EKSELANS BY ITS

USER MANUAL

SWG 24 L2

334200

Switch Ethernet Layer2. 24 ports x GB
Ethernet + 4 x SFP. 1Gbps

V01

ITS Partner O.B.S S.L · Av. Cerdanyola 79-81 Local C
08172 Sant Cugat del Vallés · Barcelona (Spain)
Phone: +34935839543 · info@ek.plus · www.ek.plus

TABLE OF CONTENTS

Introduction.

Description.

Switch Ethernet Layer2. 24 ports x GB Ethernet + 4 x SFP. 1Gbps.

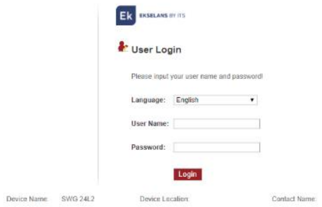
Main characteristics.

- 24 Port 10/100/1000Mbps + 4 SFP port.
- Layer 2+ funtion for an efficient routing.
- Standard IEEE802.3, 802.3u, 802.3ab, 802.3x.
- VLAN management, IGMP snooping, MACs admin, port mirroring.
- Web management interface, SSH, TELNET, SNMP.
- 1U / Rack 19".
- Multi-cast facilities (compnies, hotels, hospitals, SoHo).
- Suitable product to include in GPON by EK, EK CAST, EK HOTEL or Wi-Fi by EK installations.

WEB MANAGEMENT LANDING PAGE.

Log in to the switch management page WEB.

Configuration computer's IP address and the switch must be set to the same subnet (switch default IP address is 192.168.2.10, the default subnet mask of 255.255.255.0). Run WEB browser, in the address bar enter http://192.168.2.10. Enter, enter the user name and password (default user name:admin; password:admin), click "Login" button or directly enter into the WEB management.



User Login

Please input your user name and password!

Language: English ▾

User Name:

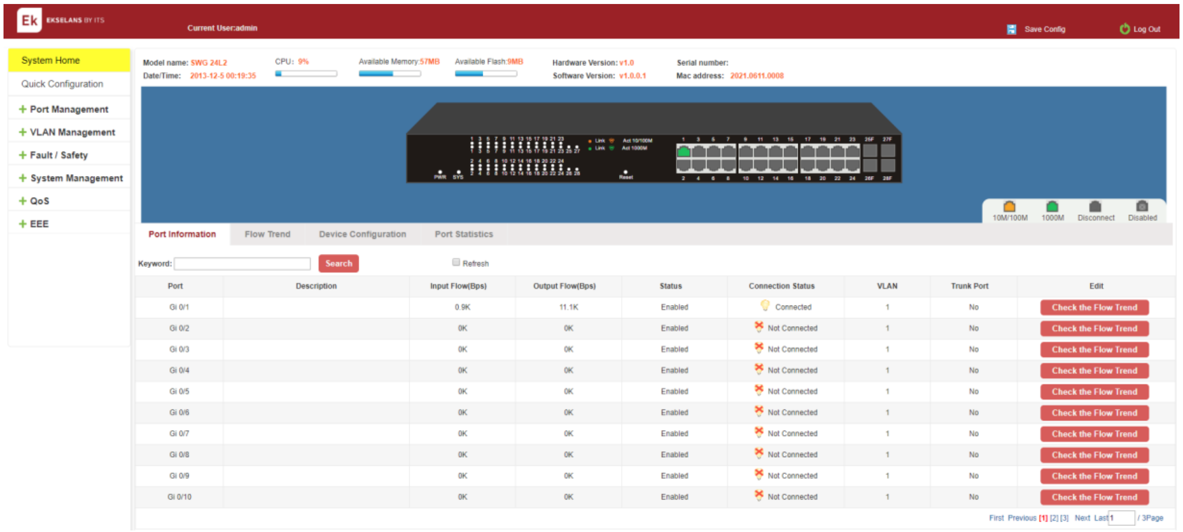
Password:

Login

Device Name: SWG 24L2 | Device Location: | Contact Name:

Figure 1-1: The login page WEB.

After landing successfully, the switch management page WEB page:



Current User:admin

Model name: SWG 24L2
Date/Time: 2013-12-5 00:19:35
CPU: 9%
Available Memory:57MB
Available Flash:9MB
Hardware Version: v1.0
Software Version: v1.0.0.1
Serial number:
Mac address: 2021.0611.0008

Keyword:

Port	Description	Input Flow(Bps)	Output Flow(Bps)	Status	Connection Status	VLAN	Trunk Port	Edit
Gi 0/1		0.9K	11.1K	Enabled	Connected	1	No	Check the Flow Trend
Gi 0/2		0K	0K	Enabled	✗ Not Connected	1	No	Check the Flow Trend
Gi 0/3		0K	0K	Enabled	✗ Not Connected	1	No	Check the Flow Trend
Gi 0/4		0K	0K	Enabled	✗ Not Connected	1	No	Check the Flow Trend
Gi 0/5		0K	0K	Enabled	✗ Not Connected	1	No	Check the Flow Trend
Gi 0/6		0K	0K	Enabled	✗ Not Connected	1	No	Check the Flow Trend
Gi 0/7		0K	0K	Enabled	✗ Not Connected	1	No	Check the Flow Trend
Gi 0/8		0K	0K	Enabled	✗ Not Connected	1	No	Check the Flow Trend
Gi 0/9		0K	0K	Enabled	✗ Not Connected	1	No	Check the Flow Trend
Gi 0/10		0K	0K	Enabled	✗ Not Connected	1	No	Check the Flow Trend

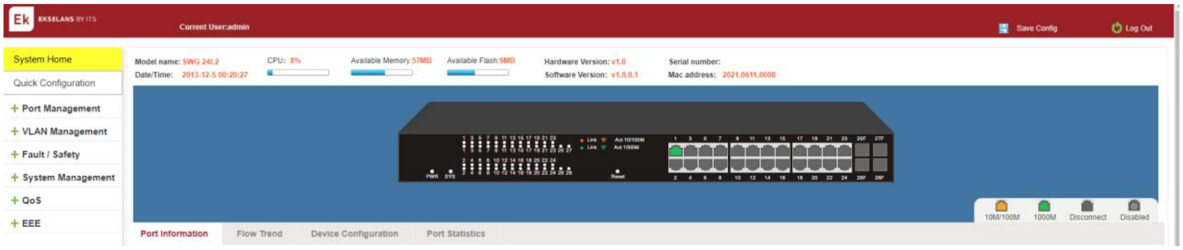
First Previous [1] [2] [3] Next Last 1 / 3Page

Figure 1-2: switch WEB management page Home.

System home.

Device panel.

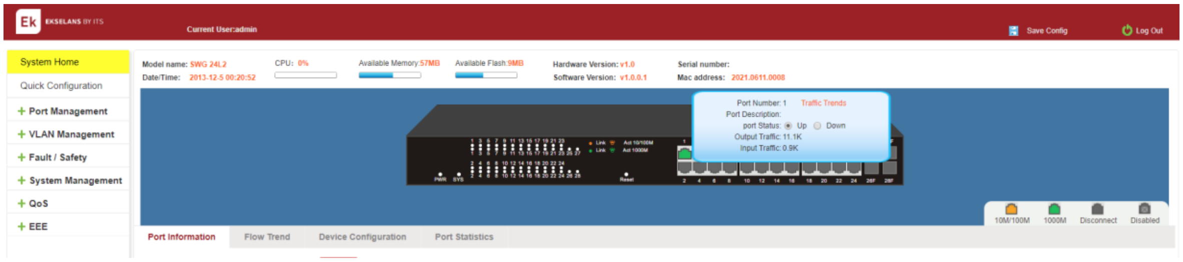
Through the HTTP page, a quick understanding of the operation of the device, panel information, port information, such as the general network of common management information.



Model name: SWG 24L2
Date/Time: 2013-12-5 00:20:27
CPU: 8%
Available Memory:57MB
Available Flash:9MB
Hardware Version: v1.0
Software Version: v1.0.0.1
Serial number:
Mac address: 2021.0611.0008

Figure 2-1: Device Panel.

Click on the specific port, you can see the following information.



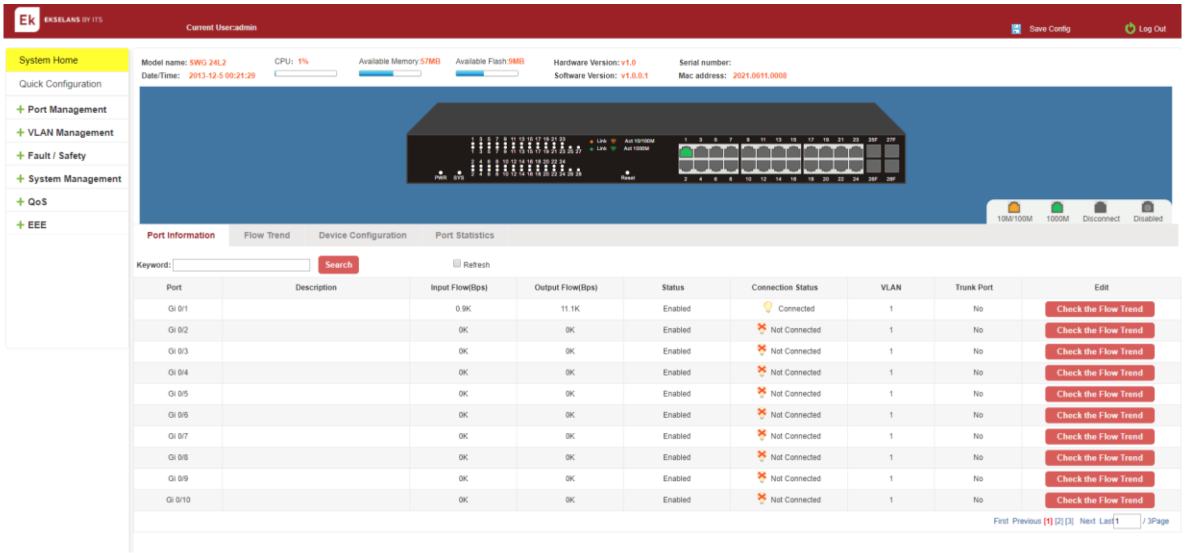
Model name: SWG 24L2
Date/Time: 2013-12-5 00:20:52
CPU: 0%
Available Memory:57MB
Available Flash:9MB
Hardware Version: v1.0
Software Version: v1.0.0.1
Serial number:
Mac address: 2021.0611.0008

Port Number: 1
Port Description:
port Status: ● Up ○ Down
Output Traffic: 11.1K
Input Traffic: 0.9K

Figure 2-2: View the port status.

Port information.

The configuration of the SWG 24L2-10P is as follows: "System Home", "Port Information".



Current User:admin

Model name: SWG 24L2
Date/Time: 2013-12-5 00:21:29
CPU: 1%
Available Memory:57MB
Available Flash:9MB
Hardware Version: v1.0
Software Version: v1.0.0.1
Serial number:
Mac address: 2021.0611.0008

Keyword:
□ Refresh

Port	Description	Input Flow(Bps)	Output Flow(Bps)	Status	Connection Status	VLAN	Trunk Port	Edit
Gi 0/1		0.9K	11.1K	Enabled	Connected	1	No	Check the Flow Trend
Gi 0/2		0K	0K	Enabled	✗ Not Connected	1	No	Check the Flow Trend
Gi 0/3		0K	0K	Enabled	✗ Not Connected	1	No	Check the Flow Trend
Gi 0/4		0K	0K	Enabled	✗ Not Connected	1	No	Check the Flow Trend
Gi 0/5		0K	0K	Enabled	✗ Not Connected	1	No	Check the Flow Trend
Gi 0/6		0K	0K	Enabled	✗ Not Connected	1	No	Check the Flow Trend
Gi 0/7		0K	0K	Enabled	✗ Not Connected	1	No	Check the Flow Trend
Gi 0/8		0K	0K	Enabled	✗ Not Connected	1	No	Check the Flow Trend
Gi 0/9		0K	0K	Enabled	✗ Not Connected	1	No	Check the Flow Trend
Gi 0/10		0K	0K	Enabled	✗ Not Connected	1	No	Check the Flow Trend

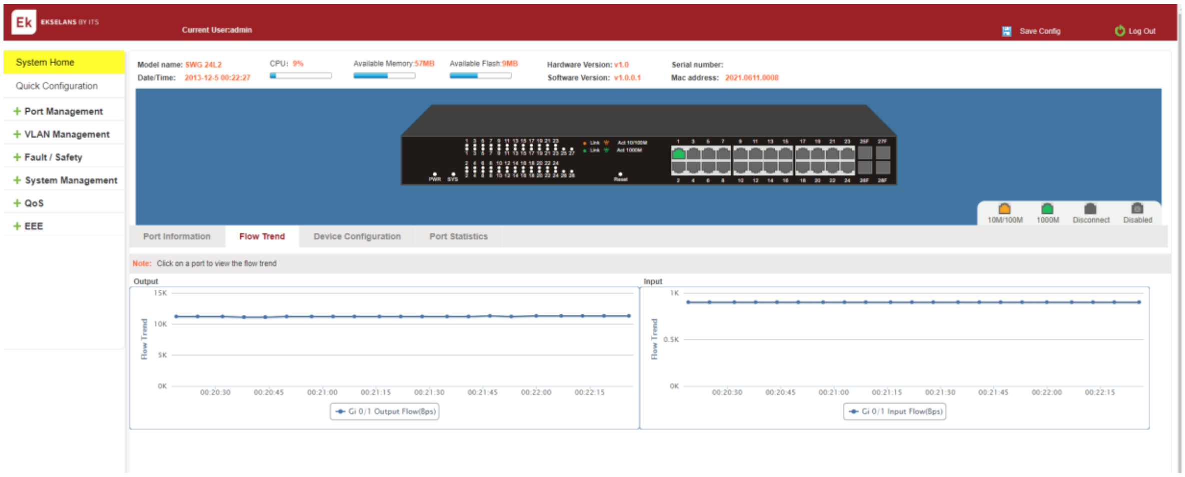
First Previous [1] [2] [3] Next Last 1 / 3Page

Figure 2-3: Port Information.

On the panel you seen the device port, description, input flow, output flow, state of the port, connection state, the VLAN, whether trunk.

Flow trend.

Use the mouse to click the device port on the panel port, can view the port Flow trends.



Current User:admin

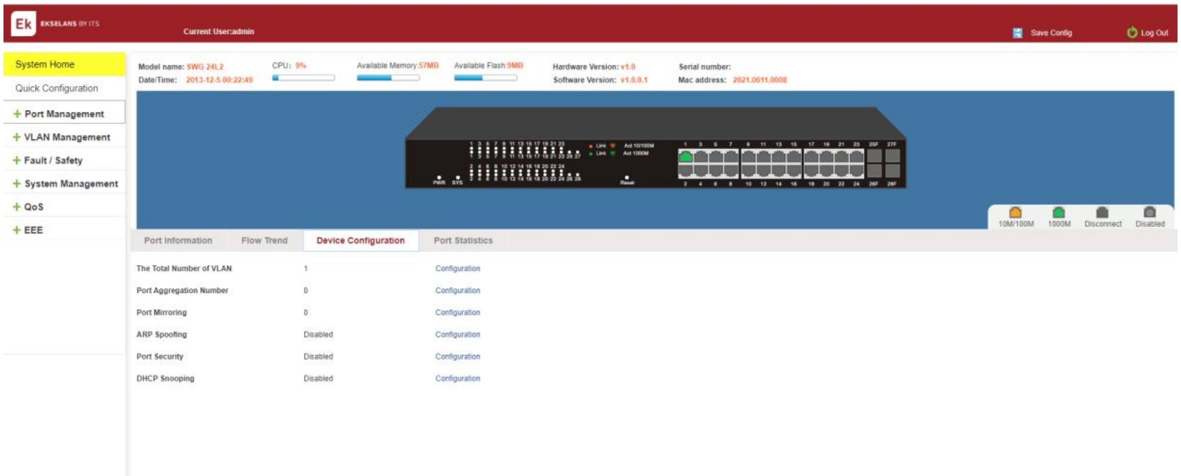
Model name: SWG 24L2
Date/Time: 2013-12-5 00:22:27
CPU: 9%
Available Memory:57MB
Available Flash:9MB
Hardware Version: v1.0
Software Version: v1.0.0.1
Serial number:
Mac address: 2021.0611.0008

Note: Click on a port to view the flow trend

Figure 2-4 View the Flow Trend.

Device configuration.

With the HTTP page, click “Device Configuration” to view and change the configuration of the device.



Current User:admin

Model name: SWG 24L2
Date/Time: 2013-12-5 00:22:49
CPU: 9%
Available Memory:57MB
Available Flash:9MB
Hardware Version: v1.0
Software Version: v1.0.0.1
Serial number:
Mac address: 2021.0611.0008

The Total Number of VLAN	1	Configuration
Port Aggregation Number	0	Configuration
Port Mirroring	0	Configuration
ARP Spoofing	Disabled	Configuration
Port Security	Disabled	Configuration
DHCP Snooping	Disabled	Configuration

Figure 2-5: Device Configuration.

“Device configuration” can quickly configure the following modules:

1 Total number of VLAN.

2 Port Aggregation Number.

3 Port Mirroring.

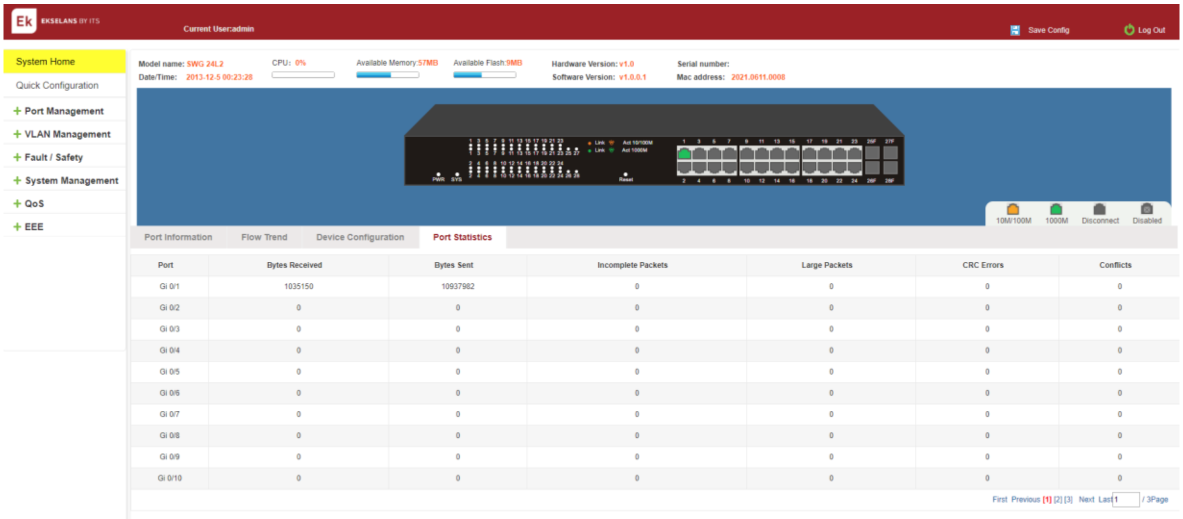
4 ARP Spoofing.

5 Port Security.

6 DHCP Snooping.

Port statistics.

Through the HTTP page, the user can quickly understand the number of bytes received, the number of bytes sent, the number of incomplete packets, the number of large packets, CRC error packets, the number of conflicts.



Model name: SWG 24L2
Date/Time: 2013-12-5 00:23:28
CPU: 0%
Available Memory:57MB
Available Flash:9MB
Hardware Version: v1.0
Software Version: v1.0.0.1
Serial number:
Mac address: 2021.0611.0008

Port	Bytes Received	Bytes Sent	Incomplete Packets	Large Packets	CRC Errors	Conflicts
Gi 0/1	1035150	10937982	0	0	0	0
Gi 0/2	0	0	0	0	0	0
Gi 0/3	0	0	0	0	0	0
Gi 0/4	0	0	0	0	0	0
Gi 0/5	0	0	0	0	0	0
Gi 0/6	0	0	0	0	0	0
Gi 0/7	0	0	0	0	0	0
Gi 0/8	0	0	0	0	0	0
Gi 0/9	0	0	0	0	0	0
Gi 0/10	0	0	0	0	0	0

First Previous [1] [2] [3] Next Last 1 / 3Page

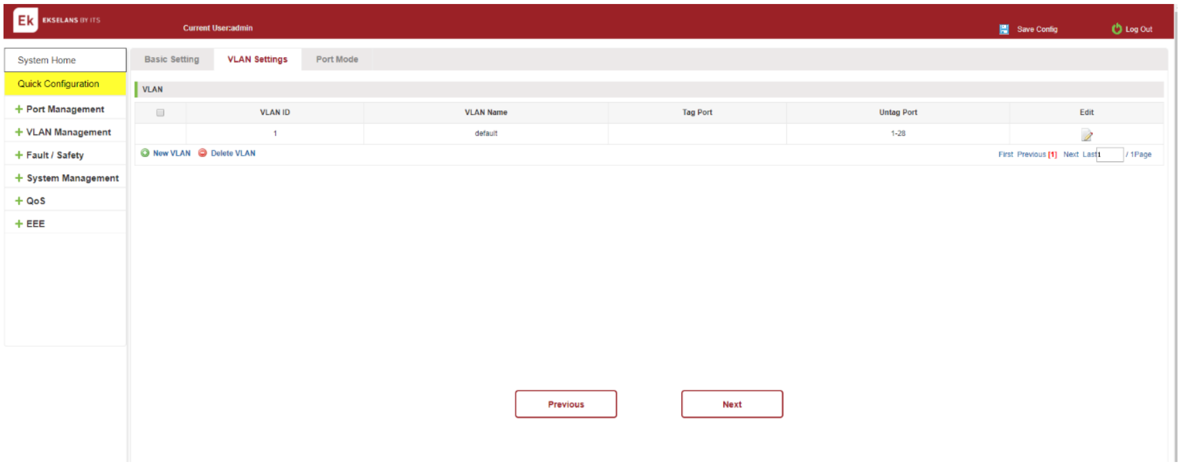
Figure 2-6: View the port Statistics.

Quick configuration.

The quick configuration contains five chapters. Click on "Quick Configuration", can quickly to Configuration of the device commonly used functions, such as a VLAN, Trunk port and others. According to the steps, the configurations of step by step, also can choose configuration.

VLAN setting.

Click on "Quick Configuration" "VLAN Settings" into the Quick Configuration of VLAN Configuration page. Can view the current equipment VLAN information, according to the demand of new VLAN, modify VLAN, delete VLAN, etc.

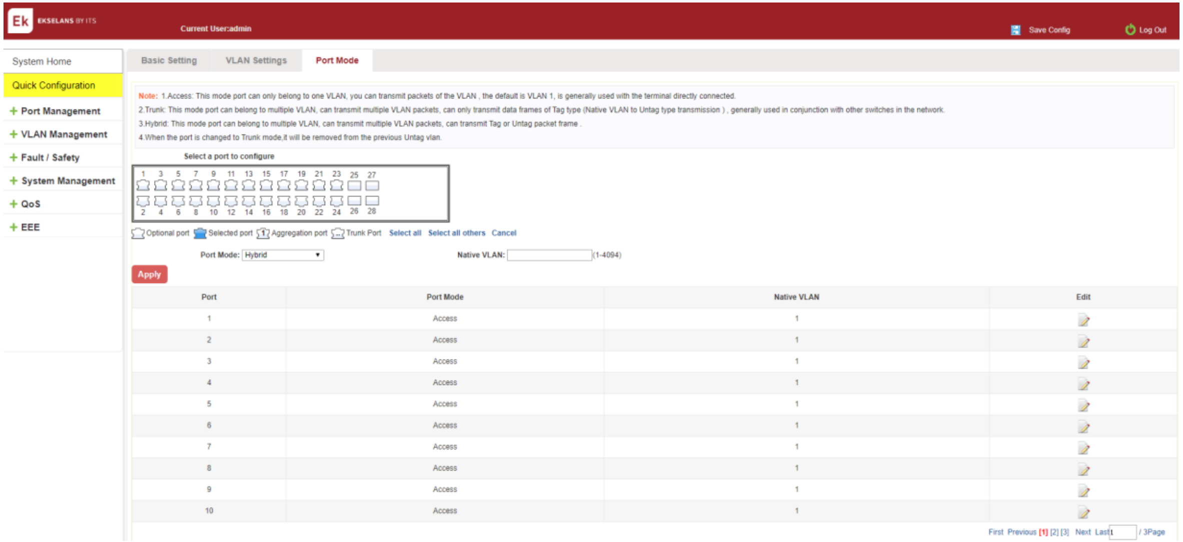


□	VLAN ID	VLAN Name	Tag Port	Untag Port	Edit
	1	default		1-28	✎

Figure 3-1: VLAN Setting.

PORT MODE.

Click on "Quick Configuration" "Port Mode" into the port mode configuration settings page. You can change the port mode and allowed some vlans on trunk or hybrid mode, notice:When the port is changed to trunk mode,it will be removed from the previous untag vlan.



Note: 1.Access: This mode port can only belong to one VLAN, you can transmit packets of the VLAN , the default is VLAN 1, is generally used with the terminal directly connected.
2.Trunk: This mode port can belong to multiple VLAN, can transmit multiple VLAN packets, can only transmit data frames of Tag type (Native VLAN to Untag type transmission) , generally used in conjunction with other switches in the network.
3.Hybrid: This mode port can belong to multiple VLAN, can transmit multiple VLAN packets, can transmit Tag or Untag packet frame .
4.When the port is changed to Trunk mode,it will be removed from the previous Untag vlan.

Port Mode: Hybrid   Native VLAN: (1-4094)

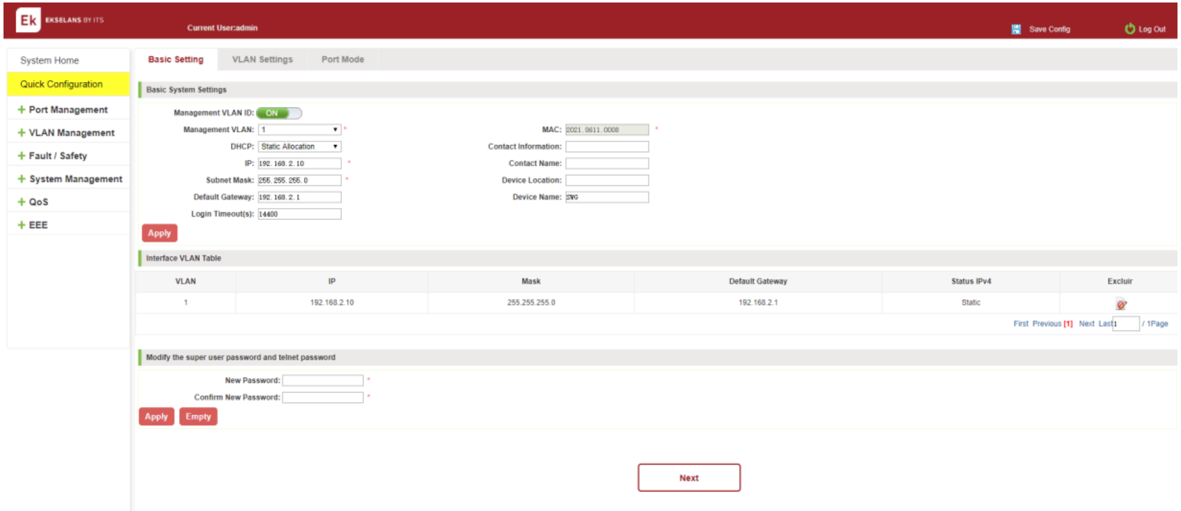
Port	Port Mode	Native VLAN	Edit
1	Access	1	✎
2	Access	1	✎
3	Access	1	✎
4	Access	1	✎
5	Access	1	✎
6	Access	1	✎
7	Access	1	✎
8	Access	1	✎
9	Access	1	✎
10	Access	1	✎

First Previous [1] [2] [3] Next Last 1 / 3Page

Figure 3-2: Trunk Port Setting.

BASIC SETTING.

Click "Quick Configuration" "Basic Setting" into the quick Configuration of equipment information system Settings page. Can the current equipment basic information system and manage password configured.



Basic System Settings

Management VLAN ID: ON
Management VLAN: 1 *
DHCP: Static Allocation
IP: 192. 168. 2. 10 *
Subnet Mask: 255. 255. 255. 0 *
Default Gateway: 192. 168. 2. 1
Login Timeout(s): 14400
MAC: 2021. 0611. 0008 *
Contact Information:
Contact Name:
Device Location:
Device Name: SWG

Interface VLAN Table

VLAN	IP	Mask	Default Gateway	Status IPv4	Excluir
1	192.168.2.10	255.255.255.0	192.168.2.1	Static	✎

First Previous [1] Next Last 1 / 1Page

Modify the super user password and telnet password

New Password: *
Confirm New Password: *

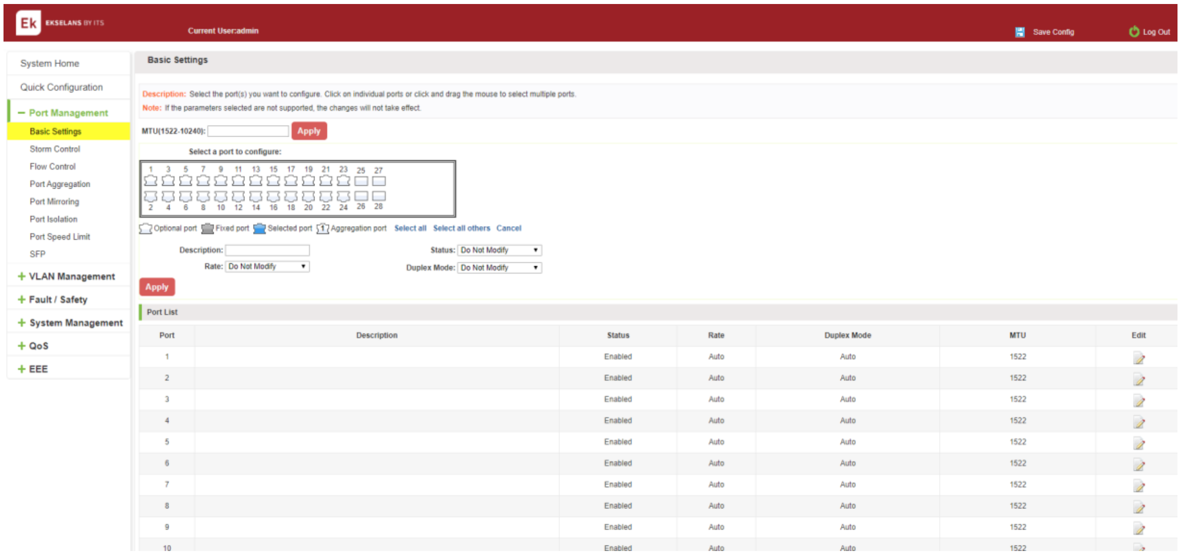
Figure 3-3: other settings.

Port Management.

Basic Settings.

Check the port configuration.

Click on the navigation bar "Port Management" "Basic Settings" to view the current configuration of the switch ports:



Description: Select the port(s) you want to configure. Click on individual ports or click and drag the mouse to select multiple ports.
Note: If the parameters selected are not supported, the changes will not take effect.

MTU(1522-10240):

Description:
Rate: Do Not Modify
Status: Do Not Modify
Duplex Mode: Do Not Modify

Port	Description	Status	Rate	Duplex Mode	MTU	Edit
1		Enabled	Auto	Auto	1522	✎
2		Enabled	Auto	Auto	1522	✎
3		Enabled	Auto	Auto	1522	✎
4		Enabled	Auto	Auto	1522	✎
5		Enabled	Auto	Auto	1522	✎
6		Enabled	Auto	Auto	1522	✎
7		Enabled	Auto	Auto	1522	✎
8		Enabled	Auto	Auto	1522	✎
9		Enabled	Auto	Auto	1522	✎
10		Enabled	Auto	Auto	1522	✎

Figure 4-1: Port list information.

In the port list attribute, which shows the current switch port configuration information:

1 Port: The number of the port.

2 Port Description: Displays the contents of the switch port description.

3 Port Status: switch port status information, on / off.

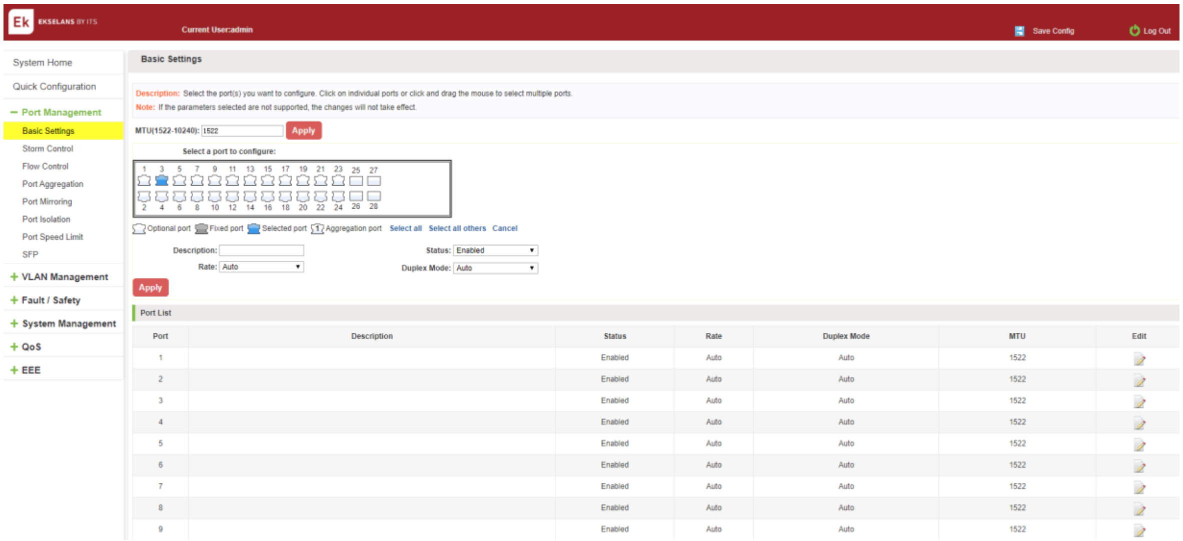
4 Port Rate: Displays the switch port speed configuration, auto-negotiation / 10/100/1000.

5 Working Mode: Displays the switch port configuration duplex, auto-negotiation / full / half duplex.

6 MTU: Indicates the port is the maximum length of the packet.

Configuring Port Properties.

After the icon, you can configure the selected port attributes:



Basic Settings

Description: Select the port(s) you want to configure. Click on individual ports or click and drag the mouse to select multiple ports.

Note: If the parameters selected are not supported, the changes will not take effect.

MTU(1522-10240): 1522

Select a port to configure:

Description:

Status: Enabled

Rate: Auto

Duplex Mode: Auto

Port List

Port	Description	Status	Rate	Duplex Mode	MTU	Edit
1		Enabled	Auto	Auto	1522	✎
2		Enabled	Auto	Auto	1522	✎
3		Enabled	Auto	Auto	1522	✎
4		Enabled	Auto	Auto	1522	✎
5		Enabled	Auto	Auto	1522	✎
6		Enabled	Auto	Auto	1522	✎
7		Enabled	Auto	Auto	1522	✎
8		Enabled	Auto	Auto	1522	✎
9		Enabled	Auto	Auto	1522	✎

Figure 4-2: Port Properties configuration of FIG.

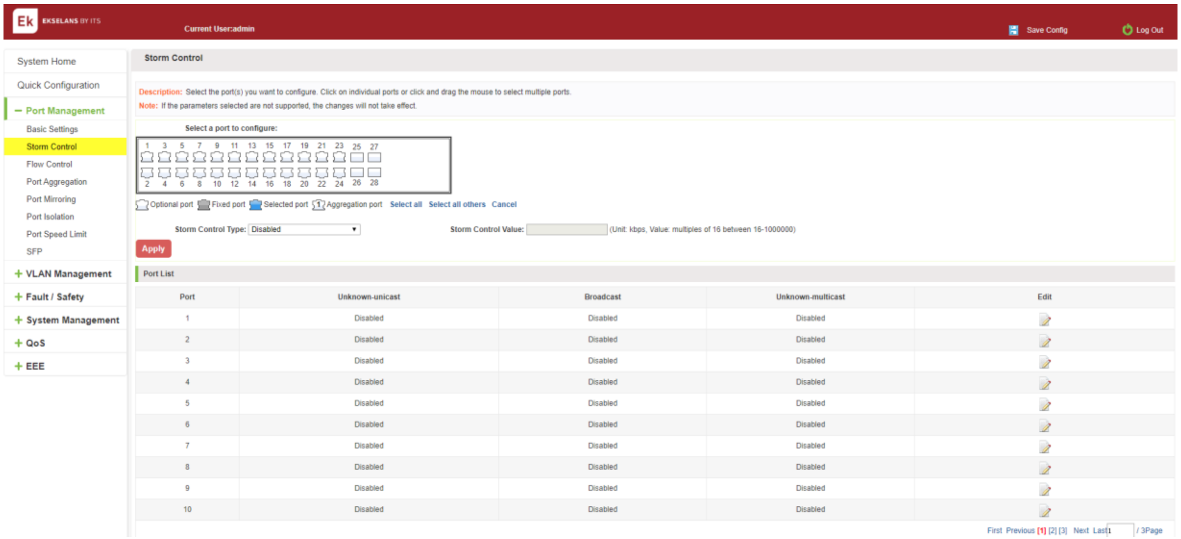
To configure port properties as follows:

Step1: Click the "Edit" icon ✎ ,step2: In the Port Properties configuration page Fill / select the value to be configured, step3: Click the "Apply" button to complete the configuration.

Storm Control.

Check the port settings Storm.

Click on the navigation bar "Port Management" "Storm Control" to view the current switch port storm control information:



Description: Select the port(s) you want to configure. Click on individual ports or click and drag the mouse to select multiple ports.
Note: If the parameters selected are not supported, the changes will not take effect.

Select a port to configure:

Storm Control Type: Disabled

Storm Control Value: (Unit: kbps, Value: multiples of 16 between 16-1000000)

Port List

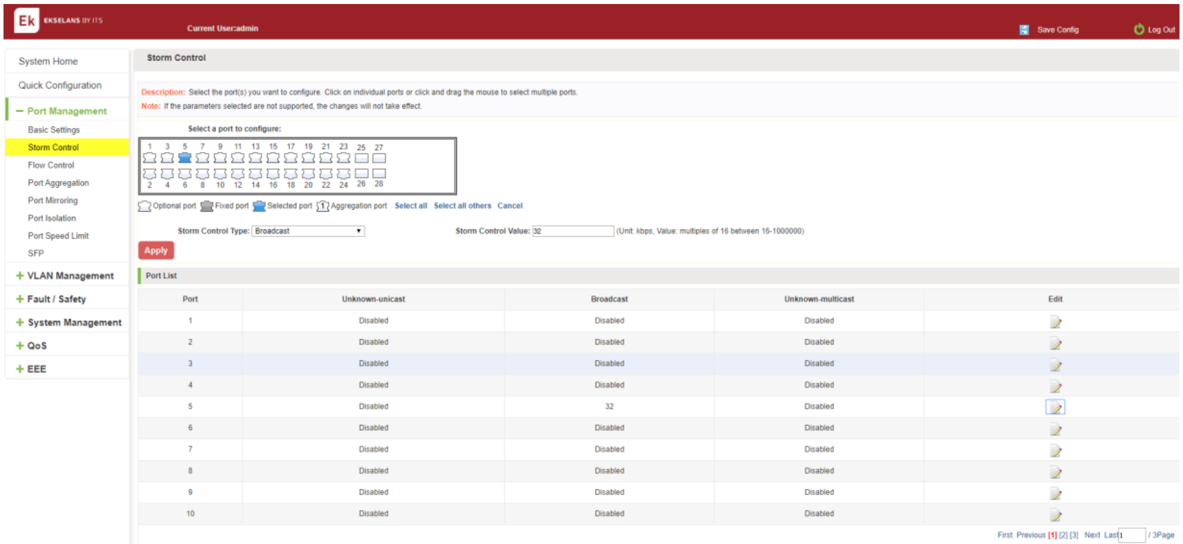
Port	Unknown-unicast	Broadcast	Unknown-multicast	Edit
1	Disabled	Disabled	Disabled	✎
2	Disabled	Disabled	Disabled	✎
3	Disabled	Disabled	Disabled	✎
4	Disabled	Disabled	Disabled	✎
5	Disabled	Disabled	Disabled	✎
6	Disabled	Disabled	Disabled	✎
7	Disabled	Disabled	Disabled	✎
8	Disabled	Disabled	Disabled	✎
9	Disabled	Disabled	Disabled	✎
10	Disabled	Disabled	Disabled	✎

Figure 4-3: Storm Control List information.

In the list of ports which shows the property values of the current storm control switch:

1. Port: The number of the port.
2. Unicast: unknown unicast packets control.
3. Broadcast: Broadcast packet control.
4. Multicast: multicast packets control prompt.
5. When set the control value is not a multiple of 16, the system automatically matches similar multiples of 16.
6. Control value unicast, broadcast, multicast, while only a single value for the control.

By clicking on the port panel " " corresponding port" , select the port to be controlled.



EKSELANS BY ITS Current User:admin Save Config Log Out

Storm Control

Description: Select the port(s) you want to configure. Click on individual ports or click and drag the mouse to select multiple ports.
Note: If the parameters selected are not supported, the changes will not take effect.

Select a port to configure:

1 3 5 7 9 11 13 15 17 19 21 23 25 27
2 4 6 8 10 12 14 16 18 20 22 24 26 28
Optional port Fixed port Selected port Aggregation port Select all Select all others Cancel

Storm Control Type: Broadcast   Storm Control Value: 32 (Unit: kbps, Value: multiples of 16 between 16-1000000)

Apply

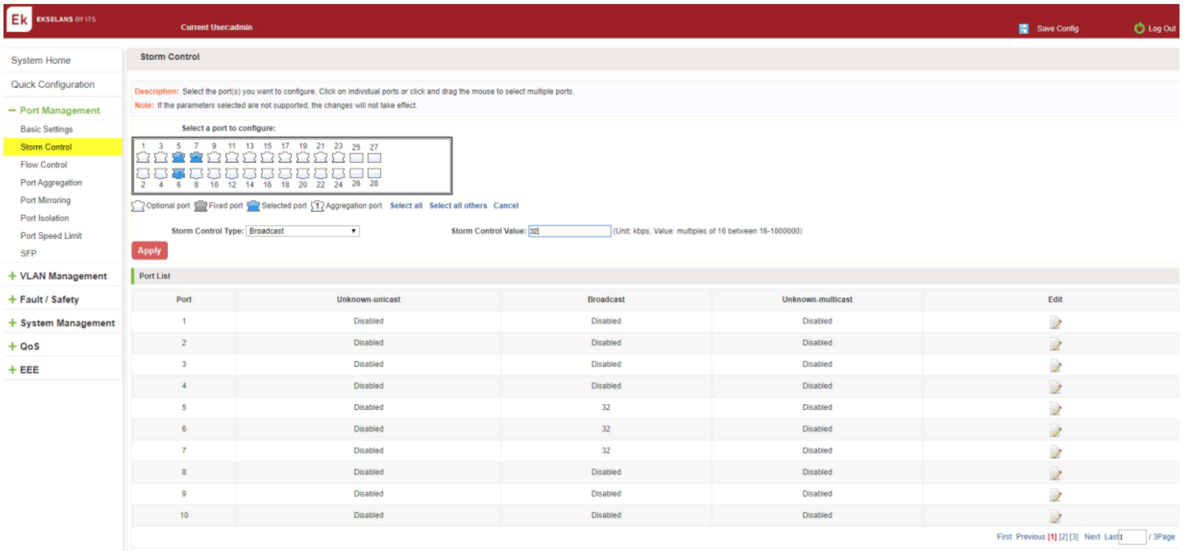
Port List

Port	Unknown-unicast	Broadcast	Unknown-multicast	Edit
1	Disabled	Disabled	Disabled	✎
2	Disabled	Disabled	Disabled	✎
3	Disabled	Disabled	Disabled	✎
4	Disabled	Disabled	Disabled	✎
5	Disabled	32	Disabled	✎
6	Disabled	Disabled	Disabled	✎
7	Disabled	Disabled	Disabled	✎
8	Disabled	Disabled	Disabled	✎
9	Disabled	Disabled	Disabled	✎
10	Disabled	Disabled	Disabled	✎

First Previous [1] [2] [3] Next Last 1 / 3Page

Figure 4-3: Configuring Storm Control information.

After You can also select multiple ports, and batch editing.



EKSELANS BY ITS Current User:admin Save Config Log Out

Storm Control

Description: Select the port(s) you want to configure. Click on individual ports or click and drag the mouse to select multiple ports.
Note: If the parameters selected are not supported, the changes will not take effect.

Select a port to configure:

1 3 5 7 9 11 13 15 17 19 21 23 25 27
2 4 6 8 10 12 14 16 18 20 22 24 26 28
Optional port Fixed port Selected port Aggregation port Select all Select all others Cancel

Storm Control Type: Broadcast   Storm Control Value: 32 (Unit: kbps, Value: multiples of 16 between 16-1000000)

Apply

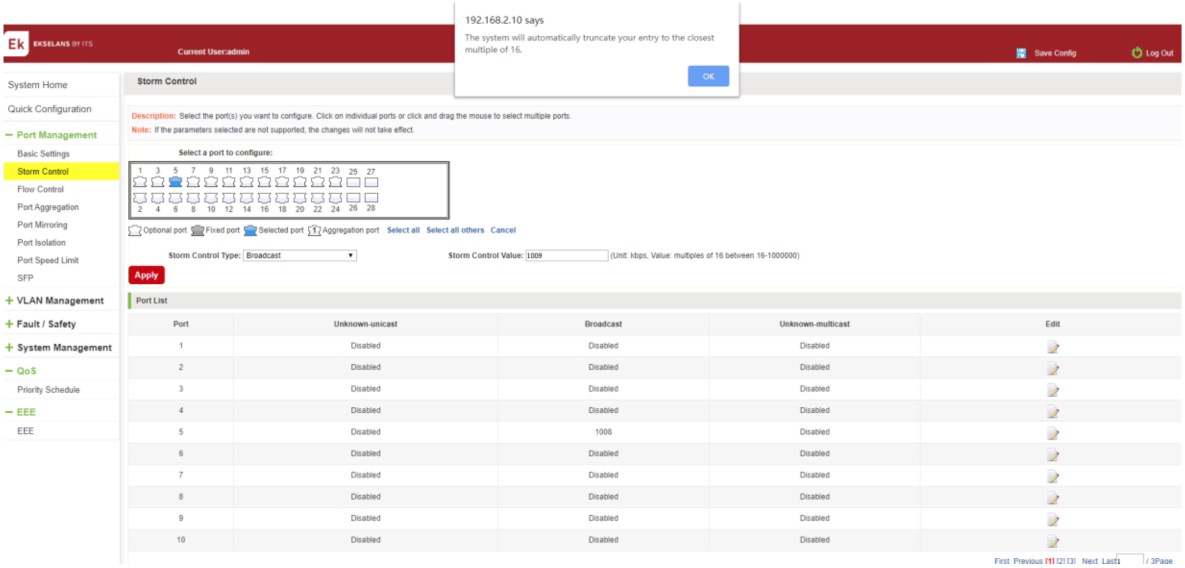
Port List

Port	Unknown-unicast	Broadcast	Unknown-multicast	Edit
1	Disabled	Disabled	Disabled	✎
2	Disabled	Disabled	Disabled	✎
3	Disabled	Disabled	Disabled	✎
4	Disabled	Disabled	Disabled	✎
5	Disabled	32	Disabled	✎
6	Disabled	32	Disabled	✎
7	Disabled	32	Disabled	✎
8	Disabled	Disabled	Disabled	✎
9	Disabled	Disabled	Disabled	✎
10	Disabled	Disabled	Disabled	✎

First Previous [1] [2] [3] Next Last 1 / 3Page

Figure 4-4: Bulk edit configuration information.

After the selected ports in the Storm Control category, set the unicast, multicast, broadcast value, such as setting the port number 1 unicast storm control is 1009. Click Apply Settings.



192.168.2.10 says

The system will automatically truncate your entry to the closest multiple of 16.

Description: Select the port(s) you want to configure. Click on individual ports or click and drag the mouse to select multiple ports.

Note: If the parameters selected are not supported, the changes will not take effect.

Storm Control Type: Broadcast

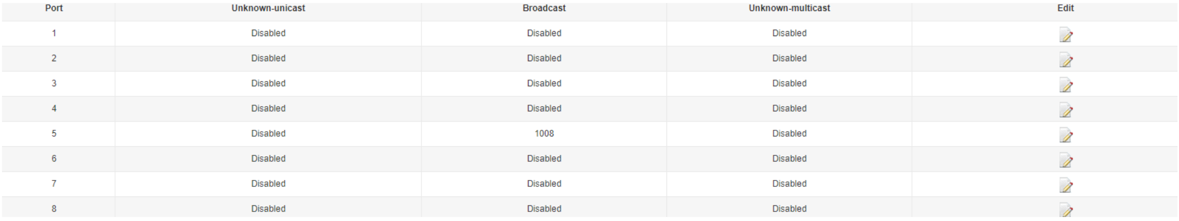
Storm Control Value: 1009 (Unit: kbps, Value: multiples of 16 between 16-1000000)

Port	Unknown-unicast	Broadcast	Unknown-multicast	Edit
1	Disabled	Disabled	Disabled	✎
2	Disabled	Disabled	Disabled	✎
3	Disabled	Disabled	Disabled	✎
4	Disabled	Disabled	Disabled	✎
5	Disabled	1008	Disabled	✎
6	Disabled	Disabled	Disabled	✎
7	Disabled	Disabled	Disabled	✎
8	Disabled	Disabled	Disabled	✎
9	Disabled	Disabled	Disabled	✎
10	Disabled	Disabled	Disabled	✎

First Previous [1] [2] [3] Next Last 1 / 3Page

Figure 4-5: Configuring Storm Control information.

After the configuration, as shown below:

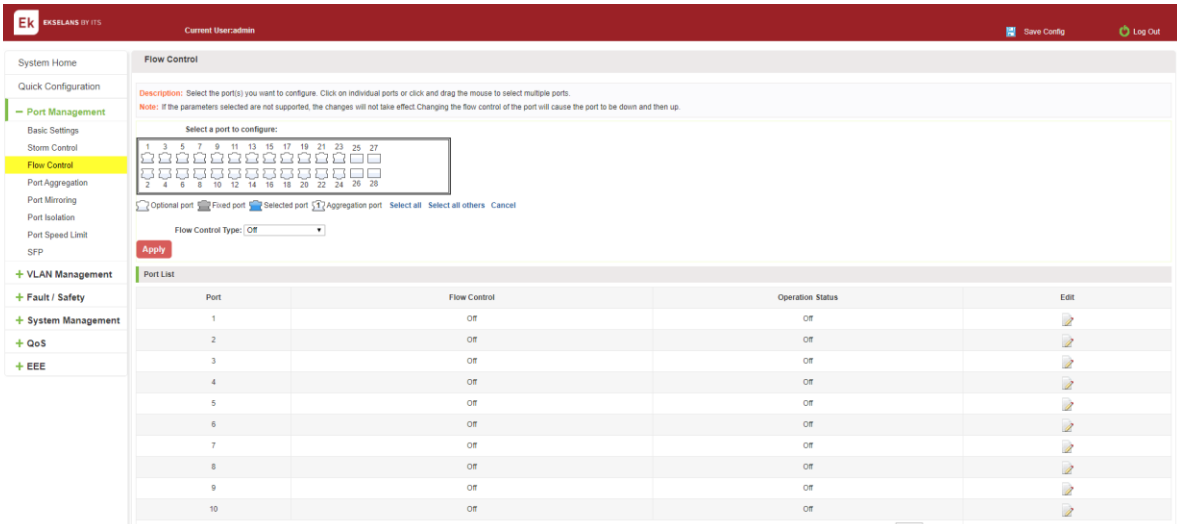


Port	Unknown-unicast	Broadcast	Unknown-multicast	Edit
1	Disabled	Disabled	Disabled	✎
2	Disabled	Disabled	Disabled	✎
3	Disabled	Disabled	Disabled	✎
4	Disabled	Disabled	Disabled	✎
5	Disabled	1008	Disabled	✎
6	Disabled	Disabled	Disabled	✎
7	Disabled	Disabled	Disabled	✎
8	Disabled	Disabled	Disabled	✎

Figure 4-6: Configuration successfully Storm Control information flow control.

FLOW CONTROL.

Click "Port Management" "Flow Control" view of the switch:



Flow Control

Description: Select the port(s) you want to configure. Click on individual ports or click and drag the mouse to select multiple ports.
Note: If the parameters selected are not supported, the changes will not take effect.Changing the flow control of the port will cause the port to be down and then up.

Select a port to configure:

Flow Control Type: Off

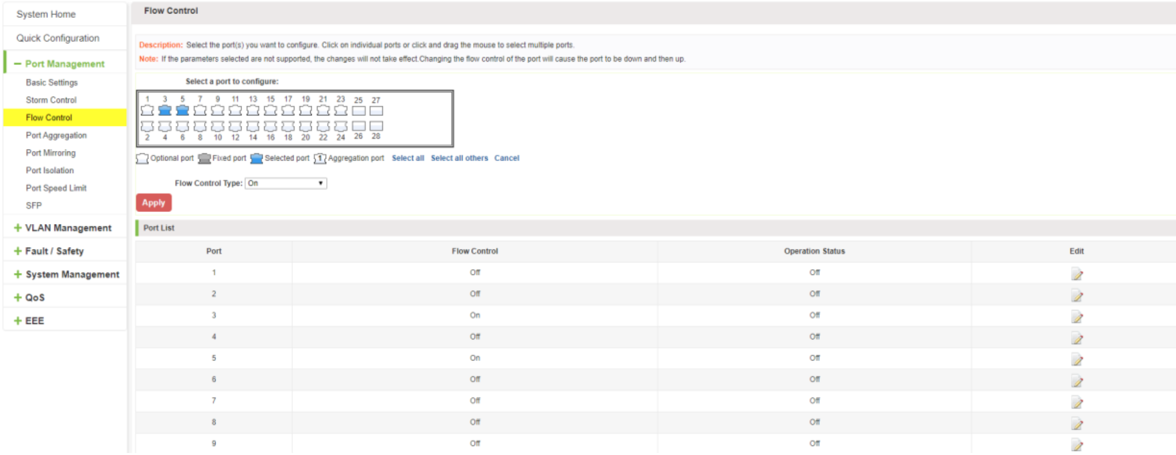
Port List

Port	Flow Control	Operation Status	Edit
1	Off	Off	
2	Off	Off	
3	Off	Off	
4	Off	Off	
5	Off	Off	
6	Off	Off	
7	Off	Off	
8	Off	Off	
9	Off	Off	
10	Off	Off	

Figure 4-7: Flow Control Information.

Configuring Flow Control.

Open port flow control function: select to open port traffic control, click the "Flow control type" Select "On", "Apply":



Flow Control

Description: Select the port(s) you want to configure. Click on individual ports or click and drag the mouse to select multiple ports.
Note: If the parameters selected are not supported, the changes will not take effect.Changing the flow control of the port will cause the port to be down and then up.

Select a port to configure:

Flow Control Type: On

Port List

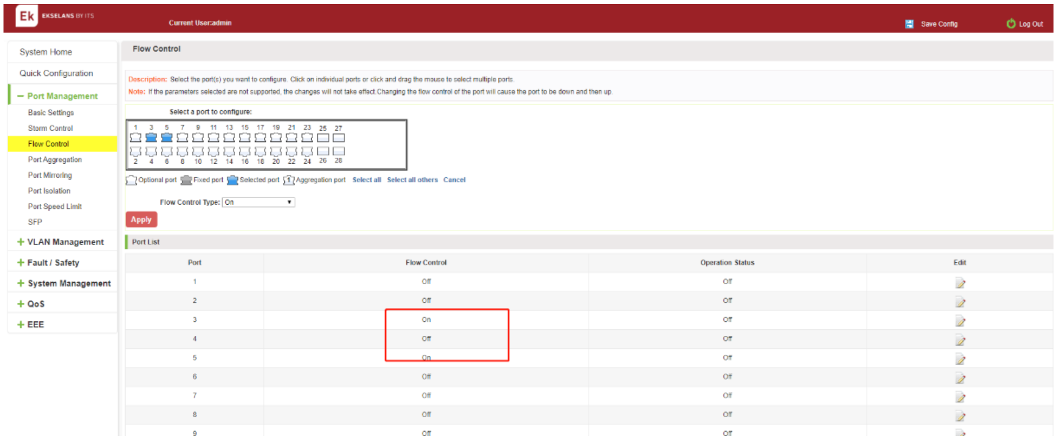
Port	Flow Control	Operation Status	Edit
1	Off	Off	
2	Off	Off	
3	On	Off	
4	Off	Off	
5	On	Off	
6	Off	Off	
7	Off	Off	
8	Off	Off	
9	Off	Off	

Figure 4-8: Open port flow control function.

Open port traffic control, follow these steps:

Step1: Select Open port traffic control; step2: Select Open in "Flow control type" on; step3: Click "Apply".

View Configuration list to display configuration is successful:



Flow Control

Description: Select the port(s) you want to configure. Click on individual ports or click and drag the mouse to select multiple ports.

Note: If the parameters selected are not supported, the changes will not take effect.Changing the flow control of the port will cause the port to be down and then up.

Select a port to configure:

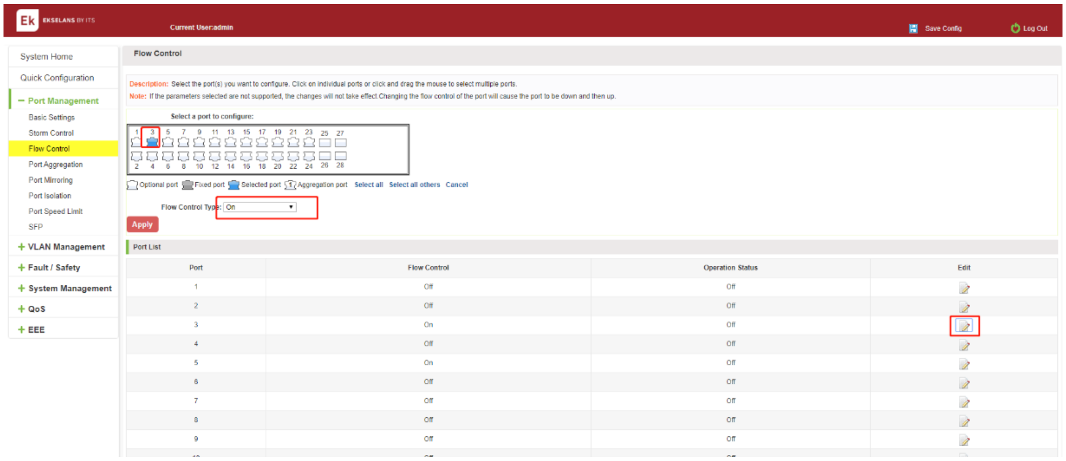
Flow Control Type: On

Port List

Port	Flow Control	Operation Status	Edit
1	Off	Off	✎
2	Off	Off	✎
3	On	Off	✎
4	Off	Off	✎
5	On	Off	✎
6	Off	Off	✎
7	Off	Off	✎
8	Off	Off	✎
9	Off	Off	✎

Figure 4-9: Port flow control status.

Modify the port flow control function: Click on port traffic control list corresponding to the rear port of the " ✎ " button in the Port Settings page "Flow control type" select "Off", "Apply Settings":



Flow Control

Description: Select the port(s) you want to configure. Click on individual ports or click and drag the mouse to select multiple ports.

Note: If the parameters selected are not supported, the changes will not take effect.Changing the flow control of the port will cause the port to be down and then up.

Select a port to configure:

Flow Control Type: On

Port List

Port	Flow Control	Operation Status	Edit
1	Off	Off	✎
2	Off	Off	✎
3	On	Off	✎
4	Off	Off	✎
5	On	Off	✎
6	Off	Off	✎
7	Off	Off	✎
8	Off	Off	✎
9	Off	Off	✎

Figure 4-10: Close the port flow control.

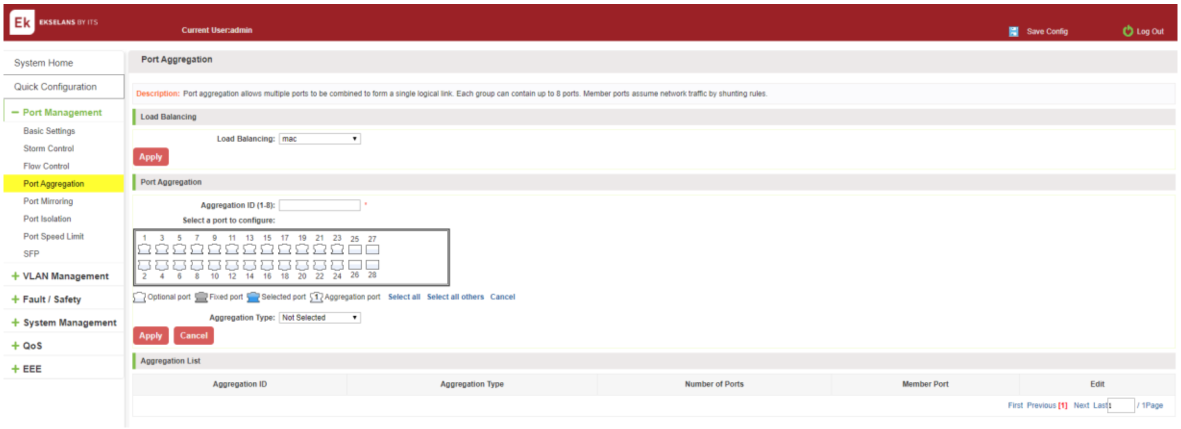
Close port traffic control, follow these steps:

Step1: Select the button to the right of the port or directly selected port; step2: In the "Flow control type" select Off; step3: Click "Apply".

Port Aggregation.

Viewing Port Aggregation Configuration.

Click "Port Management" "Port Aggregation" to view the current switch configured port aggregation information:



Port Aggregation

Description: Port aggregation allows multiple ports to be combined to form a single logical link. Each group can contain up to 8 ports. Member ports assume network traffic by shunting rules.

Load Balancing

Load Balancing: mac

Port Aggregation

Aggregation ID (1-8): *

Select a port to configure:

Aggregation Type: Not Selected

Aggregation List

Aggregation ID	Aggregation Type	Number of Ports	Member Port	Edit

Figure 4-12: Aggregation port configuration information.

In the port aggregation list which shows the current switch port configuration information for the polymerization properties:

1 Aggregation number: display link aggregation group number value.

2 Load Balancing: Displays the current link aggregation group load balancing judgment condition.

3 Aggregate types: Displays whether to use a polymerization port LACP protocol.

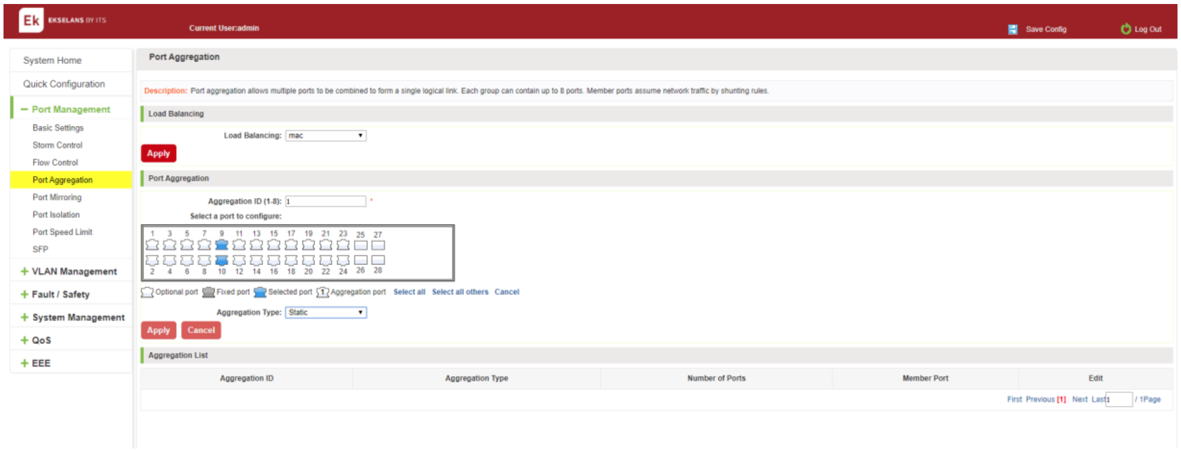
4 Member ports quantity: Displays the number of ports in the link aggregation group contains a total of member port: Displays the current port link aggregation group member prompt

5 Each aggregate port can bind up to eight member ports, port to transfer data among members of the network traffic through the shunt rules.

6 Port aggregation group must ensure that the port speed, duplex, port state agreement, or can not ATTACH after configuration.

Add port aggregation.

Enter aggregation port number, select the desired aggregation port, select aggregation type, click "Apply"



Port Aggregation

Description: Port aggregation allows multiple ports to be combined to form a single logical link. Each group can contain up to 8 ports. Member ports assume network traffic by shunting rules.

Load Balancing

Load Balancing: mac

Port Aggregation

Aggregation ID (1-8): 1 *

Select a port to configure:

Aggregation Type: Static

Aggregation List

Aggregation ID	Aggregation Type	Number of Ports	Member Port	Edit

First Previous [1] Next Last 1 / 1Page

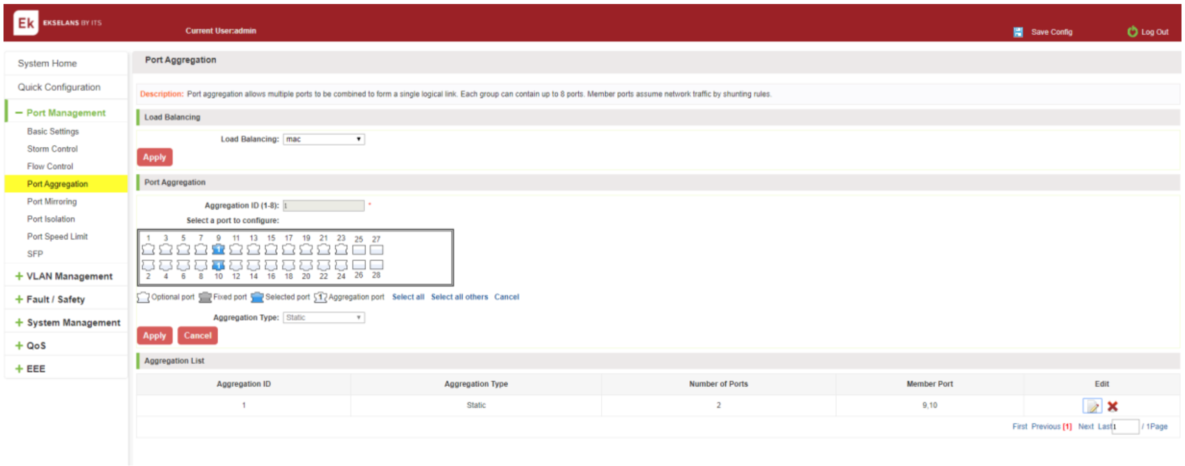
Figure 4-13: Port Aggregation Configuration area.

Increase port aggregation, follow these steps:

Step1：Select the option to load the shunt in the load balancing list. Step2：Enter the number in the "Aggregation number" in. Step3：Select the aggregated ports in the panel. Step4: Select the aggregation type. Step5: Click the "Apply" button to complete the configuration.

Modifying port aggregation.

Click on "Aggregation List" in the need to modify the port aggregation right icon in this area to the port aggregation port aggregation group corresponding modification:



Port Aggregation

Description: Port aggregation allows multiple ports to be combined to form a single logical link. Each group can contain up to 8 ports. Member ports assume network traffic by shunting rules.

Load Balancing

Load Balancing: mac

Port Aggregation

Aggregation ID (1-8): 1 *

Select a port to configure:

Aggregation Type: Static

Aggregation List

Aggregation ID	Aggregation Type	Number of Ports	Member Port	Edit
1	Static	2	9,10	✎ ✖

First Previous [1] Next Last 1 / 1Page

Figure 4-14: To modify the port aggregation.

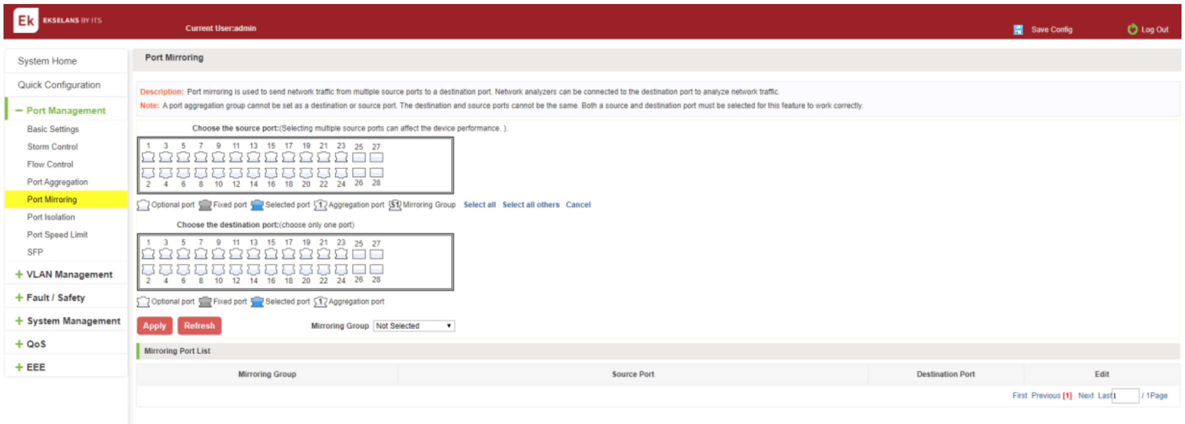
Modify Link Aggregation Procedure:

Step1: In the "Aggregation List Click to modify the right of the port aggregation, step2: In the port aggregation configuration page to modify the load balancing type and click Next to "Apply". step3: Select the port to be added to the aggregation port. step4: Click the "Apply" button to complete the configuration.

Port Mirroring.

Port Mirroring Configuration.

Click "Port Management" "configuration of port mirroring "Port Mirroring" view of the switch:



Port Mirroring

Description: Port mirroring is used to send network traffic from multiple source ports to a destination port. Network analyzers can be connected to the destination port to analyze network traffic.

Note: A port aggregation group cannot be set as a destination or source port. The destination and source ports cannot be the same. Both a source and destination port must be selected for this feature to work correctly.

Choose the source port:(Selecting multiple source ports can affect the device performance.).

Choose the destination port:(choose only one port)

Mirroring Group: Not Selected

Mirroring Port List

Mirroring Group	Source Port	Destination Port	Edit

Figure 4-15: Port mirroring configuration information.

In the Port Mirroring is a property list which shows the configuration of the current mirror switch:

Mirroring group: mirroring group ID, can be configured up to seven mirroring group.

Source Port: The port forwarding on the source data is mirrored to the destination port.

Destination port: mirror data sent to the destination port.

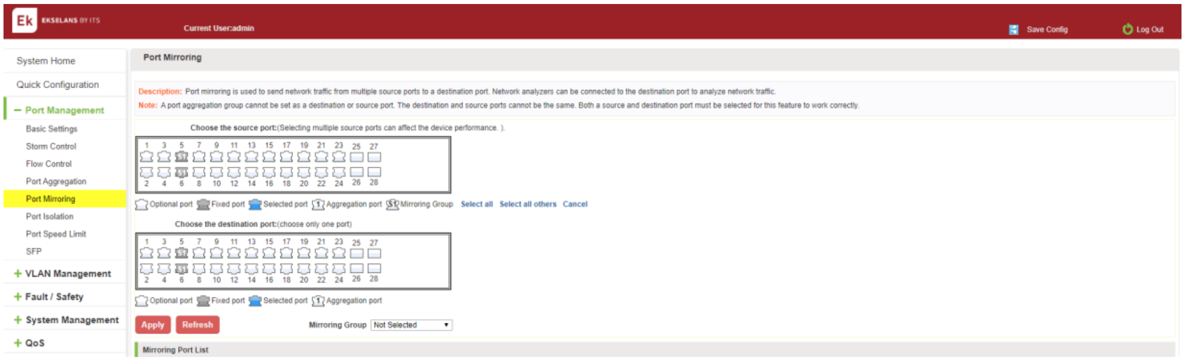
1 Port aggregation port can not be used as the destination port and source port.

2 Destination port and source port can not be the same.

3 Same group mirroring group can have only one destination port.

Add port mirroring group.

On the panel, select "Source Port" and "Destination Port" add port mirroring group.



Port Mirroring

Description: Port mirroring is used to send network traffic from multiple source ports to a destination port. Network analyzers can be connected to the destination port to analyze network traffic.

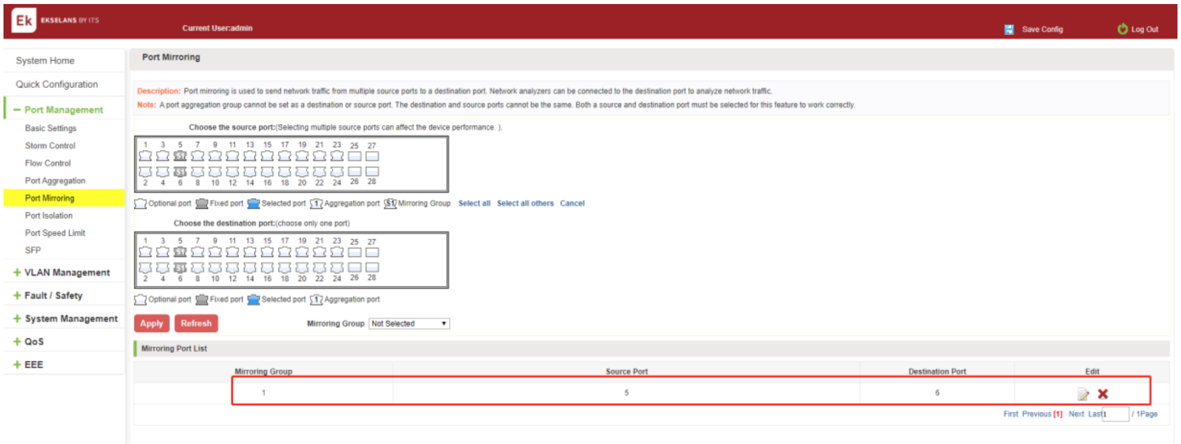
Note: A port aggregation group cannot be set as a destination or source port. The destination and source ports cannot be the same. Both a source and destination port must be selected for this feature to work correctly.

Choose the source port:(Selecting multiple source ports can affect the device performance.).

Choose the destination port:(choose only one port)

Mirroring Group: Not Selected

Figure 4-16: Add port mirroring group.



Port Mirroring

Description: Port mirroring is used to send network traffic from multiple source ports to a destination port. Network analyzers can be connected to the destination port to analyze network traffic.

Note: A port aggregation group cannot be set as a destination or source port. The destination and source ports cannot be the same. Both a source and destination port must be selected for this feature to work correctly.

Choose the source port:(Selecting multiple source ports can affect the device performance.).

Choose the destination port:(choose only one port)

Mirroring Group: Not Selected

Mirroring Port List

Mirroring Group	Source Port	Destination Port	Edit
1	5	6	✎ ✕

Figure 04-17: Add port mirroring group results.

Port mirroring configuration steps are as follows:

Step1: Select "Source Port", Step2: Select "Destination Port", Step3: select mirroring group, Step4, Click"Apply".

Configuration instructions:

1 On the switch can be configured 7 mirroring group.

2 Aggregated port mirroring can not be configured are shown in gray in the panel.

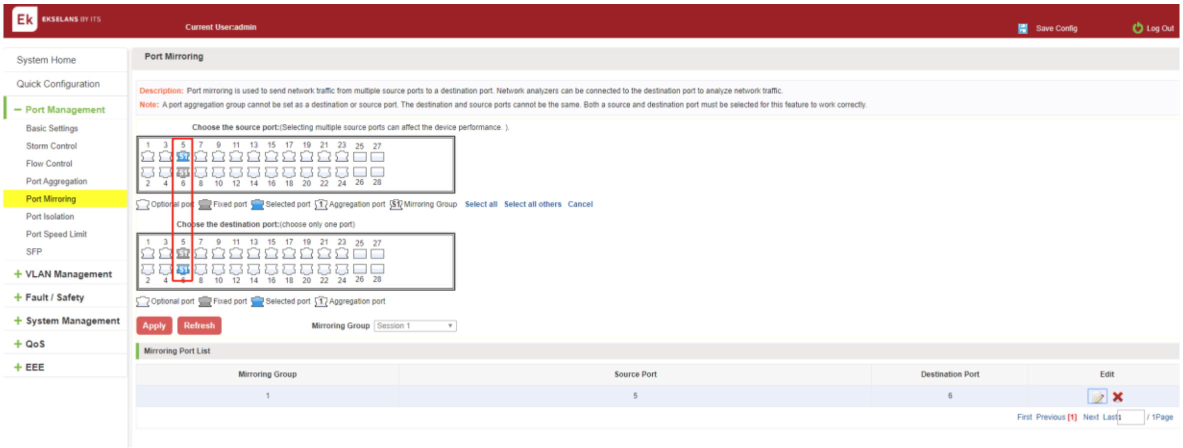
3 Has been selected port mirroring port, displayed in the faceplate is gray.

4 Aggregated port mirroring can not be configured are shown in gray in the panel.

5 Has been selected port mirroring port, displayed in the faceplate is gray.

To modify the port mirroring group.

Select the group to modify, click on the action bar " ✎ " button. Modify the corresponding mirroring group.



Description: Port mirroring is used to send network traffic from multiple source ports to a destination port. Network analyzers can be connected to the destination port to analyze network traffic.

Note: A port aggregation group cannot be set as a destination or source port. The destination and source ports cannot be the same. Both a source and destination port must be selected for this feature to work correctly.

Choose the source port:(Selecting multiple source ports can affect the device performance.).

Choose the destination port:(choose only one port)

Mirroring Group: Session 1

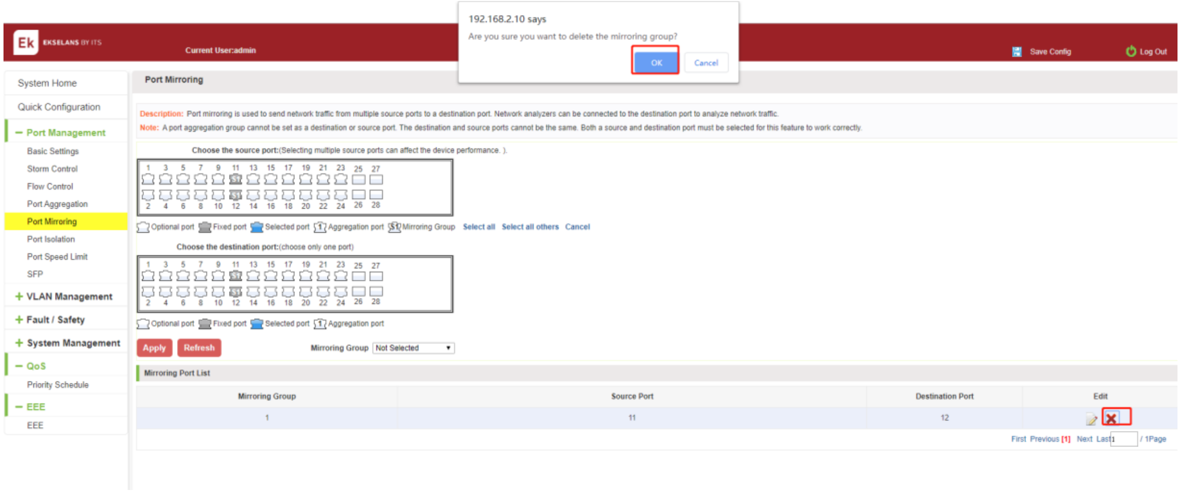
Mirroring Group	Source Port	Destination Port	Edit
1	5	6	✎ ✗

Figure 4-18: To modify the port mirroring group.

Modify the port mirroring configuration steps are as follows:

Step1: In the image you want to modify the operation of the group column, click on " ✎ " ; step2: Add or remove the corresponding port in the panel; step3: Click "Apply".

Delete a port mirroring group.



192.168.2.10 says

Are you sure you want to delete the mirroring group?

OK Cancel

Current User:admin

Port Mirroring

Description: Port mirroring is used to send network traffic from multiple source ports to a destination port. Network analyzers can be connected to the destination port to analyze network traffic.

Note: A port aggregation group cannot be set as a destination or source port. The destination and source ports cannot be the same. Both a source and destination port must be selected for this feature to work correctly.

Choose the source port:(Selecting multiple source ports can affect the device performance.).

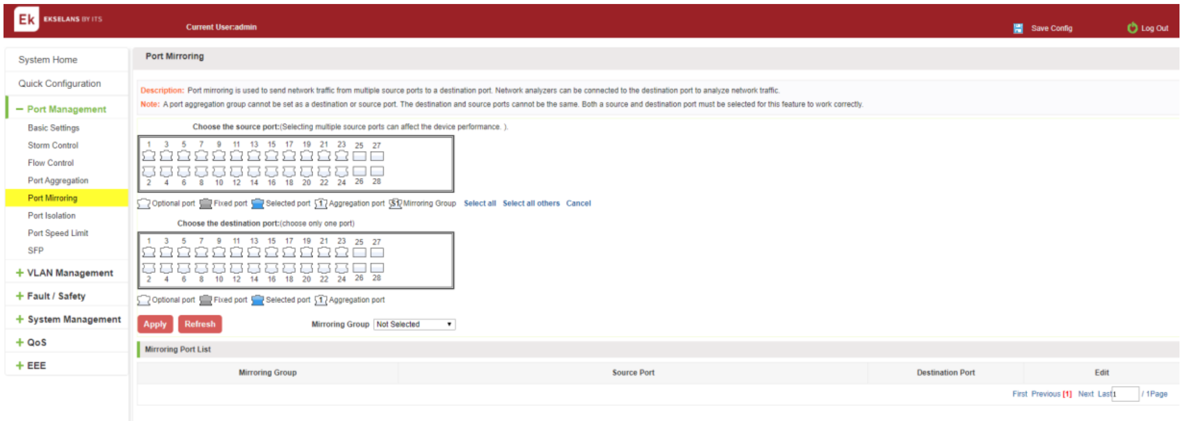
Choose the destination port:(choose only one port)

Mirroring Group: Not Selected

Mirroring Port List

Mirroring Group	Source Port	Destination Port	Edit
1	11	12	

Figure 4-19: Delete port mirroring group.



Current User:admin

Port Mirroring

Description: Port mirroring is used to send network traffic from multiple source ports to a destination port. Network analyzers can be connected to the destination port to analyze network traffic.

Note: A port aggregation group cannot be set as a destination or source port. The destination and source ports cannot be the same. Both a source and destination port must be selected for this feature to work correctly.

Choose the source port:(Selecting multiple source ports can affect the device performance.).

Choose the destination port:(choose only one port)

Mirroring Group: Not Selected

Mirroring Port List

Mirroring Group	Source Port	Destination Port	Edit

Figure 4-20: Deleted successfully port mirroring.

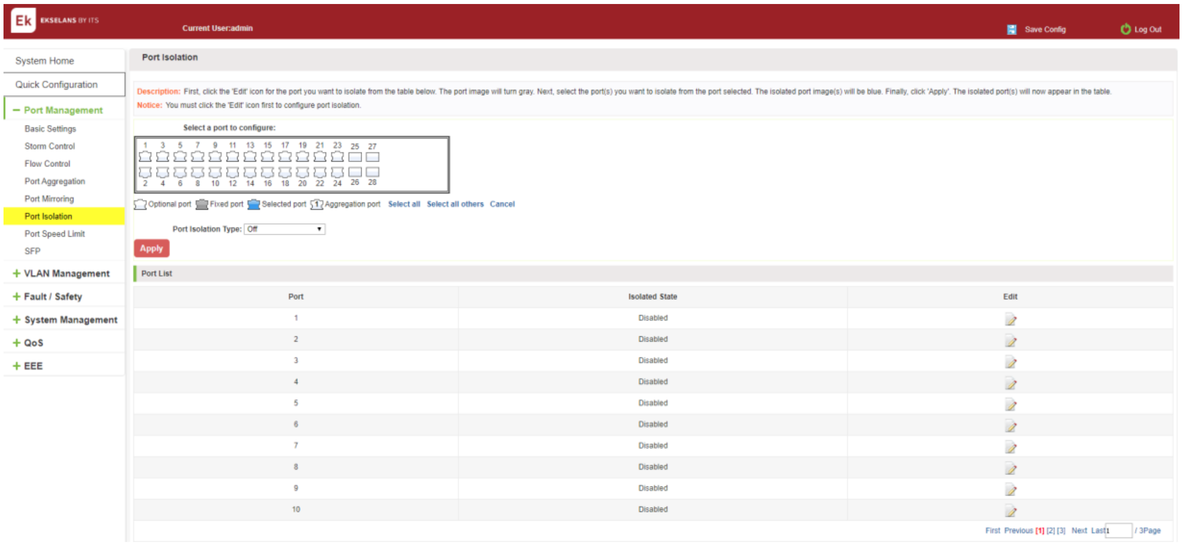
Remove port mirroring configuration steps are as follows:

Step1: In the image you want to modify the operation of the group column, click " 📝 " ; step2: In the panel, click Cancel the source port, destination port and then click Cancel; step3: In the panel, click Cancel the source port, destination port and then click Cancel;step4:Click "Apply".

Port ISOLATION.

Port ISOLATION Configuration.

Click "Port Management" "configuration of port mirroring "Port Isolation" view of the switch:



Port Isolation

Description: First, click the 'Edit' icon for the port you want to isolate from the table below. The port image will turn gray. Next, select the port(s) you want to isolate from the port selected. The isolated port image(s) will be blue. Finally, click 'Apply'. The isolated port(s) will now appear in the table.

Notice: You must click the 'Edit' icon first to configure port isolation.

Select a port to configure:

Port Isolation Type: Off

Port List

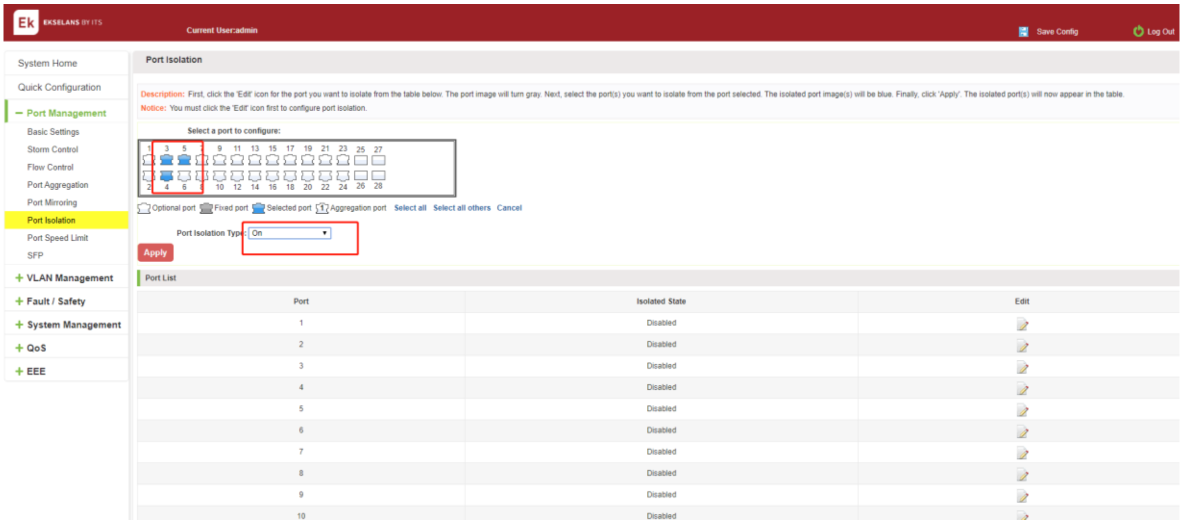
Port	Isolated State	Edit
1	Disabled	
2	Disabled	
3	Disabled	
4	Disabled	
5	Disabled	
6	Disabled	
7	Disabled	
8	Disabled	
9	Disabled	
10	Disabled	

First Previous [1] [2] [3] Next Last 1 /3Page

Figure 4-21: Port Isolation configuration information.

Configuring port isolation.

Open Port Isolation function: select the port on which you want to open port isolation, click the "port isolation type" Select "On", "Apple":



Port Isolation

Description: First, click the 'Edit' icon for the port you want to isolate from the table below. The port image will turn gray. Next, select the port(s) you want to isolate from the port selected. The isolated port image(s) will be blue. Finally, click 'Apply'. The isolated port(s) will now appear in the table.

Notice: You must click the 'Edit' icon first to configure port isolation.

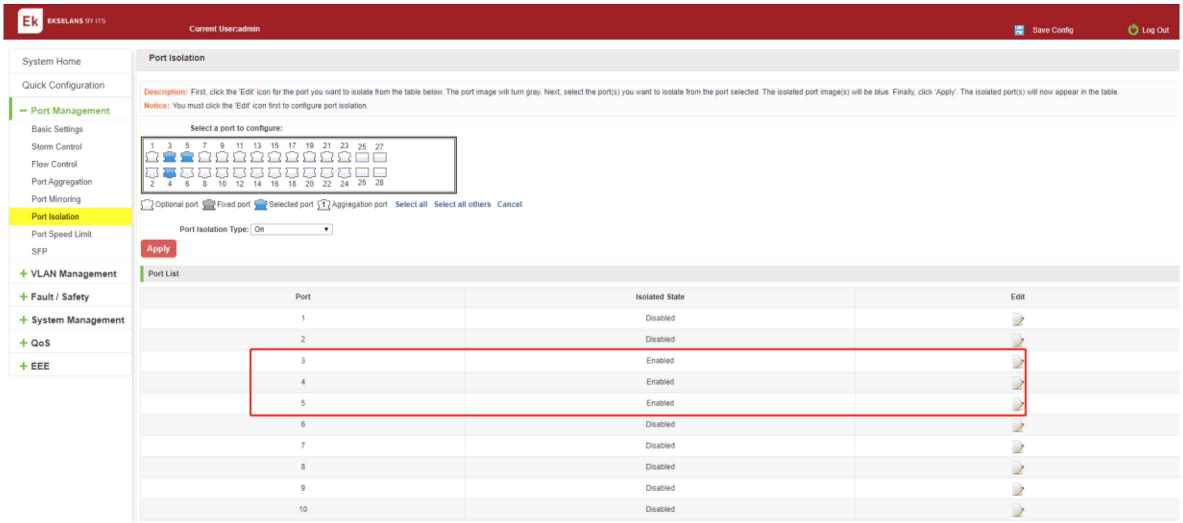
Select a port to configure:

Port Isolation Type: On

Port List

Port	Isolated State	Edit
1	Disabled	
2	Disabled	
3	Disabled	
4	Disabled	
5	Disabled	
6	Disabled	
7	Disabled	
8	Disabled	
9	Disabled	
10	Disabled	

Figure 4-22: enable port isolation function.



Port Isolation

Description: First, click the 'Edit' icon for the port you want to isolate from the table below. The port image will turn gray. Next, select the port(s) you want to isolate from the port selected. The isolated port image(s) will be blue. Finally, click 'Apply'. The isolated port(s) will now appear in the table.

Notice: You must click the 'Edit' icon first to configure port isolation.

Select a port to configure:

Port Isolation Type: On

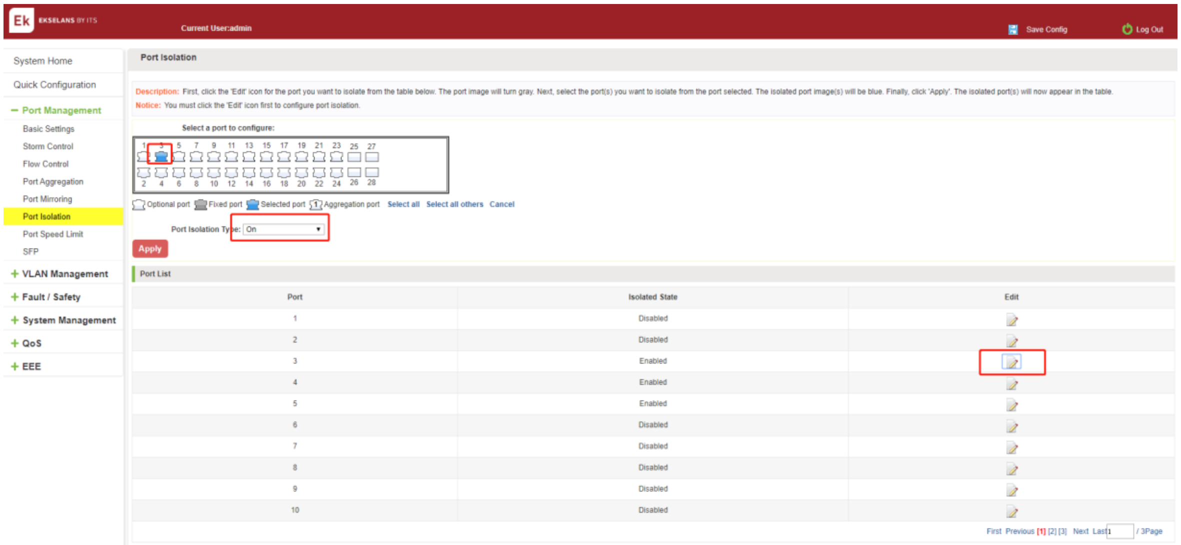
Port List

Port	Isolated State	Edit
1	Disabled	✎
2	Disabled	✎
3	Enabled	✎
4	Enabled	✎
5	Enabled	✎
6	Disabled	✎
7	Disabled	✎
8	Disabled	✎
9	Disabled	✎
10	Disabled	✎

Figure 04-23: enable port isolation results.

Modify the port isolation.

Select the port to modify, click on the action bar " ✎ " button. Modify the corresponding port isolation.



Port Isolation

Description: First, click the 'Edit' icon for the port you want to isolate from the table below. The port image will turn gray. Next, select the port(s) you want to isolate from the port selected. The isolated port image(s) will be blue. Finally, click 'Apply'. The isolated port(s) will now appear in the table.

Notice: You must click the 'Edit' icon first to configure port isolation.

Select a port to configure:

Port Isolation Type: On

Port List

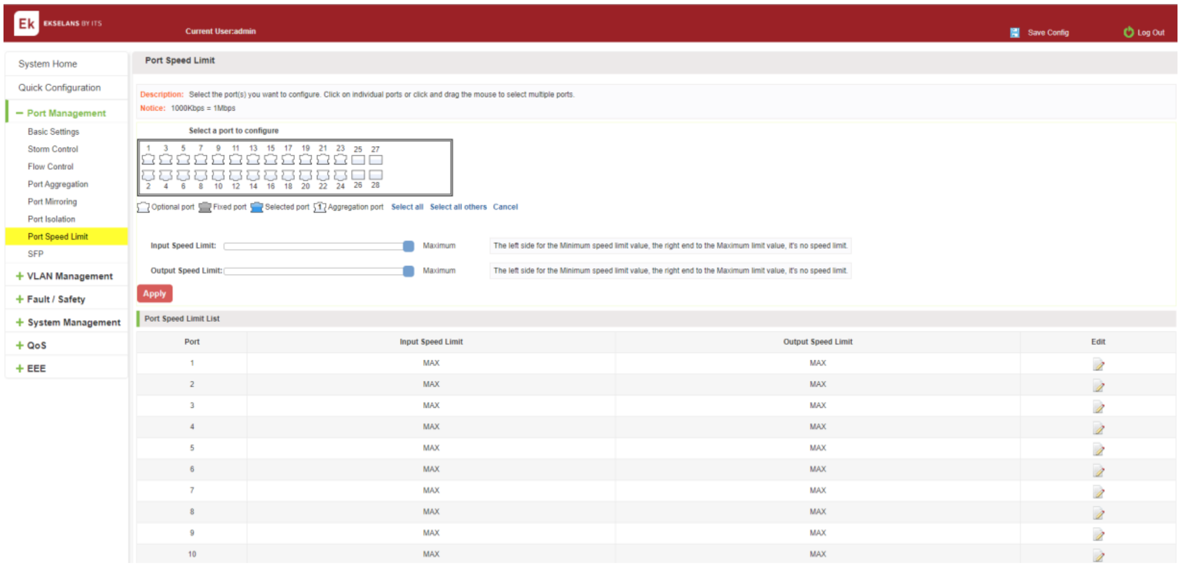
Port	Isolated State	Edit
1	Disabled	✎
2	Disabled	✎
3	Enabled	✎
4	Enabled	✎
5	Enabled	✎
6	Disabled	✎
7	Disabled	✎
8	Disabled	✎
9	Disabled	✎
10	Disabled	✎

Figure 4-24: To modify the port isolation.

Port speed limit.

View port rate limit.

Click "Port Management" "Port Speed Limit" switch to view the current port speed configured information:



Current User:admin

Port Speed Limit

Description: Select the port(s) you want to configure. Click on individual ports or click and drag the mouse to select multiple ports.
Notice: 1000Kbps = 1Mbps

Select a port to configure

Input Speed Limit: Maximum — The left side for the Minimum speed limit value, the right end to the Maximum limit value, it's no speed limit.

Output Speed Limit: Maximum — The left side for the Minimum speed limit value, the right end to the Maximum limit value, it's no speed limit.

Port Speed Limit List

Port	Input Speed Limit	Output Speed Limit	Edit
1	MAX	MAX	✎
2	MAX	MAX	✎
3	MAX	MAX	✎
4	MAX	MAX	✎
5	MAX	MAX	✎
6	MAX	MAX	✎
7	MAX	MAX	✎
8	MAX	MAX	✎
9	MAX	MAX	✎
10	MAX	MAX	✎

Figure 4-25: View Rate Configuration information.

In the port speed list which shows the current speed limit switch attribute configuration information:

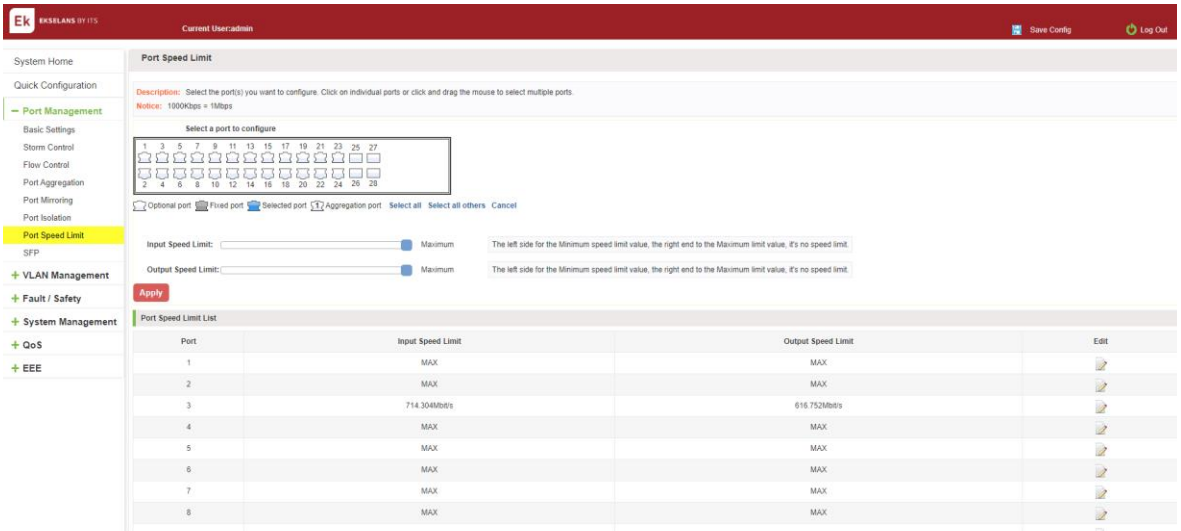
Port: The number of the port.

Input limit: uplink port speed.

Output speed: port downstream rate.

Configure port access rate.

Select the panel to set the speed limit of the port, set the rate limit value by dragging the speed bar.



Port Speed Limit

Description: Select the port(s) you want to configure. Click on individual ports or click and drag the mouse to select multiple ports.
Notice: 1000Kbps = 1Mbps

Select a port to configure

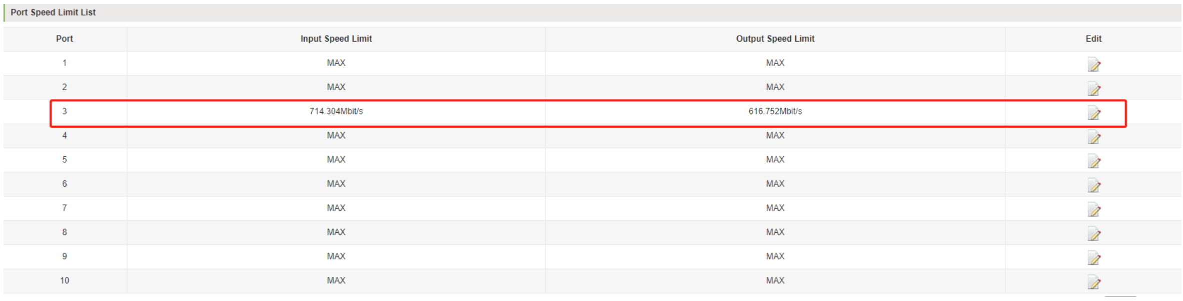
Input Speed Limit: Maximum — The left side for the Minimum speed limit value, the right end to the Maximum limit value, it's no speed limit.

Output Speed Limit: Maximum — The left side for the Minimum speed limit value, the right end to the Maximum limit value, it's no speed limit.

Port Speed Limit List

Port	Input Speed Limit	Output Speed Limit	Edit
1	MAX	MAX	✎
2	MAX	MAX	✎
3	714.304Mbit/s	616.752Mbit/s	✎
4	MAX	MAX	✎
5	MAX	MAX	✎
6	MAX	MAX	✎
7	MAX	MAX	✎
8	MAX	MAX	✎

Figure 4-26 Configure port rate limiting entrance.



Port Speed Limit List

Port	Input Speed Limit	Output Speed Limit	Edit
1	MAX	MAX	✎
2	MAX	MAX	✎
3	714.304Mbit/s	616.752Mbit/s	✎
4	MAX	MAX	✎
5	MAX	MAX	✎
6	MAX	MAX	✎
7	MAX	MAX	✎
8	MAX	MAX	✎
9	MAX	MAX	✎
10	MAX	MAX	✎

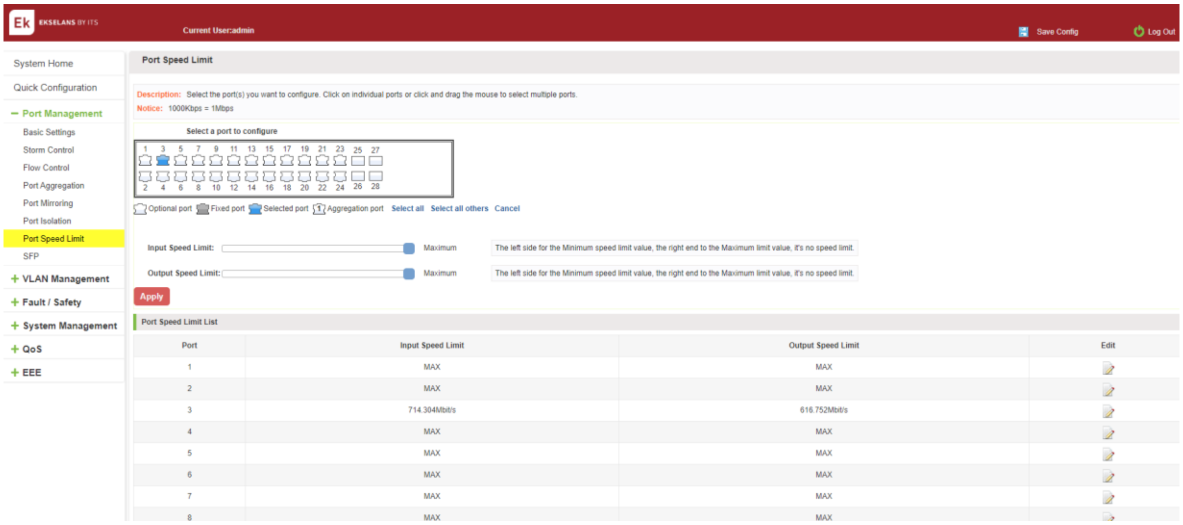
Figure 4-27: Port entrance speed limit results.

Entrance port rate limiting configuration steps are as follows:

Step1： Click on the right side of the port "▭" Icon or select multiple icons; step2: Set rate limiting strip port value; step3: Click the lower right corner "Apply" button to complete the configuration.

Remove the port speed limit.

Click the need to remove the limit on the right port icon '' in the configuration area of the port rate value pull bar to the far right, "Apply" to complete the operation.



Current User:admin

Port Speed Limit

Description: Select the port(s) you want to configure. Click on individual ports or click and drag the mouse to select multiple ports.
Notice: 1000Kbps = 1Mbps

Input Speed Limit: Maximum — The left side for the Minimum speed limit value, the right end to the Maximum limit value, it's no speed limit.

Output Speed Limit: Maximum — The left side for the Minimum speed limit value, the right end to the Maximum limit value, it's no speed limit.

Port Speed Limit List

Port	Input Speed Limit	Output Speed Limit	Edit
1	MAX	MAX	✎
2	MAX	MAX	✎
3	714.304Mbit/s	616.752Mbit/s	✎
4	MAX	MAX	✎
5	MAX	MAX	✎
6	MAX	MAX	✎
7	MAX	MAX	✎
8	MAX	MAX	✎

Figure 4-28: Remove the port speed limit.

Remove uplink port rate limiting steps are as follows:

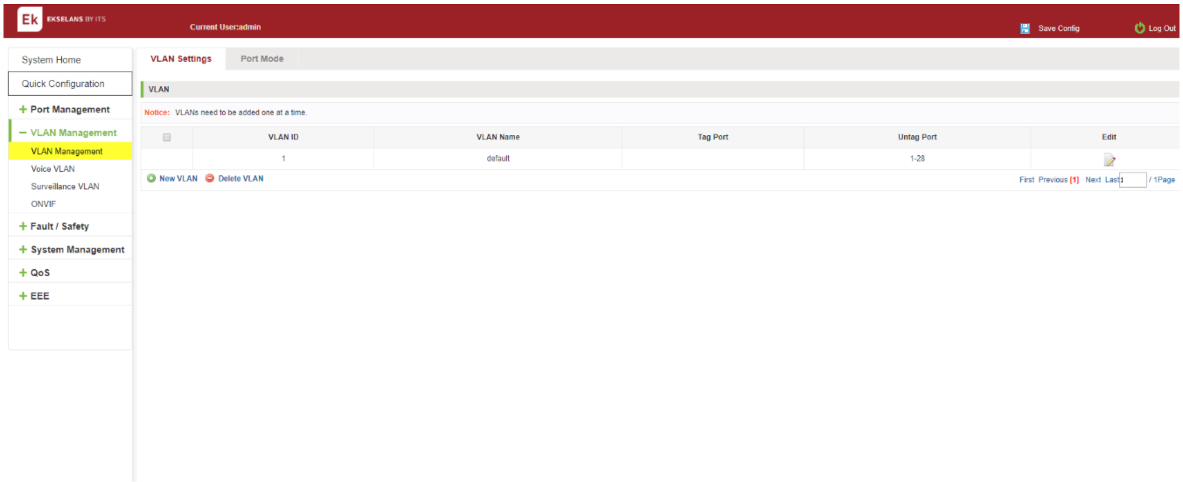
Step1: Click on the right side of the port ✎ icon ; step2: In the area of the port rate configuration value rate strip pulled to the far right; step3: Click the "Apply" button to complete the configuration.

Vlan management.

VLAN management.

Check VLAN configuration information.

Click on the navigation bar "VLAN Management" "VLAN management" "VLAN Settings" to view the switch configured:



Notice: VLANs need to be added one at a time.

□	VLAN ID	VLAN Name	Tag Port	Untag Port	Edit
	1	default		1-28	✎

Figure 5-1: VLAN configuration information.

In the VLAN list which shows the properties of the configuration information of the current switch VLAND:

1 VLAN ID: VLAN ID value is displayed.

2 VLAN Name: The name of the VLAN, the default VLAN ID to name.

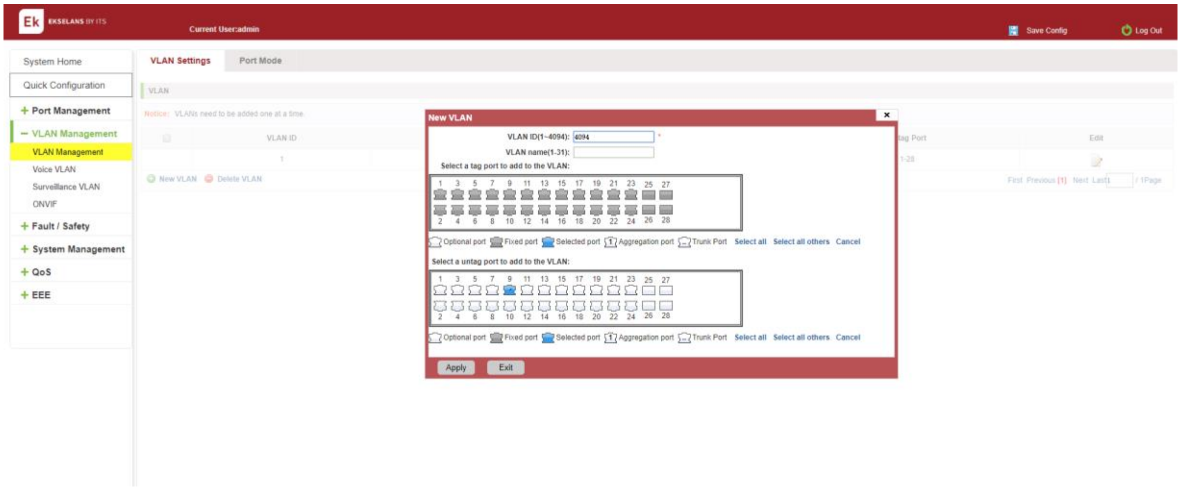
3 VLAN IP address: Displays the switch's management IP.

4 Port: Displays the port VLAN that exist.

5 By default, all ports belong to VLAN 1.

Adding a VLAN.

Click "NEW VLAN" button, you can increase the VLAN configurations:



Notice: VLANs need to be added one at a time.

VLAN ID(1~4094): 4094 *

VLAN name(1-31):

Select a tag port to add to the VLAN:

Select a untag port to add to the VLAN:

Figure 5-2: Adding a VLAN.

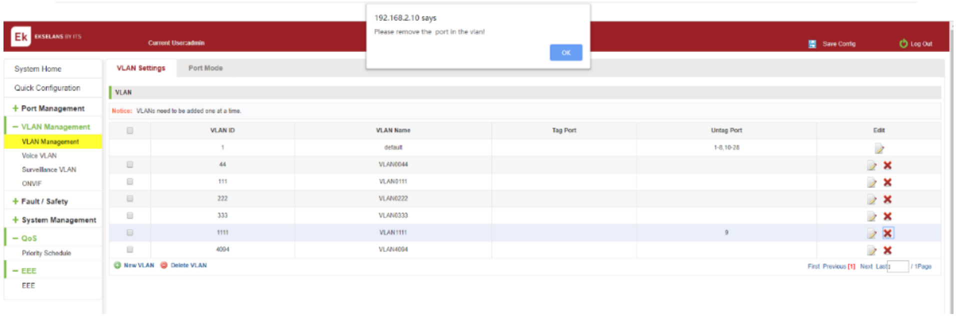
Adding a VLAN, follow these steps:

Step1: Click "NEW vlan" connection; step2: Value added VLAN VLAN ID of the page to fill in; step3: Select the ports; step4: Click the lower right corner "Apply" button to complete the configuration.

Remove VLAN.

- SINGLE VLAN delete:

To delete the selected VLAN, click the "X" button to delete the selected VLAN,if the VLAN do not have ports ,You can directly delete the VLAN;if the VLAN have some ports,you must be remove the ports in the VLAN firstly and then you can delete the selected VLAN.



192.168.2.10 says
Please remove the port in the vlan!
OK

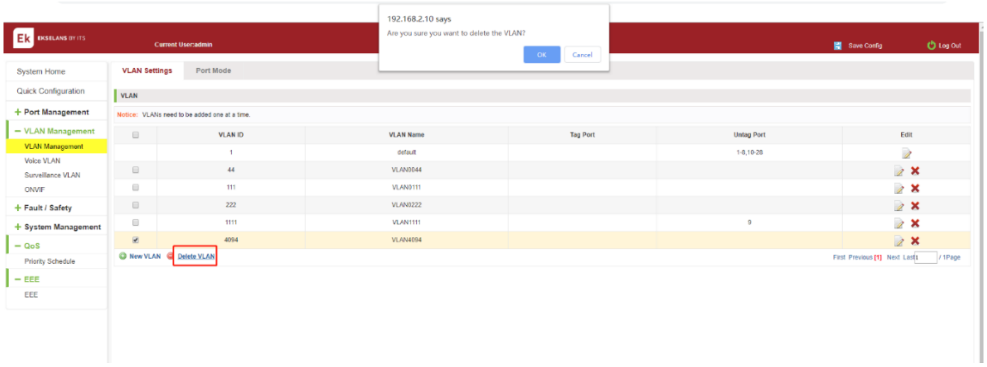
Notice: VLANs need to be added one at a time.

□	VLAN ID	VLAN Name	Tag Port	Untag Port	Edit
	1	default		1-8,10-28	
□	44	VLAN0044			✗
□	111	VLAN0111			✗
□	222	VLAN0222			✗
□	333	VLAN0333			✗
□	1111	VLAN1111		9	✗
□	4094	VLAN4094			✗

Figure 5-3: Delete a single VLAN.

- DELETE MULTIPLE VLAN:

First select the VLAN you want to be deleted before the " " checkbox, then click "Delete VLAN" button to delete the selected VLAN,if the VLANs have some ports the VLAN can not be removed because of there are member ports.The others will be removed.



192.168.2.10 says
Are you sure you want to delete the VLAN?
OK Cancel

Notice: VLANs need to be added one at a time.

□	VLAN ID	VLAN Name	Tag Port	Untag Port	Edit
	1	default		1-8,10-28	
□	44	VLAN0044			✗
□	111	VLAN0111			✗
□	222	VLAN0222			✗
□	1111	VLAN1111		9	✗
☑	4094	VLAN4094			✗

Figure 5-4: Delete multiple VLAN

Delete multiple VLAN, follow these steps:

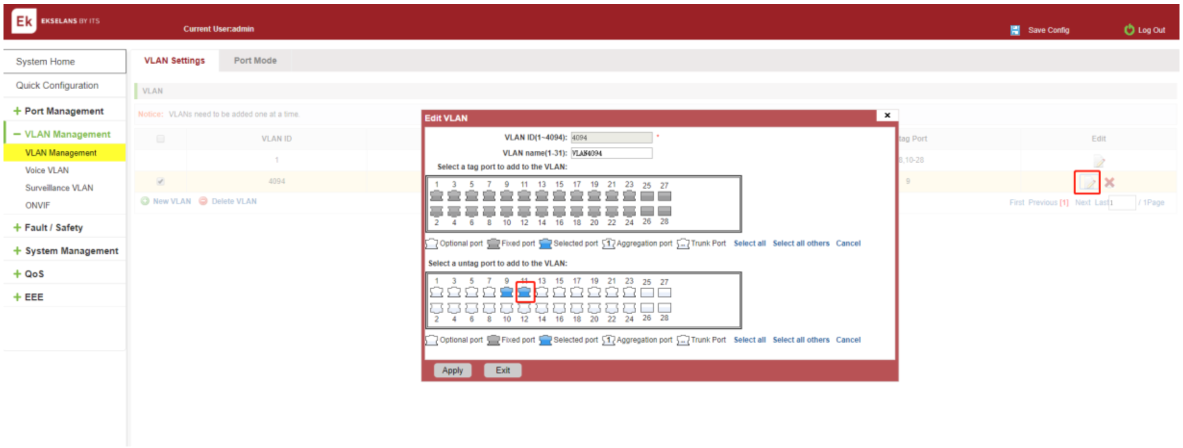
1 Step1:I want to delete VLAN check box;

2 Setp2:Click on the bottom left "Delete VLAN" connection;

3 Step3:Confirm delete.

VLAN PORT TO A VLAN.

Click on the icon can be added to the selected port in the VLAN:



VLAN ID(1~4094): 4094 *
VLAN name(1-31): VLAN4094
Select a tag port to add to the VLAN:
Select a untag port to add to the VLAN:

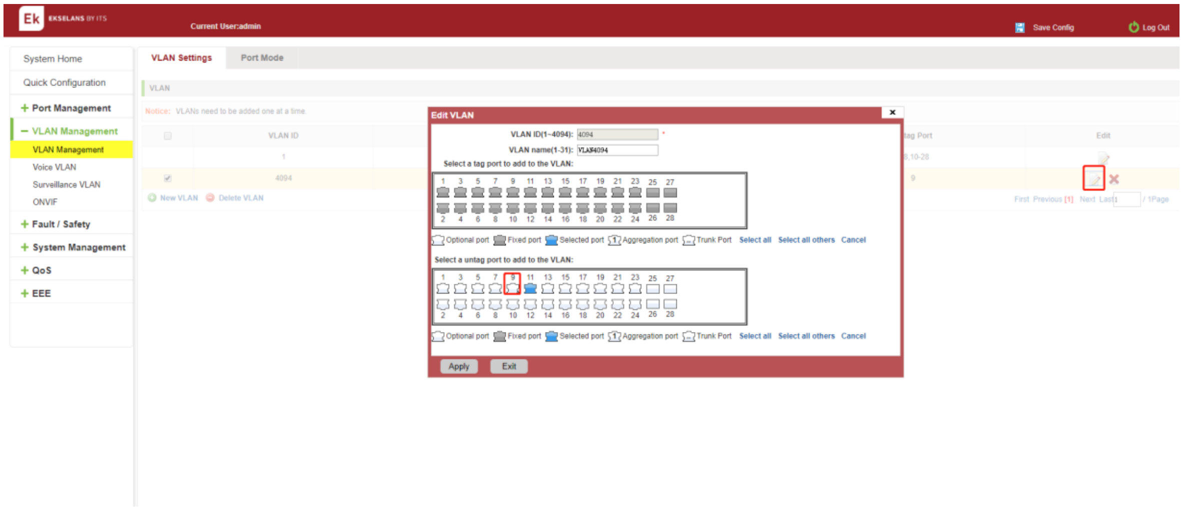
Figure 5-5: Add the port to the VLAN

Add the port to the VLAN, follow these steps:

1. Step1: Click" ✎ "icon.
2. step2: Selected to join the ports in the port panel.
3. step3: Click the lower right corner "Apply" button to complete the configuration.

TO REMOVE THE PORT FROM A VLAN.

Click on the icon, you can remove the port from this VLAN:



Notice: VLANs need to be added one at a time.

VLAN ID(1~4094): 4094

VLAN name(1-31): VLAN4094

Select a tag port to add to the VLAN:

Select a untag port to add to the VLAN:

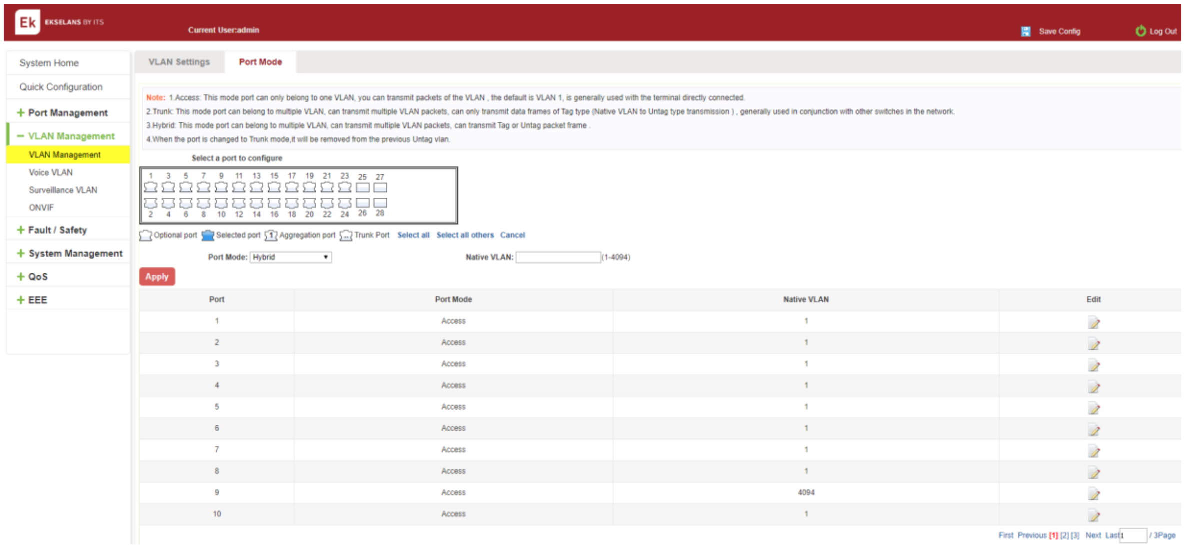
Figure 5-6: To remove the port from the VLAN.

Procedure to remove the port from VLAN as follows:

Step1: Click on the icon " 📝 "； step2: Remove the port to be removed from the port panel; step3: Click on the lower right corner of the "Apply" button to complete the configuration.

View port MODE.

Click on the "Vlan Management" "Port Mode" view switches has been configured port mode information:



Note: 1.Access: This mode port can only belong to one VLAN, you can transmit packets of the VLAN , the default is VLAN 1, is generally used with the terminal directly connected.
2.Trunk: This mode port can belong to multiple VLAN, can transmit multiple VLAN packets, can only transmit data frames of Tag type (Native VLAN to Untag type transmission) , generally used in conjunction with other switches in the network.
3.Hybrid: This mode port can belong to multiple VLAN, can transmit multiple VLAN packets, can transmit Tag or Untag packet frame .
4.When the port is changed to Trunk mode,it will be removed from the previous Untag vlan.

Port Mode: Hybrid

Native VLAN: (1-4094)

Port	Port Mode	Native VLAN	Edit
1	Access	1	
2	Access	1	
3	Access	1	
4	Access	1	
5	Access	1	
6	Access	1	
7	Access	1	
8	Access	1	
9	Access	4094	
10	Access	1	

Figure 5-7: View port mode configuration information.

Displayed in the port mode list is the property value of the port configuration of the current switch:

1 The port name: display port number used.

2 The Native VLAN: display native VLAN.

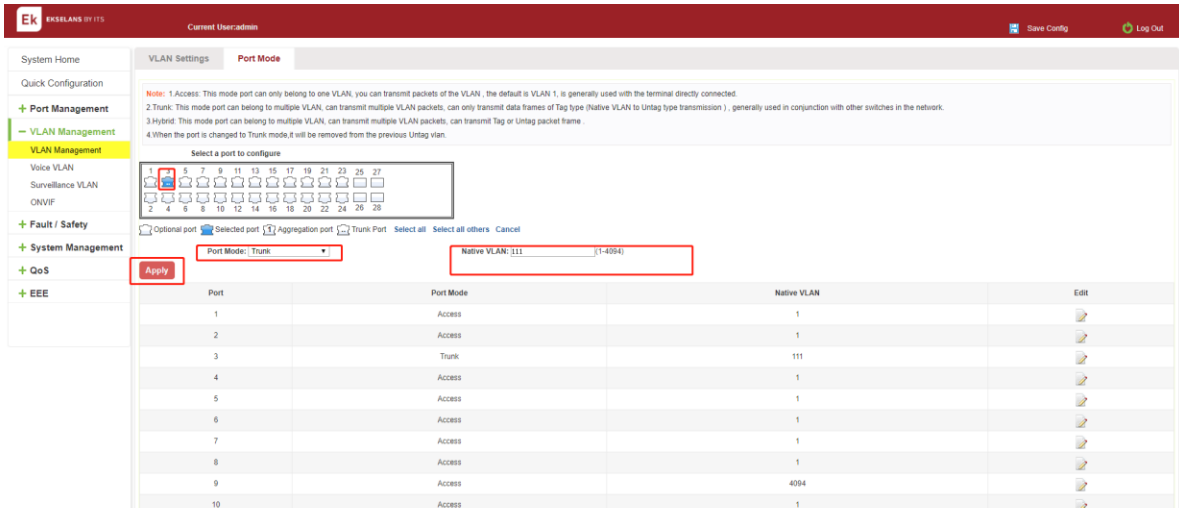
3 the allowed VLAN: The VLAN allows the display message can be through VLAN.

4 The default port is 1 VLAN native VLAN.

5 The default port mode is access.

CHANGE THE PORT MODE IS TRUNK.

Select the port you want to change the mode and click the "port mode " list, you can set the port mode is trunk:



Current User:admin

Note: 1.Access: This mode port can only belong to one VLAN, you can transmit packets of the VLAN , the default is VLAN 1, is generally used with the terminal directly connected.
2.Trunk: This mode port can belong to multiple VLAN, can transmit multiple VLAN packets, can only transmit data frames of Tag type (Native VLAN to Untag type transmission) , generally used in conjunction with other switches in the network.
3.Hybrid: This mode port can belong to multiple VLAN, can transmit multiple VLAN packets, can transmit Tag or Untag packet frame .
4.When the port is changed to Trunk mode,it will be removed from the previous Untag vlan.

Select a port to configure

Port Mode: Trunk

Native VLAN: 111 (1-4094)

Port	Port Mode	Native VLAN	Edit
1	Access	1	
2	Access	1	
3	Trunk	111	
4	Access	1	
5	Access	1	
6	Access	1	
7	Access	1	
8	Access	1	
9	Access	4094	
10	Access	1	

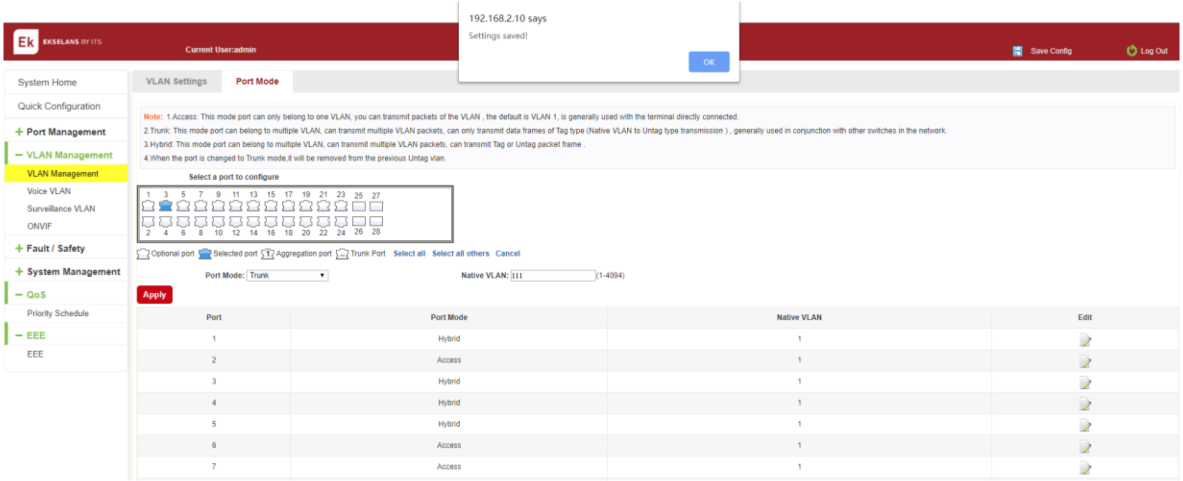
Figure 5-8: Change the port mode is trunk.

The steps to set port mode is trunk are as follows :

Step1:Chose one or more ports; step2:Click the port mode list chose the mode is :trunk; step3:Set Native VLAN, the VLAN must be is exist; step4:Set by allowing the VLAN number, the default allowed VLAN is empty if you want to allowed the native VLAN ,you must be configure allowed the native vlan; step5:Click on the lower right corner of the "Apply" button to complete the configuration.

Change the port mode is hybrid.

Select the port you want to change the mode and click the "port mode " list, you can set the port mode is hybrid.



192.168.2.10 says

Settings saved!

Note: 1.Access: This mode port can only belong to one VLAN, you can transmit packets of the VLAN , the default is VLAN 1, is generally used with the terminal directly connected.
2.Trunk: This mode port can belong to multiple VLAN, can transmit multiple VLAN packets, can only transmit data frames of Tag type (Native VLAN to Untag type transmission) , generally used in conjunction with other switches in the network.
3.Hybrid: This mode port can belong to multiple VLAN, can transmit multiple VLAN packets, can transmit Tag or Untag packet frame .
4.When the port is changed to Trunk mode,it will be removed from the previous Untag vlan.

Select a port to configure

Optional port · Selected port · Aggregation port · Trunk Port

Port Mode: Trunk

Native VLAN: 111 (1-4094)

Port	Port Mode	Native VLAN	Edit
1	Hybrid	1	✎
2	Access	1	✎
3	Hybrid	1	✎
4	Hybrid	1	✎
5	Hybrid	1	✎
6	Access	1	✎
7	Access	1	✎

Figure 5-9: Change the port mode is hybrid.

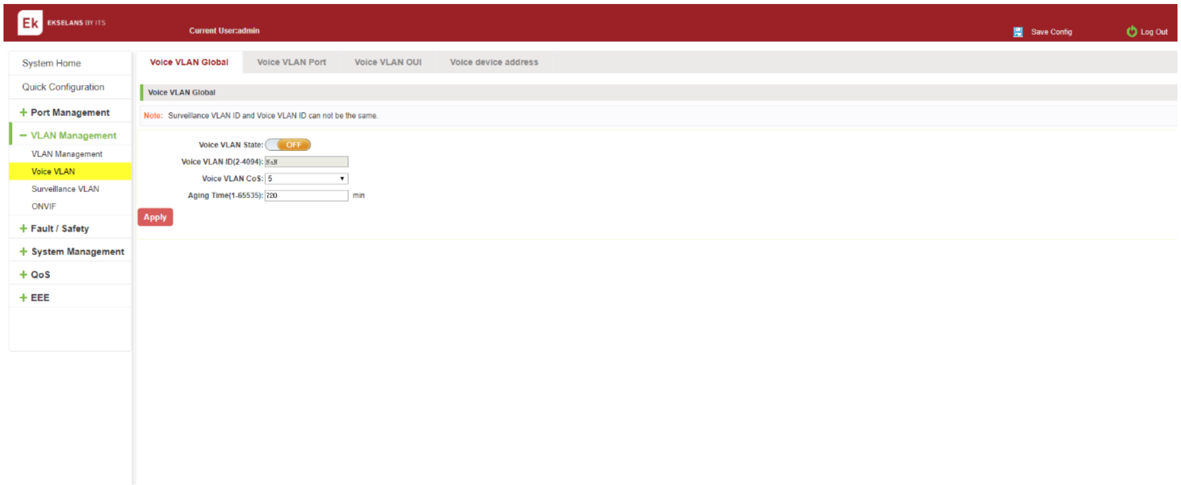
The steps to set port mode is hybrid are as follows ：

Step1:Chose one or more ports ；step2:Click the port mode list chose the mode is :hybrid; step3: Set Native VLAN,the VLAN must be is exist; step4:Set by allowing the VLAN number ,the default allowed VLAN 1,if you want to allowed the native VLAN ,you must be configure allowed the native vlan; step5: Click on the lower right corner of the "Apply" button to complete the configuration.

Voice VLAN.

View voice VLAN information

Click on the navigation bar "VLAN Management" "Voice VLAN" " Voice VLAN Global" to view the switch configured:



Voice VLAN Global

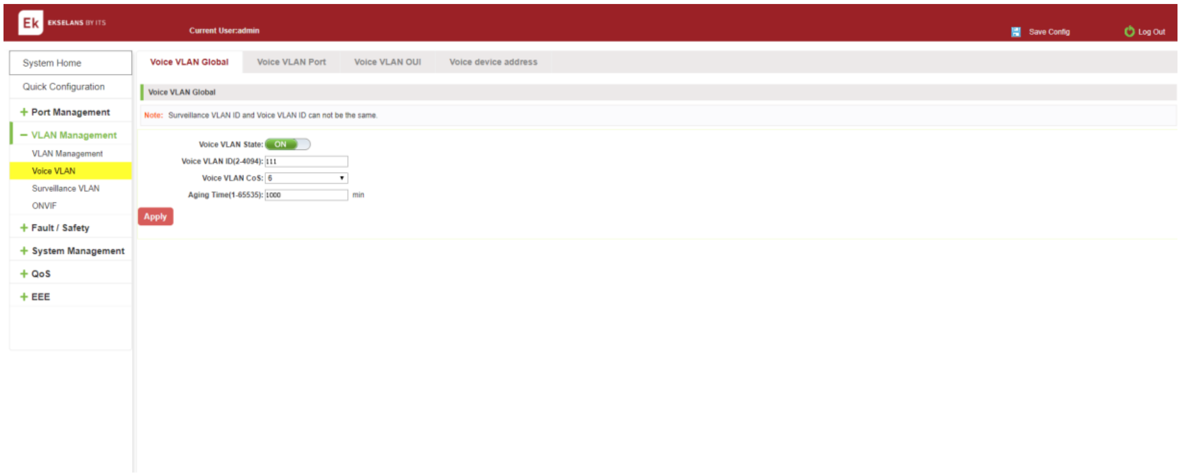
Note: Surveillance VLAN ID and Voice VLAN ID can not be the same.

Voice VLAN State: OFF
Voice VLAN ID(2-4094): NaN
Voice VLAN CoS: 5
Aging Time(1-65535): 720 min

Figure 5-10: view voice VLAN information.

Configure voice VLAN global.

Click on the navigation bar "VLAN Management" "Voice VLAN" " Voice VLAN Global" to configure the voice VLAN;



Voice VLAN Global

Note: Surveillance VLAN ID and Voice VLAN ID can not be the same.

Voice VLAN State: ON
Voice VLAN ID(2-4094): 111
Voice VLAN CoS: 6
Aging Time(1-65535): 1000 min

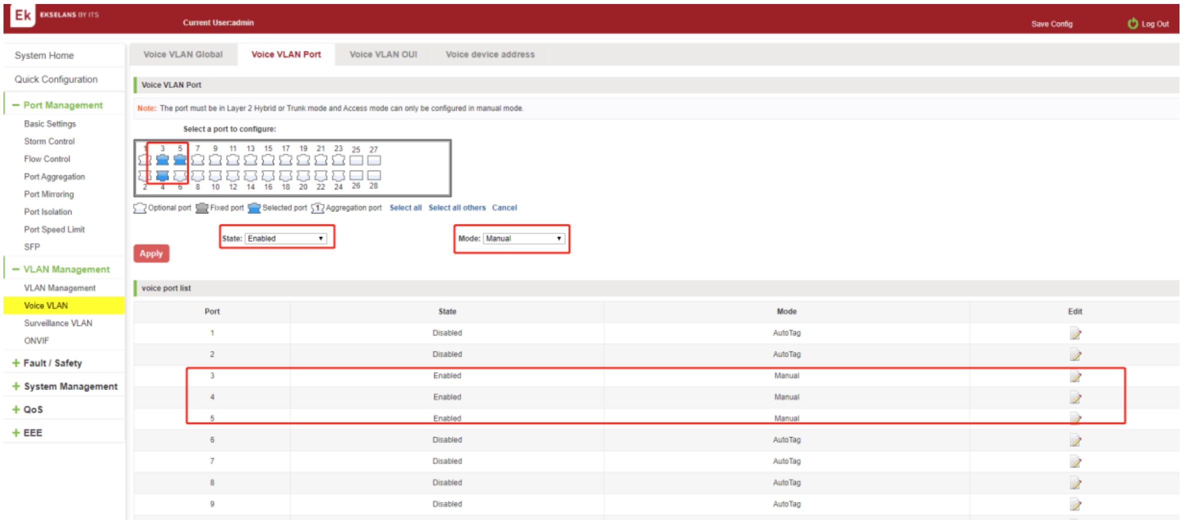
Figure 5-11: view voice VLAN information.

To configure the voice VLAN global steps as follows:

Step1:in the voice VLAN state TEXT BOX, click ON the "OFF" to "ON", Step2:in the voice VLAN ID text box, enter the ID, such as 111; step3: in the voice VLAN COS text box, choose 6; step 4:in the aging time text box, enter aging time, such as 1000; step5: click on Apply.

Configure voice VLAN port.

Click on the navigation bar "VLAN Management" "Voice VLAN" " Voice VLAN port" to configure the voice VLAN port;



Voice VLAN Port

Note: The port must be in Layer 2 Hybrid or Trunk mode and Access mode can only be configured in manual mode.

Select a port to configure:

State: Enabled

Mode: Manual

voice port list

Port	State	Mode	Edit
1	Disabled	AutoTag	
2	Disabled	AutoTag	
3	Enabled	Manual	
4	Enabled	Manual	
5	Enabled	Manual	
6	Disabled	AutoTag	
7	Disabled	AutoTag	
8	Disabled	AutoTag	
9	Disabled	AutoTag	

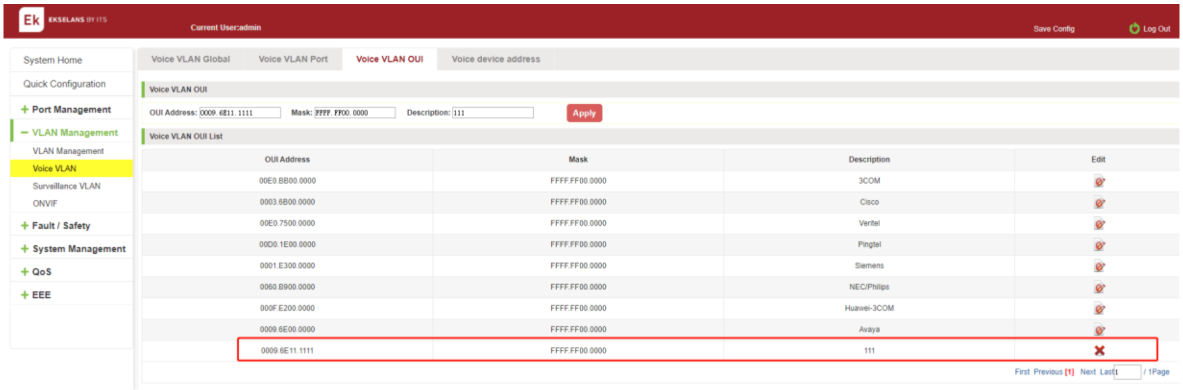
Figure 5-12: configure voice VLAN port.

To configure the voice VLAN port steps as follows:

Step1: select ports to configure, step2:in the state text box, choose enable step 3: in the mode text box, choose manual. step 3:click on Apply.

Configure voice VLAN OUI.

Click on the navigation bar "VLAN Management" "Voice VLAN" " Voice VLAN OUI" to configurethe voice VLAN OUI;



Voice VLAN OUI

OUI Address: 0009.6E11.1111 Mask: FFFF.FF00.0000 Description: 111

Voice VLAN OUI List

OUI Address	Mask	Description	Edit
00E0.BB00.0000	FFFF.FF00.0000	3COM	
0003.6B00.0000	FFFF.FF00.0000	Cisco	
00E0.7500.0000	FFFF.FF00.0000	Veritel	
00D0.1E00.0000	FFFF.FF00.0000	Pingtel	
0001.E300.0000	FFFF.FF00.0000	Siemens	
0060.B900.0000	FFFF.FF00.0000	NEC/Philips	
000F.E200.0000	FFFF.FF00.0000	Huawei-3COM	
0009.6E00.0000	FFFF.FF00.0000	Avaya	
0009.6E11.1111	FFFF.FF00.0000	111	✕

Figure 5-13: configure voice VLAN OUI.

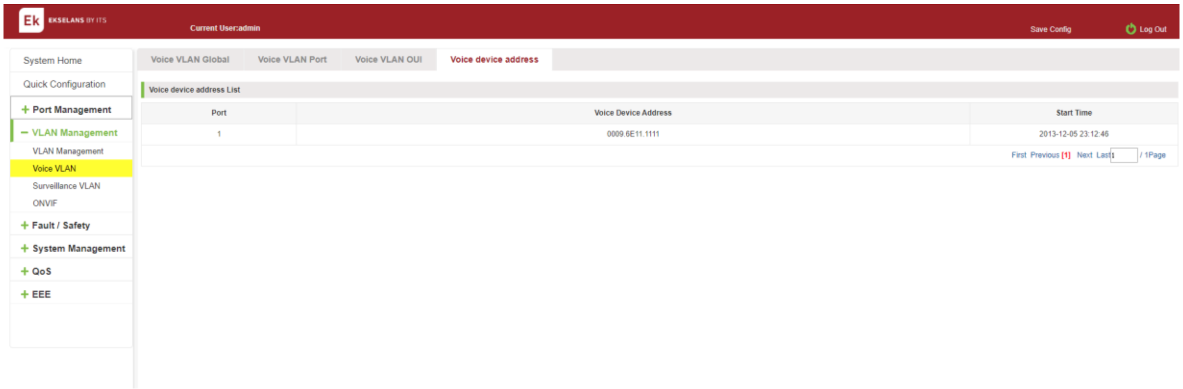
To configure the voice VLAN OUI steps as follows:

Step1: In the OUI address text box, enter OUI address, such as 0009.6E11.1111.

Step2: In the mask text box ,enter the mask ,such as FFFF.FF00.0000;step 3:in the description text box ,enter the description ,such as testOUI;step4:click Apply;

Voice device address.

Click on the navigation bar "VLAN Management" "Voice VLAN" " Voice device address" to view the voice device:



Voice device address List

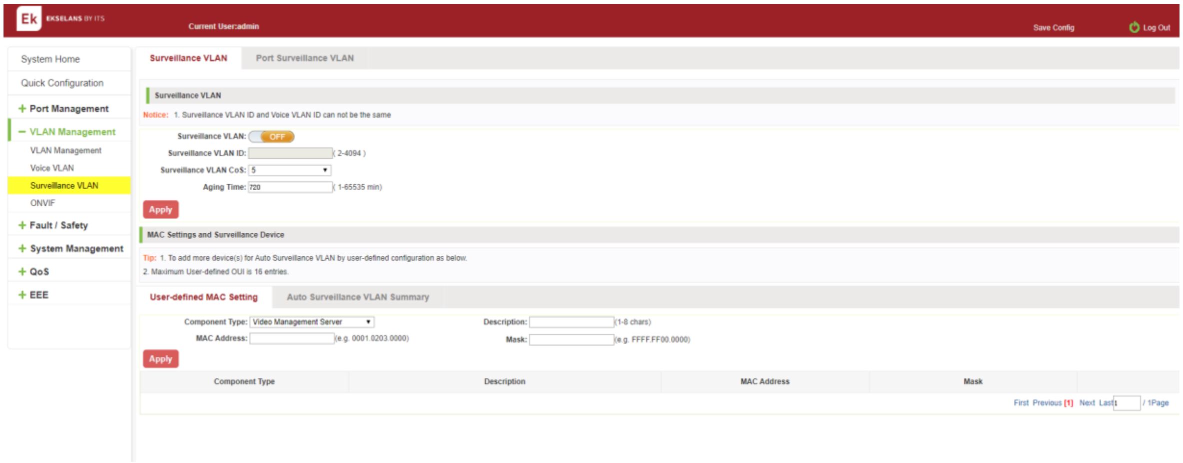
Port	Voice Device Address	Start Time
1	0009.6E11.1111	2013-12-05 23:12:46

Figure 5-14: VOICE VLAN address.

Surveillance VLAN.

View surveillance VLAN information.

Click on the navigation bar "VLAN Management" "surveillance VLAN" " surveillance VLAN" to view the switch configured:



Surveillance VLAN

Notice: 1. Surveillance VLAN ID and Voice VLAN ID can not be the same

Surveillance VLAN: OFF
Surveillance VLAN ID: (2-4094)
Surveillance VLAN CoS: 5
Aging Time: 720 (1-65535 min)

MAC Settings and Surveillance Device

Tip: 1. To add more device(s) for Auto Surveillance VLAN by user-defined configuration as below.
2. Maximum User-defined OUI is 16 entries.

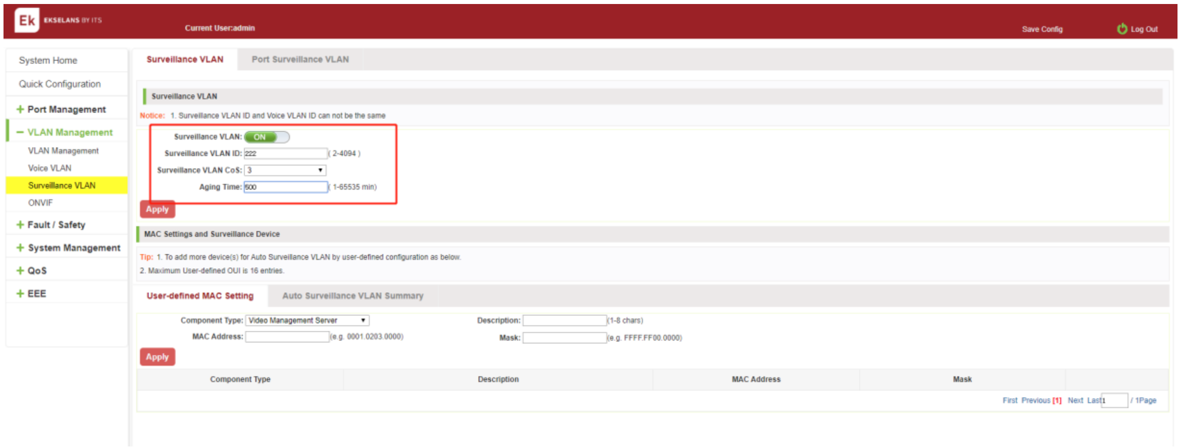
Component Type: Video Management Server
Description: (1-8 chars)
MAC Address: (e.g. 0001.0203.0000)
Mask: (e.g. FFFF.FF00.0000)

Component Type	Description	MAC Address	Mask

Figure 5-15: surveillance VLAN information.

Configure surveillance VLAN.

Click on the navigation bar "VLAN Management" "surveillance VLAN" " surveillance VLAN" to configure the switch surveillance VLAN.



Surveillance VLAN

Notice: 1. Surveillance VLAN ID and Voice VLAN ID can not be the same

Surveillance VLAN: ON
Surveillance VLAN ID: 222 (2-4094)
Surveillance VLAN CoS: 3
Aging Time: 500 (1-65535 min)

MAC Settings and Surveillance Device

Tip: 1. To add more device(s) for Auto Surveillance VLAN by user-defined configuration as below.
2. Maximum User-defined OUI is 16 entries.

Component Type: Video Management Server
Description: (1-8 chars)
MAC Address: (e.g. 0001.0203.0000)
Mask: (e.g. FFFF.FF00.0000)

Component Type	Description	MAC Address	Mask

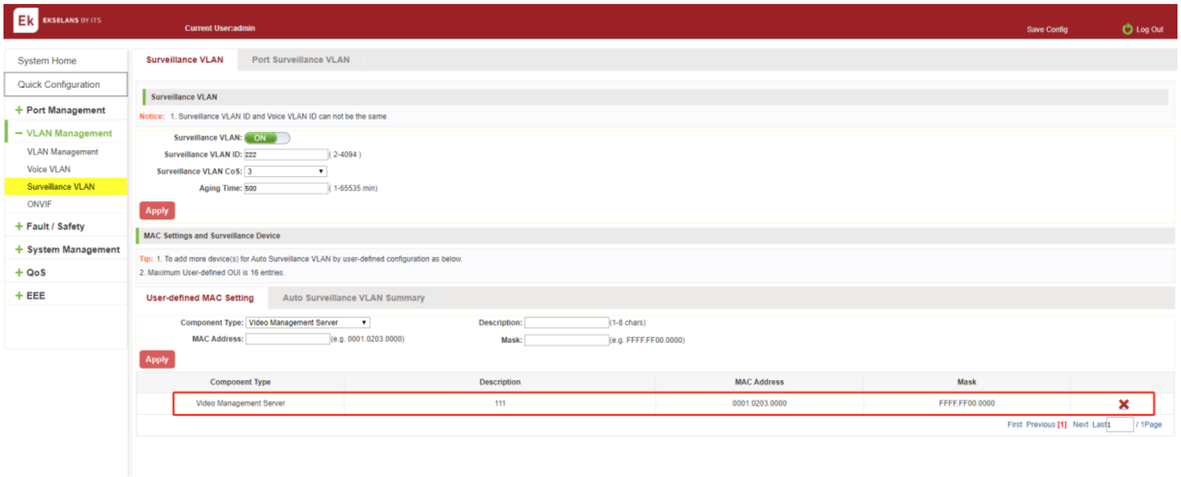
Figure 5-16: configure surveillance VLAN.

To configure the surveillance VLAN steps as follows:

Step1:in the surveillance VLAN TEXT BOX, click ON the "OFF" to "ON", Step2:in the surveillance VLAN ID text box, enter the ID, such as 222; step3: in the surveillance VLAN COS text box, choose 3; step 4:in the aging time text box, enter aging time, such as 500; step5: click on Apply.

MAC Settings and Surveillance Device.

Click on the navigation bar "VLAN Management" "surveillance VLAN" " surveillance VLAN" “MAC Settings and Surveillance Device” to configure the user-defined mac settings.



Surveillance VLAN

Notice: 1. Surveillance VLAN ID and Voice VLAN ID can not be the same

Surveillance VLAN: ON

Surveillance VLAN ID: 222 (2-4094)

Surveillance VLAN CoS: 3

Aging Time: 500 (1-65535 min)

MAC Settings and Surveillance Device

Tip: 1. To add more device(s) for Auto Surveillance VLAN by user-defined configuration as below.
2. Maximum User-defined OUI is 16 entries.

Component Type: Video Management Server   Description: (1-8 chars)

MAC Address: (e.g. 0001.0203.0000)   Mask: (e.g. FFFF.FF00.0000)

Component Type	Description	MAC Address	Mask	
Video Management Server	111	0001.0203.0000	FFFF.FF00.0000	✗

Figure 5-17: configure the user-defined mac settings.

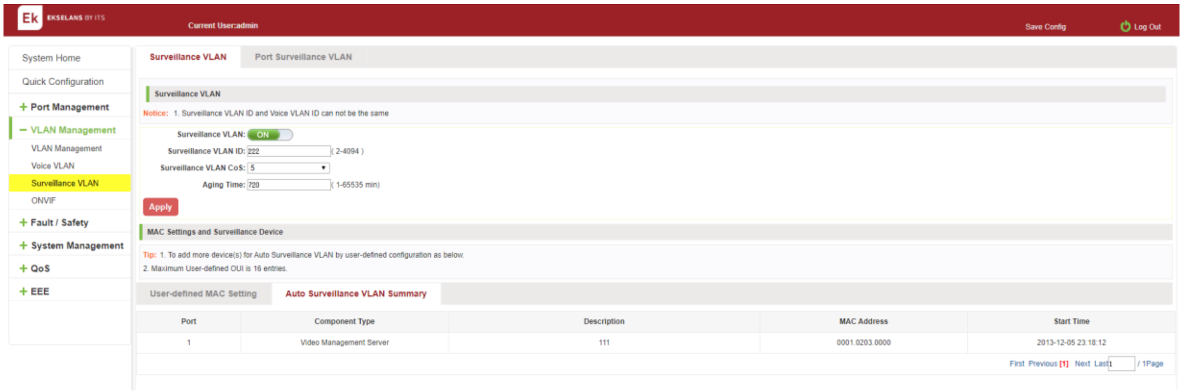
To configure the surveillance VLAN steps as follows:

Step1:in the component type EXT BOX, choose video management server; Step2: in the description text box, enter testOUI; step 3: in the mac address text box, enter mac address such as 0001.0203.0000. step4: in the mask text box ,enter the mask ,such as FFFF.F000.0000,step 5:click on Apply;

MAC Settings and Surveillance Device.

Click on the navigation bar "VLAN Management" "surveillance VLAN" " surveillance VLAN" “

MAC Settings and Surveillance Device” to view the information:



Surveillance VLAN

Notice: 1. Surveillance VLAN ID and Voice VLAN ID can not be the same

Surveillance VLAN: ON

Surveillance VLAN ID: 222 (2-4094)

Surveillance VLAN CoS: 5

Aging Time: 720 (1-65535 min)

MAC Settings and Surveillance Device

Tip: 1. To add more device(s) for Auto Surveillance VLAN by user-defined configuration as below.
2. Maximum User-defined OUI is 16 entries.

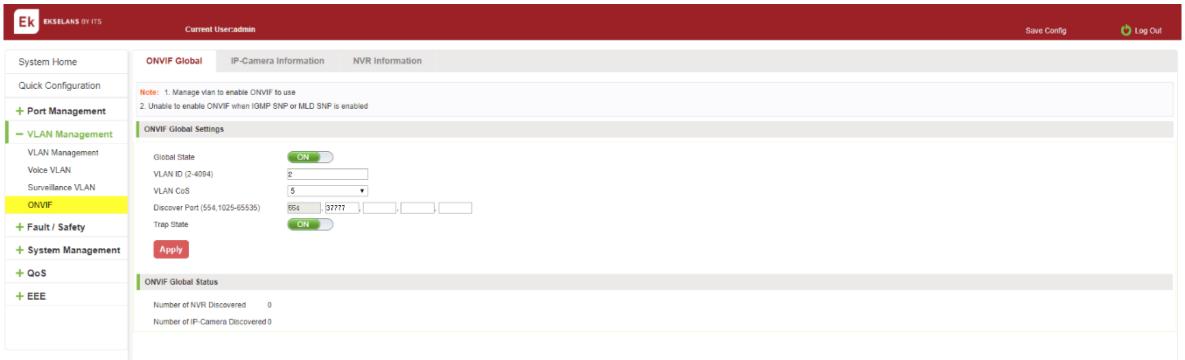
Port	Component Type	Description	MAC Address	Start Time
1	Video Management Server	111	0001.0203.0000	2013-12-05 23:18:12

Figure 5-18: configure the user-defined mac settings.

ONVIF.

View ONVIF.

Click on the navigation bar "VLAN Management" "ONVIF" " ONVIF Global" to view the switch configured:



Note: 1. Manage vlan to enable ONVIF to use
2. Unable to enable ONVIF when IGMP SNP or MLD SNP is enabled

ONVIF Global Settings

Global State: ON
VLAN ID (2-4094): 2
VLAN CoS: 5
Discover Port (554,1025-65535): 554, 37777
Trap State: ON

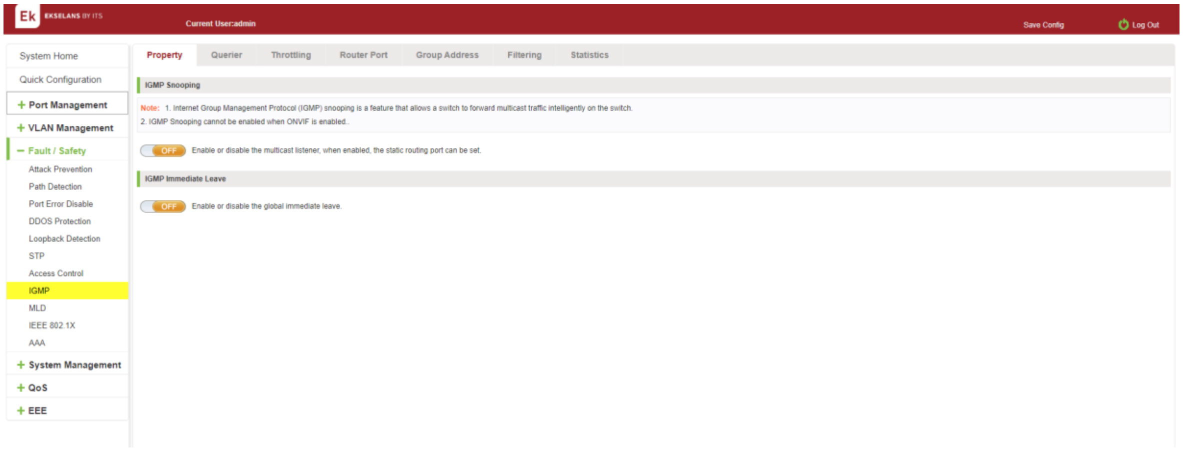
ONVIF Global Status

Number of NVR Discovered 0
Number of IP-Camera Discovered 0

Figure 5-19: ONVIF information.

To configure the ONVIF steps as follows:

Step1: Turn off IGMP and MLD functions



IGMP Snooping

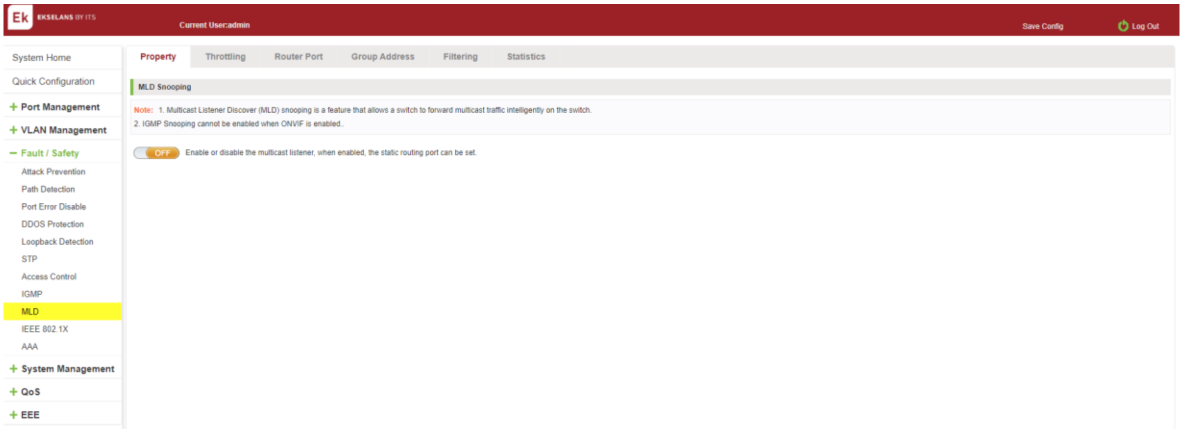
Note: 1. Internet Group Management Protocol (IGMP) snooping is a feature that allows a switch to forward multicast traffic intelligently on the switch.
2. IGMP Snooping cannot be enabled when ONVIF is enabled..

OFF Enable or disable the multicast listener, when enabled, the static routing port can be set.

IGMP Immediate Leave

OFF Enable or disable the global immediate leave.

Figure 5-20: igmp.

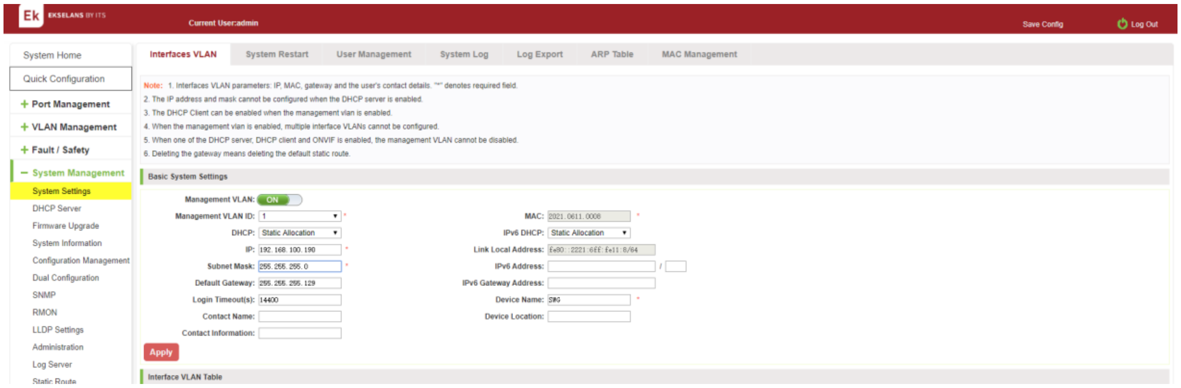


Note: 1. Multicast Listener Discover (MLD) snooping is a feature that allows a switch to forward multicast traffic intelligently on the switch.
2. IGMP Snooping cannot be enabled when ONVIF is enabled..

OFF Enable or disable the multicast listener, when enabled, the static routing port can be set.

Figure 5-21: mld.

Step2: Enable Management VLAN.



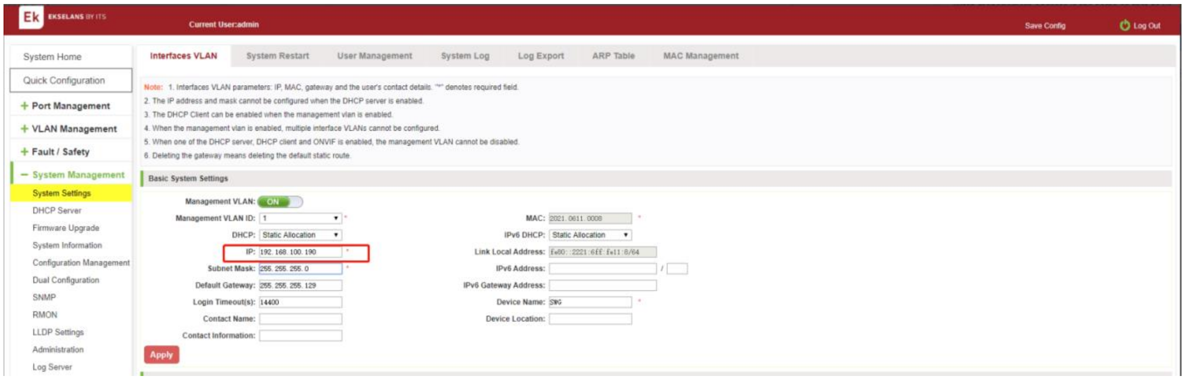
Note: 1. Interfaces VLAN parameters: IP, MAC, gateway and the user's contact details. "*" denotes required field.
2. The IP address and mask cannot be configured when the DHCP server is enabled.
3. The DHCP Client can be enabled when the management vlan is enabled.
4. When the management vlan is enabled, multiple interface VLANs cannot be configured.
5. When one of the DHCP server, DHCP client and ONVIF is enabled, the management VLAN cannot be disabled.
6. Deleting the gateway means deleting the default static route.

Management VLAN: ON
Management VLAN ID: 1 *
DHCP: Static Allocation
IP: 192.168.100.190 *
Subnet Mask: 255.255.255.0 *
Default Gateway: 255.255.255.129
Login Timeout(s): 14400
Contact Name:
Contact Information:

MAC: 2021.0611.0008 *
IPv6 DHCP: Static Allocation
Link Local Address: fe80::2221:6ff:fe11:8/64
IPv6 Address: /
IPv6 Gateway Address:
Device Name: SWG *
Device Location:

Figure 5-22: management vlan.

Step3: Confirm that the IP address segment of switch management address is the same as that of IPC and NVR.



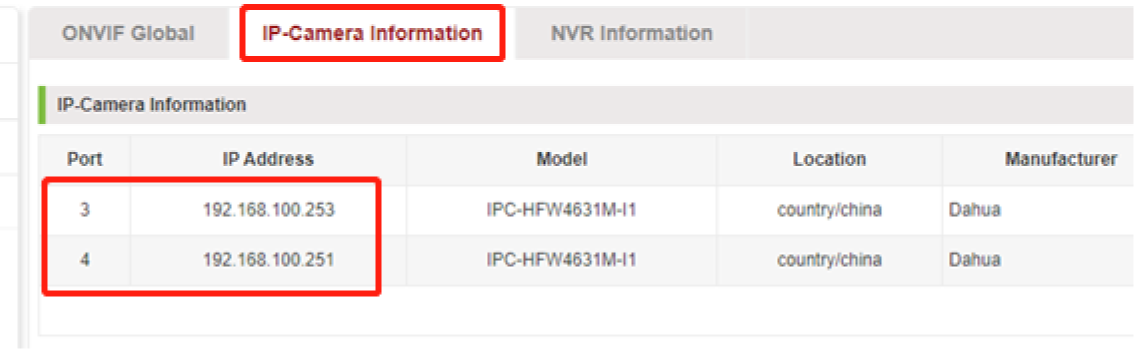
Note: 1. Interfaces VLAN parameters: IP, MAC, gateway and the user's contact details. "*" denotes required field.
2. The IP address and mask cannot be configured when the DHCP server is enabled.
3. The DHCP Client can be enabled when the management vlan is enabled.
4. When the management vlan is enabled, multiple interface VLANs cannot be configured.
5. When one of the DHCP server, DHCP client and ONVIF is enabled, the management VLAN cannot be disabled.
6. Deleting the gateway means deleting the default static route.

Basic System Settings

Management VLAN: ON
Management VLAN ID: 1 *
DHCP: Static Allocation
IP: 192. 168. 100. 190 *
Subnet Mask: 255. 255. 255. 0 *
Default Gateway: 255. 255. 255. 129
Login Timeout(s): 14400
Contact Name:
Contact Information:

MAC: 2021. 0611. 0008 *
IPv6 DHCP: Static Allocation
Link Local Address: fe80::2221:6ff:fe11:8/64
IPv6 Address: /
IPv6 Gateway Address:
Device Name: SWG *
Device Location:

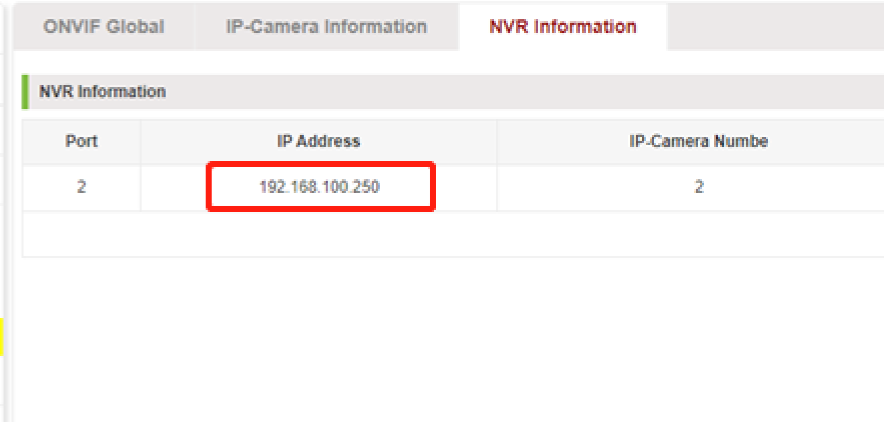
Figure 5-23: management vlan.



IP-Camera Information

Port	IP Address	Model	Location	Manufacturer
3	192.168.100.253	IPC-HFW4631M-I1	country/china	Dahua
4	192.168.100.251	IPC-HFW4631M-I1	country/china	Dahua

Figure 5-24: ip-camera information.

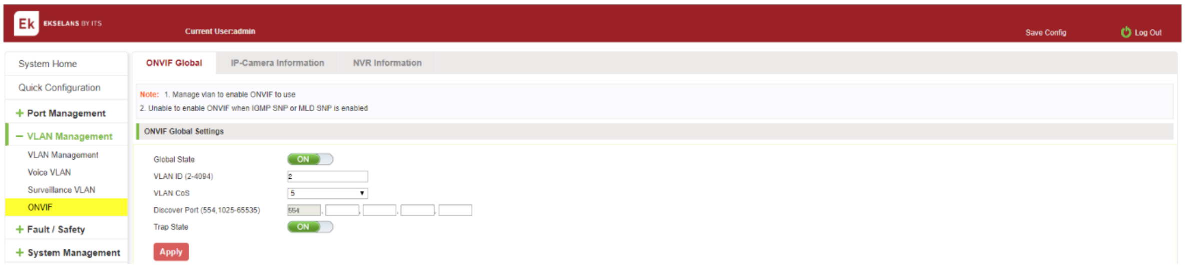


NVR Information

Port	IP Address	IP-Camera Numbe
2	192.168.100.250	2

Figure 5-25: nvr information.

Step4: Configure the VLAN ID



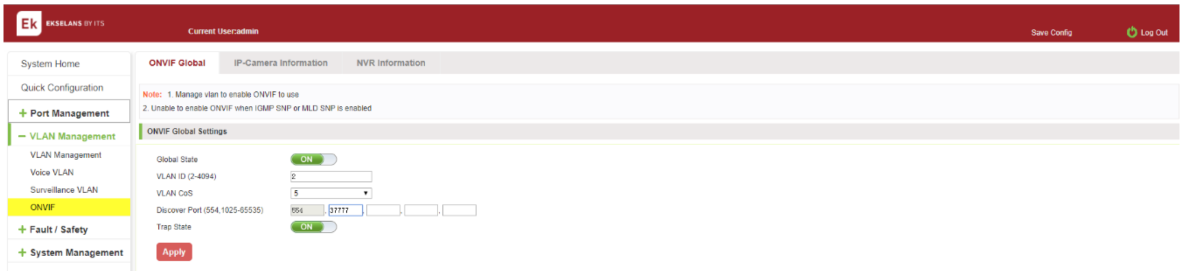
Note: 1. Manage vlan to enable ONVIF to use
2. Unable to enable ONVIF when IGMP SNP or MLD SNP is enabled

ONVIF Global Settings

Global State: ON
VLAN ID (2-4094): 2
VLAN CoS: 5
Discover Port (554,1025-65535): 554
Trap State: ON

Figure 5-26: onvif global.

Step5: Configure the port number used by the onvif protocol, The default is 554.



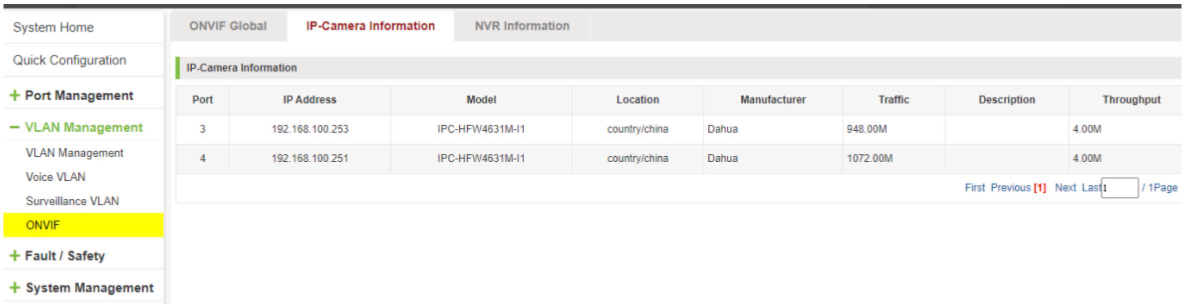
Note: 1. Manage vlan to enable ONVIF to use
2. Unable to enable ONVIF when IGMP SNP or MLD SNP is enabled

ONVIF Global Settings

Global State: ON
VLAN ID (2-4094): 2
VLAN CoS: 5
Discover Port (554,1025-65535): 554, 37777
Trap State: ON

View IP-Camera information.

Click on the navigation bar "VLAN Management" "ONVIF" " IP-Camera Information" to view the IP-Camera information:



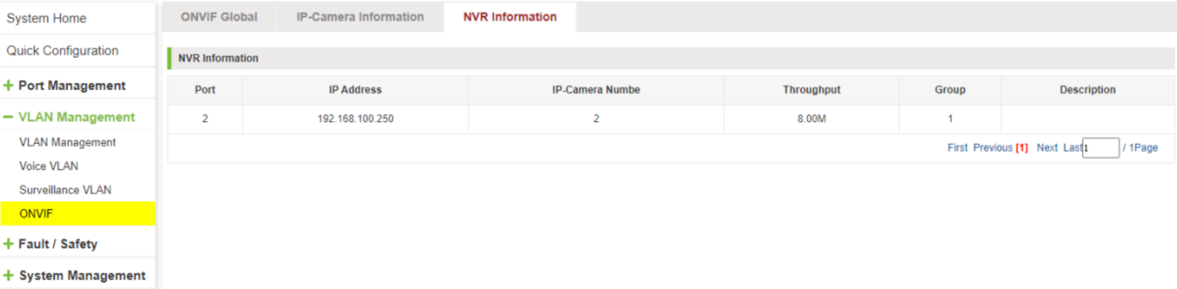
IP-Camera Information

Port	IP Address	Model	Location	Manufacturer	Traffic	Description	Throughput
3	192.168.100.253	IPC-HFW4631M-I1	country/china	Dahua	948.00M		4.00M
4	192.168.100.251	IPC-HFW4631M-I1	country/china	Dahua	1072.00M		4.00M

Figure 5-27: IP-Camera information.

View Nvr information information.

Click on the navigation bar "VLAN Management" "ONVIF" " NVR infromation" to view the switch NVR information:



NVR Information

Port	IP Address	IP-Camera Numbe	Throughput	Group	Description
2	192.168.100.250	2	8.00M	1	

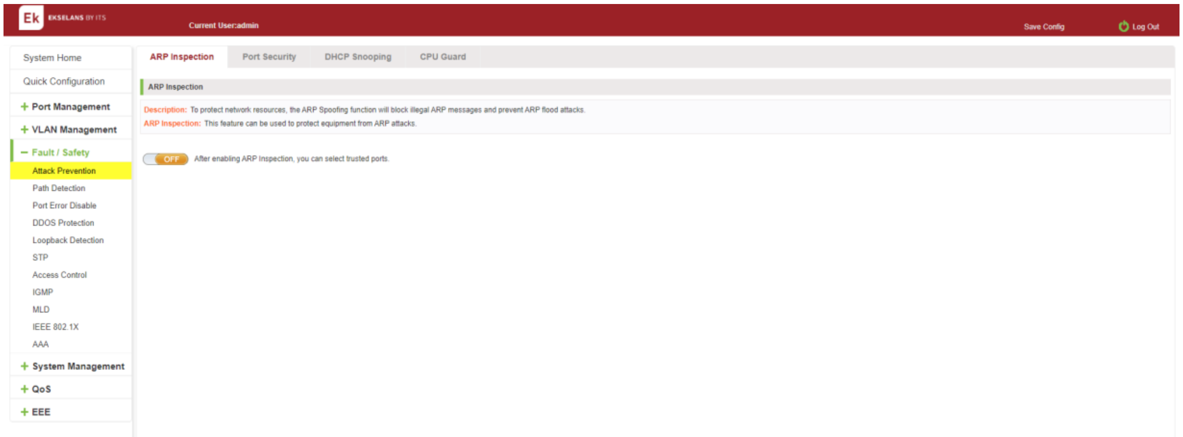
Figure 5-28: NVR information.

Fault / safety.

ATTACK PREVENTION.

VIEW ARP CONFIGURATION.

Click the "Fault/Safety" "Attack Prevention " "ARP Inspection " to check the current switches has been configured for ARP information, this feature is turned off by default.



ARP Inspection

Description: To protect network resources, the ARP Spoofing function will block illegal ARP messages and prevent ARP flood attacks.

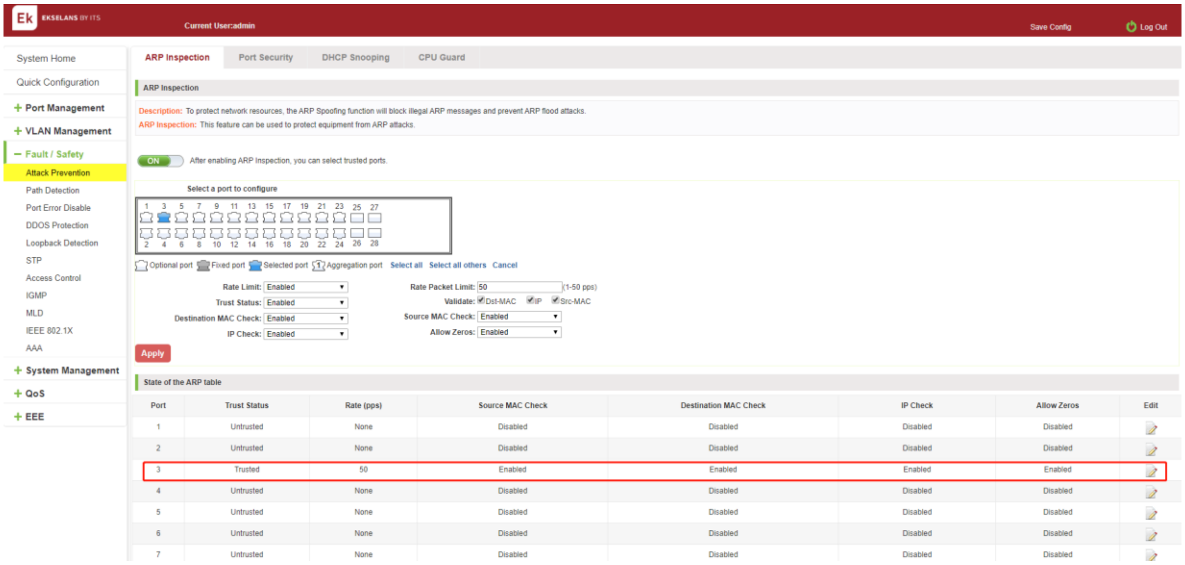
ARP Inspection: This feature can be used to protect equipment from ARP attacks.

After enabling ARP inspection, you can select trusted ports.

Figure 6-1: View port ARP Inspection information.

ARP INSPECTION FUNCTION.

In the ARP Inspection configuration, enable this function and then selected a port to configure some parameters .Click the "Apply" button to complete the configuration.



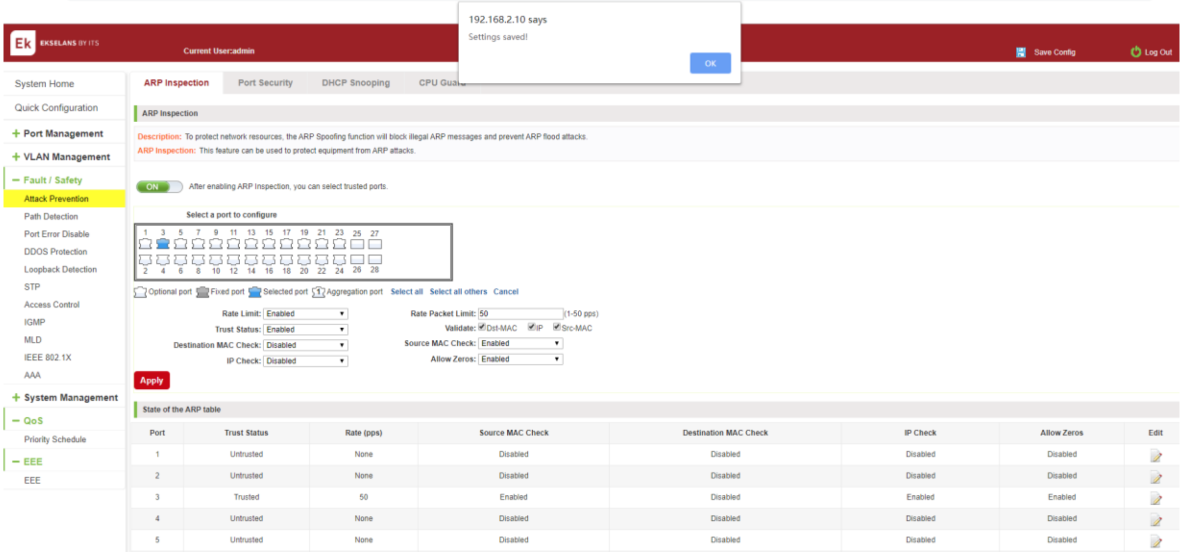
Description: To protect network resources, the ARP Spoofing function will block illegal ARP messages and prevent ARP flood attacks.
ARP Inspection: This feature can be used to protect equipment from ARP attacks.

After enabling ARP Inspection, you can select trusted ports.

Rate Limit: Enabled
Trust Status: Enabled
Destination MAC Check: Enabled
IP Check: Enabled
Rate Packet Limit: 50 (1-50 pps)
Validate: ☑Dst-MAC ☑IP ☑Src-MAC
Source MAC Check: Enabled
Allow Zeros: Enabled

Port	Trust Status	Rate (pps)	Source MAC Check	Destination MAC Check	IP Check	Allow Zeros	Edit
1	Untrusted	None	Disabled	Disabled	Disabled	Disabled	
2	Untrusted	None	Disabled	Disabled	Disabled	Disabled	
3	Trusted	50	Enabled	Enabled	Enabled	Enabled	
4	Untrusted	None	Disabled	Disabled	Disabled	Disabled	
5	Untrusted	None	Disabled	Disabled	Disabled	Disabled	
6	Untrusted	None	Disabled	Disabled	Disabled	Disabled	
7	Untrusted	None	Disabled	Disabled	Disabled	Disabled	

Figure 6-2: ARP Inspection configuration.



192.168.2.10 says
Settings saved!

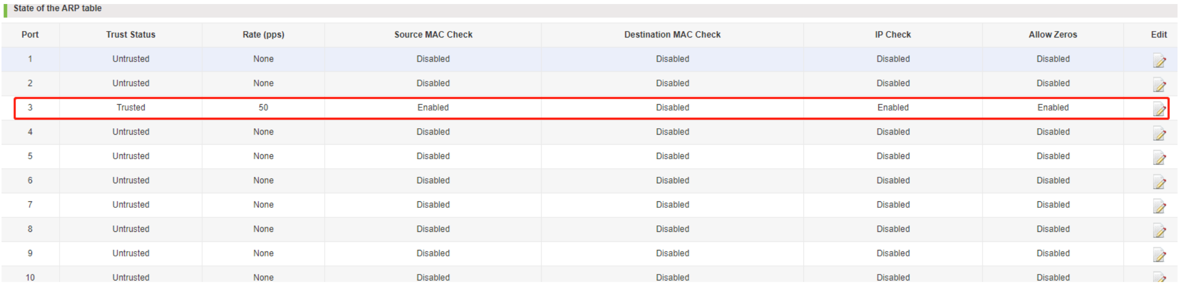
Description: To protect network resources, the ARP Spoofing function will block illegal ARP messages and prevent ARP flood attacks.
ARP Inspection: This feature can be used to protect equipment from ARP attacks.

After enabling ARP Inspection, you can select trusted ports.

Rate Limit: Enabled
Trust Status: Enabled
Destination MAC Check: Disabled
IP Check: Disabled
Rate Packet Limit: 50 (1-50 pps)
Validate: ☑Dst-MAC ☑IP ☑Src-MAC
Source MAC Check: Enabled
Allow Zeros: Enabled

Port	Trust Status	Rate (pps)	Source MAC Check	Destination MAC Check	IP Check	Allow Zeros	Edit
1	Untrusted	None	Disabled	Disabled	Disabled	Disabled	
2	Untrusted	None	Disabled	Disabled	Disabled	Disabled	
3	Trusted	50	Enabled	Disabled	Enabled	Enabled	
4	Untrusted	None	Disabled	Disabled	Disabled	Disabled	
5	Untrusted	None	Disabled	Disabled	Disabled	Disabled	

Figure 6-3: Change ARP Inspection configure.



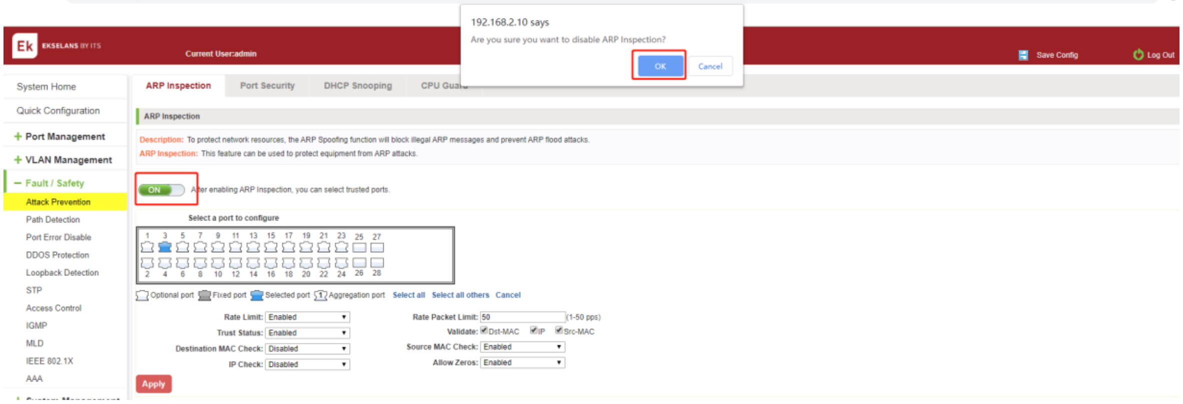
State of the ARP table

Port	Trust Status	Rate (pps)	Source MAC Check	Destination MAC Check	IP Check	Allow Zeros	Edit
1	Untrusted	None	Disabled	Disabled	Disabled	Disabled	
2	Untrusted	None	Disabled	Disabled	Disabled	Disabled	
3	Trusted	50	Enabled	Disabled	Enabled	Enabled	
4	Untrusted	None	Disabled	Disabled	Disabled	Disabled	
5	Untrusted	None	Disabled	Disabled	Disabled	Disabled	
6	Untrusted	None	Disabled	Disabled	Disabled	Disabled	
7	Untrusted	None	Disabled	Disabled	Disabled	Disabled	
8	Untrusted	None	Disabled	Disabled	Disabled	Disabled	
9	Untrusted	None	Disabled	Disabled	Disabled	Disabled	
10	Untrusted	None	Disabled	Disabled	Disabled	Disabled	

Figure 6-4: Change ARP Inspection configure success.

DISABLE ARP INSPECTION FUNCTION.

In the ARP Inspection configuration table, click the button from on to off to disable the ARP Inspection and then click the "OK" button to complete the configuration.



192.168.2.10 says

Are you sure you want to disable ARP Inspection?

OK Cancel

Current User:admin

ARP Inspection

Description: To protect network resources, the ARP Spoofing function will block illegal ARP messages and prevent ARP flood attacks.

ARP Inspection: This feature can be used to protect equipment from ARP attacks.

ON After enabling ARP Inspection, you can select trusted ports.

Select a port to configure

Rate Limit: Enabled

Trust Status: Enabled

Destination MAC Check: Disabled

IP Check: Disabled

Rate Packet Limit: 50 (1-50 pps)

Validate: ☑ Dst-MAC ☑ IP ☑ Src-MAC

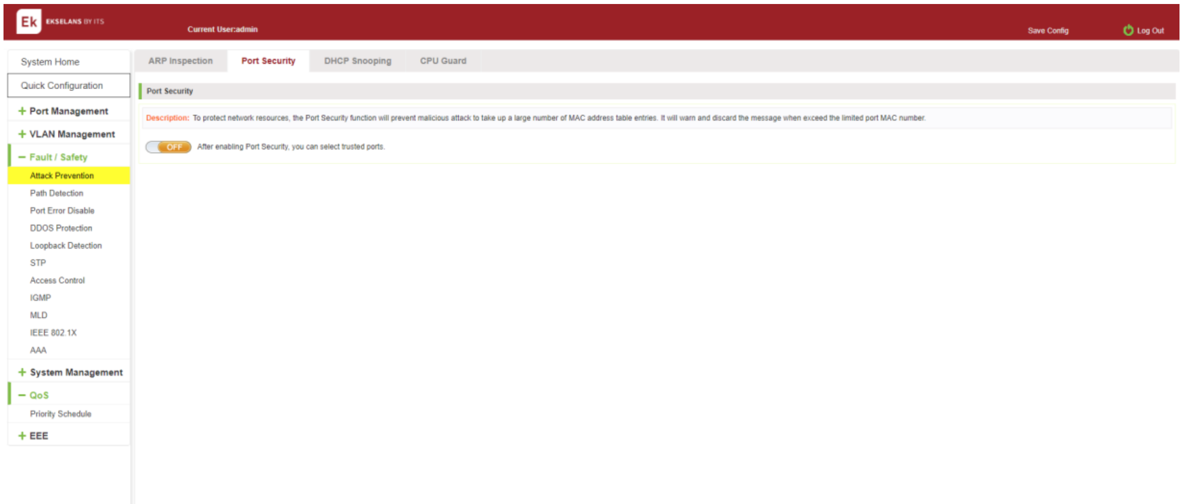
Source MAC Check: Enabled

Allow Zeros: Enabled

Figure 6-5: Disable ARP Inspection function.

CONFIGURATION PORT SECURITY.

Click the "Fault/Safety" "Attack prevention" "Port Security", configure the switch port security:



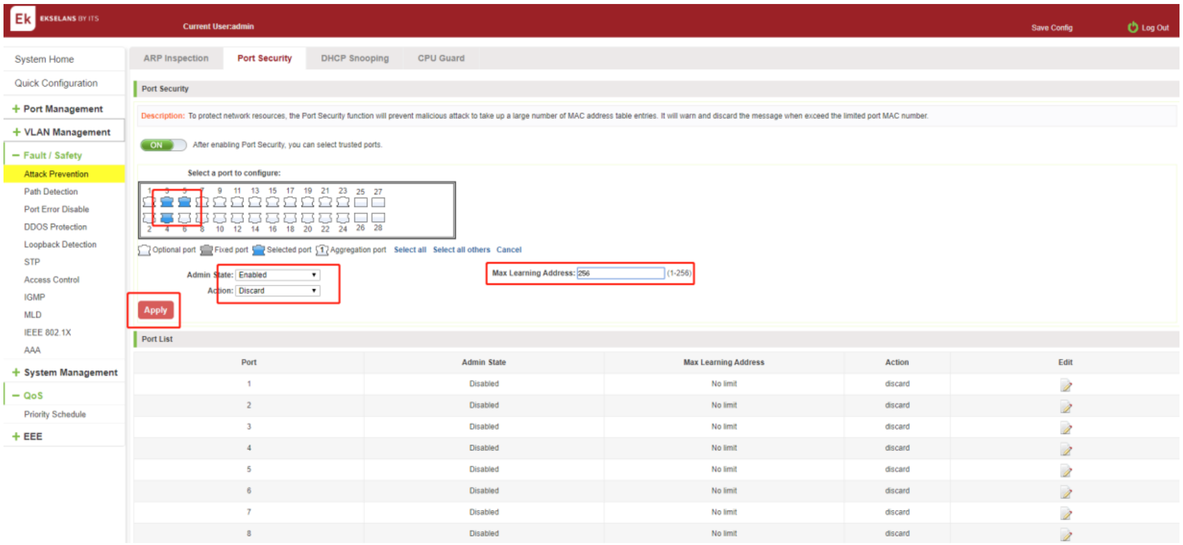
Port Security

Description: To protect network resources, the Port Security function will prevent malicious attack to take up a large number of MAC address table entries. It will warn and discard the message when exceed the limited port MAC number.

After enabling Port Security, you can select trusted ports.

Figure 6-6: Port security configuration.

In the configuration pag, selected one or more ports, enable the admin state and configure the port max learning address. Finally click "Apply" button.



Port Security

Description: To protect network resources, the Port Security function will prevent malicious attack to take up a large number of MAC address table entries. It will warn and discard the message when exceed the limited port MAC number.

After enabling Port Security, you can select trusted ports.

Select a port to configure:

Admin State: Enabled

Action: Discard

Max Learning Address: 256 (1-256)

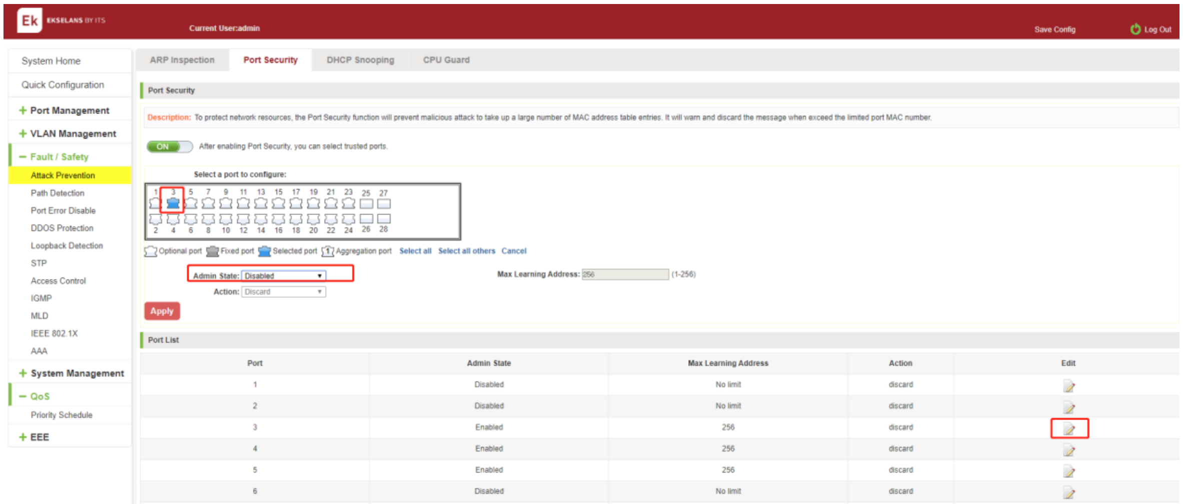
Port List

Port	Admin State	Max Learning Address	Action	Edit
1	Disabled	No limit	discard	✎
2	Disabled	No limit	discard	✎
3	Disabled	No limit	discard	✎
4	Disabled	No limit	discard	✎
5	Disabled	No limit	discard	✎
6	Disabled	No limit	discard	✎
7	Disabled	No limit	discard	✎
8	Disabled	No limit	discard	✎

Figure 6-7: Port security manual configuration.

CHANGE PORT SECURITY STATUS.

In the port list, select the port to edit, change some parameters or disable the port security and click the button of "Apply".



Port Security

Description: To protect network resources, the Port Security function will prevent malicious attack to take up a large number of MAC address table entries. It will warn and discard the message when exceed the limited port MAC number.

ON After enabling Port Security, you can select trusted ports.

Select a port to configure:

Admin State: Disabled

Action: Discard

Max Learning Address: 256 (1-256)

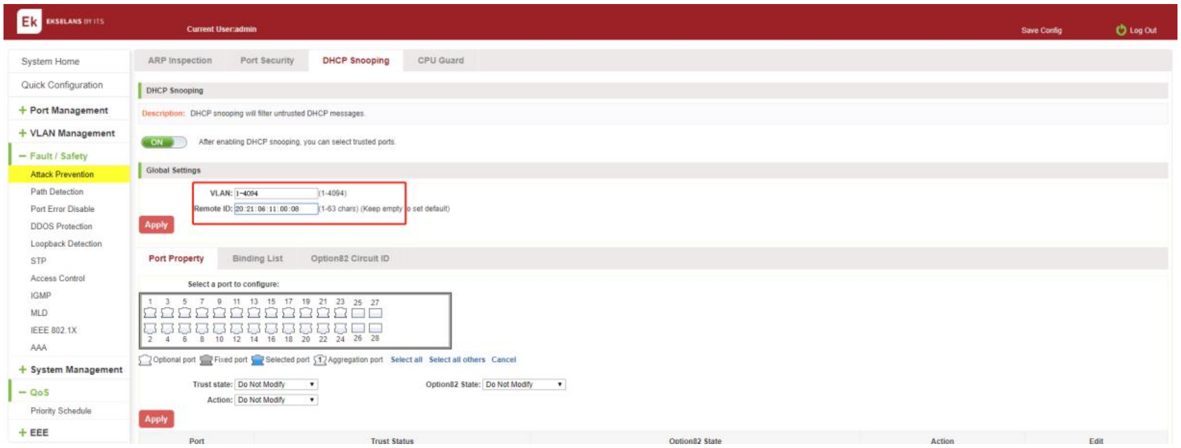
Port List

Port	Admin State	Max Learning Address	Action	Edit
1	Disabled	No limit	discard	
2	Disabled	No limit	discard	
3	Enabled	256	discard	
4	Enabled	256	discard	
5	Enabled	256	discard	
6	Disabled	No limit	discard	

Figure 6-8: Change port security status.

VIEW DHCP snooping CONFIGURATION.

Click the "Fault/Safety" "Attack prevention" "DHCP snooping", the configuration information show the anti DHCP attack:



Current User:admin

DHCP Snooping

Description: DHCP snooping will filter untrusted DHCP messages.

ON After enabling DHCP snooping, you can select trusted ports.

Global Settings

VLAN: 1-4094 (1-4094)
Remote ID: 20:21:06:11:00:08 (1-63 chars) (Keep empty to set default)

Select a port to configure:

Optional port · Fixed port · Selected port · Aggregation port

Trust state: Do Not Modify · Option82 State: Do Not Modify
Action: Do Not Modify

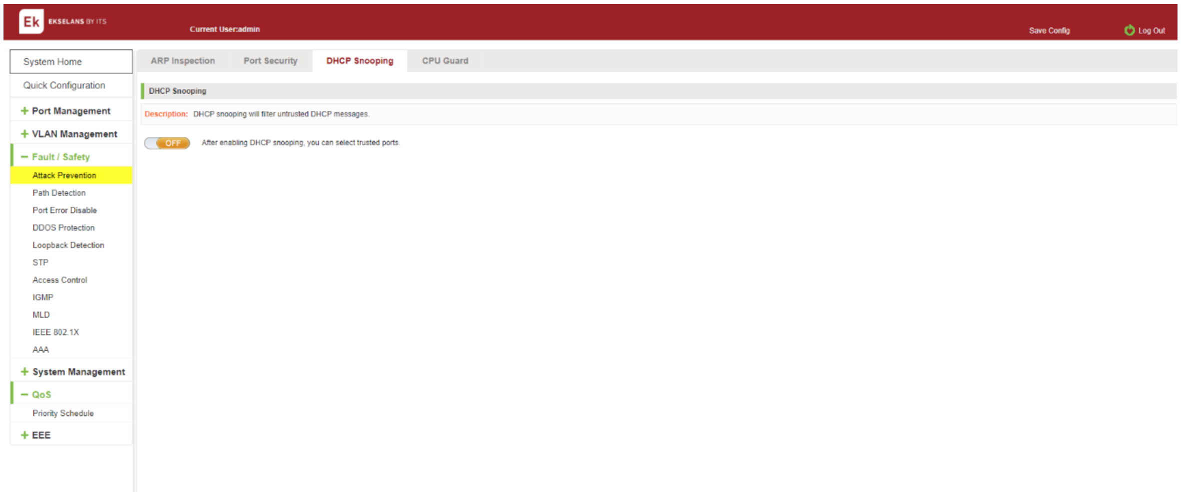
Port	Trust Status	Option82 State	Action	Edit

Figure 6-9: View anti DHCP snooping configuration information.

Display refresh configuration information.

OPEN DHCP snooping FUNCTION.

Click on a "Fault/Safety" "DHCP Snooping "click the button OFF to open the DHCP snooping:



Current User:admin

DHCP Snooping

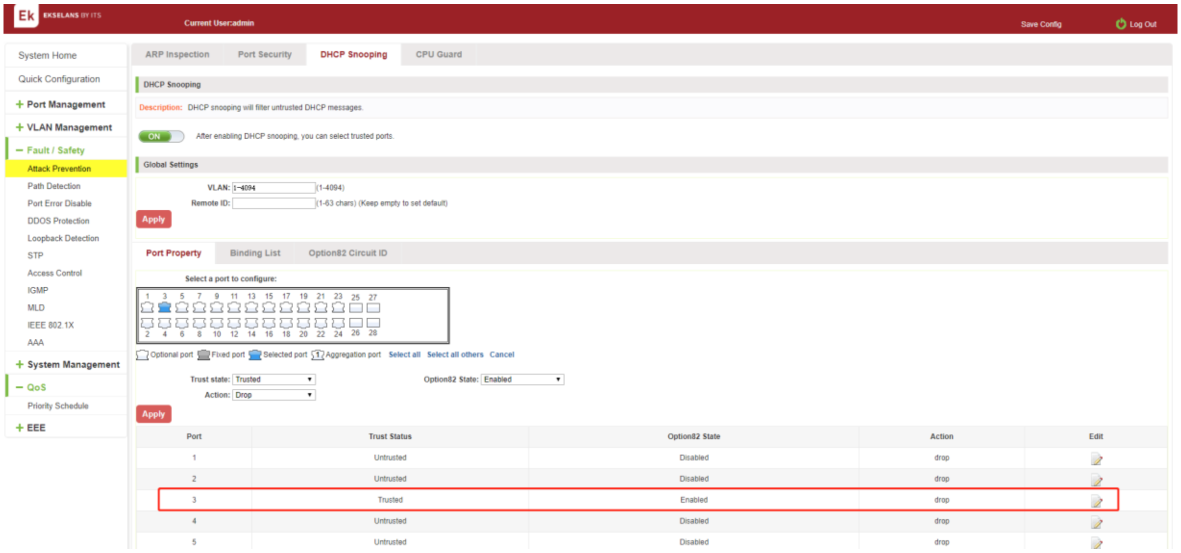
Description: DHCP snooping will filter untrusted DHCP messages.

OFF After enabling DHCP snooping, you can select trusted ports.

Figure 6-10: Activation of DHCP snooping function.

SET THE PORT TO DHCP SNOOPING TRUSTED PORT.

In the trusted port list, select the port that needs to be disabled to prevent DHCP attacks, and click the "Apply" button and enable option82 function



DHCP Snooping

Description: DHCP snooping will filter untrusted DHCP messages.

ON After enabling DHCP snooping, you can select trusted ports.

Global Settings

VLAN: 1-4094 (1-4094)

Remote ID: (1-63 chars) (Keep empty to set default)

Select a port to configure:

Trust state: Trusted

Option82 State: Enabled

Action: Drop

Port	Trust Status	Option82 State	Action	Edit
1	Untrusted	Disabled	drop	
2	Untrusted	Disabled	drop	
3	Trusted	Enabled	drop	
4	Untrusted	Disabled	drop	
5	Untrusted	Disabled	drop	

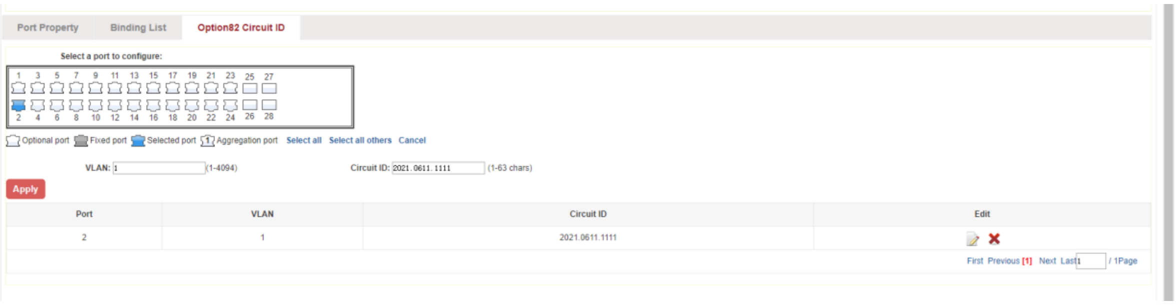
Figure 6-11: Disable anti-illegal DHCP server functions and enable option 82.

The activation of anti DHCP attack function, is the port setting for trust status.

Disable - preventing DHCP attack, is set to a non-trusted state port.

Configure CID information.

Click the "option82 circuit id" button, configure the CID information:



Select a port to configure:

VLAN: 1 (1-4094)

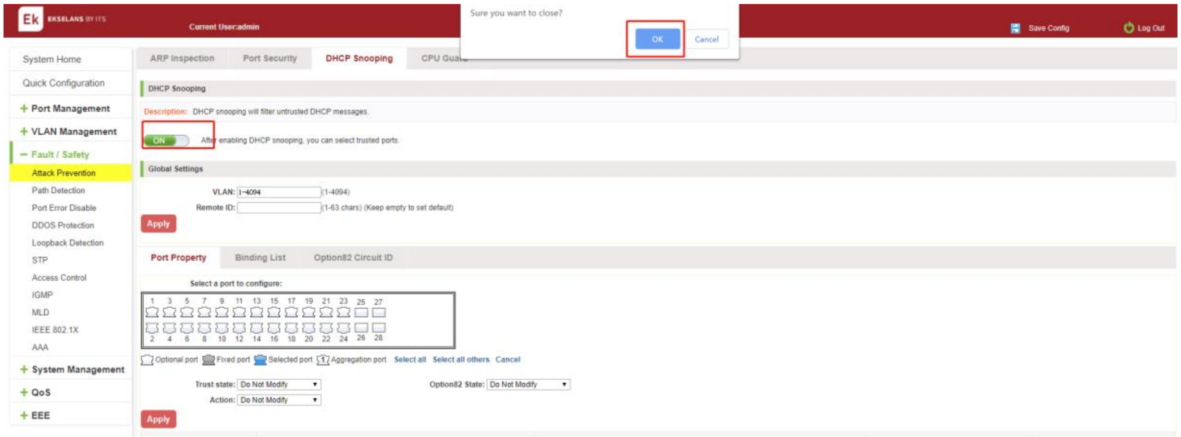
Circuit ID: 2021.0611.1111 (1-63 chars)

Port	VLAN	Circuit ID	Edit
2	1	2021.0611.1111	📝 ✖

Figure 6-12: CID information.

OFF DHCP snooping FUNCTION.

Click the "ON" button, will prevent the DHCP attack function off:



Sure you want to close?

Description: DHCP snooping will filter untrusted DHCP messages.

After enabling DHCP snooping, you can select trusted ports.

VLAN: 1-4094 (1-4094)

Remote ID: (1-63 chars) (Keep empty to set default)

Select a port to configure:

Trust state: Do Not Modify

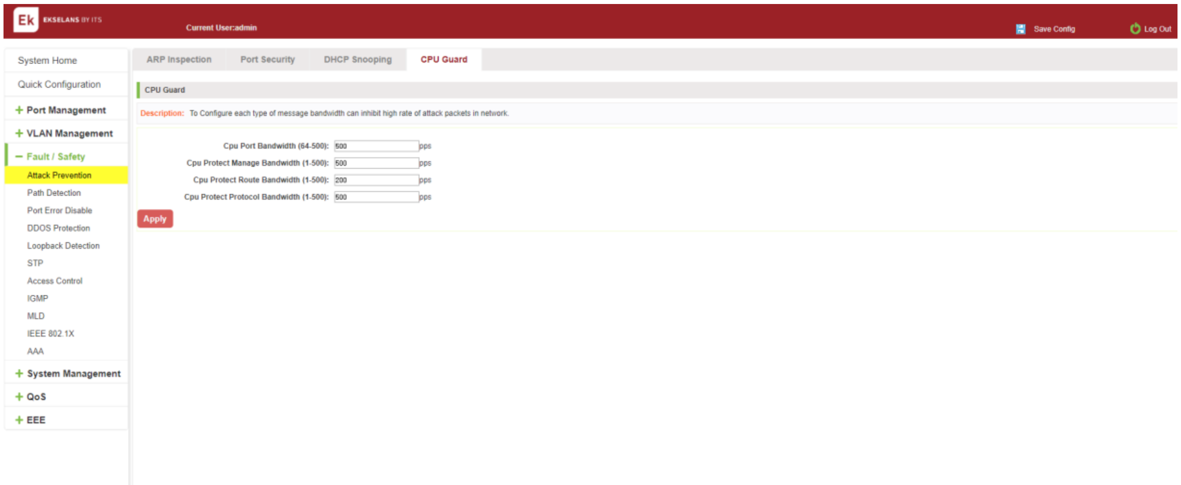
Action: Do Not Modify

Option82 State: Do Not Modify

Figure 6-13: Off DHCP snooping function.

CPU GUARD.

Click the "Fault/Safety" "Attack prevention" "CPU Guard", the configuration information show the CPU guard.



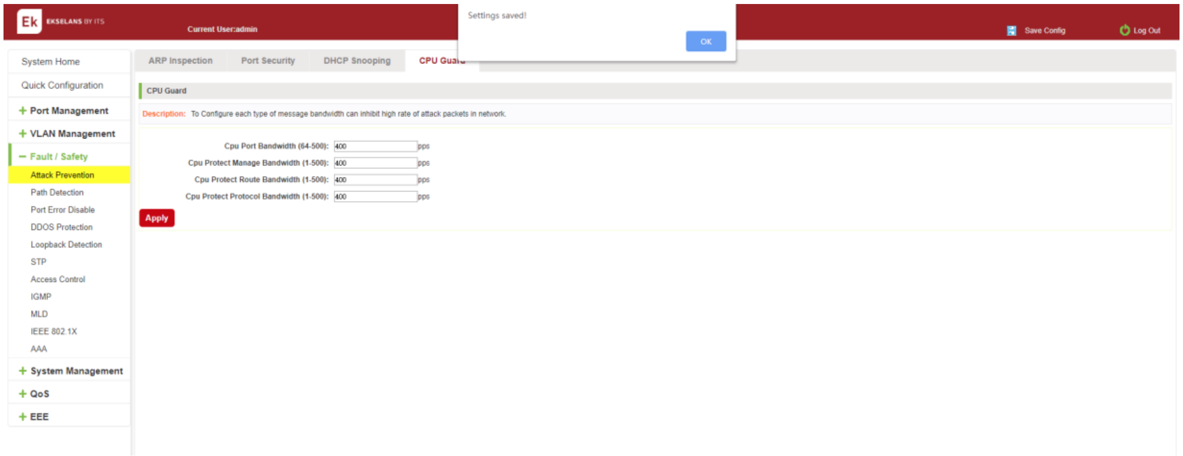
CPU Guard

Description: To Configure each type of message bandwidth can inhibit high rate of attack packets in network.

Cpu Port Bandwidth (64-500): 500 pps
Cpu Protect Manage Bandwidth (1-500): 500 pps
Cpu Protect Route Bandwidth (1-500): 200 pps
Cpu Protect Protocol Bandwidth (1-500): 500 pps

Figure 6-14: CPU Guard information.

Change CPU guard configuration:



Settings saved!

CPU Guard

Description: To Configure each type of message bandwidth can inhibit high rate of attack packets in network.

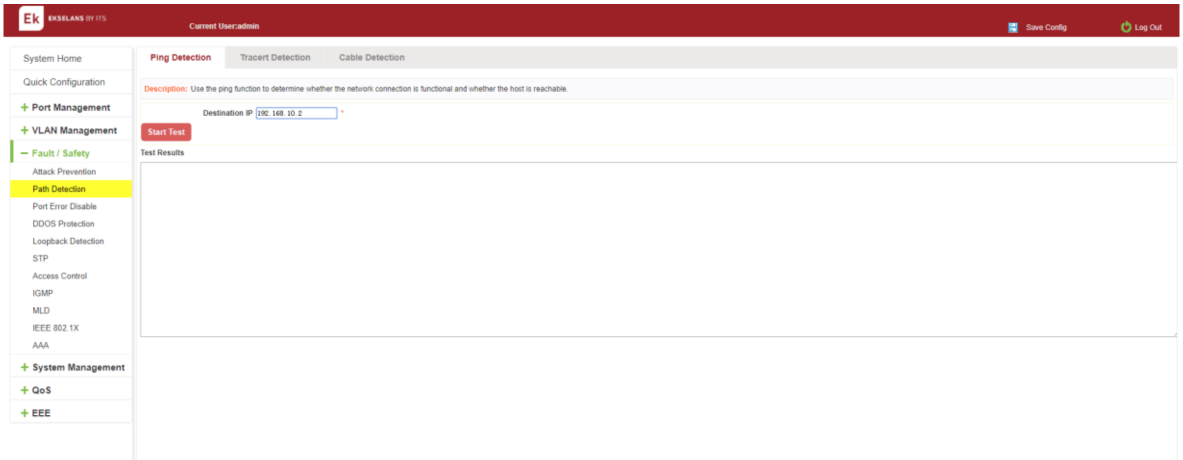
Cpu Port Bandwidth (64-500): 400 pps
Cpu Protect Manage Bandwidth (1-500): 400 pps
Cpu Protect Route Bandwidth (1-500): 400 pps
Cpu Protect Protocol Bandwidth (1-500): 400 pps

Figure 6-15: Change CPU Guard configuration.

Path detection.

Path /Tracert detection.

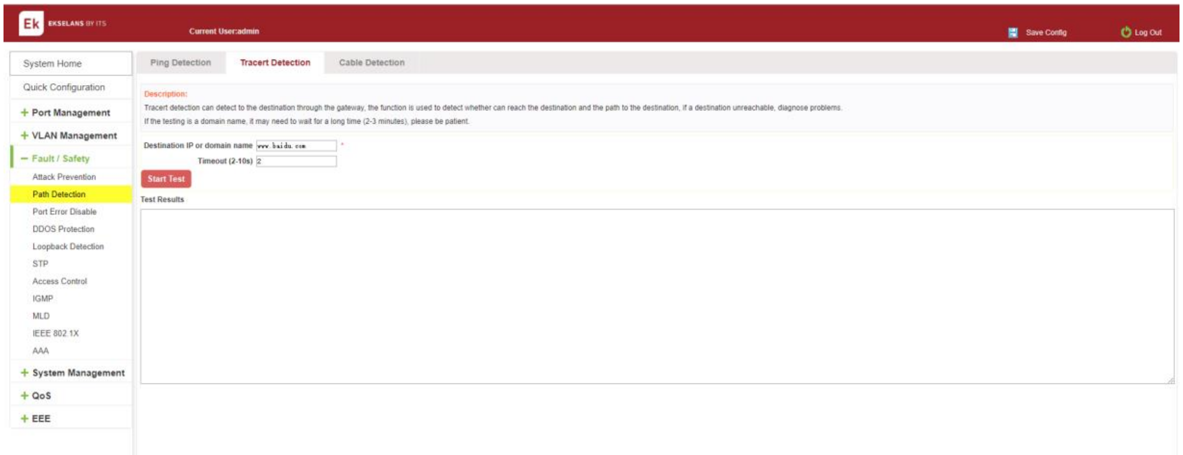
Click the "Fault/Safety" "path Detection" or “Tracert detection” can view the Path Detection configuration:



Description: Use the ping function to determine whether the network connection is functional and whether the host is reachable.

Destination IP: 192.168.10.2 *

Figure 6-16: Path detection information.



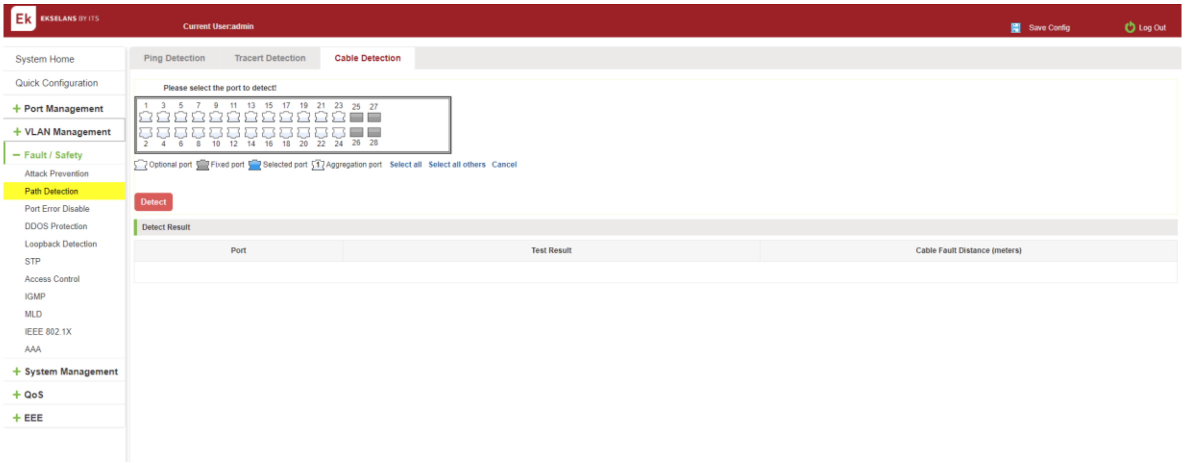
Description:
Tracert detection can detect to the destination through the gateway, the function is used to detect whether can reach the destination and the path to the destination, if a destination unreachable, diagnose problems.
If the testing is a domain name, it may need to wait for a long time (2-3 minutes), please be patient.

Destination IP or domain name: www.baidu.com *
Timeout (2-10s): 2

Figure 6-17: Tracert detection information.

Cable Detection.

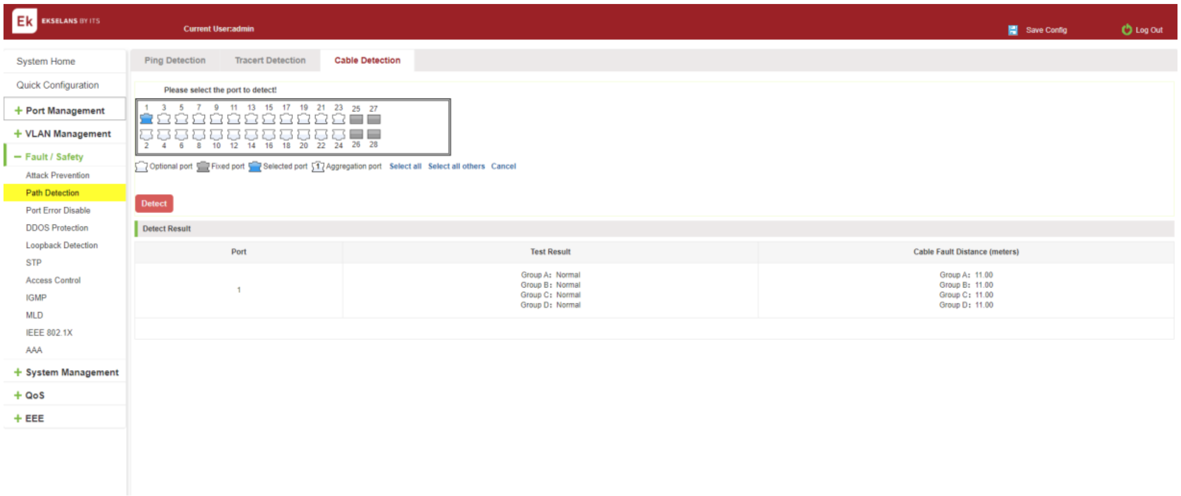
Click the "Fault/Safety" "path Detection" "Cable Detection" can view the Cable Detection configuration:



Port	Test Result	Cable Fault Distance (meters)

Figure 6-18: Cable detection information.

The cable detection only selected one port:

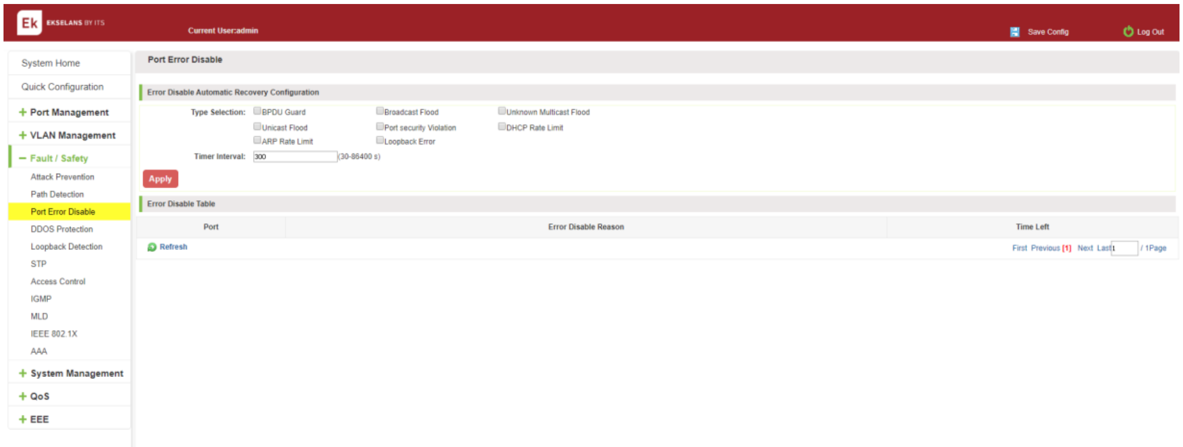


Port	Test Result	Cable Fault Distance (meters)
1	Group A: Normal Group B: Normal Group C: Normal Group D: Normal	Group A: 11.00 Group B: 11.00 Group C: 11.00 Group D: 11.00

Figure 6-19: Port cable detection result.

DDOS PROTECTION.

Click the "Fault/Safety" "DDOS Protection" can view the DDOS protection configuration:



Port Error Disable

Error Disable Automatic Recovery Configuration

Type Selection: □BPDU Guard □Broadcast Flood □Unknown Multicast Flood
□Unicast Flood □Port security Violation □DHCP Rate Limit
□ARP Rate Limit □Loopback Error

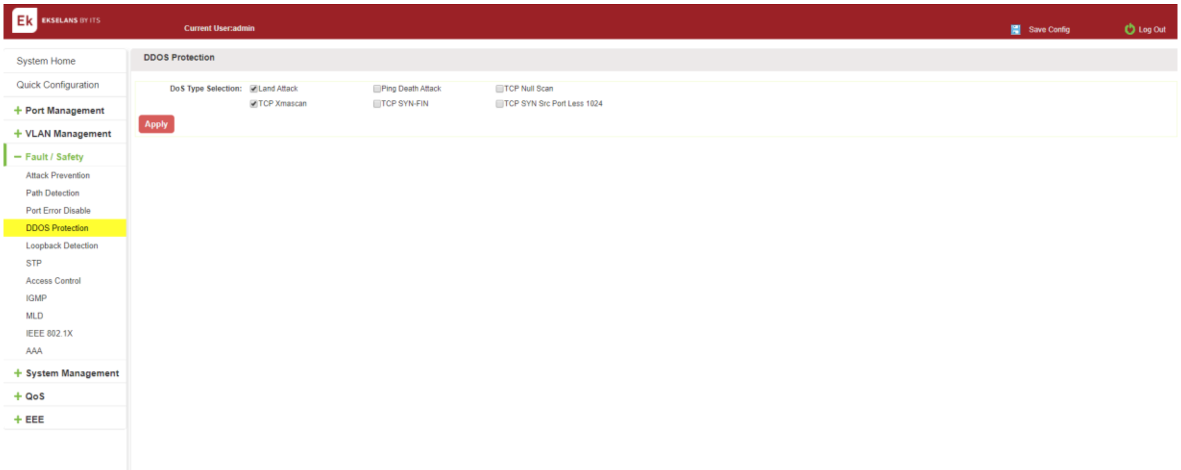
Timer Interval: 300 (30-86400 s)

Error Disable Table

Port	Error Disable Reason	Time Left

Figure 6-20: DDOS Protection information.

Selected dos type to prevent multiple computers from sending attack packets.



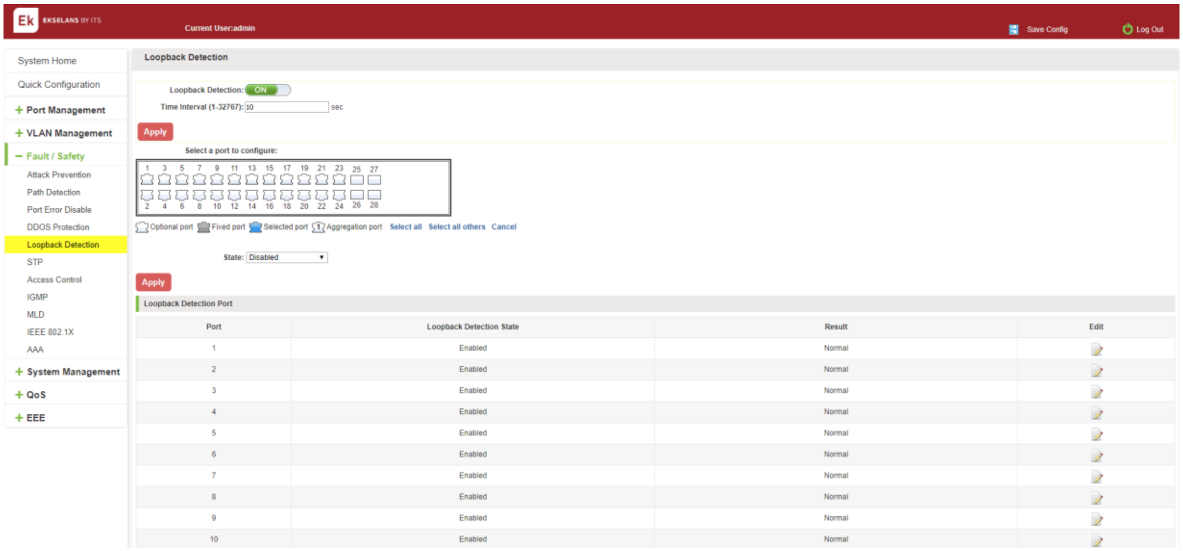
DDOS Protection

DoS Type Selection: ☑Land Attack □Ping Death Attack □TCP Null Scan
☑TCP Xmascan □TCP SYN-FIN □TCP SYN Src Port Less 1024

Figure 6-21: selected dos type.

Loop detection

Click the "Fault/Safety" "loop detection" can view the current loop detection configuration:



Loopback Detection

Loopback Detection: ON

Time Interval (1-32767): 10 sec

Select a port to configure:

State: Disabled

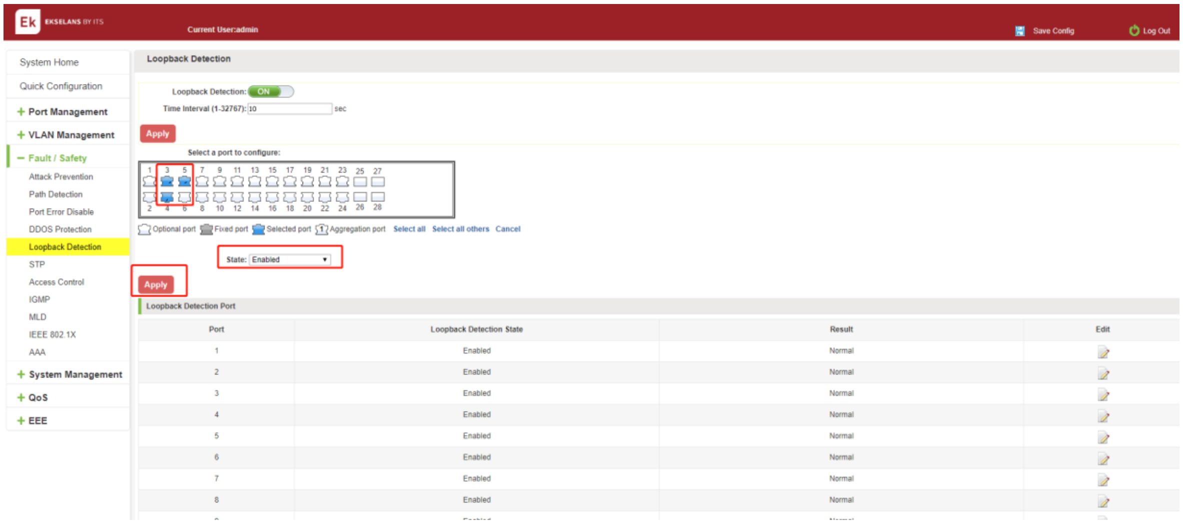
Loopback Detection Port

Port	Loopback Detection State	Result	Edit
1	Enabled	Normal	
2	Enabled	Normal	
3	Enabled	Normal	
4	Enabled	Normal	
5	Enabled	Normal	
6	Enabled	Normal	
7	Enabled	Normal	
8	Enabled	Normal	
9	Enabled	Normal	
10	Enabled	Normal	

Figure 6-22: View loopback detection configuration information.

Choose the port to configure.

Selected one or more ports to change the loopback detection status:



Loopback Detection

Loopback Detection: ON

Time Interval (1-32767): 10 sec

Select a port to configure:

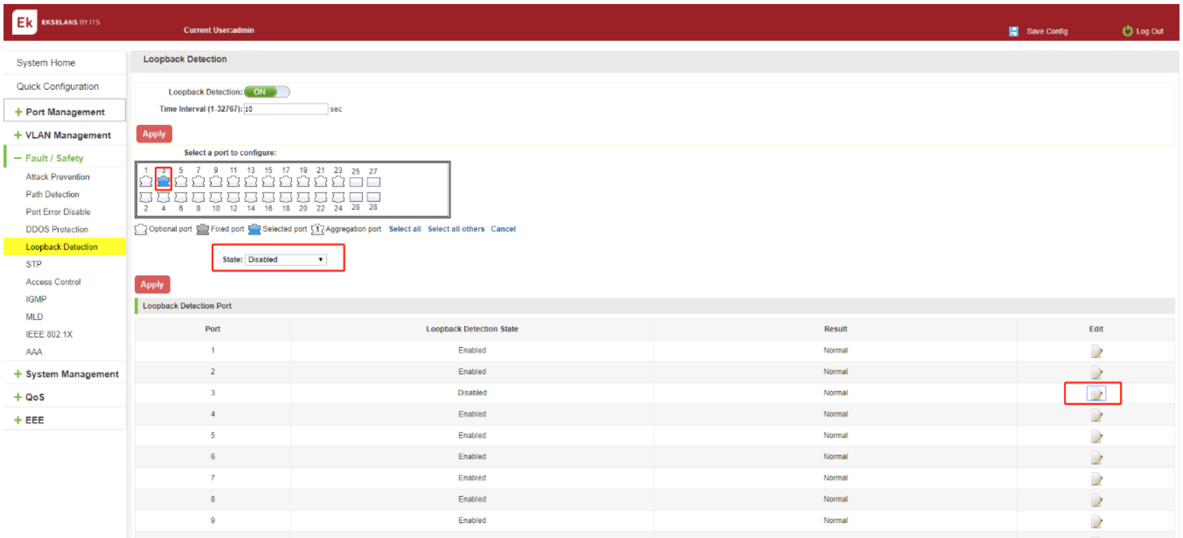
State: Enabled

Loopback Detection Port

Port	Loopback Detection State	Result	Edit
1	Enabled	Normal	
2	Enabled	Normal	
3	Enabled	Normal	
4	Enabled	Normal	
5	Enabled	Normal	
6	Enabled	Normal	
7	Enabled	Normal	
8	Enabled	Normal	

Figure 6-24: configure ports parameter.

Click “Edit” button, change the port status:



Loopback Detection

Loopback Detection: ON

Time Interval (1-32767): 10 sec

State: Disabled

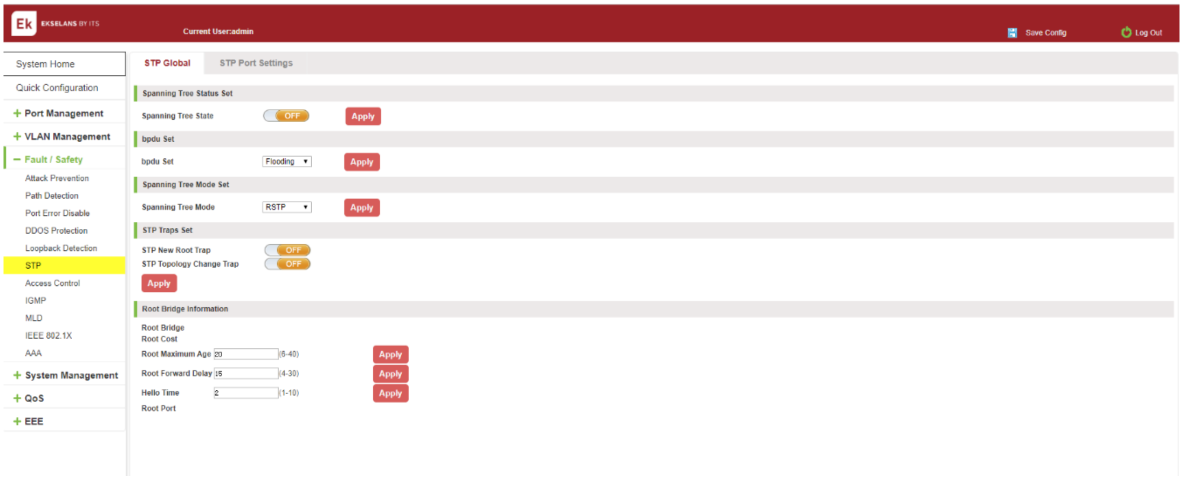
Loopback Detection Port

Port	Loopback Detection State	Result	Edit
1	Enabled	Normal	✎
2	Enabled	Normal	✎
3	Disabled	Normal	✎
4	Enabled	Normal	✎
5	Enabled	Normal	✎
6	Enabled	Normal	✎
7	Enabled	Normal	✎
8	Enabled	Normal	✎
9	Enabled	Normal	✎

Figure 6-25: change the port configure.

STP.

Click the "Fault/Safety" "STP" "STP Global" can view the current STP global configuration:



Spanning Tree Status Set
Spanning Tree State: OFF

bpdu Set
bpdu Set: Flooding

Spanning Tree Mode Set
Spanning Tree Mode: RSTP

STP Traps Set
STP New Root Trap: OFF
STP Topology Change Trap: OFF

Root Bridge Information
Root Bridge
Root Cost
Root Maximum Age 20 (6-40)
Root Forward Delay 15 (4-30)
Hello Time 2 (1-10)
Root Port

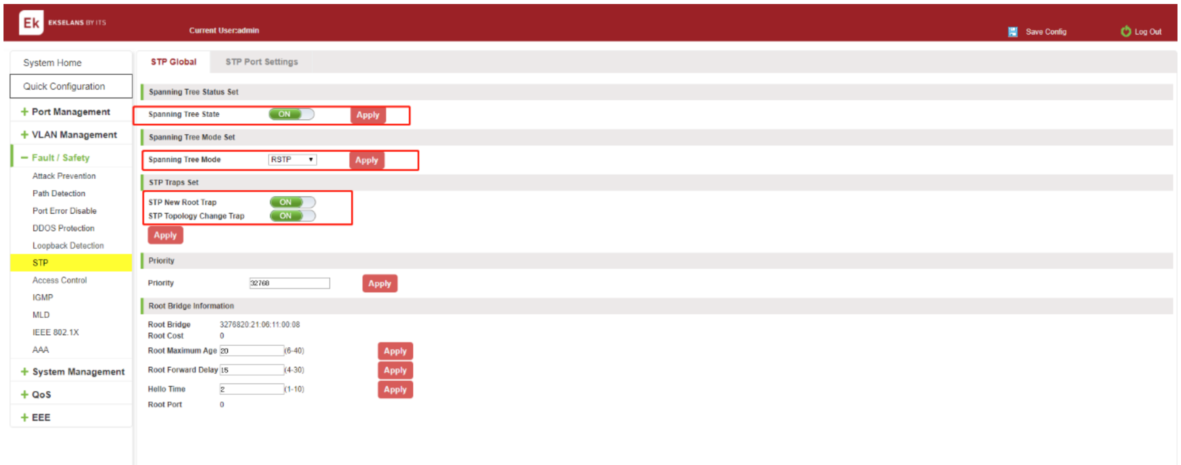
Figure 6-26: STP Global view.

ENABLE STP function.

Enbale STP global state and configuration mode and traps.

Notice:

1. 1When the loopback detection and STP functions are mutually exclusive.
2. 2LLDP PDU FLooding enabled prevents executing mstp enable.



Spanning Tree Status Set
Spanning Tree State: ON

Spanning Tree Mode Set
Spanning Tree Mode: RSTP

STP Traps Set
STP New Root Trap: ON
STP Topology Change Trap: ON

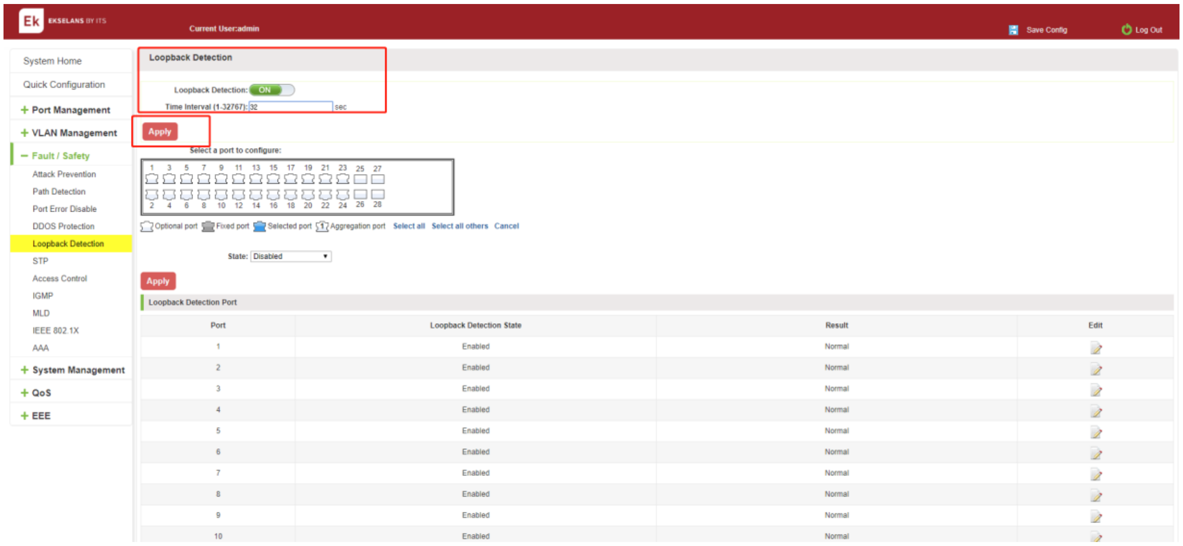
Priority
Priority 32768

Root Bridge Information
Root Bridge 3276820:21:06:11:00:08
Root Cost 0
Root Maximum Age 20 (6-40)
Root Forward Delay 15 (4-30)
Hello Time 2 (1-10)
Root Port 0

Figure 6-27: enable STP change mode and traps.

ENABLE LOOPBACK DETECTION.

Enable the loopback detection and configuration some parameters, click" Apply" button:



Loopback Detection

Loopback Detection: ON

Time Interval (1-32767): 32 sec

Apply

Select a port to configure:

State: Disabled

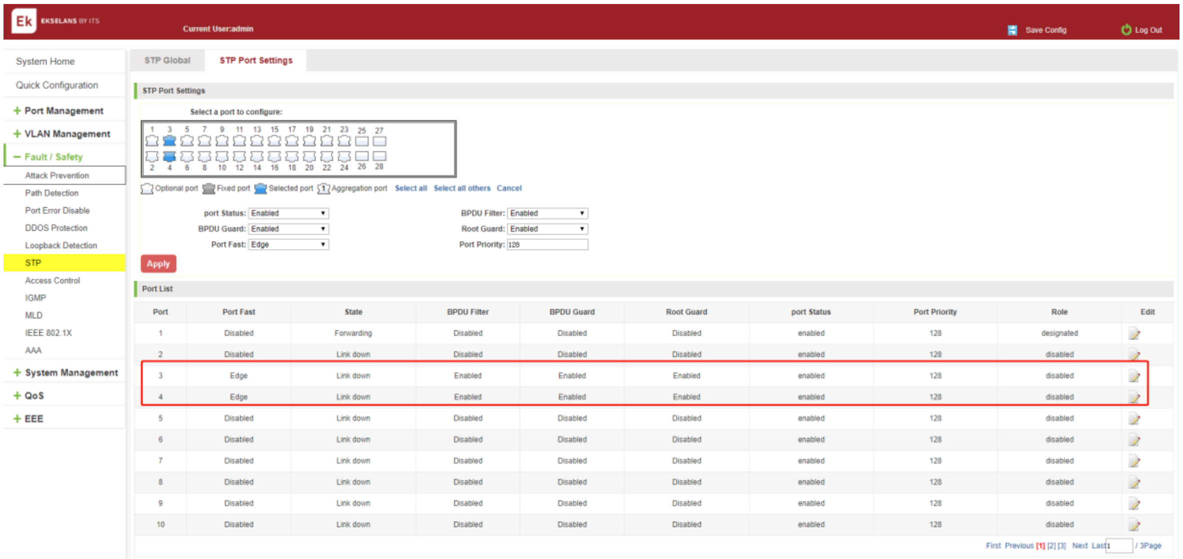
Apply

Loopback Detection Port

Port	Loopback Detection State	Result	Edit
1	Enabled	Normal	✎
2	Enabled	Normal	✎
3	Enabled	Normal	✎
4	Enabled	Normal	✎
5	Enabled	Normal	✎
6	Enabled	Normal	✎
7	Enabled	Normal	✎
8	Enabled	Normal	✎
9	Enabled	Normal	✎
10	Enabled	Normal	✎

STP PORT SETTINGS.

Selected port to configuration STP.



STP Port Settings

Select a port to configure:

port Status: Enabled

BPDU Guard: Enabled

Port Fast: Edge

BPDU Filter: Enabled

Root Guard: Enabled

Port Priority: 128

Apply

Port List

Port	Port Fast	State	BPDU Filter	BPDU Guard	Root Guard	port Status	Port Priority	Role	Edit
1	Disabled	Forwarding	Disabled	Disabled	Disabled	enabled	128	designated	✎
2	Disabled	Link down	Disabled	Disabled	Disabled	enabled	128	disabled	✎
3	Edge	Link down	Enabled	Enabled	Enabled	enabled	128	disabled	✎
4	Edge	Link down	Enabled	Enabled	Enabled	enabled	128	disabled	✎
5	Disabled	Link down	Disabled	Disabled	Disabled	enabled	128	disabled	✎
6	Disabled	Link down	Disabled	Disabled	Disabled	enabled	128	disabled	✎
7	Disabled	Link down	Disabled	Disabled	Disabled	enabled	128	disabled	✎
8	Disabled	Link down	Disabled	Disabled	Disabled	enabled	128	disabled	✎
9	Disabled	Link down	Disabled	Disabled	Disabled	enabled	128	disabled	✎
10	Disabled	Link down	Disabled	Disabled	Disabled	enabled	128	disabled	✎

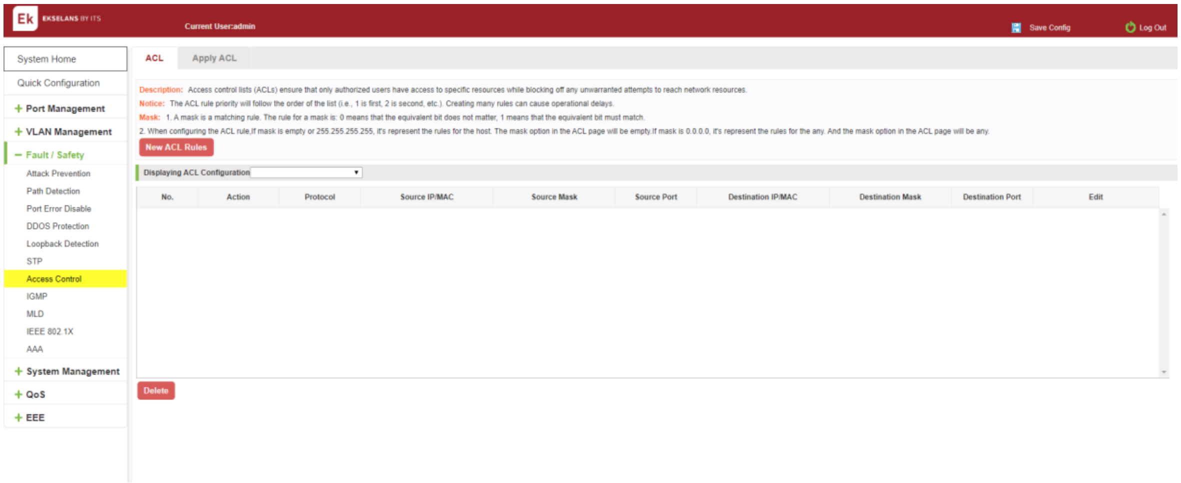
First Previous [1] [2] [3] Next Last 1 / 3Page

Figure 6-28: selected port to configuration STP.

Access control

VIEW ACCESS CONTROL LIST.

Click the "Fault/Safety" "Access Control" you can view the configuration information of the access control list:



Description: Access control lists (ACLs) ensure that only authorized users have access to specific resources while blocking off any unwarranted attempts to reach network resources.

Notice: The ACL rule priority will follow the order of the list (i.e., 1 is first, 2 is second, etc.). Creating many rules can cause operational delays.

Mask: 1. A mask is a matching rule. The rule for a mask is: 0 means that the equivalent bit does not matter, 1 means that the equivalent bit must match.

2. When configuring the ACL rule,If mask is empty or 255.255.255.255, it's represent the rules for the host. The mask option in the ACL page will be empty.If mask is 0.0.0.0, it's represent the rules for the any. And the mask option in the ACL page will be any.

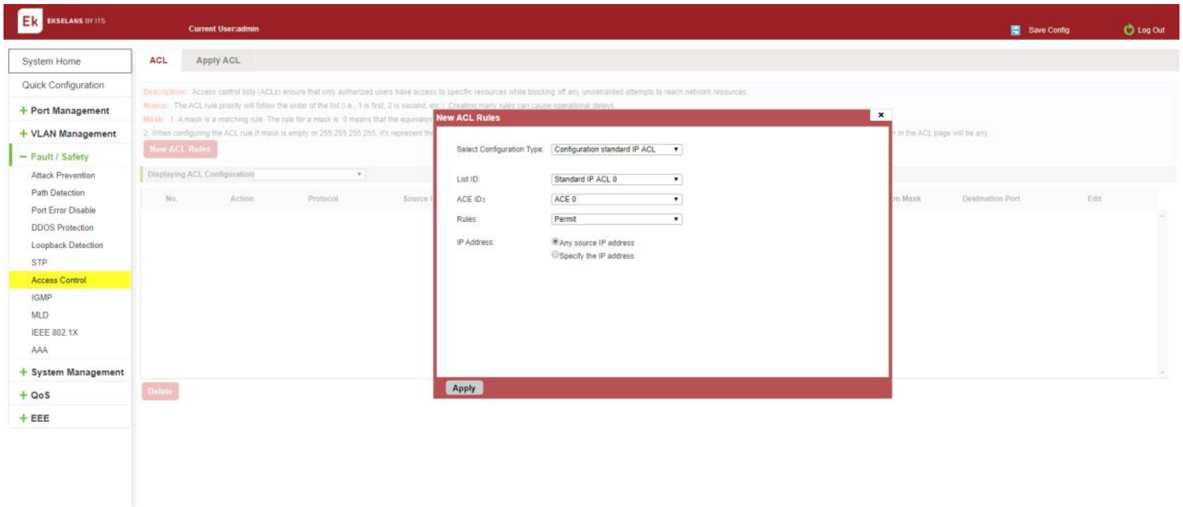
Displaying ACL Configuration

No.	Action	Protocol	Source IP/MAC	Source Mask	Source Port	Destination IP/MAC	Destination Mask	Destination Port	Edit

Figure 6-29: Access control list.

INCREASE THE STANDARD IP ACCESS RULES.

Click "ACL rules New", in the pop-up dialog box, select "standard IPV4 ACL Configuration", in the list of ID:0, ID:0 ACE, rules to allow. IP address is: any source IP address. Click "Apply" to complete the new rules:



New ACL Rules

Select Configuration Type: Configuration standard IP ACL

List ID: Standard IP ACL 0

ACE ID: ACE 0

Rules: Permit

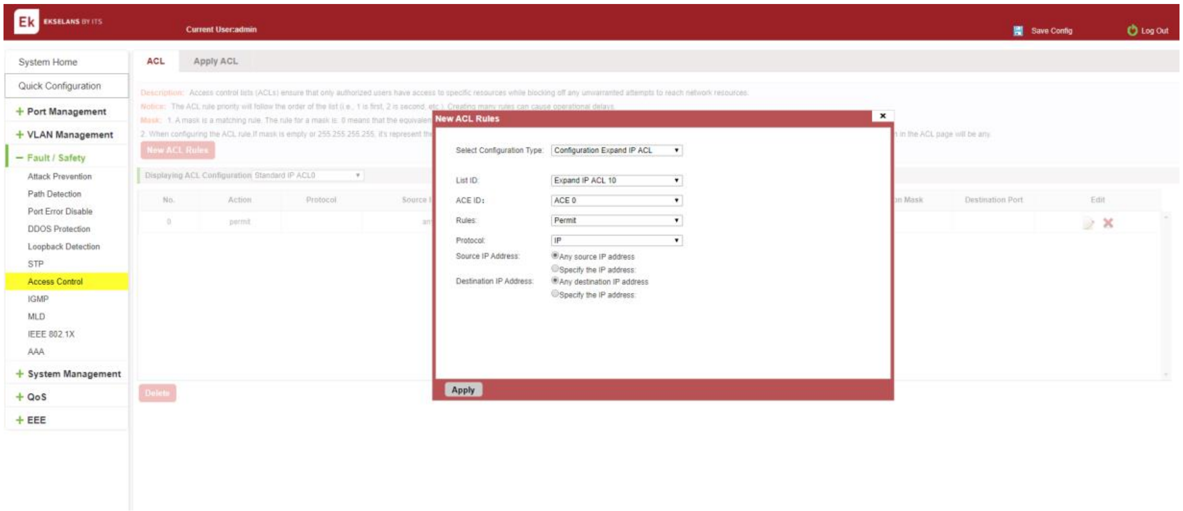
IP Address: ● Any source IP address ○ Specify the IP address:

Apply

Figure 6-30: Configuration standard IP access control list.

INCREASE THE EXTENDED IP ACCESS RULE.

Click "ACL rules New", in the pop-up dialog box, select "Expand IPV4 ACL Configuration", in the list of ACE, ID:0 ID:10, rules for "Permit". Agreement: TCP, source IP address: any source IP address; purpose IP address: any destination IP address, click "Apply" to complete the new:



New ACL Rules

Select Configuration Type: Configuration Expand IP ACL

List ID: Expand IP ACL 10

ACE ID: ACE 0

Rules: Permit

Protocol: IP

Source IP Address: ● Any source IP address ○ Specify the IP address:

Destination IP Address: ● Any destination IP address ○ Specify the IP address:

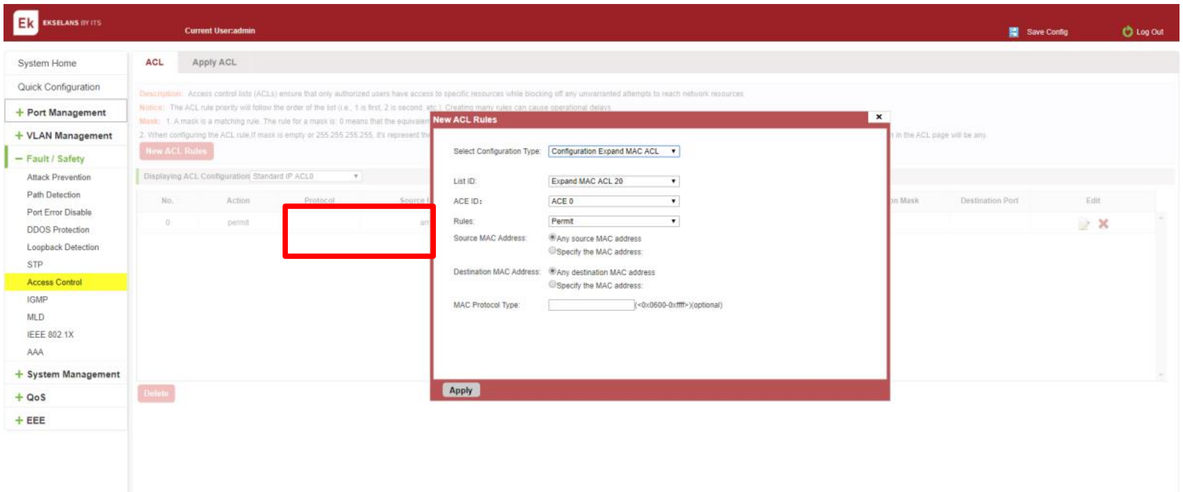
Apply

Figure 6-31: Configuration standard IP access control list.

INCREASING EXPAND MAC ACCESS RULES.

Click “New ACL rules”, select "Configuration Expand MAC ACL" in the pop-up window, in list ID ：20 , ACE ID：0, Rules "Deny"、Source MAC address：0088.9999.999A

Destination MAC address is the random MAC。MAC protocol type：0x0086。After the configuration is complete, click "Apply" :



New ACL Rules

Select Configuration Type: Configuration Expand MAC ACL

List ID: Expand MAC ACL 20

ACE ID： ACE 0

Rules: Permit

Source MAC Address: ● Any source MAC address ○ Specify the MAC address:

Destination MAC Address: ● Any destination MAC address ○ Specify the MAC address:

MAC Protocol Type: (<0x0600-0xffff>)(optional)

Apply

Figure 6-32: Configuration extended MAC access control list.

Configuration instructions.

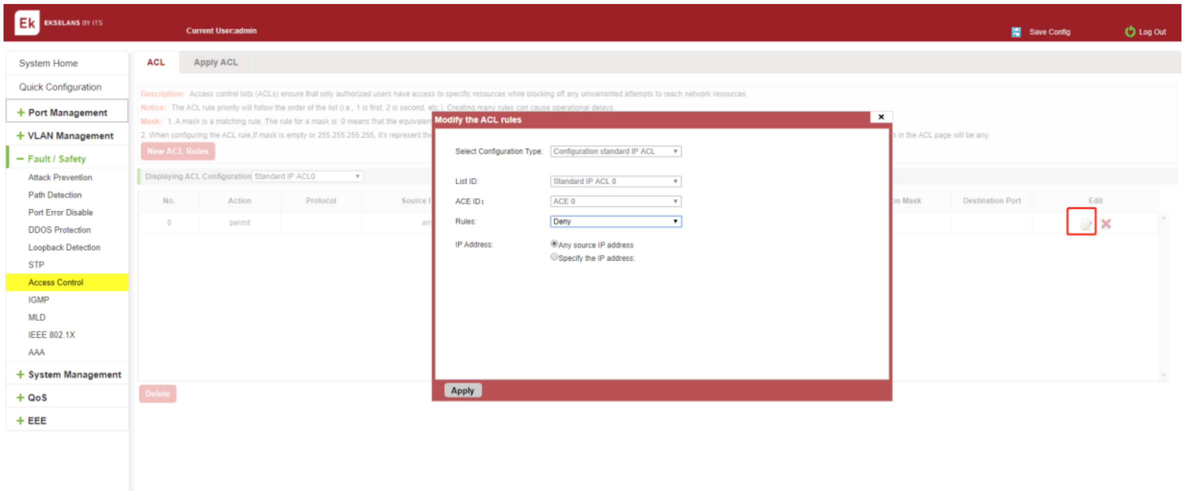
ACE ID is an optional rule. Do not fill: the default is 0.

The extended IP protocol access control list, type: TCP, UDP, IP.

MODIFY CONFIGURATION.

Rules for modifying port applications

Select the rules to be replaced, click " ✎ ", enter the modified ACL rules page, the rules are: "Deny", click "Apply":



Modify the ACL rules

Select Configuration Type: Configuration standard IP ACL

List ID: Standard IP ACL 0

ACE ID: ACE 0

Rules: Deny

IP Address: ● Any source IP address ○ Specify the IP address:

Apply

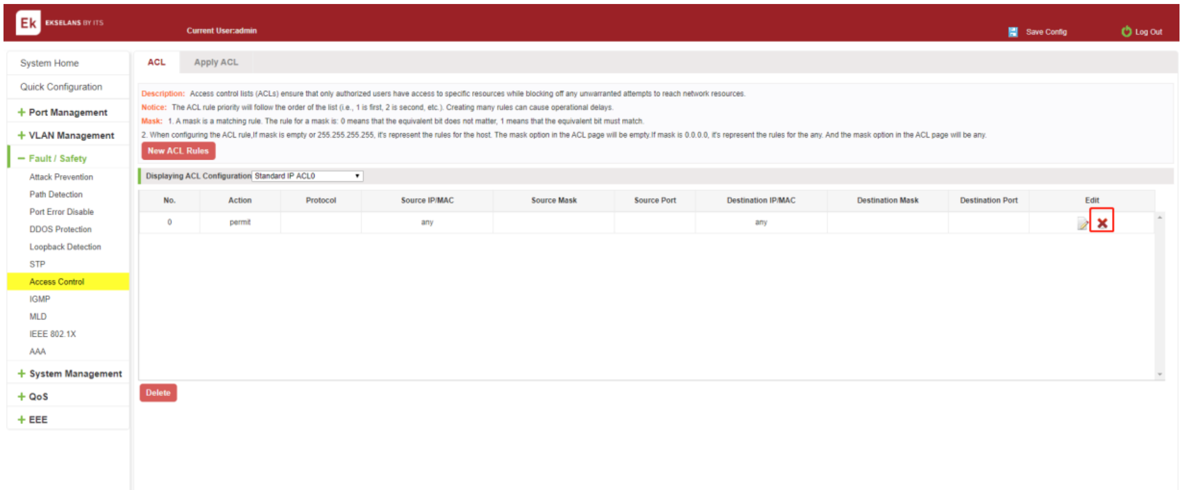
Figure 6-33: To modify the ACL rule.

Configuration instructions

The modified extended MAC and extended IP for the same operation.

DELETE RULE.

To delete the rule, click "X" to delete the current list of ACE under a ACL rule:



Description: Access control lists (ACLs) ensure that only authorized users have access to specific resources while blocking off any unwarranted attempts to reach network resources.

Notice: The ACL rule priority will follow the order of the list (i.e., 1 is first, 2 is second, etc.). Creating many rules can cause operational delays.

Mask: 1. A mask is a matching rule. The rule for a mask is: 0 means that the equivalent bit does not matter, 1 means that the equivalent bit must match.

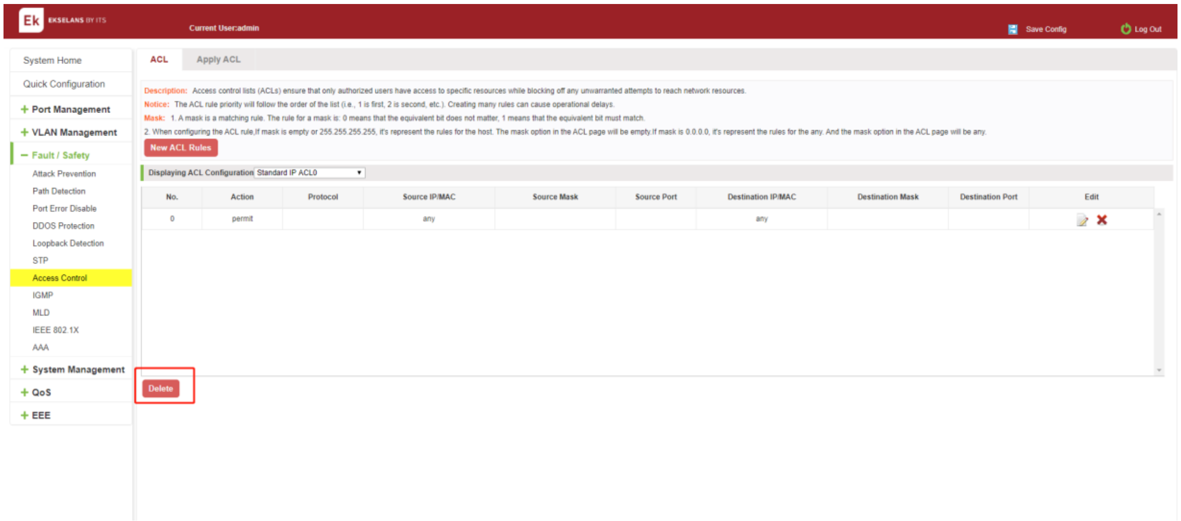
2. When configuring the ACL rule,If mask is empty or 255.255.255.255, it's represent the rules for the host. The mask option in the ACL page will be empty.If mask is 0.0.0.0, it's represent the rules for the any. And the mask option in the ACL page will be any.

Displaying ACL Configuration: Standard IP ACL0

No.	Action	Protocol	Source IP/MAC	Source Mask	Source Port	Destination IP/MAC	Destination Mask	Destination Port	Edit
0	permit		any			any			✎ ✖

Figure 6-34: Delete rules.

Remove all of the ACE rule table under ACL, click "Delete":



Description: Access control lists (ACLs) ensure that only authorized users have access to specific resources while blocking off any unwarranted attempts to reach network resources.
Notice: The ACL rule priority will follow the order of the list (i.e., 1 is first, 2 is second, etc.). Creating many rules can cause operational delays.
Mask: 1. A mask is a matching rule. The rule for a mask is: 0 means that the equivalent bit does not matter, 1 means that the equivalent bit must match.
2. When configuring the ACL rule,If mask is empty or 255.255.255.255, it's represent the rules for the host. The mask option in the ACL page will be empty.If mask is 0.0.0.0, it's represent the rules for the any. And the mask option in the ACL page will be any.

Displaying ACL Configuration: Standard IP ACL0

No.	Action	Protocol	Source IP/MAC	Source Mask	Source Port	Destination IP/MAC	Destination Mask	Destination Port	Edit
0	permit		any			any			✎ ✖

Figure 6-35: Delete ACL rules.

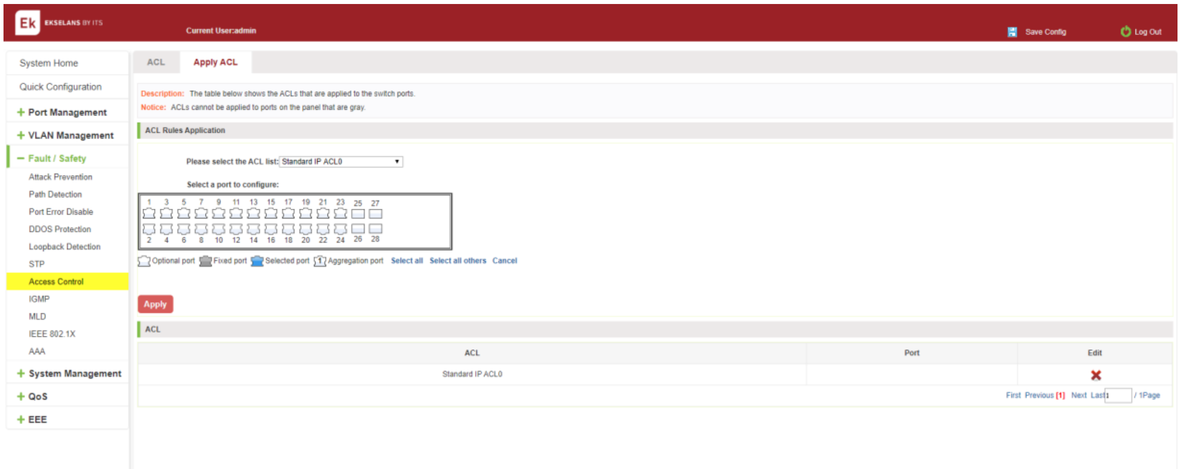
Configuration instructions.

Delete - after the success of the kneeling in port configuration table deleted together.

VIEW APPLICATION ACL.

"Apply"->"Access Control"->"Fault/Safety" ACL:

The configuration information and click on the "Fault/Safety" "Access Control" "Apply ACL" can view access control using ACL:



Description: The table below shows the ACLs that are applied to the switch ports.
Notice: ACLs cannot be applied to ports on the panel that are gray.

Please select the ACL list: Standard IP ACL0

Select a port to configure:

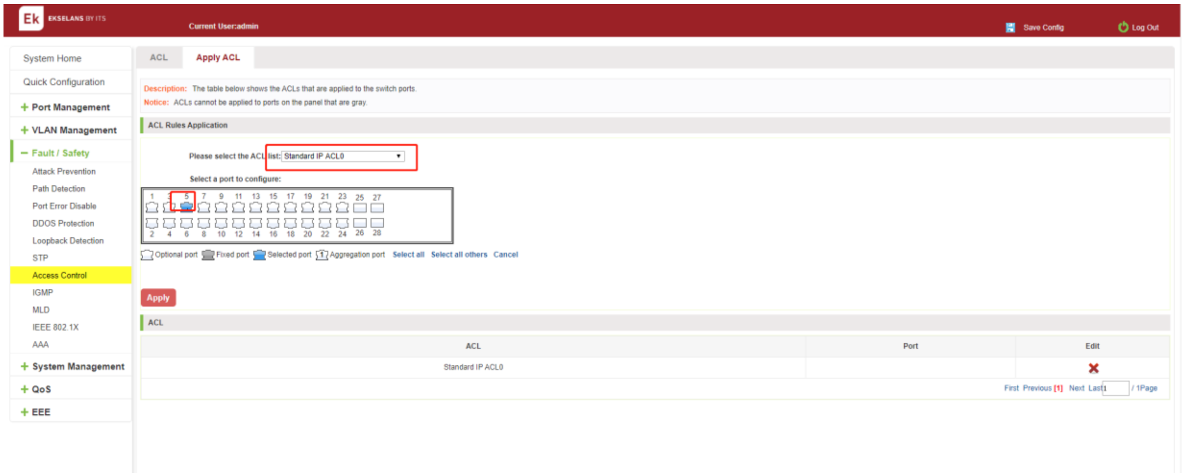
ACL	Port	Edit
Standard IP ACL0		✖

Figure 6-36: View application ACL rules.

INCREASED APPLICATION ACL.

"Apply":

Select the rules that need to be applied, then select the port of application, click "Apply" to complete the configuration:



Description: The table below shows the ACLs that are applied to the switch ports.
Notice: ACLs cannot be applied to ports on the panel that are gray.

Please select the ACL list: Standard IP ACL0

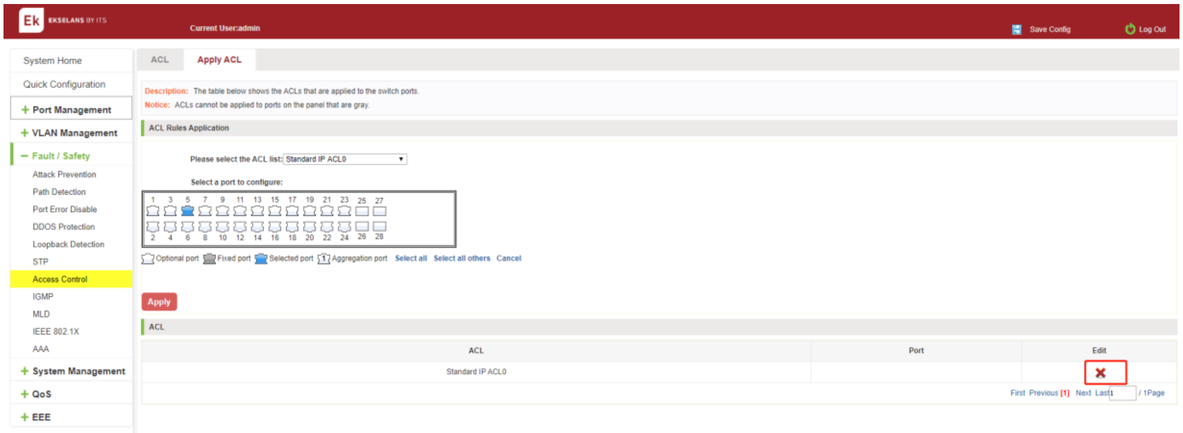
Select a port to configure:

ACL	Port	Edit
Standard IP ACL0		✖

Figure 6-37: Add applications ACL.

DELETE APPLICATION ACL.

Click to delete the application rule on the right side, cancel the application of the rules in the port:



Description: The table below shows the ACLs that are applied to the switch ports.
Notice: ACLs cannot be applied to ports on the panel that are gray.

ACL Rules Application

Please select the ACL list: Standard IP ACL0

Select a port to configure:

ACL

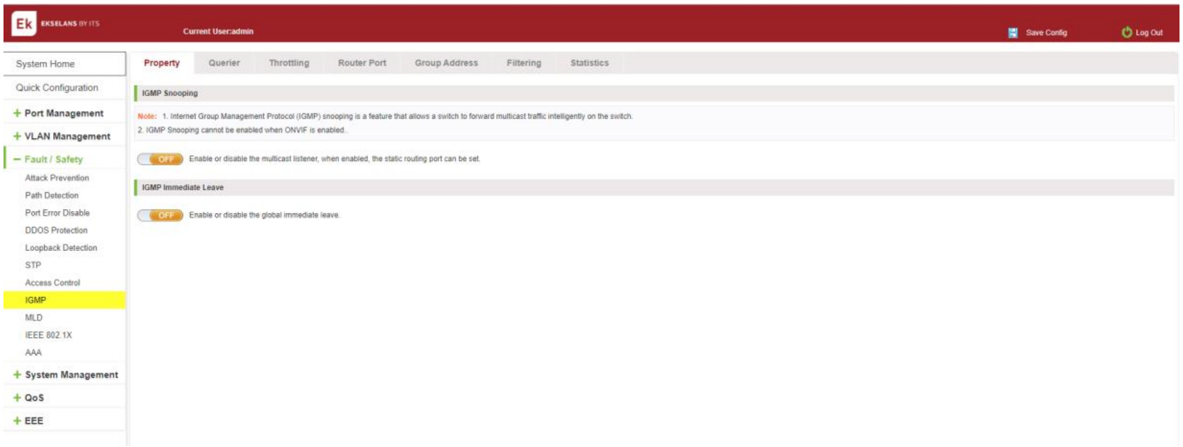
ACL	Port	Edit
Standard IP ACL0		✗

Figure 6-38: Delete application ACL.

IGMP Snooping.

VIEW IGMP SNOOPING CONFIGURATION.

Click the "Fault/Safety" "IGMP Snooping" to check the current switch configured multicast monitoring information:



IGMP Snooping

Note: 1. Internet Group Management Protocol (IGMP) snooping is a feature that allows a switch to forward multicast traffic intelligently on the switch.
2. IGMP Snooping cannot be enabled when ONVIF is enabled.

OFF Enable or disable the multicast listener, when enabled, the static routing port can be set.

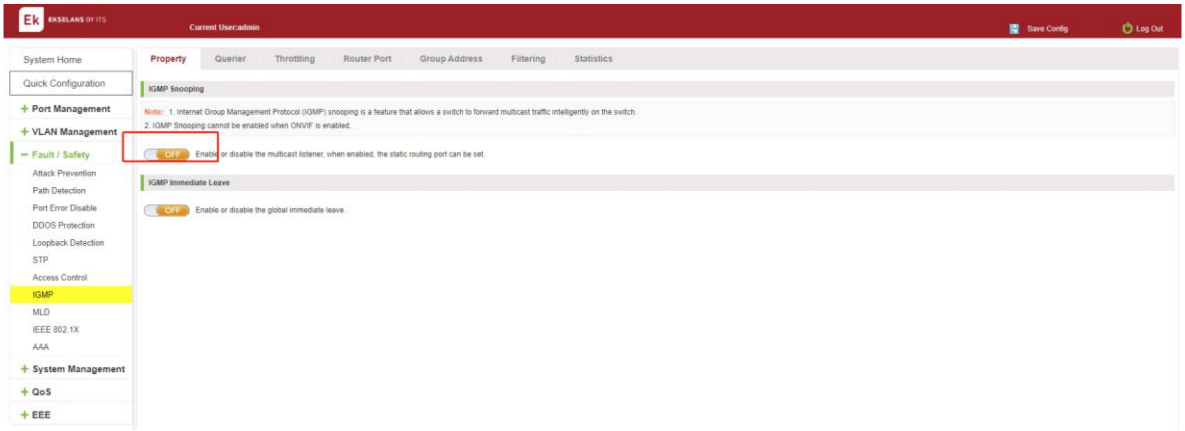
IGMP Immediate Leave

OFF Enable or disable the global immediate leave.

Figure 6-39: View Snooping IGMP configuration information.

ACTION MULTICAST LISTENER FUNCTION.

Click the "Fault/Safety" "IGMP Snooping", click "Off" button to activate the multicast monitoring function:



Current User:admin

IGMP Snooping

Note: 1. Internet Group Management Protocol (IGMP) snooping is a feature that allows a switch to forward multicast traffic intelligently on the switch.
2. IGMP Snooping cannot be enabled when ONVIF is enabled.

OFF Enable or disable the multicast listener, when enabled, the static routing port can be set.

IGMP Immediate Leave

OFF Enable or disable the global immediate leave.

Figure 6-40: Open multicast listener configuration.

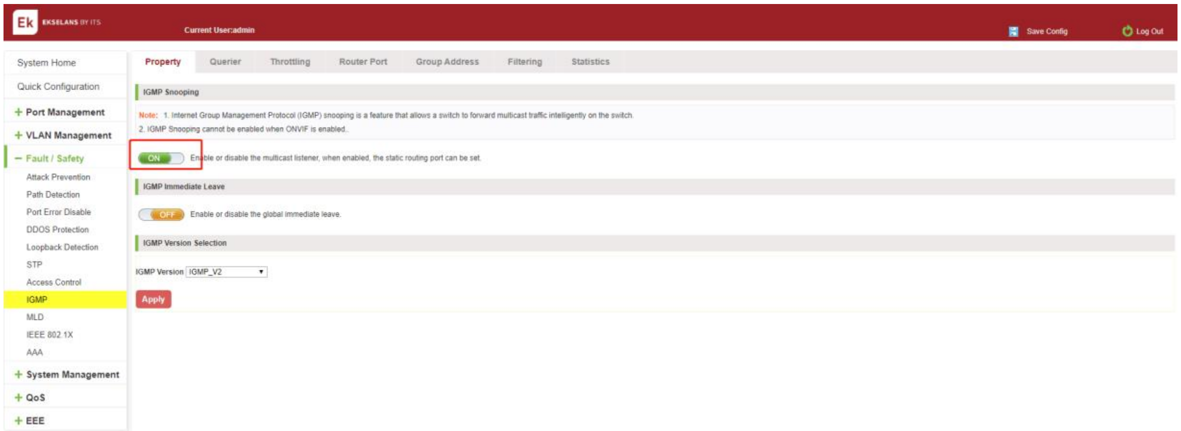
The default multicast listener (IGMP Snooping) did not open.

The default on multicast listener (IGMP Snooping), all VLAN are open.

The default version of V2 - IGMP.

DISABLE MULTICAST LISTENNER FUNCTION.

Click the "Fault/Safety" "IGMP Snooping", click "ON" button to disable multicast monitoring function:



Current User:admin

IGMP Snooping

Note: 1. Internet Group Management Protocol (IGMP) snooping is a feature that allows a switch to forward multicast traffic intelligently on the switch.
2. IGMP Snooping cannot be enabled when ONVIF is enabled.

ON Enable or disable the multicast listener, when enabled, the static routing port can be set.

IGMP Immediate Leave

OFF Enable or disable the global immediate leave.

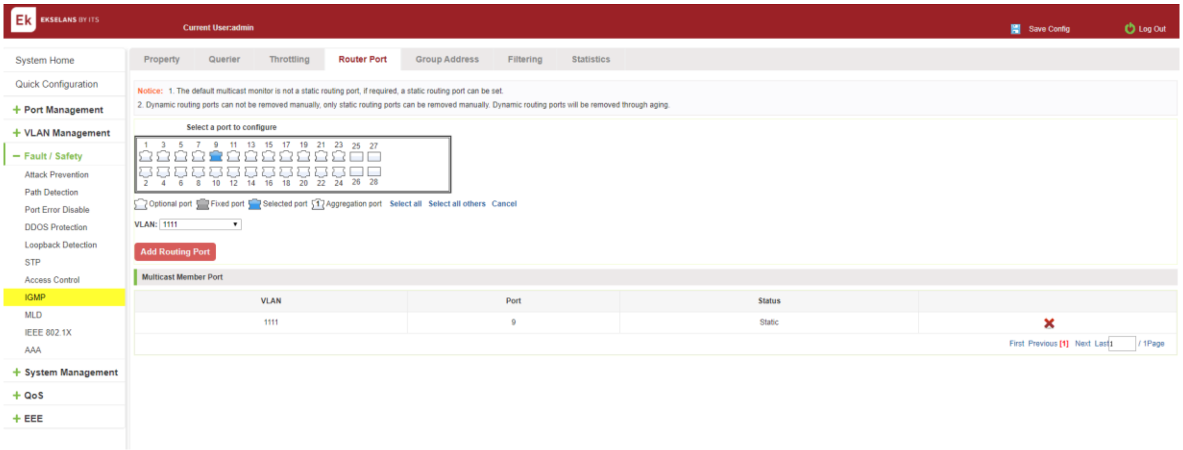
IGMP Version Selection

IGMP Version IGMP_V2

Figure 6-41: Closed multicast listener function operation.

CONFIGURATION MULTICAST ROUTING.

Select VLAN, click "Router Port Add" button, to configure the multicast routing in the port panel:



Notice: 1. The default multicast monitor is not a static routing port, if required, a static routing port can be set.
2. Dynamic routing ports can not be removed manually, only static routing ports can be removed manually. Dynamic routing ports will be removed through aging.

VLAN: 1111

VLAN	Port	Status	
1111	9	Static	✖

Figure 6-42: Configuration of multicast routing.

Multicast routing configuration steps are as follows:

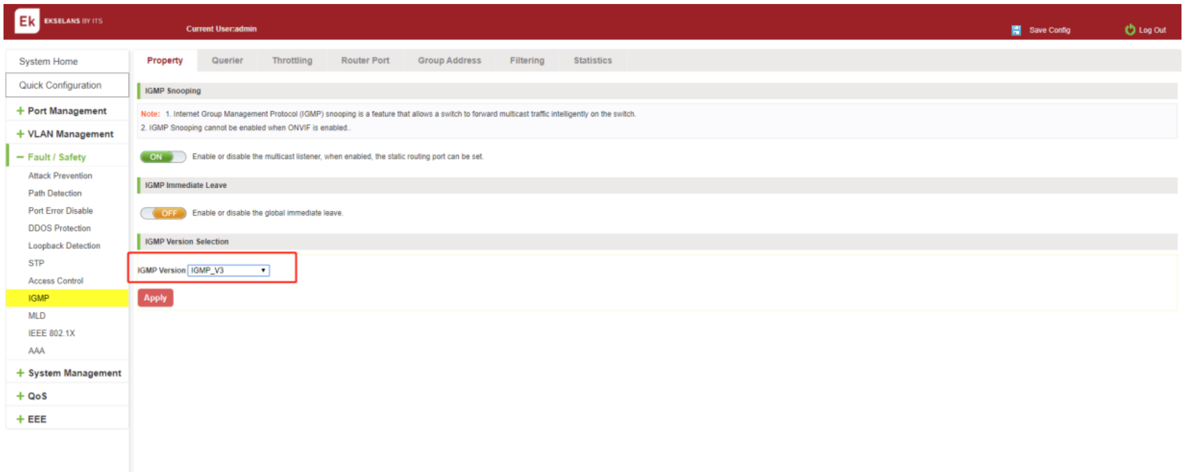
Step1: In the port panel to select multicast listener routing port.

step2: Select VLAN.

Step3: Click on the "Add Router Port" button to complete the configuration.

IGMP VERSION.

Click the "Fault/Safety" "IGMP Snooping", set the IGMP version of the page:



IGMP Snooping

Note: 1. Internet Group Management Protocol (IGMP) snooping is a feature that allows a switch to forward multicast traffic intelligently on the switch.
2. IGMP Snooping cannot be enabled when ONVIF is enabled..

ON Enable or disable the multicast listener, when enabled, the static routing port can be set.

IGMP Immediate Leave

OFF Enable or disable the global immediate leave.

IGMP Version Selection

IGMP Version IGMP_V3

Figure 6-43: Configuration IGMP version.

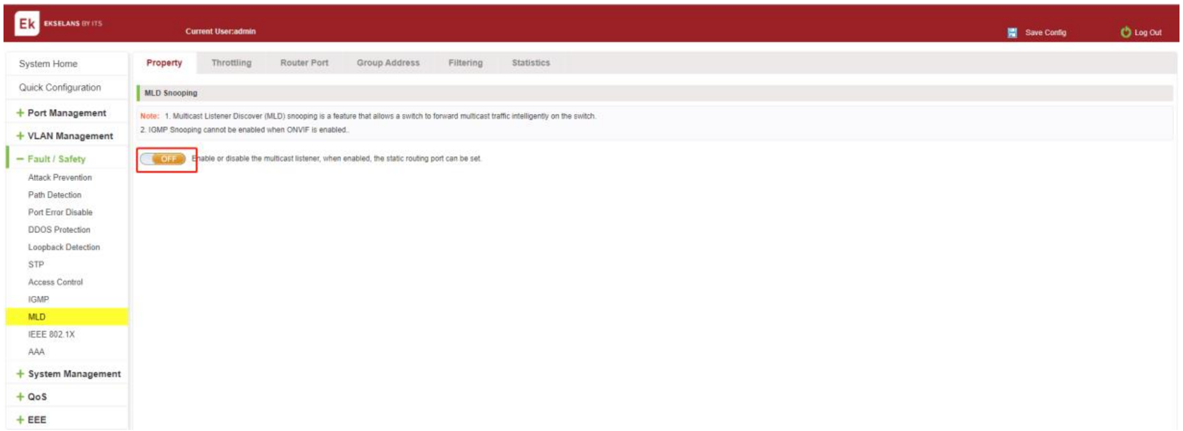
IGMP version configuration steps are as follows:

Step1: Select the required version number.

step2: Click the "Apply" button to complete the configuration.

VIEW MLD CONFIGURATION.

Click the "Fault/Safety" "IGMP Snooping" to check the current switch configured multicast monitoring information:



MLD Snooping

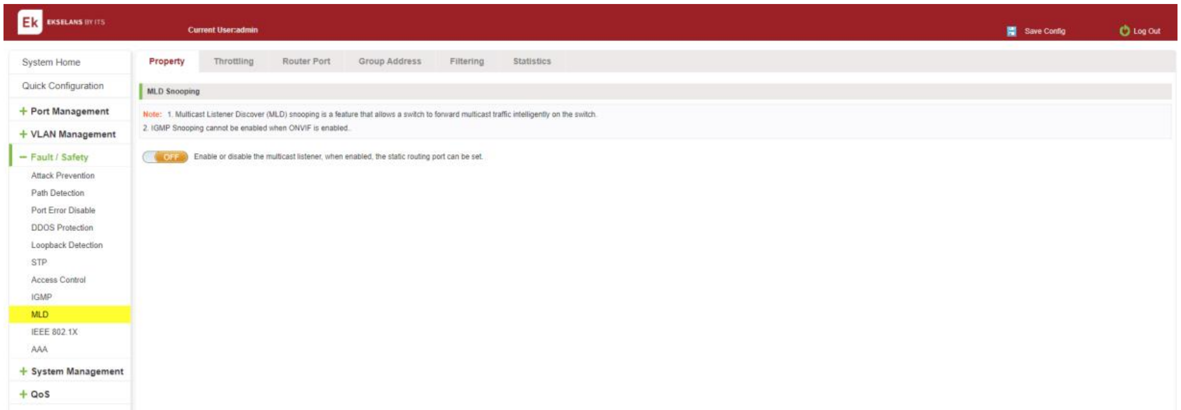
Note: 1. Multicast Listener Discover (MLD) snooping is a feature that allows a switch to forward multicast traffic intelligently on the switch.
2. IGMP Snooping cannot be enabled when ONVIF is enabled..

OFF Enable or disable the multicast listener, when enabled, the static routing port can be set.

Figure 6-44: View MLD configuration information.

ACTIVE MULTICAST LISTENER FUNCTION.

Click the "Fault/Safety" "MLD", click "Off" button to activate the multicast monitoring function:



Current User:admin

MLD Snooping

Note: 1. Multicast Listener Discover (MLD) snooping is a feature that allows a switch to forward multicast traffic intelligently on the switch.
2. IGMP Snooping cannot be enabled when ONVIF is enabled.

OFF Enable or disable the multicast listener, when enabled, the static routing port can be set.

Figure 6-45: Open multicast listener configuration.

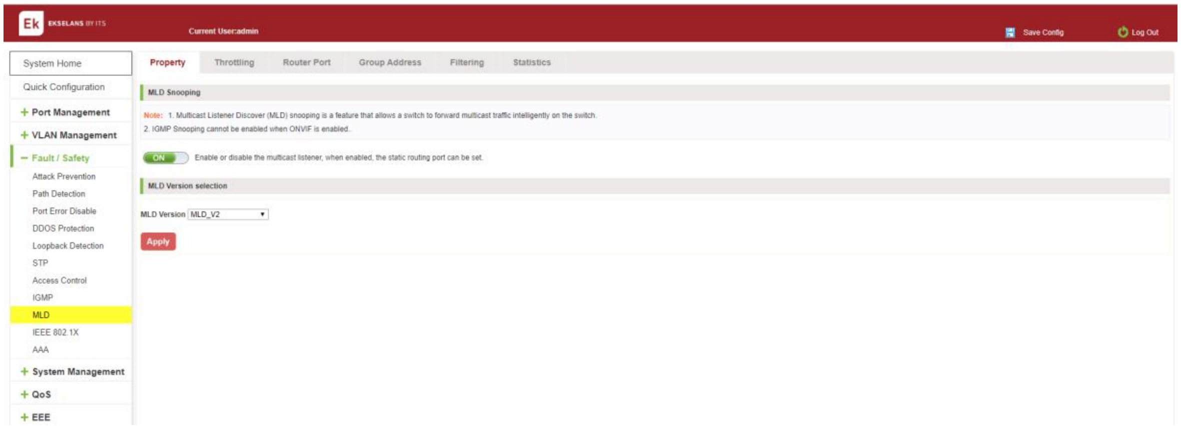
The default multicast listener (MLD) did not open.

The default on multicast listener (MLD), all VLAN are open.

The default version of V1 - MLD.

DISABLE MULTICAST LISTENER FUNCTION.

Click the "Fault/Safety" "IGMP Snooping", click "ON" button to disable multicast monitoring function:



Current User:admin

MLD Snooping

Note: 1. Multicast Listener Discover (MLD) snooping is a feature that allows a switch to forward multicast traffic intelligently on the switch.
2. IGMP Snooping cannot be enabled when ONVIF is enabled.

ON Enable or disable the multicast listener, when enabled, the static routing port can be set.

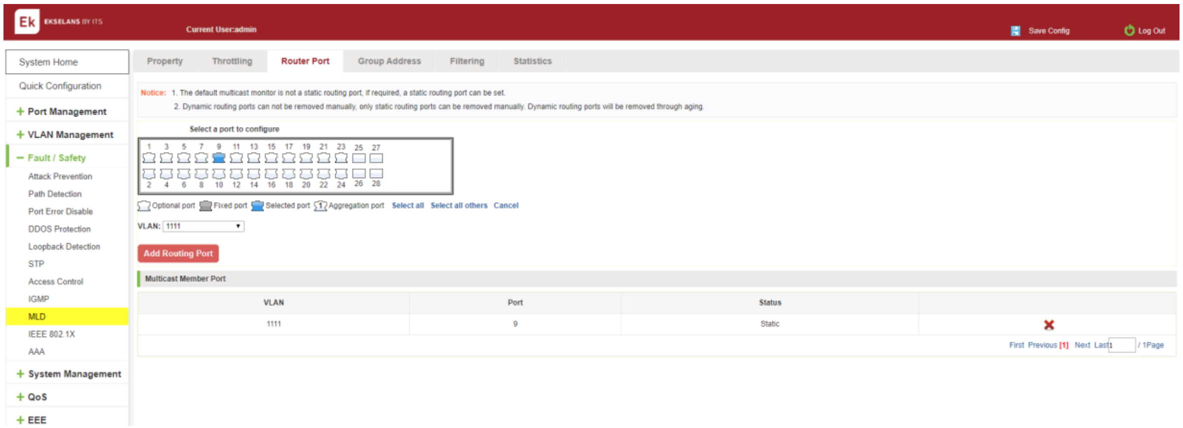
MLD Version selection

MLD Version MLD_V2

Figure 6-46: Closed multicast listener function operation.

CONFIGURATION MULTICAST ROUTING.

Select VLAN, click "Router Port Add" button, to configure the multicast routing in the port panel:



Notice: 1. The default multicast monitor is not a static routing port, if required, a static routing port can be set.
2. Dynamic routing ports can not be removed manually, only static routing ports can be removed manually. Dynamic routing ports will be removed through aging.

VLAN: 1111

VLAN	Port	Status	
1111	9	Static	✗

Figure 6-47: Configuration of multicast routing.

Multicast routing configuration steps are as follows:

Step1: In the port panel to select multicast listener routing port.

Step2: Select VLAN.

Step3: Click on the "Add Router Port" button to complete the configuration.

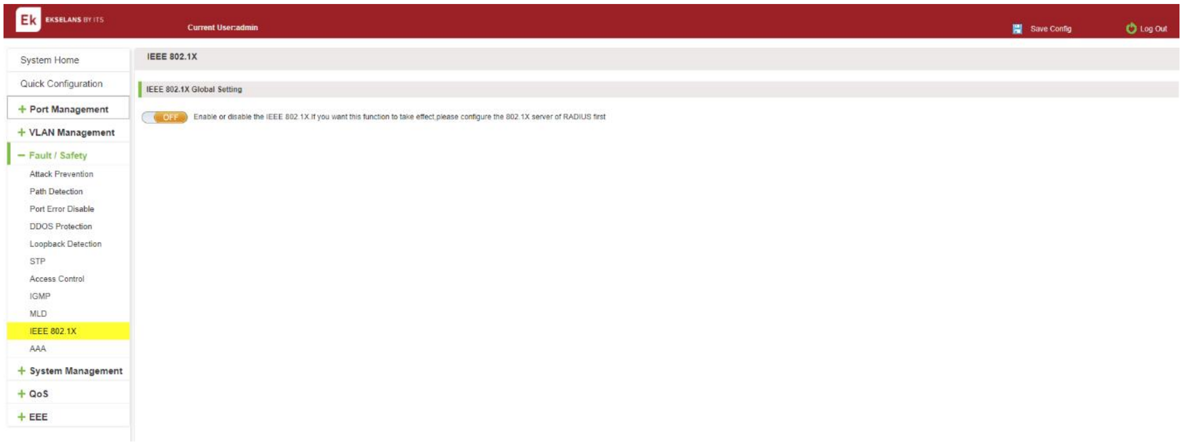
IEEE 802.1X.

IEEE 802.1X is a port-based authentication protocol, is a method and strategy for authenticating users.

Configure the PC 192.168.2.145, and connect with switch by Gi 0/2

Configure the radius sever 192.168.2.100, and connect with switch by Gi 0/1

Click ON "Fault / safety" "IEEE 802.1X".



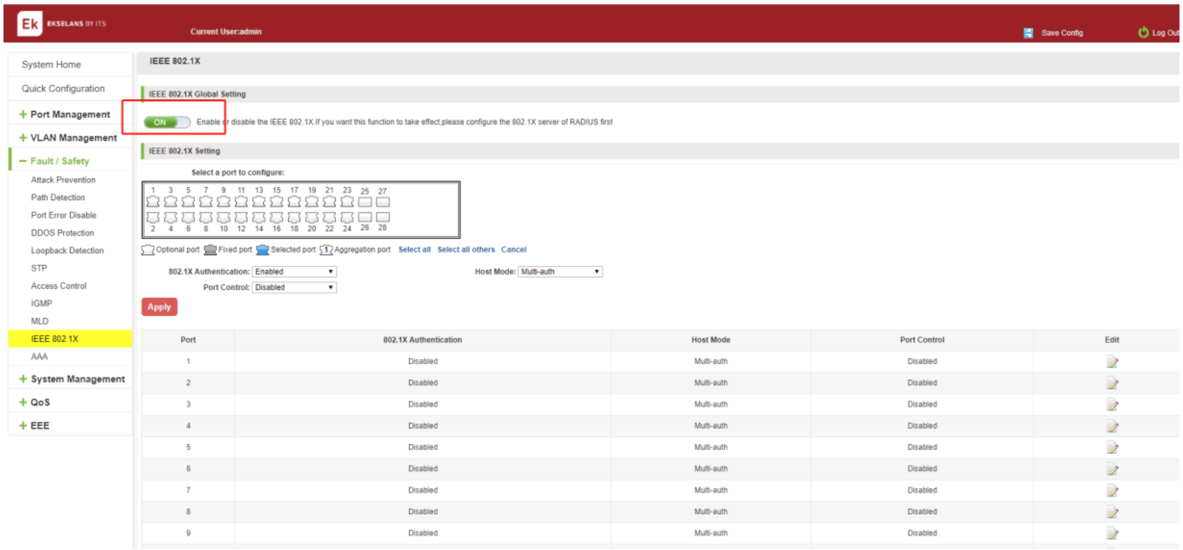
IEEE 802.1X

IEEE 802.1X Global Setting

OFF Enable or disable the IEEE 802.1X.If you want this function to take effect,please configure the 802.1X server of RADIUS first

Figure 6-48: IEEE 802.1X.

Click to OPEN.



IEEE 802.1X

IEEE 802.1X Global Setting

ON Enable or disable the IEEE 802.1X.If you want this function to take effect,please configure the 802.1X server of RADIUS first

IEEE 802.1X Setting

Select a port to configure:

802.1X Authentication: Enabled

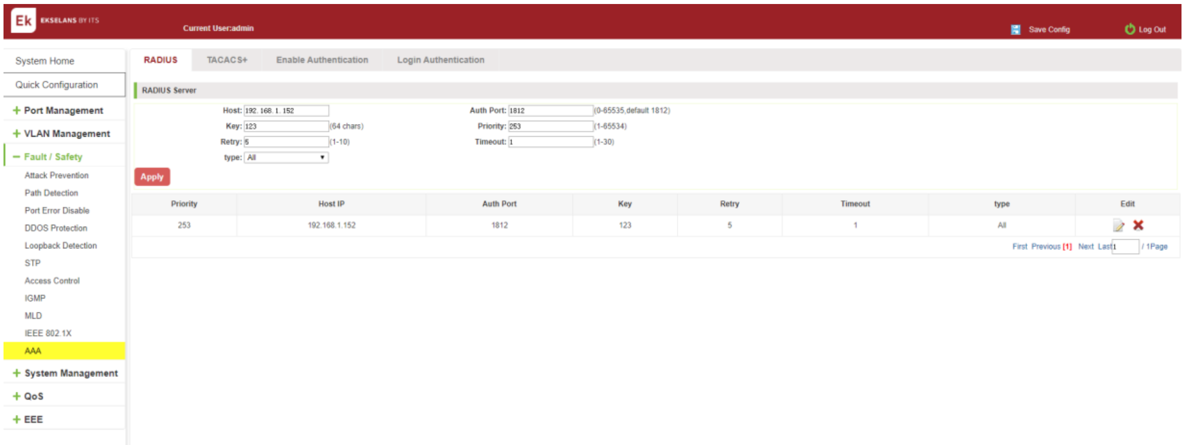
Host Mode: Multi-auth

Port Control: Disabled

Port	802.1X Authentication	Host Mode	Port Control	Edit
1	Disabled	Multi-auth	Disabled	✎
2	Disabled	Multi-auth	Disabled	✎
3	Disabled	Multi-auth	Disabled	✎
4	Disabled	Multi-auth	Disabled	✎
5	Disabled	Multi-auth	Disabled	✎
6	Disabled	Multi-auth	Disabled	✎
7	Disabled	Multi-auth	Disabled	✎
8	Disabled	Multi-auth	Disabled	✎
9	Disabled	Multi-auth	Disabled	✎

Figure 6-49: Enable IEEE 802.1X.

Switch config AAA RADIUS server addres:192.168.1.152, Auth Port: 1812, Key:123, type: all.



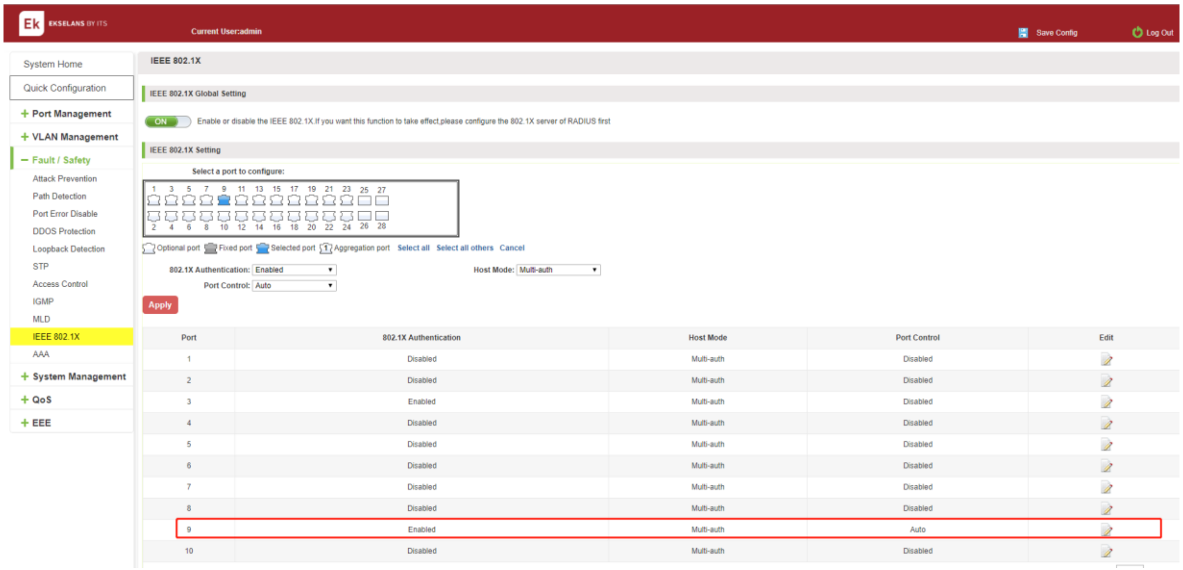
RADIUS Server

Host: 192. 168. 1. 152
Key: 123 (64 chars)
Retry: 5 (1-10)
type: All
Auth Port: 1812 (0-65535,default 1812)
Priority: 253 (1-65534)
Timeout: 1 (1-30)

Priority	Host IP	Auth Port	Key	Retry	Timeout	type	Edit
253	192.168.1.152	1812	123	5	1	All	

First Previous [1] Next Last 1 / 1Page

Switch enable 802.1X port Gi 0/9, Port Control: auto, Host Mode: multi-auth.



IEEE 802.1X

IEEE 802.1X Global Setting

ON Enable or disable the IEEE 802.1X.If you want this function to take effect,please configure the 802.1X server of RADIUS first

IEEE 802.1X Setting

Select a port to configure:

802.1X Authentication: Enabled
Port Control: Auto
Host Mode: Multi-auth

Port	802.1X Authentication	Host Mode	Port Control	Edit
1	Disabled	Multi-auth	Disabled	
2	Disabled	Multi-auth	Disabled	
3	Enabled	Multi-auth	Disabled	
4	Disabled	Multi-auth	Disabled	
5	Disabled	Multi-auth	Disabled	
6	Disabled	Multi-auth	Disabled	
7	Disabled	Multi-auth	Disabled	
8	Disabled	Multi-auth	Disabled	
9	Enabled	Multi-auth	Auto	
10	Disabled	Multi-auth	Disabled	

Figure 6-51: configuration IEEE802.1X.

Tips： The IEEE802.1x function is used with the AAA function.

Auto: It indicates that the initial state of the port is unauthorized. It only allows EAPOL packets to be sent and received. It does not allow users to access network resources. If the authentication passes, the port switches to the authorized state, allowing the user to access the network resources. This is also the most common case.

Force-auth: Indicates that the port is always authorized, allowing users to access network resources without authorization.

Force-unit: Indicates that the port is always in an unauthorized state and does not allow the user to authenticate. The device does not provide authentication services to clients that pass through the port.

Single host: This port can only connect to a host, through authentication can be forwarded for data packets.

Multi-auth: This port can be connected to the following switches, including a host through the certification, other hosts can be forwarded data packets.

Multi-host: This port can be connected to the following switches, including a host through the certification, other host data packets cannot be forwarded, must also have passed authentication.

AAA.

RADIUS.

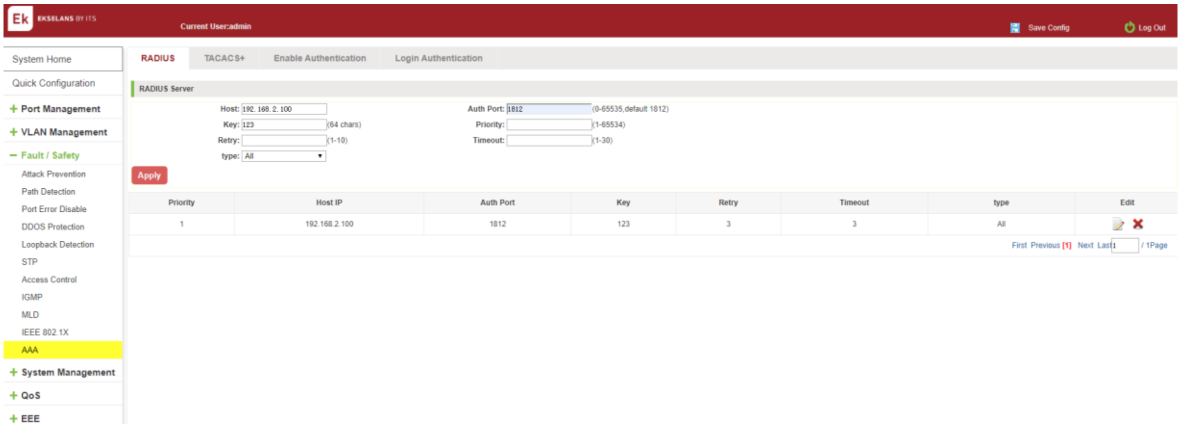
Enabled and logged in can use radius authentication.

Configure the PC 192.168.2.145 and connect with switch by Gi 0/2.

Configure the radius sever 192.168.2.100 and connect with switch by Gi 0/1.

Click ON "Fault / safety" "AAA" "RADIUS".

Switch config AAA RADIUS server addres:192.168.2.100, Auth Port:1812, Key:123, type: all.



RADIUS Server

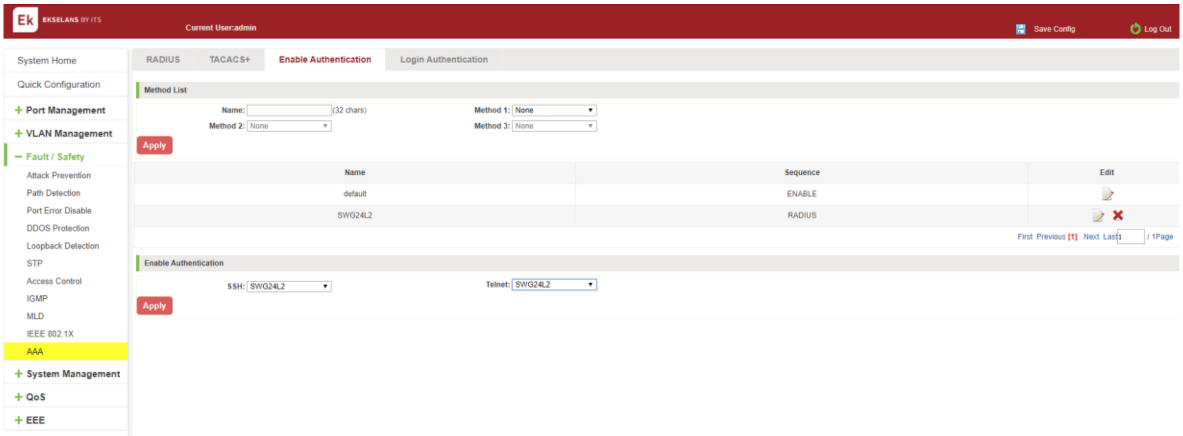
Host: 192. 168. 2. 100
Key: 123 (64 chars)
Retry: (1-10)
type: All
Auth Port: 1812 (0-65535,default 1812)
Priority: (1-65534)
Timeout: (1-30)

Priority	Host IP	Auth Port	Key	Retry	Timeout	type	Edit
1	192.168.2.100	1812	123	3	3	All	✎ ✖

Figure 6-52: configuration radius.

Switch config Method List: Name: test, Method1: RADIUS, Click Apply.

Switch config Enable Authentication: Console: SWG24L2, Telnet: SWG24L2, SSH: SWG24L2Click Apply.



Method List

Name: (32 chars)
Method 2: None
Method 1: None
Method 3: None

Name	Sequence	Edit
default	ENABLE	✎
SWG24L2	RADIUS	✎ ✖

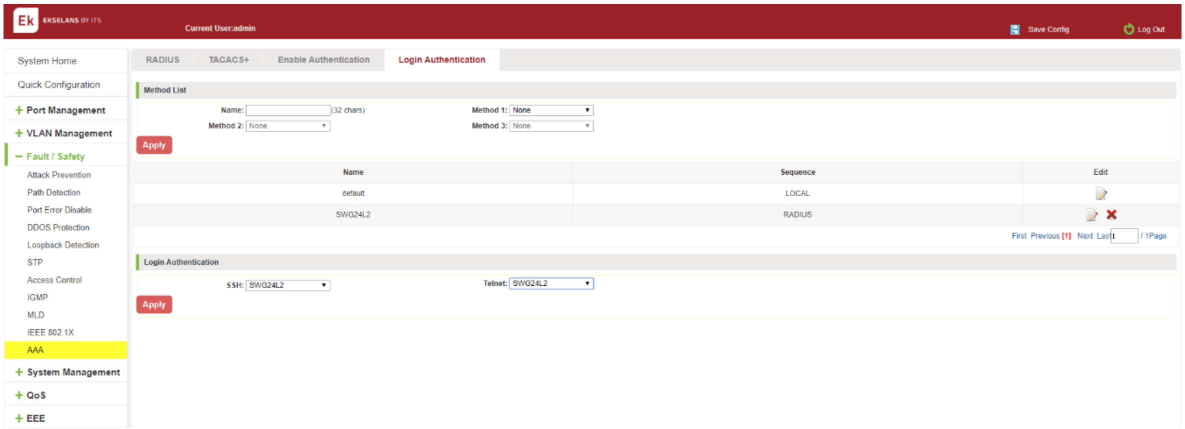
Enable Authentication

SSH: SWG24L2
Telnet: SWG24L2

Figure 6-53: configuration enable authentication

Switch config Method List: Name: SWG24L2, Method 1: RADIUS, Click Apply.

Switch config Enable Authentication: Console: SWG24L2, Telnet: SWG24L2, SSH: SWG24L2, Click Apply.



Method List

Name: (32 chars) Method 1: None
Method 2: None Method 3: None

Name	Sequence	Edit
default	LOCAL	
SWG24L2	RADIUS	

Login Authentication

SSH: SWG24L2 Telnet: SWG24L2

Figure 6-54: configuration login authentication.

TIPS:

1. PC input right username and password, PC can console, telnet and ssh switch
2. PC input right password, user can join "# mode".

TACACS+.

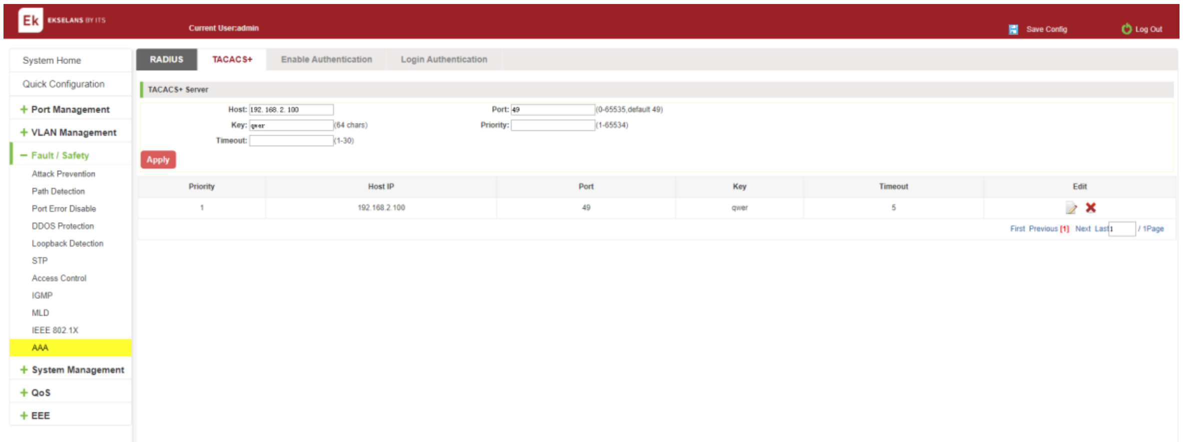
Enable and Login can use TACACS+ authentication.

Configure the PC 192.168.2.145 and connect with switch by Gi 0/2.

Configure the TACACS+ sever 192.168.2.100 and connect with switch by Gi 0/1.

Click ON "Fault / safety" "AAA" "TACACS+".

Switch config AAA TACACS+ server addres:192.168.2.100, Auth Port:49, Key: qwer.



TACACS+ Server

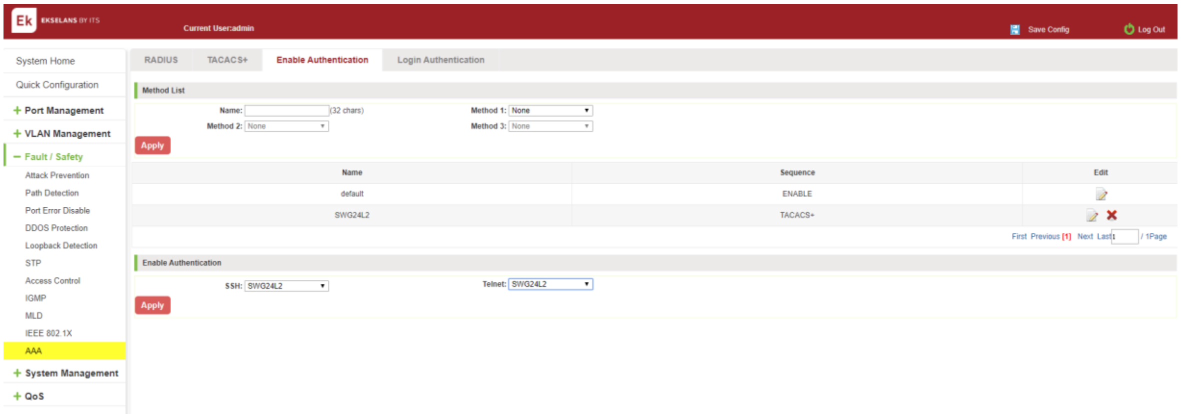
Host: 192. 168. 2. 100
Port: 49 (0-65535,default 49)
Key: qwer (64 chars)
Priority: (1-65534)
Timeout: (1-30)

Priority	Host IP	Port	Key	Timeout	Edit
1	192.168.2.100	49	qwer	5	✎ ✖

Figure 6-55: configuration TACACS+.

Switch config Method List: Name: SWG24L2, Method 1: TACACS+ Click Apply.

Switch config Enable Authentication: Console: SWG24L2, Telnet: SWG24L2, SSH: SWG24L2, Click Apply.



Method List

Name: (32 chars)
Method 1: None
Method 2: None
Method 3: None

Name	Sequence	Edit
default	ENABLE	✎
SWG24L2	TACACS+	✎ ✖

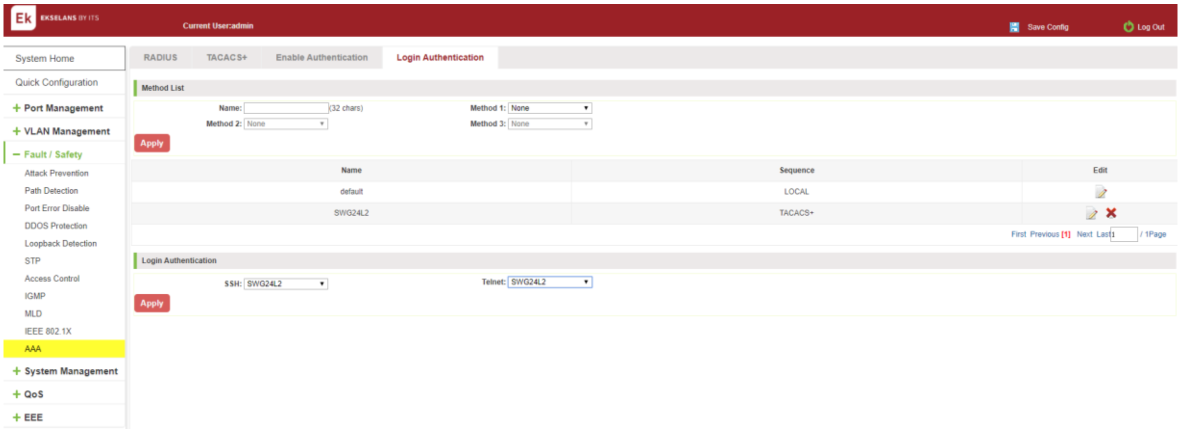
Enable Authentication

SSH: SWG24L2
Telnet: SWG24L2

Figure 6-56: configuration enable authentication.

Switch config Method List: Name: SWG24L2, Method 1: TACACS+, Click Apply.

Switch config Enable Authentication: Console: SWG24L2, Telnet: SWG24L2, SSH: SWG24L2, Click Apply.



Method List

Name: (32 chars) Method 1: None
Method 2: None Method 3: None

Name	Sequence	Edit
default	LOCAL	
SWG24L2	TACACS+	

Login Authentication

SSH: SWG24L2 Telnet: SWG24L2

Figure 6-57: configuration login authentication.

You can successfully open AAA TACACS+ function.

PC input right username and password, PC can console, telnet and ssh switch.

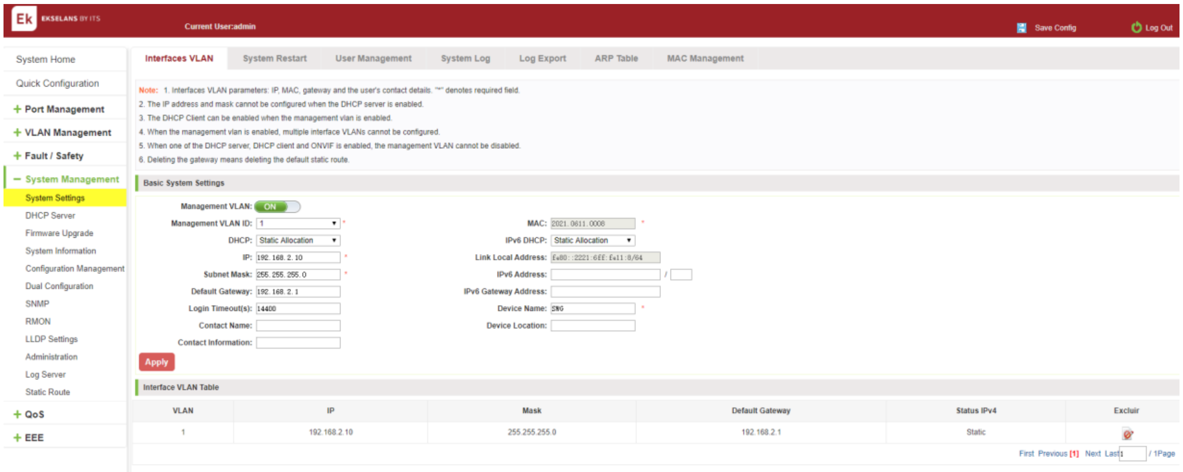
PC input right password, user can join "# mode".

System management.

System settings

CONFIGURATION BASIC SYSTEM SETTINGS.

Click on the navigation bar "System Management" "System Settings" " Management VLAN" to view the management address of the current switch configuration information:



Note: 1. Interfaces VLAN parameters: IP, MAC, gateway and the user's contact details. "*" denotes required field.
2. The IP address and mask cannot be configured when the DHCP server is enabled.
3. The DHCP Client can be enabled when the management vlan is enabled.
4. When the management vlan is enabled, multiple interface VLANs cannot be configured.
5. When one of the DHCP server, DHCP client and ONVIF is enabled, the management VLAN cannot be disabled.
6. Deleting the gateway means deleting the default static route.

Basic System Settings

Management VLAN: ON
Management VLAN ID: 1 *
DHCP: Static Allocation
IP: 192. 168. 2. 10 *
Subnet Mask: 255. 255. 255. 0 *
Default Gateway: 192. 168. 2. 1
Login Timeout(s): 14400
Contact Name:
Contact Information:
MAC: 2021. 0611. 0008 *
IPv6 DHCP: Static Allocation
Link Local Address: fe80::2221:6ff:fe11:8/64
IPv6 Address: /
IPv6 Gateway Address:
Device Name: SWG *
Device Location:

Interface VLAN Table

VLAN	IP	Mask	Default Gateway	Status IPv4	Excluir
1	192.168.2.10	255.255.255.0	192.168.2.1	Static	

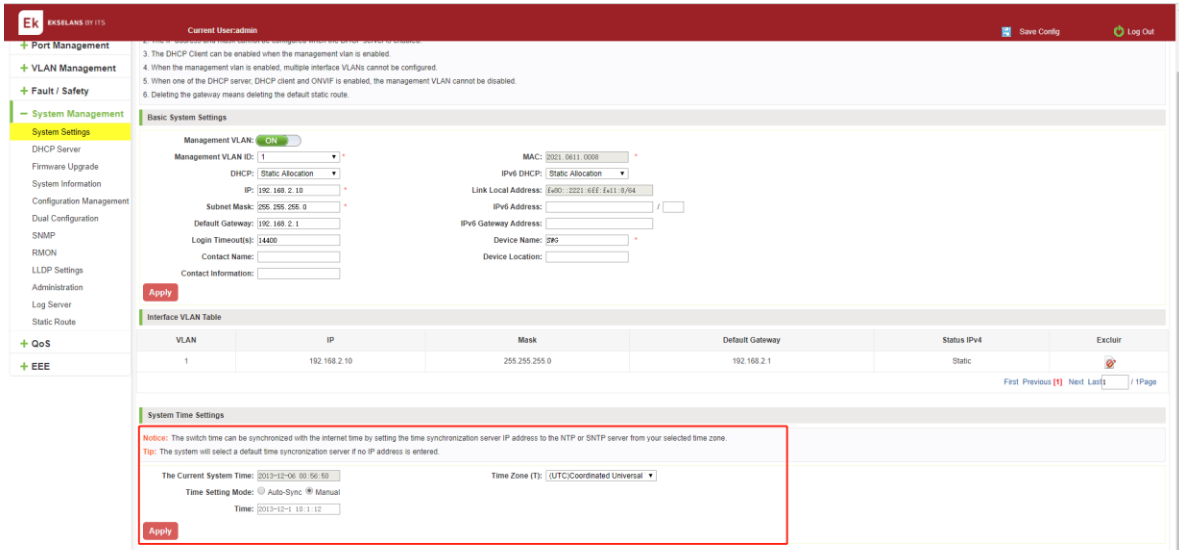
Figure 7-1: basic system settings.

To configure the switch Basic System Settings as follows:

Management VLAN: switch management VLAN ID, the default is 1:

1. In the DHCP text box, choose static allocation.
2. In the Management IP text box, enter the IP address, such as 192.168.2.10
3. In the Subnet Mask text box, enter the subnet mask, such as 255.255.255.0.
4. In the Gateway Address text box to enter the gateway address, such as 192.168.2.1.
5. In the **Device Location** text box, enter the **Device Location**, such as China.
6. In the **Contact Name** text box, enter the **Contact Name**, such as john.
7. In the **Contact Information** text box, enter **Contact Information**, such as 12345678900.
8. Click on "Apply Settings" button to complete the configuration.

SYSTEM TIME SYNCHRONIZATION.



3. The DHCP Client can be enabled when the management vlan is enabled.
4. When the management vlan is enabled, multiple interface VLANs cannot be configured.
5. When one of the DHCP server, DHCP client and ONVIF is enabled, the management VLAN cannot be disabled.
6. Deleting the gateway means deleting the default static route.

Basic System Settings

Management VLAN: ON
Management VLAN ID: 1 *
DHCP: Static Allocation
IP: 192.168.2.10 *
Subnet Mask: 255.255.255.0 *
Default Gateway: 192.168.2.1
Login Timeout(s): 14400
Contact Name:
Contact Information:
MAC: 2021.0611.0008 *
IPv6 DHCP: Static Allocation
Link Local Address: fe80::2221:6ff:fe11:8/64
IPv6 Address: /
IPv6 Gateway Address:
Device Name: SWG *
Device Location:

Interface VLAN Table

VLAN	IP	Mask	Default Gateway	Status IPv4	Excluir
1	192.168.2.10	255.255.255.0	192.168.2.1	Static	

First Previous [1] Next Last 1 / 1Page

System Time Settings

Notice: The switch time can be synchronized with the internet time by setting the time synchronization server IP address to the NTP or SNTP server from your selected time zone.
Tip: The system will select a default time syncronization server if no IP address is entered.

The Current System Time: 2013-12-06 00:56:50
Time Setting Mode: ○ Auto-Sync ● Manual
Time: 2013-12-1 10:1:12
Time Zone (T): (UTC)Coordinated Universal

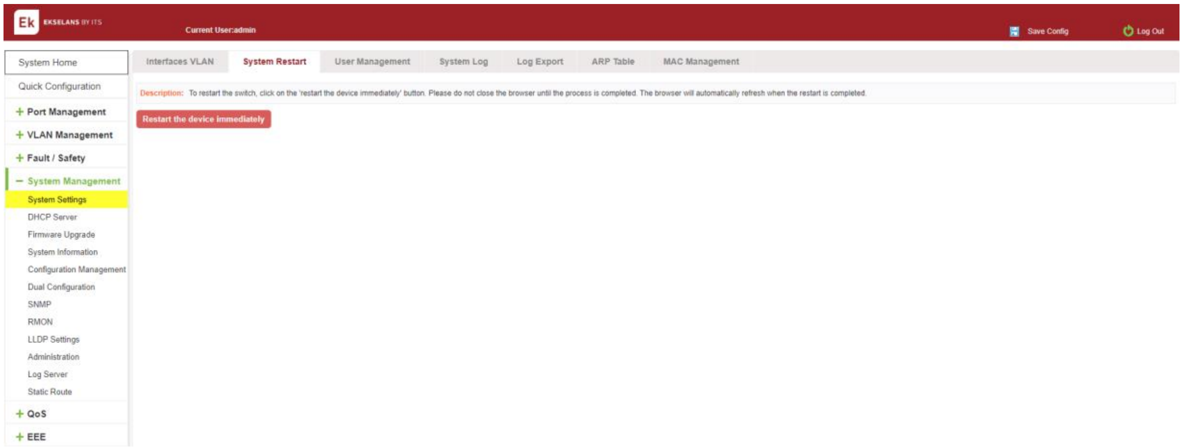
Figure 7-2: System time synchronization.

To configuration system time, You can select NTP or SNTP, enter SNTP/NTP Server IP Address such as 203.117.180.36(local SNTP/NTP servers or internet SNTP/NTP servers), in the Time Zone (T) text box, you can choose any time zone you want, such as UTC+08:00

The user can manually configure the device system time.

System restart.

Click on the navigation bar "System Management" "System Settings" "System Restart" to reboot the switch:



Description: To restart the switch, click on the 'restart the device immediately' button. Please do not close the browser until the process is completed. The browser will automatically refresh when the restart is completed.

Figure 7-6: System Restart

Restart the device, follow these steps:

step1: Click on "Restart the device immediately" button.

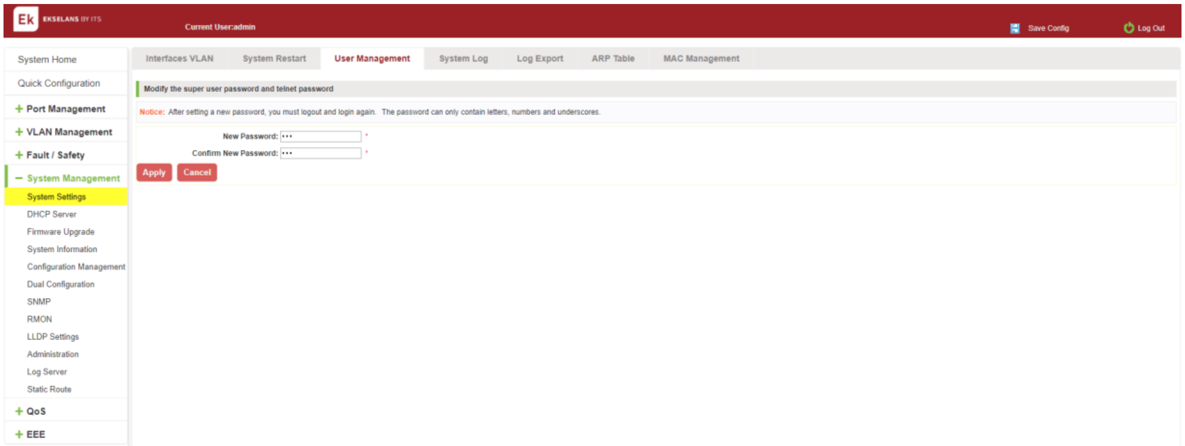
step2: Click OK in the box that pops up "OK" button.

step3: Prompted to Apply the current configuration, depending on your need to select "OK" or "Cancel".

step4: After the restart the progress bar moves to 100%, reboot the device.

Change PassWord.

Click on the navigation bar "System Management" "System Settings" "change password" to modify the super user password:



Modify the super user password and telnet password

Notice: After setting a new password, you must logout and login again. The password can only contain letters, numbers and underscores.

New Password: ••• *

Confirm New Password: ••• *

Figure 7-7: change password.

Change password follow these steps:

Step1: Enter the new password: admin.

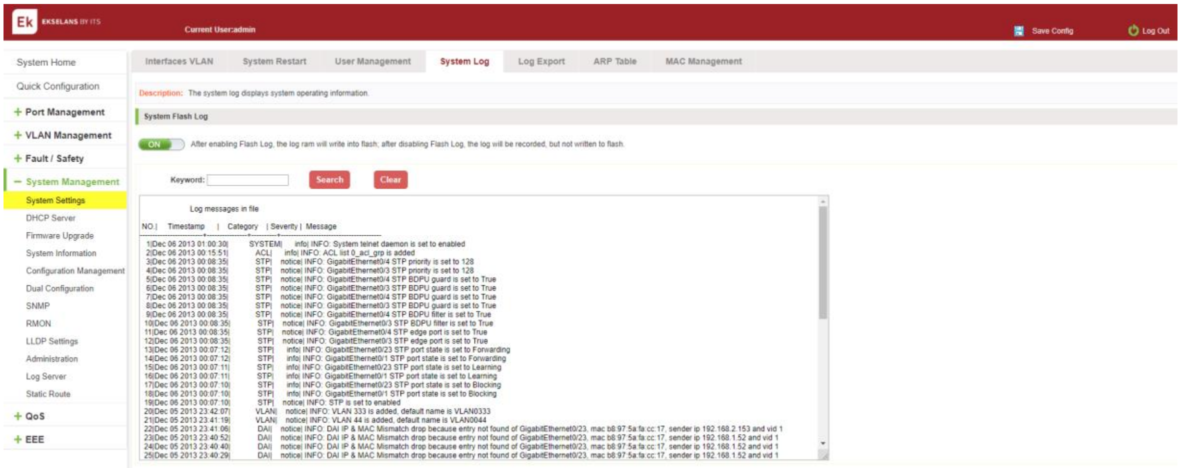
Step2: Confirm new password: admin.

Step3: Click the "Apply" button.

Step5: Pop-up dialog box, click "OK" button.

System Log.

Click on the navigation bar "System Management" "System Settings" "System Log" to enter the log management interface, you can query the system log, clear the log:



Description: The system log displays system operating information.

System Flash Log

ON After enabling Flash Log, the log ram will write into flash; after disabling Flash Log, the log will be recorded, but not written to flash.

Keyword:

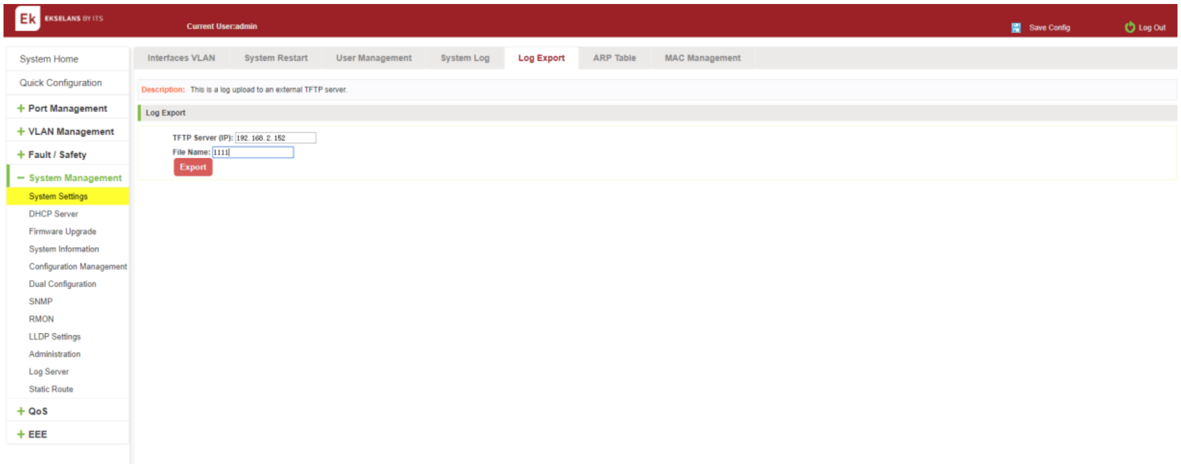
```
           Log messages in file

NO.|   Timestamp      |   Category   | Severity |  Message
-----------------------+-------------+---------+-------------------------------------
  1|Dec 06 2013 01:00:30|        SYSTEM|      info| INFO: System telnet daemon is set to enabled
  2|Dec 06 2013 00:15:51|           ACL|     info| INFO: ACL list 0_acl_grp is added
  3|Dec 06 2013 00:08:35|           STP|   notice| INFO: GigabitEthernet0/4 STP priority is set to 128
  4|Dec 06 2013 00:08:35|           STP|   notice| INFO: GigabitEthernet0/3 STP priority is set to 128
  5|Dec 06 2013 00:08:35|           STP|   notice| INFO: GigabitEthernet0/4 STP BDPU guard is set to True
  6|Dec 06 2013 00:08:35|           STP|   notice| INFO: GigabitEthernet0/3 STP BDPU guard is set to True
  7|Dec 06 2013 00:08:35|           STP|   notice| INFO: GigabitEthernet0/4 STP BDPU guard is set to True
  8|Dec 06 2013 00:08:35|           STP|   notice| INFO: GigabitEthernet0/3 STP BDPU guard is set to True
  9|Dec 06 2013 00:08:35|           STP|   notice| INFO: GigabitEthernet0/4 STP BDPU filter is set to True
 10|Dec 06 2013 00:08:35|           STP|   notice| INFO: GigabitEthernet0/3 STP BDPU filter is set to True
 11|Dec 06 2013 00:08:35|           STP|   notice| INFO: GigabitEthernet0/4 STP edge port is set to True
 12|Dec 06 2013 00:08:35|           STP|   notice| INFO: GigabitEthernet0/3 STP edge port is set to True
 13|Dec 06 2013 00:07:12|           STP|     info| INFO: GigabitEthernet0/23 STP port state is set to Forwarding
 14|Dec 06 2013 00:07:12|           STP|     info| INFO: GigabitEthernet0/1 STP port state is set to Forwarding
 15|Dec 06 2013 00:07:11|           STP|     info| INFO: GigabitEthernet0/23 STP port state is set to Learning
 16|Dec 06 2013 00:07:11|           STP|     info| INFO: GigabitEthernet0/1 STP port state is set to Learning
 17|Dec 06 2013 00:07:10|           STP|     info| INFO: GigabitEthernet0/23 STP port state is set to Blocking
 18|Dec 06 2013 00:07:10|           STP|     info| INFO: GigabitEthernet0/1 STP port state is set to Blocking
 19|Dec 06 2013 00:07:10|           STP|   notice| INFO: STP is set to enabled
 20|Dec 05 2013 23:42:07|          VLAN|   notice| INFO: VLAN 333 is added, default name is VLAN0333
 21|Dec 05 2013 23:41:19|          VLAN|   notice| INFO: VLAN 44 is added, default name is VLAN0044
 22|Dec 05 2013 23:41:06|           DAI|   notice| INFO: DAI IP & MAC Mismatch drop because entry not found of GigabitEthernet0/23, mac b8:97:5a:fa:cc:17, sender ip 192.168.2.153 and vid 1
 23|Dec 05 2013 23:40:52|           DAI|   notice| INFO: DAI IP & MAC Mismatch drop because entry not found of GigabitEthernet0/23, mac b8:97:5a:fa:cc:17, sender ip 192.168.1.52 and vid 1
 24|Dec 05 2013 23:40:40|           DAI|   notice| INFO: DAI IP & MAC Mismatch drop because entry not found of GigabitEthernet0/23, mac b8:97:5a:fa:cc:17, sender ip 192.168.1.52 and vid 1
 25|Dec 05 2013 23:40:29|           DAI|   notice| INFO: DAI IP & MAC Mismatch drop because entry not found of GigabitEthernet0/23, mac b8:97:5a:fa:cc:17, sender ip 192.168.1.52 and vid 1
```

Figure 7-8: system log.

Log management system WEB page to view the contents of the command line is consistent with the results of the command show logging; Click "Clear" button to clear the current log information switch.

Log Export.

Click on the navigation bar "System Management" "System Settings" "Log Export" to export log information into the interface, you can export the log information through tftp server.



Description: This is a log upload to an external TFTP server.

Log Export

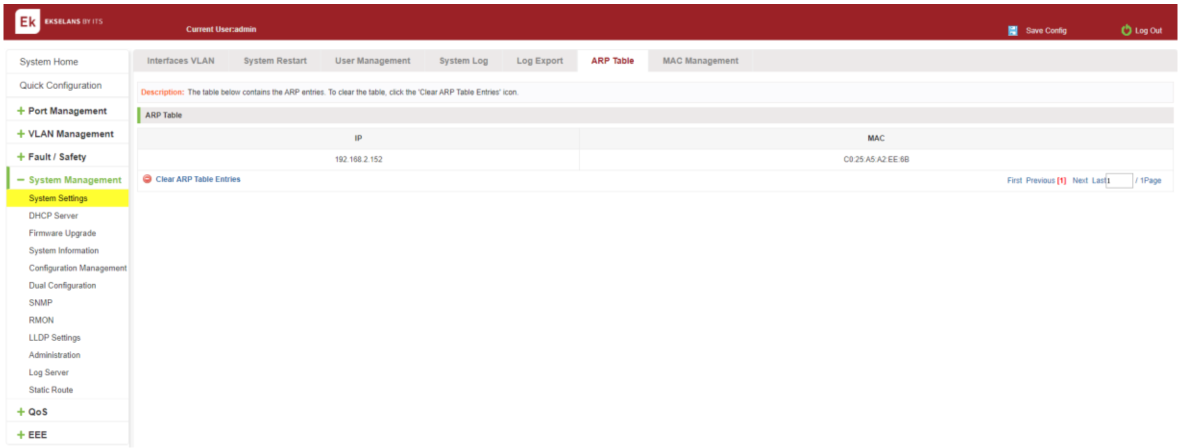
TFTP Server (IP): 192. 168. 2. 152

File Name: 1111

Figure 7-9: Log Export.

ARP table.

Click on the navigation bar "System Management" "System Settings" "ARP Table" to enter the ARP entry interface, you can view the ARP information:



Description: The table below contains the ARP entries. To clear the table, click the 'Clear ARP Table Entries' icon.

ARP Table

IP	MAC
192.168.2.152	C0:25:A5:A2:EE:6B

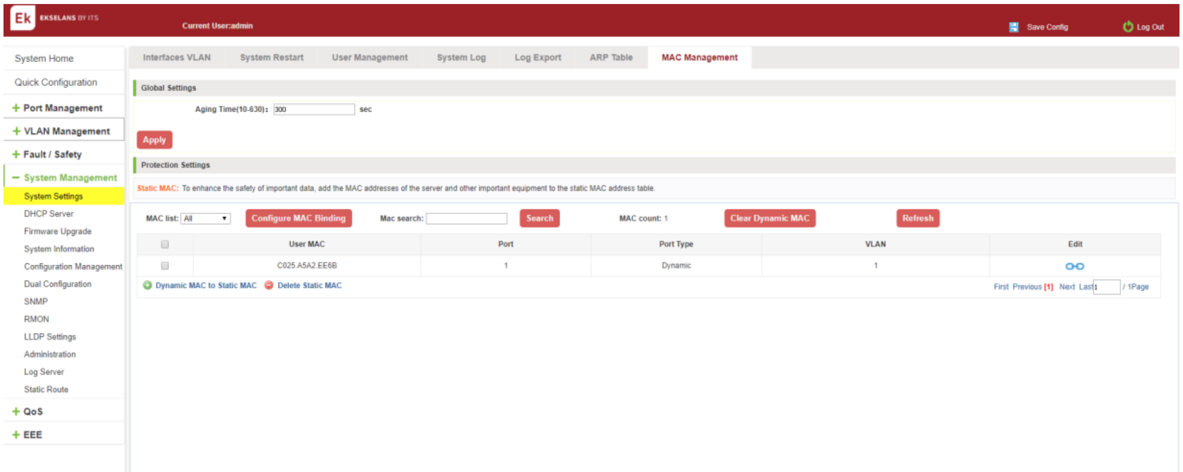
Figure 7-10: ARP message

Click "Clear ARP table entries" button to clear the display ARP information.

MAC management.

MAC ADDRESS LOOKUP

Click the "System Management" "System Settings" "MAC Management" can switch MAC address information query:



Global Settings

Aging Time(10-630): 300 sec

Protection Settings

Static MAC: To enhance the safety of important data, add the MAC addresses of the server and other important equipment to the static MAC address table.

MAC list: All

Mac search:

MAC count: 1

□	User MAC	Port	Port Type	VLAN	Edit
□	C025.A5A2.EE6B	1	Dynamic	1	⚯

Figure 7-11: MAC address lookup display.

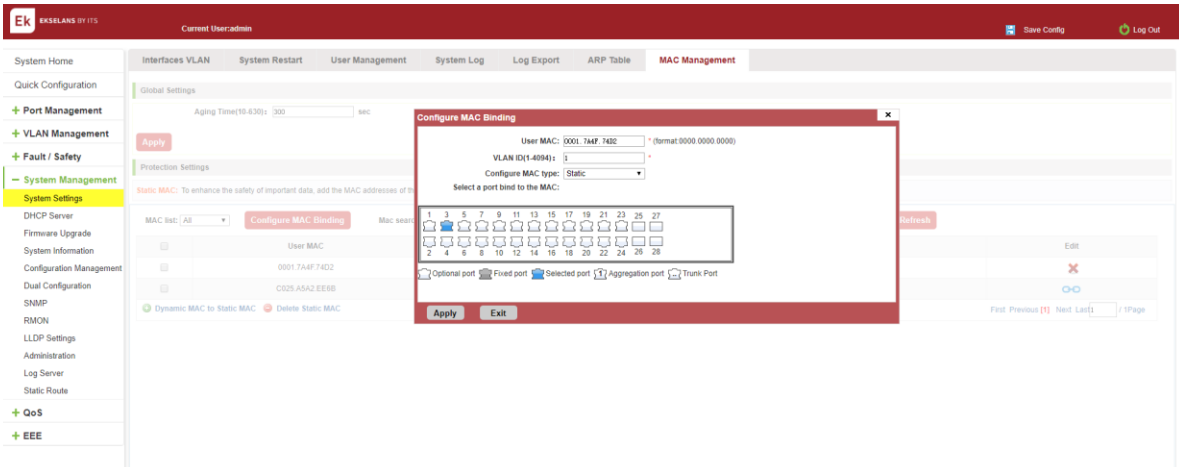
In the MAC address list, which shows the current switch port to learn MAC addresses:

1. User MAC: MAC address of the switch that currently exists is displayed.
2. Port: Displays the source port number of the MAC address.
3. Port Type: There are two types of dynamic and static.
4. VLAN: VLAN ID display value.

You can query the MAC address type: according to the type of query MAC address, Type in the MAC address MAC check list next to the drop-down box Select: All / static / dynamic.

ADD A STATIC MAC ADDRESS TYPE

1. Use manual binding MAC address Click the "Configure MAC Binding" After, you can configure a static MAC address type in the MAC address configuration area:



Aging Time(10-630): 300 sec

Static MAC: To enhance the safety of important data, add the MAC addresses of th

MAC list: All

□	User MAC
□	0001.7A4F.74D2
□	C025.A5A2.EE6B

Configure MAC Binding

User MAC: 0001. 7A4F. 74D2 * (format:0000.0000.0000)

VLAN ID(1-4094): 1 *

Configure MAC type: Static

Select a port bind to the MAC:

Figure 7-12: MAC addresses statically bound static configuration.

Statically typed MAC address configuration steps are as follows:

step1: Click the "Configure MAC Binding" button.

step2: In the "User MAC" text box to enter the MAC address, such as 0001.7A4F.74D2.

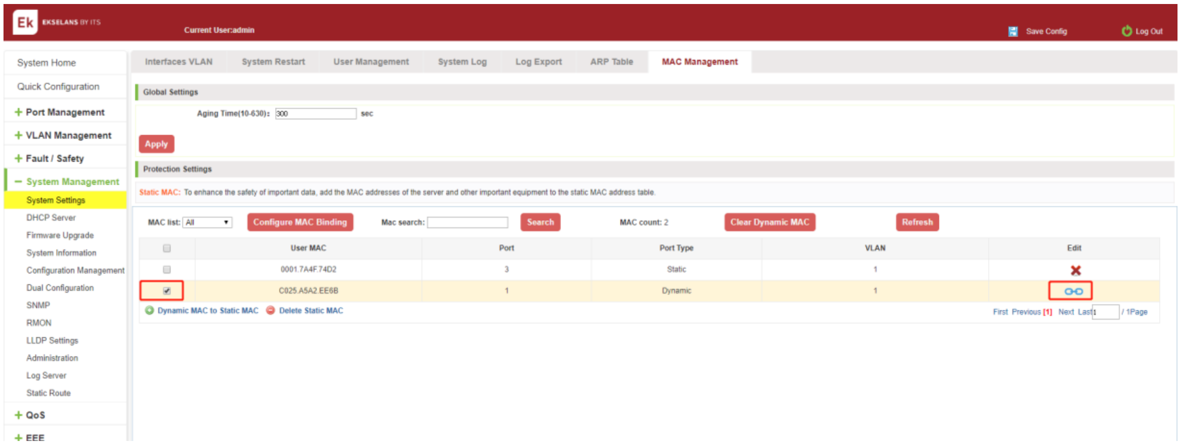
step3: In the "VLAN ID" text box to enter the VLAN ID, such as 1.

step4: Select ports in the port panel.

Step5: Click on "Apply" to complete the configuration.

2. Use " 🔗 " Button binding static MAC address

In the MAC address list, select the MAC address to be bound, click on the left " 🔗 " Button, to achieve binding:



Global Settings

Aging Time(10-630): 300 sec

Protection Settings

Static MAC: To enhance the safety of important data, add the MAC addresses of the server and other important equipment to the static MAC address table.

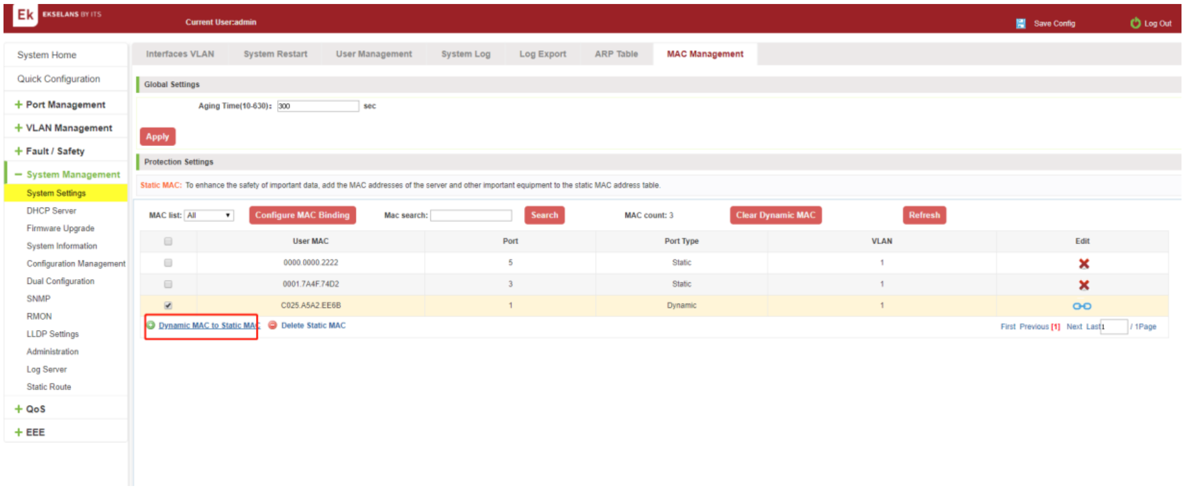
MAC list: All   Mac search: MAC count: 2

□	User MAC	Port	Port Type	VLAN	Edit
□	0001.7A4F.74D2	3	Static	1	✖
☑	C025.A5A2.EE6B	1	Dynamic	1	🔗

Figure 7-13: MAC address of the static binding configuration.

3. Using the "Dynamic MAC to Static MAC" link Bulk Bind static MAC

In the MAC address list by checking the front of the column you want to bind, "√" check box, click on the "Dynamic MAC to Static MAC" button to complete the configuration:



Global Settings

Aging Time(10-630): 300 sec

Protection Settings

Static MAC: To enhance the safety of important data, add the MAC addresses of the server and other important equipment to the static MAC address table.

MAC list: All   Mac search: MAC count: 3

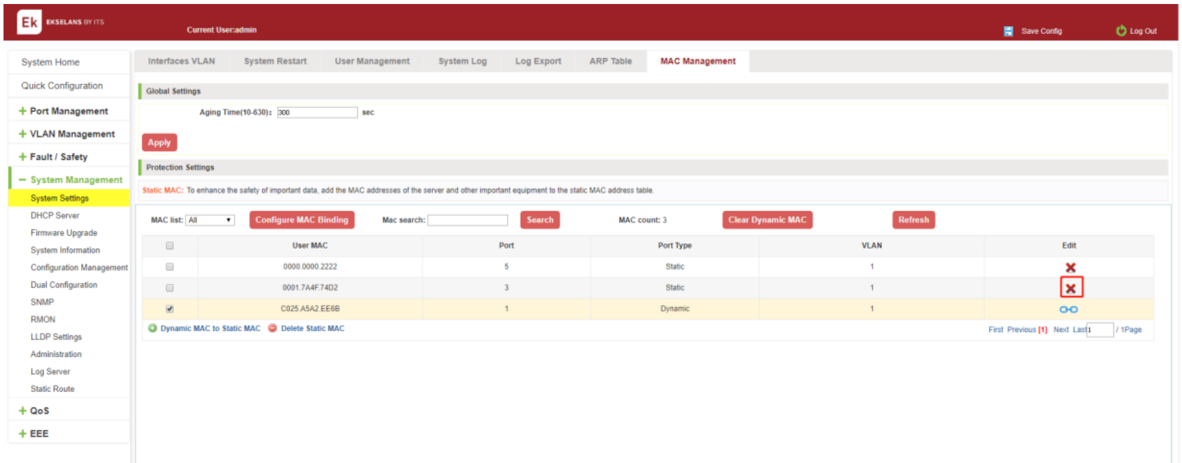
□	User MAC	Port	Port Type	VLAN	Edit
□	0000.0000.2222	5	Static	1	✖
□	0001.7A4F.74D2	3	Static	1	✖
☑	C025.A5A2.EE6B	1	Dynamic	1	🔗

Figure 7-14: Batch-MAC binding configuration.

REMOVE THE STATIC MAC ADDRESS TYPE.

1. Single MAC records are deleted.

Select the need to delete the MAC address, click the "X" button to delete a static MAC address type:



Aging Time(10-630): 300 sec

Static MAC: To enhance the safety of important data, add the MAC addresses of the server and other important equipment to the static MAC address table.

MAC list: All

Mac search:

MAC count: 3

□	User MAC	Port	Port Type	VLAN	Edit
□	0000.0000.2222	5	Static	1	✖
□	0001.7A4F.74D2	3	Static	1	✖
☑	C025.A5A2.EE6B	1	Dynamic	1	⚯

Figure 7-15: MAC address deletion.

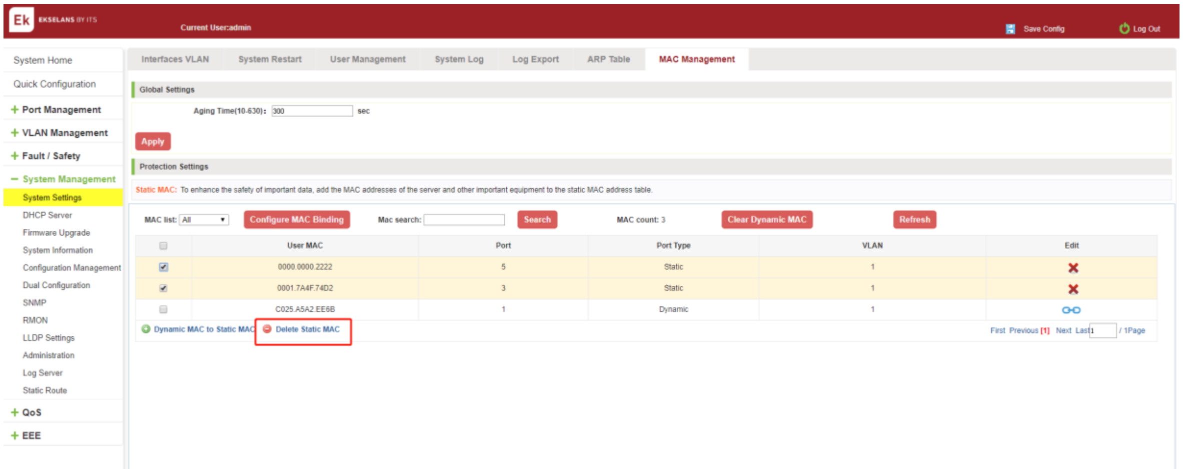
Remove MAC address configuration steps are as follows:

Step1: To delete the selected MAC address.

step2: Click " ✖ " button to delete the configuration.

1. Batch delete a static MAC address

In the MAC address list by checking the front of the column you want to bind, "√" check box, click "Delete Static MAC" button:



Aging Time(10-630): 300 sec

Static MAC: To enhance the safety of important data, add the MAC addresses of the server and other important equipment to the static MAC address table.

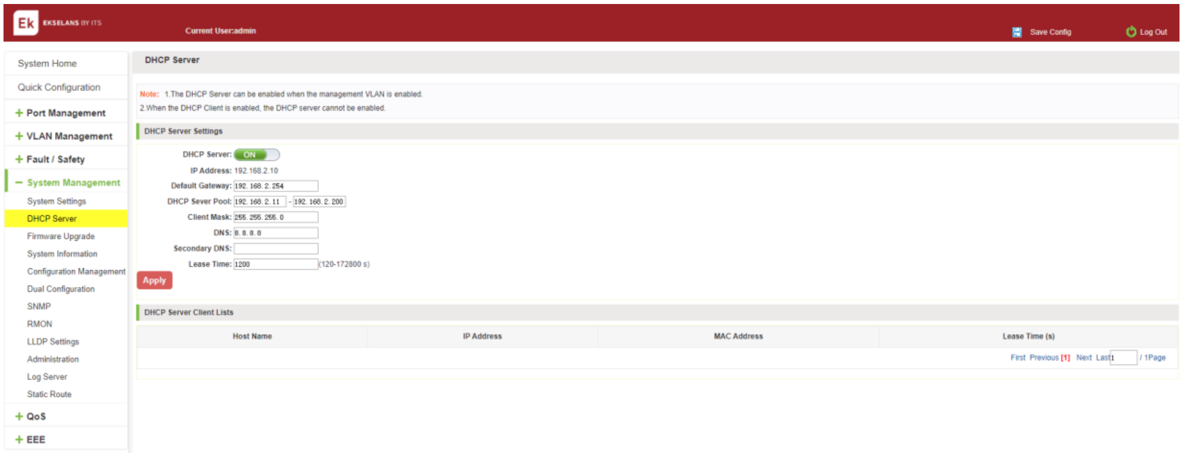
MAC list: All   Mac search: MAC count: 3

□	User MAC	Port	Port Type	VLAN	Edit
☑	0000.0000.2222	5	Static	1	✗
☑	0001.7A4F.74D2	3	Static	1	✗
□	C025.A5A2.EE6B	1	Dynamic	1	⚯

Figure 7-16: MAC address batch deletion deletion.

DHCP server.

Click on the navigation bar "System Management"   "DHCP Server" to configure the switch dhcp server:



DHCP Server

Note: 1.The DHCP Server can be enabled when the management VLAN is enabled.
2.When the DHCP Client is enabled, the DHCP server cannot be enabled.

DHCP Server Settings

DHCP Server: ON
IP Address: 192.168.2.10
Default Gateway: 192. 168. 2. 254
DHCP Sever Pool: 192. 168. 2. 11 - 192. 168. 2. 200
Client Mask: 255. 255. 255. 0
DNS: 8. 8. 8. 8
Secondary DNS:
Lease Time: 1200 (120-172800 s)

DHCP Server Client Lists

Host Name	IP Address	MAC Address	Lease Time (s)

Figure 7-5: DHCP server.

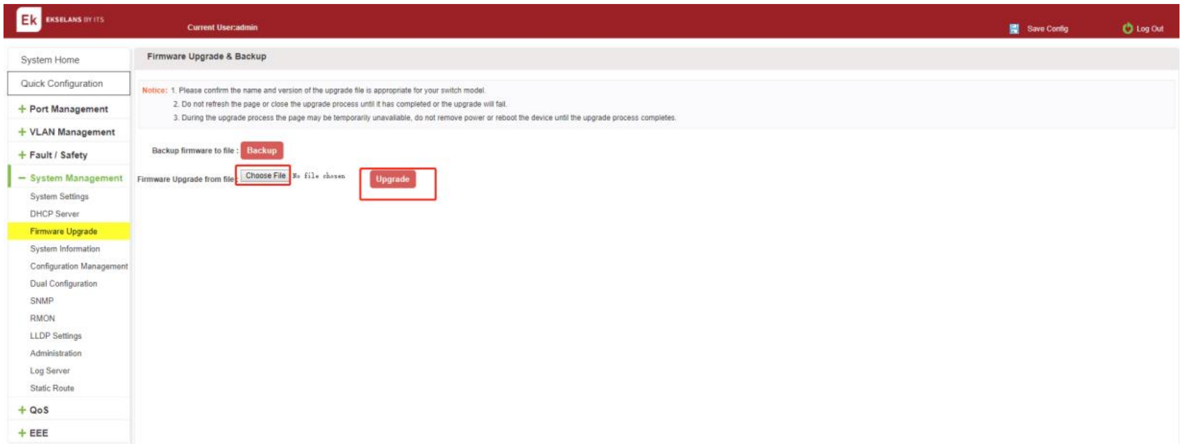
DHCP server configuration, follow these steps:

Step1: In the DHCP server, choose to enable.

Step2: In the DHCP client range, configure the server IP.

Firmware Upgrade.

Click the "System Management" "Firmware Upgrade" to upgrade the software on the switch:



Notice: 1. Please confirm the name and version of the upgrade file is appropriate for your switch model.
2. Do not refresh the page or close the upgrade process until it has completed or the upgrade will fail.
3. During the upgrade process the page may be temporarily unavailable, do not remove power or reboot the device until the upgrade process completes.

Backup firmware to file : Backup

Firmware Upgrade from file: Choose File No file chosen

Figure 7-17: Switch System Upgrade.

Switch system upgrade steps are as follows:

Step1: Click "Choose File" button to select the switch upgrade file.

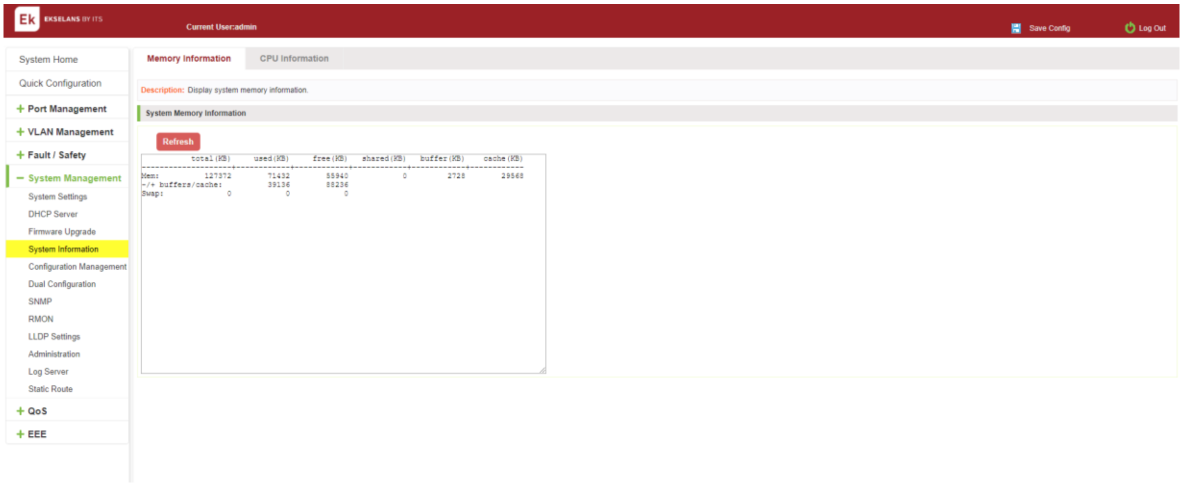
step2: Click the "Upgrade" button switch to start the upgrade new software.

step3: When the upgrade progress bar is at 100%, the switch will automatically reboot, completion of the upgrade is completed.

System information.

Memory information.

Click on the "System Management" "System Information" "of" the Memory Information into the Memory Information interface, can view the System Memory Information:



Description: Display system memory information.

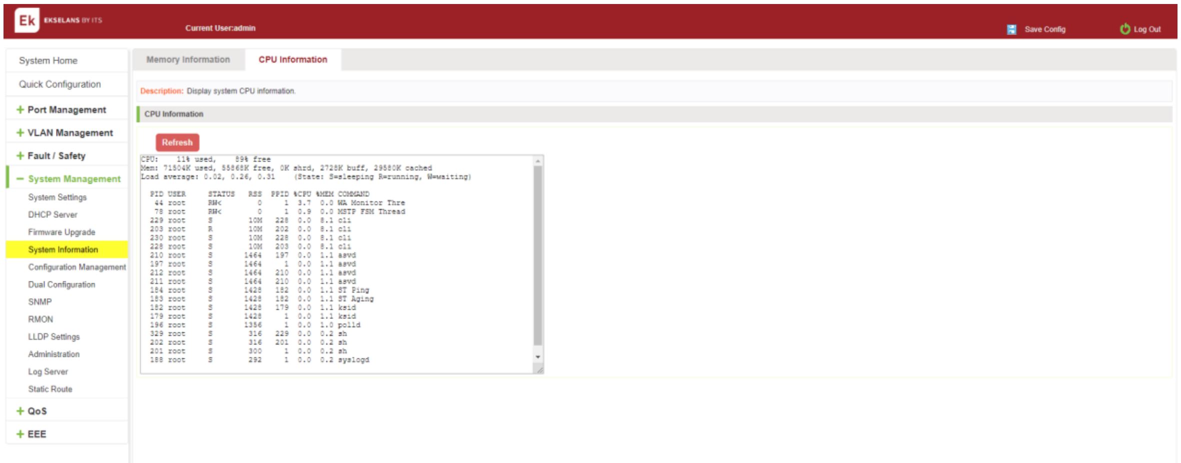
```
                  total(KB)   used(KB)   free(KB)  shared(KB)  buffer(KB)   cache(KB)
------------------+-----------+-----------+-----------+-----------+-----------
Mem:                 127372      71432      55940           0        2728       29568
-/+ buffers/cache:               39136      88236
Swap:                     0          0          0
```

Figure 7-18: System memory information.

See the WEB page of memory information content consistent with the results show the memory command command line. Click on the "Clear" button to Clear the current switches in the memory information; Click on the "Refresh" button to Refresh the current switches in the memory information.

CPU INFORMATION.

Click on the "System Management" "System Information" "CPU Information" to enter the CPU Information interface, can view the System task Information:



```
CPU:    11% used,    89% free
Mem: 71504K used, 55868K free, 0K shrd, 2728K buff, 29580K cached
Load average: 0.02, 0.26, 0.31    (State: S=sleeping R=running, W=waiting)

  PID USER     STATUS   RSS  PPID %CPU %MEM COMMAND
   44 root     RW<        0     1  3.7  0.0 WA Monitor Thre
   78 root     RW<        0     1  0.9  0.0 MSTP FSM Thread
  229 root     S        10M   228  0.0  8.1 cli
  203 root     R        10M   202  0.0  8.1 cli
  230 root     S        10M   228  0.0  8.1 cli
  228 root     S        10M   203  0.0  8.1 cli
  210 root     S       1464   197  0.0  1.1 asvd
  197 root     S       1464     1  0.0  1.1 asvd
  212 root     S       1464   210  0.0  1.1 asvd
  211 root     S       1464   210  0.0  1.1 asvd
  184 root     S       1428   182  0.0  1.1 ST Ping
  183 root     S       1428   182  0.0  1.1 ST Aging
  182 root     S       1428   179  0.0  1.1 ksid
  179 root     S       1428     1  0.0  1.1 ksid
  196 root     S       1356     1  0.0  1.0 polld
  329 root     S        316   229  0.0  0.2 sh
  202 root     S        316   201  0.0  0.2 sh
  201 root     S        300     1  0.0  0.2 sh
  188 root     S        292     1  0.0  0.2 syslogd
```

Figure 7-19: CPU information.

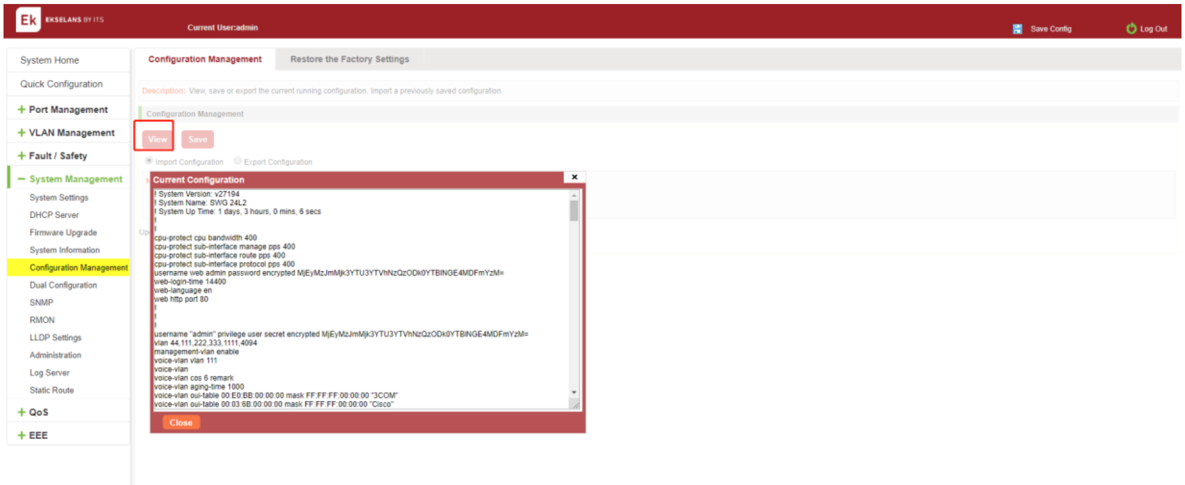
WEB pages to the content of the system task view consistent with the results show the CPU commands command line; click on the "Clear" button to remove the current switches in the system; Click on the "Refresh" button to Refresh the current switches in the system task.

Configuration management.

Configuration management.

To see the current configuration.

Click on "System Management" "Configuration Management" "Configuration Management", and click the button "View", View the current Configuration information:



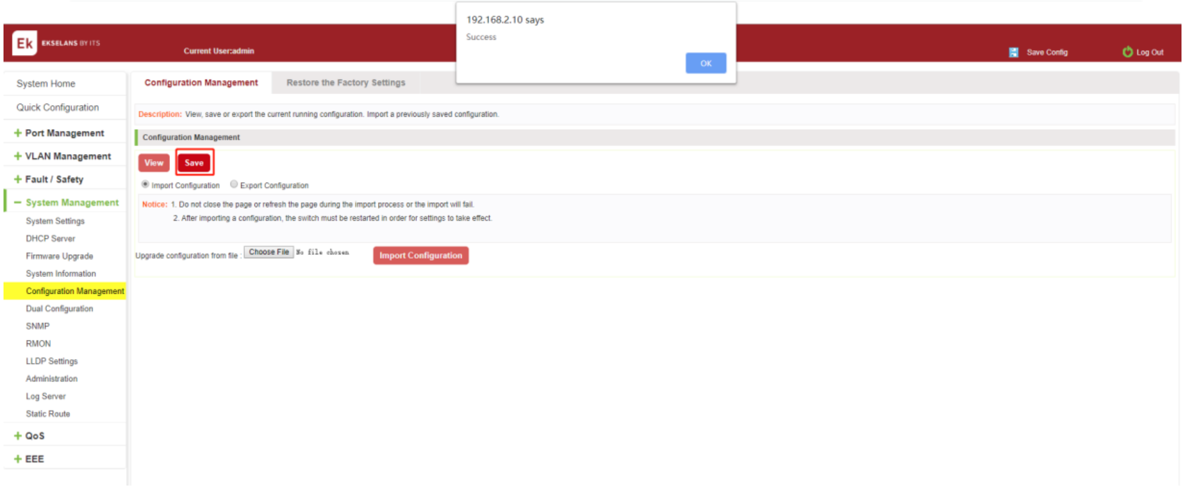
Description: View, save or export the current running configuration. Import a previously saved configuration.

```
! System Version: v27194
! System Name: SWG 24L2
! System Up Time: 1 days, 3 hours, 0 mins, 6 secs
!
!
cpu-protect cpu bandwidth 400
cpu-protect sub-interface manage pps 400
cpu-protect sub-interface route pps 400
cpu-protect sub-interface protocol pps 400
username web admin password encrypted MjEyMzJmMjk3YTU3YTVhNzQzODk0YTBINGE4MDFmYzM=
web-login-time 14400
web-language en
web http port 80
!
!
!
username "admin" privilege user secret encrypted MjEyMzJmMjk3YTU3YTVhNzQzODk0YTBINGE4MDFmYzM=
vlan 44,111,222,333,1111,4094
management-vlan enable
voice-vlan vlan 111
voice-vlan
voice-vlan cos 6 remark
voice-vlan aging-time 1000
voice-vlan oui-table 00:E0:BB:00:00:00 mask FF:FF:FF:00:00:00 "3COM"
voice-vlan oui-table 00:03:6B:00:00:00 mask FF:FF:FF:00:00:00 "Cisco"
```

Figure 7-20: View the current configuration.

Apply the current configuration.

Click on the "System Management" "Configuration Management" "Configuration Management", click "Apply" button, the running - the content of the config files Applyd to the startup --config file:



192.168.2.10 says

Success

Description: View, save or export the current running configuration. Import a previously saved configuration.

● Import Configuration ○ Export Configuration

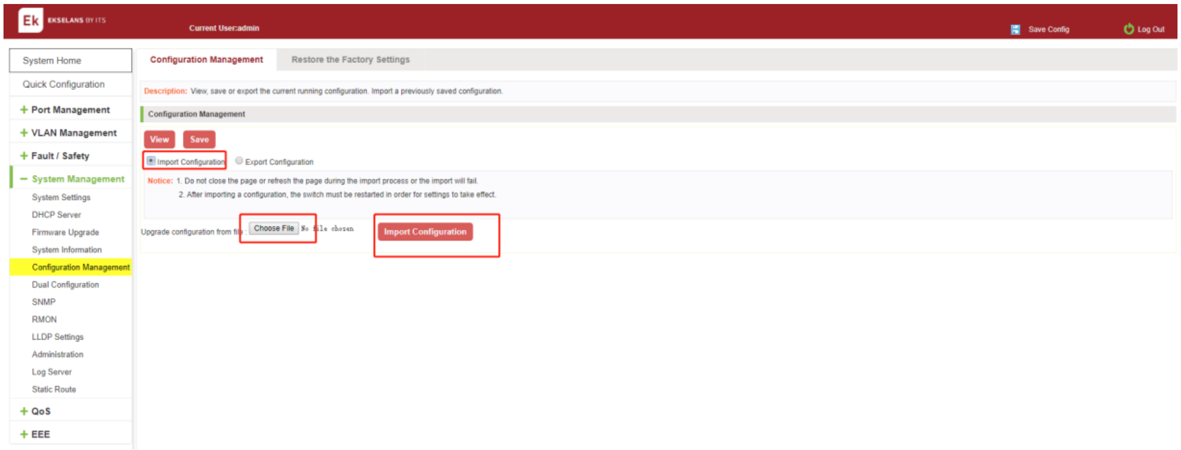
Notice: 1. Do not close the page or refresh the page during the import process or the import will fail.
2. After importing a configuration, the switch must be restarted in order for settings to take effect.

Upgrade configuration from file : No file chosen

Figure 7-21: To Apply the current configuration.

The configuration.

Click on the "System Management" "Configuration Management" "Configuration Management", select "Import Configuration", click "Choose File" button to find Configuration File to Import, click the "Import Configuration" button, complete the Configuration Import:



Description: View, save or export the current running configuration. Import a previously saved configuration.

Configuration Management

● Import Configuration ○ Export Configuration

Notice: 1. Do not close the page or refresh the page during the import process or the import will fail.
2. After importing a configuration, the switch must be restarted in order for settings to take effect.

Upgrade configuration from file : Choose File No file chosen

Figure 7-22: Imported configuration.

Import the configuration steps are as follows:

Step1: Select the "Import Configuration".

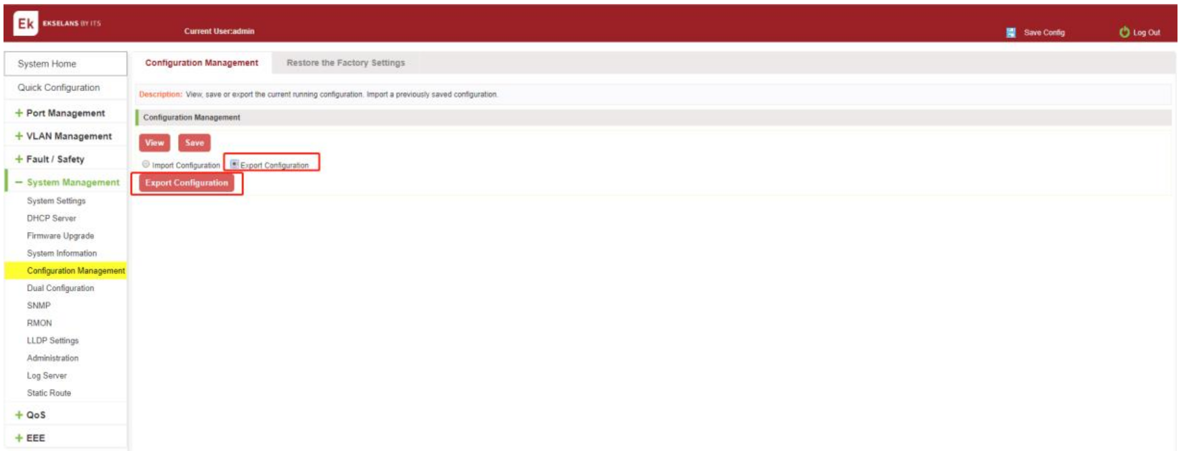
Step2: Click "Choose File" button to find you want to import the configuration File.

Step3: Click on "Import Configuration" button.

Step4: Confirm the restart.

Export configuration.

Click on the "System Management" "Configuration Management" "Configuration Management", select "Export Configuration", Export Configuration.



Description: View, save or export the current running configuration. Import a previously saved configuration.

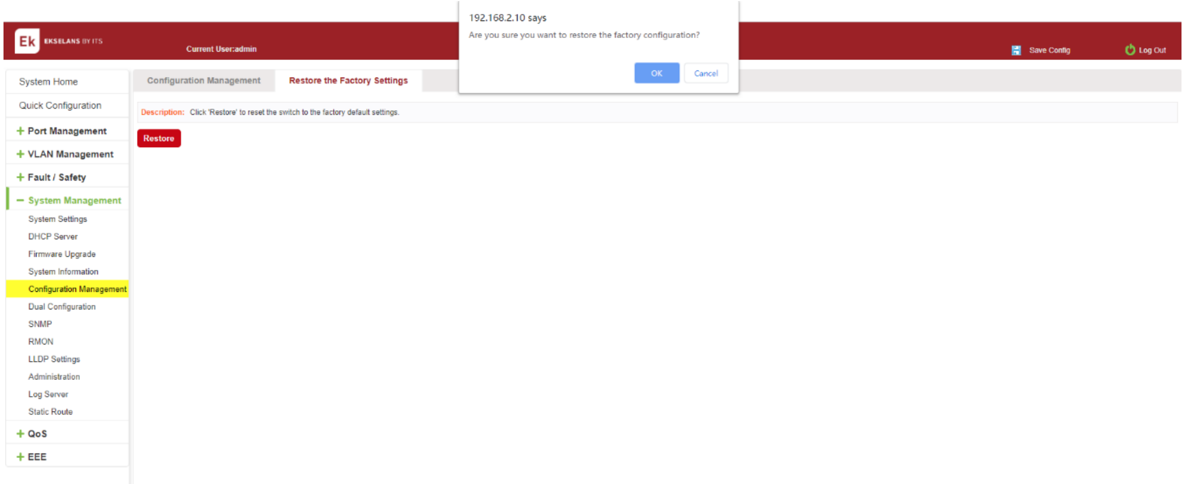
Configuration Management

○ Import Configuration ● Export Configuration

Figure 7-23: Export configuration.

Restore factory Settings.

Click on the "System Management" "Configuration Management" "Restore the Factory Settings" to switch to Restore the Factory Configuration actions:



192.168.2.10 says

Are you sure you want to restore the factory configuration?

Description: Click 'Restore' to reset the switch to the factory default settings.

Figure 7-24: Restore factory Settings.

Factory default operation steps are as follows:

Step1: Click the "Restore the Factory Settings" button.

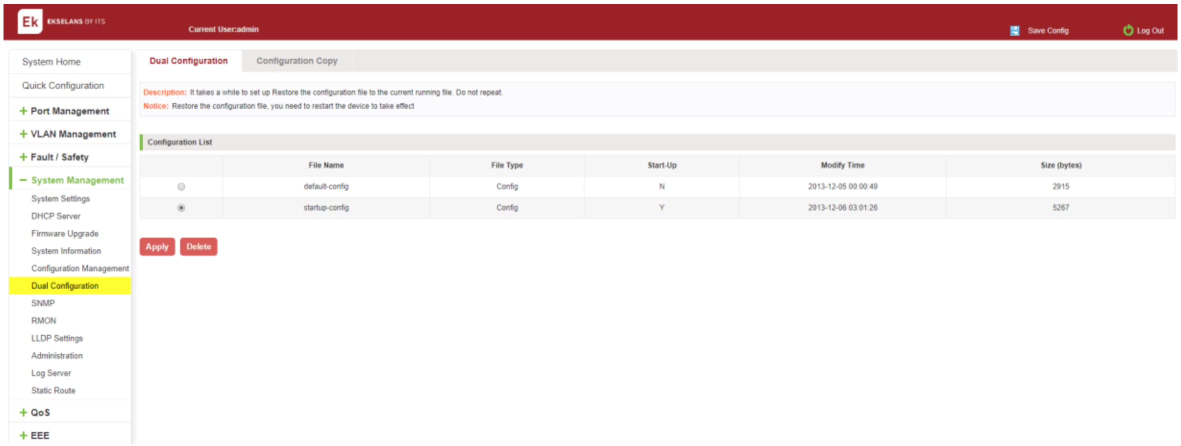
step2: In the pop-up confirmation box, click the "OK" button.

step3: After the completion of the reset switch, wait for equipment to restart, switch back to factory default configuration.

Dual Configuration.

BACK UP AND RESTORE THE CURRENT CONFIGURATION FILE.

1. Click on "System Management" "Dual Configuration".

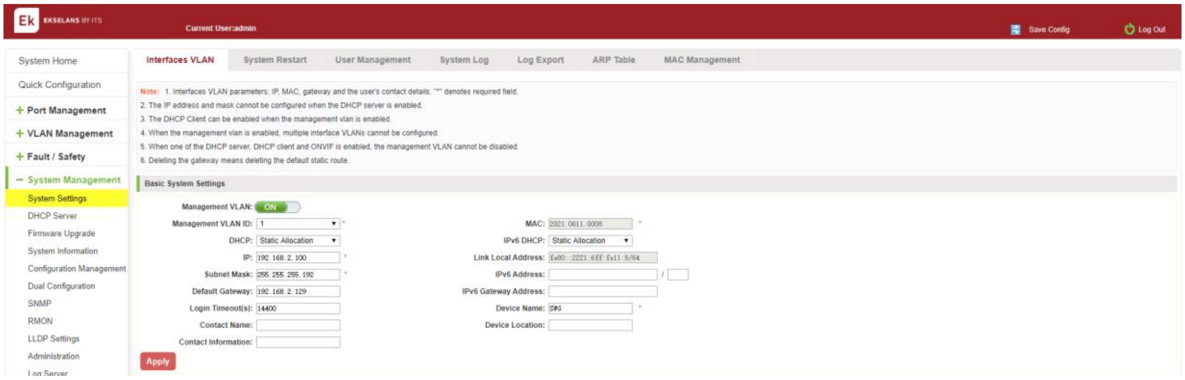


Description: It takes a while to set up Restore the configuration file to the current running file. Do not repeat.
Notice: Restore the configuration file, you need to restart the device to take effect

Configuration List

	File Name	File Type	Start-Up	Modify Time	Size (bytes)
○	default-config	Config	N	2013-12-05 00:00:49	2915
●	startup-config	Config	Y	2013-12-06 03:01:26	5267

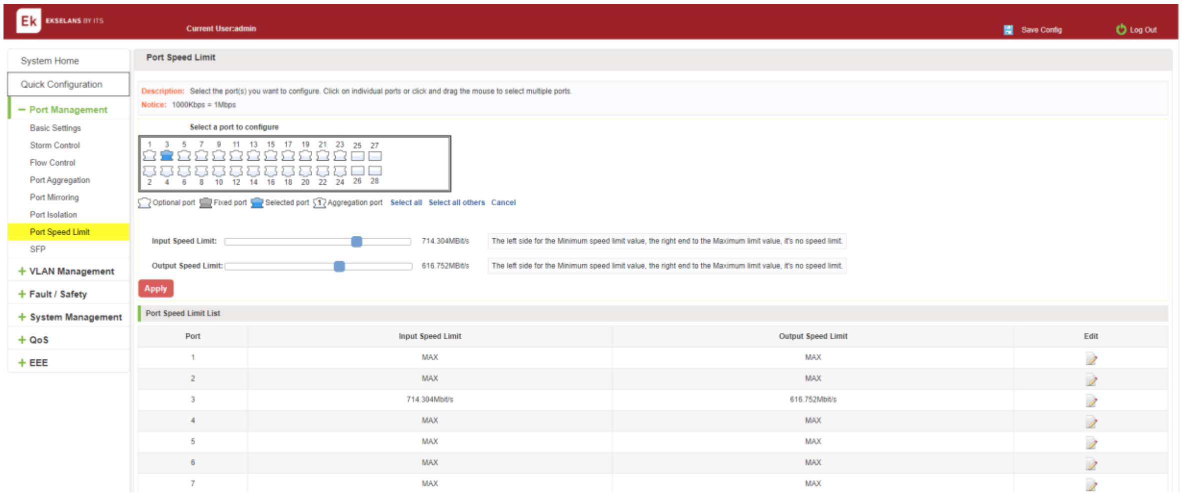
2. Configure some functions, such as: IP address, port speed limit, port mirroring and other functions.



Note: 1. Interfaces VLAN parameters: IP, MAC, gateway and the user's contact details. "*" denotes required field.
2. The IP address and mask cannot be configured when the DHCP server is enabled.
3. The DHCP Client can be enabled when the management vlan is enabled.
4. When the management vlan is enabled, multiple interface VLANs cannot be configured.
5. When one of the DHCP server, DHCP client and ONVIF is enabled, the management VLAN cannot be disabled.
6. Deleting the gateway means deleting the default static route.

Basic System Settings

Management VLAN: ON
Management VLAN ID: 1 *
DHCP: Static Allocation
IP: 192.168.2.100 *
Subnet Mask: 255.255.255.192 *
Default Gateway: 192.168.2.129
Login Timeout(s): 14400
Contact Name:
Contact Information:
MAC: 2021.0611.0008 *
IPv6 DHCP: Static Allocation
Link Local Address: fe80::2221:6ff:fe11:8/64
IPv6 Address: /
IPv6 Gateway Address:
Device Name: SWG *
Device Location:



Port Speed Limit

Description: Select the port(s) you want to configure. Click on individual ports or click and drag the mouse to select multiple ports.

Notice: 1000Kbps = 1Mbps

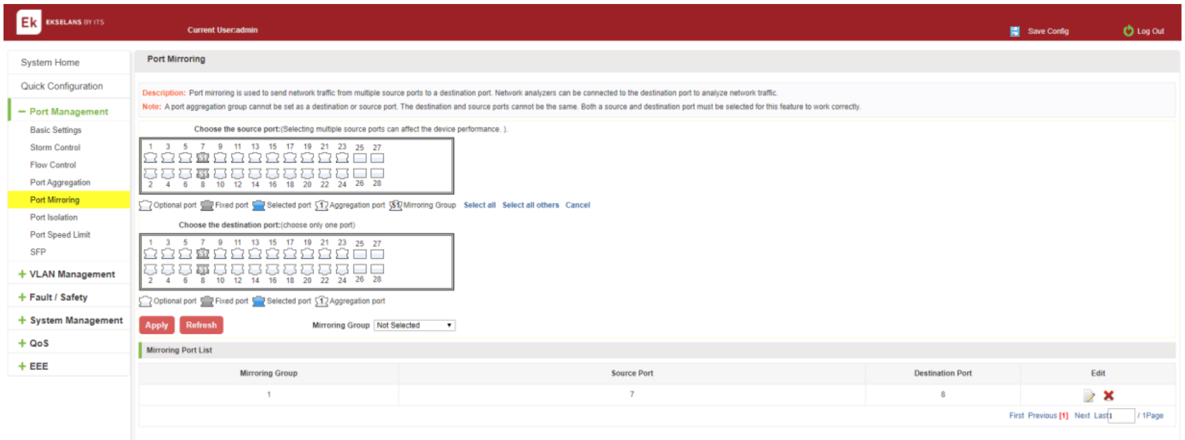
Select a port to configure

Input Speed Limit: 714.304MBit/s The left side for the Minimum speed limit value, the right end to the Maximum limit value, it's no speed limit.

Output Speed Limit: 616.752MBit/s The left side for the Minimum speed limit value, the right end to the Maximum limit value, it's no speed limit.

Port Speed Limit List

Port	Input Speed Limit	Output Speed Limit	Edit
1	MAX	MAX	
2	MAX	MAX	
3	714.304Mbit/s	616.752Mbit/s	
4	MAX	MAX	
5	MAX	MAX	
6	MAX	MAX	
7	MAX	MAX	



Port Mirroring

Description: Port mirroring is used to send network traffic from multiple source ports to a destination port. Network analyzers can be connected to the destination port to analyze network traffic.

Note: A port aggregation group cannot be set as a destination or source port. The destination and source ports cannot be the same. Both a source and destination port must be selected for this feature to work correctly.

Choose the source port:(Selecting multiple source ports can affect the device performance.).

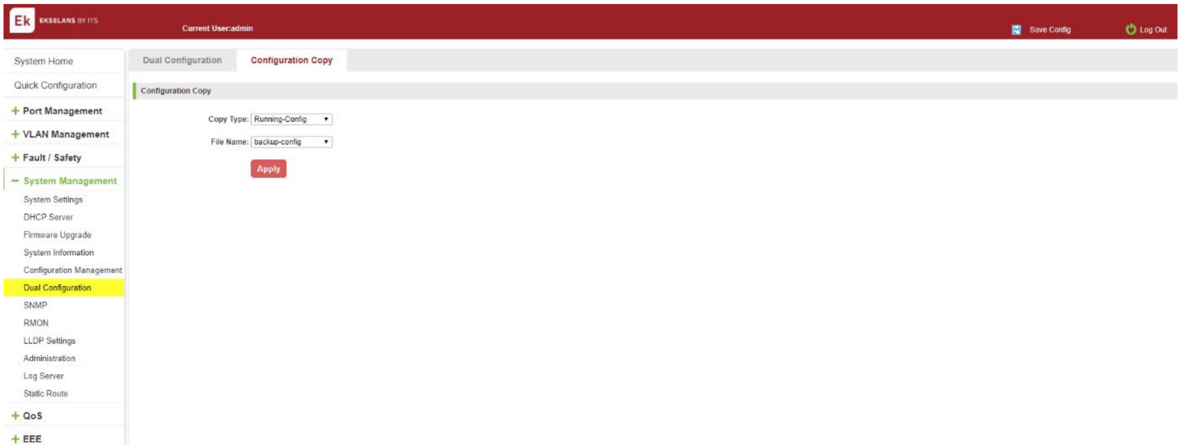
Choose the destination port:(choose only one port)

Mirroring Group: Not Selected

Mirroring Port List

Mirroring Group	Source Port	Destination Port	Edit
1	7	8	

3. Click on the "System Management" "Dual configuration" To configure the switch Back up the current running profile.

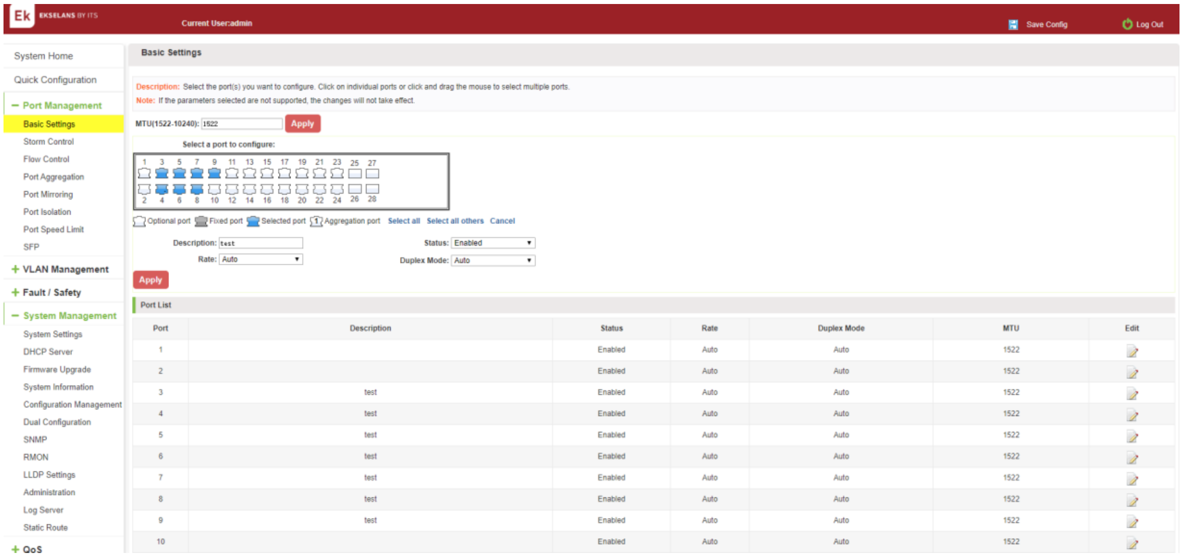


Configuration Copy

Copy Type: Running-Config

File Name: backup-config

4. Based on step 1, add or remove the function configuration. such as: port description.



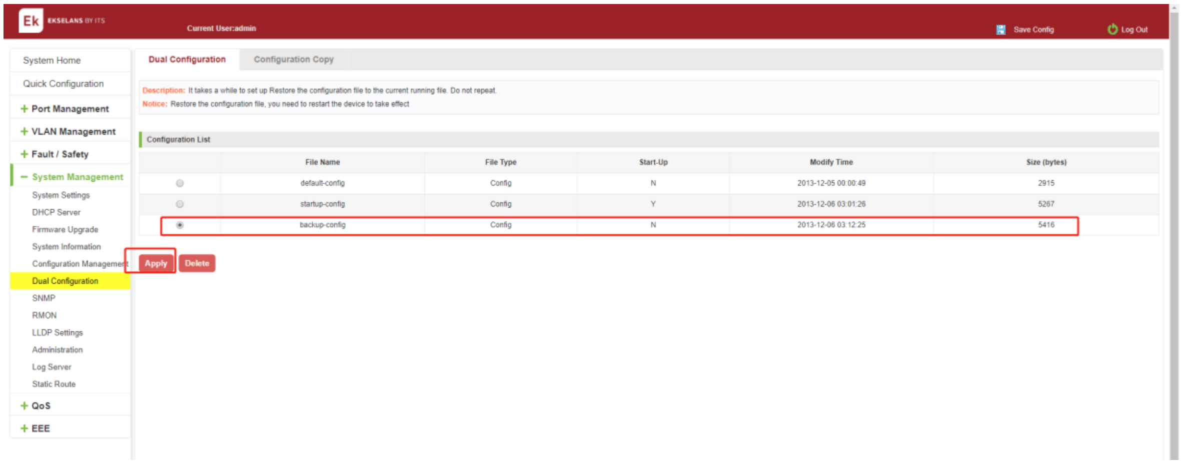
Description: Select the port(s) you want to configure. Click on individual ports or click and drag the mouse to select multiple ports.
Note: If the parameters selected are not supported, the changes will not take effect.

MTU(1522-10240): 1522

Description: test
Status: Enabled
Rate: Auto
Duplex Mode: Auto

Port	Description	Status	Rate	Duplex Mode	MTU	Edit
1		Enabled	Auto	Auto	1522	
2		Enabled	Auto	Auto	1522	
3	test	Enabled	Auto	Auto	1522	
4	test	Enabled	Auto	Auto	1522	
5	test	Enabled	Auto	Auto	1522	
6	test	Enabled	Auto	Auto	1522	
7	test	Enabled	Auto	Auto	1522	
8	test	Enabled	Auto	Auto	1522	
9	test	Enabled	Auto	Auto	1522	
10		Enabled	Auto	Auto	1522	

5. Click on the "Dual configuration" and restore the configuration file to the current running file.



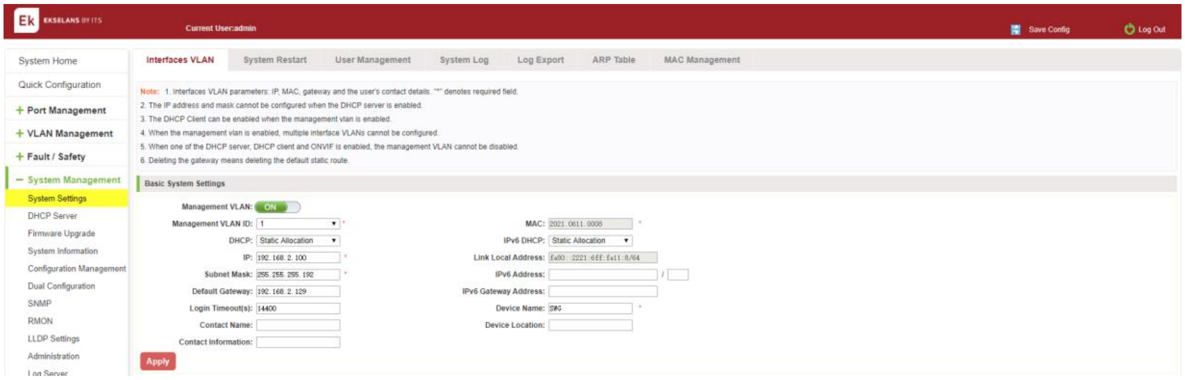
Description: It takes a while to set up Restore the configuration file to the current running file. Do not repeat.
Notice: Restore the configuration file, you need to restart the device to take effect

	File Name	File Type	Start-Up	Modify Time	Size (bytes)
○	default-config	Config	N	2013-12-05 00:00:49	2915
○	startup-config	Config	Y	2013-12-06 03:01:26	5267
●	backup-config	Config	N	2013-12-06 03:12:25	5416

The switch should restore the configuration to the current running file for the previous backup (Restore to the configuration of step 4).

BACK UP AND RESTORE THE STARTUP CONFIGURATION FILE.

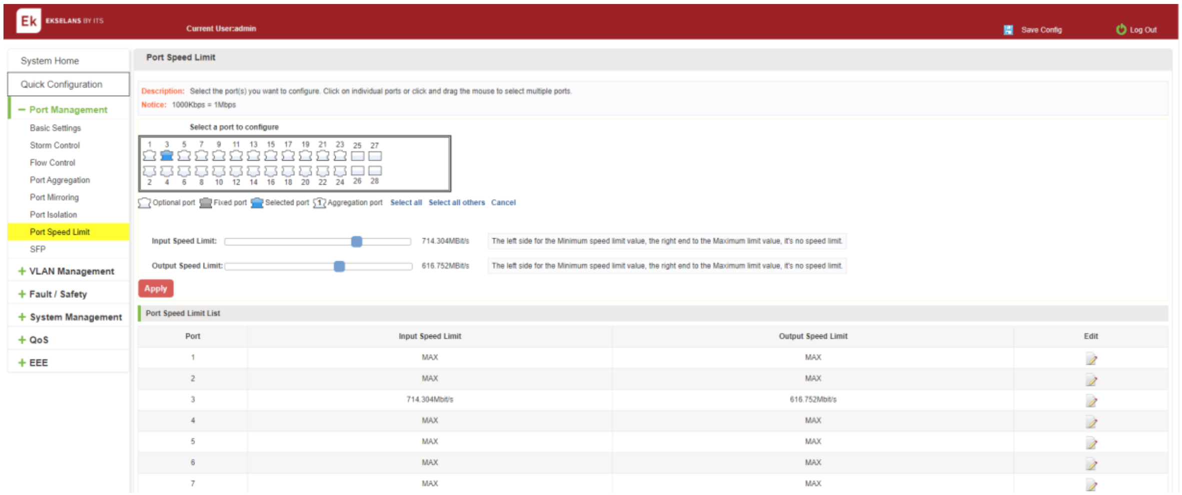
1. Configure some functions, such as: IP address, port speed limit, port mirroring and other functions.



Note: 1. Interfaces VLAN parameters: IP, MAC, gateway and the user's contact details. "*" denotes required field.
2. The IP address and mask cannot be configured when the DHCP server is enabled.
3. The DHCP Client can be enabled when the management vlan is enabled.
4. When the management vlan is enabled, multiple interface VLANs cannot be configured.
5. When one of the DHCP server, DHCP client and ONVIF is enabled, the management VLAN cannot be disabled.
6. Deleting the gateway means deleting the default static route.

Basic System Settings

Management VLAN: ON
Management VLAN ID: 1 *
DHCP: Static Allocation
IP: 192.168.2.100 *
Subnet Mask: 255.255.255.192 *
Default Gateway: 192.168.2.129
Login Timeout(s): 14400
Contact Name:
Contact Information:
MAC: 2021.0611.0008 *
IPv6 DHCP: Static Allocation
Link Local Address: fe80::2221:6ff:fe11:8/64
IPv6 Address: /
IPv6 Gateway Address:
Device Name: SWG *
Device Location:



Port Speed Limit

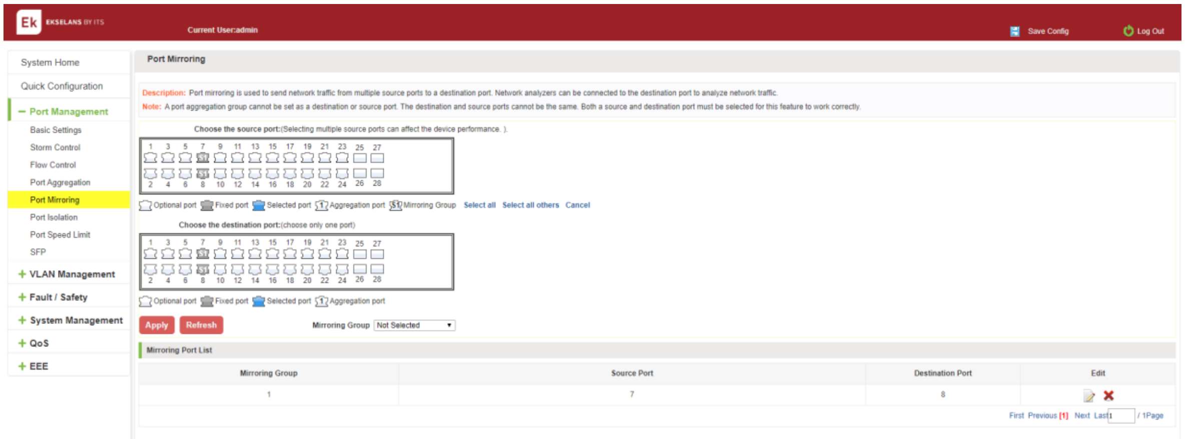
Description: Select the port(s) you want to configure. Click on individual ports or click and drag the mouse to select multiple ports.
Notice: 1000Kbps = 1Mbps

Select a port to configure

Input Speed Limit: 714.304MBit/s The left side for the Minimum speed limit value, the right end to the Maximum limit value, it's no speed limit.
Output Speed Limit: 616.752MBit/s The left side for the Minimum speed limit value, the right end to the Maximum limit value, it's no speed limit.

Port Speed Limit List

Port	Input Speed Limit	Output Speed Limit	Edit
1	MAX	MAX	✎
2	MAX	MAX	✎
3	714.304Mbit/s	616.752Mbit/s	✎
4	MAX	MAX	✎
5	MAX	MAX	✎
6	MAX	MAX	✎
7	MAX	MAX	✎



Port Mirroring

Description: Port mirroring is used to send network traffic from multiple source ports to a destination port. Network analyzers can be connected to the destination port to analyze network traffic.
Note: A port aggregation group cannot be set as a destination or source port. The destination and source ports cannot be the same. Both a source and destination port must be selected for this feature to work correctly.

Choose the source port:(Selecting multiple source ports can affect the device performance.).

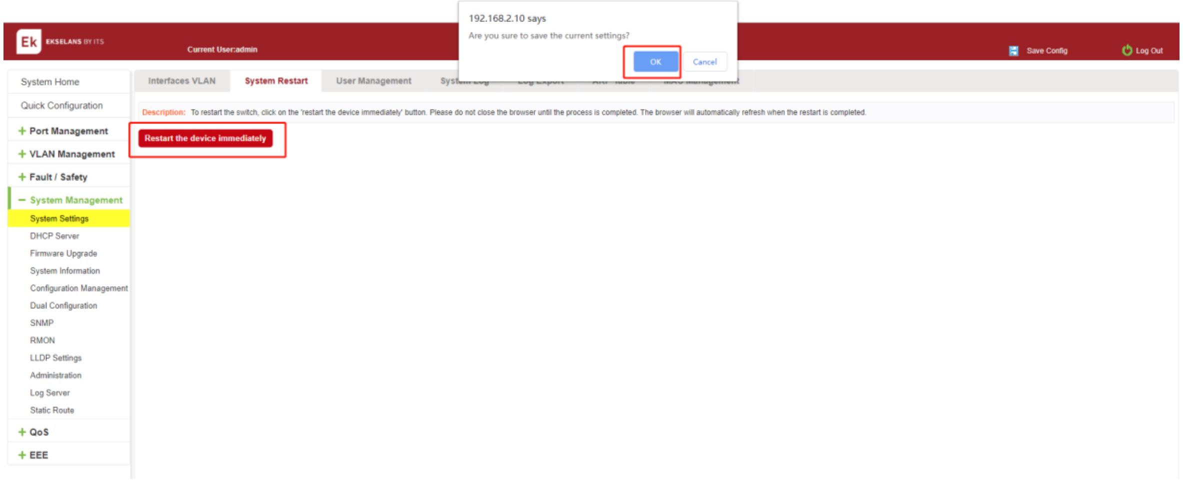
Choose the destination port:(choose only one port)

Mirroring Group: Not Selected

Mirroring Port List

Mirroring Group	Source Port	Destination Port	Edit
1	7	8	✎ ✖

2. Apply the current configuration (You can use GUI settings, or you can use CLI commands).

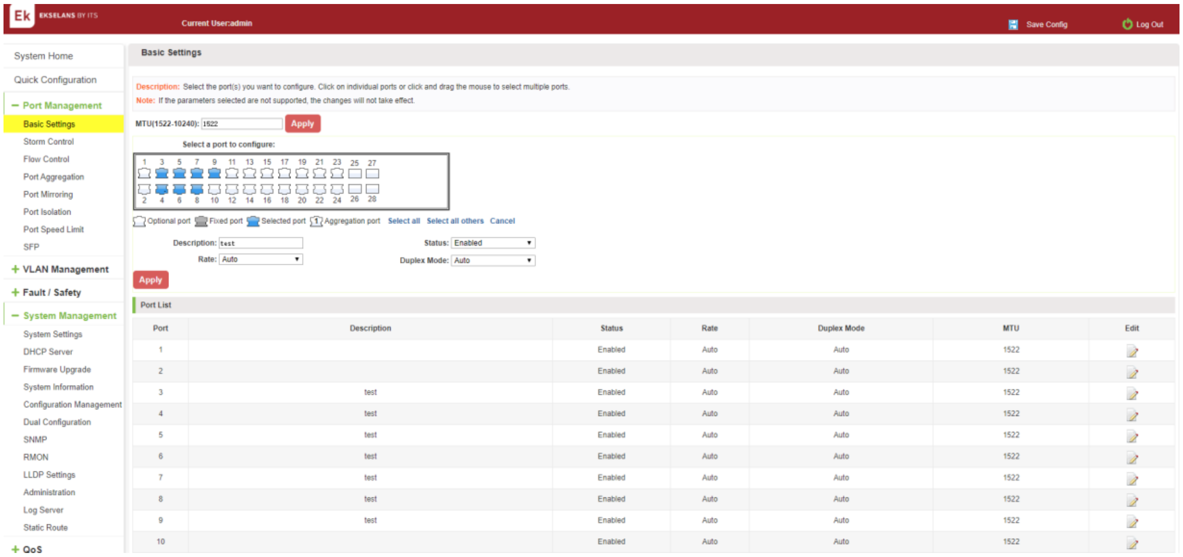


192.168.2.10 says

Are you sure to save the current settings?

Description: To restart the switch, click on the 'restart the device immediately' button. Please do not close the browser until the process is completed. The browser will automatically refresh when the restart is completed.

3. On the basis of step 1, add or remove the function configuration. Such as: port description.



Basic Settings

Description: Select the port(s) you want to configure. Click on individual ports or click and drag the mouse to select multiple ports.
Note: If the parameters selected are not supported, the changes will not take effect.

MTU(1522-10240): 1522

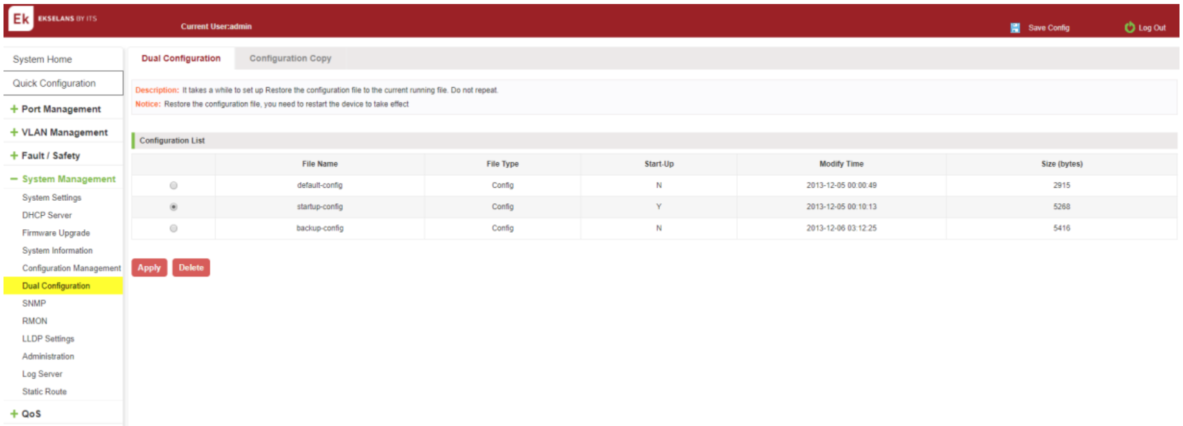
Select a port to configure:

Description: test
Rate: Auto
Status: Enabled
Duplex Mode: Auto

Port List

Port	Description	Status	Rate	Duplex Mode	MTU	Edit
1		Enabled	Auto	Auto	1522	✎
2		Enabled	Auto	Auto	1522	✎
3	test	Enabled	Auto	Auto	1522	✎
4	test	Enabled	Auto	Auto	1522	✎
5	test	Enabled	Auto	Auto	1522	✎
6	test	Enabled	Auto	Auto	1522	✎
7	test	Enabled	Auto	Auto	1522	✎
8	test	Enabled	Auto	Auto	1522	✎
9	test	Enabled	Auto	Auto	1522	✎
10		Enabled	Auto	Auto	1522	✎

4. Click on the "Dual configuration" click the “Restore the configuration file to the start-up file”.



Description: It takes a while to set up Restore the configuration file to the current running file. Do not repeat.
Notice: Restore the configuration file, you need to restart the device to take effect

Configuration List

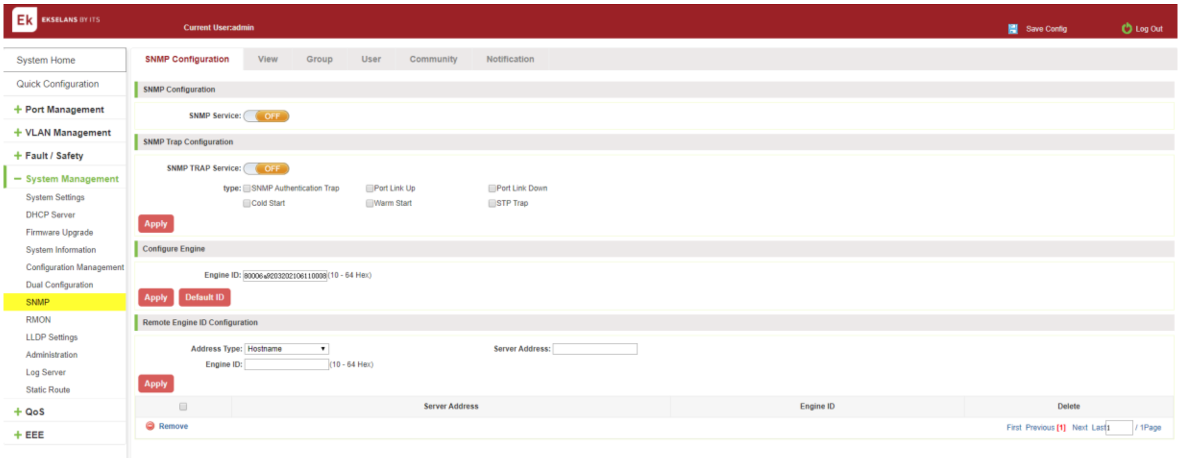
	File Name	File Type	Start-Up	Modify Time	Size (bytes)
○	default-config	Config	N	2013-12-05 00:00:49	2915
●	startup-config	Config	Y	2013-12-05 00:10:13	5268
○	backup-config	Config	N	2013-12-06 03:12:25	5416

5. Reboot the device

SNMP.

Check the SNMP.

Click on the "System Management" "SNMP", you can view the SNMP configured information:



SNMP Configuration

SNMP Service: OFF

SNMP Trap Configuration

SNMP TRAP Service: OFF

type: □ SNMP Authentication Trap □ Port Link Up □ Port Link Down
□ Cold Start □ Warm Start □ STP Trap

Configure Engine

Engine ID: 80006a9203202106110008 (10 - 64 Hex)

Remote Engine ID Configuration

Address Type: Hostname ▾ Server Address:
Engine ID: (10 - 64 Hex)

□	Server Address	Engine ID	Delete

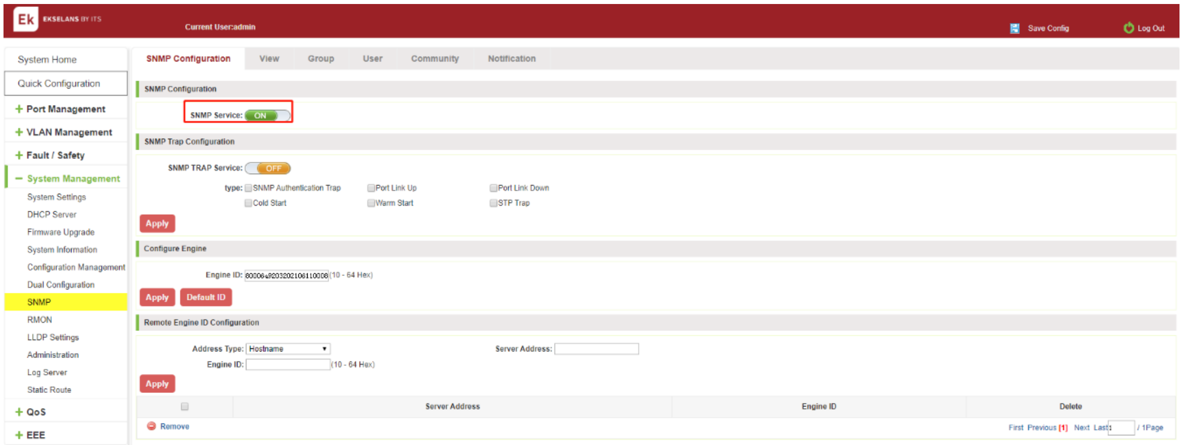
Figure 7-25: View the SNMP configuration information.

By default, SNMP is not open.

SNMP monitoring software and switches the SNMP version is consistent, if inconsistencies can lead to communication failure.

Activate the SNMP.

Click ON the "System Management" "SNMP", choose the SNMP service, click ON the "OFF" to "ON", click ok:



SNMP Configuration

SNMP Service: ON

SNMP Trap Configuration

SNMP TRAP Service: OFF

type: □ SNMP Authentication Trap □ Port Link Up □ Port Link Down
□ Cold Start □ Warm Start □ STP Trap

Configure Engine

Engine ID: 80006492032021081100006 (10 - 64 Hex)

Remote Engine ID Configuration

Address Type: Hostname Server Address:
Engine ID: (10 - 64 Hex)

□	Server Address	Engine ID	Delete

Figure 7-26: Activation SNMP function.

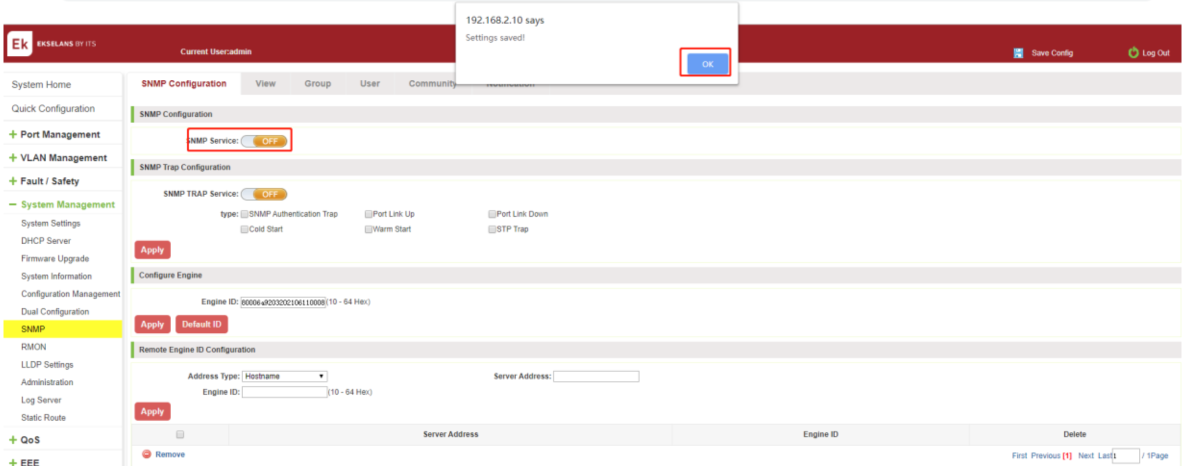
Activation function SNMP configuration steps are as follows:

Step1: Choose open SNMP options.

Step2: Click "OK" button to complete the configuration.

To disable the SNMP.

Click ON the "System Management" "SNMP", choose the SNMP service, click ON the "ON" to "OFF", complete the configuration:



192.168.2.10 says

Settings saved!

Current User:admin

SNMP Configuration

SNMP Service: OFF

SNMP Trap Configuration

SNMP TRAP Service: OFF

type: □SNMP Authentication Trap □Port Link Up □Port Link Down
□Cold Start □Warm Start □STP Trap

Configure Engine

Engine ID: 80006a9203202106110008 (10 - 64 Hex)

Remote Engine ID Configuration

Address Type: Hostname ▾ Server Address:

Engine ID: (10 - 64 Hex)

□	Server Address	Engine ID	Delete

Figure 7-27: Disable the SNMP function.

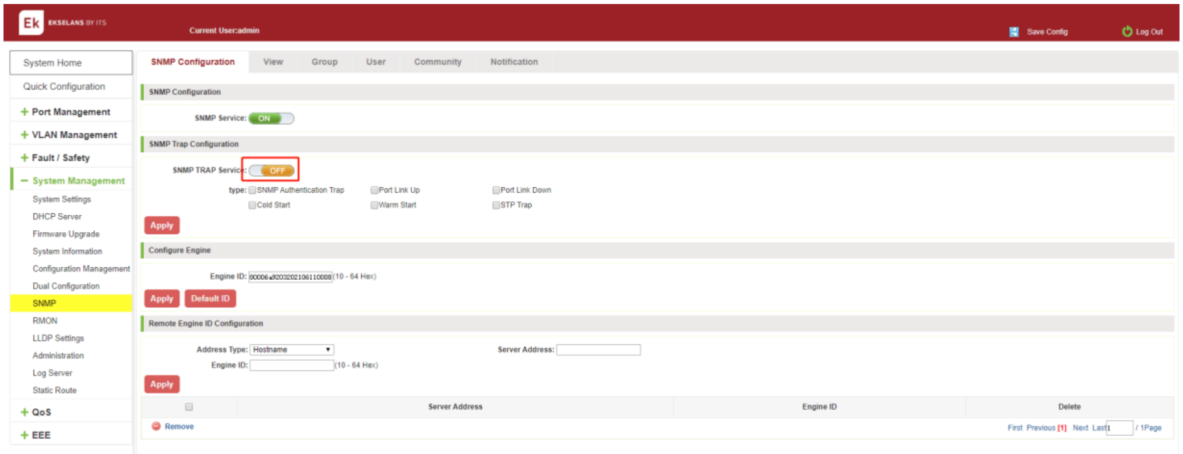
Disable the SNMP function configuration steps are as follows:

Step1: Choose close SNMP options.

Step2: Click "OK" button to complete the configuration.

Activate the TRAP.

After open the SNMP, select the SNMP TRAP service, click ON the "OFF" to "ON", click ok:



Current User:admin

SNMP Configuration

SNMP Service: ON

SNMP Trap Configuration

SNMP TRAP Service: OFF

type: □ SNMP Authentication Trap □ Port Link Up □ Port Link Down

□ Cold Start □ Warm Start □ STP Trap

Configure Engine

Engine ID: 80006a9203202106110008 (10 - 64 Hex)

Remote Engine ID Configuration

Address Type: Hostname

Server Address:

Engine ID: (10 - 64 Hex)

□	Server Address	Engine ID	Delete

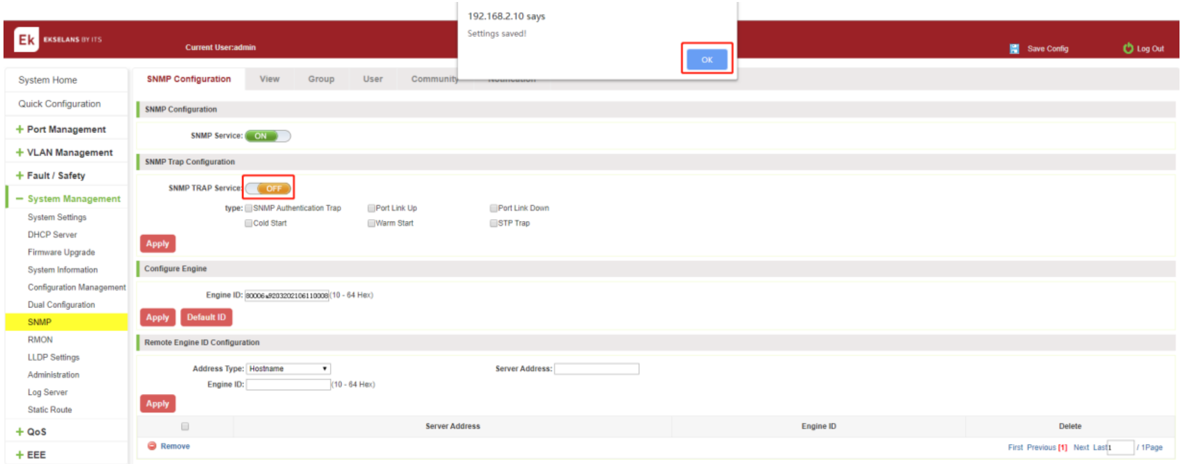
Figure 7-28: Activation function of the TRAP.

Activate the TRAP function configuration steps are as follows:

Step1: Select "ON" option; step2: Click "OK" button to complete the configuration.

Disable the TRAP.

Choose the SNMP TRAP service, click ON the "ON" to "OFF", click "OK", complete the configuration:



192.168.2.10 says
Settings saved!

SNMP Configuration

SNMP Service: ON

SNMP Trap Configuration

SNMP TRAP Service: OFF

type: □ SNMP Authentication Trap □ Port Link Up □ Port Link Down
□ Cold Start □ Warm Start □ STP Trap

Configure Engine

Engine ID: 80006a9203202106110008 (10 - 64 Hex)

Remote Engine ID Configuration

Address Type: Hostname ▾ Server Address:
Engine ID: (10 - 64 Hex)

□	Server Address	Engine ID	Delete

Figure 7-29: Disable TRAP function.

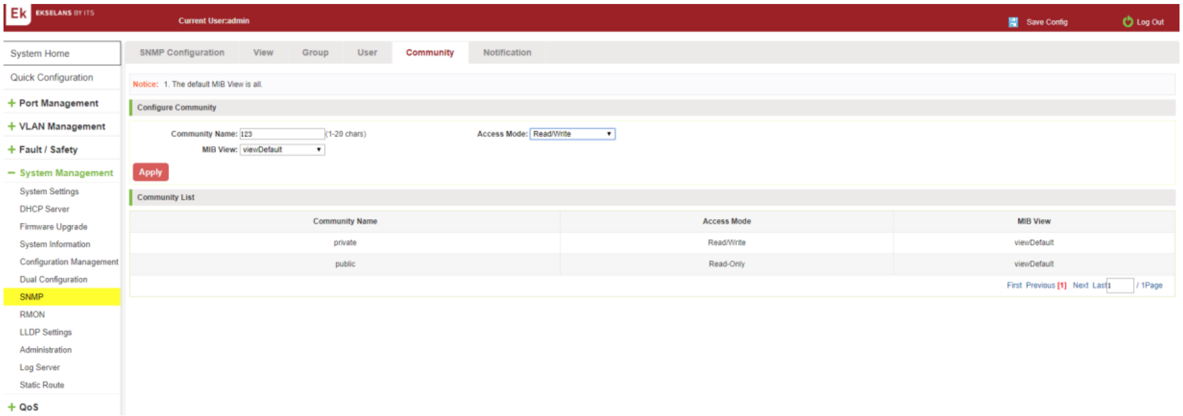
Disable the TRAP function configuration steps are as follows:

Step1: Select "ON" to "OFF" option.

Step2: Click "OK" button to complete the configuration.

CHANGE community.

Click on the "System Management" "SNMP" "Community", in the community name text box input: public, permissions choice: read and write, click the "Apply" button, complete the configuration:



Notice: 1. The default MIB View is all.

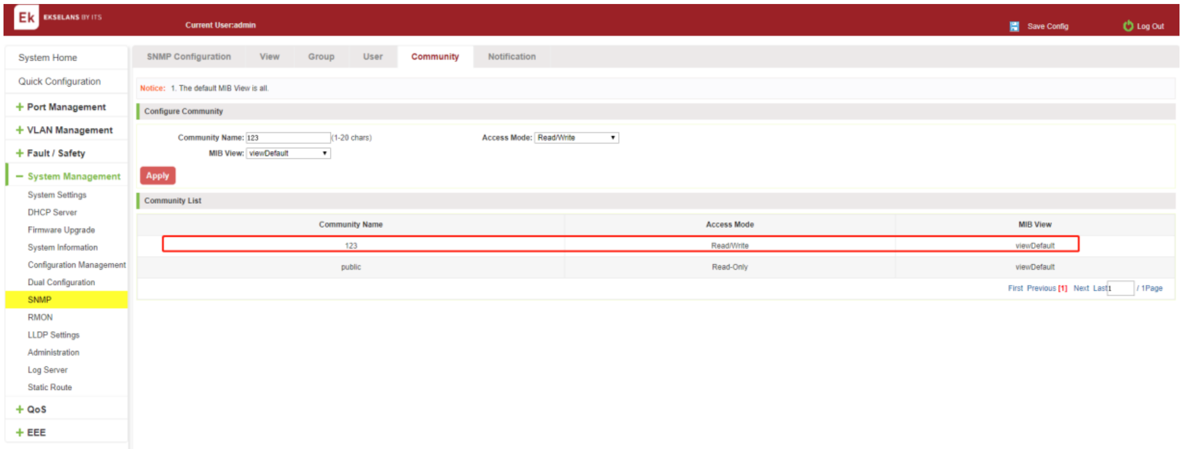
Configure Community

Community Name: 123 (1-20 chars) Access Mode: Read/Write ▾
MIB View: viewDefault ▾

Community List

Community Name	Access Mode	MIB View
private	Read/Write	viewDefault
public	Read-Only	viewDefault

Figure 7-30: Change community.



Notice: 1. The default MIB View is all.

Configure Community

Community Name: 123 (1-20 chars)

Access Mode: Read/Write

MIB View: viewDefault

Community List

Community Name	Access Mode	MIB View
123	Read/Write	viewDefault
public	Read-Only	viewDefault

Figure 7-31: Community results.

Change community configuration steps are as follows:

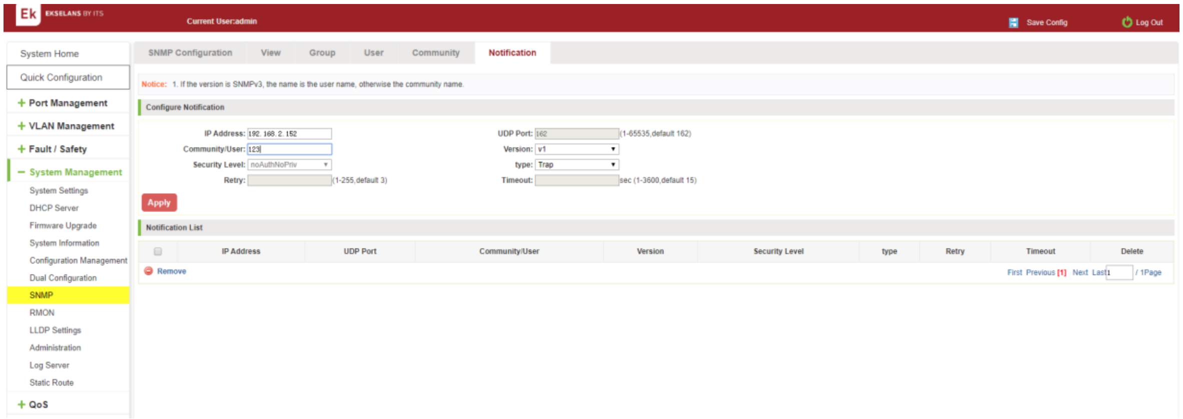
Step1: In the community's name dialog box input: the 123.

Step2: Select "Read/Write" permissions.

Step3: Click on "Apply" button, complete the configuration.

Added the SNMP TRAP service host.

Click on the "System Management" "SNMP" "Notification", in the host IP text box input: 192.168.2.150, TRAP community name: 123, SNMP version choice: 2C, click the "Apply" button, complete the configuration:



Current User:admin

Notice: 1. If the version is SNMPv3, the name is the user name, otherwise the community name.

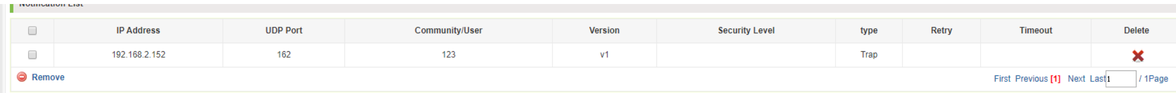
Configure Notification

IP Address: 192. 168. 2. 152
Community/User: 123
Security Level: noAuthNoPriv
Retry: (1-255,default 3)
UDP Port: 162 (1-65535,default 162)
Version: v1
type: Trap
Timeout: sec (1-3600,default 15)

Notification List

□	IP Address	UDP Port	Community/User	Version	Security Level	type	Retry	Timeout	Delete

Figure 7-32: Increases the SNMP TRAP service host.



□	IP Address	UDP Port	Community/User	Version	Security Level	type	Retry	Timeout	Delete
□	192.168.2.152	162	123	v1		Trap			✗

Figure 7-33: SNMP TRAP service host.

Increase the SNMP TRAP service host configuration steps are as follows:

Step1: In the host IP dialog box input: 192.168.2.150.

Step2: In TRAP community name dialog input: 123.

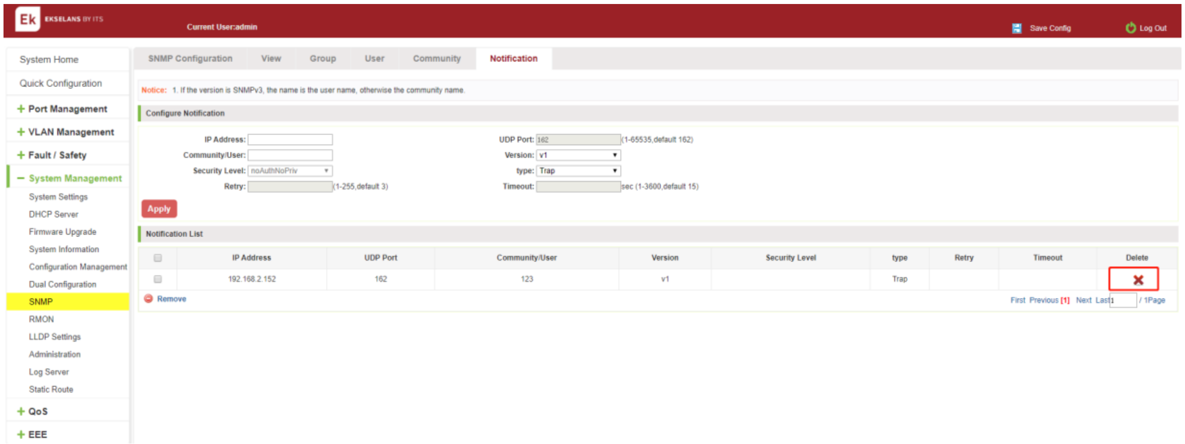
Step3: Select the SNMP version: v1.

Step4: Click on "Apply" button, complete the configuration.

When an SNMP closed, hide the SNMP TRAP service host list.

Delete the SNMP TRAP service host.

Click on the "System Management" "SNMP", in the SNMP TRAP service host list need to delete the object, click ✖ "finish" configuration:



Notice: 1. If the version is SNMPv3, the name is the user name, otherwise the community name.

Configure Notification

IP Address: (blank) UDP Port: 162 (1-65535,default 162)
Community/User: (blank) Version: v1
Security Level: noAuthNoPriv type: Trap
Retry: (1-255,default 3) Timeout: sec (1-3600,default 15)

Notification List

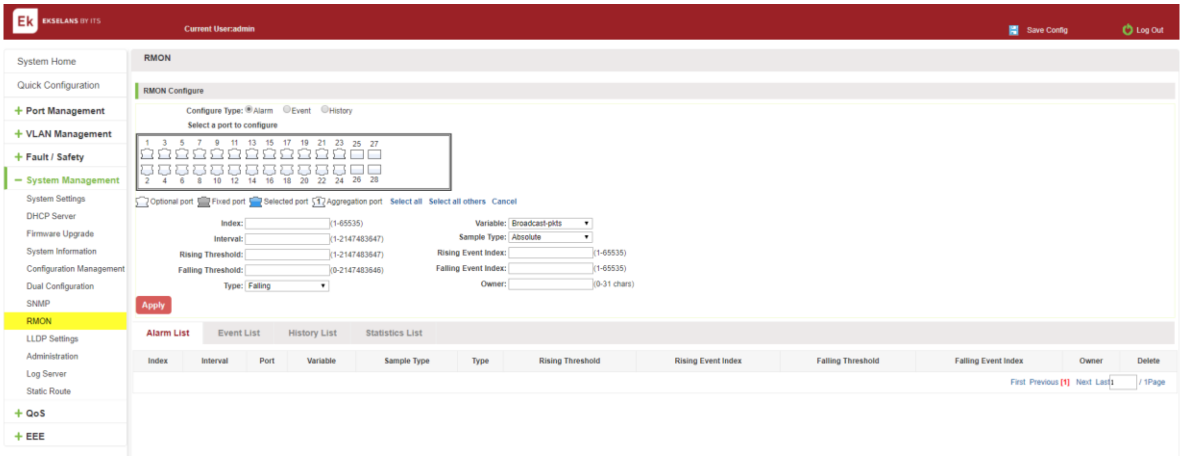
□	IP Address	UDP Port	Community/User	Version	Security Level	type	Retry	Timeout	Delete
□	192.168.2.152	162	123	v1		Trap			✖

Figure 7-34: Delete community.

RMON.

View ROMN configure information.

Click on the "System Management" "RMON", can view RMON configure information.



RMON Configure

Configure Type: ● Alarm ○ Event ○ History

Select a port to configure

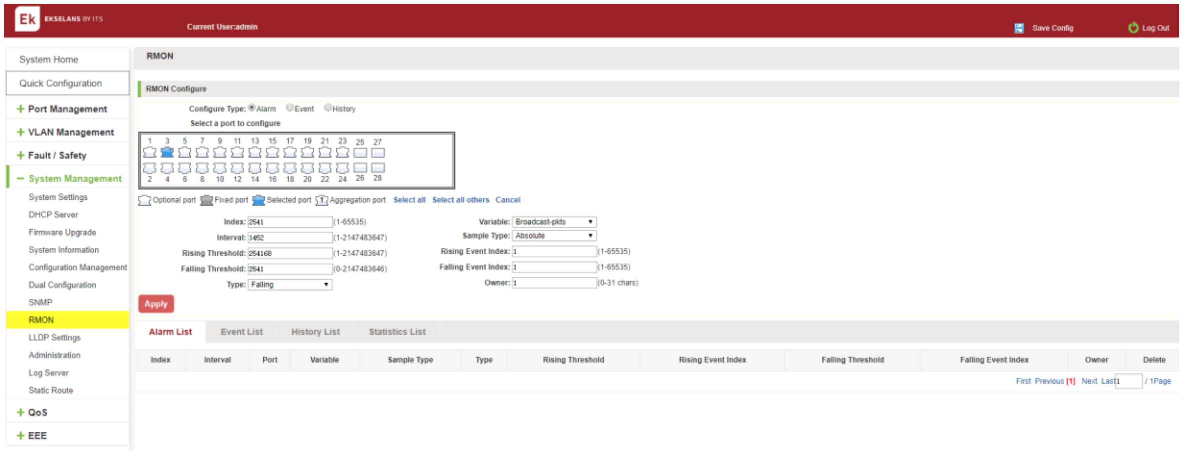
Index: (1-65535) Variable: Broadcast-pkts
Interval: (1-2147483647) Sample Type: Absolute
Rising Threshold: (1-2147483647) Rising Event Index: (1-65535)
Falling Threshold: (0-2147483646) Falling Event Index: (1-65535)
Type: Falling Owner: (0-31 chars)

Index	Interval	Port	Variable	Sample Type	Type	Rising Threshold	Rising Event Index	Falling Threshold	Falling Event Index	Owner	Delete

Figure 7-35: View RMON configure information.

Configure ROMN type.

Configure ROMN type： Alarm, selected one port to configure and setting parameters and click “Apply” button.



Configure Type: ● Alarm ○ Event ○ History

Index: 2541 (1-65535)

Interval: 1452 (1-2147483647)

Rising Threshold: 254168 (1-2147483647)

Falling Threshold: 2541 (0-2147483646)

Type: Falling

Variable: Broadcast-pkts

Sample Type: Absolute

Rising Event Index: 1 (1-65535)

Falling Event Index: 1 (1-65535)

Owner: 1 (0-31 chars)

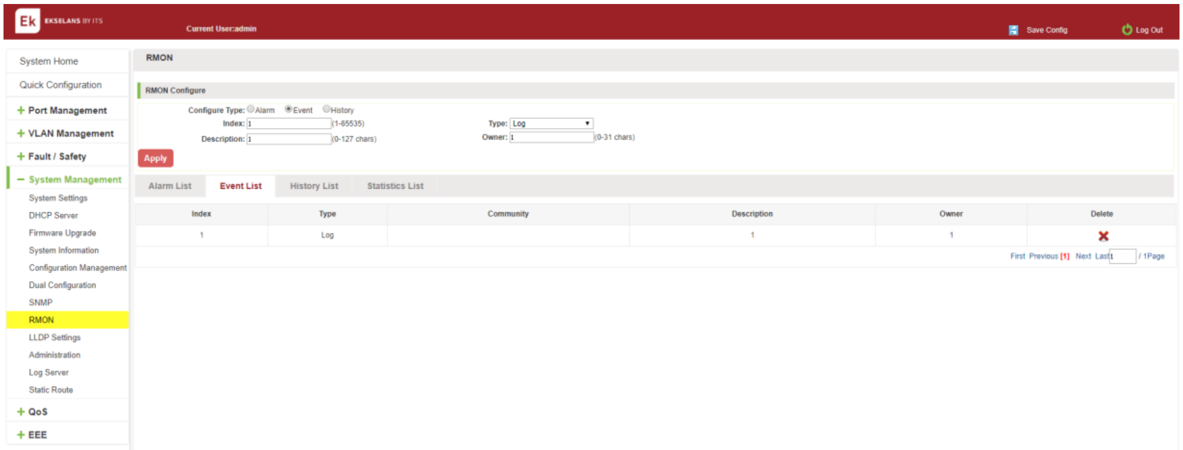
Index	Interval	Port	Variable	Sample Type	Type	Rising Threshold	Rising Event Index	Falling Threshold	Falling Event Index	Owner	Delete

Figure 7-36: configure ROMN type.

Notice: Parameters There are some special rules in the configuration. The EVENT should be created first. Please note the prompts in the configuration. ex: Rising Threshold is greater than Falling Threshold.

Change ROMN type.

On the ROMN configure page, click the type "Event" or "History" and setting parameters. Be careful the parameter of Community should be exit in SNMP Community name. Configure ok after clicking "Apply".



Configure Type: ○ Alarm ● Event ○ History

Index: 1 (1-65535)

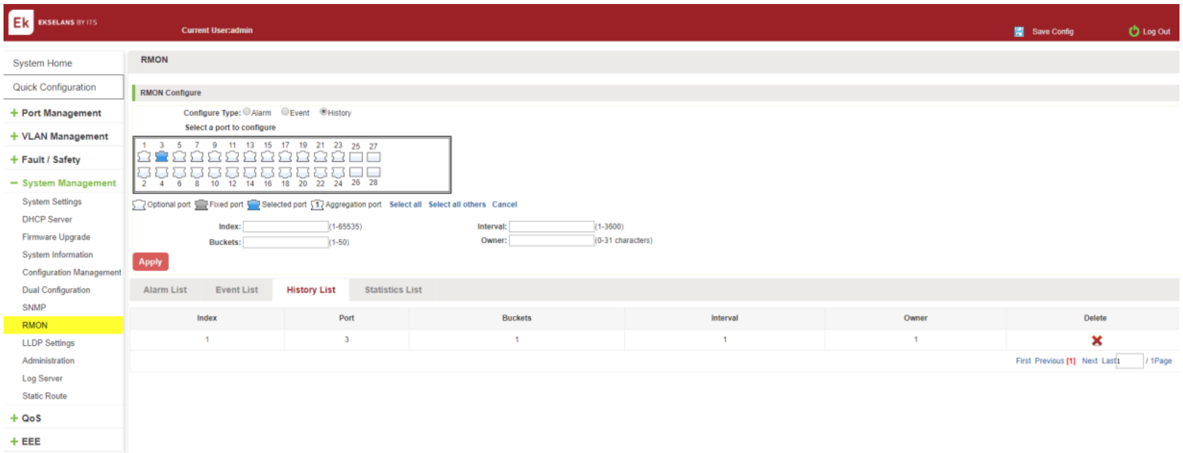
Description: 1 (0-127 chars)

Type: Log

Owner: 1 (0-31 chars)

Index	Type	Community	Description	Owner	Delete
1	Log		1	1	✖

Figure 7-37 Change ROMN type is Event.



Configure Type: ○ Alarm ○ Event ● History

Index: (1-65535)

Buckets: (1-50)

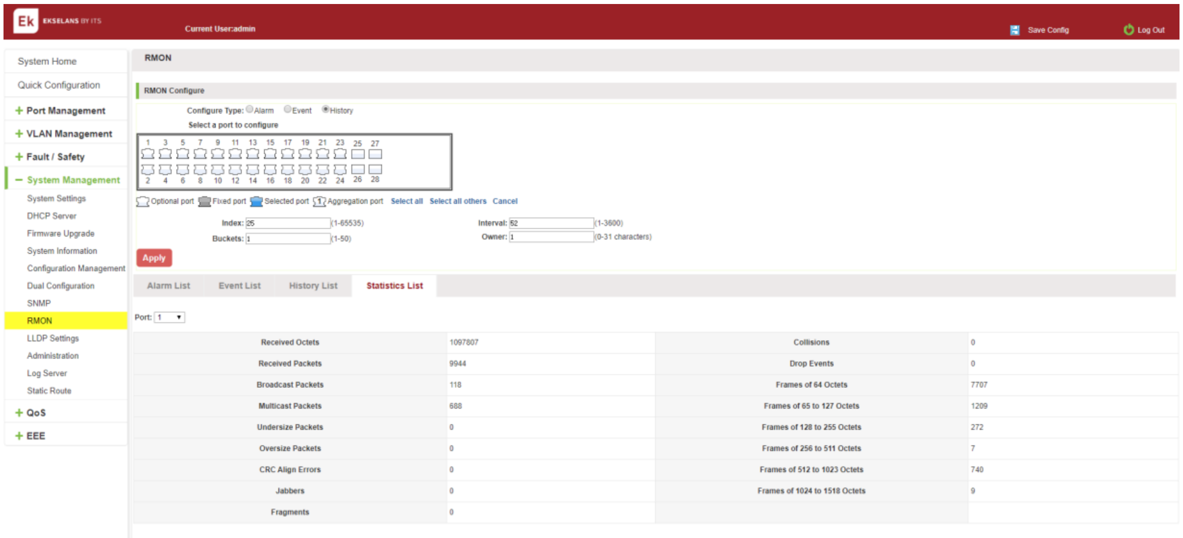
Interval: (1-3600)

Owner: (0-31 characters)

Index	Port	Buckets	Interval	Owner	Delete
1	3	1	1	1	✖

Figure 7-38: Change ROMN type is History.

When the parameters configure is ok, click the Statistics List .We can choose the port to view the information.



Configure Type: ○ Alarm ○ Event ● History

Select a port to configure

Index: 25 (1-65535)　Interval: 52 (1-3600)

Buckets: 1 (1-50)　Owner: 1 (0-31 characters)

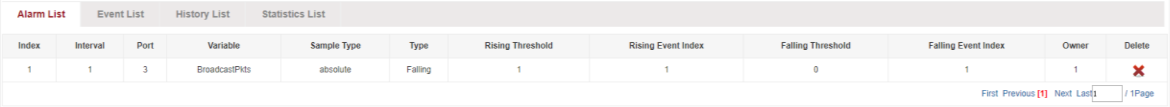
Port: 1

Received Octets	1097807	Collisions	0
Received Packets	9944	Drop Events	0
Broadcast Packets	118	Frames of 64 Octets	7707
Multicast Packets	688	Frames of 65 to 127 Octets	1209
Undersize Packets	0	Frames of 128 to 255 Octets	272
Oversize Packets	0	Frames of 256 to 511 Octets	7
CRC Align Errors	0	Frames of 512 to 1023 Octets	740
Jabbers	0	Frames of 1024 to 1518 Octets	9
Fragments	0		

Figure 7-39: View the port configure information.

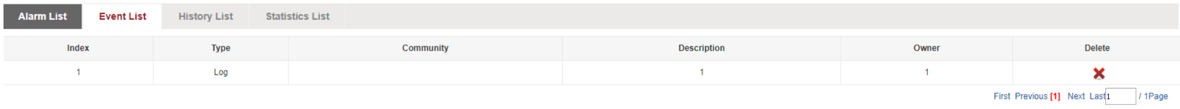
Delete the configured rule.

Select the entry you want to delete and click Fork to delete the unwanted configuration



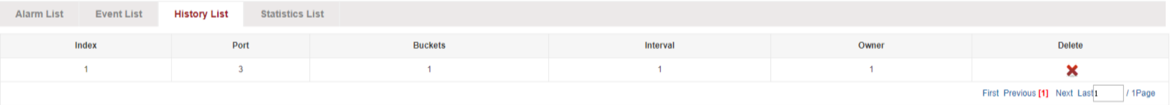
Index	Interval	Port	Variable	Sample Type	Type	Rising Threshold	Rising Event Index	Falling Threshold	Falling Event Index	Owner	Delete
1	1	3	BroadcastPkts	absolute	Falling	1	1	0	1	1	✖

Figure 7-40: Delete the Alarm list rule.



Index	Type	Community	Description	Owner	Delete
1	Log		1	1	✖

Figure 7-41: Delete the Event list rule.



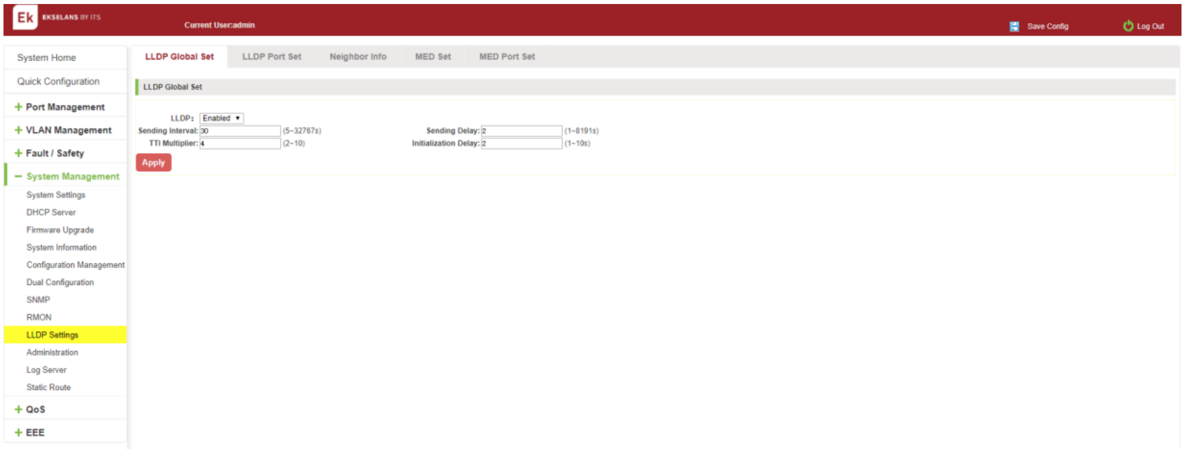
Index	Port	Buckets	Interval	Owner	Delete
1	3	1	1	1	✖

Figure 7-42: Delete the History list rule.

LLDP Settings.

LLDP settings.

Click on the "System Management" "LLDP Settings", "LLDP Settings" can view the lldp settings information. The default mode is Global settings, and this feature is turned off by default.



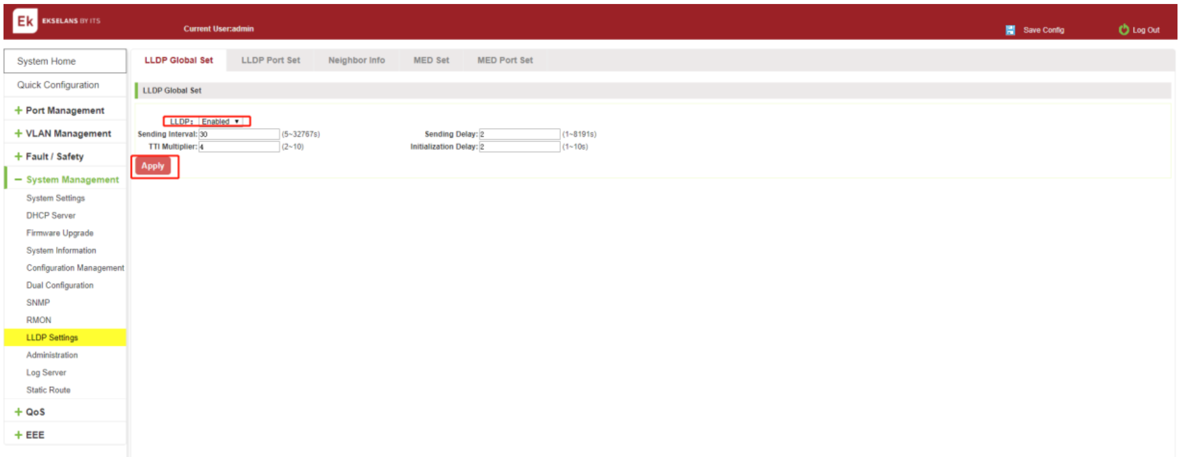
LLDP Global Set

LLDP: Enabled ▾
Sending Interval: 30 (5~32767s)
TTI Multiplier: 4 (2~10)
Sending Delay: 2 (1~8191s)
Initialization Delay: 2 (1~10s)

Figure 7-43: view LLDP settings information.

ENABLE LLDP SETTINGS.

Click the drop-down menu to select enable and configuration parameters. Finally click "Apply" button.



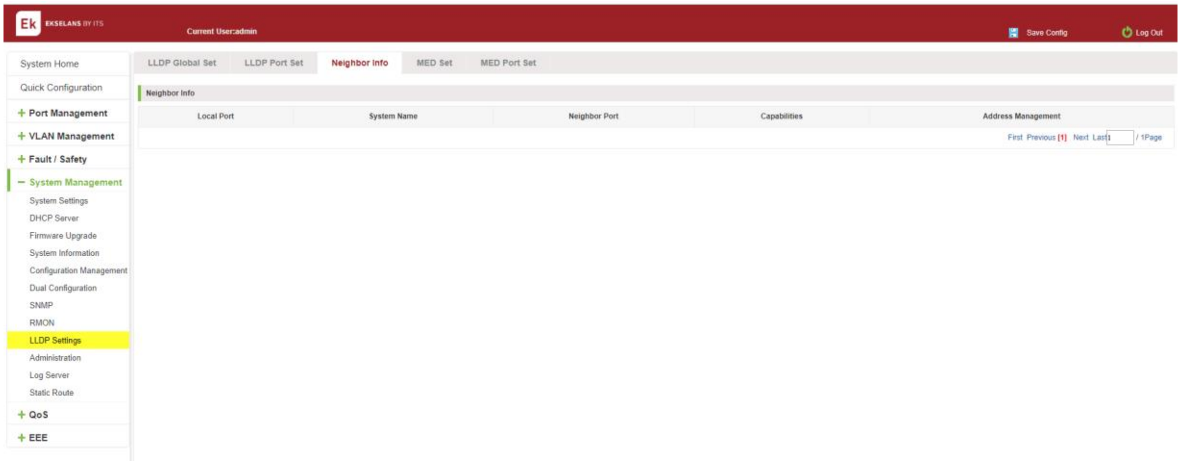
LLDP Global Set

LLDP: Enabled ▾
Sending Interval: 30 (5~32767s)
TTI Multiplier: 4 (2~10)
Sending Delay: 2 (1~8191s)
Initialization Delay: 2 (1~10s)

Figure 7-44: Enable LLDP settings.

NEIGHBOR INFO.

When the LLDP function is enabled, the neighbour information is recorded when a neighbour device is found.



Neighbor Info

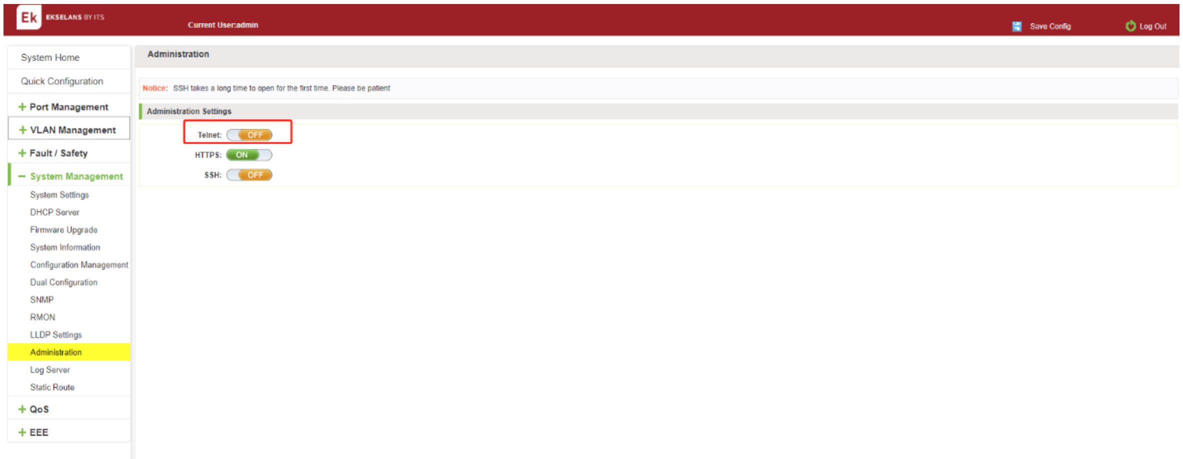
Local Port	System Name	Neighbor Port	Capabilities	Address Management

First Previous [1] Next Last 1 / 1Page

Figure 7-45: Neighbour Info.

Administration.

TELNET.



Administration

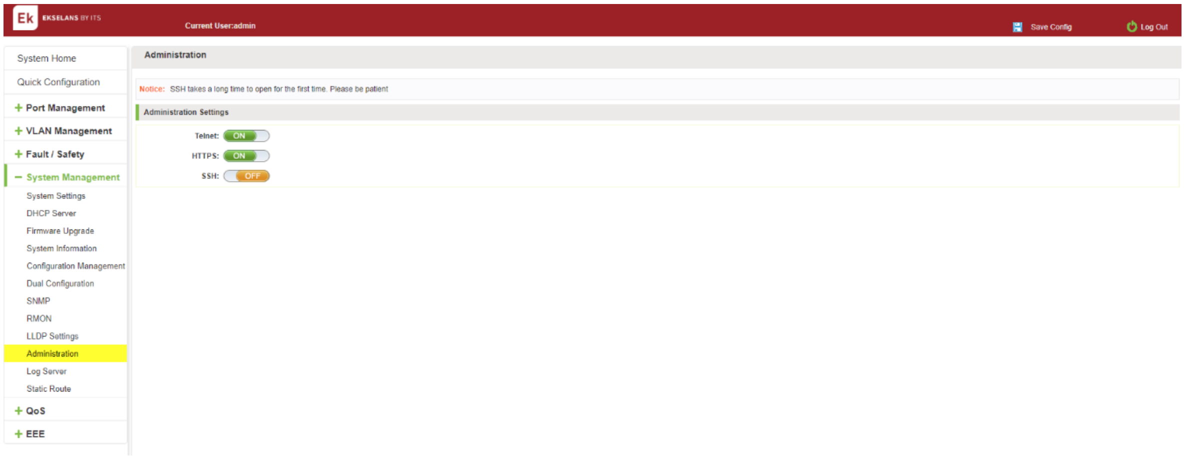
Notice: SSH takes a long time to open for the first time. Please be patient

Administration Settings

Telnet: OFF
HTTPS: ON
SSH: OFF

Figure 7-3: telnet.

After you turn on telnet, you can telnet the device to manage the device.



Current User:admin

Administration

Notice: SSH takes a long time to open for the first time. Please be patient

Administration Settings

Telnet: ON

HTTPS: ON

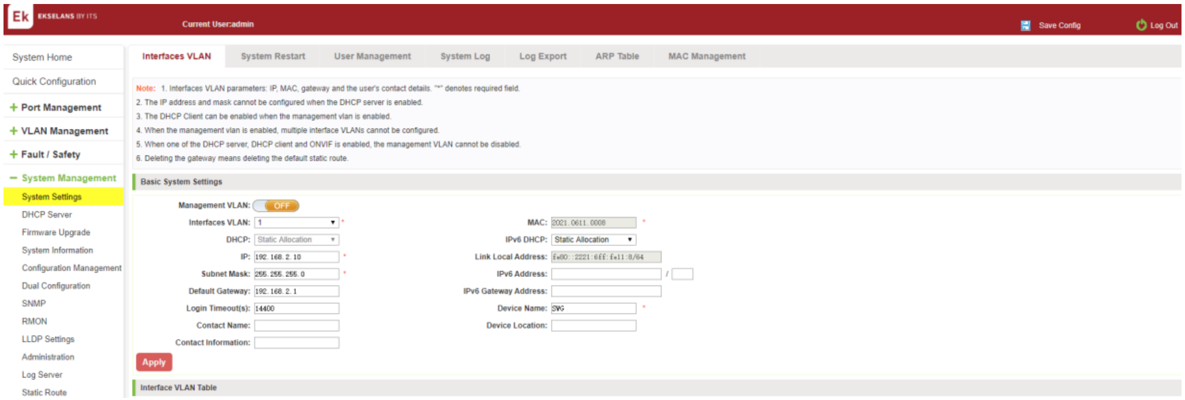
SSH: OFF

Figure 7-4: enable telnet.

Static Route.

Click on the "System Management" "Static Route"

Step1, Turn off switch management VLAN.



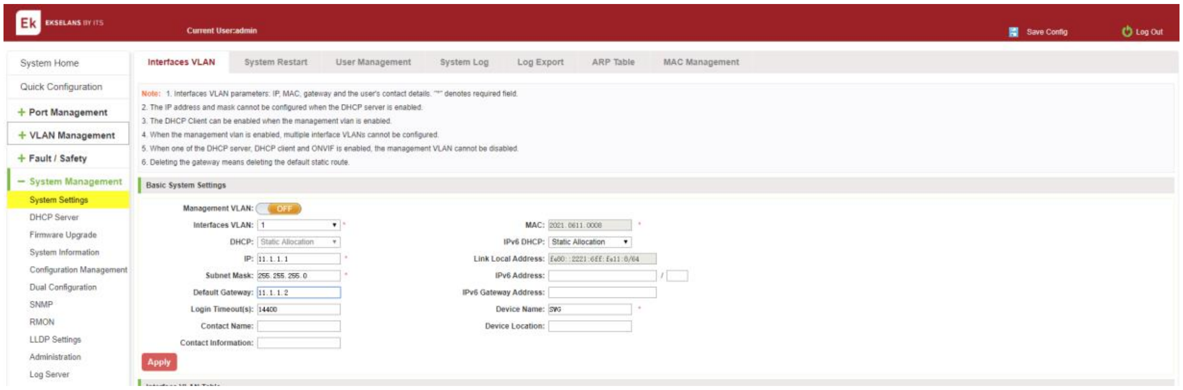
Note: 1. Interfaces VLAN parameters: IP, MAC, gateway and the user's contact details. "*" denotes required field.
2. The IP address and mask cannot be configured when the DHCP server is enabled.
3. The DHCP Client can be enabled when the management vlan is enabled.
4. When the management vlan is enabled, multiple interface VLANs cannot be configured.
5. When one of the DHCP server, DHCP client and ONVIF is enabled, the management VLAN cannot be disabled.
6. Deleting the gateway means deleting the default static route.

Basic System Settings

Management VLAN: OFF
Interfaces VLAN: 1 *
DHCP: Static Allocation
IP: 192.168.2.10 *
Subnet Mask: 255.255.255.0 *
Default Gateway: 192.168.2.1
Login Timeout(s): 14400
Contact Name:
Contact Information:
MAC: 2021.0611.0008 *
IPv6 DHCP: Static Allocation
Link Local Address: fe80::2221:6ff:fe11:8/64
IPv6 Address: /
IPv6 Gateway Address:
Device Name: SWG *
Device Location:

Figure 7-46: Static Route.

Step 2, Modify the IP address of interface vlan1 to 10.1.1.1/24.



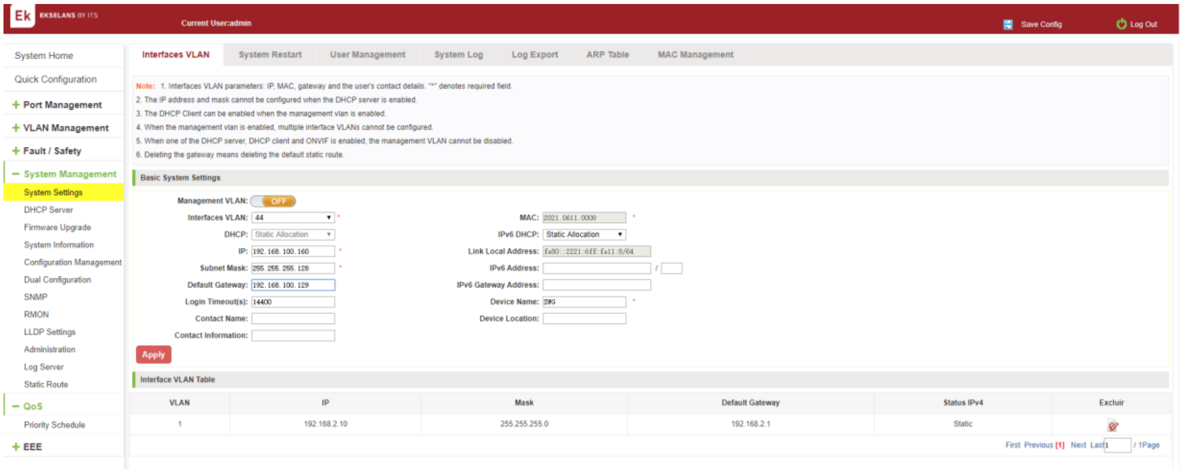
Note: 1. Interfaces VLAN parameters: IP, MAC, gateway and the user's contact details. "*" denotes required field.
2. The IP address and mask cannot be configured when the DHCP server is enabled.
3. The DHCP Client can be enabled when the management vlan is enabled.
4. When the management vlan is enabled, multiple interface VLANs cannot be configured.
5. When one of the DHCP server, DHCP client and ONVIF is enabled, the management VLAN cannot be disabled.
6. Deleting the gateway means deleting the default static route.

Basic System Settings

Management VLAN: OFF
Interfaces VLAN: 1 *
DHCP: Static Allocation
IP: 11.1.1.1 *
Subnet Mask: 255.255.255.0 *
Default Gateway: 11.1.1.2
Login Timeout(s): 14400
Contact Name:
Contact Information:
MAC: 2021.0611.0008 *
IPv6 DHCP: Static Allocation
Link Local Address: fe80::2221:6ff:fe11:8/64
IPv6 Address: /
IPv6 Gateway Address:
Device Name: SWG *
Device Location:

Figure 7-47: Static Route.

Step 3 Modify the IP address of interface vlan10 to 192.168.100.160/25.



Current User:admin

Note: 1. Interfaces VLAN parameters: IP, MAC, gateway and the user's contact details. "*" denotes required field.
2. The IP address and mask cannot be configured when the DHCP server is enabled.
3. The DHCP Client can be enabled when the management vlan is enabled.
4. When the management vlan is enabled, multiple interface VLANs cannot be configured.
5. When one of the DHCP server, DHCP client and ONVIF is enabled, the management VLAN cannot be disabled.
6. Deleting the gateway means deleting the default static route.

Basic System Settings

Management VLAN: OFF
Interfaces VLAN: 44 *
DHCP: Static Allocation
IP: 192. 168. 100. 160 *
Subnet Mask: 255. 255. 255. 128 *
Default Gateway: 192. 168. 100. 129
Login Timeout(s): 14400
Contact Name:
Contact Information:
MAC: 2021. 0611. 0008 *
IPv6 DHCP: Static Allocation
Link Local Address: fe80::2221:6ff:fe11:8/64
IPv6 Address: /
IPv6 Gateway Address:
Device Name: SWG *
Device Location:

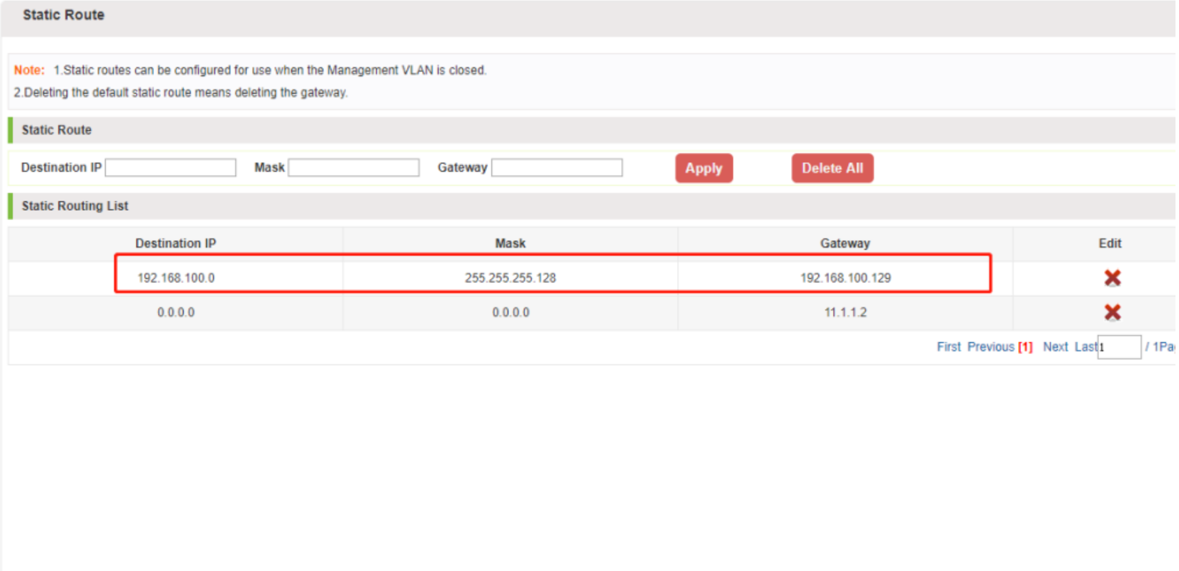
Interface VLAN Table

VLAN	IP	Mask	Default Gateway	Status IPv4	Excluir
1	192.168.2.10	255.255.255.0	192.168.2.1	Static	✎

First Previous [1] Next Last 1 / 1Page

Figure 7-48: Static Route.

Step 4, The gateway with static route 192.168.100.0/25 added is 192.168.100.129.



Static Route

Note: 1.Static routes can be configured for use when the Management VLAN is closed.
2.Deleting the default static route means deleting the gateway.

Static Route

Destination IP Mask Gateway

Static Routing List

Destination IP	Mask	Gateway	Edit
192.168.100.0	255.255.255.128	192.168.100.129	✖
0.0.0.0	0.0.0.0	11.1.1.2	✖

First Previous [1] Next Last 1 / 1Pa

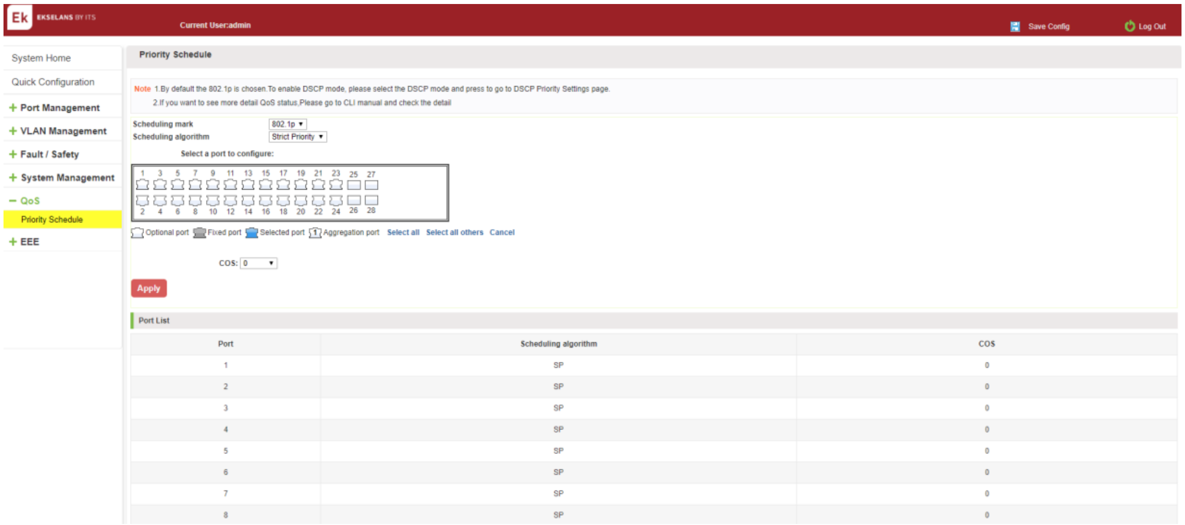
Figure 7-49: Static Route.

QOS.

Priority Schedule.

View the priority schedule.

Click on the "QOS" "priority schedule", can view the device priority schedule:



Priority Schedule

Note 1.By default the 802.1p is chosen.To enable DSCP mode, please select the DSCP mode and press to go to DSCP Priority Settings page.
2.If you want to see more detail QoS status,Please go to CLI manual and check the detail

Scheduling mark: 802.1p
Scheduling algorithm: Strict Priority

Select a port to configure:

COS: 0

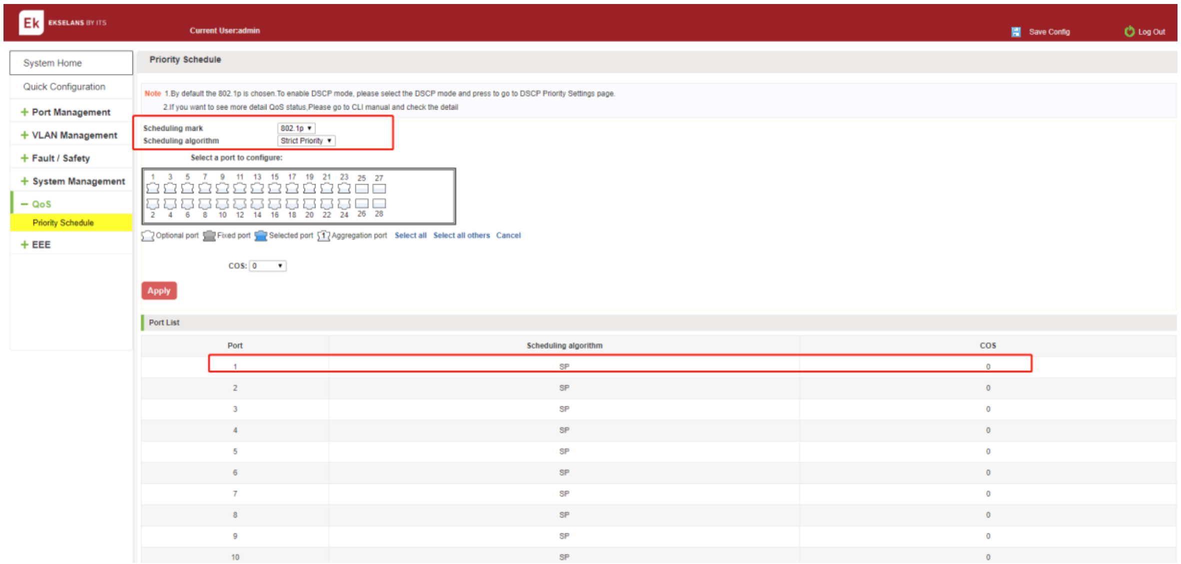
Port List

Port	Scheduling algorithm	COS
1	SP	0
2	SP	0
3	SP	0
4	SP	0
5	SP	0
6	SP	0
7	SP	0
8	SP	0

Figure 8-1: priority schedule.

THE CONFIGURATION GLOBAL SETTINGS OF 802.1P SP.

Click on "QOS" "priority schedule" “global settings”, in scheduling mark, choose 802.1p, in the Scheduling algorithm, choose strict priority.



Current User:admin

Priority Schedule

Note 1.By default the 802.1p is chosen.To enable DSCP mode, please select the DSCP mode and press to go to DSCP Priority Settings page.
2.If you want to see more detail QoS status,Please go to CLI manual and check the detail

Scheduling mark: 802.1p
Scheduling algorithm: Strict Priority

Select a port to configure:

COS: 0

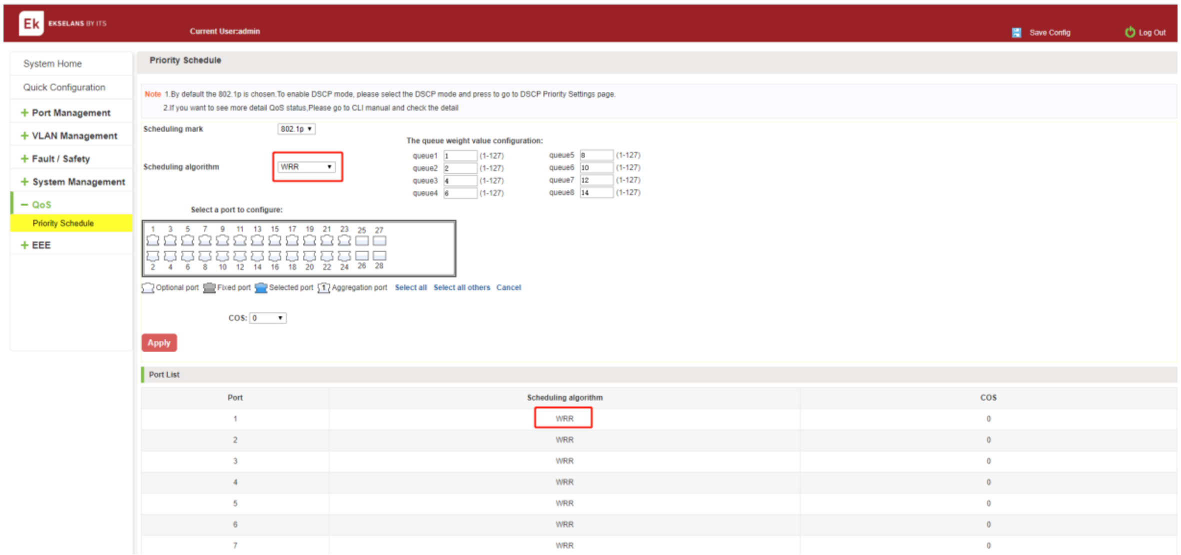
Port List

Port	Scheduling algorithm	COS
1	SP	0
2	SP	0
3	SP	0
4	SP	0
5	SP	0
6	SP	0
7	SP	0
8	SP	0
9	SP	0
10	SP	0

Figure 8-2: global settings in 802.1p and SP.

THE CONFIGURATION GLOBAL SETTINGS OF 802.1P SP ADD WRR.

Click on "QOS" "priority schedule" “global settings”, in scheduling mark, choose 802.1p, in the Scheduling algorithm,choose WRR.



Priority Schedule

Note 1.By default the 802.1p is chosen.To enable DSCP mode, please select the DSCP mode and press to go to DSCP Priority Settings page.
2.If you want to see more detail QoS status,Please go to CLI manual and check the detail

Scheduling mark: 802.1p

Scheduling algorithm: WRR

The queue weight value configuration:

queue1	1	(1-127)	queue5	8	(1-127)
queue2	2	(1-127)	queue6	10	(1-127)
queue3	4	(1-127)	queue7	12	(1-127)
queue4	6	(1-127)	queue8	14	(1-127)

Select a port to configure:

COS: 0

Port List

Port	Scheduling algorithm	COS
1	WRR	0
2	WRR	0
3	WRR	0
4	WRR	0
5	WRR	0
6	WRR	0
7	WRR	0

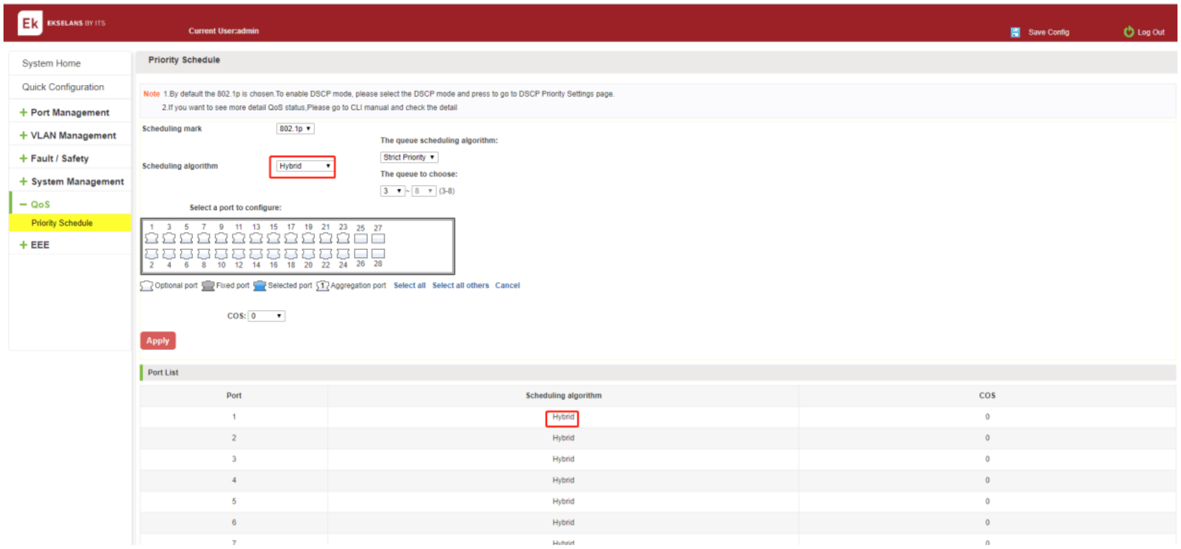
Figure 8-3: global settings in 802.1p and WRR.

Priority schedule steps are as follows:

Step1: in scheduling mark , choose 802.1p;step2:in the Scheduling algorithm, choose WRR ,step3:in queue1 text box, enter the weight value ,such as 1;step4:in queue2 text box, enter the weight value ,such as 20;step5:in queue3 text box, enter the weight value ,such as 40;Step6:in queue4 text box, enter the weight value ,such as 1.

THE CONFIGURATION GLOBAL SETTINGS OF 802.1P AND HYBRID.

Click on "QOS" "priority schedule" “global settings”, in scheduling mark, choose 802.1p, in the Scheduling algorithm, choose hybrid.



Priority Schedule

Note 1.By default the 802.1p is chosen.To enable DSCP mode, please select the DSCP mode and press to go to DSCP Priority Settings page.
2.If you want to see more detail QoS status,Please go to CLI manual and check the detail

Scheduling mark: 802.1p

Scheduling algorithm: Hybrid

The queue scheduling algorithm: Strict Priority

The queue to choose: 3 ~ 8 (3-8)

Select a port to configure:

COS: 0

Port List

Port	Scheduling algorithm	COS
1	Hybrid	0
2	Hybrid	0
3	Hybrid	0
4	Hybrid	0
5	Hybrid	0
6	Hybrid	0
7	Hybrid	0

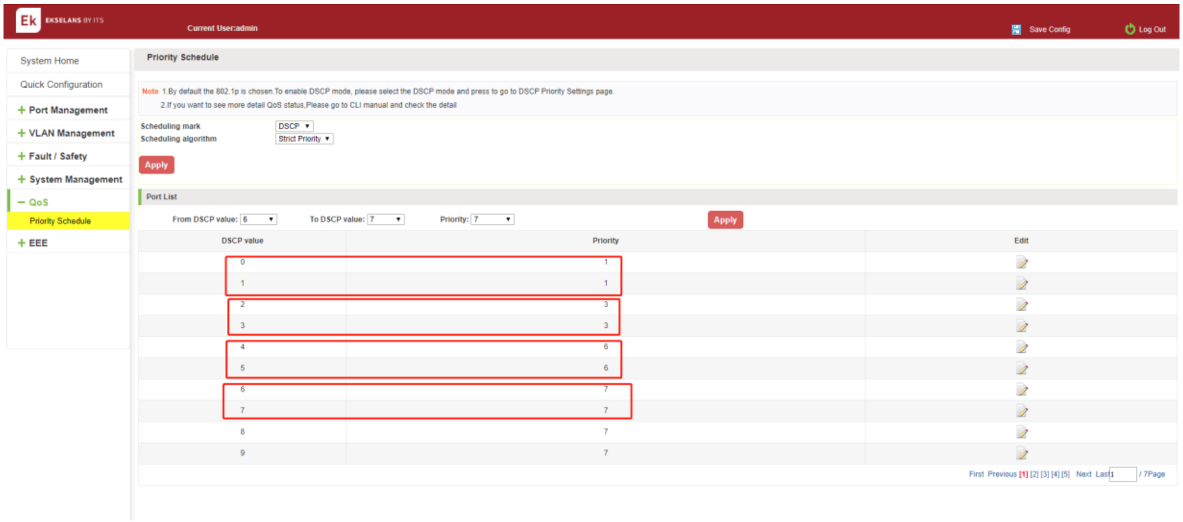
Figure 8-4: global settings in 802.1p and hybrid.

Priority schedule steps are as follows:

Step1: in scheduling mark, choose 802.1p; step2:in the Scheduling algorithm, choose hybrid, step3:in strict priority text box, choose the queue3,4;step4:in WRR text box, choose the queue 1,2 ;step5:in queue1 text box, enter the weight value ,such as 1;Step6:in queue2 text box, enter the weight value ,such as 20.

THE CONFIGURATION GLOBAL SETTINGS OF DSCP AND SP.

Click on "QOS" "priority schedule" "global settings", in scheduling mark, choose DSCP, in the Scheduling algorithm, choose strict priority.



Note 1.By default the 802.1p is chosen.To enable DSCP mode, please select the DSCP mode and press to go to DSCP Priority Settings page.
2.If you want to see more detail QoS status,Please go to CLI manual and check the detail

Scheduling mark: DSCP
Scheduling algorithm: Strict Priority

Apply

Port List

From DSCP value: 6 To DSCP value: 7 Priority: 7 Apply

DSCP value	Priority	Edit
0	1	
1	1	
2	3	
3	3	
4	6	
5	6	
6	7	
7	7	
8	7	
9	7	

First Previous [1] [2] [3] [4] [5] Next Last 1 / 7Page

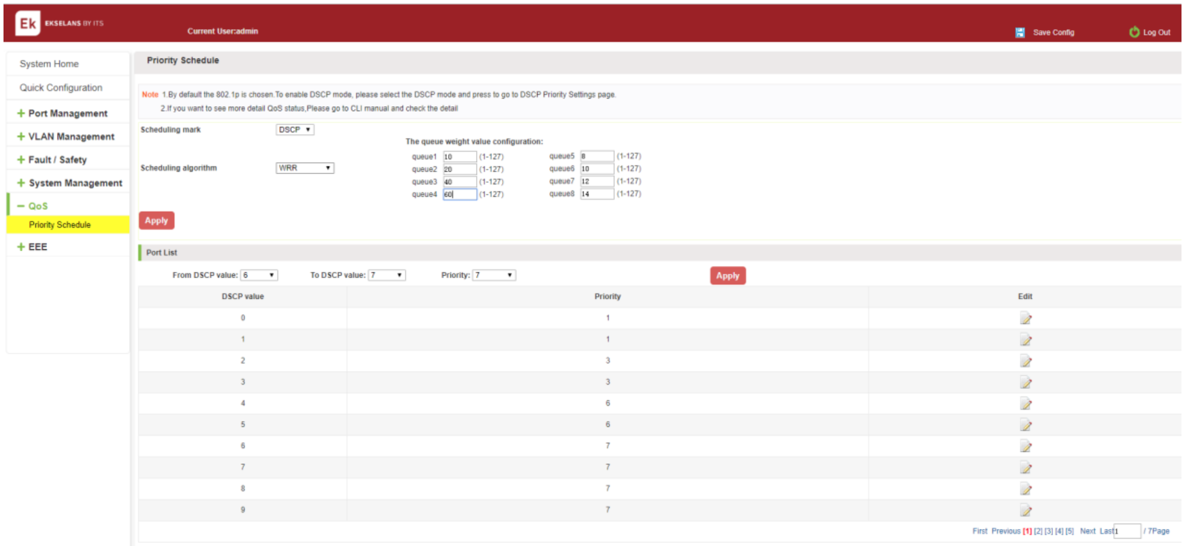
Figure 8-5: global settings in DSCP and SP.

Priority schedule steps are as follows:

- Step1: in scheduling mark, choose DSCP; step2:in the Scheduling algorithm, choose strict priority.
- Step3:in from DSCP value text box, choose 0 and in to DSCP value text box, choose 1 and in priority text box, choose 1.
- Step4:in from DSCP value text box, choose 2 and in to DSCP value text box, choose 3 and in priority text box, choose 3.
- Step5:in from DSCP value text box, choose 4 and in to DSCP value text box, choose 5 and in priority text box, choose 6.
- Step6:in from DSCP value text box, choose 6 and in to DSCP value text box, choose 8 and in priority text box, choose 7.

THE CONFIGURATION GLOBAL SETTINGS OF DSCP AND WRR.

Click on "QOS" "priority schedule" “global settings ”, in scheduling mark , choose DSCP, in the Scheduling algorithm, choose strict priority.



Priority Schedule

Note 1.By default the 802.1p is chosen.To enable DSCP mode, please select the DSCP mode and press to go to DSCP Priority Settings page.
2.If you want to see more detail QoS status,Please go to CLI manual and check the detail

Scheduling mark: DSCP

Scheduling algorithm: WRR

The queue weight value configuration:

queue1 10 (1-127)
queue2 20 (1-127)
queue3 40 (1-127)
queue4 60 (1-127)
queue5 8 (1-127)
queue6 10 (1-127)
queue7 12 (1-127)
queue8 14 (1-127)

Port List

From DSCP value: 6 To DSCP value: 7 Priority: 7

DSCP value	Priority	Edit
0	1	✎
1	1	✎
2	3	✎
3	3	✎
4	6	✎
5	6	✎
6	7	✎
7	7	✎
8	7	✎
9	7	✎

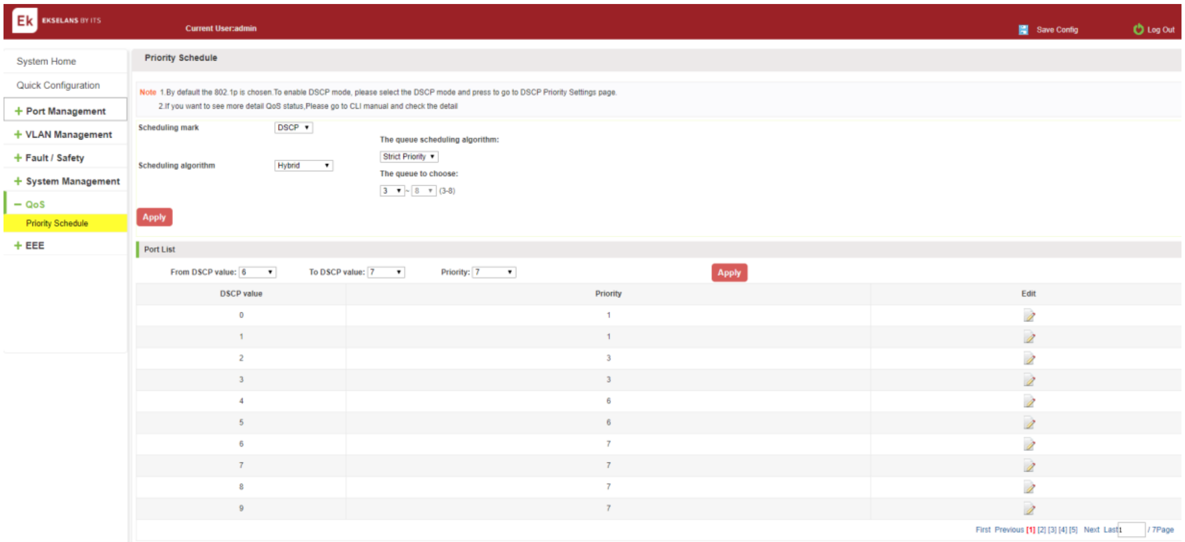
Figure 8-6: global settings in DSCP and WRR.

Priority schedule steps are as follows:

Step1: in scheduling mark, choose DSCP; step2:in the Scheduling algorithm, choose WRR ,step3:in queue1 text box, enter the weight value ,such as 10;step4:in queue2 text box, enter the weight value ,such as 20;step5:in queue3 text box, enter the weight value ,such as 30;Step6:in queue4 text box, enter the weight value ,such as 40.

THE CONFIGURATION GLOBAL SETTINGS OF DSCP AND HYBRID.

Click on "QOS" "priority schedule" “global settings”, in scheduling mark , choose DSCP, in the Scheduling algorithm, choose hybrid.



Priority Schedule

Note 1.By default the 802.1p is chosen.To enable DSCP mode, please select the DSCP mode and press to go to DSCP Priority Settings page.
2.If you want to see more detail QoS status,Please go to CLI manual and check the detail

Scheduling mark: DSCP

Scheduling algorithm: Hybrid

The queue scheduling algorithm: Strict Priority

The queue to choose: 3 ~ 8 (3-8)

Apply

Port List

From DSCP value: 6 To DSCP value: 7 Priority: 7 Apply

DSCP value	Priority	Edit
0	1	
1	1	
2	3	
3	3	
4	6	
5	6	
6	7	
7	7	
8	7	
9	7	

First Previous [1] [2] [3] [4] [5] Next Last 1 / 7Page

Figure 8-7: global settings in DSCP and HYBRID:

Priority schedule steps are as follows:

Step1: in scheduling mark, choose DSCP.

Step2:in the Scheduling algorithm, choose hybrid.

Step3:in strict priority text box, choose the queue3,4.

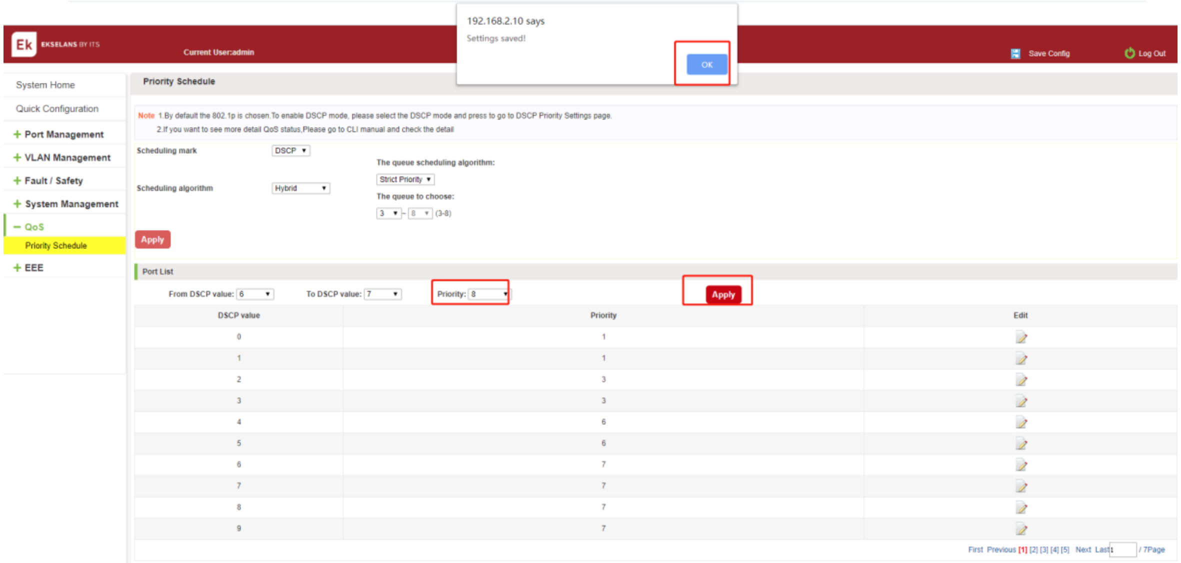
Step4:in WRR text box, choose the queue 1,2.

Step5:in queue1 text box, enter the weight value, such as 10.

Step6:in queue2 text box, enter the weight value, such as 20.

Editing the DSCP values.

Click on the " 📝 "icon to modify DSCP values:



192.168.2.10 says

Settings saved!

Priority Schedule

Note 1.By default the 802.1p is chosen.To enable DSCP mode, please select the DSCP mode and press to go to DSCP Priority Settings page.
2.If you want to see more detail QoS status,Please go to CLI manual and check the detail

Scheduling mark: DSCP

Scheduling algorithm: Hybrid

The queue scheduling algorithm: Strict Priority

The queue to choose: 3 - 8 (3-8)

Port List

From DSCP value: 6 To DSCP value: 7 Priority: 8

DSCP value	Priority	Edit
0	1	📝
1	1	📝
2	3	📝
3	3	📝
4	6	📝
5	6	📝
6	7	📝
7	7	📝
8	7	📝
9	7	📝

Figure 8-8: Add the port to the VLAN.

Modify DSCP values follow these steps:

Step1: select DSCP values and Click " 📝 "icon.

Step 2: In the priority text box, choose medium.

Step3: Click on the Apply.

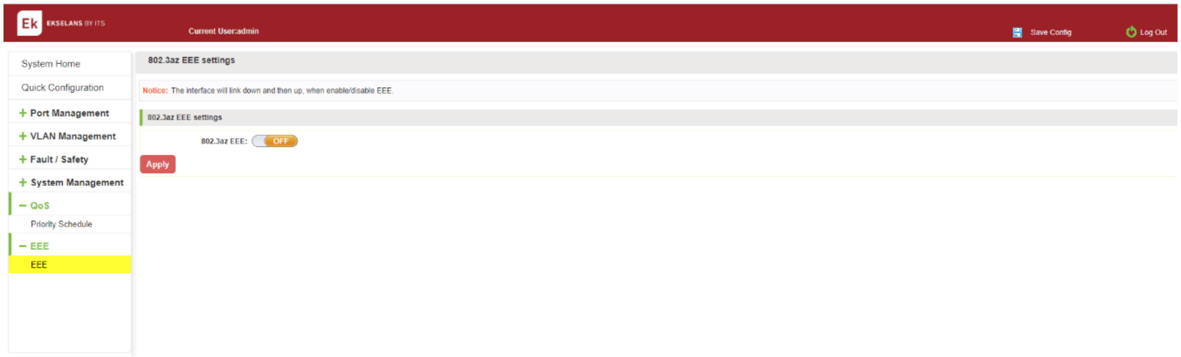
Step 4: click OK.

EEE.

EEE.

802.3AZ EEE SETTINGS.

Click on the "EEE" "EEE" "802.3az EEE settings", you can view the EEE information:



Notice: The interface will link down and then up, when enable/disable EEE.

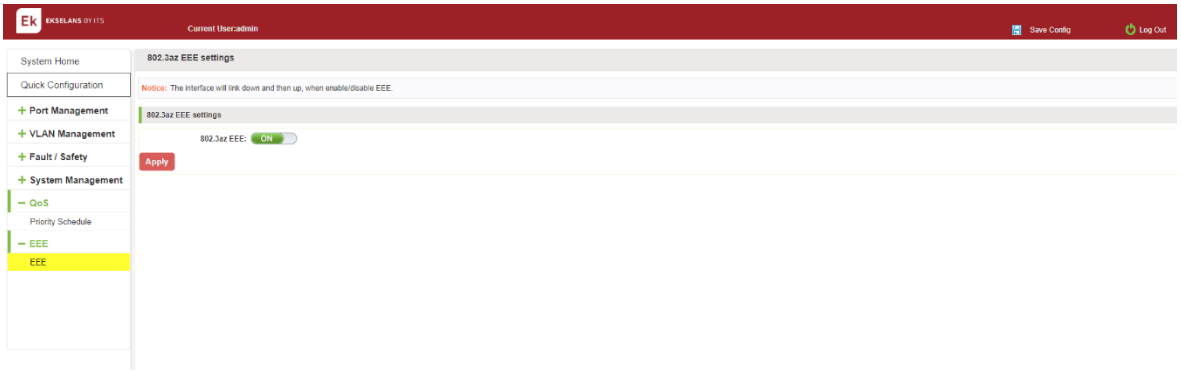
802.3az EEE settings

802.3az EEE: OFF

Figure 9-1: view the 802.3az EEE settings.

ACTIVE THE EEE.

Click ON the "EEE " "EEE" "802.3az EEE settings", choose the 802.3az EEE, click ON the "OFF" to "ON", click Apply:



Notice: The interface will link down and then up, when enable/disable EEE.

802.3az EEE settings

802.3az EEE: ON

Figure 9-2: active the 802.3az EEE settings.