



NX-IES
Industrial Switch
Series NXOS User
Guide

Copyright Statement

Nodexon Networks©2018

Nodexon Networks reserves all copyrights of this document. Any reproduction, excerption, backup, modification, transmission, translation or commercial use of this document or any portion of this document, in any form or by any means, without the prior written consent of Nodexon Networks is prohibited.

Exemption Statement

This document is provided “as is”. The contents of this document are subject to change without any notice. Please obtain the latest information through the Nodexon Networks website. Nodexon Networks endeavors to ensure content accuracy and will not shoulder any responsibility for losses and damages caused due to content omissions, inaccuracies or errors.

Preface

Thank you for using our products.

Audience

This manual is intended for:

- Network engineers
- Technical support and servicing engineers
- Network administrators

Obtaining Technical Assistance

Website:<https://www.nodexon.com/>

Technical Support Website:<https://nodexon.com/support>

Community:<http://www.nodexon.com/community>

Technical Support Email:support@nodexon.com

Case Portal :<https://www.nodexon.com/caseportal>

Related Documents

Documents	Description
Command Reference	Describes the related configuration commands, including command modes, parameter descriptions, usage guides, and related examples.
Hardware Installation and Reference Guide	Describes the functional and physical features and provides the device installation steps, hardware troubleshooting, module technical specifications, and specifications and usage guidelines for cables and connectors.

Conventions

This manual uses the following conventions:

Convention	Description
------------	-------------

boldface font	Commands, command options, and keywords are in boldface.
<i>italic</i> font	Arguments for which you supply values are in <i>italics</i> .
[]	Elements in square brackets are optional.
{ x y z }	Alternative keywords are grouped in braces and separated by vertical bars.
[x y z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.

Symbols

 Means reader take note. Notes contain helpful suggestions or references.

 Means reader be careful. In this situation, you might do something that could result in equipment damage or loss of data.

1 Smart Web Configuration

1.1 Overview

Web-based management allows you to manage switches, routers, and other network devices through browsers such as the Internet Explorer (IE).

Web-based management involves the Web server and Web client. The Web server, integrated into a device, is used to receive and process requests from the client (for reading Web files or executing commands), and return processing results to the client. The Web client is usually a Web browser, such as IE.

1.2 Configuration Environment Requirements

1.2.1 Client Requirements

- An administrator can log in to the Web-based management page of a switch from the Web browser of the Web client, to manage the switch. The client refers to a PC or some other mobile terminals such as laptops or iPads.
- Google Chrome, Firefox, IE9.0, IE11.0, and some IE kernel-based browsers (such as Maxthon) are supported. Exceptions such as garble or format error may occur if an unsupported browser is used.
- It is recommended to set the resolution to 1024 x 768, 1280 x 1024, or 1440 x 960. If other resolutions are used, the page font and format may not be aligned, the UI is unaesthetic, or other exceptions may occur.

1.2.2 Server Requirements

- The Web service needs to be enabled on the switch.
- Login authentication information for Web-based management needs to be configured for the switch.
- A management IP address needs to be configured for the switch.

1.3 Starting the Web Service

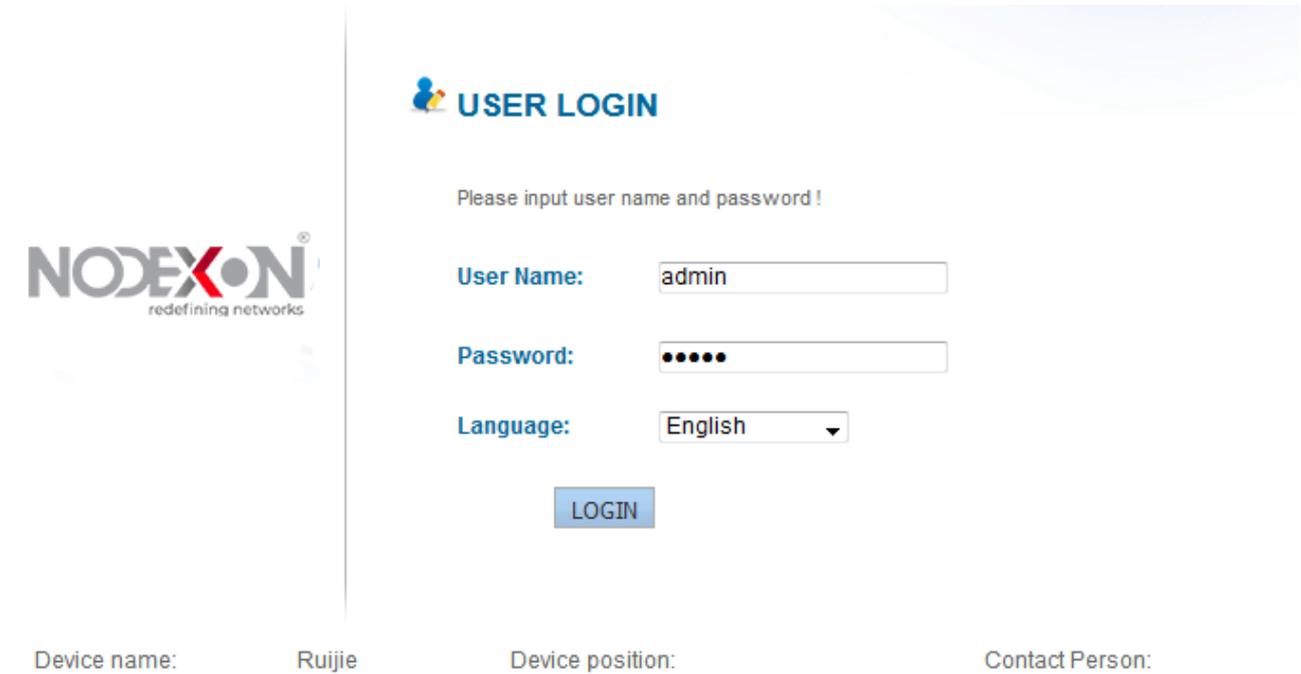
The Web service is enabled by default. You can enter **192.168.1.1** in the browser and press **Enter** to access the Web service. For details about the CLI configuration, see section 1.12 "Typical Configuration Examples".

Default Username/Password	Permission Description
admin/admin	Super administrator, having all permissions
guest/guest	Guest permission. A user with the guest permission is allowed to access the home page of the system and view the system status by default.

1.4 Logging In to Web Management Platform

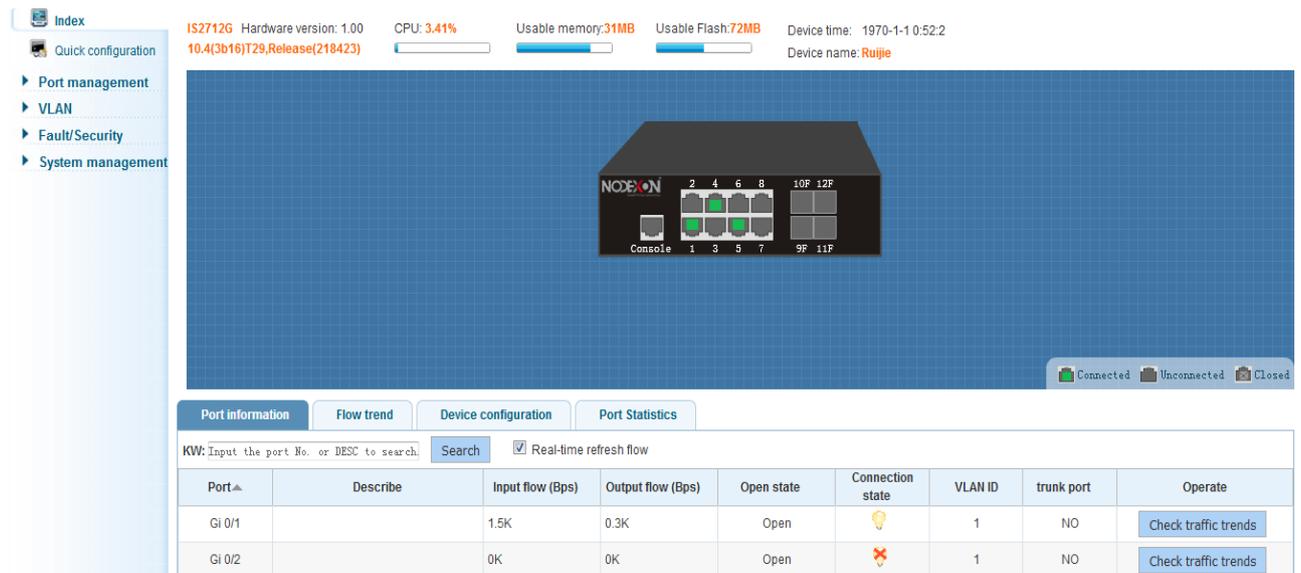
Enter the management IP address of a device in the address bar of the browser, for example, http://192.168.1.1, and press **Enter**. A page shown in the figure below is displayed.

Figure 1-1 Login Page



Enter the username and password and click **LOGIN**. After you are authenticated, the home page of the Web management platform is displayed, as shown in the figure below.

Figure 1-2 Home Page of Web Management Platform



1.5 Conventions

1.5.1 Icons and Buttons on the GUI

Icon/Button	Description
	Edit icon. Click this icon to edit the currently selected record.
	Delete icon
	Status switch icon
	Optional port, indicating that the port is available. Click it or select it to switch the port state to "selected".
	Non-optional port
	Selected port
	Aggregated port. The number illustrated indicates the aggregate port ID.
	Trunk port, displayed on the panel on the VLAN and VLAN Set pages.
	Save button. Click it to save the input information.
	Save button in the editing state. Click it to save the edited input information.
	Exit the editing state to refresh the panel and discard the input.
	Batch processing operations on ports on the panel. They are located in the lower right corner of the panel. Note: These operations are displayed only when a panel supports multiple choices.
	Mandatory item. An input box marked with this symbol indicates a mandatory item.
	Binding
	Note
	Warning

1.5.2 System Operations

Figure 1-3 Panel Diagram



Panel description: A panel indicates a switch and the port layout on the panel is consistent with that on the switch. The status displayed on the panel indicates the current port status of the device. Likewise, operations on the panel are actually performed on the device.

Panel operations: Click a port on the panel or hold and drag the mouse to select multiple ports to switch the port state to selected. You can configure a selected port, for example, add the port description and configure port mirror and port rate limited.

Port description: A port can have multiple states. As shown in the figure below, Port 7 and Port 8 can be member ports of an aggregate port and non-optional ports at the same time. Aggregate Port 1 is also a trunk port in the figure below. The selection of an aggregate port indicates that all members of the aggregate port are selected, except on the port management/aggregate port page. In general, when the mouse is moved over a non-optional port or aggregate port, information about the port is displayed in 1 or 2 seconds.

Figure 1-4 Panel Diagram



1.6 Home Page

Choose **Index** to access the home page of the system, as shown in the figure below.

Figure 1-5 Home Page

IS2712G Hardware version: 1.00
10.4(3b16)T29,Release(218423)

CPU: 2.79%
Usable memory: 30MB
Usable Flash: 72MB
Device time: 1970-1-1 3:1:38
Device name: Ruijie

CPU within 5 seconds: 3.00%
CPU within 1 minutes: 2.79%
CPU within 5 minutes: 1.43%

NOEXON
Console 2 4 6 8 10P 12P
1 3 5 7 9P 11F

Connected Unconnected Closed

Port information Flow trend Device configuration Port Statistics

KW: Input the port No. or DESC to search. Search Real-time refresh flow

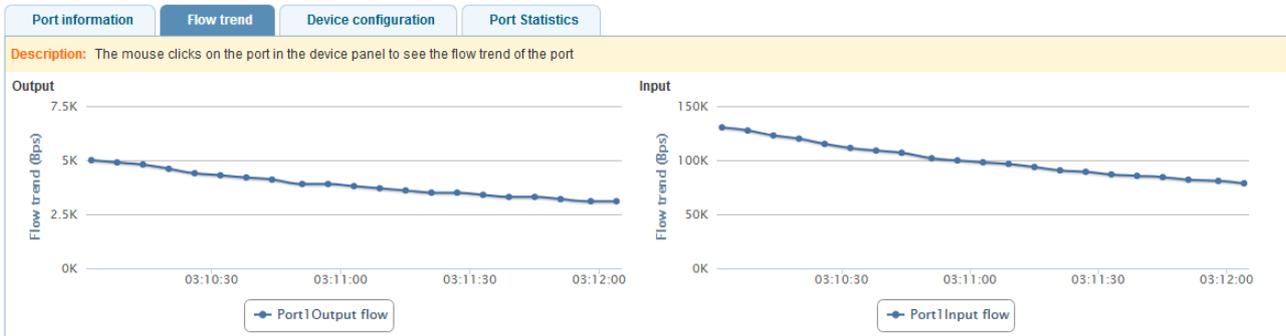
Port▲	Describe	Input flow (Bps)	Output flow (Bps)	Open state	Connection state	VLAN ID	trunk port	Operate
Gi 0/1		0.9K	0.1K	Open	💡	1	NO	Check traffic trends
Gi 0/2		0K	0K	Open	💡	1	NO	Check traffic trends
Gi 0/3		0K	0K	Open	💡	1	NO	Check traffic trends

Configuration description:

Port information: The **Port information** tab page displays the port information list of the device. Enter the port number or port description in the input box and click **Search** to search for required port information. You can click the **Port**, **Input flow**, or **Output flow** table header to sort the port list by column. If **Real-time refresh flow** is selected, the traffic data in the port list is updated at intervals. Click **Check traffic trends**. The traffic trend of the port is displayed and the **Flow trend** tab page is displayed.

Flow trend: Click **Check traffic trends** in the port list or click a port on the device panel to view the traffic trends of the port, as shown in the figure below.

Figure 1-6 Flow Trends



Device configuration: The **Device configuration** tab page displays the current overall configurations of the device. You can click **More settings** to access the specific configuration page, as shown in the figure below.

Figure 1-7 Device Configuration

Port information	Flow trend	Device configuration	Port Statistics
Total number of device VLAN	1	More settings	
Number of Aggregation Link	1	More settings	
Port mirroring	CLOSE	More settings	
Anti-DHCP attack defense	CLOSE	More settings	
Anti-DOS attack defense	CLOSE	More settings	
Anti-Loop attack defense	OPEN	More settings	

1.7 Quick Configuration

Choose **Quick configuration** to access the **Quick configuration** page. This page is displayed when a device is configured for the first time.

Figure 1-8 Quick Configuration

Note: Click the button to restart the switch. The restart process may take 1 minute. Please wait patiently. The page will be refreshed automatically after device restart. Then restore factory setting.



On the **Quick configuration** page, select **Ring network** or **Star network** based on the actual network type.

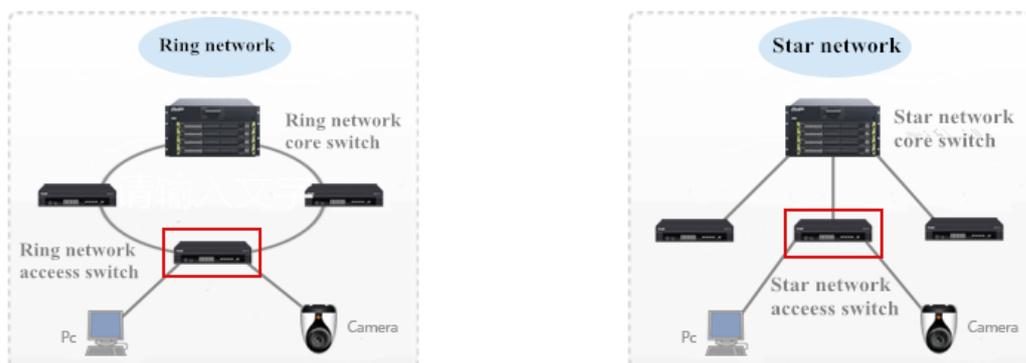
Configuration description:

Quick configuration can be used only when a device is configured for the first time. It is unavailable when a device has been configured. You need to restore the factory settings, restart the device, and then use quick configuration.

Different configuration wizards are displayed for different network types.

Figure 1-9 Selecting a Network Type

Note: Click the button to restart the switch. The restart process may take 1 minute. Please wait patiently. The page will be refreshed automatically after device restart. Then restore factory setting.



The configuration of a ring network access device includes the VLAN settings, Ethernet ring protection switching (ERPS) settings, Simple Network Management Protocol (SNMP) settings, and time synchronization settings, as shown in the figure below.

Figure 1-10 Configuring a Ring Network Access Device

1 VLAN Setting: Configure a management vlan and data VLAN for your device.

Manage VLAN ID(1-4094): 1 * i

VLAN name: VLAN0001

Manage IP: 192.168.1.1 Mask: 255.255.255.0

Default gateway: *

Data VLAN ID(1-4094): 1 *

2 ERPS Setting: When configuring the ERPS, the port mode of the selected port will be configured as the trunk mode.

ERPS VLAN ID(2-4094): 4000 *

2	4	6	8	10	12
<input checked="" type="checkbox"/>					
1	3	5	7	9	11
<input type="checkbox"/>					

Optional Non-optional Selected Aggregated Tip: Press the left button and drag to select multiple ports

All Invert Deselect

3 SNMP Setting: Configure SNMP administrator to monitor and manage nodes on the net.

SNMP service: Closed

4 Other Setting: Configure device time synchronization with NTP server, device name.

Time synchronization: Opened

Time server IP: *

Device name: Ruijie

A management VLAN is used for the switch management. An IP address and default gateway need to be configured for the management VLAN. After configuration, you need to access the management IP address to manage the switch. Port GI0/1 is the management port by default.

A data VLAN is used for devices in the user data communication network, such as the front-end PC or camera. Data VLANs differ from management VLANs, but they can use the same VLAN ID.

In the ERPS configuration, set an ID of the VLAN that needs ERPS and select two ports for connecting to the ERPS ring network.

The SNMP service is disabled by default. You can enable it and configure the trap host and SNMP password (community attributes).

The time synchronization function is enabled by default. You need to configure the IP address of the NTP server to synchronize the system time. The NTP server can be deployed on the upper-level core switch/router or on the server. If a device is capable of accessing the Internet, the public NTP server on the Internet can be used.

The configuration of a star network access device includes the VLAN settings, upper connector settings, SNMP settings, and time synchronization settings, as shown in the figure below.

Figure 1-11 Configuring a Star Network Access Device

1 VLAN setting: Configure a management VLAN and data VLAN for your device.

Manage VLAN ID(1-4094) : * i

VLAN name:

Management IP: * Mask:

Default gateway: *

Data VLAN ID(1-4094) : *

2 Upper connector: Select the port to connect to the uplink network, which will be set to the trunk port.

2	4	6	8	10	12
1	3	5	7	9	11

Optional
 Non-optional
 Selected
 Aggregated
 Trunk

3 SNMP setting: Configure SNMP administrator to monitor and manage nodes on the net.

SNMP services: Opened Closed

4 Other configurations: Can Configure device time synchronization with NTP server, device name.

Time synchronization: Opened Closed

Time server IP: *

Device name:

Step 1, Step 3, and Step 4 are the same as those for configuring a ring network access network.

In Step 2, you need to configure an uplink port, that is, the port for connecting to the upper-level switch. The selected uplink port will be set as a trunk port.

! After the management IP address is changed and saved, the page will be suspended and gives no response. Change the IP address of the client to ensure that it is in the same network segment as the management IP address, and then use the changed IP address to access the Web management system of the device.

1.8 Port Management

1.8.1 Basic Settings

Choose **Port management > Basic settings** to access the **Port Basic Settings** page.

Figure 1-12 Port Basic Settings

Port Basic Settings

Description: Setting the port on the panel, select multiple ports for batch settings, and support mouse drag to select multiple ports.
Note: If the selected parameter is not supported, the corresponding setting will not take effect!

Select the port to set:

2

4

6

8

10

12

1

3

5

7

9

11

Optional Non-optional Selected Aggregated Tip: Press the left button and drag to select multiple ports

All Invert Deselect

Port description(0-80): Port status : no modify

Port rate: Auto Work mode: Auto

Port list

port	port description	port state	port rate	mode	operation
1		Open	Auto	Auto	
2		Open	Auto	Auto	
3		Open	Auto	Auto	
4		Open	Auto	Auto	
5		Open	Auto	Auto	

Configuration description:

Port basic settings: Select a required port, set the port status, port rate, and work mode. The value **no modify** indicates that original configuration is retained. During batch setting, you can modify one or several items in batches by setting other items to **no modify**.

Batch port description setting: Click **Batch editing**. A dialog box shown in the figure below is displayed.

Figure 1-13 Batch Port Editing

the description of batch editing ✕

port	port description
1	<input type="text" value="important"/>
2	<input type="text" value="desc"/>
3	<input type="text"/>
4	<input type="text"/>
5	<input type="text"/>
6	<input type="text"/>
7	<input type="text"/>
8	<input type="text"/>
9	<input type="text"/>
10	<input type="text"/>

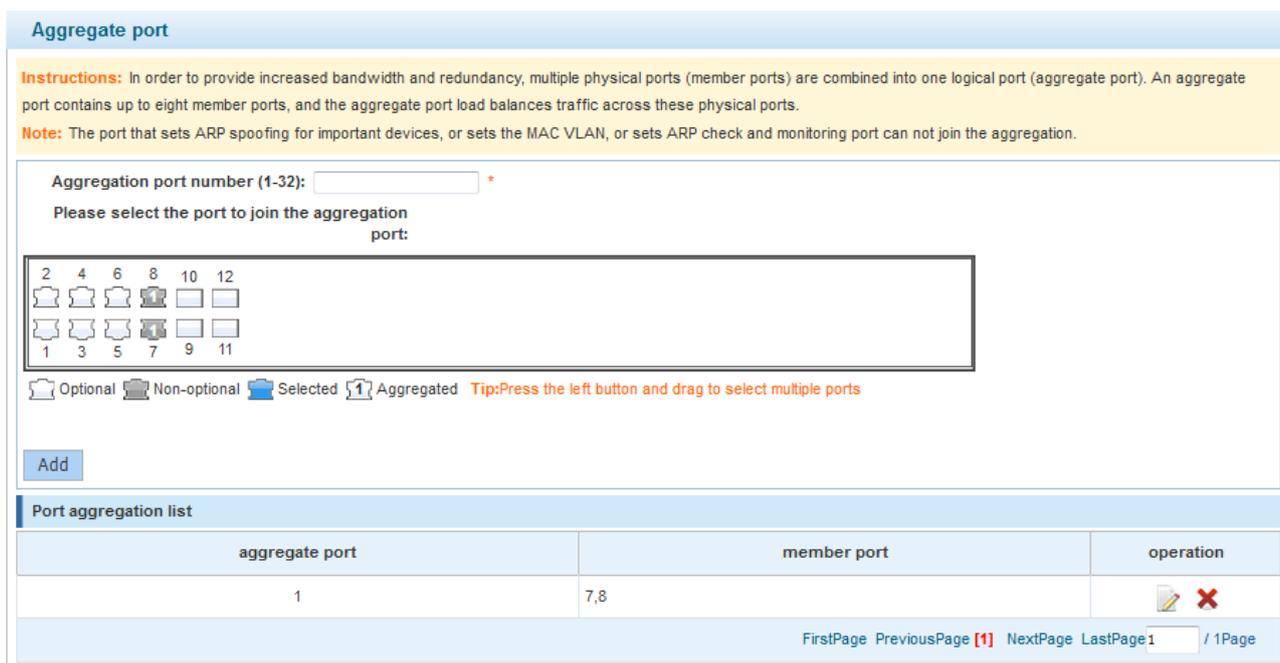
Enter port description in text boxes and click **set** for the configurations to take effect.

! When multiple ports are selected, **Port description** becomes unavailable. To set port descriptions in batches, click **Batch editing** and enter port descriptions in the displayed dialog box. If you clear the text boxes and then click **set**, the descriptions of all ports on the device will be cleared.

1.8.2 Aggregate Port

Choose **Port management > Aggregate port** to access the **Aggregate port** page.

Figure 1-14 Aggregate Port



Configuration description:

Creating an aggregate port: Enter an aggregate port number, select member ports, and then click **Add**. An adding success message is displayed, indicating that the aggregate port is created. The aggregate port is displayed on the panel after successful creation.

Editing an aggregate port: Aggregate ports displayed on the panel are non-optional. To edit an aggregate port, click the edit icon in the **operation** column in **Port aggregation list**. Member ports of the aggregate port are selected. Click a member port to deselect it and then click **Save editing** to save the modification.

Deleting an aggregate port: To delete an aggregate port, click the delete icon in the **operation** column in **Port aggregation list**. A message is displayed, asking you whether to delete the aggregate port. Click **Yes** to delete the aggregate port. After deletion, the deleted aggregate port becomes an optional port on the panel.

! ARP-enabled ports, ARP-spoofing-enabled ports on important devices, ports with the MAC VLAN function enabled, and monitoring ports in port mirror cannot be aggregated and are displayed as non-optional ports on the panel. If you move the mouse over an non-optional port, a message is displayed, indicating that these functions are enabled on the port and cannot be selected.

1.8.3 Port Mirroring

Choose **Port management > Port Mirroring** to access the **Port Mirroring** page.

Figure 1-15 Port Mirroring

Port Mirroring

Description: Port mirroring is the capability to send a copy of network packets seen on the source port to the destination port for analysis by a network analyzer. Traffic on multiple source ports can be mirrored to one single destination port.

Note: Some ports that have been added to the aggregation ports cannot be used as destination or source ports, and the destination port and the source port cannot be the same.

Please select source port:(You can select multiple ports, but it may affect device performance)

2	4	6	8	10	12
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1	3	5	7	9	11
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Optional
 Non-optional
 Selected
 Aggregated
 Tip:Press the left button and drag to select multiple ports

All Invert Deselect

Please select destination port:
port:(select only one port)

2	4	6	8	10	12
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1	3	5	7	9	11
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Optional
 Non-optional
 Selected
 Aggregated

Port mirroring list

Source port	Destination port	operation
Gi0/4	Gi0/3	✘

[FirstPage](#)
[PreviousPage](#)
1
[NextPage](#)
[LastPage](#)
1 / 1Page

Configuration description:

The **Port Mirroring** page is editable initially because the SmartWeb allows only one mirroring port. There are two panels on this page. The upper panel allows you to select a source port (mirrored port, multiple choices are supported) while the lower panel allows you to select only one destination port (mirroring port). After selecting or changing ports on the panel, click **save**. A setting success message is displayed.

- ⚠ The panel displays the status of current aggregate ports, which are editable. If you change a port and want to discard the change, click **refresh** to restore the configuration status of current aggregate ports on the panel.
- ⚠ Members of an aggregate port cannot be used as the destination port or source port, and the destination port cannot be the same as the source port.

1.8.4 Port Rate Limiting

Choose **Port management > Port rate limiting** to access the **Port rate limiting** page.

Figure 1-16 Port Rate Limiting

Port rate limiting

Description: Select one port or multiple ports on the panel to set. '-' means 'unlimited speed'.
Note: 1 MBit/s = 1000 KBit/s = 1000/8 KB/s = 125 KB/s. The theoretical rate for 1M bandwidth is 125KB/s.

Select port to set:

2	4	6	8	10	12
1	3	5	7	9	11

Optional
 Non-optional
 Selected
 Aggregated
 Tip: Press the left button and drag to select multiple ports

All Invert Deselect

Input speed limit (64-1000000): KBit/s
 Output speed limit (64-1000000): KBit/s

Port speed limit list

port	input speed limit	output speed limit	Operation
1	-	-	
2	-	-	
3	-	-	
4	-	-	

Configuration description:

Select a port on which the rate limit needs to be configured (multiple ports can be selected for batch rate limit configuration) on the panel, move the slider below the panel to adjust the input and output limits (the rate limit value is displayed on the right side of the slider). A selected port is not rate limited if the slider is moved rightmost. Click **Save**. A setting success message is displayed. The rate limits configured for the ports are displayed in **Port speed limit list**. Select a port on the panel. The slider slides to the relevant position and the specific rate limit value is displayed. You can change and save the value.

Aggregate ports cannot be rate limited.

1.8.5 ERPS Settings

Choose **Port management > ERPS setting** to access the **ERPS setting** page and configure an ERPS network.

Figure 1-17 ERPS Setting

ERPS setting

Description: 1.The port that has been added to the loop cannot modify the Trunk property of the port, and East and West ports cannot be the same.
2. Users can delete ERPS ring configuration in the ERPS ring list.

Global ERPS

Opened

Ethernet ring configuration

ERPS ID(2-4094): *

Please select the ERPS port:(only two ports can be selected)

2	4	6	8	10	12
1	3	5	7	9	11

Optional
 Non-optional
 Selected
 Aggregated
 Tip:Press the left button and drag to select multiple ports

Note: A ring can only be configured with an Owner device and a blocking port. When you select the Owner device, you should choose a port configured as a blocking port!

Owner equipment:

ERPS ring list

ERPS VLAN	West port	East port	Blocking port	Ring link state	Operation
4000	Gi0/12 (Link Failure)	Gi0/11 (Link Failure)	None	initialize	✘

Configuration description:

Global ERPS is disabled by default. After global ERPS is enabled, you can create multiple ERPS rings. Only simple ERPS rings can be configured in this system while intersecting rings and tangent rings are not supported. Enter a VLAN ID and select two ports for an ERPS ring. Only one blocking port needs to and can be specified for each ERPS ring. The device on which the blocking port exists is configured as a Ring Protection Link (RPL) owner and the selected port is configured as an RPL port.

1.8.6 Optical Module

Choose **Port management > Optical Module** to access the **Optical Module** page. On this page, you can view information about an optical module, including the temperature, voltage, receive optical power, and transmit optical power, and whether the optical module works in the normal state.

Figure 1-18 Optical Module

Optical Module

Instructions 1.List (OK): the current state is normal
2.List (warning): the current state exceeds the allowable state of the device.
3.List(alarm):the current state is severely exceeding the allowable state of the device.

fiber module port information list

port number	temperature(°C)	voltage(V)	bias current(mA)	Receive optical power(dBm)	Send optical power(dBm)	warning	operation
FirstPage PreviousPage [1] NextPage LastPage 1 / 1Page							

1.9 VLAN

1.9.1 VLAN

Choose **VLAN** to access the **VLAN** page. The **VLAN** page contains the **VLAN Set** and **Trunk Set** tab pages.

- VLAN Set

Figure 1-19 VLAN Set

VLAN ID	VLAN	VLAN IP address	port
1	VLAN0001	192.168.1.1/24	1-6,9-12,Ag1

[Create VLAN](#)
[FirstPage](#)
[PreviousPage \[1\]](#)
[NextPage](#)
[LastPage 1](#) / 1Page

Configuration description:

Creating a VLAN: To create a VLAN, enter the VLAN ID. Other information is optional. Click **Create VLAN**. A creation success message is displayed and the created VLAN is displayed in the VLAN list.

Editing a VLAN: Click the edit icon in the last column of the VLAN list. Information about the VLAN is displayed. Edit the information and click **Save editing**. An editing success message is displayed.

Deleting a VLAN: Click the delete icon in the last column of the VLAN list. A message is displayed, asking you whether to delete the VLAN. Click **Yes**. A VLAN deletion success message is displayed, indicating that the VLAN is deleted. VLAN 1 is the default VLAN and cannot be deleted.

VLAN 1 is the default management VLAN. It can be modified but cannot be deleted. When changing the IP address of VLAN 1, ensure that the new IP address is reachable. After change, the SmartWeb redirects to the login page, on which you need to log in again. If the page direction fails and a message is displayed, indicating the page cannot be found, the configured IP address may be unreachable. In this case, check the network connection.

- Trunk Set

Figure 1-20 Trunk Set

specification: If a port is allowed through multiple VLAN packet

Interface	Interface mode	Native Vlan	Allowed VLAN	Operation
-----------	----------------	-------------	--------------	-----------

[Add Trunk](#)
[Delete Trunk](#)
[FirstPage](#)
[PreviousPage \[1\]](#)
[NextPage](#)
[LastPage 1](#) / 1Page

Configuration description:

Creating a trunk port: Select a port on the panel, and enter the native VLAN and permitted VLANs (for example, 3–5, 8, 10), and click **Add Trunk**. A creation success message is displayed. The created trunk port is displayed in the trunk list.

Editing a trunk port: Click the edit icon in the **Operation** column of the trunk list. Information about the trunk port is displayed. Edit the information and click **Save editing**. An editing success message is displayed.

Deleting a trunk port: Click the edit icon in the **Operation** column of the trunk list. A message is displayed, asking you whether to delete the trunk port. Click **Yes**. A deletion success message is displayed.

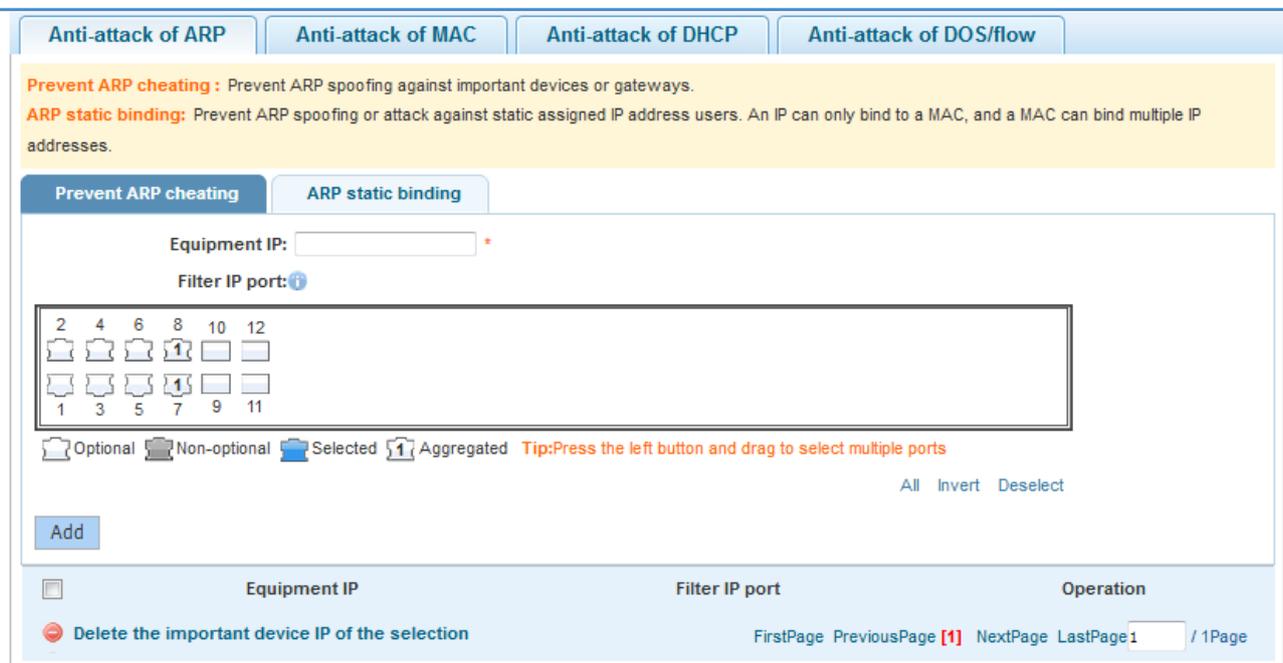
1.10 Fault/Security

1.10.1 Anti-attack

Choose **Fault/Security > Anti-attack** to access the **Anti-attack** page. The **Anti-attack** page contains four tab pages: **Anti-attack of ARP**, **Anti-attack of MAC**, **Anti-attack of DHCP**, and **Anti-attack of DOS/flow**.

- Anti-attack of ARP

Figure 1-21 Preventing ARP Cheating



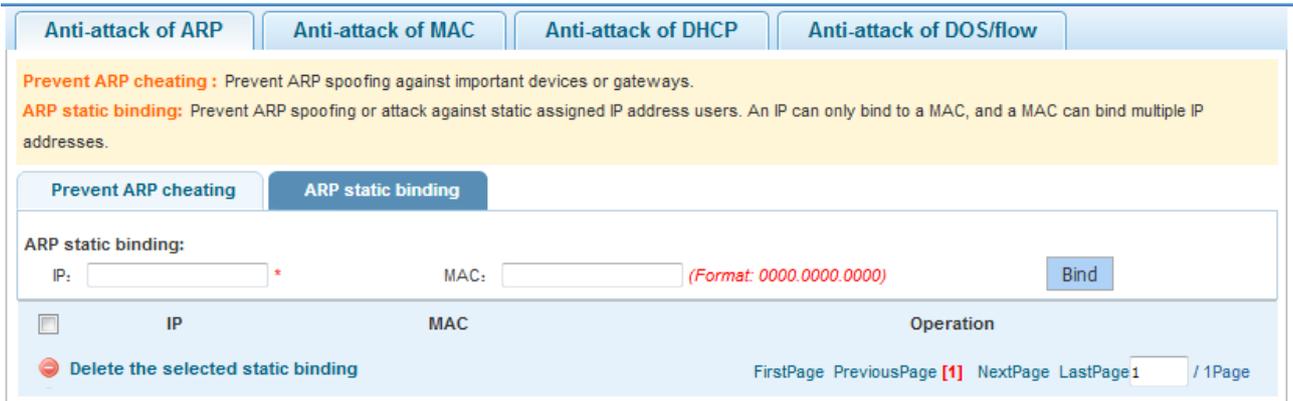
Configuration description:

Defense status: Click the status switch icon. After the ARP attack defense function is enabled, the defense settings are displayed on the page, which contains the **Prevent ARP cheating** and **ARP static binding** tab pages. After the ARP attack defense function is disabled, the defense settings are hidden and only the defense status is displayed.

Prevent ARP cheating: ARP spoofing prevention checks the source IP address of an ARP packet on the port, to determine whether the IP address matches the configured IP address of important equipment. If yes, the system discards the packet to prevent the user client from receiving incorrect ARP responses. Therefore, the IP address for packet filtering on the port need to be set. Set **Equipment IP**, select the port for filtering packets that matches the configured equipment IP address, and click **Add**. The added equipment IP address and the port for filtering are displayed in the list. Click the edit icon in the list to edit **Equipment IP** and **Filter IP port**. Click the delete icon. A message is displayed, asking you whether to delete the equipment IP. Click **Yes** to delete the IP address.

ARP static binding

Figure 1-22 ARP Static Binding



Configuration description:

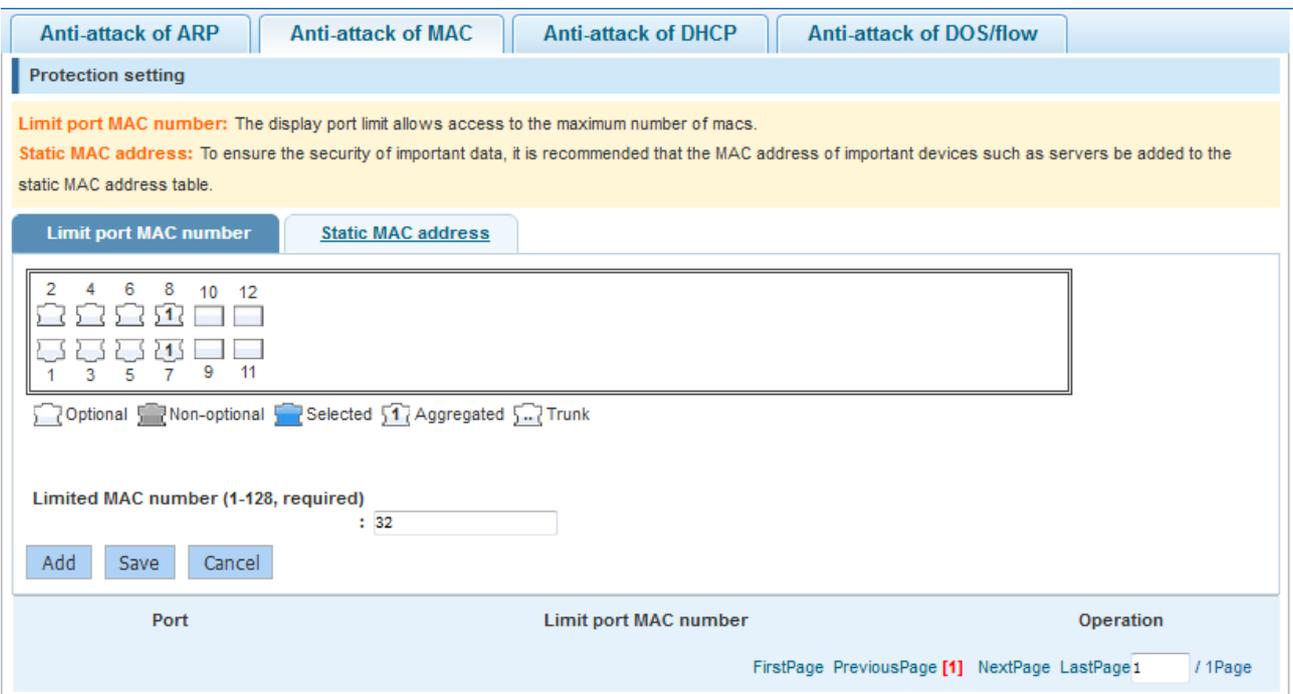
Add static binding: Manually enter an IP address and an MAC address and click **Bind**. The added static binding is displayed in the list.

Editing static binding: Click the edit icon in the list. The IP address and MAC address are displayed in the input boxes. Modify the IP address and MAC address and click **Bind** to save the modification.

Deleting static binding: Click the delete icon in the list. A message is displayed, asking you whether to delete the IP+MAC binding. Click **Yes** to delete the binding.

- Anti-attack of MAC

Figure 1-23 Limiting Port MAC Number



Configuration description:

Limit port MAC number: Select a required port and configure the limited number of MAC addresses, to limit the maximum number of MAC addresses that can be learnt by the selected port.

Static MAC address

Figure 1-24 Static MAC Address

Anti-attack of ARP
Anti-attack of MAC
Anti-attack of DHCP
Anti-attack of DOS/flow

Protection setting

Limit port MAC number: The display port limit allows access to the maximum number of macs.

Static MAC address: To ensure the security of important data, it is recommended that the MAC address of important devices such as servers be added to the static MAC address table.

Limit port MAC number

Static MAC address

MAC address list: All Manually bind MAC addresses

<input type="checkbox"/>	Users MAC	Port	Port category	Port description	Operation
<input type="checkbox"/>	000c.291f.b2cf	Gi0/1	Static		
<input type="checkbox"/>	000c.293d.c049	Gi0/1	Static		
<input type="checkbox"/>	000c.2967.96ae	Gi0/1	Static		
<input type="checkbox"/>	000c.2982.c945	Gi0/1	Static		
<input type="checkbox"/>	000e.c6cc.b7bc	Gi0/1	Static		
<input type="checkbox"/>	001a.a92a.3424	Gi0/1	Static		

Configuration description:

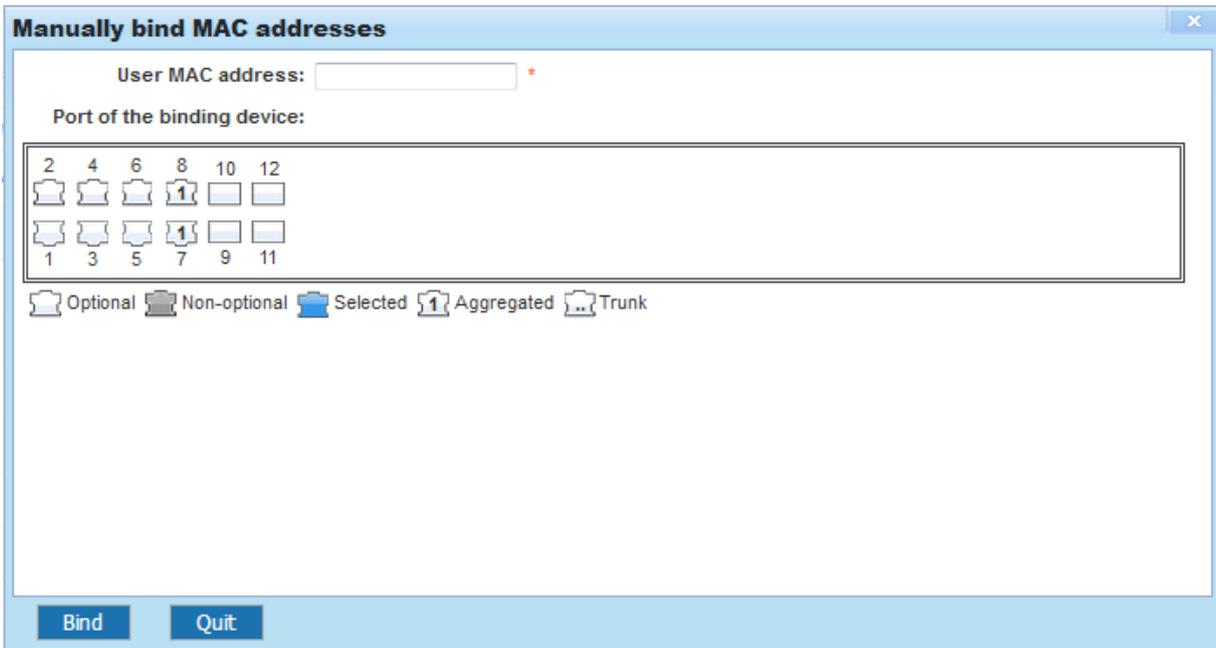
The MAC address list contains the static MAC address list and dynamic MAC address list. Select **All**, **Static**, or **Dynamic** from the **MAC address list** drop-down list to display the required MAC address list.

Setting a static MAC address:

Binding a single MAC address: Click the bind icon in the **Operation** column of the MAC address list to bind a single dynamic MAC address as a static MAC address. After binding, the bind icon is changed to the delete icon. Batch binding of MAC addresses: Select the check boxes in front of entries and choose **Dynamic >> static MAC address** in the lower left corner of the list to complete batch processing.

Manually binding MAC addresses: Click **Manually bind MAC addresses**. The **Manually bind MAC addresses** dialog box is displayed. Enter a MAC address, select the port of the device to be bound, and click **Bind** to complete the binding operation.

Figure 1-25 Manually Binding MAC Addresses



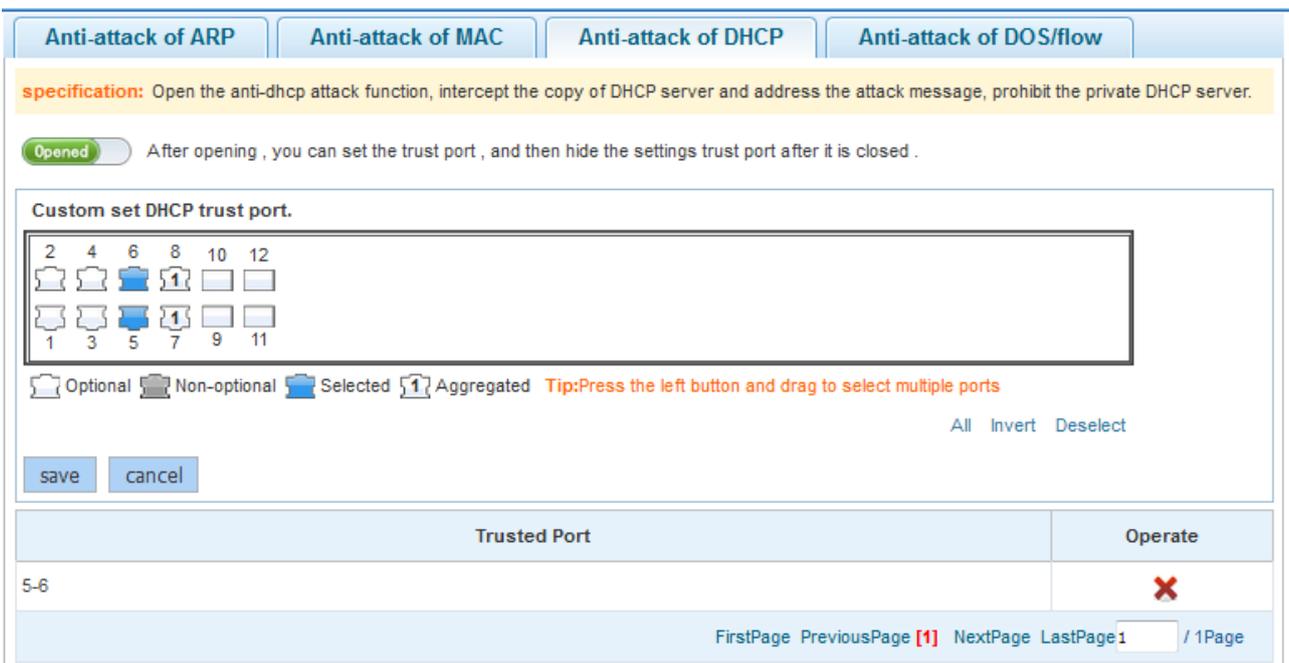
Deleting a single MAC address: Click the delete icon in the **Operation** list of the MAC address list to delete a single static MAC address.

Deleting MAC addresses in batches: Select the check boxes in front of static MAC address entries and click **Delete the static MAC address** in the lower left corner to complete batch processing.

! When you choose **Dynamic >> static MAC Address** or choose **Delete the static MAC address** to perform batch processing, the selected MAC addresses must be of the same type.

- Anti-attack of DHCP

Figure 1-26 Anti-attack of DHCP



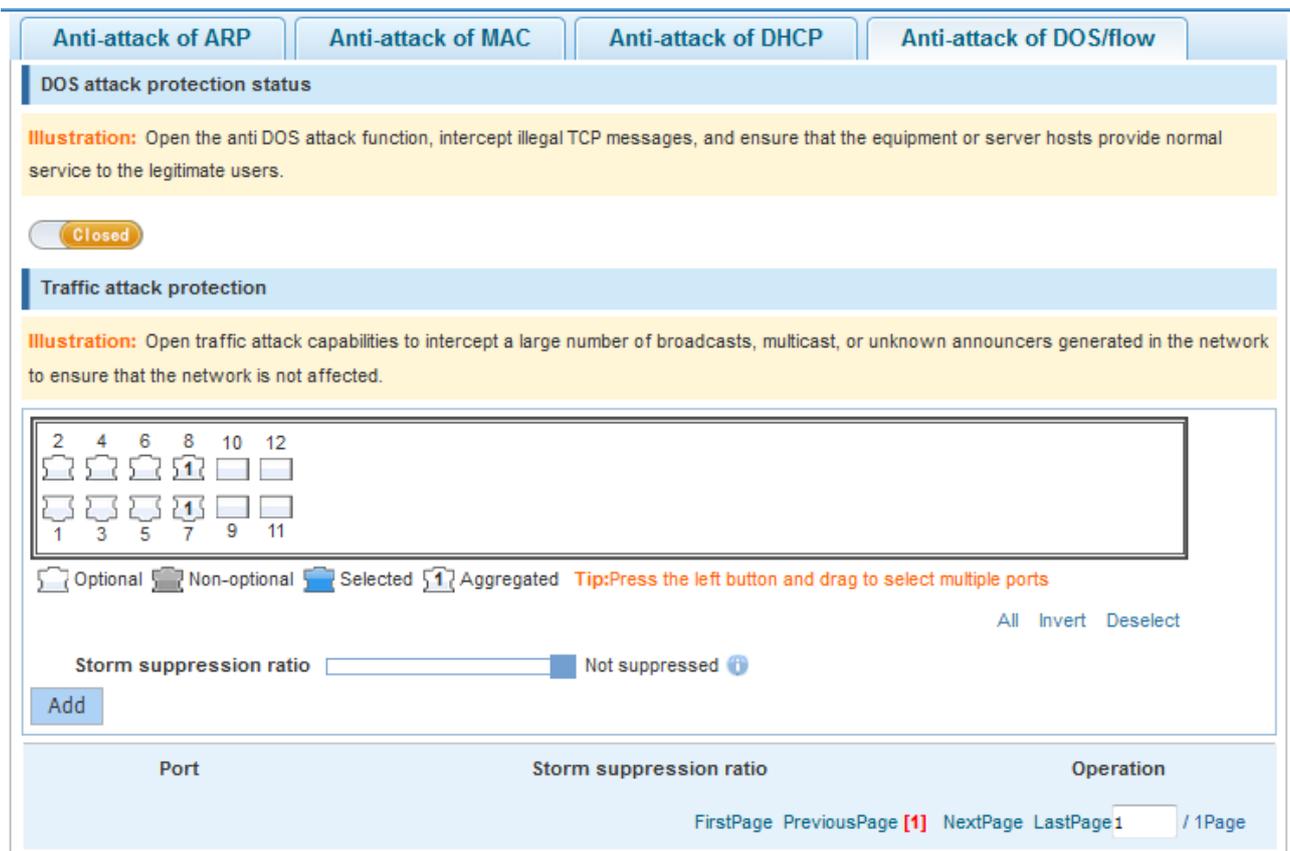
Configuration description:

A port connected to the Dynamic Host Configuration Protocol (DHCP) server needs to be configured as a DHCP trusted port. The DHCP server connected to a non-trusted port cannot work properly. A selected port on the panel indicates that the port is configured as a DHCP trusted port. You can select a port on the panel and click **save**. To delete a DHCP trusted port, select the delete icon in the **Operate** column of the port. A message is displayed, asking you whether to delete the DHCP trusted port. Click **Yes** to delete the DHCP trusted port.

 The panel displays DHCP trusted ports and is always editable. If you modify a port and want to discard the modification, click **cancel** to restore currently enabled DHCP trusted ports on the panel.

- Anti-attack of Dos/flow

Figure 1-27 Anti-attack of DOS/Flow



Configuration description:

DOS attack protection status: Click the status switch to enable or disable the Denial of Service (DoS) attack protection function.

Traffic attack protection: Select a required port and set **Storm suppression ratio** to suppress broadcast, multicast, and unknown unicast packets to prevent traffic depletion caused by broadcast storms.

1.10.2 Path Detection

Choose **Fault/Security > Path detection** access the **Path detection** page. The **Path detection** page contains the **Ping**, **Tracert**, and **Cable Detection** tab pages.

- Ping

Figure 1-28 Ping

Ping Tracert Cable Detection

Instructions: Use the ping function to detect whether the network connection and the host are accessible.

Destination IP: *

Timeout(1-10):

Repeat time(1-100):

Starting test

Test results:

Sending 5, 100-byte ICMP Echoes to 192.168.1.101, timeout is 2 seconds:
< press Ctrl+C to break >

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms

Configuration description:

Enter the destination IP address and other information and click **Starting test**. Detection results are displayed in the **Test results** area after a period of time.

- Tracert

Figure 1-29 Tracert

Ping **Tracert** Cable Detection

Instructions: Tracert detection can detect the gateway to the destination, the function is used for detecting whether the destination can reach and the path to the destination, if the destination unreachable, diagnose the problem.

Destination IP: *

Timeout(1-10):

Starting test

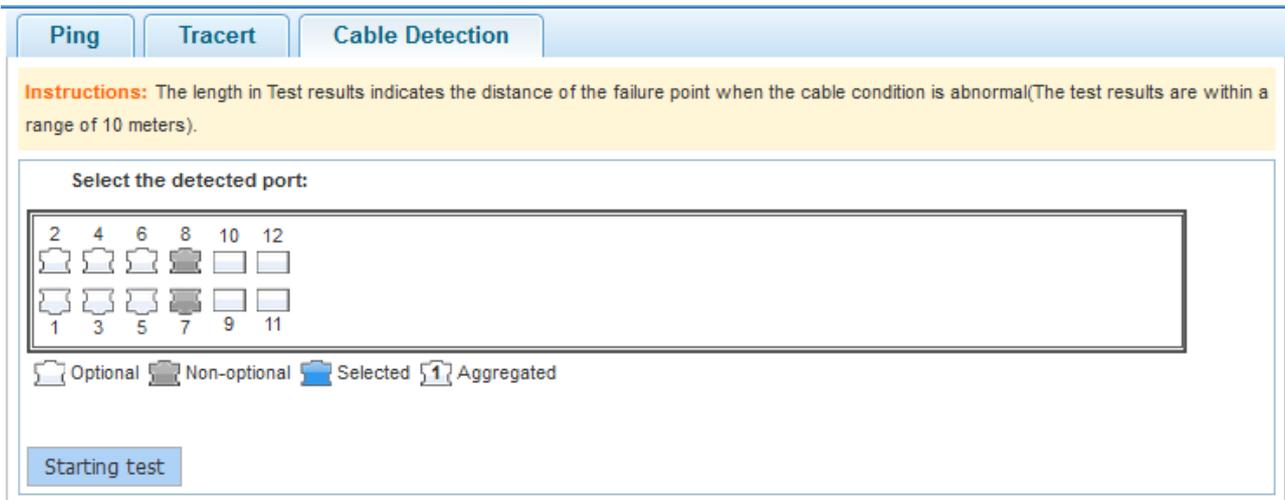
Test results:

Configuration description:

Enter the destination IP address and other information, and then click **Starting test**. Detection results are displayed in the **Test results** area after a period of time.

- Cable Detection

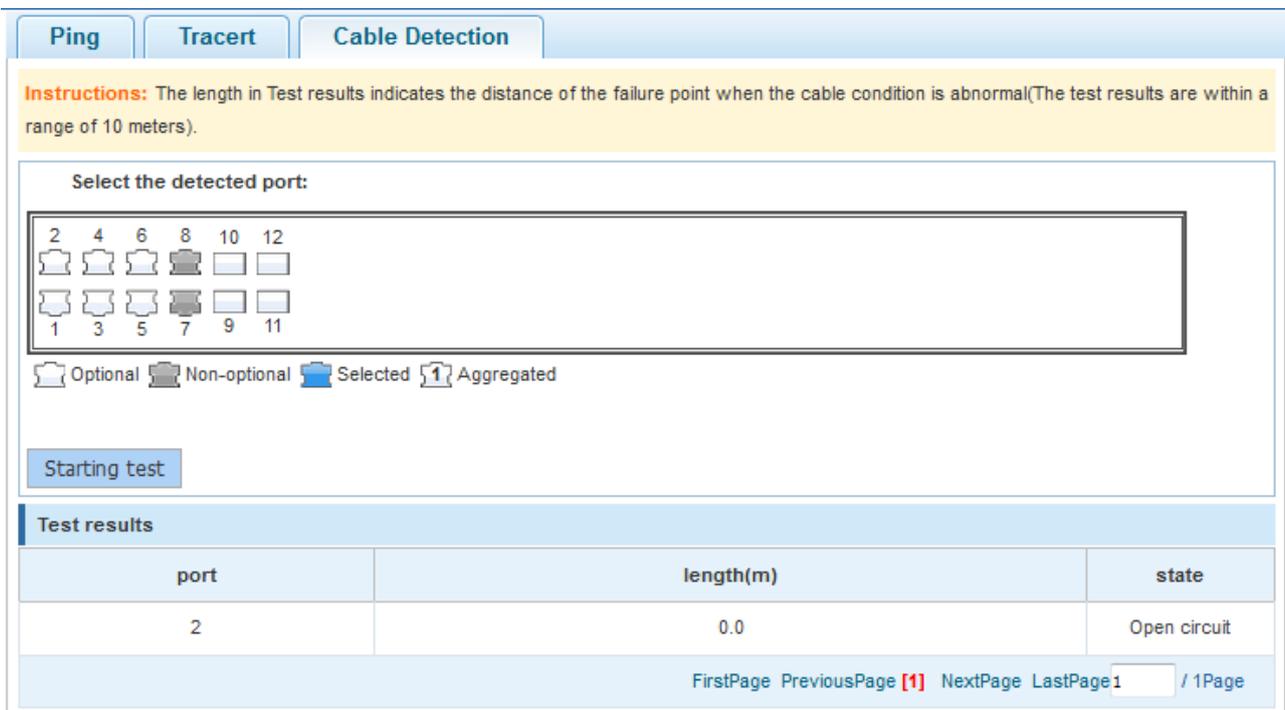
Figure 1-30 Cable Detection



Configuration description:

Select a required port on the panel and then click **Starting test**. Detection results are displayed in the **Test results** area after a period of time.

Figure 1-31 Cable Detection



1.10.3 ACL

Choose **Fault/Security > ACL** to access the **ACL** page.

- ACL effective time

Figure 1-32 ACL Effective Time

ACL effective time
Access Control List
Apply ACL

Instructions: Time object is used to define the policy effective time.

New object Select existing objects

New object name: *

Choose week:
 Monday
 Tuesday
 Wednesday
 Thursday
 Friday
 Saturday
 Sunday

Period of time: - +

Save

Time object list: ▼

Week of time	Period of time	Operation
⊖ Delete object	FirstPage PreviousPage [1] NextPage LastPage <input type="text" value="1"/> / 1Page	

Configuration description:

Adding ACL effective time: Click **New object**, enter a new object name, select a day of a week, set the time range, and then click **Save**.

Editing ACL effective time: Click the edit icon in the **Operation** column of the list to modify parameters about the ACL time object.

Deleting ACL effective time: Select an ACL time range in the list and click the delete icon.

Deleting a time object: Click **Delete object** to delete a created time object.”

- Access Control List

Figure 1-33 Access Control List

ACL effective time
Access Control List
Apply ACL

Instructions: Access Control List(ACL), By configuring a series of matching rules, allowing or prohibiting traffic for the specified data stream(e.g. defined source IP address, port number, etc.)to filter through the network interface data.

Attention: ACL rules are sequential, and the rules in the front match first.If the policy entry is too many, the operation time will be relatively long.

Wildcard: The wildcard mask specifies which bits of the IP address should be ignored when an IP address is compared to another IP address.The '1' in the wildcard mask means to ignore the digit in the IP address, and '0' means that it has to be preserved. If the wildcard mask is not configured, 0.0.0.0 will be considered the default mask.

New ACL
New ACL access control rules
Create an antivirus ACL

Select ACL access control list List of rules

Action	Protocol	Source IP/ wildcard mask	Source port	Destination IP/ wildcard mask	Destination port	Effective Time Object	Status	Order of rules	Operation

Delete ACL

Configuration description:

Creating an ACL: Click **New ACL** and set parameters to create an ACL object.

Creating an antivirus ACL: Click **Create an antivirus ACL** to add an antivirus ACL object and set rules.

Deleting an ACL object: Click **Delete ACL** to delete a created ACL object.

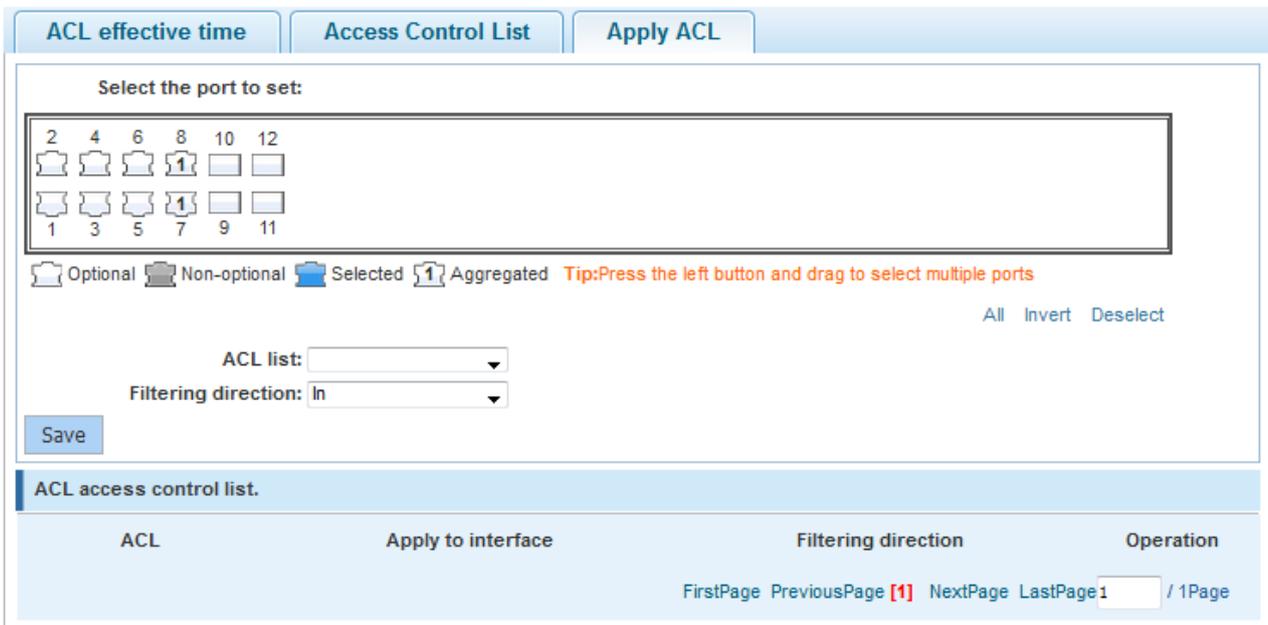
Adding an ACE: In an ACL object, enter specific information to add an ACE.

Editing an ACE: In an ACL object, click the edit icon to modify the ACE for the ACL object.

Deleting an ACE: In an ACL object, click the delete icon to delete an ACE.

- Apply ACL

Figure 1-34 Apply ACL



Configuration description:

Adding an ACL application: Specify a port, select an ACL list and the filtering direction to add an ACL application.

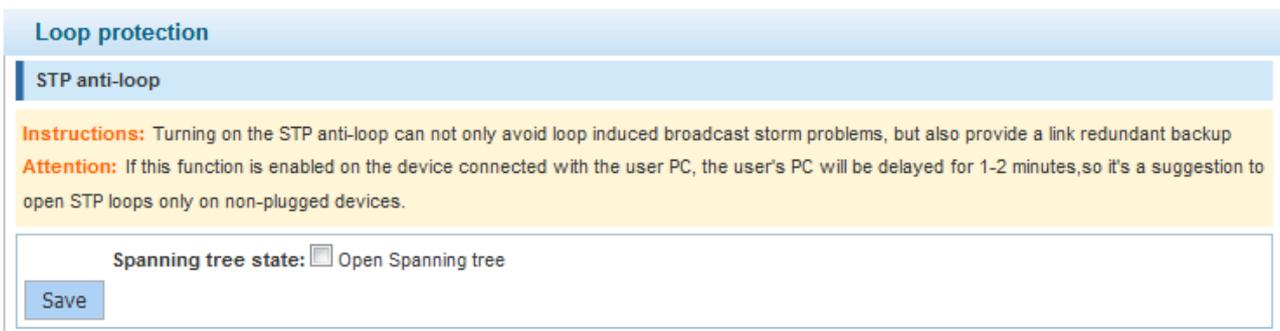
Editing an ACL application: Click the edit icon, specify another port, select the ACL list and filtering direction to modify the ACL application.

Deleting an ACL application: Click the delete icon to delete an ACL application.

1.10.4 Loop Protection

Choose **Fault/Security > Loop protection** to access the **Loop protection** page.

Figure 1-35 Loop Protection



Configuration description:

Enabling the STP anti-loop can prevent broadcast storms caused by loops and provide link redundancy backup.

1.10.5 RLDP Settings

Choose **Fault/Security > RLDP setting** to access the **RLDP setting** page.

Figure 1-36 RLDP Setting

RLDP setting

Instructions: Only the global RLDP opened, and the port RLDP will run.

RLDP state: Opened

Detection interval: *

Number of detection: *

Save

Port RLDP setting

Instructions: 1.Port open loop detection can avoid the broadcast storm problem caused by loop. It is recommended to open the RLDP loop check on the port that the Access devices connect to the user's PC
 2.The two ports corresponding to the single/double directional link detection should open RLDP configure.It is recommended to set up the link between devices.
Attention: The troubleshooting method on the port is 'close the port'.

Custom setup RLDP anti-loop port:

2	4	6	8	10	12
<input type="checkbox"/>					
1	3	5	7	9	11
<input type="checkbox"/>					

Optional
 Non-optional
 Selected
 Aggregated
 Tip:Press the left button and drag to select multiple ports

All Invert Deselect

Test type: Unidirectional Link D ▼

Save

Port	Test type	Operation
Gi0/12	Unidirectional Link Detection	<input type="checkbox"/> <input checked="" type="checkbox"/>

Configuration description:

The Rapid Link Detection Protocol (RLDP) function can be enabled on a port only after the global RLDP is enabled. Loop detection enabled on a port can prevent broadcast storms caused by loops. It is recommended to enable the RLDP function on the port of an access device connected to user clients. RLDP should be enabled on both ports for unidirectional and bidirectional link detection, and is recommended to be configured on the links between devices.

1.11 System Management

1.11.1 System Settings

Choose **System management > System settings** to access the **System settings** page. The **System settings** page contains the **System Settings**, **Restart**, **Password**, and **System Log** tab pages.

- System Settings

Figure 1-37 System Settings

System Settings	Restart	Password	System Log
System basic information settings			
Manage VLAN: 1	Device MAC: 141414141414	Device name: Ruijie	
Manage IP: 192.168.1.1 *	Device location:	Contact person:	Contact Info:
Mask: 255.255.255.0 *			
Default gateway:			
DNS server:			
Login timeout(m): 30			
Save			
System time			
Current time: 1970-1-1 1:49:54			
Reset time:			
Time zone: UTC+8(Beijing, CCT)			
<input type="checkbox"/> Automatic time server synchronization			
<input type="checkbox"/> Automatic synchronization with Internet time server			
Save			

Configuration description:

System basic information settings: Enter basic information. If incorrect information is entered, an alert is provided behind the input box. The management VLAN is VLAN 1 by default. After a different management VLAN is selected, the management IP address and mask are updated accordingly. Input boxes marked with an asterisk (*) are mandatory. The device name, device location, contact person, and contact information are displayed on the system login page. Enter information in the correct format and click **Save**. A setting success message is displayed, indicating configuration completion. If the management IP address is changed, the system displays a message, asking you whether to modify system settings. After successful modification, the system redirects to the system login page.

System time: The current system time is displayed. You can manually reset the current system time or select **Automatic time server synchronization** to adjust the system time. The server address can be set to a specified NTP server or you can select the default **Automatic synchronization with Internet time server**. Click **Save**. A time configuration success message is displayed, indicating configuration completion.

 The changed management IP address must be reachable so that you can log in to the Web management platform again.

- Restart

Figure 1-38 Restart

Configuration description: Click **Restart device immediately**. A message is displayed, asking you whether to restart the switch. Click **Yes** to restart the device. The device restart takes several minutes. Please wait patiently. The page is automatically refreshed after the device is restarted.

- Password

Figure 1-39 Password

Modify the super user password

Note: 1. If you set a new Web login password, then log in again after setting the new password. 2. Password can not contain Chinese, full-width characters, question marks and spaces.

Old password: *

New password: *

Confirm new password: *

Modify telnet login password

Telnet service: Opened

New password: *

Confirm new password: *

Modify enable password

Illustration: The Enable password refers to the password that the user enters the privileged mode Exec configuration layer by means of Cli.

New password: *

Confirm new password: *

Configuration description:

Modify the super user password: To modify a super user password, you are required to enter the old password and enter and confirm the new password. If an incorrect old password is entered, a message is displayed in red font, indicating that the old password incorrect. You are required to enter a correct old password and click **Save** to complete the password change. You can click **Clear** to clear the passwords entered in the input boxes.

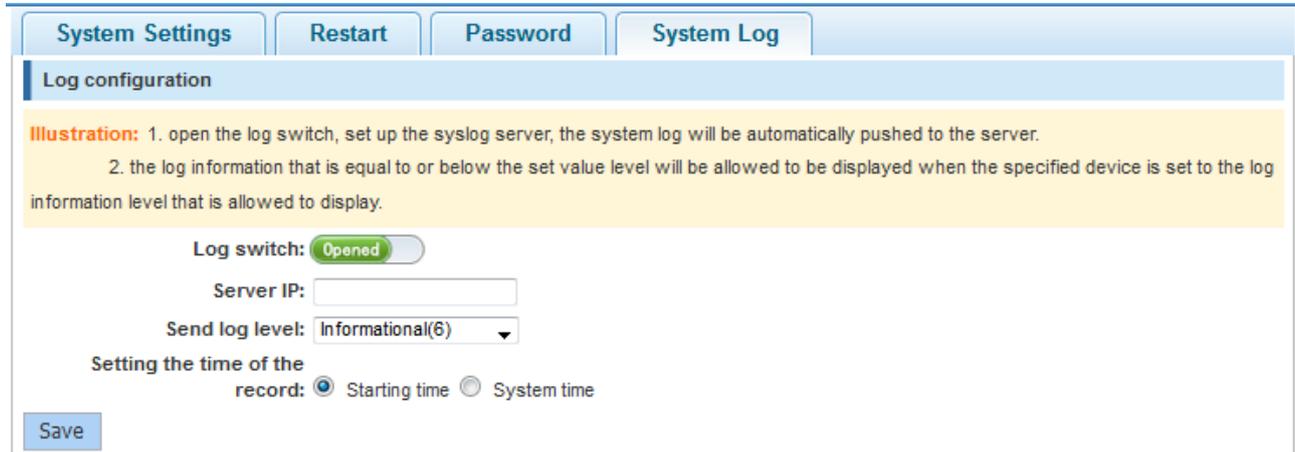
Modify telnet login password: To modify a telnet login password, enter and confirm a new password. Other operations are the same as those in the modification of the super user password.

Modify enable password: To modify an enable password, enter and confirm a new password. Other operations are the same as those in the modification of the super user password.

 After the super user password is changed, the system redirects to the login page, on which you are required to log in again.

- System Log

Figure 1-40 System Log



Configuration description:

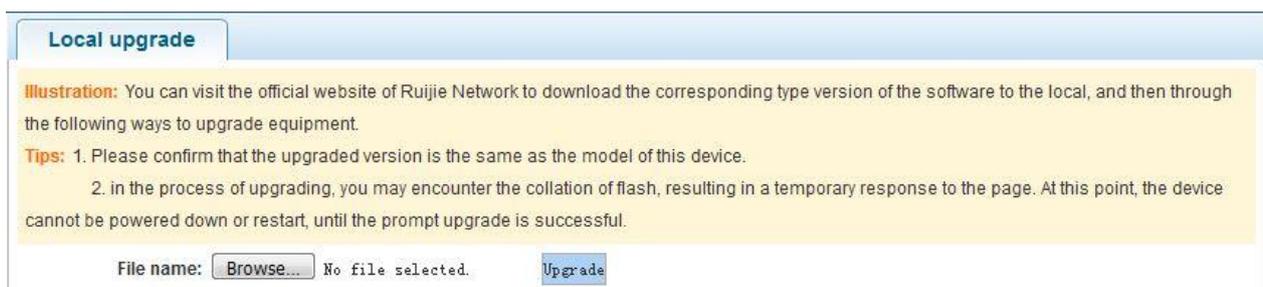
Set **Server IP** and **Send log level**. After setting, the device sends system logs to the corresponding server.

1.11.2 Upgrade

Choose **System management > Upgrade** to access the **Upgrade** page. The **Upgrade** page contains the **Local upgrade** tab page.

- Local upgrade

Figure 1-41 Local Upgrade



Configuration description:

Click **Browse**, select a file stored locally, and then click **Upgrade** to perform the local upgrade operation.

1.11.3 Configuration

Choose **System management > Configuration** to access the **Configuration** page. The **Configuration** page contains the **Current configuration**, **Configure a backup**, and **Restore the factory configuration** tab pages.

- Current configuration

Figure 1-42 Current Configuration

Figure 1-44 Import Configuration

Current configuration
Configure a backup
Restore the factory configuration

View the current configuration
Export Configuration

Backup Import configuration

You cant close or refresh the page during the import, otherwise the import will fail!

Note: After importing the new configuration, please [reboot the device](#) on this page to enable the configuration. Otherwise the configuration is not effective.

Backup Filename: No file selected.

Backup file list

File name	File size	Modification time
config_111.text	1.39K	1970-01-01 02:09:55
config_222.text	1.39K	1970-01-01 02:10:00

- Configure a backup

Figure 1-45 Configuration File Backup

Current configuration
Configure a backup
Restore the factory configuration

Illustration: Click the file name to view the content of the configuration file, and save up to 5 backup files.

Name	Size	Modification time
<input checked="" type="radio"/> config_111.text	1.39K	1970-01-01 02:09:55
<input type="radio"/> config_222.text	1.39K	1970-01-01 02:10:00

Restore the backup. Delete backup Save as backup Rename backup

Configuration description:

Backup file list: Select a file, click **Restore the backup**, **Delete backup**, **Save as backup**, or **Rename backup** as required, and then click **Determine recovery** to complete the operation on the file.

The file content is displayed after you click a file name. A maximum of five backup files can be stored.

- Restore the factory configuration

Figure 1-46 Restoring the Factory Configuration

Current configuration
Configure a backup
Restore the factory configuration

Note: After the device is reset to the factory default settings, all configurations will be removed. Please export current configuration before resetting the device. Export the current configuration

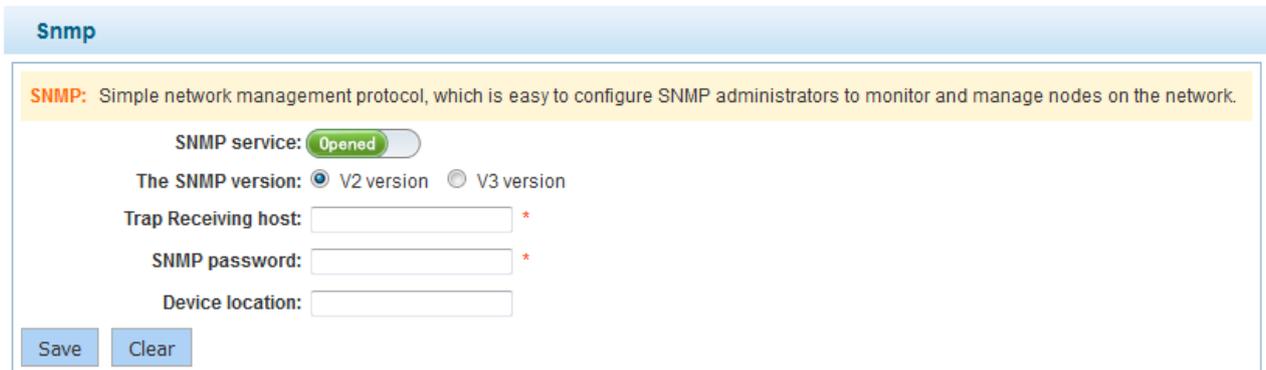
Export the current configuration
Restore the factory configuration

Configuration description: Click **Export the current configuration**. The **Save As** dialog box is displayed, in which you can select the file storage path, enter the file name, and click **Save** to export the current configuration. Click **Restore the factory configuration**. The message "Do you want to delete all the configurations? This action may cause no access to the web page!" is displayed. The factory configuration is restored only after you confirm the operation.

1.11.4 SNMP

Choose **System management > SNMP** to access the **SNMP** page.

Figure 1-47 SNMP



Sntp

SNMP: Simple network management protocol, which is easy to configure SNMP administrators to monitor and manage nodes on the network.

SNMP service: Opened

The SNMP version: V2 version V3 version

Trap Receiving host: *

SNMP password: *

Device location:

Save Clear

Configuration description:

The SNMP allows SNMP administrators to easily monitor and manage network nodes.

You can enable/disable the SNMP service, set **The SNMP version**, **Device location**, **Trap Receiving host**, and **SNMP password**.

1.11.5 Permissions

Choose **System management > Permissions** to access the **Permissions** page.

Figure 1-48 Permissions

Permissions

Instruction: This page can be accessed only by the super administrator admin, which is used to add / manage users and visitors. Users can log in to the Web management system for daily maintenance of the device. In addition to the two default outdoors for admin and guest, a maximum of 5 users can be added.

Username: *

Password: *

Retype password *

Authorization page + [Edit empowerment page](#)

User list

username	operation
admin	
guest	

[FirstPage](#) [PreviousPage \[1\]](#) [NextPage](#) [LastPage1](#) / 1Page

Configuration description:

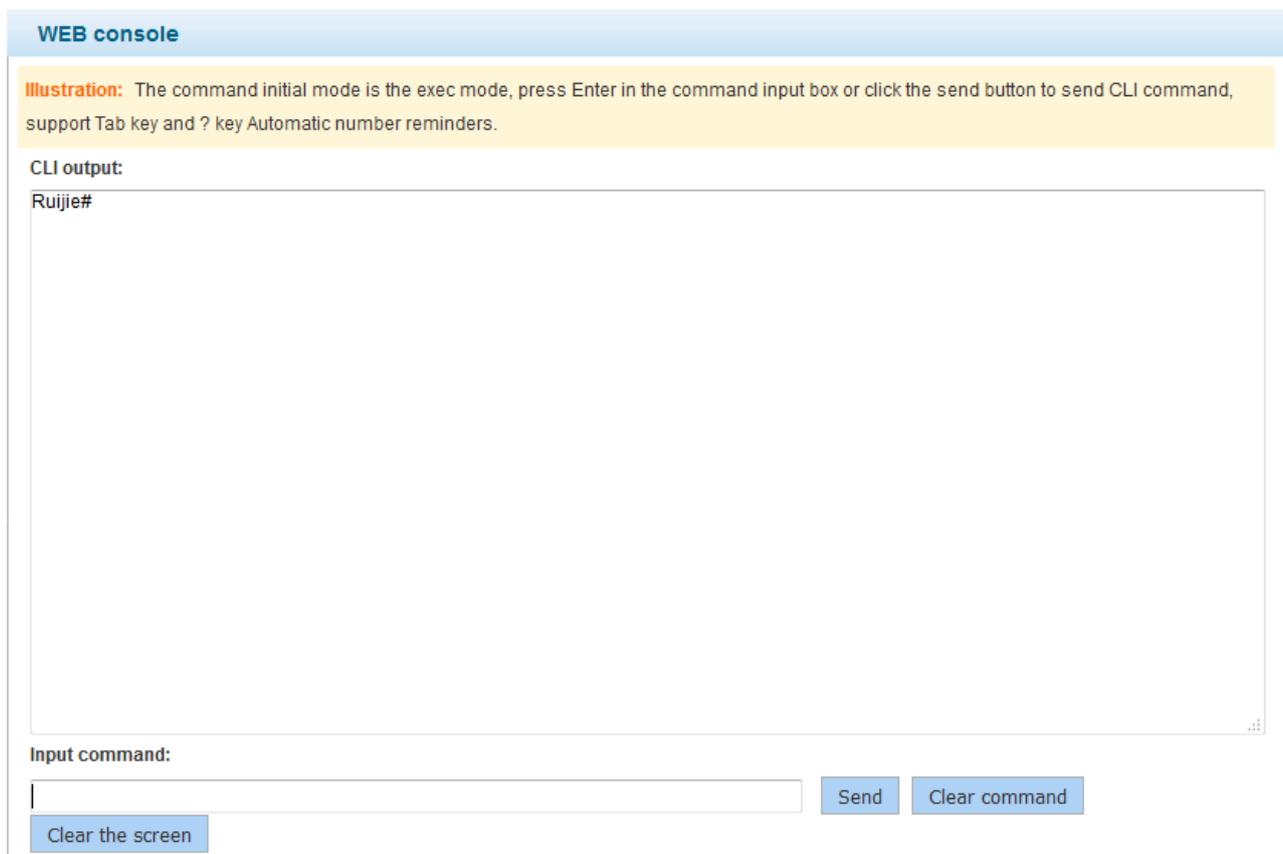
Adding a user: Enter the username and password, and set **Authorization page** (this parameter is set to all pages by default), and click **add users**. The adding success message is displayed and all users are displayed in the user list.

 There are two default users: super administrator (**admin**) and guest (**guest**). The super administrator can modify the permissions of other administrators and the guest can only access the home page by default. Defaults users cannot be deleted.

1.11.6 WEB Console

Choose **System management > WEB console** to access the **Web console** page.

Figure 1-49 WEB Console



Configuration description: Enter a CLI command in the command box, press **Ctrl+Enter** or click **Send** to send the CLI command. When entering a command, you can press **Tab** or enter **?** to obtain the command list and command description. Click **Clear command** to clear the content in the command box or click **Clear the screen** to clear the returned CLI results.

1.12 Typical Configuration Examples

Configuration Key Points

The Web service is enabled on switches before delivery. You can access the IP address 192.168.1.1 to log in to the Web management platform to manage the device. The following describes how to enable the Web service on the CLI.

Configuration Steps

To log in to the Web management platform, enable the Web service, configure an IP address, and run the **webmaster** command to configure the account and password. Then, you can access the Web management platform to complete the Web configuration.

The detailed configuration is as follows:

Enter the configuration mode.

```
Nodexon#configure
```

Enter configuration commands, one per line. End with CNTL/Z.

Enable the Web service.

```
Nodexon(config)#enable service web-server
```

Configure a local username and password. In the command below, **level** indicates the user

```
priority. Nodexon(config)# webmaster level 0 username admin password admin
```

Configure the device management IP address. The management VLAN is VLAN 1 by default. Configure the IP address for VLAN 1 and ensure that you can ping the management IP address successfully.

```
Nodexon(config)#interface vlan 1
Nodexon(config-if-VLAN 1)#ip address 192.168.1.1 255.255.255.0
```

 This command configures the username and password for Web login authentication. You can use the **no** form of this command to restore the default configurations or delete the user-defined configurations.

```
webmaster level privilege-level username name password { password | [ 0 | 7 ] encrypted-password }
```

no webmaster level *privilege-level* [username *name*]

Parameter	Description
<i>privilege-level</i>	Indicates the permission level bound to a user. The system creates two accounts by default: admin and guest . The default permission level of user guest is 2, indicating that only the system home page can be accessed. The default permission level of user admin is 0, indicating that the user can use all functions, and is allowed to edit other management accounts, and authorize accessible pages for the management accounts. The permission level of a newly added account is 1.
<i>name</i>	Indicates the username.
<i>password</i>	Indicates the user password.
0 7	Indicates an encryption type of the password. 0 indicates no encryption and 7 indicates simple encryption.
<i>encrypted-password</i>	Indicates the password text.

Verification

```
Nodexon(config)#show running-
config Building configuration...
Current configuration : 6312 bytes

!
version NXOS 10.4(3b16) Release(82376) (Fri Nov 2 2012 -R03912)
13:55:16 hostname Nodexon
!
!
webmaster level 0 username admin password 7 08022b181b29 //Username and password for Web
management authentication. The password is displayed in encrypted manner.
```

```
webmaster level 2 username guest password 7 14155f083206
http update mode auto-detect
!
!
interface VLAN 1
 ip address 192.168.1.1 255.255.255.0 //Device management IP address
 no shutdown
!
line con 0
line vty 0 4
 login
!
!
End
```