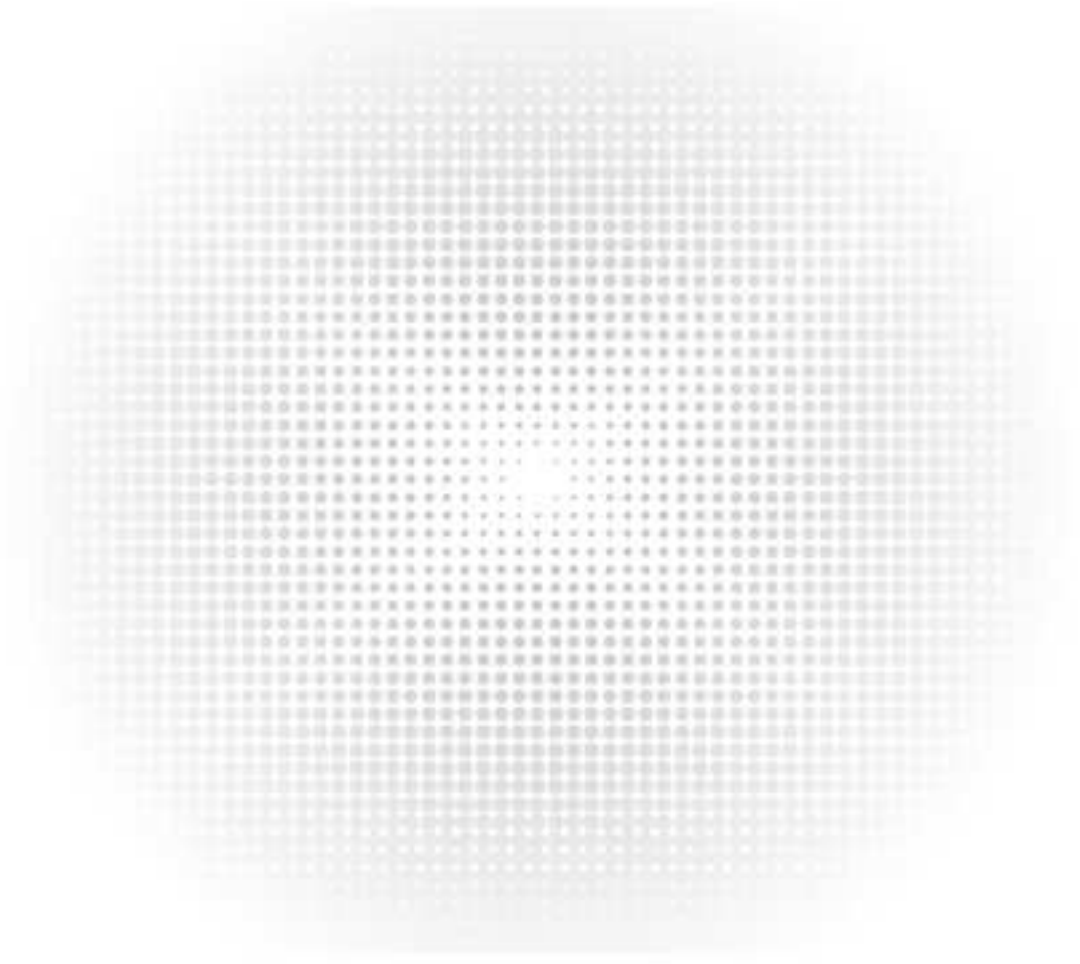
S3150-8T2F Switch Web-based Configuration Guide

Models: S3150-8T2F



Configuration Guide

Contents

Chapter 1 Configuration Preparation

1.1 HTTP Configuration

Switch configuration can be conducted not only through command lines and SNMP but also through Web browser. The switches support the HTTP configuration, the administrator can finish the configuration and so on.

1.1.1 Choosing the Prompt Language

Up-to-now switches support two languages, that is, English and Chinese, and the two languages can be switched over through the following command.

Command	Purpose
[no] ip http language { english}	Sets the prompt language of Web configuration to English.

1.1.2 Setting the HTTP Port

Generally, the HTTP port is port 80 by default, and users can access a switch by entering the IP address directly; however, switches also support users to change the service port and after the service port is changed, you have to use the IP address and the changed port to access switches. For example, if you set the IP address and the service port as 192.168.1.1 and 1234 respectively, the HTTP access address should be changed to http://192.168.1.1:1234. You'd better not use other common reserved ports (such as ftp 20, telnet 23, dns 53, snmp 161), and thus access collision should never happen. Because the ports used by a lot of protocols are not remembered, you'd better use port IDs bellow ring port 1024.

Command	Purpose
ip http port { portNumber}	Setting the HTTP Port

1.1.3 Enabling the HTTP service

Switches support to control the HTTP access. Only when the HTTP service is established can HTTP exchange happen between switch and PC and, when the HTTP service is closed, HTTP exchange stops.

Command	Purpose
ip http server	Enabling the HTTP service

1.1.4 Setting the HTTP Access Mode

You can access a switch through two access modes: HTTP access and HTTPS access, and you can use the following command to set the access mode to HTTP.

Command	Purpose
ip http http access-class	Setting the HTTP Access Mode

1.1.5 Setting the maximum number of VLAN entries displayed on a web page

A switch supports at most 4094 VLANs and in most cases Web only displays parts of VLANs, that is, those VLANs users want to see. You can use the following command to set the maximum number of VLANs. The default maximum number of VLANs is 100.

Command	Purpose
ip http max-vlan-web {max-vlan}	Sets the maximum number of VLAN entries displayed on a web page.

1.1.6 Setting the Maximum Number of Multicast Entries Displayed on a Web Page

A switch supports at most 1000 multicast entries. You can run the following command to set the maximum number of multicast entries on a Web then shows these multicast entries. The default maximum number of multicast entries is 15.

Command	Purpose
ip http web igmp group {igmp-group}	Sets the maximum number of multicast entries displayed on a web page.

1.2 HTTPS Configuration

In order to increase the security of communications, the switch not only supports the HTTP protocol but also the HTTPS protocol. HTTPS is a security-purposed HTTP channel and it is added to the SSL layer under HTTP.

1.2.1 Setting the HTTP Access Mode

You can run the following command to set the access mode to HTTPS.

Command	Purpose
ip http ssl access-class	Setting the HTTPS access mode

1.2.2 Setting the HTTPS Port

As the HTTP port, HTTPS has its default service port, port 443, and you also can run the following command to change its service port. It is recommended to use those ports following port 1024 so as to avoid collision with other protocols' ports following port 1024 so as to avoid collision with other protocols' ports.

Command	Purpose
snmp-server user /portNumber#	Sets the HTTPS port.

Chapter 2 Accessing the Switch through HTTP

2.1 Accessing the Switch through HTTP

When accessing the switch through Web, please make sure that the applied browser complies with the following requirements:

- IE(Microsoft Internet Explorer) version 6.0
- HTTP protocol version 1.1
- JavaScript™ software version 1.5

What's more, please ensure that the main program file running on a switch supports Web access and your computer has already connected the network on which the switch is located.

2.1.1 Initially Accessing the Switch

When the switch is initially used, you can use the Web access without any network settings.

1. Modify the IP address of the network adapter and subnet mask of your computer as 192.168.0.2 and 255.255.255.0 respectively.

2. Open the Web browser and enter 192.168.0.1 in the address bar. It is noted that 192.168.0.1 is the default management address of the switch.

3. If the Internet Explorer browser is used, you can see the dialog box as below. Both the original username and the password are "admin" which is case sensitive.

4. After successful authentication, the system basic information about the switch will appear on the IE browser.

2.1.2 Upgrading to the Web Supported Version

If your switch is upgraded to the Web supported version during its operation and the switch has already stored its configuration files, the Web visit cannot be directly applied on the switch. Perform the following steps one by one to enable the Web visit on the switch:

1. Connect the console port of the switch with the accessory cable, or connect to the management address of the switch through the computer.

2. Enter the global configuration mode of the switch through the command line, the DOS prompt shown on it is similar to "Switch (config)".

3. If the management address of the switch is not configured, please create the VLAN interface and configure the IP address.

4. Enter the command ip http server to enable Web service.

5. Enter the username to set the user name and password of the switch. For how to use this command, refer to the "Security Configuration" section in the user manual. After the above mentioned steps are performed, you can enter the address of the switch in the Web browser to access the switch.

6. Enter the command write, to save the current configuration to the configuration file.

2.2 Accessing a Switch through Secure Links

The data between the WEB browser and the switch will not be encrypted if you access a switch through common HTTP. To encrypt these data, you can use the secure links, which are based on the secure sockets layer, to manage the switch.

To do this, you should follow the following steps:

1. Connect the console port of the switch with the accessory cable, or connect to the management address of the switch through the computer.

2. Enter the global configuration mode of the switch through the command line, the DOS prompt shown on it is similar to "Switch (config)".

3. If the management address of the switch is not configured, please create the VLAN interface and configure the IP address.

4. Enter the command ip http server to enable Web service.

5. Enter the username to set the user name and password of the switch. For how to use this command, refer to the "Security Configuration" section in the user manual.

6. Run ip http authentication command to configure the secure link access of the switch.

7. Run no ip http http access class to access the switch through secure links.

8. Enter the command write, to save the current configuration to the configuration file.

9. Open the WEB browser on the PC that the switch connects, enter https://192.168.0.1 on the address bar; 192.168.0.1 stands for the management IP address of the switch's VLAN address of the switch, and then press the Enter key. Then the switch can be accessed through the secure links.

2.3 Introduction of Web Interface

The console Web homepage consists of the top control bar, the navigation bar, the configuration area and the bottom control bar.

2.3.1 Top Control Bar

Save all	Write the current settings in the configuration file of the device. It is equivalent to the execution of the "write" command. The configuration that is made through Web will not be promptly written to the configuration file after validation. If you click "Save All", the unsaved configuration will be lost after reboot ing.
English	The interface will turn into the English version.
Chinese	The interface will turn into the Chinese version.
Logout	Exit from the current login state. After you click "logout", you have to enter the username and the password again if you want to continue the Web configuration.
Interface panel	Displays the figure of interface panel
About	Displays the manufacturer information and sets auto refresh.

After you configure the device, the result of the previous step will appear on the left side of the top control bar. If error occurs, please check your configuration and retry it later.

2.3.2 Navigation Bar

The contents shown in the navigation bar. The commands in the navigation bar are shown in a form of list and are classified according to types. By default, the list is located at "Runtime.htm". If a certain item need be configured, please click the group name and then the sub-item. For example, to browse the flux of the current port, you have to click "Interface State" and then "Interface Flow".

Notes:

The limited user can only browse the state of the device and cannot modify the configuration of the device. If you log on to the Web as a limited user, a prompt "Only 'Interface State' will appear.

2.3.3 Configuration Area

The configuration directory area shows the route and configuration of the device. The contents of this area can be modified by the clicking of the icons in the navigation bar.

2.3.4 Configuration Area

The configuration area is to show the contents that is selected in the navigation area. The configuration area always contains one or more buttons and their functions are listed in the following table:

Refresh	Refresh the content shown in the current configuration area.
Apply	Apply the modified configuration on the device. The application of the configuration does not mean that the configuration is saved in the configuration file. To save the configuration, you have to click 'Save All' on the top control bar.
Reset	Warning: canceling the modification of the sheet. The content of the sheet will be reverted.
New	Creates a list item. For example, you can create a VLAN item on a new user.
Delete	Deletes an item in the list.
Back	Go back to the previous level configuration page.

Chapter 3 Basic Configuration

3.1 Hostname Configuration

If you click Basic Config > Hostname in the navigation bar, the Hostname Configuration page appears, as shown in the following figure.

The hostname will be displayed in the login dialog box.

The default name of the device is "Switch". You can enter the new hostname in the text box shown in figure 3 and then click "Apply".

3.2 Time Management

If you click System Mgr. > Time Setting, the Time Setting page appears.

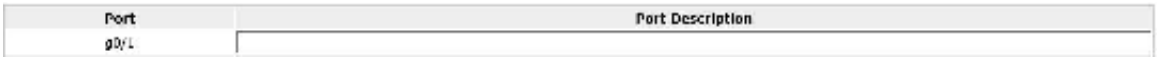
To refresh the clock of the directly connected device, click "Refresh".

In the "Select Time Zone" dropdown box, select the time zone where the device is located. When you select "Set Time Manually", you can set the time of the device manually. When you select "Network Time Synchronization", you can designate 3 SNTP servers for the device and set the interval of time synchronization.

Chapter 4 Configuration of the Physical Interface

4.1 Configuring Port Description

If you click Port Config > Port Description in the navigation bar, the Port Description Configuration page appears, as shown in the following figure.



You can modify the port description on this page and enter up to 20 characters. The description of the VLAN port cannot be set or modified.

4.2 Configuring the Attributes of the Port

If you click Port Config > Port Config > Port Attribute Config in the navigation bar, the Port Attribute Configuration page appears, as shown in the following figure.

You can change the status, speed, duplex mode, and flow control of a port on this page.

Notes:

1. After the speed or duplex mode of a port is modified, the link state of the port may be switched over and the previous communication may be impacted.

4.3 Rate Limit

If you click Port Config > Rate Limit in the navigation bar, the Port rate limit page appears, as shown in figure 4.

On this page you can set the receive speed and transmission speed of a port. By default, all ports have no speed limited. The reception speed and transmission speed are configured by a percentage or by the designated unit of the switch.

4.4 Port Mirror

If you click Port Config > Port Mirror in the navigation bar, the Port Mirror Config page appears, as shown in the following figure.

Click the drop-down list on the right side of "Mirror Port" and select a port to be the destination port of the mirror.

Click a check box and select a source port of the mirror, that is, a mirrored port.

RX	The received packets will be mirrored to the destination port.
TX	The transmitted packets will be mirrored to a destination port.
RX & TX	The received and transmitted packets will be mirrored simultaneously.

4.5 Keepalive Detection

If you click Port Config > Keepalive Detection in the navigation bar, the Setting the port loopback detection page appears, as shown in Figure 6.

You can set the loopback detection cycle on the Loopback Detection page.

4.6 Port security

4.6.1 IP Binding Configuration

If you click Port Config > Port Security > IP Bind in the navigation bar, the Configure the IP Binding Info page appears, as shown in figure 7.

Interface Name	Detail
gi0/1	Detail

Click 'Detail' here, then you can conduct the binding of the source IP address for each physical port. In this way, the IP address that is allowed to visit the port will be limited.

	Serial number	Address	Operate
☐	1	192.168.0.2	Edit
☐	2	192.168.0.3	Edit

4.6.2 MAC Binding Configuration

If you click Port Config > Port Security > MAC Bind in the navigation bar, the Configure the MAC Binding Info page appears, as shown in figure 8.

Interface Name	Detail
gi0/1	Detail

Click 'Detail' here, then you can conduct the binding of the source MAC address for each physical port. In this way, the MAC address that is allowed to visit the port will be limited.

	Serial number	Address	Operate
☐	1	1234.1234.1234	Edit
☐	2	1234.1234.1235	Edit

4.6.3 Setting the Static MAC Filtration Mode

If you click Port Config > Port Security > Static MAC Filtration Mode in the navigation bar, the Configure the static MAC filtration mode page appears, as shown in figure 10.

Interface Name	Port Mode	Static MAC Filtration Mode
gi0/1	Access	Accept

On this page you can set the static MAC filtration mode. By default, the static MAC filter is disabled. Also, the static MAC filter mode cannot be set on ports in trunk mode.

4.6.4 Static MAC Filtration Entries

If you click Port Config > Port Security > Static MAC Filtration Entries in the navigation bar, the Setting the static MAC filtration entries page appears.

Interface Name	Detail
g0/1	Detail

If you click "Detail", you can conduct the binding of the source MAC address for each physical port. According to the configured port MAC filtration mode, the MAC address of a port can be limited, allowed or forbidden to visit.

	Serial number	Filtration Mode	MAC Address	Operation
☐	1	Disable	0001-0002-0003	Edit

4.6.5 Setting the Dynamic MAC Filtration Mode

If you click Port Config > Port Security > Dynamic MAC Filtration Mode in the navigation bar, the Configure the dynamic MAC filtration mode page appears, as shown in figure 1.5.

Interface Name	Dynamic MAC Filtration Mode	Max MAC Address
g0/1	Disable	1 (1-2048)

You can set the dynamic MAC filtration mode and the available maximum number of addresses on this page. By default, the dynamic MAC filtration mode is disabled and the maximum number of addresses is 1.

4.7 Storm Control

In the navigation bar, click Port Config > Storm Control. The system then enters the page on which the broadcast/multicast/unknown unicast storm control can be set.

4.7.1 Broadcast storm control

Port	Status	Threshold
g0/1	Enable	(1-65535) 64Kbps

Through the dropdown boxes in the Status column, you can decide whether to enable broadcast storm control on a port. In the Threshold column, you can enter the threshold of the broadcast packets. The legal threshold range for each port is given behind the threshold.

4.7.2 Multicast Storm Control

Port	Status	Threshold
g0/1	Enable	(1-65535) 64Kbps

Through the dropdown boxes in the Status column, you can decide whether to enable multicast storm control on a port. In the Threshold column, you can enter the threshold of the multicast packets. The legal threshold range for each port is given behind the threshold.

4.7.3 Unknown Unicast Storm Control

Through the "Status" drop-down box, you can decide whether to enable the unknown unicast storm limit on a port. In the Threshold column you can enter the threshold of the broadcast packets. The legal threshold range for each port is given behind the threshold.

4.8 Port Protect Group Configuration

If you click Port Config > Port Protect Group Config > Port Protect Group List in the navigation bar, the Port Protect Group List page appears.

4.8.1 Port Protect Group List

If you click Port Config > Port Protect Group Config > Port Protect Group List in the navigation bar, the Port Protect Group List page appears.

If you click New, a new port protect group will be created, as shown in the following figure.

If you tick a Port Protect Group, you can delete it. The port protect group 0 is by default which cannot be deleted.

4.8.2 Port Protect Group Interface Configuration

If you click Port Config > Port Protect Group Config > Port Protect Group Interface Config in the navigation bar, the Port Protect Group Config page appears.

The port protect group must be a created group. If one port has configured the default protect group, others ports can only configure the default groups.

Chapter 5 Layer-2 Configuration

5.1 VLAN Configuration

5.1.1 VLAN List

If you click Layer 2 Config > VLAN Config in the navigation bar, the VLAN Config page appears, as shown in figure 5.

The VLAN list will display VLAN items that exist in the current device according to the ascending order. In case of lots of items, you can look for the to-be-configured VLAN through the buttons like "Prev", "Next" and "Search".

You can click "New" to create a new VLAN.

You can also click "Edit" at the end of a VLAN item to modify the VLAN name and the port's attributes in the VLAN.

If you select the checkbox before a VLAN and then click "Delete", the selected VLAN will be deleted.

Notice:

By default, a VLAN list can display up to 20 VLAN items. If you want to configure more VLANs through Web, please log on to the switch through the Console port or Telnet, enter the global configuration mode and then run the "ip http web max-vlan

command to modify the maximum number of VLANs that will be displayed.

5.1.2 VLAN Configuration

Click the link "New" or "Edit" in the VLAN List to the VLAN configuration page as below, on which new VLANs can be created or the attributes of an existent VLAN can be modified.

To create a new VLAN, enter a VLAN ID and a VLAN name; the VLAN name can be omitted.

Through the port list, you can set the access port's default VLAN, the VLAN mode (Trunk or Access), whether to allow the entrance of current VLAN packets and whether to execute the untagging of the current VLAN when the port works as the egress port.

Notes:

When a port in Trunk mode serves as an egress port, it will untag the default VLAN by default.

5.2 GVRP Configuration

5.2.1 GVRP Global Attribute Configuration

Click L2 Config > GVRP Config > GVRP Global Config in the navigation bar to enter GVRP global attribute configuration page.

You can enable or disable the global GVRP and set dynamic vlan to take effect or not only in the registered ports.

5.2.2 GVRP Port Attribute Configuration

Click L2 Config > GVRP Config > GVRP Interface Config in the navigation bar and enter GVRP interface attribute configuration page.

Port	GVRP Status
g0/1	Enable

GVRP interface configuration is mainly to enable or disable GVRP protocol of the port.

5.3 STP Configuration

5.3.1 STP Status Information

If you click Advanced Config > STP Config in the navigation bar, the STP Config page appears, as shown in figure 10.

Root STP Config	
Spanning Tree Priority	4096
MAC Address	00E0.0FBE.7025
Hello Time	2
Max Age	20
Forward Delay	15
Local STP Config	
Protocol Type	RSTP
Spanning Tree Priority	32768
MAC Address	8479.733A.2013
Hello Time	2 (1-10)s
Max Age	20 (6-40)s
Forward Delay	15 (4-30)s
BPDU Terminal	Disable
Apply	Reset

The root STP configuration information and the STP ports status are only read.

Click the drop-down box on the right side of "Protocol" to change the currently running STP mode. The supported modes include STP, RSTP and Disabled STP.

The priority and the time need to be configured for different mode.

Notes

The change of the STP mode may lead to the interruption of the network.

5.3.2 Configuring the Attributes of the STP Port

If you click the "Configure RSTP Port" option, the "Configure RSTP Port" page appears.

The configuration of the attributes of the port is irrelevant to the global STP mode. For example, if the external status is set to "Disable" and the STP mode is then changed, the port will not join the active topology of the new mode.

The default value of the path cost of the port is 0, indicating the path cost is automatically calculated according to the speed of the port. If you want to change the path cost, please enter another value.

5.4 IGMP Snooping Configuration

5.4.1 IGMP Snooping Configuration

Click L2 Config > IGMP Snooping in the navigation bar and enter the IGMP Snooping Configuration page.

On this page you can set whether to make a switch forward unknown multicasts, whether to enable IGMP snooping, and whether to configure the switch as the querier of IGMP.

5.4.2 IGMP Snooping VLAN List

In the navigation bar click L2 Config > IGMP Snooping > IGMP Snooping VLAN List in the navigation bar and enter IGMP Snooping VLAN page.

If you click New, IGMP snooping VLAN configuration can be done. Through Web, up to 8 physical ports can be set on each IGMP snooping VLAN. If you click Cancel, a selected IGMP Snooping VLAN can be deleted. If you click Edit, you can modify the member port, running status and immediate leave of IGMP Snooping VLAN.

When create new IGMP Snooping Vlan, VLAN ID can be modified; when modify IGMP Snooping Vlan, VLAN ID cannot be modified.

You can add or delete the routing port by button "add" or "del".

5.4.3 Static Multicast Address

Click "Config > IGMP Snooping > Static Multicast Address" in the navigation bar, and enter static multicast address configuration page.

This page displays the static multicast group in current network according to IGMP Snooping statistics and the port set each member has congested. Click "Refresh" to refresh the contents in the list.

5.4.4 Multicast List

Click the Multicast List Info option on the top of the page and the Multicast List Info page appears.

On this page the multicast groups, which are existent in the current network and are in the statistics of IGMP snooping, is

well as port sets which members in each group belong to are displayed.

Click 'Refresh' to refresh the contents in the list.

Note:

By default, a multicast list can display up to 15 VLAN items. You can modify the number of multicast items by running ip http web igmp-groups after you log on to the device through the Console port or Telnet.

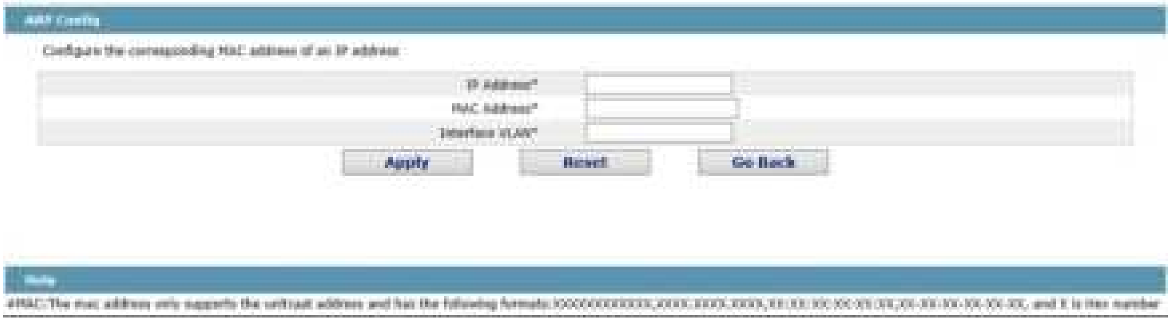
5.5 Setting Static ARP

Click L2 Config > Static ARP in the navigation bar and enter the basic ARP configuration page.

Click 'New' to add ARP entry. The VLAN interface needs to be assigned when configuring the ARP entry.

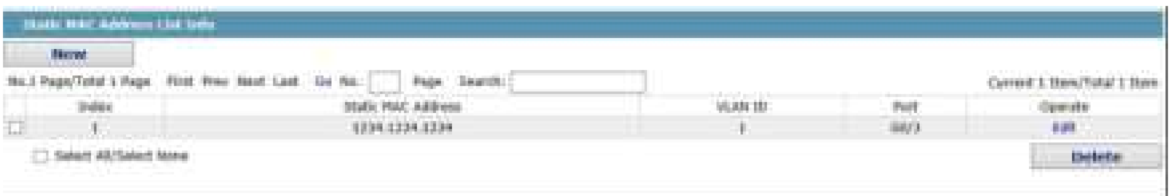
Click 'Modify' to modify the current ARP entry.

Click 'Delete' to delete the selected ARP entry.



5.6 Static MAC Configuration

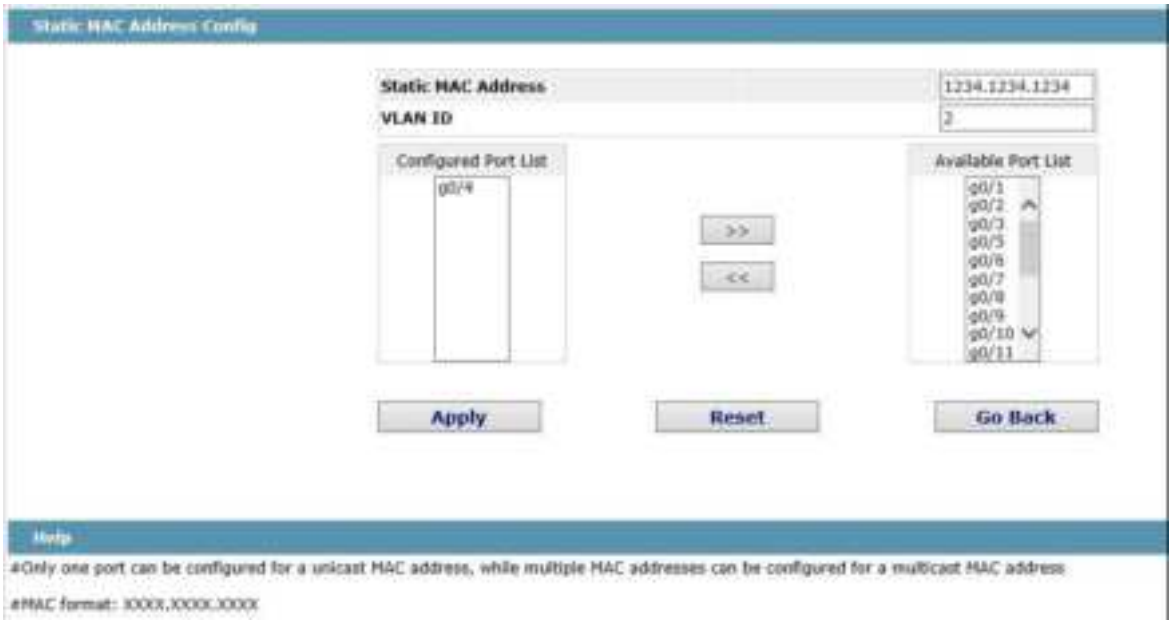
Click L2 Config > Static MAC Config in the navigation bar and enter static MAC address configuration page.



Click "New" to configure static MAC address and VLAN for the assigned port. The unicast MAC address can only be configured with one port and the multicast MAC address can be configured with multiple ports.

Click "Modify" to modify the configured static MAC address.

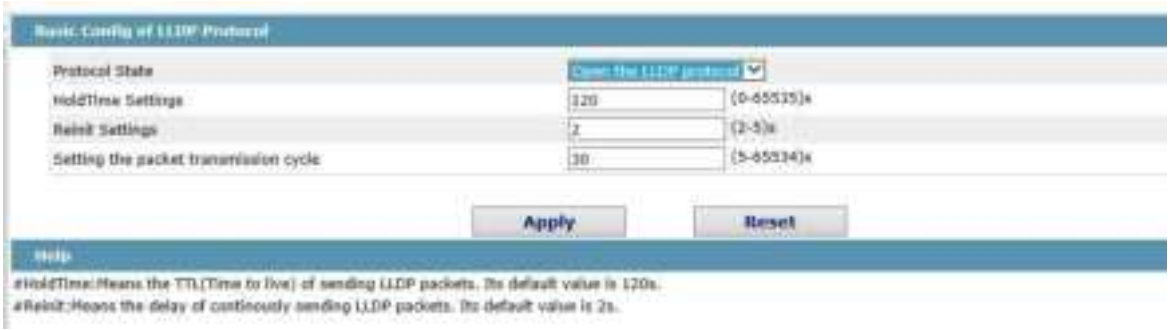
Click "Delete" to delete the static MAC address entry.



5.7 LLDP Configuration

5.7.1 Configuring the Global Attributes of LLDP

Choose link layer ? Config ? LLDP Config in the navigation bar, the Global LLDP Config page is displayed as shown in Figure 5.



You can choose to enable LLDP or disable it. When you choose to disable LLDP, you cannot configure LLDP.

The "Hold Time" parameter means the ttl value of the packet that is transmitted by LLDP, whose default value is 120s.

The "Reinit" parameter means the delay of successive packet transmission of LLDP, whose default value is 2s.

5.7.2 Configuring the Attributes of the LLDP Port

If you select Layer 2 Config > LLDP Config > LLDP Port Config in the navigation bar, the Setting the attributes of the LLDP port page appears, as shown in Figure 7.

Port	Receive LLDP Packet	Send LLDP Packet
gi0/1	Enable	Enable

LLDP interface configuration can enable or disable the port from transmitting LLDP packets.

5.8 DDM Configuration

Click L2 Config > DDM Config in the navigation bar, and enter DDM configuration page.

5.9 Link Aggregation Configuration

5.9.1 Port Aggregation Configuration

If you select Advanced Config > Link Aggregation Config in the navigation bar, the Link aggregation Config page appears, as shown in Figure 22.

If you click New, an aggregation group can be created. Up to 32 aggregation groups can be configured through Web and up to 8 physical ports in each group can be aggregated. If you click Cancel, you can delete the selected aggregation group; if you click Modify, you can modify the member port and the aggregation mode.

An aggregation group is not creatable when it is removed, but is not selectable when it is unselected.

When a member port exists in the aggregation port, you can change the aggregation mode to be Static、ACP Active or ACP Passive.

You can click add and remove to delete and add a member port in the aggregation group.

5.9.2 Configuring Load Balance of Port Aggregation Group

Some models support aggregation group based load balance mode configuration and some not, but can be configured in the global configuration mode.

You can select the aggregation load balance mode and click 'Apply' to apply it.

5.10 EAPS Ring Protection Configuration

5.10.1 EAPS Ring List

From link Layer Config > Ring Protection > EAPS Config, the 'EAPS Ring Config' page appears.

In this interface, the currently configured EAPS ring, including the status of the ring, the forwarding status of the port and the status of the link.

Click 'New' to create a new EAPS ring.

Click the 'Operate' button to configure the 'Time' parameter of the ring.

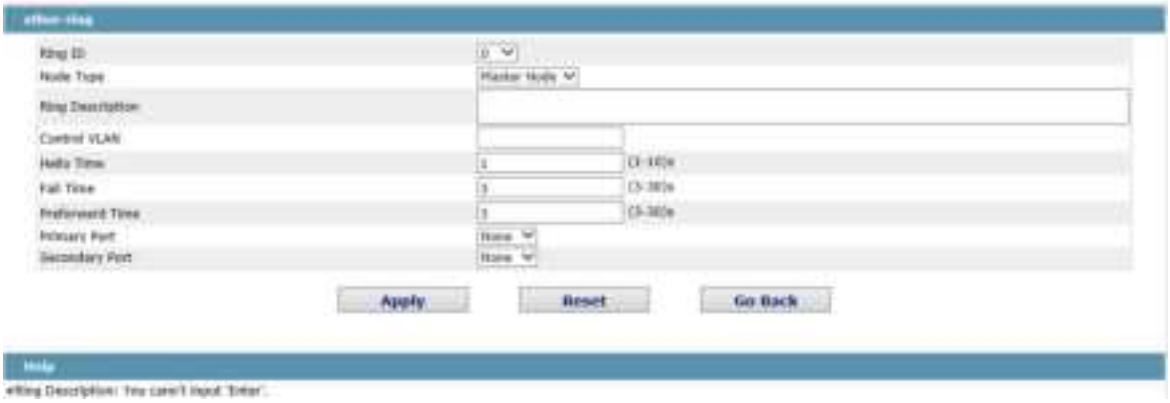
Notes:

1. The system can support 8 EAPS rings.

2. After a ring is configured, its port, node type and control Vlan cannot be modified. If the port of the ring, the node type or the control Vlan need be adjusted, please delete the ring and then create a new one.

5.10.2 EAPS Ring Configuration

If you click "New" on the EAPS ring list, or "Operate" on the right side of a ring item, the "Configure EAPS" page appears.



Notes:

If you want to modify a ring, on this page the ring ID, the control VLAN, the primary port and the secondary port cannot be modified.

In the dropdown box on the right of "Ring ID", select an ID for a ring ID. The ring ID of all devices on the same ring must be the same.

The dropdown box on the right of "Node Type" is used to select the type of the node. Please note that only one master node can be configured on a ring.

Enter a value between 1 and 4094 in the text box on the right of "Control VLAN" as the control VLAN ID. When a ring is established, the control VLAN will be automatically created in the system. Please note that if the designated control VLAN is 1 and the VLAN of the control device is not 1, the control service cannot access the control VLAN. Additionally, please do not enter a control VLAN ID that is same as that of another ring.

In the text boxes of "Primary Port" and "Secondary Port", select two ports as the ring ports respectively. If "Node Type" is selected as "Transit Node", the two ports of it are automatically set to transit ports.

Click "Apply" to finish EAPS ring configuration, or click "Reset" to resume the original values of the configuration, or click "Return" to go back to the EAPS list page.

5.11 MEAPS Configuration

5.11.1 MEAPS Ring Configuration

If you click Layer 2 Config > Multiple Ring Protection > Multiple Ring Protection on the navigation bar, the Multiple Ring Protection Configuration page appears.

The list shows the current configured MDAPS ring, including Domain ID, Ring ID, Ring type, Node type, Control Vlan, Hello Time, Failed Time, Pre-Forward Time, primary port and secondary port.

Click New to create a MDAPS ring.

Click Edit on the right side to configure the time parameter and the primary and secondary port of the ring.

Notes:

1. The system supports 4 MDAPS (0-3).

2. One domain can support 8 rings (0-7).

3. Once one MDAPS is configured, its Domain ID, ring ID, ring type, node type and control Vlan cannot be modified. If adjustment is needed, please delete the Ethernet ring and reserve.

5.11.2 MDAPS Ring Configuration

If you click New on the Multiple Ring Protection page or click Edit on the right, the New/MDAPS Global Config page appears.

Notes:

For existed MDAPS ring, the domain ID, ring ID, ring type, node type and control Vlan cannot be modified.

The primary ring can only be configured with the main node and the Transit node.

The secondary ring can be configured with the main node, the transit node, the edge node and the assistant edge node.

The primary node and the transit node can only be existed in one ring.

The edge node and the assistant edge node can be existed in multiple rings simultaneously.

On the right drop box of "Primary Port" and "Secondary Port", set the port respectively as the ring port or assort None.

5.12 Backup Link Protocol Configuration

5.12.1 Backup Link Protocol Global Configuration

Typical: Link Layer > Config > Backup Link Config > Backup Link Protocol Global

Config on the navigation bar, the Backup Link Protocol Global Config page appears.

On the page, the current configured backup link groups are shown, including Preemption Mode and Preemption Delay.

Click New to create a new link backup group.

Click Edit on the right to configure Preemption Mode and Preemption Delay.

Notes:

1. The system supports 8 link backup groups.

2. The Preemption mode determines the policy the primary port and the backup port forward packets.

5.12.2 Backup Link Protocol Interface Configuration

Typical: Link Layer > Config > Backup Link Protocol > Config > Backup Link Protocol Interface Config on the navigation bar.

the Backup link Protocol Global Config page appears.

This page shows the backup link groups, member ports, Interface Attribute, MMU Attribute, Shareload Vlan, etc.

Click Edit on the right to configure the Backup link Protocol.

The backup link group which has configured the primary port cannot take other ports as its primary port. Likewise, the backup link group which has configured the backup port cannot take other ports as its backup port.

5.13 MTU Configuration

Typical link Layer 2 Config > MTU Config on the navigation bar, the MTU Config page appears.

You can set the size of the maximum transmission unit (MTU).

5.14 PDP Configuration

5.14.1 Configuring the Global Attributes of PDP

Typical link Layer 2 Config > PDP Config in the navigation bar, the Global PDP Config page appears, as shown in figure 5-4.

You can choose to enable PDP or disable it. When you choose to disable PDP, you cannot configure PDP.

The "Hold Time" parameter indicates the time to be saved before the router discards the received information if other PDP packets are not received.

5.14.2 Configuring the Attributes of the PDP Port

Choose Link Layer > Config > PDP Config > PDP Port Config in the navigation bar, the Setting the attributes of the PDP port page appears, as shown in Figure 5.

Port	Status
g0/1	Enable PDP

After the PDP port is configured, you can enable or disable PDP on this port.

Chapter 6 Layer-3 Configuration

6.1 Vlan interface configuration

Click L3 Config > VLAN Interfaces and IP Addresses, and enter the VLAN interface configuration page.

Click New to add a new VLAN interface. Click Cancel to delete a VLAN interface. Click Modify to modify the settings of a corresponding VLAN interface.

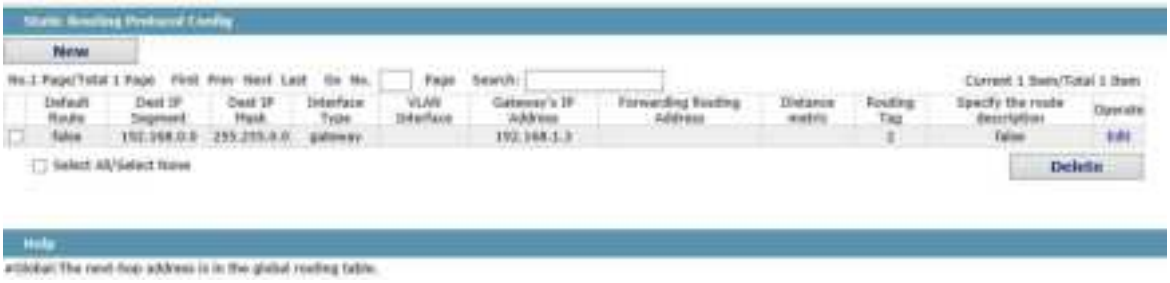
When you click New, the name of the corresponding VLAN interface can be modified; but if you click Modify, the name of the corresponding VLAN interface cannot be modified.

Notes:

Before the accessory IP of a VLAN interface is set, you have to set the main IP.

6.2 Setting the Static Route

If you click Layer 3 Config > Static Route Config, the Static route configuration page appears.



Click Create to add a static route.

If you click Edit, you can modify the current static route.

If you click Cancel, you can cancel the current static route.

Chapter 7 Advanced Configuration

7.1 Qos Configuration

7.1.1 Configuring QoS Port

If you click Advanced Config > Qos > Configure Qos Port the Port Priority Config page appears.

You can set the CoS value by clicking the dropdown box on the right of each port and selecting a value. The default CoS value of a port is 0, meaning the lowest priority. If the CoS value is 7, it means that the priority is the highest.

7.1.2 Global Qos Configuration

If you click Advanced Config > Qos > Configure Qos Port, the Port Priority Config page appears.

In WRR mode, you can set the weight values of the Qos queues. There are 4 queues in total, among which queue 4 has the highest priority and queue 1 has the lowest priority.

7.2 IP Access Control List

7.2.1 Setting the Name of the IP Access Control List

If you click Advanced Config > IP Access Control List > IP Access Control List Config, the IP ACL configuration page is accessed.

Click New to add a name of the IP access control list. Click Cancel to delete an IP access control list.

If you click Modify, the corresponding IP access control list appears and you can set the corresponding rules for the IP access control list.

7.2.2 Setting the Rules of the IP Access Control List

- Standard IP access control list

Click New to add a rule of the IP access control list. Click Cancel to delete a rule of the IP access control list. If you click Modify, the corresponding IP access control list appears and you can set the corresponding rules for the IP access control list.

➢ Extended IP access control list

Click New to add a rule of the IP access control list. Click Cancel to delete a rule of the IP access control list. If you click Modify, the corresponding IP access control list appears and you can set the corresponding rules for the IP access control list.

7.2.3 Applying the IP Access Control List

If you click Advanced Config > IP Access Control List > Applying the IP Access Control List, the Applying the IP access control list page appears.

7.3 MAC Access Control List

7.3.1 Setting the Name of the IP Access Control List

If you click Advanced Config > MAC Access Control List > MAC Access Control List Config, the MAC ACL configuration page appears.

Click New to add a name of the MAC access control list. Click Cancel to delete an ACL access control list.

7.3.2 Setting the Rules of the MAC Access Control List

If you click Modify, the corresponding MAC access control list appears and you can set the corresponding rules for the MAC access control list.

Click New to add a name of the MAC access control list. Click Cancel to delete a current ACL access control list. If you click Modify, the corresponding ACL access control list appears and you can set the corresponding rules for the MAC access control list.

7.3.3 Applying the MAC Access Control List

If you click Advanced Config > MAC Access Control List > Applying The MAC Access Control List, the Applying the MAC access control list page appears.

Port	Egress ACL	Ingress ACL
00/1		
00/2		
00/3		
00/4		
00/5		
00/6		
00/7		

Chapter 8 Network Management Configuration

8.1 SNMP Configuration

If you click Network Management Config > SNMP Management in the navigation bar, the SNMP management page appears, as shown in figure 2.

8.1.1 SNMP Community Management

On the SNMP community management page, you can view the related configuration information about SNMP community.

You can create, modify or cancel the SNMP community information. And if you click View or Edit, you can go to the configuration page of SNMP community.

On the SNMP community management page, you can create the SNMP community name, select the attributes of SNMP community, which include Read only and Read Write.

8.1.2 SNMP Host Management

On the SNMP community host page, you can know the related configuration information about SNMP host.

You can create, modify or cancel the SNMP host information, and if you click New or Edit, you can enter the configuration page of SNMP host.

On the SNMP host configuration page, you can enter SNMP host IP, SNMP Community, SNMP Message Type and SNMP Community Version. SNMP Message Type includes Trap and Inform, and as to version 1, SNMP Message Type does not support Informs.

8.2 RMON

8.2.1 RMON Statistic Information Configuration

If you click Network Management Config > Rmon > Rmon Statistics, RMON Statistics page appears.

Now, the RMON Statistics page appears.

You need to set a physical port to be the monitor terminal of the monitor data.

The index is used to identify a specific interface. If the index is same to that of the previous application interface, it will replace that of the previous application interface.

At present, the Rmon statistic information can be obtained through the command line, show rmon statistics, but the

Web does not support this function.

8.2.2 RMON History Information Configuration

Typ click Network Management Config > RMON > RMON History > Local, the RMON history page appears.

You need to select a physical port to set the request or terminal interface monitor data.

The index is used to identify a specific interface. If the index is same to that of the previous configuration interface, it will replace that of the previous application interface.

The sampling number means the items that need be preserved, whose default value is 50.

The sampling interval means the time between two data collection, whose default value is 1800s.

At present, the near-to-statistic information can be obtained through the command "show rmon history", but the Web does not support this function.

8.2.3 RMON Alarm Information Configuration

Typ click Network Management Config > Rmon > Rmon Alarm > Local, the RMON Alarm page appears.

The index is used to identify a specific alarm information; if the index is same to the previously applied index, it will replace the previous one.

The MIB node name corresponds to OID.

If the alarm type is absolute, the value of the MIB object will be directly monitored; if the alarm type is delta, the change of the value of the MIB object in two sampling will be monitored.

When the monitored MIB object reaches or exceeds the rising threshold, the event corresponding to the index of the rising event will be triggered.

When the monitored MIB object reaches or exceeds the falling threshold, the event corresponding to the index of the falling event will be triggered.

8.2.4 RMON Event Configuration

Typically, Network Management Config > RMON > RMON Event. RMON event page appears. Now, the RMON event page appears.

The index corresponds to the rising event index and the falling event index that have already been configured on the RMON alarm config page.

The owner is used to describe the owner of the information of an event.

"Enable log" means to add an item of information in the log table when the event is triggered.

"Enable trap" means a trap will be generated if the event is triggered.

Chapter 9 Diagnosis Tools

9.1 Ping

9.1.1 Ping

If you click Diagnosis Tools -> Ping, the Ping page appears.

Ping is used to test whether the switch connects other devices.

To Ping test should be conducted, please enter an IP address in the "Destination address" textbox, such as the IP address of your PC, and then click the "PING" button. If the switch connects your connected address, the device can promptly return a test result to your front, the screen will take a little more time to return the test result.

"Source IP address" is used to set the source IP address which is carried in the Ping packets.

"Size of the PING packet" is used to set the length of the Ping packet which is transmitted by the device.

Chapter 10 System Management

10.1 User Management

10.1.1 User List

If you click System Mgr. > User Mgr., the User Management page appears.

You can click "New" to create a new user.

To modify the permission or the login password, click "Edit" on the right of the user list.

Notes:

1. Please make sure that at least one system administrator exists in the system, so that you can manage the devices through

Web.

3. The limited user can only browse the status of the device.

10.1.2 Establishing a New User

If you click "New" on the User Management page, the Creating User page appears.

In the "User name" text box, enter a name, which contains letters, numbers and

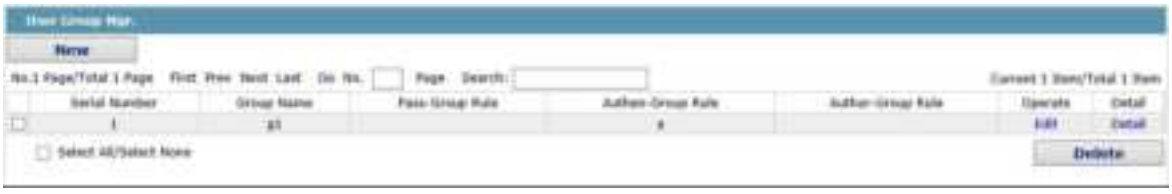
symbols except "?", "", "&", "#" and the "Space" symbol.

In the "Password" textbox enter a login password, and in the "Confirming password"

Textbox enter this login password again.

10.1.3 User Group Management

Click the Tab to get into user group management and enter user group management page.



Click "create new" to create a new user group.

Click "delete" to delete the user group.

The new user group name must be unused before. The password rule name, authentication rule name and authorization rule name must have been created, or you cannot create a new user group. Configure the password rule, authentication rule and authorization rule in other 3 tabs pages.

10.1.4 Password Rule Management

Click password rule management Tab page to enter password rule management page.

Click "create new" to create new password rule.

Click "delete" to delete password rule.

Set some password rules including whether the password can be the same with the user name, whether the password must contain numbers, lower-case, upper-case, special characters, the minimum length and the period of validity.

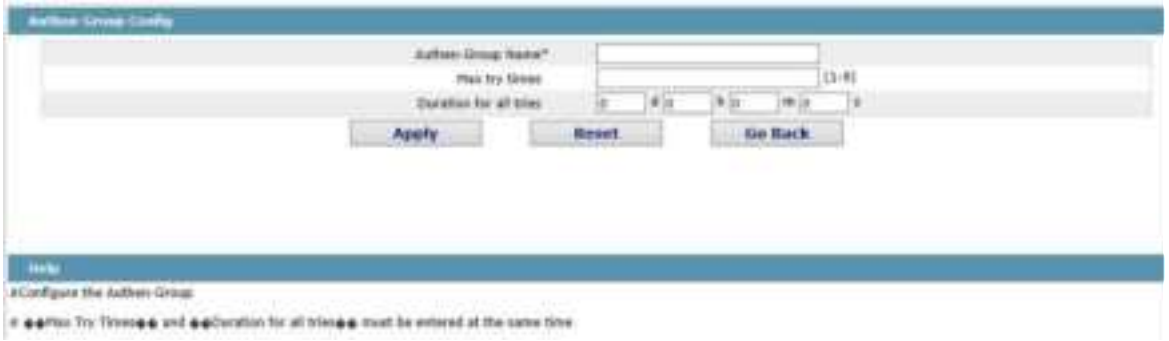
When the rule is created and applied on the user management, the user password will show invalid if the user password is not compliied with the password rule, vice versa.

10.1.5 Authentication Rule Management

Click the Tab page of authentication rule management to enter authentication management page.

Click "create new" to create the new authentication rule.

Click "delete" to delete the authentication rule.



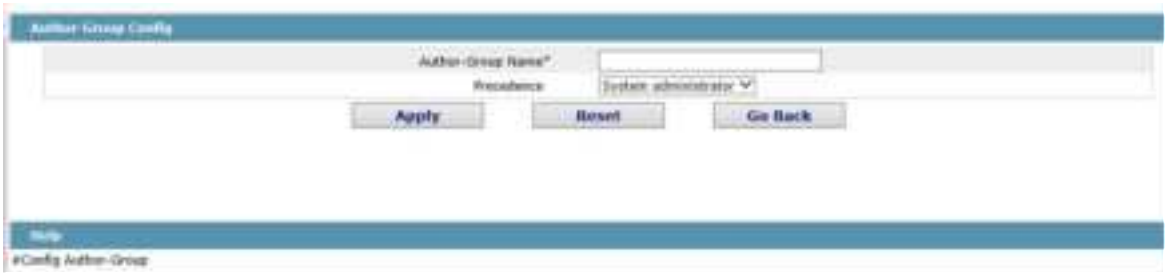
You can configure the maximum number of attempts and services or you don't, but you must configure them simultaneously or not them.

10.1.6 Authorization Rule Management

Click the Tab page of authorization rule and enter the authorization rule management page.

Click "create new" to create new authorization rule.

Click "delete" to delete the authorization rule.



The authorization rule determines your permission of the administrator or the limited user. If you are the administrator, you have the administrator right. If you are the limited user, you can only check the web.

10.2 Log Management

If you click System Mgmt > Log Mgt, the Log Management page appears.

If "Enabling the log server" is selected, the device will transmit the log information to the designated server. In this case, you need enter the address of the server in the "Address of the system log server" textbox and select the log's grade in the "Grade of the system log information" dropdown box.

If "Enabling the log buffer" is selected, the device will record the log information to the memory. By logging on the device through the Console port or Telnet, you can run the command "show log" to browse the logs which are stored on the device. The log information cached in the memory will be lost after reboot ing. Please enter the size of the buffer area in the "Size of the system log buffer" textbox and select the grade of the cached log in the "Grade of the cached log information" dropdown box.

10.3 Managing the Configuration Files

If you click System Mgmt > Configuration file, the Configuration file page appears.

10.3.1 Exporting the Configuration Information

The current configuration file can be exported, saved to the client PC or to the mobile storage device as the backup file.

To export the configuration file, please click the "Export" button and then select the "Save" option in the pop-up download dialog box.

The default name of the configuration file is "startup-config", but you are suggested to save it to an easily memorable name.

10.3.3 Importing the Configuration Information

You can import the configuration files from PC to the device and recover the configuration file that is currently being used. For example, by importing the backup configuration files, you can resume the device to its configuration of a previous moment.

Notes:

1. Please make sure that the imported configuration file has the legal format for the configuration file with illegal format can not lead to the normal start-up of the device.

2. If the error occurs during the process of importation, please try it once again, or click the "Save All" button to make the device re-establish the configuration file with the current configuration, avoiding the incomplete file and the abnormality of the device.

3. After the configuration file is imported, if you want to use the imported configuration file immediately, do not click "Save All", but reboot the device directly.

10.4 Software Management

Click System Mgt. > Software Update in the navigation bar to enter the device software management page.

10.4.1 Backup System Software

The current running software version is displayed on the page. If you need to backup the system, please click "Backup

system software", then select "save" in the pop-up file download dialog box and save the system profile to your computer disk, transfer to flash device or other positions in the network.

Notes:

Default name of the system profile is "boot.bin". You are suggested to change the default name to a name that is easy to identify.

10.4.2 Update System Software

Notes:

1. Please ensure your update system profile matches with the device type. Otherwise, the system cannot operate normally.

2. The system profile update may need 1 to 2 minutes. After clicking and confirming the "update" button, the prompt box of update to the device. Please be patient.

3. Please do not restart or interrupt the device if errors occur in the update process or the device cannot start up. Please try update again later.

4. Please save the configuration and restart the device after updating, so that the new system can operate.

The update software is usually used for resolving the existing problems or improving certain functions. You don't need to update the system software regularly. If your device operates normally.

If your system needs to be updated, please enter the full path of the new system profile in the text box right of "update system software" or click "browse" button to select new system profile and click "update".

10.4.3 Rebooting the Device

If you click System > Reboot, the Rebooting page appears.

If the device need be rebooted, please first make sure that the modified configuration of the device have already been saved, and then click the "Reboot" button.