AC+AP User Manual

RLTECH

Contents

1. Matters needing Attention

1.1 Notice

This manual describes certain characteristics and functionalities of the product and its accessories, which are subject to the design and performance of the local network, as well as the software you have installed. Some characteristics and functionalities may not be available due to lack of support from the local ISP or network service provider, settings of the local network, or limitations of the installed software. Therefore, the descriptions in this manual may not fully correspond to the product or its accessories that you have purchased.

The company reserves the right to modify any information in this manual at any time without prior notice and takes no responsibility for the ensuing consequences.

1.2 Disclaimer of Warranty

The contents of this manual are provided "AS IS". Unless required by applicable law, the company makes no express or implied warranties of any kind regarding the contents herein, including but not limited to warranties of merchantability or fitness for a particular purpose.

To the maximum extent permitted by applicable law, the company shall in no event be liable for any special, incidental, indirect, consequential damages, or any loss of profits, data, goodwill, or anticipated savings arising from the use of this manual.

1.3 Install

- Please use the power adapter provided with this product. Using other power adapters may damage the device or cause it to malfunction.
- Be mindful of the electrical load capacity of your power outlet and power cord. Overloaded outlets or damaged cables and plugs can lead to electric shock or fire. Regularly inspect the related electrical cords; if there is any external damage, replace them immediately.

- Do not attempt to disassemble the device. Prevent children from using the device unsupervised to avoid swallowing small components.
- Do not place this product near heat sources or in high-temperature environments. Avoid direct exposure to sunlight.
- Do not place this product in excessively humid areas or near water sources. Never allow any liquids to spill onto the product.
- We recommend that you use the installation CD for setup and configuration operations.

1.4 Use

- After disconnecting the power, you must wait at least 15 seconds before reconnecting it.
- Ensure that the ventilation holes remain unobstructed; do not block the device's vents with any objects.
- Keep the device well-ventilated and ensure the power plug is clean and dry. If any abnormal conditions occur (such as smoking, unusual sounds, or strange odors), immediately disconnect the power plug.

1.5 Service

To maintain your warranty rights, do not attempt to open or repair this product yourself. If you encounter any issues with this product, especially the following situations, please contact your service provider promptly.

- The power cord or power plug is damaged.
- Any liquid has dripped into the casing of the product.
- The product has been submerged in rainwater or other liquids.
- The product fails to operate correctly even when used according to the operating instructions.
- The casing is damaged due to drops or heavy impacts.
- Abnormal operation indicators appear on the product.

2. Product Introduction

Dear Customer,

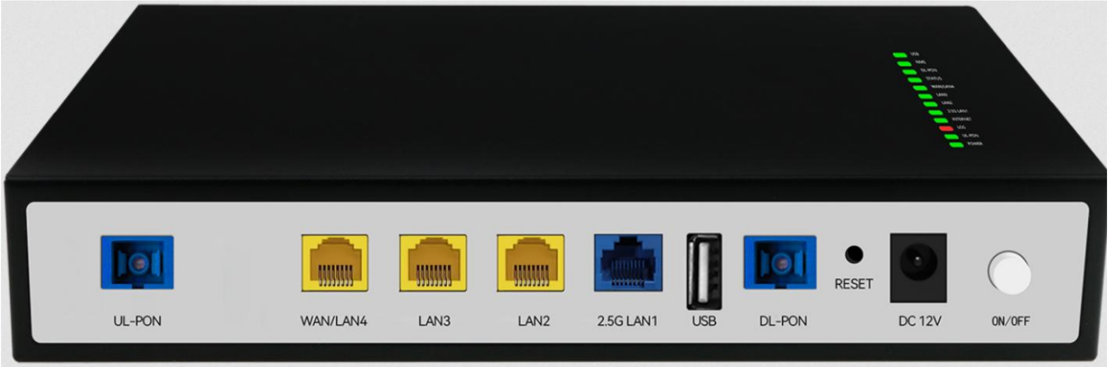
The FTTR terminal device is a comprehensive optical network main router launched by our company to meet the requirements of FTTO and POL network construction. The ONU functions and performance comply with international standards such as IEEE 802.3ah, CTC 2.1, ITU G.984, ITU G.987, or ITU G.9807 series standards, ensuring adherence to both international and industry technical specifications. It supports central office adaptability.It features high reliability, excellent QoS assurance, manageability, scalability, and flexible networking capabilities, making it well-suited to meet users' high-speed broadband access requirements.

3. Indicator Lights and Ports

3.1 RH804G-BF

The uplink optical port is GPON, supporting Huawei, ZTE, Nokia, and other OLTs and switches. The LAN4 port can be switched to an ETH WAN uplink.The downstream ports are compatible with all manufacturers' ONUs. Downstream ports include one GPON optical port, one 2.5G Ethernet port, and three 1G Ethernet ports. This device offers high reliability, excellent QoS, manageability, flexible network configuration, and easy scalability, fully meeting users' requirements for high-speed broadband. RH804G-BF does not support Wi-Fi but allows users to configure Wi-Fi settings for downstream ONU devices.This means that Wi-Fi parameters can be configured on the RH804G-BF, and these settings will automatically apply to the downstream ONU devices.

As shown in the diagram below:



RH804G-BF

3.1.1 Indicators of Device

Indicator Light Panel Description as Shown in the Table Below:

Indica	Description	Function

tor Light			
Power	Power Indicator Light	Light Off	Main router not powered on or indicator light off.
		Light On	Main router powered on and startup complete, now operating normally.
		Blink	Main router powered on and starting.
UL-PON	Upstream Optical Port Indicator Light	Light Off	Not yet registered with OLT or indicator light off.
		Light On	Already registered with OLT or authorized successfully.
		Blink	OLT registration in progress.
LOS	Upstream Optical Signal Light (Red)	Light Off	Optical signal received normally or indicator light off.
		Light On	PON port optical module power off.
		Blink	Optical signal below receiver sensitivity.
INTERNET	Internet Status Light	Light Off	WAN connection with "INTERNET" keyword not configured, or configured but not active, or indicator light off.
		Light On	WAN connection with "INTERNET" keyword active (bridge WAN configuration has taken effect, routed wan connection has acquired IP address and DNS information).
		Blink	WAN connection with "INTERNET" keyword acquiring address.
LAN1-LAN4	Network Port Status Light	Light Off	Network port not connected.
		Light On	Network port connected, but no data transmission.
		Blink	Network port connected with data transmission.
STATUS	System Status Indicator Light	Light Off	Main router not powered on or indicator light off.
		Light On	System operating normally.
DL-PON	Downstream PON Status Light	Light Off	System not powered on or indicator light off.
		Light On	System powered on and downstream pon port operating normally.
		Blink	Optical link connection abnormal (such as continuous light emission from downstream devices).
NMS	Cloud Management Status Light	Light Off	Not connected to AVASA cloud management.
		Light On	Connected to AVASA cloud management.
		Blink	Cloud management has traffic with the device.
USB	USB Status Light	Light Off	Main router not powered on, or no storage devices connected, or indicator light off.

		Light On	Storage device connected but no data transmission.
		Blink	Data transmission with storage device.

3.1.2 Interfaces

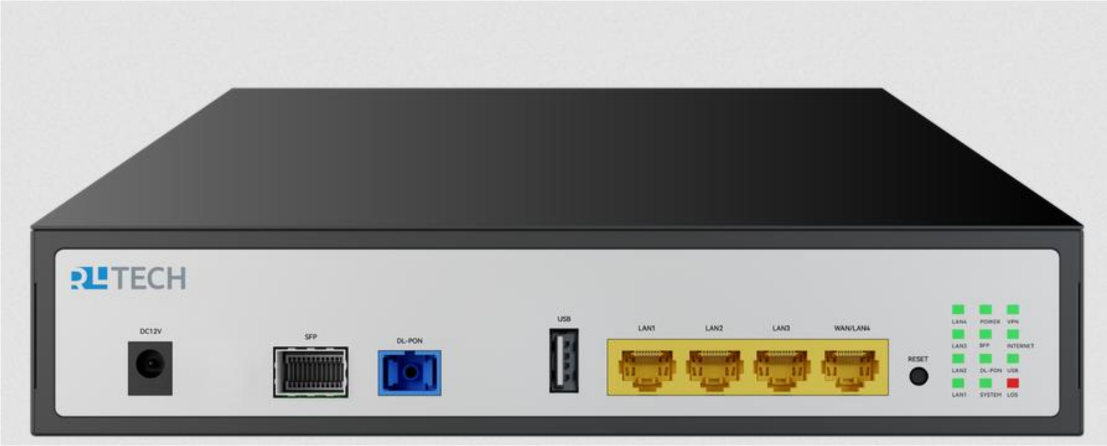
Interface panel port descriptions as shown in the table below:

Interface/Button	Description	Notes
ON/OFF	Power Switch	Power switch button.
DC 12V	Power Interface	Power input interface, for external power adapter connection.
RESET	Reset Button	Factory reset button, long press for more than 5 seconds to automatically restore factory default settings.
UPSTREAM OPTICAL PORT	UL-PON	GPON port, supports SC/UPC fiber optic connectors for upstream optical signal connection.
USB	USB	One USB 2.0 port for storage.
INTERNET PORT	LAN1-LAN4	Four RJ-45 lan ports, one 2.5g port and three gigabit ports.
DOWNSTREAM OPTICAL PORT	DL-PON	GPON port, supports SC/UPC fiber optic connectors, plug-and-play with downstream ONU devices.

3.2 RH8001GR

Upstream optical port can be selected as an SFP module port, supporting GPON/XG-PON/XGS-PON/GE/10GE/Optoelectronic Conversion Module; LAN4 can be switched to ETH WAN uplink. The downstream ports include one GPON optical port and four Gigabit Ethernet ports, with the optical port supporting up to 128 sub router. The RH8001GR does not support Wi-Fi but can configure Wi-Fi settings for downstream ONU devices. This means that Wi-Fi parameters can be configured on the RH8001GR, and these settings will automatically apply to the connected ONU devices.

As shown in the diagram below:



RH8001GR

3.2.1 Indicators of Device

Indicator Light Panel Description as Shown in the Table Below:

Indicator Light	Description	Function	
Power	Power Indicator Light	Light Off	Main router not powered on or indicator light off.
		Light on	Main router powered on and startup complete, now operating normally.
		Blink	Main router powered on and starting.
UL-PON	Upstream Optical Port Indicator Light	Light Off	Not yet registered with OLT or indicator light off.
		Light On	Already registered with OLT or authorized successfully.
		Blink	OLT registration in progress.
LOS	Upstream Optical Signal Light (Red)	Light Off	Optical signal received normally or indicator light off.
		Light On	PON port optical module power off.
		Blink	Optical signal below receiver sensitivity.
DL-PON	Downstream PON Status Light	Light Off	System not powered on or indicator light off.
		Light On	System powered on and downstream PON port operating normally.

		Blink	Optical link connection abnormal (such as continuous light emission from downstream devices).
INTERNET	Internet Status Light	Light Off	WAN connection with "INTERNET" keyword not configured, or configured but not active, or indicator light off.
		Light On	WAN connection with "INTERNET" keyword active (bridge WAN configuration has taken effect, routed wan connection has acquired IP address and DNS information).
		Blink	WAN connection with "INTERNET" keyword acquiring address.
SYSTEM	System Status Indicator Light	Light Off	Indicates main router not powered on or indicator light off.
		Light On	Indicates system operating normally.
VPN	VPN status indicator light.	Light Off	Indicates VPN connection not established.
		Light On	Indicates VPN connection established, but no traffic flow.
		Blink	Indicates VPN traffic transmission in progress.
USB	USB Status Light	Light Off	Main router not powered on, or no storage devices connected, or indicator light off.
		Light On	Storage device connected but no data transmission.
		Blink	Data transmission with storage device.
LAN1-LAN4	Network Port Status Light	Light Off	Network port not connected.
		Light On	Network port connected, but no data transmission.
		Blink	Network port connected with data transmission.

3.2.2 Interfaces

Interface panel port descriptions as shown in the table below:

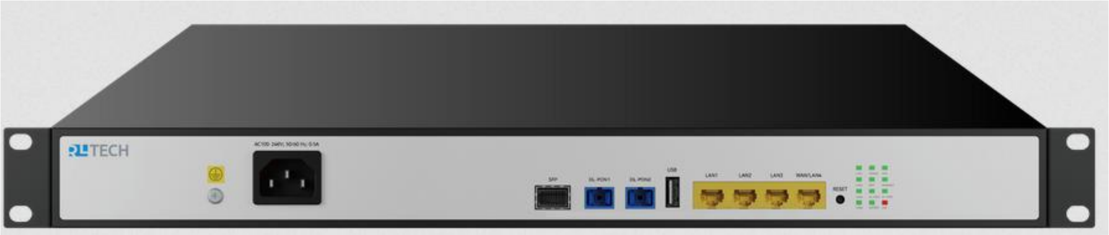
Interface	Description	Notes
DC 12V	Power Interface	Power input interface, for external power adapter connection.
UPSTREAM OPTICAL PORT	UL-PON	SFP module port, used for upstream access network optical signal.
DOWNSTREAM OPTICAL PORT	DL-PON	GPON port, supports SC/UPC optical fiber connectors, plug-and-play with downstream ONU devices.
USB	USB	One USB 2.0 port for storage.
INTERNET	LAN1-LAN4	RJ-45 ethernet port, supports WAN/LAN auto-detection, with a

PORT		port speed of 1000 Mbps.
RESET	Reset Button	Factory reset button, long press for more than 5 seconds to automatically restore factory default settings.

3.3 RH8002GR

Upstream optical port can be selected as an SFP module port, supporting GPON/XG-PON/XGS-PON/GE/10GE/Optoelectronic Conversion Module； LAN4 can be switched to eth wan uplink. The downstream ports include two GPON optical ports and four Gigabit Ethernet ports, with the optical port supporting up to 128 sub router. The RH8002GR does not support Wi-Fi but can configure Wi-Fi settings for downstream ONU devices. This means that Wi-Fi parameters can be configured on the RH8002GR, and these settings will automatically apply to the connected ONU devices.

As shown in the diagram below:



RH8002GR

3.3.1 Indicators of Device

Indicator Light Panel Description as Shown in the Table Below:

Indicator Light	Description	Function	
Power	Power Indicator Light	Light Off	Main router not powered on or indicator light off.
		Light On	Main router powered on and startup complete, now operating normally.
		Blink	Main router powered on and starting.

UL-PON	Upstream Optical Port Indicator Light	Light Off	Not yet registered with OLT or indicator light off.
		Light On	Already registered with OLT or authorized successfully.
		Blink	OLT registration in progress.
LOS	Upstream Optical Signal Light (Red)	Light Off	Optical signal received normally or indicator light off.
		Light On	PON port optical module power off.
		Blink	Optical signal below receiver sensitivity.
DL-PON 1/2	Downstream PON Status Light	Light Off	System not powered on or indicator light off.
		Light On	System powered on and downstream pon interface operating normally.
		Blink	Optical link connection abnormal (such as continuous light emission from downstream devices).
INTERNET	Internet Status Light	Light Off	WAN connection with "INTERNET" keyword not configured, or configured but not active, or indicator light off.
		Light On	WAN connection with "INTERNET" keyword active (bridge WAN configuration has taken effect, routed wan connection has acquired IP address and DNS information).
		Blink	WAN connection with "INTERNET" keyword acquiring address.
SYSTEM	System Status Indicator Light	Light Off	Indicates main router not powered on or indicator light off.
		Light On	Indicates system operating normally.
VPN	VPN Status Indicator Light.	Light Off	Indicates VPN connection not established.
		Light On	Indicates VPN connection established, but no traffic flow.
		Blink	Indicates VPN traffic transmission in progress.
USB	USB Status Light.	Light Off	Indicates VPN connection not established.
		Light On	Indicates VPN connection established, but no traffic flow.
		Blink	Indicates VPN traffic transmission in progress.
LAN1-LAN4	Network Port Status Light	Light Off	Network port not connected.
		Light On	Network port connected, but no data transmission.
		Blink	Network port connected with data transmission.

3.3.2 Interfaces

Interface panel port descriptions as shown in the table below:

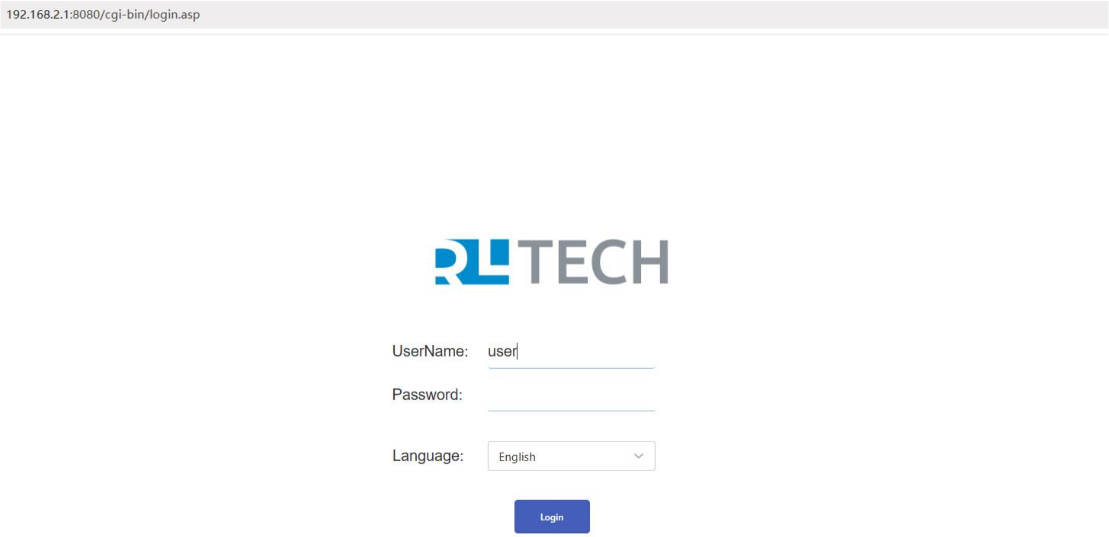
Interface	Description	Notes
AC100V～240V, 50/60Hz	Power Interface	Power input interface, for external power adapter connection.
UPSTREAM OPTICAL PORT	UL-PON	SFP module port, used for upstream access network optical signal.
DOWNSTREAM OPTICAL PORT	DL-PON	Two GPON ports, support SC/UPC optical fiber connectors, plug-and-play with downstream ONU devices.
USB	USB	One USB 2.0 port for storage.
INTERNET PORT	LAN1-LAN4	RJ-45 ethernet port for LAN4/WAN, with a port speed of 1000 Mbps.
RESET	Reset Button	Factory reset button, long press for more than 5 seconds to automatically restore factory default settings.

4. Quick Configuration

4.1 AVASA Service Quick Configuration

4.1.1 WAN Configurationa

Enter "http://192.168.2.1:8080/cgi-bin/login.asp" in the browser's address bar, press the "Enter" key to jump to the Web GUI login page. Enter the username in the login window (please refer to the product label for the initial username and password).



192.168.2.1:8080/cgi-bin/login.asp

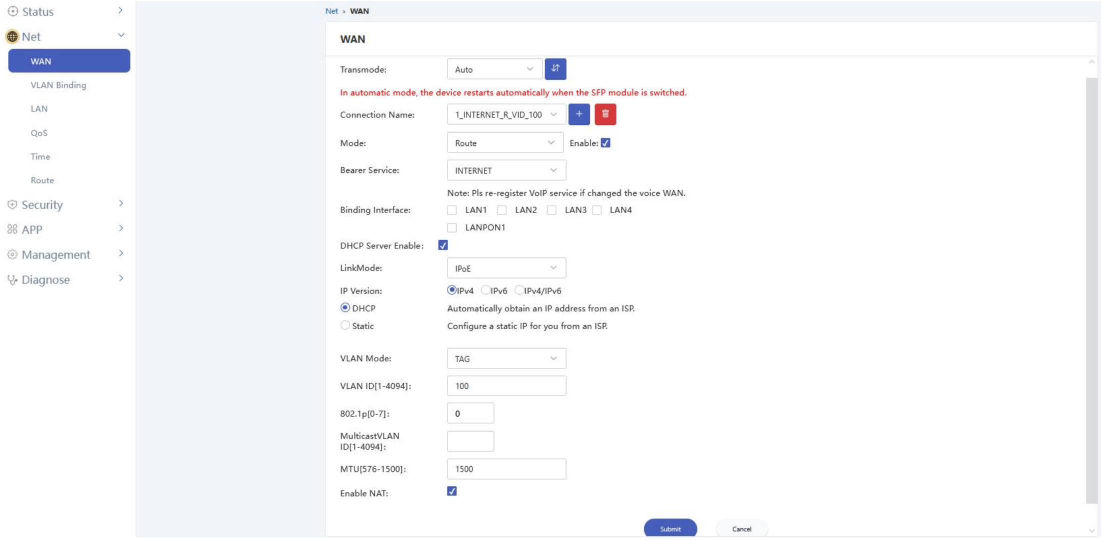
UserName: user

Password:

Language: English

Note : If you enter your password incorrectly 3 times in a row, you will be banned from logging in for 1 minute and you will have to wait for 1 minute before you can log in.

Select "Net" -> "WAN", and create a Route Internet WAN to enable the main router to access the AVASA and the Internet.



WAN

Transmode: Auto

In automatic mode, the device restarts automatically when the SFP module is switched.

Connection Name: 1_INTERNET_R_VID_100

Mode: Route Enable: ☑

Bearer Service: INTERNET

Note: Pls re-register VoIP service if changed the voice WAN.

Binding Interface: □ LAN1 □ LAN2 □ LAN3 □ LAN4 □ LANPON1

DHCP Server Enable: ☑

LinkMode: IPoE

IP Version: ● IPv4 ○ IPv6 ○ IPv4/IPv6

● DHCP Automatically obtain an IP address from an ISP.

○ Static Configure a static IP for you from an ISP.

VLAN Mode: TAG

VLAN ID[1-4094]: 100

802.1p[0-7]: 0

MulticastVLAN ID[1-4094]:

MTU[576-1500]: 1500

Enable NAT: ☑

Parameter Description Table for Route Mode

Operating Mode	Configuration Parameters	Parameter Description
Route mode	Connection Name	WAN connection name
	Mode	Configurable as a route
		Route:The PC is assigned an ip by the device and is on the same LAN
	Service type	Optional services including INTERNET,SPECIAL_SERVICE_1/2/3/4,OTHER
	Binding Interface	Lan port or wifi binding
	DHCP Server Enable	DHCP Server startup switch,In routing mode,if you need to assign ip by the device,you need to turn it on
	LinkMode	Configurable for IPoE or PPPoE

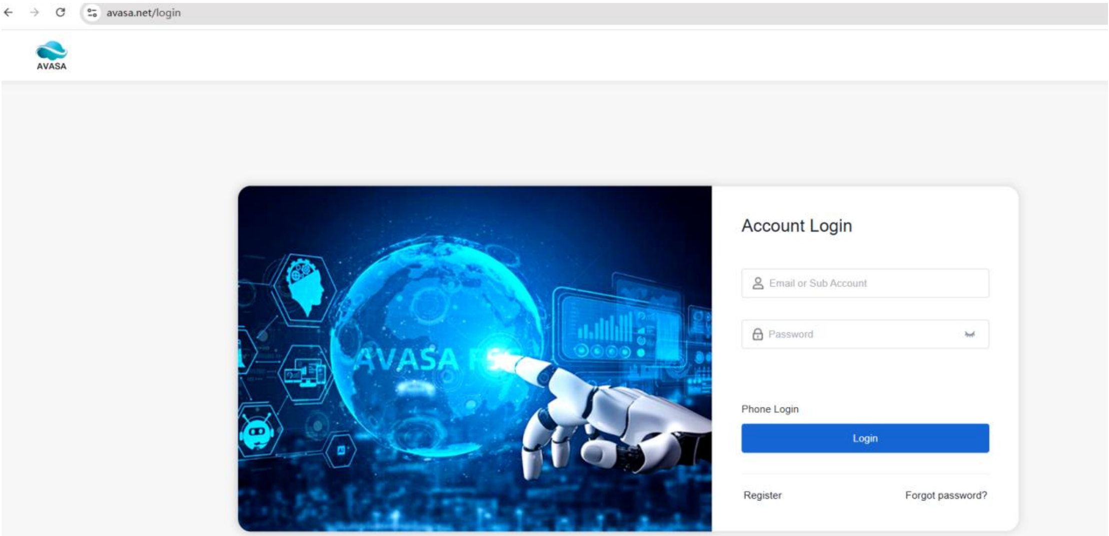
		IPoE:DHCP technology as the core,to realize the IP user session mechanism and other authentication systems.
		PPPoE:Provides access,control and billing functions for users in a peer-to-peer manner by establishing PPP sessions and encapsulating PPP messages as PPPoE messages
	IP Version	Configurable as IPv4/IPv6 single stack or IPv4&IPv6 dual stack
	VLAN Mode	Configure vlan mode
		TAG:VLAN tags are added when the device sends Ethernet frames
		UNTAG:VLAN tags are not added when the device sends Ethernet frames
	VLAN ID	Configure vlan,range:1-4094
	802.1p	Configuration priority,range:0-7
	Multicast VLAN ID	Configure multicast vlan,range:1-4094
	MTU	1) Maximum amount of data that an IP packet can carry over Ethernet,in bytes,range:1280-1500 2) Range 1280-1492 when pppoe wan,fixed 1492
	Enable NAT	Enabling address translation and communication between private and public networks
	IPv6 AddrType	Get IPv6 address type
		SLAAC:stateless configuration
		DHCP:stateful configuration
	Enable PD	ipv6 Prefix Proxy switch for assigning address prefixes in IPv6 networks

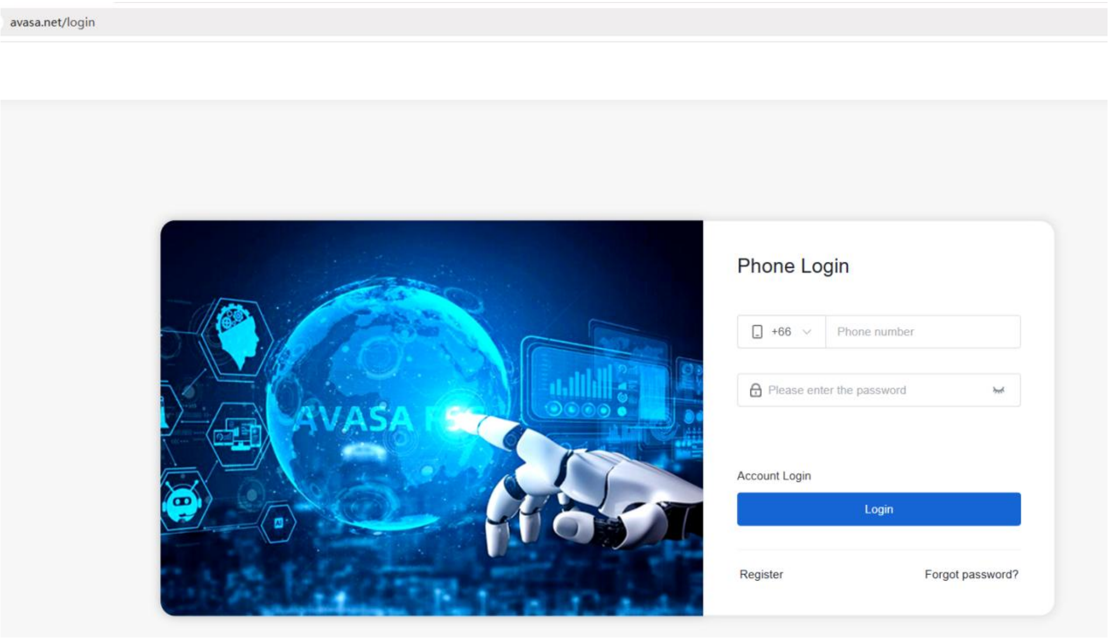
	Prefix Mode	Prefix Mode
		Auto:auto-configuration
		Manual:Manual Configuration
	Prefix Address	Prefix address to identify the network or subnet.Used in prefix mode configured as manual or static wan scenarios
	Preferred Lifeime	Preferred Lifeime,range:600 - 4294967295s for prefix mode configured as manual or static wan scenarios
	Valid Lifetime	Valid Lifetime,range:600 - 4294967295s. Used in prefix mode configured as manual or static wan scenarios
	DS-Lite Enable	DS-Lite is an IPv4 NAT technology that uses IPv4 over IPv6 tunneling to enable users with IPv4 private addresses to traverse IPv6 networks to access IPv4 public networks
	DS-Lite Mode	DS-Lite Configuration Mode: Auto or Manual.
	DS-Lite Server	Configure a DS-Lite server.
	IP Address	IP address for static wan
	Subnet Mask	Subnet mask for static wan
	Default Gateway	Gateway to static wan
	Primary DNS Server	Primary DNS servers for static wan
	Secondary DNS Server	Secondary DNS servers for static wan
	IPv6 AddrType	IPv6 AddrType for static wan,only configure static
	IPv6 Address	IPv6 address for static wan
	IPv6 Default Gateway	IPv6 gateway to static wan

	Primary IPv6 DNS Server	IPv6 primary DNS servers for static wan
	Secondary IPv6 DNS Server	IPv6 secondary DNS servers for static wan
	UserName	Dial-up username for pppoe wan
	Password	Dial-up password for pppoe wan
	Service Name	service Name for pppoe wan
	Enable PPPoE Routing/Bridge Hybrid Mode	A network connection that combines the features of routing and bridging modes for pppoe wan

4.1.2 AVASA Login

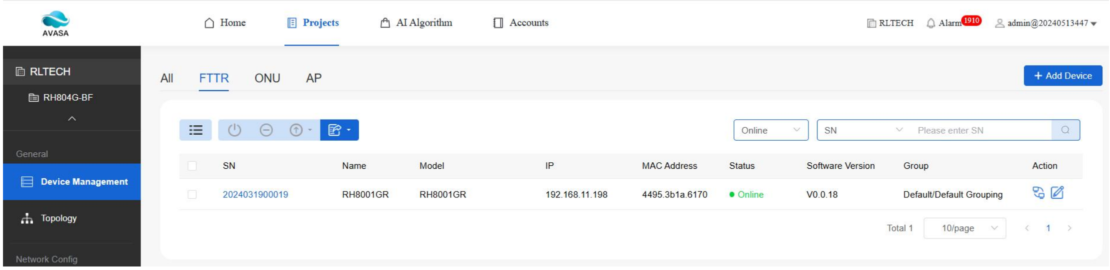
Enter "https://avasa.net/login" in the browser's address bar and press the "Enter" key to navigate to the login page. Log in with your correct username and password or use Phone login.





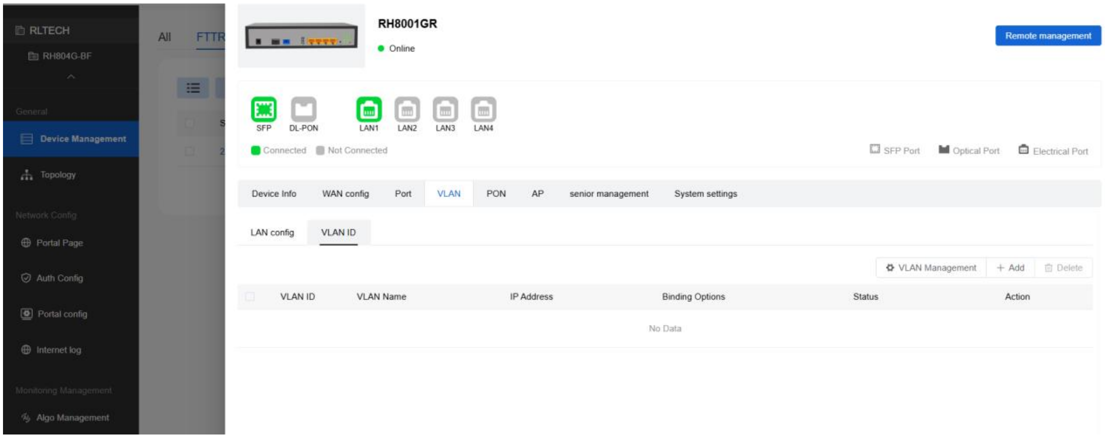
4.1.3 Multi-VLAN Configuration

On the "Projects" interface, select "Device Management" -> "FTTR" list, and click the FTTR device to be configured.

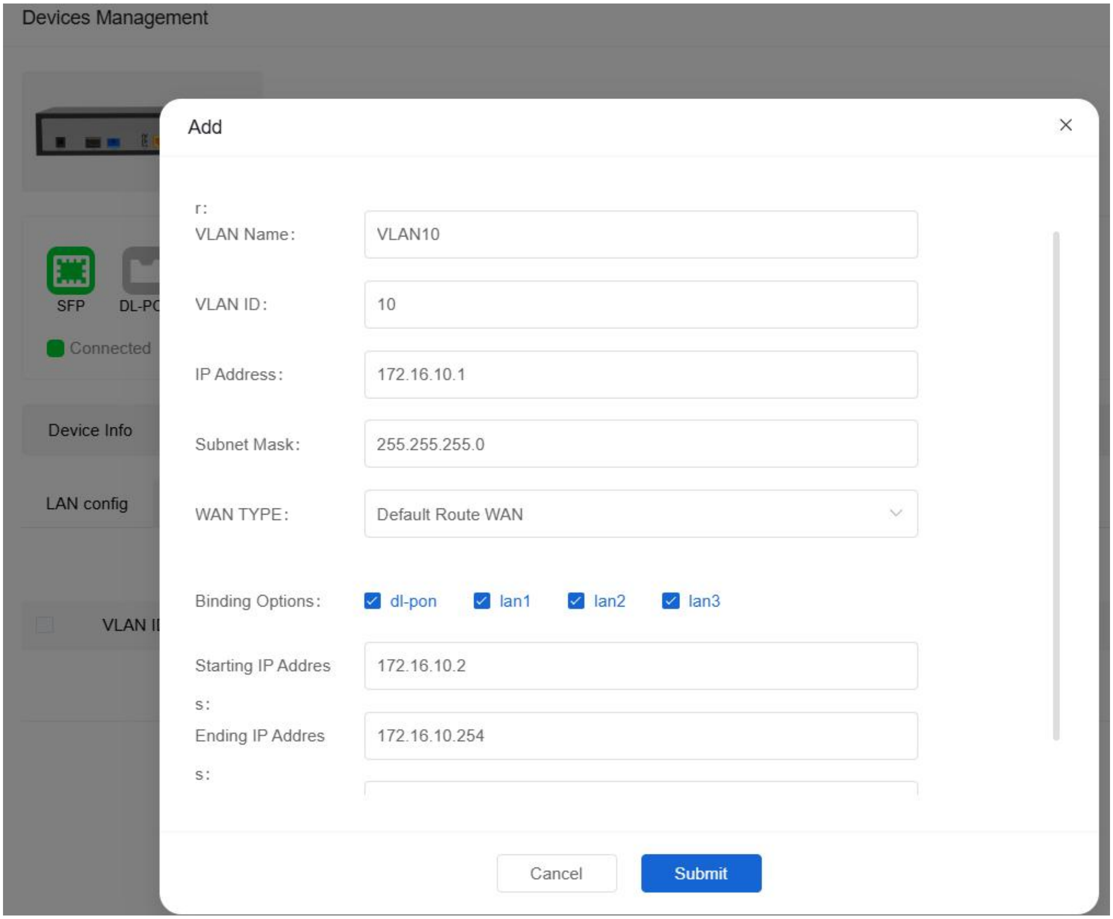


SN	Name	Model	IP	MAC Address	Status	Software Version	Group	Action
2024031900019	RH8001GR	RH8001GR	192.168.11.198	4495.3b1a.6170	● Online	V0.0.18	Default/Default Grouping	

Select "VLAN" -> "VLAN ID", click on "+ Add" to create a Multi-VLAN instance.



□	VLAN ID	VLAN Name	IP Address	Binding Options	Status	Action
			No Data			



r:

VLAN Name: VLAN10

VLAN ID: 10

IP Address: 172.16.10.1

Subnet Mask: 255.255.255.0

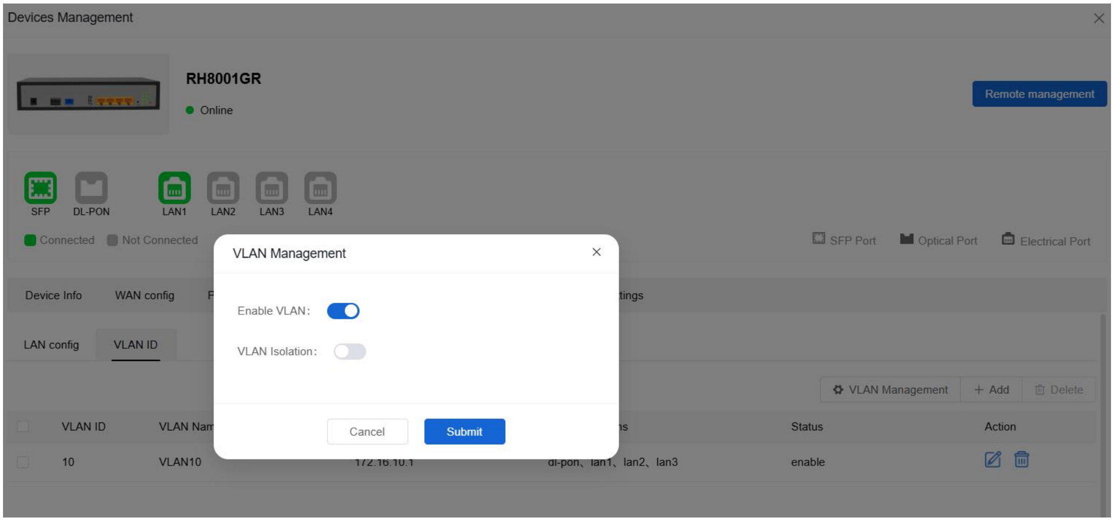
WAN TYPE: Default Route WAN

Binding Options: ☑ dl-pon ☑ lan1 ☑ lan2 ☑ lan3

Starting IP Address: 172.16.10.2

Ending IP Address: 172.16.10.254

Click on "VLAN Management", enable "Enable VLAN", and then click on "Submit" to save the configuration.



VLAN Management

Enable VLAN: ●

VLAN Isolation: ○

	VLAN ID	VLAN Nam		s	Status	Action
□	10	VLAN10	172.16.10.1	dl-pon、lan1、lan2、lan3	enable	

Multi-VLAN Parameter Description table

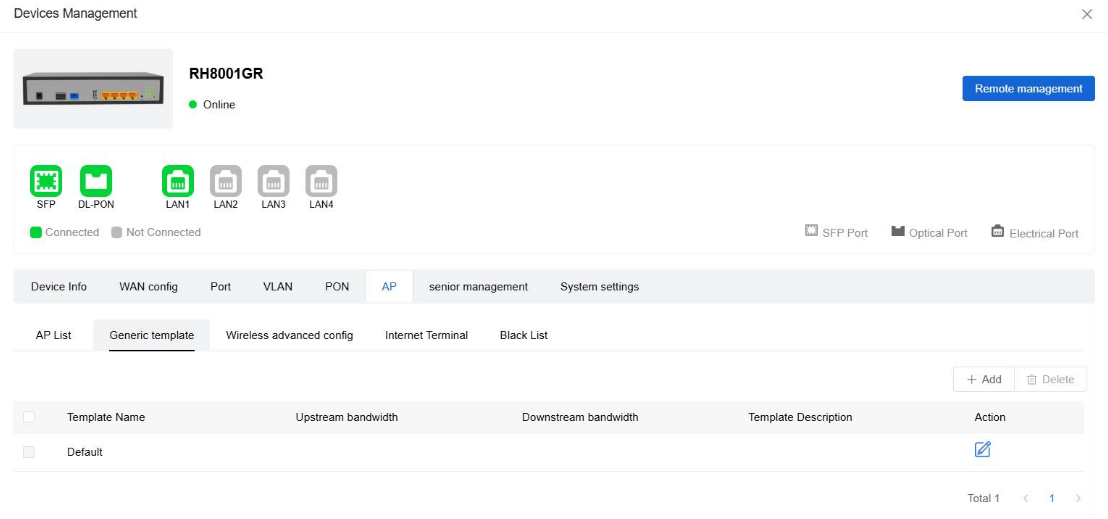
Operating Mode	Configuration Parameters	Parameter Description
VLAN Management	Enable DHCP Serve	Enable/Disable Dynamic IP Address Allocation (Enabled by default)
	VLAN Name	VLAN name
	VLAN ID	Configure vlan,range:2-4094
	IP Address	Enter the IPv4 Gateway Address for the VLAN
	Subnet Mask	Enter Subnet Mask
	WAN TYPE	Selectable WAN Types: Default Route WAN/Specified Interface WAN/Disable WAN Access
	Binding Options	LAN Port Binding
	Starting IP Address	Starting Address of the Dynamically Allocated IP Address Range by the Server
	Ending IP Address	Ending Address of the Dynamically Allocated IP Address Range by the Server
	Lease Time	Selectable IP Address Lease Time:1 Minute/1 Hour/1 Day/1 Week

	Enable VLAN	Enable/Disable Multi-VLAN Function
	VLAN Isolation	Enable/Disable Multi-VLAN Traffic Isolation Feature

Note : The dynamically allocated IP range is determined by the configured subnet mask.

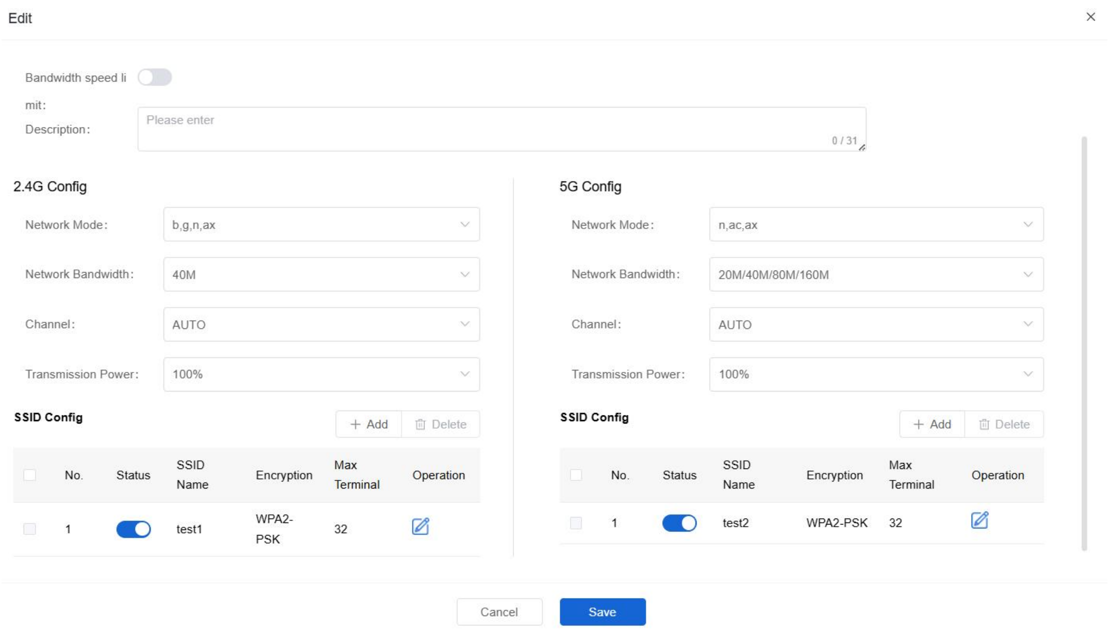
4.1.4 Configure Multi-VLAN Binding to WiFi Template

Select "AP" -> "Generic template", and click the edit option after the "Default" template.



	Template Name	Upstream bandwidth	Downstream bandwidth	Template Description	Action
□	Default				✎

Select the SSID under 2.4G and 5G configurations, click "Edit" to set the desired configuration according to the parameter table, then click "Submit" to complete the setup.



Bandwidth speed limit: ○

Description: Please enter 0 / 31

2.4G Config

Network Mode: b,g,n,ax

Network Bandwidth: 40M

Channel: AUTO

Transmission Power: 100%

SSID Config

□	No.	Status	SSID Name	Encryption	Max Terminal	Operation
□	1	●	test1	WPA2-PSK	32	✎

5G Config

Network Mode: n,ac,ax

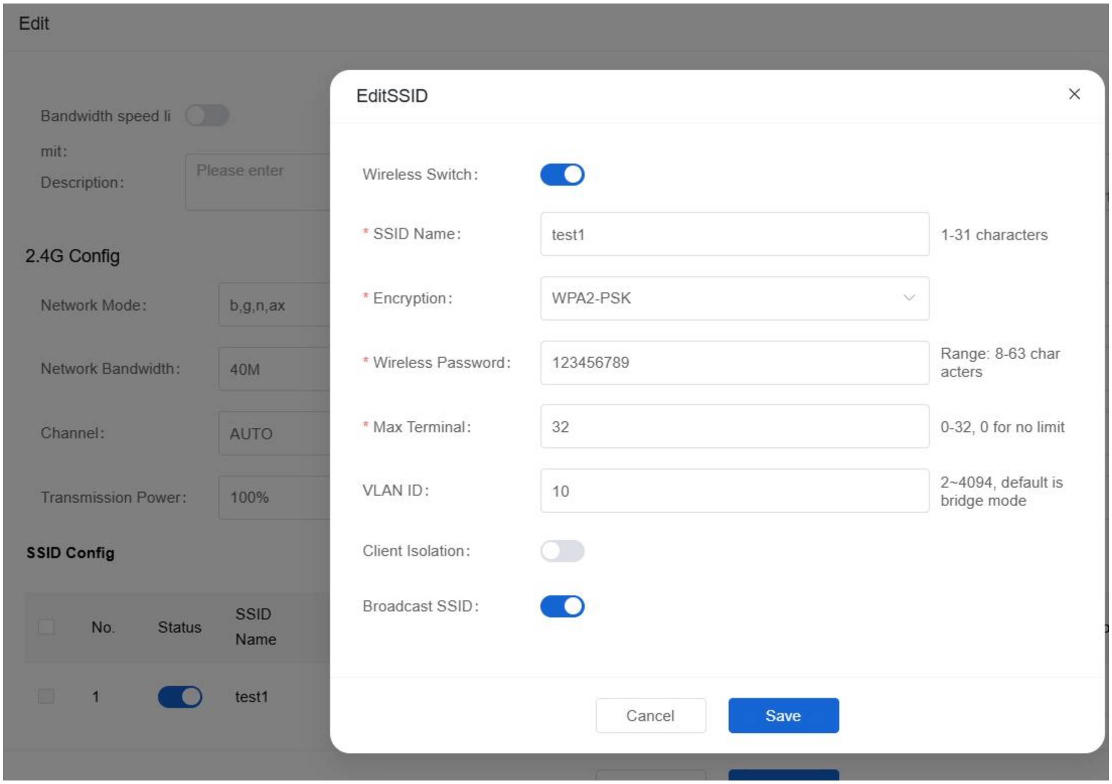
Network Bandwidth: 20M/40M/80M/160M

Channel: AUTO

Transmission Power: 100%

SSID Config

□	No.	Status	SSID Name	Encryption	Max Terminal	Operation
□	1	●	test2	WPA2-PSK	32	✎



Edit

Bandwidth speed limit:

Description: Please enter

2.4G Config

Network Mode: b,g,n,ax

Network Bandwidth: 40M

Channel: AUTO

Transmission Power: 100%

SSID Config

No.	Status	SSID Name
1	●	test1

EditSSID

Wireless Switch: ●

* SSID Name: test1 1-31 characters

* Encryption: WPA2-PSK

* Wireless Password: 123456789 Range: 8-63 characters

* Max Terminal: 32 0-32, 0 for no limit

VLAN ID: 10 2~4094, default is bridge mode

Client Isolation: ○

Broadcast SSID: ●

Wi-Fi Generic Template Parameter Description Table

Operating Mode	**Configuration Parameters**	**Parameter Description**
Basic Info	Name	Profile Name, Range: 1-15 characters.
	Bandwidth speed limit	Enable or disable speed limit function.
	Upstream bandwidth	Maximum Upload Bandwidth. Value range: 0 - 1048576, where 0 means unlimited. Unit: Kbps/Mbps.
	Downstream bandwidth	Maximum Download Bandwidth. Value range: 0 - 1048576, where 0 means unlimited. Unit: Kbps/Mbps.

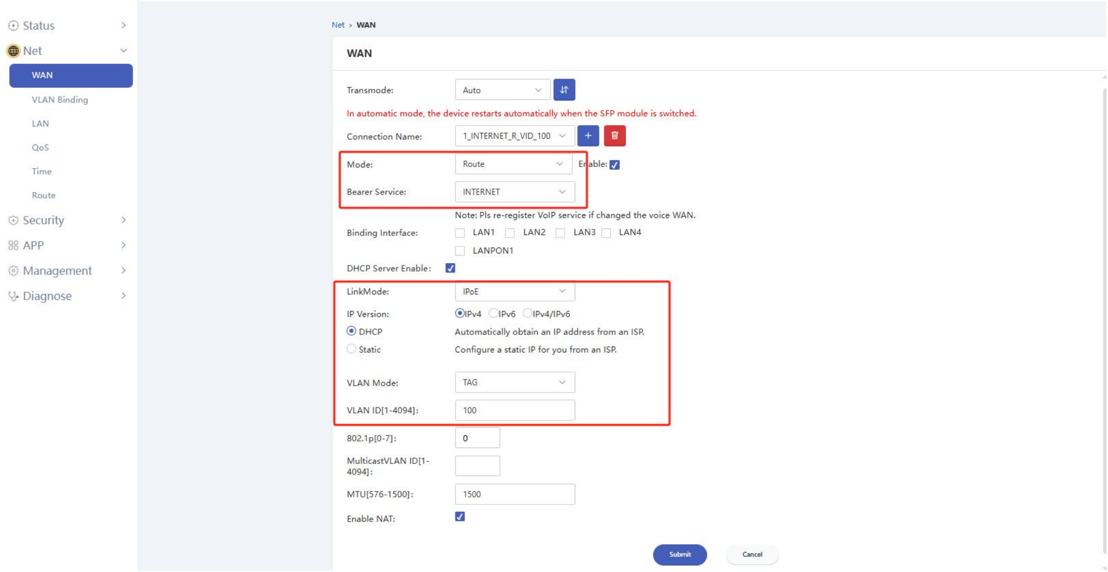
	Description	Profile Description, Range: 0 to 31 characters.
2.4G Config	Network Mode	This item is used to set the wireless working mode of the router. 2.4G:802.11b/g/n mixed mode is recommended.
	Network Bandwidth	Wireless Channel Width. 2.4G Range: 20M, 40M.
	Channel	The channel for data signal transmission with wireless signal as the transmission medium. If Auto is selected, the terminal will automatically select a best channel according to the surrounding environment. 2.4G:Channel can choose 1~13.
	Transmission Power	Wireless transmit power, it is recommended to keep the default value of 100%.
5G Config	Network Mode	This item is used to set the wireless working mode of the router. 5G:802.11ac/n/a mixed mode is recommended.
	Network Bandwidth	Wireless Channel Width. 5G Range:20M,40M.80M, 160M.
	Channel	The channel for data signal transmission with wireless signal as the transmission medium. If Auto is selected, the terminal will automatically select a best channel according to the surrounding environment. 5G:Channel can choose 36/40/46/48/52 and so on.
	Transmission Power	Wireless transmit power, it is recommended to keep the default value of 100%.
SSID Config	No	SSID Instance Serial Number.
	Status	Enable/Disable Wireless Switch.
	SSID Name	SSID name. Range: 1-31 characters.
	Encryption	Security modes,including OPEN/WPA-PSK/WPA2-PSK/WPA3-SAETransition,etc.
	Max Terminal	The maximum number of connected clients for the SSID, range: 0-32,0 represents no limit.
	VLAN ID	After selecting the Vlan parameter, the SSID will be bound to the Multi-VLAN instance. Devices connected

		to this SSID will obtain IP addresses from the subnet of the Multi-VLAN instance. The range is 2 to 4094, and the default is bridge mode.
	Client Isolation	Enable or Disable Client Isolation.
	Broadcast SSID	Enable/Disable SSID Broadcasting. When enabled: The SSID can be found in the list of wireless networks and connected to. When disabled: This SSID will not be displayed in the list of wireless networks searched by the wireless network card.

4.1.5 Examples

- Create a Route INTERNET WAN with VLAN Tag 100 in the Web GUI to enable the main router to access the AVASA and connect to the internet.
- Log in to the AVASA and create two Multi-VLAN instances: VLAN 10 with the IP address 172.16.10.1/24; VLAN 20 with the IP address 172.16.20.1/24.
- Configure the 2.4G SSID1 to bind VLAN 10 and the 5G SSID1 to bind VLAN 20.

Step 1. In the Web GUI, select "Net" -> "WAN" and create a Route WAN with tag 100.



WAN

Transmode: Auto

In automatic mode, the device restarts automatically when the SFP module is switched.

Connection Name: 1_INTERNET_R_VID_100

Mode: Route Enable: ☑

Bearer Service: INTERNET

Note: Pls re-register VoIP service if changed the voice WAN.

Binding Interface: □ LAN1 □ LAN2 □ LAN3 □ LAN4 □ LANPON1

DHCP Server Enable: ☑

LinkMode: IPoE

IP Version: ● IPv4 ○ IPv6 ○ IPv4/IPv6

● DHCP Automatically obtain an IP address from an ISP.

○ Static Configure a static IP for you from an ISP.

VLAN Mode: TAG

VLAN ID[1-4094]: 100

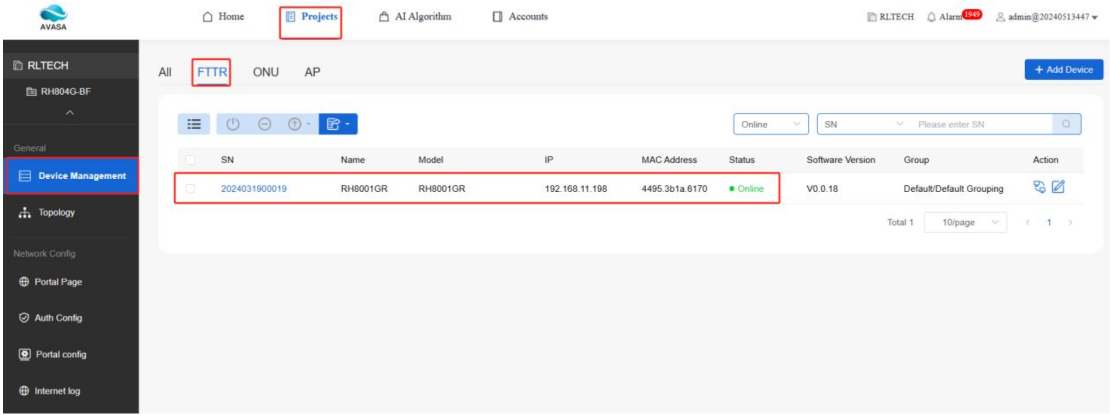
802.1p[0-7]: 0

MulticastVLAN ID[1-4094]:

MTU[576-1500]: 1500

Enable NAT: ☑

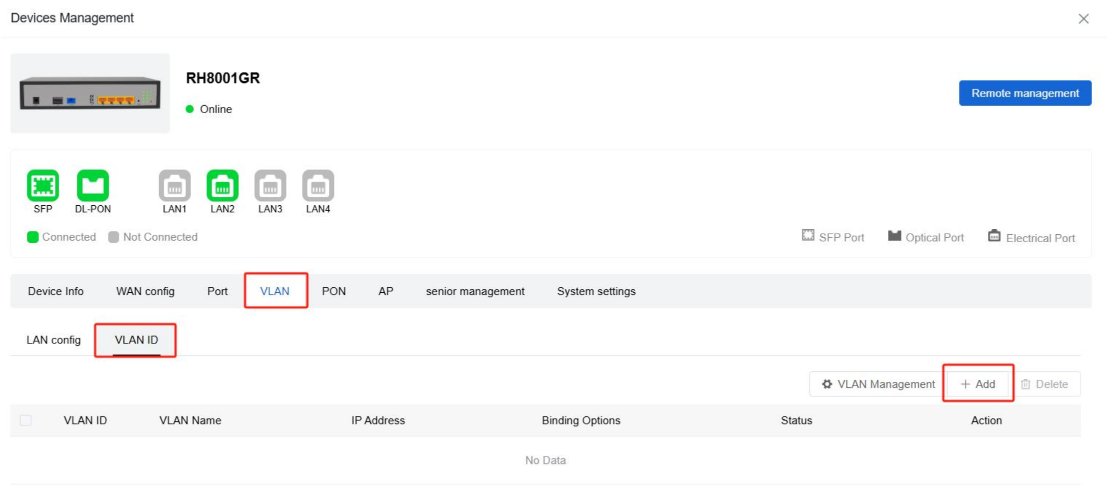
Step 2. Log in to the AVASA, select "Projects" -> "Device Management", and click on the main router to be configured in the FTTR list.



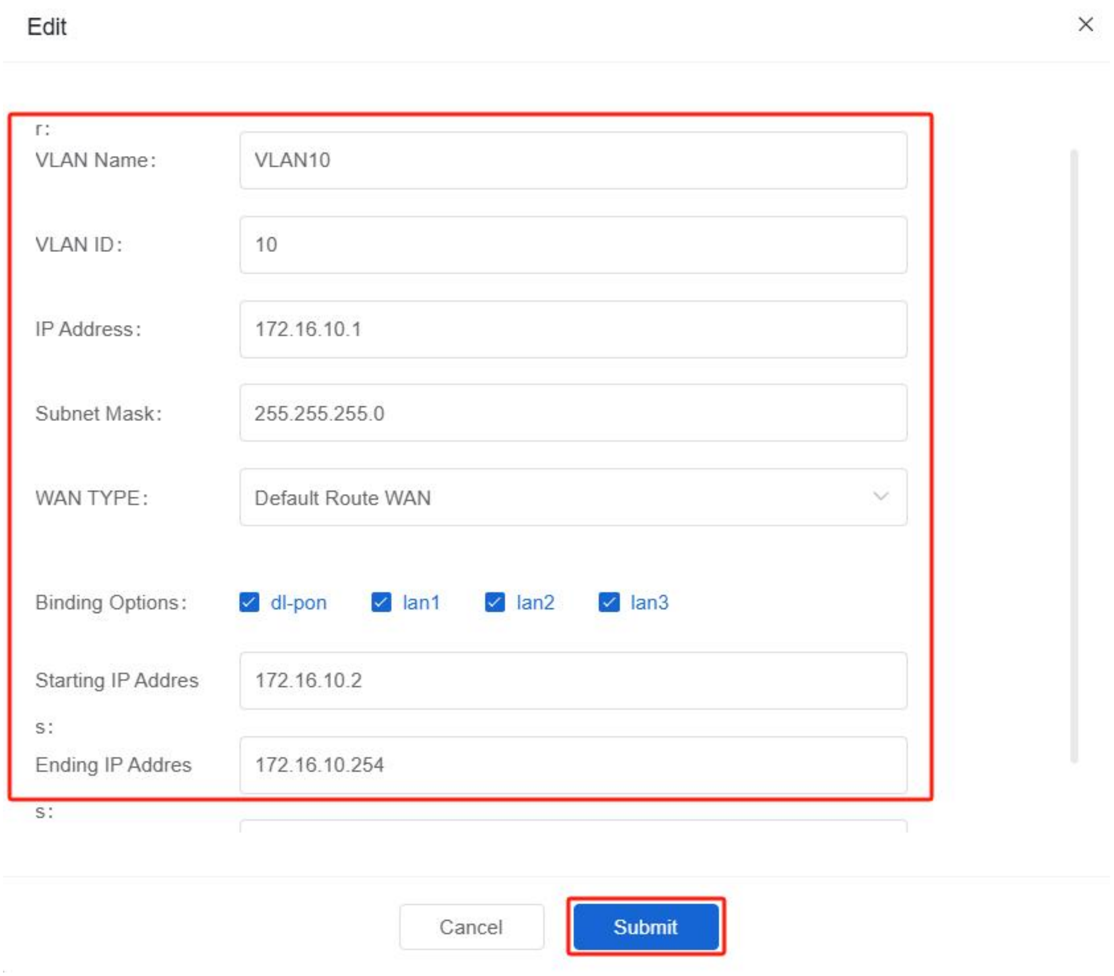
SN	Name	Model	IP	MAC Address	Status	Software Version	Group	Action
2024031900019	RH8001GR	RH8001GR	192.168.11.198	4495.3b1a.6170	● Online	V0.0.18	Default/Default Grouping	

Total 1 10/page < 1 >

Step 3.Select "VLAN" -> "VLAN ID", click "+Add", and create VLAN10 with the IP address 172.16.10.1/24 and VLAN20 with the IP address 172.16.20.1/24.



□	VLAN ID	VLAN Name	IP Address	Binding Options	Status	Action
			No Data			



Edit

r:

VLAN Name: VLAN10

VLAN ID: 10

IP Address: 172.16.10.1

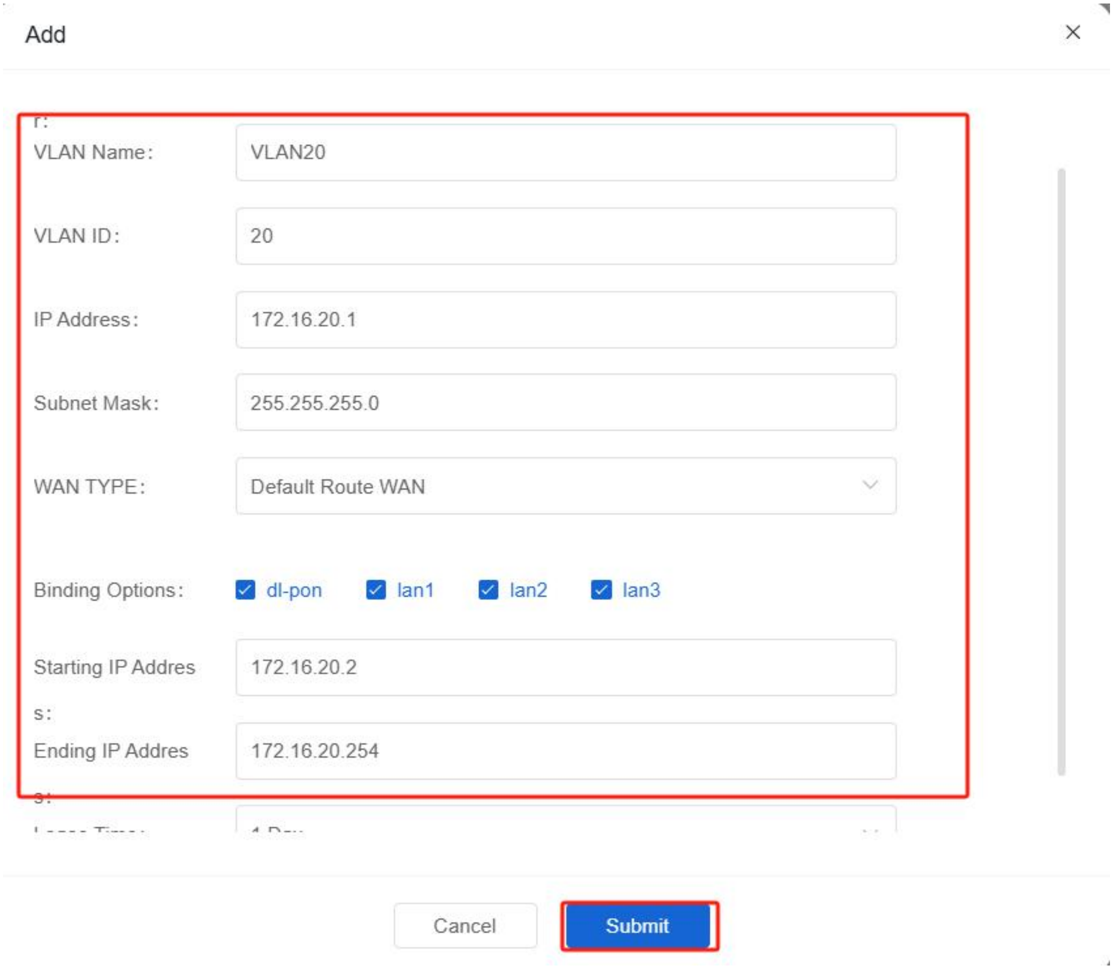
Subnet Mask: 255.255.255.0

WAN TYPE: Default Route WAN

Binding Options: ☑ dl-pon ☑ lan1 ☑ lan2 ☑ lan3

Starting IP Addres
s: 172.16.10.2

Ending IP Addres
s: 172.16.10.254



r:

VLAN Name: VLAN20

VLAN ID: 20

IP Address: 172.16.20.1

Subnet Mask: 255.255.255.0

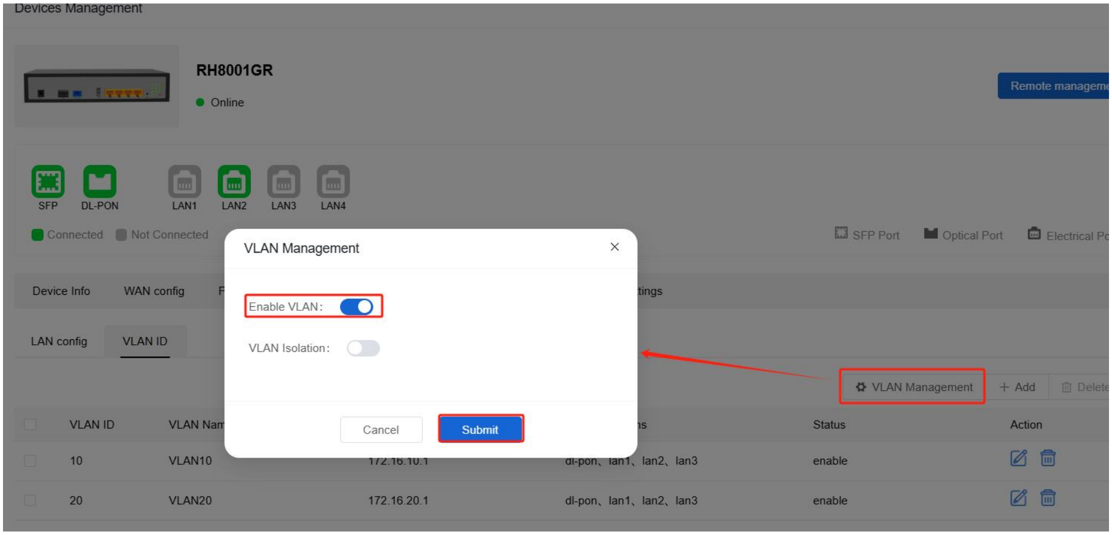
WAN TYPE: Default Route WAN

Binding Options: ☑ dl-pon ☑ lan1 ☑ lan2 ☑ lan3

Starting IP Address: 172.16.20.2

Ending IP Address: 172.16.20.254

Step 4. Click "VLAN Management", enable "Enable VLAN", and then click "Submit" to save the settings.



VLAN Management

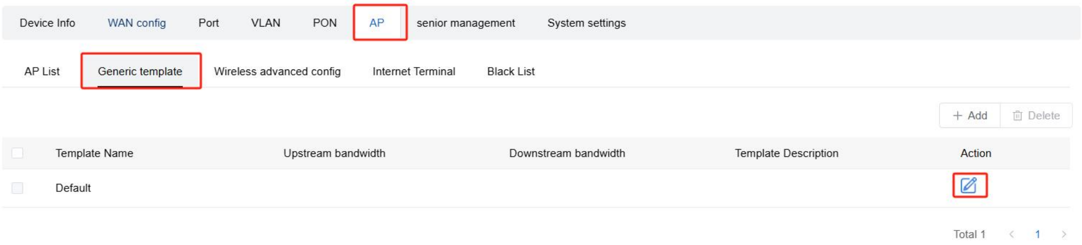
Enable VLAN: ●

VLAN Isolation: ○

Cancel | Submit

	VLAN ID	VLAN Nam		ns	Status	Action
□	10	VLAN10	172.16.10.1	dl-pon、lan1、lan2、lan3	enable	
□	20	VLAN20	172.16.20.1	dl-pon、lan1、lan2、lan3	enable	

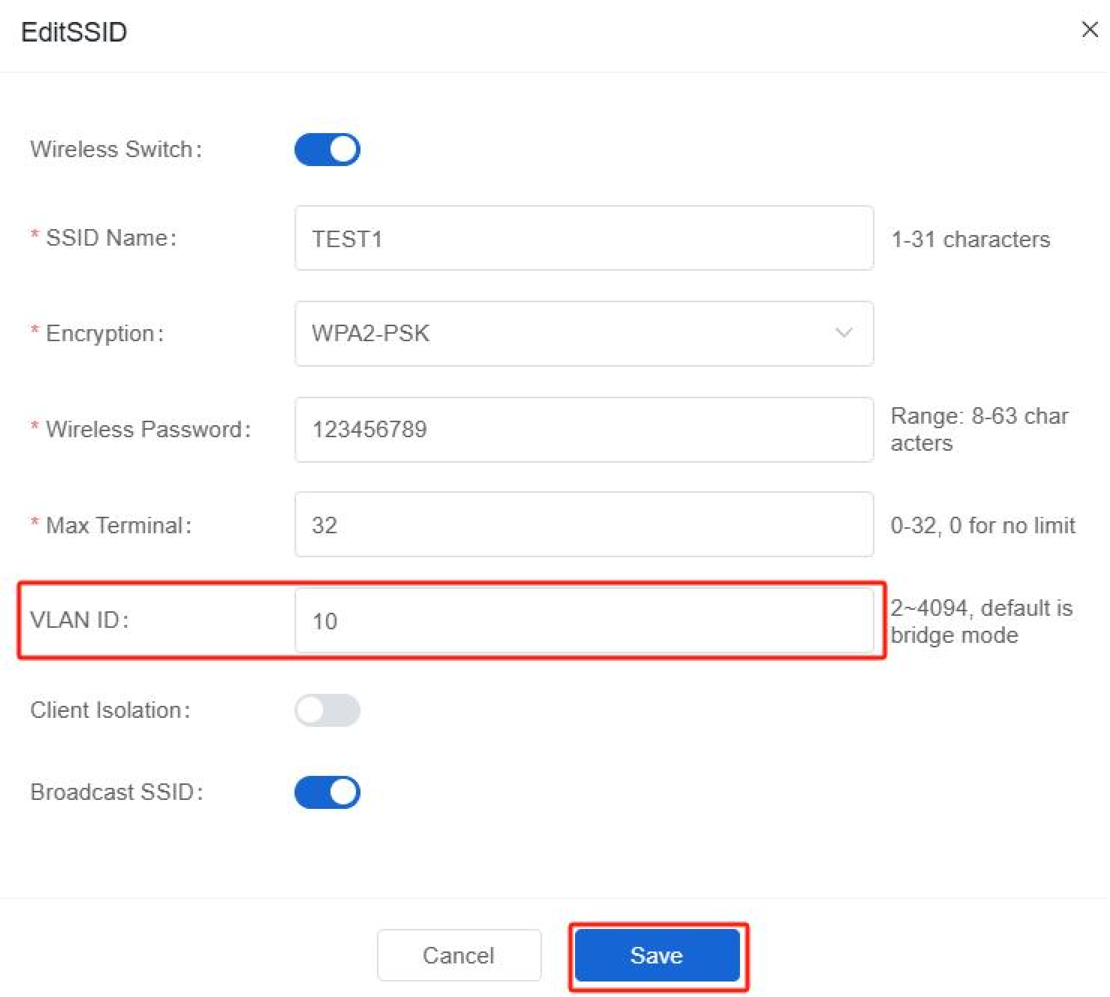
Step 5. Select "AP" -> "Generic template", choose the default template, and click "Edit".



□	Template Name	Upstream bandwidth	Downstream bandwidth	Template Description	Action
□	Default				

Total 1 ‹ 1 ›

Step 6. Configure the 2.4G SSID1 to be bound to VLAN10; configure the 5G SSID1 to be bound to VLAN20.



EditSSID

Wireless Switch: ●

* SSID Name: TEST1 — 1-31 characters

* Encryption: WPA2-PSK

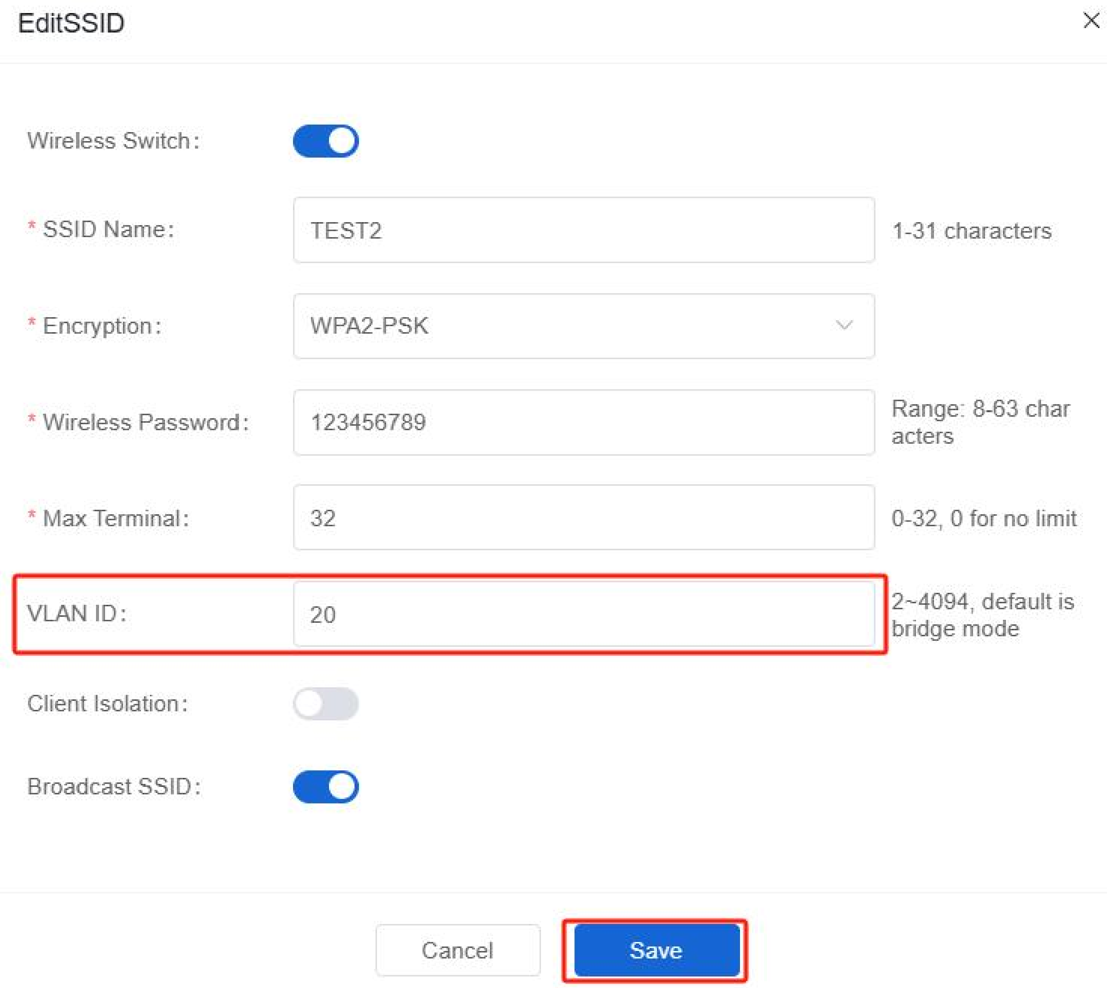
* Wireless Password: 123456789 — Range: 8-63 characters

* Max Terminal: 32 — 0-32, 0 for no limit

VLAN ID: 10 — 2~4094, default is bridge mode

Client Isolation: ○

Broadcast SSID: ●



EditSSID

Wireless Switch: ●

* SSID Name: TEST2 1-31 characters

* Encryption: WPA2-PSK

* Wireless Password: 123456789 Range: 8-63 characters

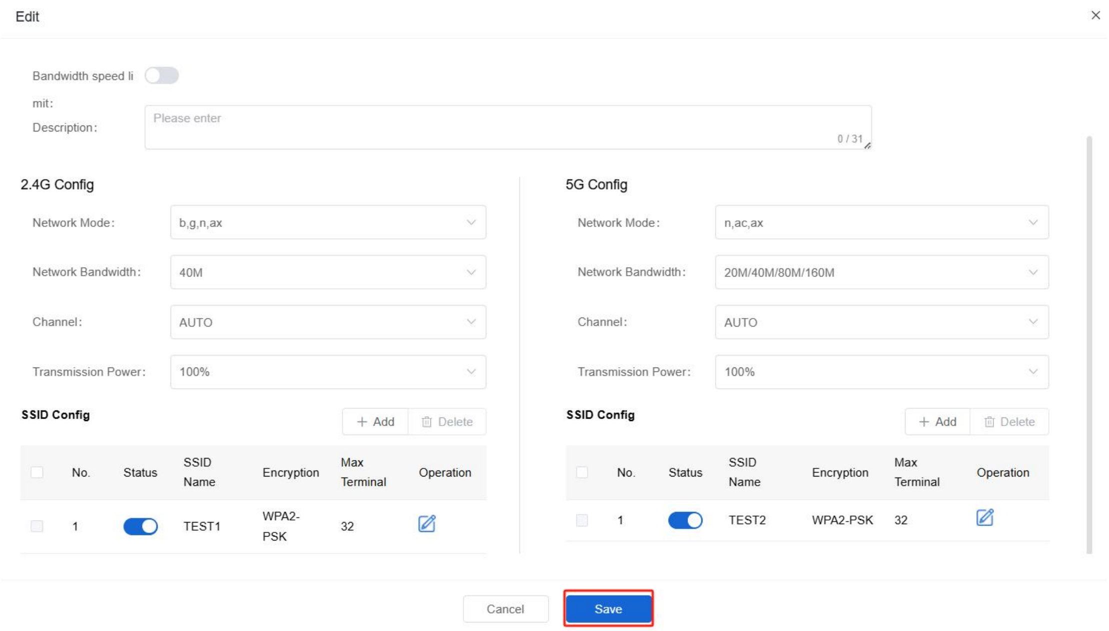
* Max Terminal: 32 0-32, 0 for no limit

VLAN ID: 20 2~4094, default is bridge mode

Client Isolation: ○

Broadcast SSID: ●

Step 7. Click "Submit" to save the SSID Config.



Bandwidth speed limit: ○

Description: Please enter 0 / 31

2.4G Config

Network Mode: b,g,n,ax

Network Bandwidth: 40M

Channel: AUTO

Transmission Power: 100%

SSID Config

□	No.	Status	SSID Name	Encryption	Max Terminal	Operation
□	1	●	TEST1	WPA2-PSK	32	✎

5G Config

Network Mode: n,ac,ax

Network Bandwidth: 20M/40M/80M/160M

Channel: AUTO

Transmission Power: 100%

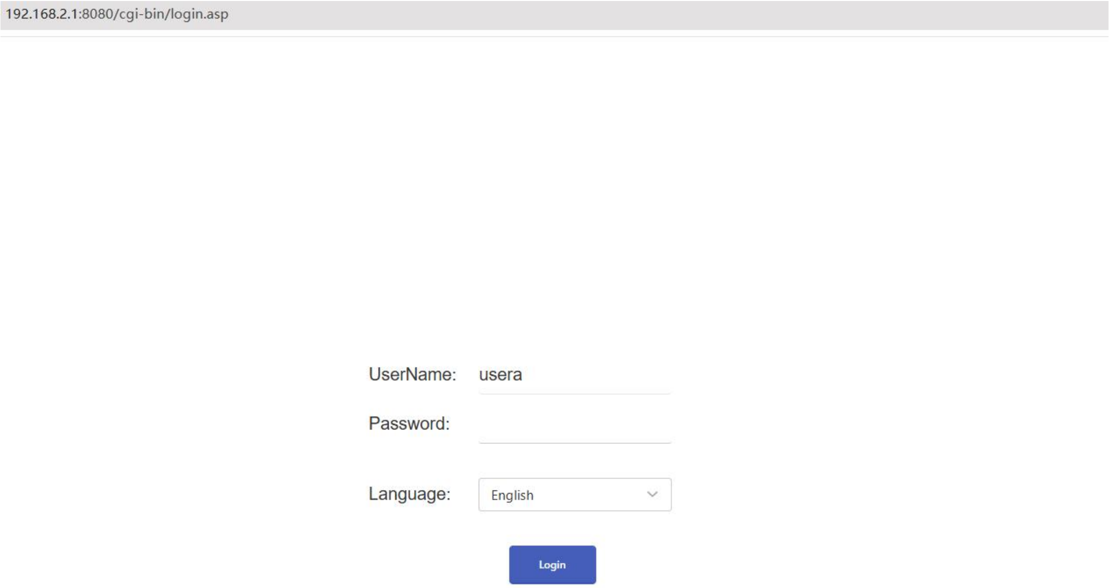
SSID Config

□	No.	Status	SSID Name	Encryption	Max Terminal	Operation
□	1	●	TEST2	WPA2-PSK	32	✎

4.2 Web Service Quick Configuration

4.2.1 Login WEB

Enter "http://192.168.2.1:8080/cgi-bin/login.asp"in the address bar of the browser, and then press the "Enter" key to jump to the login page.Enter the username in the login window (please refer to the product label for the initial username and password).

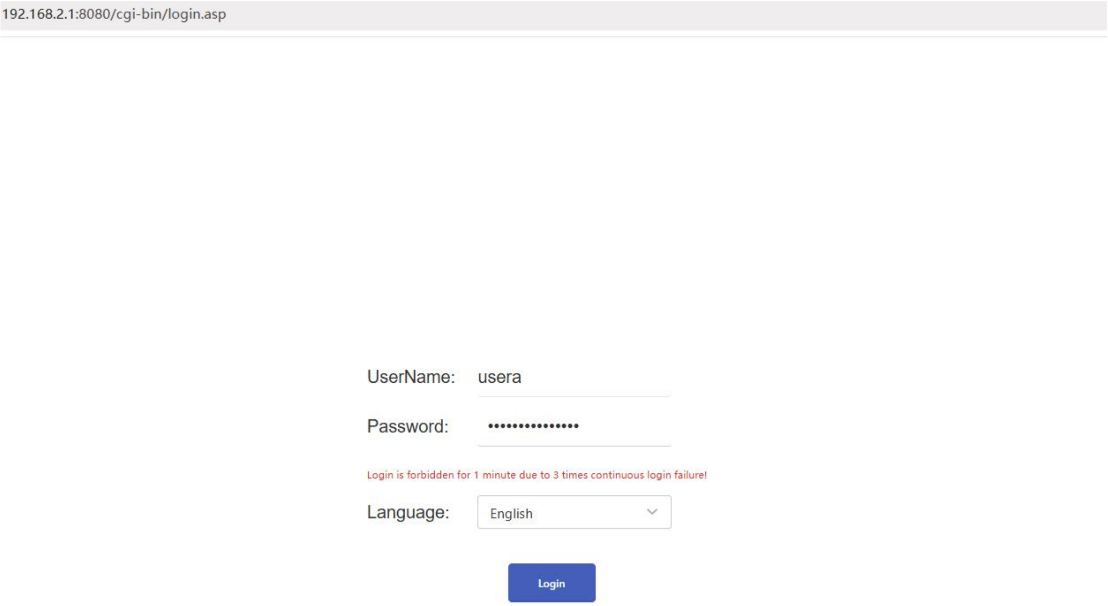


192.168.2.1:8080/cgi-bin/login.asp

UserName: usera

Password:

Language: English



192.168.2.1:8080/cgi-bin/login.asp

UserName: usera

Password: •••••••••••••••

Login is forbidden for 1 minute due to 3 times continuous login failure!

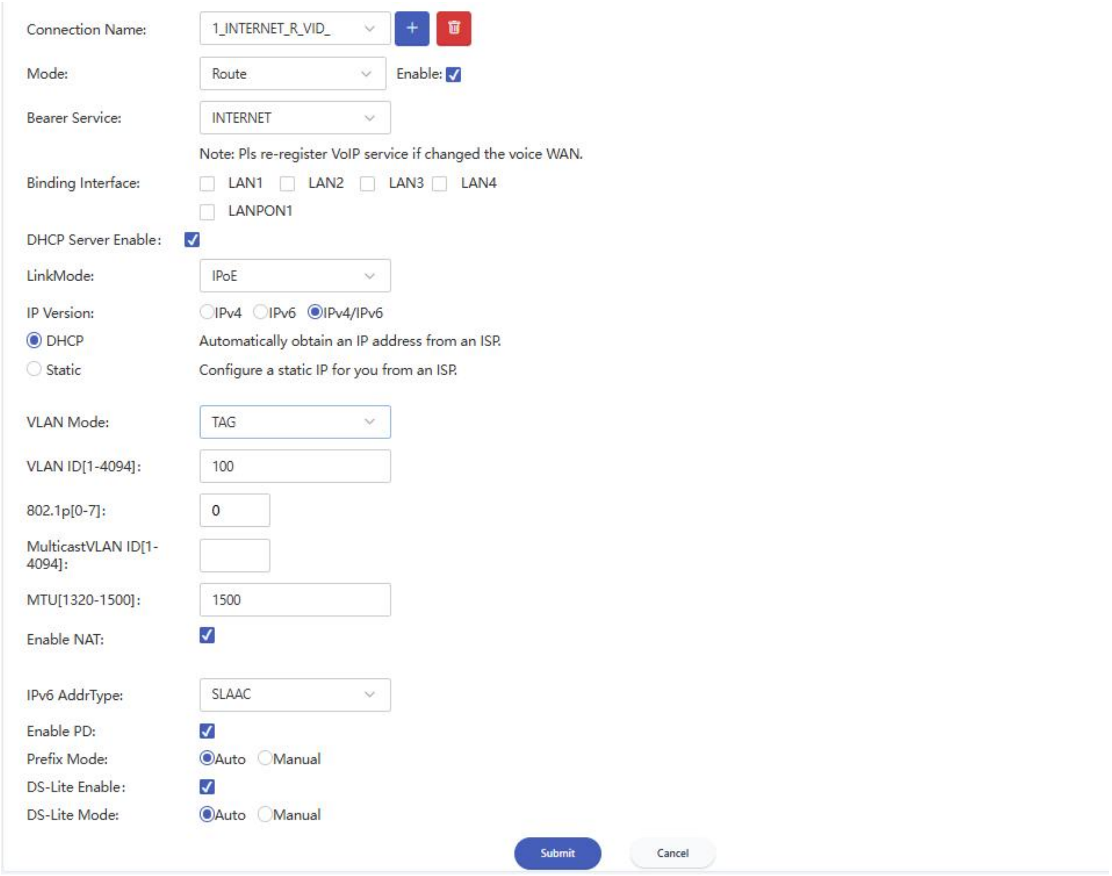
Language: English

Note : If you enter your password incorrectly 3 times in a row, you will be banned from logging in for 1 minute and you will have to wait for 1 minute before you can log in.

4.2.2 WAN Configuration

Configure a Route to WAN:

- Click "New" to create a new WAN.
- According to the parameter table, set the required configuration, click "Submit" to complete the configuration.



Connection Name: 1_INTERNET_R_VID_

Mode: Route Enable: ☑

Bearer Service: INTERNET

Note: Pls re-register VoIP service if changed the voice WAN.

Binding Interface: □ LAN1 □ LAN2 □ LAN3 □ LAN4
□ LANPON1

DHCP Server Enable: ☑

LinkMode: IPoE

IP Version: ○IPv4 ○IPv6 ●IPv4/IPv6

● DHCP Automatically obtain an IP address from an ISP.

○ Static Configure a static IP for you from an ISP.

VLAN Mode: TAG

VLAN ID[1-4094]: 100

802.1p[0-7]: 0

MulticastVLAN ID[1-4094]:

MTU[1320-1500]: 1500

Enable NAT: ☑

IPv6 AddrType: SLAAC

Enable PD: ☑

Prefix Mode: ●Auto ○Manual

DS-Lite Enable: ☑

DS-Lite Mode: ●Auto ○Manual

Parameter Description Table for Route Mode

Operating Mode	Configuration Parameters	Parameter Description
Route mode	Connection Name	WAN connection name
	Mode	Configurable as a route

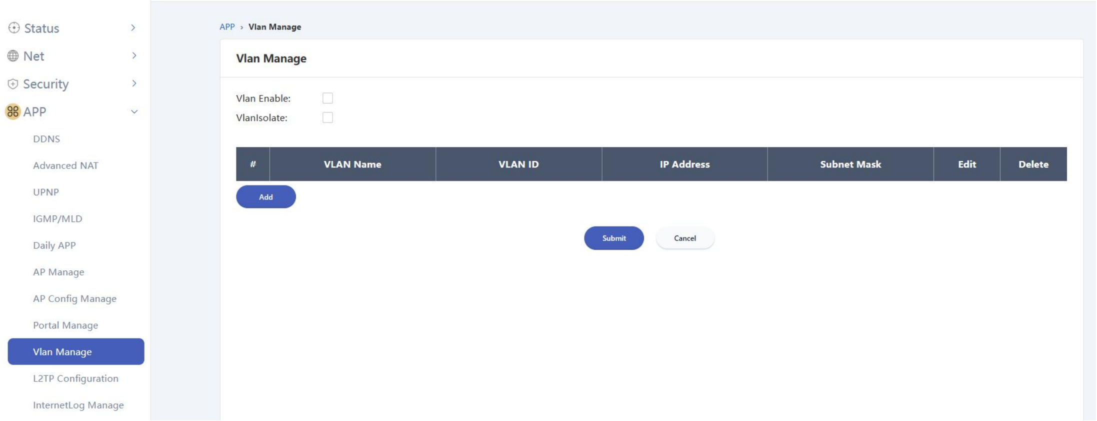
		Route:The PC is assigned an ip by the device and is on the same LAN
	Service type	Optional services including INTERNET,SPECIAL_SERVICE_1/2/3/4,OTHER
	Binding Interface	Lan port or wifi binding
	DHCP Server Enable	DHCP Server startup switch,In routing mode,if you need to assign ip by the device,you need to turn it on
	LinkMode	Configurable for IPoE or PPPoE
		IPoE:DHCP technology as the core,to realize the IP user session mechanism and other authentication systems.
		PPPoE:Provides access,control and billing functions for users in a peer-to-peer manner by establishing PPP sessions and encapsulating PPP messages as PPPoE messages
	IP Version	Configurable as IPv4/IPv6 single stack or IPv4&IPv6 dual stack
	VLAN Mode	Configure vlan mode
		TAG:VLAN tags are added when the device sends Ethernet frames
		UNTAG:VLAN tags are not added when the device sends Ethernet frames
	VLAN ID	Configure vlan,range:1-4094
	802.1p	Configuration priority,range:0-7
	Multicast VLAN ID	Configure multicast vlan,range:1-4094
	MTU	1) Maximum amount of data that an IP packet can carry over Ethernet,in bytes,range:1280-1500

		2) Range 1280-1492 when pppoe wan,fixed 1492
	Enable NAT	Enabling address translation and communication between private and public networks
	IPv6 AddrType	Get IPv6 address type
		SLAAC:stateless configuration
		DHCP:stateful configuration
	Enable PD	ipv6 Prefix Proxy switch for assigning address prefixes in IPv6 networks
	Prefix Mode	Prefix Mode
		Auto:auto-configuration
		Manual:Manual Configuration
	Prefix Address	Prefix address to identify the network or subnet.Used in prefix mode configured as manual or static wan scenarios
	Preferred Lifeime	Preferred Lifeime,range:600 - 4294967295s for prefix mode configured as manual or static wan scenarios
	Valid Lifetime	Valid Lifetime,range:600 - 4294967295s. Used in prefix mode configured as manual or static wan scenarios
	DS-Lite Enable	DS-Lite is an IPv4 NAT technology that uses IPv4 over IPv6 tunneling to enable users with IPv4 private addresses to traverse IPv6 networks to access IPv4 public networks
	DS-Lite Mode	DS-Lite Configuration Mode: Auto or Manual.
	DS-Lite Server	Configure a DS-Lite server.
	IP Address	IP address for static wan

	Subnet Mask	Subnet mask for static wan
	Default Gateway	Gateway to static wan
	Primary DNS Server	Primary DNS servers for static wan
	Secondary DNS Server	Secondary DNS servers for static wan
	IPv6 AddrType	IPv6 AddrType for static wan,only configure static
	IPv6 Address	IPv6 address for static wan
	IPv6 Default Gateway	IPv6 gateway to static wan
	Primary IPv6 DNS Server	IPv6 primary DNS servers for static wan
	Secondary IPv6 DNS Server	IPv6 secondary DNS servers for static wan
	UserName	Dial-up username for pppoe wan
	Password	Dial-up password for pppoe wan
	Service Name	service Name for pppoe wan
	Enable PPPoE Routing/Bridge Hybrid Mode	A network connection that combines the features of routing and bridging modes for pppoe wan

4.2.3 Multi-VLAN Configuration

Click "Add", set the relevant parameters of Multi-VLAN according to the parameter table. After confirming that they are correct, click "Submit" to complete the configuration.

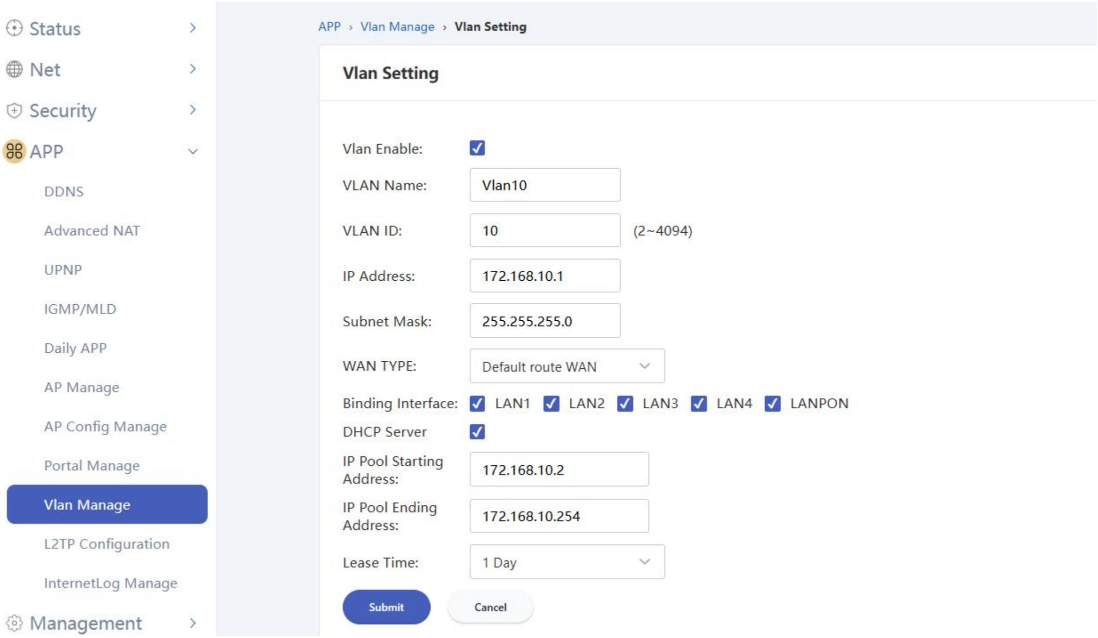


Vlan Manage

Vlan Enable: □

VlanIsolate: □

#	VLAN Name	VLAN ID	IP Address	Subnet Mask	Edit	Delete



Vlan Setting

Vlan Enable: ☑

VLAN Name: Vlan10

VLAN ID: 10 (2~4094)

IP Address: 172.168.10.1

Subnet Mask: 255.255.255.0

WAN TYPE: Default route WAN

Binding Interface: ☑ LAN1 ☑ LAN2 ☑ LAN3 ☑ LAN4 ☑ LANPON

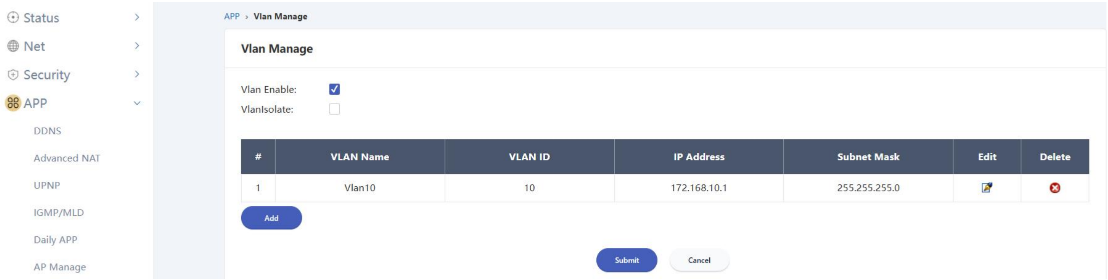
DHCP Server ☑

IP Pool Starting Address: 172.168.10.2

IP Pool Ending Address: 172.168.10.254

Lease Time: 1 Day

Check the "Vlan Enable" option and click "Submit" to turn on the Multi-VLAN functionality.



Vlan Manage

Vlan Enable: ☑

VlanIsolate: □

#	VLAN Name	VLAN ID	IP Address	Subnet Mask	Edit	Delete
1	Vlan10	10	172.168.10.1	255.255.255.0	✎	✖

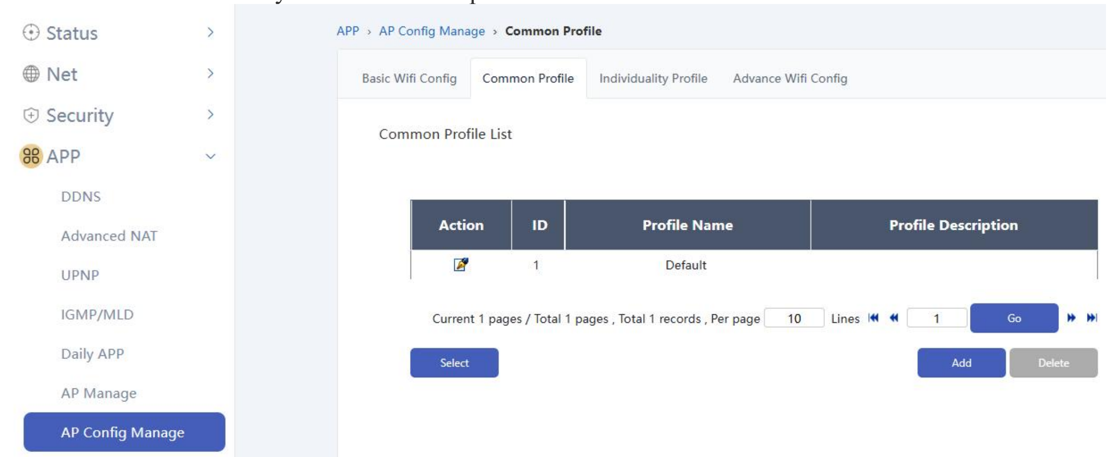
Multi-VLAN Parameter Description table

Operating Mode	**Configuration Parameters**	**Parameter Description**
Vlan Manage	Vlan Enable	Enable/Disable Multi-VLAN Function
	Vlan Isolate	Enable/Disable Multi-VLAN Traffic Isolation Feature
	VLAN Name	VLAN name
	VLAN ID	Configure vlan,range:2-4094
	IP Address	Enter the IPv4 Gateway Address for the VLAN
	Subnet Mask	Enter Subnet Mask
	WAN TYPE	Selectable WAN Types: Default route WAN/Specified interface WAN/Disable WAN access
	Binding Interface	LAN Port Binding
	DHCP Server	Enable/Disable DHCP Server
	IP Pool Starting Address	Starting Address of the Dynamically Allocated IP Address Range by the Server
	IP Pool Ending Address	Ending Address of the Dynamically Allocated IP Address Range by the Server
	Lease Time	Selectable IP Address Lease Time:1 Minute/1 Hour/1 Day/1 Week

Note : The dynamically allocated IP range is determined by the configured subnet mask.

4.2.4 Configure Multi-VLAN Binding to Wi-Fi Template

Click 'Edit' to Modify the Default Template of Common Profile.



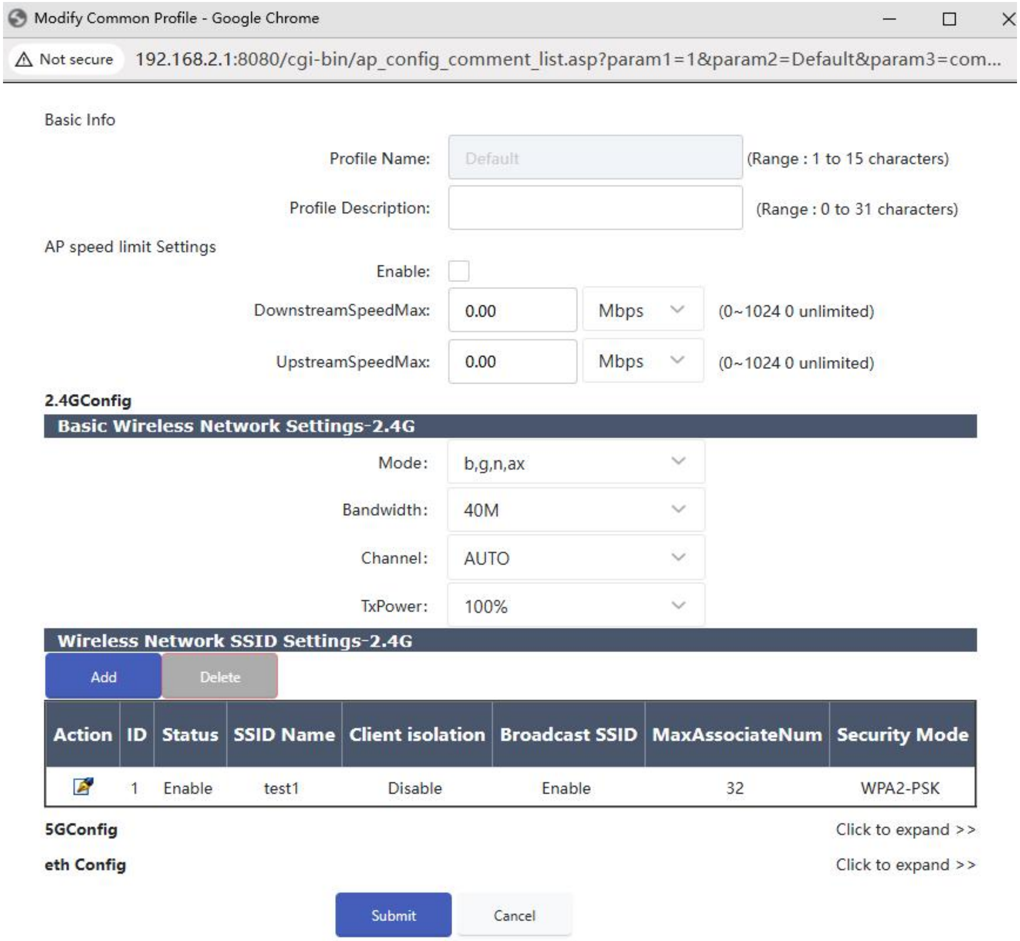
Common Profile List

Action	ID	Profile Name	Profile Description
✎	1	Default	

Current 1 pages / Total 1 pages , Total 1 records , Per page 10 Lines ⏮ ⏪ 1 ⏩ ⏭

4.2.4.1 Wireless Network SSID Configuration

Select the SSID under 2.4G and 5G configurations, click "Edit" to set the desired configuration according to the parameter table, then click "Submit" to complete the setup.


Modify Common Profile - Google Chrome
Not secure
192.168.2.1:8080/cgi-bin/ap_config_comment_list.asp?param1=1&param2=Default&param3=com...

Basic Info

Profile Name: Default (Range : 1 to 15 characters)

Profile Description: (Range : 0 to 31 characters)

AP speed limit Settings

Enable: □

DownstreamSpeedMax: 0.00 Mbps (0~1024 0 unlimited)

UpstreamSpeedMax: 0.00 Mbps (0~1024 0 unlimited)

2.4GConfig

Basic Wireless Network Settings-2.4G

Mode: b,g,n,ax

Bandwidth: 40M

Channel: AUTO

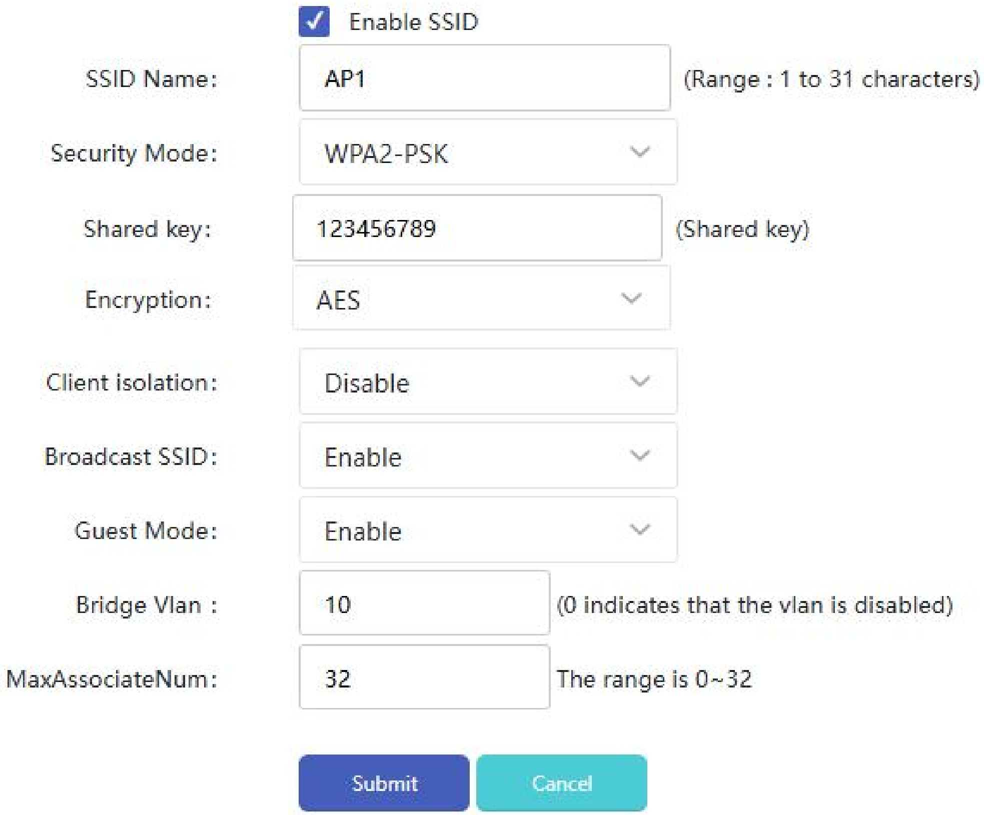
TxPower: 100%

Wireless Network SSID Settings-2.4G

Action	ID	Status	SSID Name	Client isolation	Broadcast SSID	MaxAssociateNum	Security Mode
📝	1	Enable	test1	Disable	Enable	32	WPA2-PSK

5GConfig Click to expand >>

eth Config Click to expand >>



☑ Enable SSID

SSID Name: AP1 (Range : 1 to 31 characters)

Security Mode: WPA2-PSK

Shared key: 123456789 (Shared key)

Encryption: AES

Client isolation: Disable

Broadcast SSID: Enable

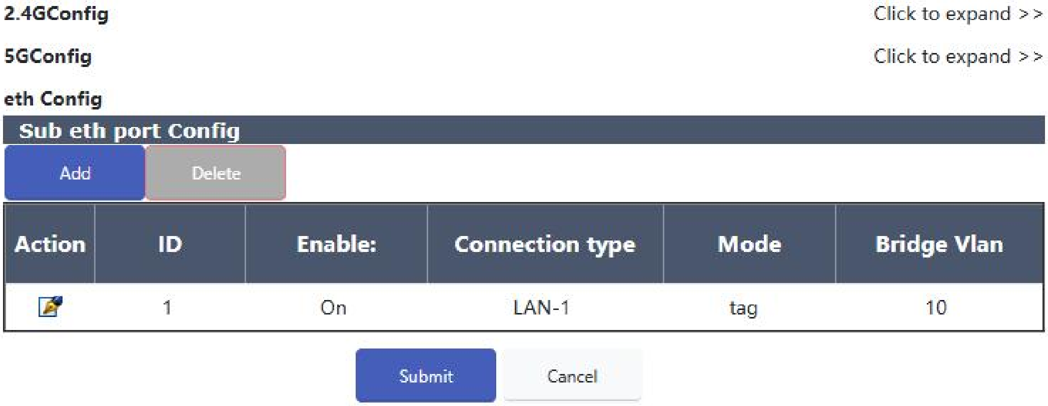
Guest Mode: Enable

Bridge Vlan : 10 (0 indicates that the vlan is disabled)

MaxAssociateNum: 32 The range is 0~32

4.2.4.2 Configure eth Config

Click 'Add' to Create a Sub eth Port Config Instance with Multi-VLAN Binding.



2.4GConfig Click to expand > >

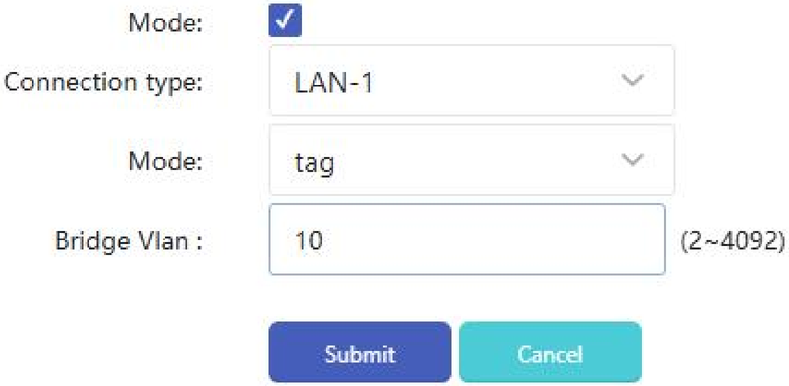
5GConfig Click to expand > >

eth Config

Sub eth port Config

Action	ID	Enable:	Connection type	Mode	Bridge Vlan
📝	1	On	LAN-1	tag	10

Set the relevant configurations as per the parameter table and click 'Submit' to finalize the setup.



Mode: ☑

Connection type: LAN-1

Mode: tag

Bridge Vlan : 10 (2~4092)

4.2.4.3 AP Modify Generic Template Configuration Parameter Description Table

Operating Mode	**Configuration Parameters**	**Parameter Description**
Basic Info	Profile Name	Profile Name, Range: 1 to 15 characters
	Profile Description	Profile Description, Range: 0 to 31 characters
AP speed limit Settings	Enable	Enable or disable speed limit function

	DownstreamSpeedMax	Downstream Maximum Speed, Range: 0~1024, where 0 indicates unlimited, unit: Mbps or Kbps
	UpstreamSpeedMax	Upstream Maximum Speed, Range: 0~1024, where 0 indicates unlimited, unit: Mbps or Kbps
Basic Wireless Network	Mode	This item is used to set the wireless working mode of the router. 2.4G:802.11b/g/n mixed mode is recommended. 5G:802.11ac/n/a mixed mode is recommended.
	Bandwidth	Wireless Channel Width. 2.4G Range: 20M, 40M, 5G Range:20M,40M.80M, 160M.
	Channel	The channel for data signal transmission with wireless signal as the transmission medium. If Auto is selected, the terminal will automatically select a best channel according to the surrounding environment. 2.4G:Channel can choose 1~13. 5G:Channel can choose 36/40/46/48/52 and so on.
	TxPower	Wireless transmit power, it is recommended to keep the default value of 100%.
	Enable SSID	Single 2.4G/5G Wi-Fi on/off switch
	SSID Name	SSID name
	Security Mode	Security modes,including OPEN/WPA-PSK/WPA2-PSK/WPA3-SAE Transition,etc.
	Shared key	Password for SSID
	Encryption	Encryption methods,including AES/TKIP/AES+TKIP,etc.
	Client isolation	Enable or Disable Client Isolation
	Broadcast SSID	Enable or disable SSID broadcast. After enabling, devices can discover and connect to this SSID.
	Bridge Vlan	After selecting the Bridge Vlan parameter, the SSID will be bound to the Multi-Vlan instance. Devices connected to this SSID will obtain IP addresses from the Multi-VLAN instance's subnet.0 indicates that the vlan is disabled

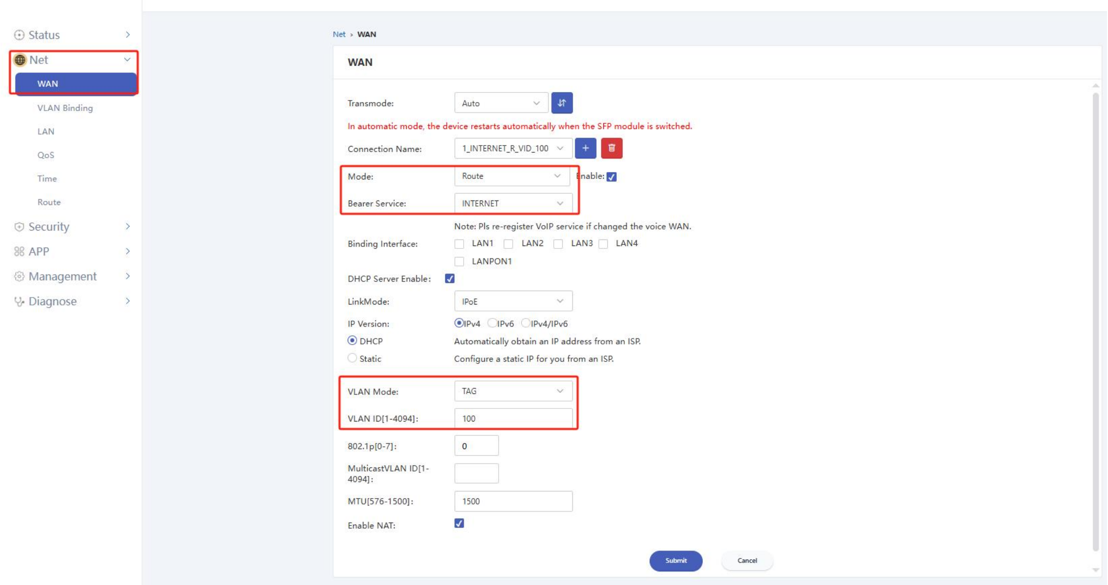
	MaxAssociateNum	The maximum number of connected clients for the SSID, range: 0-32,0 represents no limit.
Sub eth port Config	ID	Sub eth port Config Instance ID
	Enable	ON or OFF Sub eth port Config
	Connection type	Select the AP LAN-side port to configure, range: LAN1, LAN2, LAN3, LAN4
	Mode	Tag mode :transparent, tag, untag
	Bridge Vlan	The VLAN bound to the specified port, range: 2-4094.

Note : The value range of Bridge VLAN is determined by the created Multi-VLAN.

4.2.5 Examples

- Create a Route WAN with Tag 100 as the default WAN for Multi - VLAN.
- Enable "Vlan Enable" and create Multi-VLAN with VLAN 10 (172.168.10.1/24) and VLAN 20 (172.16.20.1/24).
- Configure the default template "Common Profile": bind 2.4G SSID1 to VLAN10; bind 5G SSID1 to VLAN20; In "eth Config", bind LAN1 to VLAN10.

Step 1. Click "Net" -> "WAN" to enter the WAN configuration interface, click "New" to create a Route WAN with Tag 100.



Transmode: Auto

In automatic mode, the device restarts automatically when the SFP module is switched.

Connection Name: 1_INTERNET_R_VID_100

Mode: Route Enable: ☑

Bearer Service: INTERNET

Note: Pls re-register VoIP service if changed the voice WAN.

Binding Interface: □ LAN1 □ LAN2 □ LAN3 □ LAN4 □ LANPON1

DHCP Server Enable: ☑

LinkMode: IPoE

IP Version: ● IPv4 ○ IPv6 ○ IPv4/IPv6

● DHCP Automatically obtain an IP address from an ISP.

○ Static Configure a static IP for you from an ISP.

VLAN Mode: TAG

VLAN ID[1-4094]: 100

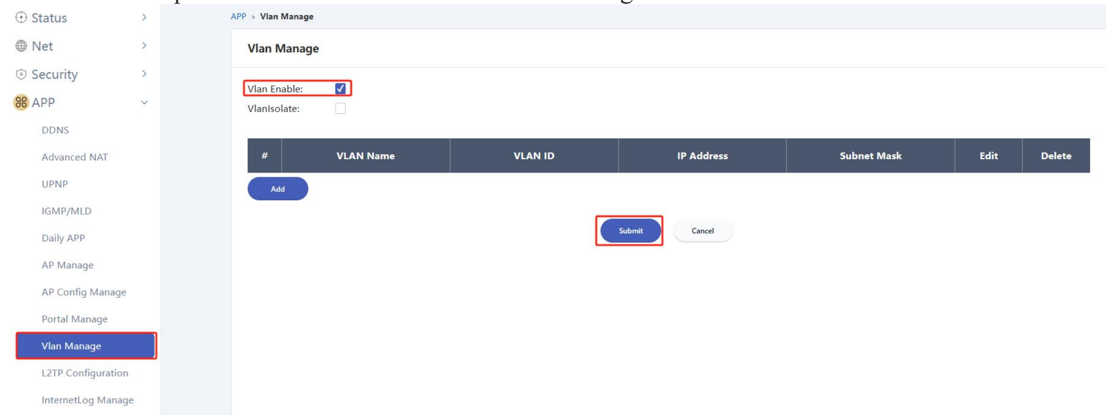
802.1p[0-7]: 0

MulticastVLAN ID[1-4094]:

MTU[576-1500]: 1500

Enable NAT: ☑

Step 2. Click "APP" -> "Vlan Manage" to enter the Multi-VLAN configuration interface. Check the "Vlan Enable" option and click "Submit" to save the configuration.

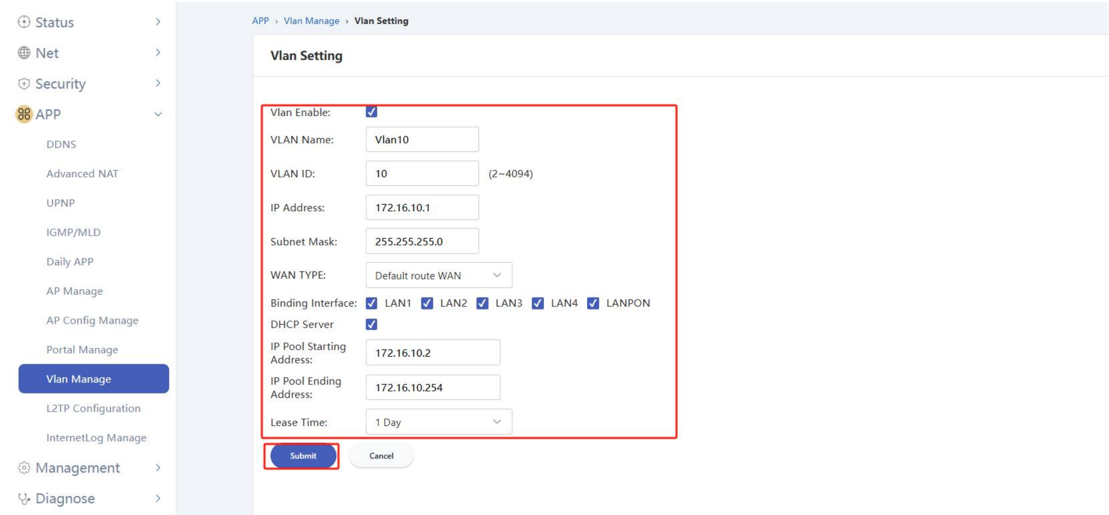


Vlan Enable: ☑

VlanIsolate: □

#	VLAN Name	VLAN ID	IP Address	Subnet Mask	Edit	Delete

Step 3. Click "Add" to create VLAN 10 and VLAN 20.



Vlan Setting

Vlan Enable: ☑

VLAN Name: Vlan10

VLAN ID: 10 (2~4094)

IP Address: 172.16.10.1

Subnet Mask: 255.255.255.0

WAN TYPE: Default route WAN

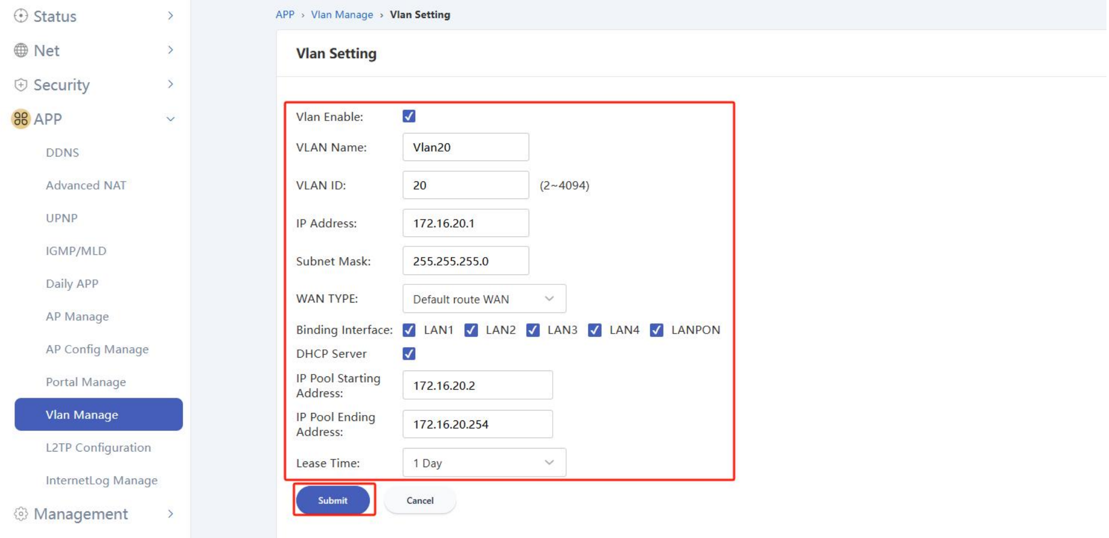
Binding Interface: ☑ LAN1 ☑ LAN2 ☑ LAN3 ☑ LAN4 ☑ LANPON

DHCP Server ☑

IP Pool Starting Address: 172.16.10.2

IP Pool Ending Address: 172.16.10.254

Lease Time: 1 Day



Vlan Setting

Vlan Enable: ☑

VLAN Name: Vlan20

VLAN ID: 20 (2~4094)

IP Address: 172.16.20.1

Subnet Mask: 255.255.255.0

WAN TYPE: Default route WAN

Binding Interface: ☑ LAN1 ☑ LAN2 ☑ LAN3 ☑ LAN4 ☑ LANPON

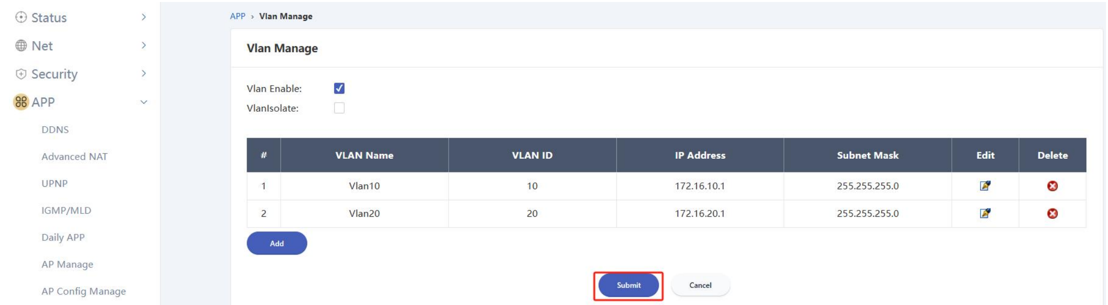
DHCP Server ☑

IP Pool Starting Address: 172.16.20.2

IP Pool Ending Address: 172.16.20.254

Lease Time: 1 Day

Step 4. Click "Submit" to save the Multi-VLAN configuration.

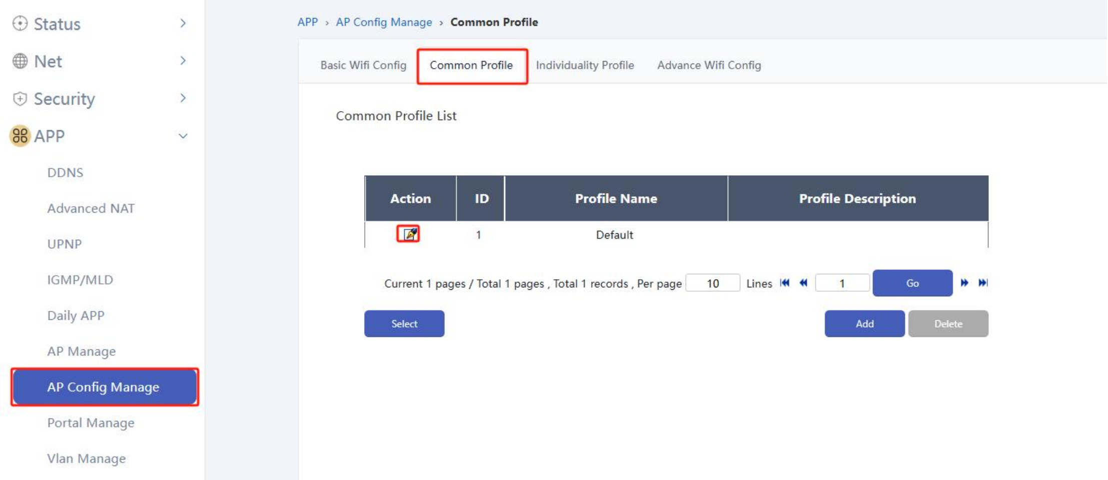


Vlan Enable: ☑

VlanIsolate: □

#	VLAN Name	VLAN ID	IP Address	Subnet Mask	Edit	Delete
1	Vlan10	10	172.16.10.1	255.255.255.0	✎	⊗
2	Vlan20	20	172.16.20.1	255.255.255.0	✎	⊗

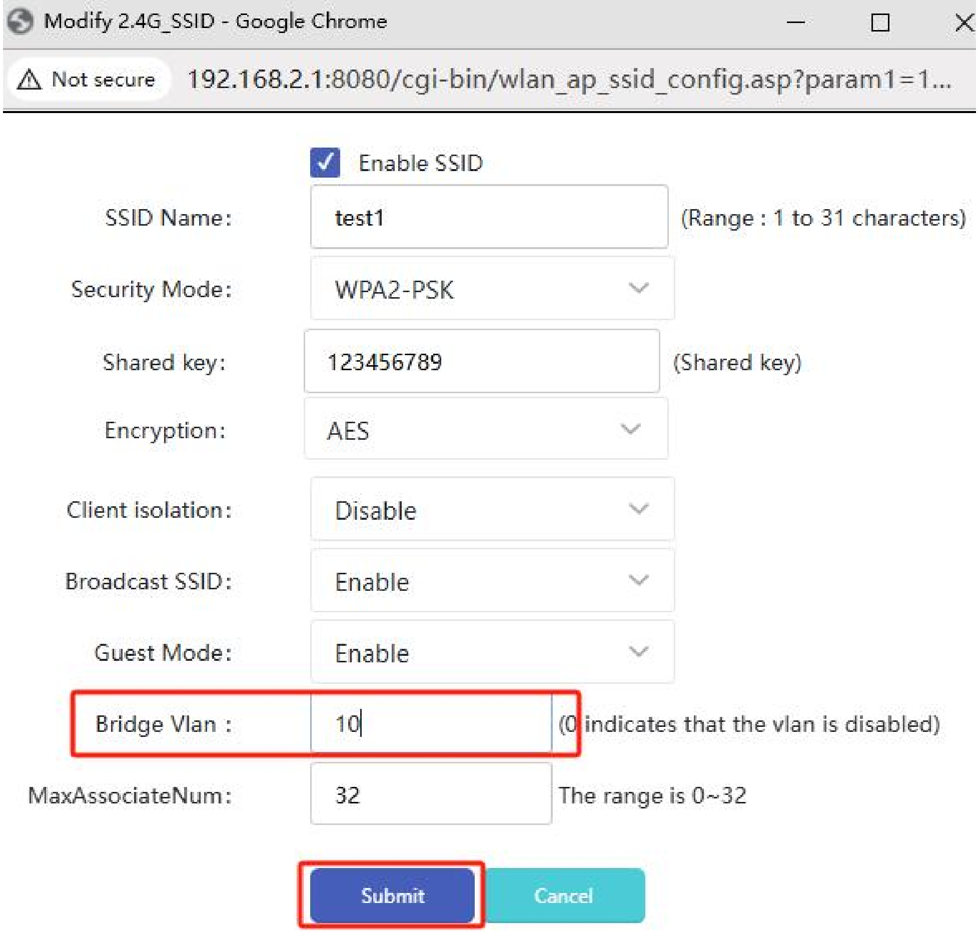
Step 5. Click "APP" -> "AP Config Manage"-> "Common Profile", click "Edit" to enter the Default Template configuration interface.



Action	ID	Profile Name	Profile Description
✎	1	Default	

Current 1 pages / Total 1 pages , Total 1 records , Per page 10 Lines 1

Step 6. Click "Edit" and configure the following: Bind the 2.4G SSID1 to VLAN10 and the 5G SSID1 to VLAN20.

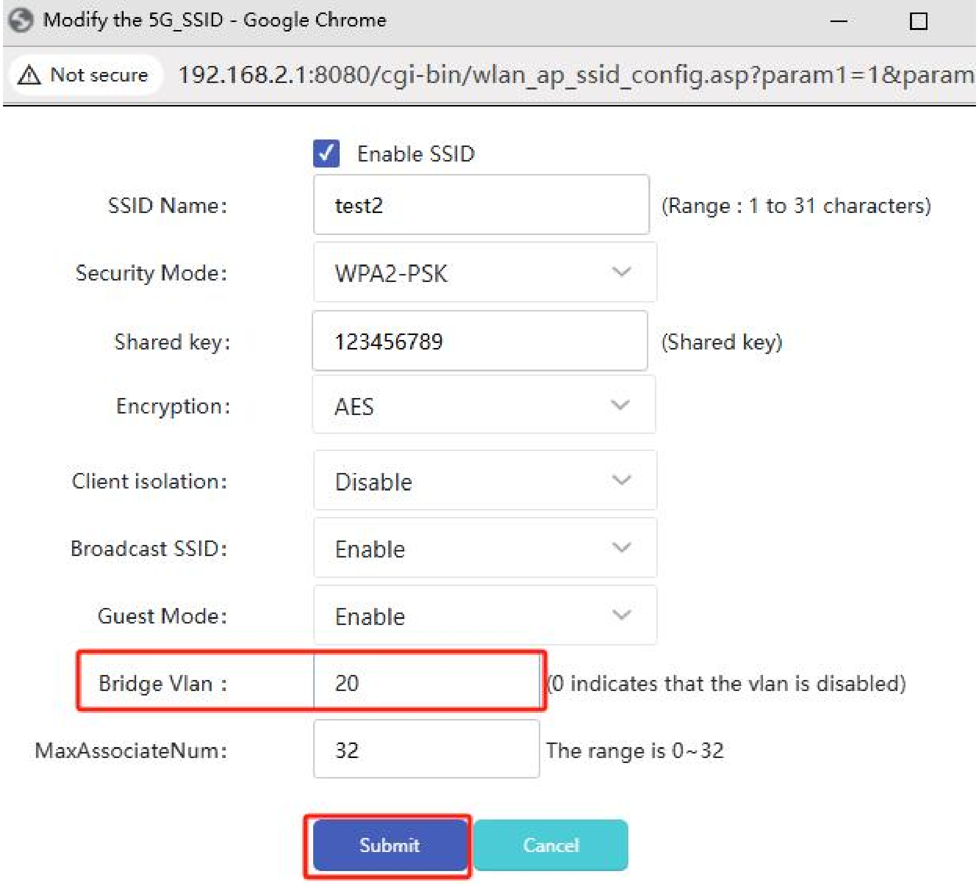


Modify 2.4G_SSID - Google Chrome

Not secure 192.168.2.1:8080/cgi-bin/wlan_ap_ssid_config.asp?param1=1...

☑ Enable SSID

SSID Name:	test1	(Range : 1 to 31 characters)
Security Mode:	WPA2-PSK	
Shared key:	123456789	(Shared key)
Encryption:	AES	
Client isolation:	Disable	
Broadcast SSID:	Enable	
Guest Mode:	Enable	
Bridge Vlan :	10	(0 indicates that the vlan is disabled)
MaxAssociateNum:	32	The range is 0~32


Modify the 5G_SSID - Google Chrome
Not secure
192.168.2.1:8080/cgi-bin/wlan_ap_ssid_config.asp?param1=1&param

☑ Enable SSID

SSID Name: test2 (Range : 1 to 31 characters)

Security Mode: WPA2-PSK

Shared key: 123456789 (Shared key)

Encryption: AES

Client isolation: Disable

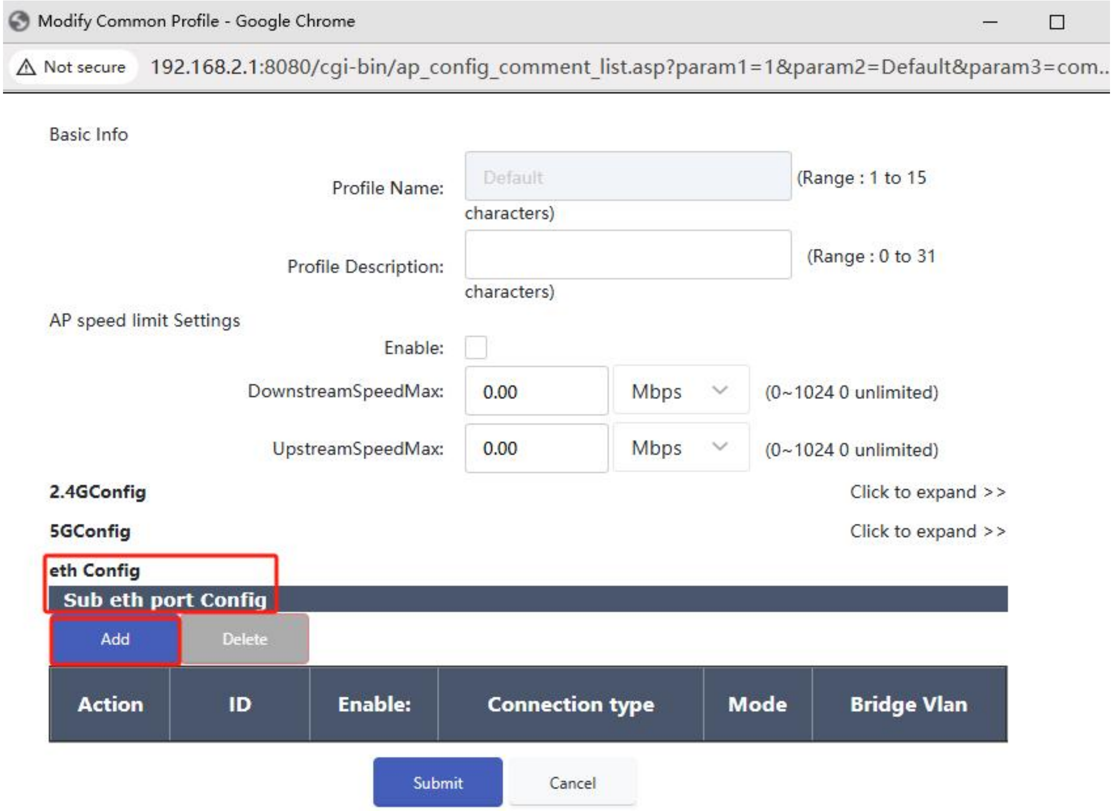
Broadcast SSID: Enable

Guest Mode: Enable

Bridge Vlan : 20 (0 indicates that the vlan is disabled)

MaxAssociateNum: 32 The range is 0~32

Step 7. Click "eth Config" to enter the "Sub eth port Config" configuration interface, click "Add" to set LAN1 to be bound to VLAN10, and click 'Submit' to save the configuration.


Modify Common Profile - Google Chrome
Not secure
192.168.2.1:8080/cgi-bin/ap_config_comment_list.asp?param1=1&param2=Default&param3=com..

Basic Info

Profile Name: Default (Range : 1 to 15 characters)

Profile Description: (Range : 0 to 31 characters)

AP speed limit Settings

Enable: □

DownstreamSpeedMax: 0.00 Mbps (0~1024 0 unlimited)

UpstreamSpeedMax: 0.00 Mbps (0~1024 0 unlimited)

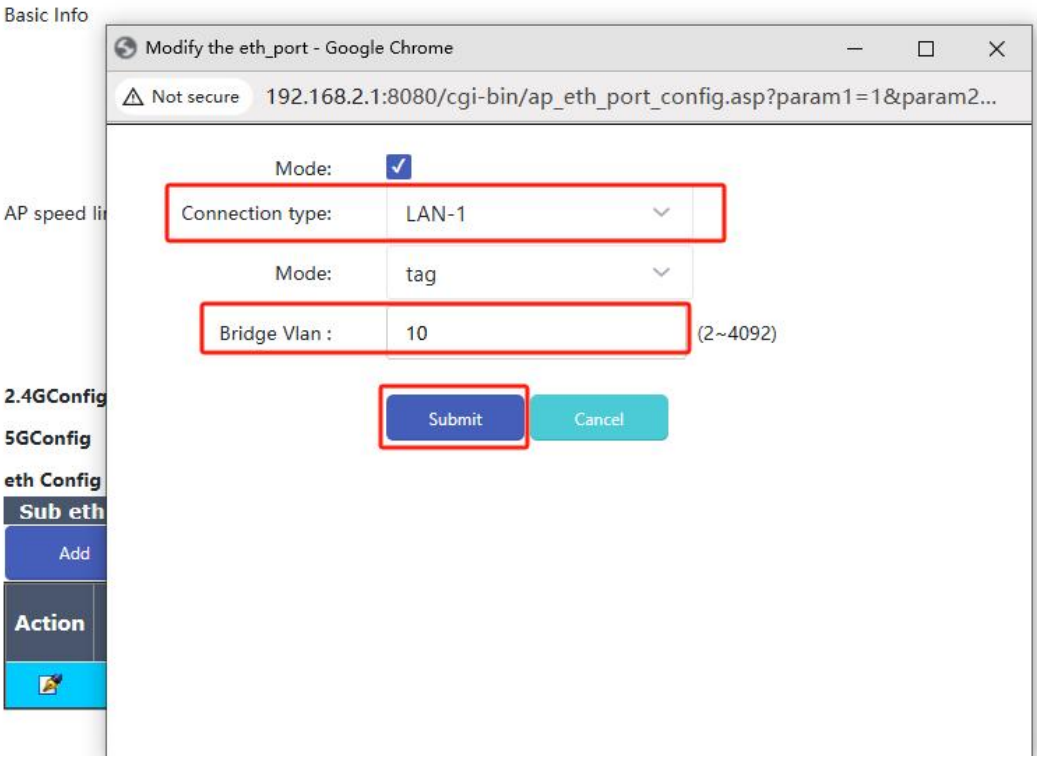
2.4GConfig Click to expand >>

5GConfig Click to expand >>

eth Config

Sub eth port Config

Action	ID	Enable:	Connection type	Mode	Bridge Vlan



192.168.2.1:8080/cgi-bin/ap_eth_port_config.asp?param1=1&param2...

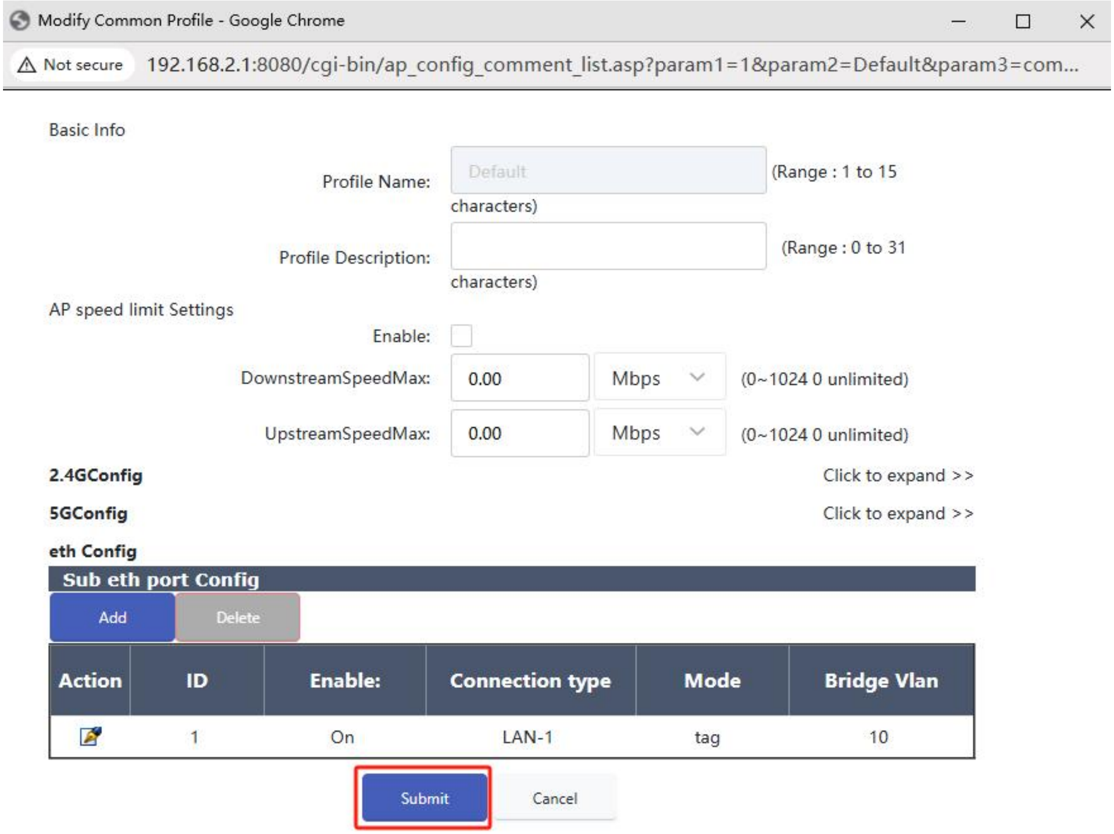
Mode: ☑

Connection type: LAN-1

Mode: tag

Bridge Vlan : 10 (2~4092)

Step 8. Click "Submit" to complete the default template configuration for Common Profile.


Modify Common Profile - Google Chrome

Not secure 192.168.2.1:8080/cgi-bin/ap_config_comment_list.asp?param1=1&param2=Default&param3=com...

Basic Info

Profile Name: Default (Range : 1 to 15 characters)

Profile Description: (Range : 0 to 31 characters)

AP speed limit Settings

Enable: □

DownstreamSpeedMax: 0.00 Mbps (0~1024 0 unlimited)

UpstreamSpeedMax: 0.00 Mbps (0~1024 0 unlimited)

2.4GConfig Click to expand >>

5GConfig Click to expand >>

eth Config

Sub eth port Config

Add Delete

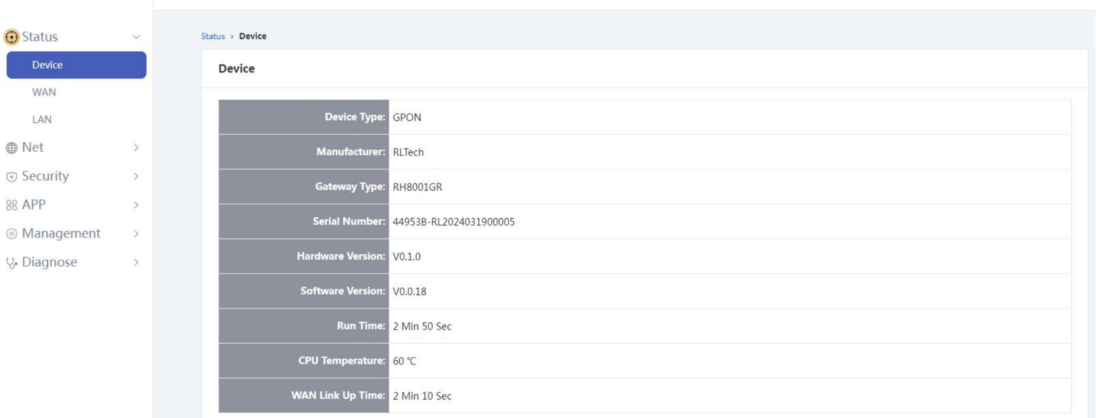
Action	ID	Enable:	Connection type	Mode	Bridge Vlan
	1	On	LAN-1	tag	10

Submit Cancel

5. Status Information

5.1 Device Information

View device model, hardware version, and software version information.Click on the menu "Status -> Device" as shown in the figure.



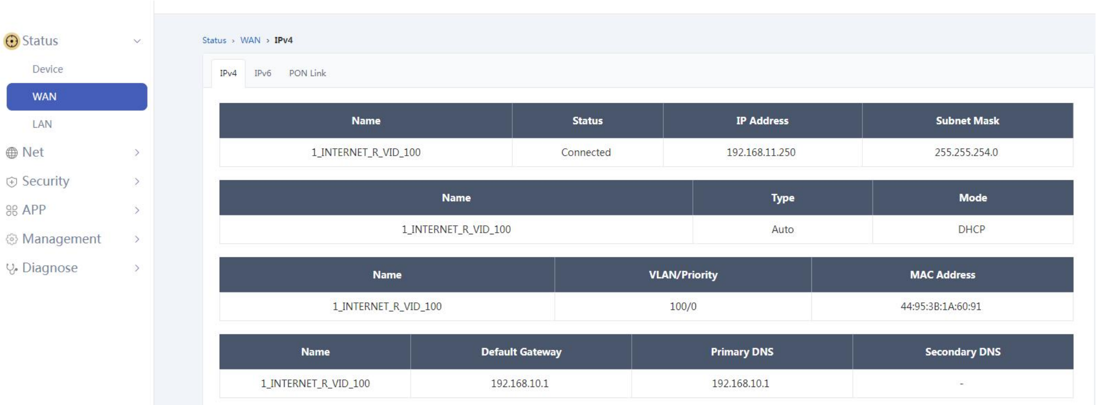
Device

Device Type:	GPON
Manufacturer:	RLTech
Gateway Type:	RH8001GR
Serial Number:	44953B-RL2024031900005
Hardware Version:	V0.1.0
Software Version:	V0.0.18
Run Time:	2 Min 50 Sec
CPU Temperature:	60 ℃
WAN Link Up Time:	2 Min 10 Sec

5.2 WAN

5.2.1 IPv4 Connection Information

View the status of the IPv4 WAN, IP acquisition method, IP address, and subnet mask information. Click on "Status -> WAN" as shown in the figure.



Name	Status	IP Address	Subnet Mask
1_INTERNET_R_VID_100	Connected	192.168.11.250	255.255.254.0

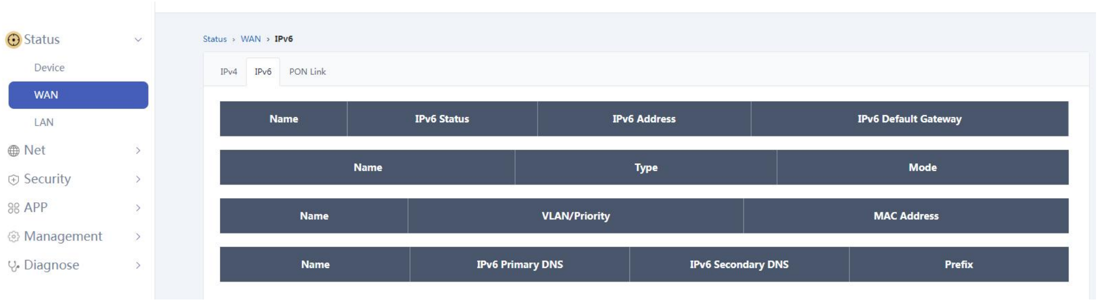
Name	Type	Mode
1_INTERNET_R_VID_100	Auto	DHCP

Name	VLAN/Priority	MAC Address
1_INTERNET_R_VID_100	100/0	44:95:3B:1A:60:91

Name	Default Gateway	Primary DNS	Secondary DNS
1_INTERNET_R_VID_100	192.168.10.1	192.168.10.1	-

5.2.2 IPv6 Connection Information

View the status of the IPv6 WAN, IP address, and gateway information. Click on "Status -> WAN -> IPv6" as illustrated in the figure below.



Name	IPv6 Status	IPv6 Address	IPv6 Default Gateway

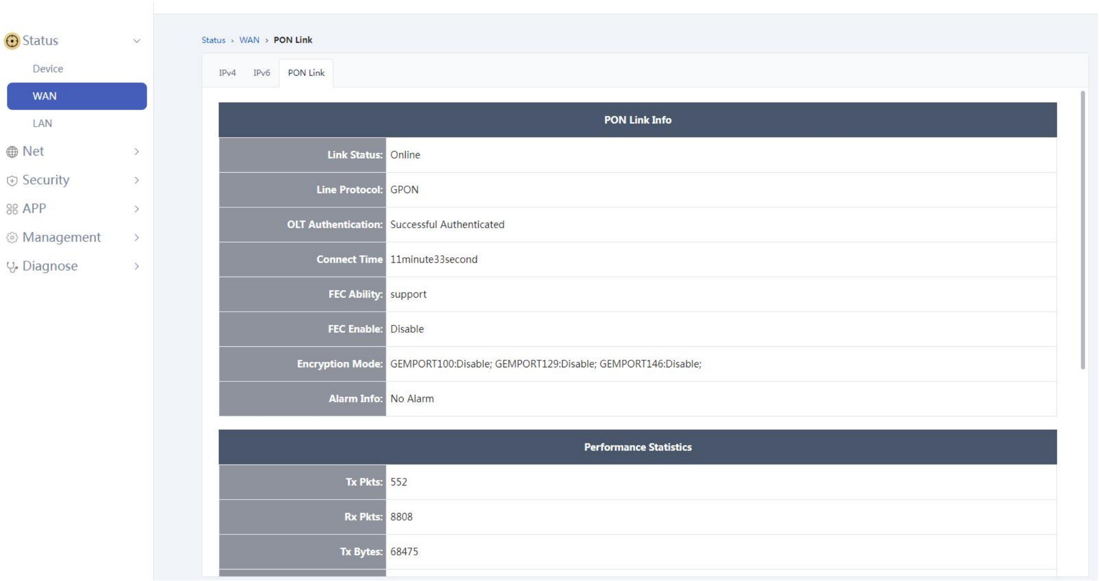
Name	Type	Mode

Name	VLAN/Priority	MAC Address

Name	IPv6 Primary DNS	IPv6 Secondary DNS	Prefix

5.2.3 PON Link Connection Information

View the transmit and receive optical power of the device's optical module. Click on "Status -> WAN -> PON Link " as shown in the figure.



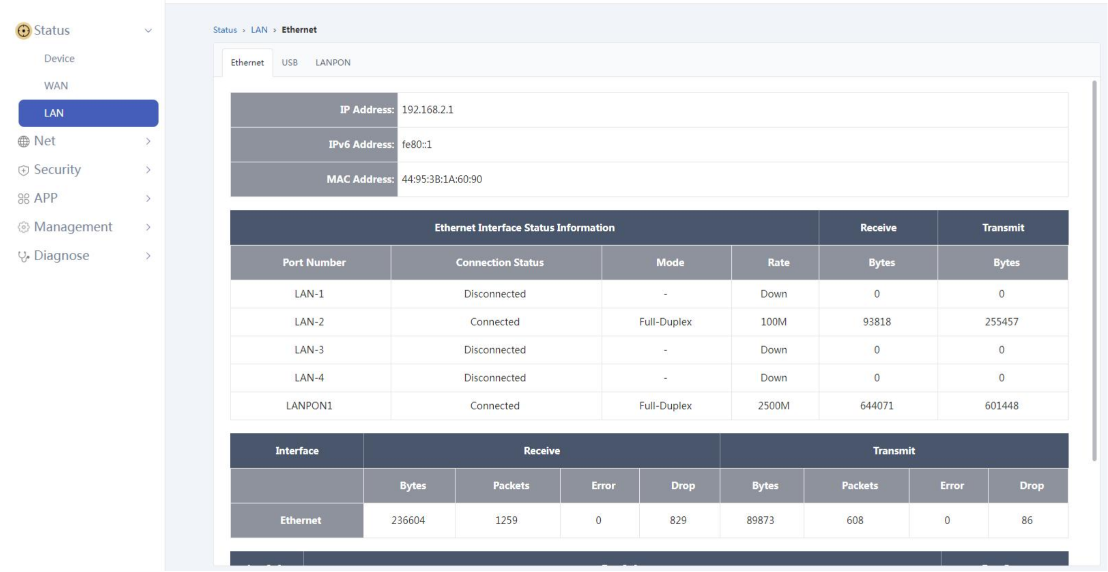
PON Link Info	
Link Status:	Online
Line Protocol:	GPON
OLT Authentication:	Successful Authenticated
Connect Time	11minute33second
FEC Ability:	support
FEC Enable:	Disable
Encryption Mode:	GEMPORT100:Disable; GEMPORT129:Disable; GEMPORT146:Disable;
Alarm Info:	No Alarm

Performance Statistics	
Tx Pkts:	552
Rx Pkts:	8808
Tx Bytes:	68475

5.3 LAN

5.3.1 Ethernet Interface Information

View duplex mode, speed, and status information for each ethernet port. Click on "Status -> LAN" as shown in the figure.



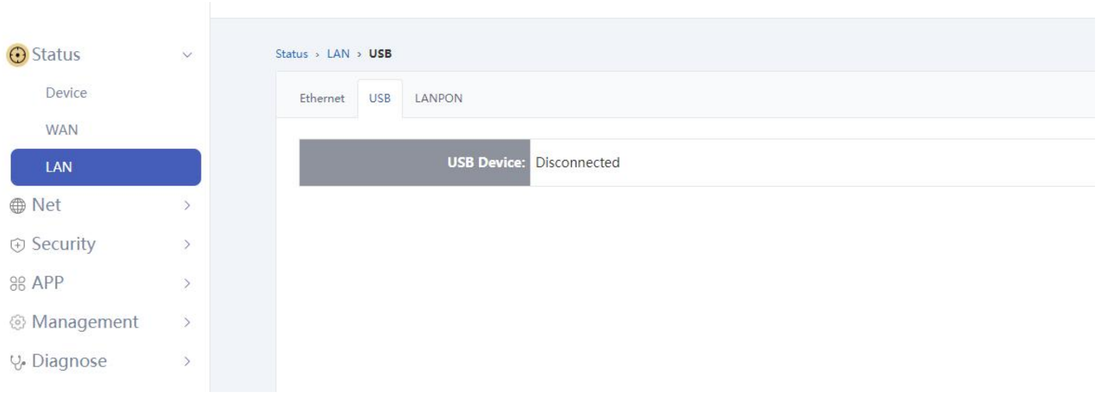
IP Address:	192.168.2.1
IPv6 Address:	fe80::1
MAC Address:	44:95:3B:1A:60:90

Ethernet Interface Status Information				Receive	Transmit
Port Number	Connection Status	Mode	Rate	Bytes	Bytes
LAN-1	Disconnected	-	Down	0	0
LAN-2	Connected	Full-Duplex	100M	93818	255457
LAN-3	Disconnected	-	Down	0	0
LAN-4	Disconnected	-	Down	0	0
LANPON1	Connected	Full-Duplex	2500M	644071	601448

Interface	Receive				Transmit			
	Bytes	Packets	Error	Drop	Bytes	Packets	Error	Drop
Ethernet	236604	1259	0	829	89873	608	0	86

5.3.2 USB Interface Information

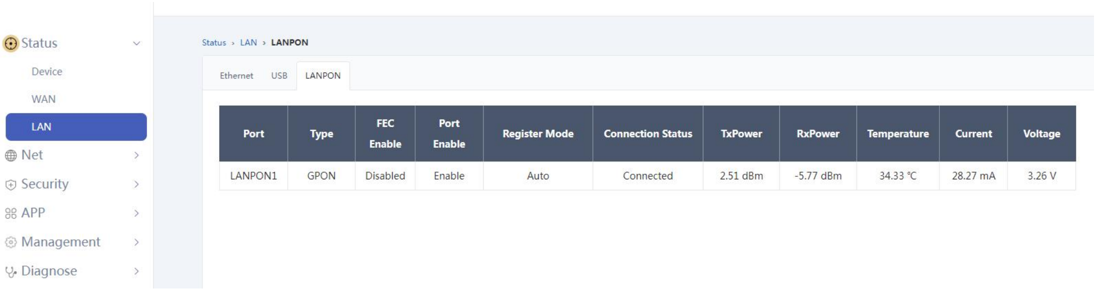
View the connection status of the USB interface. Click on "Status -> LAN -> USB" as shown in the figure.



USB Device: Disconnected

5.3.3 LANPON Information

View the connection status, transmit optical power, and receive optical power of the downstream optical module.Click on "Status -> LAN -> LANPON" as shown in the figure.



Port	Type	FEC Enable	Port Enable	Register Mode	Connection Status	TxPower	RxPower	Temperature	Current	Voltage
LANPON1	GPON	Disabled	Enable	Auto	Connected	2.51 dBm	-5.77 dBm	34.33 ℃	28.27 mA	3.26 V

6. Device Parameter Configuration

6.1 NET

6.1.1 Broadband Setting

On the network side, the device can work with network equipment to complete user access, IP address allocation, and user information authentication management functions, supporting network operations.

On the user side, the device supports enterprise network operation by providing IP address allocation, address resolution, and other management services.

A. Support for acquiring IPv4 addresses.

   a) Supports establishing two IPv4 routing network connections simultaneously with consistent service types and binding relationships. Both connections can acquire IPv4 addresses and be effective at the same time.

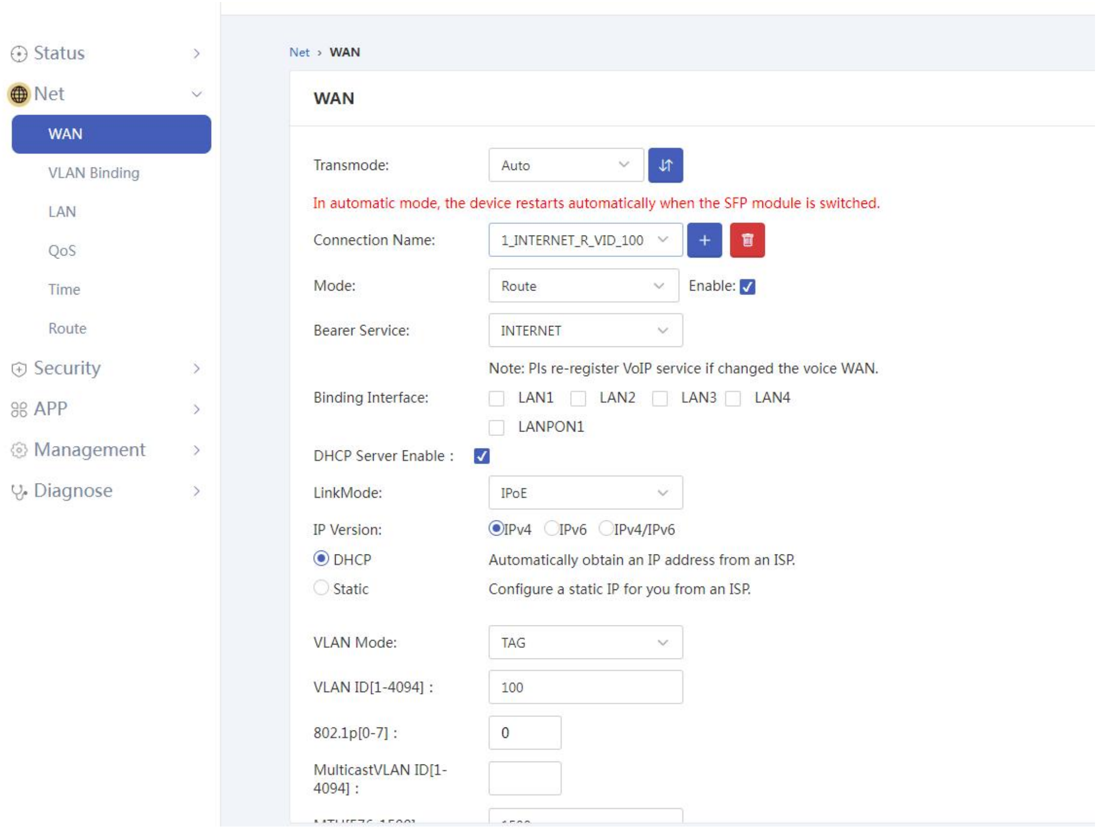
   b) Supports establishing one IPv4 network connection, acquiring an IPv4 address, and supporting IPv4 applications.

B. Can automatically enable the corresponding protocol stack based on the type of acquired IP address.

C. When accessing the internet, it can automatically select the appropriate network connection or enable the corresponding protocol stack based on the type of the destination IP address.

D. Supports routing mode, bridge mode, and hybrid bridge-routing mode, all of which can forward IPv4 packets simultaneously.

After logging in successfully, click on the menu "Net -> WAN" to enter the broadband settings page, as illustrated in the figure below.



WAN

Transmode: Auto

In automatic mode, the device restarts automatically when the SFP module is switched.

Connection Name: 1_INTERNET_R_VID_100

Mode: Route Enable: ☑

Bearer Service: INTERNET

Note: Pls re-register VoIP service if changed the voice WAN.

Binding Interface: □ LAN1 □ LAN2 □ LAN3 □ LAN4 □ LANPON1

DHCP Server Enable : ☑

LinkMode: IPoE

IP Version: ● IPv4 ○ IPv6 ○ IPv4/IPv6

● DHCP Automatically obtain an IP address from an ISP.

○ Static Configure a static IP for you from an ISP.

VLAN Mode: TAG

VLAN ID[1-4094] : 100

802.1p[0-7] : 0

MulticastVLAN ID[1-4094] :

Parameter description table for Route Mode:

Operating mode	Configuration parameters	Parameter description
Route mode	Transmode	Select upstream mode, options include Auto(adaptive), GPON, XG-PON, XGS-PON, GE/10GE, Ethernet.
	Connection Name	WAN connection name.
	Mode	Configurable as a route.
		Route:The PC is assigned an ip by the device and is on the same LAN.
	Bearer Server	Optional services including INTERNET/OTHER.
	Binding Interface	Lan port or Wi-Fi binding.

DHCP Server Enable	DHCP Server startup switch, in routing mode, if you need to assign ip by the device, you need to turn it on.
LinkMode	Configurable for IPoE or PPPoE.
	IPoE:DHCP technology as the core, to realize the IP user session mechanism and other authentication systems.
	PPPoE: Provides access, control and billing functions for users in a peer-to-peer manner by establishing PPP sessions and encapsulating PPP messages as PPPoE messages.
IP Version	Configurable as IPv4/IPv6 single stack or IPv4&IPv6 dual stack.
VLAN Mode	Configure vlan mode.
	TAG:VLAN tags are added when the device sends Ethernet frames.
	UNTAG:VLAN tags are not added when the device sends Ethernet frames.
VLAN ID	Configure vlan, range:1-4094.
802.1p	Configuration priority,range:0-7.
Multicast VLAN ID	Configure multicast vlan,range:1-4094.
MTU	1) Maximum amount of data that an IP packet can carry over Ethernet,in bytes,range:1280-1500. 2) Range 1280-1492 when pppoe wan,fixed 1492.
Enable NAT	Enabling address translation and communication between private and public networks.
IPv6 AddrType	Get IPv6 address type.
	SLAAC:stateless configuration.
	DHCP:stateful configuration.
Enable PD	IPv6 Prefix Proxy switch for assigning address prefixes in IPv6 networks.
Prefix Mode	Prefix Mode.
	Auto:auto-configuration.
	Manual:Manual Configuration.
Prefix Address	Prefix address to identify the network or subnet.Used in prefix mode configured as manual or static wan scenarios
Preferred Lifetime	Preferred Lifetime,range:600 - 4294967295s for prefix mode configured as manual or static wan scenarios.

	Valid Lifetime	Valid Lifetime,range:600 - 4294967295s. Used in prefix mode configured as manual or static wan scenarios.
	DS-Lite Enable	DS-Lite is an IPv4 NAT technology that uses IPv4 over IPv6 tunneling to enable users with IPv4 private addresses to traverse IPv6 networks to access IPv4 public networks.
	IP Address	IP address for static wan.
	Subnet Mask	Subnet mask for static wan.
	Default Gateway	Gateway to static wan.
	Primary DNS Server	Primary DNS servers for static wan.
	Secondary DNS Server	Secondary DNS servers for static wan.
	IPv6 AddrType	IPv6 AddrType for static wan,only configure static.
	IPv6 Address	IPv6 address for static wan.
	IPv6 Default Gateway	IPv6 gateway to static wan.
	Primary IPv6 DNS Server	IPv6 primary DNS servers for static wan.
	Secondary IPv6 DNS Server	IPv6 secondary DNS servers for static wan.
	UserName	Dial-up username for pppoe wan.
	Password	Dial-up password for pppoe wan.
	Service Name	Service Name for pppoe wan.
	Enable PPPoE Routing/Bridge Hybrid Mode	A network connection that combines the features of routing and bridging modes for pppoe wan.

Parameter description table for Bridge Mode:

Operating mode	Configuration parameters	Parameter description
Bridge Mode	Transmode	Select upstream mode, options include Auto(adaptive), GPON, XG-PON, XGS-PON, GE/10GE, Ethernet.
	Connection Name	WAN connection name.
	Mode	Configurable as a bridge.
		Bridge:The PC is assigned ip directly by the upper layer server,without going through the device.
	Bearer Server	Optional services,including INTERNET/OTHER.
	Binding Interface	Lan port or Wi-Fi binding.

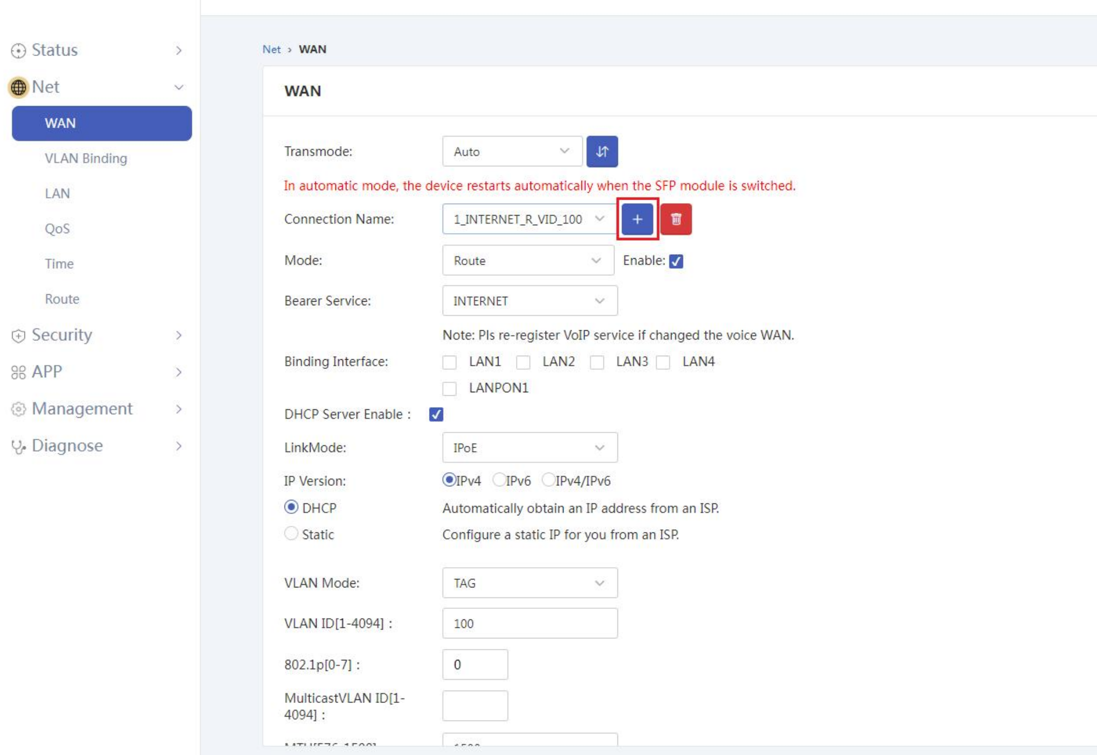
	DHCP Server Enable	DHCP Server startup switch,automatically turned off when server is configured as other.
	IP Version	Configurable as IPv4/IPv6 single stack or IPv4&IPv6 dual stack.
	Bridge Mode	Configurable as IP_Bridged or PPPoE_Bridged.
	DHCP Transparent Transmit	DHCP Relay provides transparent transmit of DHCP broadcast messages,and is automatically checked when server is configured as other.
	VLAN Mode	Configure vlan mode.
		TAG:VLAN tags are added when the device sends Ethernet frames.
		UNTAG:VLAN tags are not added when the device sends Ethernet frames.
		TRANSPARENT:When the device sends an Ethernet frame,it does not do any processing and forwards it directly.
	VLAN ID	Configure vlan,range:1-4094.
	802.1p	Configuration priority,range:0-7.
	Multicast VLAN ID	Configure multicast vlan,range:1-4094.

Note:

- Routing WAN Mode: Used as a gateway device. The ONU's IP address can be obtained via DHCP, Static, or PPPoE. IP addresses for downstream user-side devices are obtained through the device's DHCP pool or manually set.
- Bridge WAN Mode: The gateway WAN does not obtain an IP address from upstream devices and cannot have a static IP address manually set. It acts as a transparent device without processing data. IP addresses for downstream user-side devices can be obtained via DHCP, PPPoE, or manual setting.
- DHCP: Dynamically acquires IP addresses.
- Static:Manually sets IP addresses, requiring input of IP address, subnet mask, preferred DNS, alternate DNS, and default gateway.
- PPPoE:Uses PPPoE dial-up method.

6.1.1.1 Adding Network Connection Settings

Step 1: Select the operation type and choose to create a new connection in the connection name field as illustrated in the figure below.



WAN

Transmode: Auto

In automatic mode, the device restarts automatically when the SFP module is switched.

Connection Name: 1_INTERNET_R_VID_100

Mode: Route Enable: ☑

Bearer Service: INTERNET

Note: Pls re-register VoIP service if changed the voice WAN.

Binding Interface: □ LAN1 □ LAN2 □ LAN3 □ LAN4 □ LANPON1

DHCP Server Enable : ☑

LinkMode: IPoE

IP Version: ● IPv4 ○ IPv6 ○ IPv4/IPv6

● DHCP Automatically obtain an IP address from an ISP.

○ Static Configure a static IP for you from an ISP.

VLAN Mode: TAG

VLAN ID[1-4094] : 100

802.1p[0-7] : 0

MulticastVLAN ID[1-4094] :

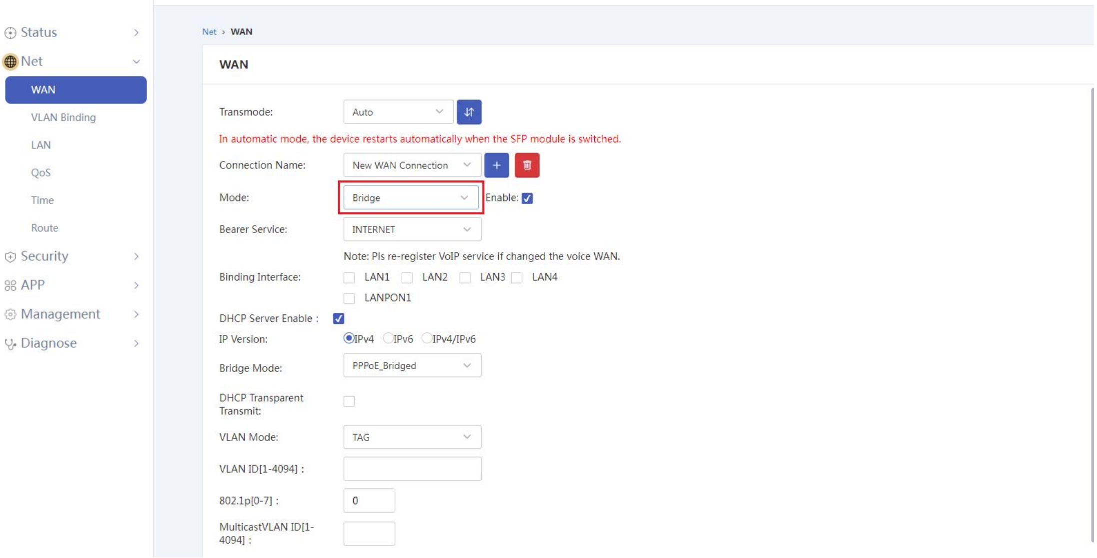
Step 2: Choose the connection mode.

The terminal device supports two connection modes: bridge and route, as illustrated in the figure below.

Example 1: Adding a Bridge Other VLAN 5 WAN

Step:

1.After selecting Bridge in the connection mode, as illustrated in the figure below.



WAN

Transmode: Auto

In automatic mode, the device restarts automatically when the SFP module is switched.

Connection Name: New WAN Connection

Mode: Bridge Enable: ☑

Bearer Service: INTERNET

Note: Pls re-register VoIP service if changed the voice WAN.

Binding Interface: □ LAN1 □ LAN2 □ LAN3 □ LAN4 □ LANPON1

DHCP Server Enable : ☑

IP Version: ● IPv4 ○ IPv6 ○ IPv4/IPv6

Bridge Mode: PPPoE_Bridged

DHCP Transparent Transmit: □

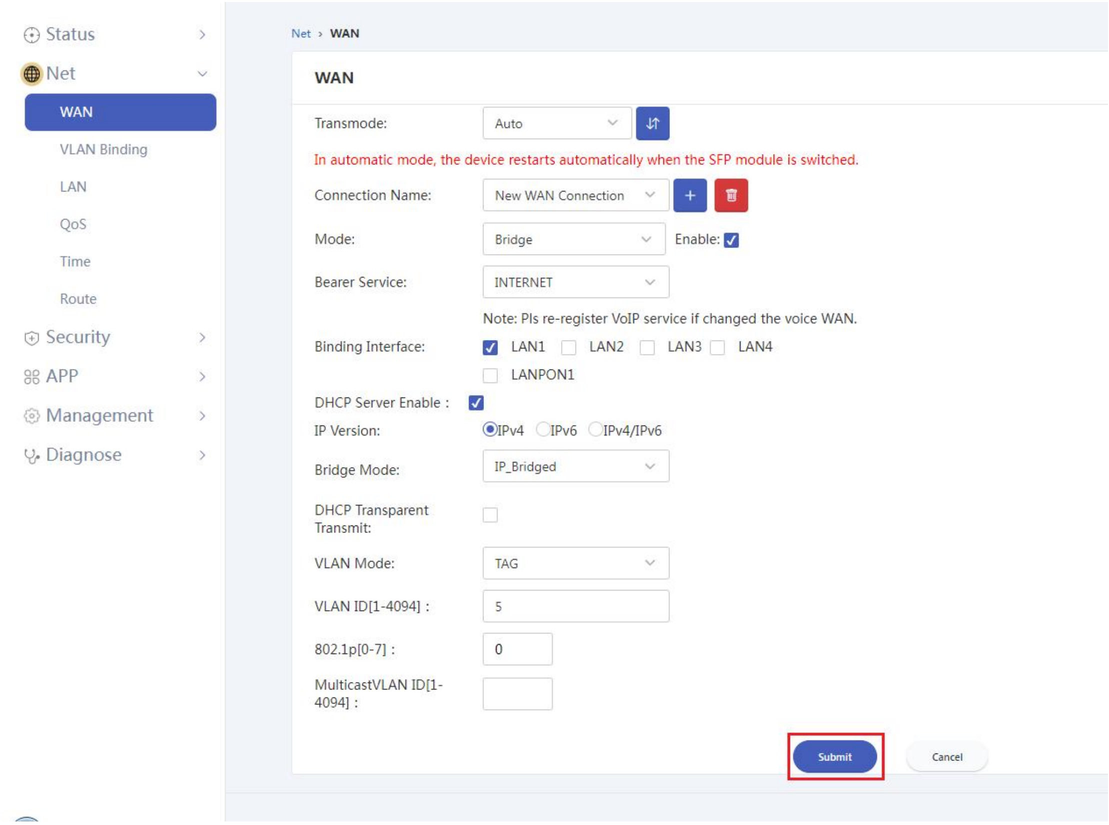
VLAN Mode: TAG

VLAN ID[1-4094] :

802.1p[0-7] : 0

MulticastVLAN ID[1-4094] :

2. Set the relevant parameters and click "Submit" to complete the configuration as illustrated in the figure below.



WAN

Transmode: Auto

In automatic mode, the device restarts automatically when the SFP module is switched.

Connection Name: New WAN Connection

Mode: Bridge Enable: ☑

Bearer Service: INTERNET

Note: Pls re-register VoIP service if changed the voice WAN.

Binding Interface: ☑ LAN1 □ LAN2 □ LAN3 □ LAN4 □ LANPON1

DHCP Server Enable : ☑

IP Version: ● IPv4 ○ IPv6 ○ IPv4/IPv6

Bridge Mode: IP_Bridged

DHCP Transparent Transmit: □

VLAN Mode: TAG

VLAN ID[1-4094] : 5

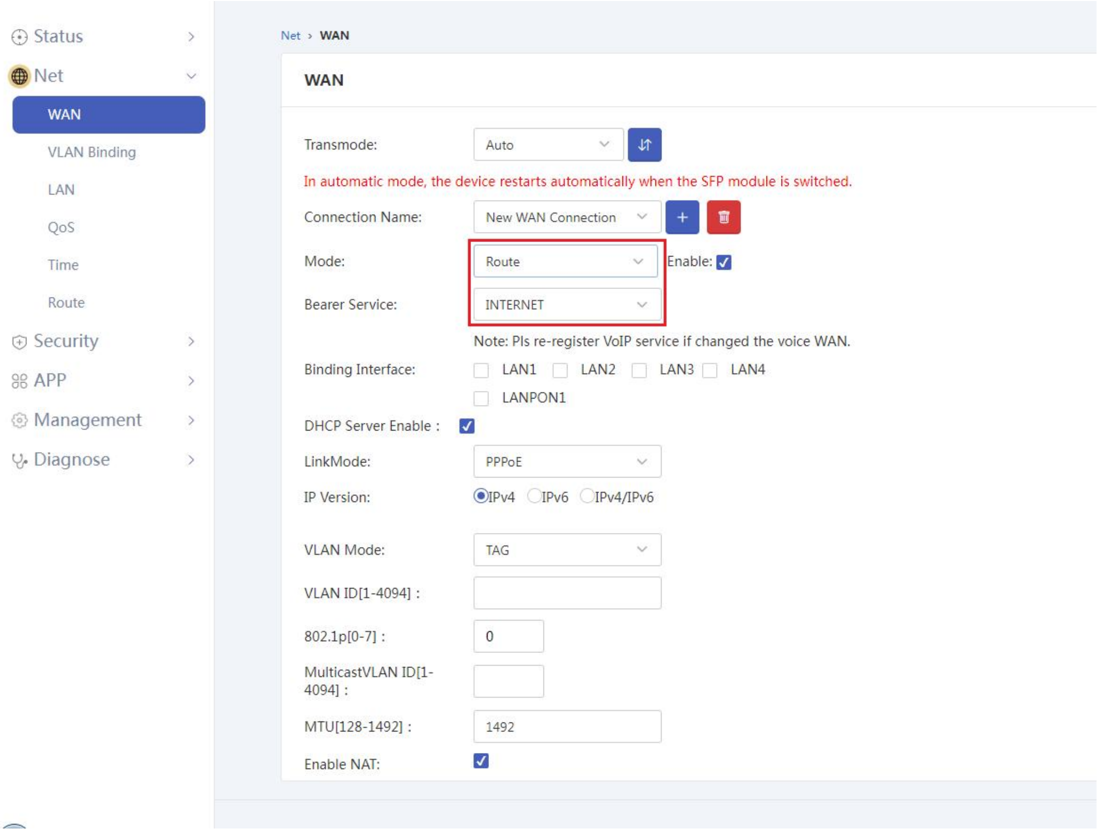
802.1p[0-7] : 0

MulticastVLAN ID[1-4094] :

Example 2: Adding a Route Internet PPPoE VLAN 3 WAN Connection

Step:

1.After selecting Route in the connection mode, as illustrated in the figure below.



Net › WAN

WAN

Transmode: Auto

In automatic mode, the device restarts automatically when the SFP module is switched.

Connection Name: New WAN Connection

Mode: Route Enable: ☑

Bearer Service: INTERNET

Note: Pls re-register VoIP service if changed the voice WAN.

Binding Interface: □ LAN1 □ LAN2 □ LAN3 □ LAN4 □ LANPON1

DHCP Server Enable : ☑

LinkMode: PPPoE

IP Version: ● IPv4 ○ IPv6 ○ IPv4/IPv6

VLAN Mode: TAG

VLAN ID[1-4094] :

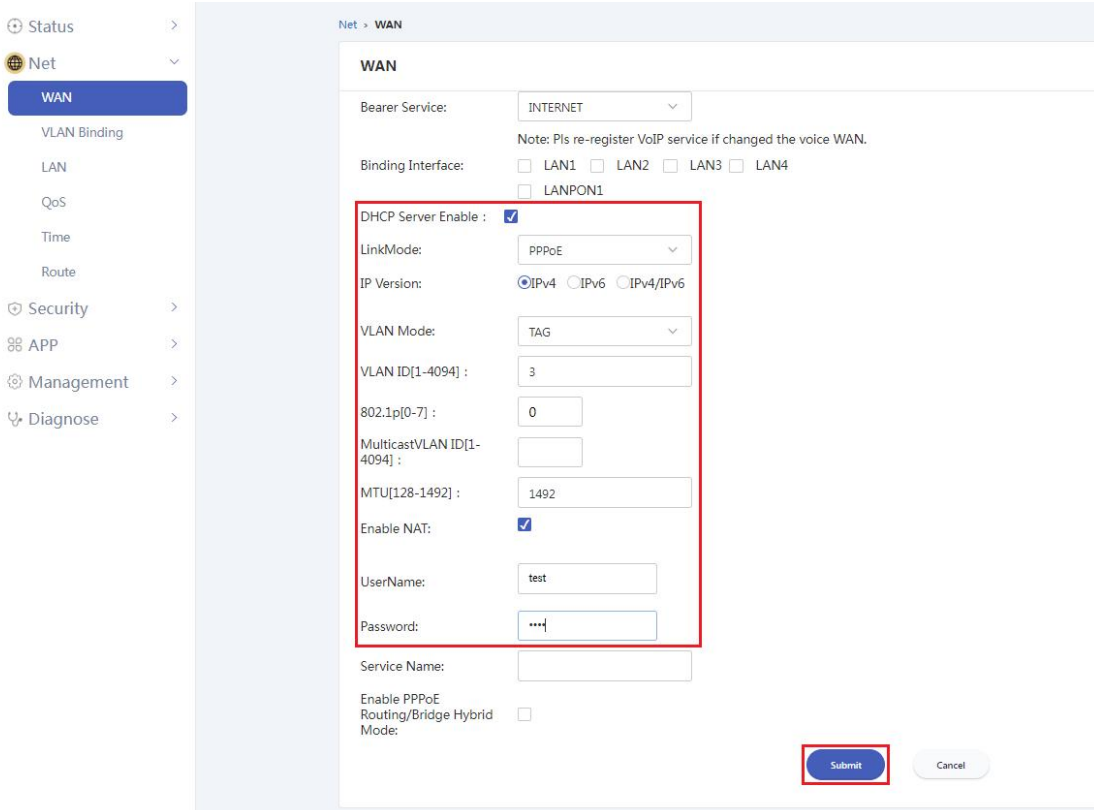
802.1p[0-7] : 0

MulticastVLAN ID[1-4094] :

MTU[128-1492] : 1492

Enable NAT: ☑

2. Configure the relevant parameters as illustrated in the figure below.



WAN

Bearer Service: INTERNET

Note: Pls re-register VoIP service if changed the voice WAN.

Binding Interface: □ LAN1 □ LAN2 □ LAN3 □ LAN4 □ LANPON1

DHCP Server Enable : ☑

LinkMode: PPPoE

IP Version: ● IPv4 ○ IPv6 ○ IPv4/IPv6

VLAN Mode: TAG

VLAN ID[1-4094] : 3

802.1p[0-7] : 0

MulticastVLAN ID[1-4094] :

MTU[128-1492] : 1492

Enable NAT: ☑

UserName: test

Password: ••••

Service Name:

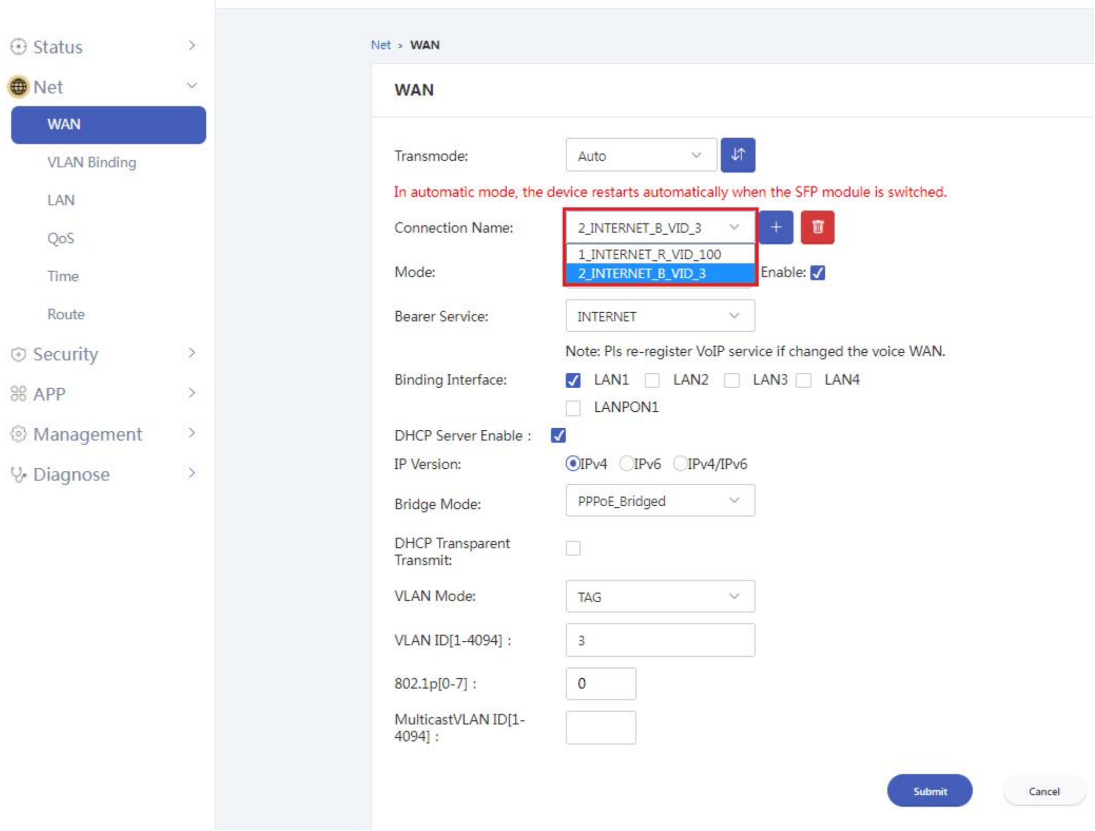
Enable PPPoE Routing/Bridge Hybrid Mode: □

3. Click "Submit" to complete the addition.

6.1.1.2 Modifying Network Connection Settings

The content required for modifying a network connection is the same as when adding one, so only the key steps are described here.

Step 1: In the connection name field, select the connection you want to modify.For example, to modify the connection named "2_INTERNET_R_VID_3", select this connection for modification as illustrated in the figure below.



Transmode: Auto

In automatic mode, the device restarts automatically when the SFP module is switched.

Connection Name: 2_INTERNET_B_VID_3

1_INTERNET_R_VID_100

2_INTERNET_B_VID_3

Mode:

Enable: ☑

Bearer Service: INTERNET

Note: Pls re-register VoIP service if changed the voice WAN.

Binding Interface: ☑ LAN1 □ LAN2 □ LAN3 □ LAN4 □ LANPON1

DHCP Server Enable : ☑

IP Version: ● IPv4 ○ IPv6 ○ IPv4/IPv6

Bridge Mode: PPPoE_Bridged

DHCP Transparent Transmit: □

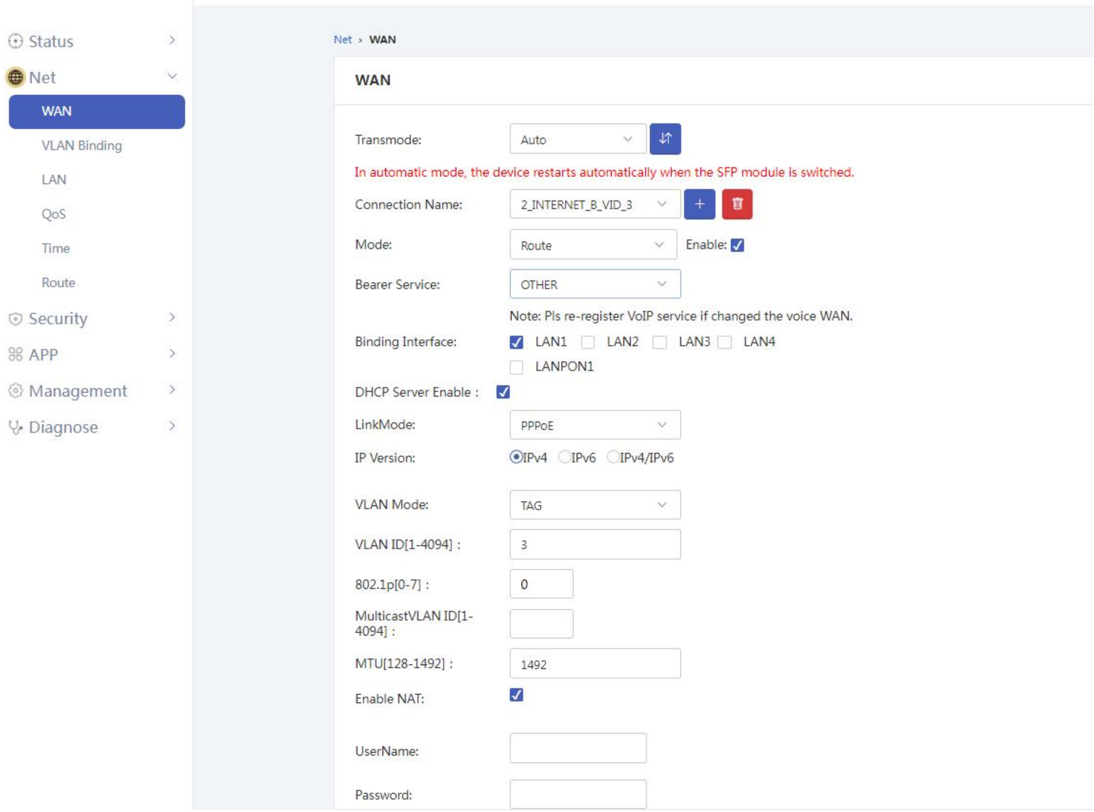
VLAN Mode: TAG

VLAN ID[1-4094] : 3

802.1p[0-7] : 0

MulticastVLAN ID[1-4094] :

Step 2: Modify the corresponding parameters; all parameter names are consistent with those used when adding a connection.



Net › WAN

WAN

Transmode: Auto

In automatic mode, the device restarts automatically when the SFP module is switched.

Connection Name: 2_INTERNET_B_VID_3

Mode: Route Enable: ☑

Bearer Service: OTHER

Note: Pls re-register VoIP service if changed the voice WAN.

Binding Interface: ☑ LAN1 □ LAN2 □ LAN3 □ LAN4 □ LANPON1

DHCP Server Enable : ☑

LinkMode: PPPoE

IP Version: ● IPv4 ○ IPv6 ○ IPv4/IPv6

VLAN Mode: TAG

VLAN ID[1-4094] : 3

802.1p[0-7] : 0

MulticastVLAN ID[1-4094] :

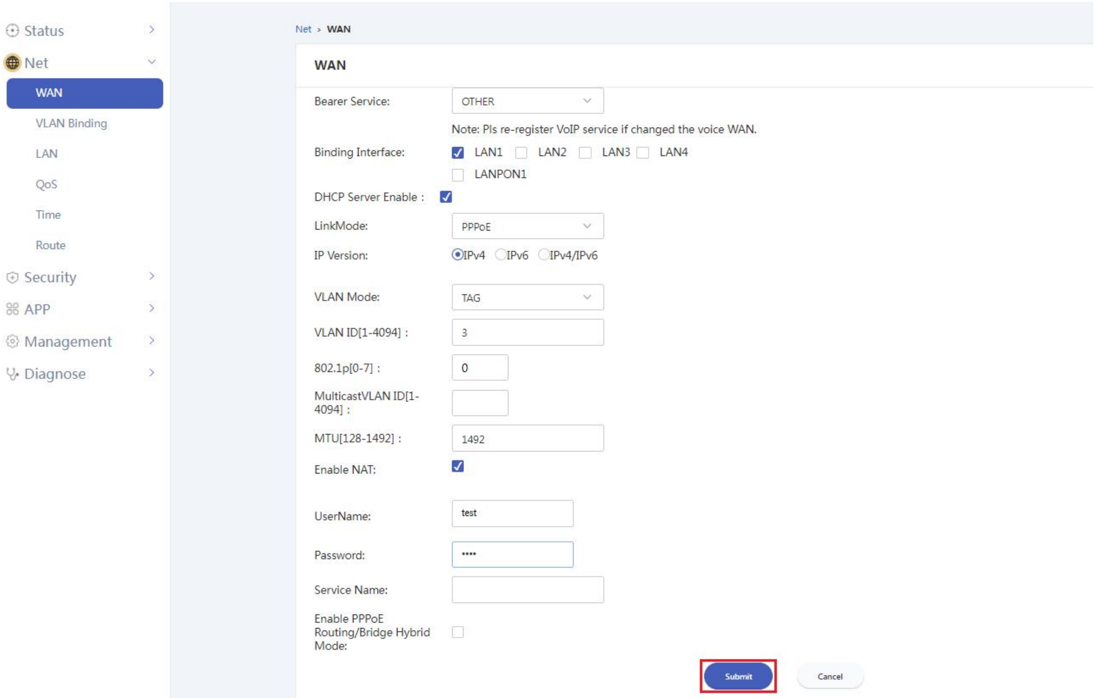
MTU[128-1492] : 1492

Enable NAT: ☑

UserName:

Password:

Step 3: Click "Submit" to complete the modification as illustrated in the figure below.



Bearer Service: OTHER

Note: Pls re-register VoIP service if changed the voice WAN.

Binding Interface: ☑ LAN1 □ LAN2 □ LAN3 □ LAN4 □ LANPON1

DHCP Server Enable : ☑

LinkMode: PPPoE

IP Version: ● IPv4 ○ IPv6 ○ IPv4/IPv6

VLAN Mode: TAG

VLAN ID[1-4094] : 3

802.1p[0-7] : 0

MulticastVLAN ID[1-4094] :

MTU[128-1492] : 1492

Enable NAT: ☑

UserName: test

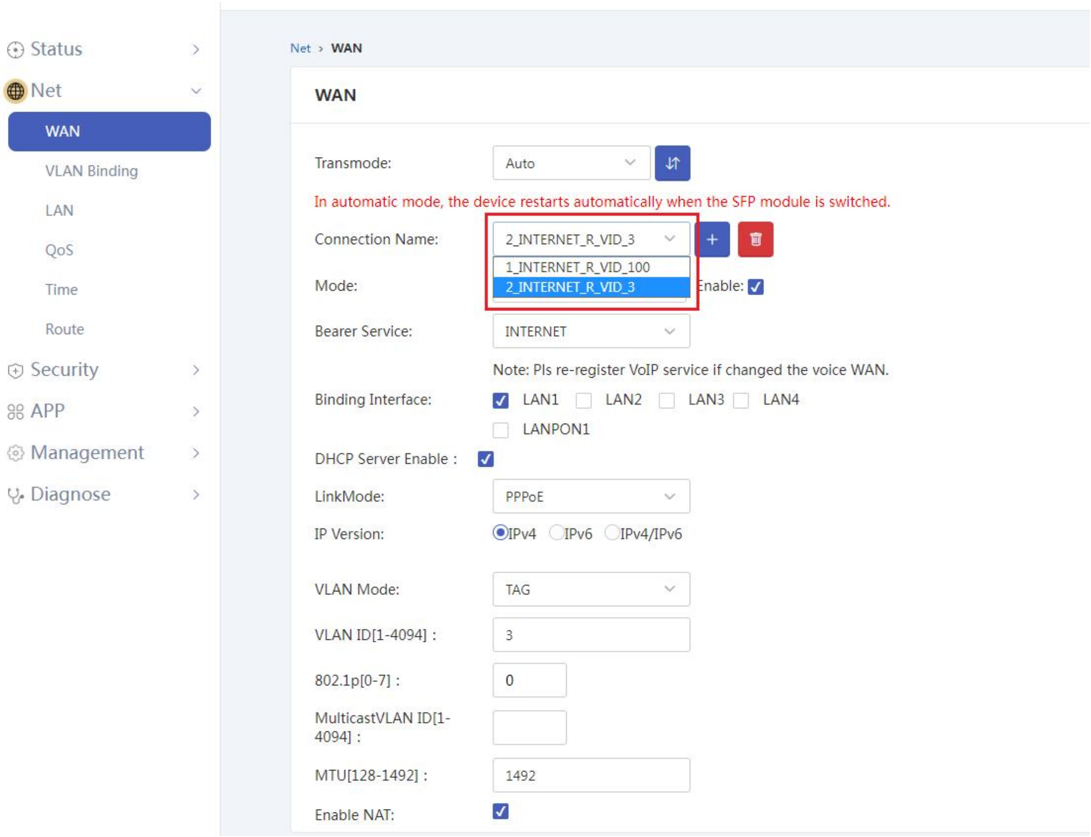
Password: ••••

Service Name:

Enable PPPoE Routing/Bridge Hybrid Mode: □

6.1.1.3 Deleting Network Connection Settings

Step 1: Select the connection you wish to delete, such as the network connection "2_INTERNET_R_VID_3" as illustrated in the figure below.



WAN

Transmode: Auto

In automatic mode, the device restarts automatically when the SFP module is switched.

Connection Name: 2_INTERNET_R_VID_3

1_INTERNET_R_VID_100
2_INTERNET_R_VID_3

Mode: Enable: ☑

Bearer Service: INTERNET

Note: Pls re-register VoIP service if changed the voice WAN.

Binding Interface: ☑ LAN1 □ LAN2 □ LAN3 □ LAN4 □ LANPON1

DHCP Server Enable : ☑

LinkMode: PPPoE

IP Version: ● IPv4 ○ IPv6 ○ IPv4/IPv6

VLAN Mode: TAG

VLAN ID[1-4094] : 3

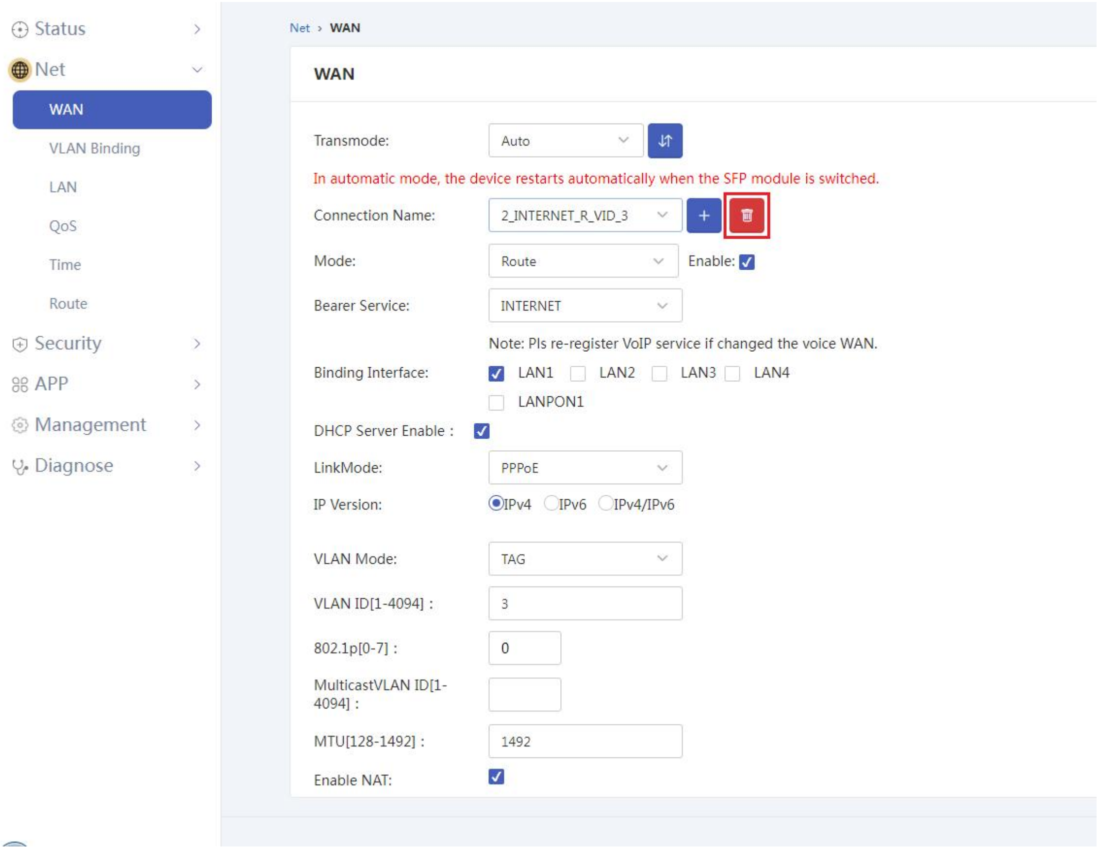
802.1p[0-7] : 0

MulticastVLAN ID[1-4094] :

MTU[128-1492] : 1492

Enable NAT: ☑

Step 2: Click the "Delete" button as illustrated in the figure below.



WAN

Transmode: Auto

In automatic mode, the device restarts automatically when the SFP module is switched.

Connection Name: 2_INTERNET_R_VID_3

Mode: Route Enable: ☑

Bearer Service: INTERNET

Note: Pls re-register VoIP service if changed the voice WAN.

Binding Interface: ☑ LAN1 □ LAN2 □ LAN3 □ LAN4 □ LANPON1

DHCP Server Enable : ☑

LinkMode: PPPoE

IP Version: ● IPv4 ○ IPv6 ○ IPv4/IPv6

VLAN Mode: TAG

VLAN ID[1-4094] : 3

802.1p[0-7] : 0

MulticastVLAN ID[1-4094] :

MTU[128-1492] : 1492

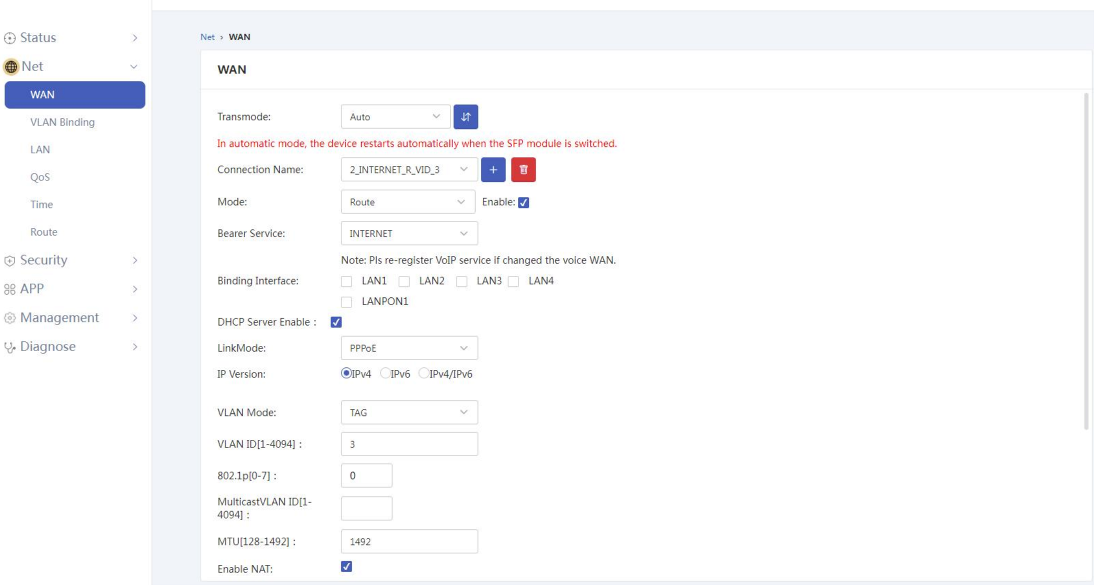
Enable NAT: ☑

6.1.1.4 Port Binding

Port Binding Definition: Bind the device's hardware interfaces (including LAN1-LAN4) to service type groups (including Internet) based on the requirements of end users or operators.

Binding steps:

Step 1: Click on the menu "Net -> WAN" as illustrated in the figure below.



WAN

Transmode: Auto

In automatic mode, the device restarts automatically when the SFP module is switched.

Connection Name: 2_INTERNET_R_VID_3

Mode: Route Enable: ☑

Bearer Service: INTERNET

Note: Pls re-register VoIP service if changed the voice WAN.

Binding Interface: □ LAN1 □ LAN2 □ LAN3 □ LAN4 □ LANPON1

DHCP Server Enable : ☑

LinkMode: PPPoE

IP Version: ● IPv4 ○ IPv6 ○ IPv4/IPv6

VLAN Mode: TAG

VLAN ID[1-4094] : 3

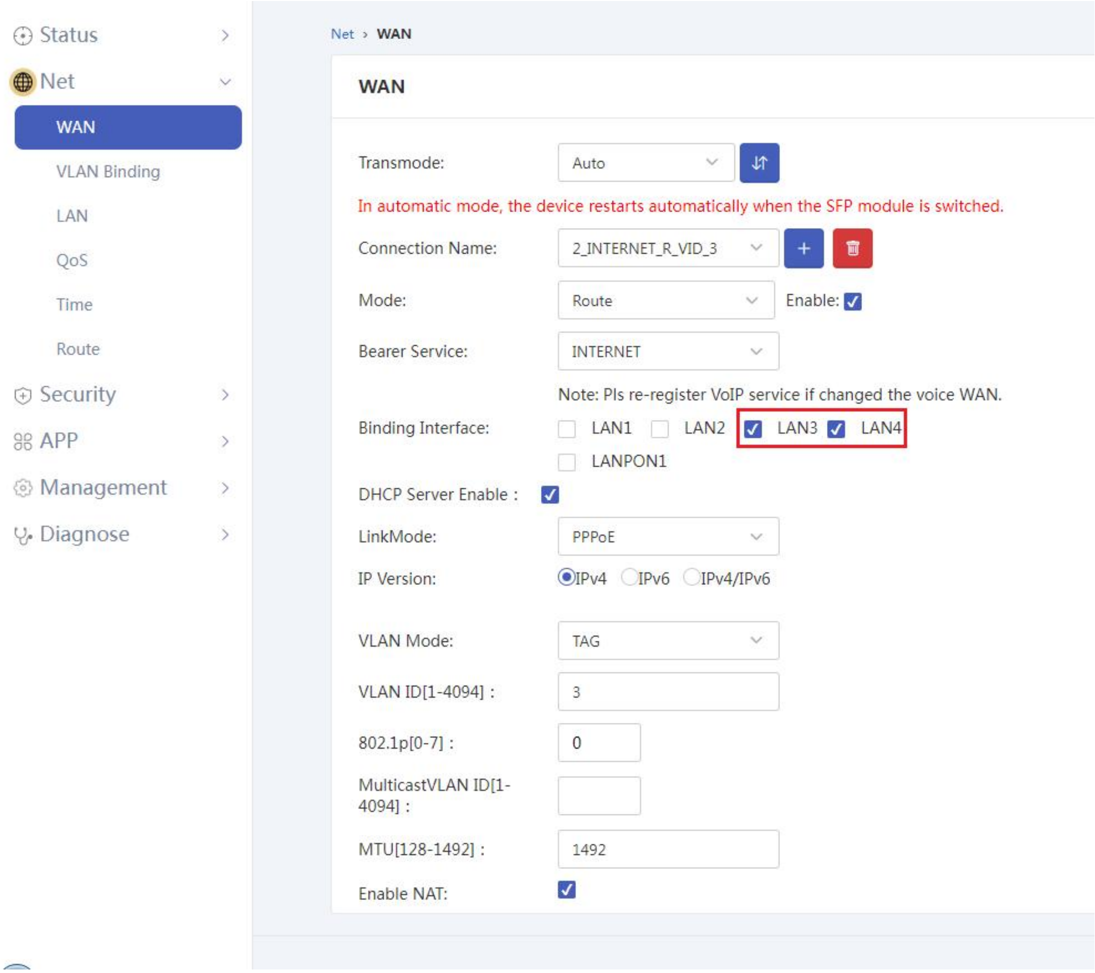
802.1p[0-7] : 0

MulticastVLAN ID[1-4094] :

MTU[128-1492] : 1492

Enable NAT: ☑

Step 2: Select the port you need to bind from the port binding items as illustrated in the figure below.



WAN

Transmode: Auto

In automatic mode, the device restarts automatically when the SFP module is switched.

Connection Name: 2_INTERNET_R_VID_3

Mode: Route Enable: ☑

Bearer Service: INTERNET

Note: Pls re-register VoIP service if changed the voice WAN.

Binding Interface: □ LAN1 □ LAN2 ☑ LAN3 ☑ LAN4 □ LANPON1

DHCP Server Enable : ☑

LinkMode: PPPoE

IP Version: ● IPv4 ○ IPv6 ○ IPv4/IPv6

VLAN Mode: TAG

VLAN ID[1-4094] : 3

802.1p[0-7] : 0

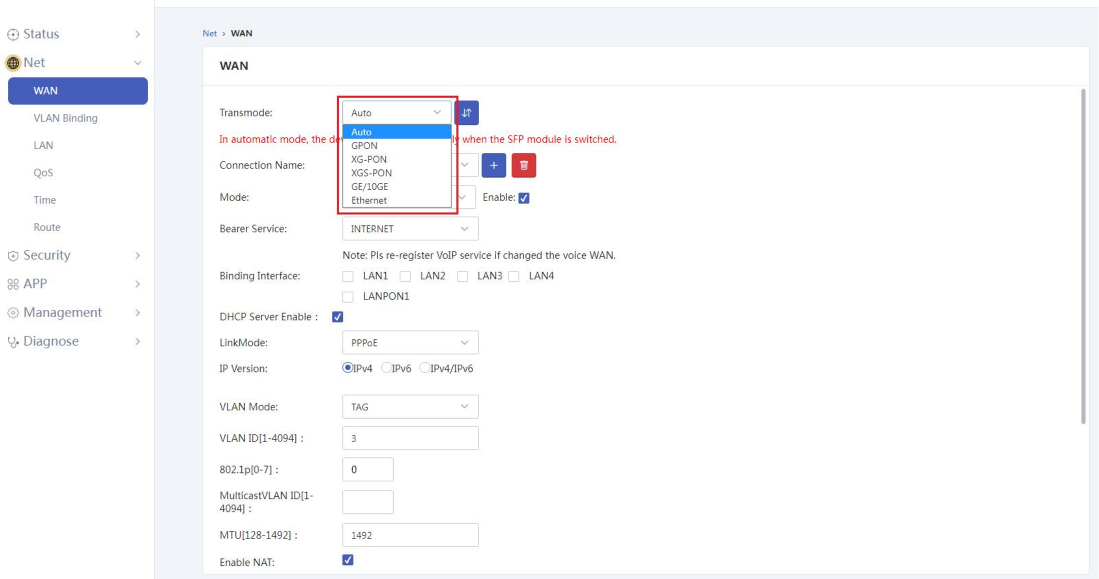
MulticastVLAN ID[1-4094] :

MTU[128-1492] : 1492

Enable NAT: ☑

6.1.1.5 Selecting Transmission Mode

Step 1: Manually select the upstream mode from Auto, GPON, XG-PON, XGS-PON, GE/10GE, Ethernet.



WAN

Transmode: Auto

In automatic mode, the de ly when the SFP module is switched.

Connection Name:

Mode: Enable: ☑

Bearer Service: INTERNET

Note: Pls re-register VoIP service if changed the voice WAN.

Binding Interface: □ LAN1 □ LAN2 □ LAN3 □ LAN4 □ LANPON1

DHCP Server Enable : ☑

LinkMode: PPPoE

IP Version: ● IPv4 ○ IPv6 ○ IPv4/IPv6

VLAN Mode: TAG

VLAN ID[1-4094] : 3

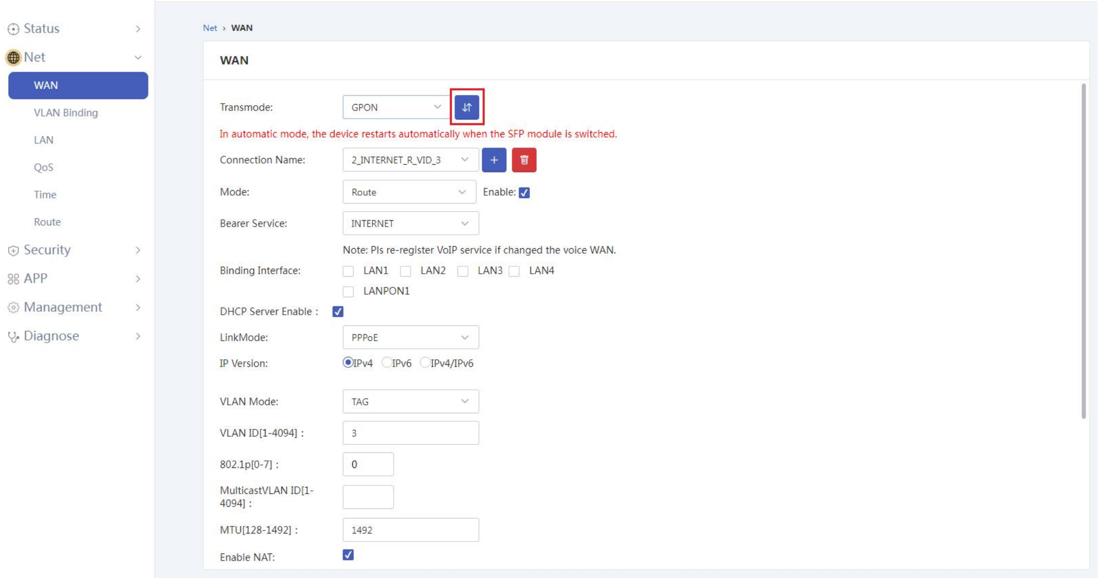
802.1p[0-7] : 0

MulticastVLAN ID[1-4094] :

MTU[128-1492] : 1492

Enable NAT: ☑

Step 2: Click the switch button. After clicking the switch button, as illustrated in the figure below. Click "OK" to reboot the device.



Transmode: GPON

In automatic mode, the device restarts automatically when the SFP module is switched.

Connection Name: 2_INTERNET_R_VID_3

Mode: Route Enable: ☑

Bearer Service: INTERNET

Note: Pls re-register VoIP service if changed the voice WAN.

Binding Interface: □ LAN1 □ LAN2 □ LAN3 □ LAN4 □ LANPON1

DHCP Server Enable : ☑

LinkMode: PPPoE

IP Version: ● IPv4 ○ IPv6 ○ IPv4/IPv6

VLAN Mode: TAG

VLAN ID[1-4094] : 3

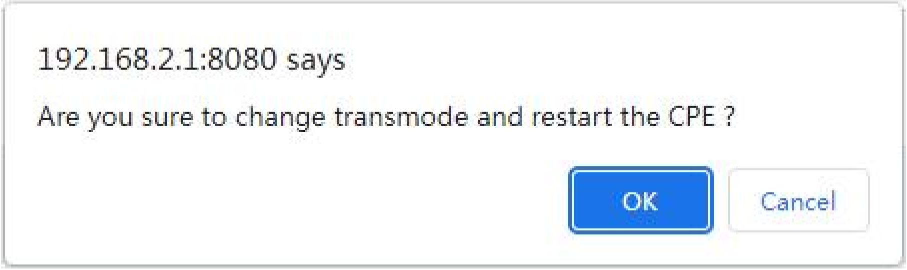
802.1p[0-7] : 0

MulticastVLAN ID[1-4094] :

MTU[128-1492] : 1492

Enable NAT: ☑

After clicking the switch button, as illustrated in the figure below.Click "OK" to reboot the device.



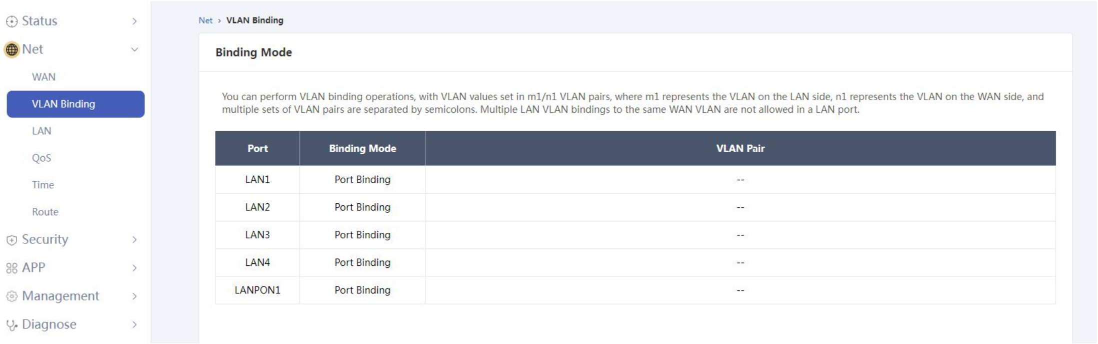
192.168.2.1:8080 says

Are you sure to change transmode and restart the CPE ?

6.1.2 VLAN Binding Setting

When "VLAN binding" is selected, the VLAN pair of the port is bound; you can perform VLAN binding operations, and the value of VLAN is set in the form of m1/n1 VLAN pair, where m1 represents the VLAN on the user side, and n1 represents the VLAN on the outgoing interface. In VLAN configuration, multiple groups of VLAN pairs are separated by semicolons. If you select "Port Binding", you don't need to configure the VLAN pair, and use the VLAN configured in "Broadband Settings".

Click on the menu "Net -> VLAN Binding" to enter the VLAN binding page as illustrated in the figure below.

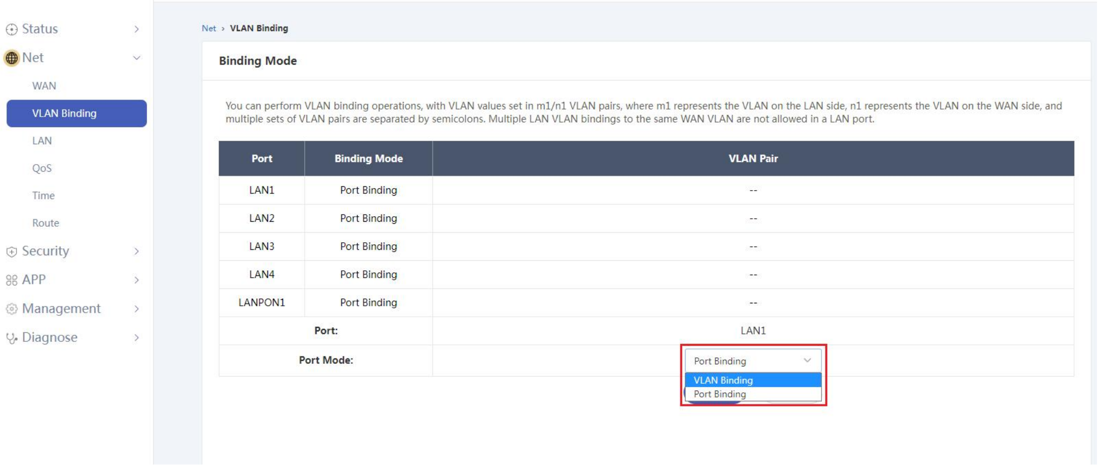


Binding Mode

You can perform VLAN binding operations, with VLAN values set in m1/n1 VLAN pairs, where m1 represents the VLAN on the LAN side, n1 represents the VLAN on the WAN side, and multiple sets of VLAN pairs are separated by semicolons. Multiple LAN VLAN bindings to the same WAN VLAN are not allowed in a LAN port.

Port	Binding Mode	VLAN Pair
LAN1	Port Binding	--
LAN2	Port Binding	--
LAN3	Port Binding	--
LAN4	Port Binding	--
LANPON1	Port Binding	--

Step 1: Click the port that requires VLAN binding configuration, and set the binding relationship between the port and the VLAN, as illustrated in the figure below.



Binding Mode

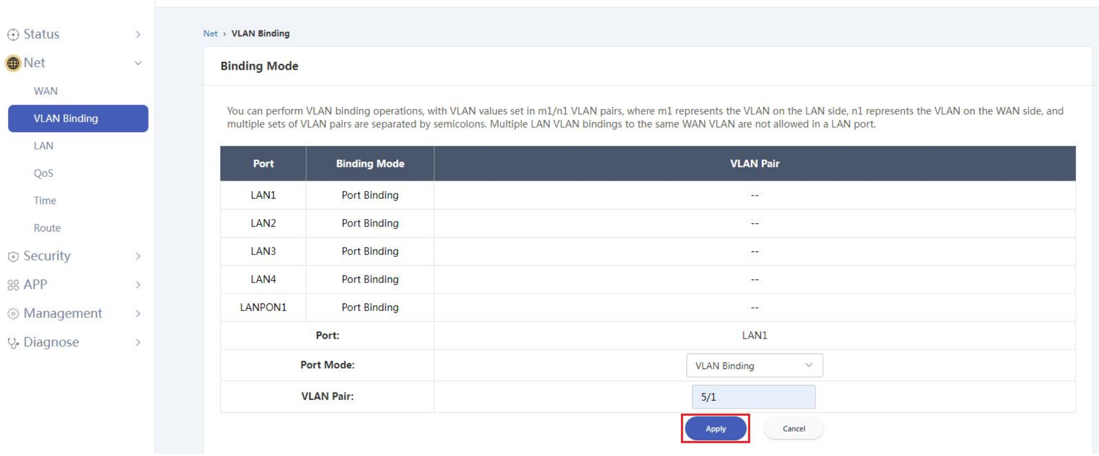
You can perform VLAN binding operations, with VLAN values set in m1/n1 VLAN pairs, where m1 represents the VLAN on the LAN side, n1 represents the VLAN on the WAN side, and multiple sets of VLAN pairs are separated by semicolons. Multiple LAN VLAN bindings to the same WAN VLAN are not allowed in a LAN port.

Port	Binding Mode	VLAN Pair
LAN1	Port Binding	--
LAN2	Port Binding	--
LAN3	Port Binding	--
LAN4	Port Binding	--
LANPON1	Port Binding	--

Port: LAN1

Port Mode: Port Binding

Step 2: Configure the bound VLAN pairs and click "Apply" to complete the configuration as illustrated in the figure below.



Net › VLAN Binding

Binding Mode

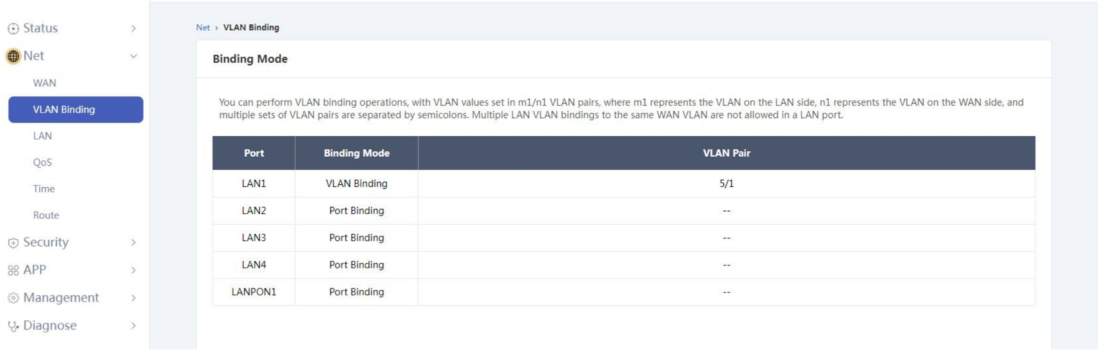
You can perform VLAN binding operations, with VLAN values set in m1/n1 VLAN pairs, where m1 represents the VLAN on the LAN side, n1 represents the VLAN on the WAN side, and multiple sets of VLAN pairs are separated by semicolons. Multiple LAN VLAN bindings to the same WAN VLAN are not allowed in a LAN port.

Port	Binding Mode	VLAN Pair
LAN1	Port Binding	--
LAN2	Port Binding	--
LAN3	Port Binding	--
LAN4	Port Binding	--
LANPON1	Port Binding	--

Port: LAN1

Port Mode: VLAN Binding

VLAN Pair: 5/1



Net › VLAN Binding

Binding Mode

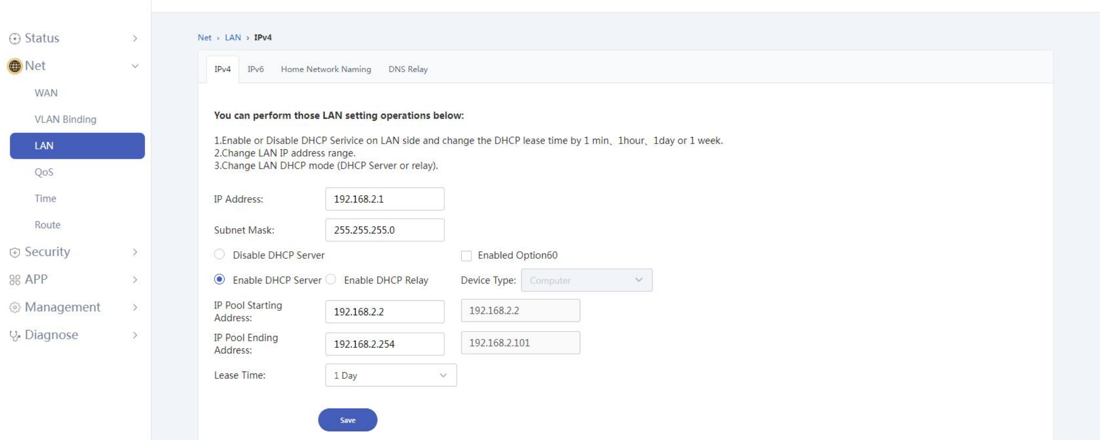
You can perform VLAN binding operations, with VLAN values set in m1/n1 VLAN pairs, where m1 represents the VLAN on the LAN side, n1 represents the VLAN on the WAN side, and multiple sets of VLAN pairs are separated by semicolons. Multiple LAN VLAN bindings to the same WAN VLAN are not allowed in a LAN port.

Port	Binding Mode	VLAN Pair
LAN1	VLAN Binding	5/1
LAN2	Port Binding	--
LAN3	Port Binding	--
LAN4	Port Binding	--
LANPON1	Port Binding	--

Do not bind user-side VLANs to a WAN port if multiple VLANs are associated with the same WAN port.

6.1.3 LAN Setting

6.1.3.1 IPv4 Setting



You can perform those LAN setting operations below:

1.Enable or Disable DHCP Serivice on LAN side and change the DHCP lease time by 1 min、1hour、1day or 1 week.
2.Change LAN IP address range.
3.Change LAN DHCP mode (DHCP Server or relay).

IP Address: 192.168.2.1

Subnet Mask: 255.255.255.0

○ Disable DHCP Server □ Enabled Option60

● Enable DHCP Server ○ Enable DHCP Relay Device Type: Computer

IP Pool Starting Address: 192.168.2.2 192.168.2.2

IP Pool Ending Address: 192.168.2.254 192.168.2.101

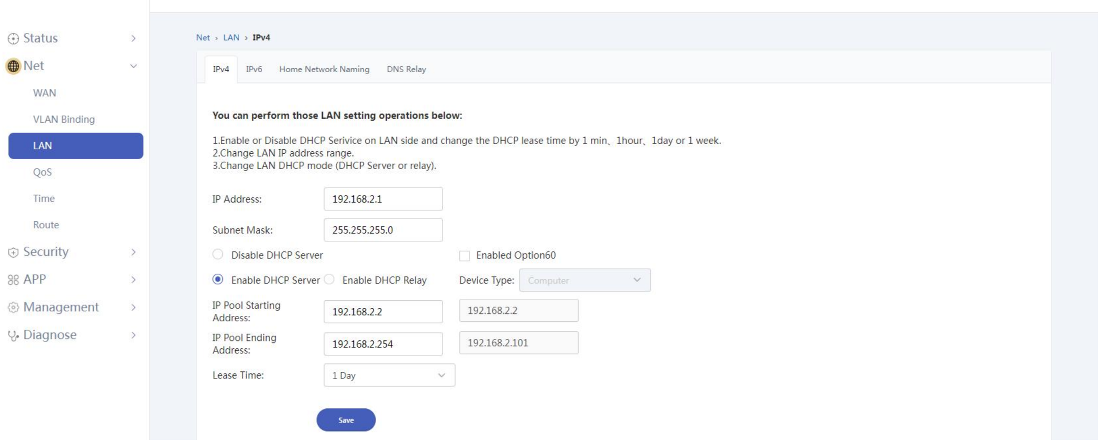
Lease Time: 1 Day

- IP Address: Enter the IP address of the LAN port of the terminal. The default is 192.168.2.1, and LAN users can manage the terminal through this IP address .
- Subnet Mask: Enter the subnet mask of this terminal for the LAN. By default, the class C IP address corresponds to the subnet mask 255.255.255.0.
- Enable DHCP server : Configure the range of IP addresses automatically obtained by various terminals. By default, it is enabled.
- Lease time: The default is 1 day, which can be manually modified to 1 minute, 1 hour, or 1 week.

Note: When users are using it, they can enlarge the initial and initial address pools according to actual needs, so as to increase the number of users who can automatically obtain IP addresses and access the network.

The basic operation steps are as follows:

Step 1: Click on the menu "Net -> LAN" as illustrated in the figure below.



You can perform those LAN setting operations below:

1.Enable or Disable DHCP Serivice on LAN side and change the DHCP lease time by 1 min、1hour、1day or 1 week.
2.Change LAN IP address range.
3.Change LAN DHCP mode (DHCP Server or relay).

IP Address: 192.168.2.1

Subnet Mask: 255.255.255.0

○ Disable DHCP Server □ Enabled Option60

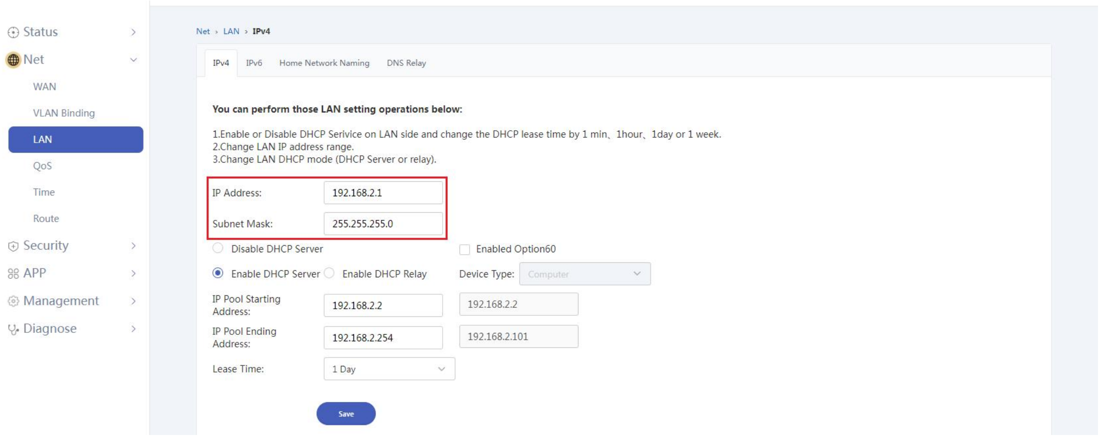
● Enable DHCP Server ○ Enable DHCP Relay Device Type: Computer

IP Pool Starting Address: 192.168.2.2 192.168.2.2

IP Pool Ending Address: 192.168.2.254 192.168.2.101

Lease Time: 1 Day

Step 2: Modify DHCP parameters such as start IP address, end IP address, lease time, and click "Save".



You can perform those LAN setting operations below:

1.Enable or Disable DHCP Serivice on LAN side and change the DHCP lease time by 1 min、1hour、1day or 1 week.
2.Change LAN IP address range.
3.Change LAN DHCP mode (DHCP Server or relay).

IP Address: 192.168.2.1

Subnet Mask: 255.255.255.0

○ Disable DHCP Server □ Enabled Option60

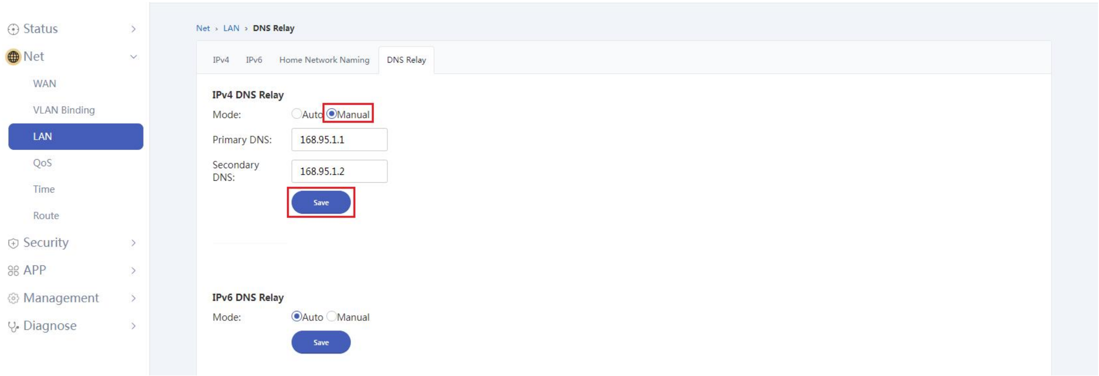
● Enable DHCP Server ○ Enable DHCP Relay Device Type: Computer

IP Pool Starting Address: 192.168.2.2 192.168.2.2

IP Pool Ending Address: 192.168.2.254 192.168.2.101

Lease Time: 1 Day

Step 3: Enable the manual DNS server function, configure the specified DNS server address, and click "Save".



IPv4 DNS Relay

Mode: ○Auto ●Manual

Primary DNS: 168.95.1.1

Secondary DNS: 168.95.1.2

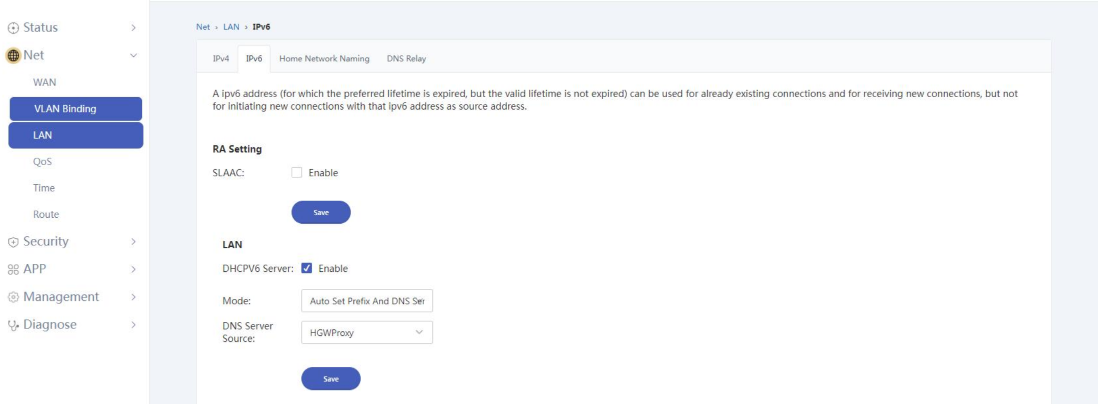
IPv6 DNS Relay

Mode: ●Auto ○Manual

6.1.3.2 IPv6 Setting

6.1.3.2.1 RA Setting (SLAAC)

Click on the menu "Net -> LAN -> IPv6" as illustrated in the figure below.



A ipv6 address (for which the preferred lifetime is expired, but the valid lifetime is not expired) can be used for already existing connections and for receiving new connections, but not for initiating new connections with that ipv6 address as source address.

RA Setting

SLAAC: □ Enable

LAN

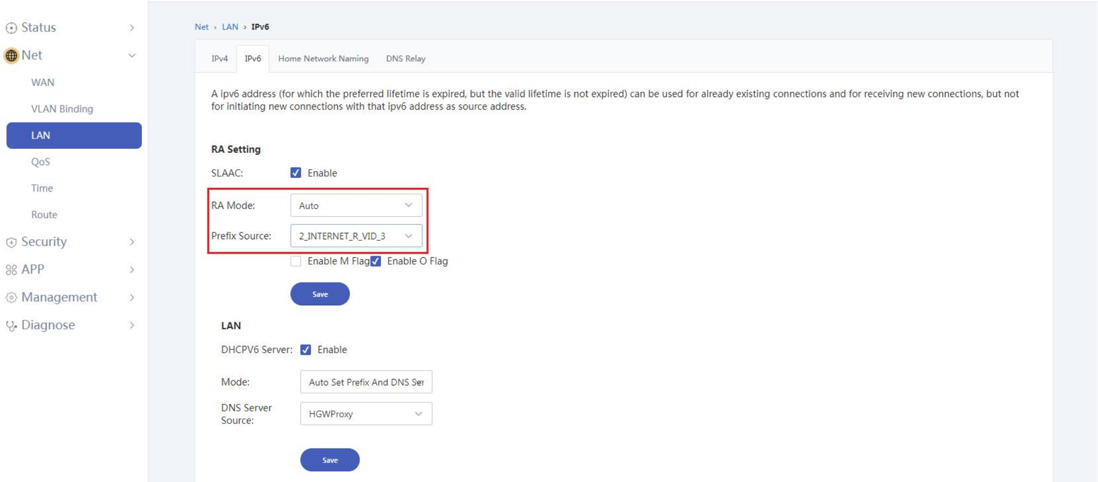
DHCPV6 Server: ☑ Enable

Mode: Auto Set Prefix And DNS Ser

DNS Server Source: HGWProxy

6.1.3.2.1.1 Auto mode

On the IPv6 Configuration page, under RA Setting, set the RA Mode to "Auto", select the corresponding WAN for Prefix Source, and click "Save" to complete the configuration, as illustrated in the figure below.



A ipv6 address (for which the preferred lifetime is expired, but the valid lifetime is not expired) can be used for already existing connections and for receiving new connections, but not for initiating new connections with that ipv6 address as source address.

RA Setting

SLAAC: ☑ Enable

RA Mode: Auto

Prefix Source: 2_INTERNET_R_VID_3

□ Enable M Flag ☑ Enable O Flag

LAN

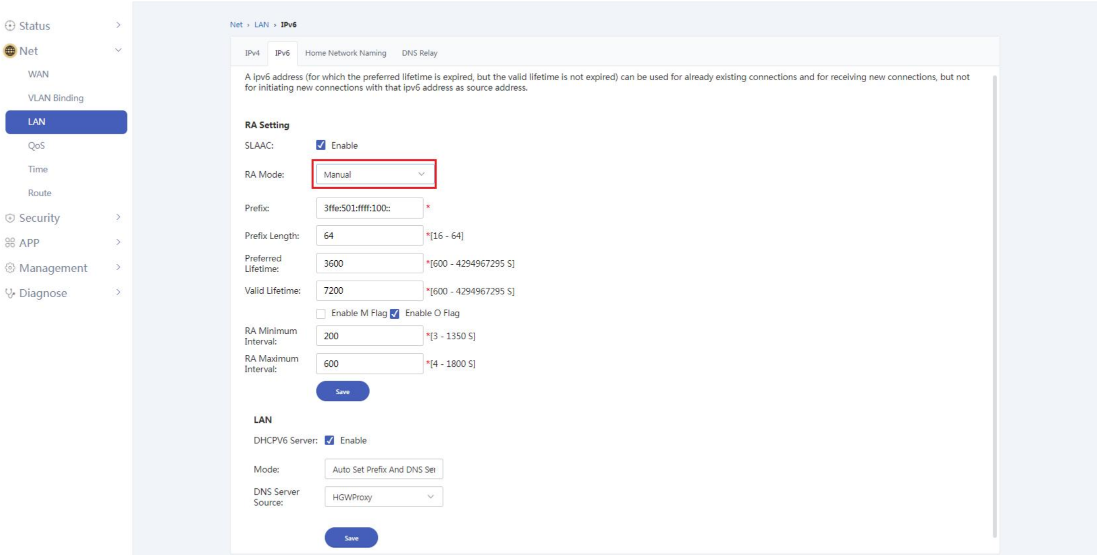
DHCPV6 Server: ☑ Enable

Mode: Auto Set Prefix And DNS Ser

DNS Server Source: HGWProxy

6.1.3.2.1.2 Manual Mode

On the IPv6 configuration page, under RA Setting, select the configuration mode as "Manual"; fill in the corresponding parameters and click "Save" to complete the configuration as illustrated in the figure below.



A ipv6 address (for which the preferred lifetime is expired, but the valid lifetime is not expired) can be used for already existing connections and for receiving new connections, but not for initiating new connections with that ipv6 address as source address.

RA Setting

SLAAC: ☑ Enable

RA Mode: Manual

Prefix: 3ffe:501:ffff:100:: *

Prefix Length: 64 *[16 - 64]

Preferred Lifetime: 3600 *[600 - 4294967295 S]

Valid Lifetime: 7200 *[600 - 4294967295 S]

□ Enable M Flag ☑ Enable O Flag

RA Minimum Interval: 200 *[3 - 1350 S]

RA Maximum Interval: 600 *[4 - 1800 S]

LAN

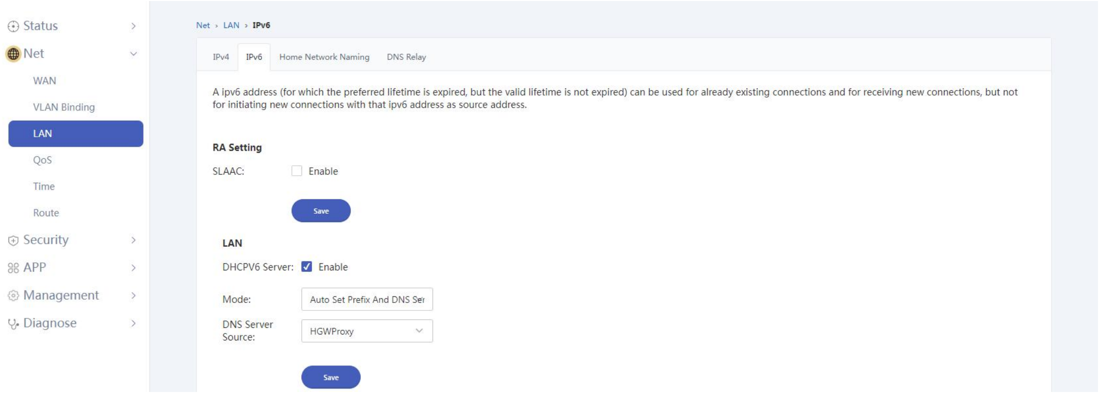
DHCPV6 Server: ☑ Enable

Mode: Auto Set Prefix And DNS Ser

DNS Server Source: HGWProxy

6.1.3.2.2 DHCPv6 Setting

Click on the menu "Net -> LAN -> IPv6" as illustrated in the figure below.



A ipv6 address (for which the preferred lifetime is expired, but the valid lifetime is not expired) can be used for already existing connections and for receiving new connections, but not for initiating new connections with that ipv6 address as source address.

RA Setting

SLAAC: □ Enable

LAN

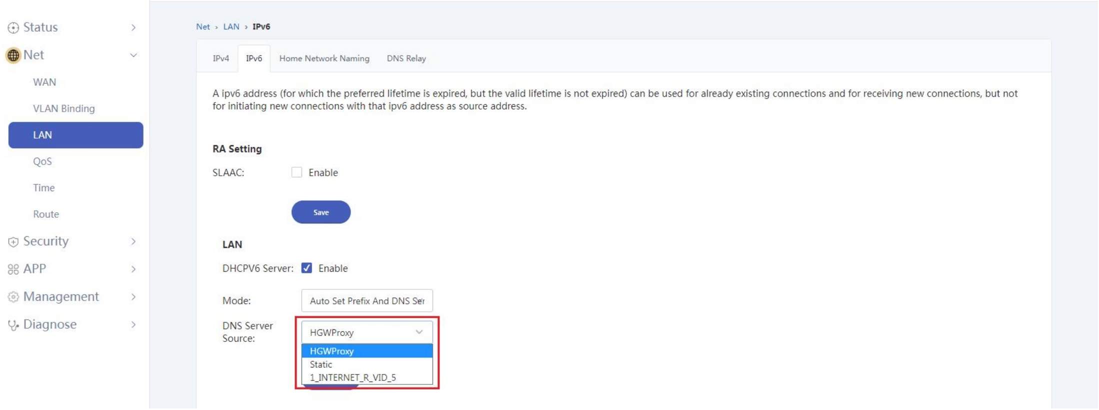
DHCPV6 Server: ☑ Enable

Mode: Auto Set Prefix And DNS Ser

DNS Server Source: HGWProxy

6.1.3.2.2.1 Auto Set Prefix and DNS Server

On the IPv6 setting page, under DHCP configuration, select the configuration mode as "Auto Set Prefix And DNS Server". Choose the "DNS Server Source" from HGWProxy, Static, or WAN, select the corresponding mode, and click "Save" to complete the configuration as illustrated in the figure below.



A ipv6 address (for which the preferred lifetime is expired, but the valid lifetime is not expired) can be used for already existing connections and for receiving new connections, but not for initiating new connections with that ipv6 address as source address.

RA Setting

SLAAC: □ Enable

LAN

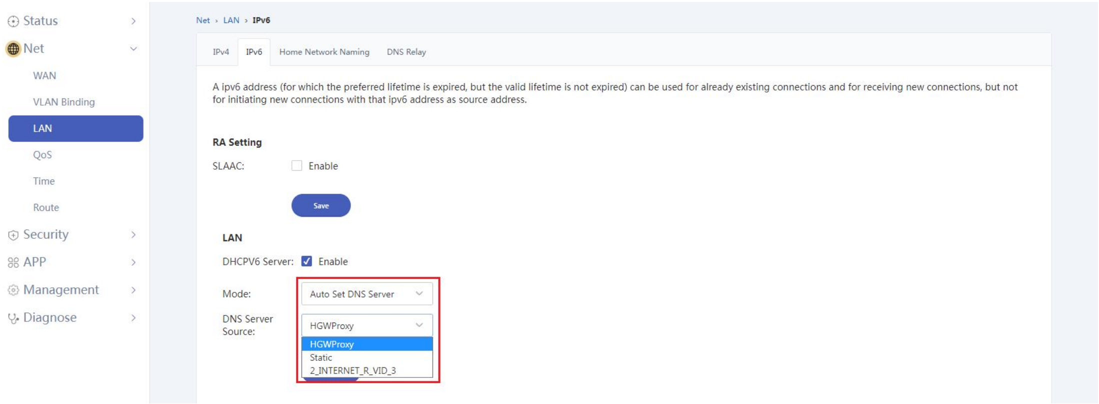
DHCPV6 Server: ☑ Enable

Mode: Auto Set Prefix And DNS Ser

DNS Server Source: HGWProxy

6.1.3.2.2.2 Auto Set DNS Server

On the IPv6 setting page, under DHCP configuration, select the configuration mode as "Auto Set DNS Server". Choose the "DNS Server Source" from HGWProxy, Static, or WAN, select the corresponding mode, and click "Save" to complete the configuration as illustrated in the figure below.



A ipv6 address (for which the preferred lifetime is expired, but the valid lifetime is not expired) can be used for already existing connections and for receiving new connections, but not for initiating new connections with that ipv6 address as source address.

RA Setting

SLAAC: □ Enable

LAN

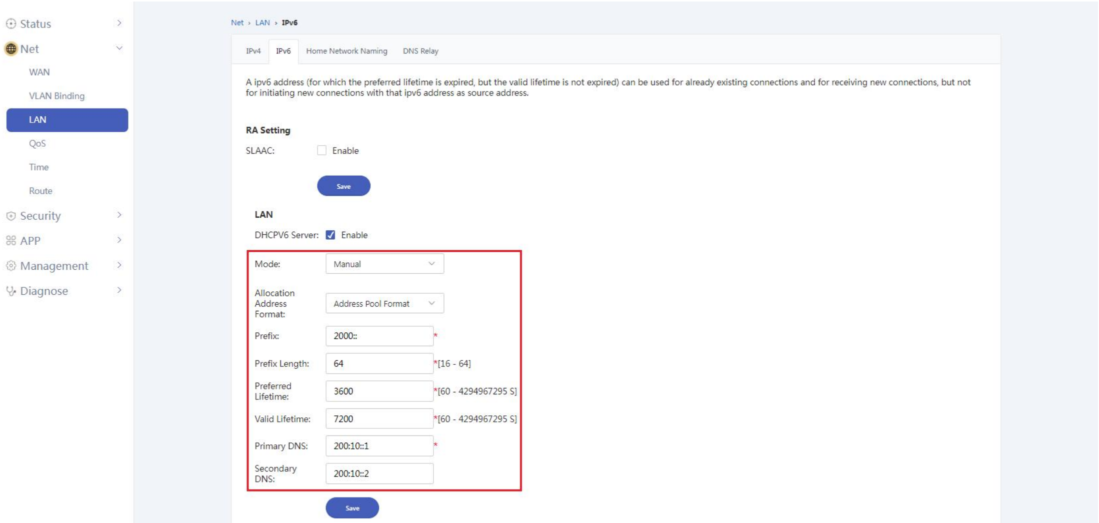
DHCPV6 Server: ☑ Enable

Mode: Auto Set DNS Server

DNS Server Source: HGWProxy

6.1.3.2.2.3 Manual Mode

On the IPv6 setting page, under DHCP configuration, select the "Mode" as "Manual", fill in the corresponding parameters, and click "Save" to complete the configuration as illustrated in the figure below.



A ipv6 address (for which the preferred lifetime is expired, but the valid lifetime is not expired) can be used for already existing connections and for receiving new connections, but not for initiating new connections with that ipv6 address as source address.

RA Setting

SLAAC: □ Enable

LAN

DHCPV6 Server: ☑ Enable

Mode: Manual

Allocation Address Format: Address Pool Format

Prefix: 2000:: *

Prefix Length: 64 *[16 - 64]

Preferred Lifetime: 3600 *[60 - 4294967295 S]

Valid Lifetime: 7200 *[60 - 4294967295 S]

Primary DNS: 200:10::1 *

Secondary DNS: 200:10::2

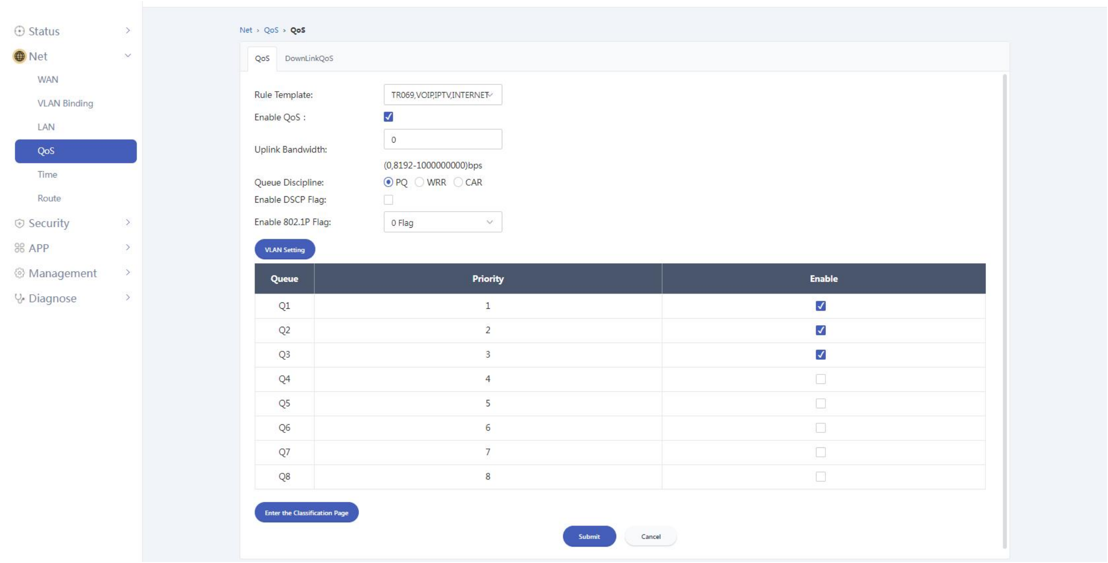
6.1.4 QoS Setting

As the data hub of home network and external network, it can classify uplink data flows according to user-side ports (including wired and wireless interfaces) and service discovery results, and perform QoS adaptation for different data flows.

QoS configuration mainly consists of four parts: QoS enabling, QoS queue configuration, QoS rule configuration, and traffic control.

6.1.4.1 QoS Enabing

To enable QoS, click on the menu "Net -> QoS", check the box to enable QoS, and then click the "Submit" button as illustrated in the figure below.



Rule Template: TR069,VOIP,IPTV,INTERNET

Enable QoS : ☑

Uplink Bandwidth: 0 (0,8192-1000000000)bps

Queue Discipline: ● PQ ○ WRR ○ CAR

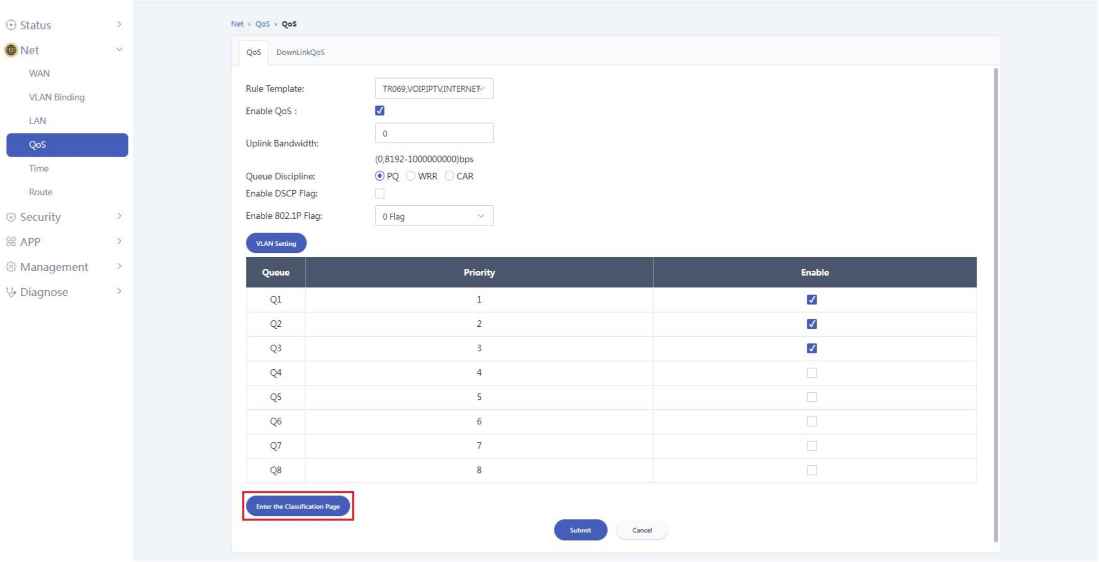
Enable DSCP Flag: □

Enable 802.1P Flag: 0 Flag

Queue	Priority	Enable
Q1	1	☑
Q2	2	☑
Q3	3	☑
Q4	4	□
Q5	5	□
Q6	6	□
Q7	7	□
Q8	8	□

6.1.4.2 Qos Queue Configuration

Step 1: Click on the menu "Net -> QoS" and then click the "Enter the Classification Page" button to enter the queue configuration page as illustrated in the figure below.



Rule Template: TR069,VOIP,IPTV,INTERNET

Enable QoS : ☑

Uplink Bandwidth: 0

(0,8192-1000000000)bps

Queue Discipline: ● PQ ○ WRR ○ CAR

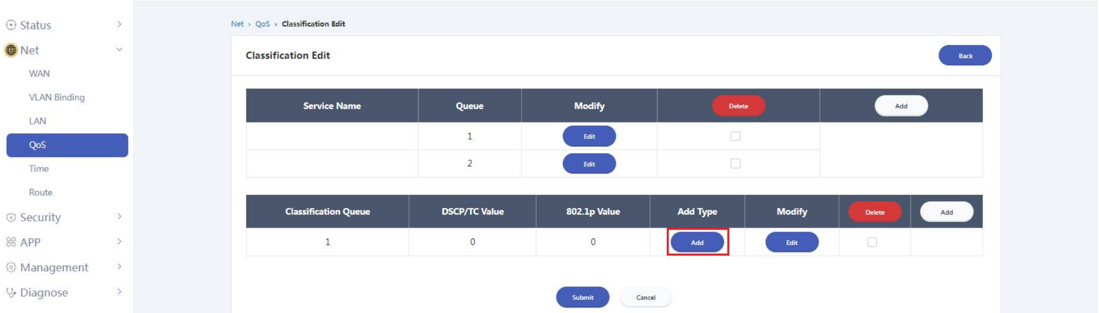
Enable DSCP Flag: □

Enable 802.1P Flag: 0 Flag

Queue	Priority	Enable
Q1	1	☑
Q2	2	☑
Q3	3	☑
Q4	4	□
Q5	5	□
Q6	6	□
Q7	7	□
Q8	8	□

6.1.4.3 QoS Classification Configuration

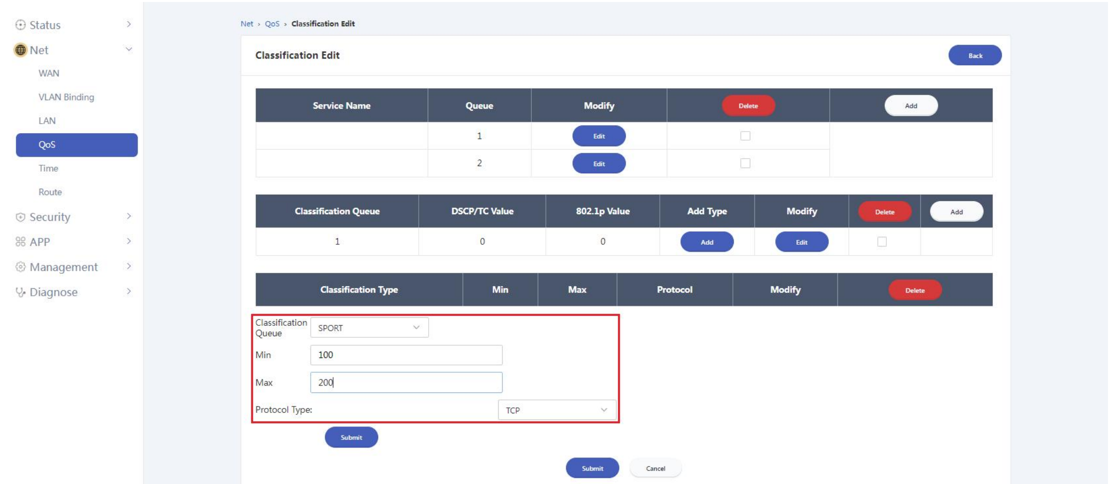
Step 1: Enter the QoS queue parameter configuration as illustrated in the figure below.



Service Name	Queue	Modify	Delete	Add
	1	Edit	□	
	2	Edit	□	

Classification Queue	DSCP/TC Value	802.1p Value	Add Type	Modify	Delete	Add
1	0	0	Add	Edit	□	

Step 2: Configure the corresponding type and parameter values, and click the "Submit" button as illustrated in the figure below.



Classification Edit

Service Name	Queue	Modify	Delete	Add
	1	Edit	□	
	2	Edit	□	

Classification Queue	DSCP/TC Value	802.1p Value	Add Type	Modify	Delete	Add
1	0	0	Add	Edit	□	

Classification Type	Min	Max	Protocol	Modify	Delete

Classification Queue: SPORT

Min: 100

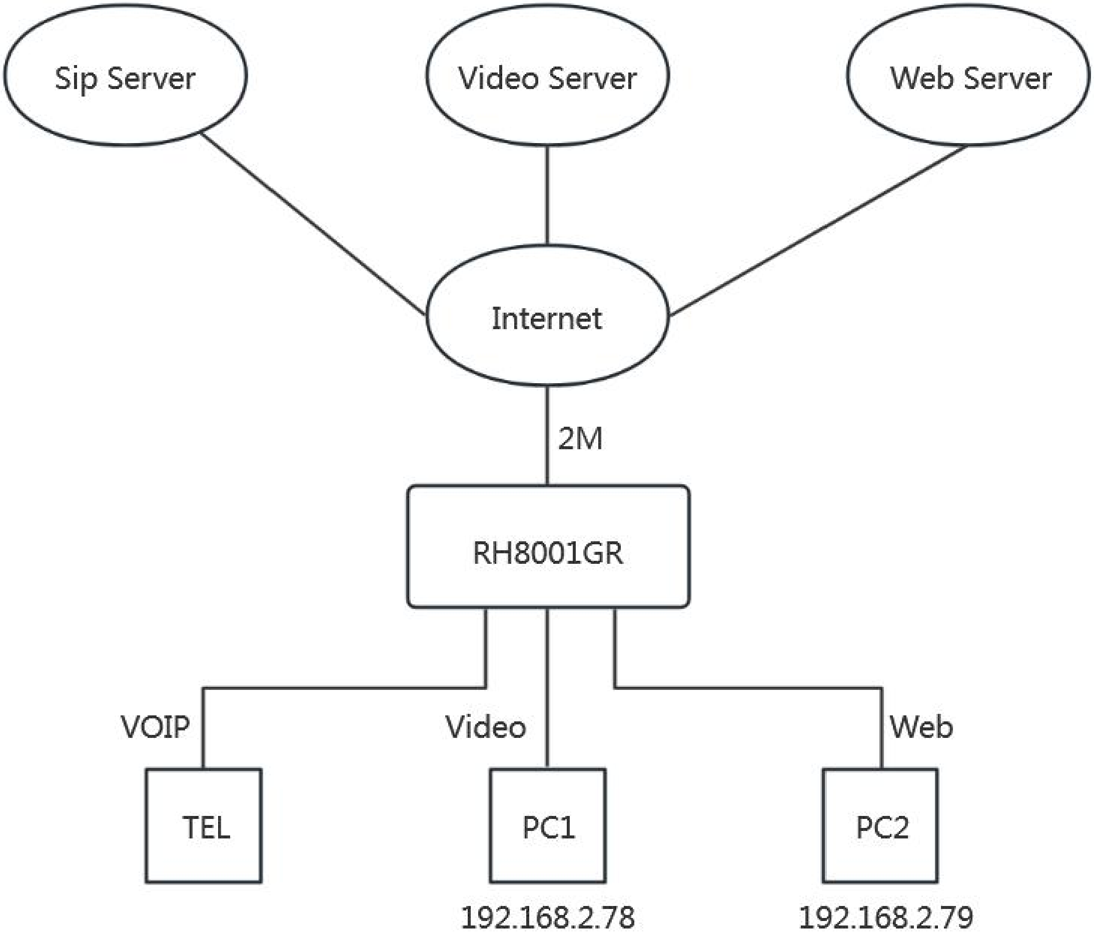
Max: 200

Protocol Type: TCP

Note: New configurations must be consistent with existing configuration item types.

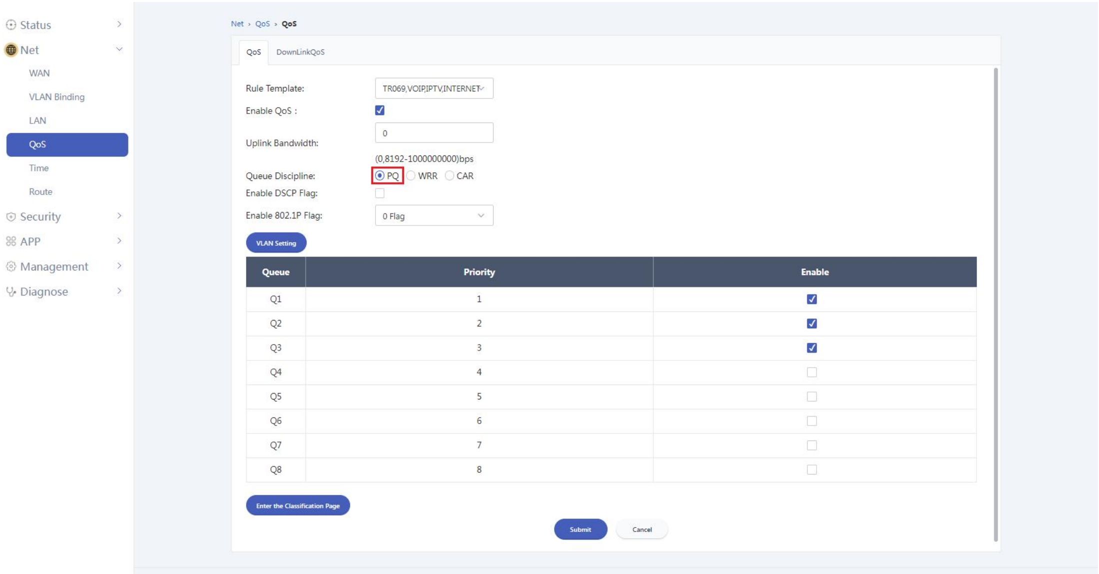
6.1.4.4 Qos Configuration Example

FTTR acts as a data hub between corporate networks and external networks, capable of classifying data streams based on user-side ports (including wired and wireless interfaces) and service discovery results, adapting QoS for different data streams.



Refer to the connection environment in the above figure. This FTTR has a bandwidth of 2Mbps. At this time, PC2 is browsing web pages and downloading files, while a phone call is in progress. PC1's online video viewing could affect VOIP communication quality. In this scenario, QoS will take effect to ensure voice communication quality. Follow these steps:

Step 1: Click on "Net -> QoS" to enter the QoS configuration page, select the PQ scheduling mode, and click apply to save as illustrated in the figure below.



Rule Template: TR069,VOIP,IPTV,INTERNET

Enable QoS : ☑

Uplink Bandwidth: 0
(0,8192-1000000000)bps

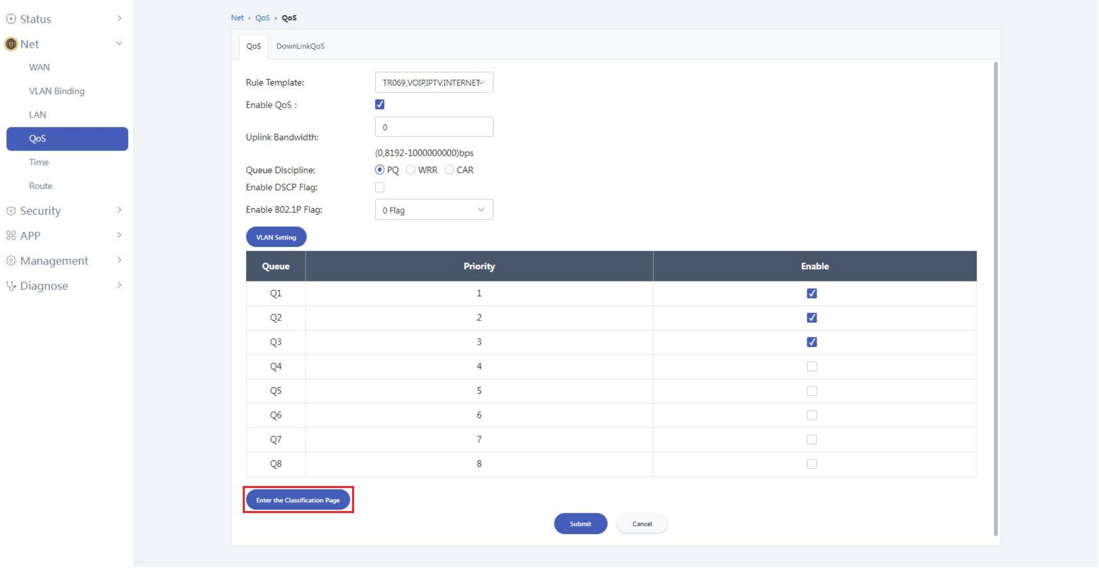
Queue Discipline: ● PQ ○ WRR ○ CAR

Enable DSCP Flag: □

Enable 802.1P Flag: 0 Flag

Queue	Priority	Enable
Q1	1	☑
Q2	2	☑
Q3	3	☑
Q4	4	□
Q5	5	□
Q6	6	□
Q7	7	□
Q8	8	□

Step 2: Click into the classification edit page to enter the QoS queue parameter configuration as illustrated in the figure below.



Rule Template: TR069,VOIP,IPTV,INTERNET

Enable QoS : ☑

Uplink Bandwidth: 0
(0,8192-1000000000)bps

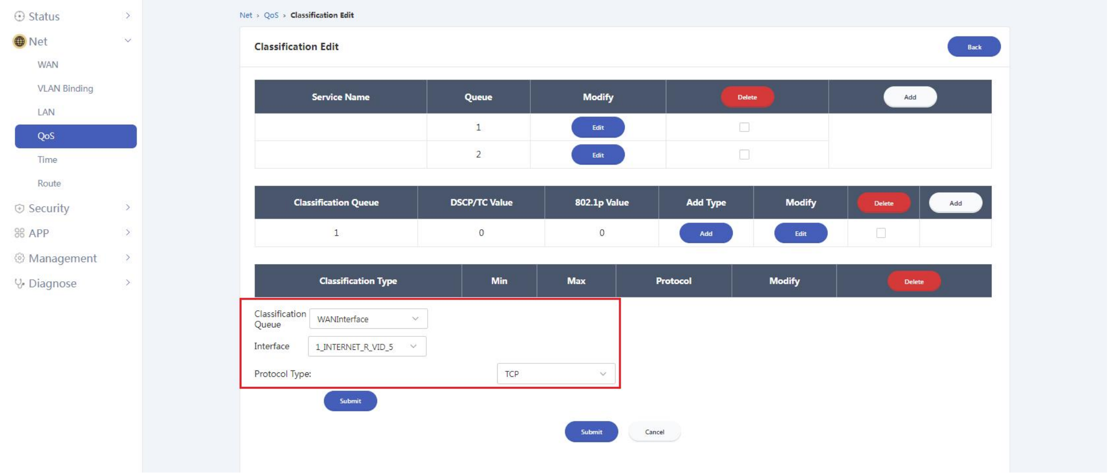
Queue Discipline: ● PQ ○ WRR ○ CAR

Enable DSCP Flag: □

Enable 802.1P Flag: 0 Flag

Queue	Priority	Enable
Q1	1	☑
Q2	2	☑
Q3	3	☑
Q4	4	□
Q5	5	□
Q6	6	□
Q7	7	□
Q8	8	□

Step 3: Configure VOIP to use Priority Queue 1, click "Add Type" to enter configuration, as illustrated in the figure below.



Classification Edit

Service Name	Queue	Modify	Delete	Add
	1	Edit	□	
	2	Edit	□	

Classification Queue	DSCP/TC Value	802.1p Value	Add Type	Modify	Delete	Add
1	0	0	Add	Edit	□	

Classification Type	Min	Max	Protocol	Modify	Delete

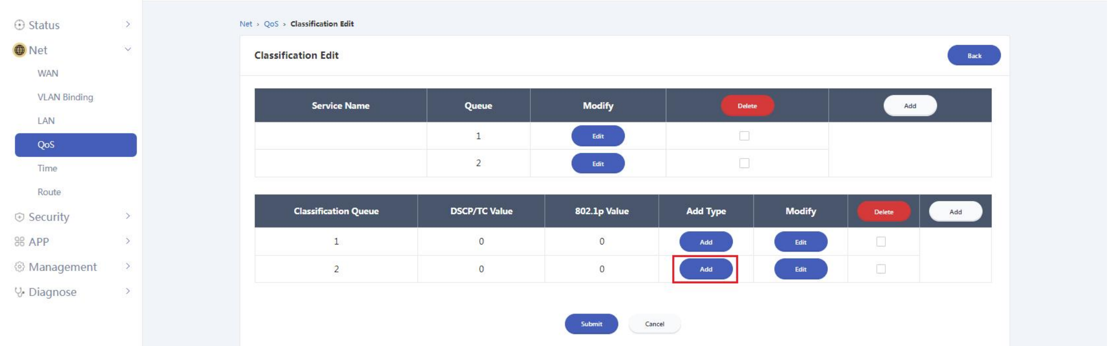
Classification Queue: WANInterface

Interface: 1_INTERNET_R_VID_5

Protocol Type: TCP

Submit

Step 4: Configure PC1's parameters and click "Add & Submit" to add a new type as illustrated in the figure below.

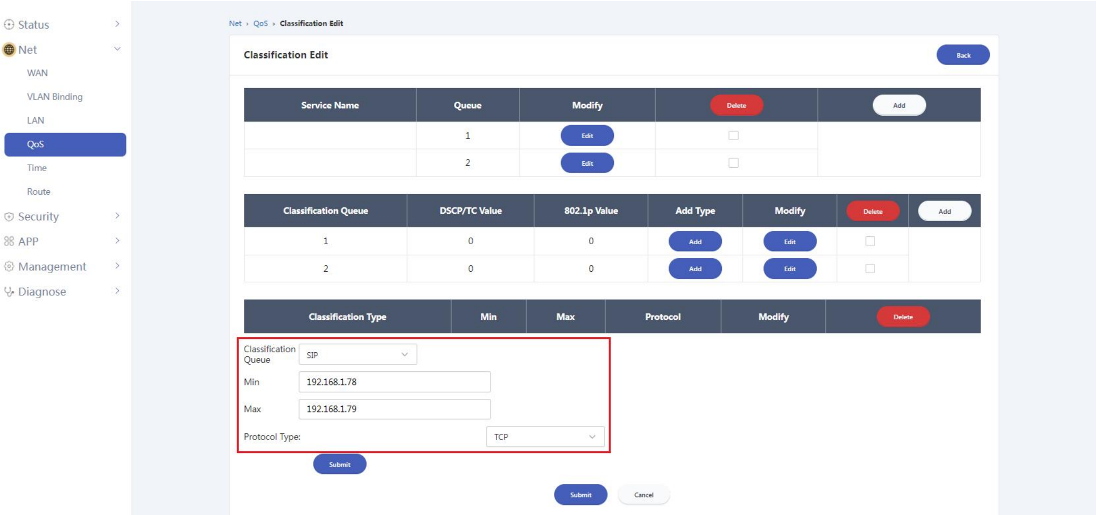


Classification Edit

Service Name	Queue	Modify	Delete	Add
	1	Edit	□	
	2	Edit	□	

Classification Queue	DSCP/TC Value	802.1p Value	Add Type	Modify	Delete	Add
1	0	0	Add	Edit	□	
2	0	0	Add	Edit	□	

Configure PC1 parameters, click "Submit" and "Submit" to add a new type, as illustrated in the figure below.



Classification Edit

Service Name	Queue	Modify	Delete	Add
	1	Edit	□	
	2	Edit	□	

Classification Queue	DSCP/TC Value	802.1p Value	Add Type	Modify	Delete	Add
1	0	0	Add	Edit	□	
2	0	0	Add	Edit	□	

Classification Type	Min	Max	Protocol	Modify	Delete

Classification Queue: SIP

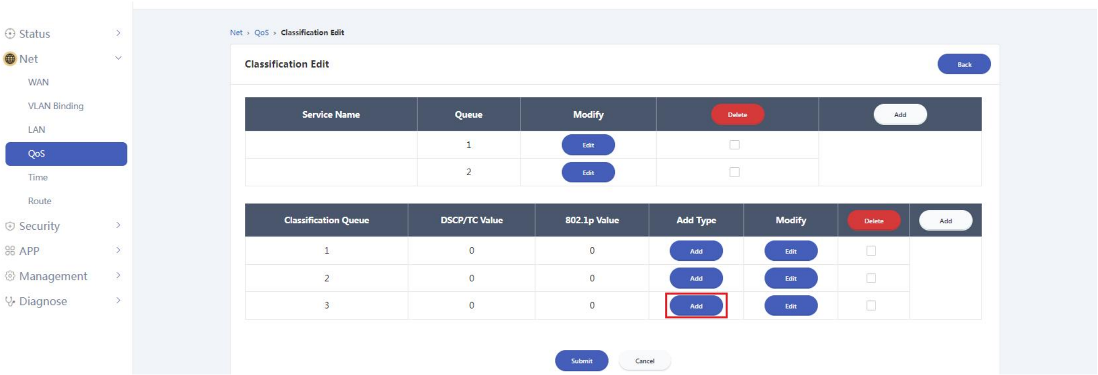
Min: 192.168.1.78

Max: 192.168.1.79

Protocol Type: TCP

Submit

Step 5: Configure PC2 to use priority queue 3, click add type, and enter the configuration as illustrated in the figure below.

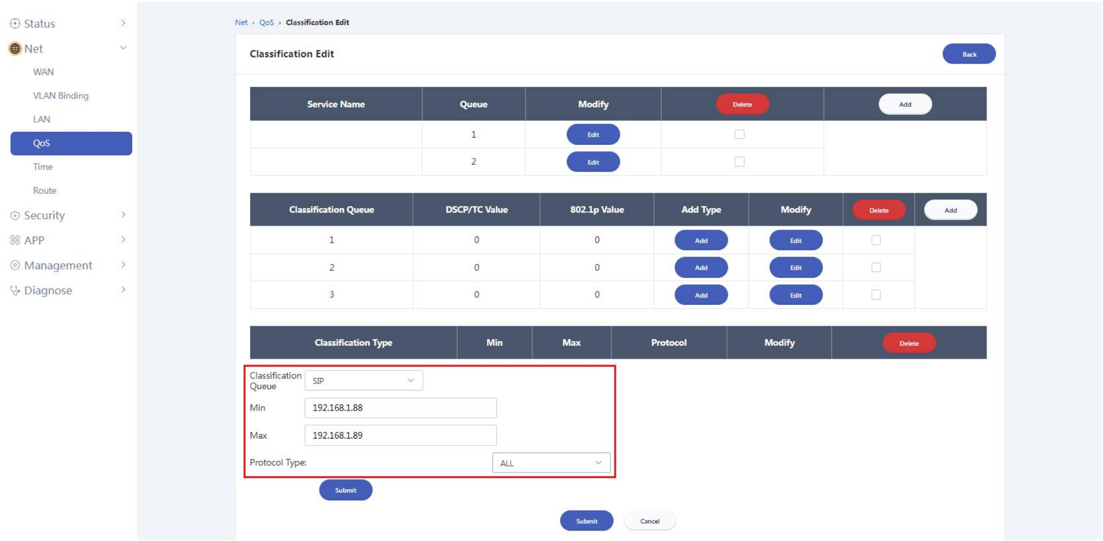


Classification Edit

Service Name	Queue	Modify	Delete	Add
	1	Edit	□	
	2	Edit	□	

Classification Queue	DSCP/TC Value	802.1p Value	Add Type	Modify	Delete	Add
1	0	0	Add	Edit	□	
2	0	0	Add	Edit	□	
3	0	0	Add	Edit	□	

Configure PC2's parameters and click "Submit" and "Submit" to add a new type as illustrated in the figure below.



Classification Edit

Service Name	Queue	Modify	Delete	Add
	1	Edit	□	
	2	Edit	□	

Classification Queue	DSCP/TC Value	802.1p Value	Add Type	Modify	Delete	Add
1	0	0	Add	Edit	□	
2	0	0	Add	Edit	□	
3	0	0	Add	Edit	□	

Classification Type	Min	Max	Protocol	Modify	Delete

Classification Queue: SIP

Min: 192.168.1.88

Max: 192.168.1.89

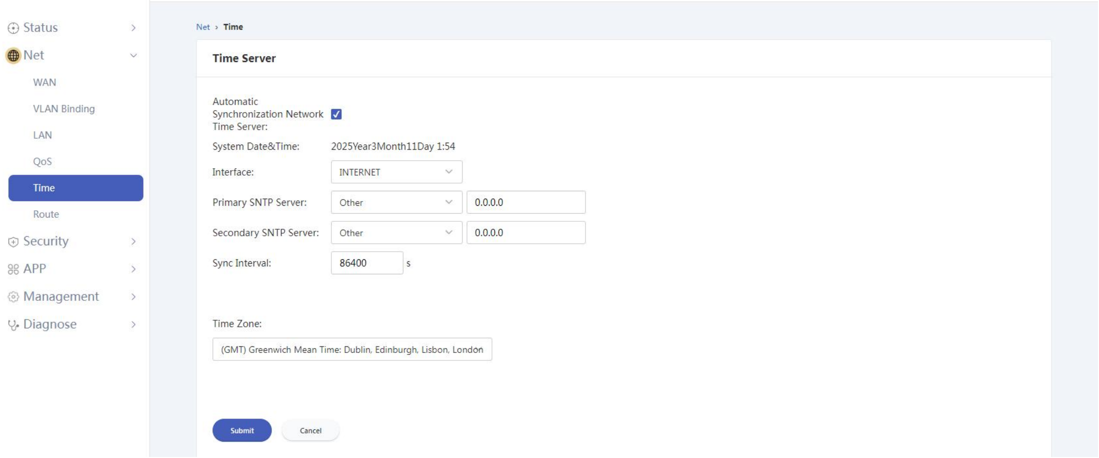
Protocol Type: ALL

After completing the configuration, click "Submit" to save and enable the current settings, making the QoS function effective.

6.1.5 Time Setting

This section implements manual setting of the terminal time, or synchronization with the time server.

Step 1: Click on the menu "Net -> Time" as illustrated in the figure below.



Time Server

Automatic Synchronization Network Time Server: ☑

System Date&Time: 2025Year3Month11Day 1:54

Interface: INTERNET

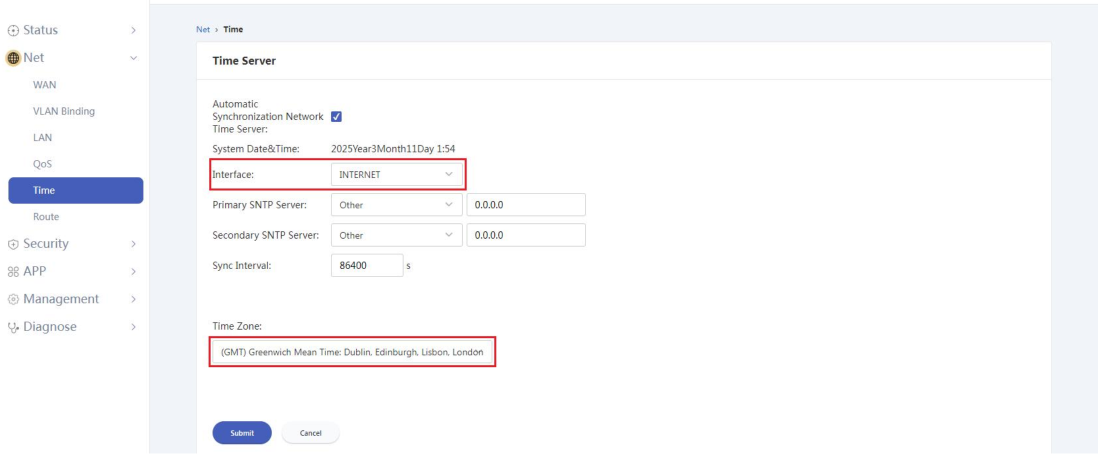
Primary SNTP Server: Other 0.0.0.0

Secondary SNTP Server: Other 0.0.0.0

Sync Interval: 86400 s

Time Zone: (GMT) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London

Step 2: Check to enable the time server, select the correct WAN interface, and choose the correct time zone as illustrated in the figure below.



Time Server

Automatic Synchronization Network Time Server: ☑

System Date&Time: 2025Year3Month11Day 1:54

Interface: INTERNET

Primary SNTP Server: Other 0.0.0.0

Secondary SNTP Server: Other 0.0.0.0

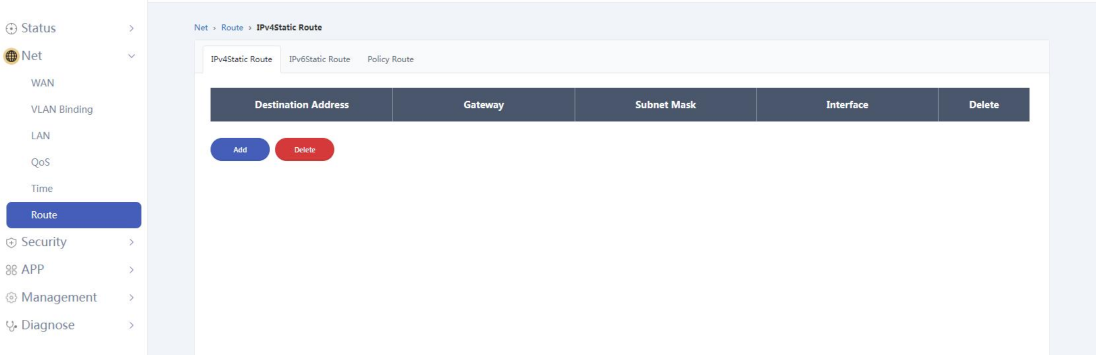
Sync Interval: 86400 s

Time Zone: (GMT) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London

6.1.6 Static Route Setting

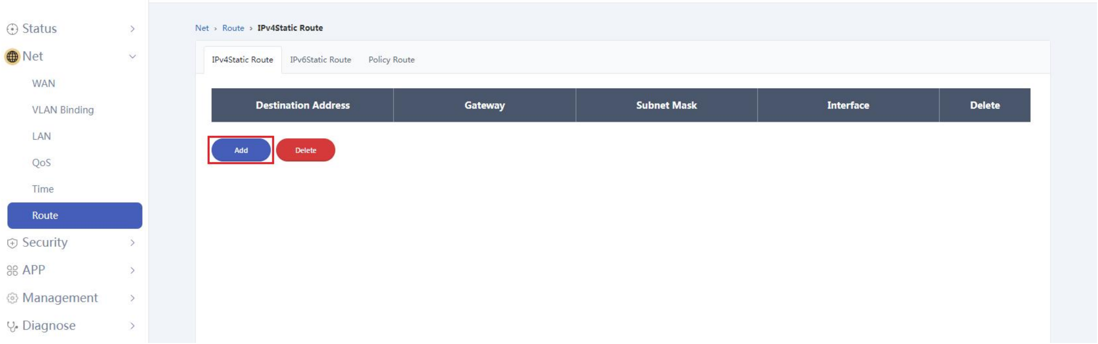
6.1.6.1 Add an IPv4 Static Route Instance

Click on the menu "Net -> Route -> IPv6Static Route" as illustrated in the figure below.



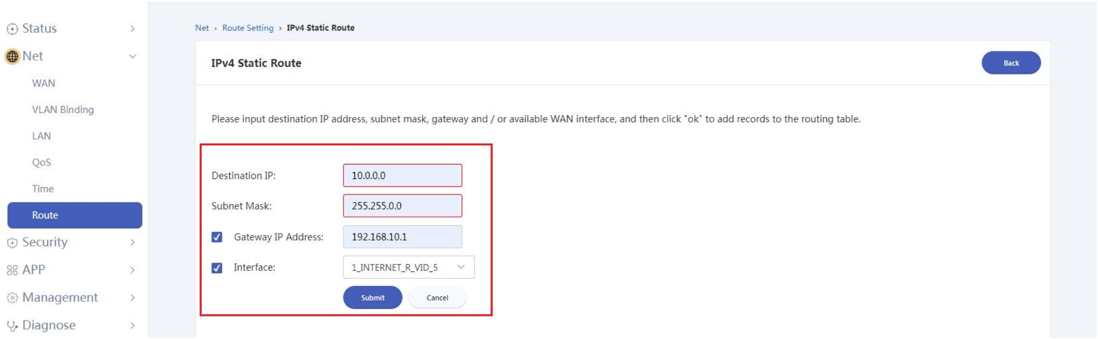
Destination Address	Gateway	Subnet Mask	Interface	Delete

Step 1: Click "Add" to enter the IPv4 static route configuration page as illustrated in the figure below.



Destination Address	Gateway	Subnet Mask	Interface	Delete

Step 2: Configure the relevant static route parameters and click "Submit" to add it to the routing table as illustrated in the figure below.



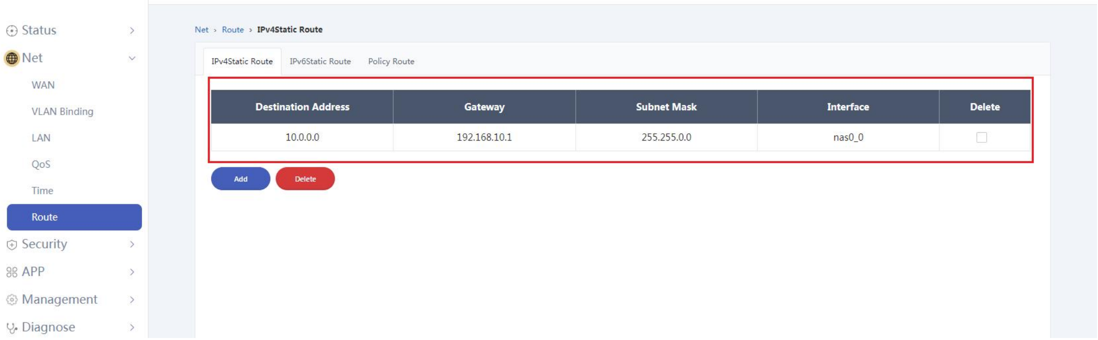
Please input destination IP address, subnet mask, gateway and / or available WAN interface, and then click "ok" to add records to the routing table.

Destination IP: 10.0.0.0

Subnet Mask: 255.255.0.0

☑ Gateway IP Address: 192.168.10.1

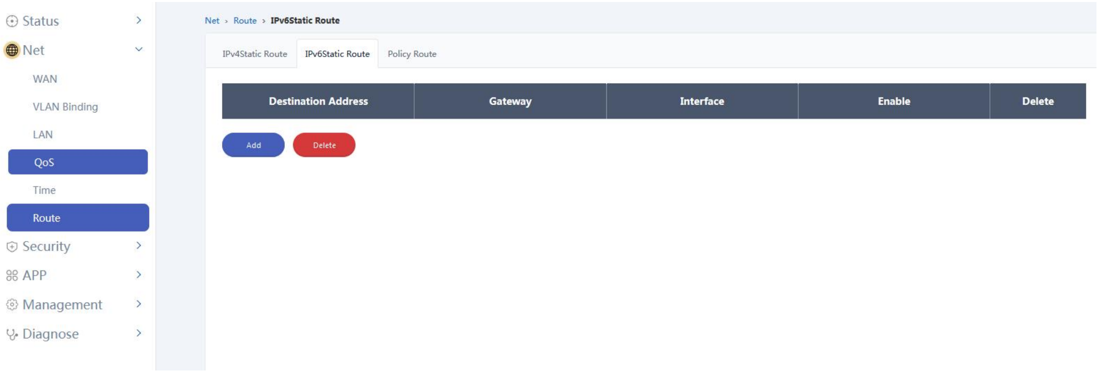
☑ Interface: 1_INTERNET_R_VID_5



Destination Address	Gateway	Subnet Mask	Interface	Delete
10.0.0.0	192.168.10.1	255.255.0.0	nas0_0	□

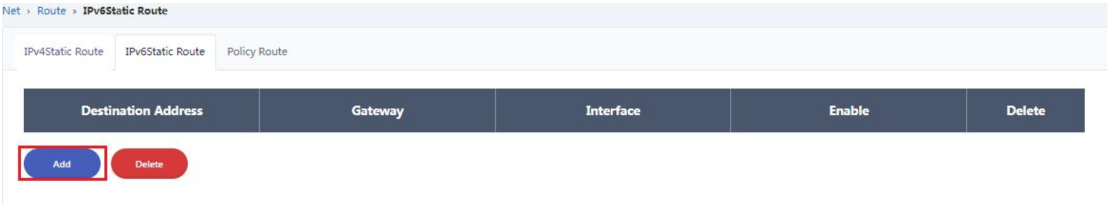
6.1.6.2 Adding an IPv6 Static Route Instance

Click on the menu "Net -> Route -> IPv6Static Route" as illustrated in the figure below.



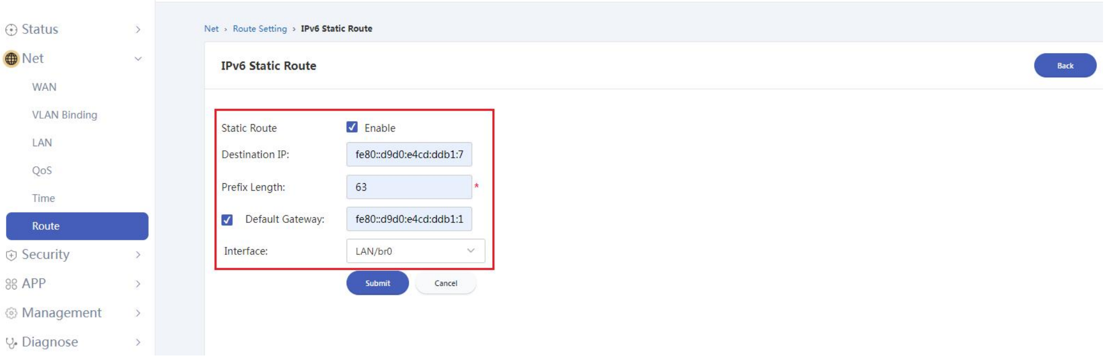
Destination Address	Gateway	Interface	Enable	Delete

Step 1: Click "Add" to enter the IPv6 static route configuration page as illustrated in the figure below.



Destination Address	Gateway	Interface	Enable	Delete

Step 2: Check "Enable" and configure the relevant IPv6 static route parameters as illustrated in the figure below.



IPv6 Static Route

Static Route ☑ Enable

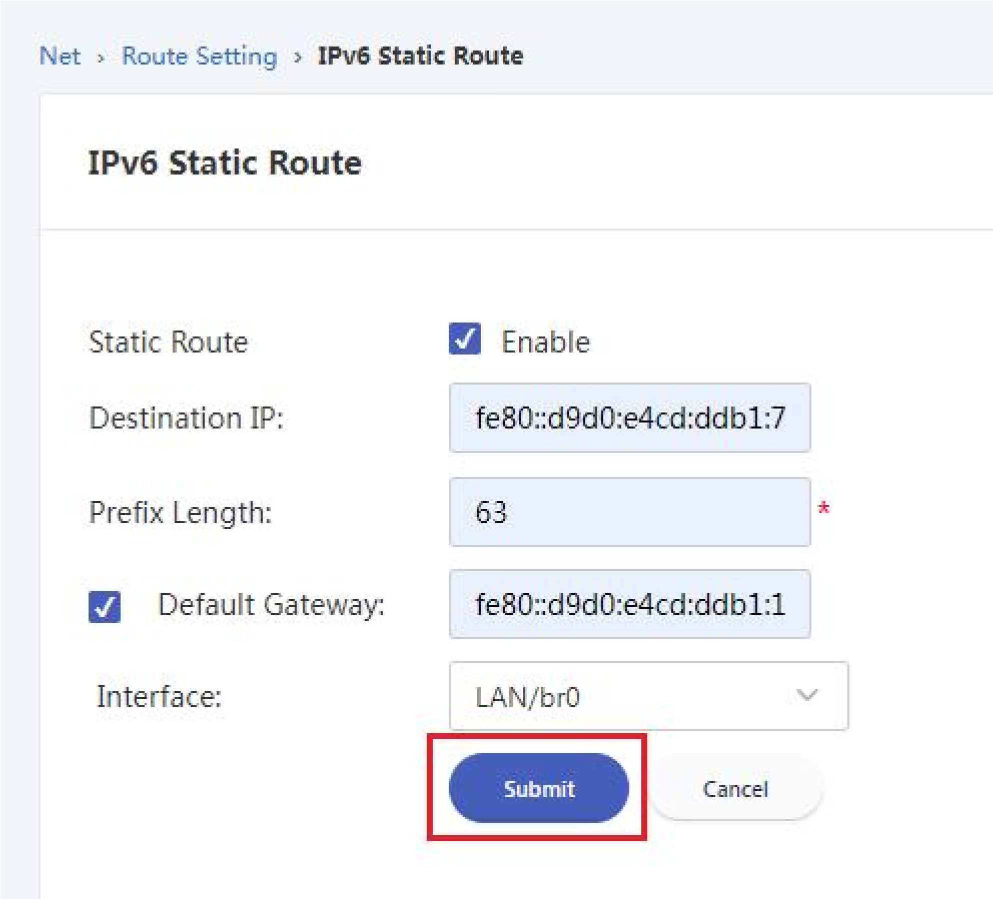
Destination IP: fe80::d9d0:e4cd:ddb1:7

Prefix Length: 63 *

☑ Default Gateway: fe80::d9d0:e4cd:ddb1:1

Interface: LAN/br0

Step 3: Click "Submit" to complete the IPv6 static route configuration.



Net › Route Setting › IPv6 Static Route

IPv6 Static Route

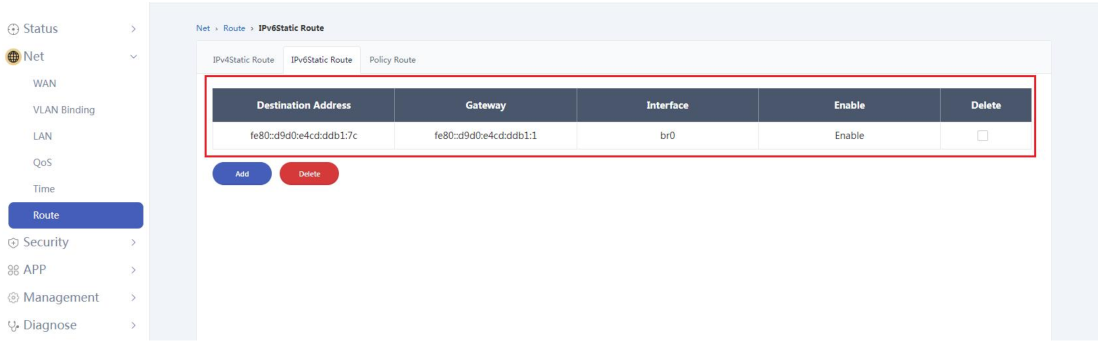
Static Route ☑ Enable

Destination IP: fe80::d9d0:e4cd:ddb1:7

Prefix Length: 63 *

☑ Default Gateway: fe80::d9d0:e4cd:ddb1:1

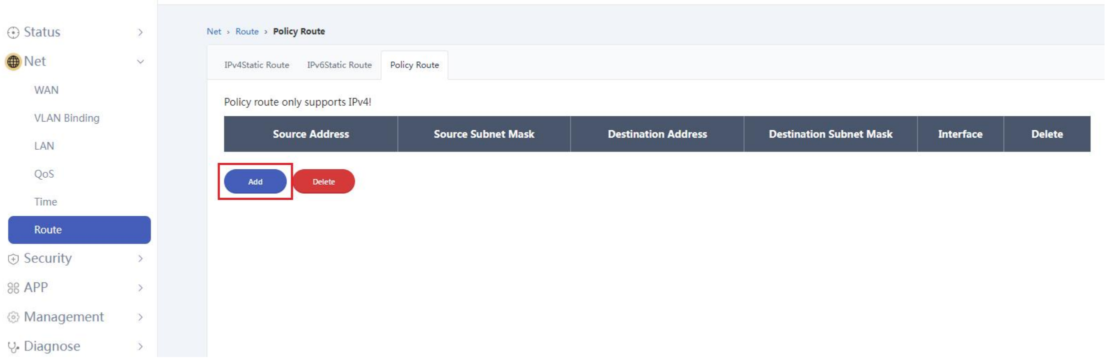
Interface: LAN/br0



Destination Address	Gateway	Interface	Enable	Delete
fe80::d9d0:e4cd:ddb1:7c	fe80::d9d0:e4cd:ddb1:1	br0	Enable	□

6.1.6.3 Adding an Policy Route Instance

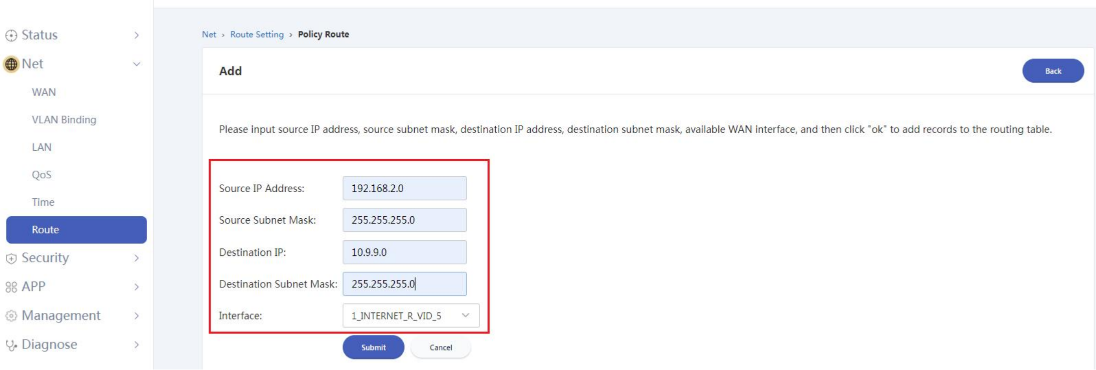
Step 1: Click "Add" to enter the Policy Route configuration page.



Policy route only supports IPv4!

Source Address	Source Subnet Mask	Destination Address	Destination Subnet Mask	Interface	Delete

Step 2: Set the relevant parameters for the policy route as illustrated in the figure below.



Net › Route Setting › Policy Route

Add

Please input source IP address, source subnet mask, destination IP address, destination subnet mask, available WAN interface, and then click "ok" to add records to the routing table.

Source IP Address: 192.168.2.0

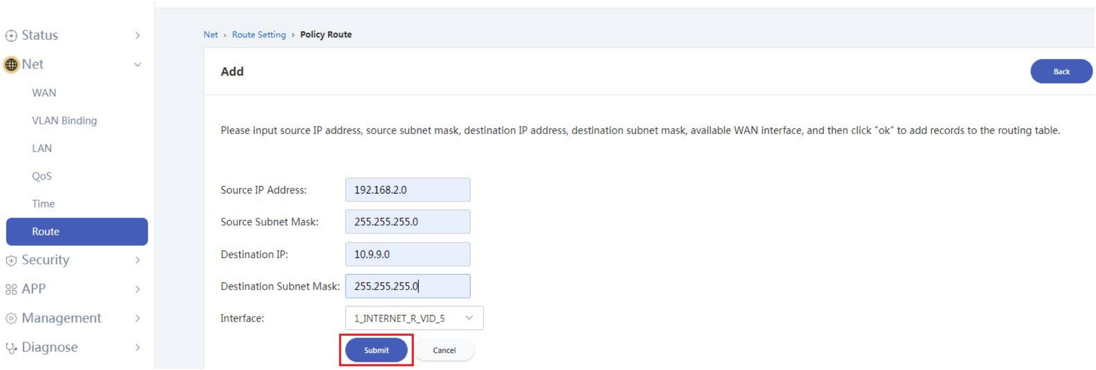
Source Subnet Mask: 255.255.255.0

Destination IP: 10.9.9.0

Destination Subnet Mask: 255.255.255.0

Interface: 1_INTERNET_R_VID_5

Step 3: Click "Submit" to complete the policy route configuration.



Net › Route Setting › Policy Route

Add

Please input source IP address, source subnet mask, destination IP address, destination subnet mask, available WAN interface, and then click "ok" to add records to the routing table.

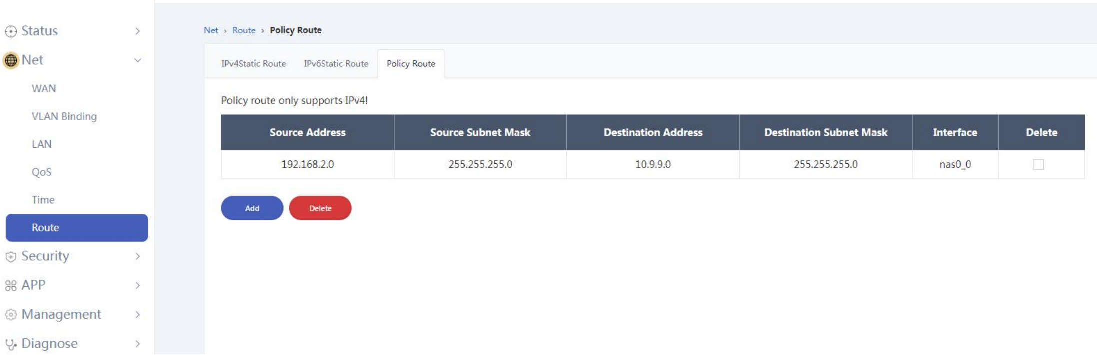
Source IP Address: 192.168.2.0

Source Subnet Mask: 255.255.255.0

Destination IP: 10.9.9.0

Destination Subnet Mask: 255.255.255.0

Interface: 1_INTERNET_R_VID_5



Net › Route › Policy Route

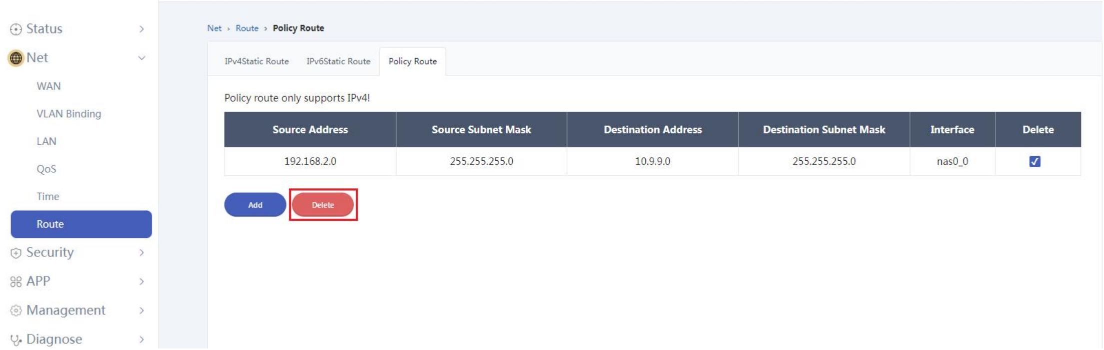
Policy route only supports IPv4!

Source Address	Source Subnet Mask	Destination Address	Destination Subnet Mask	Interface	Delete
192.168.2.0	255.255.255.0	10.9.9.0	255.255.255.0	nas0_0	□

6.1.6.4 Deleting Static Route Instances

6.1.6.4.1 Deleting an IPv4 Static Route

Select the instance you want to delete and click the "Delete" button to complete the deletion as illustrated in the figure below.

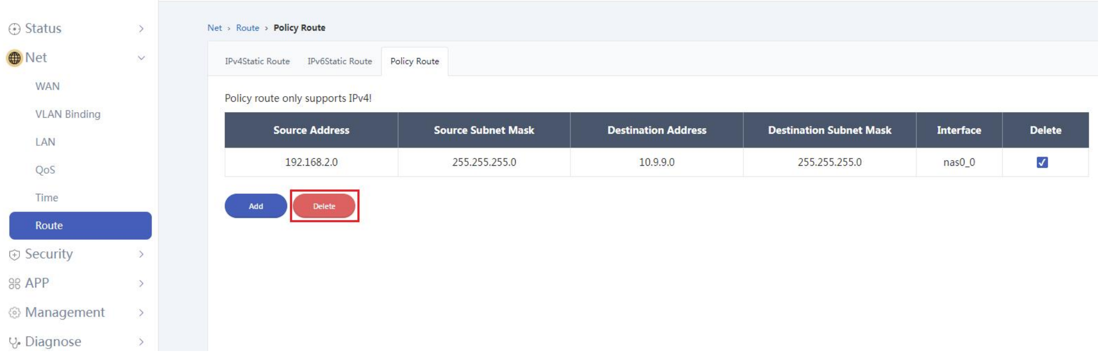


Policy route only supports IPv4!

Source Address	Source Subnet Mask	Destination Address	Destination Subnet Mask	Interface	Delete
192.168.2.0	255.255.255.0	10.9.9.0	255.255.255.0	nas0_0	☑

6.1.6.4.2 Deleting an IPv6 Static Route

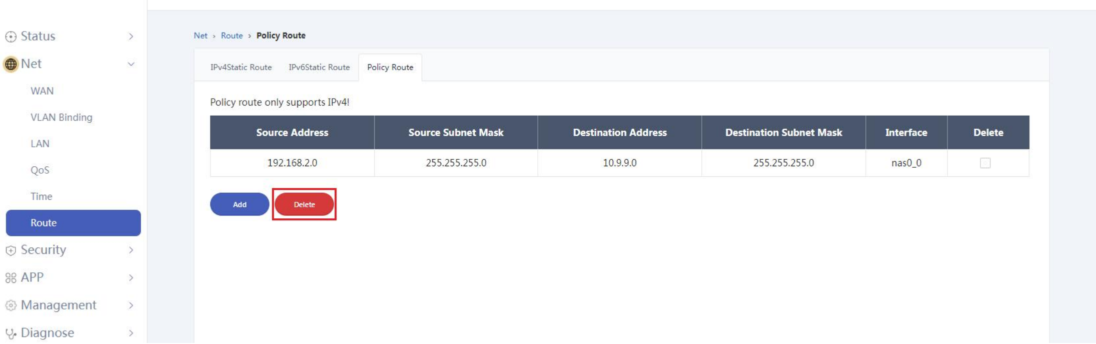
Select the instance you wish to delete and click the "Delete" button to complete the deletion as illustrated in the figure below.



Policy route only supports IPv4!

Source Address	Source Subnet Mask	Destination Address	Destination Subnet Mask	Interface	Delete
192.168.2.0	255.255.255.0	10.9.9.0	255.255.255.0	nas0_0	☑

6.1.6.4.3 Deleting a Policy Route



Policy route only supports IPv4!

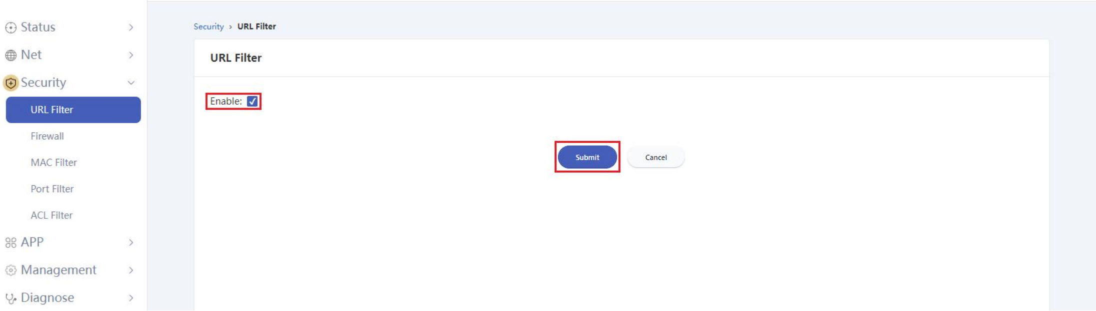
Source Address	Source Subnet Mask	Destination Address	Destination Subnet Mask	Interface	Delete
192.168.2.0	255.255.255.0	10.9.9.0	255.255.255.0	nas0_0	□

6.2 Security Setting

6.2.1 URL Filter

6.2.1.1 Enabling URL Filter

Click on the menu "Security -> URL Filter". Check the enable box and click the "Submit" button to activate as illustrated in the figure below.

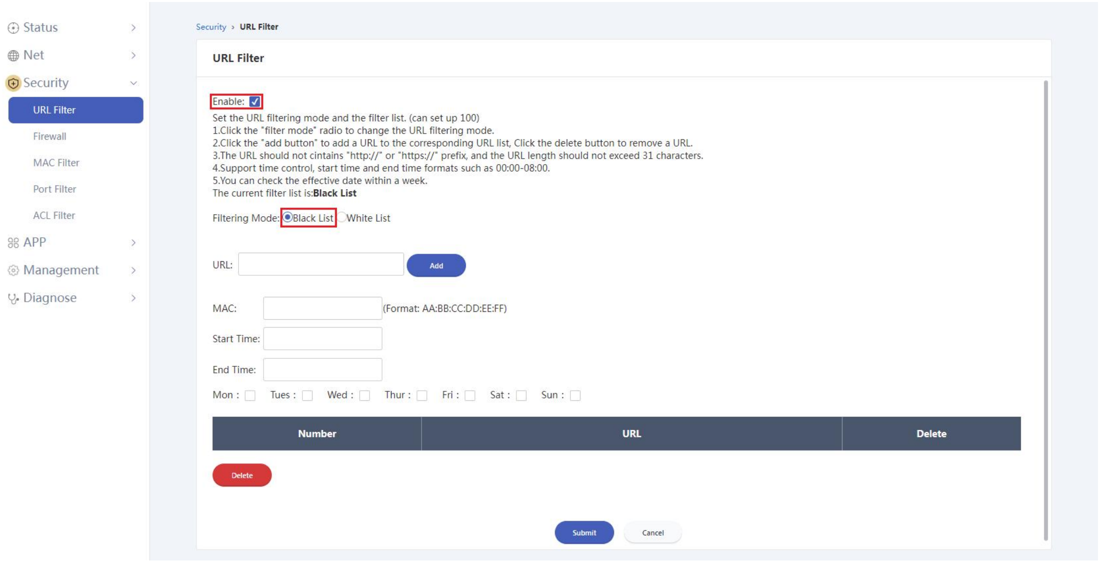


Enable: ☑

6.2.1.2 Adding URL Filter Blacklist Instance

Blacklist: URL addresses in this list are inaccessible.

Step 1: Check "Enable" and select the "Black List" mode as illustrated in the figure below.



URL Filter

Enable: ☑

Set the URL filtering mode and the filter list. (can set up 100)
1.Click the "filter mode" radio to change the URL filtering mode.
2.Click the "add button" to add a URL to the corresponding URL list, Click the delete button to remove a URL.
3.The URL should not cintains "http://" or "https://" prefix, and the URL length should not exceed 31 characters.
4.Support time control, start time and end time formats such as 00:00-08:00.
5.You can check the effective date within a week.
The current filter list is:**Black List**

Filtering Mode: ● Black List ○ White List

URL:

MAC: (Format: AA:BB:CC:DD:EE:FF)

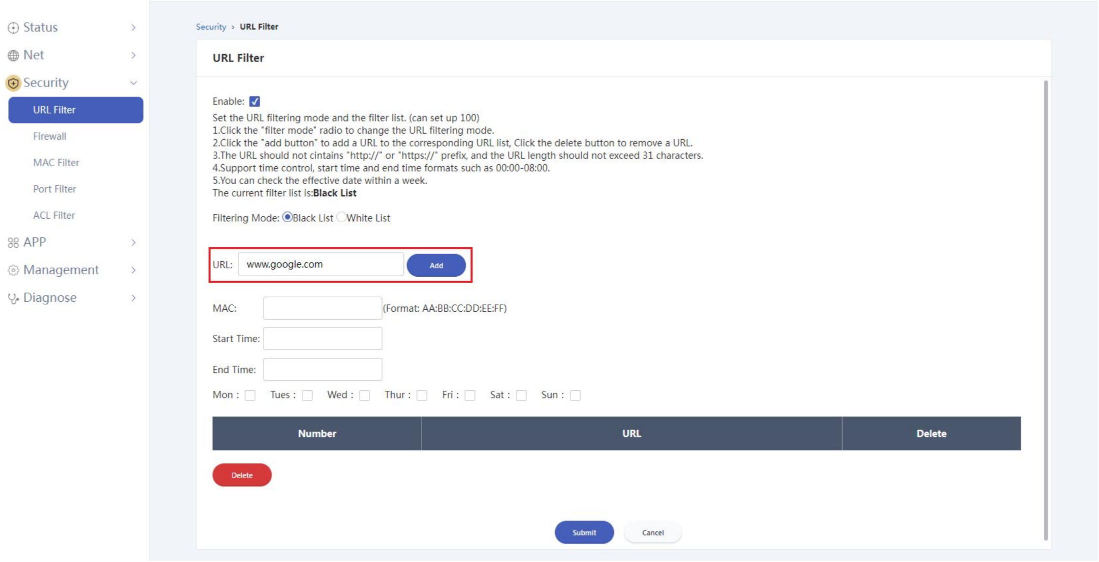
Start Time:

End Time:

Mon : □ Tues : □ Wed : □ Thur : □ Fri : □ Sat : □ Sun : □

Number	URL	Delete

Step 2: Configure the relevant filtering parameters and click "Add" to add the blacklist as illustrated in the figure below.



URL Filter

Enable: ☑

Set the URL filtering mode and the filter list. (can set up 100)
1.Click the "filter mode" radio to change the URL filtering mode.
2.Click the "add button" to add a URL to the corresponding URL list, Click the delete button to remove a URL.
3.The URL should not cintains "http://" or "https://" prefix, and the URL length should not exceed 31 characters.
4.Support time control, start time and end time formats such as 00:00-08:00.
5.You can check the effective date within a week.
The current filter list is:**Black List**

Filtering Mode: ● Black List ○ White List

URL: www.google.com

MAC: (Format: AA:BB:CC:DD:EE:FF)

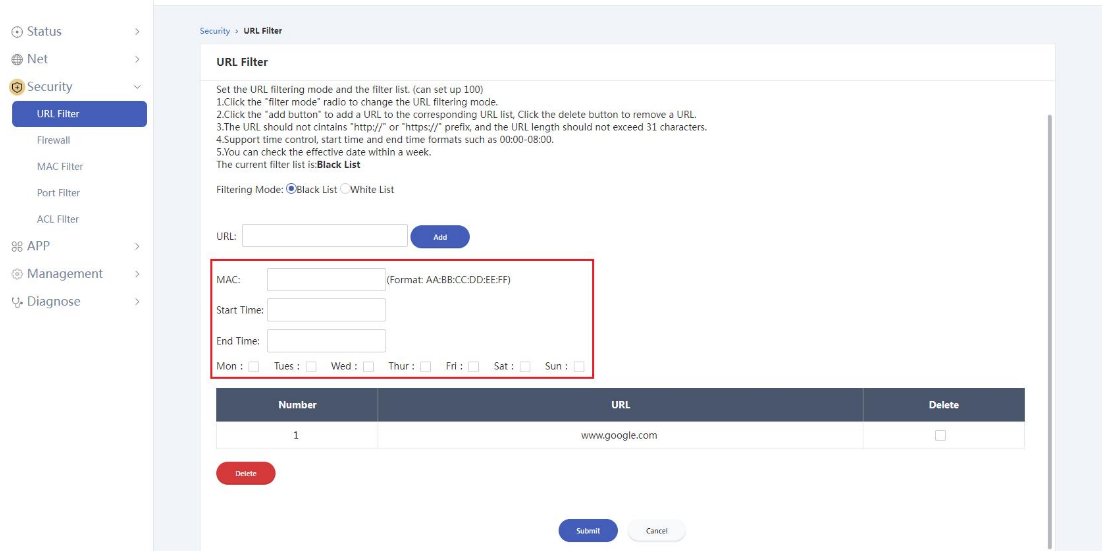
Start Time:

End Time:

Mon : □ Tues : □ Wed : □ Thur : □ Fri : □ Sat : □ Sun : □

Number	URL	Delete

Step 3: Configure the corresponding MAC address, start time, end time, and day of the week, then click "Submit" as illustrated in the figure below.



Set the URL filtering mode and the filter list. (can set up 100)
1.Click the "filter mode" radio to change the URL filtering mode.
2.Click the "add button" to add a URL to the corresponding URL list, Click the delete button to remove a URL.
3.The URL should not cintains "http://" or "https://" prefix, and the URL length should not exceed 31 characters.
4.Support time control, start time and end time formats such as 00:00-08:00.
5.You can check the effective date within a week.
The current filter list is:**Black List**

Filtering Mode: ● Black List ○ White List

URL: Add

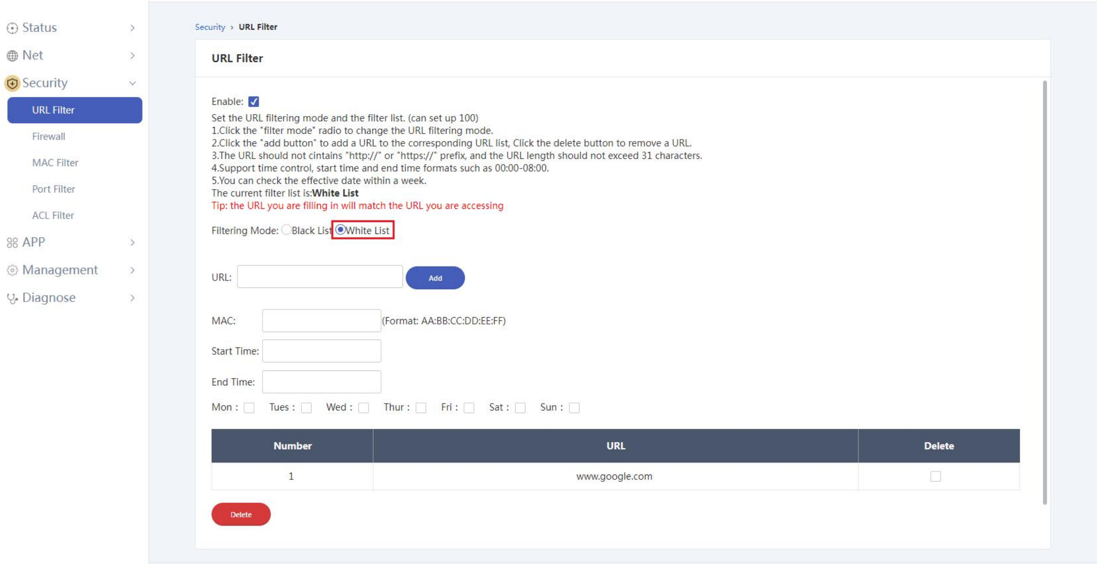
MAC: (Format: AA:BB:CC:DD:EE:FF)
Start Time:
End Time:
Mon : □ Tues : □ Wed : □ Thur : □ Fri : □ Sat : □ Sun : □

Number	URL	Delete
1	www.google.com	□

6.2.1.3 Adding URL Filter Whitelist Instance

Whitelist: Only URLs listed here are allowed to be accessed.

Step 1: Select "White list" to enter whitelist mode as illustrated in the figure below.



URL Filter

Enable: ☑

Set the URL filtering mode and the filter list. (can set up 100)
1.Click the "filter mode" radio to change the URL filtering mode.
2.Click the "add button" to add a URL to the corresponding URL list, Click the delete button to remove a URL.
3.The URL should not cintains "http://" or "https://" prefix, and the URL length should not exceed 31 characters.
4.Support time control, start time and end time formats such as 00:00-08:00.
5.You can check the effective date within a week.
The current filter list is:**White List**
Tip: the URL you are filling in will match the URL you are accessing

Filtering Mode: ○Black List ●White List

URL: [ ] Add

MAC: [ ] (Format: AA:BB:CC:DD:EE:FF)

Start Time: [ ]

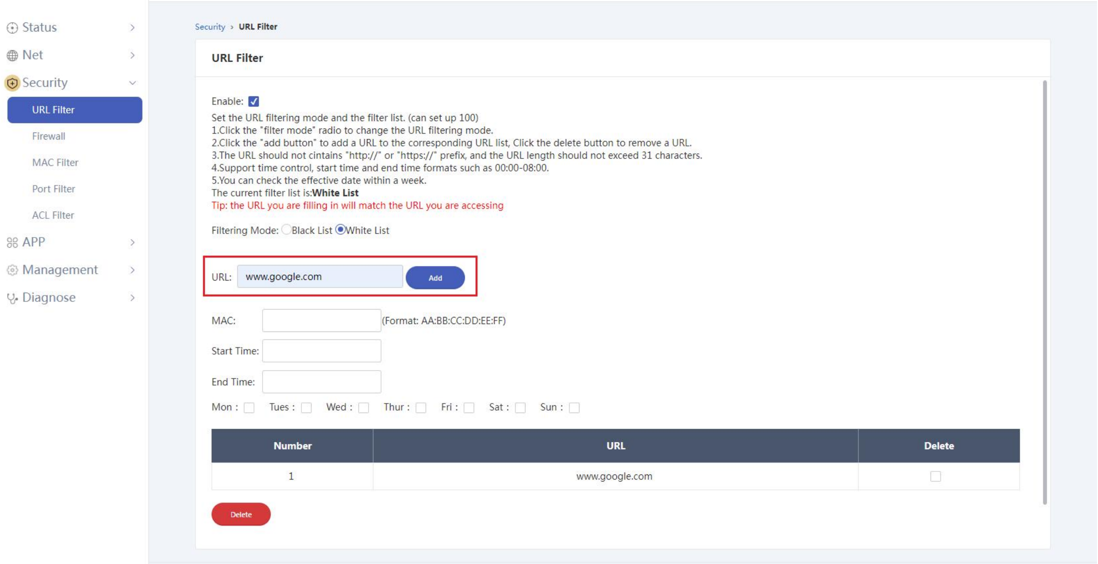
End Time: [ ]

Mon : □ Tues : □ Wed : □ Thur : □ Fri : □ Sat : □ Sun : □

Number	URL	Delete
1	www.google.com	□

Delete

Step 2: Configure the relevant filtering parameters and click "Add" to add the whitelist as illustrated in the figure below.



URL Filter

Enable: ☑

Set the URL filtering mode and the filter list. (can set up 100)
1.Click the "filter mode" radio to change the URL filtering mode.
2.Click the "add button" to add a URL to the corresponding URL list, Click the delete button to remove a URL.
3.The URL should not cintains "http://" or "https://" prefix, and the URL length should not exceed 31 characters.
4.Support time control, start time and end time formats such as 00:00-08:00.
5.You can check the effective date within a week.
The current filter list is:**White List**
Tip: the URL you are filling in will match the URL you are accessing

Filtering Mode: ○Black List ●White List

URL: www.google.com Add

MAC: [ ] (Format: AA:BB:CC:DD:EE:FF)

Start Time: [ ]

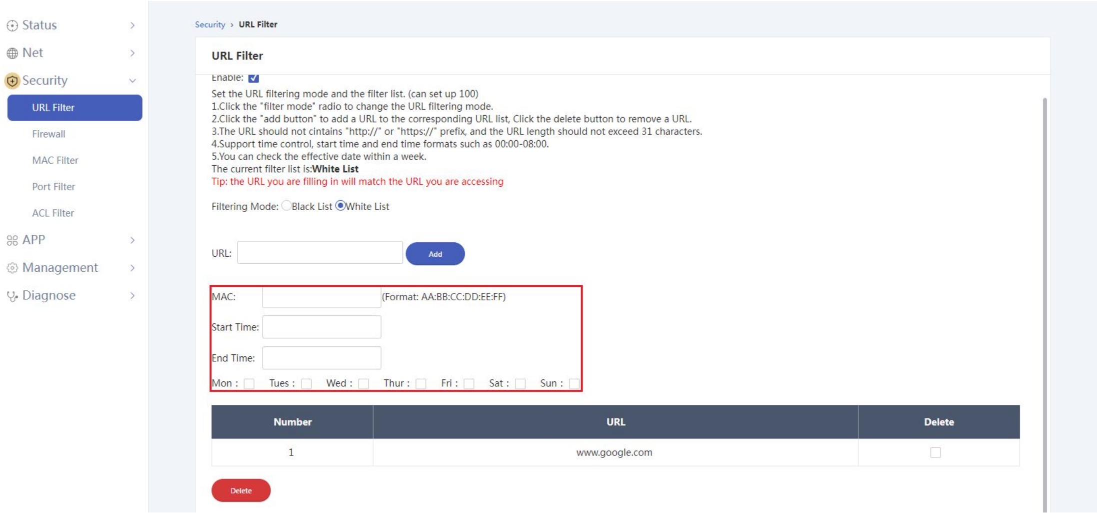
End Time: [ ]

Mon : □ Tues : □ Wed : □ Thur : □ Fri : □ Sat : □ Sun : □

Number	URL	Delete
1	www.google.com	□

Delete

Step 3: Set the corresponding MAC address, start time, end time, and day of the week, then click "Submit" as illustrated in the figure below.



URL Filter

Enable: ☑

Set the URL filtering mode and the filter list. (can set up 100)
1.Click the "filter mode" radio to change the URL filtering mode.
2.Click the "add button" to add a URL to the corresponding URL list, Click the delete button to remove a URL.
3.The URL should not cintains "http://" or "https://" prefix, and the URL length should not exceed 31 characters.
4.Support time control, start time and end time formats such as 00:00-08:00.
5.You can check the effective date within a week.
The current filter list is:**White List**
Tip: the URL you are filling in will match the URL you are accessing

Filtering Mode: ○Black List ●White List

URL: Add

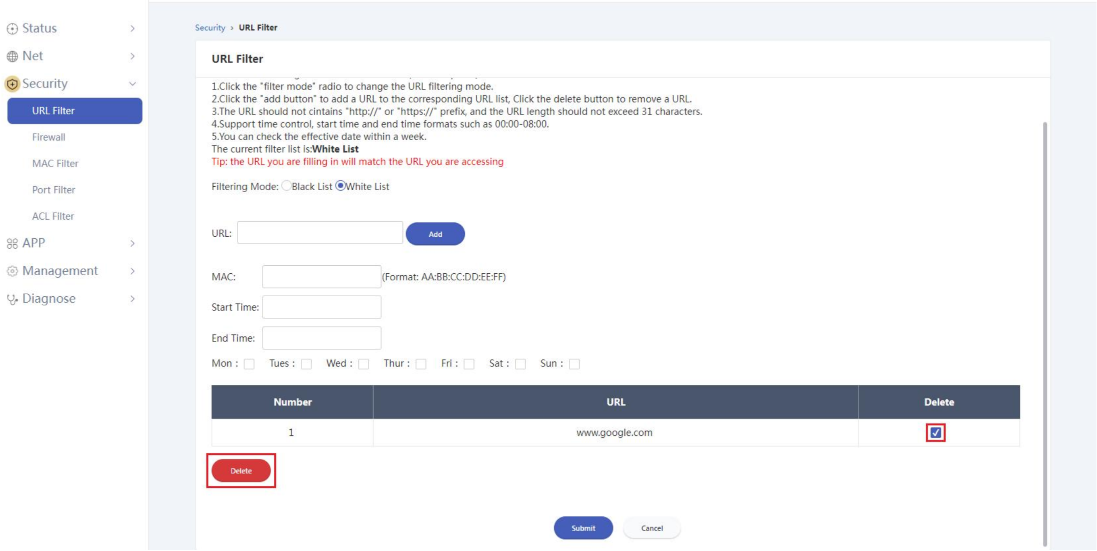
MAC: (Format: AA:BB:CC:DD:EE:FF)
Start Time:
End Time:
Mon : □ Tues : □ Wed : □ Thur : □ Fri : □ Sat : □ Sun : □

Number	URL	Delete
1	www.google.com	□

Delete

6.2.1.4 Deleting URL Filter Instance

Select the instance you wish to delete and click the "Delete" button to complete the deletion as illustrated in the figure below.



URL Filter

1.Click the "filter mode" radio to change the URL filtering mode.
2.Click the "add button" to add a URL to the corresponding URL list, Click the delete button to remove a URL.
3.The URL should not cintains "http://" or "https://" prefix, and the URL length should not exceed 31 characters.
4.Support time control, start time and end time formats such as 00:00-08:00.
5.You can check the effective date within a week.
The current filter list is:**White List**
Tip: the URL you are filling in will match the URL you are accessing

Filtering Mode: ○Black List ●White List

URL:

MAC: (Format: AA:BB:CC:DD:EE:FF)

Start Time:

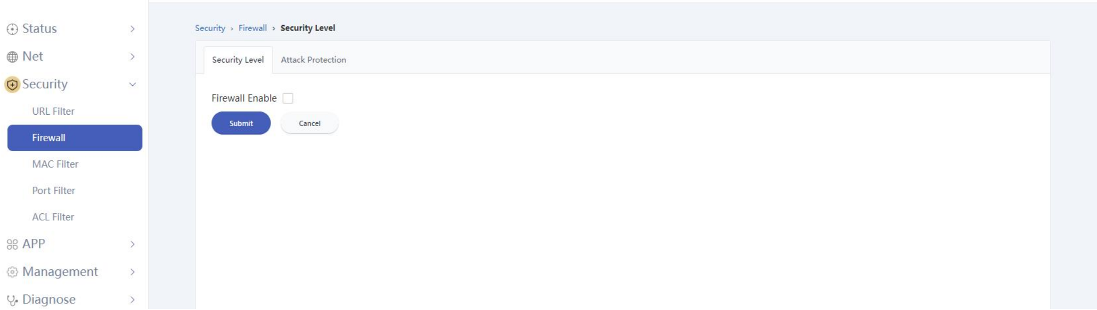
End Time:

Mon : □ Tues : □ Wed : □ Thur : □ Fri : □ Sat : □ Sun : □

Number	URL	Delete
1	www.google.com	☑

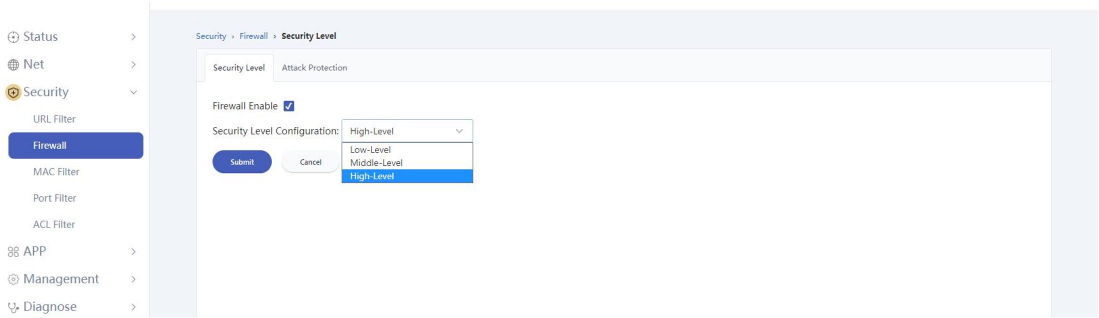
6.2.2 Firewall

Step 1: Click on the menu "Security -> Firewall" as illustrated in the figure below.



Firewall Enable □

Step 2: Check to enable the firewall and select the appropriate security level configuration. Click "Submit" to complete as illustrated in the figure below.



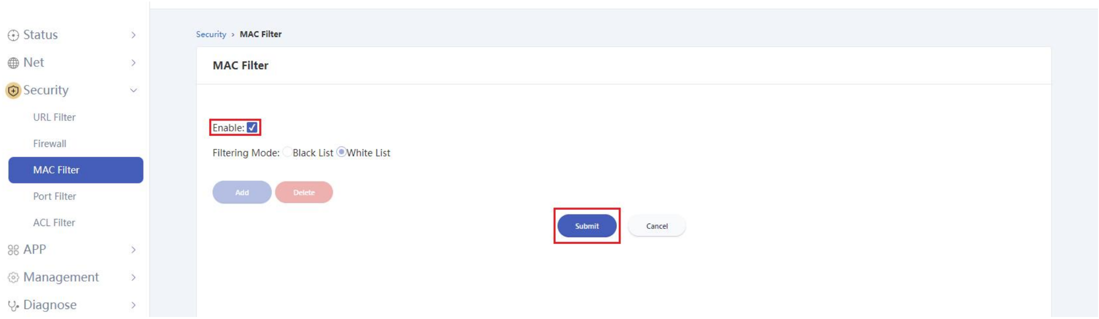
Firewall Enable ☑

Security Level Configuration: High-Level

6.2.3 MAC Filter

6.2.3.1 Enabling MAC Filter

Click on the menu "Security -> MAC Filter". Check to enable MAC filtering and click the "Submit" button as illustrated in the figure below.



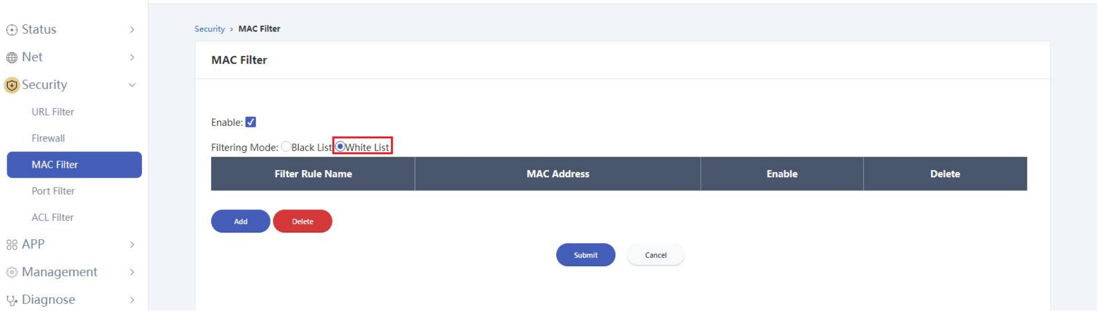
Enable: ☑

Filtering Mode: ○ Black List ● White List

6.2.3.2 Adding MAC Filter Whitelist

Whitelist: Only MAC addresses listed here can access the device.

Step 1: Check "Enable" and "White List" to enter whitelist mode as illustrated in the figure below.

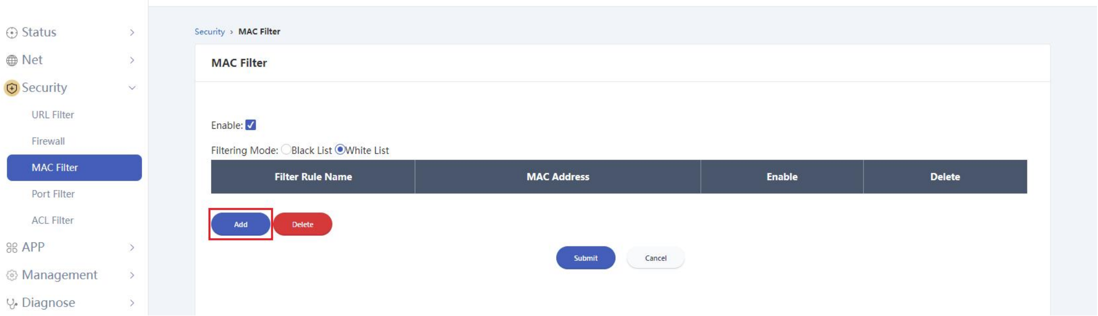


Enable: ☑

Filtering Mode: ○ Black List ● White List

Filter Rule Name	MAC Address	Enable	Delete

Step 2: Click "Add" to add the whitelist as illustrated in the figure below.

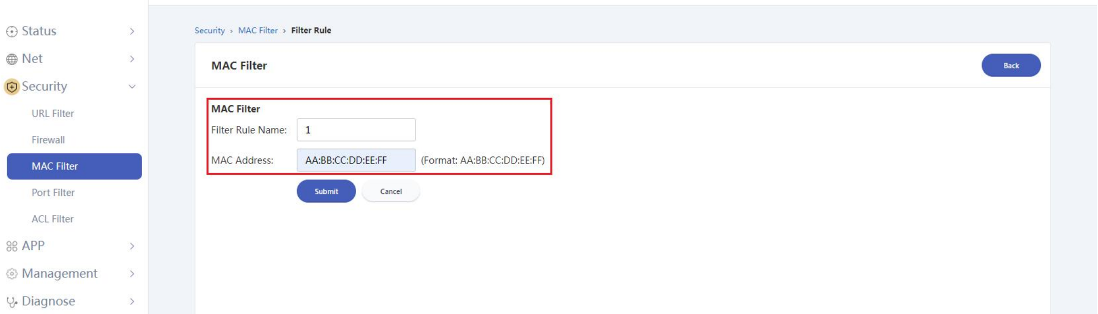


Enable: ☑

Filtering Mode: ○ Black List ● White List

Filter Rule Name	MAC Address	Enable	Delete

Step 3: Configure the relevant filtering parameters as illustrated in the figure below.

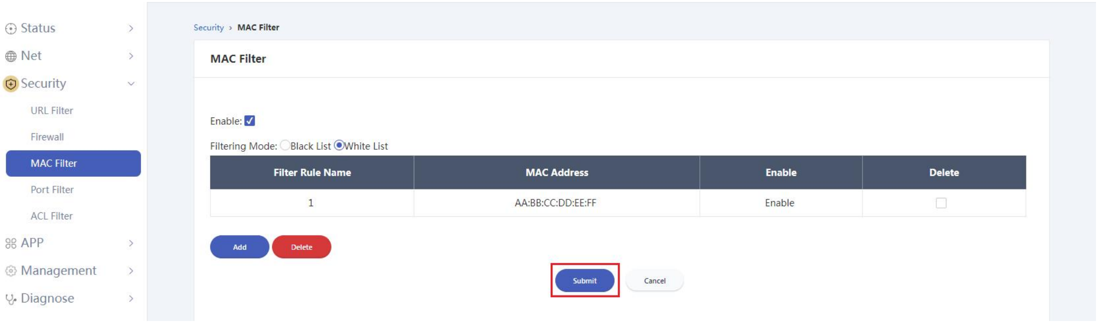


MAC Filter

Filter Rule Name: 1

MAC Address: AA:BB:CC:DD:EE:FF (Format: AA:BB:CC:DD:EE:FF)

Step 4: Click "Submit" to confirm, then click "Submit" again as illustrated in the figure below.



MAC Filter

Enable: ☑

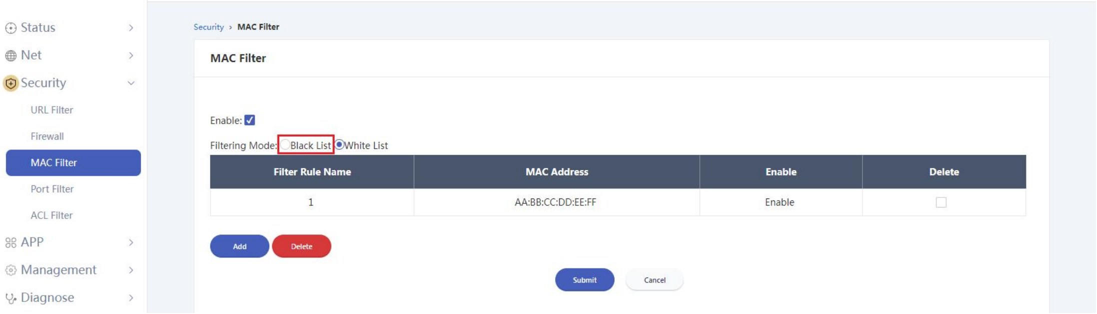
Filtering Mode: ○ Black List ● White List

Filter Rule Name	MAC Address	Enable	Delete
1	AA:BB:CC:DD:EE:FF	Enable	□

6.2.3.3 Adding MAC Filter Blacklist

Blacklist: MAC addresses listed here cannot access the device.

Step 1: Select "Black List" to enter blacklist mode.



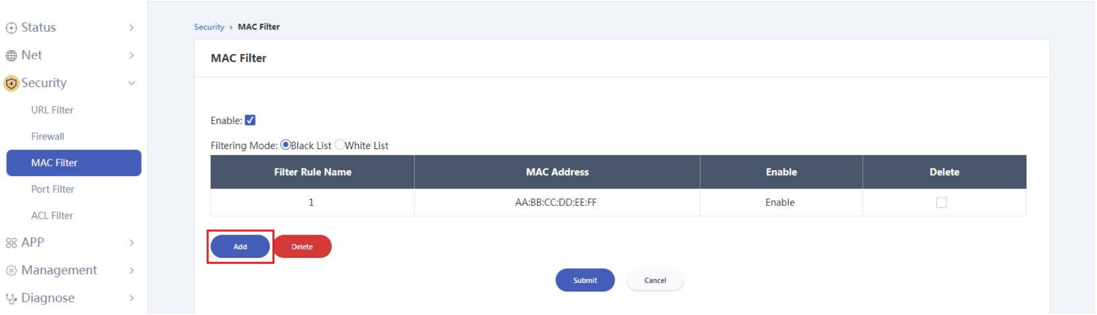
MAC Filter

Enable: ☑

Filtering Mode: ○ Black List ● White List

Filter Rule Name	MAC Address	Enable	Delete
1	AA:BB:CC:DD:EE:FF	Enable	□

Step 2: Click "Add" to add the blacklist as illustrated in the figure below.



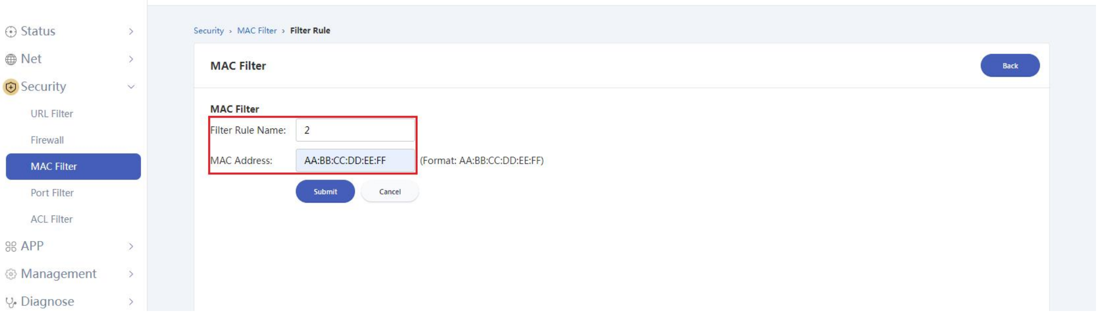
MAC Filter

Enable: ☑

Filtering Mode: ● Black List ○ White List

Filter Rule Name	MAC Address	Enable	Delete
1	AA:BB:CC:DD:EE:FF	Enable	□

Step 3: Configure the relevant MAC address parameters as illustrated in the figure below.

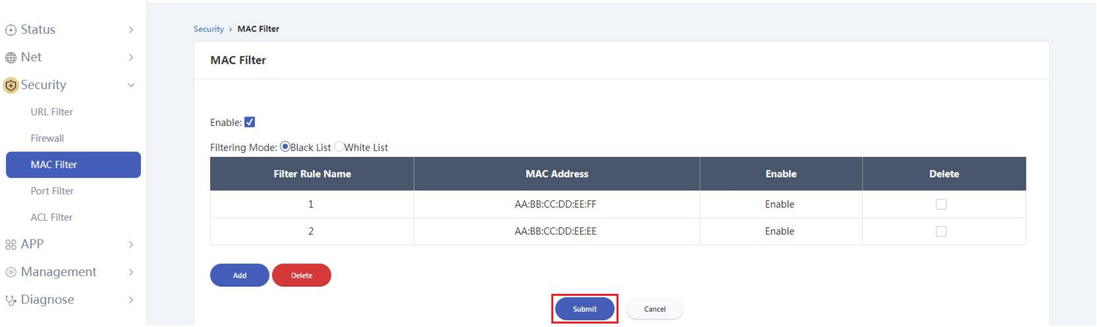


MAC Filter

Filter Rule Name: 2

MAC Address: AA:BB:CC:DD:EE:FF (Format: AA:BB:CC:DD:EE:FF)

Step 4: Click "Submit" to confirm, then click "Submit" again as illustrated in the figure below.



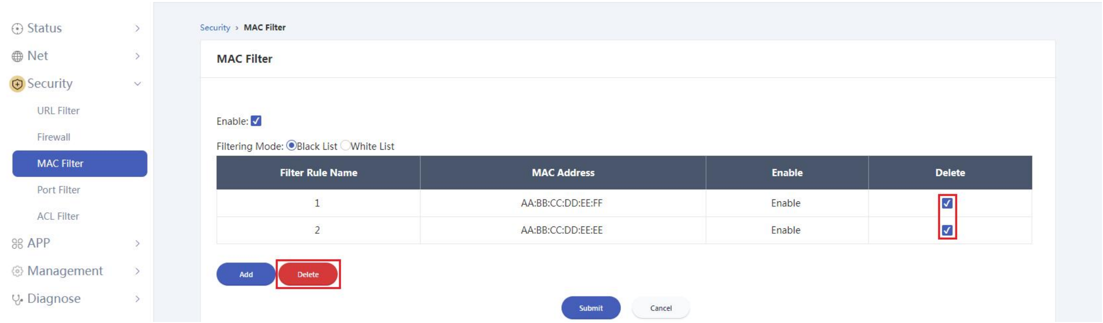
Enable: ☑

Filtering Mode: ● Black List ○ White List

Filter Rule Name	MAC Address	Enable	Delete
1	AA:BB:CC:DD:EE:FF	Enable	□
2	AA:BB:CC:DD:EE:EE	Enable	□

6.2.3.4 Deleting MAC Filter

Select the instance you wish to delete and click the "Delete" button to complete the deletion as illustrated in the figure below.



MAC Filter

Enable: ☑

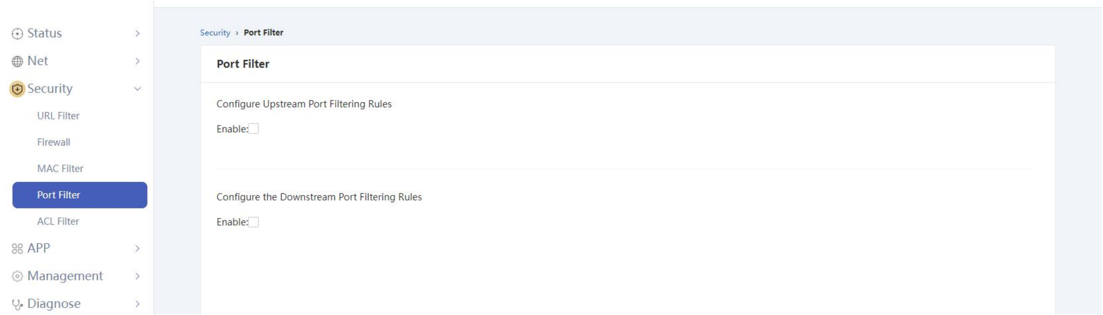
Filtering Mode: ● Black List ○ White List

Filter Rule Name	MAC Address	Enable	Delete
1	AA:BB:CC:DD:EE:FF	Enable	☑
2	AA:BB:CC:DD:EE:EE	Enable	☑

6.2.4 Port Filter

6.2.4.1 Enabling Port Filter

Click on the menu "Security -> Port Filter" as illustrated in the figure below.



Port Filter

Configure Upstream Port Filtering Rules

Enable: □

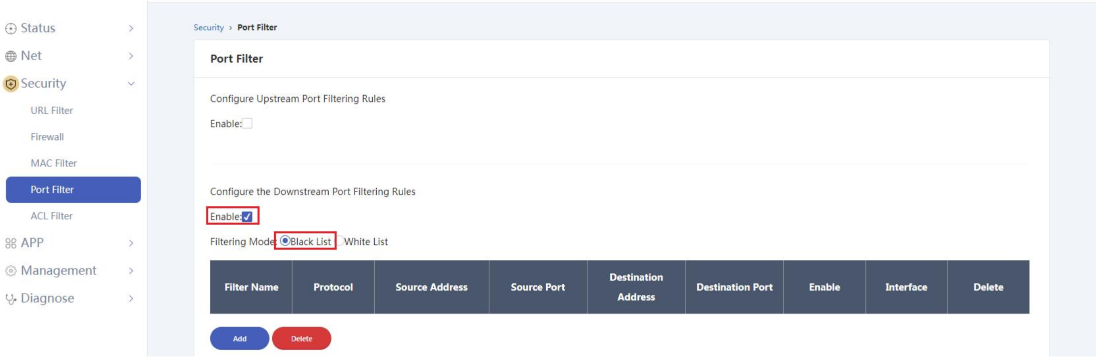
Configure the Downstream Port Filtering Rules

Enable: □

6.2.4.2 Adding Port Filter Blacklist

Blacklist: IP addresses and ports listed here cannot access the device.

Step 1: Check the "Enable" button to configure the port filtering rule for downstream traffic and select "Black List" mode as illustrated in the figure below.



Security › Port Filter

Port Filter

Configure Upstream Port Filtering Rules

Enable:□

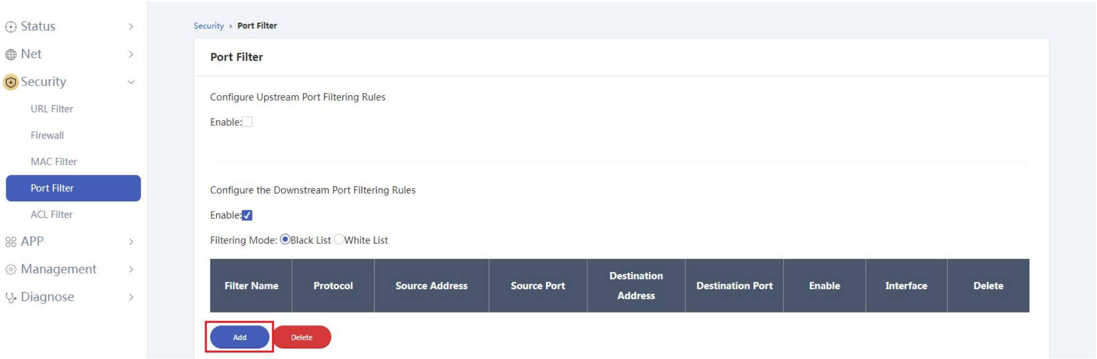
Configure the Downstream Port Filtering Rules

Enable:☑

Filtering Mode: ● Black List ○ White List

Filter Name	Protocol	Source Address	Source Port	Destination Address	Destination Port	Enable	Interface	Delete

Step 2: Click "Add" to add the blacklist as illustrated in the figure below.



Security › Port Filter

Port Filter

Configure Upstream Port Filtering Rules

Enable:□

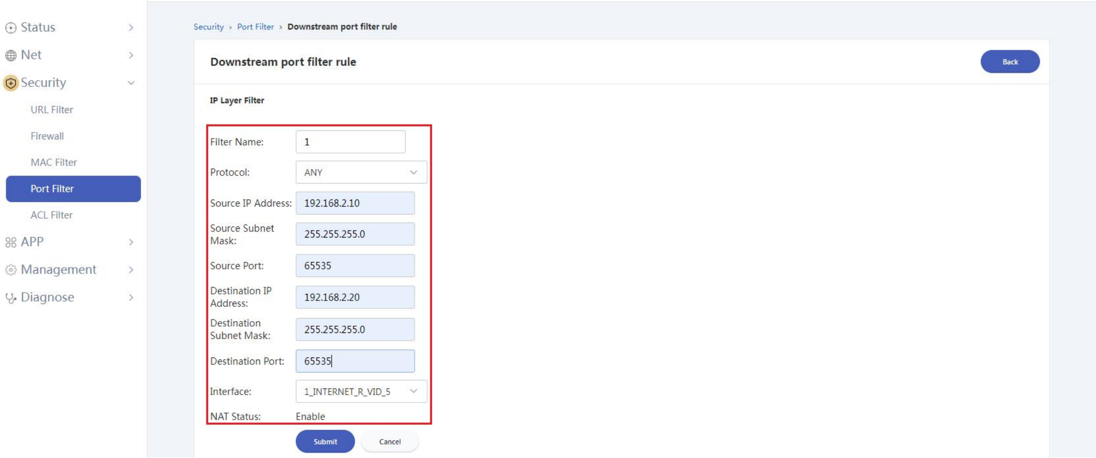
Configure the Downstream Port Filtering Rules

Enable:☑

Filtering Mode: ● Black List ○ White List

Filter Name	Protocol	Source Address	Source Port	Destination Address	Destination Port	Enable	Interface	Delete

Step 3: Configure the relevant parameters as illustrated in the figure below.

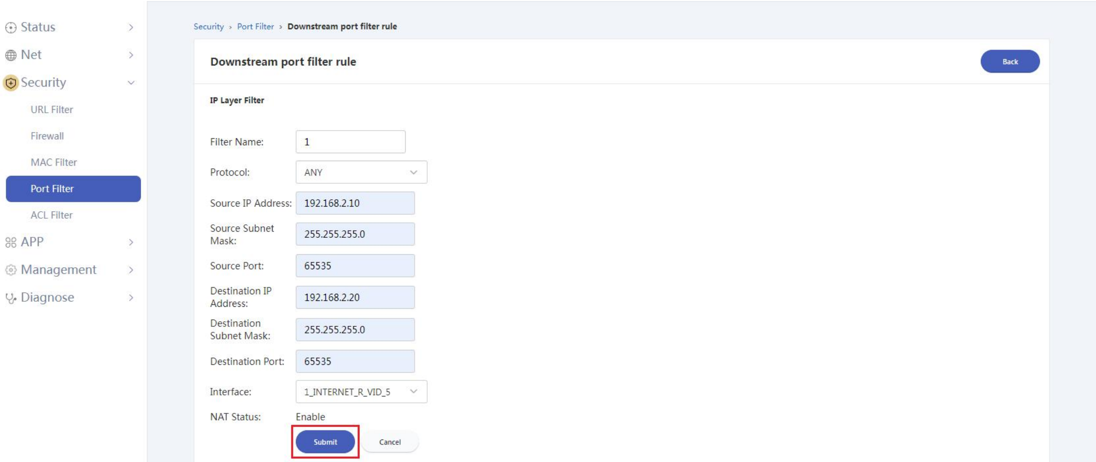


Downstream port filter rule

IP Layer Filter

Filter Name:	1
Protocol:	ANY
Source IP Address:	192.168.2.10
Source Subnet Mask:	255.255.255.0
Source Port:	65535
Destination IP Address:	192.168.2.20
Destination Subnet Mask:	255.255.255.0
Destination Port:	65535
Interface:	1_INTERNET_R_VID_5
NAT Status:	Enable

Step 4: Click "Submit" to complete the settings.



Downstream port filter rule

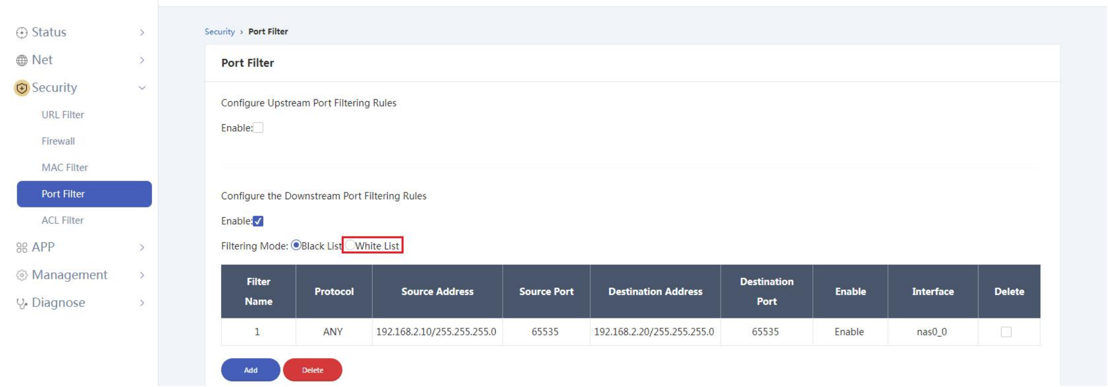
IP Layer Filter

Filter Name:	1
Protocol:	ANY
Source IP Address:	192.168.2.10
Source Subnet Mask:	255.255.255.0
Source Port:	65535
Destination IP Address:	192.168.2.20
Destination Subnet Mask:	255.255.255.0
Destination Port:	65535
Interface:	1_INTERNET_R_VID_5
NAT Status:	Enable

6.2.4.3 Adding Port Filter Whitelist

Whitelist: Only IP addresses and ports listed here can access the device.

Step 1: Select "White List" to enter whitelist mode as illustrated in the figure below.



Security › Port Filter

Port Filter

Configure Upstream Port Filtering Rules

Enable:□

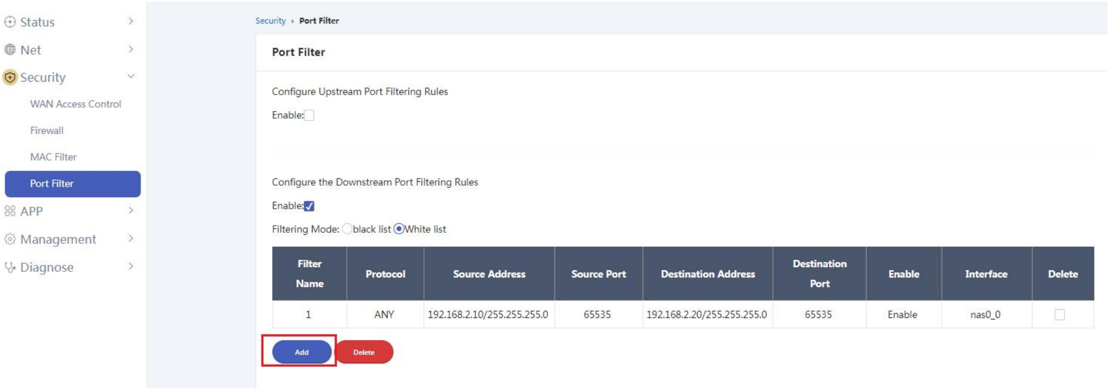
Configure the Downstream Port Filtering Rules

Enable:☑

Filtering Mode: ●Black List ○White List

Filter Name	Protocol	Source Address	Source Port	Destination Address	Destination Port	Enable	Interface	Delete
1	ANY	192.168.2.10/255.255.255.0	65535	192.168.2.20/255.255.255.0	65535	Enable	nas0_0	□

Step 2: Click "Add" to add the whitelist as illustrated in the figure below.



Security › Port Filter

Port Filter

Configure Upstream Port Filtering Rules

Enable:□

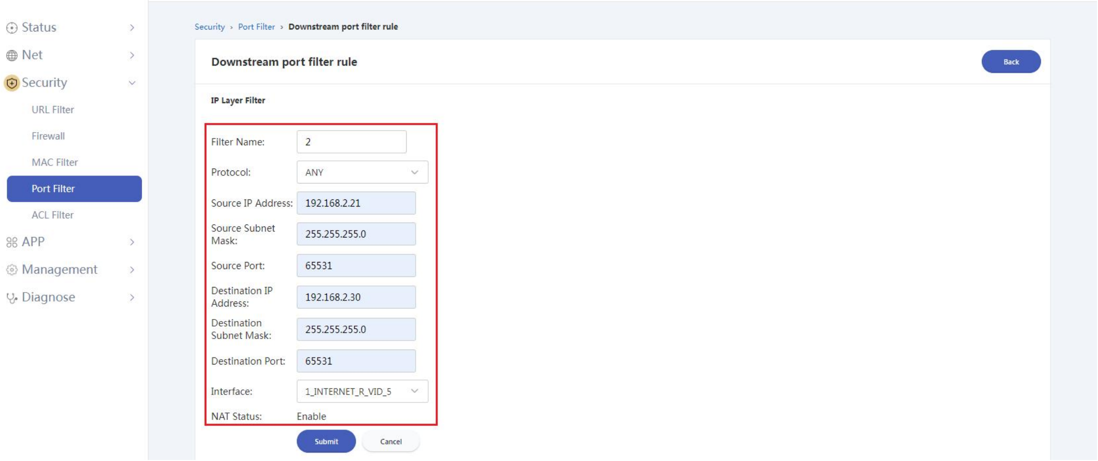
Configure the Downstream Port Filtering Rules

Enable:☑

Filtering Mode: ○black list ●White list

Filter Name	Protocol	Source Address	Source Port	Destination Address	Destination Port	Enable	Interface	Delete
1	ANY	192.168.2.10/255.255.255.0	65535	192.168.2.20/255.255.255.0	65535	Enable	nas0_0	□

Step 3: Configure the relevant parameters as illustrated in the figure below.



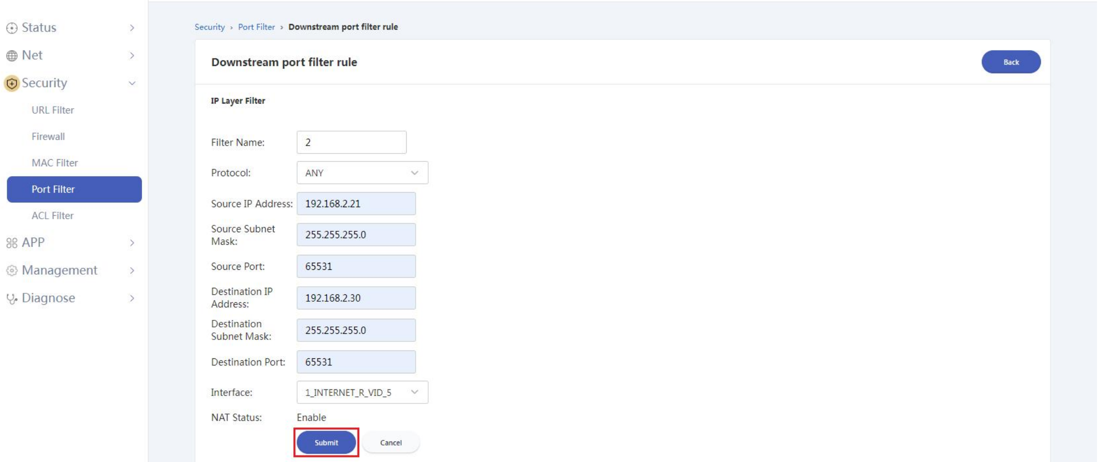
Security › Port Filter › Downstream port filter rule

Downstream port filter rule

IP Layer Filter

Filter Name:	2
Protocol:	ANY
Source IP Address:	192.168.2.21
Source Subnet Mask:	255.255.255.0
Source Port:	65531
Destination IP Address:	192.168.2.30
Destination Subnet Mask:	255.255.255.0
Destination Port:	65531
Interface:	1_INTERNET_R_VID_5
NAT Status:	Enable

Step 4: Click "Submit" to complete the settings.



Security › Port Filter › Downstream port filter rule

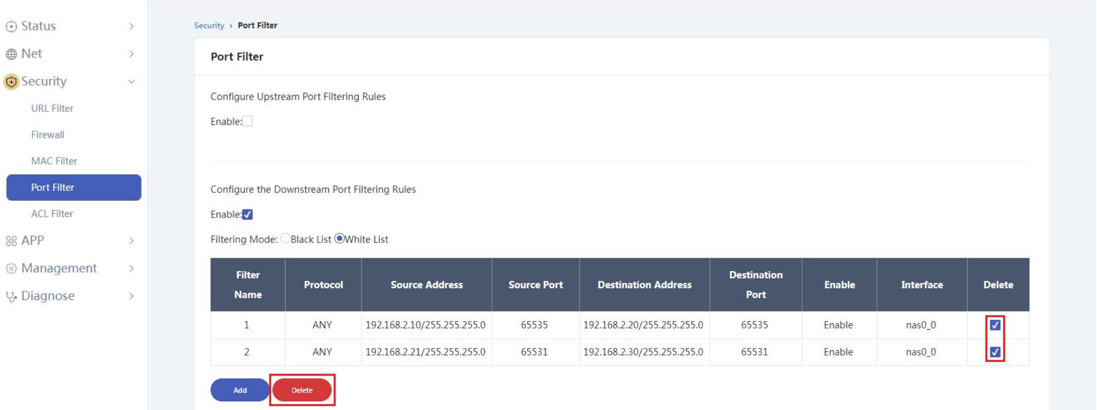
Downstream port filter rule

IP Layer Filter

Filter Name:	2
Protocol:	ANY
Source IP Address:	192.168.2.21
Source Subnet Mask:	255.255.255.0
Source Port:	65531
Destination IP Address:	192.168.2.30
Destination Subnet Mask:	255.255.255.0
Destination Port:	65531
Interface:	1_INTERNET_R_VID_5
NAT Status:	Enable

6.2.4.4 Deleting Port Filter

Select the entry you wish to delete and click the "Delete" button to complete the deletion as illustrated in the figure below.



Port Filter

Configure Upstream Port Filtering Rules

Enable: □

Configure the Downstream Port Filtering Rules

Enable: ☑

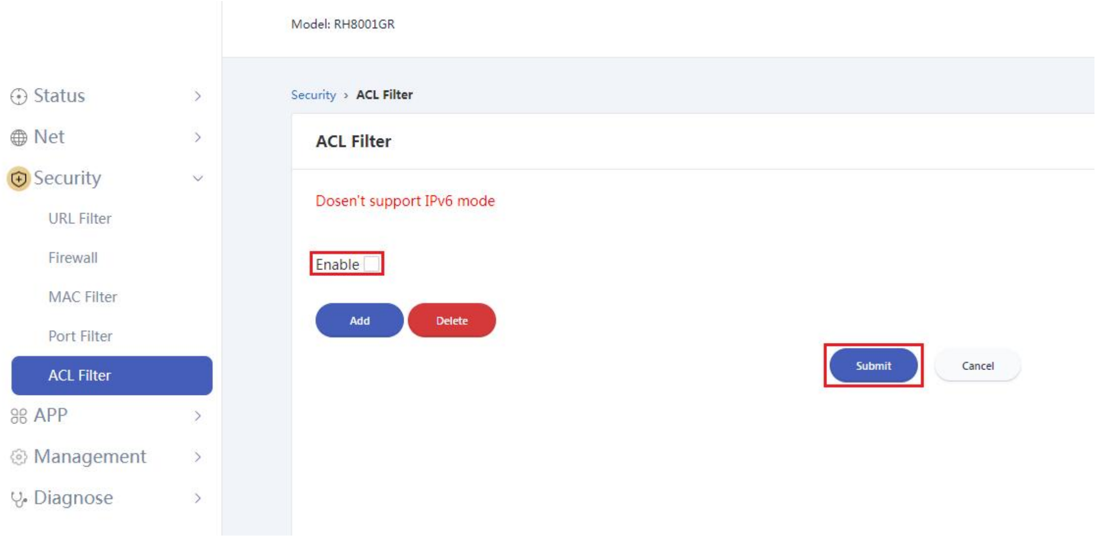
Filtering Mode: ○ Black List ● White List

Filter Name	Protocol	Source Address	Source Port	Destination Address	Destination Port	Enable	Interface	Delete
1	ANY	192.168.2.10/255.255.255.0	65535	192.168.2.20/255.255.255.0	65535	Enable	nas0_0	☑
2	ANY	192.168.2.21/255.255.255.0	65531	192.168.2.30/255.255.255.0	65531	Enable	nas0_0	☑

6.2.5 ACL Filter

6.2.5.1 Enabling ACL Filter

Click on the menu "Security -> ACL Filter". Check "Enable" and click the "Submit" button as illustrated in the figure below.IPv6 mode is currently not supported.


Model: RH8001GR

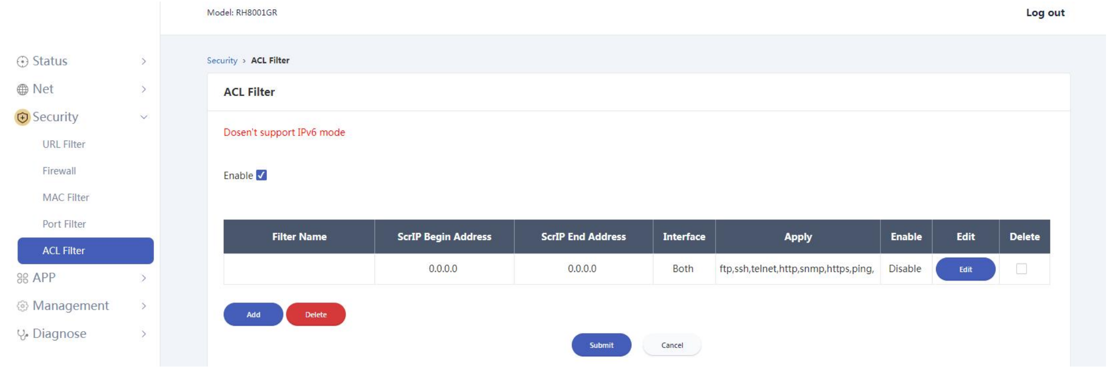
ACL Filter

Dosen't support IPv6 mode

Enable □

6.2.5.2 Adding ACL Instance

By default, a pre-configured ACL exists on the ACL configuration page, allowing all IPs and protocols. It is disabled by default. You can modify this ACL according to your specific requirements.



Model: RH8001GR

Security › ACL Filter

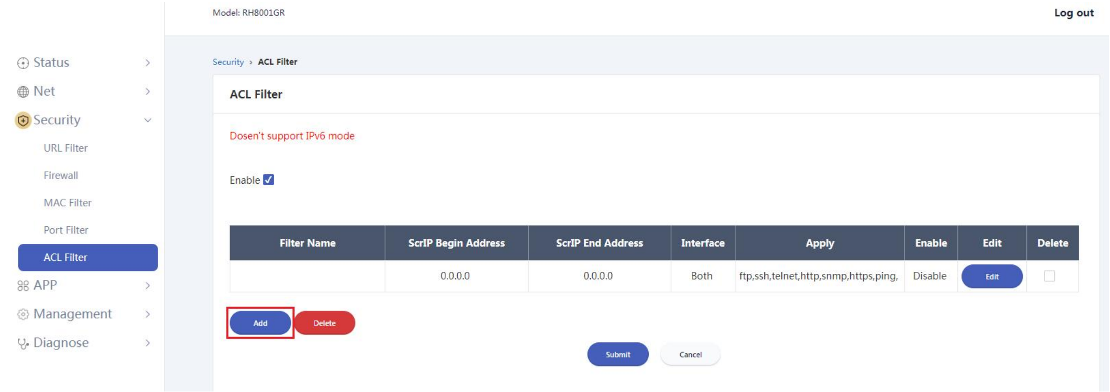
ACL Filter

Dosen't support IPv6 mode

Enable ☑

Filter Name	ScrIP Begin Address	ScrIP End Address	Interface	Apply	Enable	Edit	Delete
	0.0.0.0	0.0.0.0	Both	ftp,ssh,telnet,http,snmp,https,ping,	Disable	Edit	□

Step 1: Click the "Add" button to create an ACL, as shown below.



Model: RH8001GR

Security › ACL Filter

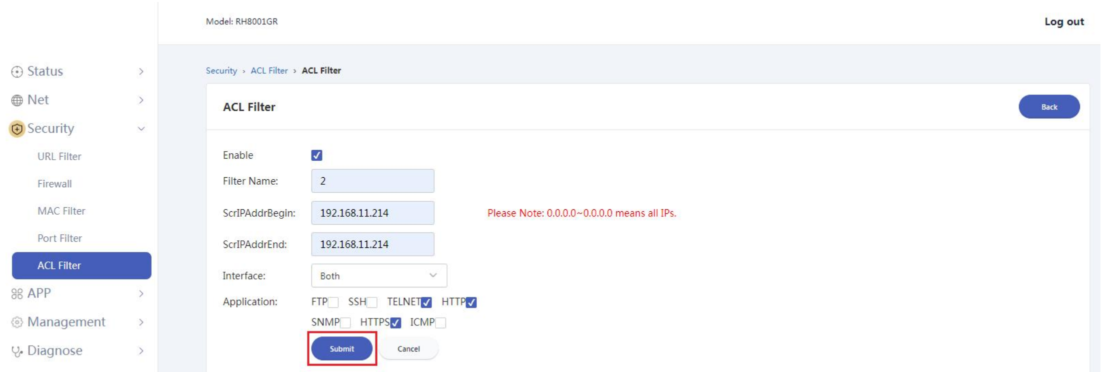
ACL Filter

Dosen't support IPv6 mode

Enable ☑

Filter Name	ScrIP Begin Address	ScrIP End Address	Interface	Apply	Enable	Edit	Delete
	0.0.0.0	0.0.0.0	Both	ftp,ssh,telnet,http,snmp,https,ping,	Disable	Edit	□

Step 2: Fill in the Filter Name, ScrIPAddrBegin, and ScrIPAddrEnd. Select the corresponding Interface and check the required Applications. Click the "Add" button as illustrated in the figure below.



Model: RH8001GR

Security › ACL Filter › ACL Filter

ACL Filter

Enable ☑

Filter Name: 2

ScrIPAddrBegin: 192.168.11.214

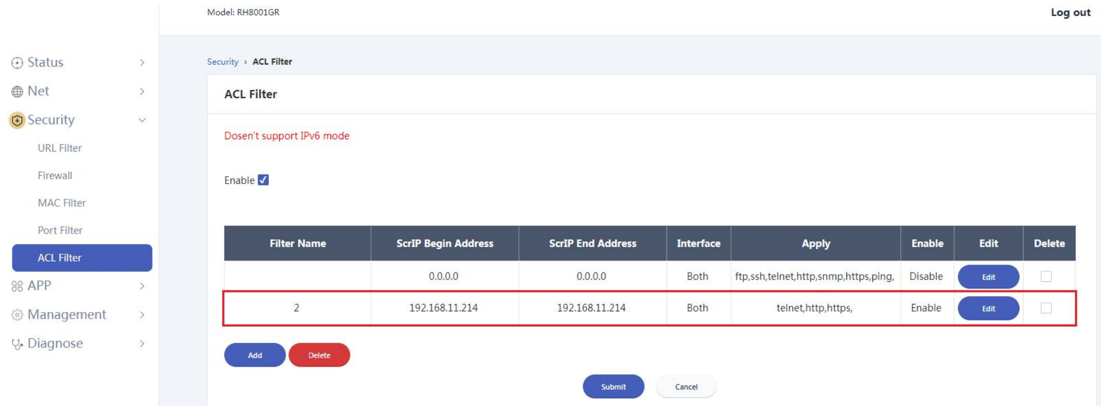
Please Note: 0.0.0.0~0.0.0.0 means all IPs.

ScrIPAddrEnd: 192.168.11.214

Interface: Both

Application: FTP□ SSH□ TELNET☑ HTTP☑ SNMP□ HTTPS☑ ICMP□

After the addition is completed, the ACL status is as shown below. Currently, only the source IP:192.168.11.214 is allowed to access this device.



Model: RH8001GR

Security › ACL Filter

ACL Filter

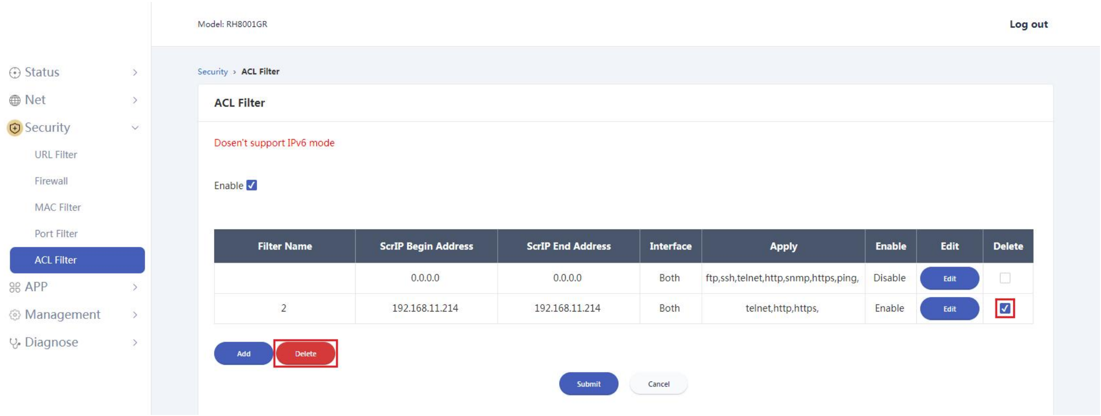
Dosen't support IPv6 mode

Enable ☑

Filter Name	ScrIP Begin Address	ScrIP End Address	Interface	Apply	Enable	Edit	Delete
	0.0.0.0	0.0.0.0	Both	ftp,ssh,telnet,http,snmp,https,ping,	Disable	Edit	□
2	192.168.11.214	192.168.11.214	Both	telnet,http,https,	Enable	Edit	□

6.2.5.3 Deleting ACL Instance

Select the ACL you want to delete and click the "Delete" button to complete the deletion as illustrated in the figure below.



ACL Filter

Dosen't support IPv6 mode

Enable ☑

Filter Name	ScrIP Begin Address	ScrIP End Address	Interface	Apply	Enable	Edit	Delete
	0.0.0.0	0.0.0.0	Both	ftp,ssh,telnet,http,snmp,https,ping,	Disable	Edit	□
2	192.168.11.214	192.168.11.214	Both	telnet,http,https,	Enable	Edit	☑

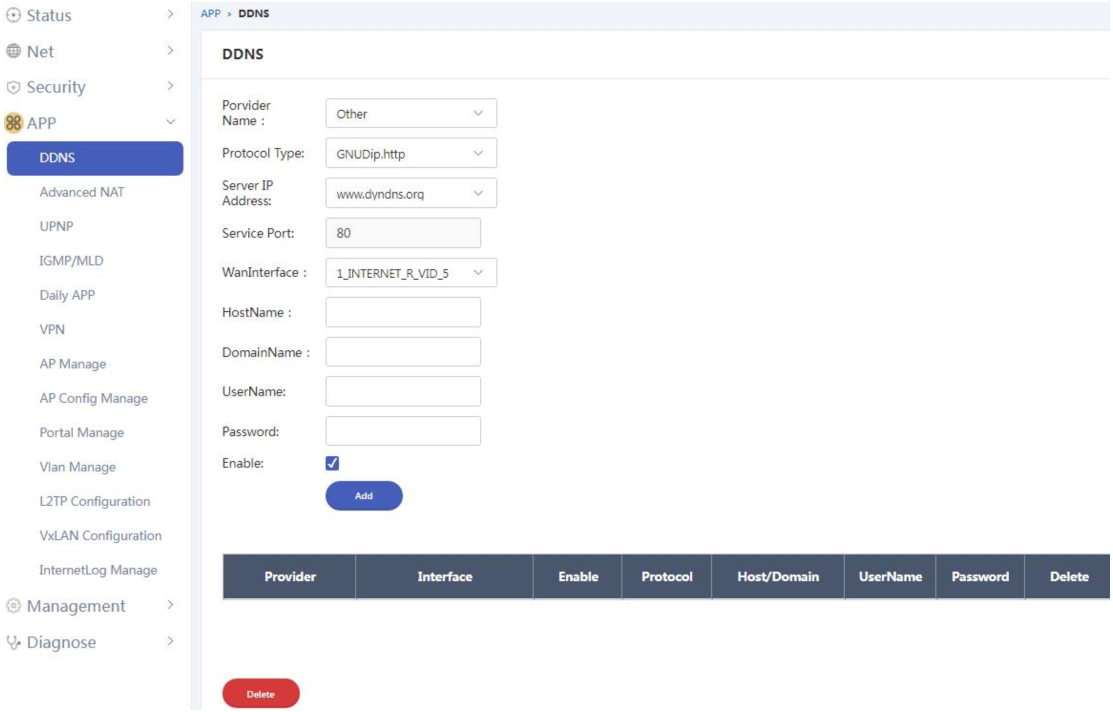
6.3 APP Setting

6.3.1 DDNS

DDNS, whose main function is to realize the resolution between fixed domain names and dynamic IP addresses.If the IP address of the WAN port of the terminal is dynamically obtained, this function allows other hosts on the Internet to access your terminal or virtual server with a fixed domain name.

DDNS function. For users who use dynamic IP addresses, after getting a new IP address every time they go online, the dynamic domain name software built in the terminal will send the IP address to the dynamic domain name resolution server provided by the DDNS service provider, and update the domain name parse database. When other users on the Internet need to access this domain name, the dynamic domain name resolution server will return the correct IP address. This function enables most users who do not use fixed IP addresses to build their own service networks economically and efficiently.

Click on the menu "APP -> DDNS" to enter the DDNS configuration page as illustrated in the figure below.



DDNS

Porvider Name : Other

Protocol Type: GNUDip.http

Server IP Address: www.dyndns.org

Service Port: 80

WanInterface : 1_INTERNET_R_VID_5

HostName :

DomainName :

UserName:

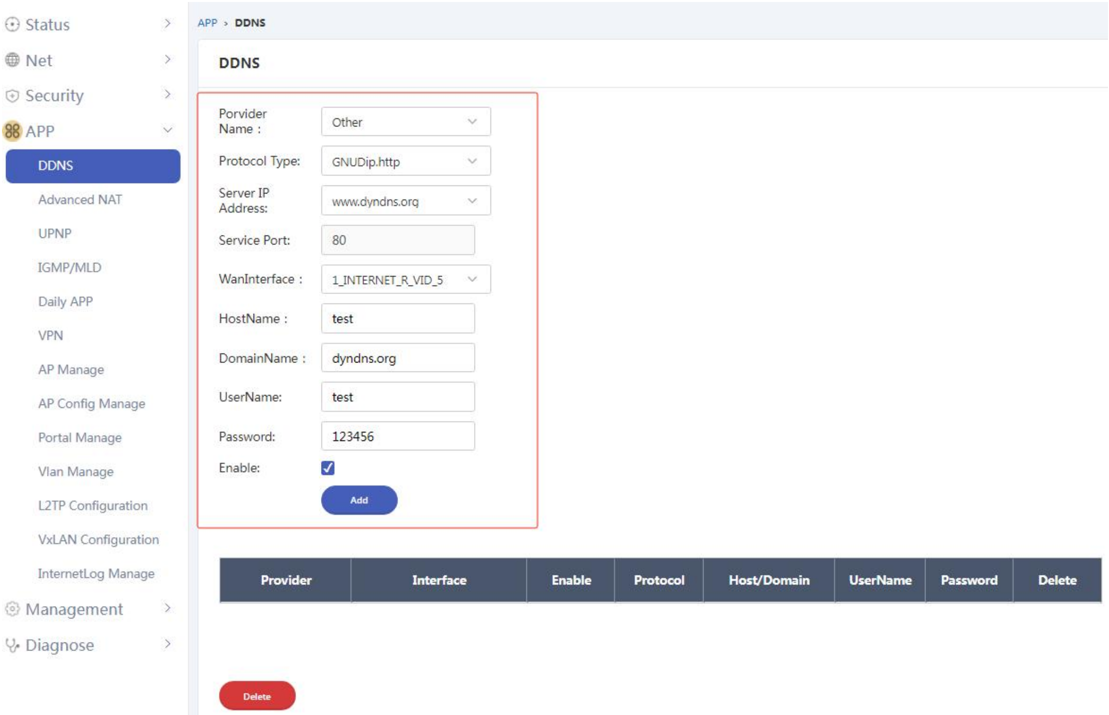
Password:

Enable: ☑

Provider	Interface	Enable	Protocol	Host/Domain	UserName	Password	Delete

6.3.1.1 Adding DDNS Instance

Step 1: Correctly configure the service provider, Protocol Type,Service IP Address, HostName, Domain Name, UserName, and Password, then click the "Add" button as illustrated in the figure below.



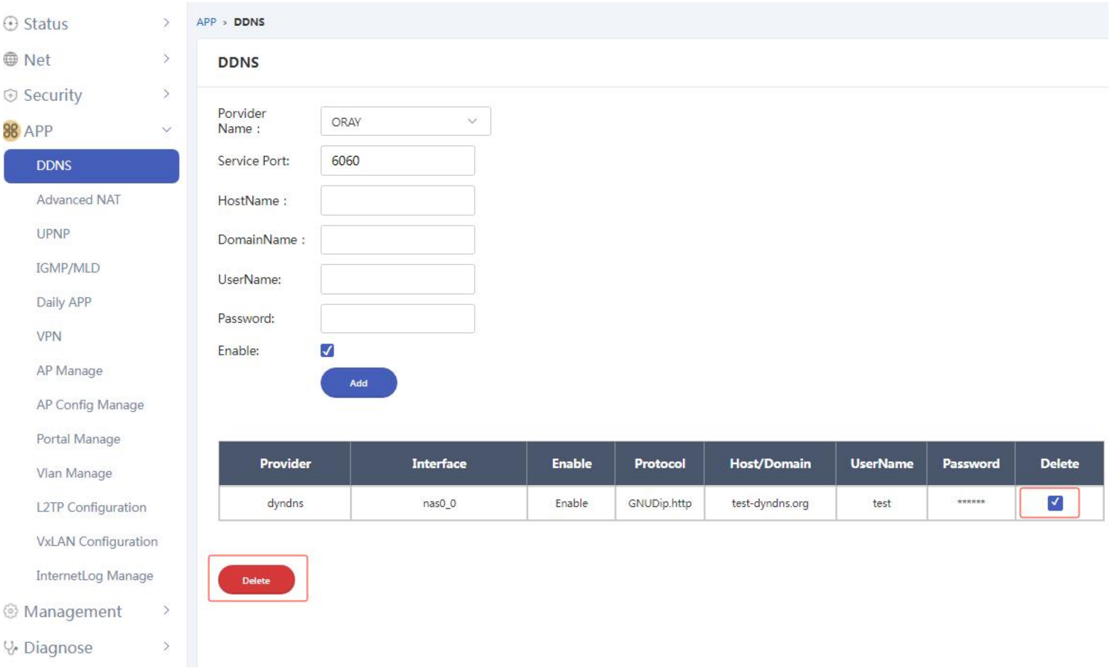
DDNS

Porvider Name :	Other
Protocol Type:	GNUDip.http
Server IP Address:	www.dyndns.org
Service Port:	80
WanInterface :	1_INTERNET_R_VID_5
HostName :	test
DomainName :	dyndns.org
UserName:	test
Password:	123456
Enable:	☑

Provider	Interface	Enable	Protocol	Host/Domain	UserName	Password	Delete

6.3.1.2 Deleting DDNS Instance

Select the instance you wish to delete and click the "Delete" button to complete the deletion as illustrated in the figure below.



DDNS

Porvider Name : ORAY

Service Port: 6060

HostName :

DomainName :

UserName:

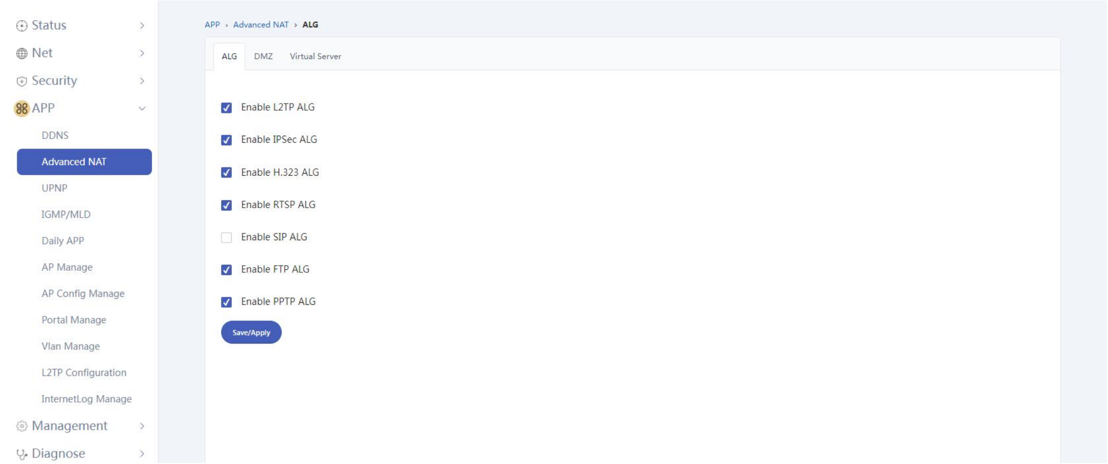
Password:

Enable: ☑

Provider	Interface	Enable	Protocol	Host/Domain	UserName	Password	Delete
dyndns	nas0_0	Enable	GNUDip.http	test-dyndns.org	test	******	☑

6.3.2 Advanced NAT

Click on the menu "APP -> Advanced NAT" to enter the advanced NAT configuration page as illustrated in the figure below.



☑ Enable L2TP ALG

☑ Enable IPSec ALG

☑ Enable H.323 ALG

☑ Enable RTSP ALG

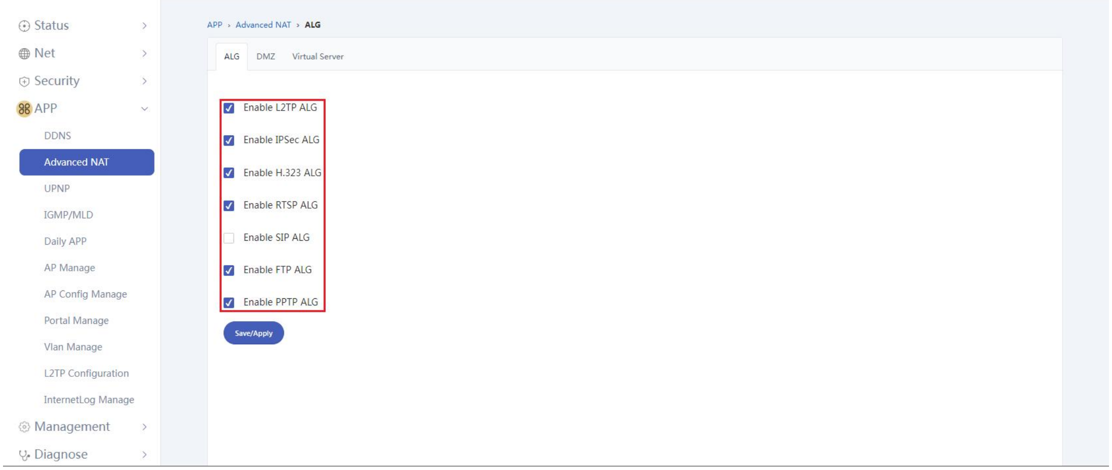
□ Enable SIP ALG

☑ Enable FTP ALG

☑ Enable PPTP ALG

6.3.2.1 Enable/Disable ALG Function

Configure the ALG function as illustrated in the figure below.



☑ Enable L2TP ALG

☑ Enable IPSec ALG

☑ Enable H.323 ALG

☑ Enable RTSP ALG

□ Enable SIP ALG

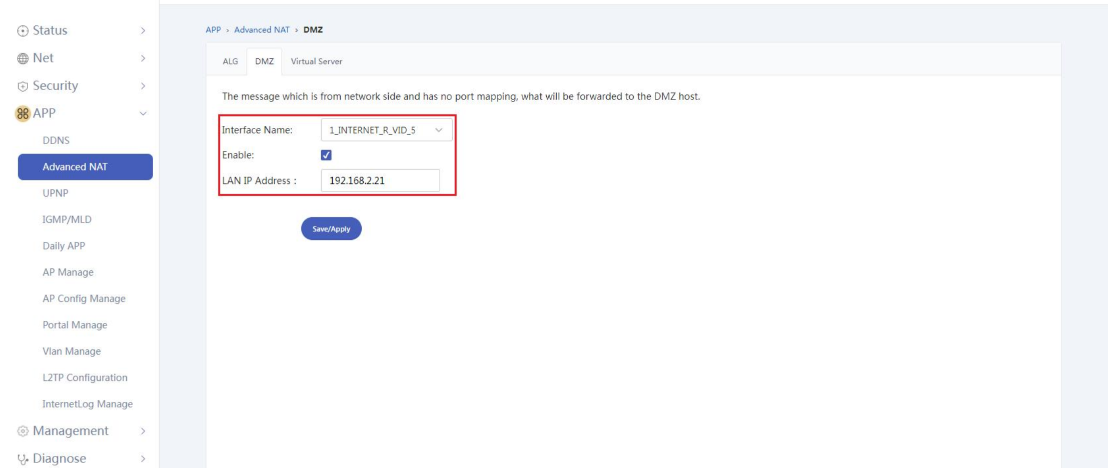
☑ Enable FTP ALG

☑ Enable PPTP ALG

6.3.2.2 Configure DMZ Function

In certain special circumstances, we need a computer within the LAN to be fully exposed to the WAN to enable bidirectional communication. In this case, the computer can be set as a DMZ host. The setup steps are as follows:

Step 1: Configure the DMZ parameters and click "Save -> Apply" after completion as illustrated in the figure below.



The message which is from network side and has no port mapping, what will be forwarded to the DMZ host.

Interface Name: 1_INTERNET_R_VID_5

Enable: ☑

LAN IP Address : 192.168.2.21

6.3.2.3 Virtual Server Configuration

Port forwarding is essentially a type of NAT address translation that translates public addresses into private addresses.

Internal IP: The IP address of the computer within the LAN serving as a server.

Internal Port: The service port provided by the WAN end, i.e., the port the router offers to the WAN.

Protocol: Select the type of protocol packet, options include TCP, UDP, or TCP/UDP.

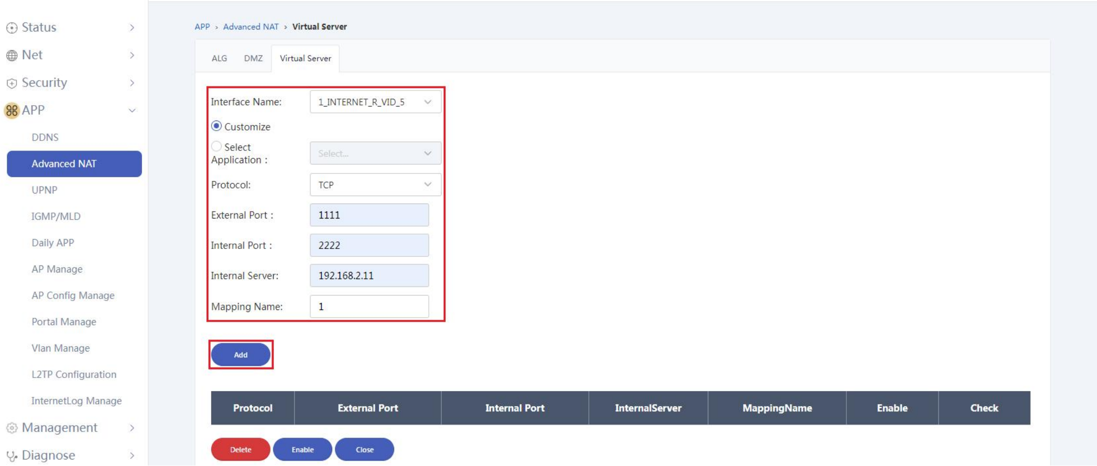
Remote IP: The external IP address used to access the server; 0.0.0.0 means any external IP can access it; specifying a single IP, such as 192.168.10.12, restricts access to only that IP.

External Port: The port used to access the server.

Enable: This entry's settings will take effect only if this option is selected.

Note: It's best to set ports other than 80, as setting the service port to 80 may conflict with the web port, causing the virtual server not to work properly.

Step 1: Configure the relevant parameters and click "Add" as illustrated in the figure below.



Interface Name: 1_INTERNET_R_VID_5

● Customize

○ Select Application : Select...

Protocol: TCP

External Port : 1111

Internal Port : 2222

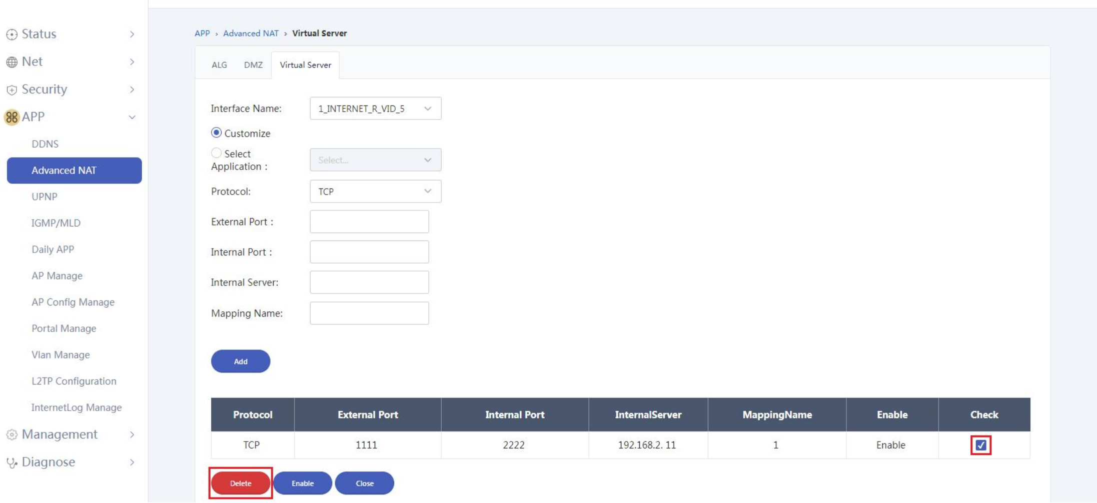
Internal Server: 192.168.2.11

Mapping Name: 1

Protocol	External Port	Internal Port	InternalServer	MappingName	Enable	Check

6.3.2.4 Deleting Virtual Server Configuration

Select the instance you wish to delete and click the "Delete" button to complete the deletion as illustrated in the figure below.



Interface Name: 1_INTERNET_R_VID_5

● Customize

○ Select Application : Select...

Protocol: TCP

External Port :

Internal Port :

Internal Server:

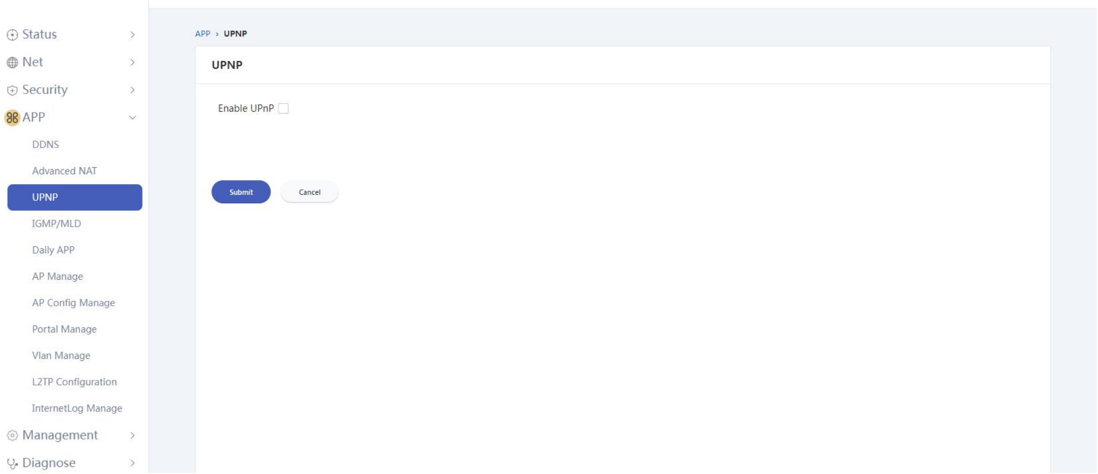
Mapping Name:

Protocol	External Port	Internal Port	InternalServer	MappingName	Enable	Check
TCP	1111	2222	192.168.2. 11	1	Enable	☑

6.3.3 UPnP

The UPnP (Universal Plug and Play) protocol can implement automatic port mapping. Unlike manually configured port mapping, the UPnP protocol automatically recognizes user devices and automatically opens ports or certain programs to communicate.

Click on the menu "APP -> UPNP" to enter the port forwarding configuration page as illustrated in the figure below.

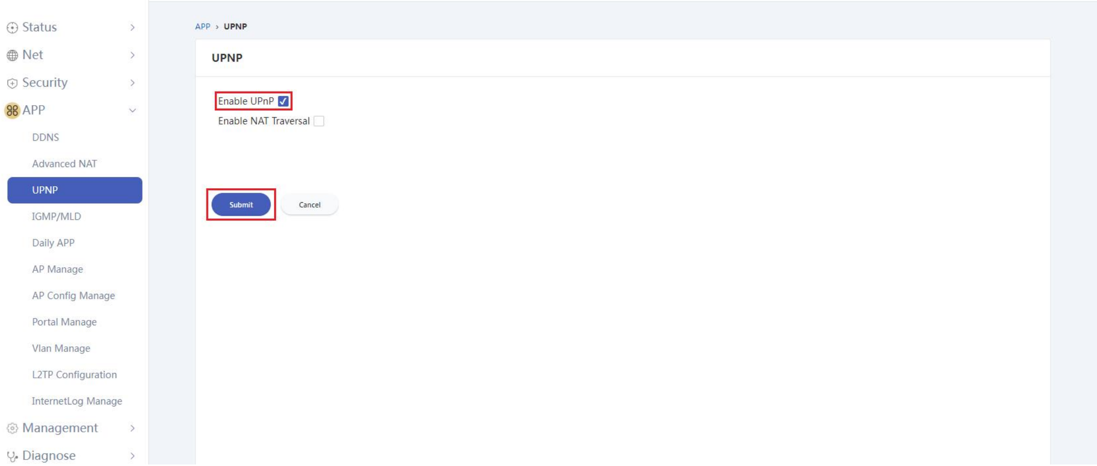


Enable UPnP □

6.3.3.1 UPNP Configuration Example

Relying on the UPNP (Universal Plug and Play) protocol, hosts within the LAN can request the router to perform specific port translations, allowing external hosts to access resources on internal hosts when needed.

Step 1: Enable UPNP as illustrated in the figure below.

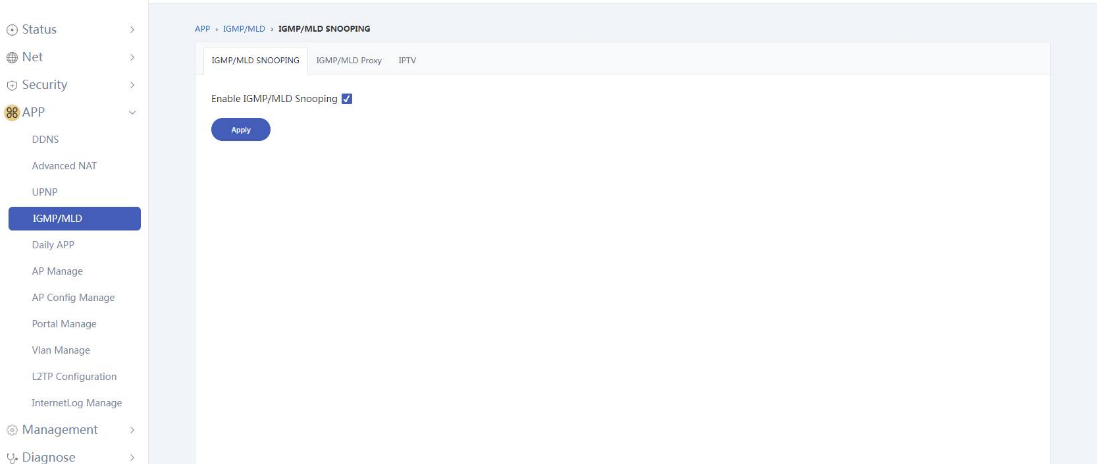


Enable UPnP ☑

Enable NAT Traversal □

6.3.4 IGMP/MLD

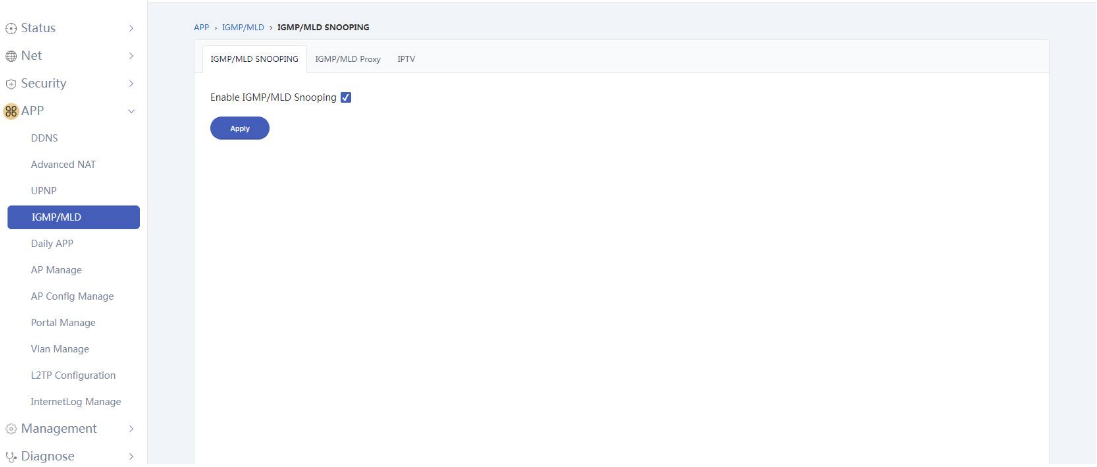
By default, IGMP/MLD Snooping and Proxy are enabled. Click on the menu "APP -> IGMP/MLD" to enter the IGMP/MLD configuration page as illustrated in the figure below.



Enable IGMP/MLD Snooping ☑

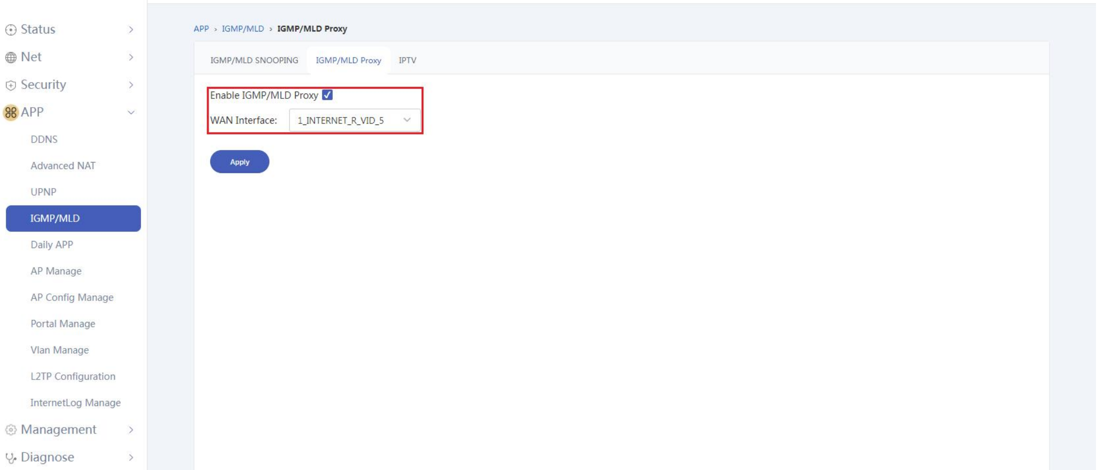
6.3.4.1 IGMP/MLD Snooping Configuration

The IGMP/MLD Snooping function is enabled by default.



Enable IGMP/MLD Snooping ☑

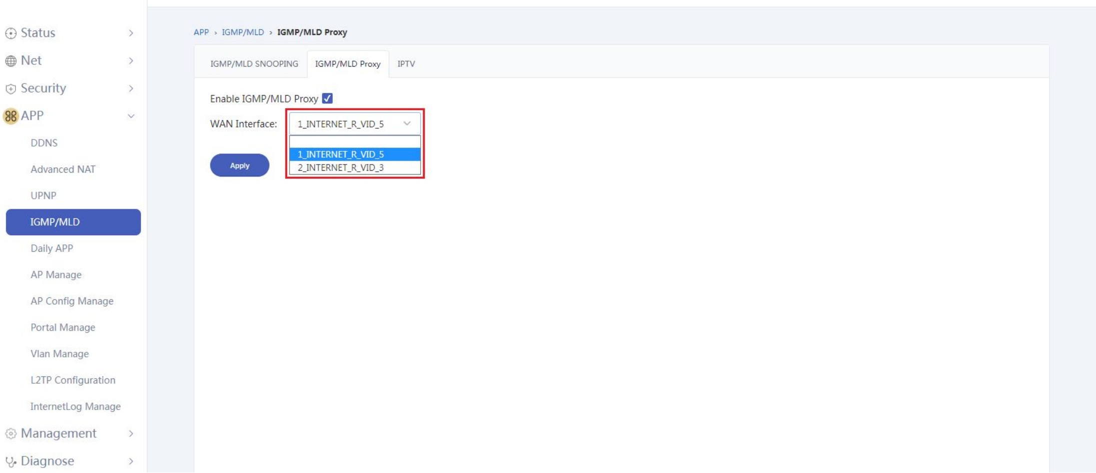
6.3.4.2 IGMP/MLD Proxy Configuration



Enable IGMP/MLD Proxy ☑

WAN Interface: 1_INTERNET_R_VID_5

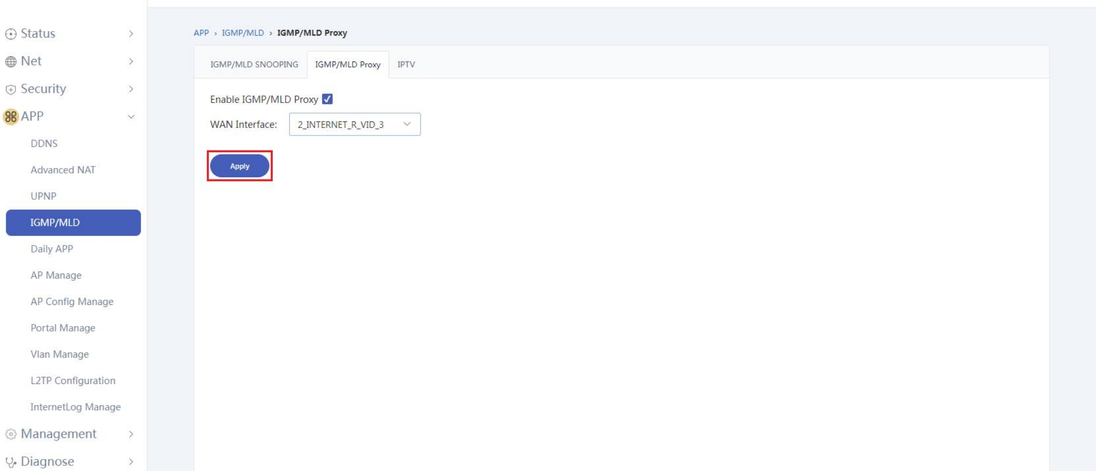
Step 1: Select the WAN interface where you want to enable the IGMP/MLD Proxy function as illustrated in the figure below.



Enable IGMP/MLD Proxy ☑

WAN Interface: 1_INTERNET_R_VID_5

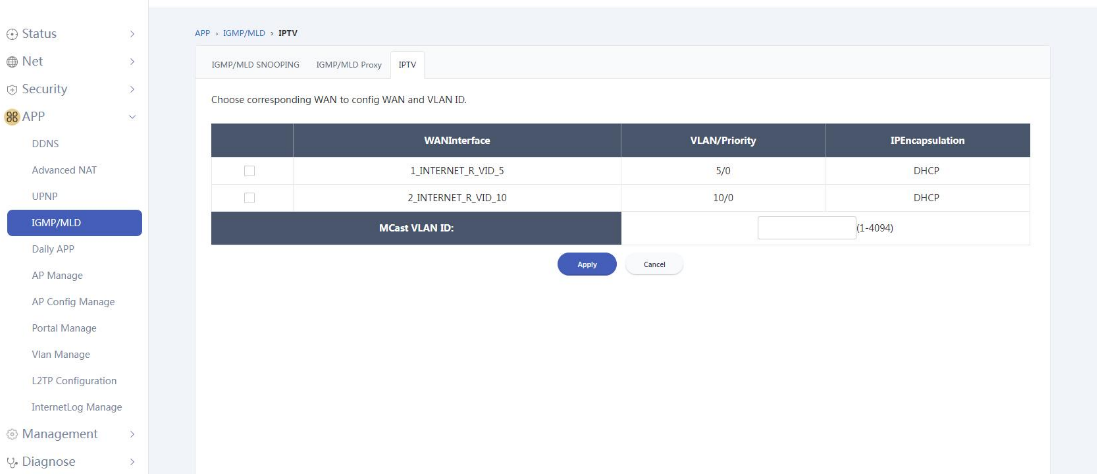
Step 2: Click "Apply" to complete the configuration as illustrated in the figure below.



Enable IGMP/MLD Proxy ☑

WAN Interface: 2_INTERNET_R_VID_3

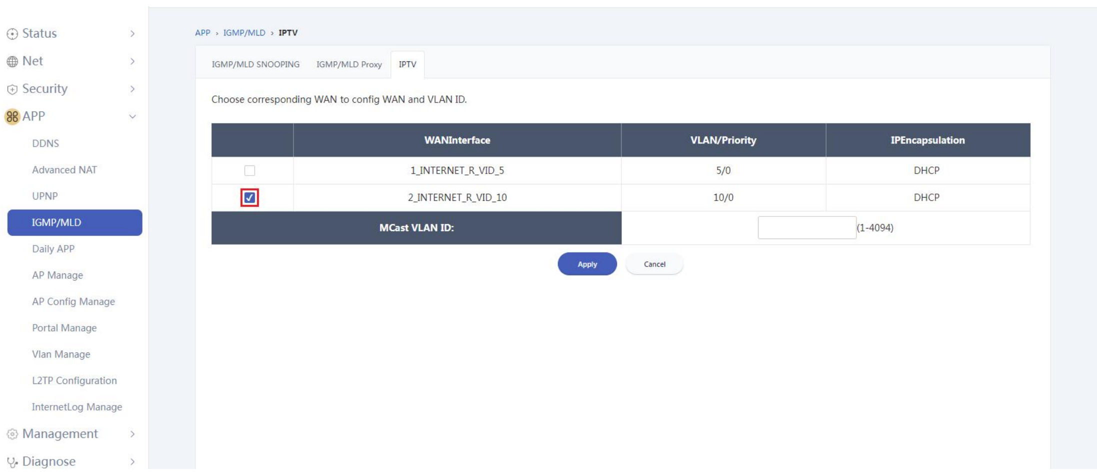
6.3.4.3 IPTV Configuration



Choose corresponding WAN to config WAN and VLAN ID.

	WANInterface	VLAN/Priority	IPEncapsulation
□	1_INTERNET_R_VID_5	5/0	DHCP
□	2_INTERNET_R_VID_10	10/0	DHCP
MCast VLAN ID:		(1-4094)	

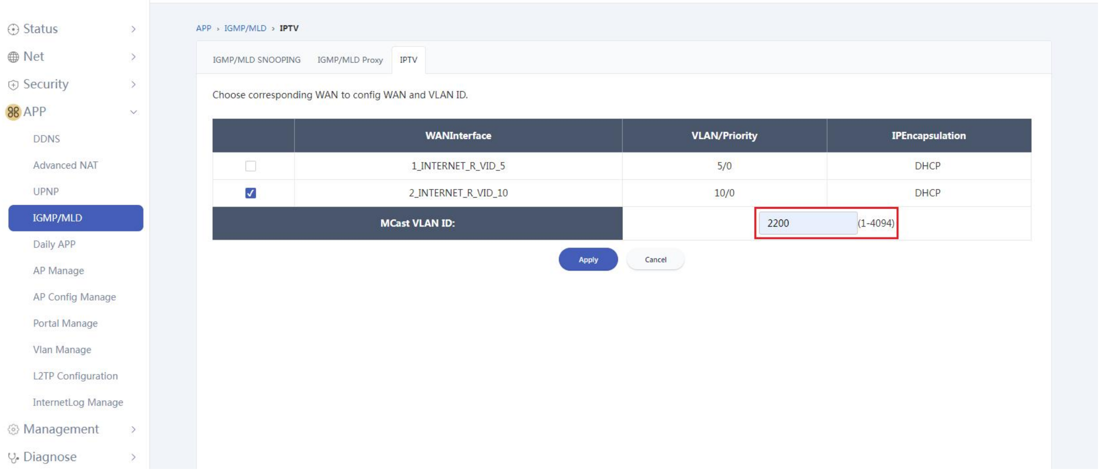
Step 1: Check the WAN port that requires multicast VLAN configuration as illustrated in the figure below.



Choose corresponding WAN to config WAN and VLAN ID.

	WANInterface	VLAN/Priority	IPEncapsulation
□	1_INTERNET_R_VID_5	5/0	DHCP
☑	2_INTERNET_R_VID_10	10/0	DHCP
MCast VLAN ID:		(1-4094)	

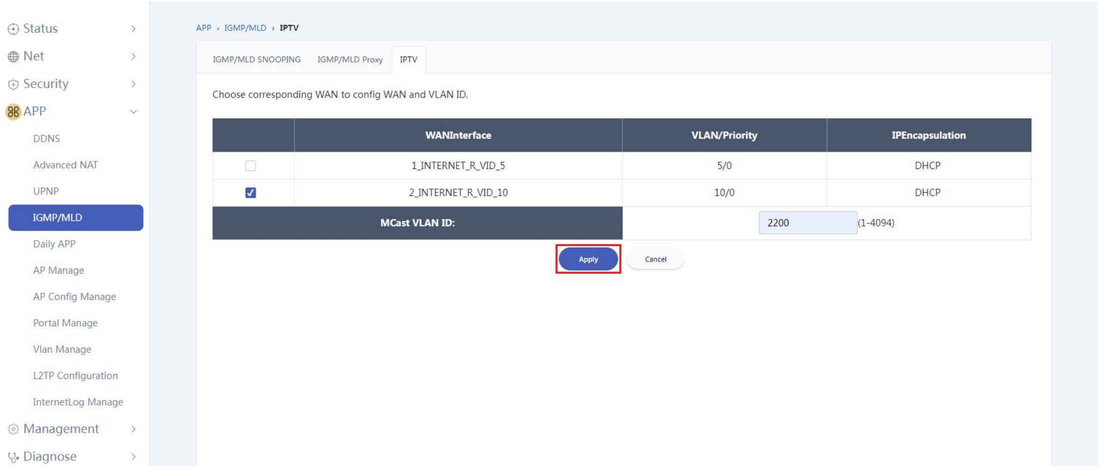
Step 2: Configure the multicast VLAN ID as illustrated in the figure below.



Choose corresponding WAN to config WAN and VLAN ID.

	WANInterface	VLAN/Priority	IPEncapsulation
□	1_INTERNET_R_VID_5	5/0	DHCP
☑	2_INTERNET_R_VID_10	10/0	DHCP
MCast VLAN ID:		2200 (1-4094)	

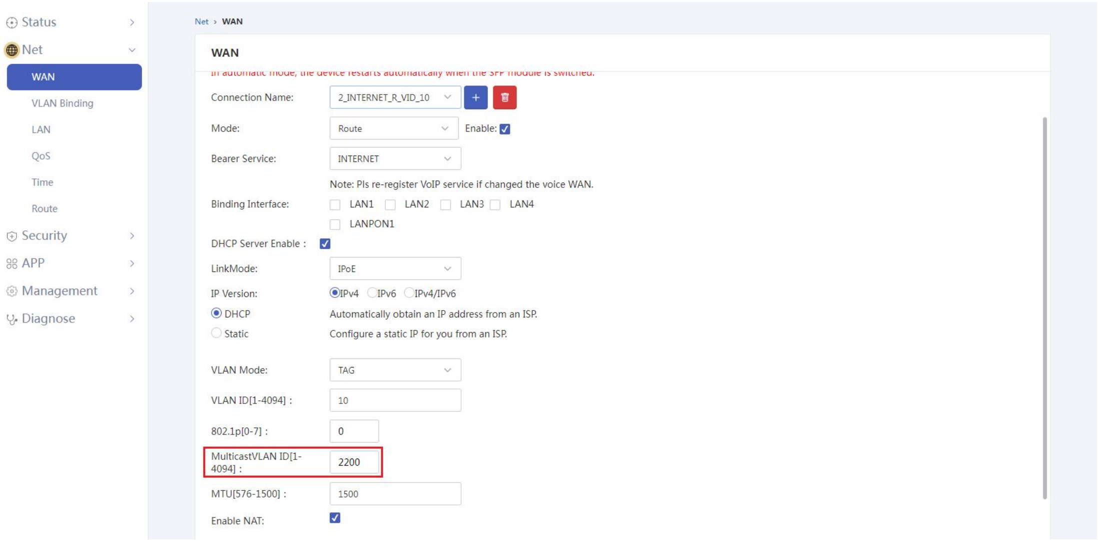
Step 3: Click "Apply" to complete the configuration.



Choose corresponding WAN to config WAN and VLAN ID.

	WANInterface	VLAN/Priority	IPEncapsulation
□	1_INTERNET_R_VID_5	5/0	DHCP
☑	2_INTERNET_R_VID_10	10/0	DHCP
MCast VLAN ID:		2200 (1-4094)	

The multicast VLAN configuration will be synchronized with the corresponding WAN (select the WAN that requires multicast VLAN configuration).



WAN

In automatic mode, the device restarts automatically when the SFP module is switched.

Connection Name: 2_INTERNET_R_VID_10

Mode: Route Enable: ☑

Bearer Service: INTERNET

Note: Pls re-register VoIP service if changed the voice WAN.

Binding Interface: □ LAN1 □ LAN2 □ LAN3 □ LAN4 □ LANPON1

DHCP Server Enable : ☑

LinkMode: IPoE

IP Version: ● IPv4 ○ IPv6 ○ IPv4/IPv6

● DHCP Automatically obtain an IP address from an ISP.

○ Static Configure a static IP for you from an ISP.

VLAN Mode: TAG

VLAN ID[1-4094] : 10

802.1p[0-7] : 0

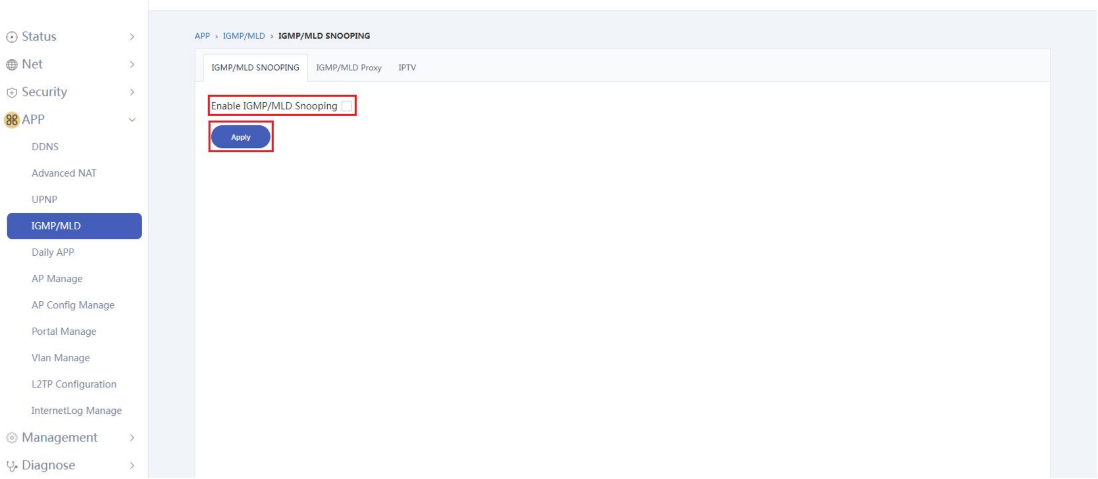
MulticastVLAN ID[1-4094] : 2200

MTU[576-1500] : 1500

Enable NAT: ☑

6.3.4.4 Disabling IGMP/MLD Snooping Functions

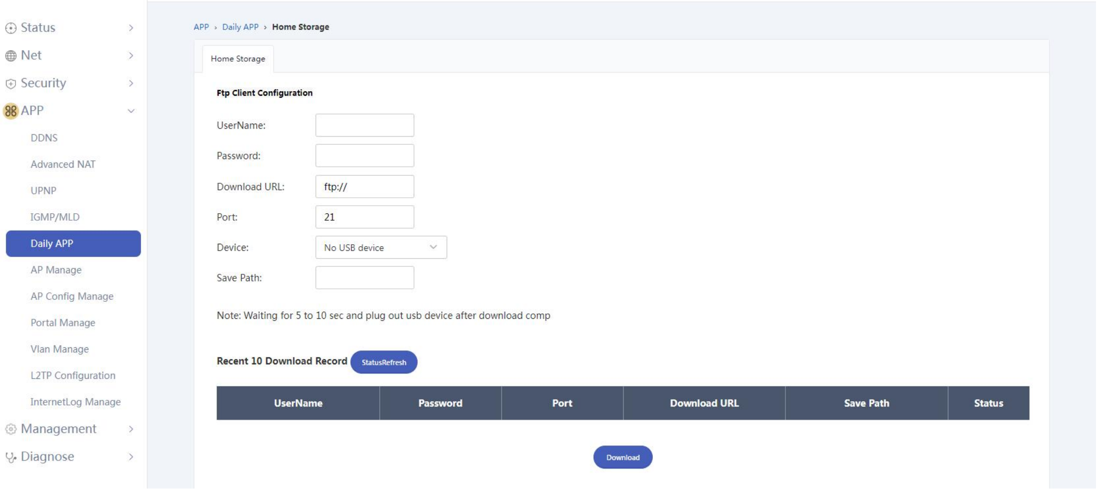
Uncheck the box and click "Apply" to disable the IGMP/MLD Snooping function as illustrated in the figure below.



Enable IGMP/MLD Snooping □

6.3.5 Daily APP

Click on the menu "APP -> Daily APP" to enter the daily applications page as illustrated in the figure below. FTP download to USB storage sdevice



Ftp Client Configuration

UserName:

Password:

Download URL: ftp://

Port: 21

Device: No USB device

Save Path:

Note: Waiting for 5 to 10 sec and plug out usb device after download comp

Recent 10 Download Record

UserName	Password	Port	Download URL	Save Path	Status

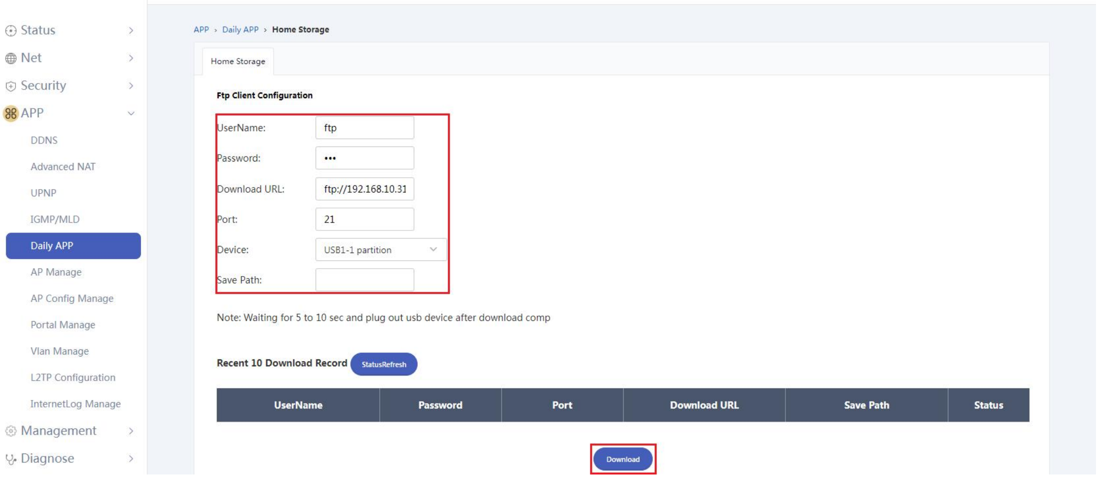
6.3.5.1 FTP Download Configuration Example

1.Connect a USB storage device.

Fill in the relevant information: FTP username, password, FTP download url, FTP port, select storage device, and Save path.

2.Click the "Download" button.

The following section can be used to view the download status and historical download records as illustrated in the figure below.



Ftp Client Configuration

UserName: ftp

Password: •••

Download URL: ftp://192.168.10.31

Port: 21

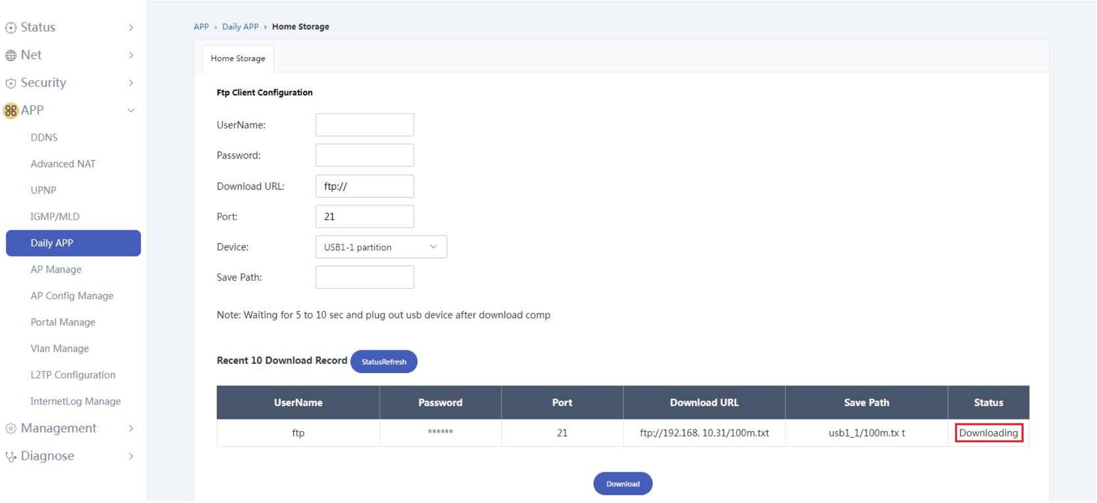
Device: USB1-1 partition

Save Path:

Note: Waiting for 5 to 10 sec and plug out usb device after download comp

Recent 10 Download Record

UserName	Password	Port	Download URL	Save Path	Status



Ftp Client Configuration

UserName:

Password:

Download URL: ftp://

Port: 21

Device: USB1-1 partition

Save Path:

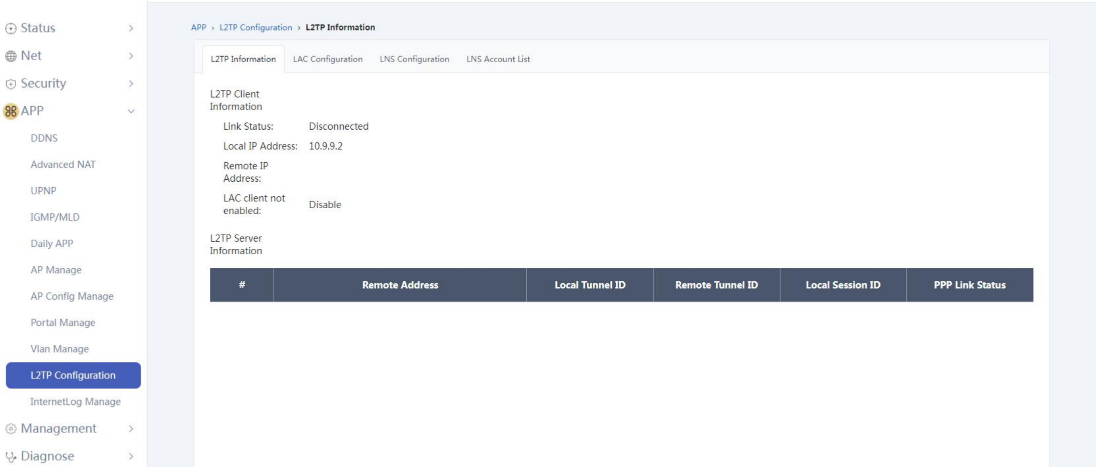
Note: Waiting for 5 to 10 sec and plug out usb device after download comp

Recent 10 Download Record

UserName	Password	Port	Download URL	Save Path	Status
ftp	******	21	ftp://192.168. 10.31/100m.txt	usb1_1/100m.tx t	Downloading

6.3.6 L2TP Configuration

Click on the menu "APP -> L2TP Configuration" to enter the configuration page as illustrated in the figure below.



L2TP Client Information

Link Status: Disconnected

Local IP Address: 10.9.9.2

Remote IP Address:

LAC client not enabled: Disable

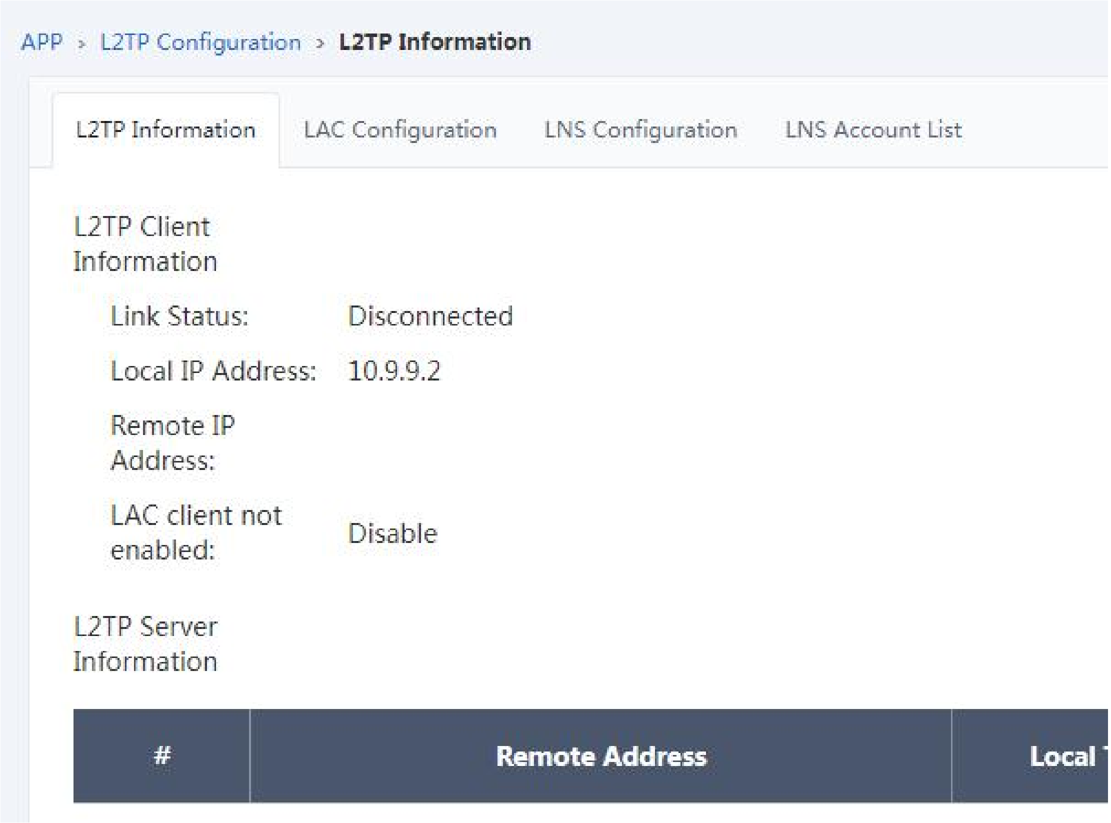
L2TP Server Information

#	Remote Address	Local Tunnel ID	Remote Tunnel ID	Local Session ID	PPP Link Status

6.3.6.1 L2TP Information

6.3.6.1.1 L2TP Client Information

Displays the link status of the L2TP client, local IP, and remote IP.



APP > L2TP Configuration > **L2TP Information**

L2TP Client Information

Link Status: Disconnected

Local IP Address: 10.9.9.2

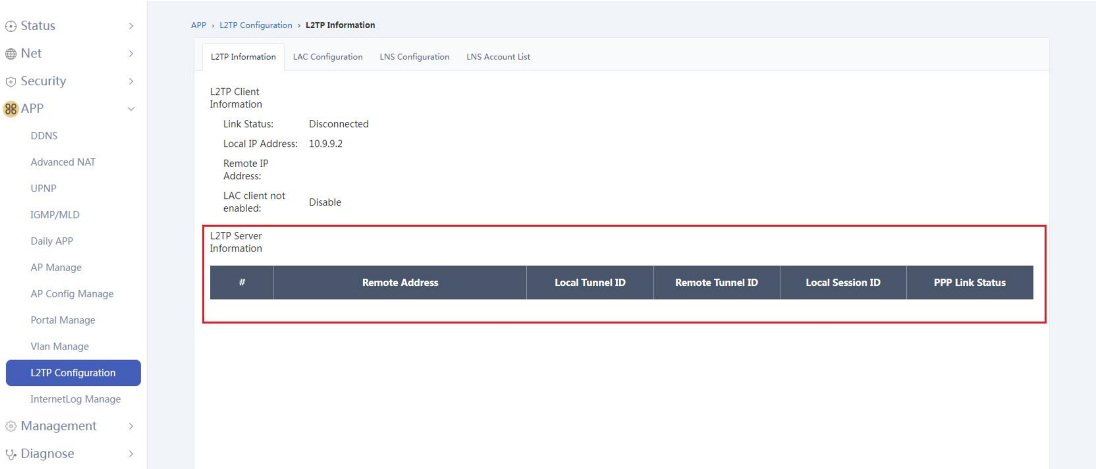
Remote IP Address:

LAC client not enabled: Disable

L2TP Server Information

#	Remote Address	Local

6.3.6.1.2 Server Information



L2TP Client Information

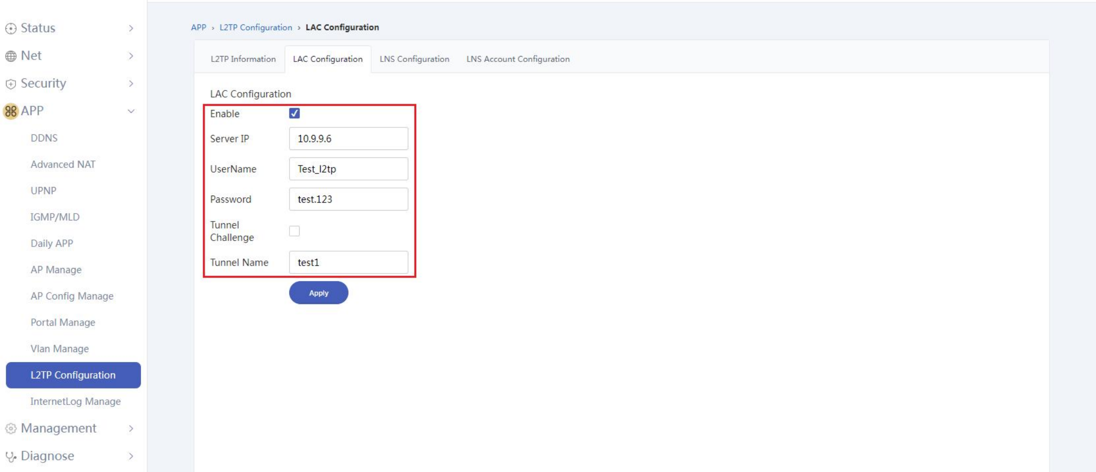
Link Status:	Disconnected
Local IP Address:	10.9.9.2
Remote IP Address:	
LAC client not enabled:	Disable

L2TP Server Information

#	Remote Address	Local Tunnel ID	Remote Tunnel ID	Local Session ID	PPP Link Status

6.3.6.1.3 LAC Configuration

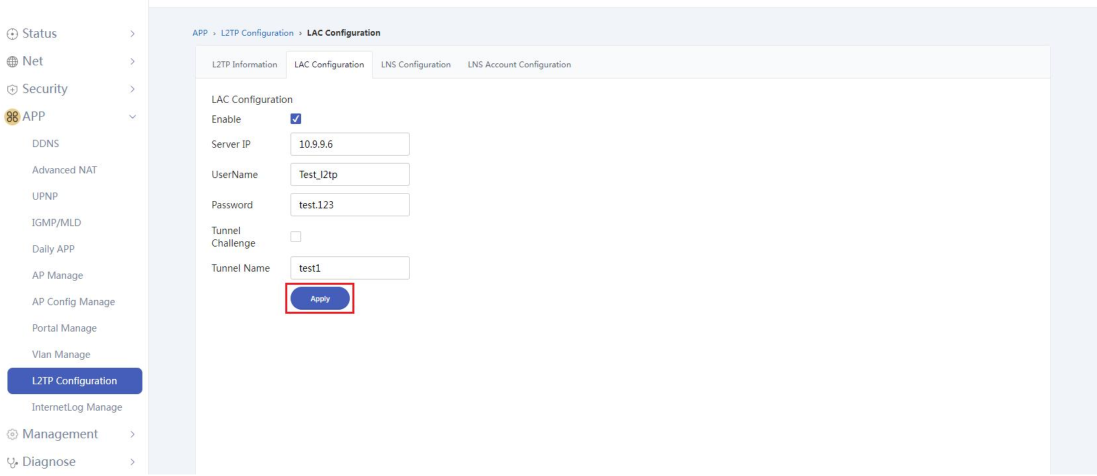
Step 1: Enable LAC and configure the relevant parameters as illustrated in the figure below.



LAC Configuration

Enable	☑
Server IP	10.9.9.6
UserName	Test_l2tp
Password	test.123
Tunnel Challenge	□
Tunnel Name	test1

Step 2: After setting is complete, click "Add" as illustrated in the figure below.



LAC Configuration

Enable ☑

Server IP: 10.9.9.6

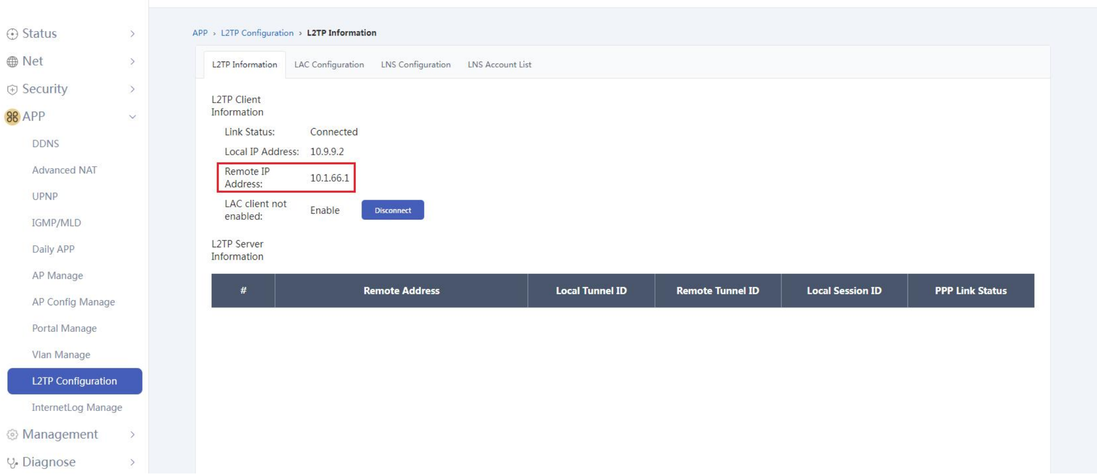
UserName: Test_l2tp

Password: test.123

Tunnel Challenge ☐

Tunnel Name: test1

After successful setup, you can see the remote IP address in the L2TP client information.



L2TP Client Information

Link Status: Connected

Local IP Address: 10.9.9.2

Remote IP Address: 10.1.66.1

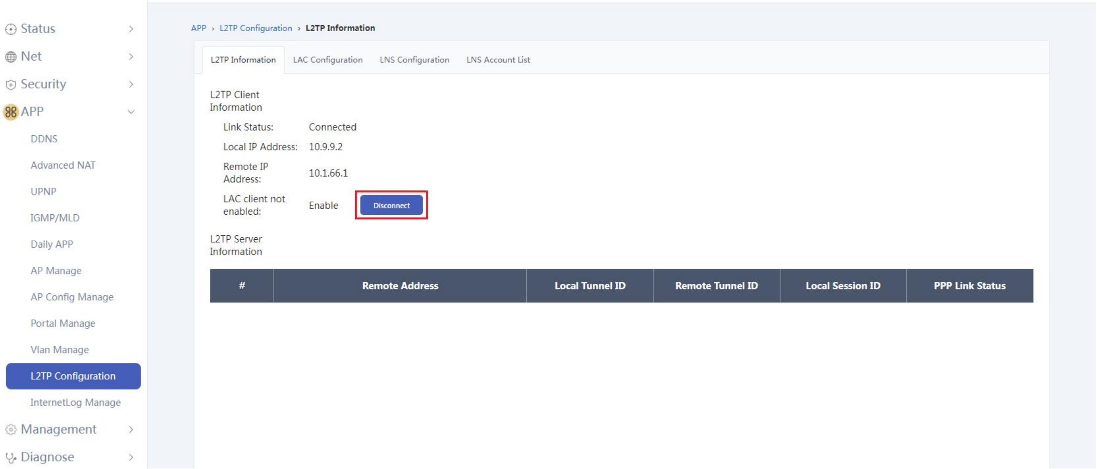
LAC client not enabled: Enable

L2TP Server Information

#	Remote Address	Local Tunnel ID	Remote Tunnel ID	Local Session ID	PPP Link Status

6.3.6.1.4 Removing LAC Configuration Example

Click "Disconnect" to complete the removal operation as illustrated in the figure below.



L2TP Client Information

Link Status: Connected

Local IP Address: 10.9.9.2

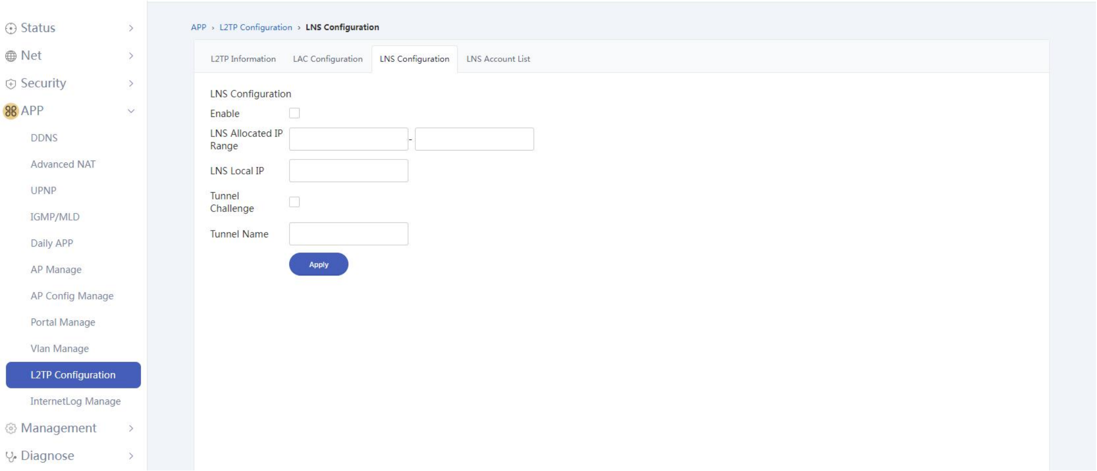
Remote IP Address: 10.1.66.1

LAC client not enabled: Enable

L2TP Server Information

#	Remote Address	Local Tunnel ID	Remote Tunnel ID	Local Session ID	PPP Link Status

6.3.6.3 LNS Configuration



LNS Configuration

Enable □

LNS Allocated IP Range ______ - ______

LNS Local IP ______

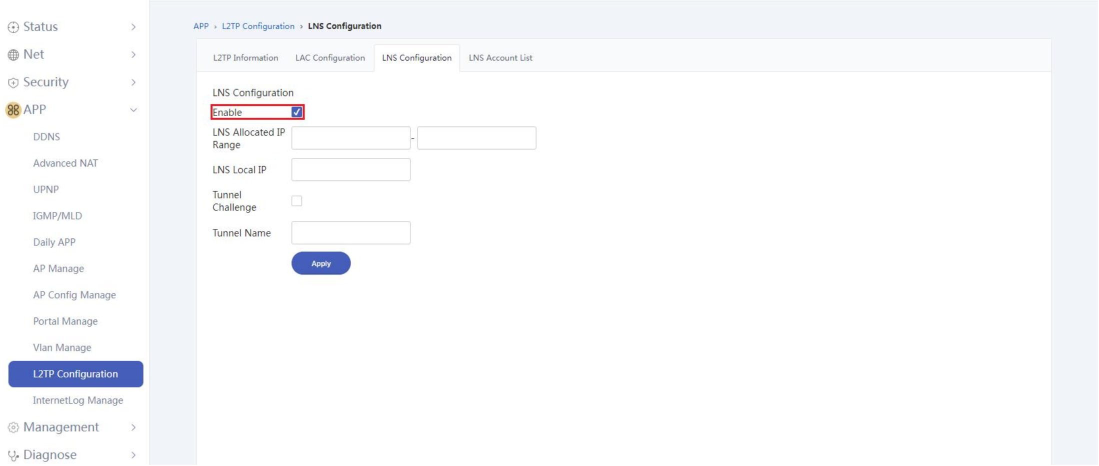
Tunnel Challenge □

Tunnel Name ______

LNS can use different virtual interface profiles to receive tunnel creation requests from various LACs. Upon receiving a tunnel creation request from an LAC, the LNS checks if the LAC's name matches the authorized tunnel peer name to decide whether to allow the tunnel creation.

6.3.6.3.1 Adding an LNS Instance

Step 1: Check "Enable" to enable LNS as illustrated in the figure below.



LNS Configuration

Enable ☑

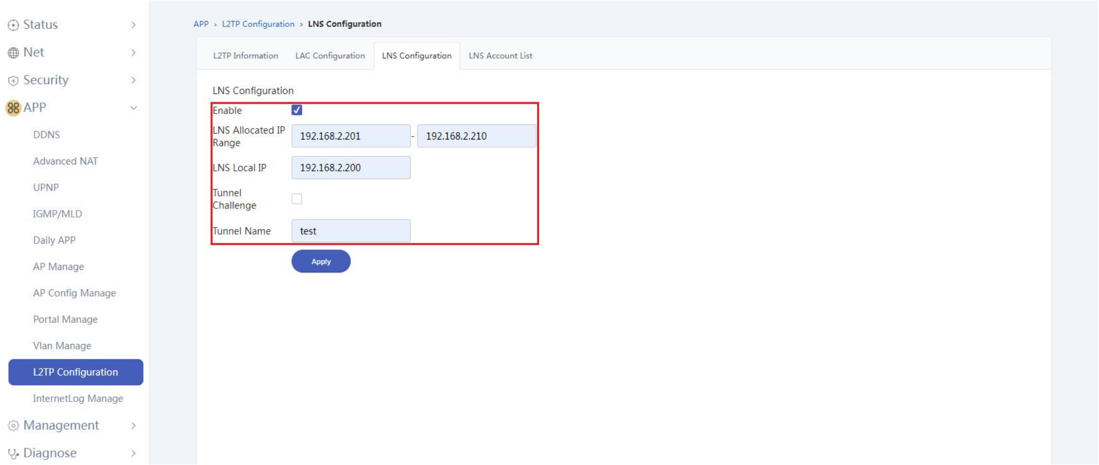
LNS Allocated IP Range -

LNS Local IP

Tunnel Challenge □

Tunnel Name

Step 2: Configure the relevant LNS parameters as illustrated in the figure below.



LNS Configuration

Enable ☑

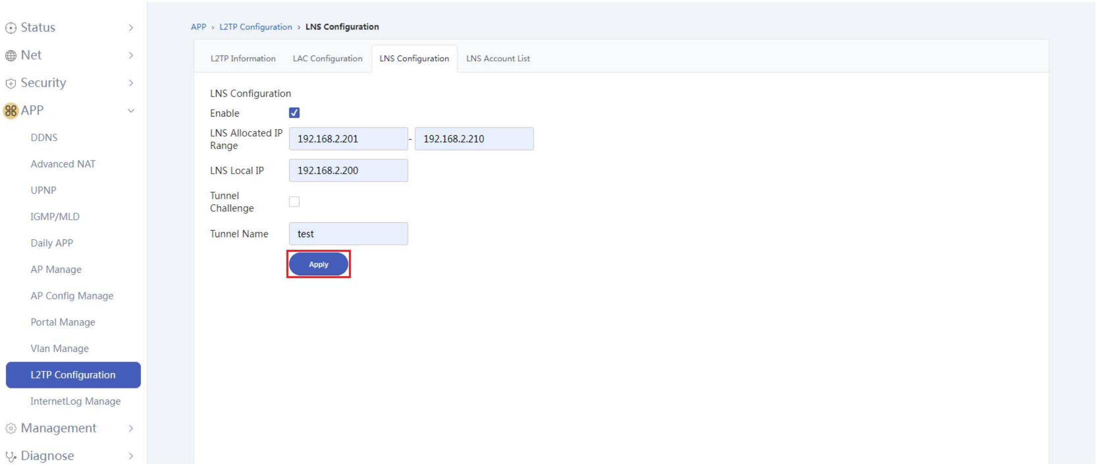
LNS Allocated IP Range 192.168.2.201 - 192.168.2.210

LNS Local IP 192.168.2.200

Tunnel Challenge □

Tunnel Name test

Step 3: Click "Add" to add the LNS configuration as illustrated in the figure below.



LNS Configuration

Enable ☑

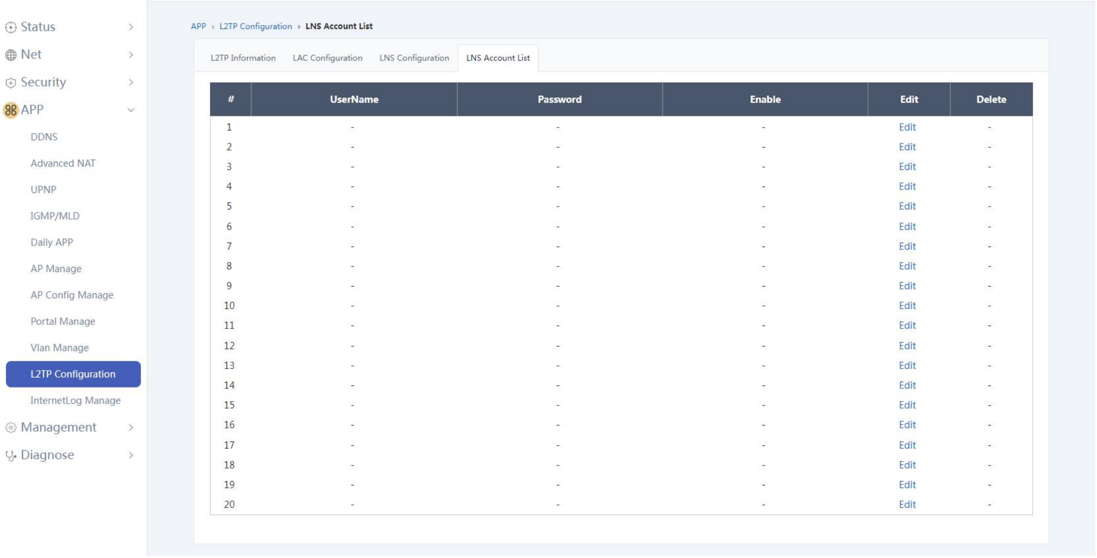
LNS Allocated IP Range: 192.168.2.201 - 192.168.2.210

LNS Local IP: 192.168.2.200

Tunnel Challenge ☐

Tunnel Name: test

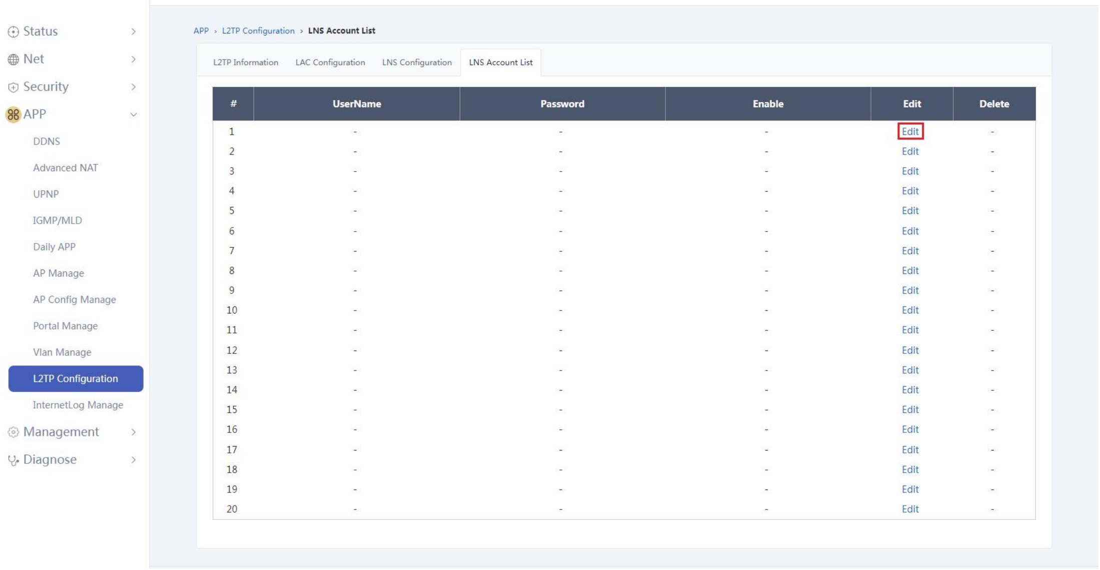
6.3.6.4 LNS Account List



#	UserName	Password	Enable	Edit	Delete
1	-	-	-	Edit	-
2	-	-	-	Edit	-
3	-	-	-	Edit	-
4	-	-	-	Edit	-
5	-	-	-	Edit	-
6	-	-	-	Edit	-
7	-	-	-	Edit	-
8	-	-	-	Edit	-
9	-	-	-	Edit	-
10	-	-	-	Edit	-
11	-	-	-	Edit	-
12	-	-	-	Edit	-
13	-	-	-	Edit	-
14	-	-	-	Edit	-
15	-	-	-	Edit	-
16	-	-	-	Edit	-
17	-	-	-	Edit	-
18	-	-	-	Edit	-
19	-	-	-	Edit	-
20	-	-	-	Edit	-

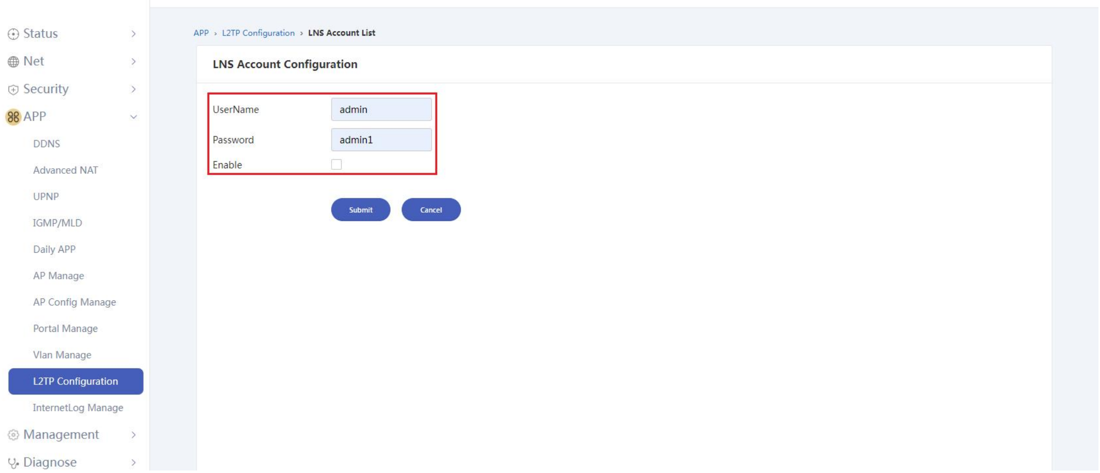
6.3.6.4.1 Creating LNS Account Instance

Step 1: Click "Edit" to enter the LNS account configuration as illustrated in the figure below.



#	UserName	Password	Enable	Edit	Delete
1	-	-	-	Edit	-
2	-	-	-	Edit	-
3	-	-	-	Edit	-
4	-	-	-	Edit	-
5	-	-	-	Edit	-
6	-	-	-	Edit	-
7	-	-	-	Edit	-
8	-	-	-	Edit	-
9	-	-	-	Edit	-
10	-	-	-	Edit	-
11	-	-	-	Edit	-
12	-	-	-	Edit	-
13	-	-	-	Edit	-
14	-	-	-	Edit	-
15	-	-	-	Edit	-
16	-	-	-	Edit	-
17	-	-	-	Edit	-
18	-	-	-	Edit	-
19	-	-	-	Edit	-
20	-	-	-	Edit	-

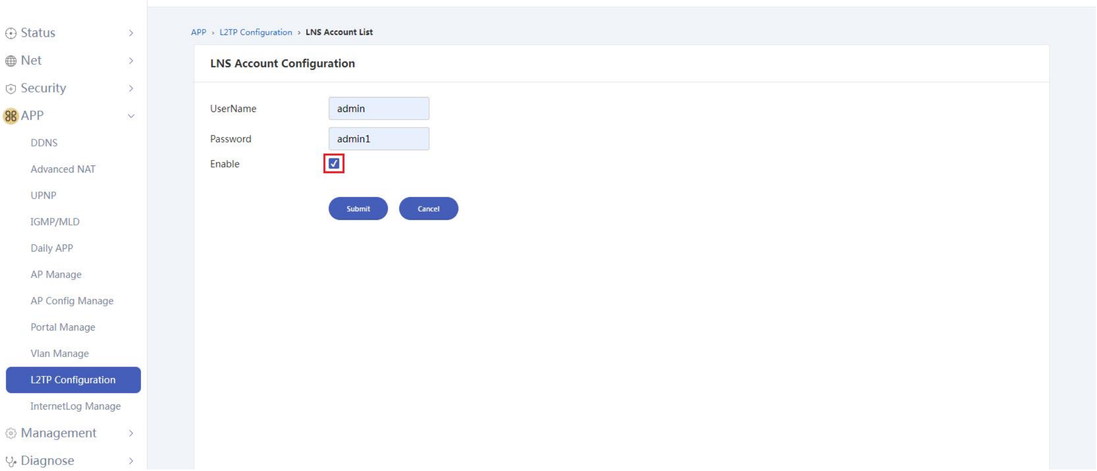
Step 2: Set the username and password for LNS user authentication.



LNS Account Configuration

UserName	admin
Password	admin1
Enable	□

Step 3: Check "Enable" to enable the LNS user.



APP › L2TP Configuration › LNS Account List

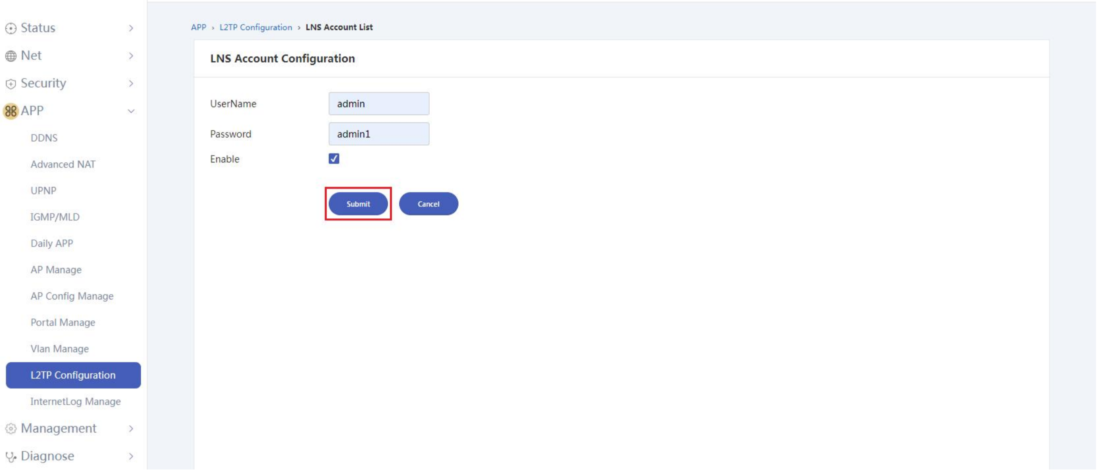
LNS Account Configuration

UserName: admin

Password: admin1

Enable: ☑

Step 4: Click "Submit" to complete the creation of the LNS account.



APP › L2TP Configuration › LNS Account List

LNS Account Configuration

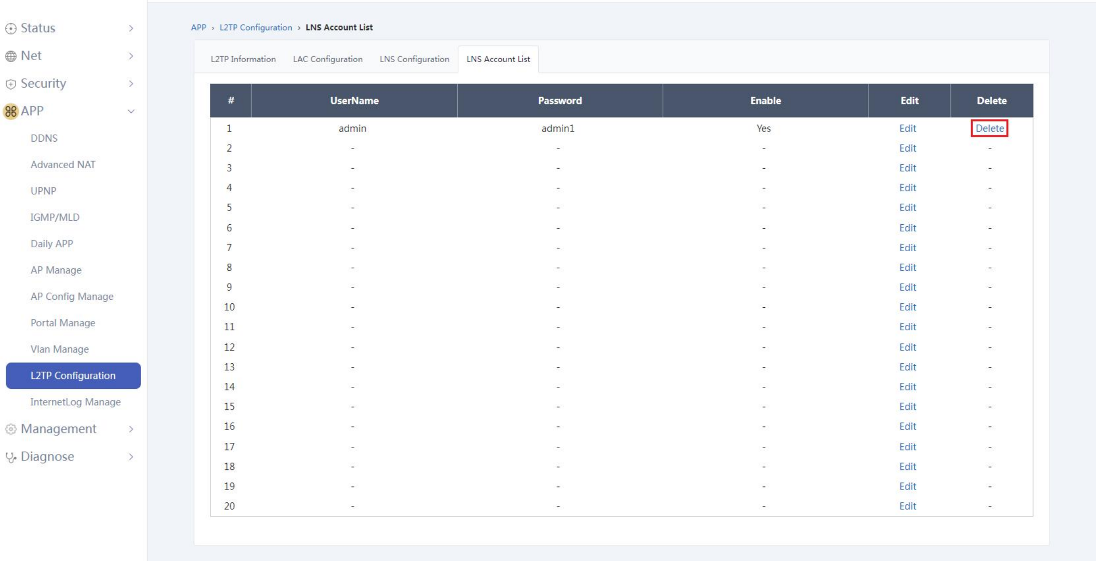
UserName: admin

Password: admin1

Enable: ☑

6.3.6.4.2 Deleting LNS Account Instance

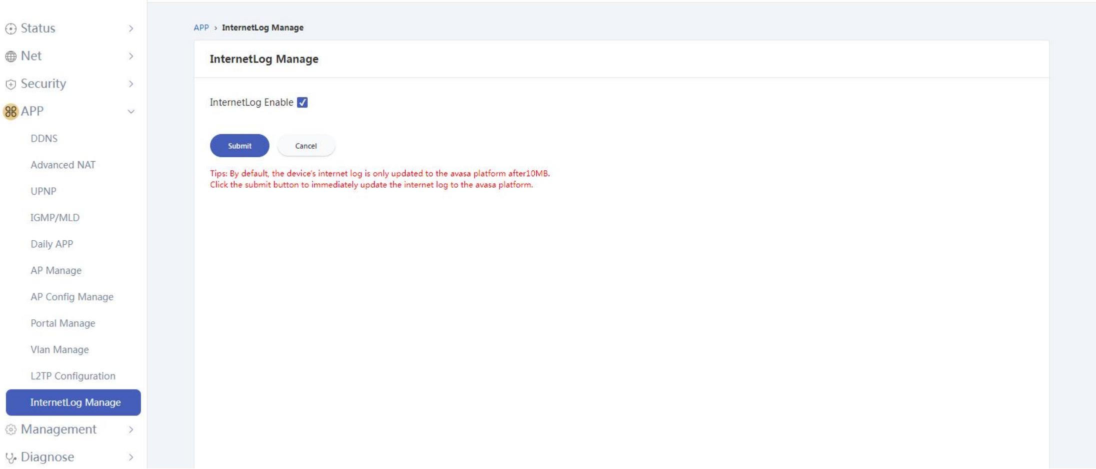
Select the instance you wish to delete and click the "Delete" button to complete the deletion as illustrated in the figure below.



#	UserName	Password	Enable	Edit	Delete
1	admin	admin1	Yes	Edit	Delete
2	-	-	-	Edit	-
3	-	-	-	Edit	-
4	-	-	-	Edit	-
5	-	-	-	Edit	-
6	-	-	-	Edit	-
7	-	-	-	Edit	-
8	-	-	-	Edit	-
9	-	-	-	Edit	-
10	-	-	-	Edit	-
11	-	-	-	Edit	-
12	-	-	-	Edit	-
13	-	-	-	Edit	-
14	-	-	-	Edit	-
15	-	-	-	Edit	-
16	-	-	-	Edit	-
17	-	-	-	Edit	-
18	-	-	-	Edit	-
19	-	-	-	Edit	-
20	-	-	-	Edit	-

6.3.7 InternetLog Manage

Click on the menu "APP -> InternetLog Manage" to enter the InternetLog management as illustrated in the figure below.

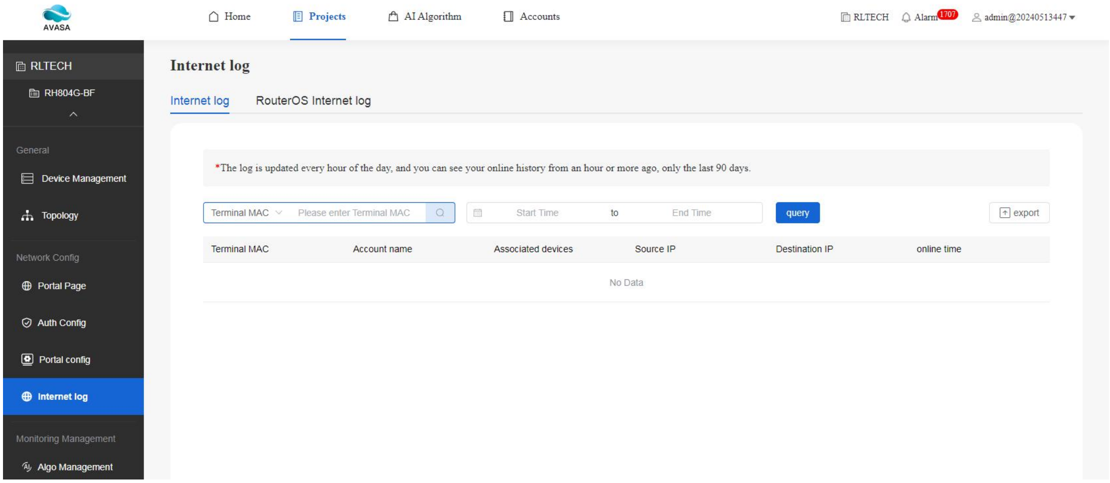


InternetLog Enable ☑

Tips: By default, the device's internet log is only updated to the avasa platform after10MB.
Click the submit button to immediately update the internet log to the avasa platform.

When the InternetLog manage is enabled, the device's internet logs will be uploaded to the AVASA when a single log file reaches 10MB. Logs stored on the AVASA are updated once every hour. Clicking the "Submit" button will immediately sync the latest logs to the AVASA.

The uploaded internet log information can be viewed on the AVASA under "Projects -> Internet log".



*The log is updated every hour of the day, and you can see your online history from an hour or more ago, only the last 90 days.

Terminal MAC	Account name	Associated devices	Source IP	Destination IP	online time
		No Data			

6.4 Management

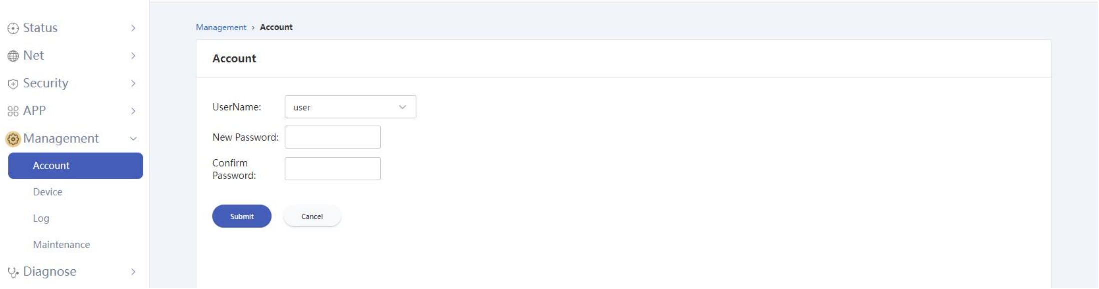
6.4.1 Account

End-user account password modification after verification (Verify the original password first and is only available to end users), as illustrated in the figure below.

(1) Each account allows only one user to log in at a time; a second user will be denied.

(2) The system will automatically log out the user if there is no activity for five consecutive minutes after login.

(3) If the username and password are entered incorrectly 3 times consecutively, the user will be unable to enter the username and password for verification within 1 minute.



Account

UserName: user

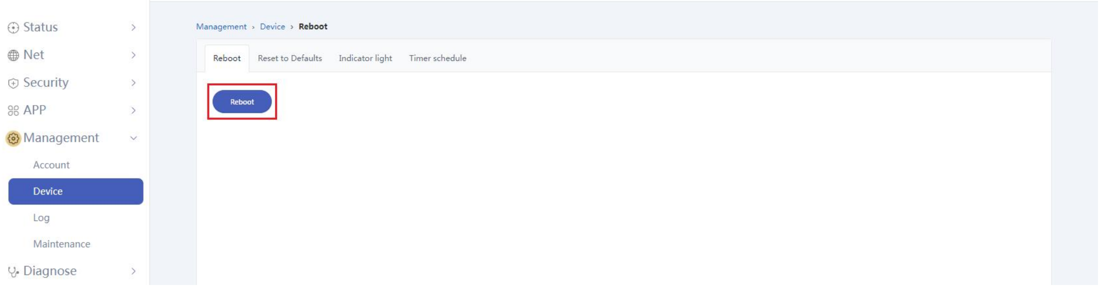
New Password:

Confirm Password:

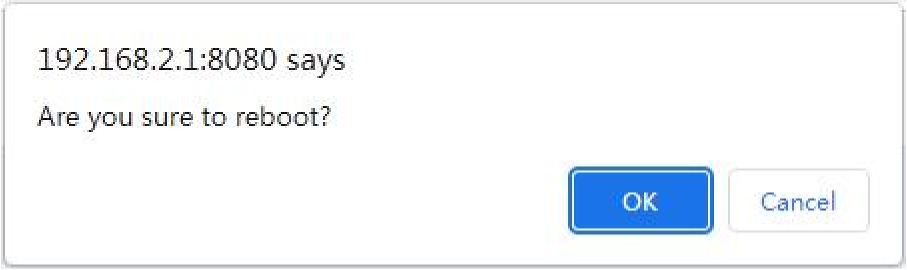
6.4.2 Device

6.4.2.1 Reboot

Supports device reboot as illustrated in the figure below.



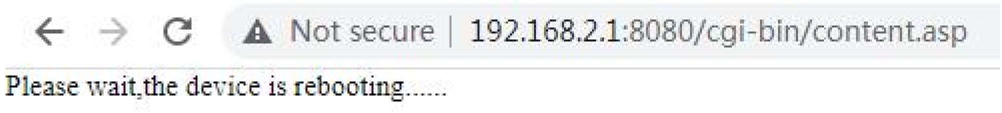
After clicking "Reboot", the following message appears.



192.168.2.1:8080 says

Are you sure to reboot?

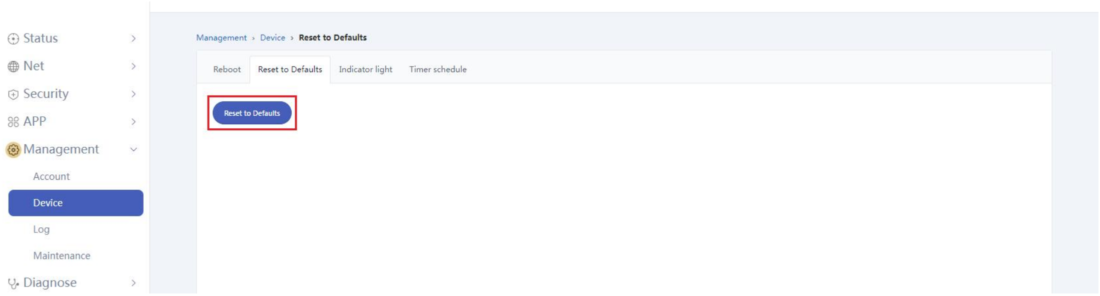
After clicking "OK", the process continues as illustrated in the figure below.



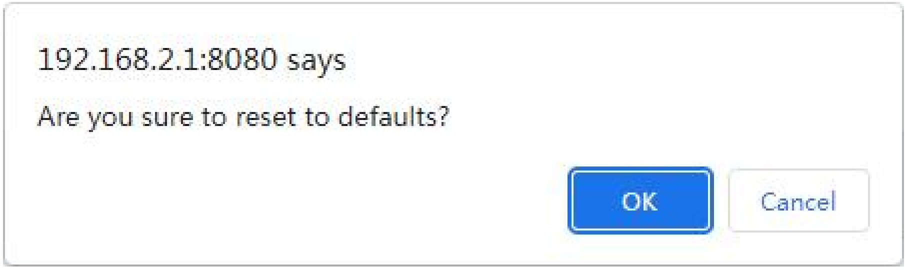
Please wait,the device is rebooting......

6.4.2.2 Reset to Defaults

Step 1: Reset to defaults via the page button as illustrated in the figure below.



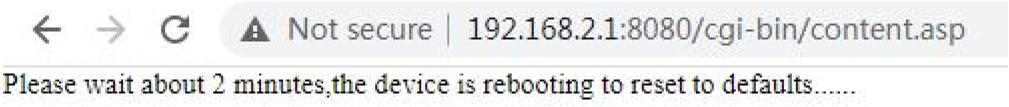
Step 2: A confirmation dialog appears as follows.



192.168.2.1:8080 says

Are you sure to reset to defaults?

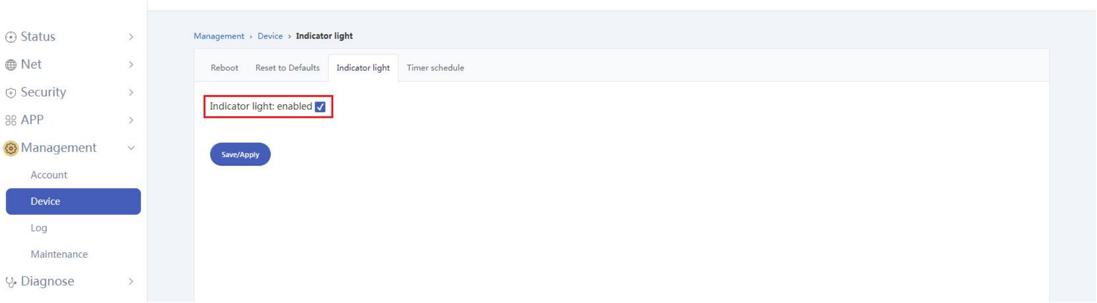
Step 3: After clicking "OK" the following message appears.



Please wait about 2 minutes,the device is rebooting to reset to defaults......

6.4.2.3 Indicator Light

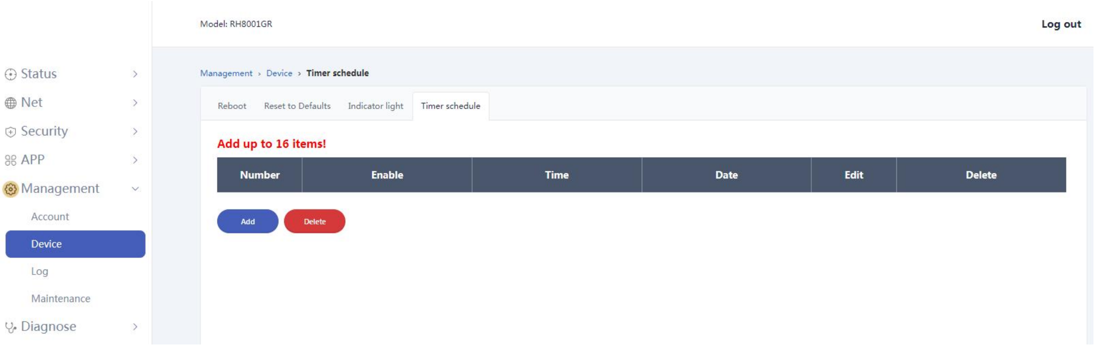
Check or uncheck "Enable" to control the indicator light on/off.



Indicator light: enabled ☑

6.4.2.4 Timer Schedule

Click "Management -> Device -> Timer Schedule" to access the scheduled reboot configuration page, as shown below.

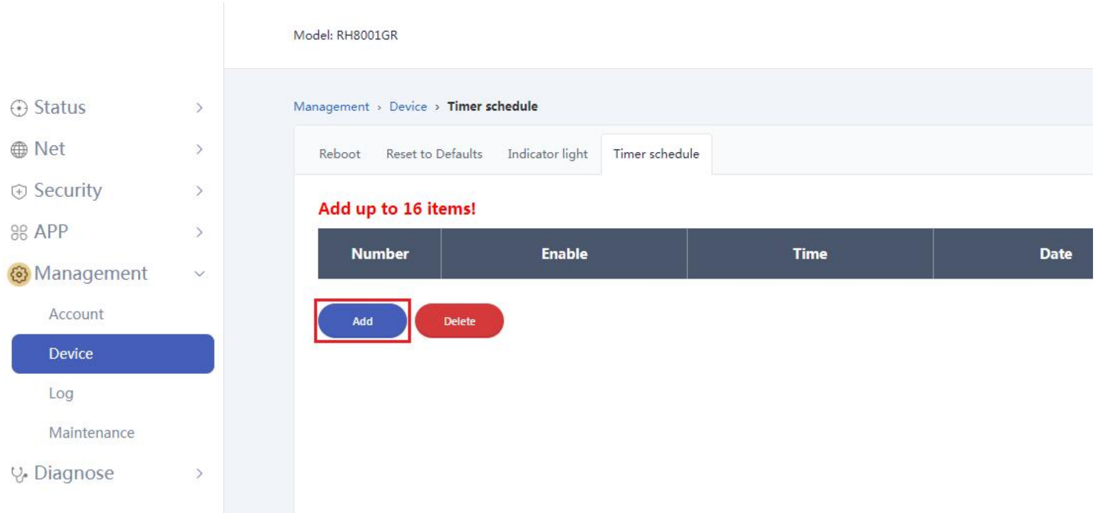


Model: RH8001GR

Add up to 16 items!

Number	Enable	Time	Date	Edit	Delete

Step 1: Click "Add" to create a schedule reboot rule.



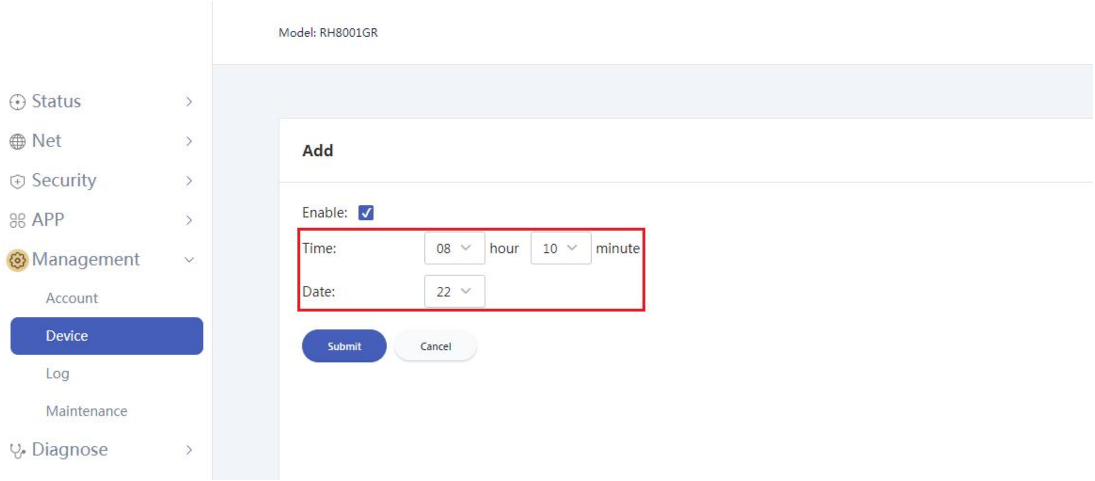
Model: RH8001GR

Management › Device › **Timer schedule**

Add up to 16 items!

Number	Enable	Time	Date

Step 2: Navigate to the schedule reboot configuration page. Check "Enable" and set the scheduled reboot time. Click "Submit" as illustrated in the figure below.



Model: RH8001GR

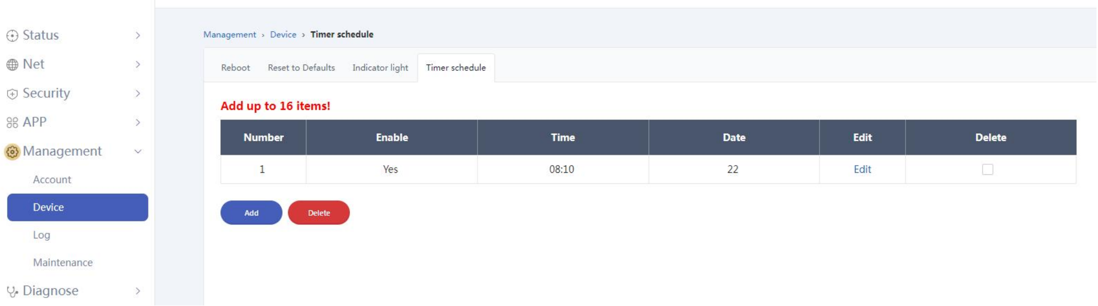
Add

Enable: ☑

Time: 08 hour 10 minute

Date: 22

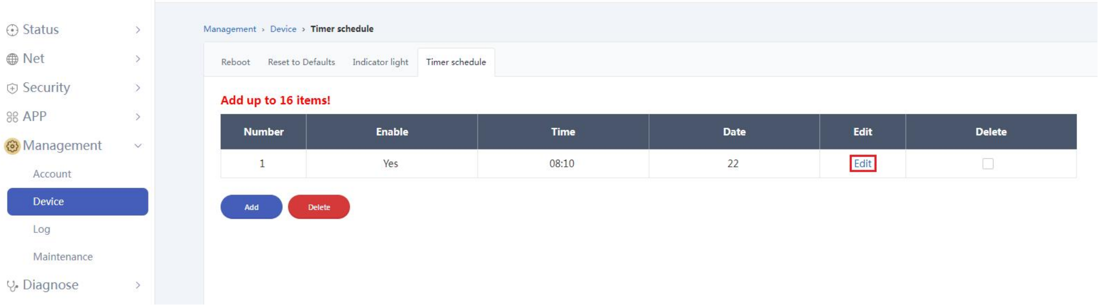
Step 3: The configured scheduled reboot rule is shown below. The device will automatically reboot at 08:10 on the 22nd of every month.



Add up to 16 items!

Number	Enable	Time	Date	Edit	Delete
1	Yes	08:10	22	Edit	□

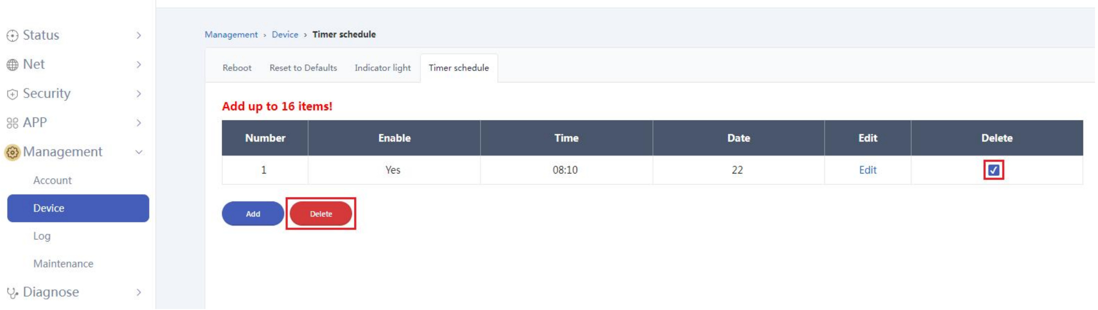
Step 4: Click "Edit" to modify the scheduled reboot rule as illustrated in the figure below.



Add up to 16 items!

Number	Enable	Time	Date	Edit	Delete
1	Yes	08:10	22	Edit	□

Step 5: Check "Delete" and click the "Delete" button to remove the scheduled reboot rule as illustrated in the figure below.

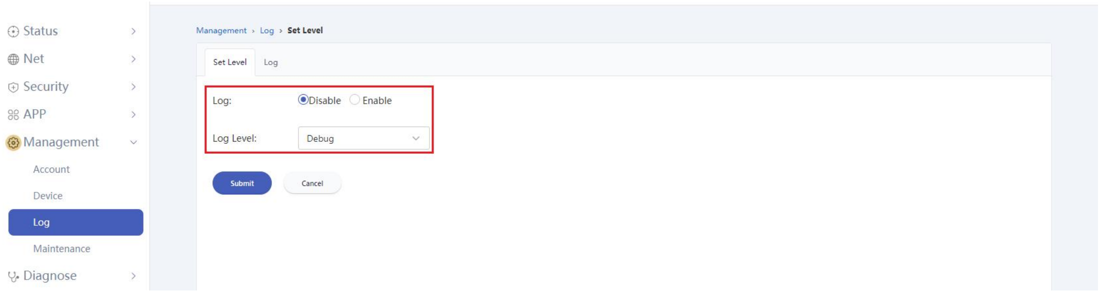


Add up to 16 items!

Number	Enable	Time	Date	Edit	Delete
1	Yes	08:10	22	Edit	☑

6.4.3 Log

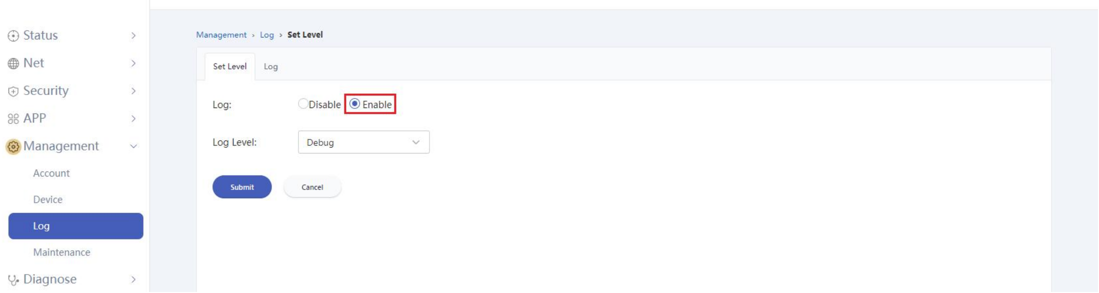
Click on the menu "Management -> Log" to enter the system log configuration page as illustrated in the figure below.



Log: ● Disable ○ Enable

Log Level: Debug

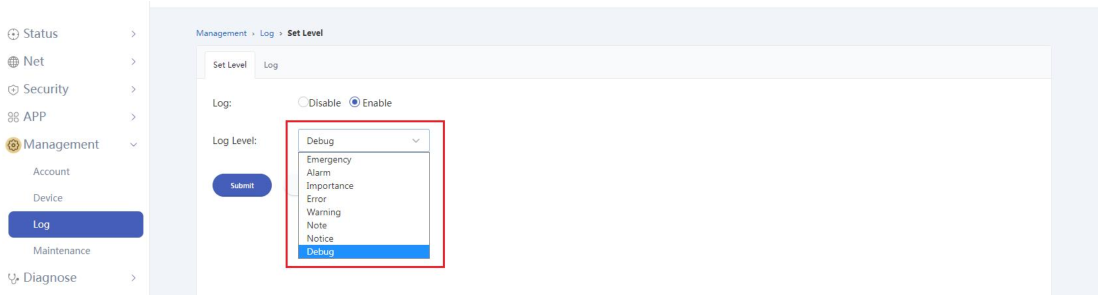
Step 1: Enable the system log function and click "Submit" as illustrated in the figure below.



Log: ○ Disable ● Enable

Log Level: Debug

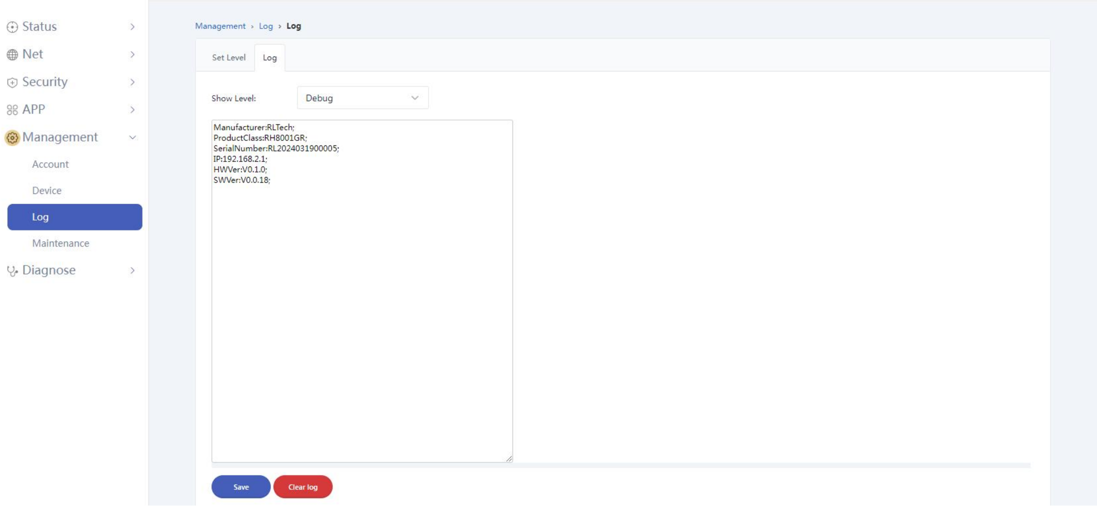
Step 2: Select the log level settings to view the desired system log information and click "Submit" as illustrated in the figure below.



Log: ○ Disable ● Enable

Log Level: Debug

Step 3: View detailed log information by log level as illustrated in the figure below.



Show Level: Debug

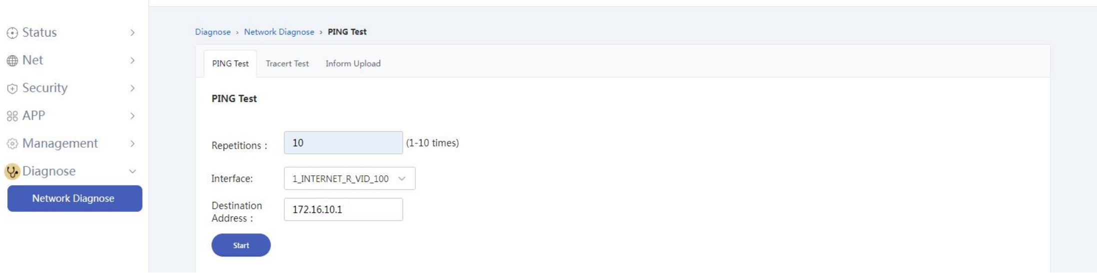
```
Manufacturer:RLTech;
ProductClass:RH8001GR;
SerialNumber:RL2024031900005;
IP:192.168.2.1;
HWVer:V0.1.0;
SWVer:V0.0.18;
```

6.5 Diagnosis

6.5.1 Network Diagnosis

Network diagnosis using PING and Traceroute under the selected WAN connection to test network connectivity. The destination address for testing supports both IP addresses and domain names.

6.5.1.1 Network Diagnosis Using Ping



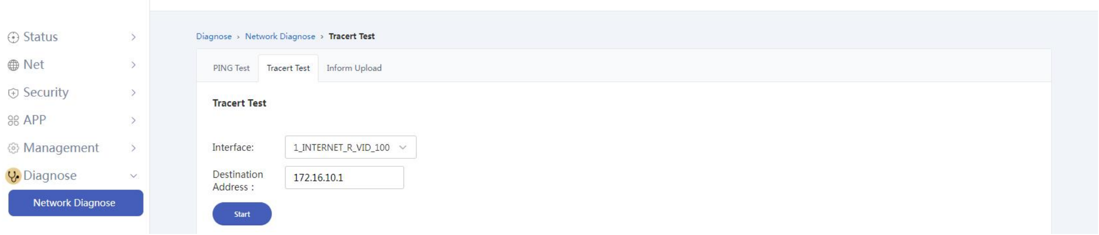
PING Test

Repetitions : 10 (1-10 times)

Interface: 1_INTERNET_R_VID_100

Destination Address : 172.16.10.1

6.5.1.2 Network Diagnosis Using Traceroute



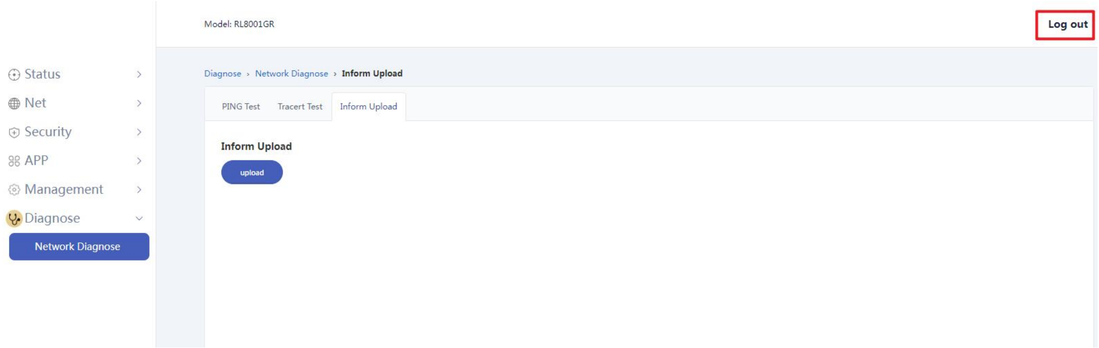
Tracert Test

Interface: 1_INTERNET_R_VID_100

Destination Address : 172.16.10.1

6.6 Logout

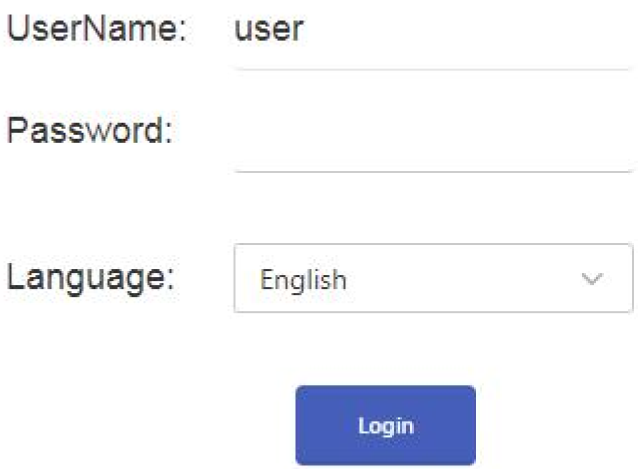
Log out the currently logged-in user as illustrated in the figure below.



Model: RL8001GR

Inform Upload

The logout process will return you to the login page as illustrated in the figure below.



UserName: user

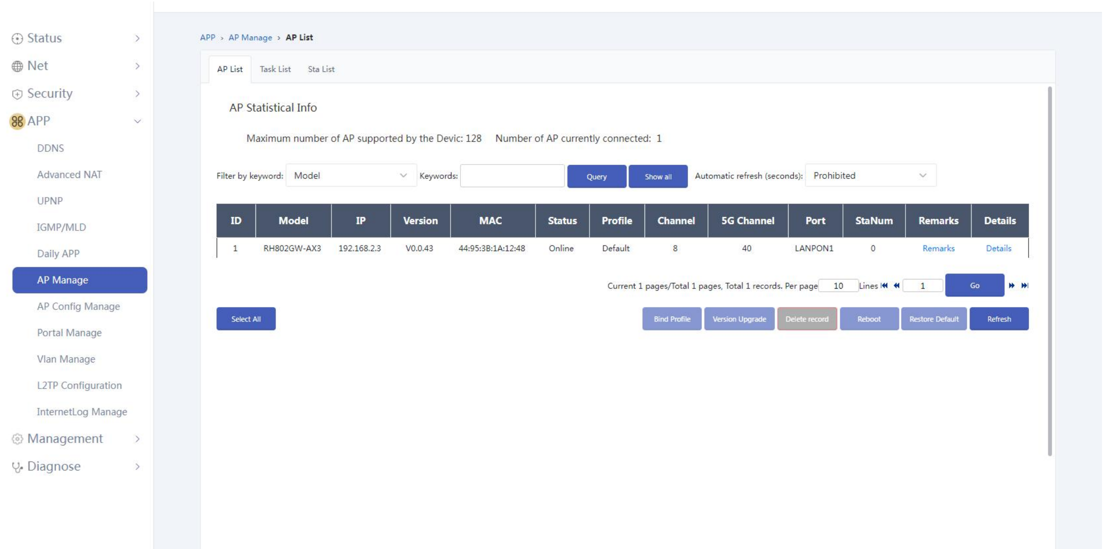
Password:

Language: English

7. ACAP Solution

7.1 AP Manage

Click on the menu "APP -> AP Manage" to enter the AP information list page as illustrated in the figure below.



AP Statistical Info

Maximum number of AP supported by the Devic: 128   Number of AP currently connected: 1

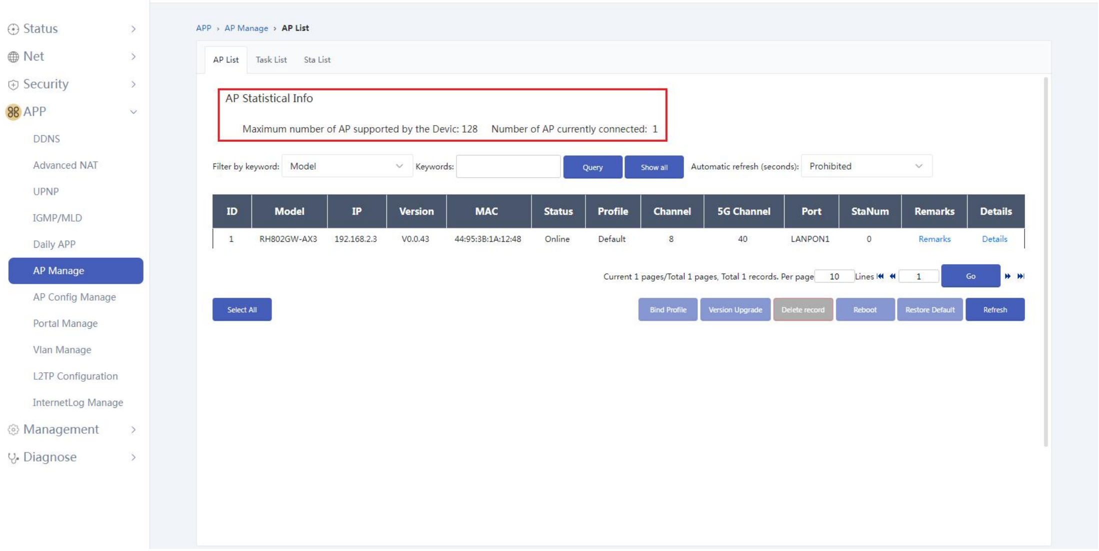
Filter by keyword: Model   Keywords: Automatic refresh (seconds): Prohibited

ID	Model	IP	Version	MAC	Status	Profile	Channel	5G Channel	Port	StaNum	Remarks	Details
1	RH802GW-AX3	192.168.2.3	V0.0.43	44:95:3B:1A:12:48	Online	Default	8	40	LANPON1	0	Remarks	Details

Current 1 pages/Total 1 pages, Total 1 records. Per page 10 Lines ⏮ ⏪ 1

7.1.1 AP List

7.1.1.1 AP Statistical Info



AP Statistical Info

Maximum number of AP supported by the Devic: 128   Number of AP currently connected: 1

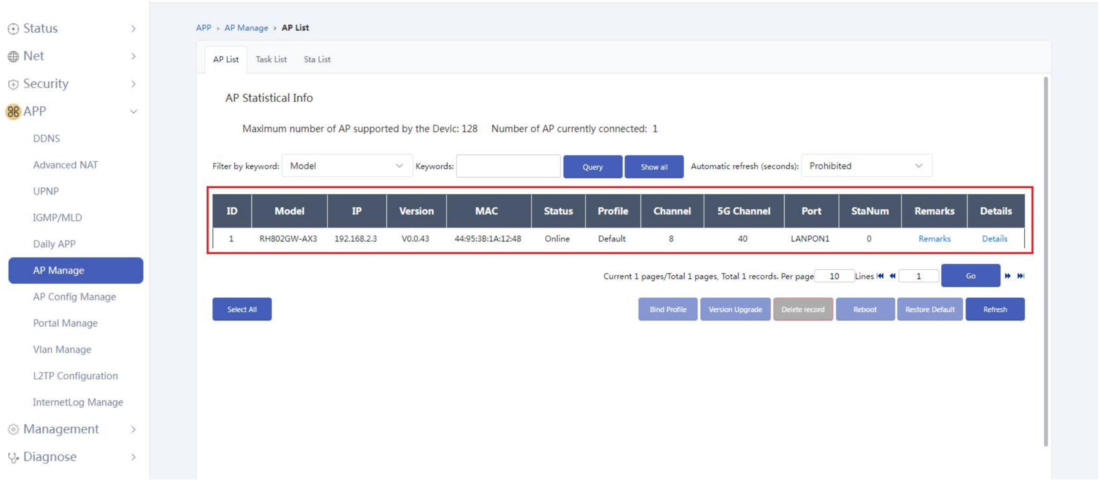
Filter by keyword: Model   Keywords: Automatic refresh (seconds): Prohibited

ID	Model	IP	Version	MAC	Status	Profile	Channel	5G Channel	Port	StaNum	Remarks	Details
1	RH802GW-AX3	192.168.2.3	V0.0.43	44:95:3B:1A:12:48	Online	Default	8	40	LANPON1	0	Remarks	Details

Current 1 pages/Total 1 pages, Total 1 records. Per page 10 Lines 1

Displays the maximum number of APs supported by the device and the current number of connected APs.

7.1.1.2 AP List



AP Statistical Info

Maximum number of AP supported by the Devic: 128   Number of AP currently connected: 1

Filter by keyword: Model   Keywords: Automatic refresh (seconds): Prohibited

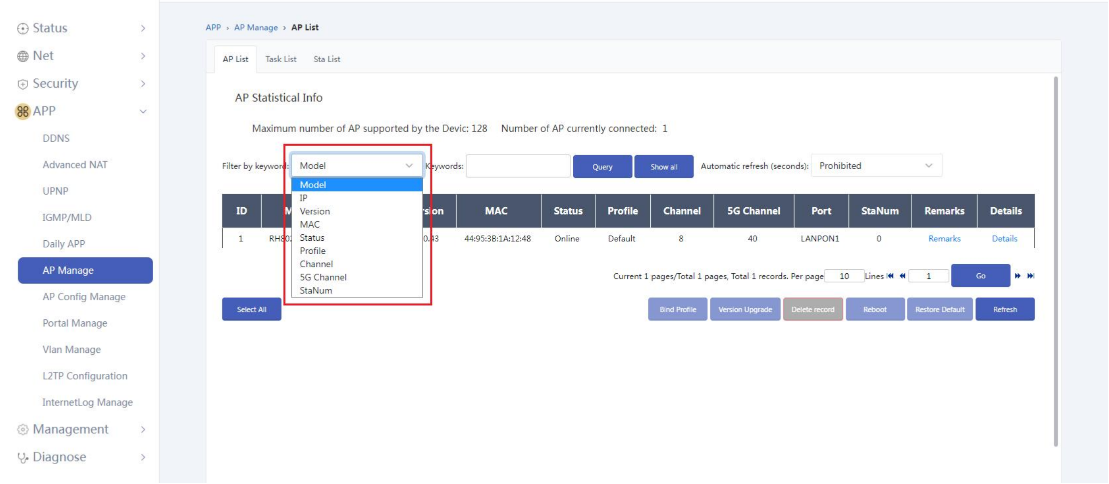
ID	Model	IP	Version	MAC	Status	Profile	Channel	5G Channel	Port	StaNum	Remarks	Details
1	RH802GW-AX3	192.168.2.3	V0.0.43	44:95:3B:1A:12:48	Online	Default	8	40	LANPON1	0	Remarks	Details

Current 1 pages/Total 1 pages, Total 1 records. Per page 10 Lines 1

The page displays various basic information about online and offline AP devices, offering features such as filtering the AP list by conditions, automatically refreshing the list, and viewing detailed information.

Displayed information includes: AP model, IP address, AP version, AP MAC, status, profile, channel, 5G channel,ports and number of AP clients.

◆ Keyword Filtering



AP Statistical Info

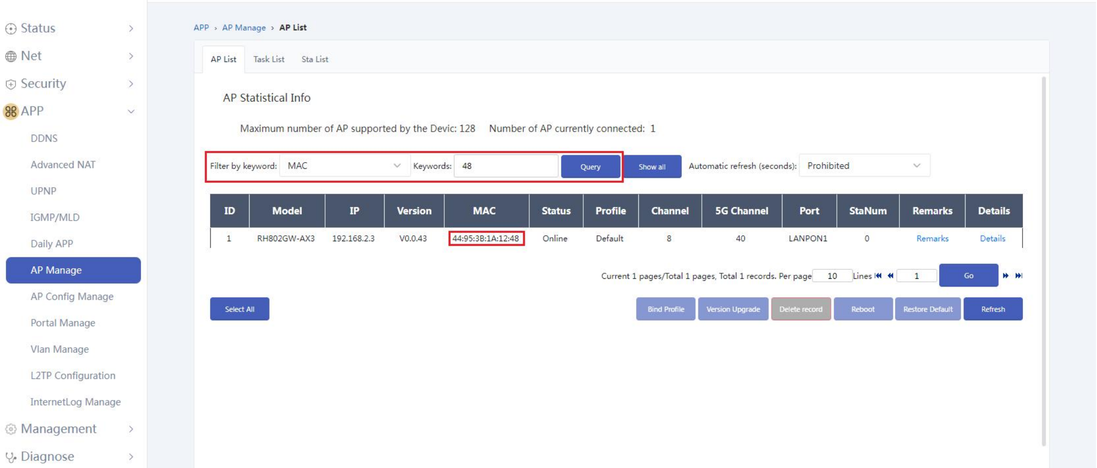
Maximum number of AP supported by the Devic: 128   Number of AP currently connected: 1

Filter by keyword: Model   Keywords: Automatic refresh (seconds): Prohibited

ID	M	rsion	MAC	Status	Profile	Channel	5G Channel	Port	StaNum	Remarks	Details
1	RH80	0.43	44:95:3B:1A:12:48	Online	Default	8	40	LANPON1	0	Remarks	Details

Current 1 pages/Total 1 pages, Total 1 records. Per page 10 Lines 1

Keywords that can be used include AP model, IP, version, MAC, status, profile, channel, 5G channel, and Stanum. After selecting a filter rule, enter relevant keywords and click the query button to filter:



AP Statistical Info

Maximum number of AP supported by the Devic: 128 Number of AP currently connected: 1

Filter by keyword: MAC Keywords: 48

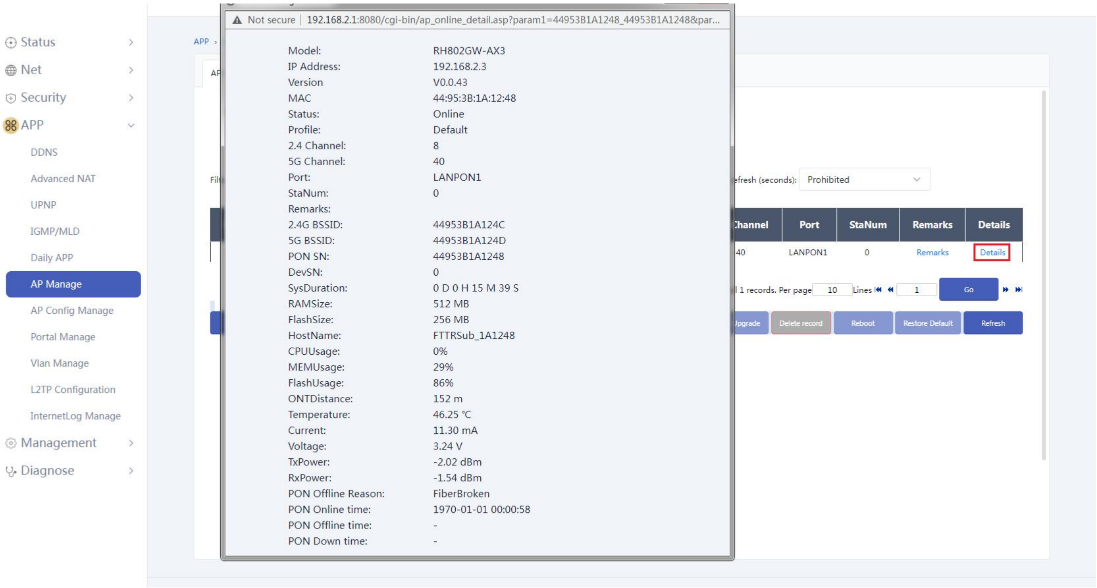
Automatic refresh (seconds): Prohibited

ID	Model	IP	Version	MAC	Status	Profile	Channel	5G Channel	Port	StaNum	Remarks	Details
1	RH802GW-AX3	192.168.2.3	V0.0.43	44:95:3B:1A:12:48	Online	Default	8	40	LANPON1	0	Remarks	Details

Current 1 pages/Total 1 pages, Total 1 records. Per page 10 Lines 1

Click the show all button to remove filter conditions.

◆ Detailed Information



Not secure | 192.168.2.1:8080/cgi-bin/ap_online_detail.asp?param1=44953B1A1248_44953B1A1248&par...

Model:	RH802GW-AX3
IP Address:	192.168.2.3
Version	V0.0.43
MAC	44:95:3B:1A:12:48
Status:	Online
Profile:	Default
2.4 Channel:	8
5G Channel:	40
Port:	LANPON1
StaNum:	0
Remarks:	
2.4G BSSID:	44953B1A124C
5G BSSID:	44953B1A124D
PON SN:	44953B1A1248
DevSN:	0
SysDuration:	0 D 0 H 15 M 39 S
RAMSize:	512 MB
FlashSize:	256 MB
HostName:	FTTRSub_1A1248
CPUUsage:	0%
MEMUsage:	29%
FlashUsage:	86%
ONTDistance:	152 m
Temperature:	46.25 ℃
Current:	11.30 mA
Voltage:	3.24 V
TxPower:	-2.02 dBm
RxPower:	-1.54 dBm
PON Offline Reason:	FiberBroken
PON Online time:	1970-01-01 00:00:58
PON Offline time:	-
PON Down time:	-

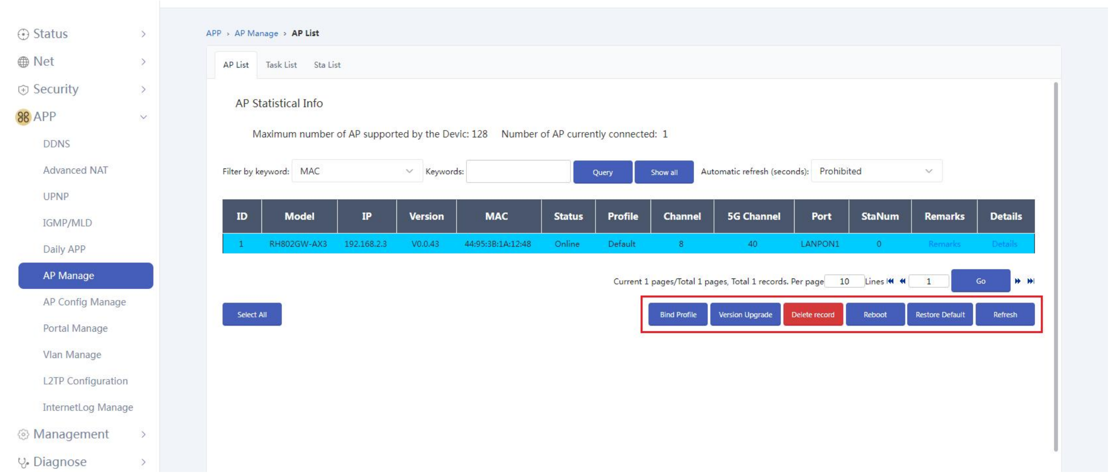
Automatic refresh (seconds): Prohibited

Channel	Port	StaNum	Remarks	Details
40	LANPON1	0	Remarks	Details

1 records. Per page 10 Lines 1

Click the "Details" button to view more detailed information about the AP.

7.1.1.3 AP Management



AP Statistical Info

Maximum number of AP supported by the Devic: 128 Number of AP currently connected: 1

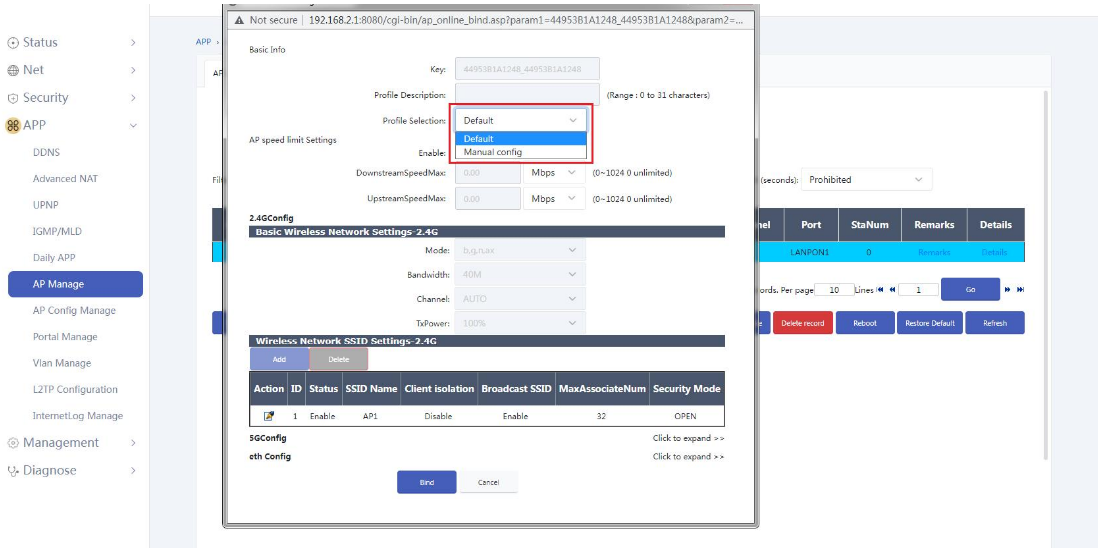
Filter by keyword: MAC Keywords: Automatic refresh (seconds): Prohibited

ID	Model	IP	Version	MAC	Status	Profile	Channel	5G Channel	Port	StaNum	Remarks	Details
1	RH802GW-AX3	192.168.2.3	V0.0.43	44:95:3B:1A:12:48	Online	Default	8	40	LANPON1	0	Remarks	Details

Current 1 pages/Total 1 pages, Total 1 records. Per page 10 Lines 1

After selecting one or multiple APs, you can perform operations such as bind profile, version upgrade, delete record, reboot, and restore default.

◆ Bind Profile



Not secure | 192.168.2.1:8080/cgi-bin/ap_online_bind.asp?param1=44953B1A1248_44953B1A1248&param2=...

Basic Info

Key: 44953B1A1248_44953B1A1248

Profile Description: (Range : 0 to 31 characters)

Profile Selection: Default (Default / Manual config)

AP speed limit Settings

Enable:

DownstreamSpeedMax: 0.00 Mbps (0~1024 0 unlimited)

UpstreamSpeedMax: 0.00 Mbps (0~1024 0 unlimited)

2.4GConfig

Basic Wireless Network Settings-2.4G

Mode: b,g,n,ax

Bandwidth: 40M

Channel: AUTO

TxPower: 100%

Wireless Network SSID Settings-2.4G

Add Delete

Action	ID	Status	SSID Name	Client isolation	Broadcast SSID	MaxAssociateNum	Security Mode
	1	Enable	AP1	Disable	Enable	32	OPEN

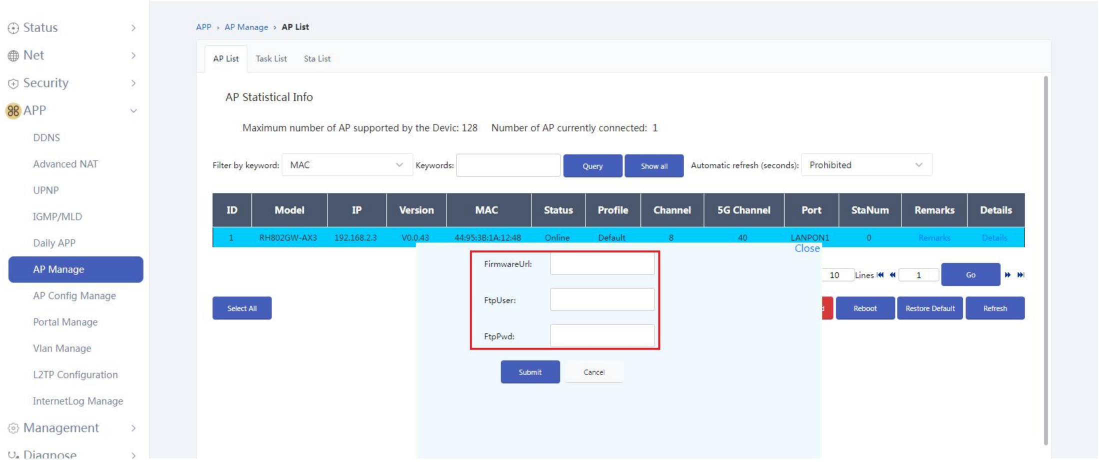
5GConfig Click to expand >>

eth Config Click to expand >>

Bind Cancel

After selecting an AP, you can modify the bound profile or choose manual configuration for personalized settings.

◆ Version Upgrade



APP > AP Manage > AP List

AP List Task List Sta List

AP Statistical Info

Maximum number of AP supported by the Devic: 128 Number of AP currently connected: 1

Filter by keyword: MAC Keywords: Automatic refresh (seconds): Prohibited

ID	Model	IP	Version	MAC	Status	Profile	Channel	5G Channel	Port	StaNum	Remarks	Details
1	RH802GW-AX3	192.168.2.3	V0.0.43	44:95:3B:1A:12:48	Online	Default	8	40	LANPON1	0	Remarks	Details

10 Lines 1

Close

FirmwareUrl:

FtpUser:

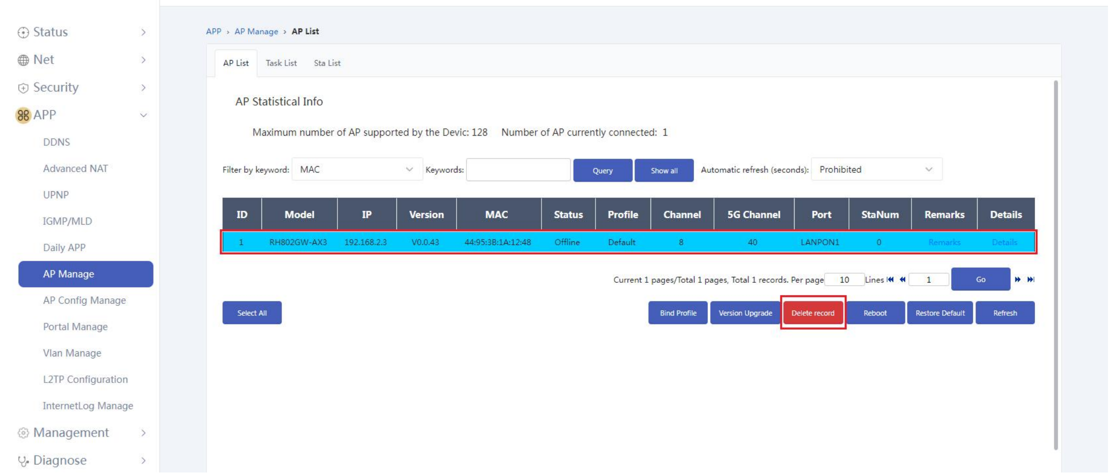
FtpPwd:

Submit Cancel

Enter the URL of the upgrade firmware and the account credentials of the remote server to remotely upgrade the AP.

Upgrading to the same version number is not allowed.

◆ Delete Records



AP Statistical Info

Maximum number of AP supported by the Devic: 128 Number of AP currently connected: 1

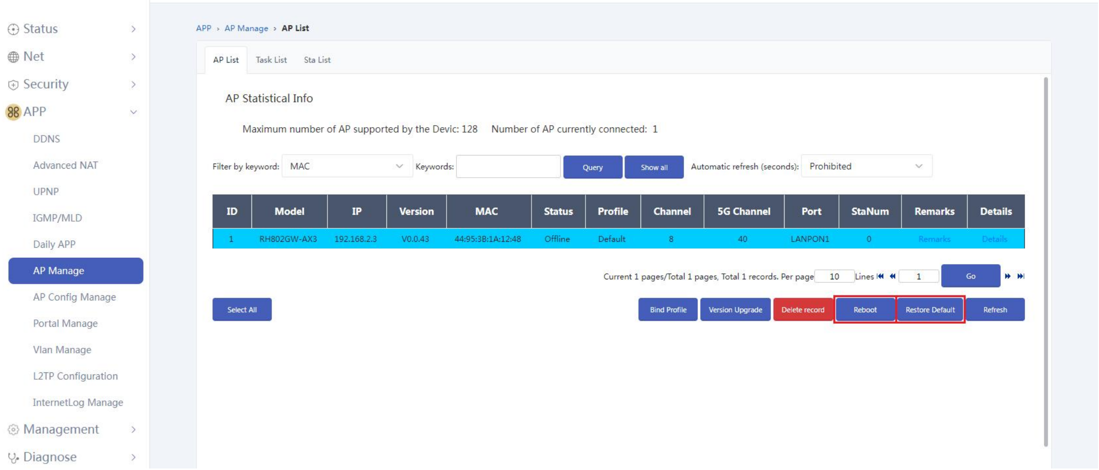
Filter by keyword: MAC Keywords: Automatic refresh (seconds): Prohibited

ID	Model	IP	Version	MAC	Status	Profile	Channel	5G Channel	Port	StaNum	Remarks	Details
1	RH802GW-AX3	192.168.2.3	V0.0.43	44:95:3B:1A:12:48	Offline	Default	8	40	LANPON1	0	Remarks	Details

Current 1 pages/Total 1 pages, Total 1 records. Per page 10 Lines 1

Select APs with an offline status and click the "Delete record" button to remove the offline AP records. You cannot delete records of online AP devices.

◆ Reboot and Restore Default



AP Statistical Info

Maximum number of AP supported by the Devic: 128 Number of AP currently connected: 1

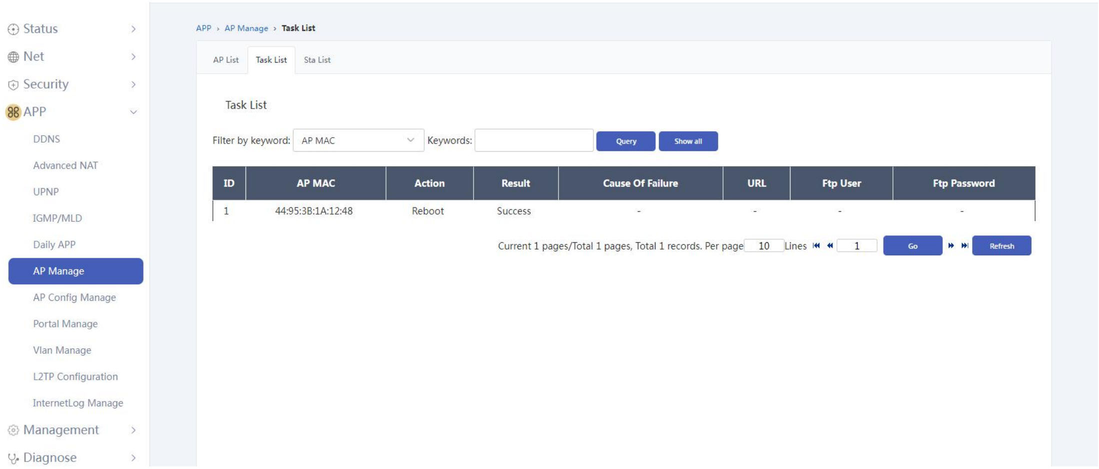
Filter by keyword: MAC Keywords: Query Show all Automatic refresh (seconds): Prohibited

ID	Model	IP	Version	MAC	Status	Profile	Channel	5G Channel	Port	StaNum	Remarks	Details
1	RH802GW-AX3	192.168.2.3	V0.0.43	44:95:3B:1A:12:48	Offline	Default	8	40	LANPON1	0	Remarks	Details

Current 1 pages/Total 1 pages, Total 1 records. Per page 10 Lines 1 Go

Select an AP to perform reboot or restore default operations.

7.1.2 Task List



Task List

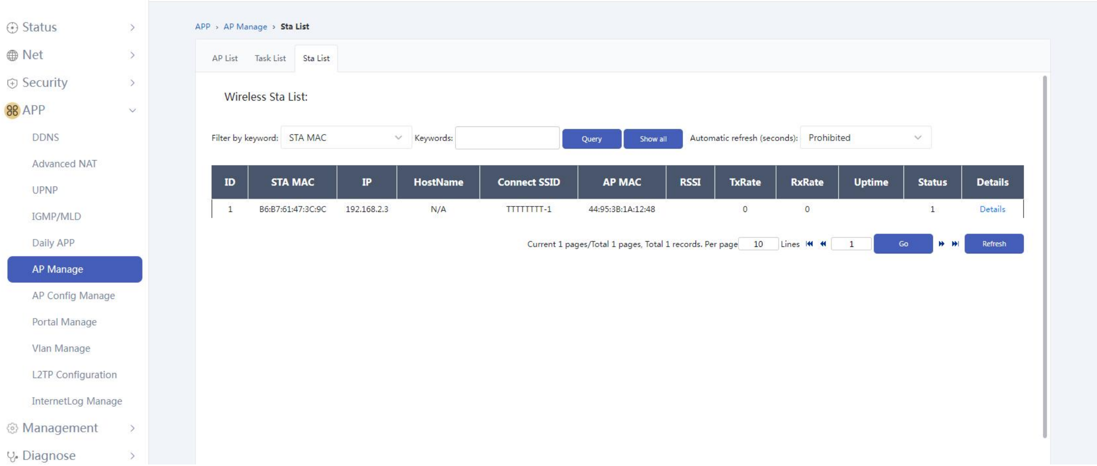
Filter by keyword: AP MAC Keywords: Query Show all

ID	AP MAC	Action	Result	Cause Of Failure	URL	Ftp User	Ftp Password
1	44:95:3B:1A:12:48	Reboot	Success	-	-	-	-

Current 1 pages/Total 1 pages, Total 1 records. Per page 10 Lines 1 Go Refresh

Displays the latest tasks issued to each AP through the AP management function, including AP MAC, action, result, etc. Each AP only shows one task record. The page also provides filtering functionality.

7.1.3 Sta List



Wireless Sta List:

Filter by keyword: STA MAC Keywords: Query Show all Automatic refresh (seconds): Prohibited

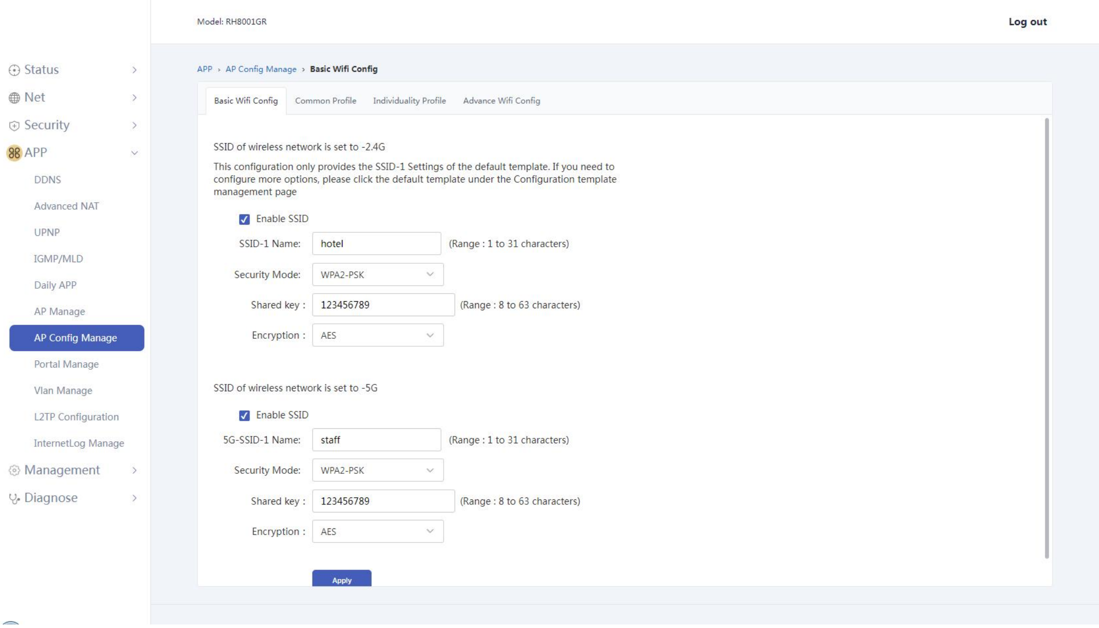
ID	STA MAC	IP	HostName	Connect SSID	AP MAC	RSSI	TxRate	RxRate	Uptime	Status	Details
1	B6:B7:61:47:3C:9C	192.168.2.3	N/A	TTTTTTTT-1	44:95:3B:1A:12:48		0	0		1	Details

Current 1 pages/Total 1 pages, Total 1 records. Per page 10 Lines 1 Go Refresh

Displays information about wireless access devices in the network, including MAC address, IP address, and connected SSID. You can click the "Details" button corresponding to each STA to view detailed information.The page also provides filtering functionality.

7.2 AP Config Manage

Click on the menu "APP -> AP Config Manage" to enter the AP management configuration page as illustrated in the figure below.



SSID of wireless network is set to -2.4G

This configuration only provides the SSID-1 Settings of the default template. If you need to configure more options, please click the default template under the Configuration template management page

☑ Enable SSID

SSID-1 Name: hotel (Range : 1 to 31 characters)

Security Mode: WPA2-PSK

Shared key : 123456789 (Range : 8 to 63 characters)

Encryption : AES

SSID of wireless network is set to -5G

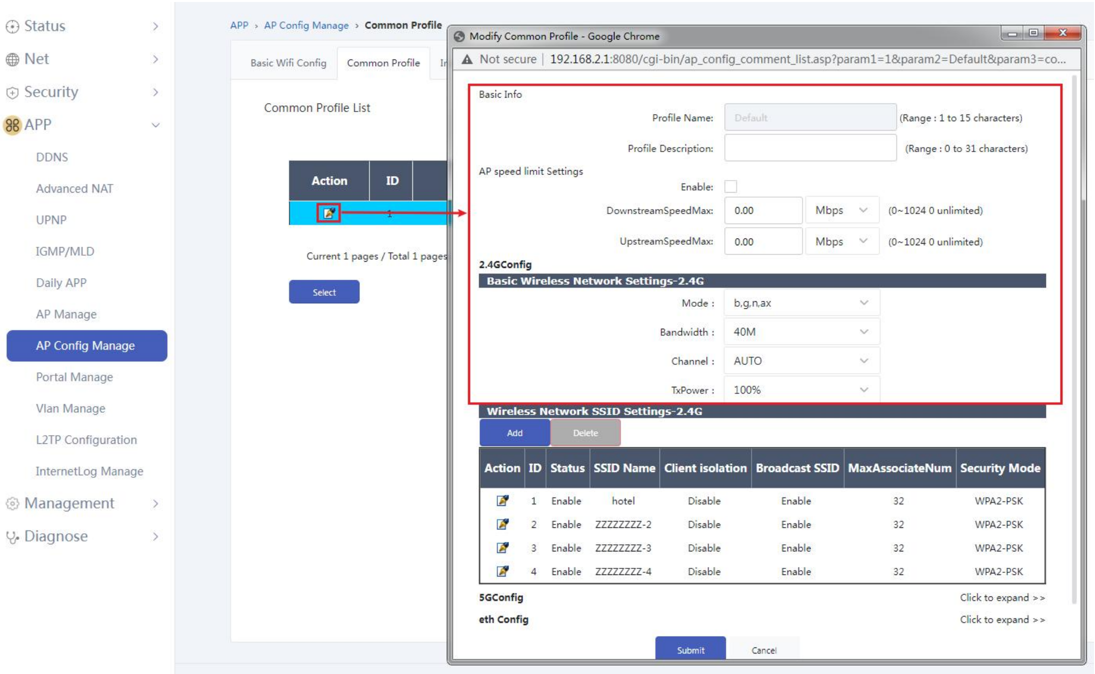
☑ Enable SSID

5G-SSID-1 Name: staff (Range : 1 to 31 characters)

Security Mode: WPA2-PSK

Shared key : 123456789 (Range : 8 to 63 characters)

Encryption : AES



Common Profile List

Action	ID
	1

Current 1 pages / Total 1 pages

192.168.2.1:8080/cgi-bin/ap_config_comment_list.asp?param1=1&param2=Default&param3=co...

Basic Info

Profile Name: Default (Range : 1 to 15 characters)

Profile Description: (Range : 0 to 31 characters)

AP speed limit Settings

Enable: □

DownstreamSpeedMax: 0.00 Mbps (0~1024 0 unlimited)

UpstreamSpeedMax: 0.00 Mbps (0~1024 0 unlimited)

2.4GConfig

Basic Wireless Network Settings-2.4G

Mode : b,g,n,ax

Bandwidth : 40M

Channel : AUTO

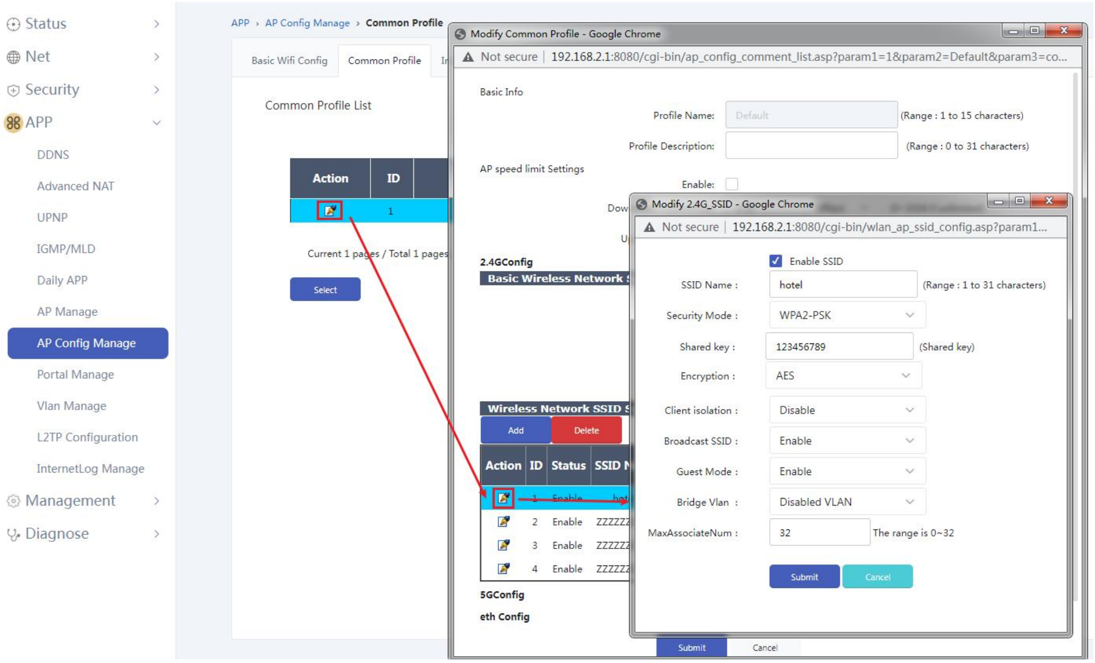
TxPower : 100%

Wireless Network SSID Settings-2.4G

Action	ID	Status	SSID Name	Client isolation	Broadcast SSID	MaxAssociateNum	Security Mode
	1	Enable	hotel	Disable	Enable	32	WPA2-PSK
	2	Enable	ZZZZZZZZ-2	Disable	Enable	32	WPA2-PSK
	3	Enable	ZZZZZZZZ-3	Disable	Enable	32	WPA2-PSK
	4	Enable	ZZZZZZZZ-4	Disable	Enable	32	WPA2-PSK

5GConfig Click to expand >>

eth Config Click to expand >>


Status
Net
Security
APP
DDNS
Advanced NAT
UPNP
IGMP/MLD
Daily APP
AP Manage
AP Config Manage
Portal Manage
Vlan Manage
L2TP Configuration
InternetLog Manage
Management
Diagnose
APP › AP Config Manage › Common Profile
Basic Wifi Config
Common Profile
Common Profile List
Select
Modify Common Profile - Google Chrome
Not secure | 192.168.2.1:8080/cgi-bin/ap_config_comment_list.asp?param1=1&param2=Default&param3=co...
Modify 2.4G_SSID - Google Chrome
Not secure | 192.168.2.1:8080/cgi-bin/wlan_ap_ssid_config.asp?param1...
Add
Delete
Submit
Cancel
Submit
Cancel

Action	ID
✎	1

Current 1 pages / Total 1 pages

Basic Info

Profile Name: Default (Range : 1 to 15 characters)

Profile Description: (Range : 0 to 31 characters)

AP speed limit Settings

Enable: □

2.4GConfig

Basic Wireless Network S

Wireless Network SSID S

Action	ID	Status	SSID N
✎	1	Enable	hot
✎	2	Enable	ZZZZZZ
✎	3	Enable	ZZZZZZ
✎	4	Enable	ZZZZZZ

5GConfig

eth Config

☑ Enable SSID

SSID Name : hotel (Range : 1 to 31 characters)

Security Mode : WPA2-PSK

Shared key : 123456789 (Shared key)

Encryption : AES

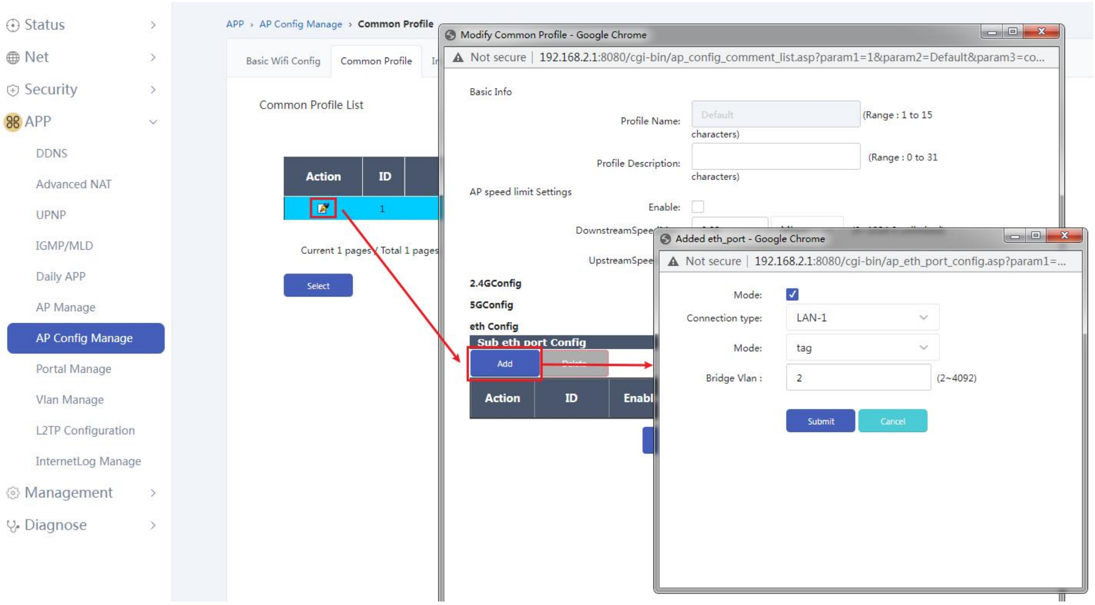
Client isolation : Disable

Broadcast SSID : Enable

Guest Mode : Enable

Bridge Vlan : Disabled VLAN

MaxAssociateNum : 32 The range is 0~32



192.168.2.1:8080/cgi-bin/ap_config_comment_list.asp?param1=1&param2=Default&param3=co...

Profile Name: Default (Range : 1 to 15 characters)

Profile Description: (Range : 0 to 31 characters)

192.168.2.1:8080/cgi-bin/ap_eth_port_config.asp?param1=...

Mode: ☑

Connection type: LAN-1

Mode: tag

Bridge Vlan : 2 (2~4092)

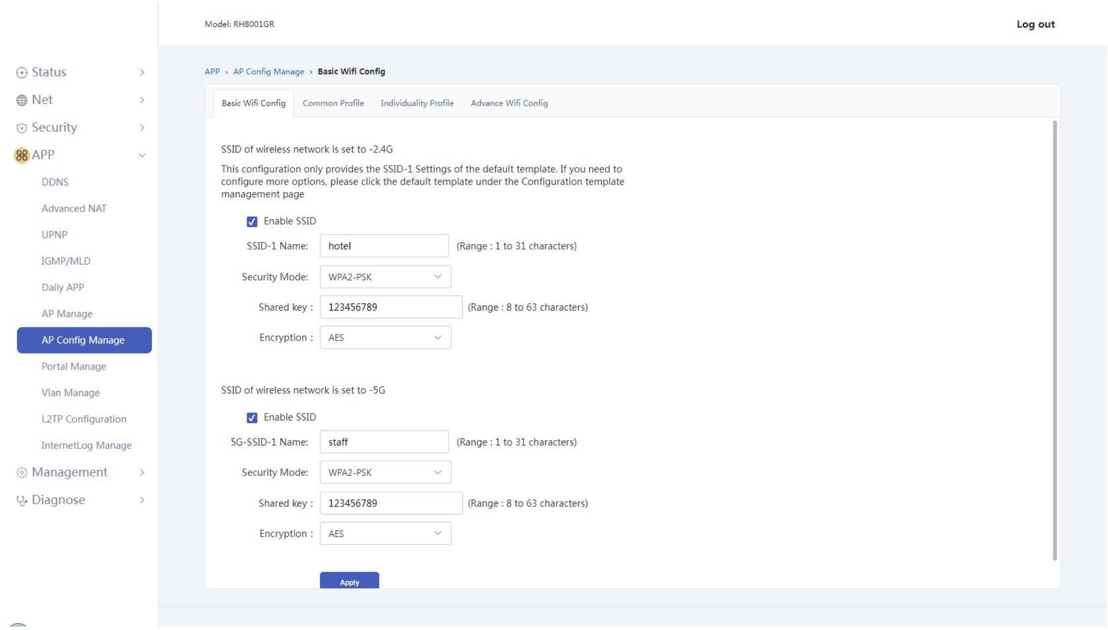
Parameter Description Table for Wi-Fi

Operating mode	Configuration parameters	Parameter description
Basic WiFi Config	Enable SSID	Single 2.4G/5G Wi-Fi on/off switch.
	SSID-1 Name	SSID-1 name.
	Security Mode	Security modes, including OPEN/WPA2-PSK/WPA3-SAE Transition, etc.
	Shared key	Password for SSID.
	Encryption	Encryption methods, including AES/TKIP/AES+TKIP,etc.
Basic Info	Profile Name	Profile name, range: 1 to 15 characters.
	Profile Description	Profile description, range: 0 to 31 characters.

AP speed limit Settings	DownstreamSpeedMax	Downstream maximum speed: 0~1024 (Mbps/Kbps selectable, 0 indicates unlimited)
	UpstreamSpeedMax	Upstream maximum speed: 0~1024 (Mbps/Kbps selectable, 0 indicates unlimited)
Basic Wireless Network Settings	Mode	This item is used to set the wireless working mode of the router. 2.4G:802.11b/g/n mixed mode is recommended. 5G:802.11ac/n/a mixed mode is recommended.
	Bandwidth	Wireless Channel Width. 2.4G Range: 20M, 40M, 5G Range:20M,40M.80M, 160M.
	Channel	The channel for data signal transmission with wireless signal as the transmission medium. If AUTO is selected, the terminal will automatically select a best channel according to the surrounding environment. 2.4G:Channel can choose 1~13 . 5G:Channel can choose 36/40/46/48/52/56/60/64 and so on
	TxPower	Wireless transmit power, it is recommended to keep the default value of 100%.
Modify 2.4G/5G_SSID	Enable SSID	Enable or disable this SSID.
	SSID Name	The name of this SSID. Range : 1 to 31 characters.
	Security Mode	Security modes, including OPEN/WPA2-PSK/WPA3-SAE Transition, etc.
	Shared Key	Password for SSID.
	Encryption	Encryption methods, including AES/TKIP/AES+TKIP,etc.
	Client isolation	Once the client isolation feature is enabled, devices connected to the

		same SSID will be unable to communicate with or access each other.
	Broadcast SSID	Enable or disable SSID broadcast. After enabling, devices can discover and connect to this SSID.
	Bridge VLAN	After selecting the Bridge VLAN parameter, the SSID will be bound to the Multi-VLAN instance. Devices connected to this SSID will obtain IP addresses from the Multi-VLAN instance's subnet.
	MaxAssociateNum	The maximum number of connected clients for this SSID. The range is 0~32.
Sub eth port Config	ID	Sub eth port config instance ID.
	Enable	ON or OFF sub eth port config
	Connection type	Select the AP LAN-side port to configure, range: LAN1, LAN2, LAN3, LAN4.
	Mode	Tag mode :transparent, tag, untag.
	Bridge VLAN	The VLAN bound to the specified port, range: 2-4094.

7.2.1 Basic WiFi Config



SSID of wireless network is set to -2.4G

This configuration only provides the SSID-1 Settings of the default template. If you need to configure more options, please click the default template under the Configuration template management page

☑ Enable SSID

SSID-1 Name: hotel (Range : 1 to 31 characters)

Security Mode: WPA2-PSK

Shared key : 123456789 (Range : 8 to 63 characters)

Encryption : AES

SSID of wireless network is set to -5G

☑ Enable SSID

5G-SSID-1 Name: staff (Range : 1 to 31 characters)

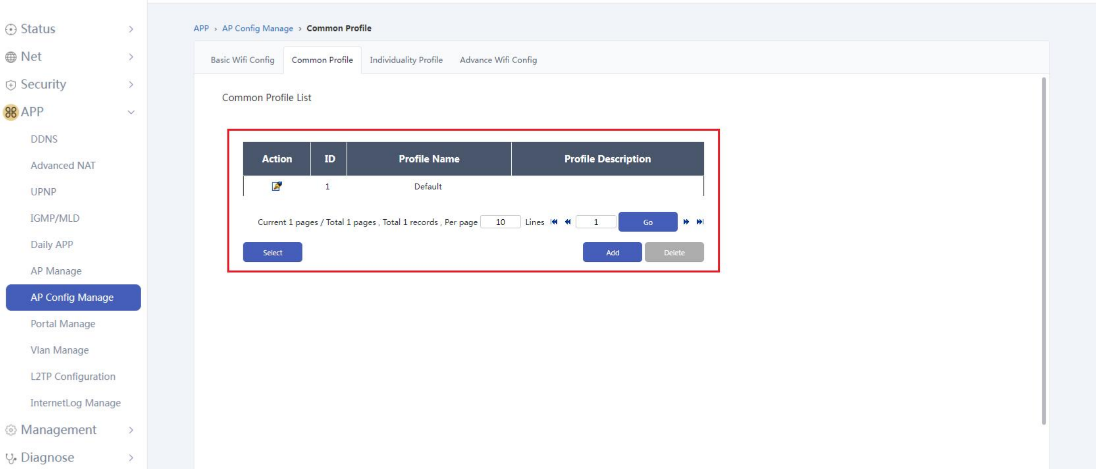
Security Mode: WPA2-PSK

Shared key : 123456789 (Range : 8 to 63 characters)

Encryption : AES

The basic wireless settings of the default profile can be configured, including 2.4G and 5G configurations: whether to enable SSID, SSID Name, Security Mode, Shared key and Encryption.

7.2.2 Common Profile



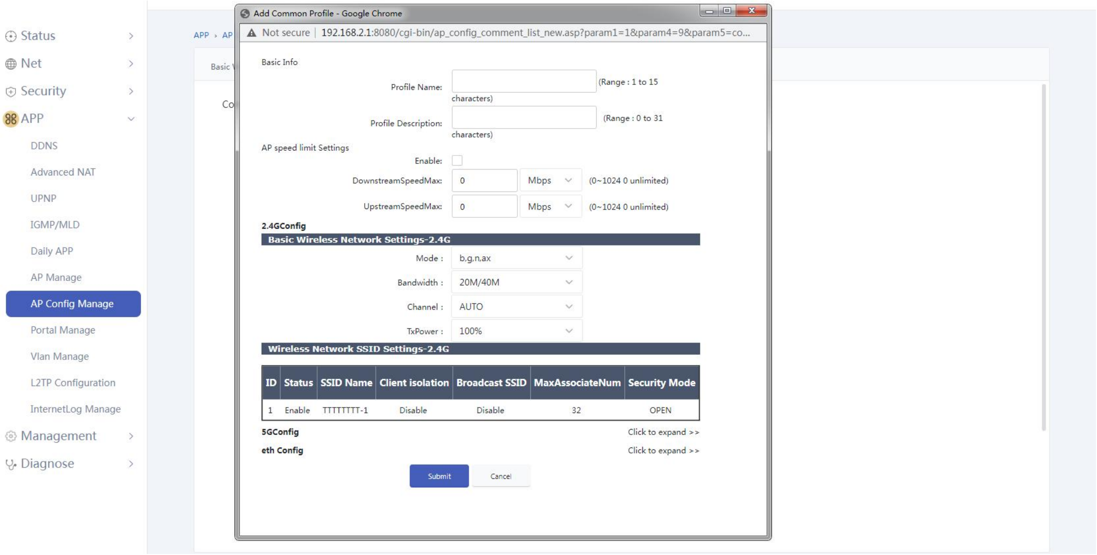
Common Profile List

Action	ID	Profile Name	Profile Description
✎	1	Default	

Current 1 pages / Total 1 pages , Total 1 records , Per page 10 Lines ⏮ ⏪ 1 Go ⏩ ⏭

Manage profiles by adding, deleting, modifying, and querying them.

a. Add Profile



Not secure | 192.168.2.1:8080/cgi-bin/ap_config_comment_list_new.asp?param1=1&param4=9&param5=co...

Basic Info

Profile Name: (Range : 1 to 15 characters)

Profile Description: (Range : 0 to 31 characters)

AP speed limit Settings

Enable: □

DownstreamSpeedMax: 0 Mbps (0~1024 0 unlimited)

UpstreamSpeedMax: 0 Mbps (0~1024 0 unlimited)

2.4GConfig

Basic Wireless Network Settings-2.4G

Mode : b,g,n,ax

Bandwidth : 20M/40M

Channel : AUTO

TxPower : 100%

Wireless Network SSID Settings-2.4G

ID	Status	SSID Name	Client isolation	Broadcast SSID	MaxAssociateNum	Security Mode
1	Enable	TTTTTTTT-1	Disable	Disable	32	OPEN

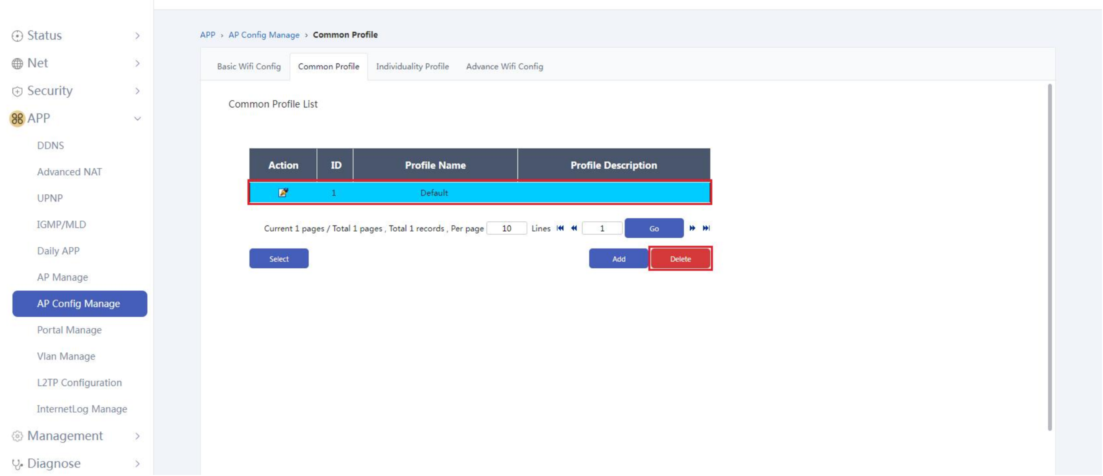
5GConfig Click to expand >>

eth Config Click to expand >>

When adding a profile, only the profile name and description can be set initially; specific wireless settings can only be modified after the profile is added.

b. Delete Profile

Profiles other than the default profile can be deleted.

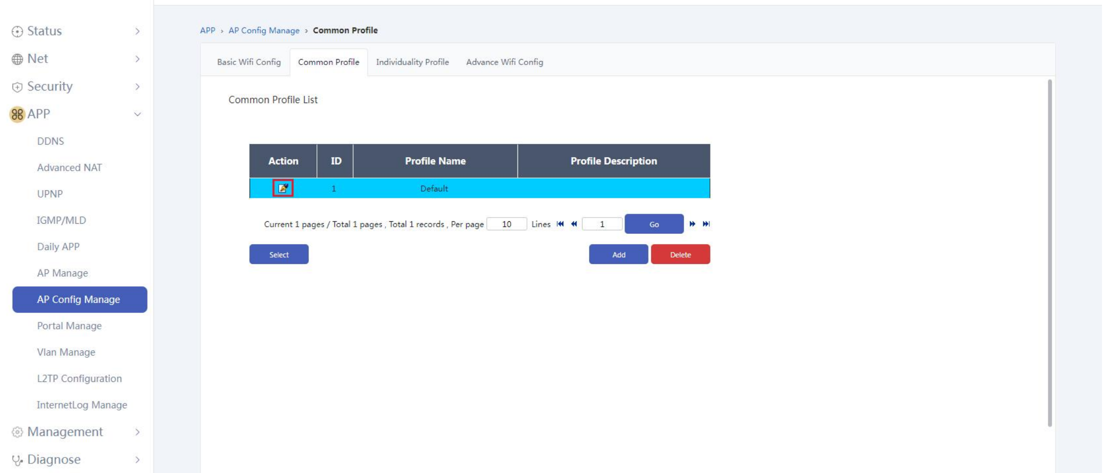


Common Profile List

Action	ID	Profile Name	Profile Description
📝	1	Default	

Current 1 pages / Total 1 pages , Total 1 records , Per page 10 Lines ⏮ ⏪ 1 Go ⏩ ⏭

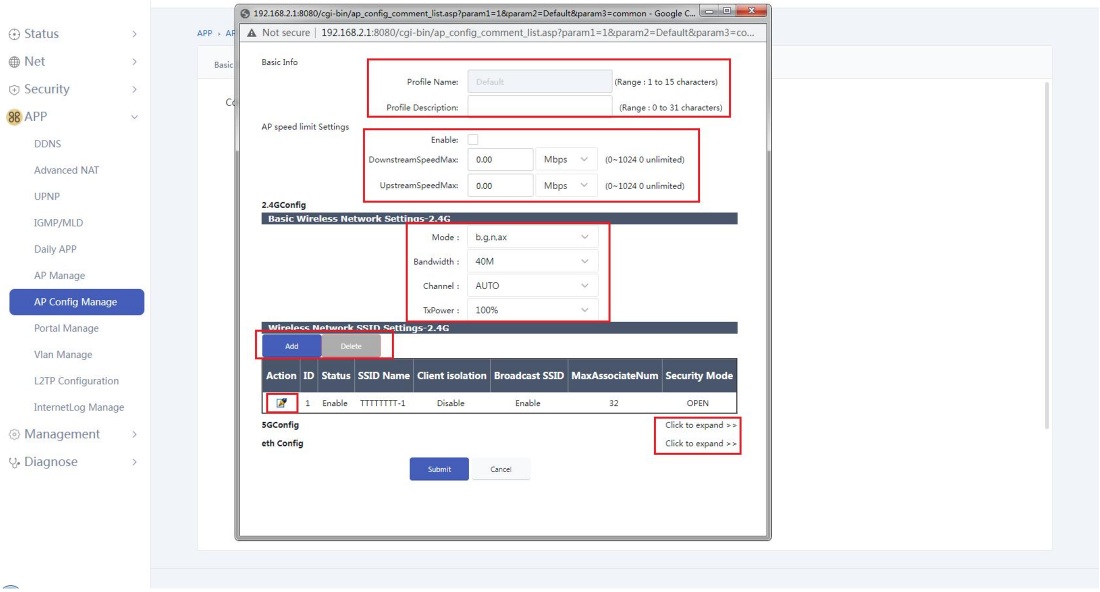
c. Modify Profile



Common Profile List

Action	ID	Profile Name	Profile Description
📝	1	Default	

Current 1 pages / Total 1 pages , Total 1 records , Per page 10 Lines ⏮ ⏪ 1 Go ⏩ ⏭



192.168.2.1:8080/cgi-bin/ap_config_comment_list.asp?param1=1&param2=Default&param3=common - Google C...

Not secure | 192.168.2.1:8080/cgi-bin/ap_config_comment_list.asp?param1=1&param2=Default&param3=co...

Basic Info

Profile Name: Default (Range : 1 to 15 characters)

Profile Description: (Range : 0 to 31 characters)

AP speed limit Settings

Enable: □

DownstreamSpeedMax: 0.00 Mbps (0~1024 0 unlimited)

UpstreamSpeedMax: 0.00 Mbps (0~1024 0 unlimited)

2.4GConfig

Basic Wireless Network Settings-2.4G

Mode : b,g,n,ax

Bandwidth : 40M

Channel : AUTO

TxPower : 100%

Wireless Network SSID Settings-2.4G

Add Delete

Action	ID	Status	SSID Name	Client isolation	Broadcast SSID	MaxAssociateNum	Security Mode
✎	1	Enable	TTTTTTTT-1	Disable	Enable	32	OPEN

5GConfig Click to expand >>

eth Config Click to expand >>

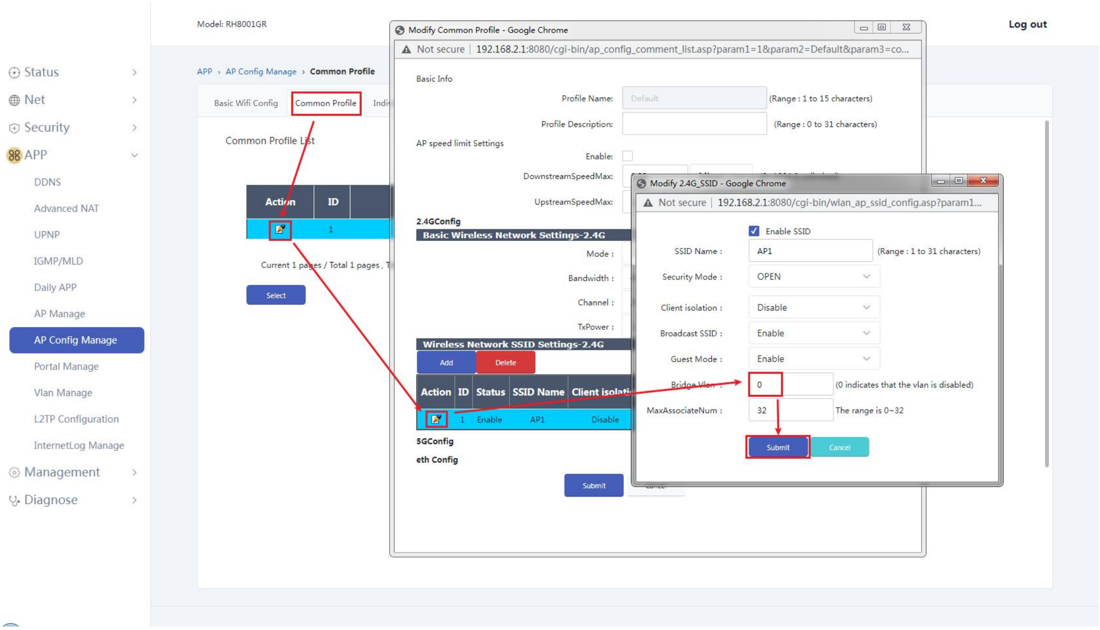
Submit Cancel

Modify the profile name (except for the default profile name), profile description, wireless configuration, and multiple SSIDs.

7.2.3 Multi-SSID Setup

7.2.3.1 SSID to VLAN Association

On the fourth line of the web configuration page, select "APP", choose "AP Config Manage", configure the general profile in the second column, select the "Default" profile, click "Edit", select the wireless network SSID setting 2.4G or 5G setting, and you can view the default SSID1 configuration; Click "Edit" and fill in the corresponding VLAN in "Bridge VLAN". The default value is 0, which means going to the default network segment 192.168.2.x/24. After making the changes, click "Submit".



Common Profile List

Action	ID
	1

Current 1 pages / Total 1 pages , T

Modify Common Profile - Google Chrome

Not secure | 192.168.2.1:8080/cgi-bin/ap_config_comment_list.asp?param1=1&param2=Default&param3=co...

Basic Info

Profile Name: Default (Range : 1 to 15 characters)

Profile Description: (Range : 0 to 31 characters)

AP speed limit Settings

Enable: □

DownstreamSpeedMax:

UpstreamSpeedMax:

2.4GConfig

Basic Wireless Network Settings-2.4G

Mode :

Bandwidth :

Channel :

TxPower :

Wireless Network SSID Settings-2.4G

Action	ID	Status	SSID Name	Client isolati
	1	Enable	AP1	Disable

5GConfig

eth Config

Modify 2.4G_SSID - Google Chrome

Not secure | 192.168.2.1:8080/cgi-bin/wlan_ap_ssid_config.asp?param1...

☑ Enable SSID

SSID Name : AP1 (Range : 1 to 31 characters)

Security Mode : OPEN

Client isolation : Disable

Broadcast SSID : Enable

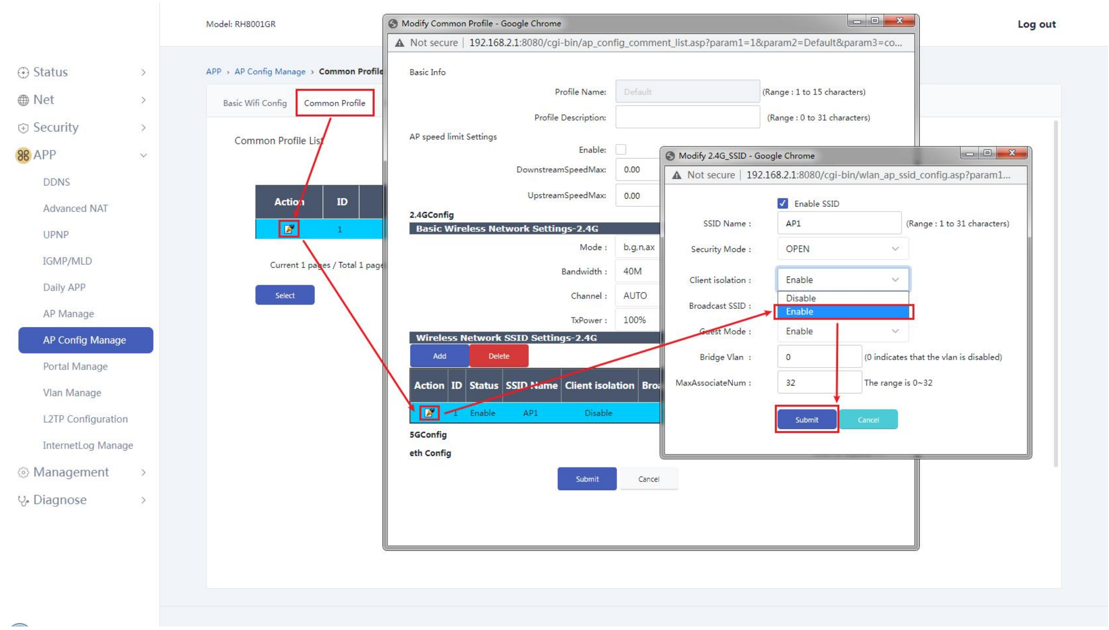
Guest Mode : Enable

Bridge Vlan : 0 (0 indicates that the vlan is disabled)

MaxAssociateNum : 32 The range is 0~32

7.2.3.2 Client Isolation

On the fourth line of the web configuration page, select "App", choose "AP Config Manage", configure the general profile in the second column, select the"Default" profile, click "Edit", select the wireless network SSID setting 2.4G or 5G setting, and you can view the default SSID1 configuration; Click "Edit", change the default setting from "Disable" to "Enable" in "Client isolation", then click "Submit" after modification.


Model: RH8001GR
Log out
Status
Net
Security
APP
DDNS
Advanced NAT
UPNP
IGMP/MLD
Daily APP
AP Manage
AP Config Manage
Portal Manage
Vlan Manage
L2TP Configuration
InternetLog Manage
Management
Diagnose
APP › AP Config Manage › Common Profile
Basic Wifi Config
Common Profile
Common Profile List
Action
ID
Current 1 pages / Total 1 pages
Select
Modify Common Profile - Google Chrome
Not secure | 192.168.2.1:8080/cgi-bin/ap_config_comment_list.asp?param1=1&param2=Default&param3=co...
Modify 2.4G_SSID - Google Chrome
Not secure | 192.168.2.1:8080/cgi-bin/wlan_ap_ssid_config.asp?param1...
Add
Delete
Submit
Cancel

Basic Info

Profile Name: Default (Range : 1 to 15 characters)

Profile Description: (Range : 0 to 31 characters)

AP speed limit Settings

Enable: □

DownstreamSpeedMax: 0.00

UpstreamSpeedMax: 0.00

2.4GConfig

Basic Wireless Network Settings-2.4G

Mode : b.g.n.ax

Bandwidth : 40M

Channel : AUTO

TxPower : 100%

Wireless Network SSID Settings-2.4G

Action	ID	Status	SSID Name	Client isolation	Bro
	1	Enable	AP1	Disable	

5GConfig

eth Config

☑ Enable SSID

SSID Name : AP1 (Range : 1 to 31 characters)

Security Mode : OPEN

Client isolation : Enable (Disable / Enable)

Broadcast SSID :

Guest Mode : Enable

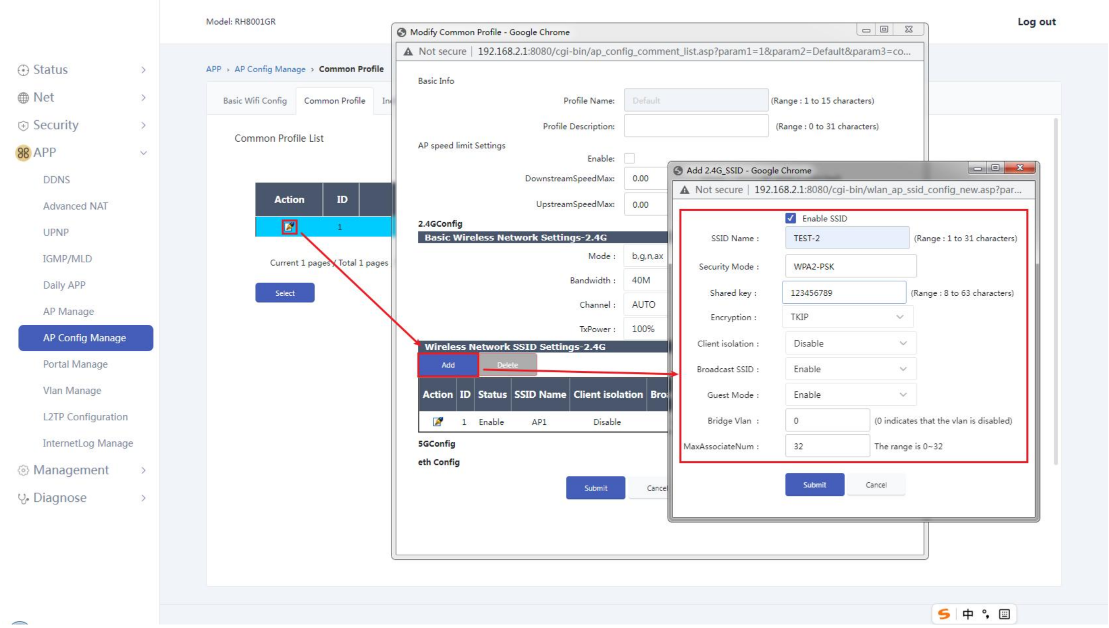
Bridge Vlan : 0 (0 indicates that the vlan is disabled)

MaxAssociateNum : 32 The range is 0~32

Once the client isolation feature is enabled, devices connected to the same SSID will be unable to communicate with or access each other.

7.2.3.3 Adding New SSID

On the fourth line of the web configuration page, select "APP", choose "AP Config Manage", configure the "Common Profile" in the second column, select the "Default" profile, click "Edit", select the wireless network SSID setting 2.4G or 5G setting, click "Add" to create SSID2, fill in the SSID parameters, and click "Submit" after modification; up to 4 SSIDs can be set.



Action	ID
	1

Current 1 pages / Total 1 pages

Modify Common Profile - Google Chrome

Not secure | 192.168.2.1:8080/cgi-bin/ap_config_comment_list.asp?param1=1&param2=Default&param3=co...

Basic Info

Profile Name: Default (Range : 1 to 15 characters)

Profile Description: (Range : 0 to 31 characters)

AP speed limit Settings

Enable: □

DownstreamSpeedMax: 0.00

UpstreamSpeedMax: 0.00

2.4GConfig

Basic Wireless Network Settings-2.4G

Mode : b.g.n.ax

Bandwidth : 40M

Channel : AUTO

TxPower : 100%

Wireless Network SSID Settings-2.4G

Action	ID	Status	SSID Name	Client isolation	Bro
	1	Enable	AP1	Disable	

5GConfig

eth Config

Add 2.4G_SSID - Google Chrome

Not secure | 192.168.2.1:8080/cgi-bin/wlan_ap_ssid_config_new.asp?par...

☑ Enable SSID

SSID Name : TEST-2 (Range : 1 to 31 characters)

Security Mode : WPA2-PSK

Shared key : 123456789 (Range : 8 to 63 characters)

Encryption : TKIP

Client isolation : Disable

Broadcast SSID : Enable

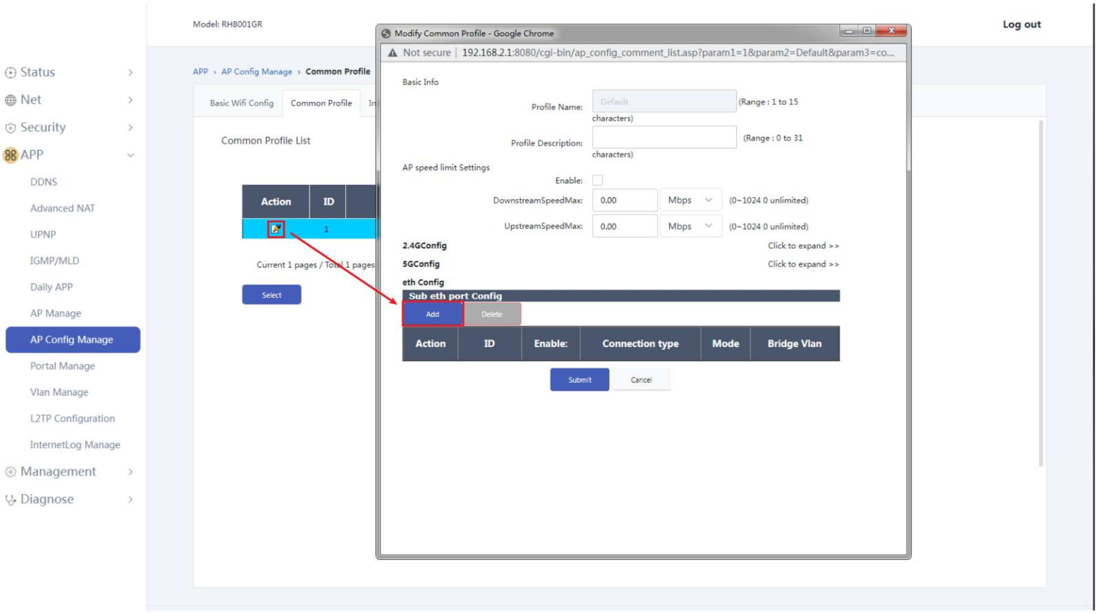
Guest Mode : Enable

Bridge Vlan : 0 (0 indicates that the vlan is disabled)

MaxAssociateNum : 32 The range is 0~32

7.2.3.4 Sub eth Port Config

Step 1: Click "Add ".



Action	ID
	1

Current 1 pages / Total 1 pages

Basic Info

Profile Name: Default (Range : 1 to 15 characters)

Profile Description: (Range : 0 to 31 characters)

AP speed limit Settings

Enable: □

DownstreamSpeedMax: 0.00 Mbps (0~1024 0 unlimited)

UpstreamSpeedMax: 0.00 Mbps (0~1024 0 unlimited)

2.4GConfig

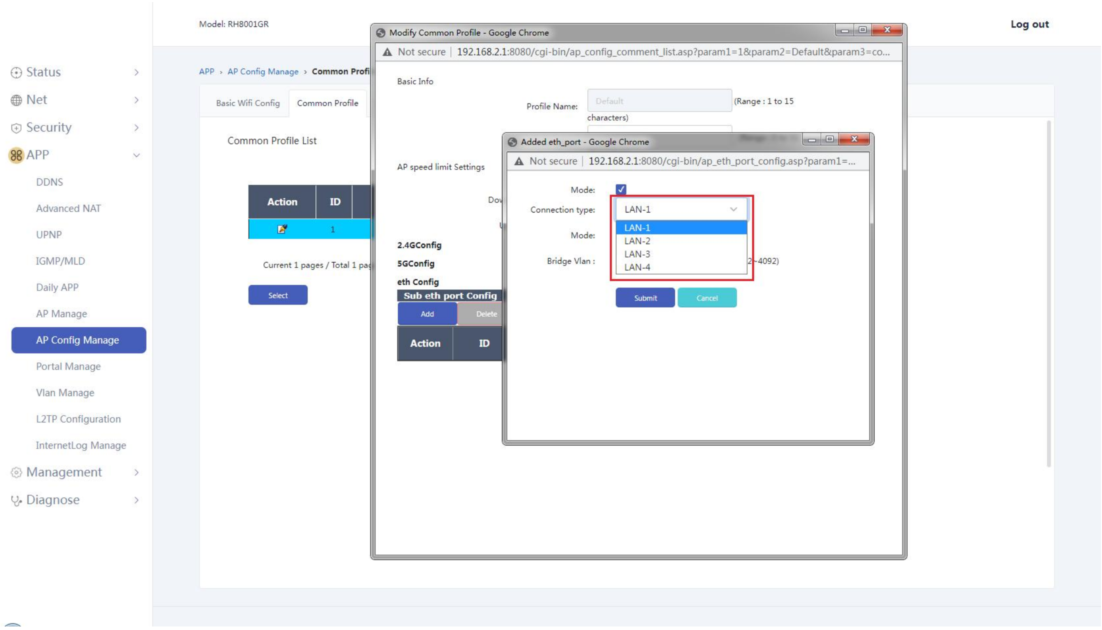
5GConfig

eth Config

Sub eth port Config

Action	ID	Enable:	Connection type	Mode	Bridge Vlan

Step 2: Select the LAN interface that you want to set up.



192.168.2.1:8080/cgi-bin/ap_config_comment_list.asp?param1=1&param2=Default&param3=co...

Profile Name: Default (Range : 1 to 15 characters)

192.168.2.1:8080/cgi-bin/ap_eth_port_config.asp?param1=...

Mode: ☑

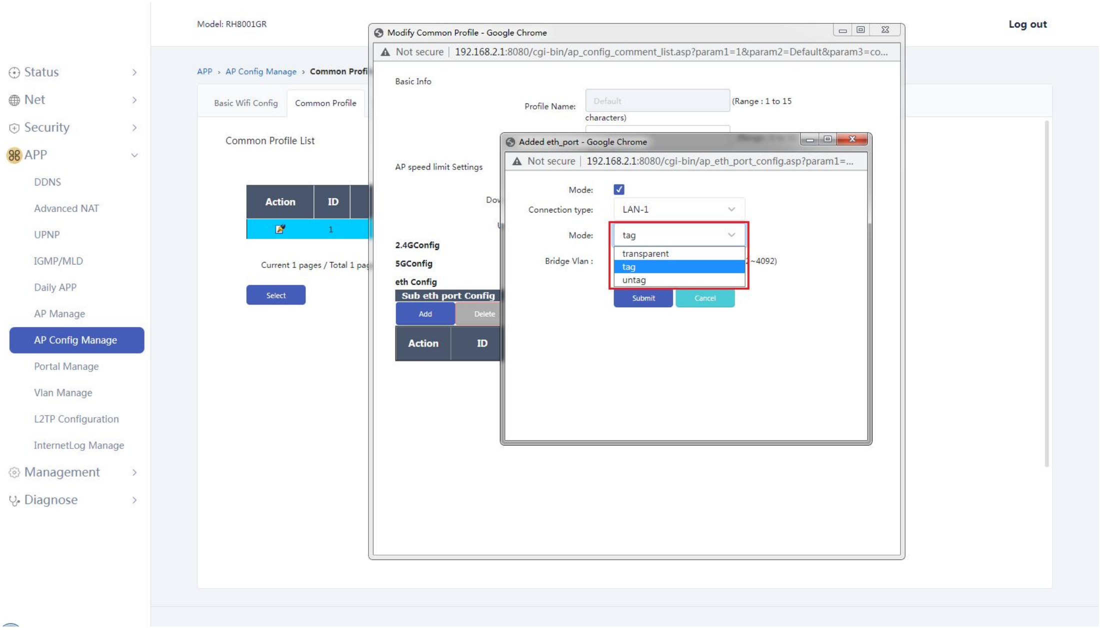
Connection type: LAN-1

LAN-1
LAN-2
LAN-3
LAN-4

Mode:

Bridge Vlan : 2~4092)

Step 3: Select a mode.



192.168.2.1:8080/cgi-bin/ap_config_comment_list.asp?param1=1&param2=Default&param3=co...

Profile Name: Default (Range : 1 to 15 characters)

192.168.2.1:8080/cgi-bin/ap_eth_port_config.asp?param1=...

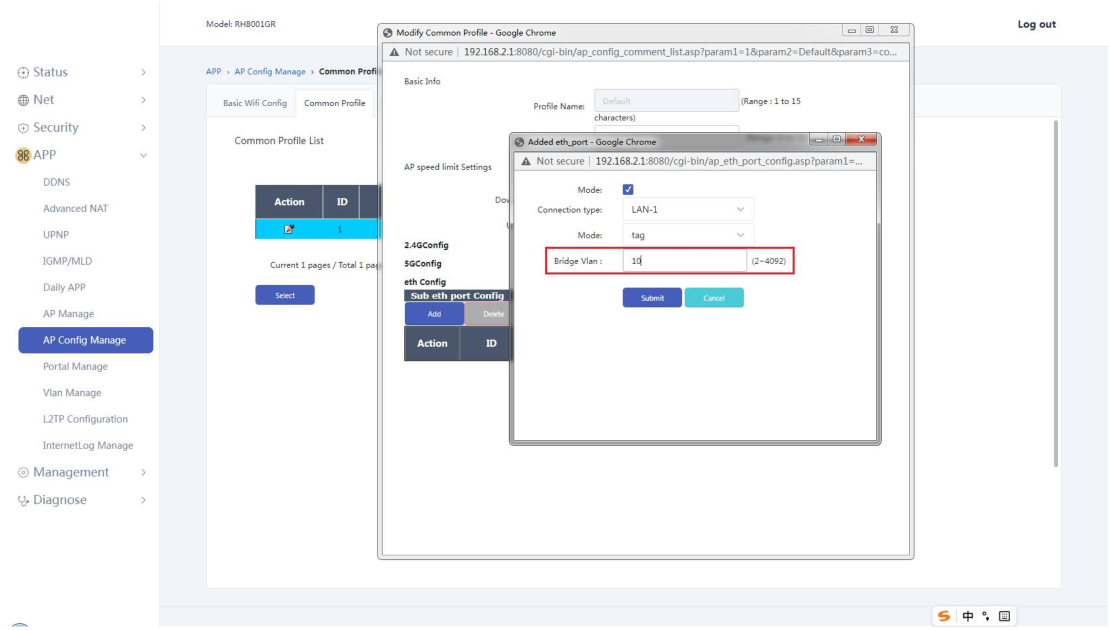
Mode: ☑

Connection type: LAN-1

Mode: tag

Bridge Vlan : ~4092)

Step 4: Set the bridge VLAN ID.



Profile Name: Default (Range : 1 to 15 characters)

Mode: ☑

Connection type: LAN-1

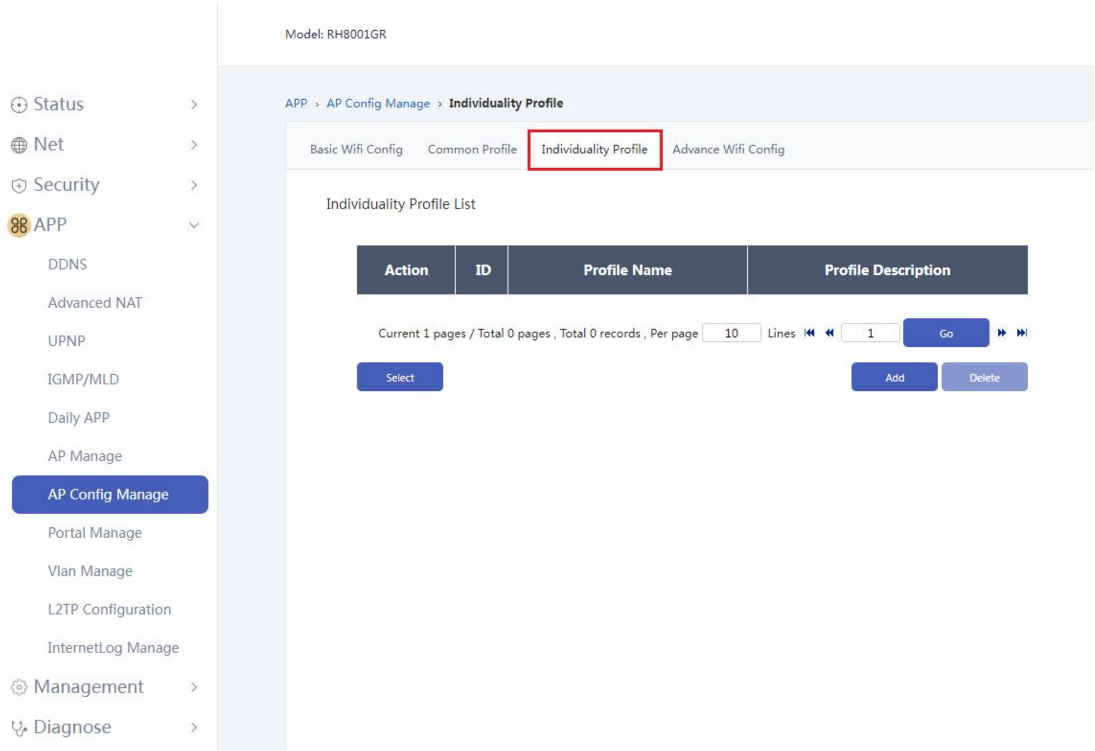
Mode: tag

Bridge Vlan : 10 (2~4092)

Note: The configured Bridged VLAN ID must have been created in the Multi-VLAN management for the configuration to take effect.

Step 5: Click "Submit" to complete the settings.

7.2.4 Individuality Profile

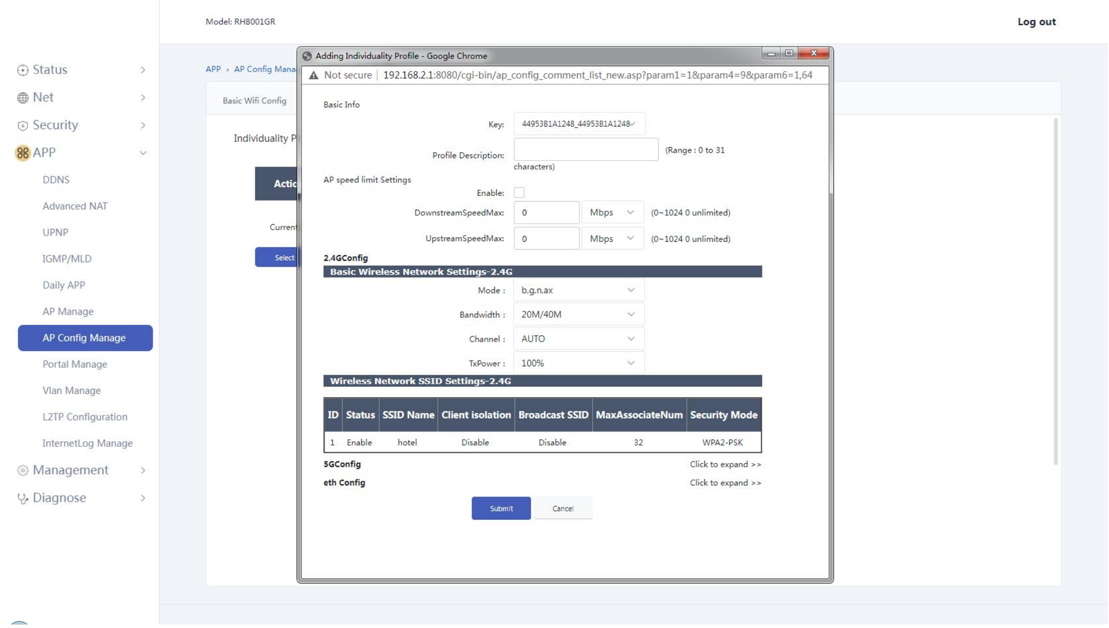


Individuality Profile List

Action	ID	Profile Name	Profile Description

Current 1 pages / Total 0 pages , Total 0 records , Per page 10 Lines 1

◆Add Profile



Basic Info

Key: 44953B1A1248_44953B1A1248

Profile Description: (Range : 0 to 31 characters)

AP speed limit Settings

Enable: □

DownstreamSpeedMax: 0 Mbps (0~1024 0 unlimited)

UpstreamSpeedMax: 0 Mbps (0~1024 0 unlimited)

2.4GConfig

Basic Wireless Network Settings-2.4G

Mode : b,g,n,ax

Bandwidth : 20M/40M

Channel : AUTO

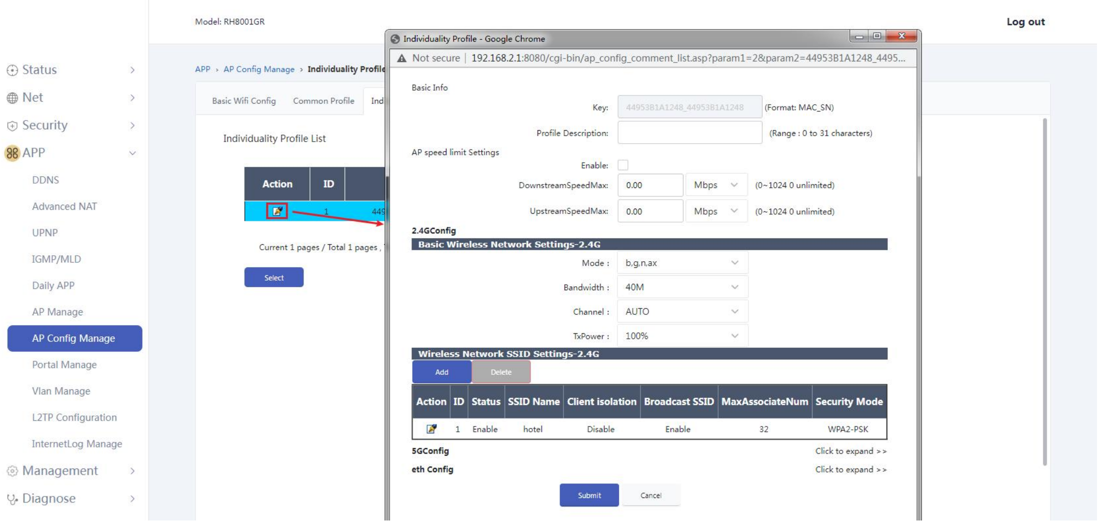
TxPower : 100%

Wireless Network SSID Settings-2.4G

ID	Status	SSID Name	Client isolation	Broadcast SSID	MaxAssociateNum	Security Mode
1	Enable	hotel	Disable	Disable	32	WPA2-PSK

Personalized profiles are only for individual APs, with the key being mac_sn. These profiles can only be bound to the corresponding AP.

◆Modify Profile



Basic Info

Key: 44953B1A1248_44953B1A1248 (Format: MAC_SN)

Profile Description: (Range : 0 to 31 characters)

AP speed limit Settings

Enable: □

DownstreamSpeedMax: 0.00 Mbps (0~1024 0 unlimited)

UpstreamSpeedMax: 0.00 Mbps (0~1024 0 unlimited)

2.4GConfig

Basic Wireless Network Settings-2.4G

Mode : b,g,n,ax

Bandwidth : 40M

Channel : AUTO

TxPower : 100%

Wireless Network SSID Settings-2.4G

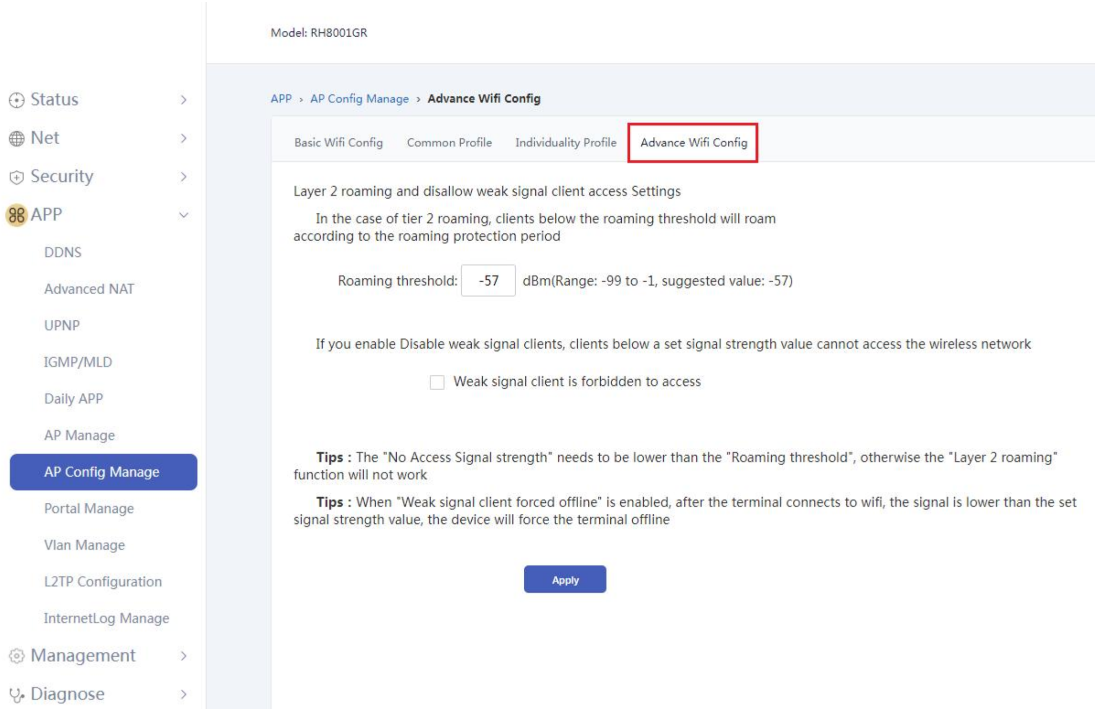
Action	ID	Status	SSID Name	Client isolation	Broadcast SSID	MaxAssociateNum	Security Mode
📝	1	Enable	hotel	Disable	Enable	32	WPA2-PSK

5GConfig Click to expand > >

eth Config Click to expand > >

7.2.5 Advance Wi-Fi Config

Supports roaming threshold and blocking weak-signal client access.



Layer 2 roaming and disallow weak signal client access Settings

In the case of tier 2 roaming, clients below the roaming threshold will roam according to the roaming protection period

Roaming threshold: -57 dBm(Range: -99 to -1, suggested value: -57)

If you enable Disable weak signal clients, clients below a set signal strength value cannot access the wireless network

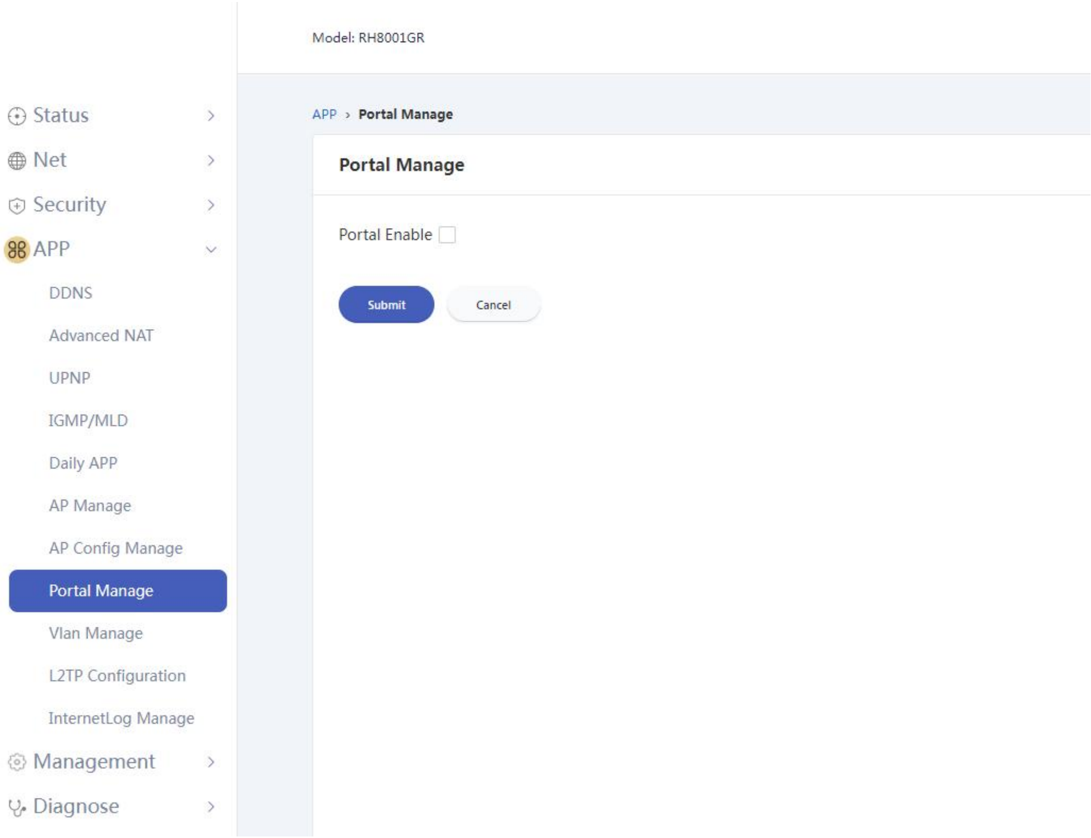
□ Weak signal client is forbidden to access

Tips : The "No Access Signal strength" needs to be lower than the "Roaming threshold", otherwise the "Layer 2 roaming" function will not work

Tips : When "Weak signal client forced offline" is enabled, after the terminal connects to wifi, the signal is lower than the set signal strength value, the device will force the terminal offline

7.3 Portal Manage

Click on the menu "APP -> Portal manage" to enter the Portal management page as illustrated in the figure below.



Model: RH8001GR

APP › Portal Manage

Portal Manage

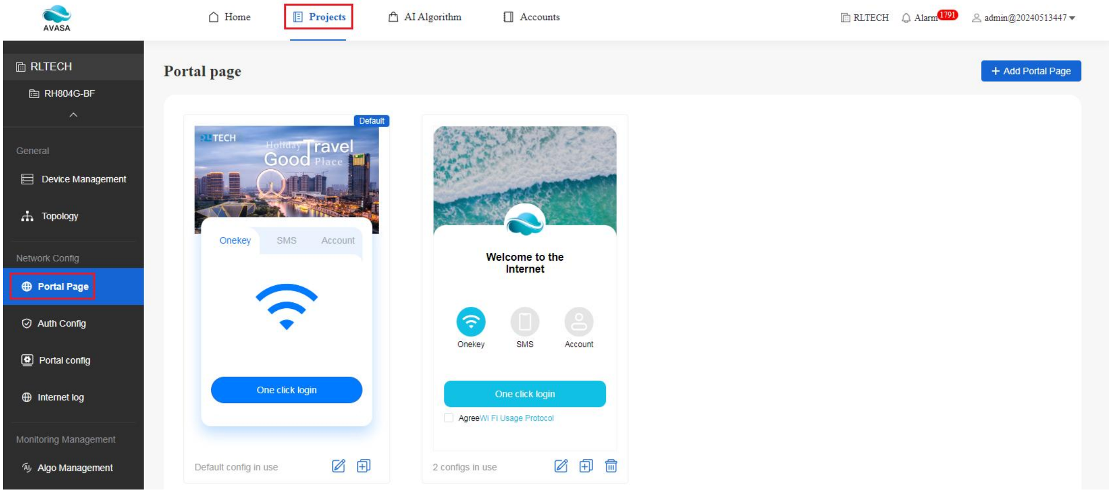
Portal Enable □

After enabling Portal, access terminals will be authenticated, and they can access the internet after successful authentication.

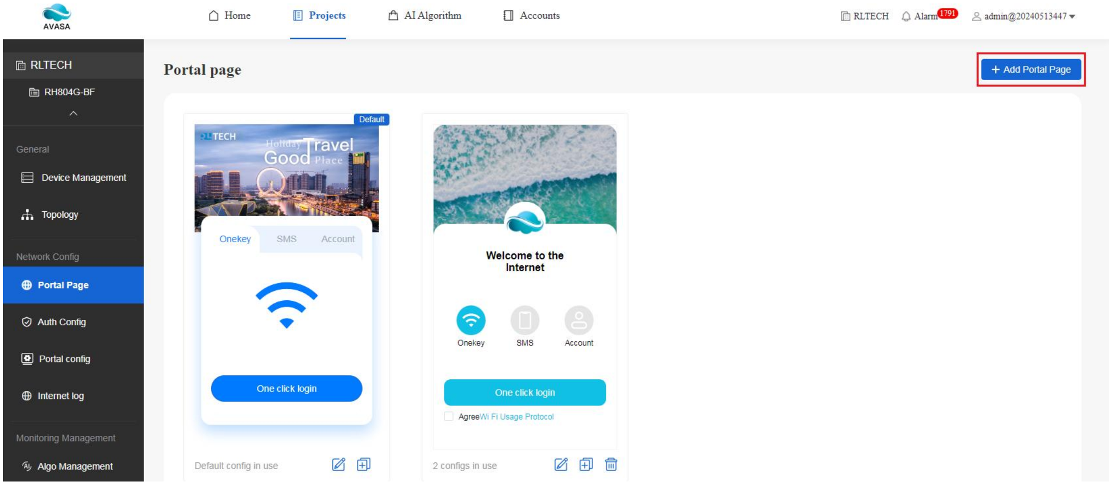
Note: The device must be added in AVASA first before proceeding with subsequent operations. Refer to section 8.1.

7.3.1 Adding a Portal Page on the AVASA

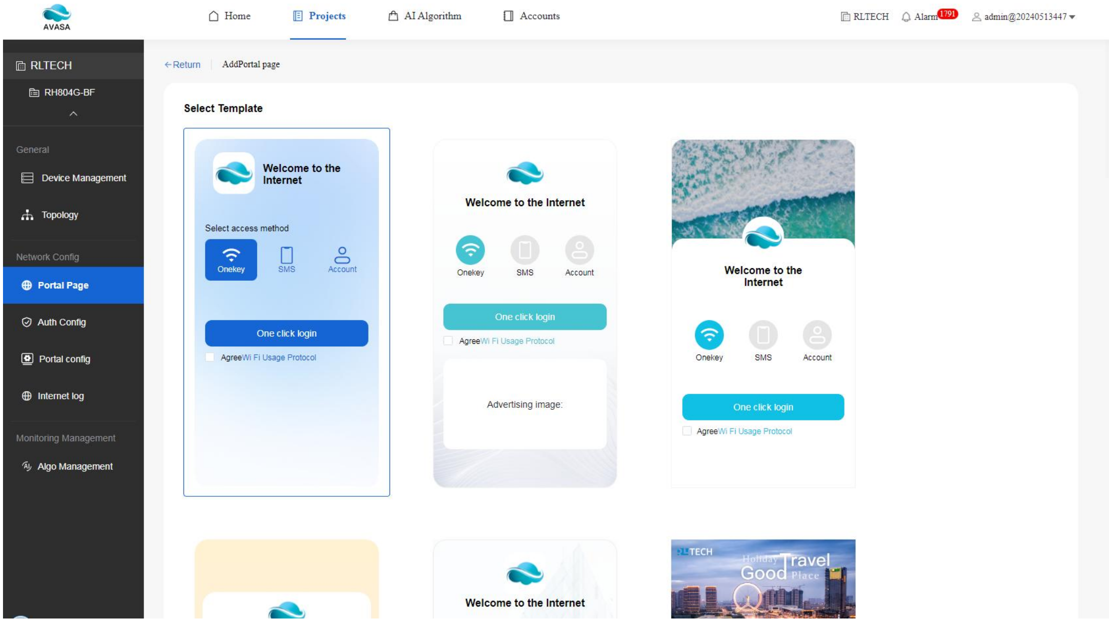
Step 1: Click on the menu "Projects -> Portal Page" to enter the Portal page.

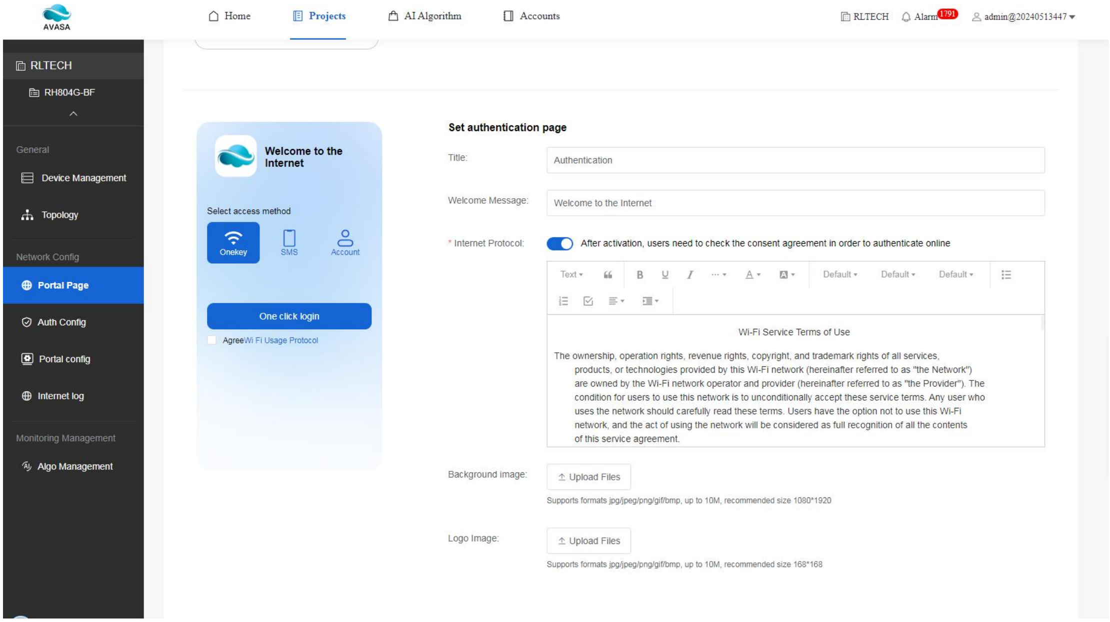


Step 2: Click the "+ Add Portal Page" button at the top right corner to enter the Portal configuration page.



Step 3: Select the Portal page authentication profile or design a custom authentication profile, as shown in the figure.


AVASA
Home
Projects
AI Algorithm
Accounts
RLTECH
Alarm 1791
admin@20240513447
RLTECH
RH804G-BF
General
Device Management
Topology
Network Config
Portal Page
Auth Config
Portal config
Internet log
Monitoring Management
Algo Management
← Return
AddPortal page
Select Template
Welcome to the Internet
Select access method
Onekey
SMS
Account
One click login
Agree Wi Fi Usage Protocol
Welcome to the Internet
Onekey
SMS
Account
One click login
Agree Wi Fi Usage Protocol
Advertising image:
Welcome to the Internet
Onekey
SMS
Account
One click login
Agree Wi Fi Usage Protocol
Welcome to the Internet
RLTECH
Holiday Travel
Good Place



Set authentication page

Title: Authentication

Welcome Message: Welcome to the Internet

* Internet Protocol: After activation, users need to check the consent agreement in order to authenticate online

Wi-Fi Service Terms of Use

The ownership, operation rights, revenue rights, copyright, and trademark rights of all services, products, or technologies provided by this Wi-Fi network (hereinafter referred to as "the Network") are owned by the Wi-Fi network operator and provider (hereinafter referred to as "the Provider"). The condition for users to use this network is to unconditionally accept these service terms. Any user who uses the network should carefully read these terms. Users have the option not to use this Wi-Fi network, and the act of using the network will be considered as full recognition of all the contents of this service agreement.

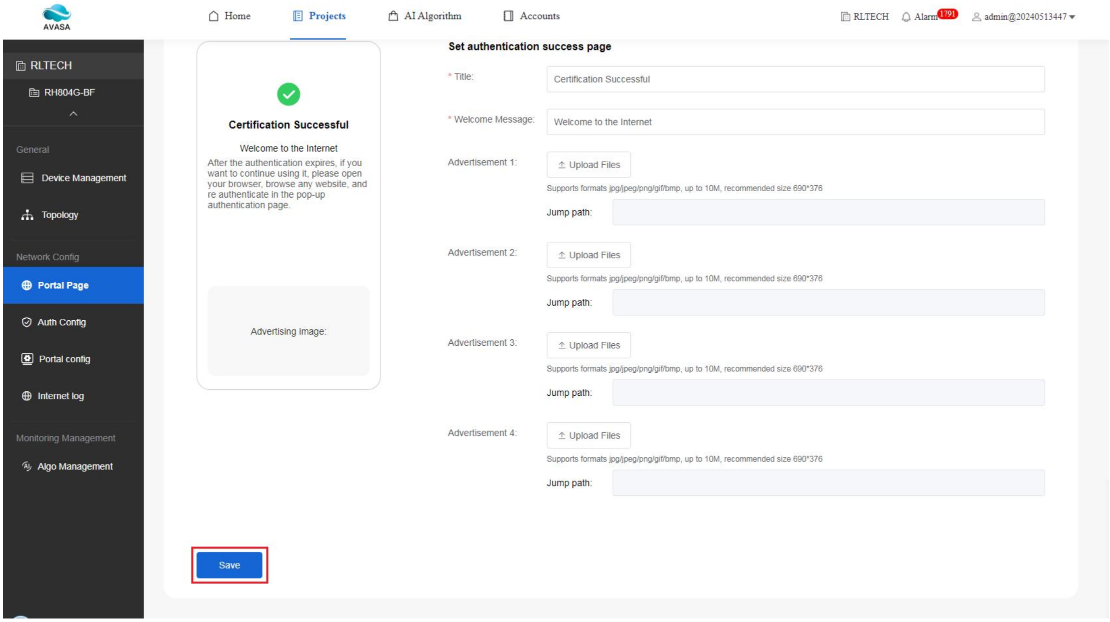
Background image: Upload Files

Supports formats jpg/jpeg/png/gif/bmp, up to 10M, recommended size 1080*1920

Logo Image: Upload Files

Supports formats jpg/jpeg/png/gif/bmp, up to 10M, recommended size 168*168

Step 4: Click "Save" to complete adding the Portal page.



Certification Successful

Welcome to the Internet

After the authentication expires, if you want to continue using it, please open your browser, browse any website, and re authenticate in the pop-up authentication page.

Advertising image:

Set authentication success page

* Title: Certification Successful

* Welcome Message: Welcome to the Internet

Advertisement 1: Upload Files

Supports formats jpg/jpeg/png/gif/bmp, up to 10M, recommended size 690*376

Jump path:

Advertisement 2: Upload Files

Supports formats jpg/jpeg/png/gif/bmp, up to 10M, recommended size 690*376

Jump path:

Advertisement 3: Upload Files

Supports formats jpg/jpeg/png/gif/bmp, up to 10M, recommended size 690*376

Jump path:

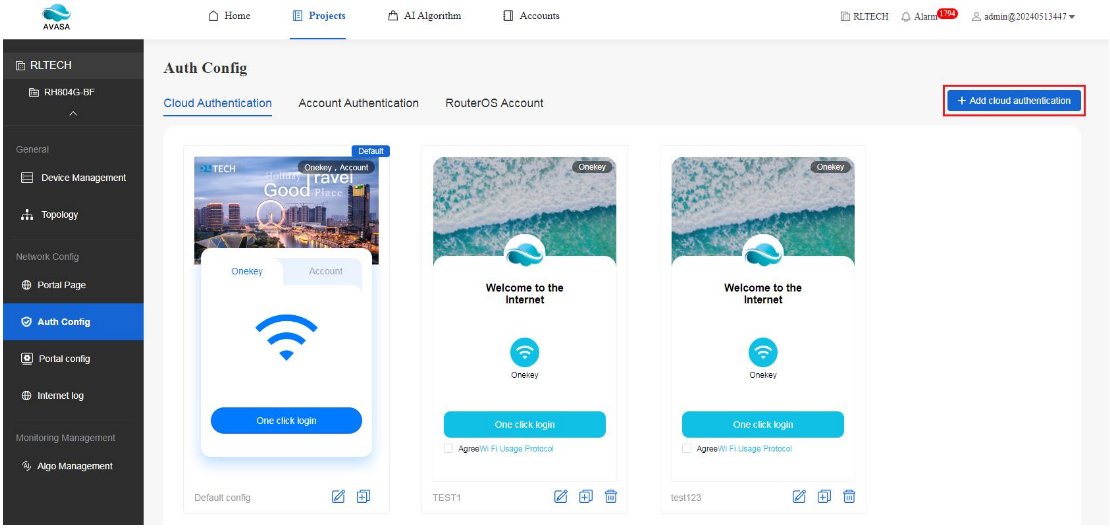
Advertisement 4: Upload Files

Supports formats jpg/jpeg/png/gif/bmp, up to 10M, recommended size 690*376

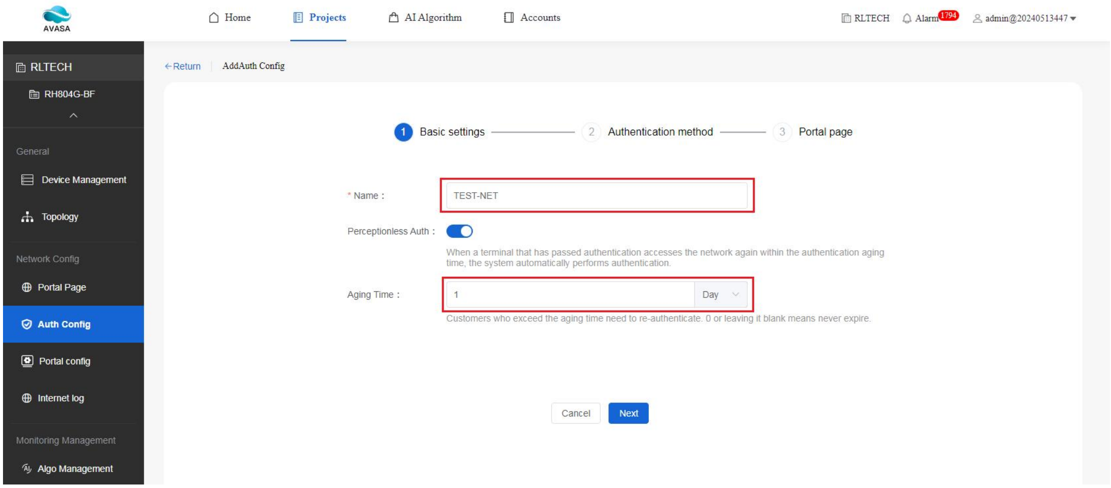
Jump path:

7.3.2 Portal Auth Config

Step 1: Click on "Projects -> Auth config" then click the "+ Add cloud authentication" button at the top right corner to enter the cloud authentication configuration page as illustrated in the figure below.



a.Fill in the authentication name. If seamless authentication is enabled, set the authentication aging time, then click "Next".



* Name : TEST-NET

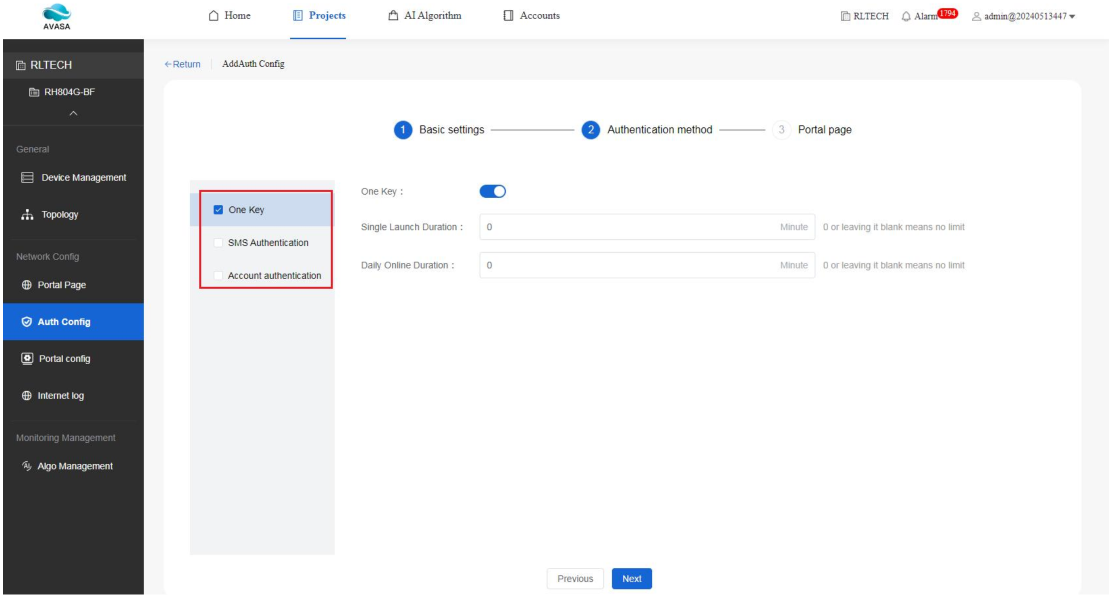
Perceptionless Auth : ●

When a terminal that has passed authentication accesses the network again within the authentication aging time, the system automatically performs authentication.

Aging Time : 1 Day

Customers who exceed the aging time need to re-authenticate. 0 or leaving it blank means never expire.

b.Select one of the three authentication methods: "One Key", "SMS Authentication", or "Account Authentication", then click "Next".



☑ One Key

□ SMS Authentication

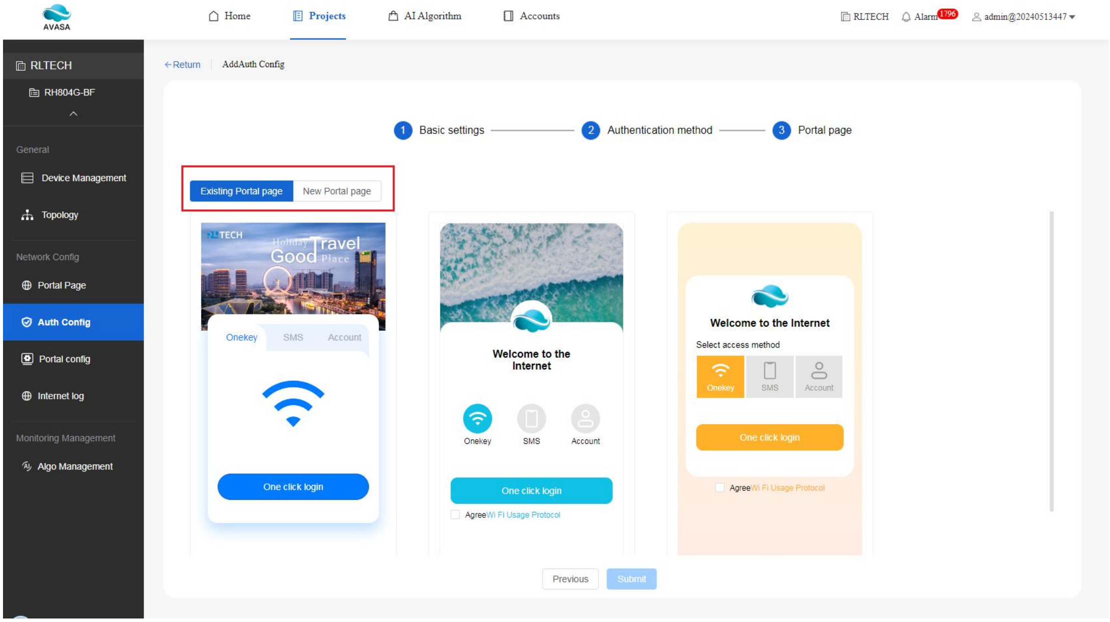
□ Account authentication

One Key : ●

Single Launch Duration : 0 Minute 0 or leaving it blank means no limit

Daily Online Duration : 0 Minute 0 or leaving it blank means no limit

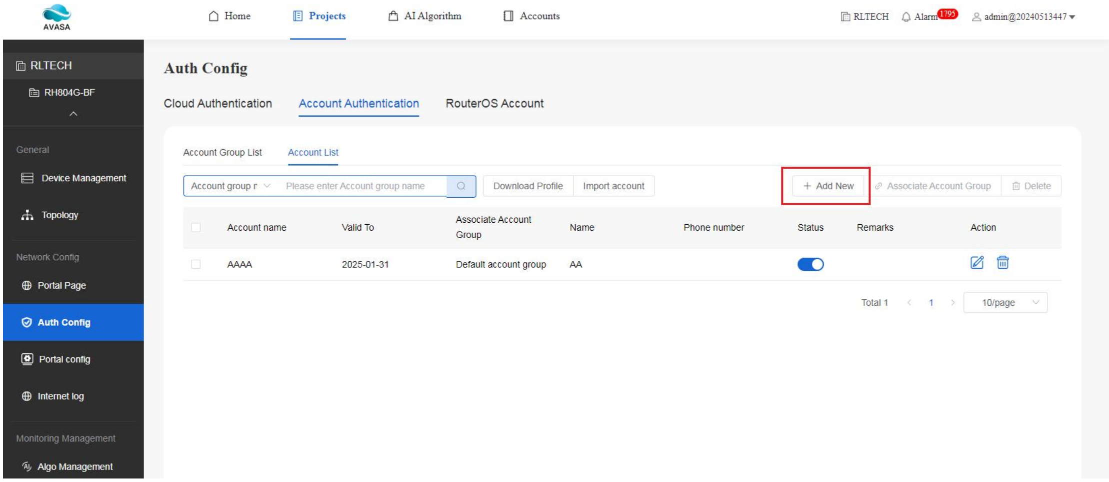
c.Choose an existing Portal page binding or create a new Portal page binding for the authentication configuration, and click "Submit" to complete adding cloud authentication.



Step 2: Add Account Authentication

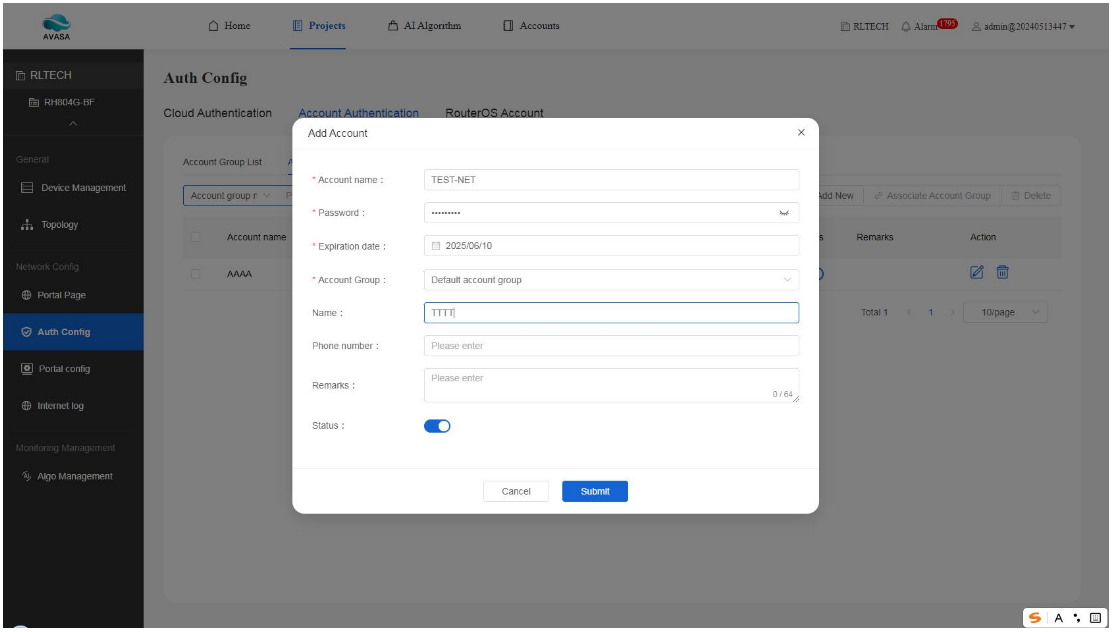
Note: For account authentication, users log in with a username and password to use Wi-Fi internet.

a.Click on "Auth Configuration -> Account Authentication -> Account List" to enter the account management page, and click "+ Add New".



	Account name	Valid To	Associate Account Group	Name	Phone number	Status	Remarks	Action
□	AAAA	2025-01-31	Default account group	AA		●		

b.Set the relevant account information, click "Submit" to complete adding the account.



Add Account

* Account name : TEST-NET

* Password : •••••••••

* Expiration date : 2025/06/10

* Account Group : Default account group

Name : TTTT

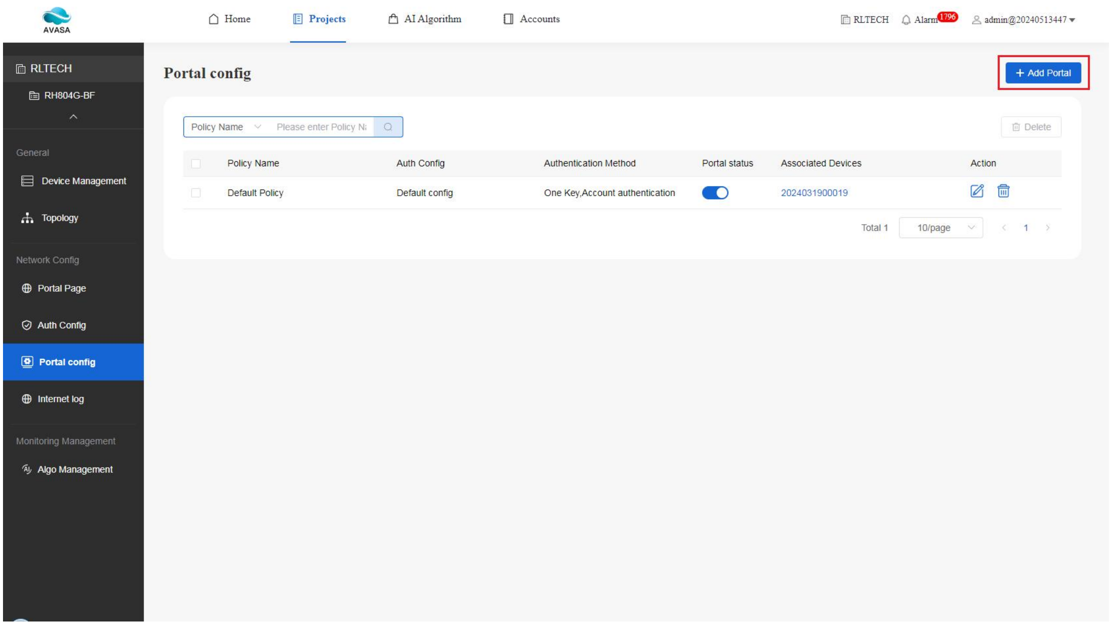
Phone number : Please enter

Remarks : Please enter 0 / 64

Status : ●

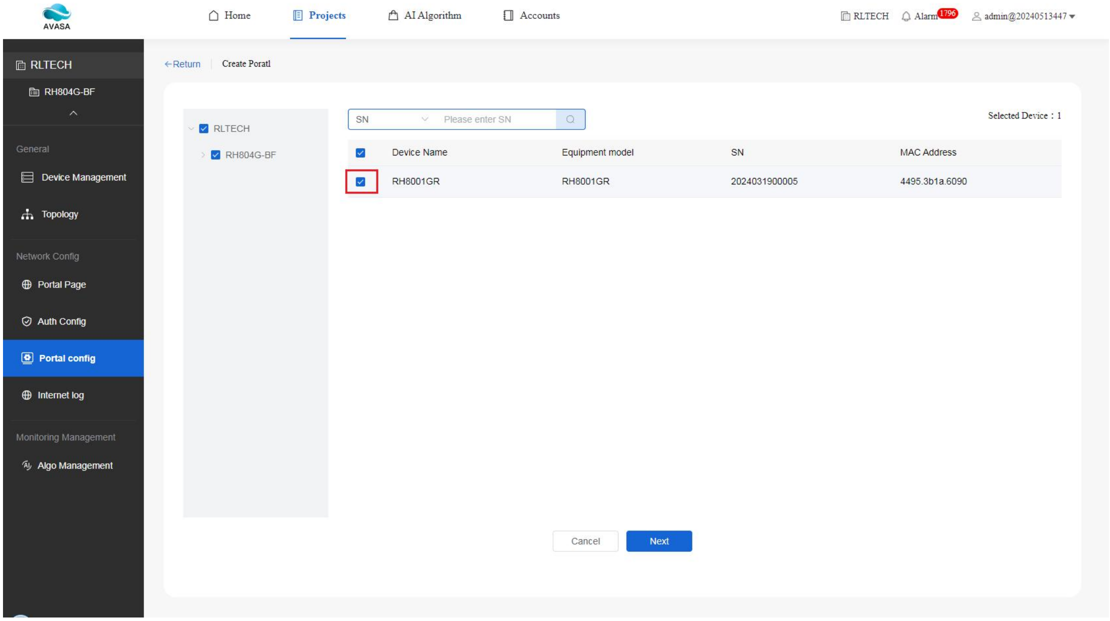
Step 3: Portal Configuration

a.Click on "Projects -> Portal config" to enter the Portal configuration page, and click "+ Add Portal."



	Policy Name	Auth Config	Authentication Method	Portal status	Associated Devices	Action
□	Default Policy	Default config	One Key,Account authentication	●	2024031900019	

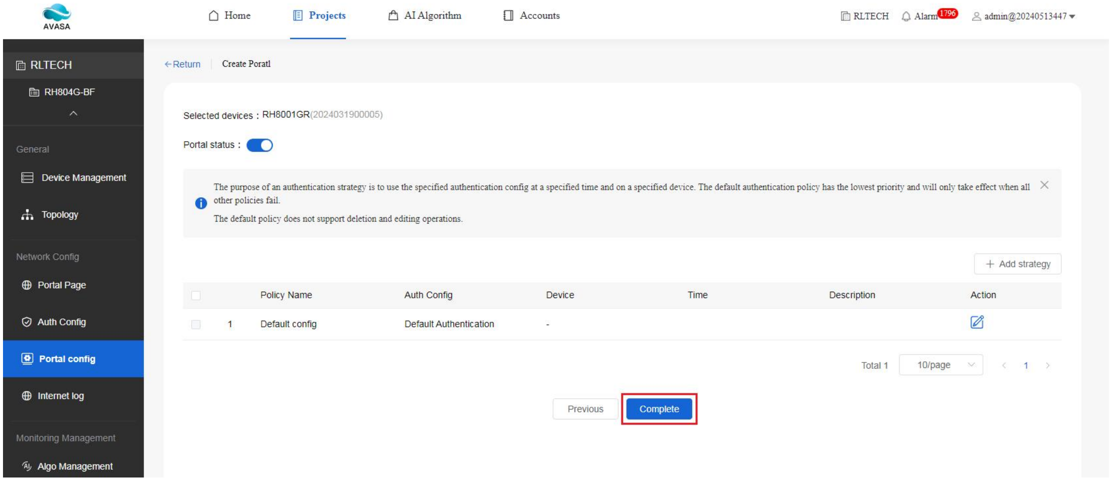
b.Check the devices that need Portal enabled and click "Next".



Selected Device：1

☑	Device Name	Equipment model	SN	MAC Address
☑	RH8001GR	RH8001GR	2024031900005	4495.3b1a.6090

c.Set the Portal authentication policy and click "Complete" to enable Portal authentication.



Selected devices：RH8001GR(2024031900005)

Portal status：●

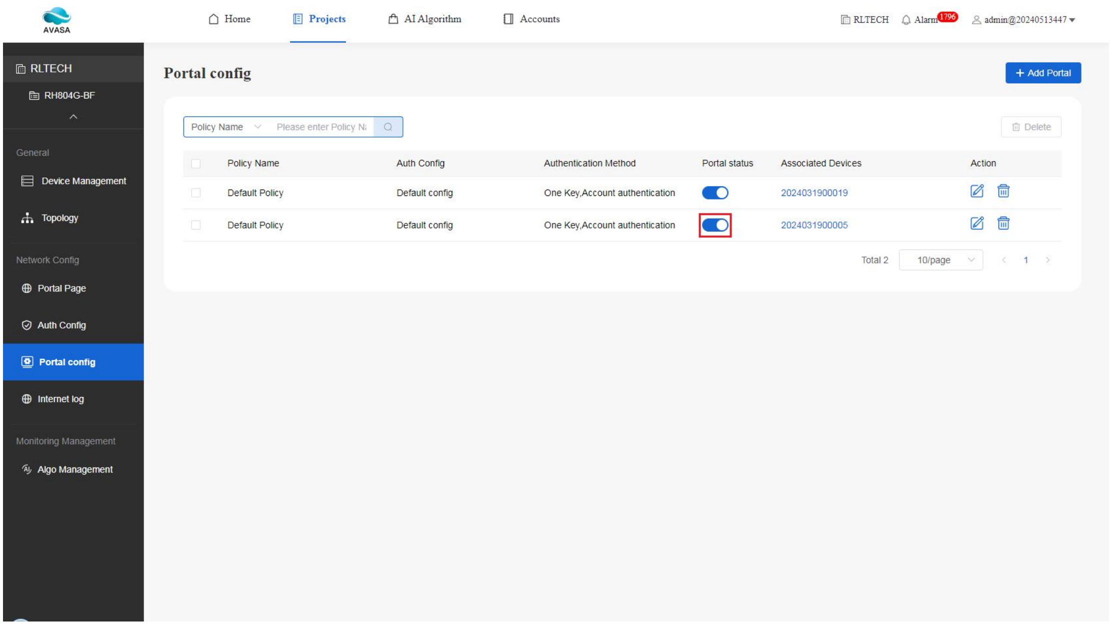
The purpose of an authentication strategy is to use the specified authentication config at a specified time and on a specified device. The default authentication policy has the lowest priority and will only take effect when all other policies fail.

The default policy does not support deletion and editing operations.

□		Policy Name	Auth Config	Device	Time	Description	Action
□	1	Default config	Default Authentication	-			✎

7.3.3 Disabling Portal Authentication on the AVASA

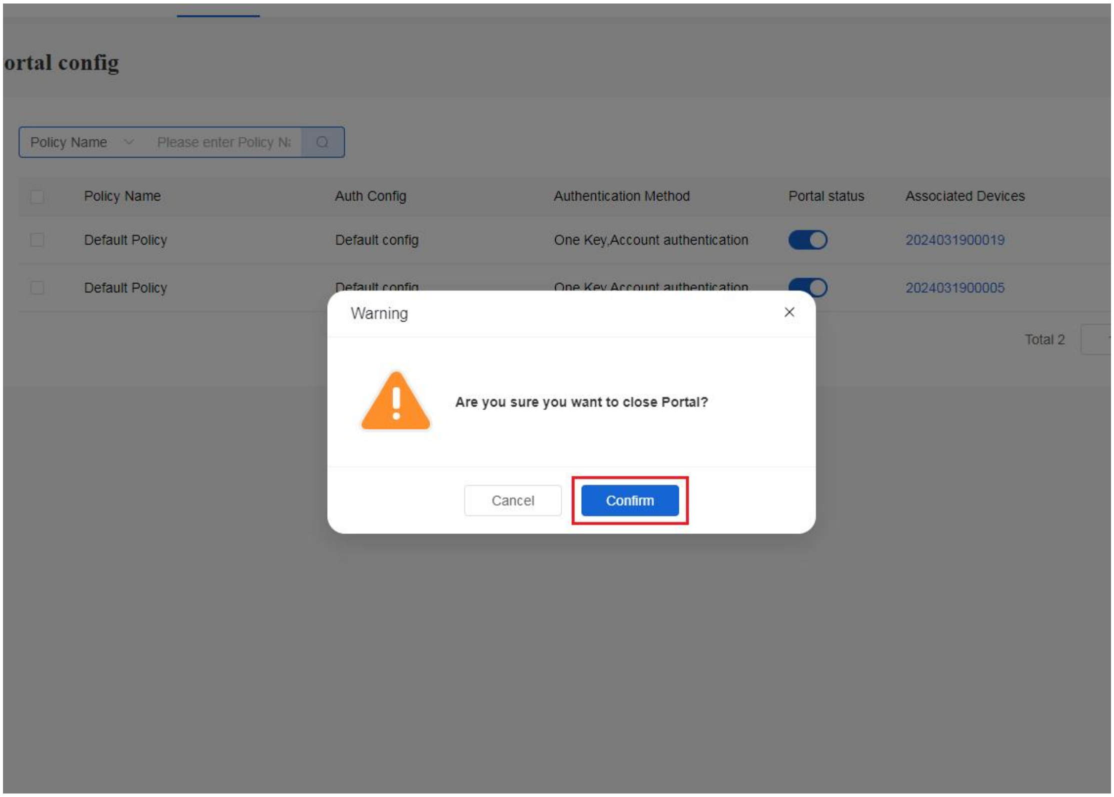
Step 1: On the Portal configuration page, select the device for which you want to disable authentication and click the Portal switch as illustrated in the figure below.



Portal config

□	Policy Name	Auth Config	Authentication Method	Portal status	Associated Devices	Action
□	Default Policy	Default config	One Key,Account authentication	●	2024031900019	
□	Default Policy	Default config	One Key,Account authentication	●	2024031900005	

Step 2: In the pop-up window, click "Confirm" to disable Portal authentication.



ortal config

□	Policy Name	Auth Config	Authentication Method	Portal status	Associated Devices
□	Default Policy	Default config	One Key,Account authentication	●	2024031900019
□	Default Policy	Default config	One Key,Account authentication	●	2024031900005

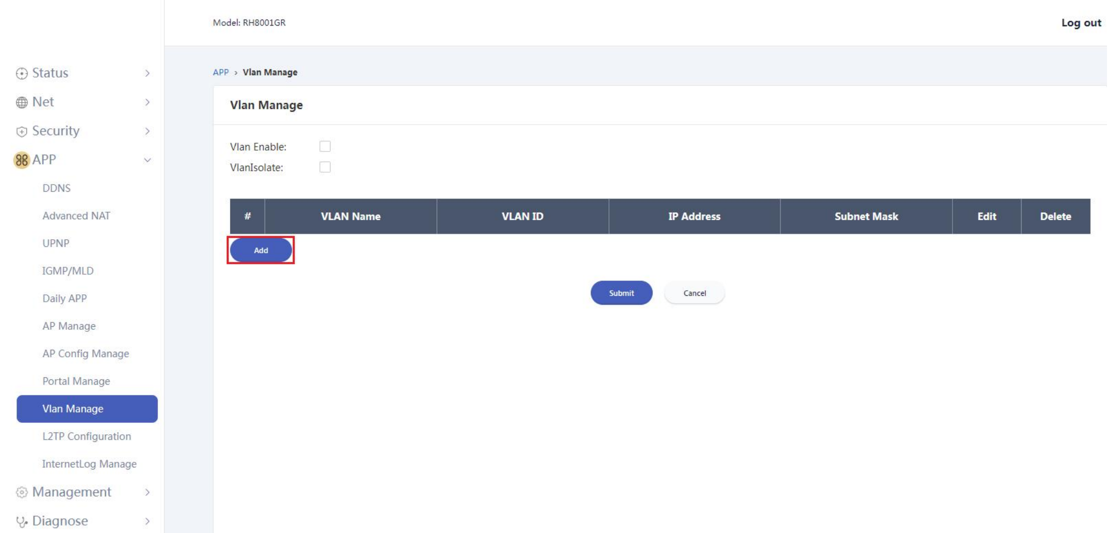
Are you sure you want to close Portal?

7.4 VLAN Management

7.4.1 Multi-VLAN Management

7.4.1.1 Creating Multi-VLAN Instances

Step 1: On the "App -> VLAN Manage" page, click the "Add" button to enter the VLAN configuration page, as illustrated in the figure below.



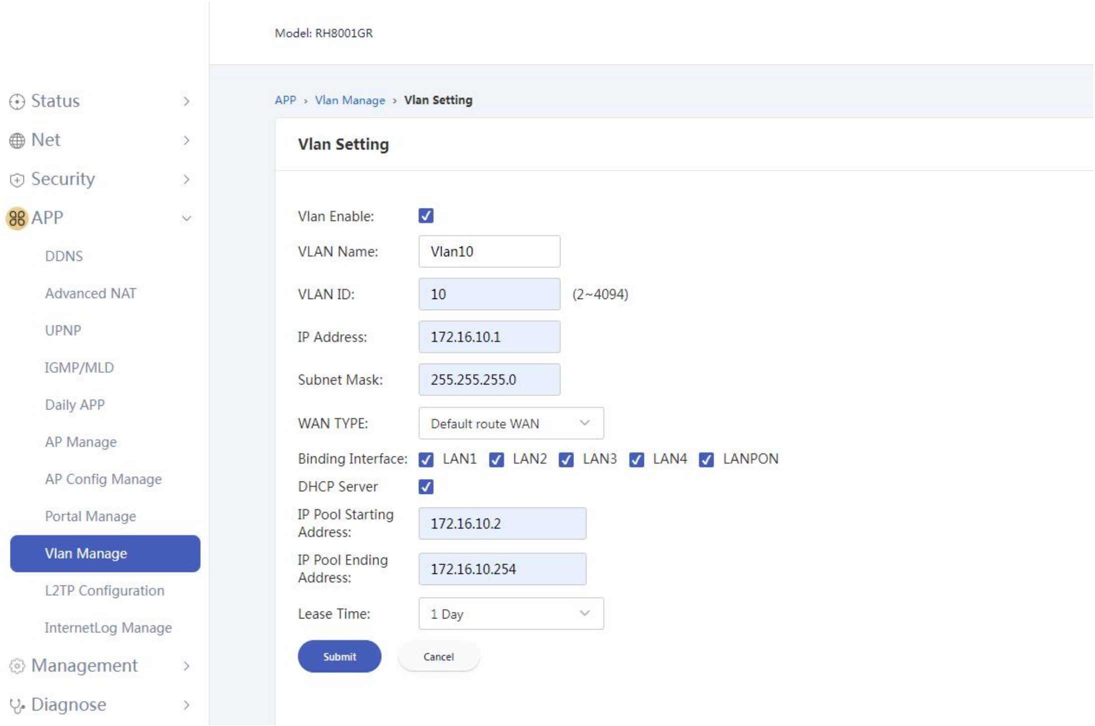
Vlan Manage

Vlan Enable: □

VlanIsolate: □

#	VLAN Name	VLAN ID	IP Address	Subnet Mask	Edit	Delete

Step 2: Check "VLAN Enable", and set the relevant parameters, for example, set the VLAN name to VLAN10, VLAN ID to 10, IP address to 172.168.10.1, and subnet mask to 255.255.255.0, as illustrated in the figure below.



Vlan Setting

Vlan Enable: ☑

VLAN Name: Vlan10

VLAN ID: 10 (2~4094)

IP Address: 172.16.10.1

Subnet Mask: 255.255.255.0

WAN TYPE: Default route WAN

Binding Interface: ☑ LAN1 ☑ LAN2 ☑ LAN3 ☑ LAN4 ☑ LANPON

DHCP Server ☑

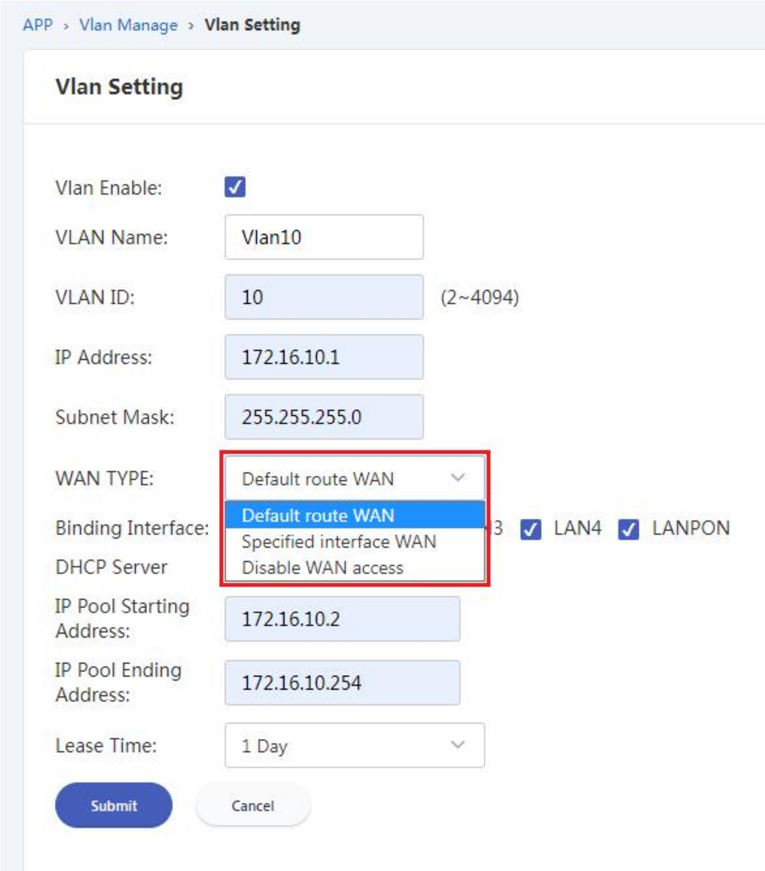
IP Pool Starting Address: 172.16.10.2

IP Pool Ending Address: 172.16.10.254

Lease Time: 1 Day

Step 3: Select the WAN type, as shown in the figure.

- Default Route WAN: Defaults to Internet Route WAN.
- Specified Interface WAN: Designates a specific Route WAN (can be Internet Route WAN or Other Route WAN), applicable to scenarios with multiple Route WANs.
- Disable WAN Access: Blocks external network access for this subnet.



APP › Vlan Manage › Vlan Setting

Vlan Setting

Vlan Enable: ☑

VLAN Name: Vlan10

VLAN ID: 10 (2~4094)

IP Address: 172.16.10.1

Subnet Mask: 255.255.255.0

WAN TYPE: Default route WAN

Binding Interface: 3 ☑ LAN4 ☑ LANPON

DHCP Server

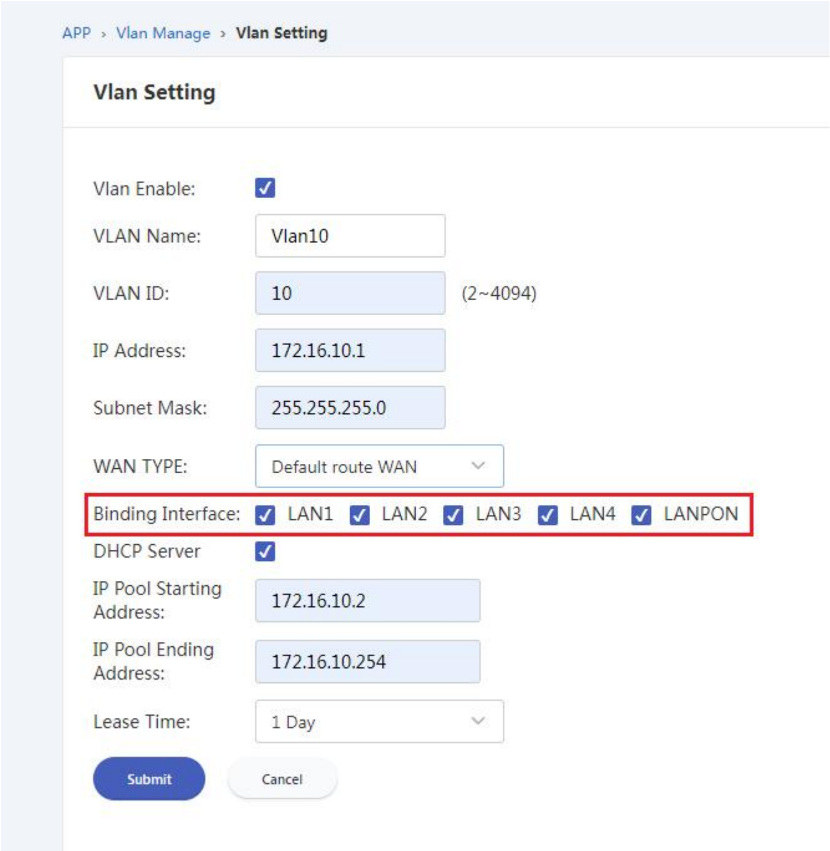
IP Pool Starting Address: 172.16.10.2

IP Pool Ending Address: 172.16.10.254

Lease Time: 1 Day

Step 4: Select the LAN-side interfaces to be bound, as shown in the figure.

Note: All ports here are in transparent mode.



APP › Vlan Manage › **Vlan Setting**

Vlan Setting

Vlan Enable: ☑

VLAN Name: Vlan10

VLAN ID: 10 (2~4094)

IP Address: 172.16.10.1

Subnet Mask: 255.255.255.0

WAN TYPE: Default route WAN

Binding Interface: ☑ LAN1 ☑ LAN2 ☑ LAN3 ☑ LAN4 ☑ LANPON

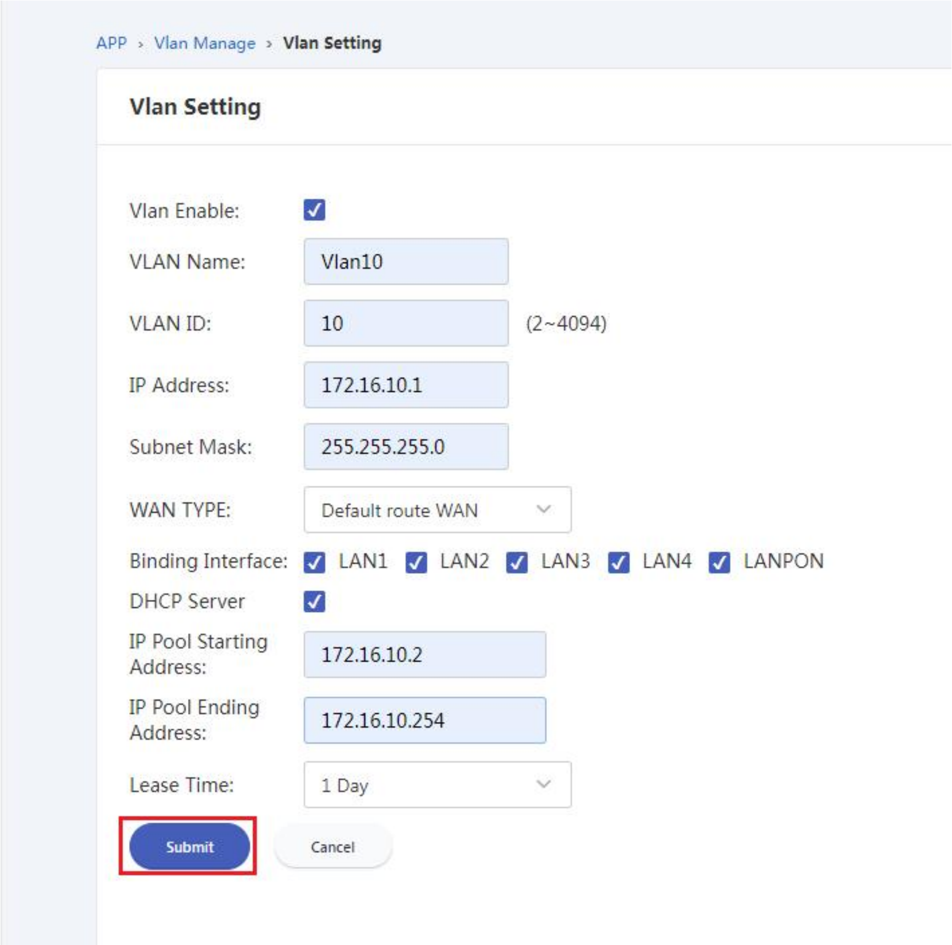
DHCP Server ☑

IP Pool Starting Address: 172.16.10.2

IP Pool Ending Address: 172.16.10.254

Lease Time: 1 Day

Step 5: Click "Submit" to complete the VLAN configuration. A maximum of 8 VLANs can be configured.



Vlan Setting

Vlan Enable: ☑

VLAN Name: Vlan10

VLAN ID: 10 (2~4094)

IP Address: 172.16.10.1

Subnet Mask: 255.255.255.0

WAN TYPE: Default route WAN

Binding Interface: ☑ LAN1 ☑ LAN2 ☑ LAN3 ☑ LAN4 ☑ LANPON

DHCP Server ☑

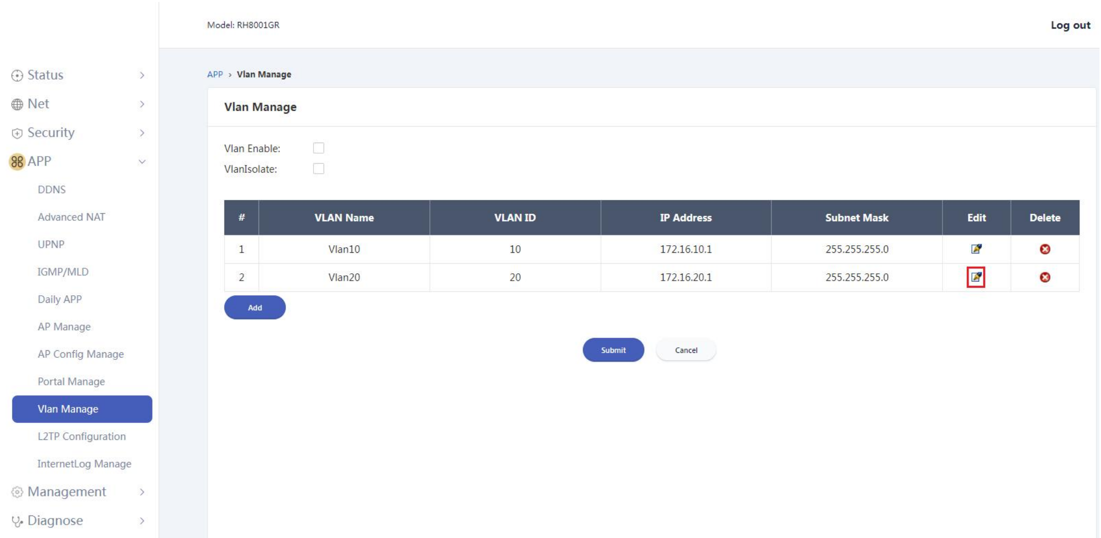
IP Pool Starting Address: 172.16.10.2

IP Pool Ending Address: 172.16.10.254

Lease Time: 1 Day

7.4.1.2 Modifying Multi-VLAN Instances

Select the instance that needs to be modified, click "Edit" as shown in the figure.



Vlan Manage

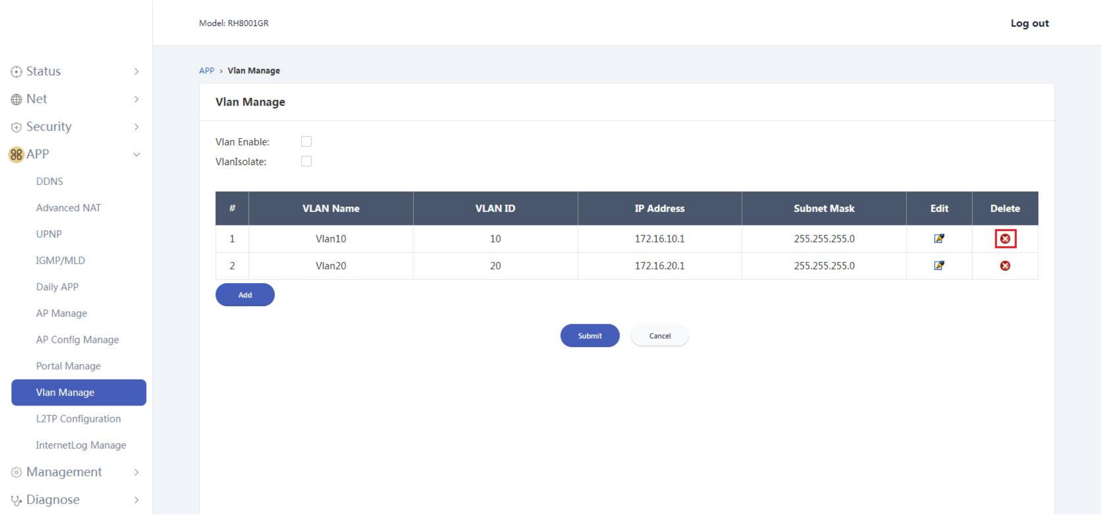
Vlan Enable: □

VlanIsolate: □

#	VLAN Name	VLAN ID	IP Address	Subnet Mask	Edit	Delete
1	Vlan10	10	172.16.10.1	255.255.255.0	✎	⊗
2	Vlan20	20	172.16.20.1	255.255.255.0	✎	⊗

7.4.1.3 Deleting Multi-VLAN Instances

Select the instance to be deleted, click "Delete" as shown in the figure.



Vlan Manage

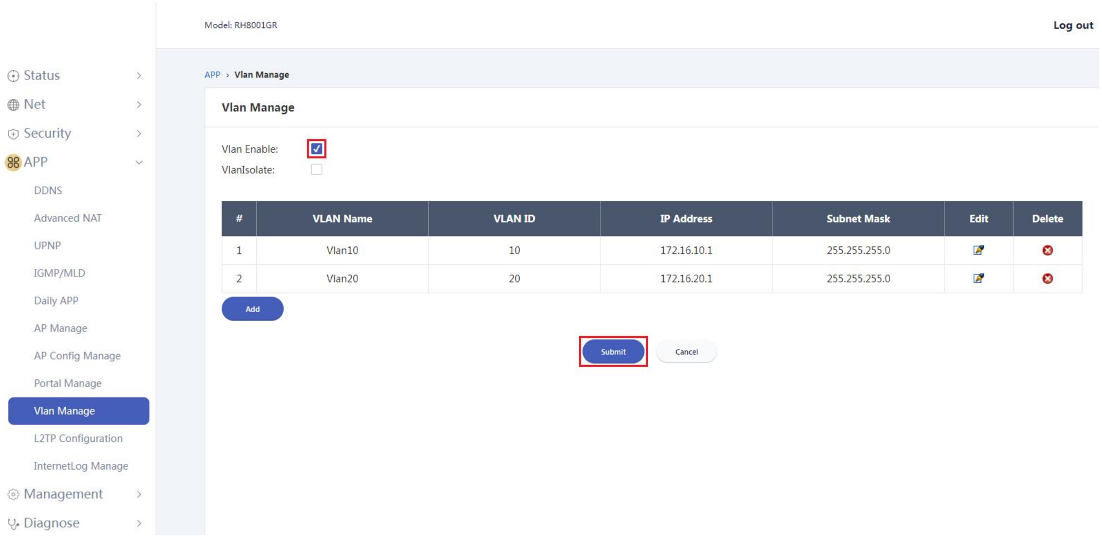
Vlan Enable: □

VlanIsolate: □

#	VLAN Name	VLAN ID	IP Address	Subnet Mask	Edit	Delete
1	Vlan10	10	172.16.10.1	255.255.255.0	✎	⊗
2	Vlan20	20	172.16.20.1	255.255.255.0	✎	⊗

7.4.1.4 Enabling Multi-VLAN

Check "VLAN Enable", click "Submit" to enable the multi-VLAN function as shown in the figure.



Vlan Manage

Vlan Enable: ☑

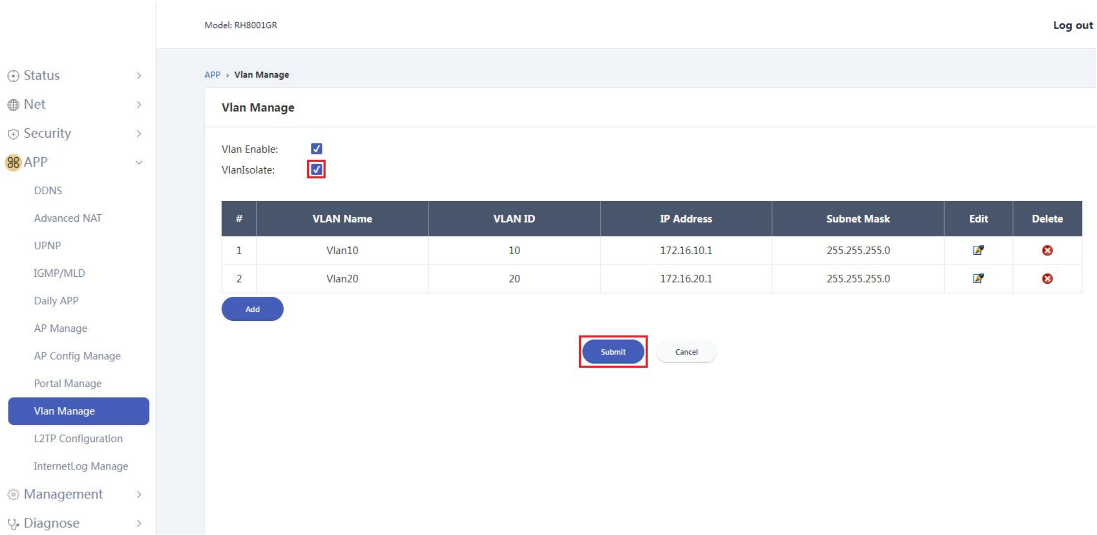
VlanIsolate: □

#	VLAN Name	VLAN ID	IP Address	Subnet Mask	Edit	Delete
1	Vlan10	10	172.16.10.1	255.255.255.0	✎	⊗
2	Vlan20	20	172.16.20.1	255.255.255.0	✎	⊗

7.4.2 VLANIsolate

7.4.2.1 Enabling VLAN Isolation Function

Check the "VLAN Isolation" option and click "Submit" to enable the VLAN isolation function.



Vlan Manage

Vlan Enable: ☑

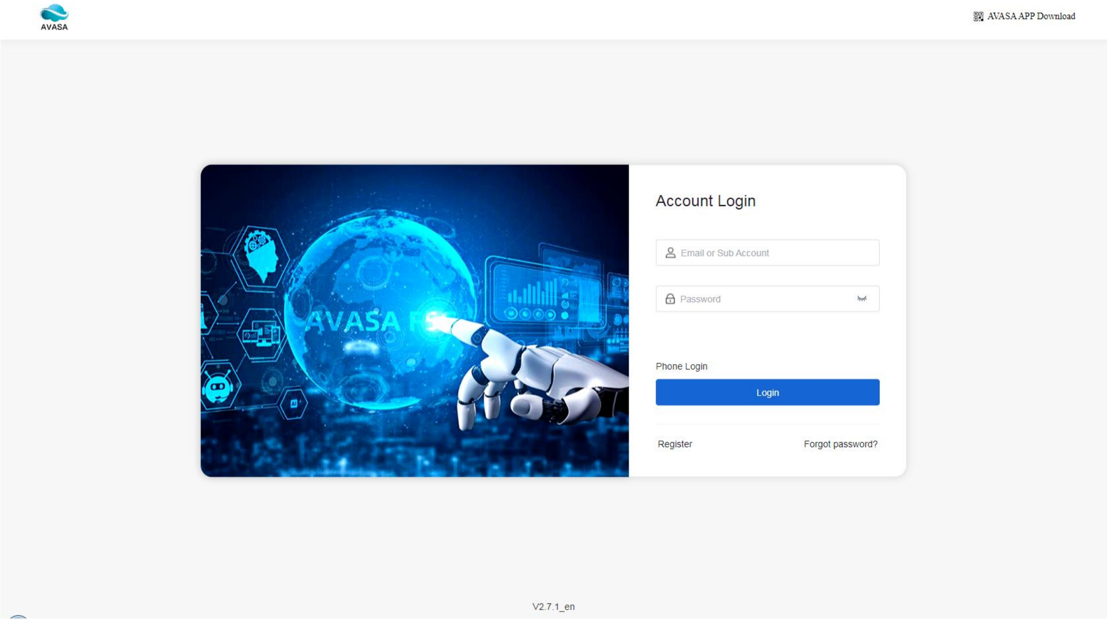
VlanIsolate: ☑

#	VLAN Name	VLAN ID	IP Address	Subnet Mask	Edit	Delete
1	Vlan10	10	172.16.10.1	255.255.255.0	✎	⊗
2	Vlan20	20	172.16.20.1	255.255.255.0	✎	⊗

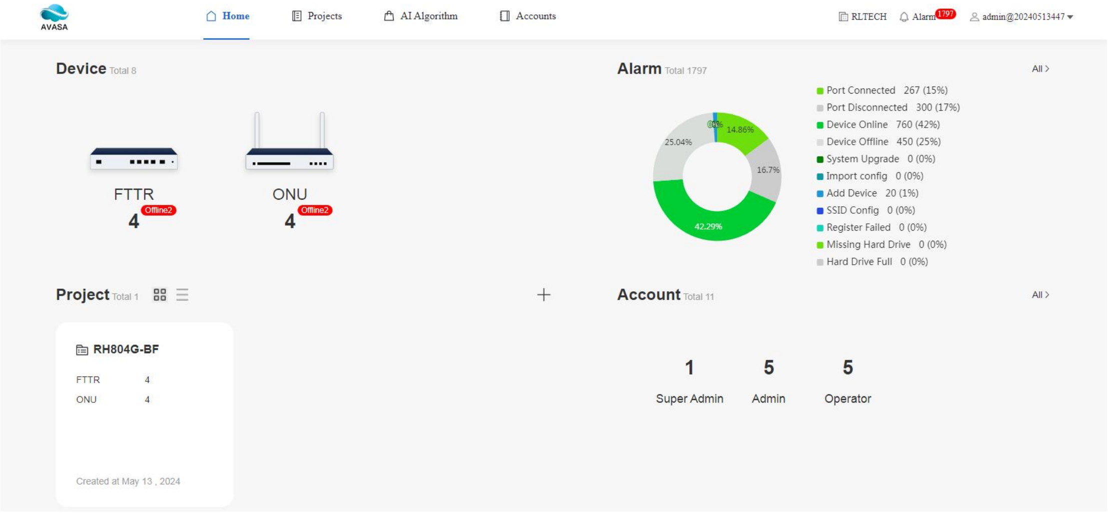
After enabling VLAN isolation, users in VLAN10 and VLAN20 will be unable to access each other. By default, users in VLAN10 and VLAN20 can communicate with each other.

8. AVASA

Open a web browser and type "**https://avasa.net/login**" in the address bar, then press Enter.



Log in using the AVASA account and password. Enter the correct password, and the browser will enter the main management page of the AVASA.



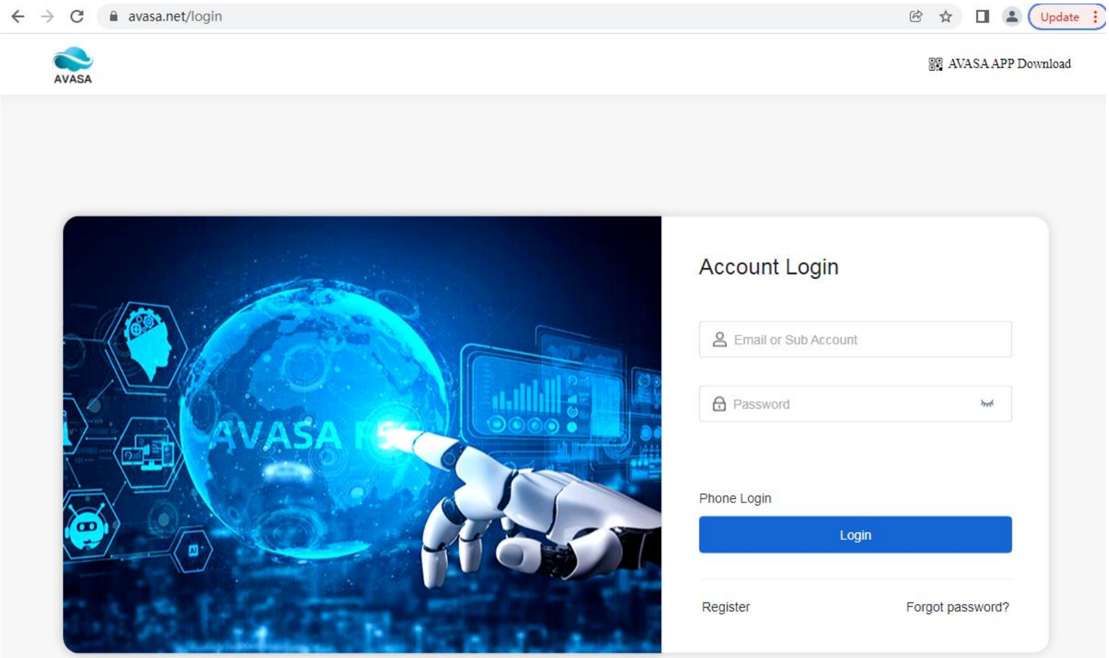
FTTR	4
ONU	4

🟩 Port Connected	267 (15%)
▨ Port Disconnected	300 (17%)
🟩 Device Online	760 (42%)
▨ Device Offline	450 (25%)
🟩 System Upgrade	0 (0%)
■ Import config	0 (0%)
🟦 Add Device	20 (1%)
🟦 SSID Config	0 (0%)
■ Register Failed	0 (0%)
🟩 Missing Hard Drive	0 (0%)
▨ Hard Drive Full	0 (0%)

8.1 Adding Managed Devices

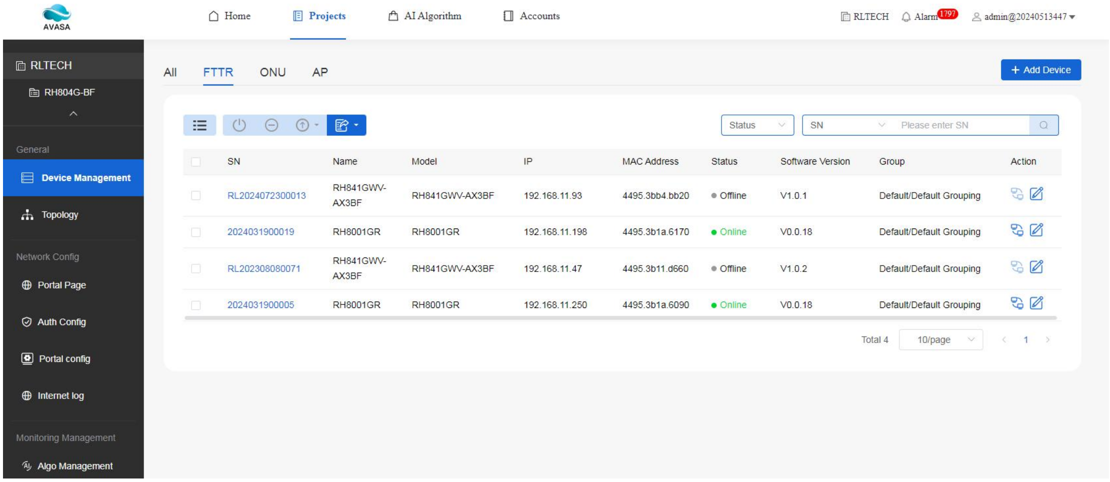
The device needs a route that can access the internet normally.

Step1:Open the browser, enter https://www.avasa.net in the web browser and then enter the Avasa login page.



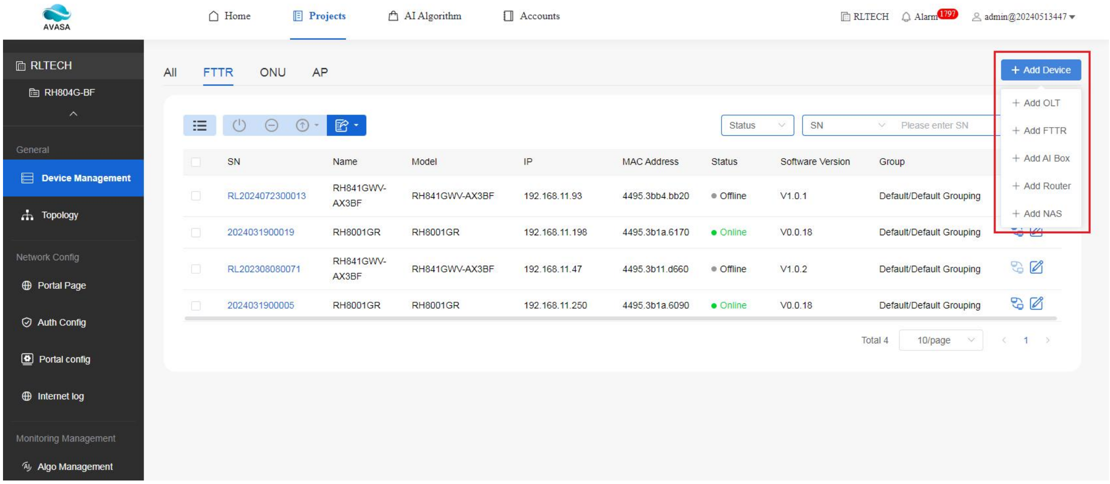
If it is your first time to register, please do so. If you have already registered, directly enter your account number and password to login.

Step 2: Click on "Projects" then click "Device Management" under general options on the left to enter the device management page.



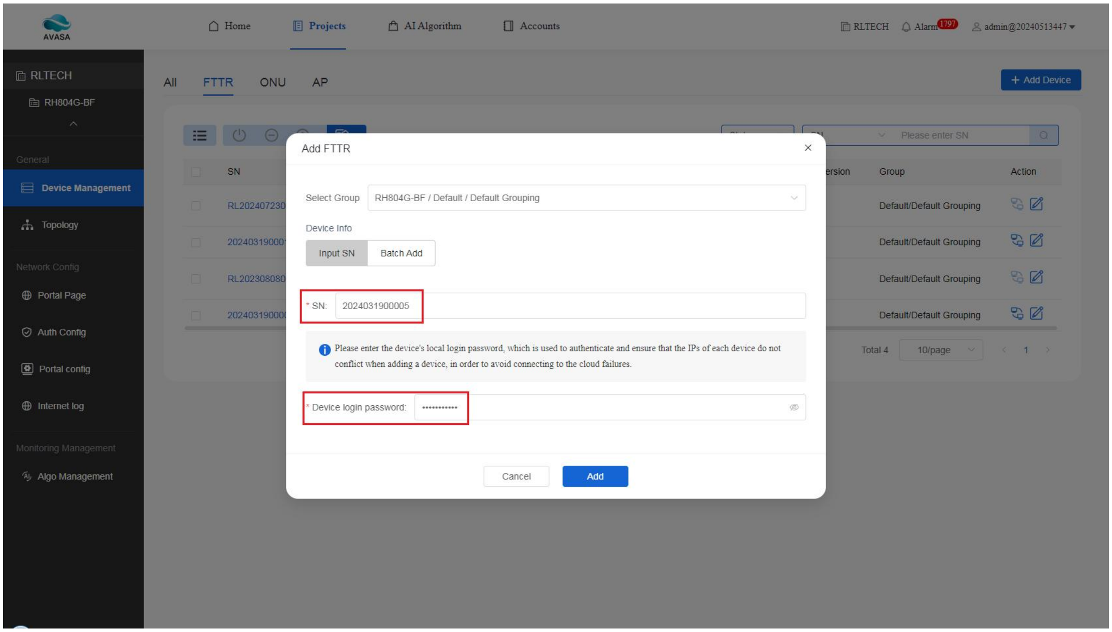
□	SN	Name	Model	IP	MAC Address	Status	Software Version	Group	Action
□	RL2024072300013	RH841GWV-AX3BF	RH841GWV-AX3BF	192.168.11.93	4495.3bb4.bb20	● Offline	V1.0.1	Default/Default Grouping	
□	2024031900019	RH8001GR	RH8001GR	192.168.11.198	4495.3b1a.6170	● Online	V0.0.18	Default/Default Grouping	
□	RL202308080071	RH841GWV-AX3BF	RH841GWV-AX3BF	192.168.11.47	4495.3b11.d660	● Offline	V1.0.2	Default/Default Grouping	
□	2024031900005	RH8001GR	RH8001GR	192.168.11.250	4495.3b1a.6090	● Online	V0.0.18	Default/Default Grouping	

Step 3: Click "+ Add Device" and select the type of device you wish to add as illustrated in the figure below.



□	SN	Name	Model	IP	MAC Address	Status	Software Version	Group
□	RL2024072300013	RH841GWV-AX3BF	RH841GWV-AX3BF	192.168.11.93	4495.3bb4.bb20	● Offline	V1.0.1	Default/Default Grouping
□	2024031900019	RH8001GR	RH8001GR	192.168.11.198	4495.3b1a.6170	● Online	V0.0.18	Default/Default Grouping
□	RL202308080071	RH841GWV-AX3BF	RH841GWV-AX3BF	192.168.11.47	4495.3b11.d660	● Offline	V1.0.2	Default/Default Grouping
□	2024031900005	RH8001GR	RH8001GR	192.168.11.250	4495.3b1a.6090	● Online	V0.0.18	Default/Default Grouping

Step 4: Enter the correct device serial number and login password,the serial number and login password can be found on the label of the device's outer shell.



Add FTTR

Select Group: RH804G-BF / Default / Default Grouping

Device Info

Input SN | Batch Add

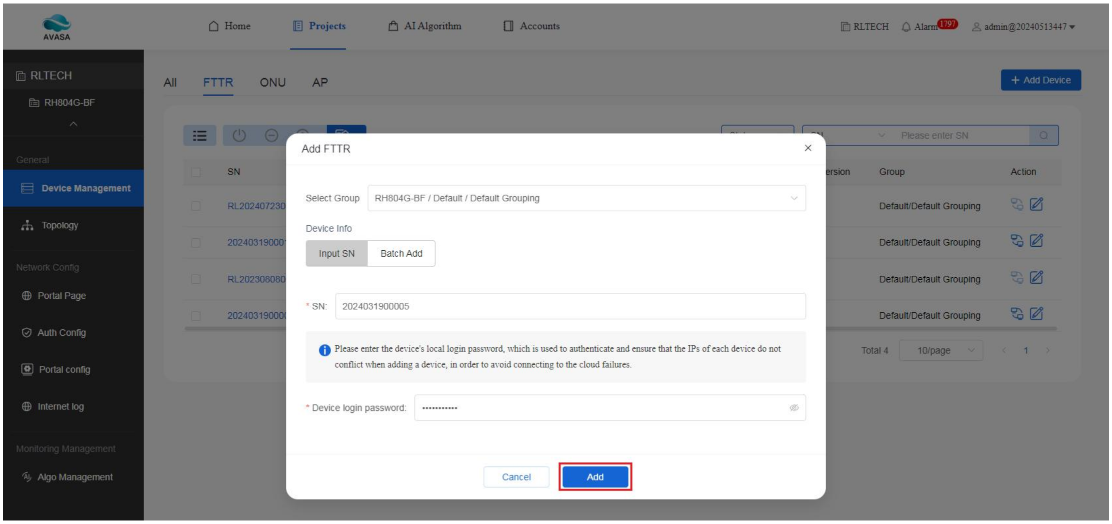
* SN: 2024031900005

Please enter the device's local login password, which is used to authenticate and ensure that the IPs of each device do not conflict when adding a device, in order to avoid connecting to the cloud failures.

* Device login password: ••••••••••••

Cancel | Add

Step 5: Click "Add" to complete the addition process.



Add FTTR

Select Group: RH804G-BF / Default / Default Grouping

Device Info

Input SN | Batch Add

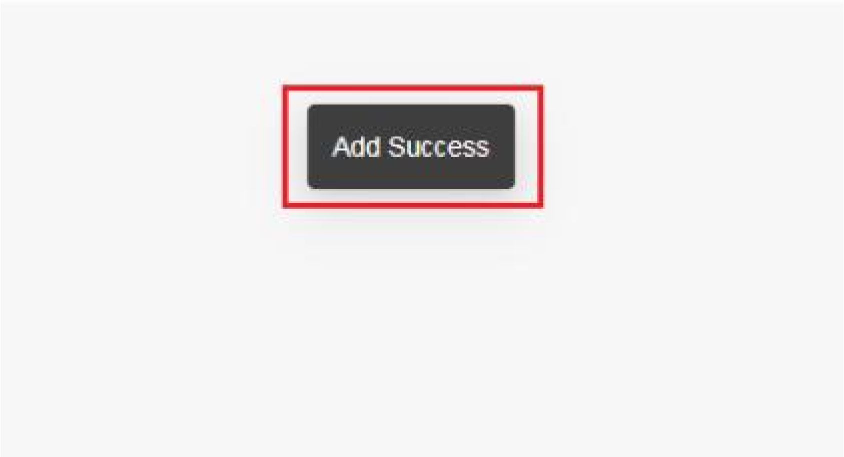
* SN: 2024031900005

Please enter the device's local login password, which is used to authenticate and ensure that the IPs of each device do not conflict when adding a device, in order to avoid connecting to the cloud failures.

* Device login password: ••••••••••••

Cancel | Add

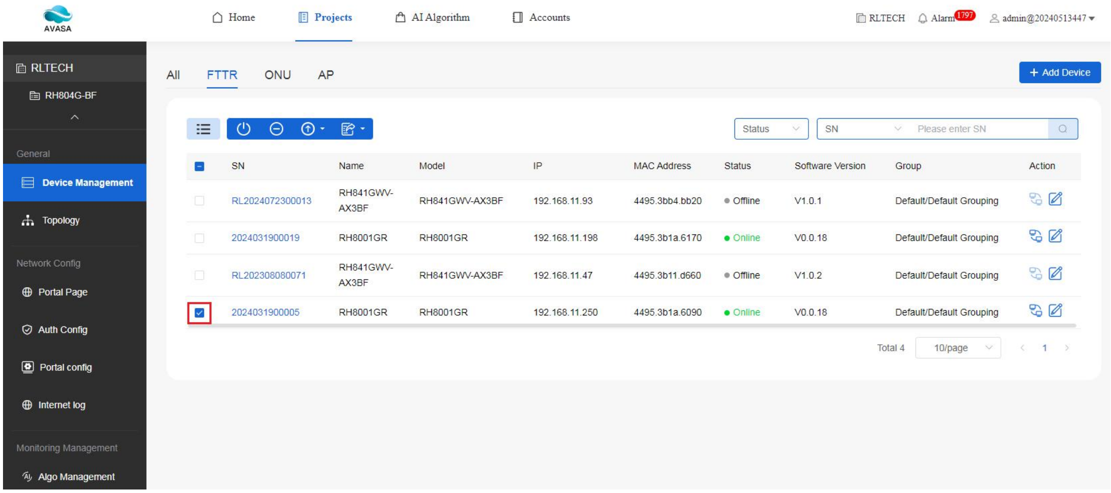
A successful addition will show the following prompt.



Add Success

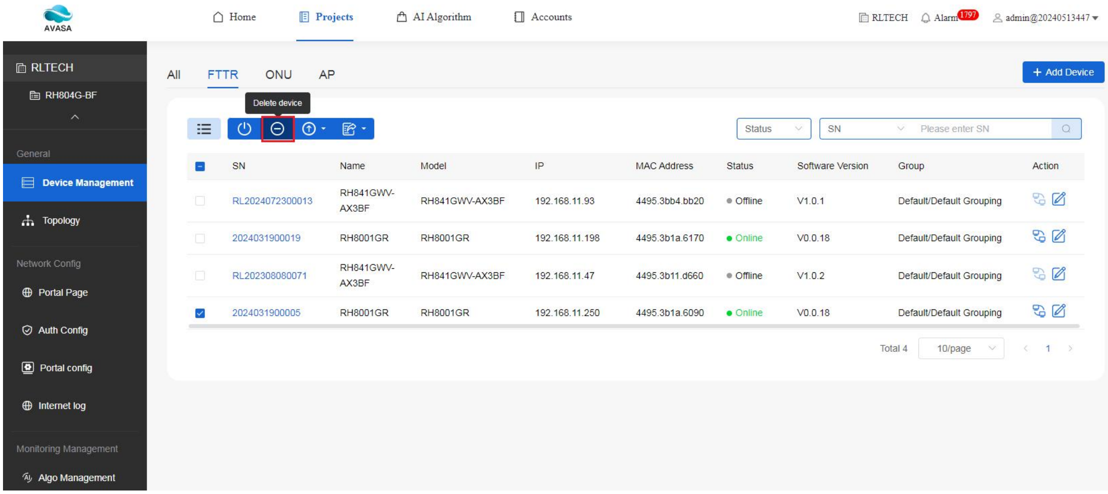
8.2 Deleting Added Managed Devices

Step 1: Check the box next to the device you want to delete as illustrated in the figure below.



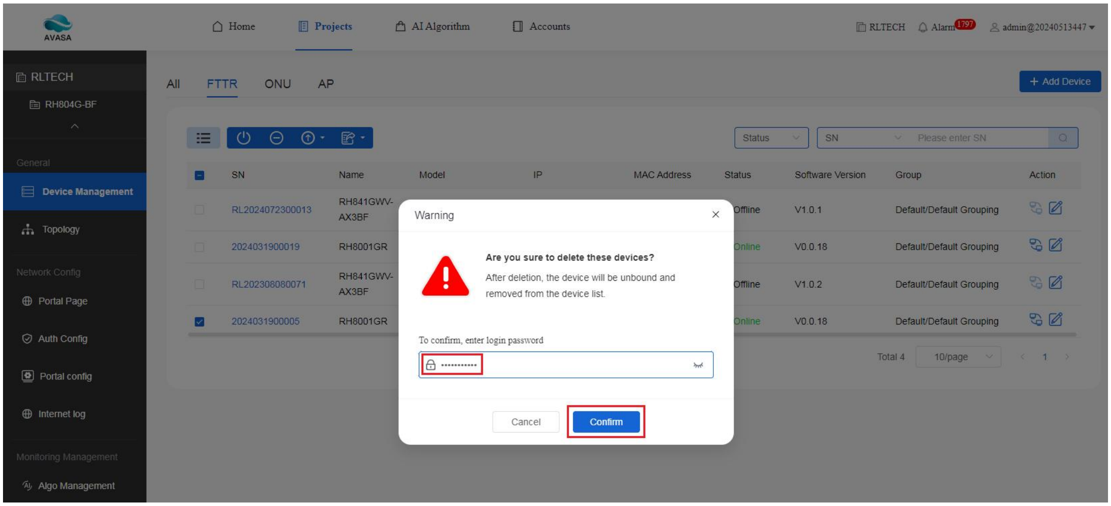
☐	SN	Name	Model	IP	MAC Address	Status	Software Version	Group	Action
☐	RL2024072300013	RH841GWV-AX3BF	RH841GWV-AX3BF	192.168.11.93	4495.3bb4.bb20	● Offline	V1.0.1	Default/Default Grouping	
☐	2024031900019	RH8001GR	RH8001GR	192.168.11.198	4495.3b1a.6170	● Online	V0.0.18	Default/Default Grouping	
☐	RL202308080071	RH841GWV-AX3BF	RH841GWV-AX3BF	192.168.11.47	4495.3b11.d660	● Offline	V1.0.2	Default/Default Grouping	
☑	2024031900005	RH8001GR	RH8001GR	192.168.11.250	4495.3b1a.6090	● Online	V0.0.18	Default/Default Grouping	

Step 2: Click the delete device button.



☐	SN	Name	Model	IP	MAC Address	Status	Software Version	Group	Action
☐	RL2024072300013	RH841GWV-AX3BF	RH841GWV-AX3BF	192.168.11.93	4495.3bb4.bb20	● Offline	V1.0.1	Default/Default Grouping	
☐	2024031900019	RH8001GR	RH8001GR	192.168.11.198	4495.3b1a.6170	● Online	V0.0.18	Default/Default Grouping	
☐	RL202308080071	RH841GWV-AX3BF	RH841GWV-AX3BF	192.168.11.47	4495.3b11.d660	● Offline	V1.0.2	Default/Default Grouping	
☑	2024031900005	RH8001GR	RH8001GR	192.168.11.250	4495.3b1a.6090	● Online	V0.0.18	Default/Default Grouping	

Step 3: In the pop-up dialog, enter the correct AVASA login password and click "Confirm" to complete the deletion.



Warning

Are you sure to delete these devices?

After deletion, the device will be unbound and removed from the device list.

To confirm, enter login password

••••••••••

9. Frequently Asked Question

1) Why Can't I Connect to WLAN?

Answer:

1. Confirm that the WLAN switch is turned on.
2. Check if the wireless network card settings are correct, and verify that the network name, encryption method, and key match those of the terminal device.

2) Why Does My Computer Establish a Wireless Connection with the Terminal But Has Weak or Unstable Signal?

Answer:

1. There may be strong magnetic fields or radio waves interfering with the wireless network near your location. Try to keep the terminal and computer away from appliances with strong magnetic or electric fields.
2. Obstructions like concrete walls or wooden boards can affect wireless signal transmission. It's recommended to choose an open area during installation so that there are no obstructions between the computer and the device.
3. Your computer might be too far from the terminal device; try moving your computer closer to the terminal.
4. Thunderstorms can impact the performance of wireless networks.

3) Why Can My Computer Detect the Wireless Network but Cannot Access the Internet When Using Wireless?

Answer:

1. If the computer cannot establish a wireless connection with the terminal, check whether the wireless network card has the correct SSID or key settings.
2. If a wireless connection can be established but internet access fails, ensure that dial-up was successful.

4) What Should I Do If None of the Terminal's Indicator Lights Are On?

Answer:

1. Check if the power cord for the terminal is properly connected.

2. Ensure the power switch on the terminal is turned on.
3. Verify that the power adapter matches the terminal.
4. Confirm that the mains voltage meets the input requirements of the terminal's power adapter.

5) The LAN Light Is Not On, What Should I Do?

Answer:

1. Check if the type of Ethernet cable between the terminal and the computer is correct.
2. Ensure the Ethernet cable connecting the terminal to the computer is securely connected and undamaged.
3. Verify that the network card indicator light on the computer is lit.
4. Confirm that the network card is functioning normally by checking in Windows Device Manager under "Network adapters" for any "?" or "!" symbols.

6) Unable to Access the Internet, What Should I Do?

Answer: For example, in bridge mode:

1. Try using the "ping" command to test the network connection between the computer and the terminal. The default IP address for the terminal is "192.168.2.1."

2. Confirm that you have entered the correct username and password.

3. Ensure that the PPP dial-up software is correctly installed and configured.

4. If dial-up succeeds but internet access still fails, check if the browser's proxy server settings are correct; it should be set to not use a proxy server.

5. Try accessing multiple websites to confirm that the issue isn't due to a specific website server failure.

6. Attempt to disconnect the dial-up connection, wait five minutes, and then reconnect.

7) ADSL Frequently Disconnects, What Should I Do?

Answer:

1. Check if the cable line is making good contact with the terminal.
2. Ensure the terminal is kept away from appliances that generate strong magnetic or electric fields.

10. Factory Default Settings

Parameter Item	Default Settings
LAN Interface IP Address	Please check the printed label on the bottom of the casing
LAN Interface Subnet Mask	Please check the printed label on the bottom of the casing
DHCP Server Functionality	Enable
Username for Web Configuration Page Login	Please check the printed label on the bottom of the casing
Password for Web Configuration Page Login	Please check the printed label on the bottom of the casing
Wireless Network Name (WLAN SSID)	Please check the printed label on the bottom of the casing
Wireless Network Access Password (PSK Key)	Please check the printed label on the bottom of the casing

11. Declaration of Toxic and Hazardous Substances in Electronic Information Products

Part Name	Toxic and Hazardous Substances or Elements					
	Lead （Pb）	Mercury （Hg）	Cadmium （Cd）	Hexavalent Chromium （Cr(VI)）	Polybrominated Biphenyls （PBB）	Polybrominated Diphenyl Ethers （PBDE）
Structural Component	○	○	○	○	○	○
Single Board/Circuit Module	×	○	○	○	○	○
Signal Line	○	○	○	○	○	○
Cable Connector	○	○	○	○	○	○
Power Adapter	×	○	○	○	○	○
Ancillary Equipment	○	○	○	○	○	○

○：Indicates that the concentration of the hazardous substance in all homogeneous materials of this component is below the limit requirement specified in SJ/T 11363-2006 "Requirements for Concentration Limits for Certain Hazardous Substances in Electronic Information Products".

×：Indicates that the concentration of the hazardous substance in at least one homogeneous material of this component exceeds the limit requirement specified in SJ/T 11363-2006.

Notes：

1. Single Board/Circuit Module:

■ Ceramic cores of resistors/capacitors on the board contain lead.

- Copper alloys in components contain lead.
- High-temperature solder used for transistor chip bonding is lead-based.
- Lead in resistor layers and protective glass layers is exempt.
- Leads and solder of ICs, power components, etc., on the board contain lead.

2. Power Adapter：Internal components contain lead.

12. Warranty Card

Warranty Card

Dear customer, thank you for choosing our company's products. To ensure we can provide you with the best service, please read, complete, and keep this warranty card.

User Name	
User Address/ZIP Code	
Contact Number	
Product Model	
Product Serial Number	
Purchase Date	
Invoice Number	
Sales Unit Name	
Sales Unit Address	
Phone	

User to preserve. Non-replaceable if lost.

Sales Unit: (Seal)

13. Warranty Statement

Warranty Statement

Products purchased through legitimate channels enjoy a one-year warranty for non-human-induced malfunctions from the date of purchase.

To protect your legitimate rights and interests, please note the following:

(1) The warranty card must be stamped by the sales department to become valid.The warranty card must be stamped by the sales unit to become valid.

(2) The warranty card shall be properly kept by the user. It will not be reissued if lost, and any alterations will nullify it.

(3) For non-human-induced malfunctions occurring within the warranty period, the user can go to the designated service center for free repair with the warranty card and purchase invoice on which the product serial number is.

What is Not Covered:

(1) Malfunctions or damages caused during transportation or loading/unloading..

(2) Failures caused by unauthorized disassembly, modification, or other human factors.

(3) Failures to keep the product under a hospitable environment as required in the manual.

(4) Damages caused by force majeure (e.g., fire, earthquake, lightning strike).

(5) Failures to use and maintain the product as required in the manual.

(6) Damaged device casing, power supply, etc., caused during daily use.

(7) Inconsistent product serial numbers on the warranty card or tampered warranty card.

(8) Blurred or removed product label, SN barcode, or anti-tamper sea.

For malfunctions and other conditions that don’t apply to free warranty, users should pay for repair services. The company reserves the final right to interpret these warranty terms