Tenda

User Guide

AX3000 Dual Band Wi-Fi 6 Wireless Hotspot Router

W30E

www.tendacn.com

Version 1.0

Copyright Statement

Disclaimer

Pictures, images and product specifications herein are for references only. To improve internal design, operational function, and/or reliability, Tenda reserves the right to make changes to the products without obligation to notify any person or organization of such revisions or changes. Tenda does not assume any liability that may occur due to the use or application of the product described herein. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information and recommendations in this document do not constitute a warranty of any kind, express or implied.

Version 1.0

Preface

Thank you for choosing Tenda! Please read this user guide carefully before you start.

Conventions

This user guide applies to the Tenda AX3000 Dual Band Wi-Fi 6 Wireless Hotspot Router W30E.

The contained images and UI screenshots are subject to the actual products.

The typographical elements that may be found in this document are defined as follows.

Item	Presentation	Example
Cascading menus	>	**System** > **Live Users**
Parameter and value	Bold	Set **User Name** to **Tom**.
Variable	Italic	Format: *XX:XX:XX:XX:XX:XX*
UI control	Bold	On the **Policy** page, click the **OK** button.
Message	“ ”	The “Success” message appears.

The symbols that may be found in this document are defined as follows.

Symbol	Meaning
NOTE	This format is used to highlight information of importance or special interest. Ignoring this type of note may result in ineffective configurations, loss of data or damage to device.
TIP	This format is used to highlight a procedure that will save time or resources.

For more documents

Go to our website at www.tendacn.com and search for the latest documents for this product.

Document	Description
Quick Installation Guide	It introduces how to set up the device quickly for internet access, the descriptions of LED indicators, ports, and buttons, FAQ, statement information, and so on.
User Guide	It introduces how to set up more functions of the device for more requirements, including all functions on the web UI of the device.
Data Sheet	It introduces the basic information of the device, including product overview, selling points, and specifications.

Technical Support

If you need more help, contact us by any of the following means. We will be glad to assist you as soon as possible.

☎ **Hotline**	Global: (86) 755-27657180 (China Time Zone)	✉ **Email**	support@tenda.com.cn
	United States: 1-800-570-5892 (Toll Free: 7 x 24 hours)		
	Canada: 1-888-998-8966 (Toll Free: Mon - Fri 9 am - 6 pm PST)		
	Hong Kong: 00852-81931998		
Website	www.tendacn.com		

Revision History

Tenda is constantly searching for ways to improve its products and documentation. The following table indicates any changes that might have been made since the user guide was released.

Version	Date	Description
V1.0	2022-08-23	Original publication

Contents

1 Login

1.1 Log in to the web UI

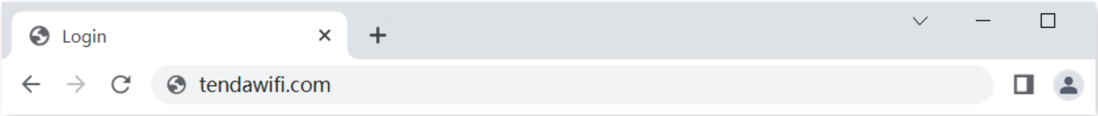
If you use this router for the first time or have reset it to factory settings, refer to the quick installation guide to complete the setup wizard. Otherwise, refer to the following steps.

1.1.1 Log in with your computer

Step 1 Connect your computer to a LAN port of the router with an Ethernet cable.

Step 2 Set the local connection of your computer to **Obtain an IP address automatically** and **Obtain DNS server address automatically**.

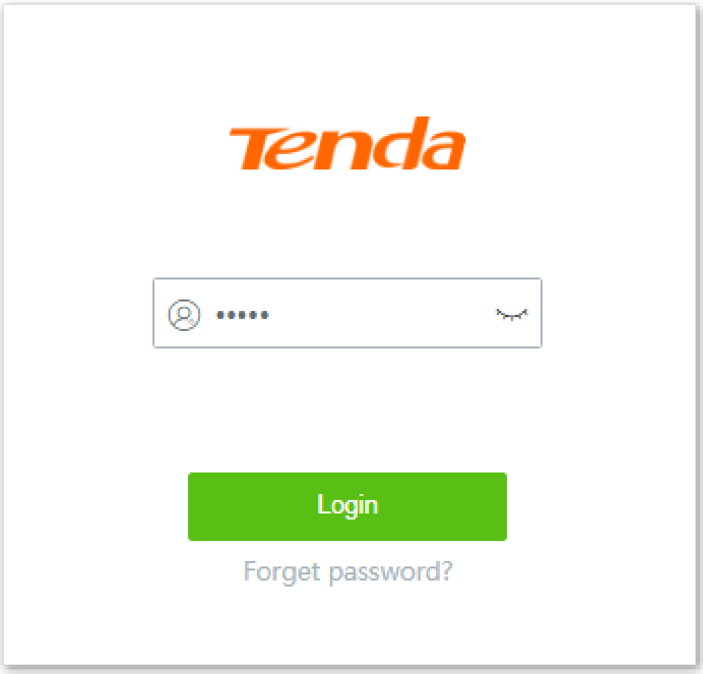
Step 3 Start a web browser, and visit **tendawifi.com**.



Step 4 Enter the login password of the router you set, and click **Login**.

TIP

- By default, the WiFi password is set as the login password automatically. Thus, if you forget the login password, try with the WiFi password.
- If the above fails, reset the router to factory settings and then set the login password. After reset, you need to reconfigure the network.



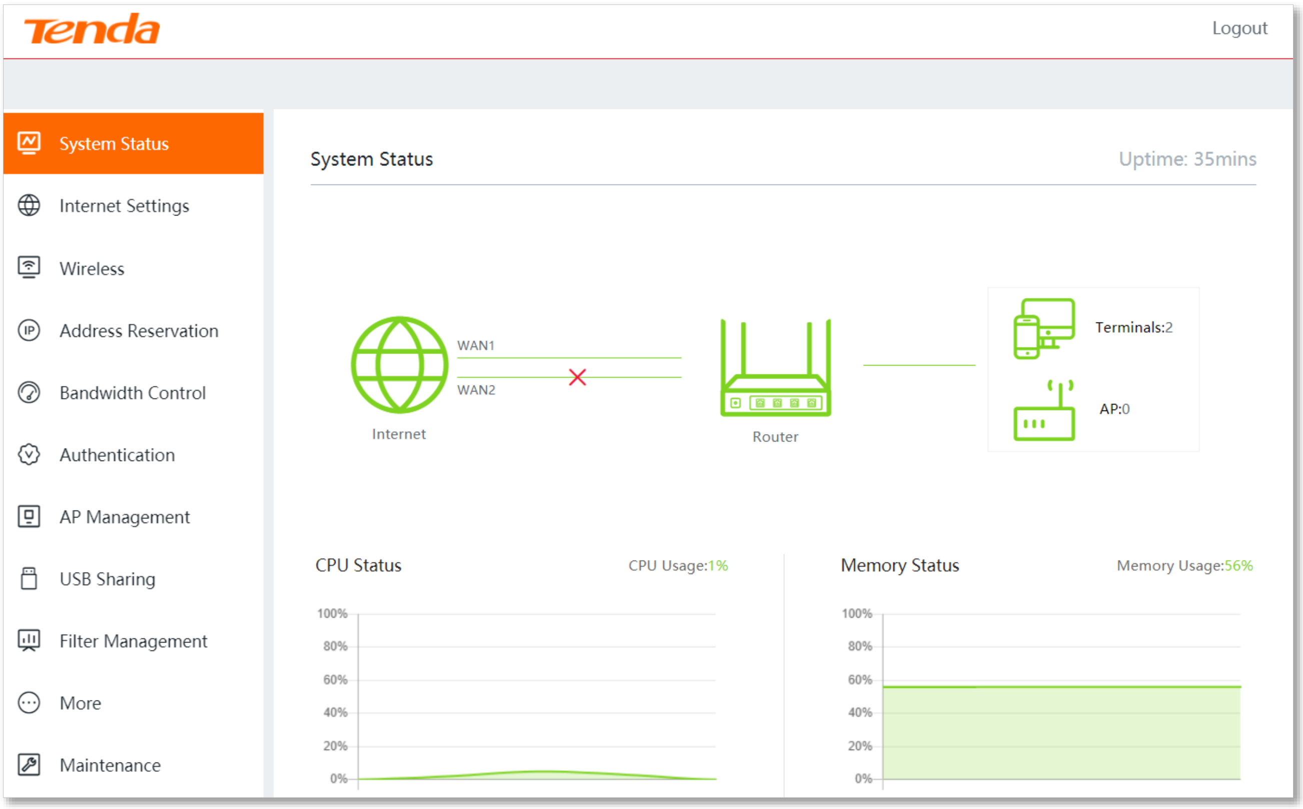
----End

TIP

If the above page does not appear, try the following solutions:

- Ensure that the router is powered on properly.
- Ensure that the computer is connected to a LAN port of the router, and the corresponding indicator lights solid on or blinks.
- Reset the router to factory settings, and log in again.

Log in to the web UI successfully. See the following figure.



Uptime: 35mins

Terminals:2

AP:0

CPU Usage:1%

Memory Usage:56%

1.1.2 Log in with your smartphone

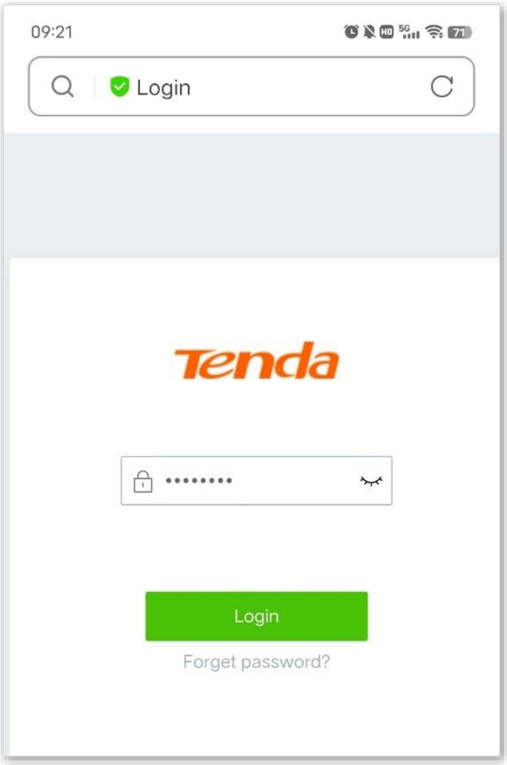
Step 1 Connect your smartphone to the SSID of the router.

Step 2 Start a web browser on the smartphone, and visit **tendawifi.com**.

Step 3 Enter the login password of the router you set, and click **Login**.

TIP

- By default, the WiFi password is set as the login password automatically. Thus, if you forget the login password, try with the WiFi password.
- If the above fails, reset the router to factory settings and then set the login password. After reset, you need to reconfigure the network.



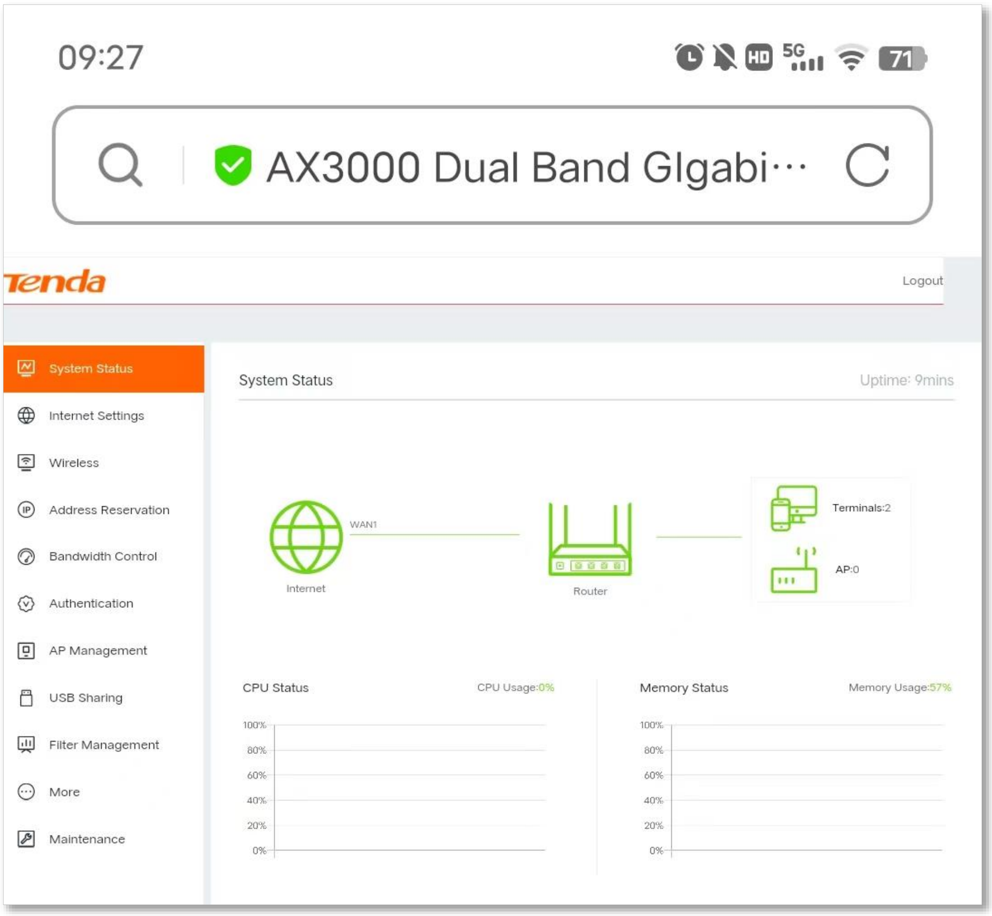
----End

TIP

If the above page does not appear, try the following solutions:

- Ensure that your smartphone is connected to the WiFi network of the router.
- Ensure that the mobile data is disabled.
- Reset the router to factory settings, and log in again.

Log in to the web UI successfully. See the following figure.



1.2 Logout

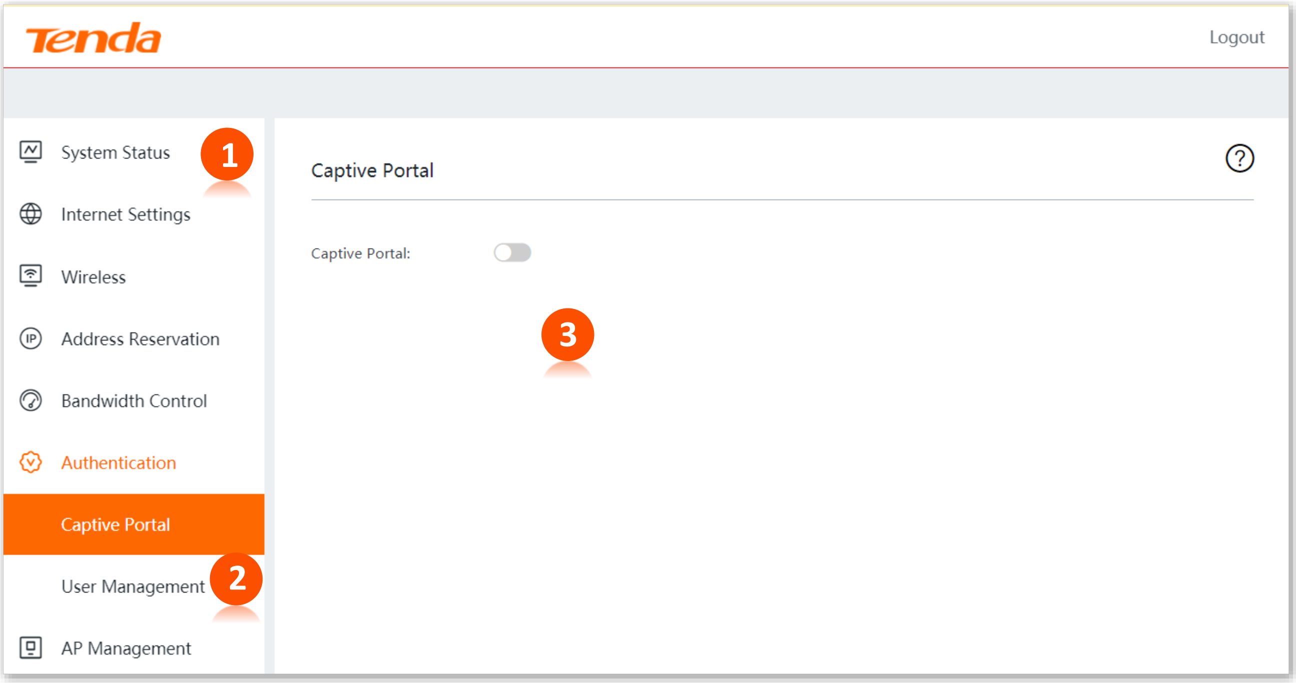
If you log in to the web UI of the router and perform no operation within **20** minutes, the router logs you out automatically.

You can log out by clicking **Logout** on the upper right corner of the web UI as well.

2 Web UI

2.1 Web UI layout

The web UI of the router consists of three sections, including the level-1, level-2 navigation bar, and configuration area. See the following figure:



TIP

Features and parameters in gray indicate that they are not available or cannot be changed under the current condition.

No.	Name	Description
1	Level-1 navigation bar	Used to display the function menu of the router. Users can select functions in the navigation bars and the configuration appears in the configuration area.
2	Level-2 navigation bar	
3	Configuration area	Used to modify or view your configuration.

2.2 Frequently-used buttons

The following table describes the frequently-used buttons available on the web UI of the router.

Button	Description
+ Add	Used to add a new rule or policy.
🗑 Delete	Used to delete the selected rule or policy.
Save	Used to save the configuration on the current page and enable the configuration to take effect.
Cancel	Used to change the current configuration on the current page back to the original configuration.
Refresh	Used to refresh the page information.
?	Used to view help information for the current page.

3 System status

In the **System Status** module, you can:

- Check physical connections and system status
- View CPU and memory status
- Monitor traffic
- Manage online devices
- Control bandwidth of online devices
- Add devices to or remove devices from blacklist
- Manage APs

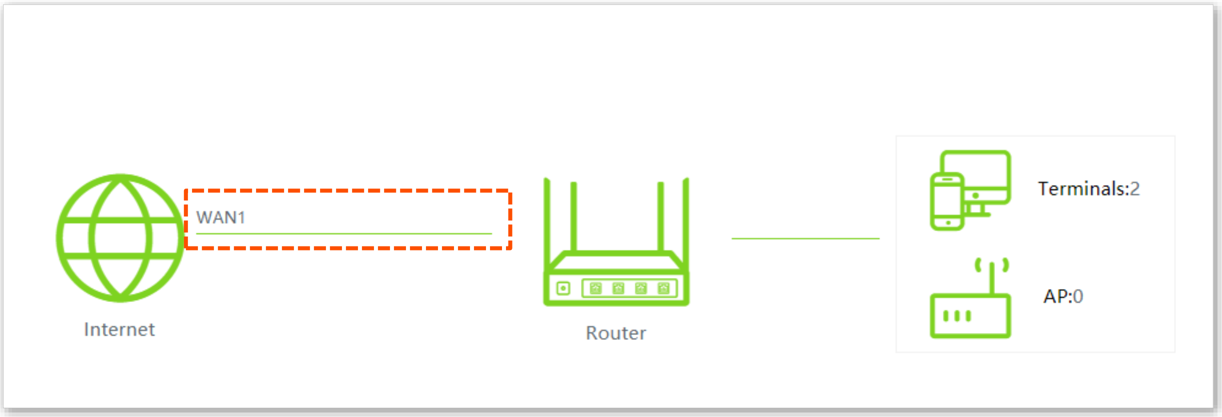
3.1 Check physical connections and system status

Click **System Status** to enter the page.

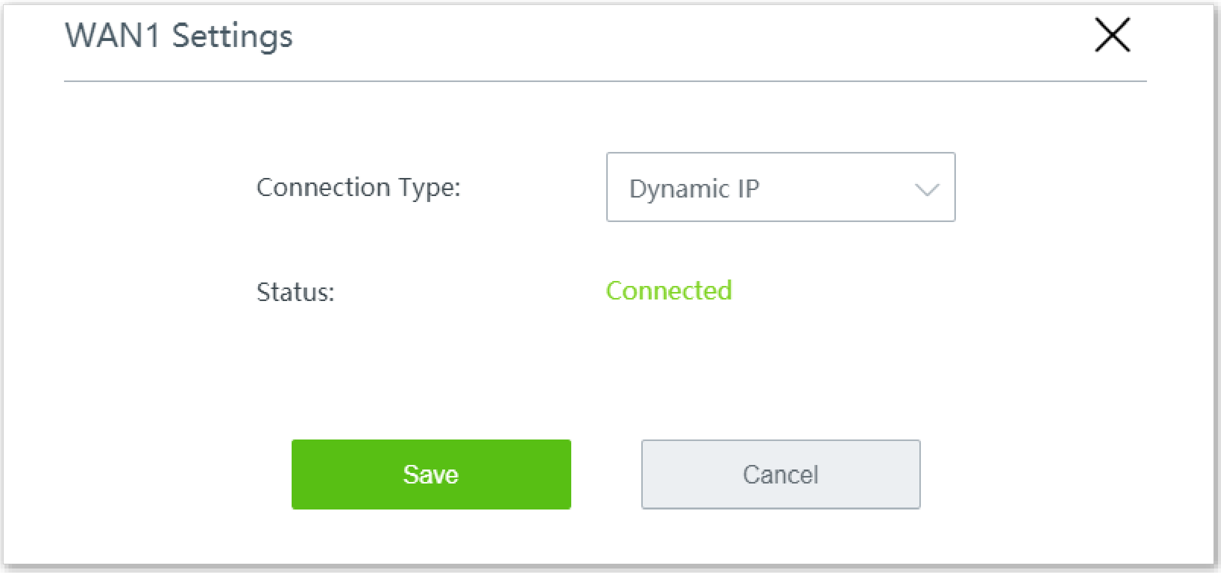
Here, you can check if the physical connections are proper, or view the router's system status.

3.1.1 Check physical connections

The following figure indicates that the router is connected to the internet properly through the WAN1 port.



You can click **WAN1** to view the connection type and status.

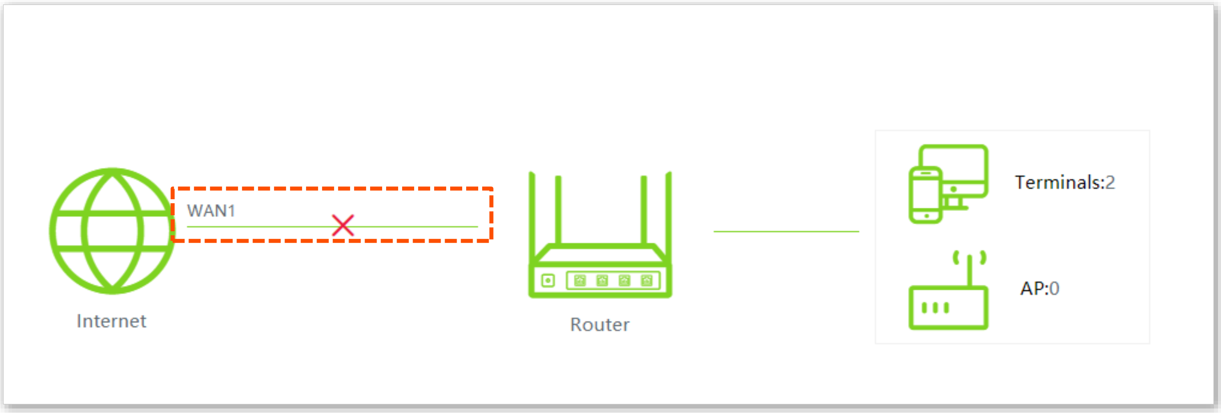


WAN1 Settings

Connection Type: Dynamic IP

Status: Connected

The following figure indicates that the router is disconnected from the internet. Check whether the Ethernet cable is connected properly.



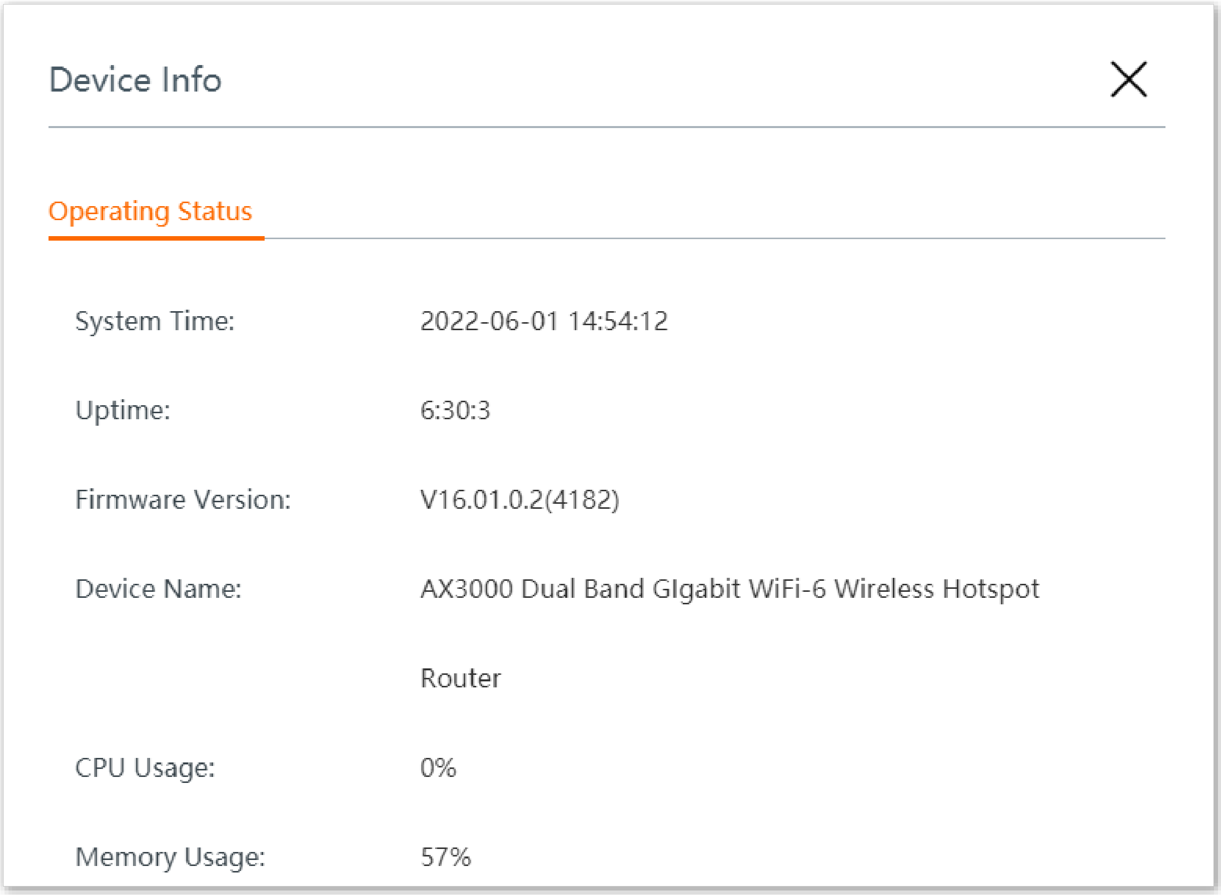
3.1.2 View system status

Click the **Router** icon , then the **Device Info** window pops up.

The **Device Info** window consists of four parts: Operating Status, LAN Port Status, WAN Info and IPv6 Status.

Operating status

This module displays the router's operating status about the system time, uptime, firmware version and so on.



System Time: 2022-06-01 14:54:12

Uptime: 6:30:3

Firmware Version: V16.01.0.2(4182)

Device Name: AX3000 Dual Band GIgabit WiFi-6 Wireless Hotspot Router

CPU Usage: 0%

Memory Usage: 57%

Parameter description

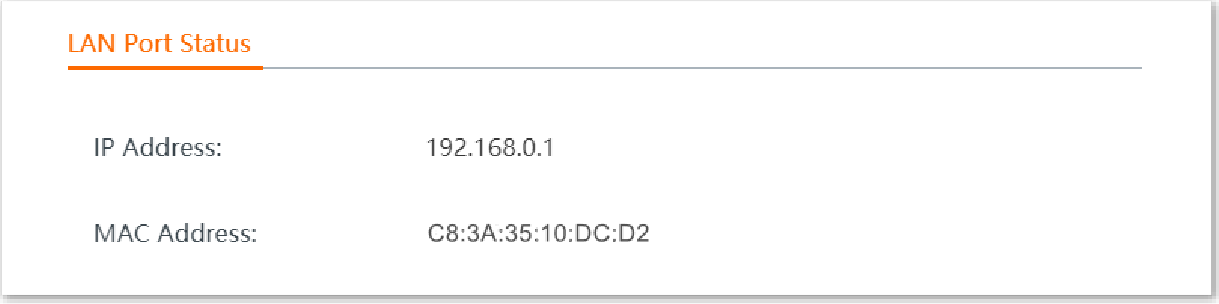
Parameter	**Description**
System Time	Specifies the current system time of the router. You can set system time by navigating to **Maintenance** > **System time**.
Uptime	Specifies the time that has elapsed since the router was started last time.
Firmware Version	Specifies the firmware version number of the router.
Device Name	Specifies the name of your router.
CPU Usage	Specifies the current CPU usage of the router.
Memory Usage	Specifies the current memory usage of the router.

LAN port status

This module displays the LAN IP address and the MAC address of the router.

TIP

You can modify LAN settings by navigating to **More** > LAN settings.



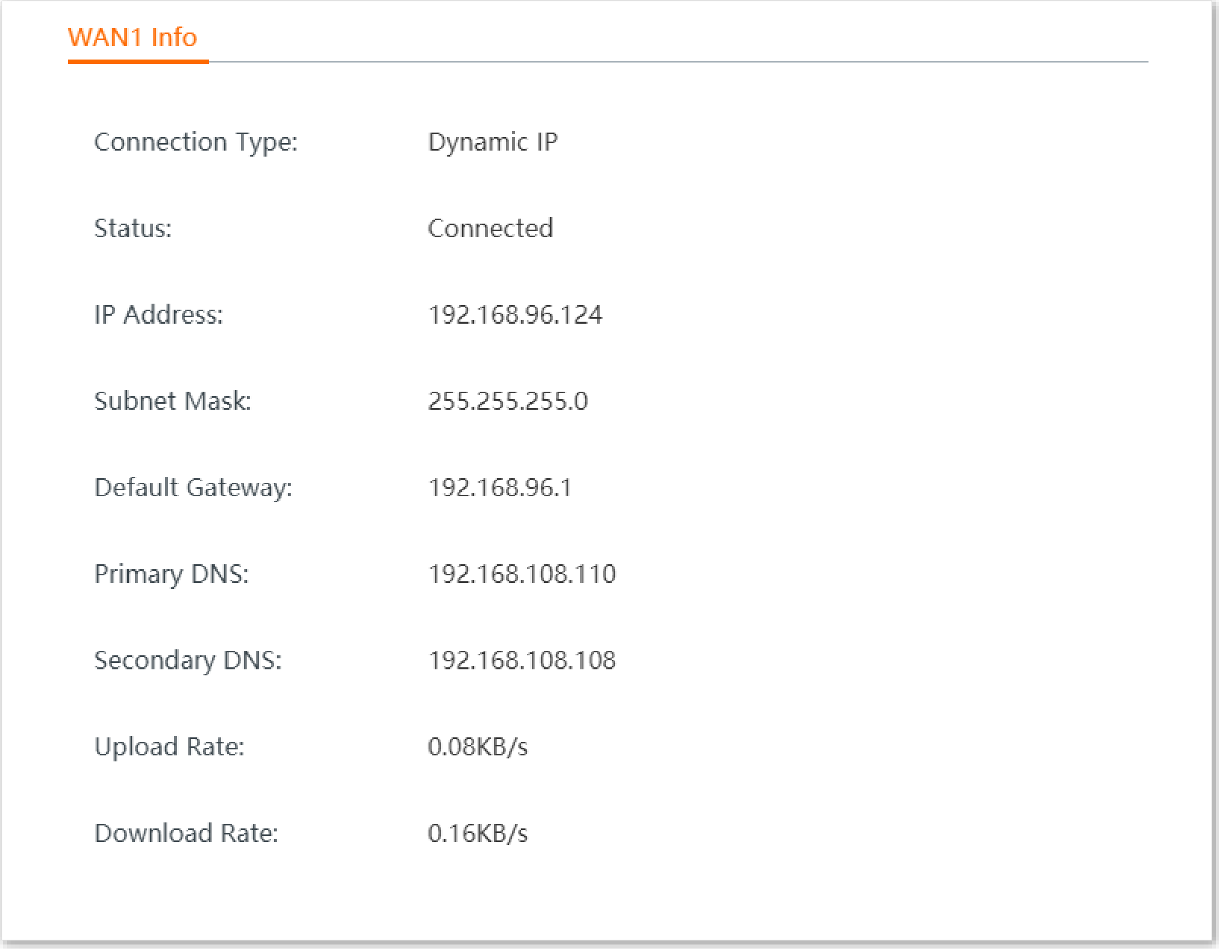
LAN Port Status

IP Address: 192.168.0.1

MAC Address: C8:3A:35:10:DC:D2

WAN info

This module displays parameters about all enabled WAN ports, including connection type, status, IP address and so on.



WAN1 Info

Connection Type: Dynamic IP

Status: Connected

IP Address: 192.168.96.124

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.96.1

Primary DNS: 192.168.108.110

Secondary DNS: 192.168.108.108

Upload Rate: 0.08KB/s

Download Rate: 0.16KB/s

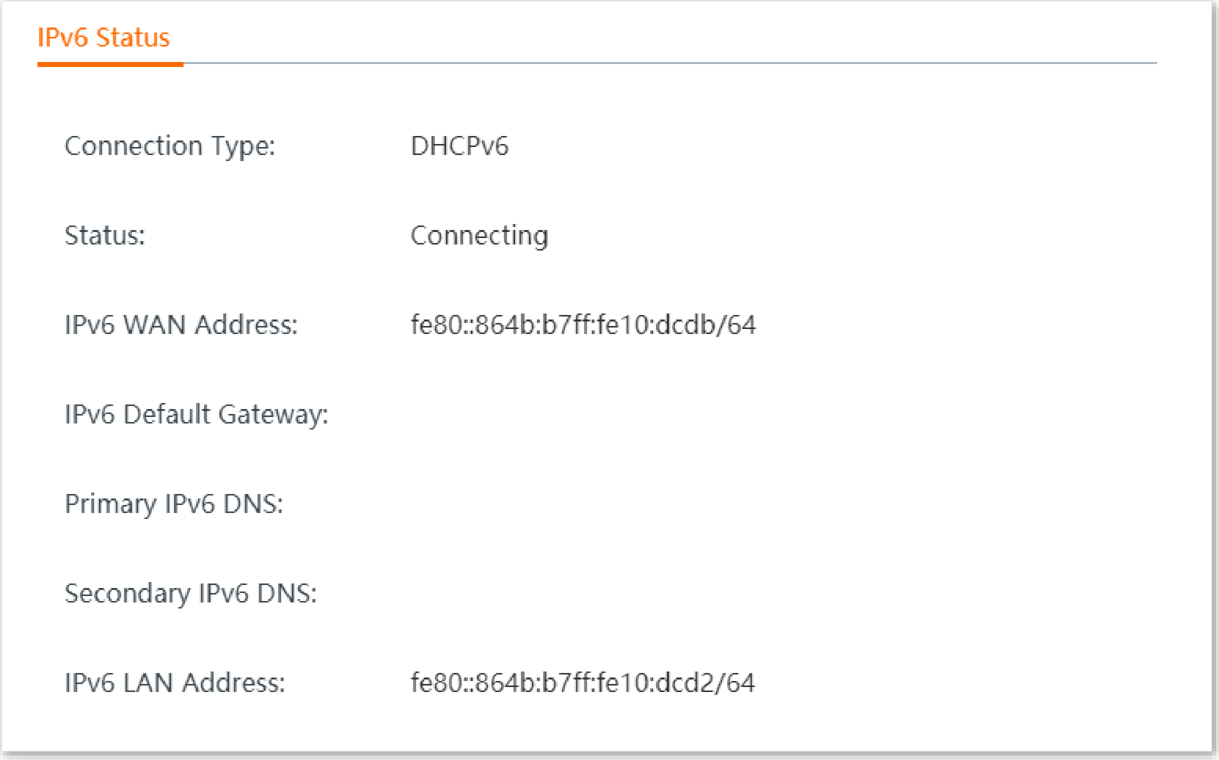
Parameter description

Parameter	Description
Connection Type	Specifies the internet connection type of the corresponding WAN port.

Parameter	Description
Status	Specifies whether or not the WAN port is plugged. If **Disconnected** appears, check its physical connection.
IP Address	Specifies the IP address of the corresponding WAN port.
Subnet Mask	Specifies the subnet mask of the corresponding WAN port.
Default Gateway	Specifies the gateway IP address of the corresponding WAN port.
Primary DNS	Specify the primary/secondary DNS server addresses of the corresponding WAN port.
Secondary DNS	
Upload Rate	Specify the upload and download rates of the corresponding WAN port.
Download Rate	

IPv6 status

This module displays the **Connection Type**, **Status** and other parameters of the IPv6 WAN port and the IPv6 LAN address (This part appears when you enable the IPv6 function).



IPv6 Status

Connection Type: DHCPv6

Status: Connecting

IPv6 WAN Address: fe80::864b:b7ff:fe10:dcdb/64

IPv6 Default Gateway:

Primary IPv6 DNS:

Secondary IPv6 DNS:

IPv6 LAN Address: fe80::864b:b7ff:fe10:dcd2/64

Parameter description

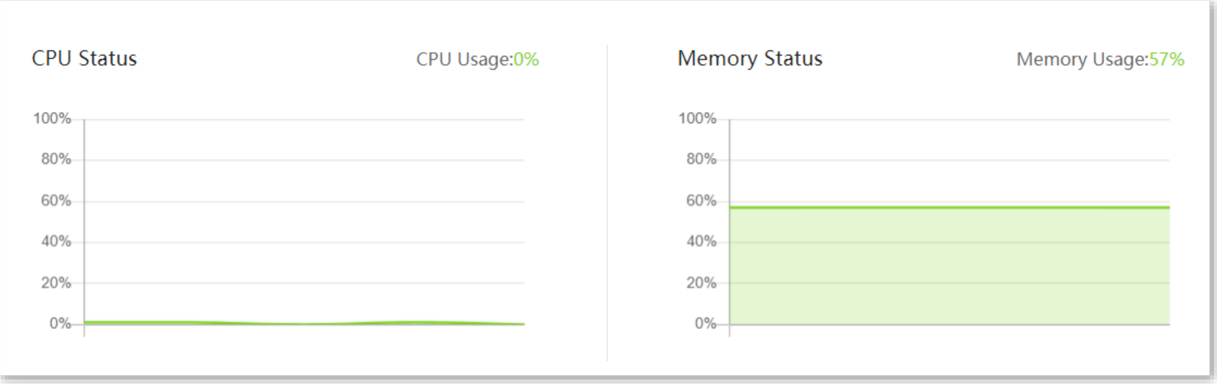
Parameter	Description
Connection Type	Specifies the internet connection type of the corresponding IPv6 WAN port.

Parameter	Description
Status	Specifies whether or not the IPv6 WAN port is plugged. If **Unplugged** appears, check its physical connection.
IPv6 WAN Address	Specifies the IP address of the corresponding IPv6 WAN port.
IPv6 Default Gateway	Specifies the gateway IP address of the corresponding IPv6 WAN port.
Primary IPv6 DNS	Specify the primary/secondary DNS server addresses of the corresponding IPv6 WAN port.
Secondary IPv6 DNS	
IPv6 LAN Address	Specifies the IP address of the corresponding IPv6 LAN port.

3.2 View CPU and memory status

Click **System Status** > **CPU Status/Memory Status** to enter the page.

Here, you can view the CPU and memory usage rates of the router.



CPU Status CPU Usage:0%

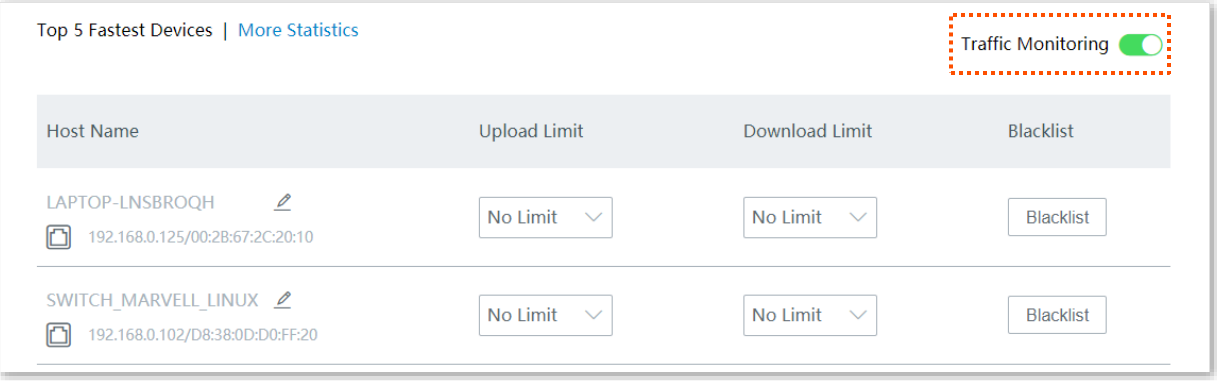
Memory Status Memory Usage:57%

3.3 Monitor traffic

3.3.1 Enable traffic monitoring

Click **System Status** > **Top 5 Fastest Devices** to enter the page.

Here, you can toggle on **Traffic Monitoring** to view the traffic statistics of the router. By default, it is disabled.



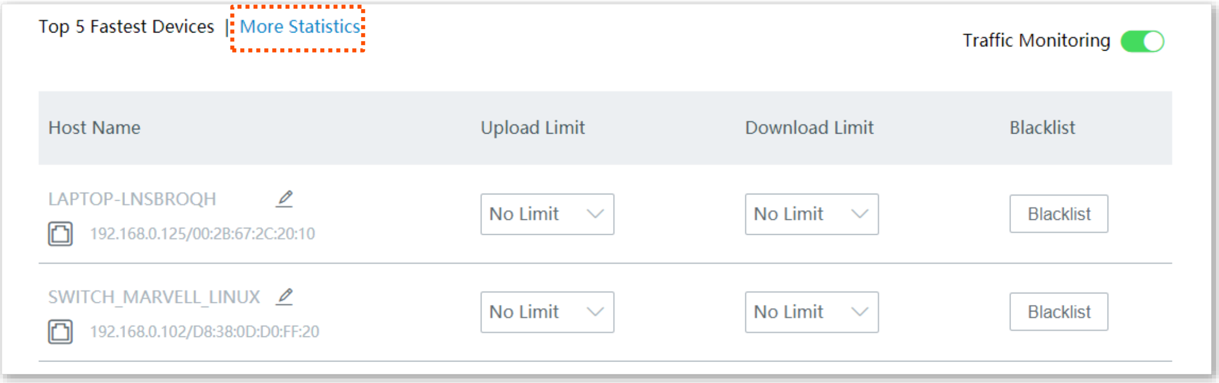
Top 5 Fastest Devices | More Statistics

Traffic Monitoring

Host Name	Upload Limit	Download Limit	Blacklist
LAPTOP-LNSBROQH 192.168.0.125/00:2B:67:2C:20:10	No Limit	No Limit	Blacklist
SWITCH_MARVELL_LINUX 192.168.0.102/D8:38:0D:D0:FF:20	No Limit	No Limit	Blacklist

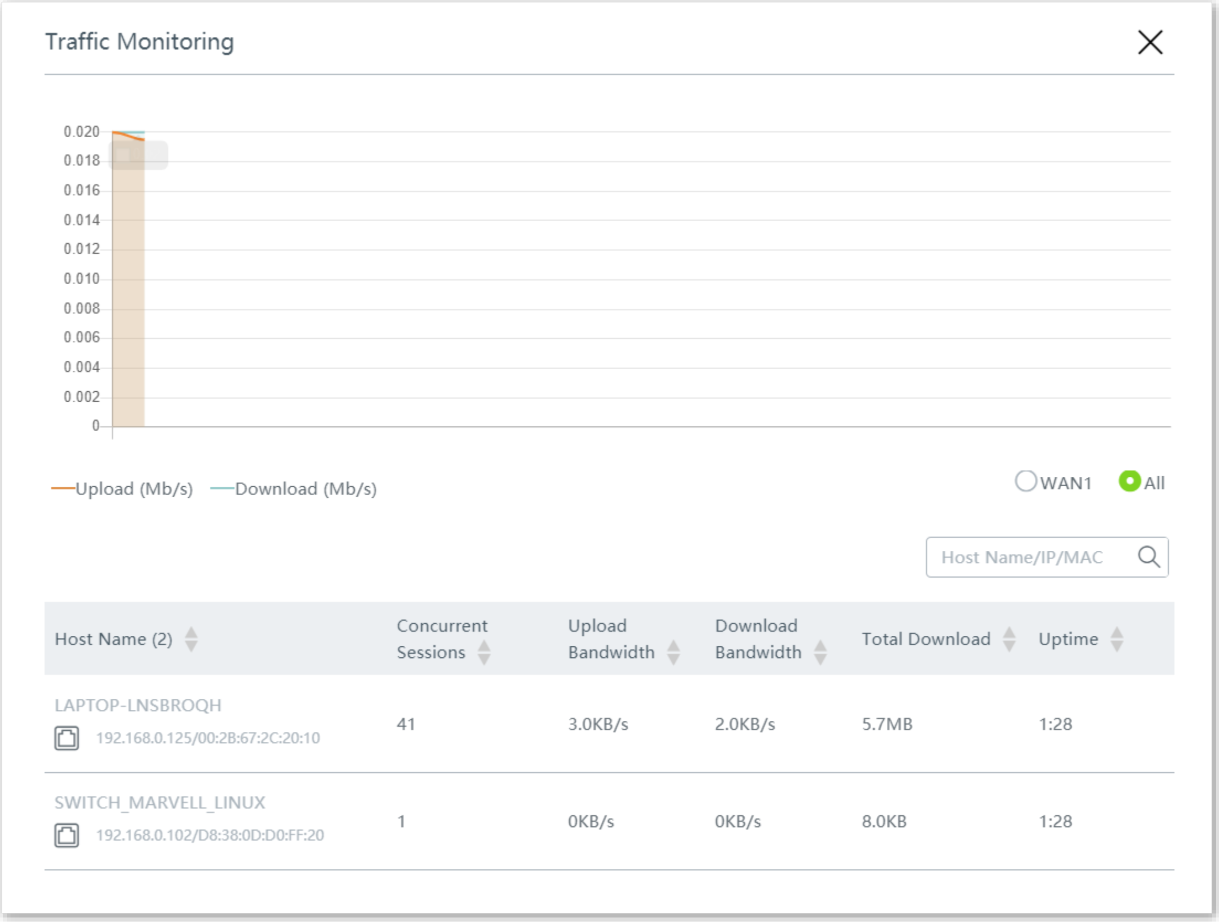
3.3.2 View traffic statistics

Click **System Status** > **More Statistics** to enter the page.



Host Name	Upload Limit	Download Limit	Blacklist
LAPTOP-LNSBROQH 192.168.0.125/00:2B:67:2C:20:10	No Limit	No Limit	Blacklist
SWITCH_MARVELL_LINUX 192.168.0.102/D8:38:0D:D0:FF:20	No Limit	No Limit	Blacklist

Here, you can view the dynamic flow of upload and download traffic on the WAN port of the router, and can also learn the basic information of certain client and relevant parameters such as **Upload Bandwidth**, **Download Bandwidth** and **Uptime**.



Host Name (2)	Concurrent Sessions	Upload Bandwidth	Download Bandwidth	Total Download	Uptime
LAPTOP-LNSBROQH 192.168.0.125/00:2B:67:2C:20:10	41	3.0KB/s	2.0KB/s	5.7MB	1:28
SWITCH_MARVELL_LINUX 192.168.0.102/D8:38:0D:D0:FF:20	1	0KB/s	0KB/s	8.0KB	1:28

Parameter description

Parameter	Description
Host Name	Specifies the names of clients connected to the router, connection way, their IP addresses, and MAC addresses.
Concurrent Sessions	Specifies the number of TCP connections between the client and the router.

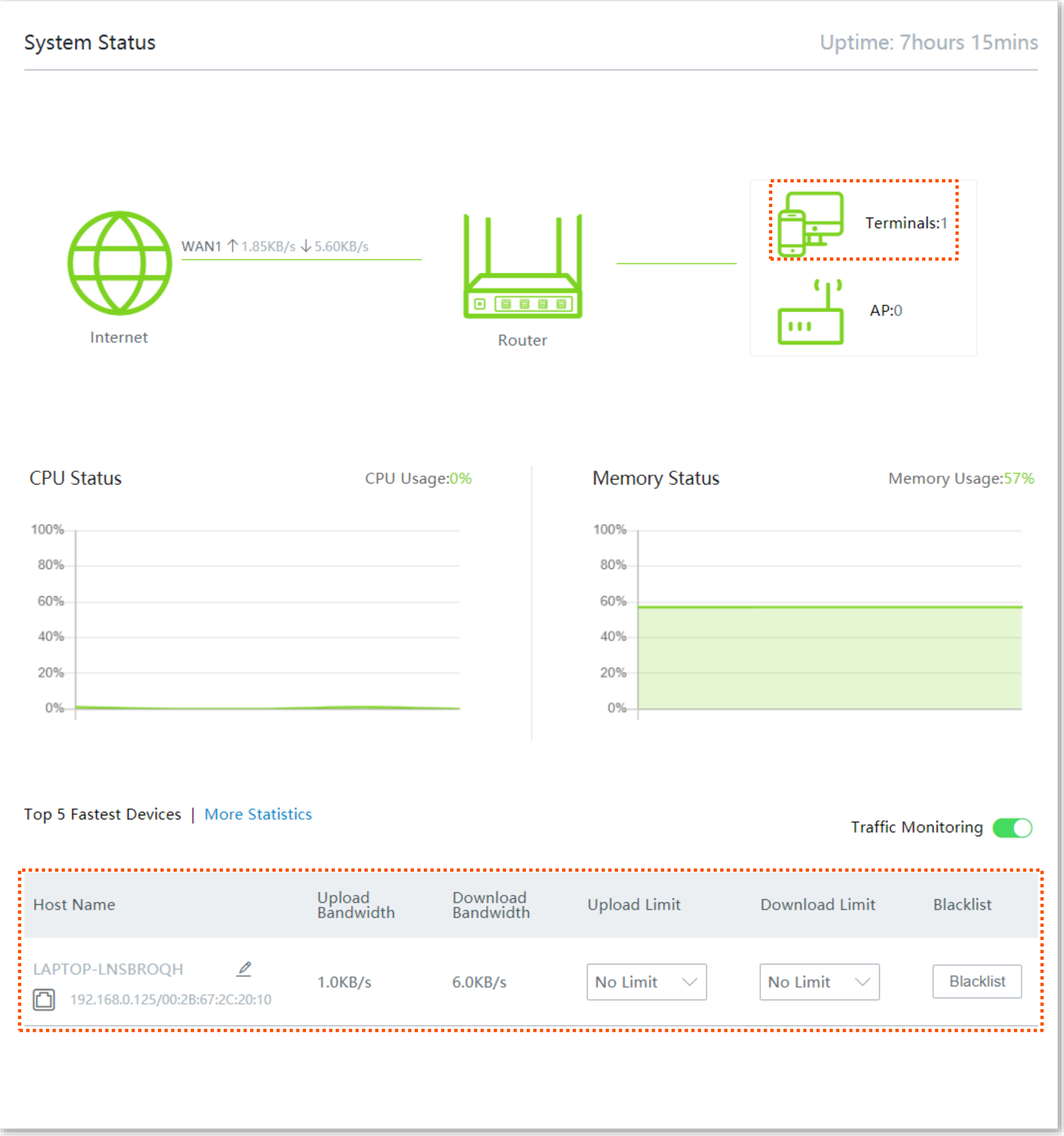
Parameter	Description
Upload Bandwidth	Specify the real-time upload/download bandwidth of each client.
Download Bandwidth	
Total Download	Specify the total download traffic utilized by each client.
Uptime	Specifies the connection time of each client. The format is **Hour:Minute**.

3.4 Manage online devices

Click **System Status** to enter the page.

Here, you can view and manage the top 5 fastest terminals, or click **Terminals** to view and manage all online terminal devices.

When managing all online terminal devices, you can enter the host name, IP address, MAC address in the search bar to filter them quickly.



Host Name	Upload Bandwidth	Download Bandwidth	Upload Limit	Download Limit	Blacklist
LAPTOP-LNSBROQH 192.168.0.125/00:2B:67:2C:20:10	1.0KB/s	6.0KB/s	No Limit	No Limit	Blacklist

3.5 Control bandwidth of online devices

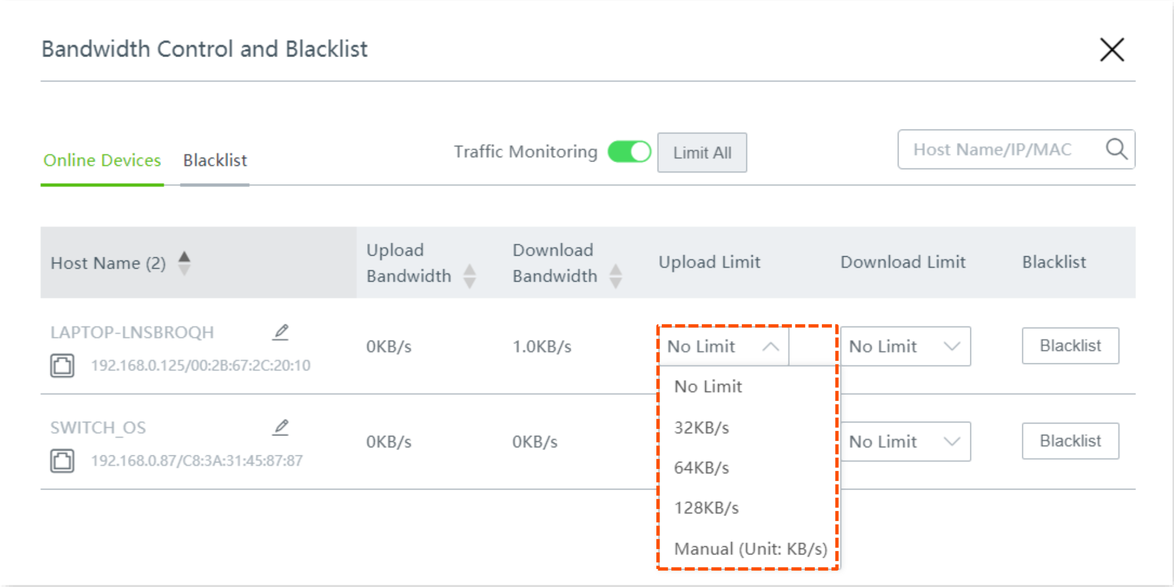
Click **System Status** to enter the page.

Here, you can control the bandwidth of top 5 fastest terminals, or click **Terminals** to control the bandwidth of all online terminal devices. Here takes all online terminal devices as an example.

Control bandwidth of online devices individually:

Step 1 Click **Terminals** to enter the **Bandwidth Control and Blacklist** page.

Step 2 Locate the devices as required, select a pre-defined value from the drop-down list menu of **Upload Limit** and/or **Download Limit**, or select **Manual** to specify a value manually.



Bandwidth Control and Blacklist

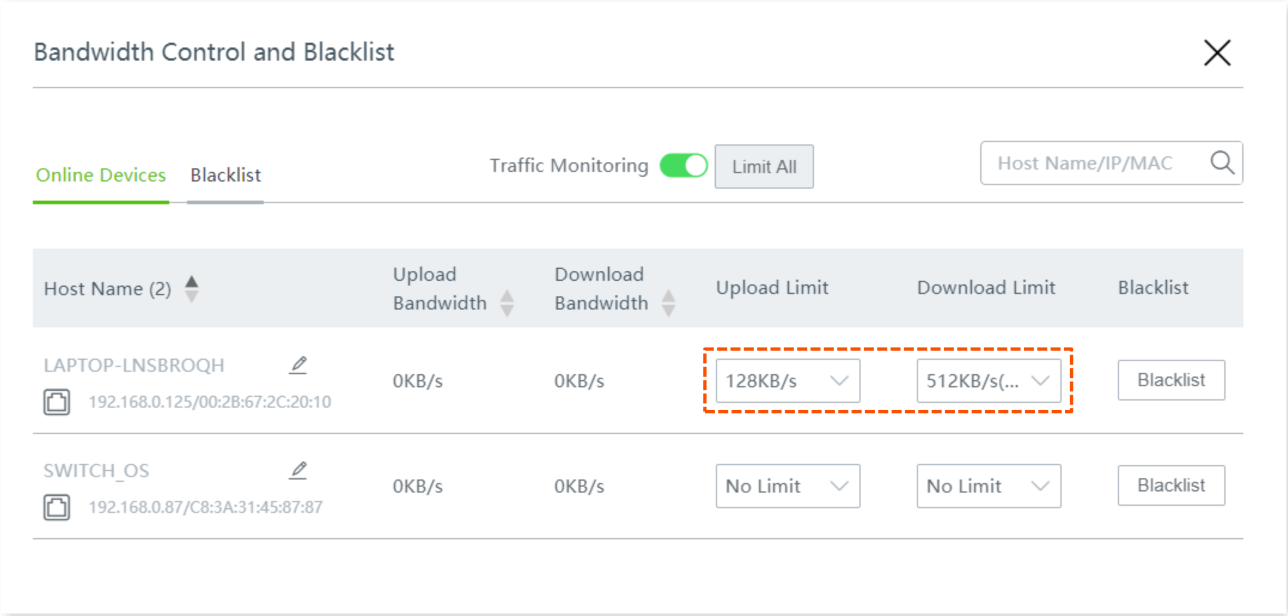
Online Devices | Blacklist

Traffic Monitoring | Limit All | Host Name/IP/MAC

Host Name (2)	Upload Bandwidth	Download Bandwidth	Upload Limit	Download Limit	Blacklist
LAPTOP-LNSBROQH 192.168.0.125/00:2B:67:2C:20:10	0KB/s	1.0KB/s	No Limit	No Limit	Blacklist
SWITCH_OS 192.168.0.87/C8:3A:31:45:87:87	0KB/s	0KB/s		No Limit	Blacklist

----End

You can view the configured upload and download limits of a device as shown below.



Bandwidth Control and Blacklist

Online Devices | Blacklist

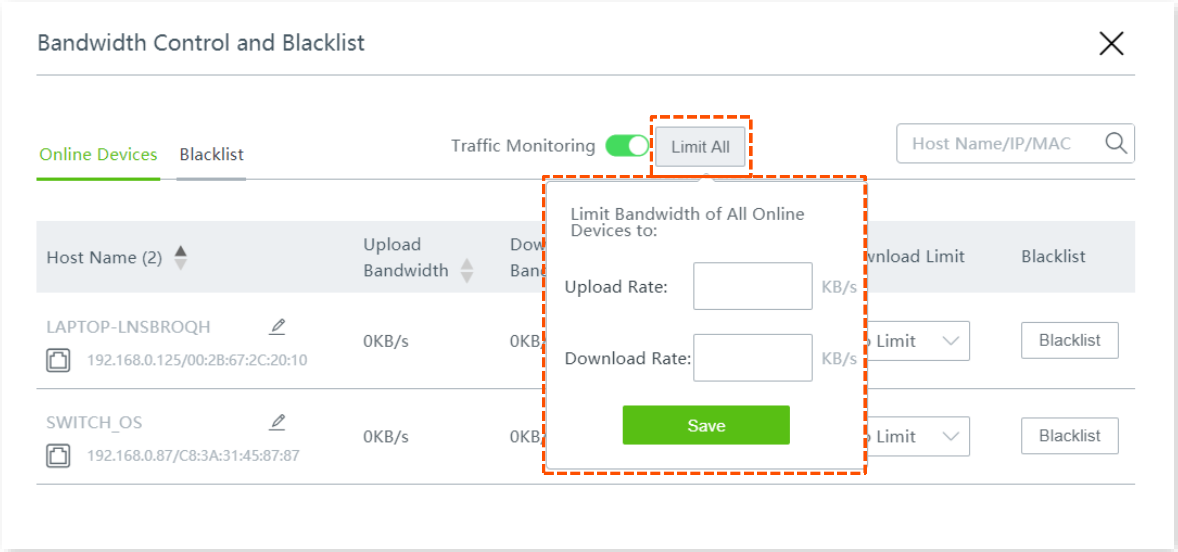
Traffic Monitoring | Limit All | Host Name/IP/MAC

Host Name (2)	Upload Bandwidth	Download Bandwidth	Upload Limit	Download Limit	Blacklist
LAPTOP-LNSBROQH 192.168.0.125/00:2B:67:2C:20:10	0KB/s	0KB/s	128KB/s	512KB/s(...	Blacklist
SWITCH_OS 192.168.0.87/C8:3A:31:45:87:87	0KB/s	0KB/s	No Limit	No Limit	Blacklist

Control bandwidth of online devices in batches:

Step 1 Click **Terminals** to enter the **Bandwidth Control and Blacklist** page.

Step 2 Click **Limit All**, specify the values according to your actual situation, and click **Save**.



Bandwidth Control and Blacklist

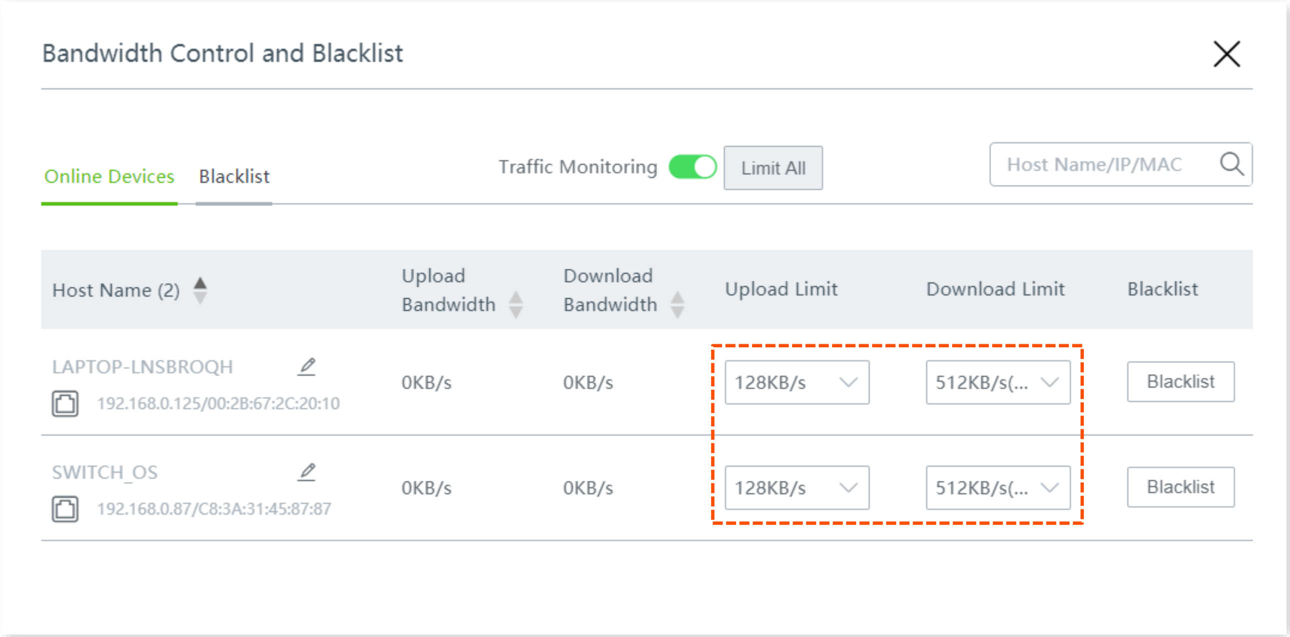
Limit Bandwidth of All Online Devices to:

Upload Rate: KB/s

Download Rate: KB/s

Host Name (2)	Upload Bandwidth	Dow Band	wnload Limit	Blacklist
LAPTOP-LNSBROQH 192.168.0.125/00:2B:67:2C:20:10	0KB/s	0KB	Limit	Blacklist
SWITCH_OS 192.168.0.87/C8:3A:31:45:87:87	0KB/s	0KB	Limit	Blacklist

You can view the configured upload and download limits of all online devices as shown below.



Bandwidth Control and Blacklist

Host Name (2)	Upload Bandwidth	Download Bandwidth	Upload Limit	Download Limit	Blacklist
LAPTOP-LNSBROQH 192.168.0.125/00:2B:67:2C:20:10	0KB/s	0KB/s	128KB/s	512KB/s(...	Blacklist
SWITCH_OS 192.168.0.87/C8:3A:31:45:87:87	0KB/s	0KB/s	128KB/s	512KB/s(...	Blacklist

NOTE

Upload/download limits of devices that are configured by Limit by Group policy cannot be modified here.

3.6 Blacklist

Click **System Status** to enter the page.

Here, you can add devices to or remove devices from the blacklist.

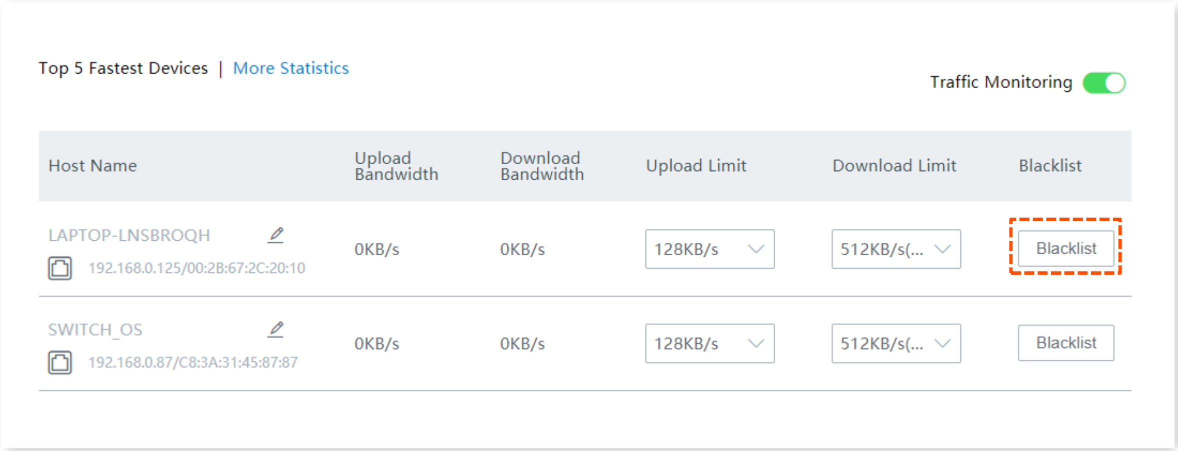
3.6.1 Add devices to blacklist

The blocked devices will be moved to the **Blacklist** section, and cannot connect to your router.

Add top 5 fastest devices to blacklist:

Step 1 Locate the device on the **System Status** page.

Step 2 Click **Blacklist**.



Top 5 Fastest Devices | More Statistics

Traffic Monitoring

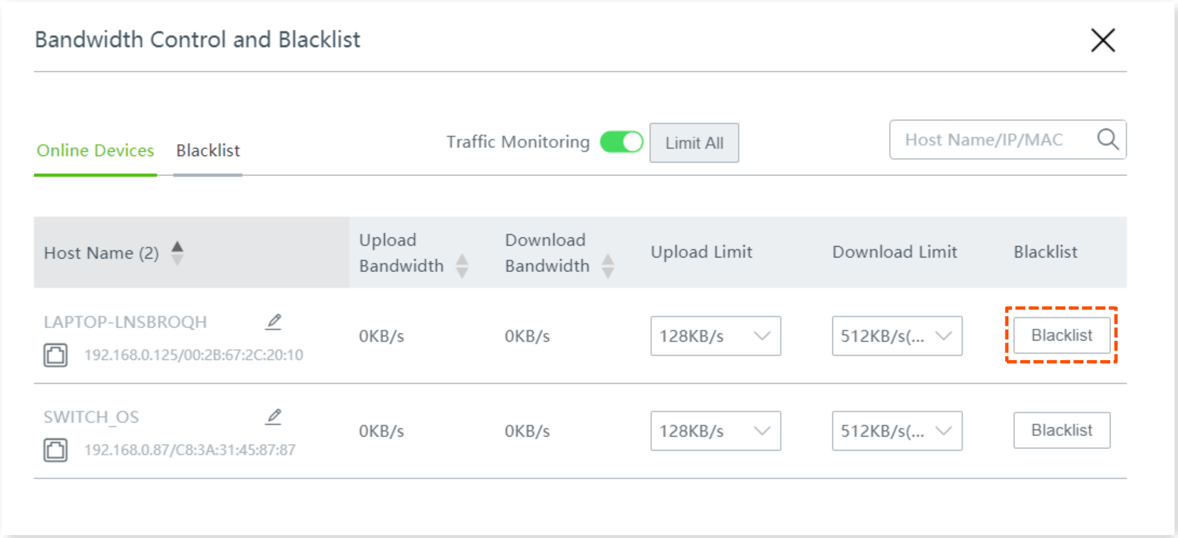
Host Name	Upload Bandwidth	Download Bandwidth	Upload Limit	Download Limit	Blacklist
LAPTOP-LNSBROQH 192.168.0.125/00:2B:67:2C:20:10	0KB/s	0KB/s	128KB/s	512KB/s(...	Blacklist
SWITCH_OS 192.168.0.87/C8:3A:31:45:87:87	0KB/s	0KB/s	128KB/s	512KB/s(...	Blacklist

----End

Add other online devices to blacklist:

Step 1 Click **Terminals** to enter the **Bandwidth Control and Blacklist** page.

Step 2 Locate the device among **Online Devices**, and click **Blacklist**.

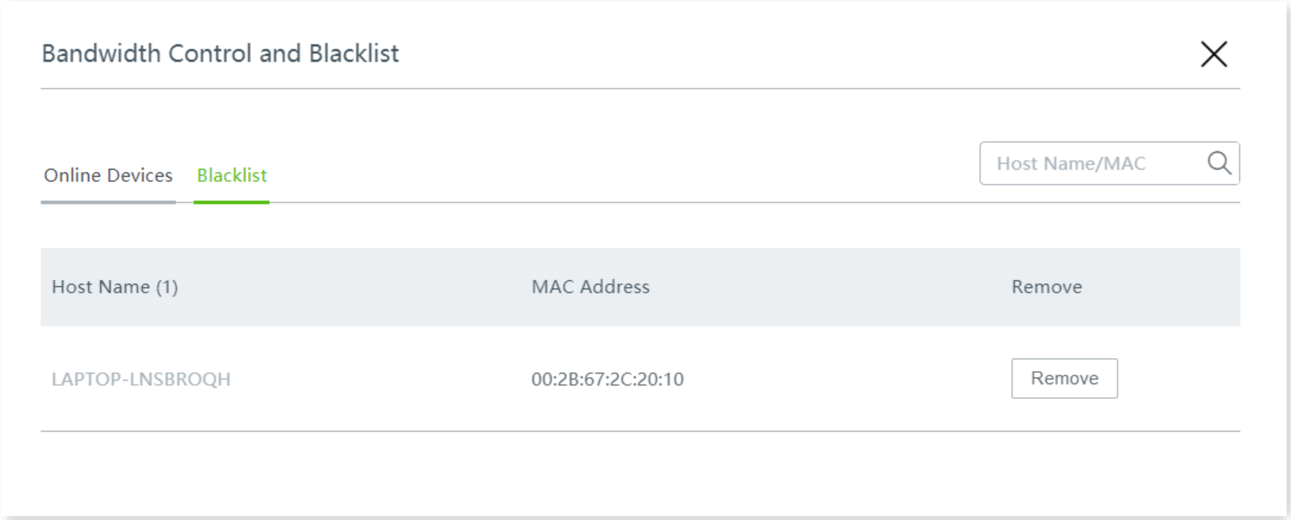


Bandwidth Control and Blacklist

Host Name (2)	Upload Bandwidth	Download Bandwidth	Upload Limit	Download Limit	Blacklist
LAPTOP-LNSBROQH 192.168.0.125/00:2B:67:2C:20:10	0KB/s	0KB/s	128KB/s	512KB/s(...	Blacklist
SWITCH_OS 192.168.0.87/C8:3A:31:45:87:87	0KB/s	0KB/s	128KB/s	512KB/s(...	Blacklist

----End

You can view the blocked devices on the **Blacklist** page as shown below.



Bandwidth Control and Blacklist

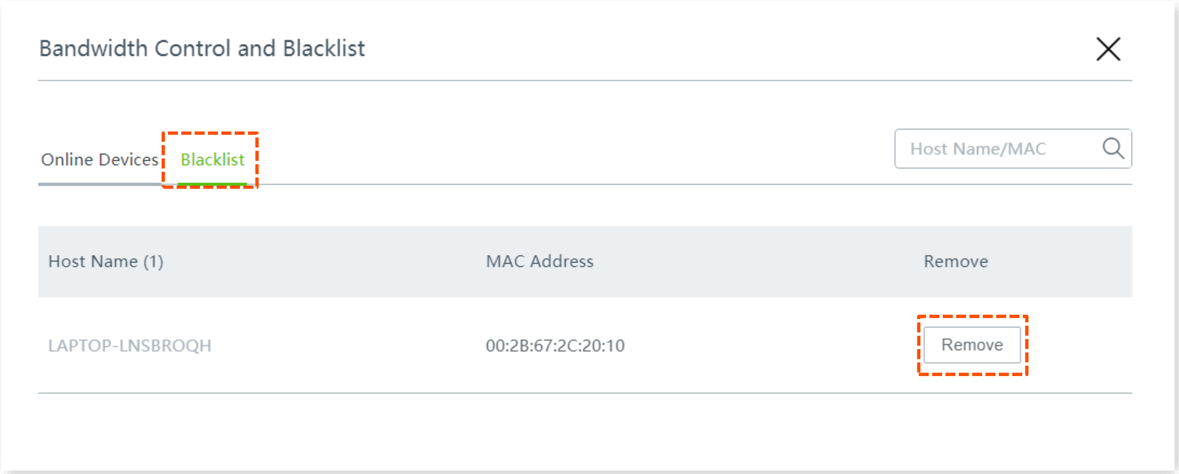
Host Name (1)	MAC Address	Remove
LAPTOP-LNSBROQH	00:2B:67:2C:20:10	Remove

3.6.2 Remove devices from blacklist

The unblocked devices can connect to your router again.

Step 1 Click **Terminals** to enter the **Bandwidth Control and Blacklist** page.

Step 2 Locate the device among the **Blacklist**, and click **Remove**.



Bandwidth Control and Blacklist

Host Name (1)	MAC Address	Remove
LAPTOP-LNSBROQH	00:2B:67:2C:20:10	Remove

----End

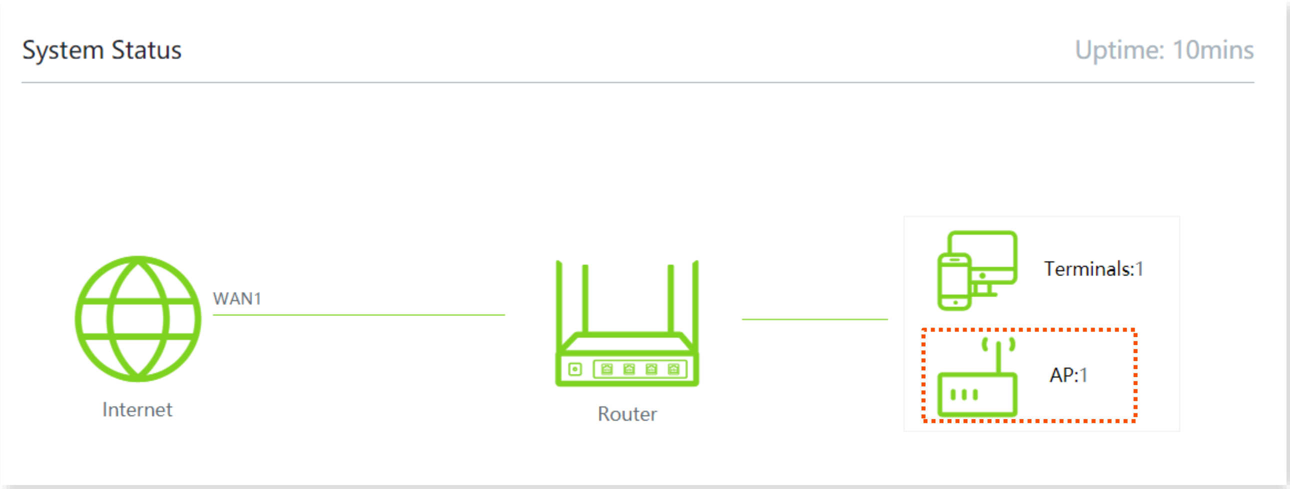
3.7 Manage APs

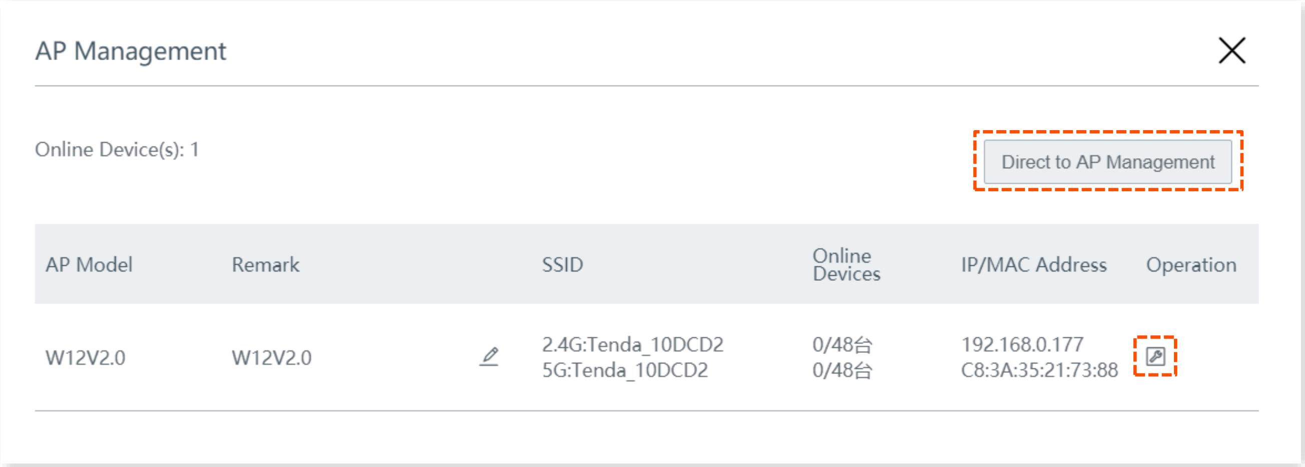
Click **System Status** to enter the page.

Here, you can view and manage the online APs in the network.

If you want to perform further configurations concerning the connected APs, please refer to AP management.

To access the configuration page, click the **AP** icon. The **AP Management** window appears.





Online Device(s): 1

AP Model	Remark	SSID	Online Devices	IP/MAC Address	Operation
W12V2.0	W12V2.0 ✎	2.4G:Tenda_10DCD2 5G:Tenda_10DCD2	0/48台 0/48台	192.168.0.177 C8:3A:35:21:73:88	✎

Parameter description

Parameter	Description
AP Model	Specifies the model of the corresponding AP.
Remark	Specifies the remark name that you leave for the corresponding AP.
SSID	Specifies the WiFi SSID of the corresponding AP, including 2.4G and 5G WiFi. You can change the remark for the AP by clicking ✎
Online Devices	Specifies the number of online devices of each wireless network.
IP/MAC Address	Specifies the IP address and MAC address of the corresponding AP.

Parameter	Description
Operation	By clicking ⚙, you are directed to the web UI of the AP.
Direct to AP Management	By clicking this button, you are directed to the configuration page of **AP Management.**

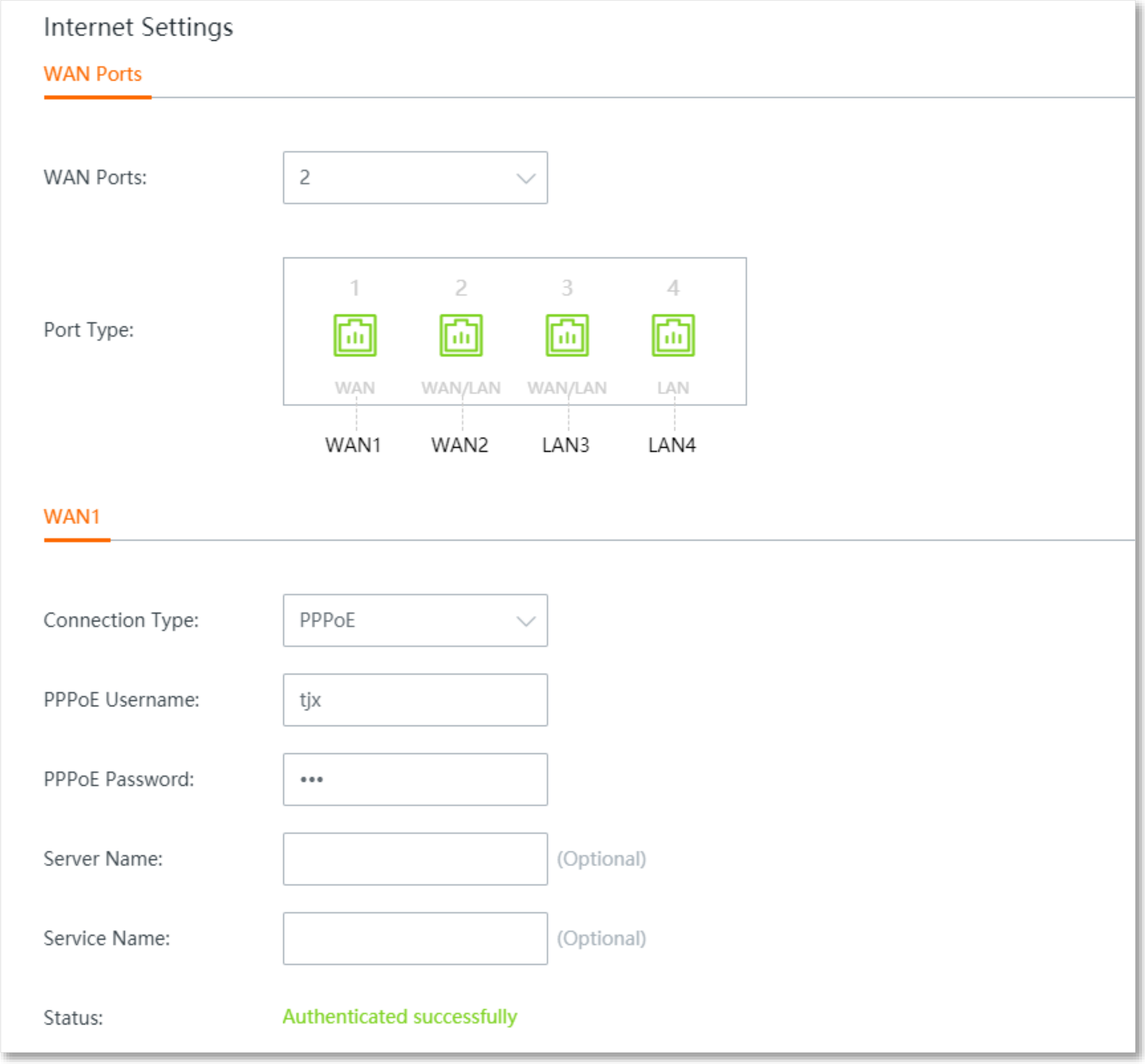
4 Internet settings

4.1 Internet Settings

4.1.1 Overview

Click **Internet Settings** to enter the page.

Here, you can configure the internet settings of the router for multiple devices in the LAN to share.



Internet Settings

WAN Ports

WAN Ports: 2

Port Type:

WAN1

Connection Type: PPPoE

PPPoE Username: tjx

PPPoE Password: •••

Server Name: (Optional)

Service Name: (Optional)

Status: Authenticated successfully

Parameter description

Parameter	Description
WAN Ports	Specifies how many WAN ports you can set on the router. By default, the router has only one WAN port (the WAN1 port), and you can set **3** WAN ports at most.

Parameter	Description
Port Type	Indicates that the port functions as a WAN port or a LAN port, as well as the port is connected or not. 🟩: The port is connected properly. ⬜: The port is disconnected or improperly connected.
Connection Type	Specifies in which way the router is connected to the internet. The router supports **PPPoE**, **Static IP**, and **Dynamic IP**. Refer to the table [Choose your connection type]() for details. TIP The router supports **PPPoE Russia**, **PPTP/PPTP Russia**, and **L2TP/L2TP Russia** as well. These three connection types are only applicable to Russia and its vicinity.
PPPoE Username	These two parameters are required only when your internet connection type is **PPPoE** or **PPPoE Russia**. You can obtain them from your ISP.
PPPoE Password	
Server Name	These two parameters are required only when your internet connection type is **PPPoE** or **PPPoE Russia**. Enter these two parameters (optional) provided by your ISP.
Service Name	
PPTP Server Address	This parameter is required only when your internet connection type is **PPTP/PPTP Russia**. You can obtain it from your ISP.
L2TP Server Address	This parameter is required only when your internet connection type is **L2TP/L2TP Russia**. You can obtain it from your ISP.
User Name	These two parameters are required only when your internet connection type is **PPTP/PPTP Russia** or **L2TP/L2TP Russia**. You can obtain them from your ISP.
Password	
Obtain an IP address	This parameter appears when your internet connection type is **PPPoE Russia**, **PPTP/PPTP Russia**, or **L2TP/L2TP Russia**. If there is no DHCP server in the network, select **Manual** and enter the IP address and related parameters. If there is a DHCP server in the network, select **Auto**, and the device will obtain these parameters from the DHCP server.
IP Address	These parameters are required only when your internet connection type is **Static IP** or if you set **Obtain an IP address** to **Manual** when your internet connection type is **PPPoE Russia**, **PPTP/PPTP Russia**, or **L2TP/L2TP Russia**. The **Secondary DNS** parameter is optional. You can obtain them from your ISP.
Subnet Mask	
Default Gateway	
Primary DNS	
Secondary DNS	

Parameter	Description
Status	Specifies the connection status of the corresponding WAN port. ● **Authenticated successfully/networked**: The WAN port is connected to the internet or server. ● **Connecting…**: The router is connecting to the internet or server. ● **Disconnected**: The port is physically disconnected, or fails to connect to the internet or server. Please check if the physical connections are proper, or the parameters you entered are correct.

4.1.2 Configure multiple WAN ports

The router supports **3** WAN ports at most. The multi-WAN port feature allows you to aggregate bandwidth, enjoy uninterrupted broadband service even in case of connection malfunction, and make ISP route selection, thus getting better utilization of your bandwidth.

Assume that:

WAN1 internet connection type is **PPPoE**, and PPPoE information is as follows:

- PPPoE username: tdxy123
- PPPoE password: ipxz456

WAN2 internet connection type is **Dynamic IP**.

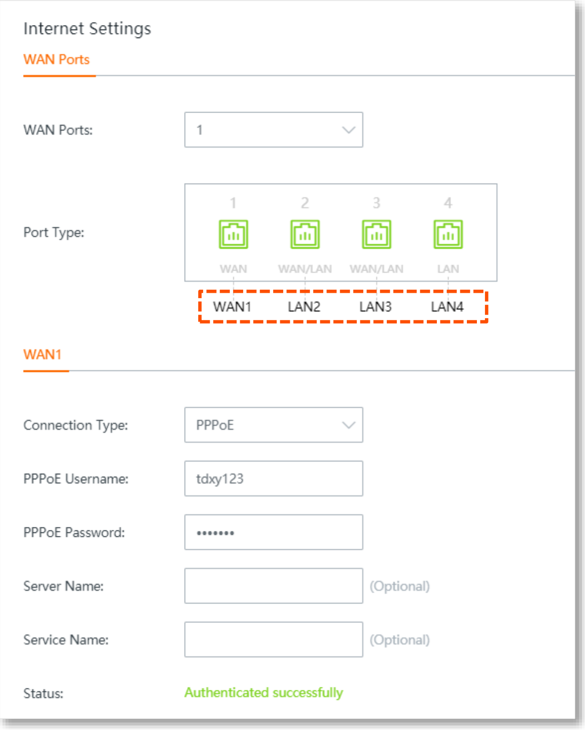
Configuration procedure

TIP

- Parameters for internet access are provided by your ISP. Refer to Choose your connection type table for detailed description. Values used here are only for examples.
- Modifying number of WAN ports makes the router reboot.
- The following procedure describes how to configure 2 WAN ports. You can refer to the following steps to increase or decrease WAN ports as needed.

Step 1 Select the number of WAN ports from the **WAN Ports** drop-down list menu, which is **2** in this example.

The port marked with **LAN2** changes into **WAN2**, and the WAN2 configuration area appears.



Internet Settings

WAN Ports

WAN Ports: 1

Port Type:

WAN1

Connection Type: PPPoE

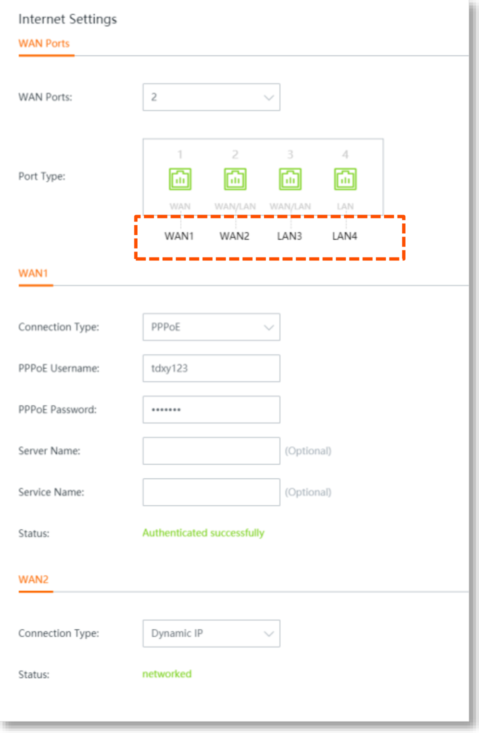
PPPoE Username: tdxy123

PPPoE Password: •••••••

Server Name: (Optional)

Service Name: (Optional)

Status: Authenticated successfully



Internet Settings

WAN Ports

WAN Ports: 2

Port Type:

WAN1

Connection Type: PPPoE

PPPoE Username: tdxy123

PPPoE Password: •••••••

Server Name: (Optional)

Service Name: (Optional)

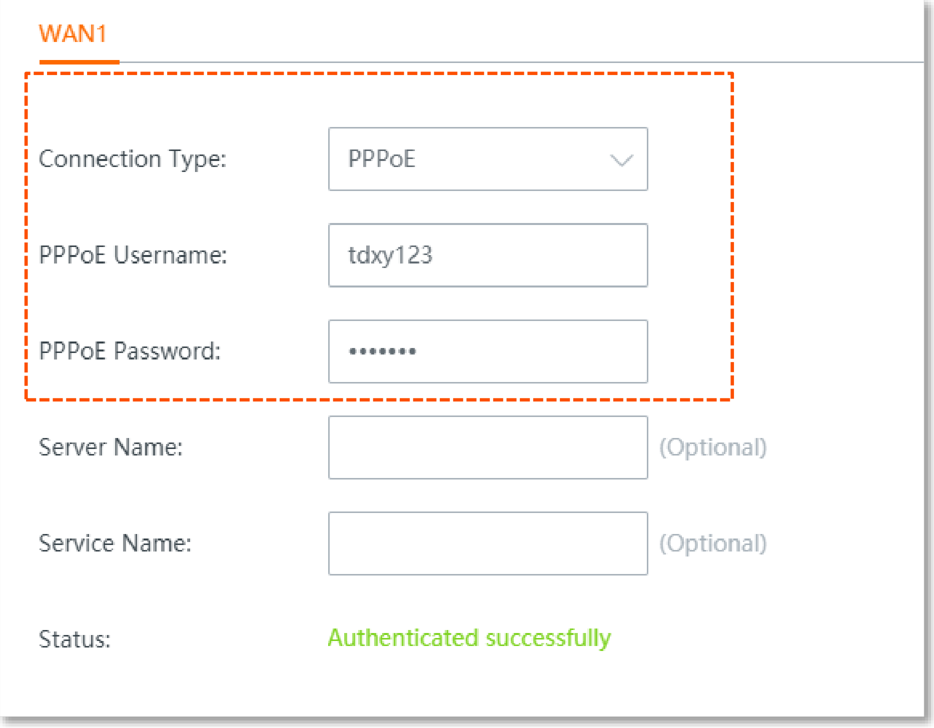
Status: Authenticated successfully

WAN2

Connection Type: Dynamic IP

Status: networked

Step 2 On the **WAN1** configuration area, enter the PPPoE information provided by your ISP.



WAN1

Connection Type: PPPoE

PPPoE Username: tdxy123

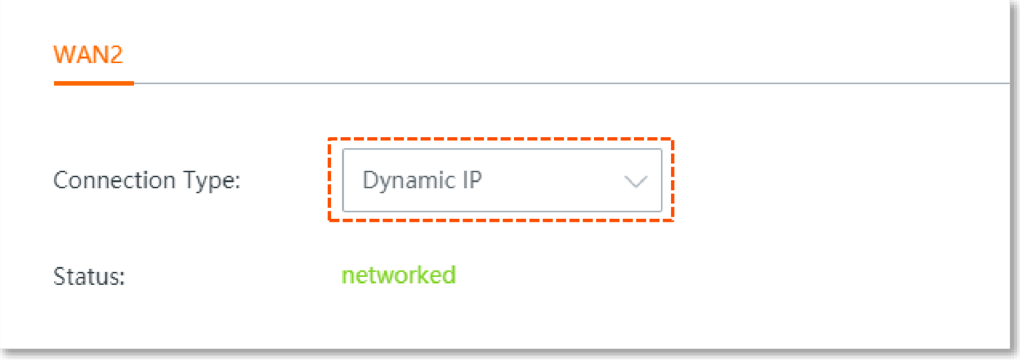
PPPoE Password: •••••••

Server Name: (Optional)

Service Name: (Optional)

Status: Authenticated successfully

Step 3 On the **WAN2** configuration area, set **Connection Type** to **Dynamic IP**.



WAN2

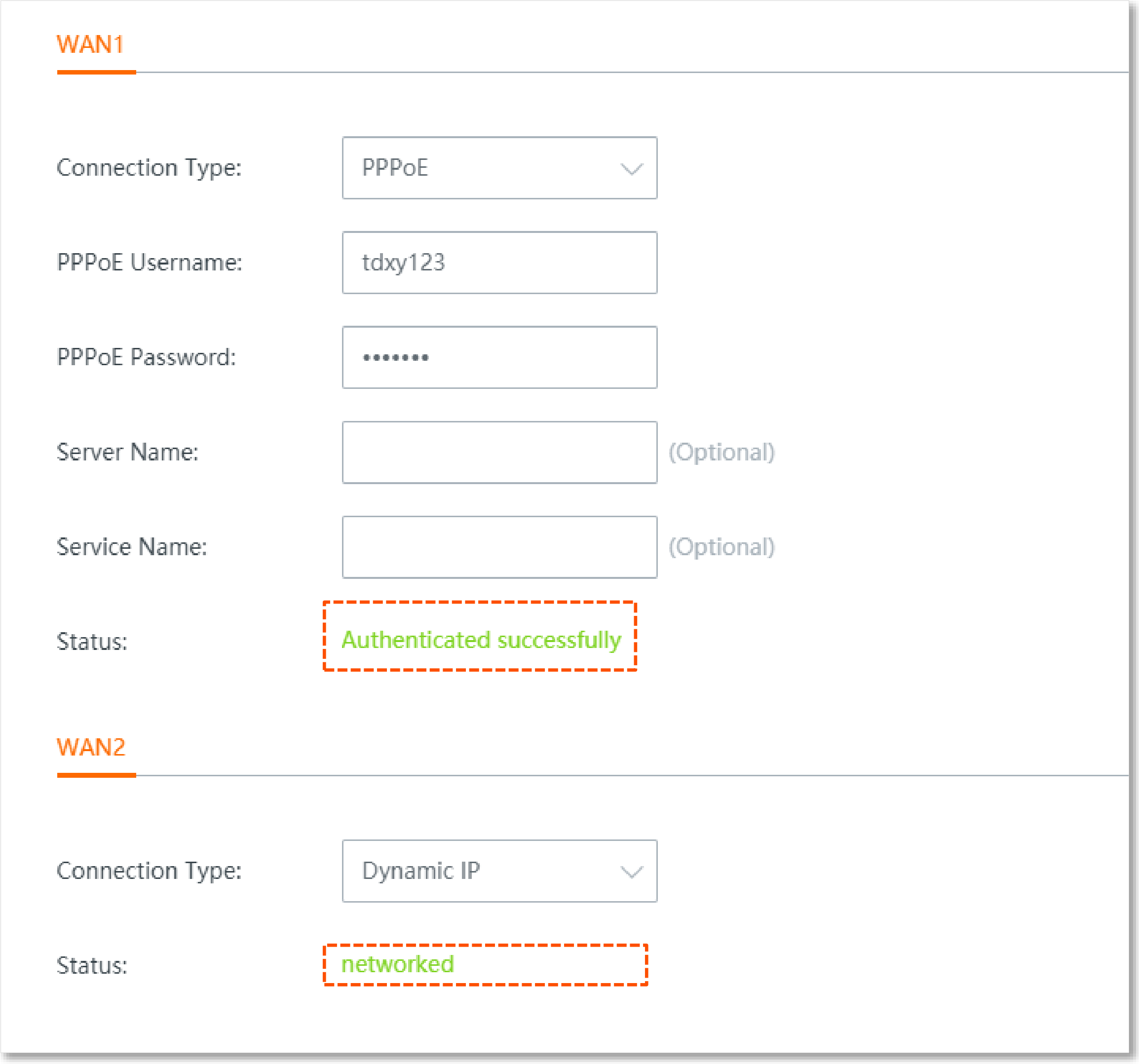
Connection Type: Dynamic IP

Status: networked

Step 4 Click **Save** at the bottom of the page to apply your settings.

----End

Wait a moment. The router performs rebooting to apply your settings. When the status shows **Authenticated successfully** or **networked**, your configuration is successful. See the following figure:



WAN1

Connection Type:	PPPoE
PPPoE Username:	tdxy123
PPPoE Password:	•••••••
Server Name:	(Optional)
Service Name:	(Optional)
Status:	Authenticated successfully

WAN2

Connection Type:	Dynamic IP
Status:	networked

4.1.3 Set up for internet access

This section describes how to set up to access the internet using different connection types.

Choose the proper connection type according to your actual environment. Use the table below to help you select your internet connection type if you are uncertain about how to select one.

Choose your connection type:

Connection Type	Available Parameters
PPPoE	PPPoE username, PPPoE password, server name, and service name.
Static IP	IP address, subnet mask, default gateway, primary DNS, and secondary DNS (optional).
Dynamic IP	None or the device is connected to an upstream device which can access the internet and has its DHCP server enabled.
PPPoE Russia	PPPoE username, PPPoE password, server name, and service name. If the DHCP server of the upstream device is disabled (means you have to select **Manual** for **Obtain an IP address**), then the IP address, subnet mask, default gateway, and primary DNS are required.
PPTP/PPTP Russia	PPTP server address, user name, and password. If the DHCP server of the upstream device is disabled (means you have to select **Manual** for **Obtain an IP address**), then the IP address, subnet mask, default gateway, and primary DNS are required.
L2TP/L2TP Russia	L2TP server address, user name, and password. If the DHCP server of the upstream device is disabled (means you have to select **Manual** for **Obtain an IP address**), then the IP address, subnet mask, default gateway, and primary DNS are required.

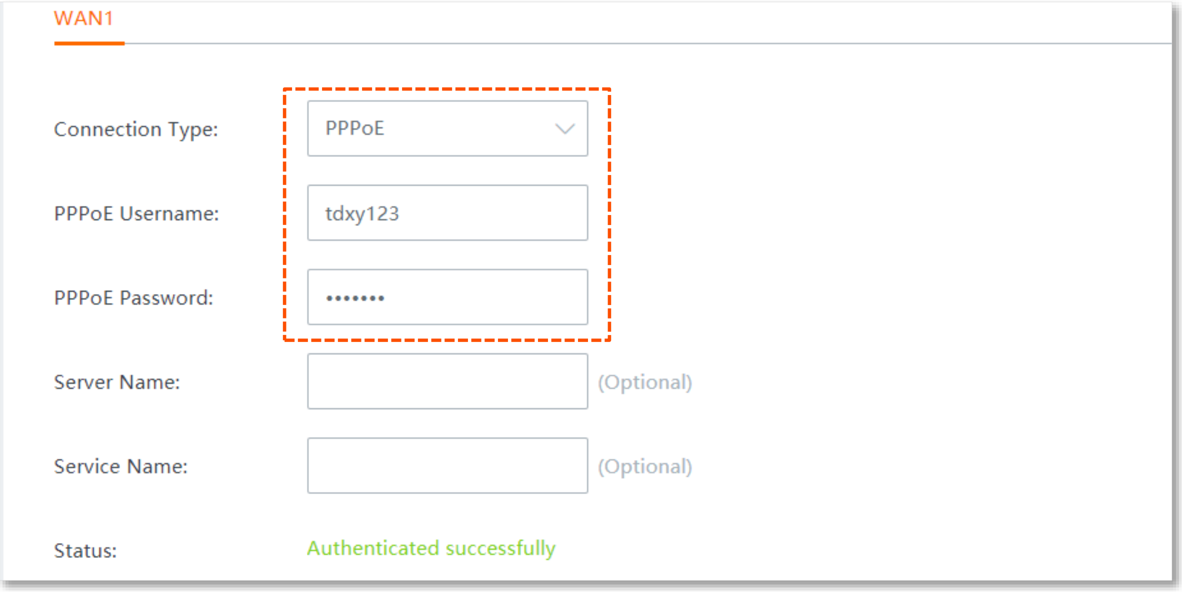
PPPoE

Step 1 Navigate to **Internet Settings** > **Internet Settings**.

Step 2 Set **Connection Type** to **PPPoE**.

Step 3 Enter the **PPPoE Username** and **PPPoE Password** provided by your ISP.

Step 4 Click **Save** at the bottom of the page to apply your settings.



WAN1

Connection Type: PPPoE

PPPoE Username: tdxy123

PPPoE Password: •••••••

Server Name: (Optional)

Service Name: (Optional)

Status: Authenticated successfully

----End

Wait a moment. When the **Status** shows **Authenticated successfully**, the router is connected to the internet successfully

If the username and password you entered are correct but the router fails to connect to the internet, try to modify WAN parameters in **Internet Settings** > **WAN Parameters**.

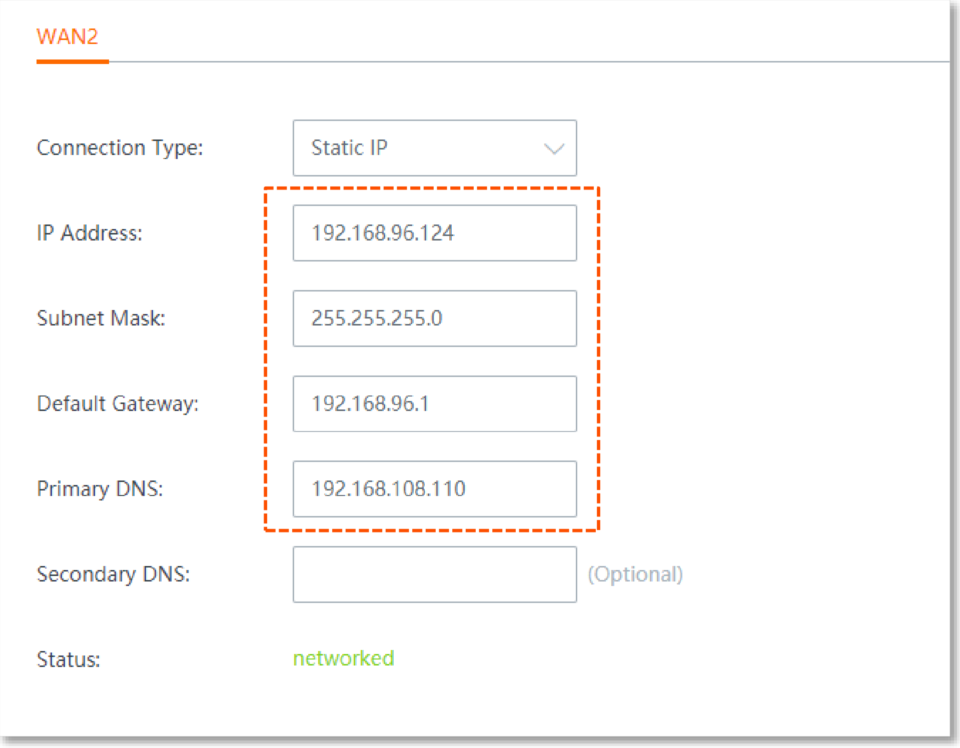
Static IP

Step 1 Navigate to **Internet Settings** > **Internet Settings**.

Step 2 Set **Connection Type** to **Static IP.**

Step 3 Enter the **IP Address**, **Subnet Mask**, **Default Gateway and Primary/Secondary DNS** provided by your ISP.

Step 4 Click **Save** at the bottom of the page to apply your settings.



WAN2

Connection Type:	Static IP
IP Address:	192.168.96.124
Subnet Mask:	255.255.255.0
Default Gateway:	192.168.96.1
Primary DNS:	192.168.108.110
Secondary DNS:	(Optional)
Status:	networked

----End

Wait a moment. When the **Status** shows **networked**, the router is connected to the internet successfully.

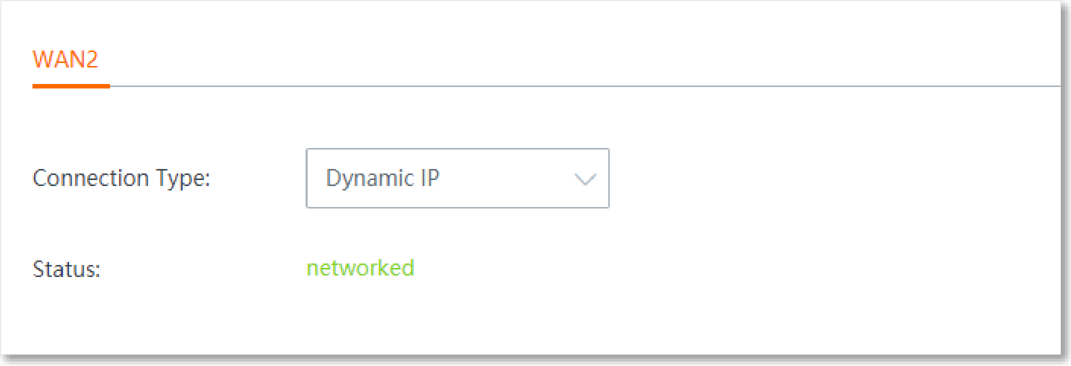
If the router fails to connect to the internet, try to modify WAN parameters in **Internet Settings** > **WAN Parameters**.

Dynamic IP

Step 1 Navigate to **Internet Settings** > **Internet Settings**.

Step 2 Set **Connection Type** to **Dynamic IP.**

Step 3 Click **Save** at the bottom of the page to apply your settings.



Connection Type: Dynamic IP

Status: networked

----End

Wait a moment. When the **Status** shows **networked**, the router is connected to the internet successfully.

If the router fails to connect to the internet, try to modify WAN parameters in **Internet Settings** > **WAN Parameters**.

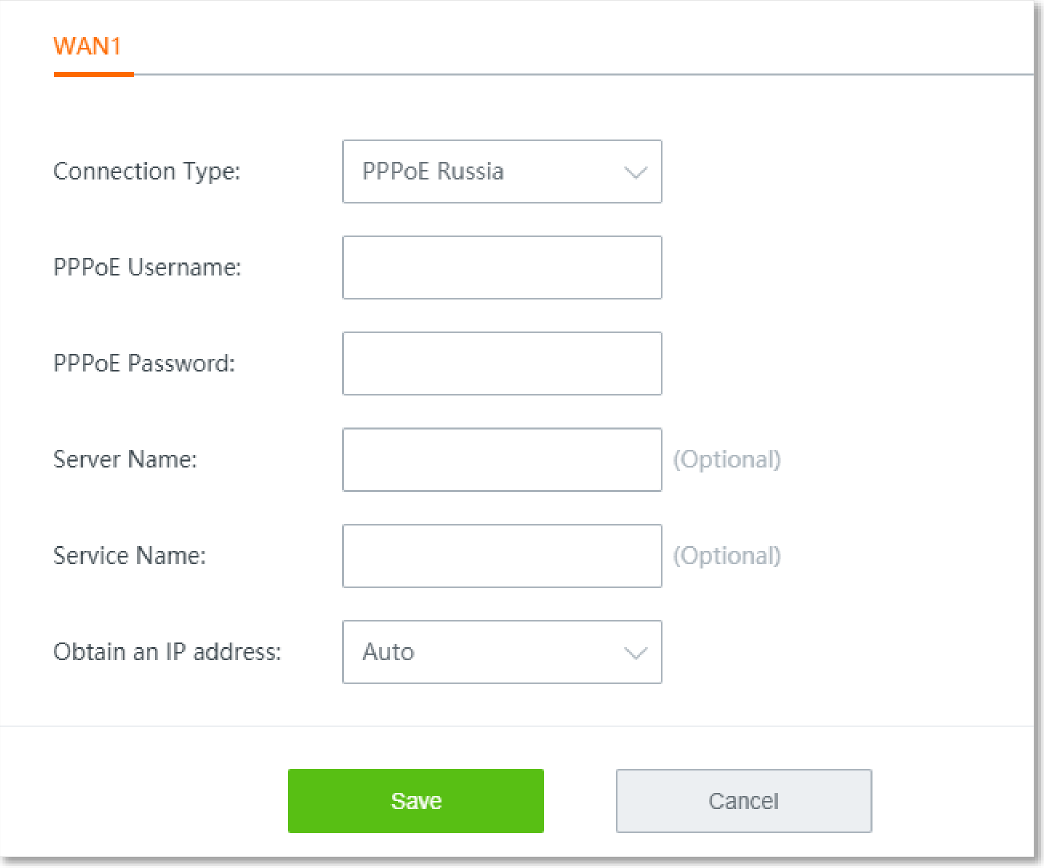
PPPoE Russia

Step 1 Navigate to **Internet Settings** > **Internet Settings**.

Step 2 Set **Connection Type** to **PPPoE Russia**.

Step 3 Enter the **PPPoE Username**, **PPPoE Password** provided by your ISP. If the **Server Name**, **Service Name**, **IP Address** and other related parameters are also provided, enter them in the corresponding input box as well.

Step 4 Click **Save** at the bottom of the page to apply your settings.



WAN1

Connection Type: PPPoE Russia

PPPoE Username:

PPPoE Password:

Server Name: (Optional)

Service Name: (Optional)

Obtain an IP address: Auto

----End

Wait a moment. When the **Status** shows **Authenticated successfully**, the router is connected to the internet successfully

If the username and password you entered are correct but the router fails to connect to the internet, try to modify WAN parameters in **Internet Settings** > WAN Parameters.

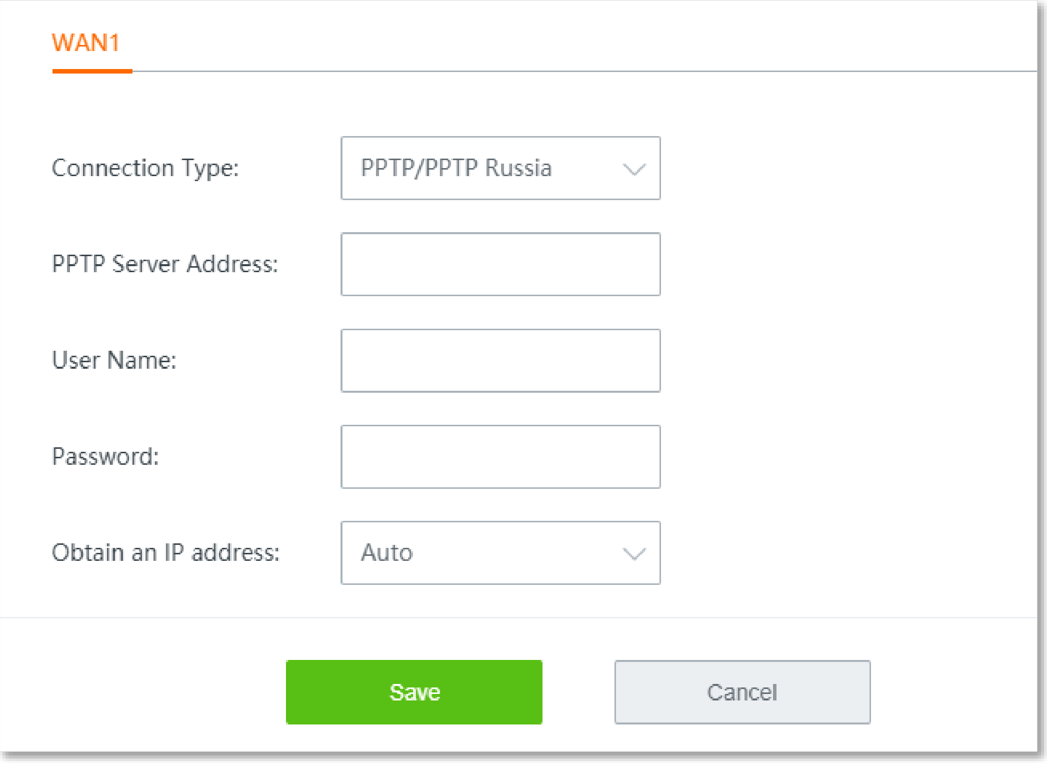
PPTP/PPTP Russia

Step 1 Navigate to **Internet Settings** > **Internet Settings**.

Step 2 Set **Connection Type** to **PPTP/PPTP Russia**.

Step 3 Enter the **PPTP Server Address**, **User Name,** and **Password** provided by your ISP. If the **IP Address** and related parameters are also provided, enter them in the corresponding input box as well.

Step 4 Click **Save** at the bottom of the page to apply your settings.



WAN1

Connection Type: PPTP/PPTP Russia

PPTP Server Address:

User Name:

Password:

Obtain an IP address: Auto

----End

Wait a moment. When the **Status** shows **networked**, the router is connected to the internet successfully.

If the router fails to connect to the internet, try to modify WAN parameters in **Internet Settings** > WAN Parameters.

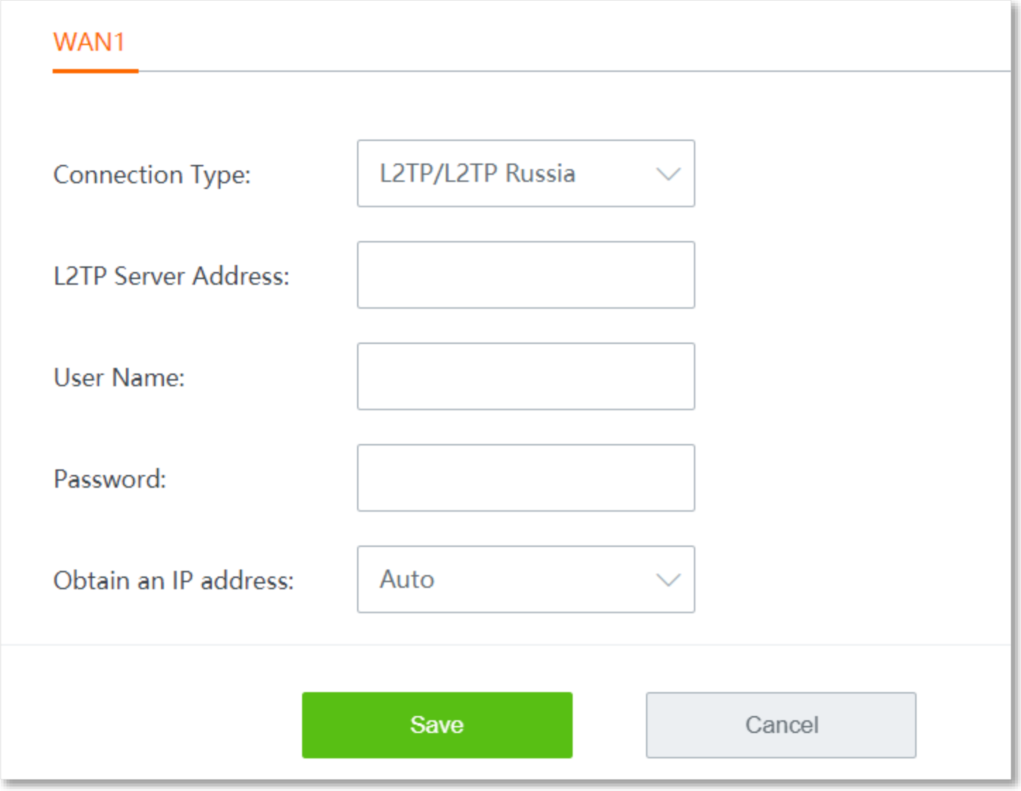
L2TP/L2TP Russia

Step 1 Navigate to **Internet Settings** > **Internet Settings**.

Step 2 Set **Connection Type** to **L2TP/L2TP Russia**.

Step 3 Enter the **L2TP Server Address**, **User Name,** and **Password** provided by your ISP. If the **IP Address** and related parameters are also provided, enter them in the corresponding input box as well.

Step 4 Click **Save** at the bottom of the page to apply your settings.



WAN1

Connection Type: L2TP/L2TP Russia

L2TP Server Address:

User Name:

Password:

Obtain an IP address: Auto

---End

Wait a moment. When the **Status** shows **networked**, the router is connected to the internet successfully.

If the router fails to connect to the internet, try to modify WAN parameters in **Internet Settings** > WAN Parameters.

4.2 WAN parameters

Click **Internet Settings** > **WAN Parameters** to enter the page.

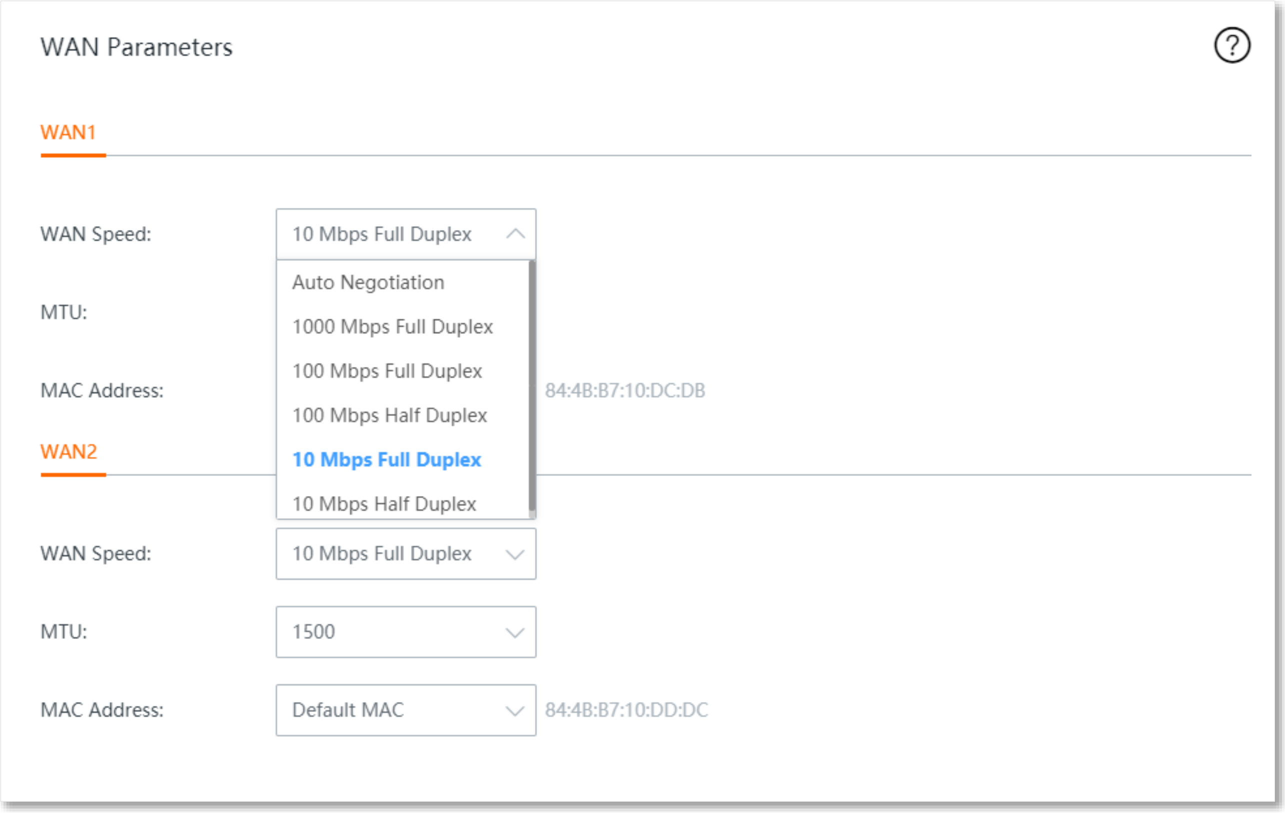
If you have configured Internet Settings but your LAN devices cannot access the internet, try modifying WAN port parameters here.

4.2.1 WAN speed

The speed of an Ethernet physical port is determined through negotiation with its peer device. The negotiated speed can be any speed within the interface capability.

If an Ethernet cable is connected to a WAN port but the WAN port does not light, or the WAN port lights up after a while (5 seconds or above), you can try to change the **WAN Speed** to **10 Mbps Full Duplex** or **10 Mbps Half Duplex** to fix this issue.

In other cases, it is recommended to set the **WAN Speed** to **Auto Negotiation**.



WAN Parameters

WAN1

WAN Speed: 10 Mbps Full Duplex

MTU:

MAC Address: 84:4B:B7:10:DC:DB

WAN2

WAN Speed: 10 Mbps Full Duplex

MTU: 1500

MAC Address: Default MAC 84:4B:B7:10:DD:DC

Duplex modes supported by the router and their scenarios:

Speed and Duplex	Applicable scenario
Auto Negotiation	The duplex mode of the port is determined through auto negotiation between the router and its peer device. You are recommended to keep the default settings since auto negotiation is the default option for most of Ethernet network devices. If the router uses auto negotiation, while its peer uses non-auto negotiation, the negotiated duplex mode is half duplex.

Speed and Duplex	Applicable scenario
10/100/1000 Mbps Full Duplex	The interface can receive and send packets simultaneously, leading to low latency and high efficiency. **10/100/1000 Mbps** indicates the maximum link speed that both ends can negotiate. NOTE You are recommended to use the same speed link and duplex modes for both ends. Otherwise, network connection issues may occur.
10/100 Mbps Half Duplex	The interface can either receive or send packets at a time. **10/100 Mbps** indicates the maximum link speed that both ends can negotiate. NOTE You are recommended to use the same speed link and duplex modes for both ends. Otherwise, network connection issues may occur.

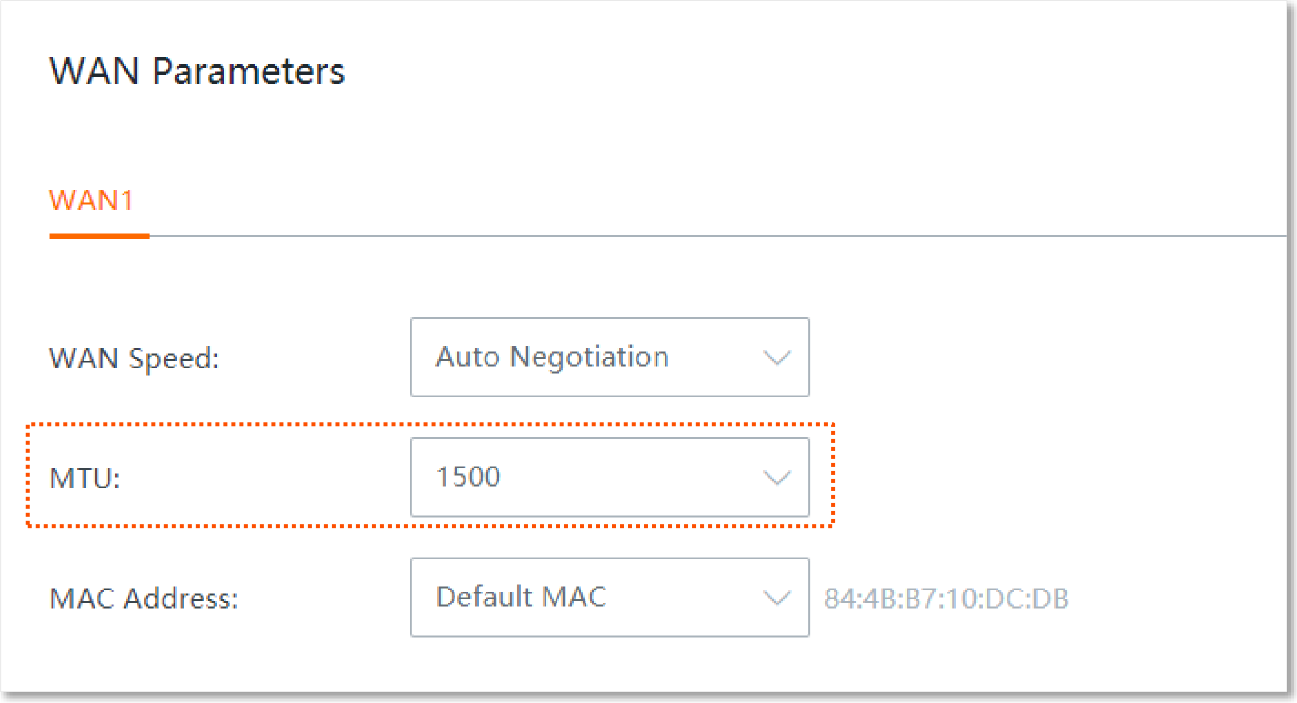
4.2.2 MTU

MTU is abbreviated for Maximum Transmission Unit. It specifies the maximum size of a packet that can be transmitted by a network device. Either larger or smaller MTU value affects the network performance.

Do not modify the default settings unless the following situations happen:

- Some websites are inaccessible, or secure websites cannot be displayed properly, such as online banking websites, or PayPal.
- Email service suspends, or servers, such as FTP/POP servers, are inaccessible.

In such situations, try to reduce the MTU value from the maximum of 1500 to a smaller value (Recommended range: 1400 – 1500) until the problem is solved.



WAN Parameters

WAN1

WAN Speed: Auto Negotiation

MTU: 1500

MAC Address: Default MAC 84:4B:B7:10:DC:DB

Commonly-used MTU value in different scenarios:

MTU (Bytes)	Scenario
1500	It is the most common value for non-PPPoE connections and non-VPN connections.
1492	It is used for PPPoE connections.
1480	It is the maximum value for the ping function. (If a greater value is used, packets are split.)
1450	It is used for DHCP, which assigns dynamic IP addresses to connected devices.
1400	It is used for VPNs or PPTP.

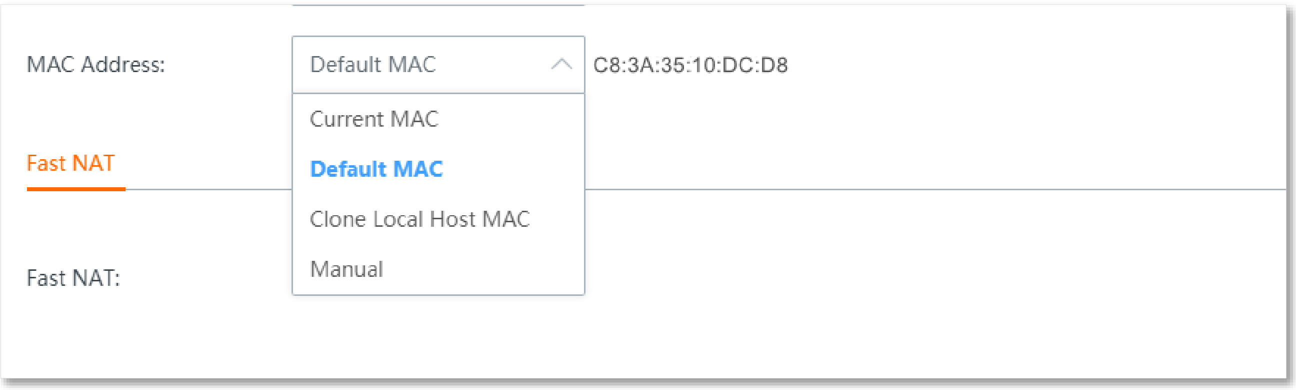
4.2.3 Clone MAC address

Some ISPs allow only a single or a certain number of computers to use the broadband service you subscribed, and register the MAC address of your computer when you first use their cable modem for internet access. Therefore, you may find yourself in the following situations after setting up the router:

- Only one computer can access the internet normally.
- No internet connection at all.

The reason why such a problem happens is that your ISP does not accept MAC addresses other than the registered one. To resolve this, you need to clone the MAC address of the registered computer to the router to pretend that the router has the same MAC address as the registered one.

The cloning MAC address function is designed for this purpose.



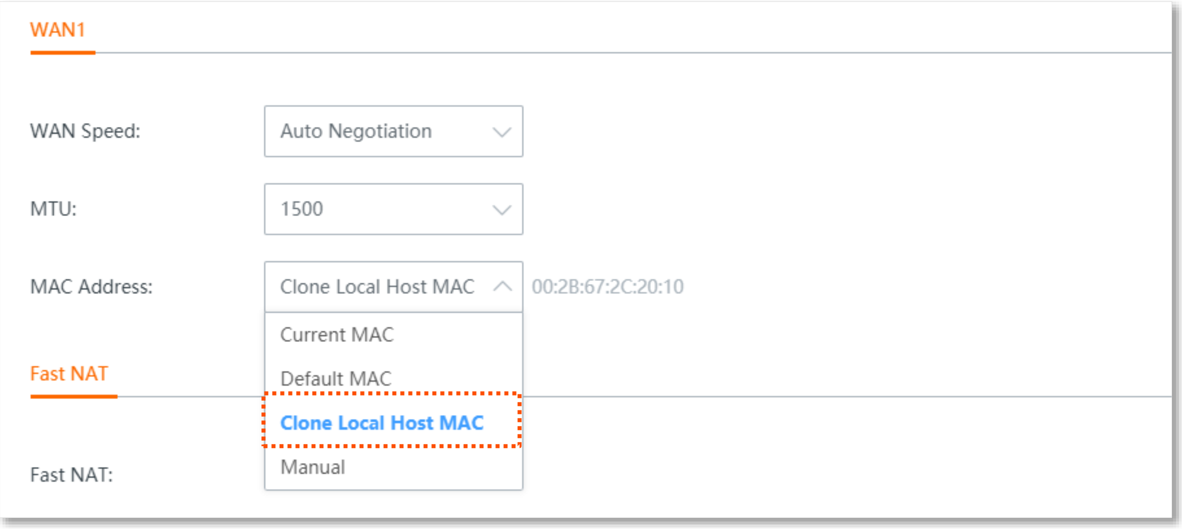
MAC Address: Default MAC C8:3A:35:10:DC:D8

Option A: Clone Local Host MAC

Step 1 Connect a computer already with internet connectivity to the router.

Step 2 Log in to the web UI of the router, navigate to **Internet Settings** > **WAN Parameters**, and set **MAC Address** to **Clone Local Host MAC**.

Step 3 Click **Save** at the bottom of the page to apply your settings.



----End

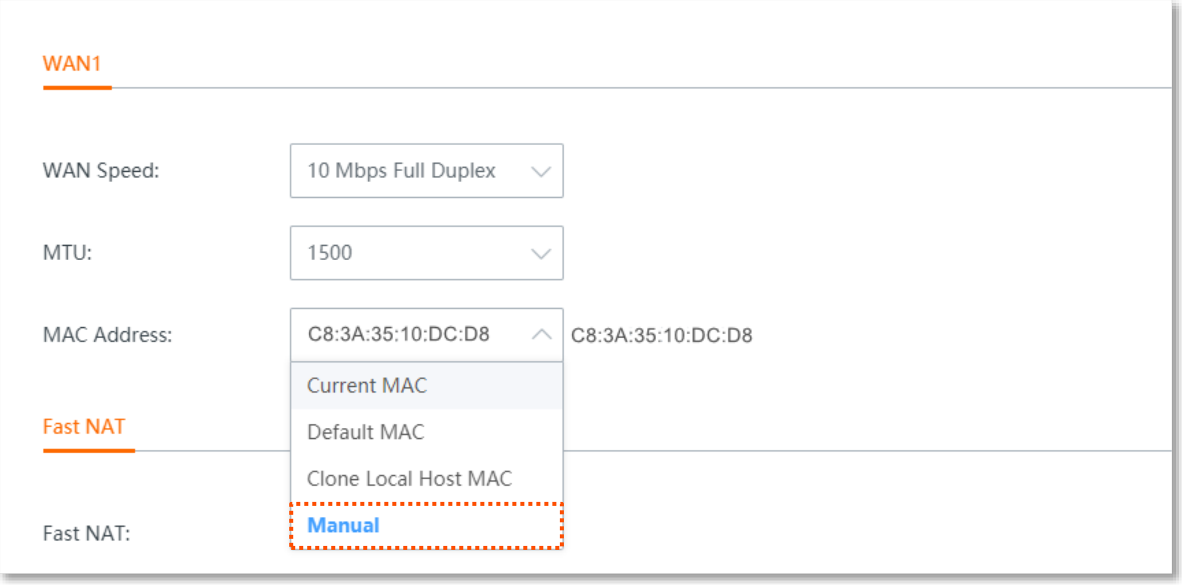
Option B: Manual MAC

Step 1 Record the correct MAC address.

Step 2 Log in to the web UI of the router and navigate to **Internet Settings** > **WAN Parameters**.

Step 3 Set **MAC Address** to **Manual**, then enter the correct MAC address ("the MAC address of the computer which directly connects to the Ethernet jack and has internet connectivity" or "the MAC address of the WAN port of the router on which you set up the internet connection").

Step 4 Click **Save** at the bottom of the page to apply your settings.



----End

TIP

If you want to restore the MAC address of the WAN port to the default MAC address, set **MAC Address** to **Default MAC**, and click **Save**.

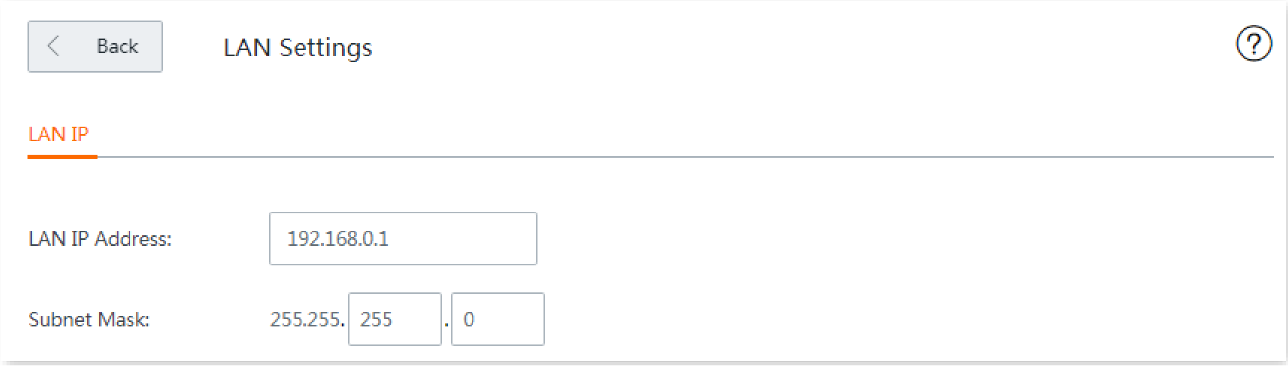
4.3 LAN settings

Click **Internet Settings** > **LAN Settings** to enter the page.

Here, you can view and modify the LAN IP address of the router, and configure the DHCP server.

4.3.1 Modify LAN IP address of the router

The LAN IP address is also the login IP address of the router. The default LAN IP address is **192.168.0.1**.



LAN IP Address: 192.168.0.1

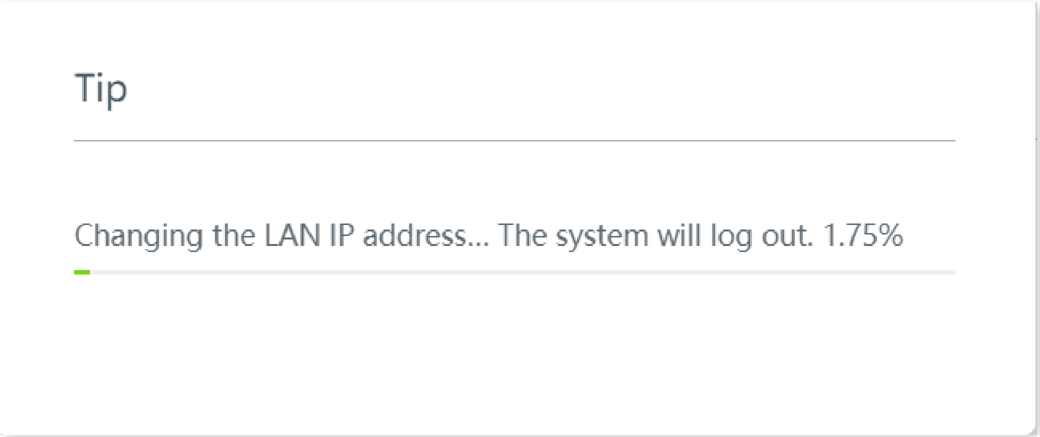
Subnet Mask: 255.255. 255 . 0

TIP

In case of IP address conflict, for example, "The router's WAN IP address and LAN IP address are in the same network segment.", the IP network segment of LAN ports will automatically be incremented by 1 and changed to 192.168.1.1.

Generally, you do not need to modify the LAN IP address of the router. When other management devices in the LAN network need to be set to 192.168.0.*X*, you can modify this router's LAN IP address to a network segment different from 192.168.0.*X*.

After the LAN IP address is changed successfully, you will be redirected to the login page.



Tip

Changing the LAN IP address... The system will log out. 1.75%

TIP

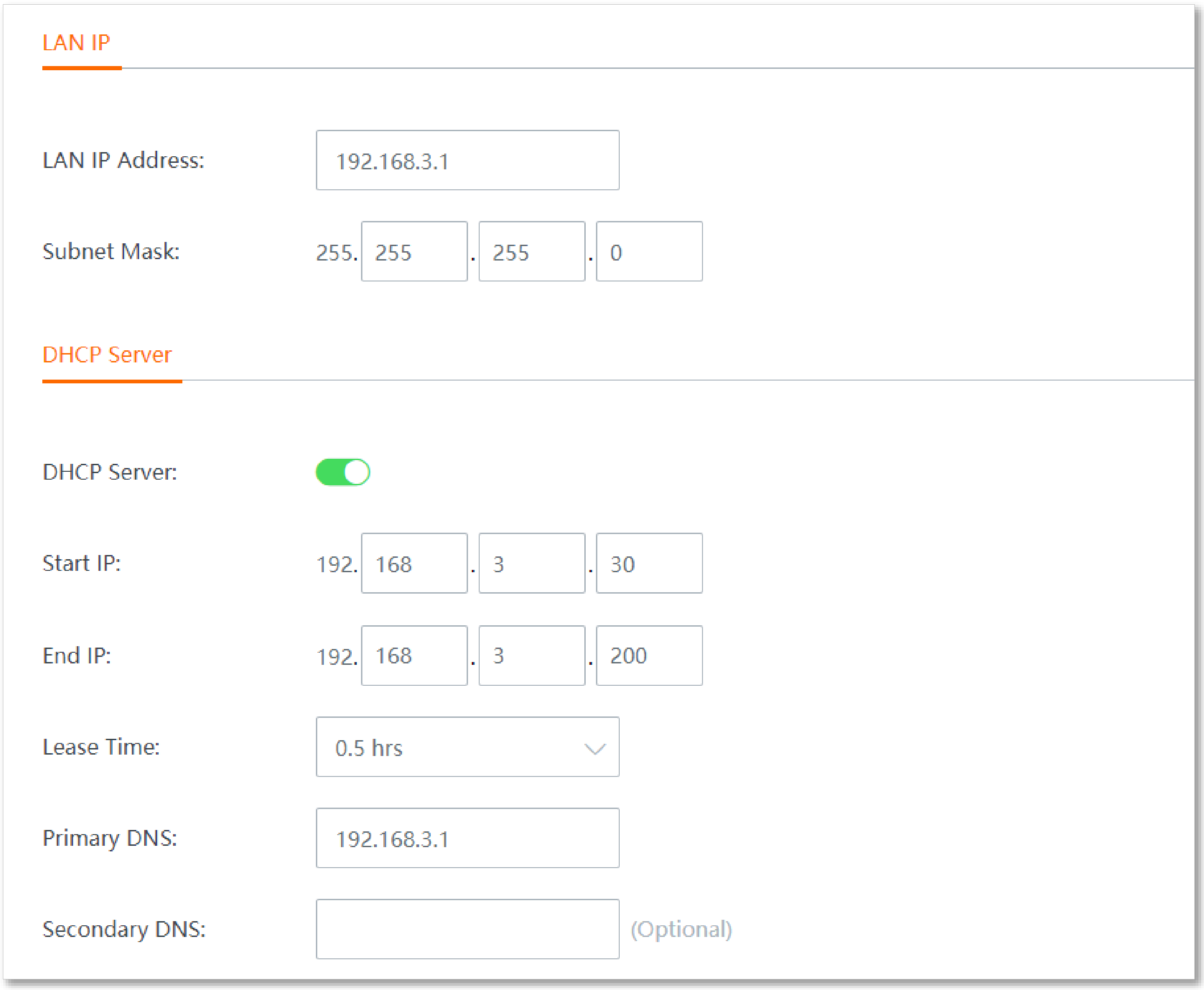
If the network segment of the new LAN IP address is different from the original one, the router modifies the network segment of the DHCP server automatically.

4.3.2 Modify DHCP server

DHCP server can automatically assign IP addresses, subnet mask, gateway and other internet parameters to devices connected to the router. If this function is disabled, you have to manually set IP address settings for your connected devices for internet access. Therefore, you are recommended to keep the DHCP server enabled.

TIP

With this function enabled, IP address-based functions, such as port forwarding and IP address filter may be affected.



LAN IP

LAN IP Address: 192.168.3.1

Subnet Mask: 255. 255 . 255 . 0

DHCP Server

DHCP Server: ●

Start IP: 192. 168 . 3 . 30

End IP: 192. 168 . 3 . 200

Lease Time: 0.5 hrs

Primary DNS: 192.168.3.1

Secondary DNS: (Optional)

Parameter description

Parameter	Description
DHCP Server	Enable or disable the DHCP server function.
Start IP	Specifies the range of IP addresses that the DHCP server can assign. The start IP address is 192.168.0.30 and the end IP address is 192.168.0.200 by default.
End IP	

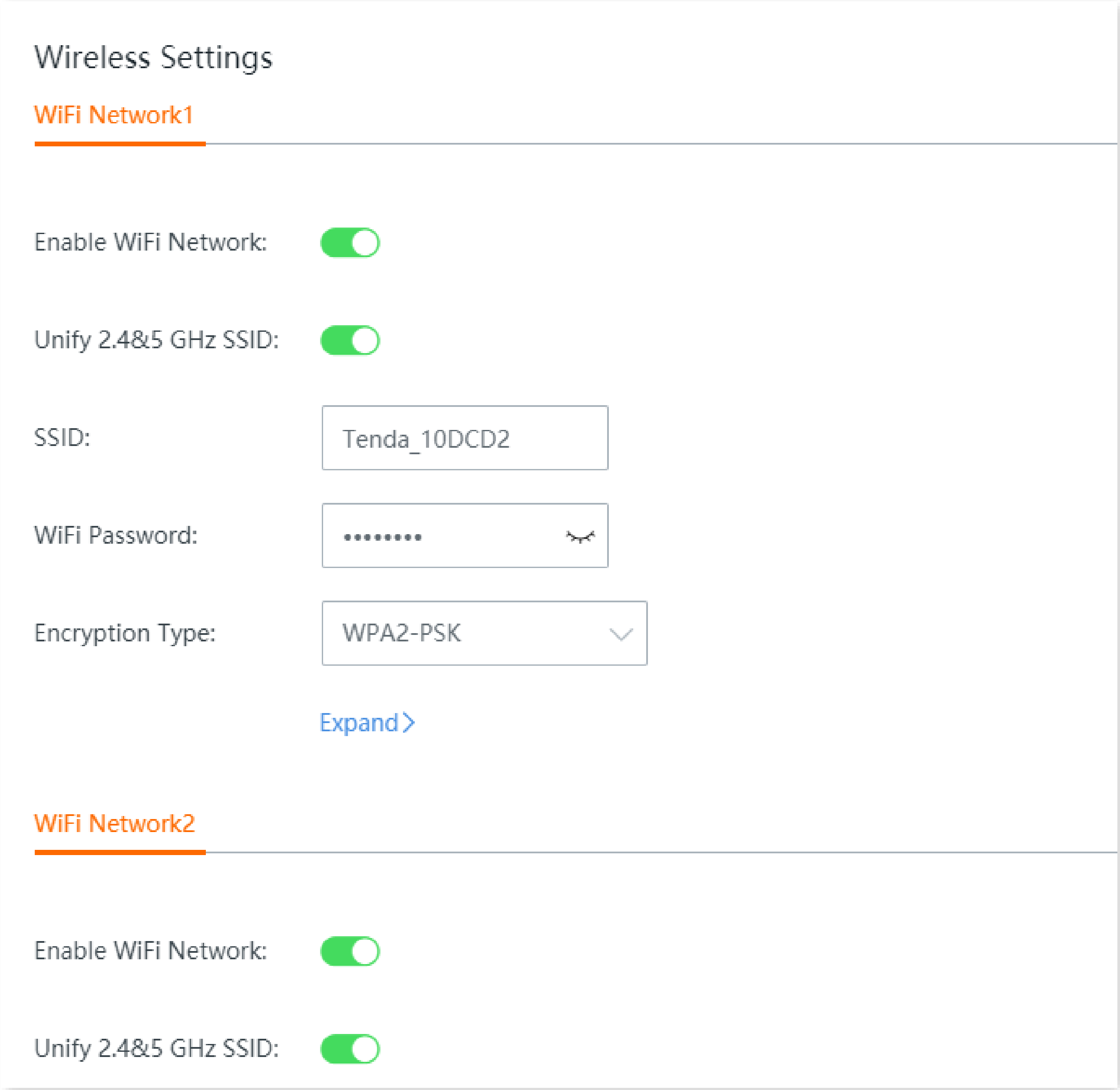
Parameter	Description
Lease Time	Specifies the validity period of the IP address assigned by the DHCP server to LAN devices. By default, the time is 30 minutes. When the IP address expires: ● If the device is still connected to the network, the device will automatically renew and continue to occupy the IP address. ● If the device is not connected to the network, the router will release the IP address. If other devices later request IP address information, the router can assign this IP address to other devices. You are recommended to keep the default settings unless in special circumstances.
Primary DNS	Specifies the primary DNS server IP address assigned by the DHCP server to LAN devices. By default, the primary DNS server address is the LAN IP address of the device. TIP If you enabled the DHCP server, to ensure LAN devices can access the internet properly, make sure that the primary DNS you set is the correct DNS server address or DNS proxy IP address.
Secondary DNS	Specifies the secondary DNS server IP address assigned by the DHCP server to LAN devices. If this parameter is left blank, the DHCP server does not assign the secondary DNS server IP address.

5 Wireless

5.1 Wireless settings

Click **Wireless** > **Wireless Settings** to enter the page.

Here, you are allowed to set up WiFi network-related parameters, such as view and edit wireless network names (SSID), WiFi passwords, configure 2.4 GHz and 5 GHz WiFi networks separately, hide your WiFi network so that nearby wireless clients cannot detect it, and specify how many wireless clients can connect to a wireless network.



Wireless Settings

WiFi Network1

Enable WiFi Network: enabled

Unify 2.4&5 GHz SSID: enabled

SSID: Tenda_10DCD2

WiFi Password: ••••••••

Encryption Type: WPA2-PSK

Expand >

WiFi Network2

Enable WiFi Network: enabled

Unify 2.4&5 GHz SSID: enabled

Parameter description

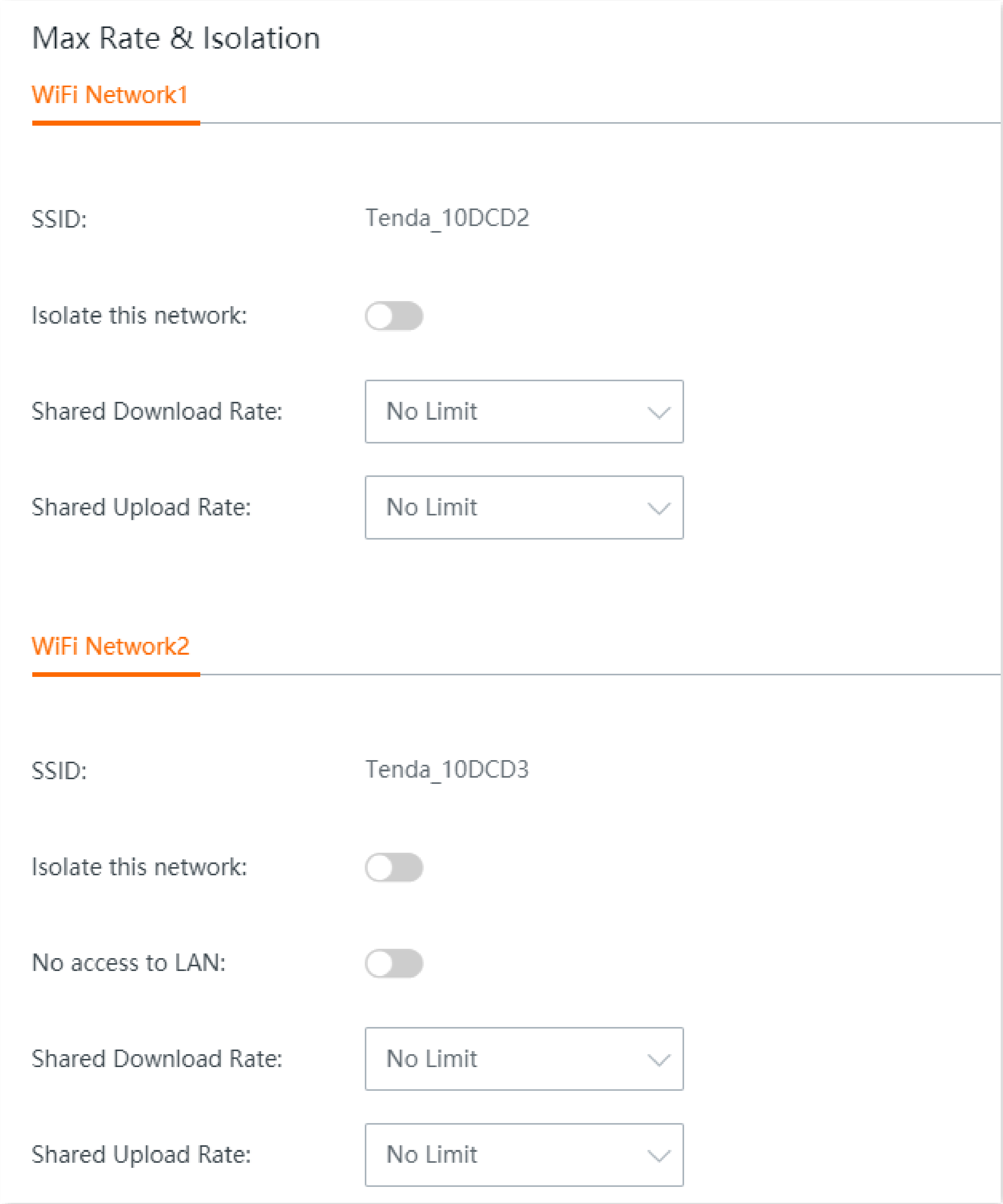
Parameter	Description
Enable WiFi Network	Enable or disable the wireless network of the router.
Unify 2.4&5 GHz SSID	After this function is enabled, the 2.4 GHz guest network and the 5 GHz guest network share the same WiFi network name and password. A wireless client will be automatically connected to the WiFi network with the best network quality when connecting to the guest network.
SSID	Specifies the wireless network name of the corresponding WiFi network.
WiFi Password	Specifies the password used for wireless internet connection. You are recommended to use the combination of digits, letters and special characters for higher security.
Encryption Type	Specifies the encryption types supported by the router. • **None**: Open wireless network. No password is required when a client connects to the wireless network. To secure the network, this option is not recommended. • **WPA-PSK**: The wireless network adopts the WPA-PSK authentication method (AES encryption rule). It is featured with better compatibility than WPA2-PSK. • **WPA2-PSK**: The wireless network adopts the WPA2-PSK authentication method (AES encryption rule). It is featured with higher security level than WPA-PSK. • **WPA-PSK/WPA2-PSK**: The wireless network adopts both WPA-PSK and WPA2-PSK. • **WPA2-PSK/WPA3-SAE**: The wireless network adopts both WPA2-PSK and WPA3-SAE. With Simultaneous Authentication of Equals (SAE) and Protected Management Frames (PMF), WPA3-SAE provides protection against dictionary attacks and information disclosure, saving you the trouble to set a complicated password. Through such mixed encryption mode, the router allows clients that do not support WPA3 to access the wireless network, ensuring both compatibility and security. TIP WPA3-SAE is an upgraded version of WPA2-PSK. If your wireless client does not support WPA3-SAE, or the actual WiFi experience is bad, it is recommended to set the encryption type to WPA2-PSK.
Hide SSID	With this function enabled, nearby wireless clients cannot detect the SSID, and you need to manually enter the SSID on the wireless client to access the wireless network. TIP The function appears when you enable Unify 2.4&5 GHz SSID.
Hide 2.4 GHz SSID	With this function enabled, nearby wireless clients cannot detect the 2.4 GHz SSID, and you need to manually enter the SSID on the wireless client to access the wireless network. TIP The function appears when you disable Unify 2.4&5 GHz SSID.

Parameter	Description
Hide 5 GHz SSID	With this function enabled, nearby wireless clients cannot detect the 5 GHz SSID, and you need to manually enter the SSID on the wireless client to access the wireless network. TIP The function appears when you disable Unify 2.4&5 GHz SSID.
Max. Clients	Maximum number of wireless clients that can be connected to the wireless network with the SSID at the same time. After the value is reached, this wireless network denies new connection requests. Clients connected to all the enabled wireless networks (including guest networks) of the router cannot exceed 128 on 2.4 GHz and 5 GHz bands respectively. If you enable multiple SSIDs, plan your maximum number of clients to each SSID first.

5.2 Max rate & isolation

Click **Wireless** > **Max Rate & Isolation** to enter the page.

Here, you can limit the rate of wireless networks or isolate networks. Isolating a network makes clients connected to it cannot communicate with clients connected to another network.



Max Rate & Isolation

WiFi Network1

SSID: Tenda_10DCD2

Isolate this network:

Shared Download Rate: No Limit

Shared Upload Rate: No Limit

WiFi Network2

SSID: Tenda_10DCD3

Isolate this network:

No access to LAN:

Shared Download Rate: No Limit

Shared Upload Rate: No Limit

Parameter description

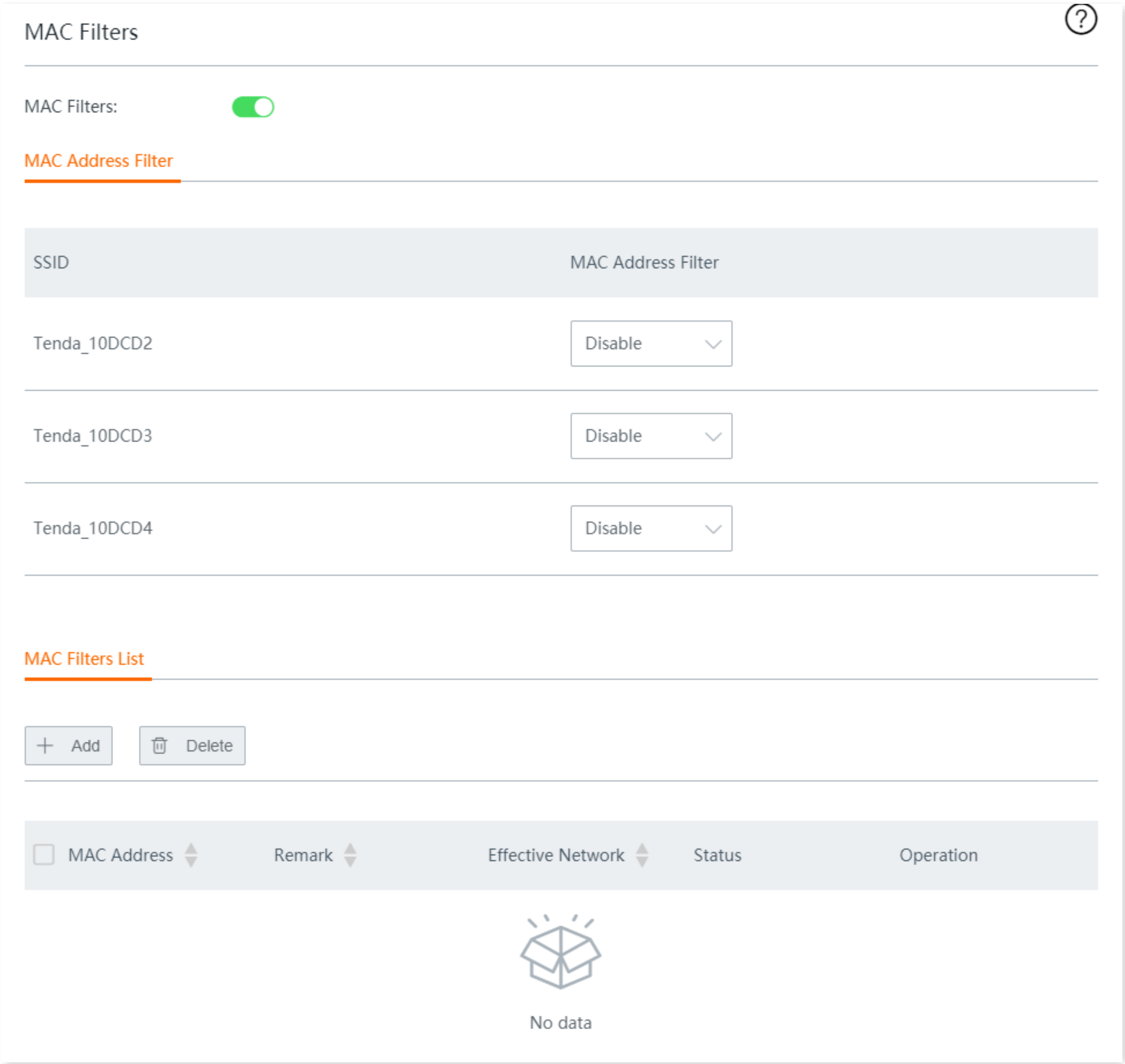
Parameter	Description
SSID	Specifies the wireless network name of the corresponding WiFi network.
Isolate this network	With this function enabled, clients connected to different wireless networks of this device cannot communicate with each other, leading to higher wireless network security. By default, this function is disabled.
Shared Download Rate	Specifies the maximum download and upload rates shared by all clients connected to the wireless network.
Shared Upload Rate	
No access to LAN	This function is only applicable to **WiFi Network2/3**. With this function enabled, clients connected to this wireless network cannot access the web UI and private network (LAN) of this router, protecting your LAN network security. By default, this function is disabled.

5.3 MAC filters

5.3.1 Overview

Click **Wireless** > **MAC Filters** to enter the page.

Here, you can configure MAC address-based wireless access control rules. By default, this function is disabled.



MAC Filters

MAC Filters: ●

MAC Address Filter

SSID	MAC Address Filter
Tenda_10DCD2	Disable
Tenda_10DCD3	Disable
Tenda_10DCD4	Disable

MAC Filters List

□ MAC Address	Remark	Effective Network	Status	Operation

No data

Parameter description

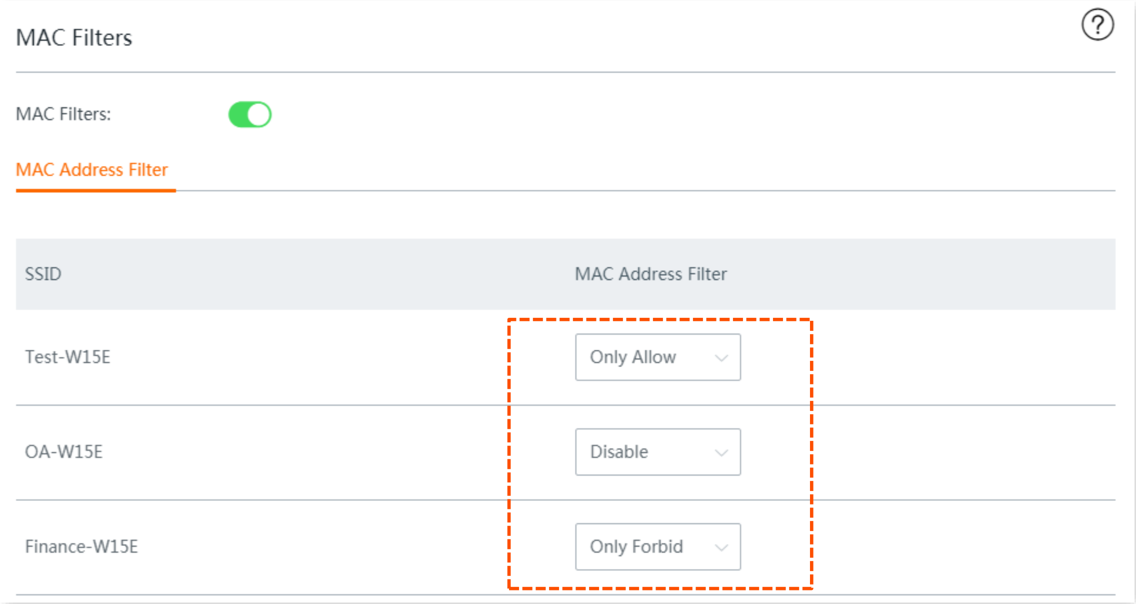
Parameter		Description
MAC Address Filter	SSID	Lists all the main wireless networks that the router supports. TIP If you unify the SSIDs for 2.4 GHz and 5 GHz bands, the corresponding wireless network only displays one SSID here.

Parameter		Description
	MAC Address Filter	Specifies the three kinds of rules you can perform on the corresponding wireless network. - **Disable**: This function is disabled, and all wireless clients can connect to this wireless network. - **Only Allow**: Only wireless clients with the specified MAC address **can** connect to this wireless network. - **Only Forbid**: Only wireless clients with the specified MAC address **cannot** connect to this wireless network.
MAC Filters List	MAC Address	Specifies the MAC address of the client to which the rule applies.
	Remark	(Optional) Specifies the brief description you set for the corresponding MAC address.
	Effective Network	Specifies the wireless network(s) to which the wireless client with this MAC address applies.
	Status	Specifies whether or not the rule is enabled.

5.3.2 Configure a MAC filter rule

Step 1 Enable **MAC Filters**, and click **Save** at the bottom of the page.

Step 2 Configure the MAC address filter mode for each SSID by selecting from the **MAC Address Filter** drop-down list menu.



MAC Filters

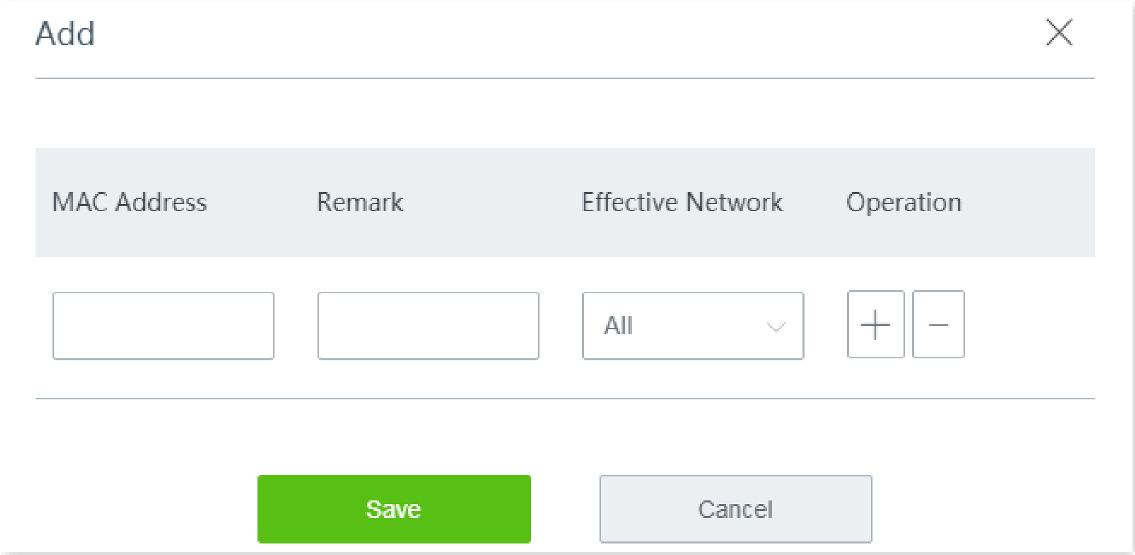
MAC Filters: ●

MAC Address Filter

SSID	MAC Address Filter
Test-W15E	Only Allow
OA-W15E	Disable
Finance-W15E	Only Forbid

Step 3 Add rule(s).

1. Click **Add**.

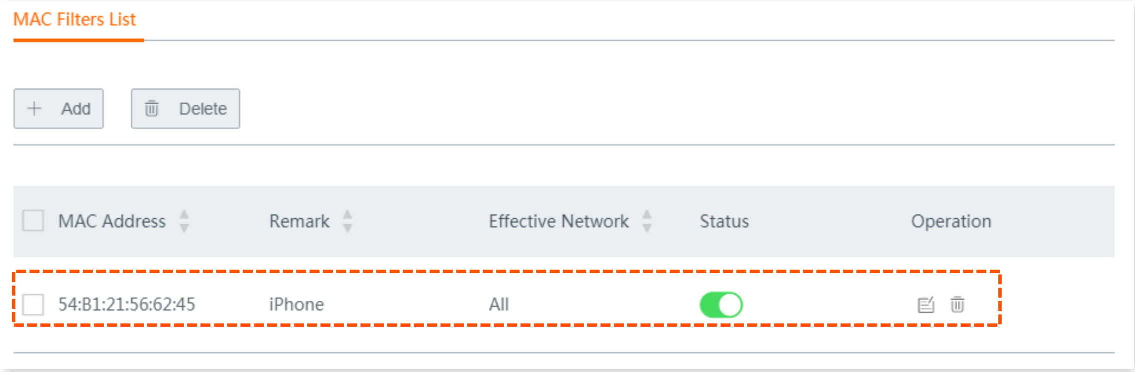


Add

MAC Address	Remark	Effective Network	Operation
		All	+ −

2. Enter the **MAC Address** of a client to which a rule applies to, then enter the **Remark** of the client, and select the wireless network from the drop-down list menu of the **Effective Network**.

3. Click **Save**. The rule appears on the **MAC Filter List**.



MAC Filters List

□	MAC Address	Remark	Effective Network	Status	Operation
□	54:B1:21:56:62:45	iPhone	All	●	

----End

5.3.3 Example of configuring MAC filters rule

Networking requirement

An enterprise uses the wireless router to set up a network.

Requirement: Only a procurement manager's computer is allowed to connect to the WiFi network (Procurement) of the router for internet access. Other staff cannot connect to the network.

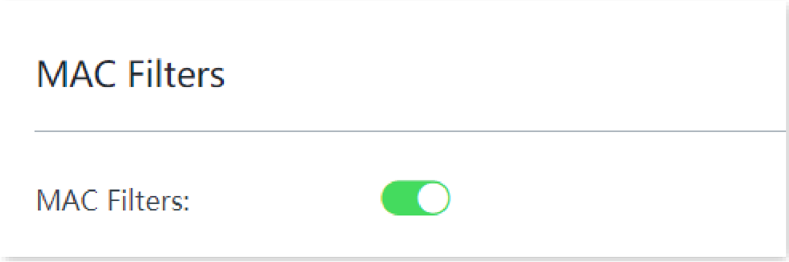
Solution

The MAC filters function can meet this requirement. Assume that the physical address of the computer of the procurement manager is CC:3A:61:71:1B:6E.

Configuration procedure

Step 1 Enable the MAC filters function.

1. Navigate to **Wireless** > **MAC Filters**.
2. Toggle on **MAC Filters**.
3. Click **Save**.

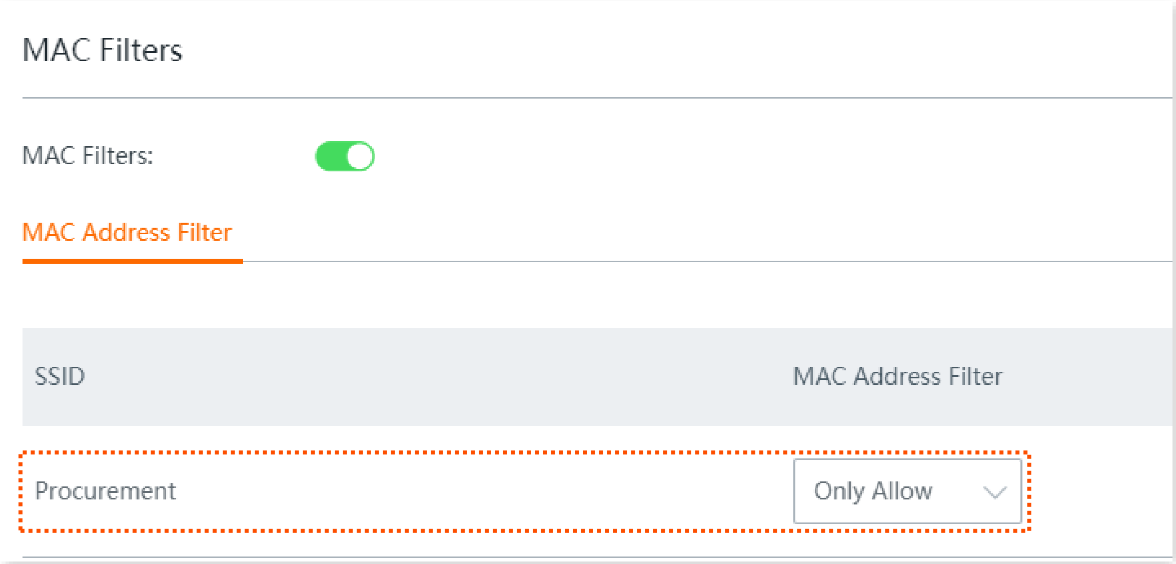


MAC Filters

MAC Filters: ●

Step 2 Set the MAC address filter mode.

1. Select a MAC address filter mode for the WiFi network **Procurement**, which is **Only Allow** in this example.
2. Click **Save** at the bottom of the page.



MAC Filters

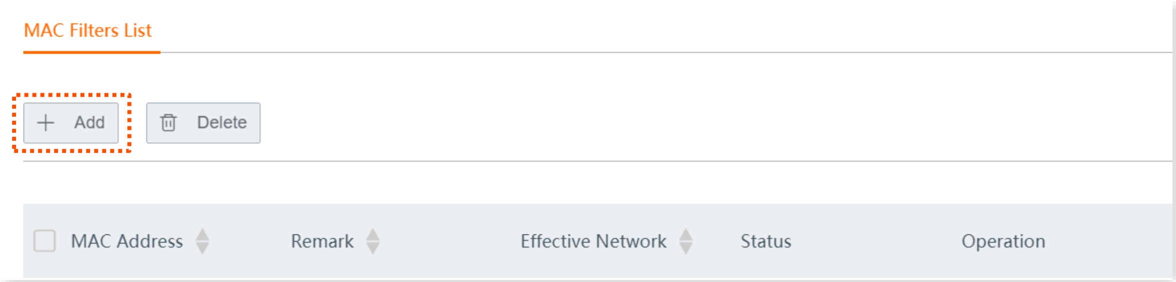
MAC Filters: ●

MAC Address Filter

SSID	MAC Address Filter
Procurement	Only Allow

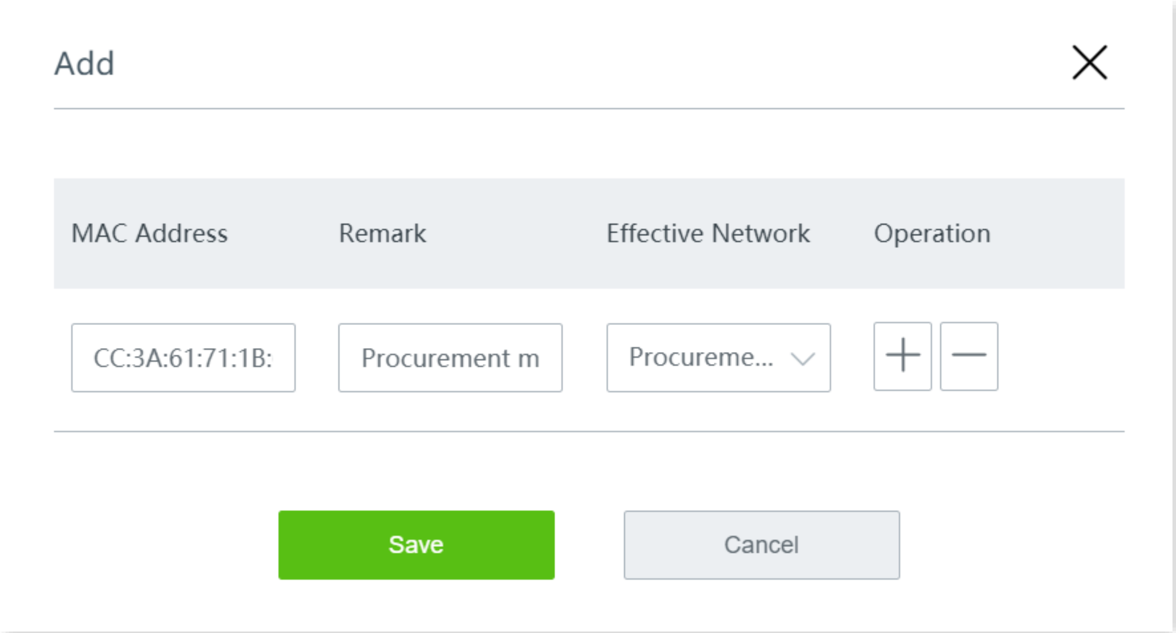
Step 3 Add a MAC filter rule.

1. Click **+Add**.



□ MAC Address	Remark	Effective Network	Status	Operation

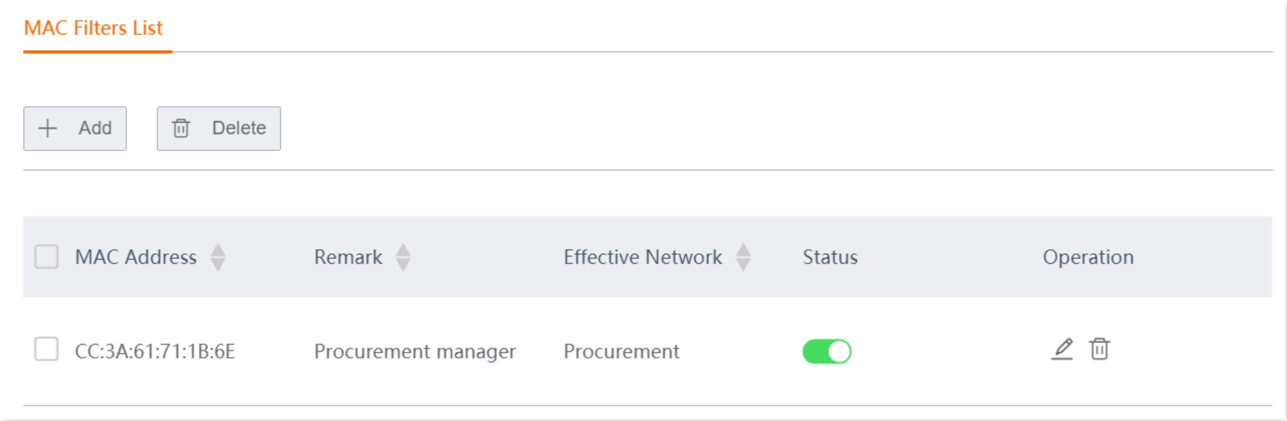
2. On the **Add** configuration window, set the following parameters:
   (1) Set **MAC Address** to **CC:3A:61:71:1B:6E**.
   (2) (Optional) Set **Remark** to **Procurement manager**.
   (3) Select **Procurement** from the drop-down list of **Effective Network**.
   (4) Click **Save**.



MAC Address	Remark	Effective Network	Operation
CC:3A:61:71:1B:	Procurement m	Procureme...	+ —

----End

Added successfully. See the following figure.



□ MAC Address	Remark	Effective Network	Status	Operation
□ CC:3A:61:71:1B:6E	Procurement manager	Procurement	●	

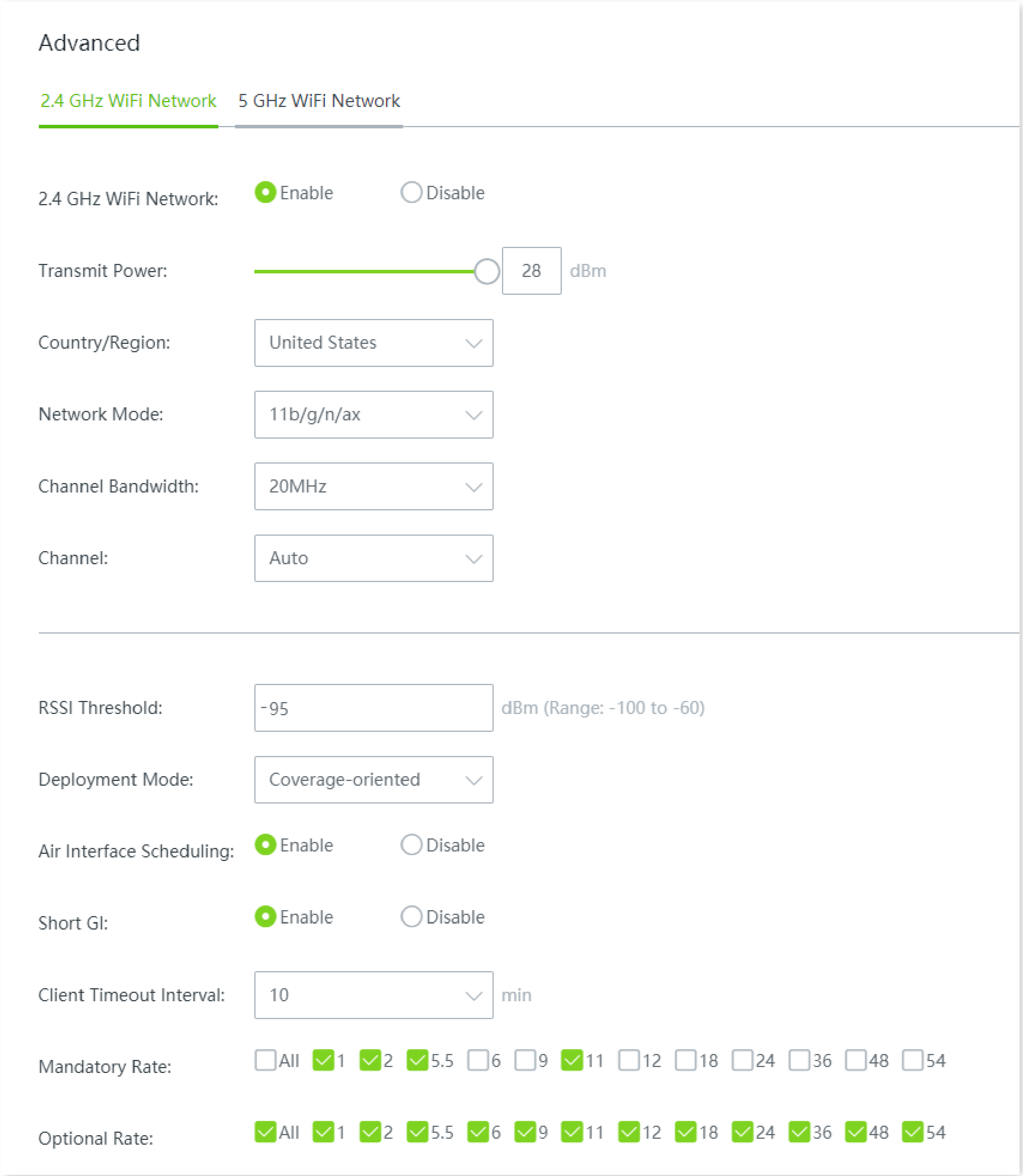
Verification

Only the before-mentioned wireless client can connect to the WiFi network **Procurement** while other clients are blocked.

5.4 Advanced settings

Click **Wireless** > **Advanced** to enter the page.

Here, you can configure the wireless-related advanced settings such as transmit power, network mode, channel and channel bandwidth.



Advanced

2.4 GHz WiFi Network: ● Enable ○ Disable

Transmit Power: 28 dBm

Country/Region: United States

Network Mode: 11b/g/n/ax

Channel Bandwidth: 20MHz

Channel: Auto

RSSI Threshold: -95 dBm (Range: -100 to -60)

Deployment Mode: Coverage-oriented

Air Interface Scheduling: ● Enable ○ Disable

Short GI: ● Enable ○ Disable

Client Timeout Interval: 10 min

Mandatory Rate: ☐ All ☑ 1 ☑ 2 ☑ 5.5 ☐ 6 ☐ 9 ☑ 11 ☐ 12 ☐ 18 ☐ 24 ☐ 36 ☐ 48 ☐ 54

Optional Rate: ☑ All ☑ 1 ☑ 2 ☑ 5.5 ☑ 6 ☑ 9 ☑ 11 ☑ 12 ☑ 18 ☑ 24 ☑ 36 ☑ 48 ☑ 54

Parameter description

Parameter	Description
2.4 GHz WiFi Network	Enable or disable the 2.4 GHz wireless network of the router.
5 GHz WiFi Network	Enable or disable the 5 GHz wireless network of the router.
Transmit Power	Specifies the transmit power of this device. A higher value leads to wider WiFi coverage. However, decreasing the value properly increases performance and security of the wireless network.
Country/Region	Specifies the country/region that you set for the router in order to conform to the regulations of different countries or regions concerning channels.
Network Mode	Specifies the wireless network mode (also called 802.11 mode, radio mode, or wireless mode) of the router. A proper network mode enables the clients to get the maximum transfer rate and compatibility. Available options for **2.4 GHz** band: **11b**, **11g**, **11b/g**, **11b/g/n** and **11b/g/n/ax** (default). Available options for **5 GHz** band: **11a, 11ac, 11a/n mixed, 11a/n/ac, 11a/n/ac/ax** (default)**.** You are recommended to keep the default settings.
Channel	Specifies the channel in which the wireless data is transmitted and received. The available channels are determined by the current country/region and wireless band. **Auto**: The router automatically detects the occupation rate of channels and selects the appropriate working channel accordingly. If connection drop, freeze or slow internet occurs frequently when you are using the WiFi network, you can try changing the working channel. You can check the channels with low occupation rate and little interference using software tools (such as WiFi analyzer).
Channel Bandwidth	Specifies the bandwidth of the working channel. A high channel bandwidth means a higher transmission rate, but the penetration capability is reduced and the transmission distance is shortened. • **20MHz**: The router uses the 20MHz channel bandwidth. • **40MHz**: The router uses the 40MHz channel bandwidth. • **20MHz/40MHz**: This channel bandwidth is available only for the 2.4 GHz. The router automatically adjusts the channel bandwidth to 20MHz or 40MHz based on the surrounding environment. • **80MHz**: This channel bandwidth is available only for the 5 GHz. The router uses the 80MHz channel bandwidth. • **160MHz**: This channel bandwidth is available only for the 5 GHz. The router uses the 160MHz channel bandwidth.
RSSI Threshold	Specifies the minimum wireless client signal strength acceptable to the router. A mobile client with signal strength lower than this threshold cannot connect to the router. You can set this parameter to ensure that mobile clients connect to router with strong signal strength.

Parameter	Description
Deployment Mode	Specifies the deployment mode of the router. This parameter is valid only for 2.4 GHz networks. Set this parameter based on the application scenario. The options include: • **Coverage-oriented**: Applies to scenarios with large area, multiple walls, decentralized users and less than 10 SSIDs in the ambient environment. • **Capacity-oriented**: Applies to scenarios with intensive users, open and large areas, and more than 25 SSIDs in ambient environment.
Prioritize 5 GHz	Specifies that a wireless client uses the 5 GHz SSID first to connect to the device if the wireless client supports both 5 GHz and 2.4 GHz networks and the networks use the same SSID and password.
Prioritize 5 GHz Threshold	When **Prioritize 5 GHz** is enabled, if the client signal strength received by the router in 5 GHz is larger than the threshold value, the router allows the client to connect to the 5 GHz for priority; if it is smaller than the value, the router only allows the client to connect to the 2.4 GHz. The default value is **-80** dBm. You are recommended to keep the default settings.
Air Interface Scheduling	Specifies whether to enable the air interface scheduling function. This function allows all clients to transmit data for the same duration. If a client transmits data at a low speed and does not finish data transmission within the duration, it can continue transmitting data only in its next data transmission duration. This prevents some slow clients from occupying excessive airtime resources, so as to improve the overall AP efficiency and effectively ensure AP connections for a larger number of clients and greater throughputs.
Short GI	Short guard interval for preventing data block interference. Propagation delays may occur on the receiver side due to factors such as multipath wireless signal transmission. If a data block is transmitted at an overly high speed, it may interfere with the previous data block. The short GI helps prevent such interference. Enabling the short GI can yield a 10% improvement in wireless data throughput.
APSD	Specifies whether to enable the Automatic Power Save Delivery (APSD) mode. APSD is a WMM power saving protocol created by Wi-Fi Alliance. Enabling APSD helps reduce power consumption. By default, this mode is disabled.
Client Timeout Interval	Specifies the maximum period before a WiFi client is disconnected from the router if the client exchanges no data with the router. When data is exchanged within the period, countdown stops.
Mandatory Rate	By adjusting the mandatory rate and optional rate, you can limit access from low-speed clients, thus improving the internet experience of other clients. • **Mandatory Rate**: It is a group of mandatory rates of the router. Clients must support these mandatory rates; otherwise, the clients will fail to access the WiFi network. • **Optional Rate**: It is a collection of other rates supported by the router except for mandatory rates. These optional rates help clients realize connection with the router at a higher rate.
Optional Rate	

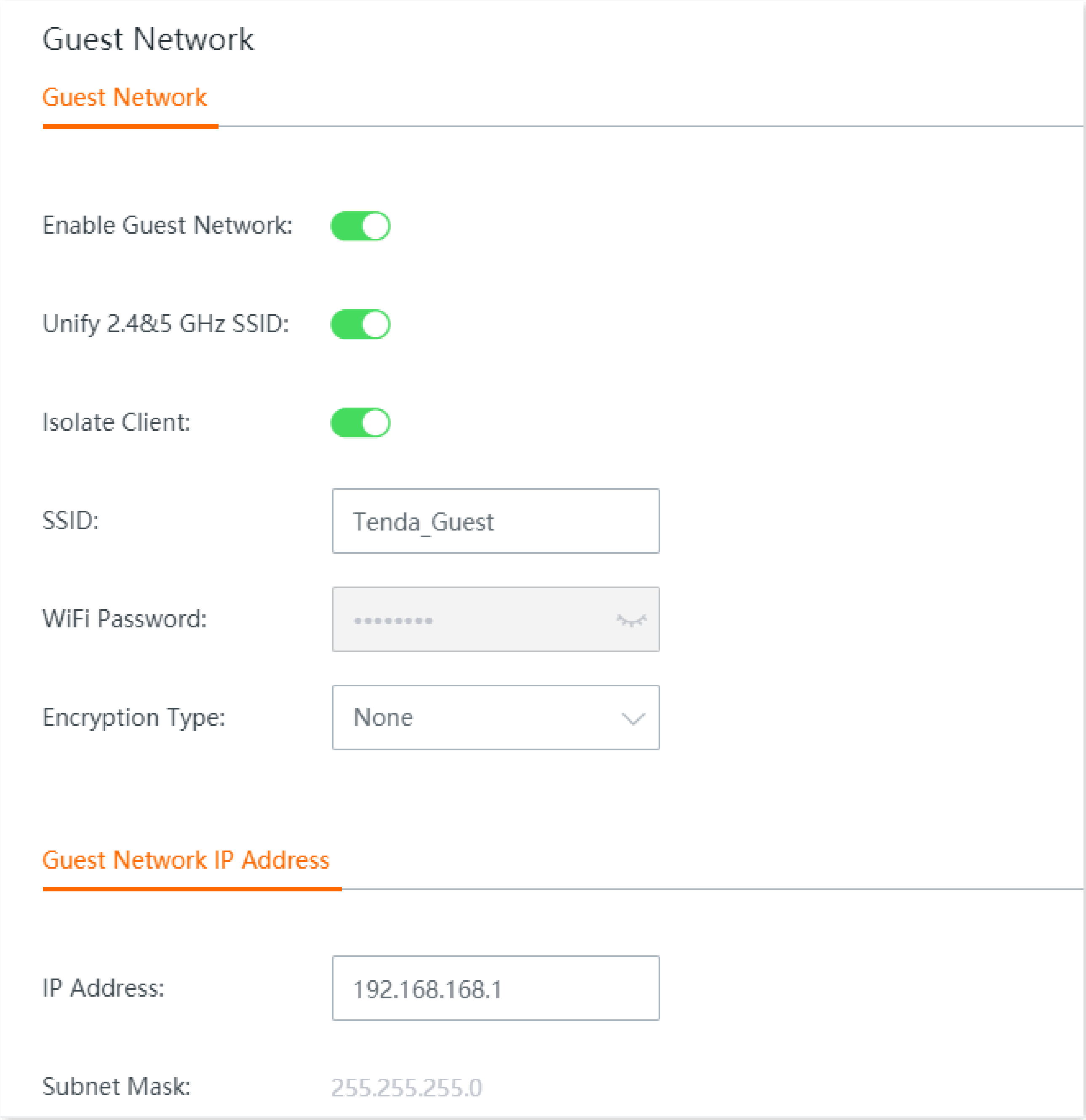
Parameter	Description
MU-MIMO	After the function is enabled, the router can communicate with multiple terminals at the same time, improving network experience.
OFDMA	After the function is enabled, multiple clients can reuse the channel resource, improving the transmission rate and reducing network latency.
TWT	After the function is enabled, the router automatically optimizes the resource allocation among devices, awakens devices by negotiation, reduces disordered competition, increases the sleep time of devices and prolongs the battery life. For some terminals with old drive, incompatibility may occur.
WMM	After the function is enabled, the router can process data packets with priority information. It is recommended to enable this function.

5.5 Guest network

Click **Wireless** > **Guest Network** to enter the page.

Here, you can configure the basic parameters of guest network, such as enable/disable guest network, modify the SSID, and set the WiFi password.

Clients connected to the guest network can only access the internet and other wireless clients connected to the guest network as well, and cannot access the web UI of the router or the LAN where the primary network is deployed. The guest network meets the internet requirement of guests and ensures the security of the primary network as well.



Guest Network

Guest Network

Enable Guest Network: ●

Unify 2.4&5 GHz SSID: ●

Isolate Client: ●

SSID: Tenda_Guest

WiFi Password: •••••••••

Encryption Type: None

Guest Network IP Address

IP Address: 192.168.168.1

Subnet Mask: 255.255.255.0

Parameter description

Parameter		Description
Guest Network	Enable Guest Network	Enable or disable the guest network.
	Unify 2.4&5 GHz SSID	After this function is enabled, the 2.4 GHz guest network and the 5 GHz guest network share the same WiFi network name and password. A wireless client will be automatically connected to the WiFi network with the best network quality when connecting to the guest network.
	Isolate Client	With this function enabled, clients connected to the guest network cannot communicate with each other, leading to higher wireless network security.
	SSID	Specifies the wireless network name of the guest network. TIP To differentiate the main network and the guest network, you are recommended to set the SSIDs differently.
	WiFi Password	Specifies the password used for wireless internet connection. You are recommended to use the combination of digits, letters and special characters for higher security.
	Encryption Type	Specifies the encryption types of the guest network.
Guest Network IP Address	IP Address	Specifies the IP address (default: **192.168.168.1)** of the guest network. The router assigns 192.168.168.*X* to wireless clients connected to it. You are recommended to keep the default settings.
	Subnet Mask	Specifies the subnet mask of the guest network, which is used to define the address space of the guest network.
Guest Network Bandwidth Limit	Uplink Bandwidth	Specify the uplink and downlink rate limits on guest network.
	Downlink Bandwidth	
	Client Limit	Specifies the maximum number of wireless devices allowed to connect to the guest network.

6 Address reservation

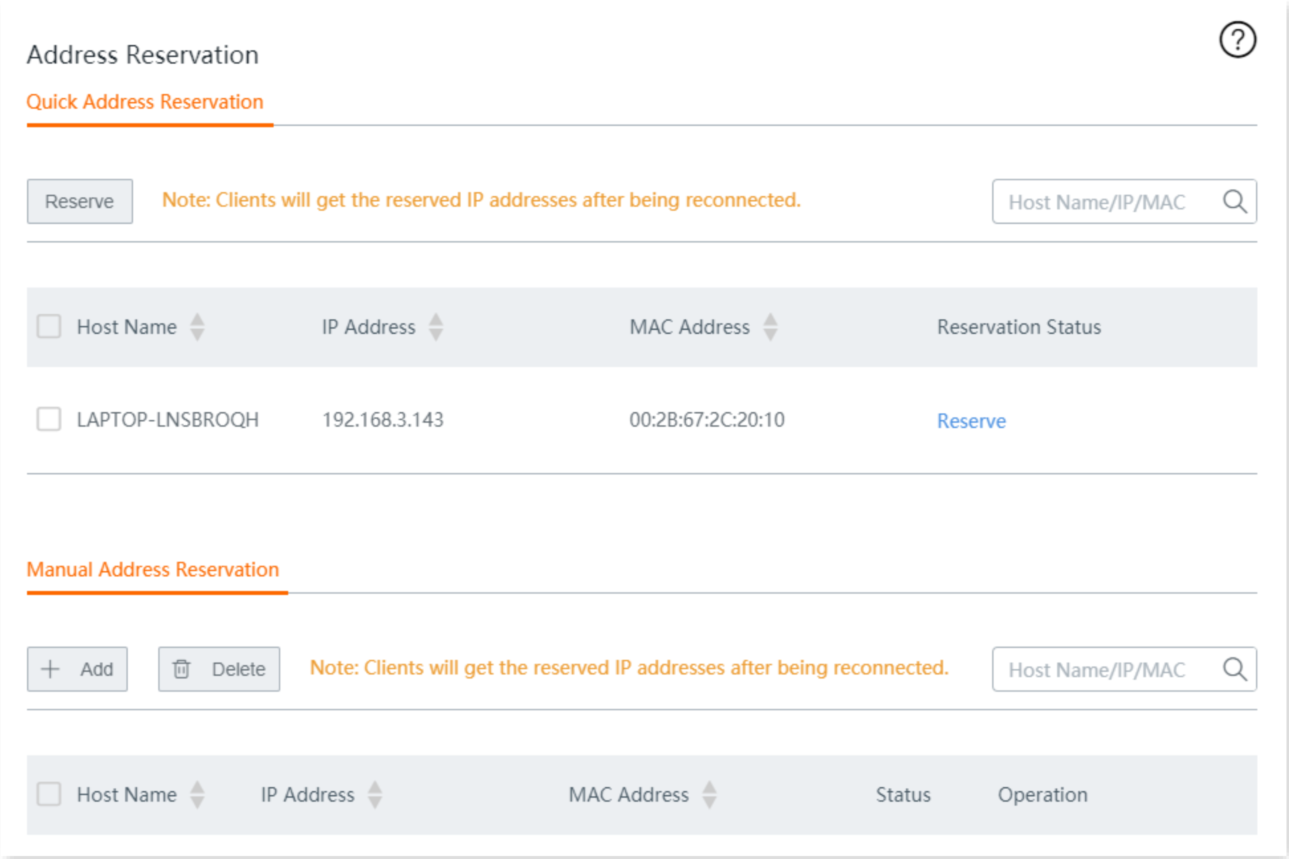
6.1 Address reservation

Click **Address Reservation** to enter the page.

Here, you can specify a pre-set IP address for the specified client and make the client obtain this IP address all the time. In this way, such functions depending on IP address as filter management, bandwidth control, and port forwarding will not be ineffective because of IP address change.

This function takes effect only when the DHCP server function of the router is enabled. The router supports the following two address reservation methods:

- **Quick Address Reservation**: You can check the information of the clients obtaining IP addresses from the DHCP server of the router, and reserve IP addresses for clients by just clicking **Reserve**. In this way, the DHCP server will assign the fixed IP address for the fixed client all the time.
- **Manual Address Reservation**: You can manually reserve address for client to let the DHCP server assign fixed IP address for fixed client all the time.



Address Reservation

Quick Address Reservation

Reserve Note: Clients will get the reserved IP addresses after being reconnected. Host Name/IP/MAC

□ Host Name	IP Address	MAC Address	Reservation Status
□ LAPTOP-LNSBROQH	192.168.3.143	00:2B:67:2C:20:10	Reserve

Manual Address Reservation

+ Add Delete Note: Clients will get the reserved IP addresses after being reconnected. Host Name/IP/MAC

□ Host Name	IP Address	MAC Address	Status	Operation

Parameter description

Parameter		Description
Quick Address Reservation	Reserve	Used to bind the IP address and MAC address of the selected client.
	Host Name	Specifies the name of the client.
	IP Address	Specifies the IP address of the client.
	MAC Address	Specifies the MAC address of the client.
	Reservation Status	Click **Reserve** to bind the IP address and MAC address together, so the client will obtain the reserved IP address all the time. If the reservation is successful, the reservation status will be displayed as **Reserved**.
Manual Address Reservation	Host Name	Specifies the name of the client or remarks of static IP address reservation rule.
	IP Address	Specifies the IP address reserved for the client with the target MAC address.
	MAC Address	Specifies the MAC address of the client.
	Status	Specifies the status of the rule. You can enable or disable the rule as required.
	Action	Specifies the operations you can perform on the rule. ✎: Click it to edit the rule. 🗑 : Click it to delete the rule.
Export Configuration		Click **Export** to back up the static IP reservation table to the local computer.
Import Configuration		Select a file and click **Import** to import the backed up static IP reservation table to the router.

6.2 Configure address reservation

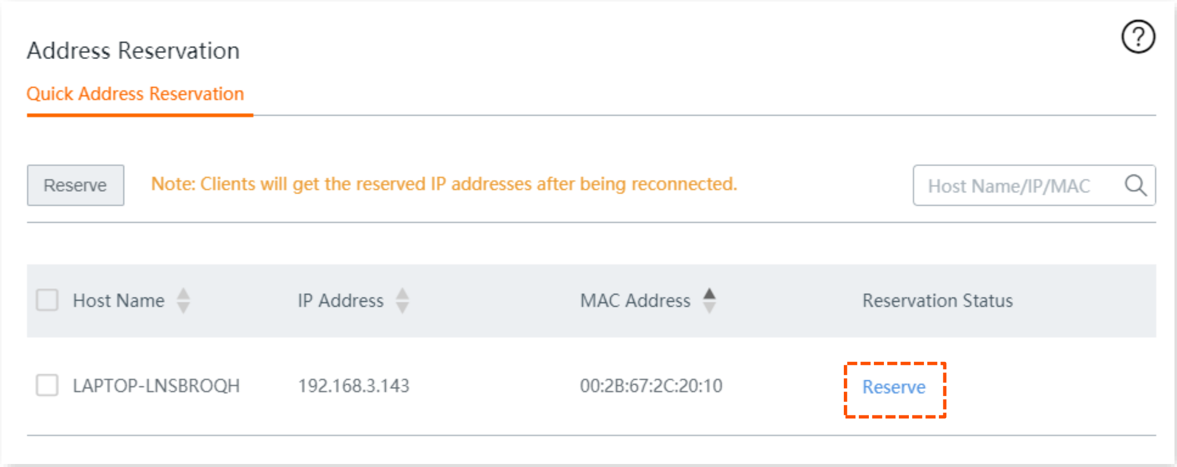
If you want to assign IP address for clients already connected to the network, it is recommended that you configure in the **Quick Address Reservation** module. Otherwise, configure in the **Manual Address Reservation** module.

6.2.1 Quick address reservation

Reserve IP address for one client

Step 1 Navigate to **Address Reservation** > **Quick Address Reservation**.

Step 2 Select the client you want to reserve a static IP address, and click **Reserve**.

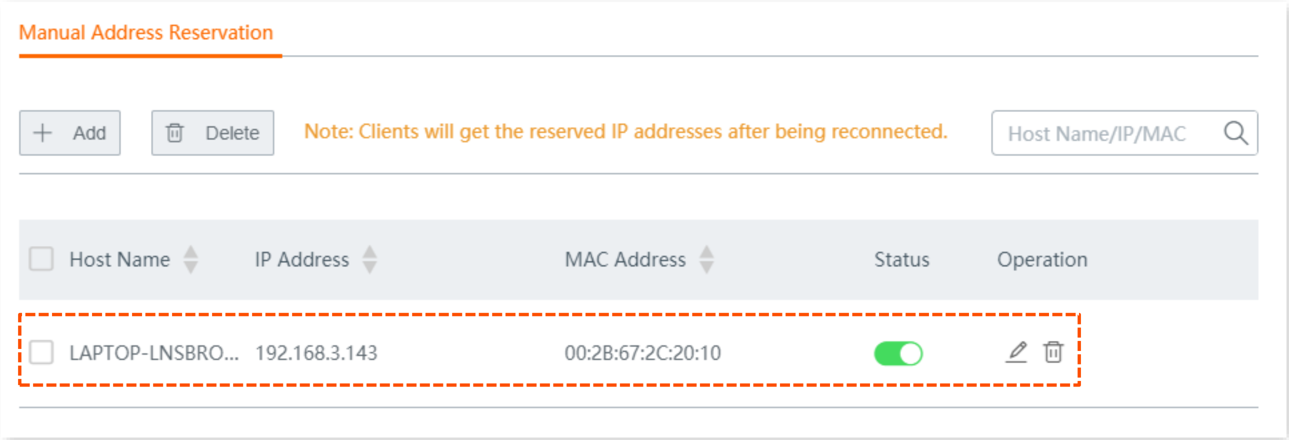


Note: Clients will get the reserved IP addresses after being reconnected.

□ Host Name	IP Address	MAC Address	Reservation Status
□ LAPTOP-LNSBROQH	192.168.3.143	00:2B:67:2C:20:10	Reserve

----End

After the IP address is reserved successfully, you can check the added rule in the **Address Reservation** > **Manual Address Reservation** module. The rule will take effect the next time when the client requests for an IP address.



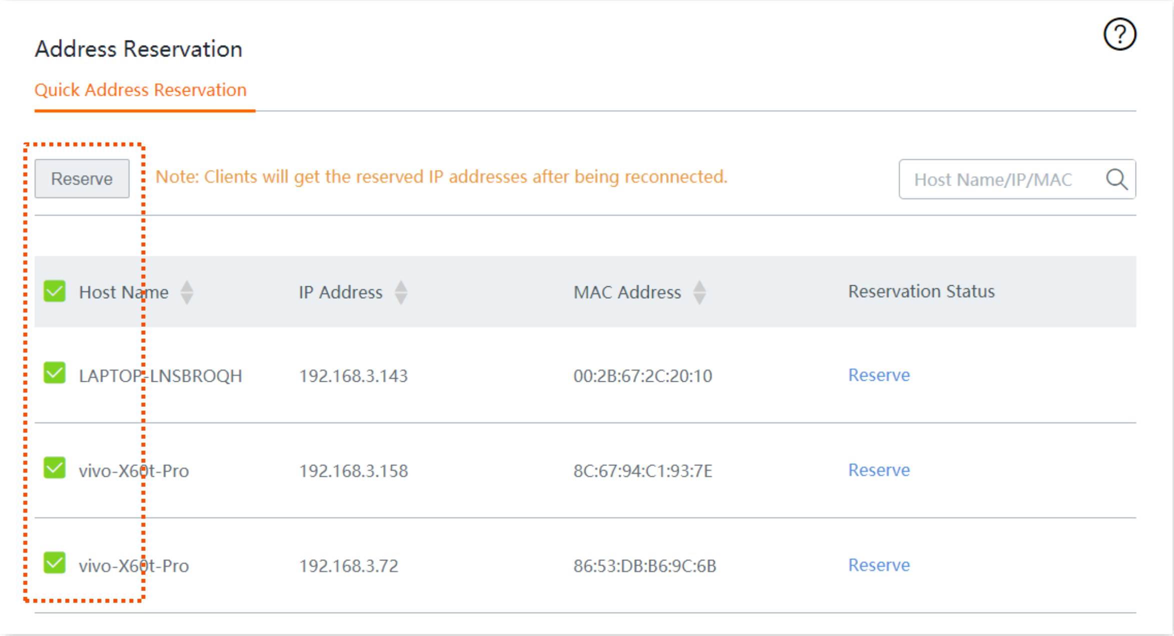
Note: Clients will get the reserved IP addresses after being reconnected.

□ Host Name	IP Address	MAC Address	Status	Operation
□ LAPTOP-LNSBRO...	192.168.3.143	00:2B:67:2C:20:10	●	✎ 🗑

Reserve IP addresses for multiple clients

Step 1 Navigate to **Address Reservation** > **Quick Address Reservation**.

Step 2 Select the multiple clients you want to reserve static IP addresses, and click the upper **Reserve**.



Address Reservation

Quick Address Reservation

Reserve

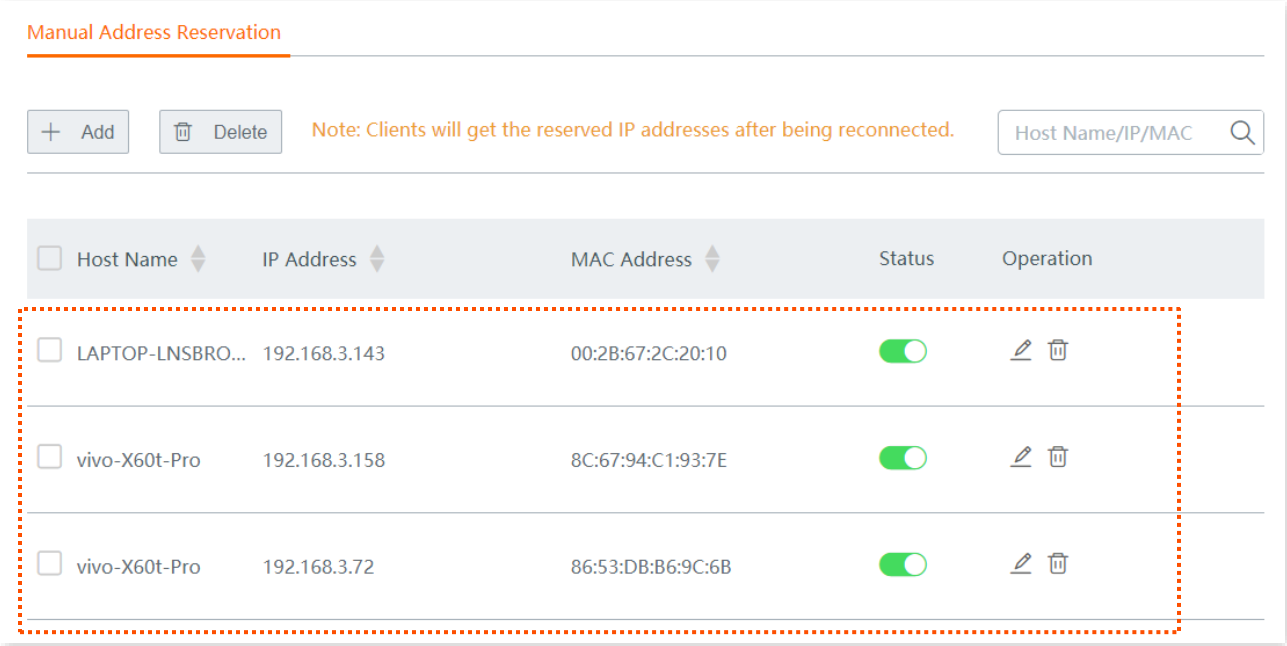
Note: Clients will get the reserved IP addresses after being reconnected.

Host Name/IP/MAC

☑ Host Name	IP Address	MAC Address	Reservation Status
☑ LAPTOP-LNSBROQH	192.168.3.143	00:2B:67:2C:20:10	Reserve
☑ vivo-X60t-Pro	192.168.3.158	8C:67:94:C1:93:7E	Reserve
☑ vivo-X60t-Pro	192.168.3.72	86:53:DB:B6:9C:6B	Reserve

----End

After the IP addresses are reserved successfully, you can check the added rules in the **Address Reservation** > **Manual Address Reservation** module. The rules will take effect the next time when the client requests for an IP address.



Manual Address Reservation

+ Add | Delete

Note: Clients will get the reserved IP addresses after being reconnected.

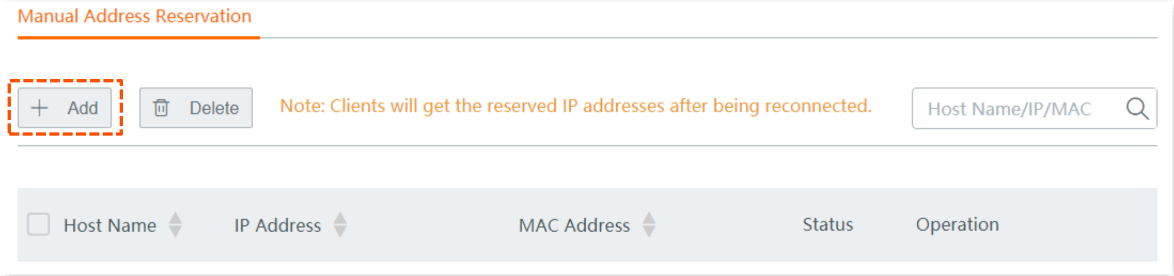
Host Name/IP/MAC

□ Host Name	IP Address	MAC Address	Status	Operation
□ LAPTOP-LNSBRO...	192.168.3.143	00:2B:67:2C:20:10	●	✎ 🗑
□ vivo-X60t-Pro	192.168.3.158	8C:67:94:C1:93:7E	●	✎ 🗑
□ vivo-X60t-Pro	192.168.3.72	86:53:DB:B6:9C:6B	●	✎ 🗑

6.2.2 Manual address reservation

Step 1 Navigate to **Address Reservation** > **Manual Address Reservation**.

Step 2 Click **+Add**.



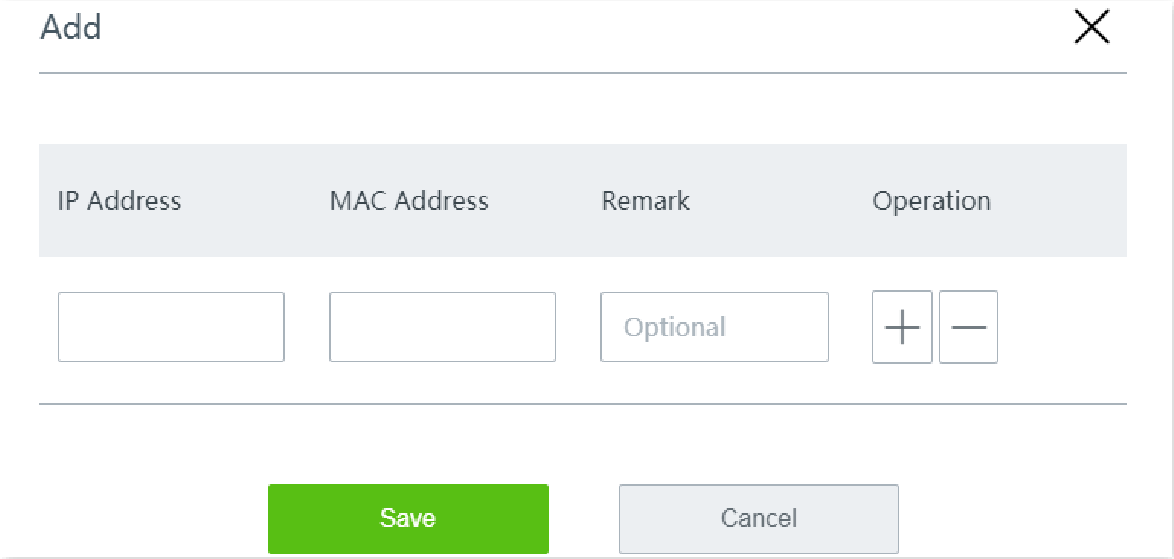
Note: Clients will get the reserved IP addresses after being reconnected.

□ Host Name	IP Address	MAC Address	Status	Operation

Step 3 Enter the **IP Address**, **MAC Address** and **Remark** (Optional), and click **Save**.

TIP

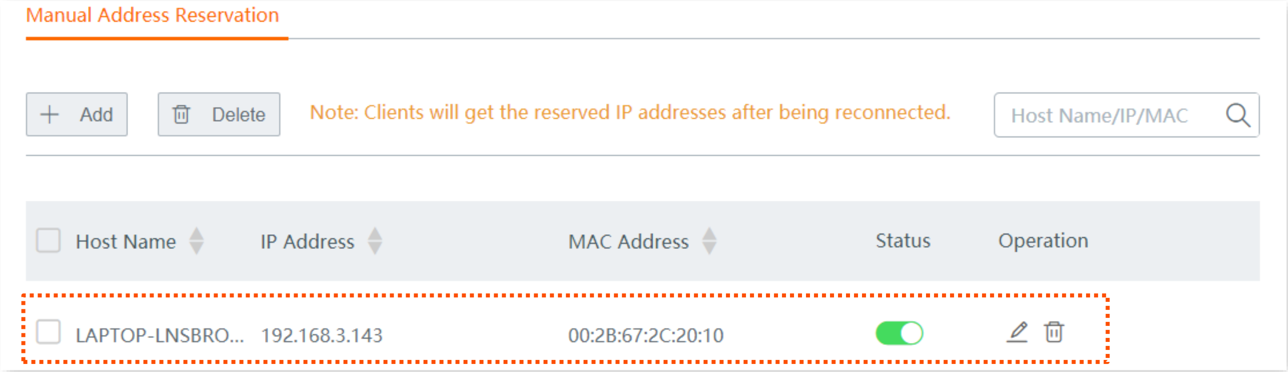
Click + to add a rule and click - to delete an unsaved rule.



IP Address	MAC Address	Remark	Operation
		Optional	+ —

----End

After the IP address is reserved successfully, you can check the added rule in the **Address Reservation** > **Manual Address Reservation** module. The rule will take effect the next time when the client requests for an IP address.



Note: Clients will get the reserved IP addresses after being reconnected.

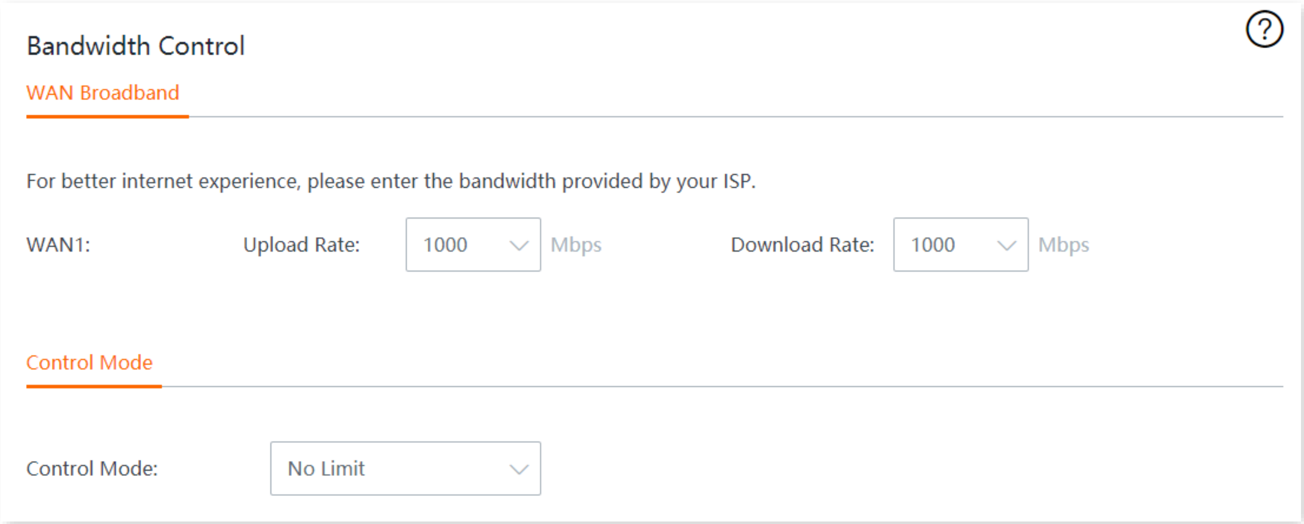
□ Host Name	IP Address	MAC Address	Status	Operation
□ LAPTOP-LNSBRO...	192.168.3.143	00:2B:67:2C:20:10	●	✎ 🗑

7 Bandwidth control

7.1 Overview

Click **Bandwidth Control** to enter the page.

Here, the network administrator can control the rate of users, so the limited bandwidth can be properly distributed.



Bandwidth Control

WAN Broadband

For better internet experience, please enter the bandwidth provided by your ISP.

WAN1: Upload Rate: 1000 Mbps Download Rate: 1000 Mbps

Control Mode

Control Mode: No Limit

Parameter description

Parameter		Description
WAN Broadband	Upload Rate	Enter the bandwidth provided by your ISP for better internet experience.
	Download Rate	
Control Mode	No Limit	No limitations are set on the upload/download rate of LAN users.
	Manual	The network administrator, based on the actual conditions, sets the maximum upload/download rate for each connected client, or set an upload/download rate for all the connected clients. The manual control mode is more flexible compared with the limit by group control mode.
	Auto	The system, based on the WAN upload/download rate set on the **Bandwidth Control** page, evenly distributes bandwidth to LAN users.
	Limit By Group	The network administrator, based on the actual conditions, sets rate limit rules for different groups. The network administrator controls the dedicated or shared upload/download rate for users in the specified IP group in the specified time group, and also, sets the concurrent sessions for each client.

7.2 Manual

Assume that you want to separately set the maximum upload/download rates for connected clients.

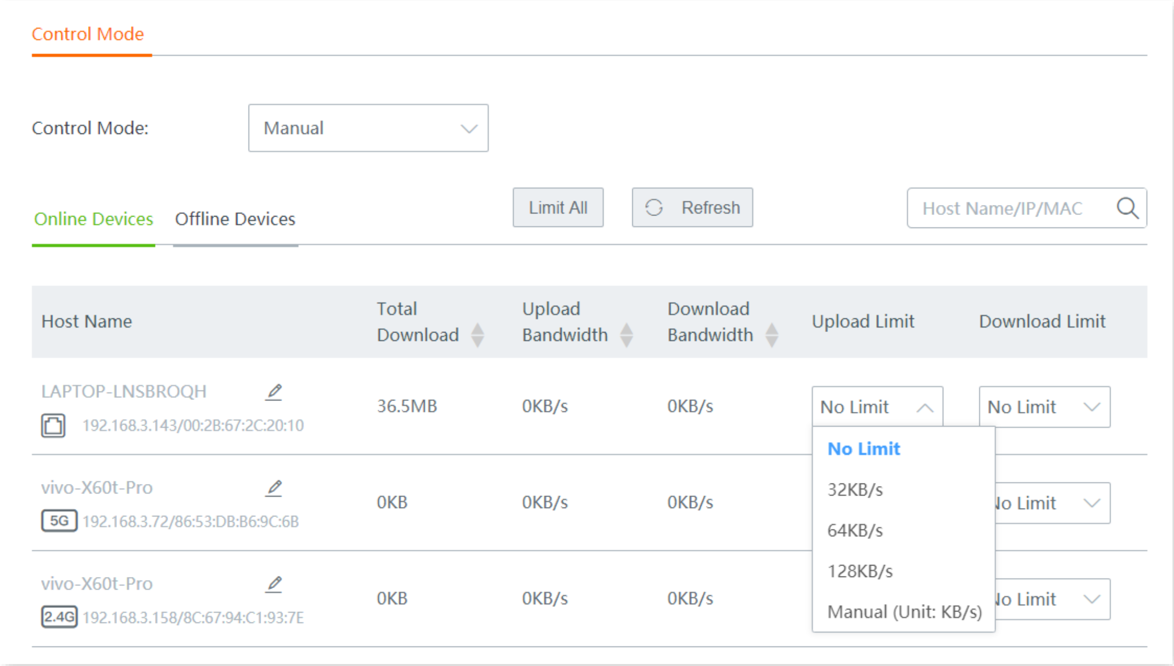
Configuration procedure

Step 1 Click **Bandwidth Control**.

Step 2 Set **Control Mode** to **Manual**.

Step 3 Select **Online Devices** or **Offline Devices** as required.

Step 4 Set **Upload/Download Limit** for the devices, and click **Save**.



Control Mode: Manual

Online Devices | Offline Devices

Host Name	Total Download	Upload Bandwidth	Download Bandwidth	Upload Limit	Download Limit
LAPTOP-LNSBROQH 192.168.3.143/00:2B:67:2C:20:10	36.5MB	0KB/s	0KB/s	No Limit	No Limit
vivo-X60t-Pro 5G 192.168.3.72/86:53:DB:B6:9C:6B	0KB	0KB/s	0KB/s		lo Limit
vivo-X60t-Pro 2.4G 192.168.3.158/8C:67:94:C1:93:7E	0KB	0KB/s	0KB/s		lo Limit

No Limit
32KB/s
64KB/s
128KB/s
Manual (Unit: KB/s)

----End

Parameter description

Parameter	Description
Host Name	Specifies the name of client connected to the router.
Total Download	Specifies the total download traffic utilized by each client.
Offline Time	Only available for offline devices. Indicates the time when the client is disconnected.
Upload Bandwidth	Indicates the real-time upload/download bandwidth of each client. 1 Mbps=128 KB/s=1024 kb/s.
Download Bandwidth	
Upload Limit	Specifies the maximum upload/download rate you set for each client.
Download Limit	

Assume that you want to set the maximum upload/download rates for all the online or offline clients in the LAN.

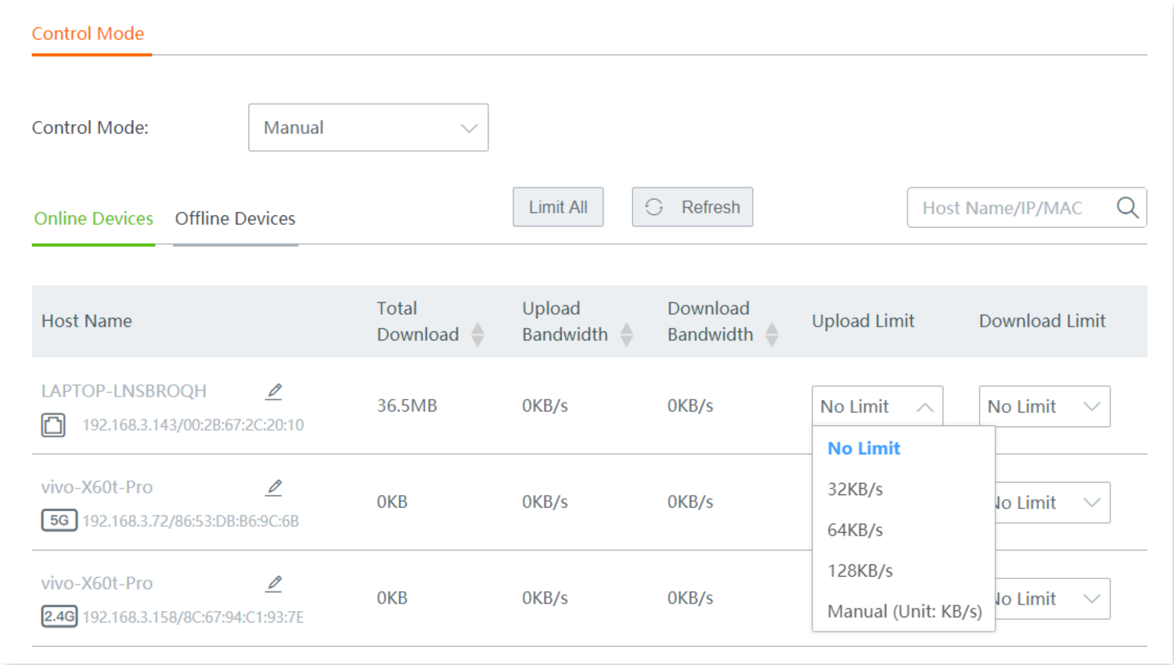
Configuration procedure

Step 1 Click **Bandwidth Control**.

Step 2 Set **Control Mode** to **Manual**.

Step 3 Select **Online Devices** or **Offline Devices** as required. Here takes **Online Devices** as an example.

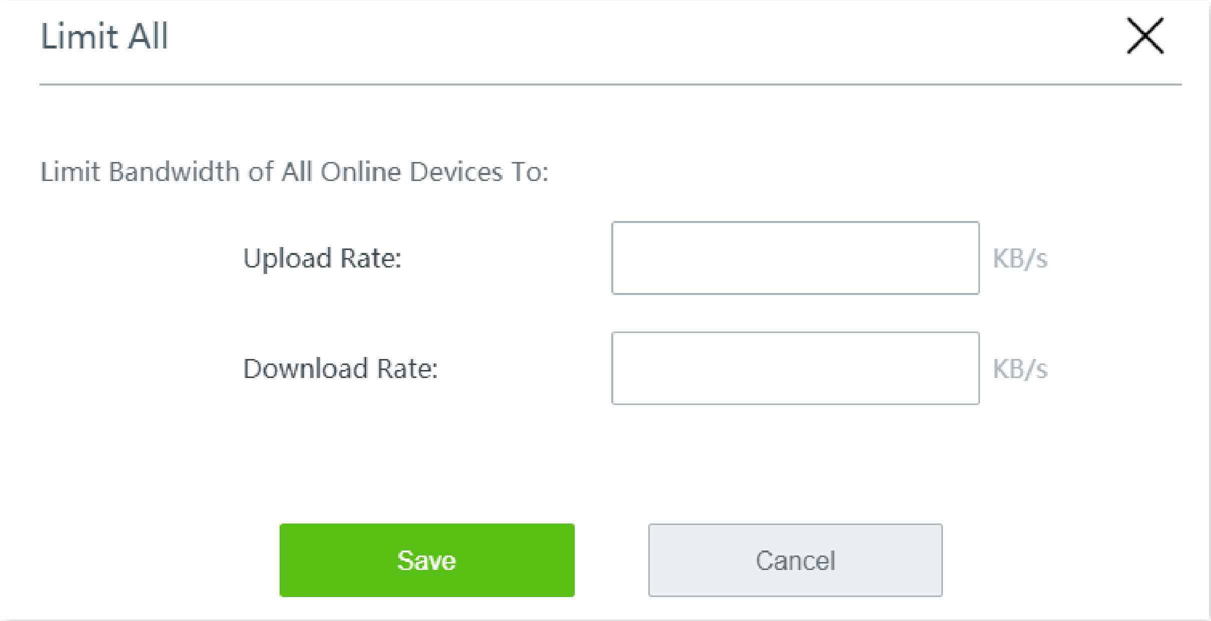
Step 4 Click **Limit All**.



Control Mode: Manual

Host Name	Total Download	Upload Bandwidth	Download Bandwidth	Upload Limit	Download Limit
LAPTOP-LNSBROQH 192.168.3.143/00:2B:67:2C:20:10	36.5MB	0KB/s	0KB/s	No Limit	No Limit
vivo-X60t-Pro 5G 192.168.3.72/86:53:DB:B6:9C:6B	0KB	0KB/s	0KB/s		No Limit
vivo-X60t-Pro 2.4G 192.168.3.158/8C:67:94:C1:93:7E	0KB	0KB/s	0KB/s		No Limit

Step 5 Set the maximum **Upload Rate** and **Download rate** for all the online and offline clients in the LAN, and click **Save**.



Limit All

Limit Bandwidth of All Online Devices To:

Upload Rate: KB/s

Download Rate: KB/s

----End

7.3 Auto

This mode distributes bandwidth evenly to the online clients connected to the router.

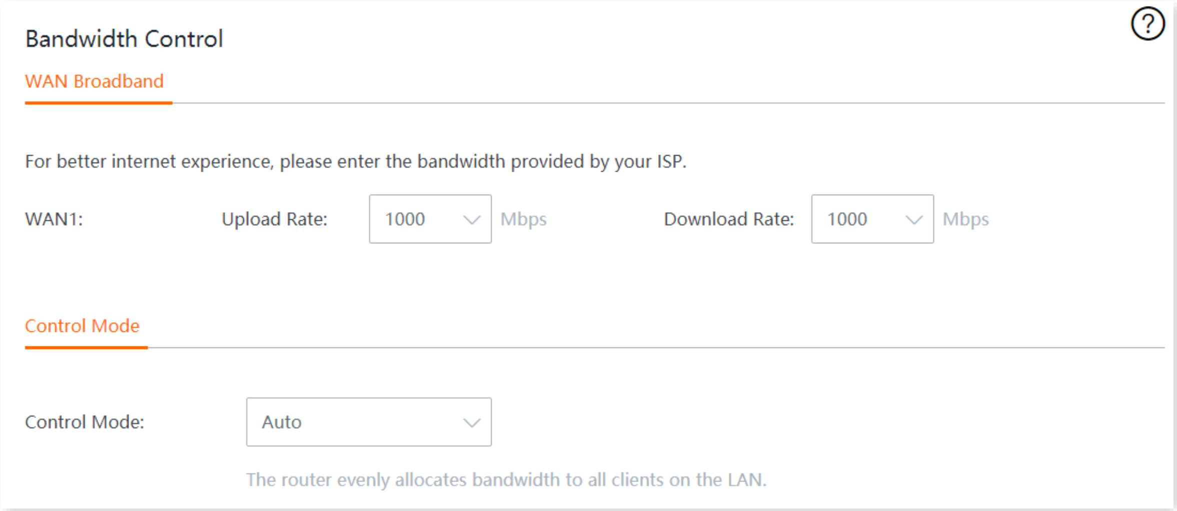
Configuration procedure

Step 1 Click **Bandwidth Control**.

Step 2 Set the **Upload Rate** and **Download Rate** of the target WAN port based on the bandwidth provided by your ISP.

Step 3 Set **Control Mode** to **Auto**.

Step 4 Click **Save** at the bottom of the page.



For better internet experience, please enter the bandwidth provided by your ISP.

WAN1: Upload Rate: 1000 Mbps Download Rate: 1000 Mbps

Control Mode: Auto

The router evenly allocates bandwidth to all clients on the LAN.

----End

7.4 Limit by group

Through the limit by group function, you can set a dedicated or shared upload/download rate for clients in an IP group to use in a period of time.

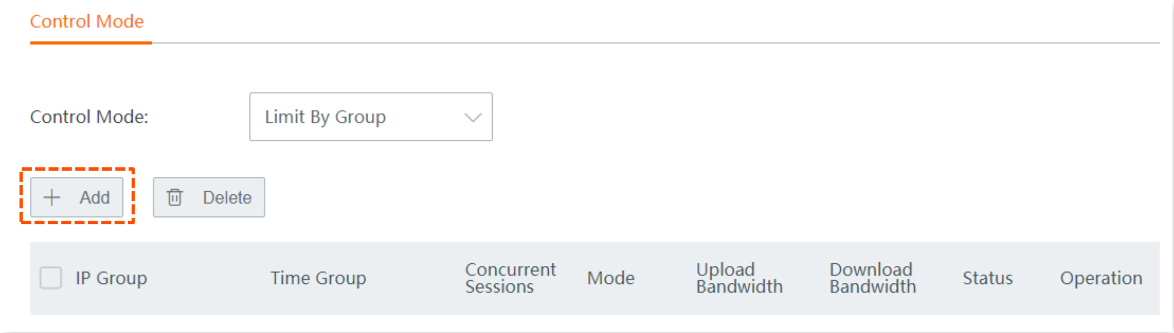
TIP

To control the bandwidth based on groups, you need to configure the IP group and time group first by navigating to **Filter Management** > IP Group/Time Group.

Step 1 Click **Bandwidth Control**.

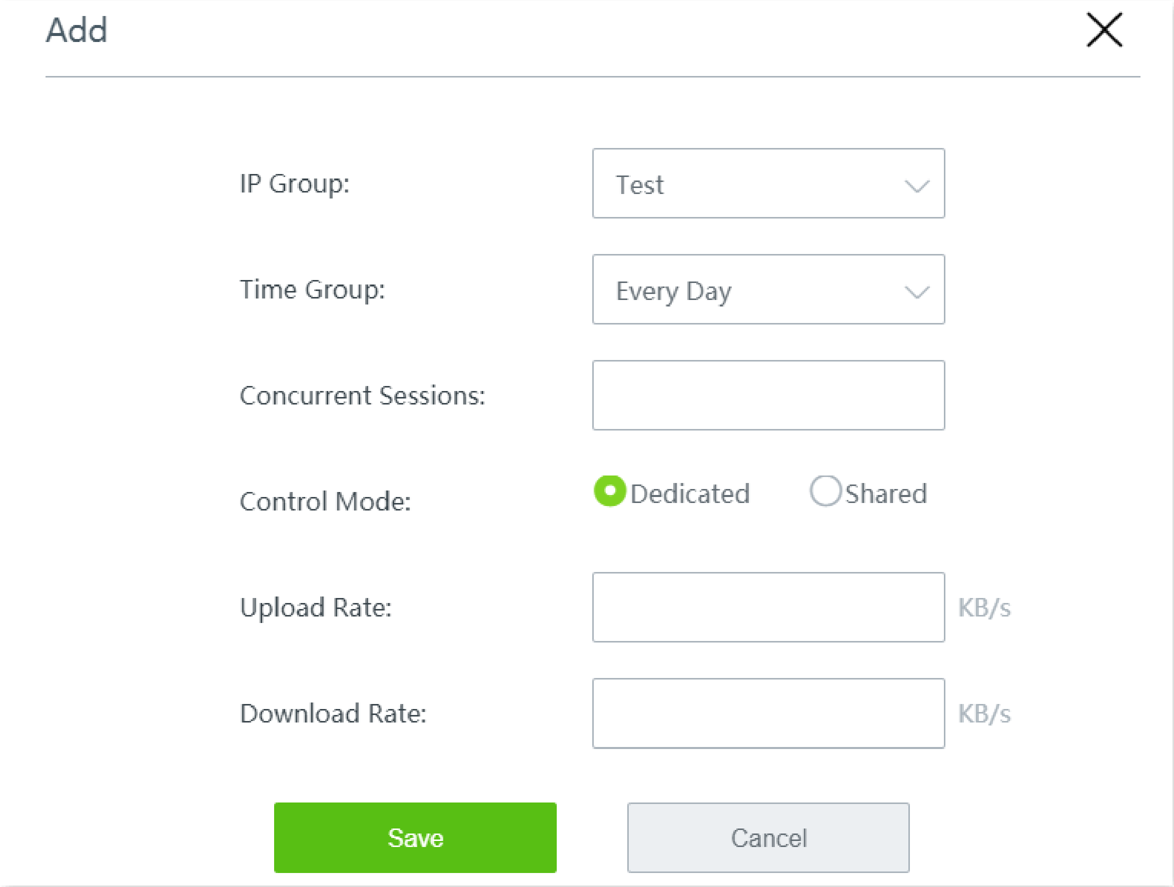
Step 2 Set **Control Mode** to **Limit By Group**.

Step 3 Click **+Add**.



Control Mode: Limit By Group

Step 4 Configure parameters in the **Add** window, and click **Save**.



IP Group: Test

Time Group: Every Day

Concurrent Sessions:

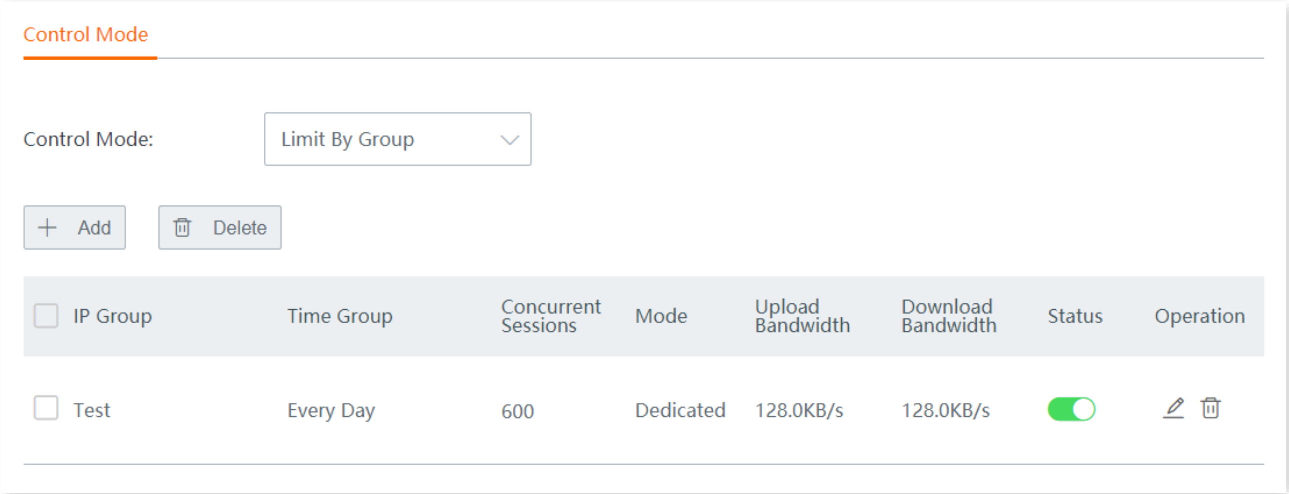
Control Mode: ● Dedicated ○ Shared

Upload Rate: KB/s

Download Rate: KB/s

----End

You can check the added rule on the page.



Control Mode: Limit By Group

□	IP Group	Time Group	Concurrent Sessions	Mode	Upload Bandwidth	Download Bandwidth	Status	Operation
□	Test	Every Day	600	Dedicated	128.0KB/s	128.0KB/s	●	✎ 🗑

Parameter description

Parameter	Description
IP Group	Specifies the IP group to be used, which is used to designate the clients with these IP addresses. IP group should be configured in advance on the **Filter Management** > **IP Group/Time Group** page.
Time Group	Specifies the time group to be used, which is used to designate the validity period of the rule. Time group should be configured in advance on the **Filter Management** > **IP Group/Time Group** page.
Concurrent Sessions	Specifies the maximum number of connections each client within the specified IP address range can use. Unless you have any special requirements, it is recommended to set the parameter to **600**.
Control Mode	Specifies the mode of bandwidth control rules. - **Dedicated**: Specifies that every client within the specified IP address range uses the set upload/download rate. Under this mode, every client obtains the same bandwidth. - **Shared**: Specifies that all clients within the specified IP address range use the set upload/download rate together. Under this mode, every client may obtain different bandwidths.
Upload Rate	Specifies the maximum upload/download rate you set.
Download Rate	
Status	Specifies the status of the rule. You can enable or disable the rule as required.
Operation	Specifies the operations you can perform on the rule. ✎: Click it to edit the rule. 🗑 : Click it to delete the rule.

7.5 Example of configuring limit by group rules

Networking requirement

An enterprise uses the wireless router to set up a network. The enterprise has the following requirements:

During business hours (08:00 to 18:00 every workday), procurement personnel's computers with IP addresses ranging from 192.168.0.2 to 192.168.0.250 can use a fixed upload and download bandwidth of 1 Mbps. For other clients in the LAN, no bandwidth control rules are added.

Group name	IP range	Effective time	Upload bandwidth	Download bandwidth
Procurement	192.168.0.2~250	08:00~18:00 on weekdays	1 Mbps	1 Mbps

Solution

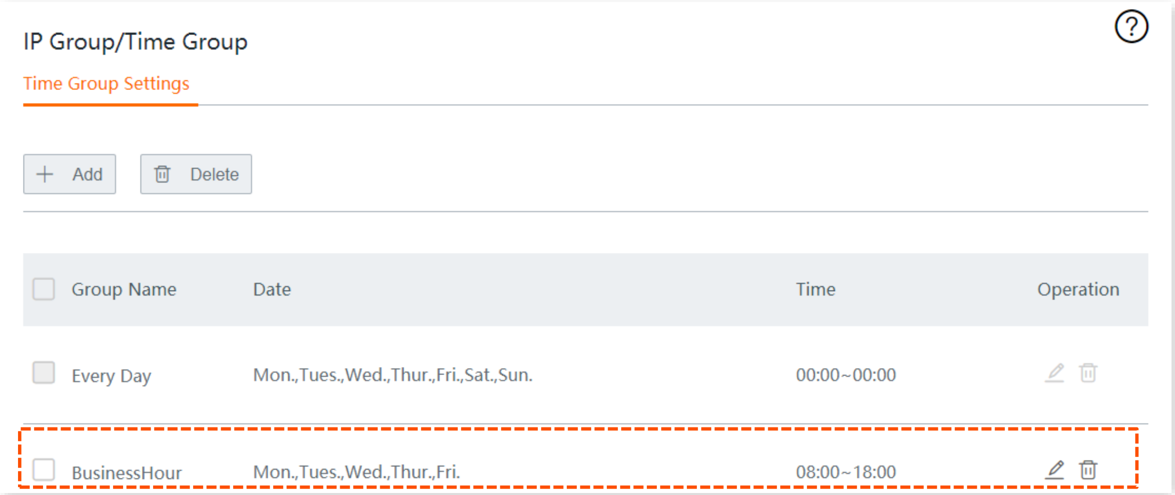
You can use the **Limit By Group** bandwidth control function of the router to meet this requirement. Assume that the concurrent sessions of each client is 600.

Configuration procedure

Step	Task	Description
1	Set a time group	Set the time group on the **Filter Management** > **IP Group/Time Group** page.
2	Set an IP group	Set the IP address group on the **Filter Management** > **IP Group/Time Group** page.
3	Set a bandwidth control rule	Set a limit by group rule on the **Bandwidth Control** page.

Step 1 Set a time group.

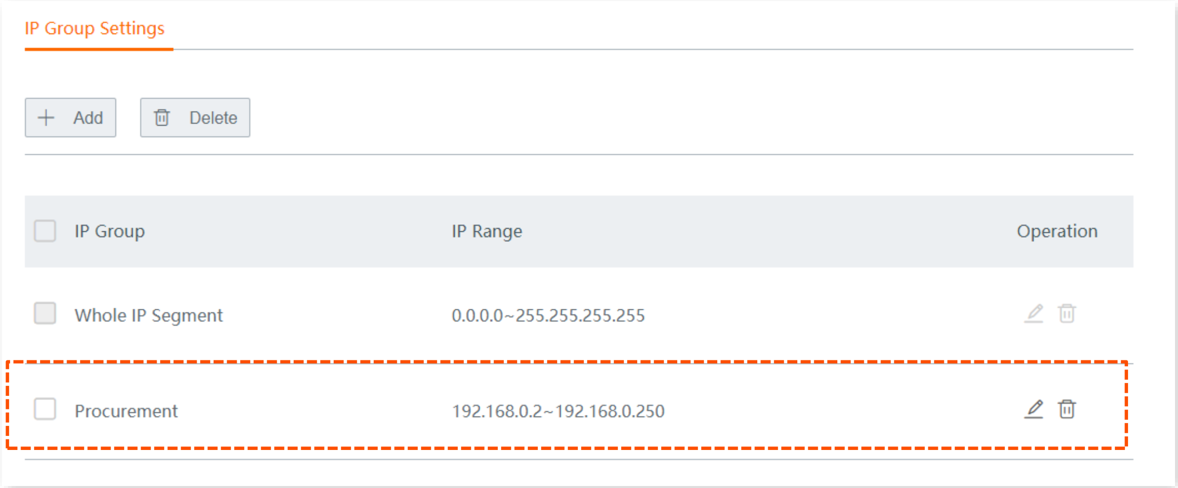
1. Navigate to **Filter Management** > **IP Group/Time Group**.
2. Set the time group shown in the following figure.



□	Group Name	Date	Time	Operation
□	Every Day	Mon.,Tues.,Wed.,Thur.,Fri.,Sat.,Sun.	00:00~00:00	
□	BusinessHour	Mon.,Tues.,Wed.,Thur.,Fri.	08:00~18:00	

Step 2 Set an IP group.

1. Navigate to **Filter Management** > **IP Group/Time Group**.
2. Set the IP group shown in the following figure.



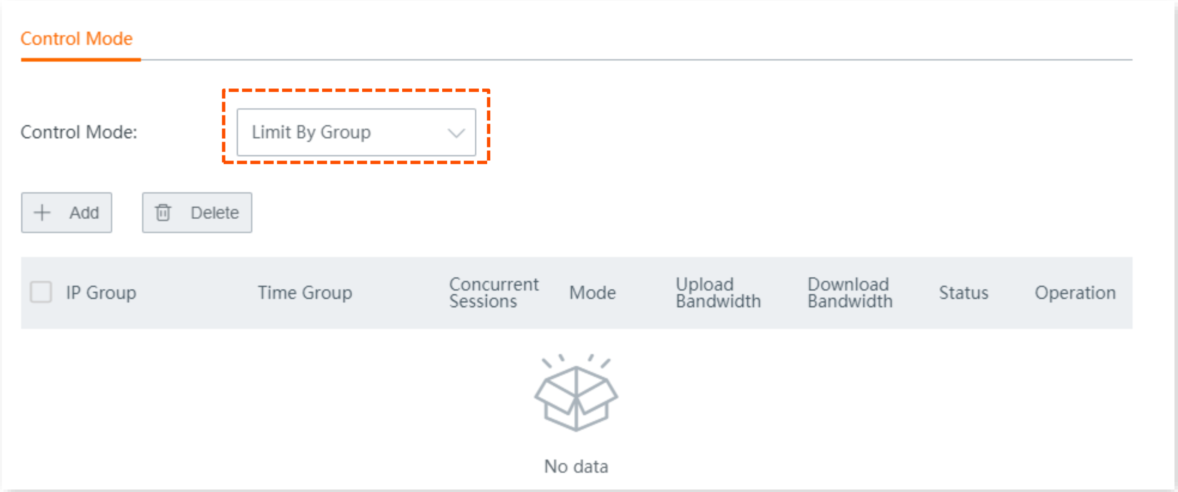
IP Group Settings

＋ Add　🗑 Delete

□	IP Group	IP Range	Operation
□	Whole IP Segment	0.0.0.0~255.255.255.255	✎ 🗑
□	Procurement	192.168.0.2~192.168.0.250	✎ 🗑

Step 3 Set a bandwidth control rule.

1. On the **Bandwidth Control** page, set **Control Mode** to **Limit By Group**.
2. Click **Save** at the bottom of the page.



Control Mode

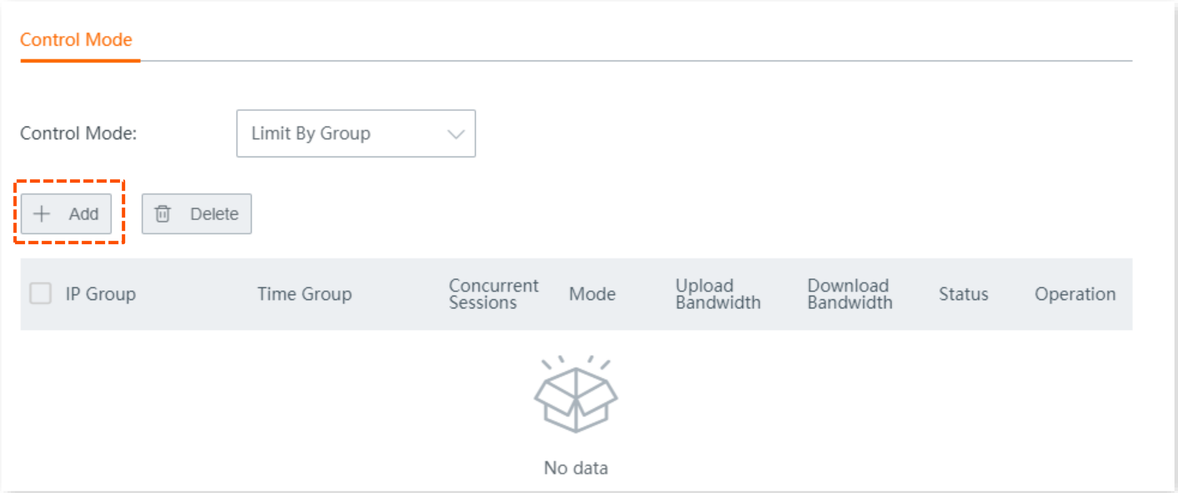
Control Mode: Limit By Group

＋ Add　🗑 Delete

□	IP Group	Time Group	Concurrent Sessions	Mode	Upload Bandwidth	Download Bandwidth	Status	Operation

No data

3. Click **+Add**.



Control Mode

Control Mode: Limit By Group

＋ Add　🗑 Delete

□	IP Group	Time Group	Concurrent Sessions	Mode	Upload Bandwidth	Download Bandwidth	Status	Operation

No data

4. Configure parameters in the **Add** window, and click **Save**.

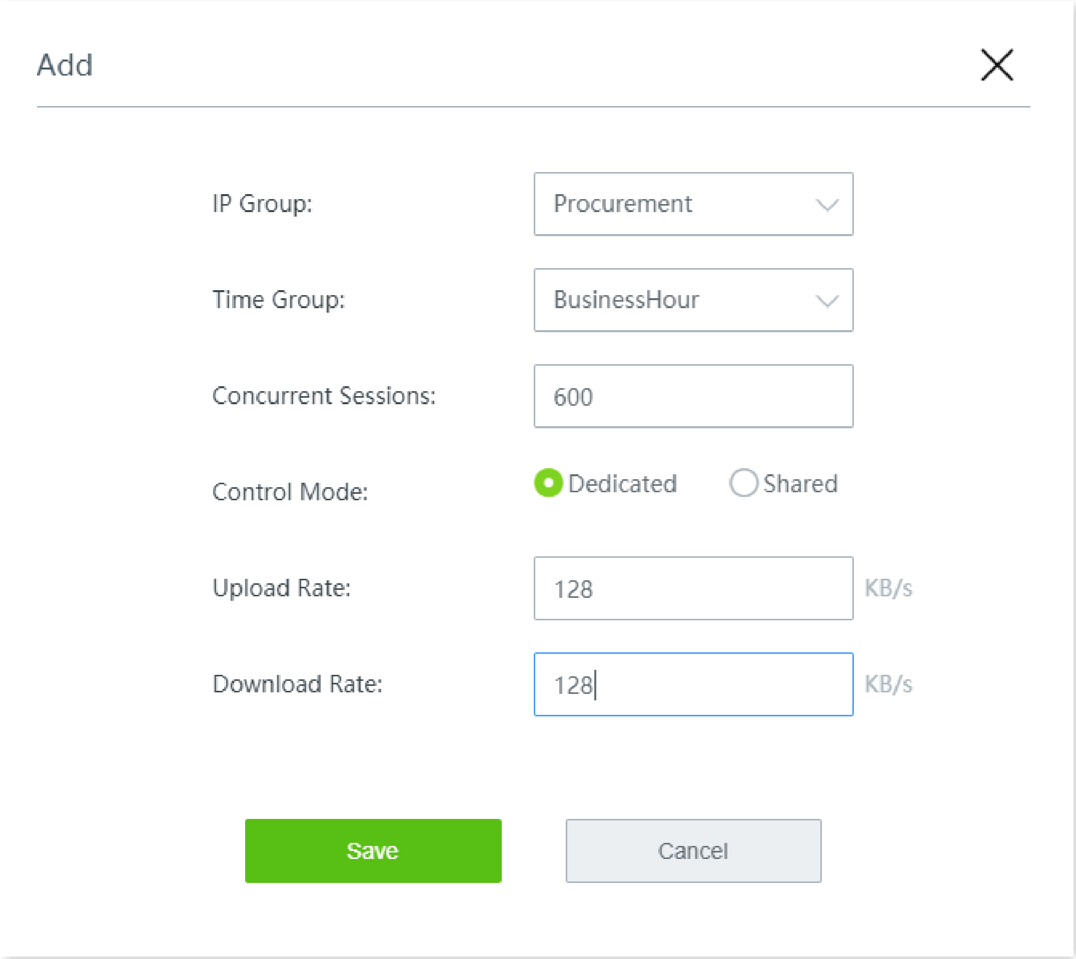
   (1) Select **Procurement** for **IP Group**.

   (2) Select **BusinessHour** for **Time Group**.

   (3) Set **Concurrent Sessions** of each client to **600** in this example.

   (4) Set **Control Mode** to **Dedicated**.

   (5) Set the maximum upload/download rate of clients to both **128 KB/s** in this example.



Add

IP Group: Procurement

Time Group: BusinessHour

Concurrent Sessions: 600

Control Mode: ● Dedicated ○ Shared

Upload Rate: 128 KB/s

Download Rate: 128 KB/s

----End

Verification

During business hours from 08:00 to 18:00 on weekdays, each computer with an IP address ranging from 192.168.0.2 to 192.168.0.250 is allocated 1 Mbps (128 KB/s) upload and download bandwidth.

8 Authentication

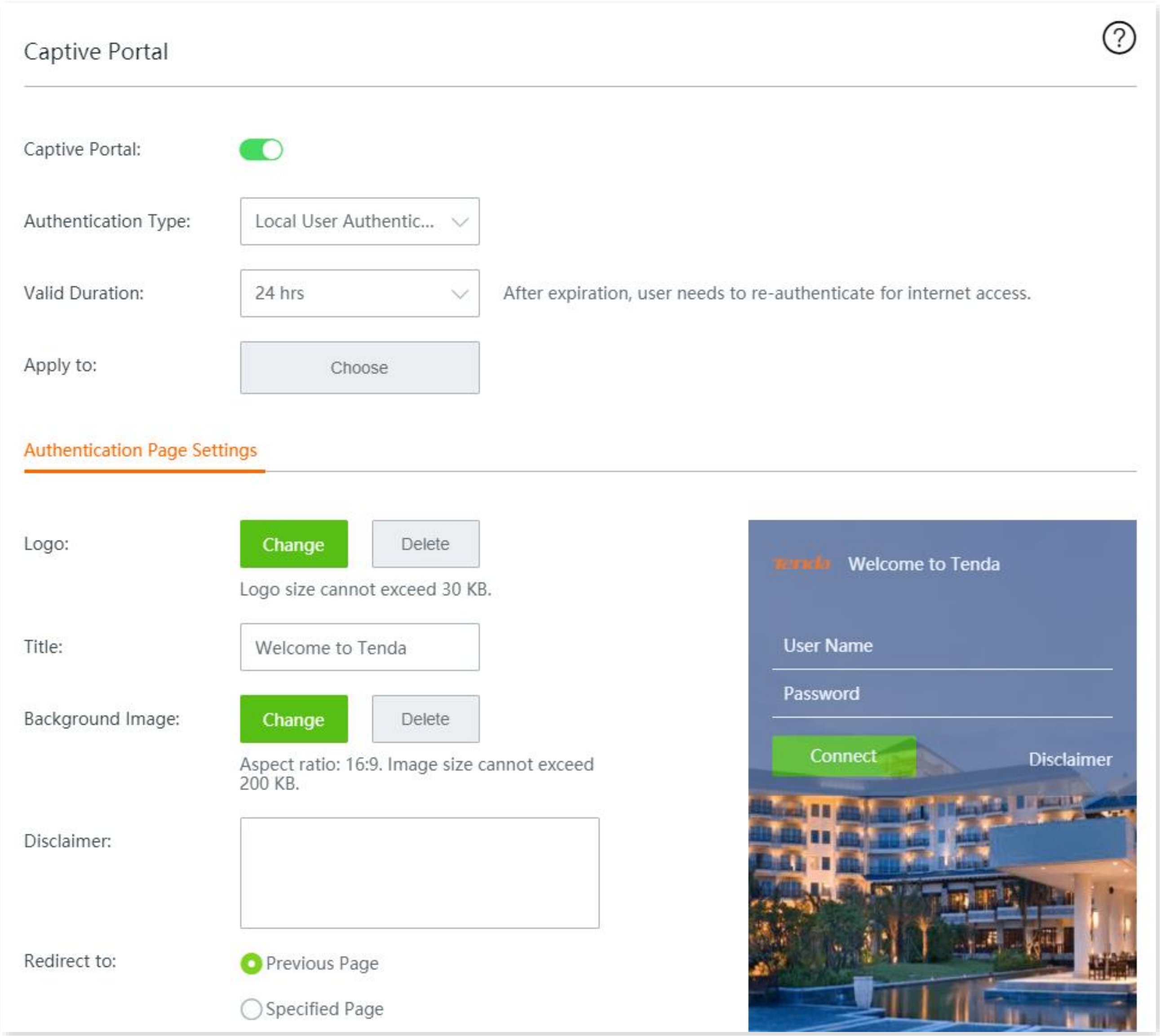
8.1 Captive portal

8.1.1 Overview

By default, after the router is connected to the internet, the LAN users will have internet availability. After the Captive Portal function is enabled, users connected to the authentication network need to pass the authentication before gaining internet access.

Click **Authentication** > **Captive Portal** to enter the page.

Here, you can configure the authentication page and authentication policy.



Captive Portal

Captive Portal: ●

Authentication Type: Local User Authentic...

Valid Duration: 24 hrs After expiration, user needs to re-authenticate for internet access.

Apply to: Choose

Authentication Page Settings

Logo: Change Delete

Logo size cannot exceed 30 KB.

Title: Welcome to Tenda

Background Image: Change Delete

Aspect ratio: 16:9. Image size cannot exceed 200 KB.

Disclaimer:

Redirect to:
● Previous Page
○ Specified Page

Parameter description

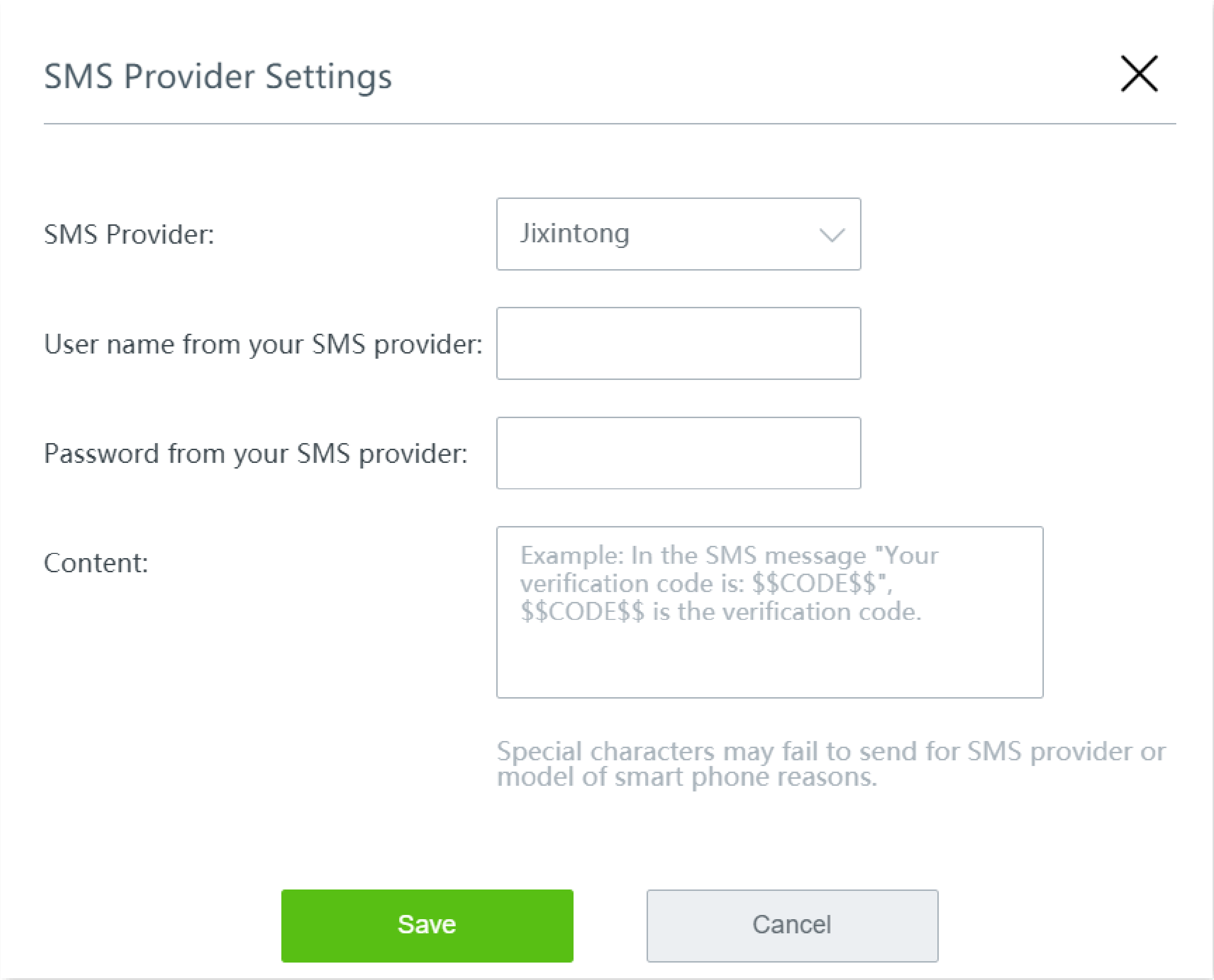
Parameter	Description
Captive Portal	Enable or disable the captive portal function of the router.
Authentication Type	Specifies the types of the captive portal. • **WiFi via SMS:** It allows a user to access the internet with a verification code sent by SMS when receiving an authentication web page. To enable this authentication type, you need to configure SMS Provider Settings first. • **Local User Authentication**: It allows a user to access the internet with a username and password on the authentication web page. The username and password should be added on **Authentication >** User Management page. • **Email Authentication**: It allows a user to access the internet with a verification code sent through email when receiving an authentication web page. To enable this authentication type, you need to configure Email Server Settings first. • **One-key Authentication**: It allows a user to access the internet by clicking **Connect** when receiving an authentication web page.
Valid Duration	Specifies the authentication validity period. A user must be re-authenticated for accessing the internet after the period expires.
Apply to	**Wired Network**: Specifies that the authentication rule will be applied to the devices connected to the router through the selected ports. **WiFi Network**: Specifies that the authentication rule will be applied to the wireless devices connected to the router through the selected WiFi networks. TIP If the user does not select a kind of network, the captive portal authentication is effective to all networks in the list.
People Shared with	Only available for **Email Authentication**. Specifies the number of users allowed to access the internet using a same email address.
Logo	Specifies the logo image of the web authentication page. Click **Change** to change the logo picture, and click **Delete** to delete the uploaded picture.
Title	Specifies the title information of the web authentication page. It is **Welcome to Tenda** by default.
Background Image	Specifies the background image of the web authentication page. Click **Change** to change the picture, and click **Delete** to delete the uploaded picture.
Disclaimer	Specifies the disclaimer information on the web authentication page.
Redirect To	Specifies the website that the client automatically redirects to after passing authentication: • **Previous Page**: When the captive portal is passed, the page would redirect to the previous page the user visited. For example, if a user is visiting Google search page before authentication, the user will stay on Google search page after passing the authentication. • **Specified Page**: Specifies the website redirected to after passing the captive portal.

SMS provider settings

SMS provider is the provider who issues authorization verification code to designated mobile phone number. At present, supported SMS providers include **Jixintong** and **NEXMO**, and you can also choose **Custom HTTP Interconnection** to use other SMS providers.

TIP

You need to purchase an SMS package in the corresponding SMS provider first, and then configure the applied interconnection information to this router.



SMS Provider Settings

SMS Provider: Jixintong

User name from your SMS provider:

Password from your SMS provider:

Content: Example: In the SMS message "Your verification code is: $$CODE$$", $$CODE$$ is the verification code.

Special characters may fail to send for SMS provider or model of smart phone reasons.

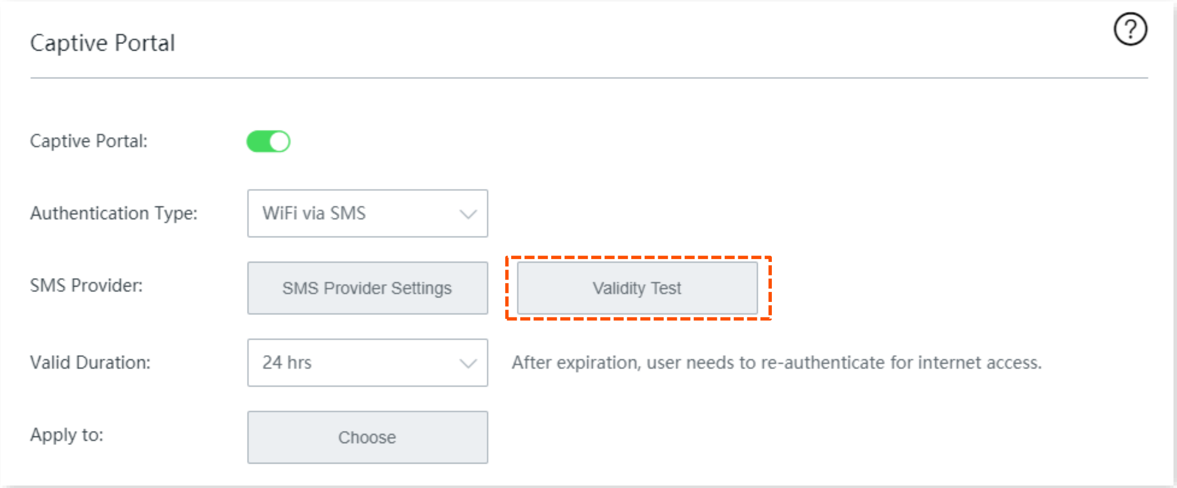
Parameter description

Parameter		Description
Jixintong	User name from your SMS provider	Enter the user name and password you've applied on the Jixintong platform.
	Password from your SMS provider	
	Content	Customize the short message sent to users. TIP The verification code format is **$$CODE$$**, which cannot be modified.

Parameter		Description
NEXMO	api_key	Enter the **api_key** you've applied on the NEXMO platform.
	api_secret	Enter the **api_secret** you've applied on the NEXMO platform.
	Content	Customize the short message sent to users. TIP The verification code format is **$$CODE$$**, which cannot be modified.
Customize HTTP Interconnection	Encoding	Specifies the character encoding format. Select the encoding format that your SMS provider supports.
	Content	Customize the short message sent to users. TIP The verification code format is **$$CODE$$**, which cannot be modified.
	SMS Gateway URL Interface	Enter the URL interface address of SMS gateway provided by SMS service provider. In general, SMS service providers provide the format of SMS Gateway URL Interface and users need to complete the URL interface address of SMS gateway according to the information applied for in SMS service providers.
	SMS Error Code	Enter the SMS error code of SMS service provider. After the SMS platform fails to send an SMS message, it will send the message to this router. Users can consult the corresponding SMS service provider based on relevant information. For the specific content of the SMS error code, consult the corresponding SMS service provider.

After the **SMS Provider Settings**, you can conduct the **Validity Test** to check whether the settings you made are correct. The steps are as follows:

Step 1 Click **Validity Test**.



Captive Portal

Captive Portal: ●

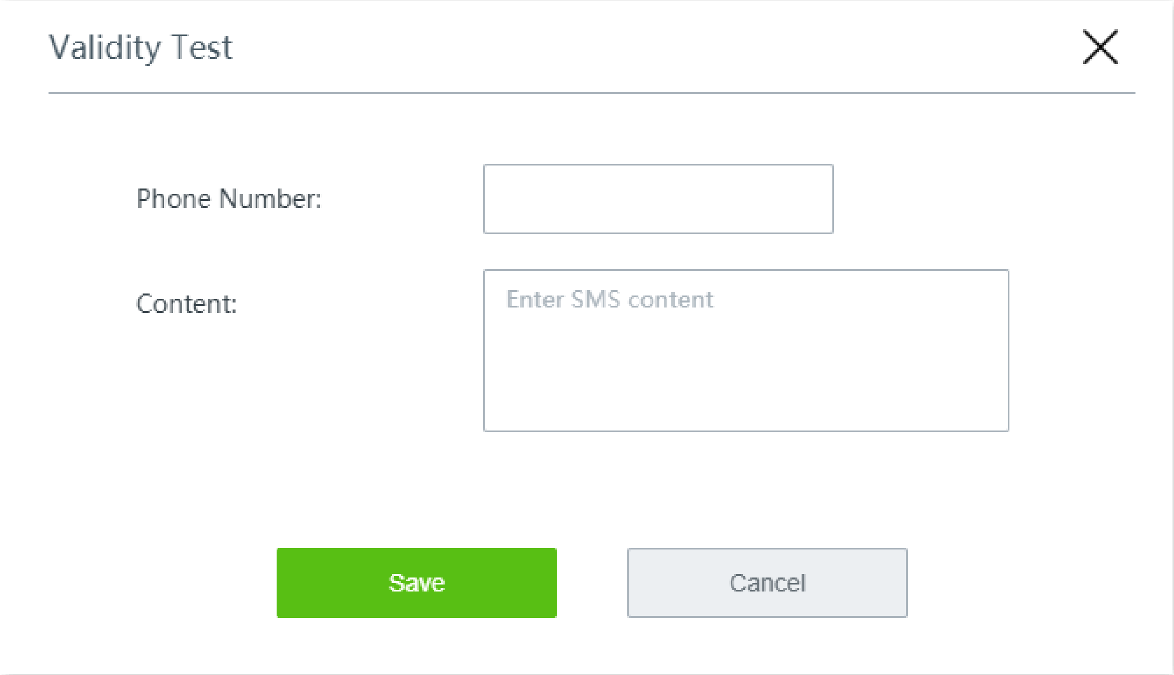
Authentication Type: WiFi via SMS

SMS Provider: SMS Provider Settings | Validity Test

Valid Duration: 24 hrs — After expiration, user needs to re-authenticate for internet access.

Apply to: Choose

Step 2 Enter the **Phone Number** and the short message **Content** sent by the SMS platform, and click **Save**.



Validity Test

Phone Number:

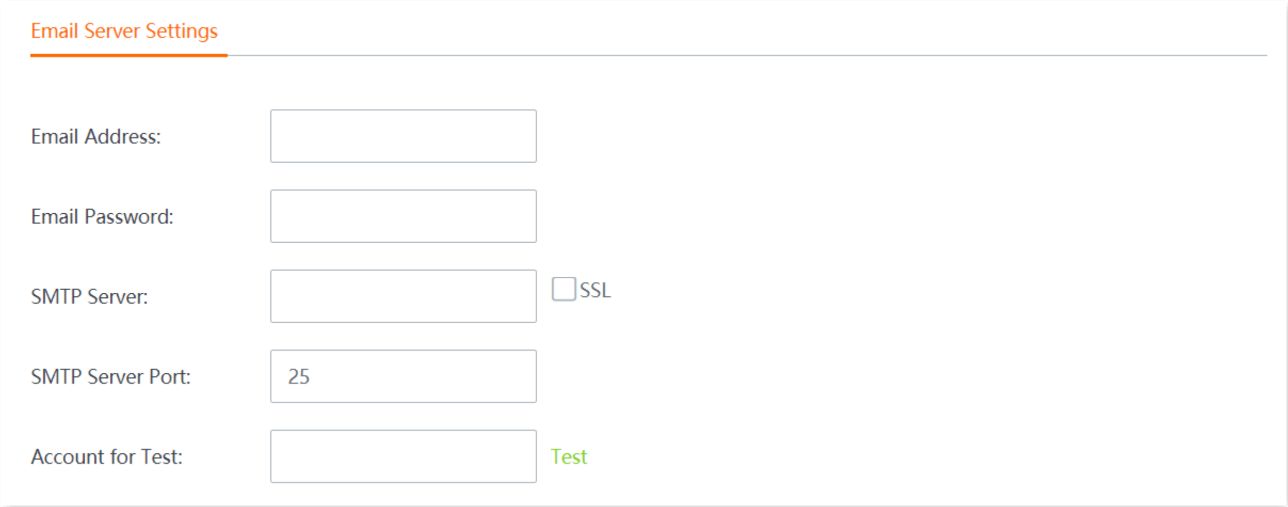
Content: Enter SMS content

----End

Wait a moment. If the interconnection is successful, the phone number will receive an SMS message containing a verification code.

Email server settings

This router supports email authentication. Related parameters are as follows.



Email Server Settings

Email Address:

Email Password:

SMTP Server: □SSL

SMTP Server Port: 25

Account for Test:

Parameter description

Parameter	Description
Email Address	Specifies the email account that sends email.
Email Password	Specifies the password or authorization code of the email account.

Parameter	Description
SMTP Server	Specifies the SMTP server address. It could be an IP address or domain name address. TIP The SMTP (Simple Mail Transfer Protocol) server is a mail delivery server. The address and port of the SMTP server of each mail service provider are different. Please check on your own.
SSL	Secure Sockets Layer, a security protocol. It uses data encryption, identity authentication and message integrity verification mechanism to ensure the security of network data transmission.
SMTP Server Port	Specifies the SMTP service port. By default, it is 25. TIP If you select SSL, the server port will change. Please contact your email service provider for the information.
Account for Test	Specifies the email account, which is used to test whether the email server settings are valid.

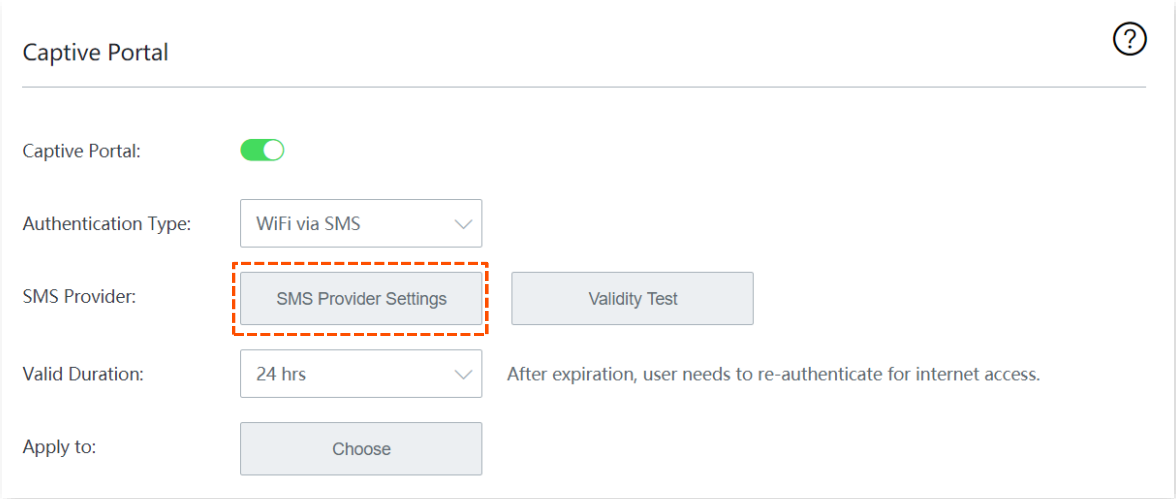
8.1.2 Configure SMS authentication

Step 1 Navigate to **Authentication** > **Captive Portal**.

Step 2 Enable **Captive Portal**.

Step 3 Configure the following parameters, then click **Save** at the bottom of the page.

1. Set **Authentication Type** to **WiFi via SMS**.
2. Click **SMS Provider Settings**, then the configuration window appears.



Captive Portal

Captive Portal: ●

Authentication Type: WiFi via SMS

SMS Provider: SMS Provider Settings | Validity Test

Valid Duration: 24 hrs — After expiration, user needs to re-authenticate for internet access.

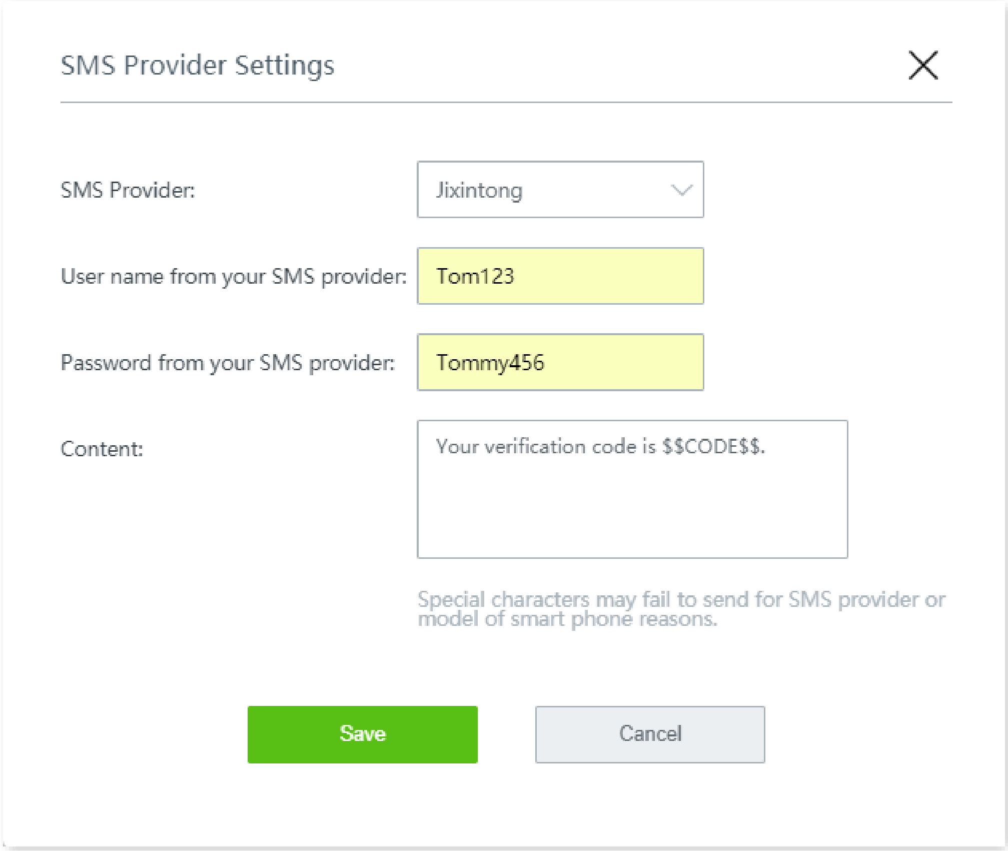
Apply to: Choose

3. Configure the following parameters related to the SMS provider, and click **Save**.

   (1) Select the **SMS provider** from which you have purchased an SMS package, such as **Jixintong**.

   (2) Enter the **User name** and **Password from your SMS provider**, such as **Tom123** and **Tommy456**.

(3) Customize the SMS **Content** sent to the user by the SMS platform for verification.



SMS Provider Settings

SMS Provider: Jixintong

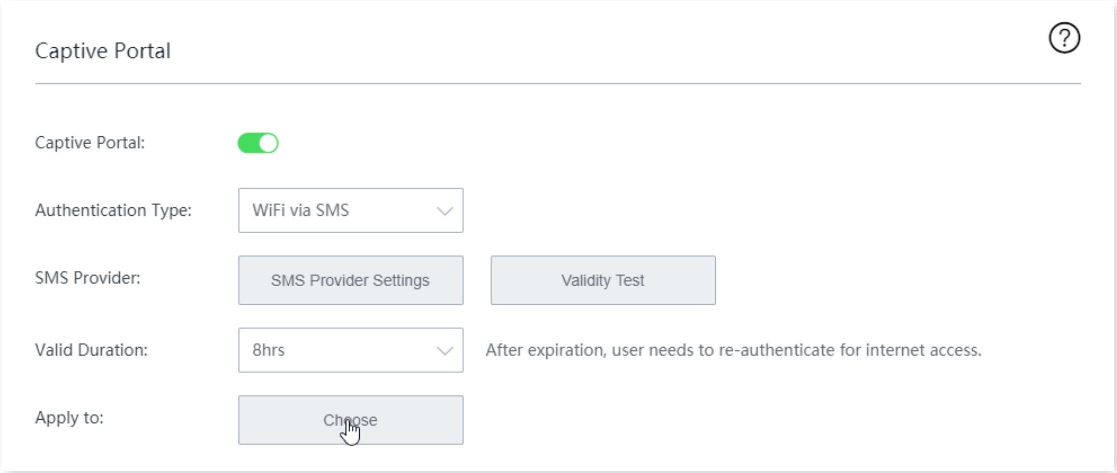
User name from your SMS provider: Tom123

Password from your SMS provider: Tommy456

Content: Your verification code is $$CODE$$.

Special characters may fail to send for SMS provider or model of smart phone reasons.

4. Set the **Valid Duration**, such as **8 hrs**.
5. Click **Choose,** choose the network(s) to be applied, and click **Save**.



Captive Portal

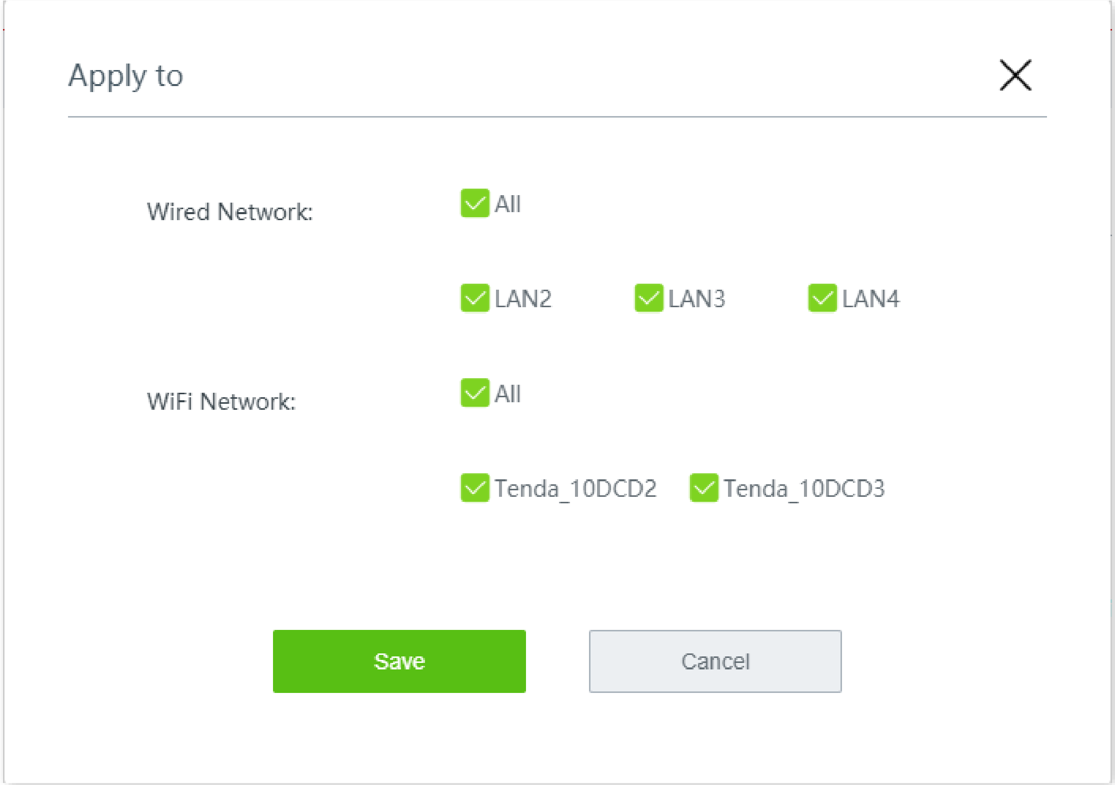
Captive Portal: ON

Authentication Type: WiFi via SMS

SMS Provider:

Valid Duration: 8hrs After expiration, user needs to re-authenticate for internet access.

Apply to:



Apply to

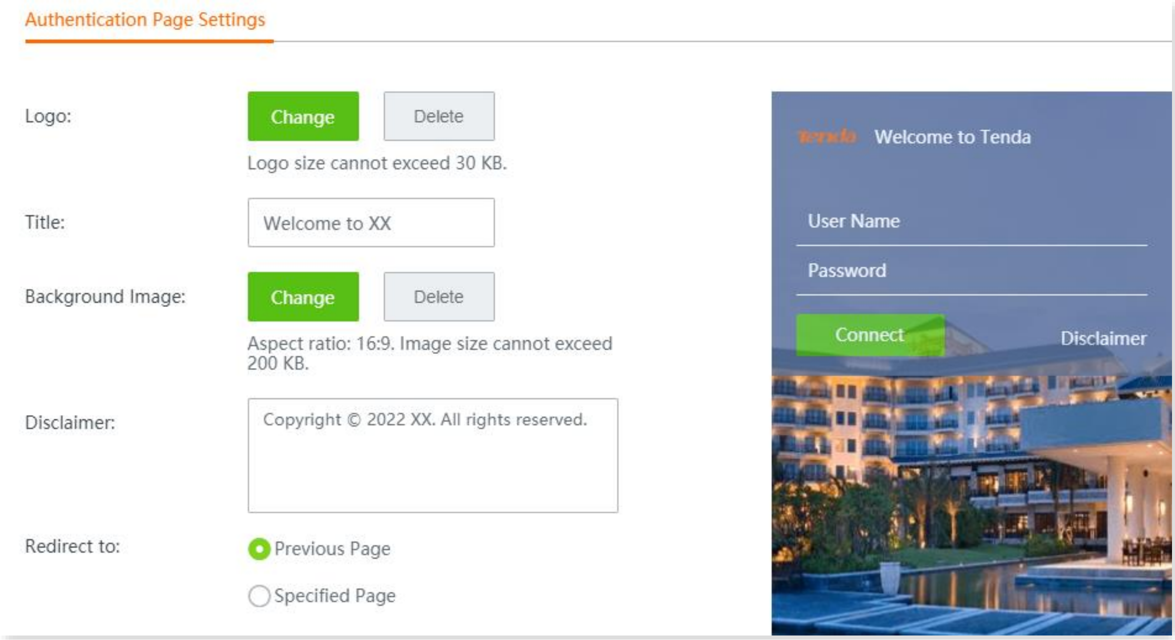
Wired Network: ☑ All

☑ LAN2 ☑ LAN3 ☑ LAN4

WiFi Network: ☑ All

☑ Tenda_10DCD2 ☑ Tenda_10DCD3

6. Configure the authentication page settings.
   (1) Click **Change** and upload the company logo image.
   (2) Set the title of the captive portal page, such as **Welcome to XX**.
   (3) Click **Change** and upload the background image of the captive portal page, such as the enterprise promotion photo.
   (4) Set the disclaimer information of the enterprise, such as **Copyright © 2022 XX. All rights reserved**.
   (5) Select the **Previous Page** or enter a **Specified Page** as the page to which the users are redirected after passing the authentication.



Authentication Page Settings

Logo: Change Delete

Logo size cannot exceed 30 KB.

Title: Welcome to XX

Background Image: Change Delete

Aspect ratio: 16:9. Image size cannot exceed 200 KB.

Disclaimer: Copyright © 2022 XX. All rights reserved.

Redirect to: ● Previous Page ○ Specified Page

----End

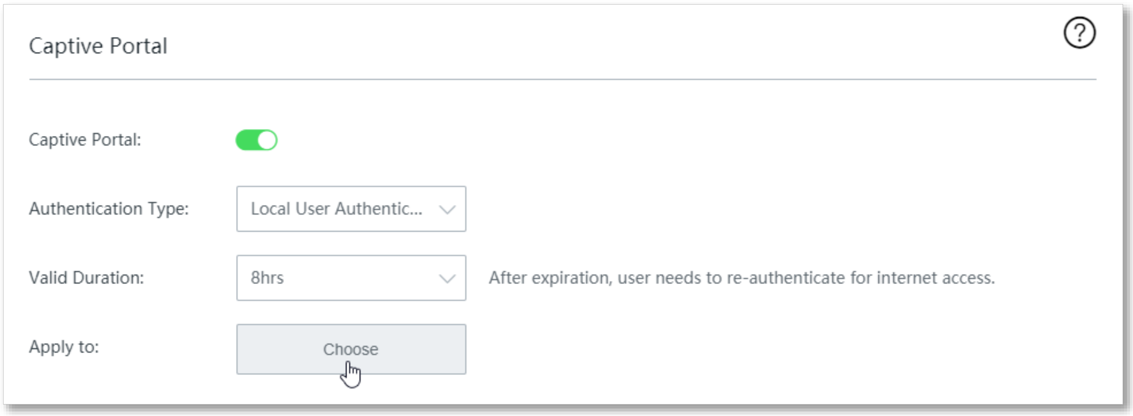
8.1.3 Configure local user authentication

Step 1 Navigate to **Authentication** > **Captive Portal**.

Step 2 Enable **Captive Portal**.

Step 3 Configure the following parameters, then click **Save** at the bottom of the page.

1. Set **Authentication Type** to **Local User Authentication**.
2. Set the **Valid Duration**, such as **8 hrs**.
3. Click **Choose,** choose the network(s) to be applied, and click **Save**.



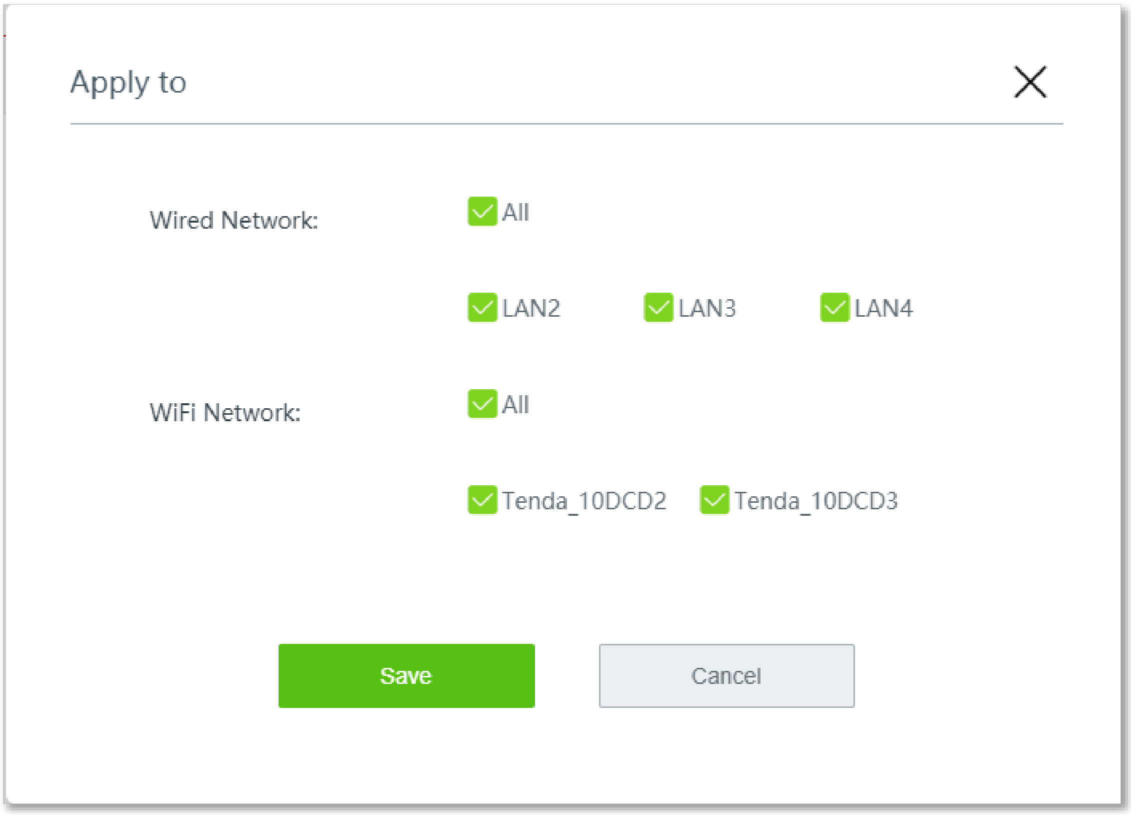
Captive Portal

Captive Portal: ●

Authentication Type: Local User Authentic...

Valid Duration: 8hrs After expiration, user needs to re-authenticate for internet access.

Apply to:



Apply to

Wired Network: ☑ All

☑ LAN2 ☑ LAN3 ☑ LAN4

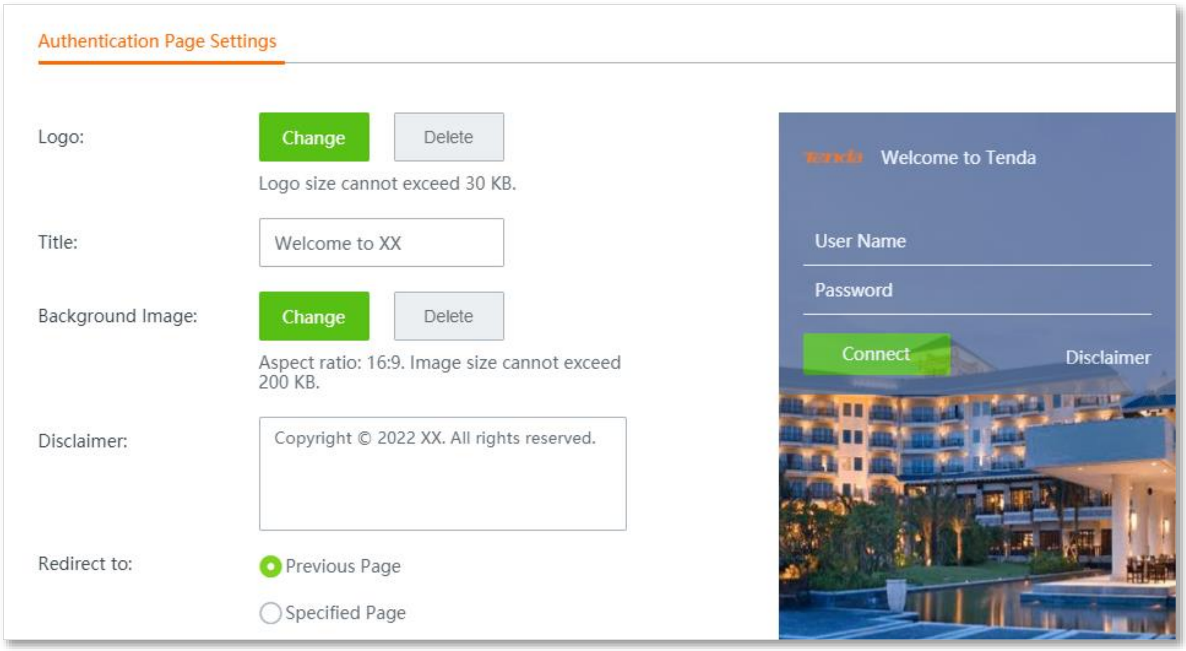
WiFi Network: ☑ All

☑ Tenda_10DCD2 ☑ Tenda_10DCD3

4. Configure the authentication page settings.
   (1) Click **Change** and upload the company logo image.
   (2) Set the title of the captive portal page, such as **Welcome to XX**.
   (3) Click **Change** and upload the background image of the captive portal page, such as the enterprise promotion photo.

(4) Set the disclaimer information of the enterprise, such as **Copyright © 2022 XX. All rights reserved**.

(5) Select the **Previous Page** or enter a **Specified Page** as the page to which the users are redirected after passing the authentication.



Authentication Page Settings

Logo: Change Delete

Logo size cannot exceed 30 KB.

Title: Welcome to XX

Background Image: Change Delete

Aspect ratio: 16:9. Image size cannot exceed 200 KB.

Disclaimer: Copyright © 2022 XX. All rights reserved.

Redirect to: ● Previous Page ○ Specified Page

Step 4 Set the **User Name** and **Password** by referring to Add user accounts for local user authentication.

----End

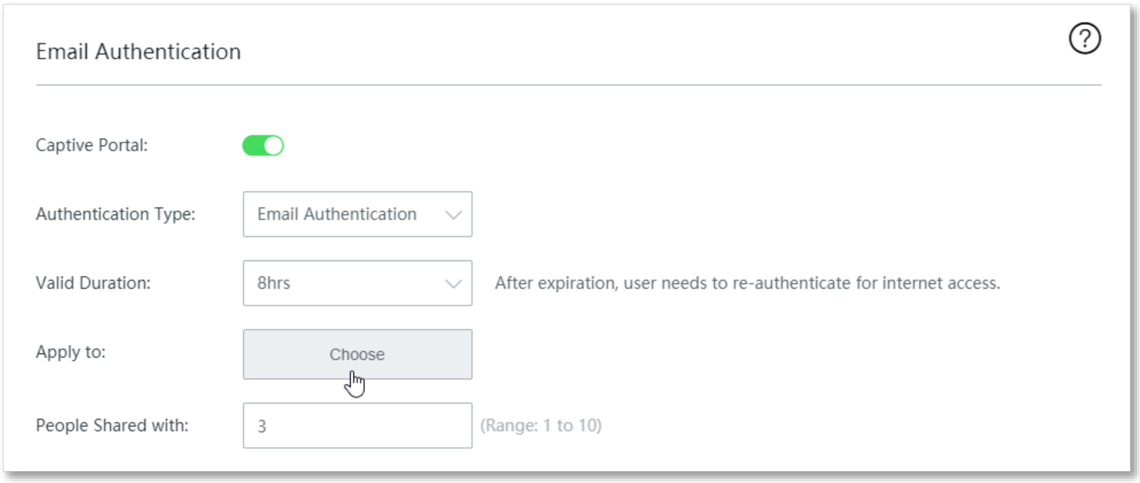
8.1.4 Configure email authentication

Step 1 Navigate to **Authentication** > **Captive Portal**.

Step 2 Enable **Captive Portal**.

Step 3 Configure the following parameters, then click **Save** at the bottom of the page.

1. Set **Authentication Type** to **Email Authentication**.
2. Set the **Valid Duration**, such as **8 hrs**.
3. Set the **People Shared with** (the number of users allowed to connect to the internet using the email at the same time), such as **3**.
4. Click **Choose,** choose the network(s) to be applied, and click **Save**.



Email Authentication

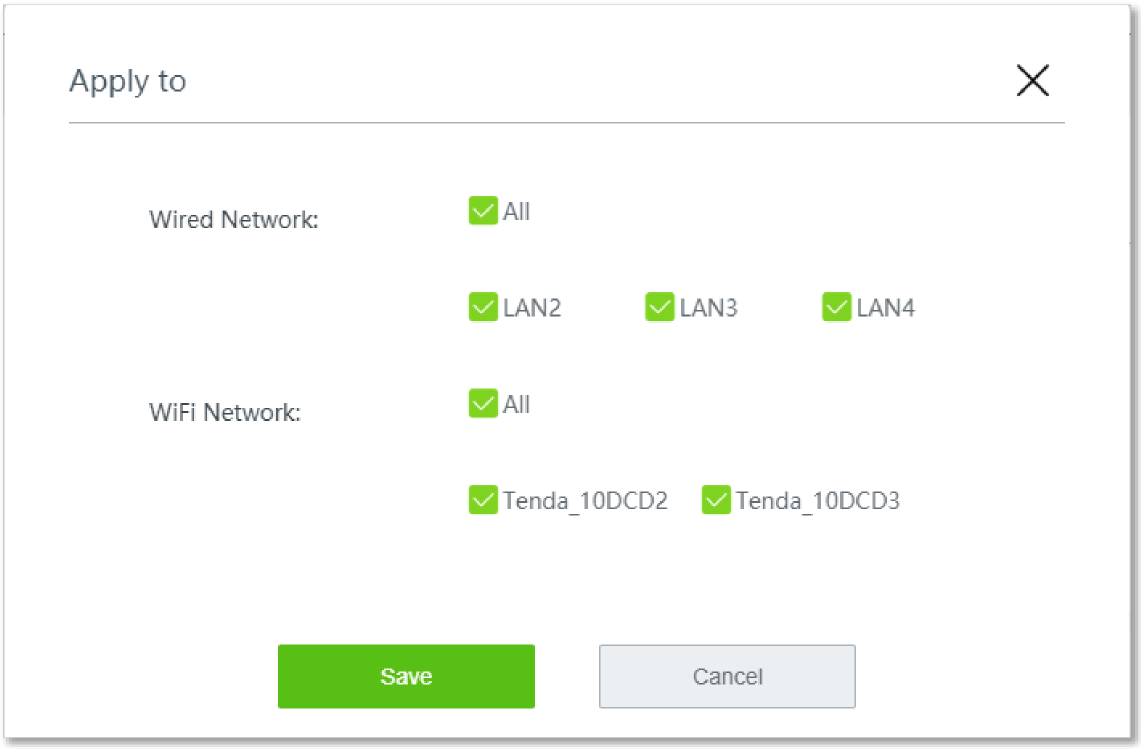
Captive Portal: ●

Authentication Type: Email Authentication

Valid Duration: 8hrs After expiration, user needs to re-authenticate for internet access.

Apply to: Choose

People Shared with: 3 (Range: 1 to 10)



Apply to

Wired Network: ☑ All

☑ LAN2 ☑ LAN3 ☑ LAN4

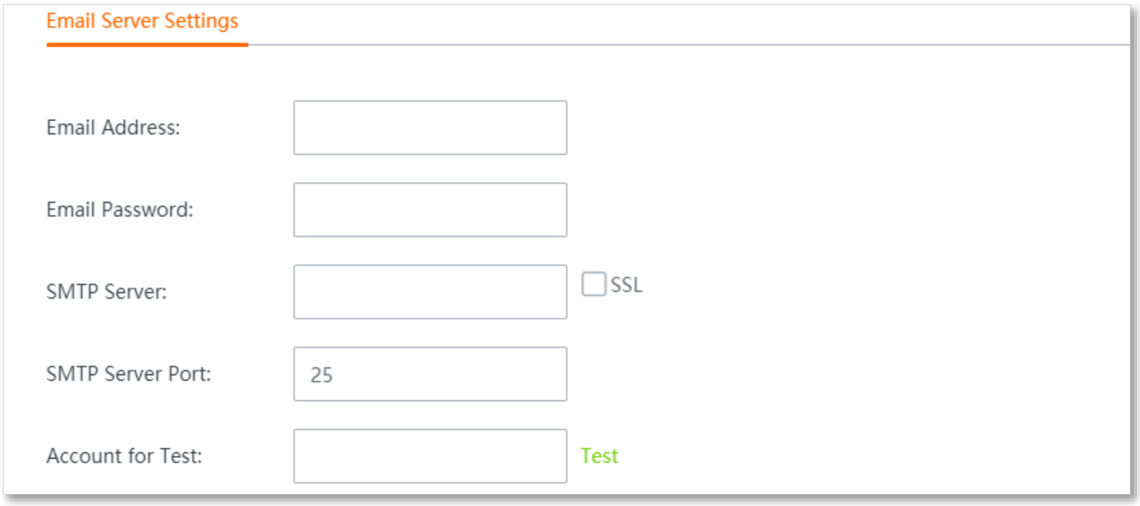
WiFi Network: ☑ All

☑ Tenda_10DCD2 ☑ Tenda_10DCD3

5. Configure the email server settings**.**
   (1) Enter the **Email Address**.
   (2) Enter the corresponding **Email Password**.
   (3) Enter the **SMTP Server** address.

(4) Enter the **SMTP Server Port**. It is recommended to keep the default settings.

(5) Enter the **Account for Test** (a valid email address) to check whether the email server is effective.



Email Server Settings

Email Address:

Email Password:

SMTP Server: □ SSL

SMTP Server Port: 25

Account for Test: Test

6. Configure the authentication page settings.

(1) Set the **Email Content** sent to users ("$$CODE$$" is the format of the email verification code and cannot be modified).

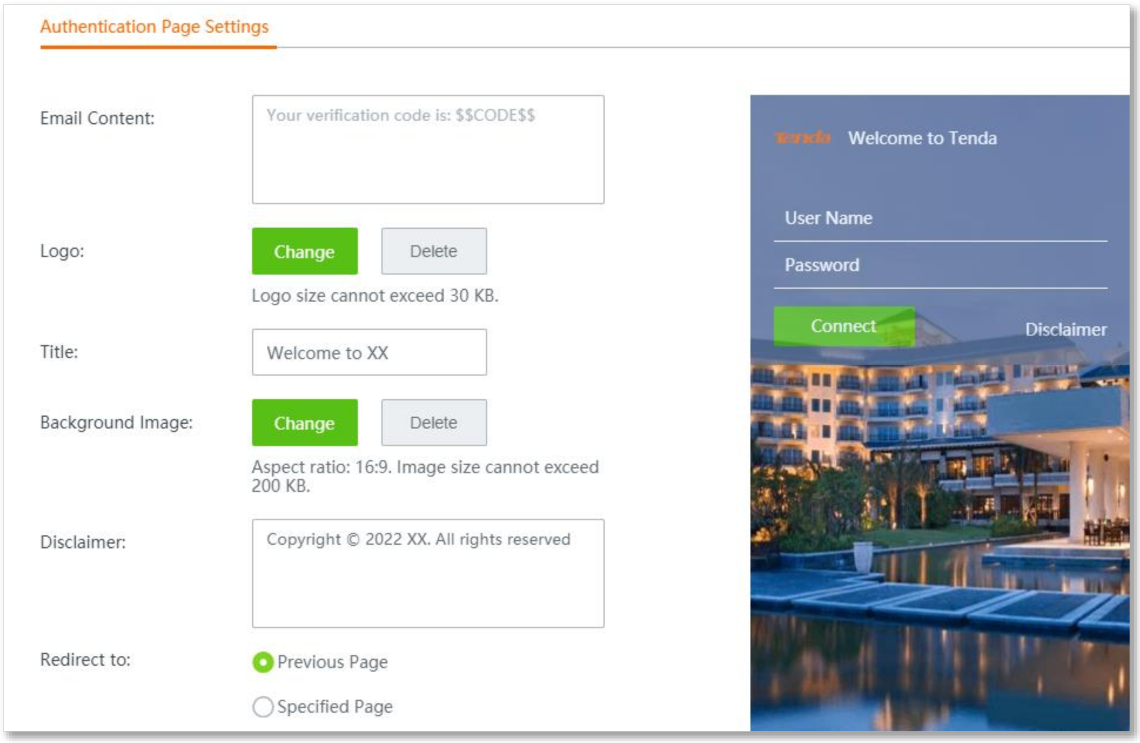
(2) Click **Change** and upload the company logo image.

(3) Set the title of the captive portal page, such as **Welcome to XX**.

(4) Click **Change** and upload the background image of the captive portal page, such as the enterprise promotion photo.

(5) Set the disclaimer information of the enterprise, such as **Copyright © 2022 XX. All rights reserved**.

(6) Select the **Previous Page** or enter a **Specified Page** as the page to which the users are redirected after passing the authentication.



Authentication Page Settings

Email Content: Your verification code is: $$CODE$$

Logo: Change Delete

Logo size cannot exceed 30 KB.

Title: Welcome to XX

Background Image: Change Delete

Aspect ratio: 16:9. Image size cannot exceed 200 KB.

Disclaimer: Copyright © 2022 XX. All rights reserved

Redirect to: ● Previous Page ○ Specified Page

----End

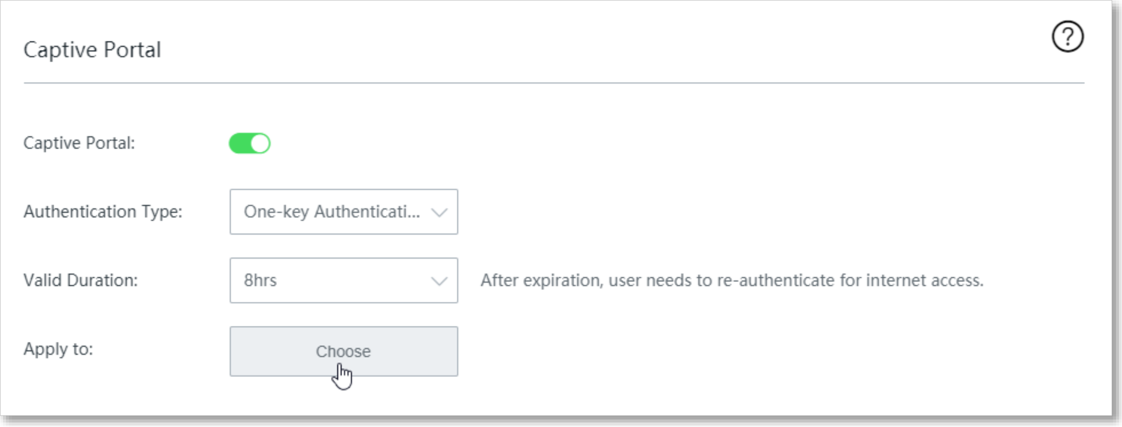
8.1.5 Configure one-key authentication

Step 1 Navigate to **Authentication** > **Captive Portal**.

Step 2 Enable **Captive Portal**.

Step 3 Configure the following parameters, then click **Save** at the bottom of the page.

1. Set **Authentication Type** to **One-key Authentication**.
2. Set the **Valid Duration**, such as **8 hrs**.
3. Click **Choose,** choose the network(s) to be applied, and click **Save**.



Captive Portal

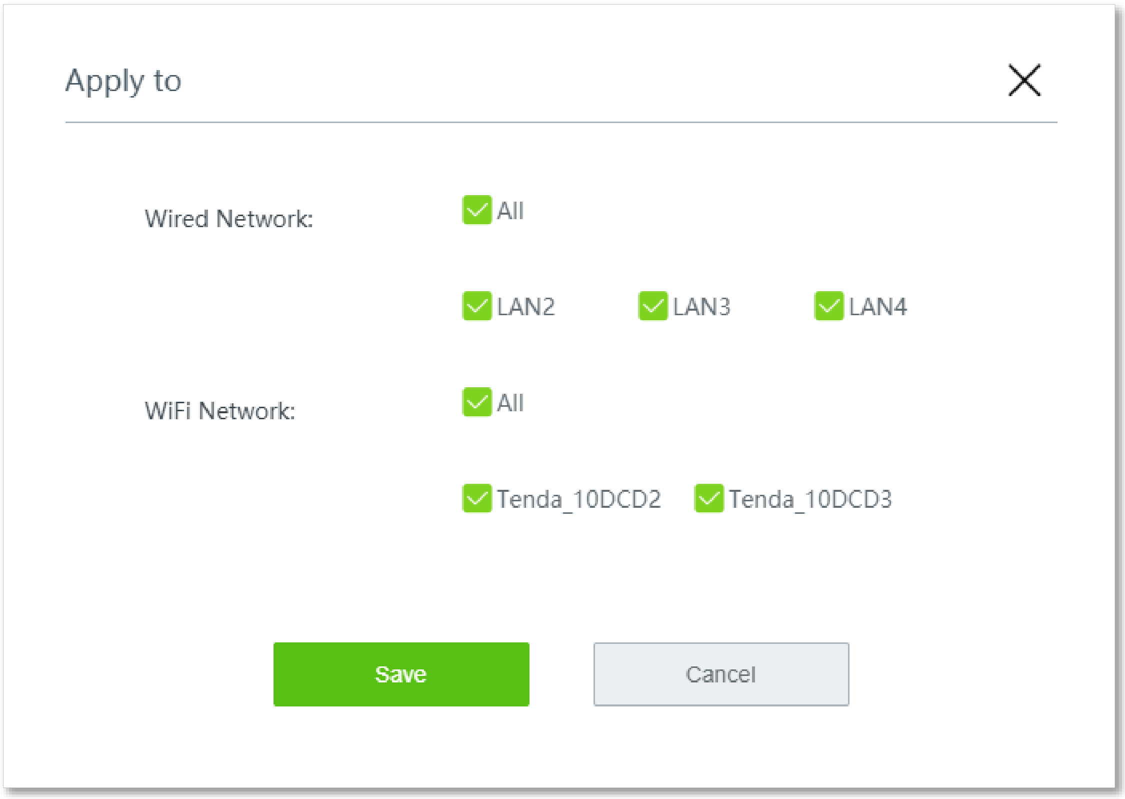
Captive Portal: ●

Authentication Type: One-key Authenticati...

Valid Duration: 8hrs

After expiration, user needs to re-authenticate for internet access.

Apply to:



Apply to

Wired Network: ☑ All

☑ LAN2 ☑ LAN3 ☑ LAN4

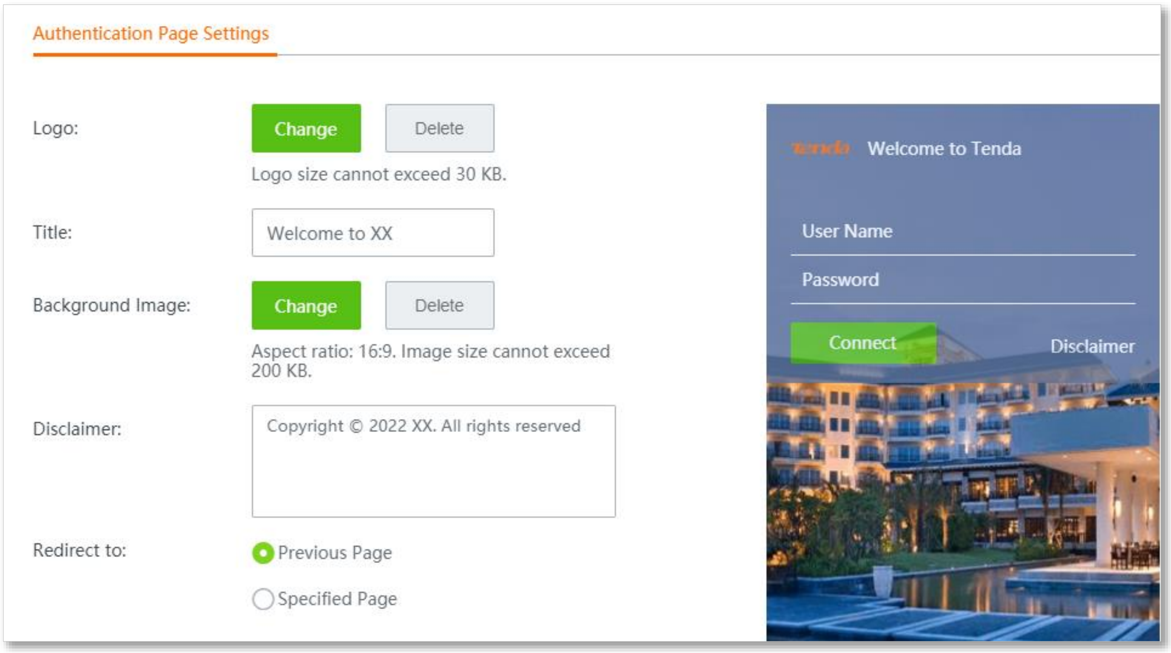
WiFi Network: ☑ All

☑ Tenda_10DCD2 ☑ Tenda_10DCD3

4. Configure the authentication page settings.
   (1) Click **Change** and upload the company logo image.
   (2) Set the title of the captive portal page, such as **Welcome to XX**.
   (3) Click **Change** and upload the background image of the captive portal page, such as the enterprise promotion photo.

(4) Set the disclaimer information of the enterprise, such as **Copyright © 2022 XX. All rights reserved**.

(5) Select the **Previous Page** or enter a **Specified Page** as the page to which the users are redirected after passing the authentication.



Authentication Page Settings

Logo: Change Delete

Logo size cannot exceed 30 KB.

Title: Welcome to XX

Background Image: Change Delete

Aspect ratio: 16:9. Image size cannot exceed 200 KB.

Disclaimer: Copyright © 2022 XX. All rights reserved

Redirect to: ● Previous Page ○ Specified Page

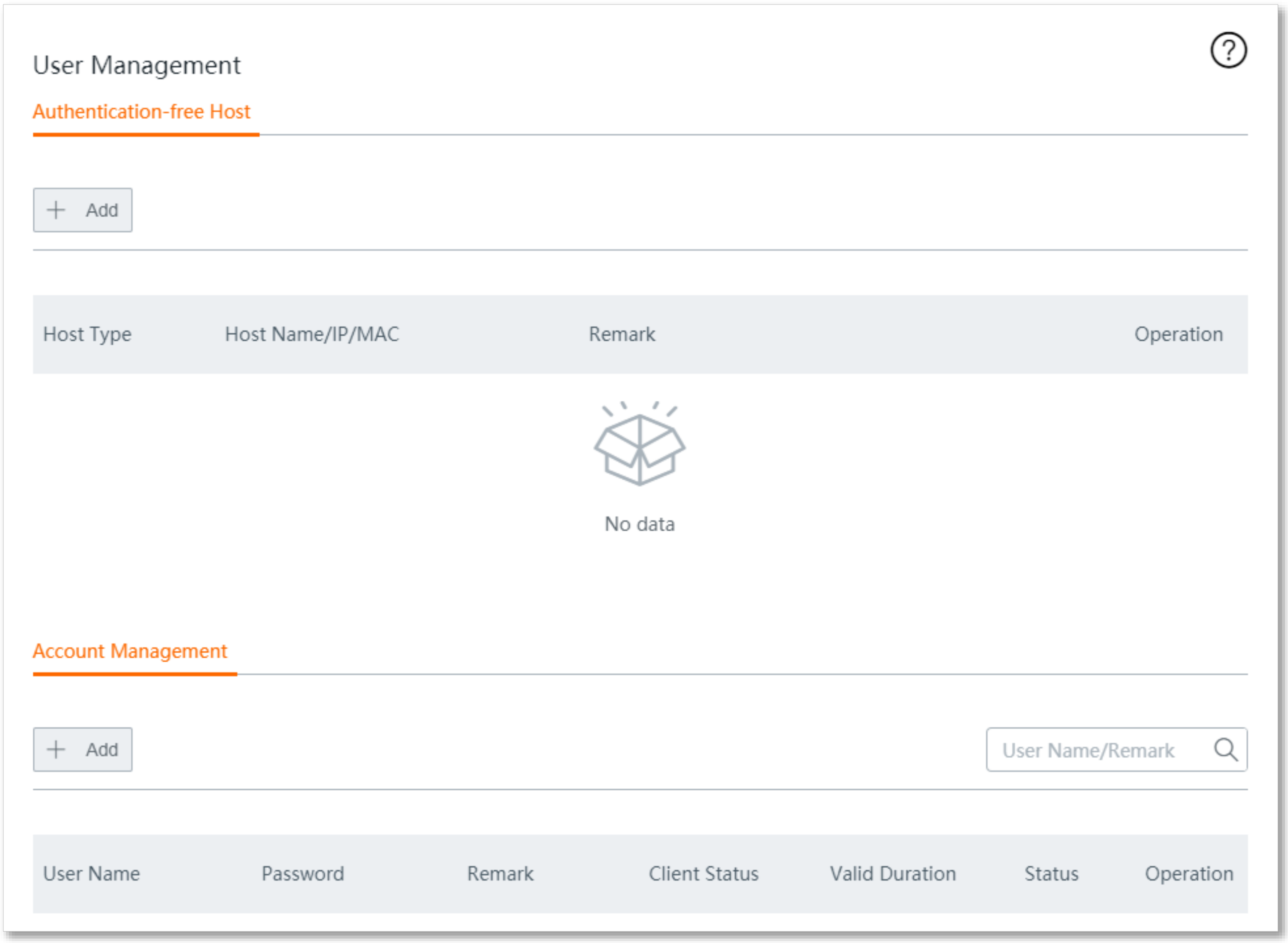
----End

8.2 User management

8.2.1 Overview

Click **Authentication** > **User Management** to enter the page.

Here, you can configure the user name and password for account authentication, export or import authentication account information, and add authentication-free hosts.



User Management

Authentication-free Host

＋ Add

Host Type	Host Name/IP/MAC	Remark	Operation

No data

Account Management

＋ Add

User Name/Remark

User Name	Password	Remark	Client Status	Valid Duration	Status	Operation

Parameter description

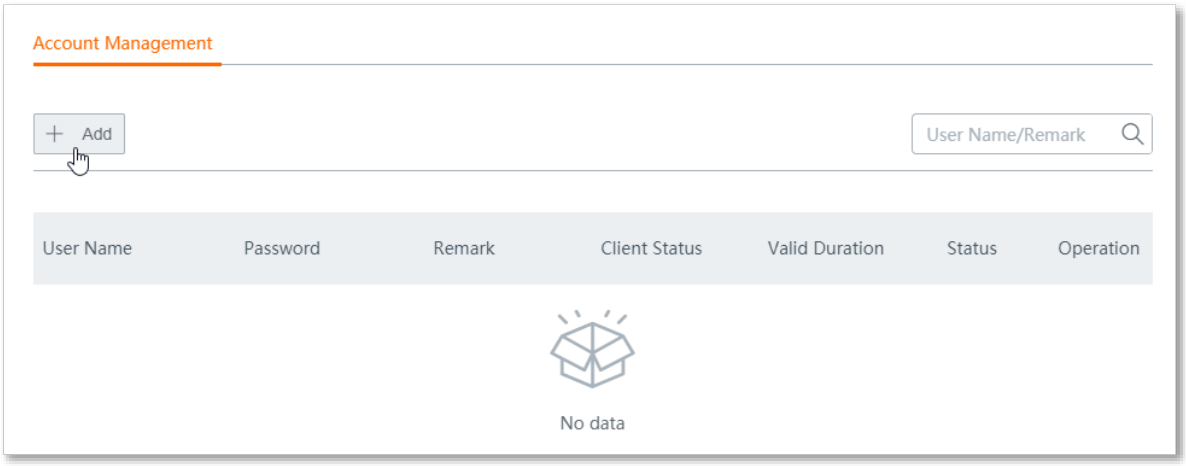
Parameter		Description
Authentication-free Host	Host Type	Specifies by which method you specify an authentication-free host. The router supports host name, IP address and MAC address.
	Host Name/IP /MAC	Specifies the information of the authentication-free host. ● If you select **Host Name**, enter the host name of the authentication-free device. Please fill in the host name on the **System Status** page. If the host name is modified, modify the host name here as well. ● If you select **IP Address**, enter the IP address of the authentication-free device. You are recommended to bind the IP address for the device on the Address Reservation page. ● If you select **MAC Address**, enter the MAC address of the authentication-free device.
	Remark	Specifies the description of the authentication-free device.

	Operation	Specifies the operations you can perform on the rule. ✎: Click it to edit the rule. 🗑 : Click it to delete the rule.
Account Management	User Name	Specifies the user name and password of the authentication account. After the account authentication function is enabled, users need to use this user name and password for authentication on the browser page before gaining internet access.
	Password	
	Remark	Specifies the account description information.
	Client Status	Specifies the status of the account (being used or not).
	Valid Duration	Specifies the valid duration of the account. After the duration expires, users cannot use this account for internet access authentication.
	Status	Specifies the status of the rule. You can enable it or disable it as needed.
	Operation	Specifies the operations you can perform on the rule. ✎: Click it to edit the rule. 🗑 : Click it to delete the rule.
	Export	Used to export the data of the configured authentication user account to the local computer.
	Import	Used to import the previously exported authentication user account data to the router.

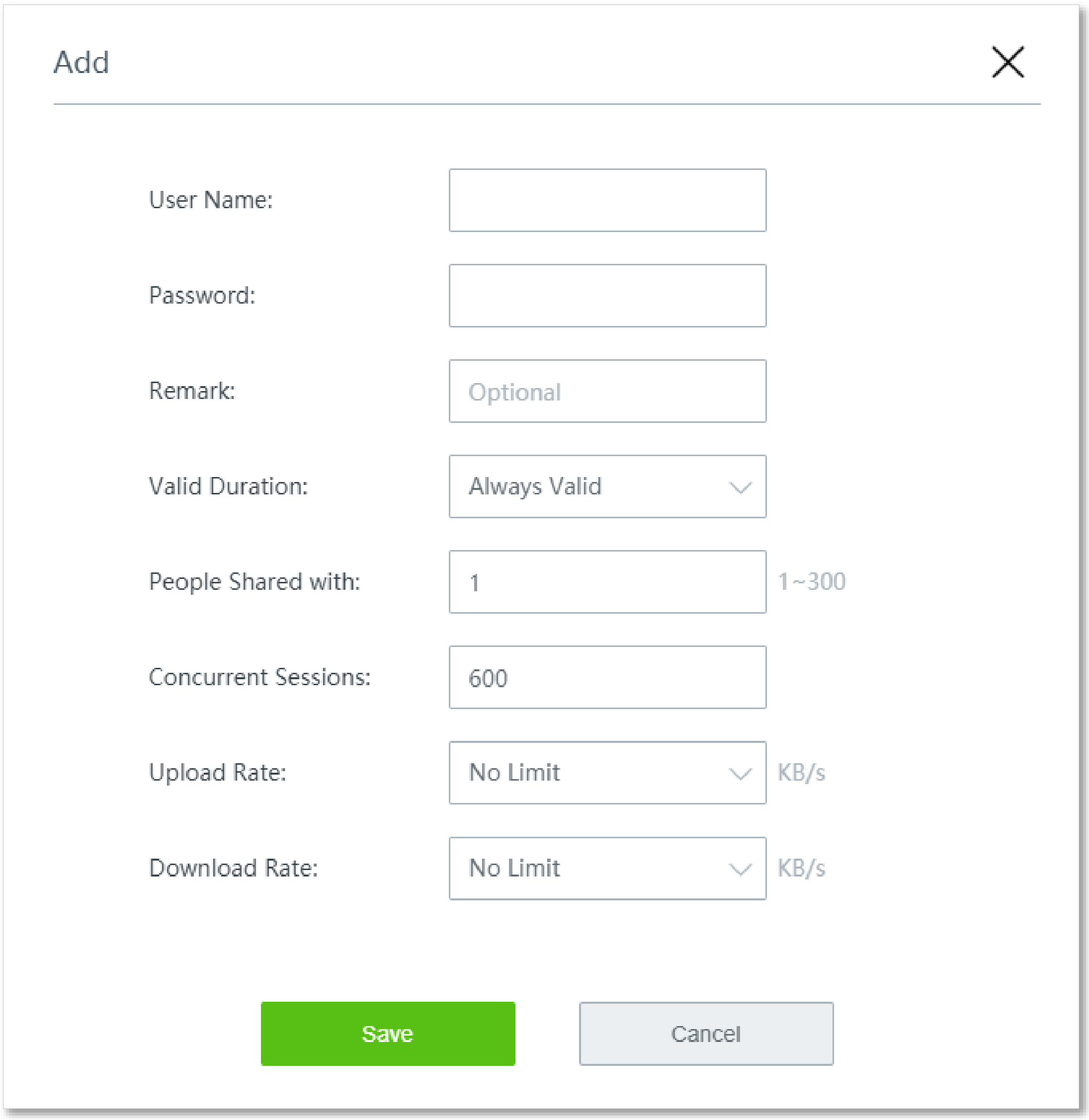
8.2.2 Add user accounts for local user authentication

Step 1 Navigate to **Authentication** > **User Management** > **Account Management**.

Step 2 Click **+Add**.



Step 3 Configure the following parameters, and click **Save**.



Add

User Name:	
Password:	
Remark:	Optional
Valid Duration:	Always Valid
People Shared with:	1 (1~300)
Concurrent Sessions:	600
Upload Rate:	No Limit KB/s
Download Rate:	No Limit KB/s

----End

Parameter description

Parameter	Description
People Shared with	Specifies the number of users allowed to access the internet using the same account.
Concurrent Sessions	Specifies the maximum number of connections that can be set up on each computer covered by the corresponding rule.
Upload Rate	Specifies the maximum upload/download rate of this account.
Download Rate	

8.3 Examples of configuring authentication

8.3.1 Example of configuring SMS authentication

Networking requirement

An enterprise wants to establish a network and regulate the use of the network with the router.

Requirements:

- SMS authentication is required for employees who want to access the internet through the LAN port of the router or the wireless network Tenda_10DCD2.
- Employees are directed to www.tendacn.com after being authenticated.
- The network administrator is free from authentication when accessing the internet.

Solution

The requirements can be achieved through the WiFi via SMS function of the router.

Assume that:

- The MAC address of the network administrator's computer is 44:37:E6:12:34:56.
- The user name applied by the enterprise in Jixintong is Tom123.
- The password of the account applied by the enterprise in Jixintong is Tommy456.

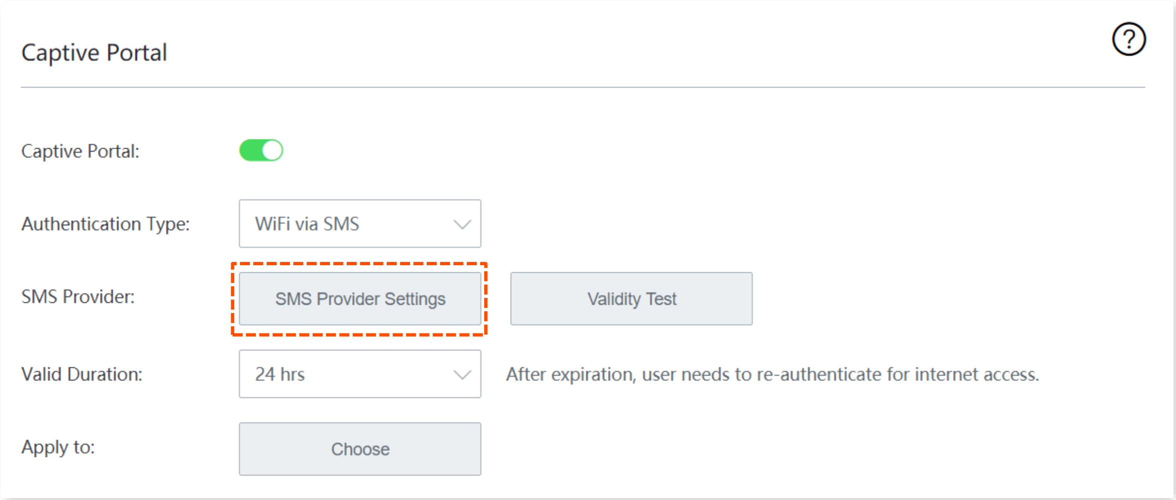
Configuration procedure

Step 1 Configure the SMS authentication settings.

1. Navigate to **Authentication** > **Captive Portal**.
2. Enable **Captive Portal**.
3. Configure the following parameters, and click **Save** at the bottom of the page.

   (1) Set **Authentication Type** to **WiFi via SMS**.

   (2) Click **SMS Provider Settings**, then the configuration window appears.



Captive Portal

Captive Portal: ●

Authentication Type: WiFi via SMS

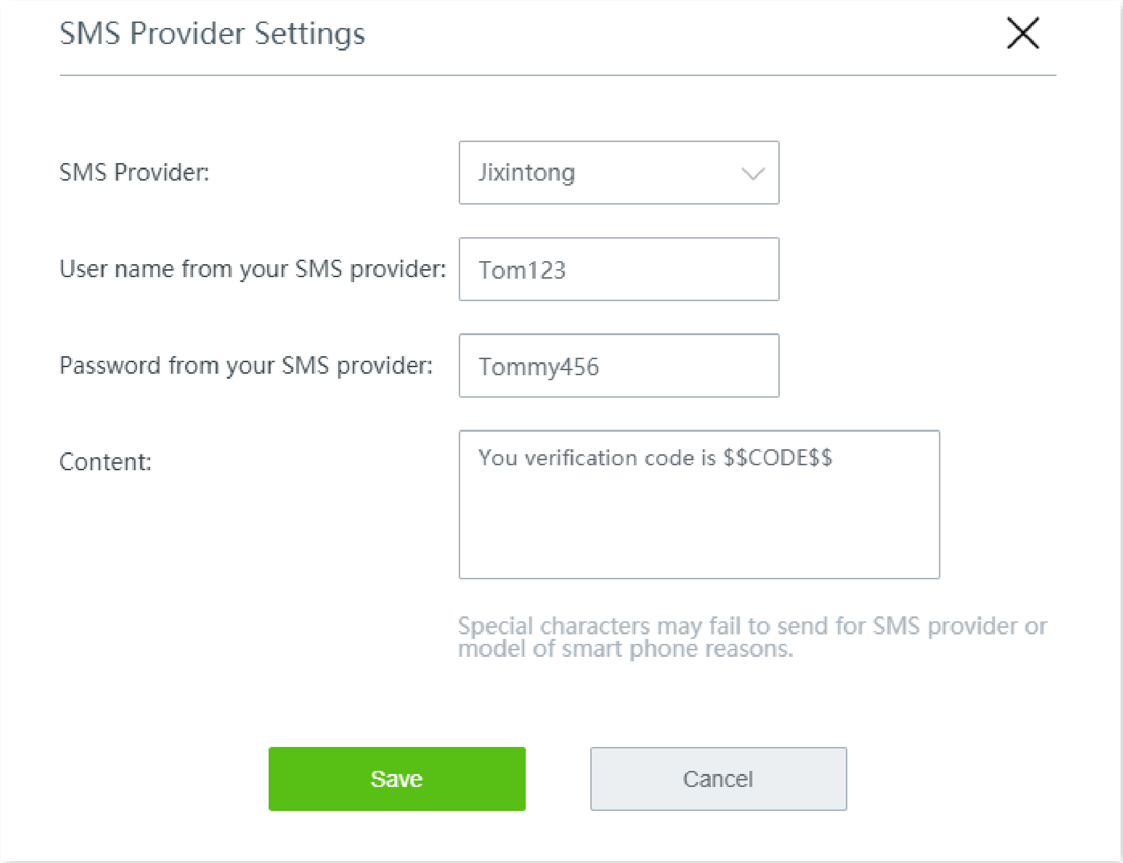
SMS Provider: SMS Provider Settings | Validity Test

Valid Duration: 24 hrs — After expiration, user needs to re-authenticate for internet access.

Apply to: Choose

(3) Configure the following parameters related to the SMS provider, and click **Save**.

- Select the **SMS provider** from which you have purchased an SMS package, such as **Jixintong**.
- Enter the **User name** and **Password from your SMS provider**, which are **Tom123** and **Tommy456** in this example.
- Customize the SMS **Content** sent to the user by the SMS platform for verification.



SMS Provider Settings

SMS Provider: Jixintong

User name from your SMS provider: Tom123

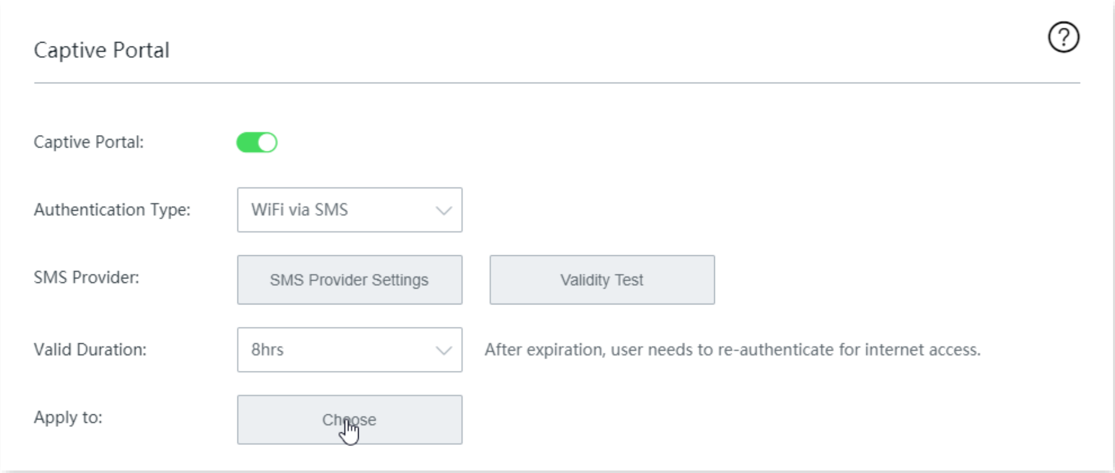
Password from your SMS provider: Tommy456

Content: You verification code is $$CODE$$

Special characters may fail to send for SMS provider or model of smart phone reasons.

(4) Set the **Valid Duration**, such as **8 hrs**.

(5) Click **Choose,** choose the network(s) to be applied, and click **Save**.

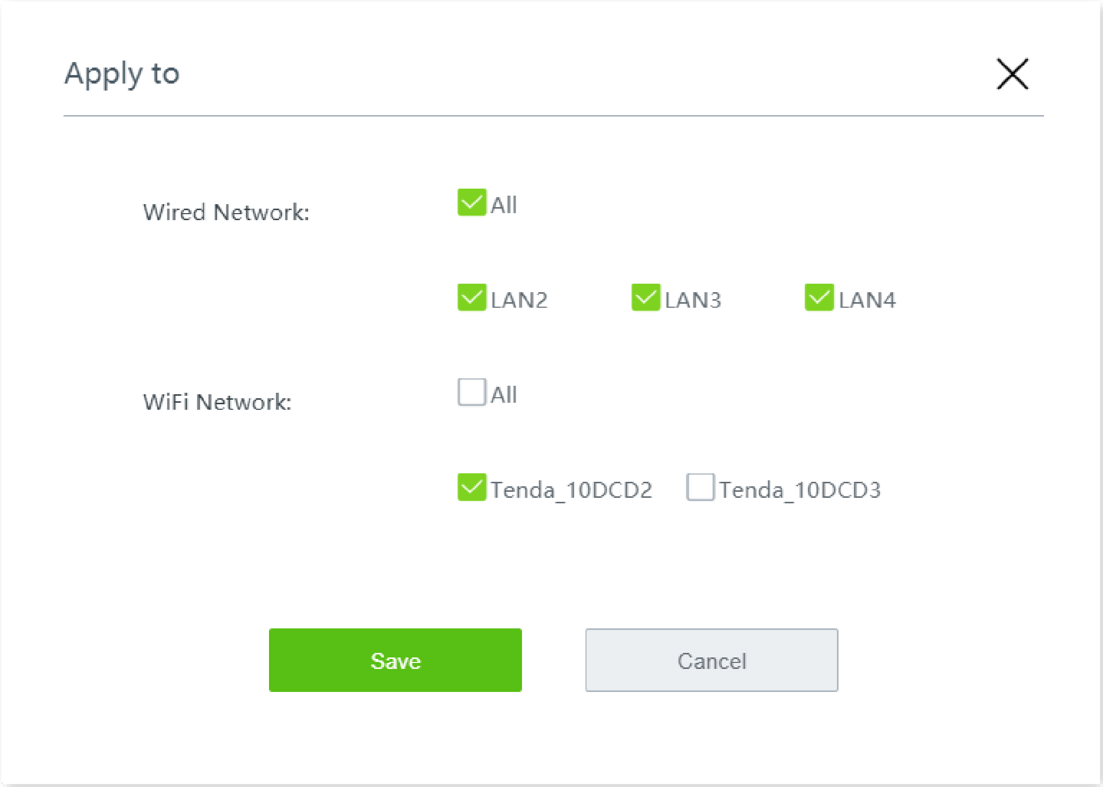


Captive Portal

Captive Portal: on

Authentication Type: WiFi via SMS

Valid Duration: 8hrs After expiration, user needs to re-authenticate for internet access.



Apply to

Wired Network: ☑ All

☑ LAN2 ☑ LAN3 ☑ LAN4

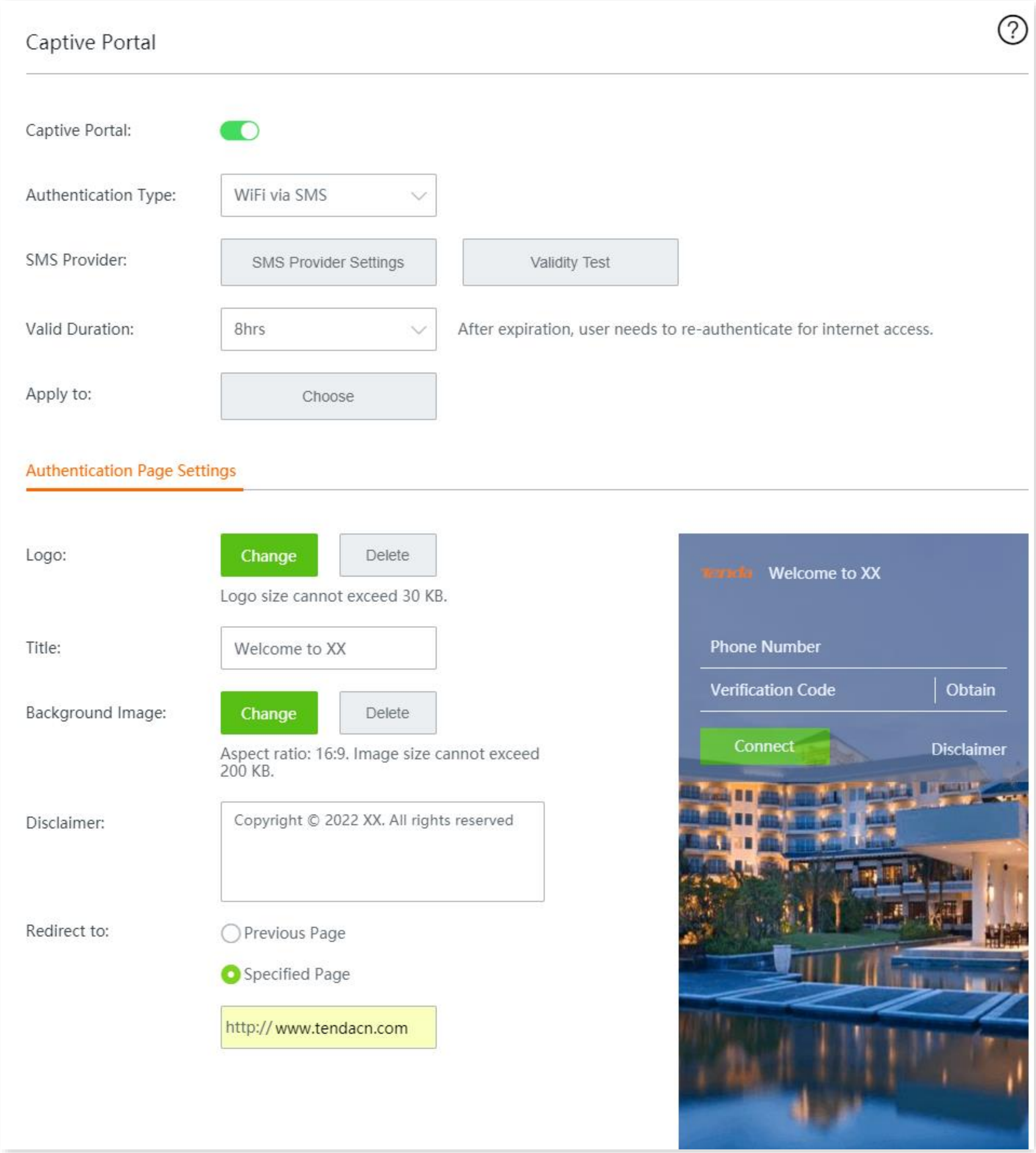
WiFi Network: □ All

☑ Tenda_10DCD2 □ Tenda_10DCD3

(6) Configure the authentication page settings.

- Click **Change** and upload the company logo image.
- Set the **Title** of the captive portal page, such as **Welcome to XX**.
- Click **Change** and upload the background image of the captive portal page, such as the enterprise promotion photo.
- Set the disclaimer information of the enterprise, such as **Copyright © 2022 XX. All rights reserved**.
- Enter the **Specified Page**, which is **www.tendacn.com** in this example.

The overall configuration of SMS authentication is shown as below.



Captive Portal

Captive Portal: ● (on)

Authentication Type: WiFi via SMS

SMS Provider: SMS Provider Settings | Validity Test

Valid Duration: 8hrs After expiration, user needs to re-authenticate for internet access.

Apply to: Choose

Authentication Page Settings

Logo: Change | Delete
Logo size cannot exceed 30 KB.

Title: Welcome to XX

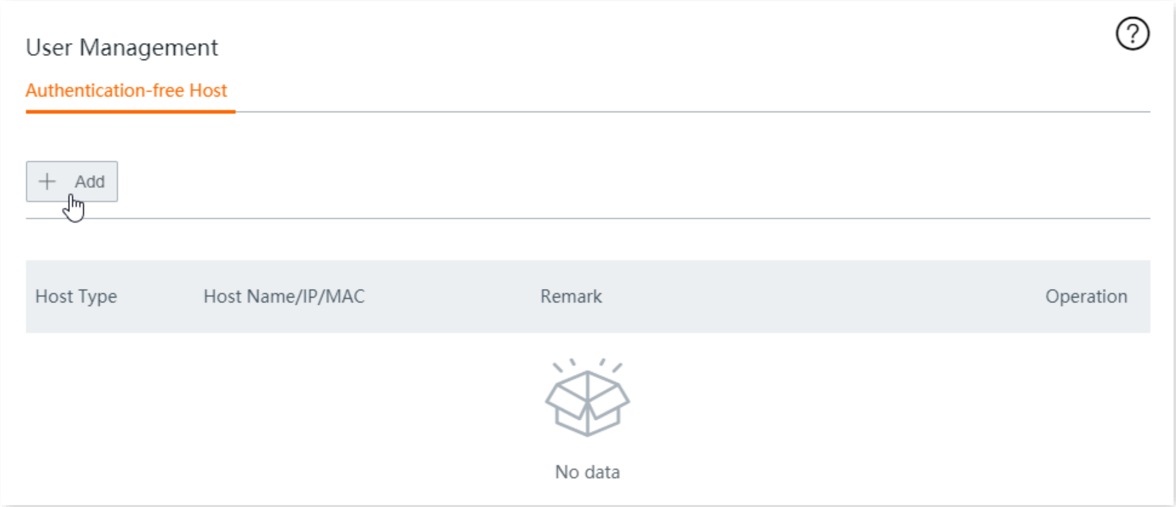
Background Image: Change | Delete
Aspect ratio: 16:9. Image size cannot exceed 200 KB.

Disclaimer: Copyright © 2022 XX. All rights reserved

Redirect to:
○ Previous Page
● Specified Page
http:// www.tendacn.com

Step 2 Add an authentication-free host.

1. Navigate to **Authentication** > **User Management**.
2. Click **+Add** in the **Authentication-free Host** module.

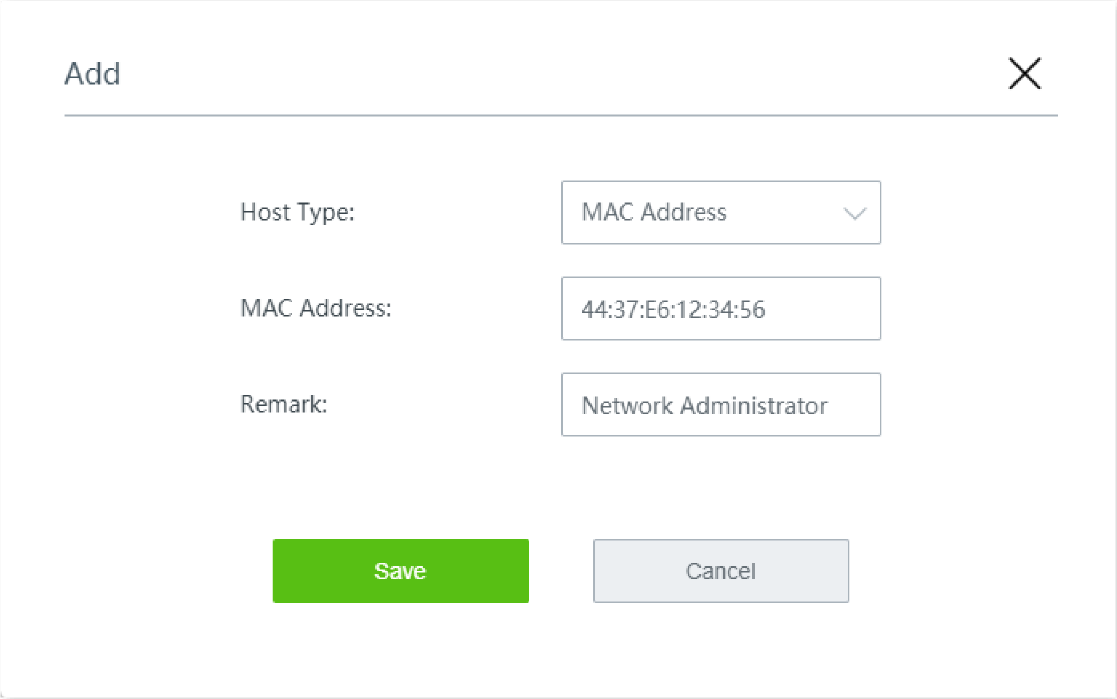


User Management

Authentication-free Host

Host Type	Host Name/IP/MAC	Remark	Operation

3. Configure the following parameters, then click **Save**.
   (1) Select **MAC Address** for **Host Type**.
   (2) Enter the **MAC Address**, which is **44:37:E6:12:34:56** in this example.
   (3) (Optional) Set a **Remark** for the host, which is **Network Administrator** in this example.



Add

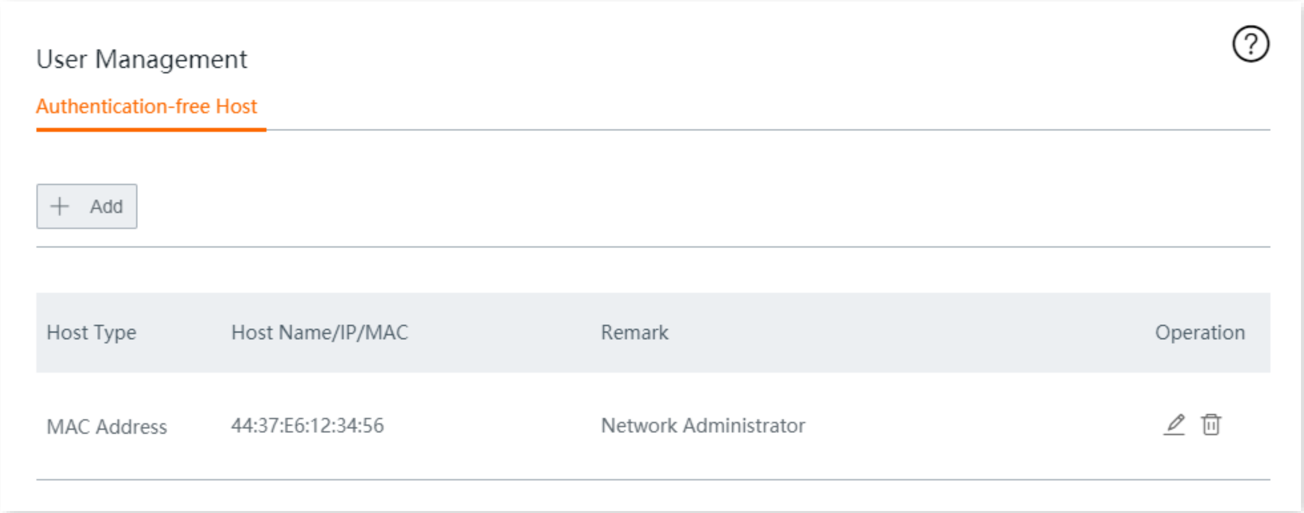
Host Type: MAC Address

MAC Address: 44:37:E6:12:34:56

Remark: Network Administrator

----End

Added successfully. See the following figure.



User Management

Authentication-free Host

Host Type	Host Name/IP/MAC	Remark	Operation
MAC Address	44:37:E6:12:34:56	Network Administrator	

Verification

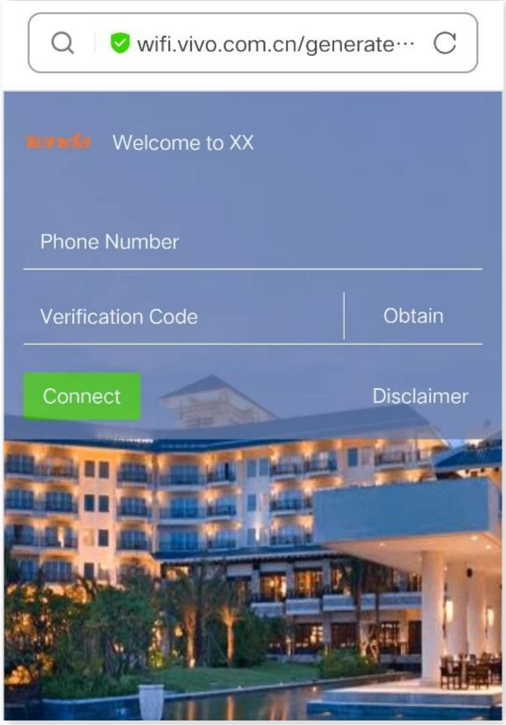
The network administrator can access the internet without authentication. Other employees have to perform SMS authentication as follows:

Step 1 Start a web browser and visit any website. The authentication page appears.

Step 2 Enter a valid phone number and tap **Obtain**.

Step 3 Enter the **Verification Code** in the SMS received.

Step 4 Tap **Connect**.



After successful authentication, the browser will automatically redirect to www.tendacn.com.

8.3.2 Example of configuring local user authentication

Networking requirement

An enterprise wants to establish a network and regulate the use of the network with the router.

Requirements:

- Local user authentication with user name and password is required for employees who want to access the internet through the LAN port of the router or the wireless network Tenda_10DCD2.
- No upload or download rate limit is specified for employees.
- Employees are directed to www.tendacn.com after being authenticated.
- The network administrator is free from authentication when accessing the internet.

Solution

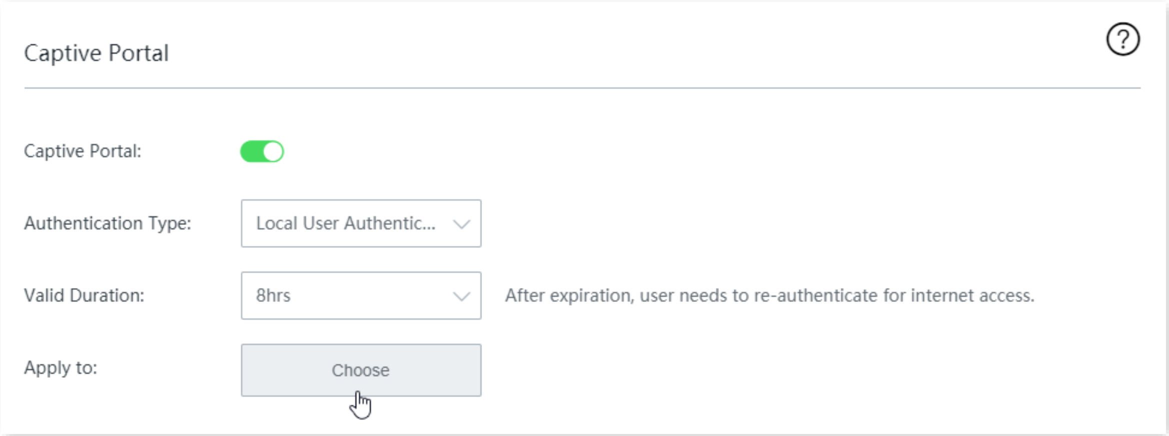
The requirements can be achieved through the local user authentication function of the router.

Assume that the MAC address of the network administrator's computer is 44:37:E6:12:34:56.

Configuration procedure

Step 1 Configure the local user authentication settings.

1. Navigate to **Authentication** > **Captive Portal**.
2. Enable **Captive Portal**.
3. Configure the following parameters, then click **Save** at the bottom of the page.
   (1) Set **Authentication Type** to **Local User Authentication**.
   (2) Set the **Valid Duration**, such as **8 hrs**.
   (3) Click **Choose,** choose the network(s) to be applied, and click **Save**.



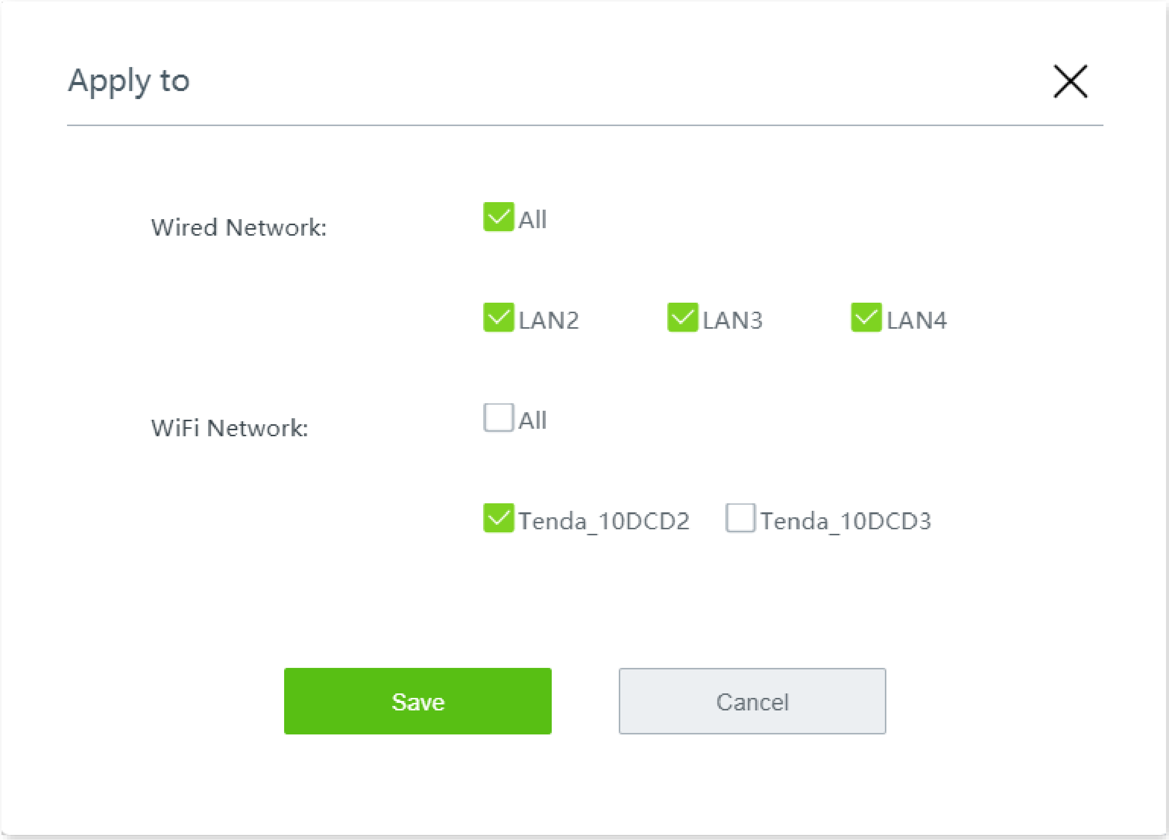
Captive Portal

Captive Portal: ●

Authentication Type: Local User Authentic...

Valid Duration: 8hrs After expiration, user needs to re-authenticate for internet access.

Apply to:



Apply to

Wired Network: ☑ All

☑ LAN2 ☑ LAN3 ☑ LAN4

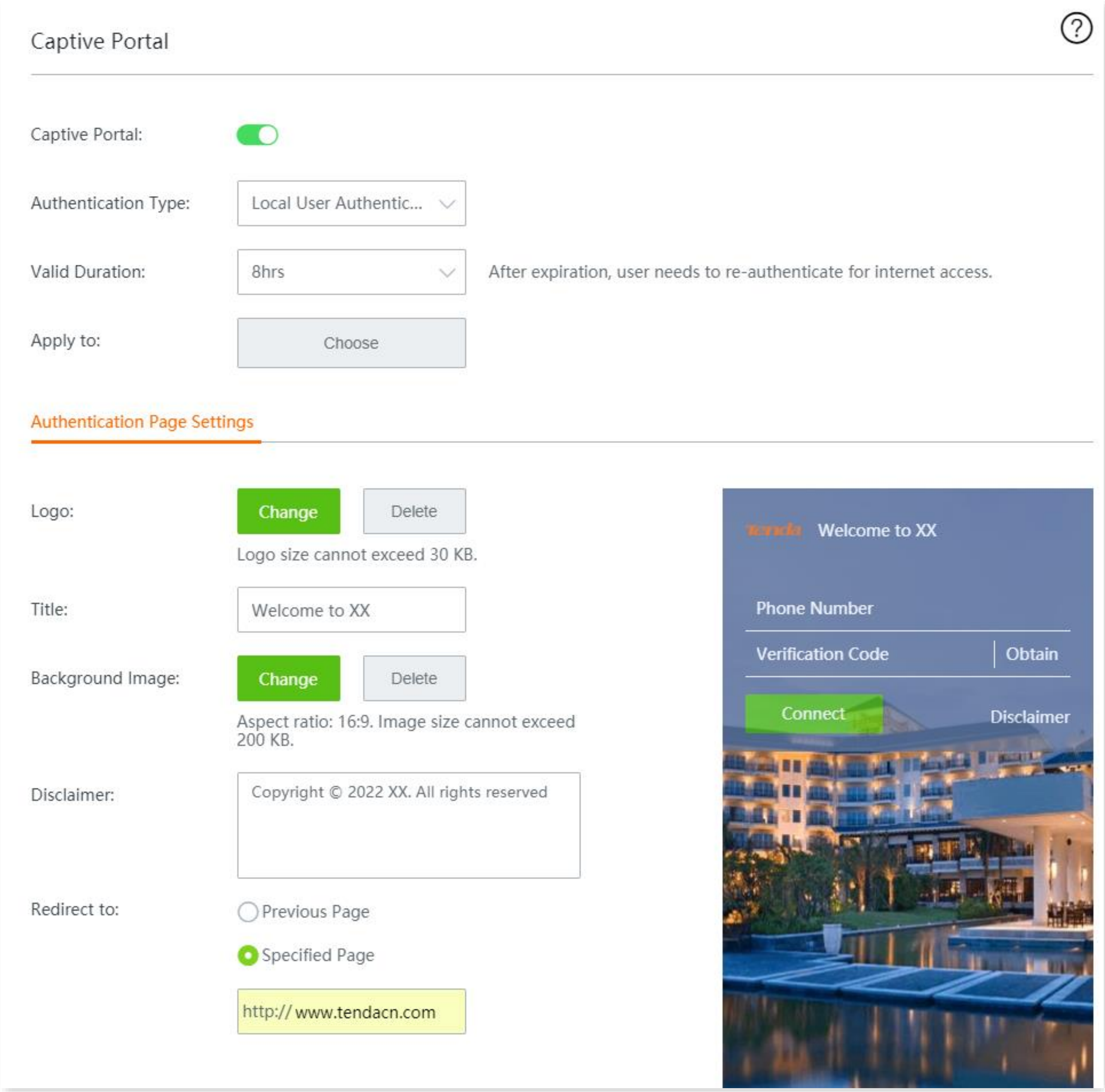
WiFi Network: □ All

☑ Tenda_10DCD2 □ Tenda_10DCD3

(4) Configure the authentication page settings.

- Click **Change** and upload the company logo image.
- Set the **Title** of the captive portal page, such as **Welcome to XX**.
- Click **Change** and upload the background image of the captive portal page, such as the enterprise promotion photo.
- Set the disclaimer information of the enterprise, such as **Copyright © 2022 XX. All rights reserved**.
- Enter the **Specified Page**, which is **www.tendacn.com** in this example.

The overall configuration of local user authentication is shown as below.



Captive Portal

Captive Portal: ●

Authentication Type: Local User Authentic...

Valid Duration: 8hrs — After expiration, user needs to re-authenticate for internet access.

Apply to: Choose

Authentication Page Settings

Logo: Change Delete

Logo size cannot exceed 30 KB.

Title: Welcome to XX

Background Image: Change Delete

Aspect ratio: 16:9. Image size cannot exceed 200 KB.

Disclaimer: Copyright © 2022 XX. All rights reserved

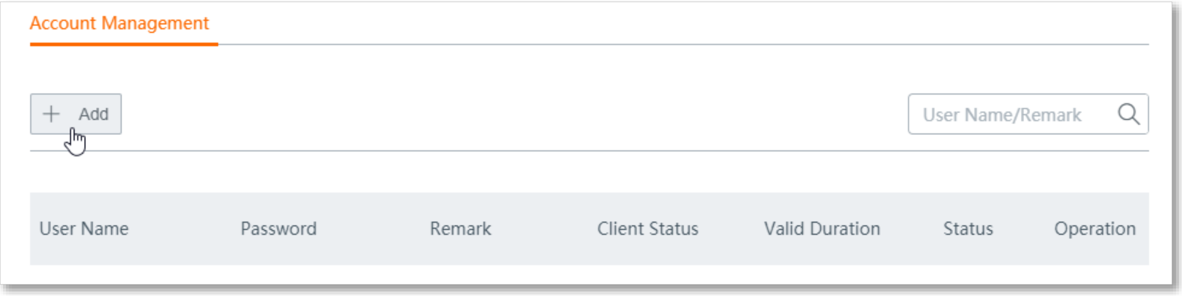
Redirect to: ○ Previous Page ● Specified Page

http:// www.tendacn.com

Step 2 Add local user authentication account(s).

1. Navigate to **Authentication** > **User Management** > **Account Management**.

2. Click **+Add**.



User Name	Password	Remark	Client Status	Valid Duration	Status	Operation

3. Configure the following parameters, and click **Save**.

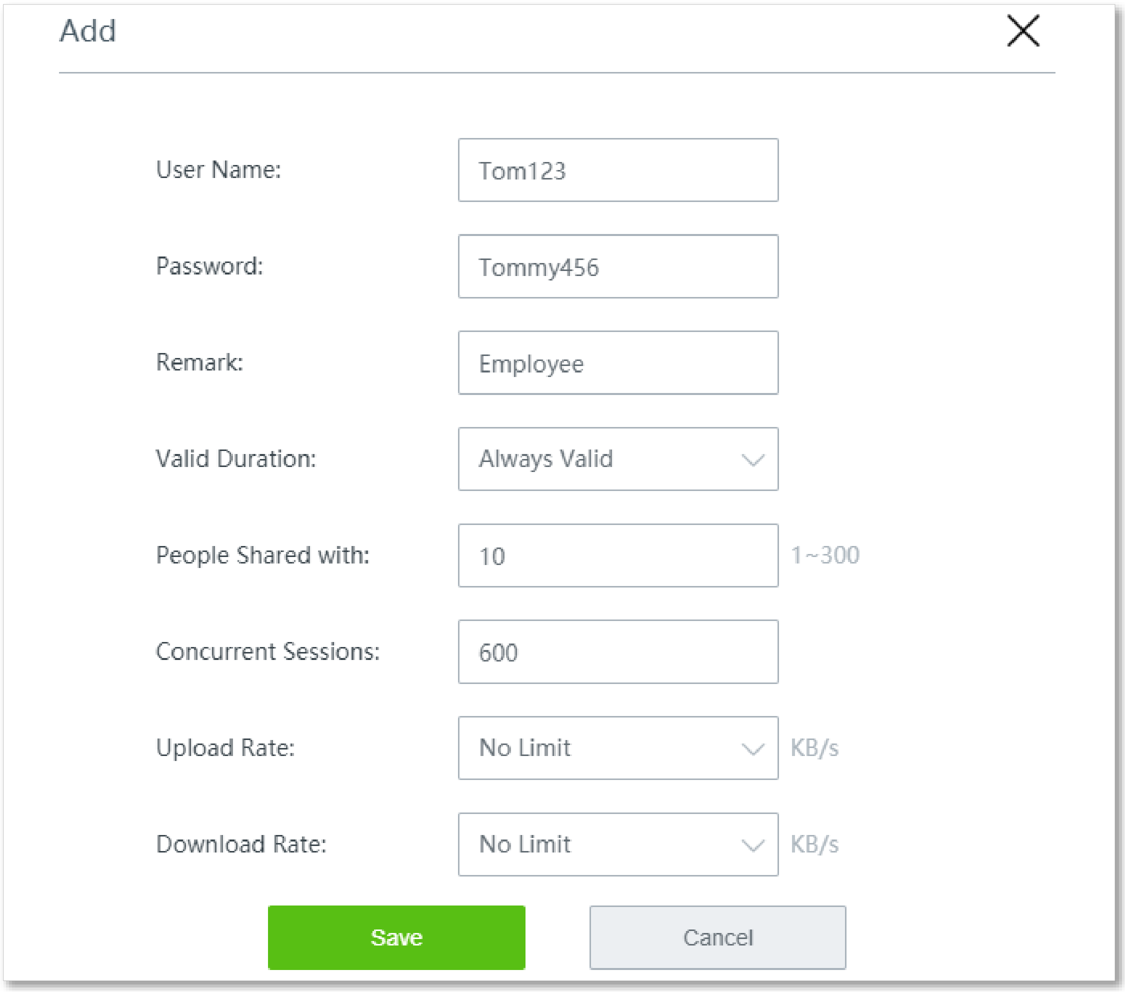
(1) Set the **User name** and **Password** for authentication, such as **Tom123 and Tommy456**.

(2) (Optional) Set a **Remark** for the user, such as **Employee**.

(3) Set **Valid Duration** to **Always valid**.

(4) Set **People Shared with** to **10**.

(5) Set the **Concurrent Sessions** established by the account device. You are recommended to keep the default settings.



User Name: Tom123

Password: Tommy456

Remark: Employee

Valid Duration: Always Valid

People Shared with: 10 1~300

Concurrent Sessions: 600

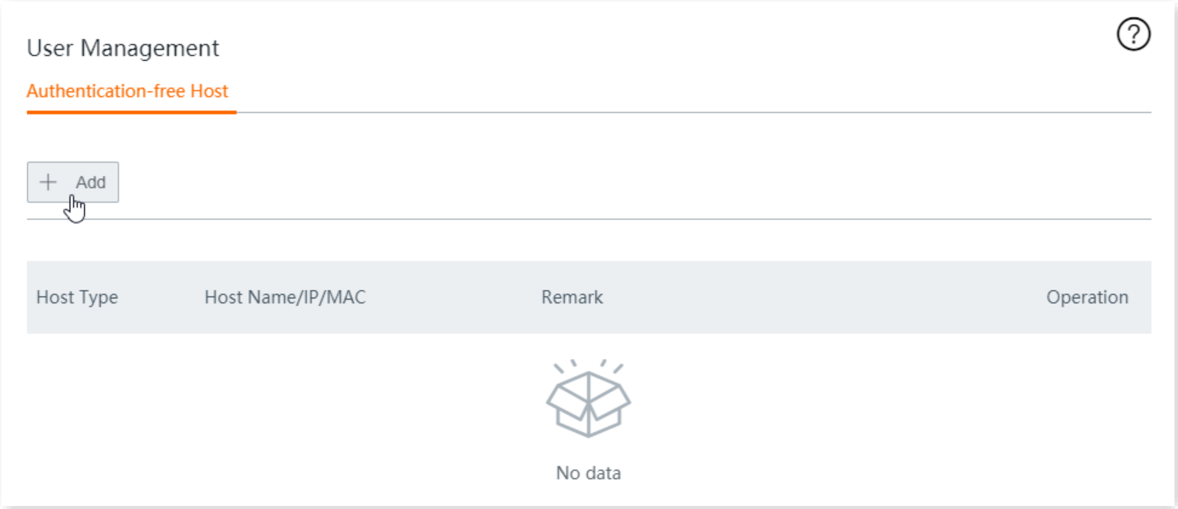
Upload Rate: No Limit KB/s

Download Rate: No Limit KB/s

Step 3 Add an authentication-free host.

1. Navigate to **Authentication** > **User Management**.

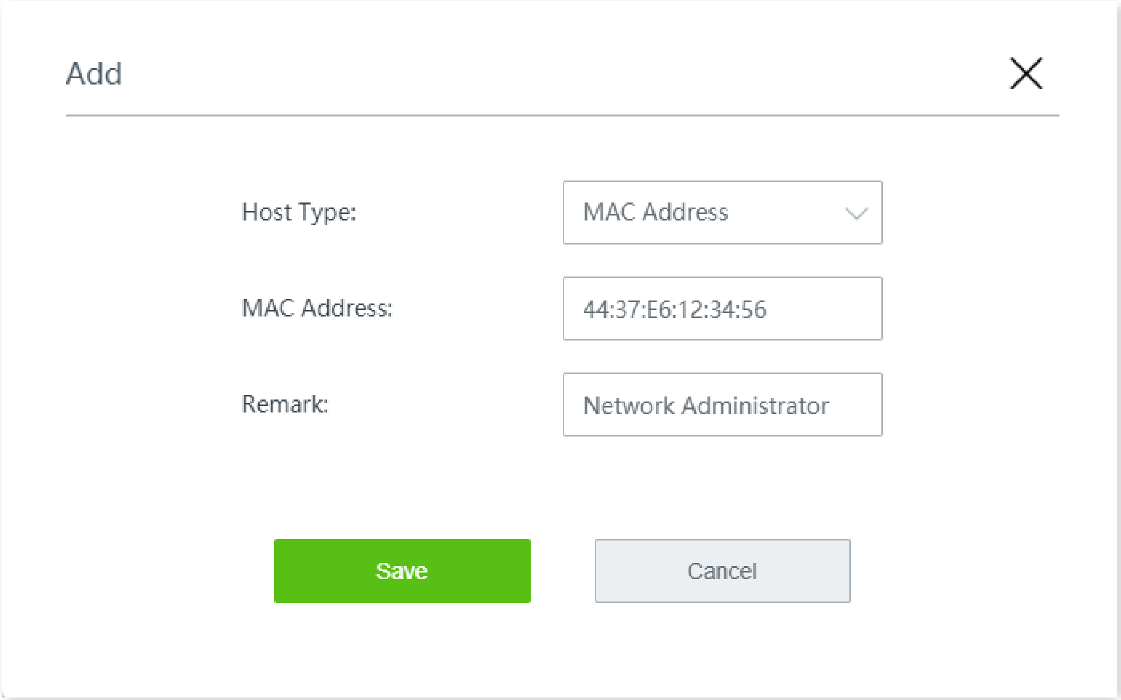
2. Click **+Add** in the **Authentication-free Host** module.



User Management

Authentication-free Host

3. Configure the following parameters, then click **Save**.
   (1) Select **MAC Address** for **Host Type**.
   (2) Enter the **MAC Address**, which is **44:37:E6:12:34:56** in this example.
   (3) (Optional) Set a **Remark** for the host, which is **Network Administrator** in this example.



Add

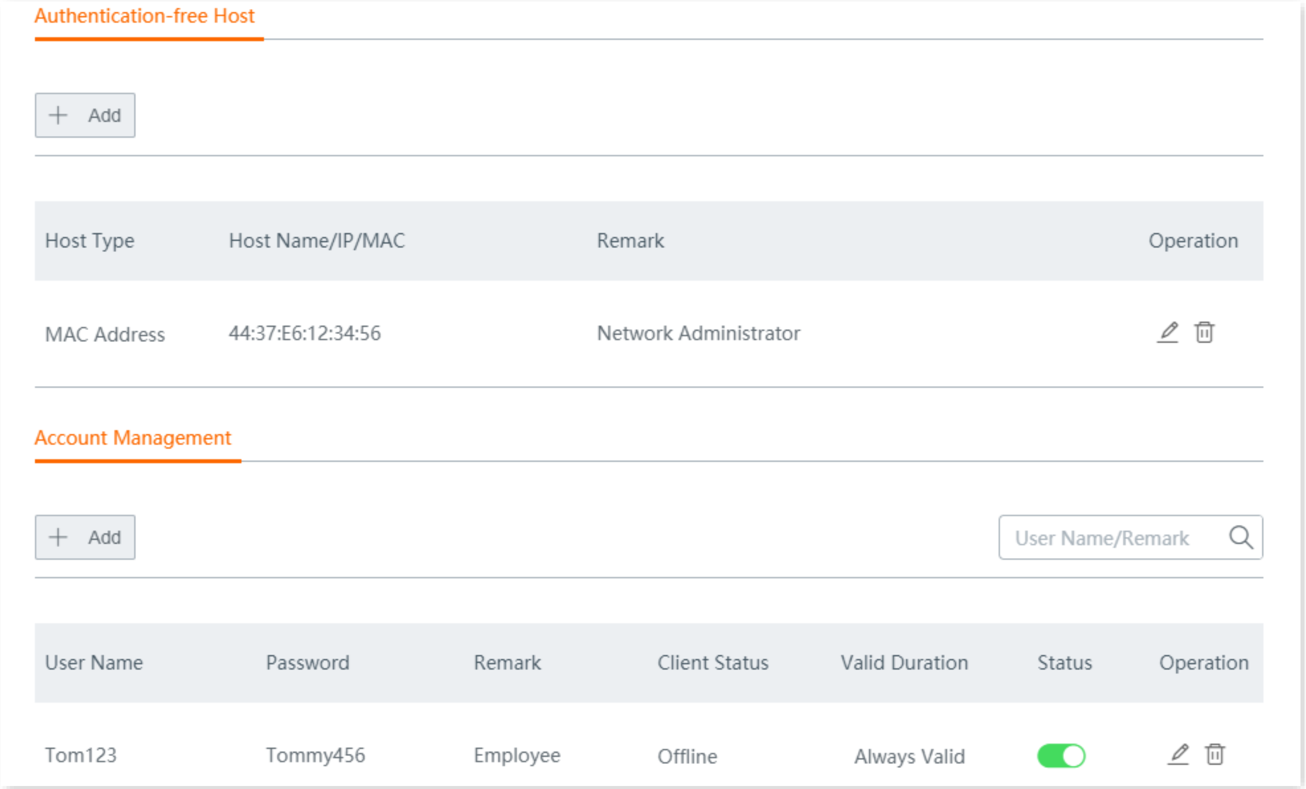
Host Type: MAC Address

MAC Address: 44:37:E6:12:34:56

Remark: Network Administrator

----End

Added successfully. See the following figure.



Authentication-free Host

+ Add

Host Type	Host Name/IP/MAC	Remark	Operation
MAC Address	44:37:E6:12:34:56	Network Administrator	✎ 🗑

Account Management

+ Add

User Name/Remark

User Name	Password	Remark	Client Status	Valid Duration	Status	Operation
Tom123	Tommy456	Employee	Offline	Always Valid	●	✎ 🗑

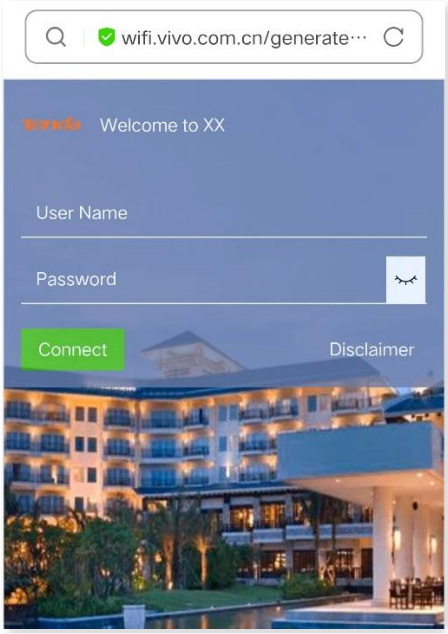
Verification

The network administrator can access the internet without authentication. Other employees have to perform local user authentication as follows:

Step 1 Start a web browser and visit any website. The authentication page appears.

Step 2 Enter the correct **User Name** and **Password**.

Step 3 Tap **Connect**.



After successful authentication, the browser will automatically redirect to www.tendacn.com.

8.3.3 Example of configuring email authentication

Networking requirement

An enterprise wants to establish a network and regulate the use of the network with the router.

Requirements:

- Email authentication is required for employees who want to access the internet through the LAN port of the router or the wireless network Tenda_10DCD2.
- No upload or download rate limit is specified for employees.
- Employees are directed to www.tendacn.com after being authenticated.
- The network administrator is free from authentication when accessing the internet.

Solution

The requirements can be achieved through the email authentication function of the router.

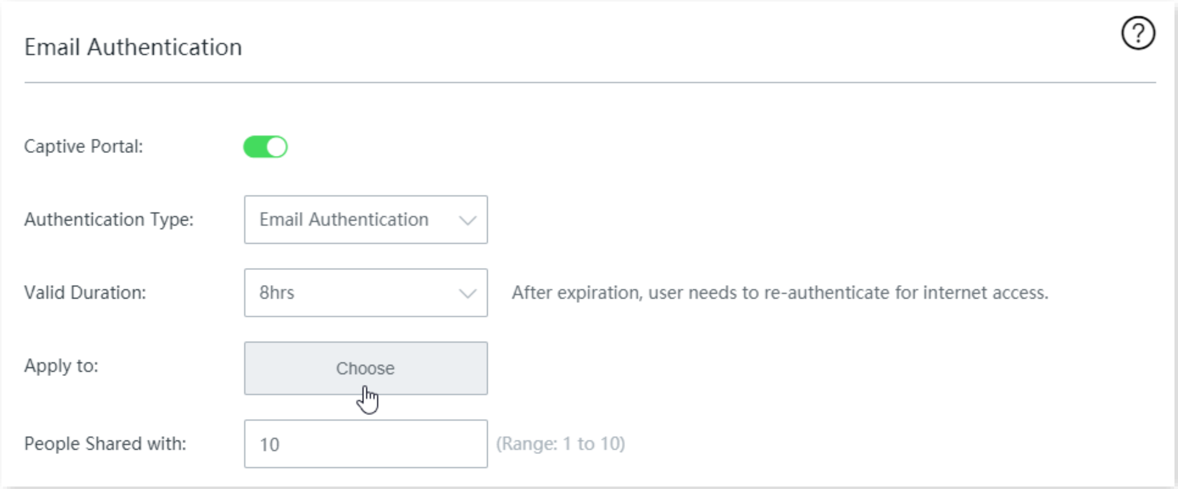
Assume the MAC address of the network administrator's computer is 44:37:E6:12:34:56, and the parameters of the email server are as follows:

- Email Address: Tom@gmail.com
- Email Password: Tom159357
- SMTP Server: smtp.gmail.com (SSL enabled)
- SMTP Server Port: 465
- Account for Test: lisi@gmail.com

Configuration procedure

Step 1 Configure the local user authentication settings.

1. Navigate to **Authentication** > **Captive Portal**.
2. Enable **Captive Portal**.
3. Configure the following parameters.
   (1) Set **Authentication Type** to **Email Authentication**.
   (2) Set the **Valid Duration**, such as **8 hrs**.
   (3) Set the **People Shared with** (the number of users allowed to connect to the internet using the email at the same time), which is **10** in this example.
   (4) Click **Choose,** choose the network(s) to be applied, and click **Save**.



Email Authentication

Captive Portal: ●

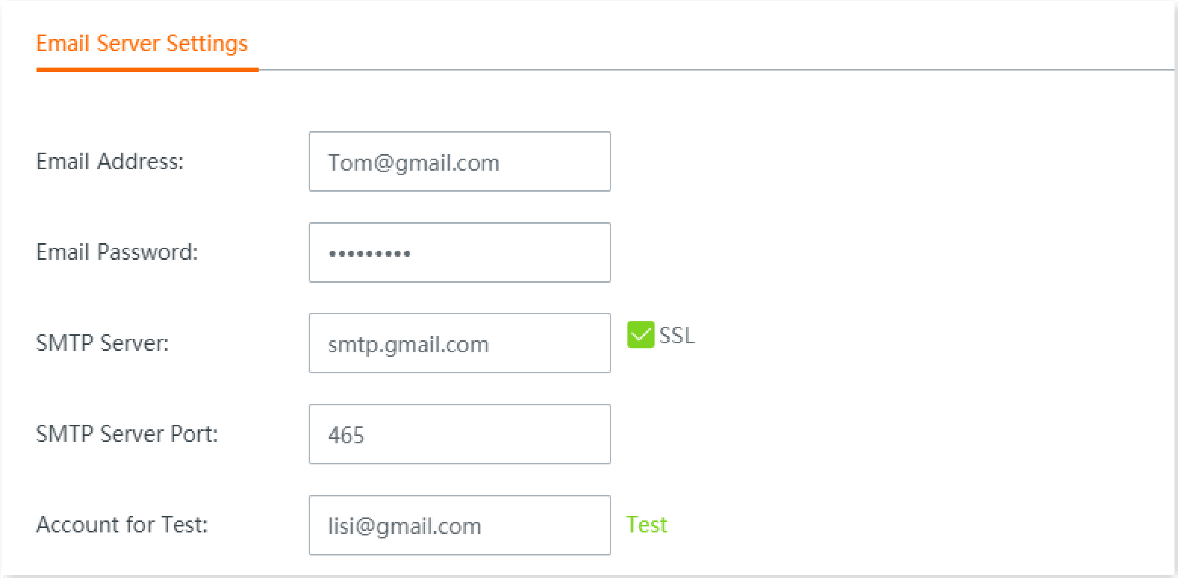
Authentication Type: Email Authentication

Valid Duration: 8hrs After expiration, user needs to re-authenticate for internet access.

Apply to: Choose

People Shared with: 10 (Range: 1 to 10)

4. Configure the email server settings.
   (1) Set **Email Address** to **Tom@gmail.com**.
   (2) Set **Email Password** to **Tom159357**.
   (3) Set **SMTP Server** to **smtp.gmail.com**.
   (4) Tick **SSL**.
   (5) Set **SMTP Server Port** to **465**.
   (6) Enter another email address in **Account for Test**, which is **lisi@gmail.com** in this example.



Email Server Settings

Email Address: Tom@gmail.com

Email Password: •••••••••

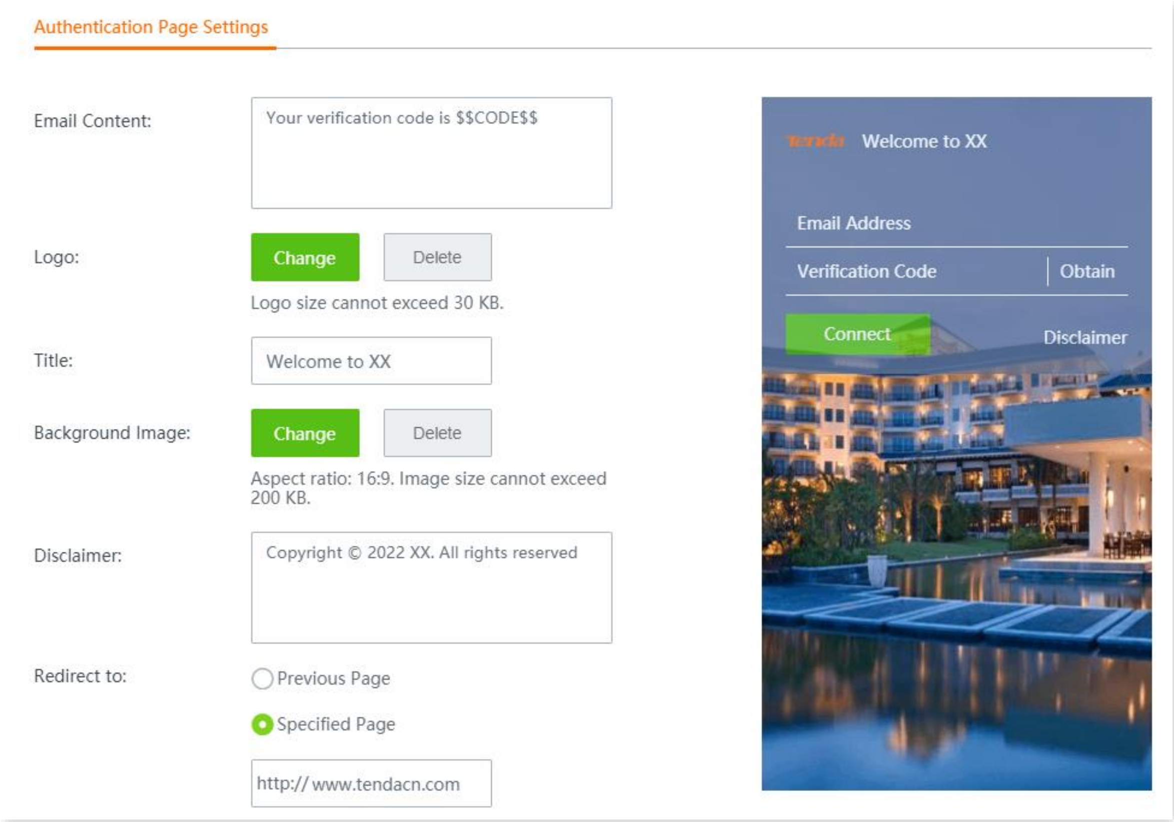
SMTP Server: smtp.gmail.com ☑ SSL

SMTP Server Port: 465

Account for Test: lisi@gmail.com Test

5. Configure the authentication page settings.
   (1) Set the **Email Content** sent to users ("$$CODE$$" is the format of the email verification code and cannot be modified).
   (2) Click **Change** to upload a logo image.
   (3) Set the **Title** of the captive portal page, such as **Welcome to XX**.
   (4) Click **Change** to upload a background image.
   (5) Set the disclaimer information of the enterprise, such as **Copyright © 2022 XX. All rights reserved**.
   (6) Enter the **Specified Page**, which is **www.tendacn.com** in this example.

6. Click **Save** at the bottom of the page.



Authentication Page Settings

Email Content: Your verification code is $$CODE$$

Logo: Change Delete

Logo size cannot exceed 30 KB.

Title: Welcome to XX

Background Image: Change Delete

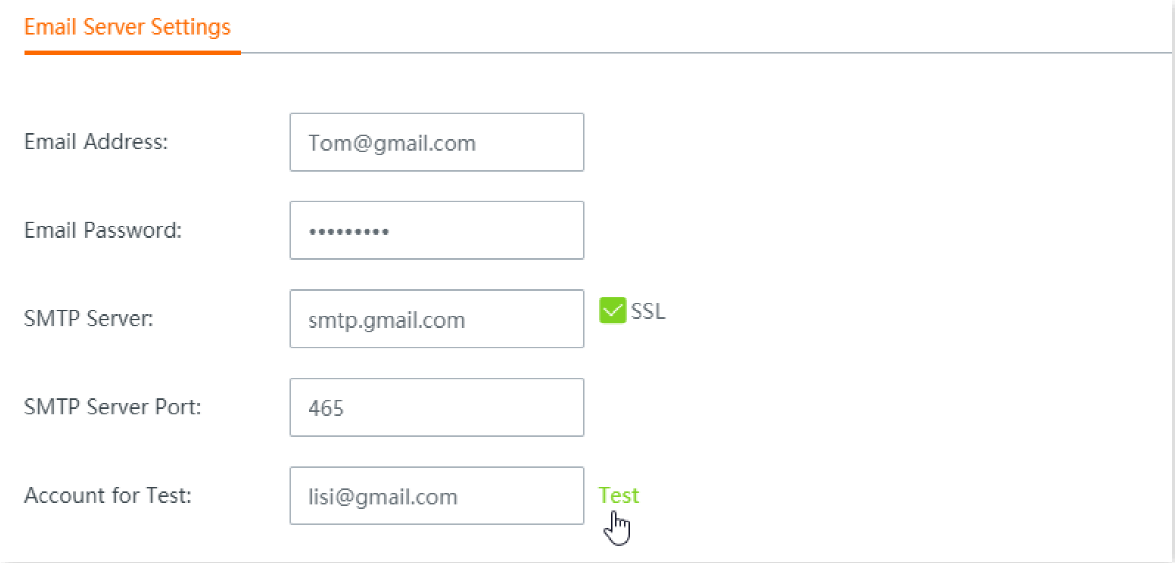
Aspect ratio: 16:9. Image size cannot exceed 200 KB.

Disclaimer: Copyright © 2022 XX. All rights reserved

Redirect to: ○ Previous Page ● Specified Page

http:// www.tendacn.com

7. Click **Test** in the **Email Server Settings** module, you can check whether the configuration of email server is correct.



Email Server Settings

Email Address: Tom@gmail.com

Email Password: •••••••••

SMTP Server: smtp.gmail.com ☑ SSL

SMTP Server Port: 465

Account for Test: lisi@gmail.com Test

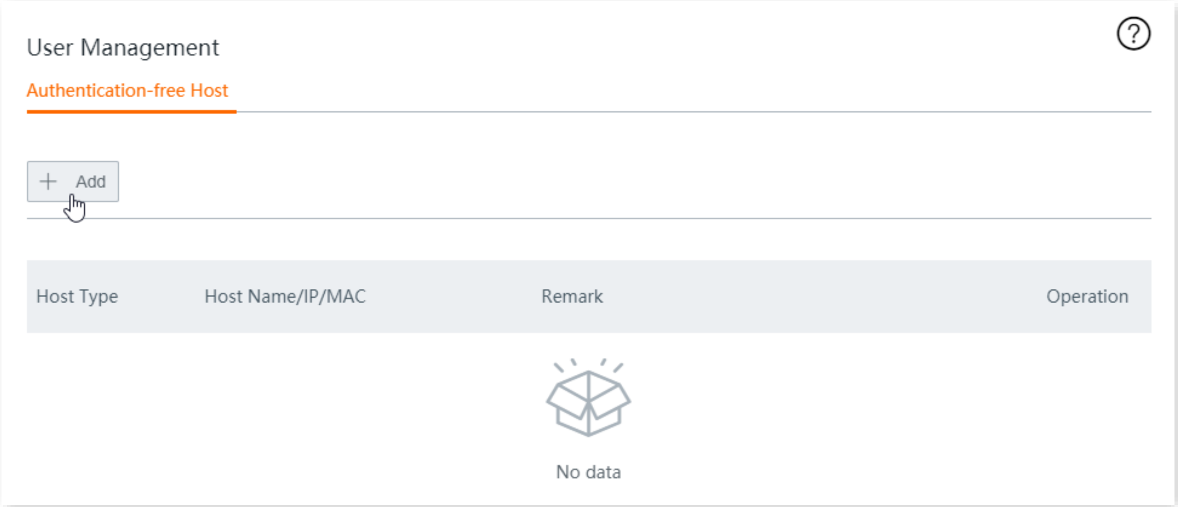
TIP

If the test fails, try the following solutions:

- Check if the SMTP service is enabled for the **Email Address**.
- Check if the **Account for Test** is valid.
- Change the **Email Content**.

Step 2 Add an authentication-free host.

1. Navigate to **Authentication** > **User Management**.
2. Click **+Add** in the **Authentication-free Host** module.

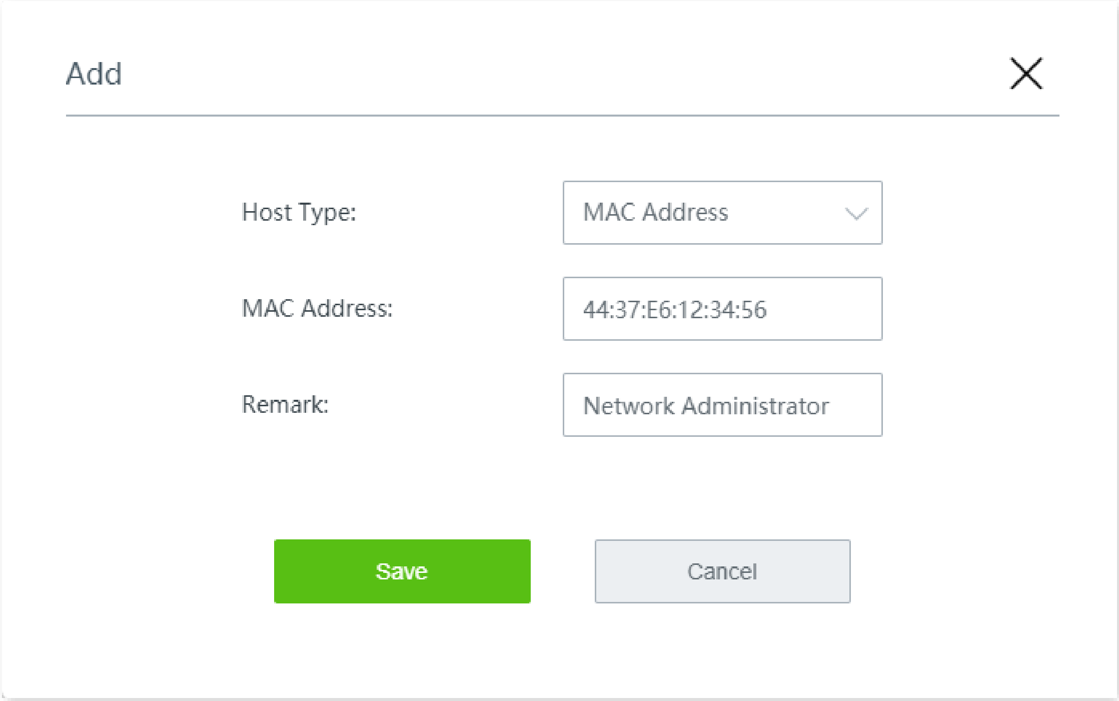


3. Configure the following parameters, then click **Save**.

(1) Select **MAC Address** for **Host Type**.

(2) Enter the **MAC Address**, which is **44:37:E6:12:34:56** in this example.

(3) (Optional) Set a **Remark** for the host, which is **Network Administrator** in this example.



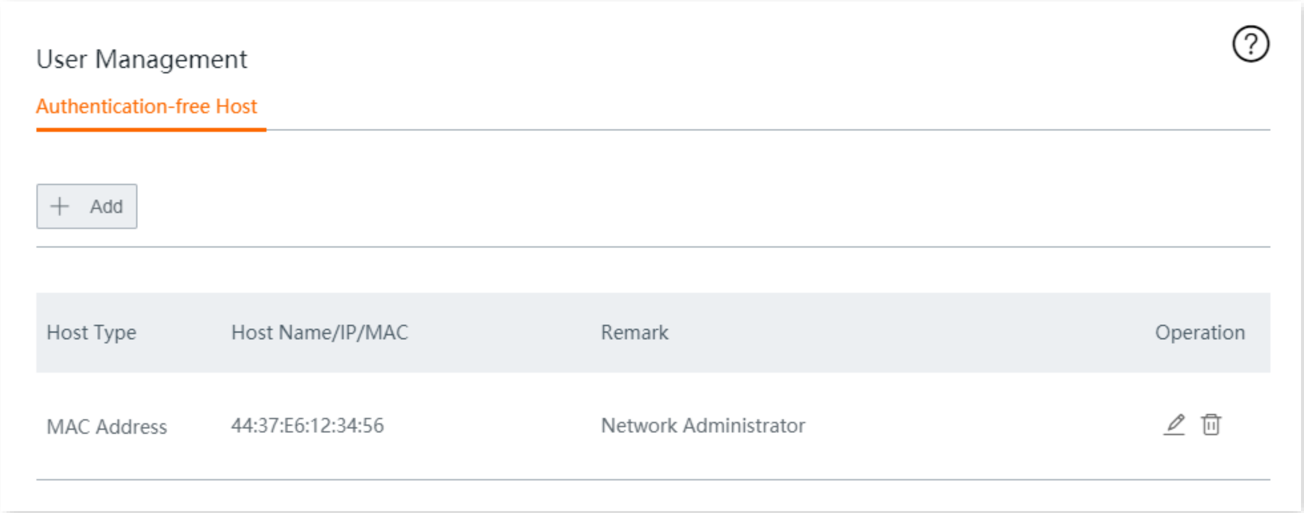
Host Type: MAC Address

MAC Address: 44:37:E6:12:34:56

Remark: Network Administrator

----End

Added successfully. See the following figure.



User Management

Authentication-free Host

Host Type	Host Name/IP/MAC	Remark	Operation
MAC Address	44:37:E6:12:34:56	Network Administrator	✎ 🗑

Verification

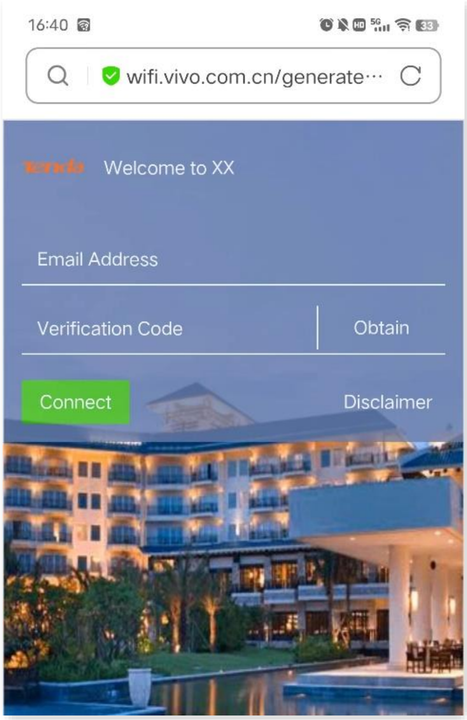
The network administrator can access the internet without authentication. Other employees have to perform email authentication as follows:

Step 1 Start a web browser and visit any website. The authentication page appears.

Step 2 Enter a valid email address and tap **Obtain**.

Step 3 Enter the **Verification Code** in the email received.

Step 4 Tap **Connect**.



After successful authentication, the browser will automatically redirect to www.tendacn.com.

9 AP mangement

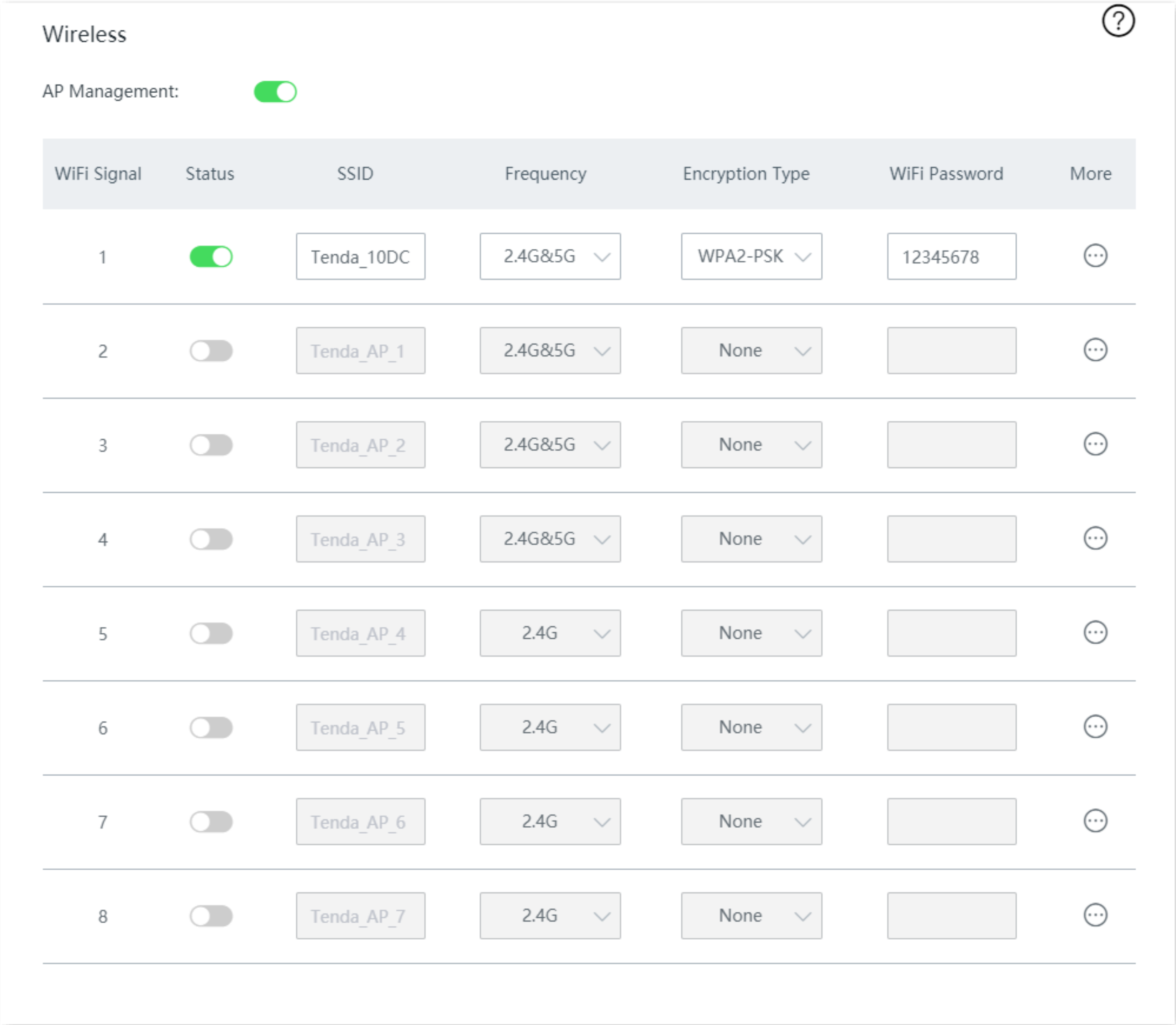
9.1 Basic settings

9.1.1 Overview

Click **AP Management** > **Basic Settings** to enter the page.

Here, you can enable or disable the AP management function of the router. After it is enabled, you can centrally set up WiFi network-related configurations of APs in your local area network, such as viewing and editing wireless network names (SSID), WiFi passwords, configuring 2.4 GHz and 5 GHz WiFi networks, hiding your WiFi network so that nearby wireless clients cannot detect it, and specifying how many wireless clients can connect to a wireless network at most.

The wireless configuration you configured here will be automatically delivered to the Tenda APs within the LAN of the router.



Wireless

AP Management: ●

WiFi Signal	Status	SSID	Frequency	Encryption Type	WiFi Password	More
1	●	Tenda_10DC	2.4G&5G	WPA2-PSK	12345678	⋯
2	○	Tenda_AP_1	2.4G&5G	None		⋯
3	○	Tenda_AP_2	2.4G&5G	None		⋯
4	○	Tenda_AP_3	2.4G&5G	None		⋯
5	○	Tenda_AP_4	2.4G	None		⋯
6	○	Tenda_AP_5	2.4G	None		⋯
7	○	Tenda_AP_6	2.4G	None		⋯
8	○	Tenda_AP_7	2.4G	None		⋯

Parameter description

Parameter	Description
WiFi Signal	Serial number of the wireless policies. • 1 to 4 policies: Used to apply to 1 to 4 wireless networks of APs • 5 to 8 policies: Used to apply to 5 to 8 wireless networks of APs.
Status	Enable or disable a wireless network policy or AP's corresponding SSID. By default, WiFi network policy 1 is enabled and the other policies are disabled.
SSID	Used to change the wireless network name.
Frequency	Select a band used by the wireless policy which will be delivered to APs. • **2.4G:** The wireless policy will be applied to the 2.4 GHz wireless networks of APs. • **5G:** The wireless policy will be applied to the 5 GHz wireless networks of APs. • **2.4G&5G**: The wireless policy will be applied to both 2.4 GHz and 5 GHz wireless networks of APs. TIP If a single band, such as 2.4G (or 5G), is selected in policies 1 to 4, the wireless networks at the other band will be disabled after the policy is delivered to APs.
Encryption Type	Specifies the encryption types of the wireless network. • **None**: Open wireless network. No password is required when a client connects to the wireless network. To secure the network, this option is not recommended. • **WPA-PSK**: The wireless network adopts the WPA-PSK authentication method (AES encryption rule). It is featured with better compatibility than WPA2-PSK. • **WPA2-PSK**: The wireless network adopts the WPA2-PSK authentication method (AES encryption rule). It is featured with higher security level than WPA-PSK. • **WPA-PSK/WPA2-PSK**: The wireless network adopts both WPA-PSK and WPA2-PSK. • **WPA2-PSK/WPA3-SAE**: The wireless network adopts both WPA2-PSK and WPA3-SAE. With Simultaneous Authentication of Equals (SAE) and Protected Management Frames (PMF), WPA3-SAE provides protection against dictionary attacks and information disclosure, saving you the trouble to set a complicated password. Through such mixed encryption mode, the router allows clients that do not support WPA3 to access the wireless network, ensuring both compatibility and security. TIP WPA3-SAE is an upgraded version of WPA2-PSK. If your wireless client does not support WPA3-SAE, or the actual WiFi experience is bad, it is recommended to set the encryption type to WPA2-PSK.
WiFi Password	Specifies the pre-shared password for WPA-PSK, WPA2-PSK or WPA3-SAE, as well as the password required for connecting to the wireless network.

Parameter	Description
More	For more settings, click the ⋯ icon and navigate to the configuration page: - **Isolate Client**: With this function enabled, clients connected to the wireless network cannot communicate with each other, improving the security of the wireless network. - **Hide SSID**: With this function enabled, nearby wireless clients cannot detect the SSID, and you need to manually enter the SSID on the wireless client to access the wireless network. - **Max. Users**: Maximum number of wireless clients that can be connected to the wireless network with the SSID. After the value is reached, this wireless network denies new connection requests. By default, it is set to **48**.

9.1.2 Distribute wireless policies to APs

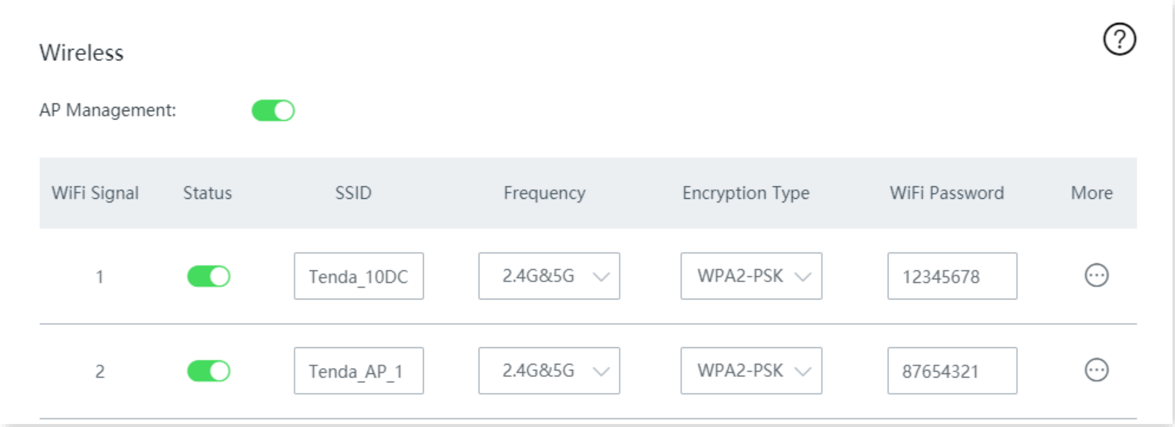
NOTE

When wireless policies are distributed to APs that do not support part of the functions, these unsupported policies will still be received but will not take effect.

For example, when policies concerning 5G network are distributed to APs that do not support 5G, these policies will be received but will not take effect in these APs.

Step 1 Choose **AP Management** > **Basic Settings**.

Step 2 Change the wireless configurations, and click **Save** at the bottom of the page.



Wireless

AP Management: ●

WiFi Signal	Status	SSID	Frequency	Encryption Type	WiFi Password	More
1	●	Tenda_10DC	2.4G&5G	WPA2-PSK	12345678	⋯
2	●	Tenda_AP_1	2.4G&5G	WPA2-PSK	87654321	⋯

----End

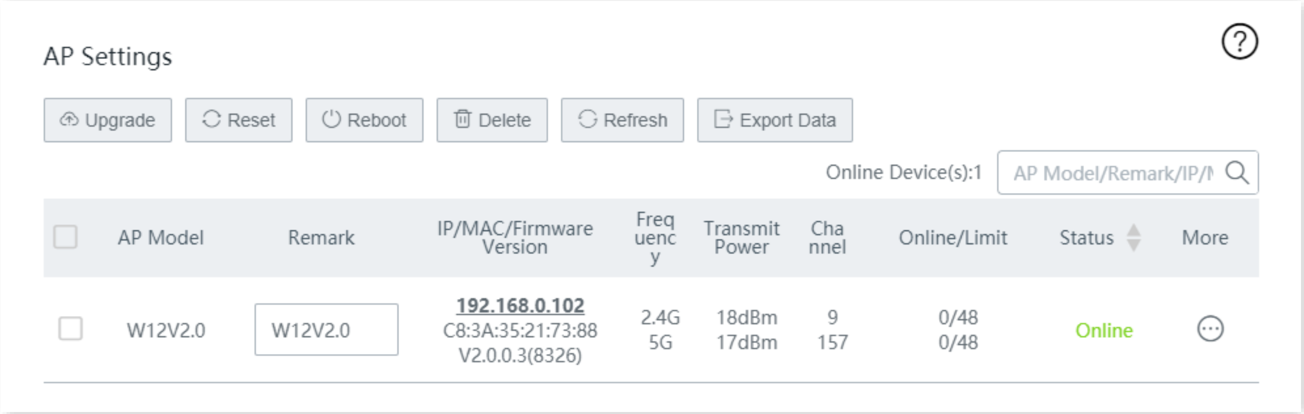
Wait a moment. The wireless configurations of APs in the LAN will be same as the wireless policies.

9.2 AP settings

9.2.1 Overview

Click **AP Management** > **AP Settings** to enter the page.

Here, you can manage Tenda APs connected to your router, such as upgrading/resetting/rebooting APs in batches, deleting offline APs in batches, modifying APs' configuration individually and viewing/exporting APs' configuration.



□	AP Model	Remark	IP/MAC/Firmware Version	Frequency	Transmit Power	Channel	Online/Limit	Status	More
□	W12V2.0	W12V2.0	192.168.0.102 C8:3A:35:21:73:88 V2.0.0.3(8326)	2.4G 5G	18dBm 17dBm	9 157	0/48 0/48	Online	⋯

Parameter description

Parameter	Description
AP Model	Specifies the model of AP.
Remark	Specifies the remark of AP.
IP/MAC/Firmware Version	Specifies the IP address, MAC address and firmware version of AP. TIP Click the IP address to visit the web UI of the AP.
Frequency	Specifies the band used by the wireless policy which will be delivered to APs. - **2.4G:** The wireless policy will be applied to the 2.4 GHz wireless networks of APs. - **5G:** The wireless policy will be applied to the 5 GHz wireless networks of APs. - **2.4G&5G**: The wireless policy will be applied to both 2.4 GHz and 5 GHz wireless networks of APs. TIP If a single band, such as 2.4G (or 5G), is selected in policies 1 to 4, the wireless networks at the other band will be disabled after the policy is delivered to APs.
Transmit Power	Specifies the transmit power of the AP. If the specified transmit power exceeds the limit power of an AP, the actual power is equal to the limit power. For example, if the specified power is greater than the maximum power of an AP, the actual power of the AP is the maximum power after the wireless policy is delivered, and vice versa.
Channel	Specifies the operating channel of AP.

Parameter	Description
Online/Limit	Specify the online devices connected to the AP and the maximum devices allowed to connect to the AP.
Status	Specifies the status of AP.
More	Click the ⋯ icon for more Advanced Settings.

9.2.2 Upgrade the APs

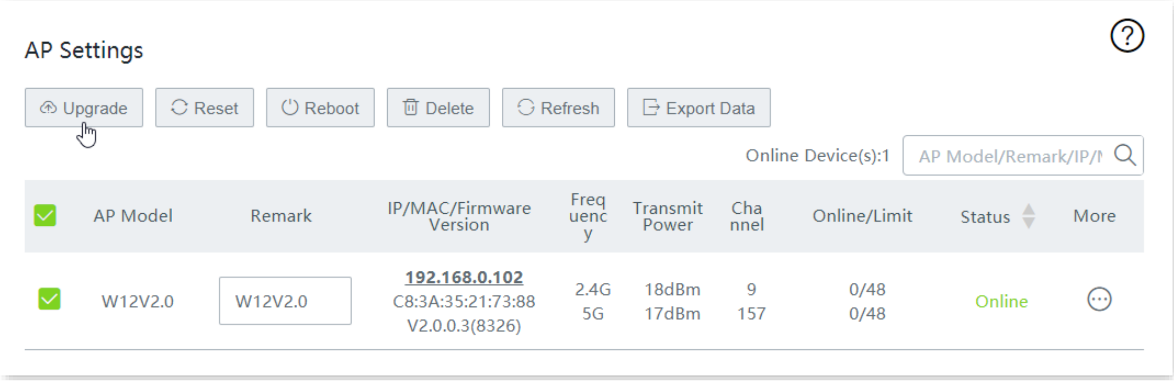
NOTE

To avoid data loss and device damage, Do NOT remove the power of APs and the router during the upgrade.

Step 1 Visit www.tendacn.com to download the latest firmware of the AP to your local computer.

Step 2 Log in to the web UI of the router, and navigate to **AP Management > AP Settings**.

Step 3 Select the AP(s) you want to upgrade, click the **Upgrade** button, and follow the instructions.



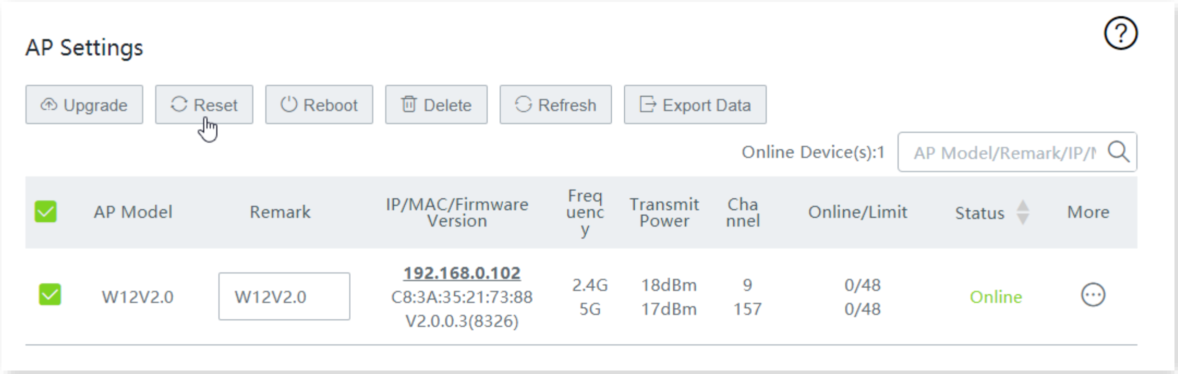
☑	AP Model	Remark	IP/MAC/Firmware Version	Frequency	Transmit Power	Channel	Online/Limit	Status	More
☑	W12V2.0	W12V2.0	192.168.0.102 C8:3A:35:21:73:88 V2.0.0.3(8326)	2.4G 5G	18dBm 17dBm	9 157	0/48 0/48	Online	⋯

----End

9.2.3 Reset the APs

Step 1 Navigate to **AP Management > AP Settings**.

Step 2 Select the AP(s) you want to reset, click the **Reset** button, and follow the instructions.



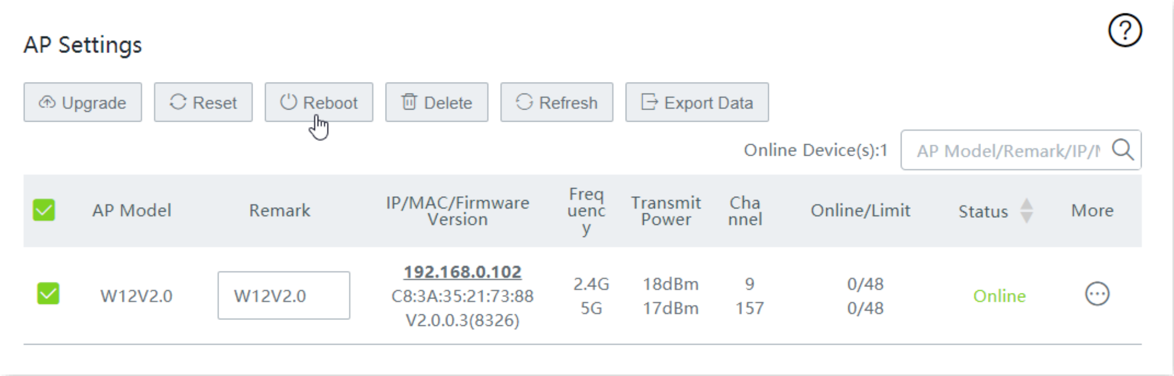
☑	AP Model	Remark	IP/MAC/Firmware Version	Frequency	Transmit Power	Channel	Online/Limit	Status	More
☑	W12V2.0	W12V2.0	192.168.0.102 C8:3A:35:21:73:88 V2.0.0.3(8326)	2.4G 5G	18dBm 17dBm	9 157	0/48 0/48	Online	⋯

----End

9.2.4 Reboot the APs

Step 1 Navigate to **AP Management > AP Settings**.

Step 2 Select the AP(s) you want to reboot, click the **Reboot** button, and follow the instructions.



☑	AP Model	Remark	IP/MAC/Firmware Version	Frequency	Transmit Power	Channel	Online/Limit	Status	More
☑	W12V2.0	W12V2.0	192.168.0.102 C8:3A:35:21:73:88 V2.0.0.3(8326)	2.4G 5G	18dBm 17dBm	9 157	0/48 0/48	Online	⋯

----End

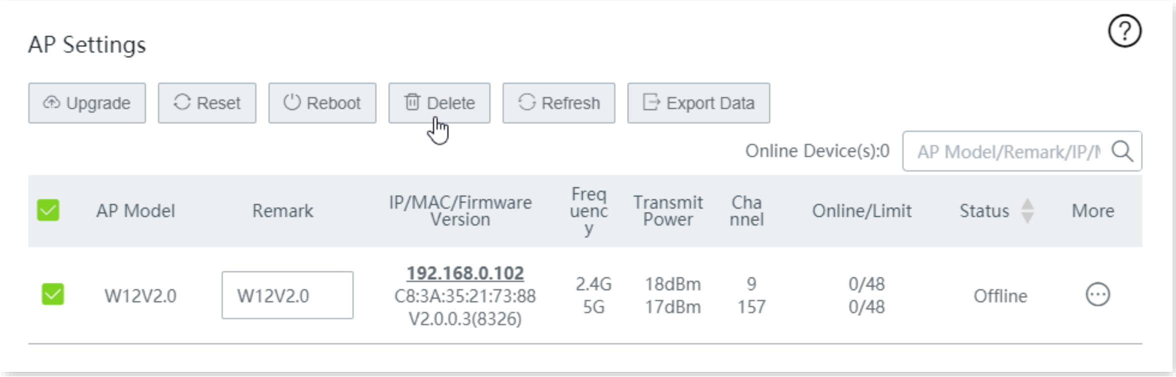
After rebooting successfully, the AP will automatically become online. The time from offline to online lasts about 1 to 2 minutes. Please wait with patience. You can click **Refresh** to view the status.

9.2.5 Delete the APs

Here, you can delete offline APs.

Step 1 Navigate to **AP Management > AP Settings**.

Step 2 Select the offline AP(s) you want to delete, click the **Delete** button, and follow the instructions.



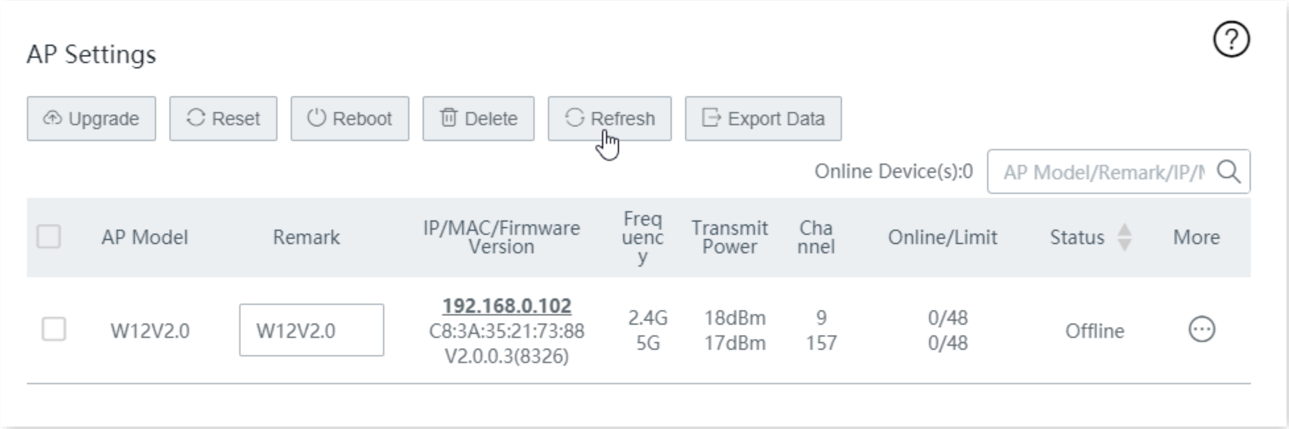
AP Settings

☑	AP Model	Remark	IP/MAC/Firmware Version	Frequency	Transmit Power	Channel	Online/Limit	Status	More
☑	W12V2.0	W12V2.0	192.168.0.102 C8:3A:35:21:73:88 V2.0.0.3(8326)	2.4G 5G	18dBm 17dBm	9 157	0/48 0/48	Offline	⋯

----End

9.2.6 Refresh the page

Here, you can click the **Refresh** button to view the latest status of AP.



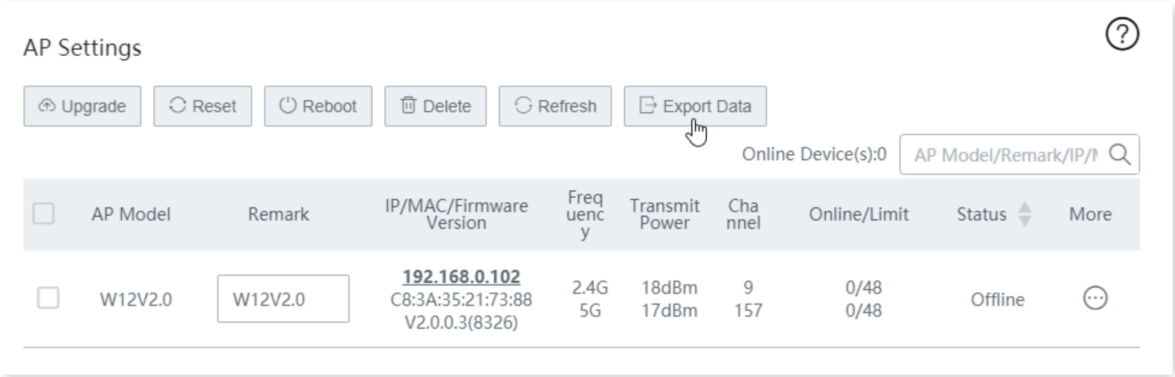
□	AP Model	Remark	IP/MAC/Firmware Version	Frequency	Transmit Power	Channel	Online/Limit	Status	More
□	W12V2.0	W12V2.0	192.168.0.102 C8:3A:35:21:73:88 V2.0.0.3(8326)	2.4G 5G	18dBm 17dBm	9 157	0/48 0/48	Offline	⋯

9.2.7 Export data

Use **Export Data** button if you want to download your APs' information displayed on the **AP Settings** page as an Excel document to your local computer.

Step 1 Navigate to **AP Management > AP Settings**.

Step 2 Click the **Export Data** button, and follow the instructions.



□	AP Model	Remark	IP/MAC/Firmware Version	Frequency	Transmit Power	Channel	Online/Limit	Status	More
□	W12V2.0	W12V2.0	192.168.0.102 C8:3A:35:21:73:88 V2.0.0.3(8326)	2.4G 5G	18dBm 17dBm	9 157	0/48 0/48	Offline	⋯

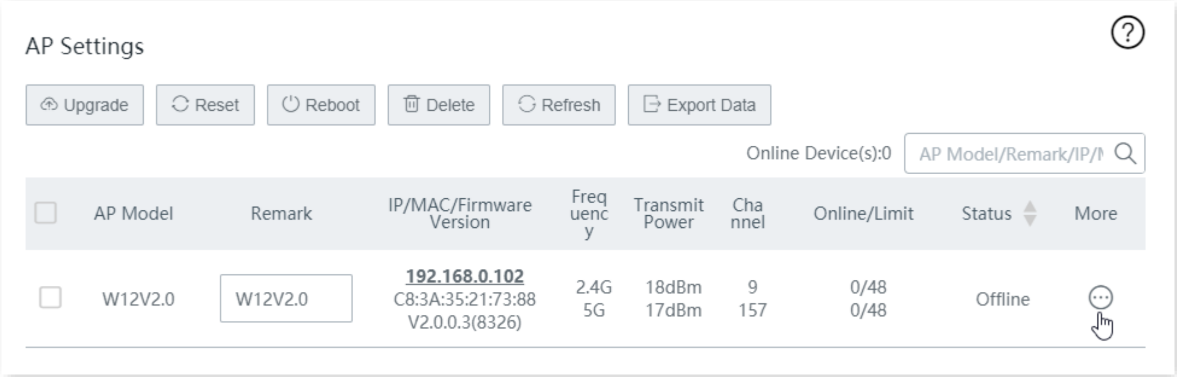
----End

9.2.8 More settings

Here, you can modify each AP's configuration, such as the country/region, channel, transmit power, and so on.

Step 1 Navigate to **AP Management > AP Settings**.

Step 2 Locate the AP as needed, and click ⋯.



AP Settings

Online Device(s):0

□	AP Model	Remark	IP/MAC/Firmware Version	Frequency	Transmit Power	Channel	Online/Limit	Status	More
□	W12V2.0	W12V2.0	192.168.0.102 C8:3A:35:21:73:88 V2.0.0.3(8326)	2.4G 5G	18dBm 17dBm	9 157	0/48 0/48	Offline	⋯

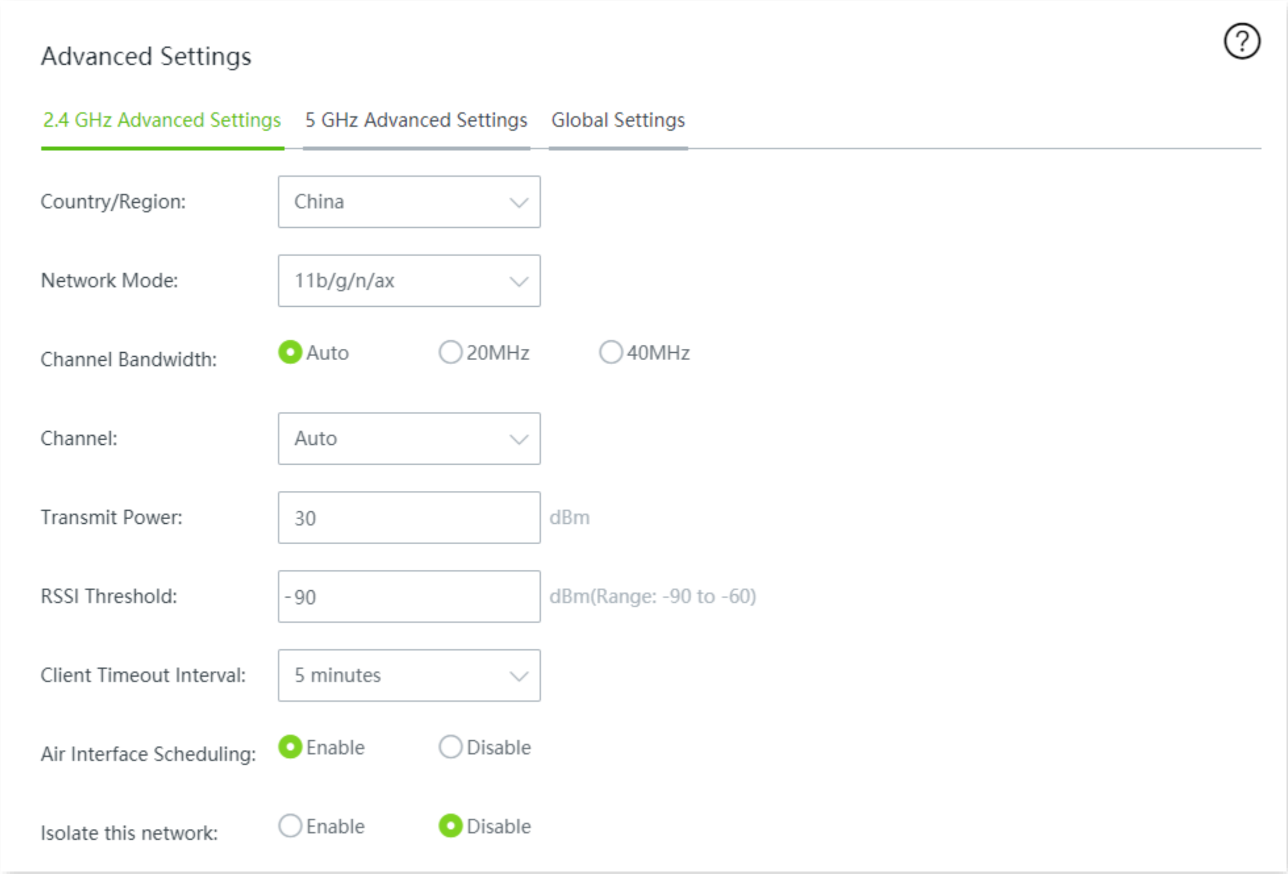
Step 3 Modify the configuration of the AP, and click **Save** at the bottom of the page.

----End

9.3 Advanced settings

Click **AP Management** > **Advanced Settings** to enter the page.

Here, you can set up the advanced settings for the APs in the LAN.



Advanced Settings

Country/Region: China

Network Mode: 11b/g/n/ax

Channel Bandwidth: ● Auto ○ 20MHz ○ 40MHz

Channel: Auto

Transmit Power: 30 dBm

RSSI Threshold: -90 dBm(Range: -90 to -60)

Client Timeout Interval: 5 minutes

Air Interface Scheduling: ● Enable ○ Disable

Isolate this network: ○ Enable ● Disable

2.4 GHz advanced settings / 5 GHz advanced settings

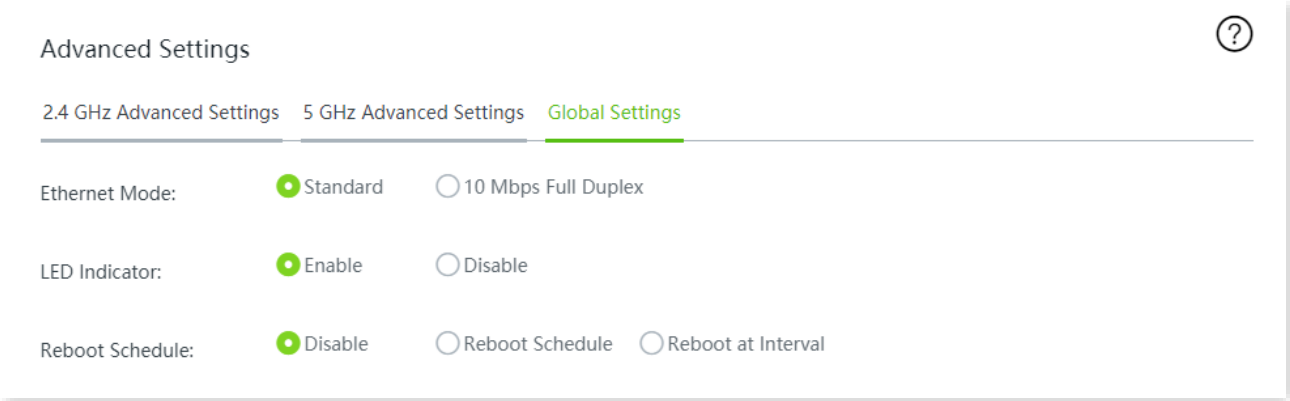
Parameter description

Parameter	Description
Country/Region	Country or region where this device is located. You can select the country or region to ensure that this device complies with the local regulations.
Network Mode	Specifies the wireless network mode (also called 802.11 mode, radio mode, or wireless mode) of the AP. A proper network mode enables the clients to get the maximum transfer rate and compatibility. Available options for **2.4 GHz** band: **11b**, **11g**, **11b/g**, **11b/g/n** and **11b/g/n/ax** (default). Available options for **5 GHz** band: **11a, 11ac, 11a/n** and **11a/n/ac/ax** (default)**.**
Channel Bandwidth	Specifies the channel bandwidth for the AP. Available options for **2.4 GHz** band: **Auto** (default), **20MHz**, and **40MHz**. Available options for **5 GHz** band: **20MHz**, **40MHz**, **80MHz**, **160MHz, and Auto** (default).

Parameter	Description
Channel	Specifies the channel in which the AP operates. The available channels are determined by the current country/region and wireless band.
Transmit Power	Specifies the transmit power of the AP. If the specified transmit power exceeds the limit power of an AP, the actual power is equal to the limit power. For example, if the specified power is greater than the maximum power of an AP, the actual power of the AP is the maximum power after the wireless policy is delivered, and vice versa.
RSSI Threshold	Used to set the minimum received signal strength threshold of wireless clients connected to the AP. After this function is enabled, wireless clients whose received signal strength is lower than this threshold cannot connect to the AP. An appropriate threshold ensures the connection quality of clients.
Client Timeout Interval	If a wireless client does not exchange data with the AP in the specified period, the AP disconnects the client.
Prioritize 5 GHz	Specifies that a wireless client compliant with dual-band wireless firstly connects to the 5 GHz band of the device if the corresponding wireless network uses the same SSID and password for both 2.4 GHz and 5 GHz. This function takes effect when: • The encryption mode is set to WPA-PSK, WPA2-PSK, or WPA-PSK&WPA2-PSK. • The SSID does not contain Chinese characters.
Air Interface Scheduling:	Air interface scheduling allocates equal download data transmission time for each client. In this way, high-speed clients can transmit more data packets and the AP has a higher throughput and client capacity.
Isolate this network	Specifies whether to disable communications among the clients connected to different wireless networks of this device. This function increases wireless network security.
WMM	After WMM is enabled, voice and video packets are transmitted with top priority. You are recommended to enable this function for better transmission of multimedia packets.
APSD	Specifies whether to enable the Automatic Power Save Delivery (APSD) mode. APSD is a WMM power saving protocol created by Wi-Fi Alliance. Enabling APSD helps reduce power consumption. By default, this mode is disabled.
Deployment Mode	Specifies the deployment mode of the router. This parameter is valid only for 2.4 GHz networks. Select a mode that conforms to your application scenario. Available options: • **Default**: This option is a balance between Coverage-oriented and Capacity-oriented. • **Coverage-oriented**: This mode applies to scenarios that the network environment is complex, users are scattered, and the interference is weak. • **Capacity-oriented**: This mode applies to scenarios that the area is open and crowded with users and the interference is strong.

Global settings

Here, you can view and configure the Ethernet mode, LED indicator status and reboot schedule of APs in a global way.



Advanced Settings

Ethernet Mode: ● Standard ○ 10 Mbps Full Duplex

LED Indicator: ● Enable ○ Disable

Reboot Schedule: ● Disable ○ Reboot Schedule ○ Reboot at Interval

Parameter description

Parameter	Description
Ethernet Mode	Select the Ethernet mode for the ports of AP. Available options: • **Standard (default)**: This mode features a high data rate but short transmission distance. • **10 Mbps Full Duplex**: This mode features long transmission distance but low data rate. If the distance between the Ethernet port of the AP and the peer device is longer than 100 meters, this mode is recommended. In this case, ensure that the peer device adopts auto negotiation mode.
LED Indicator	Used to turn on/off the LED indicators of AP. By default, it is enabled. You can judge the working status of AP through the LED indicators.
Reboot Schedule	Select the reboot schedule mode for the AP. Available options: • **Disable** (default). • **Reboot Schedule**: The AP reboots at the specified date and time. • **Reboot Interval**: The AP reboots every interval.

10 USB sharing

10.1 Overview

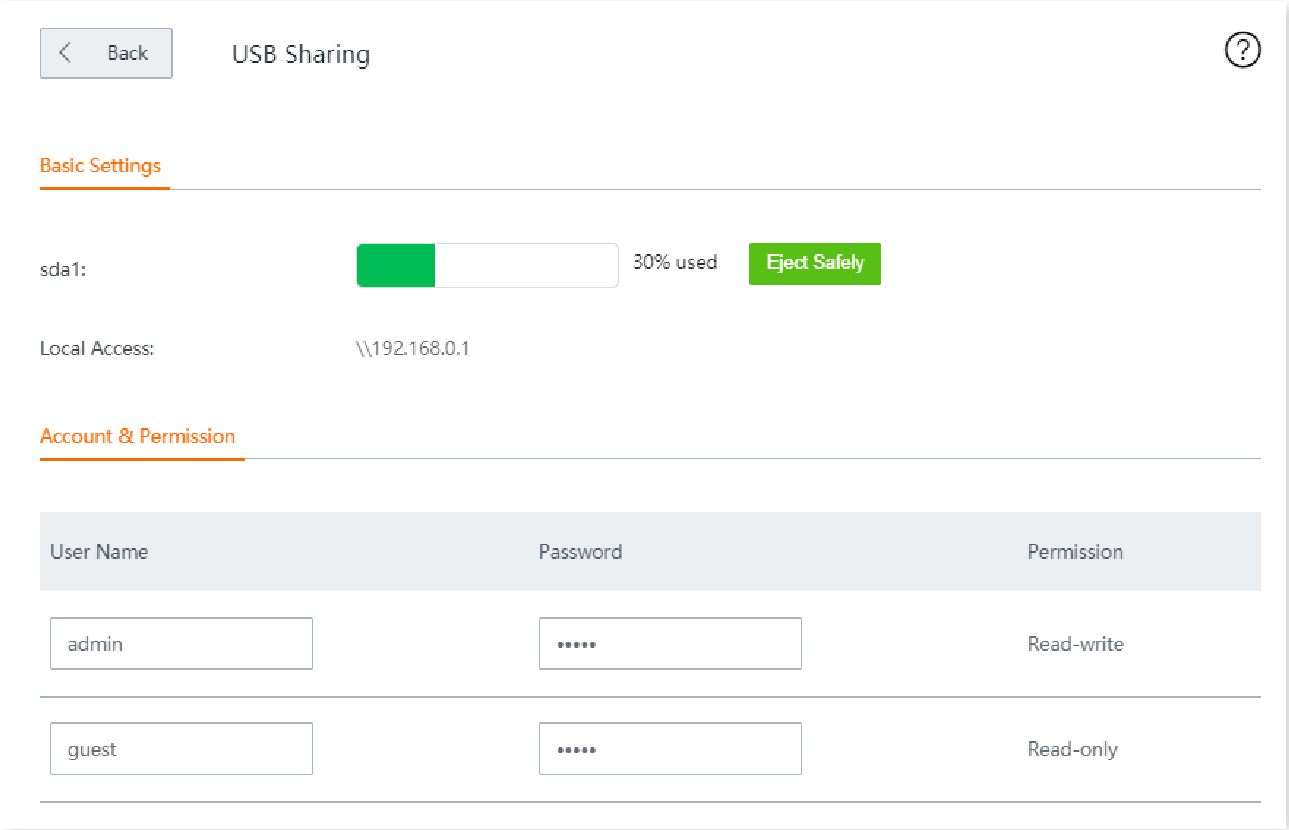
The router provides a USB port for file sharing.

The router can automatically identify the USB storage device plugged into its USB port, and display the information such as the disk usage of the USB device on the web UI. The router also supports the management on file access permission, and LAN users can access files shared on the USB storage device.

10.2 USB sharing

Click **USB Sharing** to enter the page.

After a USB device is plugged in, the router will automatically identify the device as shown below.



sda1: 30% used

Local Access: \\192.168.0.1

User Name	Password	Permission
admin	•••••	Read-write
guest	•••••	Read-only

Parameter description

Parameter	Description
sda1	Specifies the status and occupation percentage of the USB device.

Parameter	Description
Eject Safely	Click it to safely eject the USB device.
Local Access	Specifies the access address LAN users use to access the USB disk device. \\192.168.0.1: You can type this address into the **Start** > **Run** menu on your computer to get local access. 192.168.0.1 is the default LAN IP address of the router. If the address is changed, you need to type in the new address to get local access.
User Name	Specifies the user name/password of the read-write or the read-only user.
Password	
Permission	Specifies the permission of the target user. • **Read-write**: The user can read, add, or delete files on the USB device. By default, the user name and password are both **admin**. • **Read-only**: The user can only read files on the USB device. By default, the user name and password are both **guest**.

10.3 Example of configuring USB sharing

10.3.1 Networking requirement

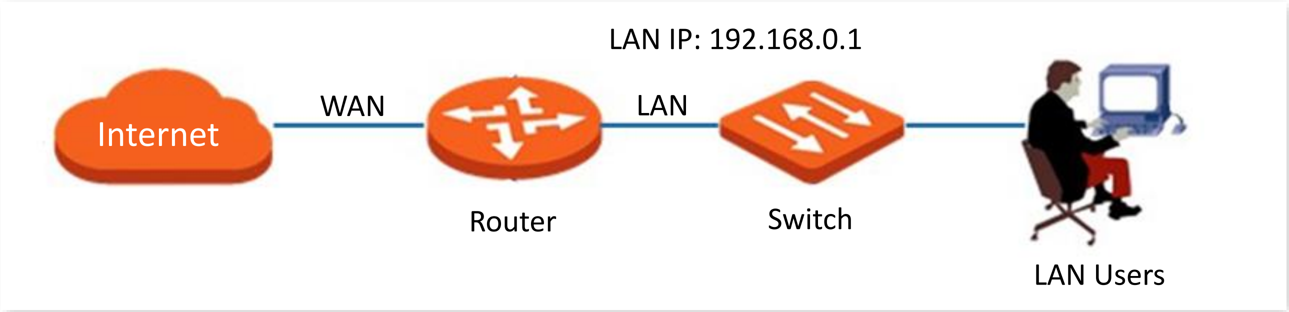
An enterprise uses the wireless router to build a network.

Requirement: A mobile storage device, connected to the USB port of the router, serves as the file server. Employees can search and download files from the file server in local network or through internet.

Assume that:

- Read-write user name/password are both xxadmin.
- Read-only user name/password are both xxguest.

10.3.2 Network topology

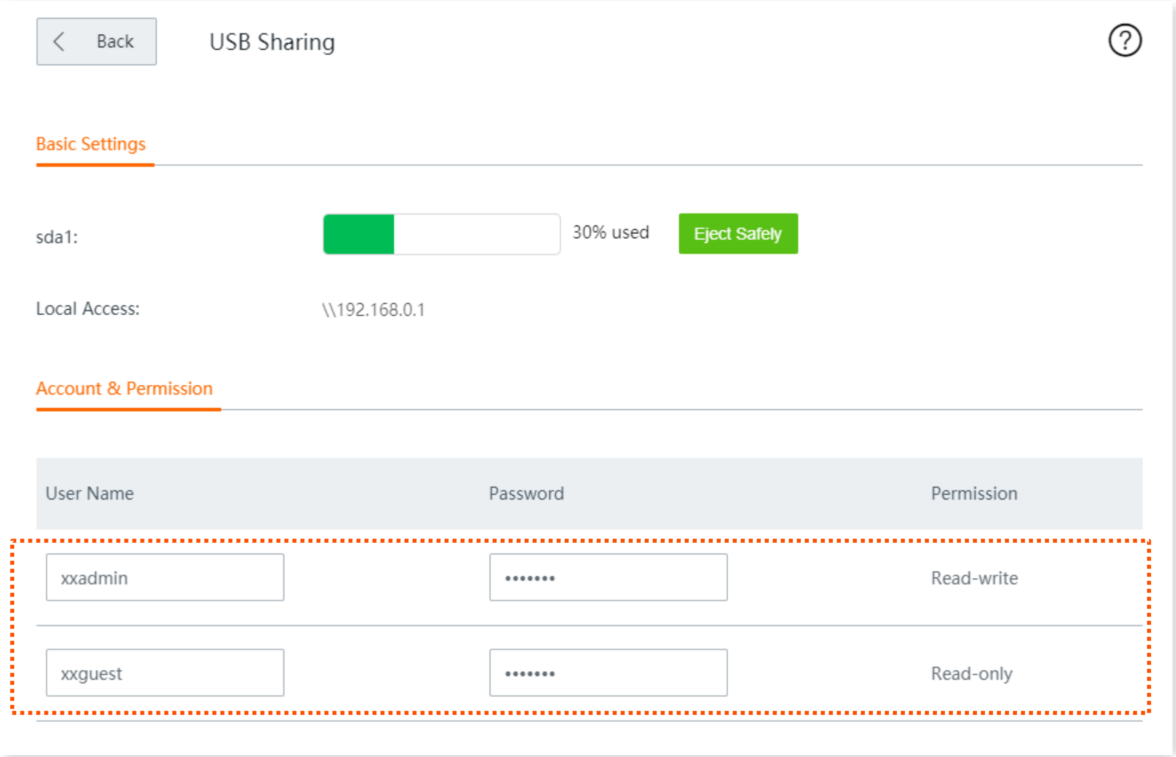


10.3.3 Configuration procedure

Step 1 Plug the mobile storage device into the router.

Step 2 Click **USB Sharing.**

Step 3 Set the read-write user name/password as **xxadmin**, and the read-only user name/password as **xxguest**, and click **Save**.



sda1: 30% used

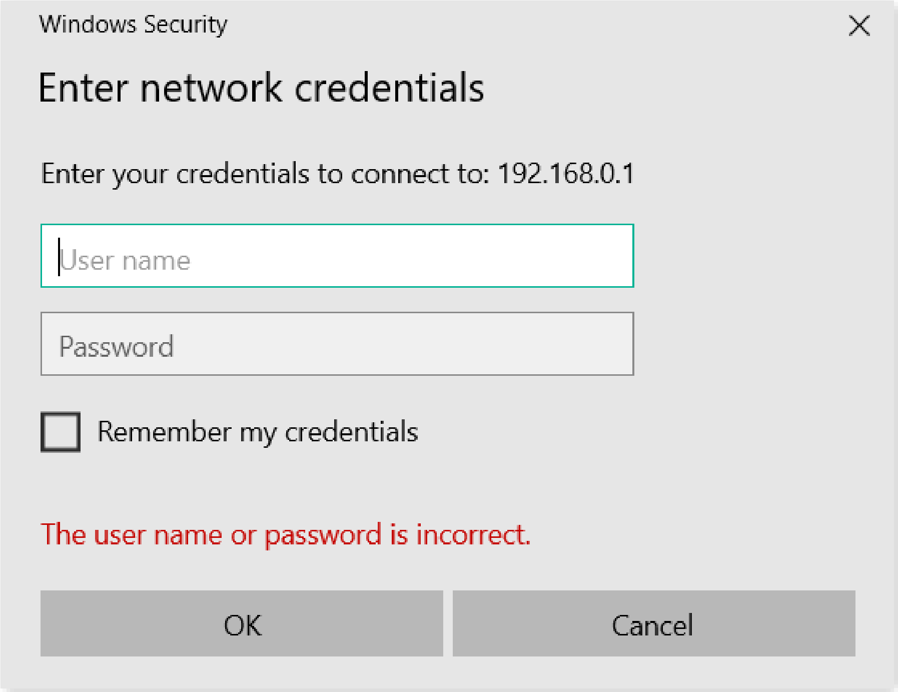
Local Access: \\192.168.0.1

User Name	Password	Permission
xxadmin	•••••••	Read-write
xxguest	•••••••	Read-only

----End

10.3.4 Verification

Take Windows 10 as an example: Enter **\\192.168.0.1** in the search bar at the lower-left of your computer screen. Then, the following page appears. Enter authorized user name and password, and click **OK**.



Windows Security

Enter network credentials

Enter your credentials to connect to: 192.168.0.1

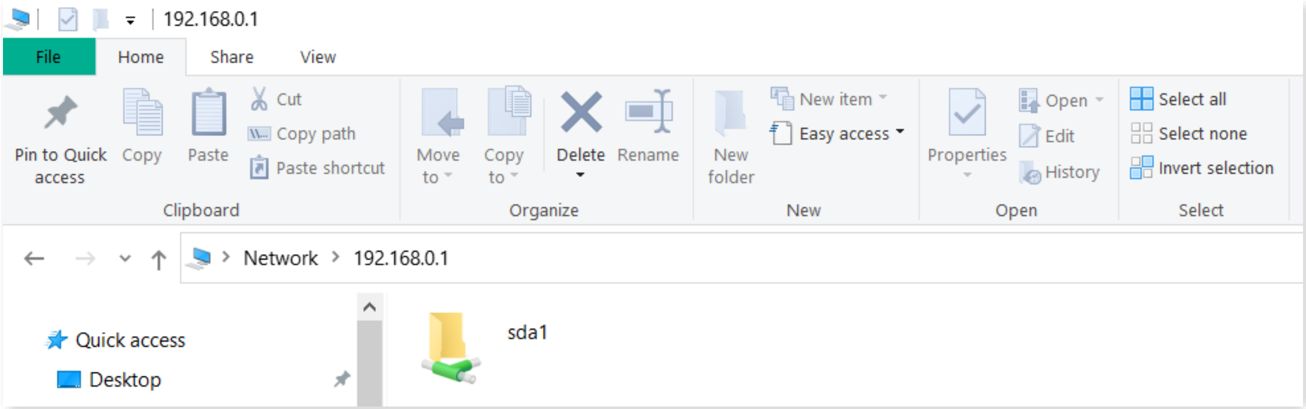
User name

Password

□ Remember my credentials

The user name or password is incorrect.

Access the files successfully.



11 Filter management

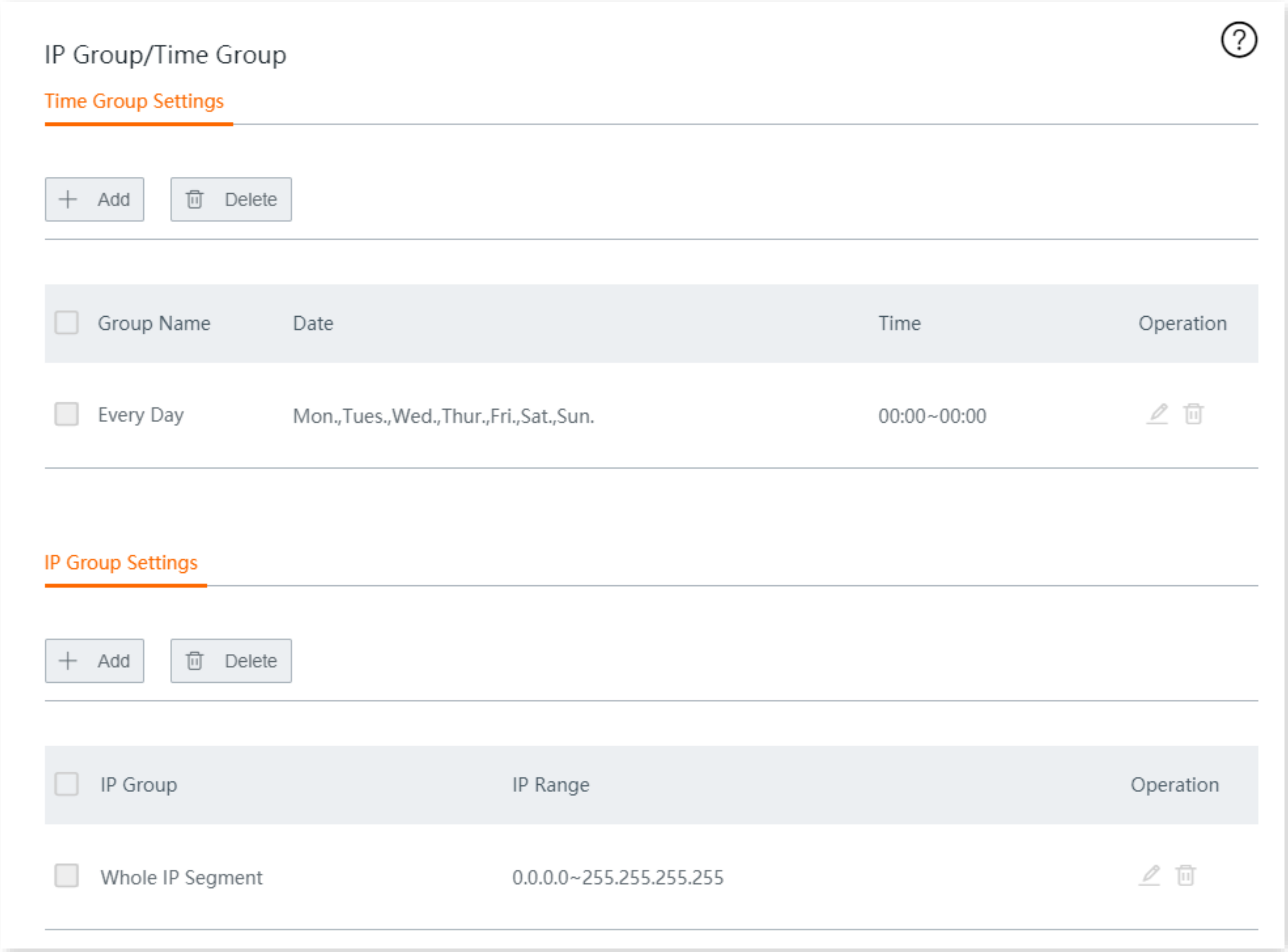
11.1 IP group/time group

11.1.1 Overview

Click **Filter Management** > **IP Group/Time Group** to enter the page.

When configuring functions which take effect depending on IP group or time group, such as MAC address filter, IP address filter, port filter, URL filter, bandwidth limit by group and multi-WAN policy, you need to first configure the target IP group and/or time group.

By default, a time group and an IP group have been added on the router, and the default time group and IP group cannot be deleted or edited.



□	Group Name	Date	Time	Operation
□	Every Day	Mon.,Tues.,Wed.,Thur.,Fri.,Sat.,Sun.	00:00~00:00	

□	IP Group	IP Range	Operation
□	Whole IP Segment	0.0.0.0~255.255.255.255	

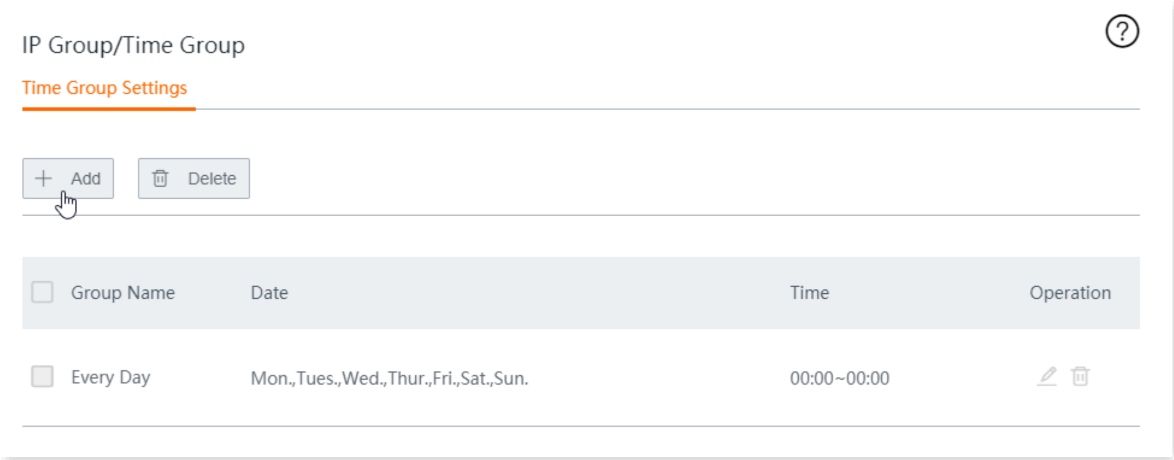
Parameter description

Parameter		Description
Time Group Settings	Group Name	Specifies the name of the time group. The name must be unique.
	Date	Specifies the dates included in the time group.
	Time	Specifies the start and end time of the time group. **00:00~00:00** indicates a whole day.
	Operation	Specifies the operations you can perform on the rule. ✎: Click it to edit the rule. 🗑 : Click it to delete the rule.
IP Group Settings	IP Group	Specifies the name of the IP group. The name must be unique.
	IP Range	Specifies the start and end IP address of the IP group.
	Operation	Specifies the operations you can perform on the rule. ✎: Click it to edit the rule. 🗑 : Click it to delete the rule.

11.1.2 Add a time group

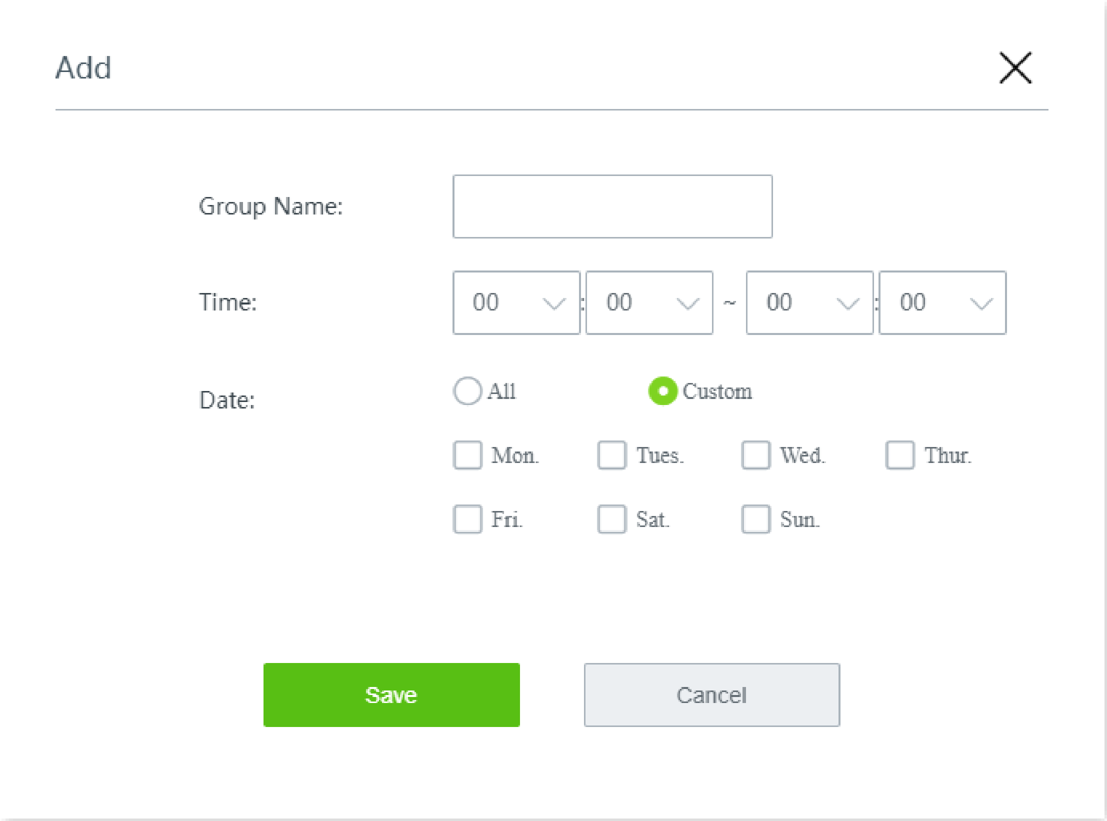
Step 1 Navigate to **Filter Management** > **IP Group/Time Group** > **Time Group Settings**.

Step 2 Click **+Add**.



	Group Name	Date	Time	Operation
□	Every Day	Mon.,Tues.,Wed.,Thur.,Fri.,Sat.,Sun.	00:00~00:00	

Step 3 Configure the following parameters in the **Add** window, and click **Save**.



Group Name:

Time: 00 : 00 ~ 00 : 00

Date: ○ All ● Custom

□ Mon. □ Tues. □ Wed. □ Thur.

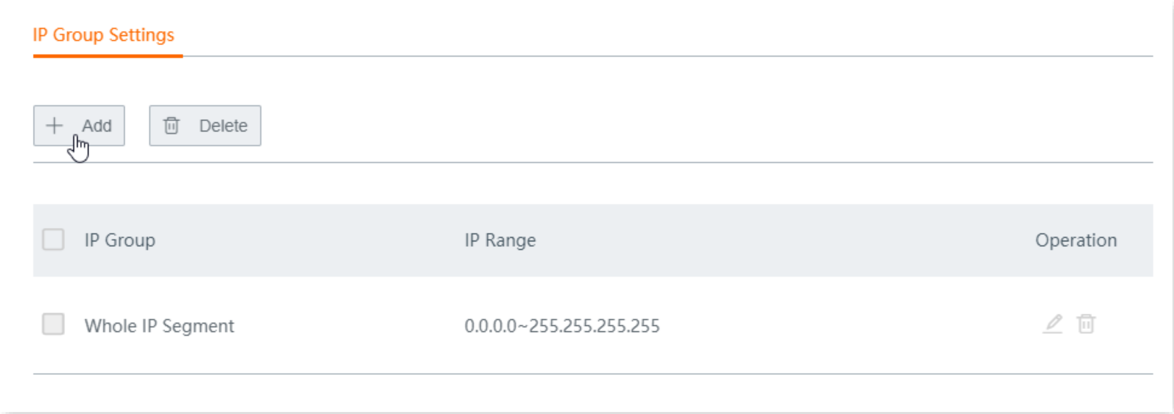
□ Fri. □ Sat. □ Sun.

----End

11.1.3 Add an IP group

Step 1 Navigate to **Filter Management** > **IP Group/Time Group** > **IP Group Settings**.

Step 2 Click **+Add**.

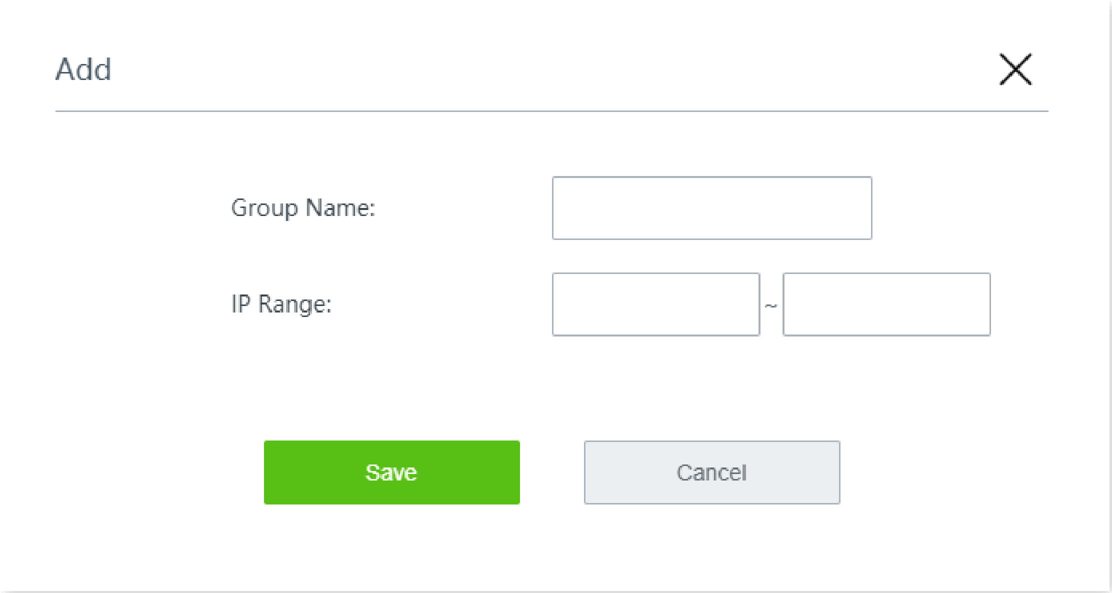


IP Group Settings

+ Add Delete

□ IP Group	IP Range	Operation
□ Whole IP Segment	0.0.0.0~255.255.255.255	✎ 🗑

Step 3 Configure the following parameters in the **Add** window, and click **Save**.



----End

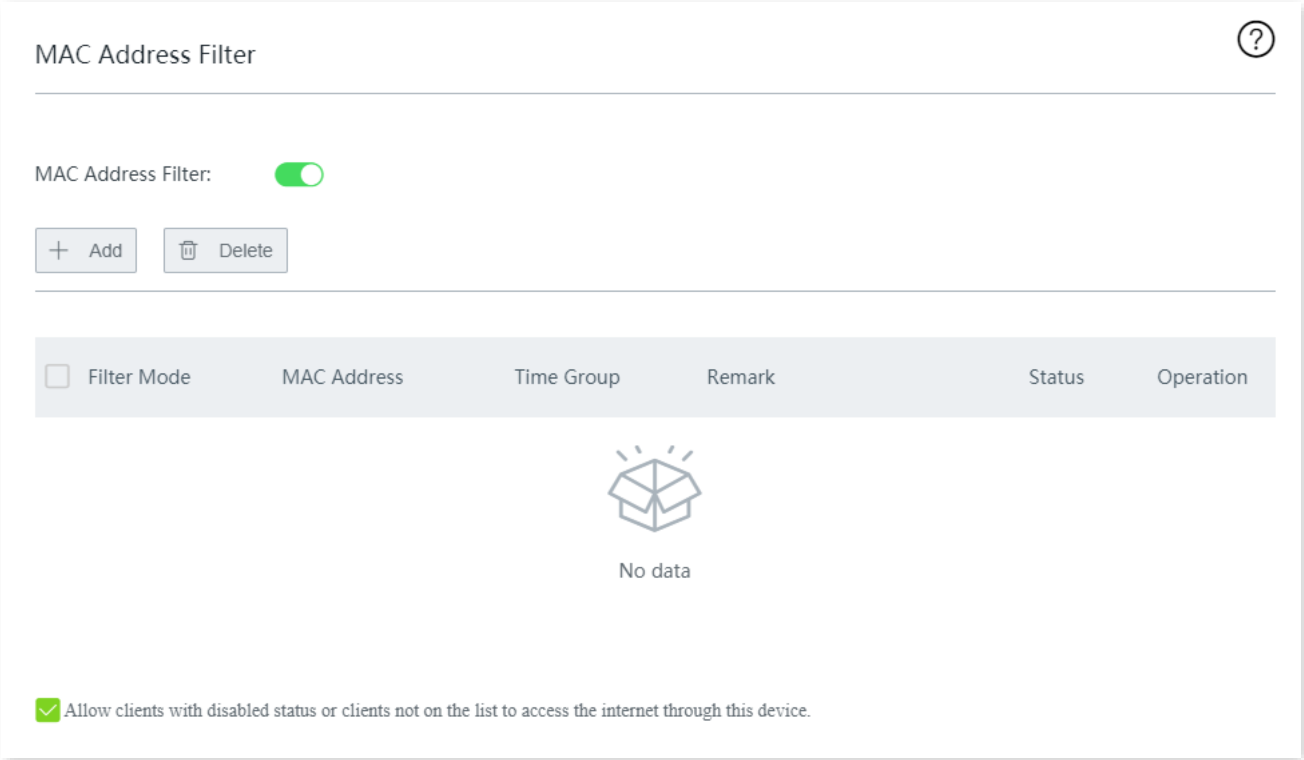
11.2 MAC address filter

11.2.1 Overview

Through MAC address filter, you can allow or block internet access through this router for specified clients.

Click **Filter Management** > **MAC Address Filter** to enter the page.

By default, this function is disabled.



MAC Address Filter

MAC Address Filter: ●

□	Filter Mode	MAC Address	Time Group	Remark	Status	Operation

No data

☑ Allow clients with disabled status or clients not on the list to access the internet through this device.

Parameter description

Parameter	Description
MAC Address Filter	Enable or disable the MAC address filter function.
Filter Mode	Specifies the MAC address filter modes. • **Whitelist**: Specifies that internet access is allowed. In this mode, clients with the specified MAC address can access the internet only within the specified time period. • **Blacklist**: Specifies that internet access is blocked. In this mode, clients with the specified MAC address cannot access the internet only within the specified time period.
MAC Address	Specifies the MAC address of the client to which the rule applies.
Time Group	The time group used to specify the time period during which the rule takes effect. The time group rule should be configured in advance on the **Filter Management** > **IP Group/Time Group** page.

Parameter	Description
Remark	Specifies the remark of the MAC address filter rule.
Status	Specifies the status of the MAC address filter rule. You can enable or disable the rule as required.
Operation	Specifies the operations you can perform on the rule. ✎: Click it to edit the rule. 🗑 : Click it to delete the rule.
Allow clients with disabled status or clients not on the list to access the internet through this device.	- If this option is selected, clients to which the disabled rules in the list apply and clients not in the list can both access the internet. - If this option is not selected, clients to which the disabled rules in the list apply and clients not in the list can neither access the internet.

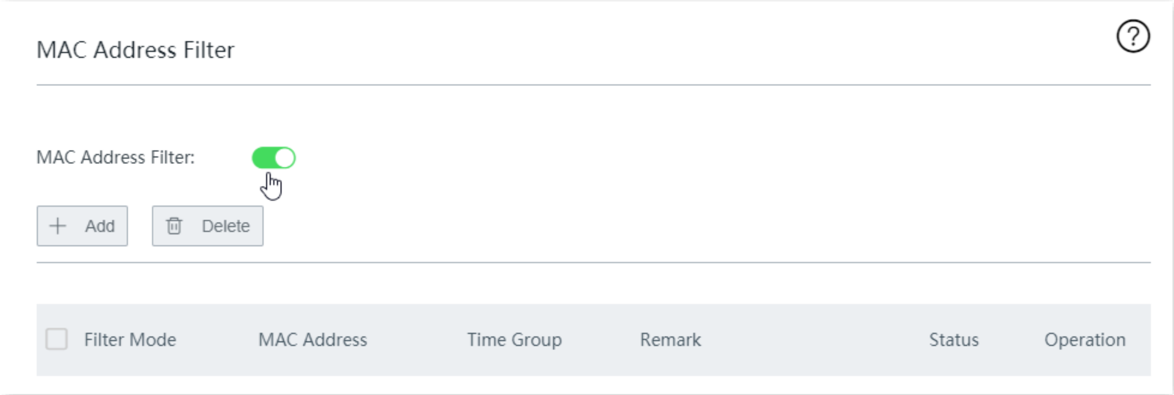
11.2.2 Configure a MAC address filter rule

TIP

Before configuring a MAC address filter rule, please configure the target time group first.

Step 1 Enable MAC address filter.

1. Navigate to **Filter Management** > **MAC Address Filter**.
2. Enable **MAC Address Filter**, and click **Save** at the bottom of the page.

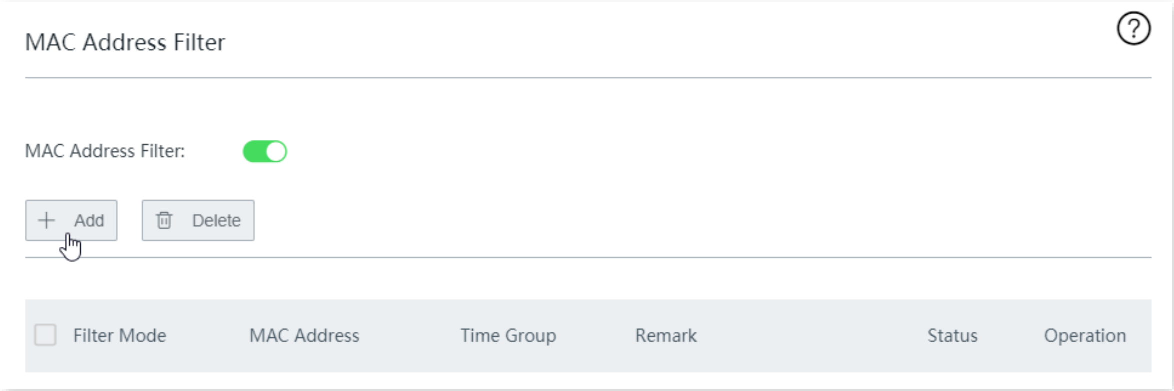


MAC Address Filter

MAC Address Filter: ●

Step 2 Add a MAC address filter rule.

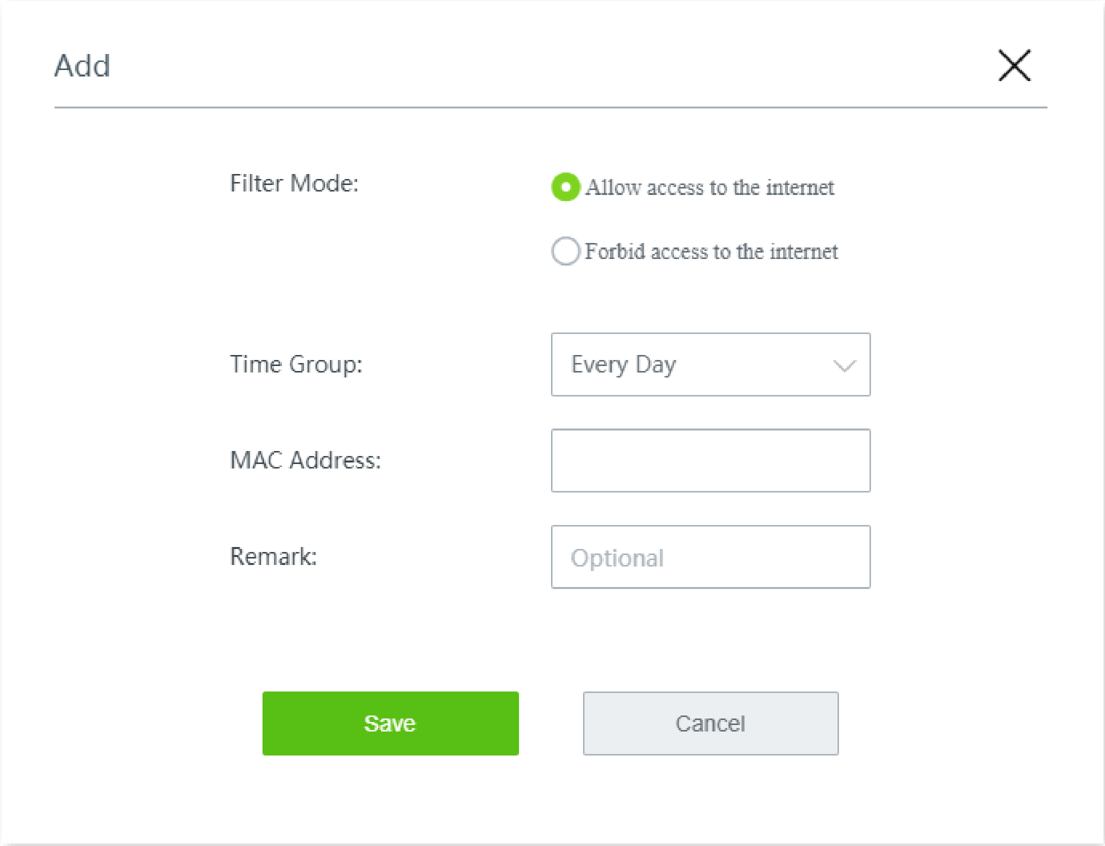
1. Click **+Add**.



MAC Address Filter

MAC Address Filter: ●

2. Configure the following parameters in the **Add** window, and click **Save**.



Add

Filter Mode: ● Allow access to the internet ○ Forbid access to the internet

Time Group: Every Day

MAC Address:

Remark: Optional

----End

11.2.3 Example of configuring a MAC address filter rule

Networking requirement

An enterprise uses the wireless router to build a network.

Requirement:

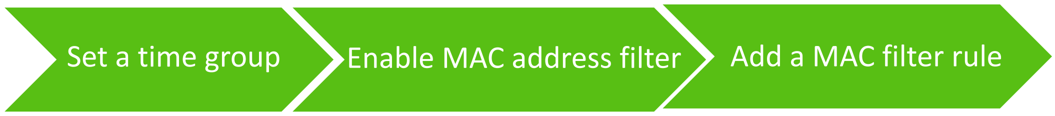
During business hours (08:00 to 18:00 on weekdays), only a purchaser is allowed to access the internet.

Solution

The MAC address filter can meet this requirement.

Assume that the MAC address of the purchaser’s computer is CC:3A:61:71:1B:6E.

Configuration procedure



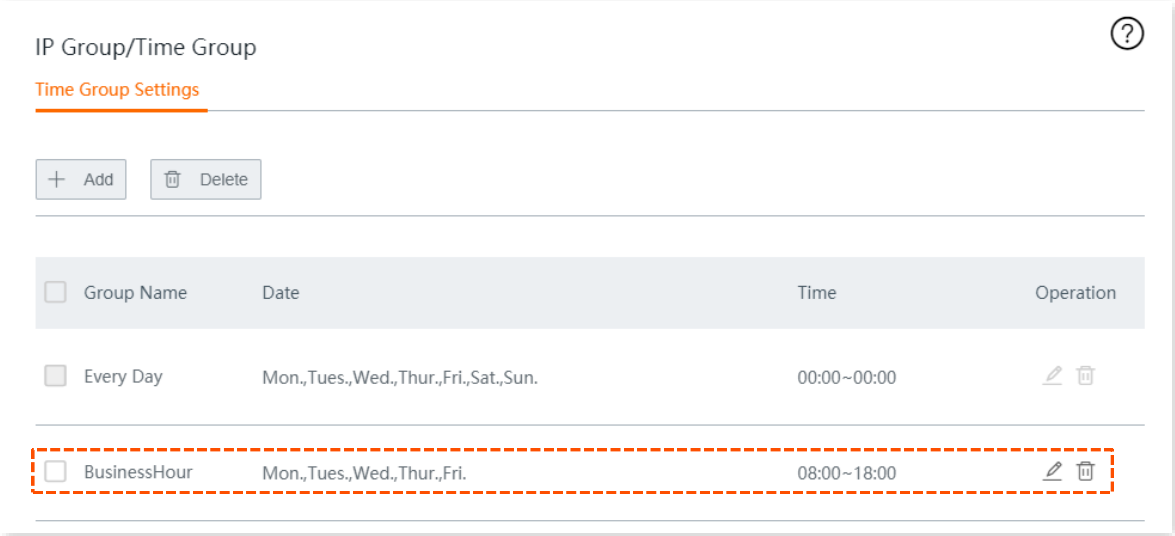
Set a time group

Enable MAC address filter

Add a MAC filter rule

Step 1 Set a time group.

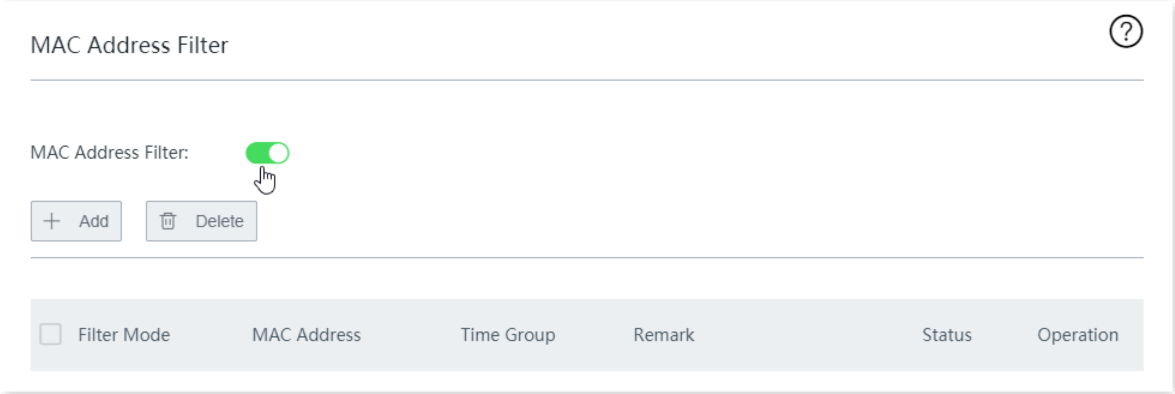
Navigate to **Filter Management** > **IP Group/Time Group**. Set a time group shown in the following figure.



□	Group Name	Date	Time	Operation
□	Every Day	Mon.,Tues.,Wed.,Thur.,Fri.,Sat.,Sun.	00:00~00:00	
□	BusinessHour	Mon.,Tues.,Wed.,Thur.,Fri.	08:00~18:00	

Step 2 Enable MAC address filter.

1. Navigate to **Filter Management** > **MAC Address Filter**.
2. Enable **MAC Address Filter**, and click **Save** at the bottom of the page.

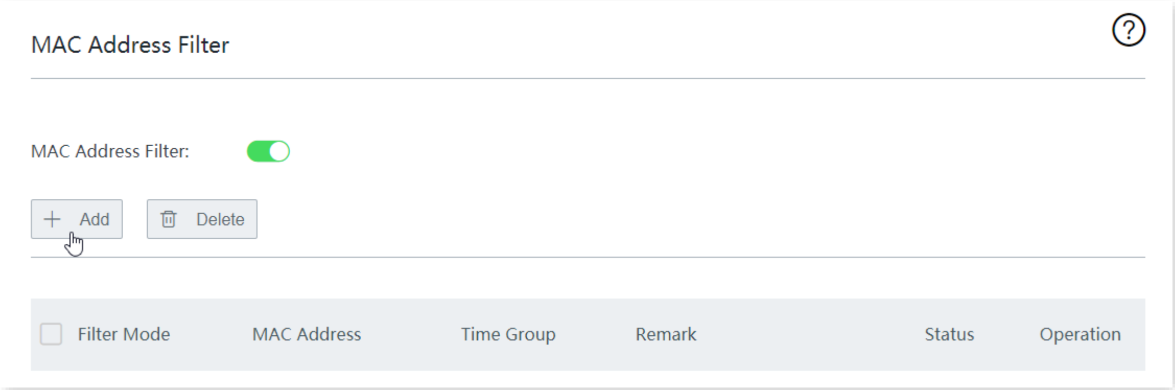


MAC Address Filter:

□	Filter Mode	MAC Address	Time Group	Remark	Status	Operation

Step 3 Add a MAC address filter rule.

1. Click **+Add**.

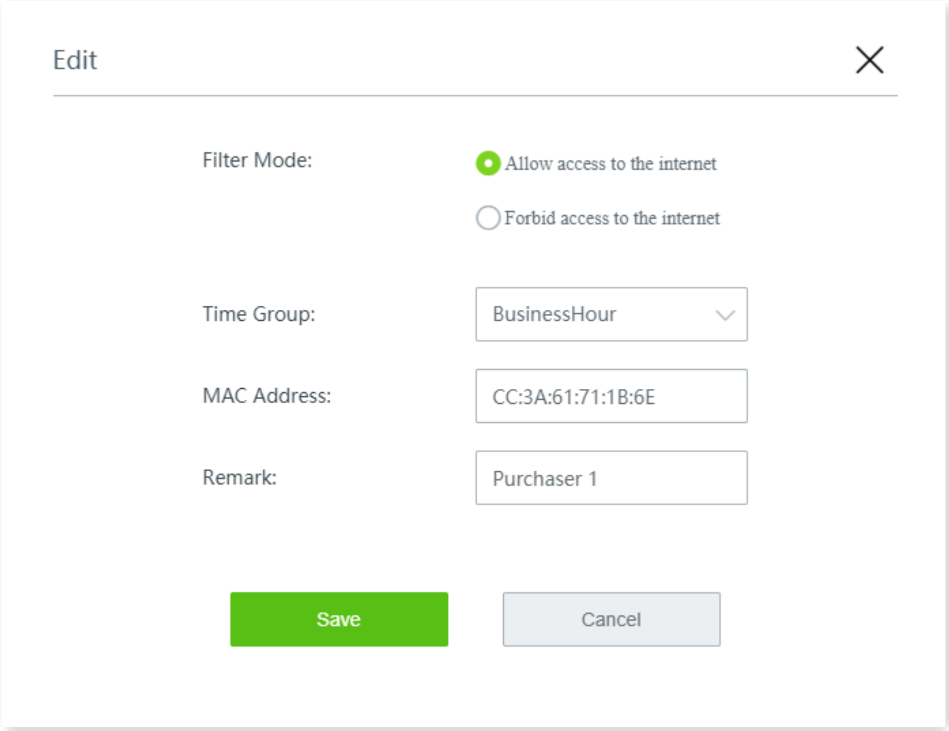


MAC Address Filter:

□	Filter Mode	MAC Address	Time Group	Remark	Status	Operation

2. Configure the following parameters, and click **Save**.
   (1) Set **Filter Mode** to **Allow access to the internet** (whitelist).
   (2) Select the target **Time Group**, which is **BusinessHour** in this example.
   (3) Enter the **MAC Address** of the purchaser's computer, which is **CC:3A:61:71:1B:6E** in this example.

(4) (Optional) Enter a **Remark** for the rule, for example, **Purchaser 1**.


Edit

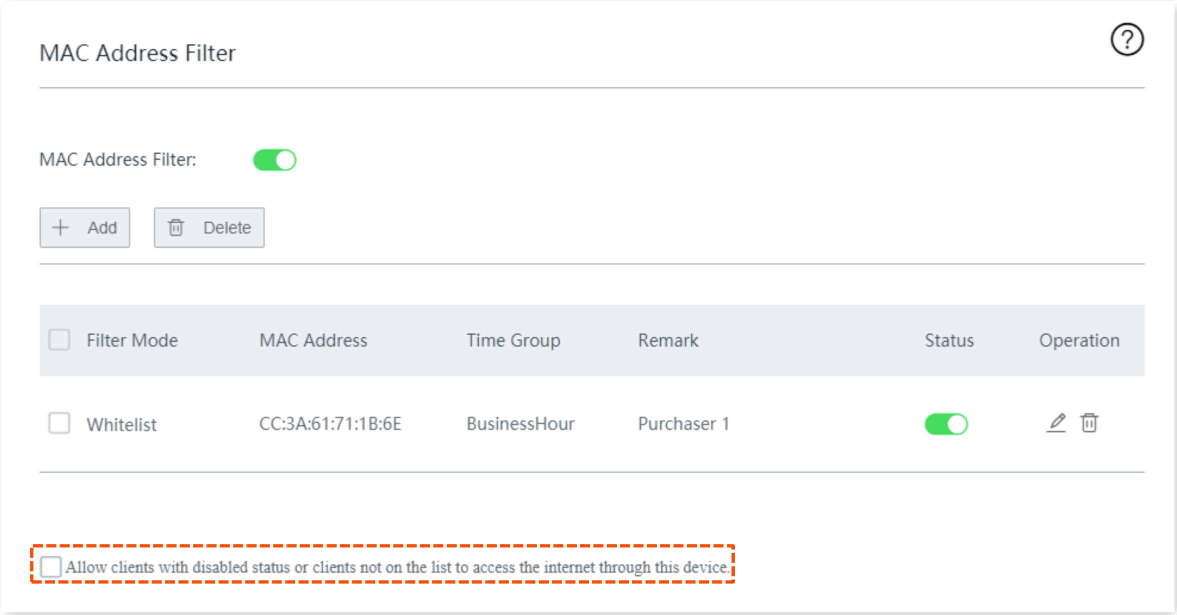
Filter Mode: ● Allow access to the internet ○ Forbid access to the internet

Time Group: BusinessHour

MAC Address: CC:3A:61:71:1B:6E

Remark: Purchaser 1

3. Deselect **Allow clients with disabled status or clients not on the list to access the internet through this device**.


MAC Address Filter

MAC Address Filter: ●

□ Filter Mode	MAC Address	Time Group	Remark	Status	Operation
□ Whitelist	CC:3A:61:71:1B:6E	BusinessHour	Purchaser 1	●	✎ 🗑

□ Allow clients with disabled status or clients not on the list to access the internet through this device.

4. Click **Save** at the bottom of the page.

----End

Verification

During 08:00 to 18:00 on weekdays, only the purchaser's computer with MAC address **CC:3A:61:71:1B:6E** can access the internet.

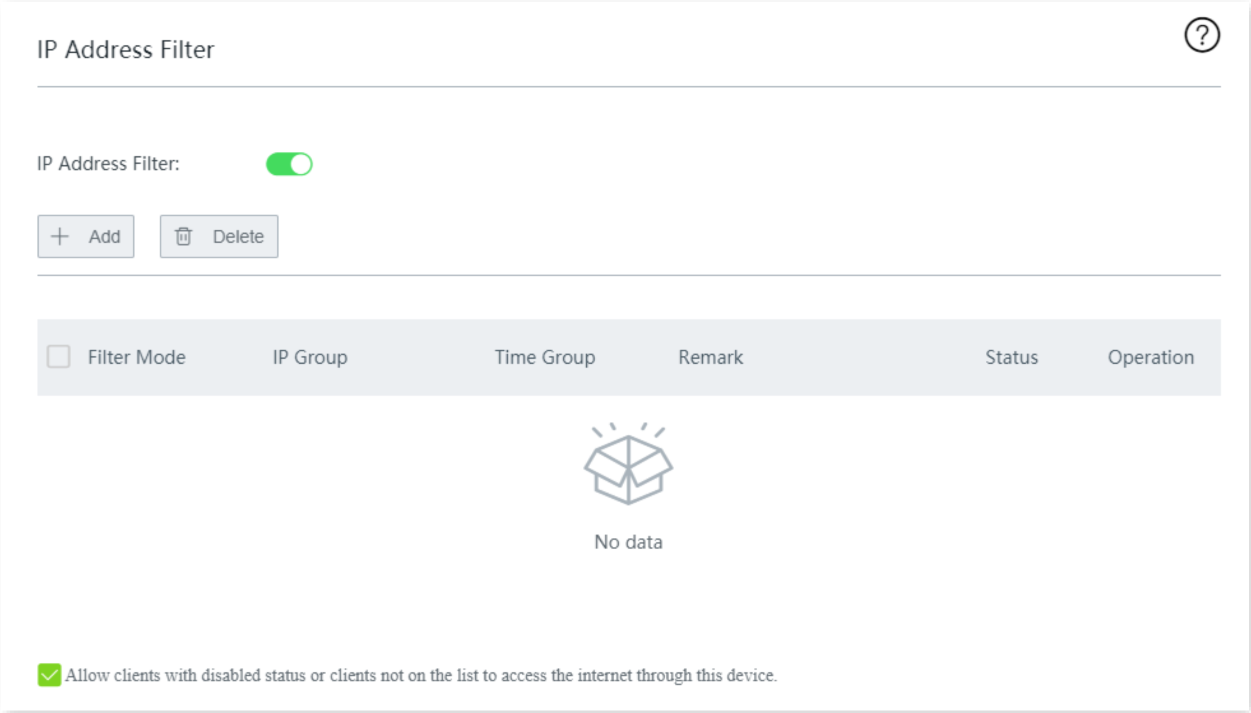
11.3 IP address filter

11.3.1 Overview

Through IP address filter, you can allow or block internet access through this router for specified clients.

Click **Filter Management** > **IP Address Filter** to enter the page.

By default, this function is disabled.



IP Address Filter

IP Address Filter:

☐ Filter Mode	IP Group	Time Group	Remark	Status	Operation

No data

☑ Allow clients with disabled status or clients not on the list to access the internet through this device.

Parameter description

Parameter	Description
IP Address Filter	Enable or disable the IP address filter function.
Filter Mode	Specifies the IP address filter modes. • **Whitelist**: Specifies that internet access is allowed. In this mode, clients with the specified IP address can access the internet only within the specified time period. • **Blacklist**: Specifies that internet access is blocked. In this mode, clients with the specified IP address cannot access the internet only within the specified time period.
IP Group	The IP group used to specify the client to which the rule applies. The IP group rule should be configured in advance on the **Filter Management** > **IP Group/Time Group** page.
Time Group	The time group used to specify the time period during which the rule takes effect. The time group rule should be configured in advance on the **Filter Management** > **IP Group/Time Group** page.

Parameter	Description
Remark	Specifies the remark of the IP address filter rule.
Status	Specifies the status of the IP address filter rule. You can enable or disable the rule as required.
Operation	Specifies the operations you can perform on the rule. ✎: Click it to edit the rule. 🗑 : Click it to delete the rule.
Allow clients with disabled status or clients not on the list to access the internet through this device.	• If this option is selected, clients to which the disabled rules in the list apply and clients not in the list can both access the internet. • If this option is not selected, clients to which the disabled rules in the list apply and clients not in the list can neither access the internet.

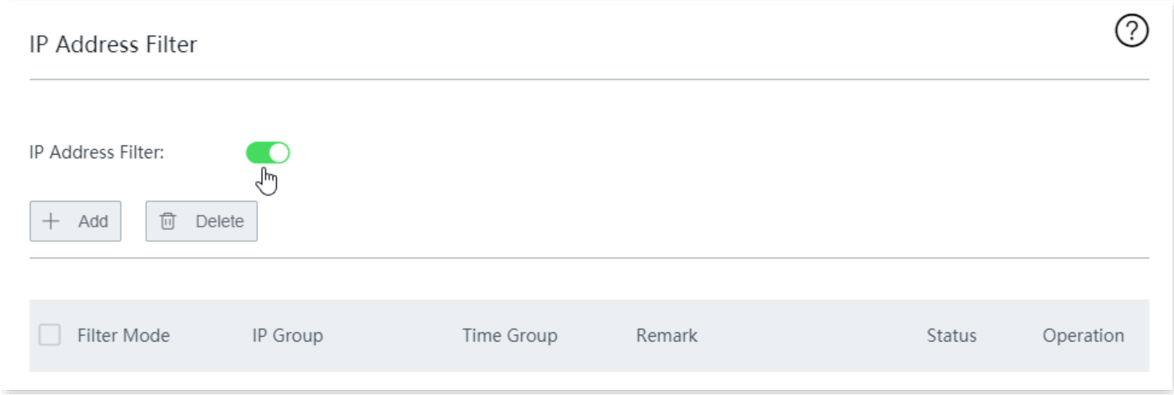
11.3.2 Configure an IP address filter rule

TIP

Before configuring an IP address filter rule, please configure the target IP group and time group first.

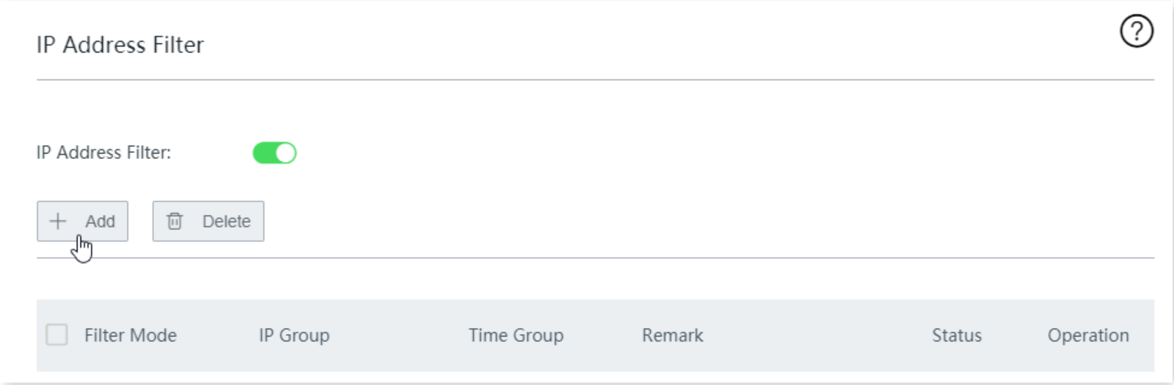
Step 1 Enable IP address filter.

1. Navigate to **Filter Management** > **IP Address Filter**.
2. Enable **IP Address Filter**, and click **Save** at the bottom of the page.

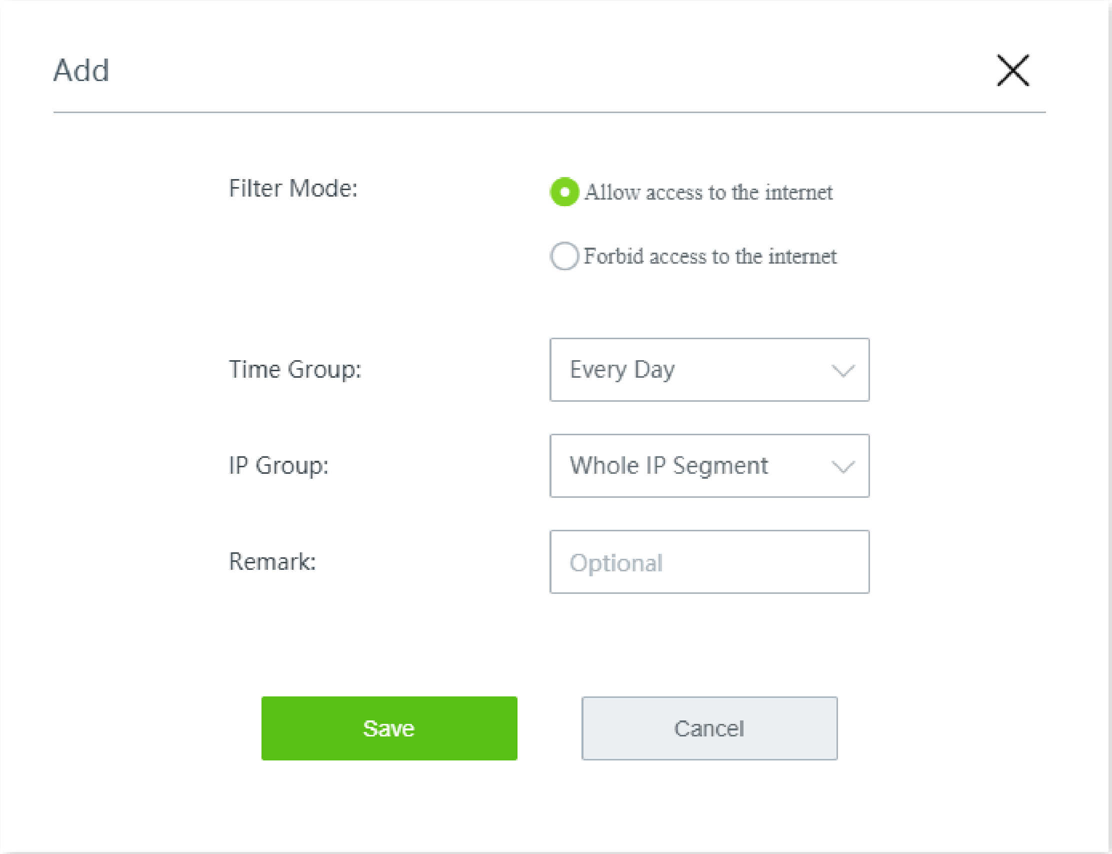


Step 2 Add an IP address filter rule.

1. Click **+Add**.



2. Configure the following parameters in the **Add** window, and click **Save**.



Add

Filter Mode: ● Allow access to the internet ○ Forbid access to the internet

Time Group: Every Day

IP Group: Whole IP Segment

Remark: Optional

----End

11.3.3 Example of configuring an IP address filter rule

Networking requirement

An enterprise uses the wireless router to build a network.

Requirement:

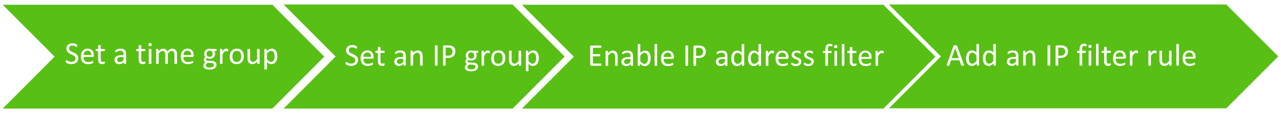
During business hours (08:00 to 18:00 on weekdays), only purchasers are allowed to access the internet.

Solution

The IP address filter can meet this requirement.

Assume that the IP addresses of the purchasers' computers range from 192.168.0.2 to 192.168.0.10.

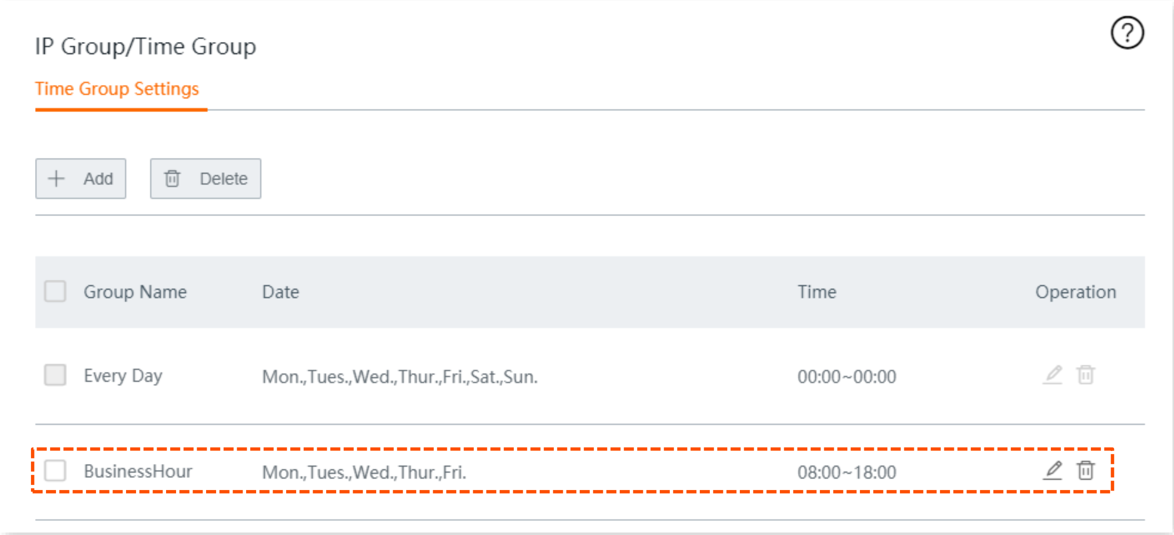
Configuration procedure



Set a time group → Set an IP group → Enable IP address filter → Add an IP filter rule

Step 1 Set a time group.

Navigate to **Filter Management** > **IP Group/Time Group**. Set a time group shown in the following figure.


IP Group/Time Group

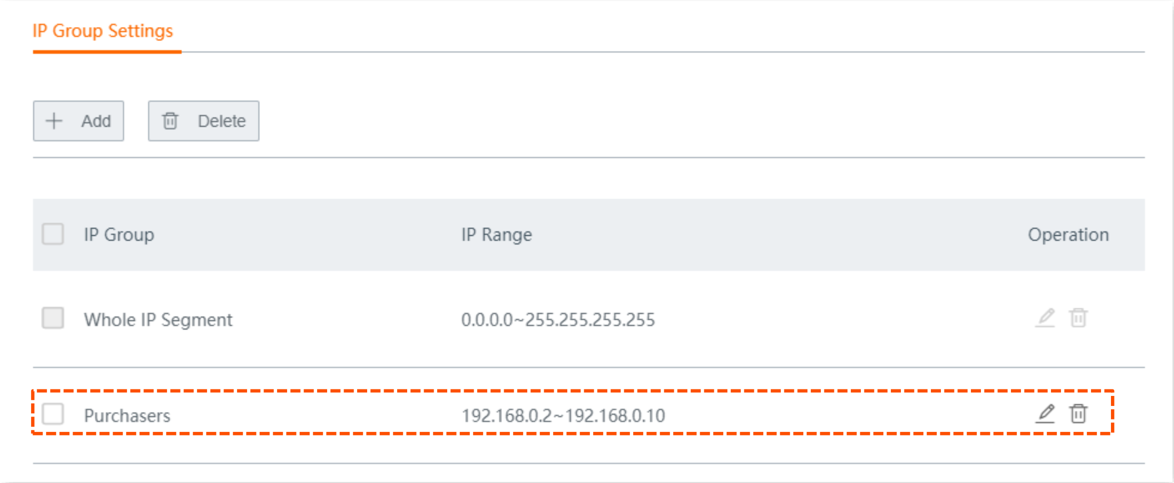
Time Group Settings

+ Add　Delete

□	Group Name	Date	Time	Operation
□	Every Day	Mon.,Tues.,Wed.,Thur.,Fri.,Sat.,Sun.	00:00~00:00	
□	BusinessHour	Mon.,Tues.,Wed.,Thur.,Fri.	08:00~18:00	

Step 2 Set an IP group.

Navigate to **Filter Management** > **IP Group/Time Group**. Set an IP group shown in the following figure.

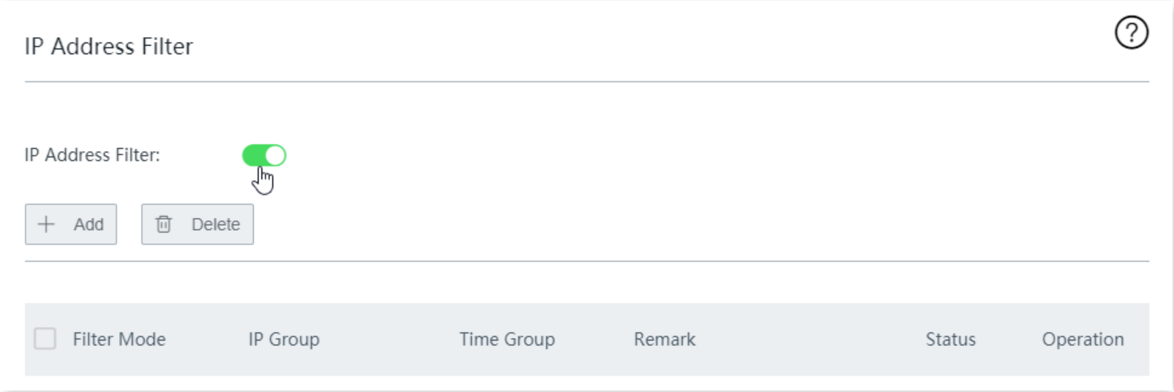

IP Group Settings

+ Add　Delete

□	IP Group	IP Range	Operation
□	Whole IP Segment	0.0.0.0~255.255.255.255	
□	Purchasers	192.168.0.2~192.168.0.10	

Step 3 Enable IP address filter.

1. Navigate to **Filter Management** > **IP Address Filter**.
2. Enable **IP Address Filter**, and click **Save** at the bottom of the page.


IP Address Filter

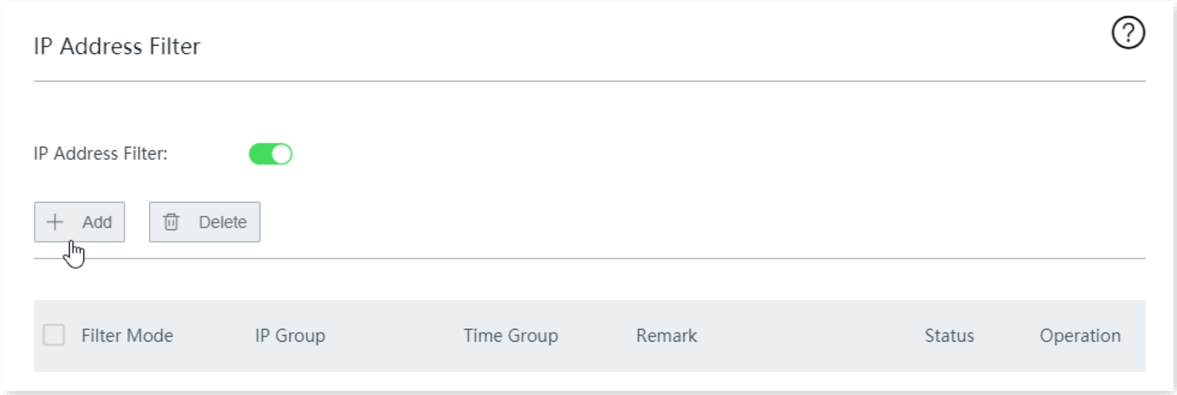
IP Address Filter:

+ Add　Delete

□	Filter Mode	IP Group	Time Group	Remark	Status	Operation

Step 4 Add an IP address filter rule.

1. Click **+Add**.



IP Address Filter

IP Address Filter: ●

□ Filter Mode	IP Group	Time Group	Remark	Status	Operation

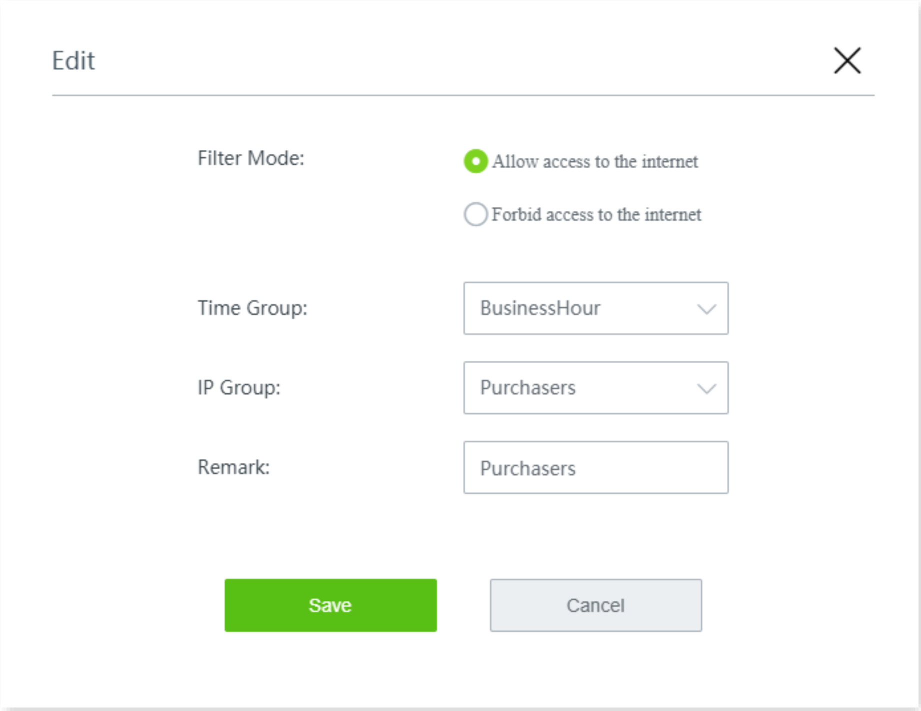
2. Configure the following parameters, and click **Save**.

   (1) Set **Filter Mode** to **Allow access to the internet** (whitelist).

   (2) Select the target **Time Group**, which is **BusinessHour** in this example.

   (3) Select the target **IP Group**, which is **Purchasers** in this example.

   (4) (Optional) Enter a **Remark** for the rule, for example, **Purchasers**.



Edit

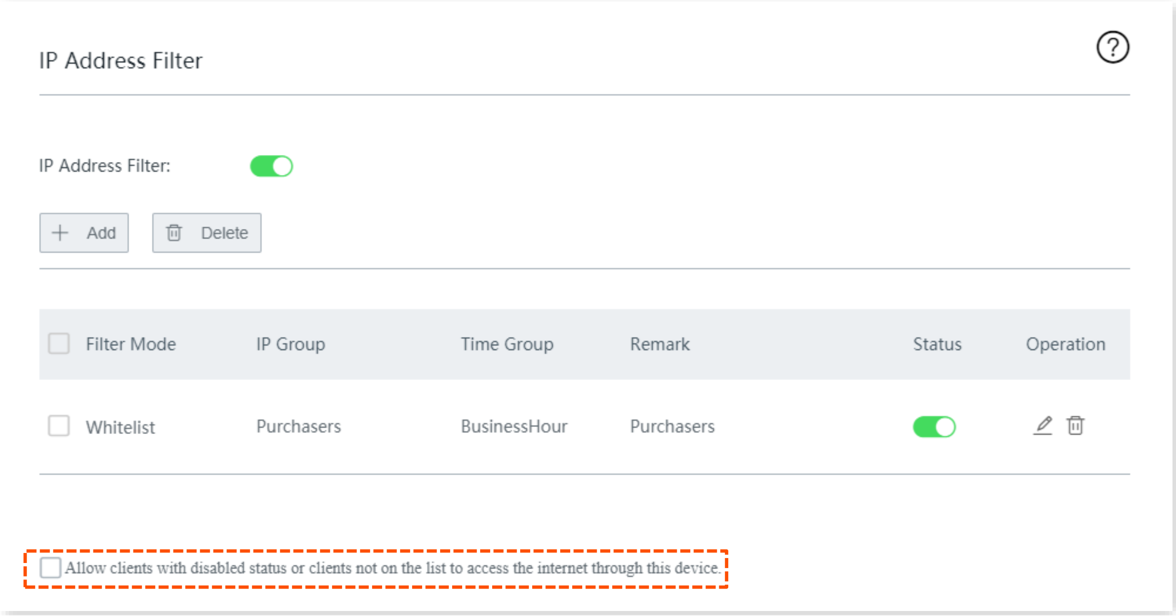
Filter Mode: ● Allow access to the internet ○ Forbid access to the internet

Time Group: BusinessHour

IP Group: Purchasers

Remark: Purchasers

3. Deselect **Allow clients with disabled status or clients not on the list to access the internet through this device**.



IP Address Filter

IP Address Filter: ●

＋ Add | Delete

□ Filter Mode	IP Group	Time Group	Remark	Status	Operation
□ Whitelist	Purchasers	BusinessHour	Purchasers	●	

□ Allow clients with disabled status or clients not on the list to access the internet through this device.

4. Click **Save** at the bottom of the page.

----End

Verification

During 08:00 to 18:00 on weekdays, only the purchasers' computers with IP addresses ranging from 192.168.0.2 to 192.168.0.10 can access the internet.

11.4 Port filter

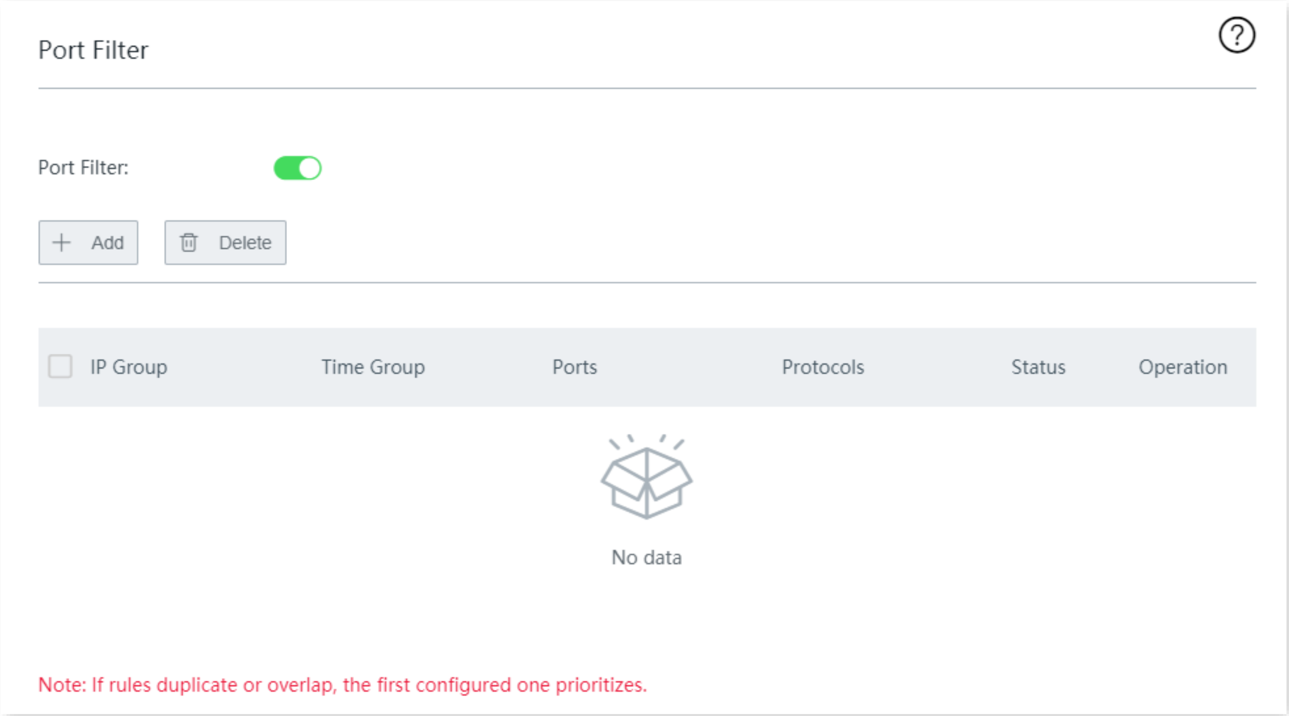
11.4.1 Overview

The protocols of various services available over the internet use dedicated port numbers. The common service port numbers range from 0 to 1023 and are generally assigned to specific services.

The port filter prevents LAN users from accessing certain internet services by disabling the users to access the port numbers of the services.

Click **Filter Management** > **Port Filter** to enter the page.

By default, this function is disabled.



Port Filter

Port Filter: ●

□ IP Group	Time Group	Ports	Protocols	Status	Operation

No data

Note: If rules duplicate or overlap, the first configured one prioritizes.

Parameter description

Parameter	Description
Port Filter	Enable or disable the port filter function.
IP Group	Specifies the IP group used to specify the client to which the rule applies. The IP group rule should be configured in advance on the **Filter Management** > **IP Group/Time Group** page.
Time Group	Specifies the time group used to specify the time period during which the rule is effective. The time group rule should be configured in advance on the **Filter Management** > **IP Group/Time Group** page.
Ports	Specifies the TCP or UDP port number used by the service to be blocked.
Protocols	Specifies the protocol used by the service to be blocked. **All** indicates TCP and UDP.

Parameter	Description
Status	Specifies the status of the port filter rule. You can enable or disable the rule as required.
Operation	Specifies the operations you can perform on the rule. ✎: Click it to edit the rule. 🗑 : Click it to delete the rule.

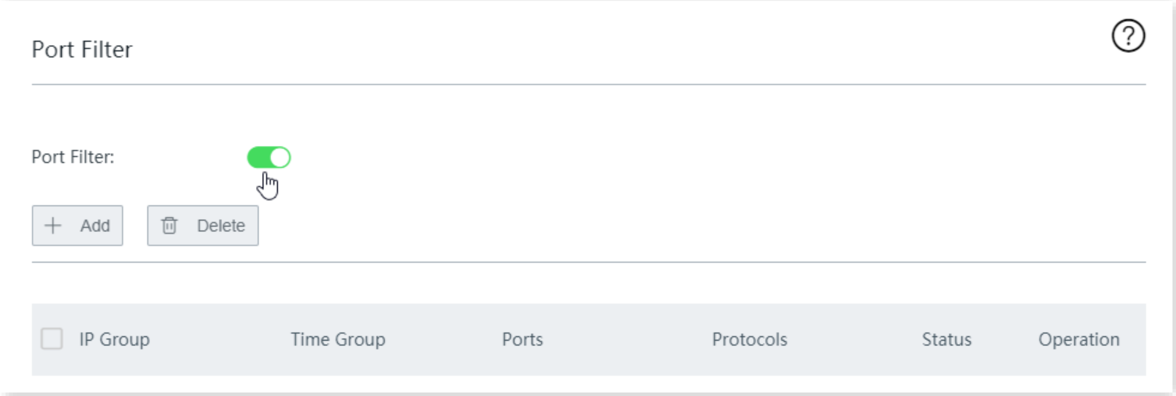
11.4.2 Configure a port filter rule

TIP

Before configuring a port filter rule, please configure the target IP group and time group first.

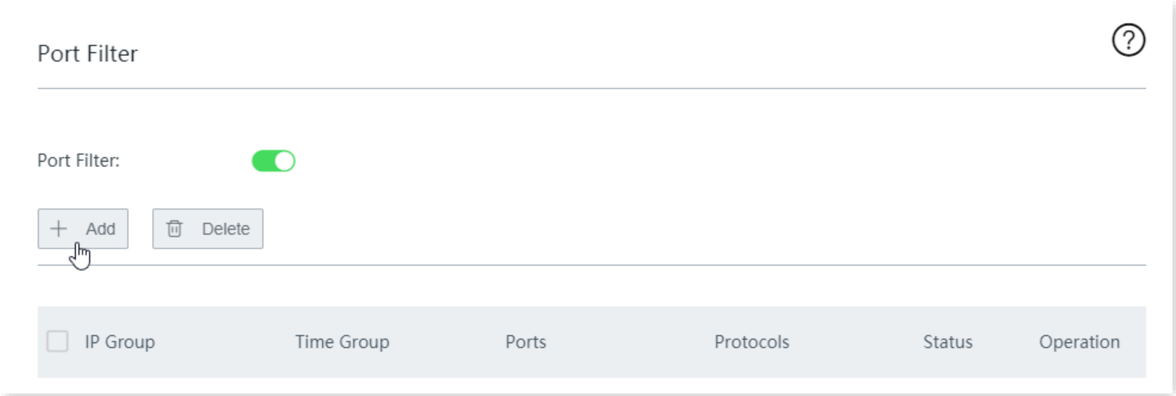
Step 1 Enable port filter.

1. Navigate to **Filter Management** > **Port Filter**.
2. Enable this function, and click **Save** at the bottom of the page.

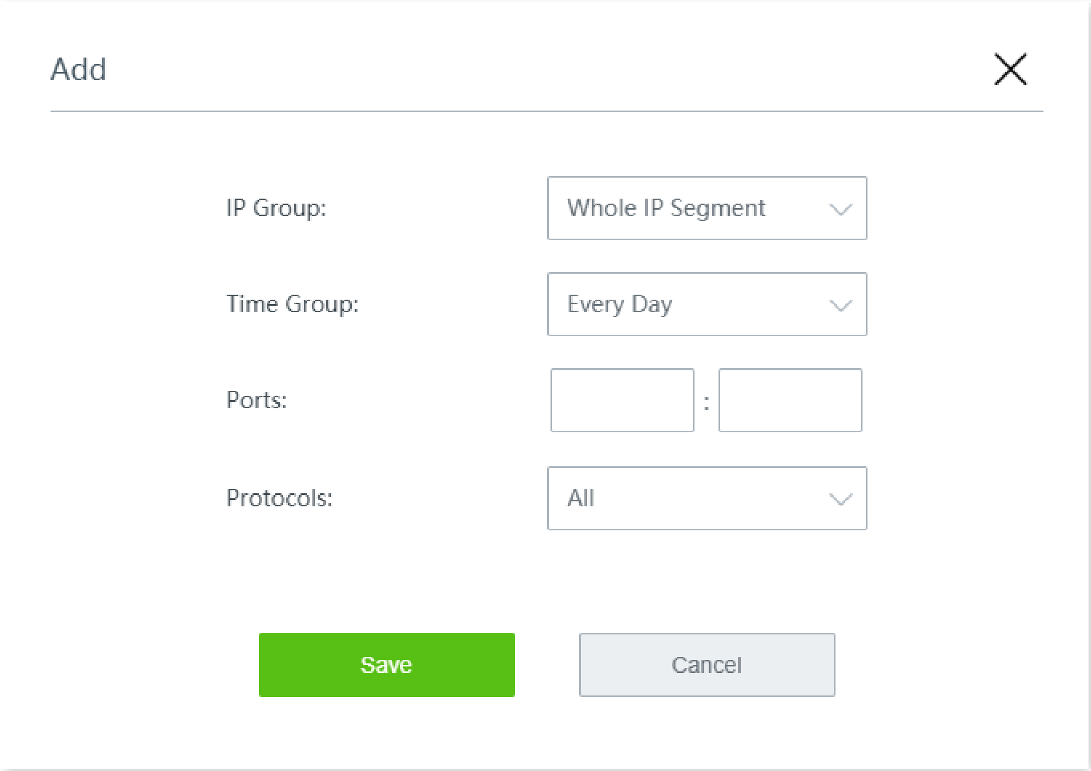


Step 2 Add a port filter rule.

1. Click **+Add**.



2. Configure the following parameters in the **Add** window, and click **Save**.



Add

IP Group: Whole IP Segment

Time Group: Every Day

Ports: :

Protocols: All

----End

11.4.3 Example of configuring a port filter rule

Networking requirement

An enterprise uses the wireless router to build a network.

Requirement:

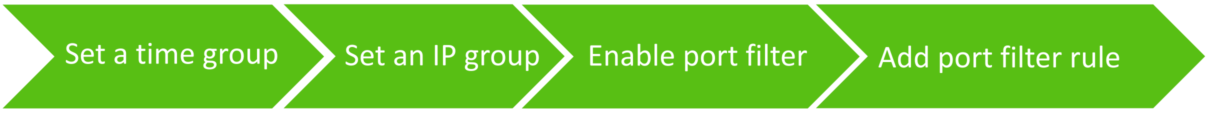
During business hours (08:00 to 18:00 on weekdays), webpage browsing is forbidden for finance department staff (The default port number of the webpage browsing service is 80).

Solution

The port filter can meet this requirement.

Assume that the IP addresses of the finance department staff range from 192.168.0.2 to 192.168.0.10.

Configuration procedure



Set a time group

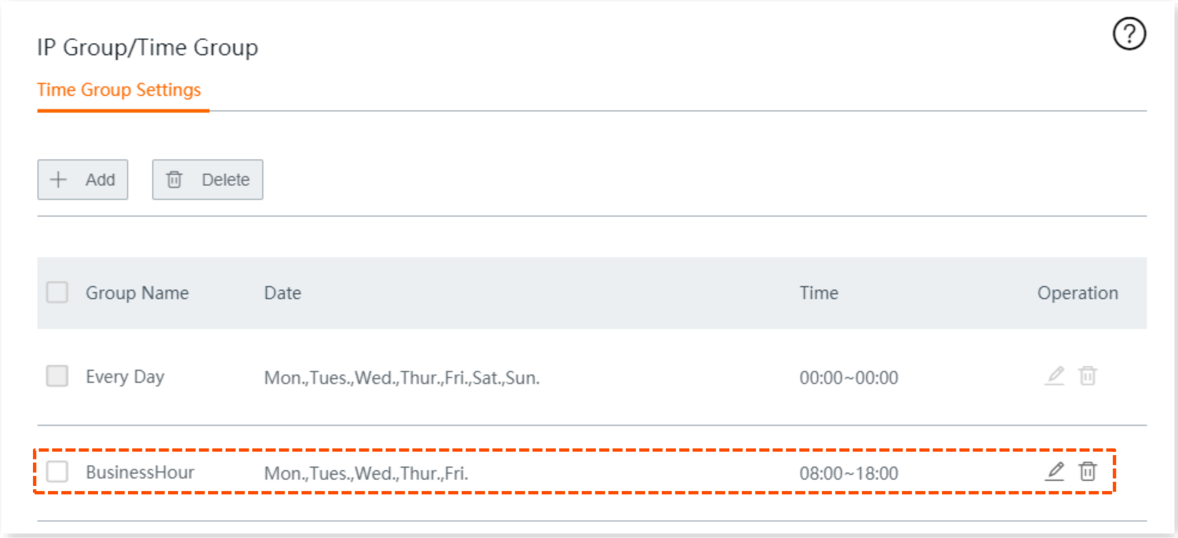
Set an IP group

Enable port filter

Add port filter rule

Step 1 Set a time group.

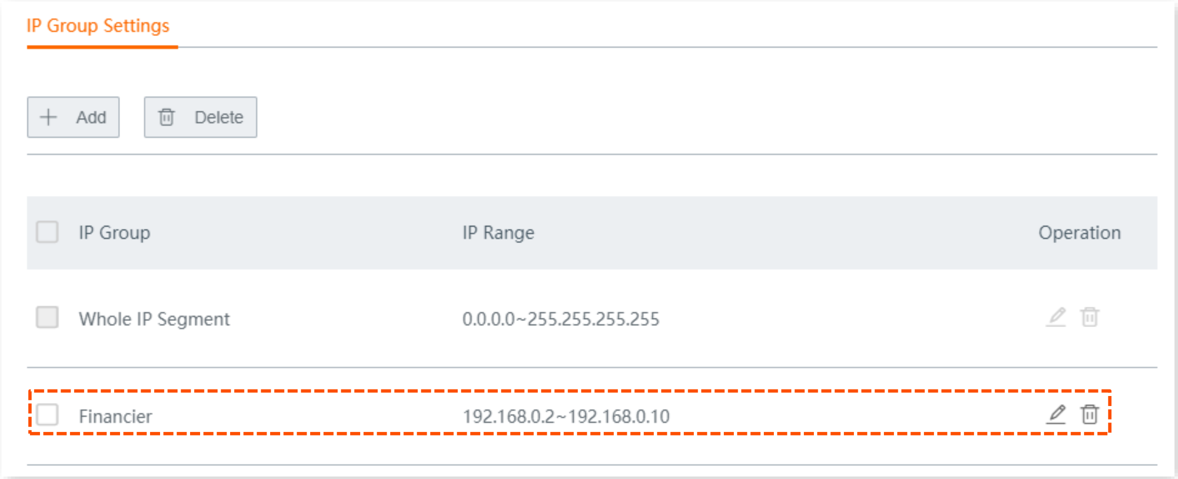
Navigate to **Filter Management** > **IP Group/Time Group**. Set a time group shown in the following figure.



□	Group Name	Date	Time	Operation
□	Every Day	Mon.,Tues.,Wed.,Thur.,Fri.,Sat.,Sun.	00:00~00:00	
□	BusinessHour	Mon.,Tues.,Wed.,Thur.,Fri.	08:00~18:00	

Step 2 Set an IP group.

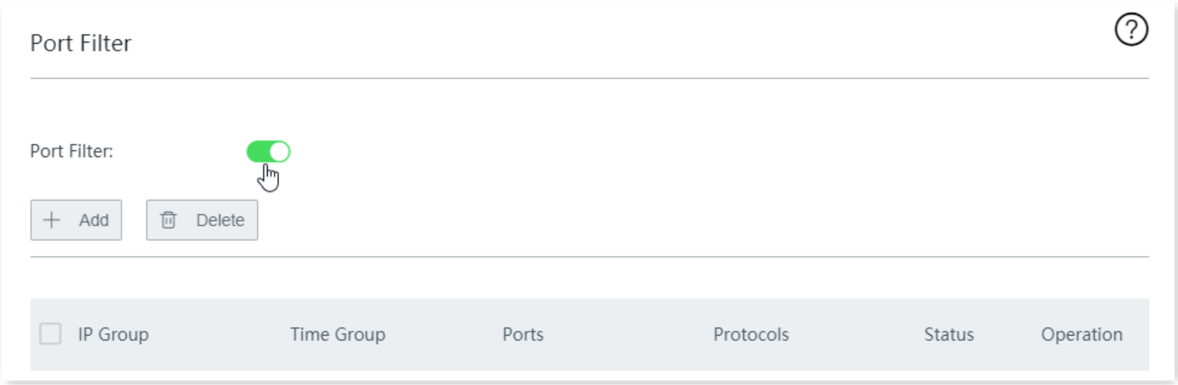
Navigate to **Filter Management** > **IP Group/Time Group**. Set an IP group shown in the following figure.



□	IP Group	IP Range	Operation
□	Whole IP Segment	0.0.0.0~255.255.255.255	
□	Financier	192.168.0.2~192.168.0.10	

Step 3 Enable port filter.

1. Navigate to **Filter Management** > **Port Filter**.
2. Enable **Port Filter**, and click **Save** at the bottom of the page.

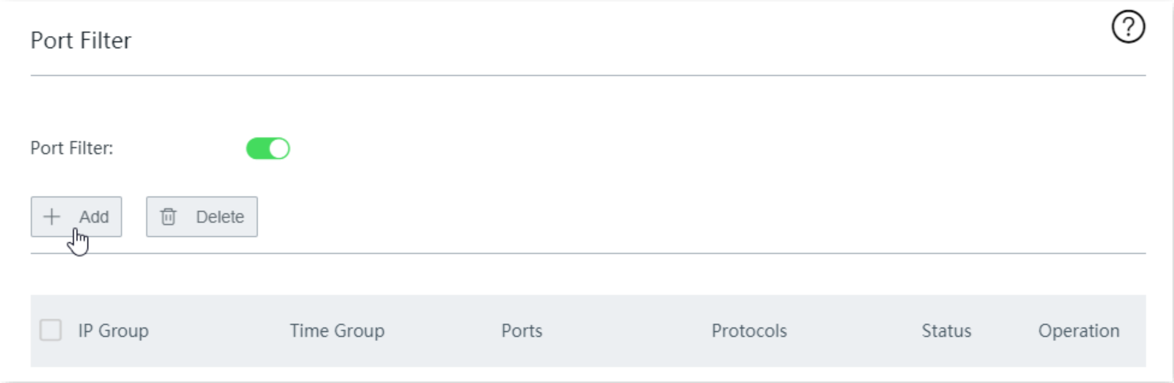


Port Filter: ●

□	IP Group	Time Group	Ports	Protocols	Status	Operation

Step 4 Add a port filter rule.

1. Click **+Add**.



Port Filter

Port Filter: ●

□ IP Group	Time Group	Ports	Protocols	Status	Operation

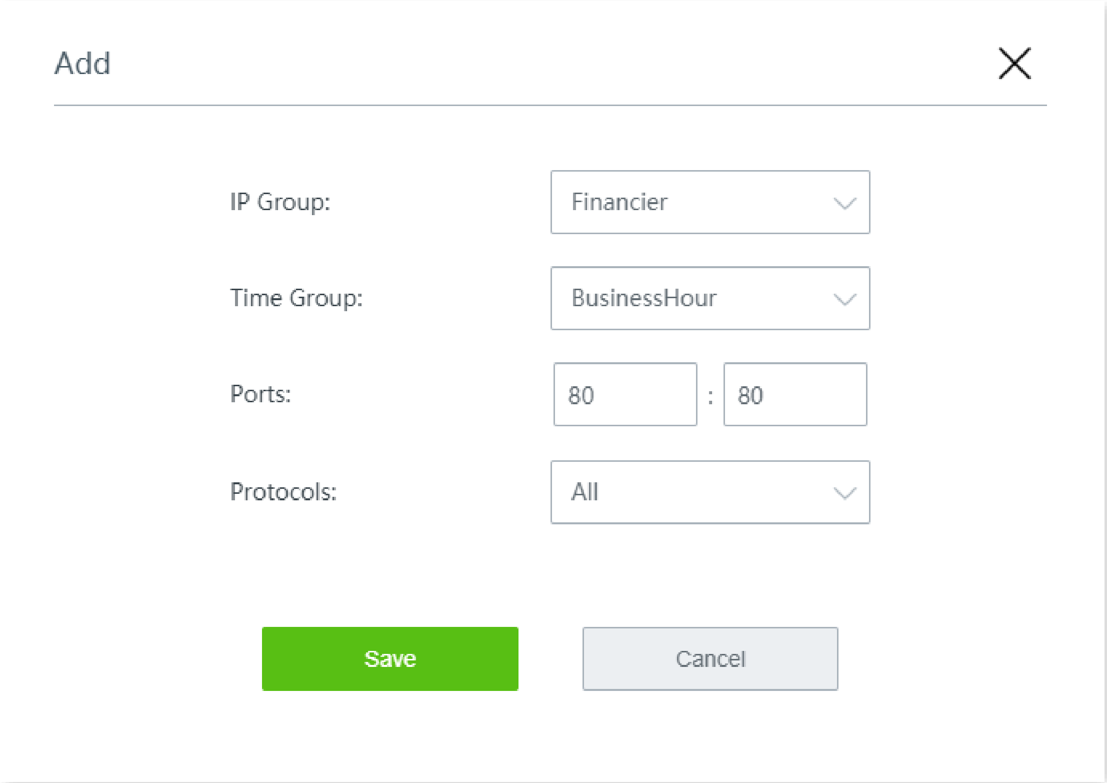
2. Configure the following parameters, and click **Save**.

   (1) Select the target **IP Group**, which is **Financier** in this example.

   (2) Select the target **Time Group**, which is **BusinessHour** in this example.

   (3) Enter the port number used by the webpage browsing service, which is **80**.

   (4) Select the protocol used by the service. You are recommended to retain the default option **All**.



Add

IP Group: Financier

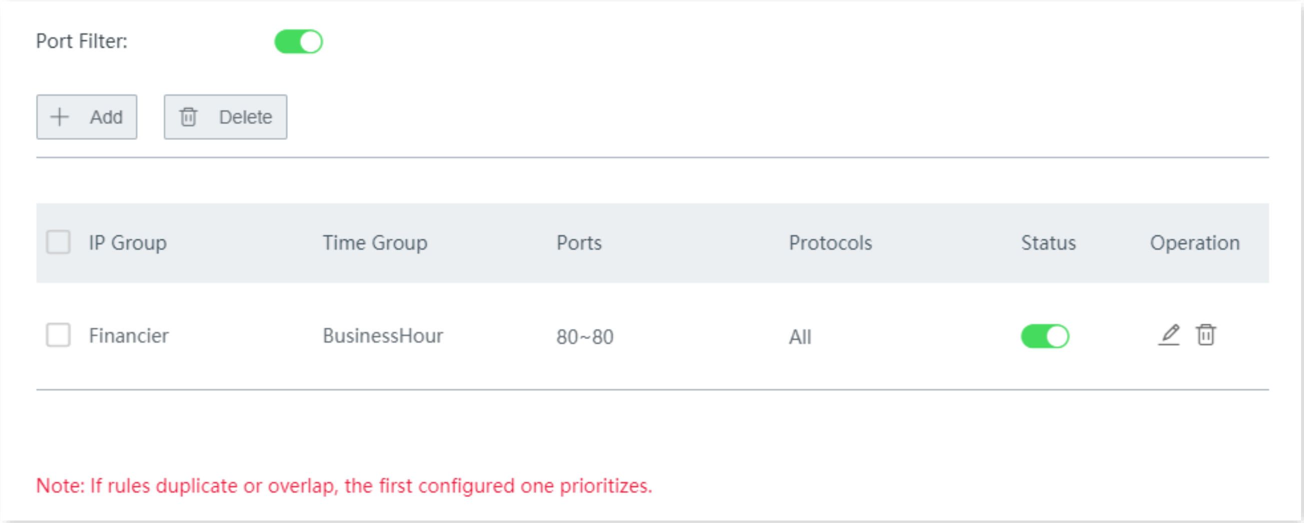
Time Group: BusinessHour

Ports: 80 : 80

Protocols: All

----End

Added successfully. See the following figure.



Port Filter:

□ IP Group	Time Group	Ports	Protocols	Status	Operation
□ Financier	BusinessHour	80~80	All	●	

Note: If rules duplicate or overlap, the first configured one prioritizes.

Verification

During 08:00 to 18:00 on weekdays, in the LAN network, the computers with IP addresses ranging from 192.168.0.2 to 192.168.0.100 cannot browse web pages.

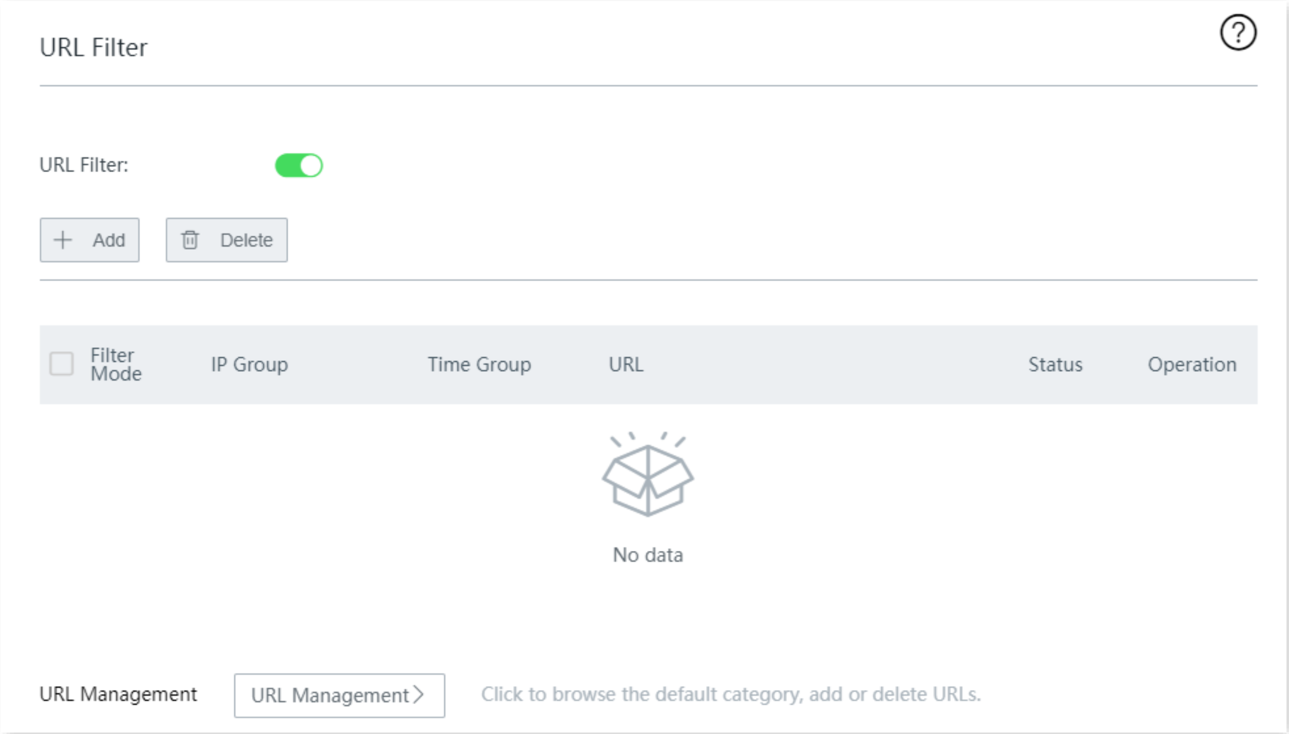
11.5 URL filter

11.5.1 Overview

The URL filter prevents LAN users from accessing specified types of website and controls internet accessibility of LAN users so that they will not spend time on websites irrelevant to their duties. Before you add web filter rules, add web categories.

Click **Filter Management** > **URL Filter** to enter the page.

By default, this function is disabled.



URL Filter

URL Filter:

□ Filter Mode	IP Group	Time Group	URL	Status	Operation

No data

URL Management Click to browse the default category, add or delete URLs.

Parameter description

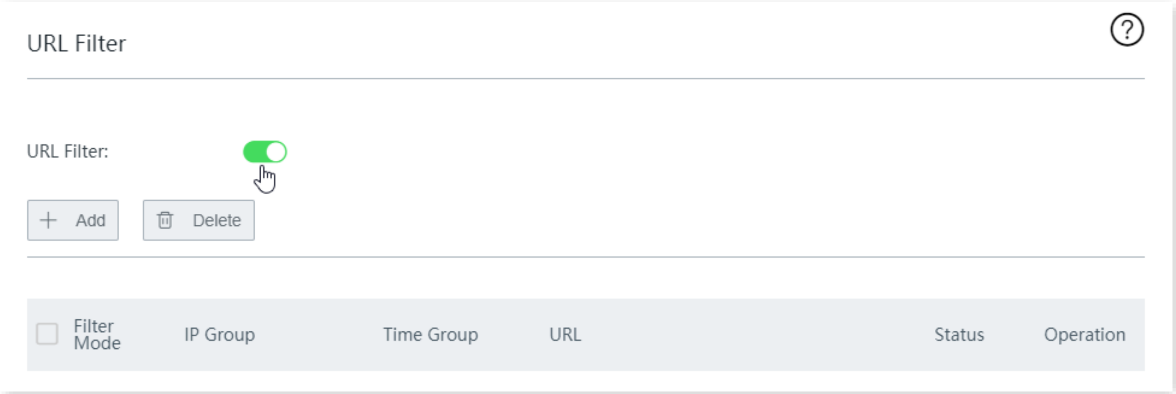
Parameter	Description
URL Filter	Enable or disable the URL filter function.
Filter Mode	Specifies the URL filter modes. • **Allow access only**: It specifies that internet access is allowed. In this mode, clients in the IP group can access only the specified website and cannot access other websites during the specified time period. During other time periods, the clients can access all the websites. • **Block access only**: It specifies that internet access is blocked. In this mode, clients in the IP group cannot access only the specified website and can access other websites during the specified time period. During other time periods, the clients can access all the websites.
IP Group	The IP group used to specify the client to which the rule applies. The IP group rule should be configured in advance on the **Filter Management** > **IP Group/Time Group** page.

Parameter	Description
Time Group	The time group used to specify the time period during which the rule takes effect. The time group rule should be configured in advance on the **Filter Management** > **IP Group/Time Group** page.
URL	Specifies the URL category the rule uses. The URL category should be configured in advance.
Status	Specifies the status of the URL filter rule. You can enable or disable the rule as required.
Operation	Specifies the operations you can perform on the rule. ✎: Click it to edit the rule. 🗑 : Click it to delete the rule.
URL Management	Specifies the customized URL category. TIP The device does not have a pre-set default URL category.

11.5.2 Customize a URL group

Step 1 Enable URL filter.

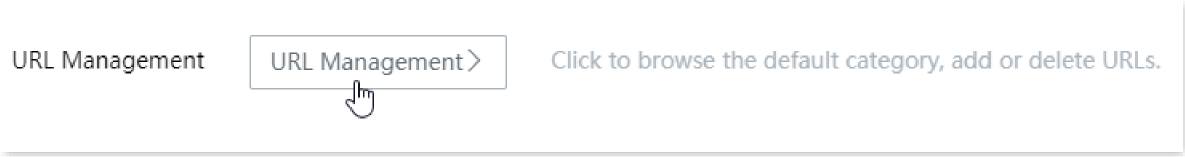
1. Navigate to **Filter Management** > **URL Filter**.
2. Enable **URL Filter**, and click **Save** at the bottom of the page.


URL Filter

URL Filter: ●

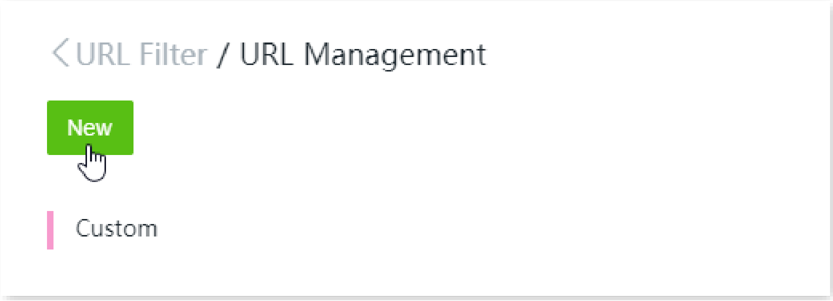
Step 2 Add a customized URL group.

1. Click **URL Management**.

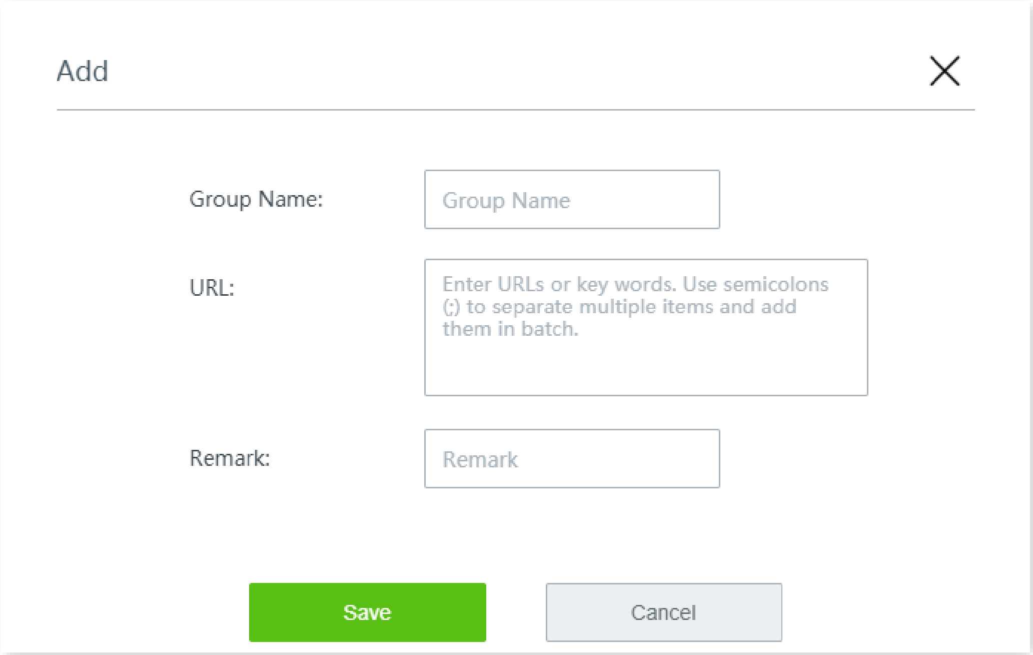

URL Management

Click to browse the default category, add or delete URLs.

2. Click **New**.



3. Configure the following parameters in the **Add** window, and click **Save**.



Add
Group Name:
Group Name
URL:
Enter URLs or key words. Use semicolons (;) to separate multiple items and add them in batch.
Remark:
Remark
Save
Cancel

----End

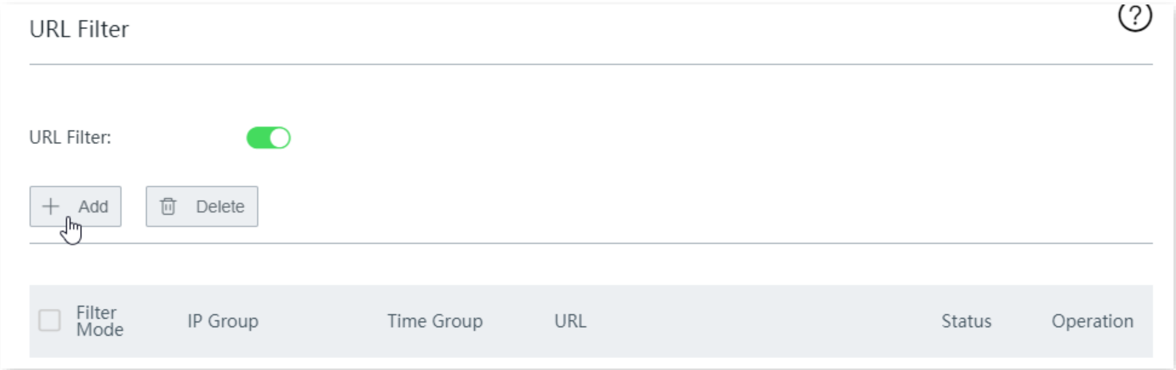
11.5.3 Configure a URL filter rule

TIP

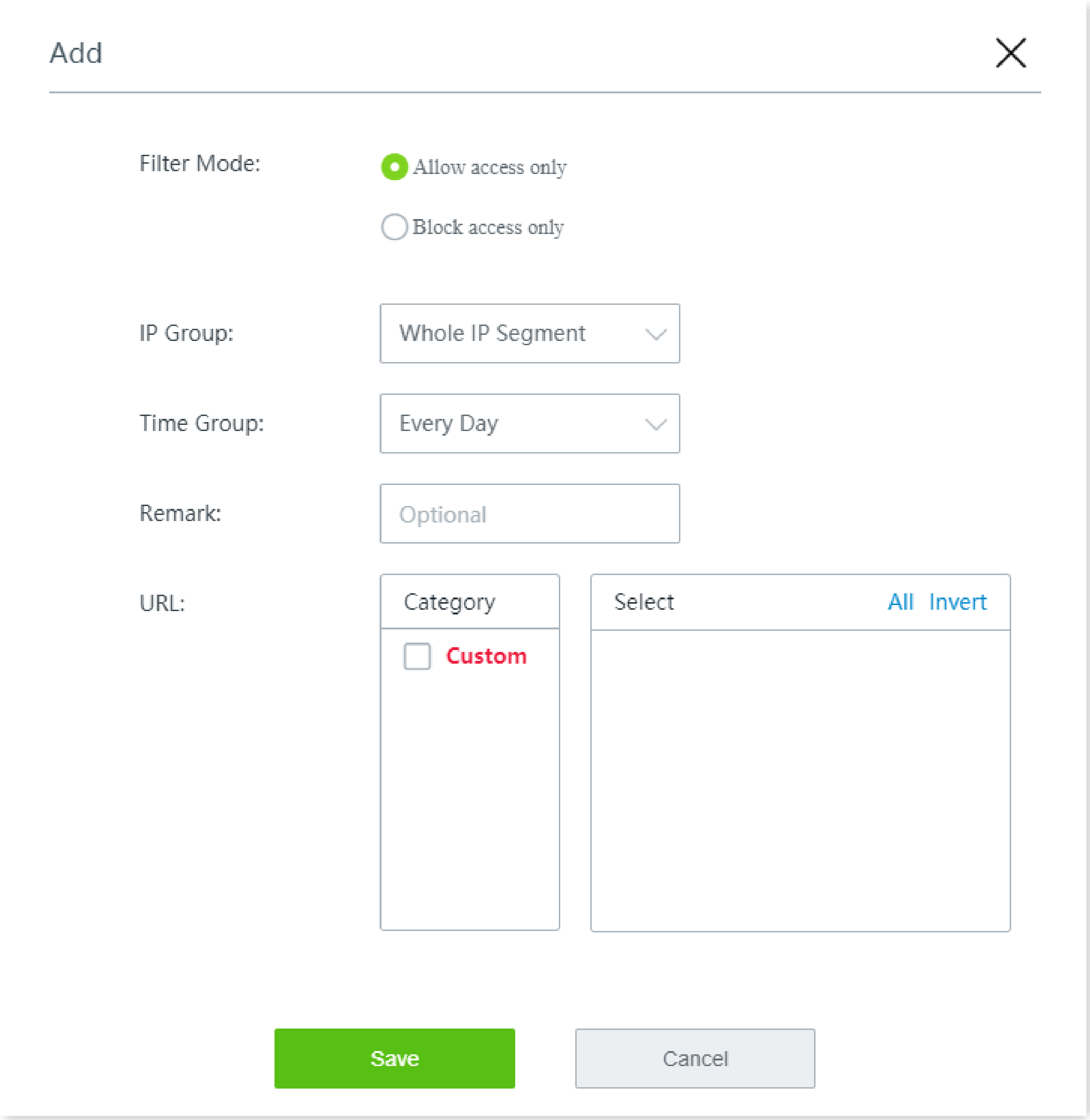
Before configuring a URL filter rule, please configure the target IP group and time group first.

Step 1 Navigate to **Filter Management** > **URL Filter**.

Step 2 Click **+Add**.



Step 3 Configure the following parameters in the **Add** window, and click **Save**.



Add

Filter Mode: ● Allow access only ○ Block access only

IP Group: Whole IP Segment

Time Group: Every Day

Remark: Optional

URL:

Category

□ Custom

----End

11.5.4 Example of configuring a URL filter rule

Networking requirement

An enterprise uses the wireless router to build a network.

Requirement:

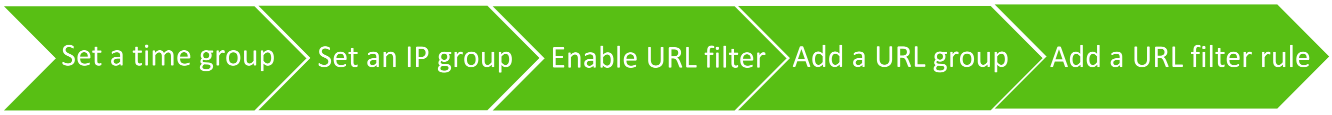
During business hours (08:00 to 18:00 on weekdays), designing department staff are disallowed to access social media like Facebook and Tumblr.

Solution

The URL filter can meet this requirement.

Assume that the IP addresses of the designing department staff's computers range from 192.168.0.2 to 192.168.0.10.

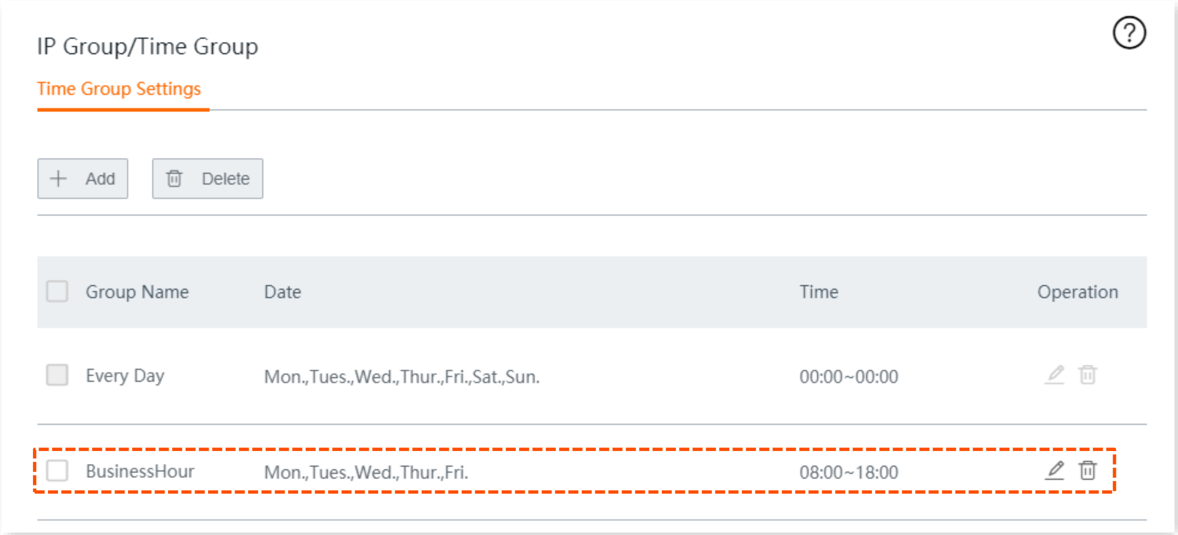
Configuration procedure



Set a time group > Set an IP group > Enable URL filter > Add a URL group > Add a URL filter rule

Step 1 Set a time group.

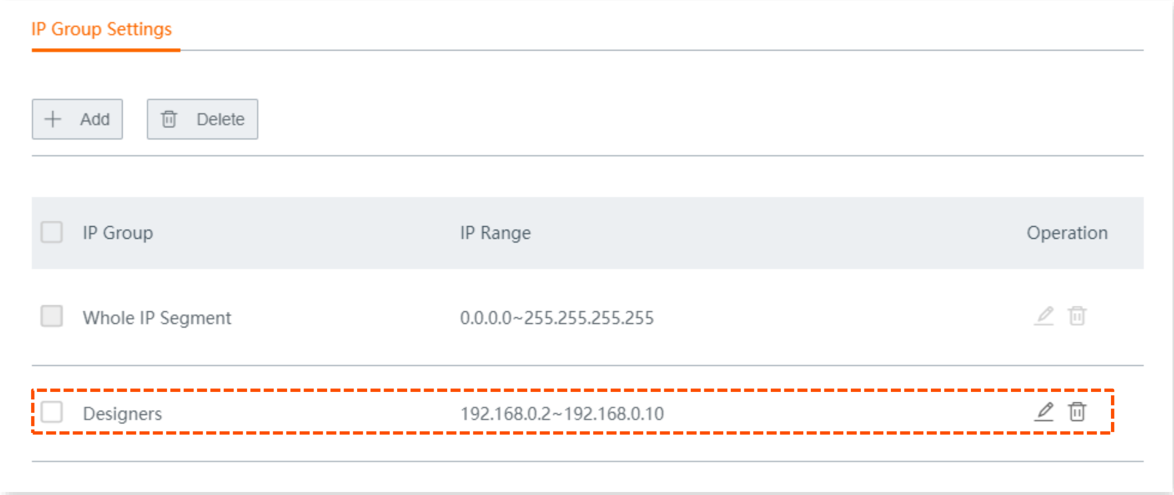
Navigate to **Filter Management** > **IP Group/Time Group**. Set a time group shown in the following figure.



☐ Group Name	Date	Time	Operation
☐ Every Day	Mon.,Tues.,Wed.,Thur.,Fri.,Sat.,Sun.	00:00~00:00	
☐ BusinessHour	Mon.,Tues.,Wed.,Thur.,Fri.	08:00~18:00	

Step 2 Set an IP group.

Navigate to **Filter Management** > **IP Group/Time Group**. Set an IP group shown in the following figure.

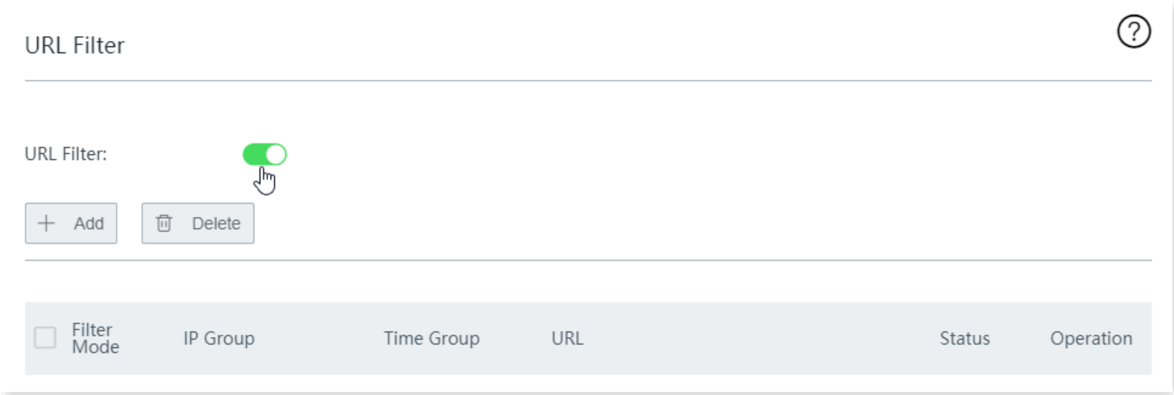


IP Group Settings

□	IP Group	IP Range	Operation
□	Whole IP Segment	0.0.0.0~255.255.255.255	
□	Designers	192.168.0.2~192.168.0.10	

Step 3 Enable URL filter.

1. Navigate to **Filter Management** > **URL Filter**.
2. Enable **URL Filter**, and click **Save** at the bottom of the page.



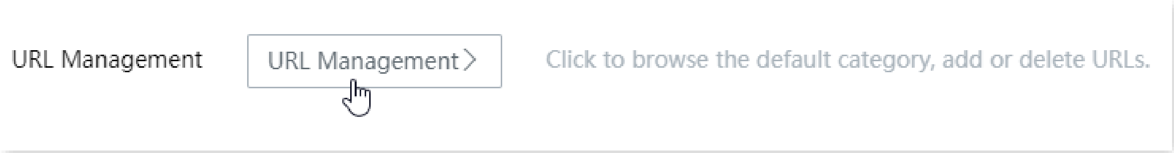
URL Filter

URL Filter:

□	Filter Mode	IP Group	Time Group	URL	Status	Operation

Step 4 Add a customized URL group.

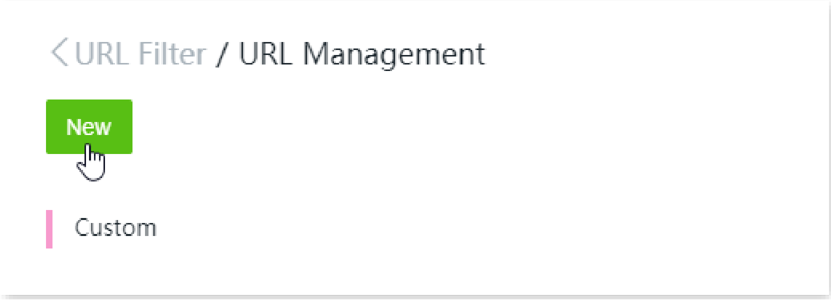
1. Click **URL Management**.



URL Management

Click to browse the default category, add or delete URLs.

2. Click **New**.



< URL Filter / URL Management

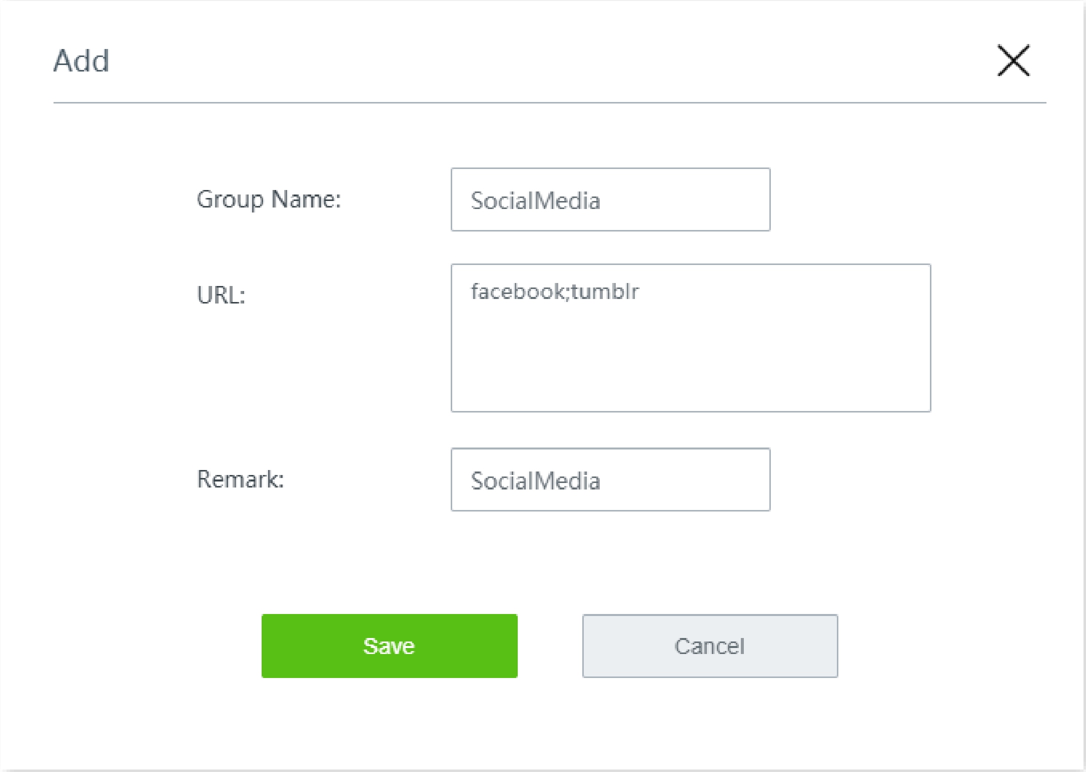
Custom

3. Configure the following parameters in the **Add** window, and click **Save**.

   (1) Enter the **Group Name**, which is **SocialMedia** in this example.

   (2) Enter the keywords of the domain name of the website to be blocked, which are **facebook;tumblr** in this example.

   (3) Enter a **Remark** for the URL group, for example, **SocialMedia**.



Add

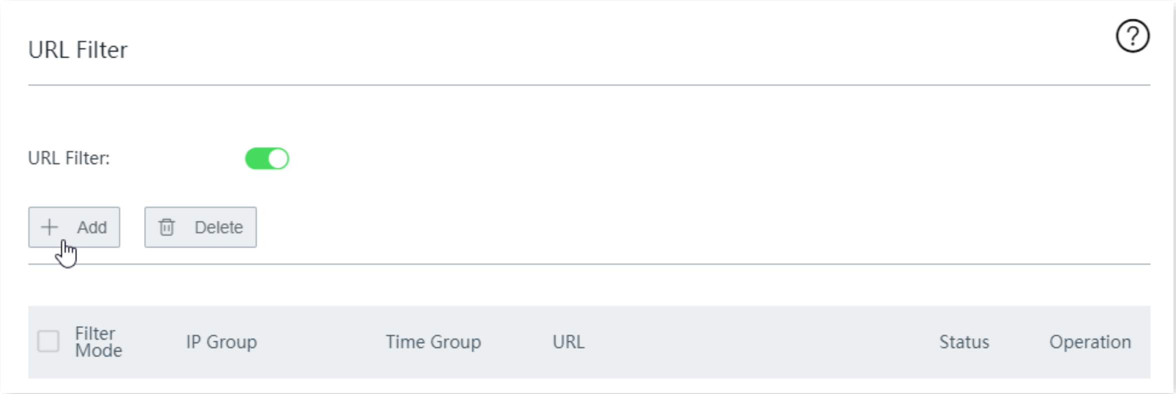
Group Name: SocialMedia

URL: facebook;tumblr

Remark: SocialMedia

Step 5 Add a URL filter rule.

1. Click **+Add**.



URL Filter

URL Filter: ●

Filter Mode	IP Group	Time Group	URL	Status	Operation

2. Configure the following parameters, and click **Save**.

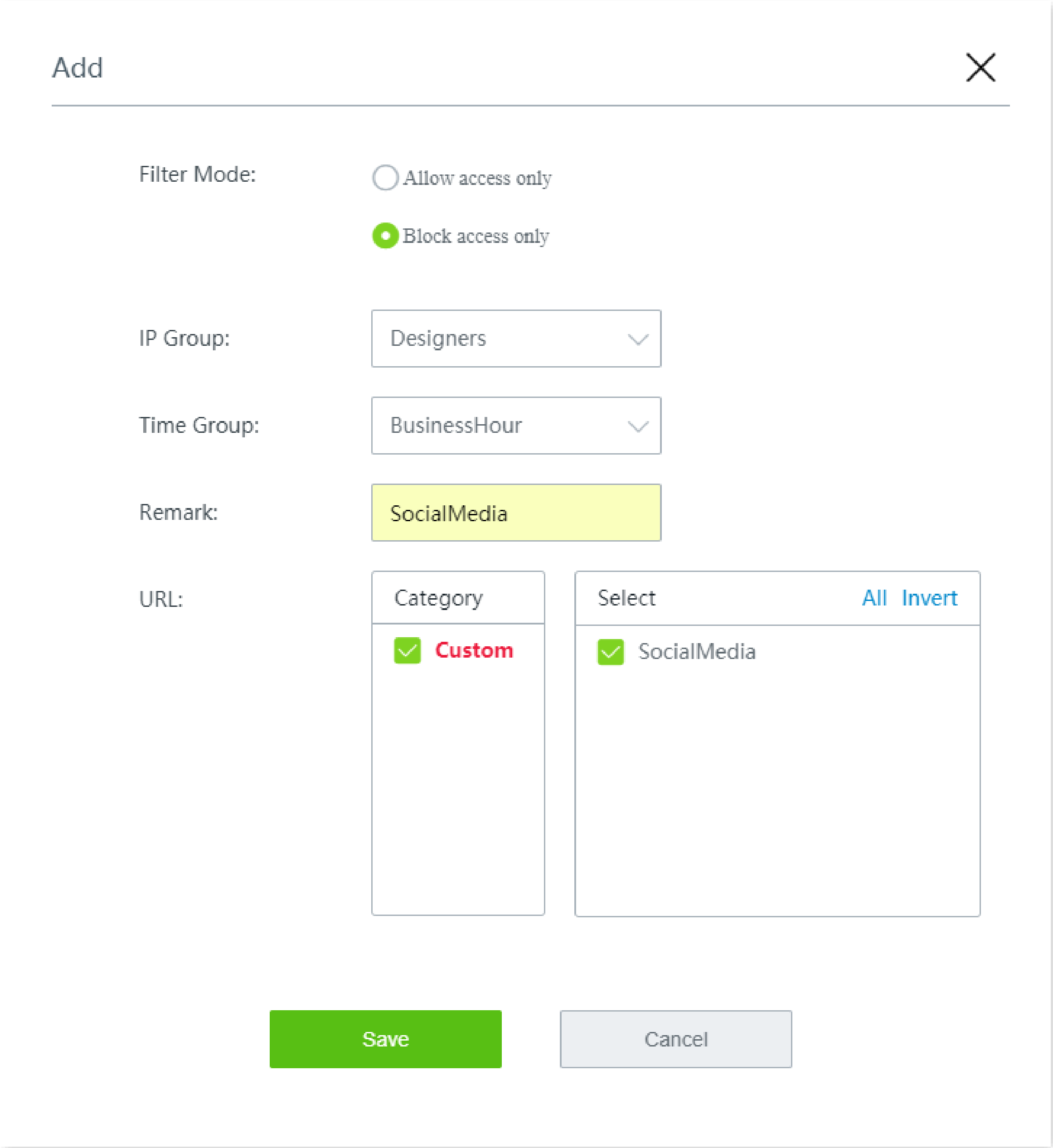
   (1) Set **Filter Mode** to **Block access only**.

   (2) Select the target **IP Group**, which is **Designers** in this example.

   (3) Select the target **Time Group**, which is **BusinessHour** in this example.

   (4) (Optional) Enter a **Remark** for the URL filter rule. You can also choose to leave it blank.

   (5) Select the target URL, which is **SocialMedia** in this example.



Add

Filter Mode: ○ Allow access only ● Block access only

IP Group: Designers

Time Group: BusinessHour

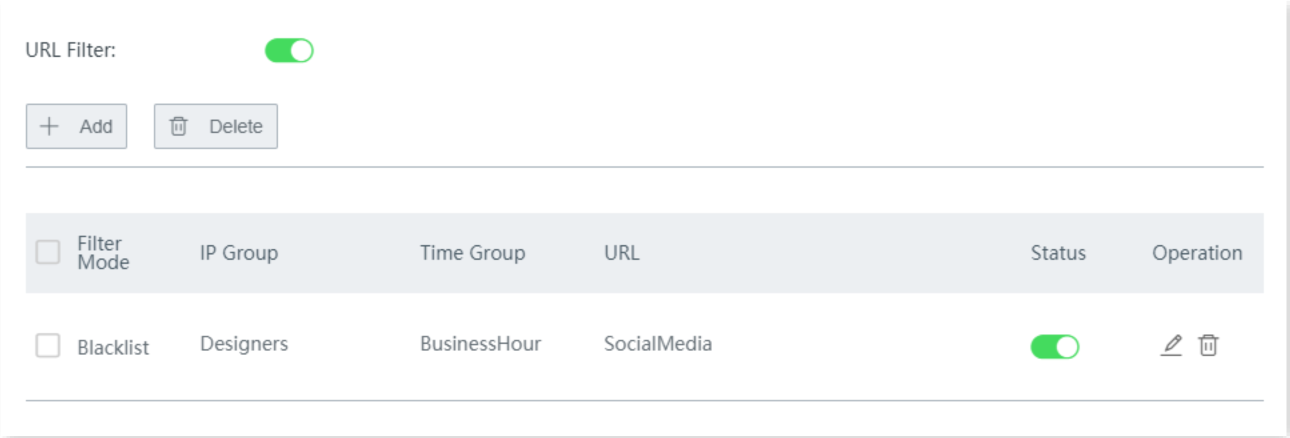
Remark: SocialMedia

URL:

Category	Select
☑ Custom	☑ SocialMedia

----End

Added successfully. See the following figure.



URL Filter: ●

□	Filter Mode	IP Group	Time Group	URL	Status	Operation
□	Blacklist	Designers	BusinessHour	SocialMedia	●	

Verification

During 08:00 to 18:00 on weekdays, clients with the IP addresses ranging from 192.168.0.2 to 192.168.0.10 cannot access Facebook and Tumblr.

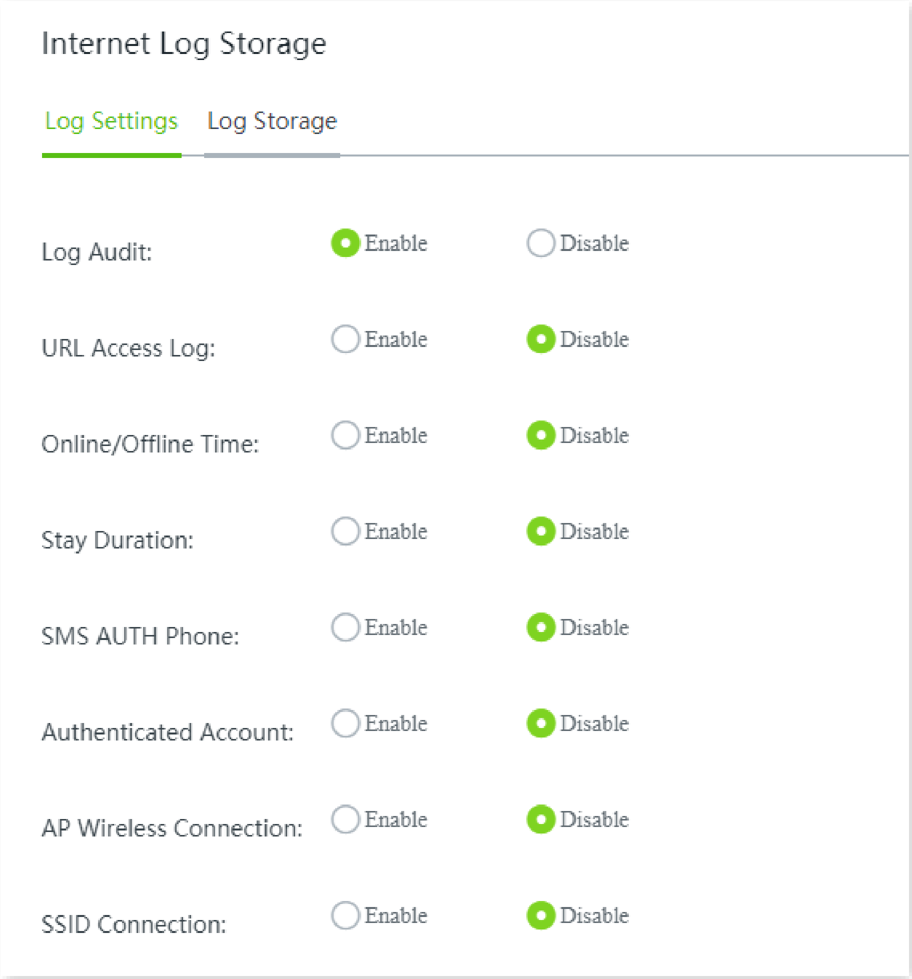
11.6 Log audit

11.6.1 Log settings

Click **Filter Management** > **Log Audit** > **Log Settings** to enter the page.

Here, you can enable or disable the internet log audit function. When it is enabled, the router will collect specified types of log records as required.

By default, this function is disabled.



Internet Log Storage

Log Audit: ● Enable ○ Disable

URL Access Log: ○ Enable ● Disable

Online/Offline Time: ○ Enable ● Disable

Stay Duration: ○ Enable ● Disable

SMS AUTH Phone: ○ Enable ● Disable

Authenticated Account: ○ Enable ● Disable

AP Wireless Connection: ○ Enable ● Disable

SSID Connection: ○ Enable ● Disable

Parameter description

Parameter	Description
Log Audit	Enable or disable the log audit function. After it is enabled, the router can collect specified types of log records.
URL Access Log	After it is enabled, the router records users' MAC addresses, IP addresses and visited websites.
Online/Offline Time	After it is enabled, the router records users' MAC addresses, IP addresses, online time and offline time.
Stay Duration	After it is enabled, the router records users' MAC addresses, IP addresses and the duration from online to offline.

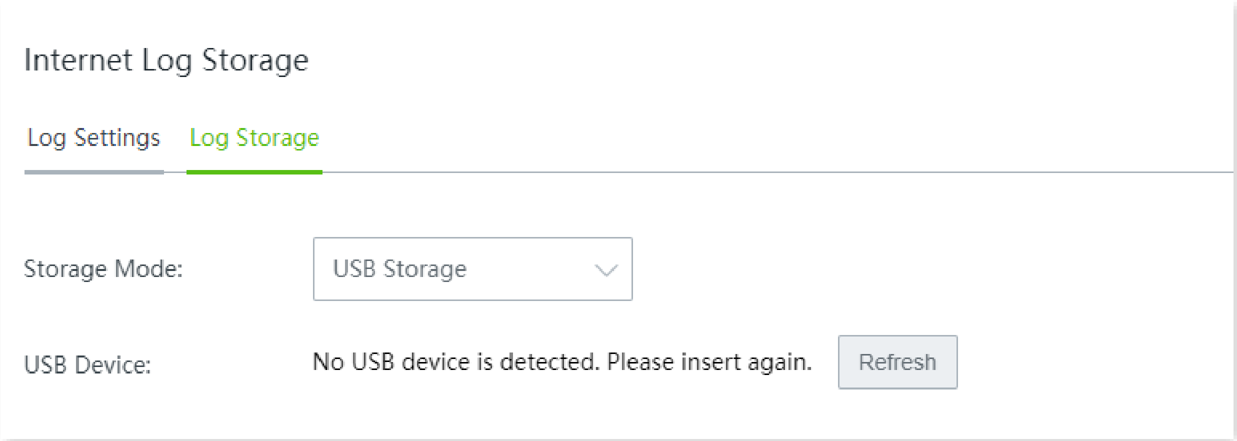
Parameter	Description
SMS AUTH Phone	After it is enabled, the router records users’ MAC addresses, IP addresses, mobile phone numbers for SMS authentication and the time for such authentication.
Authenticated Account	After it is enabled, the router records users’ MAC addresses, IP addresses and the account information used for authentication.
AP Wireless Connection	After it is enabled, the router records users’ MAC addresses, IP addresses, the names of connected mobile phones and APs.
SSID Connection	After it is enabled, the router records users’ MAC addresses, IP addresses and connected Wi-Fi names.

11.6.2 Log storage

Click **Filter Management** > **Log Audit** > **Log Storage** to enter the page.

After Log audit is enabled, the log records can be saved to a local PC or a USB device.

By default, it is set to USB storage.



Internet Log Storage

Storage Mode: USB Storage

USB Device: No USB device is detected. Please insert again.

Parameter description

Parameter	Description
Storage Mode	Specifies the storage location of log records. - **USB Storage**: The log records are stored in a USB device. Ensure that a USB device is already plugged. - **Local Storage**: The log records are stored in a local computer. Ensure that the computer is installed with log tools, such as **syslog**.
USB Device	Displays the available space of the USB storage device.
Host IP Address	Enter the IP address of the local computer.

12 More settings

12.1 Static route

12.1.1 Overview

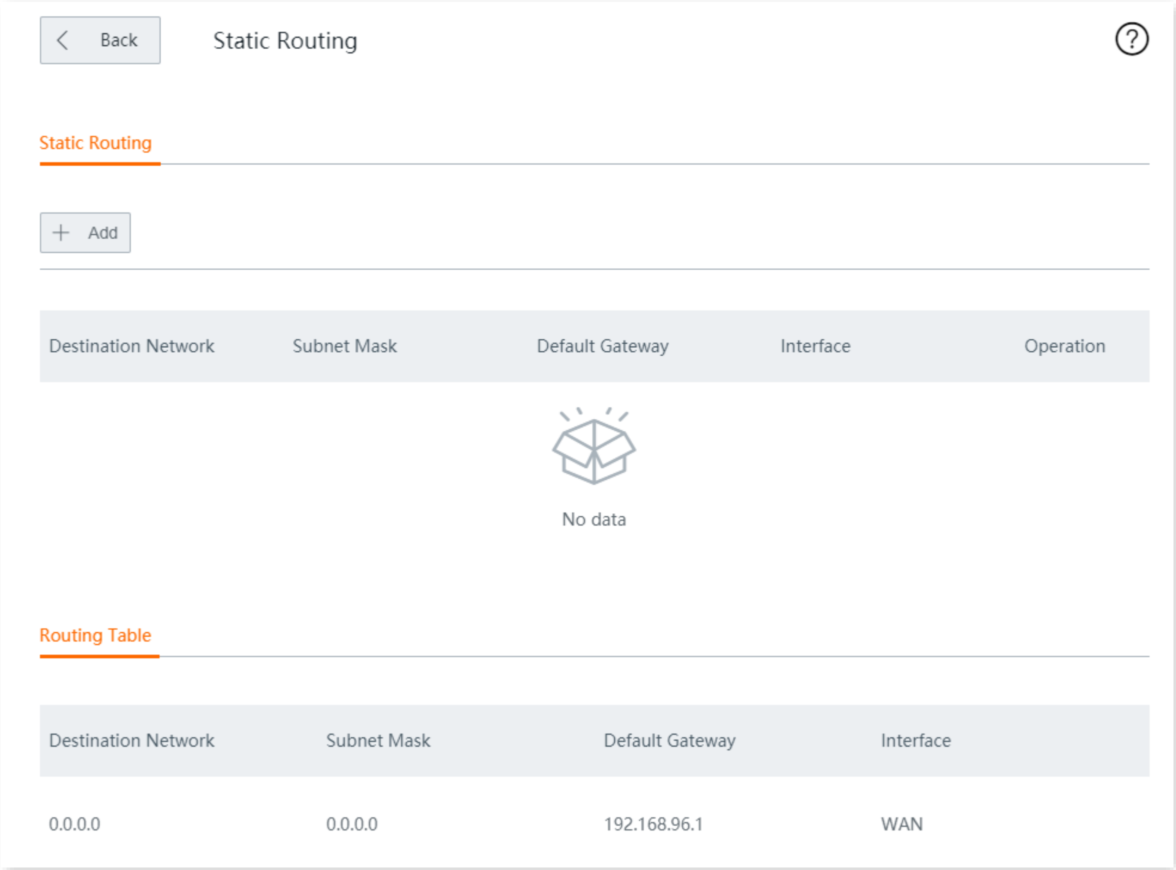
Routing is an operation to select the optimal route for delivering data from a source to a destination. A static route is a special route configured manually, which is simple, efficient, and reliable. Proper static routes help reduce route selection issues and prevent overload caused by route selection data flows, accelerating packet forwarding.

To define a static route, specify the network segment and subnet mask used to identify a destination network or host, the gateway IP address, and the router WAN port for forwarding packets. After a static route is defined, all the packets indented for the destination of the static route are directly forwarded through the WAN port of the router to the gateway IP address.

TIP

If only static routes are used in a large-scale complex network, destinations may be unreachable in case of a network fault or topology change, which results in network interruption. If the problem occurs, manually modify the static routes.

Click **More** > **Static Routing** to enter the page.



Destination Network	Subnet Mask	Default Gateway	Interface	Operation

No data

Routing Table

Destination Network	Subnet Mask	Default Gateway	Interface
0.0.0.0	0.0.0.0	192.168.96.1	WAN

Parameter description

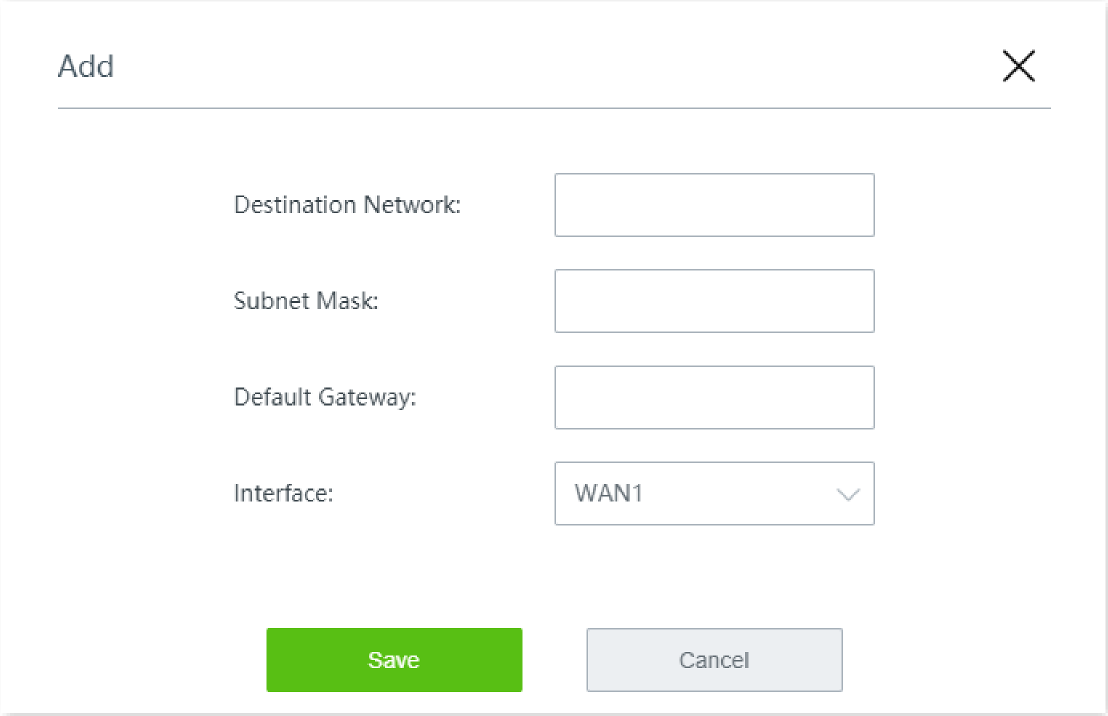
Parameter	Description
Destination Network	Specifies the IP address of the target network. **0.0.0.0** destination network and **0.0.0.0** subnet mask indicate the default route. TIP If no accurate route is found in the route table, the router chooses the default route to forward data packets.
Subnet Mask	Specifies the subnet mask of the destination network.
Default Gateway	Specifies the ingress port IP address of the next hop route after data packets egress from the router. **0.0.0.0** indicates that the destination network is directly connected to the interface of the router.
Interface	Specifies the interface from which packets egress. Select it as required.
Operation	Specifies the operations you can perform on the rule. ✎: Click it to edit the rule. 🗑 : Click it to delete the rule.

12.1.2 Configure a static routing rule

TIP

If a static route conflicts with a user-defined multi-WAN policy, the static route prioritizes.

Click **More** > **Static Routing** to enter the page. Click **+Add**, and configure the following parameters in the window, then click **Save**.



Add

Destination Network:

Subnet Mask:

Default Gateway:

Interface: WAN1

12.1.3 Example of configuring static route

Networking requirement

An enterprise uses the wireless router to build a network.

Requirements:

The internet and the intranet are deployed on different networks. The WAN1 port of the router accesses the internet using a PPPoE connection and the WAN2 port of the router accesses the intranet (enterprise LAN) using a dynamic IP address.

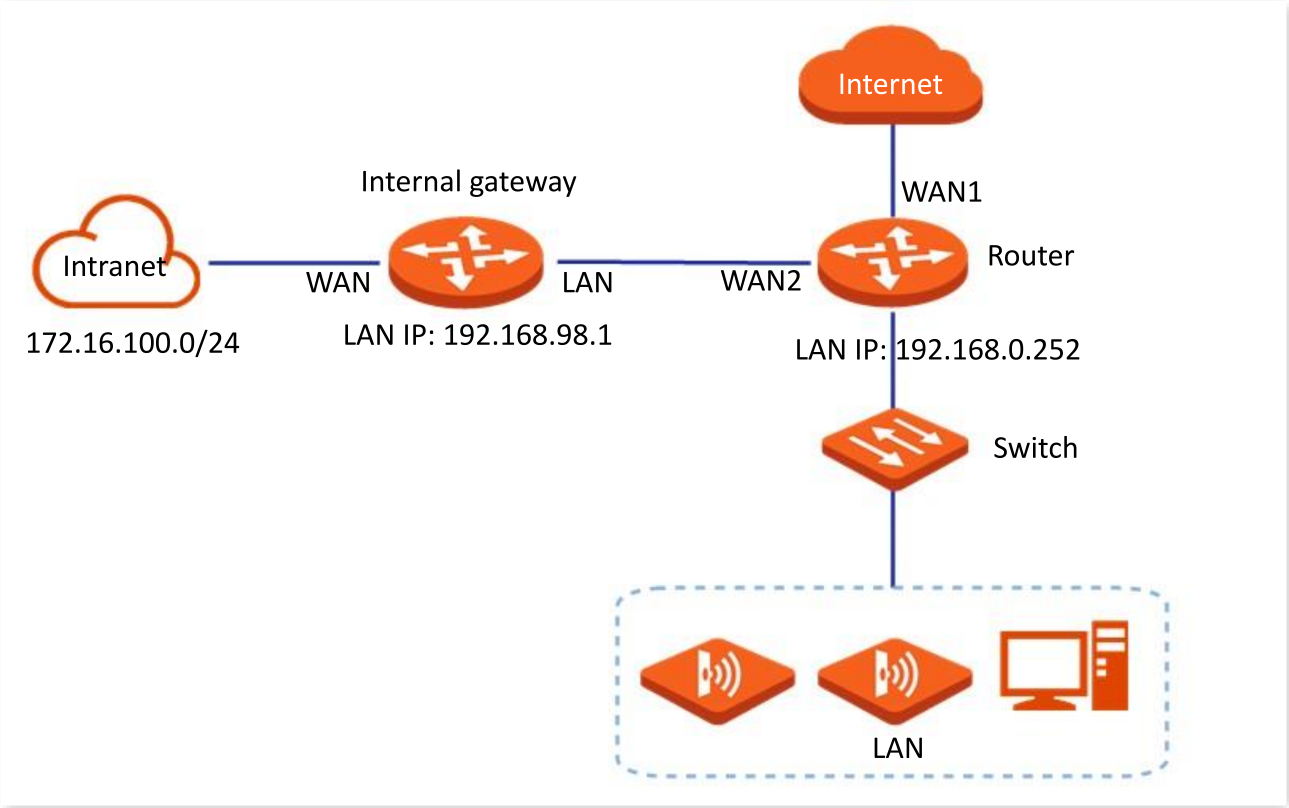
Users on the router's LAN are allowed to access both the internet and intranet.

Solution

The static routing function can meet this requirement.

Assume that:

- PPPoE user name: tdxy123
- PPPoE password: ipxz456

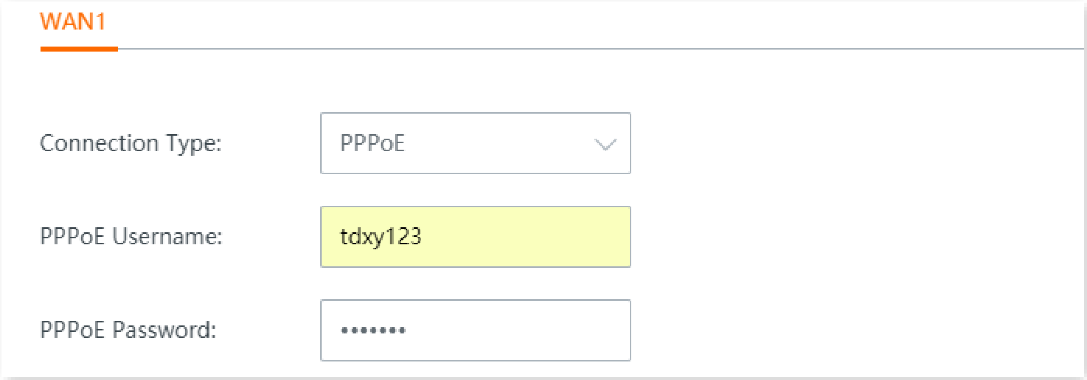


Configuration procedure

Step 1 Enable two WAN ports, and configure the internet settings.

1. Navigate to **Internet Settings** > **Internet Settings**.
2. Select the number of WAN ports from the **WAN Ports** drop-down list menu, which is **2** in this example.

3. On the **WAN1** configuration area, set **Connection Type** to **PPPoE**, and enter the **PPPoE Username** and **PPPoE Password** provided by your ISP, which are **tdxy123** and **ipxz456** in this example.



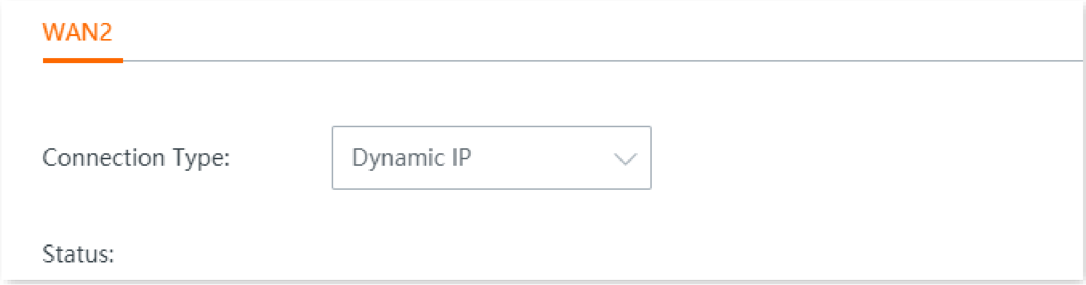
WAN1

Connection Type: PPPoE

PPPoE Username: tdxy123

PPPoE Password: •••••••

4. On the **WAN2** configuration area, set **Connection Type** to **Dynamic IP**.



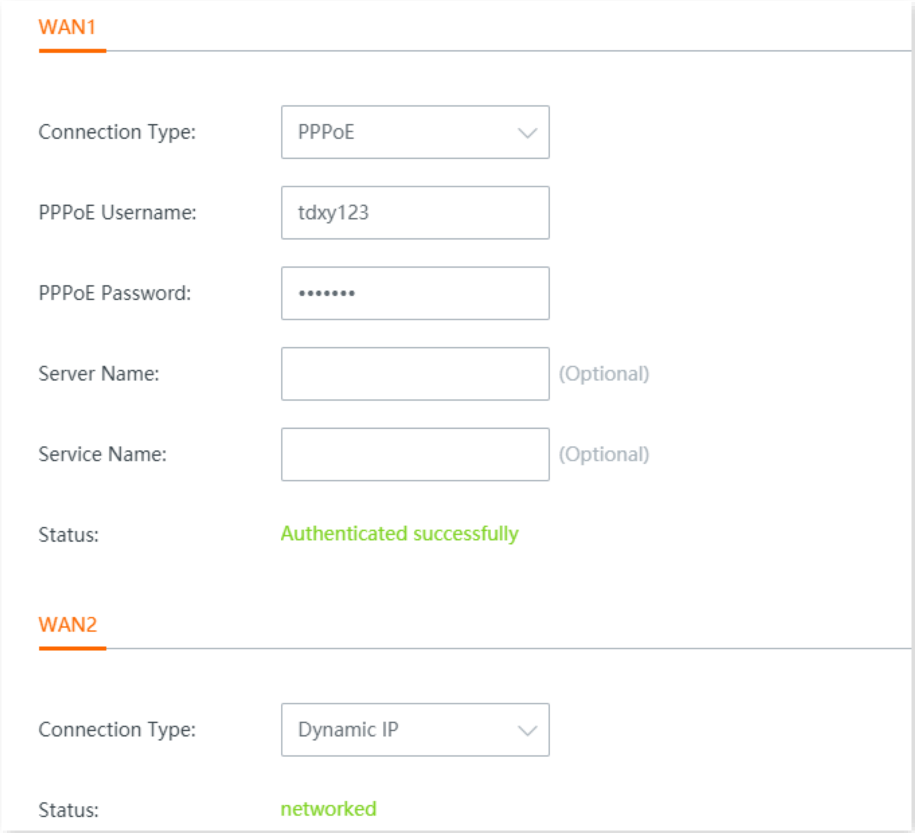
WAN2

Connection Type: Dynamic IP

Status:

5. Click **Save** at the bottom of page.

   Wait a moment. When the status of WAN1 shows **Authenticated successfully**, the WAN1 is connected to the internet; when the status of WAN2 shows **networked**, the WAN2 is connected to the internet.



WAN1

Connection Type: PPPoE

PPPoE Username: tdxy123

PPPoE Password: •••••••

Server Name: (Optional)

Service Name: (Optional)

Status: Authenticated successfully

WAN2

Connection Type: Dynamic IP

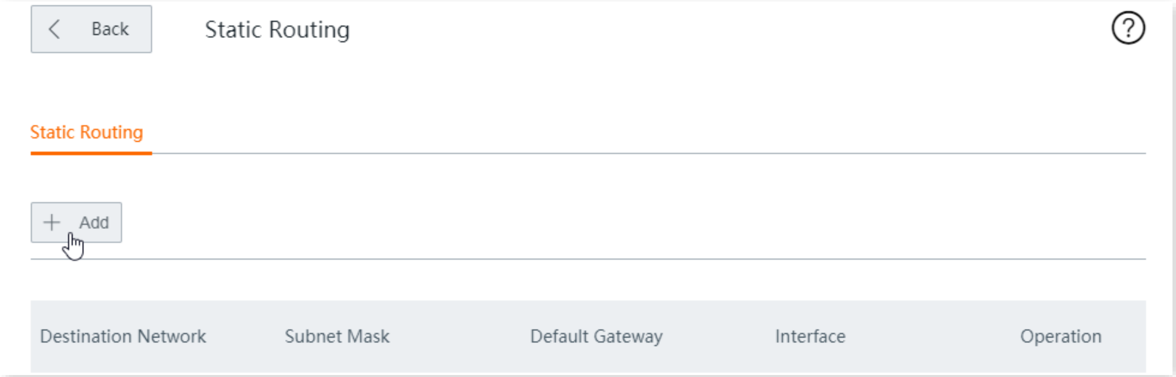
Status: networked

Step 2 Configure static routing.

1. Click **System Status** > , and view the IP information of WAN2. Assume that:
   - IP Address: 192.168.98.190
   - Subnet Mask: 255.255.255.0
   - Default Gateway: 192.168.98.1
   - Primary DNS: 192.168.96.1
2. Add a static routing rule.

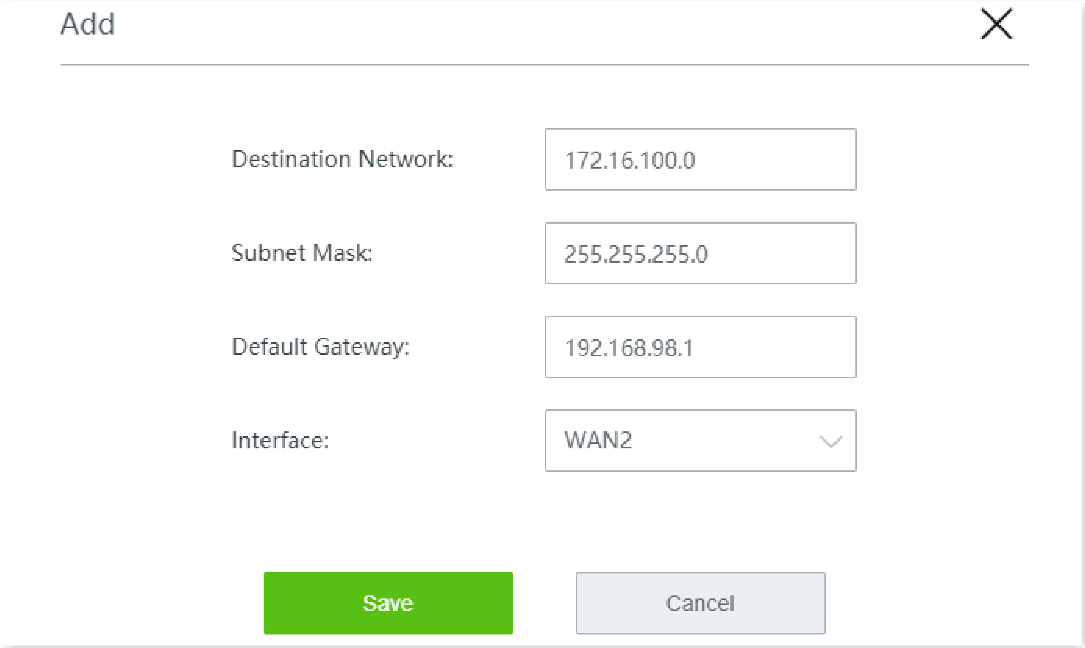
(1) Navigate to **More** > **Static Routing**.

(2) Click **+Add**.



(3) Configure the following parameters, and click **Save**.

- Enter the **Destination Network**, which is **172.16.100.0** in this example.
- Enter the **Subnet Mask** of the destination network, which is **255.255.255.0** in this example.
- Enter the **Default Gateway** (the ingress port IP address of the next hop route after data packets egress from the router), which is **192.168.98.1** in this example.
- Enter the **Interface** between the router and the destination network, which is **WAN2** in this example.



Destination Network: 172.16.100.0

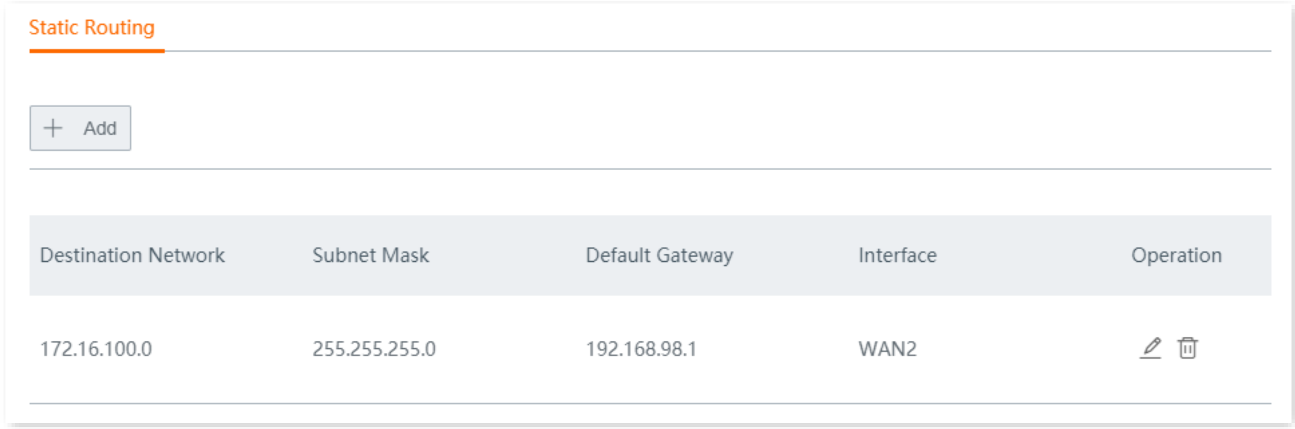
Subnet Mask: 255.255.255.0

Default Gateway: 192.168.98.1

Interface: WAN2

----End

Add successfully. See the following figure.



Destination Network	Subnet Mask	Default Gateway	Interface	Operation
172.16.100.0	255.255.255.0	192.168.98.1	WAN2	✎ 🗑

Verification

Computers in the LAN can access the internet and the intranet simultaneously.

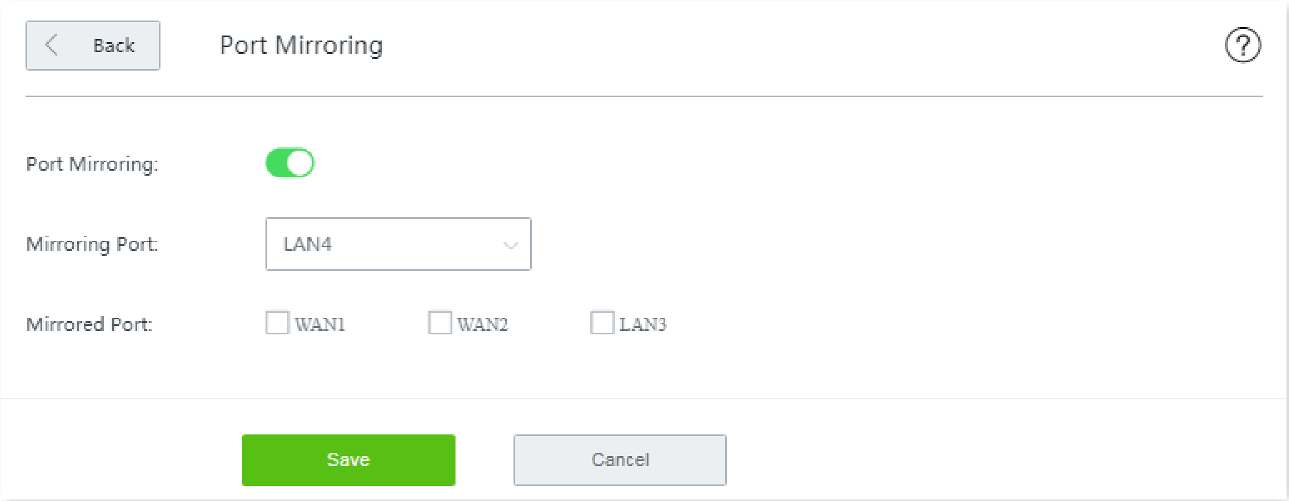
12.2 Port mirroring

12.2.1 Overview

Port mirroring function forwards a copy of data of one or more mirrored ports to the specified mirroring port. The network administrator uses data monitoring devices to monitor traffic, analyze performance and perform network diagnose.

Click **More** > **Port Mirroring** to enter the page.

By default, this function is disabled.



Port Mirroring: ●

Mirroring Port: LAN4

Mirrored Port: □ WAN1 □ WAN2 □ LAN3

Parameter description

Parameter	Description
Port Mirroring	Enable or disable the port mirroring function.
Mirroring Port	Specifies the monitoring port. A piece of monitoring software must be installed on the computer with this port to perform monitoring. The default mirroring port is **LAN4**, which can be customized.
Mirrored Port	Specifies the monitored ports. After the port mirroring function is enabled, packets of the mirrored ports are replicated to the mirroring port for monitoring.

12.2.2 Example of configuring port mirroring

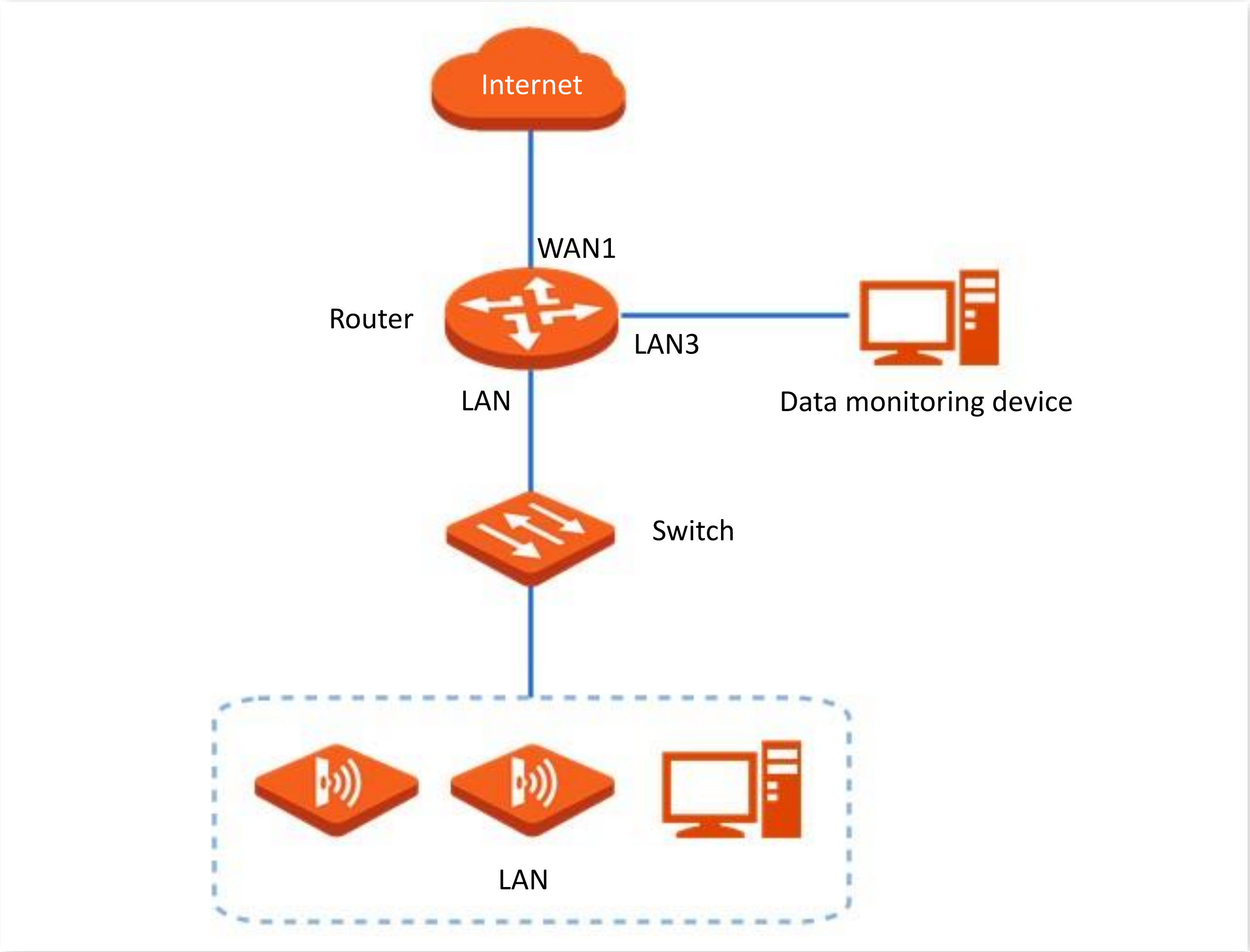
Networking requirement

An enterprise uses the router to build a network. Recently, internet access failures occur frequently and the network administrator needs to capture data packets from the WAN and LAN ports of the router for analysis.

Solution

The port mirroring function of the router can meet this requirement.

Assume that a data monitoring device is connected to the LAN3 to monitor the data of other ports.



Configuration procedure

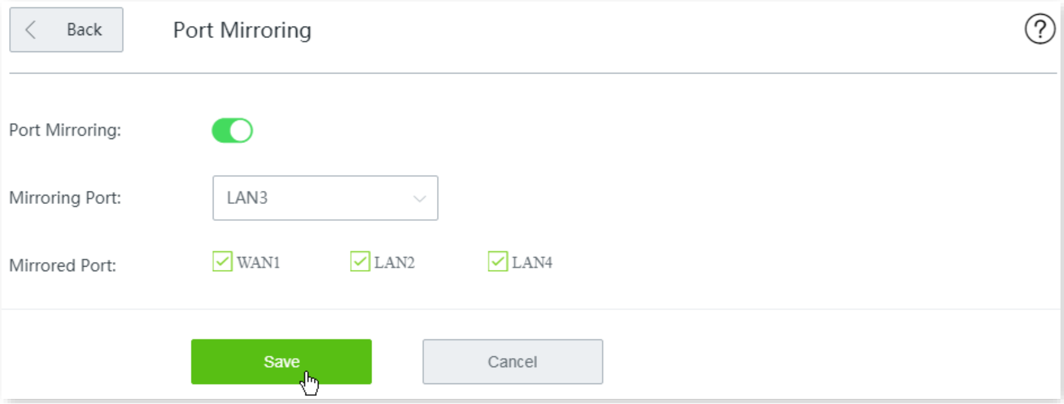
Step 1 Navigate to **More** > **Port Mirroring**.

Step 2 Enable **Port Mirroring**.

Step 3 Select the **Mirroring Port**, which is **LAN3** in this example.

Step 4 Select the **Mirrored Ports**, which are **WAN1**, **LAN2** and **LAN4** in this example.

Step 5 Click **Save** at the bottom of the page.



Port Mirroring: ●

Mirroring Port: LAN3

Mirrored Port: ☑ WAN1 ☑ LAN2 ☑ LAN4

----End

Verification

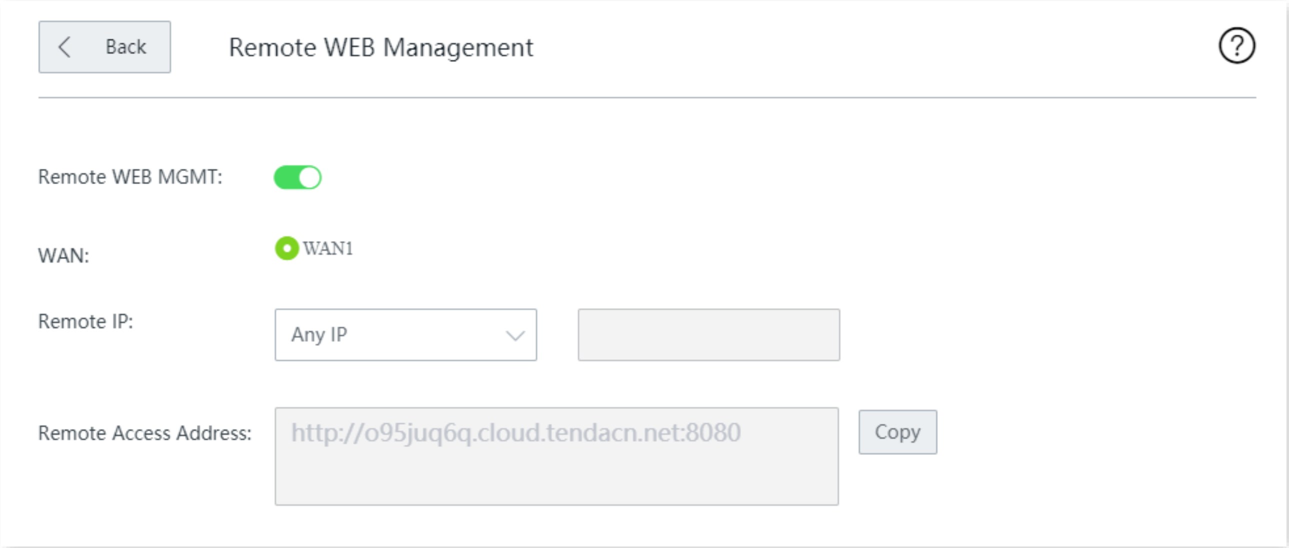
Run monitoring software such as Wireshark on the monitoring computer to verify the software can capture data packets from the mirrored ports.

12.3 Remote web management

12.3.1 Overview

Generally, the web UI of the router can only be accessed on devices that are connected to the router in wired or wireless manner. This costs in case of seeking technician to fix network problems. The remote web management function is designed to address such requirement. When you encounter network faulty, you can ask technicians far away to diagnose and fix your problems, improving efficiency and reducing costs and efforts.

Click **More** > **Remote WEB Management** to enter the page.



Remote WEB Management

Remote WEB MGMT: enabled

WAN: ● WAN1

Remote IP: Any IP

Remote Access Address: http://o95juq6q.cloud.tendacn.net:8080

Parameter description

Parameter	Description
Remote WEB MGMT	Enable or disable the remote web management function.
WAN	Specifies the WAN port of the router, which is also the WAN port used to remotely access the web UI of the router.
Remote IP	IP address of the computer that can access the router remotely. - **Any IP**: Any computers can access the router over the internet. Choose this option only when necessary since it lowers network security. - **Specified IP**: Only a computer with the specified IP address can access the router over the internet. If the computer is on a LAN, enter the WAN port IP address of the gateway of the computer.
Remote Access Address	With this function enabled, the router automatically generates one unique domain name that can be used to manage the router remotely.

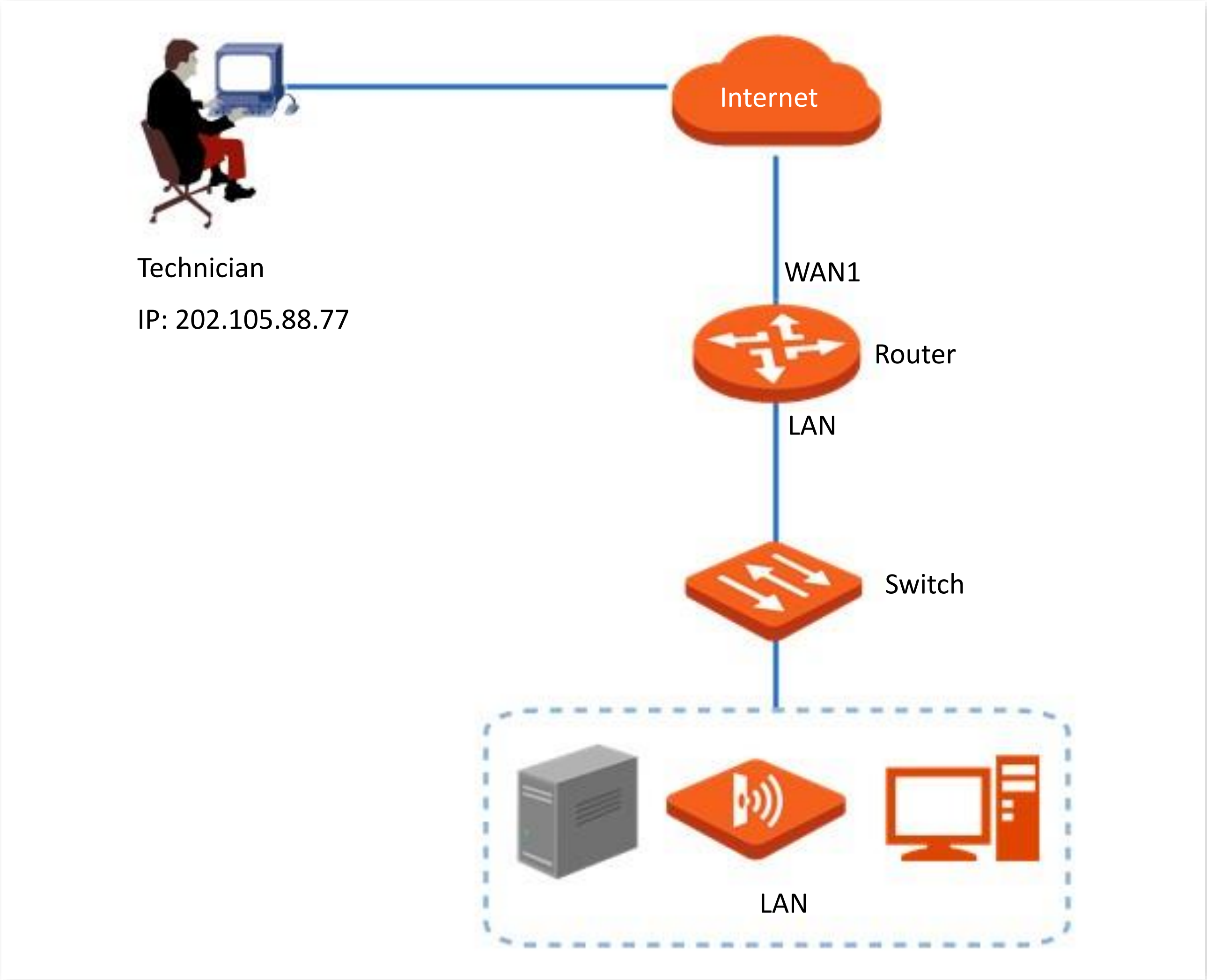
12.3.2 Example of configuring remote web management

Networking requirement

An enterprise uses the wireless router to deploy its network. The network administrator needs to seek a Tenda technician to solve a problem remotely.

Solution

The remote web management function can meet this requirement.



Configuration procedure

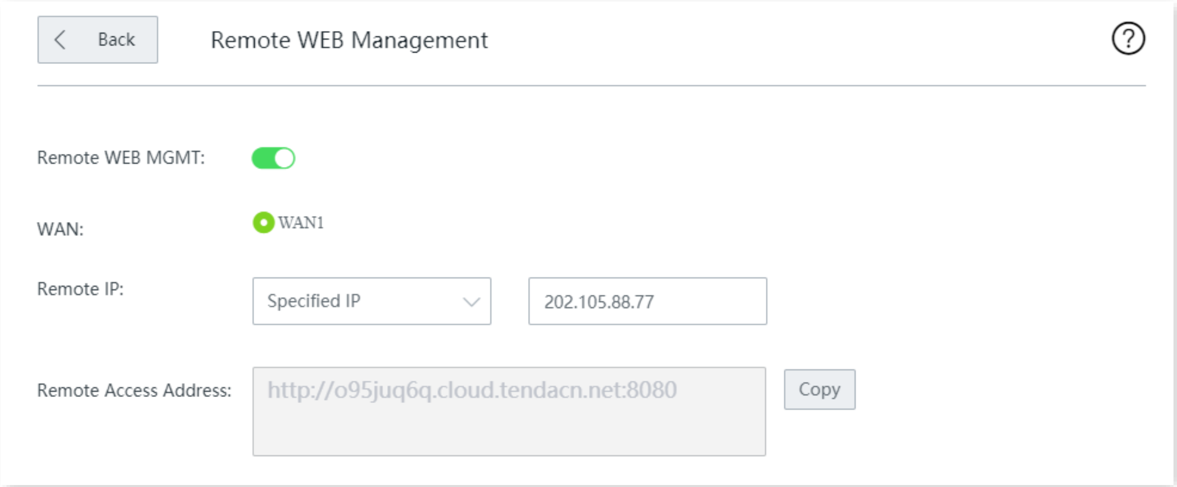
Step 1 Navigate to **More** > **Remote WEB Management**.

Step 2 Enable **Remote WEB MGMT**.

Step 3 Select the **WAN** port for remote management, which is **WAN1** in this example.

Step 4 Select the **Specified IP**, and enter the IP address of the computer of the Tenda support technician, which is **202.105.88.77** in this example.

Step 5 Click **Save** at the bottom of the page.



Remote WEB MGMT: ●

WAN: ● WAN1

Remote IP: Specified IP 202.105.88.77

Remote Access Address: http://o95juq6q.cloud.tendacn.net:8080 Copy

----End

Verification

Tenda technician with a computer IP address 202.105.88.77 can use http://o95juq6q.cloud.tendacn.net:8080 to access the web UI of the router remotely.

12.4 DDNS

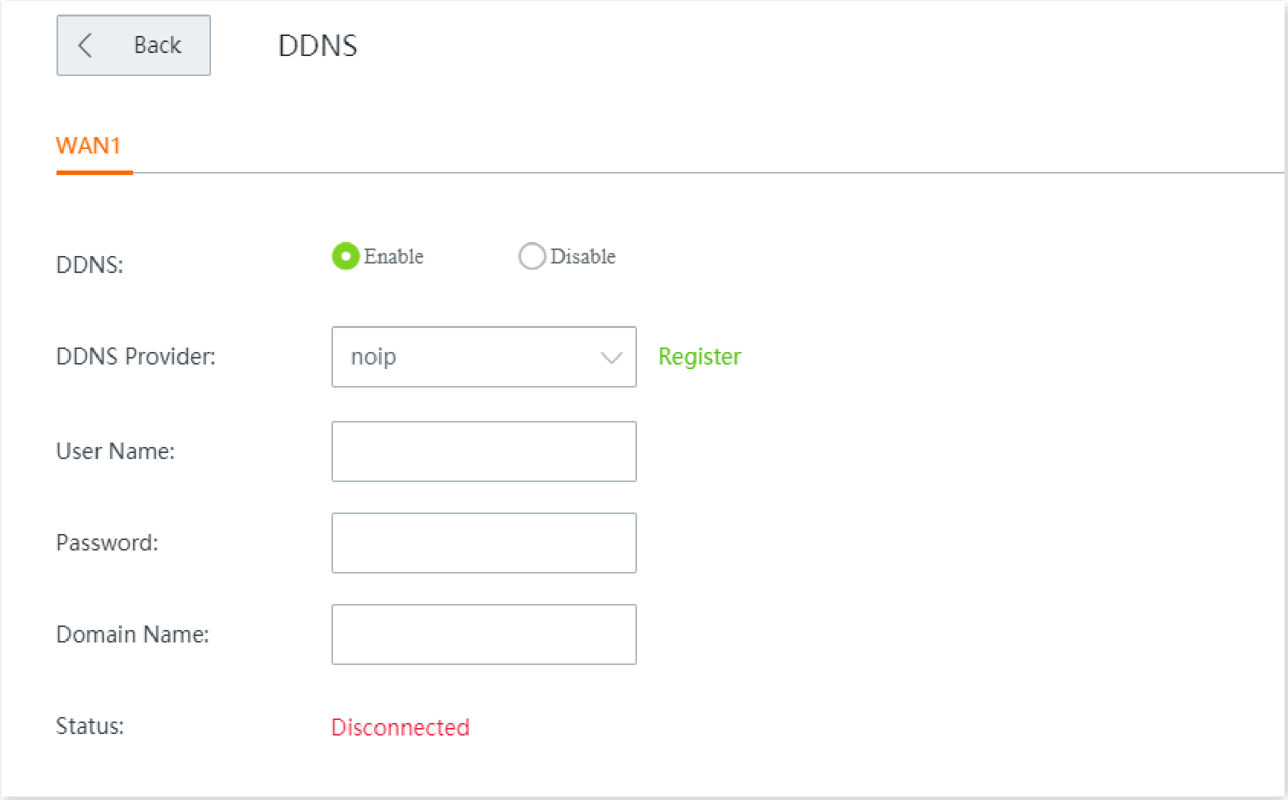
12.4.1 Overview

DDNS is abbreviated for Dynamic Domain Name Service. When a service is running, the DDNS client on the router sends the IP address of the current WAN port of the router to the DDNS server, and the server updates the mapping relationships between the domain name and IP address in the database, achieving dynamic domain name resolution.

On this page, you can map the dynamic WAN IP address of the router (public IP address) to a fixed domain name. The DDNS function is generally used with such functions as port forwarding and DMZ host to enable internet users to access the LAN server or the web UI of the router through domain name without caring about the change of the WAN IP address.

Click **More** > **DDNS** to enter the page.

By default, this function is disabled.



DDNS: ● Enable ○ Disable

DDNS Provider: noip

User Name:

Password:

Domain Name:

Status: Disconnected

Parameter description

Parameter	Description
DDNS	Enable or disable the DDNS function.
DDNS Provider	The router supports four DDNS providers: **noip**, **dyndns**, **oray**, and **gnway**.
Service Type	Specifies the type of the DDNS account. This parameter appears when **DDNS Provider** is set to **oray**.
User Name	Specifies the user name/password used to log in to a DDNS provider. They are registered on the website of the provider.
Password	
Domain Name	Specifies the domain name obtained from the DDNS provider. If **DDNS Provider** is set to other DDNS provider other than **oray**, you need to manually enter the domain name applied from the target website.
Status	Specifies the DDNS service status.

12.4.2 Example of configuring DDNS

Networking requirement

An enterprise uses the wireless router to set up a network. The router has been connected to the internet and can offer internet service to LAN users.

The enterprise has the following requirement:

The intranet web server is open to internet users to enable staff to access the intranet even when they are not physically in the enterprise.

Solution

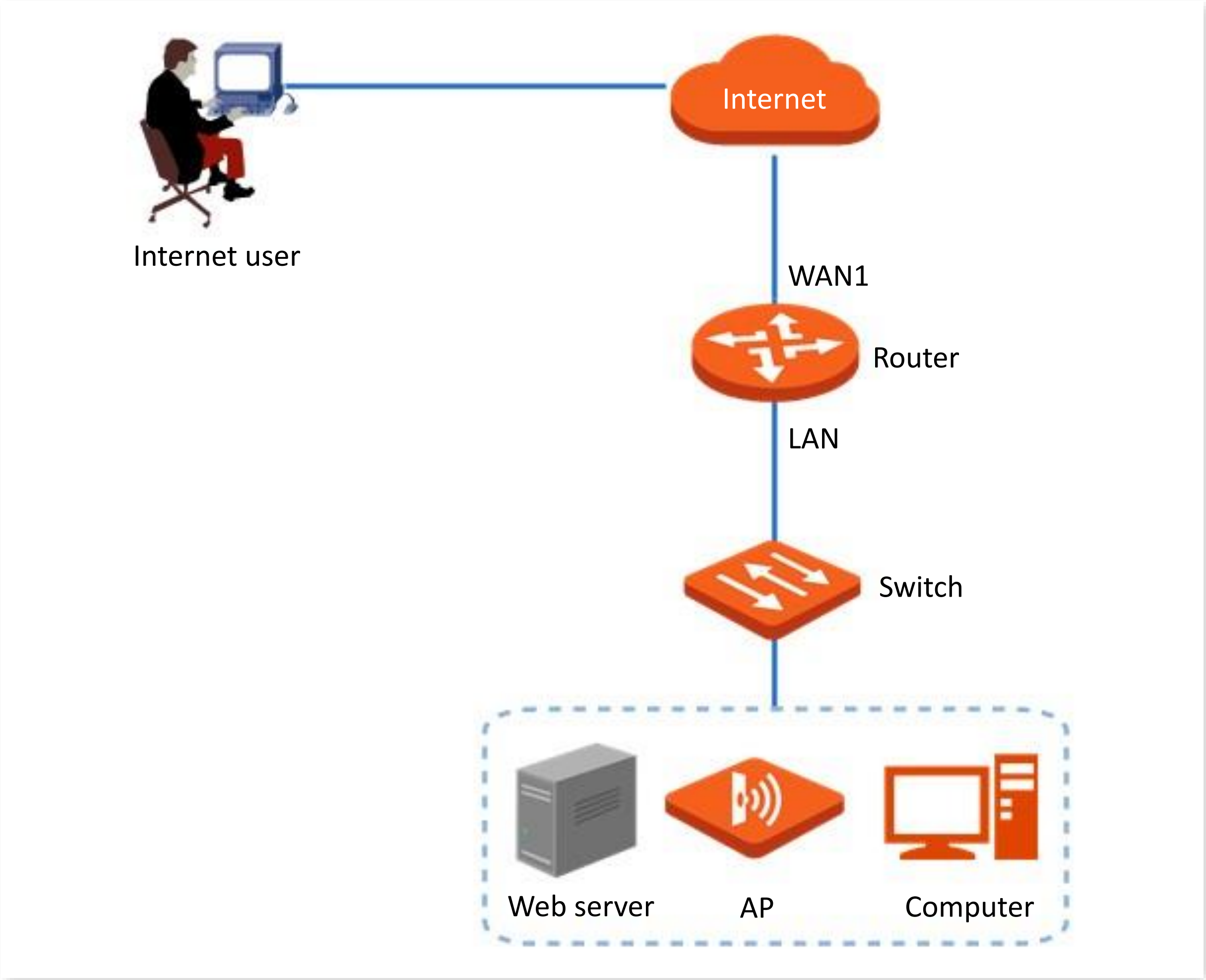
- You can use the **Port Forwarding** function to enable internet users to access the intranet web server.
- You can use the **DDNS** function to enable internet users to access the intranet web server through a fixed domain name, avoiding access failure caused by WAN IP address change.
- You can use the **Address Reservation** function to avoid access failure caused by web server address change.

Assume that the information of the web server is shown as below:

- IP address of the web server: 192.168.0.250
- MAC address of the host that runs the web server: C8:9C:DC:60:54:69
- Service port: 9999

TIP

- Before the configuration, ensure that the WAN port of the router obtains a public IP address; if the WAN port obtains a private IP address or an intranet IP address assigned by the ISP (starting with 100), the function may not take effect. Commonly-used IPv4 private IP addresses include 10.0.0.0 to 10.255.255.255, 172.16.0.0 to 172.31.255.255, and 192.168.0.0 to 192.168.255.255.
- ISP may not support unreported web service accessed using the default port number 80. Therefore, when setting port forwarding, you are recommended to set the external port as a non-familiar port (1024 to 65535), such as 9999, to ensure normal access.
- Internal and external ports can be different.

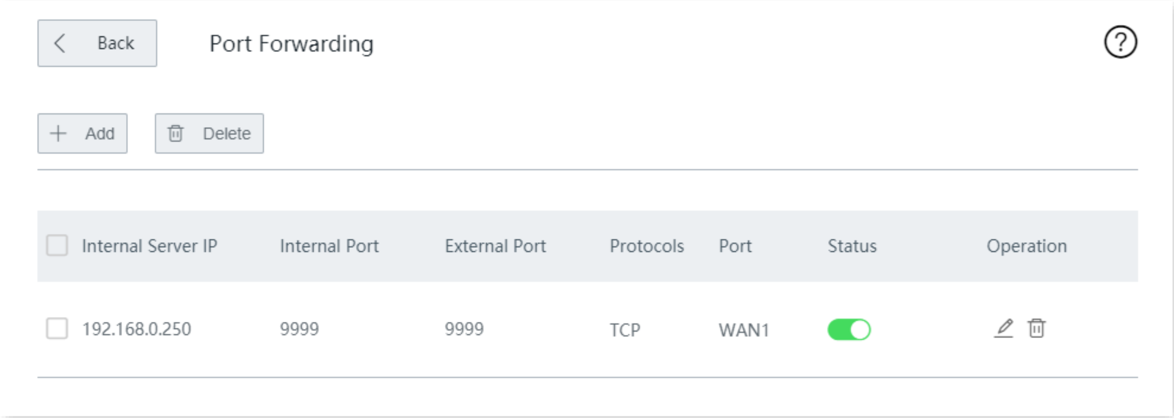


Configuration procedure

Configure port forwarding > Reserve a fixed IP address for the server > Configure DDNS

Step 1 Configure port forwarding.

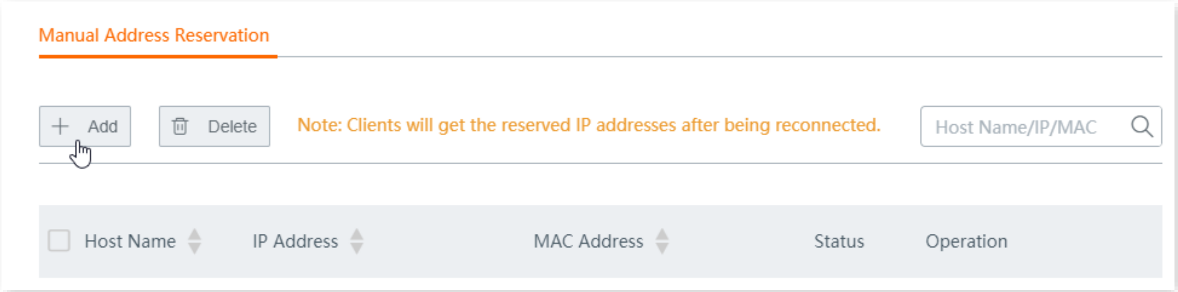
Navigate to **More** > **Port Forwarding**, and add a rule. Refer to Configure a port forwarding rule.



□ Internal Server IP	Internal Port	External Port	Protocols	Port	Status	Operation
□ 192.168.0.250	9999	9999	TCP	WAN1	●	

Step 2 Reserve a fixed IP address for the server host.

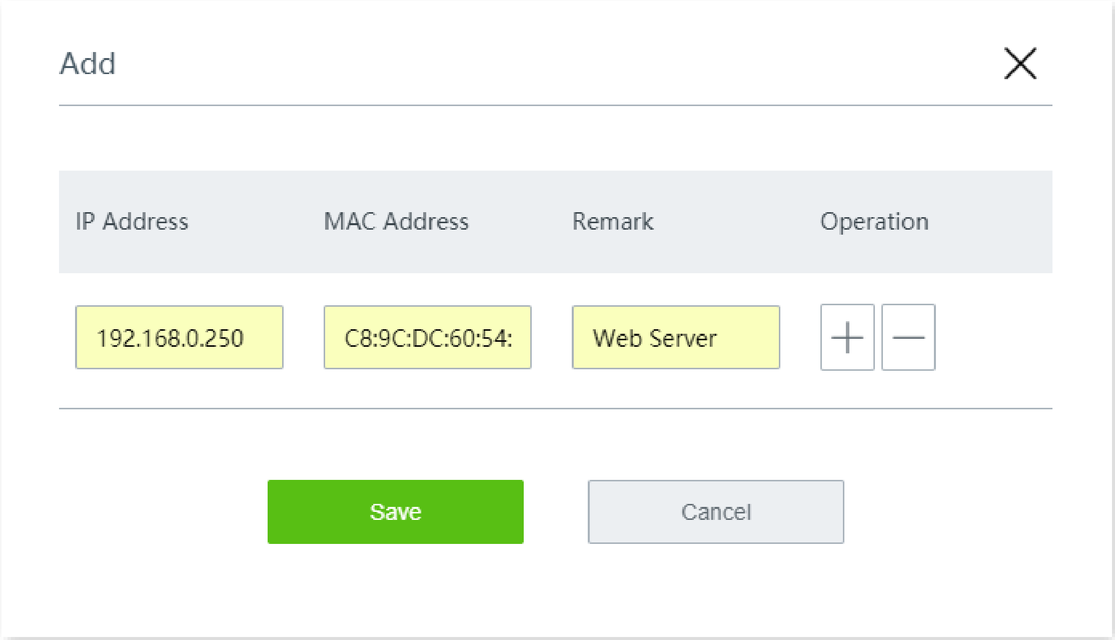
1. Navigate to **Address Reservation** > **Manual Address Reservation**.
2. Click **+Add**.



Note: Clients will get the reserved IP addresses after being reconnected.

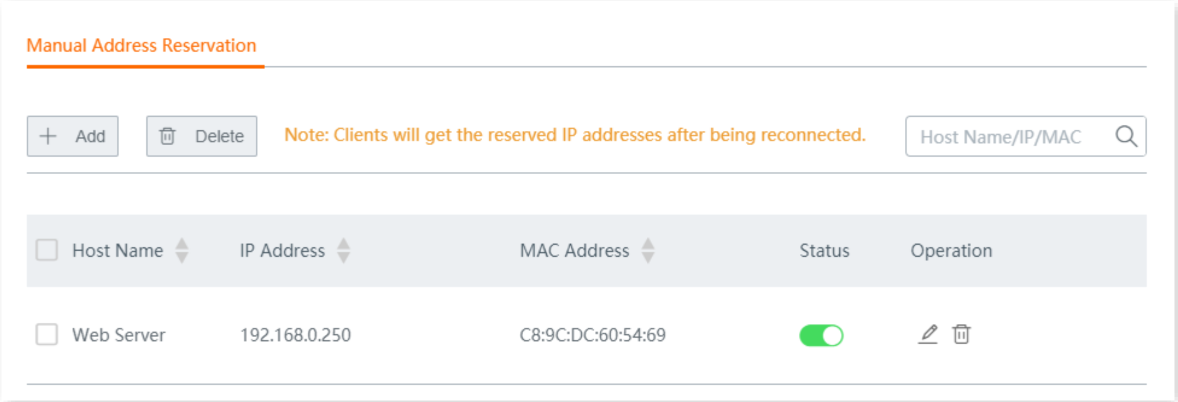
□ Host Name	IP Address	MAC Address	Status	Operation

3. Configure the following parameters in the **Add** window, and click **Save**.
   (1) Set the fixed IP address assigned to the server host, which is **192.168.0.250** in this example.
   (2) Enter the MAC address of the server host, which is **C8:9C:DC:60:54:69** in this example.
   (3) (Optional) Enter a remark, such as **Web Server**.



IP Address	MAC Address	Remark	Operation
192.168.0.250	C8:9C:DC:60:54:	Web Server	+ —

Reserved successfully. See the following figure.



Note: Clients will get the reserved IP addresses after being reconnected.

□ Host Name	IP Address	MAC Address	Status	Operation
□ Web Server	192.168.0.250	C8:9C:DC:60:54:69	●	✎ 🗑

Step 3 Configure DDNS.

1. Register a domain name.

   Log in to the DDNS provider website. Assume that the DDNS provider where you applied the domain name is **noip**, the user name you registered is **Tenda**, the password is **tdxy123**, and the domain name is **tenda.ddns.net**

2. Log in to the web UI of the router and configure DDNS.

   (1) Navigate to **More** > **DDNS**.

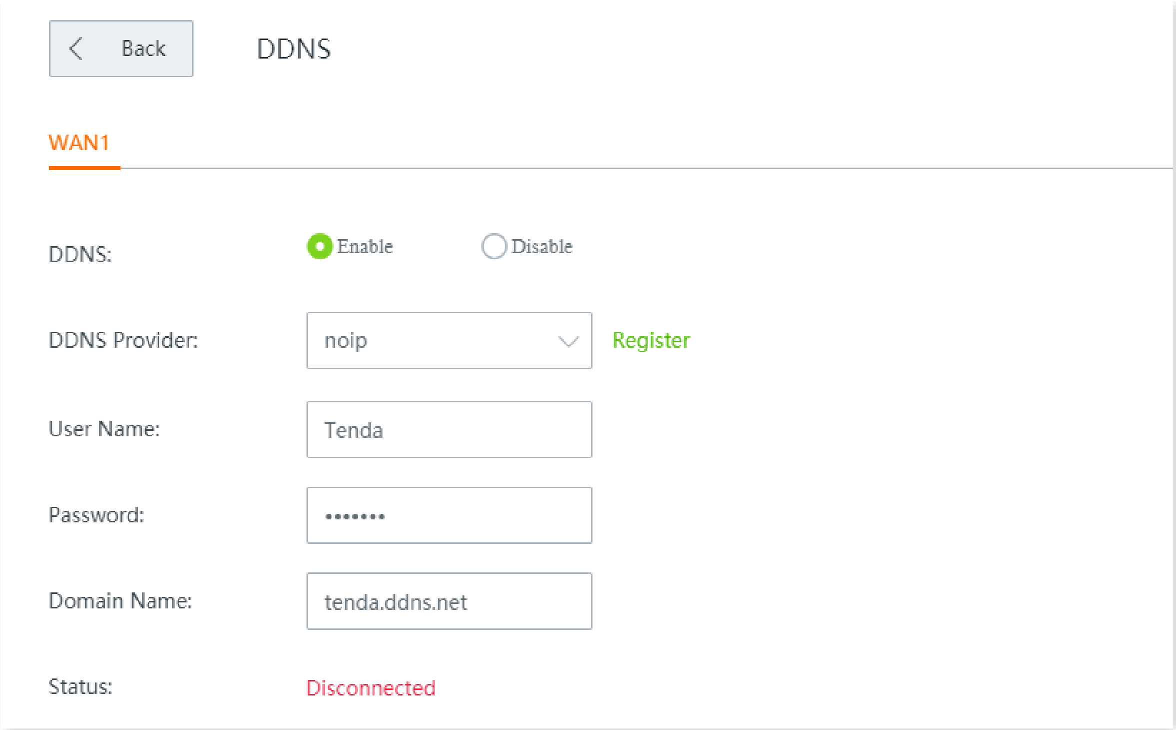
   (2) Enable **DDNS**.

   (3) Select **noip** from the **DDNS Provider** drop-down list.

   (4) Enter the user name and password, which is **Tenda** and **tdxy123** in this example.

   (5) Enter the domain name, which is **tenda.ddns.net** in this example.

   (6) Click **Save** at the bottom of the page.



DDNS: ● Enable ○ Disable

DDNS Provider: noip

User Name: Tenda

Password: •••••••

Domain Name: tenda.ddns.net

Status: Disconnected

----End

Wait a moment, and refresh the page. When the **Status** shows **Connected**, the configuration completes successfully.

Verification

Internet users can successfully access the intranet server by using **intranet service application layer protocol name**://**WAN port domain name**:**external port**, which is **http://tenda.ddns.net:9999** in this example.

If you set the default port of the intranet service as the external port when configuring port forwarding, the external port number can be excluded from the access address. Under such circumstances, the access address is **intranet service application layer protocol name**://**WAN port domain name**.

TIP

If internet users still cannot access the LAN server after the configuration, try the following methods:

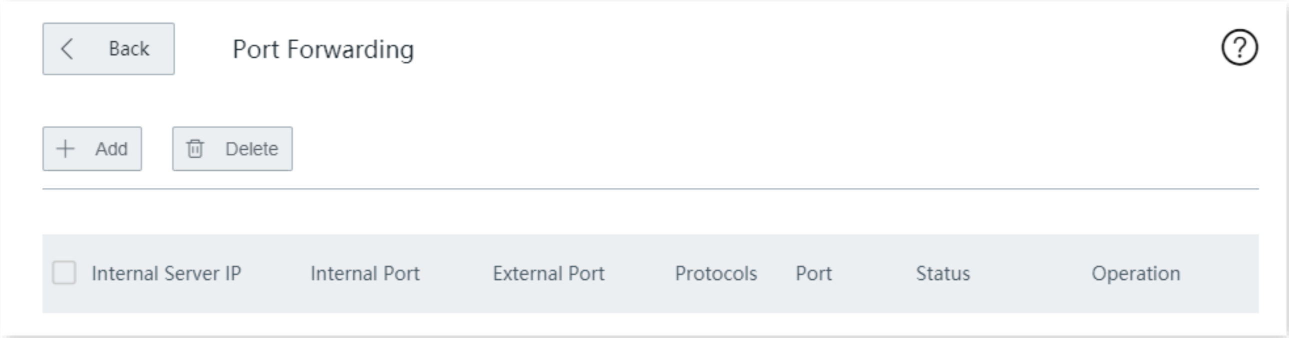
- Make sure that the internal port you entered is correct.
- Maybe the system firewall, anti-virus software and security guard on the LAN server blocked internet user access. Please disable these programs and try again.

12.5 Port forwarding

12.5.1 Overview

By default, internet users cannot access LAN devices. However, with port forwarding function, you can open one or multiple service ports (TCP or UDP) of the router and forwards these ports to the specified LAN server. In this way, service requests sent to those ports of the node can be forwarded to the target LAN server. Internet users can access the LAN server and the LAN is defended against attacks.

Navigate to **More** > **Port Forwarding** to enter the page.



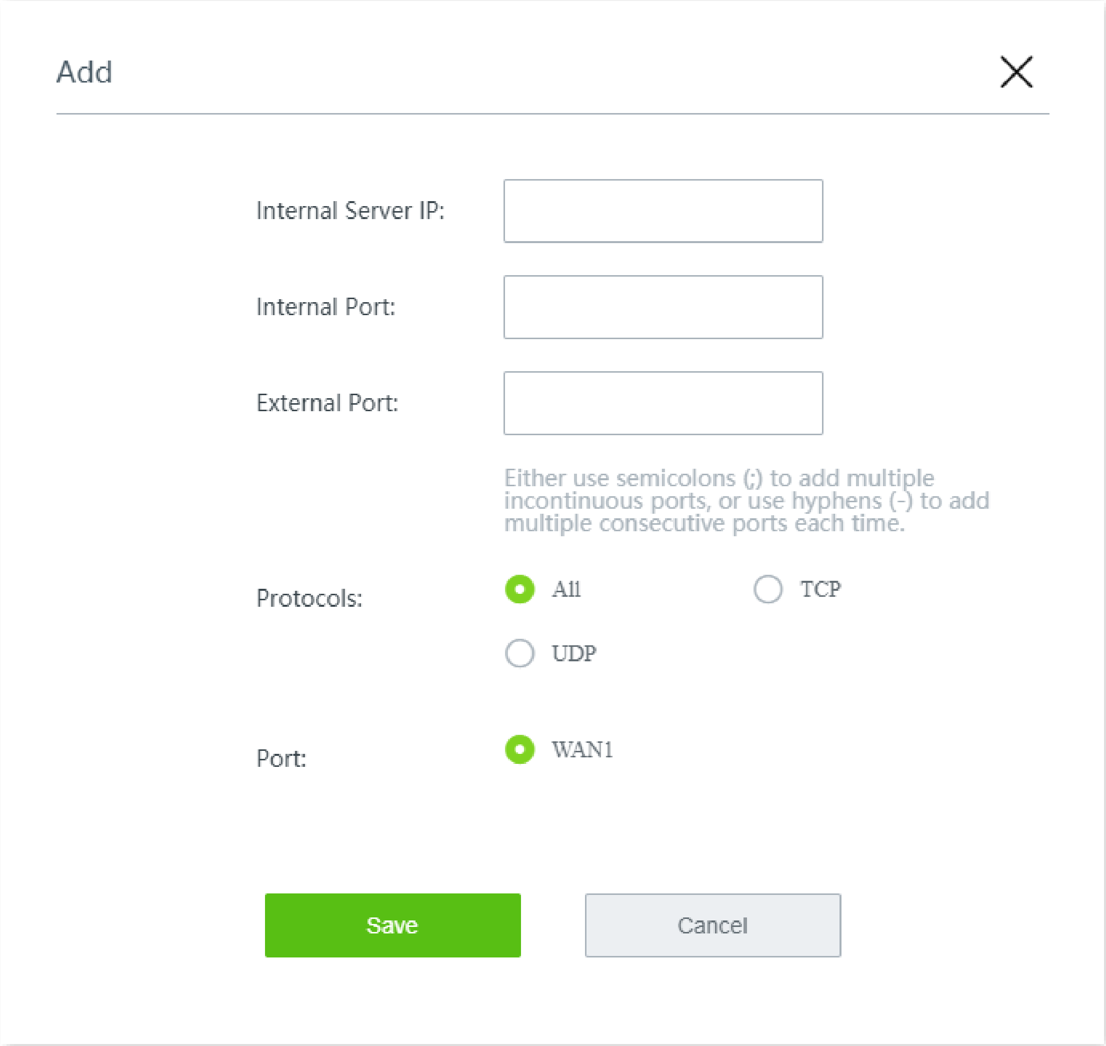
□ Internal Server IP	Internal Port	External Port	Protocols	Port	Status	Operation

Parameter description

Parameter	Description
Internal Server IP	Specifies the IP address of the internal server.
Internal Port	Specifies the service port of the internal server.
External Port	Specifies the port opened to internet users to access.
Protocols	Specify the types of the transfer layer protocol used by the LAN service. **All** indicates both TCP and UDP. Select **All** if you are uncertain about the service type.
Port	Specifies the WAN port internet users use to access the LAN service.
Status	Specifies the status of the rule. You can enable or disable the rule as required.
Operation	Specifies the operations you can perform on the rule. ✎: Click it to edit the rule. 🗑 : Click it to delete the rule.

12.5.2 Configure a port forwarding rule

Click **More** > **Port Forwarding** to enter the page. Click **+Add**, configure the following parameters, and click **Save**.



Add

Internal Server IP:

Internal Port:

External Port:

Either use semicolons (;) to add multiple incontinuous ports, or use hyphens (-) to add multiple consecutive ports each time.

Protocols: ● All ○ TCP ○ UDP

Port: ● WAN1

12.5.3 Example of configuring a port forwarding rule

Networking requirement

An enterprise uses the wireless router to set up a network. The router has been connected to the internet and can offer internet service to LAN users.

The enterprise has the following requirement:

The intranet web server is open to internet users to enable staff to access the intranet even when they are not physically in the enterprise.

Solution

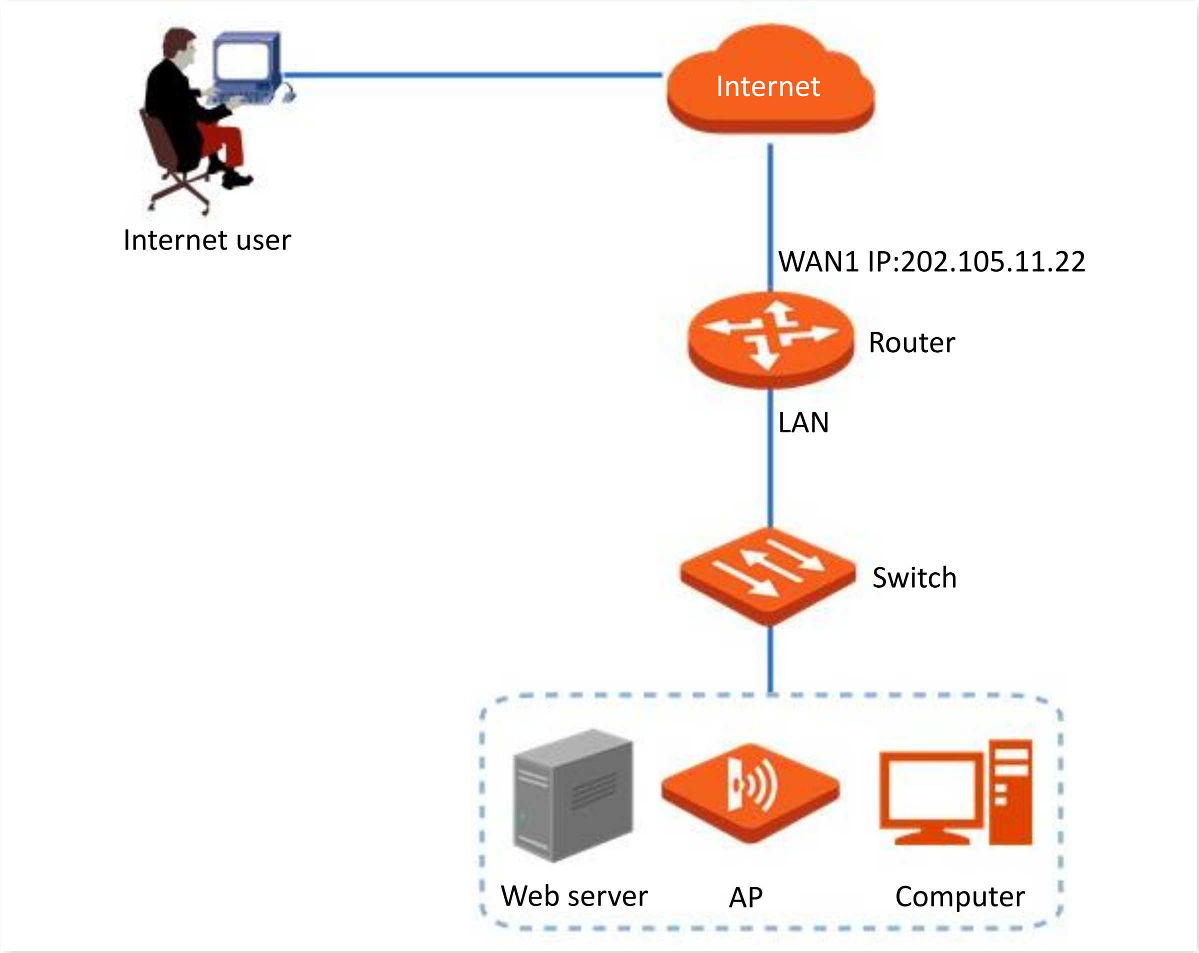
- You can use the **Port Forwarding** function to enable internet users to access the intranet web server. Assume that the open port of the router is 9999.
- You can use the **Address Reservation** function to avoid access failure caused by web server address change.

Assume that the information of the web server is shown as below:

- IP address of the web server: 192.168.0.250
- MAC address of the host that runs the web server: C8:9C:DC:60:54:69
- Service port: 9999

TIP

- Before the configuration, ensure that the WAN port of the router obtains a public IP address; if the WAN port obtains a private IP address or an intranet IP address assigned by the ISP (starting with 100), the function may not take effect. Commonly-used IPv4 private IP addresses include 10.0.0.0 to 10.255.255.255, 172.16.0.0 to 172.31.255.255, and 192.168.0.0 to 192.168.255.255.
- ISP may not support unreported web service accessed using the default port number 80. Therefore, when setting port forwarding, you are recommended to set the external port as a non-familiar port (1024 to 65535), such as 9999, to ensure normal access.
- Internal and external ports can be different.

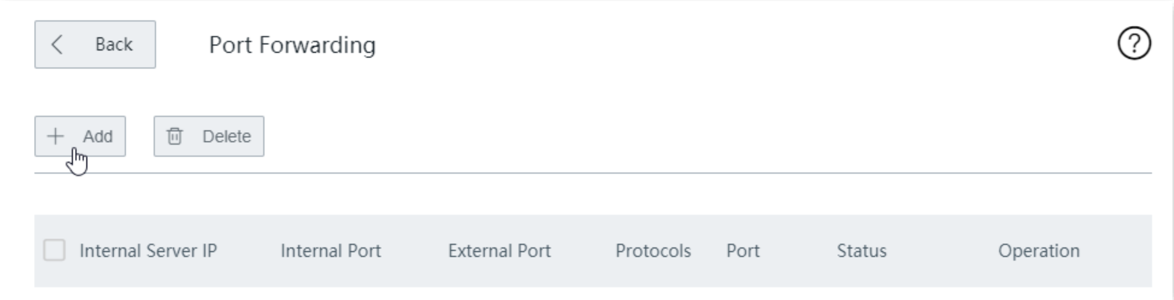


Configuration procedure

Configure port forwarding > Reserve a fixed IP address for the server host

Step 1 Configure port forwarding.

1. Navigate to **More** > **Port Forwarding**.
2. Click **+Add**.



□ Internal Server IP	Internal Port	External Port	Protocols	Port	Status	Operation

3. Configure the following parameters in the **Add** window, and click **Save**.

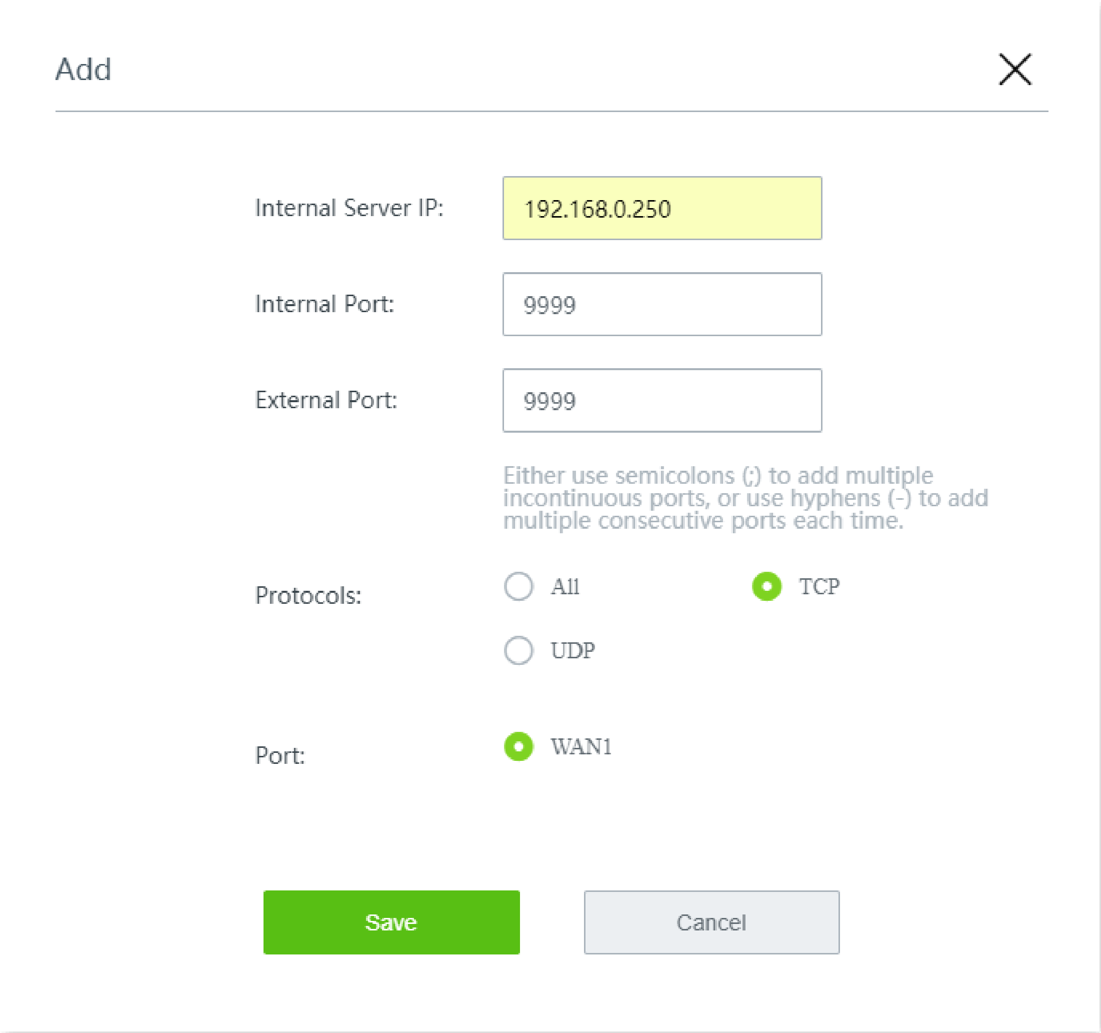
(1) Enter the **Internal Server IP**, which is **192.168.0.250** in this example.

(2) Enter the **Internal Port**, which is **9999** in this example.

(3) Enter the **External Port**, which is **9999** in this example.

(4) Choose the protocol used by the web server, which is **TCP** in this example.

(5) Select **WAN1** as the port through which WAN users get access to the LAN server.



Add

Internal Server IP: 192.168.0.250

Internal Port: 9999

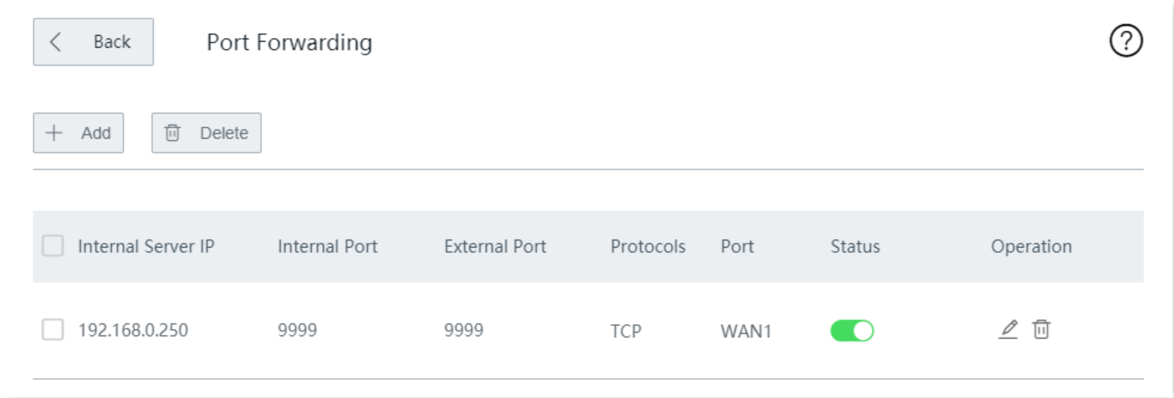
External Port: 9999

Either use semicolons (;) to add multiple incontinuous ports, or use hyphens (-) to add multiple consecutive ports each time.

Protocols: ○ All ● TCP ○ UDP

Port: ● WAN1

Added successfully. See the following figure.

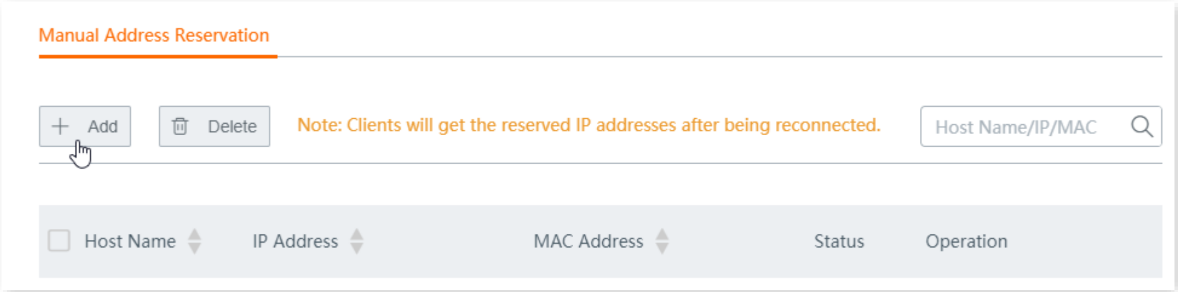


Port Forwarding

□ Internal Server IP	Internal Port	External Port	Protocols	Port	Status	Operation
□ 192.168.0.250	9999	9999	TCP	WAN1	●	✎ 🗑

Step 2 Reserve a fixed IP address for the server host.

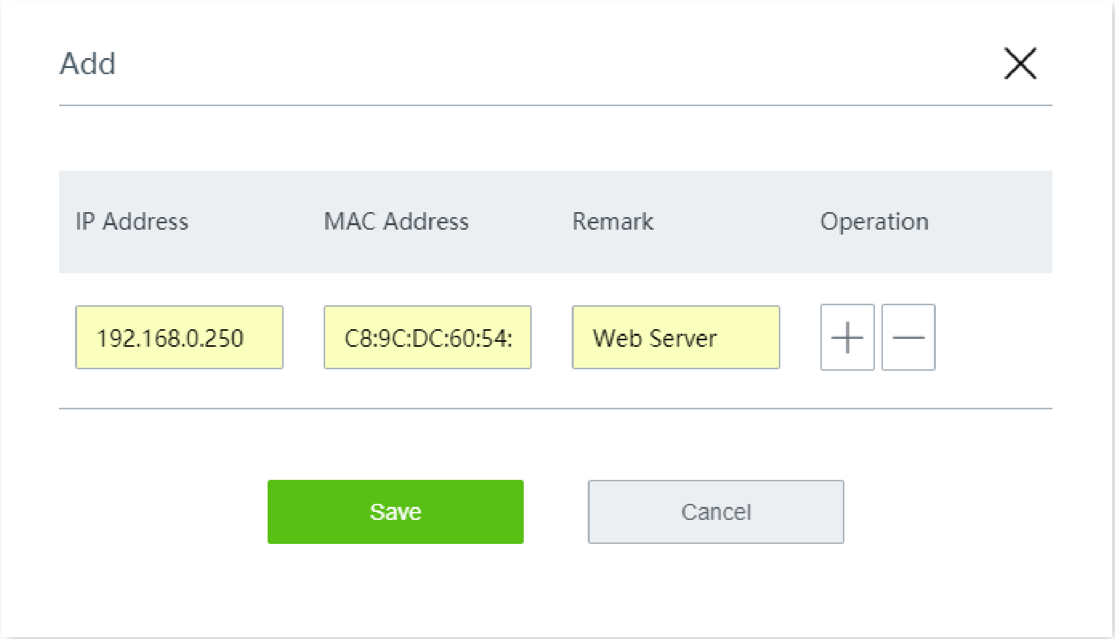
1. Navigate to **Address Reservation** > **Manual Address Reservation**.
2. Click **+Add**.



Note: Clients will get the reserved IP addresses after being reconnected.

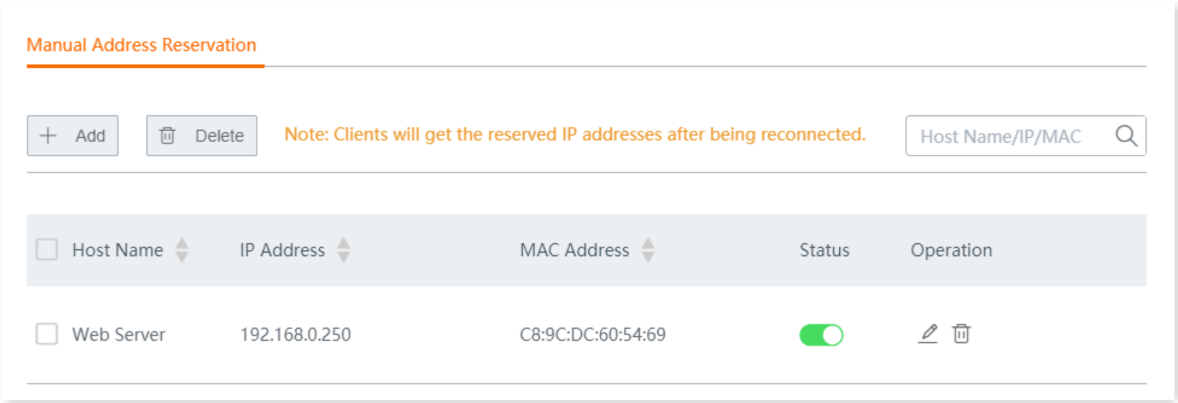
□ Host Name	IP Address	MAC Address	Status	Operation

3. Configure the following parameters in the **Add** window, and click **Save**.
   (1) Set the fixed IP address assigned to the server host, which is **192.168.0.250** in this example.
   (2) Enter the MAC address of the server host, which is **C8:9C:DC:60:54:69** in this example.
   (3) (Optional) Enter a remark, such as **Web Server**.



IP Address	MAC Address	Remark	Operation
192.168.0.250	C8:9C:DC:60:54:	Web Server	+ —

Reserved successfully. See the following figure.



Note: Clients will get the reserved IP addresses after being reconnected.

□ Host Name	IP Address	MAC Address	Status	Operation
□ Web Server	192.168.0.250	C8:9C:DC:60:54:69	●	✎ 🗑

----End

Verification

Internet users can successfully access the intranet server by using **intranet service application layer protocol name**://**WAN port IP address**:**external port**. If you set the default port of the intranet service as the external port when configuring port forwarding, the external port number can be excluded from the access address. Under such circumstances, the access address is **intranet service application layer protocol name**://**WAN port IP address**.

In this example, the access address is http://202.105.11.22:9999

You can check the current WAN IP address on the System Status page.

If DDNS is enabled on the WAN port, internet users can also access the intranet server by using **intranet service application layer protocol name**://**WAN port domain name**:**external port**.

TIP

If internet users still cannot access the LAN server after the configuration, try the following methods:

- Make sure that the internal port you entered is correct.
- Maybe the system firewall, anti-virus software and security guard on the LAN server blocked internet user access. Please disable these programs and try again.

12.6 DMZ host

12.6.1 Overview

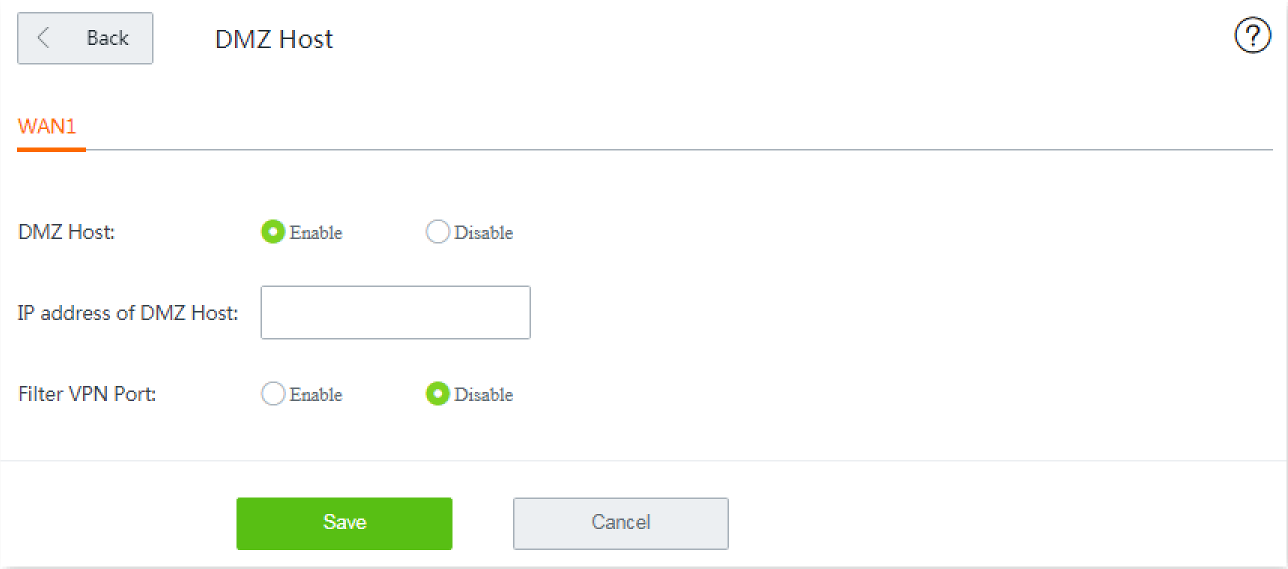
After setting a device in the LAN as the DMZ host, it enjoys no limitations when communicating with the internet. For example, if video meeting or online games are under way on a computer, you can set that computer as the DMZ host to make the video meeting and online games go smoother. In addition, you can also set the LAN server as the DMZ host when internet users access the LAN server resources.

NOTE

- After you set a LAN device as a DMZ host, that device will be completely exposed to the internet and the firewall of the node does not take effect on the device.
- Hackers may fire attacks on the local network by using the DMZ host. Please exercise caution to use the DMZ host function.
- The security guard, anti-virus software and system firewall on the DMZ host may affect the DMZ host function. Disable them when using this function. When you are not using the DMZ host function, you are recommended to disable the function and enable the firewall, security guard and anti-virus software on the DMZ host.

Click to **More** > **DMZ Host** to enter the page.

By default, this function is disabled.



DMZ Host: ● Enable ○ Disable

IP address of DMZ Host:

Filter VPN Port: ○ Enable ● Disable

Parameter description

Parameter	Description
DMZ Host	Enable or disable the DMZ host function.
IP Address of DMZ Host	Specifies the IP address of the LAN device to be set as the DMZ host.

Parameter	Description
Filter VPN Port	Enable or disable the filter VPN port function. After this function is enabled and you enabled the DMZ host function at the same time, the VPN service of the router will respond to the VPN requests from the internet. TIP If the router has already enabled the VPN server function and is about to enable the DMZ host function, to ensure the validity of the VPN server of the router, enable the filter VPN port function as well.

12.6.2 Example of configuring DMZ host

Networking requirement

An enterprise uses the wireless router to set up a network. The router has been connected to the internet and can offer internet service to LAN users.

The enterprise has the following requirement:

The intranet web server is open to internet users to enable staff to access the intranet even when they are not physically in the enterprise.

Solution

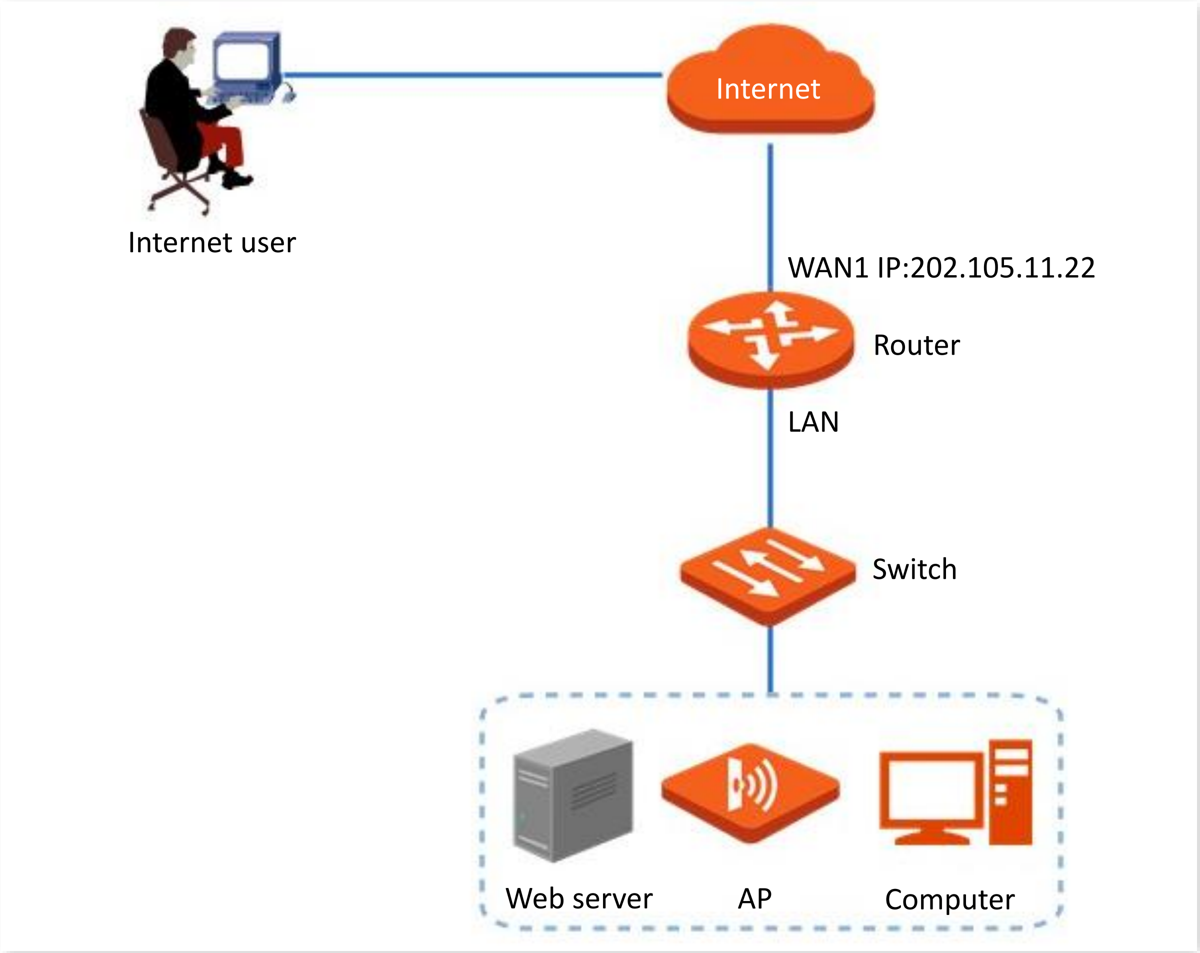
- You can use the **DMZ Host** function to enable internet users to access the intranet web server.
- You can use the **Address Reservation** function to avoid access failure caused by web server address change.

Assume that the information of the web server is shown as below:

- IP address of the web server: 192.168.0.250
- MAC address of the host that runs the web server: C8:9C:DC:60:54:69
- Service port: 9999

TIP

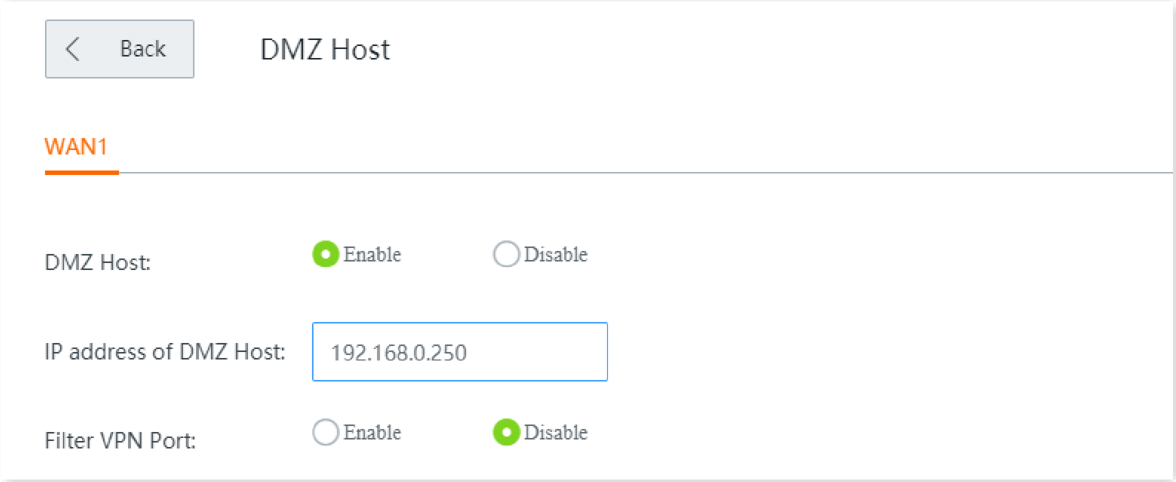
- Before the configuration, ensure that the WAN port of the router obtains a public IP address; if the WAN port obtains a private IP address or an intranet IP address assigned by the ISP (starting with 100), the function may not take effect. Commonly-used IPv4 private IP addresses include 10.0.0.0 to 10.255.255.255, 172.16.0.0 to 172.31.255.255, and 192.168.0.0 to 192.168.255.255.
- ISP may not support unreported web service accessed using the default port number 80. Therefore, when setting port forwarding, you are recommended to set the external port as a non-familiar port (1024 to 65535), such as 9999, to ensure normal access.



Configuration procedure

Step 1 Configure the DMZ host.

1. Navigate to **More** > **DMZ Host**.
2. Enable **DMZ Host**.
3. Enter the IP address of the LAN device to be set as the DMZ host, which is **192.168.0.250** in this example.
4. Click **Save** at the bottom of the page.



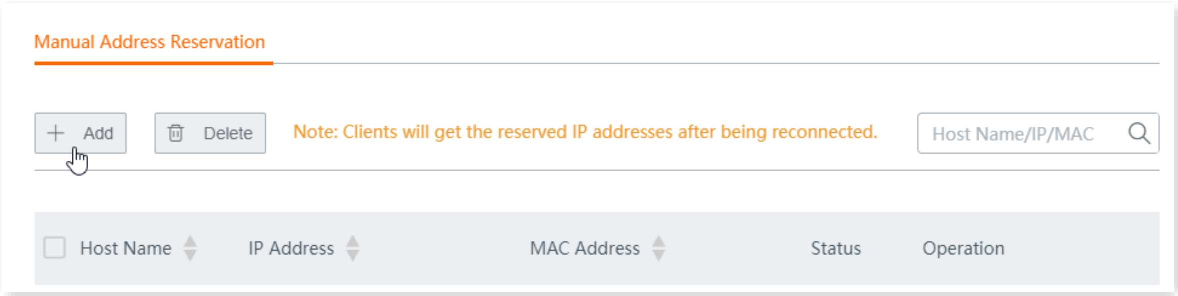
DMZ Host: ● Enable ○ Disable

IP address of DMZ Host: 192.168.0.250

Filter VPN Port: ○ Enable ● Disable

Step 2 Reserve a fixed IP address for the DMZ host.

1. Navigate to **Address Reservation** > **Manual Address Reservation**.
2. Click **+Add**.



Note: Clients will get the reserved IP addresses after being reconnected.

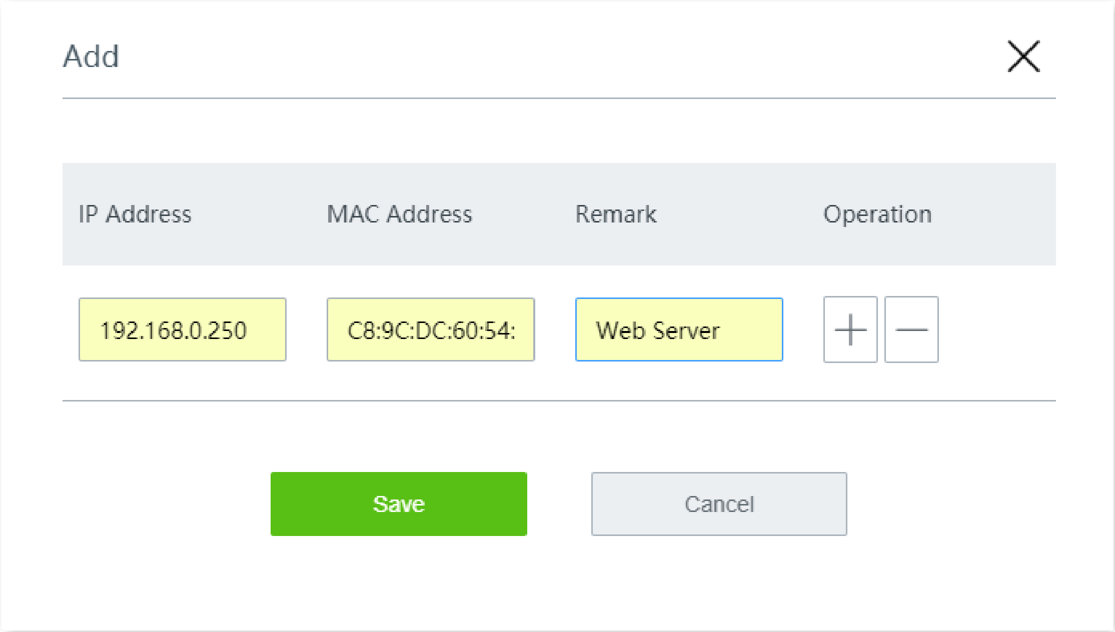
□ Host Name	IP Address	MAC Address	Status	Operation

3. Configure the following parameters in the **Add** window, and click **Save**.

   (1) Set the fixed IP address assigned to the server host, which is **192.168.0.250** in this example.

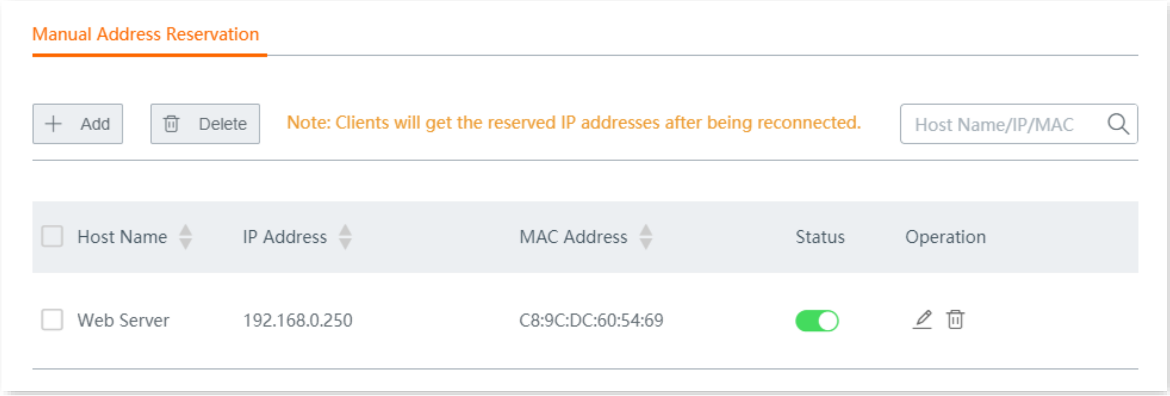
   (2) Enter the MAC address of the server host, which is **C8:9C:DC:60:54:69** in this example.

   (3) (Optional) Enter a remark, such as **Web Server**.



IP Address	MAC Address	Remark	Operation
192.168.0.250	C8:9C:DC:60:54:	Web Server	+ —

Reserved successfully. See the following figure.



Note: Clients will get the reserved IP addresses after being reconnected.

□ Host Name	IP Address	MAC Address	Status	Operation
□ Web Server	192.168.0.250	C8:9C:DC:60:54:69	●	

----End

Verification

Internet users can successfully access the intranet server by using **intranet service application layer protocol name**://**WAN port IP address**:**internal service port**. If you use the default port for the intranet service, the intranet service port number can be excluded from the access address. Under such circumstances, the access address is **intranet service application layer protocol name**://**WAN port IP address**.

In this example, the access address is http://202.105.11.22:9999

You can check the current WAN IP address on the System Status page.

If DDNS is enabled on the WAN port, internet users can also access the intranet server by using **intranet service application layer protocol name**://**WAN port domain name:internal service port**.

TIP

After the configuration, if internet users still cannot access the LAN server, disable the system firewall, anti-virus software or security guard on the DMZ host and try again.

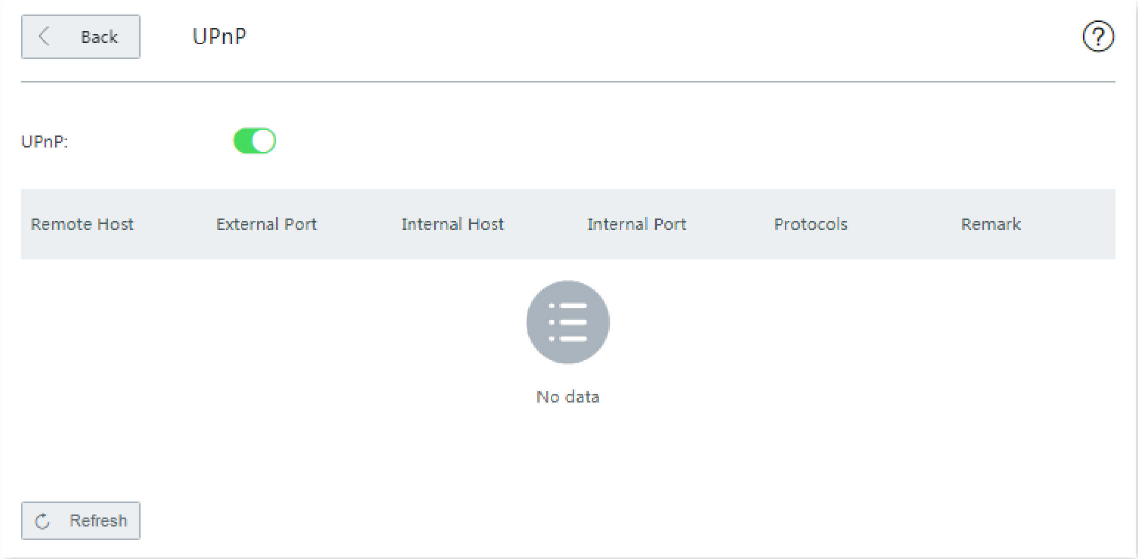
12.7 UPnP

12.7.1 Overview

UPnP is abbreviated for Universal Plug and Play. After the UPnP function is enabled, the router can automatically open port for UPnP-supporting programs in the LAN (such as BitComet and AnyChat) and make these applications run smoother.

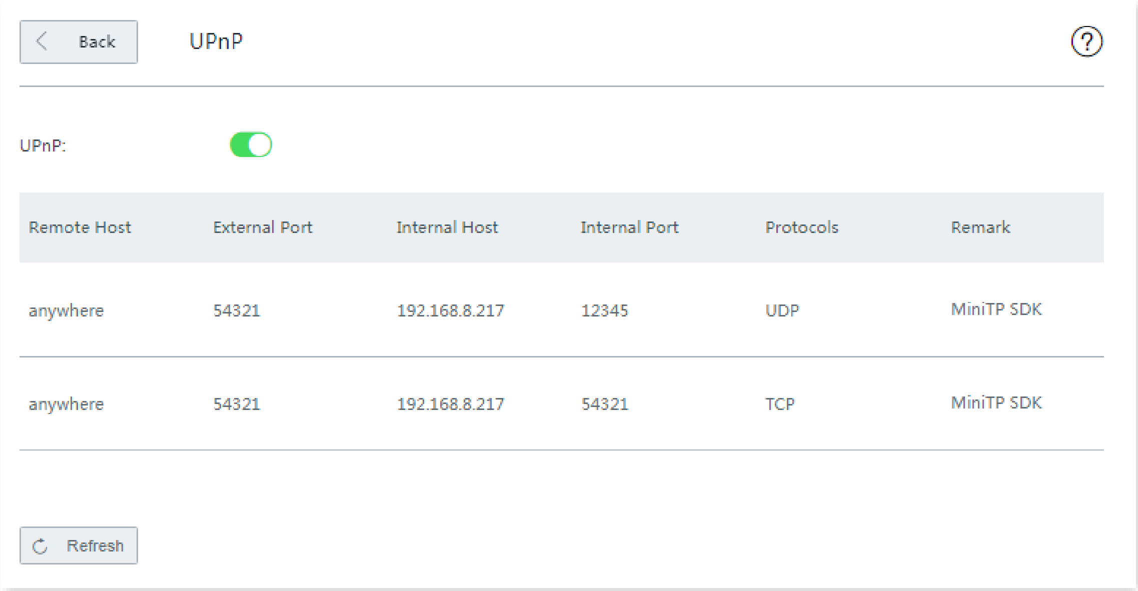
12.7.2 Enable UPnP

Click **More** > **UPnP** to enter the page, and enable **UPnP**.



Remote Host	External Port	Internal Host	Internal Port	Protocols	Remark

If you enable the UPnP function, when UPnP-based programs, such as BitComet and AnyChat, are running on the local network, the external and internal mapping relationships are displayed on the page.



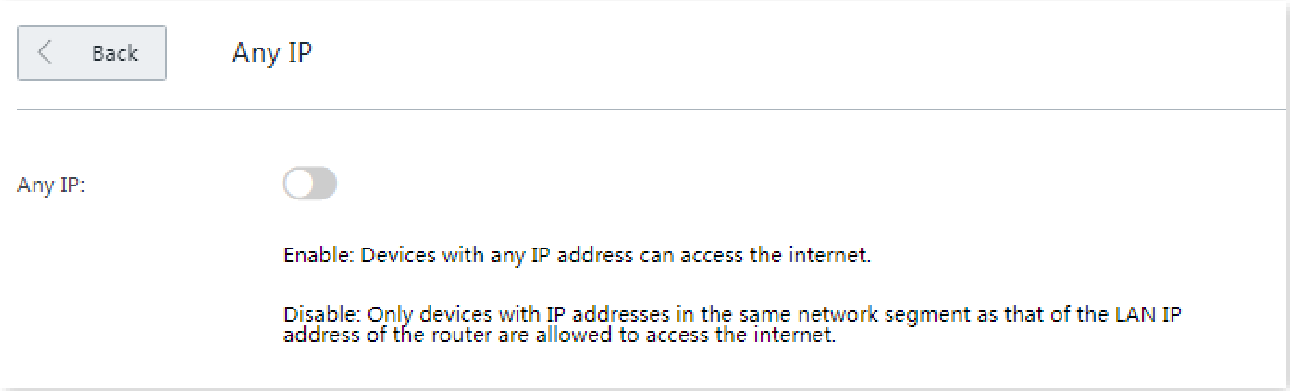
Remote Host	External Port	Internal Host	Internal Port	Protocols	Remark
anywhere	54321	192.168.8.217	12345	UDP	MiniTP SDK
anywhere	54321	192.168.8.217	54321	TCP	MiniTP SDK

12.8 Any IP

Click **More** > **Any IP** to enter the page.

This function is typically used in public spaces, such as at a hotel. With this function enabled, devices in the LAN network with any IP address, gateway and DNS can access the internet through the router, avoiding the issue that the private IP addresses of guests do not match with the hotel network.

By default, this function is disabled. Enable it when necessary.



Any IP: ○

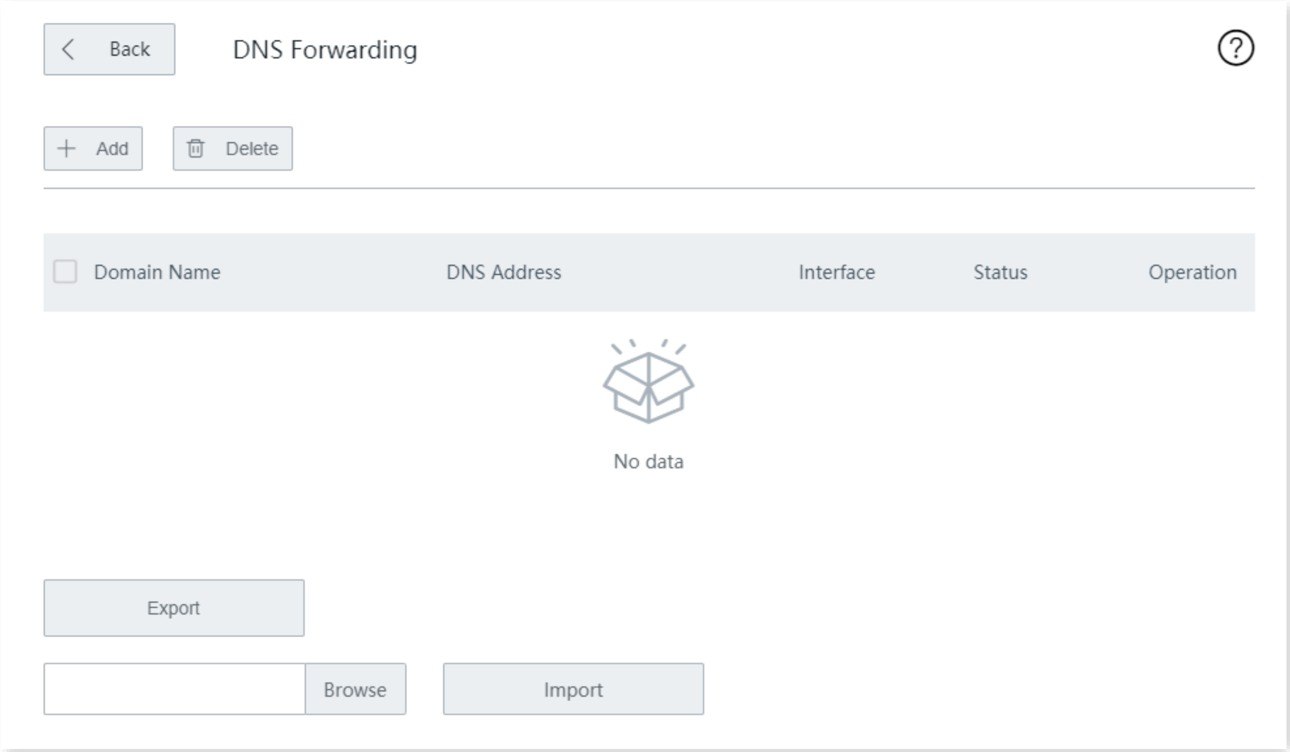
Enable: Devices with any IP address can access the internet.

Disable: Only devices with IP addresses in the same network segment as that of the LAN IP address of the router are allowed to access the internet.

12.9 DNS forwarding

The DNS forwarding function forwards specified domain names to specified DNS servers through the fixed WAN port for DNS address resolution, improving access speed.

Click **More** > **DNS Forwarding** to enter the page.



Parameter description

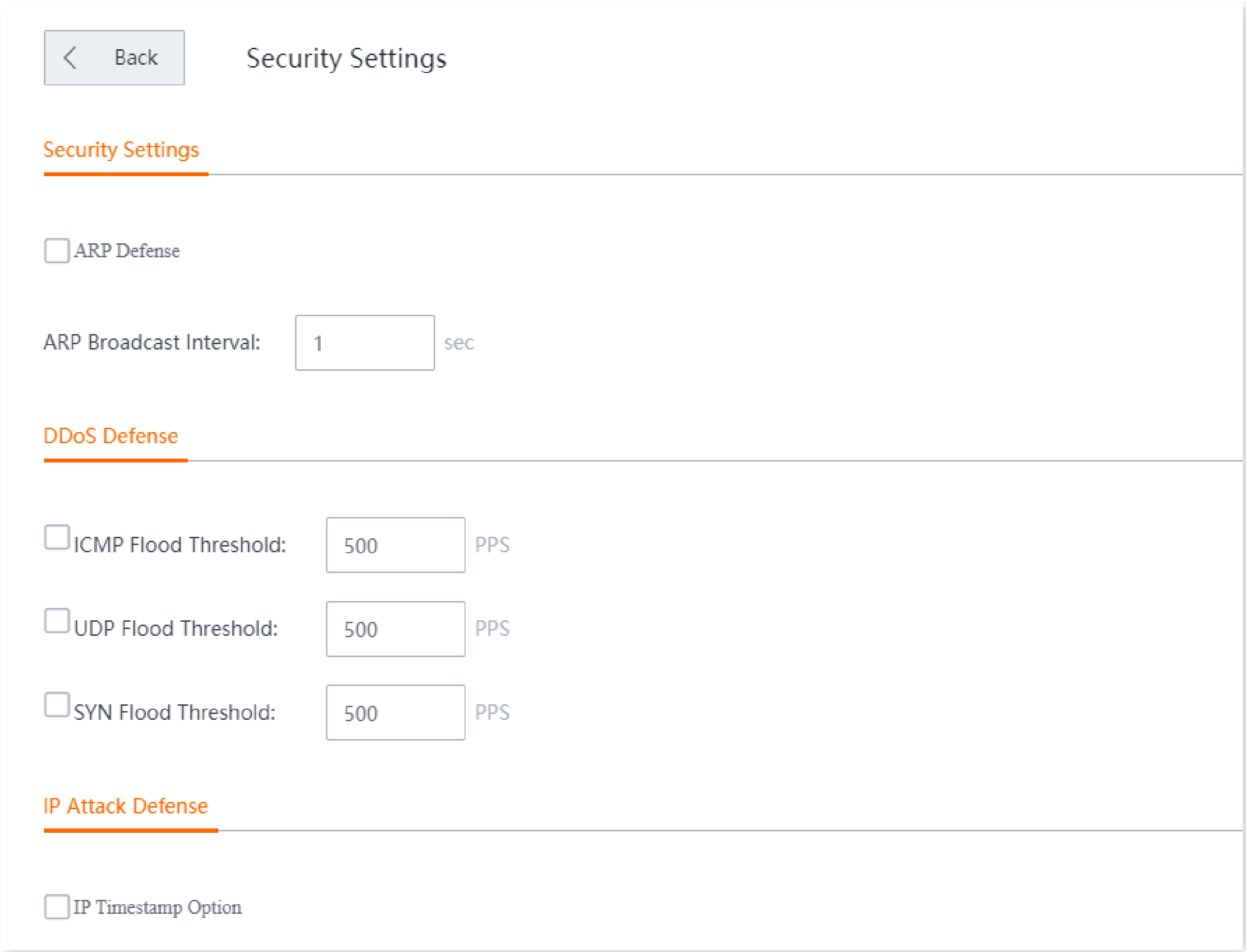
Parameter	Description
Domain Name	Specifies the domain name to be forwarded and resolved.
DNS Address	Specifies the server address that requires DNS resolution.
Interface	Specifies the port through which data goes out of the router. Please set the corresponding WAN port as needed.
Status	Enable or disable the rule.
Operation	Specifies the operations you can perform on the rule. ✎: Click it to edit the rule. 🗑 : Click it to delete the rule.

12.10 Security settings

The router supports ARP Defense, DDoS Defense, IP Attack Defense, and Block WAN Ping security settings.

- **ARP Defense**: This function can identify the ARP spoofing in the local network, and record the MAC addresses of the attacker.
- **DDoS Defense**: DDoS attack, abbreviated for Distributed Denial of Service Attack, makes network resource unavailable to its intended users. The router can block DDoS attack, including ICMP Flood, UDP Flood, and SYN Flood attacks.
- **IP Attack Defense**: With this function enabled, the router can intercept some packets with specified IP options. These IP options include IP Timestamp Option, IP Security Option, IP Stream Option, IP Record Route Option, IP Loose Source Route Option and illegal IP options.
- **Block WAN Ping**: With this function enabled, the router automatically ignores WAN IP address ping requests from internet hosts; therefore, the router avoids exposing itself and defends the external ping attacks.

Click **More** > **Security Settings** to enter the page.



Security Settings

Security Settings

□ ARP Defense

ARP Broadcast Interval: 1 sec

DDoS Defense

□ ICMP Flood Threshold: 500 PPS

□ UDP Flood Threshold: 500 PPS

□ SYN Flood Threshold: 500 PPS

IP Attack Defense

□ IP Timestamp Option

Parameter description

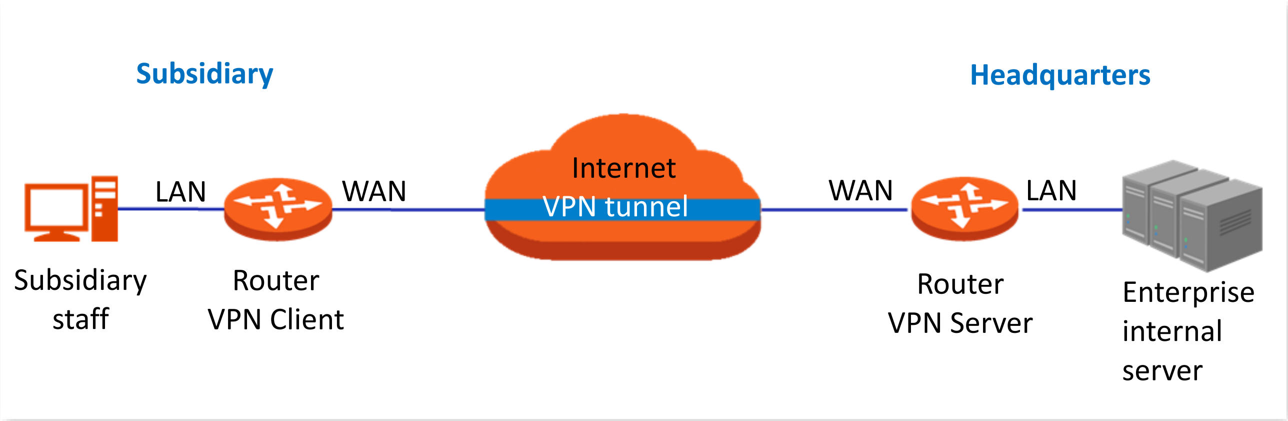
Parameter		Description
Security Settings	ARP Defense	Enable or disable the ARP defense function.
	ARP Broadcast Interval	Specifies the interval at which the router sends ARP broadcast messages.
DDoS Defense	ICMP Flood Threshold	If ICMP request packets from a same host in LAN received by the router exceed this threshold within 1 second, the router suffers ICMP flood attack.
	UDP Flood Threshold	If UDP request packets from a same host in LAN received by the router exceed this threshold within 1 second, the router suffers UDP flood attack.
	SYN Flood Threshold	If TCP SYN request packets from a same host in LAN received by the router exceed this threshold within 1 second, the router suffers SYN flood attack.
IP Attack Defense	IP Timestamp Option	With this function enabled, the router blocks IP packets that contain the Internet Timestamp option in the local network.
	IP Security Option	With this function enabled, the router blocks IP packets that contain the Security option in the local network.
	IP Stream Option	With this function enabled, the router blocks IP packets that contain the Stream ID option in the local network.
	IP Record Route Option	With this function enabled, the router blocks IP packets that contain the Record Route option in the local network.
	IP Loose Source Route Option	With this function enabled, the router blocks IP packets that contain the Loose Source Route option in the local network.
	Rouge IP Option	With this function enabled, the router blocks IP packets that fail to pass integrity and correctness check in the local network.
Block WAN Ping		Enable or disable the block WAN ping function. By default, this function is disabled. After the block WAN ping function is enabled, the router automatically ignores WAN IP address ping requests from internet hosts; therefore, the router avoids exposing itself and defends external ping attacks.

12.11 VPN

12.11.1 Overview

VPN, abbreviated for Virtual Private Network, is a special network set up on the public network (generally the internet). It exists only logically, and does not have any physical lines. The VPN technology is widely used in enterprise networks and is used to achieve resource sharing between a subsidiary and the headquarters, and at the same time, protects these resources from being exposed to other users in the internet.

The typical network topology is shown as below.



The router supports the following VPN services:

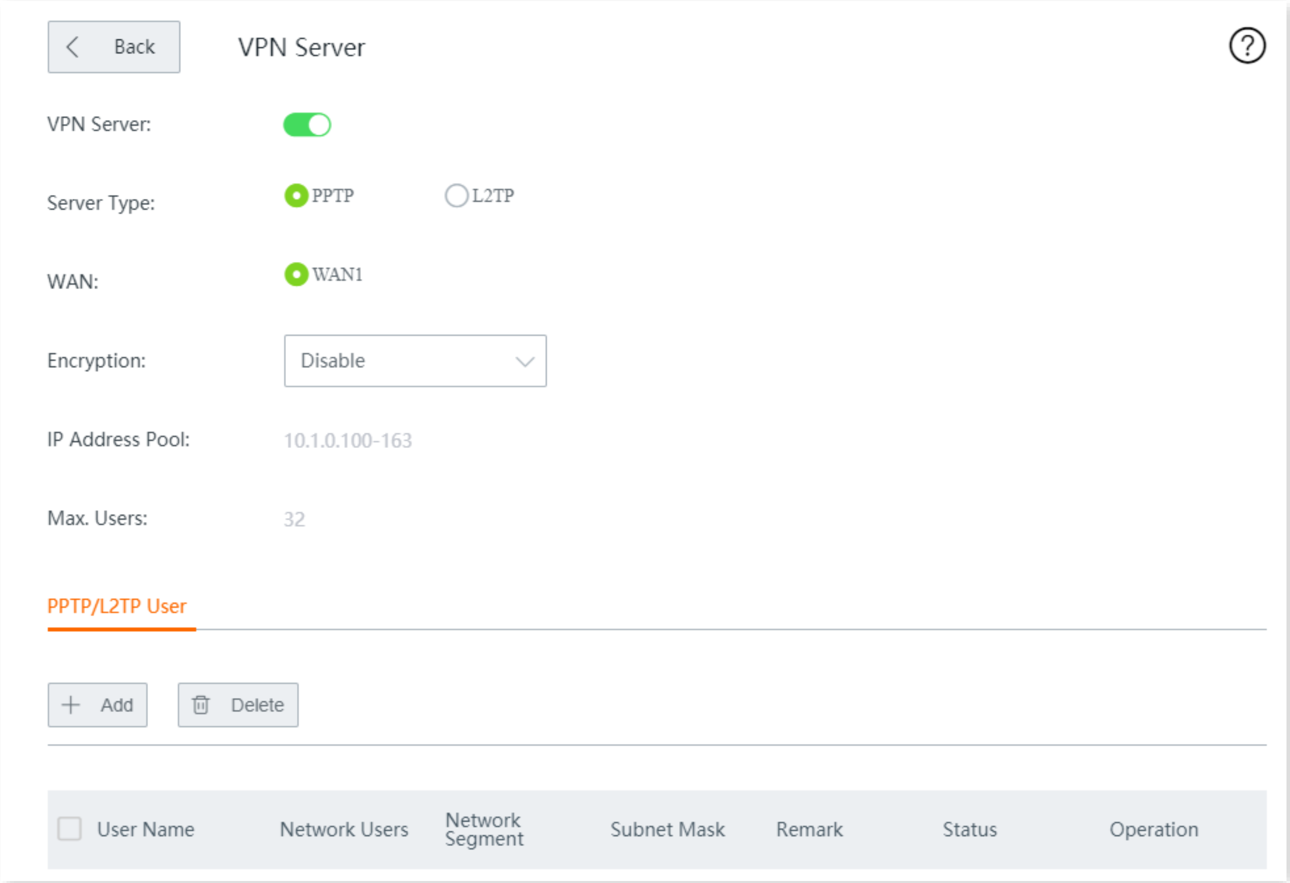
- PPTP/L2TP VPN Server
- PPTP/L2TP VPN Client
- IPSec

12.11.2 VPN server

The router can be used as a PPTP/L2TP server to accept connections from PPTP/L2TP clients.

Click **More** > **VPN Server** to enter the page.

By default, this function is disabled.


VPN Server

VPN Server: on

Server Type: ● PPTP ○ L2TP

WAN: ● WAN1

Encryption: Disable

IP Address Pool: 10.1.0.100-163

Max. Users: 32

PPTP/L2TP User

□ User Name	Network Users	Network Segment	Subnet Mask	Remark	Status	Operation

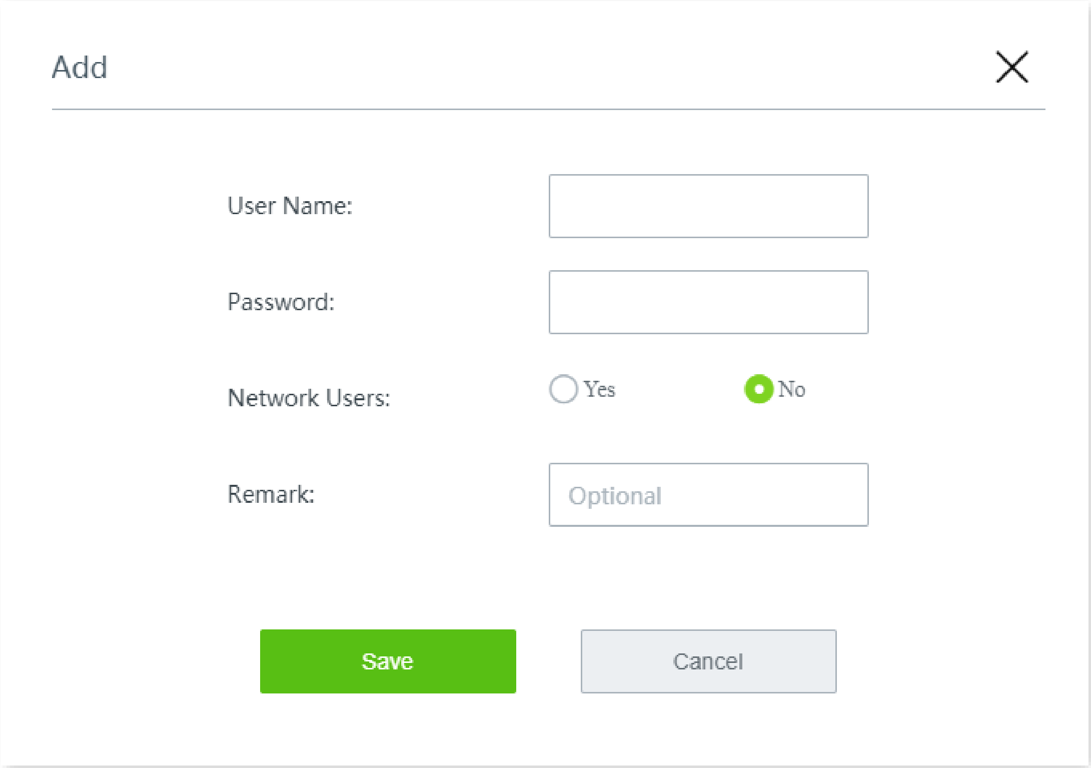
Parameter description

Parameter	Description
VPN Server	Enable or disable the VPN server function. After this function is enabled, the router serves as a VPN server.
Server Type	Specifies the VPN protocol type the router uses, including PPTP and L2TP. Both PPTP and L2TP are layer-2 VPN tunnel protocol and use the PPP to encapsulate data, and both add an additional head for data. - **PPTP:** The router serves as a PPTP server and accepts connections from PPTP clients. - **L2TP:** The router serves as an L2TP server and accepts connections from L2TP clients.
WAN	Specifies the WAN port for setting up a VPN tunnel between the VPN server and the clients. The IP address or domain name of the WAN port is the server IP address/domain name of VPN client.

Parameter	Description
Encryption	Enable or disable 128-bit data encryption. This parameter only appears when PPTP is selected. The encryption configuration of the client and server must be the same. Otherwise, the communication cannot be performed properly.
IPSec Encryption	Enable or disable the IPSec encryption. This parameter only appears when L2TP is selected. If you want to configure IPSec encryption, select the IPSec rules whose encapsulation mode is transport mode.
IP Address Pool	Specifies IP address range that the PPTP/L2TP clients can obtain from the VPN server to be connected.
Max. Users	Specifies the maximum number of VPN clients allowed to connect to the PPTP/L2TP server. The value is fixed to **32**.
User Name	Specifies the user name and password used to dial in a PPTP/L2TP VPN connection.
Password	
Network Users	Specifies the type of the VPN client. • **Yes**: Choose this option when the VPN client is a network. Under such circumstances, you need to set the network segment, subnet mask of the VPN client. • **No**: Choose this option when the VPN client is a host.
Network Segment	When the VPN client is a network, enter the private network prefix of the client.
Subnet Mask	When the VPN client is a network, enter the subnet mask of the client.
Remark	Specifies the remarks of the account.
Status	Specifies whether the corresponding rule is enabled.
Operation	Specifies the operations you can perform on the rule. ✎: Click it to edit the rule. 🗑 : Click it to delete the rule.

Add a PPTP/L2TP user account

Navigate to **More** > **VPN Server** > **PPTP/L2TP User**, click **+Add**, configure the following parameters in the **Add** window, and click **Save**.



User Name:

Password:

Network Users: ○ Yes ● No

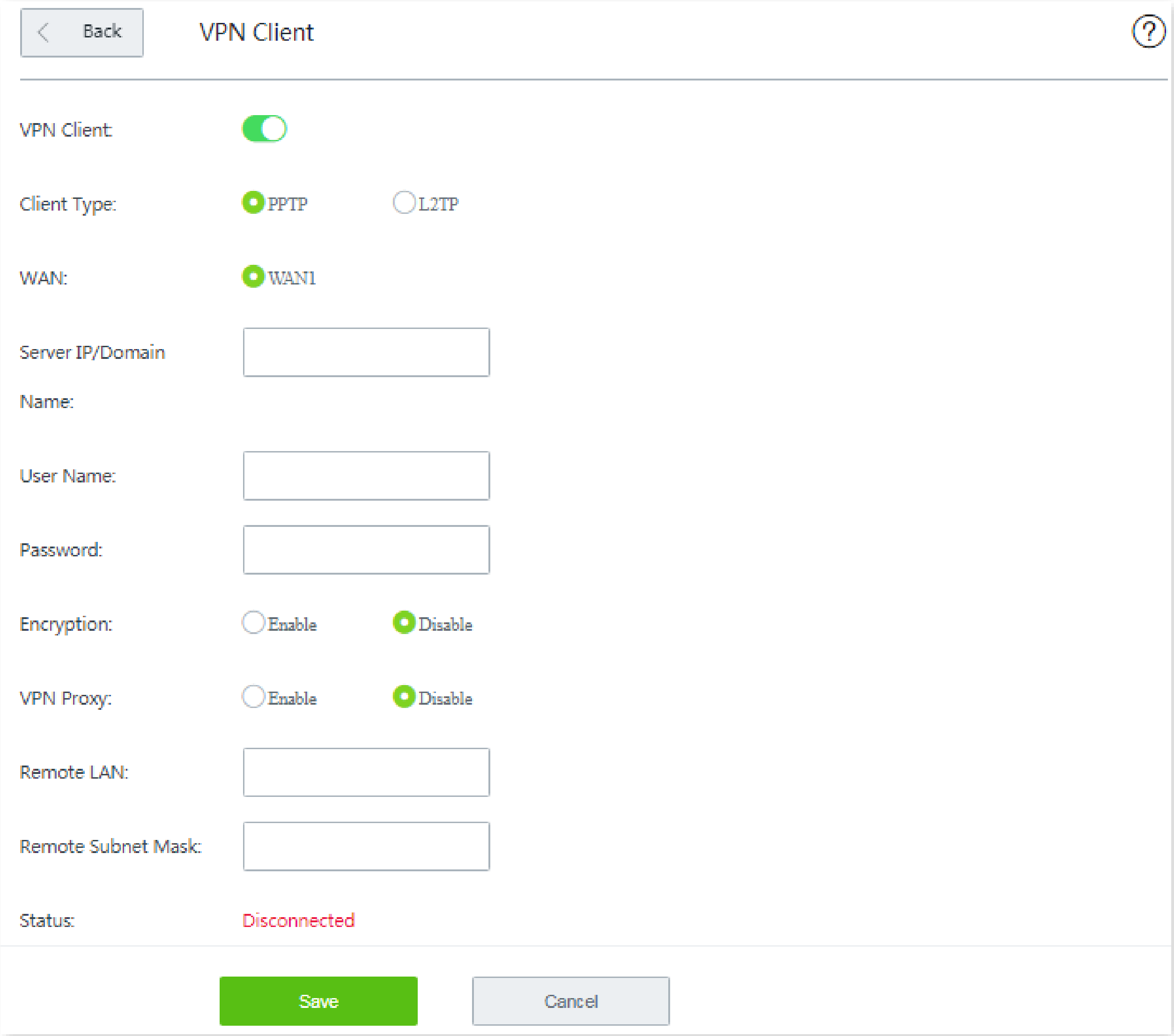
Remark: Optional

12.11.3 VPN client

The router can be used as a PPTP/L2TP client connected to the PPTP/L2TP server.

Click **More** > **VPN Client** to enter the page.

By default, VPN Client is disabled.



VPN Client: ●

Client Type: ● PPTP ○ L2TP

WAN: ● WAN1

Server IP/Domain Name:

User Name:

Password:

Encryption: ○ Enable ● Disable

VPN Proxy: ○ Enable ● Disable

Remote LAN:

Remote Subnet Mask:

Status: Disconnected

Parameter description

Parameter	Description
VPN Client	Enable or disable the VPN client function. After this function is enabled, the router serves as a VPN client.
Client Type	Specifies the VPN protocol type the router uses, including PPTP and L2TP. Both PPTP and L2TP are layer-2 VPN tunnel protocol and use the PPP to encapsulate data, and both add an additional head for data. - **PPTP:** Choose this option if the VPN server to be connected is a PPTP server. - **L2TP:** Choose this option if the VPN server to be connected is an L2TP server.
WAN	Specifies the WAN port the router uses for VPN dial-up.

Parameter	Description
Server IP/Domain Name	Specifies the IP address or domain name of the VPN server to be connected, which is generally the IP address or domain name of the WAN port enabling the PPTP/L2TP server function of the peer VPN router.
User Name	Specifies the PPTP/L2TP user account, which is the user name and password assigned by the VPN server.
Password	
Encryption	Enable or disable data encryption. This parameter only appears when PPTP is selected. The encryption configuration of the client and server must be the same. Otherwise, the communication cannot be performed properly.
VPN Proxy	After this function is enabled, LAN users access the internet through the VPN server-side router.
Remote LAN	Specifies the network segment of the LAN of the VPN server.
Remote Subnet Mask	Specifies the subnet mask of the LAN of the VPN server.
Status	Specifies the current connection status of the VPN.

12.11.4 IPSec

IP Security (IPSec) is a protocol suite for transmitting data over the internet in a secure and encrypted manner.

- **Encapsulation mode**

  Encapsulation mode specifies encapsulation mode of the data transmitted by IPSec. IPSec supports **Tunnel** and **Transport** modes.

  - **Tunnel**: This mode adds an additional IP head and is most commonly used between gateways. The whole IP data packet of the user is used to calculate the AH or ESP head. AH or ESP head and the user data encrypted by ESP are encapsulated in a new IP data packet.
  - **Transport**: This mode does not change the original IP head and is most commonly used between hosts. Only the data at the transmission layer is used to calculate AH or ESP head. AH or ESP head or user data encrypted by ESP are placed behind the original IP packet head.

- **Security gateway**

  It refers to a gateway (secure and encrypted router) with the IPSec functionality. IPSec is used to protect data exchanged between such gateways from being tampered and peeped.

- **IPSec peer**

  The two IPSec terminals are called IPSec peers. The two peers (security gateways) can securely exchange data only after a Security Association (SA) is set up between them.

- **SA**

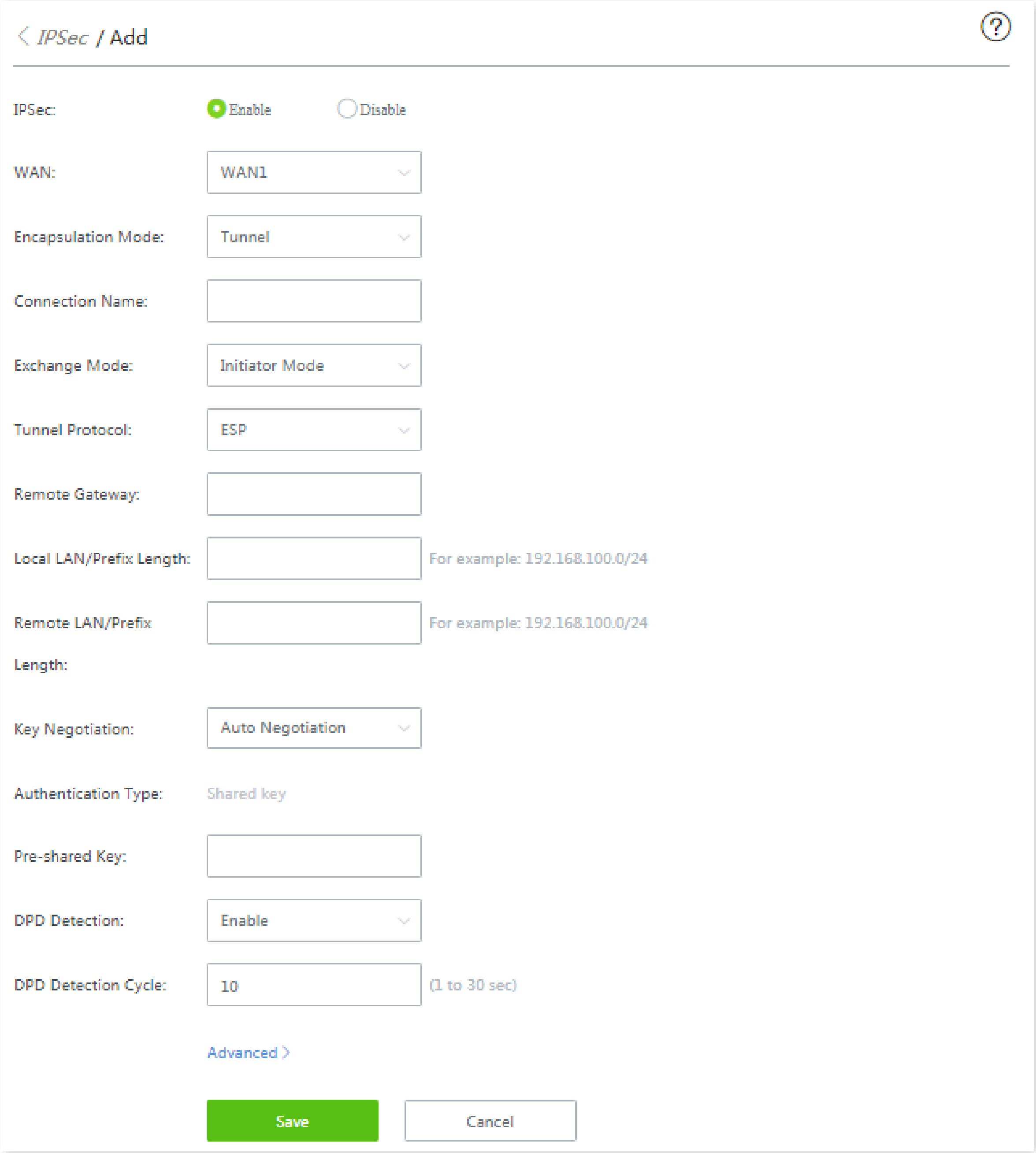
  SA specifies some elements of the peers, such as the base protocol (AH, ESP, or both), encapsulation mode (transport or tunnel), encryption algorithm (DES, 3DES, or AES), shared key for data protection in specified flows, and life cycle of the key. SA has the following features:

  - A triplet {SPI, Destination IP address, Security protocol identifier} is used as a unique ID.
  - An SA specifies the protocol, algorithm, and key for processing packets.
  - Each IPsec SA is unidirectional with a life cycle.
  - An SA can be created manually or generated automatically using internet Key Exchange (IKE). The IKE protocol has two versions of IKEv1 and IKEv2. The device supports IKEv1 and the IKE hereinafter stands for IKEv1.

Configure IPSec connection: Tunnel mode

Click **More** > **IPSec** to enter the page. Click **+Add**, select the **Tunnel** mode, configure the following parameters in the window, and click **Save**.

The router supports both **Tunnel** mode (default) and **Transport** mode.



IPSec / Add

IPSec: ● Enable ○ Disable

WAN: WAN1

Encapsulation Mode: Tunnel

Connection Name:

Exchange Mode: Initiator Mode

Tunnel Protocol: ESP

Remote Gateway:

Local LAN/Prefix Length: For example: 192.168.100.0/24

Remote LAN/Prefix Length: For example: 192.168.100.0/24

Key Negotiation: Auto Negotiation

Authentication Type: Shared key

Pre-shared Key:

DPD Detection: Enable

DPD Detection Cycle: 10 (1 to 30 sec)

Parameter description

Parameter	Description
IPSec	Enable or disable the IPSec function.
WAN	Specifies the WAN port over which the IPSec function takes effect. The remote gateway address of the IPSec peer device should be the IP address of this interface.

Parameter	Description
Encapsulation Mode	Specifies the IPSec data encapsulation mode. • **Tunnel**: This mode is generally used between two security gateways. • **Transport:** This mode is generally used between hosts or host and gateway.
Connection Name	Specifies the name of the IPSec connection.
Exchange Mode	Specifies the exchange mode of the IPSec tunnel. • **Initiator Mode**: The device sends a connection request to the peer device. • **Responder Mode**: The device waits for the peer device to send a connection request. TIP Do not set both ends of the IPSec tunnel as **Responder Mode**; otherwise, the IPSec tunnel setup fails.
Tunnel Protocol	Specifies the protocol which offers the security service for IPSec. • **AH**: It is abbreviated for Authentication Header. This protocol is used for verifying data integrity. If a packet is tampered during transmission, the receiver discards it during data integrity verification. • **ESP**: It is abbreviated for Encapsulating Security Payload. This protocol is used for verifying data integrity and encrypting data. If a packet processed using this protocol is intercepted during transmission, it is difficult for the intercepting party to obtain the real information contained in the packet. This compatible protocol is widely used in gateway products. • **AH+ESP**: It indicates that the function features both AH and ESP.
Remote Gateway	Specifies the IP address or domain name of the peer gateway of the IPSec tunnel.
Local LAN/Prefix Length	Specifies the network segment/prefix length of the LAN of the device. For example, if the IP address of the LAN port of the device is 192.168.0.1 and the subnet mask is 255.255.255.0, the local LAN/prefix length can be 192.168.0.0/24.
Remote LAN/Prefix Length	Specifies the network segment/prefix length of the LAN of the peer gateway of the IPSec tunnel. If the peer device is a host, this parameter can be set as “the IP address of the device/32”.
Key Negotiation	Specifies the key negotiation mode of the IPSec security tunnel. • **Auto Negotiation**: It indicates that an SA is set up, maintained, and deleted automatically using IKE (Internet Key Exchange). This reduces configuration complexity and simplifies IPSec usage and management. Such an SA (Security Association) has a life cycle and is updated regularly, leading to higher security. • **Manual:** It indicates that an SA is set up by manually specifying encryption and authentication algorithms and keys. Such an SA does not have a life cycle, and therefore it remains valid unless being manually deleted, leading to security risks. Generally, this mode is used only for commissioning.

Key negotiation: Auto negotiation

To protect information confidentiality when using auto negotiation, IKE is in place to negotiate keys for secure communication between IPSec peers. The IKE protocol is a hybrid of three other protocols:

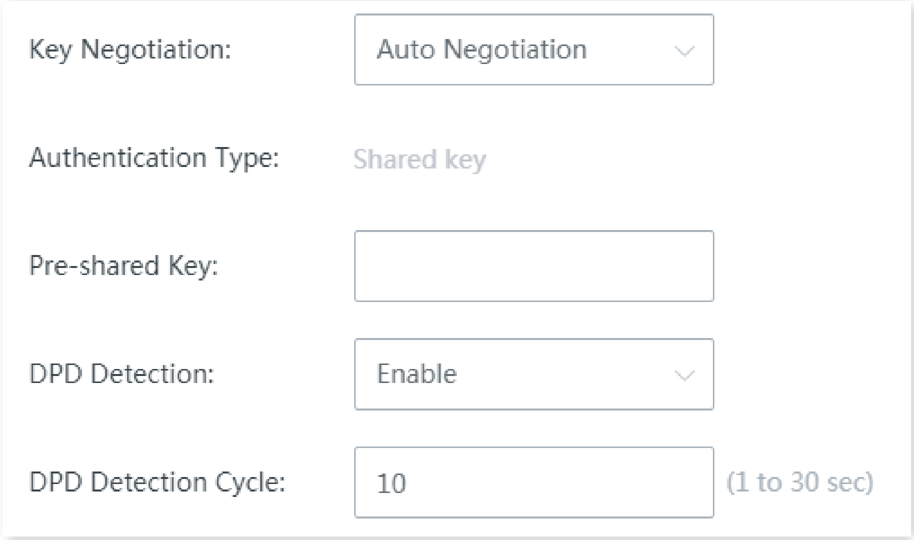
- **ISAKMP**: Internet Security Association and Key Management Protocol. It defines the procedures for authenticating a communicating peer, creation and management of Security Associations, key generation techniques, and threat mitigation.
- **Oakley**: Oakley Key Determination Protocol. It defines the specific key negotiation mechanism.
- **SKEME**: A secure and versatile key exchange protocol for key management over internet is presented.

IKE negotiation can be broken down into two periods.

Period 1: The communicating parties negotiate exchange and authentication algorithm, encryption algorithm and other security protocols, and generate an ISAKMP SA which is used to exchange more information in phase II.

Period 2: The ISAKMP SA set up in phase I is used as the security agreement negotiation parameter of IPSec to create IPSec SA, which is used to protect the communication data of both parties

When **Auto Negotiation** is selected, the following page appears.



Key Negotiation: Auto Negotiation

Authentication Type: Shared key

Pre-shared Key:

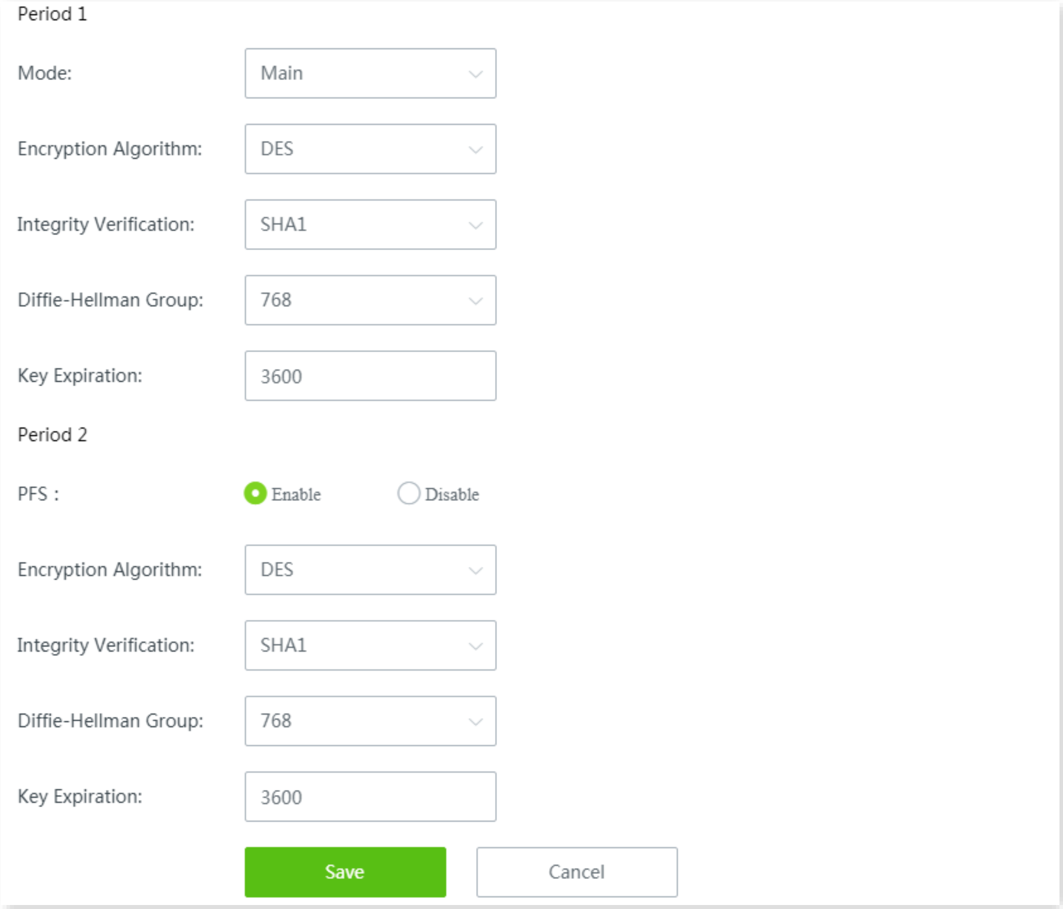
DPD Detection: Enable

DPD Detection Cycle: 10 (1 to 30 sec)

Parameter description

Parameter	Description
Authentication Type	Specifies the shared key mode, which indicates a shared key string negotiated by IPSec parties with some way in advance.
Pre-shared Key	Specifies the pre-shared key used during negotiation. This parameter must be the same with that of the peer gateway. A maximum of 128 characters are allowed.
DPD Detection	Enable or disable the DPD Detection. This function can detect whether the remote tunnel site is valid.
DPD Detection Cycle	Specifies the cycle of transmitting DPD packets. The device transmits DPD packets based on the cycle set here. If the DPD packets are not confirmed by the remote peer device during the cycle period, the device re-initializes the IPSec SA between the both sides.

Click **Advanced**, and the following configuration area appears.



Period 1

Mode: Main

Encryption Algorithm: DES

Integrity Verification: SHA1

Diffie-Hellman Group: 768

Key Expiration: 3600

Period 2

PFS : ● Enable ○ Disable

Encryption Algorithm: DES

Integrity Verification: SHA1

Diffie-Hellman Group: 768

Key Expiration: 3600

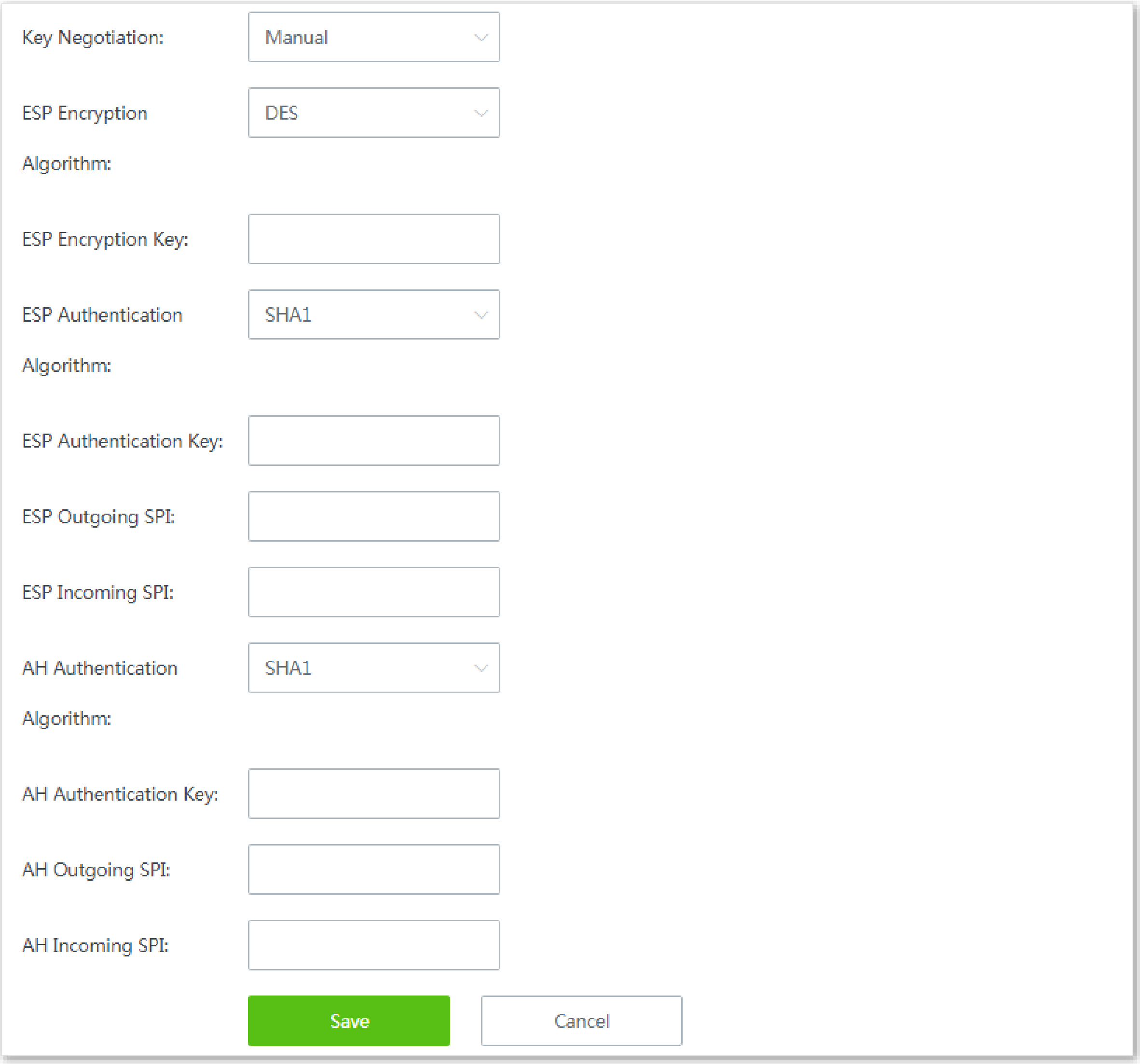
Parameter description

Parameter	Description
Mode	Specifies the exchange mode in IKE phase I, which should be the same as that of peer gateway. - **Main**: This mode is the primary mode. In this mode, exchanged packets are huge to offer identity protection, which is applicable to scenarios where identity protection is rigorous. - **Aggressive**: This mode does not offer identity protection. In this mode, the exchanged packets are few in number and negotiation rate is high, which is applicable to scenarios where identity protection is loose.
Encryption Algorithm	Specifies the IKE session encryption algorithm. The router supports the following algorithms: - **DES (Data Encryption Standard)**: A 56-bit key is used to encrypt 64-bit data. The last 8 bits of the 64-bit data are used for parity check. **3DES** indicates that three 56-bit keys are used for encryption. - **AES (Advanced Encryption Standard)**: **AES 128/192/256** indicates that 128/192/256-bit keys are used for encryption respectively.
Integrity Verification	Specifies the IKE session verification algorithm. The router supports the following algorithms: - **MD5 (Message Digest Algorithm)**: A 128-bit message digest is generated to prevent message tampering. - **SHA1 (Secure Hash Algorithm)**: A 160-bit message digest is generated to prevent message tampering, leading to higher security than MD5.

Parameter	Description
Diffle-Hellman Group	Specifies the group information for the Diffie-Hellman algorithm for generating a session key used to encrypt an IKE tunnel.
Local ID Type	Specifies the ID of the local gateway. - **IP Address**: The router uses the IP address of the specified WAN port for negotiation with the remote gateway. - **FQDN**: Fully Qualified Domain Name. If you select FQDN, you need to manually set a string of characters, which should be identical with the remote ID. TIP **Local ID Type** and **Peer ID Type** should be the same. Under such circumstances, you are recommended to modify the **Mode** to **Aggressive**.
Peer ID Type	Specifies the ID of the remote gateway. - **IP Address**: By default, the remote gateway uses the WAN IP address of the router for negotiation. - **FQDN**: Fully Qualified Domain Name. If you select FQDN, you need to manually set a string of characters, which should be identical with the local ID. TIP **Local ID Type** and **Peer ID Type** should be the same. Under such circumstances, you are recommended to modify the **Mode** to **Aggressive**.
Key Expiration	Specifies the life cycle of ISAKMP SA.
PFS	This feature generates a new key in IKE Phase II, which is unrelated to the key generated in IKE Phase I, ensuring that the key generated in Phase II is secure even if the key generated in IKE1 Phase I is cracked. With the PFS disabled, generation of the new key in IKE Phase II depends on the key in Phase I. Once the key generated in IKE Phase I is cracked, the key generated in Phase II will suffer threats, and further threatens the communication security.

Key negotiation: Manual

The following displays the page when **Manual** is selected for **Key Negotiation** (Tunnel protocol AH+ESP is used for illustration here).



Key Negotiation: Manual

ESP Encryption Algorithm: DES

ESP Encryption Key:

ESP Authentication Algorithm: SHA1

ESP Authentication Key:

ESP Outgoing SPI:

ESP Incoming SPI:

AH Authentication Algorithm: SHA1

AH Authentication Key:

AH Outgoing SPI:

AH Incoming SPI:

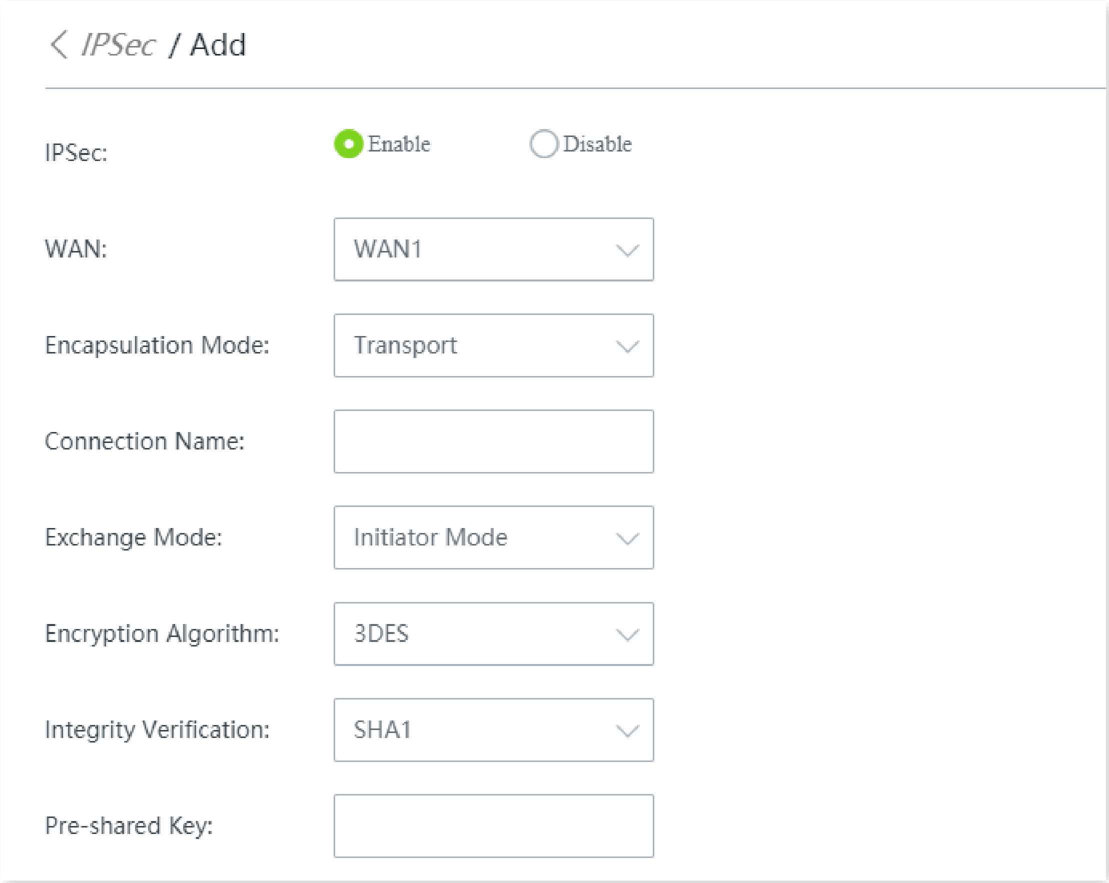
Parameter description

Parameter	Description
ESP Encryption Algorithm	When the **Tunnel Protocol** is set to **ESP**, the **ESP** encryption algorithm is required. The router supports the following algorithms: • **DES**: A 56-bit key is used to encrypt 64-bit data. The last 8 bits of the 64-bit data are used for parity check. **3DES** indicates that three 56-bit keys are used for encryption. • **AES**: A 128/192/256-bit key is used for encryption.
ESP Encryption Key	Specifies the ESP encryption key. Both IPSec communication parties should have the same key.
ESP/AH Authentication Algorithm	When the **Tunnel Protocol** is set to **ESP** or **AH**, the corresponding encryption algorithm is required. The router supports the following algorithms: • **MD5**: A 128-bit message digest is generated to prevent message tampering. • **SHA1**: A 160-bit message digest is generated to prevent message tampering.

Parameter	Description
ESP/AH Authentication Key	When the **Tunnel Protocol** is set to **ESP** or **AH**, the corresponding authentication key is required. Both IPSec communication parties should have the same key.
ESP/AH Outgoing SPI	Specifies the outgoing SPI. SPI, remote gateway address, protocol type identify an IPSec security community. This parameter must be the same with the incoming SPI of the peer device.
ESP/AH Incoming SPI	Specifies the incoming SPI. SPI, remote gateway address, protocol type identify an IPSec security community. This parameter must be the same with the outgoing SPI of the peer device.

Configure IPSec connection: Transport mode

Click **More** > **IPSec** to enter the page. Click **+Add**, select the **Transport** mode, configure the following parameters in the window, and click **Save**.



< *IPSec* / Add

IPSec: ● Enable ○ Disable

WAN: WAN1

Encapsulation Mode: Transport

Connection Name:

Exchange Mode: Initiator Mode

Encryption Algorithm: 3DES

Integrity Verification: SHA1

Pre-shared Key:

Parameter description

Parameter	Description
IPSec	Enable or disable the IPSec function.
WAN	Specifies the WAN port over which the IPSec function takes effect. The remote gateway address of the IPSec peer device should be the IP address of this interface.
Encapsulation Mode	Specifies the IPSec data encapsulation mode. • **Tunnel**: This mode is generally used between two security gateways. • **Transport:** This mode is generally used between hosts or host and gateway.
Connection Name	Specifies the name of the IPSec connection.
Exchange Mode	Specifies the exchange mode of the IPSec tunnel. • **Initiator Mode**: The device sends a connection request to the peer device. • **Responder Mode**: The device waits for the peer device to send a connection request. TIP Do not set both ends of the IPSec tunnel as **Responder Mode**; otherwise, the IPSec tunnel setup fails.

Parameter	Description
Encryption Algorithm	Specifies the IKE session encryption algorithm. The router supports the following algorithms: - **DES (Data Encryption Standard)**: A 56-bit key is used to encrypt 64-bit data. The last 8 bits of the 64-bit data are used for parity check. **3DES** indicates that three 56-bit keys are used for encryption. - **AES (Advanced Encryption Standard)**: **AES 128/192/256** indicates that 128/192/256-bit keys are used for encryption respectively.
Integrity Verification	Specifies the IKE session verification algorithm. The router supports the following algorithms: - **MD5 (Message Digest Algorithm)**: A 128-bit message digest is generated to prevent message tampering. - **SHA1 (Secure Hash Algorithm)**: A 160-bit message digest is generated to prevent message tampering, leading to higher security than MD5.
Pre-shared Key	Specifies the pre-shared key used during negotiation. This parameter must be the same with that of the peer gateway. A maximum of 128 characters are allowed.

12.11.5 Example of configuring a PPTP/L2TP VPN

Networking requirement

An enterprise and its subsidiary both use the wireless routers to set up a network and the routers have been connected to the internet.

The enterprise has the following requirement:

Subsidiary staff can access the LAN resources through the internet, such as documents, OA, ERP system, CRM system, project management system and other resources.

Solution

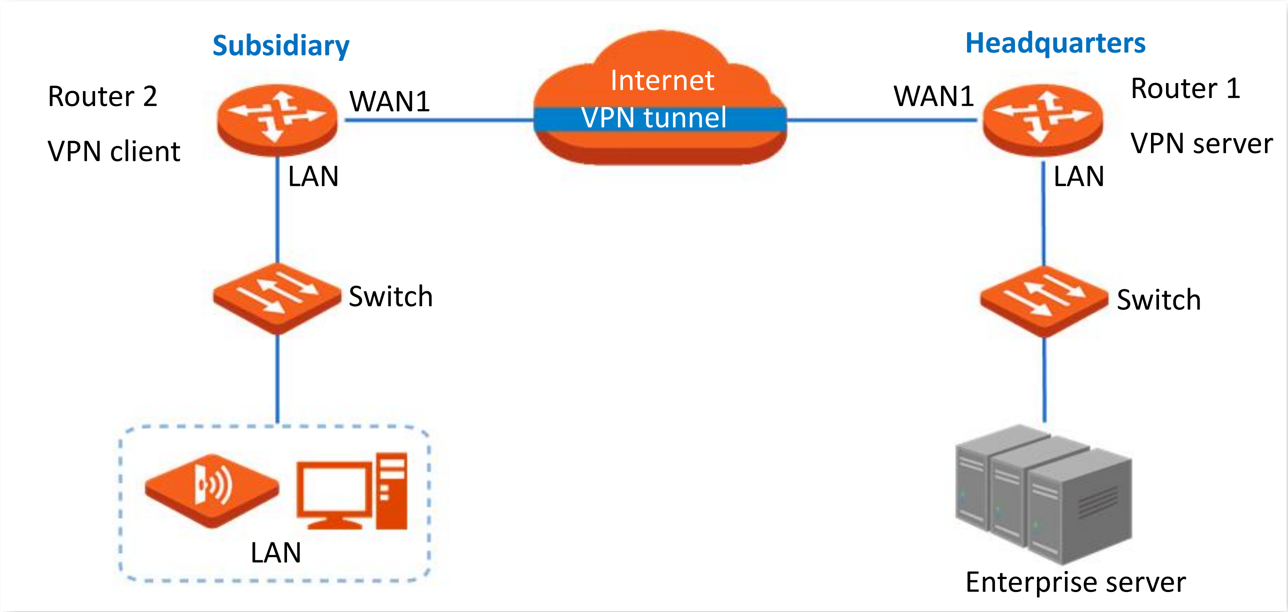
Set a router as the VPN server and the other as the VPN client to enable remote users to securely access the LAN through the internet. PPTP VPN is taken as an example here and the configuration for L2TP VPN is the same.

Assume that router 1 is set as the PPTP server and its basic information is as follows:

- User name and password assigned by the PPTP server: Subsidiary 1
- IP address of the PPTP server: 202.105.11.22
- Data encryption is enabled on the PPTP server.
- Intranet of the PPTP server: 192.168.0.0/24
- Port of the PPTP server to establish a VPN tunnel: WAN1

Assume that router 2 is set as the PPTP client and its basic information is as follows:

- Intranet of the PPTP client: 192.168.1.0/24
- Port of the PPTP client to establish a VPN tunnel: WAN1



Configuration procedure

Set router 1 as VPN server → Set router 2 as VPN client

Step 1 Set router 1 as the VPN server.

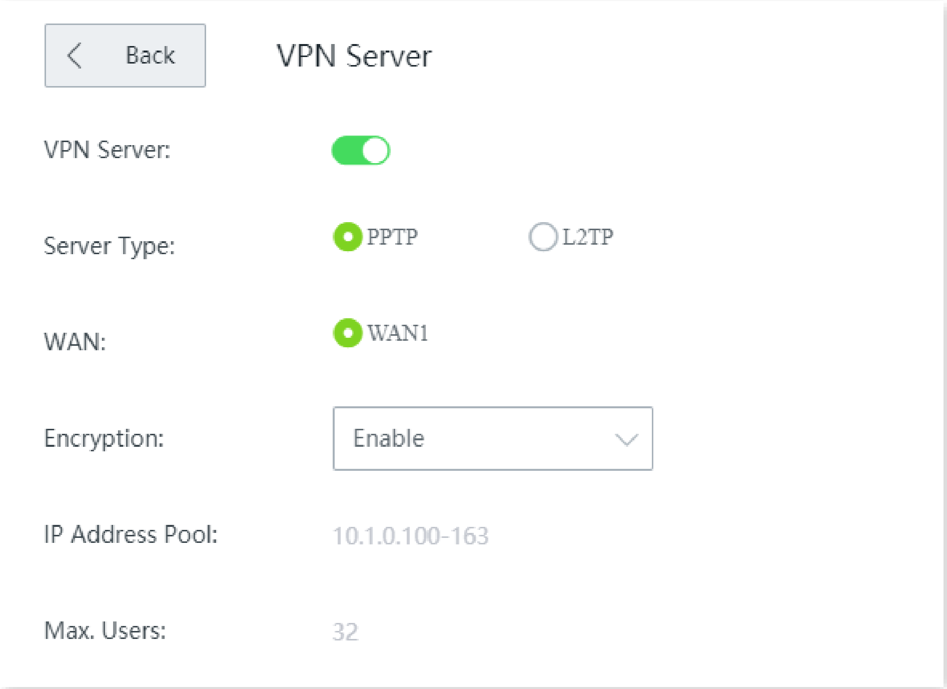
1. Enable the PPTP server.

   (1) Log in to the web UI of router 1, and navigate to **More** > **VPN Server**.

   (2) Enable **VPN Server**.

   (3) Configure the following parameters, and click **Save** at the bottom of the page.

   - Select **Server Type**, which is **PPTP** in this example.
   - Select the WAN port for setting up a VPN tunnel between the VPN server and client, which is **WAN1** in this example.
   - Enable **Encryption**.



VPN Server

VPN Server: ●

Server Type: ● PPTP ○ L2TP

WAN: ● WAN1

Encryption: Enable

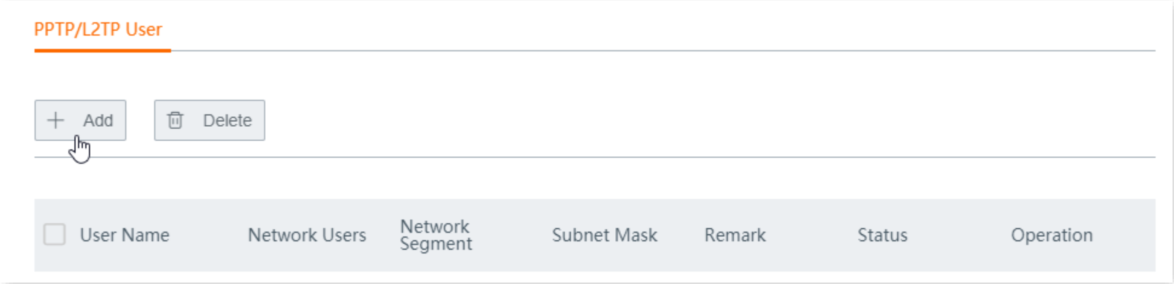
IP Address Pool: 10.1.0.100-163

Max. Users: 32

2. Configure the PPTP/L2TP user.

   (1) Navigate to **More** > **VPN Server** > **PPTP/L2TP user**.

   (2) Click **+Add**.

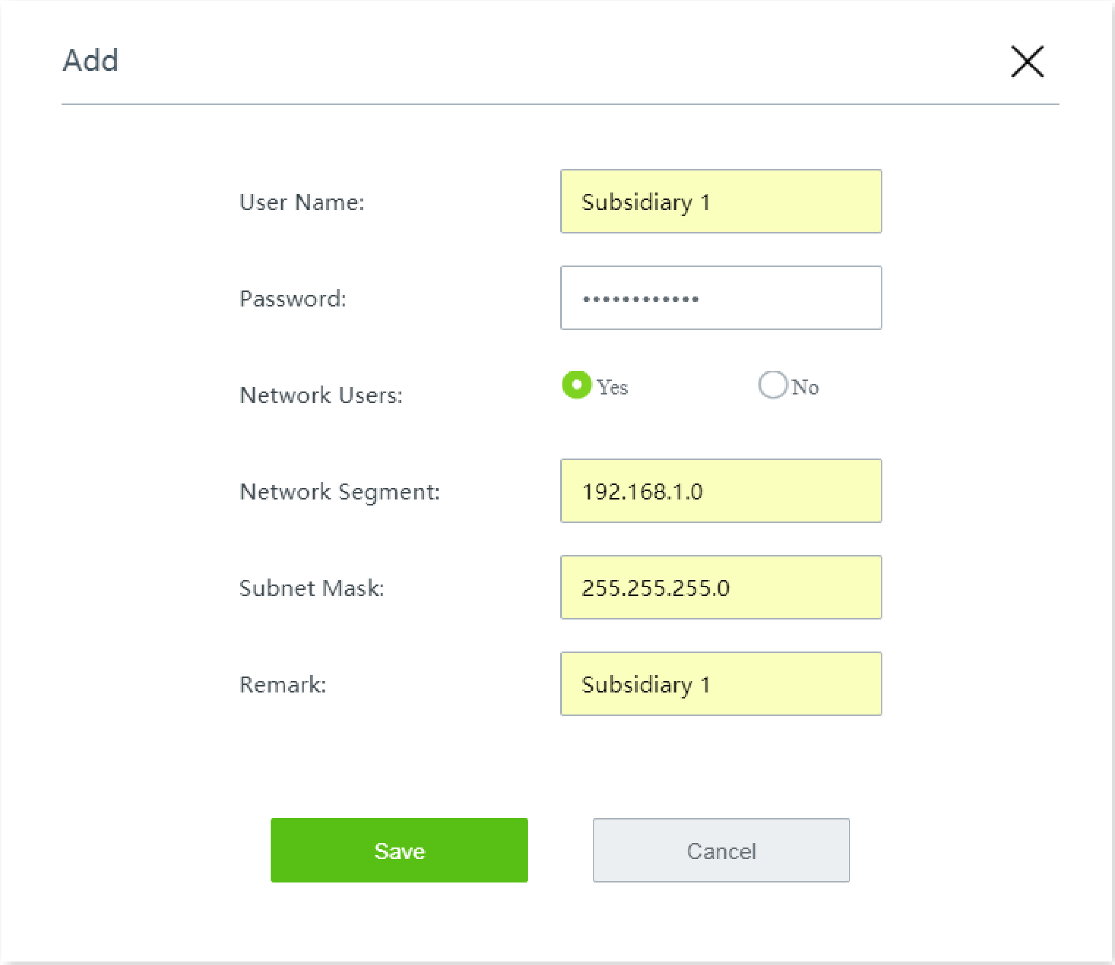


□ User Name	Network Users	Network Segment	Subnet Mask	Remark	Status	Operation

   (3) Configure the following parameters in the **Add** window, and click **Save**.

   - Enter the **User Name** the VPN client uses for VPN connection, which is **Subsidiary 1** in this example.
   - Enter the **Password**, which is **Subsidiary 1** in this example.
   - Select **Yes** for **Network Users**.
   - Enter the **Network Segment** of the VPN client LAN, which is **192.168.1.0** in this example.
   - Enter the **Subnet Mask**, which is **255.255.255.0** in this example.

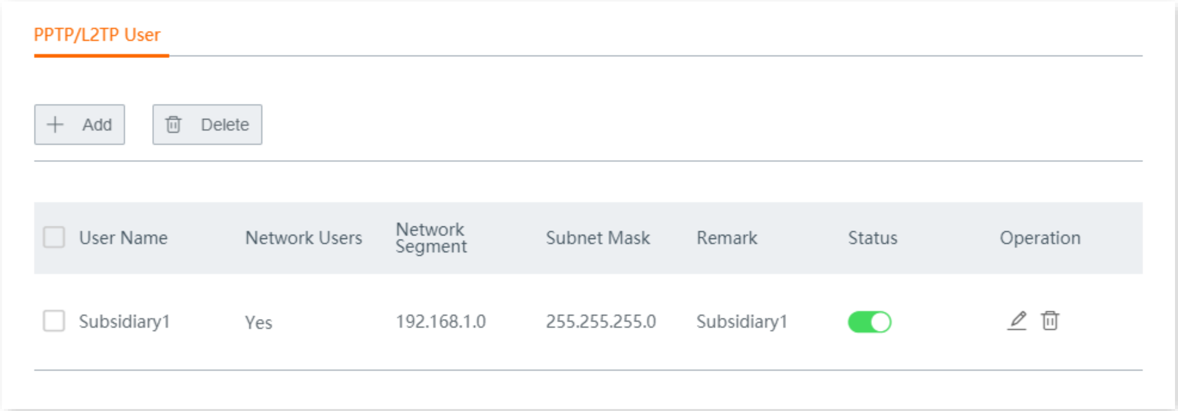
- Enter a **Remark** for the user account, which is **Subsidiary 1** in this example.



Add

User Name:	Subsidiary 1
Password:	••••••••••••
Network Users:	● Yes ○ No
Network Segment:	192.168.1.0
Subnet Mask:	255.255.255.0
Remark:	Subsidiary 1

Added successfully. See the following figure.



PPTP/L2TP User

□ User Name	Network Users	Network Segment	Subnet Mask	Remark	Status	Operation
□ Subsidiary1	Yes	192.168.1.0	255.255.255.0	Subsidiary1	●	✎ 🗑

Step 2 Set router 2 as the VPN client.

1. Log in to the web UI of router 2, and navigate to **More** > **VPN Client**.
2. Enable **VPN Client**.
3. Configure the following parameters, and click **Save** at the bottom of the page.

(1) Select the **Client Type** same as the server type, which is **PPTP** in this example.

(2) Select the WAN port for setting up a VPN tunnel between the VPN server and client, which is **WAN1** in this example.

(3) Enter the **Serve IP/Domain Name** of the WAN port which serves as the egress at the VPN server side, which is **202.105.11.22** in this example.

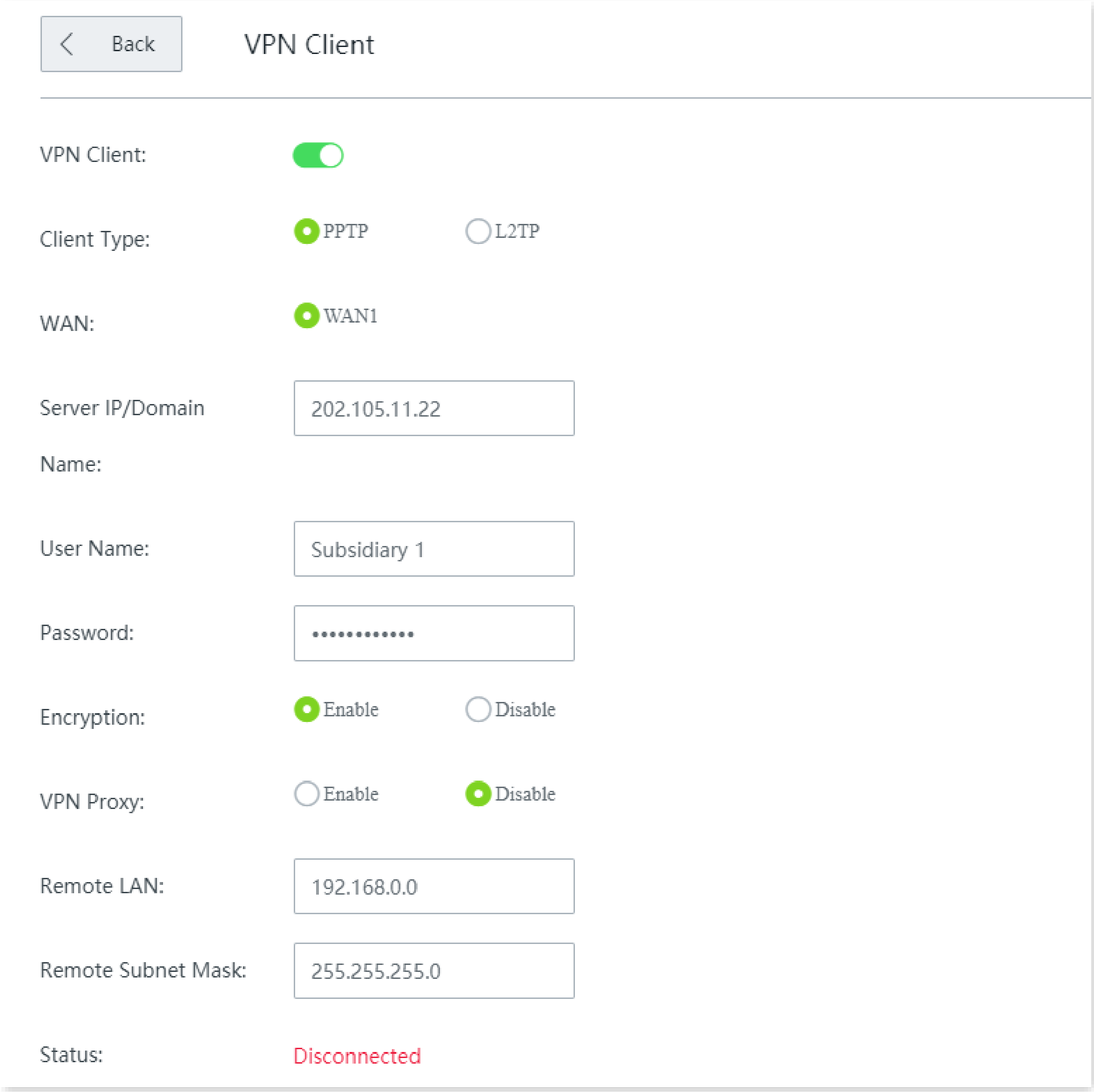
(4) Enter the **User Name** assigned by the VPN server, which is **Subsidiary 1** in this example.

(5) Enter the **Password**, which is **Subsidiary 1** in this example.

(6) Enable **Encryption**.

(7) Enter the **Remote LAN**, which is **192.168.0.0** in this example.

(8) Enter the **Remote Subnet Mask**, which is **255.255.255.0** in this example.



VPN Client: ON

Client Type: ● PPTP ○ L2TP

WAN: ● WAN1

Server IP/Domain Name: 202.105.11.22

User Name: Subsidiary 1

Password: ••••••••••••

Encryption: ● Enable ○ Disable

VPN Proxy: ○ Enable ● Disable

Remote LAN: 192.168.0.0

Remote Subnet Mask: 255.255.255.0

Status: Disconnected

----End

When the **Status** shows **Connected**, the VPN connection is successful. Staff of the headquarters and the subsidiary can securely access the LAN resources through the internet.

Verification

Assume that the subsidiary is about to access the FTP server of the headquarters. The headquarters project data is stored on an FTP server and the server information is as follows:

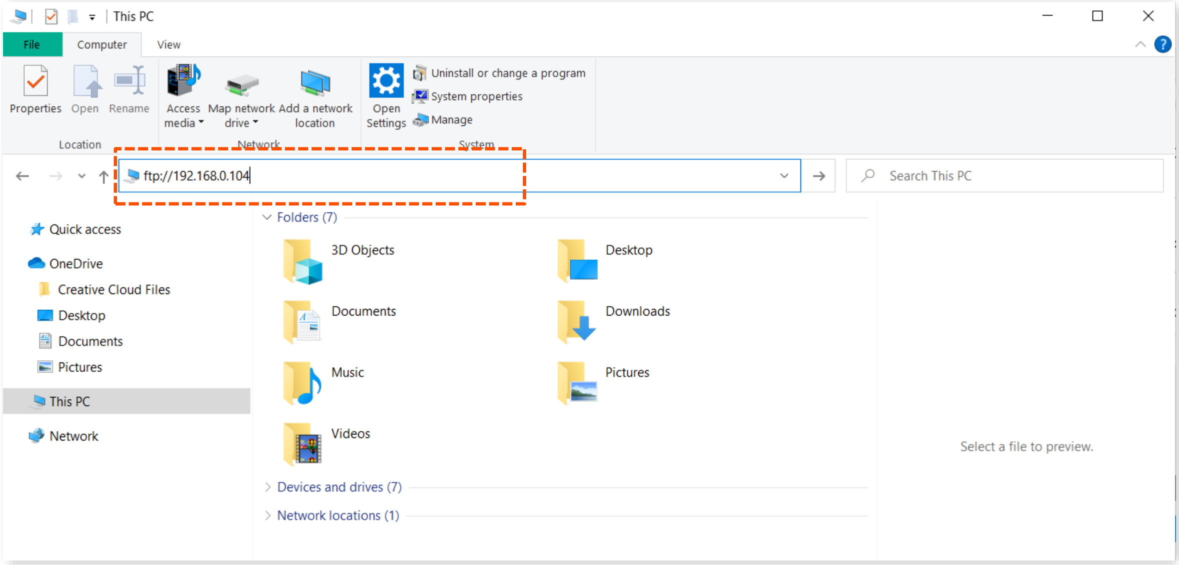
- FTP server IP address: 192.168.0.104
- Server port: 21
- Login username/password: Tom123/Tommy456

When subsidiary staff access the headquarters project materials, perform the following procedures:

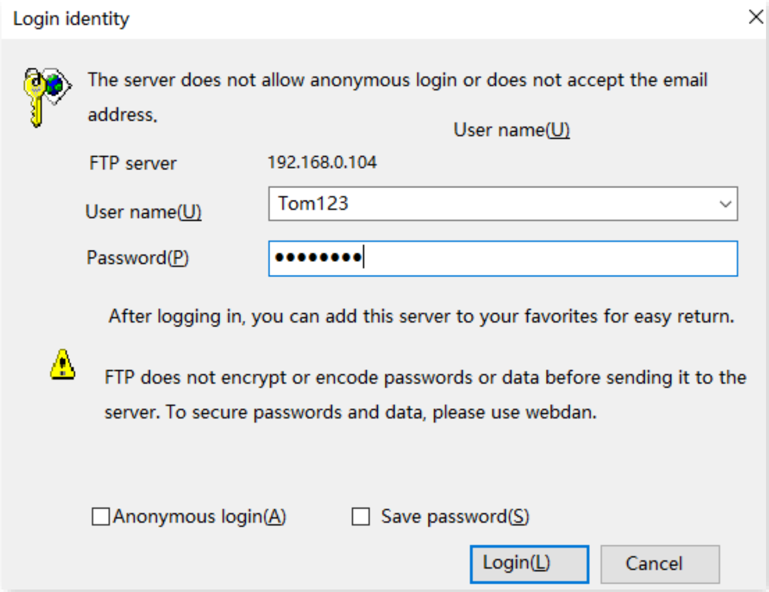
Step 1 Enter **ftp://server IP address** in a browser or **This PC**, which is **ftp://192.168.0.104** in this example.

TIP

If the LAN service port is not the default port number, the access format is **LAN service application layer protocol name://server IP address:LAN service port**.


ftp://192.168.0.104

Step 2 Enter the user name and password, which are **Tom123** and **Tommy 456** in this example, and click **Login**.


Login identity

The server does not allow anonymous login or does not accept the email address.

User name(U)

FTP server 192.168.0.104

User name(U) Tom123

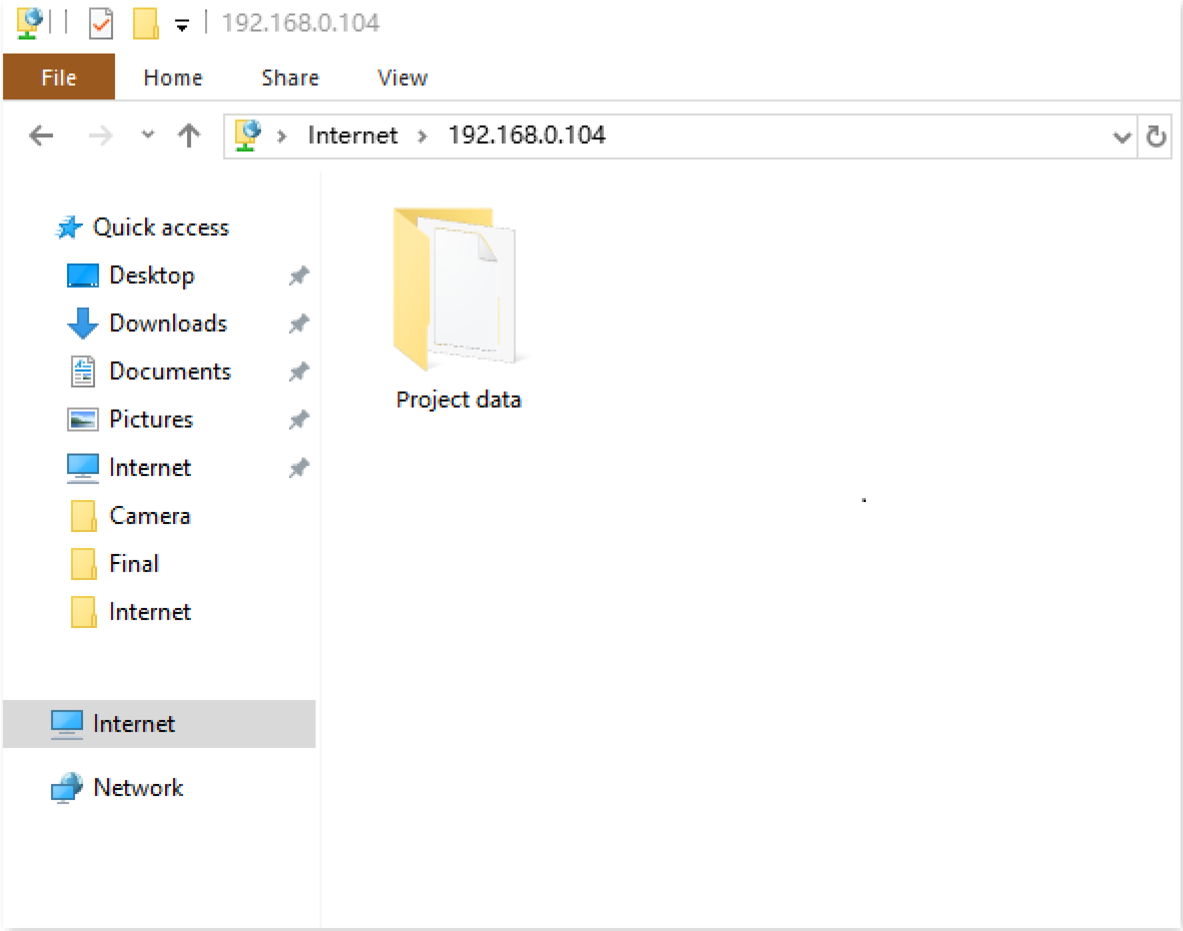
Password(P) ••••••••

After logging in, you can add this server to your favorites for easy return.

FTP does not encrypt or encode passwords or data before sending it to the server. To secure passwords and data, please use webdan.

□ Anonymous login(A) □ Save password(S)

The access is successful. See the following figure.



12.11.6 Example of configuring an IPSec VPN

Networking requirement

An enterprise and its subsidiary both use routers to set up a network and the routers have been connected to the internet.

The enterprise has the following requirement:

Subsidiary staff can access the LAN resources through the internet, such as documents, OA, ERP system, CRM system, project management system and other resources.

Solution

Set up an IPSec tunnel on the two routers for the remote users to securely access the LAN through the internet.

Assume that router 1 is deployed in the headquarters and its basic information is as follows:

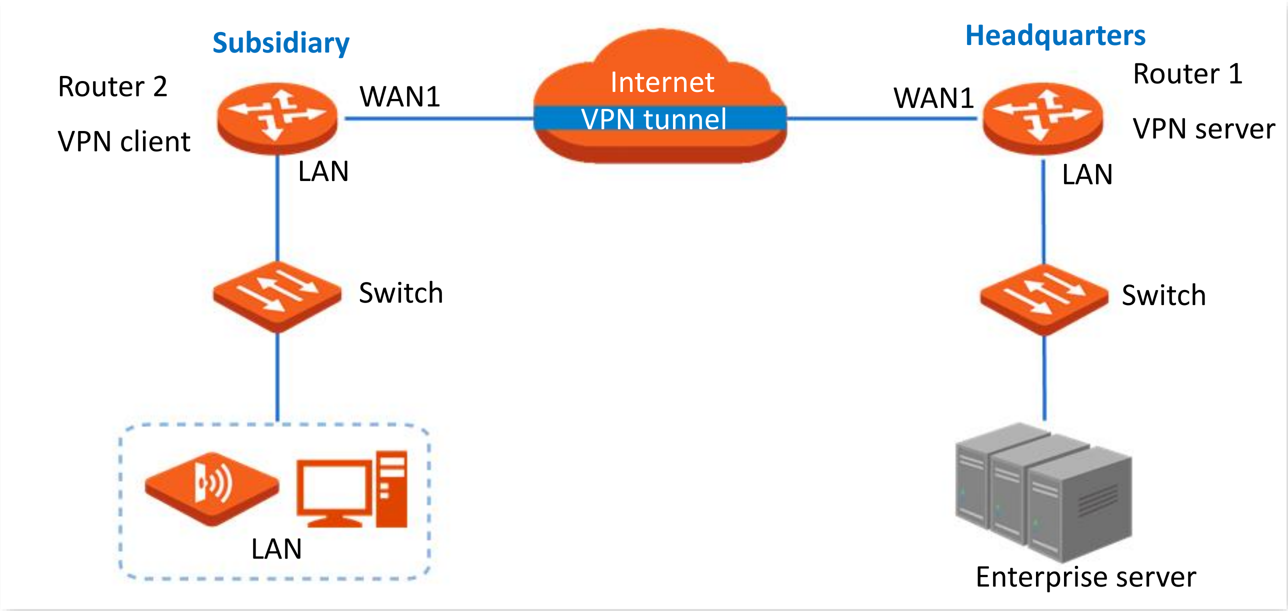
- Port used to establish an IPSec tunnel: WAN1
- WAN1 IP address: 202.105.11.22
- IP address of the LAN: 192.168.0.0/24

Assume that router 2 is deployed in the subsidiary and its basic information is as follows:

- Port used to establish an IPSec tunnel: WAN1
- WAN IP address: 202.105.88.77
- IP address of the LAN: 192.168.1.0/24

Assume that the basic information of the IPSec connection between the two routers is:

- Encapsulation mode: Tunnel
- Key negotiation mode: Auto negotiation
- Pre-shared key: td159357



Configuration procedure

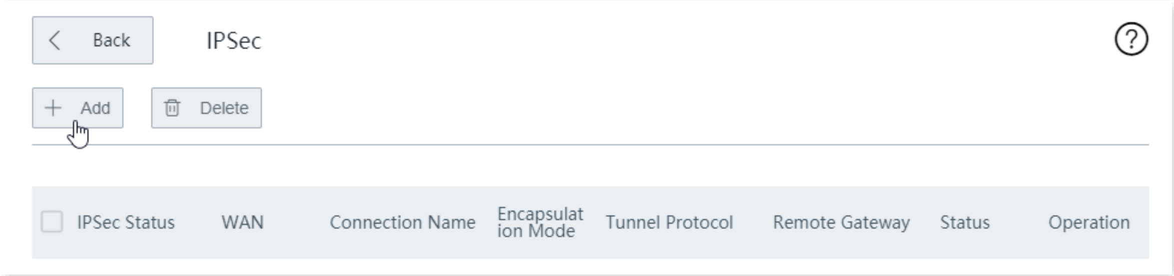
Configure router 1 > Configure router 2

TIP

During the configuration, if you want to configure the advanced settings of IPSec connection, make sure the parameters of the two routers are the same.

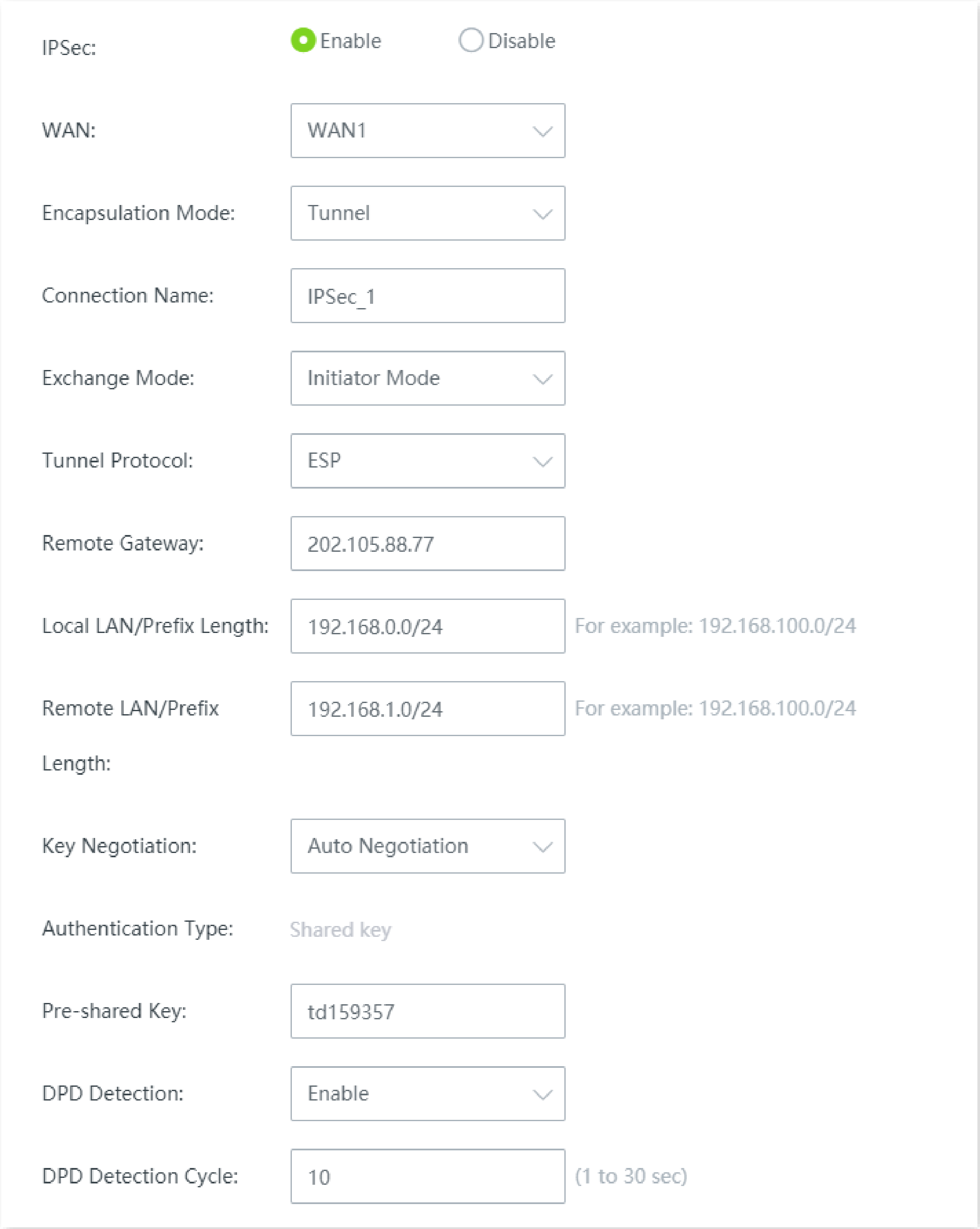
Step 1 Configure router 1.

1. Log in to the web UI of the router 1, and navigate to **More** > **IPSec**.
2. Click **+Add**.



□	IPSec Status	WAN	Connection Name	Encapsulation Mode	Tunnel Protocol	Remote Gateway	Status	Operation

3. Configure the parameters in the **Add** window, and click **Save** at the bottom of the page.
   (1) Select the WAN port to establish an IPSec tunnel, which is **WAN1** this example.
   (2) Set **Encapsulation Mode** to **Tunnel**.
   (3) Set the **Connection Name**, which is **IPSec_1** in this example.
   (4) Enter the **Remote Gateway**, which is **202.105.88.77** in this example.
   (5) Enter the **Local LAN/Prefix Length**, which is **192.168.0.0/24** in this example.
   (6) Enter the **Remote LAN/Prefix Length**, which is **192.168.1.0/24** in this example.
   (7) Set the **Pre-shared Key**, which is **td159357** in this example.



IPSec: ● Enable ○ Disable

WAN: WAN1

Encapsulation Mode: Tunnel

Connection Name: IPSec_1

Exchange Mode: Initiator Mode

Tunnel Protocol: ESP

Remote Gateway: 202.105.88.77

Local LAN/Prefix Length: 192.168.0.0/24 For example: 192.168.100.0/24

Remote LAN/Prefix Length: 192.168.1.0/24 For example: 192.168.100.0/24

Key Negotiation: Auto Negotiation

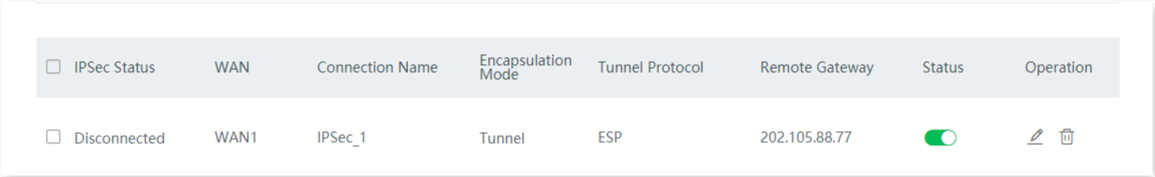
Authentication Type: Shared key

Pre-shared Key: td159357

DPD Detection: Enable

DPD Detection Cycle: 10 (1 to 30 sec)

The IPSec is added successfully. See the following figure.

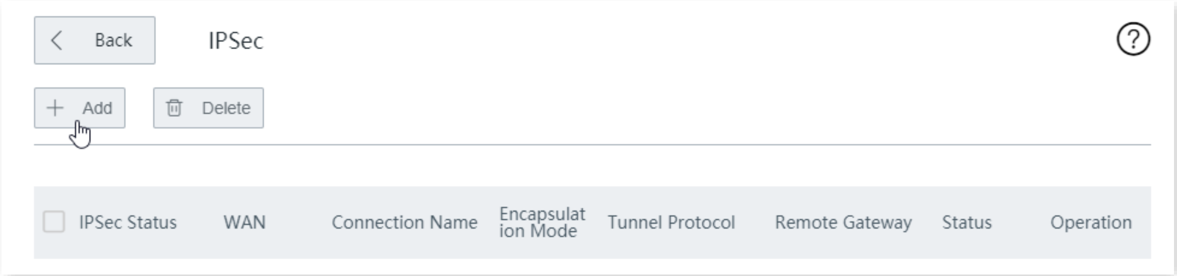


□ IPSec Status	WAN	Connection Name	Encapsulation Mode	Tunnel Protocol	Remote Gateway	Status	Operation
□ Disconnected	WAN1	IPSec_1	Tunnel	ESP	202.105.88.77	●	✎ 🗑

Step 2 Configure router 2.

1. Log in to the web UI of the router 2 and navigate to **More** > **IPSec**.

2. Click **+Add**.



3. Configure the parameters in the **Add** window, and click **Save** at the bottom of the page.

   (1) Select the WAN port to establish an IPSec tunnel, which is **WAN1** this example.

   (2) Set **Encapsulation Mode** to **Tunnel**.

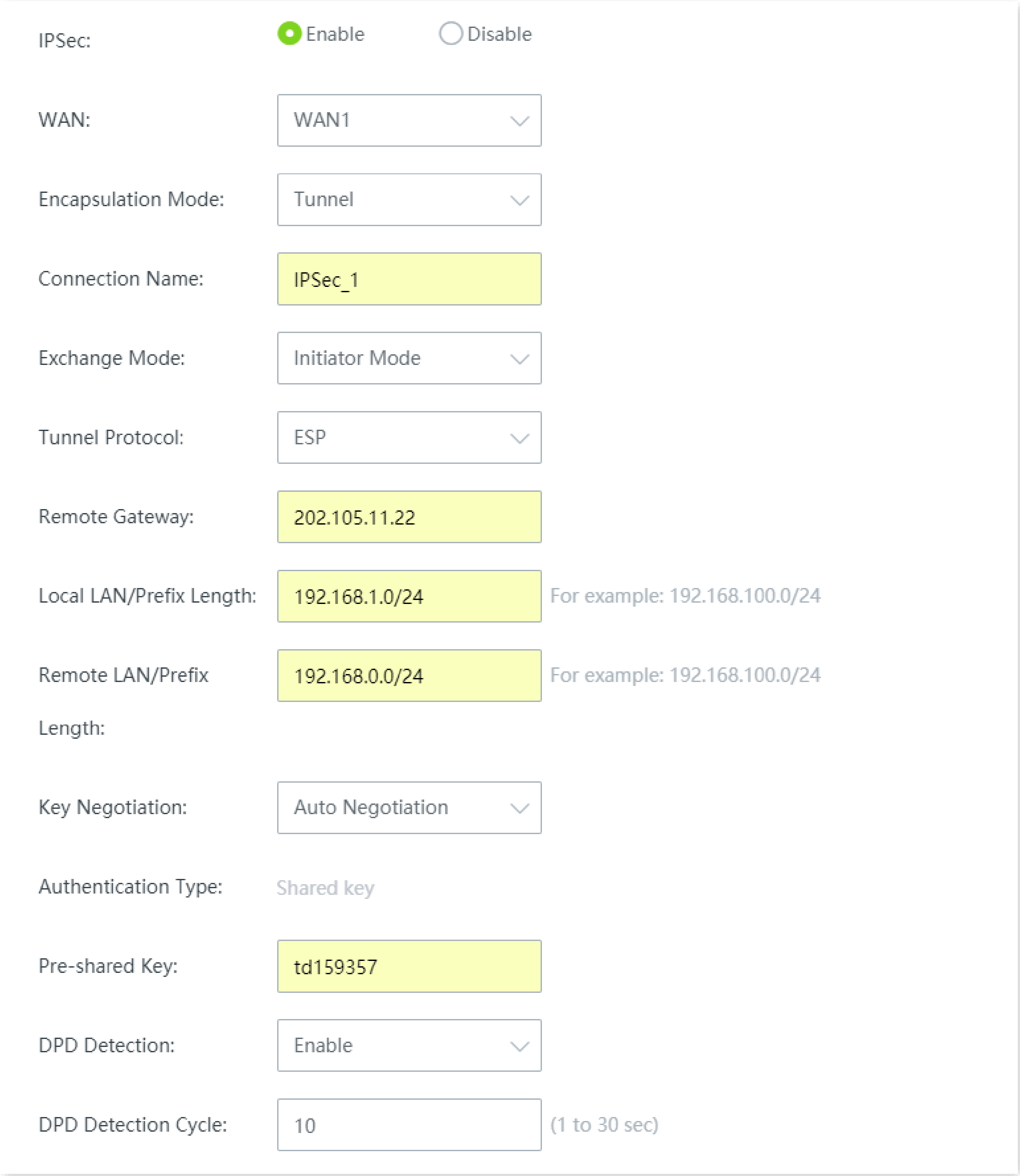
   (3) Set the **Connection Name**, which is **IPSec_1** in this example.

   (4) Enter the **Remote Gateway**, which is **202.105.11.22** in this example.

   (5) Enter the **Local LAN/Prefix Length**, which is **192.168.1.0/24** in this example.

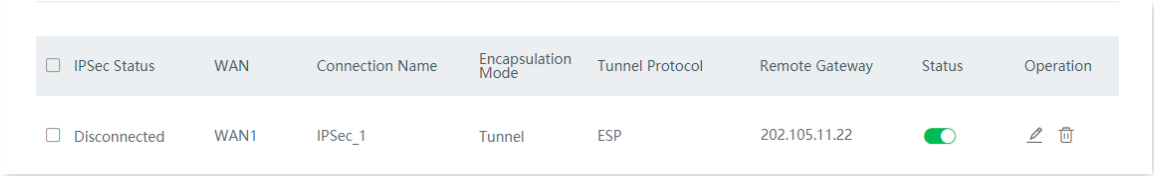
   (6) Enter the **Remote LAN/Prefix Length**, which is **192.168.0.0/24** in this example.

   (7) Set the **Pre-shared Key**, which is **td159357** in this example.



IPSec:	● Enable ○ Disable
WAN:	WAN1
Encapsulation Mode:	Tunnel
Connection Name:	IPSec_1
Exchange Mode:	Initiator Mode
Tunnel Protocol:	ESP
Remote Gateway:	202.105.11.22
Local LAN/Prefix Length:	192.168.1.0/24 For example: 192.168.100.0/24
Remote LAN/Prefix Length:	192.168.0.0/24 For example: 192.168.100.0/24
Key Negotiation:	Auto Negotiation
Authentication Type:	Shared key
Pre-shared Key:	td159357
DPD Detection:	Enable
DPD Detection Cycle:	10 (1 to 30 sec)

The IPSec is added successfully. See the following figure.



□ IPSec Status	WAN	Connection Name	Encapsulation Mode	Tunnel Protocol	Remote Gateway	Status	Operation
□ Disconnected	WAN1	IPSec_1	Tunnel	ESP	202.105.11.22	●	✎ 🗑

----End

Verification

When **IPSec Status** shows **Connected**, the IPSec tunnel is set up successfully and headquarters and subsidiary staff can securely access the LAN resources of each other through internet.

12.11.7 Example of configuring a L2TP over IPSec VPN

Networking requirement

An enterprise and its branch have used the wireless routers to set up LANs and access the internet. Branch employees need to access the headquarters' internal resources through the internet, such as internal data, OA, ERP, CRM, and project management systems.

Solution

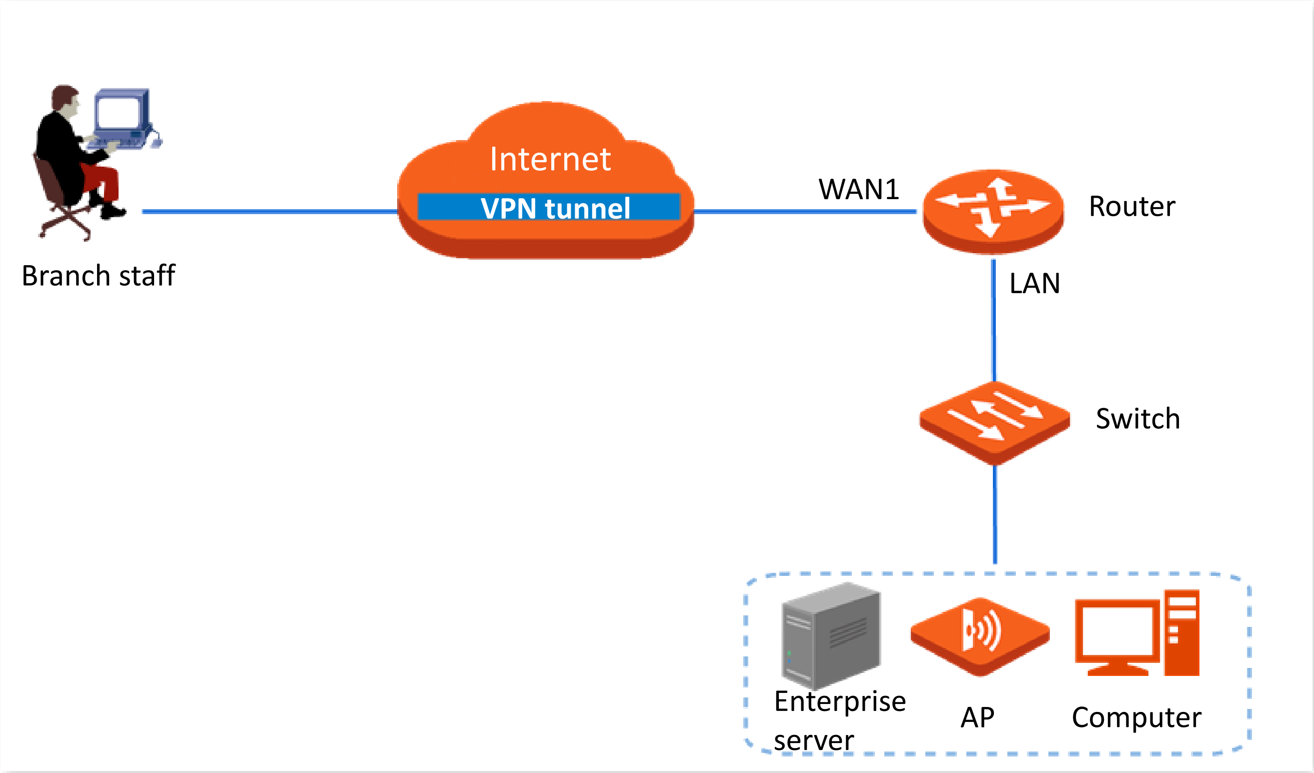
IPSec and L2TP server function of the router can meet this requirement.

Assume that the related information is shown as below:

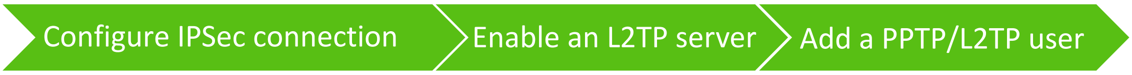
- Port used to establish an IPSec tunnel: WAN1
- Port used to establish an L2TP VPN tunnel: WAN1
- IP address of WAN1: 202.105.11.22
- LAN: 192.168.0.0/24

Assume that the related information of IPSec connection of the router is shown as below:

- Encapsulation Mode: Tunnel mode
- Key Negotiation: Auto negotiation
- Pre-shared Key: ip159357

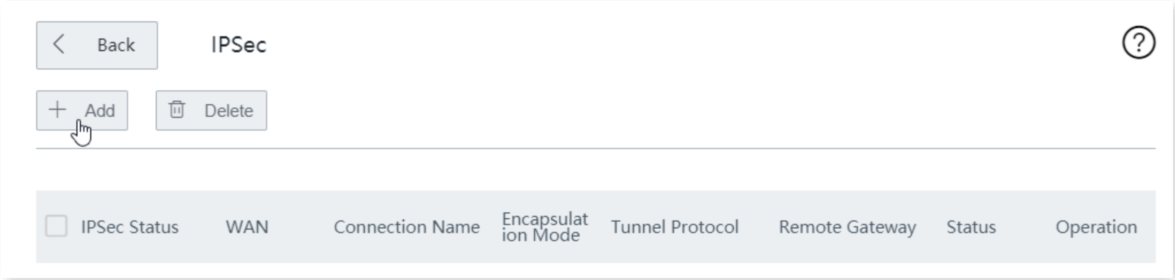


Configuration Procedure



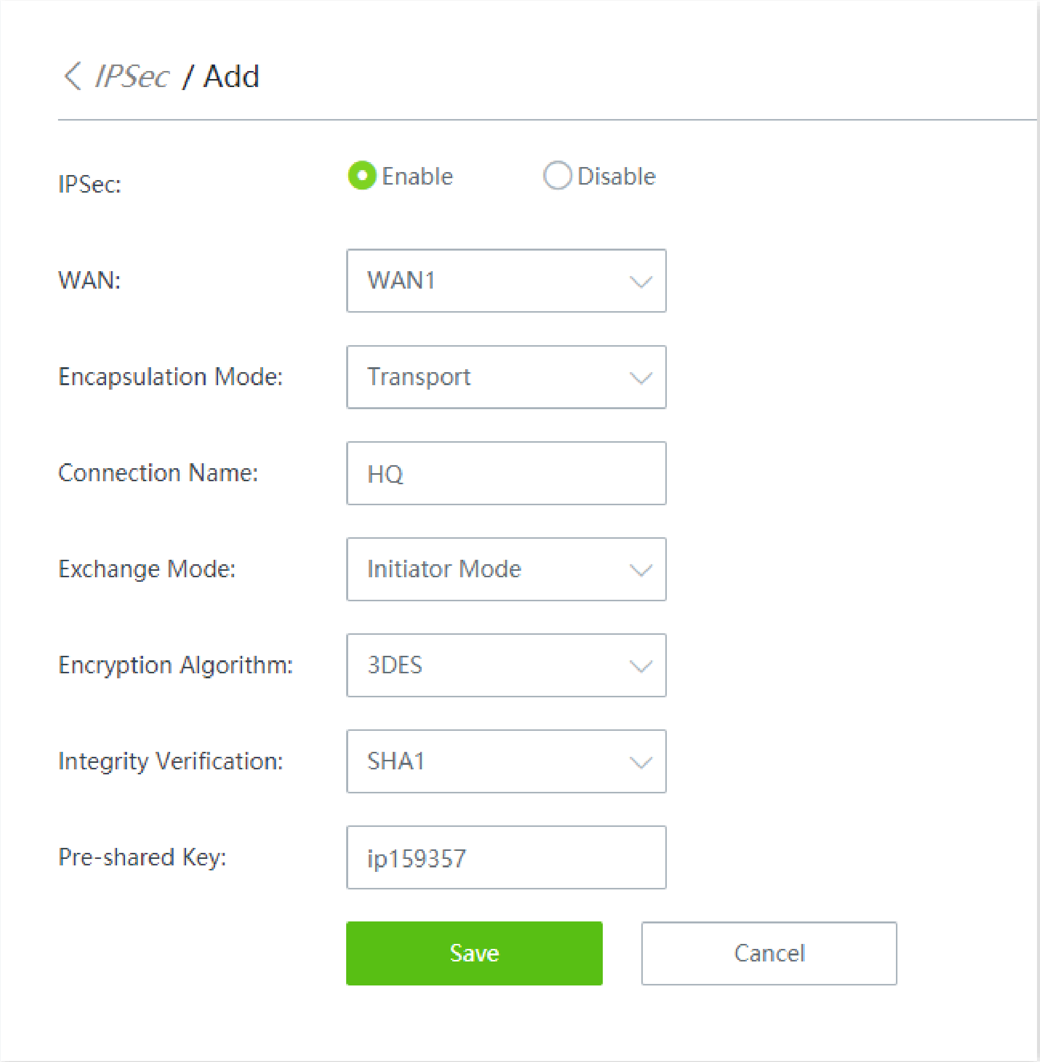
Step 1 Configure the IPSec connection.

1. Navigate to **More** > **IPSec**.
2. Click **+Add.**



□ IPSec Status	WAN	Connection Name	Encapsulation Mode	Tunnel Protocol	Remote Gateway	Status	Operation

3. Configure the following parameters in the **Add** window, and click **Save**.
   (1) Select a **WAN** port for the IPSec VPN connection, which is **WAN1** in this example.
   (2) Select **Encapsulation Mode**, which is **Transport** in this example.
   (3) Set **Connection Name** to the name of the IPSec tunnel, which is **HQ** in this example.
   (4) Specify **Pre-shared Key**, which is **ip159357** in this example.


IPSec / Add

IPSec: ● Enable ○ Disable

WAN: WAN1

Encapsulation Mode: Transport

Connection Name: HQ

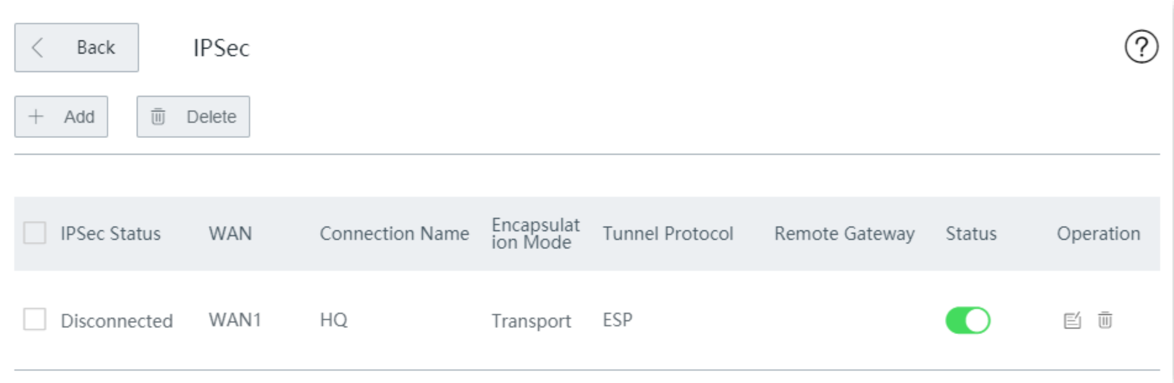
Exchange Mode: Initiator Mode

Encryption Algorithm: 3DES

Integrity Verification: SHA1

Pre-shared Key: ip159357

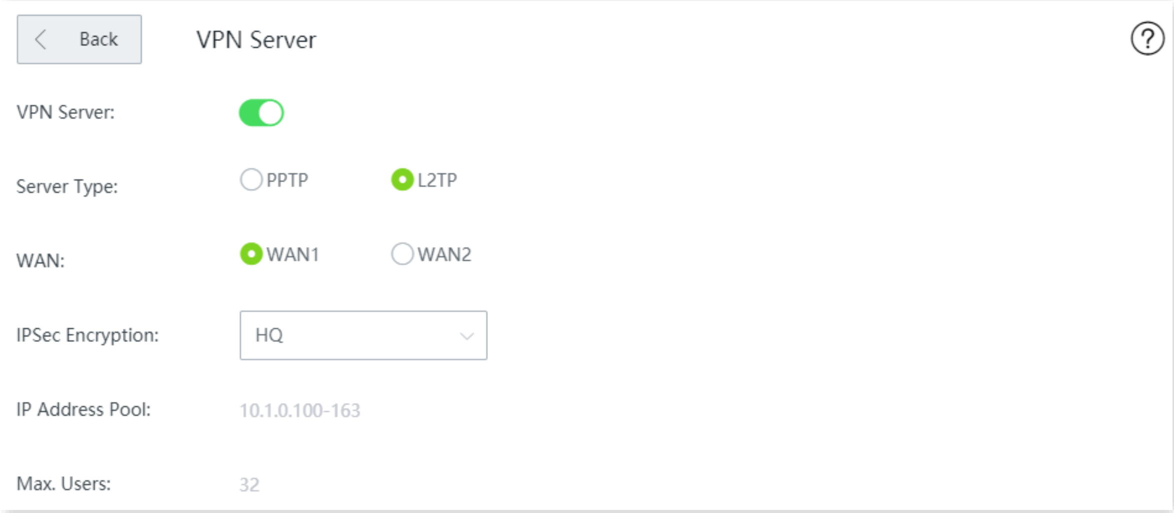
The IPSec connection is configured successfully. See the following figure.



□ IPSec Status	WAN	Connection Name	Encapsulation Mode	Tunnel Protocol	Remote Gateway	Status	Operation
□ Disconnected	WAN1	HQ	Transport	ESP		●	

Step 2 Enable the L2TP server.

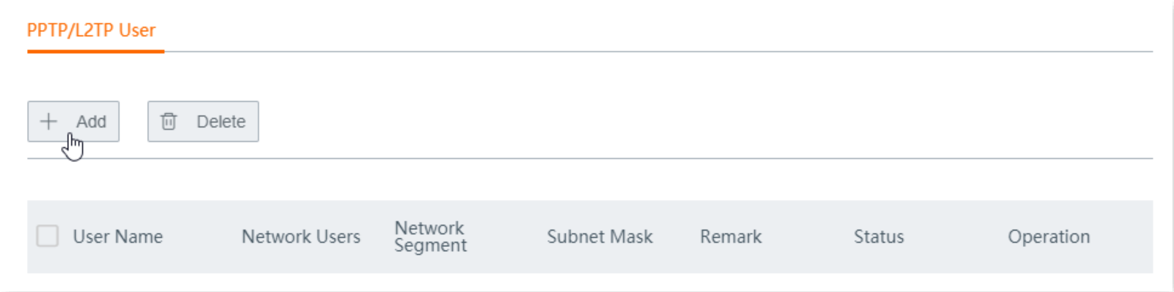
1. Navigate to **More** > **VPN Server**.
2. Enable **VPN Server**.
3. Set **Server Type** to **L2TP**.
4. Select a **WAN** port for the IPSec VPN connection, which is **WAN1** in this example.
5. Set **IPSec Encryption** of the IPSec tunnel, which is **HQ** in this example.
6. Click **Save**.



VPN Server:	●	
Server Type:	○ PPTP	● L2TP
WAN:	● WAN1	○ WAN2
IPSec Encryption:	HQ	
IP Address Pool:	10.1.0.100-163	
Max. Users:	32	

Step 3 Add a PPTP/L2TP User.

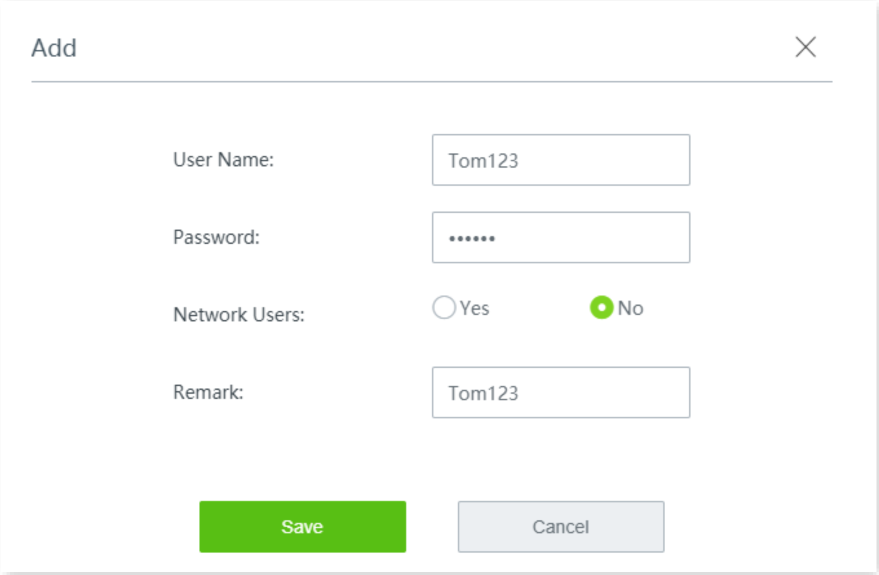
1. Navigate to **More** > **VPN Server** > **PPTP/L2TP User**.
2. Click **+Add**.



□ User Name	Network Users	Network Segment	Subnet Mask	Remark	Status	Operation

Step 4 Configure the following parameters in the **Add** window, and click **Save**.

1. Enter the **User Name** and **Password** assigned by the VPN client, which are both **Tom123** in this example.
2. Set **Network User** to **No**.
3. Enter a **Remark** to your account, which is **Tom123** in this example.



Add

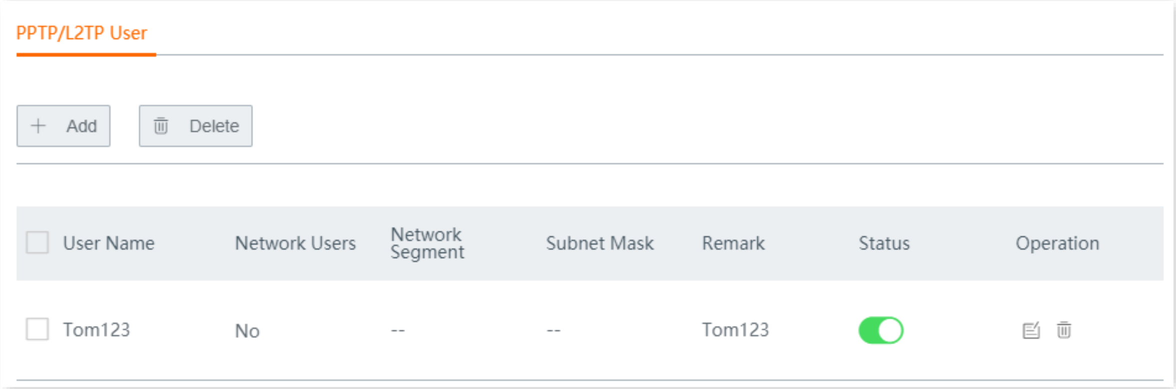
User Name: Tom123

Password: ••••••

Network Users: ○ Yes ● No

Remark: Tom123

The L2TP over IPSec VPN is added successfully. See the following figure.



PPTP/L2TP User

□ User Name	Network Users	Network Segment	Subnet Mask	Remark	Status	Operation
□ Tom123	No	--	--	Tom123	●	

----End

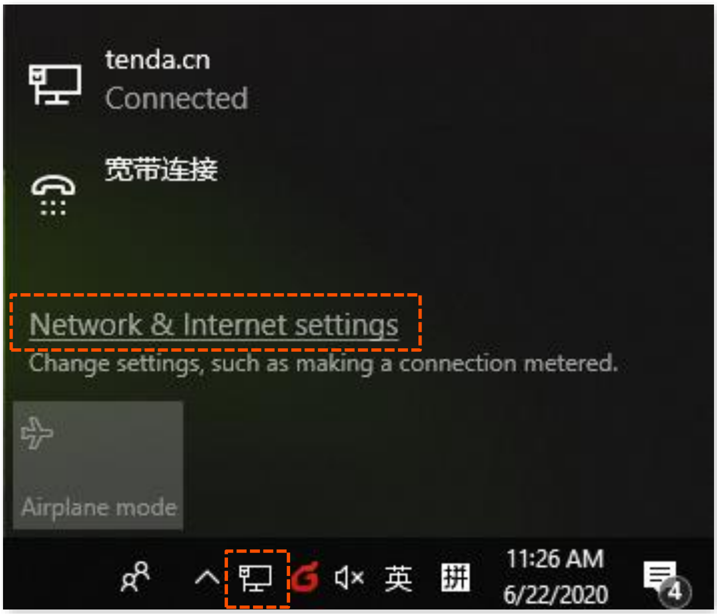
Verification

To access the headquarters LAN resources, you have to configure your client. The document introduces how to create VPN dialing on Windows 10 and iOS. Choose the scenario according to your actual situations.

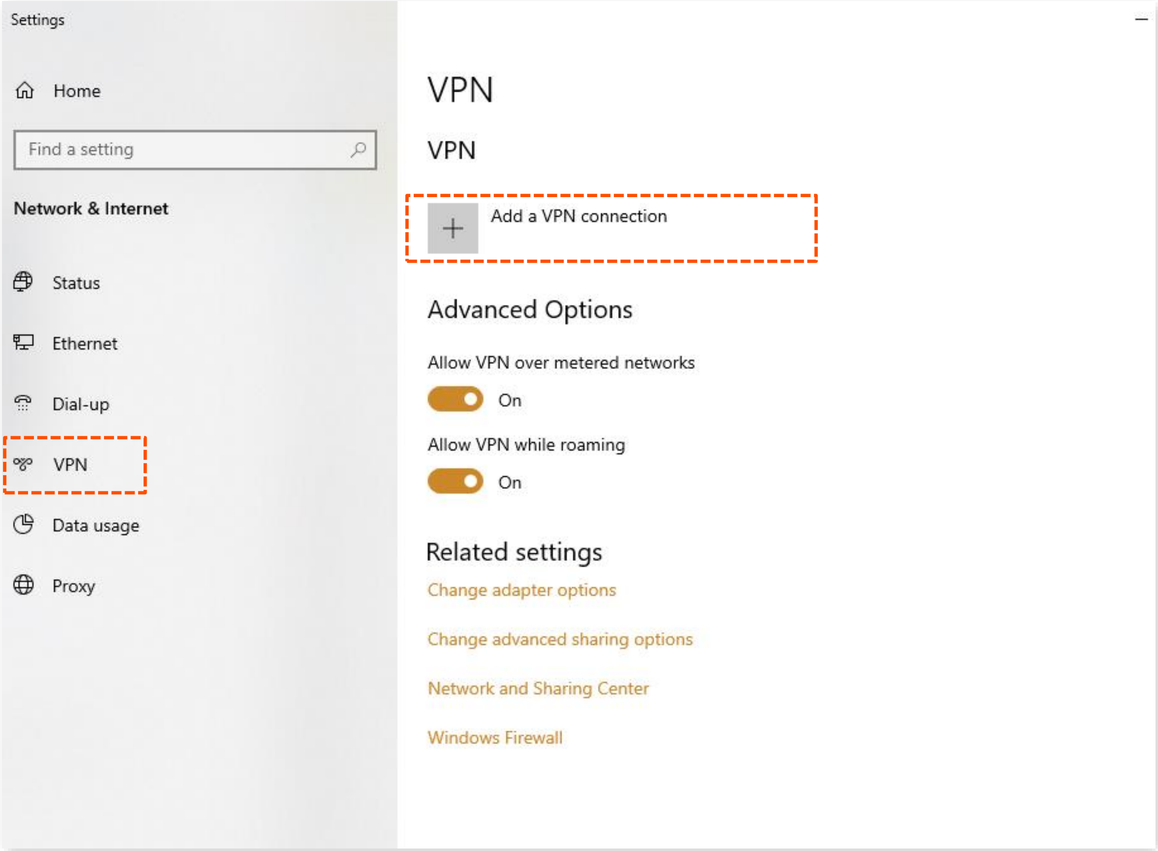
Create VPN connection on Windows 10

Step 1 Create VPN connections.

1. Click 🖳 in the lower right corner of the desktop, click **Network & Internet settings**.


tenda.cn
Connected
宽带连接
Network & Internet settings
Change settings, such as making a connection metered.
Airplane mode
英
拼
11:26 AM
6/22/2020
4

2. Click **VPN**, click **Add a VPN connection**.



3. Set VPN connection parameters, and then click **Save**.

   (1) Select **VPN provider**, which is **Windows (built-in)** in this example.

   (2) Set the **Connection name** of VPN, which is **VPN Access** in this example.

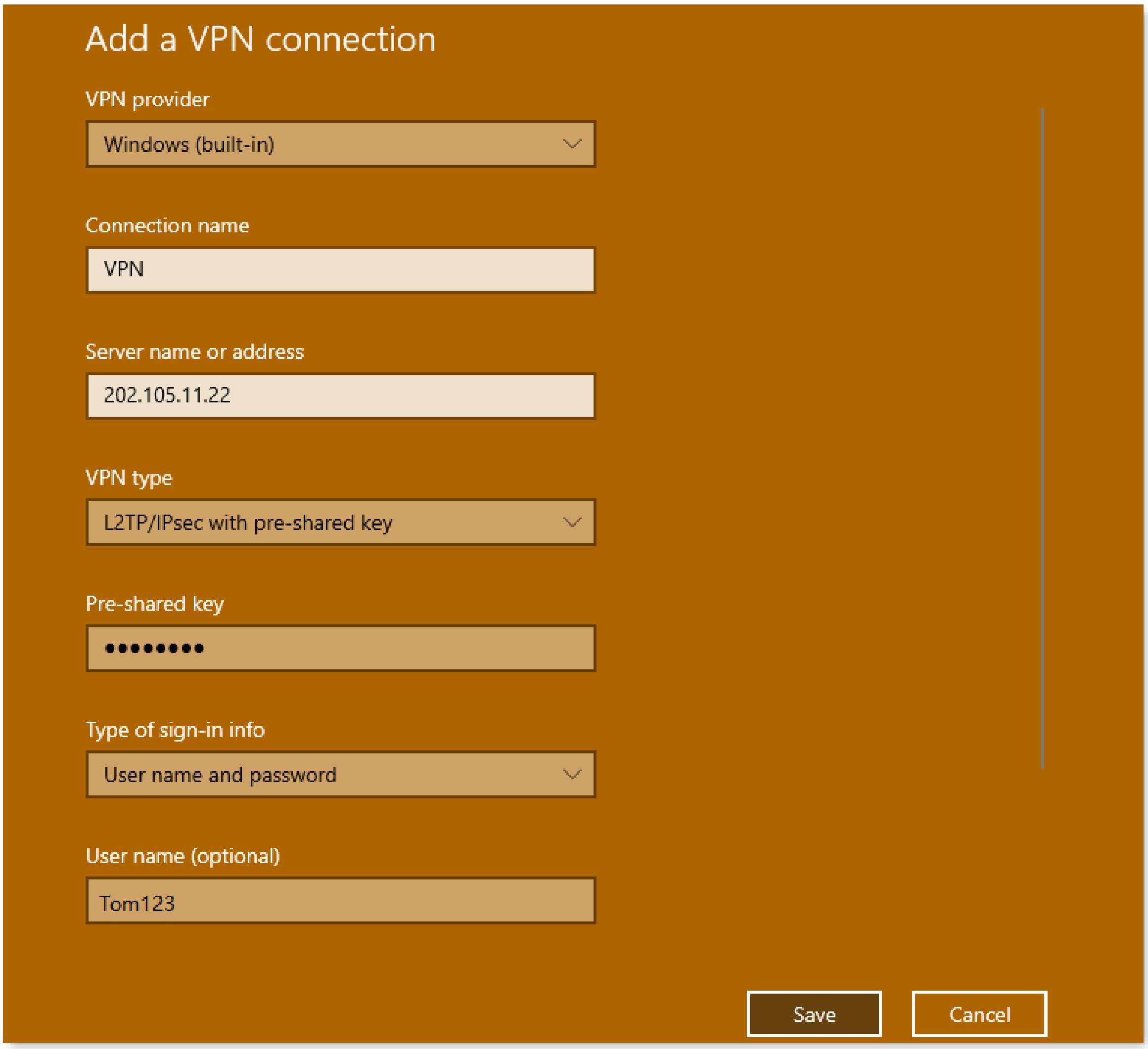
   (3) Enter **Server name or address**, which is **202.105.11.22** in this example.

   (4) Select **VPN type**, which is **L2TP/IPsec with pre-shared key**.

   (5) Enter **Pre-shared key** of the IPSec tunnel, which is **ip159357** in this example.

   (6) Pull down the scroll bar, select **Type of sign-in info**, which is **User name and password** in this example.

   (7) Enter **User name and Password**, which are both **Tom123** in this example.



Add a VPN connection

VPN provider: Windows (built-in)

Connection name: VPN

Server name or address: 202.105.11.22

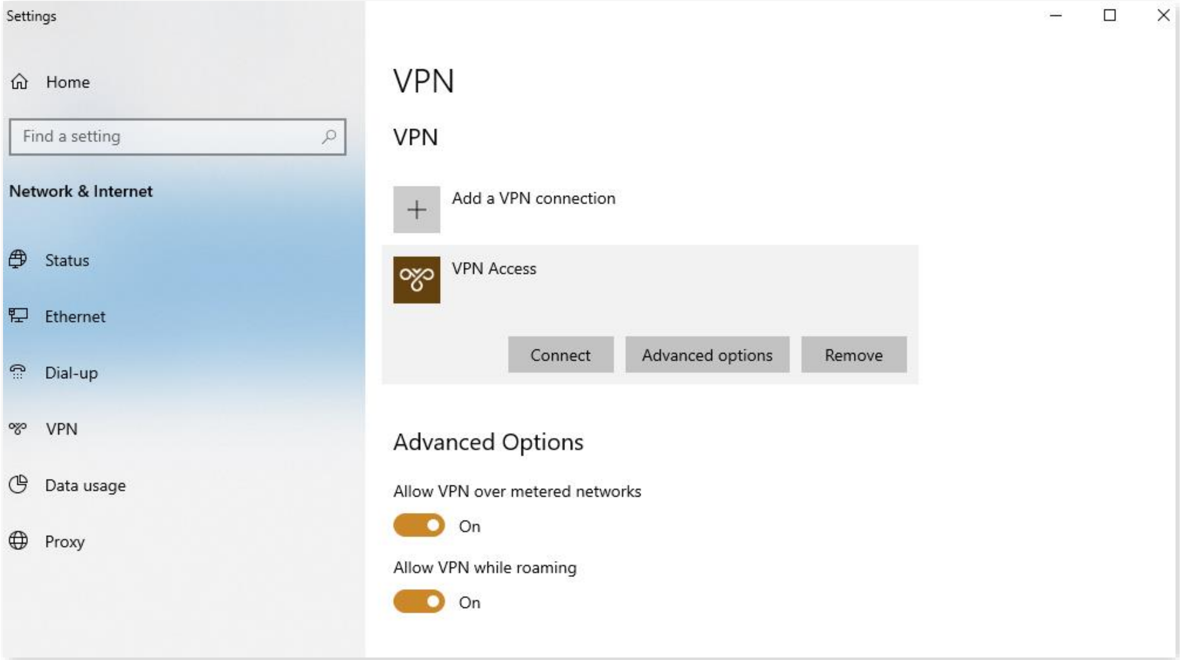
VPN type: L2TP/IPsec with pre-shared key

Pre-shared key: ●●●●●●●●●

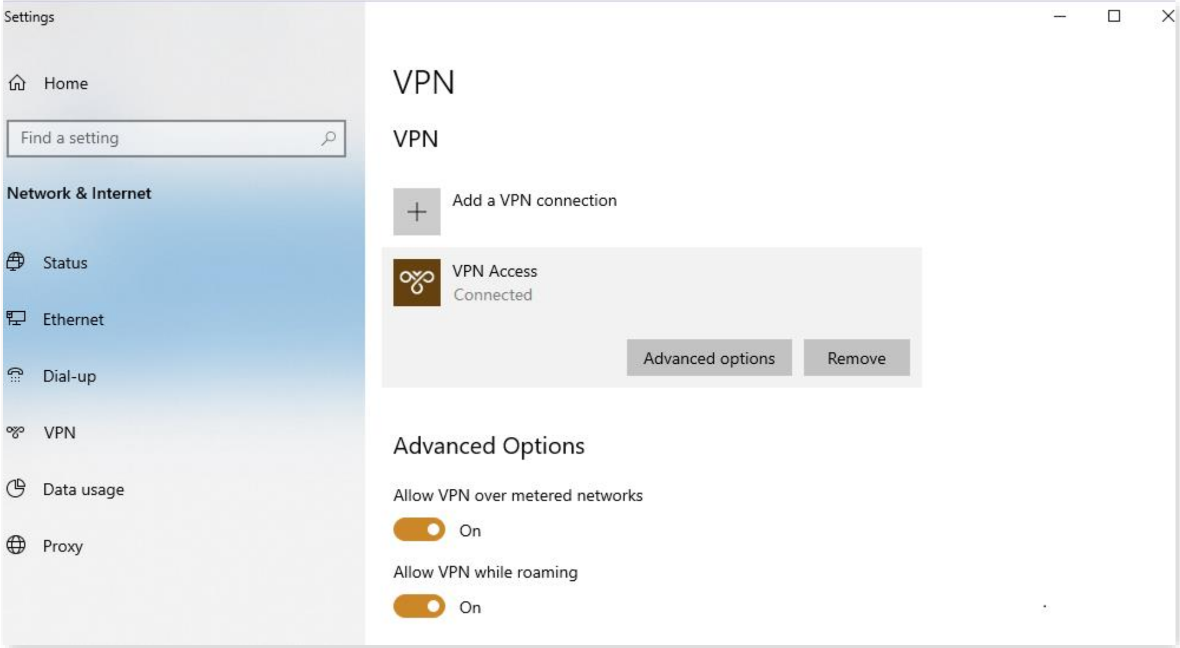
Type of sign-in info: User name and password

User name (optional): Tom123

4. Click **VPN Access,** then click **Connect**.



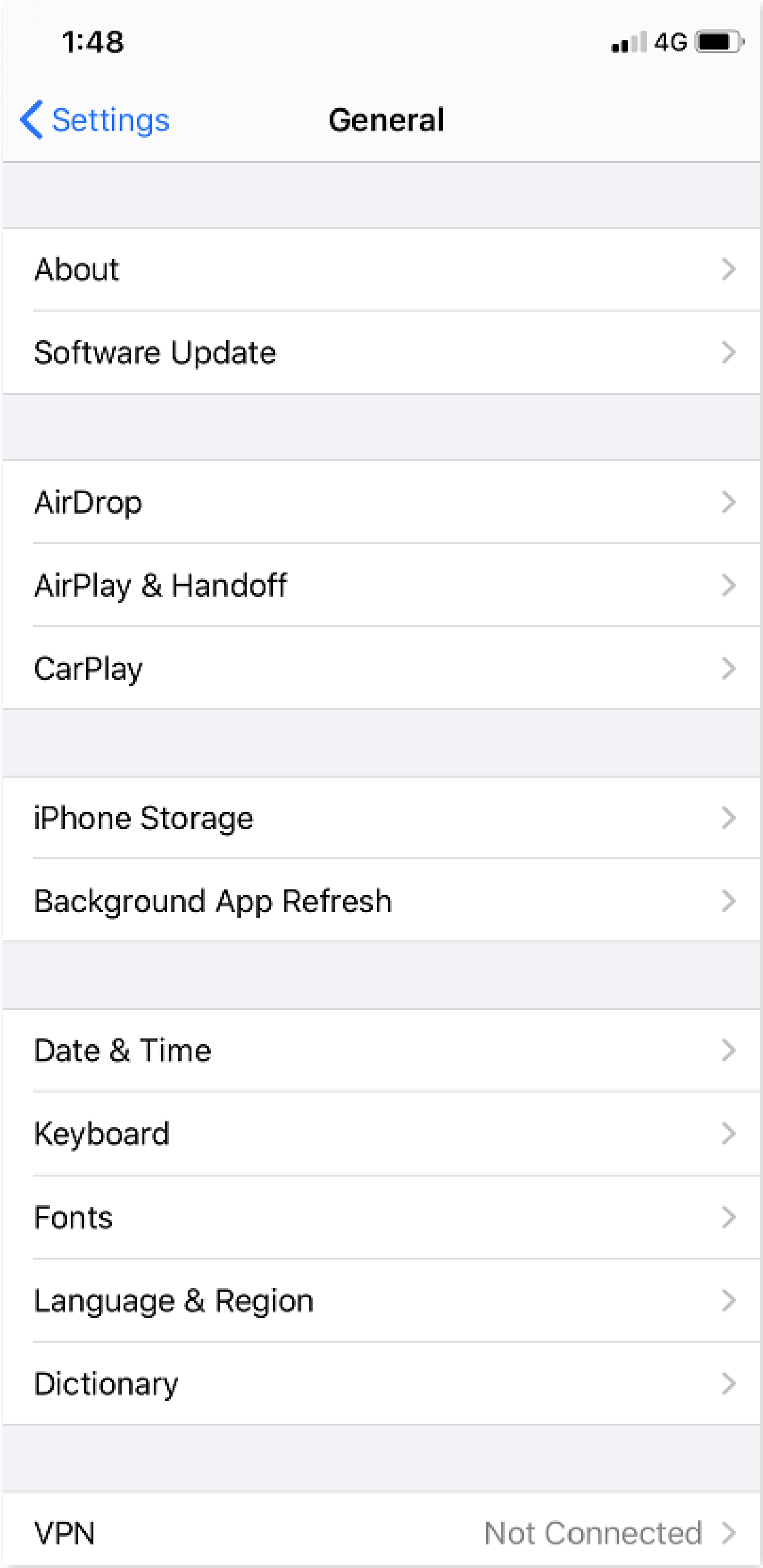
Wait until a connection is established.



Create VPN connection on a mobile device (Example: iOS).

Step 1 Click **Settings** ⚙ on your smartphone.

Step 2 Tap **VPN.**



1:48 4G

< Settings General

About

Software Update

AirDrop

AirPlay & Handoff

CarPlay

iPhone Storage

Background App Refresh

Date & Time

Keyboard

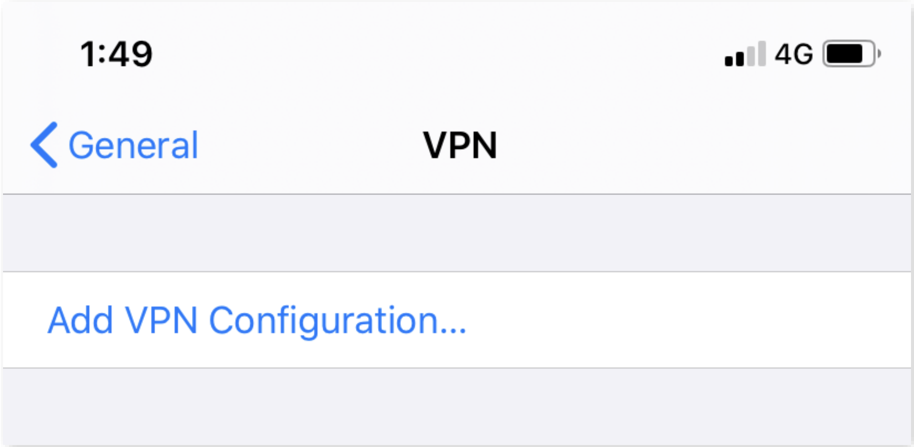
Fonts

Language & Region

Dictionary

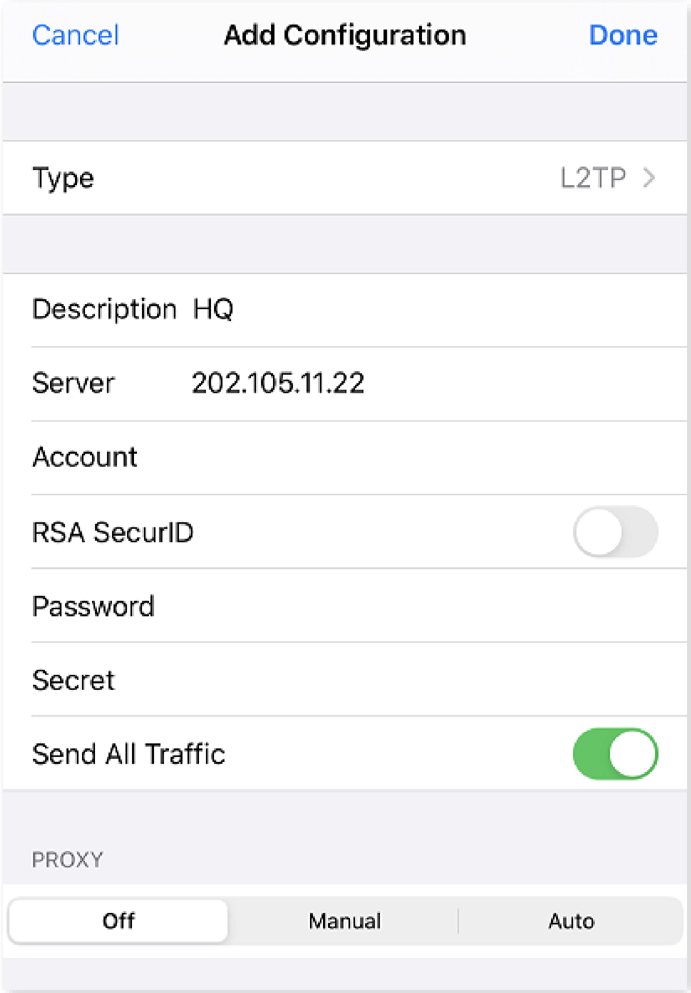
VPN Not Connected

Step 3 Tap **Add VPN Configuration....**



Step 4 Set the VPN connection parameters.

1. Select the **Type**, which is **L2TP** in this example.
2. Set the name of VPN connection in **Description**, which is **HQ** in this example.
3. Enter the IP address of L2TP Server, which is **202.105.11.22** in this example.
4. Enter the **Account** and **Password** of L2TP VPN, which are both **Tom123** in this example.
5. Enter the **Secret** of IPSec tunnel, which is **ip159357** in this example.
6. Tap **Done**.



Type L2TP

Description HQ

Server 202.105.11.22

Account

RSA SecurID

Password

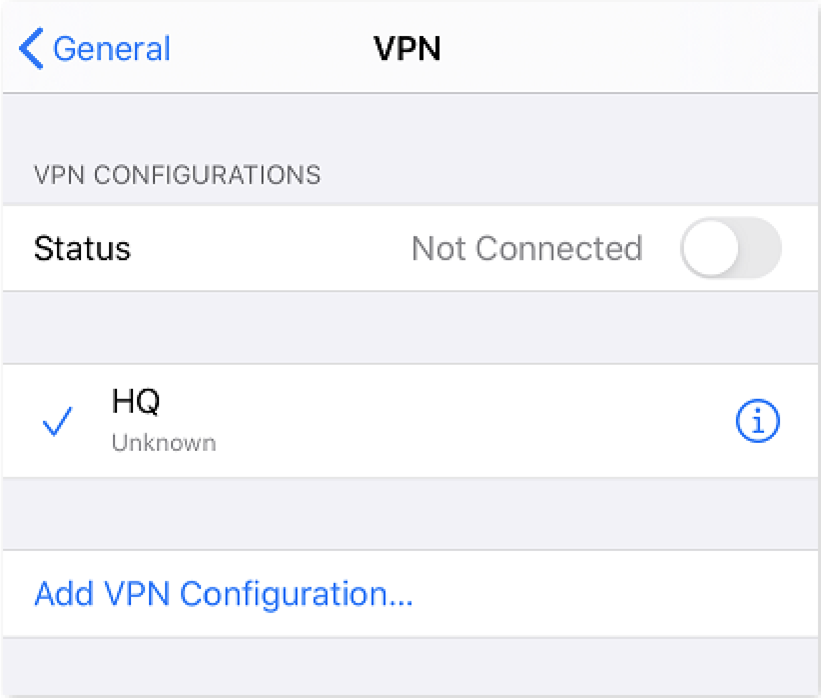
Secret

Send All Traffic

PROXY

Off Manual Auto

Step 5 Tap ○.



< General VPN

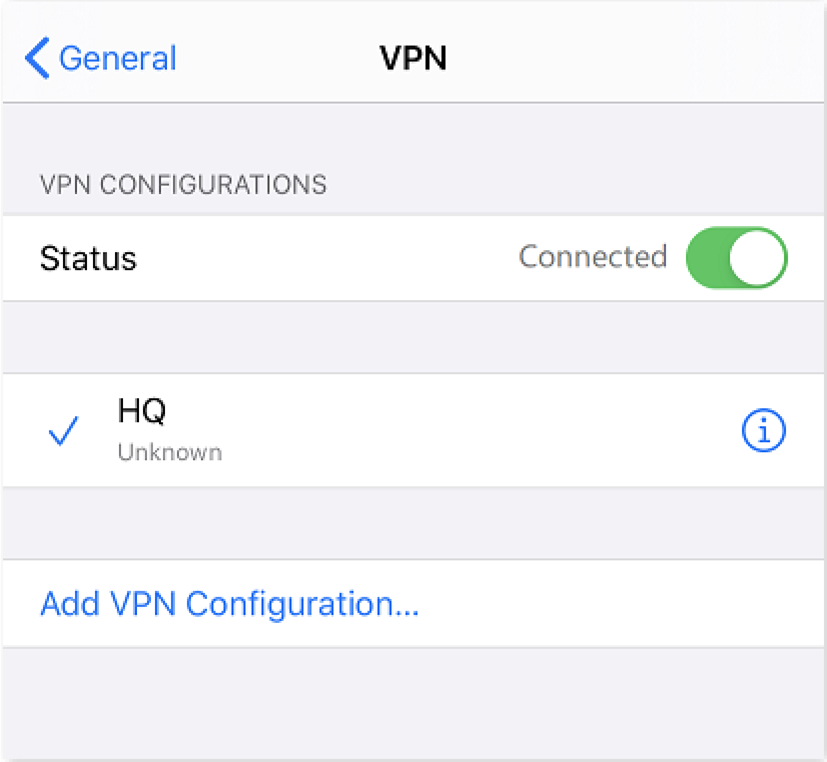
VPN CONFIGURATIONS

Status Not Connected ○

✓ HQ
Unknown ⓘ

----End

Wait until the **Status** turns to **Connected** ●, the IPSec connection is created successfully.



< General VPN

VPN CONFIGURATIONS

Status Connected ●

✓ HQ
Unknown ⓘ

Employees accessing headquarters resources on business trip

Assume that a branch needs to access the FTP server of headquarters. The project data of the headquarters is stored on the FTP server. Assume that the server information is as follows:

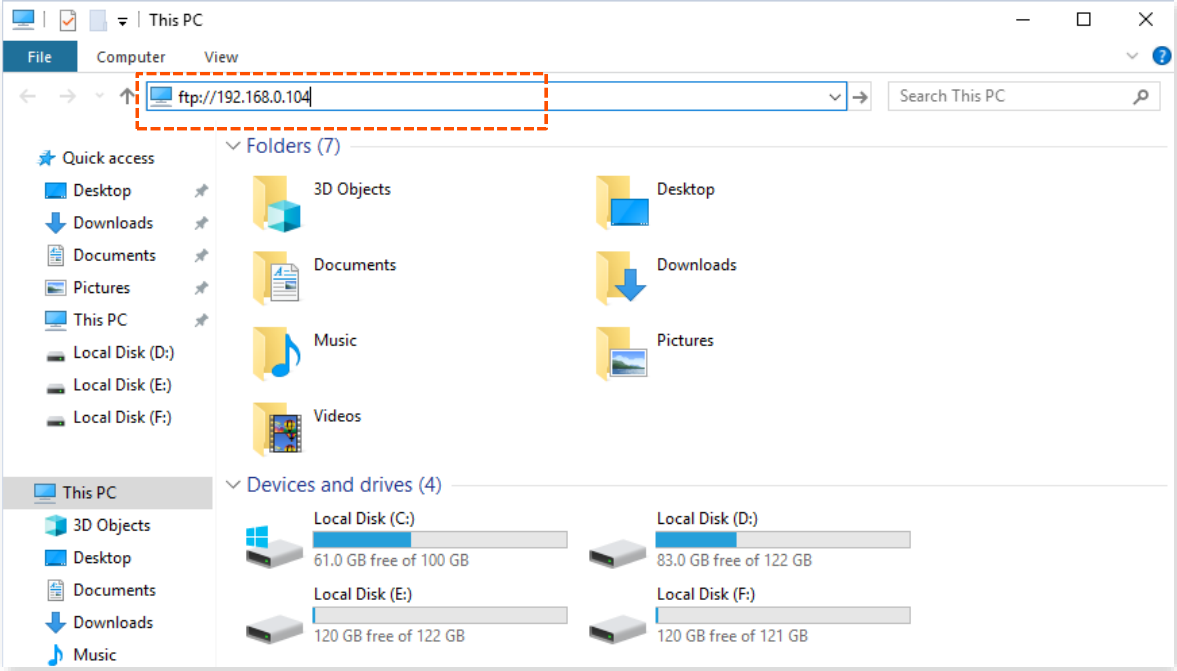
- FTP server IP address: **192.168.0.104**
- Server port: **21**
- FTP server login user name and password: **Tom123**

When branch staff access the project data of the headquarters, they perform the following steps:

Step 1 Access the link **ftp://server IP address: server port** on a computer, which is **ftp://192.168.0.104** in this example.

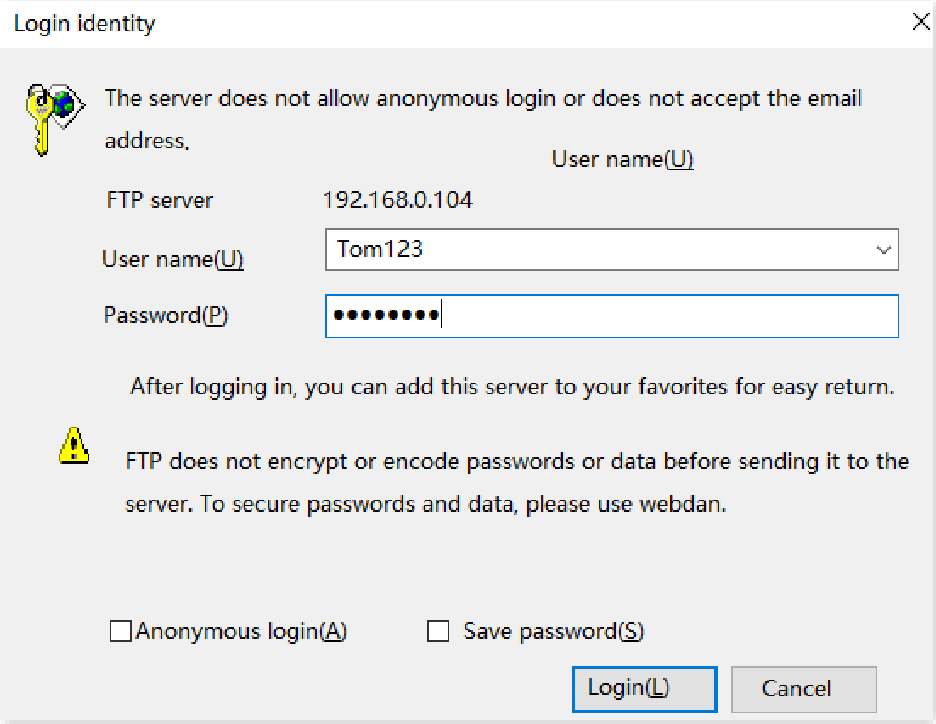
TIP

If the server port of the LAN is not port number by default, the access format is **LAN service application layer protocol name://server IP address: Server port of the LAN**.



ftp://192.168.0.104

Step 2 Enter the **User name** and **Password**, which are both **Tom123** in this example, then click **Login**.



Login identity

The server does not allow anonymous login or does not accept the email address.

User name(U)

FTP server 192.168.0.104

User name(U) Tom123

Password(P) ●●●●●●●●●

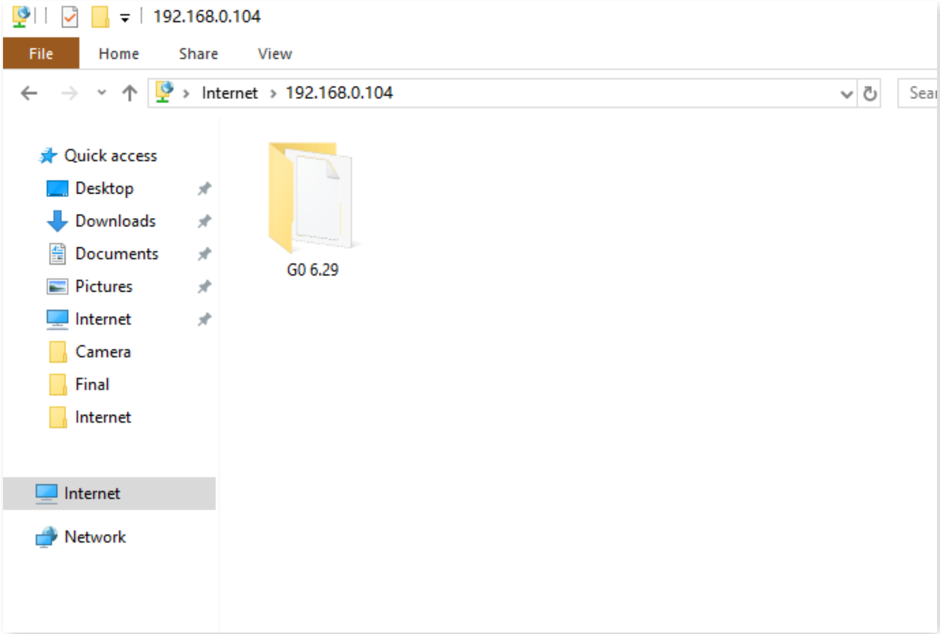
After logging in, you can add this server to your favorites for easy return.

FTP does not encrypt or encode passwords or data before sending it to the server. To secure passwords and data, please use webdan.

☐ Anonymous login(A) ☐ Save password(S)

----End

The headquarters LAN resources can be accessed successfully. See the following figure.



TIP

If you want to use the mobile device (such as smartphone and tablet) to access the FTP server, you should install an FTP client on your mobile device first.

12.12 Multi-WAN policy

12.12.1 Overview

The router supports the following types of multi-WAN policy:

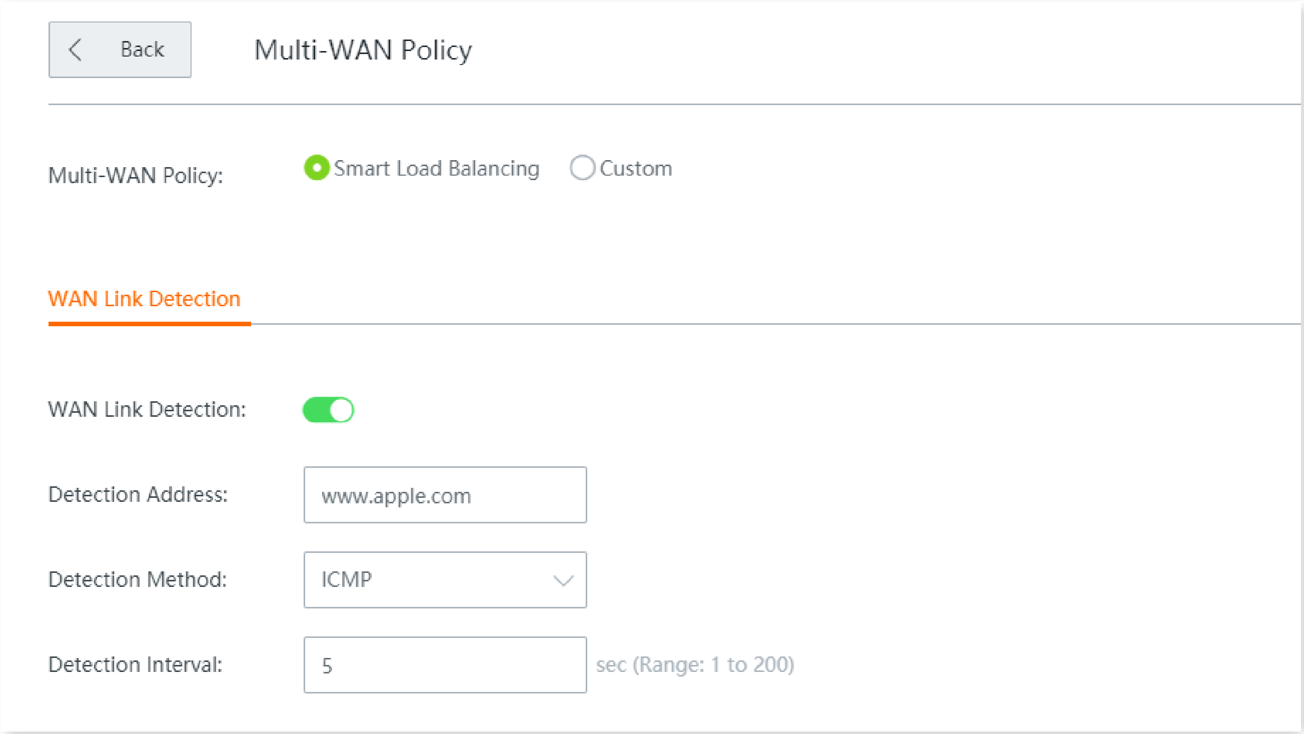
- **Smart load balancing (default)**

  If such a policy is applied, the router automatically distributes traffic based on the bandwidth on the **Bandwidth Control** page through the WAN ports to achieve load balancing.

- **Custom**

  Such a policy is configured by an administrator to distribute traffic of specified IP address groups to specified WAN ports.

Click **More** > **Multi-WAN Policy** to enter the page.



Multi-WAN Policy: ● Smart Load Balancing ○ Custom

WAN Link Detection: ●

Detection Address: www.apple.com

Detection Method: ICMP

Detection Interval: 5 sec (Range: 1 to 200)

Parameter description

Parameter	Description
Mutil-WAN Policy	Specifies the policy through the WAN ports. • **Smart Load Balancing**: The system automatically distributes traffic through the WAN ports with the smallest amount of traffic. • **Custom**: It enables you to assign WAN ports to source IP addresses as required.
WAN Link Detection	The router regularly detects the connection status between the WAN ports and detection address. • **Detection Address:** The IP address or domain name to detect. • **Detection Method:** When the route is unreachable, the network sends the TCP or ICMP packets with error messages to the router. • **Detection Interval:** The interval of detection, 5 seconds by default.

12.12.2 Customize a multi-WAN policy

TIP

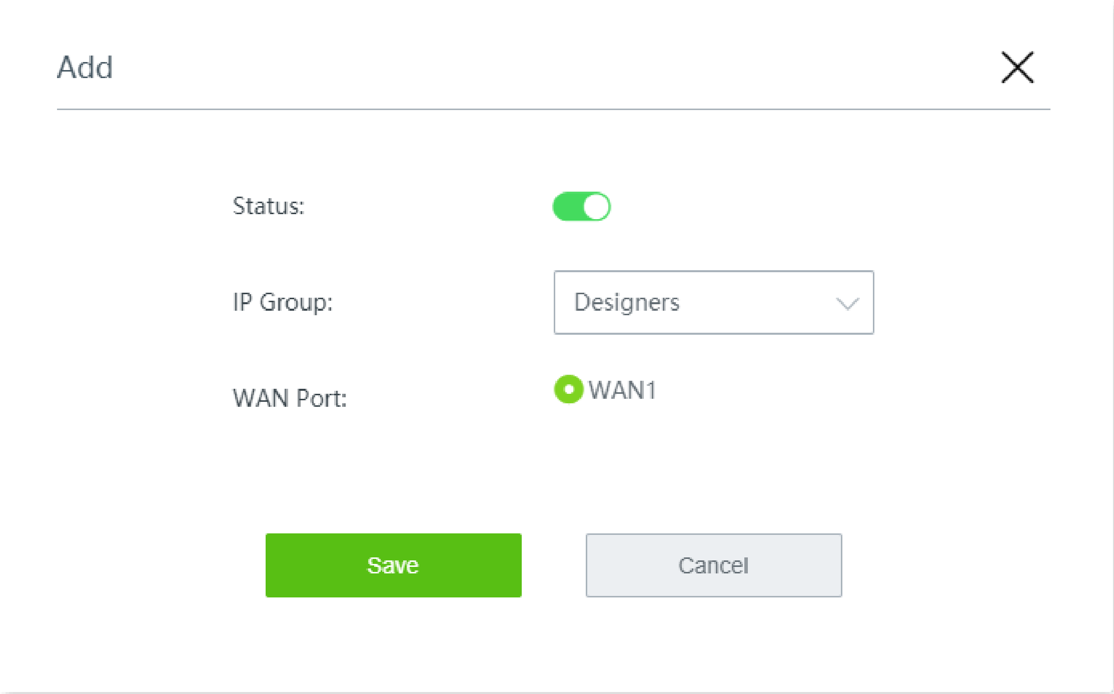
Before configuring the multi-WAN policy, go to **Filter Management** > **IP Group/Time Group** to add an IP group first.

Step 1 Navigate to **More** > **Multi-WAN Policy**, select **Custom** and click **+Add**.

Step 2 Select the **IP Group** you set.

Step 3 Select the **WAN** port to which the policy applies.

Step 4 Click **Save**.



Add

Status: ●

IP Group: Designers

WAN Port: ● WAN1

----End

Parameter description

Parameter	Description
Status	Enable or disable the rule.
IP Group	Create or select the IP group to which the rule applies. To create an IP group, choose **Filter Management** > **IP Group/Time Group**.
WAN Port	Specifies the WAN port for incoming and outgoing traffic.

12.12.3 Example of customizing a multi-WAN policy

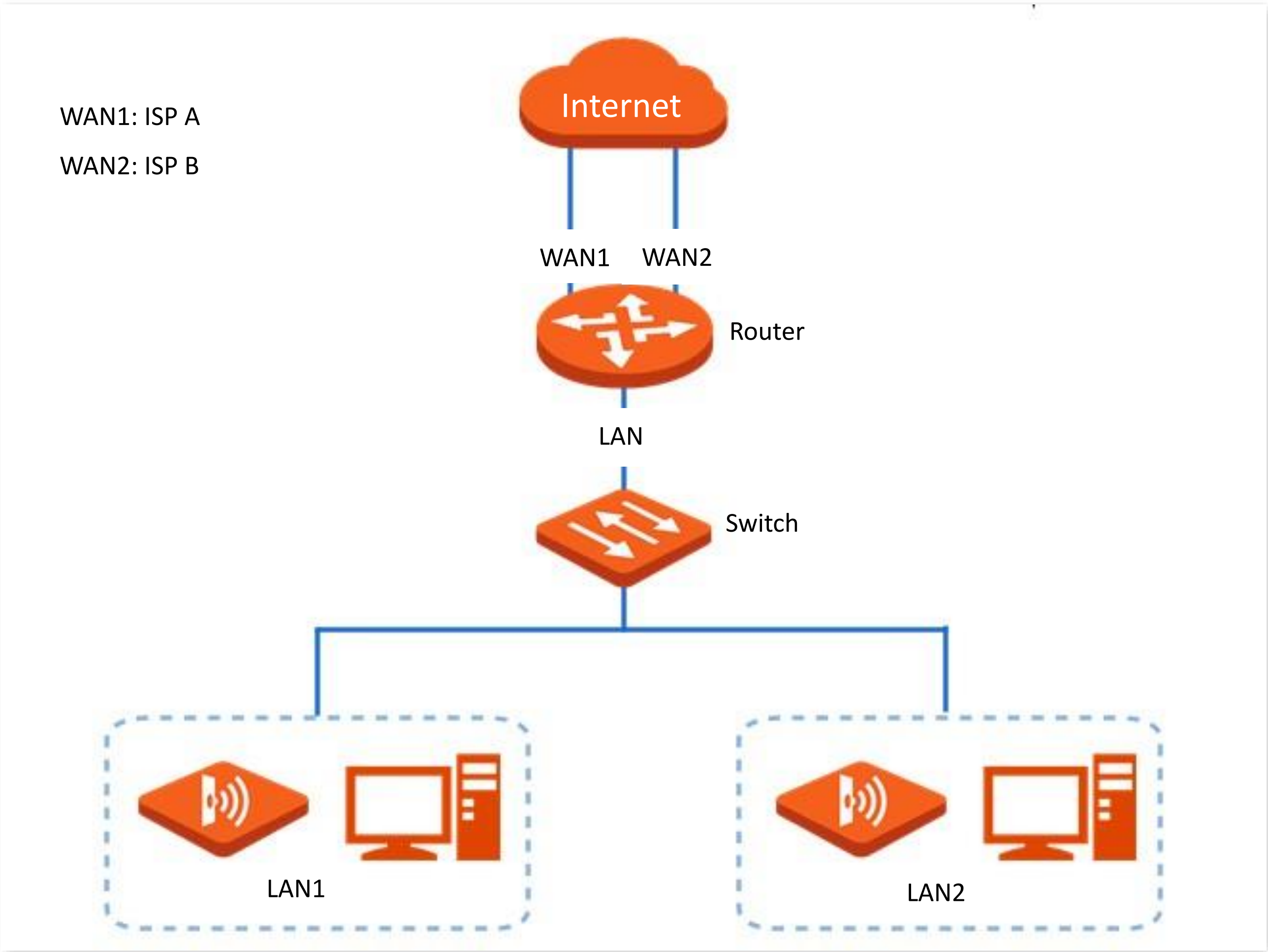
Networking Requirement

An enterprise and its branch use the wireless router to set up a network and access the internet. To meet its internet access requirement, the enterprise has set up two broadband connections with two different ISPs and can now access the Internet properly. To achieve load balancing, the enterprise raises the following LAN requirements:

- The devices with IP addresses ranging from 192.168.0.2 to 192.168.0.100 access the internet through the fixed-line broadband connection with ISP A.
- The devices with IP addresses ranging from 192.168.0.101 to 192.168.0.250 access the internet through the mobile broadband connection with ISP B.

Solution

You can use the multi-WAN policy function of the router to meet this requirement.

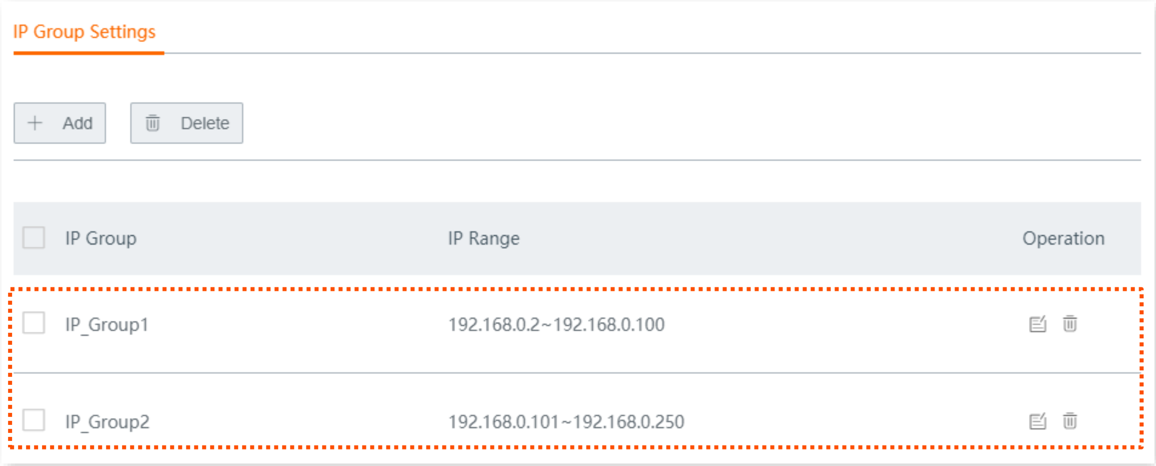


Configuration Procedure

Configure IP Group/Time Group > Enable customize multi-WAN policy > Customize multi-WAN policy rule

Step 1 Set IP address groups.

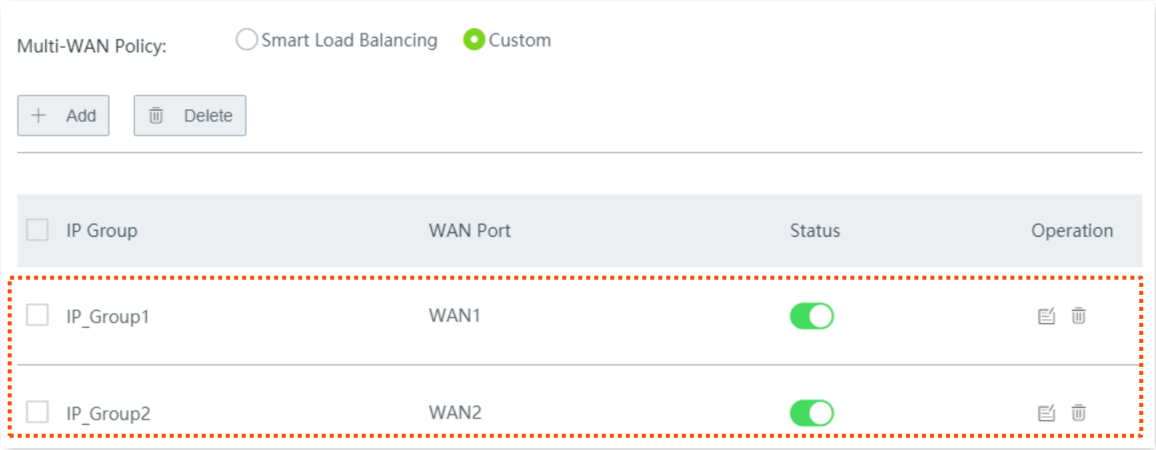
Navigate to **Filter Management** > **IP Group/Time Group**, and add the IP groups as follows.



□	IP Group	IP Range	Operation
□	IP_Group1	192.168.0.2~192.168.0.100	
□	IP_Group2	192.168.0.101~192.168.0.250	

Step 2 Customize multi-WAN policies.

1. Navigate to **More** > **Multi-WAN Policy**.
2. Select **Custom**, and click **Save**.
3. Click **+Add**, and set the rules shown in the following figure.



Multi-WAN Policy: ○ Smart Load Balancing ● Custom

□	IP Group	WAN Port	Status	Operation
□	IP_Group1	WAN1	●	
□	IP_Group2	WAN2	●	

----End

Verification

The computers with IP addresses ranging from 192.168.0.2 to 192.168.0.100 access the internet through WAN1.

The computers with IP addresses ranging from 192.168.0.101 to 192.168.0.250 access the internet through WAN2.

12.13 IPv6

TIP

Only the WAN1 port of the router supports IPv6, so you need to connect the broadband with IPv6 service to WAN1 before configuring the following functions.

12.13.1 Overview

IPv6 is abbreviated for Internet Protocol version 6, a second-generation standard network layer protocol. It is an upgraded version of IPv4 and addresses many defects in IPv4. The most significant difference between IPv6 and IPv4 is that IP addresses are lengthened from 32 bits to 128 bits.

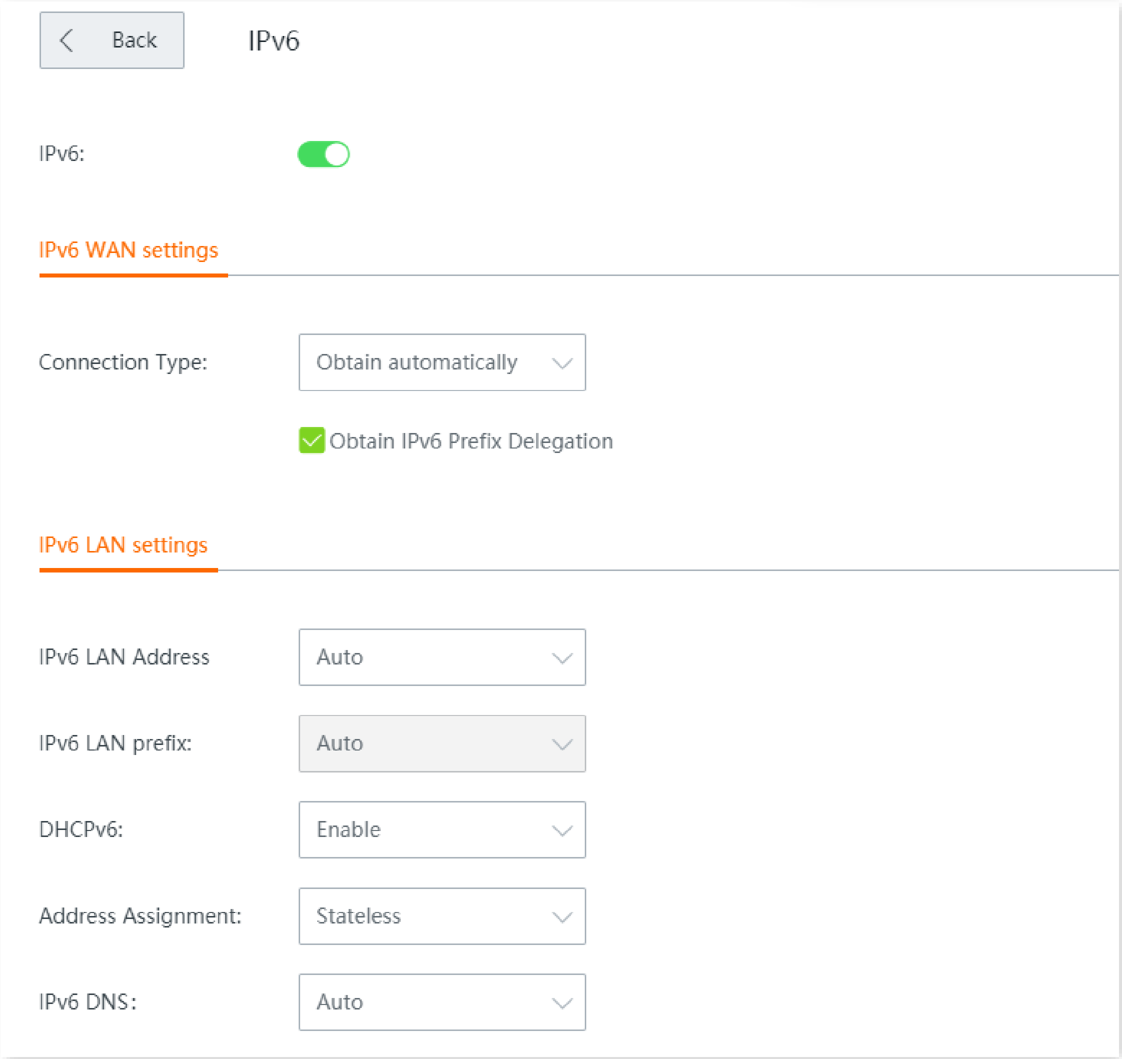
IPv6 addresses are represented as eight groups of four hexadecimal digits each, separated by colons.

An IPv6 address consists of a network prefix and an interface ID.

- A network prefix has n bits and is similar to the network ID in an IPv4 address.
- An interface identifier has (128 – n) bits and is similar to the host ID in an IPv4 address.

Click **More** > **IPv6** to enter the page.

By default, IPv6 is disabled.



IPv6: ●

IPv6 WAN settings

Connection Type: Obtain automatically

☑ Obtain IPv6 Prefix Delegation

IPv6 LAN settings

IPv6 LAN Address: Auto

IPv6 LAN prefix: Auto

DHCPv6: Enable

Address Assignment: Stateless

IPv6 DNS: Auto

12.13.2 IPv6 WAN settings

The router can access the IPv6 network of ISPs through three connection types. Choose the connection type by referring to the following chart.

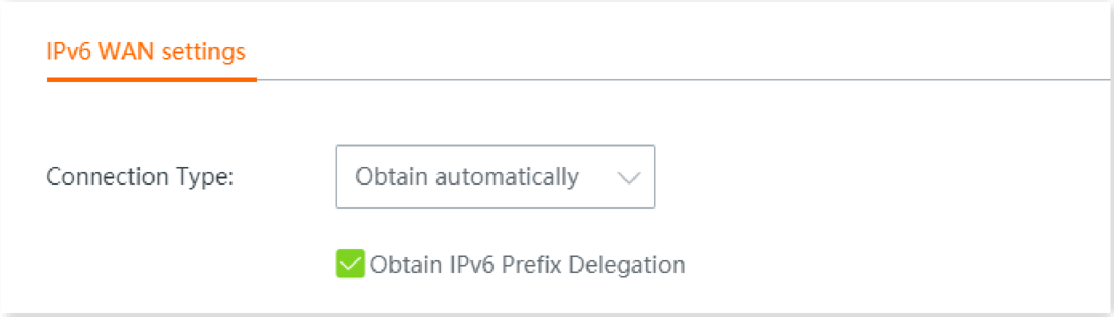
Scenario	Connection Type
- The ISP does not provide any PPPoEv6 user name and password. - The ISP does not provide information about IPv6 address. - You have a router that can access IPv6 network.	Obtain Automatically
IPv6 service is included in the PPPoE user name and password.	PPPoEv6
- The ISP provides you with a set of information including IPv6 address, subnet mask, default gateway and DNS server, etc. - The LAN port of the upstream device disables the DHCPv6 function	Static IPv6 Address

TIP

Before configuring the IPv6 function, ensure that you are within the coverage of IPv6 network and already subscribe the IPv6 internet service. Contact your ISP for any doubt about it.

Obtain automatically

This type enables the router to obtain an IPv6 address from a DHCPv6 server to access the internet.


IPv6 WAN settings

Connection Type: Obtain automatically

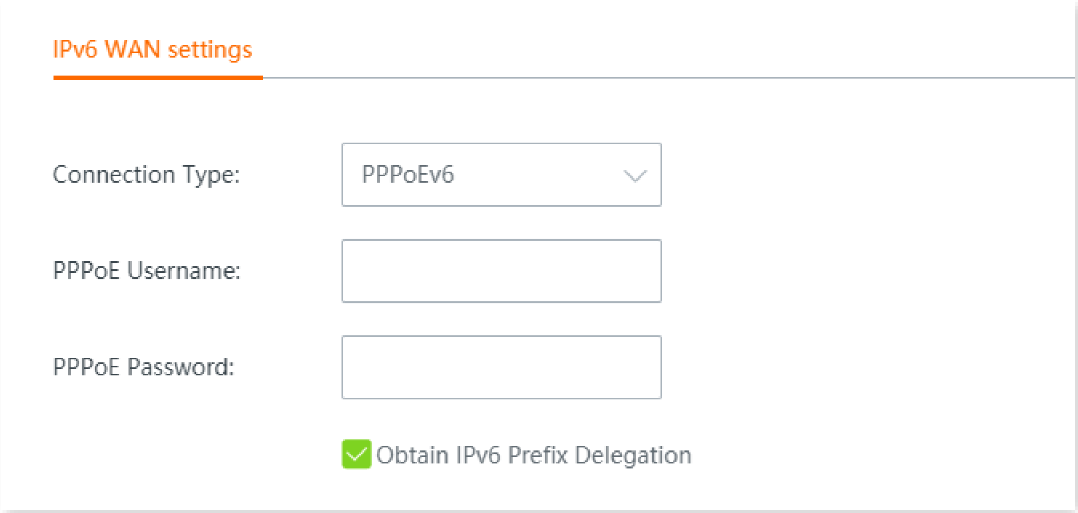
☑ Obtain IPv6 Prefix Delegation

Parameter description

Parameter	Description
Obtain IPv6 Prefix Delegation	When the option is selected, the LAN port of router obtains IPv6 prefix from its upstream device. It is recommended to keep the default setting (Selected). TIP If the LAN port cannot obtain the PD prefix, it is because the upstream device does not support PD prefix delivery. Contact your ISP to solve this problem.

PPPoEv6

If your ISP provides you with the PPPoE user name and password with IPv6 service, you can choose PPPoEv6 to access the internet.



IPv6 WAN settings

Connection Type: PPPoEv6

PPPoE Username:

PPPoE Password:

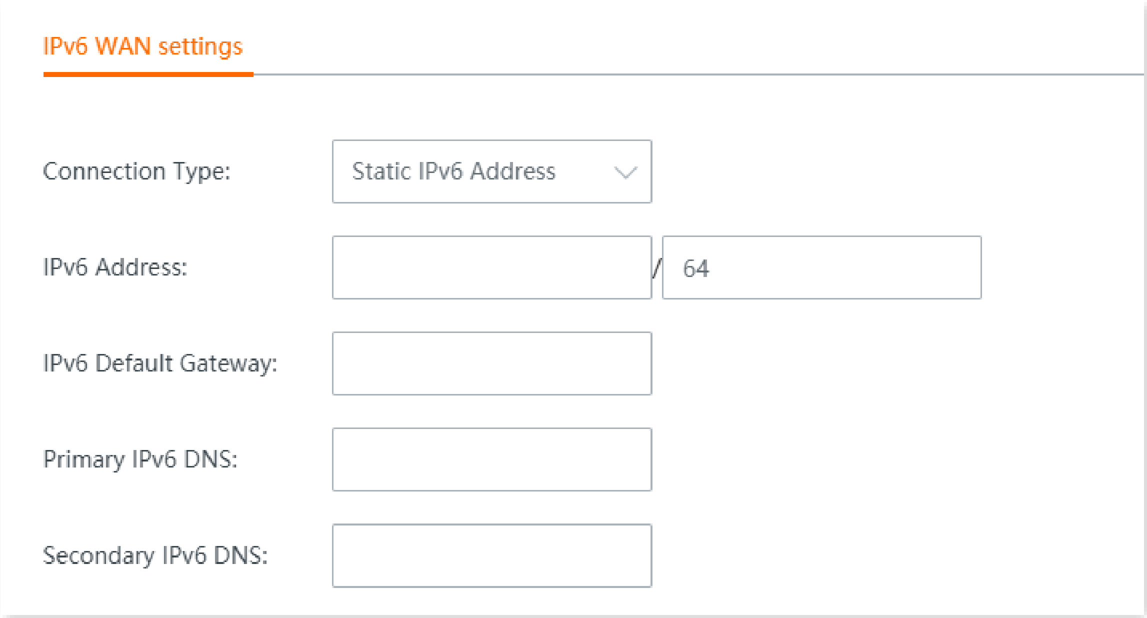
☑ Obtain IPv6 Prefix Delegation

Parameter description

Parameter	Description
PPPoE Username	Specifies the PPPoE user name and password provided by your ISP.
PPPoE Password	
Obtain IPv6 Prefix Delegation	When the option is selected, the LAN port of router obtains IPv6 prefix from its upstream device. It is recommended to keep the default setting (Selected). TIP If the LAN port cannot obtain the PD prefix, it is because the upstream device does not support PD prefix delivery. Contact your ISP to solve this problem.

Static IPv6 Address

When your ISP provides you with information including IPv6 address, subnet mask, default gateway and DNS server, you can choose this connection type to access the internet with IPv6.



Connection Type: Static IPv6 Address

IPv6 Address: / 64

IPv6 Default Gateway:

Primary IPv6 DNS:

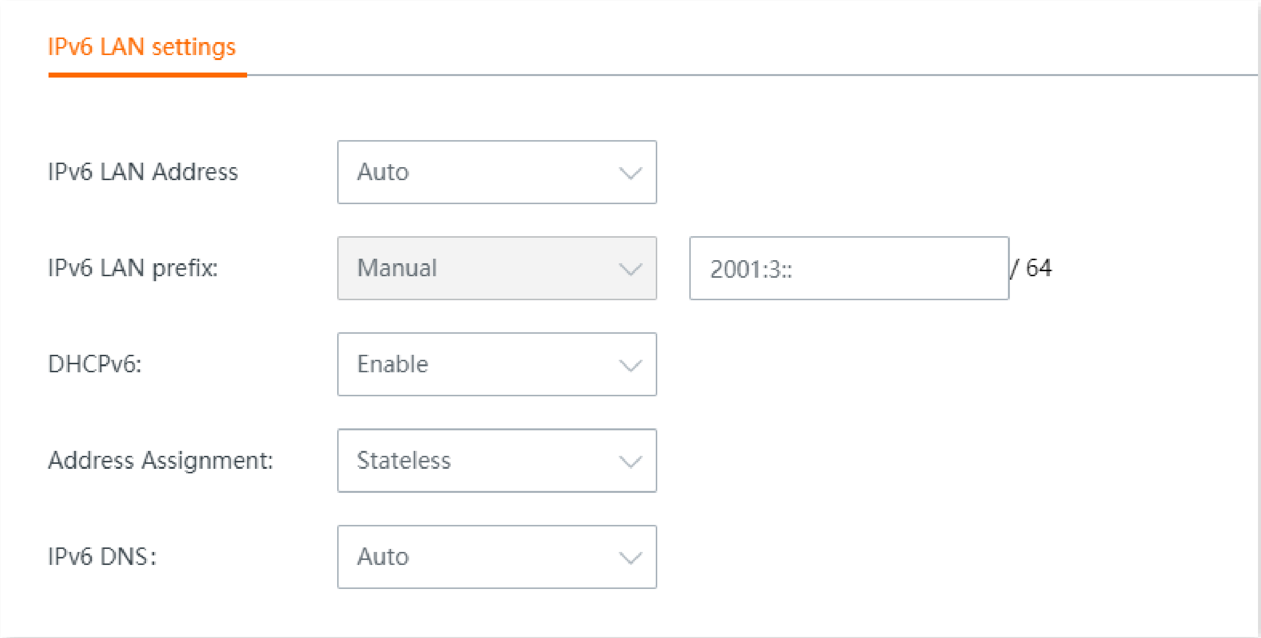
Secondary IPv6 DNS:

Parameter description

Parameter	Description
IPv6 Address	Specifies the fixed IP address information provided by your ISP. TIP If your ISP only provides one DNS server address, you can leave the **Secondary IPv6 DNS** blank.
IPv6 Default Gateway	
Primary IPv6 DNS	
Secondary IPv6 DNS	

12.13.3 IPv6 LAN settings

To enable LAN devices to access the IPv6 network, you can change the IPv6 LAN settings here.



IPv6 LAN settings

IPv6 LAN Address: Auto

IPv6 LAN prefix: Manual 2001:3:: / 64

DHCPv6: Enable

Address Assignment: Stateless

IPv6 DNS: Auto

Parameter description

Parameter	Description
IPv6 LAN Address	Specifies two types of IPv6 LAN address assignment. - **Auto**: The router generates the IPv6 address according to its LAN IPv6 address. By default, the prefix has 64 digits. - **Manual**: You need to set the IPv6 LAN address manually.
IPv6 LAN Prefix	Specifies two types IPv6 LAN prefix address assignment. - **Auto**: The router obtains a LAN prefix from the upstream device. Available when you select **Obtain IPv6 Prefix Delegation**. - **Manual**: You need to set the IPv6 LAN prefix manually. Available when you deselect **Obtain IPv6 Prefix Delegation**.
DHCPv6	DHCPv6 (Dynamic Host Configuration Protocol for IPv6) is used to assign IP addresses and prefix to IPv6 hosts on a network. It is the IPv6 equivalent of the DHCP for IPv4. This is also known as a stateful autoconfiguration.
Address Assignment	Specifies the assignment type of DHCPv6 address for the clients connected to the router. - **Stateless**: DHCPv6 stateless configuration. Clients obtain their IPv6 address through Router Advertisement (Stateless Auto Address Configuration) and other parameters are allocated by the DHCPv6 server. - **Stateful**: DHCPv6 stateful configuration. The DHCPv6 server automatically assigns IPv6 addresses/prefixes and other network configuration parameters (for example, DNS server addresses and so on) to clients. The user needs to manually configure the start ID and the end ID.
Start ID	The configuration is required when the IPv6 **Address Assignment** is set to **Stateful**. Specifies the range of the last segment of the IPv6 address that the DHCPv6 server
End ID	

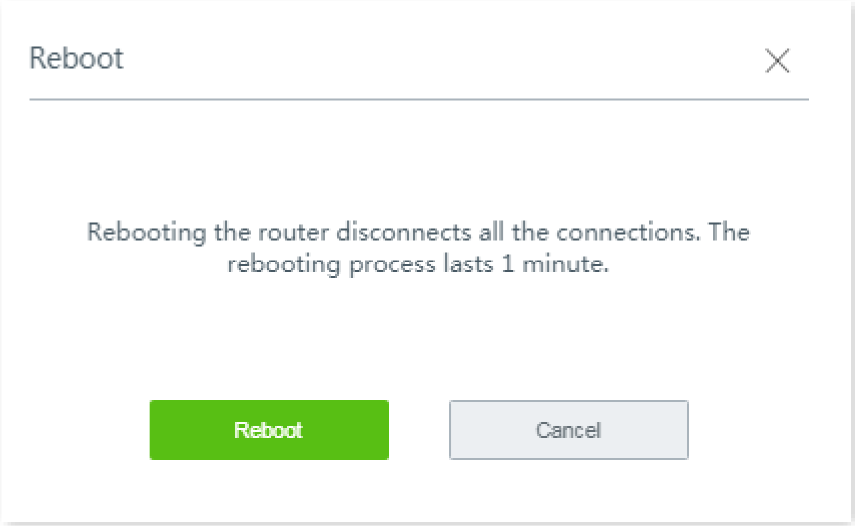
Parameter	Description
	assigns to the devices. Range: 1 to ffff.
IPv6 DNS	Specifies the LAN IPv6 DNS configuration method. ● **Auto**: Obtain the IPv6 DNS address from the upstream device. ● **Manual**: Configure the IPv6 DNS address manually.
Primary IPv6 DNS	Specifies the fixed IPv6 DNS address provided by your ISP here. Available when you set **IPv6 DNS** to **Manual**. TIP If your ISP only provides one DNS server address, you can leave the **Secondary IPv6 DNS** blank.
Secondary IPv6 DNS	

13 Maintenance

13.1 Reboot

If any parameter fails to take effect or the router does not work properly, you can try rebooting the router.

Click **Maintenance > Reboot**, and follow the on-screen instruction to reboot the device.



Reboot

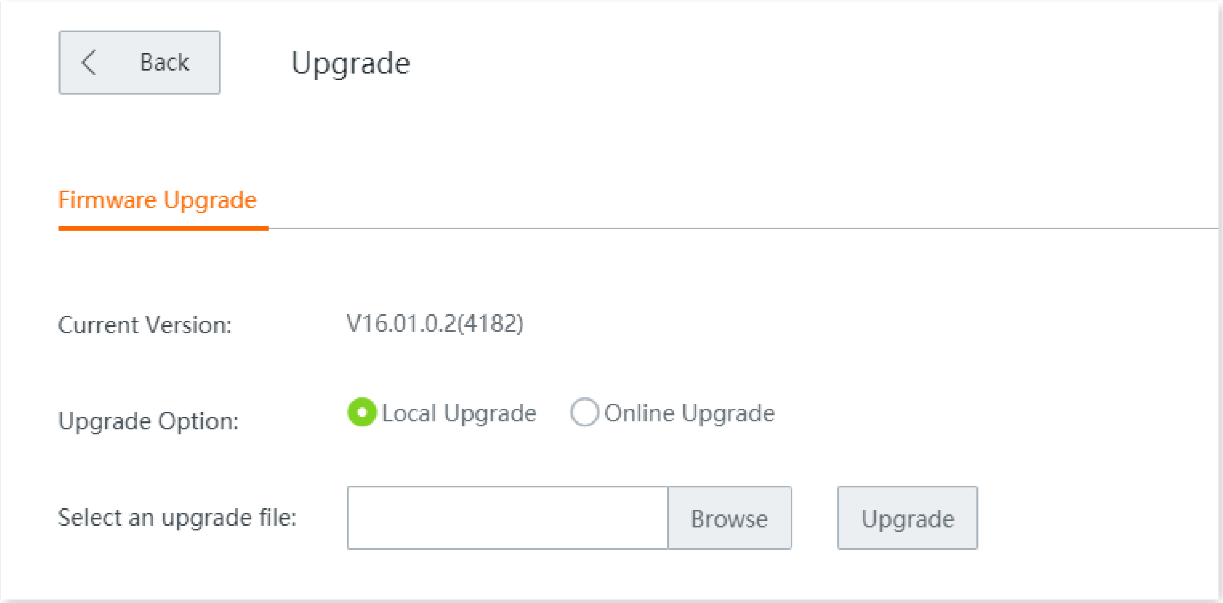
Rebooting the router disconnects all the connections. The rebooting process lasts 1 minute.

13.2 Upgrade

13.2.1 Overview

The router supports **Local Upgrade** and **Online Upgrade**.

Click **Maintenance** > **Upgrade** to enter the page.



Current Version: V16.01.0.2(4182)

Upgrade Option: ● Local Upgrade ○ Online Upgrade

Select an upgrade file:

13.2.2 Local upgrade

TIP

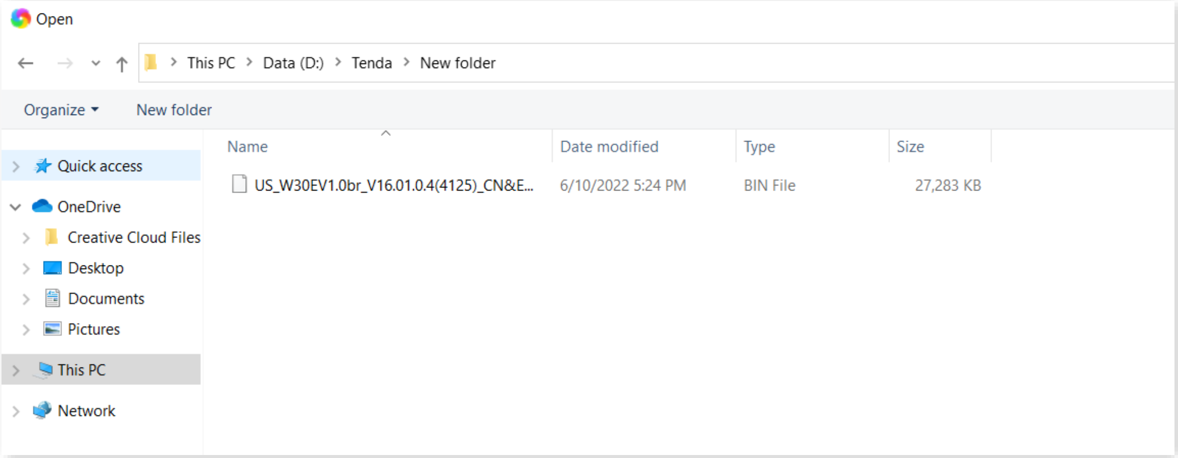
- To enable your router to work properly after an upgrade, ensure that the firmware used to upgrade complies with your product model.
- When upgrading, do not power off the router.

Step 1 Visit www.tendacn.com, search the product model, and download the latest firmware to your computer.

Step 2 Log in to the web UI of your router, and navigate to **Maintenance** > **Upgrade**.

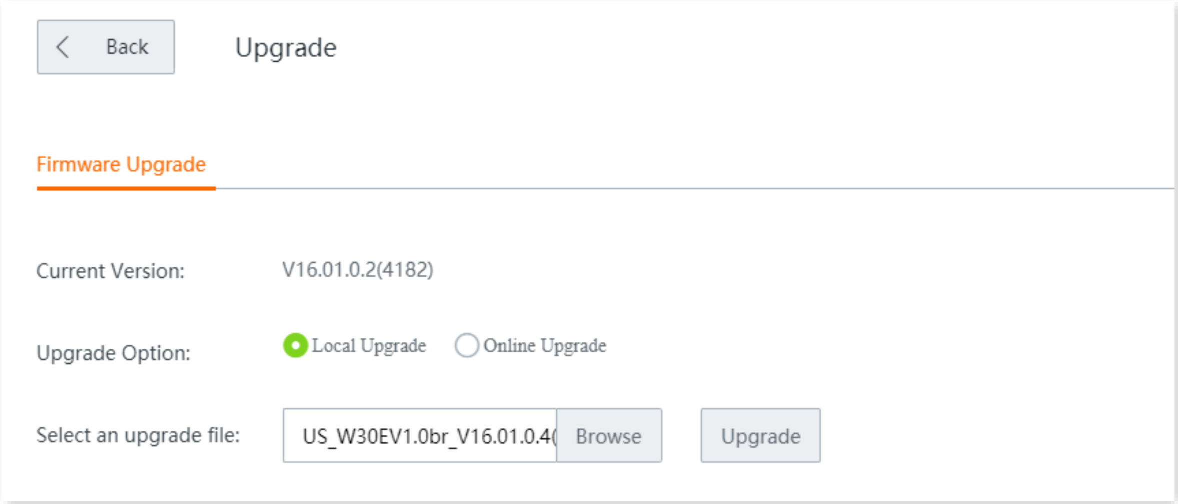
Step 3 Set **Upgrade Option** to **Local Upgrade**.

Step 4 Click **Browse**, select and upload the firmware that has been downloaded to your computer. Ensure that the suffix of the firmware is **.bin**.



Name	Date modified	Type	Size
US_W30EV1.0br_V16.01.0.4(4125)_CN&E...	6/10/2022 5:24 PM	BIN File	27,283 KB

Step 5 Click **Upgrade**.



Current Version: V16.01.0.2(4182)

Upgrade Option: ● Local Upgrade ○ Online Upgrade

Select an upgrade file: US_W30EV1.0br_V16.01.0.4(

----End

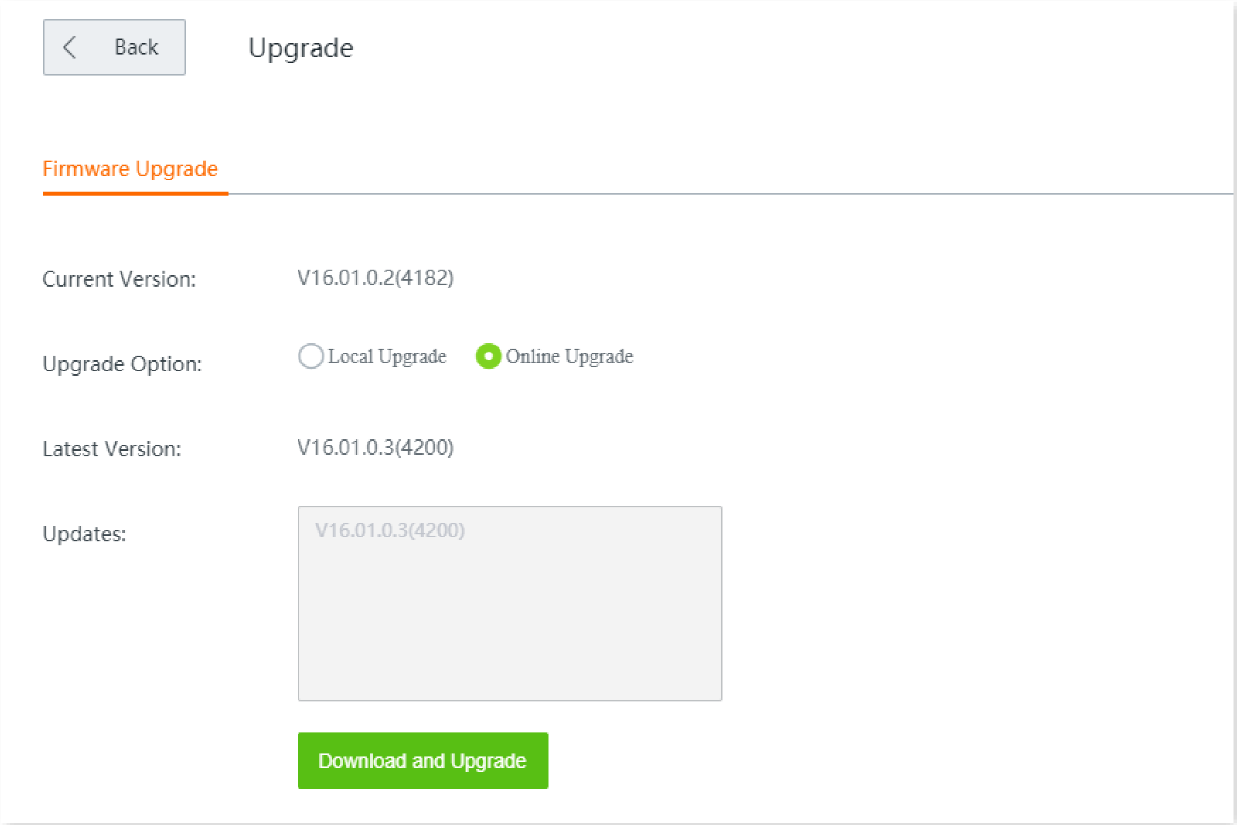
Wait for the upgrade to complete, then reset your router and configure it again to access the internet. To know whether the upgrade succeeds, go to the System Status or **Maintenance** > **Upgrade** page and check the current firmware version.

TIP

To better experience the stability and new features of the latest firmware, you are recommended to reset the router and configure it again after the upgrade completes.

13.2.3 Online upgrade

When the router is connected to the internet, it checks whether there is the latest firmware version, and displays the detected information on the page. If you want to upgrade the firmware, click **Download and Upgrade**.



Current Version: V16.01.0.2(4182)

Upgrade Option: ○ Local Upgrade ● Online Upgrade

Latest Version: V16.01.0.3(4200)

Updates: V16.01.0.3(4200)

13.3 Reset

13.3.1 Overview

If the internet is inaccessible for unknown reasons, or you forget the login password, you can reset the router to resolve the problems.

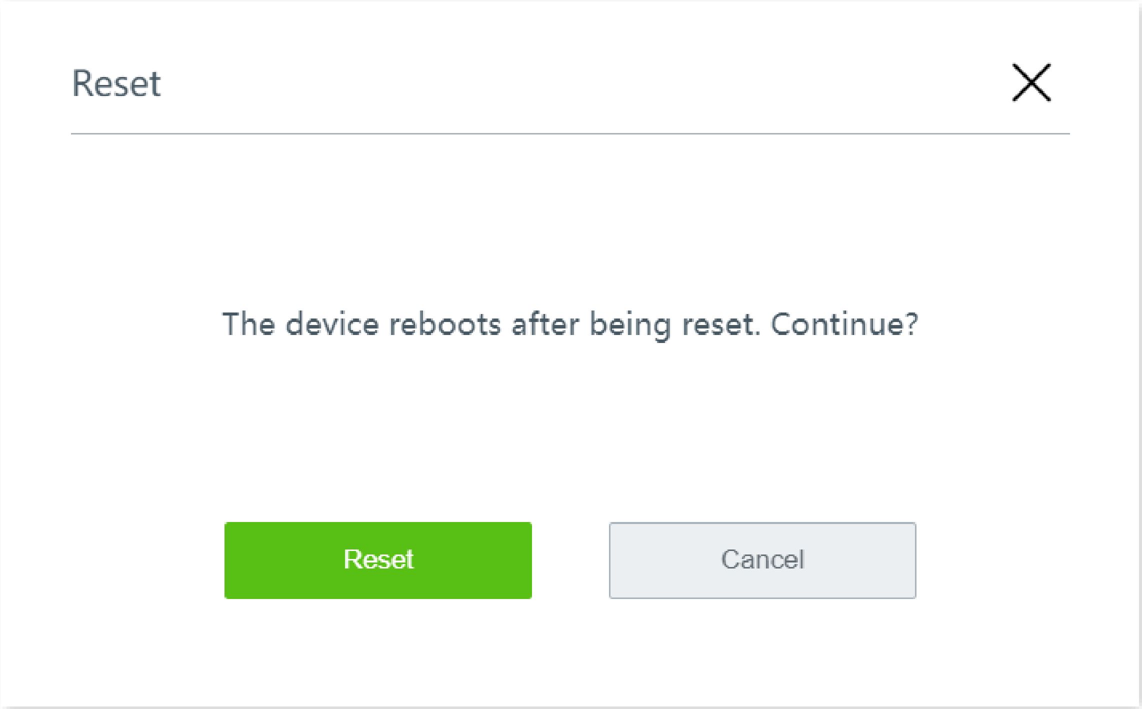
The router supports two resetting methods: Reset the router using web UI and Reset the router using the reset button.

TIP

- Resetting the router deletes all your current configurations and you need to reconfigure the router to access the internet.
- When resetting, do not power off the router.

13.3.2 Reset the router using web UI

Choose **Maintenance > Reset**, and follow the on-screen instruction to reset the device.



Reset

The device reboots after being reset. Continue?

13.3.3 Reset the router using the reset button

With the **SYS** LED indicator blinking, hold down the **Reset** button for about 8 seconds, and then release it. When all LED indicators light up, the router is reset to factory settings successfully.

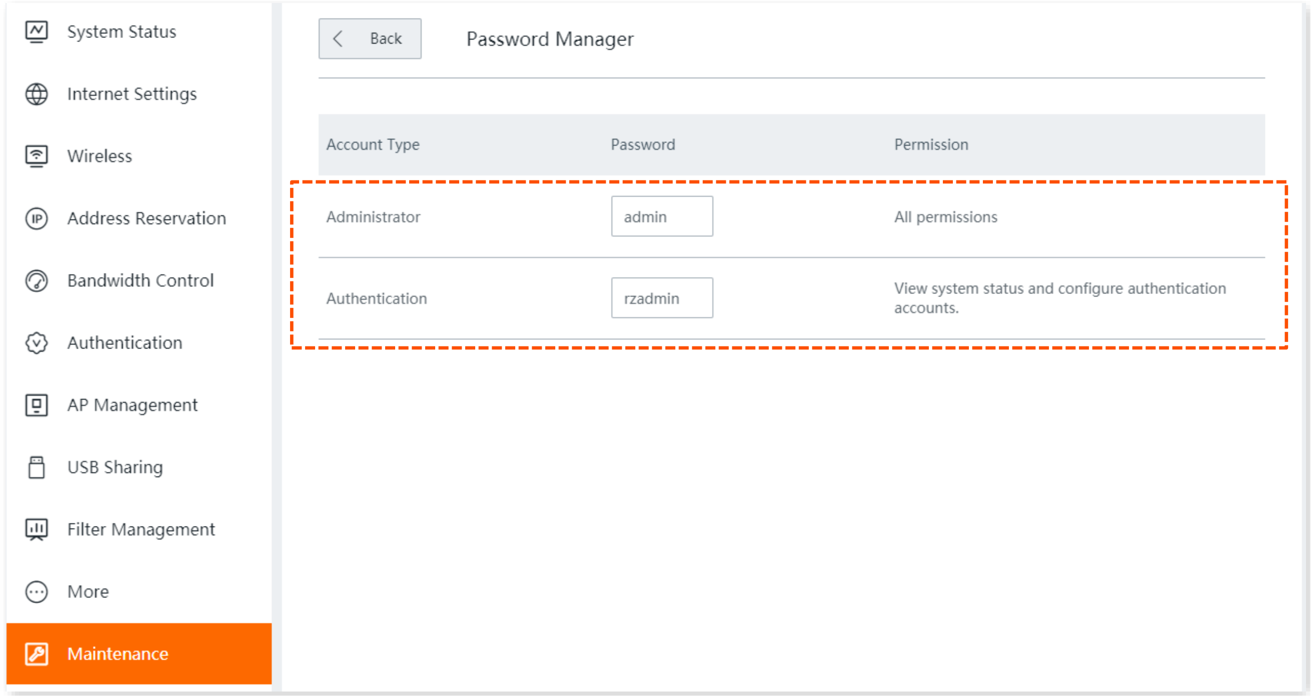
13.4 Password manager

13.4.1 Overview

The router supports two account types: **Administrator** and **Authentication**. The difference between them is their access permission.

- The **Administrator** account enjoys all access permission. Password for administrator account is the login password you set during initial setup. The default password for this account is **admin**.
- The **Authentication** account only has permission for accessing **System Status** and **Authentication** modules. The default password for this account is **rzadmin**.

Click **Maintenance > Password Manager** to enter the page.



Password Manager

Account Type	Password	Permission
Administrator	admin	All permissions
Authentication	rzadmin	View system status and configure authentication accounts.

13.4.2 Modify login password

Step 1 Navigate to **Maintenance** > **Password Manager**.

Step 2 Locate the account type and modify the password.

Step 3 Click **Save** on the bottom of the page to apply your settings.

----End

Then you will be redirected to the login page. Enter the password corresponding to the administrator account you set just now, and click **Login** to log in to the router.

13.5 Reboot schedule

13.5.1 Overview

Click **Maintenance** > **Reboot Schedule** to enter the page.

On this page, you can set the router to automatically reboot periodically to avoid such phenomena as deteriorating performance and instability caused by long time operation.

13.5.2 Customize reboot schedule

TIP

To enable reboot schedule function to work properly, ensure that the System time of your router is correct.

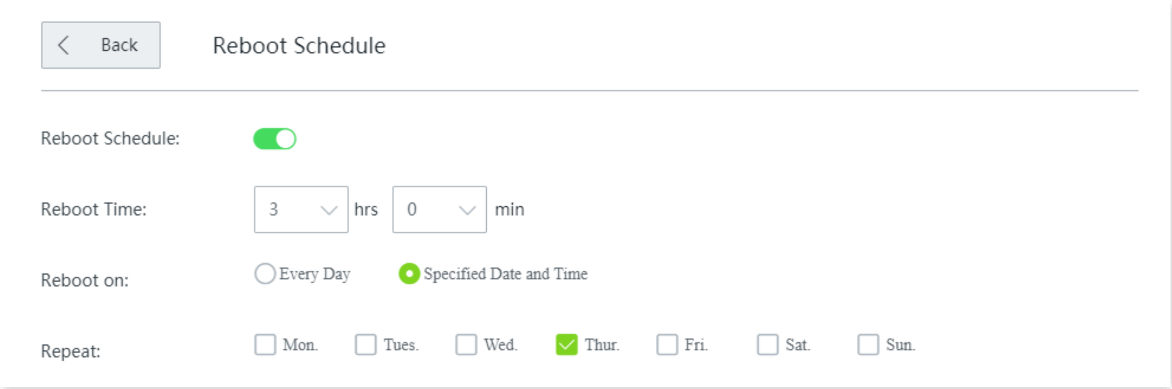
Step 1 Navigate to **Maintenance** > **Custom Reboot**.

Step 2 Enable **Reboot Schedule**.

Step 3 Set the time to reboot, such as **3 hrs 0 min**.

Step 4 Set the date to reboot, such as **Thursday**.

Step 5 Click **Save** at the bottom of the page.



Reboot Schedule: ●

Reboot Time: 3 hrs 0 min

Reboot on: ○ Every Day ● Specified Date and Time

Repeat: □ Mon. □ Tues. □ Wed. ☑ Thur. □ Fri. □ Sat. □ Sun.

----End

The device automatically reboots at 3 am on each Thursday.

13.6 Backup/Restore

13.6.1 Overview

The backup function is used to export the current configuration of the router to your computer. The restore function is used to import a configuration file to the router.

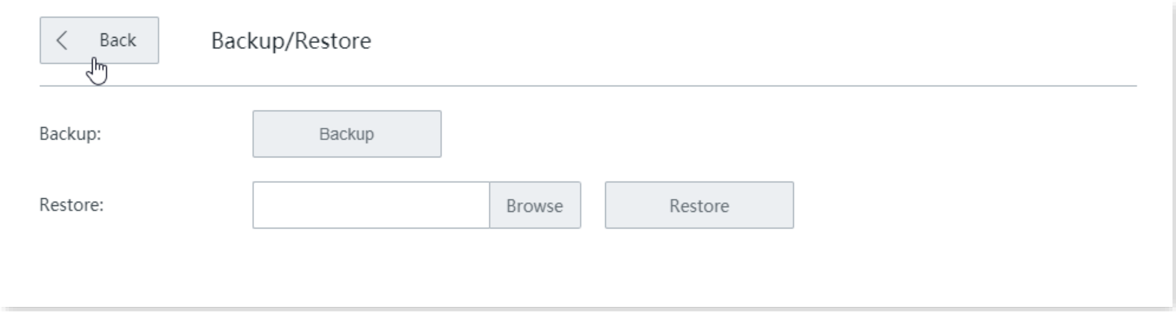
You are recommended to back up the configuration after it is significantly changed. When the performance of your router decreases because of an improper configuration, or after you restore the router to factory settings, you can use this function to restore the configuration that has been backed up.

Click **Maintenance** > **Backup/Restore** to enter the page.

13.6.2 Back up your current configuration

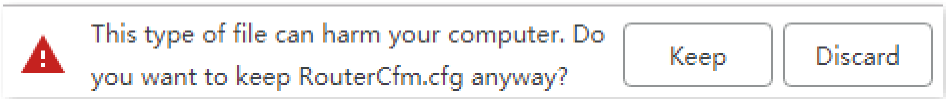
Step 1 Navigate to **Maintenance** > **Backup/Restore**.

Step 2 Click **Backup**. The system exports the configuration file to your local computer.



TIP

If the following warning message appears, click **Keep**.



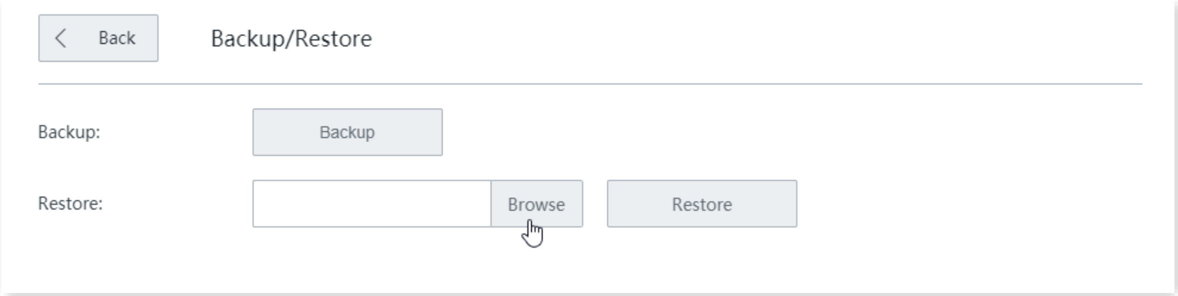
This type of file can harm your computer. Do you want to keep RouterCfm.cfg anyway?

----End

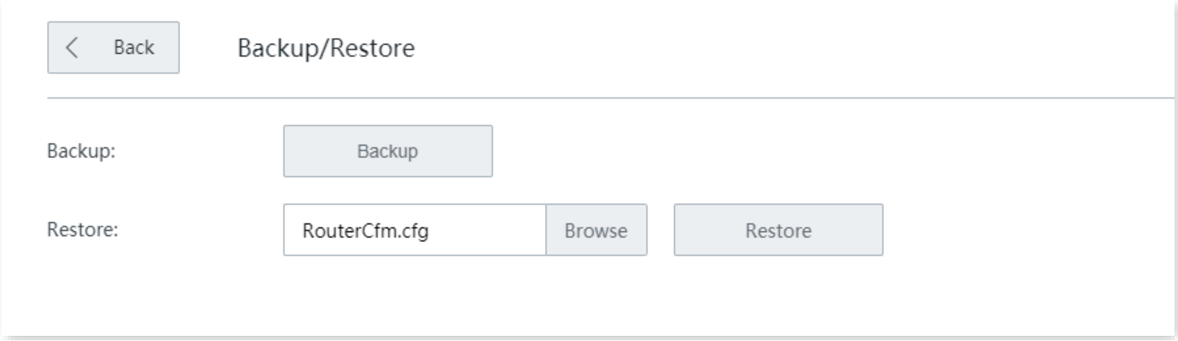
13.6.3 Restore your previous configuration

Step 1 Navigate to **Maintenance** > **Backup/Restore**.

Step 2 Click **Browse**, and upload the configuration file ending with **.cfg**.



Step 3 Click **Restore** and follow the on-screen instruction to restore the configuration.



Restore: RouterCfm.cfg

----End

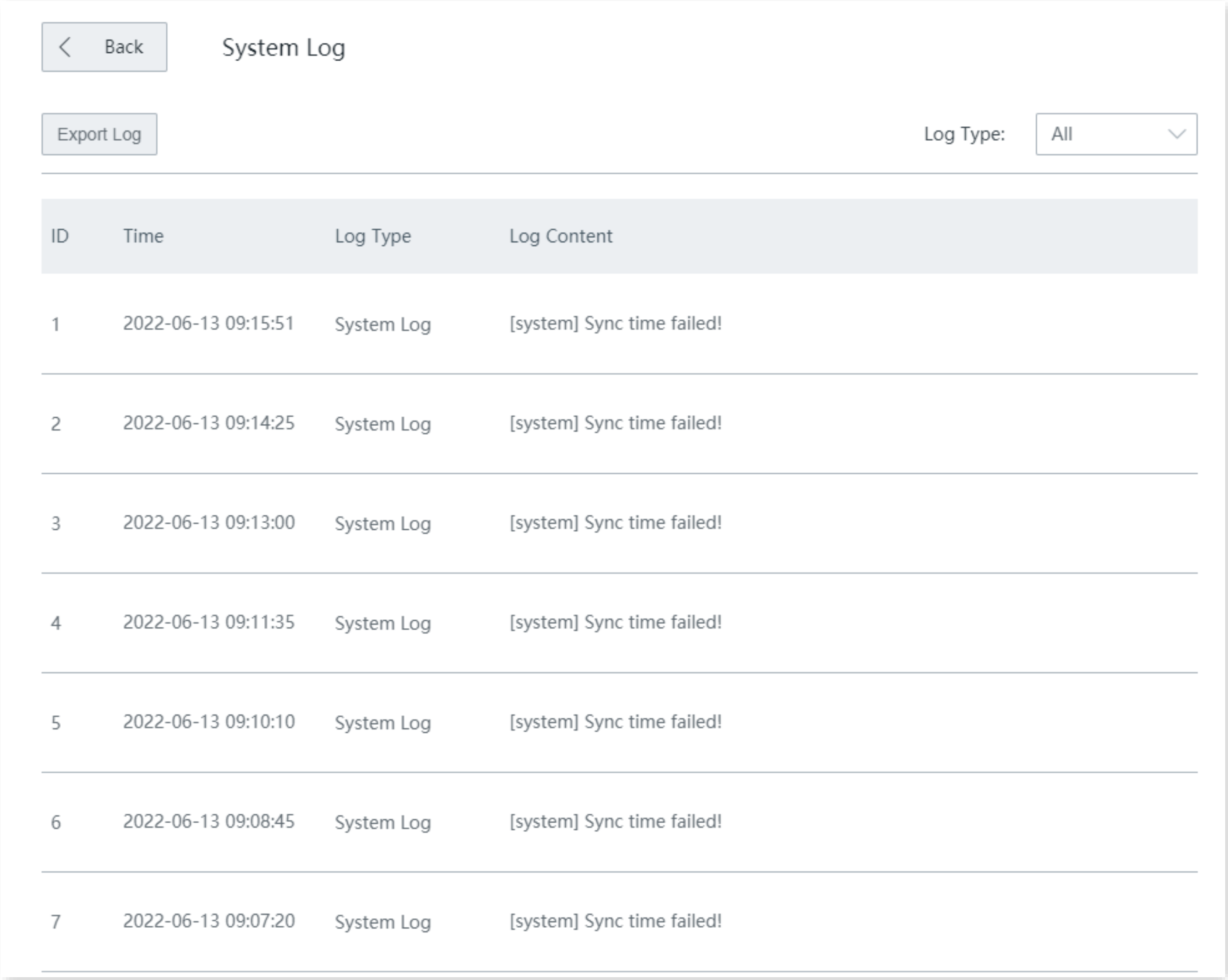
13.7 System log

System logs record information about the system running statuses such as system startup, dialing, time synchronization, device login and WAN connection. When system malfunctions occur, you can use the system log for troubleshooting.

Click **Maintenance** > **System Log** to enter the page.

Click **Export Log**, the log file will be downloaded to your local computer.

The router records three log types: **System Log**, **Attack Log**, and **Error Log**. You can view all logs or filter the logs to view as needed.



ID	Time	Log Type	Log Content
1	2022-06-13 09:15:51	System Log	[system] Sync time failed!
2	2022-06-13 09:14:25	System Log	[system] Sync time failed!
3	2022-06-13 09:13:00	System Log	[system] Sync time failed!
4	2022-06-13 09:11:35	System Log	[system] Sync time failed!
5	2022-06-13 09:10:10	System Log	[system] Sync time failed!
6	2022-06-13 09:08:45	System Log	[system] Sync time failed!
7	2022-06-13 09:07:20	System Log	[system] Sync time failed!

The time of log depends on the system time of the router. To make sure it is correct, please set correctly the System time of the router first.

TIP

- The router only records the logs occurred after the last reboot.
- After a power cutoff, such operations as power-on again, firmware upgrade, backup/restore, and reset will all cause the router to reboot.

13.8 Diagnostic tool

13.8.1 Overview

Click **Maintenance** > **Diagnostic Tool** to enter the page.

You can execute Ping/Traceroute command on this page.

- **Ping**: Used to check whether the connection is correct and the connection quality.
- **Traceroute**: Used to detect the route from the bridge to the destination IP address or domain name.

13.8.2 Execute Ping command

Assume that:

You need to detect the connectivity between the router and the **Bing** website.

Step 1 Navigate to **Maintenance** > **Diagnostic Tool**.

Step 2 Select **Ping** as the **Diagnostic Tool**.

Step 3 Enter the IP address or domain name of the ping target, which is **cn.bing.com** in this example.

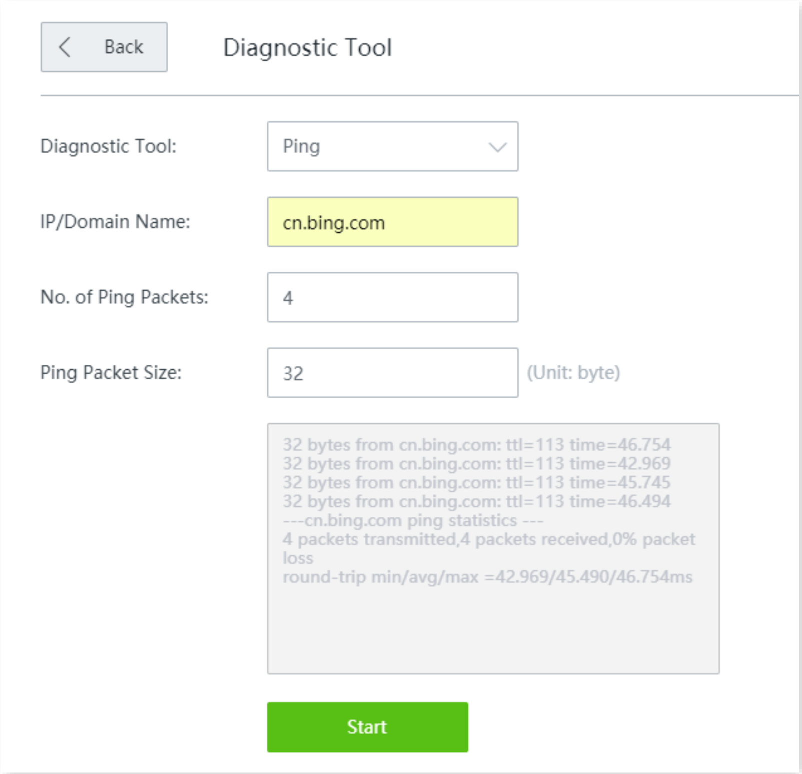
Step 4 Set **No. of Ping Packets** as required.

Step 5 Set **Ping Packet Size** as required.

Step 6 Click **Start**.

----End

Wait a moment. The ping result will be displayed in the result box.



Diagnostic Tool: Ping

IP/Domain Name: cn.bing.com

No. of Ping Packets: 4

Ping Packet Size: 32 (Unit: byte)

```
32 bytes from cn.bing.com: ttl=113 time=46.754
32 bytes from cn.bing.com: ttl=113 time=42.969
32 bytes from cn.bing.com: ttl=113 time=45.745
32 bytes from cn.bing.com: ttl=113 time=46.494
---cn.bing.com ping statistics ---
4 packets transmitted,4 packets received,0% packet
loss
round-trip min/avg/max =42.969/45.490/46.754ms
```

13.8.3 Execute Traceroute command

Assume that:

You need to detect the path from the router to **Bing** website.

Step 1 Navigate to **Maintenance** > **Diagnostic Tool**.

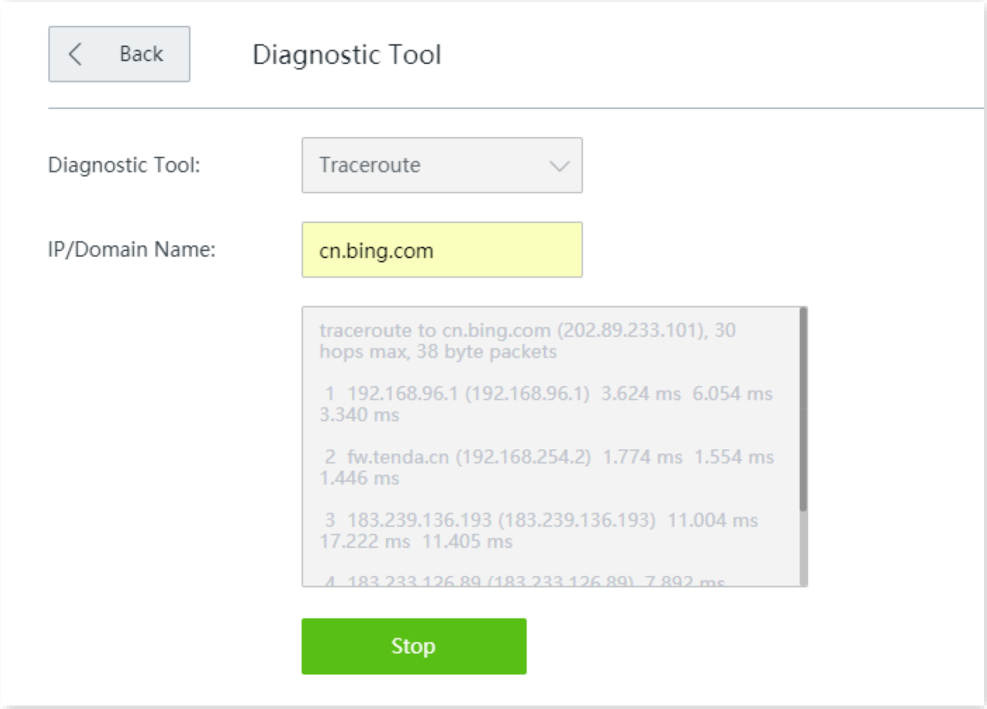
Step 2 Select **Traceroute** as the **Diagnostic Tool**.

Step 3 Enter the IP address or domain name of the traceroute target, which is **cn.bing.com** in this example.

Step 4 Click **Start**.

----End

Wait a moment. The traceroute result will be displayed in the result box.



Diagnostic Tool: Traceroute

IP/Domain Name: cn.bing.com

```
traceroute to cn.bing.com (202.89.233.101), 30
hops max, 38 byte packets

 1  192.168.96.1 (192.168.96.1)  3.624 ms  6.054 ms
3.340 ms

 2  fw.tenda.cn (192.168.254.2)  1.774 ms  1.554 ms
1.446 ms

 3  183.239.136.193 (183.239.136.193)  11.004 ms
17.222 ms  11.405 ms

 4  183.233.126.89 (183.233.126.89)  7.892 ms
```

13.9 System time

Click **Maintenance** > **System Time** to enter the page.

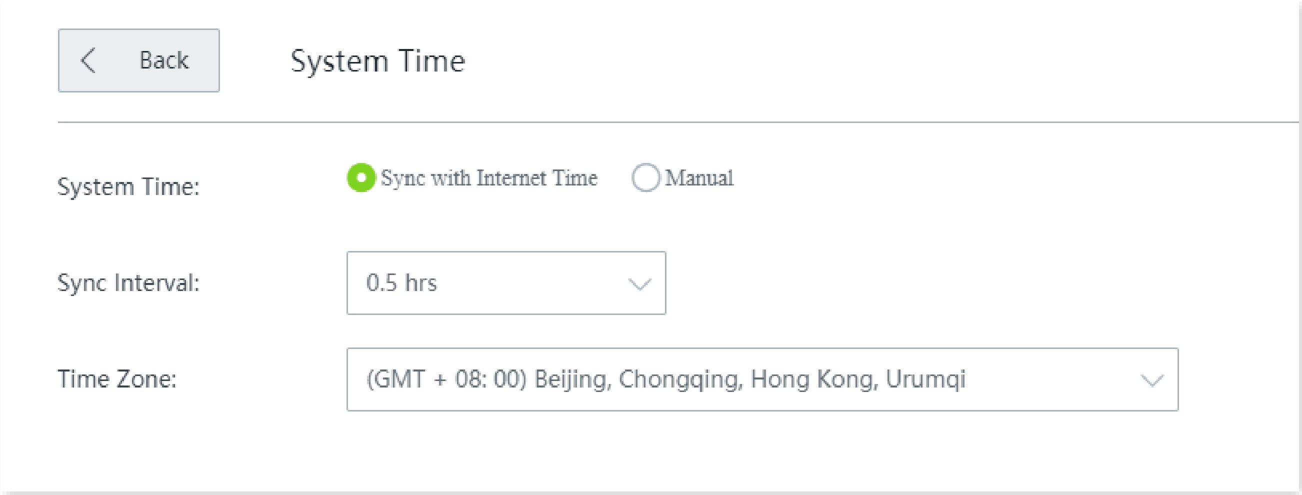
This function is used to set the system time of your router. To make the time-related functions effective, ensure that the system time of the router is set correctly.

The router supports: Synchronize with internet time (default) and Set system time manually.

13.9.1 Synchronize with internet time

With this method, the router automatically synchronizes its system time with the network time server (NTS). As long as the router is connected to the internet, the system time is correct.

After configuration, you can navigate to the System status page to check whether the system time is correct.



System Time

System Time: ● Sync with Internet Time ○ Manual

Sync Interval: 0.5 hrs

Time Zone: (GMT + 08: 00) Beijing, Chongqing, Hong Kong, Urumqi

Parameter description

Parameter	Description
System Time	Choose the configuration method of the system time.
Sync Interval	Specifies an interval at which the router synchronizes its system time with the time server on the internet.
Time Zone	Specifies the time zone where the router is deployed.

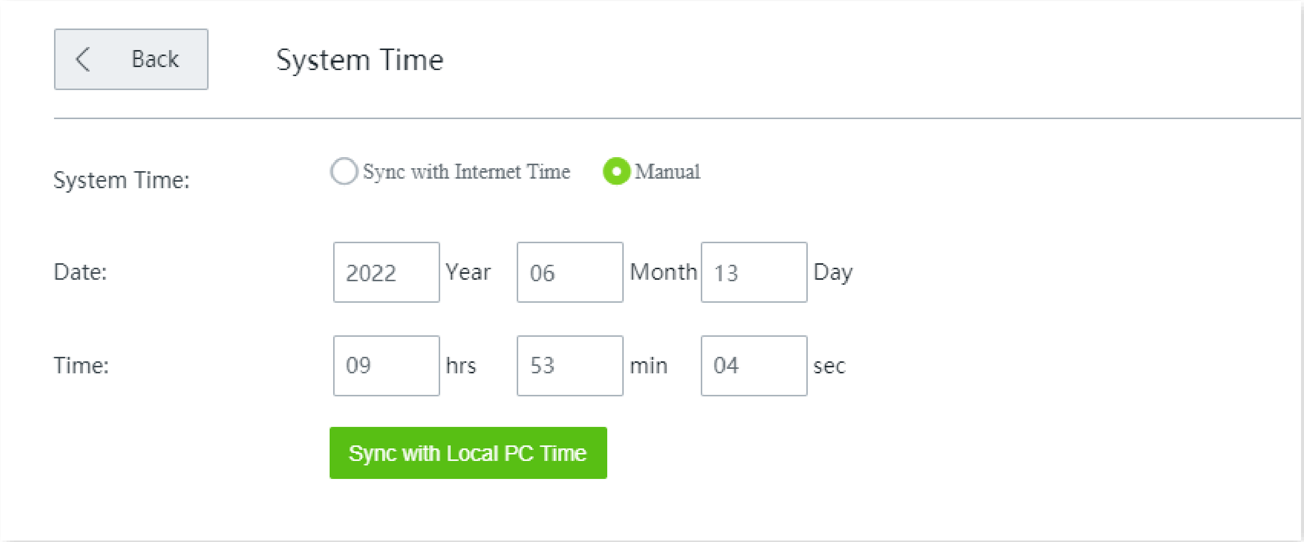
13.9.2 Set system time manually

With this method, you can manually specify a system time for the router. When **Manual** option is selected**,** the related parameters are shown as follows.

TIP

With this method, you need to manually reconfigure the system time each time the router reboots.

After configuration, you can navigate to the System status page to check whether the system time is correct.



System Time: ○ Sync with Internet Time ● Manual

Date: 2022 Year 06 Month 13 Day

Time: 09 hrs 53 min 04 sec

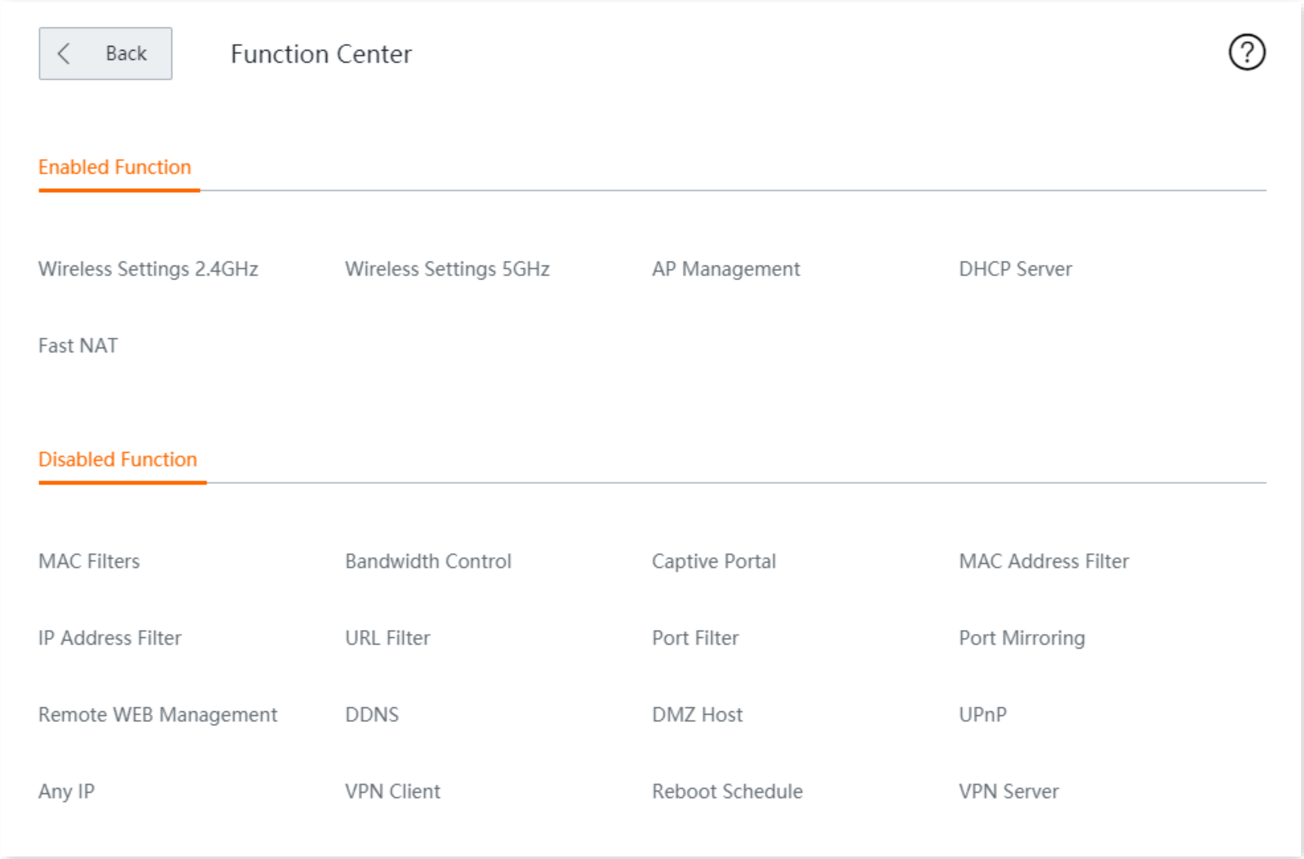
Parameter description

Parameter	Description
System Time	Choose the configuration method of the system time.
Date	You can directly enter the correct time here. Or, you can click **Sync with Local PC Time** to synchronize the time of the router with that of the computer managing the router.
Time	

13.10 Function center

Click **Maintenance** > **Function Center** to enter the page.

On this page, you can view the **Enabled Function** and **Disabled Function** of the router. You can enter the configuration page of a function after clicking it.



Enabled Function

Wireless Settings 2.4GHz   Wireless Settings 5GHz   AP Management   DHCP Server
Fast NAT

Disabled Function

MAC Filters   Bandwidth Control   Captive Portal   MAC Address Filter
IP Address Filter   URL Filter   Port Filter   Port Mirroring
Remote WEB Management   DDNS   DMZ Host   UPnP
Any IP   VPN Client   Reboot Schedule   VPN Server

Appendix

Acronyms and Abbreviations

Acronym and Abbreviation	Full Spelling
AES	Advanced Encryption Standard
AH	Authentication Header
AP	Access Point
APSD	Automatic Power Save Delivery
ARP	Address Resolution Protocol
AUTH	Authentication
CPU	Central Processing Unit
CRM	Customer Relationship Management
DDNS	Dynamic Domain Name Service
DDoS	Distributed Denial of Service
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone
DNS	Domain Name System
DPD	Dead Peer Detection
ERP	Enterprise Resource Planning
ESP	Encapsulating Security Payload
FQDN	Fully Qualified Domain Name
FTP	File Transfer Protocol
GI	Guard Interval
HQ	Headquarters
HTTP	Hypertext Transfer Protocol
ICMP	Internet Control Message Protocol

Acronym and Abbreviation	Full Spelling
IKE	Internet Key Exchange
IP	Internet Protocol
IPSec	Internet Protocol Security
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
ISAKMP	Internet Security Association Key Management Protocol
ISP	Internet Service Provider
L2TP	Layer 2 Tunneling Protocol
LAN	Local Area Network
MAC	Medium Access Control
MD5	Message Digest Algorithm
MGMT	Management
MTU	Maximum Transmission Unit
MUMIMO	Multi-User Multiple-Input Multiple-Output
NAT	Network Address Translation
NTS	Network Time Server
OA	Office Automation
OFDMA	Orthogonal Frequency Division Multiple Access
PFS	Perfect Forward Secrecy
PMF	Protected Management Frames
POP	Post Office Protocol
PPP	Point to Point Protocol
PPPoE	Point to Point Protocol over Ethernet
PPTP	Point to Point Tunneling Protocol
PST	Pacific Standard Time
RSSI	Received Signal Strength Indicator
SA	Security Association
SAE	Simultaneous Authentication of Equals

Acronym and Abbreviation	Full Spelling
SKEME	Security Key Exchange Mechanism
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
SPI	Security Parameter Index
SSID	Service Set Identifier
SSL	Secure Sockets Layer
SYN	Synchronize Sequence Numbers
SYS	System
TCP	Transmission Control Protocol
TWT	Target Wake Time
UDP	User Datagram Protocol
UI	User Interface
UPnP	Universal Plug and Play
URL	Uniform Resource Locator
USB	Universal Serial Bus
VPN	Virtual Private Network
WAN	Wide Area Network
WMM	Wi-Fi Multi-Media
WPA	Wi-Fi Protected Access
WPA-PSK	WPA-Preshared Key