



Web Management Guide

XEL-0891 8-Port L3 Managed 10G Ethernet Switch
4 x 1G/2.5G/5G/10G RJ45, 4 x 1G/2.5G/10G SFP+ Uplinks

XEL-1291 12-Port L3 Managed 10-Gigabit Ethernet Switch
8 x 1G/2.5G/5G/10G RJ45, 4 x 1G/2.5G/10G SFP+ Uplinks,
240Gbps Non-Blocking Fabric, 19-Inch Rackmount

Directory

Getting Start.....	1
Web-based Switch Configuration	3
Console Port Interface	4
1.System Config.....	5
1.1.System Homepage	5
1.2.Device Info	5
1.3.IP Config.....	6
1.3.1.IPv4 Config	6
1.3.2.IPv6 Config	7
1.4.Web Config.....	7
1.4.1.Web Timeout	7
1.4.2.HTTP	8
1.4.3.HTTPS	8
1.4.4.Security IP	9
1.4.5.ACL	9
1.5.User Management.....	10
1.5.1.User Management	10
1.5.2.Authentication Method	11
1.6.Firmware Upgrade	12
1.6.1.TFTP Service	12
1.6.2.FTP Service	12
1.6.3.HTTP Upgrade	13
1.7.Management Config	13
1.7.1.TFTP	13
1.7.2.HTTP	13
1.8.NTP	14
1.8.1.NTP Config	14
1.8.2.NTP Authentication Config	14
1.9.SNTP	15
1.9.1.Server Config	15
1.9.2.Time Zone Config	15
1.10.Device Management.....	16
1.10.1.Device Reboot/Reset	16
1.10.2.System Utilization	16
1.10.3.View System Config	16
1.10.4.View Logging Buffer	17
1.10.5.View Logging Flash	17
2.Monitor Management.....	18
2.1.SSH Config.....	18
2.2.Telnet Config	18
2.3.Port Statistics	19
2.4.DDMI Status.....	20

2.5.Ping	21
2.6.Traceroute	21
2.7.Cable Diagnostics	22
2.8.SNMP Config	22
2.8.1.Global Config	22
2.8.2.User Config	23
2.8.3.Group Config	23
2.8.4.Community Config	24
2.8.5.Trap Config	24
2.8.6.View Config	25
2.8.7.Security IP Config	26
2.8.8.SNMP Statistics	26
2.9.Onvif Config	26
2.9.1.Server Config	26
2.9.2.Detect Config	27
2.10.Loopback Detection	27
2.10.1.Port Mode	27
2.10.2.VLAN Loopback	28
2.10.3.Interval Time	28
2.10.4.Recovery Timeout	29
2.11.LLDP Config	29
2.11.1.Global Config	29
2.11.2.Port Config	30
2.11.3.TLV Config	31
2.11.4.Neighbor Info	31
3.Switch Config	32
3.1.Port Config	32
3.1.1.Port Config	32
3.1.2.Port Combo Mode(Specific)	33
3.1.3.Port 10G Mode(Specific)	33
3.2.Port Mirror	34
3.3.Port Isolate	35
3.4.Port Channel	35
3.4.1.Port Channel Group	35
3.4.2.LACP	36
3.5.Jumbo Frame	37
3.6.Port Rate	37
3.7.Storm Control	38
3.8.MAC Address Config	38
3.8.1.Static MAC	38
3.8.2.Black Hole MAC	39
3.8.3.Aging-time	40
3.8.4.MAC Address List	40
3.9.AM	41

3.10.AAA.....	41
3.10.1.Radius	41
3.10.2.Radius Accounting	43
3.10.3.Tacacs	43
4.VLAN Config.....	45
4.1.VLAN Config	45
4.1.1.VLAN ID	45
4.1.2.Show VLAN	45
4.1.3.Port Config	45
4.2.GVRP Config.....	46
4.2.1.GVRP Config	46
4.2.2.GVRP Port	47
4.3.QINQ.....	47
4.3.1.Enable Dot1q Tunnel	47
4.3.2.Dot1q Tunnel TPID	48
4.4.Protocol VLAN.....	48
4.5.Voice VLAN.....	49
4.5.1.VLAN Config	49
4.5.2.Port Config	49
4.6.MAC VLAN	50
4.6.1.VLAN Config	50
4.6.2.VLAN Member	50
4.6.3.Port Config	50
5.DHCP Config.....	51
5.1.DHCP Server.....	51
5.1.1.Global Config	51
5.1.2.Create Address Pool	51
5.1.3.Dynamic Pool	52
5.1.4.Manual Pool	53
5.1.5.Default Gateway	54
5.1.6.DNS Server	54
5.1.7.Excluded Address	55
5.1.8.Packet Statistics	56
5.1.9.Client List	56
5.2.DHCP Snooping	56
5.2.1.Global Config	56
5.2.2.VLAN Config	57
5.2.3.Static User Binding	57
5.2.4.Helper-server Config	58
5.2.5.Port Binding	59
5.2.6.Trust Port	60
5.3.DHCP Relay Config	61
5.3.1.DHCP Relay Config	61
6.ACL Config	62

6.1.Time Range Config	62
6.2.IP ACL.....	63
6.2.1.IP Standard ACL	63
6.2.2.IP Extended ACL	63
6.3.MAC ACL	64
6.3.1.MAC Standard ACL.....	64
6.3.2.MAC Extended ACL	65
6.4.MAC-IP Extended ACL.....	66
6.5.ACL Binding.....	68
6.5.1.Binding Port	68
6.5.2.Binding Vlan.....	68
7.Ring Network.....	70
7.1.Spanning-tree	70
7.1.1.Global Properties	70
7.1.2.Instance Mapping.....	71
7.1.3.Instance Properties	72
7.1.4.Port Config	72
7.1.5.Port Instance	73
7.1.6.Status	74
7.2.ERPS	74
7.2.1.ERPS Ring Config.....	74
7.2.2.ERPS Instance Config	75
7.2.3.View ERPS Statistics	76
8.Route Config	78
8.1.Static Route.....	78
8.2.RIP Route	78
8.2.1.Keychain	78
8.2.2.Basic Config.....	79
8.2.3.Network Config.....	80
8.2.4.Passive Interface.....	81
8.2.5.Neighbor Config.....	81
8.2.6.Interface Config.....	82
8.2.7.Redistribute Router	82
8.2.8.View RIP Information.....	83
8.3.OSPF Route	84
8.3.1.Basic Config.....	84
8.3.2.Network Config.....	84
8.3.3.Passive Interface.....	85
8.3.4.Area Config.....	85
8.3.5.Interface Config.....	86
8.3.6.Interface Authentication	88
8.3.7.Default Route Originate	89
8.3.8.Redistribute Router	89
8.3.9.View OSPF Information	90

8.4.BGP Route.....	90
8.4.1.Basic Config	90
8.4.2.Network Config	91
8.4.3.Aggregate Address	92
8.4.4.Redistribute Router	92
8.4.5.Neighbor Config	93
8.4.6.BGP Correlative Config	93
8.4.7.Timer Config	95
8.4.8.View BGP Information	95
8.5.Routing Table	96
9.Multicast Manage	97
9.1.IGMP Snooping Config.....	97
9.1.1.Basic Config	97
9.1.2.Static Router Port	97
9.1.3.VLAN Config	98
9.1.4.Querier Config	99
9.1.5.Multicast Table	100
9.2.MLD Snooping Config	100
9.2.1.Basic Config	100
9.2.2.Static Router Port	100
9.2.3.VLAN Config	101
9.2.4.Querier Config	102
9.2.5.Multicast Table	102
10.QoS Config.....	103
10.1.Port Config.....	103
10.1.1.Trust Config	103
10.1.2.Weight Config	103
10.1.3.CoS-To-IntP Config	106
10.1.4.DSCP-To-IntP Config	106
10.1.5.Policy Config	107
10.2.Class-Map Config	107
10.2.1.Class-Map Config	107
10.2.2.Class-Map Rule Config	108
10.3.Policy-Map Config.....	111
10.3.1.Policy Name Config	111
10.3.2.Policy Class Config	112
10.3.3.Policy Mark Config	112
10.3.4.Policy Bandwidth	113
10.3.5.Policy VLAN	114

Getting Start

This section provides an introduction to the web-based configuration utility, and covers the following topics:

- Powering on the device
- Connecting to the network
- Starting the web-based configuration utility

● Power

Connecting to Power



Power down and disconnect the power cord before servicing or wiring a switch.



Do not disconnect modules or cabling unless the power is first switched off. The device only supports the voltage outlined in the type plate. Do not use any other power components except those specifically designated for the switch.



Disconnect the power cord before installation or cable wiring.

The switch is powered by the AC 100-240 V 50/60Hz internal high-performance power supply. It is recommended to connect the switch with a single-phase three-wire power source with a neutral outlet, or a multifunctional computer professional source.

Connect the AC power connector on the back panel of the switch to the external power source with the included power cord, and check the power LED is on.



Rear View AC Power Socket

● Connecting to the Network

To connect the switch to the network:

1. Connect an Ethernet cable to the Ethernet port of a computer
2. Connect the other end of the Ethernet cable to one of the numbered Ethernet ports of the switch. The LED of the port lights if the device connected is active.
3. Repeat Step 1 and Step 2 for each device to connect to the switch.

We strongly recommend using CAT-5E or better cable to connect network devices. When connecting network devices, do not exceed the maximum cabling distance of 100 meters (328 feet). It can take up to one minute for attached devices or the LAN to be operational after it is connected. This is normal behavior.

Connect the switch to end nodes using a standard Cat 5/5e Ethernet cable (UTP/STP) to connect the switch to end nodes as shown in the illustration below.

Switch ports will automatically adjust to the characteristics (MDI/MDI-X, speed, duplex) of the device to which the switch is connected.

● Starting the Web-based Configuration Utility

This section describes how to navigate the web-based switch configuration utility. Be sure to disable any pop-up blocker.

Browser Restrictions

- If you are using older versions of Internet Explorer, you cannot directly use an IPv6 address to access the device. You can, however, use the DNS (Domain Name System) server to create a domain name that contains the IPv6 address, and then use that domain name in the address bar in place of the IPv6 address.
- If you have multiple IPv6 interfaces on your management station, use the IPv6 global address instead of the IPv6 link local address to access the device from your browser.

Launching the Configuration Utility

To open the web-based configuration utility:

1. Open a Web browser.
2. Enter the IP address of the device you are configuring in the address bar on the browser (factory default IP address is 192.168.1.1) and then press Enter.

When the device is using the factory default IP address, its power LED flashes continuously. When the device is using a DHCP assigned IP address or an administrator-configured static IP address, the power LED is lit a solid color. Your computer's IP address must be in the same subnet as the switch. For example, if the switch is using the factory default IP address, your computer's IP address can be in the following range: 192.168.1.x (whereas x is a number from 2 to 254).

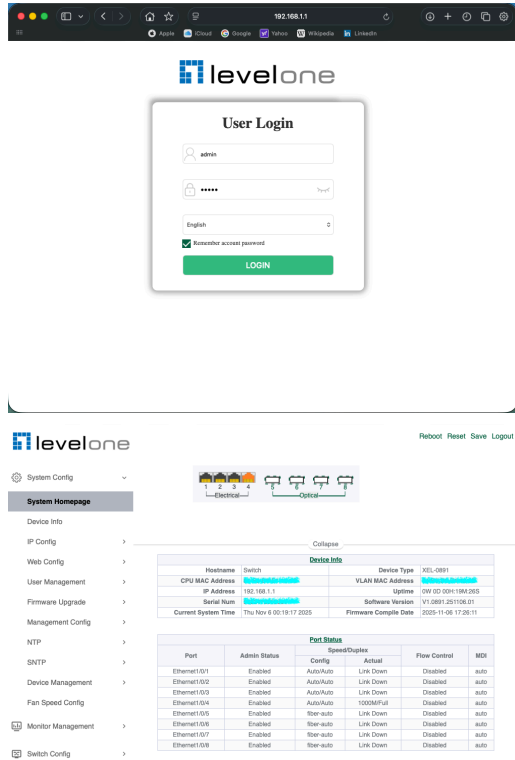
After a successful connection, the login window displays.

Logging In

The default username is admin and the default password is admin. The first time that you log in with the default username and password, you are required to enter a new password.

To log in to the device configuration utility:

1. Enter the default user ID (admin) and the default password (admin).
2. If this is the first time that you logged on with the default user ID (admin) and the default password (admin) it is recommended that you change your password immediately. When the login attempt is successful, the System Information window displays.



If you entered an incorrect username or password, an error message appears and the Login page remains displayed on the window. If you are having problems logging in, please see the Launching the Configuration Utility section in the Administration Guide for additional information.

● Logging Out

By default, the application logs out after ten minutes of inactivity.

To logout, click Logout in the top right corner of any page. The system logs out of the device. When a timeout occurs or you intentionally log out of the system, a message appears and the Login page appears, with a message indicating the logged-out state. After you log in, the application returns to the initial page.

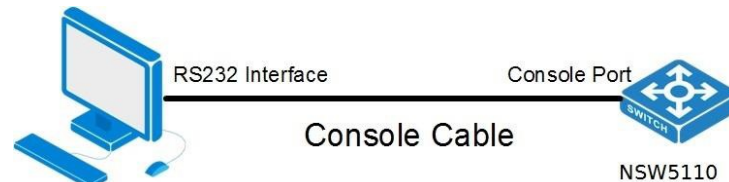
Web-based Switch Configuration

The smart switch software provides rich Layer 2 functionality for switches in your networks. This chapter describes how to use the web-based management interface (Web UI) to configure the switch's features.

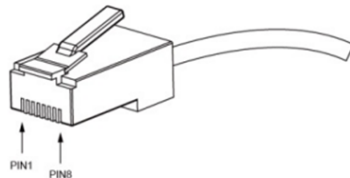
Console Port Interface

The PoE smart switch has a monitor port(Console port). Rate 9600bps, standard RJ45 plug.

Use a dedicated monitoring cable to lead the port to the PC serial port connection, as follows:



The RJ45 connector used by the Console port is shown in the figure below, and the RJ45 plug corresponds to the RJ45 socket, from left to right numbered from 1 to 8.



This cable is used to connect the console port of the switch to the external monitoring terminal. One end of the RJ45 eight-pin plug, the other end is a 25-hole plug(DB25) and 9-hole plug(DB9), RJ45 head into the switch's console port socket, DB25 and DB9 can be used according to the requirements of the terminal serial port, the cable internal connection schematic as follows:

RJ45	<===>	DB9
[RTS 1~~~8 CTS]
[DTR 2~~~6 DSR]
[TXD 3~~~2 RXD]
[GND 4~~~5 GND]
[GND 5~~~5 GND]
[RXD 6~~~3 TXD]
[DSR 7~~~4 DTR]
[CTS 8~~~7 RTS]

1.System Config

1.1.System Homepage

The system homepage contains **Device Info** and **Port Status**

Device Info					
Hostname	Switch	Device Type	XEL-0891		
CPU MAC Address	00:00:00:00:00:00	VLAN MAC Address	00:00:00:00:00:00		
IP Address	192.168.1.1	Uptime	0W 0D 00H:19M:26S		
Serial Num	0000000000000000	Software Version	V1.0891.251106.01		
Current System Time	Thu Nov 6 00:19:17 2025	Firmware Compile Date	2025-11-06 17:26:11		

Port Status					
Port	Admin Status	Speed/Duplex		Flow Control	MDI
		Config	Actual		
Ethernet1/0/1	Enabled	Auto/Auto	Link Down	Disabled	auto
Ethernet1/0/2	Enabled	Auto/Auto	Link Down	Disabled	auto
Ethernet1/0/3	Enabled	Auto/Auto	Link Down	Disabled	auto
Ethernet1/0/4	Enabled	Auto/Auto	1000M/Full	Disabled	auto
Ethernet1/0/5	Enabled	fiber-auto	Link Down	Disabled	auto
Ethernet1/0/6	Enabled	fiber-auto	Link Down	Disabled	auto
Ethernet1/0/7	Enabled	fiber-auto	Link Down	Disabled	auto
Ethernet1/0/8	Enabled	fiber-auto	Link Down	Disabled	auto

Click on **Device Info** or **Port Status** to enter the corresponding page.

1.2.Device Info

The Device Info page allows you to view device information and also set the Hostname, Device Contact, Device Location of the device and the Current System Time.

Reboot

Reset

Save

Logout

System Config

System Homepage

Device Info

IP Config

Web Config

User Management

Firmware Upgrade

Management Config

NTP

SNTP

Device Management

Fan Speed Config

Monitor Management

Switch Config

1

2

3

4

Electrical

5

6

7

8

Optical

Collapse

Device Info

Hostname	Switch
Device Contact	Default
Device Location	Im Delfdahl 10 F,44141 Dortmund,Ge
Device Type	XEL-0891
CPU MAC Address	00:00:00:00:00:00
VLAN MAC Address	00:00:00:00:00:00
IP Address	192.168.1.1
Client IP Address	192.168.1.66
Serial Num	0000000000000000
Software Version	V1.0891.251106.01
BootRom Version	V2.00
Firmware Compile Date	2025-11-06 17:26:11
Uptime	0W 0D 00H:26M:32S
Current System Time	00 Hour 26 Min 23 Sec 2025 Year 11 Month 06 Day

Apply

Hostname	Fill in the new Hostname of the switch to be changed, 1-64 characters
Device Contact	Fill in the new Device Contact of the switch to be changed, 0-255 characters
Device Location	Fill in the new Device Location of the switch to be changed, 0-255 characters
Current System Time	Manually changing the current system time, When the switch restart will invalidate.

1.3.IP Config

1.3.1.IPv4 Config

The page can be used to configure IP address and subnet mask for the VLAN interface.

To display the "IPv4 Config" page, click System Config -> IP Config -> IPv4 Config, click "Apply" to configure.

The screenshot displays the H3C iLevelOne web interface. The left sidebar contains a navigation menu with options: System Config, System Homepage, Device Info, IP Config, IPv4 Config (selected), IPv6 Config, Web Config, User Management, Firmware Upgrade, Management Config, NTP, SNTP, Device Management, Fan Speed Config, and Monitor Management. The main content area is titled 'IPv4 Config' and features a form with the following fields: VLAN Interface (VLAN0001), IP Mode (Static IP), IP Address (192.168.1.1), and Netmask (255.255.255.0). Below the form is a table showing the configuration details for VLAN0001, including IP Mode, IP Address, and Netmask. The table has a 'Delete' button and navigation controls (First, Previous, Next, Last).

VLAN Interface	VLAN ID of layer 3 interface created
IP Mode	Static IP: User self configuration Dynamic: dhcp-client Automatic acquisition
IP Address	IP Address, e.g. A.B.C.D
Netmask	Netmask:for example :255.255.255.0
Operation	Action: Apply/Delete

1.3.2.IPv6 Config

The page can be used to configure IPv6 address and subnet mask for the VLAN interface.

To display the “IPv6 Config” page, click System Config ->IP Config->IPv6 Config, click "Apply" to configure.

VLAN Interface	VLAN ID of layer 3 interface created
IPv6 Address	IPv6 Address, Example:2001::1234
Prefix-length	Prefix length is 3 to 127, Example :48
Operation	Action: Apply/Delete

1.4.Web Config

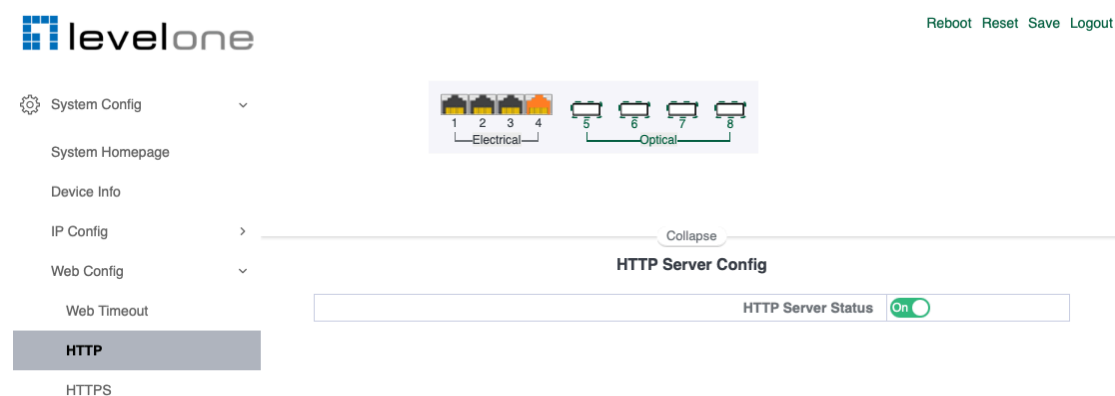
1.4.1.Web Timeout

The page can be used to configure Web Login Timeout time.

Web Login Timeout	Web Login Timeout: 1-60 minutes,default 10 minutes
--------------------------	----------------------------------------------------

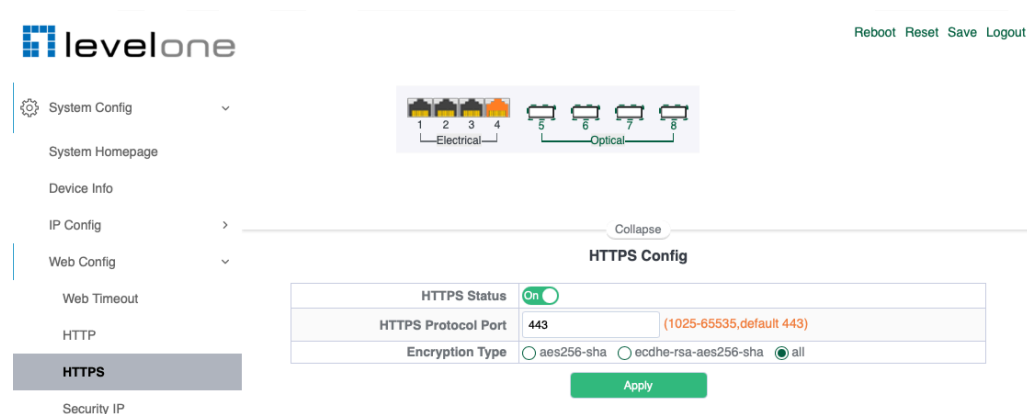
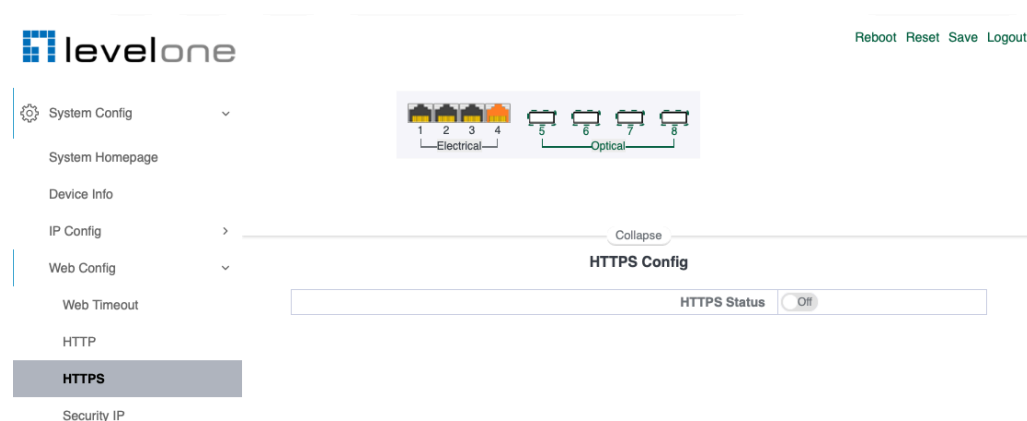
1.4.2.HTTP

HTTP Server Config module,the user can start or stop the HTTP service of the switch by using this module again.Default is On.



1.4.3.HTTPS

HTTPS Server Config module,the user can start or stop the HTTPS service of the switch by using this module again.Default is Off.



HTTPS Protocol Port	HTTPS Protocol Port: 1025-65535 ,default 443
Encryption Type	Type: aes256-sha ecdhe-rsa-aes256-sha

1.4.4.Security IP

Login user security IP configuration module, where users can configure the security IPv4 address for login switch. Login methods include Telnet/HTTP/HTTPS.

Security IP address	Fill in the specified security IPv4 address	
Operation	Apply	Add address or list number
	Delete	Delete address or list number

1.4.5.ACL

Login user login access control list module, where users can configure the IPV4 access control list. Login methods include Telnet/SSH/Web.

IPv4 access control list	Standard access control list number, scope 1-64 characters or number 1-99	
Binding Method	Binding Method include web/ssh/telnet/all	
Operation	Apply	Add address or list number
	Delete	Delete address or list number

1.5.User Management

1.5.1.User Management

levelone Reboot Reset Save Logout

System Config System Homepage Device Info IP Config Web Config User Management **User Management** Authentication Method Firmware Upgrade Management Config NTP SNTP Device Management Fan Speed Config Monitor Management

User Management

Username (1-32 characters)
Password ☐ Encrypted Text (Plain Text:1-32 characters)
Priority (number 1-15)

Apply

No.	Username	Password	State	Priority
1	admin	admin	Plain Text	15

Delete

WEB Privilege Config

Login Privilege Enable Disabled
Privilege Priority 15

Apply

User Management module, users in this module can add or delete user operations.

Username	User name to operate ,1-32 characters
Password	User password, choose the password encryption, otherwise no encryption of 1-32 characters
Priority	Used to specify permission level.

WEB Privilege Config module, users can configure permissions for user accounts to login in the web.

WEB Privilege Config


Login Privilege Enable Disabled
Privilege Priority 15

Apply


Login Privilege Enable	Change the way users log in to web pages with permissions, When the user priority is lower than the privilege priority, it changes from being unable to log in to being able to log in to the web page but not configure information, and can only view the configuration. Default is disable.
Privilege Priority	Used to specify permission level, default level 15, only the user with the level that is equal to or higher than it can login in the switch by web.

1.5.2.Authentication Method

User Login Authentication Method Configure module, the user can configure console.vty.web authentication method used in login, authentication method can be any one or combination of Local.RADIUS and TACACS preferences from left to right when the login method is combined configuration. If the user has passed the authentication method, the authentication method of the lower preference is ignored. As long as you pass an authentication method, the user can log in.AAA functions and RADIUS servers should be configured before using RADIUS authentication.If local authentication is configured without configuring a local user, the user will be able to log on to the switch through the console method.


Reboot Reset Save Logout

- System Config
- System Homepage
- Device Info
- IP Config
- Web Config
- User Management
- User Management
- Authentication Method**
- Firmware Upgrade
- Management Config
- NTP
- SNTP
- Device Management
- Fan Speed Config
- Monitor Management



User Login Authentication Method Configure

Login Method	Console
Authentication Method1	None
Authentication Method2	None
Authentication Method3	None
Operation Type	Configuration

Apply

Login Method	Authentication Method1	Authentication Method2	Authentication Method3
console	local	None	None
vtty	local	None	None
web	local	None	None

Only when the console authentication mode is 'none', can the login authentication mode be configured.

Login Authentication	Disabled
Login Authentication Password	<div style="border: 1px solid #ccc; height: 20px; width: 100%;"></div> Encrypted Text (Plain Text:1-32 characters)

Apply

Login method	Authentication method	
console	local	Authentication using the local user account database
vtty	radius	Authentication using remote Radius server
web	tacacs	Authentication using remote Tacas server
Default	Default console no authentication , vty and web local authentication	

Only when the console authentication mode is 'none', can the login authentication mode be configured.

Login Authentication	Disabled
Login Authentication Password	<div style="border: 1px solid #ccc; height: 20px; width: 100%;"></div> Encrypted Text 1-32 characters

Apply

Login Authentication	Default is Disable.
Login Authentication Password	Login Authentication password, choose the password encryption, otherwise no encryption of 1-32 characters

1.6.Firmware Upgrade

1.6.1.TFTP Service

TFTP client service module, the user can upload or download files by TFTP way, and can upgrade the firmware of the switch by this method.

TFTP Service

Server IP Address	<input type="text"/>	Example:10.10.10.1
Server File Name	<input type="text"/>	1-100 characters, Example: nos.img
Operation Type	Upload	
Transmission Type	binary	

Server IP address	TFTP address IP peer server, point decimal	
Server File name	Source name to upload or download ,1-100 characters	
Operation type	Upload	Upload upgrade files from the switch to the TFTP server
	Download	Download upgrade files from TFTP server to switch
Transmission type	binary	Transfer files in binary format (default)
	ascii	Transfer files in ascii format

1.6.2.FTP Service

FTP client service module, the user can upload or download files by FTP way, and can upgrade the firmware of the switch by this method.

FTP Service

Server IP Address	<input type="text"/>	Example:10.10.10.1
Username	<input type="text"/>	1-100 characters
Password	<input type="text"/>	1-100 characters
Server File Name	<input type="text"/>	1-100 characters, Example: nos.img
Operation Type	Upload	
Transmission Type	binary	

Server IP Address	FTP address IP peer server, point decimal	
Username	FTP server-to-server username ,1-100 characters	
Password	FTP server-side user password 1-100 characters	
Server File Name	Source name to upload or download ,1-100 characters	
Operation Type	Upload	Upload upgrade files from the switch to the TFTP server

	Download	Download upgrade files from TFTP server to switch
Transmission Type	binary	Transfer files in binary format (default)
	ascii	Transfer files in ascii format

1.6.3.HTTP Upgrade

HTTP Upgrade module, the user can select file by HTTP way, and can upgrade the firmware of the switch by this method.

Local Upgrade

Select File

Decompress the package and select the img file for upgrade.

1.7.Management Config

1.7.1.TFTP

TFTP module, the user can import or export switch configuration by tftp.

Import Configuration

Server IP Address	<input type="text"/>	Example:10.10.10.1
Server File Name	<input type="text"/>	1-100 characters, Example: startup.cfg
Transmission Type	binary	

Apply

Export Configuration

Server IP Address	<input type="text"/>	Example:10.10.10.1
Server File Name	<input type="text"/>	1-100 characters, Example: startup.cfg

Apply

Server IP Address	TFTP address IP peer server, point decimal	
Server File Name	Source name to upload or download ,1-100 characters	
Transmission Type	binary	Transfer files in binary format (default)
	ascii	Transfer files in ascii format

1.7.2.HTTP

HTTP module, the user can **Download** or **Upload** switch **Running Configuration** or **Startup Configuration** by http.

HTTP Upload or Download File

Operation Type	Download
File Type	Running Configuration

Apply

Operation Type	Download	To download files
	Upload	To upload files
File Type	Running Configuration	Switch running configuration
	Startup Configuration	Switch startup configuration

1.8.NTP

1.8.1.NTP Config

NTP Config module, user can NTP service global switch operation.

NTP Global Config

NTP Global Config

Off

NTP Global config Operation	Off	Close operation(default)
	On	Start

NTP the server configuration module, the user can configure the specified time server of the switch time source in this module.

NTP Server Config

Server Address	<input type="text"/>	IP address type,for example:10.10.10.1
Version	<input type="text"/>	Version Range:1-4
Key ID	<input type="text"/>	Key ID Range:1-4294967295

[Apply](#)

Showing

10

 Entries

Showing 1 to 1 of 1 entries

Search

<input type="checkbox"/>	No.	Server Address	Version	Key ID	
<input type="checkbox"/>	1	162.159.200.123	4	0	

[Delete](#)

[First](#) [Previous](#) [1](#) [Next](#) [Last](#)

Server address	The specified time server address decimal point	
Version	Version number, range 1-4, default 4	
Key ID	Secret key value, range 1-4294967295	
Operation	Apply	Add operations
	Delete	Delete operations

1.8.2.NTP Authentication Config

NTP verification configuration module, the user can configure the switch NTP authentication related items.

NTP Authentication Config

NTP Authentication Function	<div>Disabled</div>
Key ID	<input type="text"/> Key ID Range:1-4294967295
MD5 For Key ID	<input type="text"/> 1-16 Characters ASCII

[Apply](#)

Showing

10

 Entries

Showing 0 to 0 of 0 entries

Search

<input type="checkbox"/>	No.	Key ID	MD5 For Key ID	
0 results found.				

[Delete](#)

[First](#) [Previous](#) [Next](#) [Last](#)

NTP authenticate switch	Disable	Close NTP validation (default)
	Enable	Enable NTP validation
Key ID	Secret key value, range 1-4294967295	

MD5 For Key ID	The MD5 value of the secret key, which ranges from 1-16 of ascii code	
Operation	Apply	Add operations
	Delete	Delete operations

1.9.SNTP

1.9.1.Server Config

SNTP the server settings module, the user can add or delete the specified time server as the clock source.

SNTP Server Config

Server Address	<input type="text"/>	<small>IP address type,for example:10.10.10.1</small>
Version	<input type="text"/>	<small>Version Range:1-4</small>

<input type="checkbox"/>	No.	Server Address	Version	State

Server address	The specified time server address decimal point	
Version	Version number, range 1-4, default 4	
Operation	Apply	Add operations
	Delete	Delete operations

1.9.2.Time Zone Config

SNTP the time zone and UTC time difference setting module where the client is located, the user can set the switch's current time zone and name it.

Time Zone Config

Time Zone	<input type="text" value="UTC"/>	<small>(1-16 character)</small>
Time Difference	<input checked="" type="radio"/> After-utc <input type="radio"/> Before-utc	
Time Value	<input type="text" value="00"/> <input type="text" value="00"/>	<small>Range:0-23,0-59</small>
Operation Type	<input type="button" value="Add"/>	

Time zone	Time zone name ,1-16 characters		
Time difference	After-utc	Increased time zone behavior	
	Before-utc	Reduced time zone behavior	
Time value	Time zone specific change hours 0-23		Time zone specific change minute value 0-59
Operation	Add	Add operations	
	Default	Restore time zone default configuration	

1.10.Device Management

1.10.1.Device Reboot/Reset

Device Reboot/Reset module, the user can restart the switch by **Reboot** button. can also leave the factory initial settings restart by **Reset** button, but also can save the current set configuration by **Save** button.


Device Management		
Reboot	Reboot	Reboot the switch.
Default	Reset	Restore factory configuration and reboot the switch.
Save	Save	Save current device configure.

1.10.2. System Utilization

This module is used to display resource usage cpu current system but also display the current system memory resource usage.

levelone
Reboot Reset Save Logout

- Web Config >
- User Management >
- Firmware Upgrade >
- Management Config >
- NTP >
- SNTp >
- Device Management >
 - Device Reboot/Reset
- System Utilization**
- View System Config
- View Logging Buffer
- View Logging Flash
- Fan Speed Config



[Collapse](#)

Show cpu usage

Last 5 second CPU usage	6%
Last 30 second CPU usage	7%
Last 1 minute CPU usage	8%
Last 5 minute CPU usage	8%
From running CPU usage	8%

Show memory usage

The memory total	512 MB
Free	425009152 Bytes
Usage	20.84%

1.10.3.View System Config

This module is used to display configuration information in the current system run.

Web Config >

User Management >

Firmware Upgrade >

Management Config >

NTP >

SNTp >

Device Management >

Device Reboot/Reset

System Utilization

View System Config

View Logging Buffer

View Logging Flash

Fan Speed Config

Monitor Management >

Switch Config >

VLAN Config >

DHCP Config >

[Reboot](#)
[Reset](#)
[Save](#)
[Logout](#)

Collapse

Current System Operation Configuration

```

!
no service password-encryption
!
hostname Switch
sysLocation Im Delfahl 10 F,44141 Dortmund,Germany
sysContact Default
!
multi config access
!
username admin privilege 15 password 0 admin
!
authentication line console login local
!
!
!
fanspeed auto
!
!
!
!
!
!
vlan 1
            
```

1.10.4.View Logging Buffer

This module is used to display system logging information in the current system run.

levelone

Reboot Reset Save Logout

Web Config >

User Management >

Firmware Upgrade >

Management Config >

NTP >

SNTP >

Device Management >

Device Reboot/Reset

System Utilization

View System Config

View Logging Buffer

View Logging Flash

Fan Speed Config

Monitor Management >

Switch Config >

VLAN Config >

DHCP Config >

1 2 3 4

Electrical

5 6 7 8

Optical

Collapse

System Buffer Log

Current messages in SDRAM:5
5 %Nov 06 00:01:17.320 2025 <critical> DEFAULT[zimi]:System cold restart...
4 %Nov 06 00:00:18.760 2025 <warnings> DEFAULT[IPTimer]:%LINEPROTO-5-
UPDOWN: Line protocol on Interface Vlan1,changed state to UP
3 %Nov 06 00:00:17.750 2025 <warnings> MODULE_ETHDRV[phyDaemon]:%PORT-5-
UPDOWN: Interface Ethernet1/0/4, changed state to UP
2 %Nov 06 00:00:16.200 2025 <warnings> DEFAULT[zL2_shell]:%LINK-5-
CHANGED: Interface Vlan1, changed state to UP
1 %Nov 06 00:00:00.000 2025 <critical> DEFAULT[UserRoot]:Switch is start, software version is V1.0891.251106.01

1.10.5.View Logging Flash

This module is used to display system flash log information in the current system run.

levelone

Reboot Reset Save Logout

Web Config >

User Management >

Firmware Upgrade >

Management Config >

NTP >

SNTP >

Device Management >

Device Reboot/Reset

System Utilization

View System Config

View Logging Buffer

View Logging Flash

Fan Speed Config

Monitor Management >

Switch Config >

VLAN Config >

DHCP Config >

1 2 3 4

Electrical

5 6 7 8

Optical

Collapse

System Flash Log

Allowed max messages:655,Current messages:136
136 %Nov 06 00:01:17.320 2025 <critical> DEFAULT[zimi]:System cold restart...
135 %Nov 06 00:00:00.000 2025 <critical> DEFAULT[UserRoot]:Switch is start, software version is V1.0891.251106.01
134 %Nov 06 00:02:54.400 2025 <critical> MODULE_VPLS_PACKET[zimi]:fs_write_file 1631: FS_DEV_UNLOCK Slot:
1 dev_name:flash: file_name:flash/startup.cfg
133 %Nov 06 00:02:54.370 2025 <critical> MODULE_VPLS_PACKET[zimi]:fs_write_file 1612: FS_DEV_LOCK_NO_W
AIT Slot: 1 dev_name:flash: file_name:flash/startup.cfg
132 %Nov 06 00:01:17.330 2025 <critical> DEFAULT[zimi]:System cold restart...
131 %Nov 06 00:00:00.000 2025 <critical> DEFAULT[UserRoot]:Switch is start, software version is V1.0891.251106.01
130 %Nov 06 05:32:03.110 2025 <critical> MODULE_VPLS_PACKET[zimi]:fs_write_file 1631: FS_DEV_UNLOCK Slot:
1 dev_name:flash: file_name:flash/startup.cfg
129 %Nov 06 05:32:03.080 2025 <critical> MODULE_VPLS_PACKET[zimi]:fs_write_file 1612: FS_DEV_LOCK_NO_W
AIT Slot: 1 dev_name:flash: file_name:flash/startup.cfg
128 %Nov 06 00:01:17.750 2025 <critical> DEFAULT[zimi]:System warm restart...
127 %Nov 06 00:00:00.000 2025 <critical> DEFAULT[UserRoot]:Switch is start, software version is V1.0891.251106.01
126 %Sep 30 00:10:26.500 2025 <critical> DEFAULT[WebCfg]:System will be rebooted (warm reboot), reason: reload
via WEB
125 %Sep 30 00:10:23.830 2025 <critical> DEFAULT[WebCfg]:Write file nos.img OK
124 %Sep 30 00:10:23.830 2025 <critical> MODULE_VPLS_PACKET[WebCfg]:fs_write_file 1631: FS_DEV_UNLOCK
Slot: 1 dev_name:flash: file_name:flash/nos.img
123 %Sep 30 00:08:47.970 2025 <critical> MODULE_VPLS_PACKET[WebCfg]:fs_write_file 1612: FS_DEV_LOCK_N
O_WAIT Slot: 1 dev_name:flash: file_name:flash/nos.img
122 %Sep 30 00:08:47.970 2025 <critical> DEFAULT[WebCfg]:Begin to write file nos.img.
121 %Sep 30 00:01:16.750 2025 <critical> DEFAULT[zimi]:System cold restart...
120 %Sep 30 00:00:00.000 2025 <critical> DEFAULT[UserRoot]:Switch is start, software version is V1.250930
119 %Sep 30 00:01:16.750 2025 <critical> DEFAULT[zimi]:System cold restart...
118 %Sep 30 00:00:00.000 2025 <critical> DEFAULT[UserRoot]:Switch is start, software version is V1.250930
117 %Sep 30 00:01:16.740 2025 <critical> DEFAULT[zimi]:System warm restart...
116 %Sep 30 00:00:00.000 2025 <critical> DEFAULT[zimi]:System cold restart...

2. Monitor Management

2.1. SSH Config

SSH Config module, the user can configure the SSH status and SSH timeout.

SSH Config

Enabled ☐ Off

SSH Config

Enabled ☒ On

SSH Server Configuration

Timeout Time	180	(10-600s, Default:180s)
Maximum Connection	5	(1-16, Default:5)

Apply

Enabled Operation	Off: Close operation(default)	
	On: Start	
Timeout Time	Timeout of exit SSH login status ,10-600 seconds(default 180 s)	
Maximum Connection	Maximum number of connections logged in by SSH, range 1-16(default 5)	
Operation	Apply	Add operations

2.2. Telnet Config

Telnet server status module, where users can enabled on or off login switches by Telnet.

Telnet Server State

Enabled ☒ On

Telnet connect the maximum number module, the user can configure the maximum number of connections to the switch by Telnet.

Maximum Connection

Telnet Connection Number	5	(1-16, Default:5)
--------------------------	---	-------------------

Apply

Telnet access connection number	Maximum number of connections logged in by Telnet, range 1-16(default 5)
Operation	Apply, Add operations

2.3.Port Statistics

This page displays port statistics information.

- System Config
- Monitor Management
- SSH Config
- Telnet Config
- Port Statistics**
- DDMI Status
- Ping
- Traceroute
- Cable Diagnostics
- SNMP Config
- RMON Config
- Onvif Config

Reboot Reset Save Logout

Collapse

Port Statistics

PORT	Link Status	Rate(bps) (R/T)	Rate(pps) (R/T)	unicast packets (R/T)	multicast packets (R/T)	broadcast packets (R/T)	input errors	output errors	CRC (R)	frame alignment (R)	overrun (R)	ignored (R)	abort (R)	length error (R)	undersize (R)	jabber (R)	fragments (R)	collisions (T)	late collisions (T)	pause frame (R/T)
Ethernet1/01	Disconnect	0/0	0/0	0.0/0.0	0.0/0.0	0.0/0.0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Ethernet1/02	Disconnect	0/0	0/0	0.0/0.0	0.0/0.0	0.0/0.0	0	0	0	0	0	0	0	0	0	0	0	0	0	
Ethernet1/03	Disconnect	0/0	0/0	0.0/0.0	0.0/0.0	0.0/0.0	0	0	0	0	0	0	0	0	0	0	0	0	0	
Ethernet1/04	Connected	2305/3748	3/3	27906.6/27288.0	108.0/2.0	172.0/41.0	0	0	0	0	0	0	0	0	0	0	0	0	0	
Ethernet1/05	Disconnect	0/0	0/0	0.0/0.0	0.0/0.0	0.0/0.0	0	0	0	0	0	0	0	0	0	0	0	0	0	
Ethernet1/06	Disconnect	0/0	0/0	0.0/0.0	0.0/0.0	0.0/0.0	0	0	0	0	0	0	0	0	0	0	0	0	0	
Ethernet1/07	Disconnect	0/0	0/0	0.0/0.0	0.0/0.0	0.0/0.0	0	0	0	0	0	0	0	0	0	0	0	0	0	
Ethernet1/08	Connected	0/0	0/0	0.0/0.0	0.0/0.0	0.0/0.0	0	0	0	0	0	0	0	0	0	0	0	0	0	

Refresh
Delete

Port	physical ports
Link Status	Link Status: Connected; Disconnect
Rate(bps) (R/T)	Rate(bps): Received/Transmit;
Rate(pps) (R/T)	Rate(pps): Received/Transmit;
Unicast packets(R/T)	Unicast packets: Received/Transmit;
multicast packets(R/T)	multicast packets: Received/Transmit;
brocast packets(R/T)	brocast packets: Received/Transmit;
Input errors	Input erros
output errors	Output erros
CRC(R)	CRC(Cyclic Redundancy Check) Received;
frame alignment (R)	Frame Alignment Received;
overrun (R)	Overrun Received;
ignored (R)	Ignored Received;
abort (R)	Abort Received;
length error (R)	Length error Received;

undersize (R)	Undersize Received;
jabber (R)	Jabber Received;
fragments (R)	Fragments Received;
collisions (T)	Collisions Transmit;
late collisions (T)	Late Collisions Transmit;
pause frame (R/T)	Pause Frame Received/Transmit;
Refresh	Refresh Port Statistics
Delete	Select the port and click delete to clear Port Statistics

2.4.DDMI Status

This page displays fiber module information.

Reboot Reset Save Logout

System Config
Monitor Management
SSH Config
Telnet Config
Port Statistics
DDMI Status
Ping
Traceroute
Cable Diagnostics
SNMP Config
RMON Config

Collapse

Port	Vendor Name	Module Type	TX Power (dBm)	Send power reference value(dBm)	RX Power (dBm)	Received power reference value(dBm)	Temperature (°C)	Temperature reference value(°C)	Voltage (V)	Voltage reference value(V)	Bias (mA)	Current reference value(mA)
Ethernet1/0/5	LevelOne	SFP-3211	-6.40	Alarm(-10.50~0.00) Warn(-9.00~-1.50)	-40.00(A-)	Alarm(-26.02~0.00) Warn(-24.09~-3.00)	37	Alarm(-10~80) Warn(-6~-75)	3.28	Alarm(2.70~3.80) Warn(2.80~3.70)	21.75	Alarm(1.00~100.00) Warn(6.00~80.00)
Ethernet1/0/6	LevelOne	SFP-3001	-5.46	Alarm(-12.00~0.10) Warn(-10.00~-1.00)	-40.00(A-)	Alarm(-23.98~0.10) Warn(-23.01~-2.00)	29	Alarm(-45~90) Warn(-40~85)	3.31	Alarm(2.80~3.80) Warn(2.97~3.60)	4.35	Alarm(1.00~30.00) Warn(2.00~25.00)
Ethernet1/0/7	LevelOne	SFP-2503	-2.71	Alarm(-7.00~2.00) Warn(-6.00~1.00)	-40.00(A-)	Alarm(-26.99~0.10) Warn(-24.95~-2.00)	35	Alarm(-45~90) Warn(-40~85)	3.27	Alarm(2.80~3.80) Warn(2.97~3.60)	21.15	Alarm(0.00~80.00) Warn(0.00~70.00)
Ethernet1/0/8	LevelOne	SFP-6601	-3.00	Alarm(-7.30~0.50) Warn(-6.30~0.00)	-40.00(A-)	Alarm(-11.90~0.50) Warn(-10.90~0.00)	33	Alarm(-10~80) Warn(-6~-75)	3.26	Alarm(2.90~3.60) Warn(3.00~3.50)	6.00	Alarm(1.00~15.00) Warn(2.00~13.00)

Refresh

Port	fiber ports
Temperature (°C)	Display the temperature of the fiber module
Bias (mA)	Display the Bias of the fiber module.
RX Power (dBm)	Display the RX Power of the fiber module.
TX Power (dBm)	Display the TX Power of the fiber module.

2.5.Ping

The user can run ping command.

Ping

Server address

Apply

Ping Result

2.6.Traceroute

The user can run route tracking command.

Traceroute

Server address

Apply

Traceroute Result

2.7.Cable Diagnostics

This chapter can be used to detect port link lines.

To display the “Cable Diagnostics” page, click Monitor

Management

->Cable Diagnostics, click "Apply" to configure.

Cable Diagnostics				
<input type="checkbox"/>	Port	Test Result	Description	Cable Length(meters)
<input type="checkbox"/>	Ethernet1/0/1	-	-	-
<input type="checkbox"/>	Ethernet1/0/2	-	-	-
<input type="checkbox"/>	Ethernet1/0/3	-	-	-
<input type="checkbox"/>	Ethernet1/0/4	-	-	-
<input type="checkbox"/>	Ethernet1/0/5	-	-	-
<input type="checkbox"/>	Ethernet1/0/6	-	-	-
<input type="checkbox"/>	Ethernet1/0/7	-	-	-
<input type="checkbox"/>	Ethernet1/0/8	-	-	-
<input type="checkbox"/>	Ethernet1/0/9	-	-	-
<input type="checkbox"/>	Ethernet1/0/10	-	-	-
<input type="checkbox"/>	Ethernet1/0/11	-	-	-
<input type="checkbox"/>	Ethernet1/0/12	-	-	-
<input type="checkbox"/>	Ethernet1/0/13	-	-	-
<input type="checkbox"/>	Ethernet1/0/14	-	-	-
<input type="checkbox"/>	Ethernet1/0/15	-	-	-
<input type="checkbox"/>	Ethernet1/0/16	-	-	-
<input type="checkbox"/>	Ethernet1/0/17	-	-	-
<input type="checkbox"/>	Ethernet1/0/18	-	-	-
<input type="checkbox"/>	Ethernet1/0/19	-	-	-
<input type="checkbox"/>	Ethernet1/0/20	-	-	-
<input type="checkbox"/>	Ethernet1/0/21	-	-	-
<input type="checkbox"/>	Ethernet1/0/22	-	-	-
<input type="checkbox"/>	Ethernet1/0/23	-	-	-
<input type="checkbox"/>	Ethernet1/0/24	-	-	-

Start

Cable Diagnostics				
<input type="checkbox"/>	Port	Test Result	Description	Cable Length(meters)
<input type="checkbox"/>	Ethernet1/0/1	Disconnect	Please check whether the network cable is connectedAbnormal	(1, 2) 1 (3, 6) 1 (4, 5) 2 (7, 8) 1
<input type="checkbox"/>	Ethernet1/0/2	Normal	Normal(Correctly terminated pair)	(1, 2) 1 (3, 6) 1 (4, 5) 1 (7, 8) 1
<input type="checkbox"/>	Ethernet1/0/3	Disconnect	Please check whether the network cable is connected(Open pair:no link partner)	(1, 2) 2 (3, 6) 2 (4, 5) 1 (7, 8) 2
<input type="checkbox"/>	Ethernet1/0/4	Disconnect	Please check whether the network cable is connected(Open pair:no link partner)	(1, 2) 2 (3, 6) 2 (4, 5) 2 (7, 8) 1
<input type="checkbox"/>	Ethernet1/0/5	Disconnect	Please check whether the network cable is connected(Open pair:no link partner)	(1, 2) 2 (3, 6) 2 (4, 5) 2 (7, 8) 1
<input type="checkbox"/>	Ethernet1/0/6	Disconnect	Please check whether the network cable is connected(Open pair:no link partner)	(1, 2) 2 (3, 6) 2 (4, 5) 2 (7, 8) 1
<input type="checkbox"/>	Ethernet1/0/7	Disconnect	Please check whether the network cable is connected(Open pair:no link partner)	(1, 2) 1 (3, 6) 1 (4, 5) 2 (7, 8) 2
<input type="checkbox"/>	Ethernet1/0/8	Disconnect	Please check whether the network cable is connected(Open pair:no link partner)	(1, 2) 2 (3, 6) 1 (4, 5) 2 (7, 8) 2

2.8.SNMP Config

2.8.1.Global Config

SNMP network management function switch module, users can enable or disable SNMP functions. SNMP Agent State and Trap state default is disable.

Security IP state

SNMP Management	
Agent State	Disabled ▼
RMON	Disabled ▼
Trap	Disabled ▼
Security IP	Disabled ▼

Save

2.8.2.User Config

SNMP user management module, users can add or delete SNMP user operations in this module.

Users

Username	<input type="text"/>	(1-32 characters)
Group Name	<input type="text"/>	(1-32 characters)
Security Level	noAuthNoPriv	
IPv4 Access Control List	<input type="text"/>	(1-64 characters)
IPv6 Access Control List	<input type="text"/>	(1-64 characters)

[Apply](#)

User Configuration Status Table

Showing 10	Entries	Showing 0 to 0 of 0 entries	Search
<input type="checkbox"/>	Username	Group Name	Security Level
	Authentication Protocol	Privacy Protocol	IPv4 Access Control List
	IPv6 Access Control List		
0 results found.			
Delete			
First Previous Next Last			

Username	User name to operate ,1-32 characters	
Group Name	User group to join ,1-32 characters	
Security Level	noAuthNoPriv	Uncertified non-encrypted level
	authNoPriv	Authentication but not encryption level
	authpriv	Authentication and encryption level
Authentication protocol:	MD5	HMAC MD5 algorithm for authentication
	SHA	Authentication uses HMAC SHA algorithms
Authentication password:	Password for authentication	
Privacy protocol:	DES	Encryption DES algorithm
	AES	Encryption AES algorithm
	3DES	Encryption with 3 DES algorithm
Privacy password:	Password for encryption	
IPv4 access control list	Standard IPv4 access control list number, range 1-64 characters	
IPv6 access control list	Standard IPv6 access control list number, range 1-64 characters	

2.8.3.Group Config

SNMP group management module in which users can add or delete SNMP group operations.

Groups

Group Name	<input type="text"/>	(1-32 characters)
Security Level	noAuthNoPriv	
Read SNMP View	<input type="text"/>	(1-32 characters)
Write SNMP View	<input type="text"/>	(1-32 characters)
Notify SNMP View	<input type="text"/>	(1-32 characters)

[Apply](#)

Snmp Group Table

Showing 10	Entries	Showing 0 to 0 of 0 entries	Search
<input type="checkbox"/>	Group Name	Security Level	SNMP View
	SNMP View	SNMP View	SNMP View
0 results found.			
Delete			
First Previous Next Last			

Group Name	User group name to operate ,1-32 characters	
Security level	noAuthNoPriv	Uncertified non-encrypted level
	authNoPriv	Authentication but not encryption level
	authpriv	Authentication and encryption level
Read SNMP view	Name of readable view, including 1-32 characters	
Write SNMP view	Name of writable view, including 1-32 characters	
Notify SNMP view	Notice the name of the view, including 1-32 characters	
Operation	Apply	Add SNMP groups
	Delete	Delete SNMP groups

2.8.4.Community Config

The community management module where users can configure SNMP community management.

Community Managers

Community Name	<input type="text" value=""/>
Access Priority	Readonly (1-255 characters)

Community Managers Status Table

<input type="checkbox"/>	Community Name	Access Priority
--------------------------	----------------	-----------------

Community Name	Community string name ,1-255 characters	
Access Priority	Read only	Read-only permission level
	Read-write	Read and write permission level
Operation	Add	Do Community string add operations
	Delete	Do Community string delete operations

2.8.5.Trap Config

The trap config where users can configure trap management settings.

TRAP Manager Config

TRAP Receiver	<input type="text" value=""/>
Version	V1 Example:1.1.1.5
Community Name	<input type="text" value=""/>

TRAP Manager Status Table

<input type="checkbox"/>	TRAP Receiver	Community Config	Version	Security Level	User Config
--------------------------	---------------	------------------	---------	----------------	-------------

Trap Receiver	Recipient IPv4/IPv6 address of Trap information	
Community Name	Community string name, V1/V2 version :1-255 characters, V3 version :1-24 characters	
Version	Three versions:V1/V2C/V3	
Security level (V3 version support only)	noAuthNoPriv	Uncertified non-encrypted level
	authNoPriv	Authentication but not encryption level
	authpriv	Authentication and encryption level
Operation	Add	For Trap information receiver add operation
	Delete	For Trap information receiver remove operation

2.8.6.View Config

SNMP view management module in which users can add or delete SNMP view operations.

Views

SNMP View	<input type="text" value=""/>	(1-32 characters)
OID	<input type="text" value=""/>	Example:1.3.6.1.2.1.1.1
Type	Include ▼	

Apply

View Table

Showing 10 Entries

Showing 1 to 3 of 3 entries

Search

	SNMP View	OID	Type
<input type="checkbox"/>	v1defaultviewname	1.0.	Include
<input type="checkbox"/>	v1defaultviewname	1.2.	Include
<input type="checkbox"/>	v1defaultviewname	1.3.	Include

Delete

First
Previous
1
Next
Last

SNMP view	User view name to operate, 1-32 characters	
OID	OID number to operate, decimal	
Type:	Include	Include this OID
	Exclude	Exclude this OID
Operation	Apply	Add view
	Delete	Delete View

SNMP Engineid configuration module, the user can configure SNMP Engineid operation in this module.

SNMP engineid configuration

Engineid	<input type="text" value="18c384E5D8E01F5F"/>	Example:18c30125fa
Operation Type	Configuration ▼	

Apply

Engineid	Engine id, Hex ,1-32 characters	
Operation	configuration	Configuration operations
	Default	Restore default (default is company ID plus local MAC address)

2.8.7.Security IP Config

The administrator IP the address setting module, where the user can add or delete the SNMP manager's safe IP address.

Manager Security IP Configuration

Security IP Address

Apply

☐

Security IP Address

Delete

Security IP address	SNMP Management Security IPv4/IPv6 Address	
Operation	Apply	Add a Security IP
	Delete	Delete a Security IP

2.8.8.SNMP Statistics

SNMP statistical information module, users in this module can view the SNMP function feedback information.

SNMP Statistics

SNMP packets input	0
Bad SNMP version errors	0
Unknown community name	0
Illegal operation for community name supplied	0
Encoding errors	0
Number of requested variables	0
Number of altered variables	0
Get-request PDUs	0
Get-next PDUs	0
Set-request PDUs	0
SNMP packets output	0
Too big errors (Max packet size 1500)	0
No such name errors	0
Bad values errors	0
General errors	0
Get-response PDUs	0
SNMP trap PDUs	0

Refresh

2.9.Onvif Config

2.9.1.Server Config

Onvif server global switch configuration module, user can Onvif server global switch operation.

Server Config

Server Config

☐

Server config Operation	Off: Close operation(default)
	On: Start

2.9.2.Detect Config

Onvif detect config module, Click the **Send** button to send an Onvif detection packet to discover the device.

Detect Config

	MAC Address	IP Address	Port	Model	Description	Location
<input type="checkbox"/>						

Send Package
Delete

Detect Config

	MAC Address	IP Address	Port	Model	Description	Location
<input type="checkbox"/>						
<input type="checkbox"/>	48ea63:28:a0:63	192.168.19.72	18	IPC331S-IR3-PF40-DT	IPC331S-IR3-PF40-DT	Unknow
<input type="checkbox"/>	48ea63:60:69:83	192.168.19.8	18	NVR304-32E-B-DT	NVR304-32E-B-DT	country

Send Package
Delete

2.10.Loopback Detection

2.10.1.Port Mode

The configuration of the page is used to set the loop detection control method. To display the "Port Mode" page, click Monitor Management ->Loopback Detection->Port Mode, click "Apply" to configure.

Port Mode

	Port	<div>--Please select --</div>
	Loopback-detection Mode	<div>No ▼</div>

Apply

Port	Ethernet port name
Loopback-detection mode	Operation in case of loop: No: no control mode Shutdown: Disable port block : Block port
Operation	Operation of loop detection function: Apply: Configure control mode

Port	Loopback-detection Mode
Ethernet1/0/1	No
Ethernet1/0/2	No
Ethernet1/0/3	No
Ethernet1/0/4	No
Ethernet1/0/5	No
Ethernet1/0/6	No
Ethernet1/0/7	No
Ethernet1/0/8	No
Ethernet1/0/9	No
Ethernet1/0/10	No
Ethernet1/0/11	No
Ethernet1/0/12	No

Port	Ethernet port name
Loopback-detection mode	Shutdown: Disable port block : Block port No:Disable port loop detection

2.10.2.VLAN Loopback

This page can be used to configure VLAN loop detection function enabled or disabled.

To display the “VLAN Loopback” page, click Monitor Management ->Loopback Detection->VLAN Loopback, click "Apply" to configure.

VLAN Loopback

Port	--Please select --	
VLAN List	(1-4094, for example: 1;3-6)	

Apply

Port	VLAN List
Ethernet1/0/1	
Ethernet1/0/2	
Ethernet1/0/3	
Ethernet1/0/4	
Ethernet1/0/5	
Ethernet1/0/6	
Ethernet1/0/7	
Ethernet1/0/8	

Port	Ethernet port name
VLAN ID	VLAN ID, range 1-4094
Operation	Apply: Set VLAN loop detection

2.10.3.Interval Time

This page can be used to configure the loop detection interval.

To display the “Interval Time” page, click Monitor Management ->Loopback Detection-> Interval Time, click "Apply" to configure.

Interval Time

Loopback-detection Interval Time	5	(5-300s, Default:5s)
No Loopback-detection Interval Time	3	(1-30s, Default:3s)

Apply

Loopback-detection interval time	Interval time between loops, size 5-300 seconds, default is 5.
No Loopback-detection interval time	No loop interval, size 1-30 seconds, default is 3.
Operation	Configuration: Set the test time by yourself. Default: Restore the default configuration, there is a loop detection interval of 35 seconds, there is no loop detection interval of 15 seconds.

2.10.4.Recovery Timeout

This page is used to configure loop detection to automatically return to an uncontrolled state.

To display the "Recovery Timeout" page, click Monitor Management -> Loopback Detection-> Recovery Timeout, click "Apply" to configure.

Recovery Timeout

Recovery Switch Timeout	600	(0-3600s, Default:600s)
<div style="background-color: #28a745; color: white; padding: 5px 15px; display: inline-block; cursor: pointer;">Apply</div>		

Recovery switch timeout	<p>When a port is disabled or blocked due to a loop, it automatically recovers to an uncontrolled time, the size range is 0-3600 seconds. When it is configured as 0, the auto recovery function is disabled. Default is 600</p>
--------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

2.11.LLDP Config

2.11.1.Global Config

This page can be configured to enable or disable LLDP functionality, configure the interval between sending updates, configure the value of the message aging time multiplier, configure the sending delay time of the update message, configure the interval between sending Trap messages.

Global Config

This page is used to configure global properties of the LLDP function

Status	Disabled	
Hello Message Sending Time	30	(5-32768),Default:30
Aging Multiple	4	(2-10),Default:4
Delay Time ?	2	(1-8192),Default:2
Trap Interval ?	5	(5-3600),Default:5
Operation Type	Apply	

Apply

Status(lldp enable)	<p>Enable: Global On LLDP Function Disable: Global Off LLDP Function</p>
----------------------------	------------------------------------------------------------------------------

Hello Message Sending Time	Update message sending interval between 5-32768 seconds. the default configuration is 30 seconds.
Aging Multiple	Numerical magnitude between 2-10, the default configuration is 4
Delay Time	Value between 1-8192 seconds, the default configuration is 2
Trap Interval	Value between 5 and 3600

	seconds, the default configuration is 5
Operation Type	Apply: User self-configuration Default: Restore default configuration

2.11.2.Port Config

This page can be configured to enable or disable LLDP Port functionality.

Trust Config

This page is used to set port attributes for the LLDP function

Port	--Please select--	
LLDP Enable	Enabled ▼	
Trap Enable	Disabled ▼	
Agent State	both ▼	
Operation Type ?	Discard ▼	
Entry Max ?	100	(5-500,Default:100)

Apply

Port	Ethernet port name
LLDP port Enable type	Enable or disable LLDP functions
LLDP port Trap enable type	Enable or disable Trap functions
LLDP mode	Agent State: Send; Receive; Both; Disable;
LLDP too many neighbors value	Discard: Discard new neighbor information Delete: Delete the neighbor information with the least aging time in the remote table, and then add new neighbor information
LLDP neighbors max-num value	Remote table maximum save entry size 5-500

Port	LLDP Enable	Trap Enable	Agent State	Operation Type	Entry Max
Ethernet1/0/1	Enabled	Enabled	Both	Discard	100
Ethernet1/0/2	Enabled	Disabled	Both	Discard	100
Ethernet1/0/3	Enabled	Disabled	Both	Discard	100
Ethernet1/0/4	Enabled	Disabled	Both	Discard	100
Ethernet1/0/5	Enabled	Disabled	Both	Discard	100
Ethernet1/0/6	Enabled	Disabled	Both	Discard	100
Ethernet1/0/7	Enabled	Disabled	Both	Discard	100
Ethernet1/0/8	Enabled	Disabled	Both	Discard	100
Ethernet1/0/9	Enabled	Disabled	Both	Discard	100
Ethernet1/0/10	Enabled	Disabled	Both	Discard	100
Ethernet1/0/11	Enabled	Disabled	Both	Discard	100
Ethernet1/0/12	Enabled	Disabled	Both	Discard	100
Ethernet1/0/13	Enabled	Disabled	Both	Discard	100
Ethernet1/0/14	Enabled	Disabled	Both	Discard	100
Ethernet1/0/15	Enabled	Disabled	Both	Discard	100
Ethernet1/0/16	Enabled	Disabled	Both	Discard	100
Ethernet1/0/17	Enabled	Disabled	Both	Discard	100
Ethernet1/0/18	Enabled	Disabled	Both	Discard	100

2.11.3.TLV Config

This page can configure port TLV properties.

TLV Config

This page is used to set the properties of TLV

Port	--Please select --
TLV Config	--Please select --

Apply

Port	TLV Config
Ethernet1/0/1	
Ethernet1/0/2	
Ethernet1/0/3	
Ethernet1/0/4	
Ethernet1/0/5	
Ethernet1/0/6	
Ethernet1/0/7	
Ethernet1/0/8	

Port	Ethernet port name
LLDP Port Description	Port description name information needs to be configured
LLDP System Capability	Information describing system capabilities
LLDP System Description	Message describing the system
LLDP System Name	System name information

2.11.4.Neighbor Info

This page can be used to view LLDP configuration messages.

Neighbor Info

This page is used to view information about other neighbors

Neighbor Table

Showing 10 ▾ Entries

Showing 1 to 1 of 1 entries

Search

Number	Local Port	Chassis ID	CID	Port ID	PID	Time Mark	System Name
1	Ethernet1/0/8	30-b4-9e-bc-b7-44	4	30-b4-9e-bc-b7-44	MAC address	3373	-

FirstPrevious1NextLast

3.Switch Config

3.1.Port Config

3.1.1.Port Config

This page is mainly used to configure the basic of physical ports.

To display the “Port Config” page, click Switch Config->Port Config->Port Config, click "Apply" to configure.

Port Config

This page is used to configure basic port parameters.

Ports	Ethernet1/0/1	
Port Alias		(1-200 character) ?
Admin Status	Enabled	
Speed	Auto	
Duplex	Auto	
Flow Control	Disabled	?
MDI	auto	?

Apply

Ports	Select physical ports
Port Alias	Set port alias name, value 1-200
Admin status	Port status: Enabled Disabled
Speed	Port Speed: Auto,10M,100M,1000M
Duplex	Port Duplex: Auto, Half, Full
Flow Control	Port Flow Control: Disabled, Enabled
Mdi	Mdi: auto, across, normal, default is auto.

Port	Port Alias	Admin Status	Speed/Duplex		Flow Control	MDI
			Config	Actual		
Ethernet1/0/1		Enabled	Auto/Auto	Link Down	Disabled	auto
Ethernet1/0/2		Enabled	Auto/Auto	Link Down	Disabled	auto
Ethernet1/0/3		Enabled	Auto/Auto	1000M/Full	Disabled	auto
Ethernet1/0/4		Enabled	Auto/Auto	Link Down	Disabled	auto
Ethernet1/0/5		Enabled	Auto/Auto	Link Down	Disabled	auto
Ethernet1/0/6		Enabled	Auto/Auto	Link Down	Disabled	auto
Ethernet1/0/7		Enabled	Auto/Auto	Link Down	Disabled	auto
Ethernet1/0/8		Enabled	Auto/Auto	1000M/Full	Disabled	auto
Ethernet1/0/9		Enabled	Auto/Auto	Link Down	Disabled	auto
Ethernet1/0/10		Enabled	Auto/Auto	Link Down	Disabled	auto
Ethernet1/0/11		Enabled	Auto/Auto	Link Down	Disabled	auto
Ethernet1/0/12		Enabled	Auto/Auto	Link Down	Disabled	auto
Ethernet1/0/13		Enabled	Auto/Auto	Link Down	Disabled	auto
Ethernet1/0/14		Enabled	Auto/Auto	Link Down	Disabled	auto
Ethernet1/0/15		Enabled	Auto/Auto	Link Down	Disabled	auto
Ethernet1/0/16		Enabled	Auto/Auto	Link Down	Disabled	auto

Port	physical ports
Port Alias	Port alias description
Admin status	Port status: Enabled Disabled
Speed	Port rate: 10: 10M 100: 100M 1000: 1000M Auto: Automatic negotiation rate
Duplex	Duplex: Auto: Automatic negotiation mode Half: Half duplex mode Full: Full duplex mode
Flow control	Port Flow Control Status:
Mdi	Mdi: auto, across, normal, default is auto.

3.1.2.Port Combo Mode(Specific)

This page is mainly used to configure the basic of combo ports.

Port Combo Mode

This page is used to configure port Combo mode.

Ports	Ethernet1/0/25 ▼
Port Combo Mode	copper ▼

Apply

Ports	Port Combo Mode
Ethernet1/0/25	sfp-preferred-auto
Ethernet1/0/26	sfp-preferred-auto

Port	Select physical ports
Port Combo Mode	copper: select copper fiber: select fiber sfp-preferred-auto: auto mode

3.1.3.Port 10G Mode(Specific)

This page is mainly used to configure the basic of 10G ports.

Port 10G Mode

This page is used to configure 10G port mode.

Ports	Ethernet1/0/25 ▼
Port 10G Mode	dac-50cm ▼

Apply

Ports	Port 10G Mode
Ethernet1/0/25	fiber-auto
Ethernet1/0/26	fiber-auto
Ethernet1/0/27	fiber-auto
Ethernet1/0/28	fiber-auto

Port	Select physical ports
Port 10G Mode	dac-50cm: DAC 50cm dac-100cm: DAC 100cm dac-300cm: DAC 300cm dac-500cm: DAC 500cm fiber-10g: Fiber forced 10G fiber-1g: Fiber forced 1G fiber-2500M: Fiber forced 2500M fiber-auto: Fiber Auto mode

3.2.Port Mirror

This section can be used for port mirroring function configuration.
 To display the "Port Mirror" page, click Switch Config ->Port Mirror, click "Apply" to configure.

Port Mirror

This page is used to configure port mirror.

Session ID	1					
Destination Port	Ethernet1/0/1					
Source Port		--Please select --				
CPU Source	Disabled					
Access List		(1-7999)				
Mirror Direction	rx					

Apply

Port Mirror Table

	Session ID	Destination Port	Source Port		Access List
			Tx	Rx	
<input type="checkbox"/>	1				
<input type="checkbox"/>	2				
<input type="checkbox"/>	3				
<input type="checkbox"/>	4				

Delete

Session	Mirror Session
Destination port	Mirror destination port
Source port	Mirror Source Port
CPU Source	CPU Source: Disabled Enabled
Access list	The access control list set for the mirror source port
Mirror direction	What kind of data is needed to filter to the destination port: Both: Sending and receiving Rx: receive Tx: send

3.3.Port Isolate

This page is mainly used to configure the port isolation.

Port Isolation Configuration

This page is used to configure port isolate.

Isolate-Port Group Name	<input style="width: 90%;" type="text"/> (1-32 character)
Isolation Ports	<input style="width: 90%;" type="text"/> --Please select --

Add

Port Isolation Table

<input type="checkbox"/>	Isolate-Port Group Name	Isolation Ports
--------------------------	-------------------------	-----------------

Delete

Isolate-Port Group Name	The name of isolate-port Group,value 1-32 character
Isolation Ports	Select isolation ports to add isolate group

3.4.Port Channel

3.4.1.Port Channel Group

This section can be used to create convergent groups.

To display the “Port Channel Group” page, click Port channel -> Port Channel Group, click "Apply" to configure.

Port Channel

This page is used to configure port channel.

Load Balance Alogorithm	<div style="border: 1px solid #ccc; padding: 2px;">src-mac</div>
-------------------------	------------------------------------------------------------------

Apply

Load balance mode	<p>src-mac: Execute load balancing according to source MAC</p> <p>dst-mac: Execute load balancing according to target MAC</p> <p>src-dst-mac: Execute load balancing based on source and target MAC</p> <p>src-ip: Execute load balancing according to source IP</p> <p>dst-ip: Execute load balancing according to target IP</p> <p>dst-src-ip: Execute load balancing according to target IP source</p> <p>dst-src-mac-ip: Perform load balancing based on target and source Mac and source IP</p> <p>ingress-port : ingress port.</p>
--------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

LAG	<input type="text" value="(1-64)"/>
Name	<input type="text" value="(1-200 character)"/>
Mode	on
State	Enabled
Member Port	--Please select --

Apply

<input type="checkbox"/>	LAG	Name	Mode	State	Ports	Load Balance Alogorithm
Delete						

LAG	To create a convergent group number, value 1-8.
Name	The name of LAG group, value 1-32 character
mode	On: force port to join port channel without LACP. enabled Active: Enable the LACP on the port and set it to Active mode; Passive: Enable LACP on the port and set it to passive mode
State	Enabled Disabled
Member Port	Ethernet port name

3.4.2.LACP

This page is available with setting system priority and port priority.
To display the “LACP” page, click Switch Config -> Port channel->LACP,

LACP

This page is used to configure port channel LACP

System Priority	<input type="text" value="32768"/>	(0-65535, default 32768)
-----------------	------------------------------------	--------------------------

Apply

Port	--Please select --	
Port Priority	<input type="text" value="(0-65535, default 32768)"/>	
Timeout	long	

Apply

<input type="checkbox"/>	Port	Status	Port Priority	FLAG ?
Delete				

LACP system priority	Range :0-65535
Port list	Ethernet port name added to convergence group
LACP port priority	Range :0-65535
Timeout	long short

3.5.Jumbo Frame

This page is used to configure Jumbo Frame.

Jumbo Frame Configuration

This page is used to configure Jumbo Frame!

Status	Disabled	
Jumbo Frame Size	1500	1500-12270 (Unit: Bytes)

Apply

Status	Disabled(default) Enabled
Jumbo Frame Size(Unit: Bytes)	Size 1500-12270,default is 1500.

3.6.Port Rate

The page is configured for Port Rate.

To display the “Port Rate” page, click Switch Config -> Port Rate, click "Apply" to configure.

Port Rate

This page is used to configure port rate.

Ports	--Please select --	
Limit Type	Ingress	
Status	Disabled	
Rate(Kbps)	No Limit	1-10000000

Apply

Ports	Ethernet port name
Limit Type	Limit type: Egress: send Ingress : receive All: send and receive
Status	Disabled Enabled
Rate	Bandwidth control rate in the range of Kbps 1-1000000

Port	EgressRate(Kbps)	IngressRate(Kbps)
Ethernet1/0/1	1000000	1000000
Ethernet1/0/2	1000000	1000000
Ethernet1/0/3	1000000	1000000
Ethernet1/0/4	1000000	1000000
Ethernet1/0/5	1000000	1000000
Ethernet1/0/6	1000000	1000000
Ethernet1/0/7	1000000	1000000
Ethernet1/0/8	1000000	1000000

Port	Ethernet port name
Ingress bandwidth threshold(Kb)	Displays the current received data bandwidth limit in the range of Kbps 1-1000000
Engress bandwidth threshold(Kb)	Displays the bandwidth limit of the current sending data, ranging from 1-1000000kbps

3.7.Storm Control

This page can be configured for the storm control function of the port.
To display the “Storm Control” page, click Switch Config -> Storm Control, click "Apply" to configure.

Storm Control

This page is used to configure storm control.

Ports	--Please select --		
Type	Broadcast		
Status	Disabled		
Rate(Kbits)	No Limit	1-1000000	

Apply

Port	Ethernet port name
Type	Broadcast/Multicast/Unicast
Status	Disabled: Disable Storm Control Enabled: Turn on the storm control function and configure the speed limit
Rate	storm control rate, ranging from 1-1000000 kbps or pps 1-1488095

Port	Broadcast	Unknown Multicast	Unknown Unicast
Ethernet1/0/1	Disabled	Disabled	Disabled
Ethernet1/0/2	Disabled	Disabled	Disabled
Ethernet1/0/3	Disabled	Disabled	Disabled
Ethernet1/0/4	Disabled	Disabled	Disabled
Ethernet1/0/5	Disabled	Disabled	Disabled
Ethernet1/0/6	Disabled	Disabled	Disabled
Ethernet1/0/7	Disabled	Disabled	Disabled
Ethernet1/0/8	Disabled	Disabled	Disabled

Port	Ethernet port name
storm-control type	Broadcast/Multicast/Unicast

3.8.MAC Address Config

3.8.1.Static MAC

Configure Static MAC addresses, and establish the mapping relationship between MAC addresses and ports and VLANs.

MAC Address Config

MAC Address	00-00-00-00-00-00
VLAN ID	VLAN0001
Port	Ethernet1/0/1

[Add](#)

Static MAC List

Showing 10 Entries

Showing 0 to 0 of 0 entries

Search

No.	MAC Address	VLAN ID	Port
0 results found.			

[Delete](#)

[First](#)
[Previous](#)
[Next](#)
[Last](#)

MAC address	Hexadecimal MAC address, the format is xx-xx-xx-xx-xx-xx	
VLAN ID	Created VLAN ID	
Port	Mapped port	
Operation	Add	The mapping relationship between MAC address and port and VLAN will be added
	Remove	Delete the mapping relationship of the specified MAC address, VLAN, and port

3.8.2.Black Hole MAC

Configure Blackhole MAC addresses, and establish the mapping relationship between MAC addresses and ports and VLANs.

Black Hole MAC

VLAN ID	00-00-00-00-00-00
VLAN ID	VLAN0001
Type	both

[Add](#)

Black Hole MAC List

Showing 10 Entries

Showing 0 to 0 of 0 entries

Search

No.	MAC Address	VLAN ID	Type
0 results found.			

[Delete](#)

[First](#)
[Previous](#)
[Next](#)
[Last](#)

MAC address	Hexadecimal MAC address, the format is xx-xx-xx-xx-xx-xx, packets with this address will be discarded and will not be forwarded to the network by the switch	
VLAN ID	Created VLAN ID	
Blackhole based type	source	Source based on source address filter
	destination	Target based on target address filter
	both	Both are based on source address and destination address filters, the default value is both
Operation	Add	The mapping relationship between MAC address and port and VLAN will be added
	Delete	Delete the mapping relationship of the specified MAC address, VLAN, and port

Black Hole MAC List				
Showing	10	Entries	Showing 1 to 1 of 1 entries	Search
No.	MAC Address	VLAN ID	Type	
1	00-00-11-22-00-00	VLAN0001	both	
Delete				
First Previous 1 Next Last				

Display current existing MAC address, port, VALN mapping relationship

3.8.3.Aging-time

Each time the switch learns a MAC address, it will store the address and set the aging time. When the time is over, the address will be removed from the switch.

Aging-time	
Aging-time	300 (10-1000000)Second, default is 300, 0:No Aging
Apply	

MAC address Aging-time	The aging time range is 10-1000000, 0 means no aging	
Operation	Apply	Set the aging time into the switch

3.8.4.MAC Address List

Quickly query the MAC address in the switch.

MAC Address List					
Showing	10	Entries	Showing 1 to 3 of 3 entries	Search	
VLAN ID	MAC Address	Type	Creator	Port	
1	00-00-11-22-00-00	STATIC	User	(blackhole) (both)	
1	30-B4-9E-BC-B7-44	DYNAMIC	Hardware	Ethernet1/0/12	
1	84-E5-D8-E0-1F-5E	STATIC	System	CPU	
First Previous 1 Next Last					

VLAN ID	The created VLAN ID, showing the address in the VLAN
MAC Address	Hexadecimal MAC address, the format is xx-xx-xx-xx-xx-xx
Type	MAC address type
Creator	MAC address creator
Port	Find the MAC address by port

Note: Check the small box at the back to make the condition take effect. By default, there is no condition. When there is no condition, all MAC address information will be displayed.

3.9.AM

AM module, the user can set up AM IP segment and MAC-IP segment on the specified port, allowing / rejecting messages from within the segment to be forwarded through the port.

Access Manage(AM)

Through the port binding feature of AM access management, network administrators can bind legitimate user IP (MAC-IP) addresses to specified ports. After the binding operation, only messages sent by users with specified IP (MAC-IP) addresses can be forwarded through this port, enhancing users' monitoring of network security.

Port	<div>--Please select --</div>		
Binding Type	IP <div>▼</div>		
IP Address	<div></div>		
Number ?	1 <div>▼</div>		

Add

AM Configuration Table

<input type="checkbox"/>	Port	Binding Type	MAC Address	IP Address	Number
Delete					

Port	Designated port number
Binding Type	Select IP or MAC-IP method
IP address	Beginning IP address, decimal point
Number	Number of consecutive addresses after starting IP address , 1-32
MAC address	Source MAC address

3.10.AAA

3.10.1.Radius

Radius Global Configuration module, users in this module can configure the global Radius function services.

Radius Global Configuration

The user priority for Radius authentication login is 1

Key Type	Plain Key <div>▼</div>		
Radius Global Key	<div></div>	1-64Characters	
System Recovery Time	5	Range:1-255(Min),Default:5	
Radius Retransmit Times	3	Range:0-100,Default:3	
Radius Server Timeout	3	Range:1-1000(Sec),Default:3	

Apply

Radius Global Information				
Key Type	Radius Global Key	System Recovery Time	Radius Retransmit Times	Radius Server Timeout
Plain Key		5	3	3

Key Type	Plain Key: 1-64 character
	Cipher Key: 1-64 character, input plaintext application to encrypt ciphertext.
Radius Global Key	Key string , 1-64 characters, select Use default and click Apply can set Radius Key default.

System Recovery Time	Radius service recovery time from downtime to accessibility, 1-255 minutes, default is 5.
Radius Retransmit Times	Radius authentication packet retransmission time, 1-100 seconds, default is 3.
Radius Server Timeout	The corresponding time of the radius server, 1-1000 seconds, default is 3.

Radius Authentication Configuration module, users in this module can configure the Radius authentication server.

Radius Authentication Server Configuration

Authentication Server IP	<input type="text"/>	IPv4 or IPv6 address
Authentication Server Port(optional)	<input type="text"/>	Range:0-65535
Key Type	<div>Plain Key</div>	
Radius Key(optional)	<input type="text"/>	1-64Characters
Access Mode	<div>None</div>	
Primary Authentication Server	<div>Non-primary authentication server</div>	

Apply

Showing

10

 Entries
Showing 0 to 0 of 0 entries
Search

<input type="checkbox"/>	NO.	Server IP Address	Port Number	Primary Server	Key Type	Radius Key	Access Mode
0 results found.							

Delete

First
Previous
Next
Last

Authentication Server IP	The address of IPv4 or IPv6 of the radius authentication server	
Authentication Server port	Port number of radius authentication server(optional),0-65535	
Key Type	Plain Key: 1-64 character	
	Cipher Key: 1-64 character, input plaintext application to encrypt ciphertext.	
Radius Key	Key string ,1-64 characters	
Access Mode	None: All services can use current RADIUS server by default	
	Telnet: RADIUS server only use telnet authentication	
	Dot1x: RADIUS server only use 802.1x authentication	
	Wireless: RADIUS server only use wireless authentication	
Primary Authentication Server	Primary authentication server	Specify radius server as primary authentication server
	Non-Primary authentication server	Specify radius server as non-primary authentication server

3.10.2.Radius Accounting

Radius authentication and accounting module, users in this module can configure the Radius billing server.

Radius Accounting Server Configuration

Accounting Server IP	<input type="text"/>	IPv4 or IPv6 address
Authentication Server Port(optional)	<input type="text"/>	Range:0-65535
Key Type	Plain Key ▼	
Radius Key(optional)	<input type="text"/>	1-64Characters
Primary Authentication Server	Non-primary authentication server ▼	

Apply

Showing 10 Entries

Showing 0 to 0 of 0 entries

Search

<input type="checkbox"/>	NO.	Server IP Address	port number	Key Type	Radius Key	Primary Server
0 results found.						

Delete

First
Previous
Next
Last

Accounting Server IP	Radius authentication server IPv4 or IPv6 address	
Accounting Server Port	Radius authentication server port number (optional),0-65535	
Key Type	Plain Key: 1-64 character	
	Cipher Key: 1-64 character, input plaintext application to encrypt ciphertext.	
Radius Key	Key string ,1-64 characters	
Primary Accounting Server	Primary accounting server	Specify radius server as primary accounting server
	Non-Primary accounting server	Specify radius server as non-primary accounting server

3.10.3.Tacacs

Tacacs global configuration module, users in this module can configure the global Tacacs function services.

Tacacs Global Configuration

The user priority for Tacacs authentication login is 1

Key Type	Plain Key ▼	
Tacacs Global Key	<input type="text"/>	1-64 Characters
Tacacs Server Global Timeout	<input type="text" value="3"/>	Range:1-60(Sec),Default:3

Apply

Tacacs Global Information		
Key Type	Tacacs Global Key	Tacacs Server Global Timeout
Plain Key		3

Key Type	Plain Key: 1-64 character
	Cipher Key: 1-64 character, input plaintext application to encrypt ciphertext.
Tacacs Global Key	Tacacs authentication global key ,1-64 characters
Tacacs Server Global Timeout	Tacacs authentication timeout ,1-60 seconds, default 3 seconds

Tacacs server configuration module, users in this module can configure the Tacacs authentication server.

Tacacs Authentication Server Configuration

Authentication Server IP	<input type="text"/>	IPv4 or IPv6 address
Authentication Server Port(optional)	<input type="text"/>	Range:0-65535
Key Type	Plain Key	
Tacacs Key(optional)	<input type="text"/>	1-64Characters
Tacacs Server Timeout(optional)	<input type="text"/>	Range:1-60(Sec),Default:3
Primary Authentication Server	Non-primary authentication server	

[Apply](#)

Showing 10 Entries

Showing 0 to 0 of 0 entries

Search

NO.	Server IP Address	port number	Primary Server	Key Type	Tacacs Key	Tacacs Server Timeout
0 results found.						

[Delete](#)

[First](#)
[Previous](#)
[Next](#)
[Last](#)

Authentication Server IP	Tacacs authentication server IPv4 address, decimal point	
Authentication Server Port	Tacacs authentication server port number (optional),0-65535	
Key Type	Plain Key: 1-64 character	
	Cipher Key: 1-64 character, input plaintext application to encrypt ciphertext.	
Tacacs Key	Configure tacacs+ server encryption key 1-64 Characters	
Tacacs Server Timeout	Configure the tacacs+ server authentication time Interval <1-60> second Deafult is 3.	
Primary Authentication Server	Primary accounting server	Specify Tacacs server as primary accounting server
	Non-Primary accounting server	Specify Tacacs server as non-primary accounting server

4.VLAN Config

4.1.VLAN Config

4.1.1.VLAN ID

VLAN configuration function module, users add or delete VLANs in this module。

VLAN Configuration Management

VLAN ID

(1-4094, for example: 1;3-6)

VLAN Name

Add

Showing 10 Entries

Showing 1 to 1 of 1 entries

Search

No.	VLAN ID	VLAN Name
1	1	default

Delete

First Previous 1 Next Last

VLAN ID	The serial number of the VLAN, range: 2-4094	
VLAN name	By default, the default is VLAN plus four-digit serial number, range: 1-64 characters.	
Operation	Add	Add VLAN
	Delete	Remove VLAN

4.1.2.Show VLAN

Show VLAN function module, display VLANs in this module。

Show VLAN List

Showing 10 Entries

Showing 1 to 1 of 1 entries

Search

VLAN ID	Name	Type	Media	Ports
1	default	Static	ENET	Ethernet1/0/1, Ethernet1/0/2 Ethernet1/0/3, Ethernet1/0/4 Ethernet1/0/5, Ethernet1/0/6 Ethernet1/0/7, Ethernet1/0/8 Ethernet1/0/9, Ethernet1/0/10 Ethernet1/0/11, Ethernet1/0/12 Ethernet1/0/13, Ethernet1/0/14 Ethernet1/0/15, Ethernet1/0/16 Ethernet1/0/17, Ethernet1/0/18 Ethernet1/0/19, Ethernet1/0/20 Ethernet1/0/21, Ethernet1/0/22 Ethernet1/0/23, Ethernet1/0/24 Ethernet1/0/25, Ethernet1/0/26 Ethernet1/0/27, Ethernet1/0/28

First Previous 1 Next Last

4.1.3.Port Config

Switch port type setting, the user can change the switch port type in this module.

Port Mode Configure

Ports	--Please select --	
Mode	Access	
Native Vlan	VLAN0001	
Ingress Check	Enabled	
Tagged VLAN	Range(1-4094)	Example 1-3;8
UnTagged VLAN	Range(1-4094)	Example 1-3;8

Apply

Port	Mode	Native Vlan	Ingress Check	Tag Vlan List	Untag Vlan List
Ethernet1/0/1	Access	VLAN00020	Enabled	-	-
Ethernet1/0/2	Trunk	VLAN0001	Enabled	1-4094	-
Ethernet1/0/3	Trunk	VLAN0001	Enabled	-	-
Ethernet1/0/4	Access	VLAN0001	Enabled	-	-
Ethernet1/0/5	Access	VLAN0001	Enabled	-	-
Ethernet1/0/6	Access	VLAN0001	Enabled	-	-
Ethernet1/0/7	Access	VLAN0001	Enabled	-	-
Ethernet1/0/8	Access	VLAN0001	Enabled	-	-

Port	Port name	
Mode	Access	
	Trunk	
	Hybrid	
Native Vlan	Port PVID	
Ingress Check	Enabled	When a data packet enters the switch, the VLAN ingress filter checks whether the ingress port of the data packet belongs to the given (forwarded) VLAN
	Disabled	When a data packet enters the switch, the VLAN ingress filter does not check whether the ingress port of the data packet belongs to the given (forwarded) VLAN
Tagged VLAN	Tag VLAN range 1-4094,example 1-3;8	
UnTagged VLAN	Untag VLAN range 1-4094,example 1-3;8	

4.2.GVRP Config

4.2.1.GVRP Config

The switch starts the global GVRP setting, and the user turns on or off the global GVRP.

GVRP Config

☒ Enabled
 ☐ Off

Enable/Disable global GVRP	Enable	Start the global GVRP module function
	Disable	Disable the global GVRP module function

The switch configures GARP parameters, and the user sets the value of various timers to manage GARP.

GVRP Config

Enabled	<input checked="" type="checkbox"/>	
Join Timer	200	Range:200-500 milli-second, default is 200
Leave Timer	600	Range:500-1200 milli-second, default is 600
Leaveall Timer	10000	Range:5000-60000 milli-second, default is 10000

[Apply](#)

Join timer	200-500ms	
Leave timer	500-1200ms	
Leaveall timer	500-60000ms	
Operation	Apply	Modify the value of the timer

4.2.2.GVRP Port

The switch port starts GVRP settings, and the user opens or closes the port GVRP.

Enable GVRP On Port

Enable the port will not be able to change the port mode

Ports	--Please select --	
Status	Enabled	

[Apply](#)

Port	GVRP Status
------	-------------

Port	Port name	
Enable/Disable GVRP	Enable	Start the port GVRP module function
	Disable	Disable the port GVRP module function

4.3.QINQ

4.3.1.Enable Dot1q Tunnel

Switch dot1q tunnel configuration, the user configures the port to enable the dot1q tunnel function.

Enable Dot1q Tunnel

Ports	--Please select --	
-------	--------------------	--

[Apply](#)

Showing 10 Entries Showing 0 to 0 of 0 entries Search

Port	Status
0 results found.	

[First](#) [Previous](#) [Next](#) [Last](#)

[Delete](#)

Port	Port name	
Operation	Apply	Enable dot1q tunnel
	Delete	Disable dot1q tunnel

4.3.2.Dot1q Tunnel TPID

Switch port dot1q tunnel tpid configuration, users configure port dot1q tunnel tpid parameters.

Configure Dot1q Tunnel TPID

only configure for QinQ disable port

Ports	--Please select --
Protocol	0x8100
Protocol ID	Range:1-65535

[Apply](#)

Port	Port name	
Protocol	0x8100	Set the outer TPID to 0x8100
	0x9100	Set the outer TPID to 0x9100
	0x9200	Set the outer TPID to 0x9200
	protocol ID	Set a custom TPID
Protocol ID	The value of the custom TPID	

Port	GVRP Status
Ethernet1/0/1	
Ethernet1/0/2	
Ethernet1/0/3	
Ethernet1/0/4	
Ethernet1/0/5	
Ethernet1/0/6	
Ethernet1/0/7	
Ethernet1/0/8	

4.4.Protocol VLAN

The switch protocol vlan settings, and the user can config the protocol vlan.

Protocol VLAN Configure

Mode	ethernetII
Ethernet Type	Range:1536-65535
VLAN Name	VLAN0001
Priority	Range:0-7

[Add](#)

Showing 10 Entries Showing 0 to 0 of 0 entries Search

No.	Protocol Type	VLAN Name	Priority
0 results found.			

[Delete](#) [First](#) [Previous](#) [Next](#) [Last](#)

Mode	ethernetII	Configure EthernetII Encapsulation
	snap	Configure LLC Encapsulation
	llc	Configure SNAP Encapsulation
Ethernet Type	Packet protocol type, Configure Packet protocol type number, 1536-65535	
VLAN Name	Configure the VLAN ID.	
Priority	Configure priority value, 0-7	
Operation	Add	Add the protocol vlan
	Delete	Delete the protocol vlan

4.5.Voice VLAN

4.5.1.VLAN Config

The voice vlan configure module, and the user can select vlan to enable voice vlan

Voice VLAN Configure

Voice VLAN None

Apply

Voice VLAN	Select vlan to enable voice vlan
-------------------	----------------------------------

The voice oui configure module, and the user can set voice oui

Voice VLAN Configure

Voice VLAN VLAN0255

Apply

Voice OUI Configure

MAC address	MAC Mask	Priority	Name
00-00-00-00-00-00	FF-FF-FF-FF-FF-FF	Range:0-7	Up to 15 characters

Add

Showing 10 Entries

Showing 0 to 0 of 0 entries

Search

No.	Name	MAC address	MAC Mask	Priority
0 results found.				

First Previous Next Last

Delete

MAC address	The voice equipment MAC address, shown in xx-xx-xx-xx-xx-xx format.
MAC Mask	The last eight digit of the mask code of the MAC address, the valid values are: 0xff, 0xfe, 0xfc, 0xf8, 0xf0, 0xe0, 0xc0, 0x80, 0x0
Priority	The priority of the voice traffic, the valid range is 0–7
Name	The voice-name is the name of the voice equipment, which is to facilitate the equipment management

4.5.2.Port Config

The voice vlan port config module, and the user can select port to enable voice vlan

Port Config

Ports --Please select --

Status Enabled

Apply

Port	Status
Ethernet1/0/1(A)	Enabled
Ethernet1/0/2(T)	Enabled
Ethernet1/0/3(T)	Enabled
Ethernet1/0/4(A)	Enabled
Ethernet1/0/5(A)	Enabled
Ethernet1/0/6(A)	Enabled
Ethernet1/0/7(A)	Enabled
Ethernet1/0/8(A)	Enabled

Port	Port name	
Status	Enable	Enable voice vlan
	Disable	Disable voice vlan

4.6.MAC VLAN

4.6.1.VLAN Config

The mac vlan configure module, and the user can select vlan to add mac vlan

VLAN Config

MAC VLAN

VLAN0001

Add

Showing 10 Entries

Showing 0 to 0 of 0 entries

Search

No.	MAC VLAN	VLAN Name
0 results found.		

Delete

First Previous Next Last

MAC VLAN	Select vlan to add mac vlan
-----------------	-----------------------------

4.6.2.VLAN Member

the user can set mac vlan

MAC VLAN Configure

MAC address

00-00-00-00-00-00

MAC Mask

FF-FF-FF-FF-FF-FF

VLAN ID

VLAN0255

Priority

Range:0-7

Add

Showing 10 Entries

Showing 0 to 0 of 0 entries

Search

No.	MAC address	MAC Mask	VLAN ID	Priority
0 results found.				

Delete

First Previous Next Last

MAC address	The MAC address which is shown in the form of XX-XX-XX-XX-XX-XX
MAC Mask	The MAC address mask which is shown in the form of XX-XX-XX-XX-XX-XX
VLAN ID	Vlan-id is the ID of the VLAN with a valid range of 1-4094
Priority	Priority-id is the level of priority and is used in the VLAN tag with a valid range of 0-7

4.6.3.Port Config

The mac vlan port config module, and the user can select port to enable mac vlan

Port Config

Ports

--Please select --

Status

Enabled

Apply

Port	Status
Ethernet1/0/1(A)	Enabled
Ethernet1/0/2(T)	Enabled
Ethernet1/0/3(T)	Enabled
Ethernet1/0/4(A)	Enabled
Ethernet1/0/5(A)	Enabled
Ethernet1/0/6(A)	Enabled
Ethernet1/0/7(A)	Enabled
Ethernet1/0/8(A)	Enabled

Port	Port name	
Status	Enable	Enable mac vlan
	Disable	Disable mac vlan

5.DHCP Config

5.1.DHCP Server

5.1.1.Global Config

DHCP status configuration and query, the user configures the DHCP server status in this module, and checks the DHCP server status

Global Config

DHCP Server

Off

Global Config

DHCP Server

On

DHCP server	Off	Close DHCP server
	On	Open DHCP server

5.1.2.Create Address Pool

DHCP server address pool name configuration, user settings add and delete the address pool name.

Create Address Pool

Create Address Pool

Address Pool Name

(1-32 character)

Add

DHCP Server Address Pool Table

Showing 10 Entries

Showing 0 to 0 of 0 entries

Search

Address Pool Name

0 results found.

Delete

First

Previous

Next

Last

DHCP Address pool name	The name of the created address pool	
Operation type	Add pool	Add the address pool of the DHCP server
	Delete	Delete the address pool of the DHCP server

DHCP Server Address Pool Table

Showing 10 Entries

Showing 1 to 1 of 1 entries

Search

Address Pool Name

1

Delete

First

Previous

1

Next

Last

Display the address pool of the current DHCP server

5.1.3.Dynamic Pool

Switch DHCP address pool configuration, the user configures the DHCP address pool parameters.

Dynamic Pool

Address Pool Name	1
Domain Name	
IP Address	
Netmask	
DHCP Client Node Type	Default
Lease Time	Not Configured

Apply

Dynamic Pool Config Table

Showing 10 Entries Showing 0 to 0 of 0 entries Search

<input type="checkbox"/>	Address Pool Name	Domain Name	IP Address/Netmask	DHCP Client Node Type	Lease Time
0 results found.					

Delete First Previous Next Last

DHCP pool name	The name of the created address pool	
DHCP pool domain name	The domain name of the currently selected address pool. After configuration, you need to tick the box at the back to apply the domain name to the switch during application.	
Address range	IP address	Network number of the address pool
	Network mask	Netmask of the address pool
DHCP client node type	b-node	Broadcast node
	p-node	For point-to-point nodes
	m-node	Used for hybrid nodes to perform point-to-point communication after broadcasting
	h-node	Hybrid nodes that broadcast after peer-to-peer communication
	Designate	Hexadecimal node type, from 0 to 255
Address lease timeout	Infinite	The lease period of the address is unlimited, and the number of days/hours/minutes below do not need to be filled in
	Specified	There is a time limit for the lease of the address. You can rent it according to the lease time filled in below, and it will be automatically recovered if the time is exceeded
Operation	add	Add the above four parameters with check boxes to the switch, the parameters without check boxes will not be operated
	Delete	Restore the four parameters with check boxes to the default configuration, and the parameters without check boxes will not be operated

Dynamic Pool Config Table					
Showing	10	Entries	Showing 1 to 1 of 1 entries		Search
<input type="checkbox"/>	Address Pool Name	Domain Name	IP Address/Netmask	DHCP Client Node Type	Lease Time
<input type="checkbox"/>	1	-	1.1.1.0/255.255.255.0	0	1D 0H:0M
<div> Delete </div> <div> First Previous 1 Next Last </div>					

Information display of the currently configured address pool

5.1.4.Manual Pool

Switch static address pool configuration, and manually bind client parameters.

Manual Pool	
Address Pool Name	2
IP Address	xxx.xxx.xxx.xxx
Netmask	xxx.xxx.xxx.xxx
Binding Type	Hardware Address
ARP Hardware Type	1(ethernet)
MAC Address	xx-xx-xx-xx-xx-xx
<div>Apply</div>	

Static Pool Config Table					
Showing	10	Entries	Showing 0 to 0 of 0 entries		Search
<input type="checkbox"/>	Address Pool Name	MAC Address	IP Address/Netmask	Binding Type	ARP Hardware Type
0 results found.					
<div> Delete </div> <div> First Previous Next Last </div>					

Address Pool Name	The name of the created address pool
IP address	IP address assigned by the DHCP server to the client
Netmask	The subnet mask assigned by the DHCP server to the client IP
Binding Type	Hardware Address Client identifier: The identifier of the client,
ARP Hardware Type	The protocol type used by the client is rfc\ethernet\ieee802. RFC ID: RFC protocol number, valid range is 1-255.
MAC address	MAC address,for example: 44-11-22-33-44-55 (MAC address)
Operation	Apply
	Delete

5.1.5.Default Gateway

The switch DHCP client default gateway configuration, the user configures the gateway parameters of the DHCP address pool.

Default Gateway

Address Pool Name	1	▼
Gateway0		
Gateway1		
Gateway2		
Gateway3		
Gateway4		
Gateway5		
Gateway6		
Gateway7		
Operation	Add ▼	

Apply

DHCP pool name	The name of the created address pool	
Gateway0-7	Gateway IP address in dotted decimal format. Gateway 0 has the highest priority. The smaller the number, the higher the priority. The gateway can be set to zero or more, but the setting must start with 0 and no vacancies can appear in the middle, otherwise the gateway will be ignore the following parameters, such as setting gateway 0-1 and gateway 7, only gateway 0-1 takes effect	
Operation	Add	Add the gateway effectively set above to the currently selected DHCP address pool
	Delete	Clear all gateways and restore to the default state

5.1.6.DNS Server

The switch DHCP client DNS server configuration, the user configures the DNS server parameters of the DHCP address pool.

DNS Server

Address Pool Name	1	▼
DNS Server0		
DNS Server1		
DNS Server2		
DNS Server3		
DNS Server4		
DNS Server5		
DNS Server6		
DNS Server7		
Operation	Add ▼	

Apply

DHCP pool name	The name of the created address pool	
DNS server 0-7	For the IP address in dotted decimal format, DNS server 0 has the highest priority. The smaller the number, the higher	

	the priority. The DNS server can be set to zero or more, but the setting must start from 0 and there can be no vacancies in the middle, otherwise the DNS server The following parameters will be ignored, such as setting DNS server 0-1 and DNS server 7, only DNS server 0-1 takes effect	
Operation	Add	Add the DNS server effectively set above to the currently selected DHCP address pool
	Delete	Clear all DNS servers and restore to the default state

5.1.7.Excluded Address

Excluding the dynamic allocation address configuration, the user configures the addresses that are not used for dynamic allocation

Excluded Address

Starting address	<input type="text"/>	
Ending address	<input type="text"/>	

[Apply](#)

Exclude Address Table

Showing 10 Entries

Showing 0 to 0 of 0 entries

Search

	Starting address	Ending address
<input type="checkbox"/>		

0 results found.

[Delete](#)

[First](#)
[Previous](#)
[Next](#)
[Last](#)

Starting address	Start address not used for dynamic allocation	
Ending address	End address not used for dynamic allocation	
Operation type	Apply	Add the address range that is not used and dynamically allocated to the switch
	Delete	Delete the address range that is not used and dynamically allocated from the switch

Exclude Address Table

Showing 10 Entries

Showing 1 to 1 of 1 entries

Search

	Starting address	Ending address
<input type="checkbox"/>	1.1.1.10	1.1.1.20

[Delete](#)

[First](#)
[Previous](#)
[1](#)
[Next](#)
[Last](#)

Display the address range currently not used for dynamic allocation

5.1.8.Packet Statistics

DHCP server data packet statistics, users can view DHCP data packets.

Packet Statistics						
Address Pools	Database Agents	Automatic Bindings	Manual Bindings	Conflict Bindings	Expired Bindings	Malformed Message
1	0	0	0	0	0	0

Message Received					
BOOT REQUEST	DHCP Discover	DHCP Request	DHCP Decline	DHCP Release	DHCP Inform
0	0	0	0	0	0

Message Send					
BOOT Reply	DHCP Offer	DHCP ACK	DHCP NAK	DHCP Relay	DHCP Forward
0	0	0	0	0	0

Clear Statistics

It can be viewed in real time by clicking "Clear Statistics"

5.1.9.Client List

The DHCP server's IP and MAC binding status, the user can view the binding entries and the relationship between the bound IP and MAC.

Client List			
IP Address	Hardware Address		Lease Expiration
Type			

IP address	Client's IP address		
Hardware address	The hardware address or MAC address of the client		
Lease expiration	Client IP expiration time		
Type	Manual	Manual binding	
	Dynamic	Dynamic allocation	

5.2.DHCP Snooping

5.2.1.Global Config

With the enabling and disabling of the DHCP Snooping module, users can view and operate the status of DHCP Snooping.

Global Config

DHCP Snooping Status ☐ Off

DHCP Snooping status	Off	Disable DHCP Snooping
	On	Enable DHCP Snooping

Global Config

DHCP Snooping Status	<input checked="" type="radio"/> On
Action Num	10 (1-200,default 10)
Limit Rate	100 pps(0-100,default 100)

Apply

Display the current DHCP Snooping status

DHCP Snooping defense action number configuration, if the number of alarm messages is greater than the set number, it will force the restoration of the earliest defense measures to send new defense measures. DHCP Snooping packet receiving rate limit sets the number of DHCP messages sent per second.

DHCP Snooping action Num	Set the maximum number of defense actions to avoid exhaustion of switch resources caused by attacks.	
Limit Rate(Packet per second)	Range: 0-100	
Operation	Apply	Configure the number of defense actions filled in above, default is 10, Configure the number of packets per second

Action Num

10

(1-200,default 10)

Display the current number of DHCP Snooping defense actions

Limit Rate

100

pps(0-100,default 100)

Display the number of packets per second configured for the current DHCP Snooping.

5.2.2.VLAN Config

With the enabling and disabling of the DHCP Snooping VLAN module, users can view and operate the status of DHCP Snooping VLAN.

VLAN Config

VLAN ID	--Please select --
VLAN Enable	Disabled

Apply

VLAN ID	Trust
VLAN0001	Disabled

Port	Port name	
VLAN Enable	Enable	Enable DHCP Snooping VLAN
	Disable	Disable DHCP Snooping VLAN

5.2.3.Static User Binding

When DHCP Snooping binding is enabled and disabled, users can view and operate the status of DHCP Snooping. When configuring this binding, users must ensure that the binding status is in the on state.

Static User Binding

Binding Status

Off

DHCP Snooping binding status	Off	Disable DHCP Snooping binding function
	On	Enable DHCP Snooping binding function

Static User Binding

Binding Status	On
MAC Address	<input type="text"/>
IP Address	<input type="text"/>
VLAN ID	VLAN0001
Port	Ethernet1/0/1

Apply

DHCP Snooping Binding Table

Showing 10 Entries

Showing 0 to 0 of 0 entries

Search

	MAC Address	IP Address	Port	VLAN ID	Type
0 results found.					

Delete

First
Previous
Next
Last

Shows whether the current DHCP Snooping binding status function is enabled. When DHCP Snooping binding is enabled and disabled, users can view and operate the status of DHCP Snooping. When configuring this binding, users must ensure that the binding status is in the on state.

MAC address	The MAC address of the statically bound user is the only index of the bound user	
User IP address	Statically bind the user's IP address	
User mask	Statically bind the user's subnet mask	
VLAN ID	Statically bind the VLAN ID of the user	
Port	Bind the user's access port statically, the port is associated with the VLAN ID, and the port is required to allow the VLAN to pass	
Operation	Apply	Add DHCP Snooping binding user relationship
	Delete	Delete DHCP Snooping binding user relationship

5.2.4.Helper-server Config

DHCP SNOOPING will send the monitored binding information to HELPER SERVER for storage. If the switch starts abnormally, you can recover the bound data from the HELPER SERVER

Helper-server Config

Helper-server Address	<input type="text"/>
Helper-server UDP Port	9119 (1-65535,default 9119)
Local IP Address	<input type="text"/>
Server Address Type	Primary

Apply

	Helper-server Address	Helper-server UDP Port	Local IP Address	Server Address Type
0 results found.				

Delete

Helper-server address	HELPER server address
Helper-server UDP port	DHCP SNOOPING and HELPER SERVER use UDP protocol for communication, the port range is 1-65535.
Local IP address	The effective management IP address of the switch

Second address	Two HELPER server addresses are allowed, DHCP SNOOPING will first try to connect to the PRIMARY server. Only when the PRIMARY server cannot be accessed, the switch HELPER server will connect to the SECONDARY server. Set the PRIMARY server before setting up the SECONDARY server.	
Operation	Apply	Add HELPER server address
	Delete	Delete the HELPER server address, you can leave it blank when deleting

<input type="checkbox"/>	Helper-server Address	Helper-server UDP Port	Local IP Address	Server Address Type
<input type="checkbox"/>	192.168.2.11	9119	192.168.2.113	Primary
<input type="button" value="Delete"/>				

Display the process and error messages or results generated during application execution

5.2.5.Port Binding

DHCP SNOOPING will notify the DOT1X module of the binding information captured by the user controlled by the DOT1X. DHCP Snooping port binding dot1x function needs to enable DHCP Snooping binding configuration first.

Port Binding

Port	--Please select --	
Dot1x	Disabled	
User	<div> <div>Disabled</div> <div>Enabled</div> </div>	

Port	Dot1x	User
Ethernet1/0/1	Disabled	Disabled
Ethernet1/0/2	Disabled	Disabled
Ethernet1/0/3	Disabled	Disabled
Ethernet1/0/4	Disabled	Disabled
Ethernet1/0/5	Disabled	Disabled
Ethernet1/0/6	Disabled	Disabled
Ethernet1/0/7	Disabled	Disabled
Ethernet1/0/8	Disabled	Disabled

Port	Port name	
DHCP Snooping binding dot1x status	Enable	Enable the dot1x status of DHCP Snooping port binding
	Disable	Disable the dot1x binding status of the DHCP Snooping port

Display the dot1x binding status of each DHCP Snooping port of the switch
When this function is enabled on the port, DHCP SNOOPING will treat the captured binding information as a trusted user who is allowed to access all resources. The DHCP Snooping port binding user status function needs to enable the DHCP Snooping binding configuration first.

Port Binding

Port	--Please select --	
Dot1x	Disabled	
User	Disabled	

Disabled
Enabled
Apply

Port	Dot1x	User
Ethernet1/0/1	Disabled	Disabled
Ethernet1/0/2	Disabled	Disabled
Ethernet1/0/3	Disabled	Disabled
Ethernet1/0/4	Disabled	Disabled
Ethernet1/0/5	Disabled	Disabled
Ethernet1/0/6	Disabled	Disabled
Ethernet1/0/7	Disabled	Disabled
Ethernet1/0/8	Disabled	Disabled

Port	Port name	
DHCP Snooping binding user status	Enable	Enable DHCP Snooping port binding user status
	Disable	Disable DHCP Snooping port binding user status

Display the status of users bound to each DHCP Snooping port of the switch

5.2.6.Trust Port

When a port changes from an untrusted port to a trusted port, the original defense action of the port will be automatically deleted; all security history records will be cleared.

Trust Port

Port	--Please select --	
Trust	Disabled	

Apply

Port	Trust
Ethernet1/0/1	Disabled
Ethernet1/0/2	Disabled
Ethernet1/0/3	Disabled
Ethernet1/0/4	Disabled
Ethernet1/0/5	Disabled
Ethernet1/0/6	Disabled
Ethernet1/0/7	Disabled
Ethernet1/0/8	Disabled

Port	Port name	
DHCP Snooping binding trust status	Enable	Enable DHCP Snooping port trust attribute status
	Disable	Disable the trust attribute status of the DHCP Snooping port

Display the trust attribute status of each DHCP Snooping port of the switch

5.3.DHCP Relay Config

5.3.1.DHCP Relay Config

The switch DHCP relay configuration, the user configures the port range, and the switch sends UDP broadcast messages to the port.

DHCP Relay Config

DHCP Broadcast Suppress ? ☐ Off

DHCP Relay Forwarding ? ☒ On

Interface VLAN0001

Helper-server Address xxxx.xxxx.xxxx.xxxx

Add

DHCP Forward Protocol Table

Showing 10 Entries

Showing 1 to 1 of 1 entries

Search

	Forward Protocol	Interface	Helper-server Address
<input type="checkbox"/>	67(active)	Vlan20	192.168.20.80

Delete

First
Previous
1
Next
Last

DHCP Broadcast Suppress	On: Enable DHCP broadcast suppress function Off: Disable DHCP broadcast suppress function Default is off	
DHCP Relay Forwarding	On: Sets DHCP relay to forward UPD broadcast packets on the port Off: Disable DHCP Relay Forwarding Defaul is off	
Interface	Established Layer 3 interface	
Helper-server Address	IP address of the Layer 3 interface	
Operation	Add	Add a Layer 3 interface for DHCP to forward UDP packets
	Delete	Delete the Layer 3 interface through which DHCP forwards UDP packets

6.ACL Config

6.1.Time Range Config

Time Range configuration module, the user can add or delete the operation of in this module, which can be applied to various ACL.

In the absolute mode you must input the start-time , end-time is not necesary. You must input the weeks, start-time and end-time, but need not input the date including start and end time in the absolute-periodic.

You must input the weeks, start-time and end-time, but need not input the date including start and end time, and may input multi-week values,separate them with ",", such as:1-7:monday-sunday;31:daily;96:weekdays;127:weekend.

Input date format: YYYY.MM.DD.Input week format: number (1:Monday etc.),if input multi-week values,separate them with ",",such as:1,2 identify monday&tuesday..Input time format: HH:MM:SS.

Time Range Config

In the "Absolute" type, the start time and end time must be selected. If the start time and end time are the same time, only the start time can be work;In the "Absolute-period" type, a week value must be selected, including the start and end times, but cannot be the same;In the "Period" type, you must select a week value, including start and end times.

Time Range Name	<input type="text" value=""/>											
Time Range Type	Absolute											
Start Time	2023	-	01	-	01	:	00	:	00	:	00	
End Time	2023	-	01	-	01	:	00	:	00	:	00	

[Apply](#)

Time Range Table

Showing 10 Entries Showing 0 to 0 of 0 entries Search

<input type="checkbox"/>	Time Range Name	Absolute	Periodic	Absolute-periodic
0 results found.				

[Delete](#) [First](#) [Previous](#) [Next](#) [Last](#)

Time range name	Time period names must begin with alphabetic or numeric characters ,1-64 characters	
Time range type	absolute	Absolutely
	absolute-periodic	Absolute-periodic
	periodic	periodic
Week	Start or end weeks, "1-7":"monday-sunday"; "31":"daily"; "96":"weekdays"; "127":"weekend"	
Time	Start or end time,HH:MM:SS	
Date	Start or end date,YYYY.MM.DD, range2001.1.1-2038.12.31	
Operation type	Apply	Add operations
	Delete	Delete operations

6.2.IP ACL

6.2.1.IP Standard ACL

The digital standard IP access list configuration module, where users can create or modify parameters for the digital standard IP access list.

IP Standard ACL

ACL Name	<input type="text"/>	(1-64 string or number 1-99)
ACL Action	<input type="text" value="Permit"/>	
Source Address Type	<input type="text" value="Any IP"/>	
TPID	<input type="text"/>	(0-65535,Optional configuration)
VLANID	<input type="text" value="Not Configured"/>	
DSCP	<input type="text" value="Not Configured"/>	

IP Standard ACL Configuration Status Table

Showing 10 Entries Showing 0 to 0 of 0 entries Search

<input type="checkbox"/>	ACL Name	Source IP/Mask	TPID	VLANID/Mask	DSCP	ACL Action
--------------------------	----------	----------------	------	-------------	------	------------

0 results found.

List name	Digital Standard IP Access List Number 1-99	
Rule	permit	Rule permit
	deny	Rule deny
Source address type	Any IP	Match any IP address
	Specified IP	Match IP specified address
	Host IP	Match the specified host IP
Source IP	Source IP address, decimal point	
Reverse network mask	Source IP address mask, decimal point	
tpid	Label Protocol Identification ,0-65535	
VLANID	VLAN ID, 1-4094	
VLANID mask	VLAN mask, 0-4095	
dcsp	IP message priority ,0-63	

6.2.2.IP Extended ACL

Digital extension IP access list configuration module, where users can create or modify parameters for digital extension IP access list.

IP Extended ACL

ACL Name	<input type="text"/>	(1-64 string or number 100-299)
Operation Type	<input type="text" value="ICMP"/>	
ACL Action	<input type="text" value="Permit"/>	
Fragment Packet	<input type="text" value="Disabled"/>	
Source Address Type	<input type="text" value="Any IP"/>	
Destination Address Type	<input type="text" value="Any IP"/>	
IP Precedence	<input type="text" value="Not Configured"/>	
TOS	<input type="text" value="Not Configured"/>	
Time Range Name	<input type="text" value="Not Configured"/>	
ICMP Type	<input type="text" value="Not Configured"/>	
ICMP Code	<input type="text" value="Not Configured"/>	

IP Extended ACL Configuration Status Table

Showing 10 Entries Showing 0 to 0 of 0 entries Search

<input type="checkbox"/>	ACL Name	Operation Type	Source IP/Mask	Destination IP/Mask	Fragment Packet	IP Precedence	TOS	Operation Type Param	Time Range Name	ACL Action
--------------------------	----------	----------------	----------------	---------------------	-----------------	---------------	-----	----------------------	-----------------	------------

0 results found.

List name	Digital extensions IP access list numbers ,100-199	
Operation type	Extended operation type:ICMP.IGMP.TCP.UDP.EIGRP.GRE.IGRP.IPINIP.OSPF.IP.or Specified_protocol	
ACL Action	permit	Rule permit
	deny	Rule deny
Fragment packet	Optional whether long messages are transmitted in pieces	
Source address type	Any IP	Match any IP address
	Specified IP	Match IP specified address
	Host IP	Match the specified host IP
Source IP	Source IP address, decimal point	
Reverse network mask	Source IP address mask, decimal point	
Destination address type	Any IP	Match any IP address
	Specified IP	Match IP specified address
	Host IP	Match the specified host IP
Destination IP	Destination IP, decimal points	
Reverse network mask	Destination IPaddress mask, decimal point	
IP precedence	IP priority ,0-7	
TOS	Service type ,0-15	
Time range name	Time period names to be applied must begin with alphabetic or numeric characters ,1-64 characters	
ICMP type	ICMP message type ,0-255	
ICMP code	ICMP message code ,0-255	

6.3.MAC ACL

6.3.1.MAC Standard ACL

The digital standard MAC access list configuration module, where users can create or modify parameters for the digital standard MAC access list.

MAC Standard ACL

ACL Name	<input type="text" value="(700-799)"/>	
ACL Action	Permit	
Source Address Type	Any MAC	

[Apply](#)

MAC Standard ACL Configuration Status Table

Showing 10	▼ Entries	Showing 0 to 0 of 0 entries	Search <input type="text"/>	
<input type="checkbox"/>	ACL Name	Source MAC/Mask	ACL Action	
0 results found.				
Delete			First Previous Next Last	

List name	Digital Standard MAC Access List Number 700-799	
ACL Action	permit	Rule permit
	deny	Rule deny
Source address type	Any MAC	Match any MAC address
	Specified MAC	Match MAC specified address
	Host MAC	Match the specified host MAC
Source MAC	Source MAC address	
Reverse network mask	source MAC address inverse mask	

6.3.2.MAC Extended ACL

Name extension MAC access list configuration module, where users can create or modify parameters for named extension MAC access list.

MAC Extended ACL

ACL Name	<input type="text"/>	(1-64 string or number 1100-1199)
ACL Action	Permit	▼
Source Address Type	Any MAC	▼
Destination Address Type	Any MAC	▼
Packet Type	None	▼
Cos	Not Configured	▼
Cos Mask	Not Configured	▼
VLANID	Not Configured	▼
EtherType	<input type="text"/>	(1536-65535, Optional configure)
EtherType Mask	Not Configured	▼

[Apply](#)

MAC Extended ACL Configuration Status Table

Showing 10 Entries Showing 0 to 0 of 0 entries Search

<input type="checkbox"/>	ACL Name	Source MAC/Mask	Destination MAC/Mask	Packet Type	Cos/Mask	VLANID/Mask	EtherType/Mask	ACL Action
0 results found.								

[Delete](#) [First](#) [Previous](#) [Next](#) [Last](#)

List name	Digital Extension MAC-IP Access List Number ,3100-3199	
ACL Action	permit	Rule permit
	deny	Rule deny
Source address type	Any MAC	Match any MAC address
	Specified MAC	Match MAC specified address
	Host MAC	Match the specified host MAC
Source MAC	Source MAC address	
Reverse network mask	source MAC address inverse mask	
Destination address type	Any MAC	Match any MAC address
	Specified MAC	Match MAC specified address
	Host MAC	Match the specified host MAC
Destination MAC	Destination MAC address	

Reverse network mask	Destination MAC address inverse mask	
Packet type	none	none
	tagged-802-3	Format of marked Ethernet 802-3 packets
	tagged-eth2	Format of marked Ethernet II packets
	untagged-802-3	Format of unmarked Ethernet 802-3 packets
	untagged-eth2	Format of unmarked Ethernet II packets
cos	cos, 0-7	
cos mask	cos mask, 0-7	
VLANID	VLAN ID, 1-4094	
VLANID mask	VLAN mask, 0-4095	
etherType	Ethernet type field value, 1536-65535	
etherType mask	Ethernet type field value mask, 0-65535	

6.4.MAC-IP Extended ACL

Name extension MAC-IP access list configuration module, where users can create or modify parameters for named extension MAC-IP access list.

MAC-IP Extended ACL

ACL Name	<input type="text"/>	(1-64 string or number 3100-3299)
Operation Type	ICMP	▼
ACL Action	Permit	▼
Source Address Type	Any MAC	▼
Destination Address Type	Any MAC	▼
Source Address Type	Any IP	▼
Destination Address Type	Any IP	▼
Paramer Options	Not Configured	▼
TPID	<input type="text"/>	(0-65535,Optional configuration)
VLANID	Not Configured	▼
Time Range Name	Not Configured	▼
ICMP Type	Not Configured	▼
ICMP Code	Not Configured	▼

[Apply](#)

MAC-IP Extendar ACL Configuration Status Table

Showing 10 Entries Showing 0 to 0 of 0 entries Search

<input type="checkbox"/>	ACL Name	Operation Type	Source MAC/Mask	Destination MAC/Mask	Source IP/Mask	Destination IP/Mask	TPID	VLANID/Mask	DSCP	IP Precedence	TOS	Operation Type Paramer	Time Range Name	ACL Action
0 results found.														

[Delete](#) [First](#) [Previous](#) [Next](#) [Last](#)

List name	Digital Extension MAC-IP Access List Number ,3100-3199	
Operation type	Extension operation type: ICMP.IGMP.TCP.UDP.EIGRP.GRE.IGRP.IPINIP.OSPF.IP.or Specified_protocol	
ACL Action	permit	Rule permit
	deny	Rule deny
Source address type	Any MAC	Match any MAC address
	Specified MAC	Match MAC specified address
	Host MAC	Match the specified host MAC
Source MAC	Source MAC address	
Reverse network mask	source MAC address inverse mask	
Destination address type	Any MAC	Match any MAC address
	Specified MAC	Match MAC specified address
	Host MAC	Match the specified host MAC
Destination MAC	Destination MAC address	
Reverse network mask	Destination MAC address inverse mask	
Source address type	Any IP	Match any IP address
	Specified IP	Match IP specified address
	Host IP	Match the specified host IP
Source IP	Source IP address, decimal point	
Reverse network mask	Source IP address mask, decimal point	
Destination address type	Any IP	Match any IP address
	Specified IP	Match IP specified address
	Host IP	Match the specified host IP
Destination IP	Destination IP, decimal points	
Reverse network mask	Destination IPaddress mask, decimal point	
tpid	Label Protocol Identification ,0-65535	
VLANID	VLAN ID, 1-4094	
VLANID mask	VLAN mask, 0-4095	
dcsp	IP message priority 0-63	
IP precedence	IP priority ,0-7	
TOS	Service type ,0-15	
Time range name	Time period names to be applied must begin with alphabetic or numeric characters ,1-64 characters	
ICMP type	ICMP message type ,0-255	
ICMP code	ICMP message code ,0-255	

6.5.ACL Binding

6.5.1.Binding Port

ACL port binding module, the user can bind and delete the access list of the specified port.

Binding Port

Port

--Please select --

ACL Type

IP

ACL Name

Attached Direction

Ingress

Apply

Port Binding Status Table

Showing 10 Entries

Showing 0 to 0 of 0 entries

Search

	Port	ACL Name	ACL Type	Attached Direction
0 results found.				

Delete

First

Previous

Next

Last

Port	Designated port number	
ACL type	IP	IP type
	MAC	MAC type
	MAC-IP	MAC-IP type
List name	Specify access list name ,1-64 characters	
ACL Attached Direction	in	Application ACL only
	in and traffic-statistics	Application ACL and flow monitoring
Operation type	Apply	Add operations
	Delete	Delete operations

6.5.2.Binding Vlan

ACL vlan binding module, where users can bind and delete access lists to specified VLAN.

Binding Vlan

VLAN Interface

--Please select --

ACL Type

IP

ACL Name

Attached Direction

Ingress

Apply

VLAN Binding Status Table

Showing 10 Entries

Showing 0 to 0 of 0 entries

Search

	VLAN Interface	ACL Name	ACL Type	Attached Direction
0 results found.				

Delete

First

Previous

Next

Last

VLAN interface	Specifies the VLAN number to operate on	
ACL type	Specifies the type of ACL to bind: IP.MAC.MAC-IP	
List name	Specify access list name ,1-64 characters	
ACL Attached Direction	in	Application ACL only
	in and traffic-statistics	Application ACL and flow monitoring
Operation type	Add	Add operations
	Remove	Delete operations

7.Ring Network

7.1.Spanning-tree

7.1.1.Global Properties

This page uses the build tree function with global enable.

To display the “Global Properties” page, click Ring Network -> Spanning-tree -> Global Properties, click "Apply" to configure.

Global Properties

This page is used to configure the global basic parameters of the spanning tree.

Enabled

☐ Off

entry	describe
Operation	On: enable spanning tree function Off: disables spanning tree functionality

Global Properties

This page is used to configure the global basic parameters of the spanning tree.

Enabled	<input checked="" type="checkbox"/>
Mode	Mstp
Cost Format	dot1t
Forward Time	15 <small>Sec(4-30, default 15)</small>
Hello Time	2 <small>Sec(1-10, default 2)</small>
Max Age Time	20 <small>Sec(6-40, default 20)</small>
Max Hop Time	20 <small>(1-40, default 20)</small>
Priority	32768 <small>(0-61440, default 32768)</small>
TC Flush	Flush

Apply

Mode	Generating tree protocol type: Mstp.Stp.Rstp
Cost Format	Path cost format:Dot1t.Dot1d
Forward Time	Size range :4-30, in seconds,the following conditions shall be met: $2 * (\text{Bridge_Forward_Delay} - 1.0 \text{ seconds}) \geq \text{Bridge_Max_Age}$ $\text{Bridge_Max_Age} \geq 2 * (\text{Bridge_Hello_Time} + 1.0 \text{ seconds})$
Hello Time	Size range :1-10, in seconds,the following conditions shall be met: $2 * (\text{Bridge_Forward_Delay} - 1.0 \text{ seconds}) \geq \text{Bridge_Max_Age}$

	Bridge_Max_Age >= 2 * (Bridge_Hello_Time + 1.0 seconds)
Max Age Time	Size range :6-40, in seconds,the following conditions shall be met: 2 * (Bridge_Forward_Delay - 1.0 seconds) >= Bridge_Max_Age Bridge_Max_Age >= 2 * (Bridge_Hello_Time + 1.0 seconds)
Max Hop Time	Numerical range :1-40
Priority	Numerical range :0-61440, and an integer multiple of 4096

7.1.2.Instance Mapping

This page can be used to configure the mapping relationship between the spanning tree instance and the VLAN.

Instance Mapping

This page is used to generate tree instance mapping vlan configuration.

Instance Mapping Configuration	
Instance	0 ▼
Operation	Add ▼
VLAN List	<input type="text"/> (1-4094, for example: 1;3-6)

Apply

Instance Mapping Status

Showing 10 Entries

Showing 1 to 1 of 1 entries

Search

Instance	VLAN List
0	1-4094

First
Previous
1
Next
Last

entry	describe
Instance name	Generating tree instance ID, range 0-64
Operation	Add: Add the above configuration information Delete: Delete the above configuration information
VLAN name	VLAN ID, range : 1-4094

Instance Mapping Status

Showing 10 Entries

Showing 1 to 1 of 1 entries

Search

Instance	VLAN List
0	1-4094

First
Previous
1
Next
Last

entry	describe
Instance name	Generating tree instance ID, size range 0-64
VLAN name	VLAN ID, range : 1-4094

7.1.3.Instance Properties

This page can be used to configure MSTP domain name and MSTP revision level.

Instance Properties

This page is used for spanning tree instance parameter configuration.

Instance Properties Configuration	
Field Name	<input type="text" value=""/> (1-32 characters, and cannot special char(!%#\$%&< > *^ \), not entering indicates deletion)
Revision-level	<input type="text" value=""/> (0-65535)

Apply

Field Name	Revision-level
	0

entry	describe
Field name	MSTP domain name, the length is 1-32 characters
Revision-level	Range :0-65535
Operation	Apply: Use the above configuration

7.1.4.Port Config

This page can be used to configure enable or disable the tree generation function under the port.

Port Config

This page is used to generate tree port parameter configuration.

Port	<input type="text" value="--Please select --"/>	
Status	<input type="button" value="Enabled"/>	<input type="button" value="Disabled"/>
BPDU	<input type="button" value="Enabled"/>	<input type="button" value="Disabled"/>
Edge Port	<input type="button" value="Enabled"/>	<input type="button" value="Disabled"/>
Point-to-Point	<input type="button" value="Auto"/>	<input type="button" value="Disabled"/>
Packet Format	<input type="button" value="Auto"/>	<input type="button" value="Disabled"/>
Digest Snooping	<input type="button" value="Enabled"/>	<input type="button" value="Disabled"/>
TC Flush	<input type="button" value="Default"/>	<input type="button" value="(Default to global TC FLUSH value)"/>

Apply Protocol Migration Check

Port	Status	BPDU	Edge Port	Point-to-Point	Packet Format	Digest Snooping	TC Flush
Ethernet1/0/1	Enabled	Disabled	Disabled	Auto	Auto	Disabled	Flush
Ethernet1/0/2	Enabled	Disabled	Disabled	Auto	Auto	Disabled	Flush
Ethernet1/0/3	Enabled	Disabled	Disabled	Auto	Auto	Disabled	Flush
Ethernet1/0/4	Enabled	Disabled	Disabled	Auto	Auto	Disabled	Flush
Ethernet1/0/5	Enabled	Disabled	Disabled	Auto	Auto	Disabled	Flush
Ethernet1/0/6	Enabled	Disabled	Disabled	Auto	Auto	Disabled	Flush
Ethernet1/0/7	Enabled	Disabled	Disabled	Auto	Auto	Disabled	Flush
Ethernet1/0/8	Enabled	Disabled	Disabled	Auto	Auto	Disabled	Flush

Port	Ethernet port name
Status	Enable: Port enable spanning tree function Disable: Port disables spanning tree functionality
BPDU	Disabled; VLAN:1-4094
Edge Port	Disabled; Enabled;

	BPDU Filter; BPDU Guard;
Point-to-Point	Auto; Disabled; Enabled;
Packet Format	Auto; Privacy; Standard;
Digest Snooping	Disabled; Enabled;
TC Flush	no Flush; Flush; Limit
Operation	Apply
	Protocol Migration Check

7.1.5.Port Instance

This page can be used for configuration of instance port priority.

Port Instance

This page is used to generate tree port instance parameter configuration.

Instance	0				
Port	--Please select --				
Path Cost	0	(0-200000000)(0=>Auto)			
Priority	0				
Port Guard	Auto				

Apply

Instance	Port	Path Cost	Priority	Port Guard
0	Ethernet1/0/1	Auto	128	Auto
0	Ethernet1/0/2	Auto	128	Auto
0	Ethernet1/0/3	Auto	128	Auto
0	Ethernet1/0/4	Auto	128	Auto
0	Ethernet1/0/5	Auto	128	Auto
0	Ethernet1/0/6	Auto	128	Auto
0	Ethernet1/0/7	Auto	128	Auto
0	Ethernet1/0/8	Auto	128	Auto

Instance name	Generate tree instance name
Port	Ethernet port name
Cost	Size range :0-200000000
Priority	The size range is :0-240, multiple of 16
Priority	Auto; Root Guard; Loop Guard;
Operation	Configuration: Apply the above configuration

7.1.6.Status

This page can be used to view information for the spanning-tree status.

Runing Status Information

MSTP Bridge Config Info							
Mode	Bridge MAC	Max Age Time	Hello Time	Forward Time	Force Version		
RSTP(IEEE 802.1s)	84e5d8e01cb1	20s	2s	15s	3		

Instance0	
Self Bridge ID	32768.84e5d8e01cb1
Root ID	this switch
Ext.RootPathCost	0
Region Root ID	this switch
Int.RootPathCost	0
Root Port ID	0

Port	ID	Max Age Time	Int.RootPathCost	State	Role	DsgBridge	DsgPort
Ethernet1/0/2	128.002	0	0	Forward	DSGN	32768.84e5d8e01cb1	128.002

7.2.ERPS

7.2.1.ERPS Ring Config

This page can be used for configuration of ERPS Ring.

ERPS Ring Config

Create or delete ERPS ring.

Topology Change Propagation None

Apply

Ring Name	<input type="text"/>	(1-64 character)
Version	V2	
Ring-topo	major-ring	
Port1 Configure	Yes	
Port0	Ethernet1/0/1	
Port1	Ethernet1/0/2	
R-APS Virtual-Channel	Without	

Apply

ERPS Configuration Status Table

Showing 10 Entries

Showing 0 to 0 of 0 entries

Search

<input type="checkbox"/>	Ring Name	Port0	Port1	Ring-topo	R-APS Virtual-Channel	Version	Instance Count
0 results found.							

Delete

First Previous Next Last

Topology Change Propagation	None; ERPS; STP;
Ring Name	The ERPS ring name created,1-64 character
Version	If configured ERPS ring to support v1, this ring will not support multi-instance. ERPS ring instance does not support the management commands of MS, FS. If configured ERPS ring to support v2, the instance of this ring will deal with the ERPS packets according to the v1 format. Package the R-APS packets and resolve the fields according to v1 format. The fields defined by v2 will not be dealt.

	V1: Means to support v1 which is released in 2008-06 and the amendment (2009-04) V2: Means to support v2 which is released in 2010-03 and the amendment (2010-06)
Ring-topo	major-ring: Configure the ERPS ring as the major ring open-ring: Configure the ERPS ring as the open ring
Port1 Configure	No: Port1 is not allowed to be configured. Yes: Port1 is allowed to be configured.
Port0	Select port as Port 0 for ERPS
Port1	Select port as Port 1 for ERPS
R-APS Virtual-Channel	Configure if there is the R-APS virtual channel in ERPS ring according to the configuration. Inputting: Success or error. If there is not R-APS virtual channel on the ERPS ring, the R-APS channel of all the instances of ERPS ring will be unblocked forever and it only blocks the data channel; otherwise, the R-APS channel and the data channel will be blocked at the same time. Without: The R-APS virtual channel is not existed in this ERPS ring. With: The R-APS virtual channel is existed in this ERPS ring.
Operation	Apply
	Delete

7.2.2.ERPS Instance Config

This page can be used for configuration of ERPS Instance.

ERPS Instance Config

Ring Name	1	▼
Instance ID	1	▼
Control VLAN	VLAN0002	▼
Ring ID	1	▼
R-APS MEL	7	▼
Description	(1-64 characters)	
Revertive Mode	Revertive	▼
Protected Instance	(0-64,use '-' and '/' splice,for example:1-3-6)	
WTR Timer	5	(1-12min,default 5)
Guard Timer	50	(1-200ms,default 50)
Holdoff Timer	0	(0-10s,default 0)
Port0 Role	Common	▼
Port1 Role	Common	▼

[Apply](#)

ERPS Configuration Status Table

Showing 10 ▼ Entries												Showing 0 to 0 of 0 entries		Search	
<input type="checkbox"/>	Ring Name	Instance ID	Control VLAN	Ring ID	R-APS MEL	Description	Revertive Mode	Protected Instance	WTR Timer	Guard Timer	Holdoff Timer	Port0 Role	Port1 Role		
0 results found.															
Delete															
First Previous Next Last															

Ring Name	Select the ERPS ring you created
Instance ID	Create the ERPS ring instance ID, id of ERPS ring, the range is 1 to 16

Control Vlan	vlan id of R-APS packets, range is from 2 to 4094
Ring ID	ERPS ring id and the range is 1 to 64
R-APS MEL	The level value of APS packets, range is from 1 to 7
Description	ERPS instance name, the maximum string is 64, and it is made up with letters, numbers and underlines; the first and last characters cannot be underlines.
Revertive Mode	Configure the ERPS ring instance as non-revertive. If this ERPS ring supports v1, then cannot be configured. Only configured on the RPL owner node of the sub ring. Non-Revertive; Revertive;
Protect ID	The MSTP instance list protected by ERPS ring instance
WTR Timer	WTR timer is used to avoid the frequent protection switching of RPL owner node because of the periodic (intermittent) default. The interval is 1min and the range is from 1 to 12min, default is 5min.
Guard Timer	The guard timer is used for the Ethernet node to avoid the error handling and the close loop according to the outdated R-APS packets. The interval is 10ms and the range is 10ms to 2s, default is 500ms.
Holdoff Timer	The interval is 1s and the range is 0 to 10s, default is 0s.
Port0 Role	Common is default config, it is the ordinary transmission node type. <ul style="list-style-type: none"> • Owner • Neighbour • Common
Port1 Role	
Operation	Apply
	Delete

7.2.3.View ERPS Statistics

This page can be used for configuration of ERPS Statistics.

View ERPS Statistics															
ERPS Instance Table															
Showing	10	Entries	Showing 0 to 0 of 0 entries										Search		
Ring Name	Instance ID	Instance Port	Port Role	Port Status	Signal Status	Node Id	BPR	nrTx	nrRx	rbTx	rbRx	fsTx	fsRx	msTx	msRx
0 results found.															
First Previous Next Last															

Ring Name	The ERPS ring name whe you created
Instance ID	The ERPS ring instance ID when you create
Intance Port	The ERPS ring member ports

Port Role	ERPS ring node roles: RPL Owner, RPL neighbor, Common
Port States	Blocked: port is in block status forwarding: port is in forwarding status
Signal Status	ERPS ring port fault status: Non-failed: no fault Failed: fault happened
Last NodeID	The node ID information is the last bit of the MAC
Last Bpr	The block link information carried by the receiving last R-APS saved by ERPS ring port, it is port0 or port1 which was blocked.
rbTX	RB transport statistics
rbRX	RB receive statistics
nrTX	NR transport statistics
nrRX	NR receive statistics
fsTX	FS transport statistics
fsRX	FS receive statistics
msTX	MS transport statistics
msRX	MS receive statistics
sfTX	SF transport statistics
sfRX	SF receive statistics
eventTX	Event transport statistics
eventRX	Event receive statistics
totalTX	Total transport statistics
totalRX	Total receive statistics

8.Route Config

8.1.Static Route

This page can be used for the basic configuration of static routing.

Static Route

Destination IP Address

Mask Or Prefix-length

Nextthop Or null0

Distance

1

Apply

Static Routing Configuration Status Table

Showing 10 Entries

Showing 0 to 0 of 0 entries

Search

	Destination IP Address/Mask	Nextthop Or null0	Distance	State
0 results found.				

Delete

First Previous Next Last

Destination IP address	IP address, format :10.10.11.11
Network mask or prefix-length	Subnet mask in the following format :255.255.255.0; or mask length
Nextthop or Interface null0	IP address, format :10.10.11.11. or null0
Distance	Range :1-255
Operation type	Apply: Add the above settings Delete: Delete the above

8.2.RIP Route

8.2.1.Keychain

This page can be used for config keychain function.

Keychain

Keychain Name

(1-80 characters)

Key ID

(0-2147483647)

Key

(1-256 character)

Add

Keychain Information Table

Showing 10 Entries

Showing 0 to 0 of 0 entries

Search

No.	Keychain Name	Key ID	Key
0 results found.			

Delete Keychain

Delete Key ID

First Previous Next Last

Keychain Name	Keychain Name, range 1-80 characters
Key ID	Key ID, range 0-2147483647
Key	Key, range 1-256 character。

8.2.2.Basic Config

This page can be used for enable RIP function.

Basic Config

RIP Status ☐ Off

Basic Config

RIP Status	<input checked="" type="radio"/> On	
Add Default Route	Disabled ▼	
Default Metric	1 ▼	
Version	V2 ▼	
Recv Buffer Size	0	(8192-2147483647 Byte,default:0)
Update	30	(5-2147483647 Sec)
Timeout	180	(5-2147483647 Sec)
Garbage	120	(5-2147483647 Sec)
Maximum Prefix	10000 (1-65535)	75% ▼

Add Default Route	Control distribution of default route, distribute a default route.
Default Metric	Set a metric of redistribute routes, range is 1-16, default is 1.
Version	Config RIP version v1/v2, default is v2.
Recv Buffer Size	The RIP UDP receive buffer size value, default is 8192.
Update	Routing table update timer value in second. Default is 30.
Timeout	Routing information timeout timer. Default is 180.
Garbage	Garbage collection timer. Default is 120.
Maximum Prefix	Maximum number of RIP routes, default is 10000. Percentage of maximum routes to generate a warning (Default 75%)

8.2.3.Network Config

This page can be used for RIP network config.

Network Config

Interface Type

VLAN

Interface Value

(1-4094)

Add

Network Config Table

Showing 10 Entries

Showing 0 to 0 of 0 entries

Search

No.

Network Interface Configured

0 results found.

Delete

First

Previous

Next

Last

Network Config

Interface Type

Tunnel

Interface Value

(1-50)

Add

Network Config Table

Showing 10 Entries

Showing 0 to 0 of 0 entries

Search

No.

Network Interface Configured

0 results found.

Delete

First

Previous

Next

Last

Network Config

Interface Type

Loopback

Interface Value

(1-1024)

Add

Network Config Table

Showing 10 Entries

Showing 0 to 0 of 0 entries

Search

No.

Network Interface Configured

0 results found.

Delete

First

Previous

Next

Last

Network Config

Interface Type

IP Prefix

Interface Value

IP Address

/ Prefix

Add

Network Config Table

Showing 10 Entries

Showing 0 to 0 of 0 entries

Search

No.

Network Interface Configured

0 results found.

Delete

First

Previous

Next

Last

Interface Type	VLAN: vlan Tunnel: Tunnel interface Loopback: loopback IP Prefix: IP prefix <network>/<length>, e.g., 35.0.0.0/8
Interface Value	VLAN: interface name,1-4094. Tunnel: Tunnel interface number, 1-50. Loopback: Loopback ID <1-1024> IP Prefix: IP prefix <network>/<length>, e.g., 35.0.0.0/8

8.2.4.Passive Interface

This page can be used for RIP passive interface.

Passive Interface

The configured interface only receives and does not send data packets.

Interface Type

VLAN

Interface Value

VLAN0001

Add

Passive Interface Config Table

Showing 10 Entries

Showing 0 to 0 of 0 entries

Search

No.

Passive Interface

0 results found.

Delete

First Previous Next Last

Passive Interface

The configured interface only receives and does not send data packets.

Interface Type

Tunnel

Interface Value

(1-50)

Add

Passive Interface Config Table

Showing 10 Entries

Showing 0 to 0 of 0 entries

Search

No.

Passive Interface

0 results found.

Delete

First Previous Next Last

Interface Type	VLAN: vlan Tunnel: Tunnel interface
Interface Value	VLAN: interface name,1-4094. Tunnel: Tunnel interface number, 1-50.

8.2.5.Neighbor Config

This page can be used for RIP neighbor config.

Neighbor Config

Neighbor Address

Add

Neighbor Config Table

Showing 10 Entries

Showing 0 to 0 of 0 entries

Search

No.

Neighbor Address

0 results found.

Delete

First Previous Next Last

Neighbor Address	Neighbor address: A.B.C.D
------------------	---------------------------

8.2.6.Interface Config

This page can be used for RIP interface config.

Interface Config

VLAN Interface	VLAN0001
Send Version	Disabled
Send Packet	Enabled
Recv Version	Disabled
Recv Packet	Enabled
Authentication Mode	None
Compatible With Cisco	Disabled
Split Horizon	Poisoned

[Apply](#)

Interface Config Table

Showing 10 Entries Showing 0 to 0 of 0 entries Search

No.	VLAN Interface	Send Version	Send Packet	Recv Version	Recv Packet	Authentication Mode	Key	Keychain Name	Compatible With Cisco	Split Horizon
0 results found.										

[First](#) [Previous](#) [Next](#) [Last](#)

VLAN Interface	Select Interface VLAN
Send Version	Advertisement transmission 1: RIP version 1 2: RIP version 2 1-compatible: RIPv1-compatible 2: RIP version 2 2 1: RIP version 2 RIP version 1
Recv Version	Advertisement reception 1: RIP version 1 2: RIP version 2
Authentication Mode	None: Not config MD5: Keyed message digest Plaintext: Clear text authentication
Compatible With Cisco	Compatible with cisco
Split Horizon	Poisoned: means configure the split horizon with poison reverse.,Split Horizon with poison reverse by default.
	Enabled: enable split horizon
	Disabled: disable split horizon

8.2.7.Redistribute Router

This page can be used for RIP Redistribute Router config.

Redistribute Router

Routing Type	Connected ▼
Metric	Not Configured ▼

Add

Redistribute Router Table

Showing 10 ▼ Entries
Showing 0 to 0 of 0 entries
Search

	No.	Routing Type	OSPF Process ID	Metric
0 results found.				

Delete

First
Previous
Next
Last

Routing Type	Connected: redistribute connected routes
	Kernel: redistribute kernel routes
	OSPF Route: redistribute ospf routes
	BGP Route: redistribute bgp routes
	Static Route: redistribute static routes
Metric	0-16, default is not configured
OSPF Process ID	Redistribute OSPF Process ID, 1-65535, No parameters indicate the default process

8.2.8.View RIP Information

This page can be used for view RIP information.

View RIP Information

RIP Entries
RIP Information ▼

RIP Routing Information Table

Codes: R - RIP, K - Kernel, C - Connected, S - Static, O - OSPF, I - IS-IS,
B - BGP, a - aggregate, s - suppressed
Network Next Hop Metric From If Time Supplf

RIP Entries	RIP Information	Show the RIP related messages
	RIP Interface	Show the routes in the RIP route database
	RIP Protocol	Show the RIP process parameter and statistics information

8.3.OSPF Route

8.3.1.Basic Config

This page can be used for OSPF basic config.

Basic Config

Process ID

(0-65535)

Router ID

IP Address

Add

OSPF Process ID Table

Showing 10 Entries

Showing 1 to 1 of 1 entries

Search

	No.	Process ID	Router ID
<input type="checkbox"/>	1	1	192.168.2.1

Delete

First Previous 1 Next Last

Process ID	OSPF process ID, 0-65535.
Router ID	OSPF router-id in IP address format: A.B.C.D

8.3.2.Network Config

This page can be used for OSPF network config.

Network Config

Process ID

1

Network Address

IP Address / Prefix

Area Number

(0-4294967295 or IP)

Add

OSPF Area Network Table

Showing 10 Entries

Showing 1 to 1 of 1 entries

Search

	No.	Process ID	Network Address	Area Number
<input type="checkbox"/>	1	1	1.1.1.0/24	0

Delete

First Previous 1 Next Last

Process ID	Select OSPF process ID.
Network Address	OSPF network prefix:A.B.C.D/M
Area Number	Set the OSPF area ID OSPF area ID as a decimal value:0-4294967295 OSPF area ID in IP address format: A.B.C.D

8.3.3.Passive Interface

This page can be used for OSPF passive interface.

Passive Interface

The configured interface only receives and does not send data packets.

Process ID

1

Interface

Vlan1

Add

Passive Interface Config Table

Showing 10 Entries

Showing 0 to 0 of 0 entries

Search

No.	Process ID	Interface
0 results found.		

Delete

FirstPreviousNextLast

Process ID	Select OSPF process ID.
Interface Value	Interface name

8.3.4.Area Config

This page can be used for OSPF area config.

Area Config

Process ID

1

Area Number

0

Operation Type

Authentication

Authentication Mode

None

Apply

OSPF Area Basic Config Table

Process ID	Area Number	Authentication Mode	Cost
1	0	None	1

OSPF Area Range Config Table

Showing 10 Entries

Showing 0 to 0 of 0 entries

Search

No.	Process ID	Area Number	Range Prefix	Type	Substitute Range Prefix
0 results found.					

Delete

FirstPreviousNextLast

Process ID	Select OSPF process ID.
Area Number	Select the OSPF area ID
Operation Type	Authentication: Enable authentication Default-Cost: Set the summary-default cost of a NSSA or stub area Range: Summarize routes matching address/mask (border routers only)
Authentication Mode	None: Not config

	MD5: Use message-digest authentication Plaintext: Use text authentication
Cost	Stub's advertised default summary cost, 0-16777215
Range Prefix	Area range prefix: A.B.C.D/M
Type	Advertise: Advertise this range (default) Not-Advertise: DoNotAdvertise this range Substitute: Announce area range as another prefix

8.3.5.Interface Config

This page can be used for OSPF interface config.

Interface Config

Interface Name	Disable OSPF
Vlan1 ▼	Disabled ▼

Apply

Interface Config

Interface Name	Disable OSPF
Vlan40 ▼	Disabled ▼

Basic Configuration of OSPF Interface					
Cost	1	(1-65535,default 1)	Priority	1	(0-255, default 1)
Hello Interval	10	(1-65535s,default:10s)	Transmit Delay	1	(1-3600s,default:1s)
Dead Interval	40	(1-65535s,default:40s)	Ignore MTU	Disabled	▼
Retransmit Interval	5	(1-3600s,default:5s)	Database Filter	Disabled	▼
MTU	1500	(576-65535,default:1500)	Network Type	Broadcast	▼

Apply

Interface Name	Select Interface VLAN name
Disable OSPF	Enabled: Set Disable OSPF. Disabled: Set Enable OSPF.
Cost	Interface cost, <1-65535>
Priority	Router priority, <0-255>
Hello Interval	Time between HELLO packets, <1-65535> Seconds
Transmit Delay	Link state transmit delay <1-3600> Seconds
Dead Interval	Interval after which a neighbor is declared dead, <1-65535> Seconds
Ignore MTU	Ignores the MTU in DBD packets

	Disabled: Set disable ignore mtu Enabled: Set enable ignore mtu
Retransmit Interval	Time between retransmitting lost link state advertisements, <1-3600> Seconds
Database Filter	Filter OSPF LSA during synchronization and flooding Disabled: Set disable database filter. Enabled: Set enable database filter.
MTU	OSPF interface MTU, <576-65535> MTU size
Network Type	Network type Broadcast: Specify OSPF broadcast multi-access network non-broadcast: Specify OSPF NBMA network point-to-multipoint: Specify OSPF point-to-multipoint network point-to-point: Specify OSPF point-to-point network

OSPF Interface Status Table

Link State	Process ID	Router ID	Area Number	Network Address	Hello	State
Down	1	20.10.0.10	0.0.0.1	80.1.1.1/24	00:00:04	Backup
Neighbor/Adjacent	Hello(RX/TX)	DD(RX/TX)	LS-Req(RX/TX)	LS-Upd(RX/TX)	LS-Ack(RX/TX)	Sequence/Discarded
1/1	18132/18812	22/40	11/11	122/769	769/122	0/0
Designated Router						
Router ID			Network Address			
20.10.0.30			80.1.1.20			
Backup Designated Router						
Router ID			Network Address			
20.10.0.10			80.1.1.1			

Link State	Interface vlan link state
Process ID	OSPF process ID
Router ID	OSPF router ID
Area Number	OSPF interface area number
Network Address	OSPF interface network address
Hello	OSPF Hello due
State	OSPF interface state
Neighbor/Adjacent	OSPF interface Neighbor Count/ Adjacent neighbor count
Hello(RX/TX)	Hello received/sent
DD(RX/TX)	DD received/sent
LS-Req(RX/TX)	LS-Req received/sent
LS-Upd(RX/TX)	LS-Upd received/sent

LS-Ack(RX/TX)	LS-Ack received/sent
Sequence/Discarded	Crypt Sequence Number/Discarded
Designated Router	OSPF interface Designated Router
Router ID	Designated Router ID
Network Address	Designated Router Network Address
Backup Designated Router	OSPF interface Backup Designated Router
Router ID	Backup Designated Router ID
Network Address	Backup Designated Router Network Address

8.3.6.Interface Authentication

This page can be used for OSPF interface authentication config.

Interface Authentication

Interface Name

Vlan1

Interface Authentication Method

Authentication Method

None

Apply

Key Config

Encryption Type

Simple Key

Key Type

Plain Key

Key

(1-8 characters)

Apply

OSPF Interface Authentication Status Table

Authentication Method	
None	

Delete Simple Authentication Key

OSPF Interface MD5 Key Table

Showing 10 Entries

Showing 0 to 0 of 0 entries

Search

No.	Key ID	Key Type	Key

0 results found.

Delete

First Previous Next Last

Interface Name	Select interface vlan name
Authentication Method	None: No Authentication
	Simple: Simple Authentication
	MD5: MD5 Authentication
Simple Key	Simple Authentication Key,1-8 characters
MD5 Key	MD5 Authentication Key,1-16 characters
Plain key	1-8 characters
Cipher Key	1-16 characters, input plaintext application to encrypt ciphertext
Key ID	MD5 Key ID, 1-255

8.3.7.Default Route Originate

This page can be used for OSPF default route originate config.

Default Route Originate

OSPF Process ID	0	
Default-Information Originate	Enabled	
Always	Disabled	
Metric Type	External Type 2	
Metric		(0-16777214, No parameter indicates no setting)

[Apply](#)

OSPF Process ID	Select OSPF Process ID
Default-Information Originate	Create a default external route to OSPF route area, Enabled/Disabled
Always	Whether default route exist in the software or not, the default route is always advertised. Enabled/Disabled
Metric Type	External Type 1: Set the OSPF external type 1 metric value External Type 2: Set the OSPF External Type 2 metric value, default is External Type 2
Metric	Set the metric value for creating default route, Ranges between 0-16777214

8.3.8.Redistribute Router

This page can be used for OSPF redistribute router config.

Redistribute Router

OSPF Process ID	0	
Routing Type	Connected	
Tag Value		(0-4294967295, Default is 0, No parameters indicates default value)
Metric Type	External Type 2	
Metric		(0-16777214, No parameter indicates no setting)

[Add](#)

Redistribute Router Table

Showing	10	Entries	Showing 0 to 0 of 0 entries				Search	
<input type="checkbox"/>	No.	Routing Type	Redistribute OSPF Process ID	Tag Value	Metric Type	Metric		
0 results found.								
Delete							First Previous Next Last	

OSPF Process ID	Select OSPF Process ID
Routing Type	Connected: introduce from direct route Kernel: introduce from kernel route BGP Route: introduce from BGP route RIP Route: introduce from the RIP route OSPF Route: introduce from OSPF route Static Route: introduce from static route
Tag Value	External identification number of the external route, ranging between 0-4294967295, defaulted at 0
Redistribute OSPF Process ID	OSPF process ID, 0 by default

Metric Type	External Type 1: Set the OSPF external type 1 metric value
	External Type 2: Set the OSPF External Type 2 metric value, default is External Type 2
Metric	Set the metric value for creating default route, Ranges between 0-16777214

8.3.9.View OSPF Information

This page can be used for view OSPF Information config.

View OSPF Information

OSPF Entries

OSPF Information

OSPF Routing Information Table

Routing Process "ospf 0" with ID 192.168.20.70

Process bound to VRF default

Process uptime is 16 hours 48 minutes

Conforms to RFC2328, and RFC1583Compatibility flag is disabled

Supports only single TOS(TOS0) routes

Supports opaque LSA

Supports Graceful Restart

Grace period for Graceful Restart 60 secs

Supports helper mode for Graceful Restart

SPF schedule delay 5 secs, Hold time between two SPFs 10 secs

OSPF Entries	OSPF Information	Display OSPF main messages
	OSPF Database	Display the OSPF link state data base messages
	OSPF Neighbor	Display the OSPF adjacent point messages

8.4.BGP Route

8.4.1.Basic Config

This page can be used for BGP basic config.

Basic Config

BGP Global Config

Aggregate Nexthop Check

Disabled

RFC1771 Path Select

Disabled

RFC1771 Strict

Disabled

Apply

Create AS

AS Number

(Number:1-4294967295)

Add

AS Table

Showing 10 Entries

Showing 1 to 1 of 1 entries

Search

	No.	AS Number
<input type="checkbox"/>	1	1000

Delete

First

Previous

1

Next

Last

Aggregate Nexthop Check	Configures whether BGP checks all the route next-hop in aggregating. When check is enabled, the aggregate will not be performed if the next-hop of the covered routes are not in accordance. When checking is disabled, all covered route will be aggregated into the aggregate route. Default is disabled
RFC1771 Path Select	After this attribute is set, path selecting will follow the way defined in rfc 1771, namely not checking the AS internal metric, when different AS exist, which should be perform without this attribute set Default is disabled
RFC1771 Strict	Set whether strictly follows the rfc1771 restrictions. With this attribute set, generation types of routes from protocols such as RIP, OSPF, ISIS, etc will be regarded as IGP(internal generated),or else as incomplete.
AS Number	AS number, ranging from 1 to 4294967295, it can be shown in decimal notation(such as 6553700) or delimiter method(such as 100.100)

8.4.2.Network Config

This page can be used for BGP network config.

Network Config

AS Number	1000
IP Prefix	IP Address / Prefix
BACKDOOR ?	Disabled

[Add](#)

BGP Network Table

Showing 10 Entries

Showing 0 to 0 of 0 entries

Search

No.	IP Prefix	BACKDOOR
0 results found.		

[Delete](#)

[First](#)
[Previous](#)
[Next](#)
[Last](#)

AS Number	AS Number
IP Prefix	Network prefix identifie
BACKDOOR	back door parameters

8.4.3. Aggreate Address

This page can be used for BGP aggregate address config.

Aggregate Address

AS Number	1000
IP Prefix	IP Address / Prefix
Summary-Only	Enabled
AS	Enabled

[Add](#)

Address Aggregation Configuration Table

Showing 10 Entries
Showing 0 to 0 of 0 entries
Search

No.	IP Prefix	Summary-Only	AS
0 results found.			

[Delete](#)

[First](#)
[Previous](#)
[Next](#)
[Last](#)

AS Number	AS Number
IP Prefix	IP address, length of mask.
Summary-Only	Send summary only ignoring specific route.
AS	Show AS on the path in list, each AS is shown once.

8.4.4. Redistribute Router

This page can be used for BGP redistribute router config. Route from other ways will be distributed into the BGP route table

Redistribute Router

AS Number	1000
Routing Type	Connected

[Add](#)

Redistribute Router Table

Showing 10 Entries
Showing 0 to 0 of 0 entries
Search

No.	Routing Type	OSPF Process ID
0 results found.		

[Delete](#)

[First](#)
[Previous](#)
[Next](#)
[Last](#)

AS Number	AS Number	
Routing Type	Connected	redistribute connected route
	Kernel	Redistribute kernel route
	OSPF Route	redistribute OSPF Route
	RIP Route	redistribute RIP Route
	Static Route	redistribute Static Route

8.4.5.Neighbor Config

This page can be used for BGP neighbor config.

Neighbor Config

AS Number	1000	
Neighbor Address		(IPv4/IPv6,exp:1.1.1.1 or 2112::1111)
AS Number		(Number:1-4294967295)

[Add](#)

Neighbor Config Table

Showing 10 Entries
Showing 1 to 1 of 1 entries
Search

	No.	Neighbor Address	AS Number
<input type="checkbox"/>	1	2.1.1.1	1000

[Delete](#)

[First](#)
[Previous](#)
[1](#)
[Next](#)
[Last](#)

AS Number	AS Number
Neighbor Address	Neighbor IP address
AS Number	Neighbor AS number, ranging from 1 to 4294967295, it can be shown in decimal notation (such as 6553700) or delimiter method (such as 100.100).

8.4.6.BGP Correlative Config

This page can be used for BGP correlative config.

BGP Correlative Config

AS Number	1000	
Command	always-compare-med	
Command Enabled	Enabled	

[Apply](#)

Command	Command Value
always-compare-med	Disabled
bestpath as-path ignore	Disabled
bestpath compare-confed-aspath	Disabled
bestpath compare-routerid	Disabled
client-to-client reflection	Enabled
cluster-id	-
deterministic-med	Disabled
enforce-first-as	Disabled
fast-external-fallover	Enabled
log-neighbor-changes	Disabled
network	Disabled
router-id	-
scan-time	60
graceful-restart	Disabled
graceful-restart restart-time	-
graceful-restart stale-path-time	-
selection-deferral-time	-

AS Number	AS Number	
Command	always-compare-med	Configures If MED comparison is always performed
	bestpath as-path ignore	Set to ignore the AS-PATH length
	bestpath compare-confed-aspath	Set to concern the confederation AS-PATH length
	bestpath compare-routerid	Compare route ID

	client-to-client reflection	Configures whether the route reflection is performed
	cluster-id	Configure the route reflection ID during the route reflection
	deterministic-med	Use the best MED for the same prefix in the AS to compare with other AS
	enforce-first-as	Enforces the first AS position of the route AS-PATH contain the neighbor AS number or else disconnect this peer when the BGP is reviving the external routes
	fast-external-failover	Fast reset when the BGP neighbor connection varies at the interface other than wait for TCP timeout
	log-neighbor-changes	Output log message when BGP neighbor changes
	network	Set whether check the IGP accessibility of the BGP network route or not
	router-id	Configure the router ID manually
	scan-time	Set the time interval of the periodical next-hop validation
	graceful-restart	Enable BGP to support GR and set restart-time and stale-path-time as the default value
	graceful-restart restart-time	Configure BGP GR's restart-time(Receiving Speaker enables a timeout timer for a neighbor, it uses the restart-time as the timeout.) A restart-time specifies the longest waiting time from Receiving Speaker finds restarting to the received OPEN messages. If Receiving Speaker does not receive OPEN messages after exceed the time, it can delete SATLE route saved by neighbor.

		Default is 120s.
	graceful-restart stale-path-time	Configure stale-path-time for BGP GR. Specify the longest waiting time that delete stale route from the received OPEN messages to the received EOR for Receiving Speaker. Default is 360s.
	selection-deferral-time	Configure selection-deferral-time for BGP GR. Specify the longest waiting time that start to count selection route from the received OPEN messages to the received EOR for Restarting Speaker. If Restarting Speaker does not receive EOR after exceed the time, it can count selection route. Default is 120s.
Command Enabled	Enable Disable	

8.4.7.Timer Config

This page can be used for BGP Timer config.

Timer Config

AS Number	1000	
Keepalive Interval	60	(0-65535s, Default:60s)
Holdtime	240	(0-65535s, Default:240s)

[Apply](#)

AS Number	AS Number
Keepalive Interval	KEEPALIVE interval, default is 60s.
Holdtime	Hold Time, default is 240s.

8.4.8.View BGP Information

This page can be used for view BGP Information.

BGP Information

BGP Entries	Status
-------------	--------

[Status](#)
[BGP Neighbor](#)
[BGP Status Table](#)

BGP table version is 532, local router ID is 192.168.20.70
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
Network Next Hop Metric LocPrf Weight Path
*>i35.0.0.0 2.1.1.1 100 0 i
Total number of prefixes 1

BGP Entries	BGP Routing Messages	For displaying the routing messages permitted by BGP
	BGP Neighbor	Show neighbor information of specified BGP or total BGP processes

8.5.Routing Table

This page can be view for the basic status of routing table.

Routing Table

Routing-Table Entries
Status ▼

Routing Status Table

Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP

O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2

I - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area

* - candidate default

C 127.0.0.0/8 is directly connected, Loopback tag:0

C 192.168.2.0/24 is directly connected, Vlan1 tag:0

Total routes are : 2 Item(s)

Routing-Table Entries	Status; Database; Connect Route; RIP Route; Static Route; Statistics; OSPF Route; Kernel Route; FIB;
------------------------------	------------------------------------------------------------------------------------------------------------------------------

9.Multicast Manage

9.1.IGMP Snooping Config

9.1.1.Basic Config

Switch IGMP Snooping global switch, snooping IGMP messages

Basic Config

This page is used to configure the basic parameters of the IGMP SNOOPING function

Status

Disabled

VLAN ID

--Please select --

Apply

IGMP VLAN List

Showing 10 Entries

Showing 0 to 0 of 0 entries

Search

VLAN ID

Status

0 results found.

Delete

First Previous Next Last

Switch on-off IGMP Snooping	Enable	Turn on the global switch of IGMP Snooping on the switch
	Disable	Turn off the global switch of IGMP Snooping on the switch
VLAN ID	Created VLAN ID	

IGMP VLAN List

Showing 10 Entries

Showing 1 to 1 of 1 entries

Search

VLAN ID

Status

1

OPEN

Delete

First Previous 1 Next Last

Display the current existing VLAN interface and the running status of IGMP Snooping under the VLAN interface

9.1.2.Static Router Port

IGMP Snooping mrouter port parameter configuration.

Static Router Port Config

This page is used to configure static routing ports and corresponding aging time

VLAN ID

--Please select --

Static Router Port

--Please select --

Operation Type

Not Set

Alive Time

255

(1-65535,Default:255)

Apply

VLAN Based Static Routing Port List

Showing 10 Entries

Showing 1 to 1 of 1 entries

Search

VLAN ID

Static Router Port

Alive Time

1

255

First Previous 1 Next Last

VLAN ID	Created VLAN ID	
Mrouter port	Port name	
Mrouter port alive time	Time to live of the port, range: 1-65535	
Operation type	Apply	Add the mrouter port parameter configuration checked under the selected VLAN

VLAN Based Static Routing Port List		
Showing 10 ▾ Entries	Showing 1 to 1 of 1 entries	Search <input type="text"/>
VLAN ID	Static Router Port	Alive Time
1	1	255
First Previous 1 Next Last		

Display current configuration information

9.1.3.VLAN Config

Configure IGMP Snooping based on VLAN interface.

VLAN Config

This page is used to configure IGMP SNOOPING VLAN related parameters

VLAN ID	--Please select --		
Immediate leave	Enabled ▾		
L2-general-Querier	Enabled ▾		
Group number	50	(1-65535,Default:50)	
Source Table Number	40	(1-65535,Default:40)	

Apply

IGMP VLAN Configuration List				
Showing 10 ▾ Entries	Showing 1 to 1 of 1 entries			Search <input type="text"/>
VLAN ID	Immediate leave	L2-general-Querier	Group number	Source Table Number
1	Disable	Disable	50	40
First Previous 1 Next Last				

VLAN ID	Created VLAN ID	
Immediate leave configuration	IGMP fast leave function in VLAN	
L2-general-querier configuration	Used to send regular queries regularly to help switches in this network segment learn the mrouter port	
Group number	The upper limit of the total number of groups. When the number of joined groups reaches the limit, the newly joined groups will be rejected to prevent hostile attacks. The default is 50, and the range: 1-65535.	
Source table number	The maximum number of source entries in each group, including include sources and exclude sources. The default is 40, and the range: 1-65535.	
Operation	Configuration	Configure the checked parameters into the selected VLAN

Note: Whether it is to configure parameters or restore the default state, it is required to check the box at the back to take effect. The group number and the number of source table entries are unified functions, so the two function

parameters will take effect together (when one parameter is set, the other will be set to the default value).

IGMP VLAN Configuration List				
Showing 10 ▾ Entries	Showing 1 to 1 of 1 entries			Search <input type="text"/>
VLAN ID	Immediate leave	L2-general-Querier	Group number	Source Table Number
1	Disable	Disable	50	40
First Previous 1 Next Last				

Display the configuration parameters of the existing VLAN

9.1.4.Querier Config

IGMP Snooping query parameter configuration.

Querier Config

This page is used to configure query related parameters

VLAN ID	--Please select --	
Query-Interval	125	(1-65535,Default:125)
Query-Mrsp-Max	10	(1-25,Default:10)
Query-Robustness	2	(2-10,Default:2)
Suppression-Query-Time ?	255	(1-65535,Default:255)

Apply

Querier Configuration List

Showing 10 ▾ Entries	Showing 1 to 1 of 1 entries			Search <input type="text"/>
VLAN ID	Query-Interval	Query-Mrsp-Max	Query-Robustness	Suppression-Query-Time ?
1	125	10	2	
First Previous 1 Next Last				

VLAN ID	Created VLAN ID	
Query-Interval	IGMP Snooping query interval, range: 1-65535	
Query-mrsp configuration	Maximum response time for group query	
Query-robustness configuration	IGMP Snooping robustness, range: 2-10	
Suppression-query-time configuration	Prohibited query time, range: 1-65535	
Operation type	Apply	Add the mrouter port parameter configuration checked under the selected VLAN

Querier Configuration List				
Showing 10 ▾ Entries	Showing 1 to 1 of 1 entries			Search <input type="text"/>
VLAN ID	Query-Interval	Query-Mrsp-Max	Query-Robustness	Suppression-Query-Time ?
1	125	10	2	
First Previous 1 Next Last				

Display current configuration information

9.1.5.Multicast Table

The page displayed multicast table information.

Multicast Table

This page is used to view the multicast table

VLAN ID

VLAN0001

Apply

Multicast table

Showing 10 Entries

Showing 0 to 0 of 0 entries

Search

Number	Group IP	Member Port	Exptime	Source MAC	Version
0 results found.					

First Previous Next Last

9.2.MLD Snooping Config

9.2.1.Basic Config

Switch MLD Snooping global switch, MLD snooping messages

Basic Config

This page is used to configure the basic parameters of the MLD SNOOPING function

Status

Disabled

VLAN ID

--Please select --

Apply

MLD VLAN List

Showing 10 Entries

Showing 0 to 0 of 0 entries

Search

	VLAN ID	Status
0 results found.		

Delete

First Previous Next Last

Switch on-off IGMP Snooping	Enable	Turn on the global switch of IGMP Snooping on the switch
	Disable	Turn off the global switch of IGMP Snooping on the switch
VLAN ID	Created VLAN ID	

MLD VLAN List

Showing 10 Entries

Showing 1 to 1 of 1 entries

Search

	VLAN ID	Status
<input type="checkbox"/>	1	OPEN

Delete

First Previous 1 Next Last

Display the current existing VLAN interface and the running status of IGMP Snooping under the VLAN interface

9.2.2.Static Router Port

MLD Snooping mrouter port parameter configuration.

Static Router Port Config

This page is used to configure static routing ports and corresponding aging time

VLAN ID

--Please select --

Static Router Port

--Please select --

Operation Type

Not Set

Alive Time

255

(1-65535,Default:255)

Apply

VLAN Based Static Routing Port List

Showing 10 Entries

Showing 1 to 1 of 1 entries

Search

VLAN ID	Static Router Port	Alive Time
1		255

First Previous 1 Next Last

VLAN ID	Created VLAN ID	
Mrouter port	Port name	
Mrouter port alive time	Time to live of the port, range: 1-65535	
Operation type	Apply	Add the mrouter port parameter configuration checked under the selected VLAN

VLAN Based Static Routing Port List		
Showing 10 Entries	Showing 1 to 1 of 1 entries	Search
VLAN ID	Static Router Port	Alive Time
1	1	255
First Previous 1 Next Last		

Display current configuration information

9.2.3.VLAN Config

Configure MLD Snooping based on VLAN interface.

VLAN Config

This page is used to configure MLD SNOOPING VLAN related parameters

VLAN ID	--Please select --	
Immediate leave	Enabled	
L2-general-Querier	Enabled	
Group number	50	(1-65535,Default:50)
Source Table Number	40	(1-65535,Default:40)

Apply

MLD VLAN Configuration List				
Showing 10 Entries	Showing 1 to 1 of 1 entries	Search		
VLAN ID	Immediate leave	L2-general-Querier	Group number	Source Table Number
1	Disable	Disable	50	40
First Previous 1 Next Last				

VLAN ID	Created VLAN ID	
Immediate leave configuration	MLD fast leave function in VLAN	
L2-general-querier configuration	Used to send regular queries regularly to help switches in this network segment learn the mrouter port	
Group number	The upper limit of the total number of groups. When the number of joined groups reaches the limit, the newly joined groups will be rejected to prevent hostile attacks. The default is 50, and the range: 1-65535.	
Source table number	The maximum number of source entries in each group, including include sources and exclude sources. The default is 40, and the range: 1-65535.	
Operation	Configuration	Configure the checked parameters into the selected VLAN

Note: Whether it is to configure parameters or restore the default state, it is required to check the box at the back to take effect. The group number and the number of source table entries are unified functions, so the two function parameters will take effect together (when one parameter is set, the other will be set to the default value).

MLD VLAN Configuration List				
Showing	10	Entries	Showing 1 to 1 of 1 entries	Search
VLAN ID	Immediate leave	L2-general-Querier	Group number	Source Table Number
1	Disable	Disable	50	40
First Previous 1 Next Last				

Display the configuration parameters of the existing VLAN

9.2.4.Querier Config

MLD Snooping query parameter configuration.

Querier Config

This page is used to configure query related parameters

VLAN ID	--Please select --	
Query-Interval	125	(1-65535,Default:125)
Query-Mrsp-Max	10	(1-25,Default:10)
Query-Robustness	2	(2-10,Default:2)
Suppression-Query-Time	255	(1-65535,Default:255)

Apply

Querier Configuration List

Showing	10	Entries	Showing 1 to 1 of 1 entries	Search
VLAN ID	Query-Interval	Query-Mrsp-Max	Query-Robustness	Suppression-Query-Time
1	125	10	2	

[First](#)
[Previous](#)
[1](#)
[Next](#)
[Last](#)

VLAN ID	Created VLAN ID	
Query-Interval	MLD Snooping query interval, range: 1-65535	
Query-mrsp configuration	Maximum response time for group query	
Query-robustness configuration	MLD Snooping robustness, range: 2-10	
Suppression-query-time configuration	Prohibited query time, range: 1-65535	
Operation type	Apply	Add the mrouter port parameter configuration checked under the selected VLAN

Querier Configuration List				
Showing	10	Entries	Showing 1 to 1 of 1 entries	Search
VLAN ID	Query-Interval	Query-Mrsp-Max	Query-Robustness	Suppression-Query-Time
1	125	10	2	
First Previous 1 Next Last				

Display current configuration information

9.2.5.Multicast Table

The page displayed multicast table information.

Multicast Table

This page is used to view the multicast table

VLAN ID

VLAN0001

Apply

Multicast table

Showing	10	Entries	Showing 0 to 0 of 0 entries	Search
Number	Group IP	Member Port	Exptime	Version
0 results found.				

[First](#)
[Previous](#)
[Next](#)
[Last](#)

10.QoS Config

10.1.Port Config

10.1.1.Trust Config

Configure port trust rules

Trust Config

This page is used to set port trust configuration

Port	<input type="text" value="--Please select --"/>	
Trust Class	<div>COS</div>	
Operation Type	<div>Add</div>	

Apply

Port	Trust Class
Ethernet1/0/1	COS
Ethernet1/0/2	COS
Ethernet1/0/3	COS
Ethernet1/0/4	COS
Ethernet1/0/5	COS
Ethernet1/0/6	COS
Ethernet1/0/7	COS
Ethernet1/0/8	COS

Port	To configure the port name, click to expand the remaining ports	
Trust class	COS	Cos to int mapping based on intp field
	DSCP	Intp field based on dscp to intp mapping
Operation	add	Add a trust rule for the port
	Delete	Remove a trust rule for the port

10.1.2.Weight Config

Configure the port to process the priority of packets according to different queue scheduling algorithms

Weight Config

This page is used to set the port scheduling mode and queue weights

Scheduling Type	<div>sp</div>	
Port	<input type="text" value="--Please select --"/>	
Weight1	<div>1</div>	weight(0-127)
Weight2	<div>2</div>	weight(0-127)
Weight3	<div>3</div>	weight(0-127)
Weight4	<div>4</div>	weight(0-127)
Weight5	<div>5</div>	weight(0-127)
Weight6	<div>6</div>	weight(0-127)
Weight7	<div>7</div>	weight(0-127)
Weight8	<div>8</div>	weight(0-127)

Apply

Port	To configure the port name, click to expand the remaining ports	
Queue schedule algorithm	sp	Strict queuing priority, packet transmission in order of priority.
	wrr	Weighted round-robin scheduling. Rotate scheduling between queues to ensure that each queue gets a certain amount of service time
	wddr	Weighted difference round-robin scheduling, based on message length transmission, based on the combined effect of weight and K value to generate the length of transmission in the message queue

Configure the weight value of the eight queues of each port, and allocate the number of packets according to the weight value

Weight Config

This page is used to set the port scheduling mode and queue weights

Scheduling Type	wrr	
Port	--Please select --	
Weight1	1	weight(0-127)
Weight2	2	weight(0-127)
Weight3	3	weight(0-127)
Weight4	4	weight(0-127)
Weight5	5	weight(0-127)
Weight6	6	weight(0-127)
Weight7	7	weight(0-127)
Weight8	8	weight(0-127)

Apply

Port	To configure the port name, click to expand the remaining ports	
Weight1	The weight value of queue 1, the range is 0-127	
Weight2	The weight value of queue 2, the range is 0-127	
Weight3	The weight value of queue 3, the range is 0-127	
Weight4	The weight value of queue 4, the range is 0-127	
Weight5	The weight value of queue 5, the range is 0-127	
Weight6	The weight value of queue 6, the range is 0-127	
Weight7	The weight value of queue 7, the range is 0-127	
Weight8	The weight value of queue 8, the range is 0-127	
Operation	Apply	Add the weight of each queue to the port, and fill in all the weights of each queue before adding

Port	Queue Weight
Ethernet1/0/1	1 2 3 4 5 6 7 8
Ethernet1/0/2	1 2 3 4 5 6 7 8
Ethernet1/0/3	1 2 3 4 5 6 7 8
Ethernet1/0/4	1 2 3 4 5 6 7 8
Ethernet1/0/5	1 2 3 4 5 6 7 8
Ethernet1/0/6	1 2 3 4 5 6 7 8
Ethernet1/0/7	1 2 3 4 5 6 7 8
Ethernet1/0/8	1 2 3 4 5 6 7 8
Ethernet1/0/9	1 2 3 4 5 6 7 8
Ethernet1/0/10	1 2 3 4 5 6 7 8

Information feedback window

Configure the weight value of the eight queues of each port, transmit based on the length of the message, and generate the transmission length in the message queue based on the combined action of the weight and the K value

Weight Config

This page is used to set the port scheduling mode and queue weights

Scheduling Type	wdrr	
Port	--Please select --	
Weight1	1	weight(0-127)
Weight2	2	weight(0-127)
Weight3	4	weight(0-127)
Weight4	8	weight(0-127)
Weight5	16	weight(0-127)
Weight6	32	weight(0-127)
Weight7	64	weight(0-127)
Weight8	64	weight(0-127)

Apply

Port	To configure the port name, click to expand the remaining ports	
Weight1	The weight value of queue 1, the range is 0-32767	
Weight2	The weight value of queue 2, the range is 0-32767	
Weight3	The weight value of queue 4, the range is 0-32767	
Weight4	The weight value of queue 8, the range is 0-32767	
Weight5	The weight value of queue 16, the range is 0-32767	
Weight6	The weight value of queue 32, the range is 0-32767	
Weight7	The weight value of queue 64, the range is 0-32767	
Weight8	The weight value of queue 64, the range is 0-32767	
Operation	Apply	Add the weight of each queue to the port, and fill in all the weights of each queue before adding

Port	Queue Weight
Ethernet1/0/1	1 2 4 8 16 32 64 64
Ethernet1/0/2	1 2 4 8 16 32 64 64
Ethernet1/0/3	1 2 4 8 16 32 64 64
Ethernet1/0/4	1 2 4 8 16 32 64 64
Ethernet1/0/5	1 2 4 8 16 32 64 64
Ethernet1/0/6	1 2 4 8 16 32 64 64
Ethernet1/0/7	1 2 4 8 16 32 64 64
Ethernet1/0/8	1 2 4 8 16 32 64 64
Ethernet1/0/9	1 2 4 8 16 32 64 64
Ethernet1/0/10	1 2 4 8 16 32 64 64

Information feedback window

10.1.3.CoS-To-IntP Config

Configure the value mapped from the COS value to the internal priority (queue).

CoS-To-IntP Map

This page is used to set the mapping relationship between COS and internal priority

CoS	0	1	2	3	4	5	6	7
IntP	0	1	2	3	4	5	6	7

Apply

CoS value	The COS value carried in the message or the default COS value assigned when entering	
IntP value	The value of the internal priority (queue) to which the COS value will be mapped	
Operation type	Configuration	Configure the value of COS to IntP

Display the execution process and the current mapping relationship

10.1.4.DSCP-To-IntP Config

Configure the value mapped from the DSCP value to the IntP value.

DSCP-To-IntP Map

This page is used to set the mapping relationship between DSCP and internal priority

DSCP	--Please select --
IntP	0

Apply

DSCP value1-DSCP value8(optional)	Up to eight DSCP values can be configured to the new IntP value, among which DSCP value1 is required, DSCP value2-8 is optional, range: 0-63	
IntP value	New IntP value, range: 0-7	
Operation type	Apply	Configure DSCP to IntP value

DSCP	Internal Priority	DSCP	Internal Priority	DSCP	Internal Priority	DSCP	Internal Priority
0	0	16	2	32	4	48	6
1	0	17	2	33	4	49	6
2	0	18	2	34	4	50	6
3	0	19	2	35	4	51	6
4	0	20	2	36	4	52	6
5	0	21	2	37	4	53	6
6	0	22	2	38	4	54	6
7	0	23	2	39	4	55	6
8	1	24	3	40	5	56	7
9	1	25	3	41	5	57	7
10	1	26	3	42	5	58	7
11	1	27	3	43	5	59	7
12	1	28	3	44	5	60	7
13	1	29	3	45	5	61	7
14	1	30	3	46	5	62	7
15	1	31	3	47	5	63	7

Shows the execution process and the current mapping relationship. The vertical d1 represents the tens digit of DSCP, and the horizontal d2 represents the single digit of DSCP. The value of the intersection of the two is the mapping value.

10.1.5.Policy Config

Configure the port's policy table, and the port will process packets according to the rules of the classification table in the policy table.

Policy Config

This page is used to set policy configuration on the port

Port

--Please select --

Policy-Map Name

Operation Type

Add

Apply

Port	Policy-Map Name
Ethernet1/0/1	none
Ethernet1/0/2	none
Ethernet1/0/3	none
Ethernet1/0/4	none
Ethernet1/0/5	none
Ethernet1/0/6	none
Ethernet1/0/7	none
Ethernet1/0/8	none

Port	To configure the port name, click to expand the remaining ports	
Policy map name	The name of the policy table, added by the policy table configuration	
Operation	Add	policy for adding ports
	Delete	Delete port policy

10.2.Class-Map Config

10.2.1.Class-Map Config

Create and delete classification tables, view the currently configured classification tables

Class-Map Config

This page is used to set class map entries

Class-Map Name

Length(1-64)

Apply

Class-Map List

Showing 10 Entries

Showing 0 to 0 of 0 entries

Search

Entries	Class-Map Name
0 results found.	

Delete

FirstPreviousNextLast

Class-map name	Class-map name, range:1-64 character	
Operation	Add	Add Class-map
	Delete	Remove Class-map

Class-Map List

Showing 10 Entries
Showing 1 to 1 of 1 entries
Search

	Entries	Class-Map Name
<input type="checkbox"/>	1	1

Delete

First
Previous
1
Next
Last

Display the currently created class-map name

10.2.2.Class-Map Rule Config

Set the rules and corresponding parameters for classification matching

Class-Map Rule Config

This page is used to set the matching rules for class map

Class-Map Name	1	
Match Rule	Access Group	
ACL list name		Length(1-64)
Operation Type	Add	

Apply

Classification criteria rule	accesss-group	Match the specified IP ACL, MAC ACL or IPv6 standard ACL or MAC-IP ACL
Class-map name	The name of the created class-matching table, select by clicking the drop-down	
ACL list name	Created ACL name, 1-64 characters	
Operation	Add	Add matching rules
	Del	Remove matching rules

Class-Map Rule Config

This page is used to set the matching rules for class map

Class-Map Name	1	
Match Rule	IP DSCP	
IP DSCP 0		Length(0-63)
IP DSCP 1		Length(0-63)
IP DSCP 2		Length(0-63)
IP DSCP 3		Length(0-63)
IP DSCP 4		Length(0-63)
IP DSCP 5		Length(0-63)
IP DSCP 6		Length(0-63)
IP DSCP 7		Length(0-63)
Operation Type	Add	

Apply

Classification criteria rule	ip dscp	Match the specified DSCP value, this parameter is the DSCP list
Class-map name	The name of the created class-matching table, select by clicking the drop-down	
IP dscp0-7	One or more DSCP values can be set, up to 8 DSCP values can be set, the range is 0~63;	
Operation	Add	Add matching rules
	Del	Remove matching rules

Class-Map Rule Config

This page is used to set the matching rules for class map

Class-Map Name	1	▼
Match Rule	IP Precedence	▼
IP Precedence0		Length(0-7)
IP Precedence1		Length(0-7)
IP Precedence2		Length(0-7)
IP Precedence3		Length(0-7)
IP Precedence4		Length(0-7)
IP Precedence5		Length(0-7)
IP Precedence6		Length(0-7)
IP Precedence7		Length(0-7)
Operation Type	Add	▼

Apply

Classification criteria rule	ip precedence	Match the specified ip priority, this parameter is the IP priority list
Class-map name	The name of the created class-matching table, select by clicking the drop-down	
IP precedence0-7	One or more ip priority values can be set, the list contains up to 8 IP priority values, and the valid range is 0~7;	
Operation	Add	Add matching rules
	Del	Remove matching rules

Class-Map Rule Config

This page is used to set the matching rules for class map

Class-Map Name	1	▼
Match Rule	VLAN	▼
VLAN 0		Length(1-4094)
VLAN 1		Length(1-4094)
VLAN 2		Length(1-4094)
VLAN 3		Length(1-4094)
VLAN 4		Length(1-4094)
VLAN 5		Length(1-4094)
VLAN 6		Length(1-4094)
VLAN 7		Length(1-4094)
Operation Type	Add	▼

Apply

Classification criteria rule	vlan	Match the specified vlan, this parameter is a list of vlan id
Class-map name	The name of the created class-matching table, select by clicking the drop-down	
Vlan0-7	One or more VLAN IDs can be set, including 8 VLAN IDs at most, ranging from 1 to 4094	
Operation	Add	Add matching rules
	Del	Remove matching rules

Class-Map Rule Config

This page is used to set the matching rules for class map

Class-Map Name	1	▼
Match Rule	COS	▼
COS 0		Length(0-7)
COS 1		Length(0-7)
COS 2		Length(0-7)
COS 3		Length(0-7)
COS 4		Length(0-7)
COS 5		Length(0-7)
COS 6		Length(0-7)
COS 7		Length(0-7)
Operation Type	Add	▼

Apply

Classification criteria rule	cos	Match the specified CoS value, this parameter is a list of vlan id
Class-map name	The name of the created class-matching table, select by clicking the drop-down	
Cos 0-7	One or more cos values can be set, the parameter is a CoS list composed of up to 8 CoS, the range is 0~7;	
Operation	Add	Add matching rules
	Del	Remove matching rules

Class-Map Rule Config

This page is used to set the matching rules for class map

Class-Map Name	1	▼
Match Rule	IPv6 DSCP	▼
IPv6 DSCP 0		Length(0-63)
IPv6 DSCP 1		Length(0-63)
IPv6 DSCP 2		Length(0-63)
IPv6 DSCP 3		Length(0-63)
IPv6 DSCP 4		Length(0-63)
IPv6 DSCP 5		Length(0-63)
IPv6 DSCP 6		Length(0-63)
IPv6 DSCP 7		Length(0-63)
Operation Type	Add	▼

Apply

Classification criteria rule	ipv6 dscp	Match the specified ipv6 DSCP value, this parameter is the ipv6 DSCP list
Class-map name	The name of the created class-matching table, select by clicking the drop-down	
IPv6 dscp0-7	One or more ipv6 DSCP values can be set, up to 8 DSCP values can be set, the range is 0~63;	
Operation	Add	Add matching rules
	Del	Remove matching rules

Class-Map Rule Config

This page is used to set the matching rules for class map

Class-Map Name	1	
Match Rule	IPv6 Flowlabel	
IPv6 Flowlabel 0		Length(0-1048575)
IPv6 Flowlabel 1		Length(0-1048575)
IPv6 Flowlabel 2		Length(0-1048575)
IPv6 Flowlabel 3		Length(0-1048575)
IPv6 Flowlabel 4		Length(0-1048575)
IPv6 Flowlabel 5		Length(0-1048575)
IPv6 Flowlabel 6		Length(0-1048575)
IPv6 Flowlabel 7		Length(0-1048575)
Operation Type	Add	

Apply

Classification criteria rule	ipv6 flowlabel	Match the specified IPv6 flow label, this parameter is the value of the IPv6 flow label DSCP list
Class-map name	The name of the created class-matching table, select by clicking the drop-down	
IPv6 flowlabel0-7	One or more IPv6 flowlabel values can be set, ranging from 0 to 1048575;	
Operation	Add	Add matching rules
	Remove	Remove matching rules

Class-Map matching rule table

Showing

10

 Entries

Showing 1 to 1 of 1 entries

Search

Class-Map Name	ACL list name	VLAN	COS	IP DSCP	IP Precedence	IPv6 DSCP	IPv6 Flowlabel
1	none	none	none	none	none	none	none

First

Previous

1

Next

Last

First Previous 1 Next Last

10.3.Policy-Map Config

10.3.1.Policy Name Config

Create and delete policy tables, and collaborate with classification tables to create packet in and out rules

Policy Name Config

This page is used to set policy map entries

Policy-Map Name		Length(1-64)
-----------------	--	--------------

Apply

Policy-map name	Policy-map name, range:1-64 character	
Operation	Apply	Add policy-map
	Delete	Remove policy-map

Policy-Map List

Showing 10 ▾ Entries Showing 1 to 1 of 1 entries Search

Entries	Policy-Map Name
1	1

Delete

First Previous 1 Next Last

Display the currently created policy-map.

10.3.2.Policy Class Config

Apply the class-map to the policy-map.

Policy Class Config

This page is used to set policy classification rules

Policy-Map Name	1 ▾
Class-Map Name	1 ▾
Inserted Before The Class-Map Name	1 ▾

Apply

policy-map name	The name of the created policy-map	
class-map name	The name of the classification table created by the classification matching table, this table will be applied to the policy -map	
Inserted before the class-map name	Prior to the insertion of the classification matching table, the name of the classification table that has been applied to the strategy table, and the priority of the newly applied classification matching table is increased	
Operation	Add	Add an association between the strategy table and the classification table

Policy-Map-Class List

Showing 10 ▾ Entries Showing 1 to 1 of 1 entries Search

Policy-Map Name	Class-Map Name
1	1

Delete

First Previous 1 Next Last

Display the association between the created policy table and the classification matching table

10.3.3.Policy Mark Config

Configure the priority of packets in the policy mapping configuration mode.

Assign a new DSCP and IP priority to the classified traffic. Only the classified traffic that meets the matching criteria will be assigned a new value.

Policy Mark Config

This page is used to set policy tags

Policy-Map Name	1 ▾
Class-Map Name	1 ▾
Mark Type	COS ▾
COS	<input type="text"/> Length(0-7)
Operation Type	Add ▾

Apply

Classification criteria rule	ip dscp	Set the DSCP value again according to the rules defined in the policy-map and class-map
	ip precedence	Set the IP priority again according to the rules defined in the policy-map and class-map
	drop-precedence	Set the discarding priority again according to the rules defined in the policy-map and class-map
	internal-priority	Set the internal priority again according to the rules defined by the policy-map and class-map
	cos	Set the COS value again according to the rules defined by the policy table and the classification matching table
Policy-map name	The name of the created policy table	
Class-map name	Created classification match table	
DSCP	DSCP value, range: 0-63	
Precedence	IP priority, range:0-7	
Drop-precedence	drop priority, range: 0-2	
Internal-priority	internal priority, range: 0-7	
COS	COS value, range: 0-7	
Operation	Add	Add the priority and queue value associated with the strategy table and the classification matching table
	Delete	Remove the priority and queue value associated with the strategy table and the classification matching table

Policy Mark List						
Showing 10 Entries	Showing 1 to 1 of 1 entries			Search		
Policy-Map Name	Class-Map Name	COS	IP DSCP	IP Precedence	Internal Priority	Drop Precedence
1	1	0	none	none	none	none
First Previous 1 Next Last						

10.3.4.Policy Bandwidth

Configure the new aggregation strategy and the information rate and burst id of the aggregation strategy.

Policy Bandwidth

This page is used to set policy bandwidth configuration

Burst ID1	1024	Length(1-8192)
Burst ID2	1024	Length(1-8192)

Apply

Policy-Map Name	1	
Class-Map Name	1	
Burst ID	1	
Bandwidth Rate		Length(1-10000000)
Operation Type	Add	

Apply

Aggregate policer name	New aggregate policer name, range: 1-64 character.	
Committed Information Rate	Information Rate, range: 1-10000000kbit/s	
Policy burst id configuration	Burst id configuration, range: 1-2	
Operation	Add	Add aggregate policer
	Remove	Remove aggregate policer

Policy Bandwidth List

Showing 10 Entries

Showing 0 to 0 of 0 entries

Search

Policy-Map Name	Class-Map Name	Burst ID(Kbps)	Bandwidth Rate
0 results found.			
			<div>FirstPreviousNextLast</div>

10.3.5.Policy VLAN

Configure VLAN Association Policy.

Policy VLAN

This page is used to set policy configurations on VLANs

Policy-Map Name	1	
Vlan List		(1-100)characters
Operation Type	Add	

Apply

Policy-map name	The name of the created strategy, select by clicking the drop-down	
VLAN List	VLAN ID, range: 1-4094	
Operation	Add	Add VLAN-based policy
	Remove	Remove VLAN-based policy

VLAN Policy List

Showing 10 Entries

Showing 0 to 0 of 0 entries

Search

VLAN ID	Policy-Map Name
0 results found.	
<div>FirstPreviousNextLast</div>	