDP Neighbors	P10
<b>Chapter 4 VLAN</b>	P11
4.1 Port VLAN	P11
4.2 Port VLAN	P11
4.3 802.1Q VLAN	P12
4.4 Voice VLAN	P12
4.5 Monitor VLAN	P13

<b>Chapter 5 QoS</b>	P14
5.1 QoS Basic Configuration	P14
5.2 QoS Advanced Configuration	P14
<b>Chapter 6 Safety</b>	P15
6.1 MAC Management	P15
6.2 Storm Suppression	P16
6.3 Data Monitoring	P16
6.4 Cable Detection	P17
6.5 DHCP Snooping	P17
<b>Chapter 7 Tools</b>	P18
7.1 System Upgrade	P18
7.2 Ping Tools	P18
7.3 Backup and Restore	P19
7.4 System Recovery	P19
7.5 Save Configuration	P20
7.6 System Restart	P20

# Chapter 1 Switch Login

The default IP of the switch is 192.168.2.1, just connect your computer to the network port of the switch and set the same network segment, enter the management IP in the address bar of the browser to access the login page, enter the default account “admin” and password “admin” to enter the management page.



Cloud network switch

English ▾

Username:

Password:

Login Clear

# Chapter 2 System Management

## 2.1 System Information

System information is used to view the device's MAC address, serial number, IPV4 address, IPV6 link-local address, IPV6 global uni-cast address, sub-net mask, default gateway, DNS server, software version, hardware version, and additionally, the system name can be set.

**System Information**

System name	<input type="text" value="G2422GB-C"/>
MAC address	90:e2:fc:01:01:04
Serial number	22F010001129C40
IPv4 address	192.168.6.4
Link-local IPv6 address	FE80::92E2:FCFF:FE01:104/64 (Auto)
Global IPv6 address(es)	None
Subnet mask	255.255.255.0
Default gateway	192.168.6.254
DNS server	----
Software version	v23.11
Hardware version	EN8851

Apply

**Attention:**  
The system name length cannot exceed 32 characters.

## 2.2 IP Setting

### IP settings

DHCP settings	Disable ▾
IP address	192.168.6.4
Subnet mask	255.255.255.0
Default gateway	192.168.6.254
Auto DNS	Disable ▾
DNS server	

Apply

### IP settings

DHCP settings	Enable ▾
IP address	192.168.6.4
Subnet mask	255.255.255.0
Default gateway	192.168.6.254
Auto DNS	Enable ▾
DNS server	

Apply

- ① Configuration: System Management → IP Setting;
- ② Instructions: IP settings support static IP and DHCP auto-acquisition, when you choose static IP, you need to manually enter the IP address, sub-net mask and default gateway, after enabling DHCP auto-acquisition, the device will automatically take the address from the DHCP server, and after you get the address, the web page will automatically jump to the management page of the acquired address; in addition, the settings of the DNS also support manually enter and auto-acquisition.

## 2.3 Account Setting

### User settings

Username	admin
Old password	
New password	
Confirm password	

Apply

#### Attention:

The length of the username and new password cannot be more than 16 characters, and only numbers, English letters and underscores can be used.

- ① Configuration: System Management → Account Setting;
- ② Instructions: Account Settings enables you to change passwords and usernames for administrative users.

## 2.4 Port Management

**Port configuration**

Port	State	Automatic	Rate	Flow Control
Port 1	Enable	On	10M Half	On
Port 2			10M Full	
Port 3			100M Half	
Port 4			100M Full	
Port 5				

Port	State		Rate		Duplex		Flow Control	
	Configuration	Actual	Configuration	Actual	Configuration	Actual	Configuration	Actual
Port 1	Enable	Disable	Automatic	N/A	Automatic	N/A	On	N/A
Port 2	Enable	Disable	Automatic	N/A	Automatic	N/A	On	N/A
Port 3	Enable	Disable	Automatic	N/A	Automatic	N/A	On	N/A
Port 4	Enable	Disable	Automatic	N/A	Automatic	N/A	On	N/A
Port 5	Enable	Disable	Automatic	N/A	Automatic	N/A	On	N/A
Port 6	Enable	Disable	Automatic	N/A	Automatic	N/A	On	N/A

- ① Configuration: system management → port management
- ② Description: Port management is used to disable and enable ports, set the negotiation rate to forced or self-negotiation, and also manage the flow control of ports. Selecting multiple ports can be done one by one by “ctrl”, or by clicking on a port and then holding down the left mouse button and dragging it down, similarly for rate selection.

## Chapter 3 System Configuration

### 3.1 IGMP Snooping

**IGMP Snooping**

IGMP Snooping:  Enable  Disable

IGMP Fast-leave:  Enable  Disable

IGMP Report Suppression:  Enable  Disable

---

VLAN ID:

IGMP Querier Status:  Enable  Disable

IGMP Querier Election:  Enable  Disable

IGMP Querier Version: V2

IGMP Querier Source Address:  (If empty, the default IP address will be used!)

### IGMP Snooping Group Entry

MAC address	VLAN ID	Port
-------------	---------	------

### IGMP Snooping Querier Status

VLAN ID	State	Querier Election Mode	Version	Source Address
1	Querier	Enable	V2	192.168.0.200

### Router Port

Port	Static	Dynamic
Port 1	<input type="checkbox"/>	<input type="checkbox"/>
Port 2	<input type="checkbox"/>	<input type="checkbox"/>
Port 3	<input type="checkbox"/>	<input type="checkbox"/>
Port 4	<input type="checkbox"/>	<input type="checkbox"/>
Port 5	<input type="checkbox"/>	<input type="checkbox"/>
Port 6	<input type="checkbox"/>	<input type="checkbox"/>
Port 7	<input type="checkbox"/>	<input type="checkbox"/>
Port 8	<input type="checkbox"/>	<input type="checkbox"/>

① Configuration: System Management→IGMP Snooping

② Description: IGMP Snooping is used to enable IGMP Snooping, IGMP Fast Leave, IGMP Report Suppression, IGMP Querier Status, IGMP Querier Election, etc., to set the IGMP Querier global address, and to set the routing port.

## 3.2 Aggregation Management

### Trunk configuration

Trunk Group	Forward Port
Trunk 1 ▼	Port 1 ▲ Port 2 Port 3 Port 4 ▼

Apply

Trunk Group	Forward Port	Selection
Trunk 1	----	<input type="checkbox"/>
Trunk 2	----	<input type="checkbox"/>
Trunk 3	----	<input type="checkbox"/>
Trunk 4	----	<input type="checkbox"/>

Select All

Delete

#### Attention:

- 1, 4 is the most trunk group can we created.
2. Each aggregation group has at most 8 member ports.

- ① Configuration: system management→aggregation management
- ② Description: Aggregation management is used to configure the aggregation port, the only mode currently supported is manual mode, up to four groups of aggregation ports can be created, and each group of aggregation ports can only have a maximum of eight member ports.

### 3.3 Loopback Protection

**Loop prevention settings**

Loop prevention state:  ▼

---

Port	State
Port1	normal
Port2	normal
Port3	normal
Port4	normal
Port5	normal
Port6	normal
Port7	normal
Port8	normal
Port9	normal
Port10	normal
Port11	normal
Port12	normal

- ① Configuration: system management→loopback protection
- ② Description: After enabling the loopback protection function, if the port detects link congestion, it will automatically switch to the blocking state and will not forward messages, thus not forming a loop in the network.

### 3.4 Port Mirroring

**Port Mirror**

Session	Port mirroring is enabled	Mirror Port
1	<input type="button" value="Enable"/> ▼	<input type="button" value="Port 1"/> ▼
2	<input type="button" value="Disable"/> ▼	▼
3	<input type="button" value="Disable"/> ▼	▼
4	<input type="button" value="Disable"/> ▼	▼

Session	Mirrored port	Ingress	Egress
<input type="button" value="1"/> ▼	<input type="button" value="Port 1"/> ▲ <input type="button" value="Port 2"/> ▲ <input type="button" value="Port 3"/> ▲ <input type="button" value="Port 4"/> ▼	<input type="button" value="Disable"/> ▼	<input type="button" value="Disable"/> ▼

---

Mirrored port	Ingress	Egress
Port1	Disable	Disable
Port2	1	1
Port3	Disable	Disable
Port4	Disable	Disable

① Configuration: system management→port mirroring

② Description: Port mirroring is to forward the data traffic of one or more source ports to a specified port to monitor the network. Without seriously affecting the normal throughput traffic of the source port, you can monitor and analyze the traffic of the network through the mirrored port, you can monitor and manage the network data well, and you can locate the faults quickly when there is a failure in the network. At present, we support port mirroring with single port and aggregation port as the source port, which can mirror the data traffic of receiving, sending and transmitting in three ways.

### 3.5 Port Rate Limiting

**Port Speed Limit**

Port	Ingress Speed	Egress Speed
Port 1 Port 2 Port 3 Port 4 Port 5	<input type="text"/> *32Kbps	<input type="text"/> *32Kbps

Apply

Port	Ingress Speed	Egress Speed
Port 1	32 Kbps	32 Kbps
Port 2	Disable	Disable
Port 3	Disable	Disable
Port 4	Disable	Disable
Port 5	Disable	Disable
Port 6	Disable	Disable

① Configuration: system management→port rate limiting

② Description: The Port Speed Limit page is used to configure the speed at which traffic passes through the port, and you can limit the speed of traffic in Port inlet and outlet according to needs.

### 3.6 Jumbo frame setting

**Jumbo Frame Configuration**

Jumbo Frame Enable:  Enable  Disable

MTU size:

Apply

① Configuration: system management→jumbo frame setting

② Description: Jumbo frame setting page is used to set the size of MTU, MTU refers to the maximum transmission unit value, by setting the MTU to regulate the size of the packets on

the network, so that different networks can find the most suitable MTU so as to improve the forwarding efficiency; at present, we support the setting of the MTU value of 2K, 3K, 4K, 5K, 6K, 7K, 8K, 9K, 12K, 15K.

### 3.7 EEE Setting

**EEE configuration**

EEE state:

Port	EEE state	Selected
1	Enable	<input checked="" type="checkbox"/>
2	Disable	<input type="checkbox"/>
3	Disable	<input type="checkbox"/>
4	Disable	<input type="checkbox"/>
5	Disable	<input type="checkbox"/>
6	Disable	<input type="checkbox"/>

- ① Configuration: system management → EEE setting
- ② Description: EEE is Energy Efficient Ethernet, a set of enhancements to the backplanes of the Ethernet family of twisted pair and computer networking standards that enable them to consume less power during periods of low data activity. The goal is to reduce power consumption by more than 50% while maintaining full compatibility with existing equipment.

### 3.8 PoE Setting

**POE configuration**

POE state:

<input type="checkbox"/>	Port	POE state	Classification(s3:af,=4:at)
<input type="checkbox"/>	1	Enable	Port open or no classification
<input type="checkbox"/>	2	Enable	Port open or no classification
<input type="checkbox"/>	3	Enable	Port open or no classification
<input type="checkbox"/>	4	Enable	Port open or no classification
<input type="checkbox"/>	5	Enable	Port open or no classification
<input type="checkbox"/>	6	Enable	Port open or no classification
<input type="checkbox"/>	7	Enable	Port open or no classification
<input type="checkbox"/>	8	Enable	Port open or no classification
<input type="checkbox"/>	9	Enable	Port open or no classification
<input type="checkbox"/>	10	Enable	Port open or no classification

- ① Configuration: system management→POE setting
- ② Description: The POE Settings page is used to enable and disable the power supply function of the port, while the page can view the POE status of the port and the grading of the port.

## 3.9 Simple Network Management

**Version**

SNMP v1  Enable  Disable

SNMP v2c  Enable  Disable

---

**Communities**

read community

write community

trap community

---

**Trap**

SNMP v1 trap  Enable  Disable

SNMP v2c trap  Enable  Disable

Trap Server  By name  By IP

Trap type  Cold/Warm start  Link up/down  Authentication Failure

- ① Configuration: System Configuration → Simple Network Management
- ② Description: SNMP is a simple network management protocol, which is a standard network management protocol widely used in TCP/IP networks. It provides a way to manage devices through a central computer running network management software, and realizes efficient and batch management of network devices by “using the network to manage the network”; at the same time, SNMP also shields the differences between different products and realizes unified management among different types and manufacturers of network devices. At the same time, the SNMP protocol also shields the differences between different products, realizing the unified management between different types and manufacturers of network devices. Currently we support SNMP v1 and v2 versions, administrators can read and write using MIB Browser, a software available to test and supervise multiple SNMP devices on the network; in addition, the page can also be set up for SNMP Traps, turn on the traps, you can view the device's hot and cold startups, ports up or down, on MIB Browser. Authentication Failure.

## 3.10 Spanning Tree

**Spanning Tree Configuration**

Spanning Tree State:  Enable  Disable

Force Version:  STP  RSTP

Forward Delay:  seconds (4-30)

Max Age:  seconds (6-40)

Transmit Hold Count:  seconds (1-10)

Priority:  (0-61440, in steps of 4096)

**Port Configuration**

Port	Priority	Cost
Port1		
Port2		
Port3		
Port4		
Port5		

Port	Priority	Cost	State	Role
Port1	128	2000	Disable	Disable
Port2	128	2000	Disable	Disable
Port3	128	2000	Disable	Disable
Port4	128	2000	Disable	Disable
Port5	128	2000	Disable	Disable
Port6	128	2000	Disable	Disable
Port7	128	2000	Disable	Disable

- ① Configuration: System Configuration → Spanning Tree
- ② Description: When a network is a ring-shaped network, it will form a broadcast storm, which will take up a large amount of network bandwidth, resulting in the normal operation of the service cannot run, or even completely paralyzed. Spanning Tree will form a tree-like structure of the ringless network topology, making the network topology physical ring, logical ringless. Currently there are three protocols for spanning tree, STP, RSTP, MSTP, we currently support STP and RSTP, RSTP is improved on the basis of STP to achieve rapid convergence of the network topology, so RSTP is called Rapid Spanning Tree Protocol.

### 3.11 Cloud Network Connection

**Cloud Configuration**

Connect to the MQTT server :  Enable  Disable

---

**Attention:**

1. If enable the cloud connection, the system will try to connect to MQTT server automatically.
2. The on-premise HTTPS connection will be disabled.
3. Please visit the website to download the mobile software [HiCloudiot](#)

- ① Configuration: System Configuration → Cloud Network Connection
- ② Description: Cloud Configuration page, after enabling the connection to the MQTT server, the device will be automatically connected to the cloud server, the user can download the APP through the link on the page, and the device can be remotely managed after adding the device.

### 3.12 LLDP Configuration

**LLDP**

LLDP Global:  Enable  Disable

Tx Interval:  sec(Range:5-32768,default 30)

Tx Hold:  sec(Range:2-10,default 4)

Reinit Delay:  sec(Range:1-10,default 2)

Tx Delay:  sec(Range:1-8192,default 2)

---

Port	Admin Control
<input type="button" value="Port 1"/> <input type="button" value="Port 2"/> <input type="button" value="Port 3"/> <input type="button" value="Port 4"/>	<input type="text" value="Tx &amp; Rx"/>

---

Port	Admin Status
Port 1	Tx & Rx
Port 2	Disable
Port 3	Disable
Port 4	Disable
Port 5	Disable

① Configuration: System Configuration → LLDP

② Description: LLDP is Link Layer Discovery, a standard Layer 2 discovery method, which can organize the management address, device identification, interface identification and other information of the local device and release it to its neighboring devices, and the neighboring devices receive this information and save it in the form of a standard management information base for the network management system to query and judge the communication status of the link.

### 3.13 LLDP Neighbors

LLDP Neighbor

Local Port	Chassis ID	Port ID	System Name	TTL	Med Capabilities	Med Device Type	Network Policy	Extended Power
port 23	90-e2-8-01-01-0e	port_9	G1622GB-C	120	medCapabilities	netConnectivity	---	---

① Configuration: System Configuration → LLDP

② Description: After LLDP function is enabled, the LLDP neighbor page will display the relevant information of the neighboring devices, including Rack ID Port ID, System Name, Survival Time, Med Capability, Med Device Type, Med Network Policy, and Extended Power based on MDI.

# Chapter 4 VLAN

## 4.1 MTU VLAN

**MTU VLAN Settings**

MTU VLAN enabled:  Enable  Disable Apply

Current Uplink Port	1
Select Uplink Port	<div style="border: 1px solid gray; padding: 2px;">Port 1 Port 2 Port 3 Port 4</div>

Apply

① Configuration: VLAN→MTU VLAN

② Description: MTU VLAN is to divide the port occupied by each user and the uplinked port into a separate VLAN. ordinary ports can only communicate with the pre-set uplinked ports, and cannot communicate with each other, so that users on different ports cannot communicate directly with each other to ensure the security of the network. This situation is very suitable for use in intelligent neighborhoods, where users cannot access each other directly, thus ensuring the network security of the residents. After using MTU VLAN, port VLAN and 802.1Q VLAN will be automatically disabled and the configuration of port VLAN and 802.1Q VLAN will be lost.

## 4.2 Port VLAN

**Port-based VLAN Settings**

Port-based VLAN enabled:  Enable  Disable Apply

VLAN	(1-4094, maximum configurable number: 28)											
Port	1	2	3	4	5	6	7	8	9	10	11	12
Member	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Port	13	14	15	16	17	18	19	20	21	22	23	24
Member	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Port	25	26	27	28								
Member	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>								

Apply Delete

VLAN	Member Port
1	3-28
2	1-2

① Configuration: VLAN→Port VLAN

② Description: The Port VLAN setting page is used to create and delete VLAN values, the maximum VLAN value is 4094, the minimum value is 1, and a maximum of 28 VLAN values can be configured. After using Port VLAN, MTU VLAN and 802.1Q VLAN will be disabled automatically and the configuration of MTU VLAN and 802.1Q VLAN will be lost.

## 4.3 802.1Q VLAN

**802.1Q VLAN Settings**

802.1Q VLAN enabled:  Enable  Disable

802.1Q VLAN <input type="text"/> (1-4094)	Description <input type="text"/>	<input type="button" value="Add/Edit"/>	<input type="button" value="Delete"/>
Port	Untagged port	Tagged port	Non-member port
Select All	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Port 1	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Port 2	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Port 3	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Port 4	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Port 5	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Port 6	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Port 7	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Port 8	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

① Configuration: VLAN→802.1Q VLAN

② Description: The 802.1Q VLAN setting page is used to add and delete 802.1Q VLANs and you can add related descriptions. The value range of 802.1Q VLANs is 1-4094, and this page also allows you to set tagged and untagged ports for the 802.1Q VLAN values. After using 802.1Q VLAN, MTU VLAN and Port VLAN will be disabled automatically and the configuration of MTU VLAN and Port VLAN will be lost.

## 4.4 Voice VLAN

### Voice VLAN Configuration

Voice VLAN enabled:  Enable  Disable

VLAN ID:

Priority:

---

Enable default OUI       Default OUI description:       OUI:

Enable custom OUI       Custom OUI description:       OUI:      

Sequence Number	OUI Description	OUI	Delete
<input type="button" value="Delete"/>			

### Port Configuration

Select	Port	Port Mode	Member State
<input type="checkbox"/>		Manual <input type="button" value="Apply"/>	
<input type="checkbox"/>	Port1	Auto	Inactive
<input type="checkbox"/>	Port2	Auto	Inactive

① Configuration: VLAN→Voice VLAN

② Description: Voice VLAN is also commonly referred to as Voice VLAN. Voice VLAN is a VLAN divided for the user's voice data flow. By creating a Voice VLAN and adding the port connecting the voice device to the Voice VLAN, the user can centralize voice data for transmission in the Voice VLAN, which facilitates targeted QoS configuration of the voice stream, improves the transmission priority of voice traffic, and ensures call quality. 802.1Q VLAN must be enabled before enabling voice VLAN.

## 4.5 Monitor VLAN

### Surveillance VLAN Configuration

Surveillance VLAN enabled:  Enable  Disable

VLAN ID:

Priority:

---

Enable default OUI       Default OUI description:       OUI:

Enable custom OUI       Custom OUI description:       OUI:      

Sequence Number	OUI Description	OUI	Delete
<input type="button" value="Delete"/>			

① Configuration: VLAN → Monitor VLAN

② Description: Monitoring VLAN can control the priority of cameras of specified brands to achieve traffic priority.

## Chapter 5 QoS

### 5.1 QoS Basic Configuration

**QoS Port Select**

Select	Port
<input type="checkbox"/>	
<input checked="" type="checkbox"/>	Port 1
<input type="checkbox"/>	Port 2
<input type="checkbox"/>	Port 3
<input type="checkbox"/>	Port 4
<input type="checkbox"/>	Port 5
<input type="checkbox"/>	Port 6
<input type="checkbox"/>	Port 7
<input type="checkbox"/>	Port 8
<input type="checkbox"/>	Port 9
<input type="checkbox"/>	Port 10
<input type="checkbox"/>	Port 11

**Global Configuration**

QoS policy  SP  WRR  WFQ

Apply

① Configuration: QoS→QoS basic configuration

② Description: The QoS basic configuration page is used to select QoS ports and perform global configuration of policy selection.

### 5.2 QoS Advanced Configuration

**Global Configuration**

QoS mode  Port-based  Based on 802.1p  Based on DSCP

Apply

**Based on Port Settings**

Choice	Port	Priority
<input type="checkbox"/>		0 ▾
<input type="checkbox"/>	Port 1	0
<input type="checkbox"/>	Port 2	0
<input type="checkbox"/>	Port 3	0
<input type="checkbox"/>	Port 4	0
<input type="checkbox"/>	Port 5	0
<input type="checkbox"/>	Port 6	0
<input type="checkbox"/>	Port 7	0
<input type="checkbox"/>	Port 8	0

- ① Configuration: QoS → QoS advanced configuration
- ② Description: The QoS advanced configuration page is used to configure the QoS mode and port priority settings.

## Chapter 6 Safety

### 6.1 MAC Management

**MAC configuration**

Port Index:  Maximum MAC number:  (0-100, 0: Disabled)

Port	Maximum MAC number
1	0
2	0
3	0
4	0
5	0
6	0
7	0
8	0
9	0

---

Port Index:  VID:  MAC address:

Index	VID	MAC	Port	Selected
<input type="button" value="Delete"/>				

**Dynamic MAC Address Table**

Index	VID	MAC	Port	Aging time(in seconds)
1	1	7c10c9bf7348	23	301
2	1	90e2ff010117	23	299
3	1	90e2ff01010e	23	185
4	1	bcbac2c2c18d	23	301
5	1	e88088319c9d	23	288
6	1	c470abd157c9	23	301
7	1	90e2fc023460	23	299

- ① Configuration: Security → MAC Management
- ② Description: The MAC management page is used to configure the maximum number of MAC addresses that the device port can learn. If the number exceeds the set number, the port will

no longer learn. The value range of the maximum MAC number is 0-100, 0 means disabled; at the same time, this The page can also configure the VID value and static MAC address corresponding to the port. When the port number, VID value and static MAC address all match at the same time, the terminal can perform data communication; in addition, this page can also view the dynamic MAC address learned by each port.

## 6.2 Storm Suppression

**Storm Suppression**

Port	Unknown Unicast Packets		Multicast Packets		Broadcast Packets	
	State	Speed Kbps	State	Speed Kbps	State	Speed Kbps
Port 1	Enable	64	Enable	64	Enable	64
Port 2						
Port 3						
Port 4						
Port 5						

Apply

---

Port	Unknown Unicast Packets		Multicast Packets		Broadcast Packets	
	State	Speed	State	Speed	State	Speed
Port 1	Enable	64Kbps	Enable	64Kbps	Enable	64Kbps
Port 2	Disable	0pps	Disable	0pps	Disable	0pps
Port 3	Disable	0pps	Disable	0pps	Disable	0pps
Port 4	Disable	0pps	Disable	0pps	Disable	0pps

- ① Configuration: Security → Storm Suppression
- ② Description: The storm suppression function can limit the unknown unicast, multicast and broadcast rates of the incoming and outgoing interfaces to prevent storms. For the unit of rate setting, we support Kbps and PPS; it should be noted that whether it is unknown unicast, multicast or broadcast, as long as it is an ARP message, the suppression function is invalid. In addition, when setting the rate, the value Needs to be a multiple of 64.

## 6.3 Data Monitoring

**Traffic Monitor**

Port	Tx bytes	Rx bytes	Tx pkts	Rx pkts
Port 1	0	0	0	0
Port 2	0	0	0	0
Port 3	0	0	0	0
Port 4	0	0	0	0
Port 5	13960	4676	29	38
Port 6	0	0	0	0
Port 7	0	0	0	0
Port 8	0	0	0	0

- ① Configuration: Security → Traffic Monitoring
- ② Description: The traffic monitoring page can monitor the number of bytes sent, bytes received, packets sent, and packets received on the port.

## 6.4 Cable Detection

**Cable Diagnostics**

Port Index:

Pair	Cable Status	Cable Length (m)
A	normal	3.2
B	normal	3.2
C	normal	3.2
D	normal	3.2

Attention:  
Only support cable diagnostic for 1G speed.

- ① Configuration: Security → Cable Detection
- ② Description: The cable detection function can detect the distance between the switch interface and the terminal and the network cable condition.

## 6.5 DHCP Snooping

**DHCP Snooping**

DHCP Snooping:  Enable  Disable

**Port Configuration**

Port	Trust	Option 82	Operation	Circuit Id Custom	Circuit Id Sub-option	Remote Id Custom	Remote Id Sub-option
Port1							
Port2							
Port3	Enable	Enable	Replace	Default		MAC Address	
Port4							
Port5							

Port	Trust	Option 82	Operation	Circuit Id Custom	Circuit Id Sub-option	Remote Id Custom	Remote Id Sub-option
Port1	Disable	Disable	Keep	Default		MAC Address	
Port2	Disable	Disable	Keep	Default		MAC Address	
Port3	Disable	Disable	Keep	Default		MAC Address	
Port4	Disable	Disable	Keep	Default		MAC Address	

- ① Configuration: Security → DHCP Snooping
- ② Description: DHCP Snooping, also commonly referred to as DHCP Snooping, is a feature

used in Layer 2 network access devices. In scenarios where DHCP Snooping is enabled, interfaces directly or indirectly connected to legitimate DHCP servers are typically set as trusted interfaces, while other interfaces are set as untrusted. This ensures that DHCP request messages from DHCP clients can only be forwarded through trusted interfaces, guaranteeing that DHCP clients obtain IP addresses only from legitimate DHCP servers and preventing rogue DHCP servers from assigning IP addresses to DHCP clients. Additionally, we support Option 82 configuration. Option 82, also known as the Relay Agent Information Option, records the location information of DHCP clients. By adding Option 82 to DHCP request messages, DHCP Snooping devices inform the DHCP server of the DHCP client's location, allowing the DHCP server to assign appropriate IP addresses and other configuration information to the hosts and enabling security, billing, and other controls for the clients.

## Chapter 7 Tools

### 7.1 System Upgrade

**System upgrade**

Ready to upgrade the software? You need to restart after the upgrade is complete.

There is no file been selected

---

**Attention:**

1. Please do not power off during the upgrade process, otherwise the machine may be damaged.
2. It is recommended to backup the current configuration before upgrading.

- ① Configuration: Tools → System Upgrade
- ② Description: The System Upgrade page is used to perform software upgrades on the device.

### 7.2 Ping Tools

**Ping Tool**

Host Name/IP Address	Number of Pings
<input type="text"/>	<input checked="" type="radio"/> Default: 4 <input type="radio"/> User Defined <input type="text" value="4"/> Range: 1 - 65535

---

**Ping Status**

Host Address:	0.0.0.0
Number of Packets sent:	0
Number of Packets Received :	0
Packet Lost:	0 %
Minimum Round Trip Time:	0 ms
Maximum Round Trip Time:	0 ms
Average Round Trip Time:	0 ms
Status:	N/A

- ① Configuration: Tools → Ping Tool
- ② Description: The Ping Tool page is used to check the reachability of the destination host.

## 7.3 Backup and Restore

### System Configuration Backup

Click the configuration backup button to save the current configuration.  
It is recommended to save the current configuration before backing up.

Configuration backup

### System Configuration Restore

Select a backup configuration file and click the restore configuration button, then  
You can restore the switch to its previous configuration.

Configuration file:

#### Attention:

- 1: It takes a few minutes to backup or restore the configuration. Please do not perform other operations during this period.
- 2: Please do not power off during the backup or restore configuration, otherwise the machine may be damaged.
- 3: After restoring the configuration, the current configuration will be lost. Incorrect configuration may cause the switch to be unmanageable.

- ① Configuration: Tools → Backup and Restore
- ② Description: The Backup and Restore page are primarily used for downloading and backing up device configurations, as well as restoring configurations. After a switch has undergone various complex configurations, to prevent the loss of configurations upon device restart or being inadvertently reset to factory settings, which could disrupt many operations, it is advisable to download and backup the data ahead of time. Subsequently, performing a restore can quickly recover the device's data and configurations.

## 7.4 System Recovery

### System Recovery

Restore to factory settings and restart the system.

Reset

#### Attention:

After the system is restored, the local configuration will be lost, and all configurations will be restored to the default configuration.

① Configuration: Tools → System Recovery

② Description: The System Recovery page is used to restore the device to its factory default settings. After system recovery, local configurations will be lost, and all settings will be reset to default configurations.

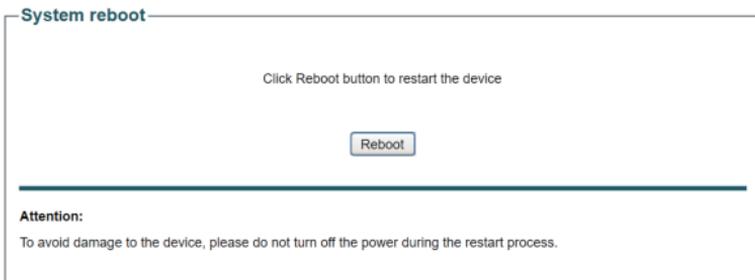
## 7.5 Save Configuration



① Configuration: Tools → Save Configuration

② Description: After the administrator has made certain configurations to the device, they need to save the configurations on this page. Otherwise, after a cold or warm restart of the device, the relevant configurations and data may be lost.

## 7.6 System Restart



① Configuration: Tools → System Restart

② Description: The System Restart page is used to restart the device's system.