
Full-Gigabit 2-Fiber 24-Copper Web-Managed PoE Switch

Light network management series

WEB Network Management Operation Guide

Model: KL-024G-SFP



www.kline.knowledgline.com

Ver 1.0.1

Declare

Copyright, all rights reserved

The copyright of this manual belongs to our company. Without the written permission of our company, no unit or individual may extract or copy part or all of the contents of this book without authorization, and may not disseminate it in any form.

Foreword

This manual mainly describes the WEB platform page of the light network management Ethernet switch. The user can manage the switch through the WEB page. This manual only gives a brief introduction to the operation of each WEB page. Please refer to the User Manual for the introduction of each function.

The preamble contains the following:

- Audience Object
- Product Introduction

Audience Object

- Network Planner
- On-site technical support and maintenance personnel
- Network administrator responsible for network configuration and maintenance

Product Introduction

The light network management Ethernet switch is independently designed and developed by our company. It is a web management Ethernet switch specially designed for building a high-security and high-performance network. T

he system uses a new software and hardware platform to provide a comprehensive security protection system, simple VLAN switching, port isolation and so on. The light network management series is easy to manage and maintain, and is an ideal convergence layer switch for office networks, campus networks, small and medium-sized enterprises, and branch offices.

[Version Update]

Ver 1.0.1

User experience optimization

Resolves known issues and provides faster response.

Related functions are optimized to make management easier.

Directory

Chapter 1 Login Management Interface	6
1.1 Logon preparation	6
1.2 Login step	7
Chapter 2 WEB Management Function	8
2.1 Interface description	8
2.2 system	9
2.2.1 System Information	9
2.2.2 IP Settings	9
2.2.3 SNTP Settings	10
2.2.4 User Settings	11
2.2.5 Port Settings	11
2.3 configurations	12
2.3.1 VLAN Settings	12
2.3.2 QoS	17
2.3.3 DHCP Snooping	20
2.3.4 IGMP Settings	21
2.3.5 Link Aggregation	22
2.3.6 Loop Protection	23
2.3.7 RSTP Global	24
2.3.8 RSTP port	25
2.3.9 Port mirroring	26
2.3.10 Port Isolation	28
2.3.11 Bandwidth Control	30
2.3.12 Jumbo frame	31
2.3.13 MAC constraint	31
2.3.14 Green Ethernet	32
2.3.15 EEE	32

2.4 safe	33
2.4.1 MAC Addr	33
2.4.2 Broadcast Storm	35
2.5 Monitor	35
2.5.1 Port Statistics	35
2.5.2 Cable Diagnostics	36
2.6 tool	36
2.6.1 Firmware upgrade	36
2.6.2 Configure Backup	37
2.6.3 Reset	37
2.6.4 save	38
2.6.5 Timed restart	38
2.6.6 Manual Restart	38
2.6.7 Logout	39

Chapter 1 Login Management Interface

1.1 Logon preparation

1. The switch is normally powered on and started, and any interface is connected with a computer network port for login management;
2. Make sure that the function switch on the front panel of the switch is in the "WEB" position (only support the function switch series);
3. At least IE 8.0 or above, the latest version of FireFox, Chrome and Safari browsers or one of the above core browser software should be installed on the management computer;
4. The IP address of the network card connecting the management computer and the switch should be in the same network segment as the management IP address of the switch. It should be 192.168. 0. * (* is any integer between 3 and 254) when it is set for the first time. The subnet mask is 255.255. 255.0.



Figure 1.1



Verify that the function switch is in the WEB position when logging in to the switch (function switch series only).

1.2 Login step

1. Open the browser and enter the management address of the switch in the address bar (the default address is the http://192.168.0.1) to log in to the management interface of the switch.
2. Enter the switch management username and password in the pop-up login window. The default username and password are admin.

Username

Password

☐ 中文 ☒ English

3. After a successful login, the switching system information page is displayed.

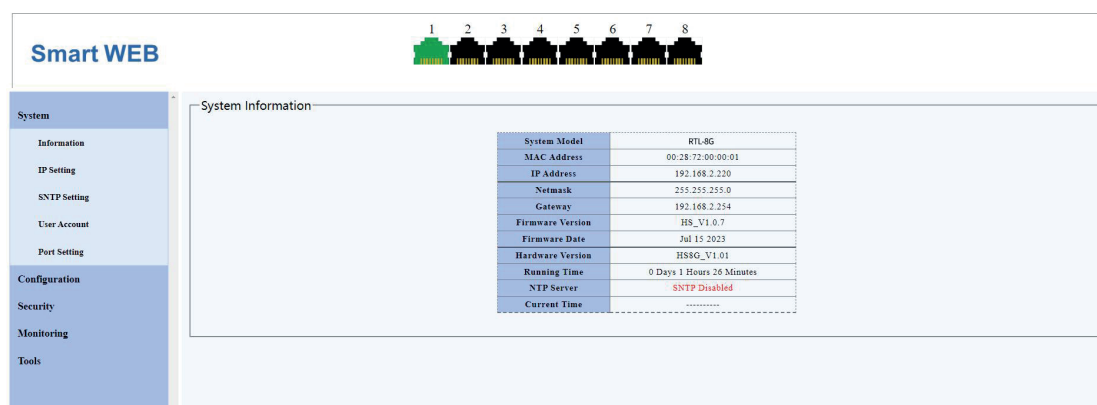


Figure 1.2 Switching System Page

Chapter 2 WEB Management Function

2.1 Interface description

- ① **Interface Status:** Displays the working status of the port. Green indicates that the port is connected. Uncolored indicates that the port is not connected.
- ② **Function navigation tree:** You can quickly switch to the corresponding function page through function navigation.
- ③ **Function details:** information display and configuration details of the currently selected function.

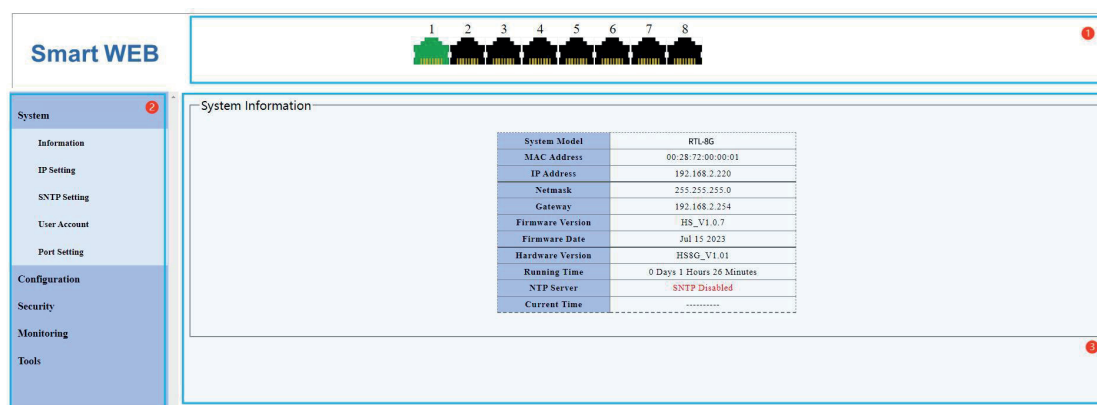


Figure 2.1 Interface description

2.2 system

2.2.1 System Information

The system information page displays the basic information of the switch system, including device model, MAC address, IP information, firmware and hardware version information.

System Information	
System Model	RTL-8G
MAC Address	00:28:72:00:00:01
IP Address	192.168.2.220
Netmask	255.255.255.0
Gateway	192.168.2.254
Firmware Version	HS_V1.0.7
Firmware Date	Jul 15 2023
Hardware Version	HS8G_V1.01
Running Time	0 Days 1 Hours 26 Minutes
NTP Server	SNTP Disabled
Current Time	-----

Figure 2.2.1 System Information Page

2.2.2 IP Settings

Displays and sets the management IP address of the switch.

When the IP mode is Static IP, you can manually configure the IP address, subnet mask, and gateway information.

When the IP mode is DHCP, the switch automatically obtains IP information from a DHCP server in the network.

DHCP Settings	
IP address	192.168.0.1
Subnet mask	255.255.255.0
Gateway	192.168.0.254

Apply

Figure 2.2.2 IP Settings Page



When switching the IP mode, you need to log in the switch again;

After modifying the management IP application, you need to use the new IP address to log in and ensure that the network segment of the management computer matches it.

2.2.3 SNTP Settings

Simple Network Time Protocol, adapted from NTP, is primarily used to synchronize computer clocks across the Internet

In this interface, you can add the corresponding time service area to synchronize the time between the time switch and the time server. The details can be viewed in the system configuration.

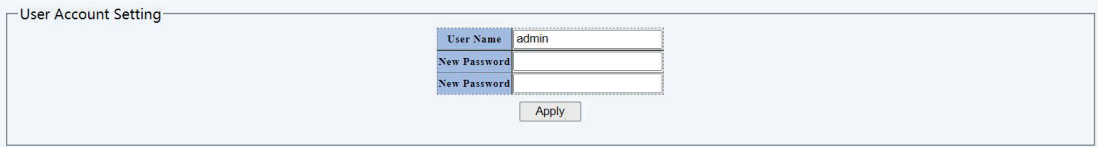
SNTP Setting	
Time Server IP	182.92.12.11
Time Server IP(Backup)	185.209.85.222
Time Zone(Ex: 8 or -3)	8

Apply

Figure 2.2.3 SNTP Setting Page

2.2.4 User Settings

On the User Settings page, you can modify the user name and password of the switch management account. If a new user name is set on this page, the original user name will be invalid. The password length is required to be between 8 and 16 digits.

A screenshot of the 'User Account Setting' web form. The form has a light blue background and a thin border. It contains three input fields: 'User Name' with the value 'admin', 'New Password', and another 'New Password' field. Below these fields is an 'Apply' button.

User Name	admin
New Password	
New Password	
Apply	

Figure 2.2.4 User Settings Page

2.2.5 Port Settings

The Port Settings page allows the user to set and display the port status, including the following:

Status: "Open" and "Close" status. If set to "Close", the port is manually closed and communication is not possible;

Speed/Duplex: All interfaces default to Auto, which is adaptive mode. It can be manually configured as "full-duplex/half-duplex mode", and the speed of 10 M, 100 M and 1000 M can be selected. It is generally recommended to select "Automatic" mode;

Flow control: When the flow control is on and the port is blocked, the switch will send a "PAUSE" frame to the information officer to inform the information source to pause for a period of time before sending the information.

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	1000Full	Off	Off
Port 2		Enabled	Auto	Link Down	Off	Off
Port 3		Enabled	Auto	Link Down	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 2.2.5 Port Settings Page

2.3 configurations

2.3.1 VLAN Settings

2.3.1.1 Static VLAN

Static VLANs are used to set the 802.1Q VLAN properties for a switch port.

VLAN ID: Identifier used to distinguish different VLANs. Terminals in different VLANs cannot communicate directly.

VLAN name: a name or description of the corresponding VLAN, usually used to visually distinguish different VLANs.

No tag: The port is marked as having no tag. When the data frame goes out of the port, if it is a frame with a VLAN tag, the tag will be removed and then sent out. If it is a data frame without a tag, it will be sent out directly. Data frames entering the port are internally tagged with the VLAN ID of the port. Commonly used for access terminal equipment.

Label: The port identified as a label carries the VLAN ID label when the d

ata frame is sent to the port. Therefore, the peer device must be able to identify the VLAN label, otherwise it cannot identify the data normally. Typically used to connect to the TRUNK, HYBRID, or VLAN-capable router ports of a managed switch.

No member: when the port is checked, it means that the current port is not a member port of this VLAN.

Add/Modify VLAN

- Fill in the VLAN ID and VLAN name to be added (optional);
- Select the corresponding option under the port name according to the tag and tag attributes required by the port (click the "VLAN" button of the corresponding option to set all ports to the corresponding attributes);
- Click the "Add/Modify" button below.

Delete VLAN

- Check the delete selection box behind the corresponding VLAN ID in the VLAN list below, and click "Delete" to delete the corresponding VLAN;
- VLAN 1 is the default VLAN and cannot be deleted. Click Select All to select all VLANs except VLAN 1 and delete all VLANs except VLAN 1.

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	☐	☐	☐	☐	☐	☐	☐	☐
Tagged	All	☐	☐	☐	☐	☐	☐	☐	☐
Not Member	All	☒	☒	☒	☒	☒	☒	☒	☒

Add / Modify

VLAN ID	VLAN Name	Member Ports	Tagged Ports	Untagged Ports	Delete
1	Default	1-8	-	1-8	☐

Delete

Select All

Figure 2.3.1.1 Static VLAN pack

2.3.1.2 VLAN Settings

The VLAN Port Settings page is used to set the PVID of the port (based on the VLAN ID of the port) and the frame format that the port receives.

PVID: All ports have one and only one PVID. When an untagged data frame enters a switch port, the switch internally tags the data frame from that port with the PVID. The default PVID for all ports is 1.

Receiving frame format

All: The designated port processes received frames regardless of whether they are tagged or not. For untagged frames, the PVID is tagged with the VLAN tag for further processing. For the tagged frame, if the port belongs to the member of the corresponding VLAN ID, the next step is processed, and if the port does not belong to the member, the frame is discarded.

Labeled Only: Specifies that the port only receives labeled data frames. Generic client devices do not support VLAN tagging, so the port to which the client is connected may not communicate when this option is selected.

Unlabeled Only: Specifies that the port only receives unlabeled data frames. If the interface of the peer device is multi-VLAN communication (such as the TRUNK interface of the switch and the router configured with VLAN-based subinterfaces), only PVID can communicate.

VLAN Port Setting

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

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 2.3.1.2-1 VLAN Setting Page

For example, as shown in the 2.3, 1.2 -2, the superior device has been configured with VLANs 10, 20, and 30, and the corresponding VLAN is allowed to pass through the port connected to the switch. The three terminals connected to port 1, 2 and 3 of this machine are respectively planned to VLAN 10, 20 and 30.

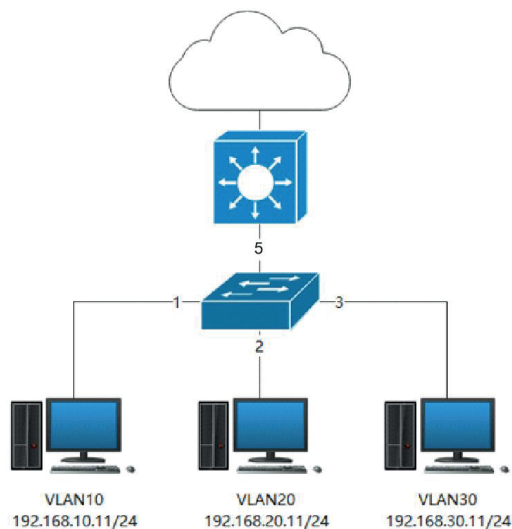


Figure 2. 3. 1. 2-2

Start by adding the appropriate VLAN and port settings on the Static VLAN N page. Take VLAN 10 as an example, fill in VLAN ID 10, select No Label under port 1, select Label under port 5, and click Add. When all VLANs have been added, you should see Figure 2.3. 1.2-3.

Static VLAN Table Setting

VLAN ID	VLAN Name								
Port	Select All	Port 1	Port 2	Port 3	Port 4	Port 5	Port 6	Port 7	Port 8
Untagged	All	☐	☐	☐	☐	☐	☐	☐	☐
Tagged	All	☐	☐	☐	☐	☐	☐	☐	☐
Not Member	All	☒	☒	☒	☒	☒	☒	☒	☒

Add / Modify

VLAN ID	VLAN Name	Member Ports	Tagged Ports	Untagged Ports	Delete
1	Default	1-8	-	1-8	☐
10		1,5	5	1	☐
20		2,5	5	2	☐
30		3,5	5	3	☐

Delete Select All

Figure 2. 3. 1. 2-3

Then enter the "VLAN Port Settings" page, select port 1, fill in PVID 10, and click Apply. Set port 2 and port 3 respectively according to this method, and set PVID to 20 and 30 respectively, as shown in Figure 2.3. 1.2 -4.

VLAN Port Setting

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

Apply

Port	PVID	Accepted Frame Type
Port 1	10	Untag-only
Port 2	20	Untag-only
Port 3	30	Untag-only
Port 4	1	All
Port 5	1	All
Port 6	1	All
Port 7	1	All
Port 8	1	All

Figure 2. 3. 1. 2-4

For example, as shown in the figure 2.3.1.2-5. When multiple broadband need to be accessed, but the number of available physical interfaces of the router is insufficient, it is necessary to expand the Wan port through the switch (this function needs to be supported by the router function).

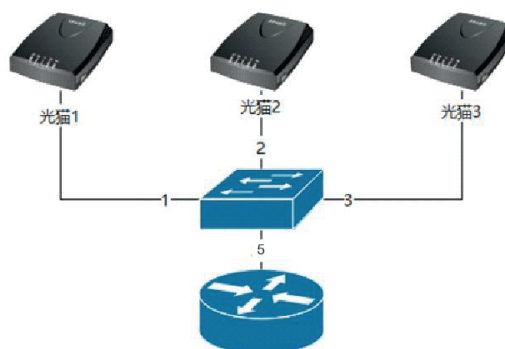


Figure 2.3.1.2-5

The relevant settings of the switch are the same as the previous example, but the difference is that 5 ports are connected to the router, and 1-3 ports are connected to the corresponding operator access equipment respectively. After that, use the corresponding VLAN ID to configure the corresponding subinterface or related Wan port configuration in the router.

2.3.2 QoS

2.3.2.1 Priority Choice

The priority selection page sets different types of priorities for packets forwarded through the switch. The higher the value, the higher the priority.

Priority selection Setting

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

Apply

Figure 2.3.2.1 Priority Selection Page

2.3.2.2 DSCP remapping

Sets the DSCP value in IP packets entering the switch port and determines the output queue for the packet based on the user-configured DSCP value and priority. Select the DSCP value to be set and the level priority value to determine

ermine the output queue of the data packet.

DSCP remapping

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

Apply

DSCP value	Priority
0	0
1	0

Figure 2.3.2.2 DSCP remapping page

2. 3. 2. 3 Priority to Queue

The queue priority page is used to sort the priority of the data packet queue output by the switch and determine the output queue of the data packet. The higher the priority value is, the higher the priority is. The data in this queue is forwarded first.

Priority to queue id Setting

Priority	Queue ID
0	
1	
2	
3	
4	
5	

Apply

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

Figure 2.3.2.3 Priority to Queue Page

2.3.2.4 Port priority

The port priority page is used to arrange the priority of the data packets transmitted by the switch port. The higher the value, the higher the priority.

Port-based Priority Setting

Port	Priority
Port 1	0
Port 2	0
Port 3	0
Port 4	0
Port 5	0
Port 6	0

Apply

Port	Priority
Port 1	0
Port 2	0
Port 3	0
Port 4	0
Port 5	0
Port 6	0
Port 7	0
Port 8	0

Figure 2.3.2.4 Port Priority Page

2.3.2.5 Queue weight

The queue scheduling page can select the scheduling strategy and the corresponding priority in the queue priority to define the weight value. (Weight value min 1 Max 15).

Queue Weight Setting

PQueue	Weight
1(lowest)	Strict priority
2	Strict priority
3	Strict priority
4(highest)	Strict priority

Apply

Queue	Weight
1	Strict priority
2	Strict priority
3	Strict priority
4	Strict priority

Figure 2.3.2.5 Queue Weight Page

2.3.3 DHCP Snooping

Through the DHCP Snooping function, IP address confusion caused by manual configuration of IP addresses by illegal DHCP servers and clients can be eliminated.

port	Select ALL	Port 1	Port 2	Port 3	Port 4	Port 5	Port 6	Port 7	Port 8
DHCP Client	Select All	☒	☒	☒	☒	☒	☒	☒	☒
DHCP Server	Select All	☐	☐	☐	☐	☐	☐	☐	☐

Figure 2.3.3-1 DHCP Snooping Page

For example, as shown in Figure 2.3.3-2, port 5 of the switch is connected to a router as a legal DHCP server to allocate an IP address to an intranet terminal, and port 4 is connected to an illegal DHCP server.

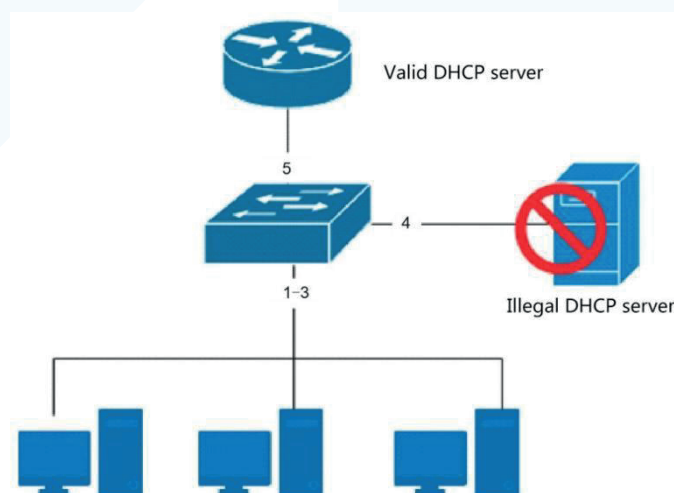


Figure2. 3. 3-2

As shown in the figure below, select ports 1-3 as DHCP Client and ports 4-5 as DHCP Server. Through the above configuration, the switch will discard the DHCP OFFER messages sent by interfaces other than 4-5, so as to prevent

nt DHCP servers other than 4-5 from providing illegal address allocation services.

DHCP Snooping config

DHCP Snooping Setting ☒

Apply

port	Select ALL	Port 1	Port 2	Port 3	Port 4	Port 5	Port 6	Port 7	Port 8
DHCP Client	Select All	☒	☒	☒	☐	☐	☐	☐	☐
DHCP Server	Select All	☐	☐	☐	☒	☒	☒	☒	☒

Apply

Figure2. 3. 3-3

At the same time, non-DHCP IP addresses obtained on the port selected as the DHCP Client will not be able to communicate.



After the DHCP Snooping function is configured, when the device on the port selected as the DHCP Client obtains the address through the DHCP service for normal communication, if the switch is restarted, the binding relationship will be invalid and the communication cannot be performed, and the device needs to obtain the address through the DHCP again for normal communication.

2. 3. 4 IGMP Settings

After the IGMP setting is enabled, the multicast packet is only forwarded to the corresponding member port, and the data packet of the multicast group is not forwarded to the non-member port, and the unknown multicast packet is discarded.

When the IGMP function is not enabled, the multicast packet will be broad

dcast and forwarded to all ports.

IGMP Enable Setting

Enable

☐

Apply

Dump IGMP entry

IP Address	Ports	Vid
------------	-------	-----

Figure 2.3.4 IGMP Settings Page

2. 3. 5 Link Aggregation

Port aggregation is mainly used to bind two or more physical links into one logical link between switches to achieve bandwidth increase, load balancing, link redundancy, and other functions.

The switch supports 2 aggregation group, and each aggregation group can support up to 4 ports.

When adding ports, you can press and hold the mouse to select multiple consecutive ports. When selecting non-consecutive ports, you can press and hold the "Ctrl" key to select multiple ports or deselect the corresponding ports.

Trunk Group Setting

Group ID	Ports
Trunk1	Port 1 Port 2 Port 3 Port 4 Port 5 Port 6

Add / Modify

Group ID	Ports	Select
----------	-------	--------

Delete

Select All

Figure 2.3.5 Link Aggregation Page



e to the closure of the port by the spanning tree protocol.

2.3.6 Loop Protection

Loop prevention settings are mainly divided into three categories: loop prevention, loop detection, and spanning tree.

Loop Prevention Setting

Loop function	Off
Time Interval (1-32767)	1 sec
Recover Time (4-65535)	4 sec

Apply

Figure 2.3.6-1 Loop Protection Page

Loop prevention: After this function is enabled, when the link has a loop, the switch will block the corresponding loop port.

Loop Prevention Setting

Loop function	Loop Prevention
Time Interval (1-32767)	1 sec
Recover Time (4-65535)	4 sec

Apply

Port	State
Port 1	Disable
Port 2	
Port 3	
Port 4	
Port 5	
Port 6	

Port	Loop State	Loop Status
Port 1	Disabled	FORWARDING
Port 2	Disabled	FORWARDING
Port 3	Disabled	FORWARDING
Port 4	Disabled	FORWARDING
Port 5	Disabled	FORWARDING
Port 6	Disabled	FORWARDING
Port 7	Disabled	FORWARDING
Port 8	Disabled	FORWARDING

Apply

Figure 2.3.6-2 Loop Prevention Page

Loop detection: After this function is enabled, it can detect whether there is a loop in the link, and the loop indicator will start flashing.

Loop Prevention Setting

Loop function
Time Interval (1~32767)
Recover Time (4~65535)

Loop Detection
1 sec
4 sec

Apply

Figure 2.3.6-3 Loop Detection

Spanning Tree: Enable this function to directly open the RSTP global.

Loop Prevention Setting

Loop function
Time Interval (1~32767)
Recover Time (4~65535)

Spanning Tree
1 sec
4 sec

Apply

Figure2.3.6-4 Spanning tree

2.3.7 RSTP Global

RSTP: (rapid spanning Tree Protocol) Rapid Spanning Tree Protocol is turned on in Loop Protection. This protocol can converge the network more quickly when the network structure changes, and is used as a backup of the designated port.

STP: Spanning Tree Protocol. The protocol can be applied to the loop network to achieve path redundancy through a certain algorithm, and at the same time, the loop network is pruned into a loop-free tree network, so as to avoid the proliferation and infinite circulation of messages in the loop network.

After opening this page, you can configure the RSTP/STP protocol and priority according to the actual environment.

Spanning tree priority: small priority, default 32768, step length 4096, value range 0 ~ 61440.

Spanning Tree Setting

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	00:27:82:00:00:01	
Root Path Cost	0	
Root Port	None	
Root Maximum Age	20 Sec	
Root Hello Time	2 Sec	
Root Forward Delay	15 Sec	

Apply

Figure 2.3.7 RSTP Global Page

2.3.8 RSTP port

After RSTP is enabled, relevant ports can be configured on this page

Path Cost, an STP metric used to represent the distance between bridges. Path Cost is the sum of all link costs along the path between two bridges.

Port priority: small priority, default 128, step 16, value range 0 ~ 240.

Point-to-point: It means that the sender transmits data to the device directly connected to it, and this device transmits data to the next device directly connected to it at an appropriate time, and the data is transmitted to the receiving end through one directly connected device.

In RSTP, when a non-edge designated port moves from blocking to forwarding, the handshake with the downstream bridge must ensure that the link is a point-to-point link.

Spanning Tree Port Setting

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

Apply

Port	State	Role	Path Cost		Priority	P2P		Edge	
			Config	Actual		Config	Actual	Config	Actual
Port 1	Forwarding	Disabled	Auto	20000	128	True	TRUE	False	False
Port 2	Forwarding	Disabled	Auto	2000000	128	True	TRUE	False	False
Port 3	Forwarding	Disabled	Auto	20000000	128	True	TRUE	False	False
Port 4	Forwarding	Disabled	Auto	20000000	128	True	TRUE	False	False
Port 5	Forwarding	Disabled	Auto	20000000	128	True	TRUE	False	False
Port 6	Forwarding	Disabled	Auto	20000000	128	True	TRUE	False	False
Port 7	Forwarding	Disabled	Auto	20000000	128	True	TRUE	False	False
Port 8	Forwarding	Disabled	Auto	20000000	128	True	TRUE	False	False

Figure 2.3.8 RSTP Ports Page

2.3.9 Port mirroring

The port mirror function can be set to copy the data of the specified direction of the port to the mirror port. Up to 4 sets of port mirroring can be set.

Mirror direction:

Ingress mirroring: Mirrors only the traffic coming in from that port.

Egress mirroring: Only the traffic originating from this port is mirrored.

Bidirectional mirroring: supports the mirroring of bidirectional traffic to and from the port.

Mirror Port: The port to which the port is mirrored. The mirrored data will be sent to this port. For example, in a packet capture application, this interface is used to connect to a computer running packet capture software.

Mirrored Port: The data source port of the port mirroring function. Packets in the specified direction of the mirrored port will be copied to the mirroring port.

Port Mirroring Setting

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

Apply

Mirror Direction	Mirroring Port	Mirrored Port List
Disabled	-	-

Delete

Figure 2.3.9-1 Port Mirroring Page

For example, as shown in 2.3.9-2, the computer installed by the administrator with packet capture software is connected to port 1 of the switch, and the data sent by the computer connected to port 2 needs to be analyzed by packet capture.

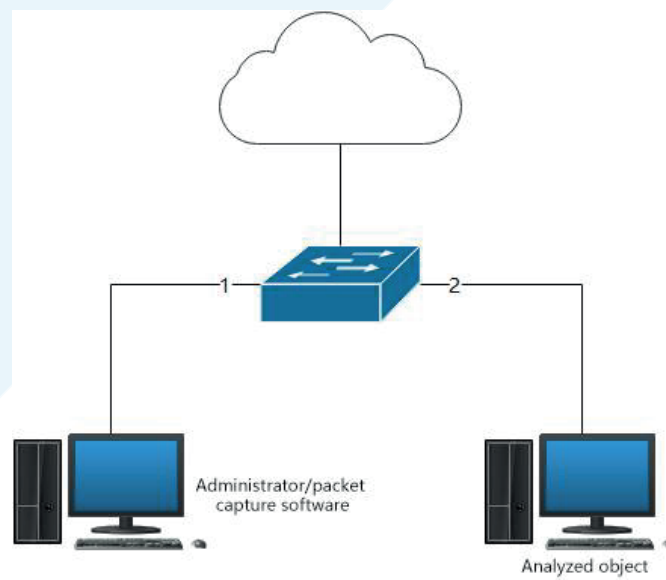


Figure 2. 3. 9-2

As shown in Figure 2.3.9-3, the direction is RX (the message sent by the device connected to the switch is received by the switch port), the monitoring port is 1, and the mirrored port is 2.

Port Mirroring Setting

Mirror Direction
Disable

Mirroring Port
Port 1

Mirrored Port List
Port 1

Apply

Mirror Direction	Mirroring Port	Mirrored Port List
Rx	1	2

Delete

Figure 2. 3. 9-3

2. 3. 10 Port Isolation

The port isolation function can realize the two-layer data isolation between different ports, and can not communicate with each other. By default, all ports are not isolated from each other.

Port: The object port to set.

Allow Forwarding Ports: Ports that are allowed to communicate with the object port, that is, ports that are not isolated from the object port mirror. Except for the allowed forwarding port, the other ports cannot communicate with the object port.

When adding ports, you can hold down the mouse and drag to select multiple consecutive ports. When selecting non-consecutive ports, you can hold down the "Ctrl" key to select multiple ports or deselect the corresponding ports.

Port Isolation Setting

Port
Port 1
Port 2
Port 3
Port 4
Port 5
Port 6

Forwarding port
Port 1
Port 2
Port 3
Port 4
Port 5
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 2.3.10-1 Port Isolation Page

For example, as shown in Figure 2.3. 10-2, the five ports of the switch are connected to the Internet through the router, and the five ports are connected to a server. It is required that all terminals on ports 1-3 cannot communicate with each other, but they are allowed to access the Internet and the server.

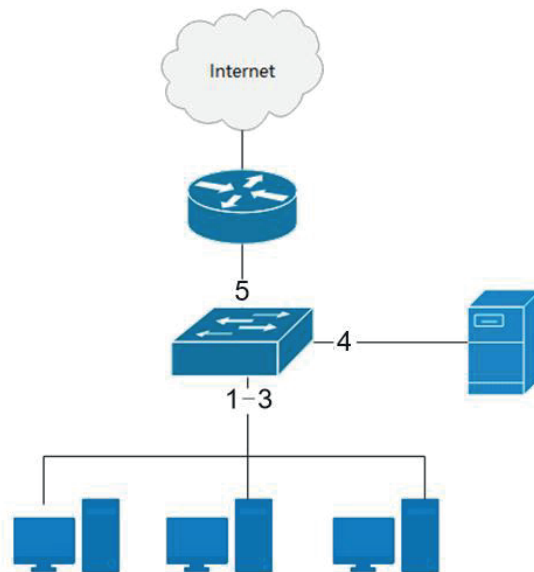


Figure2. 3. 10-2

Select ports 1-3 in the port column, select ports 4 and 5 in the allowed for warding port column, and click Apply. As shown in Figure 2.3.10-3:

Port Isolation Setting

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

Figure2. 3. 10-3

Isolation cannot be set for all upstream ports.



In general, it is necessary to ensure that the uplink port is located in the allowed forwarding port of all object ports to ensure normal communication with the superior device.

2. 3. 11 Bandwidth Control

Bandwidth control limits the maximum rate for a specified port and direction, with a minimum control granularity of 16Kbps.

Port: The object port to set.

Type: inlet or outlet

Status: Enable or disable the bandwidth control function of the object port.

Rate: The maximum rate of throttling. The rate value must be an integer multiple of 16.

Bandwidth Control Setting

Port	Type	State	Rate(Kbit/sec)
Port 1	Ingress	Disable	Unlimited (8-1000000, multiple of 8)
Port 2			
Port 3			
Port 4			
Port 5			
Port 6			

Apply

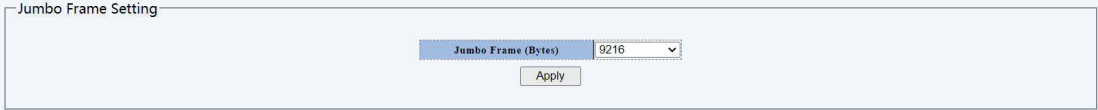
Port	Ingress Rate (Kbit/sec)	Egress Rate (Kbit/sec)
Port 1	Unlimited	Unlimited
Port 2	Unlimited	Unlimited
Port 3	Unlimited	Unlimited
Port 4	Unlimited	Unlimited
Port 5	Unlimited	Unlimited
Port 6	Unlimited	Unlimited
Port 7	Unlimited	Unlimited
Port 8	Unlimited	Unlimited

Figure 2.3.11 Broadband Control Page

2.3.12 Jumbo frame

Jumbo frames are Ethernet frames with payloads that exceed the 1500-byte limit of the IEEE 802.3 standard.

The minimum setting value of this series of switches is 1522 bytes, and the maximum is 9216 bytes.



The screenshot shows a web interface titled "Jumbo Frame Setting". Inside the panel, there is a label "Jumbo Frame (Bytes)" next to a dropdown menu that currently displays "9216". Below the dropdown is an "Apply" button.

Figure 2.3.12 Jumbo Frame Page

2.3.13 MAC constraint

Learn the overflow action mode: Flooding. The switch forwards frames coming in from a certain interface through other non-receiving interfaces. Flooding is a point-to-multipoint operation (flooding is flooding within a VLAN, and there is isolation between VLANs).

Discard, where the switch discards a frame received from an interface without forwarding it

Effective after application

MAC constraint setting, select the corresponding port and open it, set the limit range (0-2112) as required, and it will take effect after application and saving.

MAC Constraint Action Setting

Learn over Action
Drop

Apply

MAC Constraint Setting

Port	State	Entry Limits
Port 1		
Port 2		
Port 3		
Port 4	Disable	Unlimited (0-4160)
Port 5		
Port 6		

Apply

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 2.3.13 MAC Constraints Page

2. 3. 14 Green Ethernet

The port enters an inactive mode and saves power while keeping the port management state open. Click Open and Apply to take effect.

Green Ethernet Setting

Green Ethernet
Disable

Apply

Figure 2.3.14 Green Ethernet Page

2. 3. 15 EEE

When this function is turned on, the switch will automatically turn off some idle circuits, effectively reducing power consumption and saving energy.

EEE Setting

EEE function
Disable

Apply

Figure 2.3.15 EEE Page

2.4 safe

2.4.1 MAC Addr

2.4.1.1 MAC table

This page shows the access MAC information under the port.

MAC Address Information				
No.	MAC Address	VLAN ID	Type	Port
1	F4:6D:2F:26:6F:13	1	Dynamic	1
2	78:60:5B:3A:F3:5C	1	Dynamic	1
3	04:7C:16:81:21:1C	1	Dynamic	1
4	AC:9E:17:B5:07:20	1	Dynamic	1
5	4C:ED:FB:63:CD:62	1	Dynamic	1
6	00:CF:E0:4F:3B:16	1	Dynamic	1
7	00:E0:4C:0B:BC:4B	1	Dynamic	1
8	F2:FB:97:94:D3:54	1	Dynamic	1
9	4A:C1:C4:DE:B8:8E	1	Dynamic	1
10	0C:9D:92:0E:C8:C1	1	Dynamic	1
11	8A:D0:BB:5E:37:C8	1	Dynamic	1
12	30:5A:3A:83:4A:67	1	Dynamic	1
13	00:CF:E0:49:2F:28	1	Dynamic	1
14	18:5E:0F:1E:6E:6E	1	Dynamic	1

Figure 2.4.1.1 MAC Table Page

2.4.1.2 MAC lookup

Select the MAC address to be queried and the VLAN according to the actual access and query. If the queried MAC is correct, the system will display the corresponding port. An error indicates that it was not found.

MAC Addresses Searching					
<table><tr><th>MAC Address</th><th>VLAN ID</th></tr><tr><td> 00:00:00:00:00:00 </td><td> (1-4094) </td></tr></table>	MAC Address	VLAN ID	00:00:00:00:00:00	(1-4094)	Search
MAC Address	VLAN ID				
00:00:00:00:00:00	(1-4094)				

Figure 2.4.1.2 MAC Lookup Page

2. 4. 1. 3 Static MAC

The static MAC function can be set to bind or block the specified MAC on the specified port and VLAN.

MAC address: controlled MAC address object.

VLAN ID: The VLAN ID of the role (integer between 1-4094).

Port: The active port (when not selected, it is effective for all ports).

Source MAC blocking: controlled mode. If it is checked, the MAC address will be blocked. If it is not checked, the MAC address will be bound.

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	☐

Add

No.	MAC Address	VLAN ID	Port	Source MAC Blocking	Select

Delete

Figure2.4.1.3-1 Static MAC page

For example, as shown in Figure 2.4. 1.3-2, the configuration example binds the MAC address 94: E1: AC: C5: e9: E0 to port 3 and VLAN 1. At this point, the device will not be able to communicate if it is connected to another port or VLAN.

No.	MAC Address	VLAN ID	Port	Select
1	94:E1:AC:C5:E9:E0	1	3	☐

Figure2.4.1.3-2

2.4.2 Broadcast Storm

The storm control function can limit the packet rate of broadcast, multi-cast, unknown unicast and unknown multicast types of the specified port.

Storm type: controlled data packet type, including broadcast, multicast, unknown unicast and unknown multicast.

Port: acting port (multiple choices are allowed).

Status: Specifies whether the type of packet control on the port is on or off.

Speed: Maximum speed (in PPS, packets per second)

Select the corresponding port to select the type and speed to be suppressed. After the state is opened, click Apply to take effect.

Storm Control Setting

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

Apply

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

Figure 2.4.2 Broadcast Storm Page

2.5 Monitor

2.5.1 Port Statistics

Port statistics status shows the management status, link status, and statistics of sent and received packets of the port.

Click the "Clear" button to clear the statistics.

Port Statistics Information						
Port	State	Link Status	TxGoodPkt	TxBadPkt	RxGoodPkt	RxBadPkt
Port 1	Enabled	Link Up	4620	0	66730	776
Port 2	Enabled	Link Down	0	0	0	0
Port 3	Enabled	Link Down	0	0	0	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 2.5.1 Port Statistics Page

2.5.2 Cable Diagnostics

Select the corresponding port to test the cable, and click Apply to take effect.

Cable Diagnostic			
Check	Port	Test Result	Cable Fault Distance
☐	Port 1	-	-
☐	Port 2	-	-
☐	Port 3	-	-
☐	Port 4	-	-
☐	Port 5	-	-
☐	Port 6	-	-
☐	Port 7	-	-
☐	Port 8	-	-

Figure 2.5.2 Cable Diagnostics Page

2.6 tool

2.6.1 Firmware upgrade

Select the required files and upgrade them.

Firmware Upgrade	
Enter loader mode to upgrade firmware. After entering loader mode, configuration will be saved.	
Enter Loader Mode	

Figure 2.6.1 Firmware Upgrade Page

2.6.2 Configure Backup

Back up the current configuration file of the switch. Click Backup to generate a backup configuration file.

Restore the backup configuration file, select the configuration to be restored, and click Upgrade. After the upgrade is successful, restart to take effect.

The screenshot shows two sections of a web interface. The first section, titled "HTTP Backup Configuration", contains a single "Backup" button. The second section, titled "HTTP Restore Configuration", contains a "Select File" button, the text "No file selected", and an "Upload" button.

Figure 2.6.2 Configuration Backup Page

2.6.3 Reset

Restore the switch to the factory default setting state, and click "Restore factory default" to restart the switch to take effect.

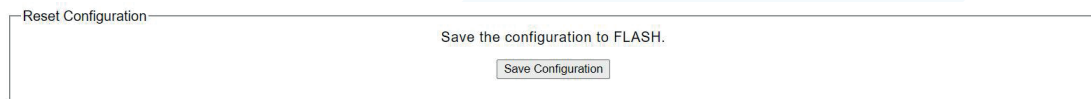
When the web management interface cannot be restored due to configuration errors or other reasons, press and hold the reset key of the switch until all the indicators flash to restore the factory settings.

The screenshot shows a single section titled "Reset Configuration". It contains the text "Reset to default factory settings and restart the system." and a "Factory Default" button.

Figure 2.6.3 Reset Page

2.6.4 save

Save the changes made in the management page. The unsaved configuration will be lost on the next reboot.



Reset Configuration

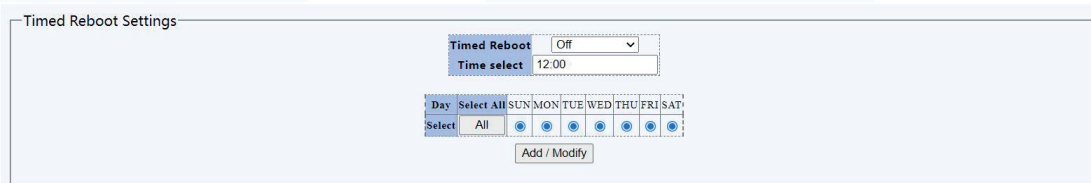
Save the configuration to FLASH.

Save Configuration

Figure 2.6.4 Save Page

2.6.5 Timed restart

Perform scheduled restart configuration operation on the switch as required, select the corresponding time of each week and the corresponding hour of each day, and enable the scheduled restart function to take effect after saving



Timed Reboot Settings

Timed Reboot: Off

Time select: 12:00

Day	Select All	SUN	MON	TUE	WED	THU	FRI	SAT
Select	All	☒	☒	☒	☒	☒	☒	☒

Add / Modify

Figure 2.6.5 Timed Restart Page

2.6.6 Manual Restart

Restart the switch. Click Restart to restart the switch.



Reboot

Reboot the switch.

Reboot

Figure 2.6.6 Manual Restart Page

2.6.7 Logout

Select the logout button to exit the current WEB interface.



Figure 2.6.7 Logoff Page

For more informaion visit our webste:



www.kline.knowledgline.com