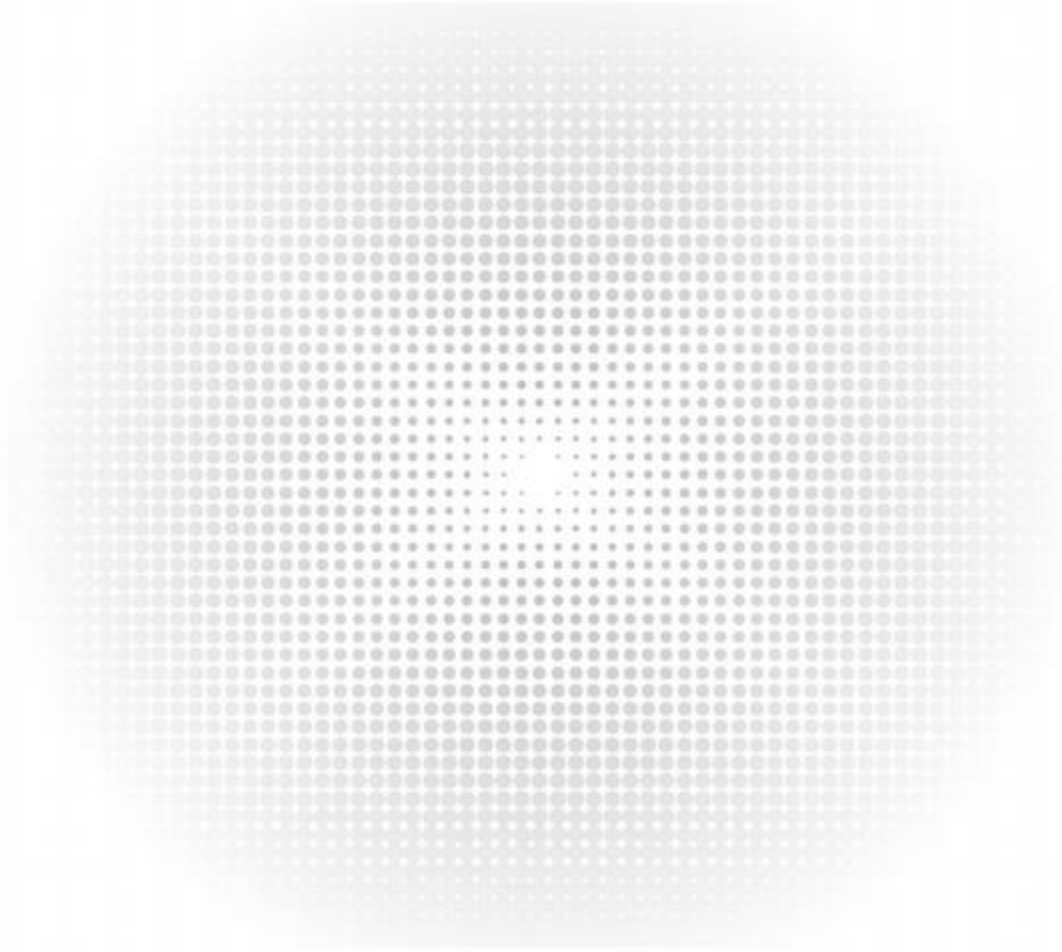
IES3100 Series Switches Configuration Guide

Models: IES3100-8TF ; IES3100-8TF-P



Configuration Guide

Contents

Chapter 1 Basic Configuration 1

1. 1 HTTP protocol configuration 1

1.1.1 Language Selection 1

1.1.2 HTTP service port configuration 1

1.1.3 Enabling the HTTP service 1

1.1.4 HTTP access mode Configuration 1

1.2 HTTPS Configuration 2

1.2.1 HTTPS Access Configuration 2

1.2.2 HTTPS Service Port Configuration 2

Chapter 2 Accessing Switch 3

2. 1 Accessing the Switch Through Web 3

2.2 Initially Accessing the Switch 3

2.3 Accessing Switch Through Secure Links 4

2.4 Introduction of Web Interface 4

2.4.1 Top Control Bar 5

2.4.2 Navigation Bar 5

2.4.3 Configuration Display Area 6

2.4.4 Bottom Control Bar 6

Chapter 3 Dashborad 8

Chapter 4 Interface 9

4.1 Port Config 9

4.1.1 Port Config 9

4.1.2 Port Rate Limiters 10

4.2 Storm Control 11

4.2.1 Broadcast Storm 11

4.2.2 Multicast Storm 12

4.2.3 Unicast Storm 12

4.3 Flow Control 13

4.3.1 Ports Statistics 13

4.3.2 Error packet statistics 14
4.3.3 SFP 14
4.4 SPAN 15
4.5 Port Filtering 16
4.5.1 Global Config 16
4.5.2 Port Config 16
4.5.3 Filter Statistics 17
4.6 Link Aggregation 18
4.6.1 Global Config 18
4.6.2 Link Aggregation 19
4.7 MAC 20
4.7.1 Global Config 20
4.7.2 Static MAC address table 21
4.8 STP 22
4.8.1 Global Config 22
4.8.2 STP Information 22
4.8.3 Port Config 23
4.8.4 MST Region 23
4.8.5 MST Instance 24
4.9 DHCP Snooping 25
4.9.1 Global Config 25
4.9.2 VLAN Configuration 25
4.9.3 Interface Config 26
4.9.4 Interface Binding List 27
4.10 Ring Protection 28
4.11 PTP Config 29
4.11.1 Global Config 29
4.11.2 Interface Config 30
4.11.3 Unicast Config 30
4.12 Backuplink 31
4.12.1 Protocol Global Config 31
4.12.2 Protocol Interface Config 32
Chapter 5 Advanced 33

5.1 QoS **33**
5.1.1 Global Config 33
5.1.2 Interface Config 33
5.1.3 QoS Policies 34
5.1.4 Congestion Management 34
5.2 ACL **35**
5.2.1 IPv4 Rule 35
5.2.2 MAC Rule 36
5.2.3 Assignment 37
Chapter 6 Network **38**
6.1 IGMP Snooping **38**
6.1.1 Global Config 38
6.1.2 Vlan Config 38
6.1.3 Static Multicast Mac 39
6.1.4 Multicast list 40
6.2 GMRP **40**
6.2.1 VLAN List 40
6.2.2 Port Config 41
6.2.3 Multicast List 42
6.3 LLDP **42**
6.3.1 Global Config 42
6.3.2 Interface Config 43
6.3.3 LLDP 43
6.3.4 LLDP-MED 44
6.4 VLAN **44**
6.4.1 VLAN Configuration 44
6.4.2 Vlan Batch Configuration 46
6.4.3 Access/Trunk Port 46
6.4.4 VLAN Interface Management 48
Chapter 7 Security **49**
7.1 RADIUS **49**
7.1.1 Global Config 49

7.1.2 Server 49

7.2 802.1X Port Authentication 50

7.2.1 Global Config 50

7.2.2 Authentication List 51

7.2.4 Statistics 52

7.3 ARP 53

7.4 Port Security 54

7.4.1 IP MAC Bind 54

7.4.2 Static MAC Filter Mode 55

7.4.3 Static MAC Filter 56

7.4.4 Dynamic MAC Mode 57

7.5 Management Access 58

7.5.1 HTTP 58

7.5.2 HTTPS 58

7.5.3 SSH 59

7.5.4 SNMP 59

7.6 SNMP 60

7.6.1 SNMPv1/v2 Community 60

7.6.2 Host Management 61

Chapter 8 System 62

8.1 Reboot/Save 62

8.1.1 Restart 62

8.1.2 Restore 62

8.2 Upgrade 62

8.2.1 Software 62

8.2.2 Load/Save 63

8.3 System Management 63

8.3.1 Global Config 63

8.3.2 Clock 64

8.3.3 NTP 64

8.3.4 System Information 65

8.4 Log 66

8.4.1 Log Manage 66

8.4.2 Log Query 67

8.5 Users 68

8.5.1 User Management 68

8.5.2 Group Management 69

8.5.3 Pass Management 70

8.5.4 Author Management 71

8.5.5 Authen Management 72

Chapter 9 Diagnostics 73

9.1 Command-Line Interface 73

9.1.1 Global Config 73

9.1.2 Login Banner 73

Chapter 1 Basic Configuration

1. 1 HTTP protocol configuration

Switches support not only being configured by CLI and SNMP protocol; it also supports being configured by web. HTTP service port configuration and time configuration of abnormal message overtime and etc are also supported.

1.1.1 Language Selection

In currently, there are supporting two languages in the Industrial Switch : you may choice English or Chinese. User can setting the language in the global configuration mode through the command line as shown as below.

Enter the command as shown as below in global configuration mode and then system language changed.

Command	Description
[no] ip http language { englis h}	Setting the Web language to English . The Web interface will turn into the English version.

1.1.2 HTTP service port configuration

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 to 192.168.1.2 and 1234 respectively, the HTTP access address should be changed to http://192.168.1.2:1234. You'd better not use other common protocols' ports so that access collision should not happen. For example, ftp-20 , telnet-23 , dns-53 , snmp- 161. Because the ports used by a lot of protocols are hard to remember, you'd better use port IDs following port 1024.

Command	Purpose
ip http port { *portNumber*}	Configuring HTTP service port

1.1.3 Enabling the HTTP service

Switches support to control the HTTP access. Only when the HTTP service is enabled can HTTP exchange happen between switch and PC and, when the HTTP service is closed, HTTP exchange stops. Configure global mode by the following command:

Command	Purpose
ip http server	Enabling HTTP service

1.1.4 HTTP access mode Configuration

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 enable	Configuring HTTP access mode

1.1.5 Setting the Max-VLAN numbers to display in Web page

Setting a value between 1 and 4094 in the global configuration mode (4094 which is the max value , default max-vlan value is 100)

Command	Description
ip http web max-vlan { *max-vlan* }	Setting the Max-VLAN numbers to display in Web page

1.1.6 Setting the IGMP-Groups number to display inWeb page

Setting a value between 1 and 100 in the global configuration mode . (100 which is the max value , default value is 15)

Command	Description
ip http web igmp-groups { *igmp-groups* }	Setting the IGMP-Groups number to display in Web page

1.2 HTTPS Configuration

In order to improve the security of communications, switches support not only 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 HTTPS Access Configuration

You can run the following command to set the access mode to **HTTPS** at global configuration mode.

Command	Description
ip http ssl-access enable	Enable the HTTPS access mod

1.2.2 HTTPS Service Port Configuration

As same as the HTTP service port, there is also the 443 port in HTTPS. User can change the port number through command line in global configuration mode. Suggesting the port number is bigger than 1024.

Command	Description
ip http secure-port {*portNumber*}	Setting the HTTPS port number

Chapter 2 Accessing Switch

2. 1 Accessing the Switch Through Web

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

- HTML of version 4.0
- HTTP of version 1. 1
- JavaScriptTM of 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 in which the switch is located.

2.2 Initially Accessing the Switch

When the switch is initially used, you can use the Web access without any extra settings:

1. Modify the IPaddress of the network adapter and subnet mask of your computer to 192.168.1.2 and 255.255.255.0 respectively.

2. Open the Web browser and enter 192.168.1.1 in the address bar. It is noted that 192.168.1.1 is the default management address of the switch.

3. If the IE browser is used, please enter the username and the password in the ID authentication dialog box. Both the original username and the password are"admin", which is capital sensitive.

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

2.2.1 Upgrading to theWeb-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 telnet 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 of which 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 ip http server command in global configuration mode and start the Web service.

5. Run username to set the username 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 write to save the current configuration to the configuration file.

Accessing SwitchThrough Secure Links

2.3 Accessing Switch Through Secure Links

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

To do this, you should follow the following steps:

1. Connect the console port of the switch with the accessory cable, or telnet 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 of which 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 ip http server command at global configuration mode and start the Web service.

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

6. Run ip http ssl-access enable to enable the secure link access of the switch.

7. Run no ip http http-access enable to forbid to access the switch through insecure links.

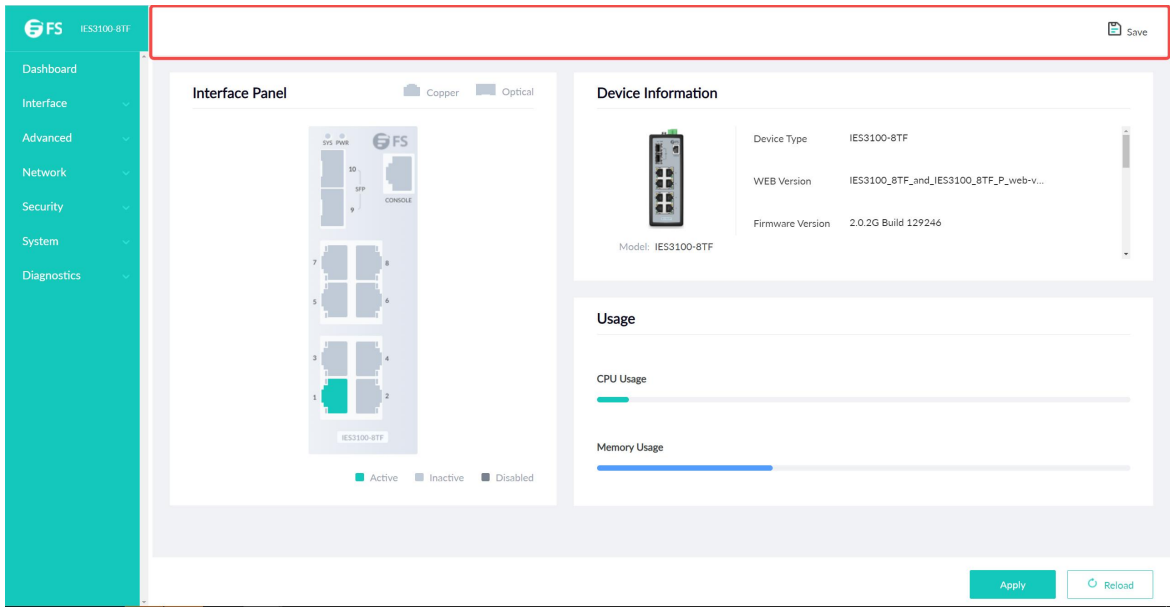
8. Enter write to store the current configuration to the configuration file.

9. Open the WEB browser on the PC that the switch connects, enter https://192.168.1.1 on the address bar (192.168.1.1 stands for the management IP address of the switch) and then press the Enter key. Then the switch can be accessed through the secure links.

2.4 Introduction of Web Interface

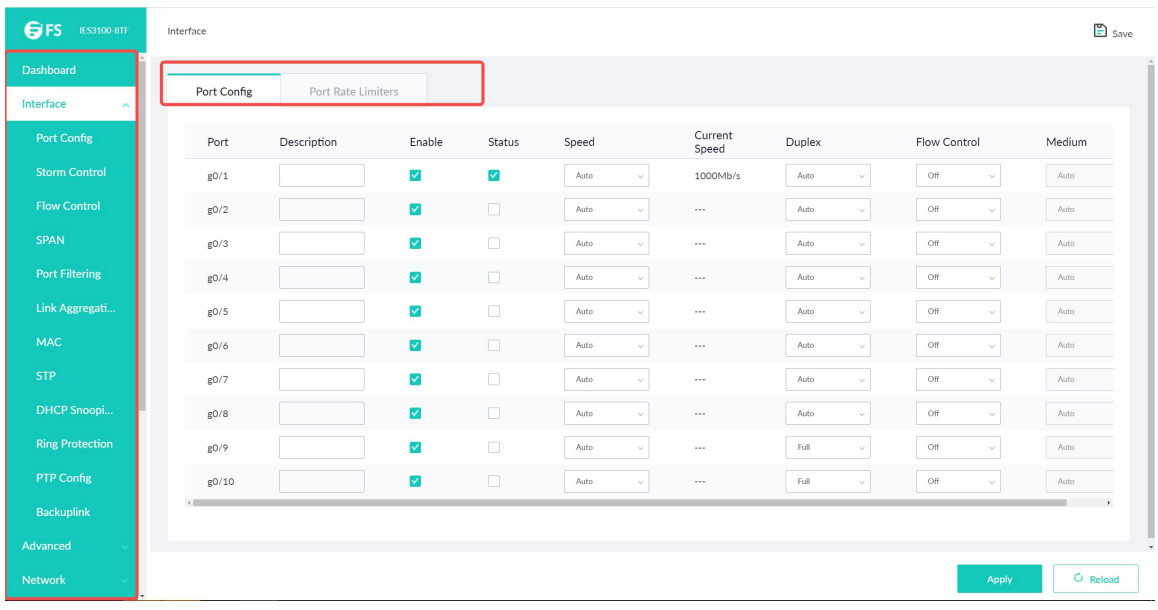
After logging in, a web page appears, which consists of the left navigation bar, top control bar, configuration display area, and bottom control bar.

2.4.1 Top Control Bar



Save	Write the current settings to 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", the unsaved configuration will be lost after rebooting.

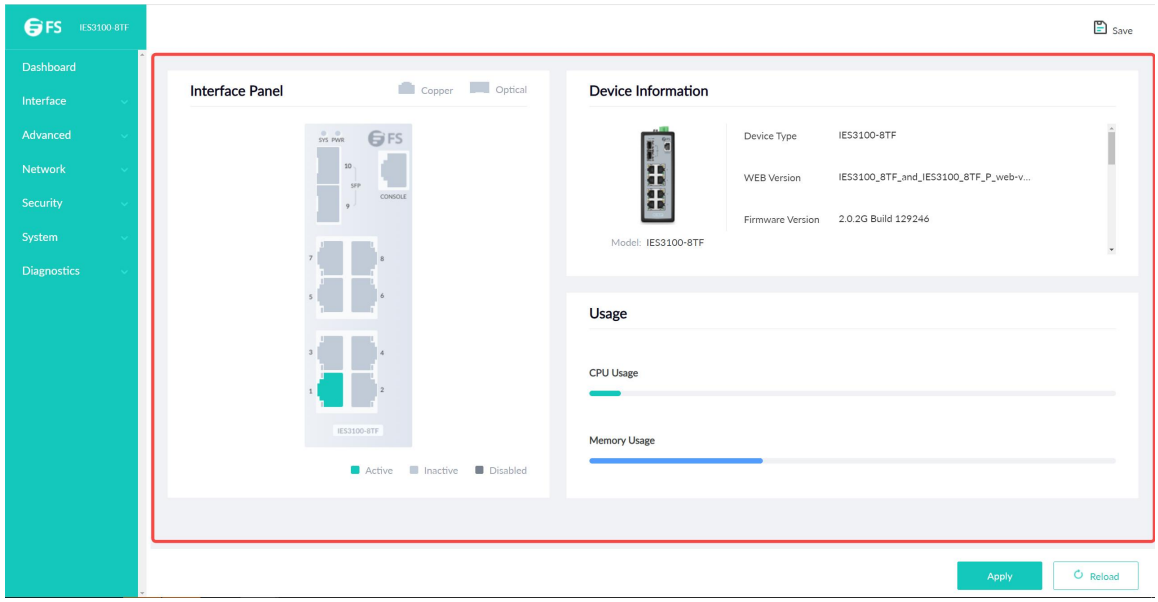
2.4.2 Navigation Bar



The contents in the navigation bar are shown in a form of list and are classified according to types. By default, the list is located at "Dashborad". 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" and then "Flow Control".

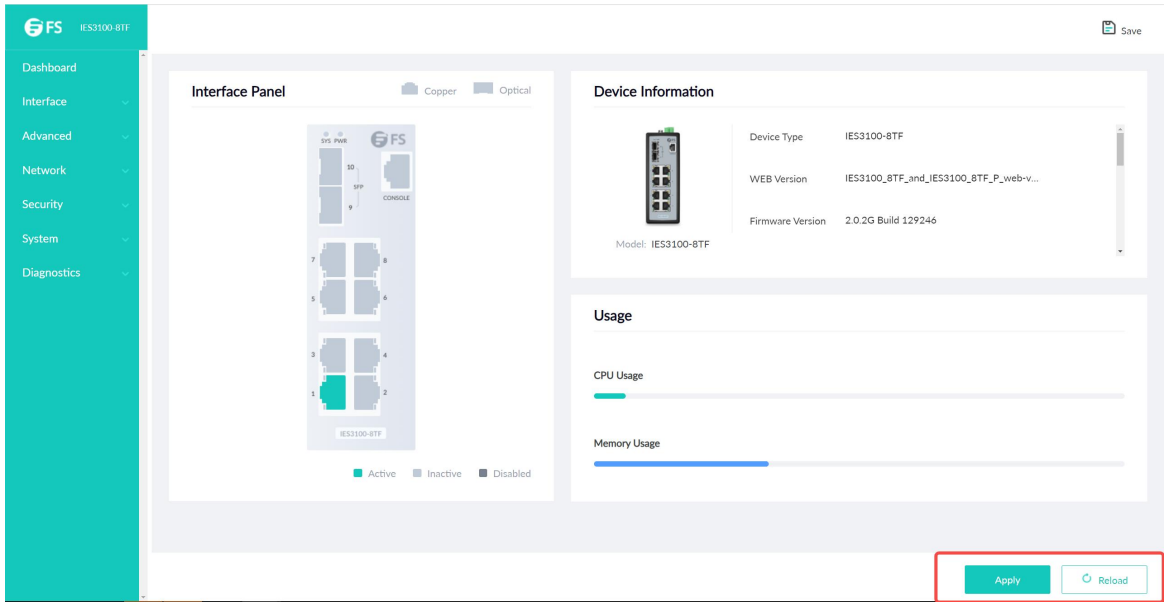
Note: The limited user can only browse the state of the device and cannot modify the configuration of the device. If you log on to the Web with limited user's permissions, only "Dashborad" will appear.

2.4.3 Configuration Display Area



The configuration display area shows the state and configuration of the device. The contents of this area can be modified by the clicking of the items in the navigation bar.

2.4.4 Bottom Control Bar

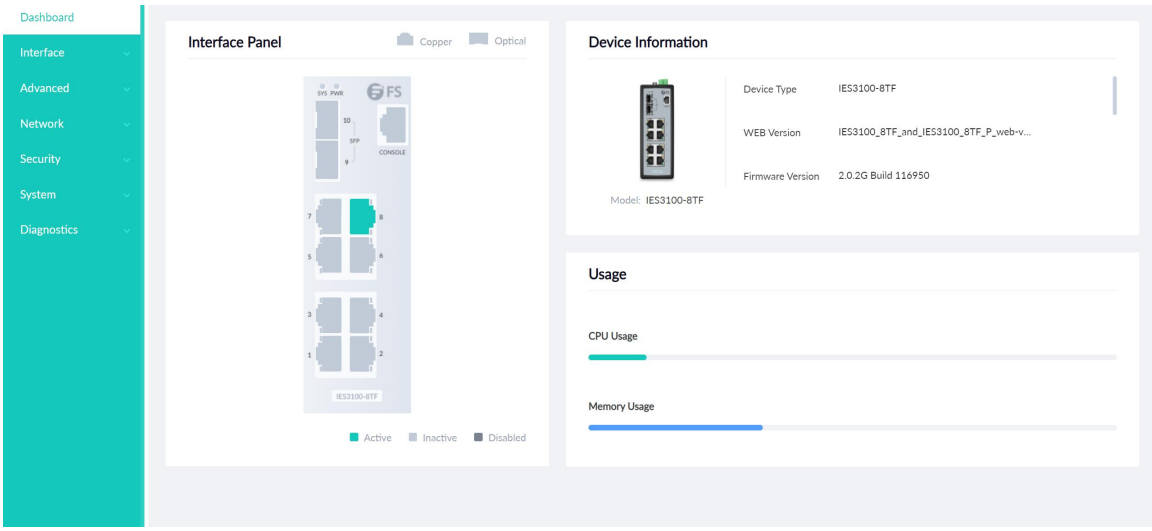


The configuration area always contains one or more buttons, and their functions are listed in the following table:

Refresh	Refresh the content shown in the current configuration area.
Apply	Apply the modified configuration to 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" on the top control bar.
Reset	Mean discarding the modification of the sheet. The content of the sheet will be reset.
Add	Create a list item. For example, you can create a VLAN item or a new user.
Delete	Delete an item in the list.
Go Back	Go back to the previous-level configuration page.

Chapter 3 Dashborad

If you click Dashborad in the navigation bar, the page appears as shown as below：



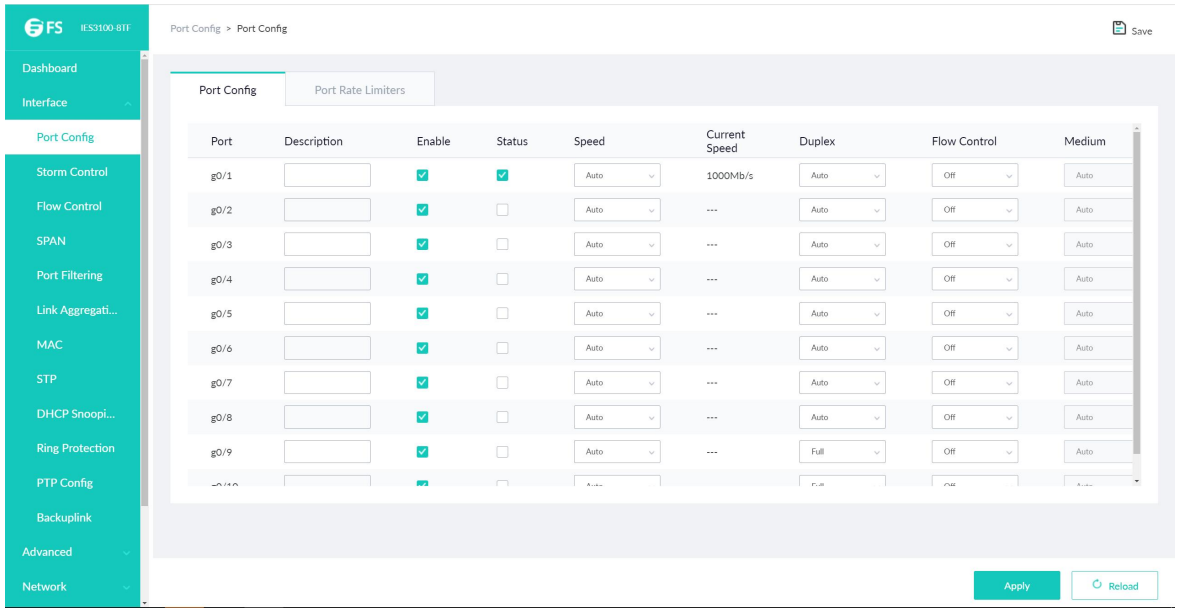
The page lists the system information, port configuration, user management port , CPU utilization, ...etc.

Chapter 4 Interface

4.1 Port Config

4.1.1 Port Config

If you click Intreface -> Port Config -> Port Config in the navigation bar, the Port Configuration page appears, as shown as below figure



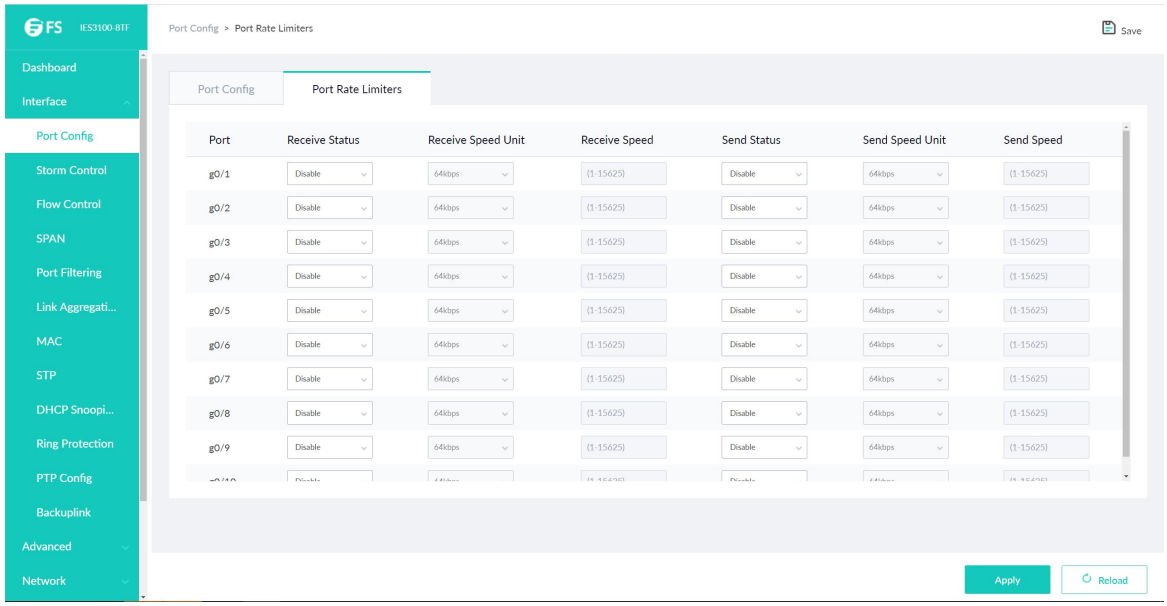
You can change the status, speed, duplex mode and flow control of a port on this page.

Note:

Port link switching might happen if modifying port's speed or duplex mode. Network communication might be affected.

4.1.2 Port Rate Limiters

Click Interface -> Port Config -> Port Rate Limiters at navigation bar in order to enter Port Rate Limiters as following:



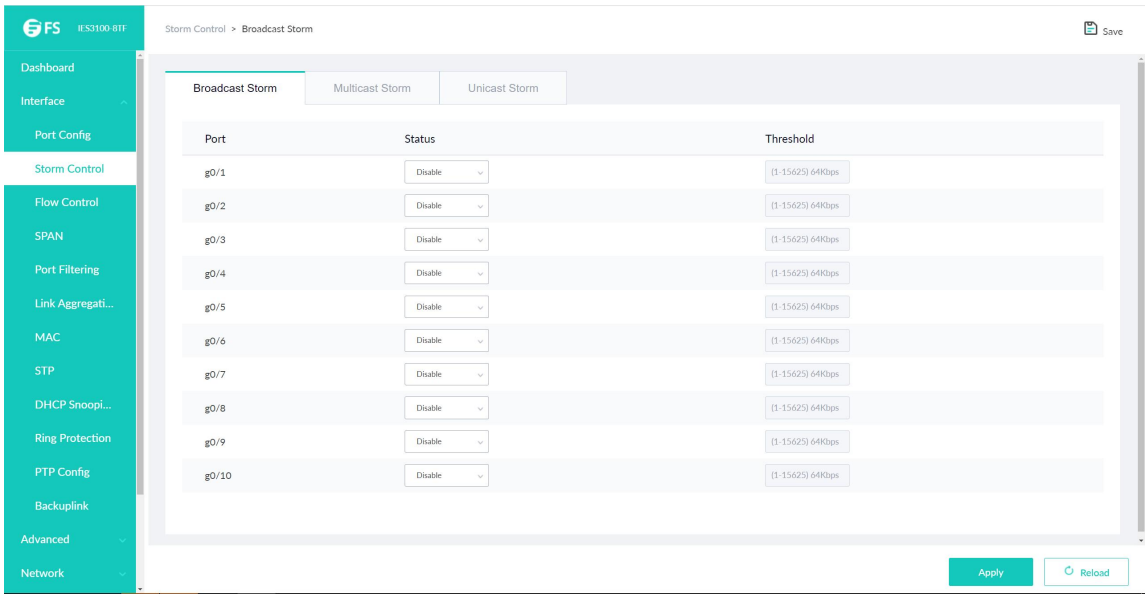
Do speed-limit on ports receive speed and send speed of port at this page. By default all ports' speed is not limited. Receive speed and send speed can be configured according to ratio or switch's defined unit.

4.2 Storm Control

Click Interface -> Storm Control at navigation bar in order to enter broadcast storm control, multicast storm control and unicast storm control as following:

4.2.1 Broadcast Storm

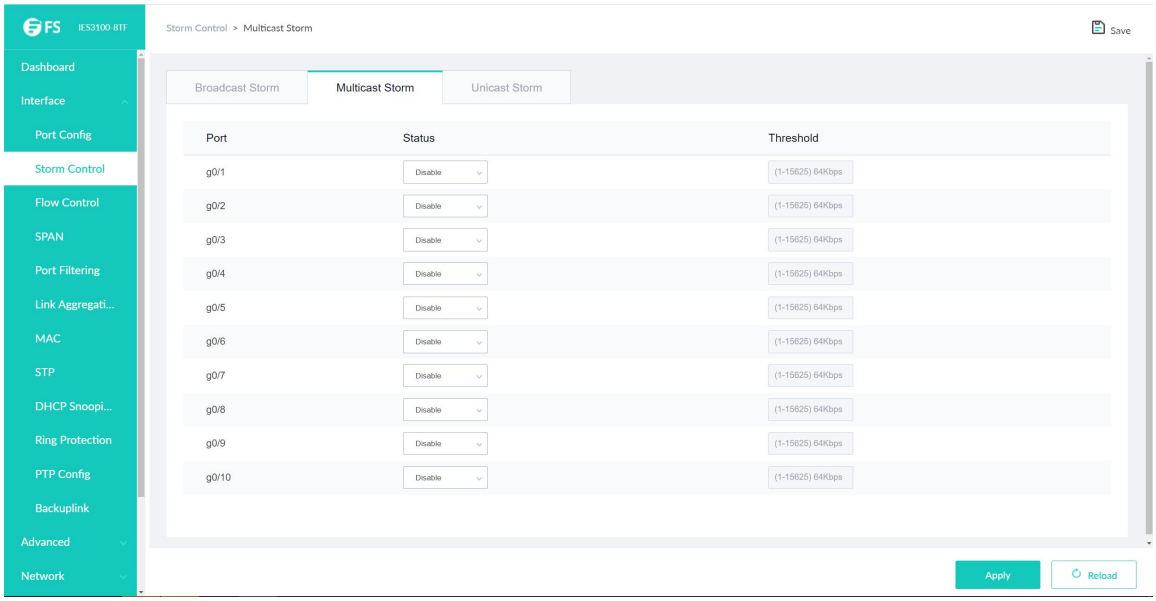
Click Interface -> Storm Control -> Broadcast Storm at navigation bar in order, and then enter the configuration page as following：



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.

4.2.2 Multicast Storm

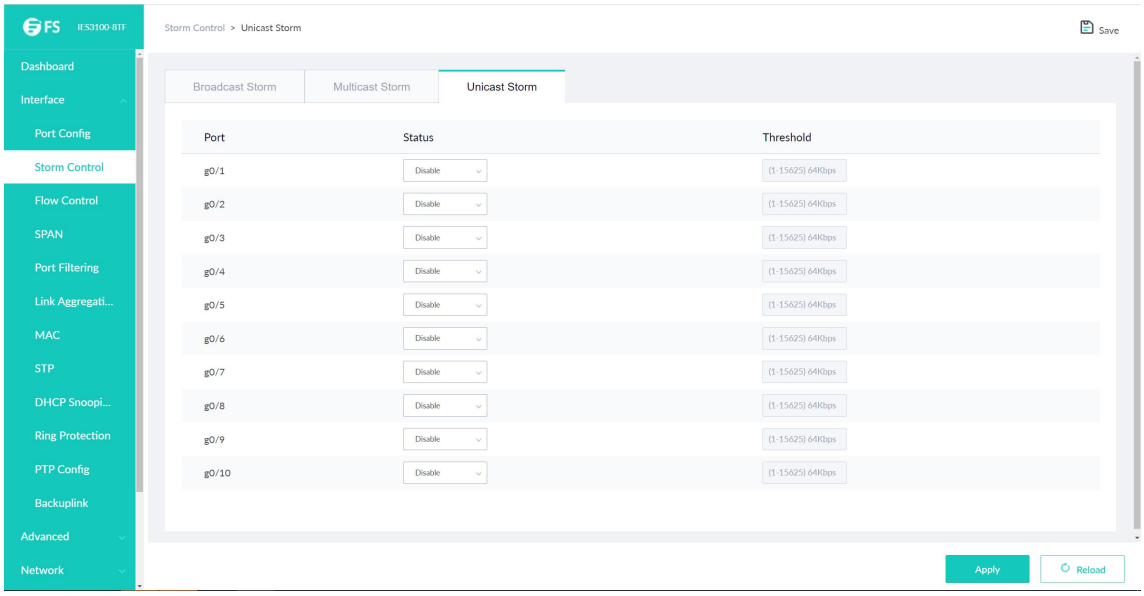
Click Interface -> Storm Control -> Multicast Storm at navigation bar in order, and then enter the configuration page as following:



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.

4.2.3 Unicast Storm

Click Interface -> Storm Control -> Unicast Storm at navigation bar in order, and then enter the configuration page as following:

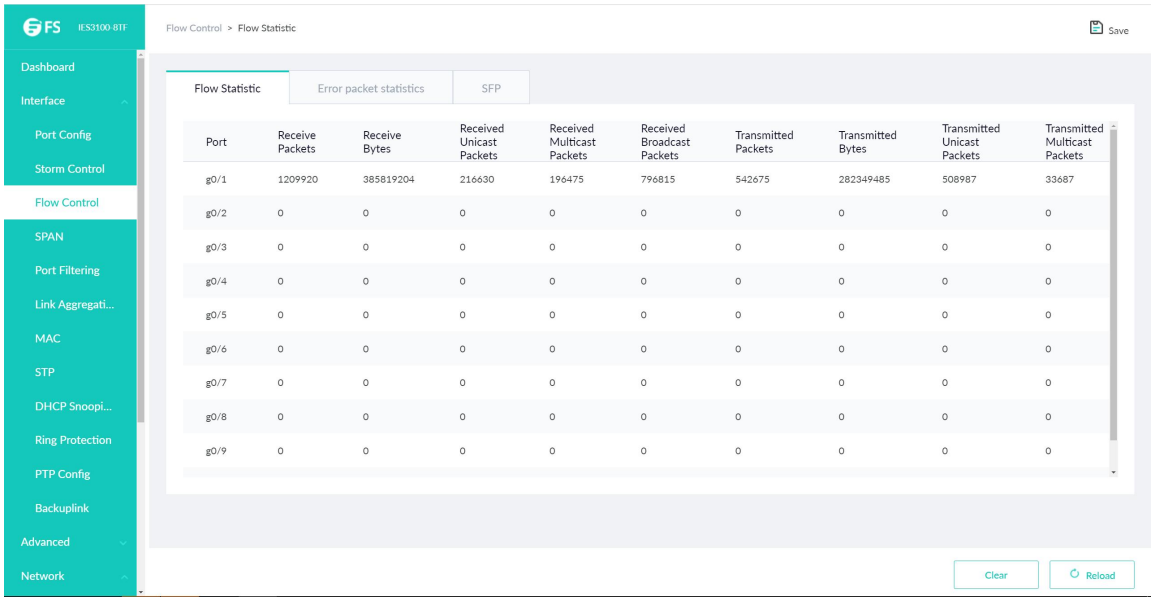


Through the dropdown boxes in the Status column, you can decide whether to enable unicast storm control on a port. In the Threshold column you can enter the threshold of the unicast packets. The legal threshold range for each port is given behind the threshold.

4.3 Flow Control

4.3.1 Ports Statistics

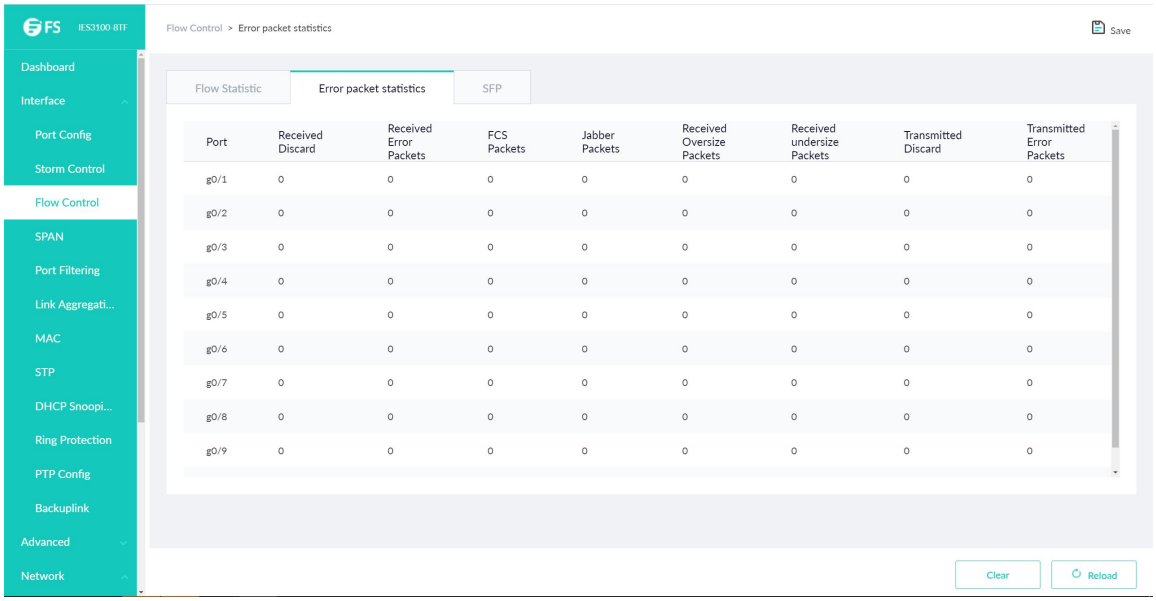
Click Interface -> Flow Control -> Port Statistics at navigation bar in order, and then enter the configuration page as following:



The page lists the port information, there are included the Receive Packets, Receive Bytes, Received Unicast Packets, Received Multicast Packets, Received Broadcast Packets...etc.

4.3.2 Error packet statistics

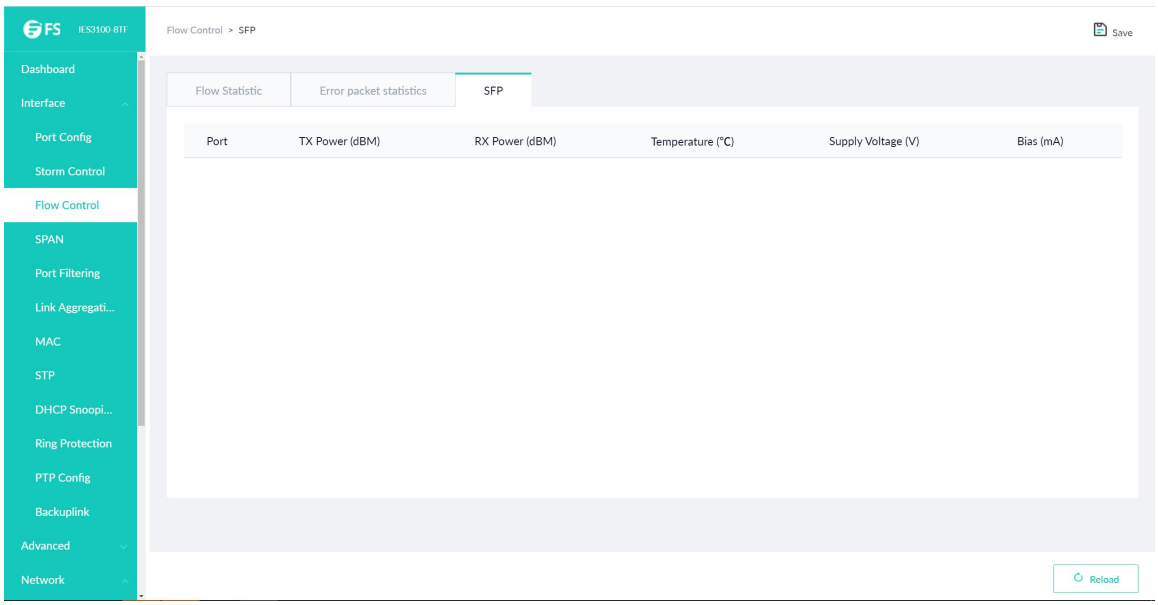
Click Interface -> Flow Control -> Error packet statistics at navigation bar in order, and then enter the configuration page as following:



The page lists the port information, there are included the Receive Packets, Receive Bytes, Received Unicast Packets, Received Multicast Packets, Received Broadcast Packets...etc.

4.3.3 SFP

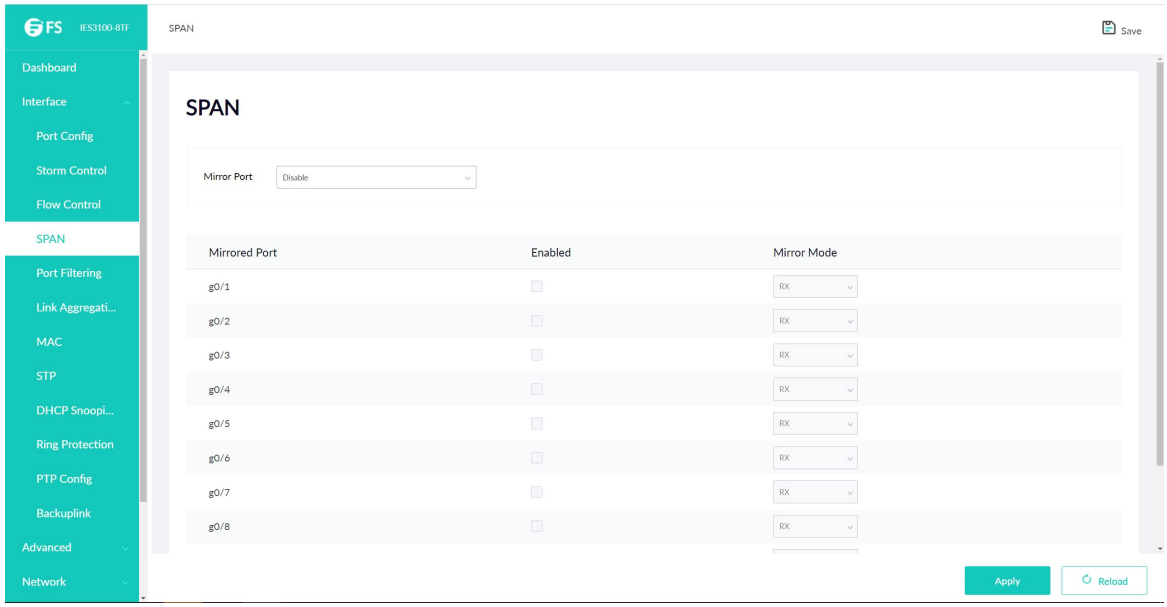
Click Interface -> Flow Control -> SFP at navigation bar in order, and then enter the configuration page as following:



Note: SFP port information can be read when the DDM has been enabled.

4.4 SPAN

Click Interface -> SPAN at navigation bar in order, and then enter the configuration page as following:



Click the dropdown box right of the Mirror Port and select a port to be the destination port of mirror.

Click the checkbox and select the mirroring source port:

RX The received packets will be mirrored to the destination port.

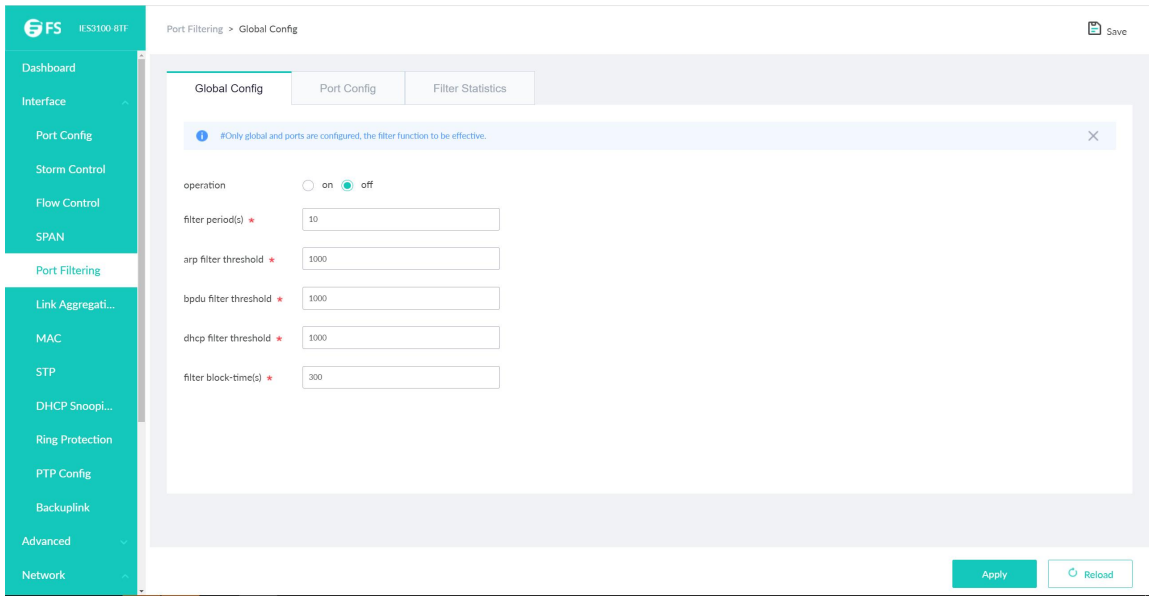
TX The transmitted packets will be mirrored to a destination port.

RX & TX The received and transmitted packets will be mirrored simultaneously.

4.5 Port Filtering

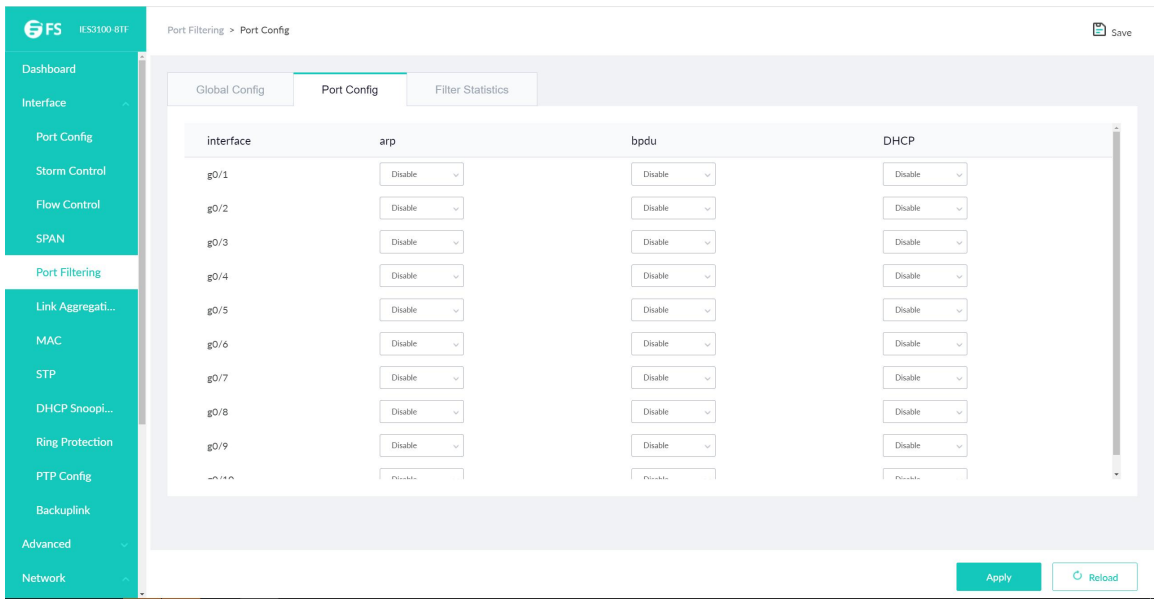
4.5.1 Global Config

Click Interface -> Port Filtering -> Global Config at navigation bar in order, and then enter the configuration page as following:



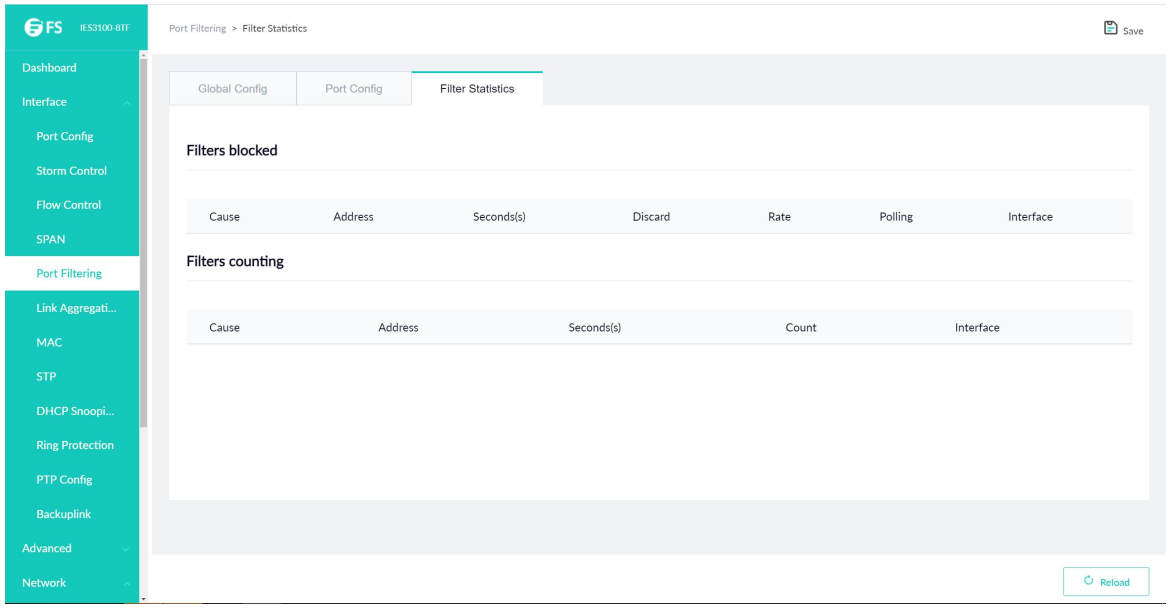
4.5.2 Port Config

Click Interface -> Port Filtering -> Port Config at navigation bar in order, and then enter the configuration page as following:



4.5.3 Filter Statistics

Click Interface -> Port Filtering -> Filter Statistics at navigation bar in order, and then enter the configuration page as following:



4.6 Link Aggregation

4.6.1 Global Config

Click Interface -> Link Aggregation -> Global Config at navigation bar in order, and then enter the link aggregation load balancing configurationpage as following：

Some models support link aggregation load balancing configuration and others not, but they can be configured in the global configuration mode.

This Layer 3 model can support the aggregation group based load balancing configuration:

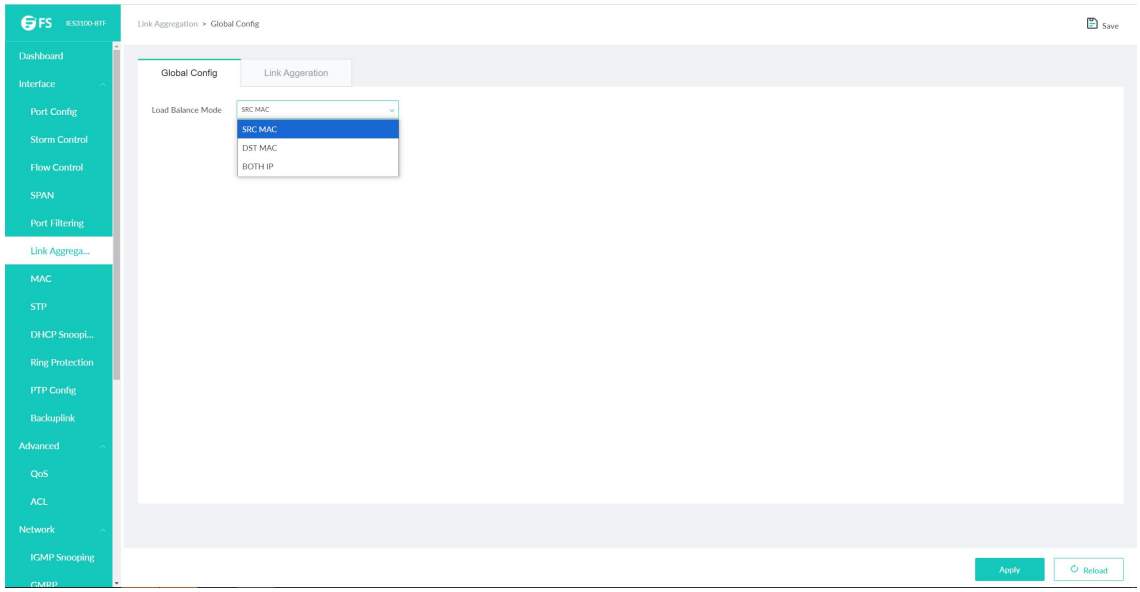


Figure: The Aggregation Group Based Load Balancing Configuration

You can use different aggregation groups to set different aggregation modes.

4.6.2 Link Aggregation

Click Interface -> Link Aggregation -> Link Aggregation at navigation bar in order, and then enter the link aggregation configuration page as following:

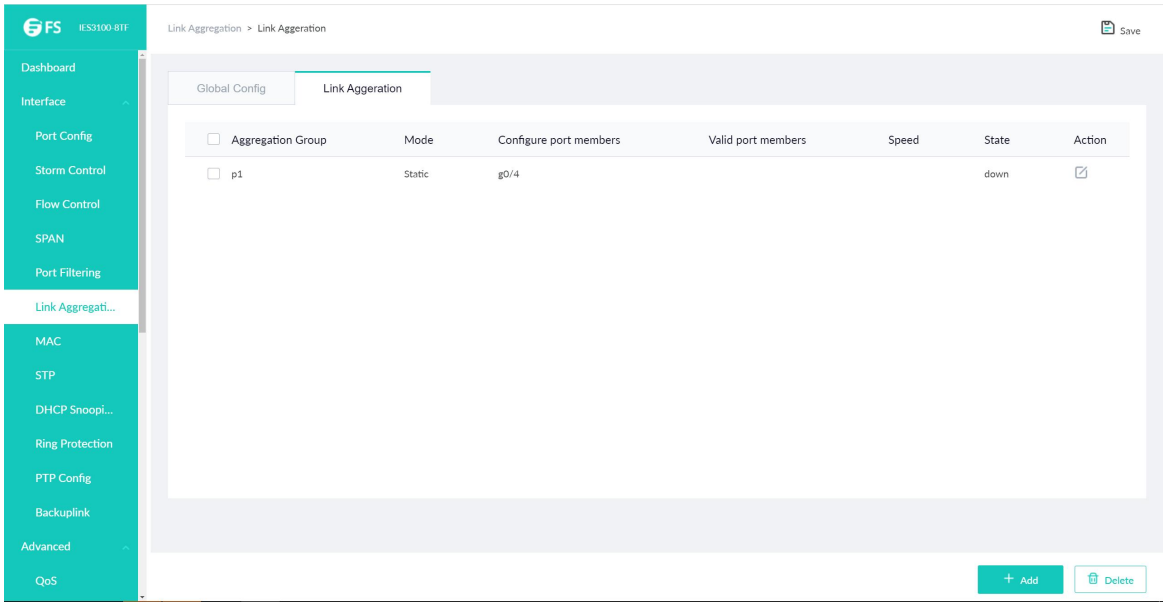


Figure: Port Aggregation Configuration

Click Add to create a new aggregation group. As much as 32 aggregation groups can be configured through Web. Each group can configure at most 8 physical port aggregations.

Click Delete to delete the selected aggregation group.

Click Edit icon to modify the member port and aggregation mode of the aggregation port.

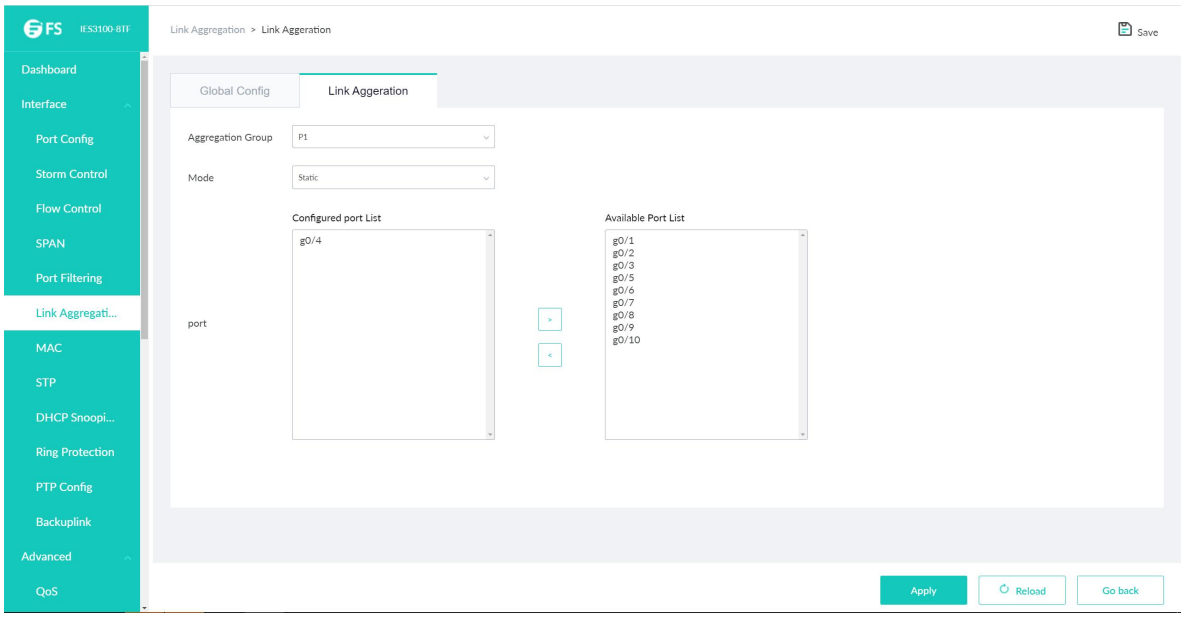


Figure: Aggregation Group Member Port Configuration

An aggregation group is selectable when it is created but is not selectable when it is modified.

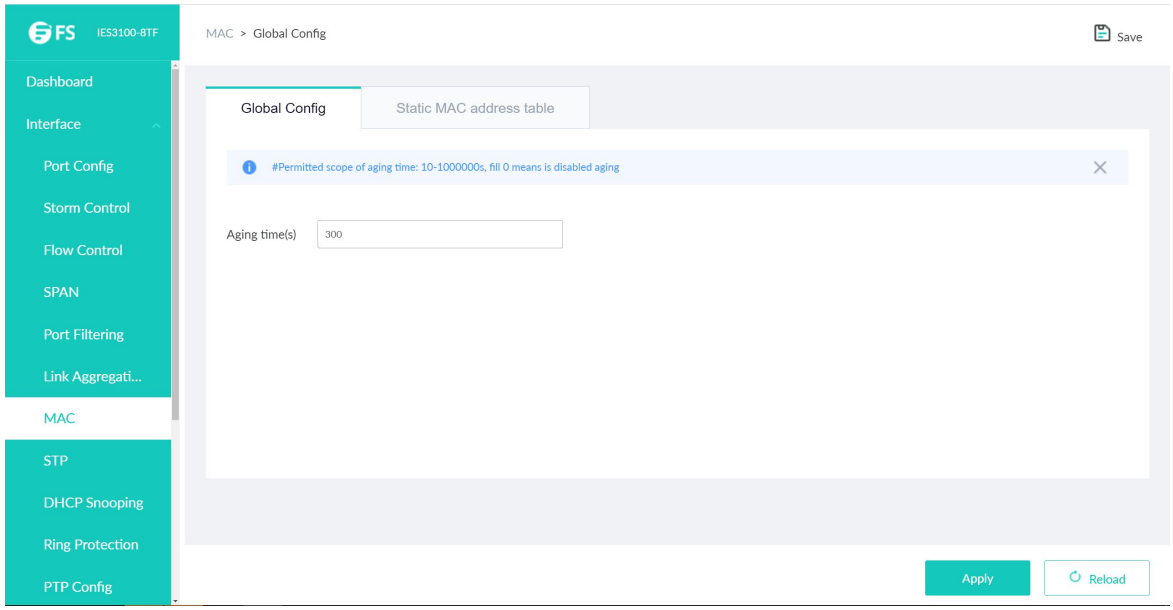
When a member port exists on the aggregation port, you can choose the aggregation mode to be Static, LACP Active or LACP Passive. You can add or delete the aggregation group member port by buttons > or <

The link backup group which has been configured the primary port cannot be configured with other port as the primary one. In the same way, the link backup group which has been configured with the backup port cannot be configured with other port as the backup one.

4.7 MAC

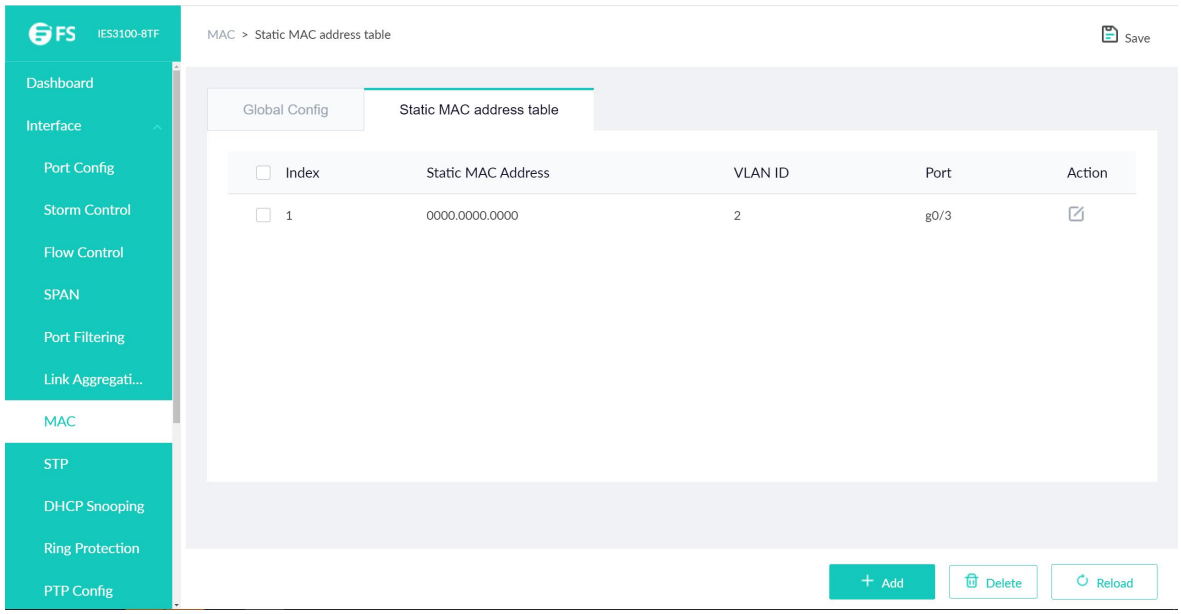
4.7.1 Global Config

Click Interface -> MAC -> Global Config at navigation bar, and then enter the configuration page as following:

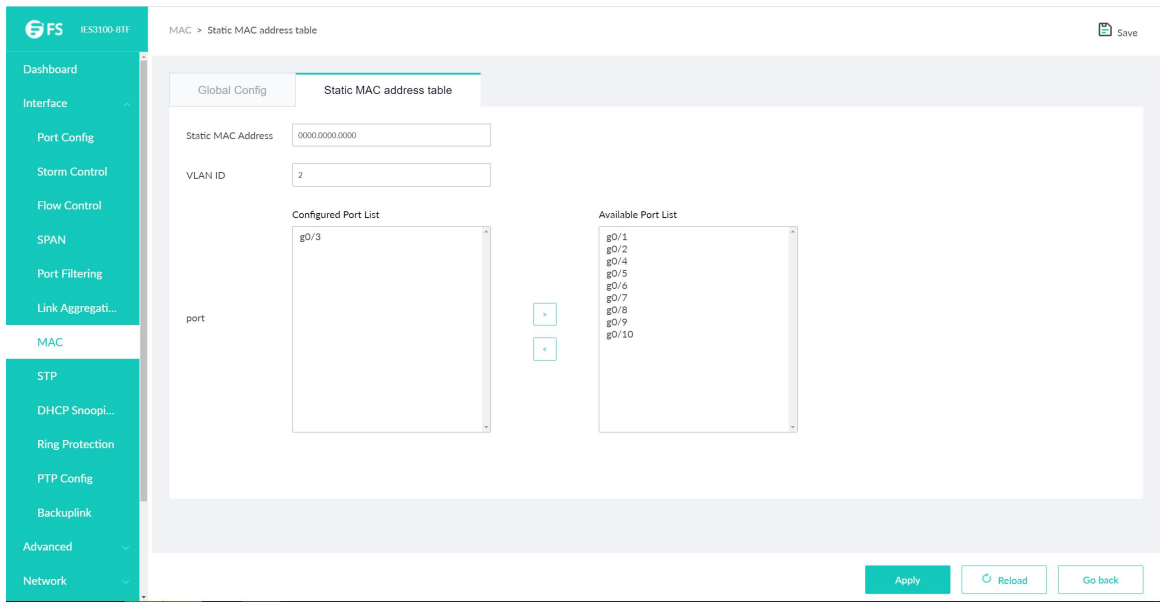


4.7.2 Static MAC address table

Click Interface -> MAC -> Static MAC address table at navigation bar in order to enter static MAC address table as following:



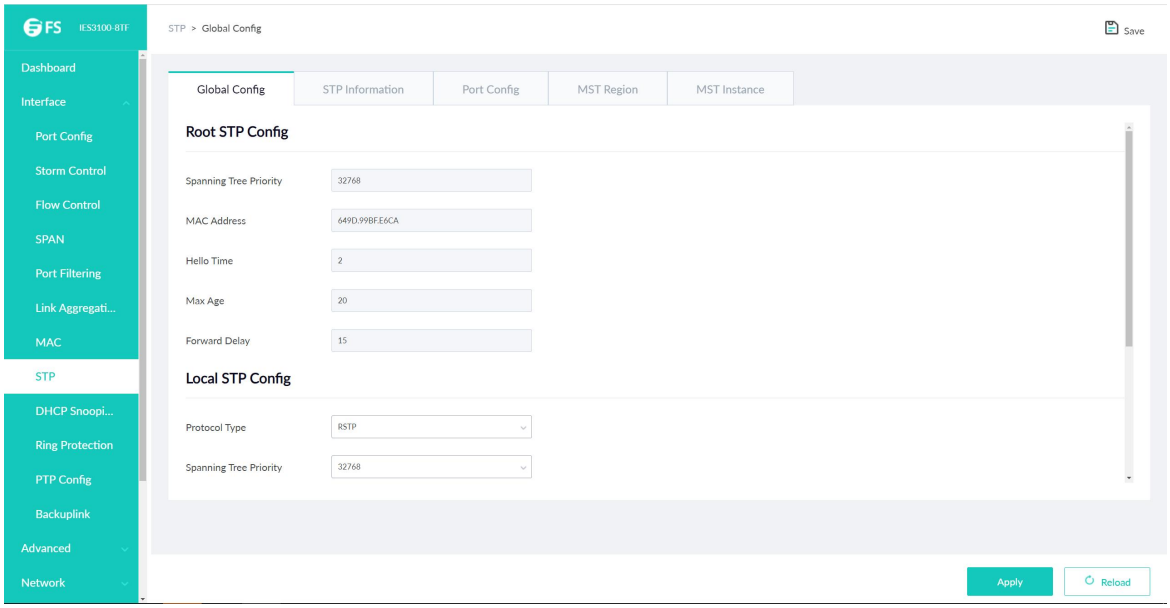
Static MAC address, VLAN ID and index are shown on the page. Click Add or edit icon to enter static MAC address configuration page and do modifications on configured static MAC address table.



4.8 STP

4.8.1 Global Config

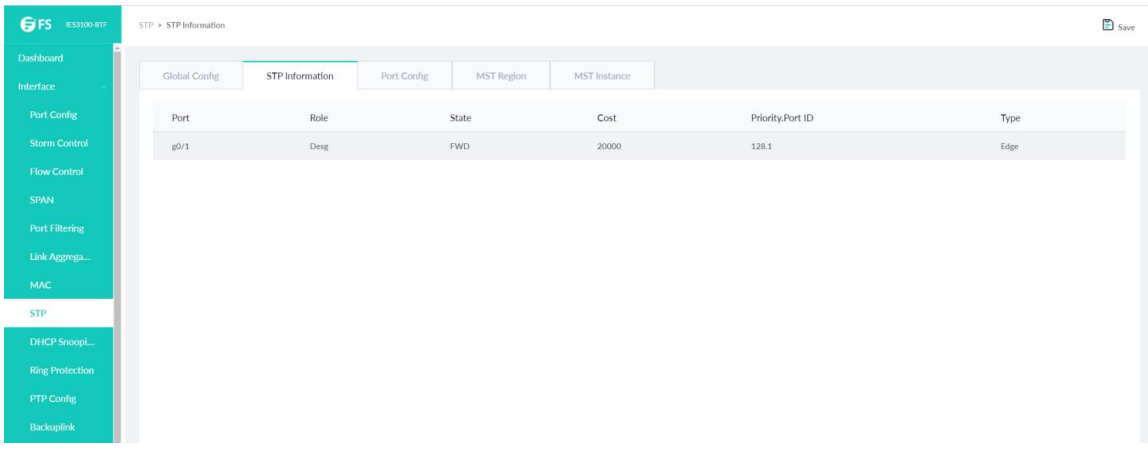
Click Interface -> STP -> Global Config at navigation bar in order, and then enter the spanning tree global configuration page as following:



The page can configure the local STP protocol, such as protocol type, spanning tree priority …etc. Click Apply to save configuration.

4.8.2 STP Information

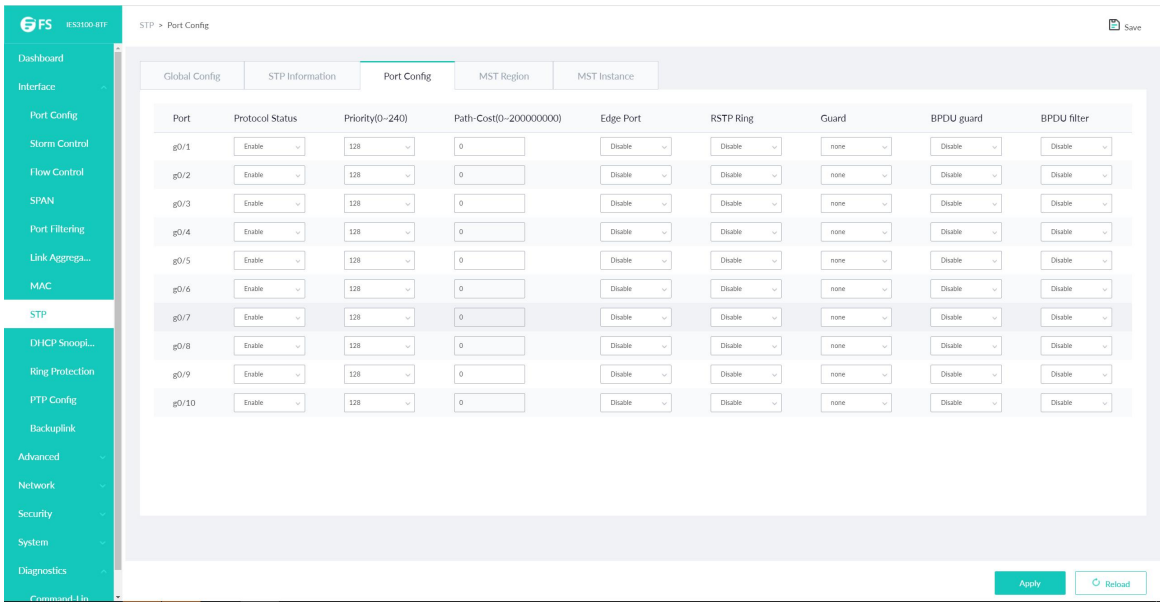
Click Interface -> STP -> STP Information at navigation bar in order, and then enter the configuration page as following:



The page lists the port information and usage status of spanning tree, Click Reload can refresh the data.

4.8.3 Port Config

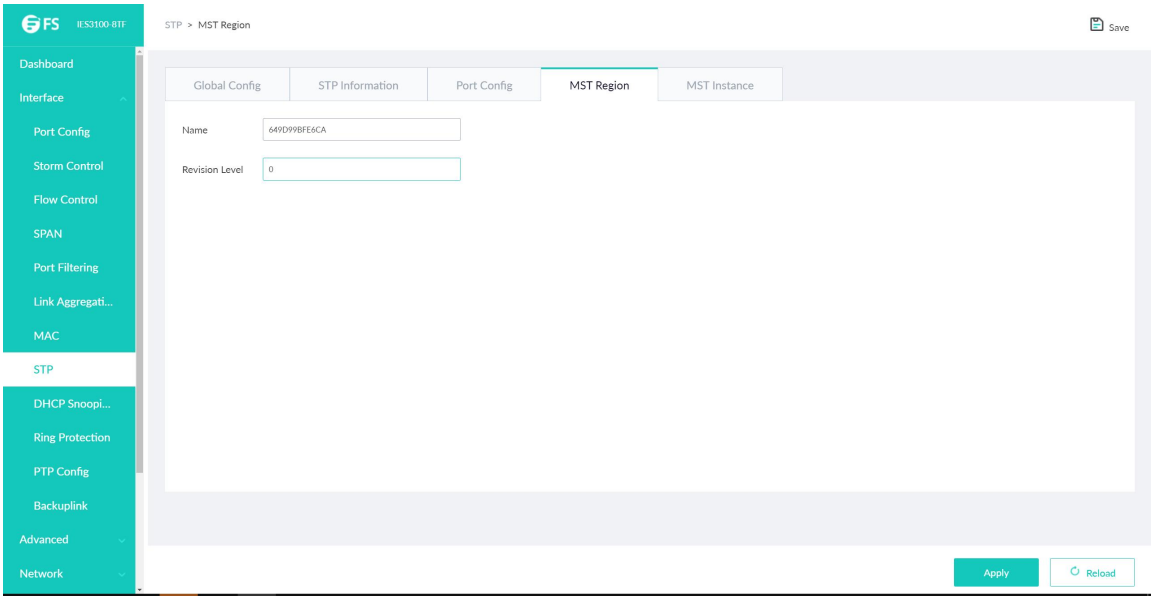
Click Interface -> STP -> Port Config at navigation bar in order, and then enter the configuration page as following:



The page lists the usage status of spanning tree per port, you can configure the parameters . click Apply then save the configuration.

4.8.4 MST Region

Click Interface -> STP -> MSTP Region at navigation bar in order, and then enter the configuration page as following:



You can configure the MST Global Revision Level in this page.

Click Apply to save configuration.

4.8.5 MST Instance

Click Interface -> STP -> MST Instance at navigation bar in order, and then enter the configuration page as following:

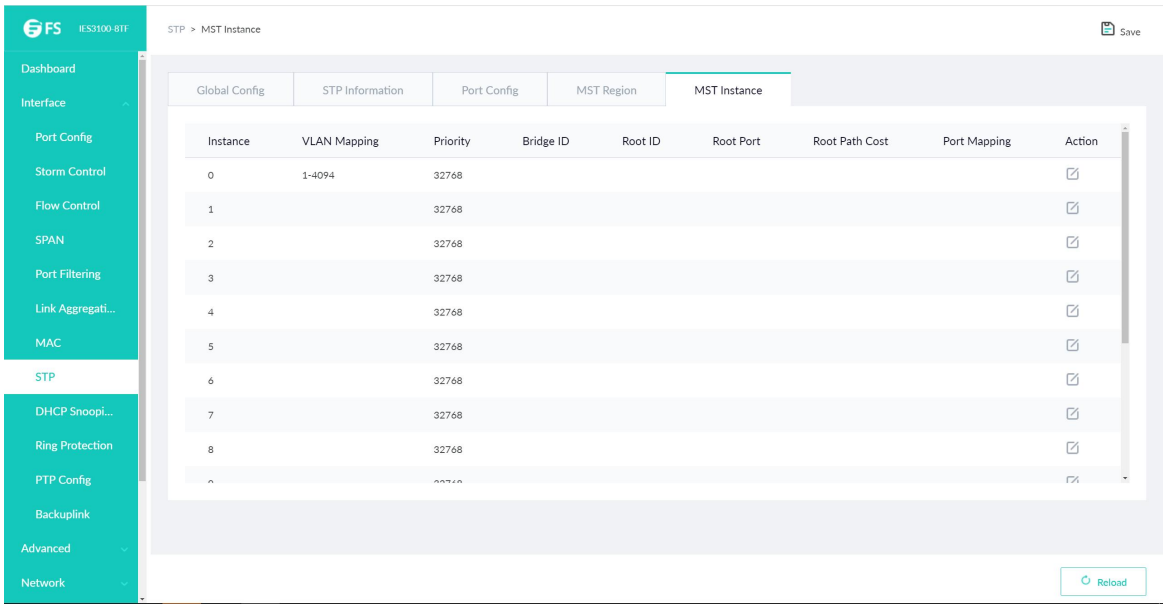
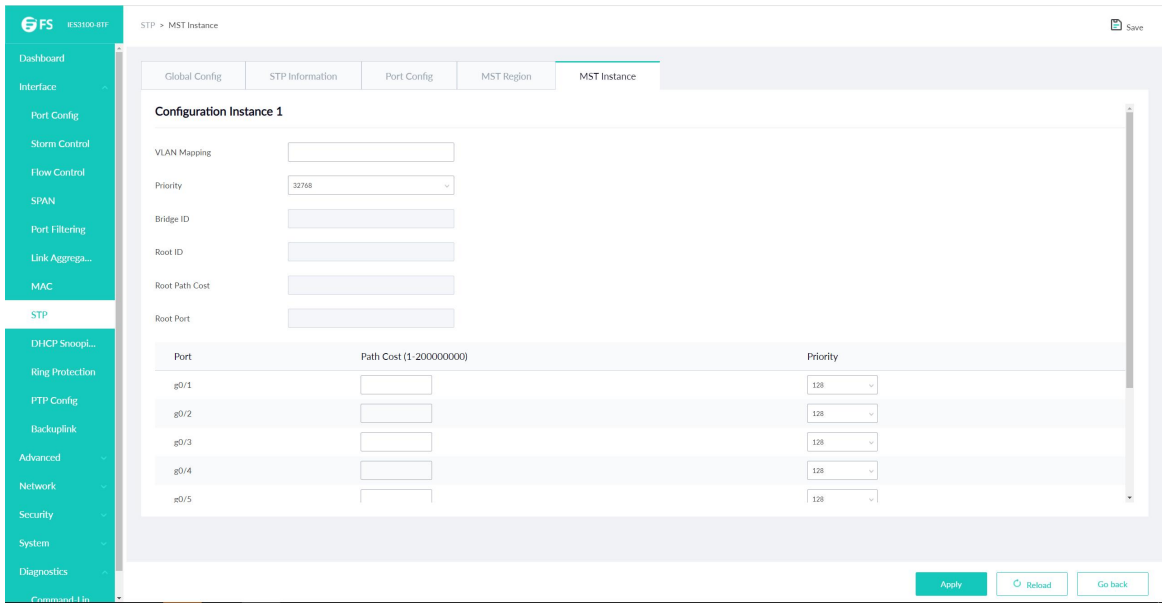


Figure: Spanning Tree MST Instance Configuration

The page lists the instance related parameter, such as VLAN mapping, Priority, Bridge ID, Root ID, Root Port, Root Path Cost, Port Mapping. Click Modify on the right of the entry and configure the MST instance.

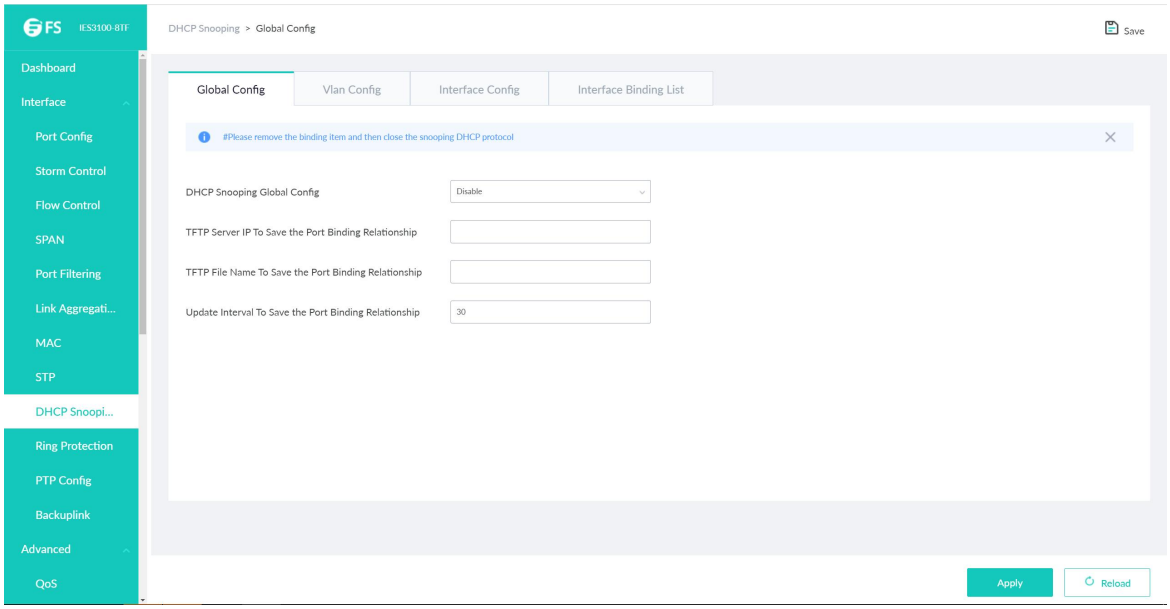


Click Apply to save configuration.

4.9 DHCP Snooping

4.9.1 Global Config

Click Interface -> DHCP Snooping -> Global Config at navigation bar in order to enter DHCP Snooping global configuration page as following:



Enable global DHCP Snooping protocol to detect all DHCP messages. Relative binding relationships forms. If client obtains addresses by the switch before the command is configured previously, switch cannot add relative binding relationships.

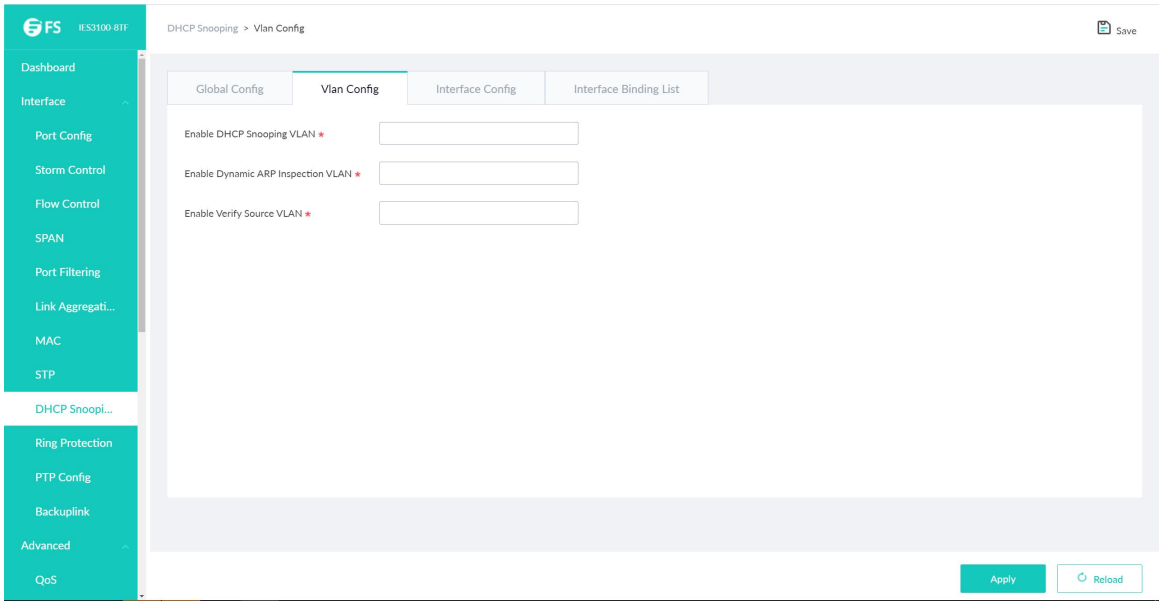
After switch's configuration is saved, restart the switch. All previous configured interface binding relationship would be dropped. At the meantime, the interface has no binding relationship, and switch would denying the forwarding of all IP messages after IP source address monitoring function is enabled. After the interface binding relationship's backup TFTP server is configured, binding relationship would be copied to server by TFTP protocol. After switch restarted, it would download binding list from TFTP server automatically to ensure network's normal operation.

When configuring backup interface binding relationships, save file name on TFTP server. Therefore, different switches can copy their interface binding relationship list to the same TFTP server.

The binding relationship list of interface's MAC address and IP address is dynamic. It is required to check whether the binding is updated. If there is (like binding items are added or deleted), backup should be done again. The default time interval is 30 minutes.

4.9.2 VLAN Configuration

Click Interface -> DHCP Snooping -> VLAN Config at navigation bar in order to enter DHCP Snooping VLAN configuration page as following:



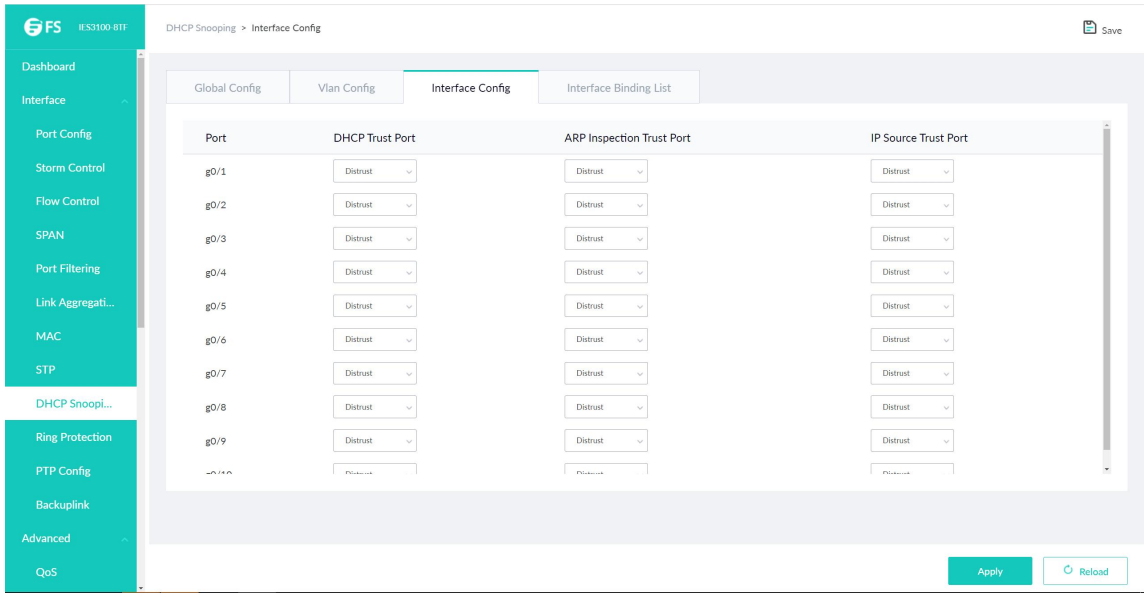
After the DHCP Snooping function is enabled on the VLAN, the DHCP messages received by all untrusted physical ports on the entire VLAN will be legally inspected. Any responded DHCP messages received by untrusted physical ports within a VLAN will be lost to prevent users from counterfeiting messages or prevent a mistaken DHCP server from assigning addresses. For the DHCP requests from untrusted ports, if the MAC address does not match the hardware address field in the messages, the requests will be considered as attacking messages counterfeited by users for the purpose of DHCP DOS (denial of service) and the switch will be abandoned too.

Monitor the ARP dynamics of all physical ports of a VLAN. If the source MAC and IP addresses of the ARP messages received by the ports do not match the MAC and IP address binding relations configured for the ports, the messages cannot be processed. The binding relations configured for the ports may be dynamic along with the DHCP or manually configured. If no MAC and IP address binding relations are configured for a physical port, the switch will refuse to forward all the ARP messages.

In a VLAN where IP source addresses are monitored, if the source MAC and IP addresses of the IP messages received by all the physical ports in the VLAN do not match the MAC and IP address binding relations configured for the ports, the messages cannot be processed. The binding relations configured for the ports may be dynamic along with the DHCP or manually configured. If no MAC and IP address binding relations are configured for a physical port, the switch will refuse to forward all the IP messages received by all the ports.

4.9.3 Interface Config

Click Interface -> DHCP Snooping -> Interface Config at navigation bar in order to enter DHCP Snooping Port configuration page as following:



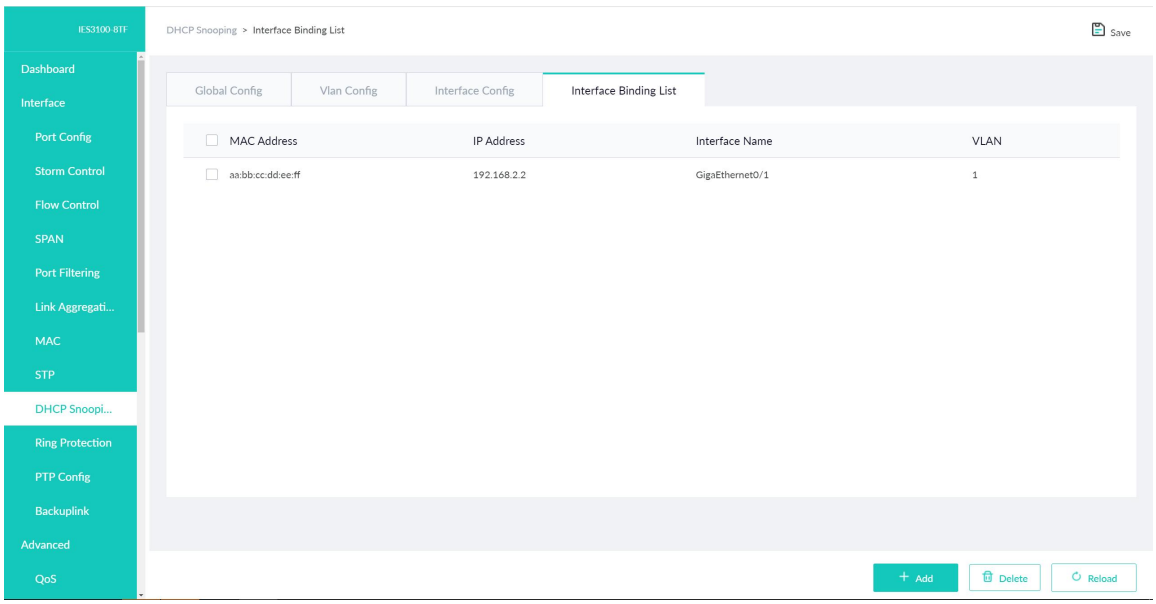
If a port is configured as the DHCP-trusted port, the DHCP messaged received by this port will not be inspected.

The ARP monitoring function will not be enabled for ARP-trusted ports. Ports are untrusted by default.

The source address inspection function is not enabled for ports trusted by IP source addresses.

4.9.4 Interface Binding List

Click Interface -> DHCP Snooping -> Interface Binding List at navigation bar in order to enter DHCP Snooping Binding configuration page as following:

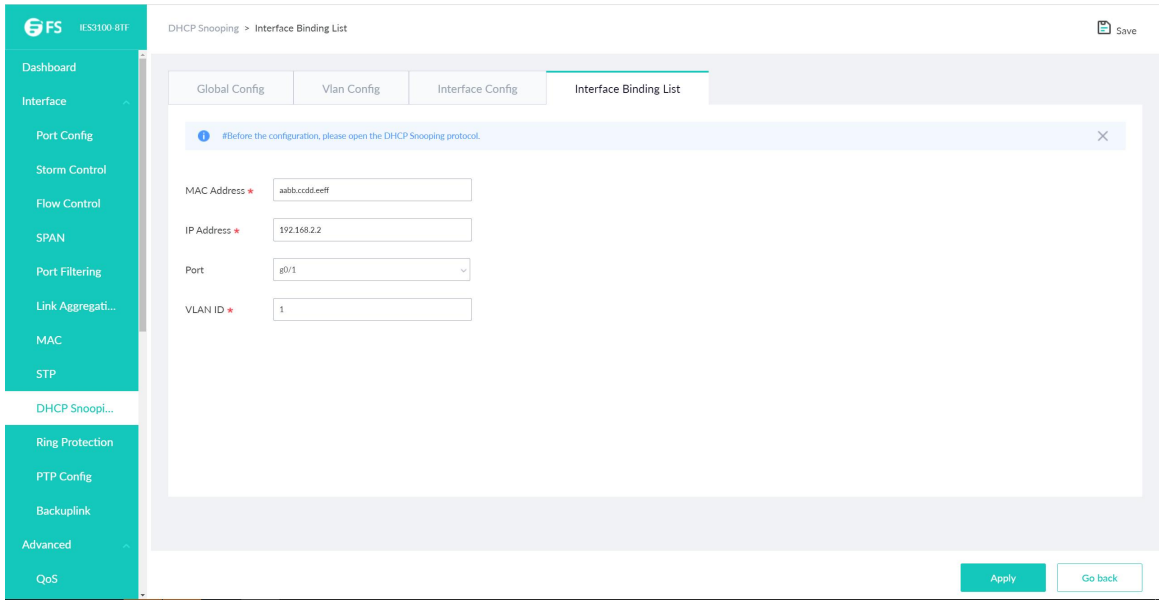


For hosts that do not use DHCP to obtain addresses, users can manually add entries for binding at the switch ports to enable the host to smoothly access the network. The no command can be used to delete the bound entries.

Entries bound manually proceed over those bound through dynamic configuration. If the MAC address of the

configured entry is the same as the MAC address of the dynamically configured entry, the latter will be updated based on the former. The MAC address is the only one index for bound entries of a port.

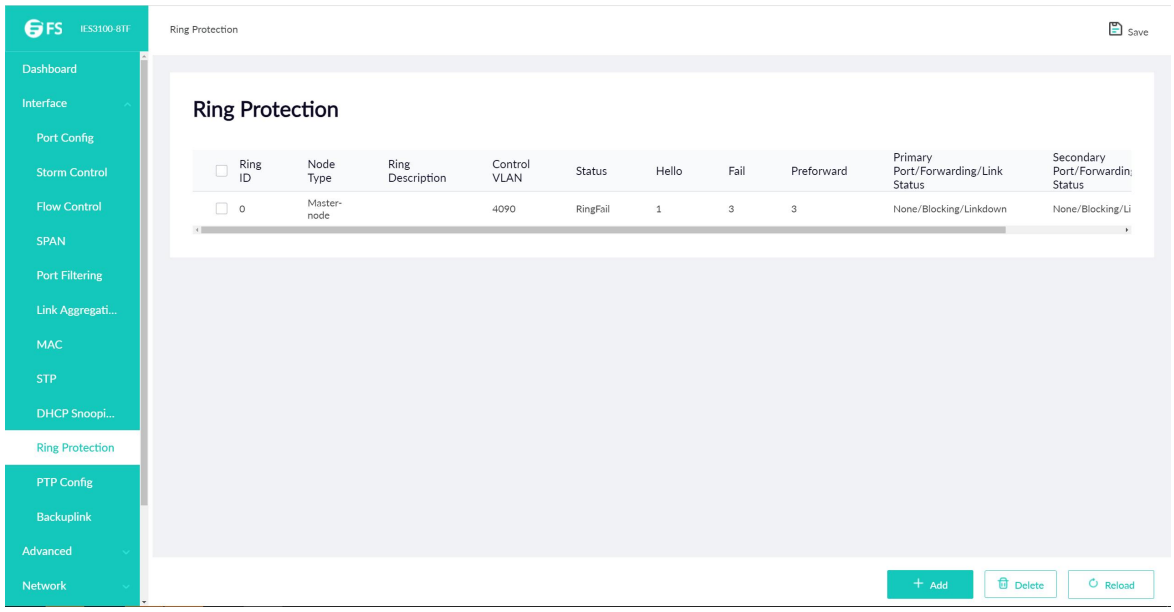
Click "Add" to create entries for binding manually configured DHCP Snooping ports.



Note: Binding entries can be created only if enabling DHCP Snooping protocol.

4.10 Ring Protection

Click Interface -> Ring Protection at navigation bar in order to enter configuration page as following:

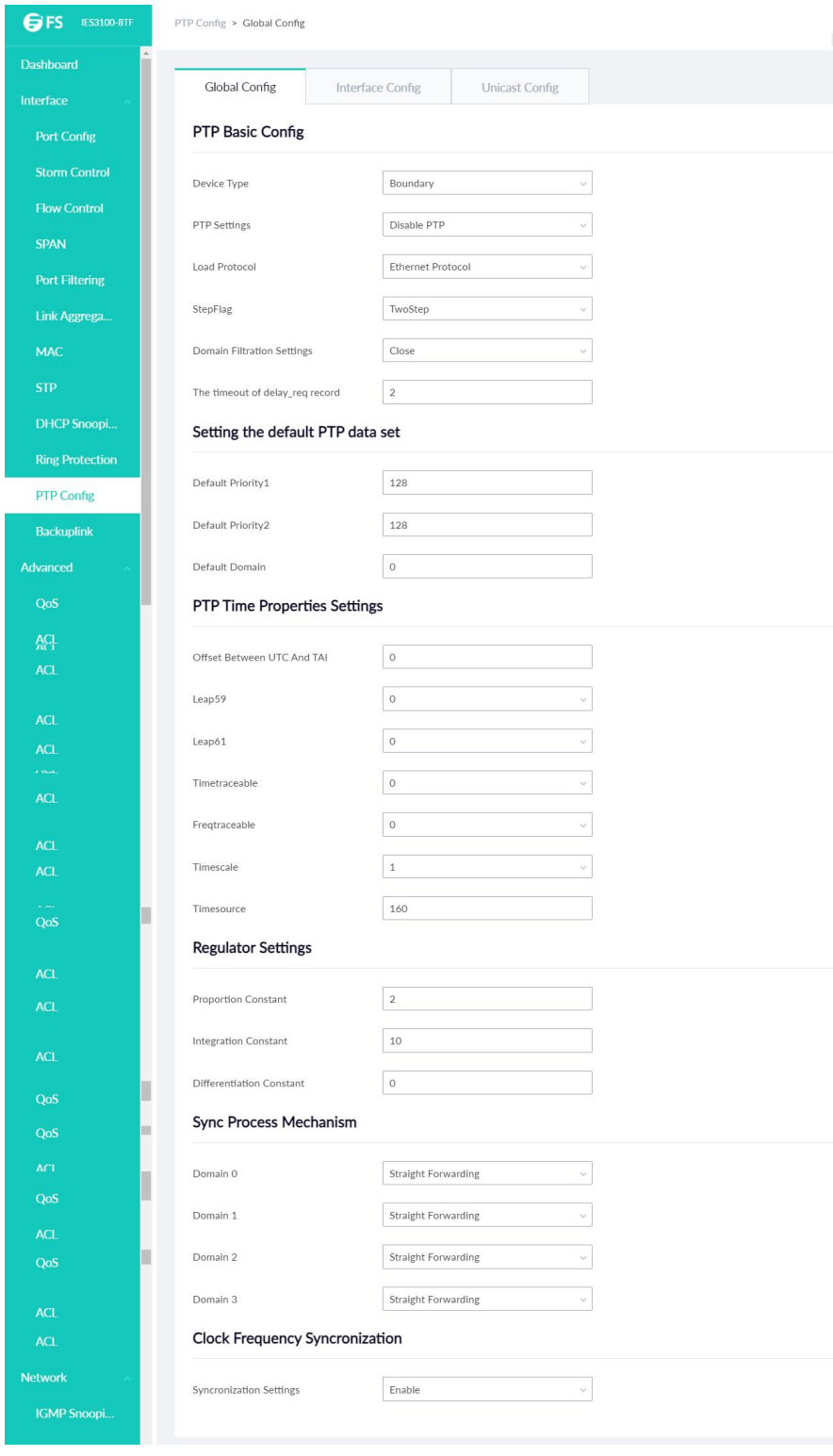


Click Add or Edit icon to enter Ring Protection configuration page and do modifications on configured Ring Protection.

4.11 PTP Config

4.11.1 Global Config

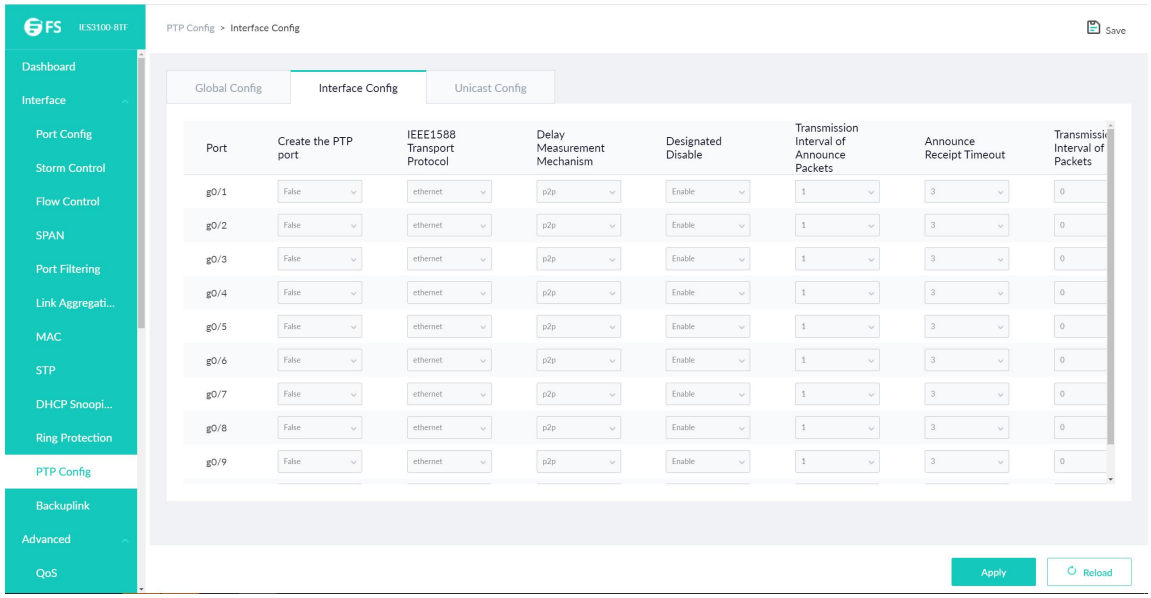
Click Interface -> PTP Config-> Global Config at navigation bar in order to enter configuration page as following:



Enabling/disabling PTP and timeout parameter can be configured at this page.

4.11.2 Interface Config

Click Interface -> PTP Config-> Interface Config at navigation bar in order to enter configuration page as following:

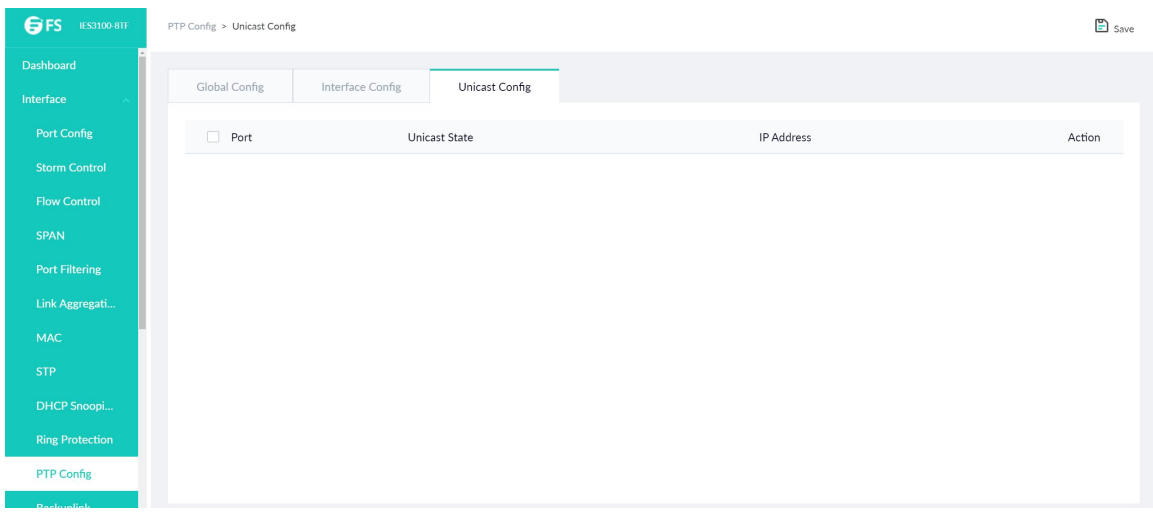


PTP port's creation, IEEE1588 Transport Protocol type, delay measurement mechanism, and etc, all of which are under port, could be configured at this page.

Note: This page could only be configured after PTP protocol is enable.

4.11.3 Unicast Config

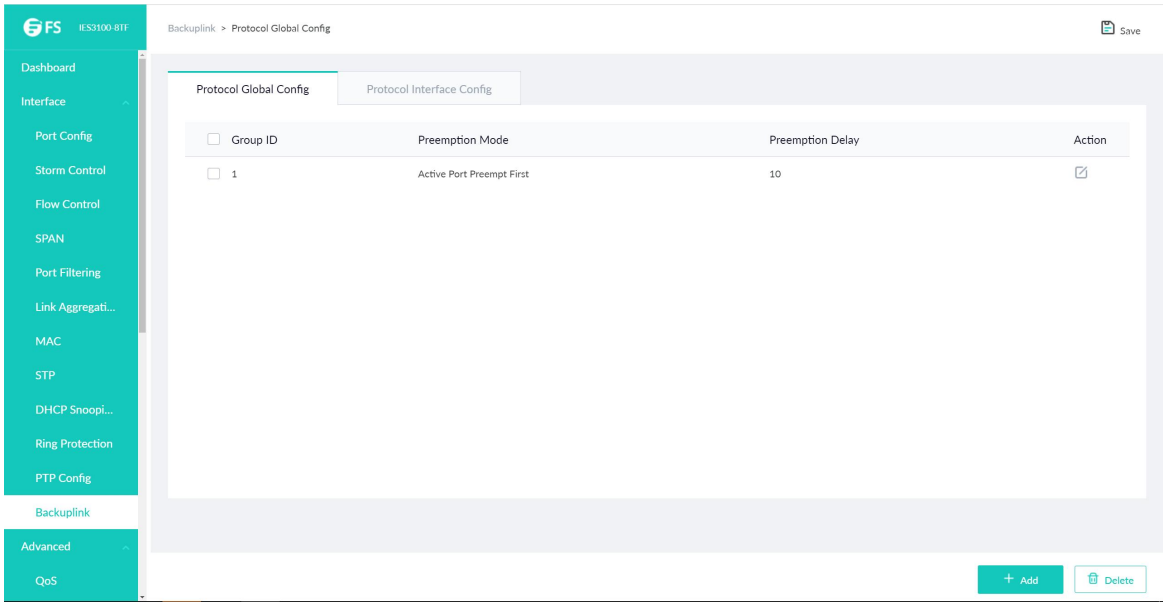
Click Interface -> PTP Config-> Unicast Config at navigation bar in order to enter configuration page as following:



4.12 Backuplink

4.12.1 Protocol Global Config

Click Interface -> Backuplink -> Protocol Global Config at navigation bar in order, and then enter the link backup protocol global configuration page as following：



The page lists current configured link backup group, including the preemption mode and the preemption delay mode. Click Add to create a new link backup group.

Click Edit Icon on the right of the entry and configure the preemption mode and the preemption delay mode of the link backup group.

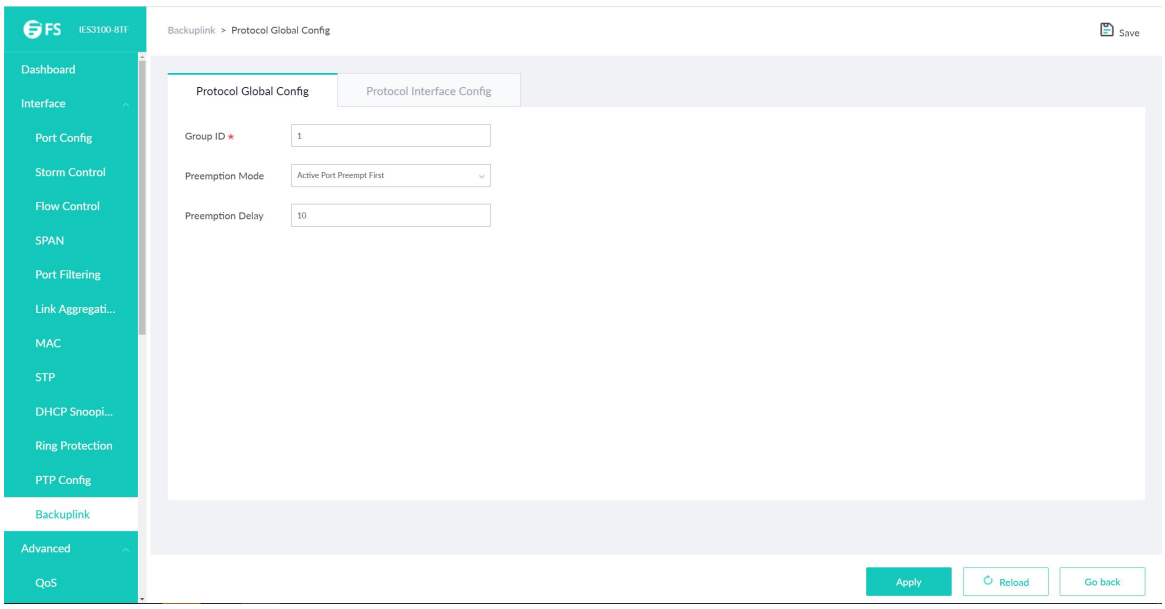


Figure: Link Backup Protocol Group Attribute Configuration

Note:

1. There are supported 8 group numbers of link backup group in this system.

2. The preemption mode of the link backup group decides the policy of the primary port and the backup port selecting forwarding packets.

4.12.2 Protocol Interface Config

Click Interface -> Backuplink -> Protocol Interface Config at navigation bar in order, and then enter the link backup protocol port configuration page as following:

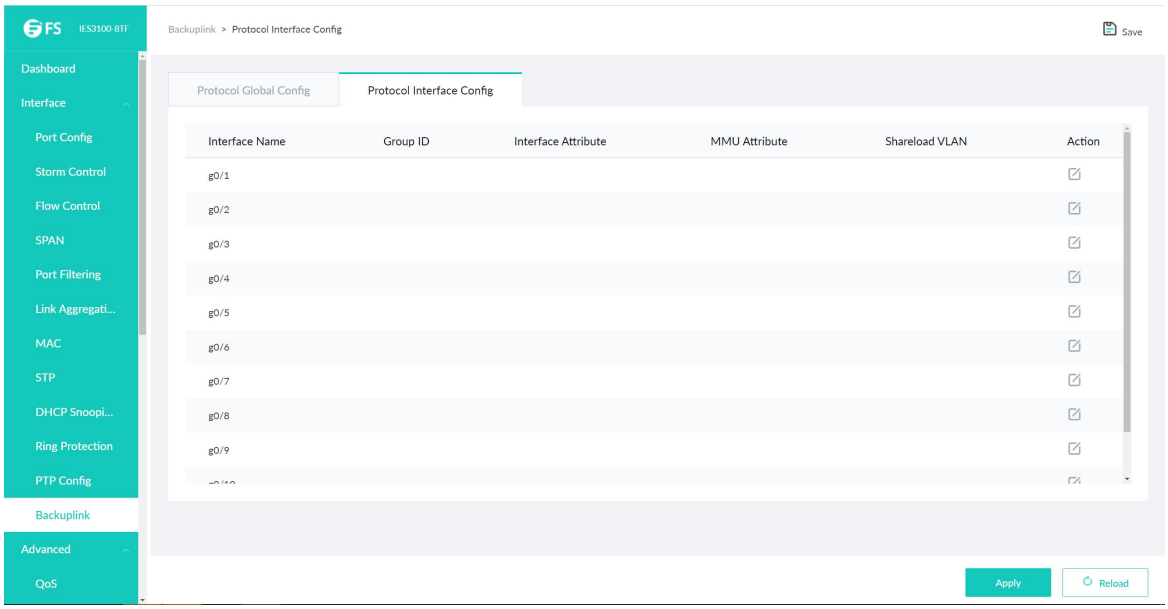
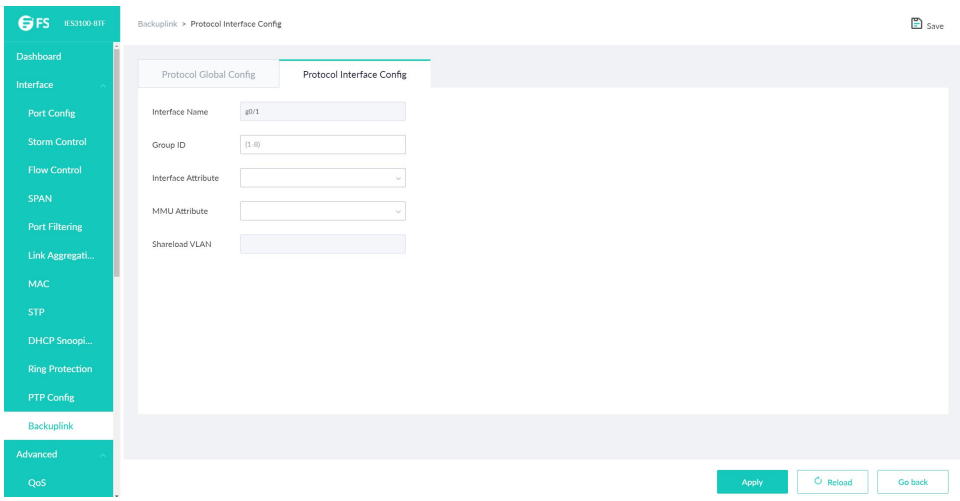


Figure: Link Backup Port List

The page lists the member port has joined the backup link group, port attribute of the member port, MMU attribute, load balance vlan. MMU sender can transmit the message to MMU receiver to make the receiver quick update the mac address table.

Click Edit icon on the right of the entry and configure the link backup protocol of the port.

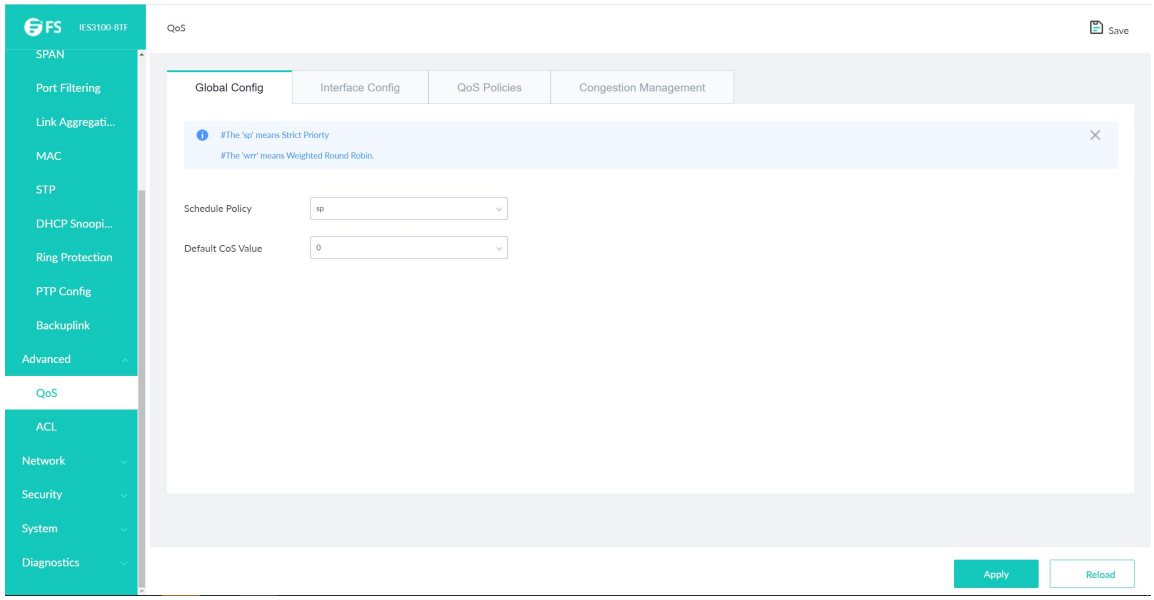


Chapter 5 Advanced

5.1 QoS

5.1.1 Global Config

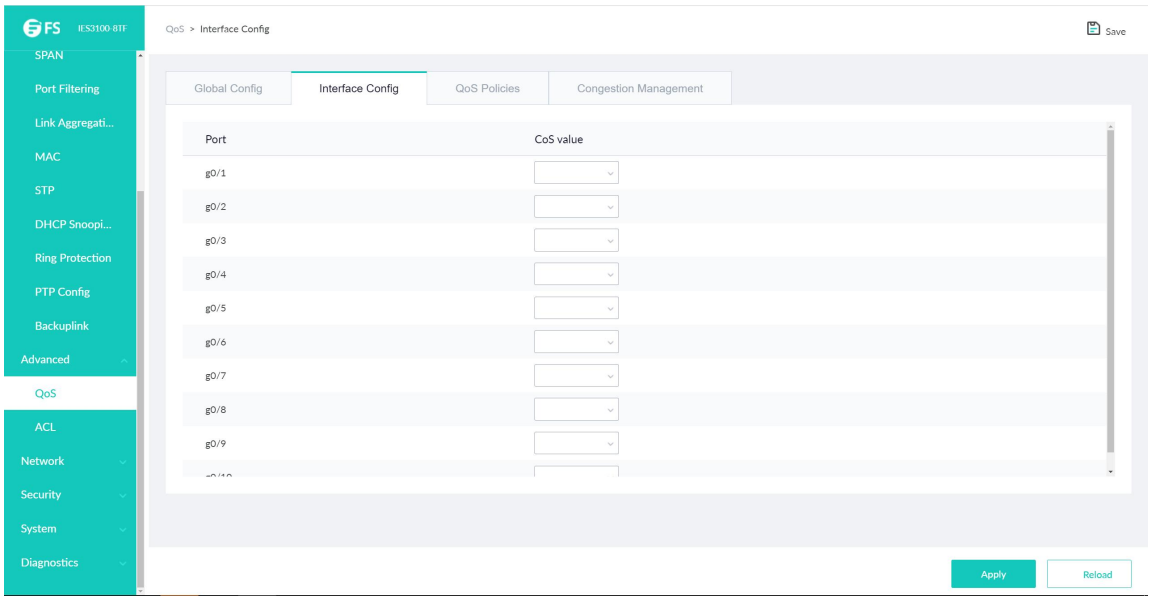
Click Advanced -> QoS -> Global Config at navigation bar in order, and then enter the configuration page as following:



You can do the setting of Schedule Policy, Default CoS Value and Trust Priority in the QoS Global page.

5.1.2 Interface Config

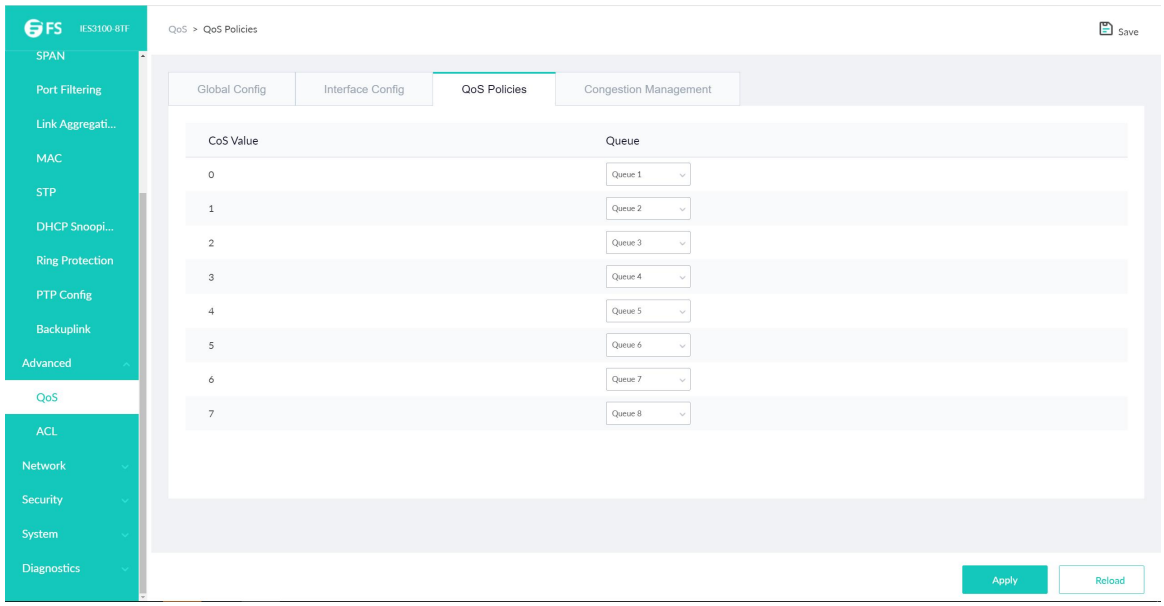
Click Advanced -> QoS -> Interface Config at navigation bar in order, and then enter the configuration page as following:



You can setting the Port CoS value by port, and then click Apply to save the changes.

5.1.3 QoS Policies

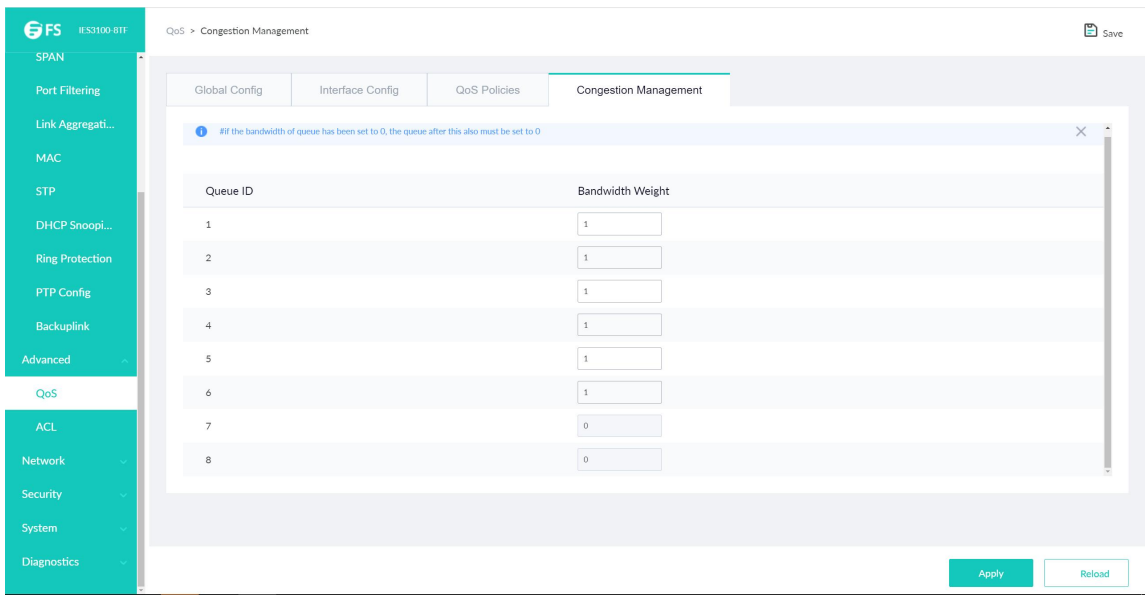
Click Advanced -> QoS -> QoS Policies at navigation bar in order, and then enter the configuration page as following：



click Apply to save all 802. 1D/p mapping configurations.

5.1.4 Congestion Management

Click Advanced -> QoS -> Congestion Management at navigation bar in order, and then enter the configuration page as following： click Apply can save all configuration.

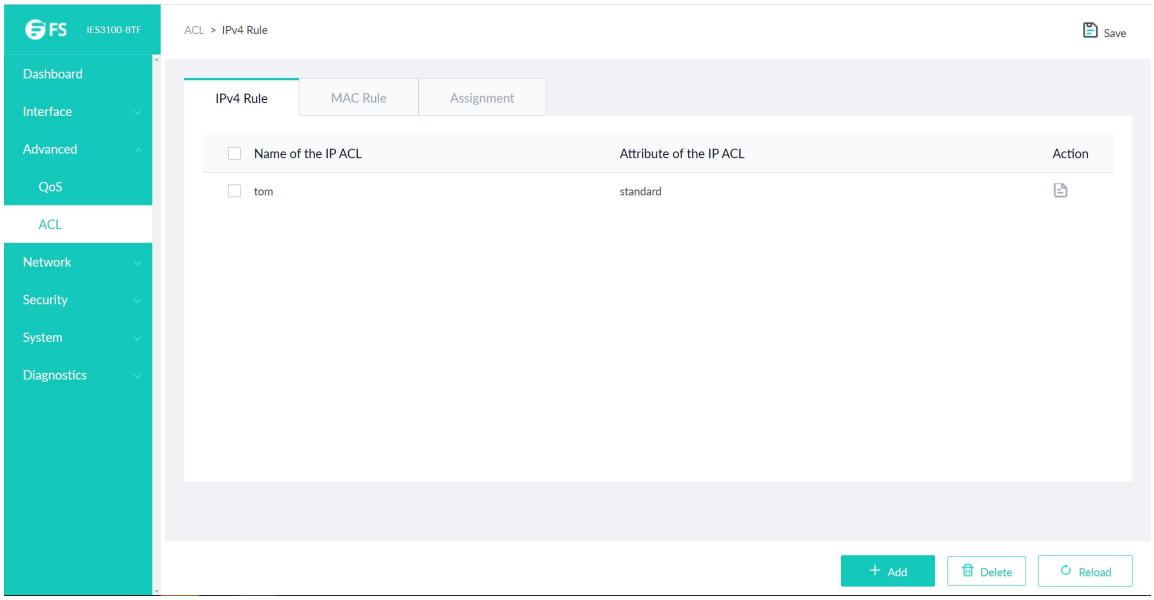


Note：If one Queue ID setting the bandwidth weight to Zero value, then the weight value must only can setting Zero that behind this Queue ID.

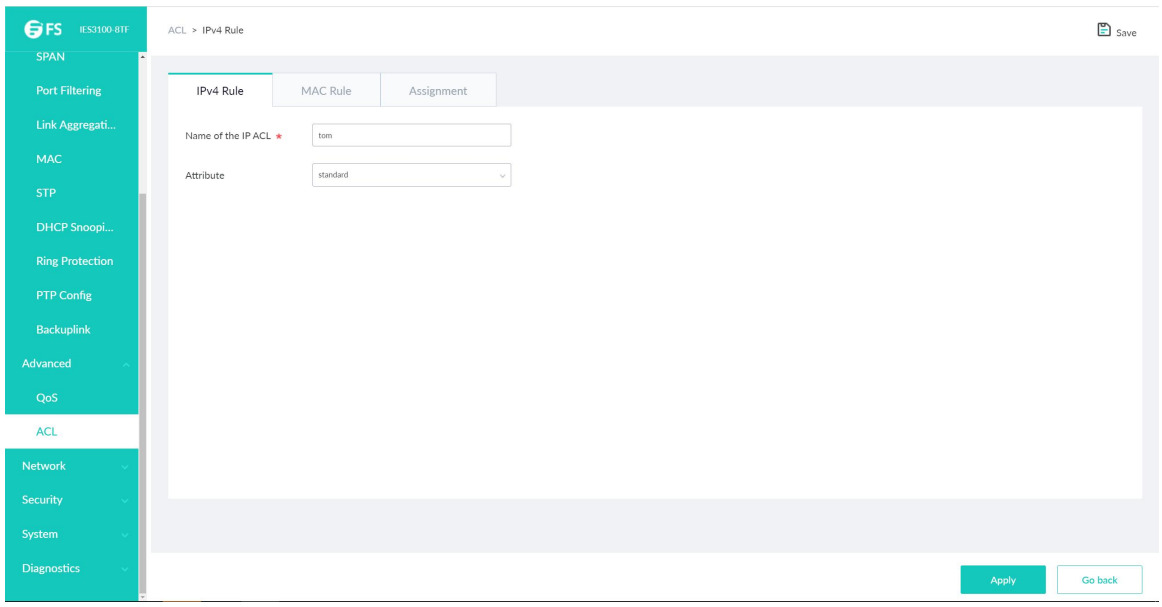
5.2 ACL

5.2.1 IPv4 Rule

Click Advanced -> ACL -> IPv4 Rule at navigation bar in order to enter IPv4 rules' page as following:



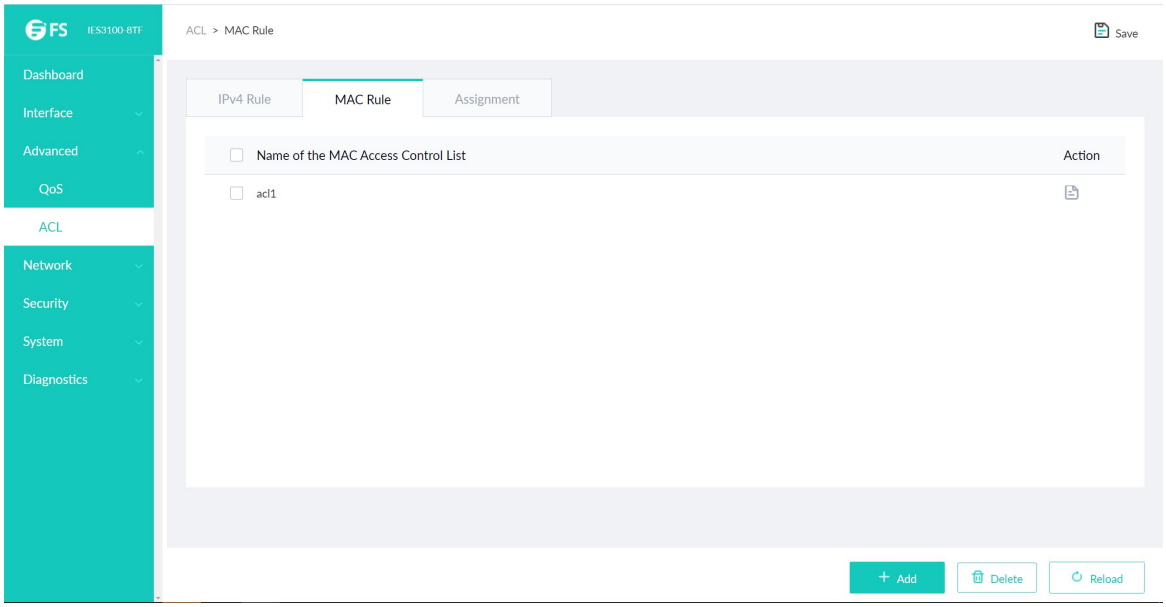
Click Add to create an IP access control list. Click Delete to delete the access control list.



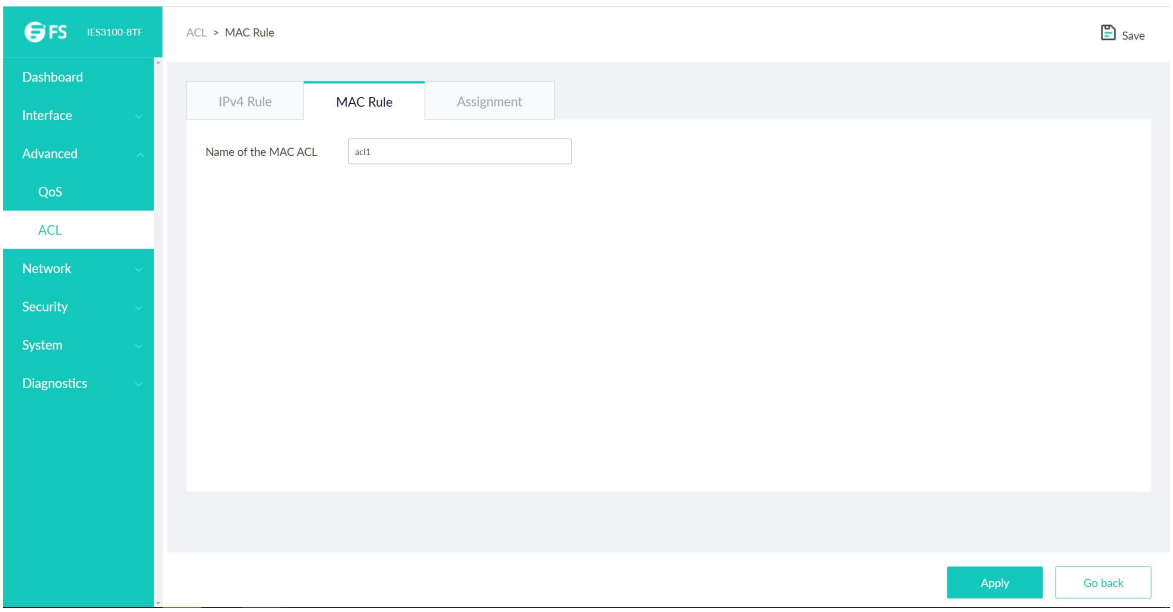
Click Edit to enter relative IP access control list to do rules' setup.

5.2.2 MAC Rule

Click Advanced -> ACL -> MAC Rule at navigation bar in order to enter MAC rules' page as following:

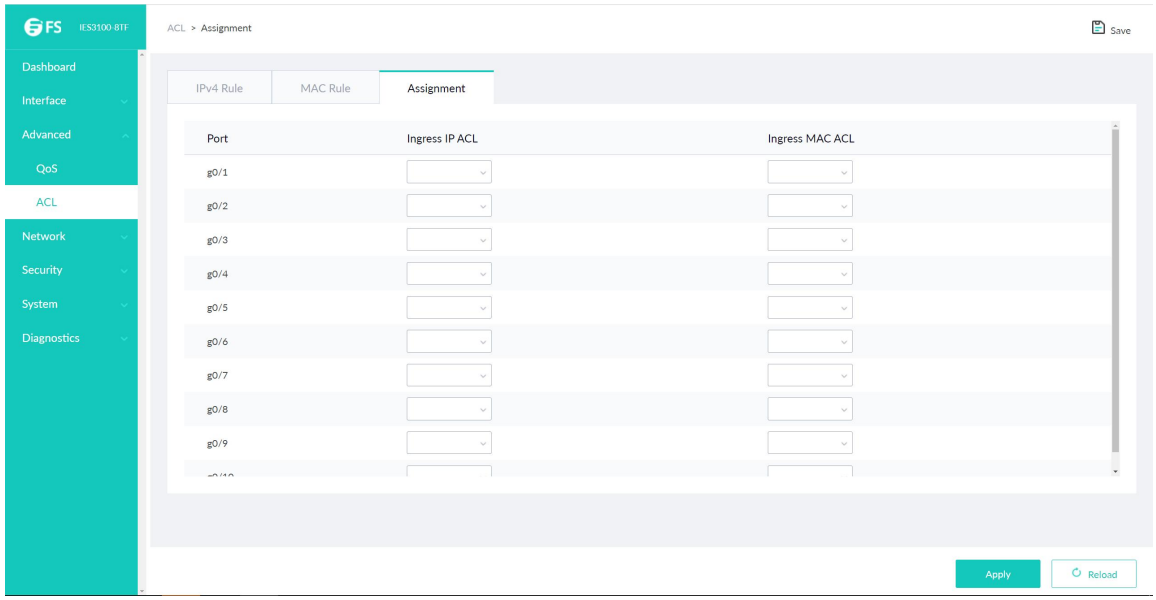


Click Add to create a MAC access control list. Click Delete to delete the access control list.



5.2.3 Assignment

Click Advanced -> ACL -> Assignment at navigation bar in order to enter distribution page of access control list as following:

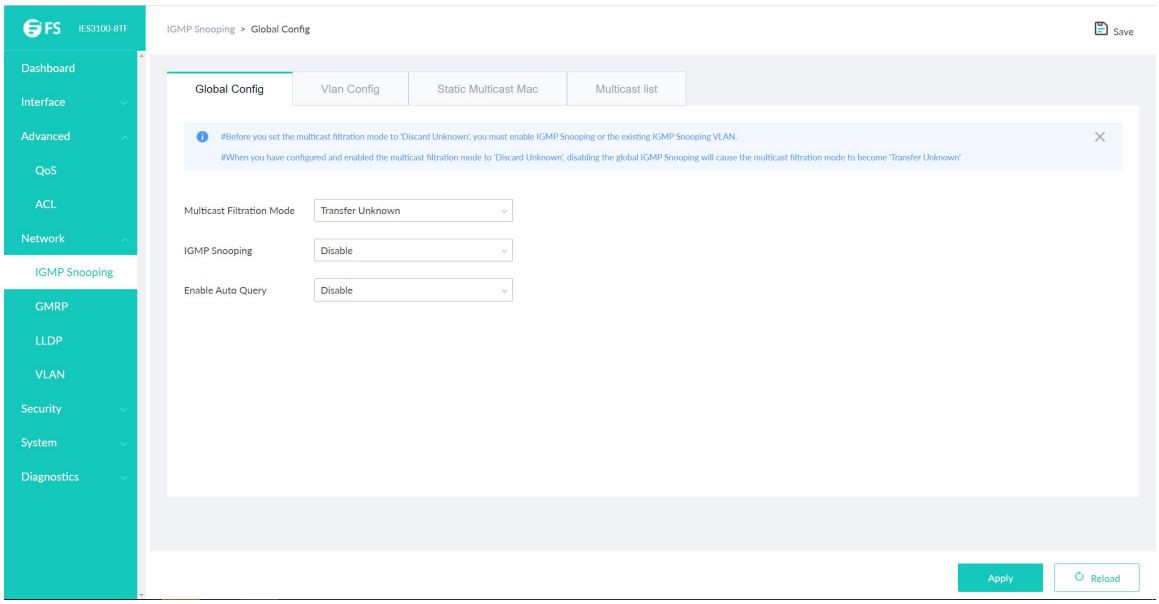


Chapter 6 Network

6.1 IGMP Snooping

6.1.1 Global Config

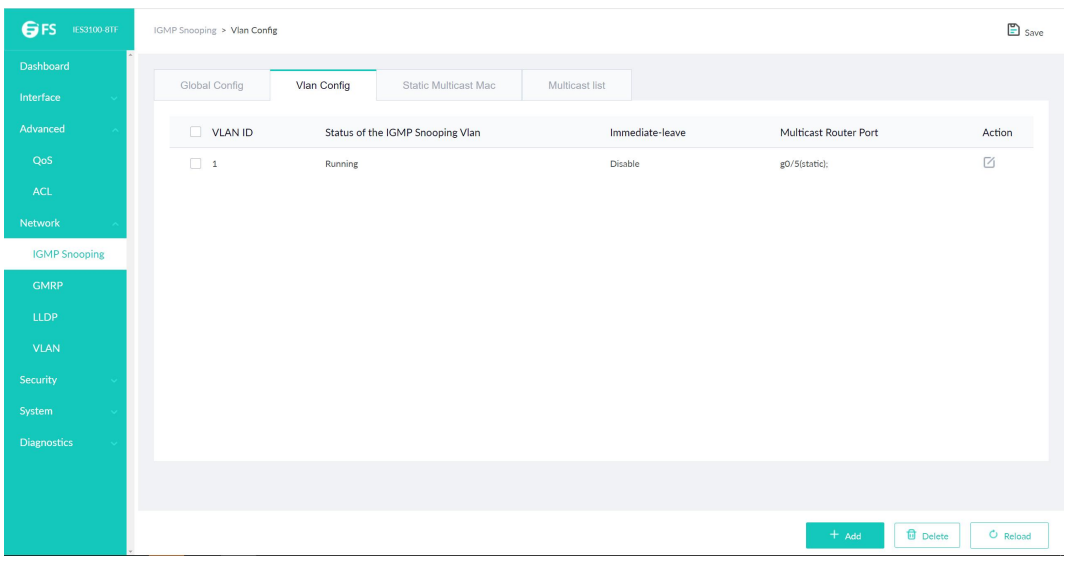
Click Network -> IGMP Snooping -> Global Config, at navigation bar in order, and select IGMP Snooping tab page to enter IGMP Snooping configuration page as following:



Whether switch forwarding unknown multicast, whether enabling IGMP-Snooping and whether taken as IGMP's Querier can be configured at this page.

6.1.2 Vlan Config

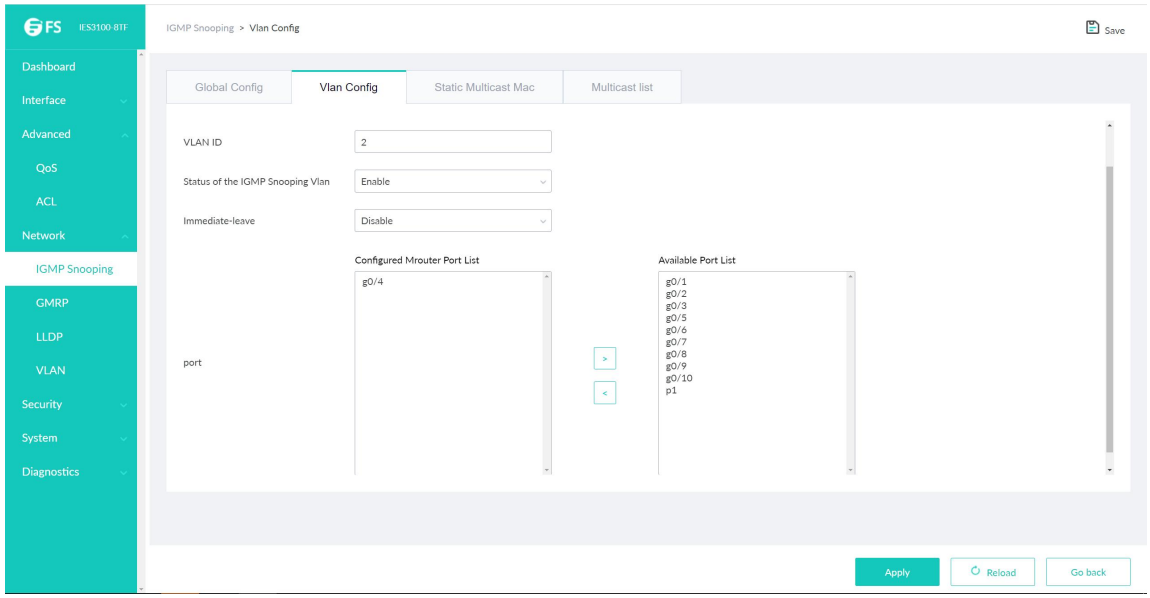
Click Network -> IGMP Snooping -> Vlan Config, at navigation bar in order, and select IGMP Snooping VLAN tab page to enter IGMP Snooping VLAN configuration page as following:



If you Click Add, 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 Delete, a selected IGMP-Snooping VLAN can be deleted;

if you click Edit icon, you can modify the member port, running status and immediate-leave of IGMP-Snooping VLAN.

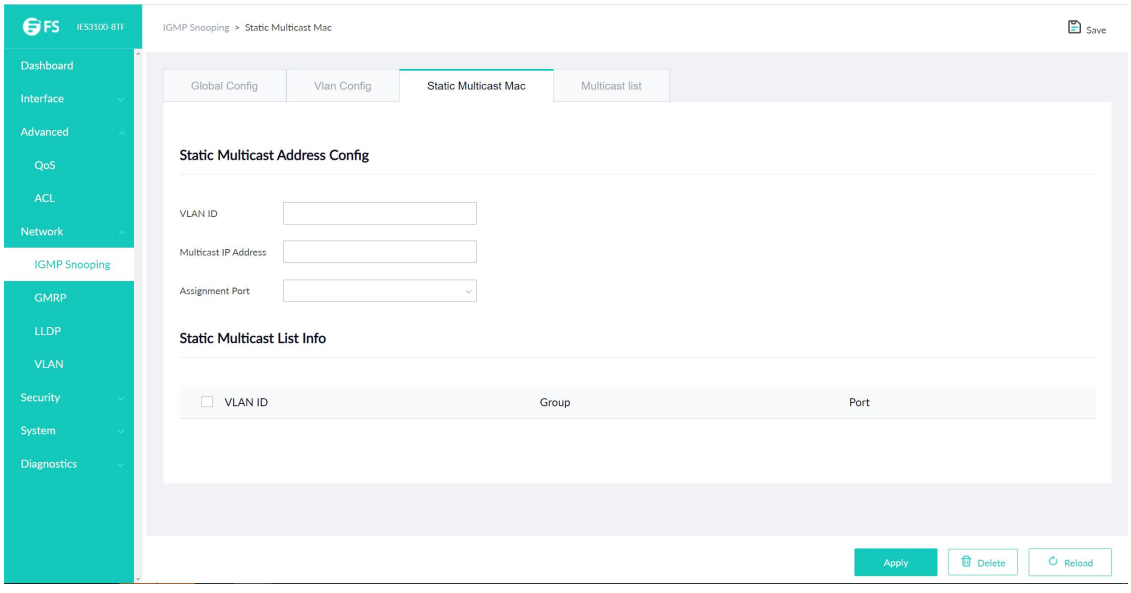


When an IGMP-Snooping VLAN is created, its VLAN ID can be modified; but when the IGMP-Snooping VLAN is modified, its VLAN ID cannot be modified.

You can click">" and "<" to delete and add a routing port.

6.1.3 Static Multicast Mac

Click Network -> IGMP Snooping -> Static Multicast Mac, at navigation bar in order, and select static multicast address tab page to enter static multicast address page as following:

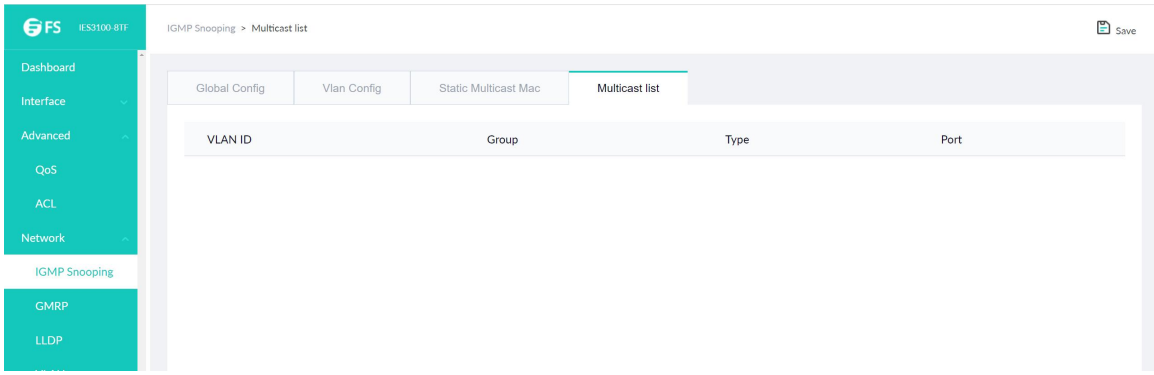


On this page, the currently existing static multicast groups and port groups in each static multicast group are shown.

Click Reload to refresh the contents in the list.

6.1.4 Multicast list

Click Network -> IGMP Snooping -> Multicast list, at navigation bar in order, and select multicast member list tab page to enter multicast member list configuration page as following:



The multicast groups in current network and ports'set where every group member exists counted by IGMP-Snooping, are shown on this page.

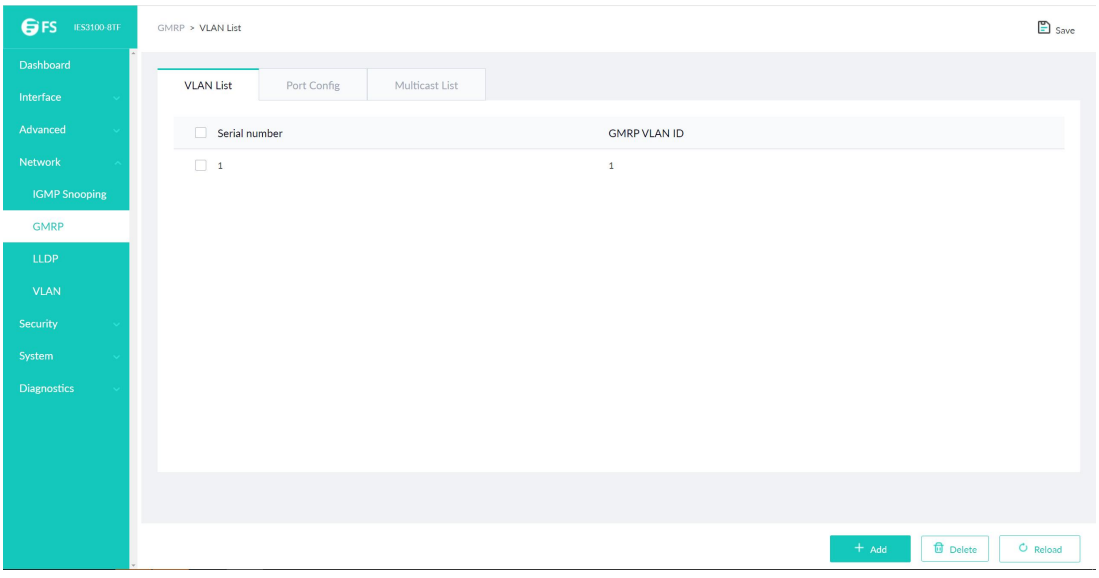
Click Reload to refresh the contents in the list.

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 orTelnet.

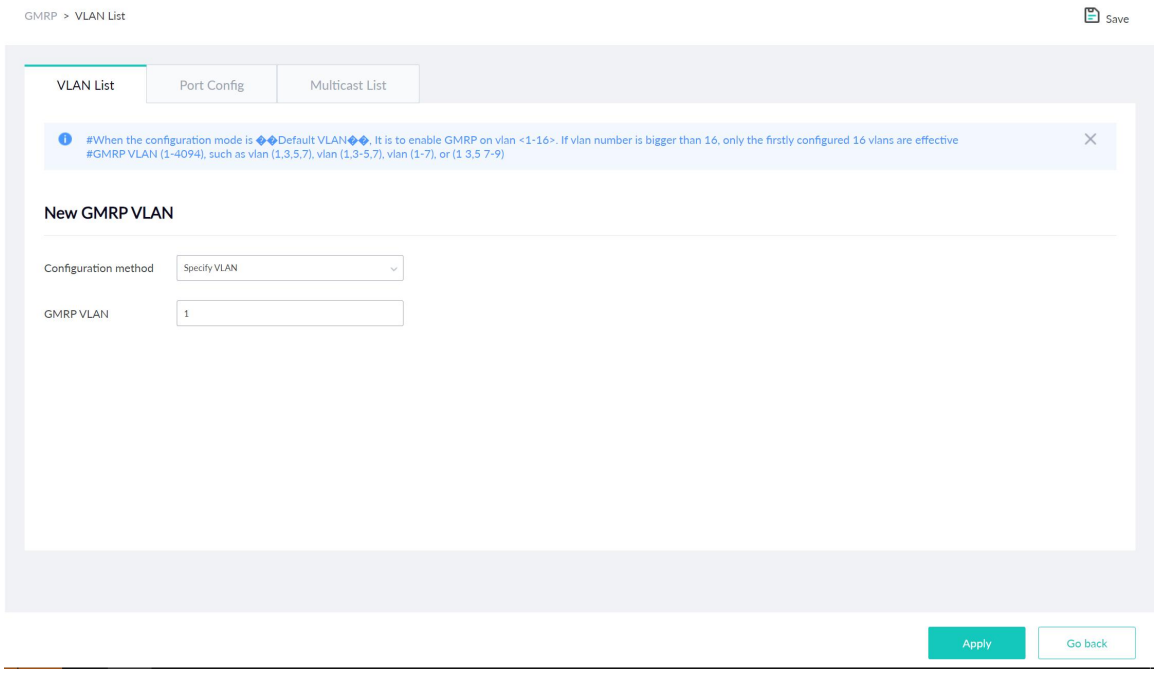
6.2 GMRP

6.2.1 VLAN List

Click Network -> GMRP-> VLAN List at navigation bar in order, and then enter the VLAN List page , as shown as below figure:



Click Add to create new GMRP VLAN item.

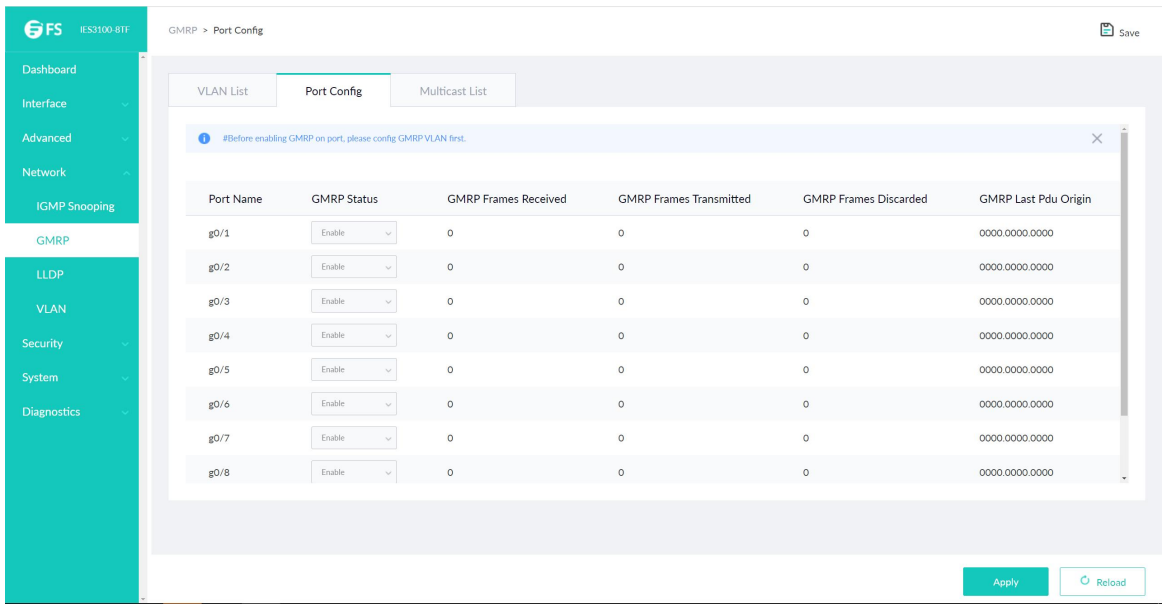


Click Edit icon to modify GMRP VLAN item;

Click Delete to delete the selected GMRP VLAN item.

6.2.2 Port Config

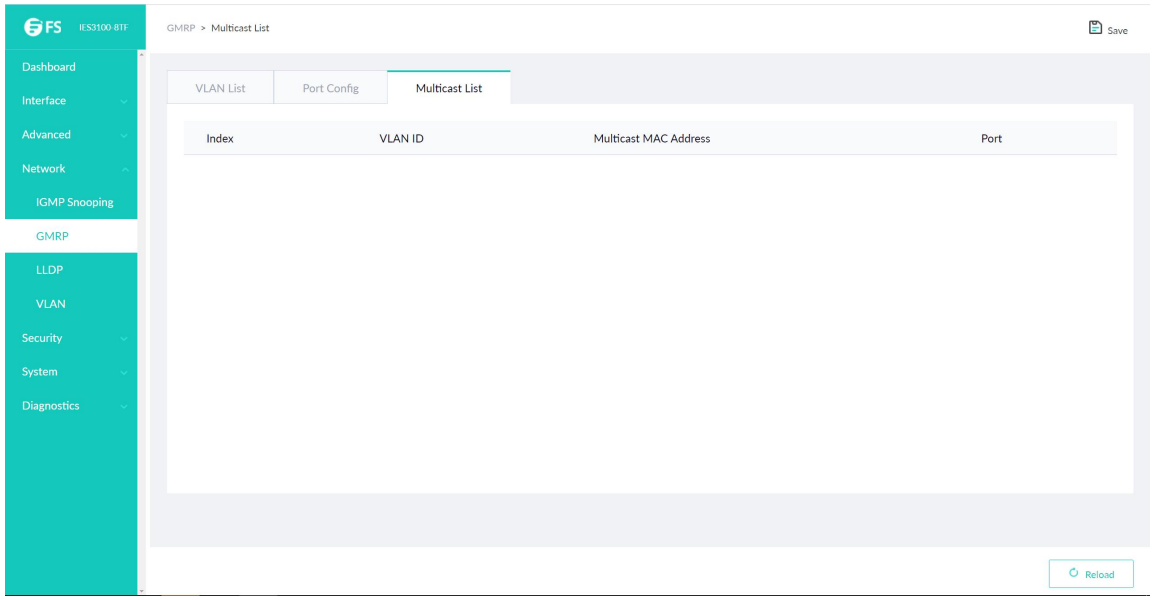
Click Network -> GMRP-> Port Config at navigation bar in order, and then enter the Port Config page , as shown as below figure:



The page lists the GMRP status of per port, you can configure the parameters . click Apply then save the configuration.

6.2.3 Multicast List

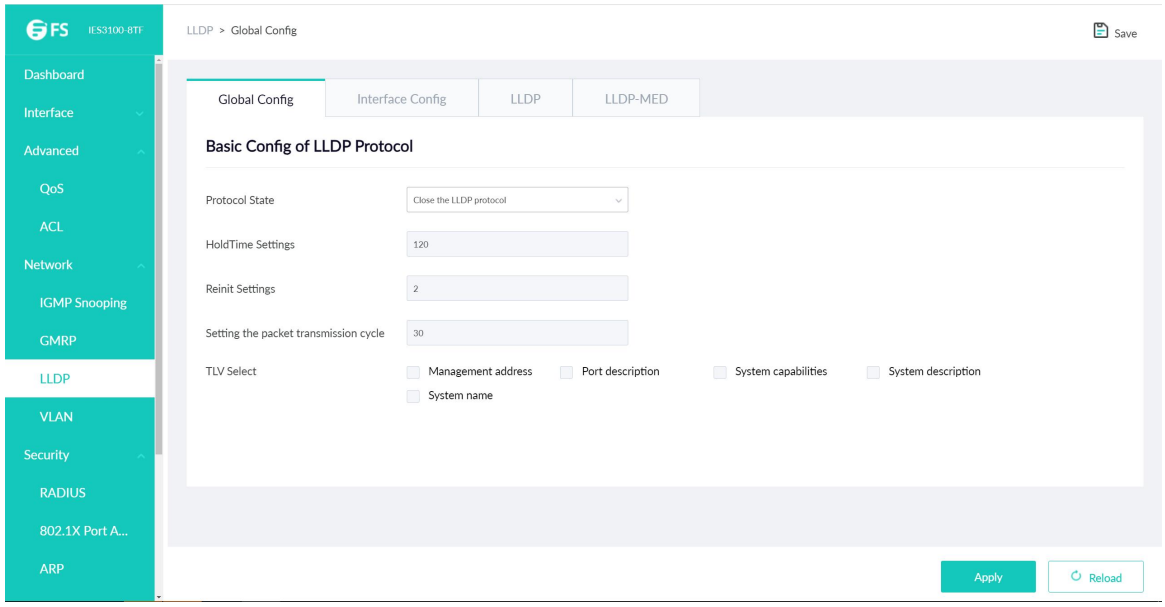
Click Network -> GMRP-> Multicast List at navigation bar in order, and then enter the Multicast List page , as shown as below figure:



6.3 LLDP

6.3.1 Global Config

Click Network -> LLDP -> Global Config at navigation bar in order, and then enter the LLDP configuration page as following:



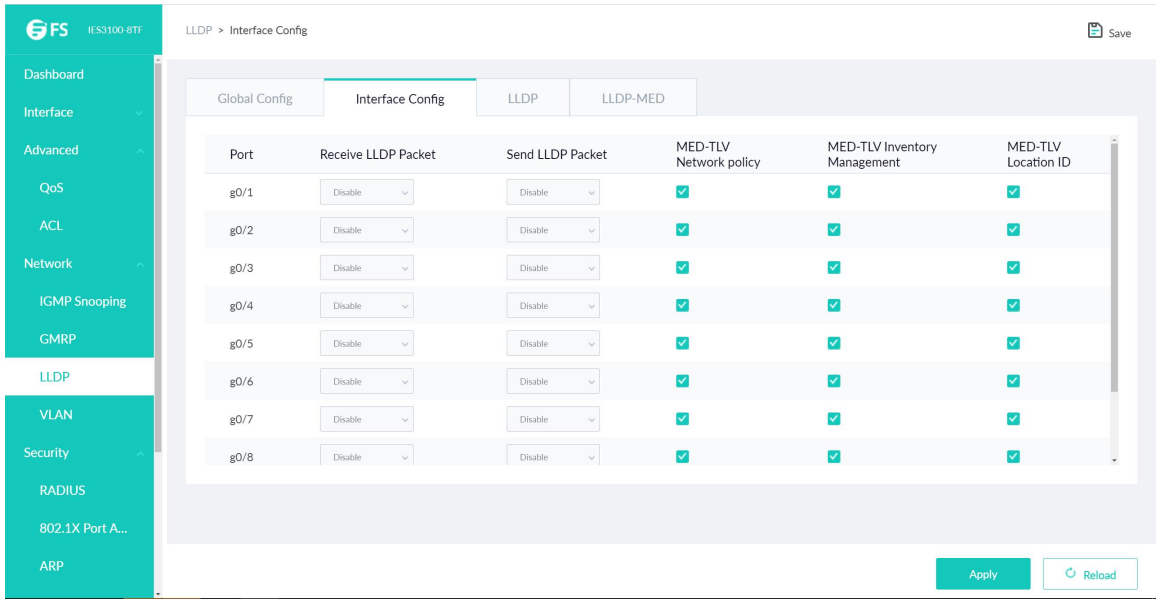
You can enable or disable the LLDP protocol. You cannot configure the LLDP protocol of the port when LLDP is disabled.

HoldTime refers to the ttl value for transmitting the LLDP message. The default value is 120s.

Reinit refers to the transmission delay of LLDP. The default value is 2s.

6.3.2 Interface Config

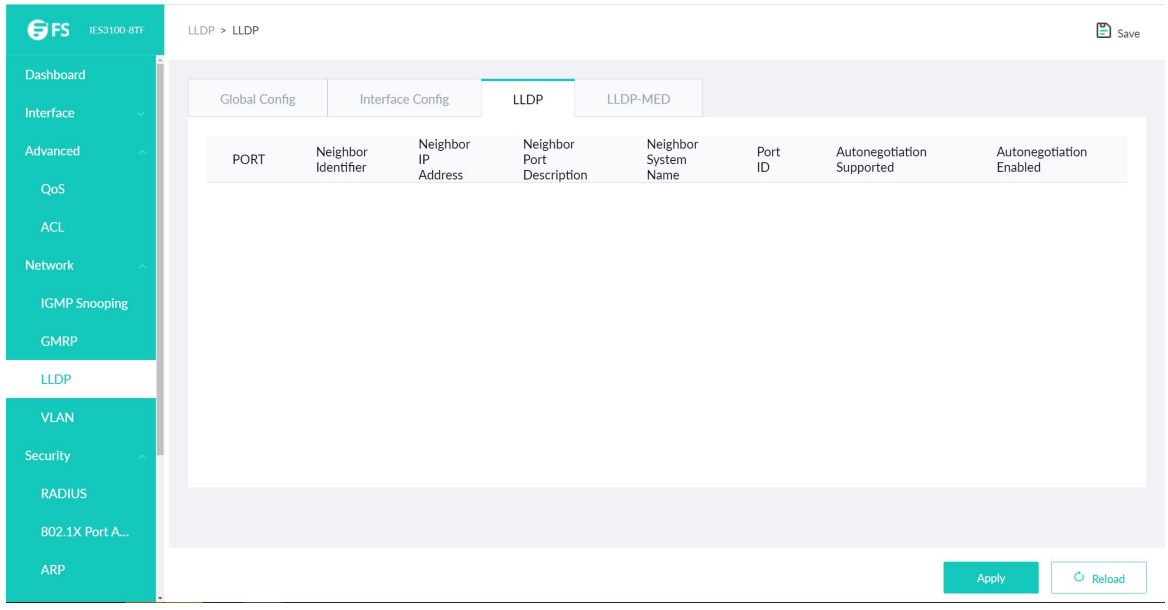
Click Network -> LLDP -> Interface Config at navigation bar in order, and then enter the LLDP port configuration page as following:



LLDP port configuration can enable or disable the port transmitting LLDP packets, the default value was disable both of receive and send LLDP packet. The default of MED-TLV is enabled.

6.3.3 LLDP

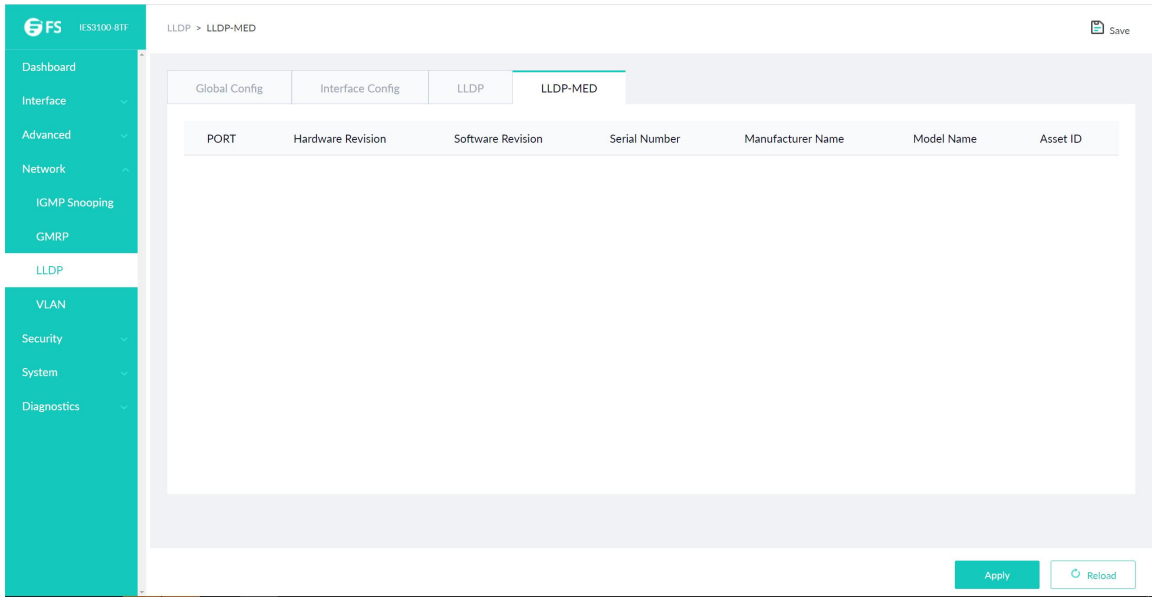
Click Diagnostics -> LLDP -> LLDP at navigation bar in order, and then enter the LLDP topology discovery and configuration page as following:



The page lists the devices that have been found.

6.3.4 LLDP-MED

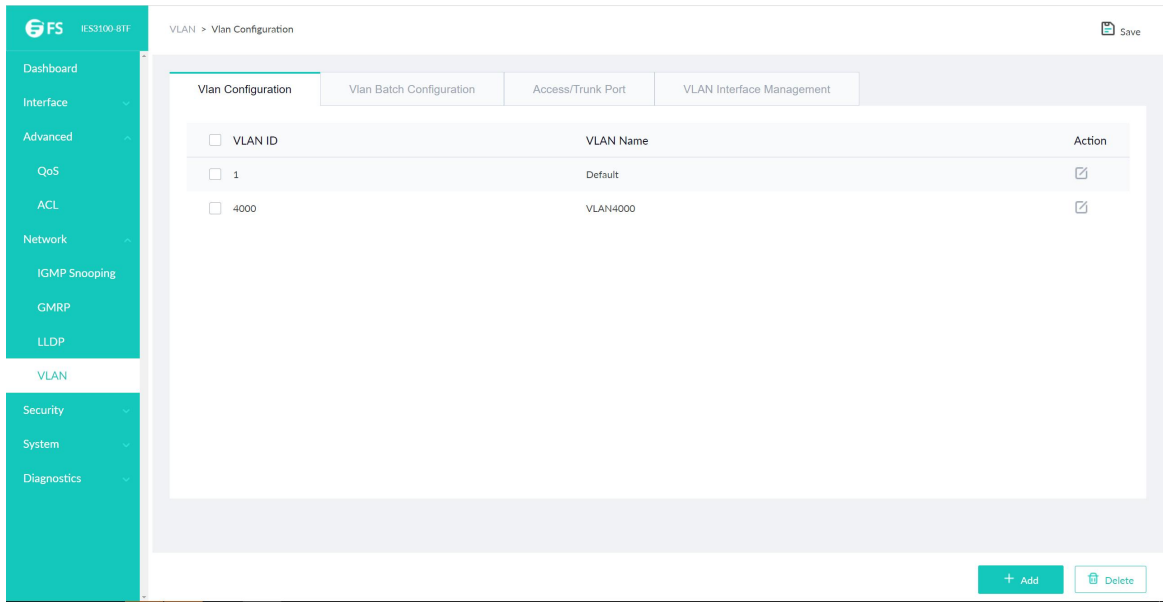
Click Diagnostics -> LLDP -> LLDP-MED at navigation bar in order, and then enter the LLDP-MED topology discovery and configuration page as following:



6.4 VLAN

6.4.1 VLAN Configuration

Click Network -> VLAN -> Vlan Configuration, at navigation bar in order, and select VLAN configuration tab page to enter VLAN configuration page as following:

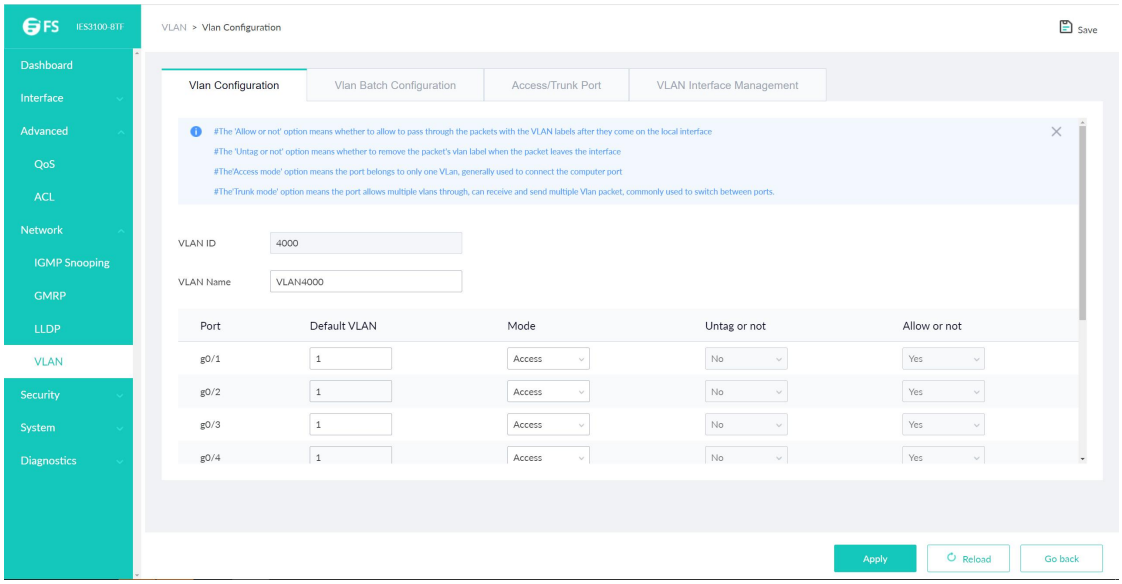


Click Edit icon after VLAN entry to change VLAN name and thisVLAN's port feature.

Select the check box before item and click Delete to delete the selected VLAN.

Note: By default, the maximum quantity of shown items of VLAN list is 100. If you want to configure more VLAN through Web, please login switch by Console port or Telnet to enter global configuration mode and use command ip http web max-vlan to modify maximum shown VLAN quantity.

Click Add or edit icon to enter VLAN configuration page.



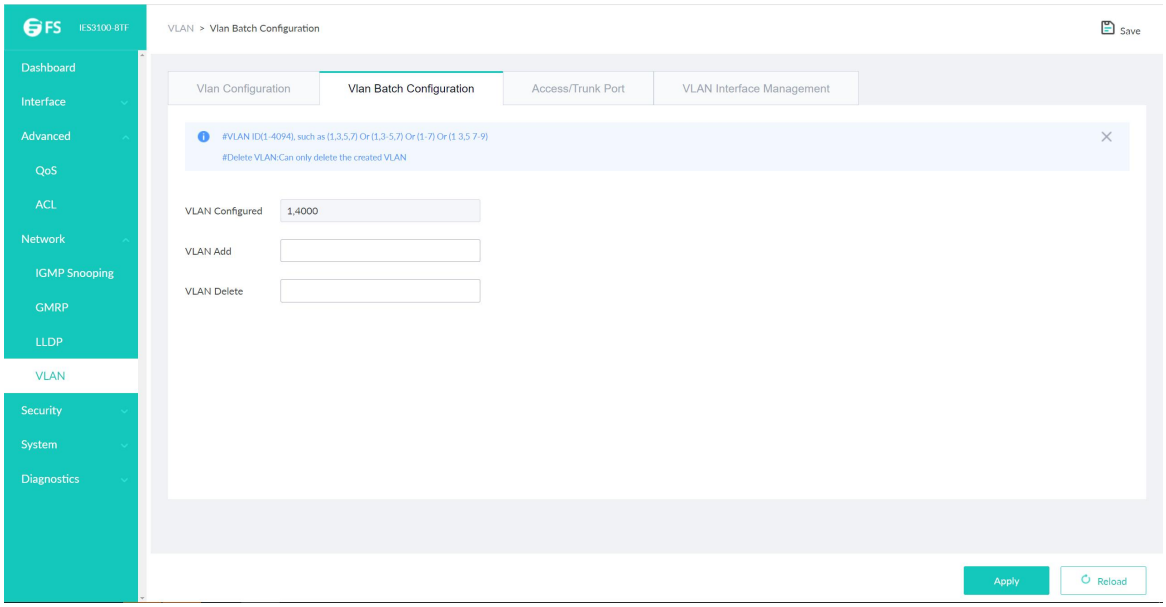
If you want to create a new VLAN, enter a VLAN ID and a VLAN name; the VLAN name can be null.

Through the port list, you can set for each port the 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.

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

6.4.2 Vlan Batch Configuration

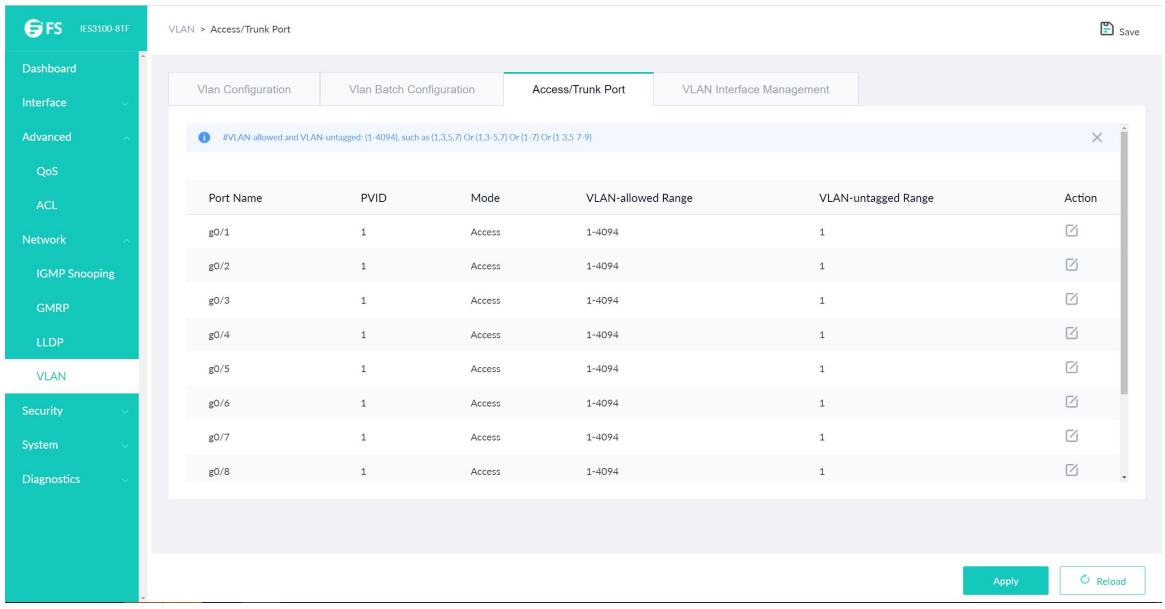
Click Network -> VLAN -> Vlan Batch Configuration, at navigation bar in order, and select VLAN batch configuration tab page to enter VLAN configuration page as following:



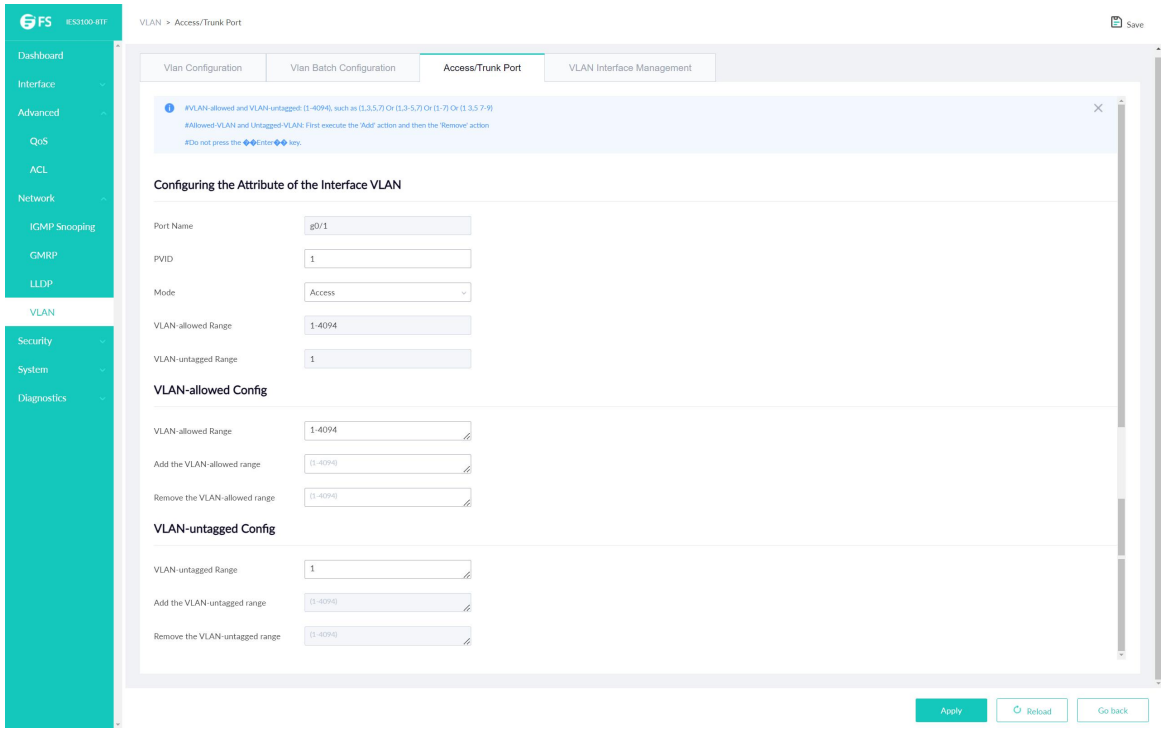
Note: Before VLAN to be deleted, it should be added first.

6.4.3 Access/Trunk Port

Click Network -> VLAN -> Access/Trunk Port, at navigation bar in order, and select VLAN tab page to enter port VLAN configuration page as following:



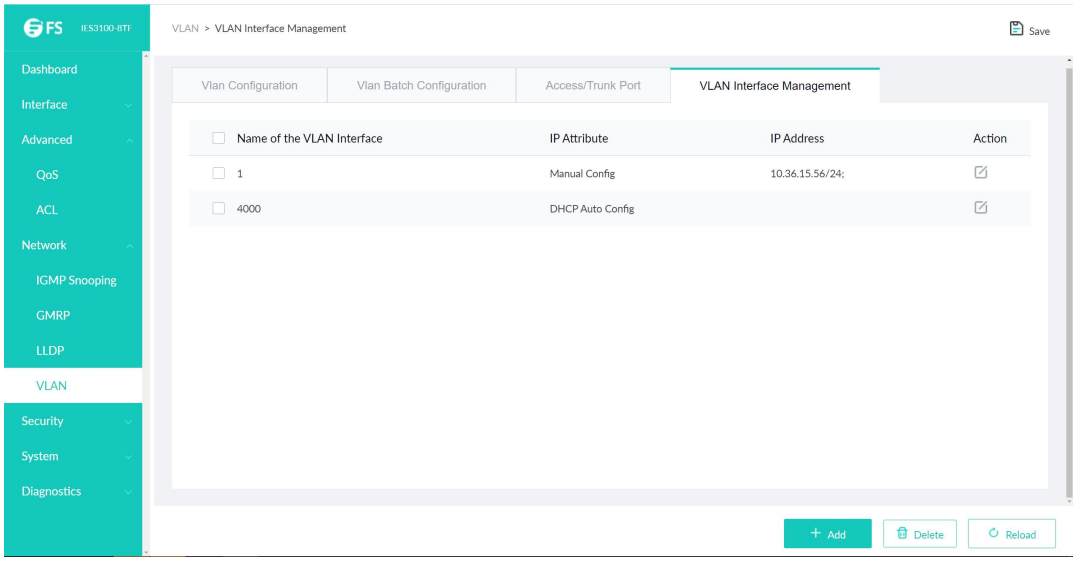
This page shows all ports'PVIDs, modes, allowed VLAN range and VLAN range without tag. Click Edit icon to change port's VLAN feature configuration, VLAN-allowed configuration and VLAN-untagged configuration.



Note: VLAN-allowed and VLAN-untagged：Please add first before do delete operation. Please do not key enter.

6.4.4 VLAN Interface Management

Click Network -> VLAN -> VLAN Interface Management at navigation bar in order, and then enter configuration page as following:

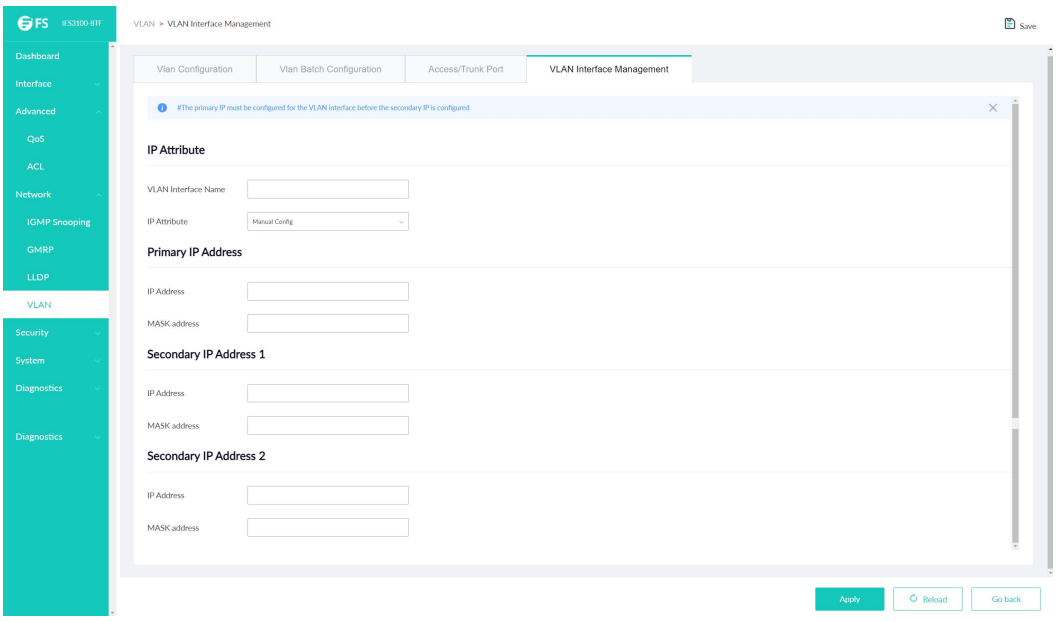


Click Add to create a new VLAN interface items.

Click Edit icon to enter relative VLAN interface items to do the modification.

Click Delete to delete the selected VLAN interface items.

You can change the VLAN name when you click the "Add" bottom, it's cannot change VLAN name when click "Edit"icon just can do the VLAN related items modification.



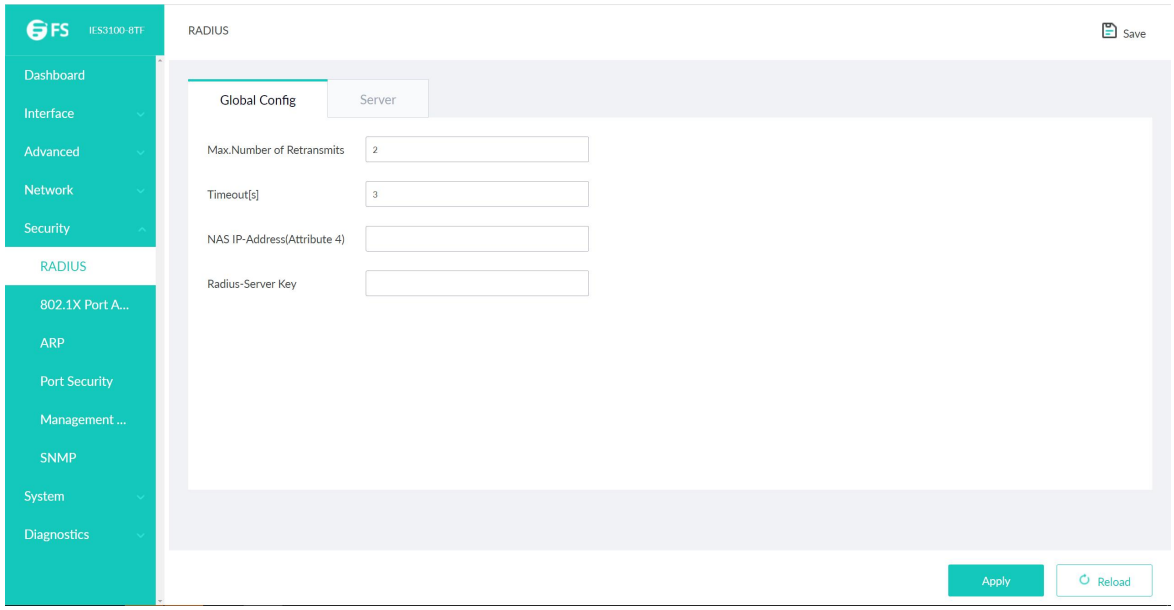
Note: Before you want setting the VLAN secondary IP address, must need setting the Primary IP Address finished.

Chapter 7 Security

7.1 RADIUS

7.1.1 Global Config

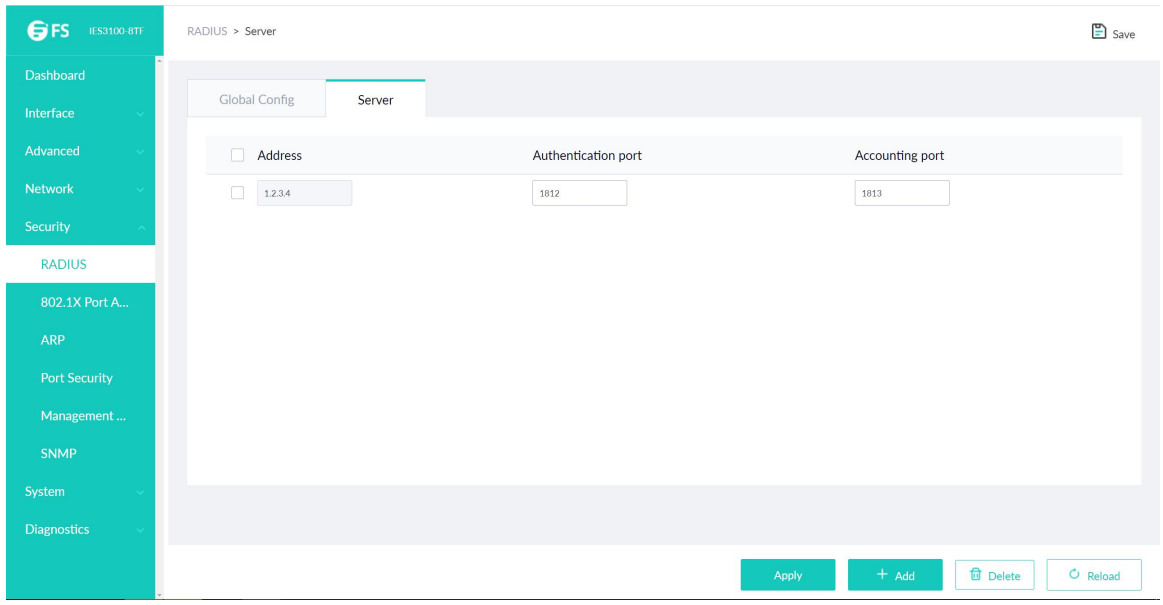
Click Security -> RADIUS -> Global Config at navigation bar in order to enter configuration page as following:



Max. Number of retransmits of radius, overtime, NAS and Radius-Server Key could be configured at this page.

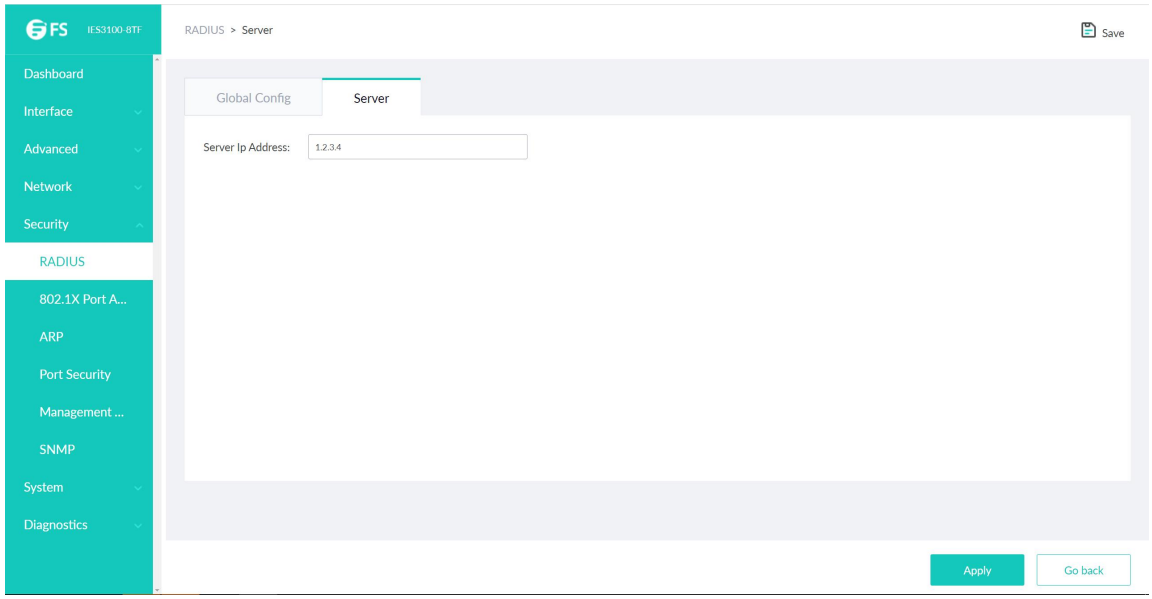
7.1.2 Server

Click Security -> RADIUS -> Server at navigation bar in order to enter configuration page as following:



Radius server's authentication port and accounting port can be configured at this page;

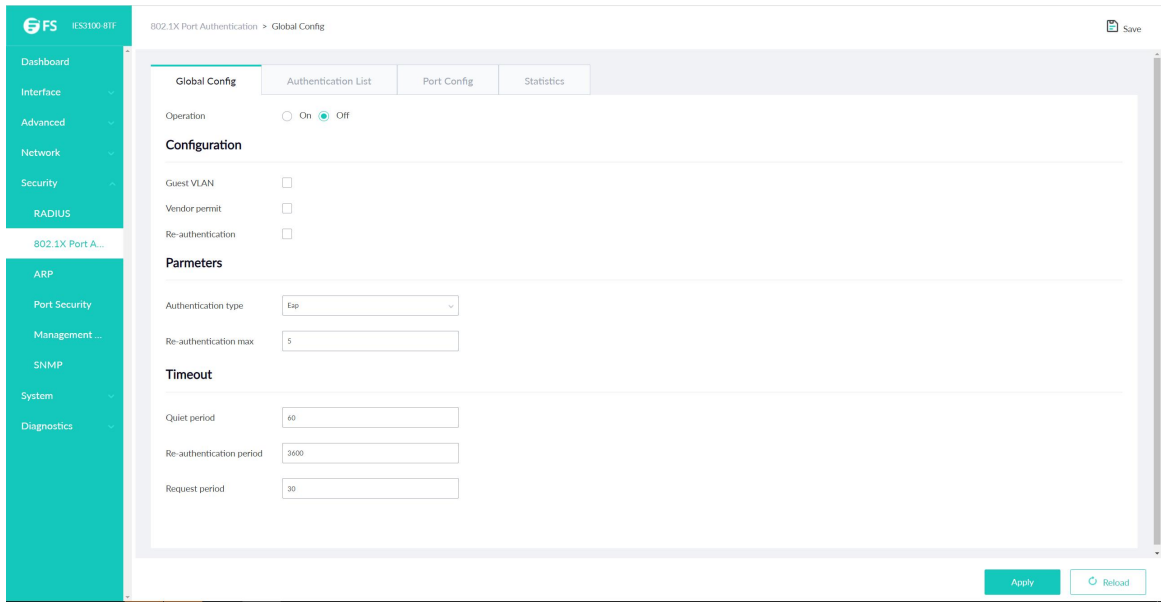
Click Add to create new radius server items:



7.2 802.1X Port Authentication

7.2.1 Global Config

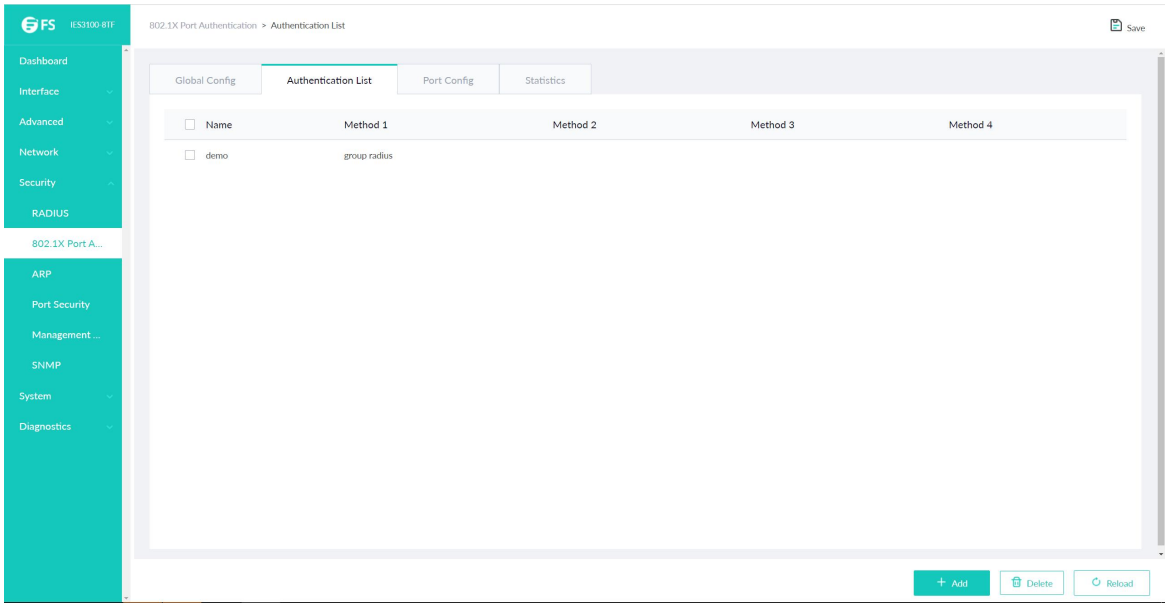
Click Security -> 802.1X Port Authentication -> Global Config at navigation bar in order to enter configuration page as following:



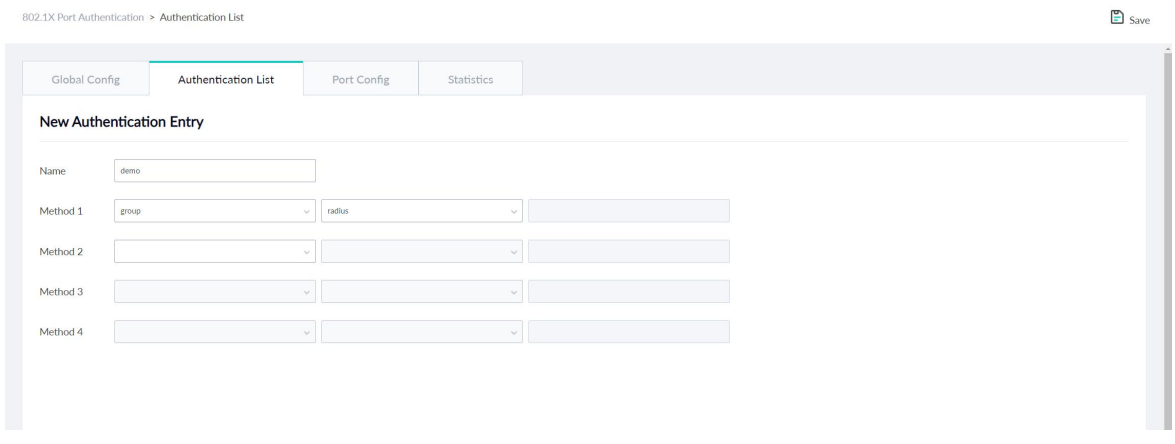
Configure the enabling/disabling operations of 802.1X Port Authentication at this page.

7.2.2 Authentication List

Click Security -> 802.1X Port Authentication -> Authentication List at navigation bar in order to enter configuration page as following:

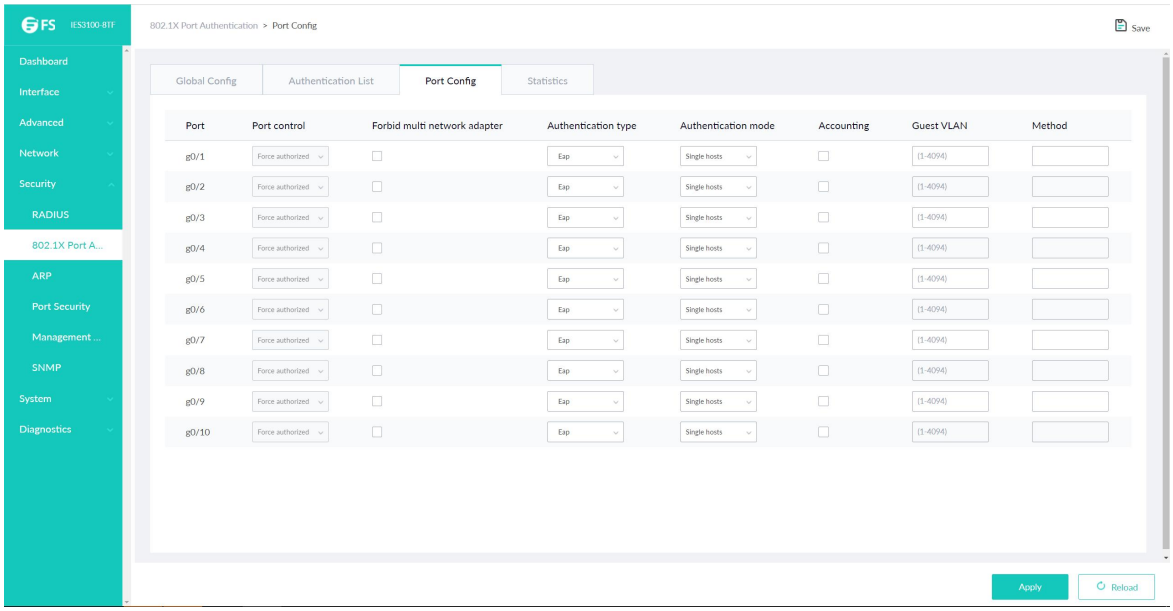


Click Add to create new authentication entry:



7.2.3 port Config

Click Security -> 802.1X Port Authentication -> Port Config at navigation bar in order to enter configuration page as following:

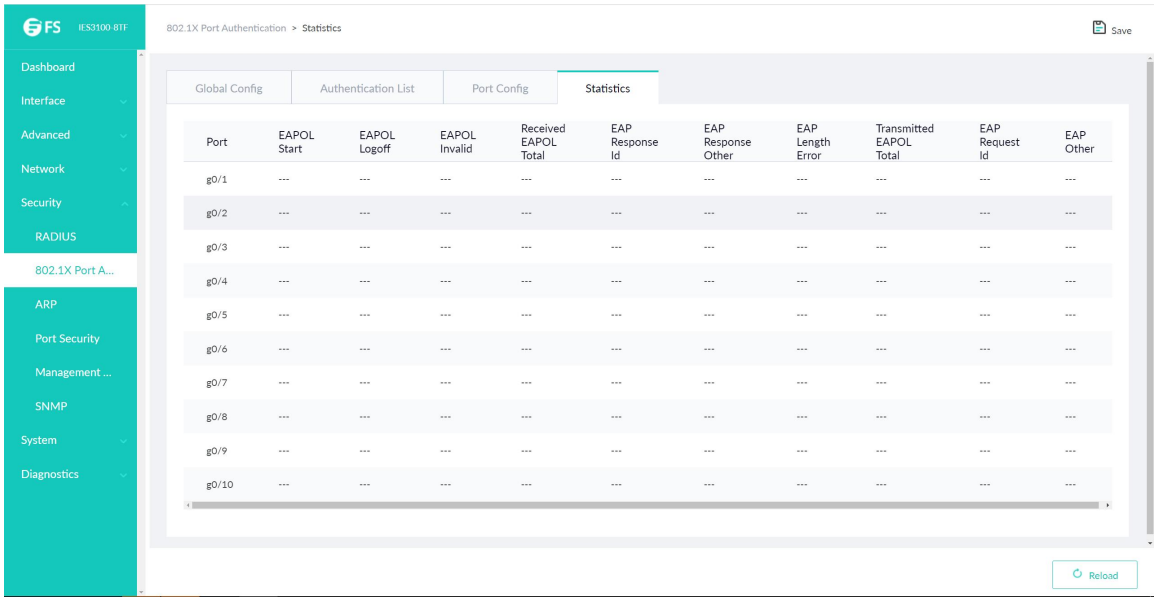


You could configure interface's enabling/disabling 802. 1x port authentication, authentication type, authentication mode, method and etc at this page.

Note: Some configurations can only be configured when 802.1X Port Authentication is enabled.

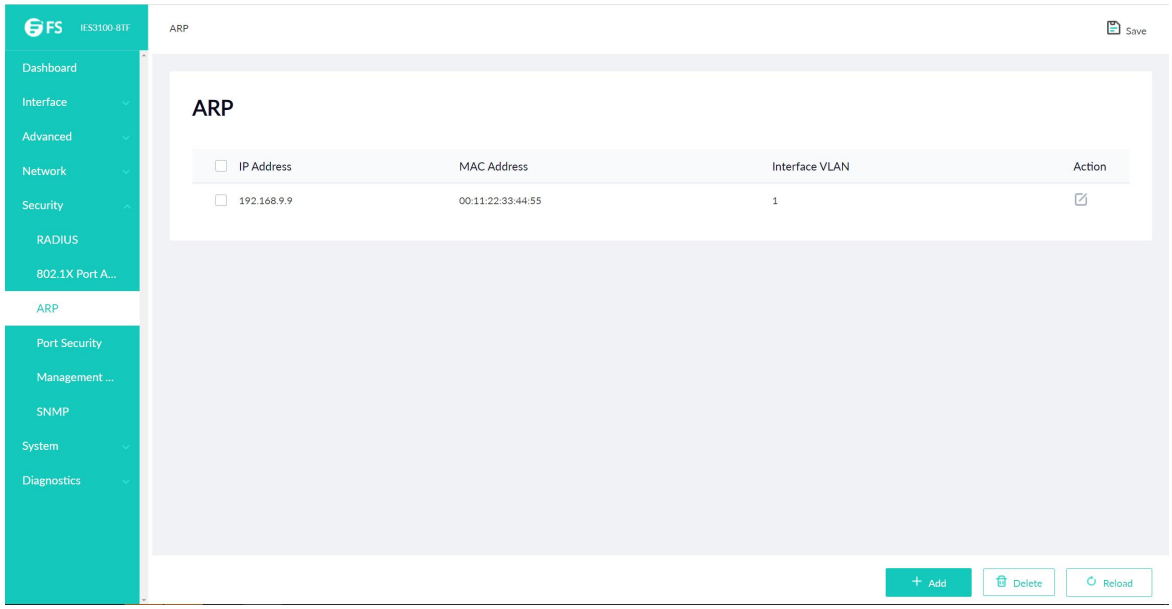
7.2.4 Statistics

Click Security -> 802.1X Port Authentication -> Statistics at navigation bar in order to enter configuration page as following:



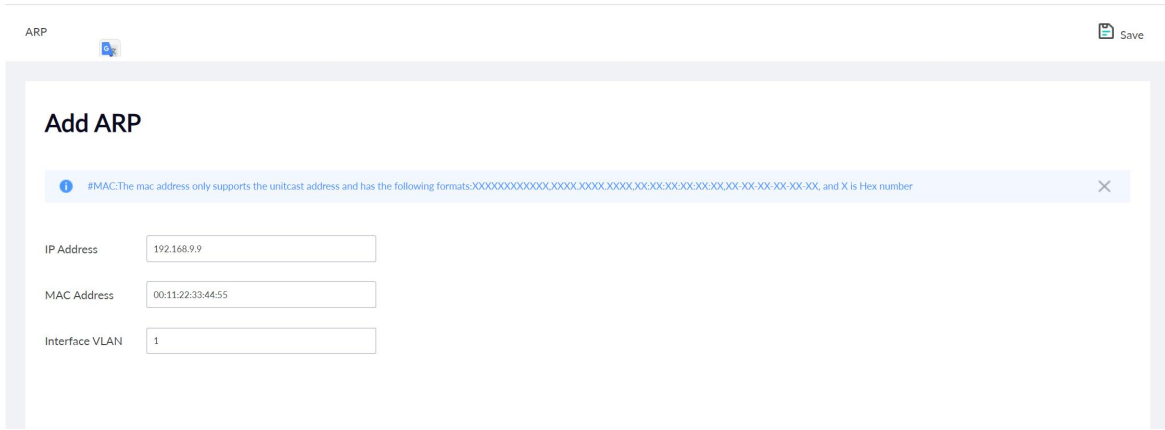
7.3 ARP

Click Security -> ARP at navigation bar in order , and then enter configuration page as following：



Click Add to create a new Static ARP.

Click Edit icon to modify the current Static ARP.

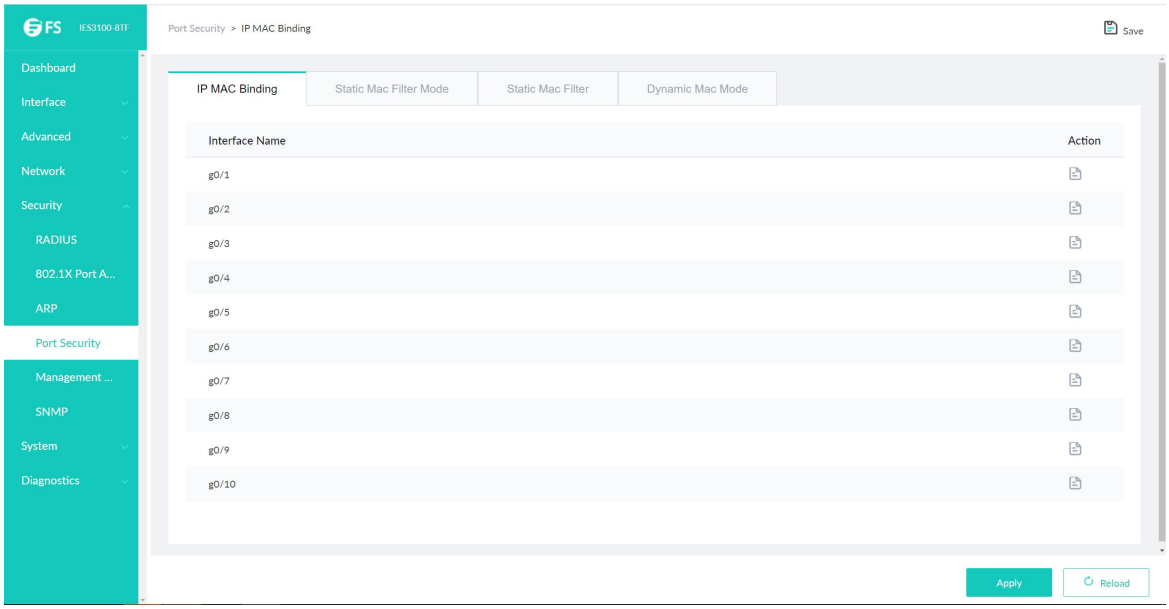


Click Delete to delete the selected Static ARP items.

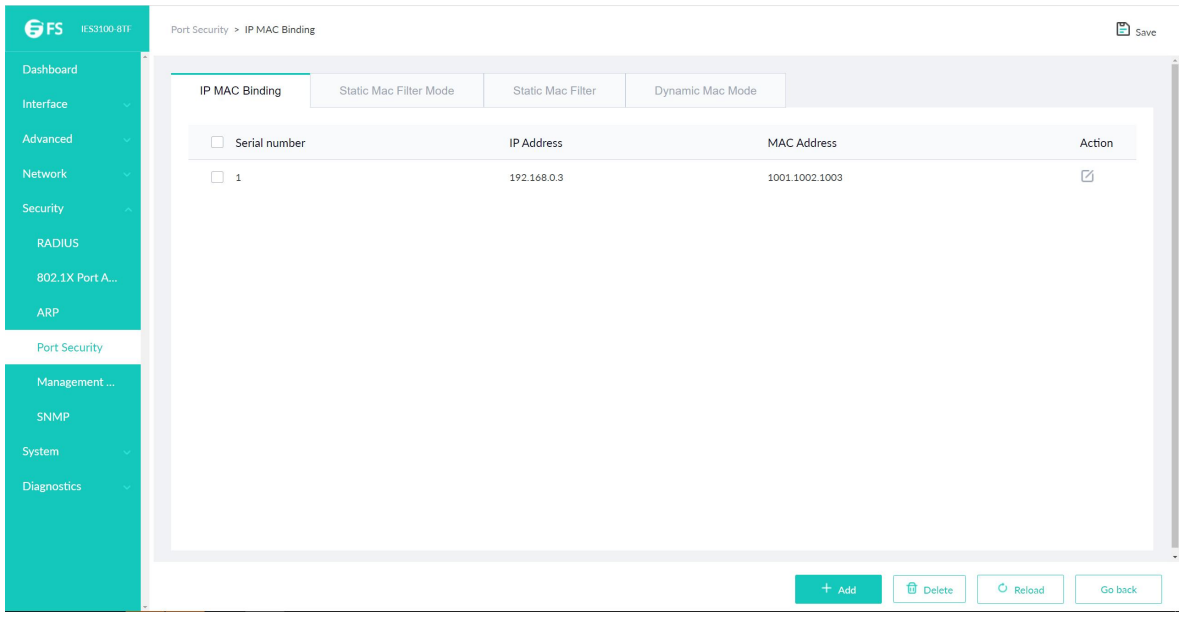
7.4 Port Security

7.4.1 IP MAC Bind

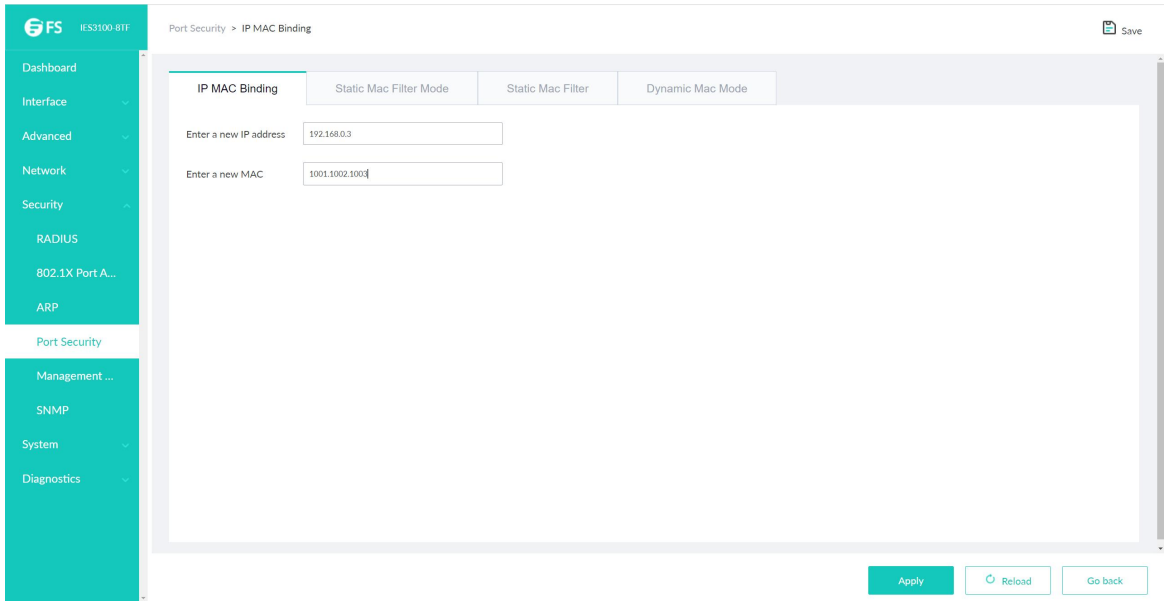
Click Security -> Port Security at navigation bar in order, and then click IP MAC Binding to enter configuration page as following:



Click Detail icon to check this interface's IP MAC binding information.



Click Add to create new IP MAC binding item.

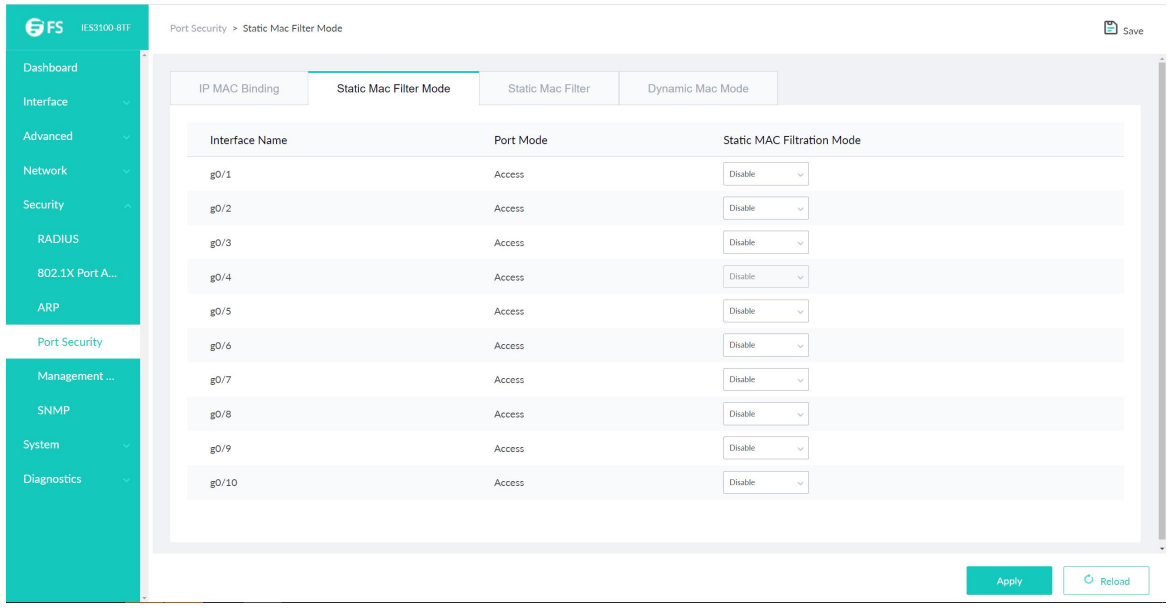


Click Edit icon to modify IP MAC binding item;

Click Delete to delete the selected IP MAC binding item.

7.4.2 Static MAC Filter Mode

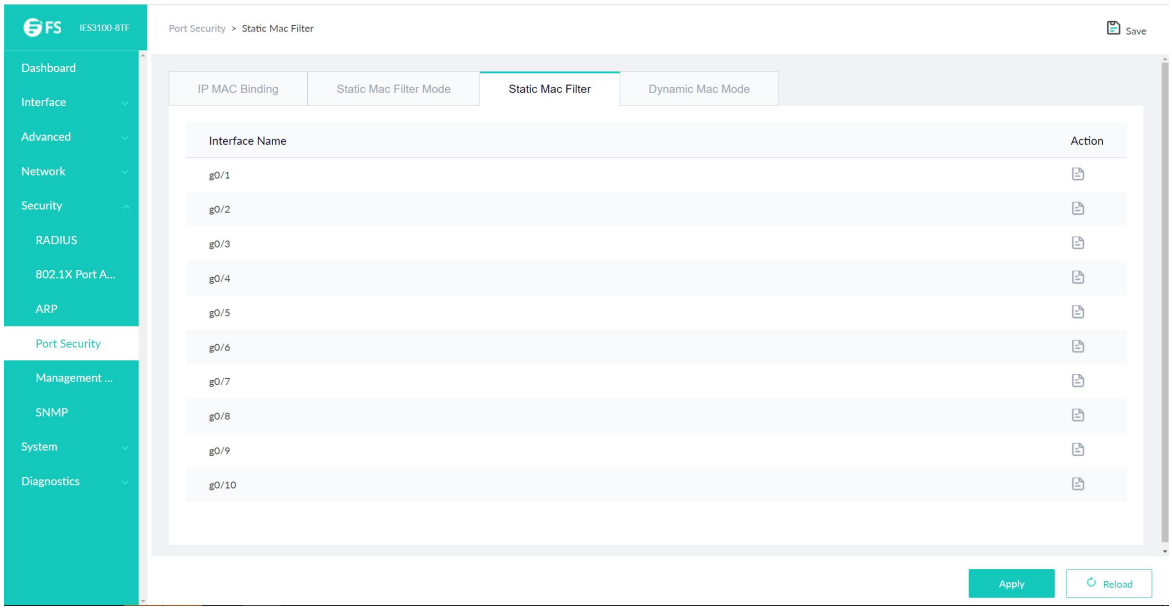
Click Security -> Port Security at navigation bar in order, and then click Static MAC Filter Mode to enter configuration page as following:



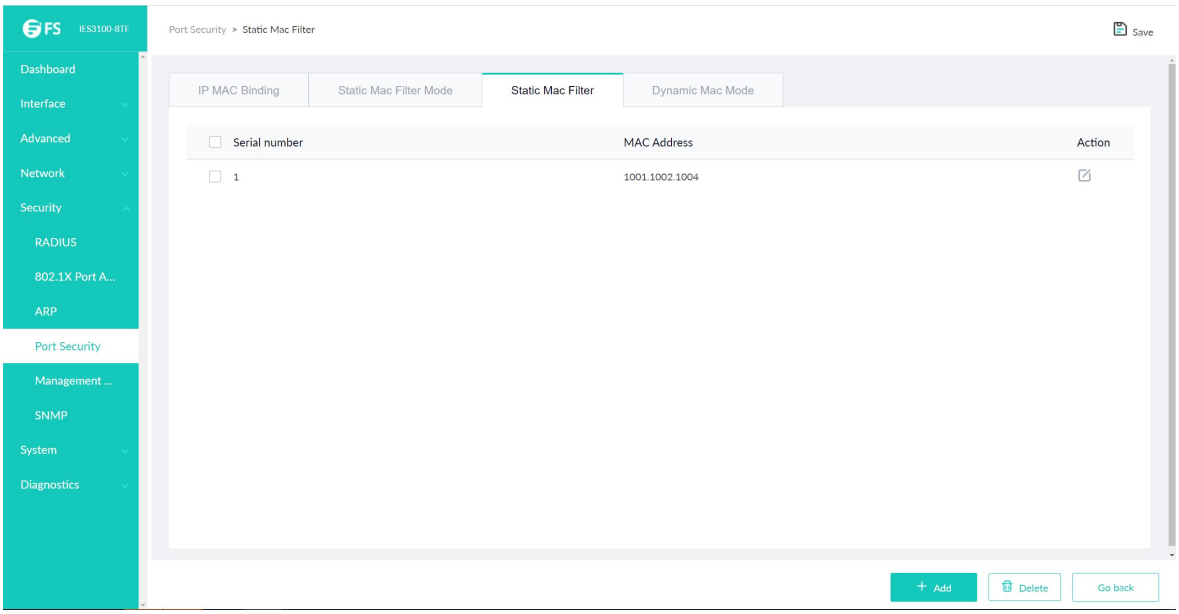
Interface's Static MAC Filteration Mode could be configured at this page.

7.4.3 Static MAC Filter

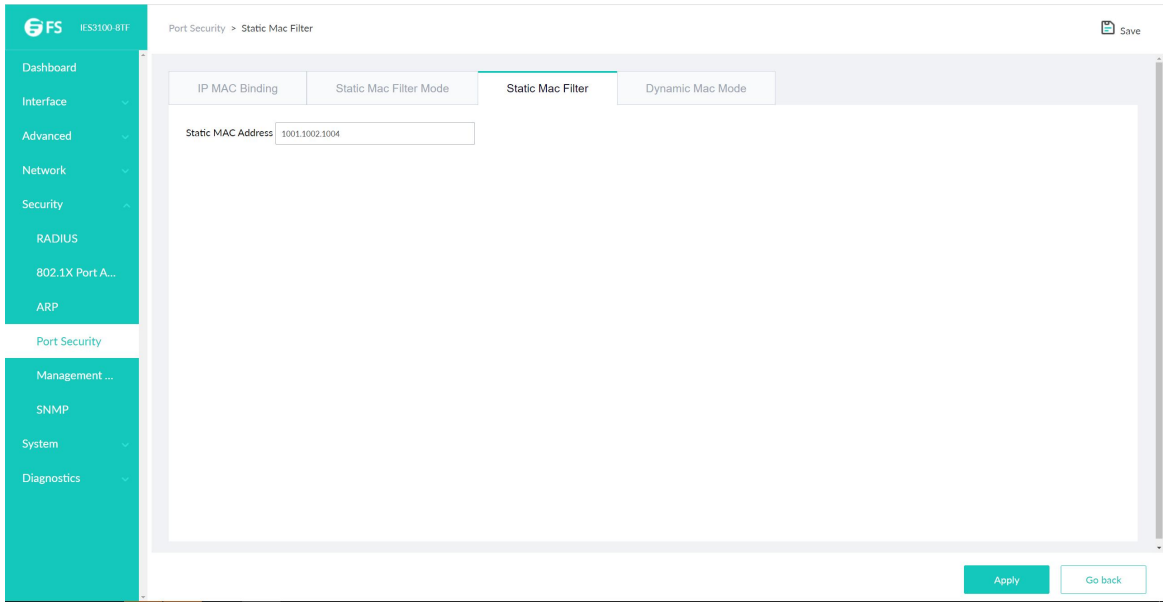
Click Security -> Port Security at navigation bar in order, and then click Static MAC Filter to enter configuration page as following:



Click Detail icon to check the interface's static MAC Filteration items.



Click Add to create new static MAC Filteration items.

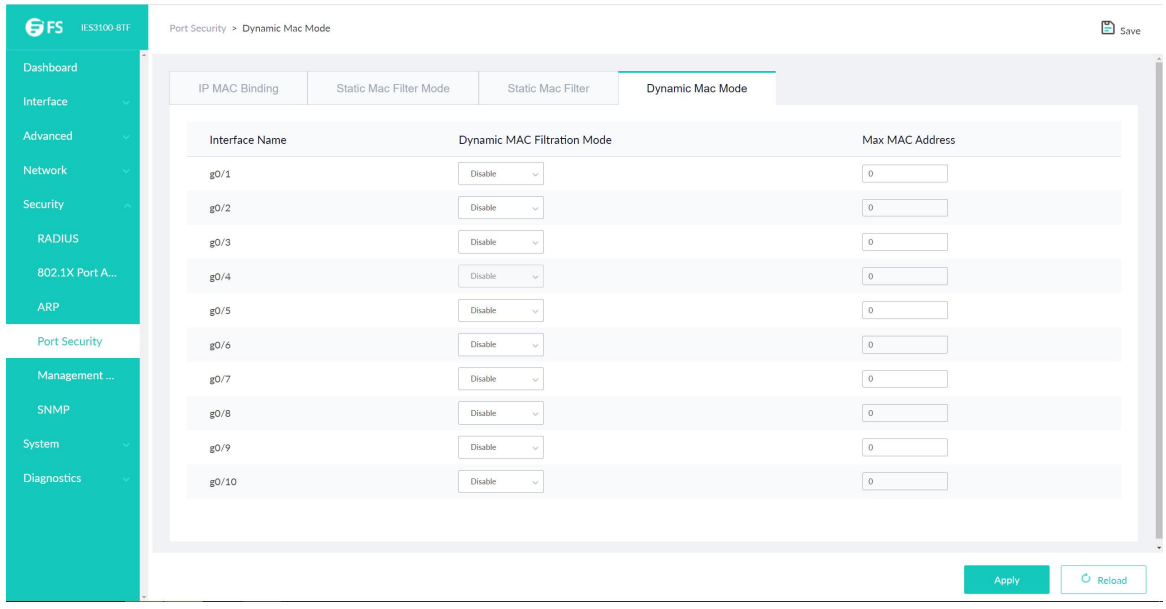


Click Edit icon to modify static MAC Filteration items;

Click Delete to delete the selected static MAC Filteration items.

7.4.4 Dynamic MAC Mode

Click Security -> Port Security at navigation bar in order, and then click Dynamic MAC Mode to enter configuration page as following:



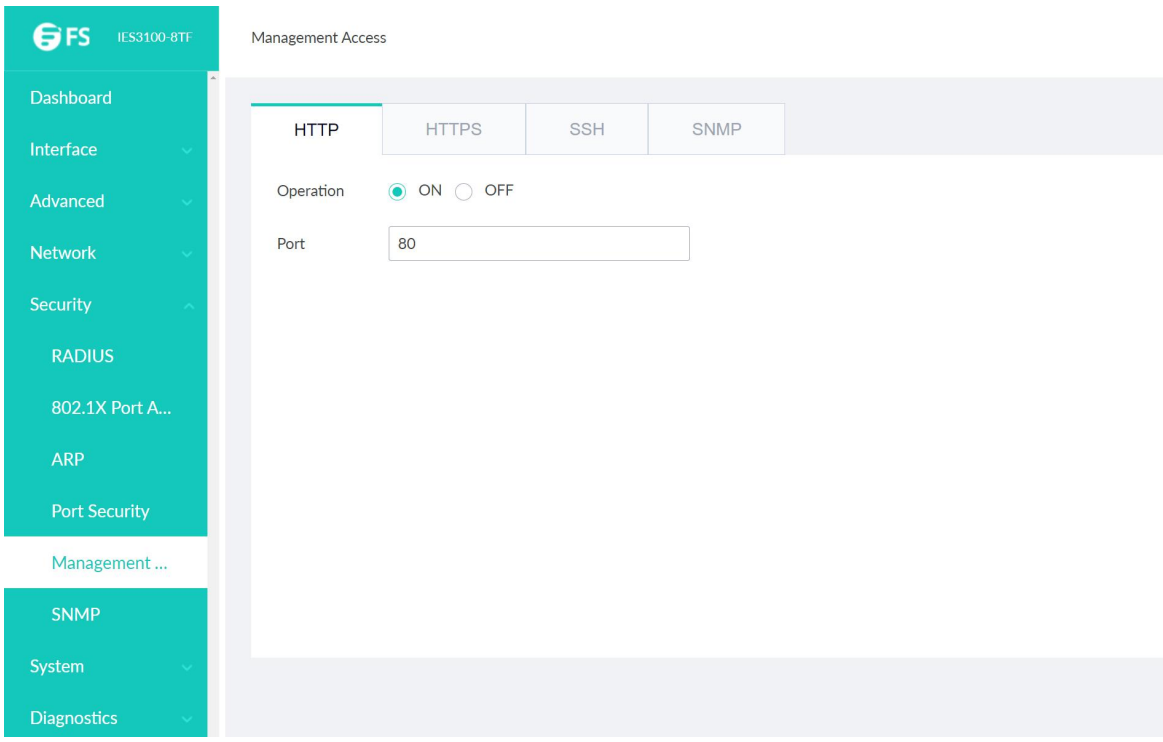
Interface's Dynamic MAC Filteration Mode could be configured at this page.

7.5 Management Access

HTTP, HTTPS, SSH and SNMP could be configured at this page.

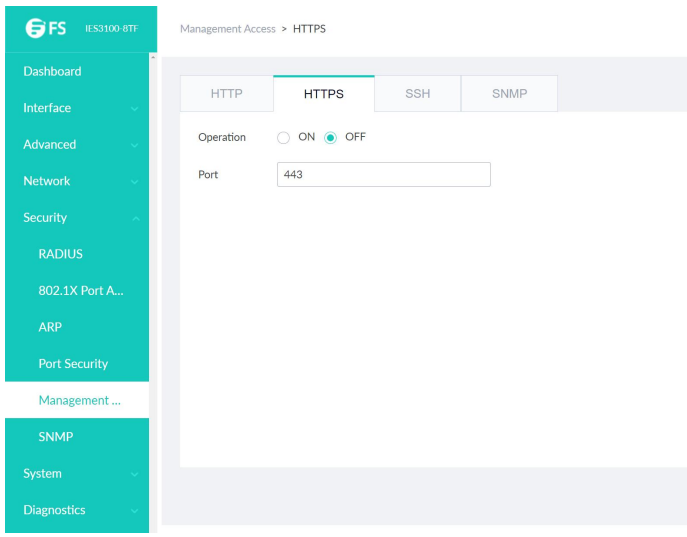
7.5.1 HTTP

Click Security -> Management Access -> HTTP at navigation bar in order , and then enter the configuration page as following:



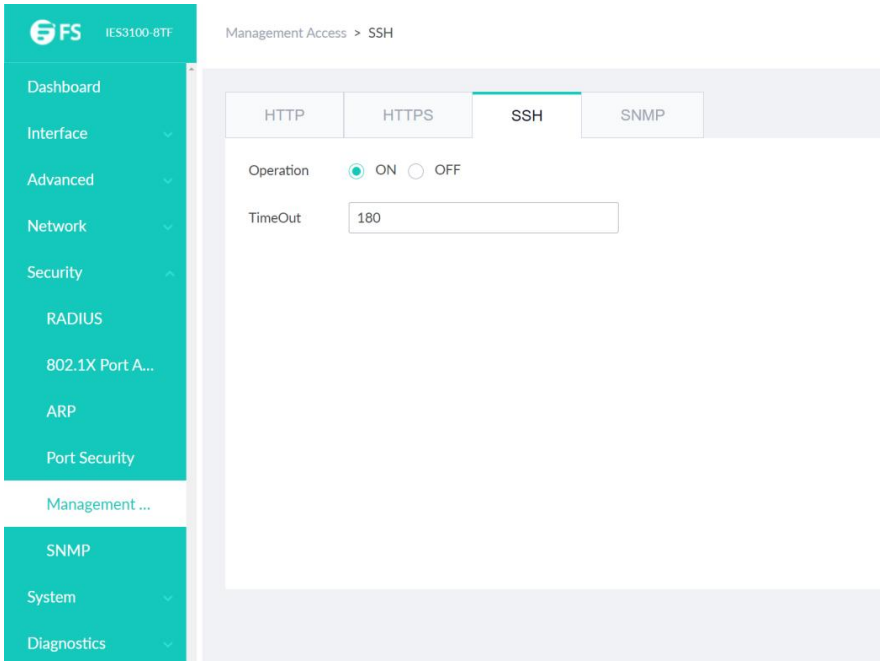
7.5.2 HTTPS

Click Security -> Management Access -> HTTPS at navigation bar in order , and then enter the configuration page as following:



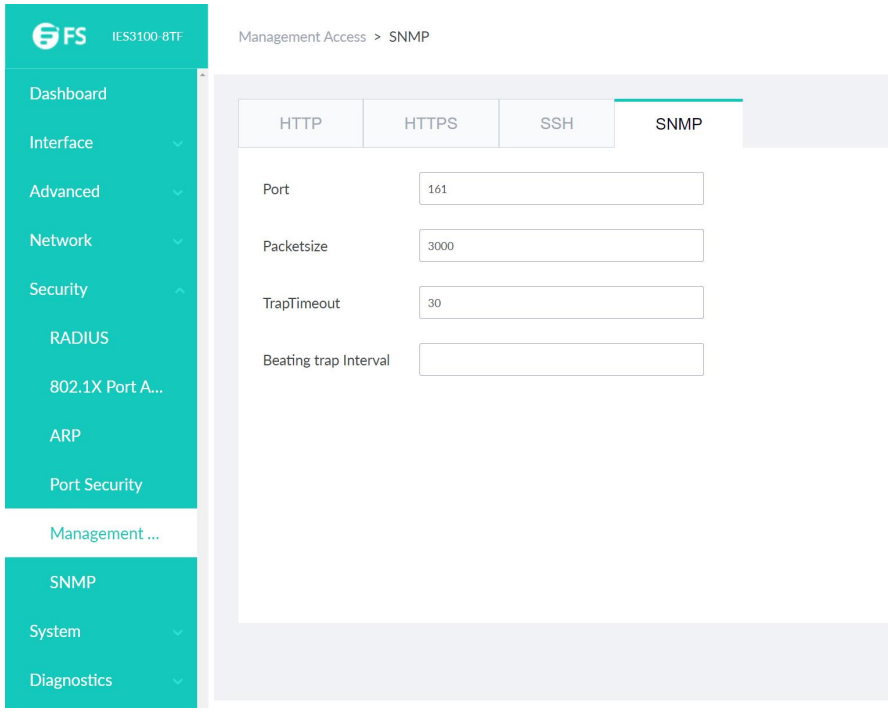
7.5.3 SSH

Click Security -> Management Access -> SSH at navigation bar in order , and then enter the configuration page as following:



7.5.4 SNMP

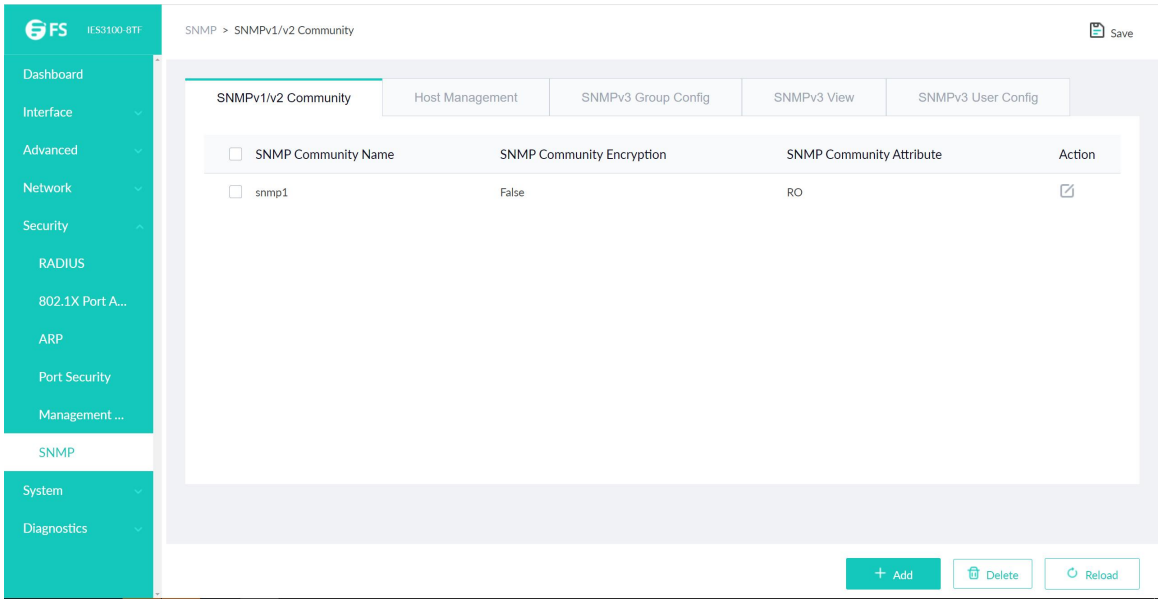
Click Security -> Management Access -> SNMP at navigation bar in order , and then enter the configuration page as following:



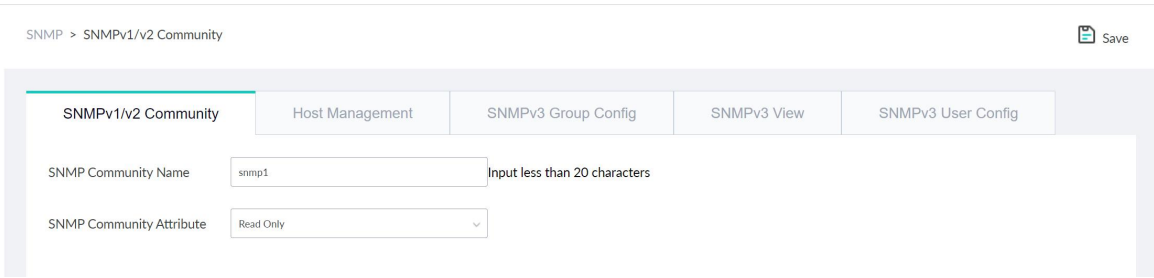
7.6 SNMP

7.6.1 SNMPv1/v2 Community

Click Security -> SNMP -> SNMPv1/v2 Community at navigation bar in order to enter configuration page as following:



Click Add to create new SNMP Community:

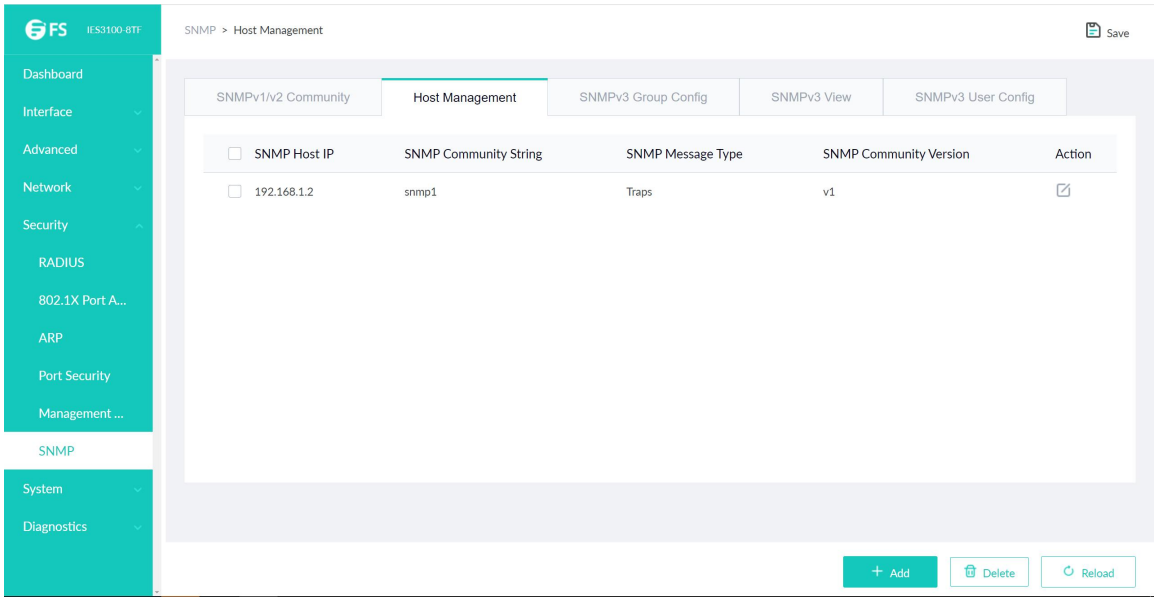


Click Edit icon to change the feature of SNMP Community;

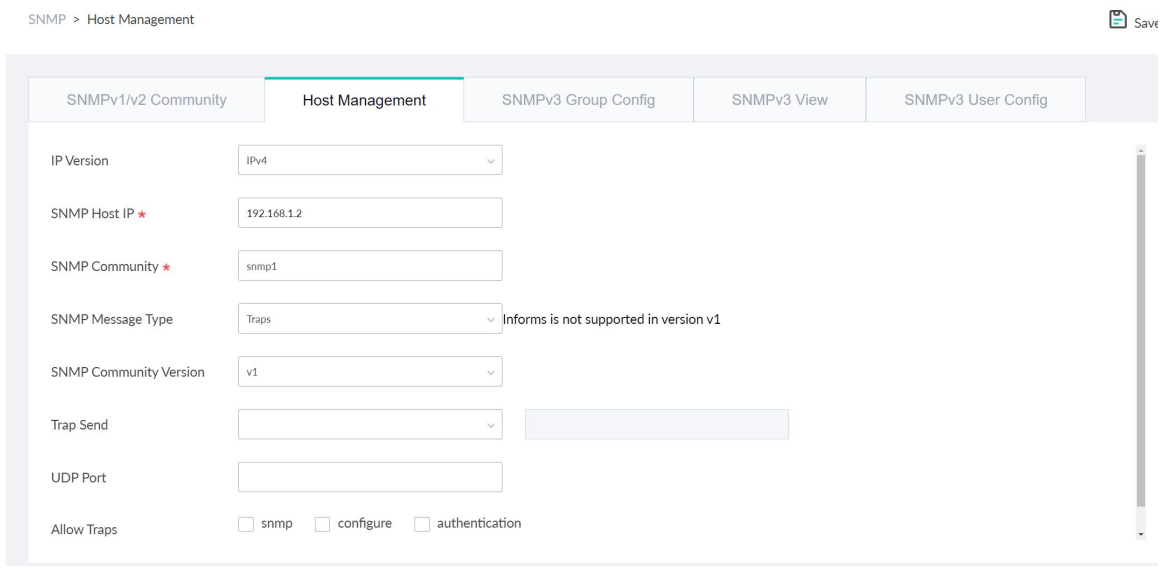
Click Delete to delete the selected SNMP Community;

7.6.2 Host Management

Click Security -> SNMP -> Host Management at navigation bar in order to enter configuration page as following:



Click Add to create new SNMP Host:



Click Edit icon to modify feature of SNMP Host;

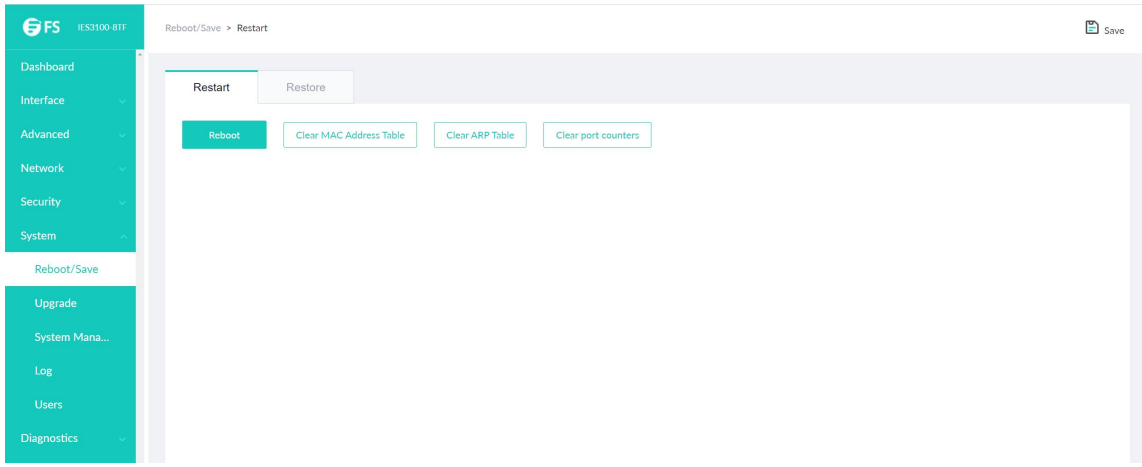
Click Delete to delete the selected SNMP Host.

Chapter 8 System

8.1 Reboot/Save

8.1.1 Restart

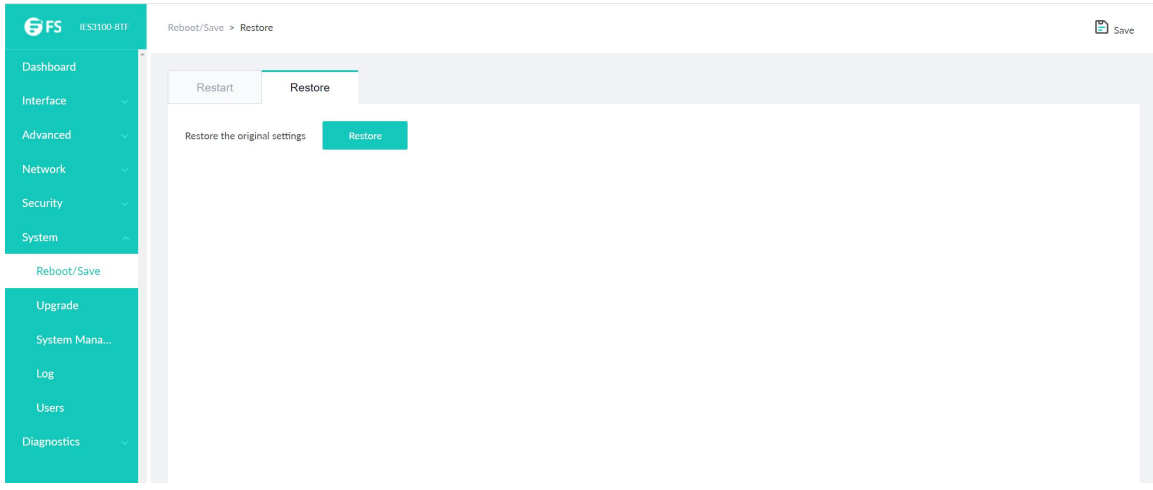
If you click System ->Reboot/Save -> Restart in the navigation bar, the page appears as shown as below figure：



You can choice"Reboot" to reboot the switch， or choice"Clear MAC Address Table" 、"Clear ARP Table"、"Clear port counters" .

8.1.2 Restore

If you click System ->Reboot/Save -> Restore in the navigation bar, the page appears as shown as below figure：



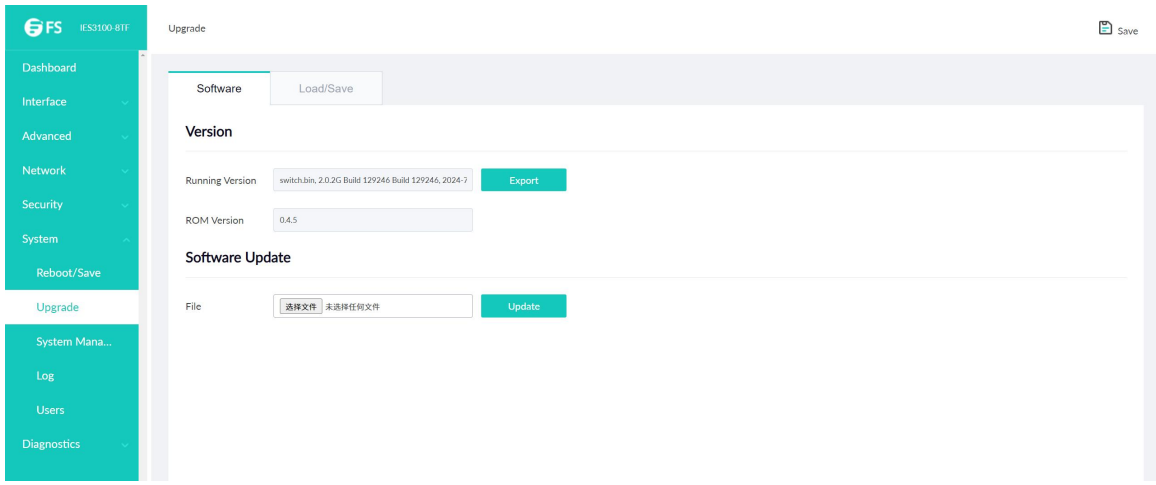
Click the Restore button to restore the original settings

8.2 Upgrade

8.2.1 Software

If you click System -> Upgrade-> Software in the navigation bar, the Software management page appears, as shown as

below figure



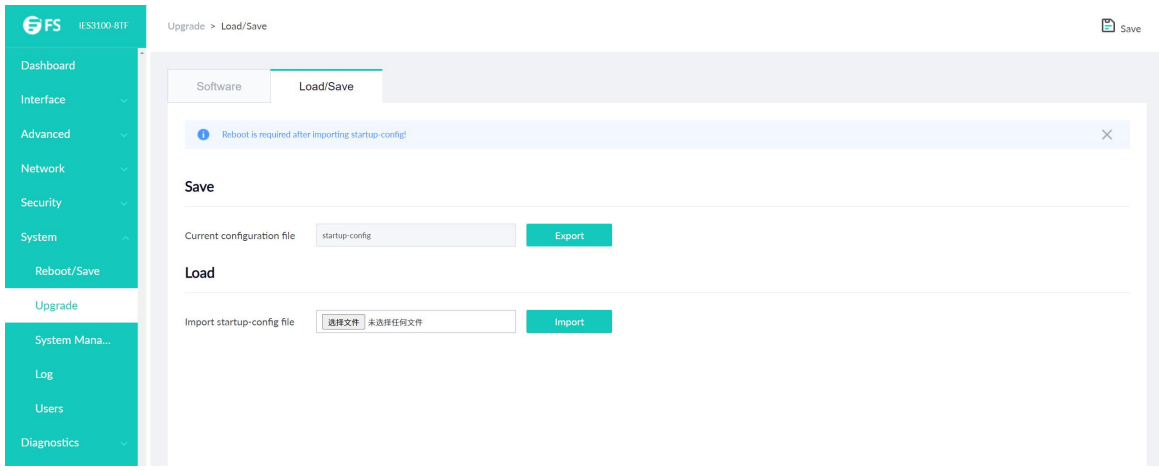
Current running version and rom version could be checked at this page. Click Export to export current running version to computer.

Choose the to-be-updated software version and click Update to change system's software version on Software Update Column.

Note: The updated system's software would be valid only if the device is restarted.

8.2.2 Load/Save

If you click System -> Upgrade-> Load/Save in the navigation bar, the page appears as shown as below figure:

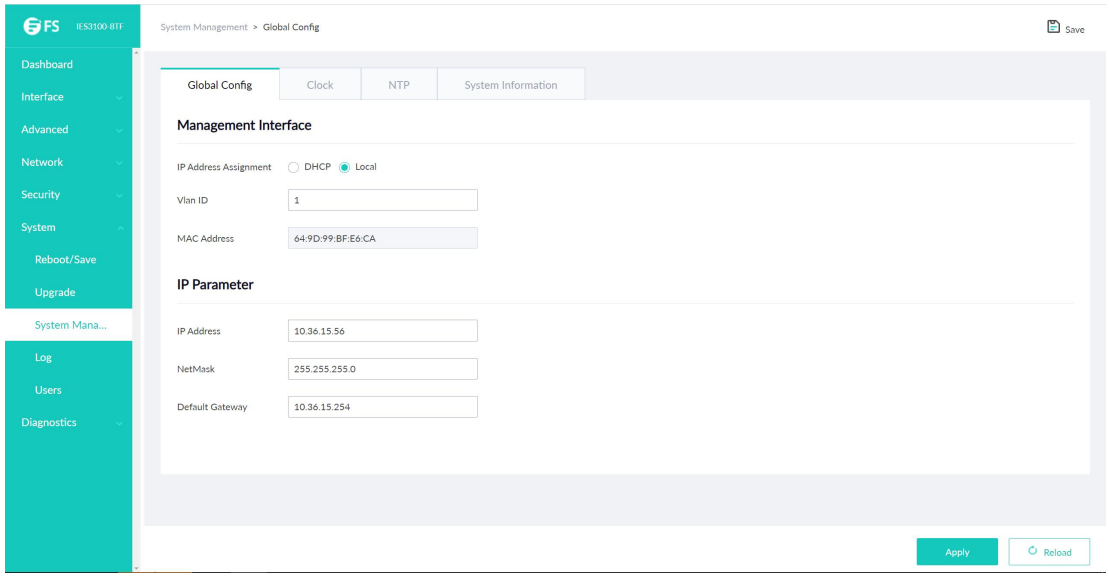


Click the "Export" then the current configuration of system will be exported to computer, if you click the " Import" then related configuration document will be imported to switch.

8.3 System Management

8.3.1 Global Config

If you click System-> System Management -> Global Config in the navigation bar, the page appears as shown as below:

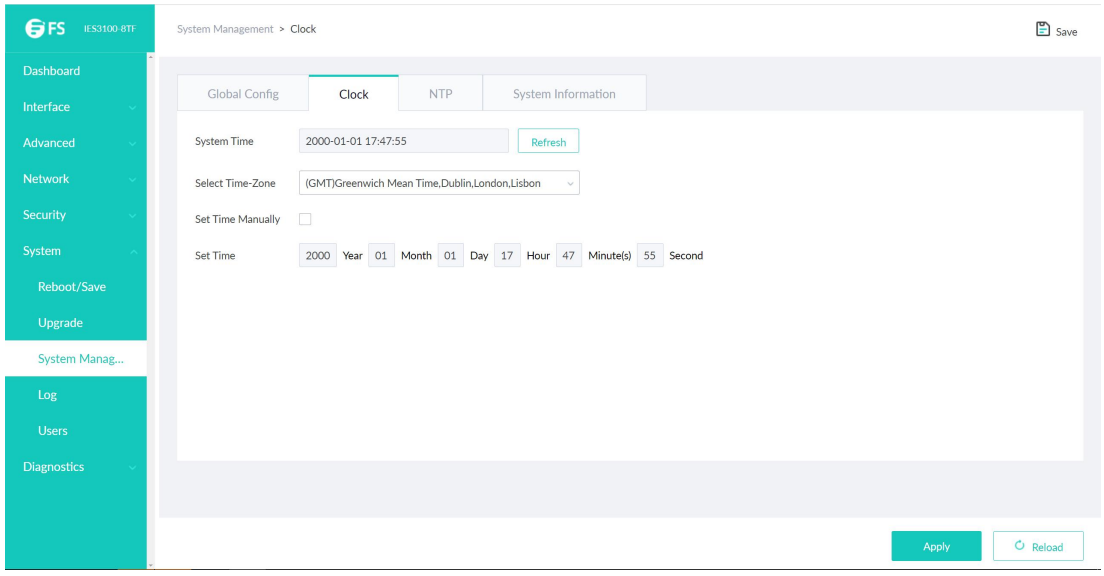


- Setting the IP address of Interface VLAN 1 , in order to access the switch

- This page is used to set the IP address of Interface Vlan 1 in the management interface of the device. In initial conditions, the MAC address of the device, the IP address, mask and gateway of the interface will appear on this page.

8.3.2 Clock

Click System -> System Management -> Clock at navigation bar in order to enter configuration page as following:

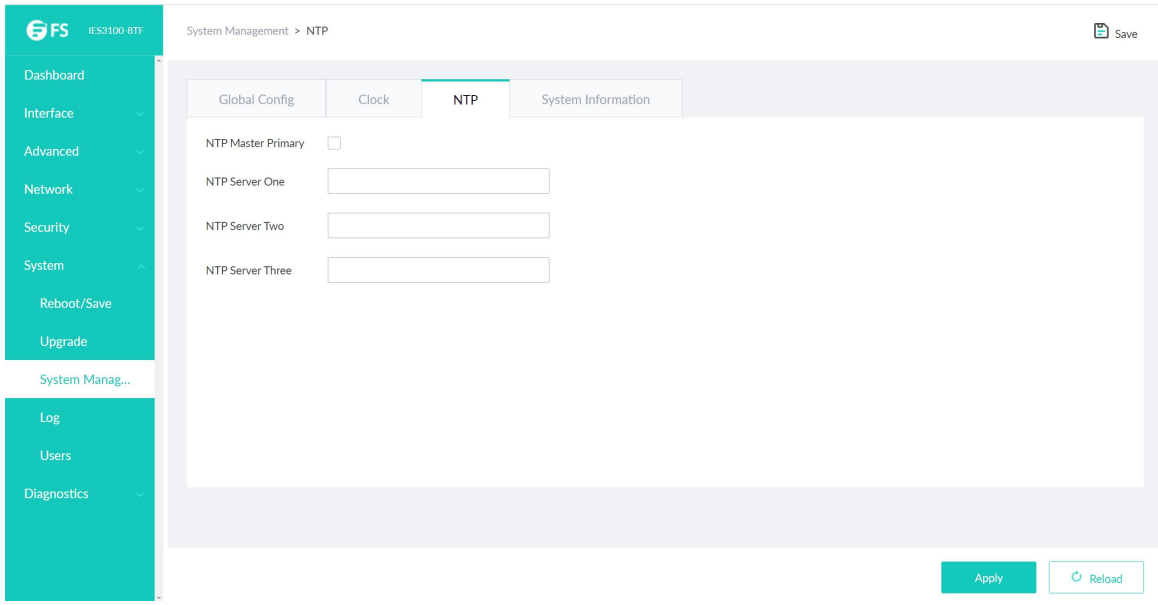


Click Reload to refresh the current displayed system time.

System's time-zone could be configured at this page. Select Set Time Manually to set system time manually.

8.3.3 NTP

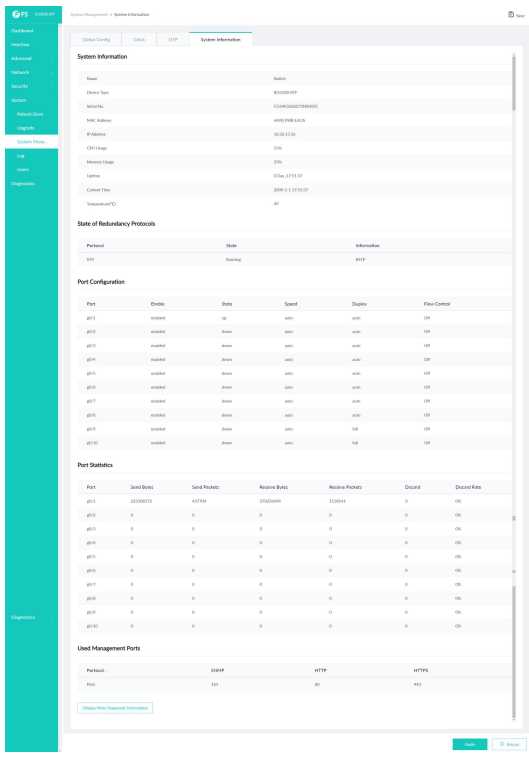
Click System -> System Management -> NTP at navigation bar in order to enter configuration page as following:



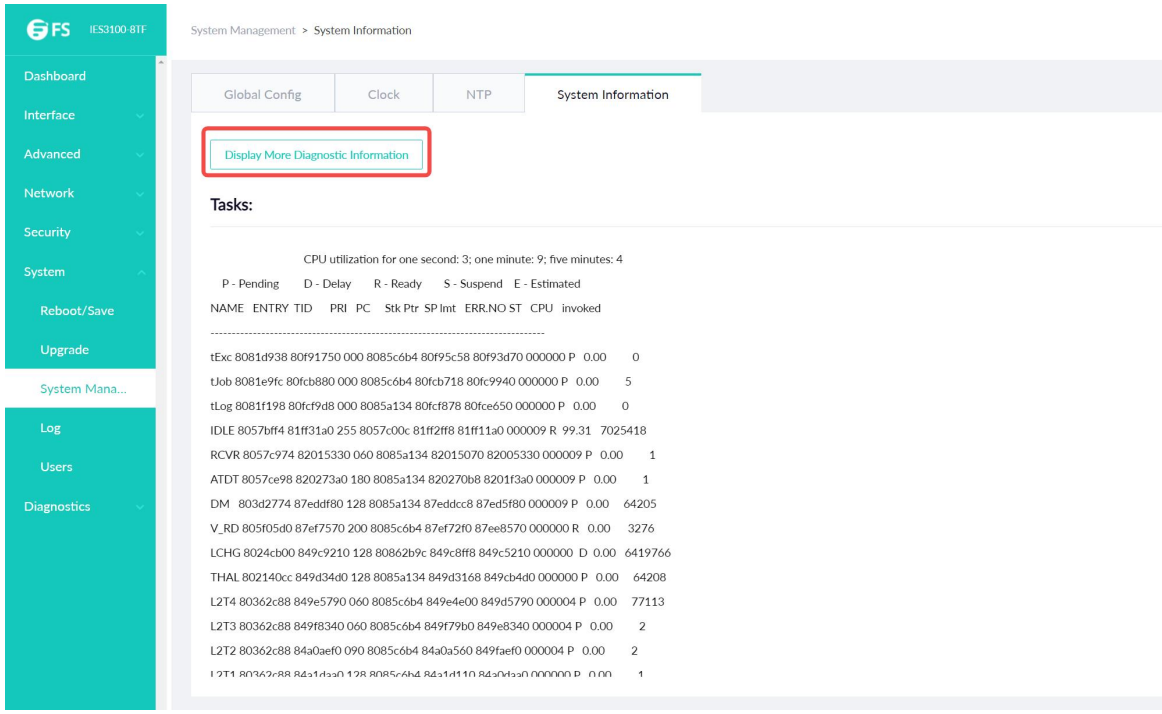
NTP server's IP address of NTP (Network Time Synchronization) could be configured at this page.

8.3.4 System Information

Click System-> System Management -> System Information at navigation bar in order, and then enter the configuration page as following:



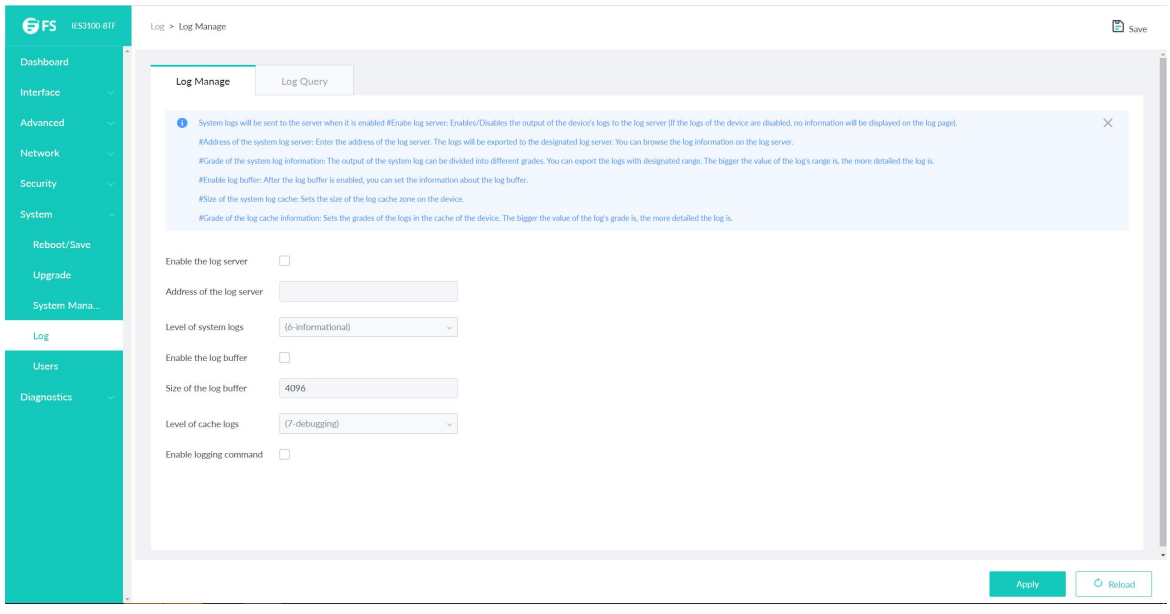
The page lists the system information, state of redundancy protocol, port configuration, port statistics, user management port; Click Display more can check more information such as CPU utilization, task information...etc.



8.4 Log

8.4.1 Log Manage

Click System-> Log -> Log Manage at navigation bar in order, and then enter the configuration page as following：

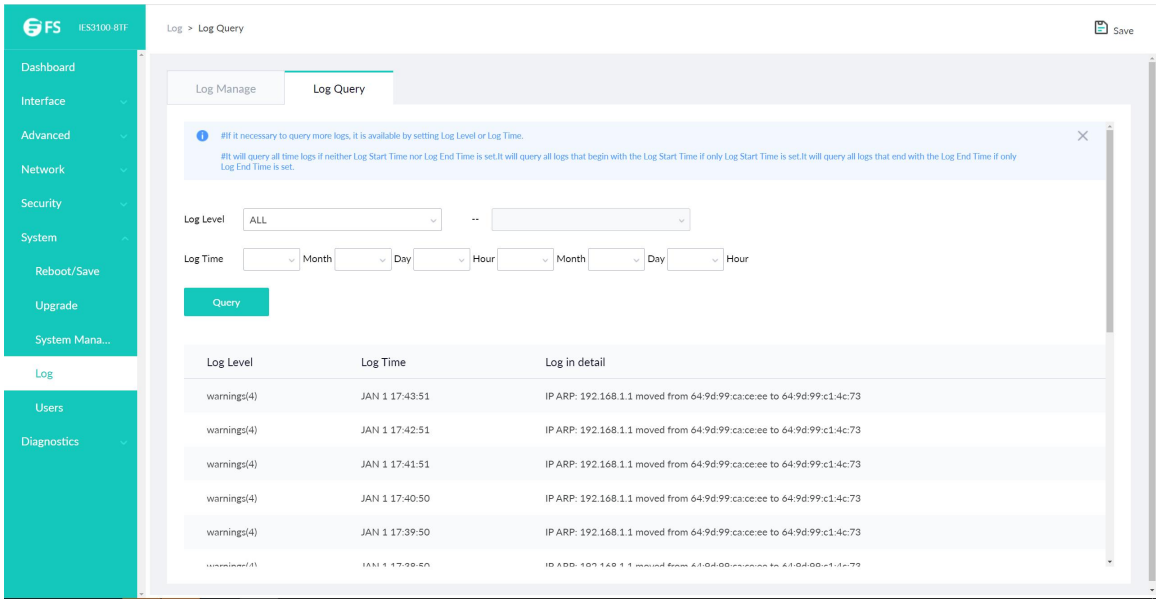


When Enabling the log server was selected, the device will transmit the log information to the designated server. In this case, you need enter the address of the server in the Web Configuration "Address of the system log server" textbox and select the log's grade in the "Grade of the system log information"dropdown box (grade 7 – debugging is the lowest grade of log).

When enabling the log buffer was selected, the device will record the log information to the memory. By logging on to the device through the Console port or Telnet, you can run the command "show log" to browse the logs which are saved on the device. The log information saved in the memory will lost when restarting the device. 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 cache log information" dropdown box.

8.4.2 Log Query

Click System -> Log -> Log Query at navigation bar in order, and then enter the configuration page as following:

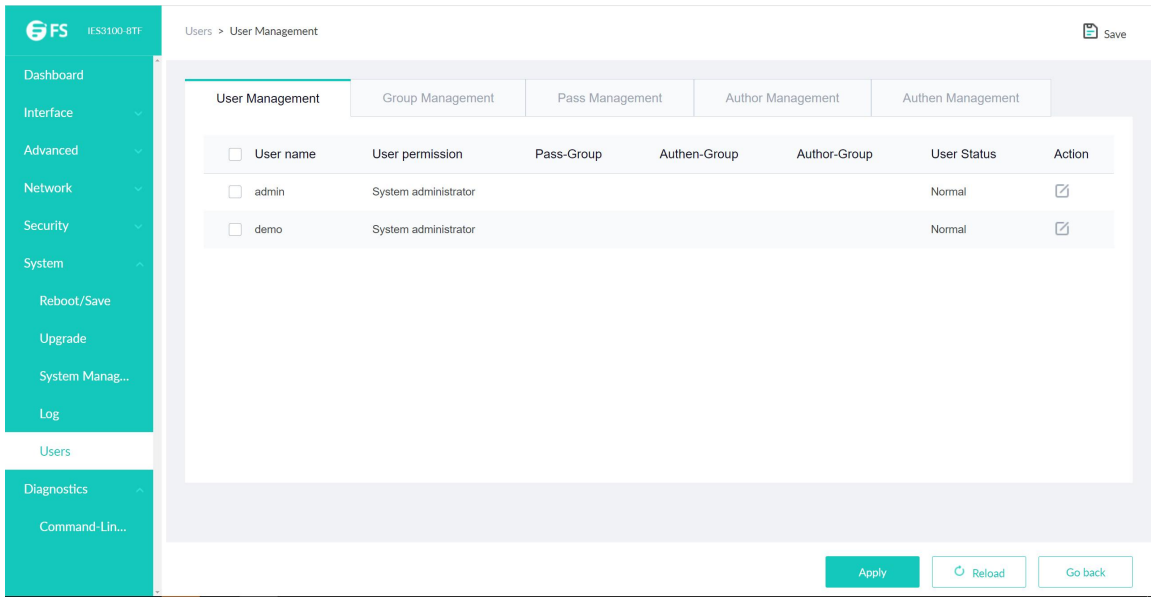


Note: If you need more information, you can Query it by setting the log level and log time. Do not set the log time means that the query log of all time;Only set the starting time of log queries are expressed by the time for starting time log of all;only set the end time means queries are expressed by the time as the end time of all log.

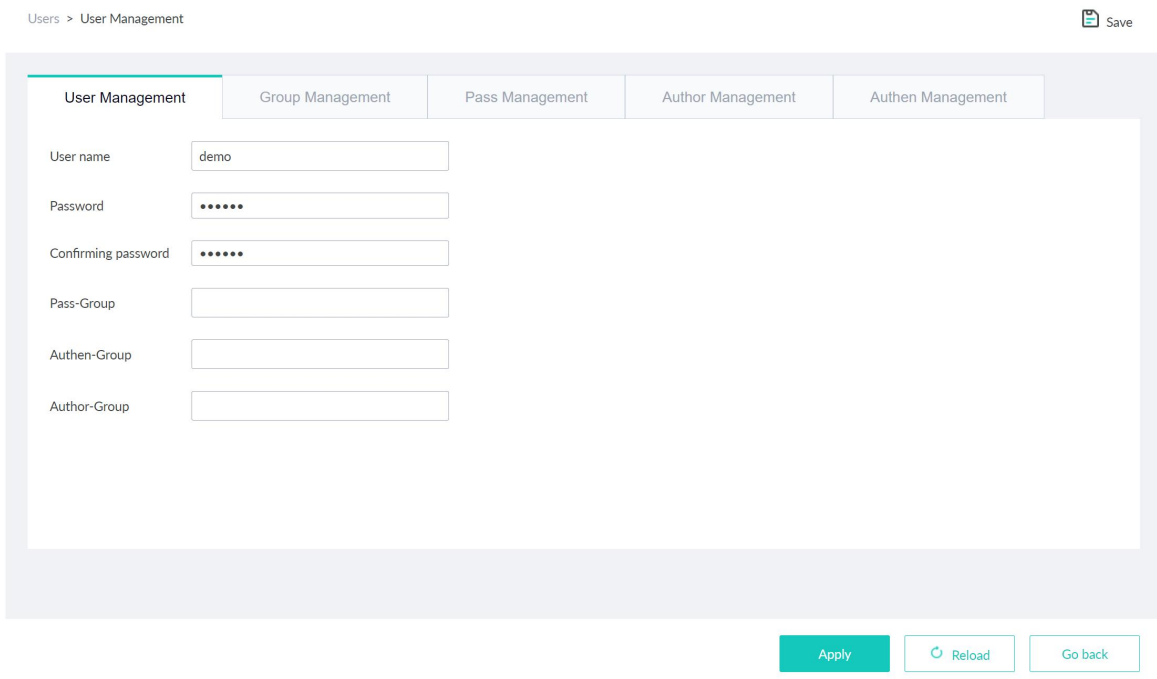
8.5 Users

8.5.1 User Management

If you click System -> Users -> User Management in the navigation bar, the page appears as shown as below figure:



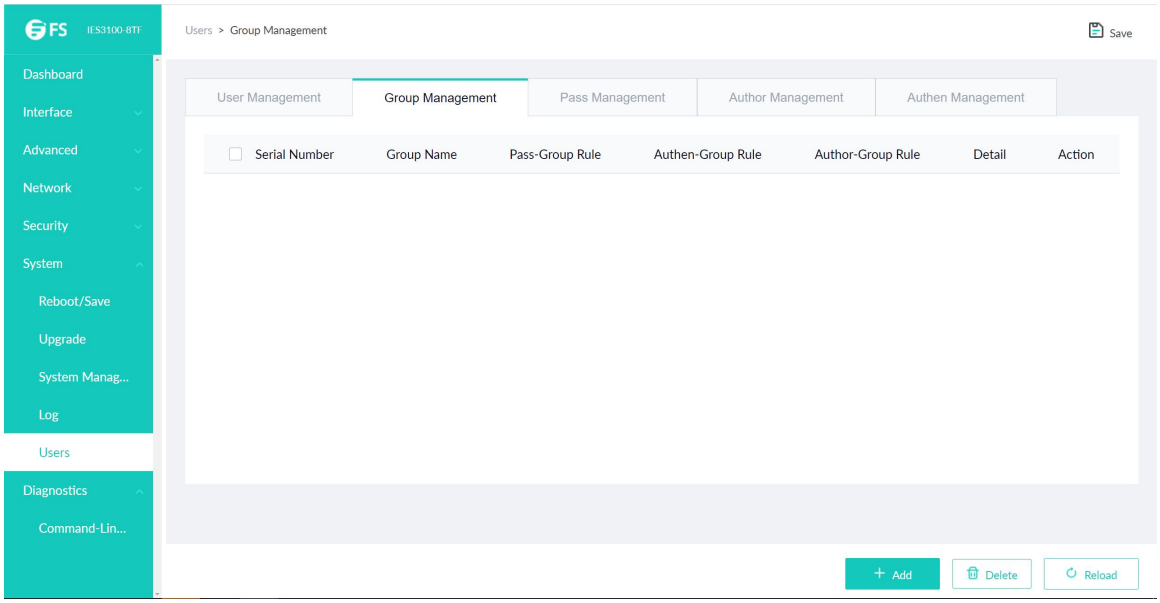
Click Edit icon to change user's configuration at this page, and then click Delete at the bottom bar after selecting user to delete user. Click Add at the bottom bar to enter the following page:



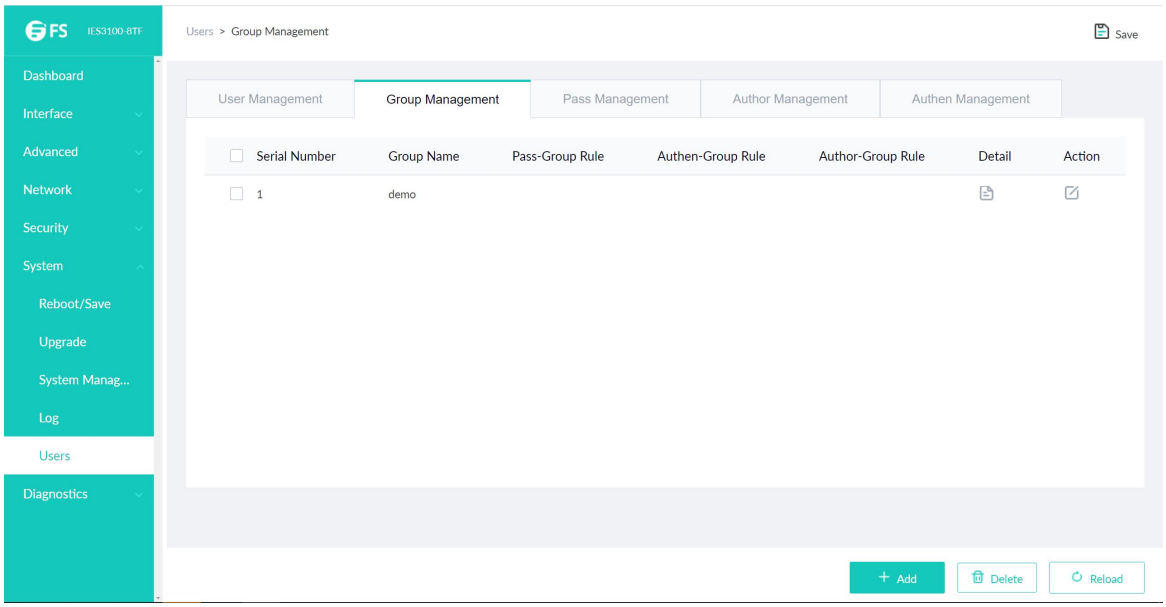
Fill in configuration at every configuration column and click Apply at the bottom bar to create new user.

8.5.2 Group Management

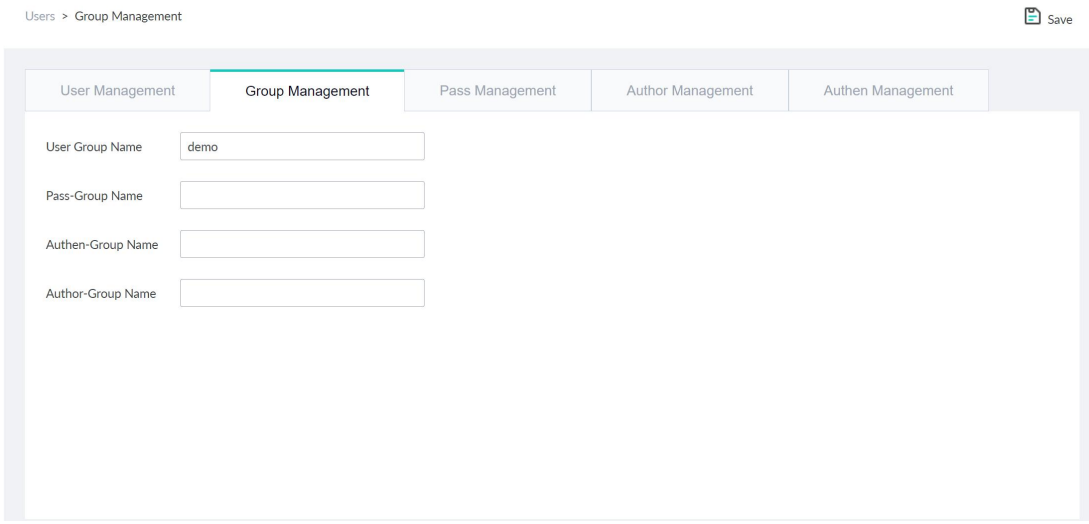
Click System -> Users -> Group Management, configuration page as following:



Click Edit icon to change user group's configuration at this page. Select user and click Delete at the bottom bar to delete user group. Click Details to check and configure members of group as following:



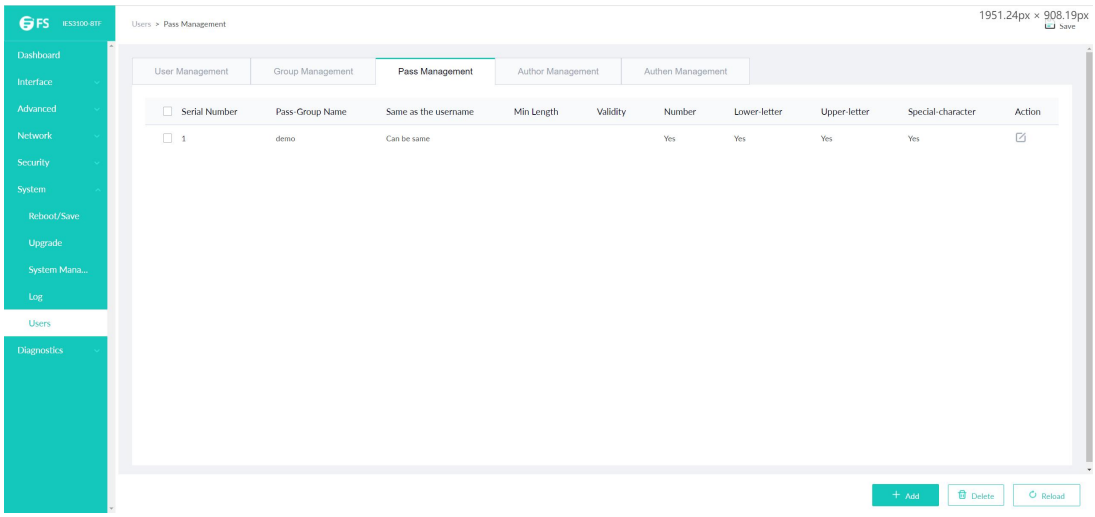
Click Add at the bottom bar of group management page to enter the following page:



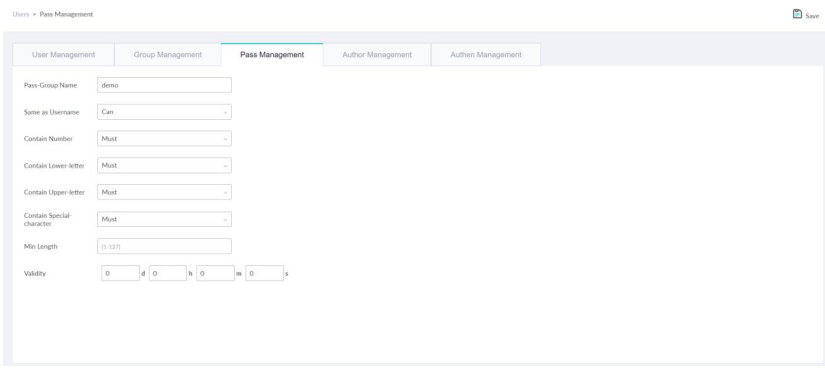
Fill in configuration at every configuration column and click Apply at the bottom bar to create new user group.

8.5.3 Pass Management

Click System -> Users -> Pass Management , configuration page as following:

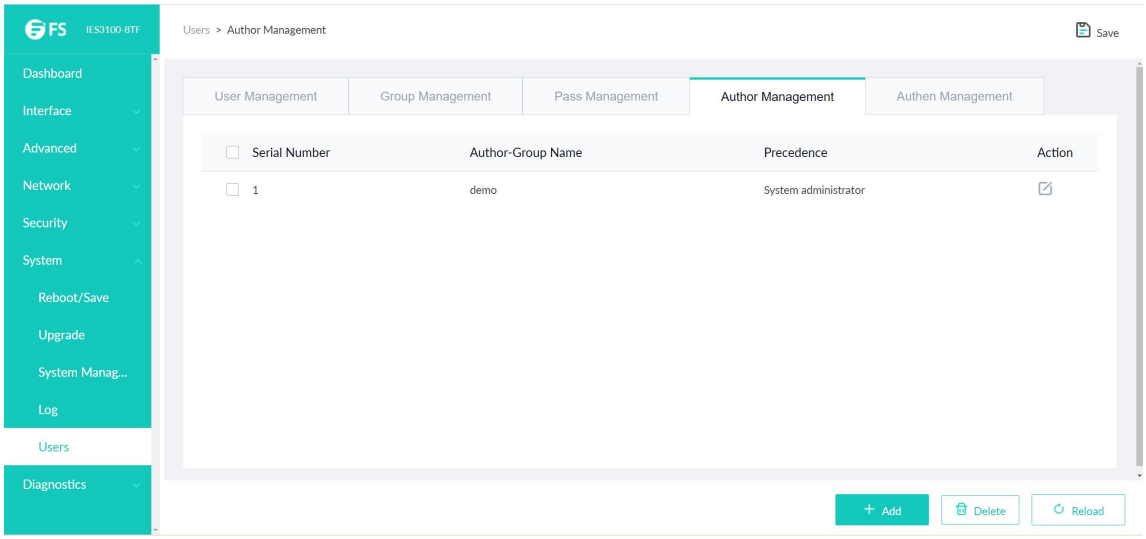


Click Edit icon to change password regulation at this page. Click Delete at the bottom bar to delete password regulation. Click Add at the bottom bar to enter the following page:



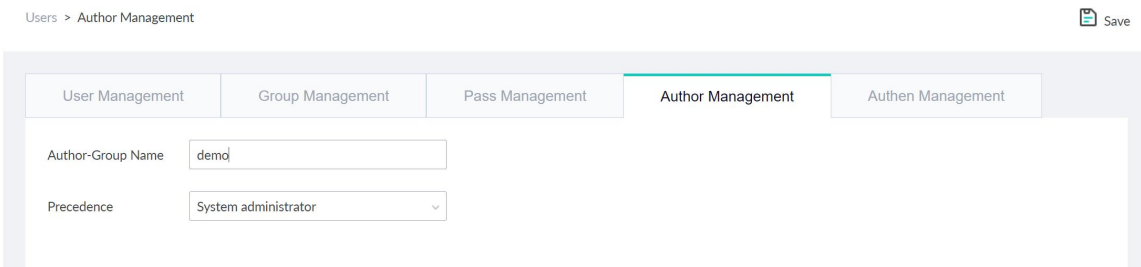
8.5.4 Author Management

Click System -> Users -> Author Management , configuration page as following:



Click Edit to change author rules at this page. Click Delete at the bottom bar to delete author rules.

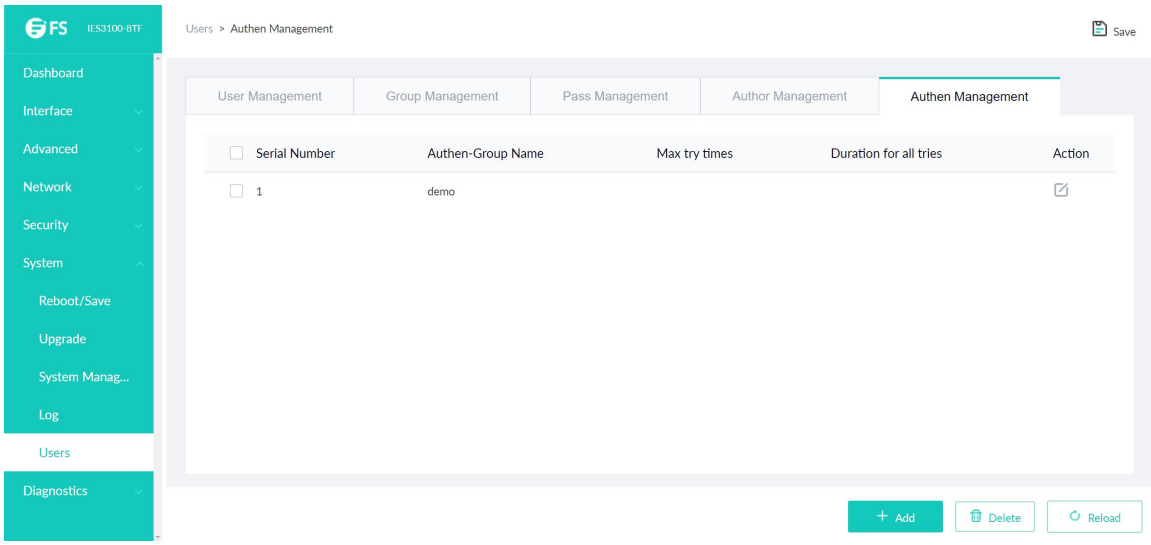
Click Add at the bottom bar to enter the following page:



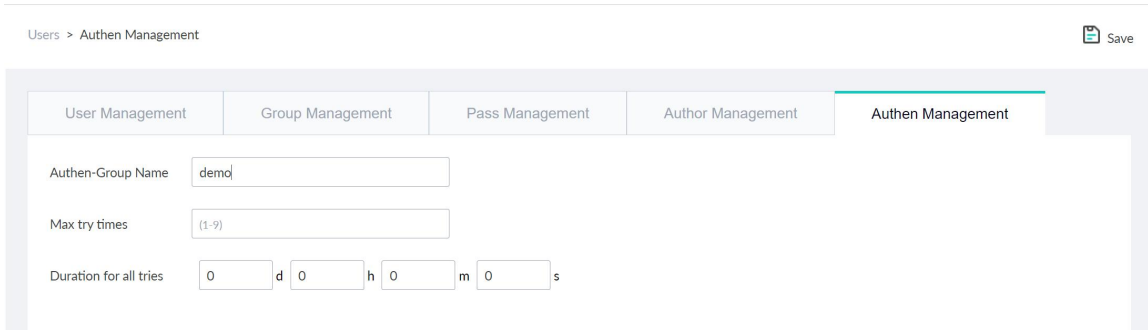
Fill in configuration at every configuration column and click Apply at the bottom bar to create new author rules.

8.5.5 Authen Management

Click System -> Users -> Authen Management , configuration page as following:



Click Edit icon to change authentication rules at this page. Click Delete at the bottom bar to delete authentication rules. Click Add at the bottom bar to enter the following page:



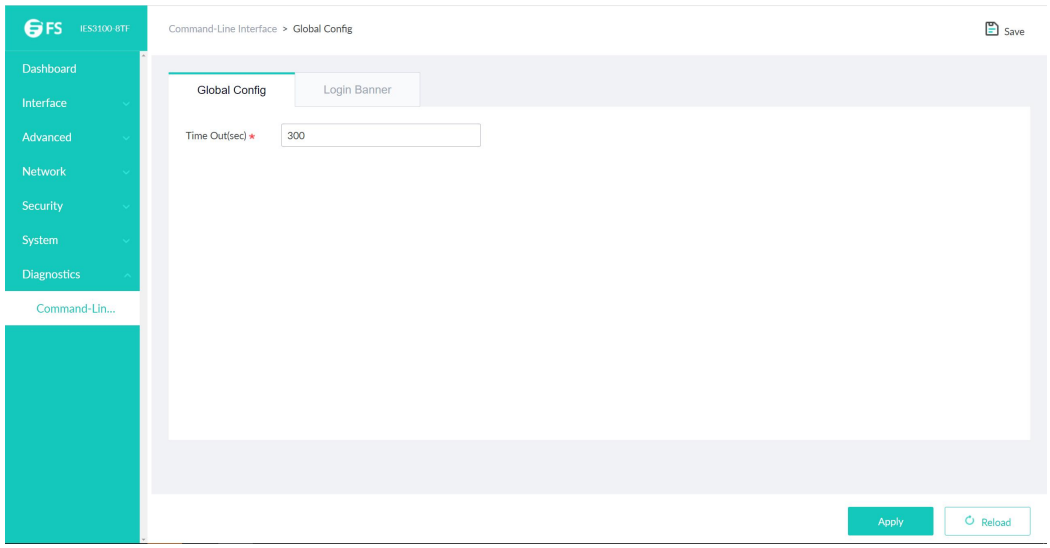
Fill in configuration at every configuration column and click Apply at the bottom bar to create new authentication rules.

Chapter 9 Diagnostics

9.1 Command-Line Interface

9.1.1 Global Config

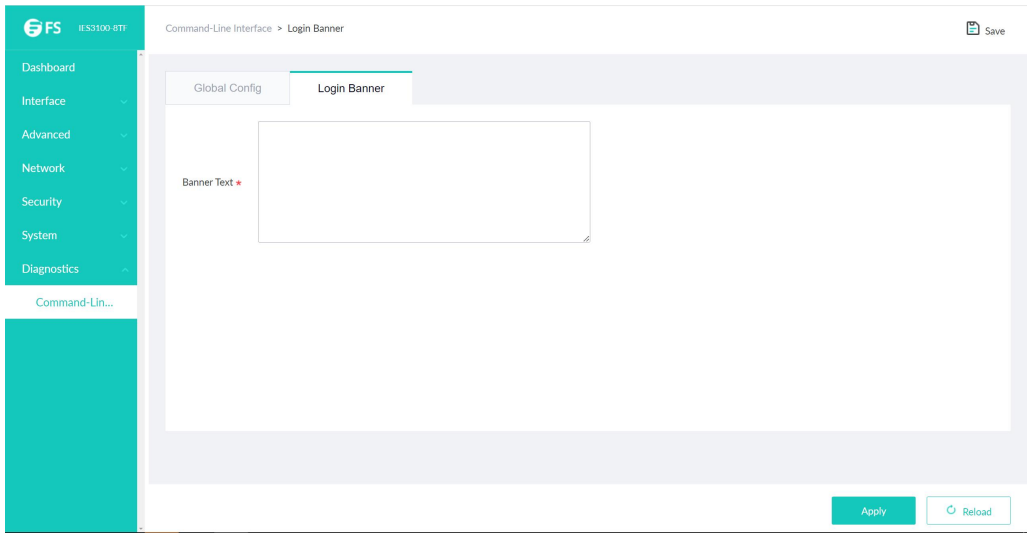
Click Diagnostics -> Command-Line Interface -> Global Config at navigation bar in order to enter configuration page as following:



Terminal's overtime time could be configured at this page, and if configured as 0, it means there would be never overtime.

9.1.2 Login Banner

Click Diagnostics -> Command-Line Interface -> Login Banner at navigation bar in order to enter configuration page as following:



Terminal's Login Banner could be configured at this page.