User Guide

24*1000Mbps SFP+4*10G SFP Fiber Managed Switch

Table of Content

Package Contents

Check the following contents of your package:

- Fiber Switch x 1
- User Manual x 1
- Power Cord x 1
- Accessories(Rack Mount Accessory Kit x2, Rubber Feet x4, Screws)

If any part is lost and damaged, please contact your local agent immediately.

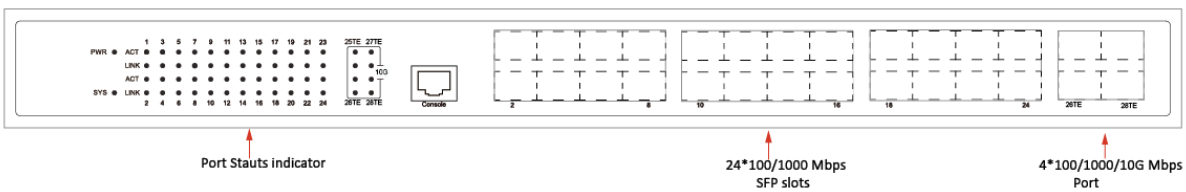
1. Introduction

The product provides 24*1000Mbps SFP Slot and 4 *10G SFP Slots ，powerful and flexible enough for users to deploy wireless access points or IP-based network surveillance cameras. The switch also comes equipped with 4*10G SFP+ slots, expanding your network flexibly. In addition, it provides high performance, enterprise-level QoS, advanced security strategies and rich layer 3 management features. With all these advanced features, the Switch is an ideal choice for WIFI coverage, Internet cafes, computer rooms, and so on.

2. Hardware Description

2.1 Front Panel

The front panel includes a 24-port Gigabit SFP+ 4-port 10GE+ 1-port console-managed PoE switch. The LED indicator is also located on the panel.



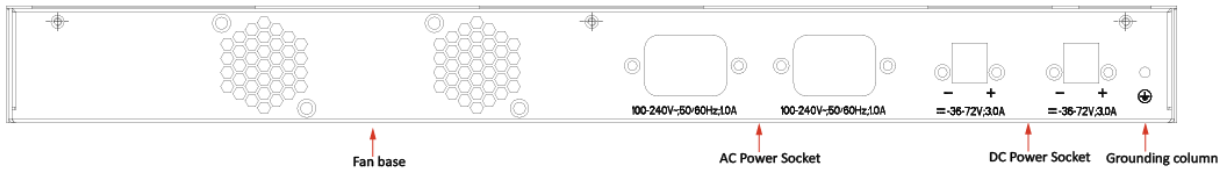
LED indicator

LED	Color	Function
PWR	Green	Off: No Power supply Light: Indicates the switch has power
LNK/ACT	Green	Off: No device is connected to the corresponding port Light: Indicates the link through that port is successfully established. Blink: Indicates that the Switch is actively sending or receiving data over that port.

SYS	Green	Blinking: the system works Out: the system is starting or has no power

2.2 Rear Panel

The rear panel shows the DC / AC inlet power outlet, fan, and grounding post.



Power socket
Connect the female connector of the power cord here, and the male connector to the AC(Alternating Current) power outlet. Please make sure the voltage of the power supply meets the requirement of the input voltage.

Grounding column
The switch already comes with lightning protection mechanism. You can also ground the switch through the PE (Protecting Earth) cable of AC cord or with Ground Cable.

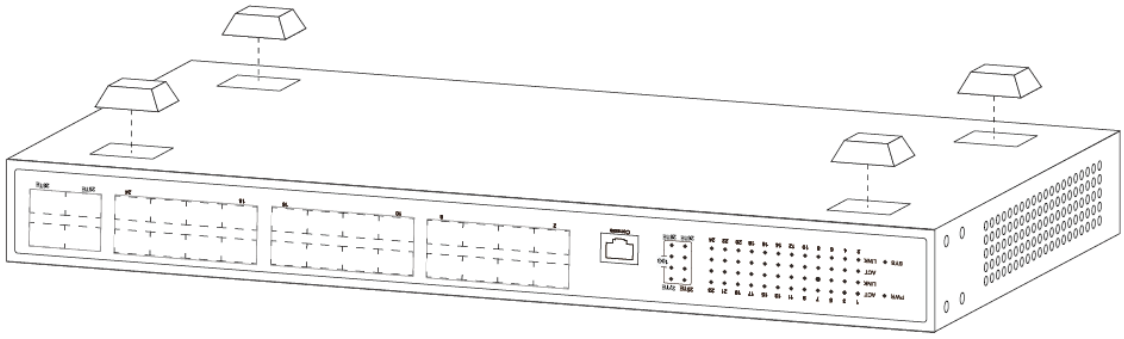
3. Installation the Switch

This part describes how to install your Fiber Switch and make connections to it. Please follow the following instructions in avoid of incorrect installation causing device damage and security threat.

- Before cleaning the switch, unplug the power plug of the switch first. Do not clean the switch with wet cloth or liquid;
- Do not place the switch near water or any damp area. Prevent water or moisture from entering the switch chassis;
- Do not place the switch on an unstable case or desk. The switch might be damaged severely in case of a fall;
- Ensure proper ventilation of the equipment room and keep the ventilation vents of the switch free of obstruction;
- Make sure that the operating voltage is the same one labeled on the switch;
- Do not open the chassis while the switch is operating or when electrical hazards are present to avoid electrical shocks.

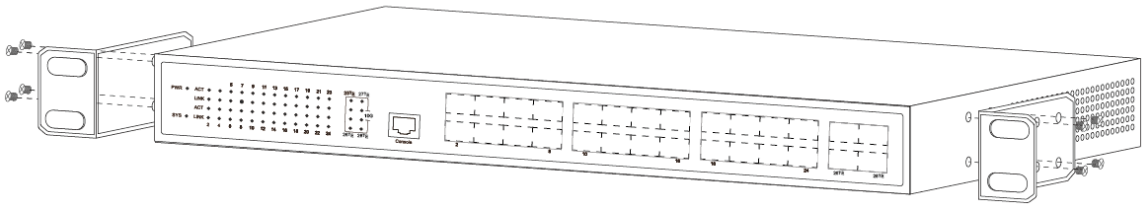
3.1 Desktop Installation

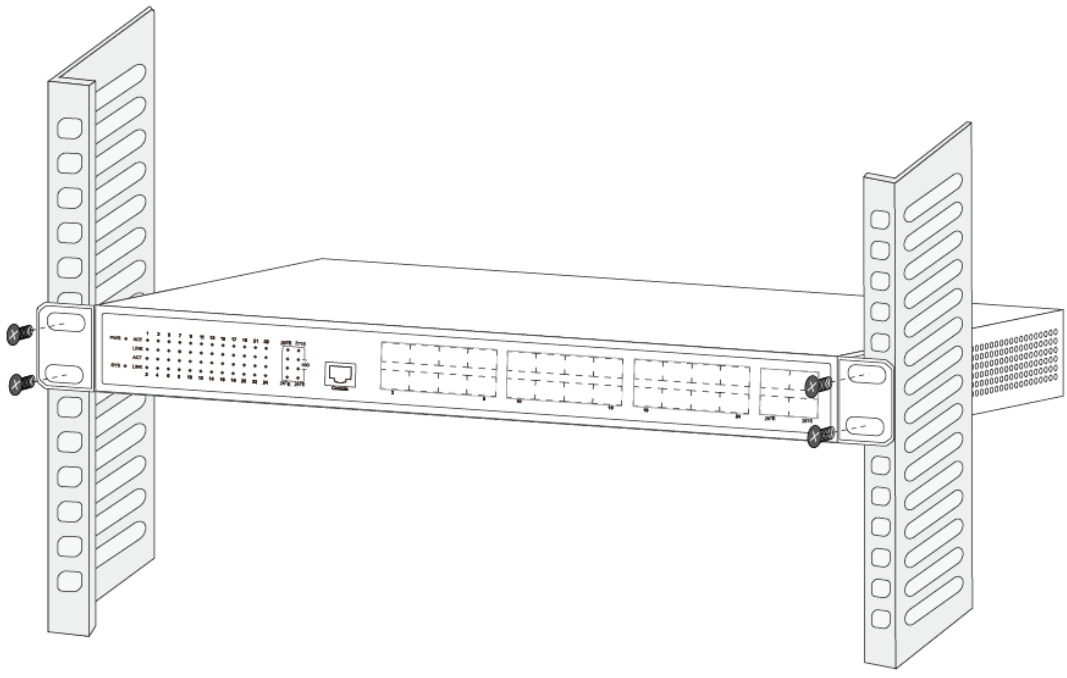
Install the Switch on a desktop, please attach these cushioning rubber feet provided on the bottom at each corner of the Switch in case of the external vibration. Allow adequate space for ventilation between the device and the objects around it.



3.2 Rack Installation

Check EIA-19inch machine Cabinet of grounding and stability, first, with screws will installation hanging ear fixed in switch front Panel sides will switch placed in machine Cabinet of a bracket, along machine Cabinet guide slot Mobile switch to right location, then, with screws will installation hanging ear fixed in machine Cabinet ends of fixed guide slot, ensure switch stable to installation in machine Cabinet slot bit of bracket. Equipment mounting brackets are not used for load-bearing, it only plays the regular role. When installing the equipment cabinet, box bottom bracket (fixed on the Cabinet) to support the device.



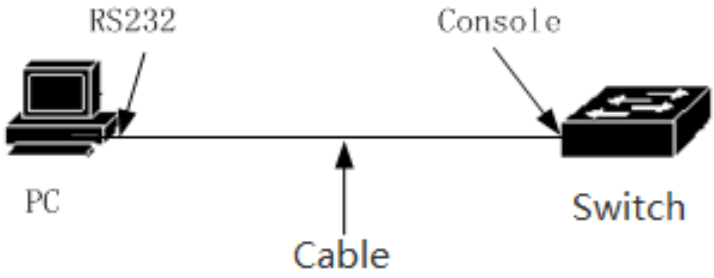


3.3 Turn on the switch

The PoE switch can be used with DC power supply. Powering on the switch, it will automatically initialize and its LED indicators will respond as follows:
1) Firstly, the Power LED indicator will light up.
2) Then, the data LED indicators will flash momentarily for 15~25 second, which represents a resetting of the system.

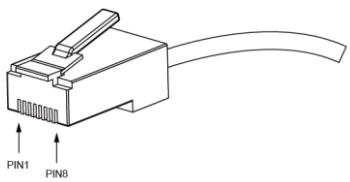
3.4 Connection Interface

3.4.1 Connection The monitor port has a monitor port (Console port), this section describes the characteristics of this monitoring port and how to use it.
First step: Rate 115200bps, standard RJ45 plug. Use a dedicated monitoring cable to lead the port to the PC serial port connection, as follows:



The second step to start the terminal emulation software on the PC (such as: Windows HyperTerminal) can be configured for the switch, monitoring and other operations. The cable is supplied with the host. The terminal serial port communication parameters can be set as right: rate -115200bps, eight bits data bit, one stop bit, no parity bit, no flow control. The communication parameters of HyperTerminal are configured 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.



Console Port PIN Definition:

Pin number	English name	Jane note
One	RTS	No connect
Two	DTR	No connect
Three	TXD	Output
Four	GND	GND
Five	GND	GND
Six	RXD	Input
Seven	DSR	No connect
Eight	CTS	No connect

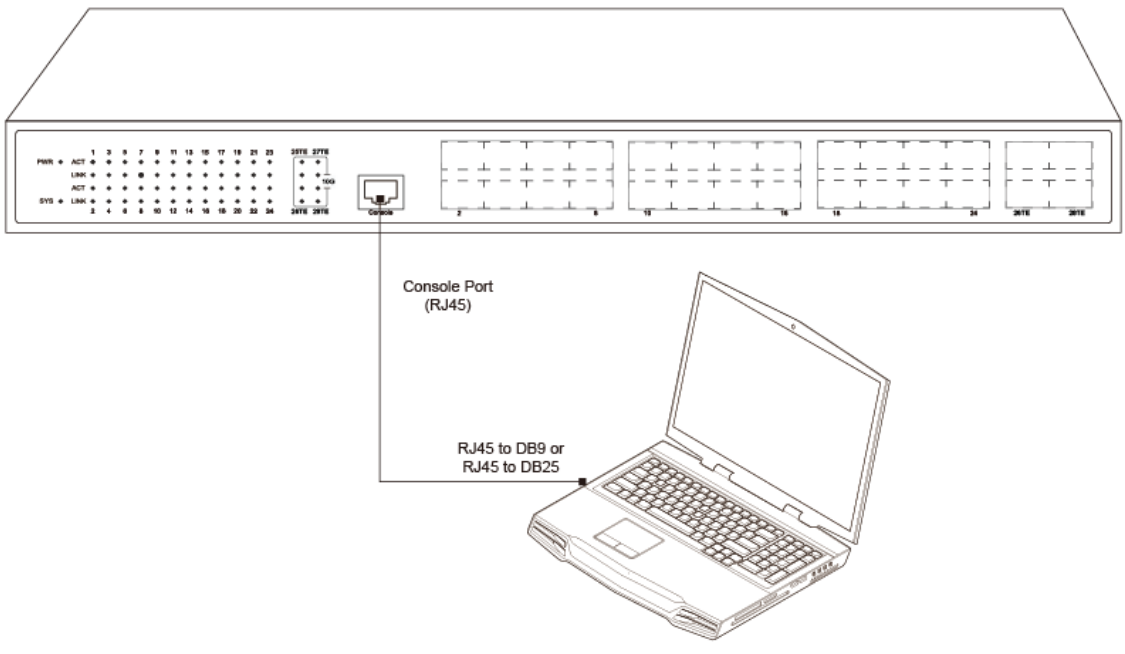
NOTE: The switch console port does not support the flow control function, so when the switch is configured with HyperTerminal, the data flow control should be set to "none", otherwise the problem of HyperTerminal single pass will occur. This cable is used to connect the console port of the switch to 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.

NOTE：
Enter "?" in the console Port command line interface Command action tips to see what features are available in pre-mode

4. How to Login the Switch

4.1 Switch to End Node

Use standard Cat.5/5e Ethernet cable (UTP/STP) to connect the Switch to end nodes as described below. The Managed Switch ports will automatically adjust to the characteristics (MDI/MDI-X, speed, duplex) of the device to which is connected.



Please refer to the LED Indicator Specification. The Link/Act LED for each port lights green when the link is available.

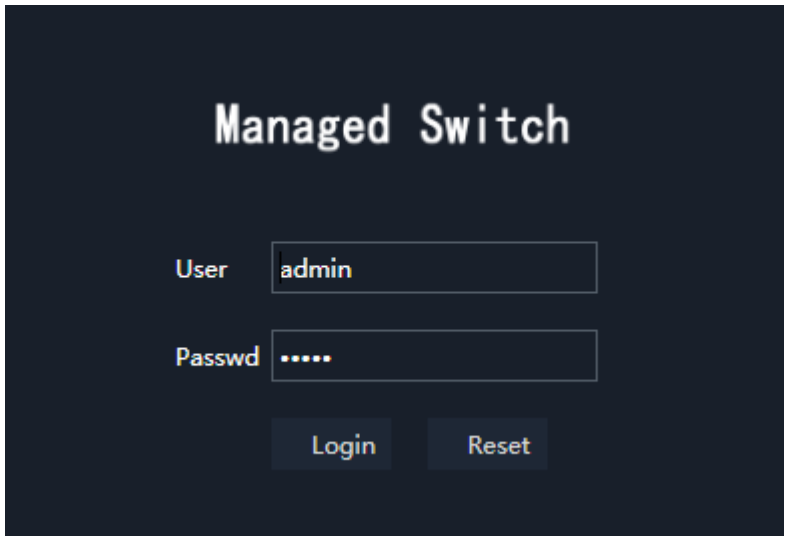
4.2 Logging on the Switch

As the Managed Switch provides Web-based management login, you can configure your computer's IP address manually to log on to the Managed Switch. The default settings of the Managed Switch are shown below.

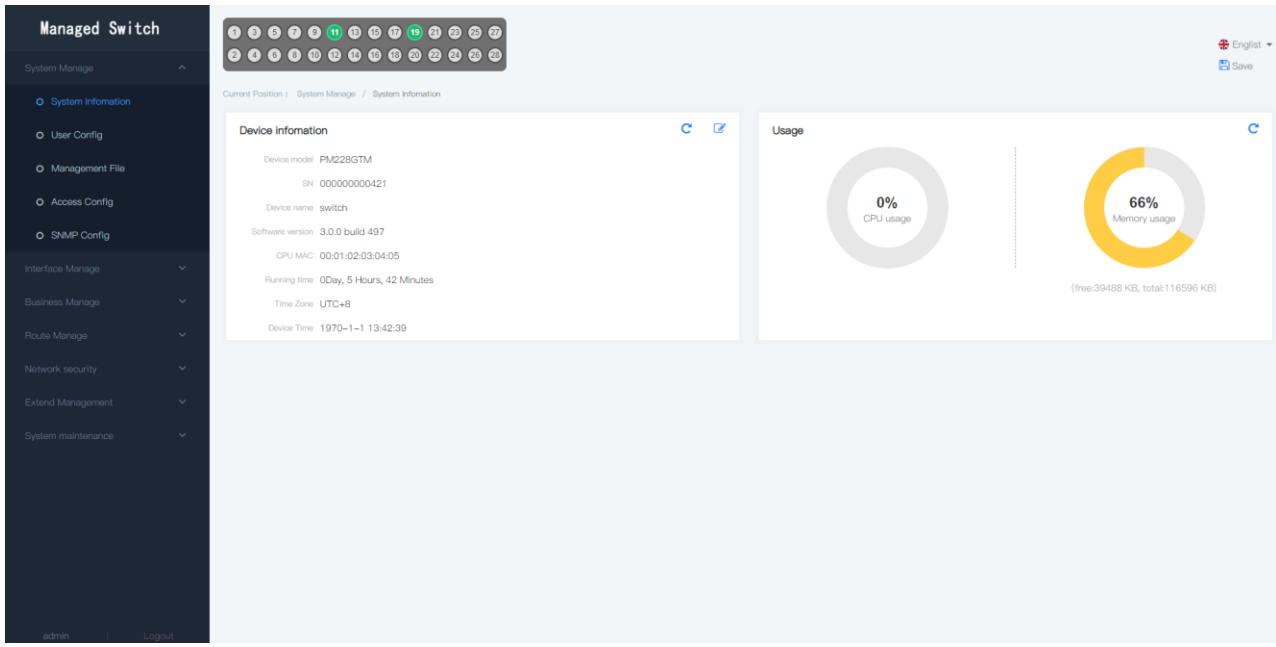
Parameter	Default Value
Default IP address	192.168.2.1
Default user name	admin
Default password	admin

You can log on to the welcome window of the Managed Switch through following steps:

1. Connect the Managed Switch with the computer NIC interface.
2. Power on the Managed Switch.
3. Check whether the IP address of the computer is within this network segment: 192.168.2.xxx ("xxx" ranges 0~255), for example, 192.168.2.100.
4. Open the browser, and enter http://192.168.2.254 and then press "Enter". The Managed Switch login window appears, as shown below.



5. Enter the user name and password (The factory default login username and password is admin), and then click "Login" to log in to the Switch configuration window as below.

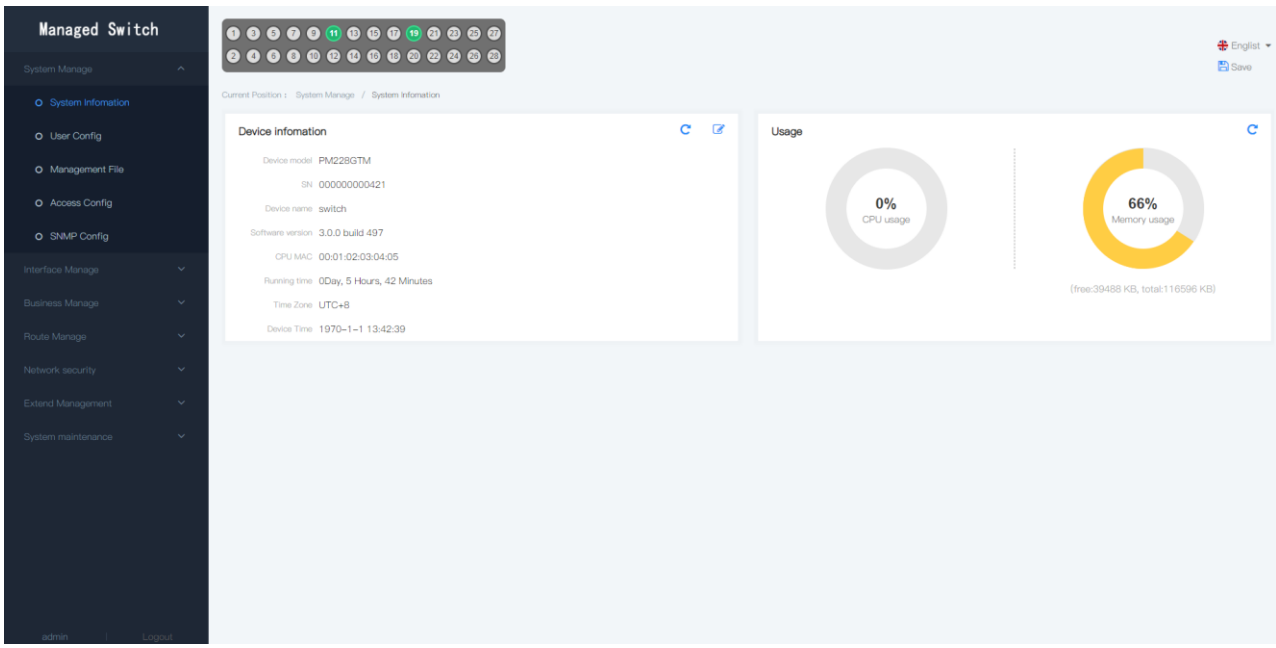


5. Management the Switch

5.1 System Manage

5.1.1 System Information

The page is used not only to display information about the device, but also to modify the device name, time zone and device time by clicking " " icon. Click " " to refresh the information.



Note: device name fields can accept "Aa~Zz", "0-9", "_", "-", "=", but do not include special characters.

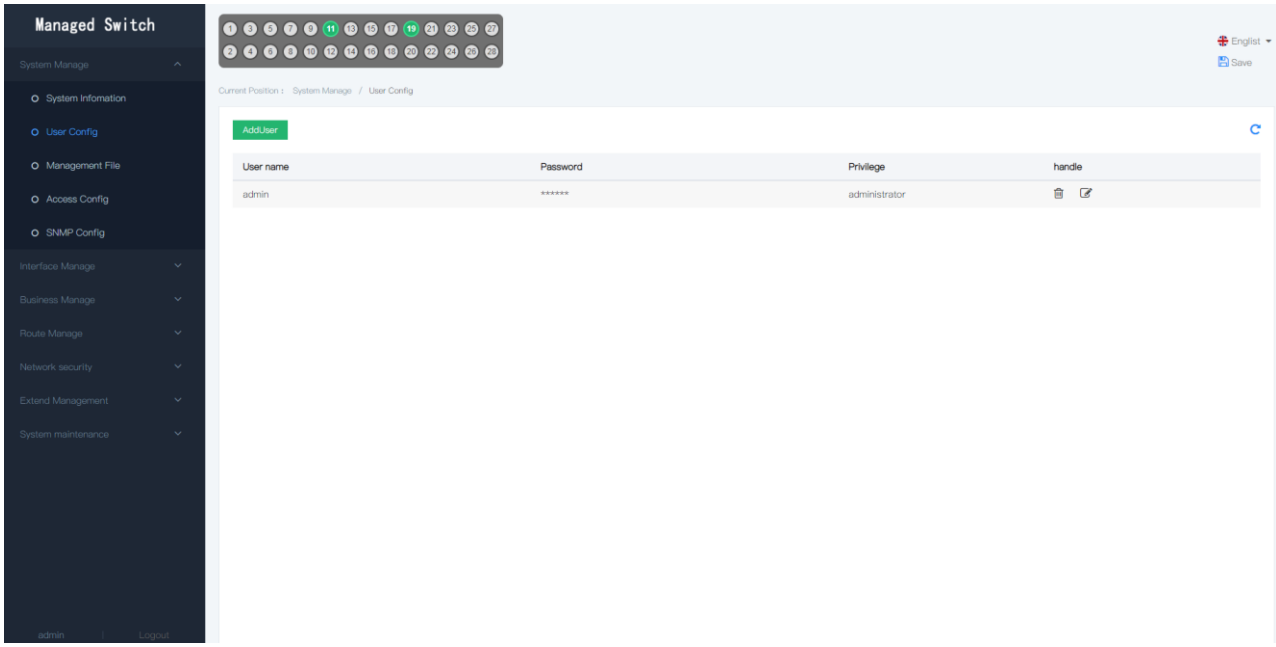
5.1.2 User Config

This page is used to display the name, password, and privilege of all current users.

AddUser: Add a new user

: Delete the user of this row

: Modify the user name, password, privilege of this row

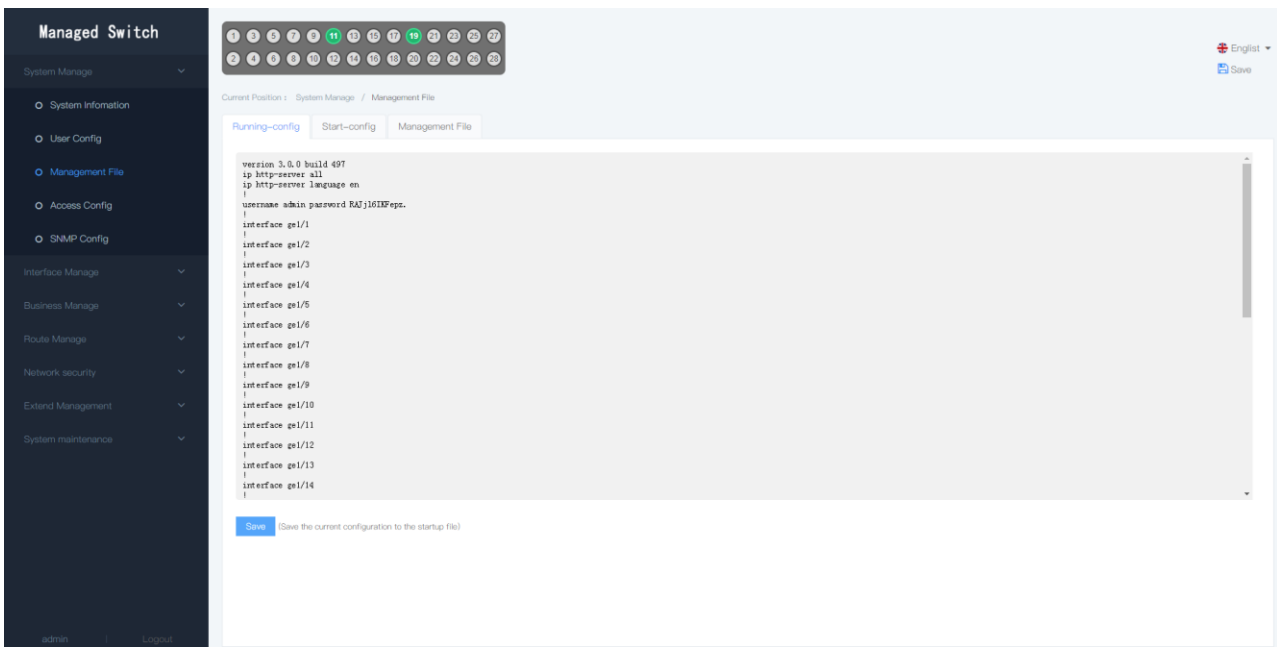


5.1.3 Management File

This page is used to view running configuration, start configuration, and management file.

RUNNING-CONFIG

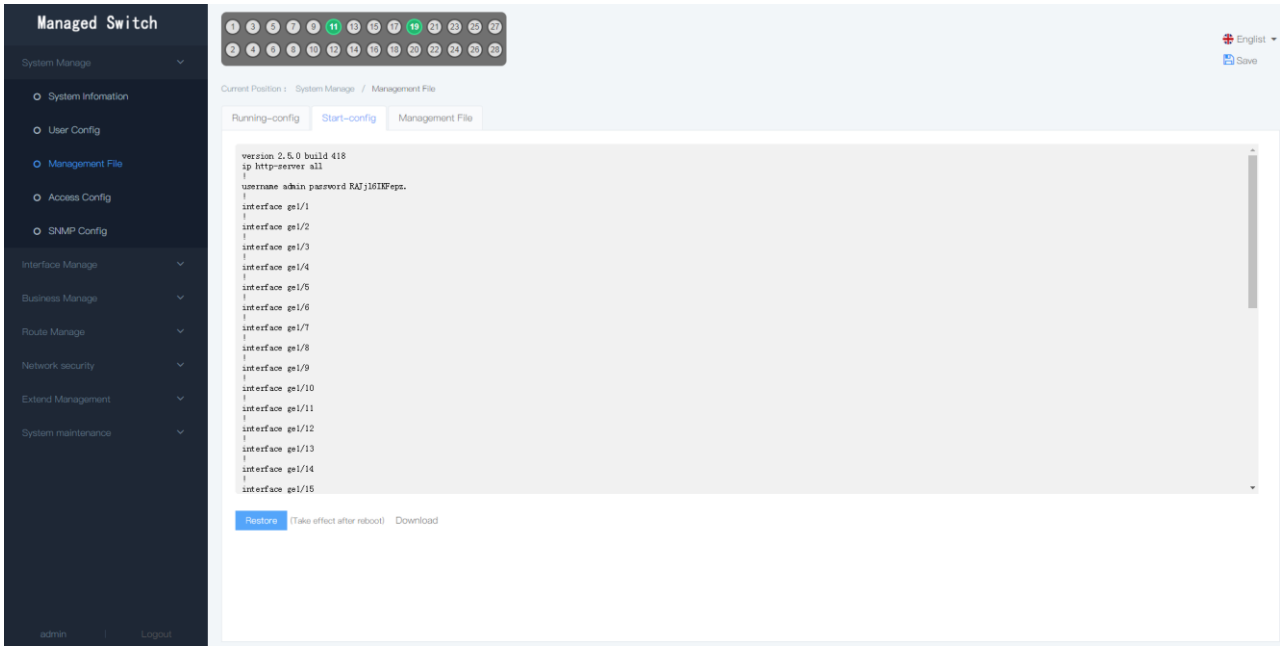
Display the device's current running state configuration



THE START CONFIGURATION

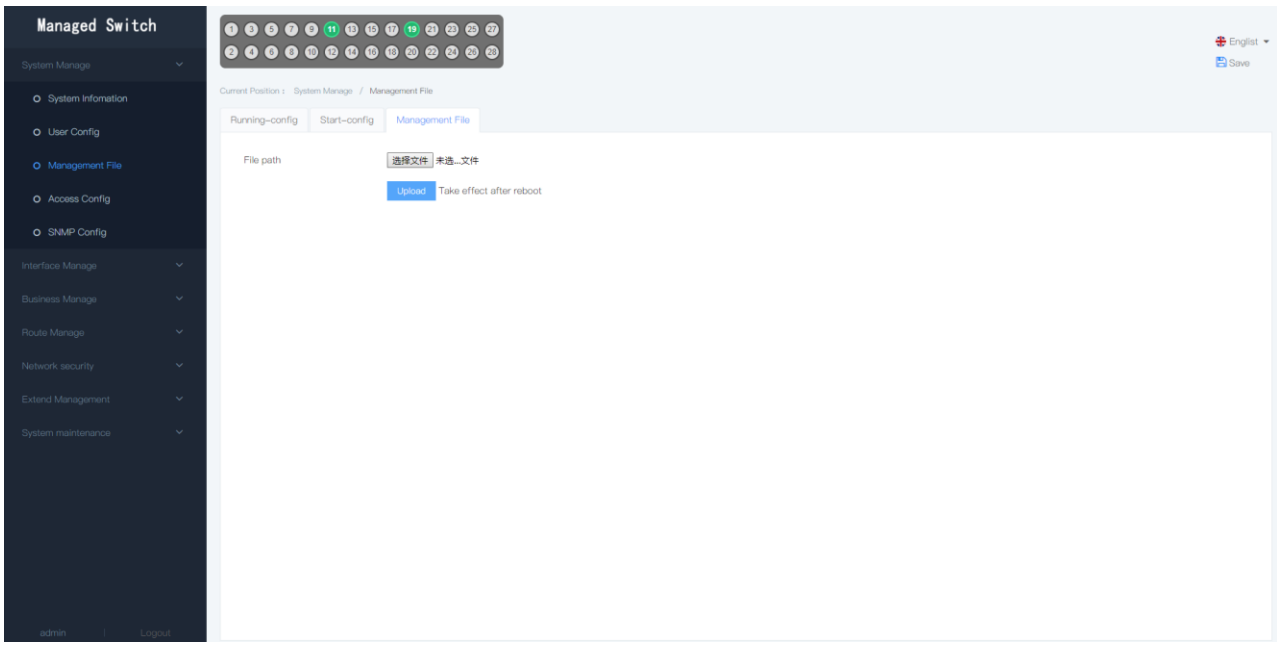
Displays the configuration loaded when the machine starts, click "Download" button to download the

configuration to your PC.



MANAGEMENT FILE

Select and unload the configuration files saved before.

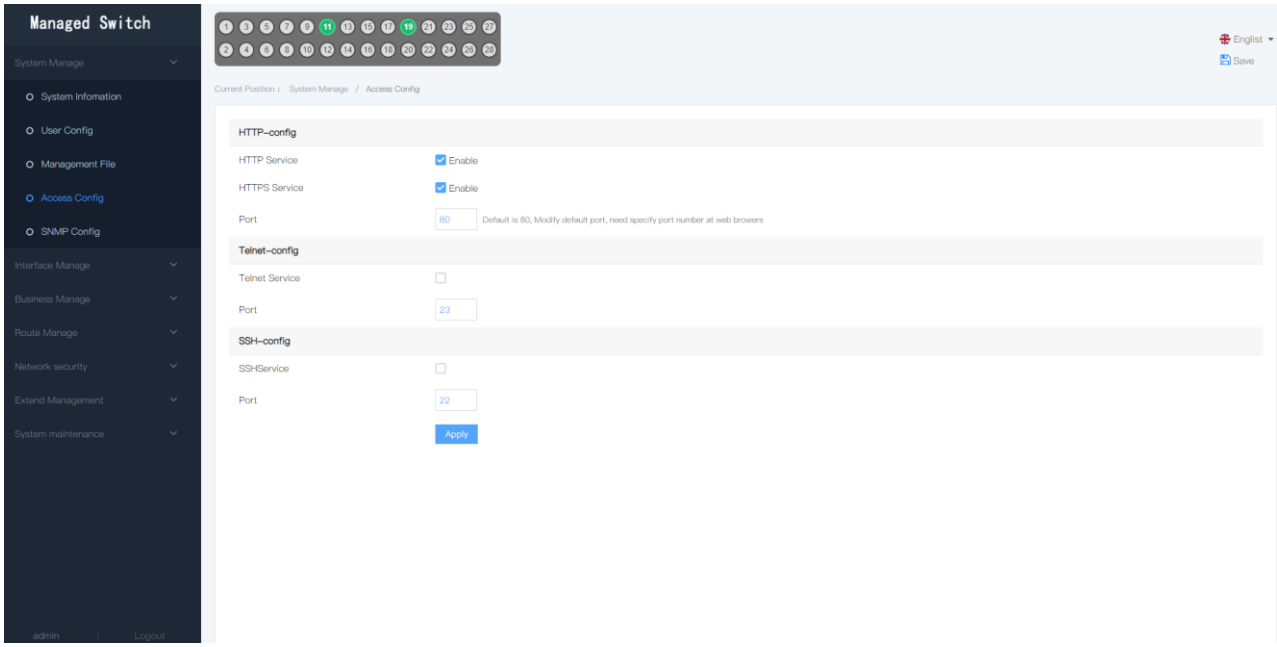


5.1.4 Access config

This page is used to determine whether to enable the http server / https server / telnet server / ssh server, and what is the port number of each server's logical port.

Apply: save changes, make configuration effective

cancel: discard modified data



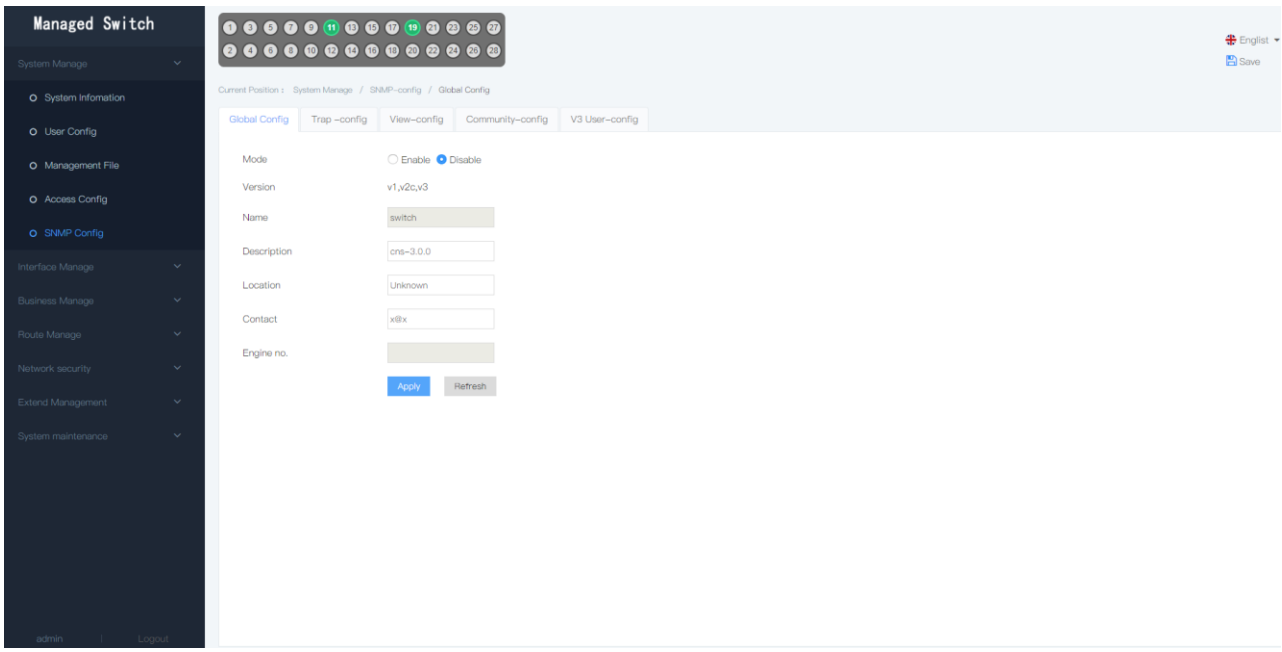
5.1.5 SNMP Config

SNMP is a network management standard based on TCP/IP protocol family. It is a standard protocol for managing network nodes (such as servers, workstations, routers, switches, etc.) in IP networks.

The SNMP protocol is composed of two parts: NMS (Network Management Station) and agent. The network management station is a central node responsible for collecting and maintaining information about each SNMP element, processing the information, and finally feedback it to the network administrator; the agent is running on each managed network node. It is responsible for counting the information of the node, interacting with the network management station, receiving and executing the commands of the management station, uploading all kinds of local network information.

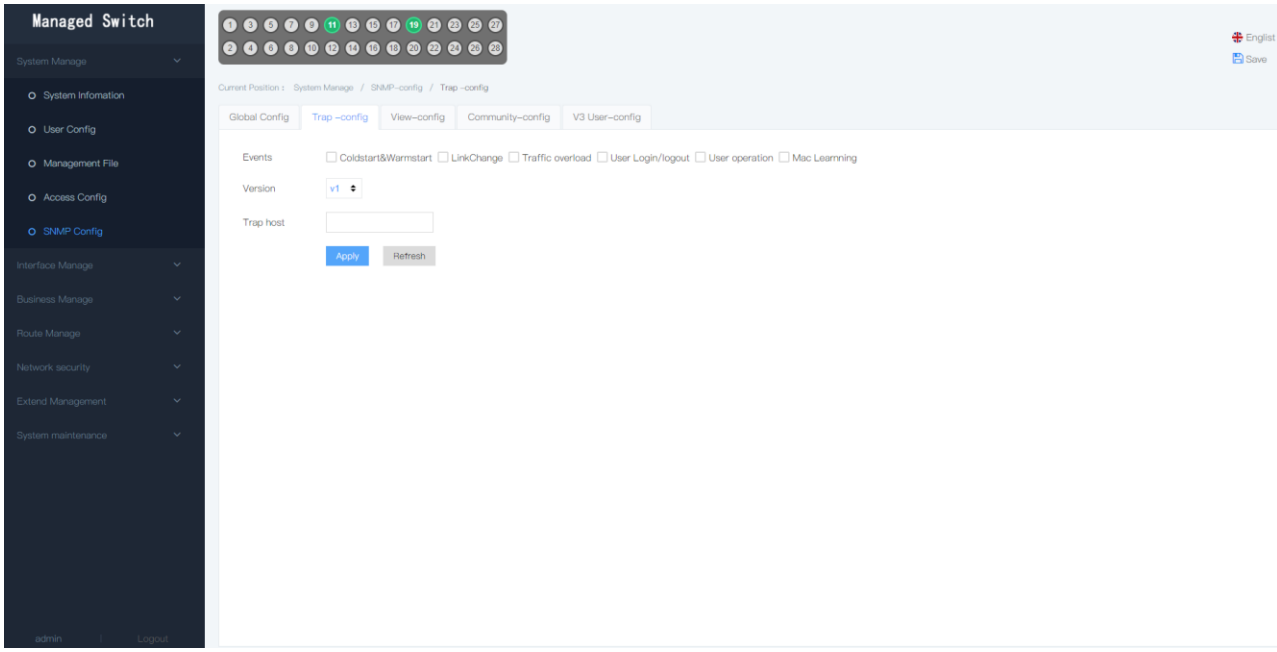
Global Config

SNMP configuration default disable, this page can be used to enable SNMP and inform SNMP server by description, location, contact



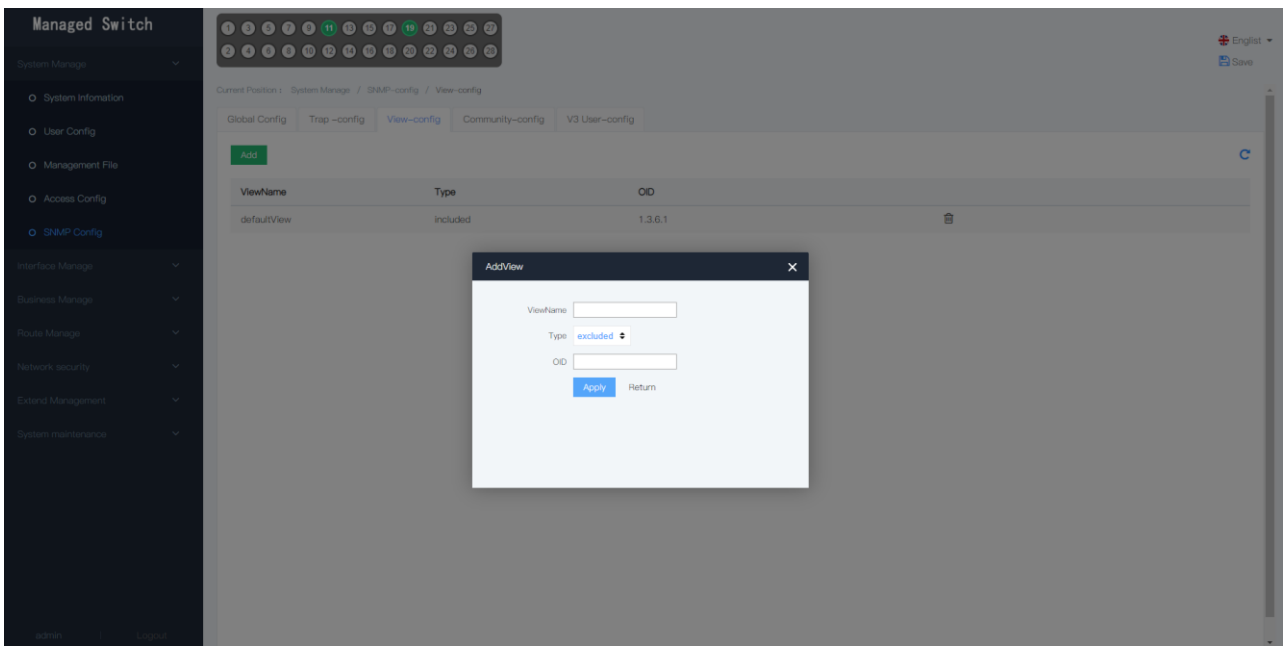
Trap-config

This page can be used to send the system startup, port status, traffic alarm, user login/logout, user operation, and MAC learning of the device to the SNMP server.



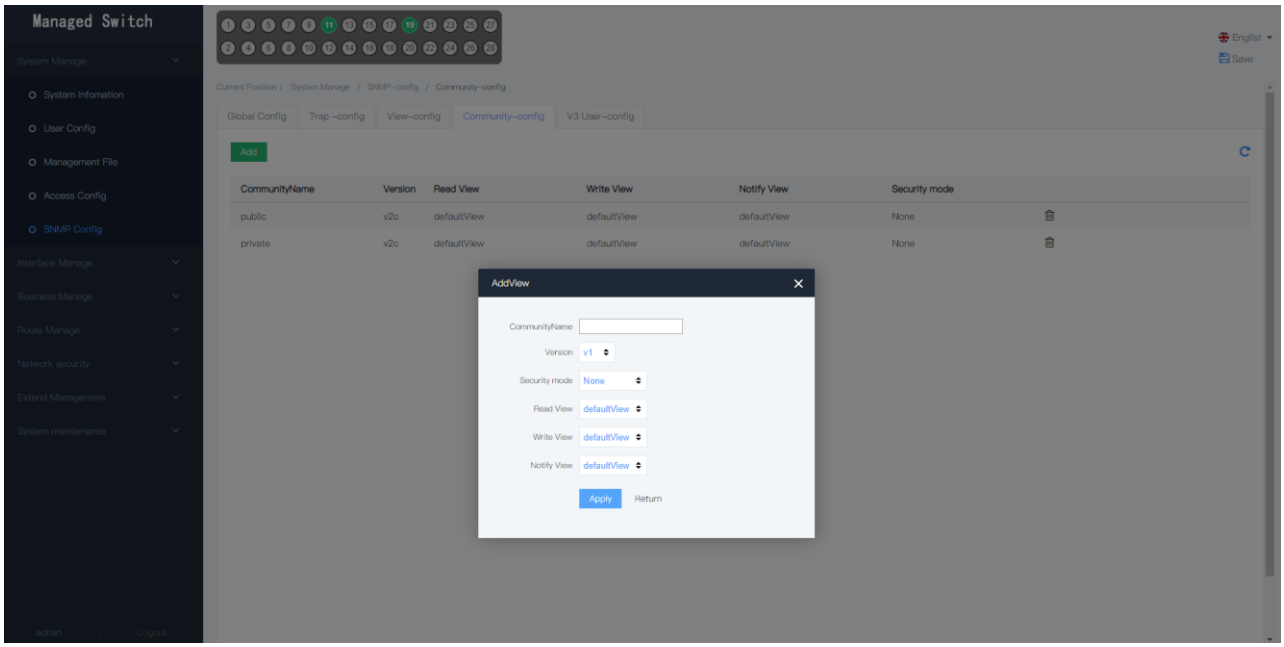
View config

The page user adds VIEW name, Type, OID



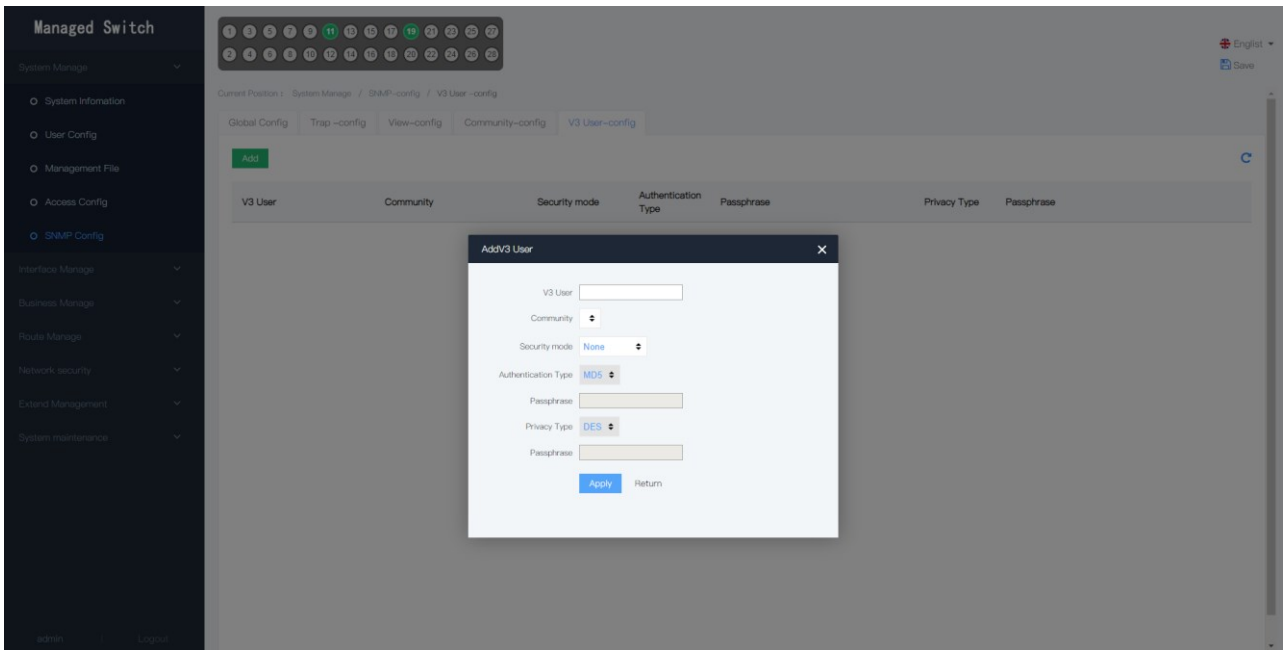
Community-config

The page user adds Community and sets the permissions of Community.



V3 User-config

To use SNMP V3, we need to create V3 user, fill in the user name, select the type of authentication algorithm, type of encryption algorithm, and fill in the authentication password and encryption password. The authentication algorithm supports MD5 and sha, the encryption algorithm supports des and esa.

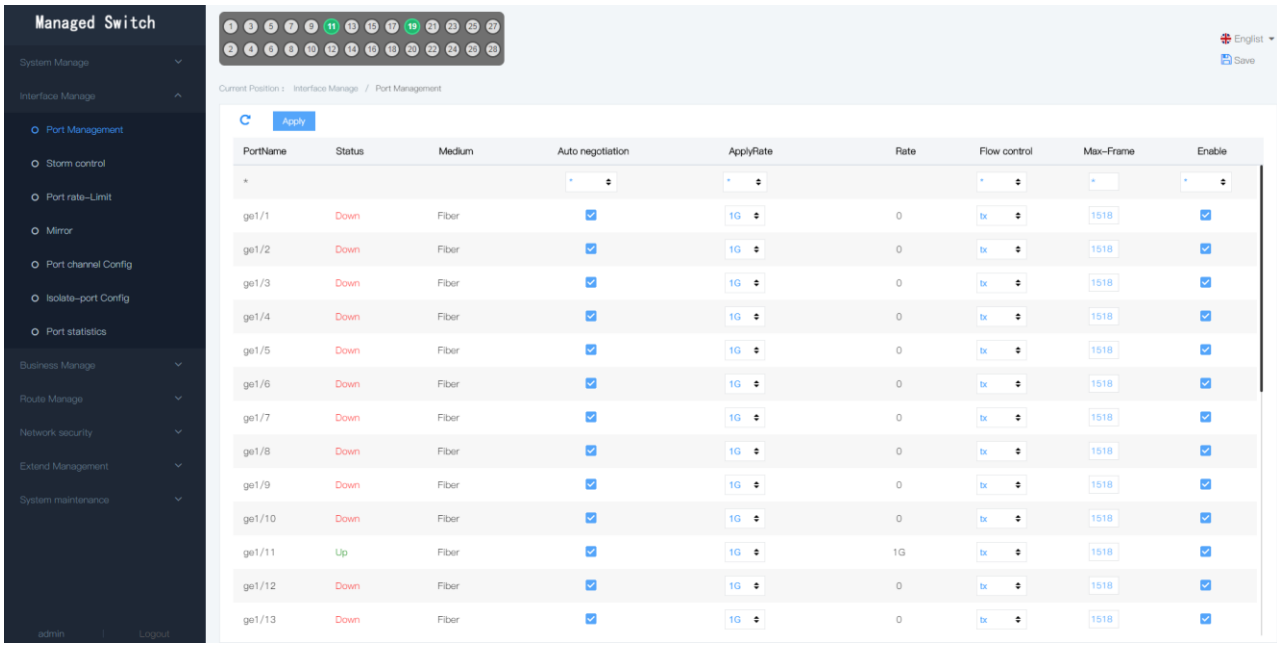


5.2 Interface Manage

5.2.1 Port management

View the current port name, status, medium, rate, settings, and management of each port's Auto-negotiation, rate, flow control, Max frame, and switch status.

* represents all ports, and the operation done on this line will apply to all ports

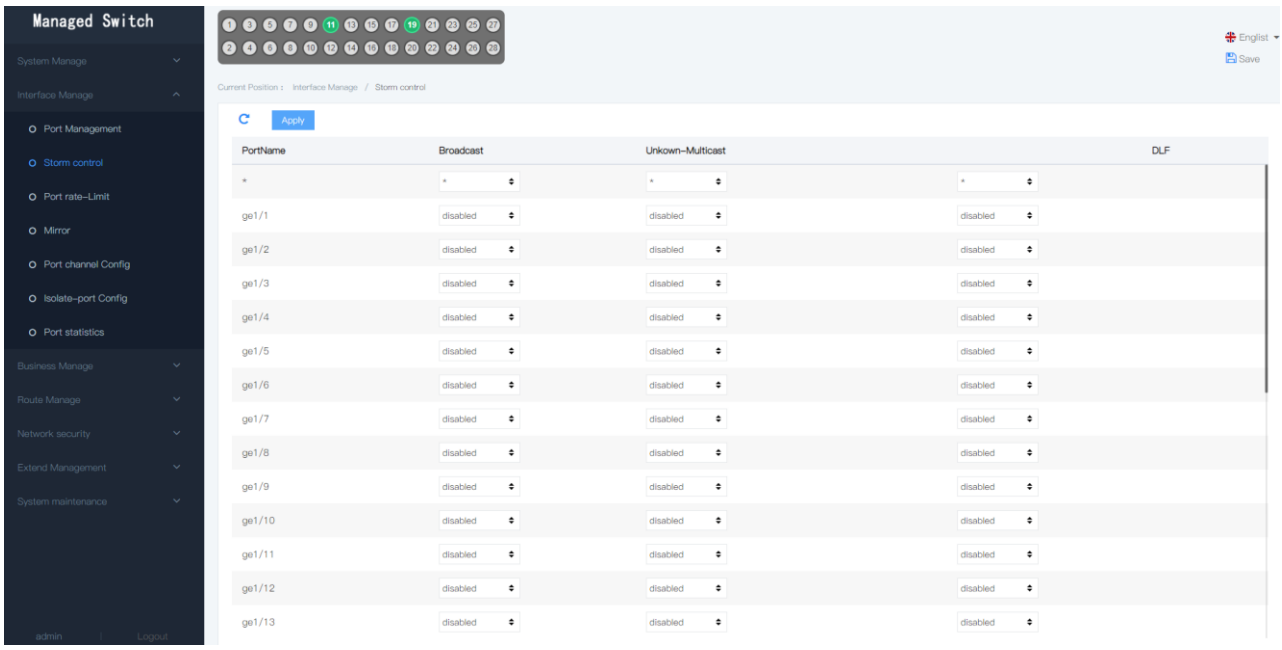


5.2.2 Storm control

Storm control allows ports to filter certain types of storm messages that appear on the network. After the storm control is turned on, when the corresponding frame received by the port accumulates to a predetermined limit, the port will automatically discard the received data frame. Avoid network congestion caused by port storms.

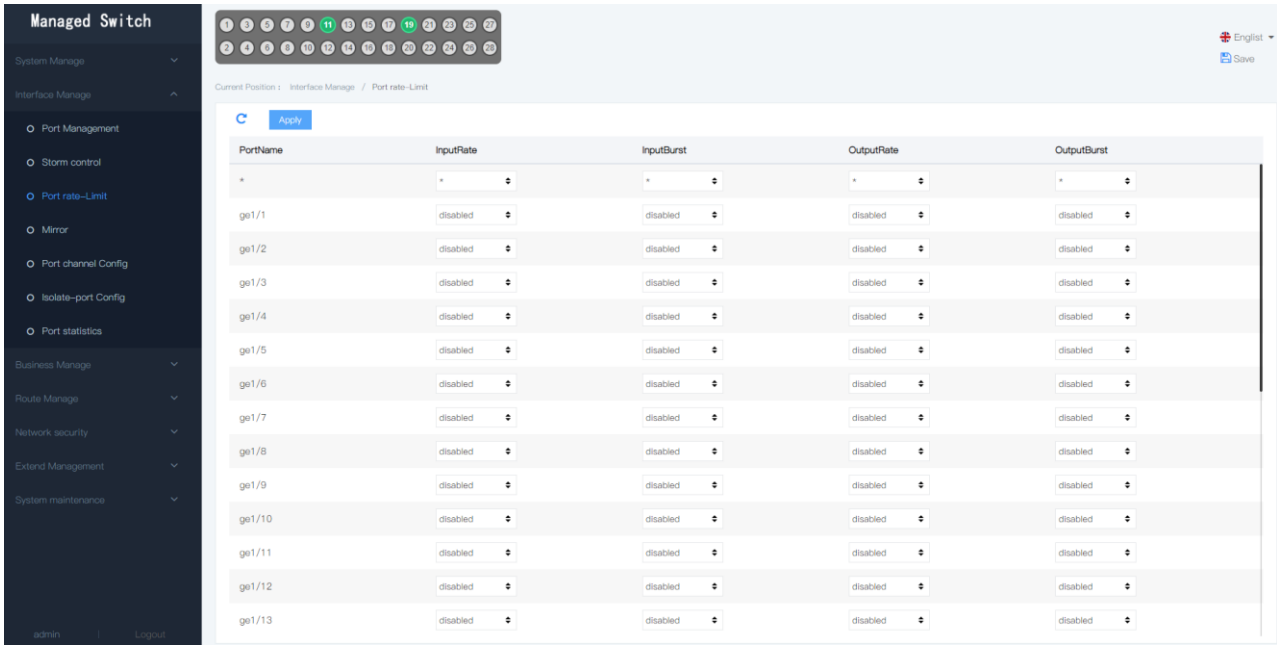
Broadcast Storm print, only configure storm suppression only fill in storm suppression value, and select the corresponding port, other storm suppression does not need to set the value to 0.

Unknown multicast and unknown unicast configuration are similar.



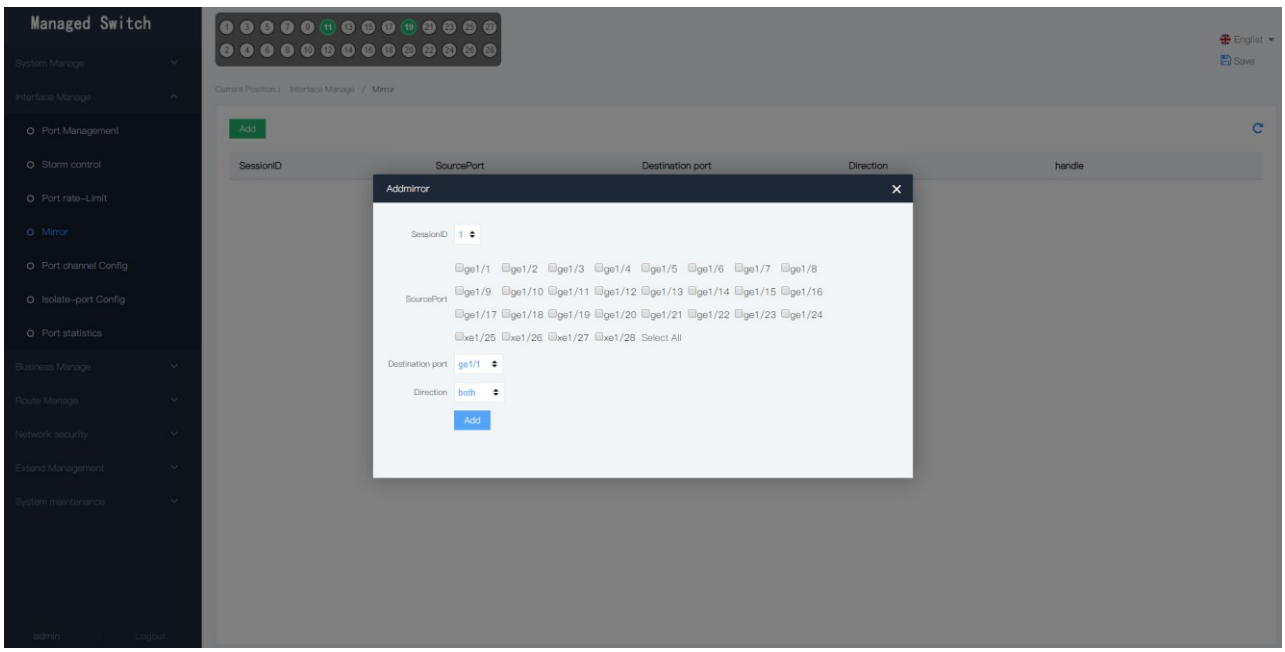
5.2.3 port rate-limit

Configuring port rate can limit the bandwidth of a port and avoid overflowing a port with too many data packets. Configuration burst and entry rate are configured together to take effect.



5.2.4 Mirror

A message sent or received by a port can be copied to the monitoring port. Mirroring is based on vlan, the default port belongs to Vlan1, testing needs to send vlan tagged data message. There are four session IDs, and different IDs can set up different mirroring groups.



5.2.5 Port channel Config

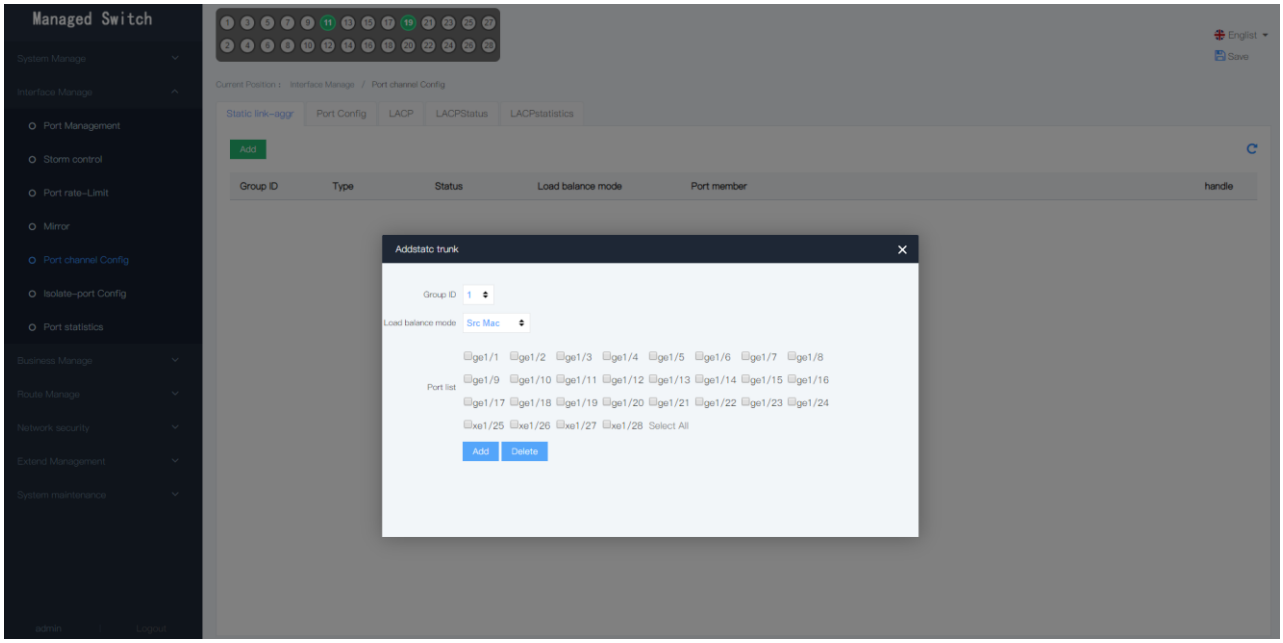
Used to organize multiple physical interfaces into one logical link

STATIC LINK-AGGR

By establishing a group and selecting the load sharing method according to the actual needs, the ports that need aggregation are added to the link aggregation group. In static aggregation mode, the lacp protocol is not enabled on the member ports within the aggregation group, and its port state is maintained manually.

Drop-down options for dot-small triangle symbols.

There are three ways to share the load： src-mac, dst-mac, both-mac.



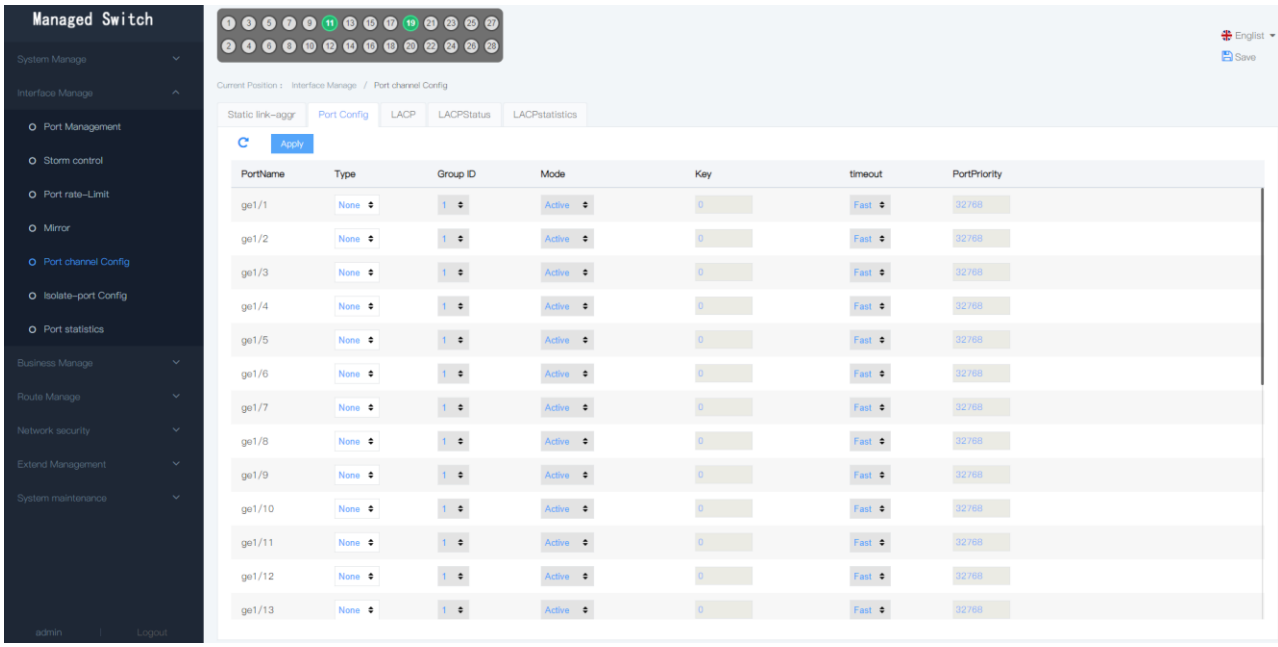
PORT CONFIG

Determine how to work by selecting the type of port.

None: No converging use.

LACP: Enable dynamic convergence of LACP

STATIC: Static link convergence



LACP

LACP provides two types of aggregation, one is active and the other is Passive, which is exchanged under Active The machine initiatively initiates the aggregation negotiation process, while the Passive mode is the passive receiving aggregate negotiation process, and the LACP is selected. When both sides of the port aggregation are Passive, the aggregation will not succeed because both ends will wait The process of initiating an end-to-end converging negotiation.

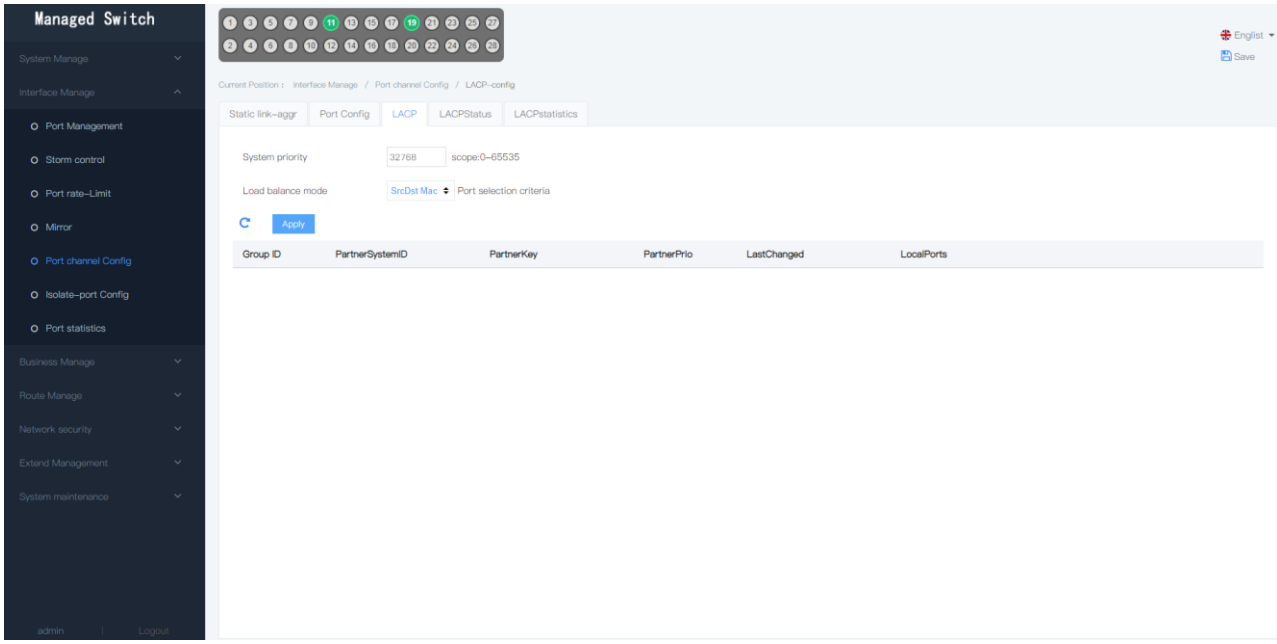
Select a way to aggregate load sharing, view aggregation group information. By adopting different types of aggregate load sharing, load sharing among aggregation groups can be realized flexibly.

Type of aggregate load sharing：

Src Mac： Aggregated load sharing according to the source MAC address of the message;

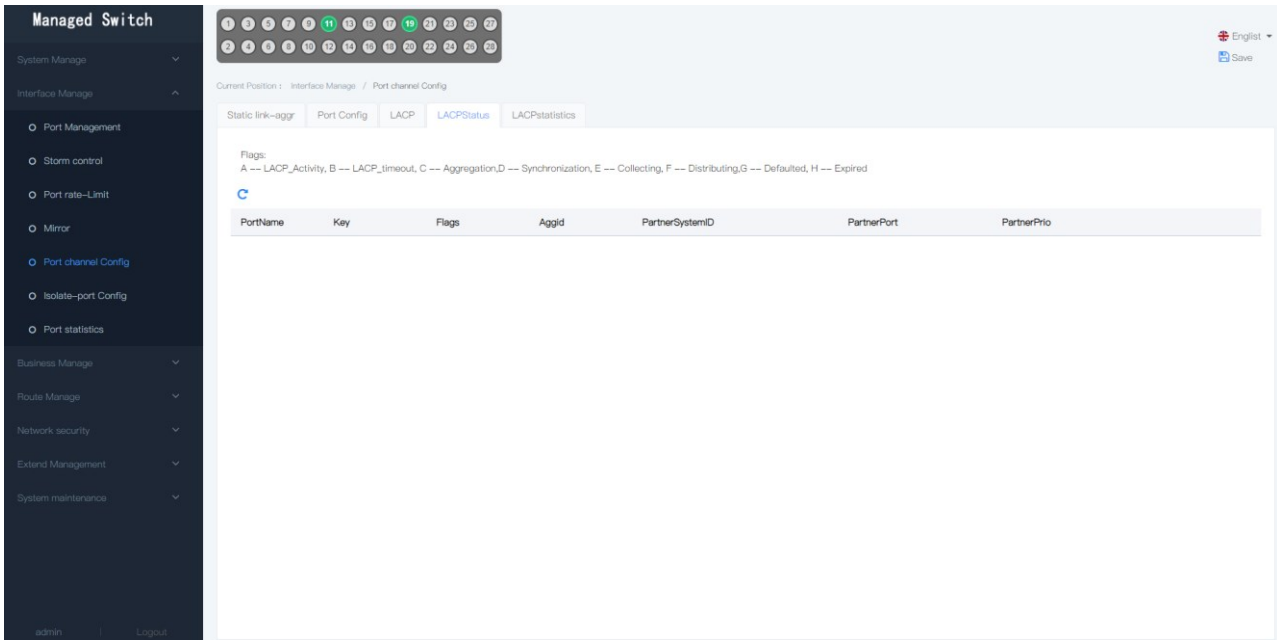
Dst Mac: Aggregate load sharing based on the destination MAC address of the message;

Src&Dst Mac: Aggregate load sharing based on the source of the message, the destination MAC address.



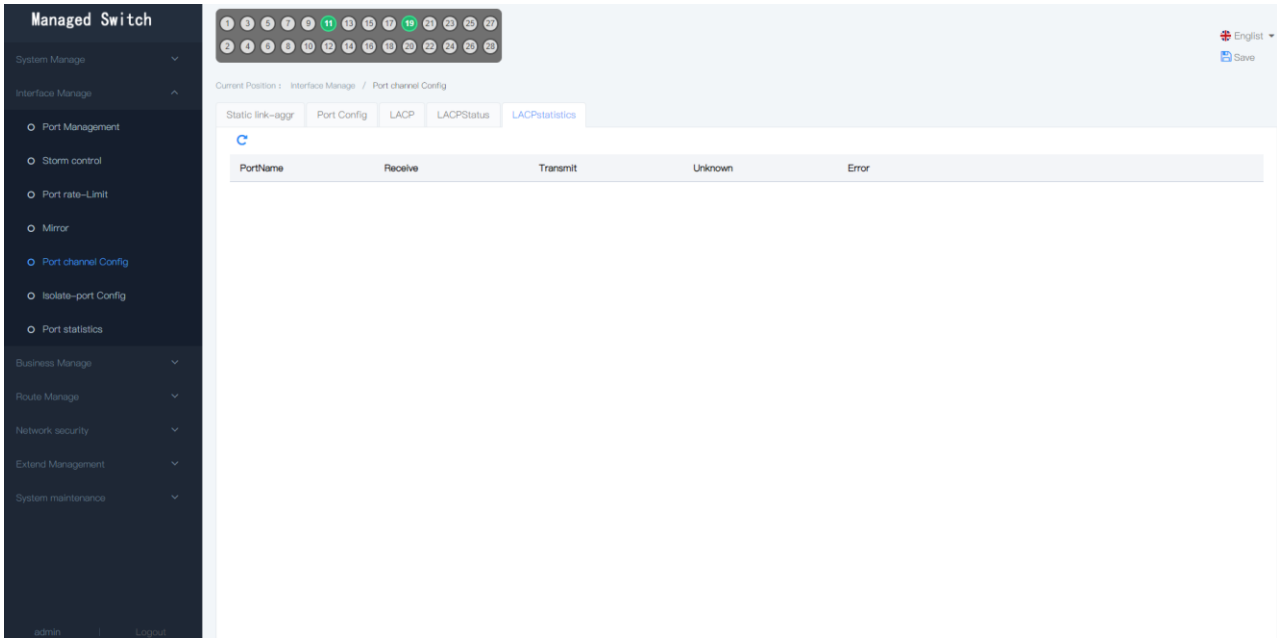
LACP STATUS

View aggregation group information, facilitating the management of information for converging groups.



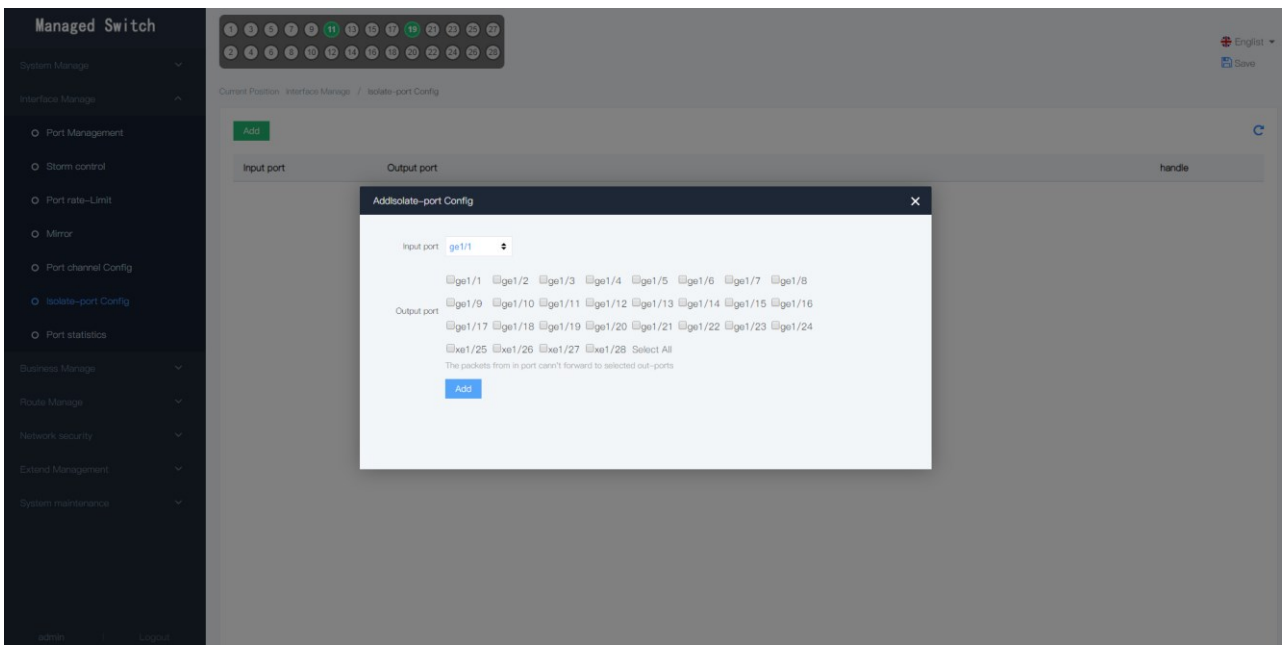
LACP STATISTICS

Check the statistics of the converging group and check the transmission status of the convergence groups.



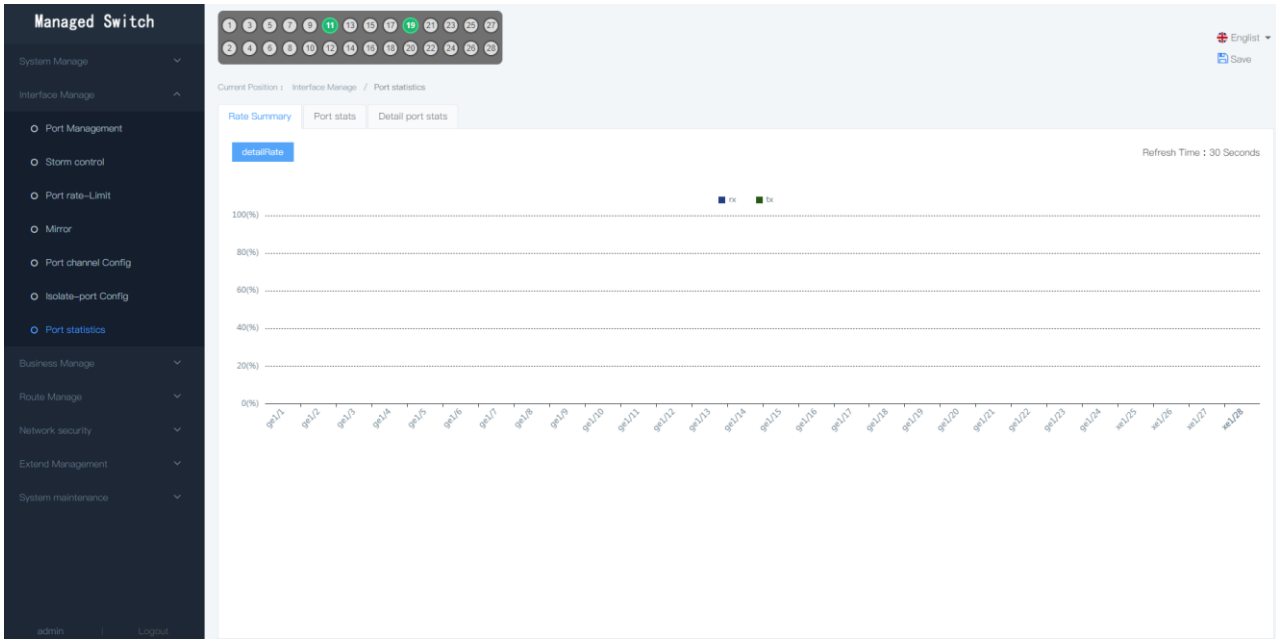
5.2.6 Isolate-port config

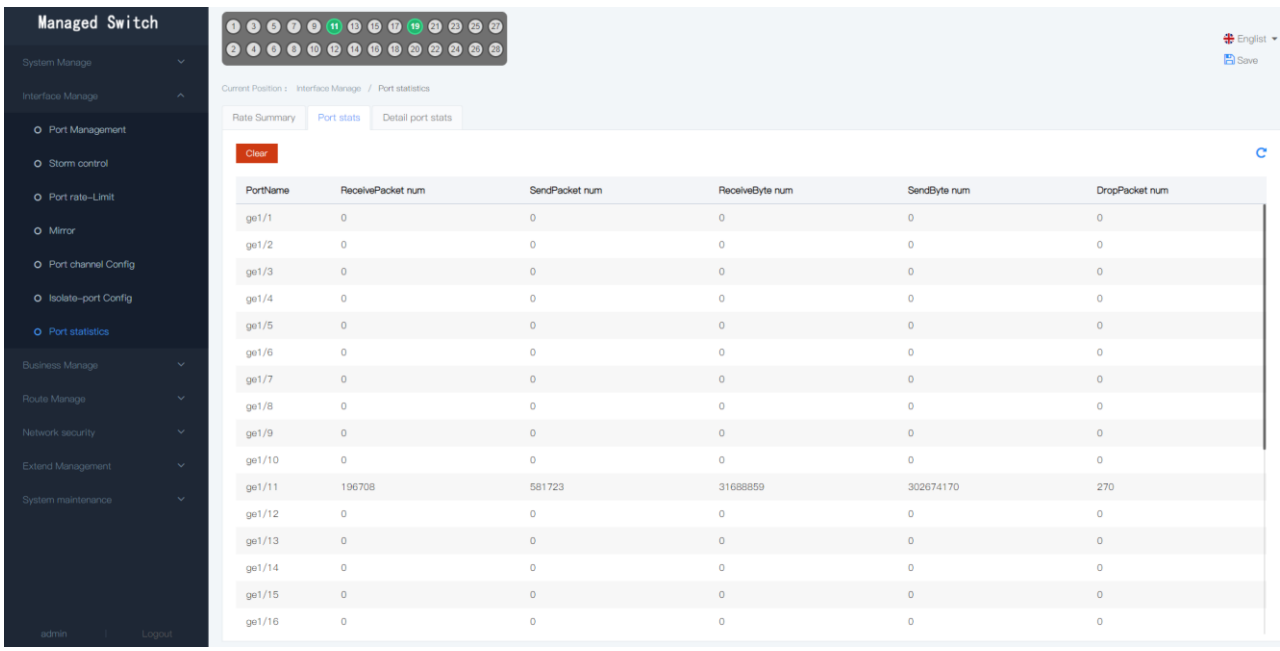
Port isolation can realize the independence of receiving and sending ports. It is convenient to designate a port to receive messages from a particular port and discard messages from some ports.



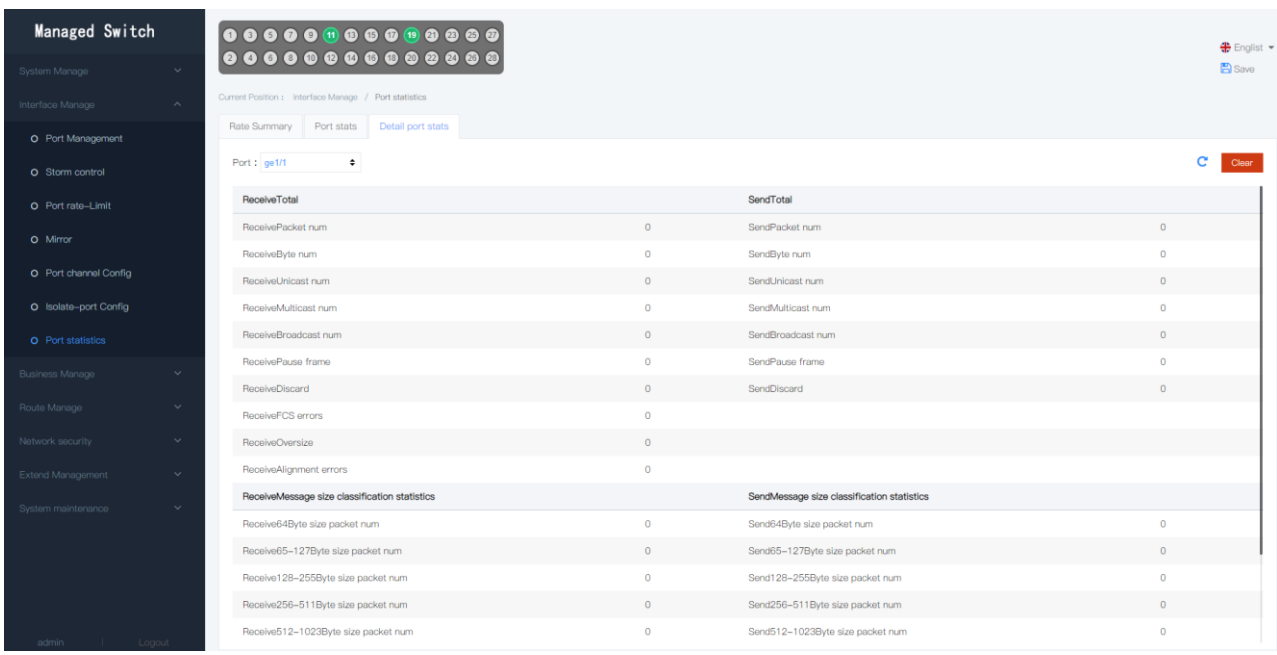
5.2.7 Port statistics

The data message received or sent by the current port can be analyzed for each port. Port statistics are divided into port summary statistics and port detailed statistics. You need to analyze different messages in detail, and you can see the port details.





PortName	ReceivePacket num	SendPacket num	ReceiveByte num	SendByte num	DropPacket num
ge1/1	0	0	0	0	0
ge1/2	0	0	0	0	0
ge1/3	0	0	0	0	0
ge1/4	0	0	0	0	0
ge1/5	0	0	0	0	0
ge1/6	0	0	0	0	0
ge1/7	0	0	0	0	0
ge1/8	0	0	0	0	0
ge1/9	0	0	0	0	0
ge1/10	0	0	0	0	0
ge1/11	196708	581723	31688859	302674170	270
ge1/12	0	0	0	0	0
ge1/13	0	0	0	0	0
ge1/14	0	0	0	0	0
ge1/15	0	0	0	0	0
ge1/16	0	0	0	0	0



ReceiveTotal		SendTotal	
ReceivePacket num	0	SendPacket num	0
ReceiveByte num	0	SendByte num	0
ReceiveUnicast num	0	SendUnicast num	0
ReceiveMulticast num	0	SendMulticast num	0
ReceiveBroadcast num	0	SendBroadcast num	0
ReceivePause frame	0	SendPause frame	0
ReceiveDiscard	0	SendDiscard	0
ReceiveFCS errors	0		
ReceiveOversize	0		
ReceiveAlignment errors	0		
ReceiveMessage size classification statistics		**SendMessage size classification statistics**	
Receive64Byte size packet num	0	Send64Byte size packet num	0
Receive65-127Byte size packet num	0	Send65-127Byte size packet num	0
Receive128-255Byte size packet num	0	Send128-255Byte size packet num	0
Receive256-511Byte size packet num	0	Send256-511Byte size packet num	0
Receive512-1023Byte size packet num	0	Send512-1023Byte size packet num	0

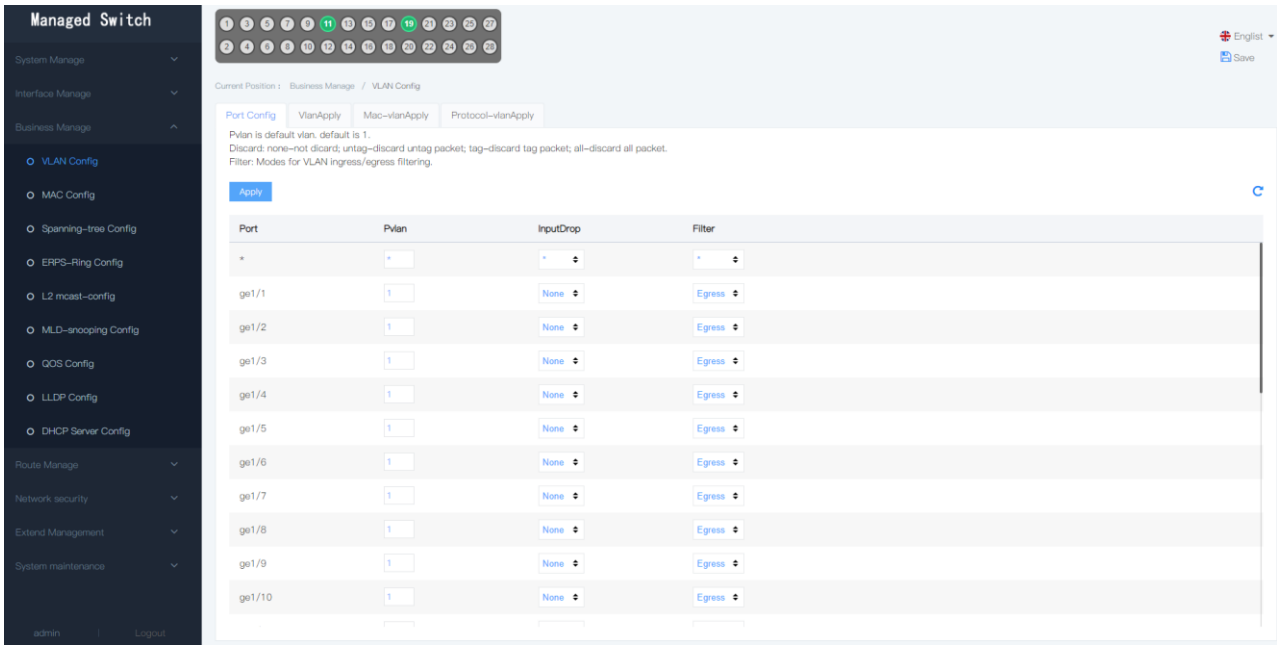
5.3 Business manage

5.3.1 VLAN config

Logically divide a physical LAN into different broadcast domains (or virtual lan, or VLANs), and each VLAN contains a set of computers with the same requirements, since VLAN is logically rather than physically partitioned. Therefore, the computers within the same VLAN need not be placed in the same physical space, that is, these computers do not necessarily belong to the same physical LAN network segment.

PORT CONFIG

View the port belongs to the VLAN, according to the definition of the port VLAN to choose the way to discard the message, select the legitimacy check is at the exit / entry.



VLAN APPLY

The switch supports the 802.1q VLAN pattern by identifying the Tag tags in the message (including 802.1p priority and VLAN ID, etc.) to process a message.

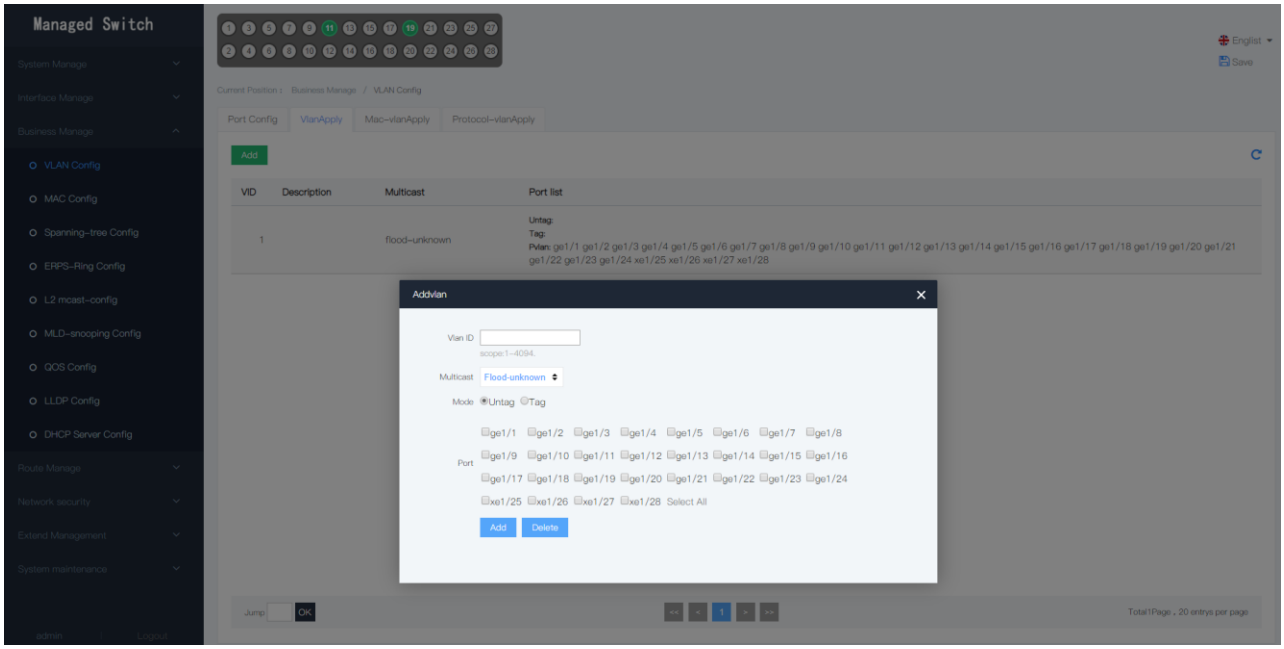
VLAN ID: The VLAN number that identifies the message is 12 bits in length and ranges from 0 to 4095. Due to 0 And 4095 are reserved for the protocol, so the VLAN ID values range from 1 to 4094.

Multicast: Used to configure the processing of multicast packets in a specified VLAN.

Drop: Represents dropping multicast packets

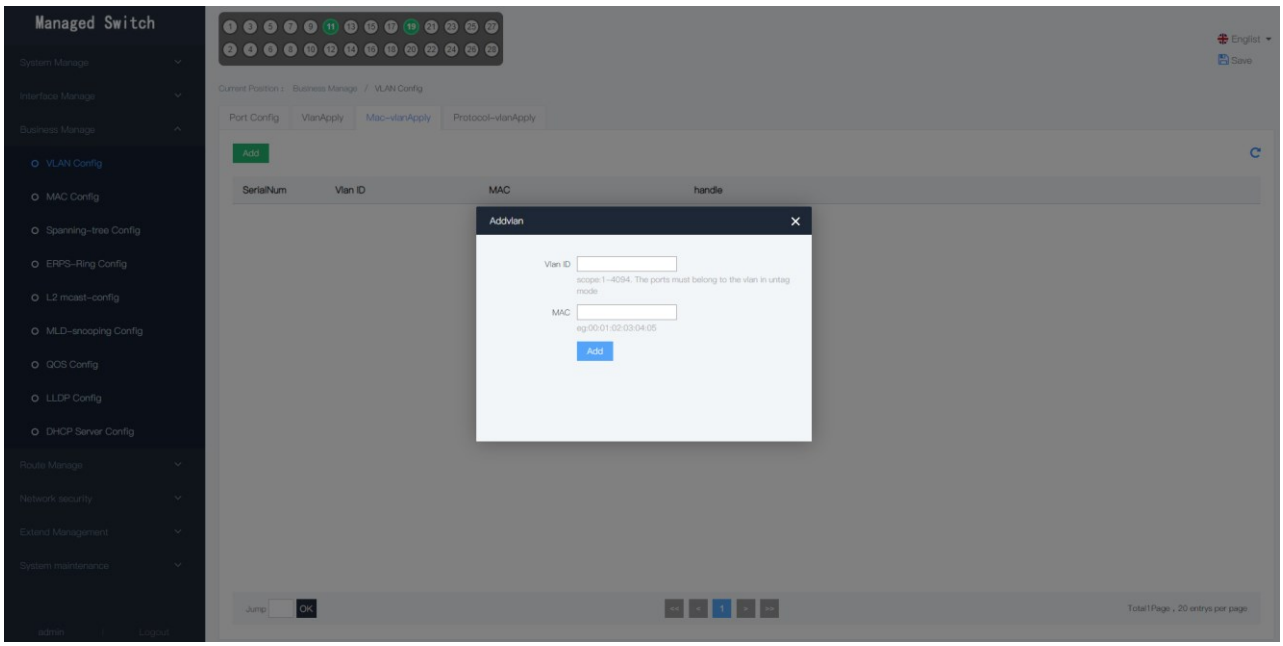
Flood all: Represents all multicast packets for flooding

Flood unknown: Multicast packets representing flooding unknown



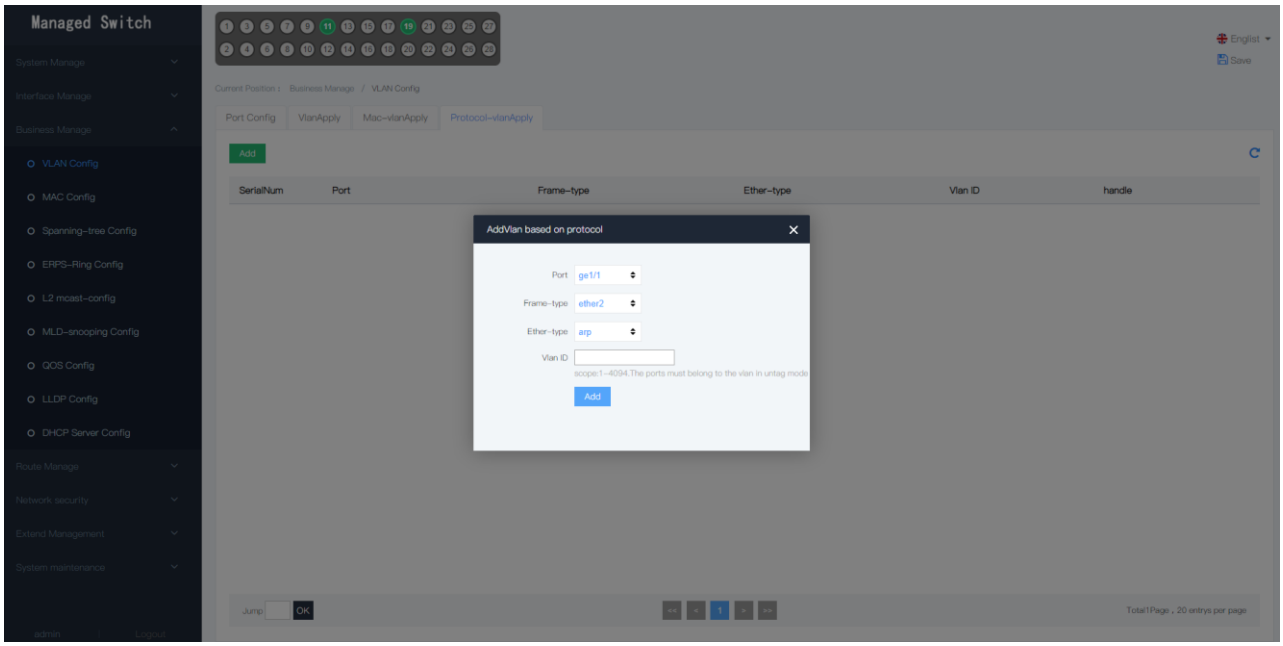
MAC-VLAN APPLY

According to the mac address, there is no need to pay attention to the physical location of the end user, which improves the security of the end user and the flexibility of access. Mac vlan only processes untagged packets, and tagged message processing mode is the same as that of port-based vlan.



PROTOCOL-VLAN APPLY

Protocol-based VLAN, also known as protocol VLAN, is another VLAN representation different from port-based VLAN Dividing method. By configuring a protocol-based VLAN, the switch can analyze any received on the port that does not carry VLAN Tag To match the message with the user-set protocol template according to the values of different encapsulation formats and special fields, automatically The corresponding VLAN tag is added to match the successful message, and the data belonging to the specified protocol is automatically distributed to the corresponding VLAN for transmission.



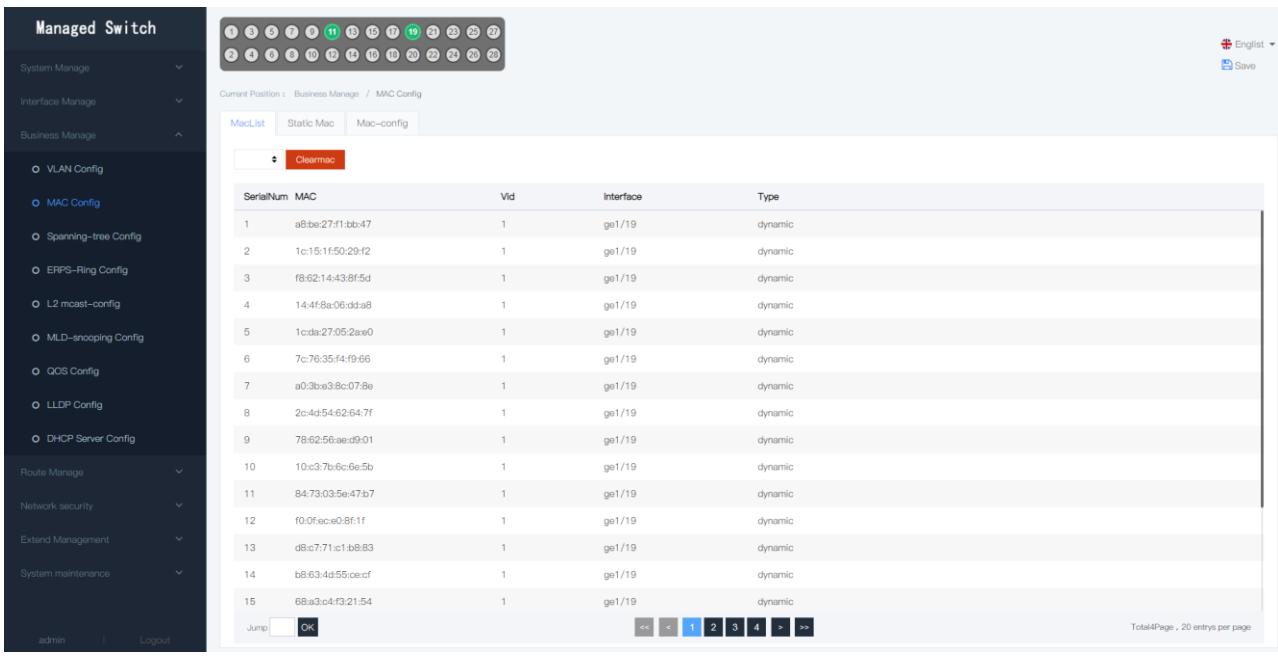
5.3.2 MAC Config

The default is dynamic mac. you can modify the mac aging time

MAC list

The MAC address table records the MAC address of the device connected to the device. Interface number and the VLAN ID. When forwarding data, the device queries the MAC location according to the destination MAC address in the message Address table to quickly locate the interface, thus reducing broadcast. Displays the MAC address of the current connection port.

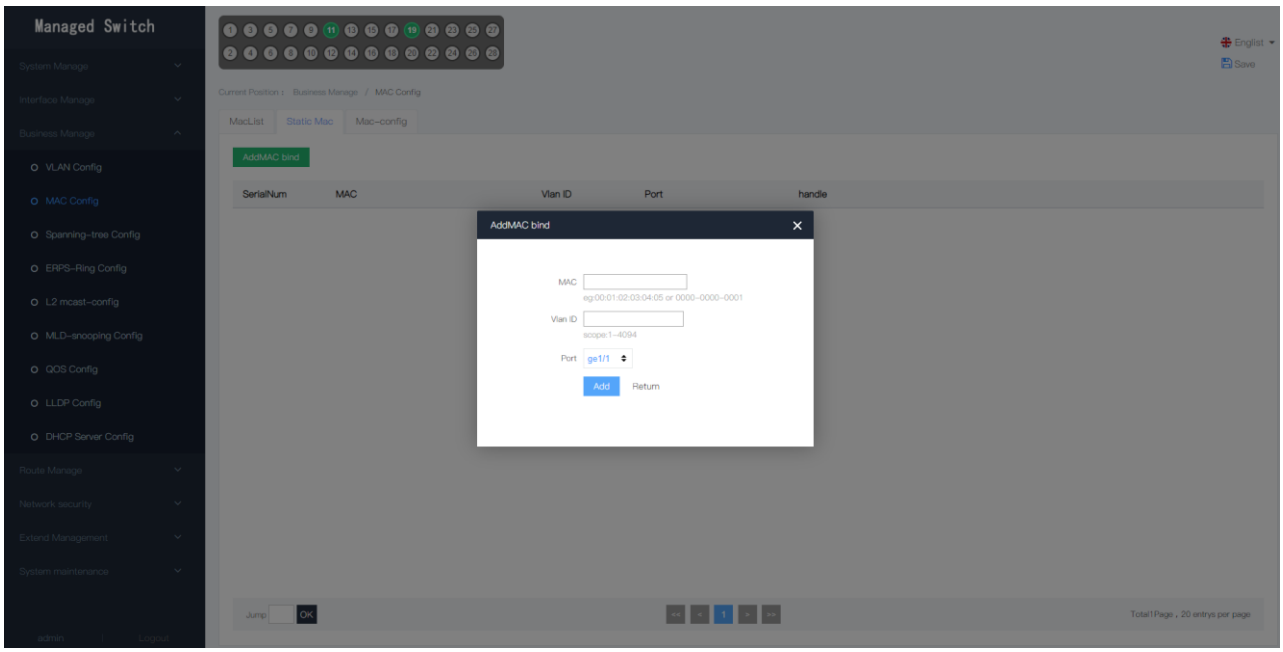
To adapt to changes in the network, the MAC address table needs to be continuously updated. The automatically generated items in the. MAC address table are not forever. Far more effective, each table item has a lifetime, items that arrive at the life cycle that have not been refreshed will be deleted, and this The life cycle is called aging time. If the record is refreshed before reaching the life cycle, the ageing time of the table item is recalculated Calculate.



STATIC MAC

When a device learns to automatically create a MAC address table through a source MAC address, it cannot

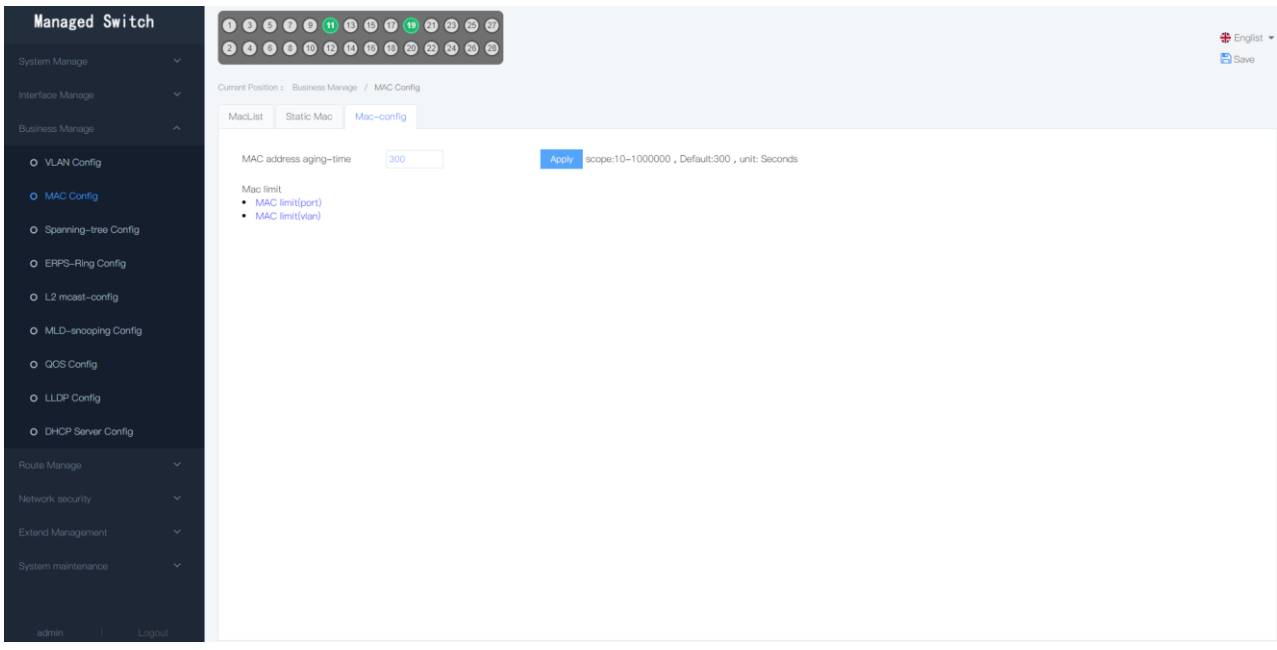
distinguish between legitimate users and hacker users Wen, brought about the hidden danger of safety. If the hacker user masquerades the source MAC address of the attack message as the legitimate user's MAC address, And get in from the other interfaces of the device, the device learns the wrong MAC address table entry, and it forwards it to the The legitimate user's message is forwarded to the hacker user. To improve interface security, network administrators can manually add a specific MAC address table entry to the MAC address table, setting the User devices are bound to the interface to prevent false identities of illegal users from obtaining data. Manually configured MAC address table entries Priority is higher than automatically generated table items.



MAC-CONFIG

If the aging time of the user configuration is too long, the device may save many outdated MAC address table items, thus exhausting the MAC address table resources, resulting in the device unable to update the MAC address table according to the change of the network. If the aging time of the user configuration is too short, the device may delete the valid MAC address table item, which may cause the device to broadcast a large number of data packets and affect the performance of the device. Therefore, users need to configure appropriate aging time according to the actual situation to effectively achieve MAC address aging function.

Mac-limit: To set the maximum number of learning for port MAC addresses



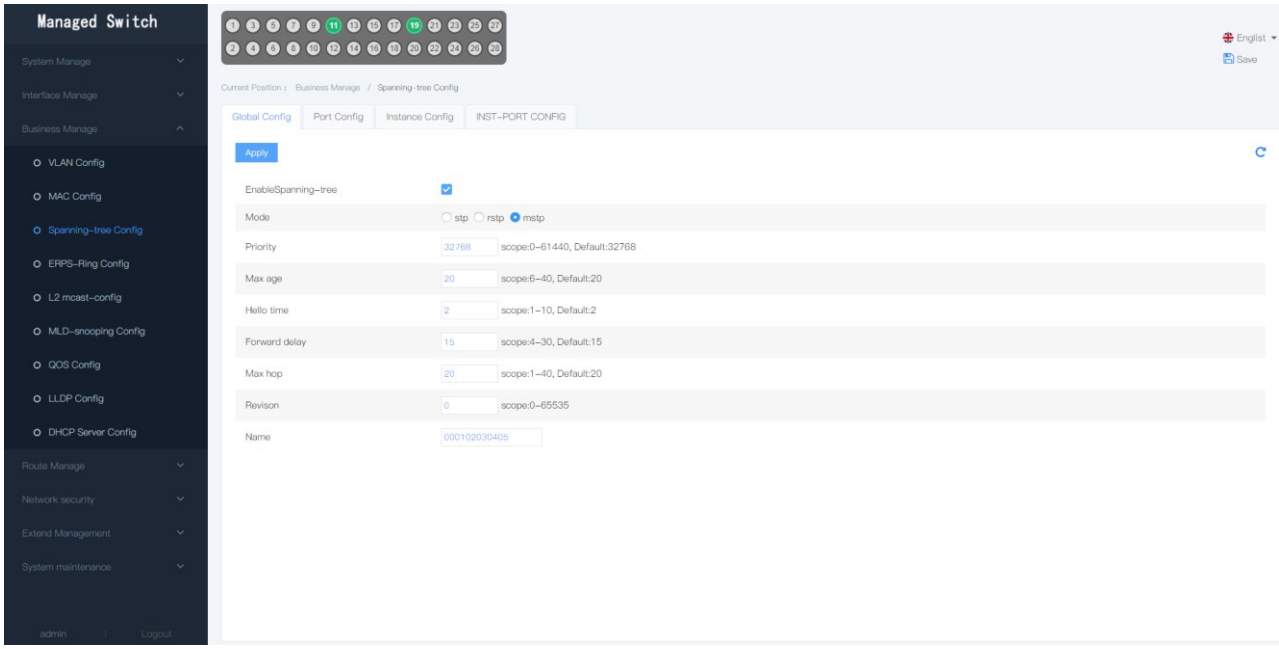
5.3.3 Spanning-tree config

GLOBAL-CONFIG

STP: The protocol can be used to establish tree topology in the network, eliminate the loop in the network, and can achieve path redundancy through a certain method, but it is not sure to achieve path redundancy. The spanning tree protocol is suitable for all vendors' network devices, and is different in configuration and function intensity, but in principle and application effect. It's the same.

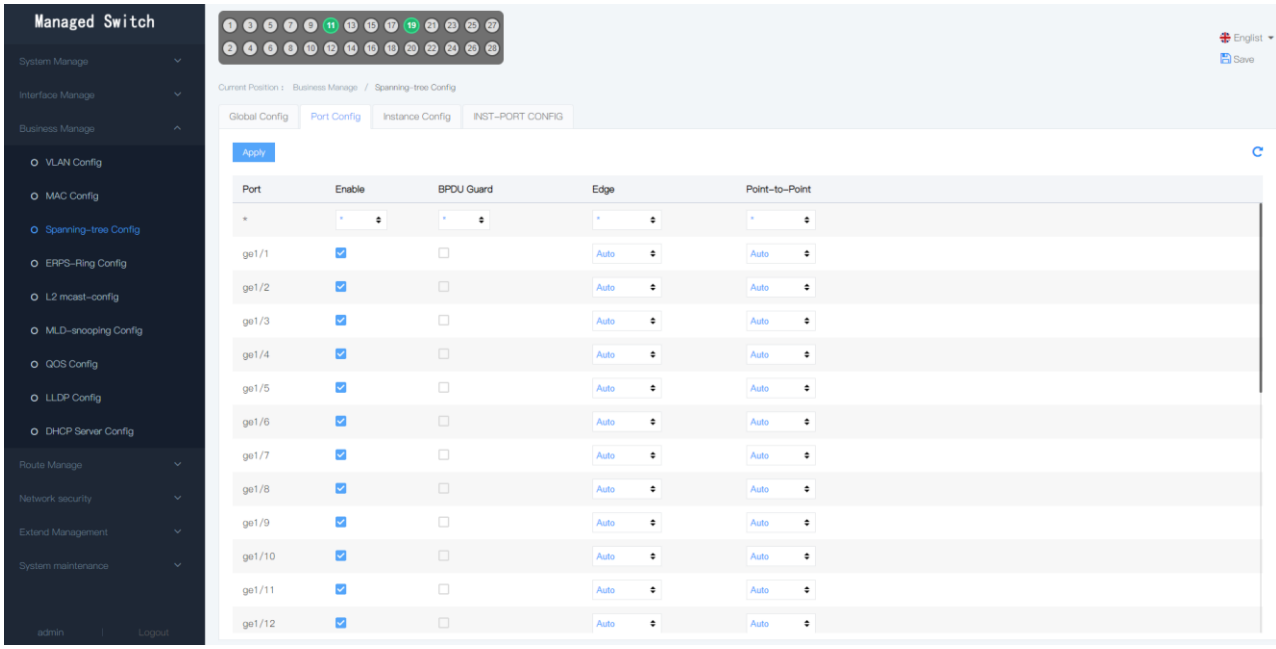
RSTP: 802.1w is developed by 802.1d. This protocol can converge faster when the network structure changes. It has two more port types than 802.1d: the alternate port and the backup port type. STP (Spanning Tree Protocol) is the abbreviation of the spanning tree protocol. The protocol can be applied to the loop network and pass through a loop network. The algorithm implements path redundancy and Pruns the loop network into a loop free tree network, thereby avoiding the proliferation and infinite loop of packets in the loop network.

MSTP: MSTP is a multi-spanning tree protocol. MSTP's "multi-spanning tree" includes two meanings: one is that multiple instances of spanning tree can be divided based on VLAN in a switching network, the other is that multiple VLANs can be included in each instance of spanning tree.



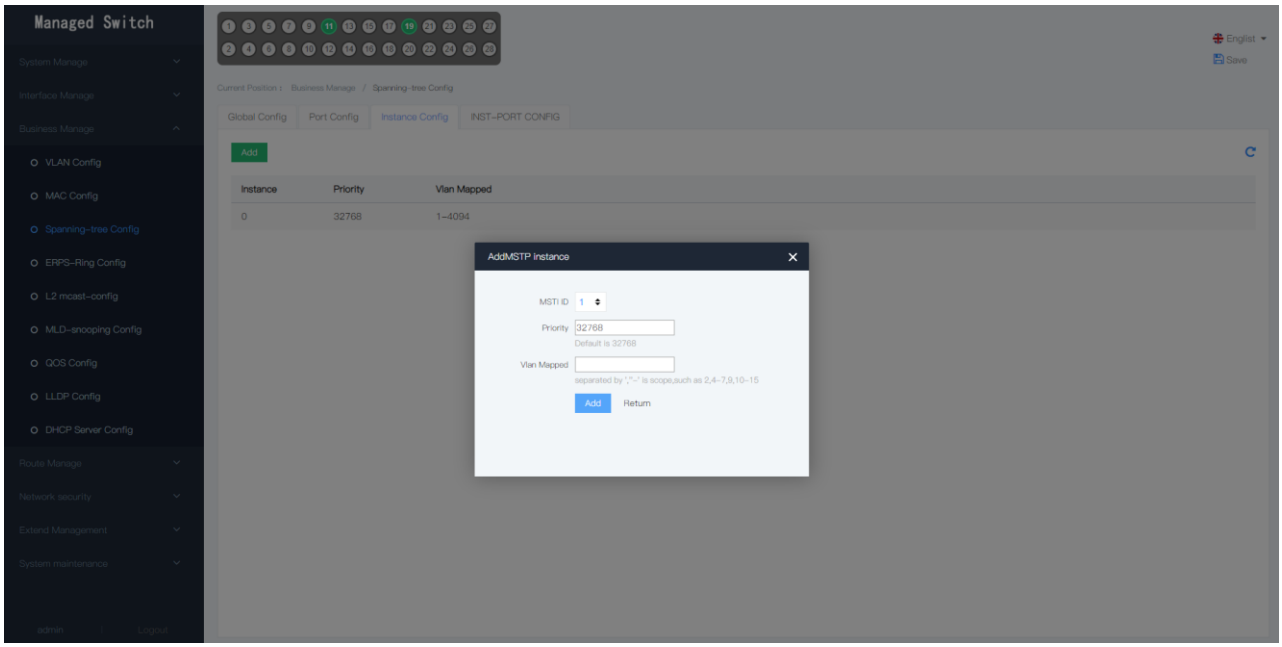
PORT CONFIG

In order to reduce excessive link computation, when configuring the ring function, the port that needs to be enabled is opened, and the function does not need to be turned off with the ring network port.



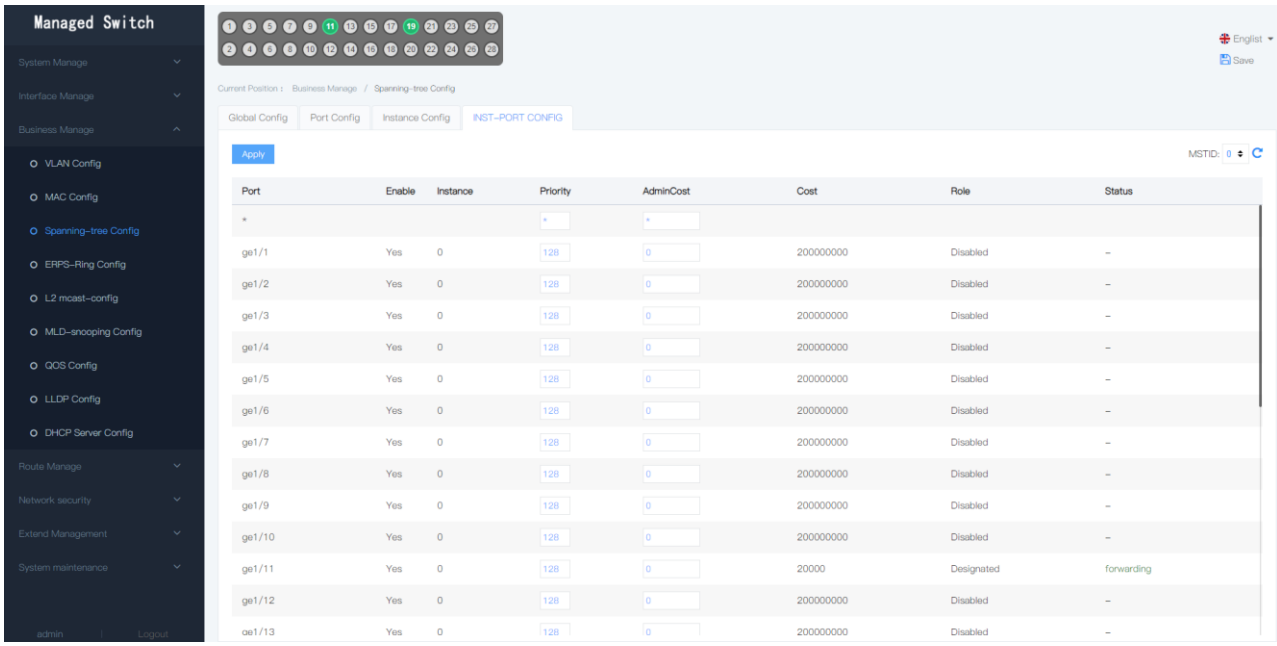
INSTANCE CONFIG

Set the number of VLAN that can be included per build tree instance.



INST-port CONFIG

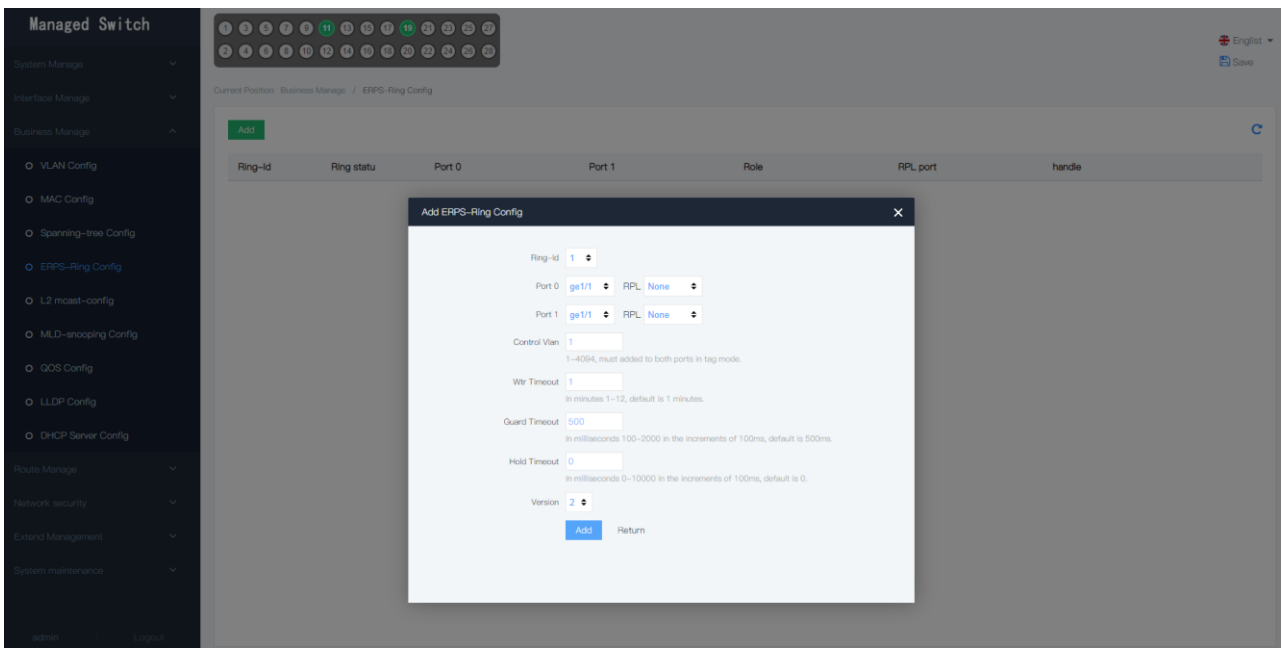
View the status of the spanning tree example and manage priorities and Cost.



5.3.4 ERPS-Ring Config

ERPS (Ethernet Ring Protection Switching), is a two-layer broken ring protocol standard defined by ITU-T. The standard number is ITU-T G.8032 / Y1344, so it is also called G. 8032 / Y1344. It defines RAPS (Ring Auto Protection Switching) protocol packets and protection switching mechanism. V2 fully compatible with v1.

Erps is a protocol for Ethernet link layer break loop. It takes the erps loop as the basic unit and contains several nodes. By blocking the rpl owner port and controlling the other common ports, the state of the port is switched between forwarding and discarding to eliminate the loop.



5.3.5 L2 mcast-config

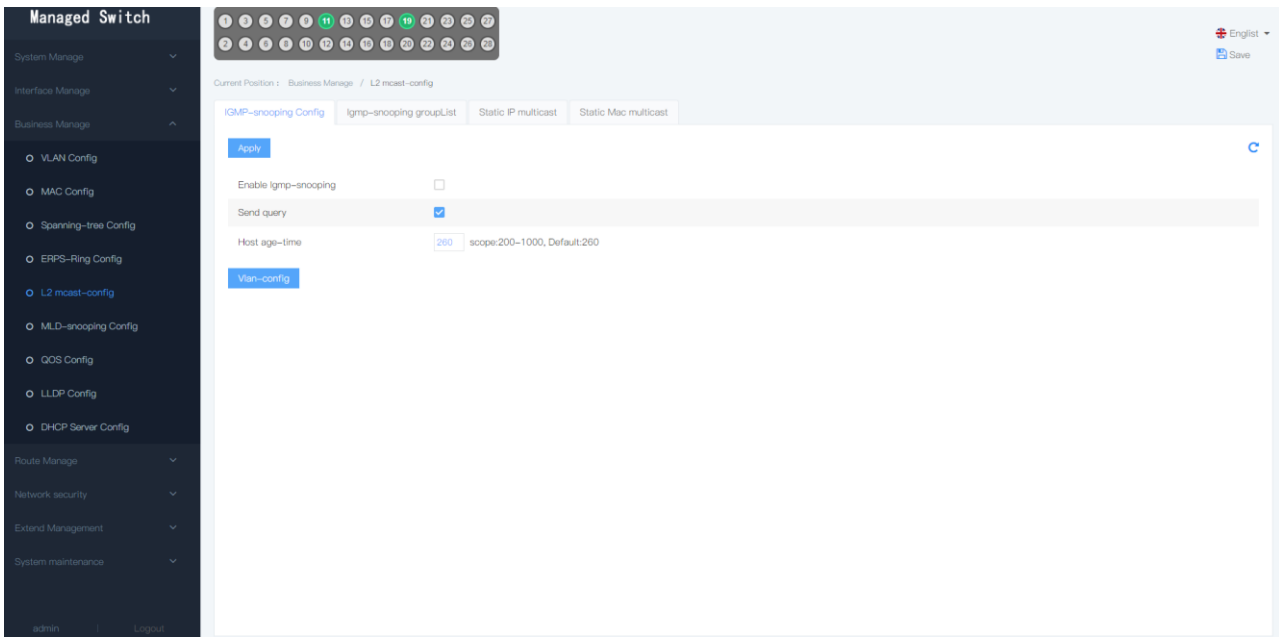
IGMP-SNOOPING working process: The switch listens for the interactive messages between the user host and the router, tracks the multicast information and the application port. When the switch detects an IGMP report message sent by the host to the router, the switch adds the port to the multicast forwarding table; when the switch listens to the IGMP leave message sent by the host, the router will send the Group-Specific query

(specific group query) message of the port. If other hosts need the group to broadcast, the router will respond to the IGMP Report message. If the router does not receive any response from the host, the switch will remove the port from the multicast forwarding table. After receiving the IGMP Query message, if the router does not receive the IGMP Report message from the host within a certain time period, the port is removed from the multicast table.

A member of a dynamic multicast message sends to join a specific multicast group, and the polling message monitors that the port is automatically added to the corresponding multicast group. Configuration as shown below, must first turn on the global function, at the same time open the active query, according to the actual use of configuration aging time, the default aging time 200s. Since IGMP is based on vlan, for the functionality to take effect, it must also be configured in IGMP-snooping VLAN.

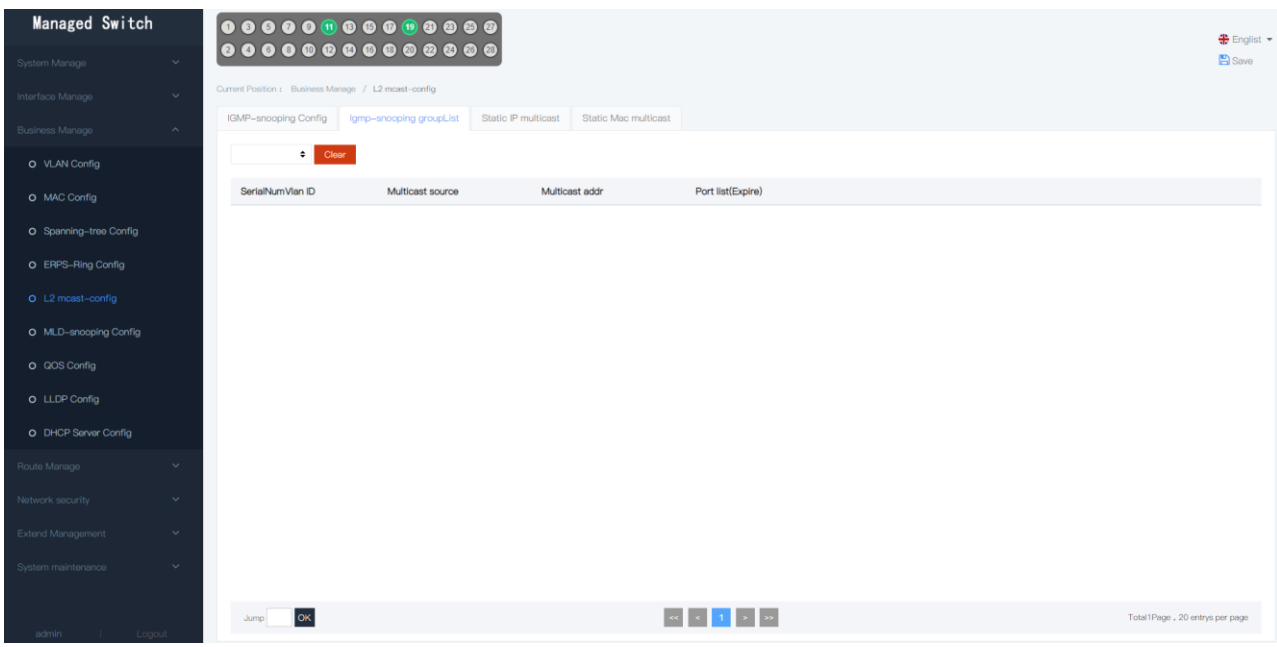
IGMP-snooping config

Send query: To enable sending master query packets



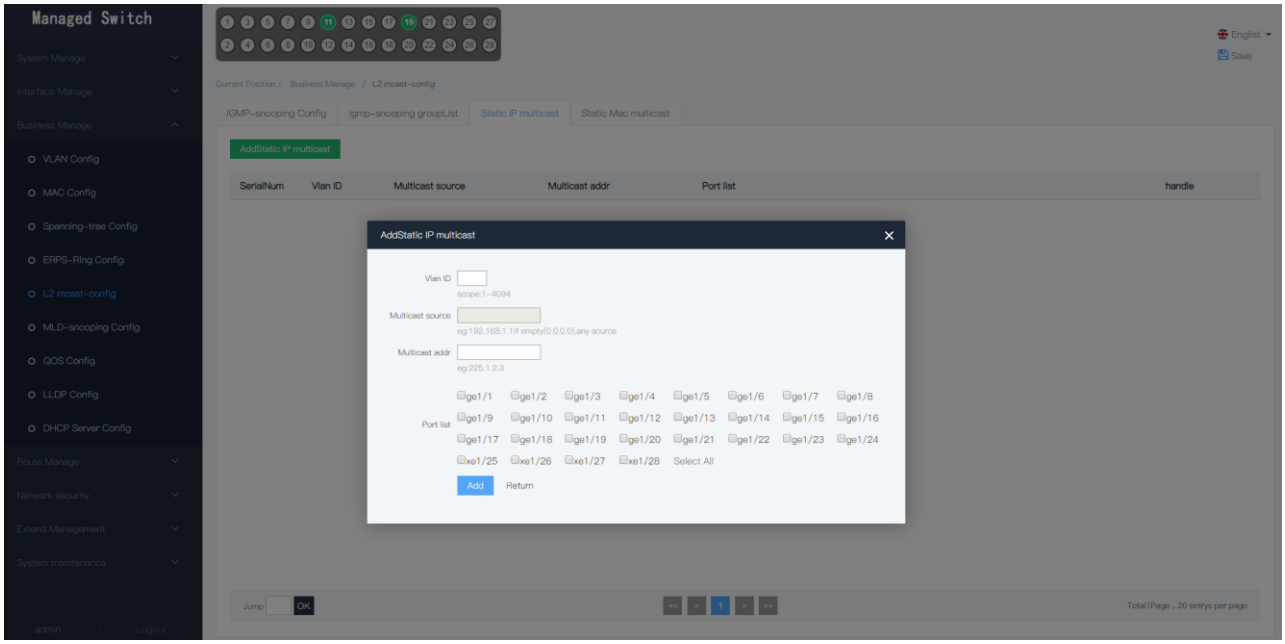
MCAST APPLY

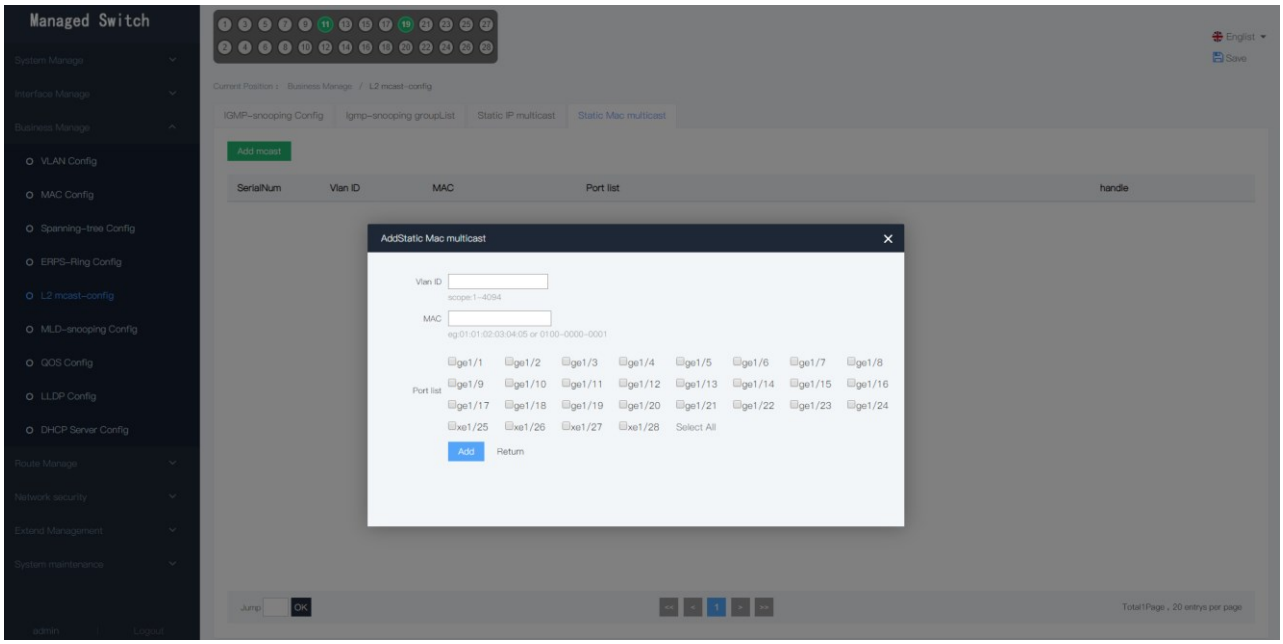
View and add multicast.



STATIC MULTICAST

Static multicast group, where ports to be set are manually added to a multicast group. If the multicast source is arbitrary, it can not be filled in.





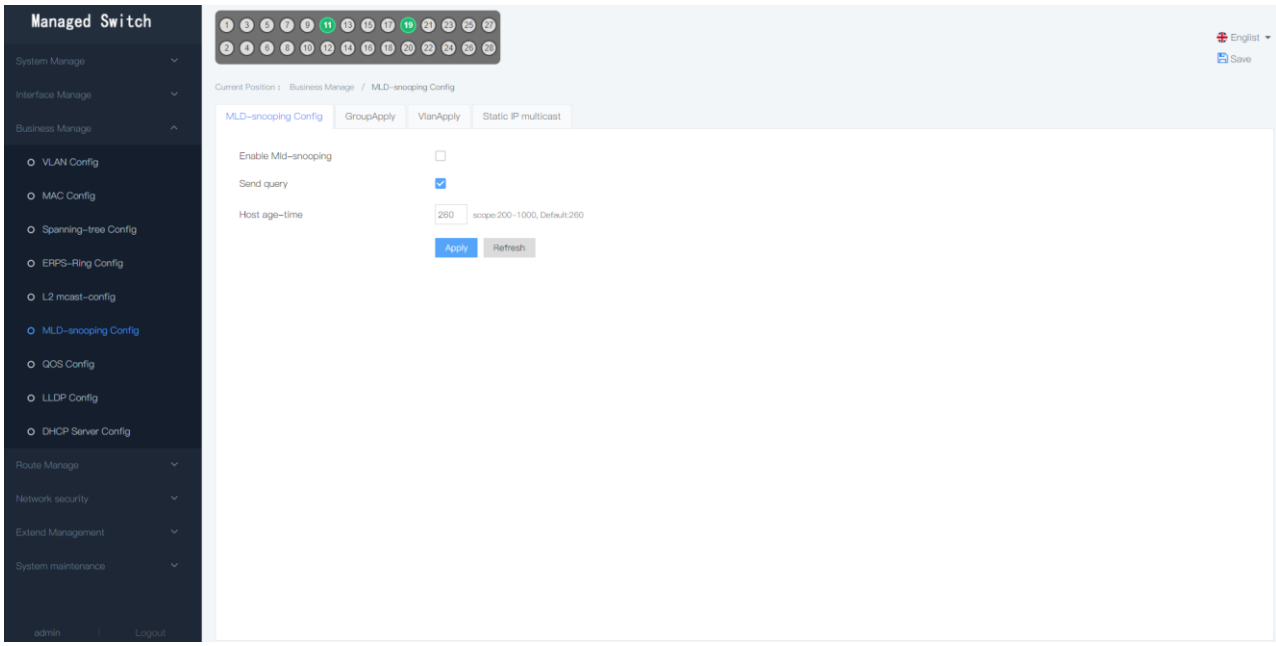
5.3.6 MLD-snooping Config

MLD Snooping is short for Multicast Listener Discovery Snooping. It runs the IPv6 multicast constraint mechanism on Layer 2 devices to manage and control IPv6 multicast groups.

It analyzes the received MLD packets, establishes a mapping relationship between the port and the MAC multicast address, and forwards the IPv6 multicast data according to the mapping relationship.

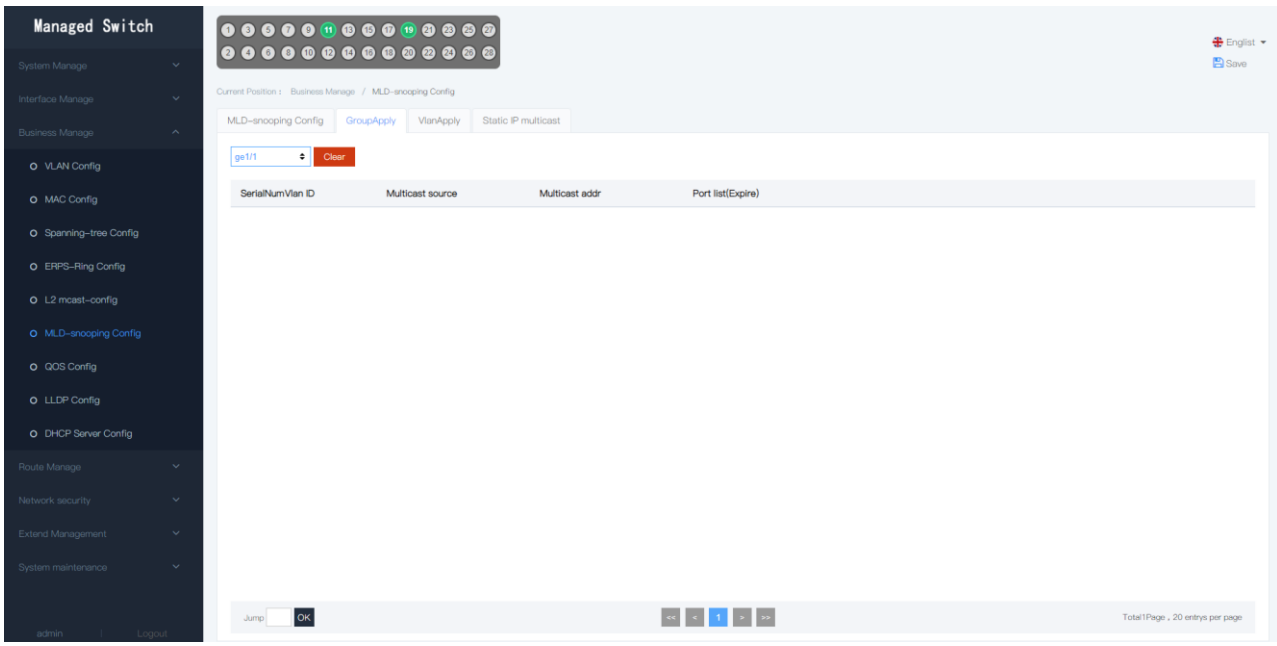
MLD-snooping config

This page is used to enable mld-snooping, start sending packets, and set the aging time.

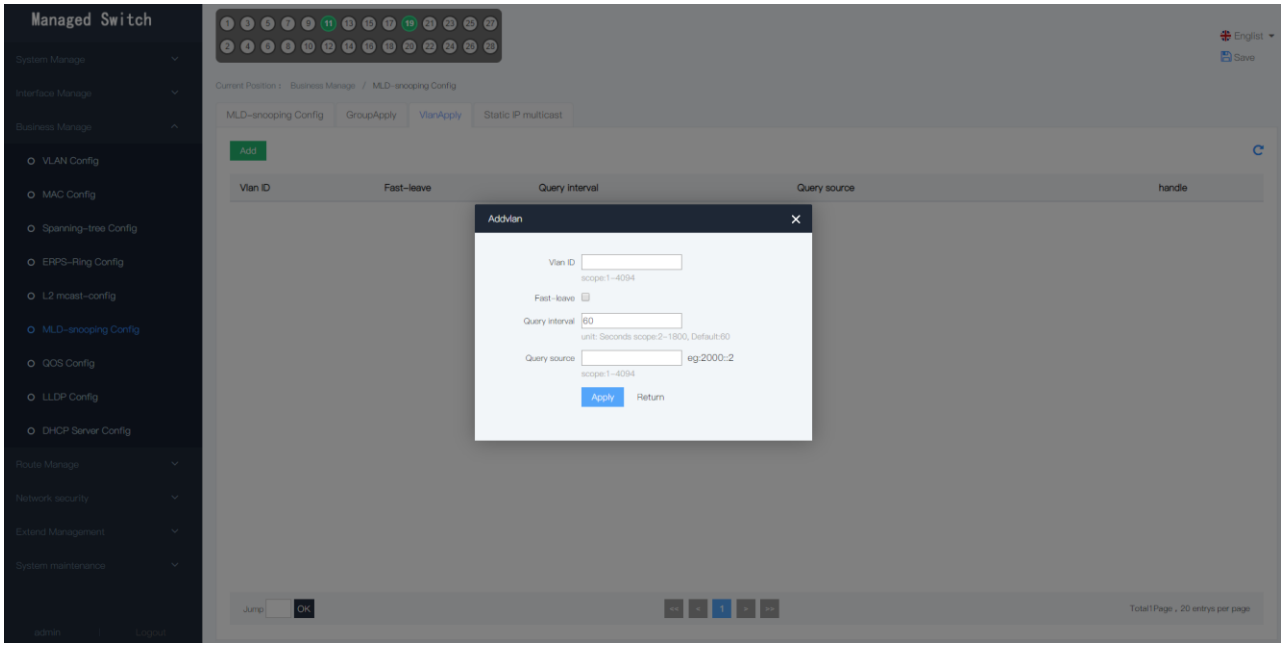


The following is the page for adding group, VLAN, and static IP to mld-snooping.

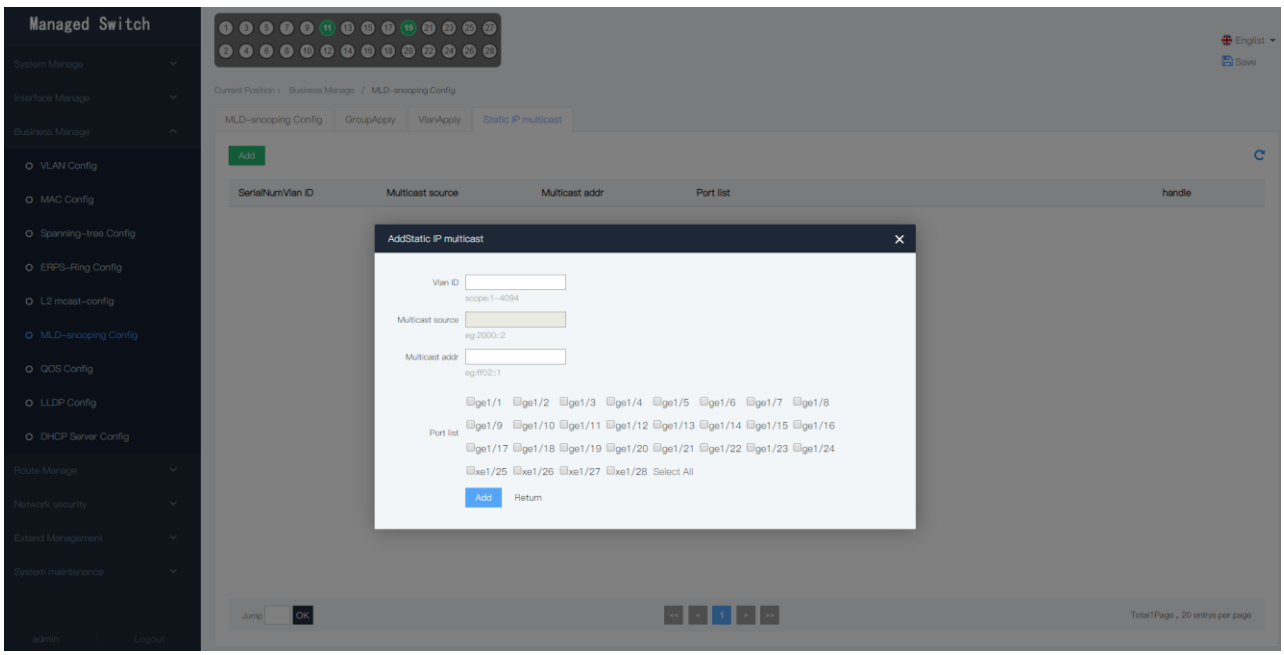
Group Apply



Vlan Apply



Static IP multicast



5.3.7 QOS Config

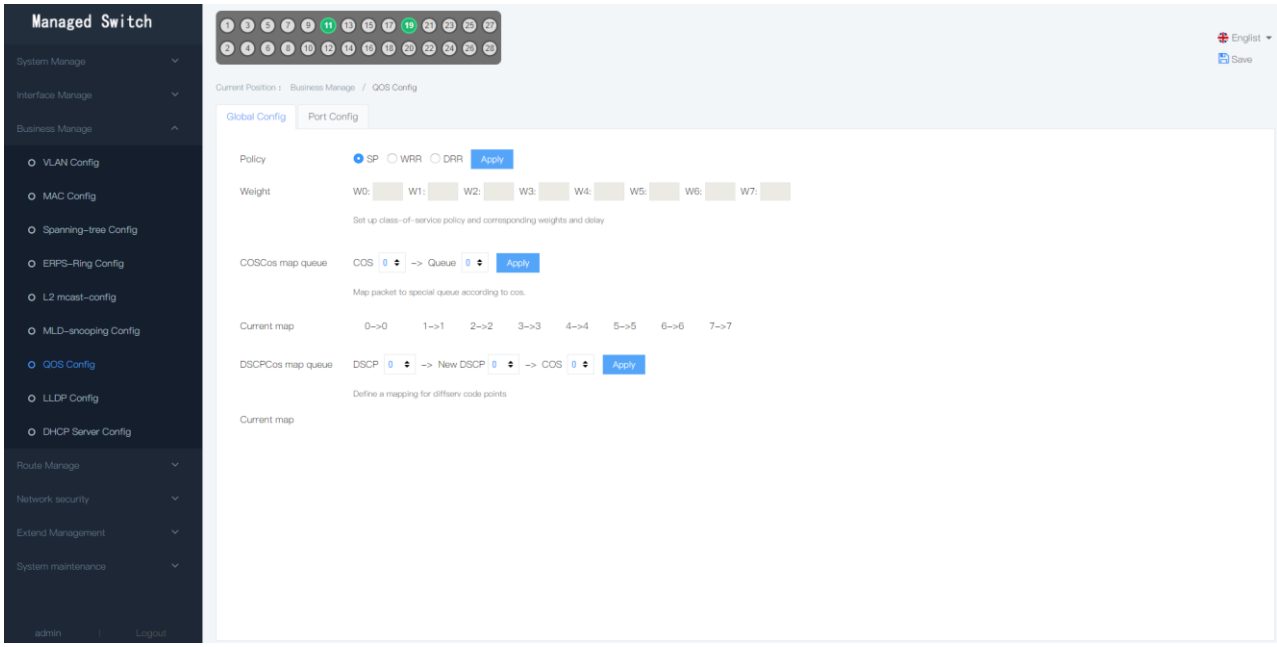
QOS (Quality of Service): For network services, the quality of service includes the bandwidth of transmission, the delay of transmission, the packet loss rate, etc. in the network, the quality of service can be improved by guaranteeing the bandwidth of the transmission, reducing the transmission delay, reducing the packet loss rate and the delay jitter.

Global config

SP: Strictly prioritize and implement the first-in-first-out principle. The default is strict priority and no configuration is required.

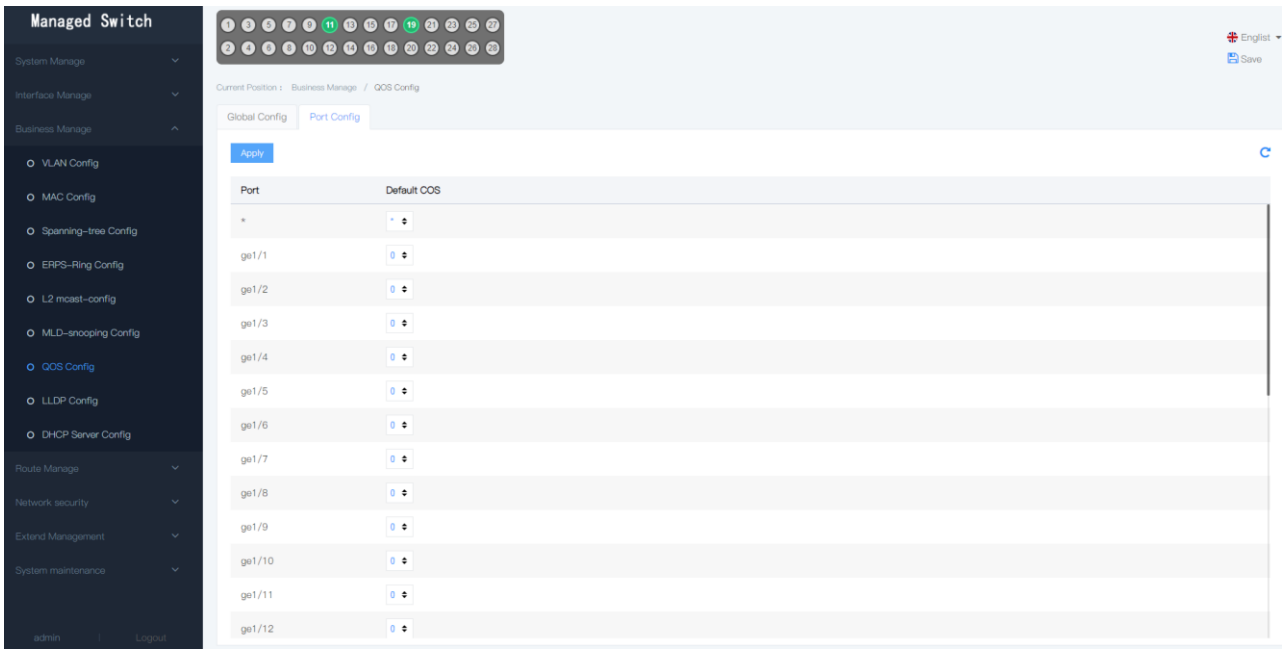
WRR：The weighted queue scheduling in wrr is the same as the weight of a packet with a length of 1518 frames and 64 frames, which may result in unfair scheduling, and the data of all large packets will take up more bandwidth.

DRR: bite schedules weighted, that is, regardless of the size of the frame, eventually scheduling at the data rate.



Port Config

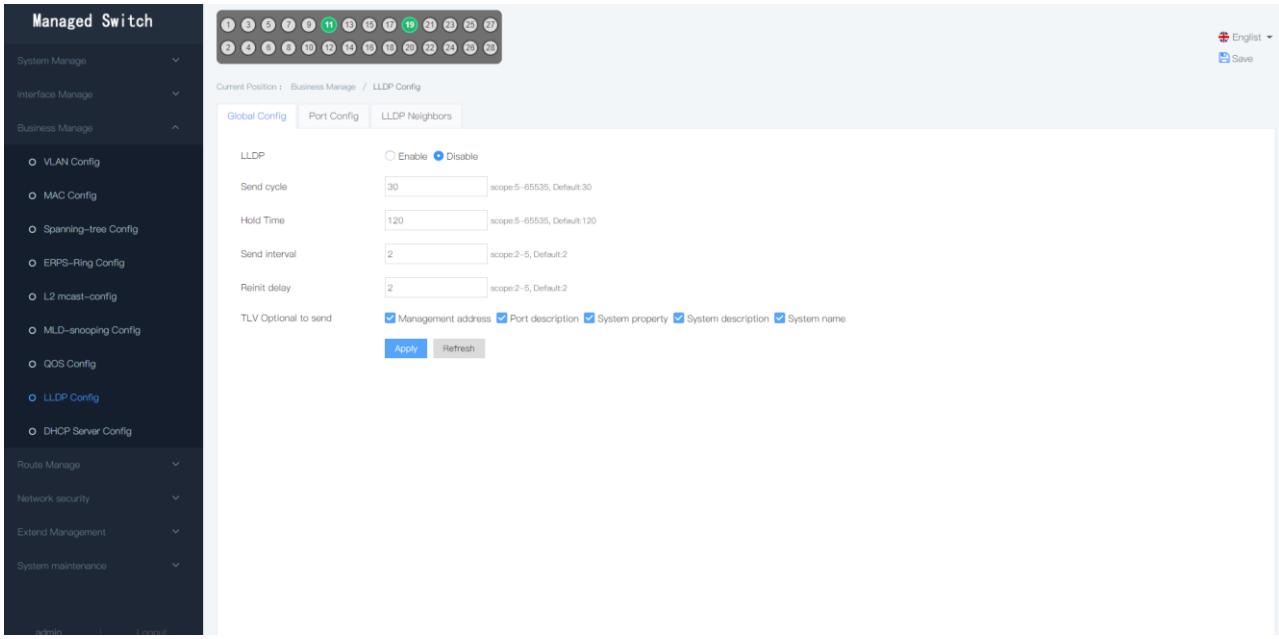
The direct port corresponds to the configuration cos value and selects the priority of the current port. Global configuration to modify the scheduling policy to the corresponding WRR or DRR mode.

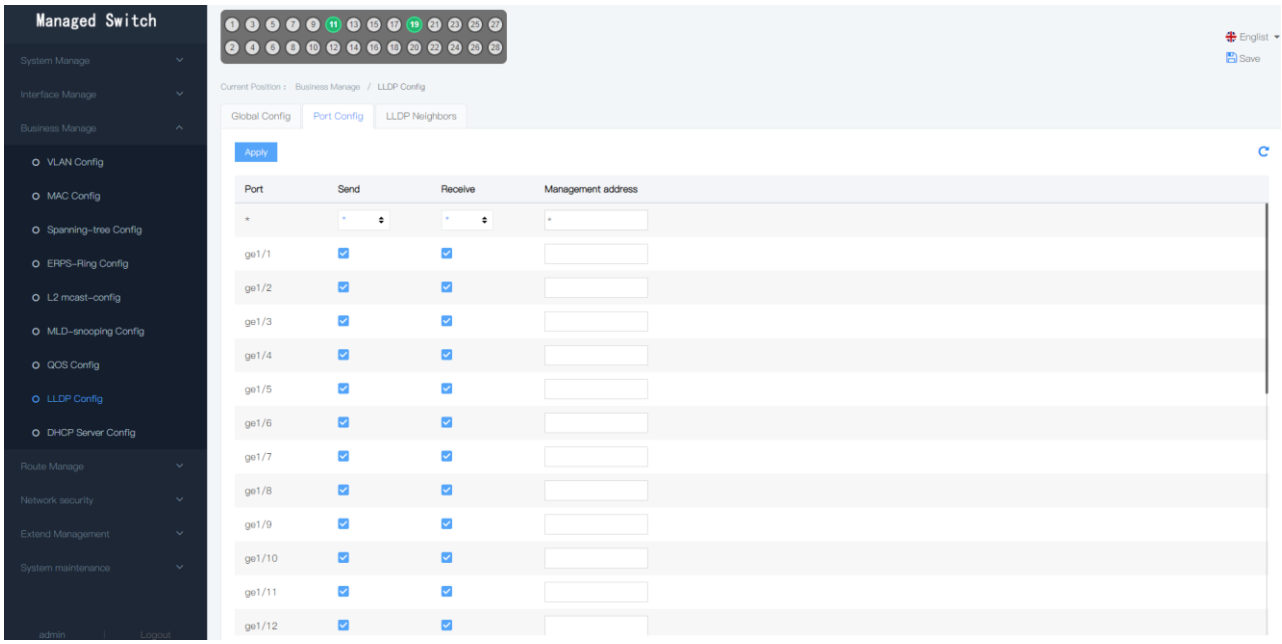


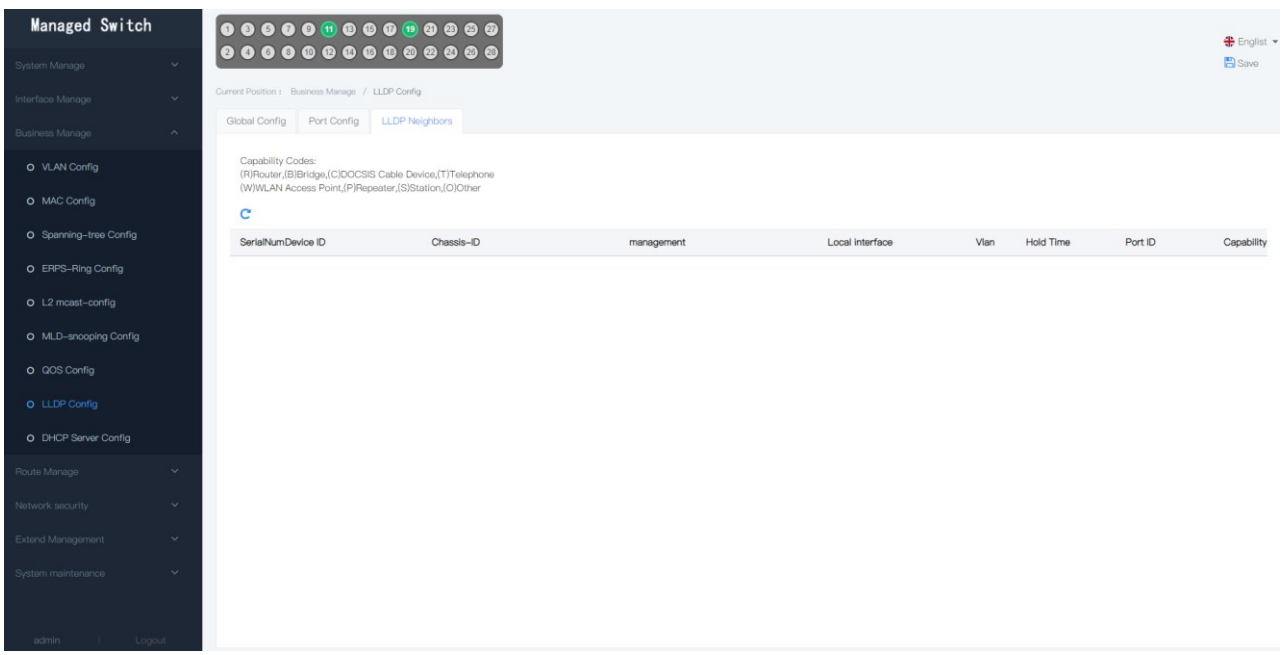
5.3.8 LLDP Config

The link layer discovery protocol (LLDP) is a vendor independent two level protocol, which allows network devices to notify their device identities and performance in the local subnet.

Open the protocol configuration parameter in the global configuration, fill in the management IP address through port configuration, and view the information in the LLDP neighbor.


Managed Switch
System Manage
Interface Manage
Business Manage
VLAN Config
MAC Config
Spanning-tree Config
ERPS-Ring Config
L2 mcast-config
MLD-snooping Config
QOS Config
LLDP Config
DHCP Server Config
Route Manage
Network security
Extend Management
System maintenance
admin
Logout
Englist
Save
Current Position : Business Manage / LLDP Config
Global Config
Port Config
LLDP Neighbors
LLDP
Enable
Disable
Send cycle
30
scope:5-65535, Default:30
Hold Time
120
scope:5-65535, Default:120
Send interval
2
scope:2-5, Default:2
Reinit delay
2
scope:2-5, Default:2
TLV Optional to send
Management address
Port description
System property
System description
System name
Apply
Refresh


Managed Switch
System Manage
Interface Manage
Business Manage
VLAN Config
MAC Config
Spanning-tree Config
ERPS-Ring Config
L2 mcast-config
MLD-snooping Config
QOS Config
LLDP Config
DHCP Server Config
Route Manage
Network security
Extend Management
System maintenance
admin
Logout
Englist
Save
Current Position : Business Manage / LLDP Config
Global Config
Port Config
LLDP Neighbors
Apply
Port
Send
Receive
Management address
ge1/1
ge1/2
ge1/3
ge1/4
ge1/5
ge1/6
ge1/7
ge1/8
ge1/9
ge1/10
ge1/11
ge1/12


Managed Switch
System Manage
Interface Manage
Business Manage
VLAN Config
MAC Config
Spanning-tree Config
ERPS-Ring Config
L2 mcast-config
MLD-snooping Config
QOS Config
LLDP Config
DHCP Server Config
Route Manage
Network security
Extend Management
System maintenance
admin
Logout
Englist
Save
Current Position : Business Manage / LLDP Config
Global Config
Port Config
LLDP Neighbors
Capability Codes:
(R)Router,(B)Bridge,(C)DOCSIS Cable Device,(T)Telephone
(W)WLAN Access Point,(P)Repeater,(S)Station,(O)Other
SerialNumDevice ID
Chassis-ID
management
Local interface
Vlan
Hold Time
Port ID
Capability

5.3.9 DHCP Server Config

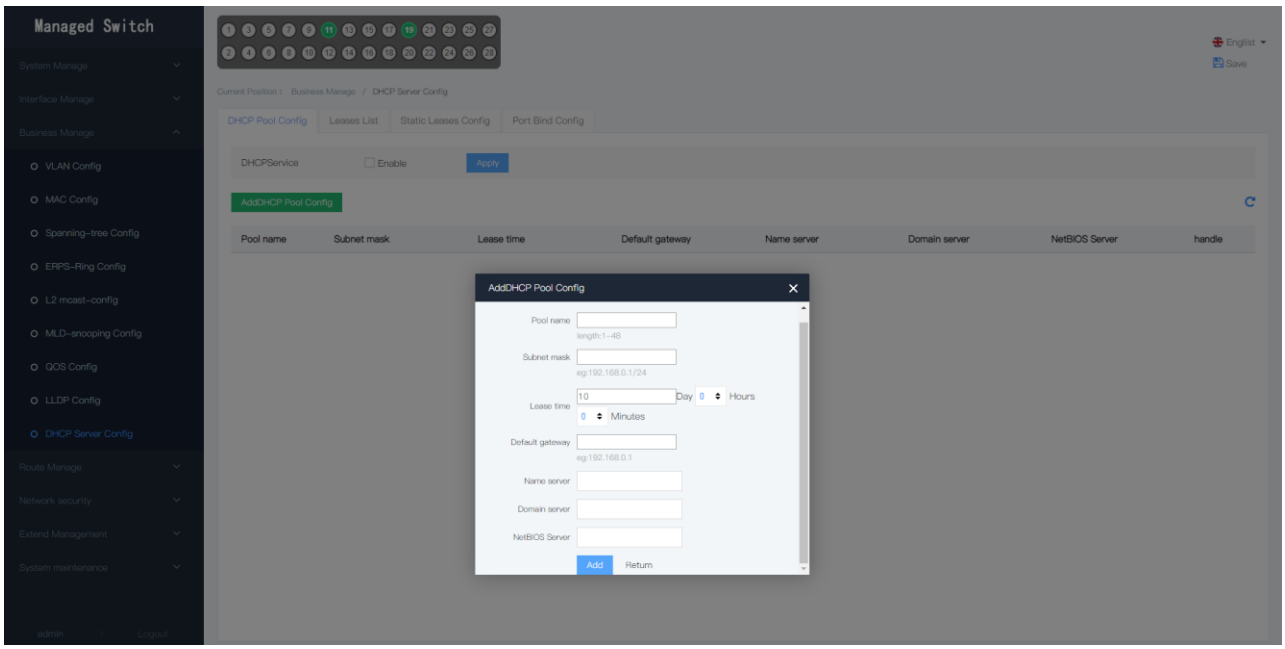
A computer DHCP server that manages the DHCP standard in a particular network is responsible for assigning IP addresses when a workstation logs in. And make sure that the IP address assigned to each workstation is different and that the DHCP server greatly simplifies some of the network management tasks that previously needed to be done manually.

DHCP POOL CONFIG

Default gateway: A configuration item for the TCP/IP protocol that is the IP address of a directly reachable IP router.

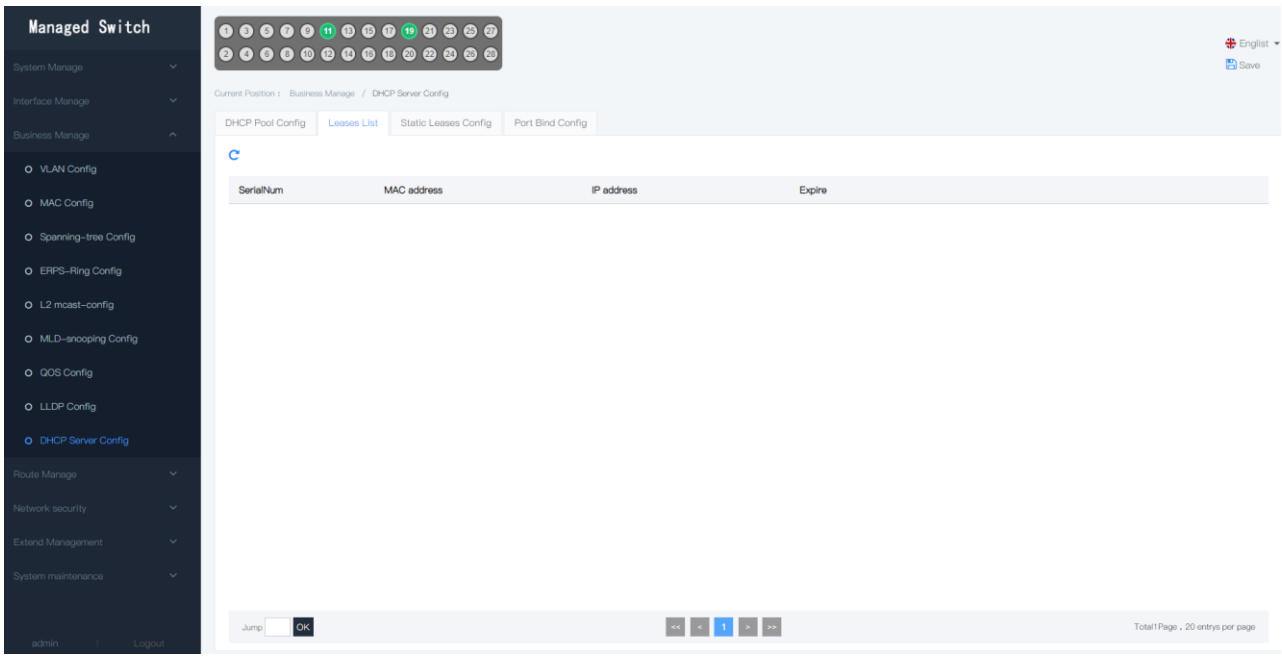
Domain server, Name server: Converting a domain name into an IP address that can be identified by the network.

NetBIOS Server: The correspondence between Host name and IP in LAN.



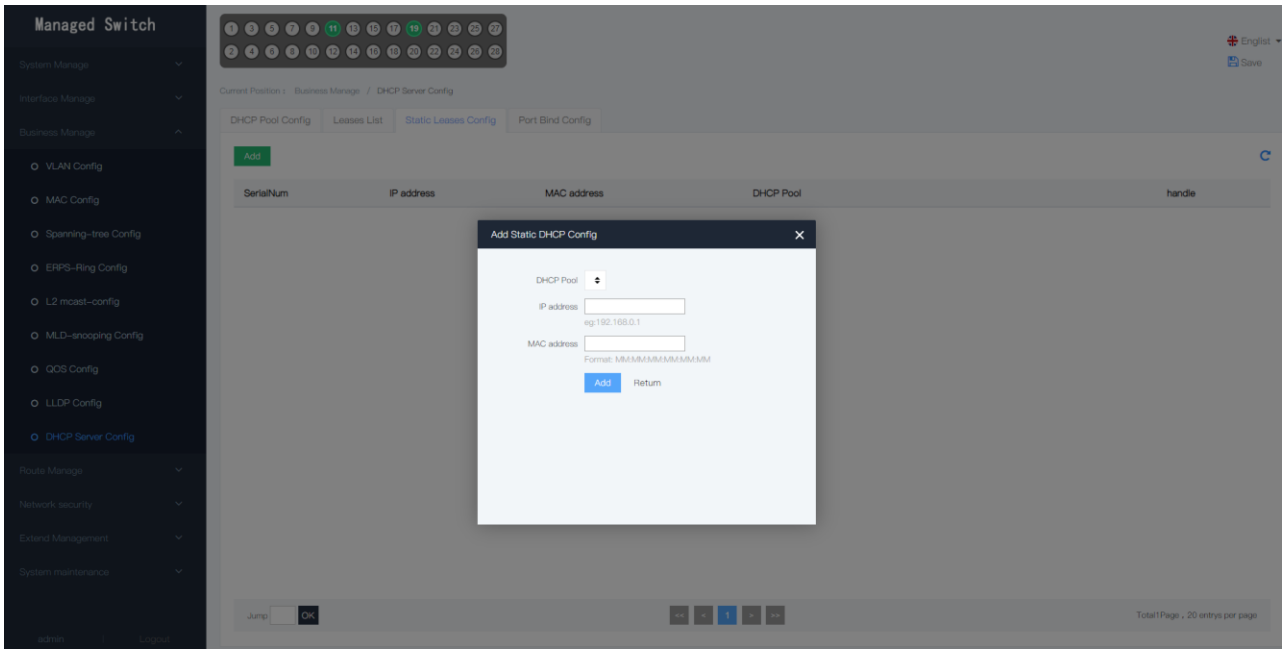
LEASES LIST

Display Leases list



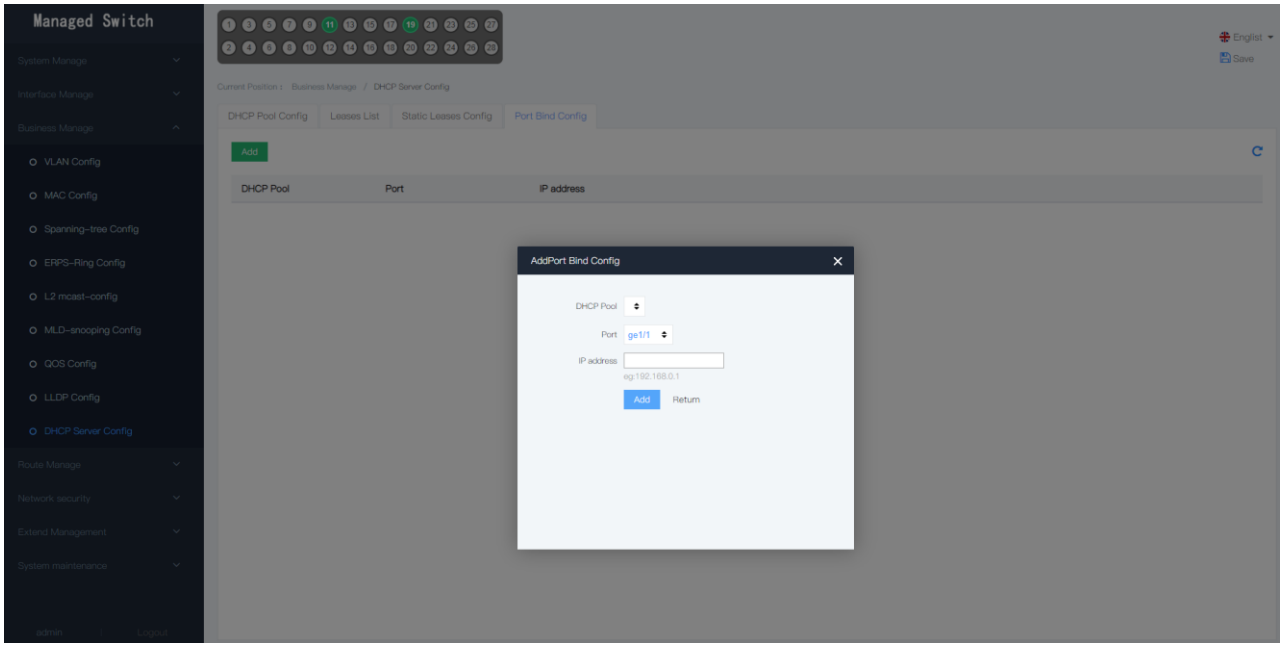
STATIC LEASES CONFIG

The DHCP server administrator manually specifies an IP address and passes it over the DHCP protocol to the client for use.



PORT BIND CONFIG

Bind a port to an IP address that can only be used on that port by binding an IP address.



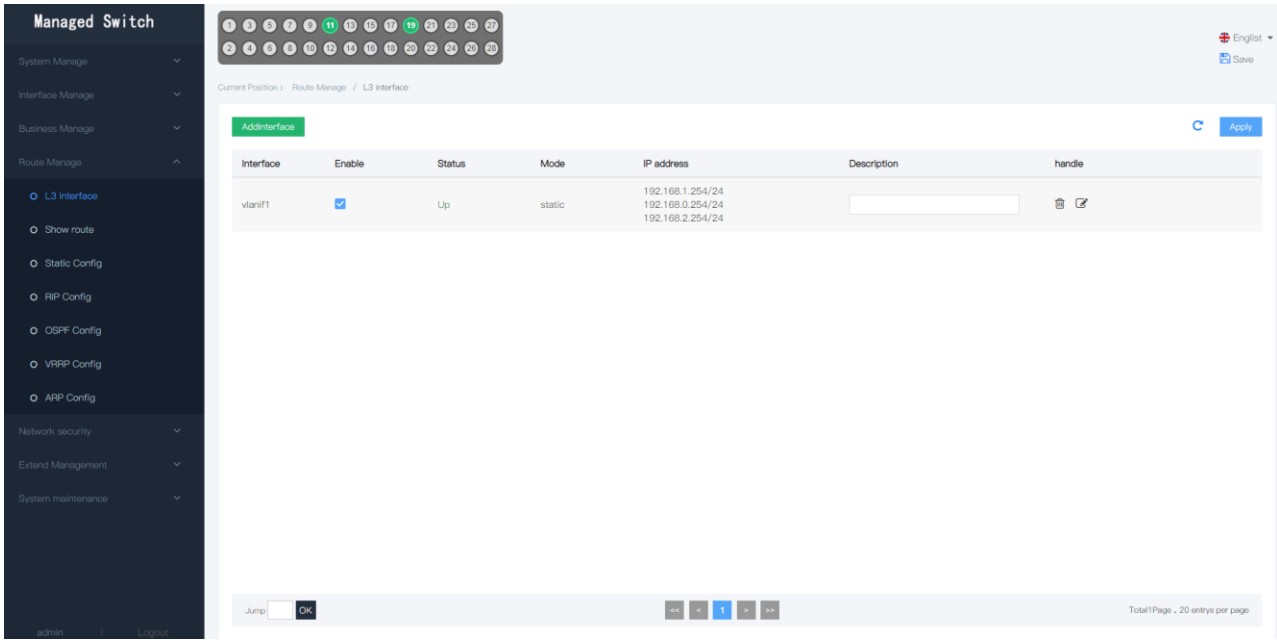
5.4 Route Manage

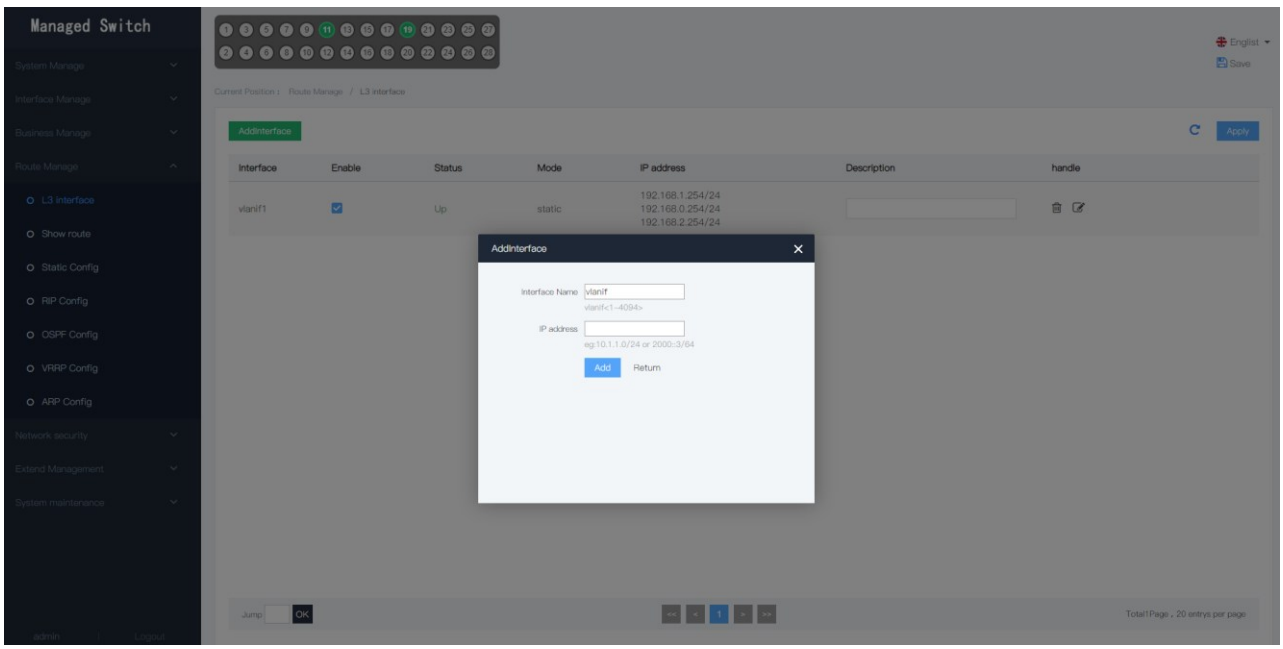
In the network, the router selects a suitable path according to the destination address of the received packet, and forwards the message to the next router. The last router in the path is responsible for forwarding messages to the destination host. Routing is the path information in the process of forwarding a message, which is used to direct the forwarding of a message.

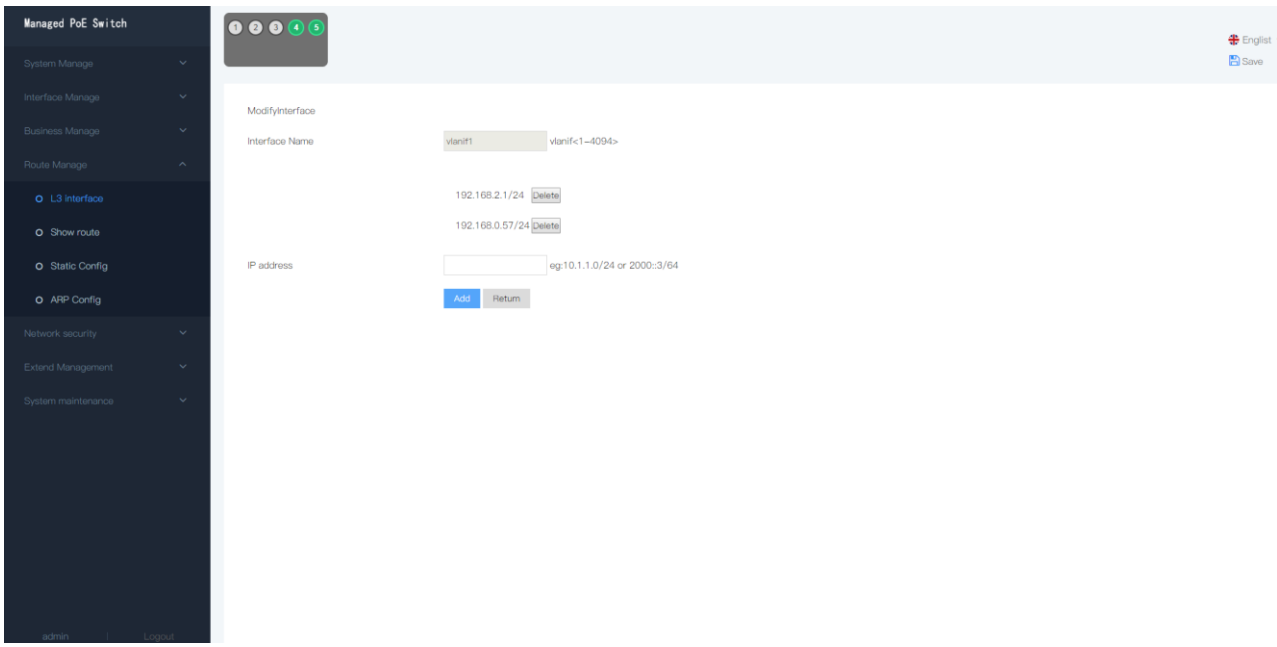
5.4.1 L3 interface

A switch virtual interface corresponds to a VLAN, when it is necessary to route traffic between virtual Lans or non-routing protocols between bridging VLAN, and to provide connections between IP hosts to the switch. You

need to configure the corresponding switch virtual interface for the corresponding virtual local area network.

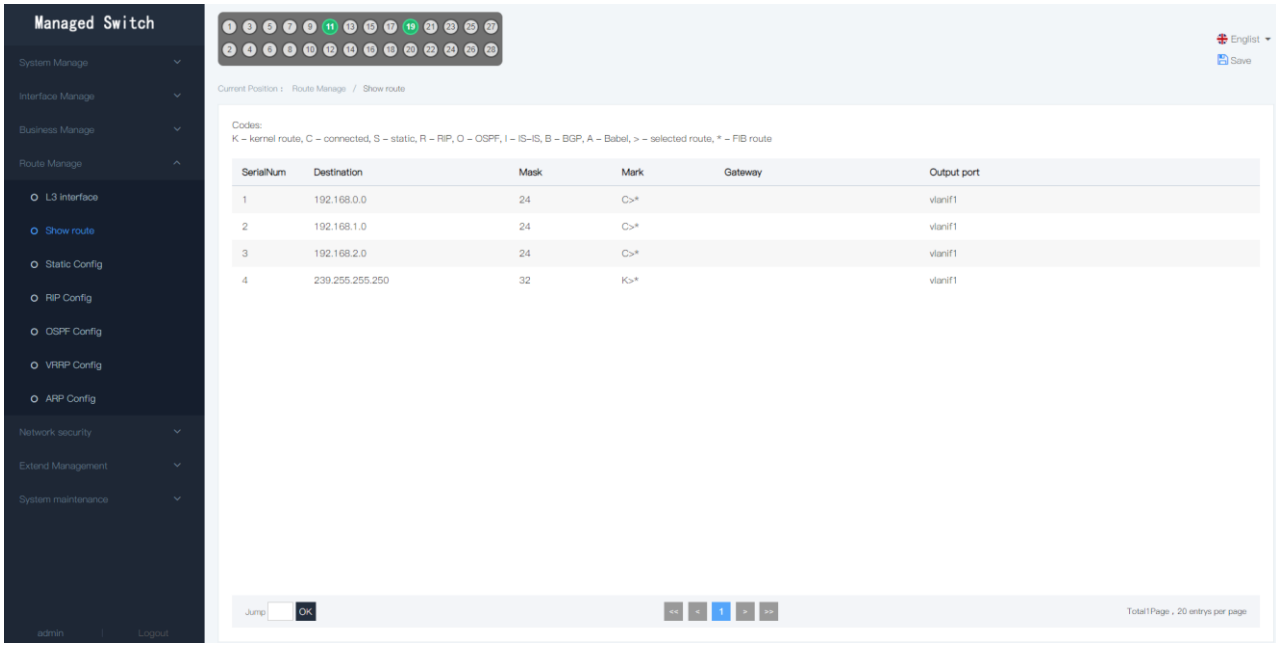






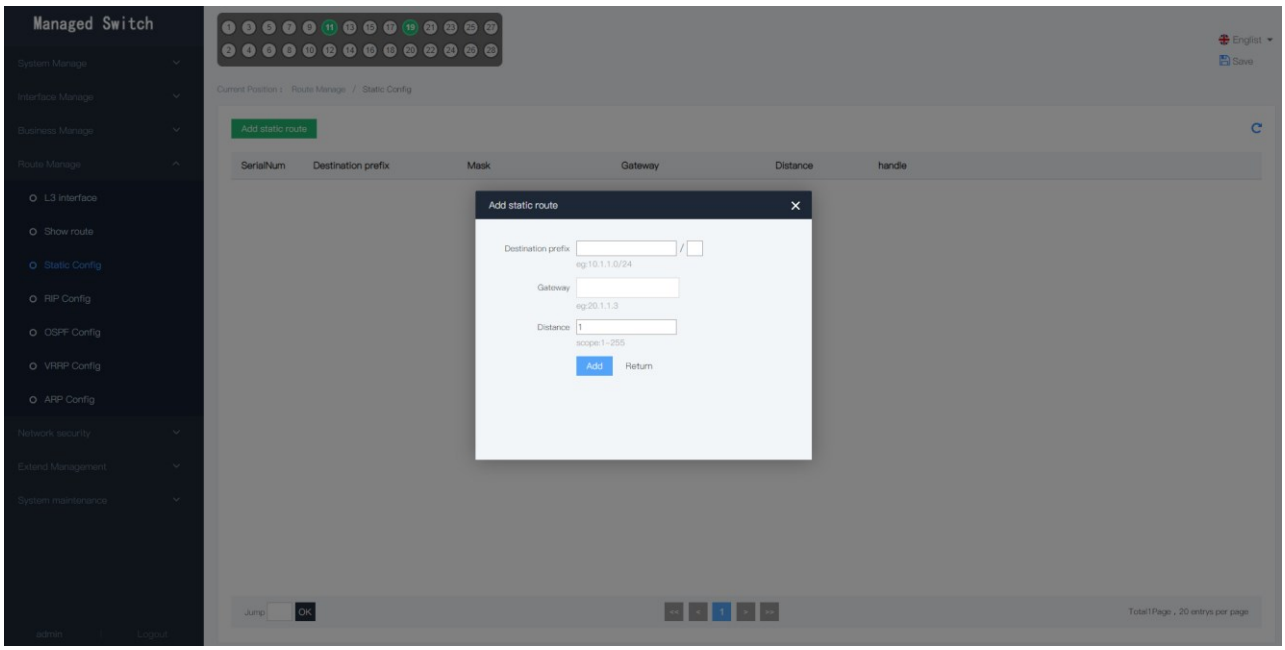
5.4.2 show route

Display switch internal routing information.



5.4.3 Static Config

Static routing is a special route that is manually configured by the administrator. After configuring static routing, the data message to the designated destination will be forwarded according to the administrator's specified path.



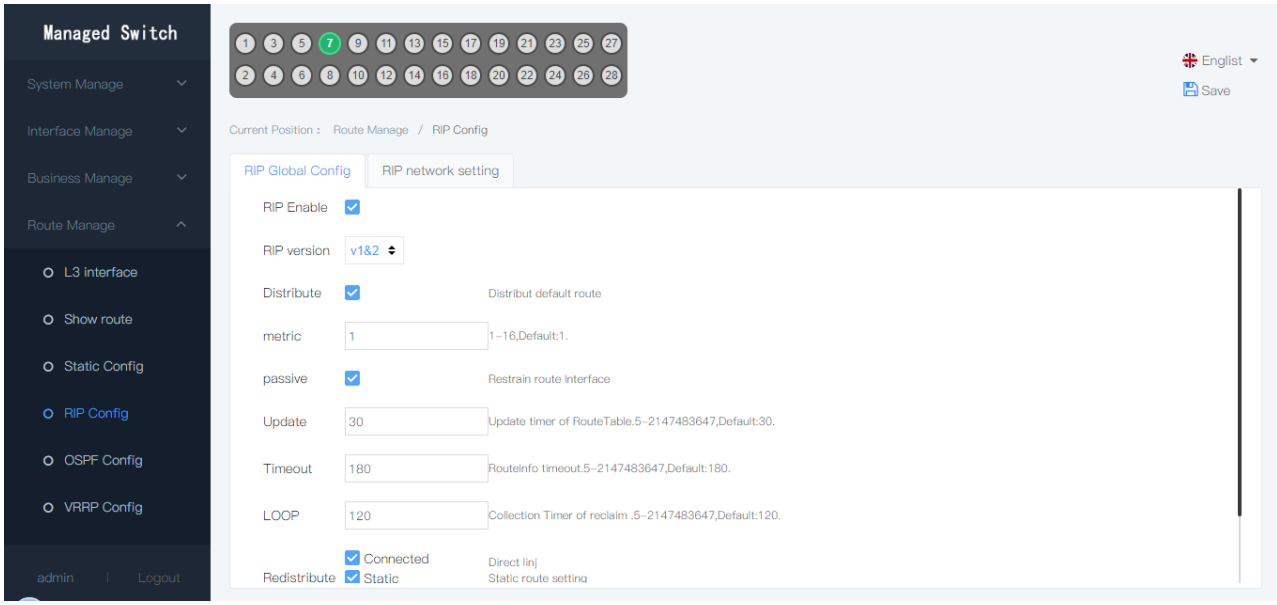
5.4.4 RIP Config

The Routing Information Protocol (RIP) is one of the most widely used Interior Gateway Protocols (IGPs). (IGP) is a routing protocol used on the internal network (in a few cases, it can also be used to connect to the Internet), which can dynamically adapt the router to changes in network connectivity by continuously exchanging information, including Which networks can be reached by routers, how far these networks are, and so on. The

RIP protocol uses broadcast or multicast for routing updates, where RIPv1 uses broadcast and RIPv2 uses multicast.

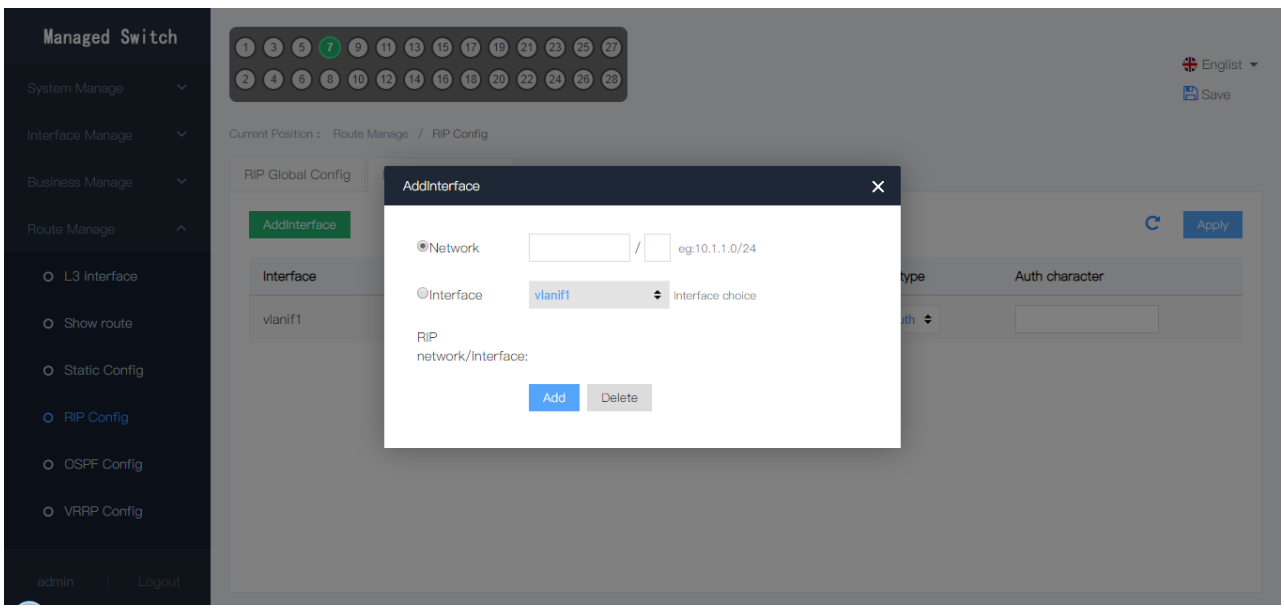
RIP global configuration

Overall configuration of the RIP routing protocol



RIP network configuration

Display Layer 3 interfaces and add RIP routes

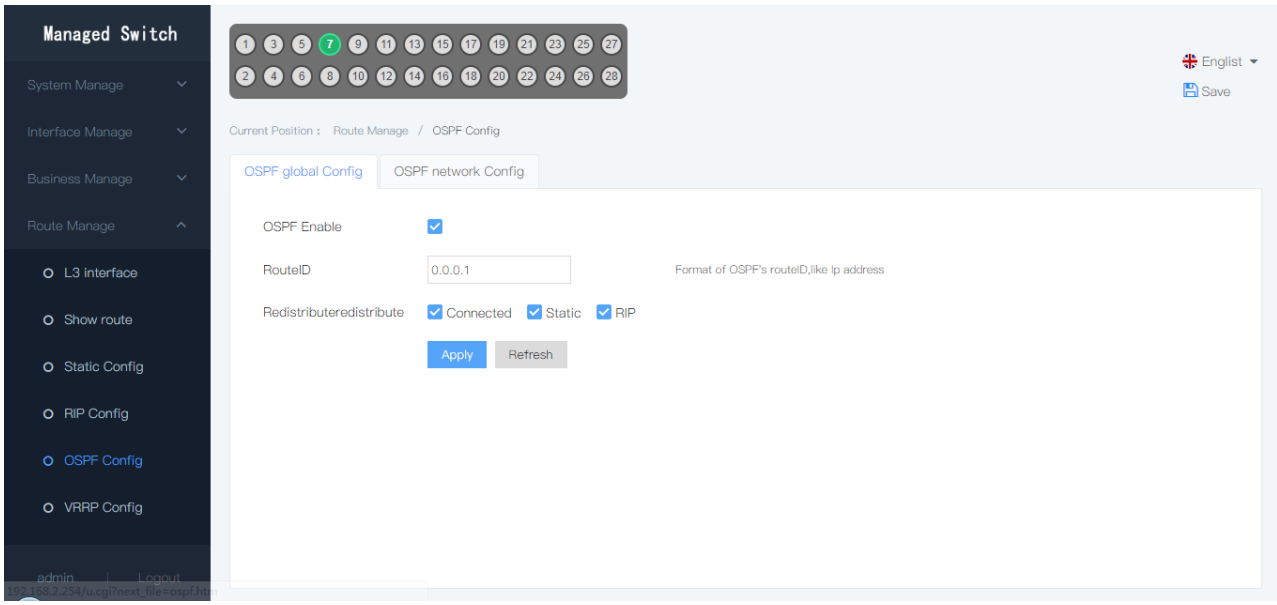


5.4.5 OSPF Config

OSPF (Open Shortest Path First) is an Interior Gateway Protocol (IGP) that is used to determine routes within a single autonomous system (AS).

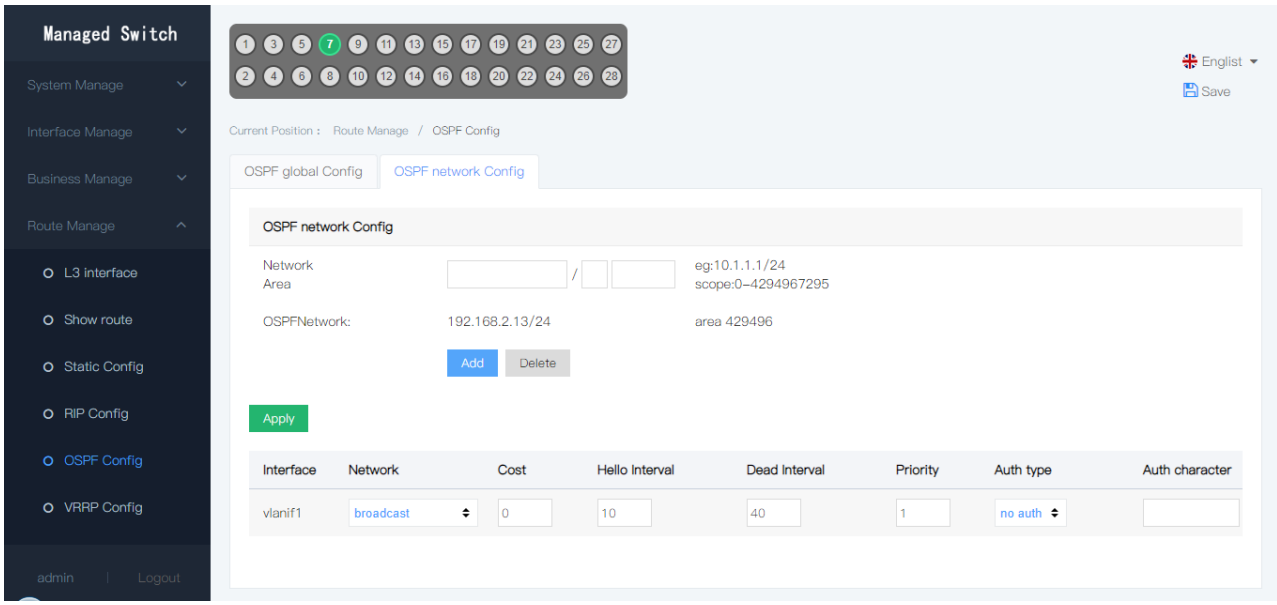
OSPF global config

Enable OSPF and specify the route ID.



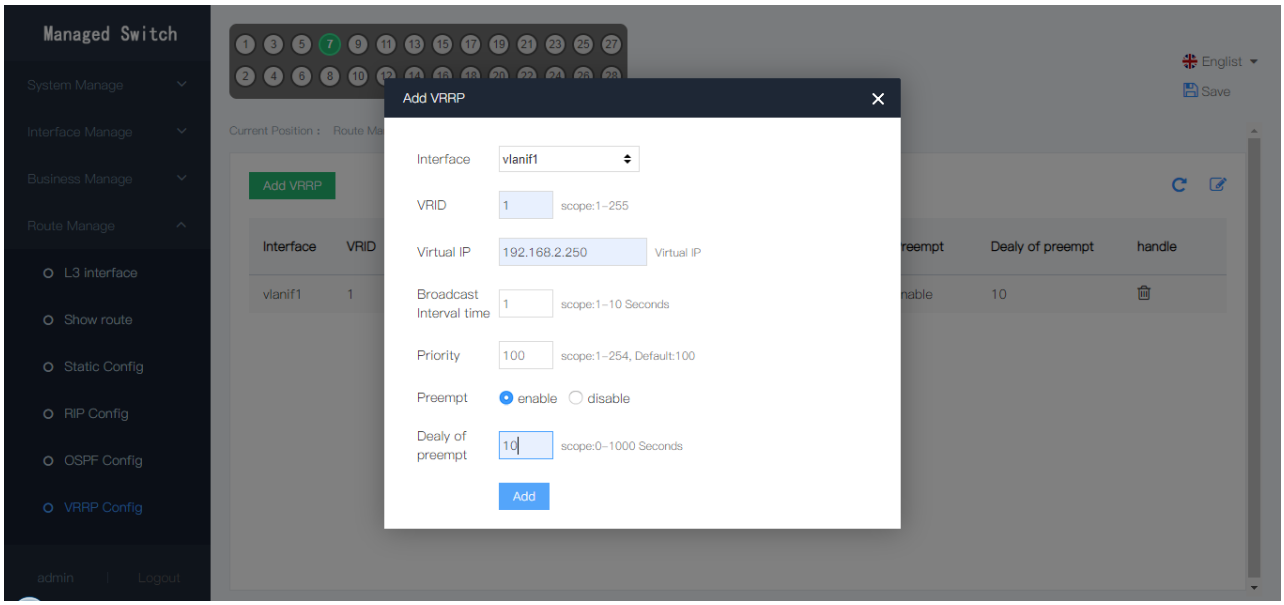
OSPF network config

Specify the area of the network



5.4.6 VRRP Config

VRRP (Virtual Router Redundancy Protocol) is a fault-tolerant protocol. Generally, all hosts in a network are configured with a default route. Therefore, packets sent from the host with the destination address not on the local network segment are sent to the router RouterA through the default route. This implements communication between the host and the external network. When the router RouterA is faulty, all hosts on the local network segment that use RouterA as the next hop of the default route will be disconnected from the external network to generate a single fault.

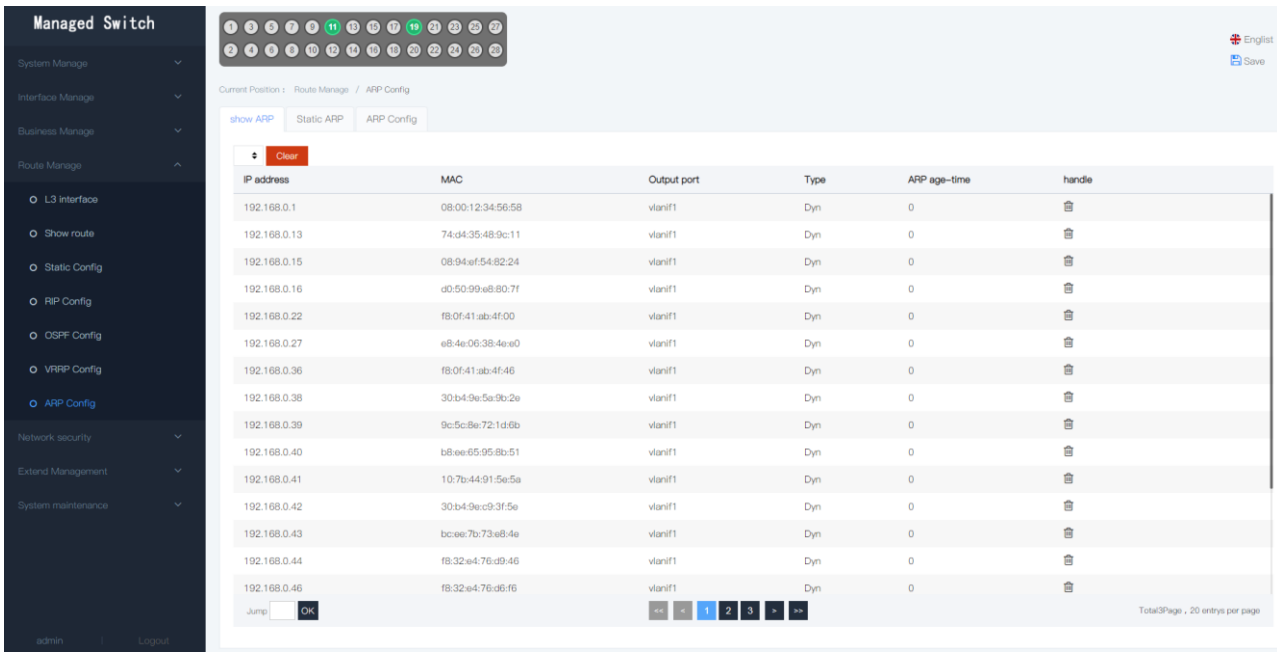


5.4.7 ARP Config

ARP (Address Resolution Protocol) is a TCP/IP protocol for obtaining physical addresses based on IP addresses. When the host sends the information, it broadcasts the ARP request containing the target IP address to all hosts on the network, and receives the return message to determine the physical address of the target. After receiving the return message, the IP address and physical address are stored in the local ARP. The cache keeps a certain amount of time, and the next time the request is made, the ARP cache is directly queried to save resources. The address resolution protocol is based on the mutual trust of each host in the network. The host on the network can send ARP reply messages autonomously. When other hosts receive the response message, they will not detect the authenticity of the message. Enter the local ARP cache;

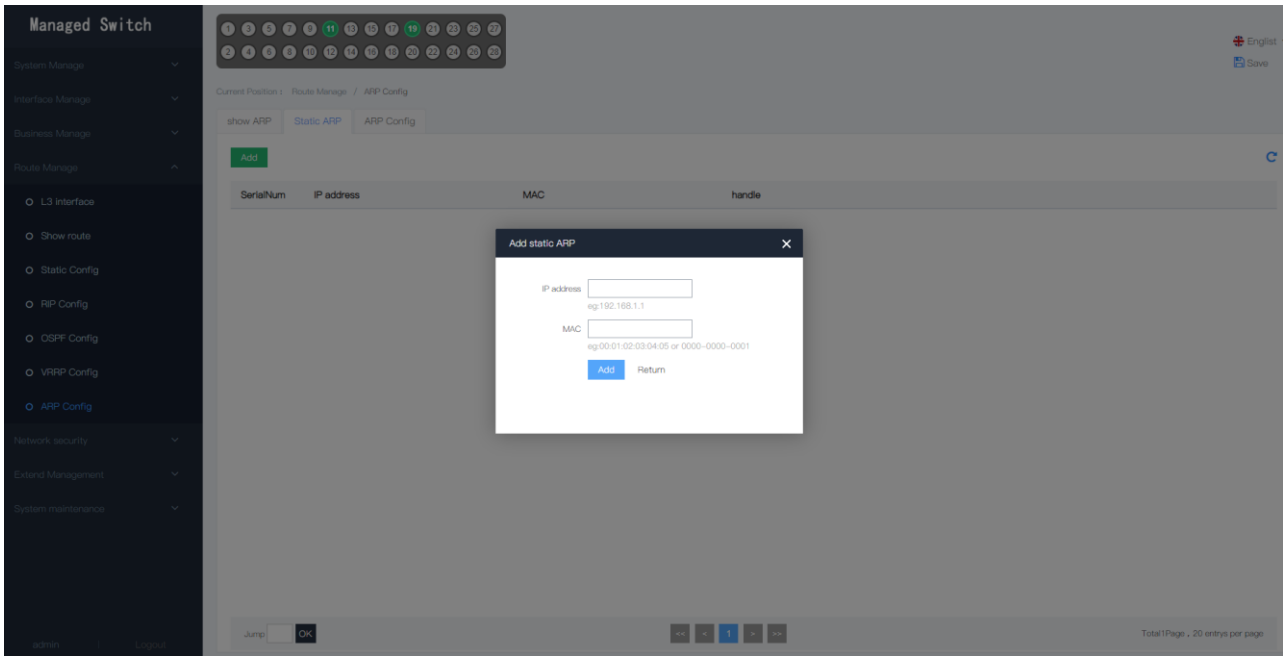
Show ARP

Display arp information



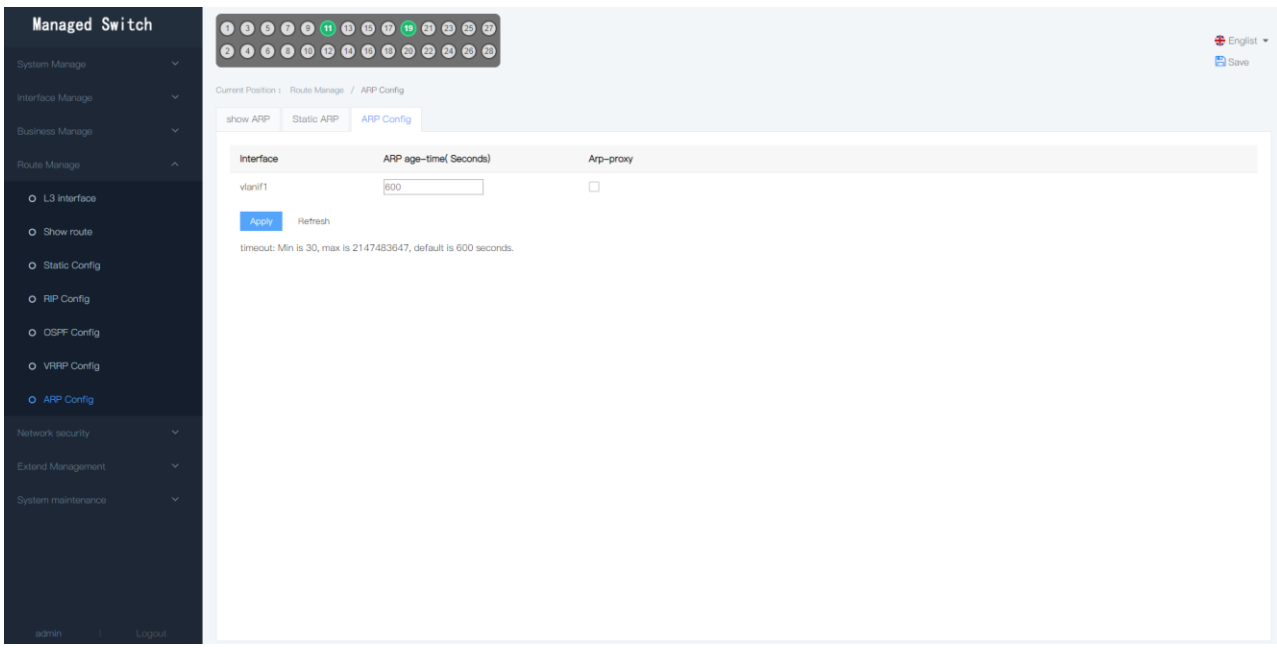
Static ARP

Add and display static ARP tables.



ARP config

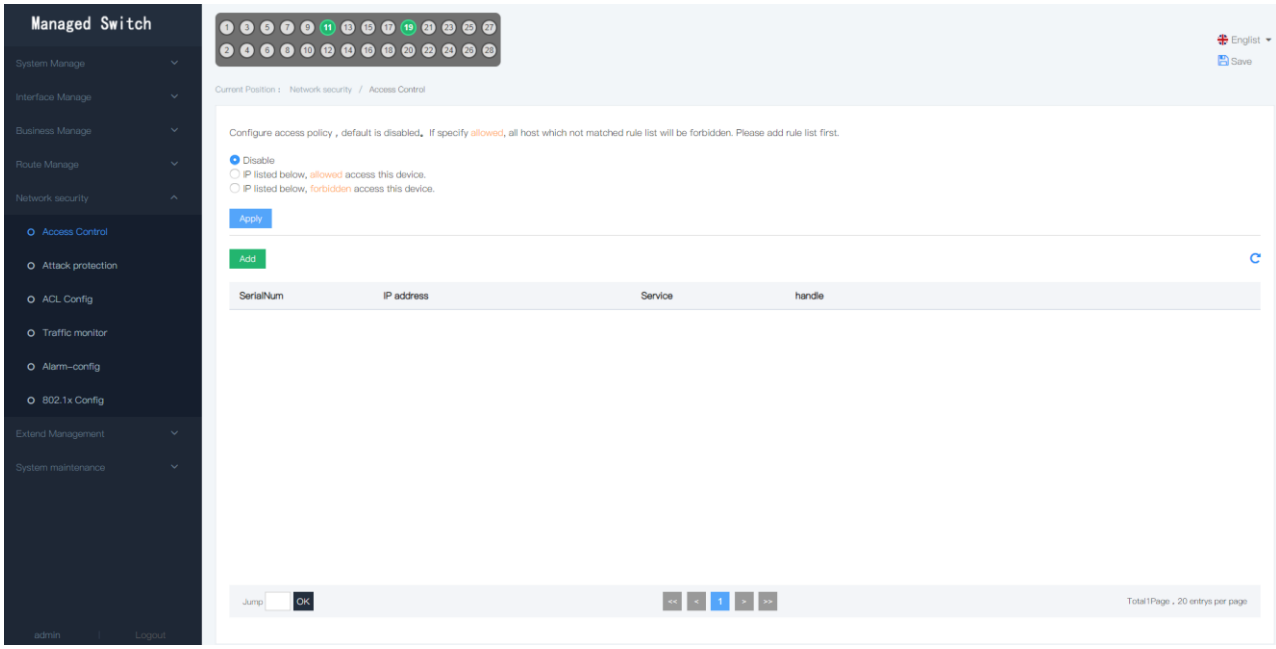
Configure aging time based on dynamic ARP.



5.5 Network Security

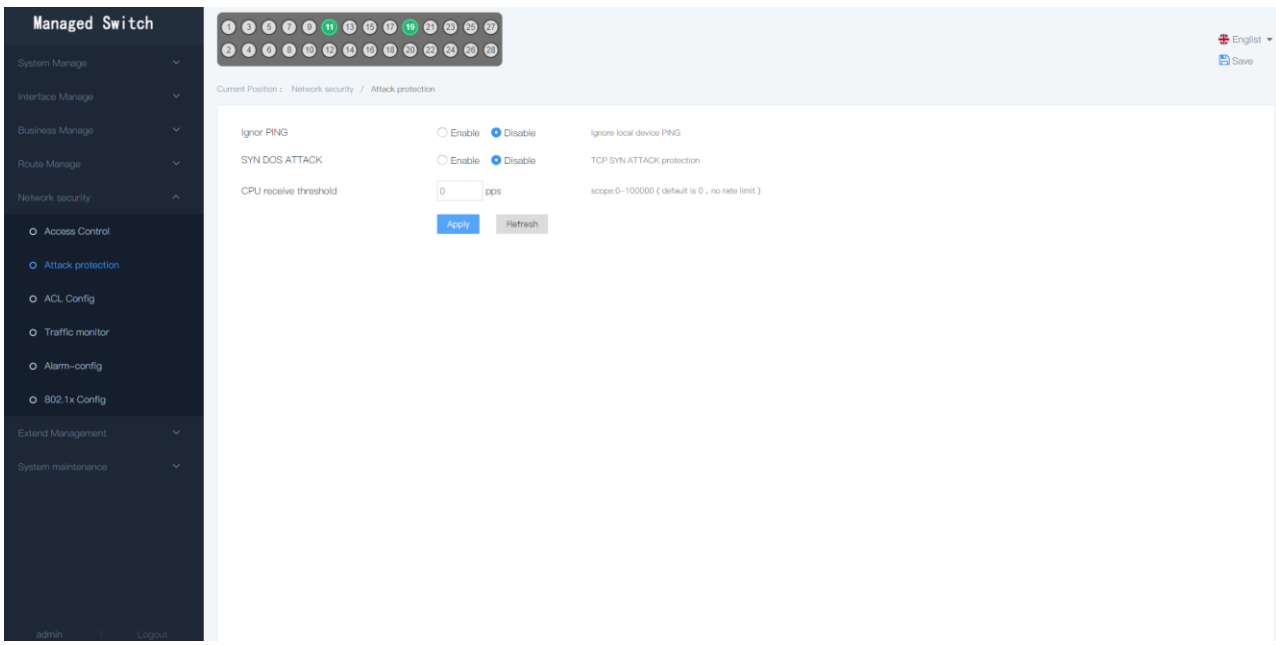
5.5.1 Access Control

Only devices that conform to the access rules can access the switch. Configure access rules before you configure them.



5.5.2 Attack protection

It mainly includes ping packet dos attack, and CPU receive packet threshold setting.

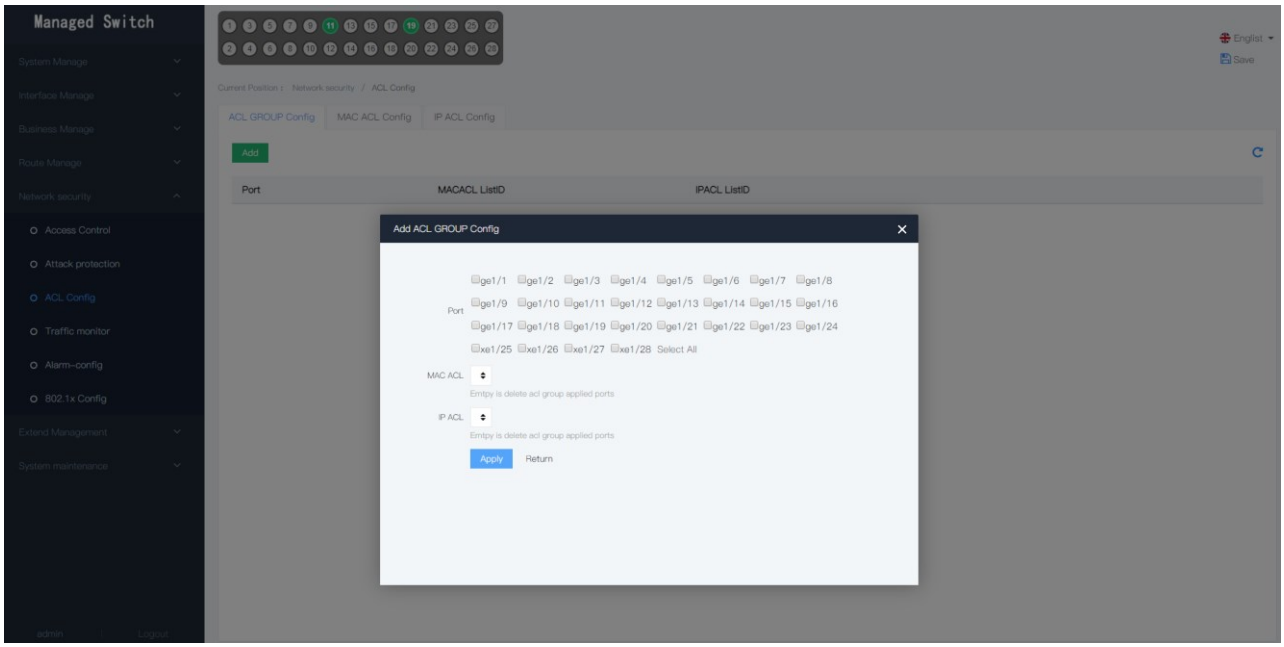


5.5.3 ACL Config

ACL (Accesss Control List) Is a collection of one or more rules used to identify message flows. A rule is a judgment statement that describes the matching conditions of a message. These conditions may be the source address, destination address, port number, etc., of the message.

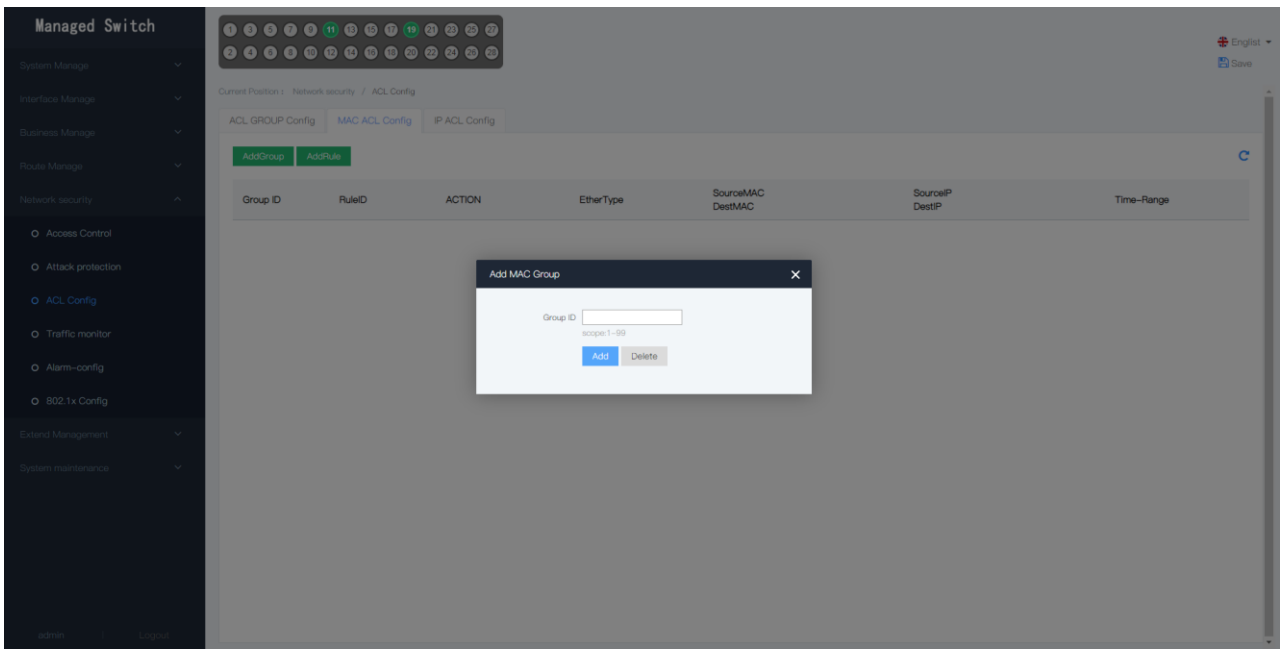
ACL GROUP CONFIG

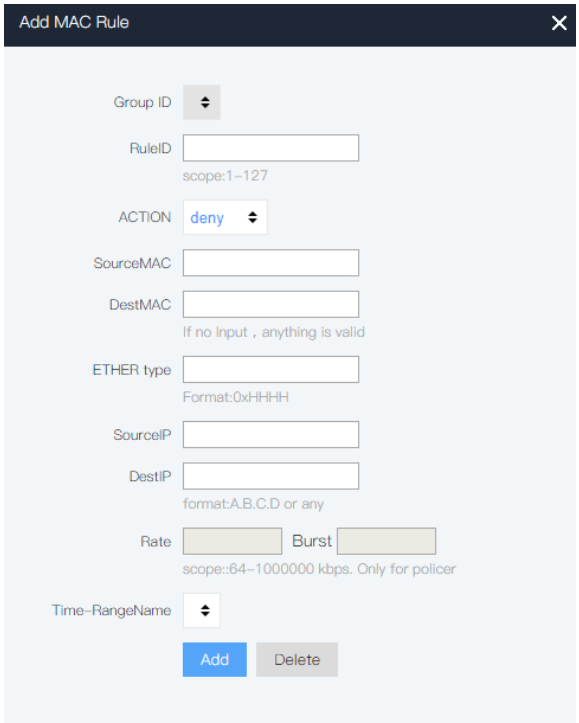
Select the port to execute and the corresponding rule ID to execute.



MAC ACL CONFIG

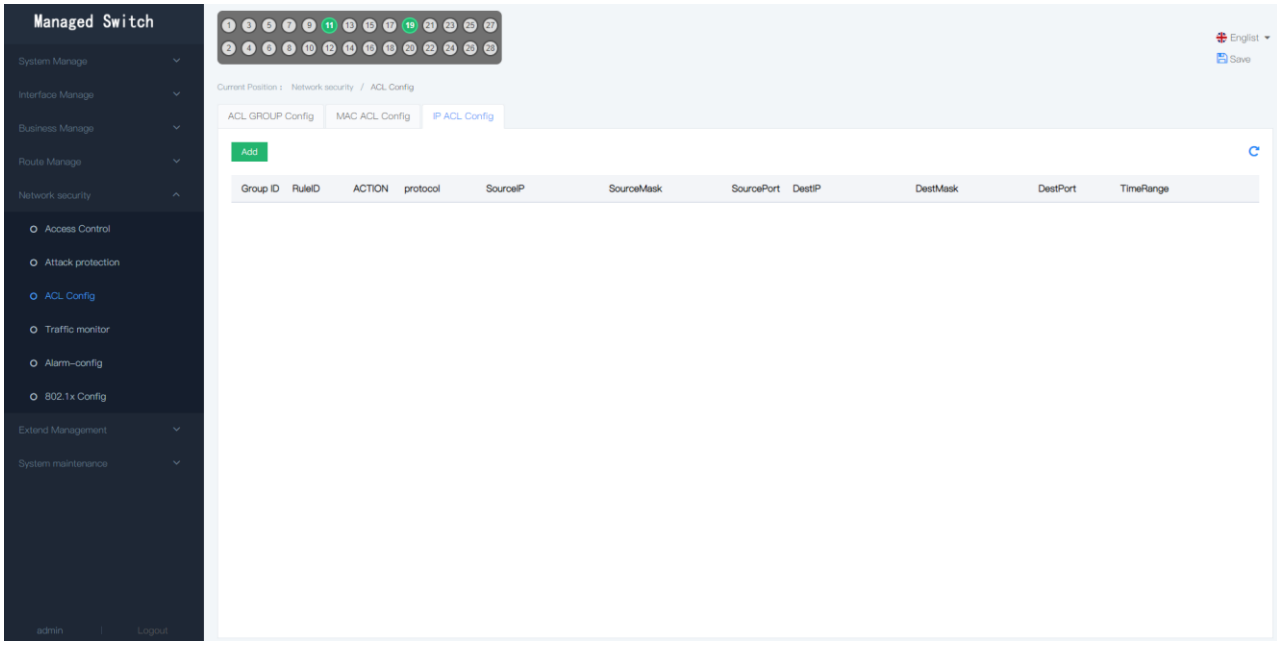
Mac acl to discard or forward the message according to the source mac address and the destination mac address of the message. The greater the value of the rule ID, the higher the priority.

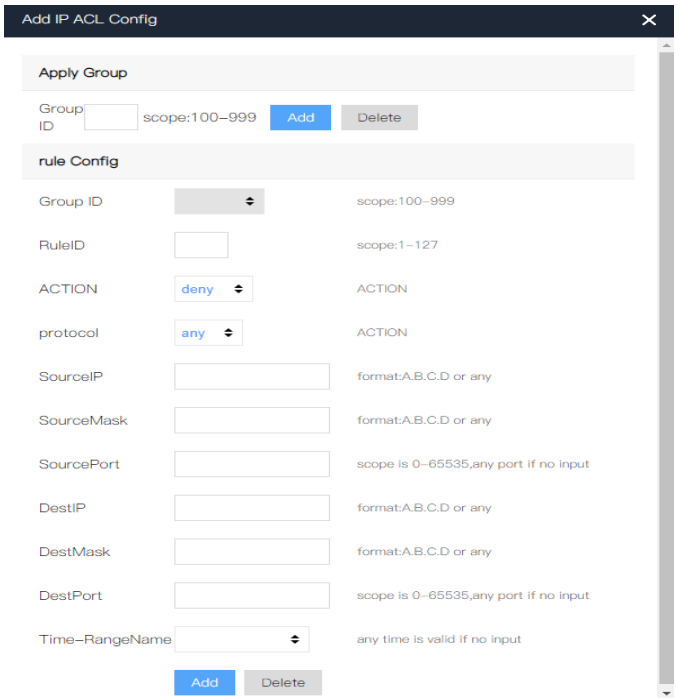




IP ACL CONFIG

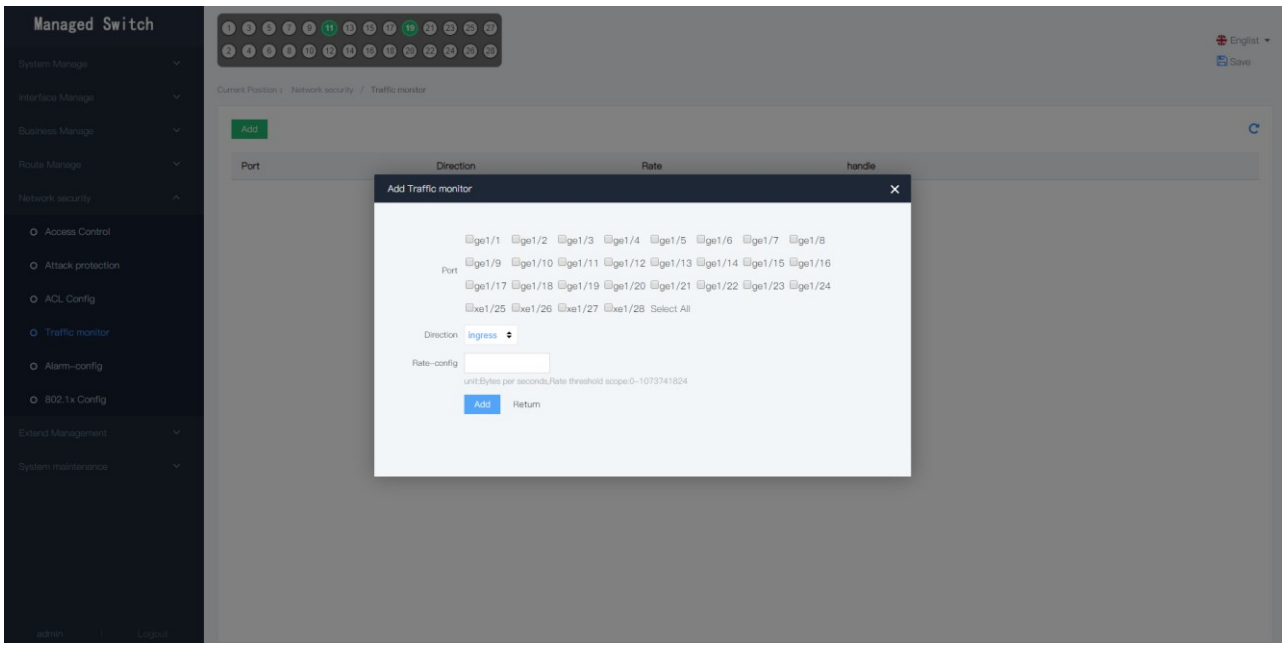
IP MAC based on message protocol, source IP address, source mask, source port number, destination IP address, destination mask and entry To discard or forward a message by its port number.





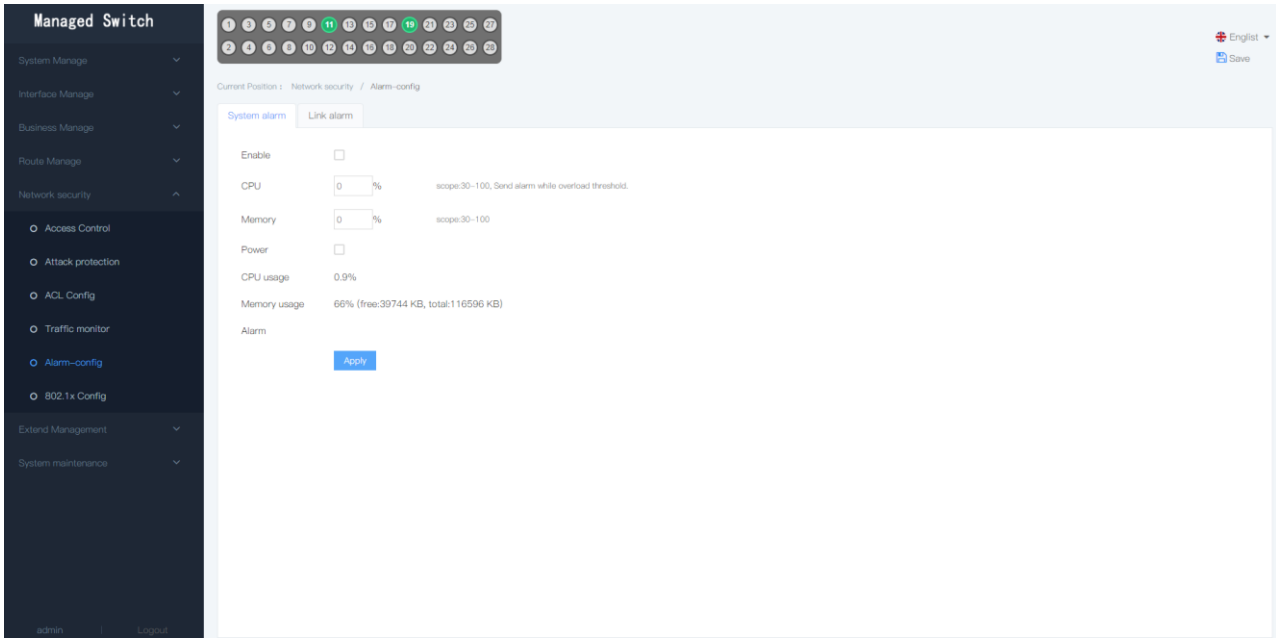
5.5.4 Traffic monitor

The traffic monitoring here is mainly in snmp. For a certain port traffic exceeding the set value trap will automatically send traffic excess information for remote management and monitoring.



5.5.5 Alarm-config

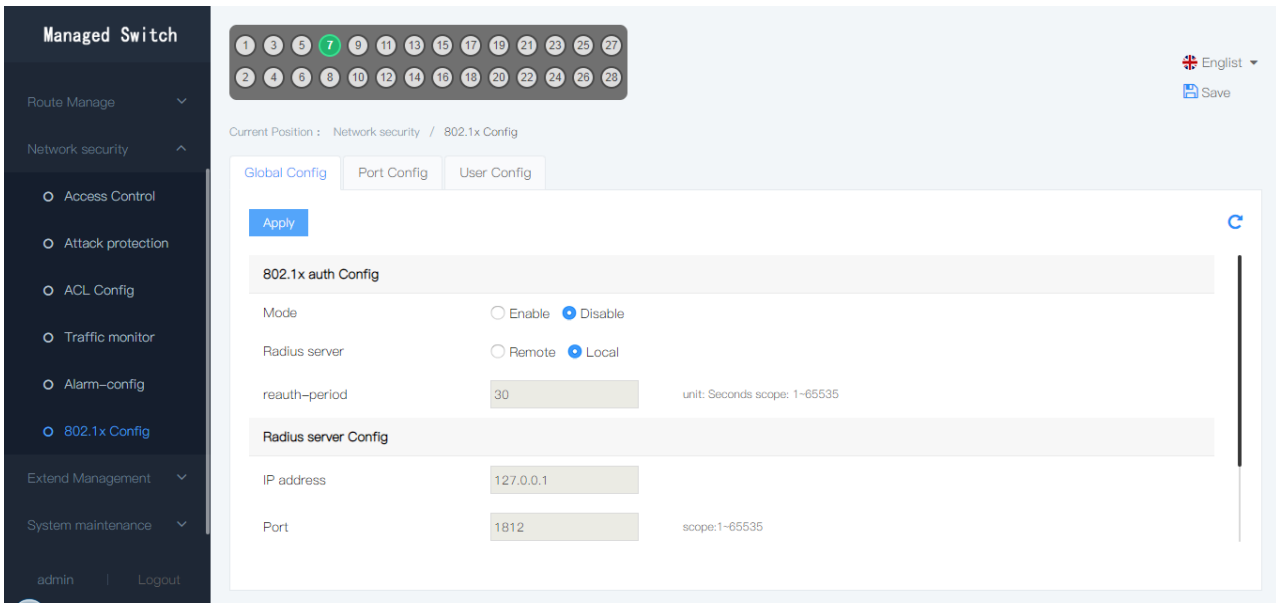
By default, the alarm is turned off. When the system alarms, the CPU exceeds the set value and the message is displayed at the alarm.

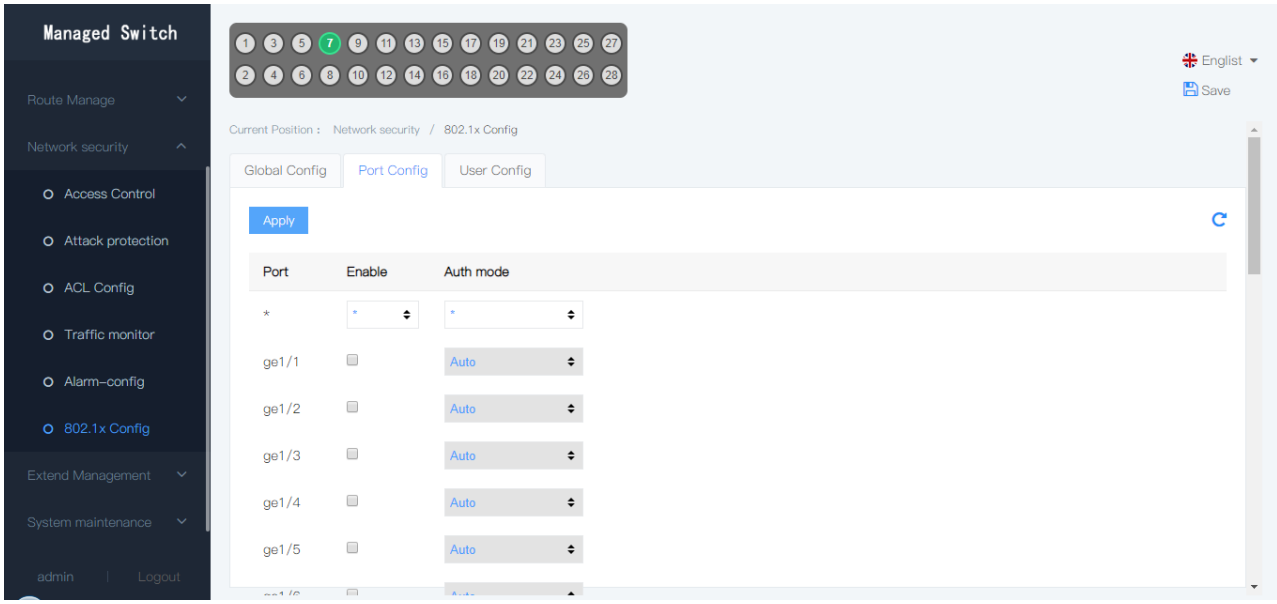


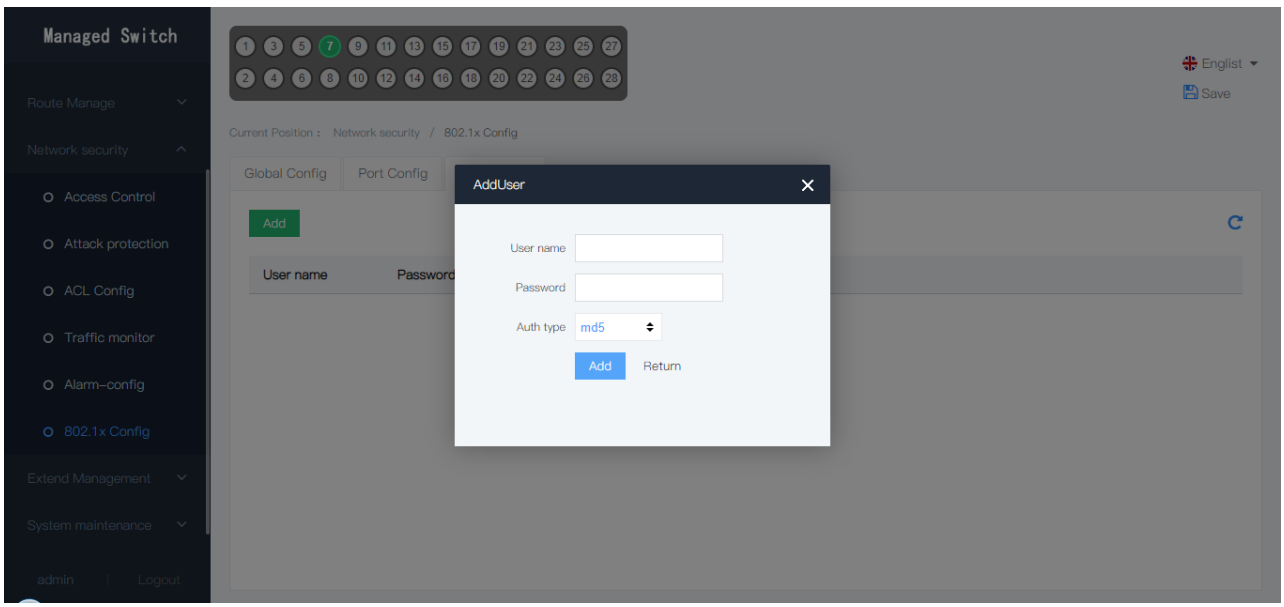
5.5.6 802.1x config

The 802.1x protocol is a port-based access control and authentication protocol. The port referred to here is a logical port, which can be a physical port. The switch implements a port-based 802.1x protocol.

802.1x is a Layer 2 protocol. The authenticated switch and the user's PC must be in the same subnet. The protocol packet cannot span the network segment. 802.1x authentication uses a model of the client server, and there must be one server to authenticate all users.







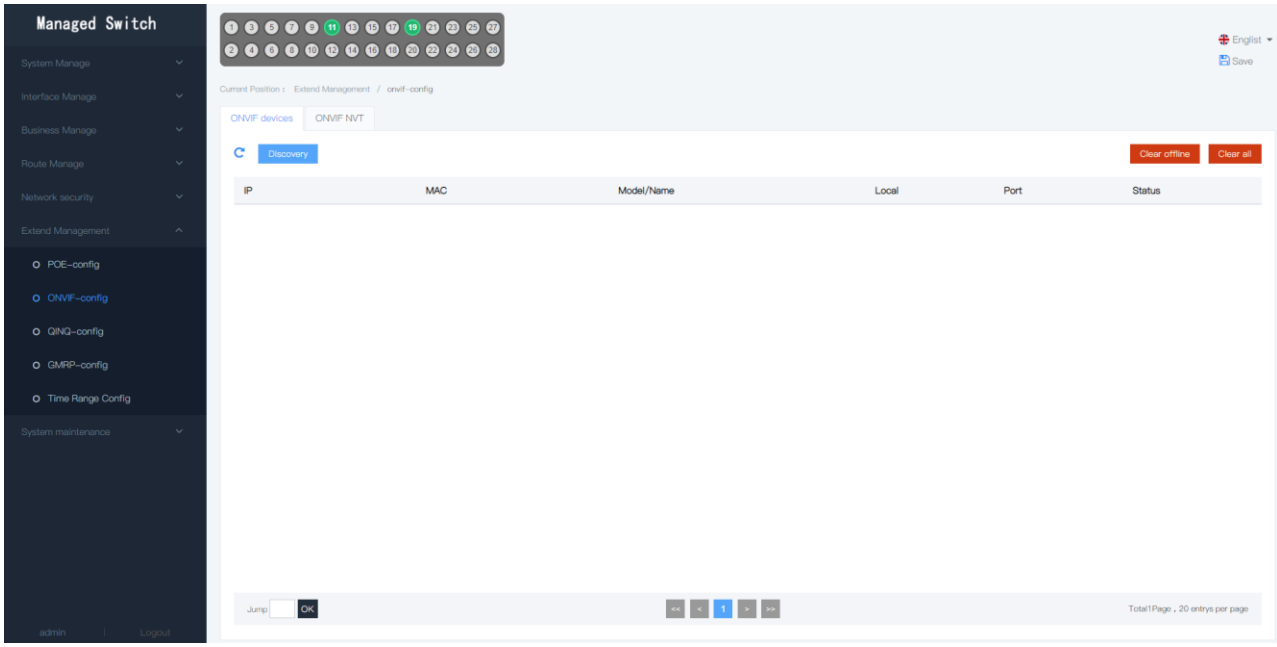
5.6 Extend management

5.6.1 ONVIF Config

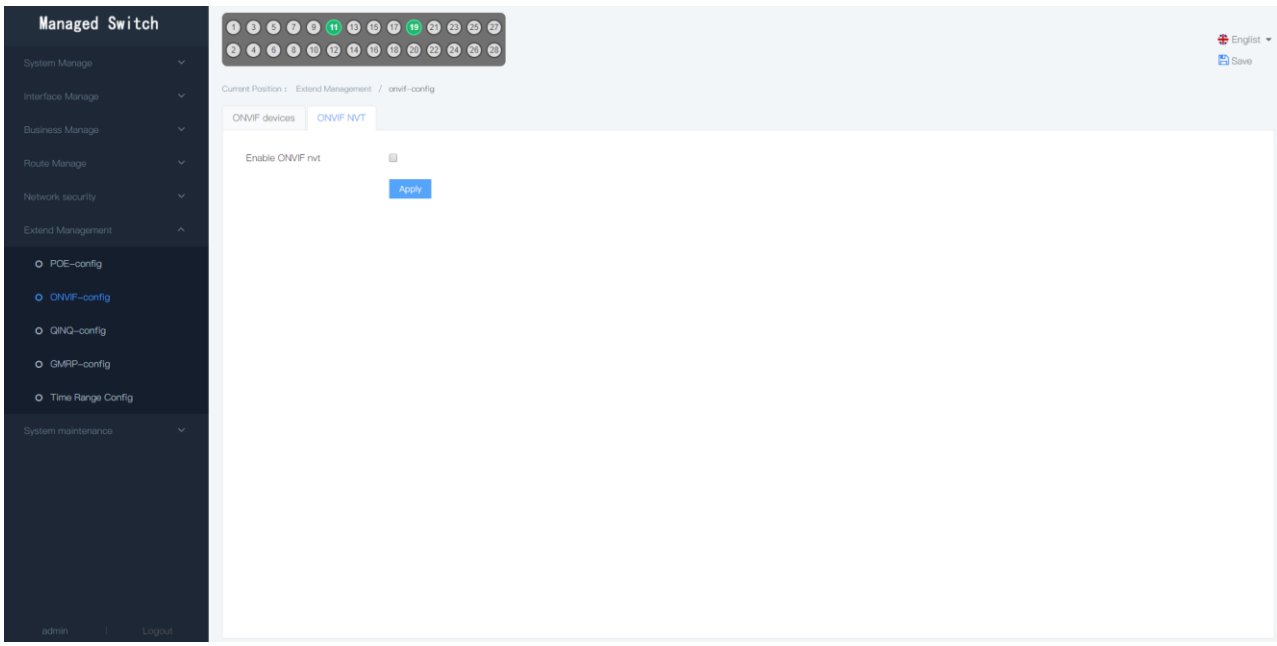
The ONVIF specification describes the models, interfaces, data types, and patterns of data interaction for network video. The goal of the ONVIF specification is to implement a network video framework protocol that enables network video products (including video front ends, video recording devices, etc.) produced by different vendors to be fully interoperable.

ONVIF devices

Discover ONVIF devices and list information about the device.



ONVIF NVT



5.6.2 QinQ-cofig

QinQBy encapsulating the outer layer of VLAN Tag for the user's private network packets on the operator's network edge device, the message carries two layers of VLAN Tag across the backbone of the operator's network (public network).

QinQ can be divided into two categories: basic QinQ and flexible QinQ:

basic QinQ

The basic QinQ is implemented in port mode. After the basic QinQ function of the port is turned on, when the port receives the message, the device will type the VLAN tag of the default VLAN of the port for the message. If a message has been received with VLAN Tag, it becomes a message of double Tag; if it is received without VLAN Tag, it becomes a message with port default VLAN Tag.

flexible QinQ

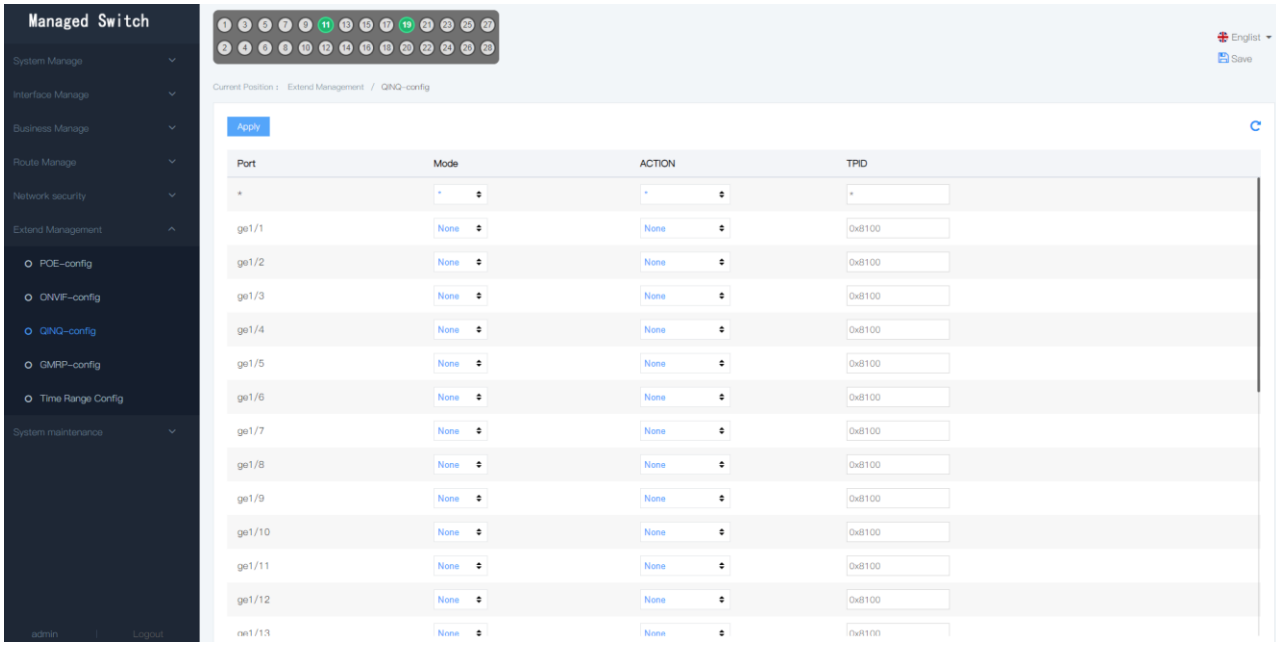
In addition to implementing all basic QinQ functions, messages received on the same port can also act differently according to different VLAN:

Add a different outer layer VLAN Tag for a message with different inner VLAN IDs;

The 802.1p priority of the outer VLAN message is marked according to the 802.1p priority of the original inner VLAN of the packet;

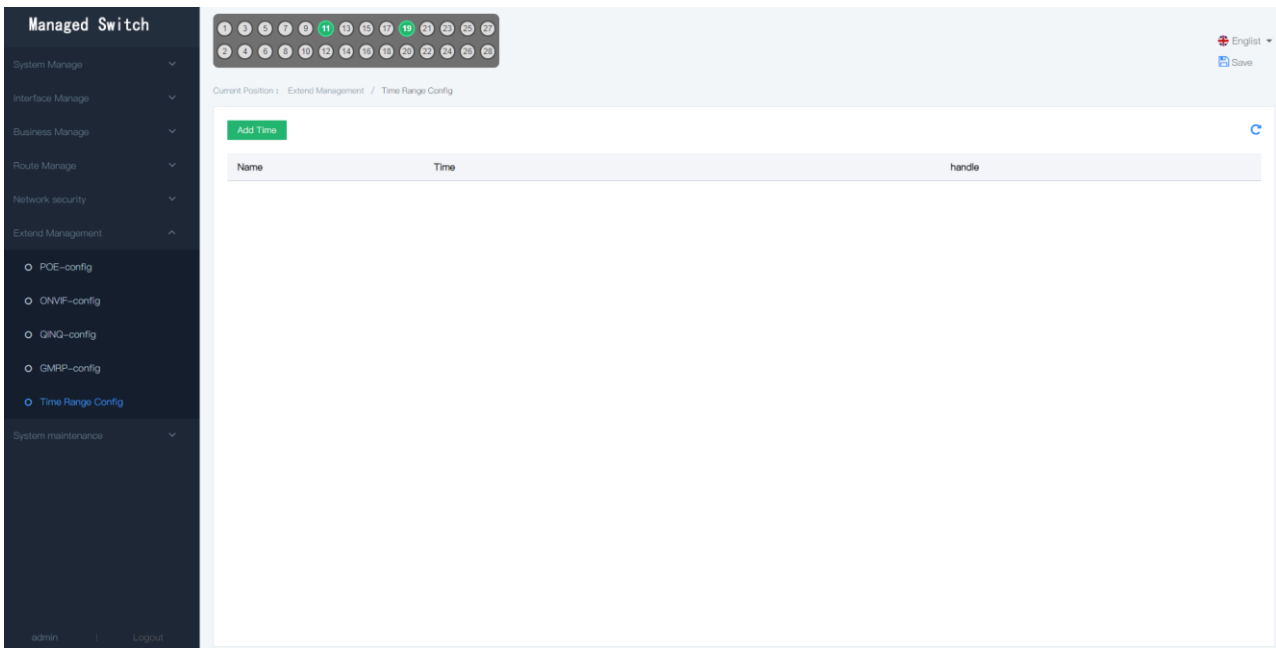
The inner user VLAN ID can be modified while the outer VLAN Tag is added.

TPID is a field in VLAN Tag that represents the protocol type of the VLAN Tag

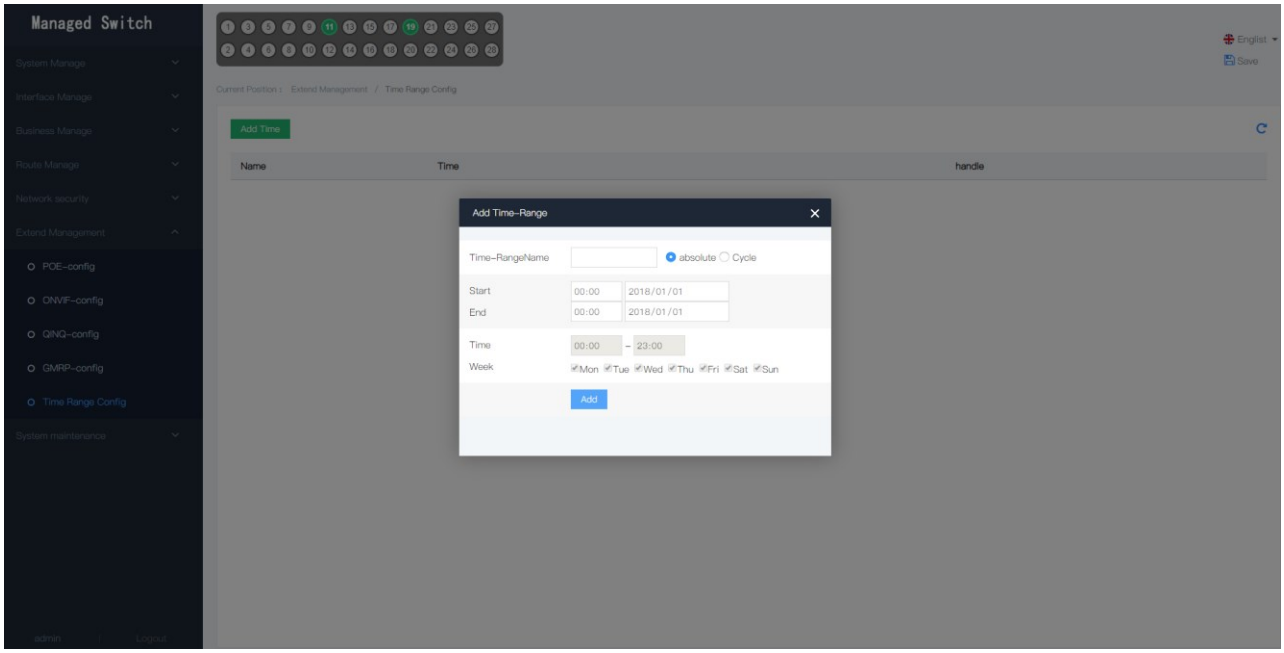


5.6.3 Time Range Config

New time schedule for other functions



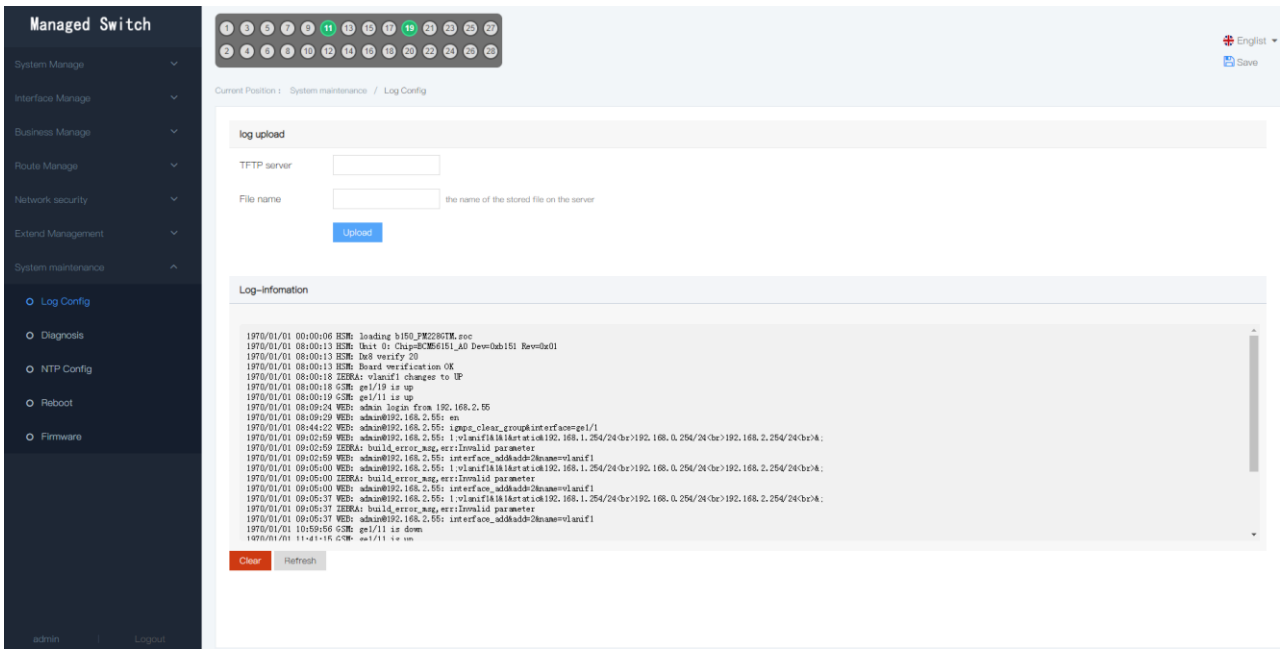
New time schedule



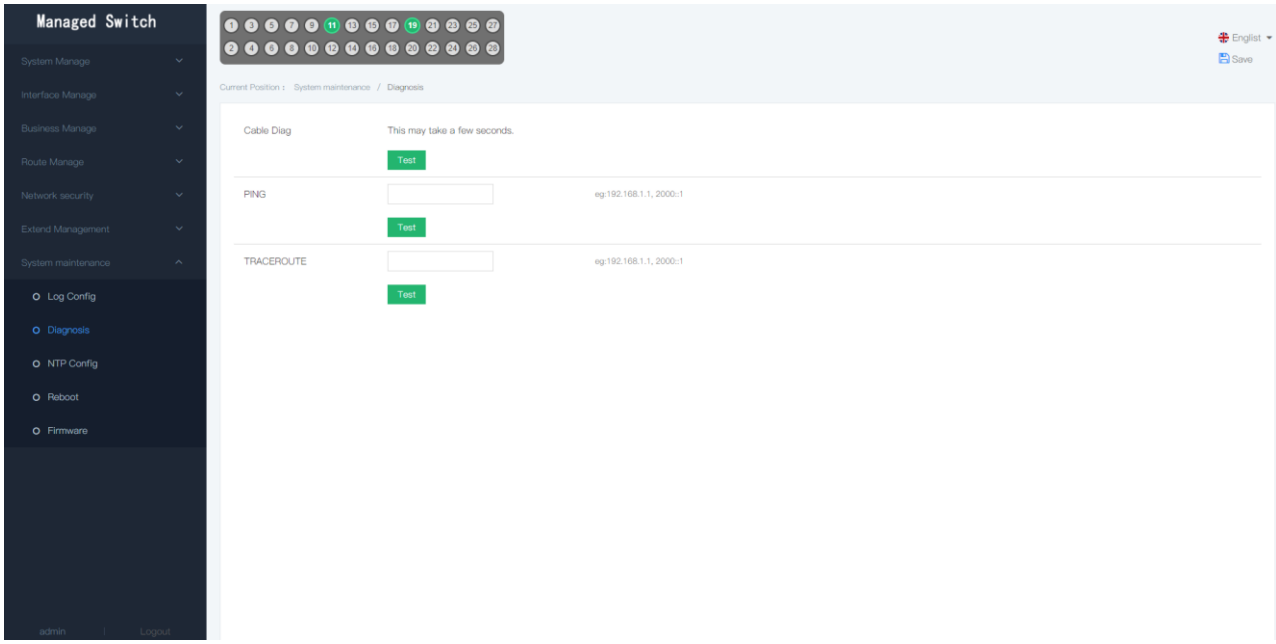
5.7 System maintenance

5.7.1 Log Config

Logs can be uploaded via the tftp server.

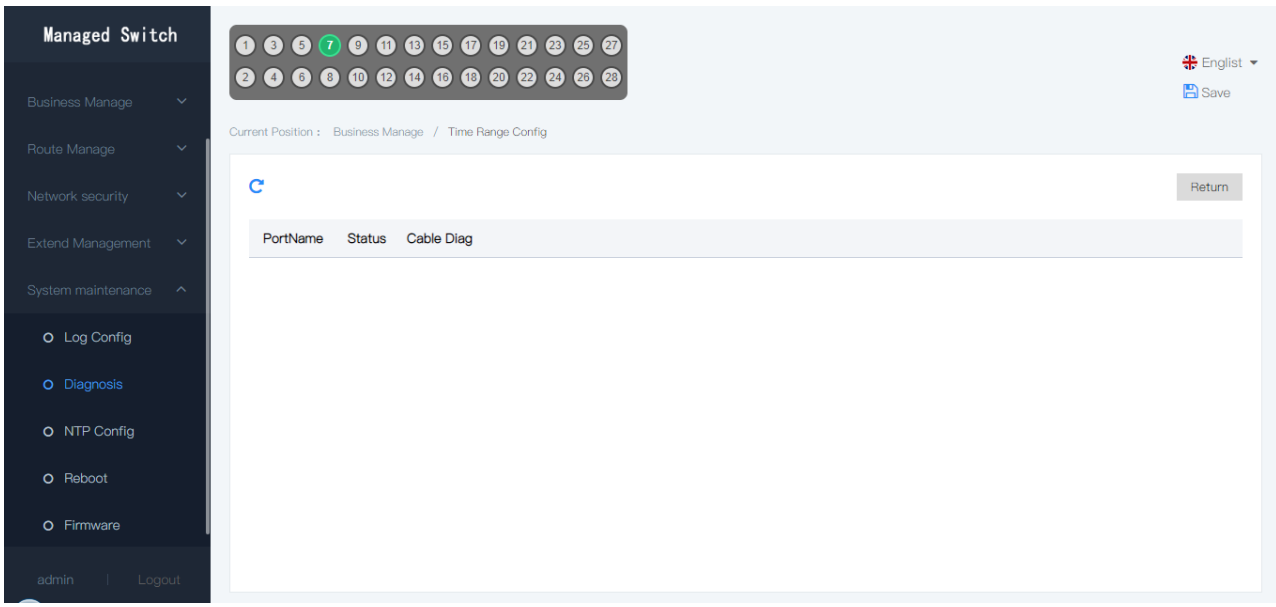


5.7.2 Diagnosis



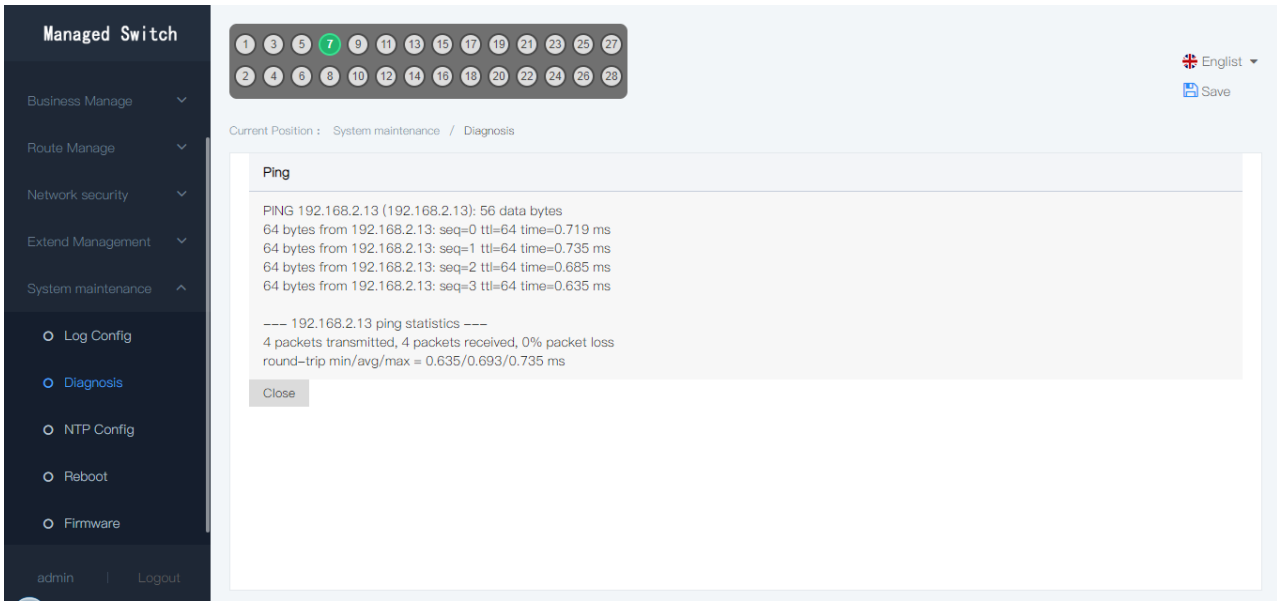
Cable Diag

Detect the cable of each port, Unable to detect optical signal



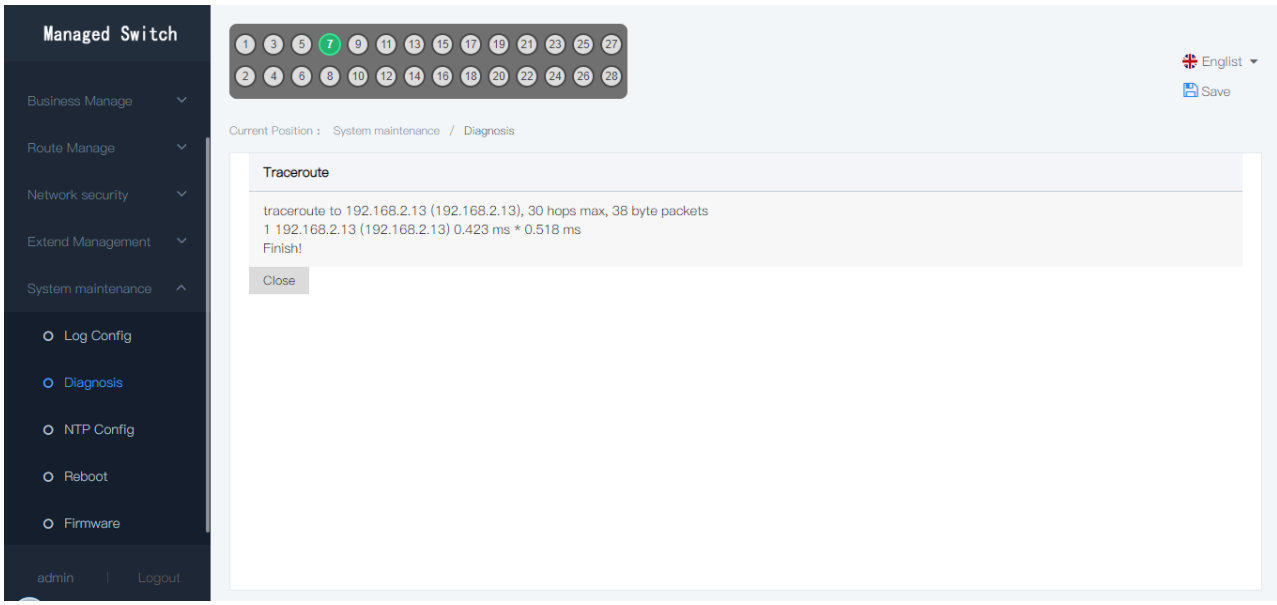
PING

Ping packets can be exported through the switch, and only ping packets can be implemented in the same network segment.



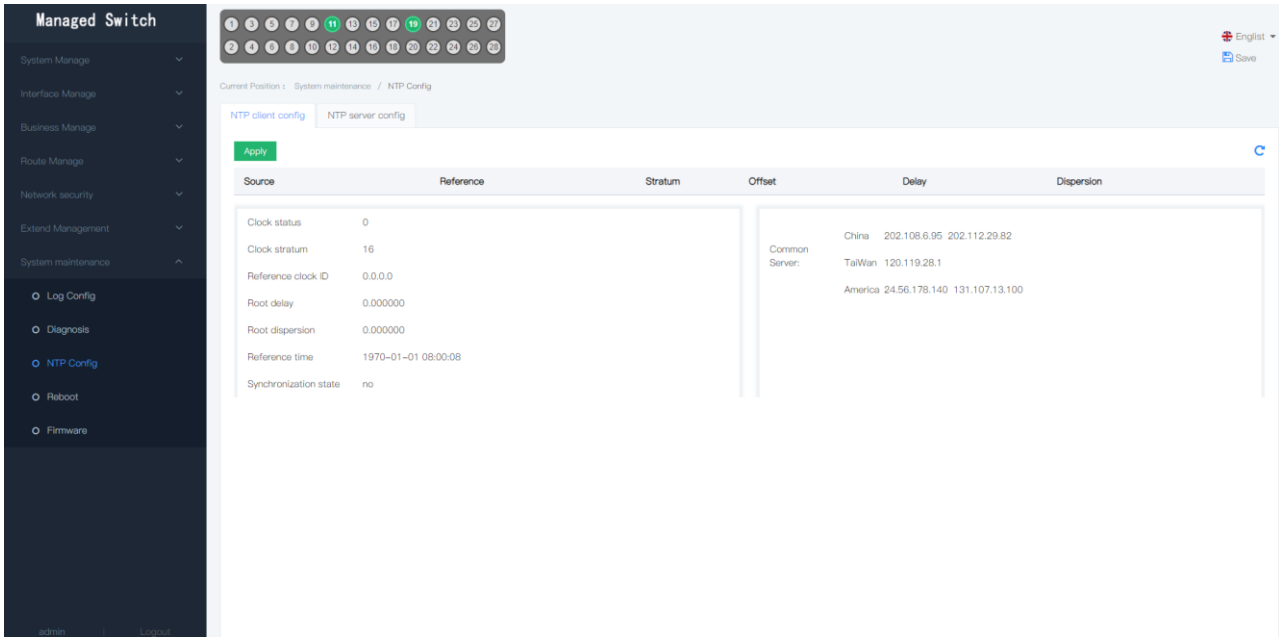
Traceroute

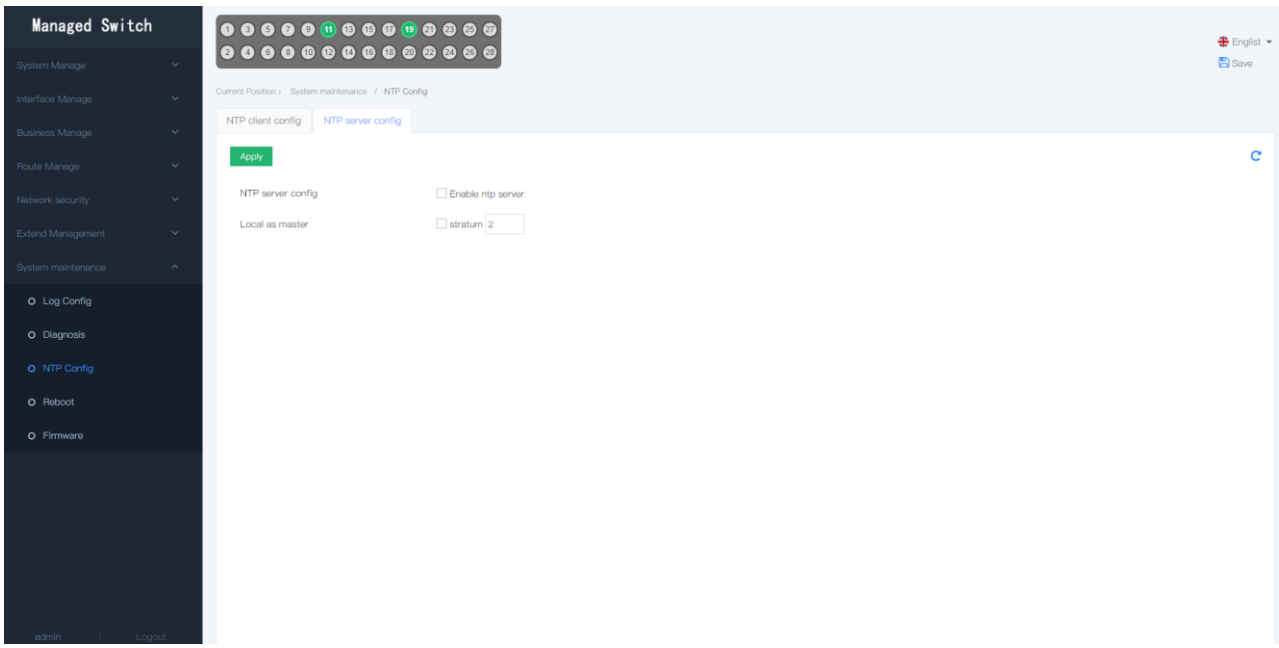
Routing tracing can be done by ping path to facilitate testing whether the current route is correct.



5.7.3 NTP Config

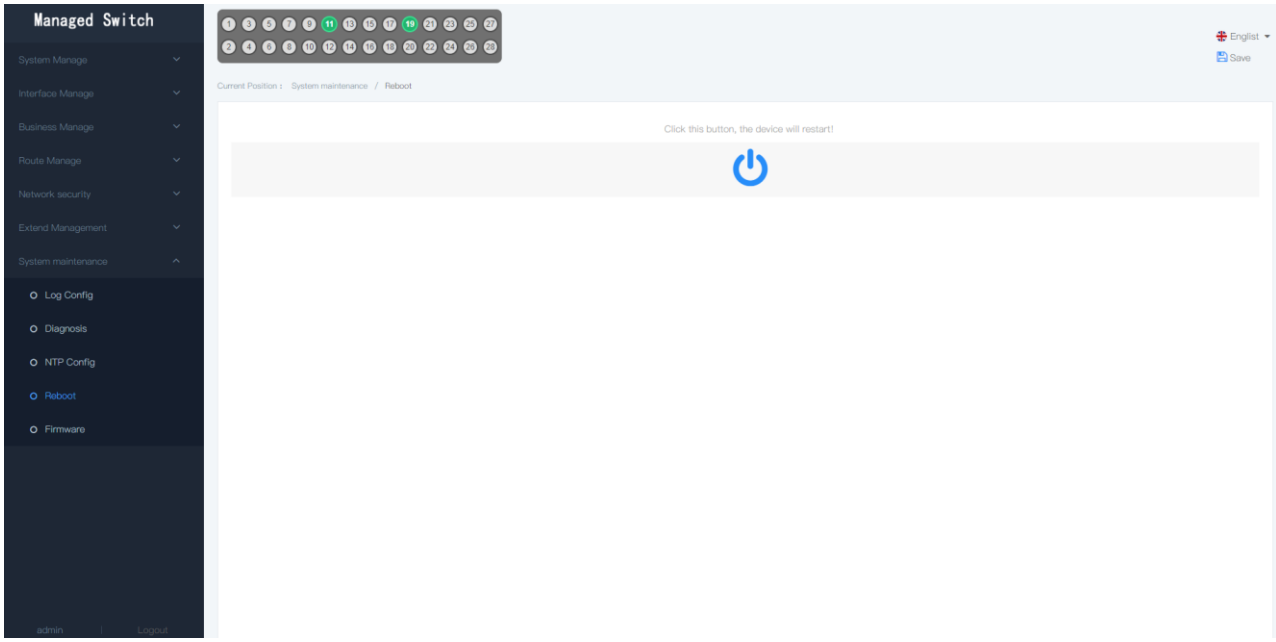
Its aim is to transmit uniform, standard time on the Internet. The specific implementation scheme is to designate several clock source websites on the network to provide time service for users, and these websites should be able to compare with each other and improve the accuracy. It can provide high precision time correction and can be confirmed by encryption to prevent malicious protocol attacks.





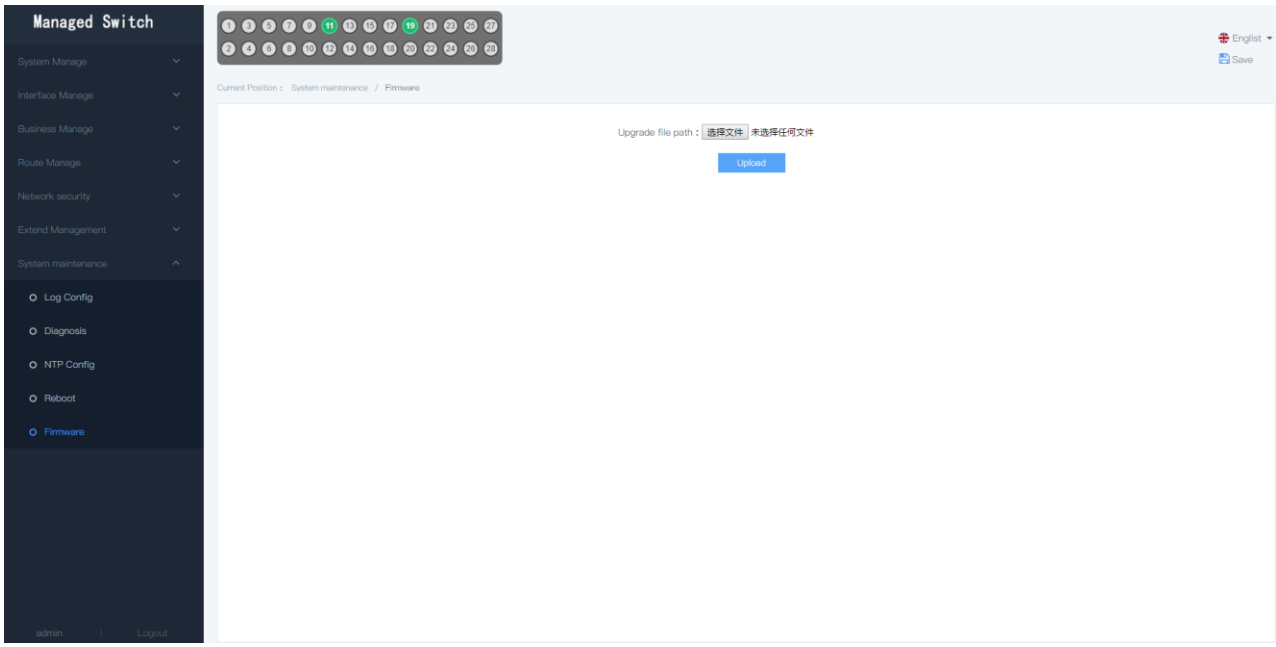
5.7.4 Reboot

Switch software restart.



5.7.5 Firmware

Click on the firmware of the upgrade switch by selecting the path to the upgrade file.



5.9 Hardware Specifications

Model	PM228GTM
Standard	IEEE 802.3、IEEE 802.3u、IEEE 802.3ab 、IEEE 802.3z、IEEE 802.3x、IEEE 802.1X、IEEE 802.1q 、IEEE 802.1p、IEEE 802.1d 、IEEE 802.1w、IEEE 802.3ad
Interface	24*1000Mbps SFP Slots 4* 10G SFP+ Slots
Indicator	PWR、LNK/ACT、SYS
Network media	10BASE-T: UTP category 3,4,5 cable（≤100m） 100BASE-TX: UTP category 5, 5e cable（≤100m） 1000BASE-T: UTP category 5e, 5 cable(≤100m) 1000BASE-X: MMF, SMF 10GBASE-X: MMF, SMF
MAC Address Table	16K, Auto-learning, Auto-aging
jumbo frame	9216Bytes
Transfer Mode	Store-and-forward
Packet Forward Speed	95Mpps
Packet buffer	1.5MB
Switching Capacity	128Gbps
Dimensions(L*W*H)	440*260*44mm
Fan Quantity	2
Green energy saving	IEEE 802.3az
Input Power Supply	12V/3A
Operating Temperature	0°C ~ 40°C
Storage Temperature	-40°C ~ 70°C
Operating Humidity	10% ~ 90% non-condensing
Storage Humidity	5% ~ 90% non-condensing
MTBF	>100000 hour