

SODOLA Lightly Managed Switch Web Manual

SL-SG008W

Tech Support: support@sodola-network.com

V1.10
2024-04-20

CATALOGS

Chapter 1 Manual Introduction	3
1.1. target audience	3
1.2. Manual Conventions	3
Chapter 2 Web Light Webmaster Features	4
2.1 Function Introduction	4
Chapter 3 Login Web Interface	5
3.1 Sign in	5
Chapter 4 Systems	6
4.1 System Information	6
IP install	7
4.2 User settings	8
4.3 Port Settings	8
Chapter 5 Configure	9
5.1 VLAN	9
5.2 QoS	10
5.2.1 Prioritisation	10
5.2.2 DSCP remap	11
5.2.3 Priority and Queue Mapping	11
5.2.4 Port Priorities	11
5.3 IGMP	12
5.4 Link aggregation	12
5.4 Loop protections	13
5.5 Spanning tree	13
5.6 Port Mirror	14
5.6 Port segregation	14
5.7 Bandwidth control	15
5.8 Giant frame	15
5.9 MAC constraints	16
5.10 Green Ethernet	16
5.11 Energy Efficient Ethernet (EEE)	16
5.12 SNMP	17
Chapter 6 Surety	17
6.1 MAC address	17
6.1.1 MAC address	17
Figure 28 MAC Address Information	17
6.1.2 MAC lookups	17
6.1.3 static MAC	18
6.2 Broadcasting storm	18
Chapter 7 Control	19
7.1 Port statistics	19
7.2 Cable Diagnostics	20
Chapter 8 Artifact	20
8.1 Firmware Upgrade	20
8.2 Configuration Backup	21
8.3 Reset	21
8.4 Save	22
8.5 Reopen	22

Chapter 1 Manual Introduction

1.1. target audience

This manual details how to configure each function of the Web Light Management Switch software. Please read this manual carefully before operation.

1.2. Manual Conventions

In this manual, we take 8-port switch as an example to show the web interface and software functions.

The --> symbol is used to indicate the order of menu entry, first-level function menu --> second-level function menu --> third-level function menu, of which, some functions have no second-level function menu.

The <> pointed brackets appear in the text to mark the text, indicating the name of the button, such as <apply>, <apply>.

The special icons used in this manual are described below:

Clarification	The description of the content of the operation, making the necessary additions and explanations.
 Take care	Reminds of the precautions to be taken during operation, improper operation may result in data loss or equipment damage.

Chapter 2 Web Light Webmaster Features

2.1 Function Introduction

Our newly developed Web light network management switch function software, support a variety of models. Provide VLAN, QoS, RSTP, SNMP, POE control, port aggregation and so on.

home page	Support for Logo, interface panel, and system information display
system	System information, IP address setting, user account, and port setting
configure	VLAN
	QOS
	IGMP
	Link aggregation
	Ring road protection
	RSTP
	Port mirror image
	Port isolation
	bandwidth control
	Giant frame
	MAC restrain
	Green Ethernet
	EEE
SNMP	
safe	MAC address
	broadcast storm
supervisory control	Port statistics
	Cable diagnosis
tool	firmware upgrade
	Configure backup
	reset
	preserve
	restart
	log off

Chapter 3 Login Web Interface

3.1 Sign in

1. The switch is powered up properly and any port is connected to the management PC.
2. The management PC has at least one of the following browsers installed: IE 8.0 or above, the latest version of Chrome, 360 browser.
3. The IP address of the management PC has been set to the same network segment as the switch port, i.e., 192.168.2.X (X is any integer between 2 and 253; the default IP of this product is 192.168.2.254), and the subnet mask is 255.255.255.0.

If you don't know how to set it up at all, follow these instructions step by step:

Step 1: Finding the Network Settings

- ① Click on the "Start" button (the Windows logo in the lower-left corner of the screen).
- ② In the search box, type "Network Settings" or "View network connections" and press Enter.
- ③ In the Network & Internet settings window, look for the option to "Change adapter options" or "View network status and tasks" (the exact text may vary depending on the Windows version).

Step 2: Changing your computer's IP Address

- (1) Right-click on the network adapter that is connected to the switch (it's usually labeled "Ethernet" or "Local Area Connection").
- (2) Select "Properties" from the context menu.
- (3) In the Properties window, scroll down and find "Internet Protocol Version 4 (TCP/IPv4)" and select it.
- (4) Click on the "Properties" button below it.
- (5) Make sure that "Use the following IP address" is selected.
- (6) Enter the IP address 192.168.2.X (replace X with any number between 2 and 253 that is not already in use on your network).
- (7) Enter the subnet mask as 255.255.255.0.
- (8) Leave the "Default gateway" and "DNS servers" fields blank or enter the appropriate values if known.
- (9) Click "OK" to save the settings.

Step 3: Accessing the Switch Management Interface

- ① 1. Open a web browser (IE 8.0 or above, the latest version of Chrome, 360 browser).
- ② 2. In the address bar, type `http://192.168.2.254` and press Enter.
- ③ 3. A login prompt will appear. Enter the username `admin` and password `admin`. Click on the "Login" or "Submit" button to access the switch's management interface.

4. To ensure a better experience of the Web interface display, it is recommended to adjust the resolution of your monitor to 1280 x 800 pixels or above.

5. Open a browser and enter the switch's default management address `http://192.168.2.254` (you can modify the management IP address according to the customer's requirements) in the address bar to log in the switch's Web management interface.

6. The switch login page is shown in the following figure, enter the user name and password for the switch management account, the factory defaults are all `admin`.

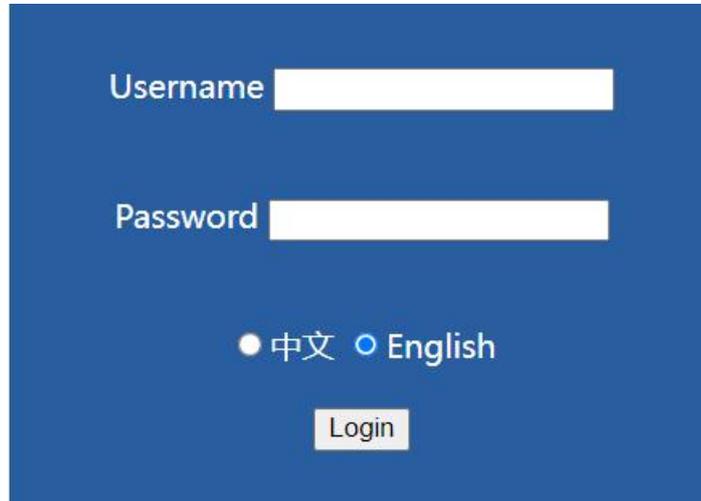


Figure 1 web login interface

7. After successful login, the homepage of the web interface is displayed as follows.

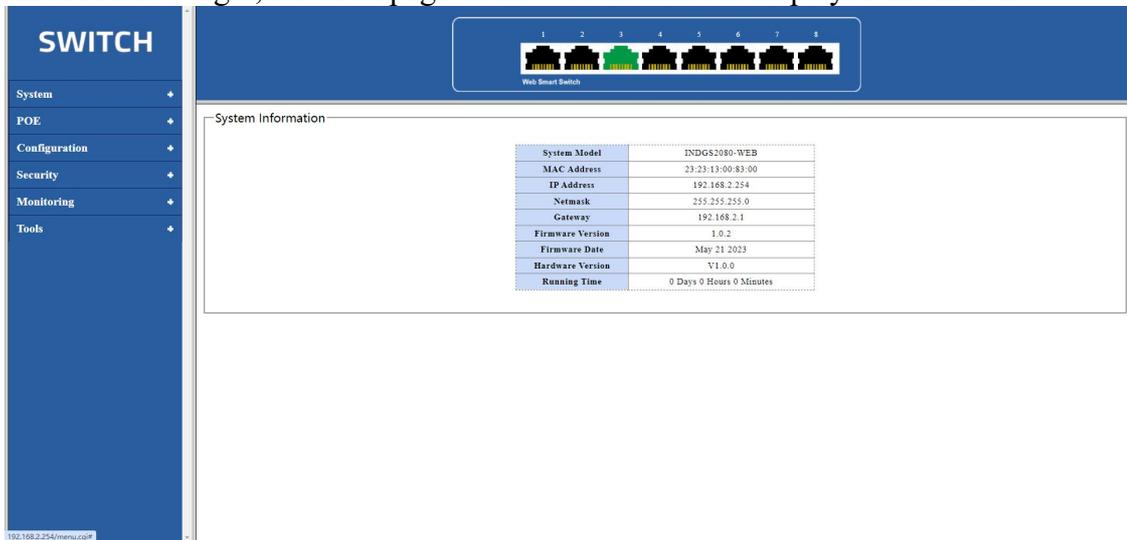


Figure 2 web home page

Left navigation bar, showing Logo, adjustable to no logo neutral. Upper right shows the model interface panel. Bottom right shows basic system information.

Chapter 4 Systems

4.1 System Information

System Information You can view the system information of the device here, as well as set the device model.

In the navigation bar, click: System --> System Information

System Information

System Model	INDGS2080-WEB
MAC Address	23:23:13:00:83:00
IP Address	192.168.2.254
Netmask	255.255.255.0
Gateway	192.168.2.1
Firmware Version	1.0.2
Firmware Date	May 21 2023
Hardware Version	V1.0.0
Running Time	0 Days 0 Hours 2 Minutes

Figure 3 System Information

Clarification:

unit type	Display device model
MAC address	Show the MAC address of the device
IP address	Display the device management IP address
subnet mask	Displays the device subnet mask
gateway	Displays the device's default gateway
Firmware version	Displays the software version
Firmware date	Displays the software version date
Hardware version	Displays the device hardware version
performance period	Displays the device startup running time

IP install

Each device in the network has an IP address through which it can log into the management interface to operate the switch.

Click the navigation bar: System --> IP Settings

IP Address Setting

DHCP Setting	Disable <input type="button" value="v"/>
IP Address	192.168.2.254
Subnet Mask	255.255.255.0
Gateway	192.168.2.1

Clarification:

DHCP Settings: Select to enable or disable the DHCP function.

Off: Select Off to manually enter the IP address, subnet mask and default gateway.

Enable: Select Enable to have the switch obtain network parameters from the DHCP

server.

IP Address: Set the IP address of the device.

Subnet Mask: Set the subnet mask of the device.

Default Gateway: Set the default gateway address of the device.

Click <Apply> System Management IP, Subnet Mask, and Gateway will be modified to the set values.

4.2 User settings

You can change the user name and password used for login here.

Click on the navigation bar: System --> User Accounts

User Account Setting

User Name	admin
New Password	
New Password	

Apply

Figure 5 User account settings

Clarification:

User Name sets the user name for logging into the switch. The user name cannot be longer than 16 characters and can only use numbers, English letters, and underscores.

New Password Reset the password for logging into the switch. The new password must be no longer than 16 characters in length and can only use numbers, letters and underscores. Make sure you enter the same password twice.

Note: Please refresh the page after changing the password. Do not change the password again before refreshing the page.

4.3 Port Settings

You can modify port name, status, duplex speed, flow control here.

Click the navigation bar: System --> Port Settings

Port Setting

Port	Name	State	Speed/Duplex	Flow Control
Port 1				
Port 2				
Port 3				
Port 4		Enable	Auto	Off
Port 5				
Port 6				

Apply

Port	Name	State	Speed/Duplex		Flow Control	
			Config	Actual	Config	Actual
Port 1		Enabled	Auto	Link Down	Off	Off
Port 2		Enabled	Auto	Link Down	Off	Off
Port 3		Enabled	Auto	1000Full	Off	Off
Port 4		Enabled	Auto	Link Down	Off	Off
Port 5		Enabled	Auto	Link Down	Off	Off
Port 6		Enabled	Auto	Link Down	Off	Off
Port 7		Enabled	Auto	Link Down	Off	Off
Port 8		Enabled	Auto	Link Down	Off	Off

Figure 6 Port Settings

Clarification:

Name: Set the port alias.

Port: Open Close, if open the port, the port can forward the message normally.

Rate/Duplex: Select 10M/Half, 10M/Full, 100M/Half, 100M/Full, Auto. When the mode select on is Auto, the rate and duplex will be decided by negotiation

Flow control function: on/off, turn on the flow control function, you can control and adjust the packet forwarding rate of each port to avoid congestion.

Note: The flow control function will actually be turned on in half duplex mode.

Chapter 5 Configure

5.1 VLAN

VLAN (Virtual Local Area Network, virtual local area network) VLAN technology is a communication technology that logically divides a physical LAN into multiple broadcast domains, and this technology is used to logically divide the physical network by defining extended fields on the LAN data frames, thus limiting the forwarding range of the LAN data frames and narrowing the broadcast domains. VLAN technology is mainly used in network devices such as switches, routers, and switches. Click on the navigation bar: Configuration --> VLAN --> Static VLAN

Static VLAN Table Setting

VLAN ID	(1-4094)	VLAN Name							
Port	Select All	Port 1	Port 2	Port 3	Port 4	Port 5	Port 6	Port 7	Port 8
Untagged	All	<input type="radio"/>							
Tagged	All	<input type="radio"/>							
Not Member	All	<input checked="" type="radio"/>							

Add / Modify

VLAN ID	VLAN Name	Member Ports	Tagged Ports	Untagged Ports	Delete
1	Default	1-8	-	1-8	<input type="checkbox"/>

Delete Select All

Figure 8 Static VLAN

Click on the navigation bar: Configuration --> VLAN --> VLAN Settings

VLAN Port Setting

Port	PVID	Accepted Frame Type
Port 1		All
Port 2		All
Port 3		All
Port 4		All
Port 5		All
Port 6		All

Apply

Port	PVID	Accepted Frame Type
Port 1	1	All
Port 2	1	All
Port 3	1	All
Port 4	1	All
Port 5	1	All
Port 6	1	All
Port 7	1	All
Port 8	1	All

Figure 9 VLAN Settings

VLANs are distinguished by the VLAN ID. all Untagged packets arriving at the port are tagged with the Tag of the port PVID.

Clarification:

You need to set the VLAN ID first and then set the port VID.

Static VLAN Set the VLAN ID, the value range is 1-4094.

Untagged port If selected as Untagged port, the output data frame is without tag information.

Tagged Port If selected as Tagged port, the output data frame is with tag information.

No Member Port When selected, it indicates that the port is not a member port of the VLAN.

5.2 QoS

The QoS (Quality of Service) feature is used to optimise network performance and provide a better network service experience. The switch is based on port, 802.1P, and DSCP priority modes.

5.2.1 Prioritisation

Click on the navigation bar: Configuration --> QOS --> Priority Selection

Priority selection Setting

Source	Decision
Port	
1Q	1
ACL	8
DSCP	1
CVLAN	1
SVLAN	1

Apply

Source	Decision
Port	7
1Q	1
ACL	8
DSCP	1
CVLAN	1
SVLAN	1
DA	1
SA	1

Figure 10 Priority Selection Settings

Clarification:

Priority Select sets the priority of the priority source and specifies the transmission queue for frames

based on the highest priority priority source.

5.2.2 DSCP remap

DSCP gives a recommended definition of the IP DSCP field. IP packets are mapped to 4 priorities (0,2,4,6) based on the DSCP value (0-63).

Click on the navigation bar: Configuration --> QOS --> DSCP Remapping

DSCP value	Priority
0	0
1	0
2	0
3	0
4	0
5	0
6	0
7	0
8	0
9	0
10	0
11	0
12	0
13	0
14	0
15	0

Figure 11 DSCP Priority Mapping

Clarification:

Sets the priority level corresponding to the DSCP value

5.2.3 Priority and Queue Mapping

Mapping different priorities to different output queues

Click on the navigation bar: Configuration --> QOS --> Priority to Queues

Priority	Queue ID
0	1
1	1
2	2
3	2
4	3
5	3
6	4
7	4

Figure 12 Priority queue mapping

5.2.4 Port Priorities

Port Priority is based on the incoming port These packets are mapped to 4 different priority levels.

Click on the navigation bar: Configuration --> QOS --> Port Priority

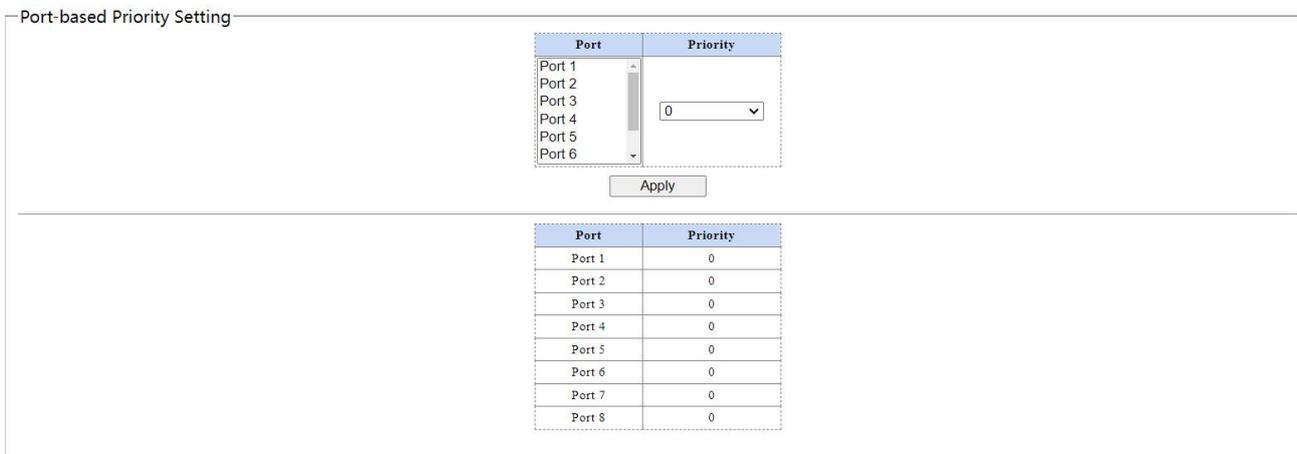


Figure 13 Port Priority Setting

5.2.5 Q Queue weights

Click on the navigation bar: Configuration --> QOS --> Q Queue Weights

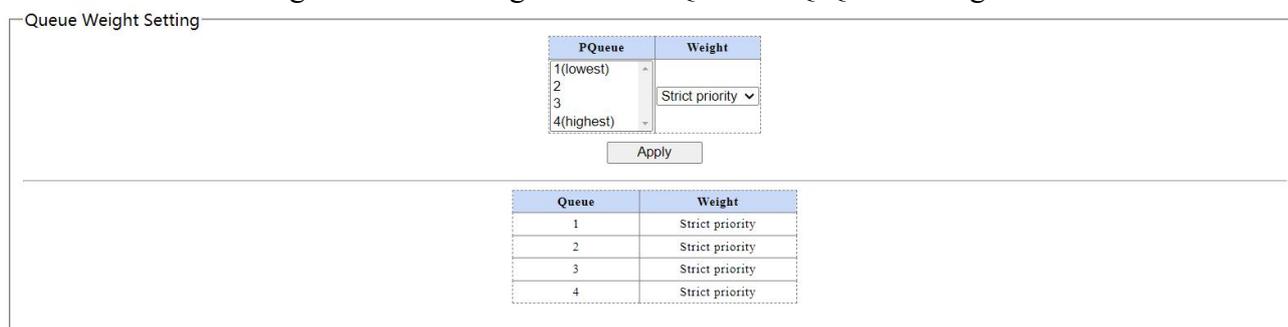


Figure 14 Q Queue Weights

5.3 IGMP

IGMP snooping (Internet Group Management Protocol Snooping) It is a multicast constraint mechanism running on Layer 2 devices for managing and controlling multicast groups. By configuring multicast VLANs, the ports of the switch are added to the multicast VLANs, so that users in different VLANs share a multicast VLAN to receive multicast data, and the multicast streams are transmitted in only one multicast VLAN, thus saving bandwidth. Moreover, since the multicast VLAN is completely isolated from the user VLAN, security and bandwidth are guaranteed.

Click the navigation bar: Configuration --> IGMP



Figure 15 IGMP Settings

Clarification:

IGMP: Enable Settings Select to enable or disable the IGMP listen function.

IP Address: View multicast IP address

Port: View the list of multicast group ports

VID: View the corresponding VLAN ID of multicast group.

5.4 Link aggregation

Link Aggregation (Link Aggregation) is a method of increasing bandwidth and reliability by bu

ndling a group of physical interfaces together as a logical interface.

Link Aggregation can be configured when there is a need for the following:

When there is insufficient bandwidth between two switch devices connected by a single link.

When the reliability of a link connection between two switch devices does not meet the requirements.

Click the navigation bar: Configuration --> Link Aggregation Settings

Figure 16 Link Aggregation Settings

Clarification:

Group ID: Aggregation group ID.

Port: Physical port belonging to the aggregation group

Member ports belonging to the same aggregation group must have a consistent configuration.

5.4 Loop protections

Loop that is, the switch under the network to form a ring topology, the loop will cause the intranet broadcast storm, will consume a lot of CPU and line bandwidth of the switch, and in serious cases, can even cause the device to die, the network is paralysed.

Click the navigation bar: Configuration --> Loop Protection

Figure 17 Loop Protection Setting

Clarification:

Time Interval: Monitor network loops at this time interval.

Recovery Time: When a loop is detected, the switch will activate the processing mechanism and the port will automatically return to normal after this time.

5.5 Spanning tree

Redundant links are often used in Ethernet switched networks for link backup and to improve network reliability. However, the use of redundant links creates loops in the switched network, causing broadcast storms and failures such as unstable MAC address tables, which leads to poor user communication quality and even communication interruption. In order to solve the problem of loops in switched networks, the Spanning Tree Protocol (STP) was proposed.

Like the development process of many protocols, the Spanning Tree Protocol is also updated with the development of the network, from the STP defined in the initial IEEE 802.1D to the Rapid Spanning Tree Protocol RSTP (Rapid Spanning Tree Protocol) defined in the IEEE 802.1W, and then to the latest IEEE 802.1S defined in the multi-spanning tree protocol MSTP. Spanning Tree .

Protocol (MSTP) defined in the latest IEEE 802.1S.

Click the navigation bar: Configuration --> RSTP Global Configuration --> RSTP Port

Spanning Tree Status	Disabled
Force Version	RSTP
Priority	32768
Maximum Age	20 (6-40 Sec)
Hello Time	2 (1-10 Sec)
Forward Delay	15 (4-30 Sec)
Root Priority	32768
Root MAC Address	23:23:13:00:83:00
Root Path Cost	0
Root Port	None
Root Maximum Age	20 Sec
Root Hello Time	2 Sec
Root Forward Delay	15 Sec

Apply

Figure 18 Spanning Tree Global Settings

Spanning Tree Port Setting

Port	Path Cost	Priority	P2P	Edge
Port 1	0 (1-200000000), 0 = Auto	128	Auto	False
Port 2				
Port 3				
Port 4				
Port 5				
Port 6				

Apply

Port	State	Role	Path Cost		Priority	P2P		Edge	
			Config	Actual		Config	Actual	Config	Actual
Port 1	Forwarding	Disabled	Auto	2000000	128	True	TRUE	False	False
Port 2	Forwarding	Disabled	Auto	2000000	128	True	TRUE	False	False
Port 3	Forwarding	Disabled	Auto	20000	128	True	TRUE	False	False
Port 4	Forwarding	Disabled	Auto	2000000	128	True	TRUE	False	False
Port 5	Forwarding	Disabled	Auto	2000000	128	True	TRUE	False	False
Port 6	Forwarding	Disabled	Auto	2000000	128	True	TRUE	False	False
Port 7	Forwarding	Disabled	Auto	2000000	128	True	TRUE	False	False
Port 8	Forwarding	Disabled	Auto	2000000	128	True	TRUE	False	False

Figure 19 Spanning Tree Port Settings

5.6 Port Mirror

Port mirroring is the process of copying messages from a specified port of a switch to a destination port; where the port being copied is called the source port and the copied port is called the destination port. The destination port will be connected to data inspection devices, and users use these devices to analyse the messages received on the destination port for network monitoring and troubleshooting.

Click the navigation bar: Configuration --> Port Mirroring

Mirror Direction	Mirroring Port	Mirrored Port List
Disable	Port 1	Port 1

Apply

Mirror Direction	Mirroring Port	Mirrored Port List
Disabled	-	-

Delete

Figure 20 Port Mirroring

Clarification:

Mirror Direction: Direction of data flow on the mirrored port (inbound, outbound, both directions)

5.6 Port segregation

Click on the navigation bar: Configuration --> Port Isolation

Port	Forwarding port
Port 1	Port 1
Port 2	Port 2
Port 3	Port 3
Port 4	Port 4
Port 5	Port 5
Port 6	Port 6

Apply

Port	Forwarding port
Port 1	1-8
Port 2	1-8
Port 3	1-8
Port 4	1-8
Port 5	1-8
Port 6	1-8
Port 7	1-8
Port 8	1-8

Figure 21 Port isolation

Clarification:

Port: Source Port

Port Isolation: Forwardable Port

Configure a forwarding port for the source port. packets received by the source port cannot be forwarded to ports that are not in the forwarding port.

5.7 Bandwidth control

Configuring port bandwidth means limiting the rate at which a physical interface can send outbound or receive inbound data.

Before traffic is sent out of an interface, configure rate limiting in the outbound direction of the interface to control all outgoing message traffic.

Before traffic is received from the interface, configure rate limiting on the inbound direction of the interface to control all incoming message traffic.

Click on the navigation bar: Configuration --> Bandwidth Control

Port	Type	State	Rate(Kbit/sec)
Port 1			
Port 2			
Port 3	Ingress	Disable	Unlimited
Port 4			
Port 5			
Port 6			

Apply

Port	Ingress Rate (Kbit/sec)	Egress Rate (Kbit/sec)
Port 1	Unlimited	Unlimited
Port 2	Unlimited	Unlimited
Port 3	Unlimited	Unlimited
Port 4	Unlimited	Unlimited
Port 5	Unlimited	Unlimited
Port 6	Unlimited	Unlimited
Port 7	Unlimited	Unlimited
Port 8	Unlimited	Unlimited

Figure 22 Bandwidth control

5.8 Giant frame

Configure the maximum message length that the system can forward

Click on the navigation bar: Configuration --> Jumbo Frames

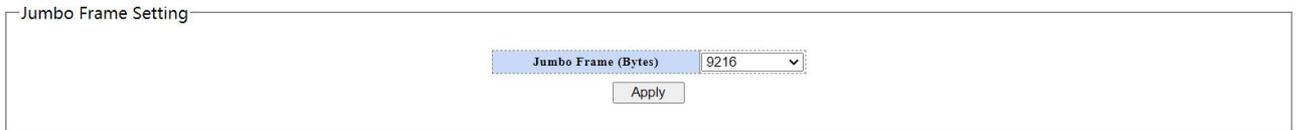


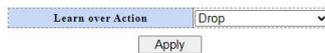
Figure 23 Giant Frame

5.9 MAC constraints

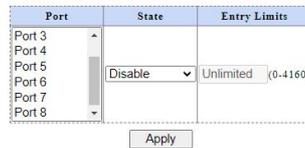
The system supports the port Mac learning restriction function. The system learns the source MAC in the user message, and when the learned MAC reaches the restriction threshold. If the source MAC of the user packet already exists in the MAC table, the user packet will continue to be forwarded; if the source MAC of the packet does not exist in the MAC table, the system will process the packet according to the MAC restriction action. For example, if the action is Discard, then the user packets will be discarded on the incoming port.

Click the navigation bar: Configuration --> Mac Constraints

MAC Constraint Action Setting



MAC Constraint Setting



Port	Entry Limits
Port 1	Unlimited
Port 2	Unlimited
Port 3	Unlimited
Port 4	Unlimited
Port 5	Unlimited
Port 6	Unlimited
Port 7	Unlimited
Port 8	Unlimited

Figure 24 Mac Constraints

5.10 Green Ethernet

Green Ethernet is a feature that is environmentally friendly and reduces the power consumption of devices. The system provides connection and dynamic detection of the cable length and dynamic adjustment of the power required for the detected cable length. High performance and low power consumption. The system supports link down power saving for ports, which greatly reduces power consumption when disconnecting the network cable. When an input signal is detected, it wakes up from link down power saving and enters normal mode.

Click the navigation bar: Configuration --> Green Ethernet

Green Ethernet Setting



Figure 25 Green Ethernet

5.11 Energy Efficient Ethernet (EEE)

Energy Efficient Ethernet (EEE) supports operation in low-power idle mode. Systems at both ends of the link can save power by disabling some functions during times of low link utilisation.

Click on the navigation bar: Configuration --> EEE

EEE function

Figure 26 EEE Settings

5.12 SNMP

SNMP is a standard network management protocol widely used in TCP/IP networks to support a network management system that monitors devices connected to the network for any conditions of managerial concern. The basic components of SNMP include the Network Management System (NMS), Agent, Managed Object and Management Information Base (MIB). Object (Managed Object) and Management Information Base (MIB).

Click on the navigation bar: Configuration --> SNMP

SNMP Function
 Trap IP Address
 Read Community
 Write Community

Figure 27 SNMP

Chapter 6 Surety

6.1 MAC address

MAC address in English is Media Access Control Address, directly translated as Media Access Control Address, also known as Local Area Network Address (LAN Address), Ethernet Address (Ethernet Address) or Physical Address (Physical Address), which is a bit address used to confirm the location of a network device. It is a bit address used to confirm the location of a network device.

6.1.1 MAC address

Hit the navigation bar: Security --> MAC Addresses --> MAC Table

MAC Address Information

No.	MAC Address	VLAN ID	Type	Port
1	68:DA:73:AE:4F:86	1	Dynamic	3

Figure 28 MAC Address Information

6.1.2 MAC lookups

Hit the navigation bar: Security --> MAC Address --> MAC Lookup

MAC Addresses Searching

MAC Address	VLAN ID
00:00:00:00:00:00	(1~4094)

Search

Figure 29 MAC Address Search

6.1.3 static MAC

Hit the navigation bar: Security --> MAC Address --> Static MAC

Static MAC Setting

MAC Address	VLAN ID	Port	Source MAC Blocking
00:00:00:00:00:00	(1~4094)	Port 1 Port 2 Port 3 Port 4 Port 5 Port 6	<input type="checkbox"/>

Add

No.	MAC Address	VLAN ID	Port	Source MAC Blocking	Select
Delete					

Figure 30 Static MAC

6.2 Broadcasting storm

A broadcast storm is a sharp increase in the number of broadcast frames on a network due to constant forwarding that affects normal network communications and severely degrades network performance. A broadcast storm can take up a considerable amount of network bandwidth, causing normal packets to fail. When broadcast data floods the network and cannot be processed and occupies a large amount of network bandwidth, resulting in the normal operation of the service can not be run, which occurs broadcast storms, resulting in local or entire network paralysis of the LAN.

Click on the navigation bar: Security --> Broadcast Storm

Storm Control Setting

Storm Type	Port	State	Rate (kbps)
Broadcast	Port 1 Port 2 Port 3 Port 4 Port 5 Port 6	Off	(8-1000000)

Apply

Port	Broadcast (kbps)	Multicast (kbps)	Unknown Unicast (kbps)	Unknown Multicast (kbps)
Port 1	10000	10000	10000	10000
Port 2	10000	10000	10000	10000
Port 3	10000	10000	10000	10000
Port 4	10000	10000	10000	10000
Port 5	10000	10000	10000	10000
Port 6	10000	10000	10000	10000
Port 7	10000	10000	10000	10000
Port 8	10000	10000	10000	10000

Figure 31 Storm Suppression

Clarification:

Figure 31 Storm Suppression Storm Type: Broadcast, Multicast, Unknown Unicast, Unknown Multicast

Port: Select port, multiple selections available

State: Turn on or off the broadcast storm suppression function

Speed: Set port broadcast, multicast packet, unknown unicast, unknown multicast bandwidth.

Chapter7 Control

7.1 Port statistics

The port statistics information displays the traffic information of each port, which is convenient for monitoring traffic and analysing network anomalies.

Click Navigation bar: Monitor --> Port Statistics.

Port	State	Link Status	TxGoodPkt	TxBadPkt	RxGoodPkt	RxBadPkt
Port 1	Enabled	Link Down	0	0	0	0
Port 2	Enabled	Link Down	0	0	0	0
Port 3	Enabled	Link Up	2430	0	3257	0
Port 4	Enabled	Link Down	0	0	0	0
Port 5	Enabled	Link Down	0	0	0	0
Port 6	Enabled	Link Down	0	0	0	0
Port 7	Enabled	Link Down	0	0	0	0
Port 8	Enabled	Link Down	0	0	0	0

Clear

Figure 32 Port statistics

Clarification:

Port: Port number

Status: Displays the status of the port, which can only forward packets normally when it is open.

Receive Status: Current LINK status of the port

Number of correct packets sent: Displays the number of correct packets sent by the port.

Error packets sent: Displays the number of packets sent incorrectly by the port.

Receive correct packets: Show the number of correct packets received by the port.

Number of packets received in error: Displays the number of packets received in error by the port.

7.2 Cable Diagnostics

When a cable is connected to a switch port, the cable test function can test the cable connection status, cable length for easy diagnosis of network failure points, the results are for reference only.

Click on the navigation bar: Monitor --> Cable Diagnostics

Port Statistics Information

Port	State	Link Status	TxGoodPkt	TxBadPkt	RxGoodPkt	RxBadPkt
Port 1	Enabled	Link Down	0	0	0	0
Port 2	Enabled	Link Down	0	0	0	0
Port 3	Enabled	Link Up	98	0	319	0
Port 4	Enabled	Link Down	0	0	0	0
Port 5	Enabled	Link Down	0	0	0	0
Port 6	Enabled	Link Down	0	0	0	0
Port 7	Enabled	Link Down	0	0	0	0
Port 8	Enabled	Link Down	0	0	0	0

Figure 33 Port Statistics Information

Clarification:

Diagnostics are not supported on ports connected to the service host.

Chapter 8 Artifact

8.1 Firmware Upgrade

The software of the switch can be upgraded here.

Click on the navigation bar: Tools --> Firmware Upgrade

Firmware Upgrade

Enter loader mode to upgrade firmware. After entering loader mode, configuration will be saved.

Figure 34 Entering Firmware Upgrade Mode

Click on the <Enter loader mode> button and the following picture appears

Enter Loader Mode

After 5 seconds, the browser will load the upgrade webpage.

Figure 35 Jump to loader mode

Finally jump to the firmware upgrade page

Click System --> HTTP Firmware Upgrade in the navigation bar, the following picture appears

Ethernet Switch

System -

HTTP Firmware Upgrade

Reboot

HTTP Firmware Upgrade

未选择任何文件

Figure 36 Firmware Upgrade Page

Click the <Select File> button to load the latest firmware file. Click <Upgrade> to start the upgrade and click <OK> in the pop-up window.



The following figure is displayed after the upgrade is completed.



Figure 38 Upgrade complete



Attention :

During the firmware upgrade process, please do not power off the device, keep the power stable and do not refresh the page .

Upgrading the firmware may lose the current unsaved configuration information, please save the configuration before upgrading.

Click the navigation bar: System --> Reboot to reboot the switch.



Figure 39 Reboot the switch

8.2 Configuration Backup

You can save the current configuration information here, it is recommended to backup the current configuration information before modifying the configuration and upgrading the software.

Click the navigation bar: Tools --> Configuration Backup



Figure 40 Configuration Backup and Restore

Backup Settings: Click <Backup> to download the current configuration file locally through your browser.

To restore settings: Click <Select File> to select the configuration file and click Upgrade. After that, reboot the switch to take effect.

8.3 Reset

In addition to the Hardware Restore Factory Settings switch, you can also restore the default settings at Web.

Hit the navigation bar: Tools --> Reset

on

Reset to default factory settings and restart the system.

Factory Default

Figure 41 Restore default settings

Click the <Restore Defaults> button and the switch restores all setting defaults. The current configuration information will be lost.

It is recommended to backup the configuration before restoring the defaults.

The default management IP address is 192.168.2.254 and the account name and password are admin.

8.4 Save

Click on the navigation bar: Tools --> Save



Figure 42 Save Configuration to FLASH

It is recommended to save the settings to FLASH after modifying the settings, otherwise the modified settings will be lost after power failure or reboot.

8.5 Reopen

After clicking Reboot, the switch will reboot. Before rebooting, it is recommended to save the configuration to prevent the loss of the currently modified configuration.

Click the navigation bar: Tools --> Save

Reboot the switch.

Reboot

Figure 43 Rebooting the Switch



Attention :

Please do not turn off the power during the reboot process, ensure the power supply is stable during the reboot process, and avoid forcible power failure.