User Guide

AC1200 Dual Band Gigabit Enterprise Wireless Router

W18E

www.tendacn.com

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.

Preface

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

This user guide walks you through all functions on the AC1200 Dual Band Gigabit Enterprise Wireless Router. The contained images and UI screenshots are subject to the actual products.

Conventions

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

If you want to get more documents of the device, visit www.tendacn.com and search for the corresponding product model.

Technical support

Contact us if you need more help. We will be glad to assist you as soon as possible.

Email address: support@tenda.cn

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	2023-10-25	Original publication.

Contents

1 Login and logout 1

1.1 Log in to the web UI 1

1.1.1 Log in with your computer 1

1.1.2 Log in with your smartphone 3

1.2 Logout 5

2 Web UI 6

2.1 Web UI layout 6

2.2 Frequently-used buttons 7

3 System status 8

3.1 View network status 8

3.1.1 View network connection status 8

3.1.2 View router (cable-free primary node) information 9

3.1.3 View secondary router (cable-free secondary node) information 10

3.2 View interfance information 13

3.3 View WAN real-time rate 14

3.4 View WAN connection status 15

3.5 Manage terminal devices 17

3.5.1 Overview 17

3.5.2 Control bandwidth of terminal devices 17

3.5.3 Add terminal devices to blacklist 18

3.5.4 Remove devices from blacklist 18

3.6 View traffic statistics 20

4 Internet settings 21

4.1 Internet Settings 21

4.1.1 Overview 21

4.1.2 Configure WAN ports 21

4.1.3 Set up for internet access 23

4.2 LAN settings 29
4.2.1 View LAN port status 29
4.2.2 Modify LAN IP address of the router 29
4.2.3 Modify DHCP server 30
4.3 DHCP reservation 32
5 Wireless 34
5.1 Wireless settings 34
5.2 Guest network 36
5.3 MAC filters 38
5.3.1 Overview 38
5.3.2 Configure a MAC filter rule 39
5.3.3 Example of configuring MAC filters rule 40
5.4 Advanced settings 43
6 Bandwidth Limit 46
6.1 WAN bandwidth 46
6.2 Group limit 47
6.3 Example of configuring group limit 49
7 Behavior 51
7.1 Group policy 51
7.1.1 Time group 51
7.1.2 IP group 53
7.2 Filtering 54
7.2.1 IP address filtering 54
7.2.2 MAC address filtering 58
7.3 Port filtering 62
7.3.1 Overview 62
7.3.2 Example of configuring a port filtering policy 63
7.4 URL filtering 66
7.4.1 Overview 66
7.4.2 Example of configuring a URL filter rule 67
8 More settings 70

8.1 Advanced routing 70
8.1.1 WAN parameters 70
8.1.2 Multi-WAN policy 72
8.1.3 Static routing 75
8.1.4 Routing table 81
8.1.5 Policy routing 82
8.2 Virtual service 86
8.2.1 DMZ 86
8.2.2 DDNS 90
8.2.3 DNS hijacking 96
8.2.4 IP hijacking 98
8.2.5 UPnP 100
8.2.6 Port mapping 101
8.3 Maintenance service 106
8.3.1 Remote web management 106
8.3.2 Security settings 109
8.4 VPN 110
8.4.1 Overview 110
8.4.2 VPN client 111
8.4.3 IPSec 114
8.5 IPv6 128
8.5.1 Overview 128
8.5.2 Internet 129
8.5.3 LAN 133
9 System maintenance 135
9.1 System time 135
9.1.1 Sync time with network time 135
9.1.2 Set system time manually 136
9.2 Diagnostic tool 137
9.2.1 Ping 137
9.2.2 Tracert 138

9.2.3 Packet capture tool 139
9.2.4 System diagnosis 142
9.2.5 Interface info 142
9.3 Log center 144
9.3.1 System log 144
9.3.2 Operating log 144
9.3.3 Running log 145
9.4 System maintenance 146
9.4.1 Device info 146
9.4.2 Restore & Backup 147
9.4.3 Factory settings restore 148
9.5 Upgrade service 150
9.5.1 Overview 150
9.5.2 System firmware upgrade 150
9.5.3 Feature-Library upgrade 151
9.6 Reboot devices 153
9.6.1 Reboot 153
9.6.2 Scheduled reboot 153
9.7 System account 155
9.8 Test 157
Appendix 158
Acronyms and Abbreviations 158

1 Login and logout

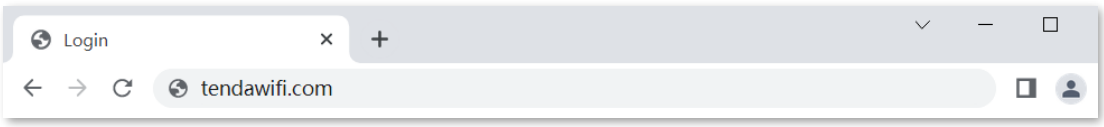
1.1 Log in to the web UI

If you use this router for the first time or have reset it to factory settings, refer to the quick installation guide (visit www.tendacn.com to download) 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, or connect your computer to the wireless network of the router.

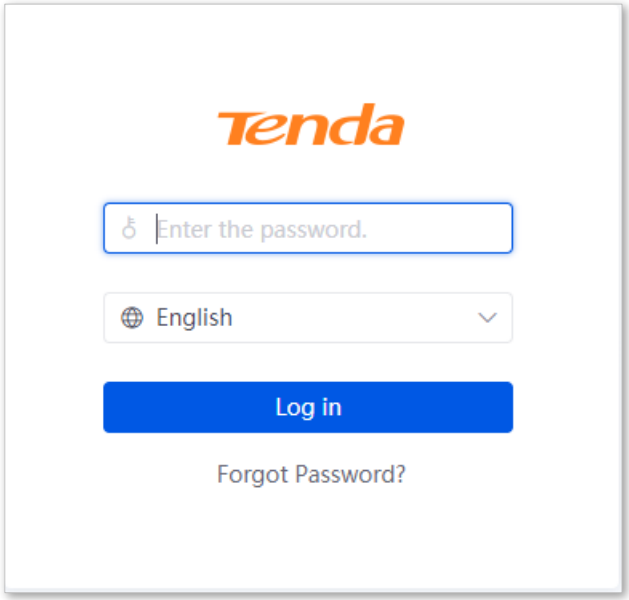
Step 2 Start a browser on the computer and enter **tendawifi.com** in the address bar to access the web UI.



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

TIP

- By default, the WiFi password is set as the login password automatically. Thus, if you forget the login password, try to use the WiFi password.
- If the problem persists, reset the router to factory settings and then set the login password. After resetting, you need to connect the router to the internet again.



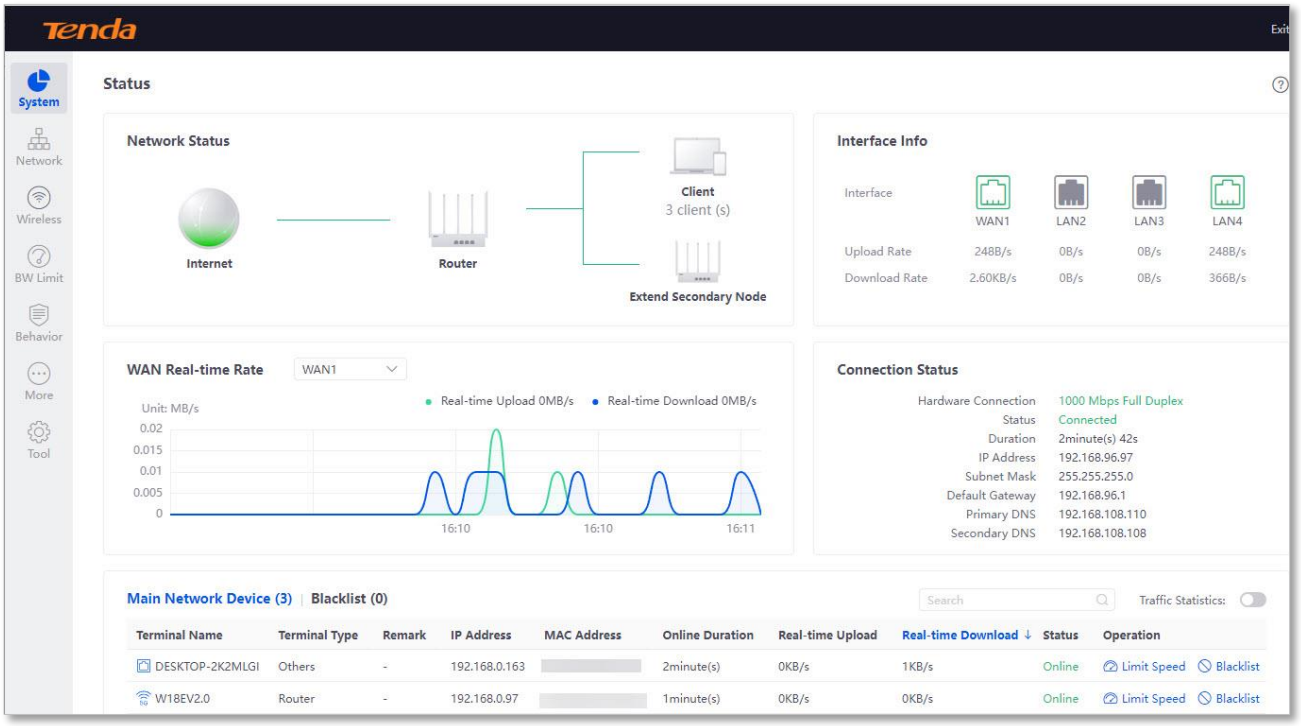
----End

TIP

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

- Ensure that the router is powered on.
- Ensure that the Ethernet port of the router is connected to the computer correctly and securely.
- Ensure that your computer has been set to **Obtain an IP address automatically** and **Obtain DNS server address automatically**.
- Reset the router to factory settings, and log in again. After resetting, you need to connect the router to the internet again.

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



1.1.2 Log in with your smartphone

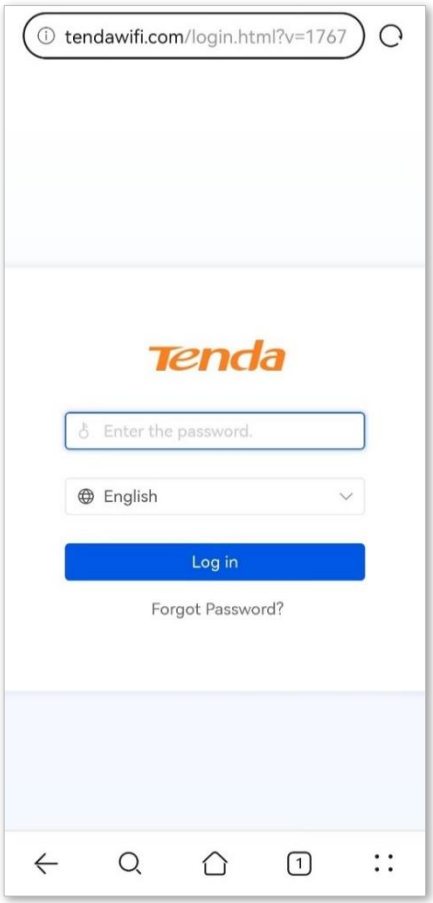
Step 1 Connect your smartphone to the WiFi network of the router.

Step 2 Start the browser on the smartphone and enter **tendawifi.com** in the address bar (not searching bar) to access the web UI.

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

TIP

- By default, the WiFi password is set as the login password automatically. Thus, if you forget the login password, try to use the WiFi password.
- If the problem persists, reset the router to factory settings and then set the login password. After resetting, you need to connect the router to the internet again.



----End

TIP

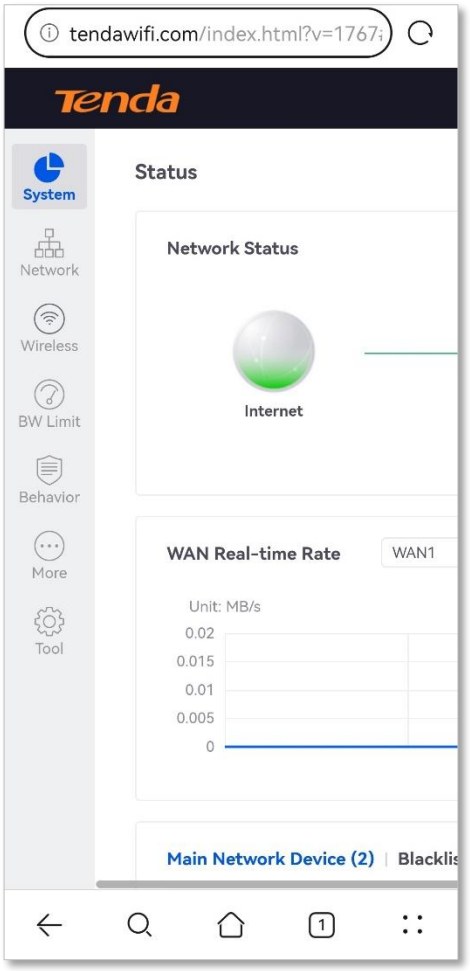
If the above page does not appear, try the following solutions:

- Ensure that the router is powered on properly.
- Ensure that your smartphone is connected to the wireless network of the router.
- Ensure that the mobile data is disabled.
- Reset the router to factory settings, and log in again. After resetting, you need to connect the router to the internet again.

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

TIP

Please scale the page to fit the screen size.



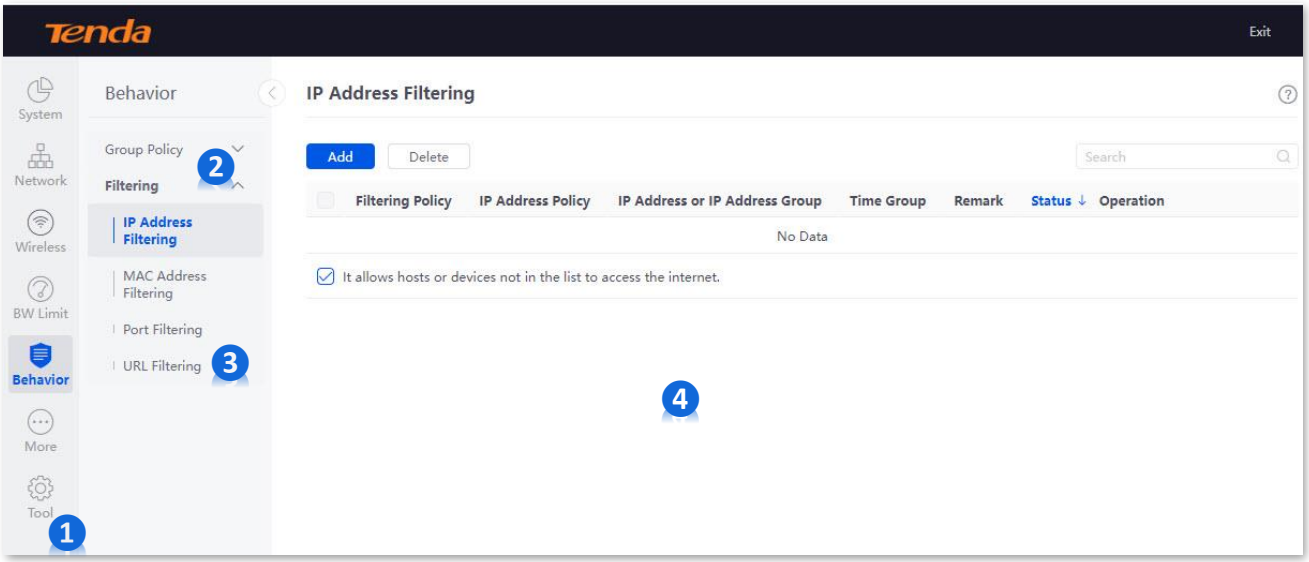
1.2 Logout

If you log in to the web UI of the router and perform no operation within the Login Timeout, the router logs you out automatically. You can also log out by clicking **Exit** at the upper right corner of the web UI

2 Web UI

2.1 Web UI layout

The web UI of the router consists of three sections, including the level-1, level-2, level-3 navigation bar, and configuration area. See the following figure:



TIP

Features or parameters displayed in gray are not available or cannot be configured 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	Level-3 navigation bar	
4	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.
Save	Used to save the configuration on the current page and enable the configuration to take effect.
Delete	Used to delete the selected rule or policy.
Cancel	Used to change the current configuration on the current page back to the original configuration.
Edit	Used to edit corresponding rules, policies or information.
	Used to view help information for the current page.

3 System status

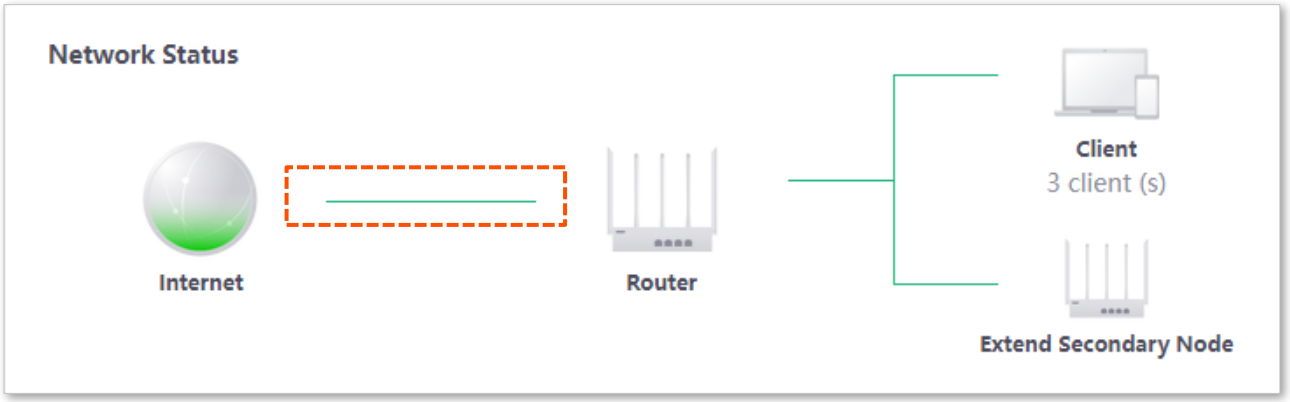
3.1 View network status

To access the configuration page, log in to the web UI of the router, and navigate to **System** to enter the page.

In the **Network Status** module, you can check if the WAN port network status is proper, and view basic information about the router and the secondary node.

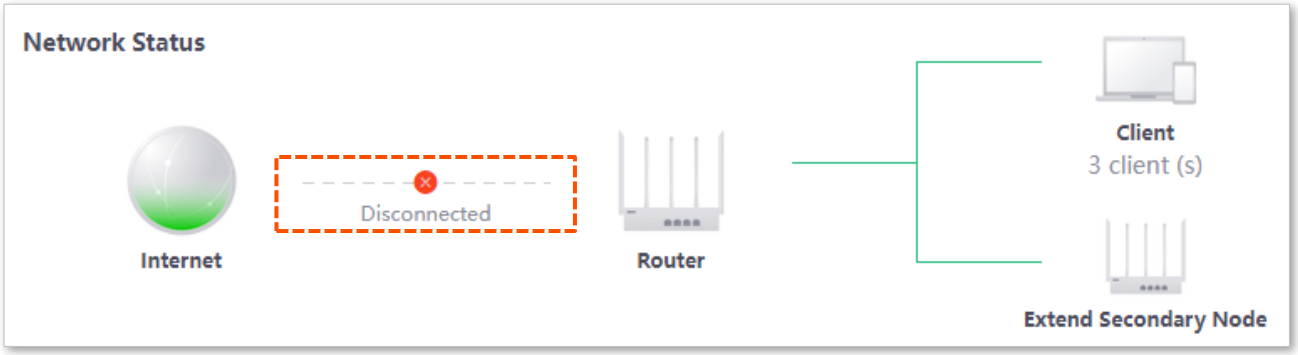
3.1.1 View network connection status

When the link between the **Internet** and the **Router** is clear as shown below, the router is connected to the internet properly.



When a red cross and "**Disconnected**" are shown between the **Internet** and the **Router**, the router is disconnected from the internet. Check whether the Ethernet cable is connected properly.

You can click the line between **Internet** and **Router** to redirect to the Internet Settings to check the internet configuration.



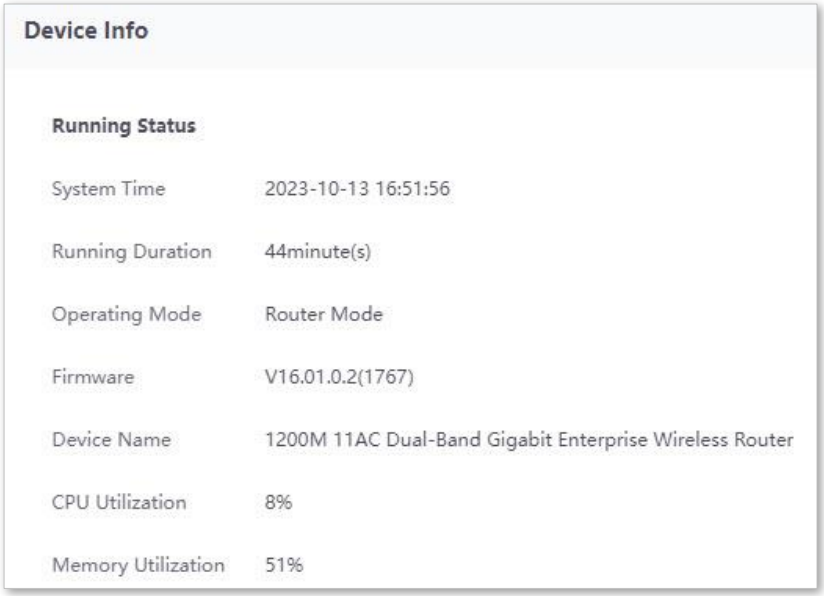
3.1.2 View router (cable-free primary node) information

To access the configuration page, log in to the web UI of the router, and navigate to **System** to enter the page.

In the **Network Status** module, click the **Router** icon, and view Running Status and WiFi Status of the router.

View running status

In the **Running Status** module, you can view such information as system time, running duration, operating mode and firmware about the router.



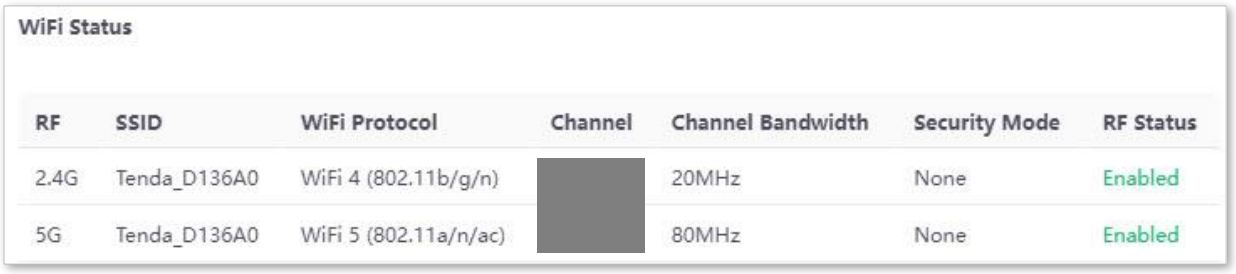
Parameter description

Parameter	Description
System Time	Specifies the current system time of the router.
Running Duration	Specifies the duration of continuous running since the router was last started.
Operating Mode	Specifies the current operating mode. - **Router Mode**: As the primary node of the cable-free network, it is connected to the wired network and is the only outlet in the cable-free network to access the external network, realizing data conversion between the cable-free network and the wired network. - **Extender Mode**: As the secondary node of the cable-free network, it expands the coverage of the existing cable-free network through the cable-free self-organizing network.
Firmware	Specifies the firmware version number of the router.
Device Name	Specifies the name of the router.

Parameter	Description
CPU Utilization	Specifies the current CPU usage of the router.
Memory Utilization	Specifies the current memory usage of the router.

View WiFi status

In the **WiFi Status** module, you can view the WiFi status of the router.



Parameter description

Parameter	Description
RF	Specifies the operating frequency of the router.
SSID	Specifies the WiFi network name of the router.
WiFi Protocol	Specifies the WiFi network protocol of the router.
Channel	Specifies the channel for wireless data transmission of the router.
Channel Bandwidth	Specifies the channel bandwidth of the wireless channel of the router.
Security Mode	Specifies the encryption mode of the WiFi network.
RF Status	Specifies whether the WiFi function of the router is enabled.

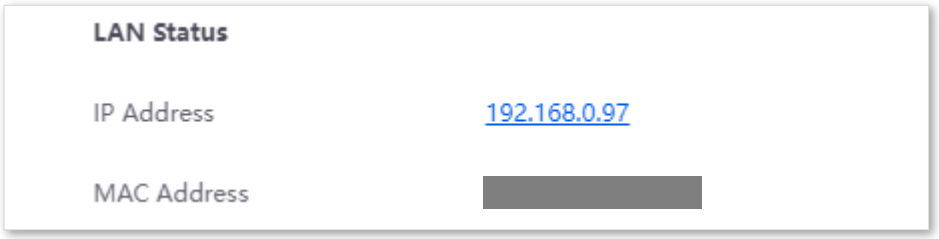
3.1.3 View secondary router (cable-free secondary node) information

To access the configuration page, log in to the web UI of the router, and navigate to **System** to enter the page.

In the **Network Status** module, you can click the **Extend Secondary Node** icon, and view Running Status, LAN Status and Link Quality of the router.

View LAN status

In the **LAN Status** module, you can view the LAN IP address and the MAC address of the secondary node.

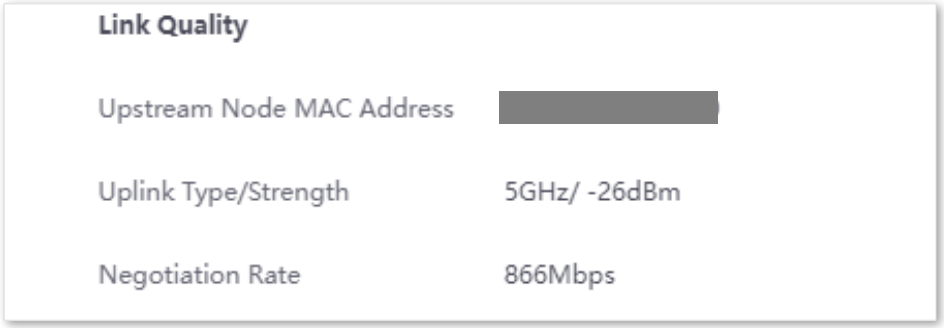


Parameter description

Parameter	Description
IP Address	Specifies the LAN IP address of the secondary node and also the management IP address of the secondary node, LAN users can use this IP address to log in to the web UI of the secondary node, the login password for the secondary node is the same as that of the primary node. TIP The IP address of the secondary node is automatically obtained from the DHCP server of the primary node.
MAC Address	Specifies the MAC address of the secondary node.

View link quality

In the **Link Quality** module, you can view the link information between the secondary node and the upstream node.



Parameter description

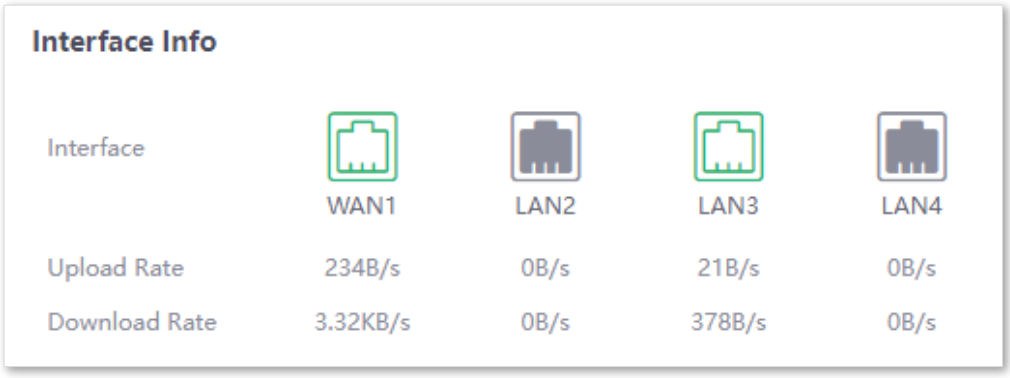
Parameter	Description
Upstream Node MAC Address	Specifies the MAC address of the upstream node used to form the Mesh link.
Uplink Type/Strength	Specifies the networking mode between this node and the upstream node, and the signal strength of the upstream node received by this node.

Parameter	Description
Negotiation Rate	Specifies the current negotiation rate between this node and the upstream node.

3.2 View interfance information

To access the configuration page, log in to the web UI of the router, and navigate to **System** to enter the page.

In the **Interface Info** module, you can view the roles, physical connection status, upload rate and download rate of each port of the router.



Parameter description

Parameter	Description
Interface	Specifies the roles and physical connection status of all ports of the router. - Green means connected. - Grey means disconnected.
Upload Rate	Specify the current upload and download rates of the router.
Download Rate	

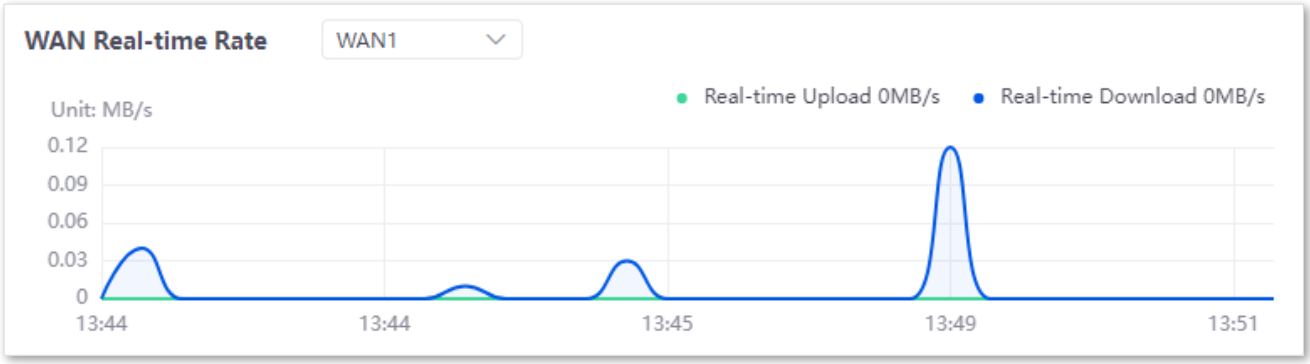
3.3 View WAN real-time rate

To access the configuration page, log in to the web UI of the router, and navigate to **System** to enter the page.

In the **WAN Real-time Rate** module, you can view the upload and download rates of a WAN port of the router.

TIP

If you set multiple WAN ports, click the drop-down box of the **WAN Real-time Rate** to select a certain WAN port of the router.



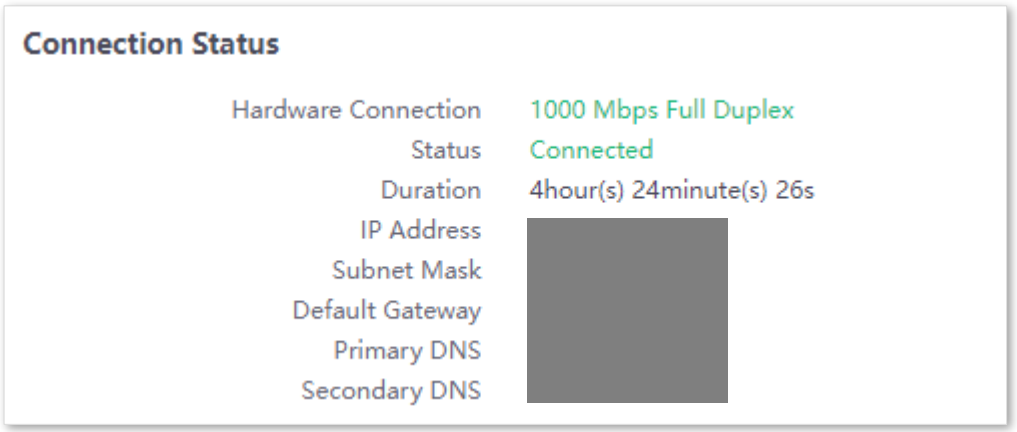
3.4 View WAN connection status

To access the configuration page, log in to the web UI of the router, and navigate to **System** to enter the page.

In the **Connection Status** module, you can view the network status of the corresponding WAN port IPv4, including the Ethernet port connection rate and duplex mode, connection status, duration and IP address.

TIP

If you set multiple WAN ports, click the drop-down box of the **WAN Real-time Rate** to select a certain WAN port of the router.



Parameter description

Parameter	Description
Hardware Connection	Specifies the negotiation rate and duplex mode of the WAN port. If the display is abnormal, you can troubleshoot based on the information on the page and the current environment.
Status	Specifies the connection status of the WAN port of the router. - **Connected**: The WAN port of the router has been plugged into the Ethernet cable, and the IPv4 address information has been obtained. - **Connecting...**: The router is connecting to the upstream network device. - **Disconnected**: If it is not connected or fails to connect, check the Ethernet cable connection status and internet settings, or consult the corresponding ISP. If other status information is displayed, take corresponding measures according to the network status prompt information.
Duration	Specifies the latest duration of the WAN port access to the IPv4 network.
IP Address	Specifies the IPv4 address of the WAN port.

Parameter	Description
Subnet Mask	Specifies the subnet mask of the WAN port.
Default Gateway	Specifies the IPv4 gateway address of the WAN port.
Primary DNS	Specify the primary/secondary DNS server address of the WAN port.
Secondary DNS	

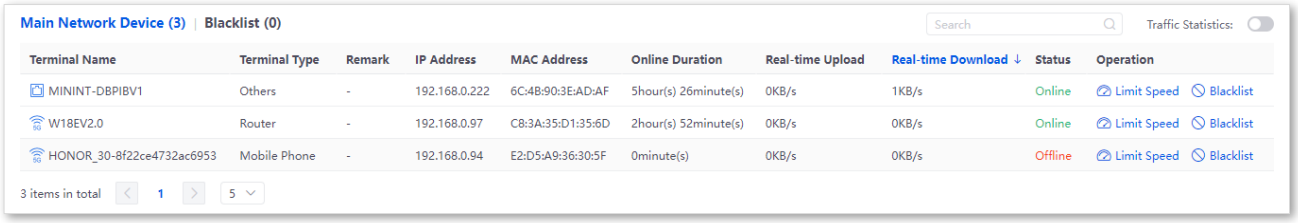
3.5 Manage terminal devices

3.5.1 Overview

To access the configuration page, log in to the web UI of the router, and navigate to **System** to enter the page.

In the **Main Network Device** module, you can view and manage the users connected to the router.

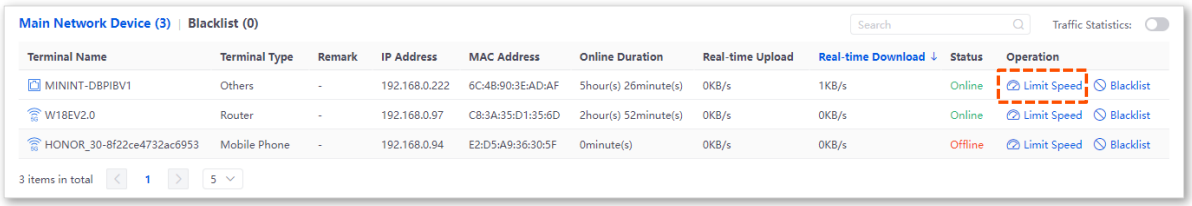
When you view or manage users, you can enter the terminal name, IP address, MAC address in the search bar to quickly filter user information.



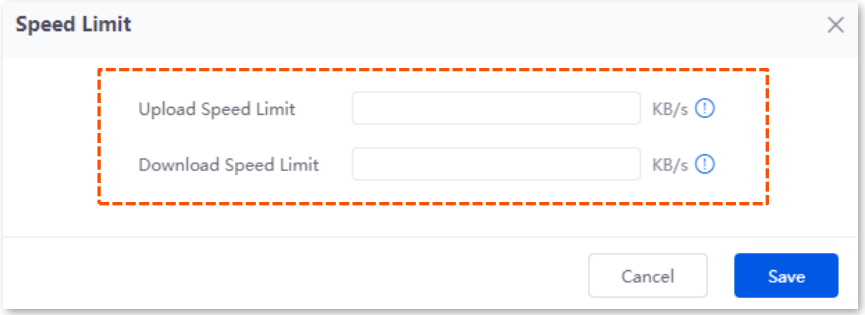
3.5.2 Control bandwidth of terminal devices

Step 1 Log in to the web UI of the router.

Step 2 Navigate to **System**. locate the devices as required on the **Main Network Device** module, and click **Limit Speed**.



Step 3 Set **Upload Speed Limit** and **Download Speed Limit**, and then click **Save**.



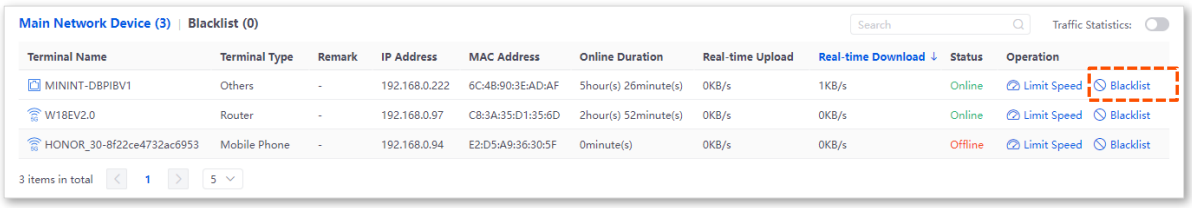
----End

3.5.3 Add terminal devices to blacklist

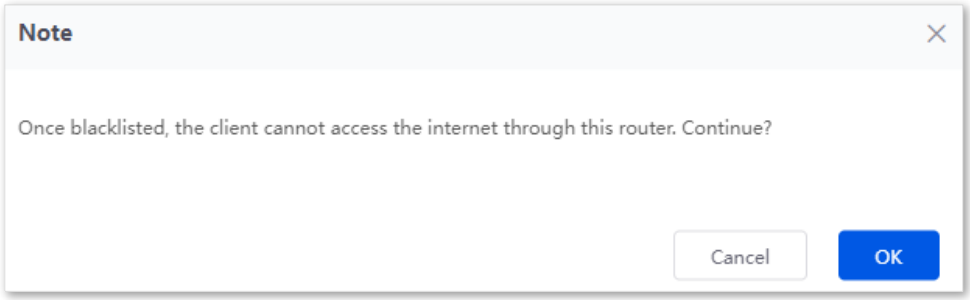
The blocked devices will be moved to the **Blacklist**, and cannot connect to your router.

Step 1 Log in to the web UI of the router.

Step 2 Navigate to **System**. Locate the devices as required on the **Main Network Device** module, and click **Blacklist**.

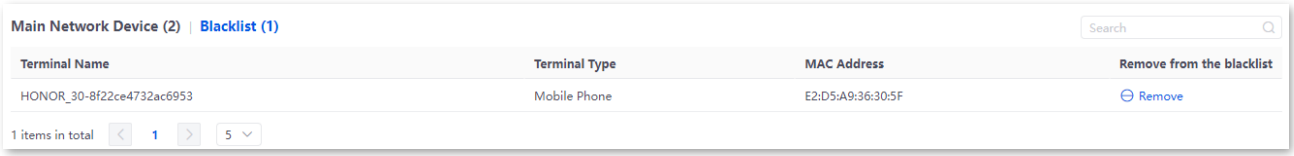


Step 3 Confirm the prompt information, and click **OK**.



----End

You can view the blocked devices on the **Blacklist** page.

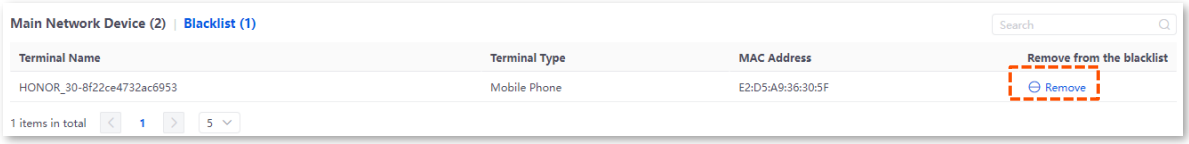


3.5.4 Remove devices from blacklist

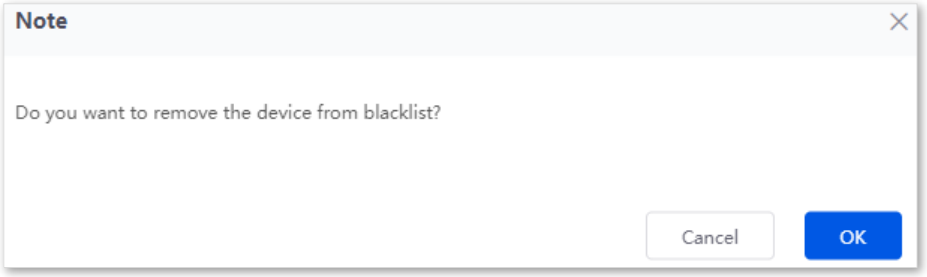
The unblocked devices can connect to your router again.

Step 1 Log in to the web UI of the router.

Step 2 Navigate to **System.** Locate the devices as required on the **Blacklist** module, and click **Remove**.



Step 3 Confirm the prompt information, and click **OK**.


Note
Do you want to remove the device from blacklist?
Cancel
OK

----End

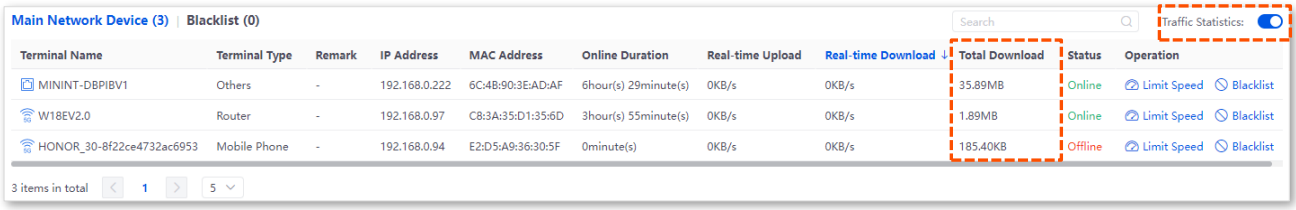
3.6 View traffic statistics

NOTE

The **Traffic Statistics** function is disabled by default. It may affect router performance after you enable it.

To access the configuration page, log in to the web UI of the router, and navigate to **System** to enter the page.

In the **Main Network Device** module, you can view the total download statistics of each terminal devices after the **Traffic Statistics** function is enabled. The function is disabled by default. When it is enabled, the page is shown as below.



4 Internet settings

4.1 Internet Settings

4.1.1 Overview

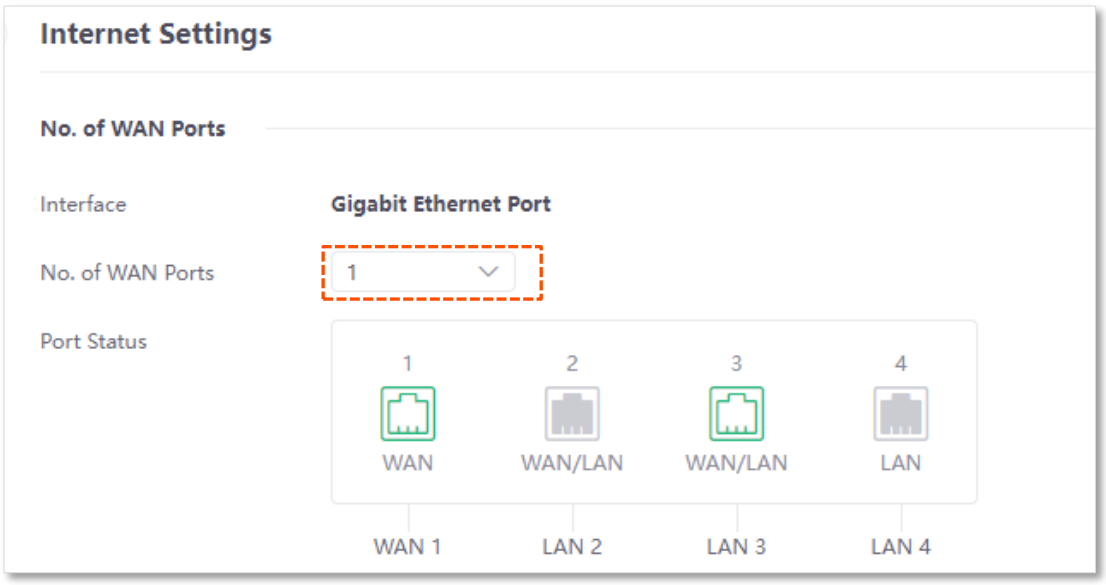
To access the configuration page, log in to the web UI of the router, and navigate to **Network** > **Internet Settings** to enter the page.

Here, you can configure or change the internet settings to enable the device to access the internet.

If you use this router for the first time or have reset it to factory settings, refer to the quick installation guide (visit www.tendacn.com to download) to complete the setup wizard. After that, you can change internet settings or set up more parameters here.

4.1.2 Configure WAN ports

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.



Parameter description

Parameter	Description
Interface	Specifies the rate type of the WAN port on the router.

Parameter	Description
No. of WAN Ports	Specifies the number of WAN ports. By default, the router has only one WAN port (the WAN1 port), and you can set **3** WAN ports at most.
Port Status	Specifies the port type and the connection status.  : The port is connected properly. : The port is disconnected or improperly connected.

4.1.3 Set up for internet access

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

Choose the proper ISP type and connection type according to your actual environment. All internet parameters for accessing the internet are provided by your ISP. If you are not clear, consult your ISP.

PPPoE, Dynamic IP Address and Static IP Address are used for illustration here.

TIP

WAN1 is used as an example here, and configurations for other WAN ports are similar.

PPPoE

If your ISP provides no setup information, except for the PPPoE user name and password, you can choose this connection type to access the internet.

Step 1 Log in to the web UI of the router.

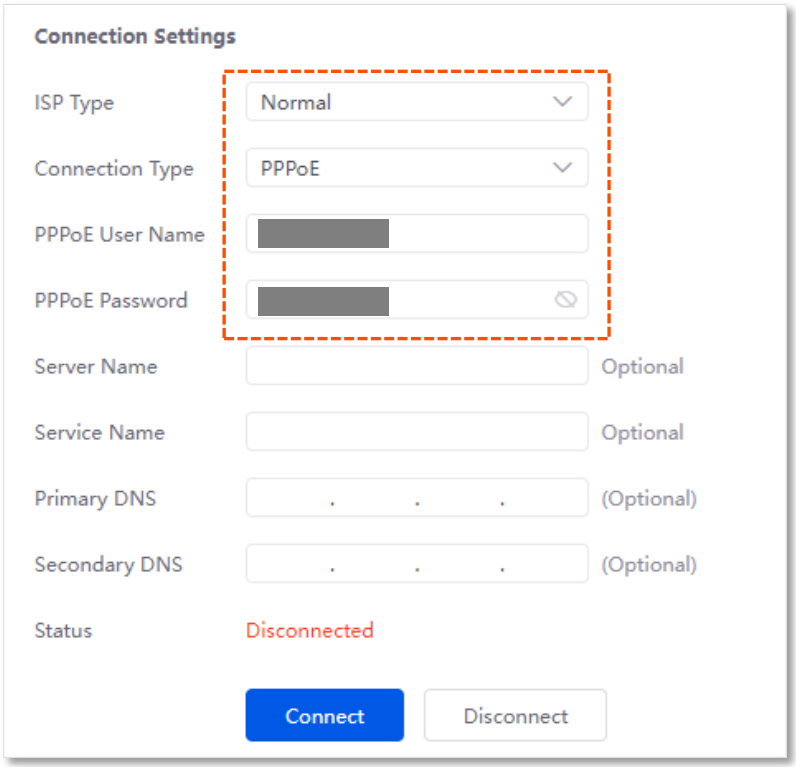
Step 2 Navigate to **Network** > **Internet Settings**.

Step 3 Set the **ISP Type**, which is **Normal** in this example.

Step 4 Set **Connection Type** to **PPPoE**.

Step 5 Enter the **PPPoE User name** and **PPPoE Password** provided by your ISP.

Step 6 Click **Connect**.



----End

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

Parameter description

Parameter	Description
ISP Type	Specifies the type of your ISP, such as **Normal**, **Russia**, **Unifi**, **Maxis** and **Manual**. Parameters required for each option may differ. Refer to the following to choose your connection type: - **Normal**, **Unifi** and **Maxis**: Select these options when your ISP provides no setup information, except for the PPPoE user name and password, or static IP address information. - **Russia:** Select this option when your ISP provides dual access information, such as PPTP, L2TP connection information. - **Manual**: Select this option when your ISP provides VLAN ID information, besides the PPPoE user name and account, or static IP address. If you are still not sure, contact your ISP for help.
Connection Type	Specifies in which way the router is connected to the internet. - **PPPoE**, **Russia PPPoE**: Select this type if you access the internet using the PPPoE account and PPPoE password. **Russia PPPoE** is available only when you set **ISP Type** to **Russia**. - **Dynamic IP Address**: Select this type if you can access the internet by simply plugging in an Ethernet cable. - **Static IP Address**: Select this type if you want to access the internet using fixed IP information.
PPPoE User name	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	
Primary DNS	Manually enter primary or secondary DNS servers. When the DNS server obtained automatically cannot resolve the URL normally, you can manually enter a correct primary or secondary DNS server here. The **Primary DNS** and **Secondary DNS** are optional.
Secondary DNS	

Dynamic IP Address

If the ISP dynamically assigns you the IP address information, you can choose this connection type to access the internet.

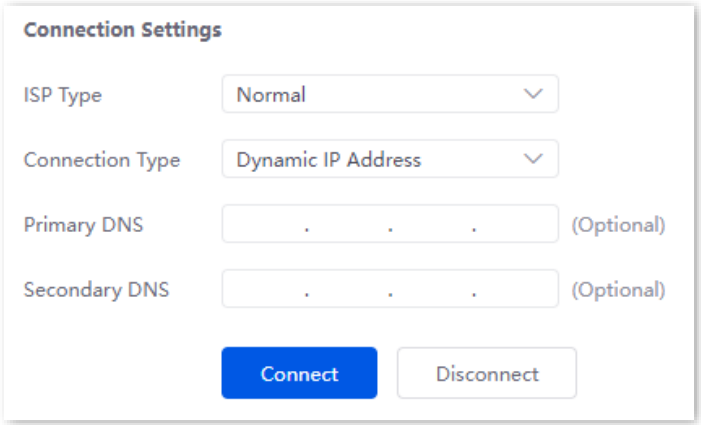
Step 1 Log in to the web UI of the router.

Step 2 Navigate to **Network** > **Internet Settings**.

Step 3 Set the **ISP Type**, which is **Normal** in this example.

Step 4 Set **Connection Type** to **Dynamic IP Address.**

Step 5 Click **Connect**.



----End

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

Parameter description

Parameter	Description
ISP Type	Specifies the type of your ISP, such as **Normal**, **Russia**, **Unifi**, **Maxis** and **Manual**. Parameters required for each option may differ. Refer to the following to choose your connection type: - **Normal**, **Unifi** and **Maxis**: Select these options when your ISP provides no setup information, except for the PPPoE user name and password, or static IP address information. - **Russia:** Select this option when your ISP provides dual access information, such as PPTP, L2TP connection information. - **Manual**: Select this option when your ISP provides VLAN ID information, besides the PPPoE user name and account, or static IP address. If you are still not sure, contact your ISP for help. TIP **Unifi** and **Maxis** are ISPs of Malaysia, only applicable when you choose the ISPs. **Russia** is only applicable to Russia and its vicinity.

Parameter	Description
Connection Type	Specifies in which way the router is connected to the internet. - **PPPoE**, **Russia PPPoE**: Select this type if you access the internet using the PPPoE account and PPPoE password. **Russia PPPoE** is available only when you set **ISP Type** to **Russia**. - **Dynamic IP Address**: Select this type if you can access the internet by simply plugging in an Ethernet cable. - **Static IP Address**: Select this type if you want to access the internet using fixed IP information.
Primary DNS	Manually enter primary or secondary DNS servers. When the DNS server obtained automatically cannot resolve the URL normally, you can manually enter a correct primary or secondary DNS server here. The **Primary DNS** and **Secondary DNS** are optional.
Secondary DNS	

Static IP Address

If your ISP provides no setup information, except for the fixed IP address, subnet mask, default gateway and DNS server information, you can choose this connection type to access the internet.

Step 1 Log in to the web UI of the router.

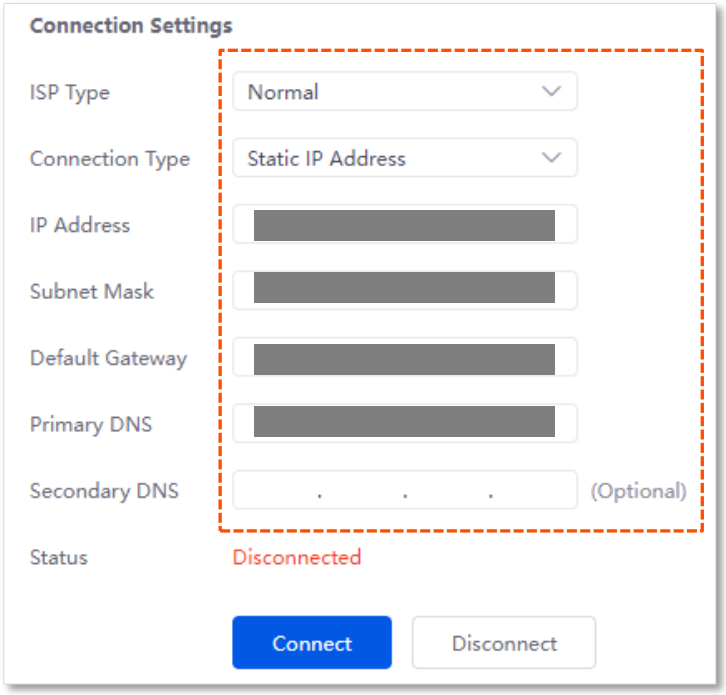
Step 2 Navigate to **Network** > **Internet Settings**.

Step 3 Set the **ISP Type**, which is **Normal** in this example.

Step 4 Set **Connection Type** to **Static IP Address.**

Step 5 Enter the **IP Address**, **Subnet Mask**, **Default Gateway and Primary/Secondary DNS** provided by your ISP.

Step 6 Click **Connect**.



----End

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

Parameter description

Parameter	Description
ISP Type	Specifies the type of your ISP, such as **Normal**, **Russia**, **Unifi**, **Maxis** and **Manual**. Parameters required for each option may differ. Refer to the following to choose your connection type: - **Normal**, **Unifi** and **Maxis**: Select these options when your ISP provides no setup information, except for the PPPoE user name and password, or static IP address information. - **Russia:** Select this option when your ISP provides dual access information, such as PPTP, L2TP connection information.

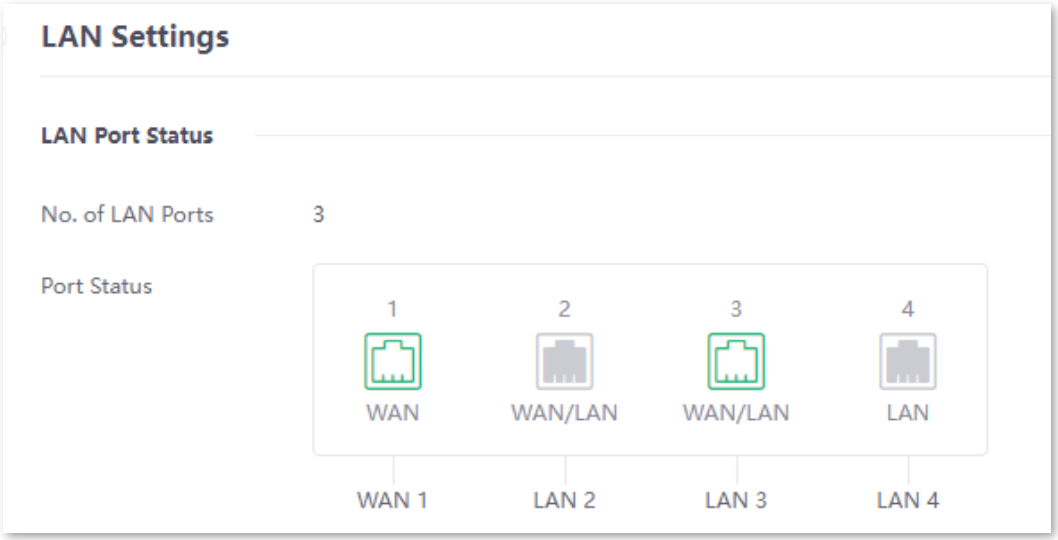
Parameter	Description
	- **Manual**: Select this option when your ISP provides VLAN ID information, besides the PPPoE user name and account, or static IP address. If you are still not sure, contact your ISP for help.  **Unifi** and **Maxis** are ISPs of Malaysia, only applicable when you choose the ISPs. **Russia** is only applicable to Russia and its vicinity.
Connection Type	Specifies in which way the router is connected to the internet. - **PPPoE**, **Russia PPPoE**: Select this type if you access the internet using the PPPoE account and PPPoE password. **Russia PPPoE** is available only when you set **ISP Type** to **Russia**. - **Dynamic IP Address**: Select this type if you can access the internet by simply plugging in an Ethernet cable. - **Static IP Address**: Select this type if you want to access the internet using fixed IP information.
IP Address	Enter the **IP Address**, **Subnet Mask**, **Default Gateway**, **Primary DNS** and **Secondary DNS** provided by the ISP.  If the ISP only provides one DNS address, the **Secondary DNS** is not required.
Subnet Mask	
Default Gateway	
Primary DNS	
Secondary DNS	

4.2 LAN settings

4.2.1 View LAN port status

To access the configuration page, log in to the web UI of the router, and navigate to **Network** > **LAN Settings** to enter the page.

In the **LAN Port Status** module, you can view the number of LAN ports, the port type and the connection status of the router.



Parameter description

Parameter	Description
No. of LAN Ports	Specifies the number of LAN ports.
Port Status	Specifies the roles and physical connection status of all ports of the router. - Green means connected. - Grey means disconnected.

4.2.2 Modify LAN IP address of the router

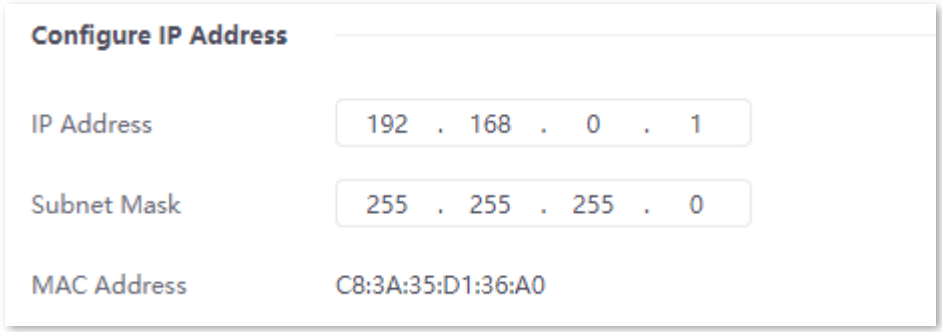
To access the configuration page, log in to the web UI of the router, and navigate to **Network** > **LAN Settings** to enter the page.

In the **Configure IP Address** module, you can view and modify the LAN information 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**.

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 router's LAN IP address. If the IP address of other network management devices on the LAN needs to be set to 192.168.0.*X*, you can modify this router's LAN IP address to be on different network segments from 192.168.0.

TIP

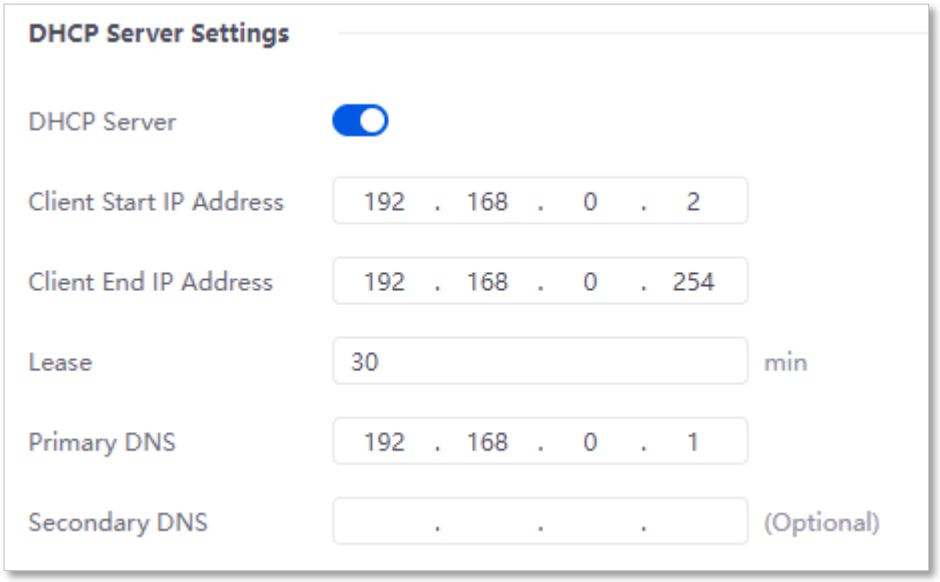
If the network segment of the new LAN IP address is different from the original one, the system automatically modifies the DHCP server to make it on the same network segment as the new LAN IP address.

4.2.3 Modify DHCP server

To access the configuration page, log in to the web UI of the router, and navigate to **Network** > **LAN Settings** to enter the page.

In the **DHCP Server Settings** module, you can modify DHCP server settings.

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. You are recommended to enable this function.



Parameter description

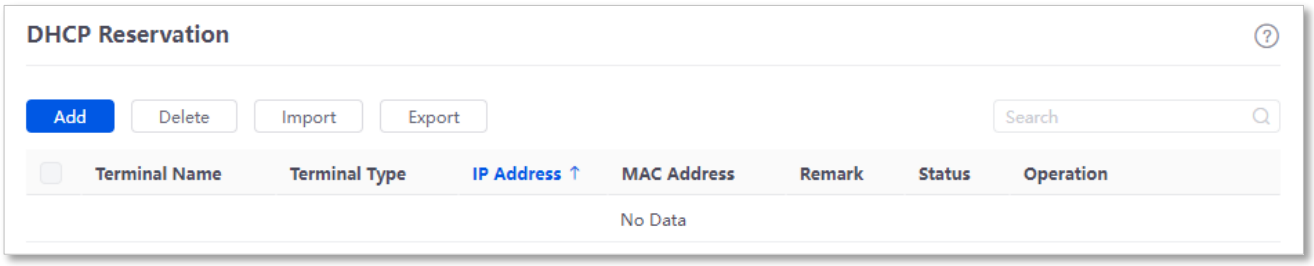
Parameter	Description
DHCP Server	Used to enable or disable the DHCP server function.
Client Start IP Address	Specifies the range of IP addresses that the DHCP server can assign to a LAN device. The start IP address is 192.168.0.2 and the end IP address is 192.168.0.254 by default.
Client End IP Address	
Lease	Specifies the validity period of the IP address assigned by the DHCP server to LAN devices. By default, the default value 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 request IP address information, the router can assign this IP address to other devices. You are recommended to keep the default settings.
Primary DNS	Specifies the primary DNS server IP address assigned by the DHCP server to LAN devices. This router supports DNS proxy function so that the primary DNS is the LAN IP address of the router by default. TIP Generally, you are recommended to keep the default settings. If it is necessary to change the default settings, set this parameter to a correct DNS server IP address or DNS proxy IP address, to enable connected devices to access the internet.
Secondary DNS	Specifies the secondary DNS server IP address assigned by the DHCP server to LAN devices. This parameter is optional. If it is empty, the DHCP server does not assign it to devices.

4.3 DHCP reservation

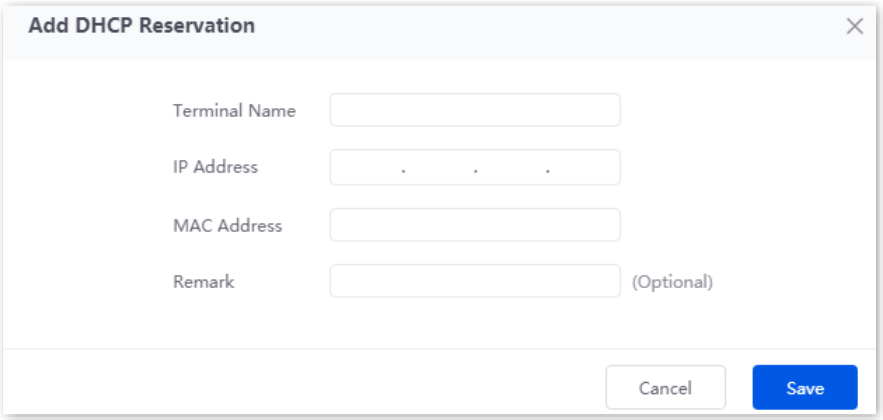
With the DHCP reservation function, you can make the specified client in the LAN always obtain the preset IP address, and avoid the functions such as **Internet Speed Control** and **Port Mapping** that take effect based on the IP address from becoming invalid due to the change of the client IP address.

To access the configuration page, log in to the web UI of the router, and navigate to **Network** > **DHCP Reservation** to enter the page.

Here, you can configure the DHCP static assignment rules and also import/export static IP address lists.



You can click **Add** to add a new DHCP reservation policy.



Parameter description

Parameter	Description
Terminal Name	Specifies the name of the terminal.
Terminal Type	Specifies the terminal types such as Mobile Phone, PAD and PC. If the terminal type is not recognized, **Others** will be displayed.
IP Address	Specifies the fixed IP address to be assigned to the terminal.
MAC Address	Specifies the MAC address of the terminal. A MAC address can be specified in the following format: 00:23:24:E8:14:5A, 00-23-24-E8-14-5A or 002324E8145A.

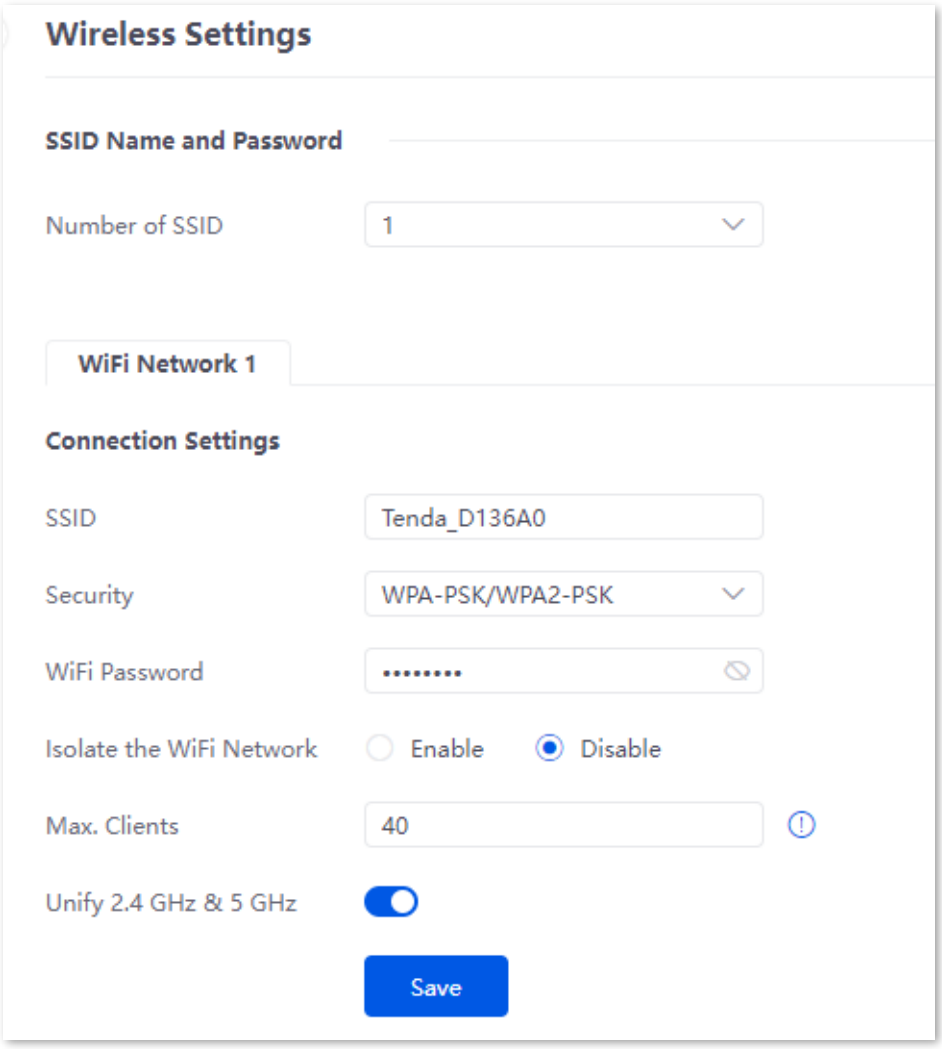
Parameter	Description
Remark	Specifies the description of the assigned static IP address.
Status	Specifies the status of the DHCP reservation, including **Enabled**, **Disabled** and **Expired**.
Delete	Used to delate the DHCP reservation policy.
Import	Used to import CSV files for adding DHCP static assignment rules.
Export	Used to export DHCP static assignment rules to your local computer as a CSV file. TIP To modify the exported file, open the file as a txt file.

5 Wireless

5.1 Wireless settings

To access the configuration page, log in to the web UI of the router, and navigate to **Wireless** > **Wireless Settings** to enter the page.

Here, you can set up WiFi network-related parameters, such as view and edit number of WiFi (SSID), WiFi names, WiFi passwords, configure 2.4 GHz and 5 GHz WiFi networks separately, and specify how many wireless clients can connect to a wireless network.



Parameter description

Parameter	Description
Number of SSID	Specifies the number of SSID. By default, the router has one SSID, and you can set **3** SSIDs at most.

Parameter	Description
SSID	Specifies the WiFi name of the corresponding WiFi network.
Security	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.
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.
Isolate the WiFi Network	Used to enable or disable the **Isolate the WiFi Network** function. After the function is enabled, users connected to the different WiFi network of the router cannot communicate with each other, which enhances the security of the WiFi network.
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.
Unify 2.4 GHz &5 GHz	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.

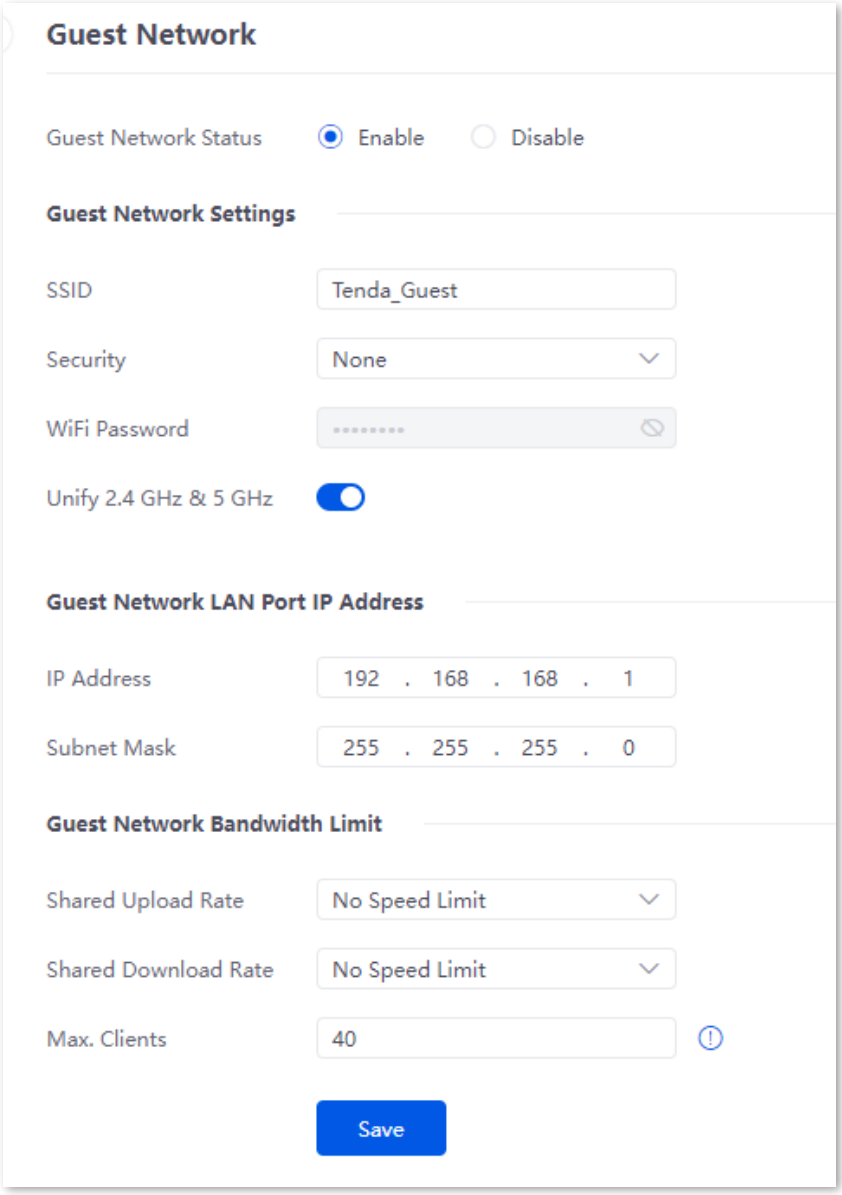
5.2 Guest network

To access the configuration page, log in to the web UI of the router, and navigate to **Wireless** > **Guest Network** to enter the page.

Here, you can configure the basic parameters of guest network, such as enable or 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.

This function is disabled by default. When it is enabled, the page is shown as below.



Parameter description

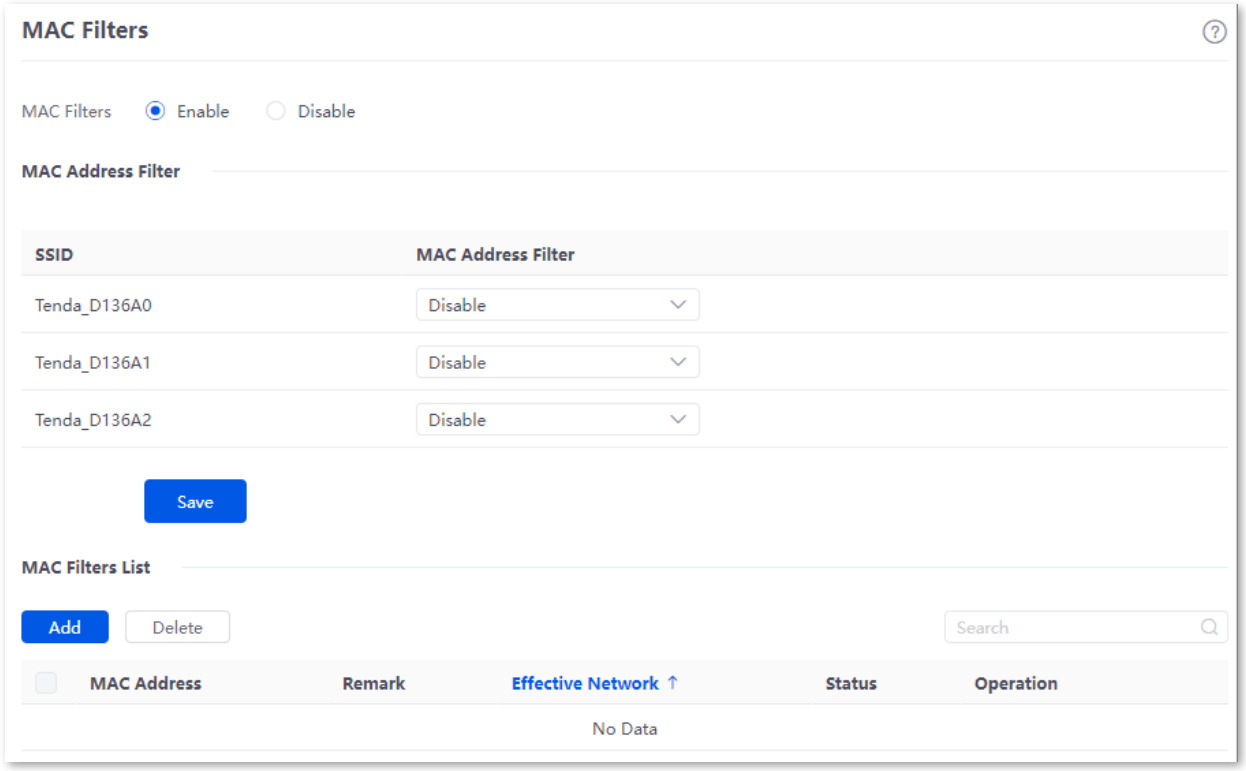
Parameter		Description
Guest Network Status		Used to enable or disable the guest network.
Guest Network Settings	SSID	Specifies the WiFi name of the guest network. TIP To differentiate the main network and the guest network, you are recommended to set the SSIDs differently.
	Security	Specifies the encryption types of the guest 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.
	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.
Guest Network LAN Port 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	Shared Upload Rate	Specify the uplink and downlink rate limits on guest network.
	Shared Download Rate	
	Max. Client	Specifies the maximum number of wireless devices allowed to connect to the guest network.

5.3 MAC filters

5.3.1 Overview

To access the configuration page, log in to the web UI of the router, and navigate to **Wireless** > **MAC Filters** to enter the page.

Here, you can configure MAC address-based wireless access control rules. By default, this function is disabled. When it is enabled, the page is shown as below.



Parameter description

Parameter		Description
MAC Filters		Used to enable or disable the MAC filters function.
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.

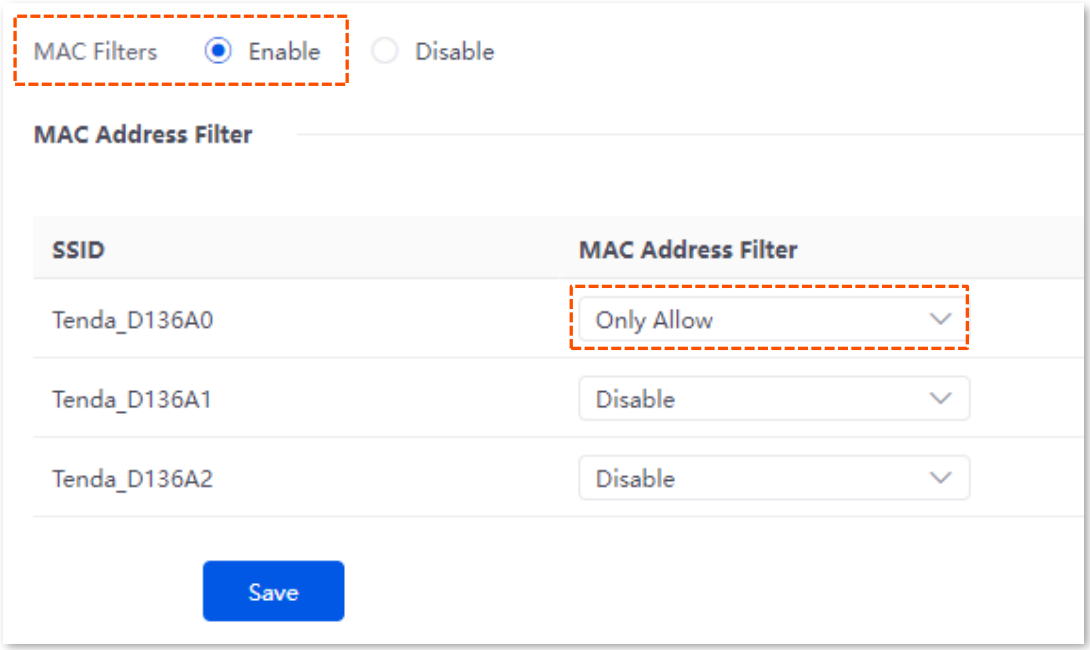
Parameter		Description
	MAC Address Filter	Specifies the three kinds of rules you can perform on the corresponding wireless network. - **Disable**: This function is disabled, and all wireless clients can connect to this wireless network. - **Only Allow**: Only wireless clients with the specified MAC 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 Log in to the web UI of the router.

Step 2 Navigate to **Wireless** > **MAC Filters**. Enable **MAC Filters**, and click **Save**.

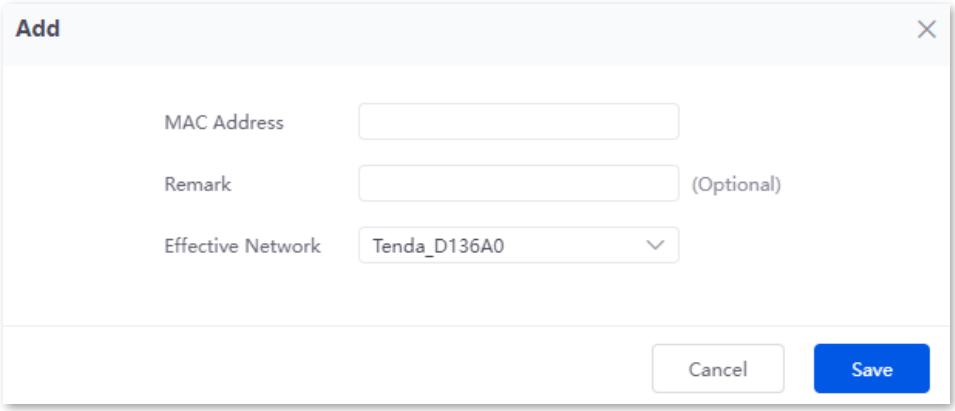
Step 3 Configure the MAC address filter mode for each SSID by selecting from the **MAC Address Filter** drop-down list menu, then click **Save**. This page is for reference only.



Step 4 Add rule(s).

1. Click **Add**.

2. On the **Add** configuration window, 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**.



----End

Rules will appear on the **MAC Filter List**.

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.

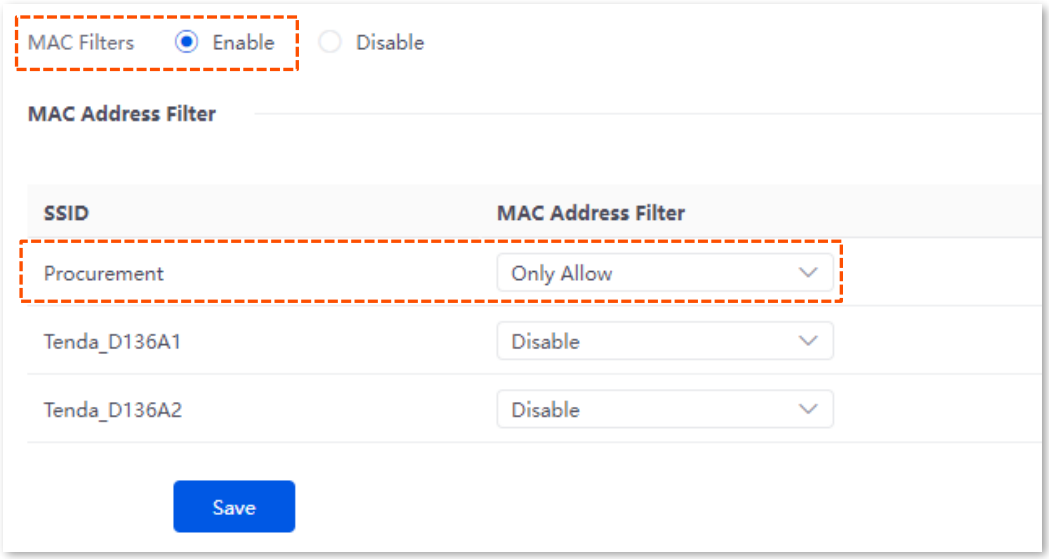
Configuration procedure

Step 1 Log in to the web UI of the router.

Step 2 Navigate to **Wireless** > **MAC Filters**. Enable **MAC Filters**, and click **Save**.

Step 3 Select a MAC address filter mode for the WiFi network **Procurement**, which is **Only Allow** in this example.

Step 4 Click **Save**.



Step 5 Add a MAC filter rule.

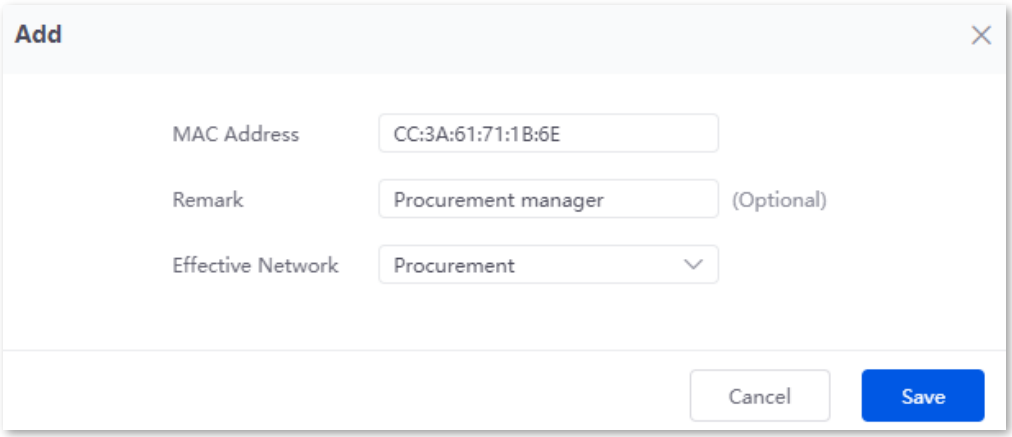
1. Click **Add**.
2. On the **Add** configuration window, set the following parameters:

   Set **MAC Address** to **CC:3A:61:71:1B:6E**.

   (Optional) Set **Remark** to **Procurement manager**.

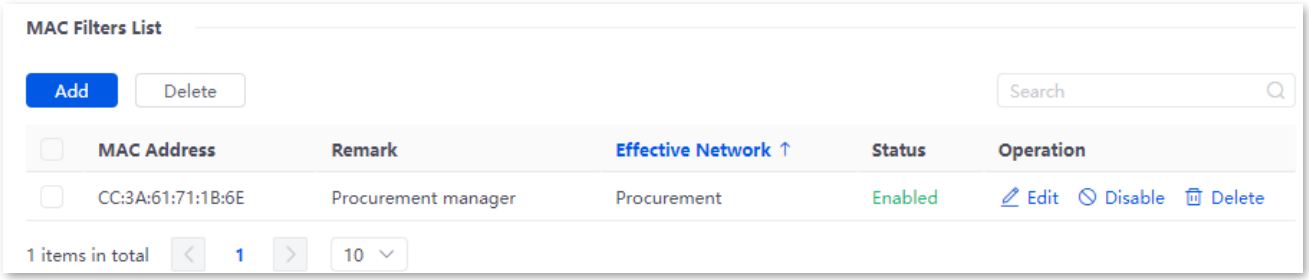
   Select **Procurement** from the drop-down list of **Effective Network**.

   Click **Save**.



----End

Added successfully. See the following figure.



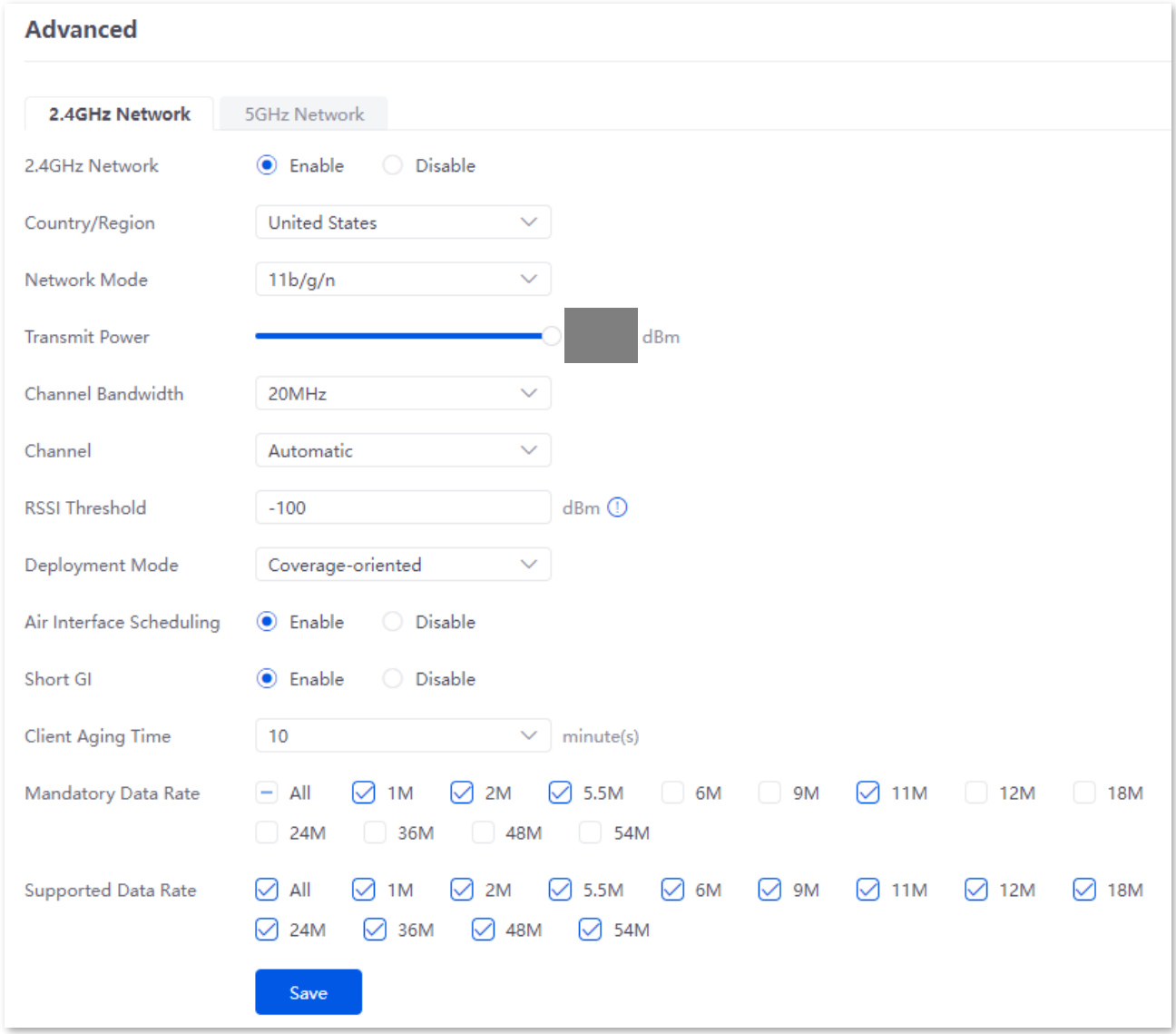
Verification

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

5.4 Advanced settings

To access the configuration page, log in to the web UI of the router, and navigate to **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.



Parameter description

Parameter	Description
2.4GHz Network	Used to enable or disable the 2.4 GHz wireless network of the router.
5GHz Network	Used to enable or disable the 5 GHz wireless network of the router.
Country/Region	Specifies the country or region that you set for the router to conform to the regulations of different countries or regions concerning channels.

Parameter	Description
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** (default). Available options for **5 GHz** band: **11a, 11a/n, 11a/n/ac** (default)**.** You are recommended to keep the default settings.
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.
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.
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. **Automatic**: 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).
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.
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.

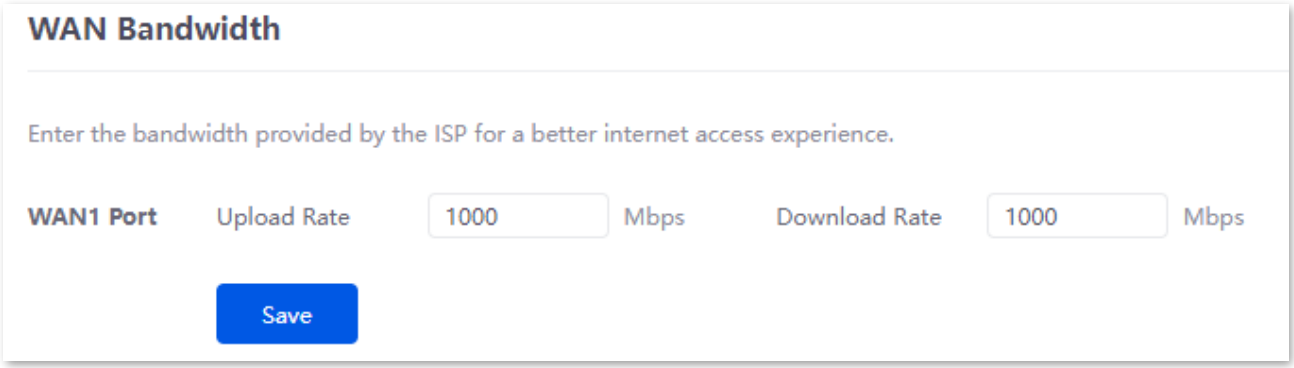
Parameter	Description
Prioritize 5 GHz	Specifies that a wireless client uses the 5 GHz SSID first to connect to the device if the wireless client supports both 5 GHz and 2.4 GHz networks and the networks use the same SSID and password. This parameter is valid only for 5 GHz networks.
Prioritize 5 GHz 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. You are recommended to keep 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. This parameter is valid only for 2.4 GHz networks. 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. This parameter is valid only for 5 GHz networks. 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 Aging Time	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 Date Rate Supported Data 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.

6 Bandwidth Limit

6.1 WAN bandwidth

To access the configuration page, log in to the web UI of the router, and navigate to **BW Limit** > **WAN Bandwidth** to enter the page.

Here, you can configure the WAN port bandwidth parameters. After you set multiple WAN ports, you can limit the bandwidth of multiple WAN ports respectively.



Parameter description

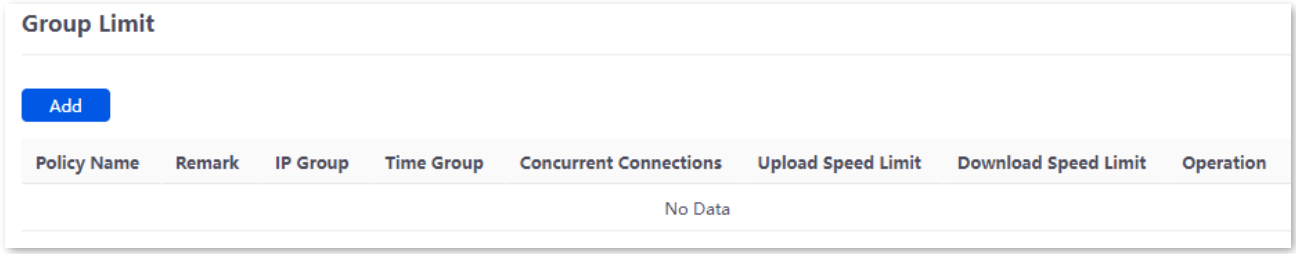
Parameter	Description
Upload Rate	Specify the bandwidth values of the broadband. If you are not clear about them, consult your ISP
Download Rate	

6.2 Group limit

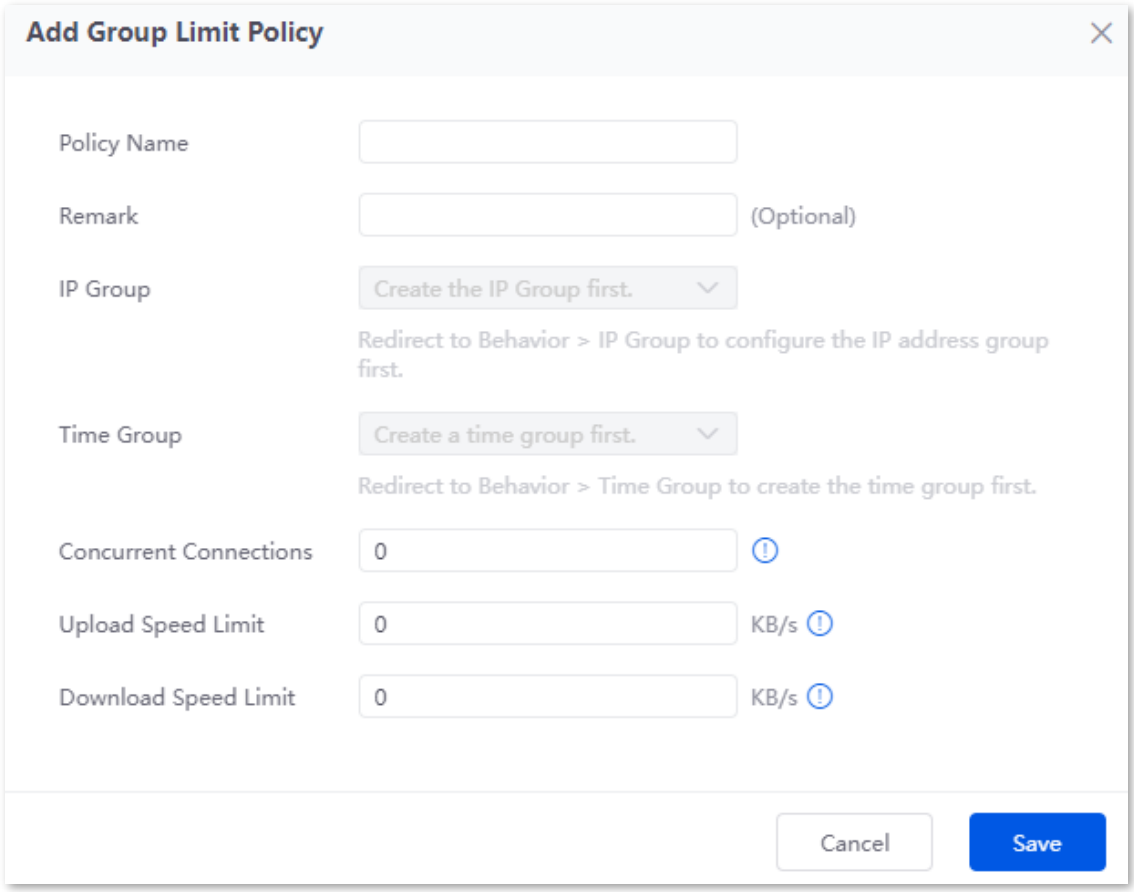
The extranet bandwidth is always limited, so the network administrator needs to control users' network speed to reasonably allocate the limited bandwidth resources, utilizing the extranet resources effectively.

To access the configuration page, log in to the web UI of the router, and navigate to **BW Limit** > **Group limit** to enter the page.

Here, you can configure the group speed limit policy of the router.



You can click **Add** to add a new group limit policy.



Parameter description

Parameter	Description
Policy Name	Specifies the name of the group limit policy.
Remark	Specifies the remark of the group limit policy. The remark is optional.
IP Group	Specifies the IP address group upon which the group speed limit policy takes effect. The group speed limit policy takes effect only when the device IP addresses are in the IP address group. TIP The IP group should be configured in **IP Group** in advance.
Time Group	Specifies the time group upon which the group speed limit policy takes effect. The group speed limit policy takes effect only in such configured time. TIP The time group should be configured in **Time Group** in advance.
Concurrent Connections	Specifies the maximum connections for a single user device in the controlled IP group. TIP **0** indicates no limit.
Upload Speed Limit Download Speed Limit	Specify the maximum upload/download rate of the controlled user device. The bandwidth obtained by each controlled device may be different. TIP **0** indicates no limit.

6.3 Example of configuring group limit

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 192.168.0.50 can use a fixed upload and download bandwidth of 1 Mbps. For other clients in the LAN, no bandwidth control rules are added.

Policy name	IP range	Effective time	Upload bandwidth	Download bandwidth
Speed limit	192.168.0.2~50	08:00~18:00 on weekdays	1 Mbps	1 Mbps

Solution

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

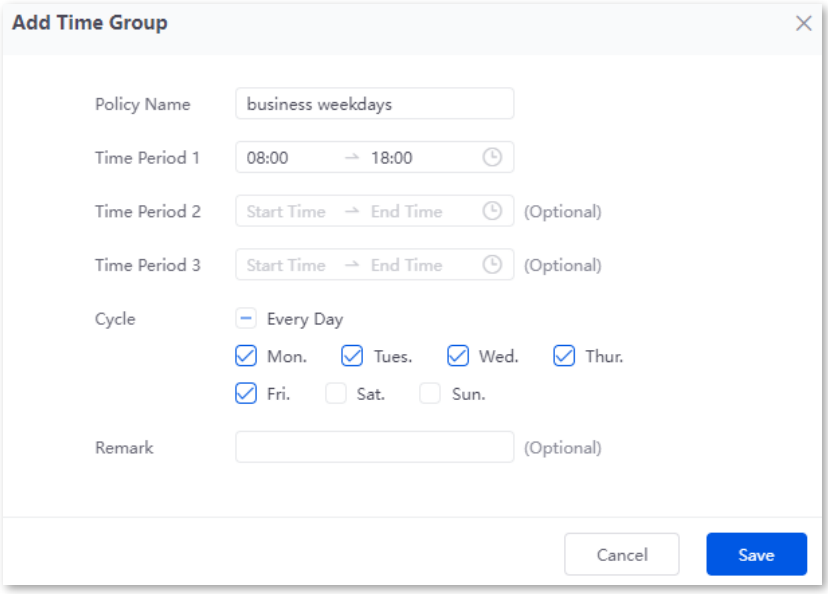
Configuration procedure

Set a time group → Set an IP group → Set a group limit policy

Step 1 Log in to the web UI of the router.

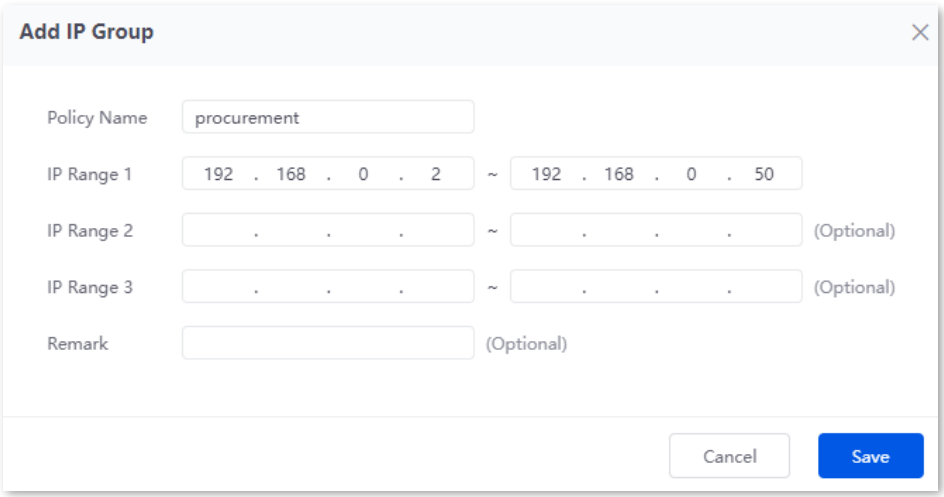
Step 2 Set a time group.

1. Navigate to **Behavior** > **Group Policy** > **Time Group**.
2. Click **Add**, and configure the following time group.



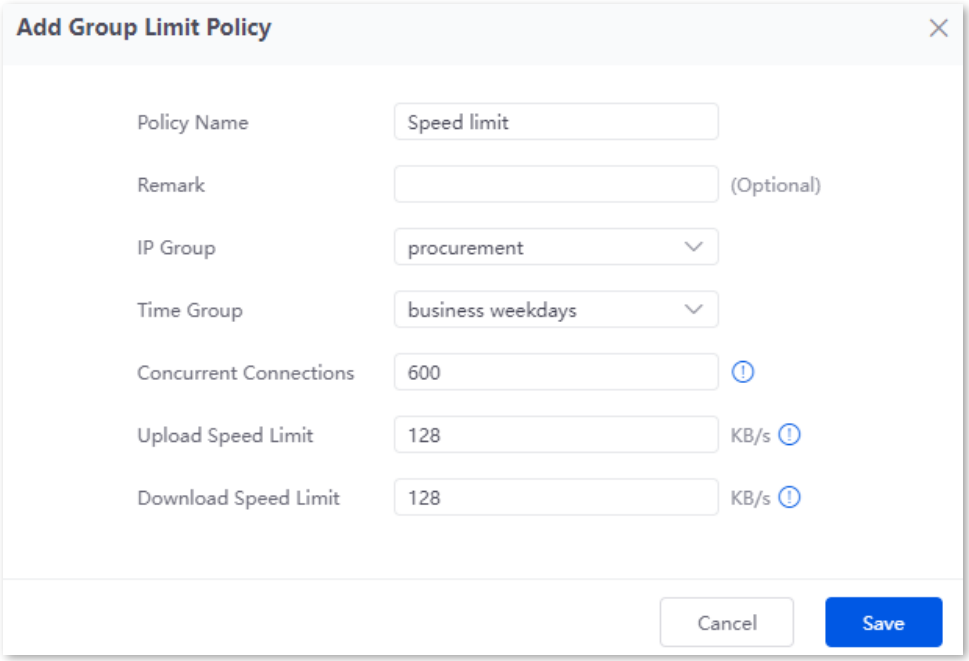
Step 3 Set an IP group.

1. Navigate to **Behavior** > **Group Policy** > **IP Group**.
2. Click **Add**, and configure the following IP group.



Step 4 Set a group limit policy.

1. Navigate to **BW Limit** > **Group limit**.
2. Click **Add**, and configure the following group limit policy.



----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 192.168.0.50 is allocated 1 Mbps (128 KB/s) upload and download bandwidth.

7 Behavior

7.1 Group policy

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.

7.1.1 Time group

The time group policy is used to divide time into different groups and combine different groups together randomly.

To access the configuration page, log in to the web UI of the router, and navigate to **Behavior** > **Group Policy** > **Time Group** to enter the page.

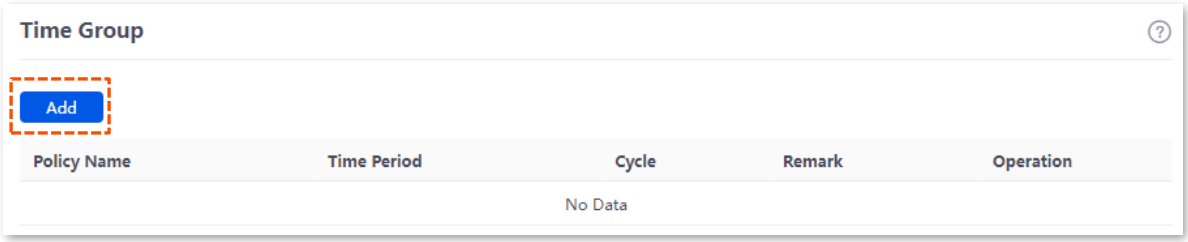
Here, you can configure the time group policy according to the actual requirements.

Configuration procedure:

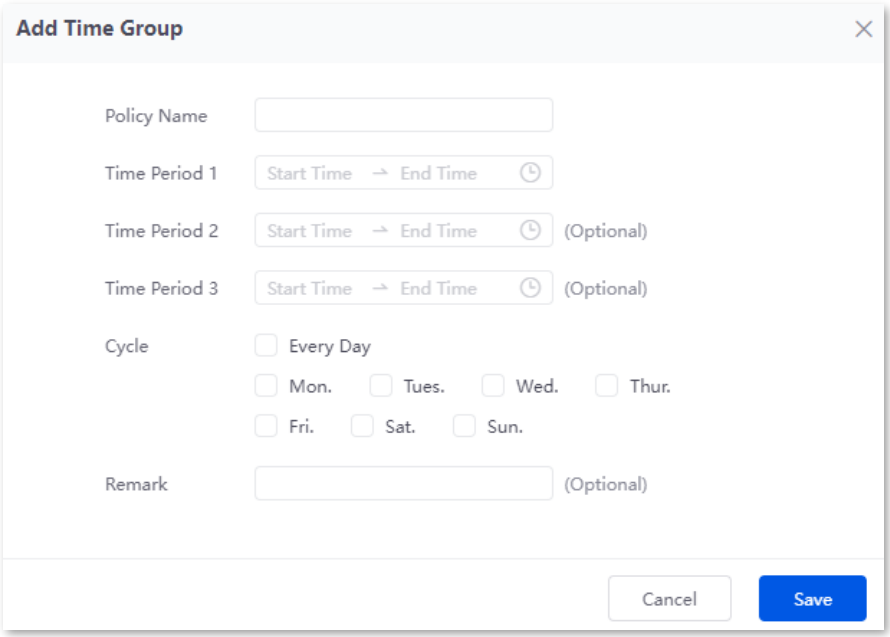
Step 1 Log in to the web UI of the router.

Step 2 Navigate to **Behavior** > **Group Policy** > **Time Group**.

Step 3 Click **Add**.



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



----End

Parameter description

Parameter	Description
Policy Name	Specifies the name of the time group policy.
Time Period	Specifies the time periods included in the time group. One policy supports at most 3 time periods, and the time periods cannot be repeated.
Cycle	Specifies the cycle upon which the time group policy takes effect.
Remark	Specifies the remark of the policy.

7.1.2 IP group

The IP group policy is used to set the hosts within the LAN into different groups based on their IP addresses.

To access the configuration page, log in to the web UI of the router, and navigate to **Behavior** > **Group Policy** > **IP Group** to enter the page.

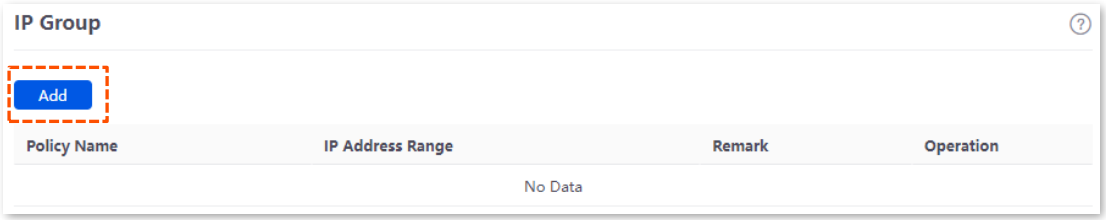
Here, you can configure the IP group policy according to the actual requirements.

Configuration procedure:

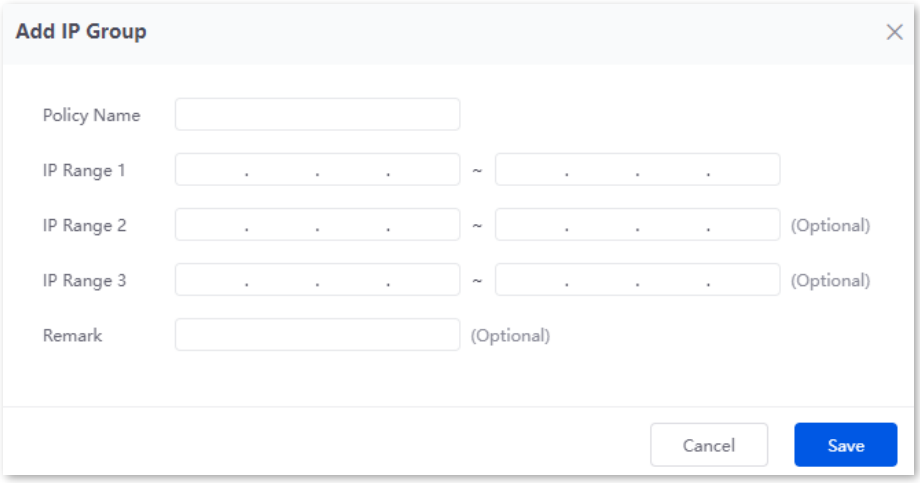
Step 1 Log in to the web UI of the router.

Step 2 Navigate to **Behavior** > **Group Policy** > **IP Group**.

Step 3 Click **Add**.



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



----End

Parameter description

Parameter	Description
Policy Name	Specifies the name of the IP group policy.
IP Address Range	Specifies the IP address ranges included in the IP group. One policy supports at most 3 IP address ranges, and the IP address ranges cannot be repeated.
Remark	Specifies the remark of the IP group policy.

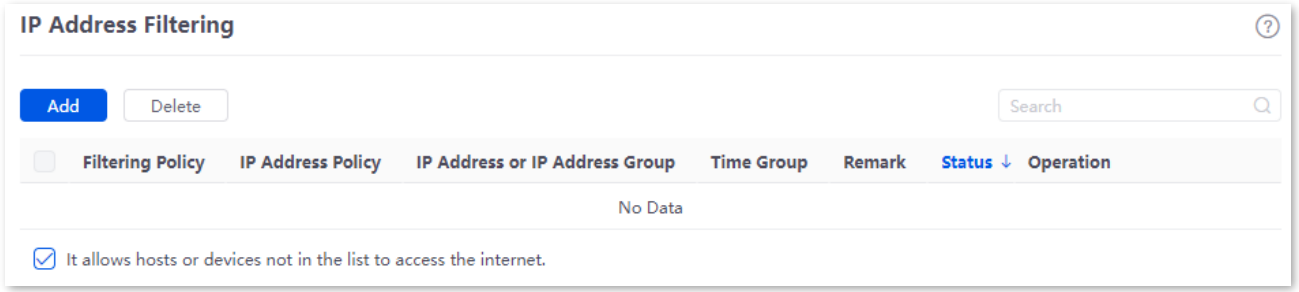
7.2 Filtering

7.2.1 IP address filtering

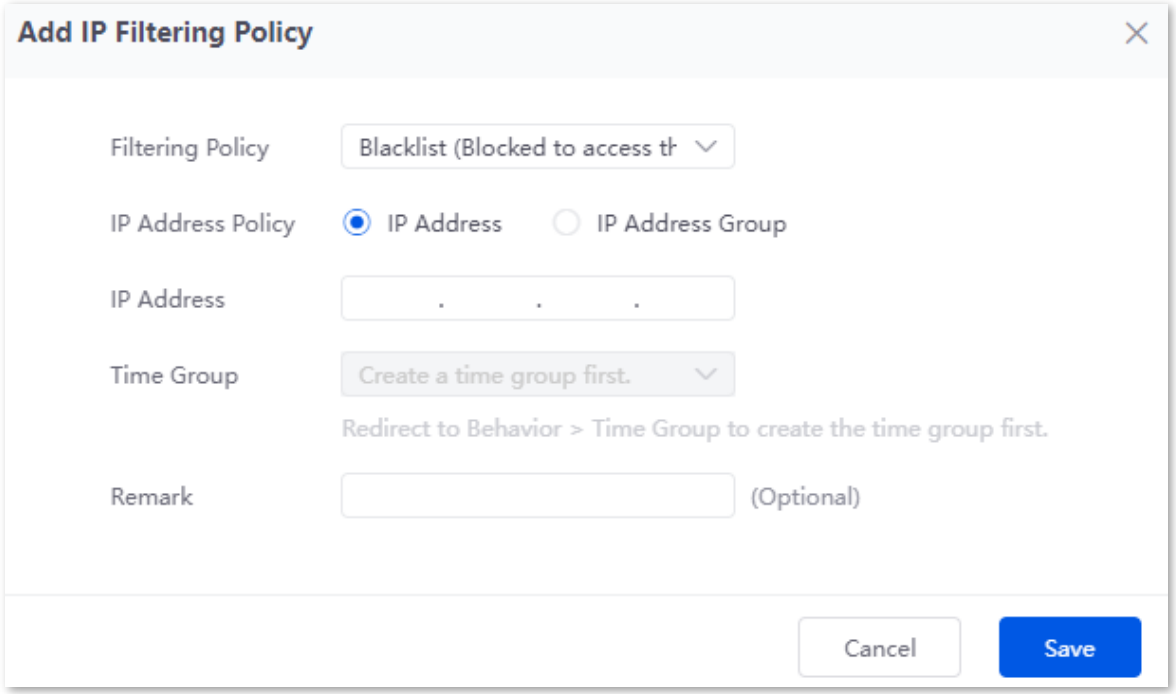
Overview

To access the configuration page, log in to the web UI of the router, and navigate to **Behavior** > **Filtering** > **IP Address Filtering** to enter the page.

Here, you can configure the IP address filtering rules to allow or block the LAN hosts to connect to the router for internet.



You can click **Add** to add a new IP address filtering policy.



Parameter description

Parameter	Description
Filtering Policy	Specifies the mode of the IP address filtering policy. - **Blacklist (Blocked to access the internet)**: The user with the specified IP address is blocked to access the internet during the specified time period, and is allowed to access the internet during other time. - **White List (Allowed to access the internet)**: The user with the specified IP address is allowed to access the internet during the specified time period, and is blocked to access the internet during other time.
IP Address Policy	To filter one IP address, select **IP Address** and enter the IP address.
IP Address or IP Group	To filter one or more IP address groups, select **IP Address Group** and select the corresponding IP group policy you set. TIP The IP group should be configured in **IP Group** in advance.
Time Group	Used to select the time group policy upon which the IP address filtering policy takes effect. TIP The time group should be configured in **Time Group** in advance.
Remark	Specifies the remark of the IP address filtering policy.
Status	Specifies the status of the IP address filtering policy, including **Enabled** and **Disabled**.
It allows hosts or devices not in the list to access the internet.	- When Selected: The devices not in the filtering list or devices with the filtering policy disabled can access the internet. - When Deselected: The devices not in the filtering list or devices with the filtering policy disabled cannot access the internet. TIP To deselect this function, configure a whitelist first.

Example of configuring an IP address filtering policy

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 filtering can meet this requirement.

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

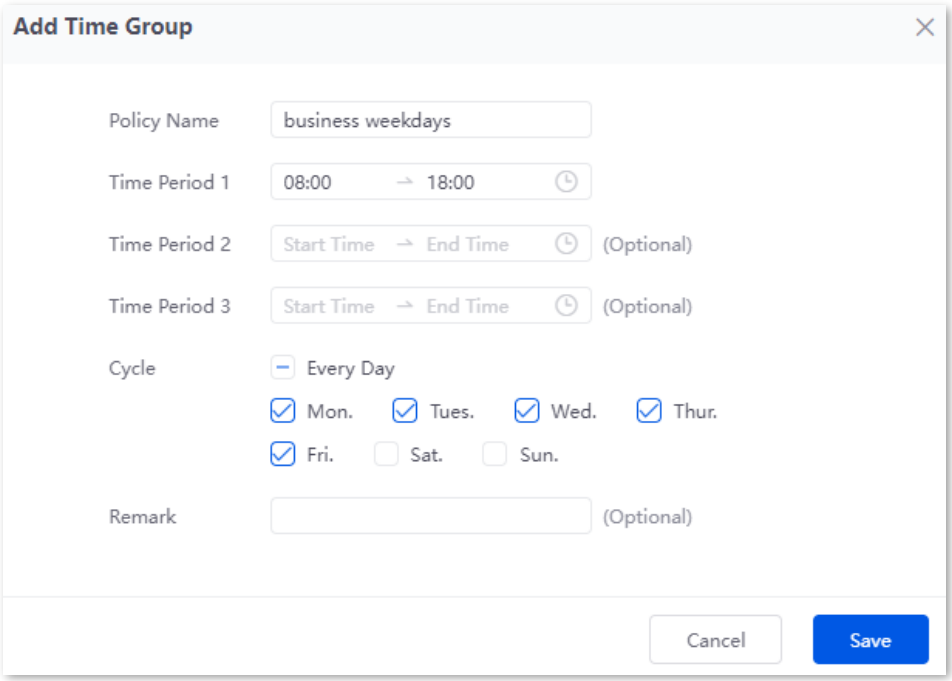
Configuration procedure

Set a time group → Set an IP group → Add an IP filtering policy

Step 1 Log in to the web UI of the router.

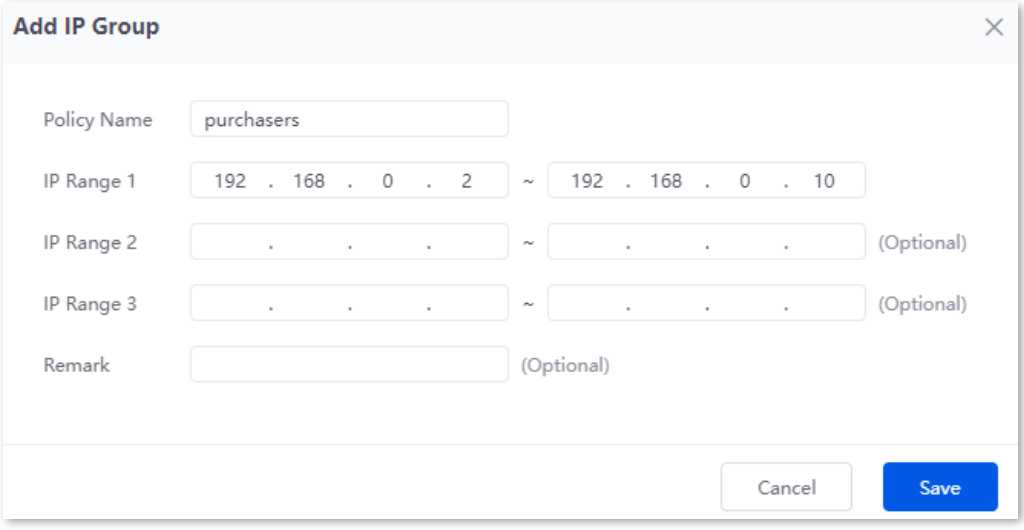
Step 2 Set a time group.

1. Navigate to **Behavior** > **Group Policy** > **Time Group**.
2. Click **Add**, and configure the following time group.



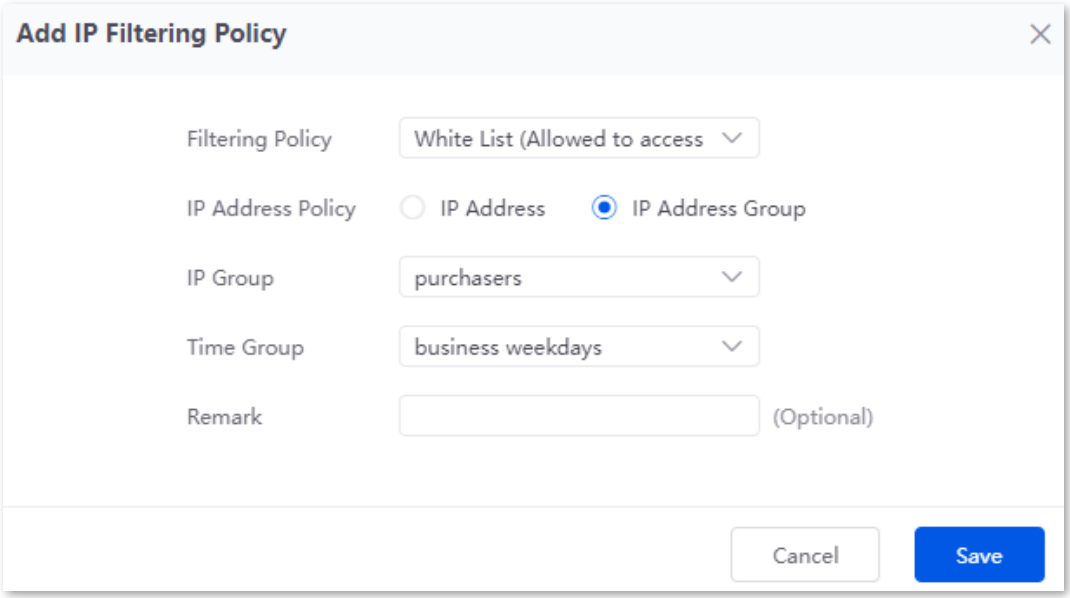
Step 3 Set an IP group.

1. Navigate to **Behavior** > **Group Policy** > **IP Group**.
2. Click **Add**, and configure the following IP group.

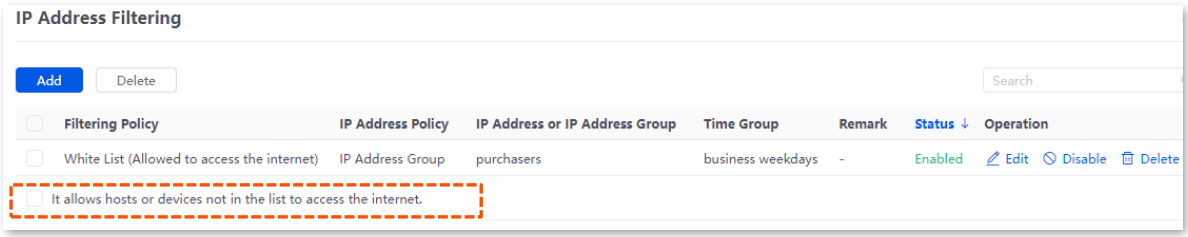


Step 4 Add an IP filtering policy.

1. Navigate to **Behavior** > **Filtering** > **IP Address Filtering**.
2. Click **Add**, and configure the following IP filtering policy.



Step 5 Deselect **It allows hosts or devices not in the list to access the internet**.



----End

Verification

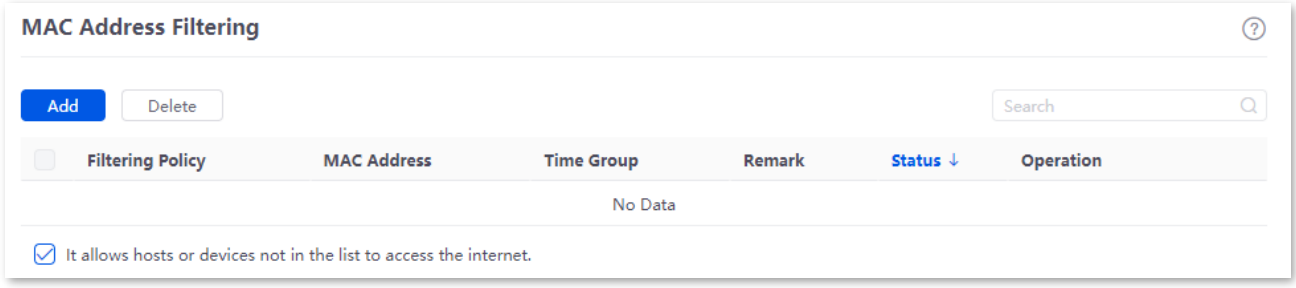
During 08:00 to 18:00 on weekdays, only the purchasers' computers with IP addresses ranging from 192.168.0.2 to 192.168.0.10 can access the internet.

7.2.2 MAC address filtering

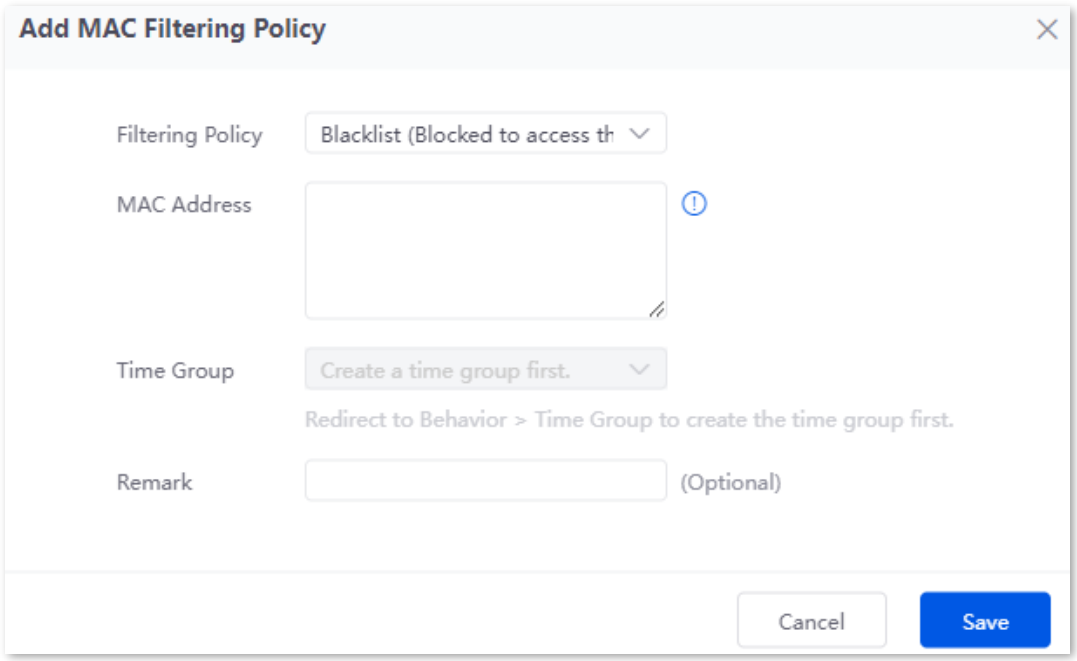
Overview

To access the configuration page, log in to the web UI of the router, and navigate to **Behavior** > **Filtering** > **MAC Address Filtering** to enter the page.

You can configure the MAC address filtering rules to allow or block the LAN hosts to connect to the router for internet.



You can click **Add** to add a new MAC address filtering policy.



Parameter description

Parameter	Description
Filtering Policy	Specifies the mode of the MAC address filtering policy. - **Blacklist (Blocked to access the internet)**: The user with the specified MAC address is blocked to access the internet during the specified time period, and is allowed to access the internet during other time. - **White List (Allowed to access the internet)**: The user with the specified MAC address is allowed to access the internet during the specified time period, and is blocked to access the internet during other time.

Parameter	Description
MAC Address	Specifies the MAC address of the client to which the rule applies.
Time Group	Used to select the time group policy upon which the MAC address filtering policy takes effect. TIP The time group should be configured in **Time Group** in advance.
Remark	Specifies the remark of the MAC address filtering policy.
Status	Specifies the status of the MAC address filter rule, including **Enabled** and **Disabled**.
It allows hosts or devices not in the list to access the internet.	- When Selected: The devices not in the filtering list or devices with the filtering policy disabled can access the internet. - When Deselected: The devices not in the filtering list or devices with the filtering policy disabled cannot access the internet. TIP To deselect this function, configure a whitelist first.

Example of configuring a MAC address filtering policy

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 filtering can meet this requirement.

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

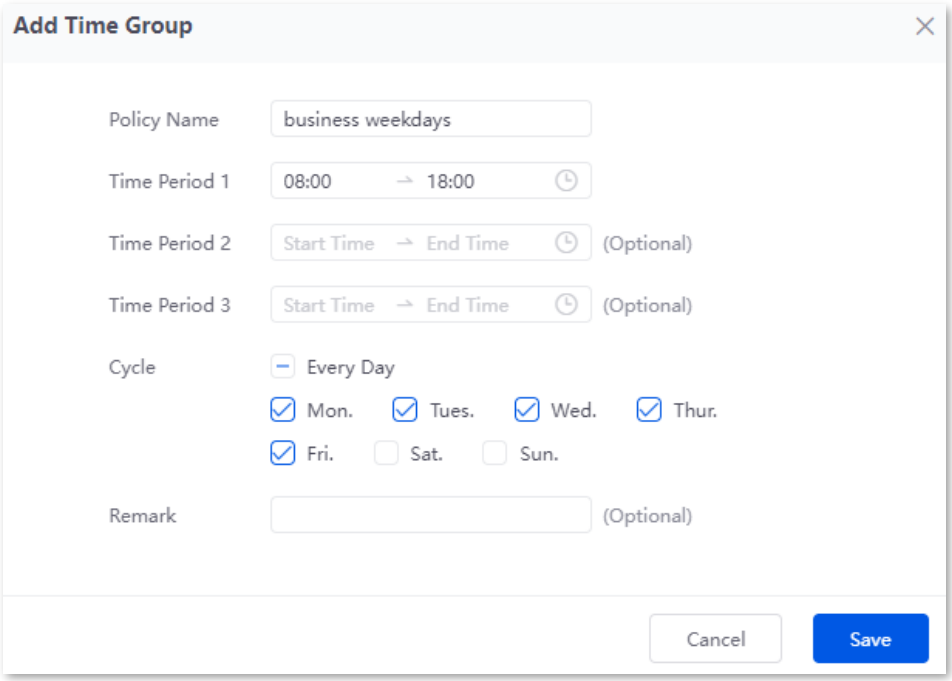
Configuration procedure

Set a time group → Add a MAC filter rule

Step 1 Log in to the web UI of the router.

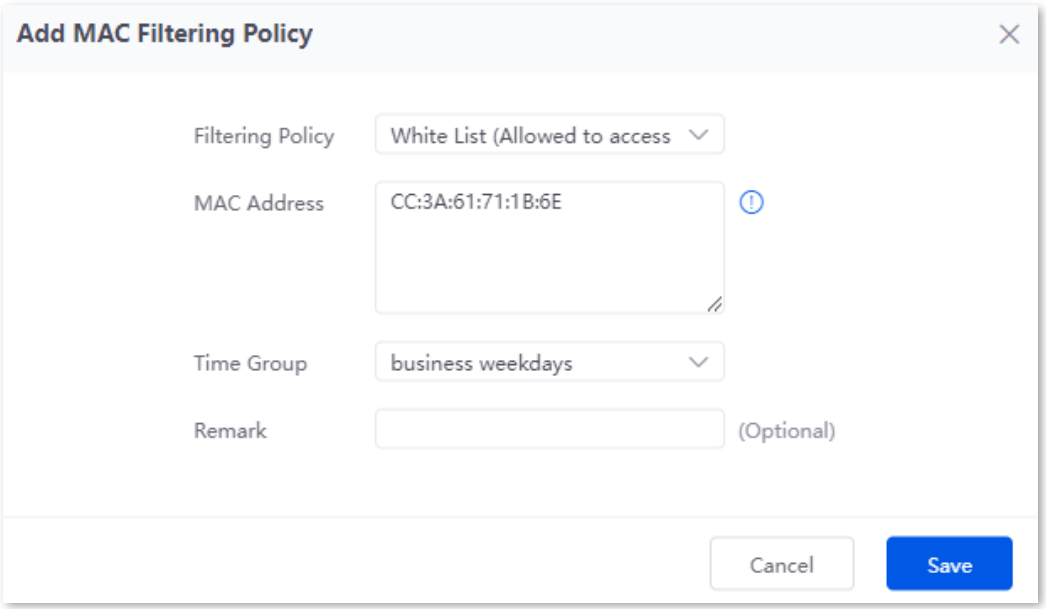
Step 2 Set a time group.

1. Navigate to **Behavior** > **Group Policy** > **Time Group**.
2. Click **Add**, and configure the following time group.

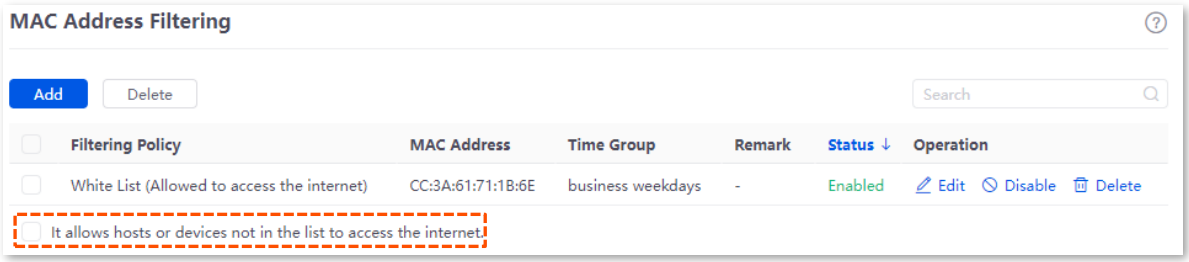


Step 3 Add a MAC address filtering policy.

1. Navigate to **Behavior** > **Filtering** > **MAC Address Filtering**.
2. Click **Add**, and configure the following MAC address filtering policy.



Step 4 Deselect **It allows hosts or devices not in the list to access the internet**.



----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.

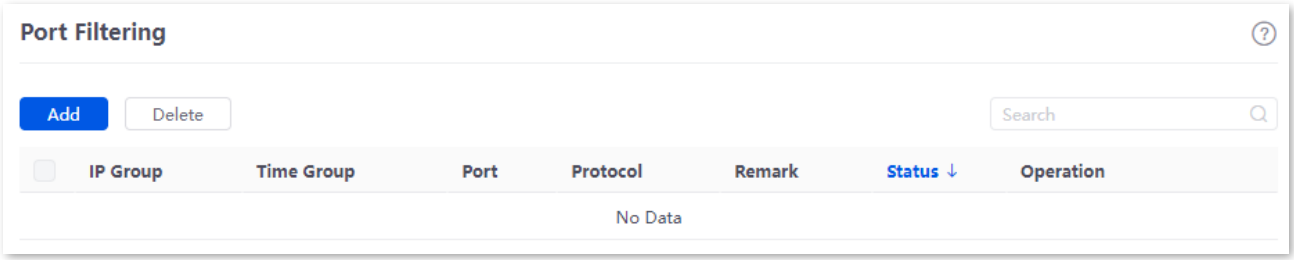
7.3 Port filtering

7.3.1 Overview

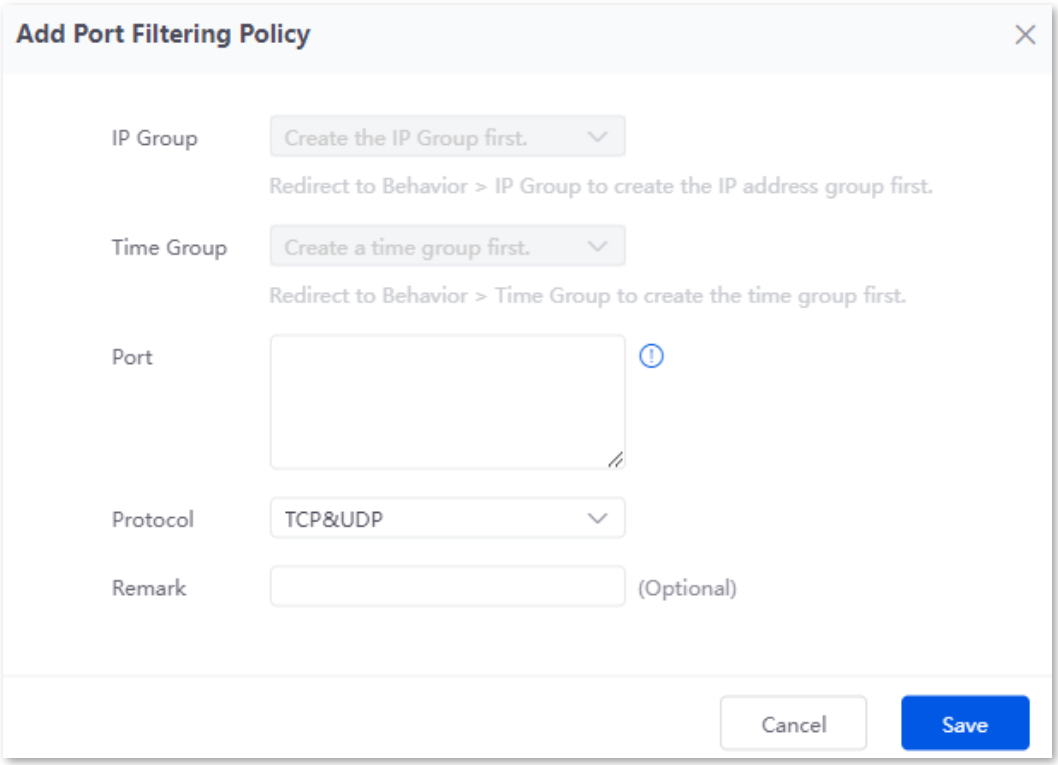
Application protocols for internet services have specific port numbers. 0 to 1023 are port numbers for some common services. These ports are generally fixed to specific services.

To access the configuration page, log in to the web UI of the router, and navigate to **Behavior** > **Filtering** > **Port Address Filtering** to enter the page.

Here, you can control users' access to certain types of internet services by forbidding their access to the specified service ports.



You can click **Add** to add a new port filtering policy.



Parameter description

Parameter	Description
IP Group	Used to select the IP address group policy upon which the port filtering policy takes effect. TIP The IP address group should be configured in IP Group in advance.
Time Group	Used to select the time group policy upon which the port filtering policy takes effect. TIP The time group should be configured in Time Group in advance.
Port	Specifies the service port forbidden to access.
Protocol	Specifies the service protocol forbidden to access.
Remark	Specifies the remark of the port filtering policy.
Status	Specifies the status of the port filtering policy, including **Enabled** and **Disabled**.

7.3.2 Example of configuring a port filtering policy

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 filtering 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.

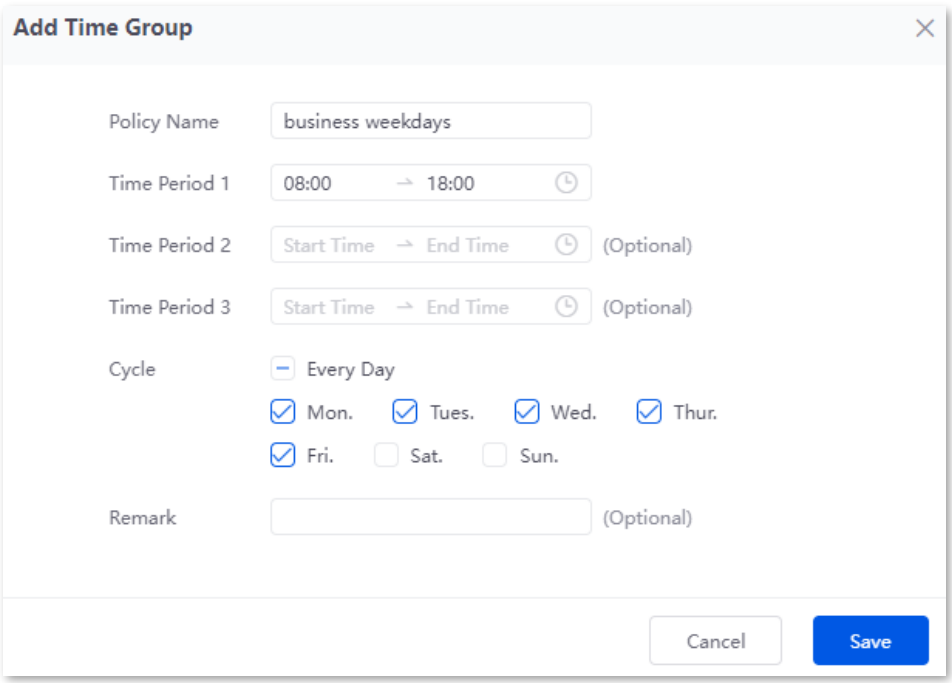
Configuration procedure

Set a time group → Set an IP group → Add port filtering policy

Step 1 Log in to the web UI of the router.

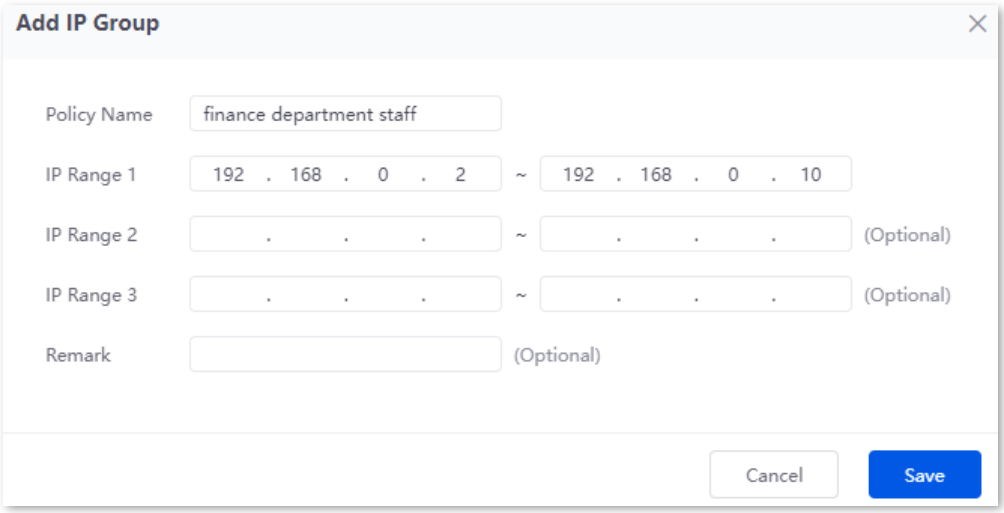
Step 2 Set a time group.

1. Navigate to **Behavior** > **Group Policy** > **Time Group**.
2. Click **Add**, and configure the following time group.



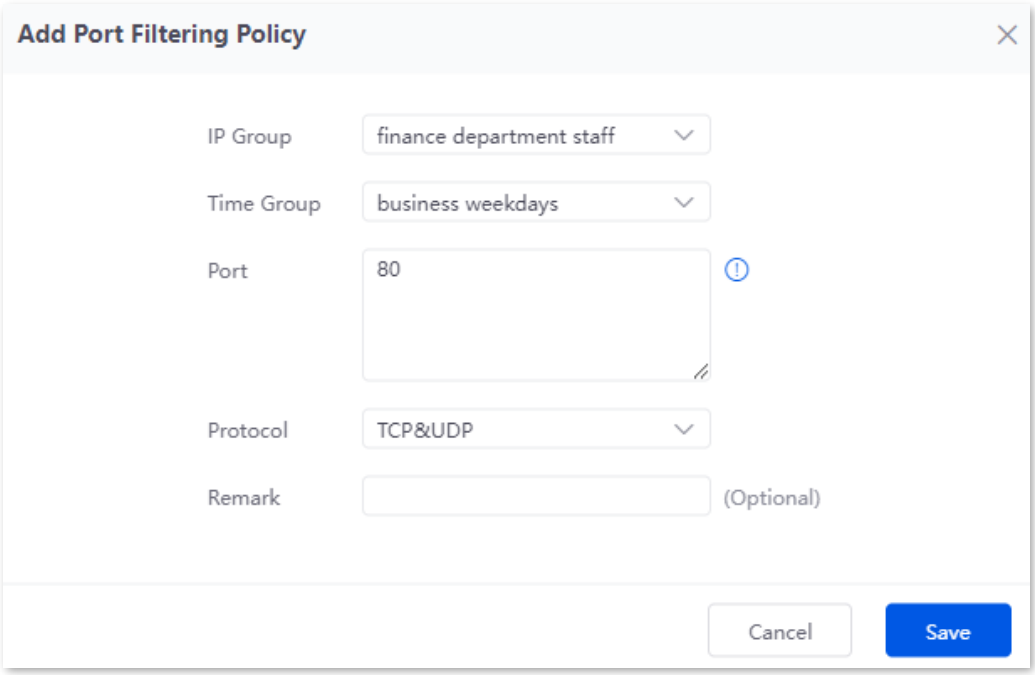
Step 3 Set an IP group.

1. Navigate to **Behavior** > **Group Policy** > **IP Group**.
2. Click **Add**, and configure the following IP group.

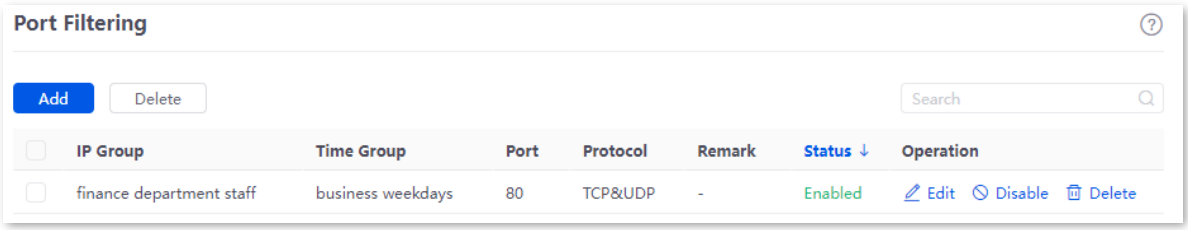


Step 4 Add a port filtering policy.

1. Navigate to **Behavior** > **Filtering** > **Port Filtering**.
2. Click **Add**, and configure the following port filtering policy.



Added successfully. See the following figure.



----End

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 192.168.0.10 cannot browse web pages.

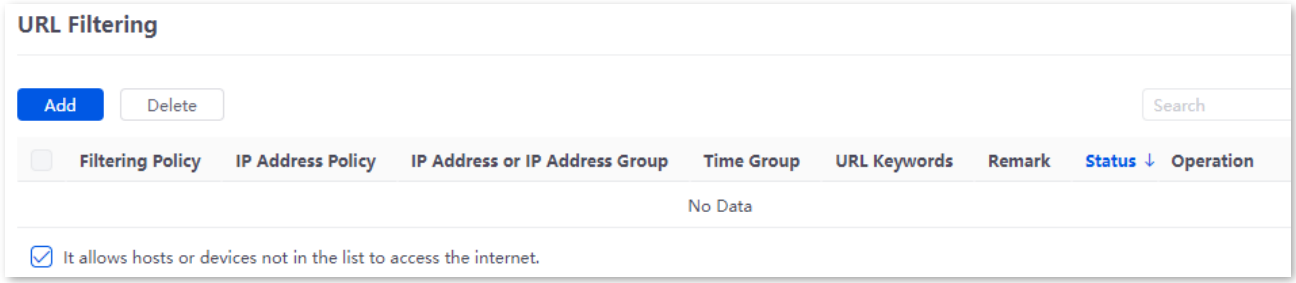
7.4 URL filtering

7.4.1 Overview

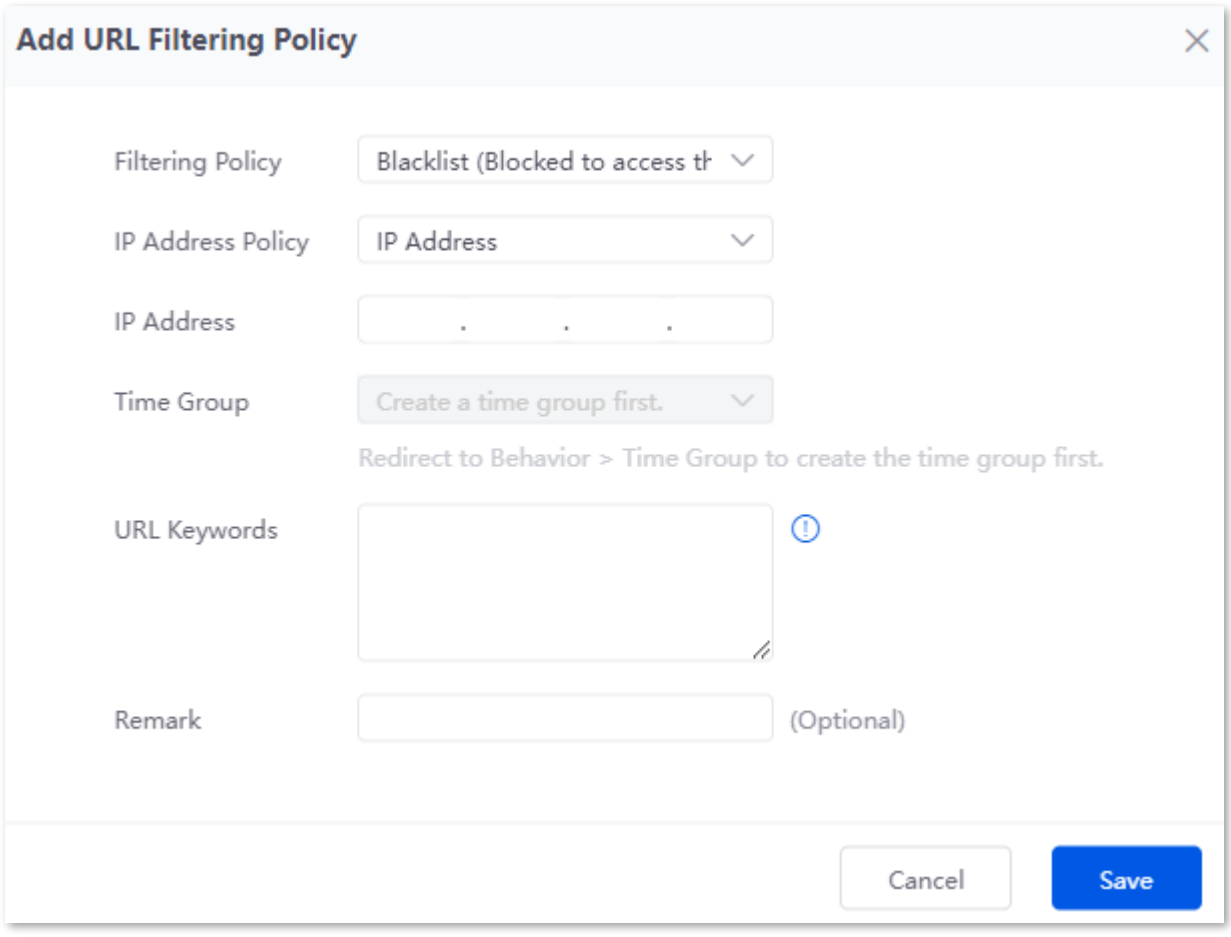
The URL filtering prevents LAN users from accessing specified types of website and controls internet accessibility of LAN users so that they will not spend time on websites irrelevant to their duties.

To access the configuration page, log in to the web UI of the router, and navigate to **Behavior** > **Filtering** > **URL Filtering** to enter the page.

Here, you can allow or block users to access specified websites to regulate users' online behavior in the LAN.



You can click **Add** to add a new URL filtering policy.



Parameter description

Parameter	Description
Filtering Policy	Specifies the mode of the URL filtering policy. - **Blacklist (Blocked to access the internet)**: The user with the specified IP address is only blocked to access specified websites during the specified time period, and is allowed to access all websites during other time. - **White List (Allowed to access the internet)**: The user with the specified IP address is only allowed to access specified websites during the specified time period, and is allowed to access all websites during other time.
IP Address Policy	To filter one IP address, select **IP Address** and enter the IP address.
IP Address or IP Address Group	To filter one or more IP address groups, select **IP Address Group** and select the corresponding IP group policy you set. TIP The IP group should be configured in **IP Group** in advance.
Time Group	Used to select the time group policy upon which the URL filtering policy takes effect. TIP The time group should be configured in **Time Group** in advance.
URL Keywords	Specifies the keywords of the URL forbidden/allowed to access.
Remark	Specifies the remark of the URL filtering policy.
Status	Specifies the status of the URL filtering policy, including **Enabled** and **Disabled**.
It allows hosts or devices not in the list to access the internet.	- When Selected: The devices not in the filtering list or devices with the filtering policy disabled can access the specified websites. - When Deselected: The devices not in the filtering list or devices with the filtering policy disabled cannot access the specified websites. TIP To deselect this function, configure a whitelist first.

7.4.2 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 filtering 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.

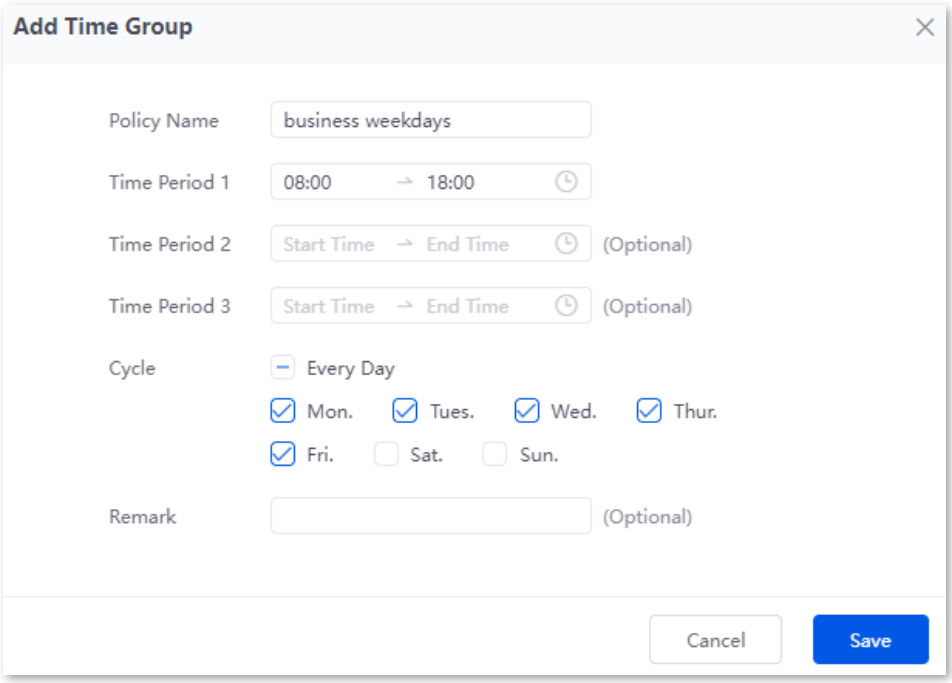
Configuration procedure

Set a time group > Set an IP group > Add a URL filtering policy

Step 1 Log in to the web UI of the router.

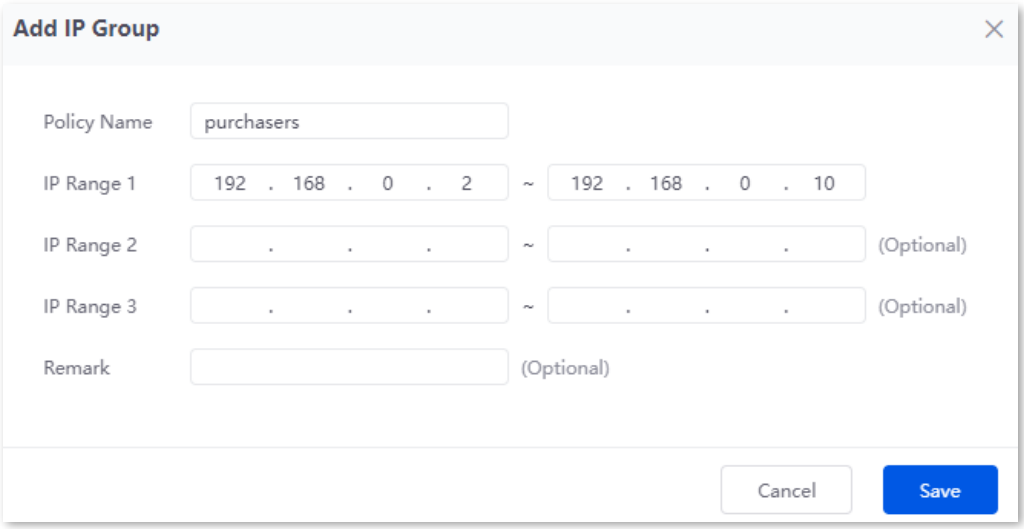
Step 2 Set a time group.

1. Navigate to **Behavior** > **Group Policy** > **Time Group**.
2. Click **Add**, and configure the following time group.



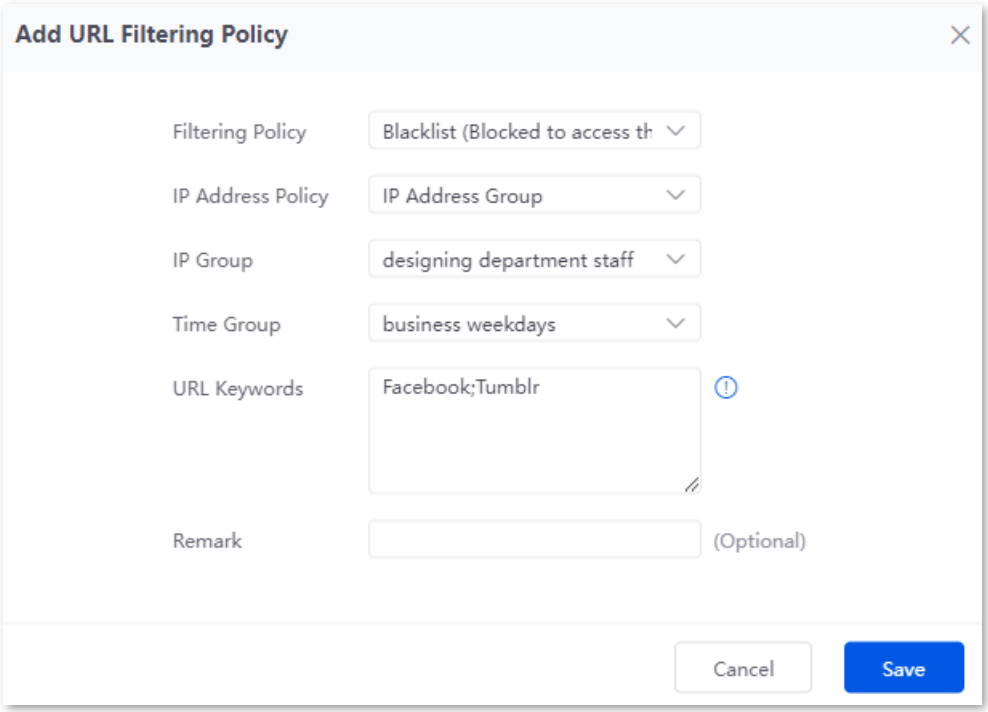
Step 3 Set an IP group.

1. Navigate to **Behavior** > **Group Policy** > **IP Group**.
2. Click **Add**, and configure the following IP group.



Step 4 Add an URL filtering policy.

1. Navigate to **Behavior** > **Filtering** > **URL Filtering**.
2. Click **Add**, and configure the following URL filtering policy.



----End

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.

8 More settings

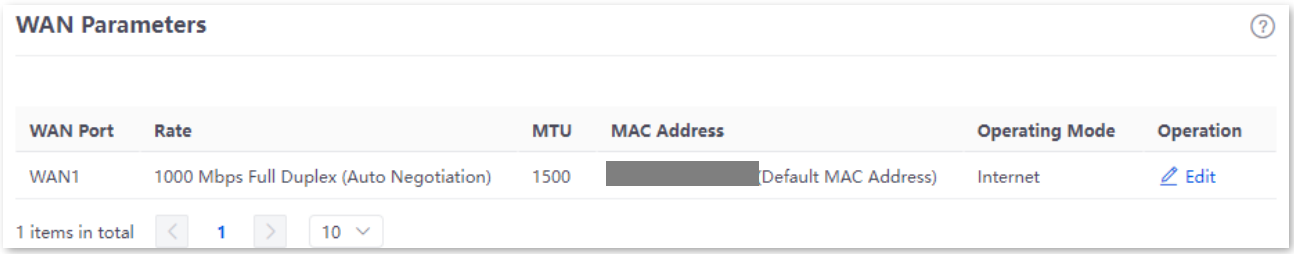
8.1 Advanced routing

8.1.1 WAN parameters

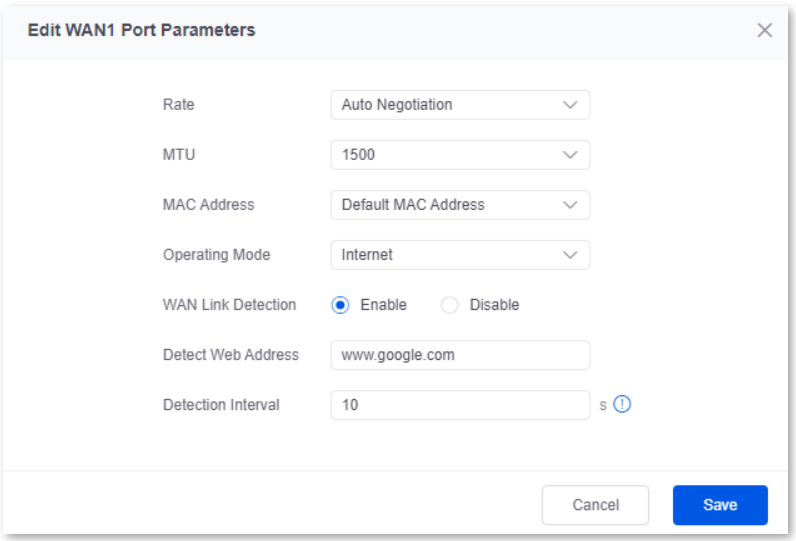
If you have completed the Internet settings correctly, but users of the router's LAN still cannot access the internet, or there is a problem with the internet, you can try to modify the WAN parameters to solve the problem.

To access the configuration page, log in to the web UI of the router, and navigate to **More** > **Advanced Routing** > **WAN Parameters** to enter the page.

Here, you can configure the parameters of the WAN port. After you set multiple WAN ports, you can modify the parameters of multiple WAN ports respectively.



You can click **Edit** to modify the WAN parameters.



Parameter description

Parameter	Description
WAN Port	Specifies the WAN port of the router.

Parameter	Description
Rate	Specifies the rate and duplex mode of the WAN port, which must be consistent with the rate and duplex mode of the WAN port at the peer side. Otherwise, the WAN port may fail to transmit and receive data normally. If the WAN port of the router is connected normally, but the corresponding interface light is not on. Or the interface light will on wait for a while (more than 5 seconds) after the Ethernet cable is plugged in. At this point, you can adjust the WAN port rate of the router to 10 Mbps half-duplex or 10 Mbps full-duplex to solve the problem. If you are uncertain about the rate and duplex mode of the WAN port of the peer side, select **Auto Negotiation**.
MTU	Maximum Transmission Unit (**MTU**) is the largest data packet that a network device transmits, and is related to the WAN port's connection type. Generally, keep the default value. If you cannot access some websites or cannot send and receive emails, you can try to modify the MTU value. The recommended modification range is 1400 to 1500. The following are scenarios where commonly used MTU apply: - **1500**: Used for the most common settings in non-PPPoE connections and non-VPN connections. - **1492**: Used for PPPoE connections. - **1480**: It is the maximum value for the Ping function (packets larger than this value will be broken down). - **1450**: Used for DHCP, which assigns dynamic IP addresses to connected devices. - **1400**: Used for VPN or PPTP.
MAC Address	Specifies the MAC address of the WAN port, which can be customized. After the networking is set up, if the router still cannot connect to the internet, the ISP may have bound the account to a certain MAC address. You can try to solve the problem by modifying the MAC address of the WAN port. - **Default MAC Address**: The default value can be changed if the MAC address is set to **Customize**. - **Customize**: You can customize the MAC address as required.
Operating Mode	Specifies the working mode of the WAN port. - **Internet**: This mode is used as a normal WAN port to connect to the internet. - **Local Network**: The WAN port cannot forward DNS requests, which means that the internet cannot be accessed. This mode is usually used for enterprise intranet.
WAN Link Detection	When the WAN Link Detection function is enabled, the router periodically detects the connectivity between **WAN Port** and **Detect Web Address**, and then selects the best WAN port link as the main egress link according to the detection results.

Parameter	Description
Detect Web Address	Specifies the domain name that needs to be detected. TIP When the WAN Link Detection function is enabled, **Detect Web Address** can be configured.
Detection Interval	Specifies the interval to perform detections. TIP When the WAN Link Detection function is enabled, **Detection Interval** can be configured.

8.1.2 Multi-WAN policy

Overview

To access the configuration page, log in to the web UI of the router, and navigate to **More** > **Advanced Routing** > **Multi-WAN Policy** to enter the page.

Here, you can configure the multi-WAN policy and E-bank data based on source in&out.

- **Multi-WAN policy**

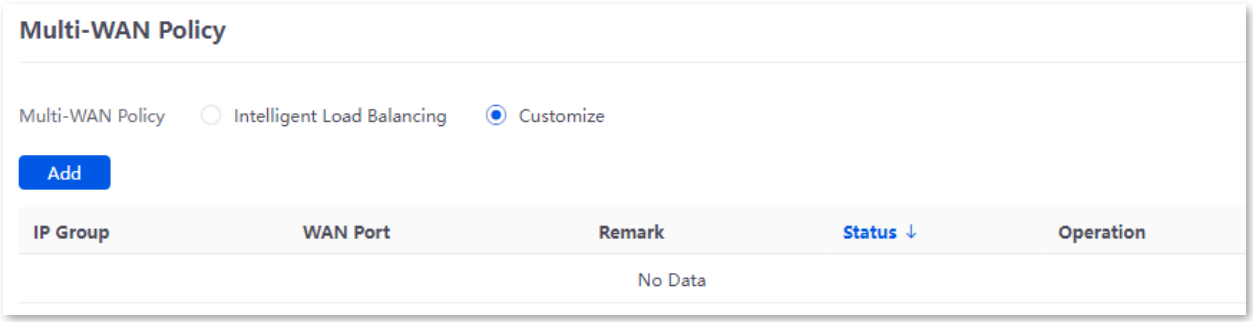
After the router enables multiple WAN ports, it can allow multiple broadband access at the same time to achieve bandwidth superposition. When multiple WAN ports are working at the same time, setting a reasonable multi-WAN policy can greatly improve the bandwidth utilization of the router.

  - **Intelligent Load Balancing**: It indicates that data traffic is allocated automatically and the system will use the WAN port with the least traffic for communication automatically.
  - **Customize**: Users can designate a WAN port for forwarding traffic of a source IP address according to actual needs.

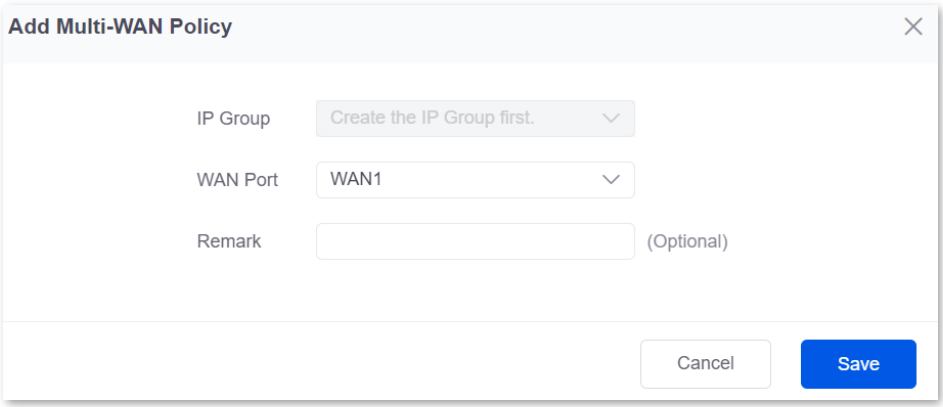
- **E-bank data based on source in&out**

When this function is enabled, the transmitting port and receiving port of E-bank traffic must be consistent, and this configuration is not affected by the load balancing policy. When this function is disabled, some E-banks cannot be used normally.

By default, the router's multi-WAN policy is **Intelligent Load Balancing**. When **Customize** is selected, the page is as follows.



You can click **Add** to customize the multi-WAN policy.



Parameter description

Parameter	Description
Add	Used to add a new multi-WAN policy.
IP Group	Specifies the IP group of the multi-WAN policy. Data traffic from this IP group which can only be forwarded through the specified WAN port. Only one rule can be configured for an IP group. You can configure the IP group in IP Group.
WAN Port	Specifies the WAN port of the multi-WAN policy. Data traffic from the specified IP group will only be forwarded through this WAN port.
Remark	Specifies the description of the multi-WAN policy.
Status	Specifies the status of the customized multi-WAN policy, including **Enabled**, **Disabled**.

Example of configuring multi-WAN policy

Networking requirements

An enterprise uses the wireless router to set up a network. To meet the requirements of the enterprise network, two broadband lines have been handled and the internet has been successfully accessed.

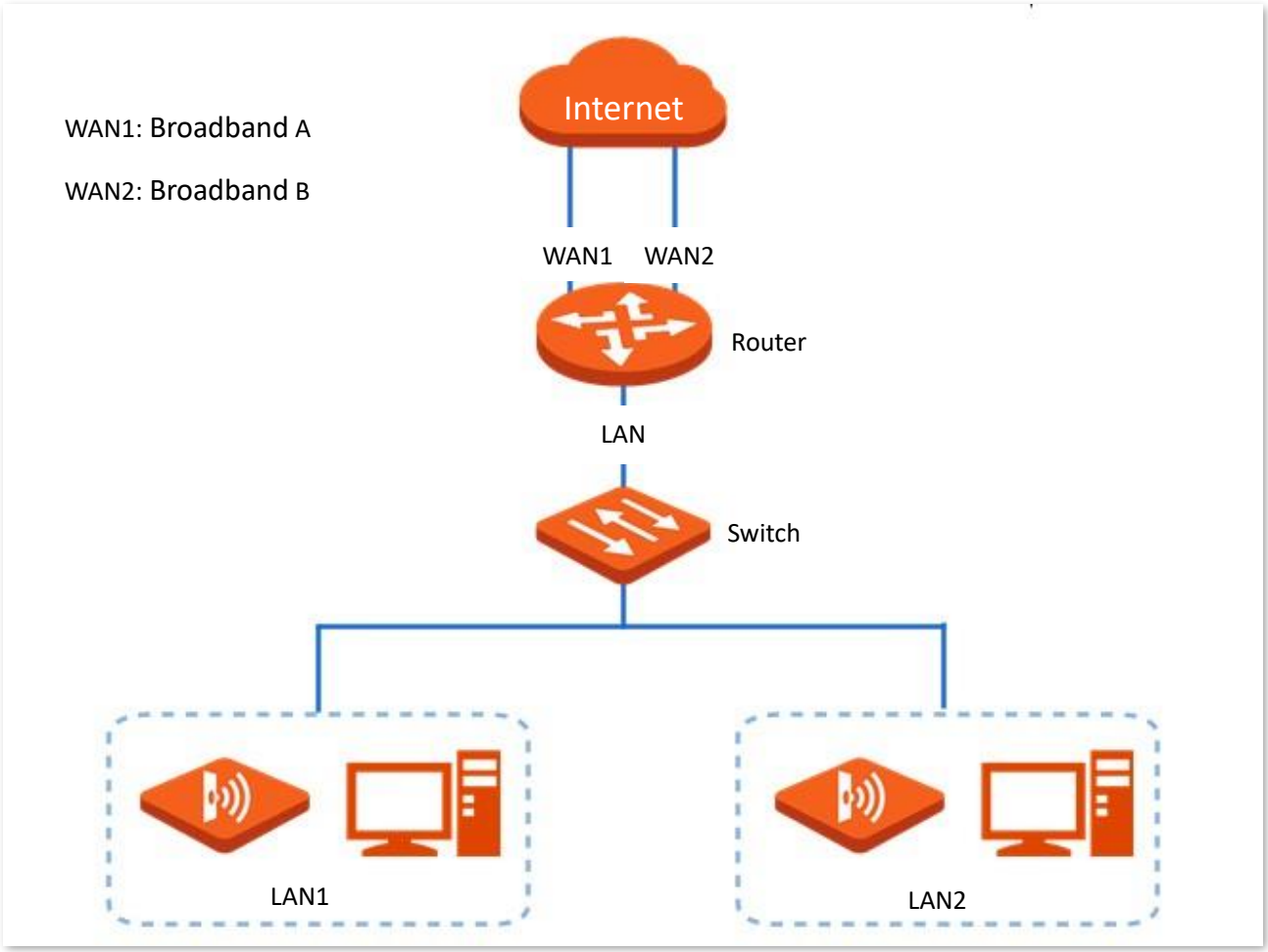
To achieve load balancing, the enterprise has the following requirements:

- Computers with IP addresses 192.168.0.2 to 192.168.0.100 access the internet through Broadband A.

- Computers with IP addresses 192.168.0.101 to 192.168.0.250 access the internet through Broadband B.

Solution

You can use the multi-WAN policy function of the router to meet this requirement.



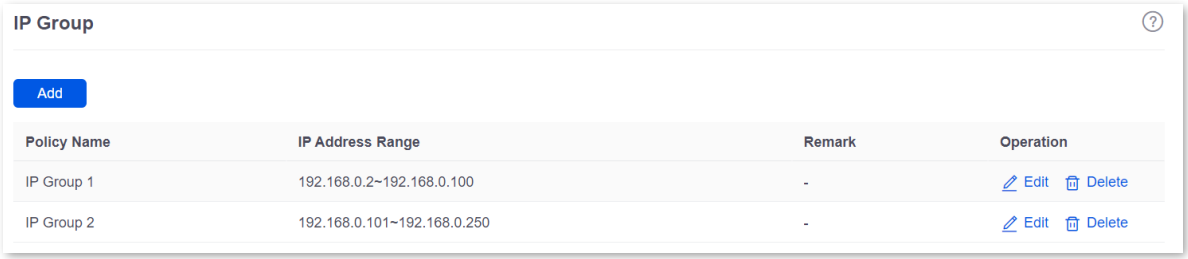
Configuration procedure

Set an IP group → Enable the multi-WAN policy function → Customize the multi-WAN policy

Step 1 Log in to the web UI of the router.

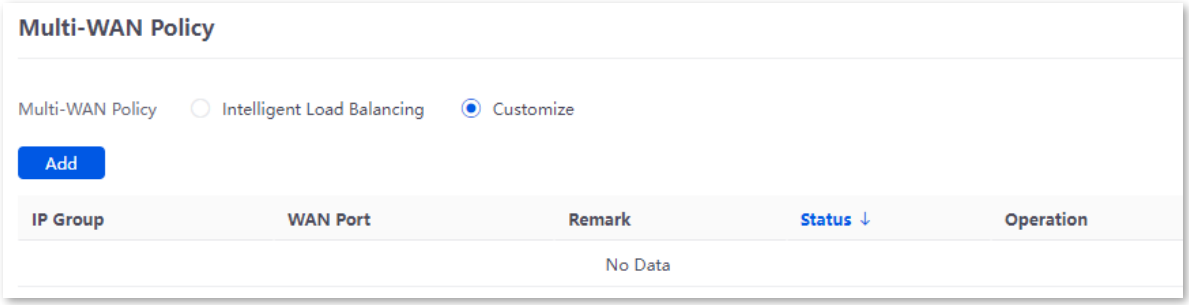
Step 2 Set an IP group.

Navigate to **Behavior** > **Group Policy** > **IP Group**, and click **Add** to configure the following two IP groups.



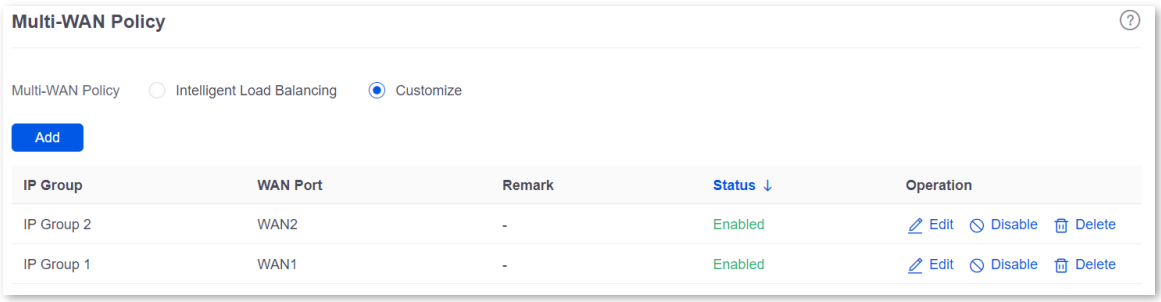
Step 3 Enable the multi-WAN policy function.

3. Navigate to **More** > **Advanced Routing** > **Multi-WAN Policy**.
4. Select **Customize** for **Multi-WAN Policy**.
5. Confirm the prompt information, and click **OK**.



Step 4 Customize the multi-WAN policy.

Navigate to **More** > **Advanced Routing** > **Multi-WAN Policy**, and click **Add** to configure the following two multi-WAN policies.



----End

Verification

When a device in the LAN with an IP address in the range of 192.168.0.2 to 192.168.0.100 accesses the internet, the data traffic is forwarded by the WAN1 port. When a device in the LAN with an IP address in the range of 192.168.0.101 to 192.168.0.250 accesses the internet, the data traffic is forwarded by the WAN2 port.

8.1.3 Static routing

Overview

Routing is an operation to choose an optimum path to convey data from the source address to the target address. A static route is a manually configured special route and is simpler, more efficient, and more reliable. An appropriate static route can reduce issues arising from route selection and ease the overflow of route selection data flow, improving the rate of data packet forwarding.

You can specify a static route by setting **Target Network**, **Subnet Mask**, **Default Gateway** and **Interface**. Among these parameters, **Target Network** and **Subnet Mask** are used to specify a target network or host. After the static route is configured successfully, all the data whose target address is

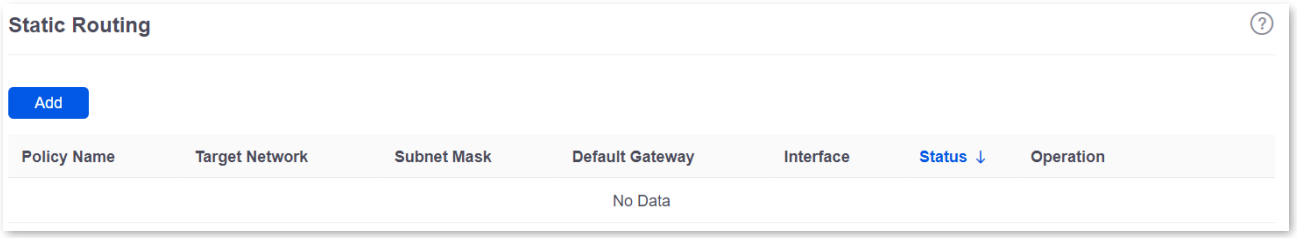
in the target network of the static routing is directly forwarded to the gateway address through the interface of the static route.

NOTE

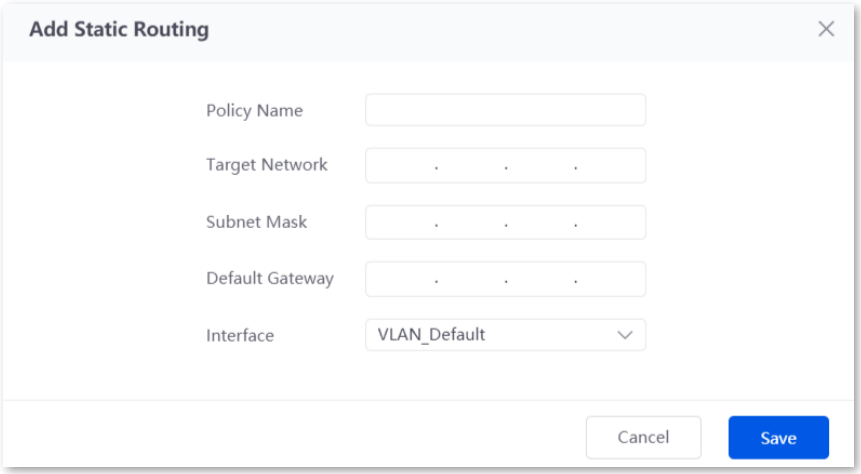
- If static routes are completely used in a large-scale and complicated network, route unavailability and network interruption may occur in case of network fault or topology change. Under such circumstances, the network administrator needs to manually change the static routing configurations.
- When a static routing policy conflicts with a customized multi-WAN policy, static routing takes precedence.

To access the configuration page, log in to the web UI of the router, and navigate to **More** > **Advanced Routing** > **Static Routing** to enter the page.

Here, you can configure the corresponding static routing according to actual network conditions.



You can click **Add** to add a new static routing policy.



Parameter description

Parameter	Description
Policy Name	Specifies the name of the static routing policy.
Target Network	Specifies the IP address of the target network. **0.0.0.0** target 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.

Parameter	Description
Subnet Mask	Specifies the subnet mask of the target 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 direct routing, which means that the target network is directly connected to the interface of the router.
Interface	Specifies the interface from which packets egress. Select it as required.
Status	Specifies the current policy status, including **Enabled** and **Disabled**.

Example of configuring static routing

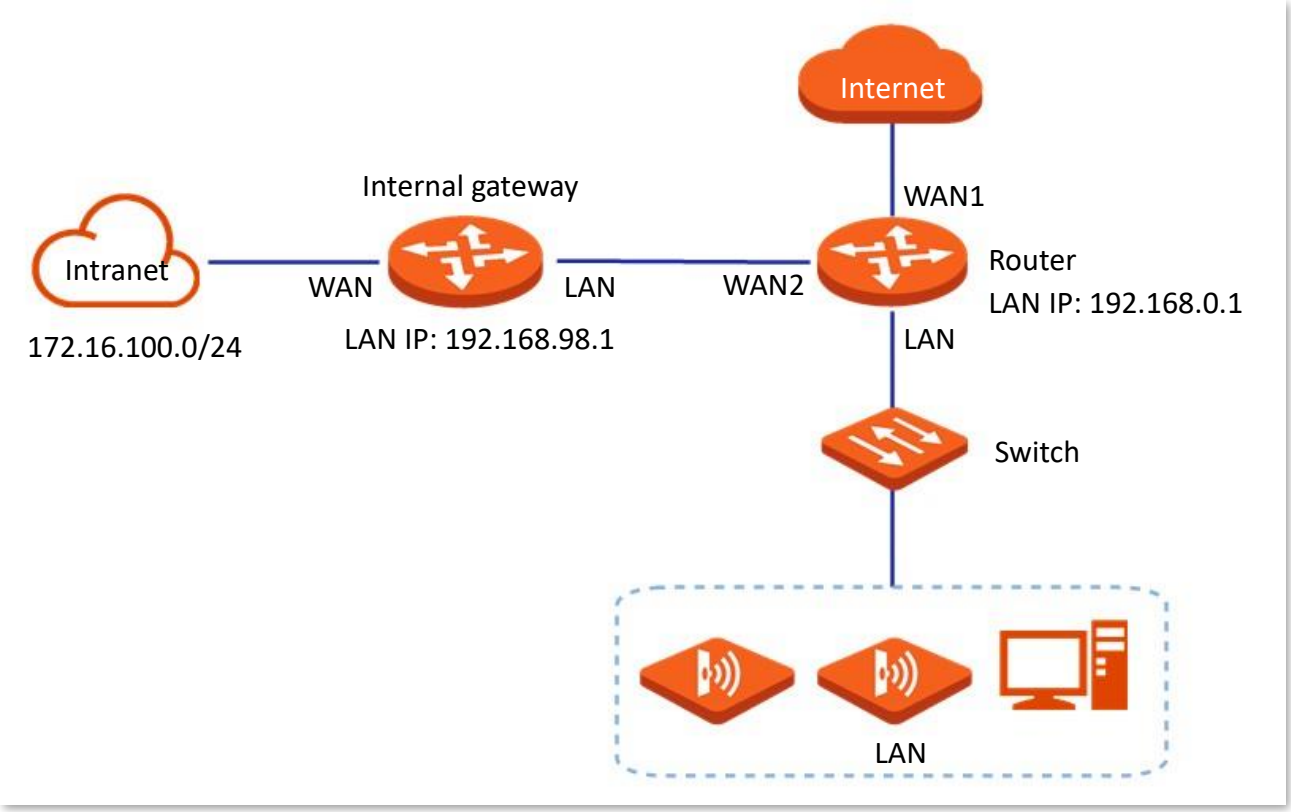
Networking requirements

An enterprise uses the wireless router to set up a network. The WAN1 port has been connected to the internet through PPPoE. Now the enterprise has set up an intranet, which is in a different network from the internet. The WAN2 port is connected to the enterprise's intranet through dynamic IP address.

The enterprise has the following requirements: LAN users can access both the internet and the intranet.

Solution

You can use the Static Routing function to meet the requirements.



Configuration procedure

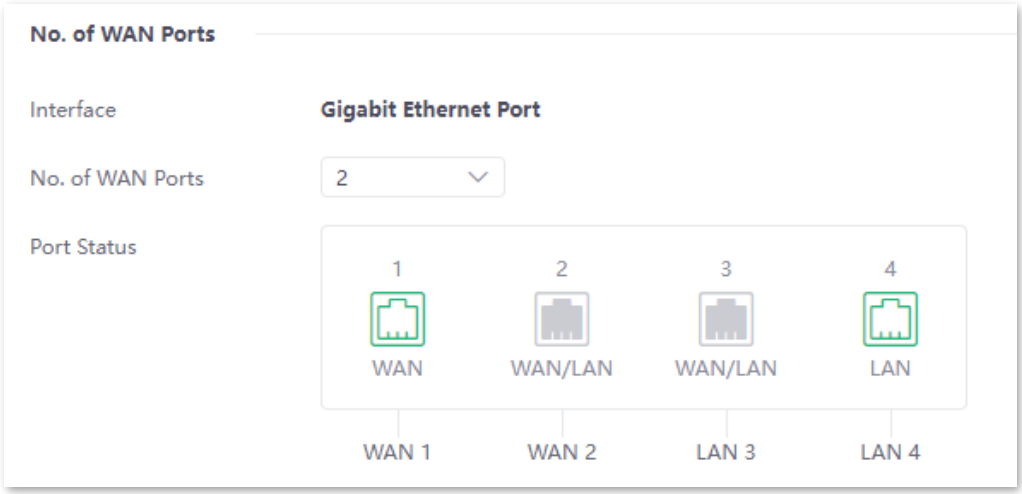
Enable two WAN ports and connect WAN2 port to the internet → Configure the static routing

Step 1 Log in to the web UI of the router.

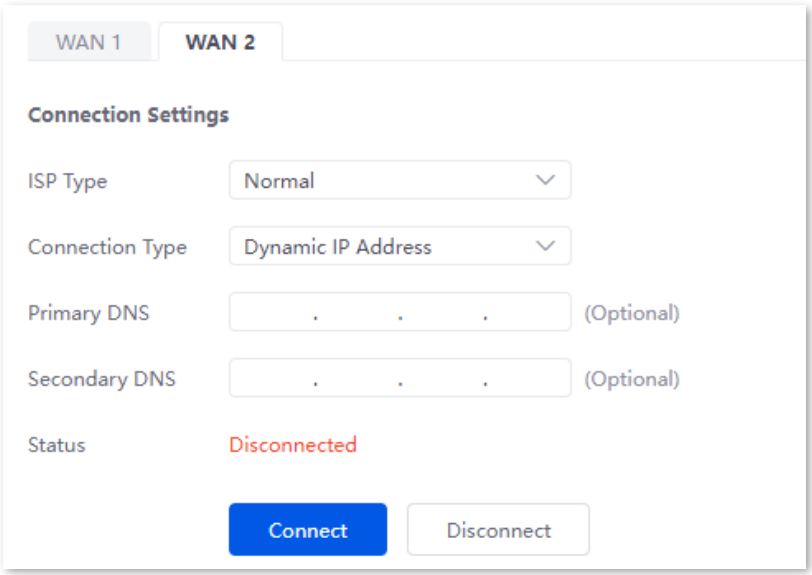
Step 2 Enable two WAN ports and connect WAN2 port to the internet.

1. Navigate to **Network** > **Internet Settings**.
2. Set **No. of WAN Ports** to **2**.
3. Confirm the prompt information and click **OK**. The router will reboot.

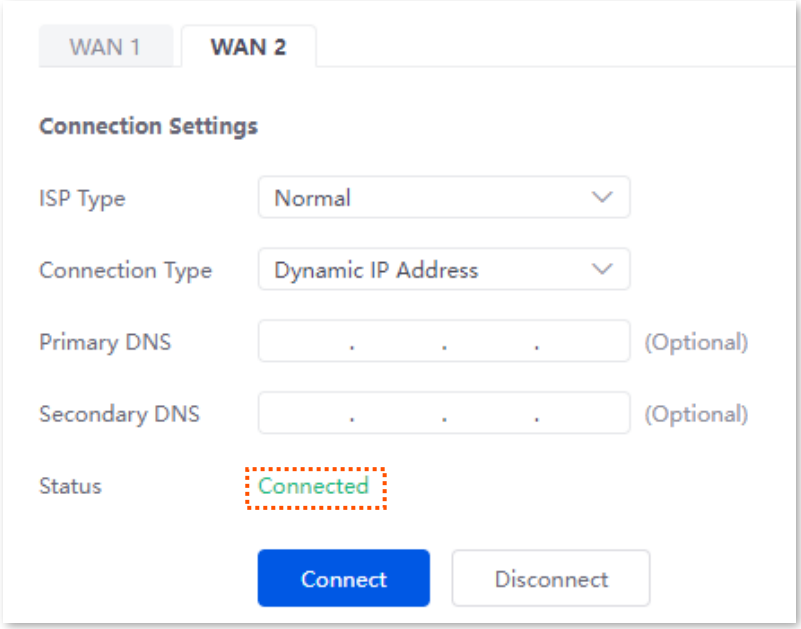
   Wait until the router complete rebooting. Click **Network** > **Connection Status**.



4. Under **WAN2**, select **Dynamic IP Address** for **Connection Type**, and click **Connect**.



When the **Status** is **Connected**, the WAN2 port is successfully connected to the network.



Step 3 Configure the static routing.

1. Obtain the IP address information of the WAN2 port.

   Click **System,** click the drop-down box next to **WAN Real-time Rate** to select **WAN2**, and view the IP address information obtained by WAN2 under **Connection Status**, assuming the following:

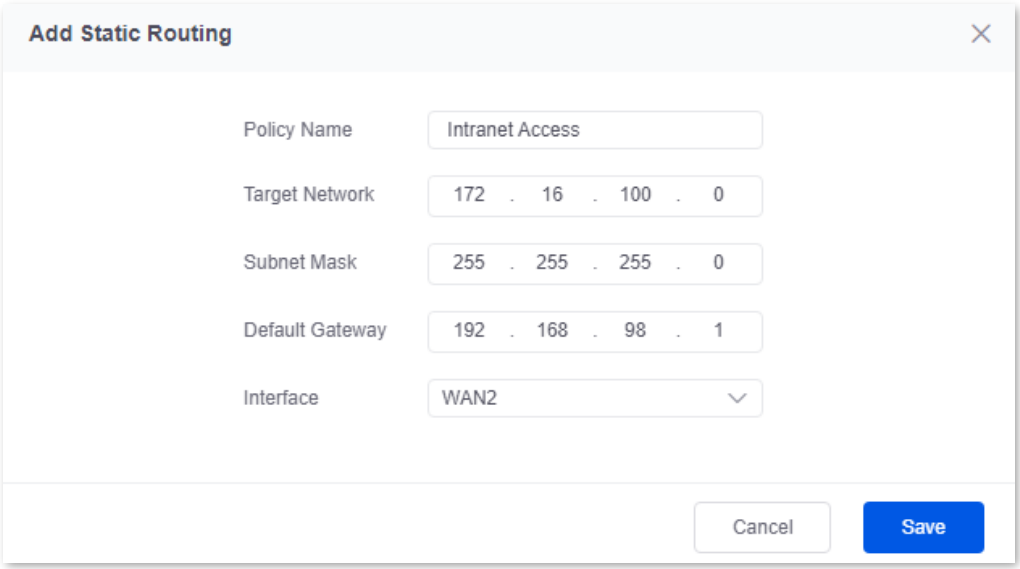
WAN2 IP Address	Subnet Mask	Default Gateway	Primary DNS
192.168.98.190	255.255.255.0	192.168.98.1	192.168.98.1

2. Configure parameters of the static routing.

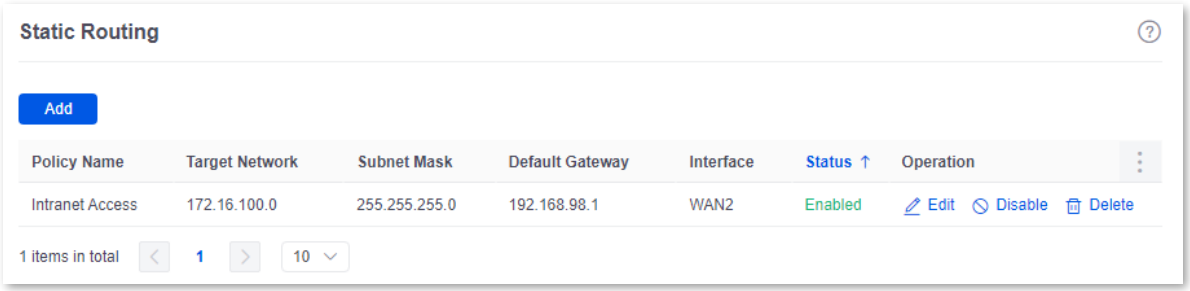
   The following table lists the static routing parameters for example:

Policy Name	Target Network	Subnet Mask	Default Gateway	Interface
Intranet Access	172.16.100.0	255.255.255.0	192.168.98.1	WAN2

   Navigate to **More** > **Advanced Routing** > **Static Routing**, click **Add** to configure parameters in the **Add Static Routing** window, and click **Save**.



Added successfully. See the following figure.



----End

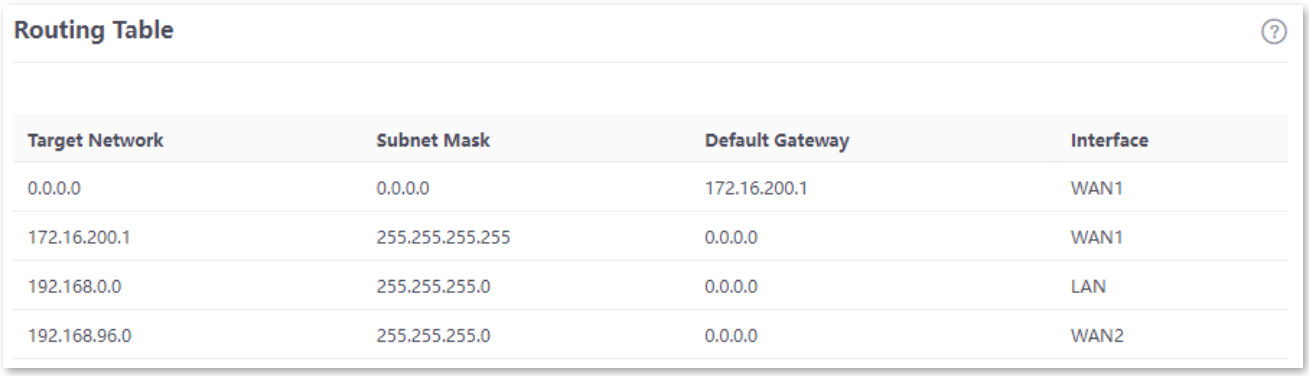
Verification

LAN users can access both the internet and the intranet.

8.1.4 Routing table

To access the configuration page, log in to the web UI of the router, and navigate to **More** > **Advanced Routing** > **Routing Table** to enter the page.

Here, you can view the detailed routing information of the router.



Parameter description

Parameter	Description
Target Network	Specifies the IP address of the destination network. If both the destination network and subnet mask are 0.0.0.0, it is the default route. TIP When a route that exactly matches the destination address of the packet cannot be found in the routing table, the router will select the default route to forward the packet.
Subnet Mask	Specifies the subnet mask of the destination network.
Default Gateway	Specifies the ingress IP address of the next hop router of data packets. The default gateway is 0.0.0.0, which means direct routing, that is, the destination network is the network directly connected to the interface of the router.
Interface	Specifies the interface of the router that data packets are forwarded.

8.1.5 Policy routing

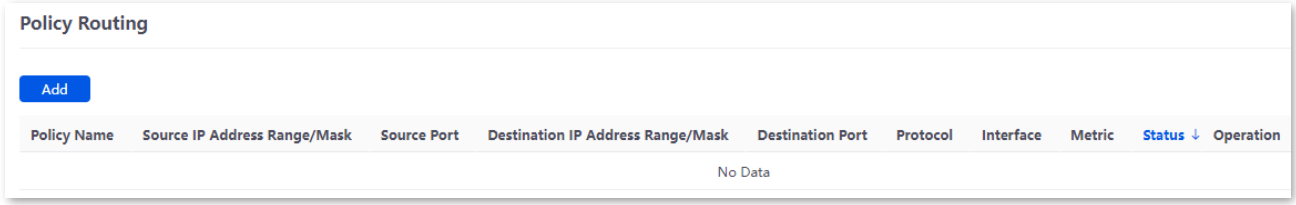
Overview

Policy routing, also known as policy-based routing, means that the next hop forwarding address of an IP packet is determined by a comprehensive consideration of multiple factors, rather than the destination or source IP address. You can set the source network, target network, destination port, protocol and WAN port with the policy routing for more accurate route selection.

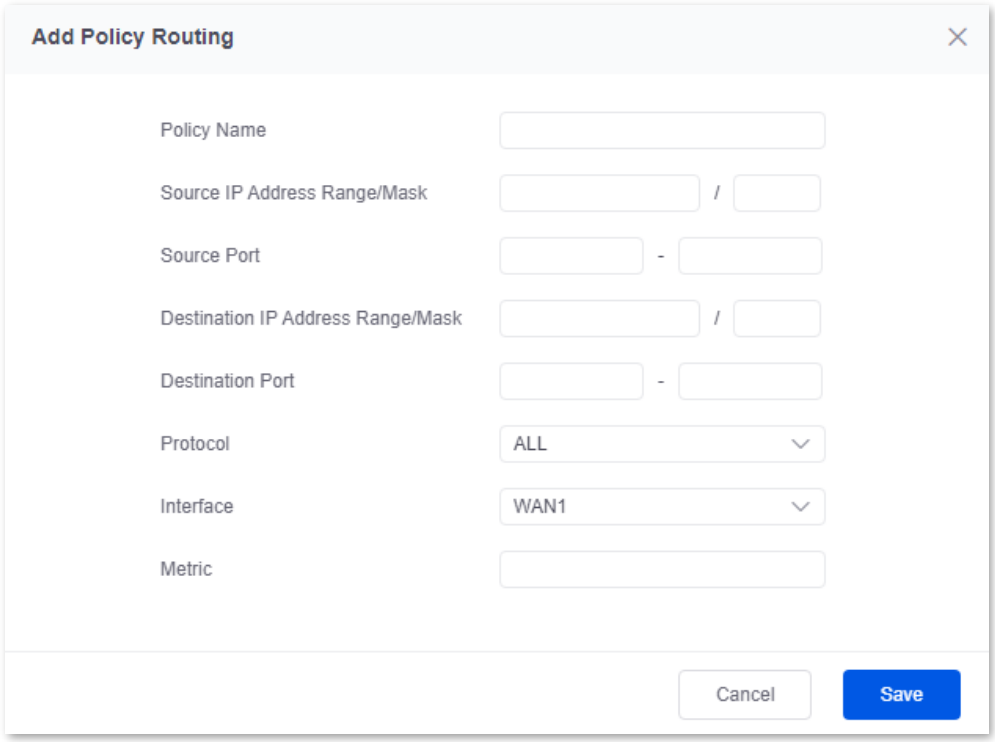
With this function enabled, the router will forward the data packets that meet the policy conditions to the specified target network through the specified WAN port.

To access the configuration page, log in to the web UI of the router, and navigate to **More** > **Advanced Routing** > **Policy Routing** to enter the page.

Here, you can configure the policy routing as required.



You can click **Add** to add a new policy routing policy.



Parameter description

Parameter	Description
Policy Name	Specifies the name of the policy routing rule.

Parameter	Description
Source IP Address Range/Mask	Specifies the source IP address range of data packets.
Source Port	Specifies the source port of data packets.
Destination IP Address Range/Mask	Specifies the destination IP address range to which data packets are forwarded.
Destination Port	Specifies the port of the device to which data packets are forwarded, which ranges from 1 to 65535.
Protocol	Specifies the protocol type of data packets. - **ALL**: If you are not sure about the protocol type, **ALL** is recommended. - **TCP**: Transmission Control Protocol is a common protocol that provides reliable data transmission. - **UDP**: User Datagram Protocol is a simple packet-oriented communication protocol.
Interface	Specifies the physical port for which the policy takes effect. Data packets that meet the conditions of the policy routing will be forwarded through this port.
Metric	Specifies the metric of the policy. A smaller metric indicates a higher priority for policy routing. The metric value ranges from 1 to 9999.
Status	Specifies the status of the policy routing rule, including **Enabled**, **Disabled** and **Expired**.

Example of configuring policy routing

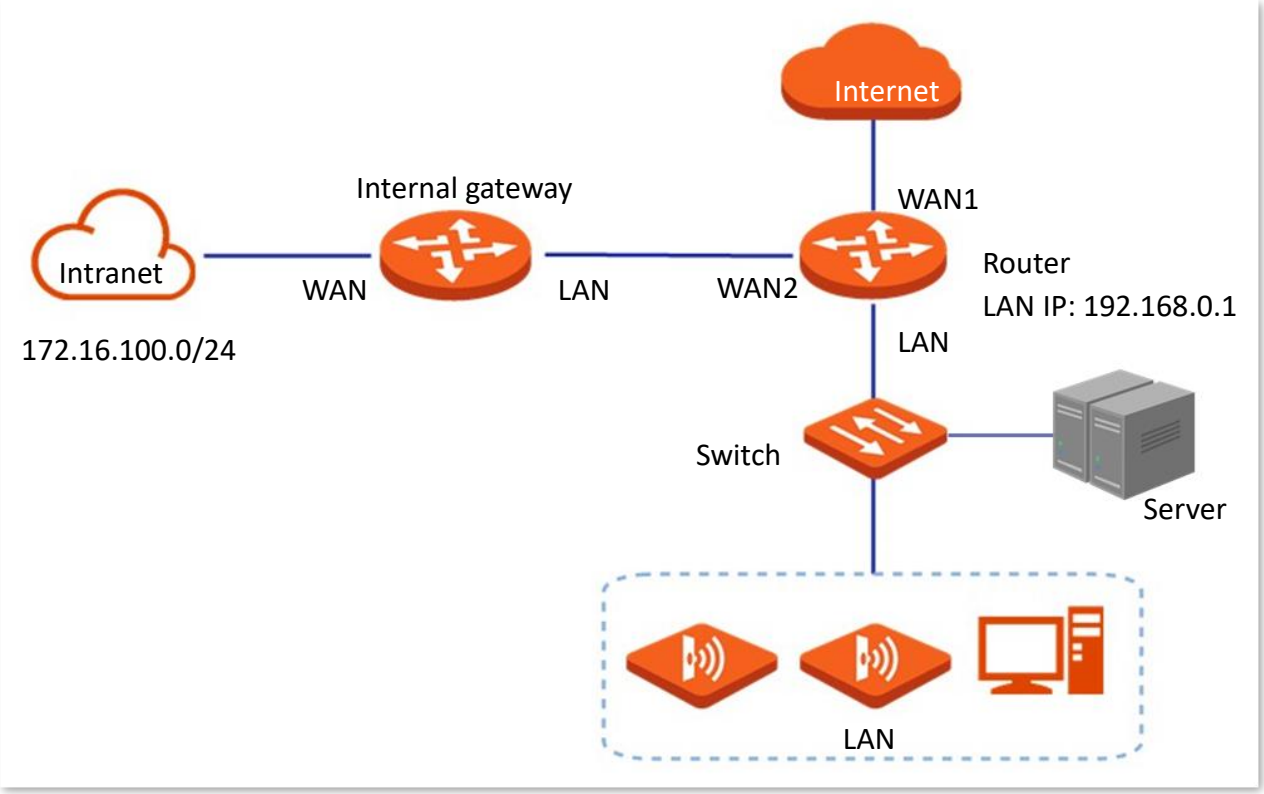
Networking requirements

An enterprise uses the wireless router to set up a network. The router is connected to the internet through PPPoE. The enterprise has built a Web server on the intranet, which is in a different network from the internet. The access mode of the enterprise's intranet is dynamic IP address.

The enterprise has the following requirements: Users whose LAN addresses are 192.168.0.2 to 192.168.0.254 can access both the internet and the Web server of the enterprise's intranet (the port number is 9999).

Solution

You can use the Policy Routing function to meet the requirements.



Configuration procedure

Enable two WAN ports and connect WAN2 port to the internet → Configure the policy routing

Step 1 Log in to the web UI of the router.

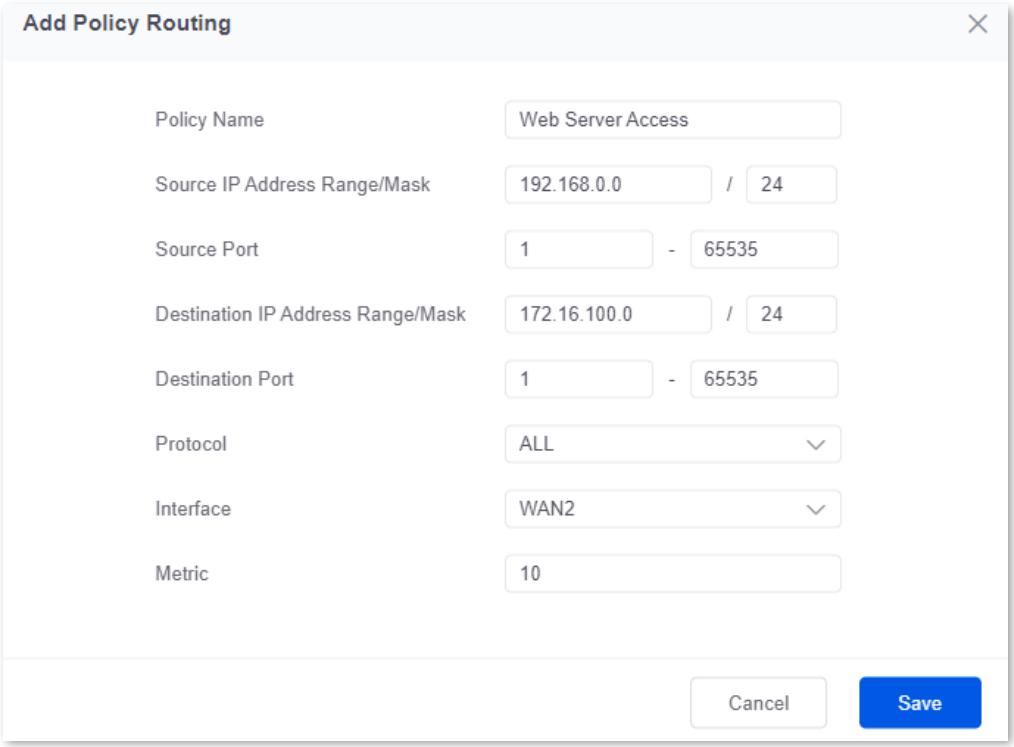
Step 2 Enable two WAN ports and connect WAN2 port to the internet.

Step 3 Configure the policy routing.

The following table provides the examples of policy routing parameters.

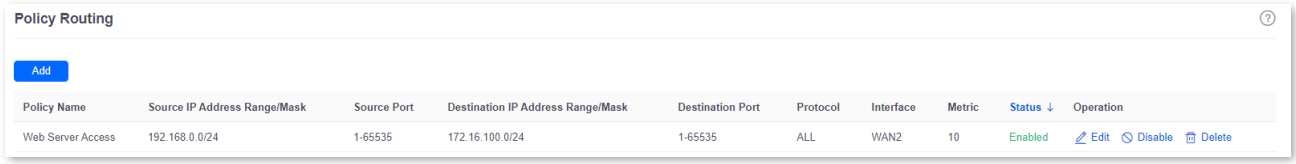
Policy Name	Source IP Address Range/Mask	Source Port	Destination IP Address Range/Mask	Destination Port	Protocol	Interface	Metric
Web Server Access	192.168.0.0/24	1–65535	172.16.100.0/24	1–65535	ALL	WAN2	10

Navigate to **More** > **Advanced Routing** > **Policy Routing**, click **Add** to configure parameters in the **Add Policy Routing** window, and click **Save**.



----End

The policy routing is added successfully.



Verification

Users whose LAN addresses ranging from 192.168.0.2 to 192.168.0.254 can access both the internet and the intranet.

8.2 Virtual service

8.2.1 DMZ

Overview

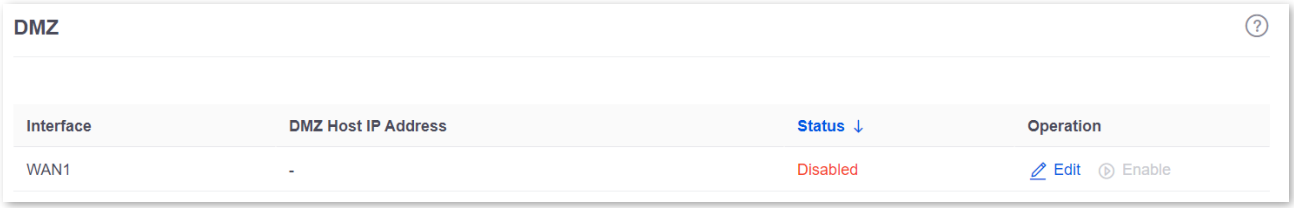
After a device in the LAN is set as the DMZ host, the device enjoys no limitations when communicating with the internet. For example, if video meeting or online games are underway on a computer, you can set that computer as the DMZ host to make the video meeting and online games go smoother.

NOTE

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

To access the configuration page, log in to the web UI of the router, and navigate to **More** > **Virtual Service** > **DMZ** to enter the page.

Here, you can modify the corresponding DMZ policy as required. The DMZ function is disabled by default.



Parameter description

Parameter	Description
Interface	Specifies the port whose DMZ service will be enabled. The default port is WAN1.
DMZ Host IP Address	Specifies the IP address of the device to be set as a DMZ host within the LAN.
Status	Specifies the status of the DMZ policy, including **Enabled** and **Disabled**.

Example of configuring DMZ

Networking requirements

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

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

Solution

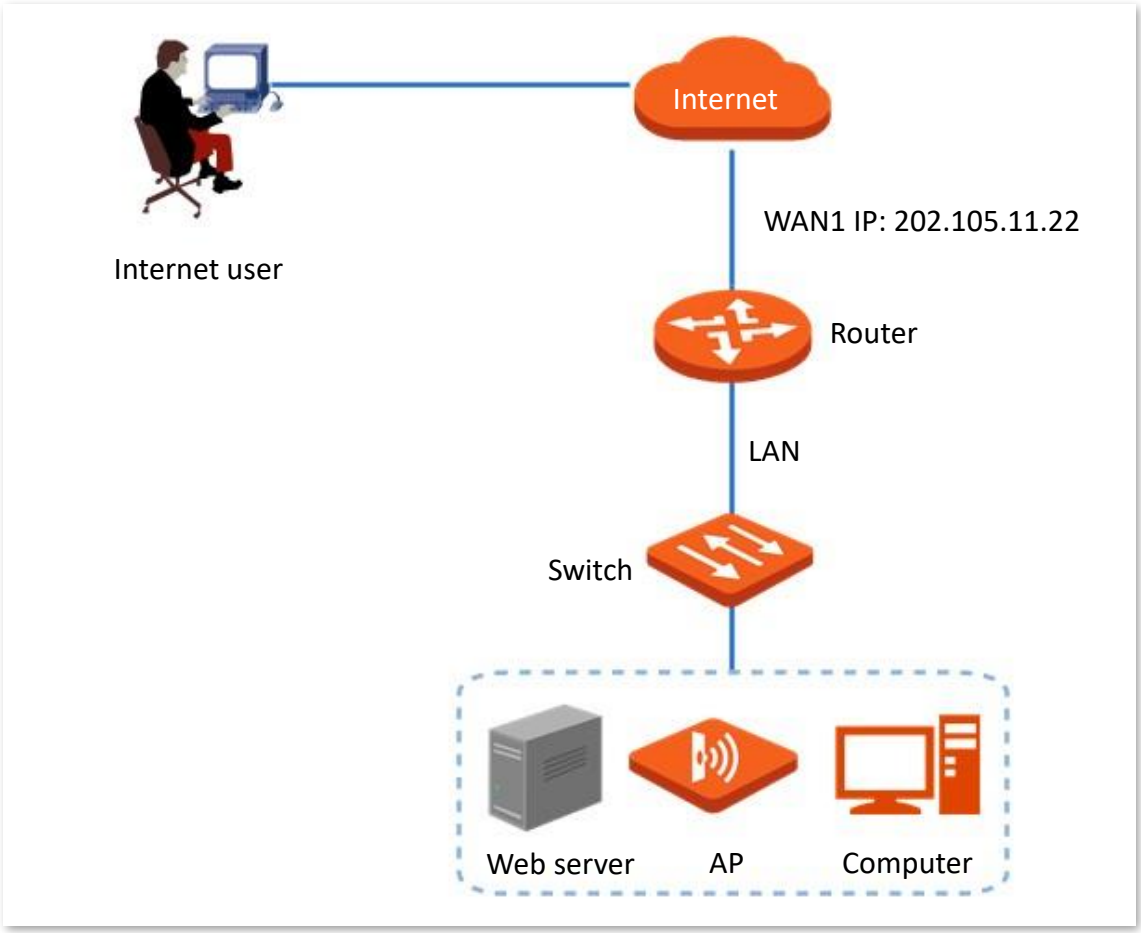
- You can use the DMZ function to enable internet users to access the intranet web server.
- You can use the DHCP Reservation function to avoid access failures caused by web server address change.

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, the DMZ function may not take effect. Common IPv4 addresses are classified into class A, class B and class C. Private IP addresses of class A range from 10.0.0.0 to 10.255.255.255. Private IP addresses of class B range from 172.16.0.0 to 172.31.255.255. Private IP addresses of class C range from 192.168.0.0 to 192.168.255.255.
- ISPs may not support unreported web service accessed using the default port number 80. Therefore, when setting DMZ host, you are recommended to set the external port as a non-familiar port (1024 to 65535), such as 9999, to ensure normal access.



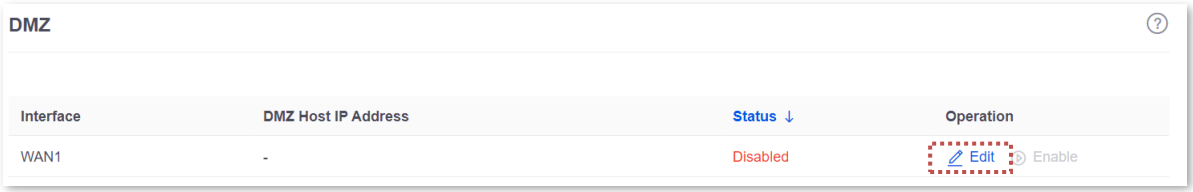
Configuration procedure

Set the DMZ host → Reserve a fixed IP address for the DMZ host

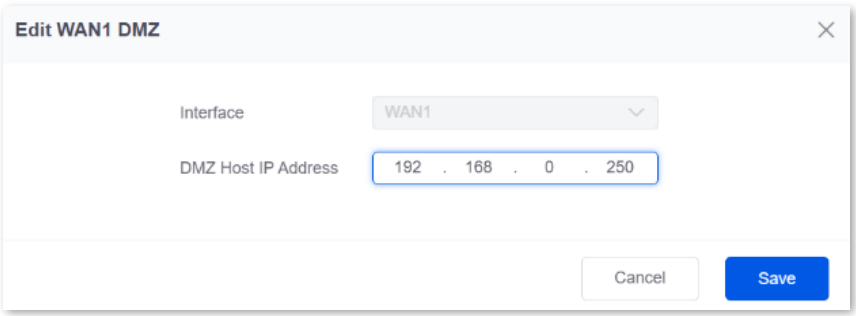
Step 1 Log in to the web UI of the router.

Step 2 Set the DMZ host.

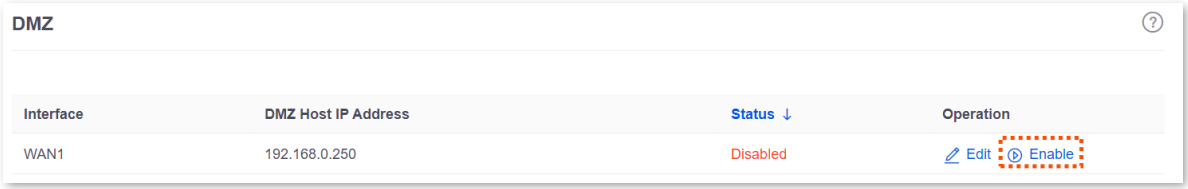
1. Navigate to **More** > **Virtual Service** > **DMZ**.
2. Locate the corresponding WAN port, and click **Edit.**



3. Set **DMZ Host IP Address** (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**.

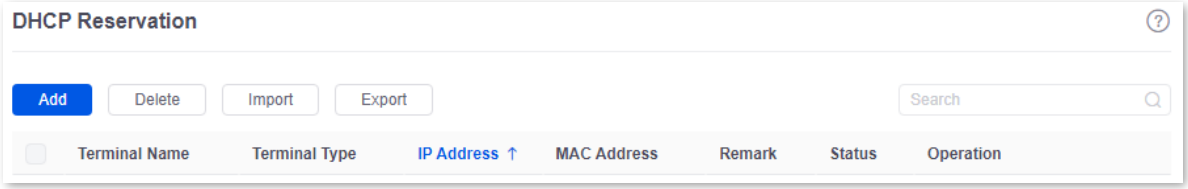


5. Click **Enable**.



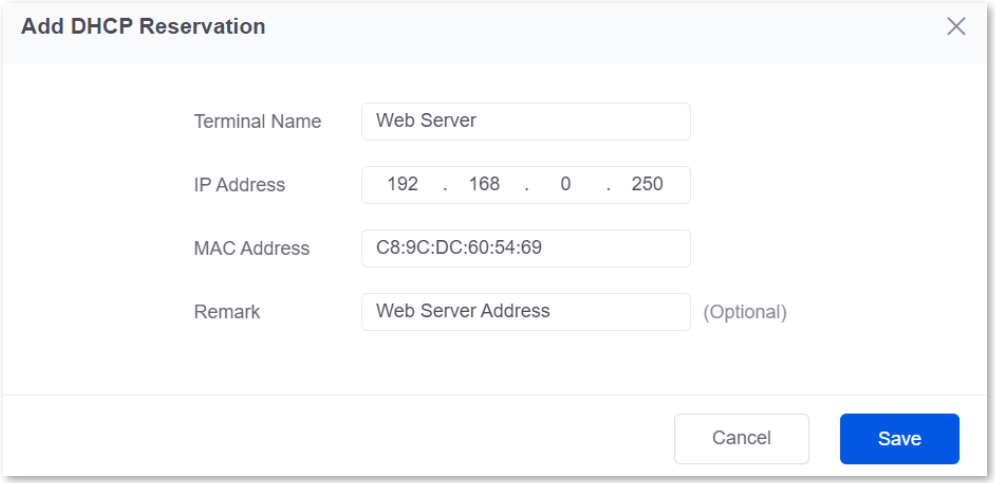
Step 3 Reserve a fixed IP address for the DMZ host.

1. Navigate to **Network** > **DHCP Reservation**, and click **Add**.



2. Set the following rules, and click **Save**.
   - Set **Terminal Name**, which is **Web Server** in this example.
   - Set **IP Address** to the fixed IP address assigned to the server host, which is **192.168.0.250** in this example.

- Set **MAC Address** of the server host, which is **C8:9C:DC:60:54:69** in this example.
- Set **Remark**, which is **Web Server Address** in this example.



----End

Verification

Internet users can successfully access the intranet server by using the **Intranet service application layer protocol name**://**WAN port IP address**. If the intranet service port is not the default port number, the access address is **Intranet service application layer protocol name**://**WAN port IP address**:**Intranet service port**.

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

You can find the router's current WAN port IP address in **Connection Status**.

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: Intranet service port**.

8.2.2 DDNS

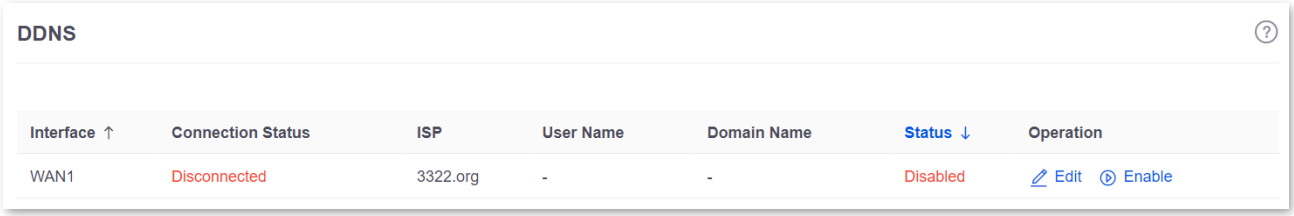
Overview

DDNS is abbreviated for Dynamic Domain Name Service. When a service is running, the DDNS client 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 mapping and DMZ host to enable internet users to access the LAN server or the web UI of the router through a domain name without caring about the change of the WAN IP address.

To access the configuration page, log in to the web UI of the router, and navigate to **More** > **Virtual Service** > **DDNS** to enter the page.

The router has created a corresponding DMZ policy for each WAN port by default, and the status is **Disabled**. On this page, you can modify the DDNS policies as required.



Parameter description

Parameter	Description
Interface	Specifies the port for which the DDNS service is enabled.
Connection Status	Specifies the connection status between the router and the domain server.
ISP	Specifies the service provider of DDNS. TIP You need to sign up at the website of the ISP for an account before configuring the DDNS service.
User Name	Specifies the user name for logging in to the DDNS service. The user name is the login user name that you have signed up at the website of the ISP.
Domain Name	Specifies the domain name information provided by the DDNS service provider. Except for **oray.com**, you have to manually enter the domain name that you have applied at the corresponding website when you use services from other service providers.
Status	Specifies the status of the DDNS service policy, including **Enabled**, **Disabled** and **Expired**.

Example of configuring DDNS

Networking requirements

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

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

Solution

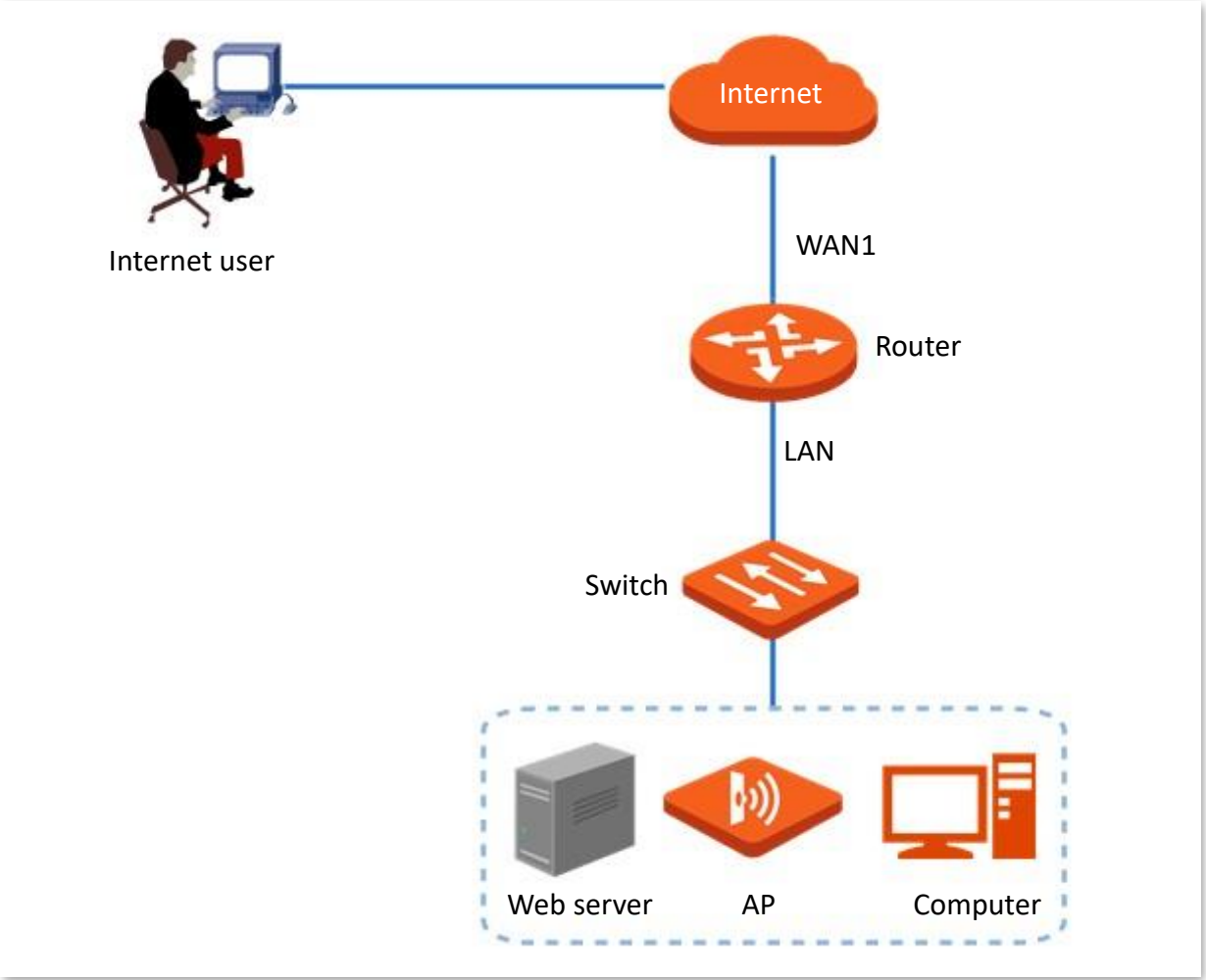
- You can use the Port Mapping function to enable internet users to access the intranet web server.
- You can use the DDNS function to enable internet users to access the intranet web server through a fixed domain name, avoiding access failures caused by WAN IP address change.
- You can use the DHCP Reservation function to avoid access failures 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, the DDNS function may not take effect. Common IPv4 addresses are classified into class A, class B and class C. Private IP addresses of class A range from 10.0.0.0 to 10.255.255.255. Private IP addresses of class B range from 172.16.0.0 to 172.31.255.255. Private IP addresses of class C range from 192.168.0.0 to 192.168.255.255.
- ISPs may not support unreported web service accessed using the default port number 80. Therefore, when setting port mapping, 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.



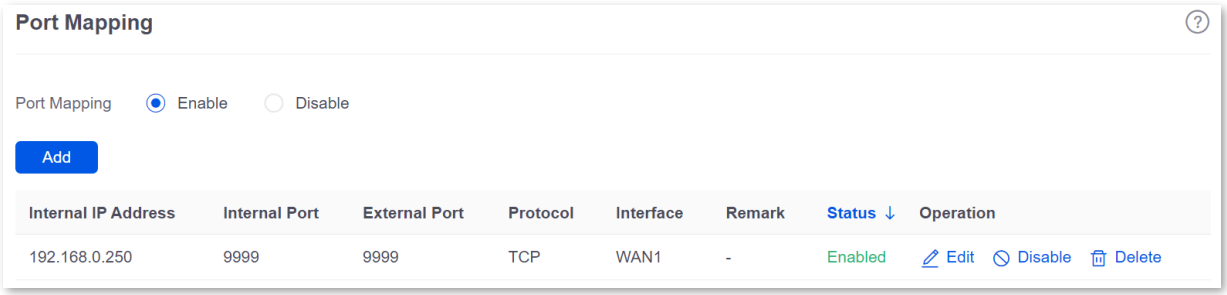
Configuration procedure

Set port mapping → Reserve a fixed IP address for the DMZ host → Set DDNS

Step 1 Log in to the web UI of the router.

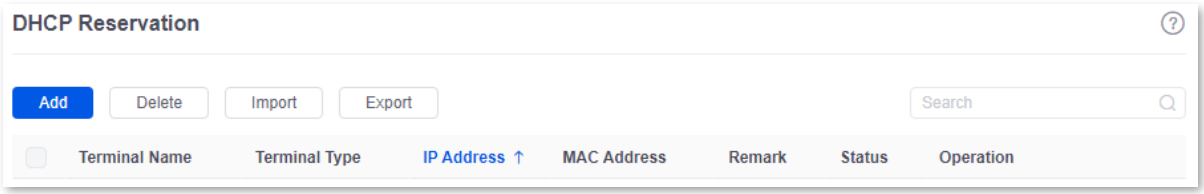
Step 2 Set port mapping.

Navigate to **More** > **Virtual Service** > **Port Mapping**, and set the following rules. If necessary, you can refer to Port mapping.

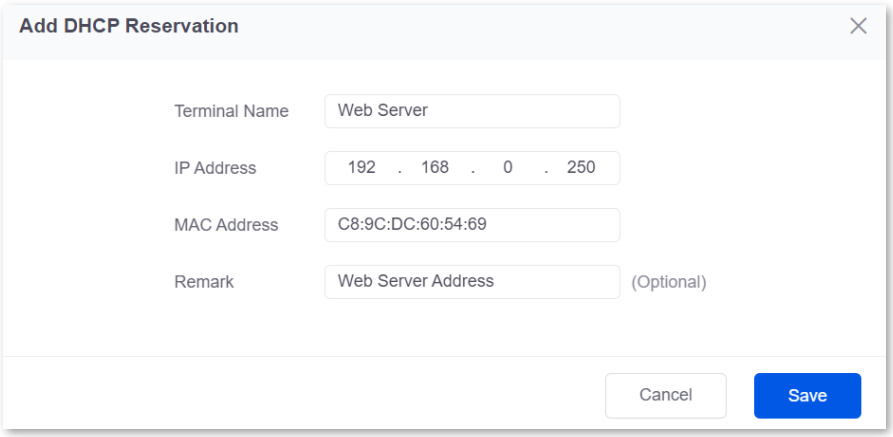


Step 3 Reserve a fixed IP address for the DMZ host.

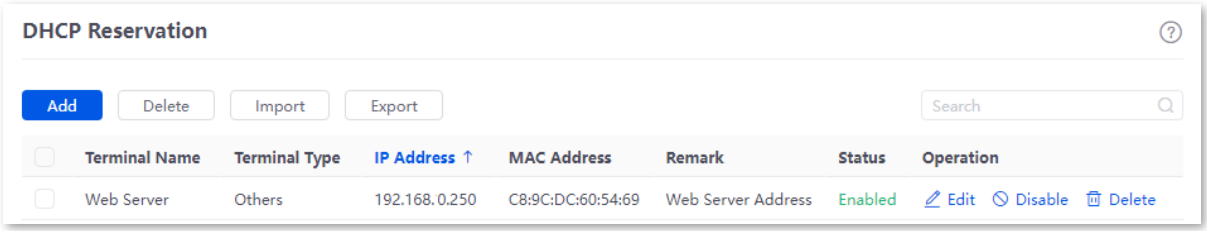
1. Navigate to **Network** > **DHCP Reservation**, and click **Add**.



2. Set the following rules, and click **Save**.
   - Set **Terminal Name**, which is **Web Server** in this example.
   - Set **IP Address** to the fixed IP address assigned to the server host, which is **192.168.0.250** in this example.
   - Set **MAC Address** of the server host, which is **C8:9C:DC:60:54:69** in this example.
   - Set **Remark**, which is **Web Server Address** in this example.



The fixed IP address is reserved successfully. See the following figure.



Step 4 Register a domain name.

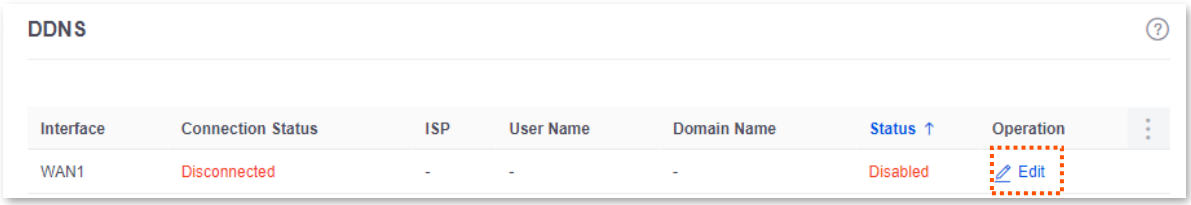
Log in to the DDNS provider website. Assume that the user name you registered is **JohnDoe**, the password is **JohnDoe123456**, and the domain name is **JohnDoe.3322.org**.

Step 5 Set DDNS.

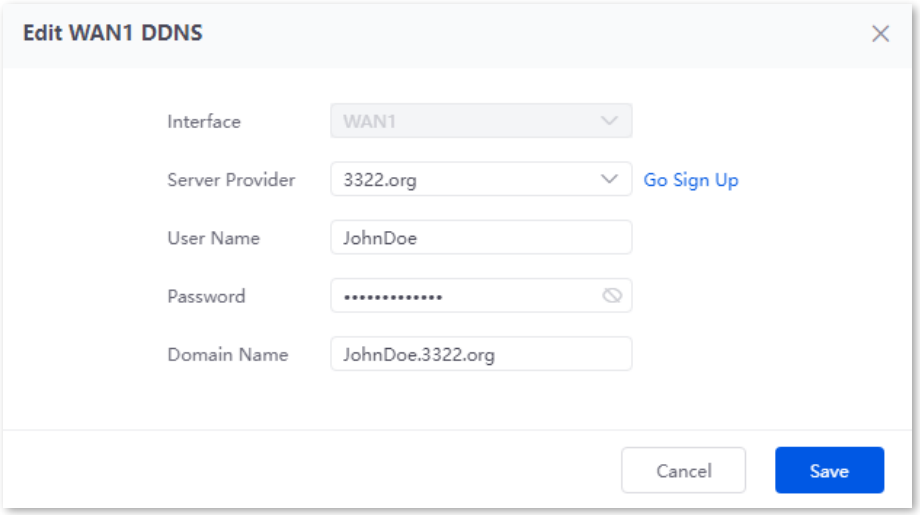
1. Register a domain name.

   Log in to the DDNS provider website. Assume that the user name you registered is **JohnDoe**, the password is **JohnDoe123456**, and the domain name is **JohnDoe.3322.org**.

2. Log in to the web UI of the router, and navigate to **More** > **Virtual Service** > **DDNS** to set DDNS.
3. Click **Edit** after the corresponding WAN port rule, which is **WAN1** in this example.



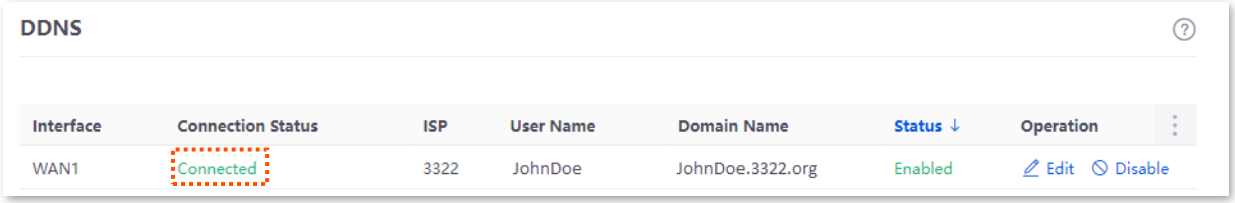
4. Configure the following parameters in the pop-up **Edit WAN1 DDNS** window, and then click **Save**.
   - Set **Server Provider** (the DDNS provider where you applied the domain name), which is **3322.org** in this example.
   - Set **User Name** and **Password**, which are **JohnDoe** and **JohnDoe123456** in this example.
   - Set **Domain Name**, which is **JohnDoe.3322.org** in this example.



5. Click **Enable**.

----End

The configuration is finished. Wait a moment, and refresh the page. When the **Connection Status** is **Connected**, the connection is successful.



Verification

Internet users can successfully access the intranet server by using the **Intranet service application layer protocol name**://**WAN port IP address**. If the intranet service port is not the default port

number, the access address is **Intranet service application layer protocol name**://**WAN port IP address**:**External port**.

In this example, the access address is http://JohnDoe.3322.org:9999.

TIP

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

- 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. Disable these programs and try again.

8.2.3 DNS hijacking

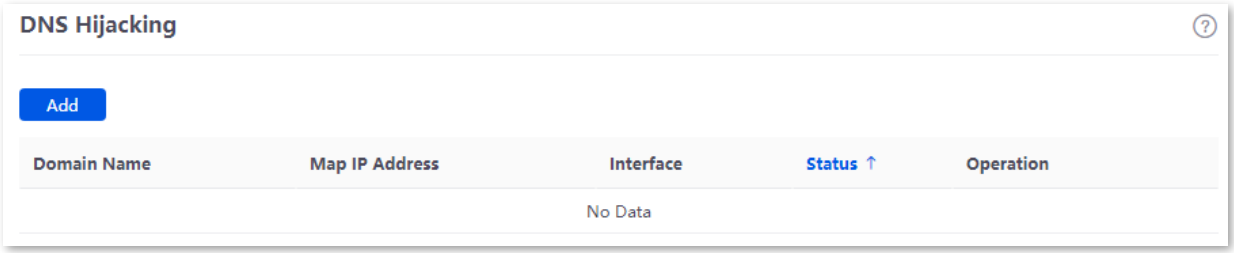
Overview

DNS is abbreviated for Domain Name Server, which is used to manage the relationships between the domain name and the IP address, and map the domain name and the IP address to each other.

After DNS hijacking is configured, when LAN users access the specified domain name, the domain name is directly parsed to the IP address corresponding to the access rule.

To access the configuration page, log in to the web UI of the router, and navigate to **More** > **Virtual Service** > **DNS Hijacking** to enter the page.

Here, you can configure the DNS hijacking policy as required.



Parameter description

Parameter	Description
Add	Used to add a new DNS hijacking policy.
Domain Name	Specifies the domain name to be hijacked.
Map IP Address	Specifies the IP address to be accessed after the hijacking.
Interface	Specifies the specified egress of the DNS hijacking policy.
Status	Specifies the current status of the DNS hijacking policy.

Example of configuring DNS hijacking

Networking requirements

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

When LAN users visit Amazon (Amazon.com), eBay (eBay.com) and other websites, they can access the web UI of the router.

Solution

The above requirements can be achieved using the DNS hijacking function of the router. Assume that the IP address of the router is 192.168.0.1.

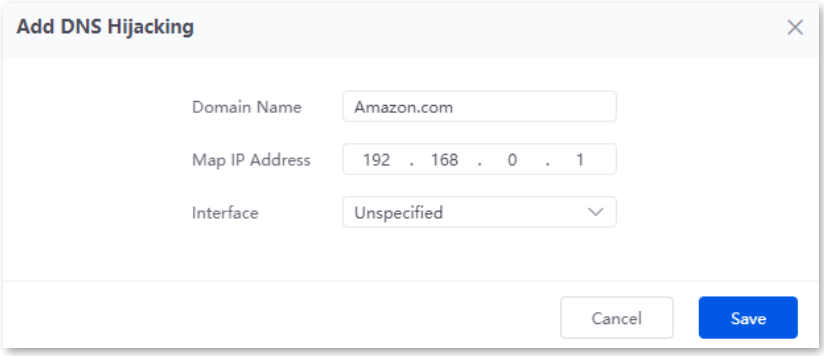
Configuration procedure

Step 1 Log in to the web UI of the router.

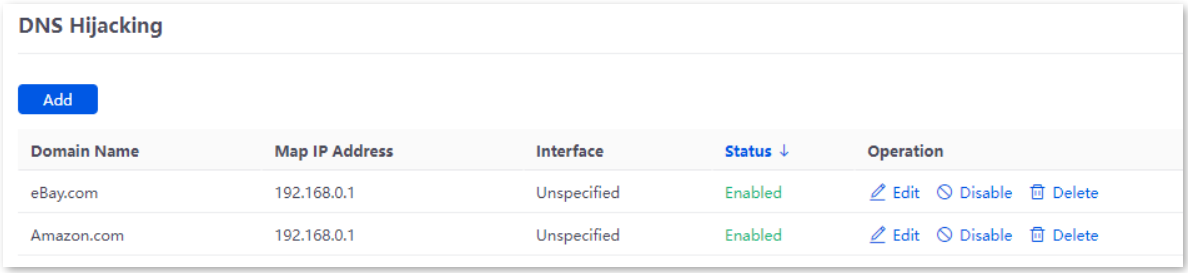
Step 2 Navigate to **More** > **Virtual Service** > **DNS Hijacking**, and click **Add**.

Step 3 Set the following rules of the DNS hijacking policy, and click **Save**.

1. Set **Domain Name** of Amazon, which is **Amazon.com** in this example.
2. Set **Map IP Address** of the router, which is **192.168.0.1** in this example.



Step 4 Refer to steps **2**-**3** to add a DNS hijacking policy whose domain name is eBay (eBay.com).



----End

Verification

When LAN users visit Amazon (Amazon.com) and eBay (eBay.com) websites, they always visit the web UI of the router.

8.2.4 IP hijacking

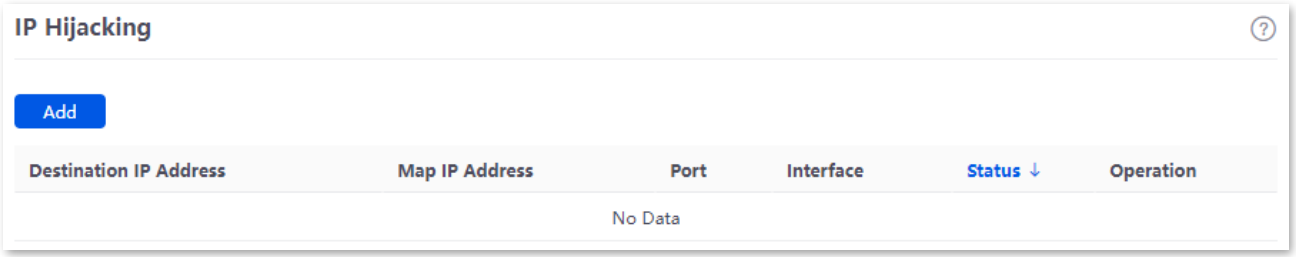
Overview

After IP hijacking is configured, when a LAN user accesses a port of the specified IP address, the IP address will be directly hijacked to the mapped address.

To access the configuration page, log in to the web UI of the router, and navigate to **More** > **Virtual Service** > **IP Hijacking** to enter the page.

Here, you can configure the IP hijacking policy as required.

Common ports: 443 (HTTPS protocol webpage service), 80 (HTTP protocol webpage service), 21 (FTP service) and so on.



Parameter description

Parameter	Description
Add	Used to add a new IP hijacking policy.
Destination IP Address	Specifies the IP address to which the IP hijacking policy applies.
Map IP Address	Specifies the IP address to be accessed after the hijacking.
Port	Specifies the port to which the IP hijacking policy applies. The IP addresses will be hijacked only when specified ports are accessed. TIP The value 0 indicates all ports.
Interface	Specifies the specified egress of the IP hijacking policy.
Status	Specifies the current status of the IP hijacking policy.

Example of configuring IP hijacking

Networking requirements

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

The LAN users are redirected to the web UI of the router when accessing 1.1.1.1.

Solution

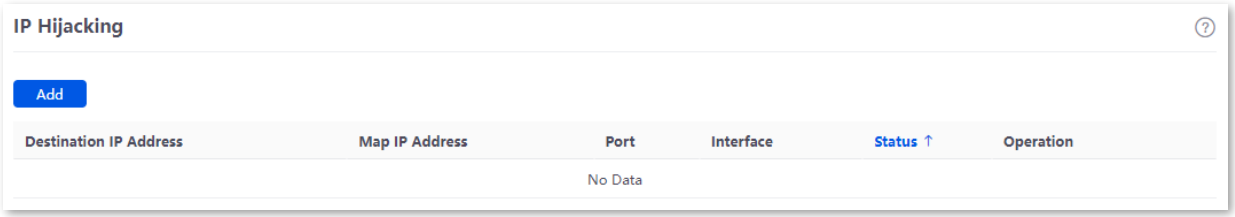
You can configure the IP hijacking function to meet the preceding requirements.

Assume that the management IP address of the router is 192.168.0.1 and the port number of the HTTPS web service is 443.

Configuration procedure

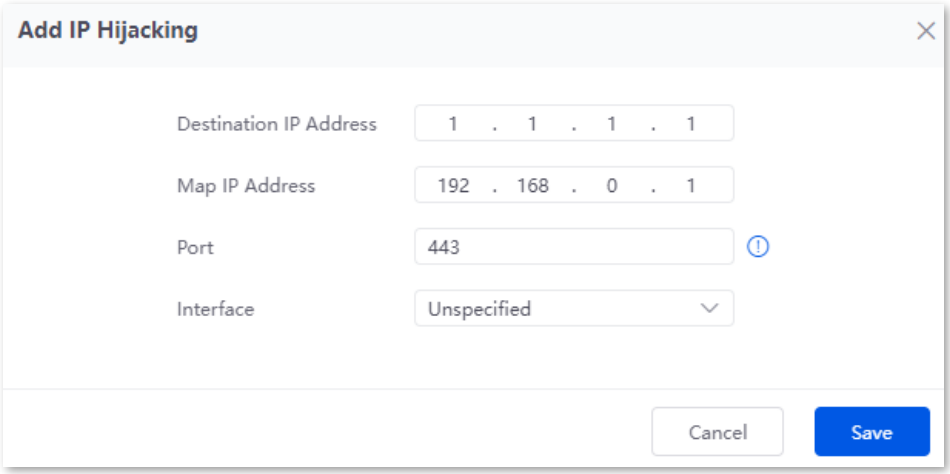
Step 1 Log in to the web UI of the router.

Step 2 Navigate to **More** > **Virtual Service** > **IP Hijacking**, and click **Add**.



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

1. Set **Destination IP Address**, which is **1.1.1.1** in this example.
2. Set **Map IP Address**, which is **192.168.0.1** in this example.
3. Set **Port**, which is **443** in this example.



----End

Verification

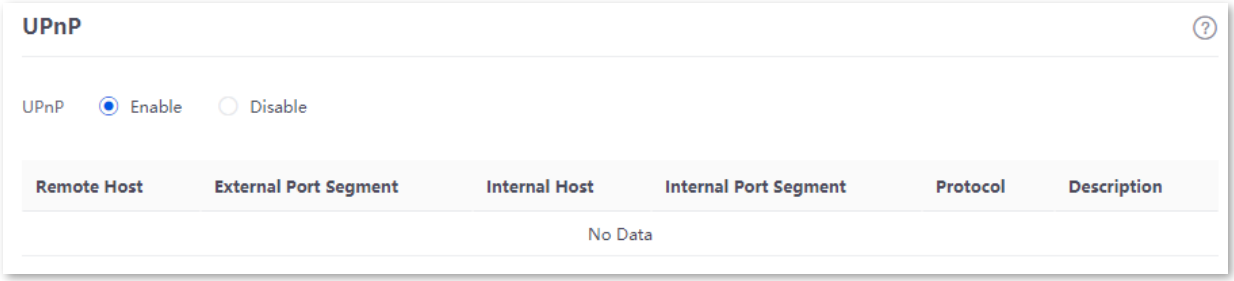
When LAN users access **1.1.1.1:443**, they actually access the web UI of the router.

8.2.5 UPnP

UPnP is abbreviated for Universal Plug and Play. After the UPnP function is enabled, the router can automatically open the ports for UPnP-supporting programs in the LAN (such as BitComet and AnyChat) and make these applications run smoother.

To access the configuration page, log in to the web UI of the router, and navigate to **More** > **Virtual Service** > **UPnP** to enter the page. The UPnP function is disabled by default.

After this function is enabled, when UPnP-supporting programs (such as BitComet) are running in the LAN, you can check the port switching information generated when application programs send requests.



Parameter description

Parameter	Description
Remote Host	Specifies the IP address of the remote server.
External Port Segment	Specifies the ports used by the remote server.
Internal Host	Specifies the server IP address for automatic port mapping of the LAN.
Internal Port Segment	Specifies the service port of the LAN server.
Protocol	Specifies the protocol type used for the service.
Description	Specifies the relevant information of the application.

8.2.6 Port mapping

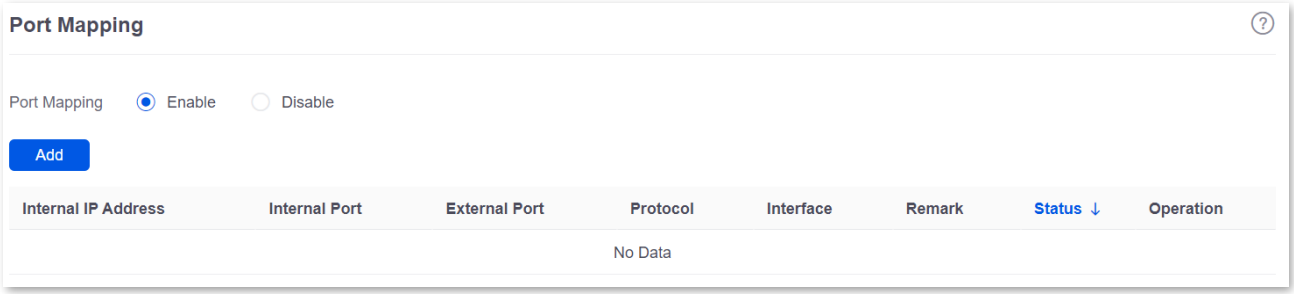
Overview

By default, users on the internet cannot access devices in the LAN. The Port Mapping function enables the router to open one or multiple service ports and specify the corresponding LAN server using the IP address and internal port. Therefore, visiting the ports from the internet are mapped to the LAN server. Such a function enables internet users to access the LAN server and prevents the LAN from being attacked.

To access the configuration page, log in to the web UI of the router, and navigate to **More** > **Virtual Service** > **Port Mapping** to enter the page.

Here, you can configure the port mapping policy as required.

The Port Mapping function is disabled by default. When it is enabled, the page is shown as below.



Parameter description

Parameter	Description
Internal IP Address	Specifies the IP address of the LAN host that needs to be mapped.
Internal Port	Specifies the service port of the LAN host.
External Port	Specifies the port opened by the router for access from internet users.
Protocol	Specifies the protocol type used by the LAN host. If you are not sure about the protocol type of the service, **TCP&UDP** is recommended.
Interface	Specifies the WAN port used by internet users to access the LAN host.
Remark	Specifies the description of the port mapping rule.
Status	Specifies the status of the port mapping policy, including **Enabled**, **Disabled** and **Expired**.

Example of configuring port mapping

Networking requirements

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

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

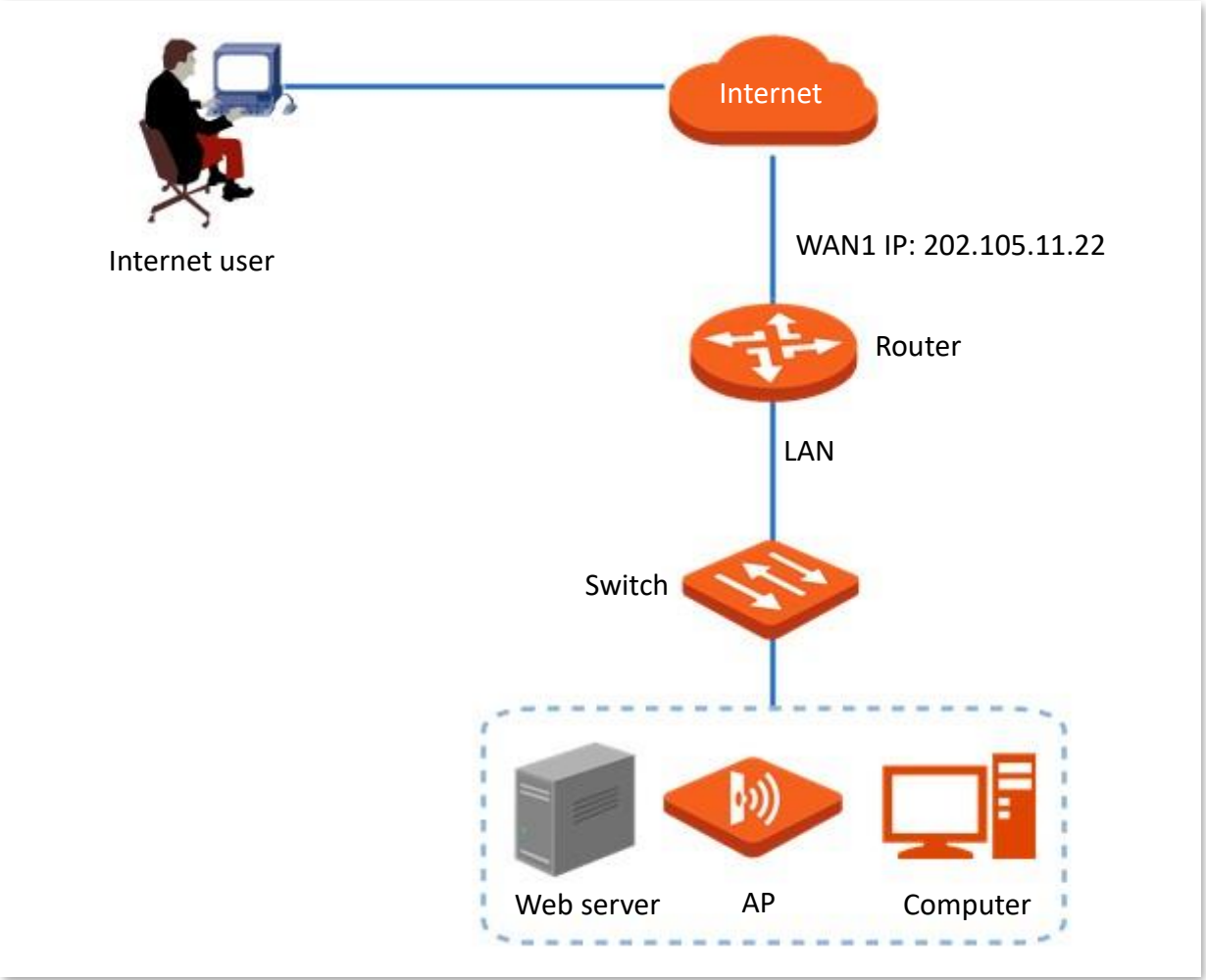
- You can use the Port Mapping function to enable internet users to access the intranet web server. Assume that the external network port opened by the router is 9999.
- You can use the DHCP Reservation function to avoid access failures caused by web server address change.

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, the Port Mapping function may not take effect. Common IPv4 addresses are classified into class A, class B and class C. Private IP addresses of class A range from 10.0.0.0 to 10.255.255.255. Private IP addresses of class B range from 172.16.0.0 to 172.31.255.255. Private IP addresses of class C range from 192.168.0.0 to 192.168.255.255.
- ISPs may not support unreported web service accessed using the default port number 80. Therefore, when setting port mapping, 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.



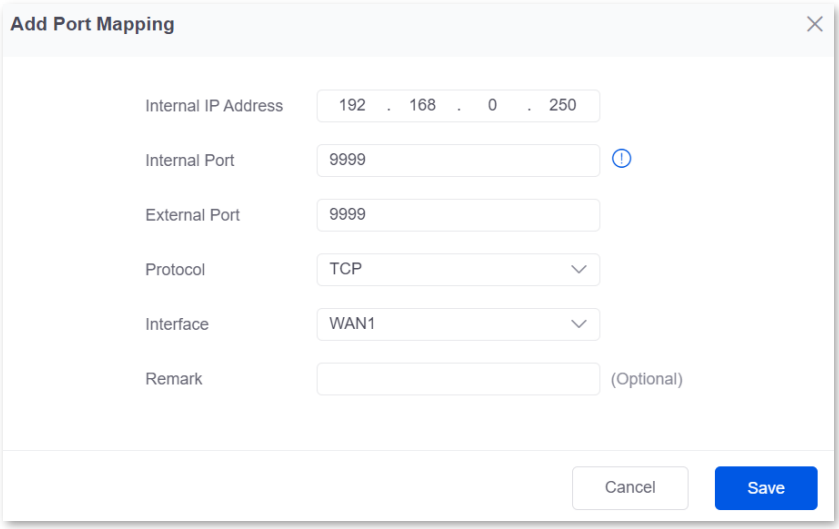
Configuration procedure

Set port mapping → Set the fixed IP address assigned to the server host

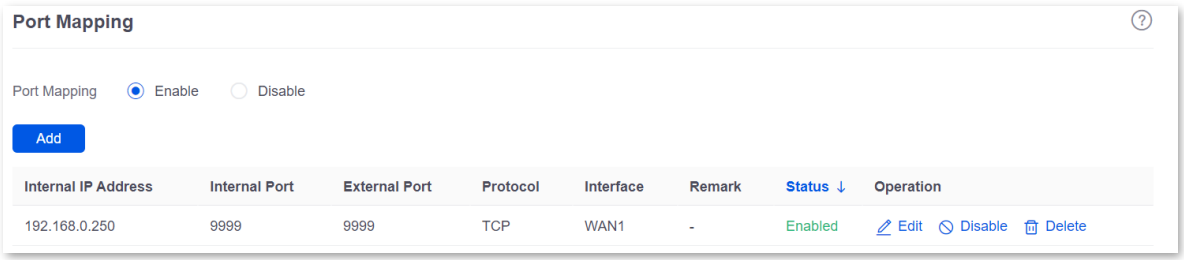
Step 1 Log in to the web UI of the router.

Step 2 Set port mapping.

1. Navigate to **More** > **Virtual Service** > **Port Mapping**.
2. Select **Enable** for **Port Mapping**, and click **Add**.
3. Configure parameters in the **Add** window, and click **Save**.
   - Set **Internal IP Address** (the IP address of the web server), which is **192.168.0.250** in this example.
   - Set **Intranet Port** (the port used by the web server), which is **9999** in this example.
   - Set **External Port** (the port that the router opens to WAN users), which is **9999** in this example.
   - Set **Protocol**, which is **TCP** in this example. If you are not sure about the protocol type of the service, **TCP&UDP** is recommended.
   - Set **Interface** (the WAN port used by Internet users to access the LAN server), which is **WAN1** in this example.

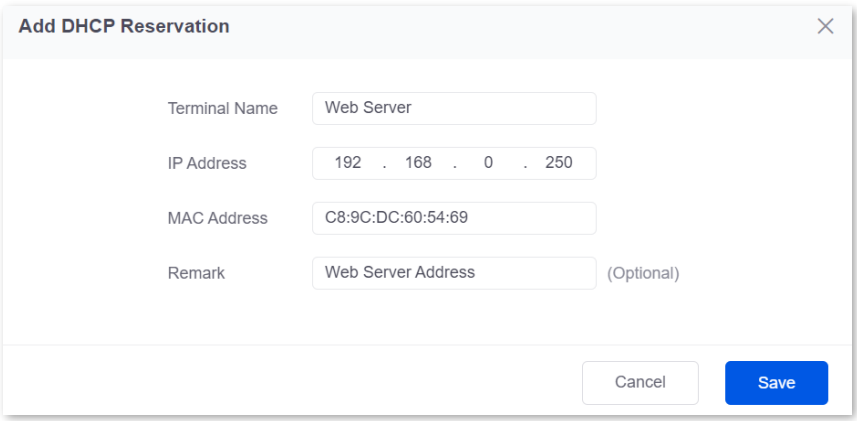


The port mapping policy is added successfully. See the following figure.



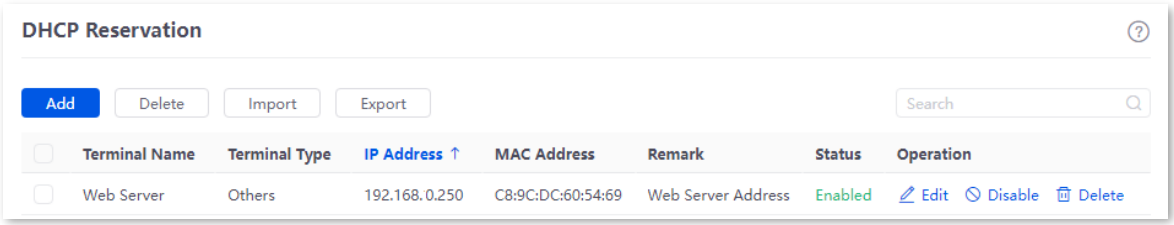
Step 3 Set the fixed IP address assigned to the server host.

1. Navigate to **Network** > **DHCP Reservation**, and Click **Add**.
2. Set the following rules, and click **Save**.
   - Set **Terminal Name**, which is **Web Server** in this example.
   - Set **IP Address** assigned to the server host, which is **192.168.0.250** in this example.
   - Set **MAC Address** of the server host, which is **C8:9C:DC:60:54:69** in this example.
   - Set **Remark**, which is **Web Server Address** in this example.



----End

The fixed IP address is reserved successfully. See the following figure.



Verification

Internet users can successfully access the intranet server by using the **Intranet service application layer protocol name**://**WAN port IP address**. If the intranet service port is not the default port number, the access address is **Intranet service application layer protocol name**://**WAN port IP address**:**External port**.

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

You can find the router's current WAN port IP address in **Connection Status**.

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 one by one:

– 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. Disable these programs and try again.

8.3 Maintenance service

8.3.1 Remote web management

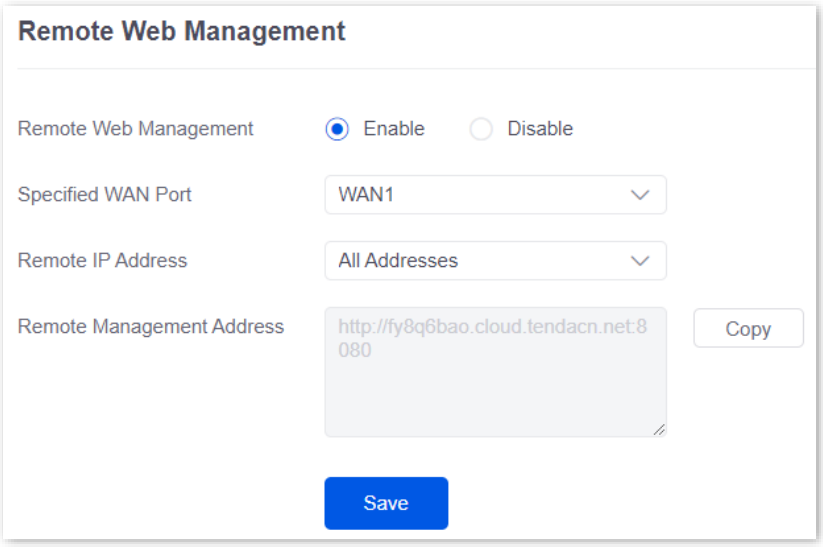
Overview

Generally, you can log in to the web UI of the router only when you connect to the LAN port or the WiFi network of the router. However, the Remote Web Management function enables access to the web UI remotely through the WAN port in special cases (like when you need remote technical support).

To access the configuration page, log in to the web UI of the router, and navigate to **More** > **Maintenance Service** > **Remote Web Management** to enter the page.

Here, you can enable or disable the remote web management and restrict the hosts that can remotely log in to the local router.

The remote web management function is disabled by default. The following displays the page when the function is enabled.



Parameter description

Parameter	Description
Remote Web Management	Used to enable or disable the Remote Web Management function.
Specified WAN Port	Specifies the WAN port used when accessing the web UI of the router from the internet remotely. When multiple WAN ports are available, you can select any one of them.

Parameter	Description
Remote IP Address	Specifies the IP address of the device that can access the web UI of the router remotely. - **All Addresses**: Devices with any IP address on the internet can access the web UI of the router. For network security, this option is not recommended. - **Specified Address**: Only devices with specified IP addresses can access the web UI of the router. If the device is in the local area network, the IP address (public IP address) of the gateway of the device should be filled in.
Remote Management Address	Specifies the domain name used for remote access. This domain name is generated by the router, and internet users can access the web UI of the router using the domain name when the Remote Web Management function is enabled.

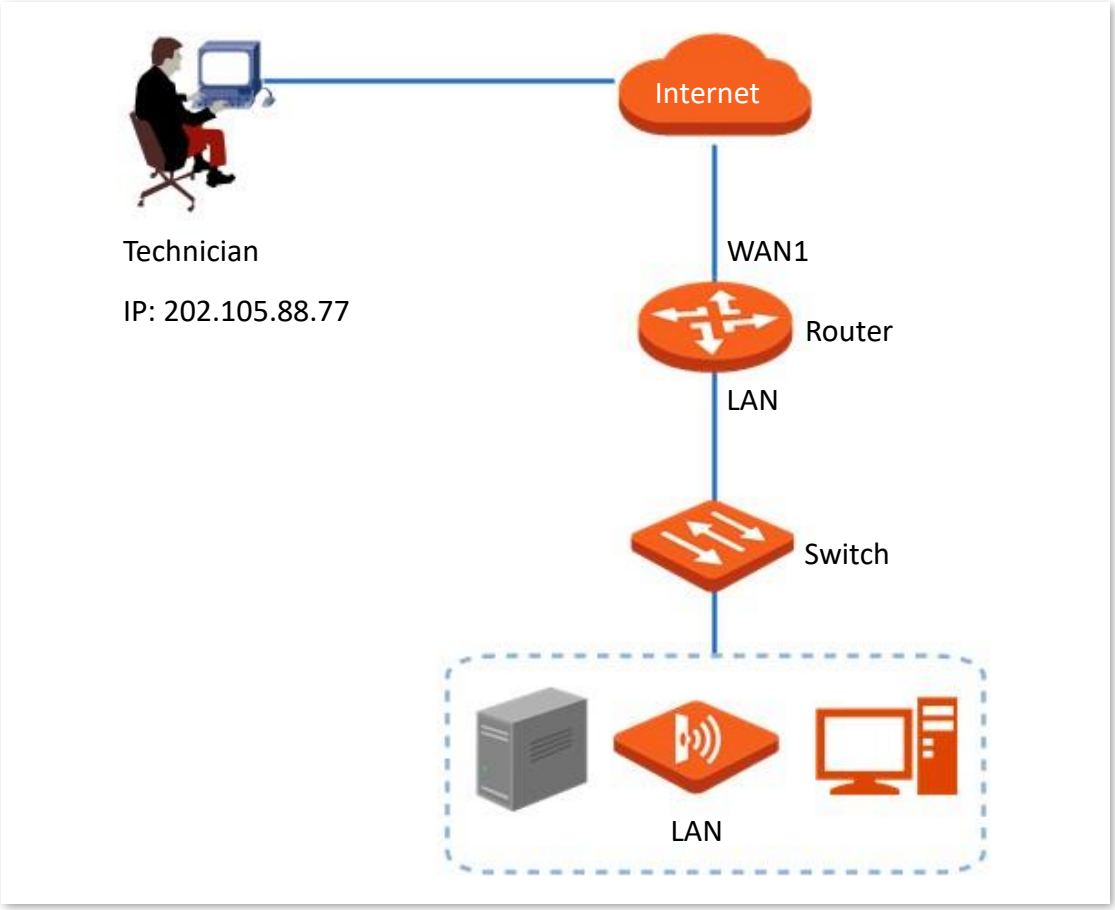
Example of configuring remote web management

Networking requirements

An enterprise uses the enterprise router to set up a network. The network administrator encountered a problem during network setup and needs the Tenda technical support to remotely log in to the web UI of the device to perform analysis and troubleshooting.

Solution

You can use the Remote Web Management function to meet the requirements.



Configuration procedure

Step 1 Log in to the web UI of the router.

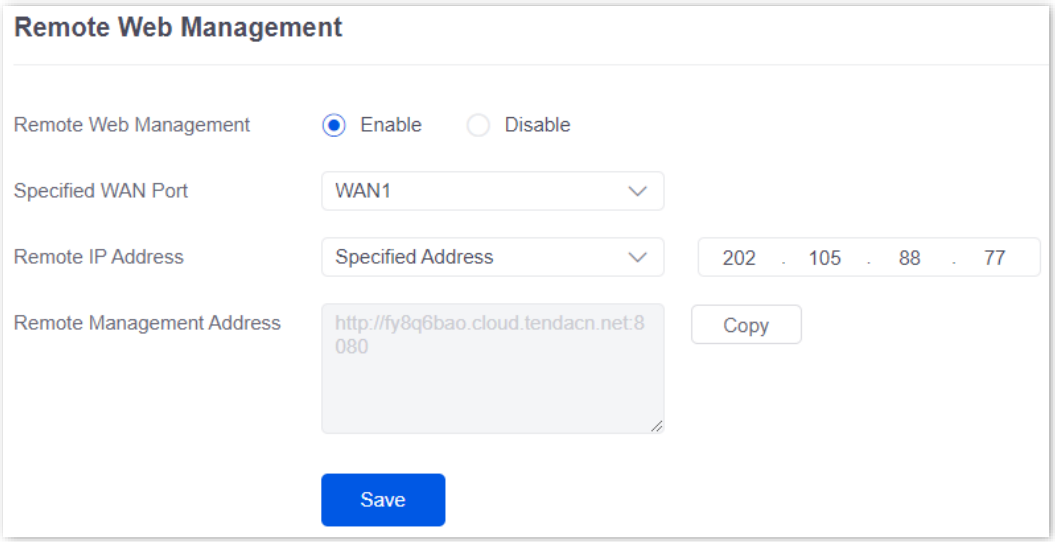
Step 2 Navigate to **More** > **Maintenance Service** > **Remote Web Management**.

Step 3 Enable **Remote Web Management.**

Step 4 Set **Specified WAN Port**, which is **WAN1** in this example.

Step 5 Set **Remote IP Address** as **Specified Address.** And enter the IP address of the computer supported by Tenda technology, which is **202.105.88.77** in this example**.**

Step 6 Click **Save**.



----End

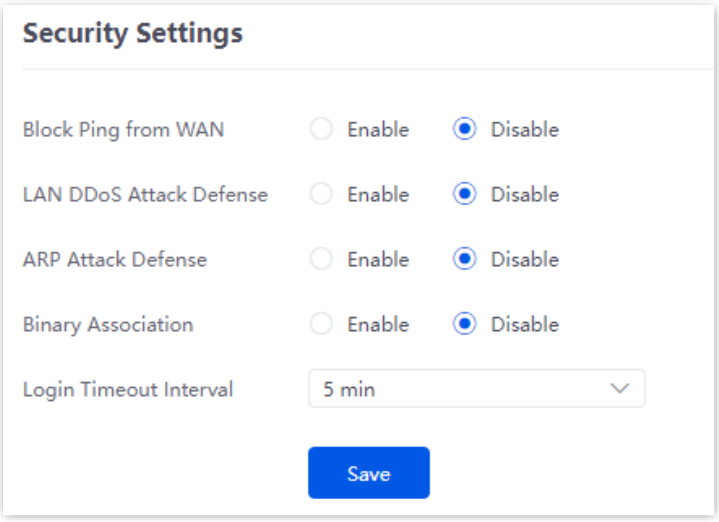
Verification

The Tenda technical support technician can Log in to the web UI of the router by visiting http://fy8q6bao.cloud.tendacn.net:8080 on the computer (the IP address of the computer is 202.105.88.77).

8.3.2 Security settings

To access the configuration page, log in to the web UI of the router, and navigate to **More** > **Maintenance Service** > **Security Settings** to enter the page.

Here, you can enable corresponding attack defense functions according to the actual network conditions.



Parameter description

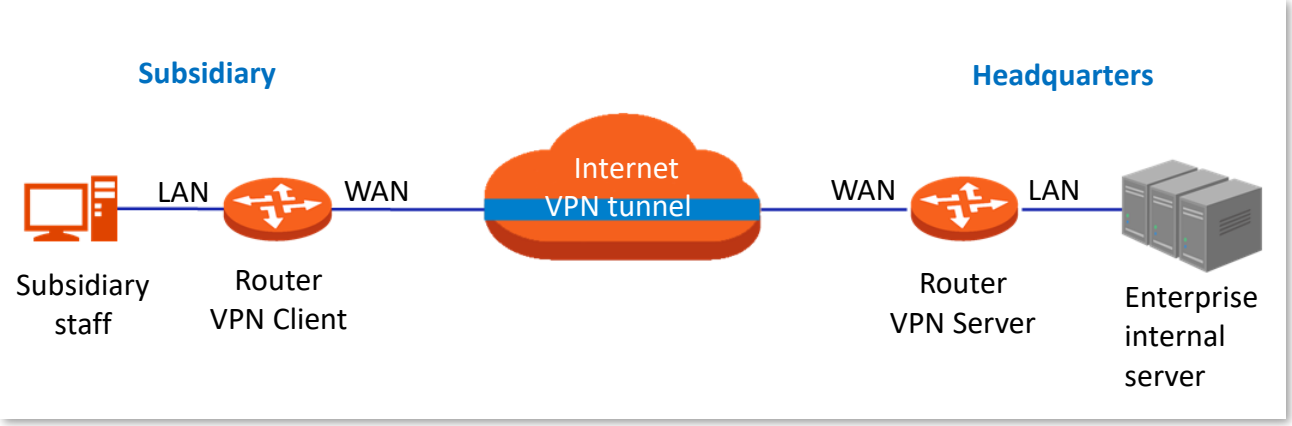
Parameter	Description
Block Ping from WAN	Used to enable or disable the Block Ping from WAN function. With this function enabled, when a WAN host pings the IP address of the WAN port on the router, the router automatically ignores the Ping request to prevent itself from being exposed and defend against external Ping attacks.
LAN DDoS Attack Defense	Used to enable or disable the LAN DDoS Attack Defense function. DDoS attack indicates the distributed denial of service attack. The attack allows an attacker to exhaust the resources of a system, making the system unable to properly provide services. With this function enabled, the router can defend common DDoS attacks from the internal network.
ARP Attack Defense	Used to enable or disable the ARP Attack Defense function. With this function enabled, the router can identify ARP spoofing in the LAN and record the MAC address of the attacker.
Binary Association	Used to enable or disable the Binary Association function. With this function enabled, only devices whose IP addresses are bound with MAC addresses in the list to access the internet.
Login Timeout Interval	Used to set the login timeout interval. After logging in to the web UI of the router, you will be automatically logged out when no operation is performed within the defined time period.

8.4 VPN

8.4.1 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 on the internet.

The typical network topology is shown as below.



The router supports the following VPN services:

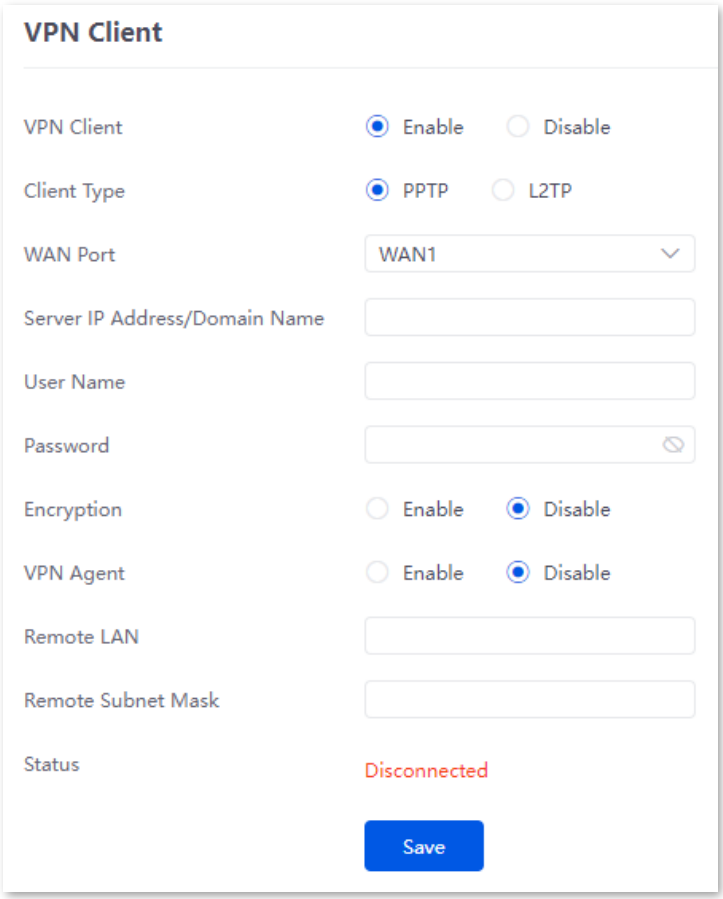
- PPTP/L2TP VPN Client
- IPSec

8.4.2 VPN client

Enable PPTP/L2TP client

This router can work as a PPTP/L2TP client to establish a VPN connection with a PPTP/L2TP server.

To access the configuration page, log in to the web UI of the router, and navigate to **More** > **VPN Client**. Set **VPN Client** to **Enable** and configure related parameters. Then click **Save**.



Parameter description

Parameter	Description
VPN Client	Used to enable or disable the VPN client function. After this function is enabled, the router works as a VPN client.
Client Type	Specifies the VPN client type of the router, including PPTP and L2TP. Both PPTP and L2TP are Layer 2 VPN tunneling protocols, use Point-to-Point Protocol (PPP) for data encapsulation, and add additional headers to the data. - **PPTP**: Select **PPTP** when the VPN server is a L2TP server. - **L2TP**: Select **L2TP** when the VPN server is a PPTP server.
WAN Port	Specifies the WAN port of the PPTP/L2TP client for setting up a connection with the PPTP/L2TP server.

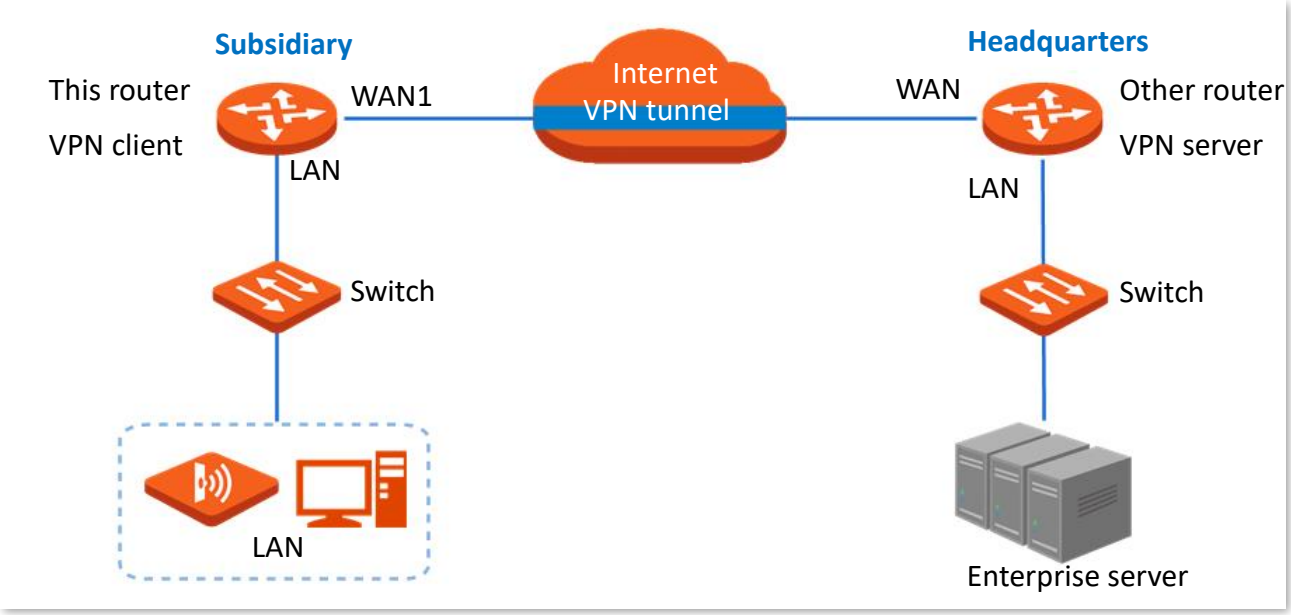
Parameter	Description
Server IP Address/Domain Name	Specifies the IP address or domain name of the VPN server. Generally, it is the IP address or domain name of the WAN port with the PPTP/L2TP server function enabled on the peer VPN router.
User Name	Specify the username and password assigned by the VPN server to the VPN client.
Password	
Encryption	Specifies whether to enable 128-bit data encryption. The value of this parameter must be consistent with that of the server. Otherwise, the client is unable to communicate with the server. Only PPTP VPNs support this parameter.
VPN Agent	With this function enabled, clients on the LAN can obtain IP addresses from the VPN server to access the internet.
Remote LAN	Specifies the network segment of the LAN of the PPTP/L2TP server.
Remote Subnet Mask	Specifies the subnet mask of the LAN of the PPTP/L2TP server.
Status	Specifies the current connection status of the VPN client.

Example of users accessing VPN resouces from ISP

Solution

You can configure the VPN client function to meet the above requirement. Assume that:

- PPTP server address is 113.88.112.220, no encryption.
- Username and password assigned by the PPTP server are both admin1.



Configuration procedure

Step 1 Log in to the web UI of the router.

Step 2 Navigate to **More** > **VPN Client**.

Step 3 Set **VPN Client** to **Enable**.

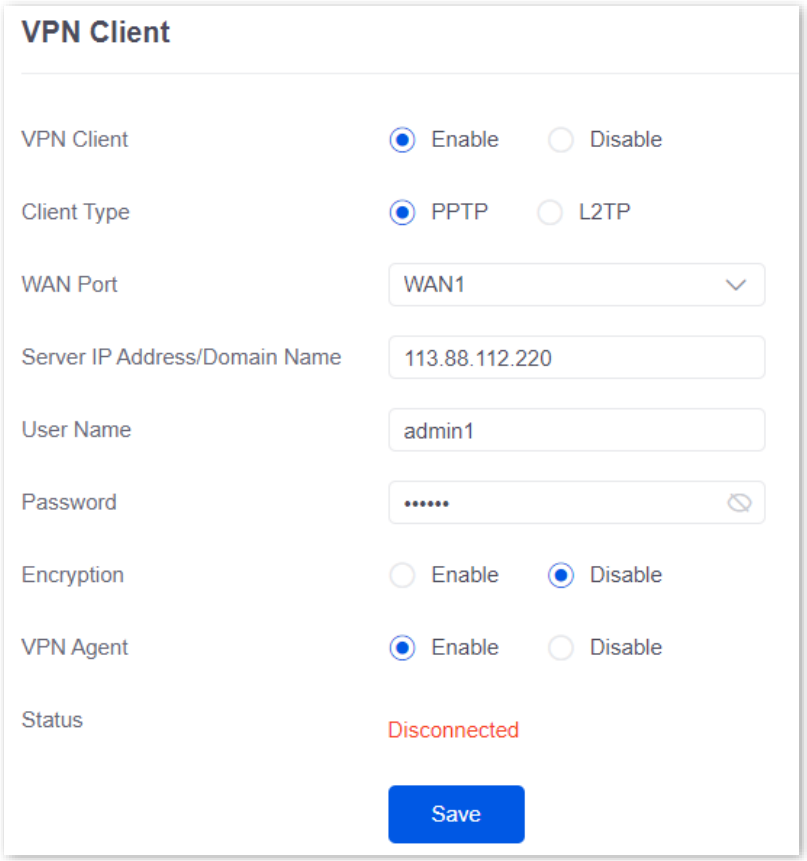
Step 4 Retain default settings **PPTP** for **Client Type**, and **WAN1** for **WAN Port**.

Step 5 Enter **Server IP Address/Domain Name**, which is **113.88.112.220** in this example.

Step 6 Enter **User Name** and **Password** used by the VPN client for VPN dial-up, both of which are **admin1** in this example.

Step 7 Retain default settings **Disable** for **Encryption**. Set **VPN Agent** to **Enable**.

Step 8 Click **Save**.



----End

Verification

When **Status** is displayed as **Connected**, Staff of the subsidiary can securely access the VPN resources from the headquarters.

8.4.3 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**

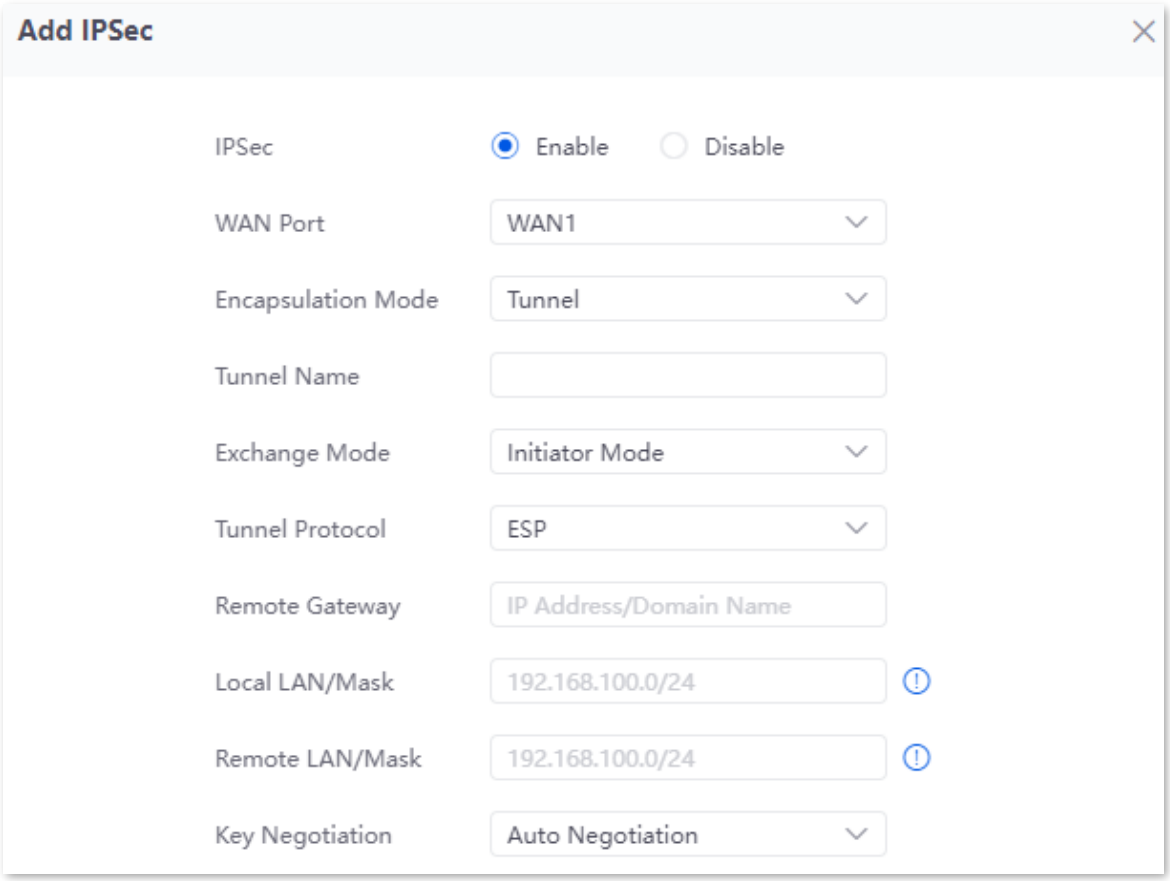
  SA specifies some elements of the peers, such as the base protocol (AH, ESP, or both), encapsulation mode (transport or tunnel), encryption algorithm (DES, 3DES, or AES), shared key for data protection in specified flows, and life cycle of the key. SA has the following features:

  - A triplet {SPI, Destination IP address, Security protocol identifier} is used as a unique ID.
  - A SA specifies the protocol, algorithm, and key for processing packets.
  - Each IPsec SA is unidirectional with a life cycle.
  - A 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

To access the configuration page, log in to the web UI of the router, and navigate to **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.



Parameter description

Parameter	Description
IPSec	Used to enable or disable the IPSec function.
WAN Port	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.
Tunnel Name	Specifies the name of the IPSec tunnel.

Parameter	Description
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/Mask	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/Mask	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 a SA is set up, maintained, and deleted automatically using IKE (Internet Key Exchange). This reduces configuration complexity and simplifies IPSec usage and management. Such a SA (Security Association) has a life cycle and is updated regularly, leading to higher security. - **Manual**: It indicates that a SA is set up by manually specifying encryption and authentication algorithms and keys. Such a 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.

Networking requirements

An enterprise’s subsidiary uses the wireless routers to set up a network and the routers have been connected to the internet.

The enterprise’s subsidiary 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.

The enterprise's Headquarters has used an enterprise-level router with VPN server function to build a network, and has configured a PPTP VPN server and successfully accessed the Internet.

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:

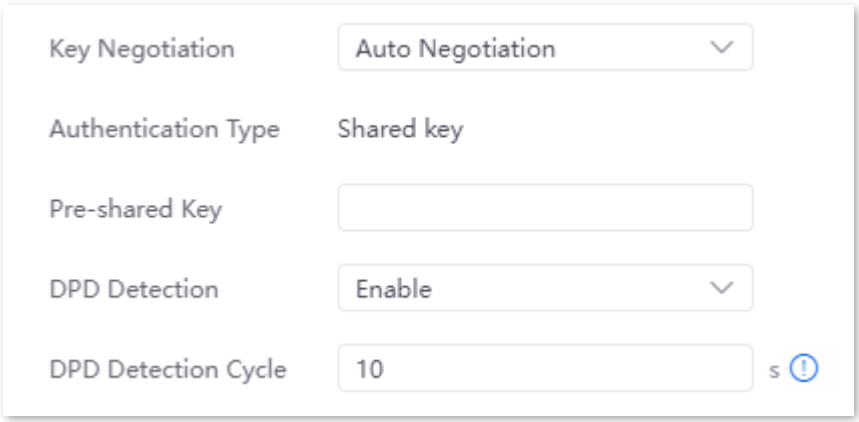
- **ISAKMP**: Internet Security Association and Key Management Protocol. It defines the procedures for authenticating a communicating peer, creation and management of Security Associations, key generation techniques, and threat mitigation.
- **Oakley**: Oakley Key Determination Protocol. It defines the 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.

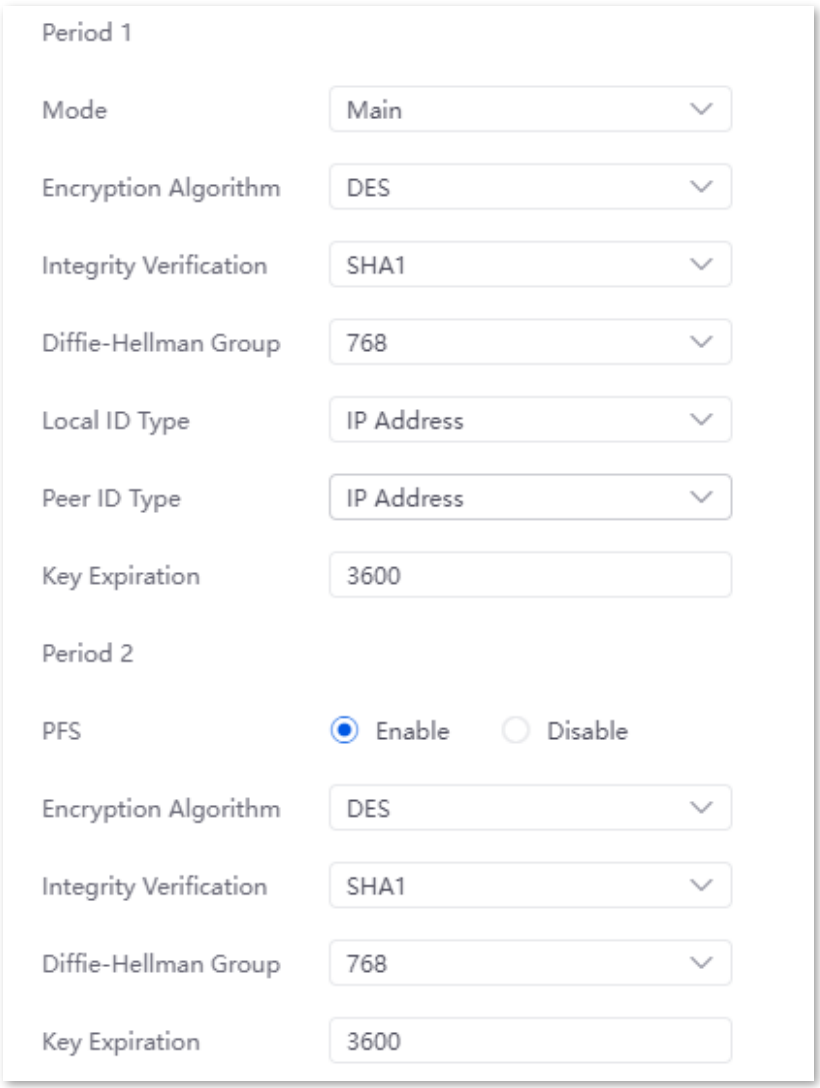


Parameter description

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	Used to enable or disable the DPD Detection. This function can detect whether the remote tunnel site is valid.

Parameter	Description
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.



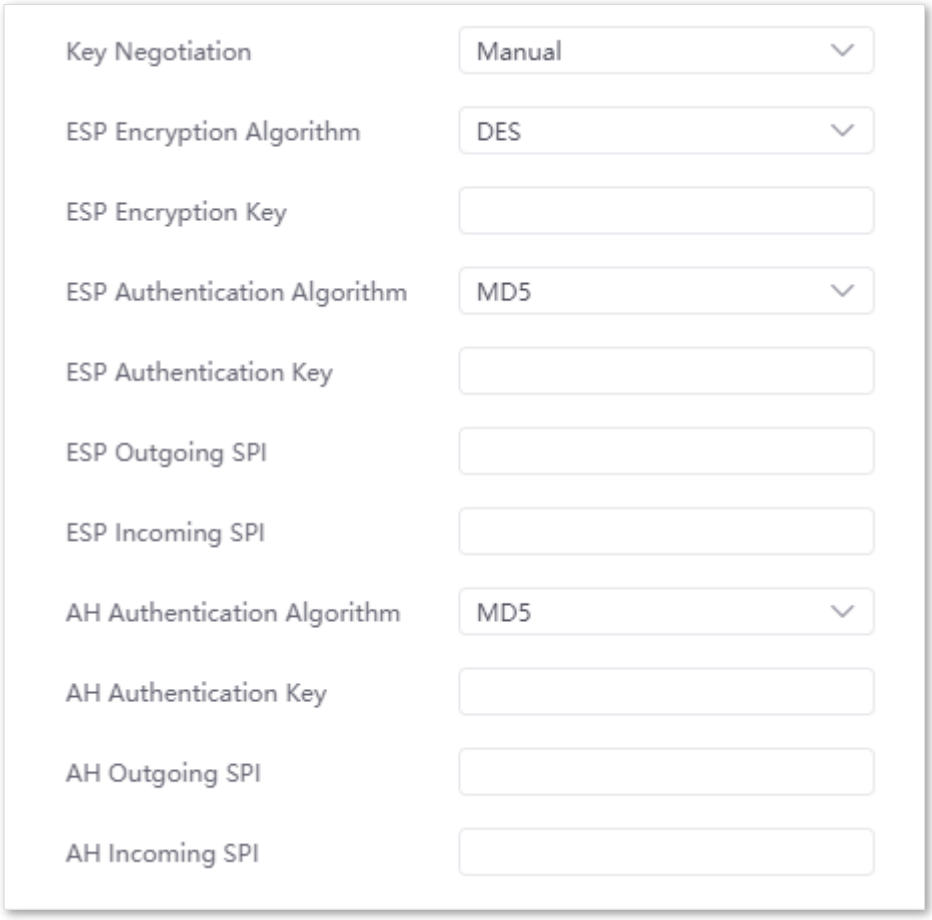
Parameter description

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.

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.
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).



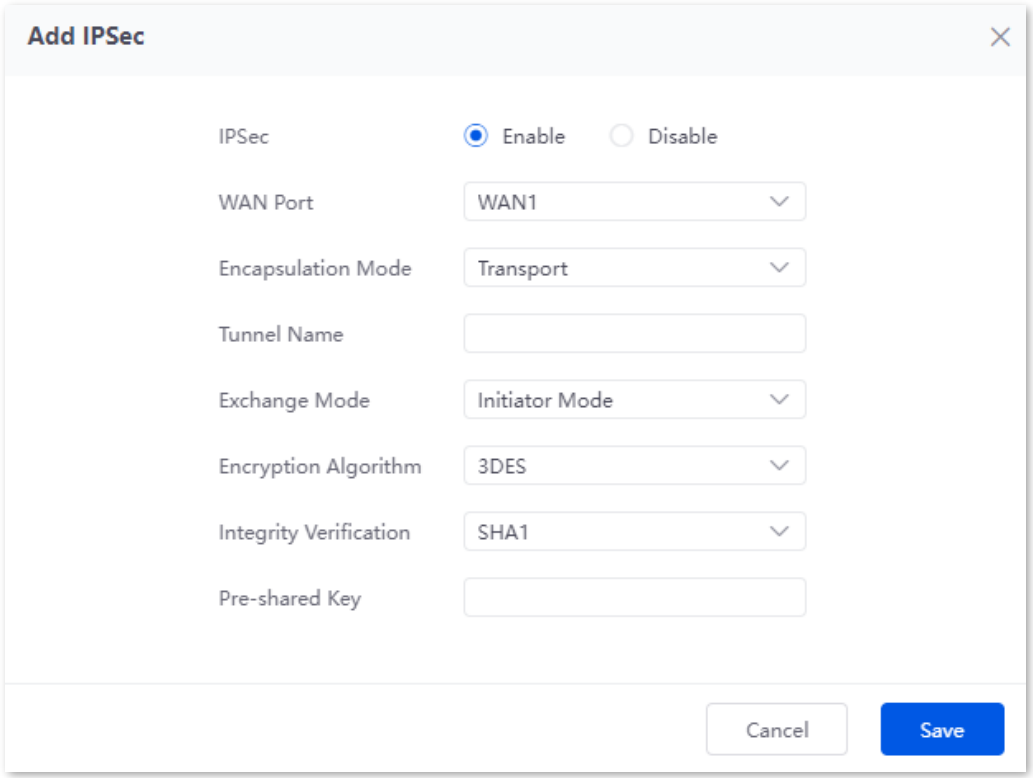
Parameter description

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

To access the configuration page, log in to the web UI of the router, and navigate to **More** > **IPSec** to enter the page. Click **+Add**, select the **Transport** mode, configure the following parameters in the window, and click **Save**.



Parameter description

Parameter	Description
IPSec	Used to enable or disable the IPSec function.
WAN Port	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.
Tunnel Name	Specifies the name of the IPSec tunnel.
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.

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

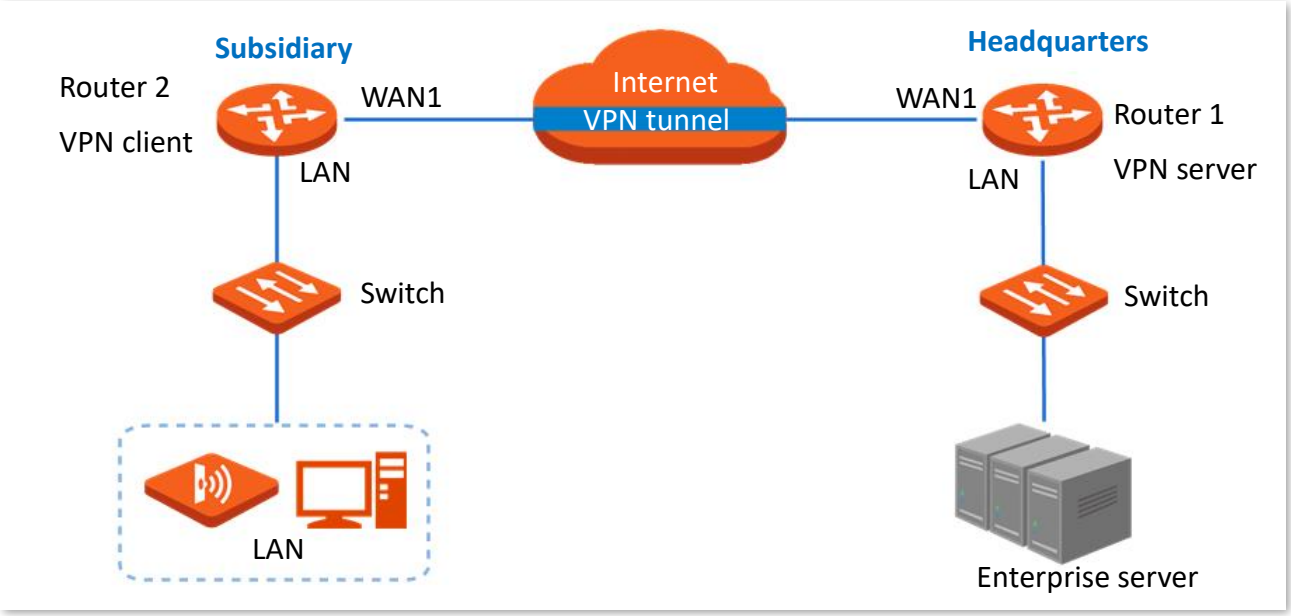
Assume that router 2 is deployed in the subsidiary and its basic information is as follows:

- 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

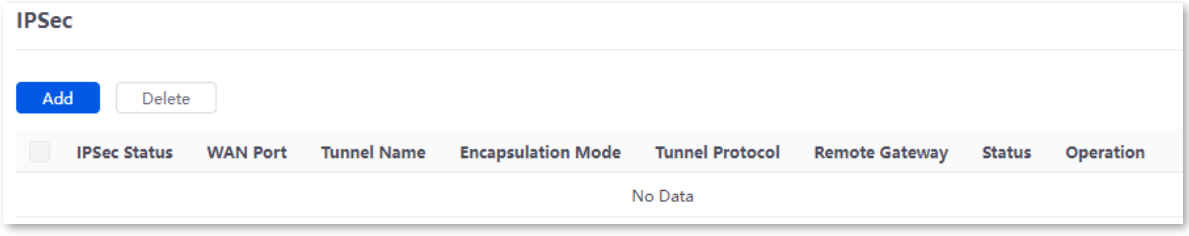
Configure router 1 > Configure router 2

NOTE

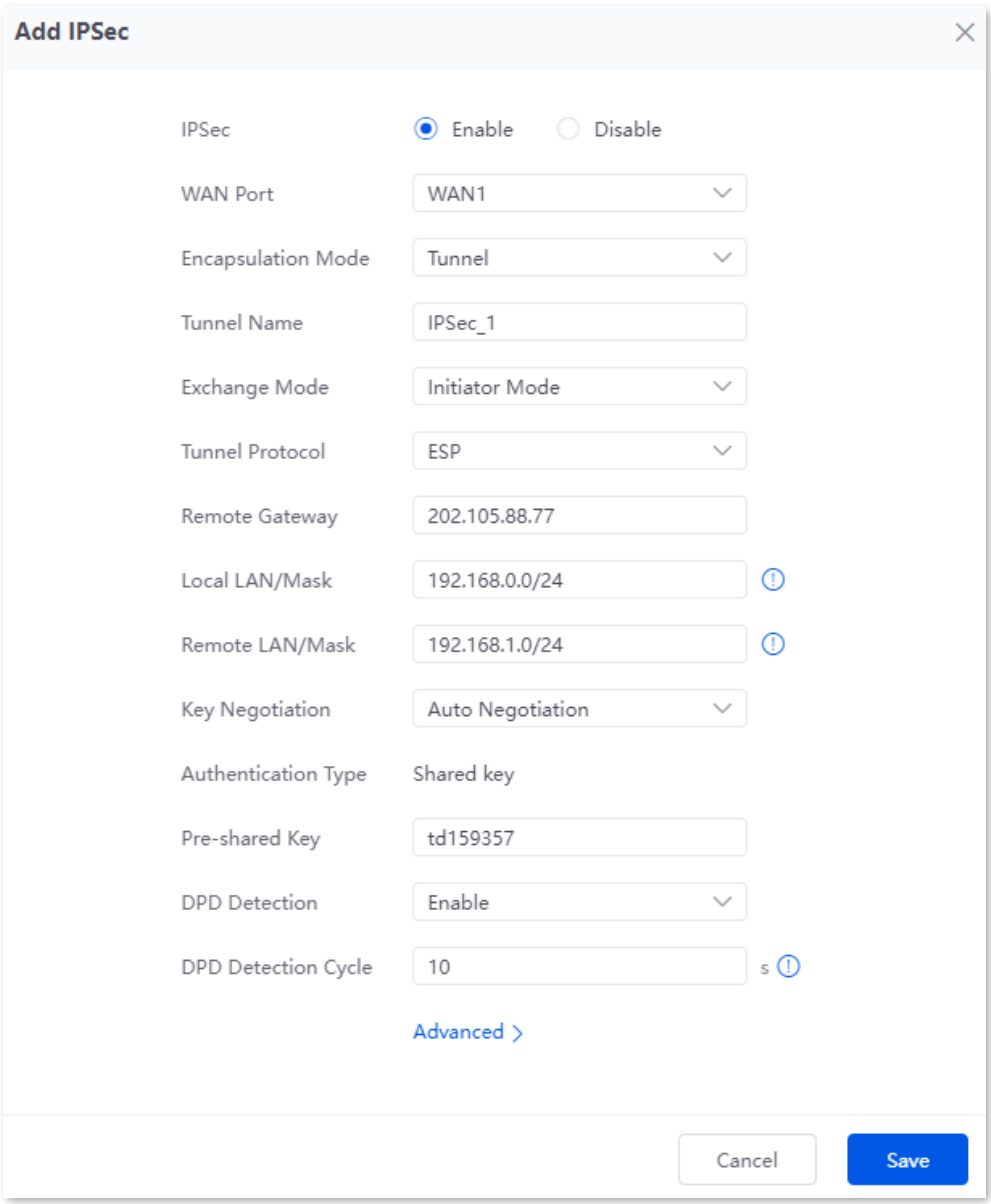
During the configuration, if you want to configure the advanced settings of IPSec connection, make sure the parameters of the two routers are the same.

Step 1 Configure router 1.

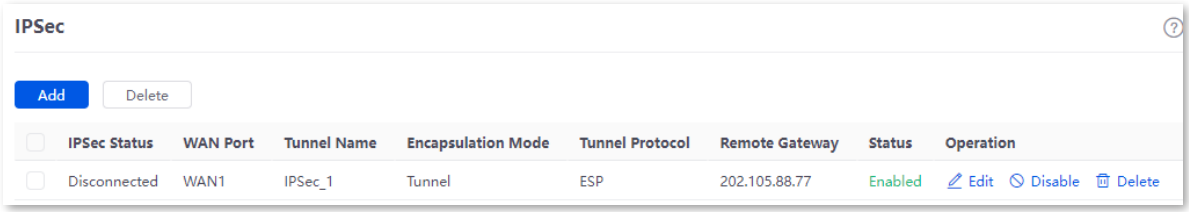
1. Log in to the web UI of the router1, and navigate to **More** > **IPSec**.
2. Click **Add**.



3. Configure the parameters in the **Add** window, and click **Save**.
   - Select the WAN port to establish an IPSec tunnel, which is **WAN1** this example.
   - Set **Encapsulation Mode** to **Tunnel**.
   - Set the **Tunnel Name**, which is **IPSec_1** in this example.
   - Enter the **Remote Gateway**, which is **202.105.88.77** in this example.
   - Enter the **Local LAN/Mask**, which is **192.168.0.0/24** in this example.
   - Enter the **Remote LAN/Mask**, which is **192.168.1.0/24** in this example.
   - Set the **Pre-shared Key**, which is **td159357** in this example.

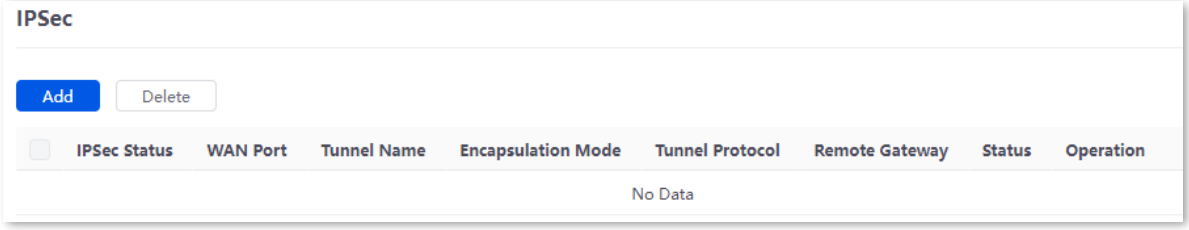


The IPSec is added successfully. See the following figure.

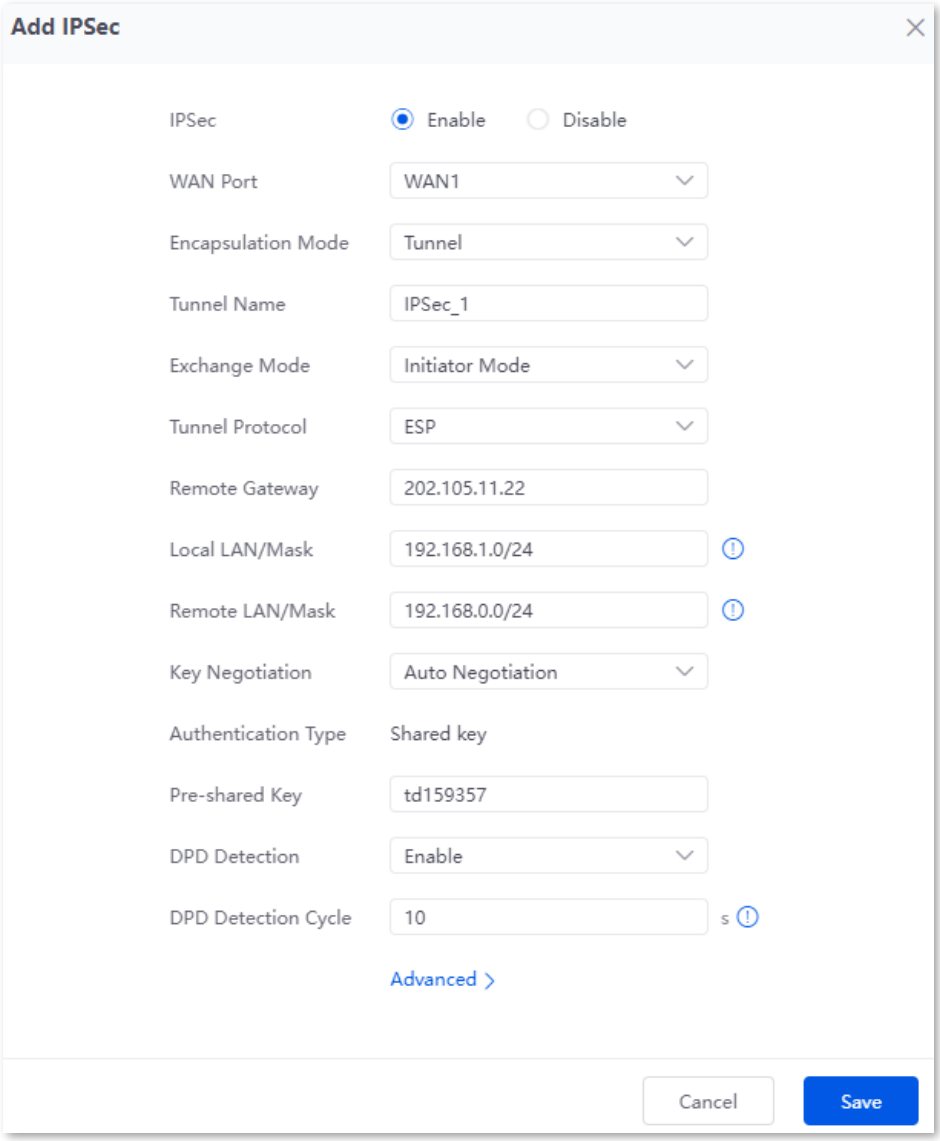


Step 2 Configure router 2.

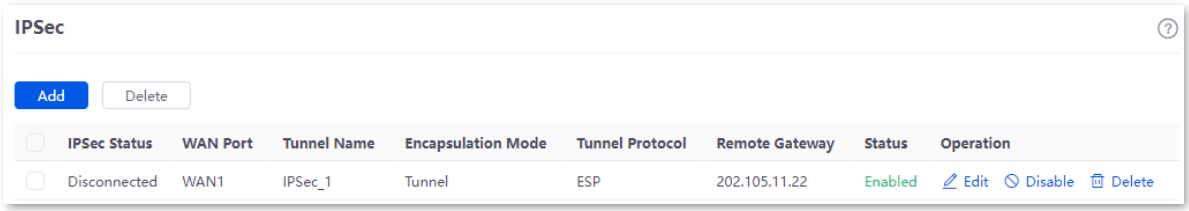
1. Log in to the web UI of the router2 and navigate to **More** > **IPSec**.
2. Click **Add**.



3. Configure the parameters in the **Add** window, and click **Save**.
   - Select the WAN port to establish an IPSec tunnel, which is **WAN1** this example.
   - Set **Encapsulation Mode** to **Tunnel**.
   - Set the **Tunnel Name**, which is **IPSec_1** in this example.
   - Enter the **Remote Gateway**, which is **202.105.11.22** in this example.
   - Enter the **Local LAN/Prefix Length**, which is **192.168.1.0/24** in this example.
   - Enter the **Remote LAN/Prefix Length**, which is **192.168.0.0/24** in this example.
   - Set the **Pre-shared Key**, which is **td159357** in this example.



The IPSec is added successfully. See the following figure.



----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.

8.5 IPv6

8.5.1 Overview

IPv6, abbreviated for Internet Protocol Version 6, is the second-generation network layer protocol. IPv6 is an upgraded version of Internet Protocol version 4 (IPv4), which is the solution that addresses the relatively limited number of IP addresses possible under IPv4.

IPv6 address

An IPv6 address is 128 bits long and is arranged in eight groups, each of which is 16 bits. Each group is expressed as four hexadecimal digits and the groups are separated by colons. An IPv6 address is split into two parts:

- Network Prefix: n bits, equivalent to the network ID in the IPv4 address.
- Interface Identifier: 128-n bits, equivalent to the host ID in the IPv4 address.

Basic concept

- **DHCPv6**

Dynamic Host Configuration Protocol for IPv6 (DHCPv6) is a stateful protocol that assigns IPv6 addresses or prefixes and other configuration parameters to hosts.

- **SLAAC**

Stateless Address Autoconfiguration (SLAAC) is a stateless protocol. Hosts automatically generate IPv6 addresses or prefixes and other configuration parameters through Router Advertisement (RA).

8.5.2 Internet

To access the configuration page, log in to the web UI of the router, and navigate to **More** > **IPv6** > **Internet** to enter the page.

Here, you can configure the IPv6 address of the corresponding WAN port.

There are two methods to obtain IPv6 addresses. Select the method based on the configuration of the upstream device.

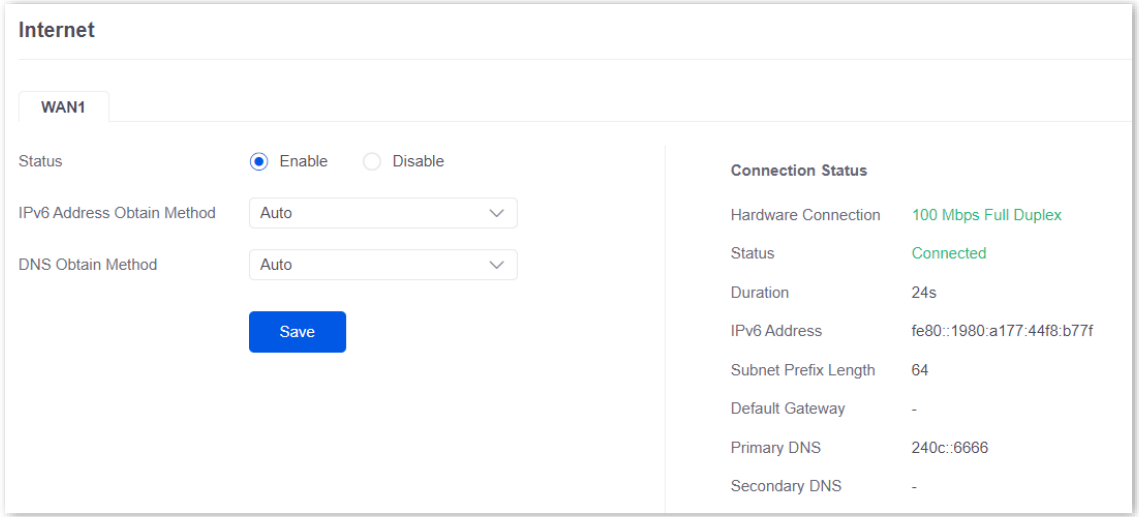
Condition	Selection
The IP address assignment modes of the LAN port on the upstream device are DHCPv6, SLAAC or DHCPv6+SLAA.	Auto
The upstream device is the ISP device, and the ISP provides a PPPoE account and password that supports IPv6 service.	
The upstream device is the ISP device, and the ISP does not provide specific network parameters.	
The upstream device does not assign IP addresses.	Manual
The upstream device is the ISP device, and the ISP provides a group of fixed IPv6 addresses for internet access, including the IP address, subnet mask, default gateway and DNS server information.	

NOTE

If the WAN port is directly connected to the ISP network, ensure that you have enabled the IPv6 internet service. If you are not sure, contact your ISP first.

Auto

The WAN port automatically obtains IPv6 internet access information through DHCPv6 or SLAAC. After the IPv6 parameters of the WAN port are configured, you can view the IPv6 networking status in the **Connection Status** module on the right. The following figure is for reference only.

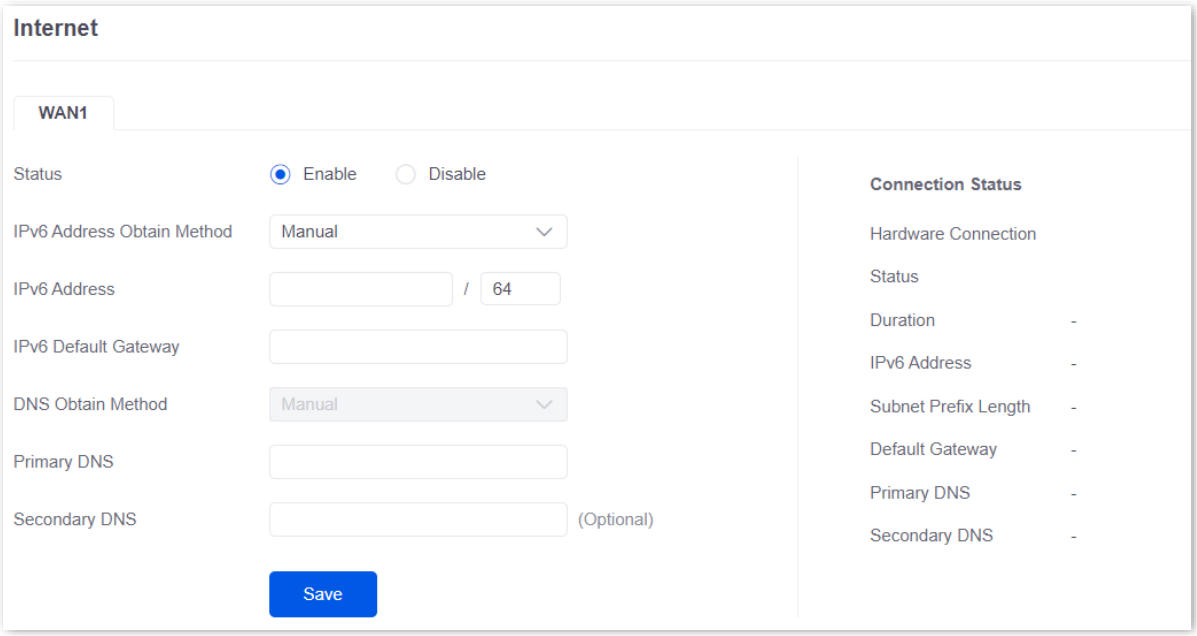


Parameter description

Parameter		Description
Mode	Status	Used to enable or disable the IPv6 function of the corresponding WAN port.
	IPv6 Address Obtain Method	Select **Auto**.
	DNS Obtain Method	Specifies the method of the WAN port to obtain the DNS server address. - **Auto**: The DNS server address is automatically obtained through DHCPv6 or SLAAC. - **Manual**: Enter the DNS server address manually.
	Primary DNS	Enter a correct IPv6 DNS server address. TIP If there is only one DNS address, **Secondary DNS** is not required.
	Secondary DNS	
Connection Status	Hardware Connection	Specifies the current rate and duplex mode of the WAN port.
	Status	Specifies the connection status of the WAN port of the router. - **Connected**: The WAN port of the router has been plugged into the Ethernet cable, and the IPv6 address information has been obtained. - **Connecting...**: The router is connecting to the upstream network device. - **Disconnected**: If it is not connected or fails to connect, check the Ethernet cable connection status and internet settings, or consult the corresponding ISP.
	Duration	Specifies the duration of the WAN port access to the IPv6 network.
	IPv6 Address	Specifies the IPv6 global unicast address of the WAN port.
	Subnet Prefix Length	Specifies the network prefix number of the IPv6 address.
	Default Gateway	Specifies the IPv6 default gateway of the WAN port.
	Primary DNS	Specify the primary or secondary IPv6 DNS server address of the WAN port.
	Secondary DNS	

Manual

Access the internet using the fixed IPv6 address provided by ISP.



Parameter description

Parameter		Description
Mode	Status	Used to enable or disable the IPv6 function of the corresponding WAN port.
	IPv6 Address Obtain Method	Select **Manual**.
	IPv6 Address	Enter the IPv6 global unicast address provided by ISP.
	IPv6 Default Gateway	Enter the IPv6 default gateway provided by ISP.
	DNS Obtain Method	Specifies the method of the WAN port to obtain the IPv6 DNS server address. Only **Manual** is allowed, which means entering the IPv6 DNS server address manually.
	Primary DNS	Enter a correct IPv6 DNS server address. TIP If there is only one DNS address, **Secondary DNS** is not required.
	Secondary DNS	

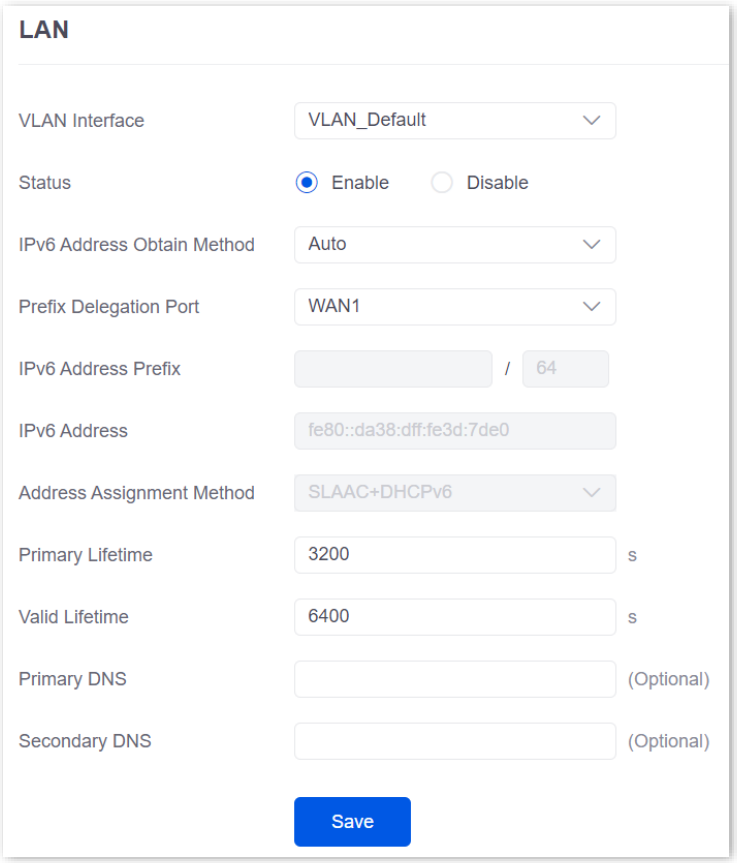
Parameter		Description
Connection Status	Hardware Connection	Specifies the current rate and duplex mode of the WAN port.
	Status	Specifies the connection status of the WAN port of the router. - **Connected**: The WAN port of the router has been plugged into the Ethernet cable, and the IPv6 address information has been obtained. - **Connecting...**: The router is connecting to the upstream network device. - **Disconnected**: If it is not connected or fails to connect, check the Ethernet cable connection status and internet settings, or consult the corresponding ISP.
	Duration	Specifies the duration of the WAN port access to the IPv6 network.
	IPv6 Address	Specifies the IPv6 global unicast address of the WAN port.
	Subnet Prefix Length	Specifies the network prefix number of the IPv6 address.
	Default Gateway	Specifies the IPv6 default gateway of the WAN port.
	Primary DNS	Specify the primary or secondary IPv6 DNS server address of the WAN port.
	Secondary DNS	

8.5.3 LAN

Log in to the web UI of the router, and click **More** > **IPv6** > **LAN** to enter the page.

Here, you can configure the IPv6 address of the corresponding VLAN so that multiple devices on the LAN can share the broadband server.

The VLAN is disabled by default. After it is enabled, the following information is displayed.



Parameter description

Parameter	Description
VLAN Interface	Specifies the VLAN interface for IPv6.
Status	Used to enable or disable the IPv6 function of the corresponding VLAN.
IPv6 Address Obtain Method	Specifies the method to obtain IPv6 addresses. - **Auto:** The IPv6 address prefix of the VLAN is automatically obtained from upstream device by **Prefix Delegation Port**. The IPv6 address is automatically generated by the router according to the standard. - **Manual:** You need to manually set the IPv6 address prefix, complete IPv6 address and address assignment mode of the VLAN.
Prefix Delegation Port	Specifies the WAN port which obtains the IPv6 address prefix of the VLAN from the upstream device. It needs to be selected when **IPv6 Address Obtain Method** is **Auto**.

Parameter	Description
IPv6 Address Prefix	Specifies the IPv6 address prefix of the VLAN.
IPv6 Address	Specifies the complete IPv6 address of the VLAN address.
Address Assignment Method	Specifies the method that the router uses to assign IPv6 addresses to LAN clients. - **DHCPv6:** The client directly obtains all IPv6 address information from the DHCPv6 server, including the DNS server. - **SLAAC:** The client automatically generates IPv6 address information through RA, including the IPv6 address and DNS server. - **SLAAC+DHCPv6:** The client automatically generates the IPv6 address through RA and obtains other address information from the DHCPv6 server, such as the DNS server.
Start Address	Specify the range of IPv6 addresses assigned by the DHCPv6 server. When **Address Assignment Method** is **DHCPv6**, you need to configure parameters.
End Address	
Primary Lifetime	Specifies the primary lifetime of the IPv6 address lease. If the client does not receive RA within the primary lifetime, it will deactivate the IPv6 address and no longer use the IPv6 address to create new connections, but can still receive messages with this IPv6 address as the destination address.
Valid Lifetime	Specifies the valid lifetime of the IPv6 address lease. After expiration, the IPv6 address will be deleted and invalid, and all sessions will be disconnected.
Primary DNS	Specify the IP address of the primary or secondary DNS server that is assigned to the client. TIP For the LAN devices to access the internet properly, ensure that the primary DNS you entered is the correct IP address of the DNS server or DNS proxy.
Secondary DNS	

9 System maintenance

9.1 System time

To access the configuration page, log in to the web UI of the router, and navigate to **Tool** > **System Time** to enter the page.

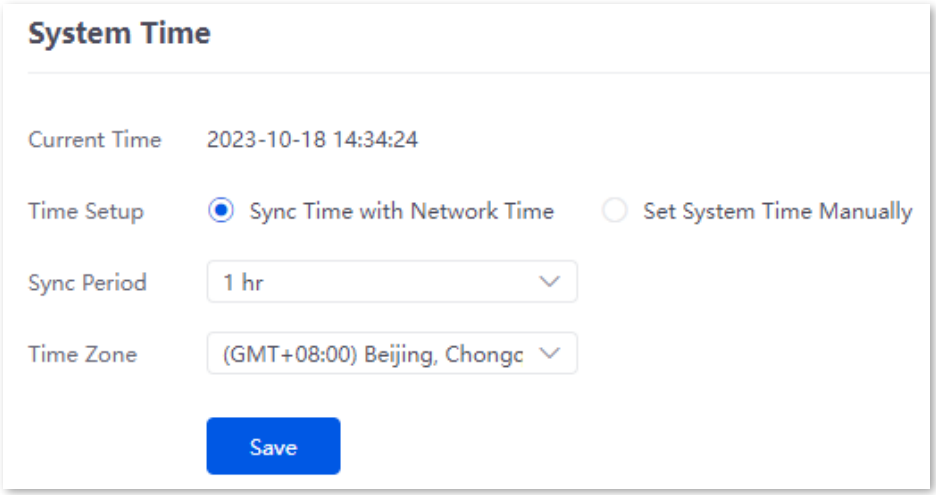
Here, you can configure the system time of the router.

To make the time-related functions effective, ensure that the system time of the router is set correctly. The router supports: Sync time with network time and Set system time manually. By default, **Sync Time with Network Time** is selected.

9.1.1 Sync time with network time

If you choose this method, the router automatically synchronizes its system time with the Network Time Server (NTS). As the router is connected to the internet, the system time is correct.

After the configuration is completed, you can refresh the page to check whether the system time of the router is correct.



Parameter description

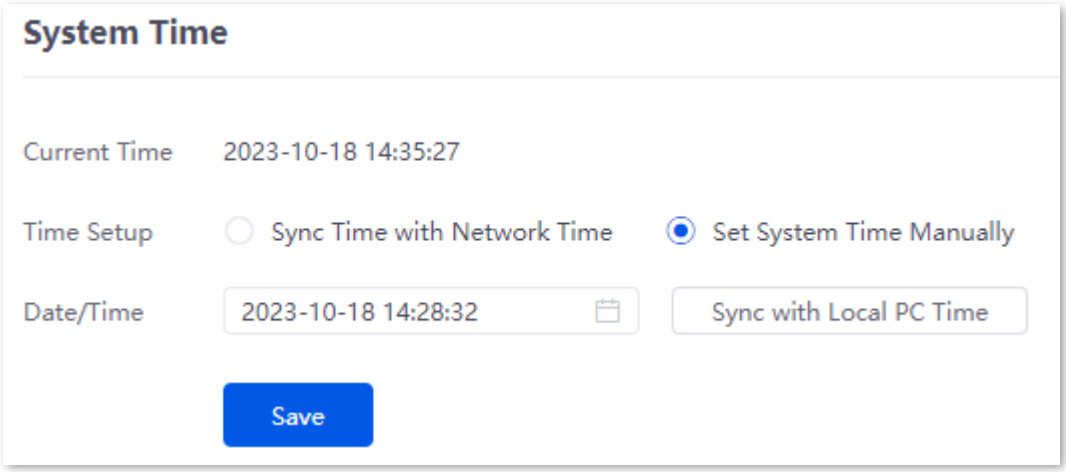
Parameter	Description
Current Time	Specifies the current system time of the router.
Time Setup	Specifies the setting mode of the system time. Select **Sync Time with Network Time**.
Sync Period	Specifies the interval at which the router synchronizes the system time with a time server on the internet.

Parameter	Description
Time Zone	Specifies the standard time zone in which the router is currently located.

9.1.2 Set system time manually

If you choose this method, you can manually set a system time for the router. Every time the router reboots, you need to reconfigure the system time.

After the configuration is completed, you can refresh the page to check whether the system time of the router is correct.



Parameter description

Parameter	Description
Current Time	Specifies the current system time of the router.
Time Setup	Specifies the setting mode of the system time. Select **Set System Time Manually**.
Date/Time	Click to select the correct time, or click **Sync with Local PC Time** to synchronize the time of the router with the computer which is managing the router.

9.2 Diagnostic tool

9.2.1 Ping

Ping is used to check whether the connection is correct and the connection quality.

To access the configuration page, log in to the web UI of the router, and navigate to **Tool** > **Diagnosis** to enter the page.

Here, you can check whether the connection is correct and the connection quality with **Ping**.

Assume that you want to detect whether the link between the router and the Google management network (www.google.com) is unblocked.

To perform Ping test:

Step 1 Log in to the web UI of the router, and navigate to **Tool** > **Diagnosis**.

Step 2 Select **Ping** from the **Tool** drop-down list box.

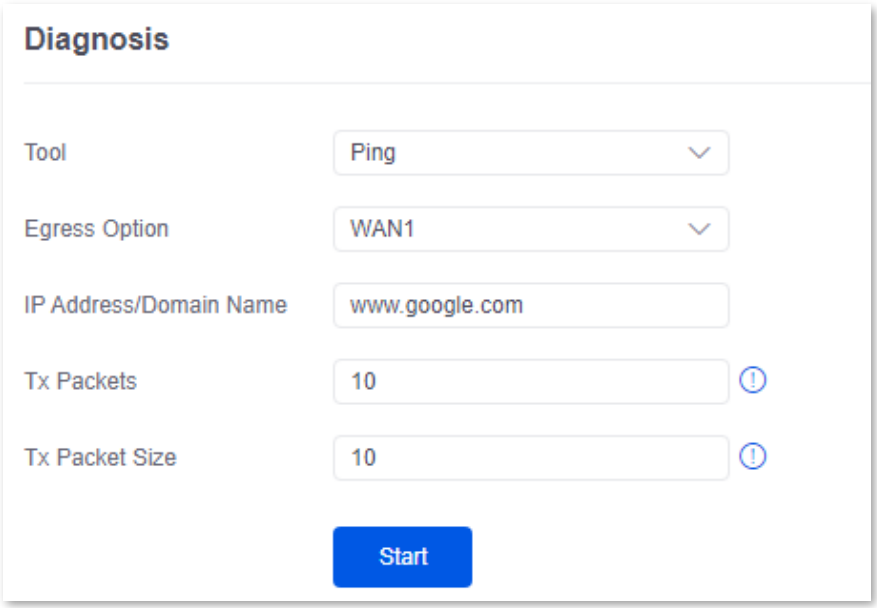
Step 3 Set **Egress Option** to the interface for the test, which is **WAN1** in this example.

Step 4 Enter the IP address or domain name of the ping target, which is **www.google.com** in this example.

Step 5 Set **Tx Packets** to the number of packets sent in the Ping test, which is **10** in this example.

Step 6 Set **Tx Packet Size** to the size of packets sent in the Ping test, which is **10** in this example.

Step 7 Click **Start**.

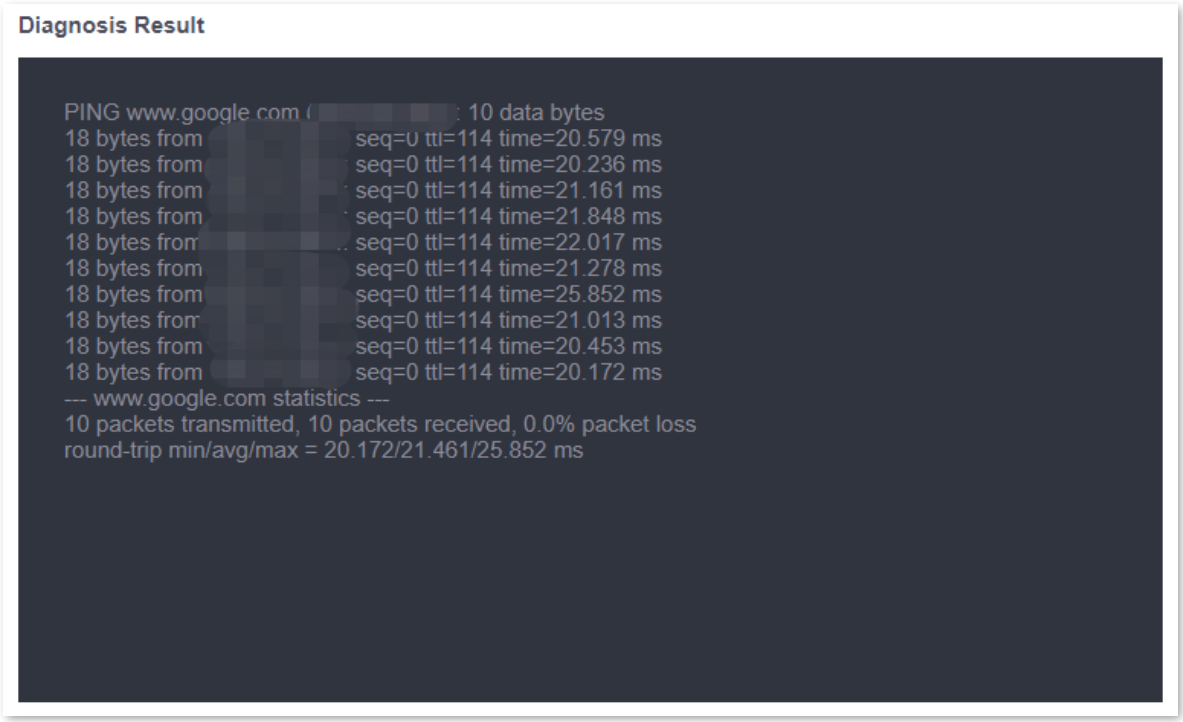


----End

Parameter description

Parameter	Description
Egress Option	Specifies the interface from which the data goes out.
IP Address/Domain Name	Specifies the IP address or domain name of the target host.
Tx Packets	Specifies the number of data packets sent in the Ping test.
Tx Packet Size	Specifies the size of data packets sent in the Ping test.

The diagnosis result is shown in the lower part of the page. See the following figure.



9.2.2 Tracert

Tracert is used to detect the routes that a packet takes from a router to a destination host.

To access the configuration page, log in to the web UI of the router, and navigate to **Tool** > **Diagnosis** to enter the page.

Here, you can detect the routes that a packet takes from a router to a destination host with **Tracert**.

Assume that you want to detect the routes from the router to the Google management network (www.google.com).

To perform Tracert test:

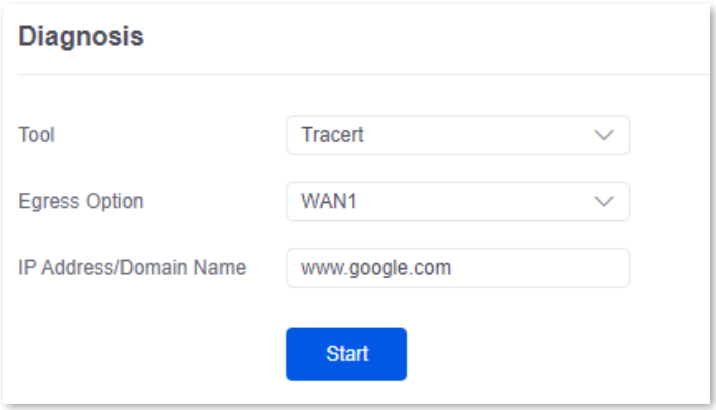
Step 1 Log in to the web UI of the router, and navigate to **Tool** > **Diagnosis**.

Step 2 Select **Tracert** from the **Tool** drop-down list box.

Step 3 Set **Egress Option** to the interface for the test, which is **WAN1** in this example.

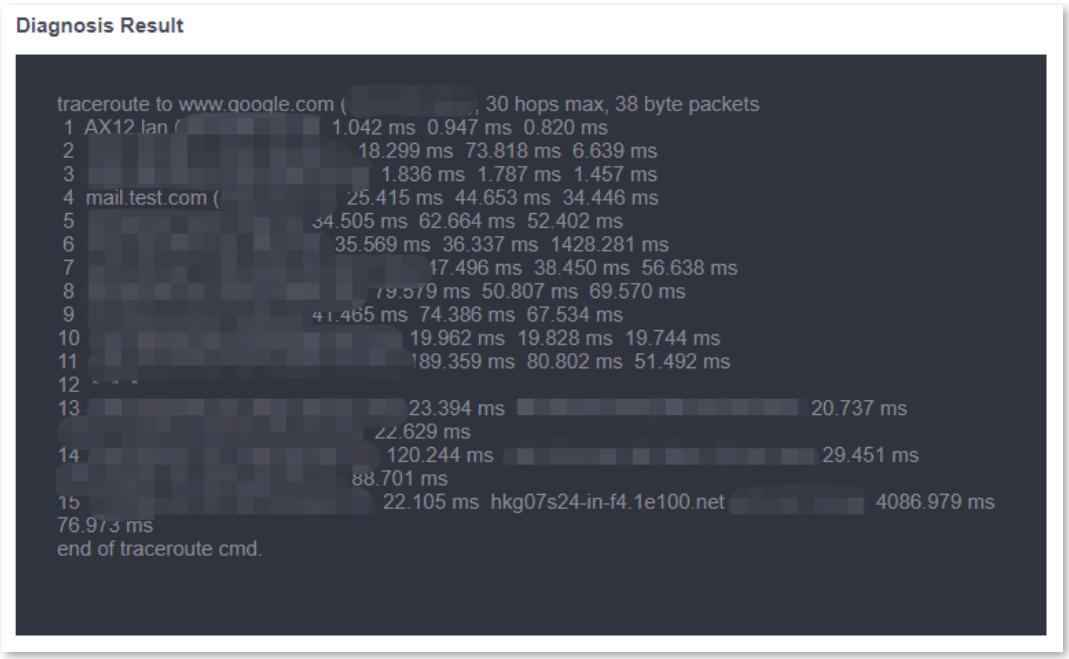
Step 4 Enter **IP Address/Domain Name** of the tracert target, which is **www.google.com** in this example.

Step 5 Click **Start**.



----End

The diagnosis result is shown in the lower part of the page. See the following figure.



Parameter description

Parameter	Description
Egress Option	Specifies the interface from which the data goes out.
IP Address/Domain Name	Specifies the IP address or domain name of the target host.

9.2.3 Packet capture tool

Packet Capture Tool is a network data collection and analysis tool, which can completely intercept the specified data packets in the network to provide analysis.

To access the configuration page, log in to the web UI of the router, and navigate to **Tool** > **Diagnosis** to enter the page.

Here, you can intercept the specified data packets of an interface with **Packet Capture Tool**.

Assume that you want to intercept all types of data packets from the router's LAN4 port. The IP address of the LAN4 port is 192.168.0.250, which belongs to **VLAN_Default**.

Configuration procedure:

Step 1 Log in to the web UI of the router, and navigate to **Tool** > **Diagnosis**.

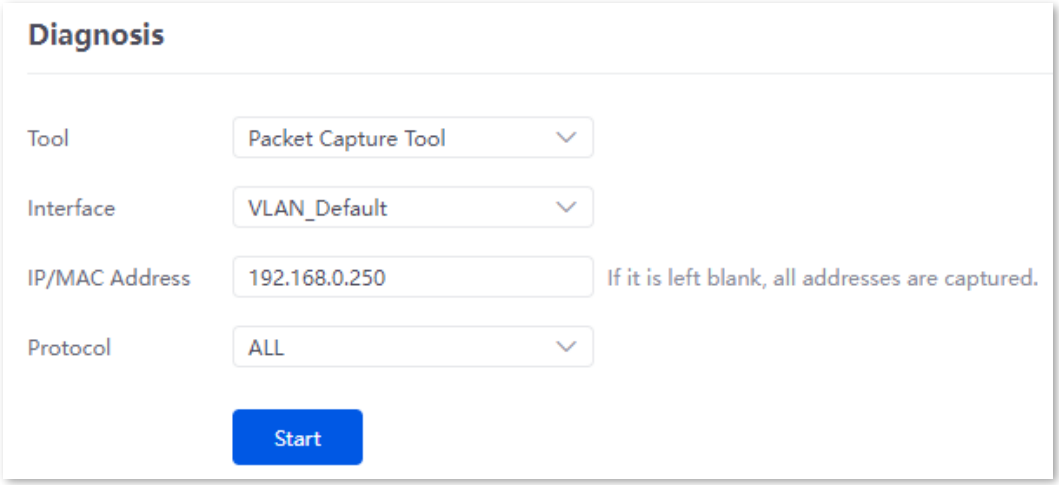
Step 2 Select **Packet Capture Tool** from the **Tool** drop-down list box.

Step 3 Set **Interface** to the VLAN interface to intercept data, which is **VLAN_Default** in this example.

Step 4 Set **IP/MAC Address** of the LAN4 port, which is **192.168.0.250** in this example.

Step 5 Set **Protocol**, which is **ALL** in this example.

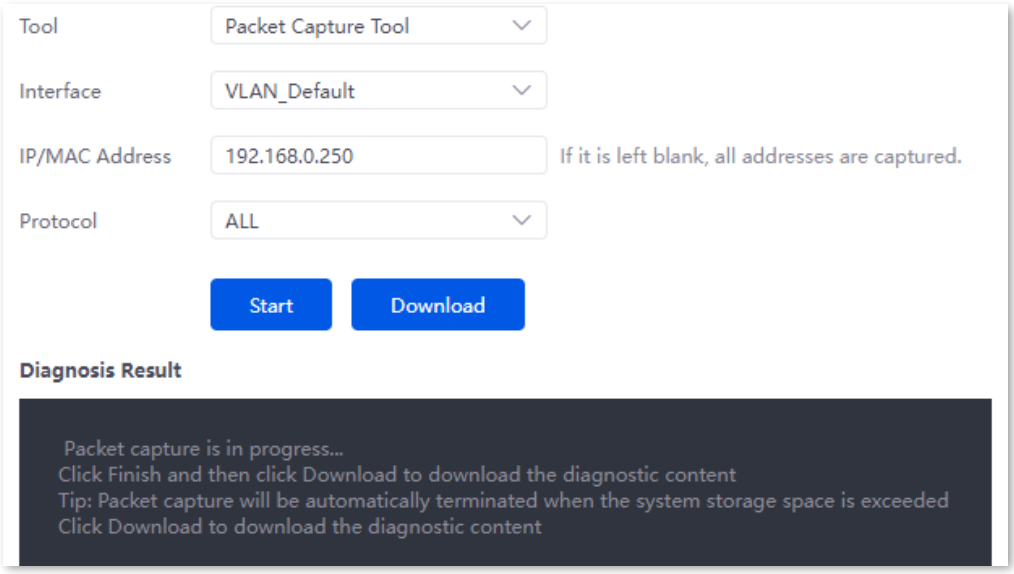
Step 6 Click **Start**.



Step 7 (Optional) During packet capture, click **End** as required.

Step 8 Click **Download**.

The pcap file will be downloaded to the local computer, which can be opened and viewed with the packet capture firmware (such as **WireShark**).



----End

Parameter description

Parameter	Description
Interface	Specifies the VLAN interface whose data will be intercepted.
IP/MAC Address	Specifies the IP address or MAC address whose data will be intercepted. TIP If the IP address or MAC address does not exist in the network or is not under the VLAN, no packets will be intercepted.
Protocol	Specifies the protocol type of data to be intercepted. **ALL** indicates that **ICMP**, **TCP**, **UDP** and **ARP** are all included. - **ICMP**: Abbreviated for Internet Control Message Protocol. It is used to transmit control messages between IP hosts and routers, including whether the network or the host is reachable, and whether the route is available. - **TCP:** Abbreviated for Transmission Control Protocol. The connection is established through the three-way handshaking. When the communication is completed, the connection should be removed. It can only be used for end-to-end communication, such as Telnet and FTP. - **UDP**: Abbreviated for User Datagram Protocol. UDP data includes destination port and source port information. The communication does not require connection, and the broadcast transmission can be realized. Services using **UDP** include DNS and SNMP. - **ARP**: Abbreviated for Address Resolution Protocol. It is a TCP/IP protocol that obtains physical addresses based on IP addresses.

9.2.4 System diagnosis

To access the configuration page, log in to the web UI of the router, and navigate to **Tool** > **Diagnosis** to enter the page.

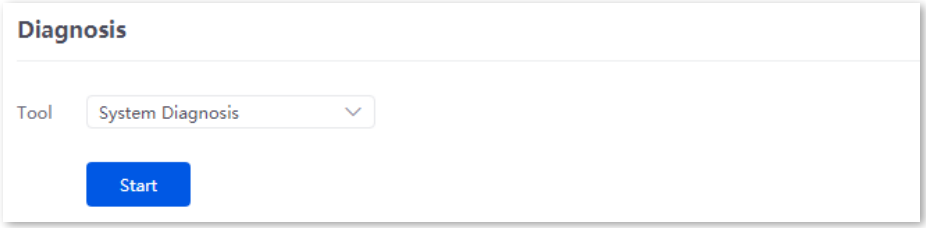
Here, you can view the status information of all processes in the system.

To perform system diagnosis:

Step 1 Log in to the web UI of the router, and navigate to **Tool** > **Diagnosis**.

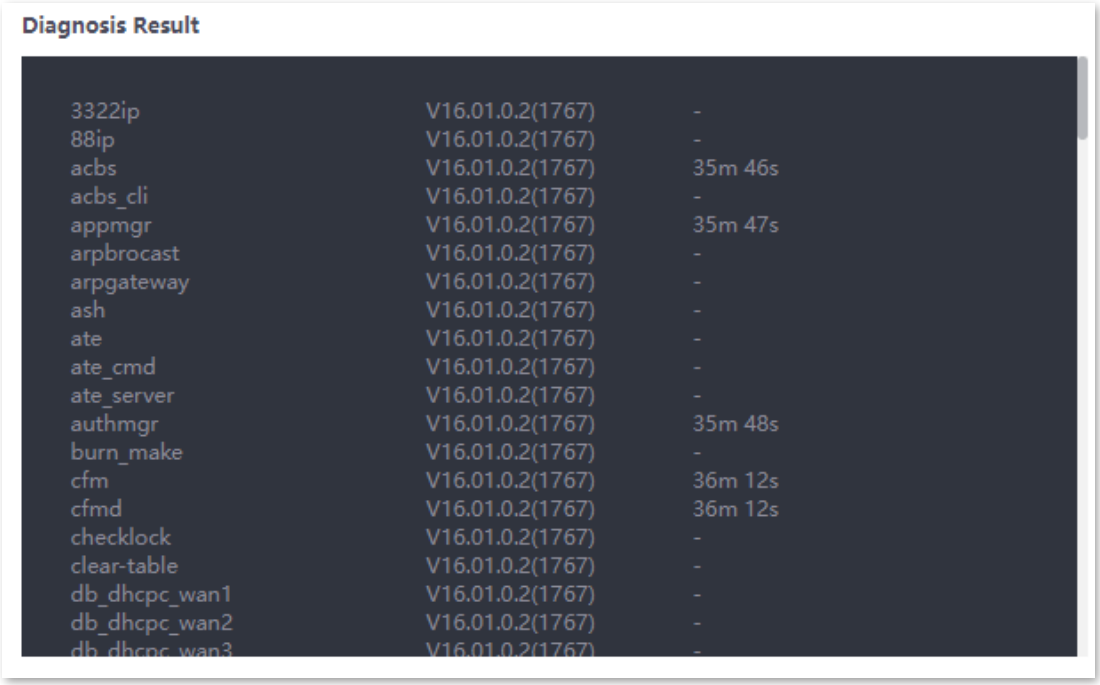
Step 2 Select **System Diagnosis** from the **Tool** drop-down list box.

Step 3 Click **Start**.



---End

The diagnosis result is shown in the lower part of the page, and you can pull the scroll bar to see more information. See the following figure.



9.2.5 Interface info

To access the configuration page, log in to the web UI of the router, and navigate to **Tool** > **Diagnosis** to enter the page.

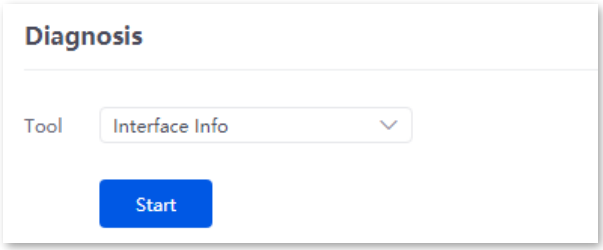
Here, you can view the interface information of the router, including the physical interface, bridging interface, tunnel interface and VLAN virtual interface. The bridging interface and the VLAN virtual interface are generated when the VLAN is created, but no VLAN virtual interface is generated when the VLAN is 0. The tunnel interface is generated when the SSID policy is created.

To check the interface information:

Step 1 Log in to the web UI of the router, and navigate to **Tool** > **Diagnosis**.

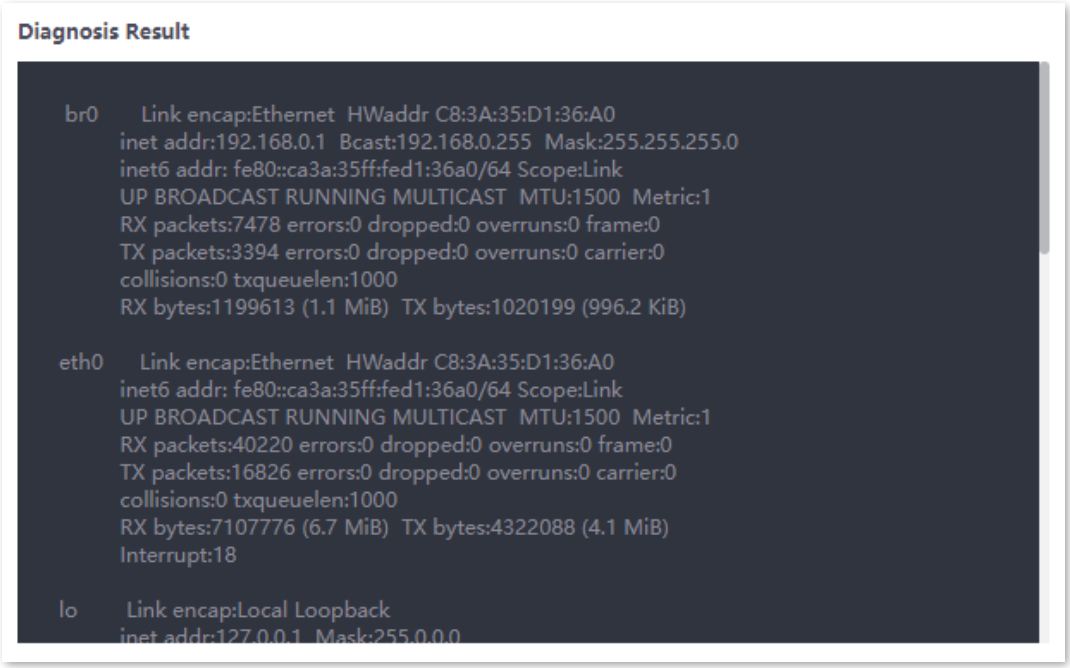
Step 2 Select **Interface Info** from the **Tool** drop-down list box.

Step 3 Click **Start**.



---End

The diagnosis result is shown in the lower part of the page, and you can pull the scroll bar to see more information. See the following figure.



9.3 Log center

To access the configuration page, log in to the web UI of the router, and navigate to **Tool** > **Log Center** to enter the page.

Here, you can view the log information recorded by the router.

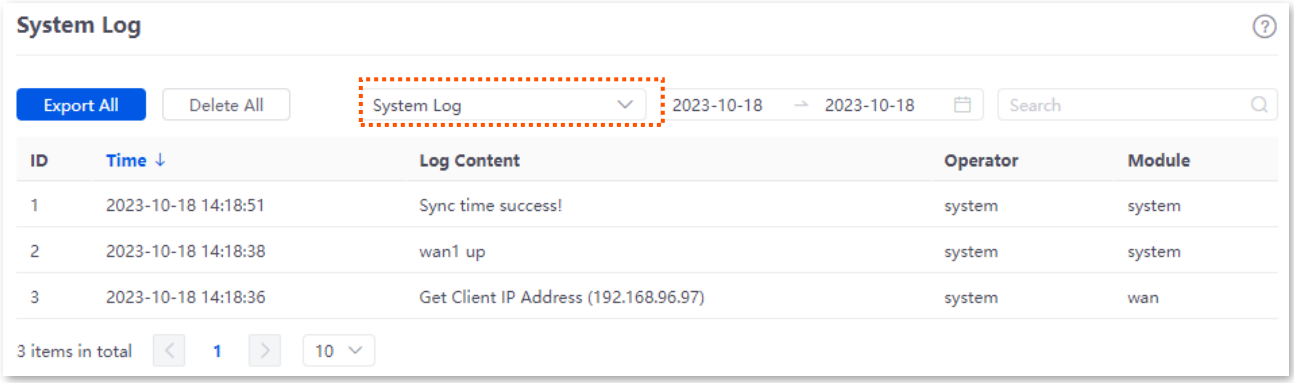
The log center records the **System Log**, **Operating Log** and **Running Log** of the router. In case of network failure, you can use the router's log center to troubleshoot the problem.

The time of the logs depends on the system time of the router. To make sure the time of the logs is correct, set correctly System time of the router first.

9.3.1 System log

The **System Log** records events of the system, such as DHCP log, dial-up log.

To access the configuration page, log in to the web UI of the router, and navigate to **Tool** > **Log Center** > **System Log** to enter the page. Click the drop-down list box on this page. You can view certain log information of the router.

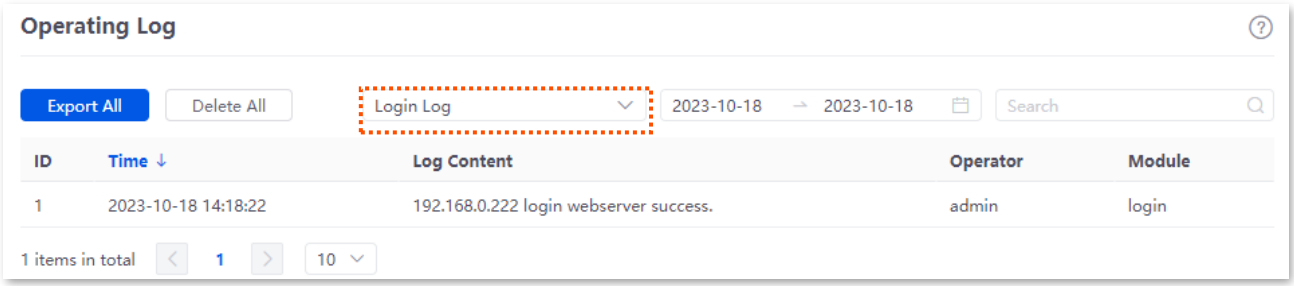


9.3.2 Operating log

The **Operating Log** records the operation information that the user performed in the system, such as login log, configuration modification.

To access the configuration page, log in to the web UI of the router, and navigate to **Tool** > **Log Center** > **Operating Log** to enter the page.

Here, you can view certain operation information of the router by selecting log types from the drop-down list box highlighted on the following figure.

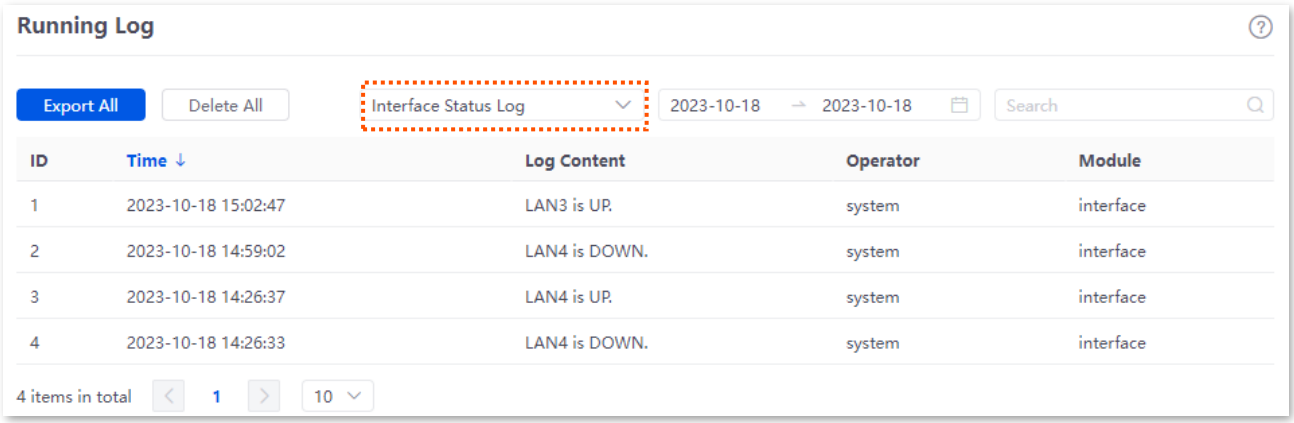


9.3.3 Running log

The **Running Log** records the information of the system process running and the interface status.

To access the configuration page, log in to the web UI of the router, and navigate to **Tool** > **Log Center** > **Running Log** to enter the page.

You can view certain information of the system process running and the interface status report of the router by selecting log types from the drop-down list box highlighted on the following figure.

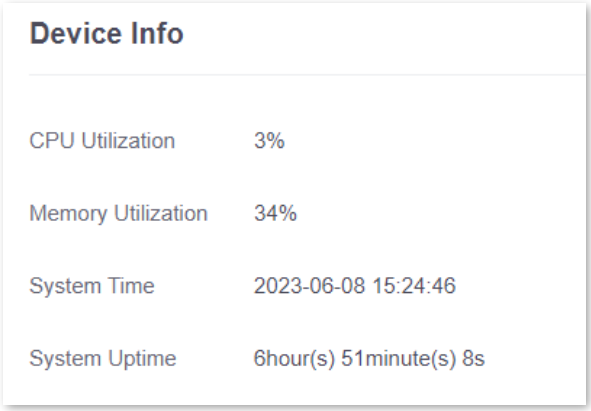


9.4 System maintenance

9.4.1 Device info

To access the configuration page, log in to the web UI of the router, and navigate to **Tool** > **Maintenance** > **Device Info** to enter the page.

Here, you can view the basic composition and usage of current system hardware, as well as system time and running time.



9.4.2 Restore & Backup

Overview

You can use the Backup function to copy the current configurations of the router to the local computer and use the Configuration Restoration function to restore the configurations of the router to the backed-up configurations.

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.

To access the configuration page, log in to the web UI of the router, and navigate to **Tool** > **Maintenance** > **Restore & Backup** to enter the page.

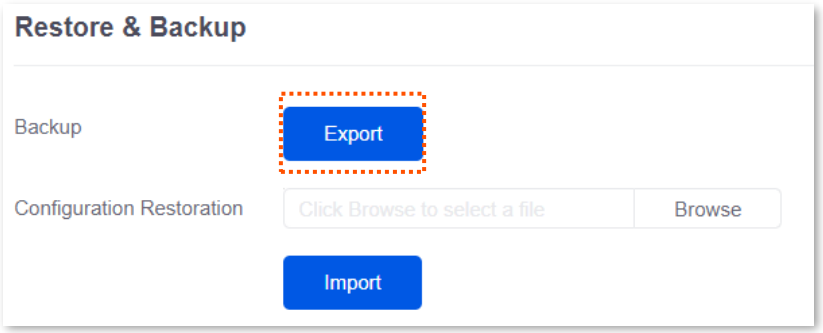
Here, you can use the backup and restore function.

Backup

Step 1 Log in to the web UI of the router.

Step 2 Navigate to **Tool** > **Maintenance** > **Restore & Backup**.

Step 3 Click **Export**.



----End

The browser will download a configuration file named **RouterCfm.cfg**.

TIP

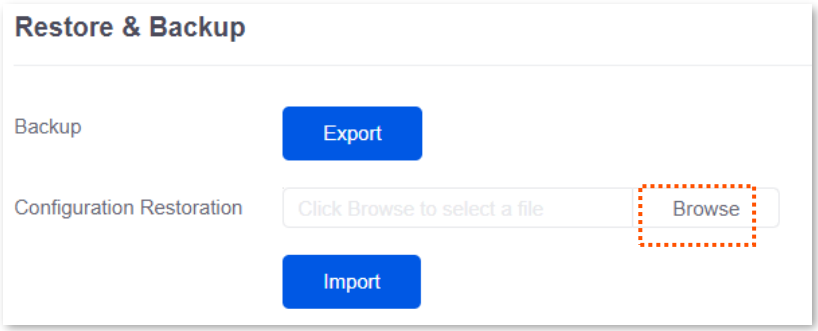
If the message “This type of file can harm your computer. Do you want to keep RouterCfm.cfg anyway?” appears on the page, click **Keep**.

Restore

Step 1 Log in to the web UI of the router.

Step 2 Navigate to **Tool** > **Maintenance** > **Restore & Backup**.

Step 3 Click **Browse**, and select the configuration file you have backed up.



Step 4 Click **Import**.

Step 5 Confirm the prompt information, and click **OK**.

----End

A reboot progress bar appears. When the progress bar reaches 100%, the router is restored successfully.

9.4.3 Factory settings restore

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 device using web UI
- Reset the device using the Reset/Extend button

After the reset, the default LAN IP address of the router is 192.168.0.1.

NOTE

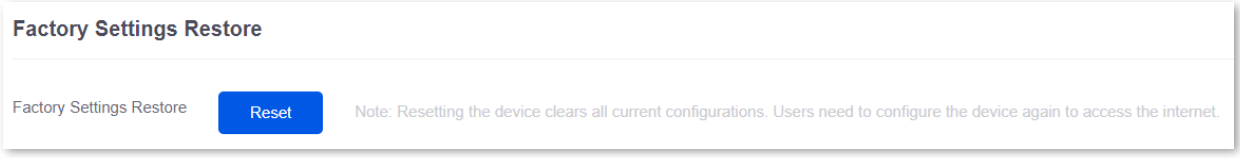
- Resetting the router clears all current configurations. It is recommended to back up the current configurations before the reset.
- After the reset, the router will be restored to factory settings and you can access the internet only after you reconfigure it. Reset the router with caution.
- To avoid damaging the router, ensure that the router is properly powered on throughout the reset.

Reset the device using web UI

Step 1 Log in to the web UI of the router.

Step 2 Navigate to **Tool** > **Maintenance** > **Factory Settings Restore**.

Step 3 Click **Reset**.



Step 4 Confirm the prompt information, and click **OK**.

----End

A reset progress bar appears. When the progress bar reaches 100%, the router is restored to factory settings successfully. Please configure the router again.

Reset the device using the Reset/Extend button

When using this method, you can restore the router to factory settings without logging in to the web UI of the router. The operation method is as follows:

When the **SYS** LED indicator is blinking, hold down the **Reset/Extend** button for about 8 seconds and release it when the **SYS** LED indicator light is solid green. When the **SYS** LED indicator blinks again, the router is reset successfully.

9.5 Upgrade service

9.5.1 Overview

To access the configuration page, log in to the web UI of the router, and navigate to **Tool** > **Upgrade Service** to enter the page.

Here, you can upgrade the system firmware and feature-library of the router to get a better user experience.

- **System firmware upgrade:** You can upgrade the system firmware of the router to experience more functions and get a better user experience. The router supports **Local Upgrade** and **Online Upgrade**. The default upgrade mode is **Local Upgrade**.
- **feature-library upgrade:** It enables you to upgrade the URL category in filter management module without updating the router's firmware. The router supports **Local Upgrade** and **Online Upgrade**. The default upgrade mode is **Local Upgrade**.

Parameter description

Parameter	Description
Local Upgrade	Download the upgrading file from the official website (www.tendacn.com) to the local computer, decompress it and upgrade the system using the decompressed file. The format of the decompressed file is ".bin".
Online Upgrade	When the router is connected to the internet, it will automatically detect whether there is a new program for upgrading and show the relevant information about the upgrading firmware detected. After you click **Upgrade**, the router will automatically download the upgrading file and perform upgrading. Do not power off the device during the process.

9.5.2 System firmware upgrade

NOTE

- To avoid damage to the router, ensure that the correct upgrade file is used. Generally, a firmware upgrade file is suffixed with **.bin**.
- During the upgrade, do not power off the router.

To access the configuration page, log in to the web UI of the router, and navigate to **Tool** > **Upgrade Service** > **System Firmware Upgrade** to enter the page.

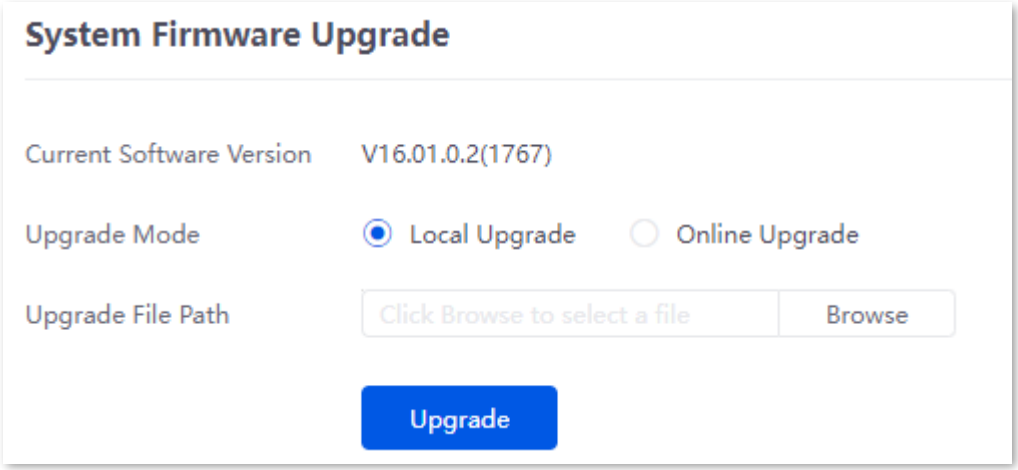
Here, you can upgrade the firmware of the router.

Step 1 Visit www.tendacn.com, download the upgrade firmware of the corresponding model to your computer and unzip it.

Step 2 Log in to the web UI of your router, and navigate to **Tool** > **Upgrade Service** > **System Firmware Upgrade**.

Step 3 Select **Local Upgrade** for **Upgrade Mode**.

Step 4 Click **Browse**. Select and upload the firmware that has been downloaded to your computer in step 1, and click **Upgrade**.



Step 5 Confirm the prompt information, and click **OK**.

----End

After the progress bar completes, you can log in to the router again and check whether **Current Software Version** in **Tool** > **Upgrade Service** > **System Firmware Upgrade** is the one that you upgraded. If yes, the upgrade is successful.

TIP

To better experience the stability and new functions of the firmware, after the upgrade, you are recommended to restore the router to factory settings and configure it again.

9.5.3 Feature-Library upgrade

NOTE

- To avoid damage to the router, ensure that the correct upgrade file is used. Generally, a feature-library upgrade file is suffixed with **.bin**.
- During the upgrade, do not power off the router.

To access the configuration page, log in to the web UI of the router, and navigate to **Tool** > **Upgrade Service** > **Feature-Library Upgrade** to enter the page.

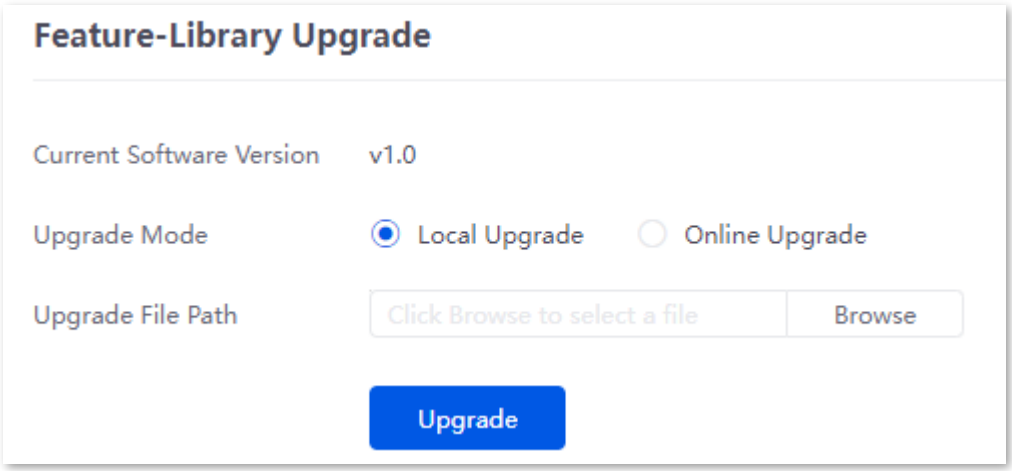
Here, you can upgrade the feature-library of the router.

Step 1 Visit www.tendacn.com, download the feature-library of the corresponding model to your computer and unzip it.

Step 2 Log in to the web UI of your router, and navigate to **Tool** > **Upgrade Service** > **Feature-Library Upgrade**.

Step 3 Select **Local Upgrade** for **Upgrade Mode**.

Step 4 Click **Browse**. Select and upload the feature-library that has been downloaded to your computer in step 1, and click **Upgrade**.



Step 5 Confirm the prompt information, and click **OK**.

----End

After the progress bar completes, you can log in to the router again and check whether **Current Software Version** in **Tool** > **Upgrade Service** > **Feature-Library Upgrade** is the one that you upgraded. If yes, the upgrade is successful.

9.6 Reboot devices

9.6.1 Reboot

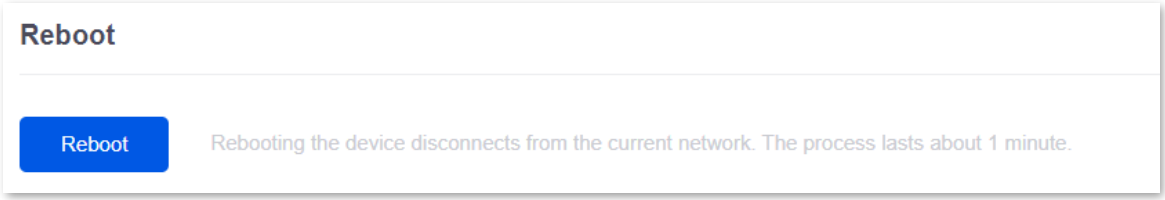
To access the configuration page, log in to the web UI of the router, and navigate to **Tool** > **Reboot Services** > **Reboot** to enter the page.

Here, you can reboot the router to make certain settings take effect and improve the performance of the router. Rebooting the device disconnects from the current network. The process lasts about 1 minute. It is recommended to reboot the device when the network is relatively idle.

Reboot steps:

Step 1 Log in to the web UI of the router.

Step 2 Navigate to **Tool** > **Reboot Services** > **Reboot**, and click **Reboot**.



Step 3 Confirm the prompt information, and click **OK**.

----End

9.6.2 Scheduled reboot

To access the configuration page, log in to the web UI of the router, and navigate to **Tool** > **Reboot Services** > **Scheduled Reboot** to enter the page.

Here, by setting the router to reboot periodically during leisure time, you can prevent the decreasing of performance and instability of the router after running for a long period.

TIP

The time of reboot depends on the system time of the router. To make sure the time of the reboot is correct, set correctly System time of the router first.

Scheduled reboot steps:

Step 1 Log in to the web UI of the router.

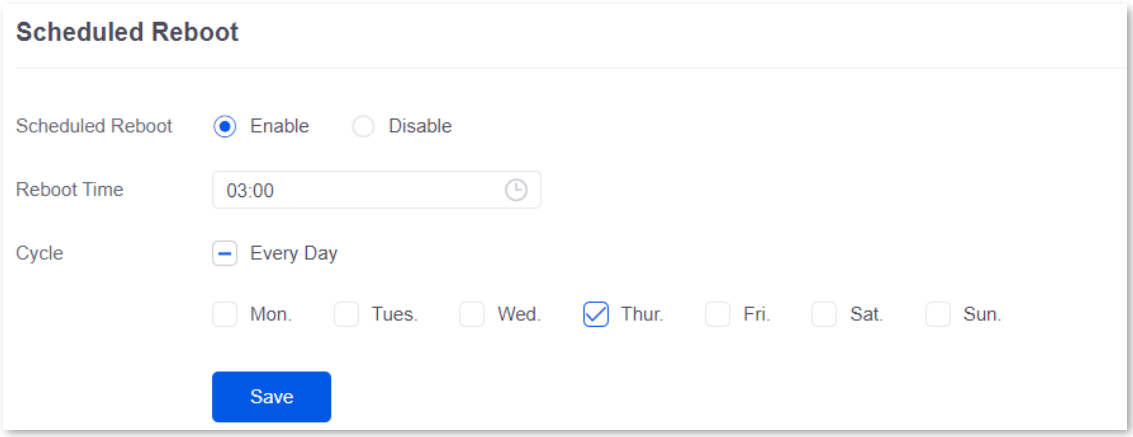
Step 2 Navigate to **Tool** > **Maintenance** > **Scheduled Reboot**.

Step 3 Select **Enable** for **Scheduled Reboot**.

Step 4 Select the time when the router will automatically reboot, which is **03:00** in this example.

Step 5 Select the reboot date, which is **Thur.** in this example.

Step 6 Click **Save**.



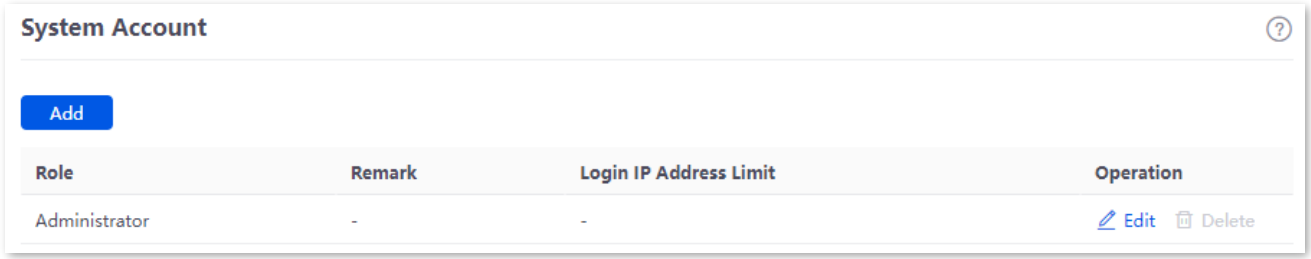
----End

After the above settings are completed, the router will automatically reboot at 3:00 am every Thursday.

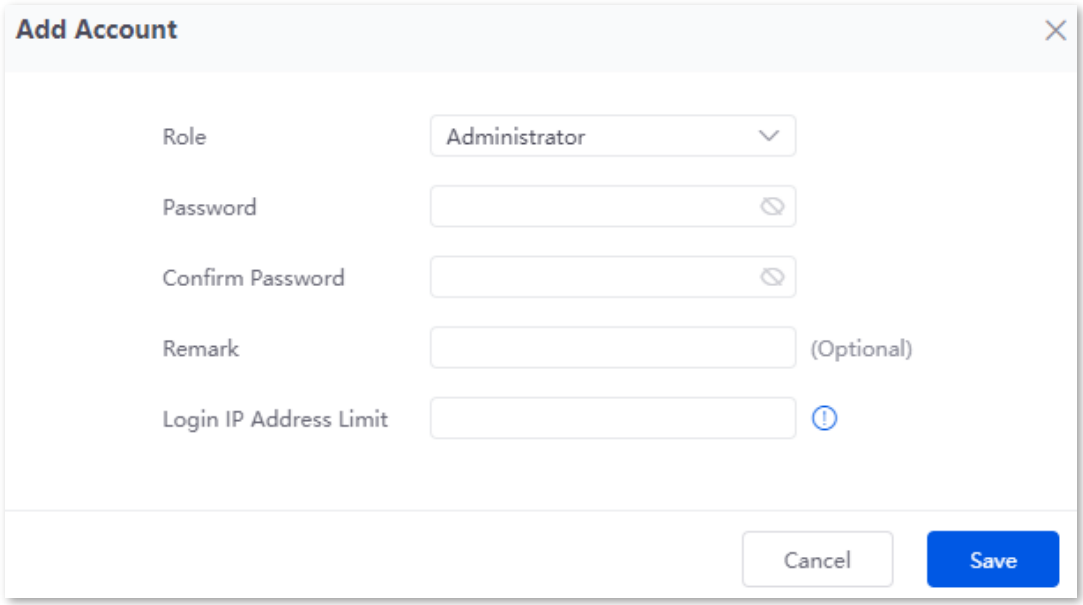
9.7 System account

To access the configuration page, log in to the web UI of the router, and navigate to **Tool** > **System Account** to enter the page.

Here, you can add, modify or delete the administrator and visitor accounts.



You can click **Add** to add an account.



Parameter description

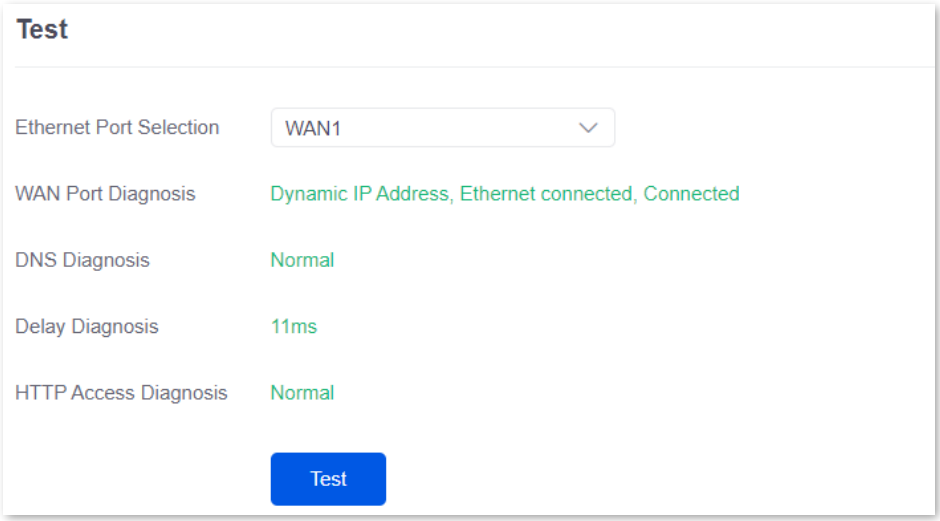
Parameter	Description
Add	Used to add a new system account.
Role	Specifies the user role in managing the web UI. There is an administrator account by default. The operation authority of corresponding user roles is described as follows: - **Administrator**: Able to view and configure all functions of the router. - **Visitor**: Only able to view configurations of the router except system account information.
Password	Used to set the login password of the account.
Confirm Password	

Parameter	Description
Remark	Specifies the remark for the account. You can enter the description for the operation permission of the account.
Login IP Address Limit	Specifies the IP addresses of the users of the account. After the configuration, only users with the IP address or within the IP address range can use the account to access the web UI.

9.8 Test

To access the configuration page, log in to the web UI of the router, and navigate to **Tool** > **Test** to enter the page.

Here, you can perform a network test on the WAN port of the router.



Parameter description

Parameter	Description
Ethernet Port Selection	Specifies the WAN port to be tested.
WAN Port Diagnosis	Used to test the WAN port's connection type, Ethernet cable connection status and internet connection status.
DNS Diagnosis	Used to test whether the WAN port can resolve the domain name properly.
Delay Diagnosis	Used to test the network delay of the WAN port.
HTTP Access Diagnosis	Used to test whether the WAN port can receive HTTP response normally.

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
DHCPv6	Dynamic Host Configuration Protocol for IPv6
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

Acronym and Abbreviation	Full Spelling
GI	Guard Interval
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ICMP	Internet Control Message Protocol
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
MTU	Maximum Transmission Unit
NAT	Network Address Translation
NTS	Network Time Server
OA	Office Automation
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

Acronym and Abbreviation	Full Spelling
RSSI	Received Signal Strength Indicator
SA	Security Association
SKEME	Security Key Exchange Mechanism
SLAAC	Stateless Address Autoconfiguration
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management 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
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WAN	Wide Area Network
WMM	WiFi Multi-Media
WPA	WiFi Protected Access
WPA-PSK	WPA-Preshared Key