www.ip-com.com.cn

User Guide

AC2600 Enterprise Mesh Wi-Fi System

IP-COM
World Wide Wireless

Copyright Statement

IP-COM is the registered trademark of IP-COM Networks Co., Ltd. Other brand and product names mentioned herein are trademarks or registered trademarks of their respective holders. Copyright of the whole product as integration, including its accessories and software, belongs to IP-COM Networks Co., Ltd. No part of this publication can be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means without the prior written permission of IP-COM Networks Co., Ltd.

Disclaimer

Pictures, images and product specifications herein are for references only. To improve internal design, operational function, and/or reliability, IP-COM reserves the right to make changes to the products described in this document without obligation to notify any person or organization of such revisions or changes. IP-COM does not assume any liability that may occur due to the use or application of the product or circuit layout(s) 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 the warranty of any kind, express or implied.

Preface

Thank you for choosing IP-COM. Please read this user guide before you start with AC1200 Enterprise Mesh WiFi System.

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 the device.
Tip	This format is used to highlight a procedure that will save time or resources.

For more documents

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

Technical Support

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

☎	✉	🏠
+86-755-27653089	info@ip-com.com.cn	www.ip-com.com.cn

Contents

1 Login

1.1 Log in to the web UI

For initial use of this device, you can refer to quick installation guide to complete the setup wizard before entering the web.

If the device has been configured, please refer to the steps as follows.

1.1.1 Log in to the Cable-Free (Router Mode) device

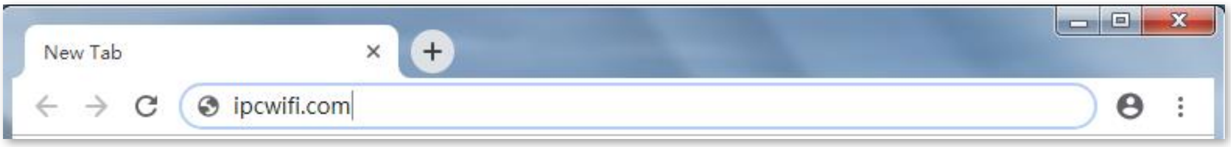
Tip

– In **Cable-Free (Router Mode)**, the PoE WAN/LAN port of the device is a WAN port.

– The device works in **Cable-Free (Router Mode)** by default.

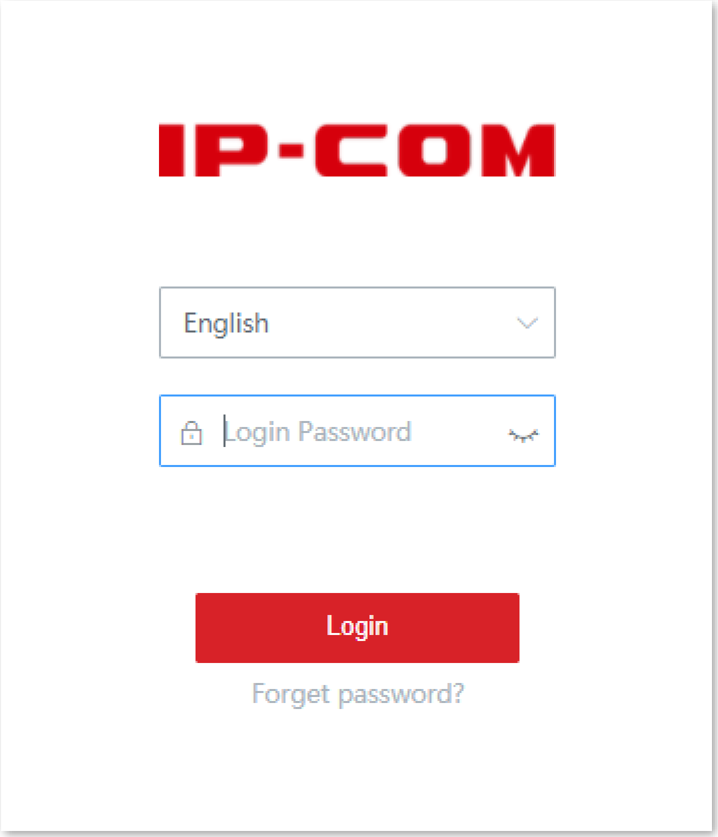
- **Log in with your computer**

1. Connect a computer to a LAN port of the device.
2. Start a browser on the computer, such as Google Chrome, and visit **www.ipcwifi.com**.



ipcwifi.com

3. Enter the login password, and click **Login**.



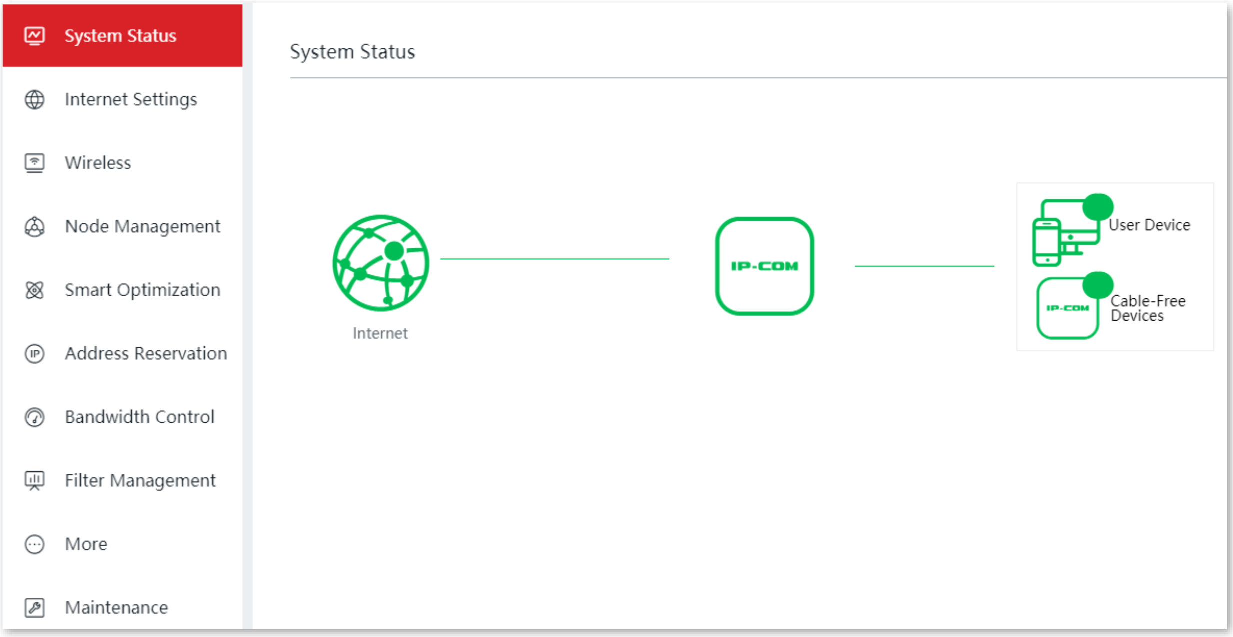
----End

Tip

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

- Ensure that the device is powered successfully.
- Ensure that your computer is connected to the LAN port of the device, and set the computer to obtain IP address and DNS server address automatically.
- Reset the device and log in again. How to rest the device: When the device system starts up, press the RESET button with a sharp object for about 8 seconds. When SYS indicator is solid on, the device will be reset. When the SYS indicator blinks again, the device is reset successfully.

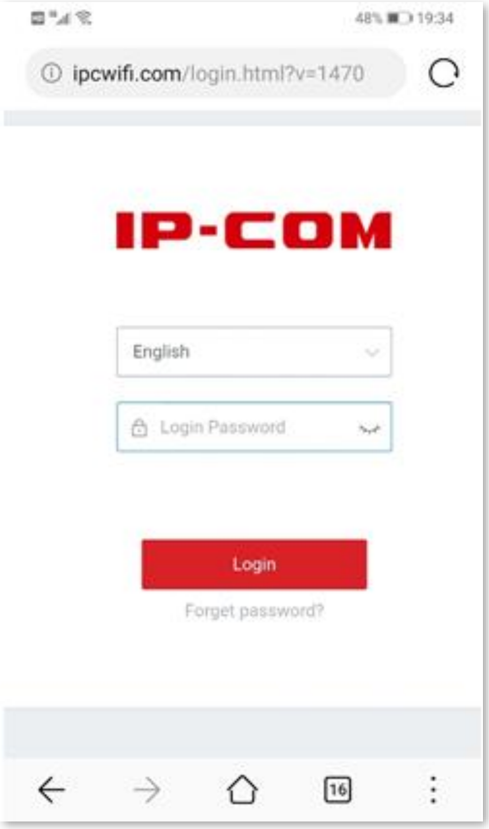
Log in to the web UI successfully. See the following figure.



- **Log in with your smart phone/ipad**

  Take smart phones for example.

1. Connect your smart phone to the WiFi network of the device.
2. Start a browser on the phone, and visit **www.ipcwifi.com**.
3. Enter the login password, and click **Login**.



Tip

If the above page does not appear, please try the following solution:

- Ensure that your smart phone is connected to the WiFi network.
- Ensure that you disable the mobile data.
- Reset the device and log in again. How to rest the device: After the system has started, press the RESET button with a sharp object for about 8 seconds. When SYS indicator is solid on, the device will restore. When the SYS indicator blinks again, the device is reset successfully.

----End

1.1.2 Log in to the Cable-Free (AP Mode) device

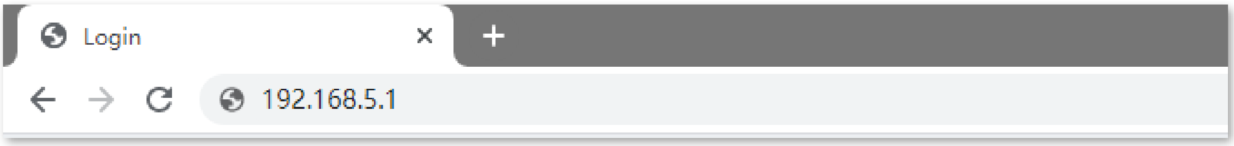
Tip

In **Cable-Free (AP Mode)**, the PoE WAN/LAN1 port of the device is a LAN port.

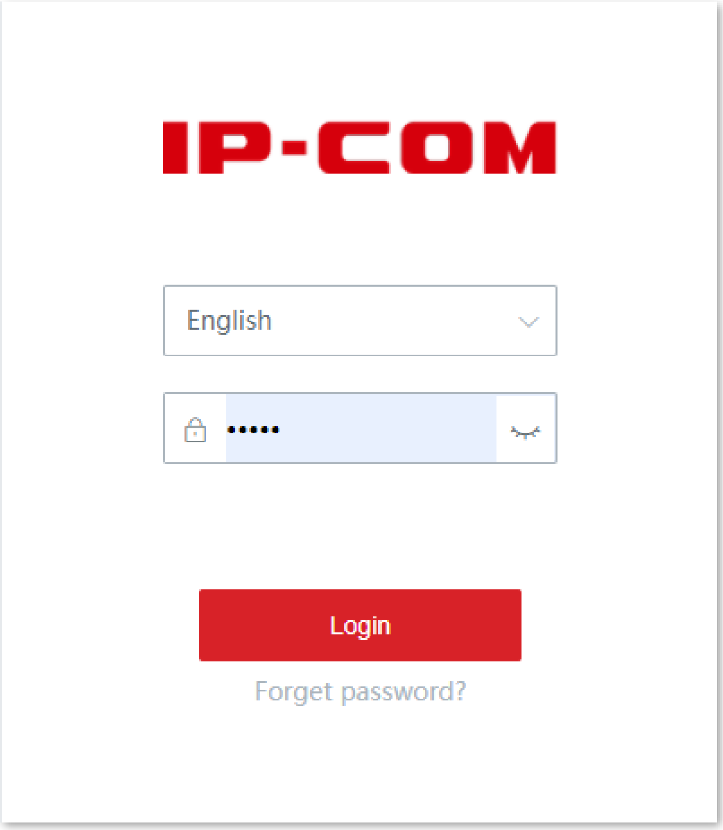
- **Log in with your computer**

1. Connect the computer to the LAN port of the device with an Ethernet cable.
2. Set the Ethernet IP address of the computer to the same segment of the device.

   For example, if the IP address of device is **192.168.5.1**, the IP address of the computer can be set to **192.168.5.X** (X ranges from 2~254 and is not occupied by other devices), and the subnet mask is **255.255.255.0**.
3. Start a browser of your computer, such as google, and enter the management IP address of the device, which is 192.168.5.1 in this example.



4. Enter the login password and click **Login**.



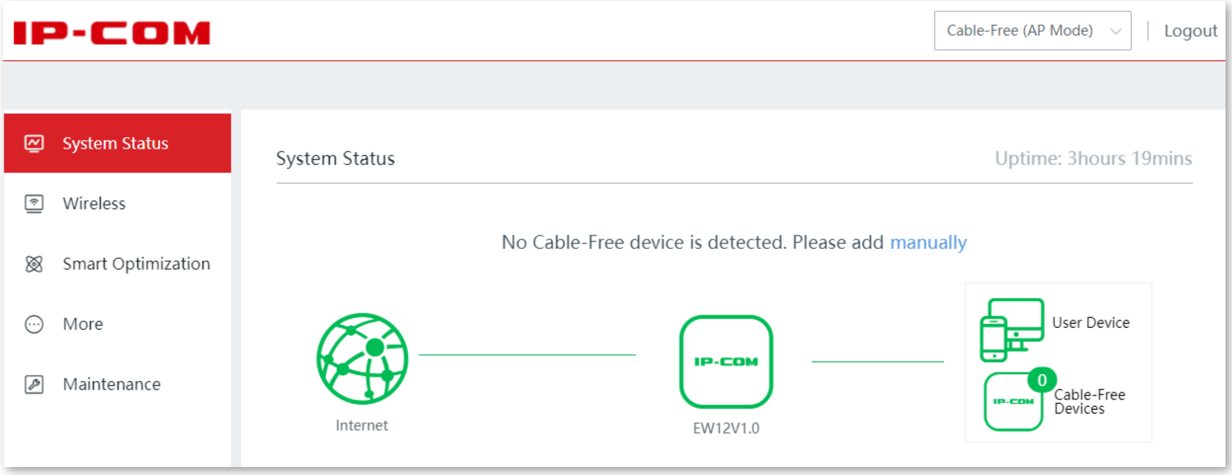
Tip

If the above page does not appear, please try the following solution:

- Ensure the device is powered successfully.
- Ensure that the computer is connected to the LAN port of the device and that the Ethernet IP address of the computer is set to the same network segment as the IP address of the device.

----End

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



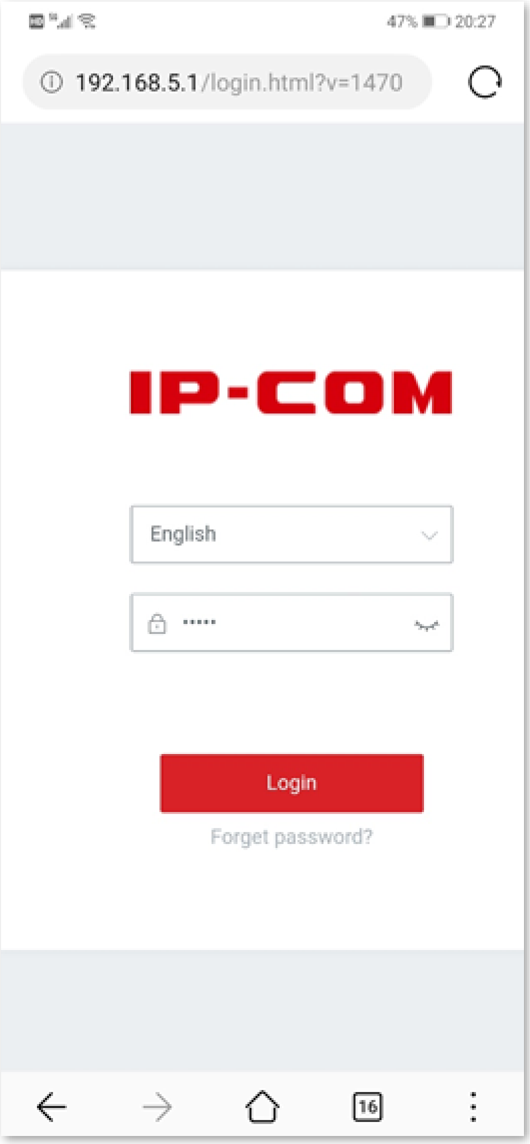
No Cable-Free device is detected. Please add manually

- **Log in with your smart phone/ipad**

Take smart phones for example.

1. Connect your smart phone to the WiFi network of the device.
2. Configure the IP address of the phone to be in the same network segment as the IP address of the device.

   For example, if the IP address of device is **192.168.5.1**, the IP address of smart phone can be set to **192.168.5.X** (X ranges from 2~254 and is not occupied by other devices), and the subnet mask is **255.255.255.0**.
3. Start a browser on the phone, and visit **192.168.5.1**.
4. Enter the login password, and click **Login**.



47% 20:27

192.168.5.1/login.html?v=1470

IP-COM

English

Login

Forget password?

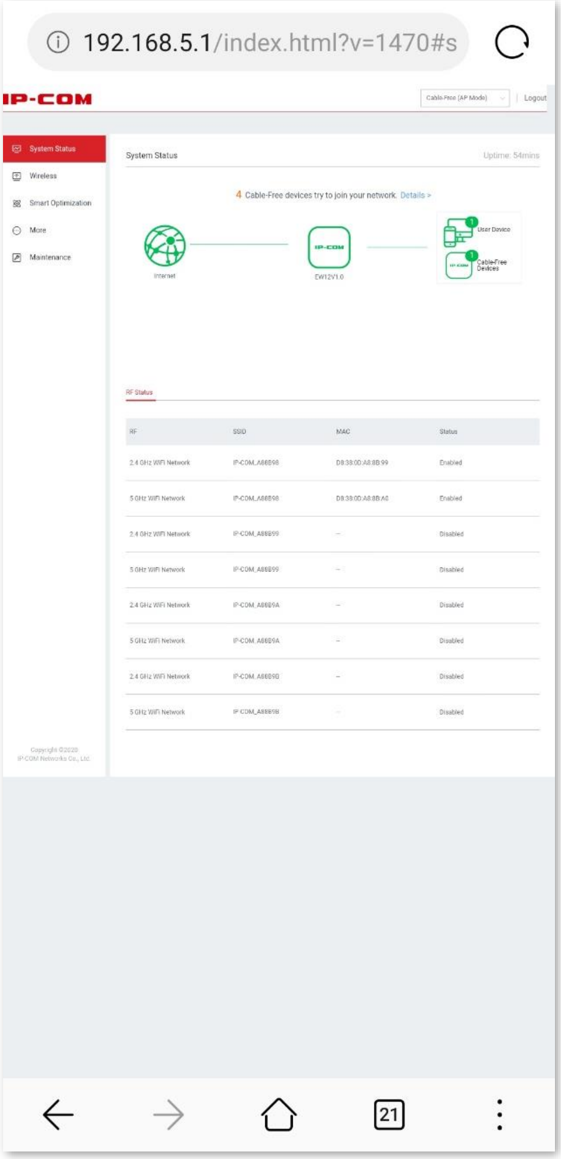
Tip

If the above page does not appear, please try the following solution:

- Ensure your phone has connected to the WiFi network of the device successfully.
- Ensure that you have disabled the mobile data.

----End

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



192.168.5.1/index.html?v=1470#s

System Status

Uptime: 54mins

4 Cable-Free devices try to join your network. Details >

RF	SSID	MAC	Status
2.4 GHz WiFi Network	IP-COM_A88B98	D8:38:0D:A8:8B:99	Enabled
5 GHz WiFi Network	IP-COM_A88B98	D8:38:0D:A8:8B:A0	Enabled
2.4 GHz WiFi Network	IP-COM_A88B99	--	Disabled
5 GHz WiFi Network	IP-COM_A88B99	--	Disabled
2.4 GHz WiFi Network	IP-COM_A88B9A	--	Disabled
5 GHz WiFi Network	IP-COM_A88B9A	--	Disabled
2.4 GHz WiFi Network	IP-COM_A88B9B	--	Disabled
5 GHz WiFi Network	IP-COM_A88B9B	--	Disabled

1.2 Log out of the web UI

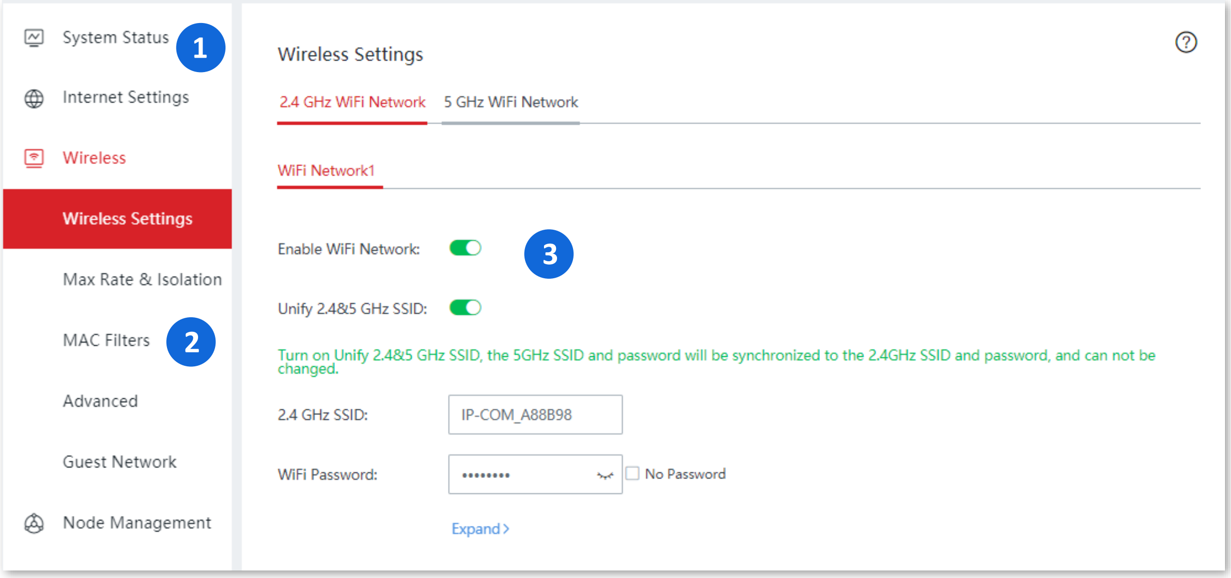
If you log in to the web UI of the device and perform no operation within 20 minutes, the device logs you out automatically.

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

2 Web UI

2.1 Web UI layout

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



Enable WiFi Network: ●

Unify 2.4&5 GHz SSID: ●

Turn on Unify 2.4&5 GHz SSID, the 5GHz SSID and password will be synchronized to the 2.4GHz SSID and password, and can not be changed.

2.4 GHz SSID: IP-COM_A88B98

WiFi Password: •••••••• □ No Password

Tip

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

NO.	Name	Description
1	Level-1 navigation bar	It is used to display the function menu of the device. Users can select functions in the navigation bars and the configuration appears in the configuration area.
2	Level-2 navigation bar	
3	Configuration area	It is used to view or modify your configuration.

2.2 Frequently-used elements

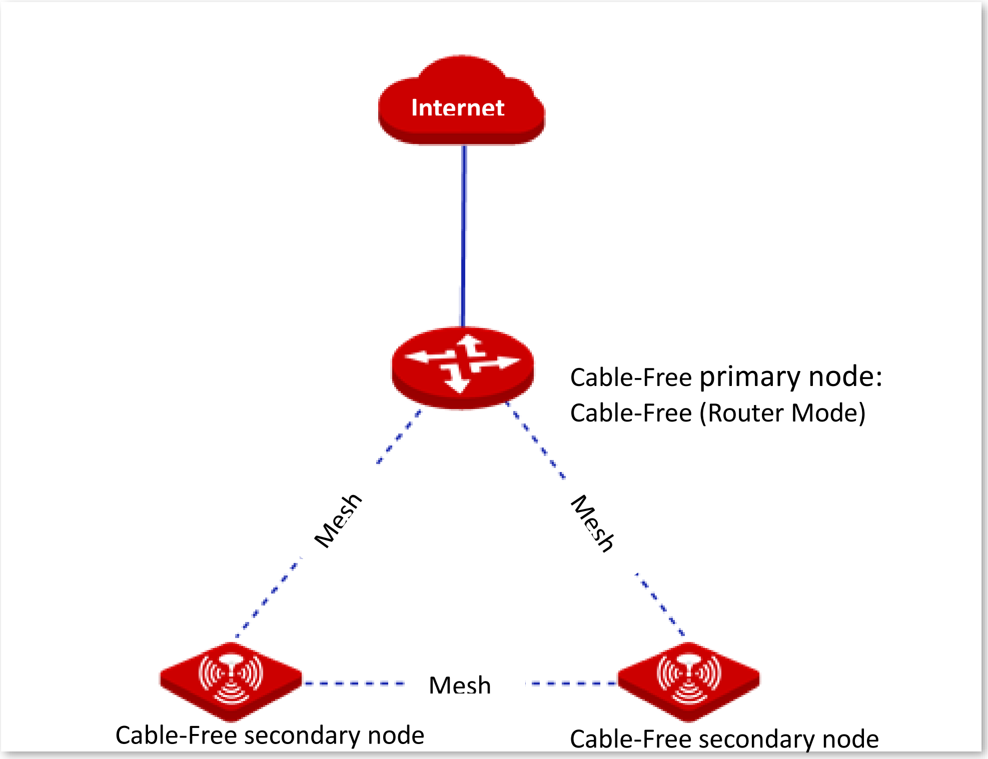
The following table describes the frequently-used buttons available on the web UI of the device.

Button	Description
Save	It is used to save the configuration on the current page and enable the configuration to take effect.
Cancel	It is used to cancel the changes you did before.
Refresh	It is used to refresh the current page to see the latest configuration.
?	It is used to view help information for the current page.
Cable-Free (Router M... ⌄	Click the drop-down box to select and switch the work mode of cable-free device. It supports switching between **Cable-Free (Router Mode)** and **Cable-Free (AP Mode)**.
+ Add	It is used to create a new rule or policy.
🗑 Delete	It is used to delete the selected rule, policy, or information.
✎	It is used to edit the corresponding rule, policy or information.
🗑	It is used to delete the corresponding rule, policy or information.
●, ○	It is used to enable/disable the function. ● specifies to enable the function, ○ specifies to disable the function.
Host Name/IP/MAC 🔍	It is used to search for relevant content on the page. The keywords supported in the search bar are shown in the search bar preset content.

3 Cable-Free (Router Mode)

3.1 Overview

In this mode, the device serves as a device, and provides internet access to form a separate cable-free network with other cable-free devices.



3.2 System status

In this section, you can:

- Check the physical connections.
- Add Mesh devices.
- Check device info.
- Manage online devices.
- Monitor traffic.

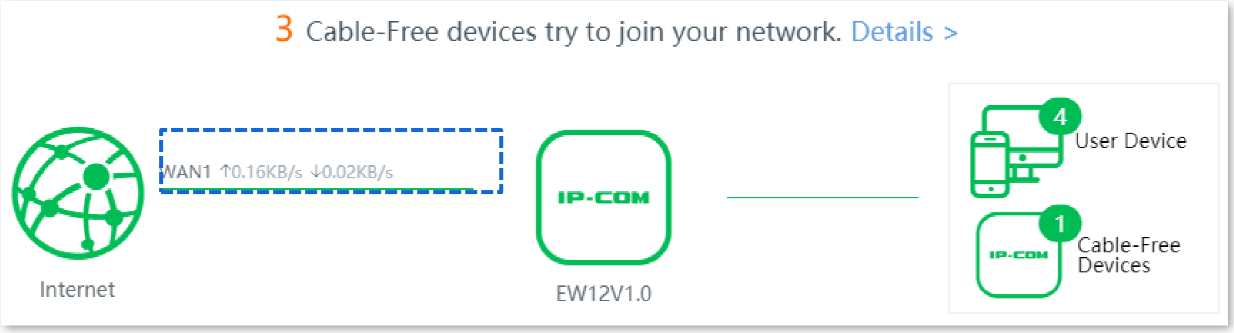
3.2.1 Check physical connections and device info

You can check if the physical connections of the Cable-Free (Router Mode) node are proper, and the basic information of each node in the cable-free network.

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

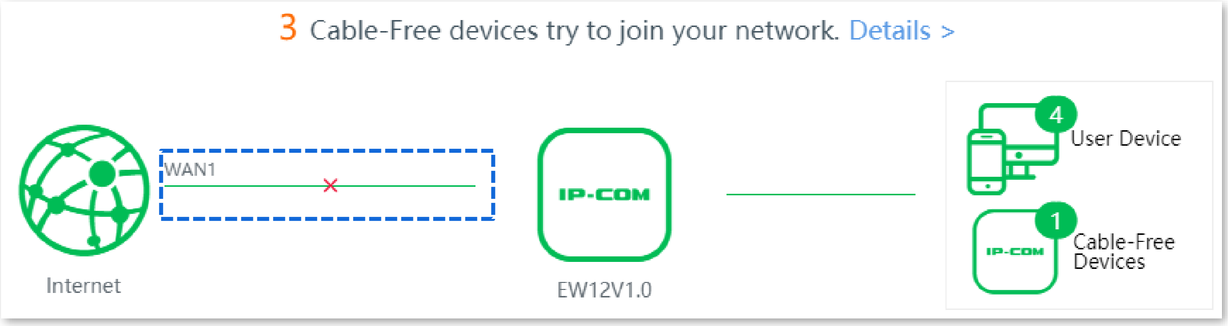
Check the physical connections

The following figure indicates that the Cable-Free (Router Mode) node is connected to the internet properly through the WAN port.



3 Cable-Free devices try to join your network. Details >

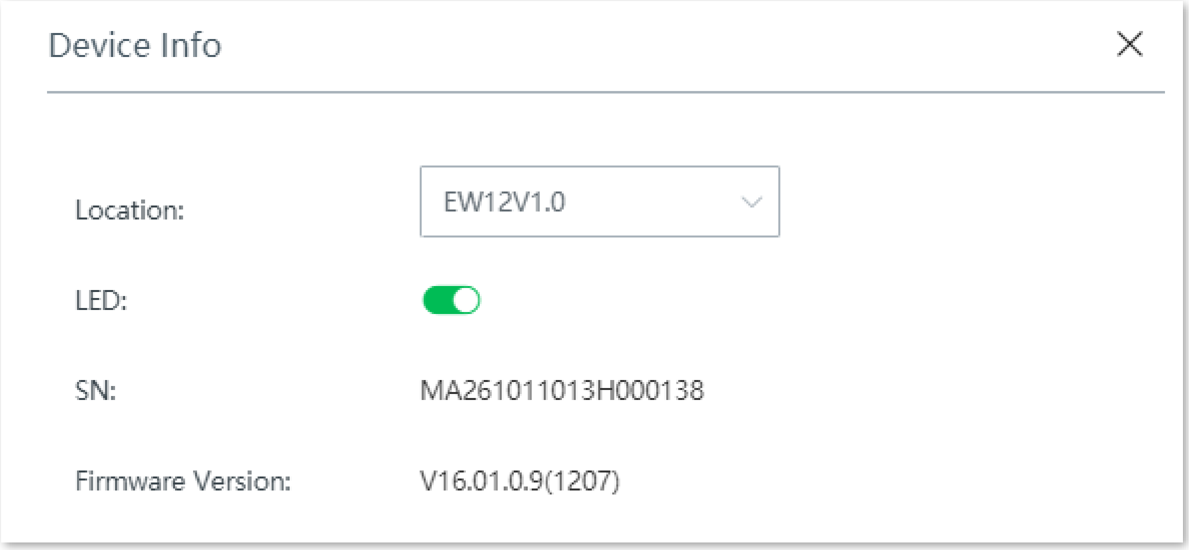
The following figure indicates that connection between the Cable-Free (Router Mode) node and the internet is abnormal. Please check if the WAN port of the device is connected to the internet properly, or the internet connection parameters you set are correct.



Check the information of cable-free primary node

On the **System Status** page, click the icon ▭. You can check the basic device info, operating state, LAN port state and WAN port state of cable-free primary node.

Device info



Device Info

Location: EW12V1.0

LED: ●

SN: MA261011013H000138

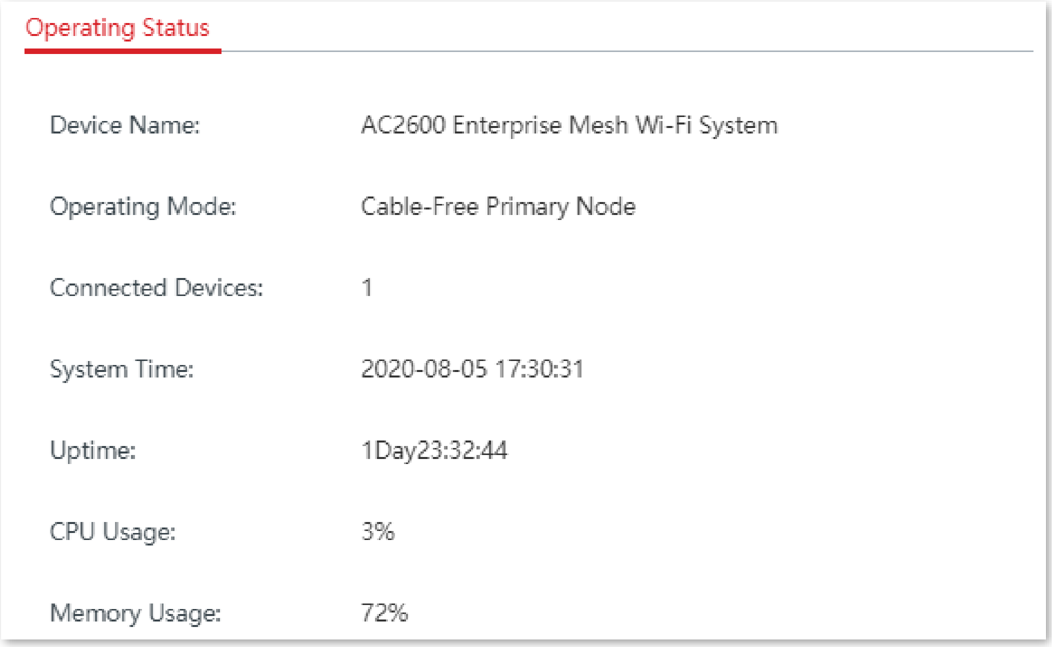
Firmware Version: V16.01.0.9(1207)

Parameter description

Parameter	Description
Location	It specifies the location information of the node, which helps you locate the node more easily while managing it. You can select a location description from the dropdown list or customize one as required.
LED	It specifies whether to turn on/off the LED indicators of the node. ●: It indicates that the LED indicators are on. You can check the operating status of the device based on the LED indicators. ○: It indicates that the LED indicators are off.
SN	It specifies the serial number of the node, which is used to add the node into a mesh network.

Parameter	Description
Firmware Version	It specifies the current version of the node.

Operating status



Device Name: AC2600 Enterprise Mesh Wi-Fi System

Operating Mode: Cable-Free Primary Node

Connected Devices: 1

System Time: 2020-08-05 17:30:31

Uptime: 1Day23:32:44

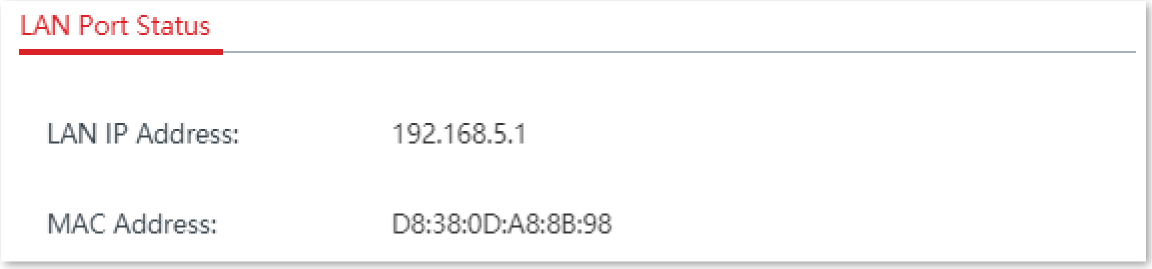
CPU Usage: 3%

Memory Usage: 72%

Parameter description

Parameter	Description
Device Name	It specifies the name of your node.
Operating Mode	It specifies the current working mode of the node. – Cable-Free Primary Node: The node serves as a primary node in the cable-free network, which is connected to wired network. It is the only exit to visit internet and realizes data transformation between Mesh networks and wired networks. – Cable-Free Secondary Node: The node serves as a secondary node in the cable-free network. It extends the coverage of the existing cable-free network through Mesh network.
Connected Devices	It specifies the number of devices connected to cable-free network currently.
System Time	It specifies the current system time of the node.
Uptime	It specifies the time that has elapsed since the node was started last time.
CPU Usage	It specifies the current CPU usage of the node.
Memory Usage	It specifies the current memory usage of the node.

LAN port status


LAN Port Status

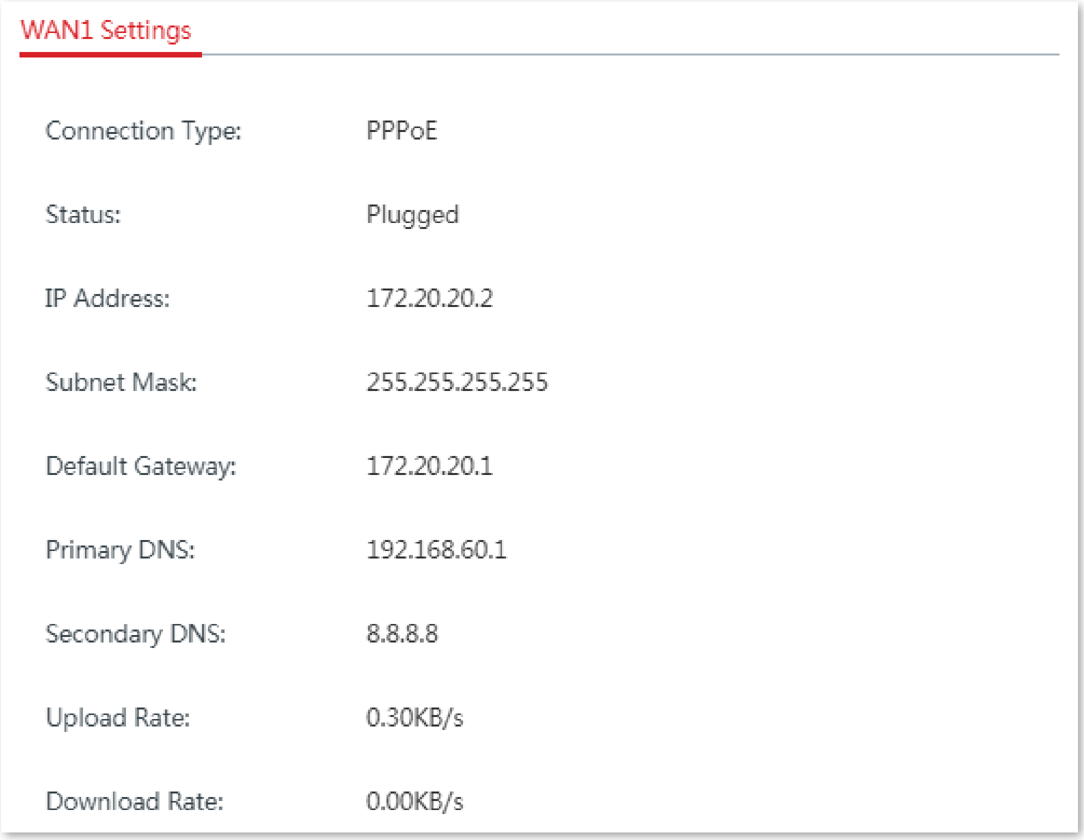
LAN IP Address: 192.168.5.1

MAC Address: D8:38:0D:A8:8B:98

Parameter description

Parameter	Description
LAN IP Address	It specifies the IP address of the LAN port of the node and also the management IP address of the node, which is 192.168.5.1 by default. LAN users can access this IP address to log into the management page of the node. The IP address of the secondary node is automatically obtained from the DHCP server of the primary node.
MAC Address	It specifies the physical address of the node's LAN port.

WAN settings


WAN1 Settings

Connection Type: PPPoE

Status: Plugged

IP Address: 172.20.20.2

Subnet Mask: 255.255.255.255

Default Gateway: 172.20.20.1

Primary DNS: 192.168.60.1

Secondary DNS: 8.8.8.8

Upload Rate: 0.30KB/s

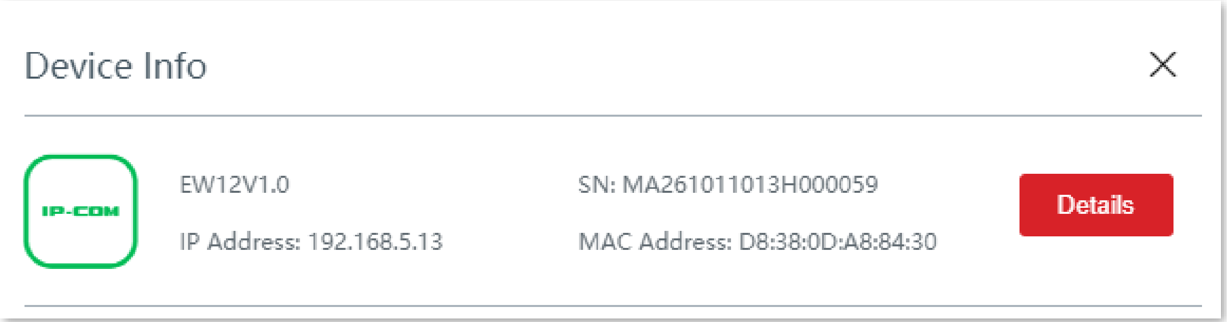
Download Rate: 0.00KB/s

Parameter description

Parameter	Description
Connection Type	It specifies the internet connection type of the node’s WAN port.
Status	It specifies whether or not the node’s WAN port is plugged. If **Unplugged** appears, please check its physical connection.
IP Address	It specifies the IP address of the node’s WAN port.
Subnet Mask	It specifies the subnet mask of the node’s WAN port.
Default Gateway	It specifies the gateway IP address of the node’s WAN port.
Primary DNS	It specifies the primary/secondary DNS server address of the node’s WAN port.
Secondary DNS	
Upload/Download Rate	It specifies the real-time upload and download rate of the node’s WAN port.

Check the information of the cable-free secondary nodes

Click the next to the in the **System Status** page, you can check the device information of the cable-free secondary node.



Device Info

EW12V1.0

IP Address: 192.168.5.13

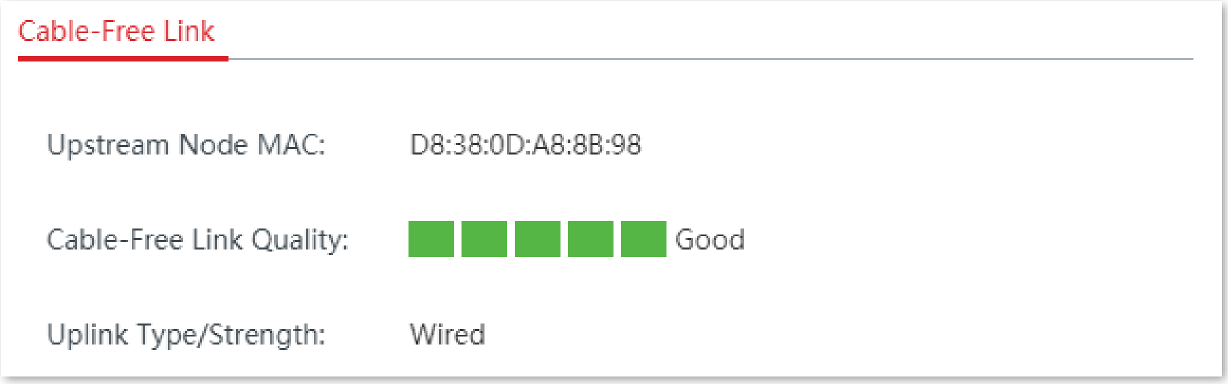
SN: MA261011013H000059

MAC Address: D8:38:0D:A8:84:30

For more information, please click the Details page after the corresponding node.

Here, you can check or set the Device info of the node, check the Operating status, LAN port status, Cable-free link information, restart or delete the node.

Cable-free link



Cable-Free Link

Upstream Node MAC: D8:38:0D:A8:8B:98

Cable-Free Link Quality: 🟩🟩🟩🟩🟩 Good

Uplink Type/Strength: Wired

Parameter description

Parameter	Description
Upstream Node MAC	It specifies the physical address of the interface used to form the Mesh link by the Mesh AD hoc network link superior node.
Cable-Free Link Quality	It specifies the connection quality of cable-free links.
Uplink Type/Strength	It specifies the networking mode between this node and the upstream node/the signal strength of the upstream node received by this node.

Reboot the node

Click Reboot and the node will be rebooted immediately.

Delete the node

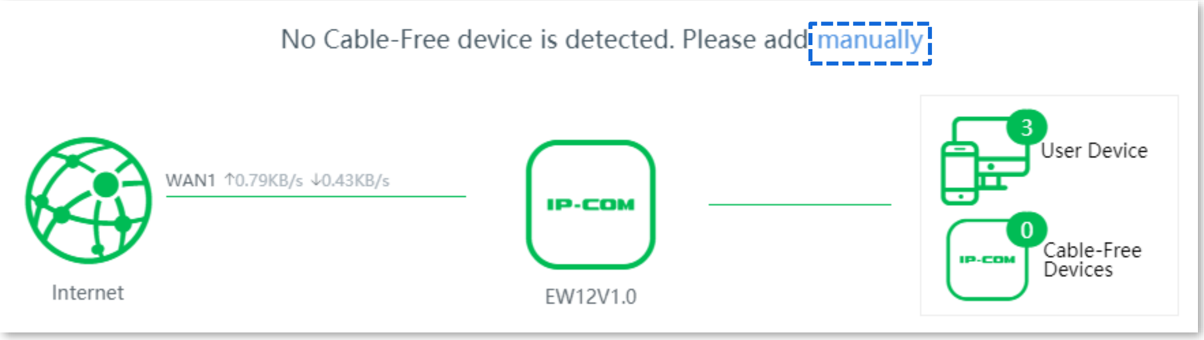
Click Delete and the node will be removed from the cable-free network. Nodes which are removed from cable-free networks, the configuration is reset to the factory state.

3.2.2 Add secondary nodes

Generally, this device can detect secondary node devices in factory settings automatically. If your secondary node device cannot be detected, you can also log in to the web UI of this device to add secondary node devices manually.

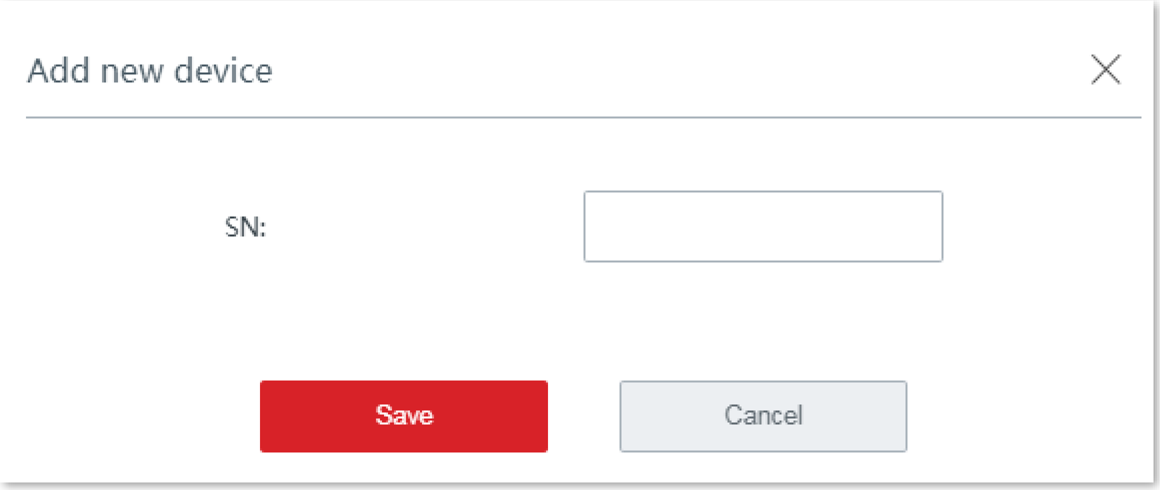
Configuration procedure

1. Click **System Status** to enter the page.
2. Click manually.


No Cable-Free device is detected. Please add manually

3. Enter the SN (on the bottom label) of the Mesh device to be added.

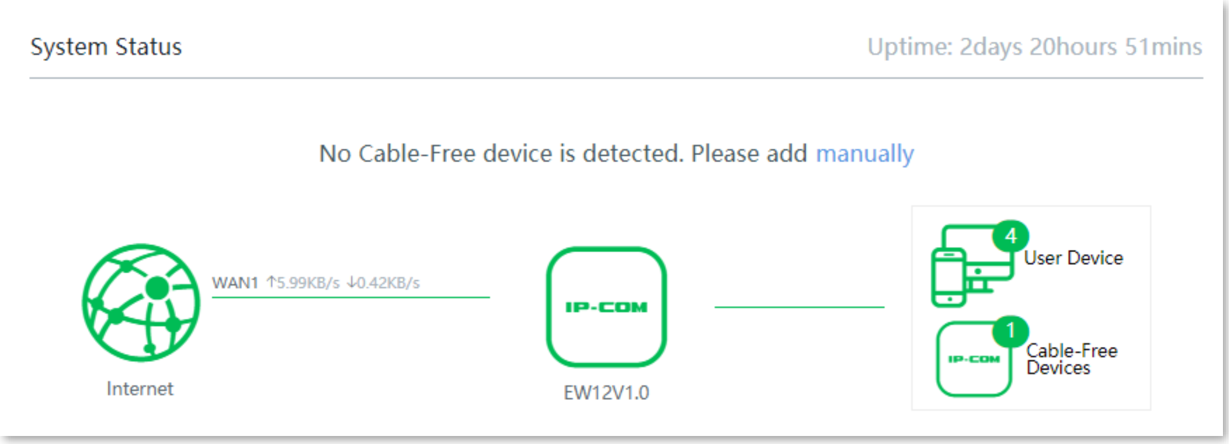
4. Click **Save**.


Add new device

SN:

----End

Wait until it is saved. The new-added Mesh device appears in the map, and you can click its icon to configure it.


System Status

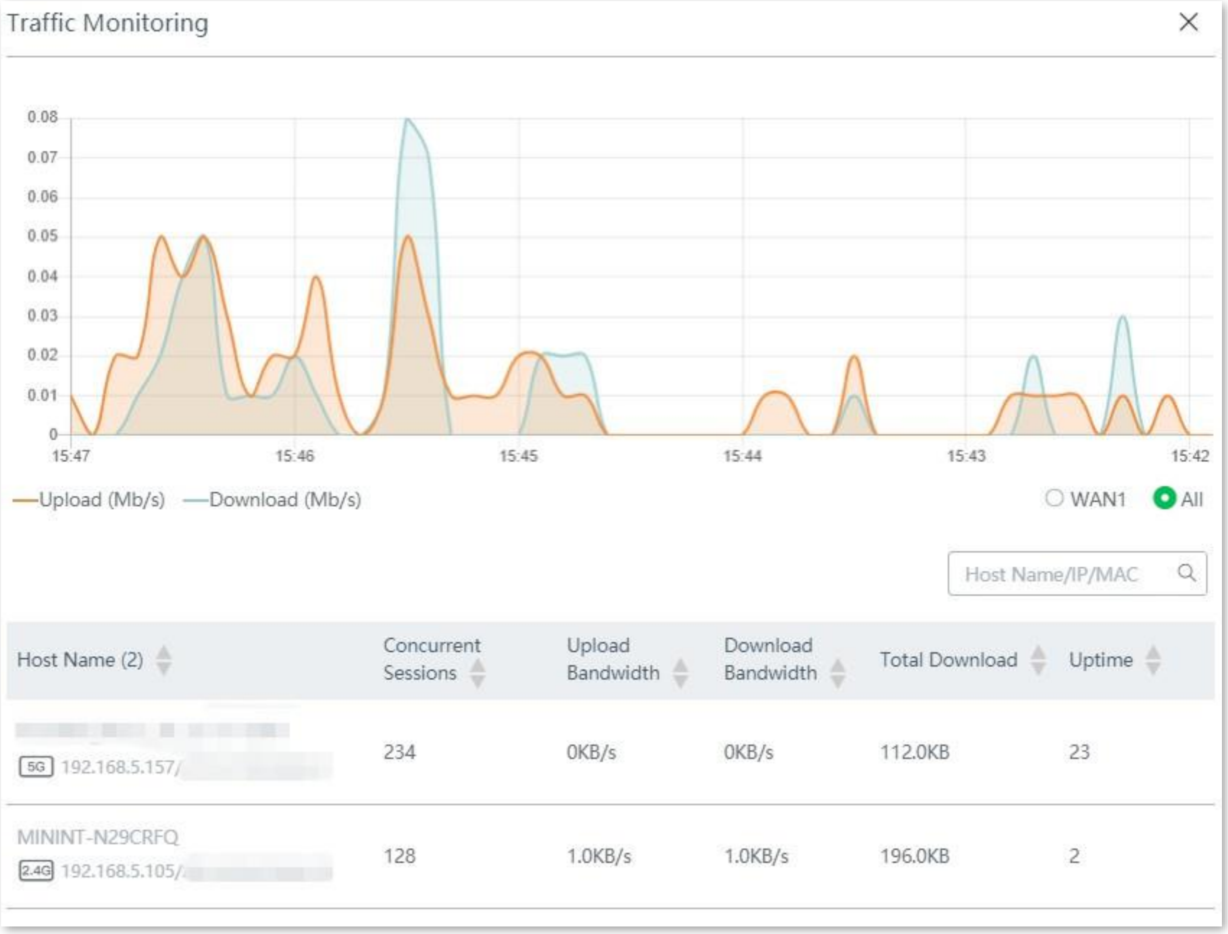
Uptime: 2days 20hours 51mins

No Cable-Free device is detected. Please add manually

3.2.3 Monitor traffic

You can view the real-time upload and download bandwidth of the WAN port, and check the basic information of a client, such as upload/download bandwidth, uptime and so on.

Click **System Status** to enter the page, and click More Statistics.



Host Name (2)	Concurrent Sessions	Upload Bandwidth	Download Bandwidth	Total Download	Uptime
[redacted] 5G 192.168.5.157/[redacted]	234	0KB/s	0KB/s	112.0KB	23
MININT-N29CRFQ 2.4G 192.168.5.105/[redacted]	128	1.0KB/s	1.0KB/s	196.0KB	2

Parameter description

Parameter	Description
Host Name	It displays the name, IP address, and MAC address of clients connected to the device. Tip For host name-based rules, such as adding authentication-free host using host name, you need to use the host name here. □ : The client connects to the device in a wired manner. 2.4G : The client connects to the 2.4 GHz WiFi network of the device. 5G : The client connects to the 5 GHz WiFi network of the device.
Concurrent Sessions	It specifies concurrent sessions established of the corresponding client.
Upload Bandwidth	It displays the current upload/download bandwidth of each client. You can

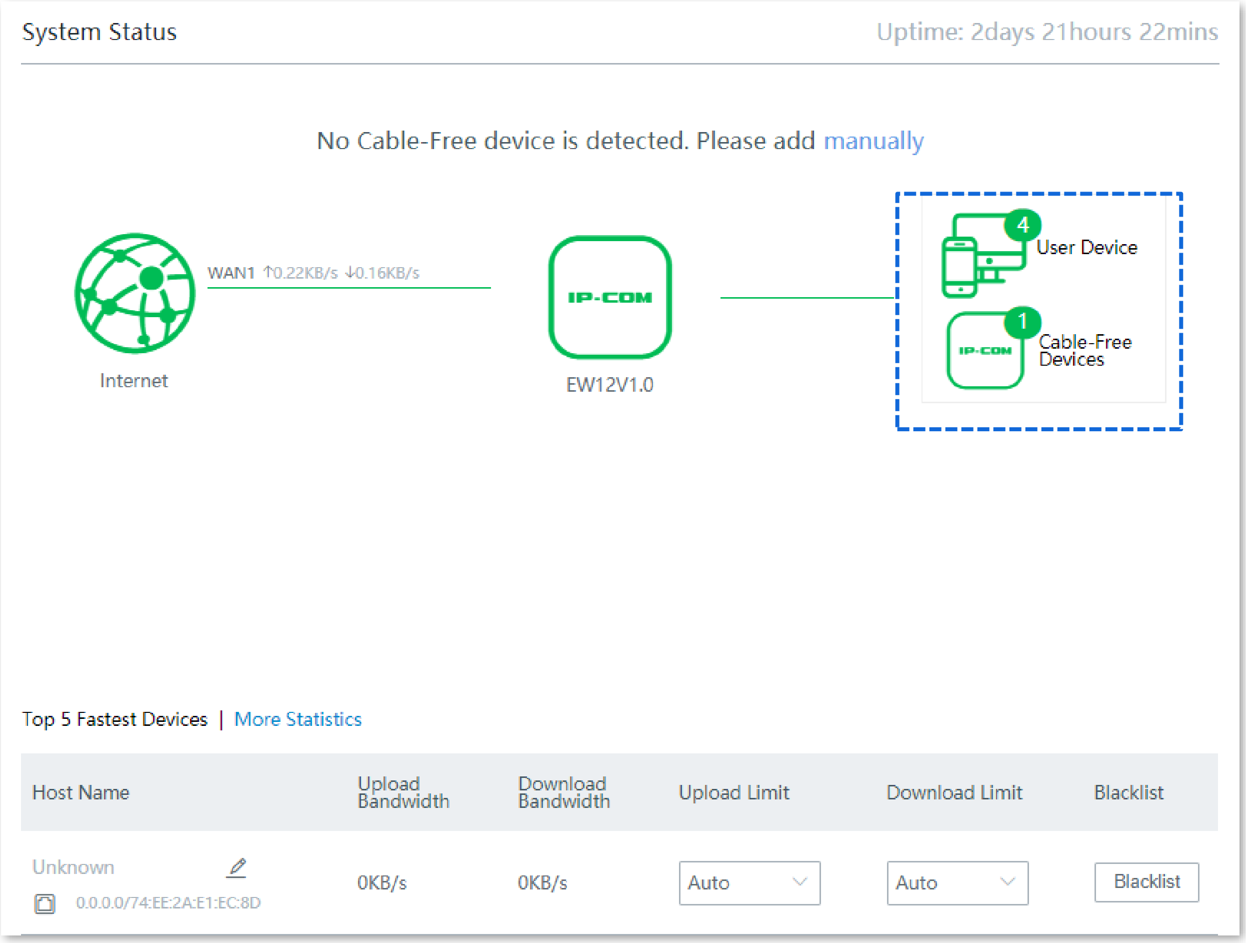
Parameter	Description
Download Bandwidth	control their maximum upload/download bandwidth manually, refer to Manage online devices.
Total Download	It specifies the total download traffic utilized by each client.
Uptime	It specifies the connection time of each client.

3.2.4 Manage online devices

You can edit the name of connected clients, control the upload and/or download bandwidth separately or in batch, and block a device from accessing your network.

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

The **System Status** page directly presents the top 5 clients with the highest speed. Click the **Connected Devices** icon to manage all connected clients.



System Status

Uptime: 2days 21hours 22mins

No Cable-Free device is detected. Please add manually

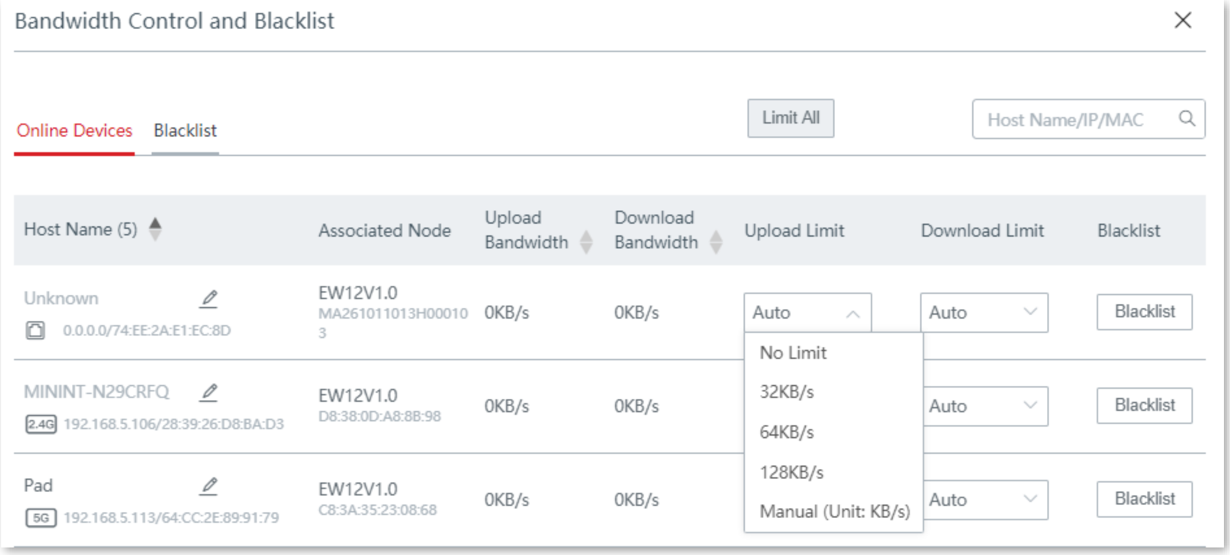
Top 5 Fastest Devices | More Statistics

Host Name	Upload Bandwidth	Download Bandwidth	Upload Limit	Download Limit	Blacklist
Unknown 0.0.0.0/74:EE:2A:E1:EC:8D	0KB/s	0KB/s	Auto	Auto	Blacklist

Control bandwidth of the connected clients

Control bandwidth of online devices

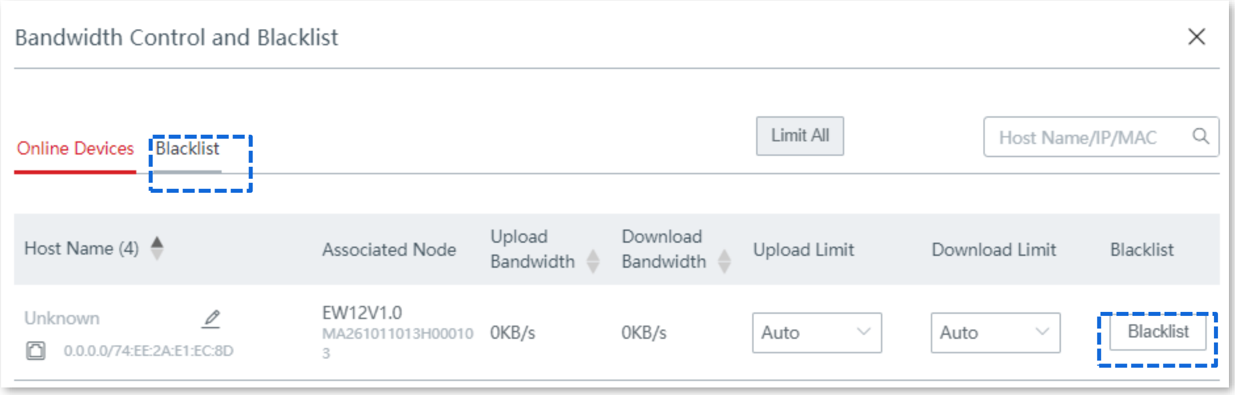
To limit the upload and/or download bandwidth of one or several devices, select a pre-defined value from the drop-down list menu of **Upload Limit** and/or **Download Limit**, or select **Manual** to specify a value manually.



Host Name (5)	Associated Node	Upload Bandwidth	Download Bandwidth	Upload Limit	Download Limit	Blacklist
Unknown 0.0.0.0/74:EE:2A:E1:EC:8D	EW12V1.0 MA261011013H000103	0KB/s	0KB/s	Auto	Auto	Blacklist
MININT-N29CRFQ 2.4G 192.168.5.106/28:39:26:D8:BA:D3	EW12V1.0 D8:38:0D:A8:8B:98	0KB/s	0KB/s		Auto	Blacklist
Pad 5G 192.168.5.113/64:CC:2E:89:91:79	EW12V1.0 C8:3A:35:23:08:68	0KB/s	0KB/s		Auto	Blacklist

Add devices into blacklist

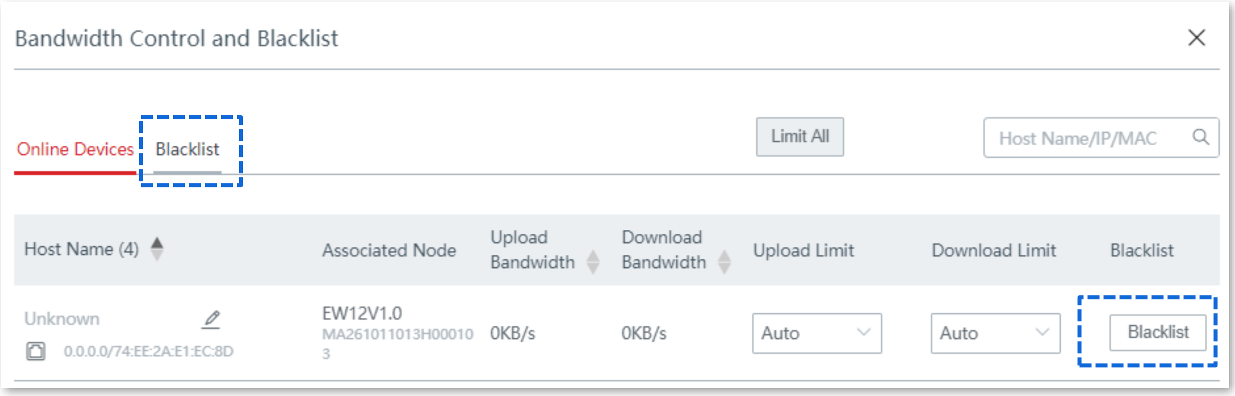
To protect your network from being accessed by unknown devices, click the **Blacklist** button to block them. The blocked devices will be moved to the **Blacklist** section, and cannot access the internet through the device.



Host Name (4)	Associated Node	Upload Bandwidth	Download Bandwidth	Upload Limit	Download Limit	Blacklist
Unknown 0.0.0.0/74:EE:2A:E1:EC:8D	EW12V1.0 MA261011013H000103	0KB/s	0KB/s	Auto	Auto	Blacklist

Remove devices from blacklist

To unblock devices from the blacklist, click the **Connected Devices** icon on the **System Status** page, click **Blacklist**, then click **Remove** corresponded to the device you want to unblock.



Bandwidth Control and Blacklist

Online Devices | Blacklist

Limit All

Host Name/IP/MAC

Host Name (4)	Associated Node	Upload Bandwidth	Download Bandwidth	Upload Limit	Download Limit	Blacklist
Unknown 0.0.0.0/74:EE:2A:E1:EC:8D	EW12V1.0 MA261011013H000103	0KB/s	0KB/s	Auto	Auto	Blacklist

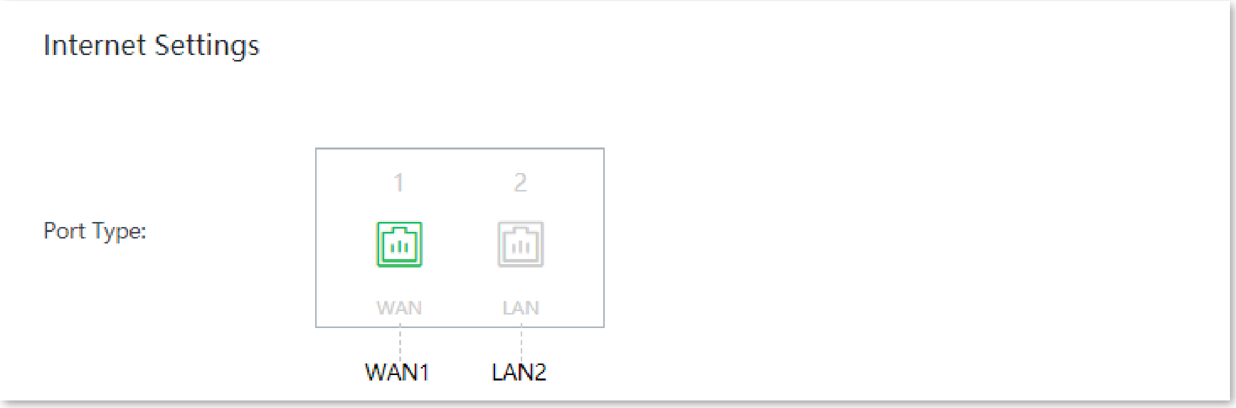
3.3 Internet settings

3.3.1 Overview

In this section, you can configure or change the internet settings to enable the device to access the internet.

For the initial use of the device, or after resetting the device to factory settings, you can follow the quick setup wizard to complete the internet settings. After that, you can change internet settings or set up more parameters here.

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

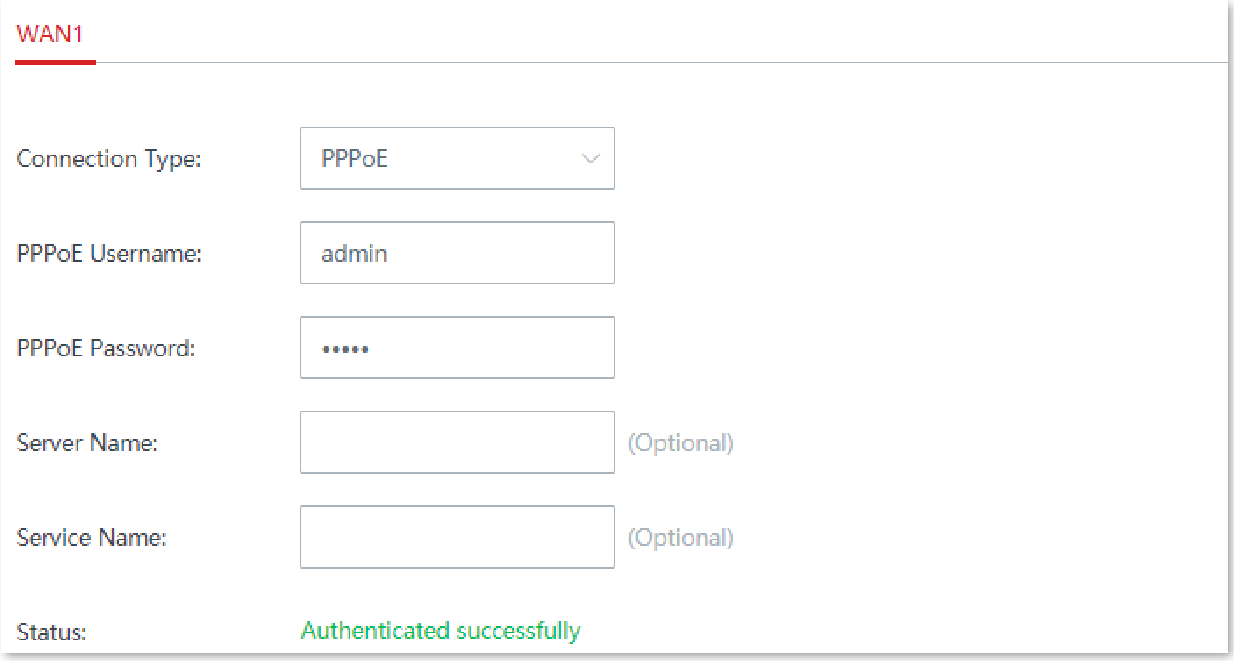


Internet Settings

Port Type:

Parameter description

Parameter	Description
Port Type	It specifies whether or not a port is connected. 🟩: The port is connected properly. □: The port is disconnected or improperly connected.



Connection Type: PPPoE

PPPoE Username: admin

PPPoE Password: •••••

Server Name: (Optional)

Service Name: (Optional)

Status: Authenticated successfully

Parameter description

Parameter	Description
Connection Type	It specifies the way in which the device is connected to the internet. The device supports **PPPoE**, **Static IP**, **Dynamic IP**, **PPPoE Russia**, **PPTP/PPTP Russia**, and **L2TP/L2TP Russia**. Refer to the table Choose your connection type for details.
PPPoE Username	These two parameters are required only when your internet connection type is PPPoE or PPPoE Russia. They are provided by your ISP.
PPPoE Password	
Server Name	These two parameters are required only when your internet connection type is PPPoE or PPPoE Russia. They are provided by your ISP. (Optional)
Service Name	
PPTP Server Address	This parameter is required only when your internet connection type is PPTP/PPTP Russia. It is provided by ISP.
L2TP Server Address	This parameter is required only when your internet connection type is L2TP/L2TP Russia. It is provided by ISP.
User name	These two parameters are required only when your internet connection type is PPTP/PPTP Russia or L2TP/L2TP Russia. They are provided by your ISP.
Password	
Obtain an IP address	This parameter appears when the connection type is set to PPPoE Russia, PPTP/PPTP Russia, and L2TP/L2TP. If there is no DHCP server is enabled in the network, select **Manual** and enter the IP address and related parameters manually. Otherwise, select **Auto**, the device obtains these parameters from the DHCP server in the network.

Parameter	**Description**
IP Address	These parameters are required only when your internet connection type is **Static IP** or when you set **Obtain an IP address** to **Manual** after the connection type is set to PPPoE Russia, PPTP/PPTP Russia, or L2TP/L2TP Russia. The **Secondary DNS** parameter is optional. These parameters are provided by your ISP.
Subnet Mask	
Default Gateway	
Primary DNS	
Secondary DNS	
Status	It indicates the internet connection status of the WAN port. – **Authenticated Successfully/Connected**: The WAN port is connected to the internet or server. – **Connecting…**: The WAN port of the device is connecting to the internet or server. – **Disconnected**: The port is physically disconnected, or fails to connect to the internet or server. Please check if the physical connections are proper, or the parameters you entered are correct.

3.3.2 Set up internet connection

Tip

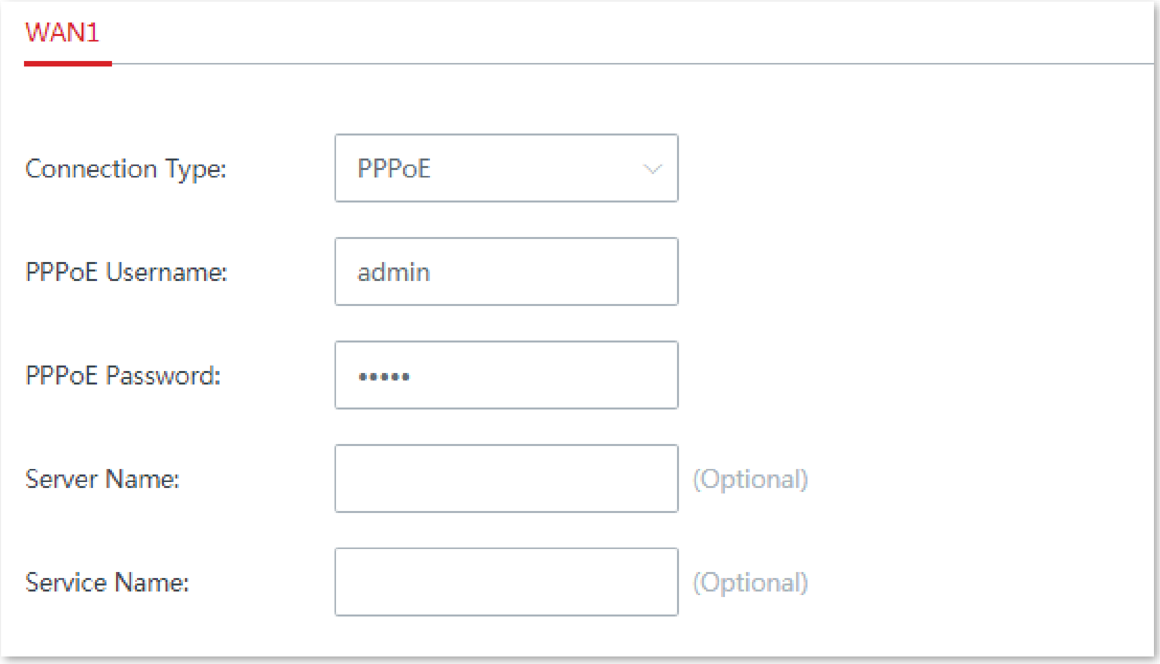
The parameters for accessing the internet are all provided by your ISP.

Choose your connection type according to the table below:

Available parameters	Connection type
PPPoE user name, PPPoE password, service name, and server name.	PPPoE
IP address, subnet mask, default gateway, primary DNS, and secondary DNS (optional)	Static IP
None or the device is connected to an upstream device which can access the internet and enables its DHCP server.	Dynamic IP
PPPoE user name, PPPoE password, service name, and server name. If IP address and related parameters. If the DHCP server of the upstream device is disabled, the IP address, subnet mask, default gateway, and primary DNS are required.	PPPoE Russia
PPTP server address, user name, and password. If the DHCP server of the upstream device is disabled, the IP address, subnet mask, default gateway, and primary DNS are required.	PPTP/PPTP Russia
L2TP server address, user name, and password. If the DHCP server of the upstream device is disabled, the IP address, subnet mask, default gateway, and primary DNS are required.	L2TP/L2TP Russia

PPPoE

1. Click **Internet Settings** to enter the page.
2. Select **Connection Type** to **PPPoE**.
3. Enter the **PPPoE Username** and **PPPoE Password** provided by your ISP. If the **Server Name** or **Service Name** is also provided, enter them in the corresponding input box as well.
4. Click **Save** at the bottom of the page.



WAN1

Connection Type: PPPoE

PPPoE Username: admin

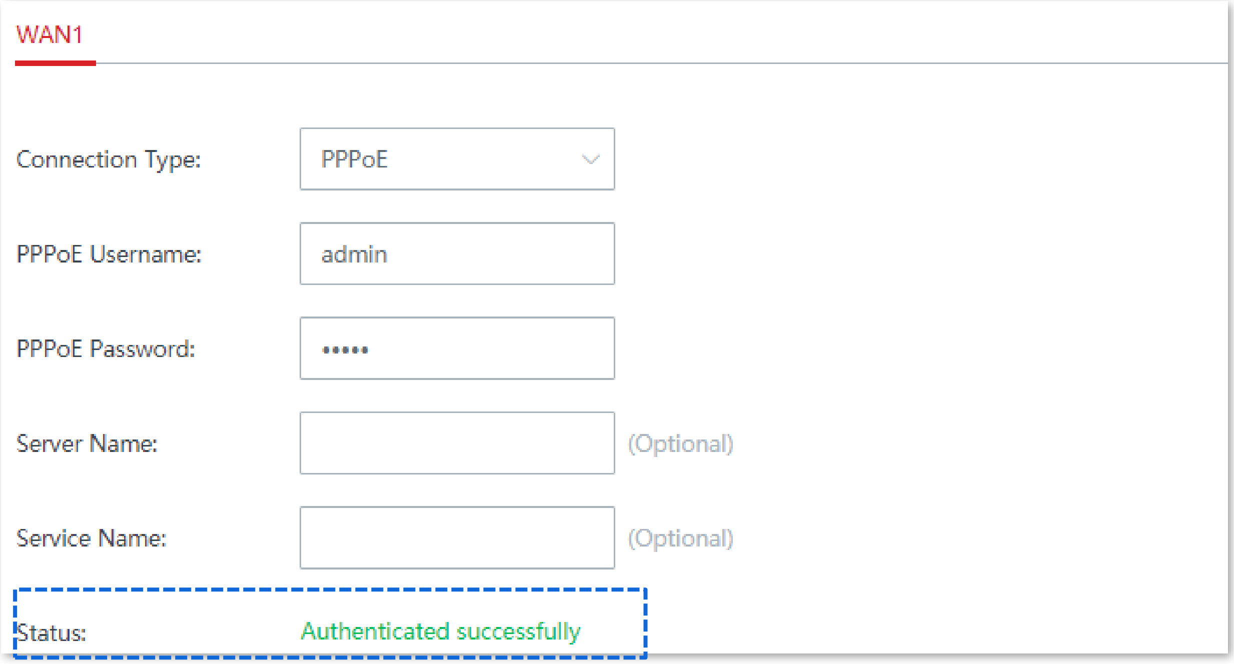
PPPoE Password: •••••

Server Name: (Optional)

Service Name: (Optional)

----End

The device connects to the internet successfully when the **Status** shows Authenticated successfully.



WAN1

Connection Type: PPPoE

PPPoE Username: admin

PPPoE Password: •••••

Server Name: (Optional)

Service Name: (Optional)

Status: Authenticated successfully

Tip

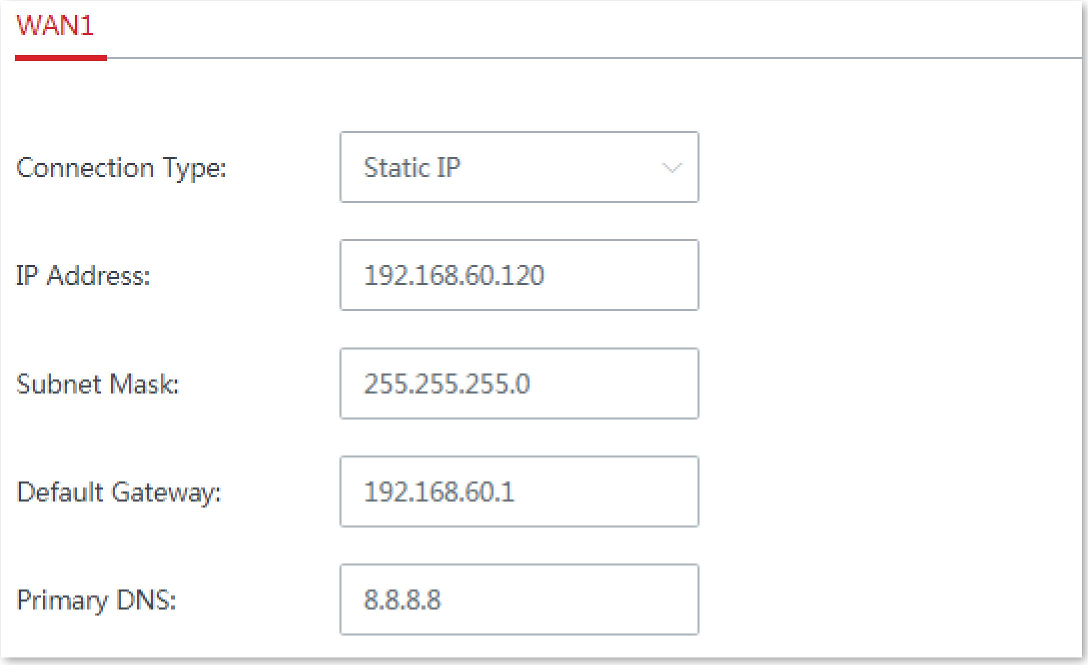
If you fail to access the internet:

– Check whether the parameters you entered are correct.

– Try changing the WAN parameters.

Static IP

1. Click **Internet Settings** to enter the page.
2. Select **Connection Type** to **Static IP**.
3. Enter the **IP Address**, **Subnet Mask**, **Default Gateway**, **Primary DNS**, and **Secondary DNS** (optional) provided by your ISP.
4. Click **Save** at the bottom of the page.



Connection Type: Static IP

IP Address: 192.168.60.120

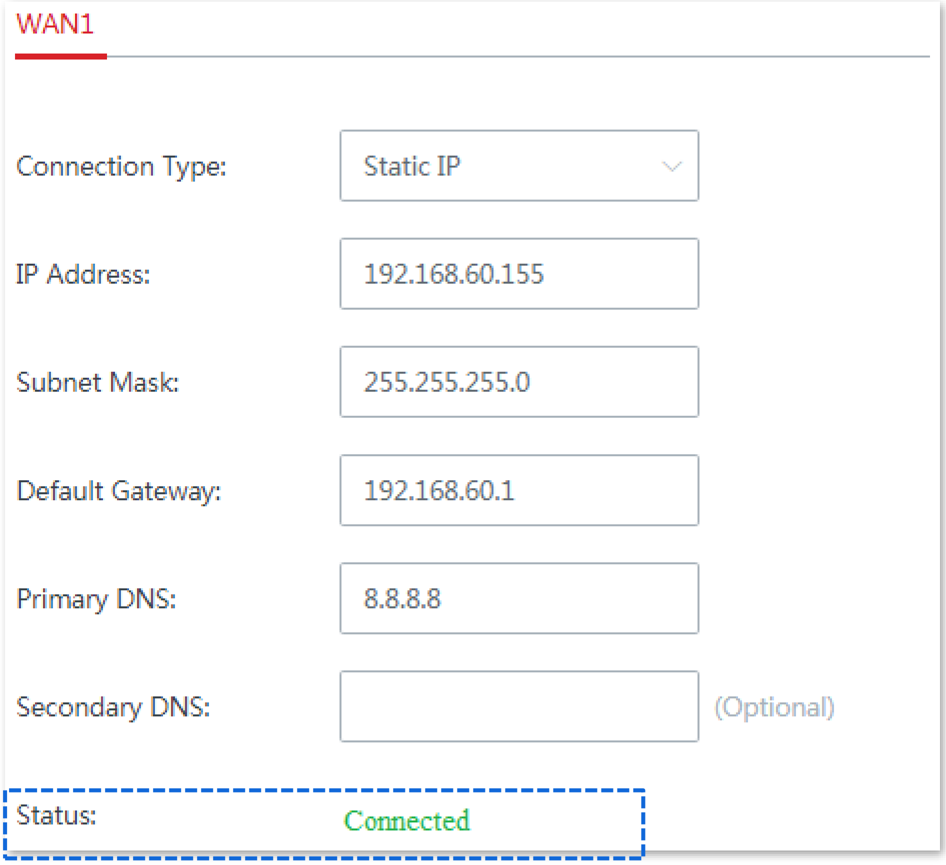
Subnet Mask: 255.255.255.0

Default Gateway: 192.168.60.1

Primary DNS: 8.8.8.8

----End

The device connects to the internet successfully when the **Status** shows Connected.



WAN1

Connection Type: Static IP

IP Address: 192.168.60.155

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.60.1

Primary DNS: 8.8.8.8

Secondary DNS: (Optional)

Status: Connected

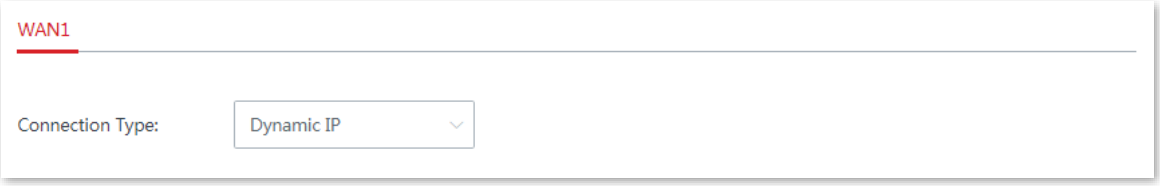
Tip

If you fail to access the internet:

– Check whether the parameters you entered are correct.
– Try changing WAN parameters.

Dynamic IP

1. Click **Internet Settings** to enter the page.
2. Select **Connection Type** to **Dynamic IP**.
3. Click **Save** at the bottom of the page.

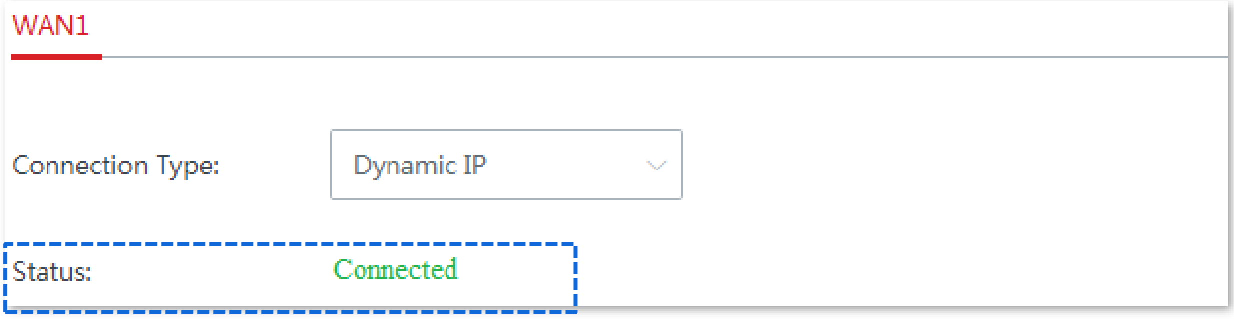


WAN1

Connection Type: Dynamic IP

----End

The device connects to the internet successfully when the **Status** shows Connected.



WAN1

Connection Type: Dynamic IP

Status: Connected

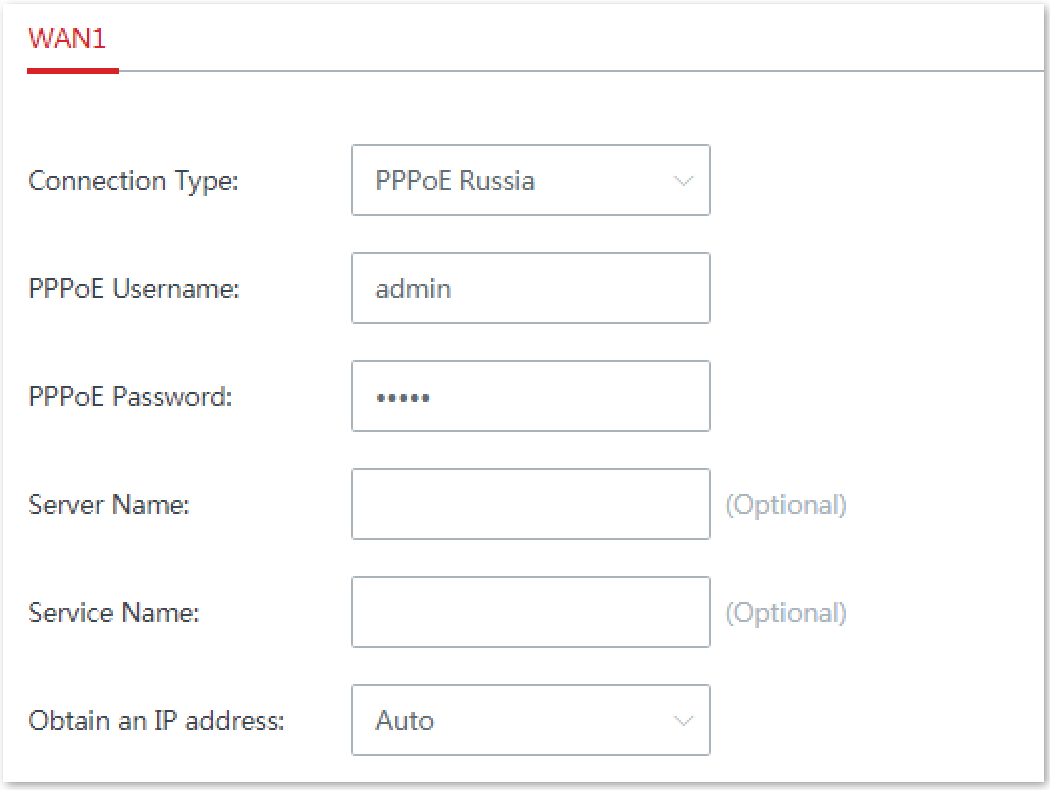
Tip

If you fail to access the internet:

- Check whether the connection type you selected is correct.
- Try changing WAN parameters.

PPPoE Russia

1. Click **Internet Settings** to enter the page.
2. Select **Connection Type** to **PPPoE Russia**.
3. Enter the **PPPoE Username**, **PPPoE Password** provided by your ISP. If the **Server Name**, **Service Name**, **IP address** and related parameters are also provided, enter them in the corresponding input box as well.
4. Click **Save** at the bottom of the page.



WAN1

Connection Type: PPPoE Russia

PPPoE Username: admin

PPPoE Password: •••••

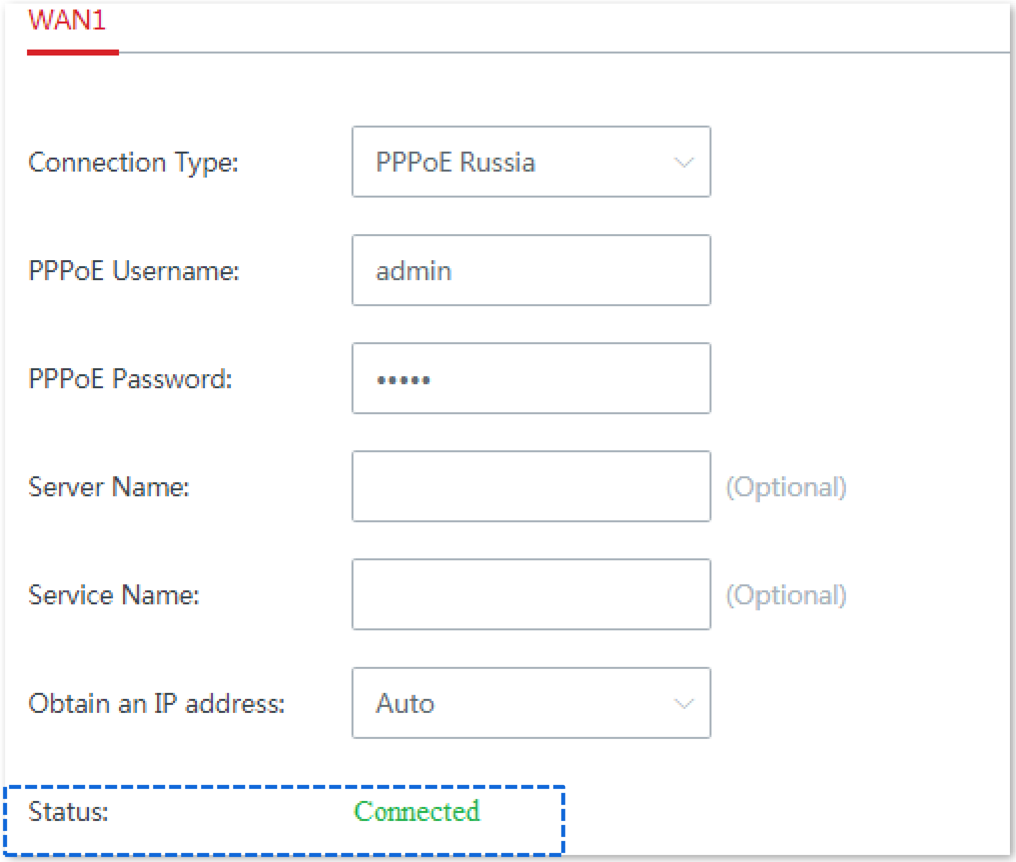
Server Name: (Optional)

Service Name: (Optional)

Obtain an IP address: Auto

----End

The device connects to the internet successfully when the **Status** shows Connected.



WAN1

Connection Type: PPPoE Russia

PPPoE Username: admin

PPPoE Password: •••••

Server Name: (Optional)

Service Name: (Optional)

Obtain an IP address: Auto

Status: Connected

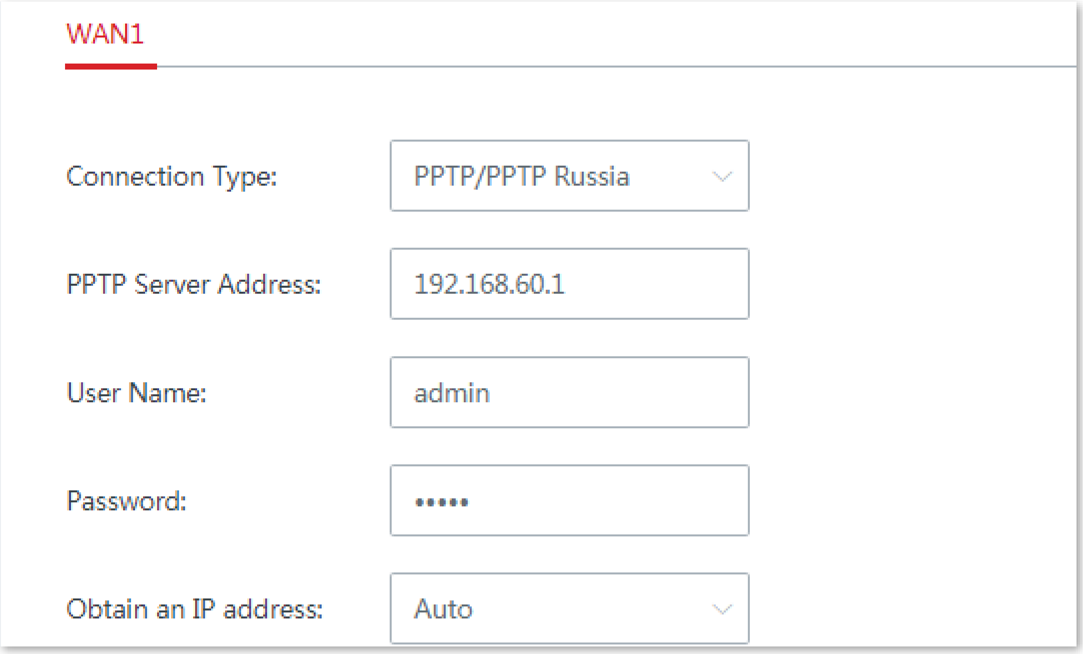
Tip

If you fail to access the internet:

- Check whether the parameters you entered are correct.
- Try changing the WAN parameters.

PPTP/PPTP Russia

1. Click **Internet Settings** to enter the page.
2. Select **Connection Type** to **PPTP/PPTP Russia**.
3. Enter the **PPTP Server Address**, **User Name,** and **Password** provided by your ISP. If the **IP address** and related parameters are also provided, enter them in the corresponding input box as well.
4. Click **Save** at the bottom of the page.



Connection Type: PPTP/PPTP Russia

PPTP Server Address: 192.168.60.1

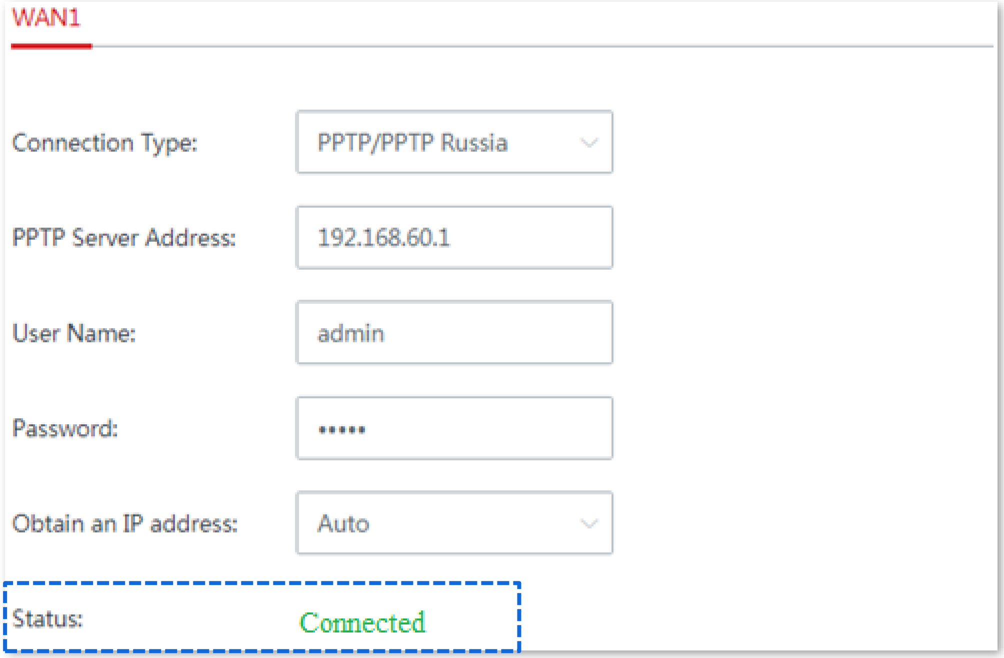
User Name: admin

Password: •••••

Obtain an IP address: Auto

----End

The device connects to the internet successfully when the **Status** shows Connected.



WAN1

Connection Type: PPTP/PPTP Russia

PPTP Server Address: 192.168.60.1

User Name: admin

Password: •••••

Obtain an IP address: Auto

Status: Connected

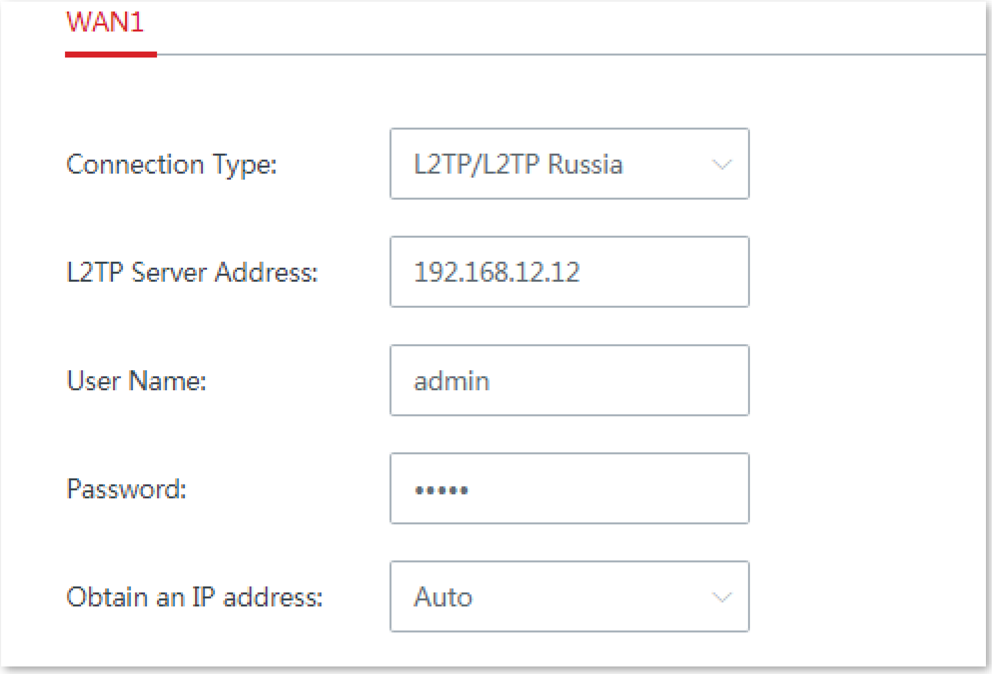
Tip

If you fail to access the internet:

- Check whether the parameters you entered are correct.
- Try changing the WAN parameters.

L2TP/L2TP Russia

1. Click **Internet Settings** to enter the page.
2. Select **Connection Type** to **L2TP/L2TP Russia**.
3. Enter the **L2TP Server Address**, **User Name,** and **Password** provided by your ISP. If the **IP address** and related parameters are also provided, enter them in the corresponding input box as well.
4. Click **Save** at the bottom of the page.



WAN1

Connection Type: L2TP/L2TP Russia

L2TP Server Address: 192.168.12.12

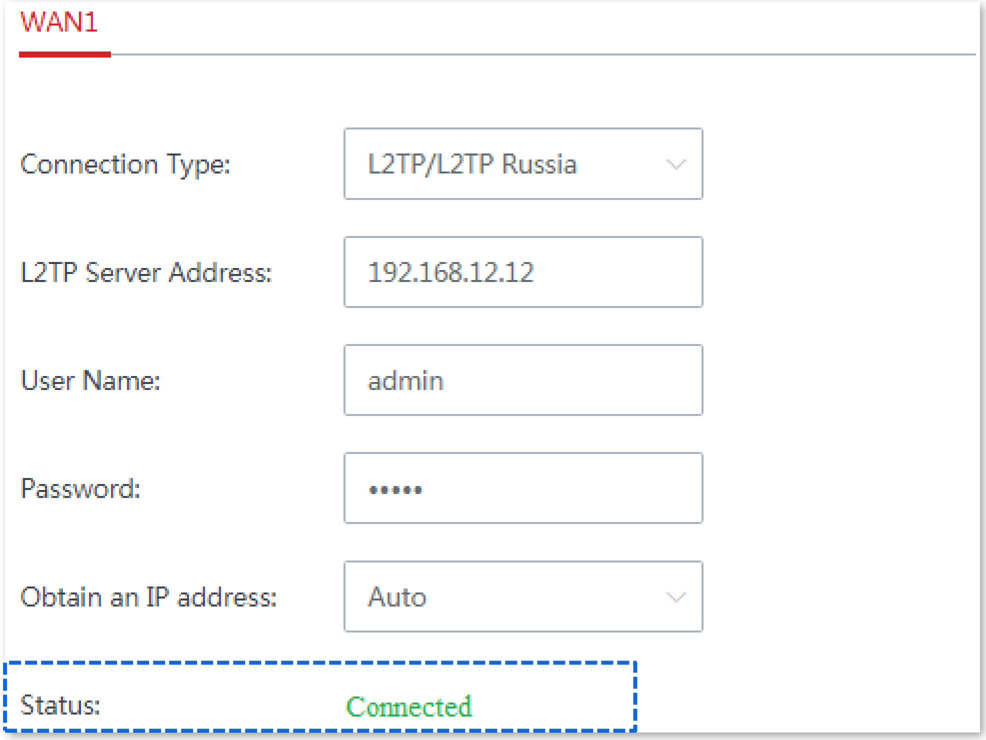
User Name: admin

Password: •••••

Obtain an IP address: Auto

----End

Wait for the device to complete rebooting. The device connects to the internet successfully when the **Status** shows Connected.



WAN1

Connection Type: L2TP/L2TP Russia

L2TP Server Address: 192.168.12.12

User Name: admin

Password: •••••

Obtain an IP address: Auto

Status: Connected

Tip

If you fail to access the internet:

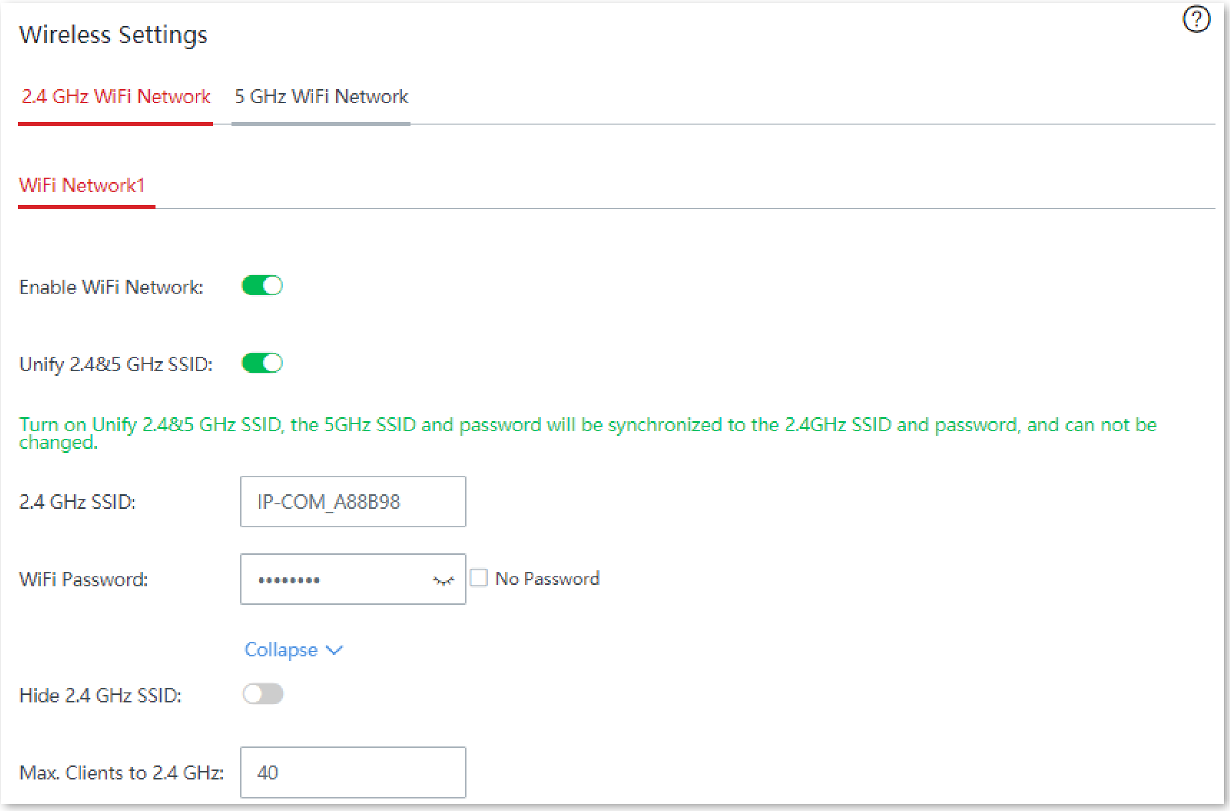
- Check whether the parameters you entered are correct.
- Try changing the WAN parameters.

3.4 Wireless

3.4.1 Wireless settings

The device supports WiFi networks of three bands at most. By default, the device wirelessly establishes a cable-free network. One 5 GHz wireless band is dedicated to establishing a cable-free link. The 2.4 GHz wireless band and another 5 GHz wireless band are used for terminal device access. When the cable-free network is set up by wired mode, the three wireless bands of the equipment are used for terminal equipment access.

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



Wireless Settings

Enable WiFi Network: ●

Unify 2.4&5 GHz SSID: ●

Turn on Unify 2.4&5 GHz SSID, the 5GHz SSID and password will be synchronized to the 2.4GHz SSID and password, and can not be changed.

2.4 GHz SSID: IP-COM_A88B98

WiFi Password: •••••••• □ No Password

Hide 2.4 GHz SSID: ○

Max. Clients to 2.4 GHz: 40

Parameter description

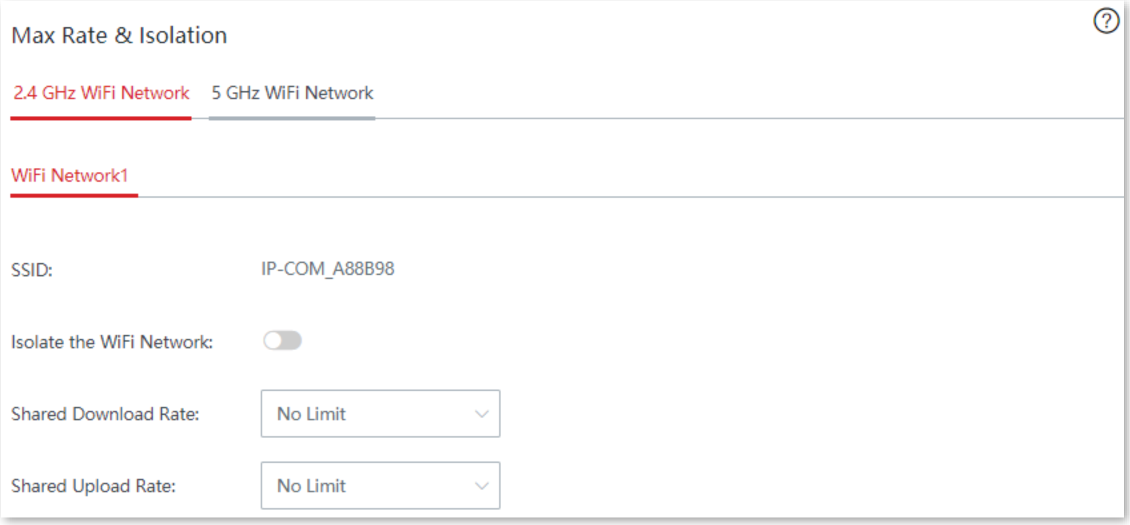
Parameter	Description
Enable WiFi Network1/2/3	It is used to enable/disable the corresponding WiFi network of the device.

Parameter	Description
Unify 2.4&5 GHz SSID	It is used to unify SSIDs for 2.4 GHz and 5 GHz WiFi networks. When this function is enabled, the 5 GHz SSID and password will be synchronized with the 2.4 GHz SSID and password, and cannot be changed. When users' devices connect to the WiFi network, they will automatically connect to the WiFi with the best network quality. Tip If there are wireless devices in your network that only support the 2.4 GHz network, it is recommended not to enable this function to prevent these devices from failing to connect to the WiFi network.
SSID	It specifies the WiFi name of the corresponding WiFi network.
WiFi Password	It specifies the password used for WiFi network. You are recommended to use the combination of digits, letters and special characters for higher security. Selecting **No Password** indicates that wireless clients can connect to the WiFi network without a password. Select this option only when necessary since it leads to weak network security.
Hide SSID	With this function enabled, wireless clients cannot detect the SSID and users need to manually enter the SSID on the wireless client to access the WiFi network. Disabling it indicates that wireless clients can detect the SSID. By default, this function is disabled.
Max. Clients	It specifies the maximum number of wireless clients that can be connected to the WiFi network at each frequency band. After the value is reached, this WiFi network denies new connection requests.

3.4.2 Max rate & isolation

Network isolation makes clients connected to different networks of the device cannot communicate with each other.

Navigate to **Wireless** > **Max Rate & Isolation** to enter this page.


Max Rate & Isolation

SSID: IP-COM_A88B98

Isolate the WiFi Network:

Shared Download Rate: No Limit

Shared Upload Rate: No Limit

Parameter description

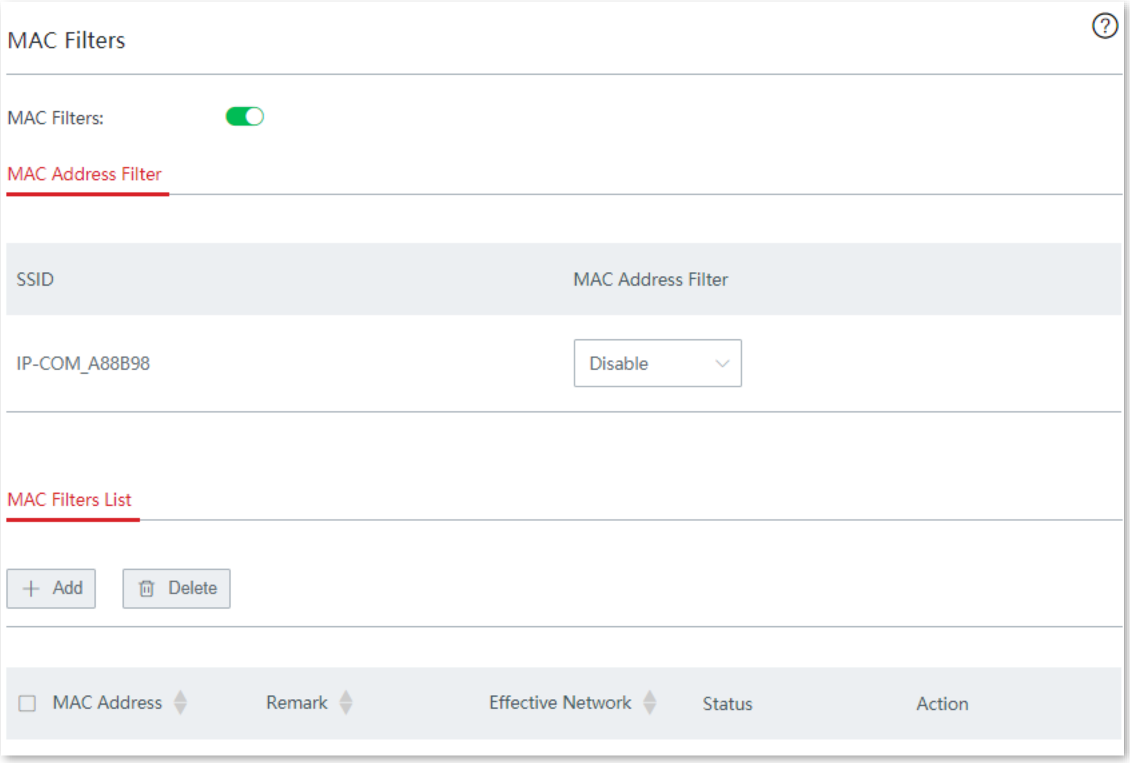
Parameter	Description
SSID	WiFi name of the corresponding WiFi network.
Isolate this network	With this function enabled, clients connected to the corresponding WiFi network cannot communicate with clients connected to other networks of this device, leading to higher WiFi network security. By default, this function is disabled.
No access to LAN	This function is only applicable to **WiFi Network2/3/4**. With this function enabled, clients connected to this WiFi network cannot access the Web UI and private network (LAN) of this device, protecting your LAN network.
Shared Upload/Download Rate	Clients connected to this WiFi network share the upload/download rate you set here. Upload and download rate allocated to individual client may vary.

3.4.3 MAC filters

Overview

In this section, you can allow or forbid devices with special MAC address to connect the WiFi network. By default, this function is disabled.

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



MAC Filters: ●

SSID	MAC Address Filter
IP-COM_A88B98	Disable

□ MAC Address	Remark	Effective Network	Status	Action

Parameter description

Parameter		Description
MAC Address Filter	SSID	It specifies all WiFi networks already enabled by the node. Tip If you unify the SSIDs of 2.4 GHz and 5 GHz bands, the corresponding WiFi networks only display one SSID here.
	MAC Address Filter	It specifies the WiFi network's MAC filter modes. There are three modes for selection: – **Disable**: This function is disabled, and all wireless clients can connect to this WiFi network. – **Only Allow**: Only wireless clients with the specified MAC address can connect to this WiFi network. – **Only Forbid**: Only wireless clients with the specified MAC address cannot connect to this WiFi network.

Parameter	Description	Parameter
MAC Filters List	MAC Filters List	It specifies the wireless filtering rules you configured.
	MAC Address	It specifies the MAC address of the client to which the rule applies.
	Remark	It specifies the brief description you set for the corresponding MAC address.
	Effective Network	It specifies the WiFi network(s) to which the rule applies.
	Status	It specifies whether the rule is enabled or not. ○: This rule is disabled. ●: This rule is enabled.
	Action	It specifies the operations you can perform to the rule. ✎: Click it to edit the rule. 🗑 : Click it to delete the rule.

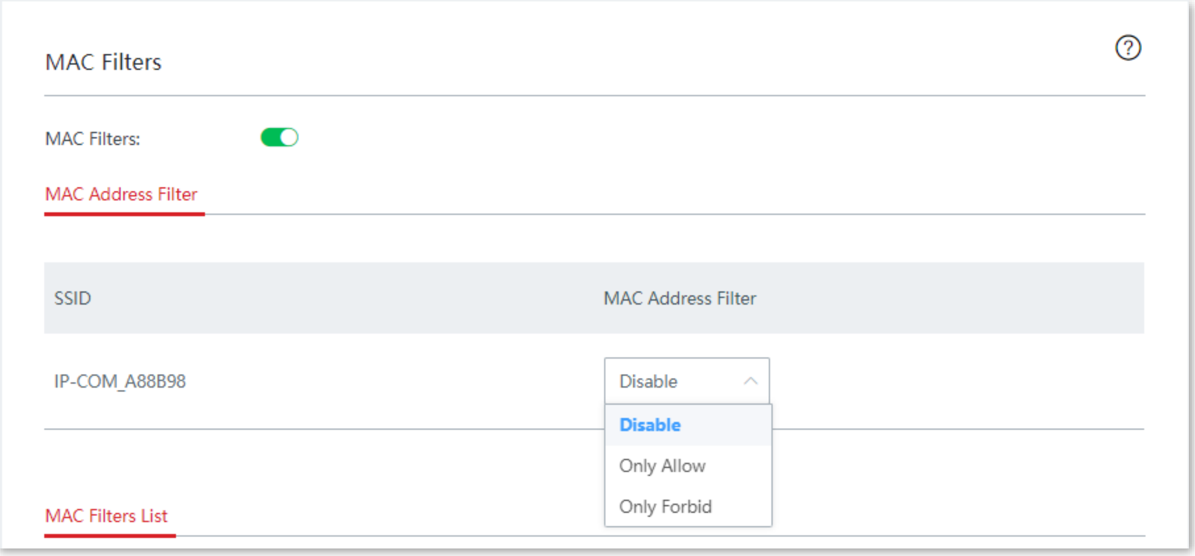
Allow/Disallow a wireless client to access the internet

1. Enable the **MAC Filters** function, and select a MAC address filter mode.

   (1) Set the **MAC Filters** from ○ to ●.

   (2) Select a **MAC Address Filter** mode for the corresponding SSID from the **MAC Address Filter** drop-down list menu.

   (3) Click **Save**.



MAC Filters

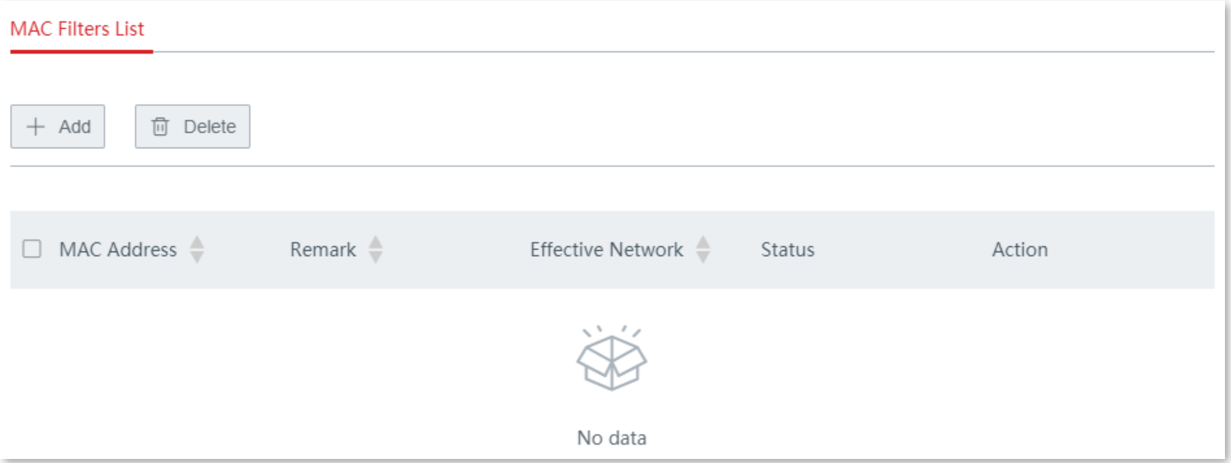
MAC Filters: ●

MAC Address Filter

SSID	MAC Address Filter
IP-COM_A88B98	Disable

2. Create a MAC filter rule.

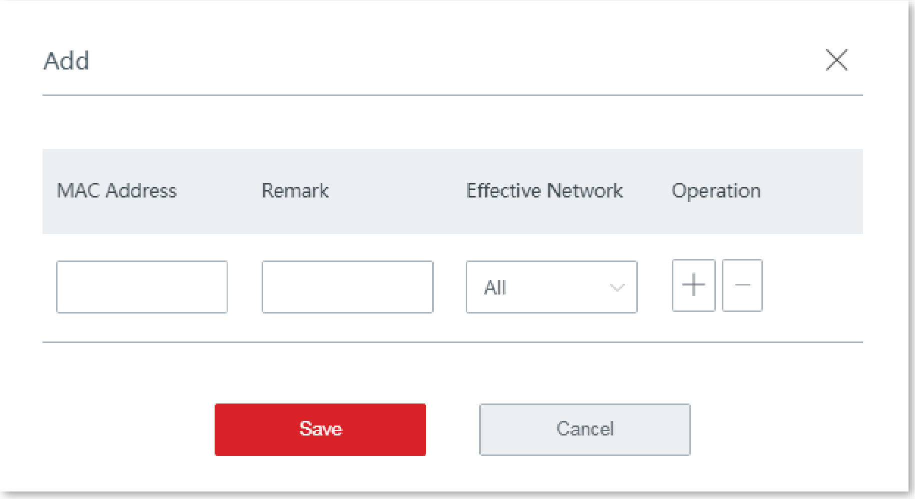
(1) Click **Add**. The **Add** configuration window appears.



(2) Configure the following settings on the **Add** window.

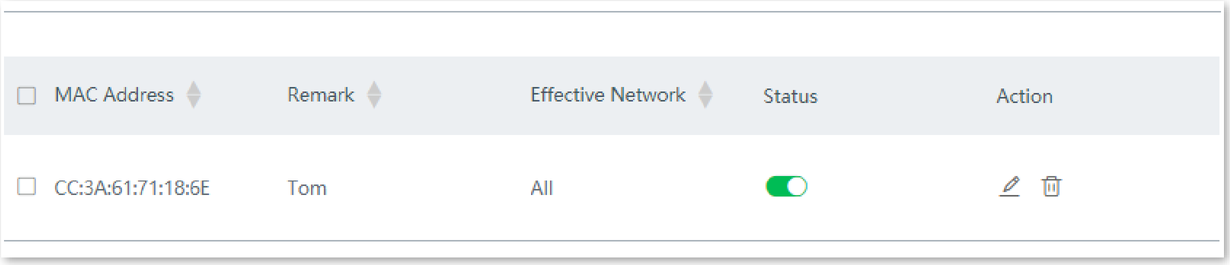
- Enter the MAC address of the wireless client to be controlled in **MAC Address** input box.
- (Optional) Specify a description for the client in **Remark** input box.
- Select the WiFi network from the drop-down list menu of the **Effective Network**.

(3) Click **Save**.



----End

After it is saved successfully, the wireless client with the added MAC address can/cannot access the specified WiFi networks.



□ MAC Address	Remark	Effective Network	Status	Action
□ CC:3A:61:71:18:6E	Tom	All	●	✎ 🗑

Example of configuring MAC filters

Network requirement

An enterprise uses EW12 to set up a LAN to meet the following requirement:

Only the purchasing staff is allowed to connect to the WiFi network (Purchase) to access the internet.

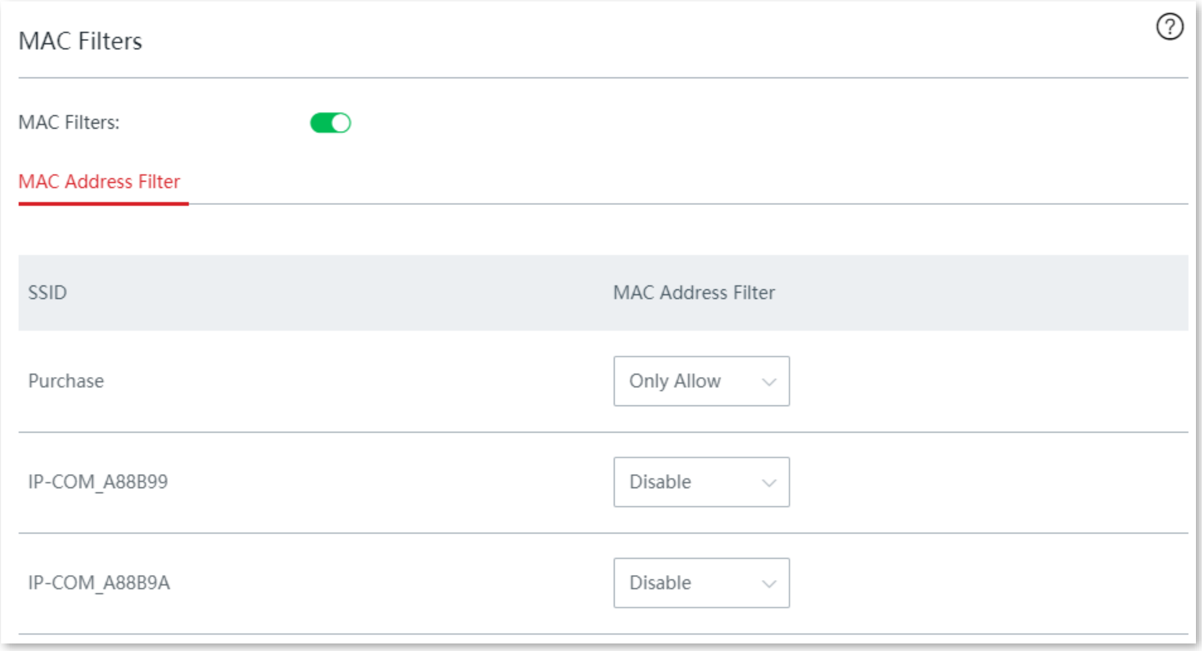
Assume that the MAC address of the purchasing staff's computer is CC:3A:61:71:1B:6E and the SSID is Purchasing.

Solutions

The MAC filters function can meet this requirement.

Configuration procedure

1. Set the **MAC Filters** from ○ to ●.
2. Select **Only Allow** for **Purchase** from the **MAC Address Filter** drop-down list menu, and click **Save**.



MAC Filters

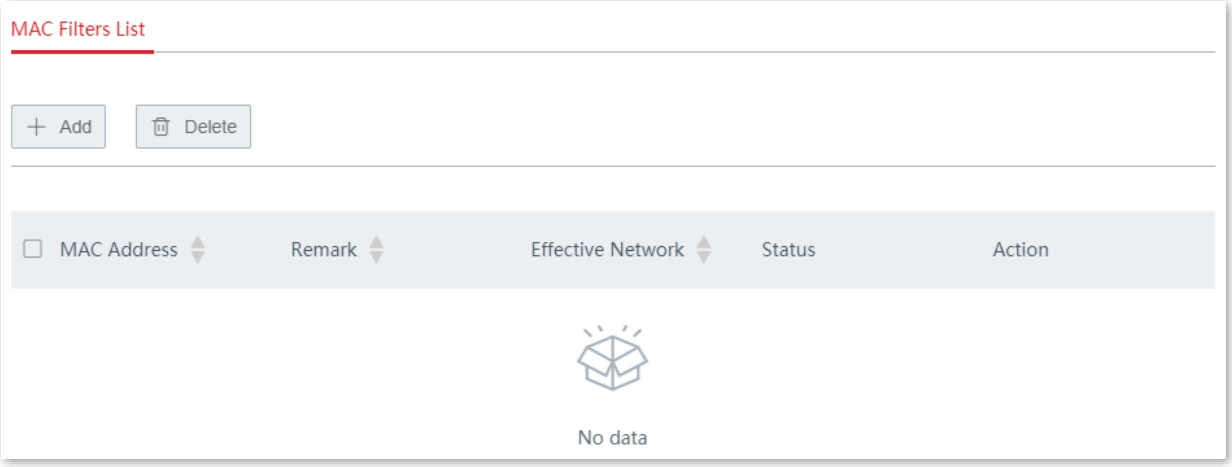
MAC Filters: ●

MAC Address Filter

SSID	MAC Address Filter
Purchase	Only Allow
IP-COM_A88B99	Disable
IP-COM_A88B9A	Disable

3. Create a MAC filter rule.

   (1) Click **Add**. The **Add** configuration window appears.



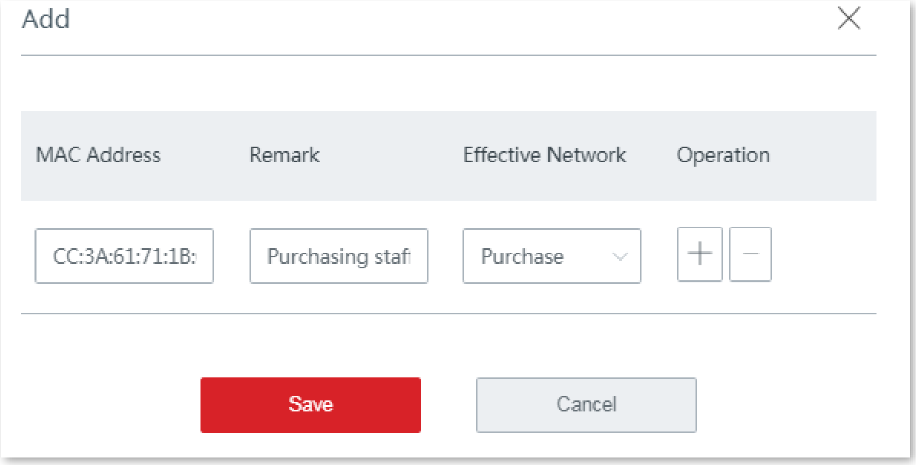
☐ MAC Address	Remark	Effective Network	Status	Action

No data

(2) Set the following parameters.

- Enter **CC:3A:61:71:1B:6E** in the **MAC Address** input box.
- Enter **Purchasing staff** in the **Remark** input box.
- Select **Purchase** from the drop-down list menu of the **Effective Network**.

(3) Click **Save**.



MAC Address	Remark	Effective Network	Operation
CC:3A:61:71:1B:	Purchasing staf	Purchase	+ −

----End

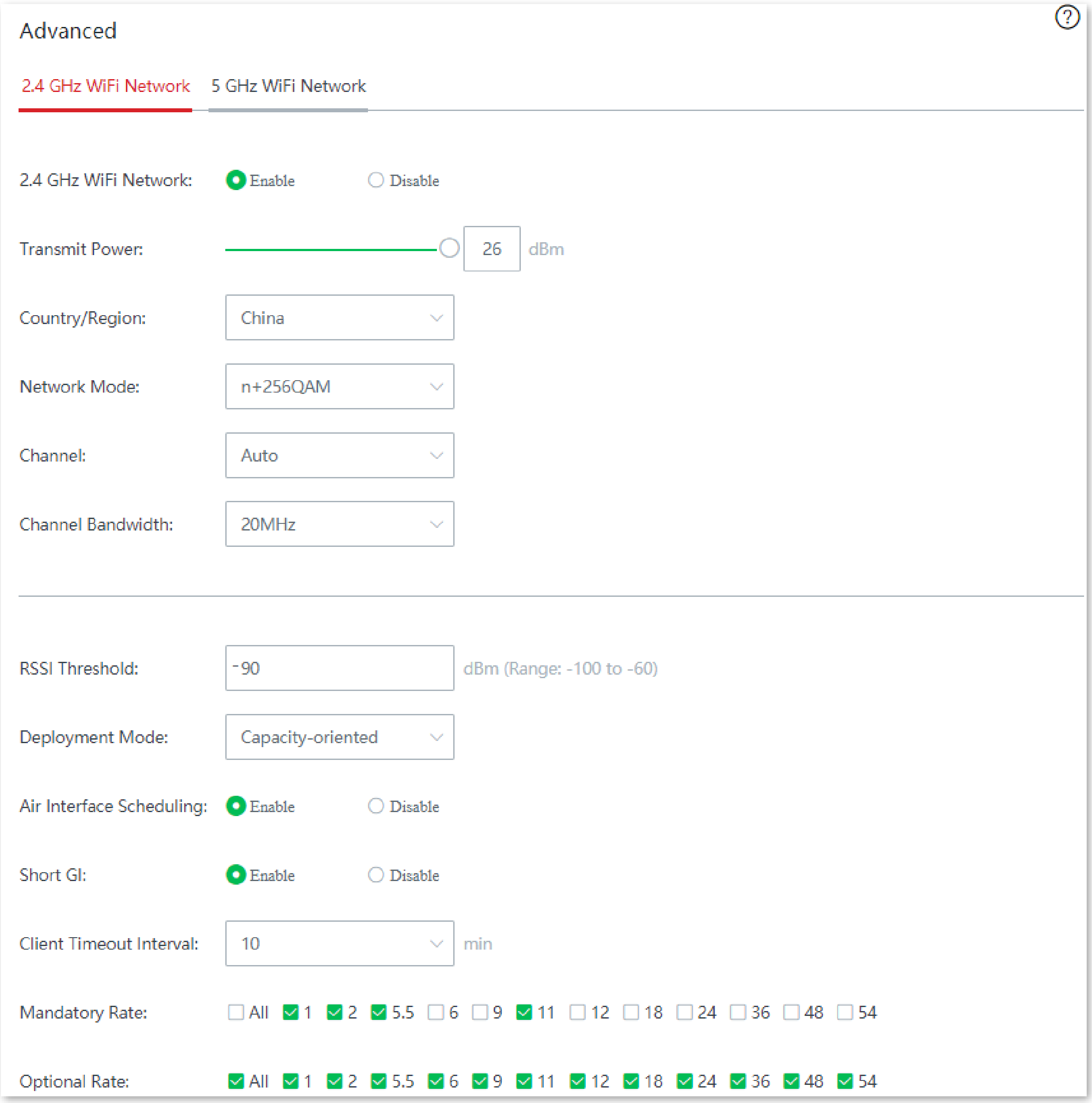
Verification

Only the computer with the MAC address of CC:3A:61:71:1B:6E can connect to the WiFi network (**Purchase**), and other devices are blocked.

3.4.4 Advanced

In this section, you can configure the advanced parameters such as transmit power, network mode, deployment mode, and air interface scheduling.

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



Advanced

2.4 GHz WiFi Network | 5 GHz WiFi Network

2.4 GHz WiFi Network: ● Enable ○ Disable

Transmit Power: 26 dBm

Country/Region: China

Network Mode: n+256QAM

Channel: Auto

Channel Bandwidth: 20MHz

RSSI Threshold: -90 dBm (Range: -100 to -60)

Deployment Mode: Capacity-oriented

Air Interface Scheduling: ● Enable ○ Disable

Short GI: ● Enable ○ Disable

Client Timeout Interval: 10 min

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

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

Parameter description

Parameter	Description
2.4 GHz WiFi Network	It is used to enable or disable the Advanced settings for 2.4 GHz WiFi network.
5 GHz WiFi Network	It is used to enable or disable the Advanced settings for 5 GHz WiFi network.

Parameter	Description
Transmit Power	It 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 WiFi network.
Network Mode	It specifies the WiFi network mode (also called 802.11 mode, radio mode, or wireless mode) of the node. A proper network mode enables the clients to get the maximum transmission rate and compatibility. Available options for 2.4 GHz band: – 11b: In this mode, only 802.11b wireless devices are allowed to access the node's 2.4 GHz WiFi network. – 11g: In this mode, only 802.11g wireless devices are allowed to access the node's 2.4 GHz WiFi network. – 11b/g: In this mode, 802.11b and 802.11g wireless devices can access the node's 2.4 GHz WiFi network. – 11b/g/n (default): In this mode, 802.11b, 802.11g and 802.11n wireless devices operating at 2.4 GHz can access the node's 2.4 GHz WiFi network. – n+256QAM: In this mode, 802.11b, 802.11g and 802.11n wireless devices operating at 2.4 GHz can access the node's 2.4 GHz WiFi network. QAM is known as Quadrature Amplitude Modulation, which is a modulation method of amplitude modulation on two orthogonal carriers. It modulates signals simultaneously by using the orthogonality of sine wave and cosine wave to improve the modulation efficiency. n+256QAM is at the 2.4 GHz band. Switch the IEEE 802.11n standard to the 256-QAM modulation mode of IEEE 802.11ac, and the single-stream rate also increases from 150 Mbps of IEEE 802.11n standard to 200 Mbps of IEEE 802.11ac standard. This enhancement is only effective when the 2.4 GHz band is supported by both the transmitter and the receiver. If either part does not support n+256QAM, the highest single-stream rate in the 2.4 GHz band is still 150 Mbps. After the modulation mode is changed to n+256QAM, the network stability and anti-interference performance are inferior to other modes. Available options for 5 GHz band: – 11a: In this mode, only 802.11a wireless devices are allowed to access the node's 5 GHz WiFi network. – 11ac (default): In this mode, only 802.11ac wireless devices are allowed to access the node's 5 GHz WiFi network. – 11a/n mixed: In this mode, 802.11a and 802.11n wireless devices operating in 5 GHz can access the node's 5 GHz WiFi network. It cannot be modified when the device works in Cable-Free (Router mode).

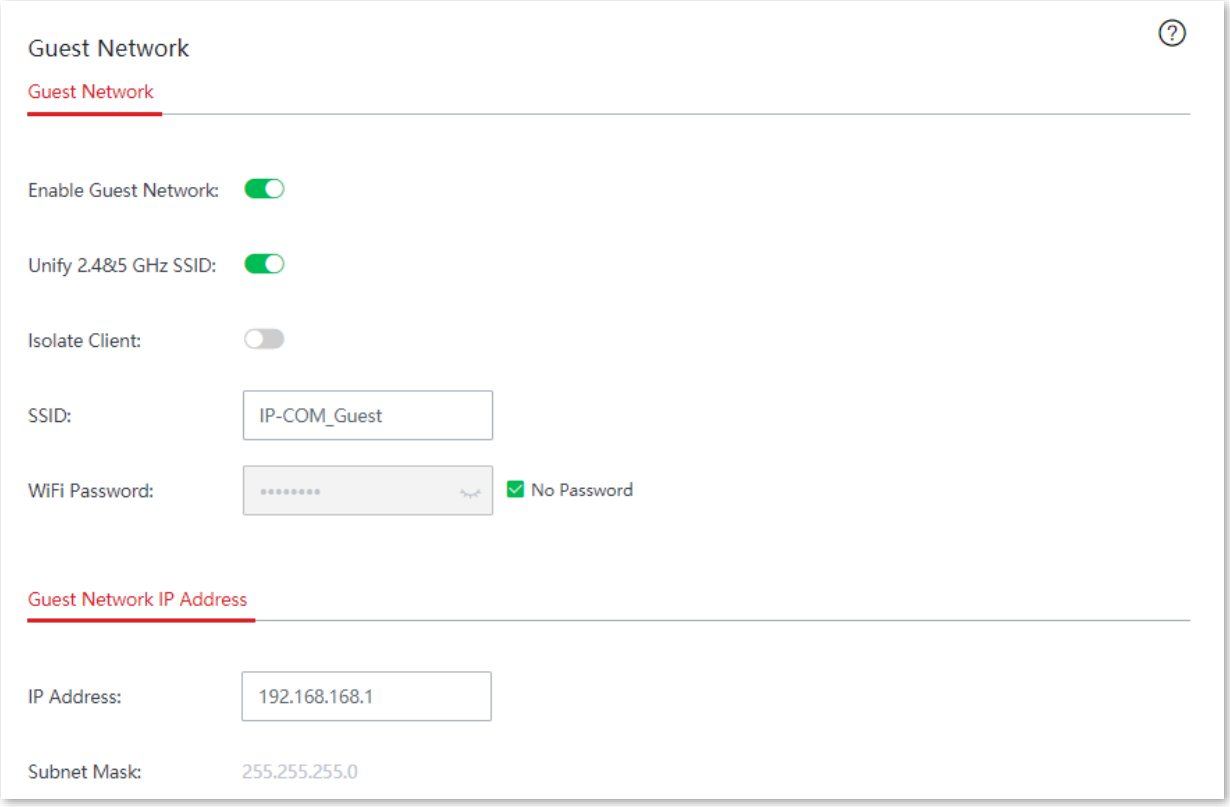
Parameter	Description
Channel	It specifies the channel in which this device operates. Select an idle channel in the ambient environment to prevent interference. **Auto** indicates that this device automatically switches to a channel rarely used in the ambient environment to prevent interference. It cannot be modified when the device works in Cable-Free (Router mode).
Channel Bandwidth	It specifies the bandwidth of the node's working channel. – 20MHz: The node uses a 20MHz channel bandwidth. – 40MHz: The node uses a 40MHz channel bandwidth. – 20/40MHz: For 2.4 GHz only. The node automatically adjusts the channel bandwidth to 20MHz or 40MHz according to the surrounding environment. – 80MHz: For 5 GHz only. The node uses 80MHz channel bandwidth. It cannot be modified when the device works in Cable-Free (Router mode).
RSSI Threshold	It specifies the minimum wireless client signal strength acceptable to the node. A mobile client with signal strength lower than this threshold cannot connect to the node. You can set this parameter to ensure that mobile clients connect to node with strong signal strength.
Air Interface Scheduling	It specifies whether to enable the air interface scheduling function. This function allows equal data transmission time for each client. This prevents some slow clients from occupying excessive airtime resources, so as to improve the overall device efficiency and effectively ensure the device connections for a larger number of clients and greater throughputs.
APSD	This parameter appears only on the 5 GHz WiFi network page It specifies whether to enable the Automatic Power Save Delivery (APSD) mode. APSD is a WMM power saving protocol created by Wi-Fi Alliance. Enabling APSD helps reduce power consumption. By default, this mode is disabled.
Short GI	It specifies short guard interval for preventing data block interference. Propagation delays may occur on the receiver side due to factors such as multipath wireless signal transmission. If a data block is transmitted at an overly high speed, it may interfere with the previous data block. The short GI helps prevent such interference. Enabling the short GI can yield a 10% improvement in wireless data throughput.
Client Timeout Interval	It specifies the maximum period before a WiFi client is disconnected from the node if the client exchanges no data with the node. When data is exchanged within the period, countdown stops.

Parameter	Description
Mandatory Rate	It specifies the basic rate sets for normal operation of the device. You can adjust the mandatory rates to restrict low-rate clients accessing the WiFi network and improve the internet experience of other clients. – **Mandatory Rate**: The clients can connect to the node only when they meet the mandatory rate required by the node. – **Optional Rate**: The clients meeting the mandatory requirement can connect to the node with higher rate.
Optional Rate	

3.4.5 Guest network

In this section, you can configure a guest network for visitors to protect the security of the main network, including enabling/disabling guest network, modifying SSID, setting WiFi password and so on. The client connected to the guest network can only access the internet and other wireless clients under the guest network and cannot access the node management page and the main network. This function can meet the online needs of guests and ensure the security of the main network.

Navigate to **Wireless** > **Guest Network** to enter the page. By default, this function is disabled.



Guest Network

Guest Network

Enable Guest Network: ●

Unify 2.4&5 GHz SSID: ●

Isolate Client: ○

SSID: IP-COM_Guest

WiFi Password: •••••••• ☑ No Password

Guest Network IP Address

IP Address: 192.168.168.1

Subnet Mask: 255.255.255.0

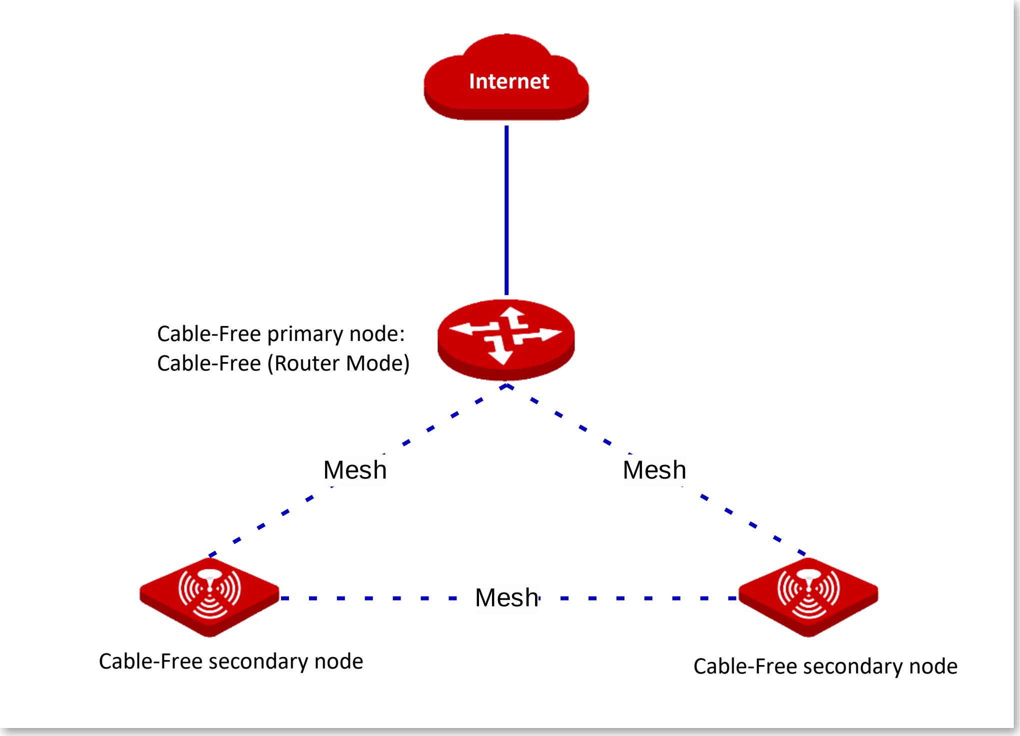
Parameter description

Parameter		Description
Guest Network	Enable Guest Network	It is used to enable or disable the guest network.
	Unify 2.4&5 GHz SSID	It is used to unify SSIDs for 2.4 GHz and 5 GHz guest WiFi networks. – Enable: The wireless name of the node’s guest network of 2.4 GHz and 5 GHz is the same, only one WiFi network name is displayed. When the user connects to the node's guest network, it will automatically connect to the network's best WiFi signal. – Disable: Set the 2.4 GHz and 5 GHz guest networks separately.
	Isolate Client	With this function enabled, clients connected to the guest network cannot communicate with each other, leading to higher WiFi network security.
	SSID	It specifies WiFi name of the guest network. Tip To differentiate the main network and the guest network, you are recommended to set the SSIDs differently.
	WiFi Password	It specifies password used for WiFi network. You are recommended to use the combination of digits, letters and special characters for higher security.
	No Password	With this function enabled, wireless clients can connect to the guest network without a password. Select this option only when necessary since it leads to weak network security.
Guest Network IP Address	IP Address	It specifies the IP address (default: 192.168.168.1) of the guest network. The node assigns 192.168.168.*X* to wireless clients connected to it. You are recommended to keep the default settings if there is no IP conflict.
	Subnet Mask	It specifies subnet mask of the guest network. It is used to define the network segment of the guest network.

3.5 Node management

3.5.1 Overview

In this section, you can centrally manage other IP-COM branded cable-free devices in the same network. The network application topology is shown below.



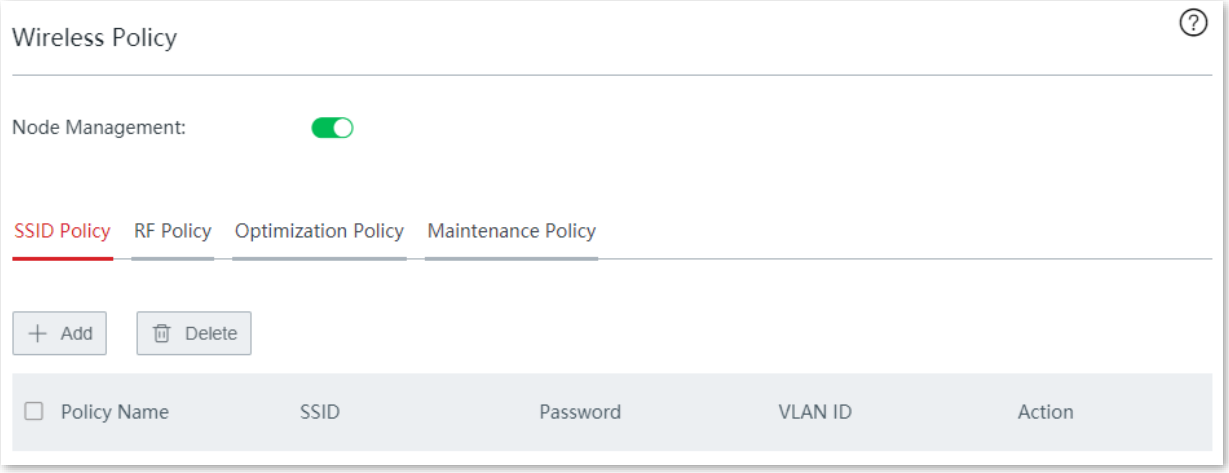
- **Configuration wizard**

The cable-free devices can be managed uniformly after joining the cable-free network. The configuration steps and tasks are described in the following table.

Step	Task	Description
1	Enable node management	Optional. This function is enabled by default.
2	Configure wireless policy	Required. Preset the node’s configuration information in form of policies.
3	Configure node group	Required. Create a node group.
4	Maintenance node	Required. Divide the nodes into a specified group and issue the configuration to the node.

- **Enable node management**

This function is enabled by default. To modify the function state, navigate to **Node Management** > **Wireless Policy** to enter this page.



Wireless Policy

Node Management: ●

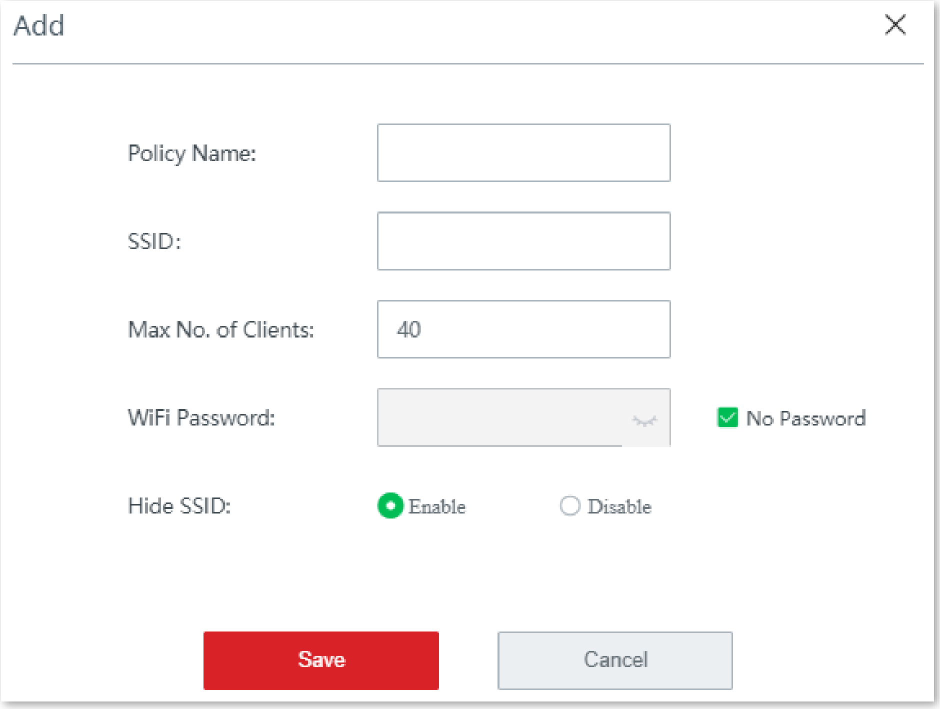
□	Policy Name	SSID	Password	VLAN ID	Action

3.5.2 Wireless policy

In this section, you are allowed to configure SSID policy, RF policy, optimization policy and maintenance policy. By configuring these policies, the node can provide different WiFi networks, enable or disable the wireless function at the corresponding band, assign downlink transmission time equally and set maintenance schedule.

- **Configure the SSID policy**

Click **SSID policy** > **Add** to enter the page. See the following figure.



Add

Policy Name:

SSID:

Max No. of Clients: 40

WiFi Password: ☑ No Password

Hide SSID: ● Enable ○ Disable

Parameter description

Parameter	Description
Policy Name	It specifies the name of SSID policies. Note The SSID policy name cannot be duplicated.
SSID	It specifies a WiFi network name. A maximum of 31 bytes is supported.
Max No. of Clients	It specifies the maximum number of wireless clients allowed to connect to the WiFi network. Range: 1 to 128. Note A node supports a maximum of 128 clients as well. If you want to deliver multiple SSID policies to a node, please set up a proper maximum number of wireless clients, and ensure that the sum of the maximum clients for each node does not exceed 128.
WiFi Password	It specifies the Wi-Fi password of the Wi-Fi network, which contains 8 to 63 ASCII characters or 8 to 64 hexadecimal characters.
Hide SSID	With the function enabled, the SSID is hidden. You need to enter the SSID and relevant parameters manually when you connect a wireless client to the WiFi network, improving the security of the WiFi network, to a certain extent.

Modify the policy

Navigate to **Node Management** > **Wireless Policy** > **SSID Policy** to enter this page. Click ✎ in the action bar.

After the modification is saved, the new policy will be issued to nodes in the corresponding group.

Delete the policy

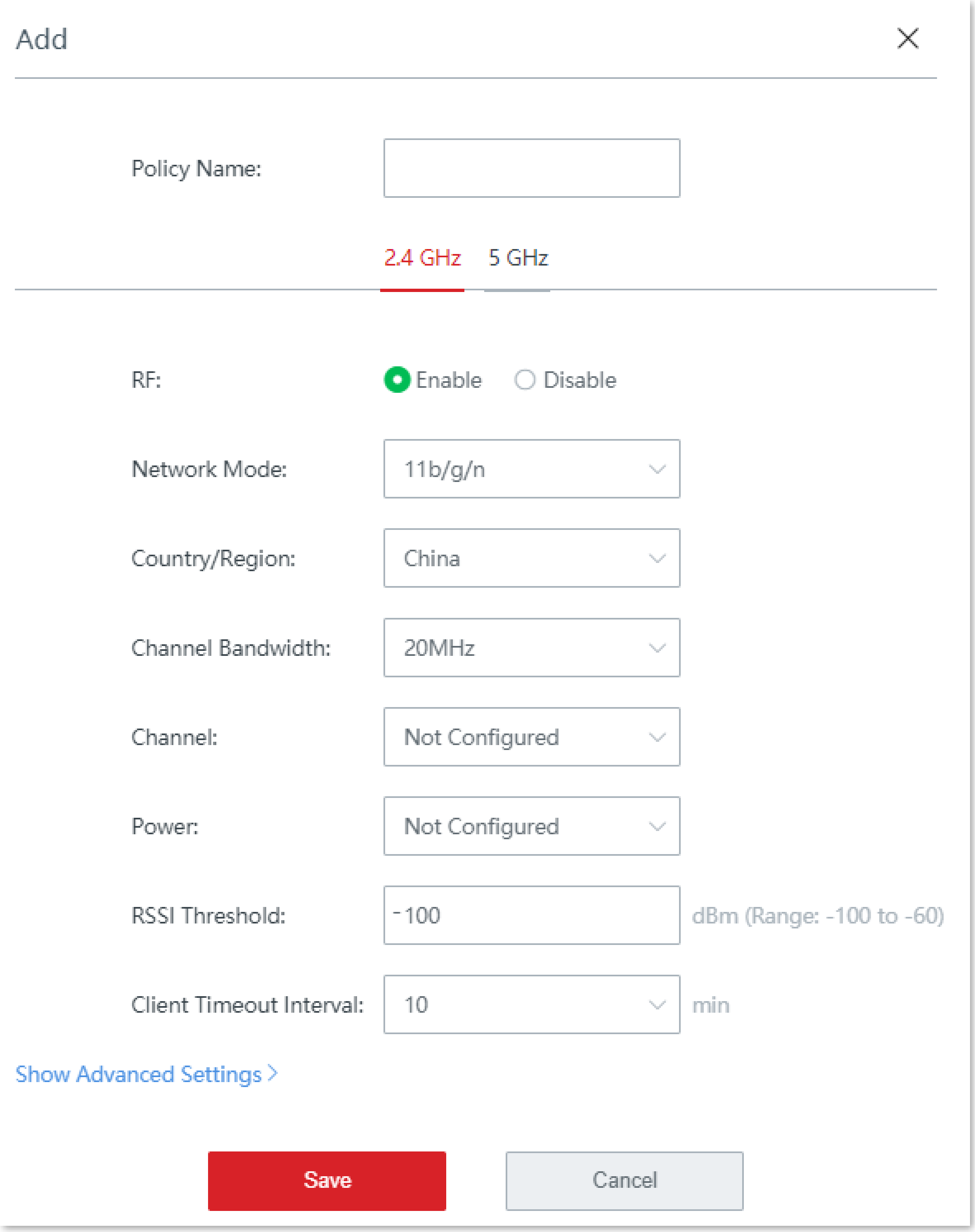
You can delete policies that are not currently used (not referenced by node groups).

Delete policies one by one: Navigate to **Node Management** > **Wireless Policy** > **SSID Policy** to enter this page. Click 🗑 in the corresponding policy's action bar.

Delete policies in batches: Navigate to **Node Management** > **Wireless Policy** > **SSID Policy** to enter this page. Select the policies you want to delete and click delete.

Configure the RF policy

Click **RF Policy** > **Add** to enter the page. See the following figure.



Add

Policy Name:

RF: ● Enable ○ Disable

Network Mode: 11b/g/n

Country/Region: China

Channel Bandwidth: 20MHz

Channel: Not Configured

Power: Not Configured

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

Client Timeout Interval: 10 min

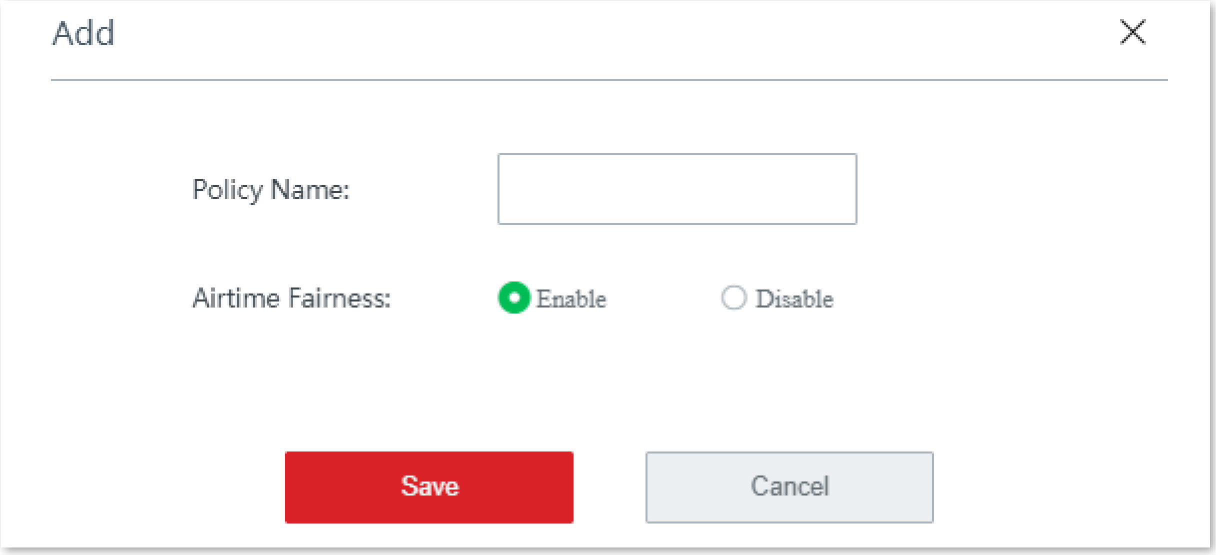
Parameter description

Parameter	Description
Policy Name	It specifies the name of a RF policy. Note the RF policy names cannot be duplicated.
RF	It is used to enable or disable the wireless function at the corresponding band.
Network Mode	The available network modes for a 2.4 GHz WiFi network include 11b, 11g, 11b/g, 11b/g/n and 11n+256 QAM. – 11b: It indicates that only the wireless clients compliant with IEEE 802.11b are allowed to connect to the 2.4 GHz WiFi network of the node. – 11g: It indicates that only the wireless clients compliant with IEEE 802.11g are allowed to connect to the 2.4 GHz WiFi network of the node. – 11b/g: It indicates that only the wireless clients compliant with IEEE 802.11b and IEEE 802.11g are allowed to connect to the 2.4 GHz WiFi network of the node. – 11b/g/n: It indicates that only the wireless clients compliant with IEEE 802.11b, IEEE 802.11g, and IEEE 802.11n of 2.4 GHz are allowed to connect to the 5 GHz WiFi network of the node. – 11n+256 QAM: It indicates that only the wireless clients compliant with IEEE 802.11b, IEEE 802.11g, IEEE 802.11n of 2.4 GHz, and 256 QAM are allowed to connect to the 2.4 GHz WiFi network of the node. The available network modes for 5 GHz WiFi network include 11a, 11ac and 11a/n. – 11a: It indicates that only the wireless clients compliant with IEEE 802.11a are allowed to connect to the 5 GHz WiFi network of the node. – 11ac: It indicates that only the wireless clients compliant with IEEE 802.11ac are allowed to connect to the 5 GHz WiFi network of the node. – 11a/n: It indicates that only the wireless clients compliant with IEEE 802.11a and IEEE 802.11n of 5 GHz are allowed to connect to the 5 GHz WiFi network of the node.
Country/Region	It is used to select a country or region in which nodes locate to meet the regulatory requirements for channel and transmitted power in different countries or regions.
Channel Bandwidth	It is used to select the wireless frequency bandwidth. – 20 MHz: Nodes can only use 20 MHz channel bandwidth. – 40 MHz: Nodes can only use 40 MHz channel bandwidth. – 20/40 MHz: Nodes use 20 MHz or 40MHz channel bandwidth based on its ambient environment. It is only supported by 2.4 GHz WiFi networks. – 80 MHz: Nodes can only use 80 MHz channel bandwidth. It is only supported by 5 GHz WiFi networks.

Parameter	Description
Channel	It is used to select a channel, Auto or Not Configured for a node. Not Configured indicates that the channel configuration is not delivered to nodes, and nodes use their own channel configurations. Please select a less-used channel in the ambient environment to reduce interference. The available range of the channel depends on the current selected country/region, wireless operating frequency band and bandwidth.
Power	It is used to set up the wireless transmitted power of nodes. Range: 8 to 30 dBm. The default is Not configured. A larger transmitted power indicates a wider WiFi coverage. But a smaller transmitted power helps improve the WiFi network performance and security.
RSSI Threshold	It is used to set up the Received Signal Strength Indicator (RSSI) value which is acceptable by nodes. If the signal strength of a wireless client received by a node is less than this value, the client cannot connect to the node. Range: -100 dBm to -60 dBm. 2.4 GHz default value: -100dBm, 5 GHz default value: -100 dBm. When multiple nodes are deployed, a proper RSSI value ensures that wireless clients connect to the WiFi network with a stronger signal.
Client Timeout Interval	It is used to set up the aging time for clients. If a client carries no traffic and is in the inactive state for a specific period of time, it will be disconnected from the WiFi network.
Mandatory Rate	It is used to set up a group of mandatory rates. Clients must support the mandatory rate set. Otherwise, they cannot connect to the WiFi network.
Optional Rate	It is used to set up a group of optional rates. Clients can either support or does not support the optional rate set.

- **Configure the Optimization policy**

Click **Optimization policy** > **Add** to enter the page. See the following figure.



Add

Policy Name:

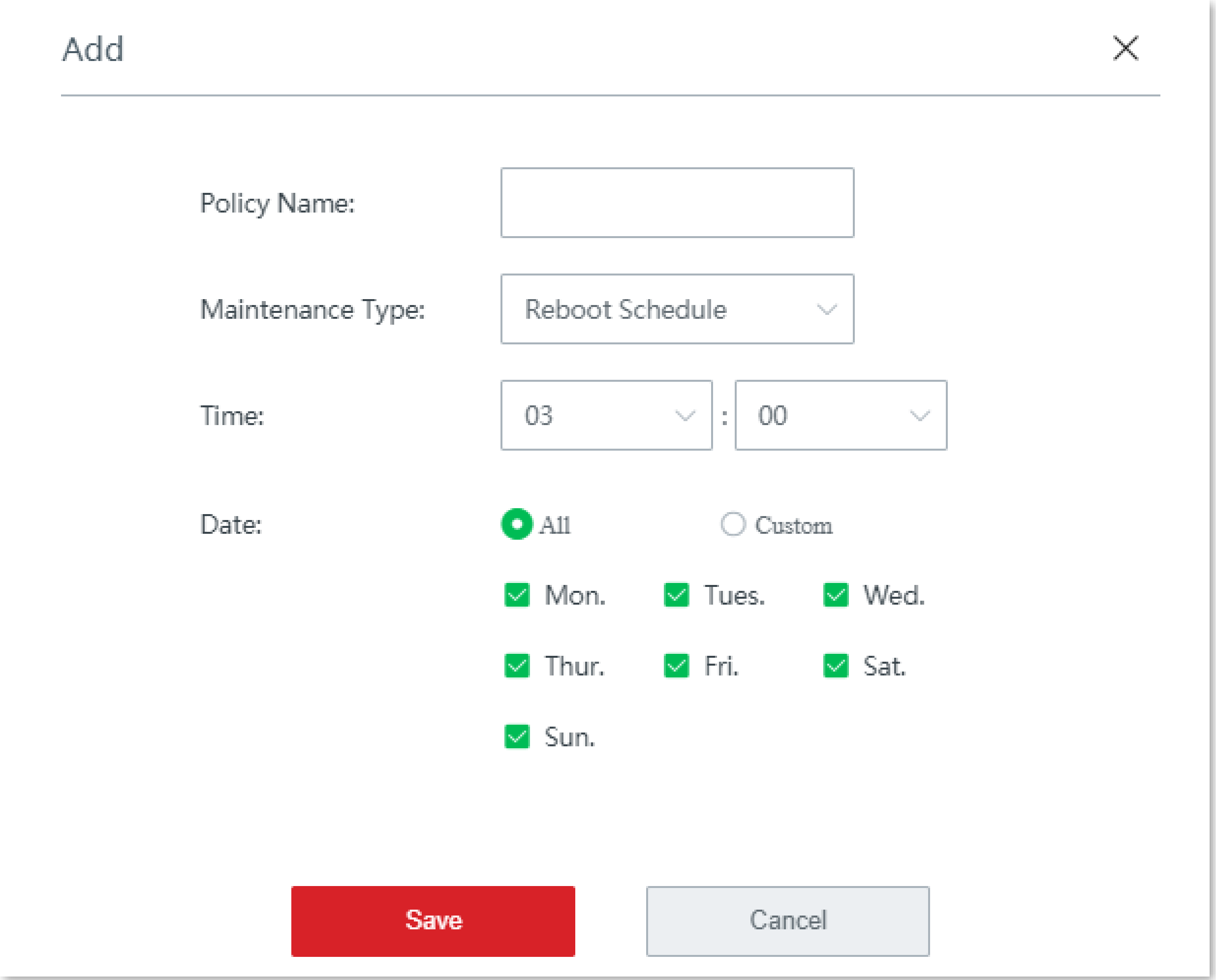
Airtime Fairness: ● Enable ○ Disable

Parameter description

Parameter	Description
Policy Name	It specifies the name of an optimization policy. Note The optimization policy names cannot be duplicated.
Airtime Fairness	With the function enabled, a node assigns downlink transmission time equally, enabling the high-speed users and low-speed users to obtain the same downlink transmission time which helps high-speed users transmit more data. Thus, the node achieves a higher system throughput and a larger number of connected users.

Configure the Maintenance policy

Click **Maintenance policy** > **Add** to enter the page. See the following figure.



Add

Policy Name:

Maintenance Type: Reboot Schedule

Time: 03 : 00

Date: ● All ○ Custom

☑ Mon. ☑ Tues. ☑ Wed.

☑ Thur. ☑ Fri. ☑ Sat.

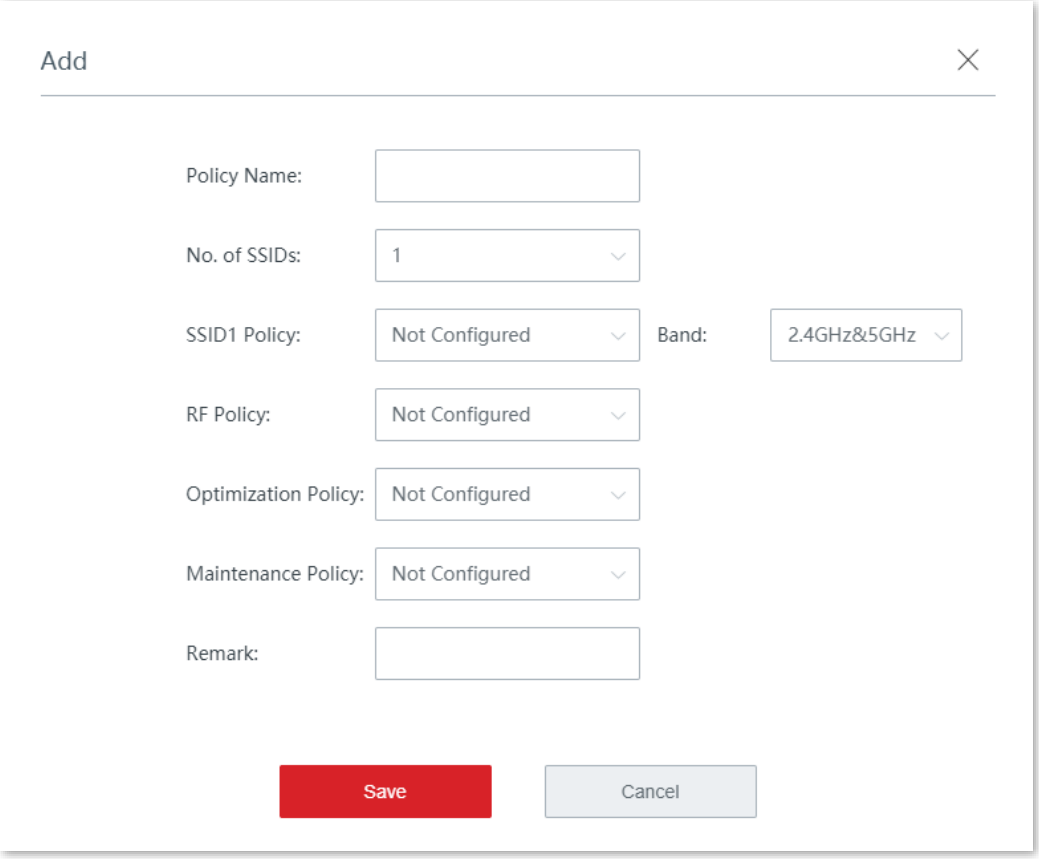
☑ Sun.

Parameter description

Parameter	Description
Policy Name	It specifies the name of a maintenance policy. Note The maintenance policy names cannot be duplicated.
Maintenance Type	– Reboot Schedule: It specifies the reboot schedule function of nodes. You can configure the reboot time and date. – Cycle Reboot: It specifies the cycle reboot function of nodes. You can configure the reboot interval at which the node reboots.
Time	When the maintenance type is **Reboot Schedule**, it is used to set the time and date at which the node will automatically reboot.
Date	
Interval	When the maintenance mode is **Cyclic Reboot**, it is used to set the interval between automatic reboot.

3.5.3 Node group

1. Click **Node Group** > **Add** to enter the page. See the following figure.



Add

Policy Name:

No. of SSIDs: 1

SSID1 Policy: Not Configured Band: 2.4GHz&5GHz

RF Policy: Not Configured

Optimization Policy: Not Configured

Maintenance Policy: Not Configured

Remark:

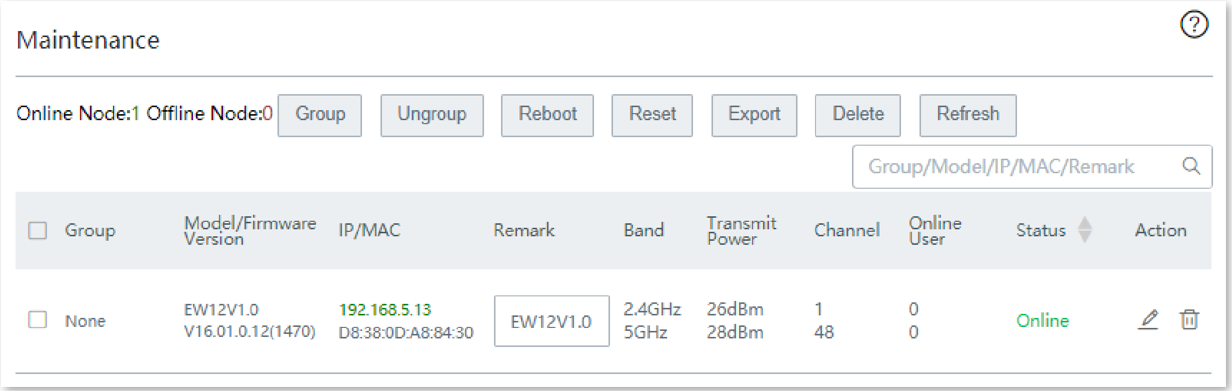
2. Set the parameters and click **Save**.

----End

Parameter description

Parameter	Description
Policy Name	It specifies the name of group policies. Note The group policy names cannot be duplicated.
No. of SSIDs	It is used to select the number of SSIDs. Range: 1 to 4. The default is 1.
SSID Policy	It is used to select an SSID policy to be involved. SSID policies must be configured in the **Wireless Policy** > **SSID Policy** page first. If multiple SSIDs are configured, each SSID must be involved a unique SSID policy.
Band	It is used to select a wireless frequency band from 2.4 GHz, 5 GHz, and 2.4 GHz & 5 GHz. Select the frequency band based on the supported bands of nodes. If the node only supports 2.4 GHz band, you can select 2.4 GHz or 2.4 GHz & 5 GHz. If 5 GHz is selected, the configuration is not effective.
RF Policy	It is used to select a RF policy to be involved. RF policies must be configured in the **Wireless Policy** > **RF Policy** page first.
Optimization Policy	It is used to select an optimization policy to be involved. Optimization policies must be configured in the **Wireless Policy** > **Optimization Policy** page first.
Maintenance Policy	It is used to select a maintenance policy to be involved. Maintenance policies must be configured in the **Wireless Policy** > **Maintenance Policy** page first.
Remark	It is used to describe the info of the node group policy.

3.5.4 Maintenance


Maintenance

Online Node:1 Offline Node:0

□	Group	Model/Firmware Version	IP/MAC	Remark	Band	Transmit Power	Channel	Online User	Status	Action
□	None	EW12V1.0 V16.01.0.12(1470)	192.168.5.13 D8:38:0D:A8:84:30	EW12V1.0	2.4GHz 5GHz	26dBm 28dBm	1 48	0 0	Online	✎ 🗑

Parameter description

Parameter		Description
Button	Group	It is used to divide nodes into a node group and reference the same configuration to improve the management efficiency.
	Ungroup	It is used to delete nodes from the node group. Nodes which are not in the group will resynchronize the configuration of the Cable-Free (Router Mode) node’s wireless module.
	Reboot	It is used to reboot the selected nodes.
	Reset	It is used to reset the selected nodes to factory settings.
	Export	It is used to export the info of all managed nodes.
	Delete	It is used to delete the info of all selected offline nodes.
	Refresh	It is used to refresh the information of the nodes shown in this page.
Group		It specifies the name of the group to which a node belongs.
Model/Firmware Version		It specifies the model/firmware version of the corresponding node.
IP/MAC		– IP address: It specifies the IP address obtained by a node from the DHCP server of the device, that is the login IP address of the node. – MAC address: It specifies the MAC address of the WiFi network of the node.
Remark		It specifies a brief description of the node
Band		It displays the frequency band at which the node operates, either 2.4 GHz or 5 GHz band.
Transmit Power		It displays the wireless transmitted power of nodes. Policy Delivery indicates that the transmit power policy is delivered based on the node group policy.
Channel		It displays the operating channel of the WiFi network connected by a client.

Parameter		Description
		Policy Delivery indicates that the operating channel policy is delivered based on the node group policy.
Online User		It specifies the number of wireless clients that connect to the corresponding band of the WiFi network of a node.
Status		It displays the current status of a node.
Action	✎	With this function, the configuration information of a node, such as country or region, channel, transmission power and other parameters can be modified separately.
	🗑	It is used to delete offline nodes and nodes that succeeded in upgrading.
Country/Region		The wireless transmitted power and channel of different countries or regions may differ. For normal use, please select a correct country or region.
Network Mode		It specifies the WiFi network mode of this band. The available network modes for a 2.4 GHz WiFi network include 11b, 11g, 11b/g, 11b/g/n and 11n+256 QAM. – 11b: It indicates that only the wireless clients compliant with IEEE 802.11b are allowed to connect to the 2.4 GHz WiFi network of the node. – 11g: It indicates that only the wireless clients compliant with IEEE 802.11g are allowed to connect to the 2.4 GHz WiFi network of the node. – 11b/g: It indicates that only the wireless clients compliant with IEEE 802.11b and IEEE 802.11g are allowed to connect to the 2.4 GHz WiFi network of the node. – 11b/g/n: It indicates that only the wireless clients compliant with IEEE 802.11b, IEEE 802.11g, and IEEE 802.11n of 2.4 GHz are allowed to connect to the 5 GHz WiFi network of the node. – 11n+256 QAM: It indicates that only the wireless clients compliant with IEEE 802.11b, IEEE 802.11g, IEEE 802.11n of 2.4 GHz, and 256 QAM are allowed to connect to the 2.4 GHz WiFi network of the node. The available network modes for 5 GHz WiFi network include 11a, 11ac and 11a/n. – 11a: It indicates that only the wireless clients compliant with IEEE 802.11a are allowed to connect to the 5 GHz WiFi network of the node. – 11ac: It indicates that only the wireless clients compliant with IEEE 802.11ac are allowed to connect to the 5 GHz WiFi network of the node. – 11a/n: It indicates that only the wireless clients compliant with IEEE 802.11a and IEEE 802.11n of 5 GHz are allowed to connect to the 5 GHz WiFi network of the node.

Parameter`	Description
Channel Bandwidth	It specifies the bandwidth of a node's wireless channel. With high channel bandwidth, it is easier to obtain a higher transmission rate, but the transmission is less penetrating and the transmission distance is shorter. – 20 MHz: Nodes can only use 20 MHz channel bandwidth. – 40 MHz: Nodes can only use 40 MHz channel bandwidth. – 20/40 MHz: Nodes use 20 MHz or 40MHz channel bandwidth based on its ambient environment. It is only supported by 2.4 GHz WiFi networks. 80 MHz: Nodes can only use 80 MHz channel bandwidth. It is only supported by 5 GHz WiFi networks.
Channel	It specifies the operating channel of a node corresponding to a frequency band. – Policy Delivery: The channel of a node depends on the RF policy it involves. – Manual: You can specify a channel for a node manually.
Transmit Power	It specifies the wireless transmission power of the corresponding frequency band of the node. The higher the transmitting power, the wider the wireless coverage will be. However, reducing the transmitting power is more useful to improve the performance and security of WiFi network. Range for signal: 8 to 30 dBm.
RSSI Threshold	It is used to set up the threshold of the wireless client signal strength accepted by the node. Range: -100 to -60 dBm. If a wireless client signal strength is less than this threshold, the node disconnects the wireless client to ensure that the client can connect to a node with stronger wireless signal.
Client Timeout Interval	If a terminal carries no traffic and is in the inactive state for a specific period of time, it will be disconnected from the WiFi network of a node.
APSD	The Automatic Power Save Delivery function is effective only when the WMM function is enabled. You are recommended to disable it.

3.6 Smart optimization

The Smart Optimization function is used to optimize the entire mesh network. Click **Smart Optimization** to enter this page.

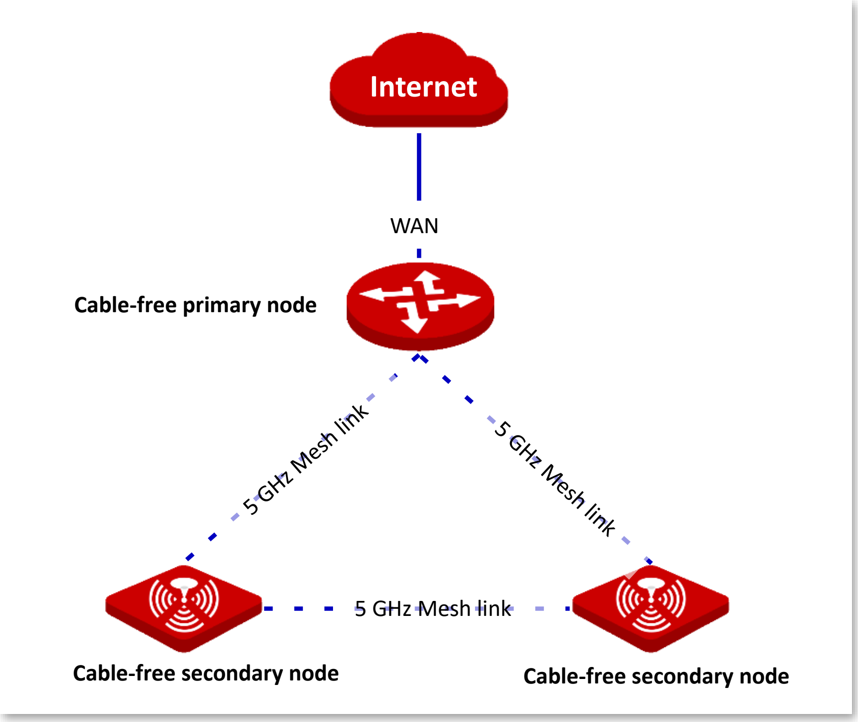
3.6.1 Wired networking

Overview

The cable-free device supports two networking modes: cable-free networking and wired networking. Cable-free networking is adopted by default.

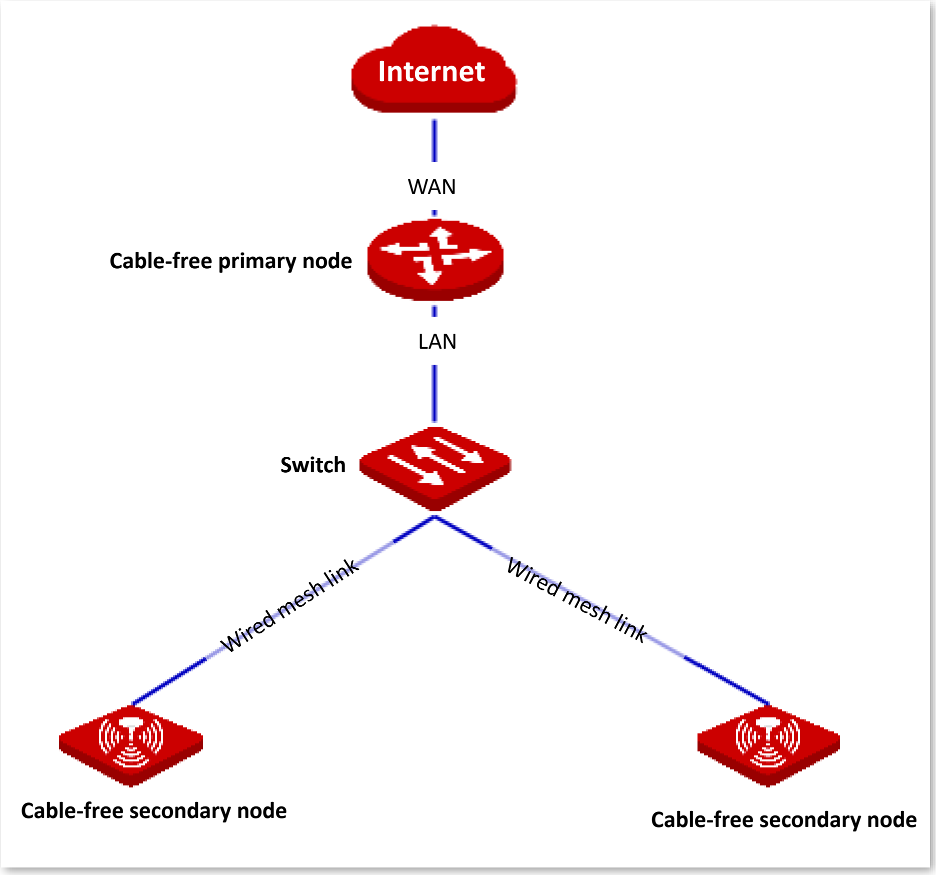
- **Cable-free networking**

The cable-free network system is set up by wireless means, and each cable-free device is connected wirelessly. The cable-free device will use one of the 5 GHz wireless frequency bands specially for establishing the wireless mesh link. The 2.4 GHz wireless frequency band and another 5 GHz wireless frequency band will be used for terminal devices' access.



- **Wired networking**

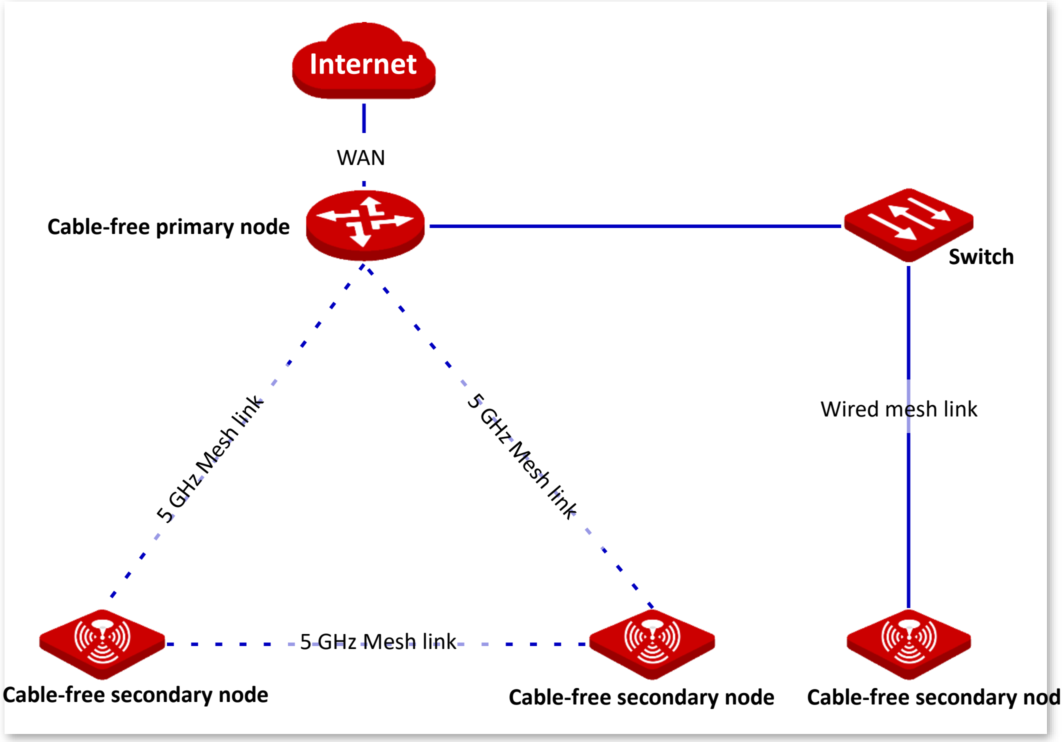
The wired network system is established in a wired manner, and each cable-free device is connected by Ethernet cable. The three wireless bands of cable-free device are used for terminal devices' access.



Cable-free networking is simpler and faster. Network wiring of a wired network should meet some requirements. There are still some advantages as follows.

- The mesh links are more stable with higher speed and longer transmission distance.
- The cable-free device capacity is larger.

In actual networking, you can also adopt mixed networking mode according to your needs. The network connection diagram is shown below as an example.

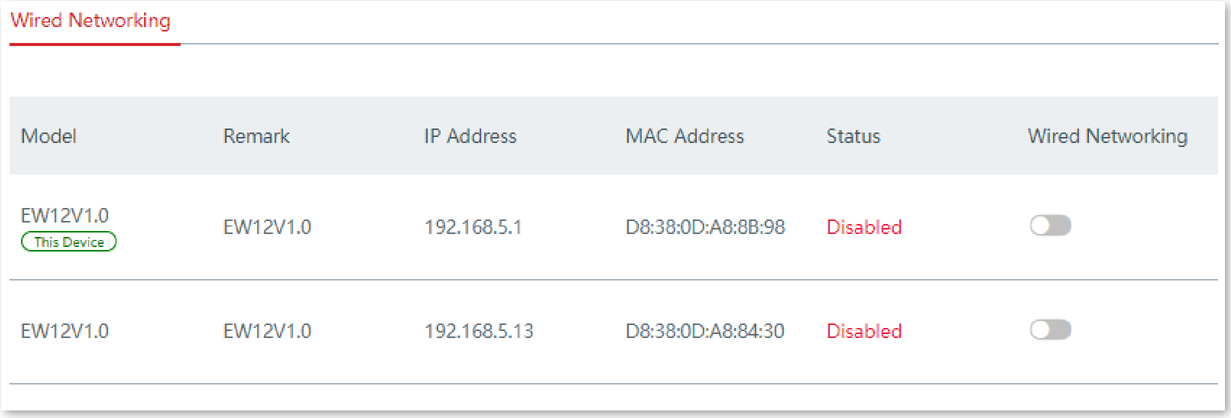


Configure wired networking

Tip

When the wired networking is enabled, the wireless networking function will be disabled automatically. Cable-free device that has connected to the network wirelessly will be disconnected.

1. Choose **Wired Networking** in **Smart Optimization** page. Select the node whose networking mode you want to change, and switch ○ to ●.



Wired Networking

Model	Remark	IP Address	MAC Address	Status	Wired Networking
EW12V1.0 This Device	EW12V1.0	192.168.5.1	D8:38:0D:A8:8B:98	Disabled	○
EW12V1.0	EW12V1.0	192.168.5.13	D8:38:0D:A8:84:30	Disabled	○

Parameter description

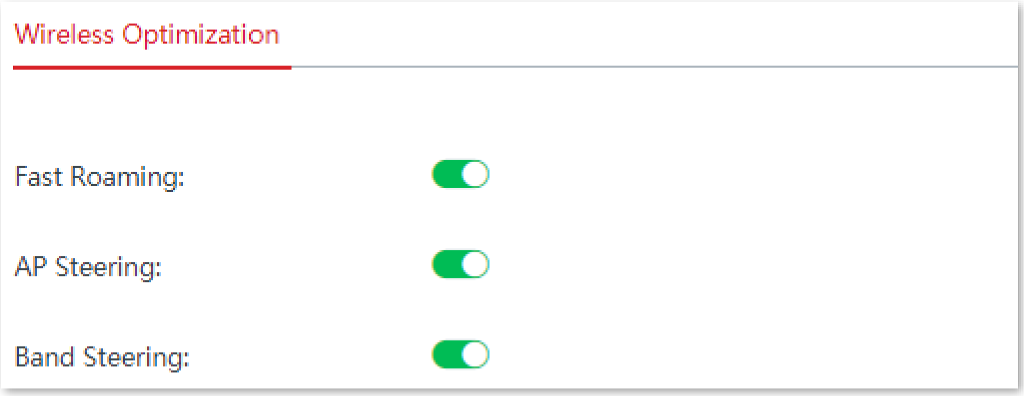
Parameter	Description
Model	It specifies the model and version of the node.
Remark	It specifies the remark for nodes. You can change it in the **Node Management** > **Maintenance** page.
IP Address	It specifies the IP address of the node.
MAC Address	It specifies the physical address of the node.
Status	It specifies the status of the wired networking function.
Wired Networking	It is used to enable/disable the wired networking function. After this function is enabled, the networking mode of nodes changes from cable-free networking to wired networking. And the three wireless bands of nodes are used for terminal access.

2. Connect nodes above with Ethernet cables.

----End

3.6.2 Wireless optimization

With this function, you can optimize the wireless experience in cable-free networking by adjusting the enabling states for fast roaming, AP steering, and band steering.



Fast Roaming: ●
AP Steering: ●
Band Steering: ●

Parameter description

Parameter	Description
Fast Roaming	With this function enabled, the device enables IEEE 802.11r fast roaming protocol, improving the user experience.
AP Steering	With this function enabled, the device leads a client to switch to another node for the higher connection quality when the current connection quality of the client is poor (week signal strength and high channel occupation ratio).

Parameter	Description
Band Steering	With this function enabled, the node leads a client to connect to the WiFi network at the frequency band with better quality (strong signal strength and low channel occupation ratio) when the current 5 GHz or 2.4 GHz connection quality of the client is poor (week signal strength and high channel occupation ratio).

3.7 Address reservation

3.7.1 Overview

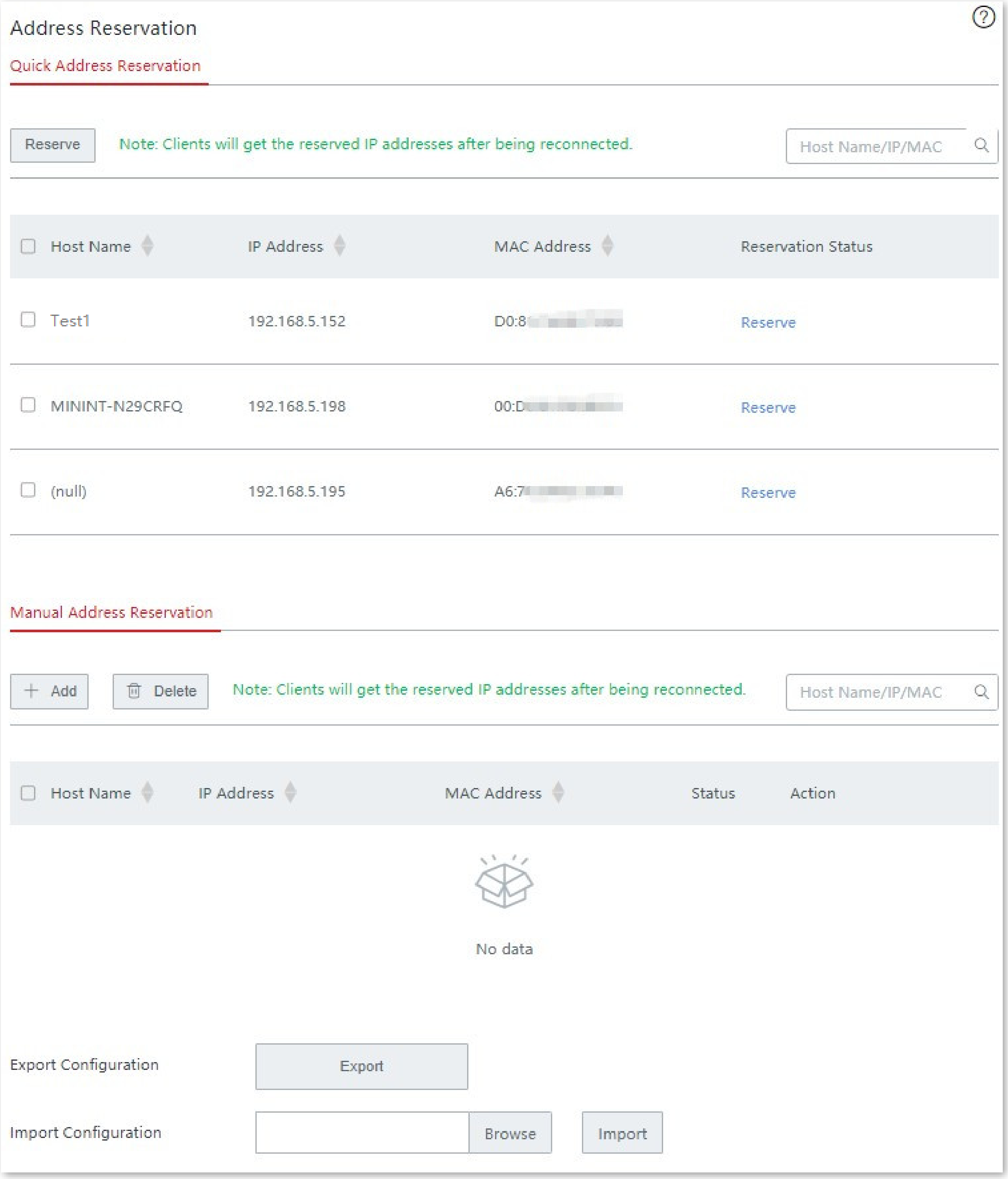
The address reservation function always allows a host, such as a computer, on LAN to receive the same IP address each time when they connect to the DHCP server. It ensures that the static IP address-based functions take effect normally, such as:

- Bandwidth control > Limit by group
- Filter Management > IP address filter
- Port forwarding > Internal server IP address
- DMZ host > IP address of DMZ Host

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

- **Quick Address Reservation**: You can directly reserve the IP addresses for online clients by clicking the **Reserve** button.
- **Manual Address Reservation:** You can manually specify addresses for the clients which are disconnected from the node.

Click **Address Reservation** to enter the page. See the following figure.



Address Reservation

Quick Address Reservation

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

□ Host Name	IP Address	MAC Address	Reservation Status
□ Test1	192.168.5.152	D0:8[redacted]	Reserve
□ MININT-N29CRFQ	192.168.5.198	00:D[redacted]	Reserve
□ (null)	192.168.5.195	A6:7[redacted]	Reserve

Manual Address Reservation

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

□ Host Name	IP Address	MAC Address	Status	Action

No data

Export Configuration   Export

Import Configuration   Browse   Import

Parameter description

Parameter		Description
Quick Address Reservation	Reserve	It is used to reserve the corresponding IP addresses for the selected hosts.
	Host Name	It specifies the name of the corresponding host.
	IP Address	It specifies the IP address of the corresponding host.
	MAC Address	It specifies the MAC address of the corresponding host.

Parameter		Description
Quick Address Reservation	Reservation Status	Click **Reserve** to reserve the corresponding IP address for the host. After the reservation, it displays **Reserved**.
Manual Address Reservation	Host Name	It specifies the name of the corresponding host, or the description of the host.
	IP Address	It specifies the IP address reserved for the specified host.
	MAC Address	It specifies the MAC address of the host to be reserved an IP address.
	Status	It specifies the status of the rule. You can enable or disable it as required.
	Operation	You can perform the following operations to the corresponding rule: ✎: Click it to edit the rule. 🗑: Click it to delete the rule.

3.7.2 Configure address reservation

Reserve addresses for online users

This function allows you to conveniently reserve static IP addresses for online hosts one by one or in batch.

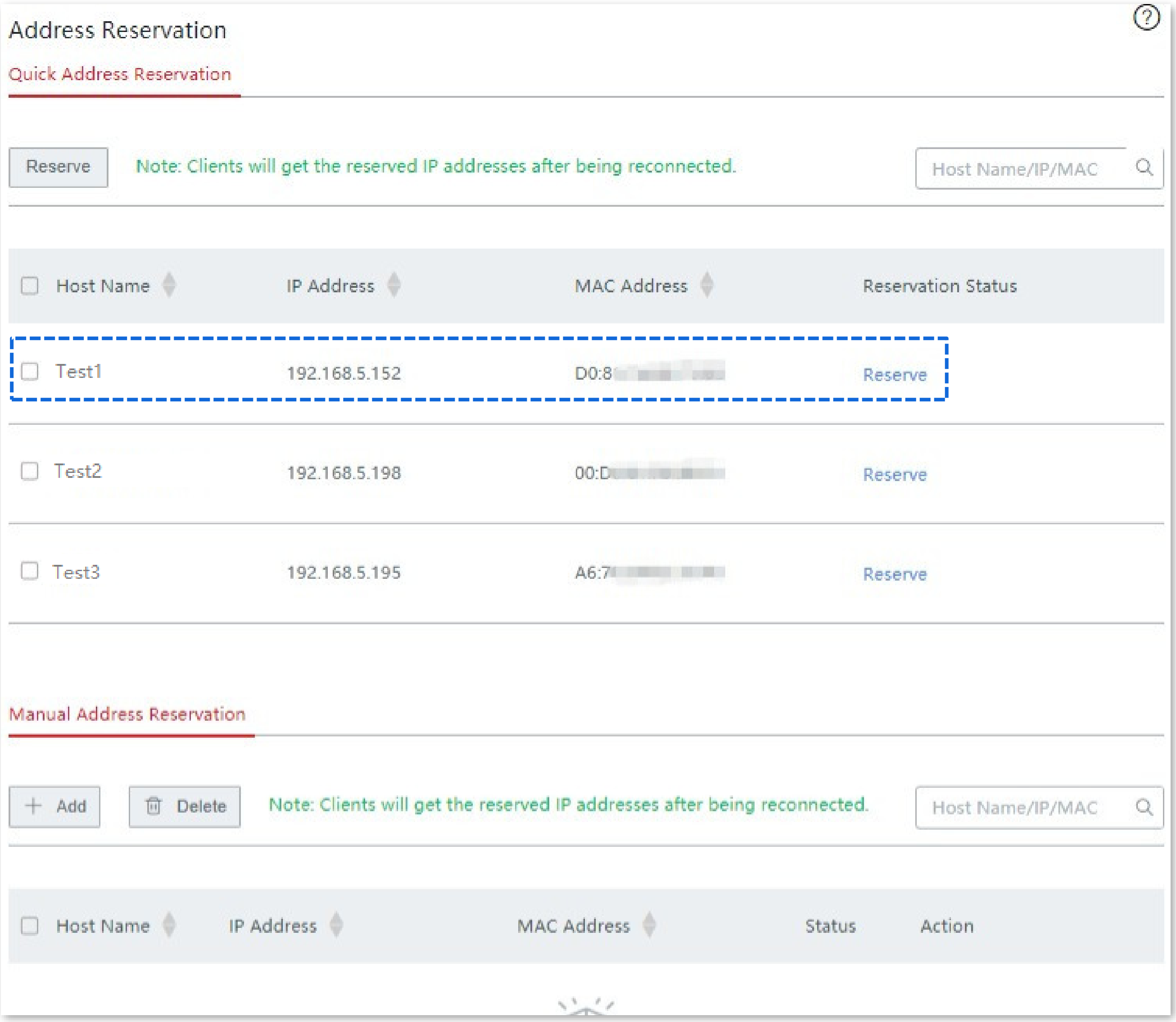
Tip

Clients will get the reserved IP addresses after being reconnected.

Configure online client-based quick address reservation

- **Method 1**

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



Address Reservation

Quick Address Reservation

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

□ Host Name	IP Address	MAC Address	Reservation Status
□ Test1	192.168.5.152	D0:8[redacted]	Reserve
□ Test2	192.168.5.198	00:D[redacted]	Reserve
□ Test3	192.168.5.195	A6:7[redacted]	Reserve

Manual Address Reservation

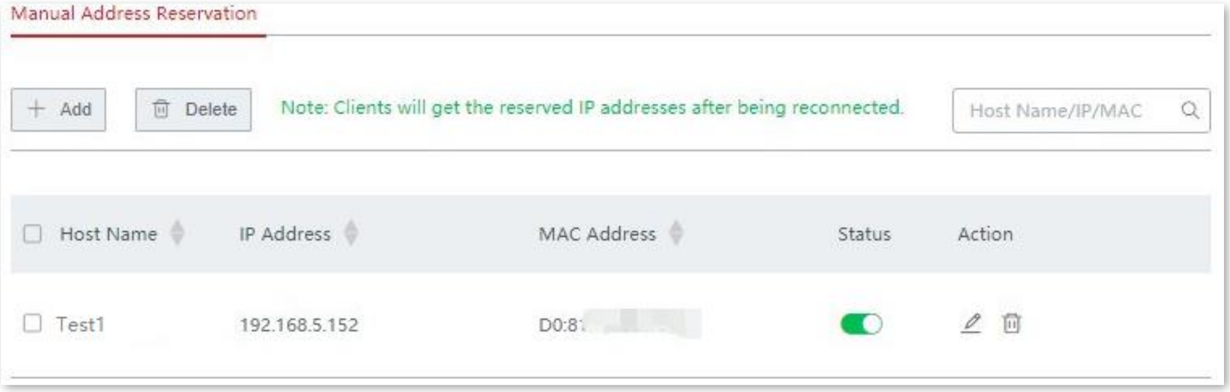
+ Add   Delete   Note: Clients will get the reserved IP addresses after being reconnected.   Host Name/IP/MAC

□ Host Name	IP Address	MAC Address	Status	Action

2. Locate the host you want to reserve a static IP address, which is **Test1** in this example, and click **Reserve** next to it.

----End

The Reservation Status of host named **Test1** is changed into **Reserved**, and displayed on the lower part of the page. See the following figure.



Manual Address Reservation

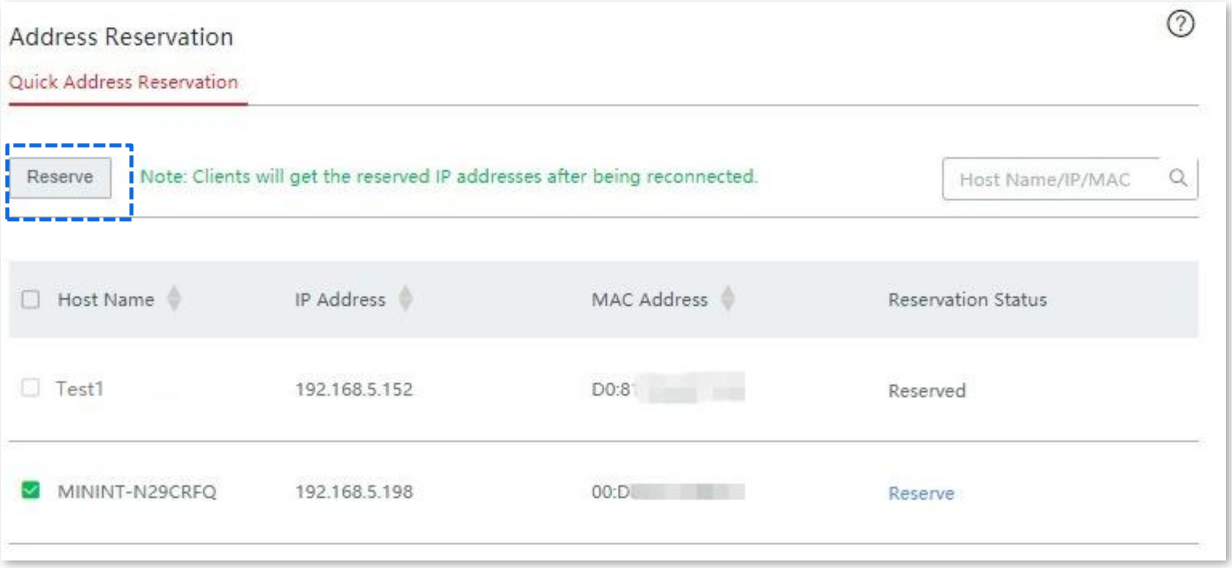
+ Add   Delete   Note: Clients will get the reserved IP addresses after being reconnected.   Host Name/IP/MAC

□ Host Name	IP Address	MAC Address	Status	Action
□ Test1	192.168.5.152	D0:8[redacted]	●	✎ 🗑

- **Method 2**

1. Choose **Address Reservation** to enter the page.
2. Select hosts you want to reserve a static IP address, and click the **Reserve** button.

   Or if you want to select all hosts on the list, check the checkbox next to Host Name.



Address Reservation

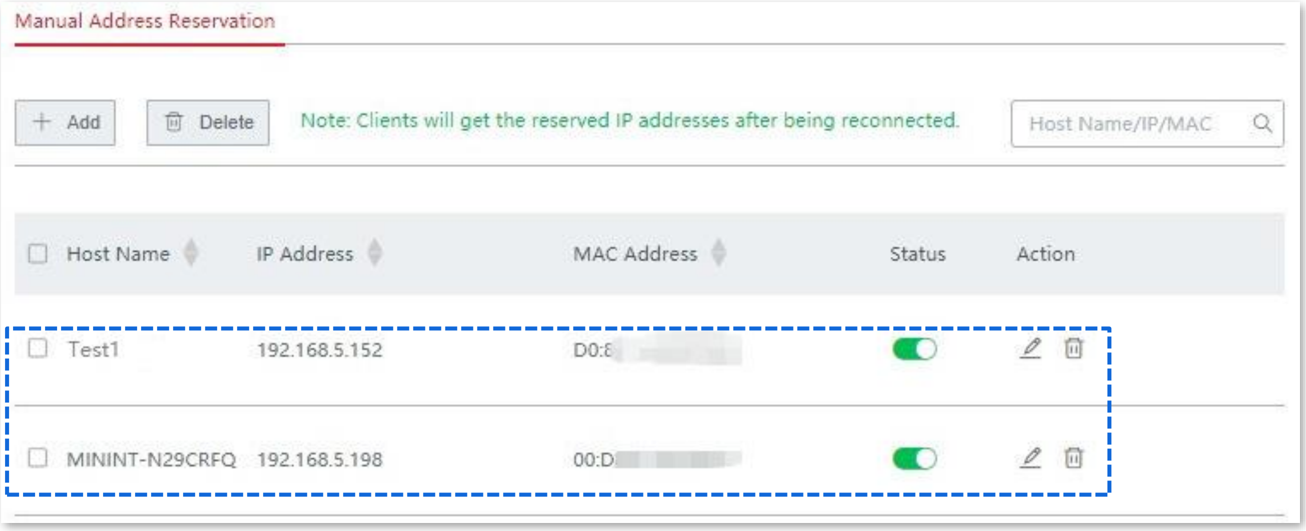
Quick Address Reservation

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

□ Host Name	IP Address	MAC Address	Reservation Status
□ Test1	192.168.5.152	D0:8[redacted]	Reserved
☑ MININT-N29CRFQ	192.168.5.198	00:D[redacted]	Reserve

----End

The **Reservation Status** of hosts are changed into **Reserved**, and displayed on the lower part of the page. See the following figure.



Manual Address Reservation

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

□ Host Name	IP Address	MAC Address	Status	Action
□ Test1	192.168.5.152	D0:8[redacted]	●	✎ 🗑
□ MININT-N29CRFQ	192.168.5.198	00:D[redacted]	●	✎ 🗑

Configure address reservation manually

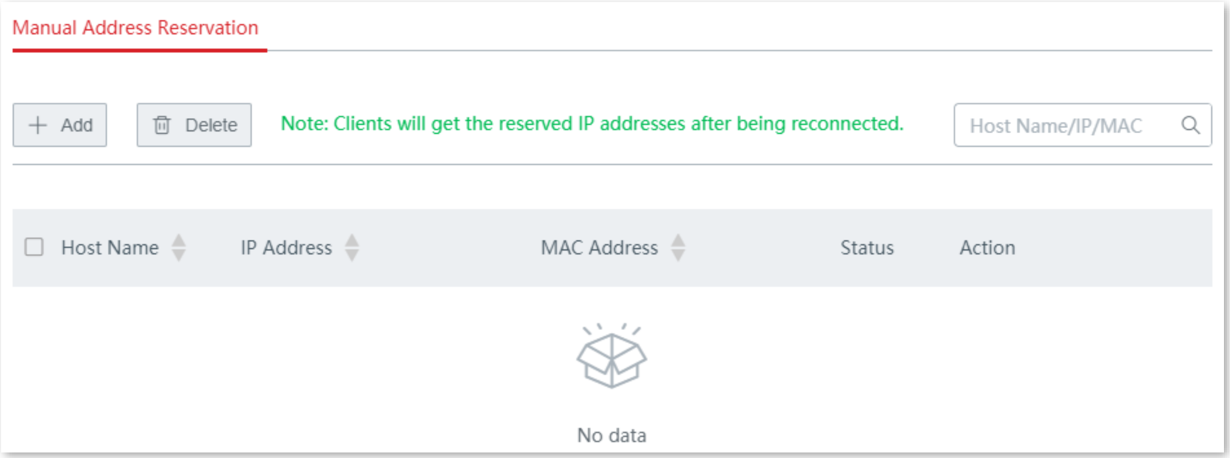
To reserve static IP addresses for hosts disconnected from the node or to reserve an easy-to-remember IP address for an online host, you can add the rule manually.

Tip

If you reserve an easy-to-remember IP address for an online host, the client gets the reserved IP addresses after being reconnected.

Configuration procedure

1. Click **Address Reservation**, and move to the **Manual Address Reservation** configuration area.



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

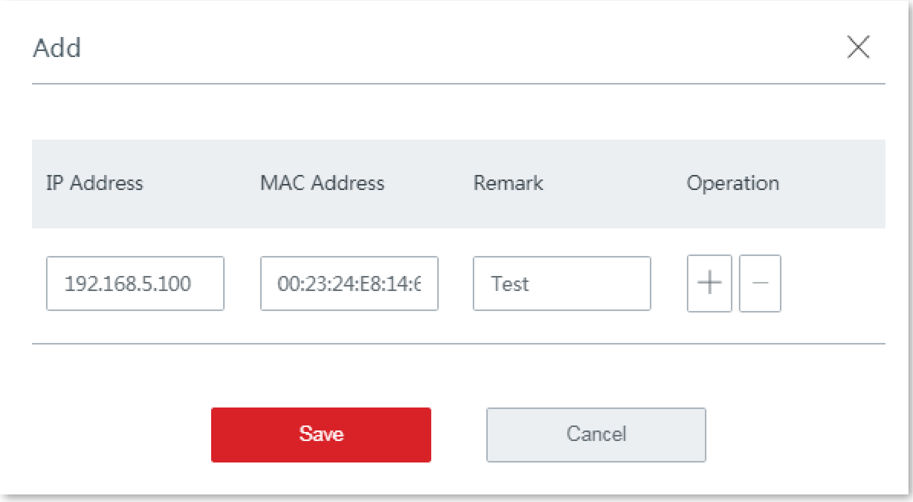
□ Host Name	IP Address	MAC Address	Status	Action

2. Click **Add**. The **Add** configuration window appears.
3. Enter the IP Address and MAC Address, which is 192.168.5.100/00:23:24:E8:14:6B in this example.
4. (Optional). Add a brief description in the **Remark** filed, which is **Test** in this example.

Tip

For convenient management later, you are recommended to enter a brief description to distinguish different hosts.

5. Click **Save**.

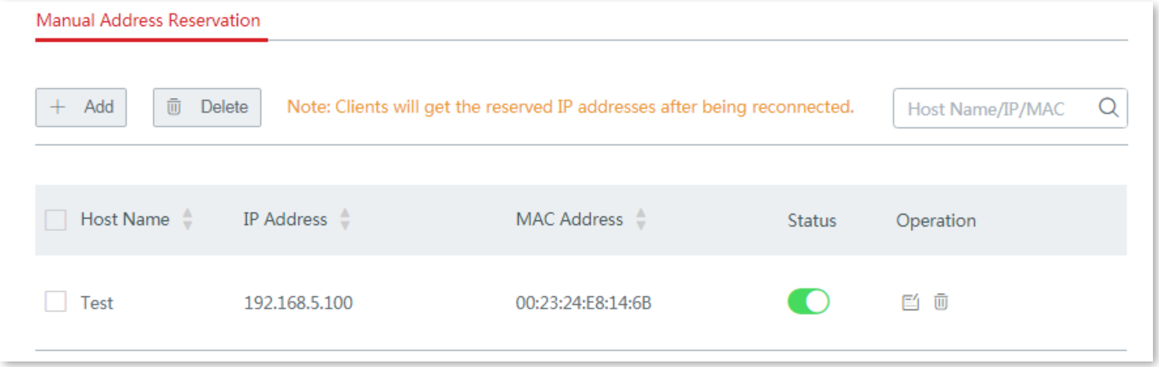


Add

IP Address	MAC Address	Remark	Operation
192.168.5.100	00:23:24:E8:14:6	Test	+ −

----End

The **Reservation Status** of hosts are changed into **Reserved**, and displayed on the lower part of the page. See the following figure.



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

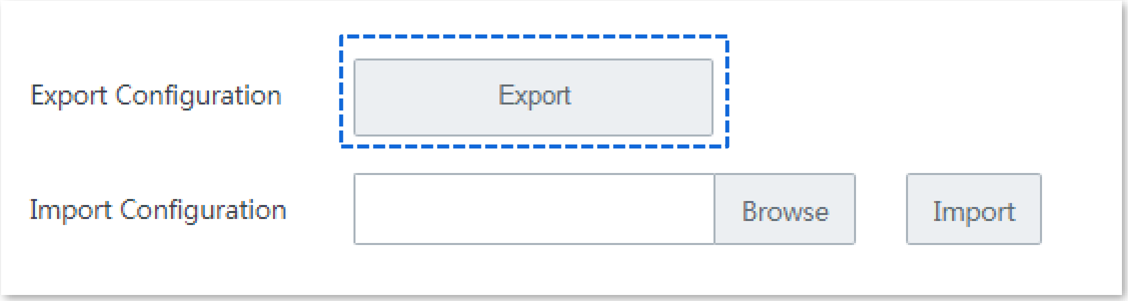
□ Host Name	IP Address	MAC Address	Status	Operation
□ Test	192.168.5.100	00:23:24:E8:14:6B	●	

3.7.3 Export/import your address reservation configuration

This function allows you to export the address reservation configuration you set to your local computer for backup, and import the configuration file you backed up to the device, relieving you from repeated laborious efforts for configuration.

Export configuration file to your local computer

1. Choose **Address Reservation**, and move to the bottom of the page.
2. Click the **Export** button.

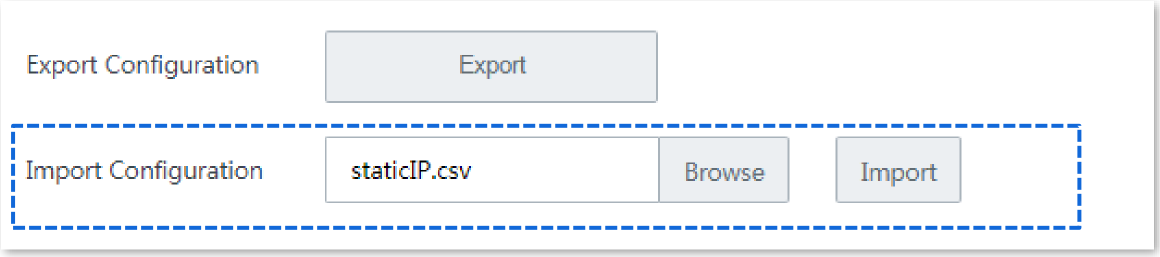


----End

A file named **staicIP.csv** is exported to the default download folder on your local computer.

Import configuration file to your device

1. Click **Browse**, and upload the address reservation configuration file you have backed up to your local computer.
2. Click the **Import** button.



staticIP.csv

----End

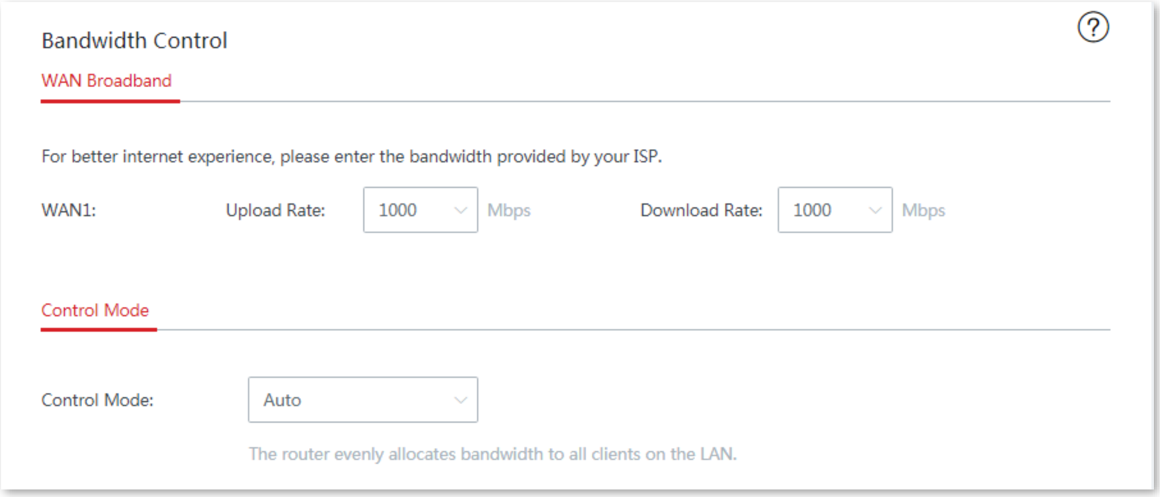
When **Imported successfully** appears, your address reservation configurations have been imported to your device.

3.8 Bandwidth control

3.8.1 Overview

The bandwidth control function allows you to assign proper bandwidth to connected clients, ensuring that the limited bandwidth is used to effectively access resources over the internet.

Choose **Bandwidth Control** to enter the page. See the following figure.



Bandwidth Control

WAN Broadband

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

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

Control Mode

Control Mode: Auto

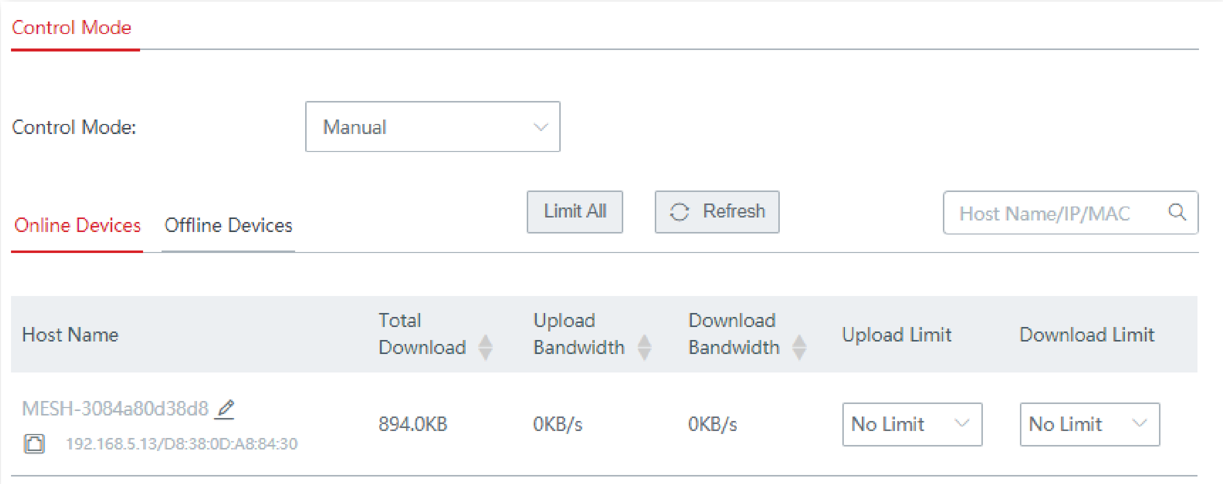
The router evenly allocates bandwidth to all clients on the LAN.

Parameter description

Parameter		Description
WAN Broadband	Upload Rate	Enter the bandwidth values of your internet service. If you are unsure about it, consult your ISP. This value will be used when the Control Mode is set to Auto.
	Download Rate	
Control Mode	No Limit	It indicates that there are no restrictions on upload/download rates for LAN users.
	Manual	It indicates that you can specify the maximum upload/download rate to each client manually, or to all clients in batch.
	Auto	It indicates that the system evenly allocates bandwidth to all clients on the LAN based on the values you entered in the WAN Broadband part.
	Limit By Group	It indicates that you can customize control rules based on IP groups and time groups.

3.8.2 Maunal

Set the **Control Mode** to **Manual**. See the following figure.



Control Mode

Control Mode: Manual

Host Name	Total Download	Upload Bandwidth	Download Bandwidth	Upload Limit	Download Limit
MESH-3084a80d38d8 192.168.5.13/D8:38:0D:A8:84:30	894.0KB	0KB/s	0KB/s	No Limit	No Limit

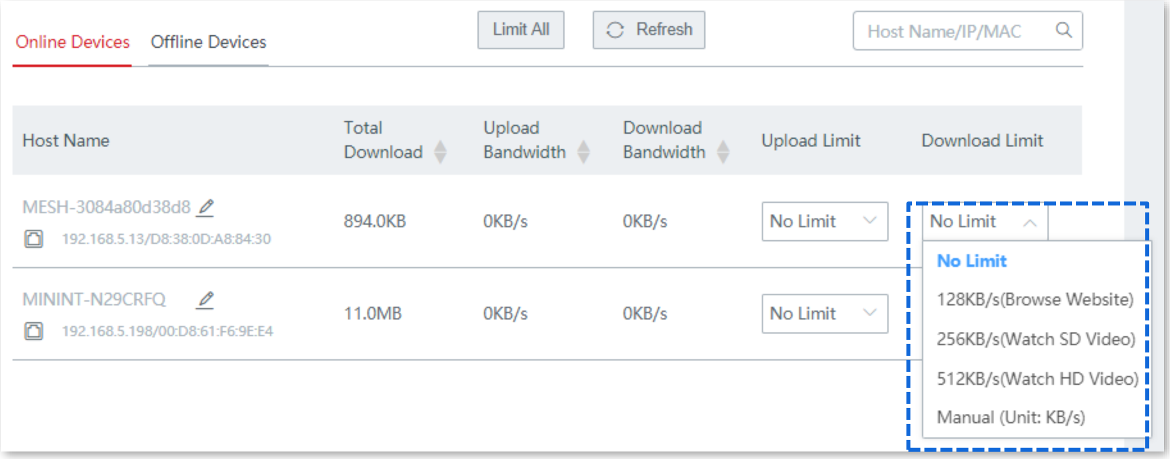
Parameter description

Parameter	Description
Host Name	It specifies the basic information about the user's device, including the device name reported by the device, how to connect to the cable-free network, IP address and MAC address. You can click ✎ to personalize the host name for convenient management. Tip For host name-based rules, such as using host name, the host name here will be used.
Total Download	It specifies the total download traffic utilized by each client.
Offline Time	It specifies the time when the client is disconnected. Only available for offline devices.
Upload Bandwidth	It specifies the real-time upload/download rate of each client. 1 Mbps=128 KB/s=1024 kb/s.
Download Bandwidth	
Upload Limit	It specifies the maximum upload/download rate you specified for each client.
Download Limit	

To control upload and download rate of online/offline devices separately

To limit the upload and/or download bandwidth of one or several devices, select a pre-defined value from the drop-down list menu of **Upload Limit** and/or **Download Limit**, or select **Manual**

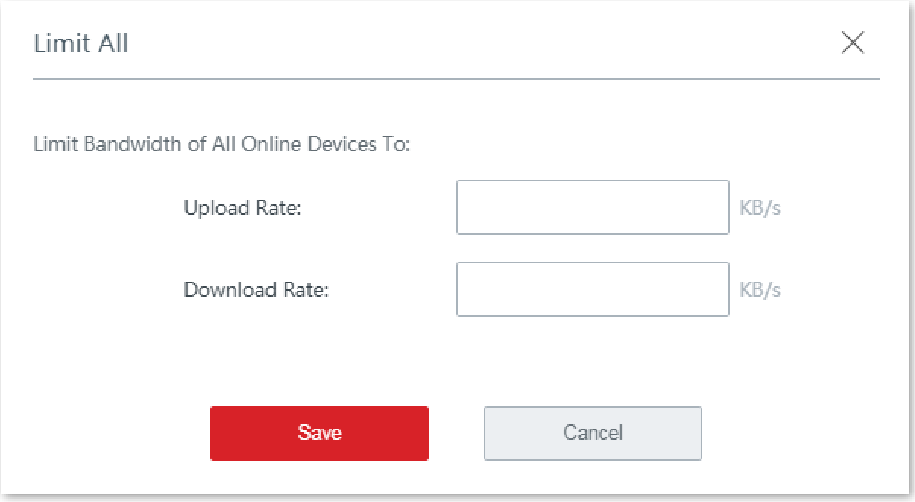
（Unit: KB/s） to specify a value manually.



Host Name	Total Download	Upload Bandwidth	Download Bandwidth	Upload Limit	Download Limit
MESH-3084a80d38d8 192.168.5.13/D8:38:0D:A8:84:30	894.0KB	0KB/s	0KB/s	No Limit	No Limit
MININT-N29CRFQ 192.168.5.198/00:D8:61:F6:9E:E4	11.0MB	0KB/s	0KB/s	No Limit	

To control upload and download rate of online/offline devices in batch

Click **Limit All**, specify the maximum upload/download rate for both Online Devices and Offline Devices on the configuration window, and click **Save** to apply your settings.



Limit Bandwidth of All Online Devices To:

Upload Rate: KB/s

Download Rate: KB/s

3.8.3 Limit by group

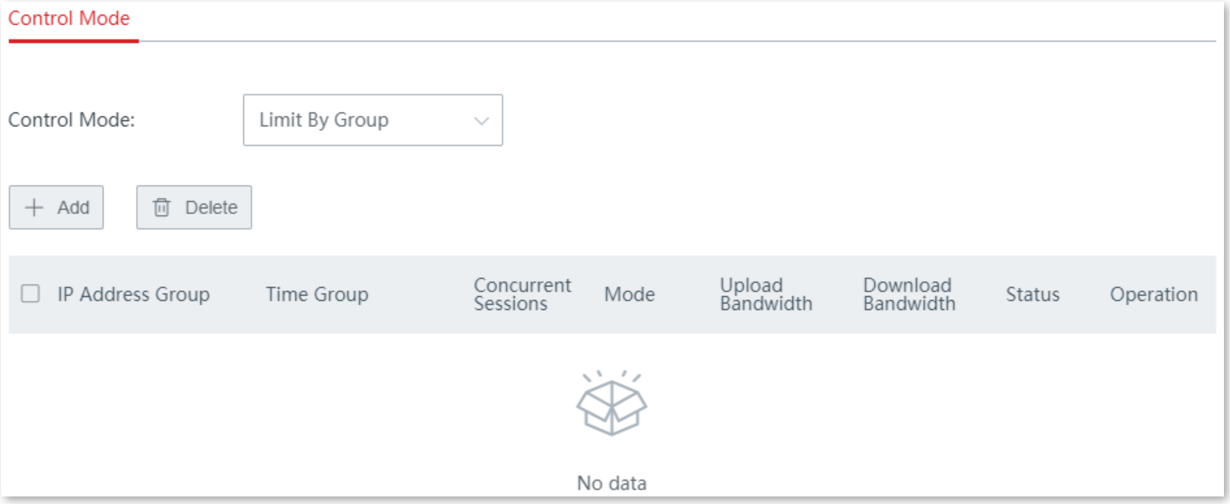
This function allows users within the IP group to share or have exclusive access to the upload/download rate which is set in a period of time.

Configuration procedure

Tip

To control bandwidth based on groups, you need to configure IP group and time group first. Refer to IP group/time group for detailed description.

1. Click **Bandwidth Control**, and move to the **Control Mode** configuration area.
2. Set **Control Mode** to **Limit By Group**, the following configuration area appears.



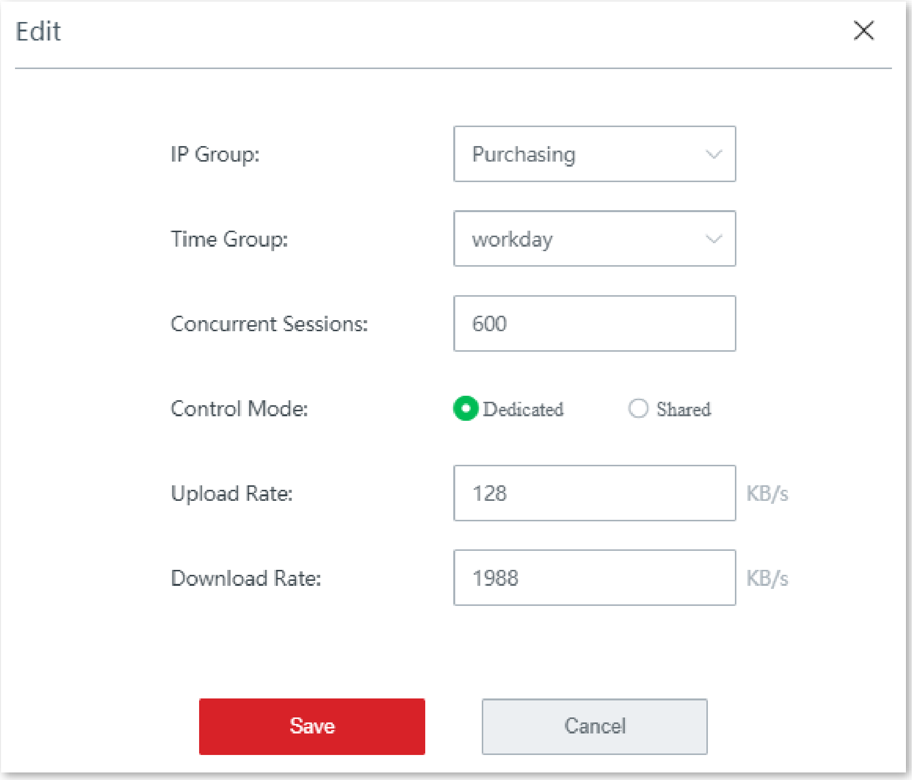
Control Mode

Control Mode: Limit By Group

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

No data

3. Click **Save** at the bottom of the page.
4. Click **+Add** to add a bandwidth control policy.
5. Set required parameters.



Edit

IP Group: Purchasing

Time Group: workday

Concurrent Sessions: 600

Control Mode: ● Dedicated ○ Shared

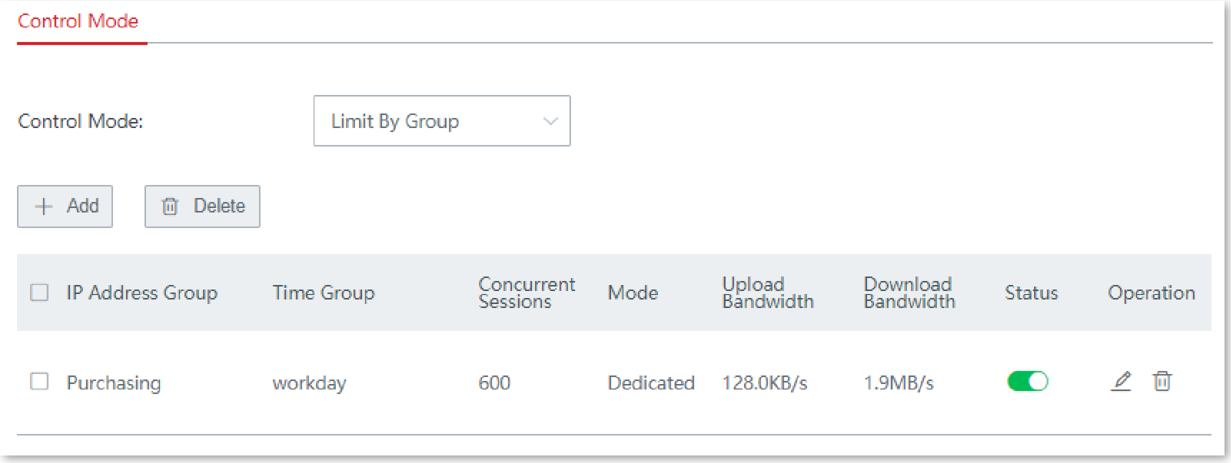
Upload Rate: 128 KB/s

Download Rate: 1988 KB/s

6. Click **Save**.

----End

The rule is added successfully. See the following figure.



Control Mode: Limit By Group

□ IP Address Group	Time Group	Concurrent Sessions	Mode	Upload Bandwidth	Download Bandwidth	Status	Operation
□ Purchasing	workday	600	Dedicated	128.0KB/s	1.9MB/s	●	✎ 🗑

Parameter description

Parameter	Description
IP Group (IP Address Group)	It specifies the IP group used by the rule to which the rule applies. This IP group should be configured on the **Filter Management** > **IP Group/Time Group** page first.
Time Group	It specifies the time group used by the rule on which the rule takes effect. This Time group should be configured on the **Filter Management** > **IP Group/Time Group** page first.
Concurrent Sessions	It specifies the maximum number of connections each controlled client can use. 600 is recommended.
Control Mode (Mode)	It specifies the control mode of the rule. – **Dedicated**: Specify the maximum upload/download rate for each client with the controlled IP address. – **Shared**: Specify the maximum upload/download rate for all clients with the controlled IP addresses. Each client may obtain different bandwidth.
Upload Rate (Upload Bandwidth)	It is used to control the upload/download rate.
Download Rate (Download Bandwidth)	
Status	It specifies the status of the rule. You can enable or disable it as required.
Operation	You can perform the following operations to the corresponding rule: ✎: Click it to edit the rule. 🗑: Click it to delete the rule.

3.8.4 Example of configuring group-based control rules

Networking requirement

An enterprise uses EW12 to set up a LAN to meet the following requirement:

During business hours (08:30 to 18:00 every workday), each computer with an IP address ranging from 192.168.5.14 to 192.168.5.100 is allocated to 1 Mbps (1 Mbps = 128 KB/s) upload and 1 Mbps download bandwidth. Assume that the number of concurrent connections per user device is 600. See the following table:

Group name	IP range	Effective time	Upload bandwidth	Download bandwidth
IP_Group	192.168.5.14 - 192.168.5.100	08:30 - 18:00 on weekdays	1 Mbps	1 Mbps

Solution

You can use the **Limit By Group** bandwidth control function of the device to meet this requirement.

Configuration procedure

Set a time group

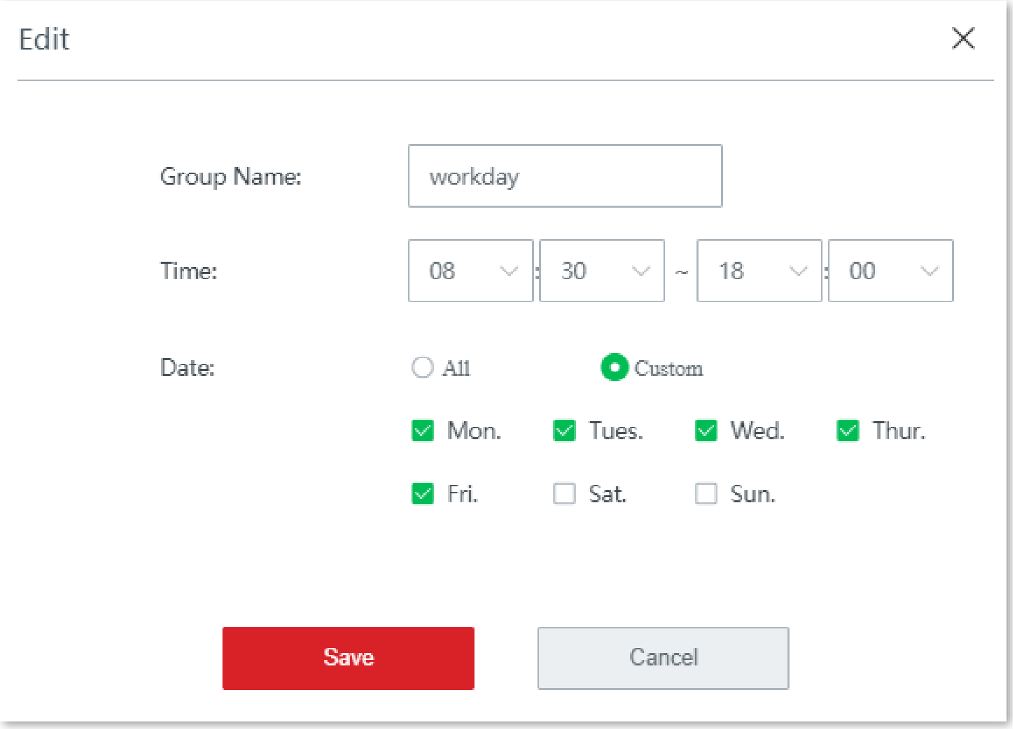
Set an IP address group

Set a bandwidth control rule

1. Set a time group.

   (1) Navigate to **Filter Management** > **IP Group/Time Group**.

   (2) Set the time group shown in the following figure.


Edit

Group Name: workday

Time: 08 : 30 ~ 18 : 00

Date: ○ All ● Custom

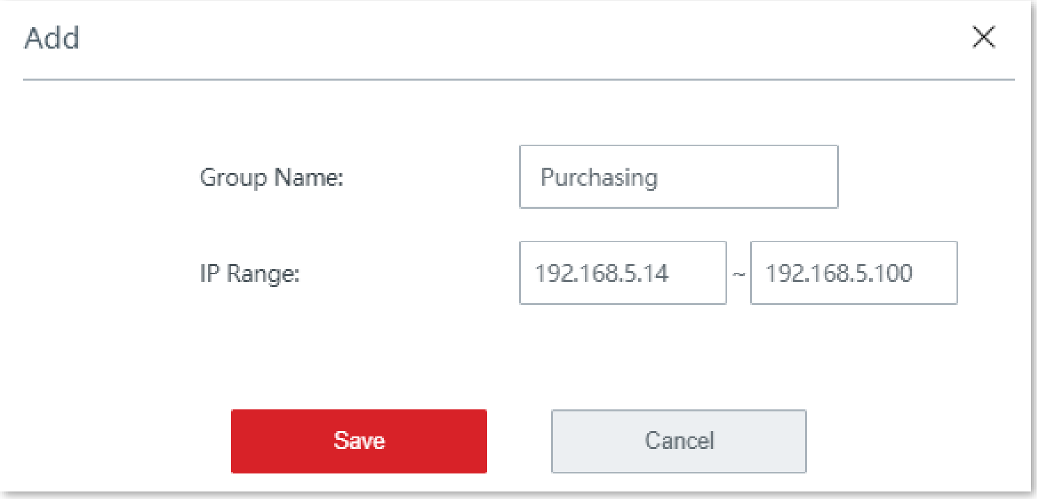
☑ Mon. ☑ Tues. ☑ Wed. ☑ Thur.

☑ Fri. □ Sat. □ Sun.

2. Set an IP address group.

   (1) Navigate to **Filter Management** > **IP Group/Time Group**.

   (2) Set the IP address group shown in the following figure.


Add

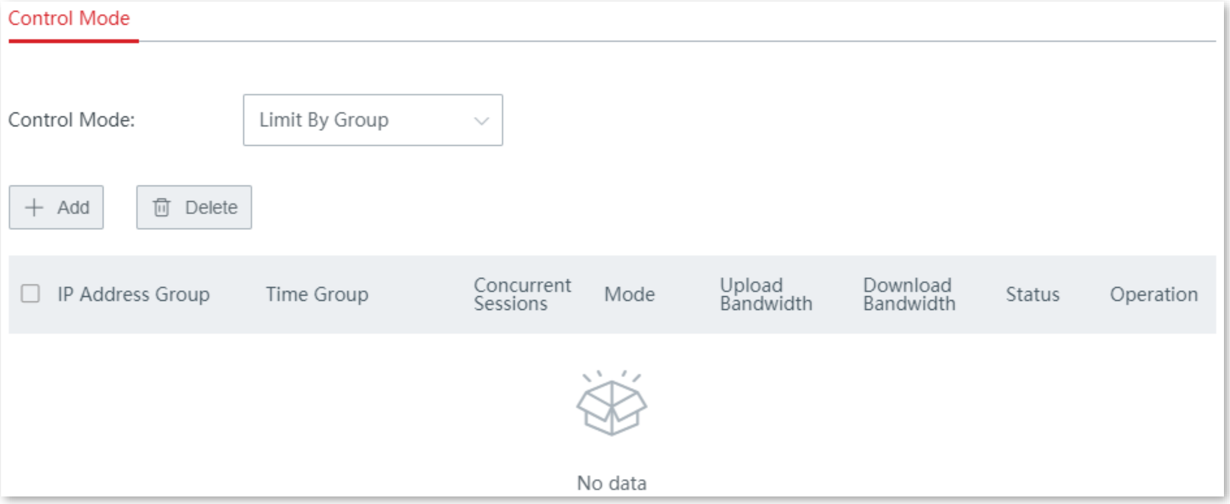
Group Name: Purchasing

IP Range: 192.168.5.14 ~ 192.168.5.100

3. Set a bandwidth control rule.

   (1) On the **Bandwidth Control** page, set **Control Mode** to **Limit By Group**.

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



Control Mode: Limit By Group

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

(3) Click **+Add**. The **Add** configuration window appears.

(4) Configure the following parameters:

IP Group: Click the drop-down list to select the IP group that the rule applies to, which is **Purchasing** in this example.

Time Group: Click the drop-down list to select the time group in which the rule will be applied, which is **workday** in this example.

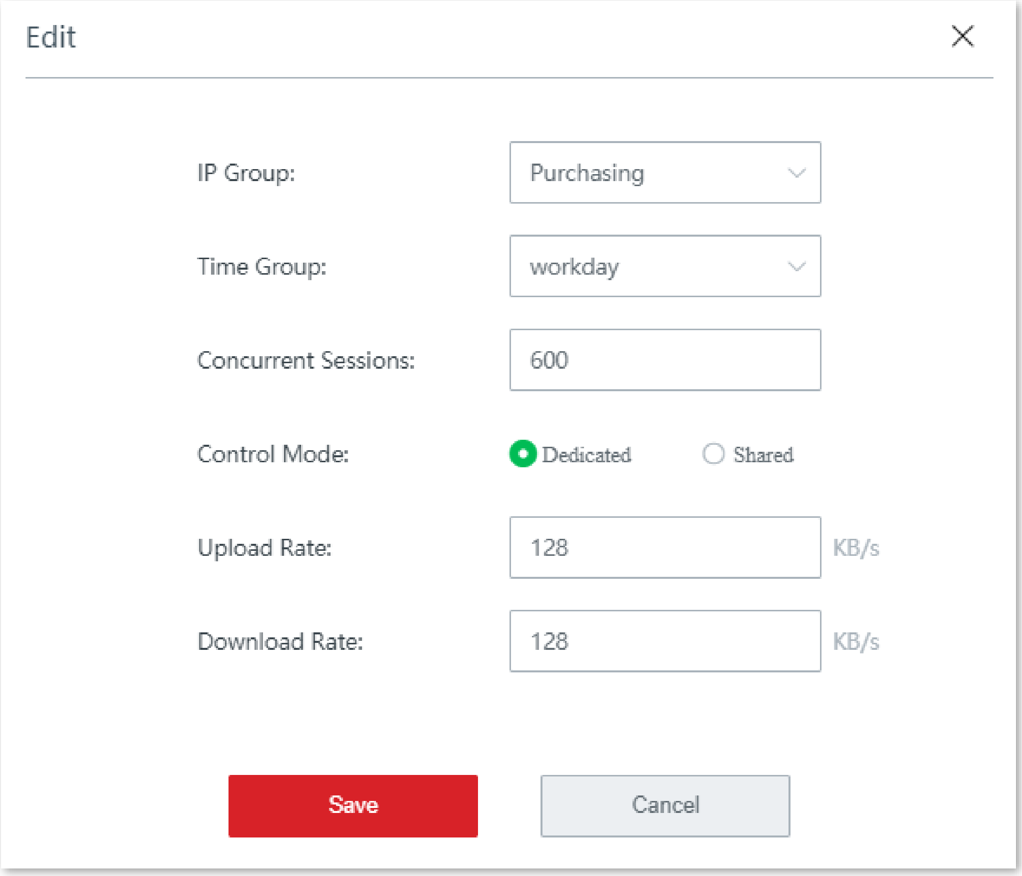
Concurrent Sessions: Set the number of concurrent connections to a single client, which is **600** in this example.

Control Mode: Select **Dedicated**.

Upload Rate: Set the maximum upload rate for the client, which is **128KB/s** in this example.

Download Rate: Set the maximum download rate for the client, which is **128KB/s** in this example.

(5) Click **Save**.



Edit

IP Group: Purchasing

Time Group: workday

Concurrent Sessions: 600

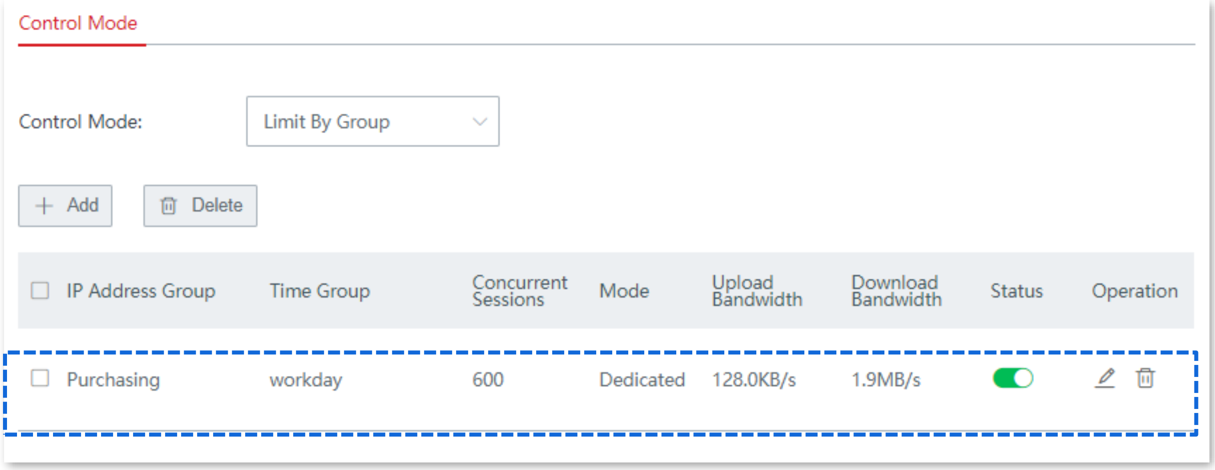
Control Mode: ● Dedicated ○ Shared

Upload Rate: 128 KB/s

Download Rate: 128 KB/s

----End

The rule is added successfully. See the following figure.



Control Mode

Control Mode: Limit By Group

□	IP Address Group	Time Group	Concurrent Sessions	Mode	Upload Bandwidth	Download Bandwidth	Status	Operation
□	Purchasing	workday	600	Dedicated	128.0KB/s	1.9MB/s	●	

Verification

During business hours from 08:30 to 18:00 every weekday, each computer with an IP address ranging from 192.168.5.2 to 192.168.5.100 is allocated 1 Mbps (128 KB/s) uploading and downloading bandwidth, while the bandwidth allocated to the computers with an IP address ranging from 192.168.5.101 to 192.168.5.254 is not limited.

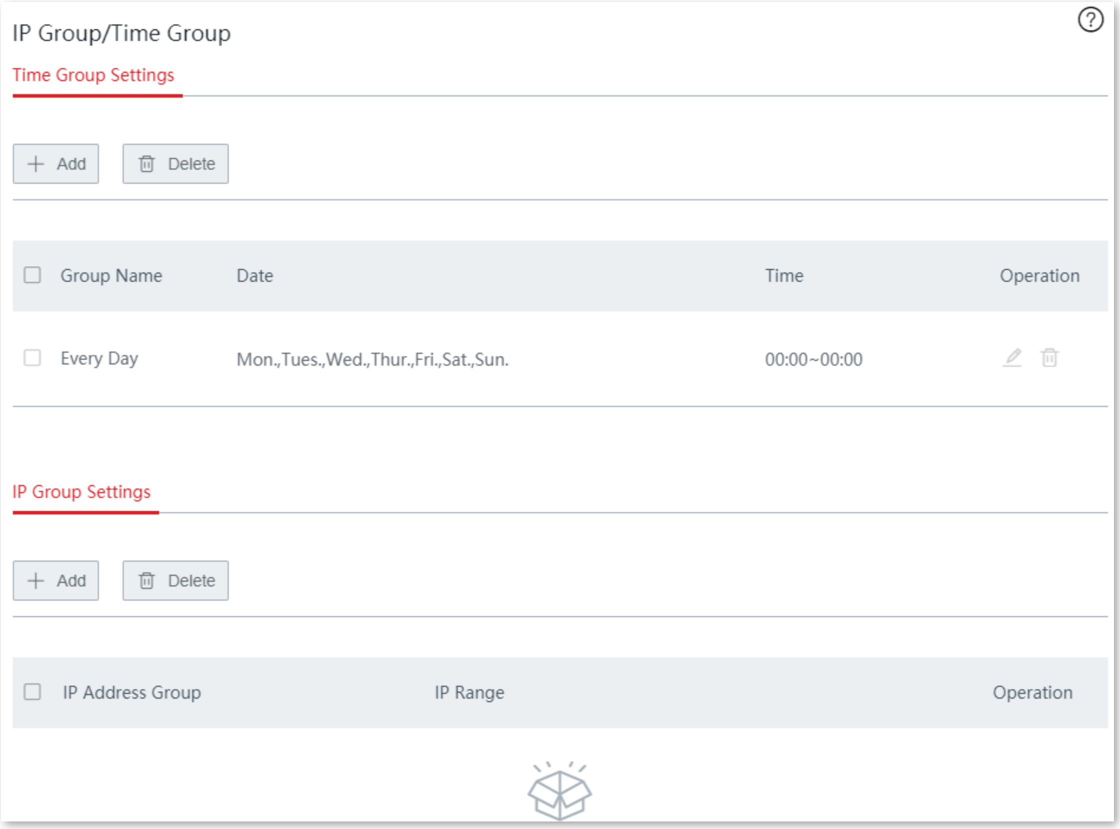
3.9 Filter management

This function allows you to configure MAC address-based, IP address-based, and URL-based filter rules to control what clients can or cannot access what websites.

3.9.1 IP group/time group

Some functions, such as MAC address filter, IP address filter, URL filter, Limit by group in bandwidth control and Custom multi-WAN policy, need to take effect based on IP group or time group. Therefore, before configure these functions, you need to add IP groups or time groups first.

To access the page for setting IP address groups and time groups, navigate to **Filter Management** > **IP Group/Time Group**. See the following figure.



IP Group/Time Group

Time Group Settings

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

IP Group Settings

□	IP Address Group	IP Range	Operation

Add time groups

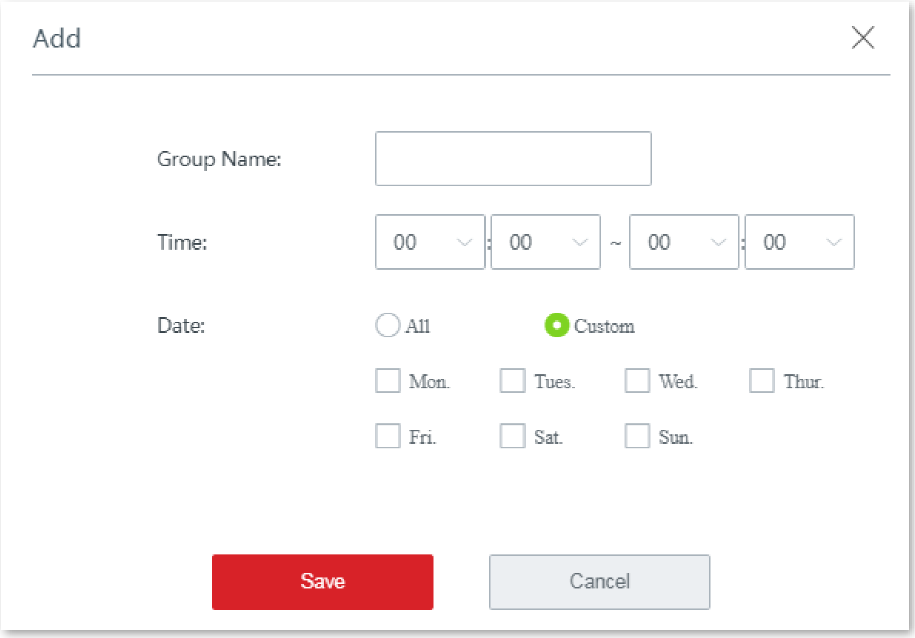
Tip

- By default, there is a time rule named **Every Day** which cannot be edited or deleted.
- A time group that has been referenced cannot be deleted.

1. Navigate to **Filter Management** > **IP Group/Time Group**, and locate the Time Group Settings configuration area.

2. Click **Add**. The **Add** configuration window appears.

3. Set the required parameters.



Add

Group Name:

Time: 00 : 00 ~ 00 : 00

Date: ○ All ● Custom

□ Mon. □ Tues. □ Wed. □ Thur.

□ Fri. □ Sat. □ Sun.

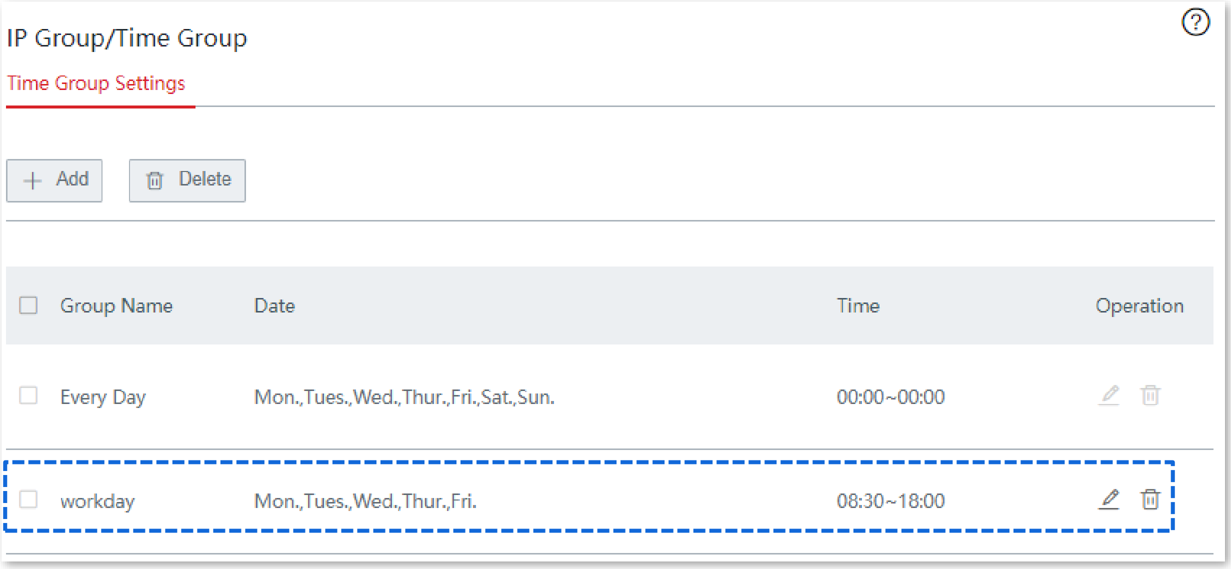
Tip

- Duplicate group names are disallowed.
- 00:00~00:00 indicates a whole day.

4. Click **Save**.

----End

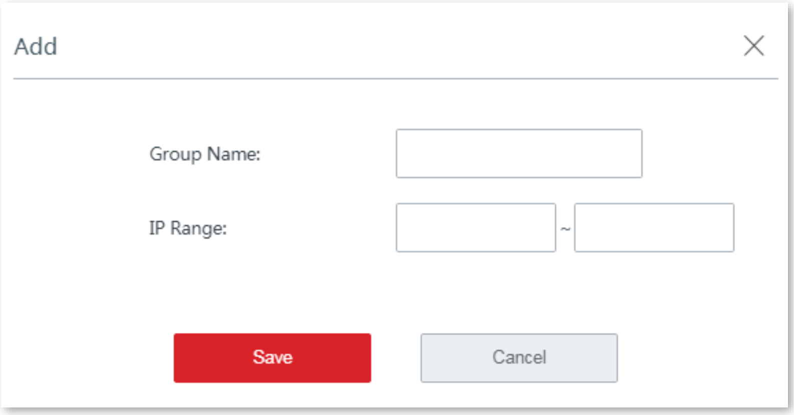
The rule is added successfully. See the following figure.



☐	Group Name	Date	Time	Operation
☐	Every Day	Mon.,Tues.,Wed.,Thur.,Fri.,Sat.,Sun.	00:00~00:00	
☐	workday	Mon.,Tues.,Wed.,Thur.,Fri.	08:30~18:00	

Add IP groups

1. Navigate to **Filter Management** > **IP Group/Time Group**, and locate the IP Group Settings configuration area.
2. Click **Add**. The **Add** configuration window appears.
3. Set the required parameters.



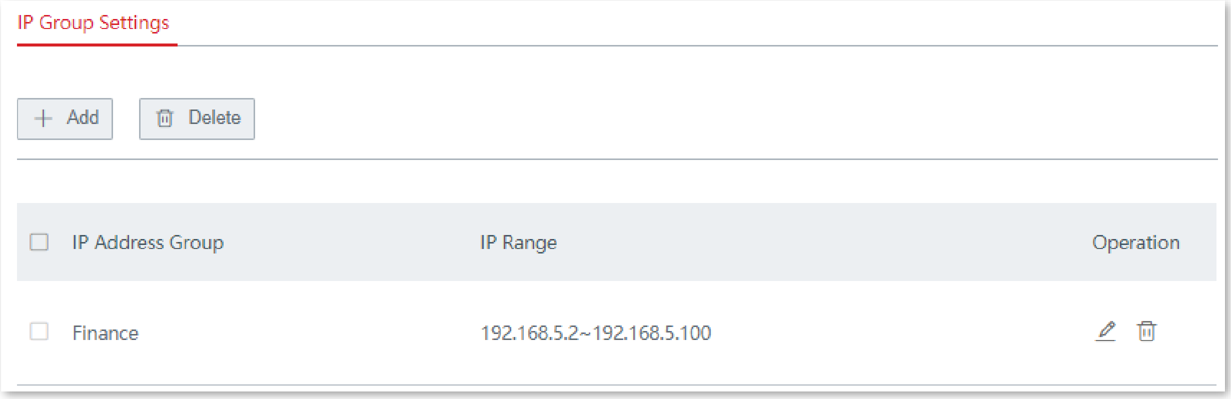
Tip

Duplicate group names are disallowed.

4. Click **Save**.

----End

The rule is added successfully. See the following figure.


IP Group Settings

□ IP Address Group	IP Range	Operation
□ Finance	192.168.5.2~192.168.5.100	

Tip

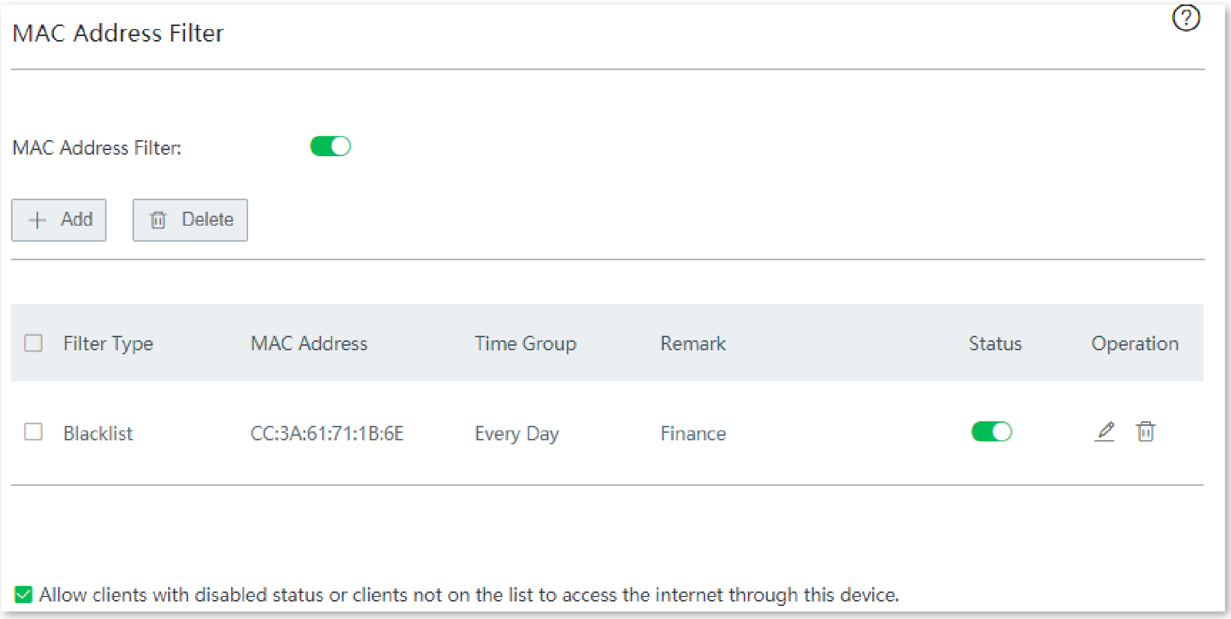
An IP address group that has been referenced cannot be deleted.

3.9.2 MAC address filter

Overview

You can create MAC address-based rules to decide whether clients can access the internet through the node on specific time. Both **Blacklist** (Forbid access to the internet) and **Whitelist** (Allow access to the internet) based on MAC addresses are supported.

Navigate to **Filter Management** > **MAC Address Filter** to enter the page. By default, this function is disabled.


MAC Address Filter

MAC Address Filter: ●

□ Filter Type	MAC Address	Time Group	Remark	Status	Operation
□ Blacklist	CC:3A:61:71:1B:6E	Every Day	Finance	●	

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

Parameter description

Parameter	Description
MAC Address Filter	It specifies whether to enable this function.
Filter Type	It specifies MAC address filter types. – **Whitelist**: Clients with this filter type will be added in the Whitelist, indicating that they can only access the internet during the specified period. – **Blacklist**: Clients with this filter type will be added in the Blacklist, indicating that they cannot access the internet during the specified period.
MAC Address	It specifies the MAC addresses corresponding to the devices.
Time Group	It is used to select a time group for the rule. It can be configured on the **Filter Management** > **IP Group/Time Group** page.
Remark	(Optional) Specify a brief description for the rule.
Status	It specifies the status of the rule. You can enable/disable it as required.
Operation	It is used to perform the following operations: Click ✎ to change the rule. Click 🗑 delete the rule.
Allow clients with disabled status or clients not on the list to access the internet through this device.	If this option is selected, devices of the entries which are disabled and devices which are not in the list are allowed to access the internet. If this option is not selected, devices of the entries which are disabled and devices which are not in the list are disallowed to access the internet.

Create a MAC address rule

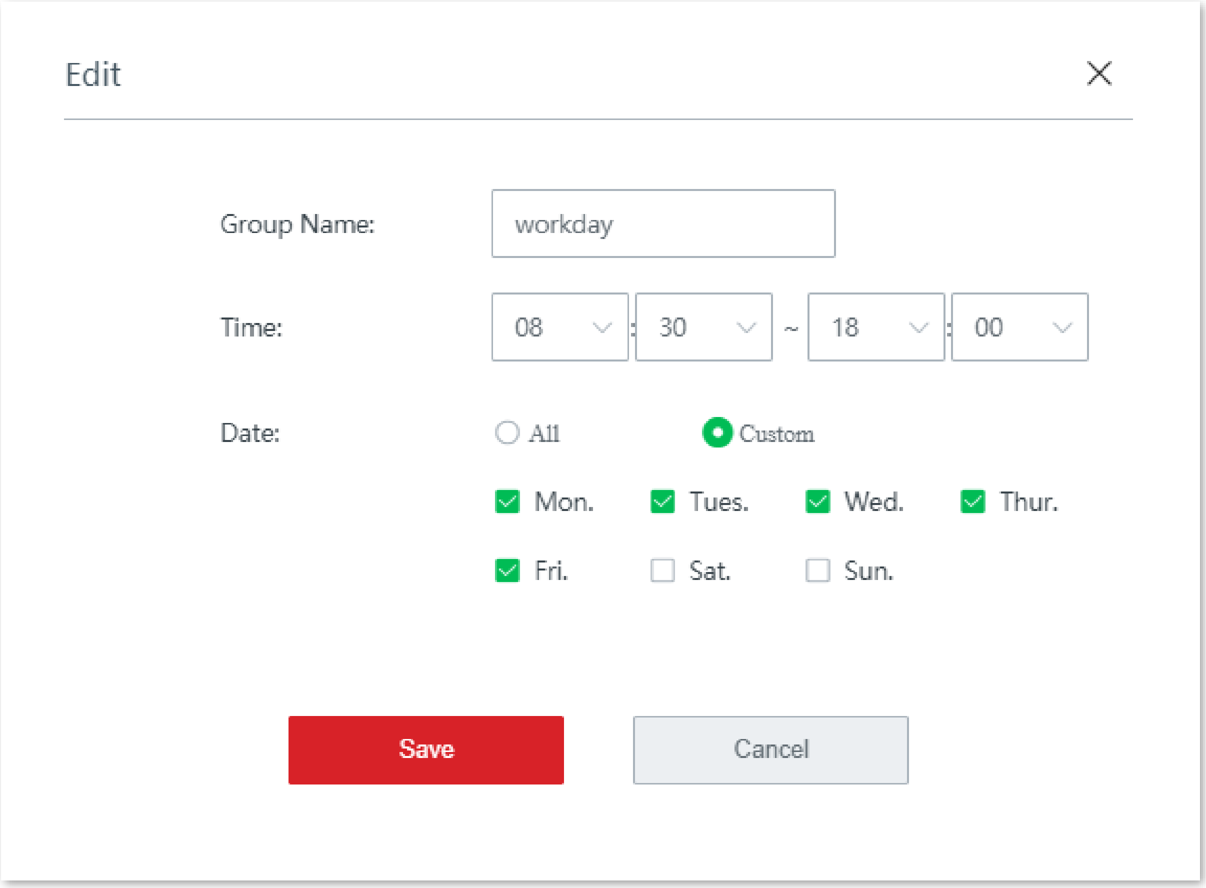
Add a time group

Create a MAC address rule

1. Add a time group.

   (1) Navigate to **Filter Management** > **IP Group/Time Group**.

   (2) Click **+Add** on the **Time Group Settings** part, and add a time group.



Edit

Group Name: workday

Time: 08 : 30 ~ 18 : 00

Date: ○ All ● Custom

☑ Mon. ☑ Tues. ☑ Wed. ☑ Thur.

☑ Fri. □ Sat. □ Sun.

2. Create a MAC address filter rule.

   (1) Navigate to **Filter Management** > **MAC Address Filter**, enable the function and click **Save**.

   (2) Click **+Add**. The configuration window appears.

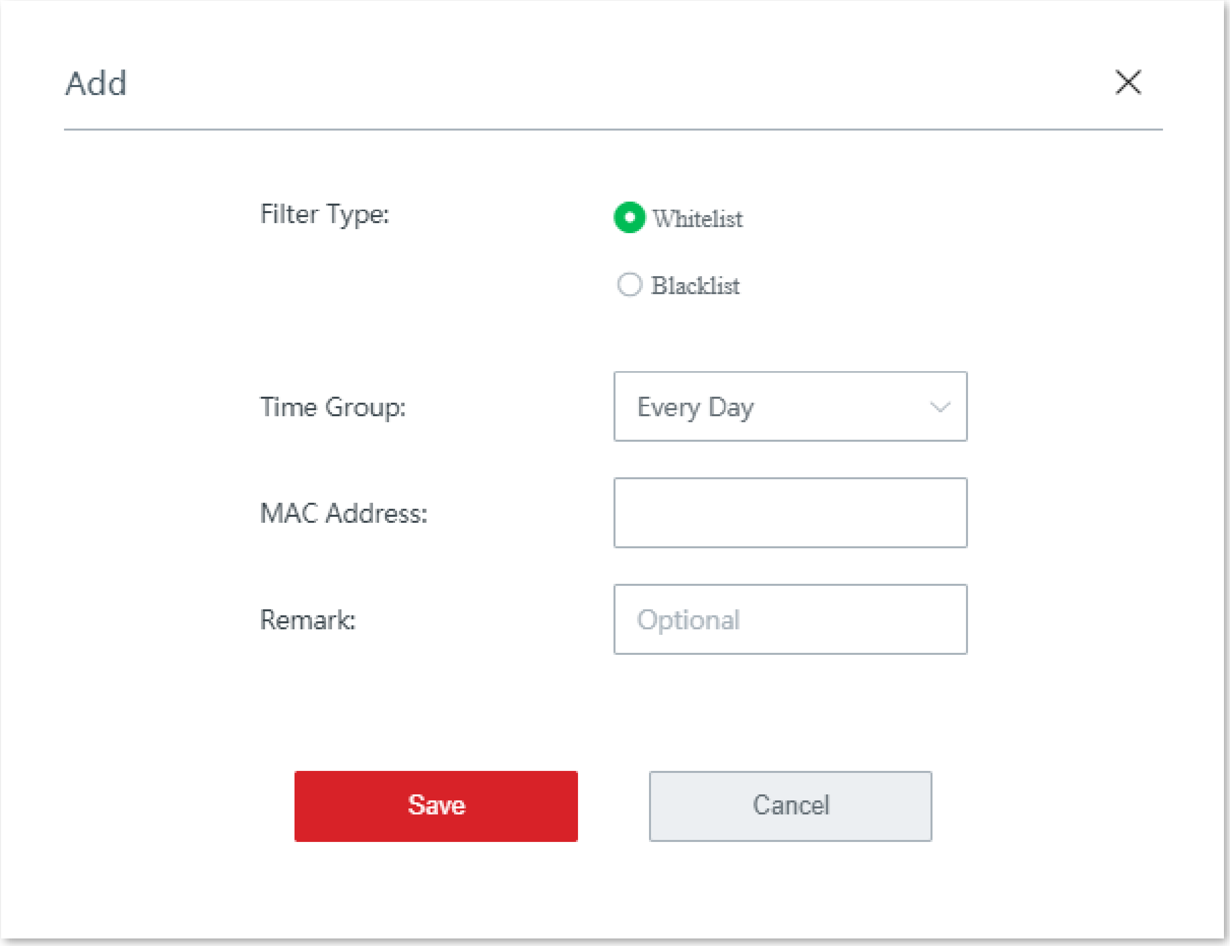
   (3) Select a filter type.

   (4) Select the **Time Group** you added.

   (5) Enter the **MAC address** of a device to which this rule applies.

   (6) (Optional) Specify a description for the rule in the **Remark** input box.

   (7) Click **Save**.



Add

Filter Type: ● Whitelist ○ Blacklist

Time Group: Every Day

MAC Address:

Remark: Optional

----End

Example of adding MAC address filter rule(s)

Network requirement

An enterprise uses EW12 to set up a LAN to meet the following requirement:

During business hours (08:30 to 18:00 on workday), only one purchasing department staff is allowed to access the internet. Assume that the MAC address of the purchaser's computer is CC:3A:61:71:1B:6E.

Solutions

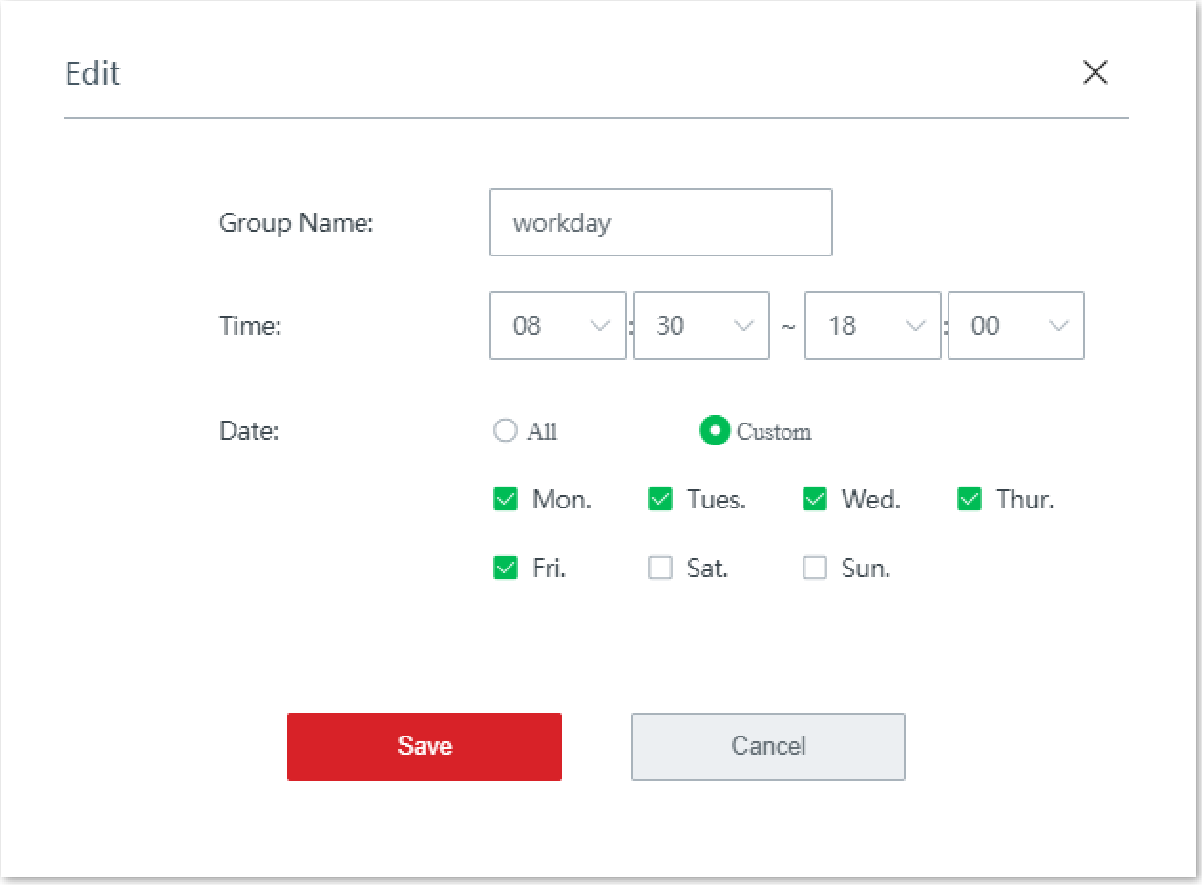
The MAC address filter can meet this requirement.

Configuration procedure

1. Add a time group.

(1) Navigate to **Filter Management** > **IP Group/Time Group**.

(2) Add a time group shown in the following figure.


Edit

Group Name: workday

Time: 08 : 30 ~ 18 : 00

Date: ○ All ● Custom

☑ Mon. ☑ Tues. ☑ Wed. ☑ Thur.

☑ Fri. □ Sat. □ Sun.

2. Create a MAC address filter rule.

   (1) Navigate to **Filter Management** > **MAC Address Filter**, enable the function and click **Save**.

   (2) Click **+Add**. The configuration window appears.

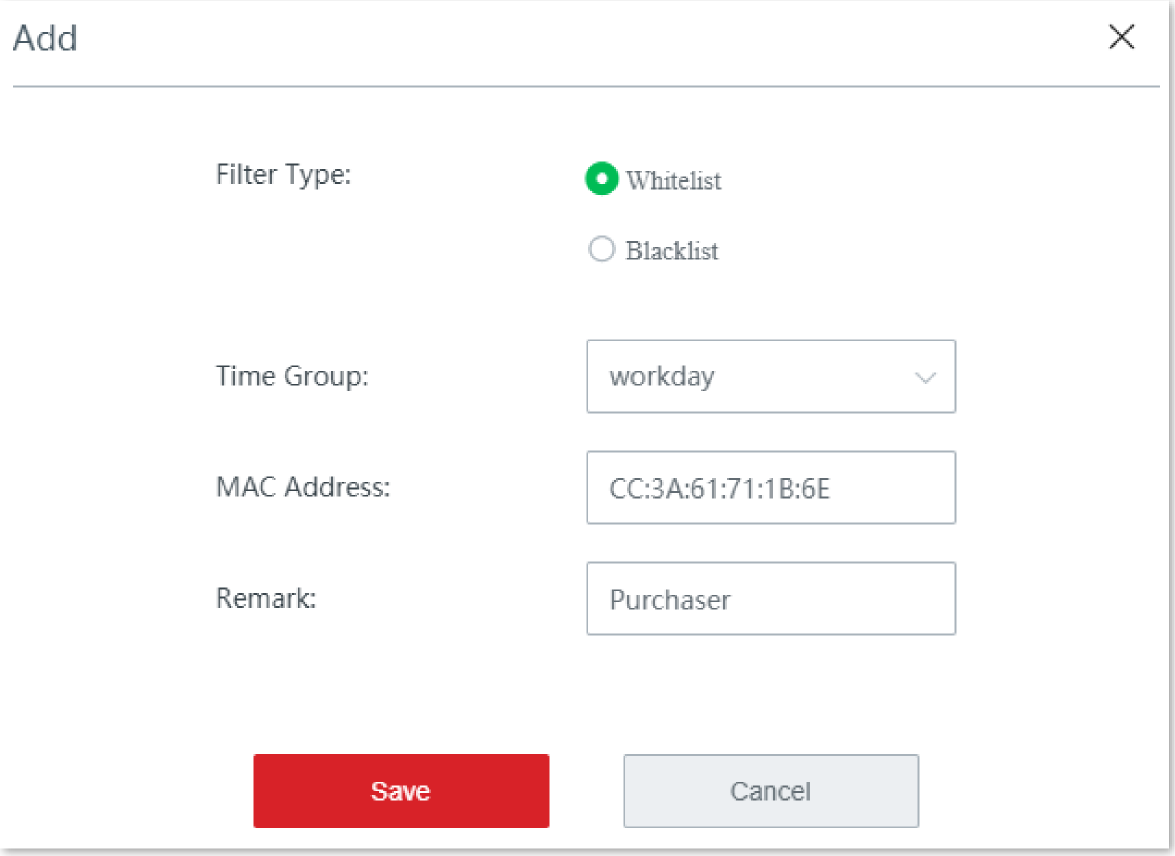
   (3) Select **Whitelist**.

   (4) Select **workday** from the **Time Group** drop-down list.

   (5) Enter **CC:3A:61:71:1B:6E** in the **MAC Address** input box.

   (6) Enter **Purchaser** in the **Remark** input box.

   (7) Click **Save**.



Add

Filter Type: ● Whitelist ○ Blacklist

Time Group: workday

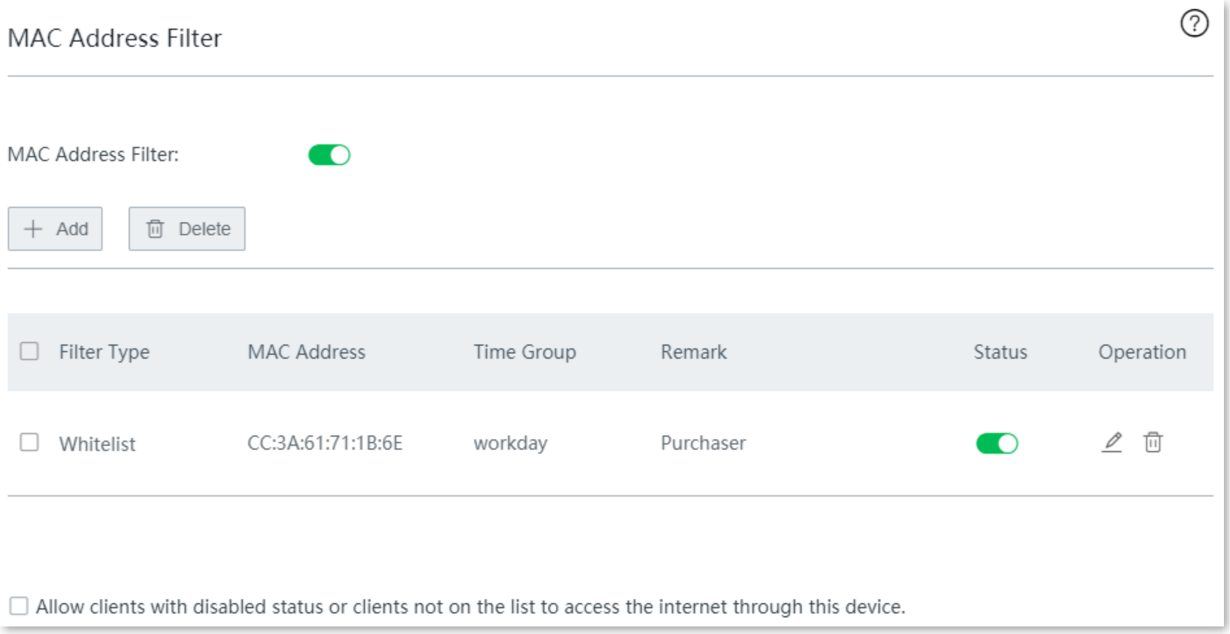
MAC Address: CC:3A:61:71:1B:6E

Remark: Purchaser

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

----End

The rule is added successfully. See the following figure.



MAC Address Filter

MAC Address Filter: enabled

□	Filter Type	MAC Address	Time Group	Remark	Status	Operation
□	Whitelist	CC:3A:61:71:1B:6E	workday	Purchaser	enabled	

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

Verification

During 08:30 to 18:00 on workdays, only the computer's MAC address is CC:3A:61:71:1B:6E can access the internet.

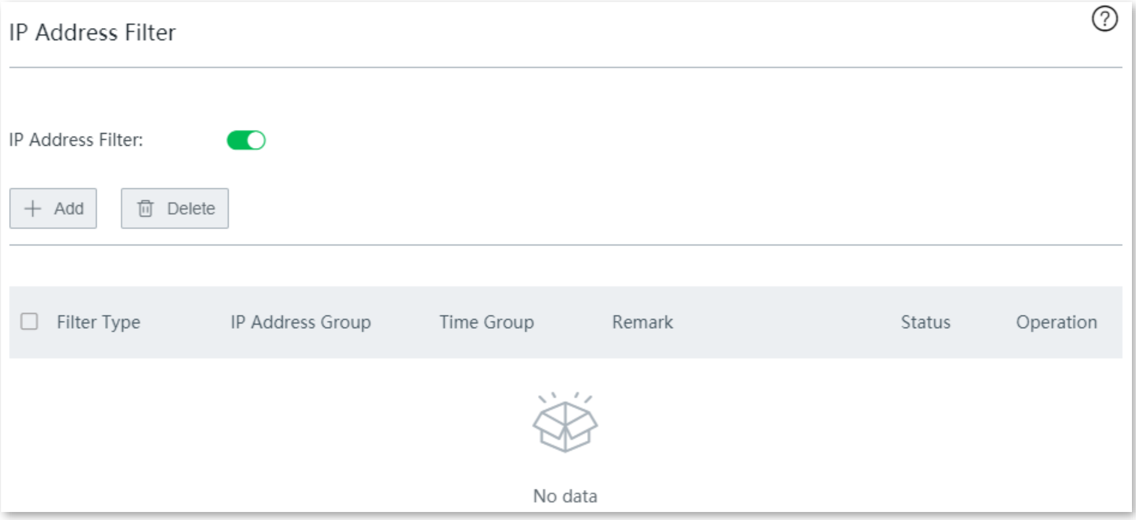
3.9.3 IP address filter

Overview

You can create IP address-based rules to decide whether clients can access the internet through the node on what time. Both Blacklist (Forbid access to the internet) and Whitelist (Allow access to the internet) based on IP addresses are supported.

The IP address filter function takes effect on basis of the IP addresses. To make this function work properly, you are recommended to reserve static IP addresses to the clients to be filtered. Refer to Address reservation for detailed procedures.

Navigate to **Filter Management** > **IP Address Filter** to enter the page. By default, this function is disabled.

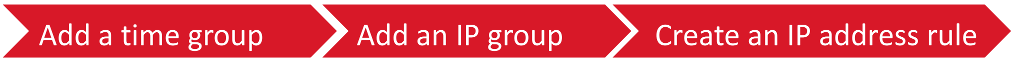


Parameter description

Parameter	Description
MAC Address Filter	It specifies whether or not to enable the IP Address Filter function.
Filter Type	It specifies IP address filter types. – **Whitelist**: Clients with this filter type will be added into the **Whitelist**, indicating that users with specified IP addresses can only access the internet during the specified period. – **Blacklist**: Clients with this filter type will be added into the **Blacklist**, indicating that users with specifies IP addresses cannot access the internet during the specified period.

Parameter	Description
IP Address	It specifies the IP addresses corresponding to the devices.
Time Group	It is used to select a time group for the rule. It should be configured on the **Filter Management** > **IP Group/Time Group** page.
IP Group	It is used to select a time group for the rule. It should be configured on the **Filter Management** > **IP Group/Time Group** page.
Remark	(Optional) It specifies a brief description for the rule.
Status	It specifies the status of the rule. You can enable/disable it as required.
Operation	It is used to perform the following operations: Click ✎ to change the rule. Click 🗑 delete the rule.
Allow clients with disabled status or clients not on the list to access the internet through this device.	If this option is selected, devices of the entries which are disabled and devices which are not in the list are allowed to access the internet. If this option is not selected, devices of the entries which are disabled and devices which are not in the list are disallowed to access the internet.

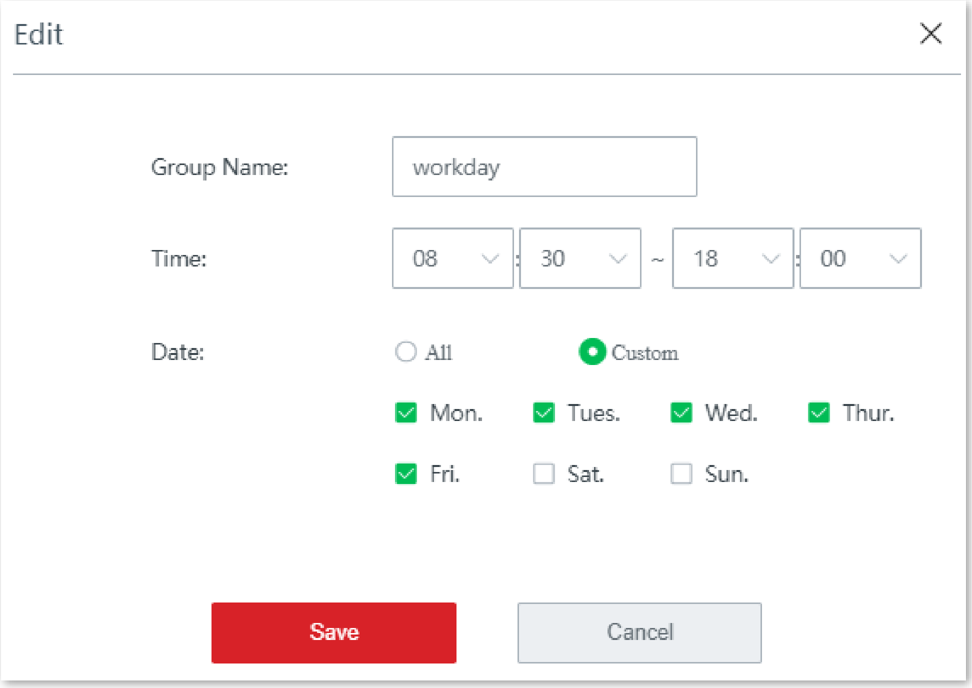
Create an IP address filter rule



1. Add a time group.

   (1) Navigate to **Filter Management** > **IP Group/Time Group**.

   (2) Click **+Add** on the **Time Group Settings** part, and add a time group.



Edit

Group Name: workday

Time: 08 : 30 ~ 18 : 00

Date: ○ All ● Custom

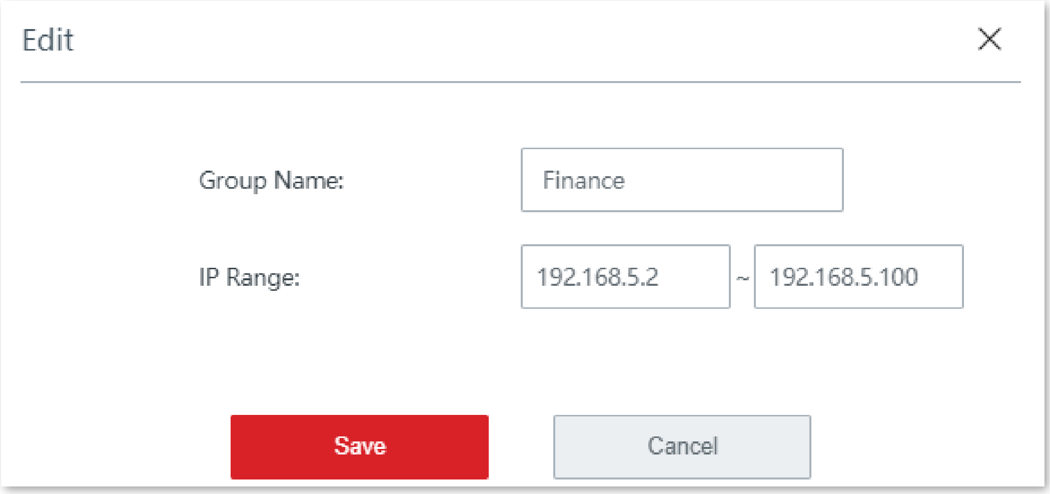
☑ Mon. ☑ Tues. ☑ Wed. ☑ Thur.

☑ Fri. □ Sat. □ Sun.

2. Set an IP group.

   (1) Navigate to **Filter Management** > **IP Group/Time Group**.

   (2) Click **+Add** on the **IP Group Settings** part, and add an IP group.



Edit

Group Name: Finance

IP Range: 192.168.5.2 ~ 192.168.5.100

3. Create an IP address filter rule.

   (1) Navigate to **Filter Management** > **IP Address Filter**, enable the function and click **Save**.

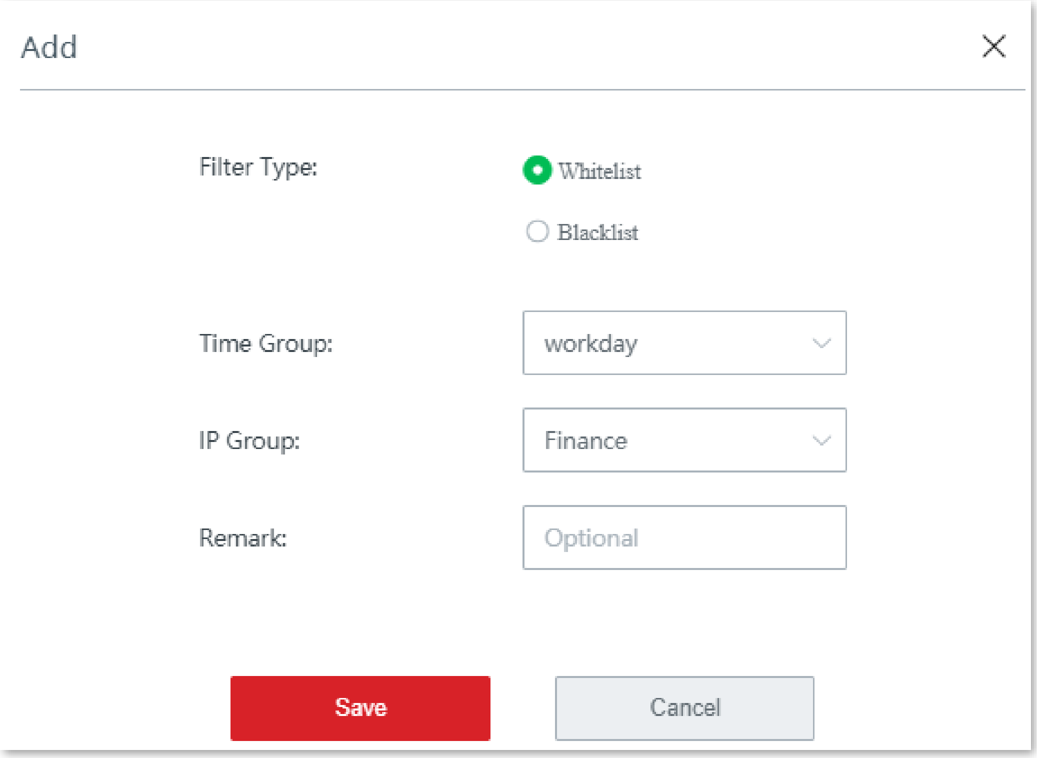
   (2) Click **+Add**. The configuration window appears.

   (3) Select a Filter Type.

   (4) Select the **Time Group** you add.

   (5) Select the **IP Group** you add.

   (6) (Optional) Specify a description for the rule in the **Remark** input box.



Add

Filter Type: ● Whitelist ○ Blacklist

Time Group: workday

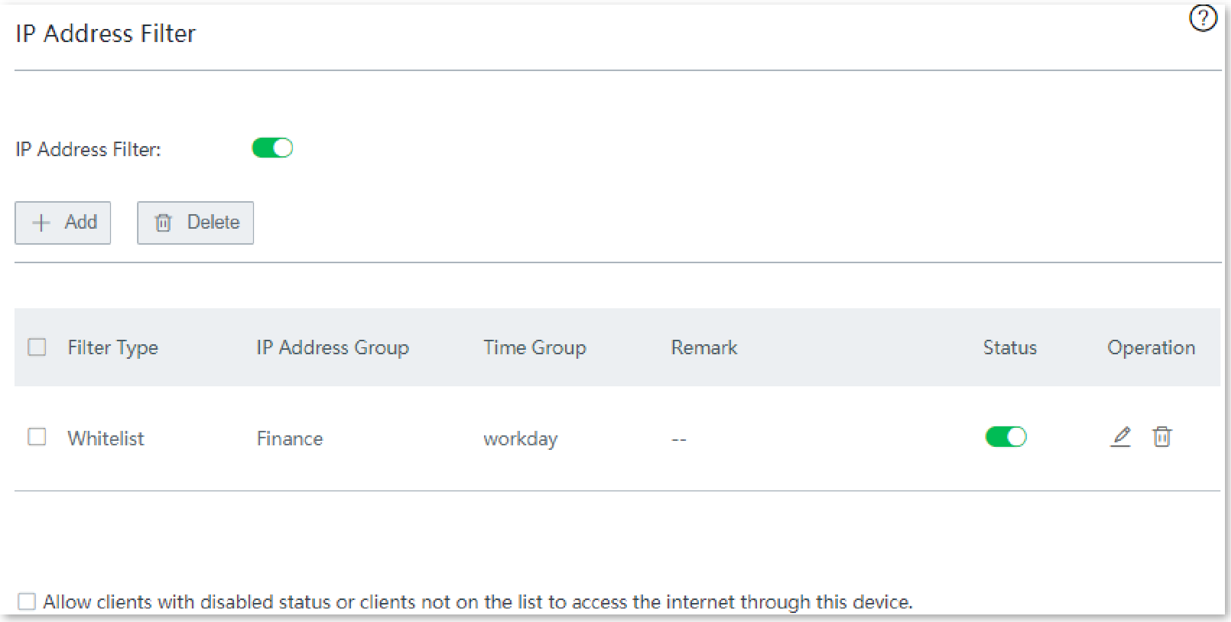
IP Group: Finance

Remark: Optional

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

----End

The rule is added successfully. See the following figure.



IP Address Filter

IP Address Filter: ●

□	Filter Type	IP Address Group	Time Group	Remark	Status	Operation
□	Whitelist	Finance	workday	--	●	

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

Example of configuring IP address filter rule(s)

Network requirement

An enterprise uses EW12 to set up a LAN to meet the following requirement:

During business hours (08:30 to 18:00 on workday), the finance department is not allowed to access the internet. Assume that the IP addresses of the financial department's computer is from 192.168.5.2 to 192.168.5.100.

Solutions

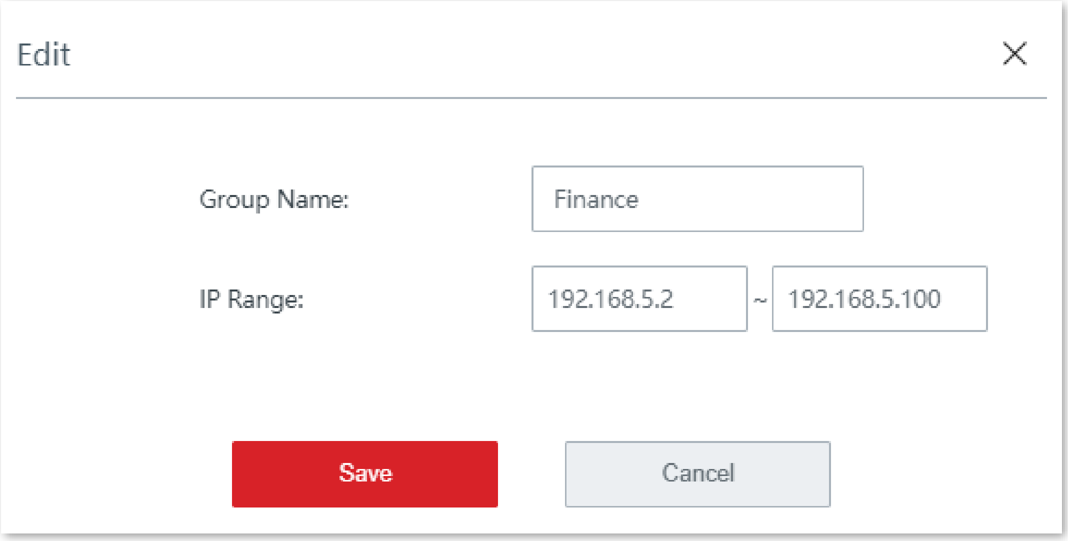
The IP address filter combining with address reservation can meet this requirement.

Configuration procedure

1. Reserve the IP addresses from 192.168.5.2 to 192.168.5.100 to the purchasing department's computers.

   (1) Click **Address Reservation**, and move to the **Manual Address Reservation** part.

   (2) Click **+Add**, and reserve the IP address to the purchasing department's computers.



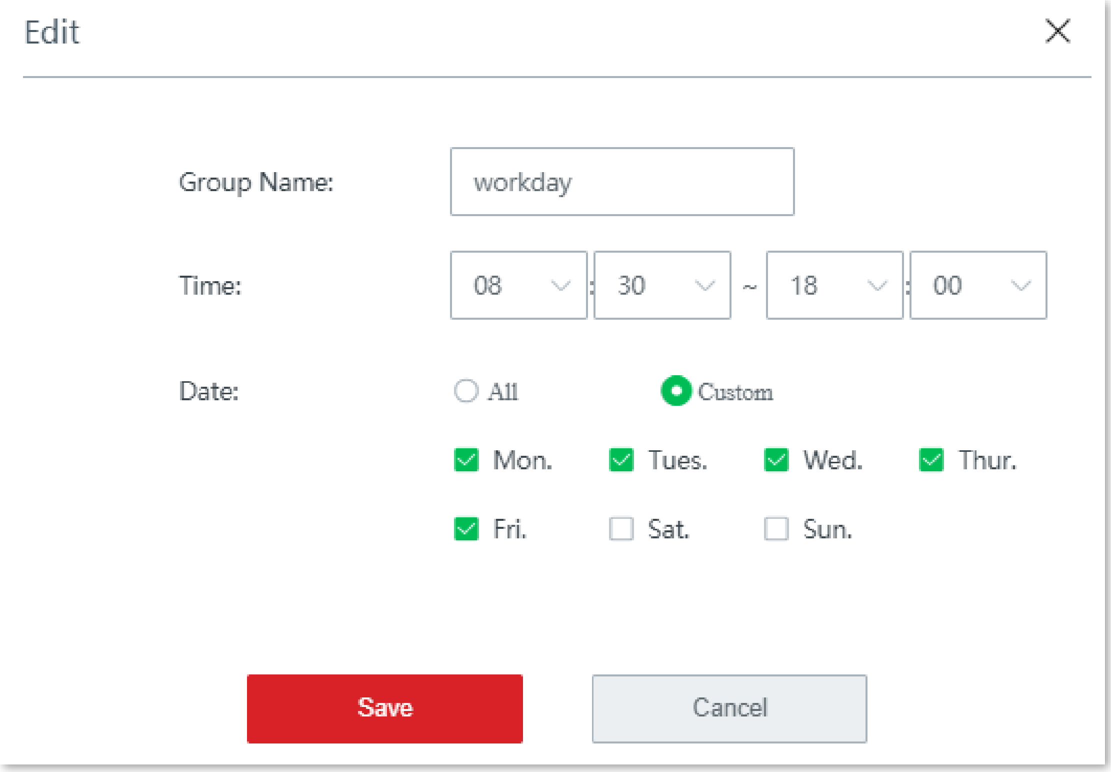
Group Name: Finance

IP Range: 192.168.5.2 ~ 192.168.5.100

2. Set up a time group.

   (1) Navigate to **Filter Management** > **IP Group/Time Group**.

   (2) Add a time group shown in the following figure.



Edit

Group Name: workday

Time: 08 : 30 ~ 18 : 00

Date: ○ All ● Custom

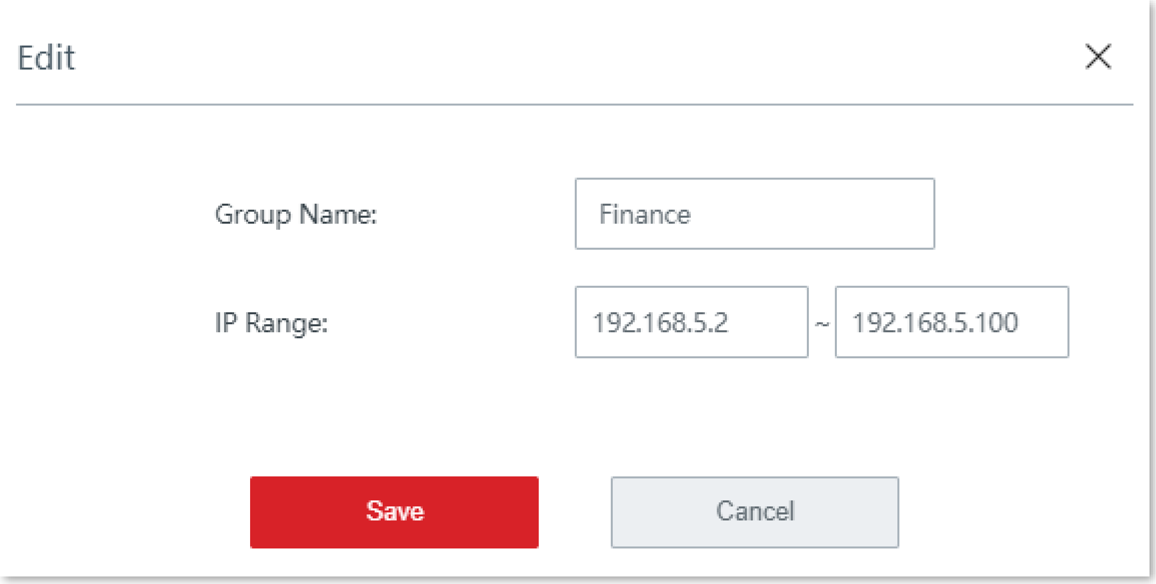
☑ Mon. ☑ Tues. ☑ Wed. ☑ Thur.

☑ Fri. □ Sat. □ Sun.

3. Add an IP group.

   (1) Navigate to **Filter Management** > **IP Group/Time Group**.

   (2) Add an IP group shown in the following figure.



Edit

Group Name: Finance

IP Range: 192.168.5.2 ~ 192.168.5.100

4. Create an IP address filter rule.

   (1) Navigate to **Filter Management** > **IP Address Filter**, enable the function and click **Save**.

   (2) Click **+Add**. The configuration window appears.

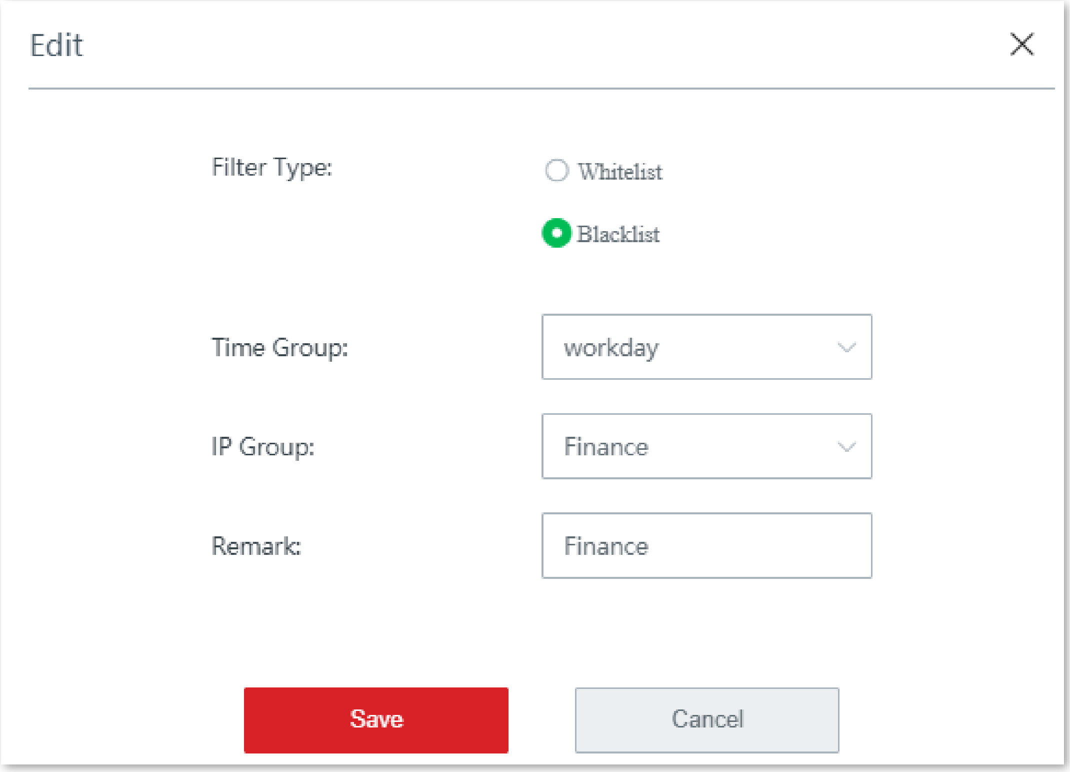
   (3) Select **Blacklist**.

(4) Select **workday** from the **Time Group** drop-down list.

(5) Select **Finance** from the **IP Group** drop-down list.

(6) Enter **Finance** in the **Remark** input box.

(7) Click **Save**.



Edit

Filter Type: ○ Whitelist ● Blacklist

Time Group: workday

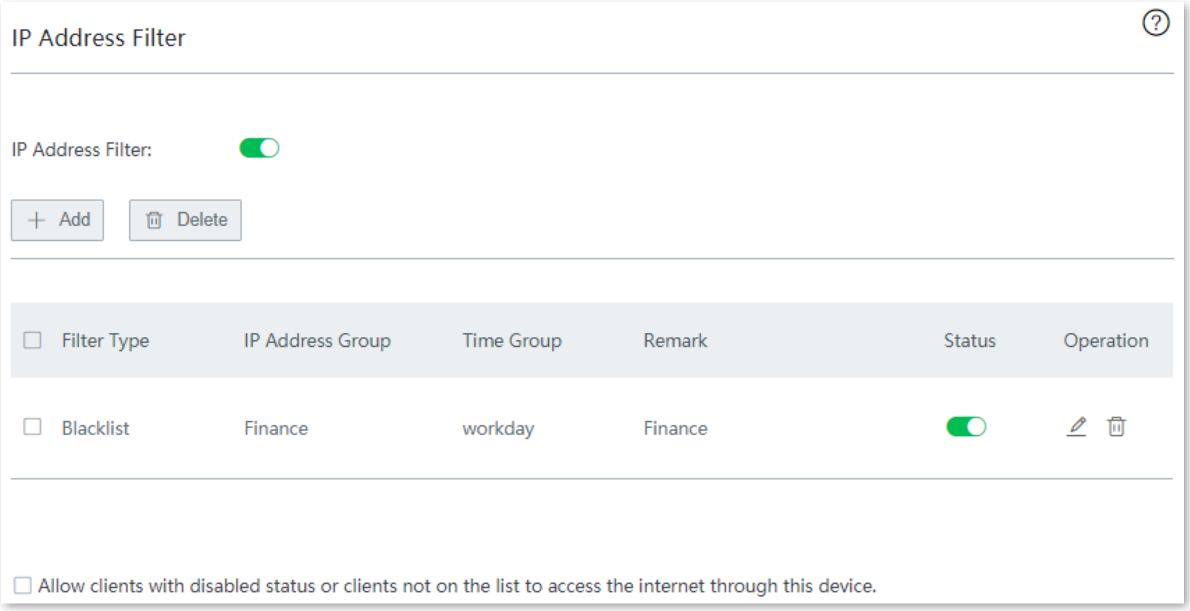
IP Group: Finance

Remark: Finance

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

----End

The rule is added successfully. See the following figure.



IP Address Filter

IP Address Filter: ●

□ Filter Type	IP Address Group	Time Group	Remark	Status	Operation
□ Blacklist	Finance	workday	Finance	●	✎ 🗑

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

Verification

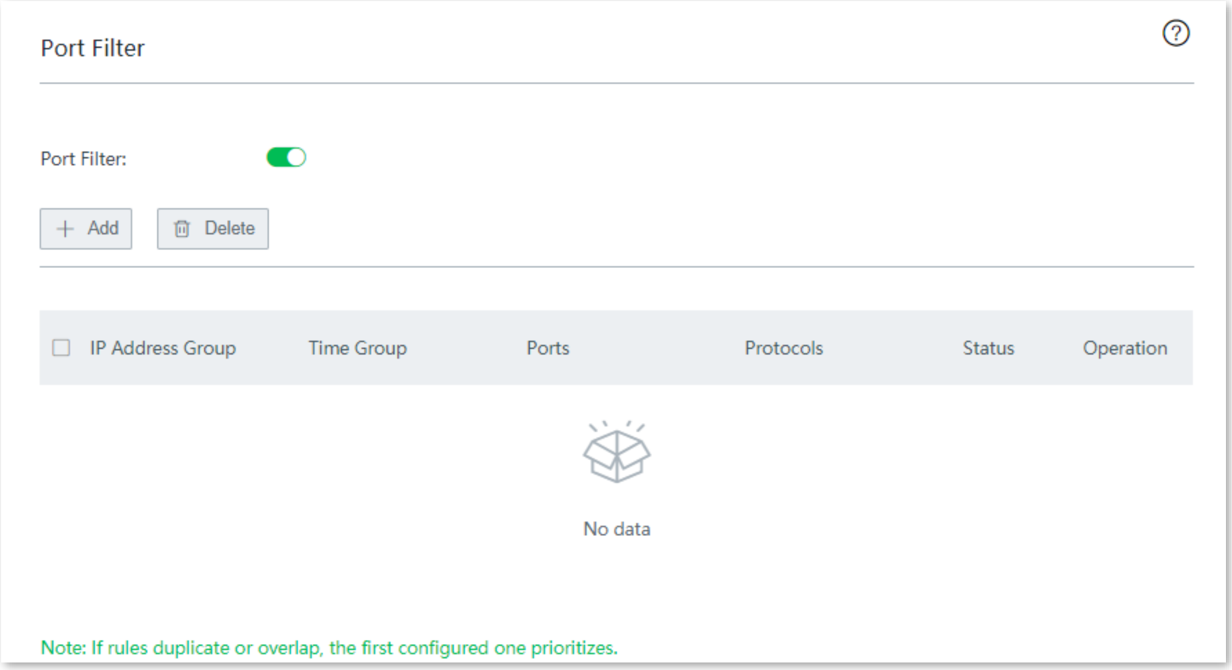
During 08:30 to 18:00 on workdays, the financial department’s computers cannot access the internet.

3.9.4 Port filter

Overview

The application protocols involved in many services on the internet have specific port numbers, which range from 0 to 1023 and are generally assigned to specific services.

Navigate to **Filter Management** > **Port Filter** to enter the page. By default, this function is disabled.



Port Filter

Port Filter: ●

□ IP Address Group	Time Group	Ports	Protocols	Status	Operation

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

Parameter description

Parameter	Description
IP/Time Group	It is used to create or select the IP/time group to which the rule applies. To create an IP/time group, navigate to **Filter Management** > **IP Group/Time Group**.
Port	It specifies the TCP or UDP port for the blocked network service. It can be a port or a port range.
Protocols	It specifies the protocol for the blocked network service. All indicates both TCP and UDP.
Status	It specifies the status of the rule. You can enable or disable it as you need.

Parameter	Description
Operation	It specifies the rules can be operated as follows: ✎: Click it to edit the rule. 🗑: Click it to delete the rule.

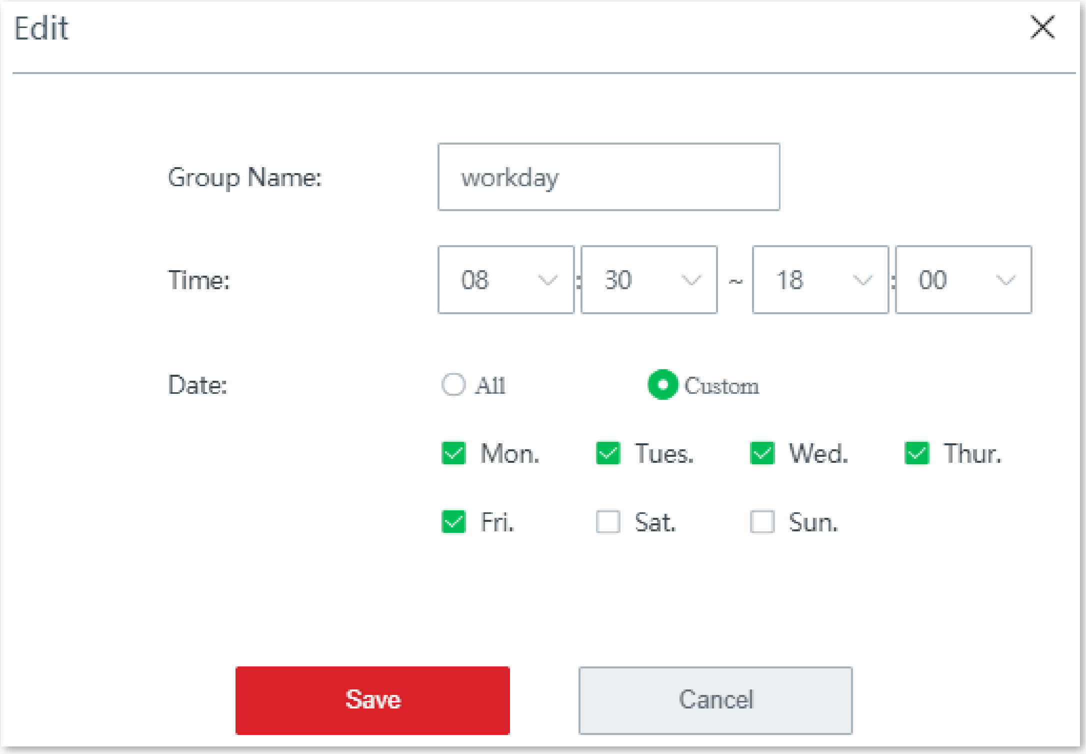
Create a port filter rule

Add a time group > Add an IP group > Create a port filter rule

1. Add a time group.

   (1) Navigate to **Filter Management** > **IP Group/Time Group**.

   (2) Click **+Add** on the **Time Group Settings** part, and add a time group.



Group Name: workday

Time: 08 : 30 ~ 18 : 00

Date: ○ All ● Custom

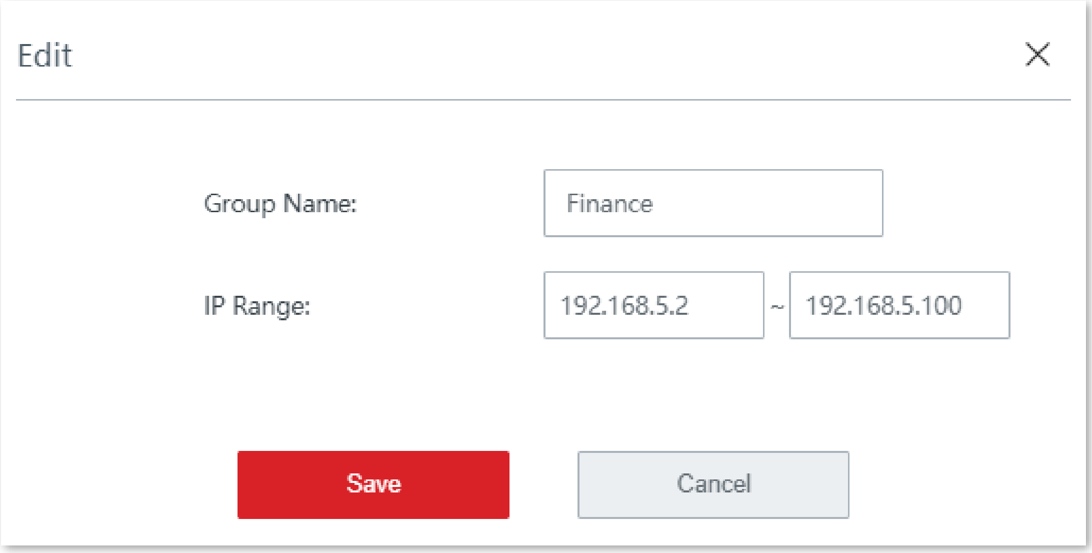
☑ Mon. ☑ Tues. ☑ Wed. ☑ Thur.

☑ Fri. □ Sat. □ Sun.

2. Add an IP group.

   (1) Navigate to **Filter Management** > **IP Group/Time Group**.

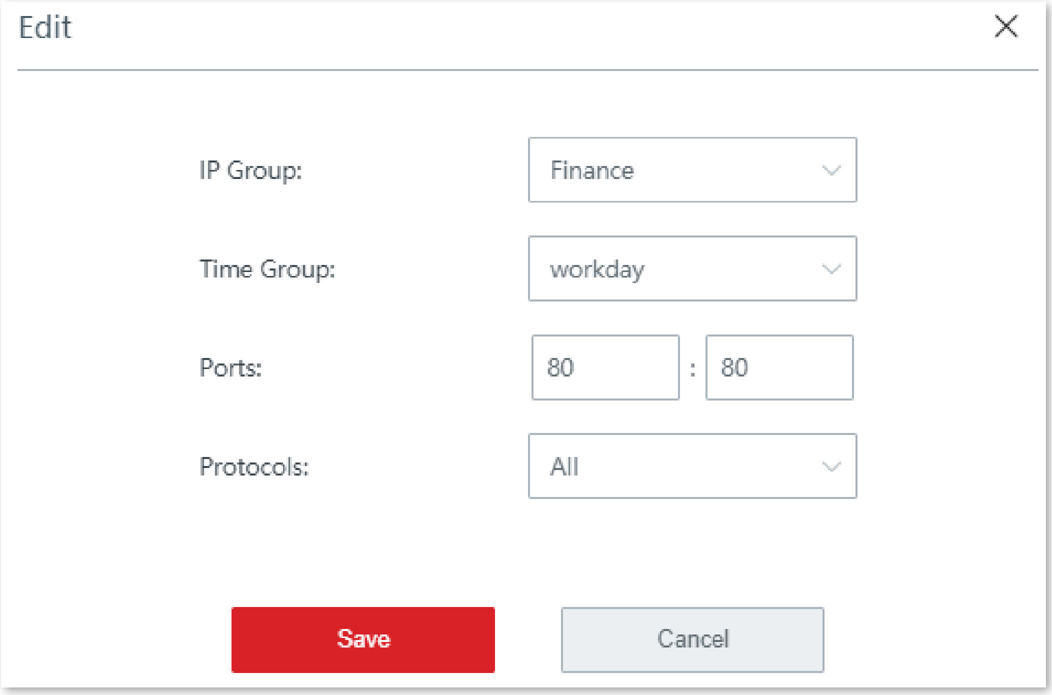
   (2) Click **+Add** on the **IP Group Settings** part, and add an IP group.



Group Name: Finance

IP Range: 192.168.5.2 ~ 192.168.5.100

3. Add a port filter rule.
   (1) Select an IP group.
   (2) Select a time group.
   (3) Enter the port range.
   (4) Select the protocols type.
   (5) Click **Save**.



IP Group: Finance

Time Group: workday

Ports: 80 : 80

Protocols: All

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

----End

Example of configuring port filter

Networking requirement

An enterprise uses EW12 to set up a LAN to meet the following requirement:

During business hours (08:30 to 18:00 on workday), finance department is not allowed to browse websites (the default port number for web services is 80).

Solutions

The port filter combined with IP address reservation can meet this requirement.

Assumption:

The IP addresses of finance department ranges from 192.168.5.2 to 192.168.5.10

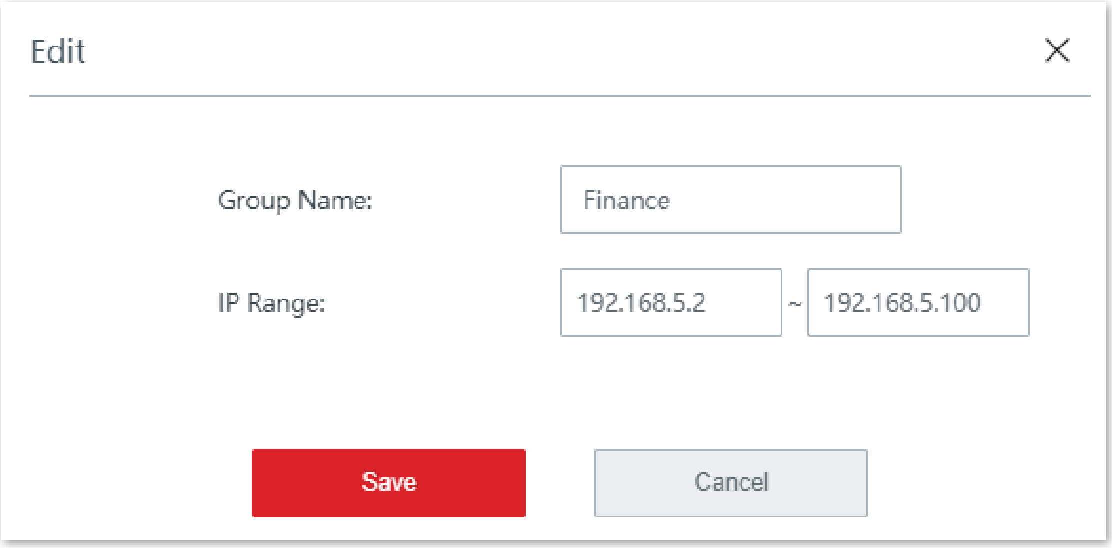
The default port number for web services is 80.

Configuration procedure

1. Reserve the IP addresses from 192.168.5.2 to 192.168.5.100 to the finance department's computers.

   (1) Click **Address Reservation**, and move to the **Manual Address Reservation** part.

   (2) Click **+Add**, and reserve the IP address for the finance department's computers.



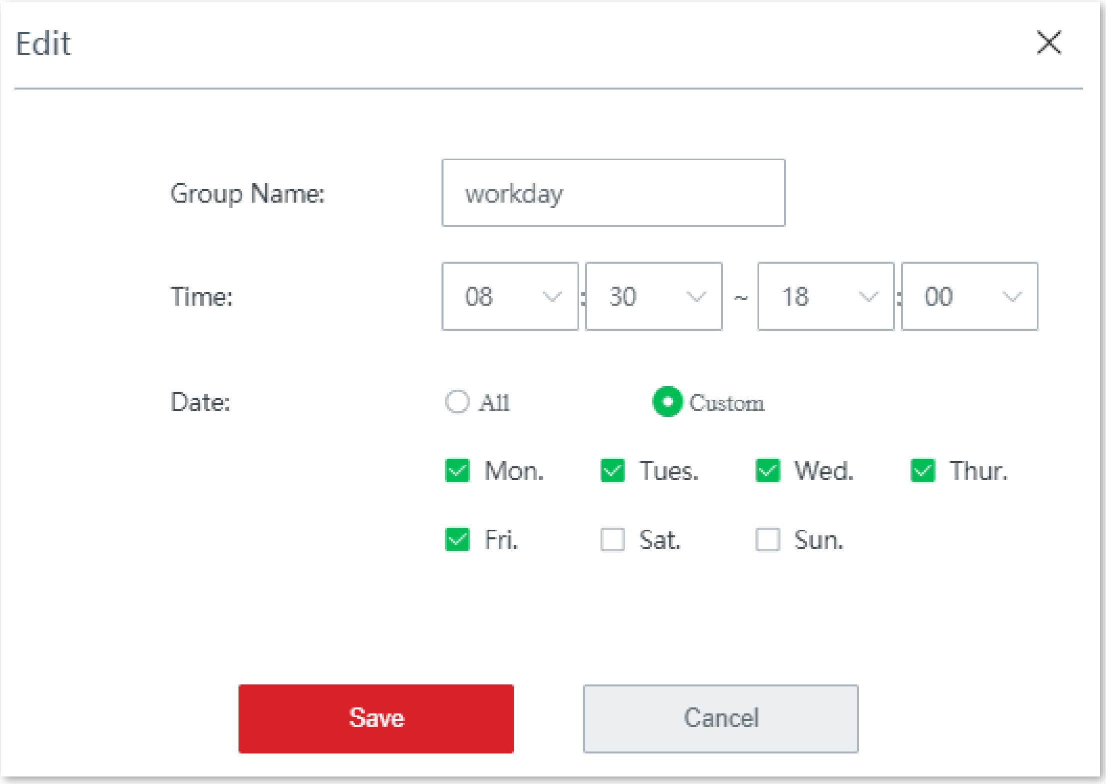
Group Name: Finance

IP Range: 192.168.5.2 ~ 192.168.5.100

2. Set up a time group.

   (1) Navigate to **Filter Management** > **IP Group/Time Group**.

   (2) Add a time group shown in the following figure.



Group Name: workday

Time: 08 : 30 ~ 18 : 00

Date: ○ All ● Custom

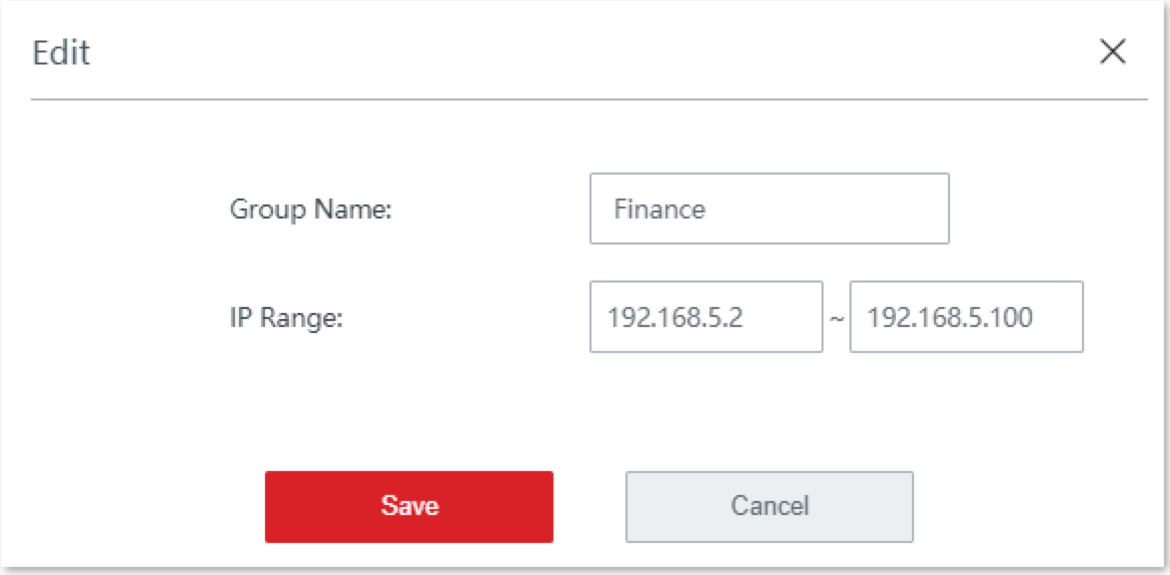
☑ Mon. ☑ Tues. ☑ Wed. ☑ Thur.

☑ Fri. □ Sat. □ Sun.

3. Add an IP group.

(1) Navigate to **Filter Management** > **IP Group/Time Group**.

(2) Add an IP group as shown in the following figure.



Group Name: Finance

IP Range: 192.168.5.2 ~ 192.168.5.100

4. Add a port filter rule.

(1) Navigate to **Filter Management** > **Port Filter**, enable the function and click **Save**.

(2) Click **+Add**. The configuration window appears.

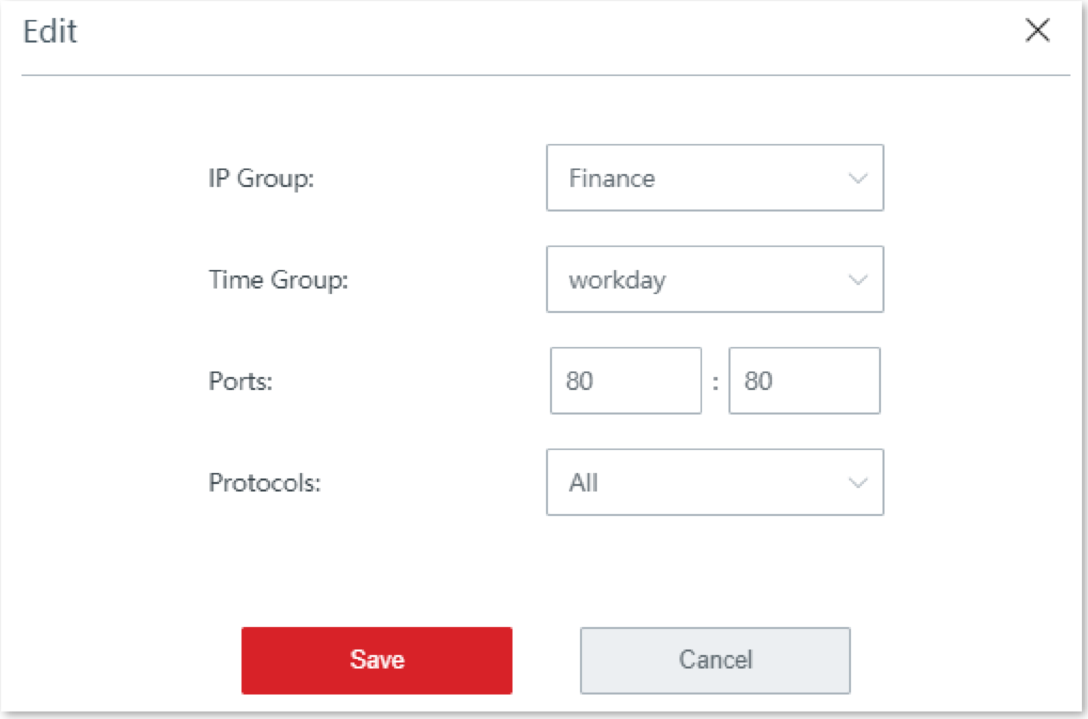
(3) Select **workday** from the **Time Group** drop-down list.

(4) Select **Finance** from the **IP Group** drop-down list.

(5) Enter **80** to **80** in the **Port**s input box.

(6) Select **All** from the **Protocols** drop-down list.

(7) Click **Save**.



Edit

IP Group: Finance

Time Group: workday

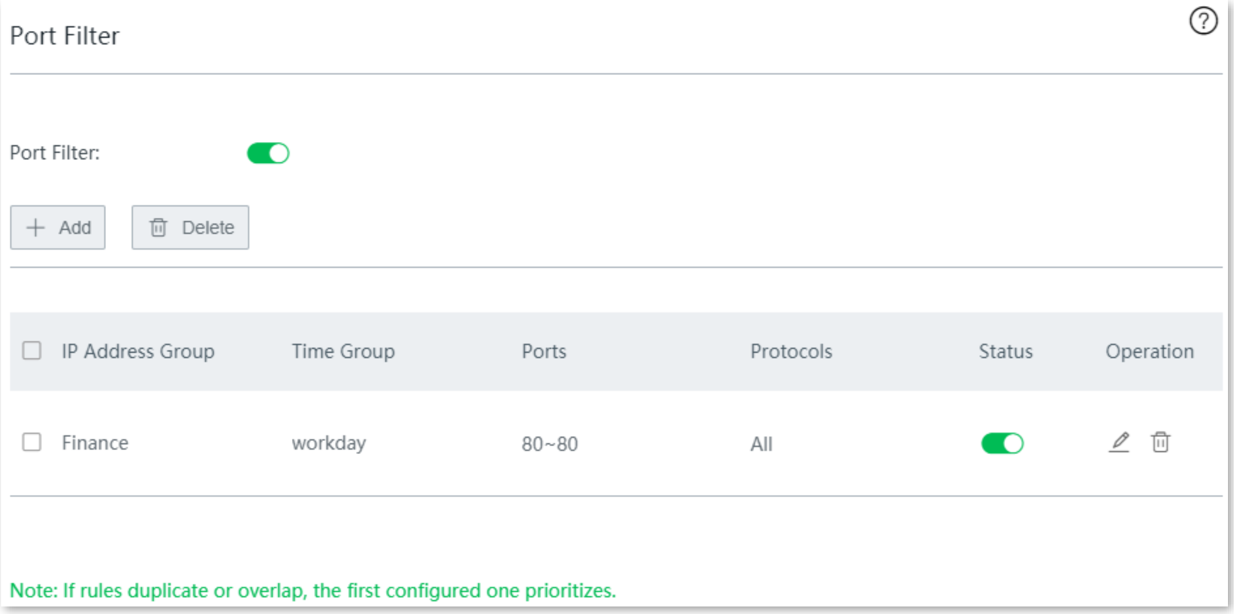
Ports: 80 : 80

Protocols: All

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

----End

The rule is added successfully. See the following figure.



Port Filter

Port Filter: ●

□ IP Address Group	Time Group	Ports	Protocols	Status	Operation
□ Finance	workday	80~80	All	●	

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

Verification

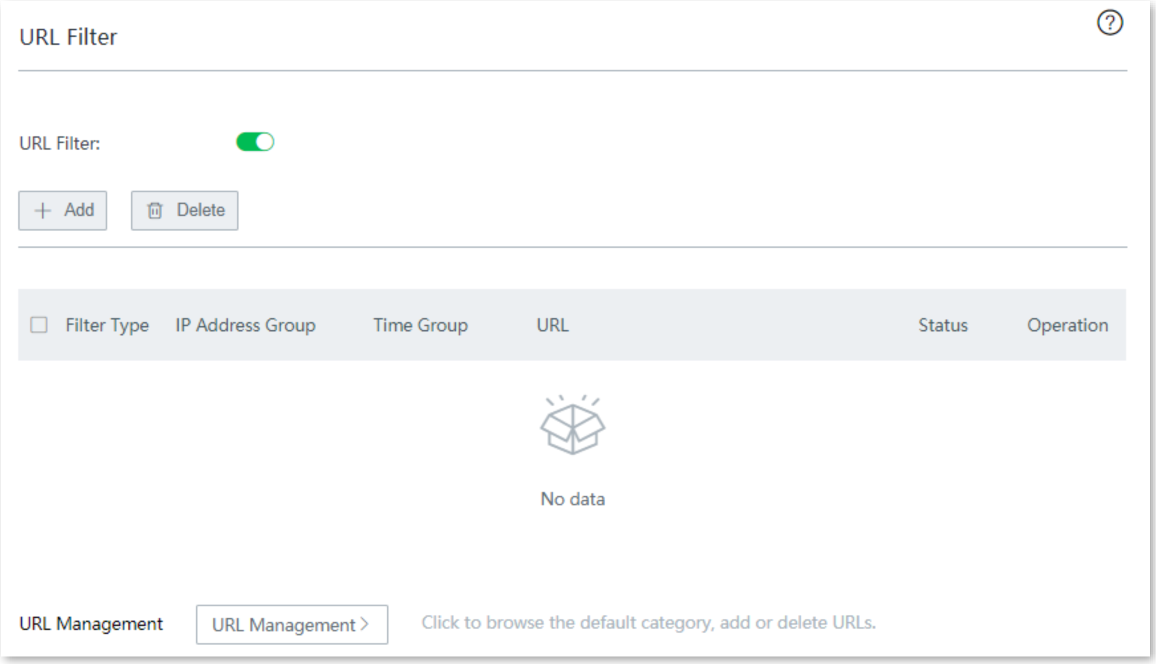
During 08:30 to 18:00 on workdays, computers whose IP addresses range from 192.168.5.2 to 192.168.5.100 cannot access the internet.

3.9.5 URL filter

Overview

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

Navigate to **Filter Management** > **URL Filter** to enter the page. By default, this function is disabled.



URL Filter

URL Filter: ●

□	Filter Type	IP Address Group	Time Group	URL	Status	Operation

No data

URL Management

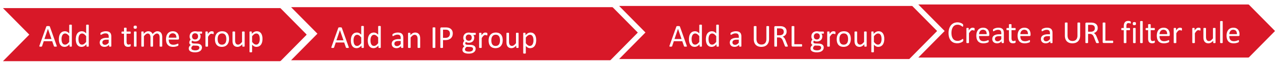
Click to browse the default category, add or delete URLs.

Parameter description

Parameter	Description
URL Filter	It specifies whether or not to enable the URL Filter function.
Filter Type	It specifies IP address filter modes. – **Allow access only**: Clients with this filter type will be added into the **Whitelist**, indicating that users in the IP group can only visit the specified websites during the specified period. – **Block access only**: Clients with this filter type will be added into the **Blacklist**, indicating that users in the IP group cannot visit the specified websites during the specified period.

Parameter	Description
IP Address	It specifies the IP addresses corresponding to the devices.
Time Group	It is used to select a time group for the rule. It should be configured on the **Filter Management** > **IP Group/Time Group** page.
IP Group	It is used to select a time group for the rule. It should be configured on the **Filter Management** > **IP Group/Time Group** page.
Remark	Optional. It Specifies a brief description for the rule.
URL	It is used to select a URL category that is predefined or you customized.
Status	It specifies the status of the rule. You can enable/disabled it as required.
Operation	It is used to perform the following operations: Click 📝 to change the rule. Click 🗑 delete the rule.
URL Management	It specifies the customize URL category.

Create a URL filter rule

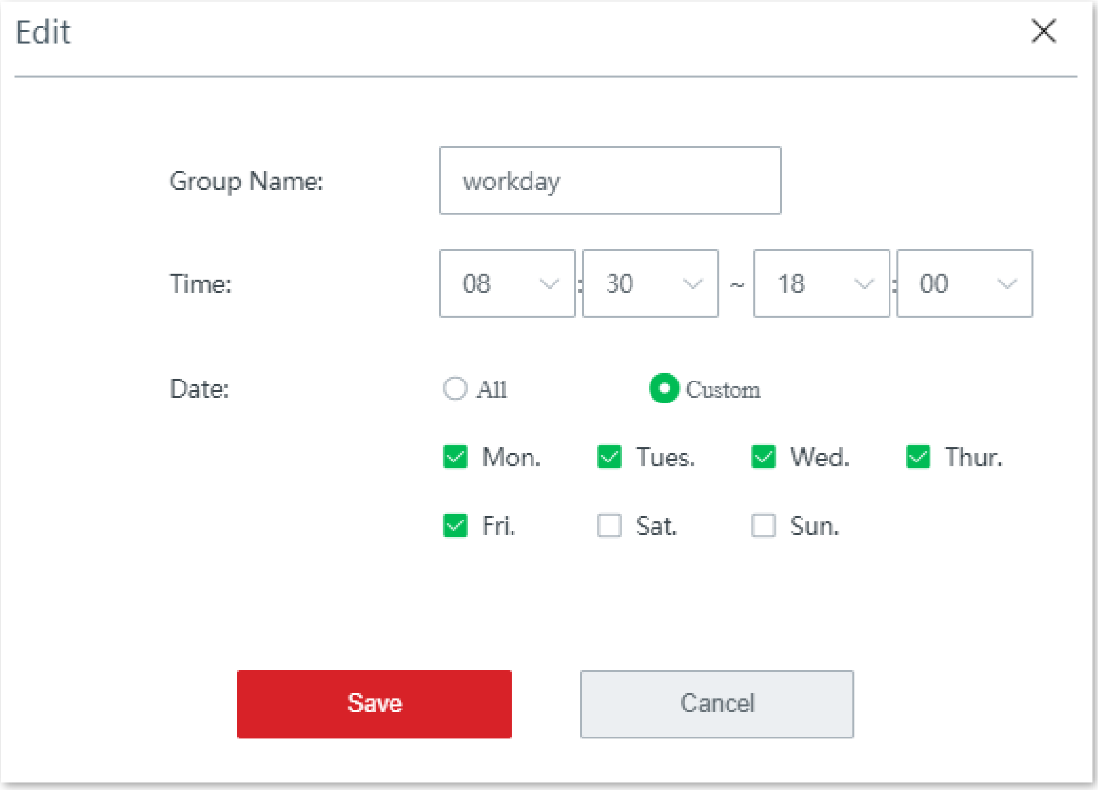


Add a time group > Add an IP group > Add a URL group > Create a URL filter rule

1. Add a time group.

   (1) Navigate to **Filter Management** > **IP Group/Time Group**.

   (2) Click **+Add** on the **Time Group Settings** part, and add a time group.



Group Name: workday

Time: 08 : 30 ~ 18 : 00

Date: ○ All ● Custom

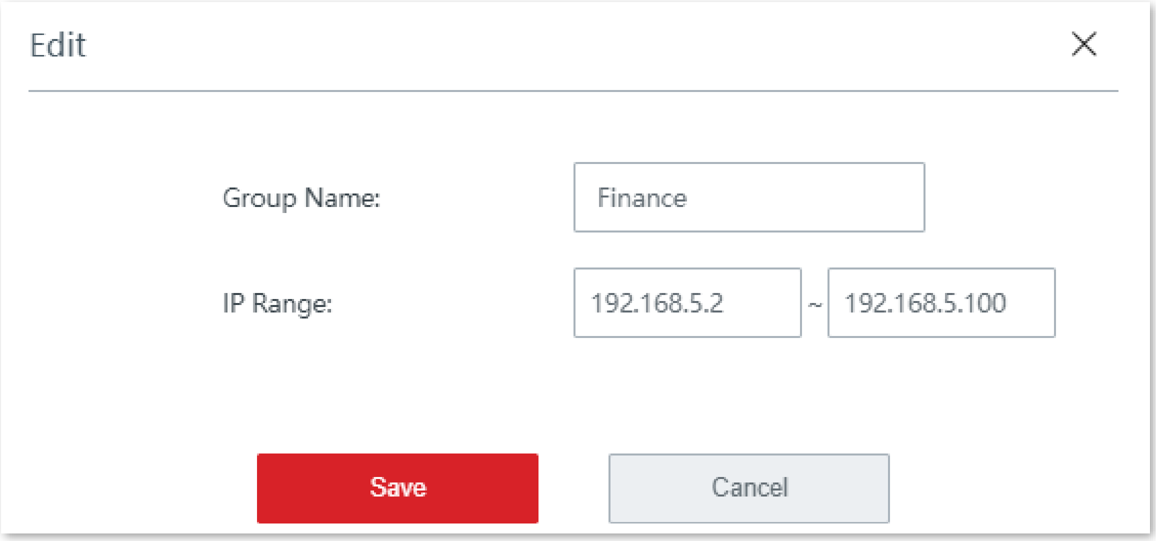
☑ Mon. ☑ Tues. ☑ Wed. ☑ Thur.

☑ Fri. □ Sat. □ Sun.

2. Add an IP group.

   (1) Navigate to **Filter Management** > **IP Group/Time Group**.

   (2) Click **+Add** on the **IP Group Settings** part, and add an IP group.



Group Name: Finance

IP Range: 192.168.5.2 ~ 192.168.5.100

3. Add a URL group.

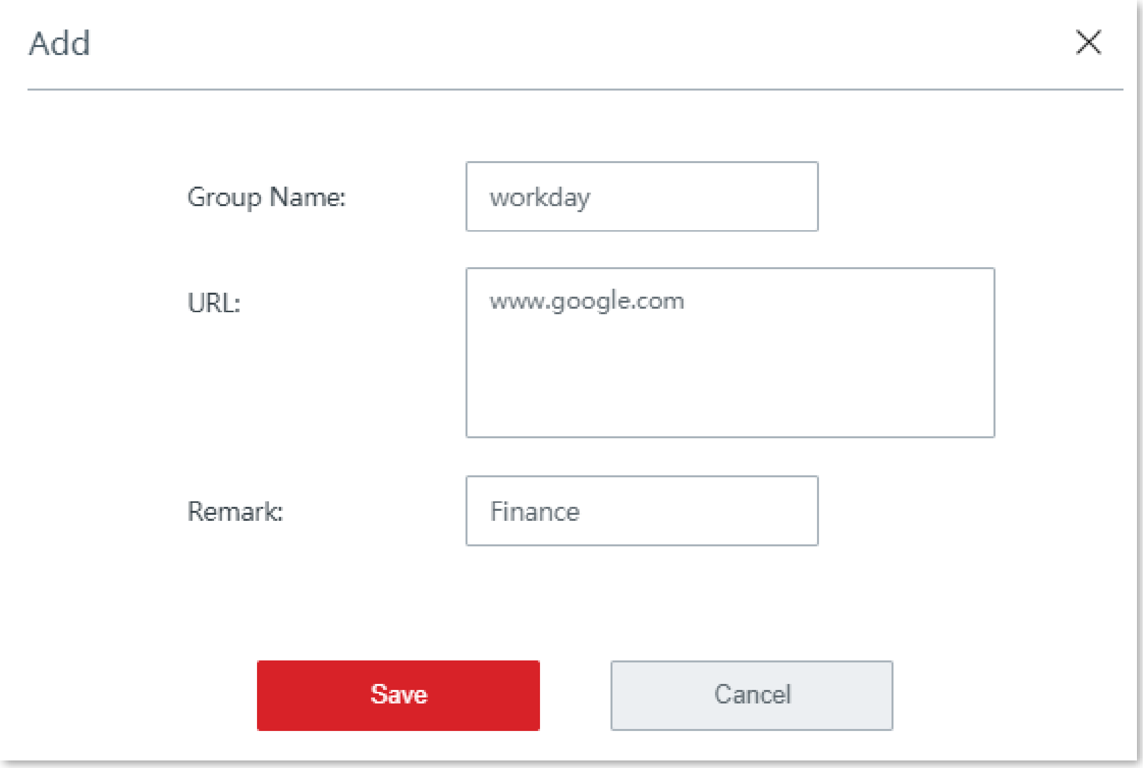
   (1) Click the **URL Management** button, The **URL Management** configuration page appears.

   (2) Click **New**. The **Add** window appears.

      – Customize a **Group Name**.

      – Enter the URLs to be filtered.

- (Optional) Specify a brief description in the **Remark** input box.
- Click **Save**.



Add

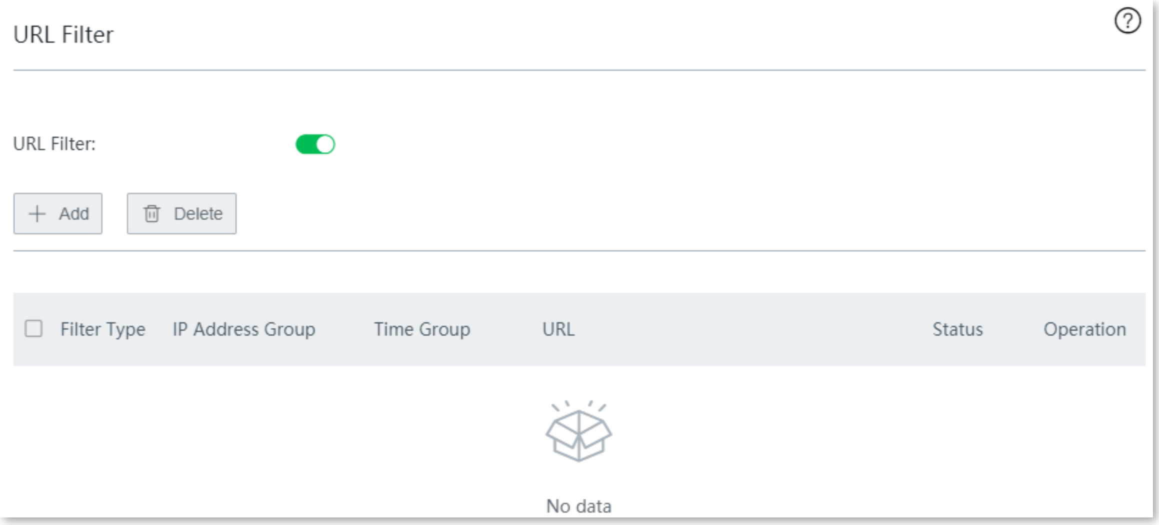
Group Name: workday

URL: www.google.com

Remark: Finance

4. Create a URL filter rule.

(1) Click **+Add**. The configuration window appears.



URL Filter

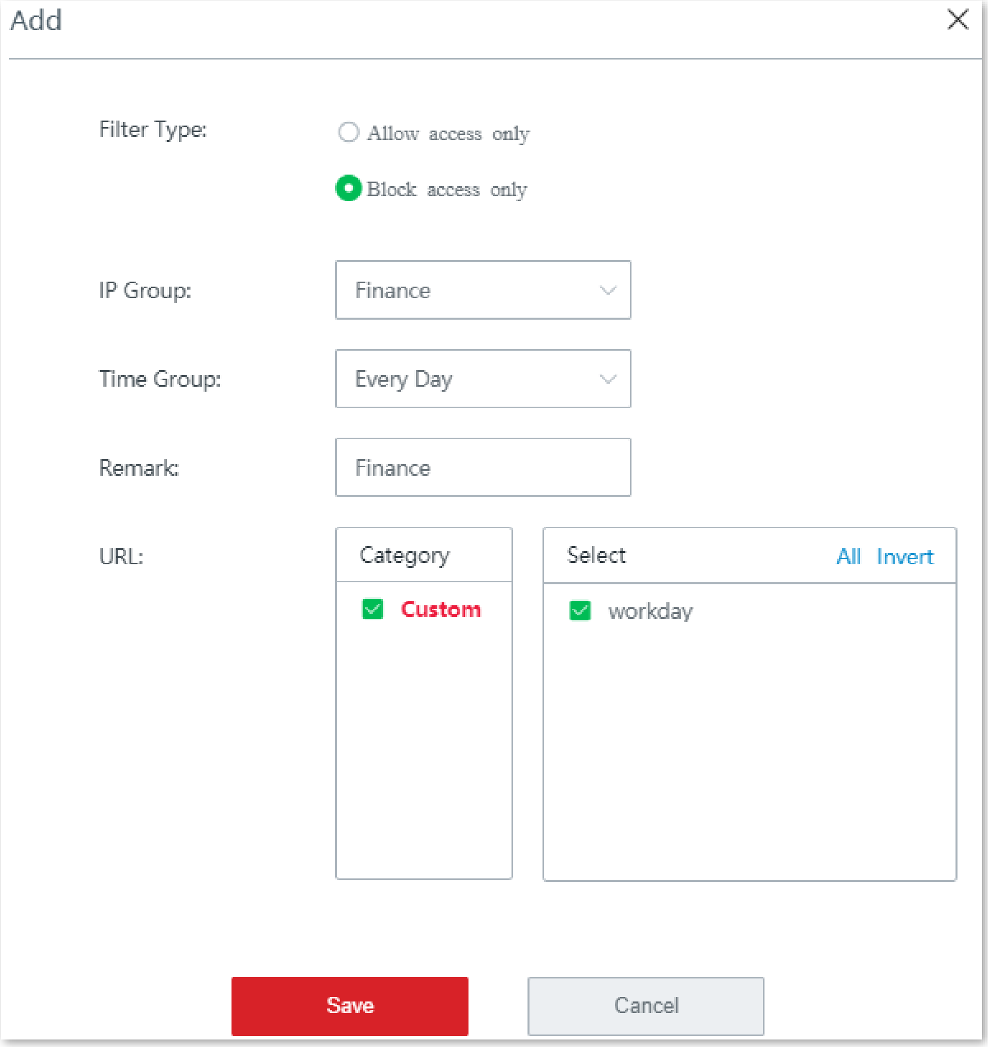
URL Filter: on

□	Filter Type	IP Address Group	Time Group	URL	Status	Operation

No data

- Select a **Filter Type**.
- Select the **IP Group** you add.
- Select the **Time Group** you add.
- (Optional) Specify a description for the rule in the Remark input box.
- Select the group you add.

– Click **Save**.



Add

Filter Type: ○ Allow access only ● Block access only

IP Group: Finance

Time Group: Every Day

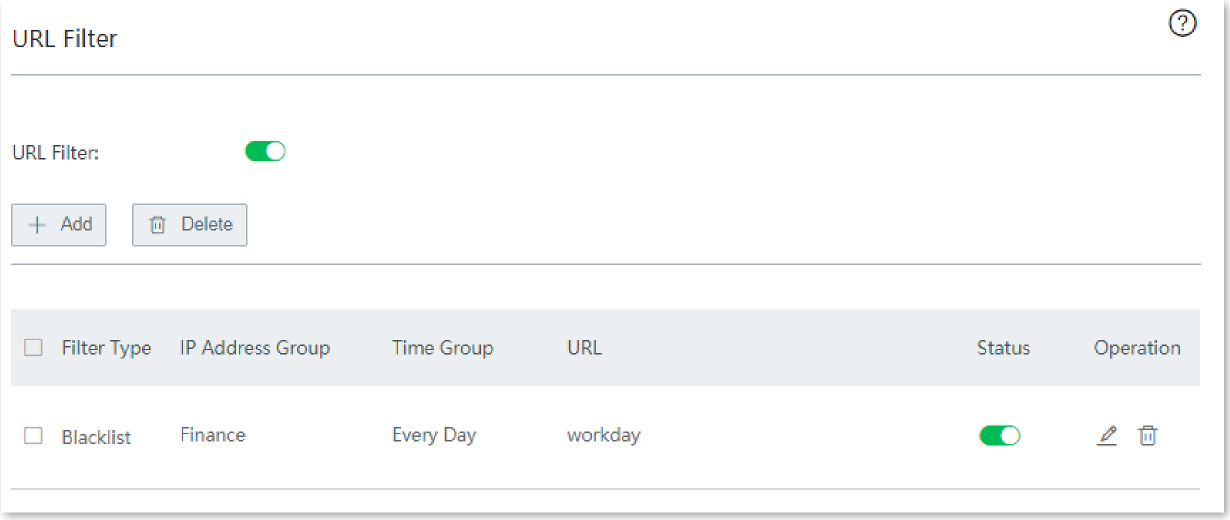
Remark: Finance

URL:

Category	Select All Invert
☑ Custom	☑ workday

----End

The rule is added successfully. See the following figure.

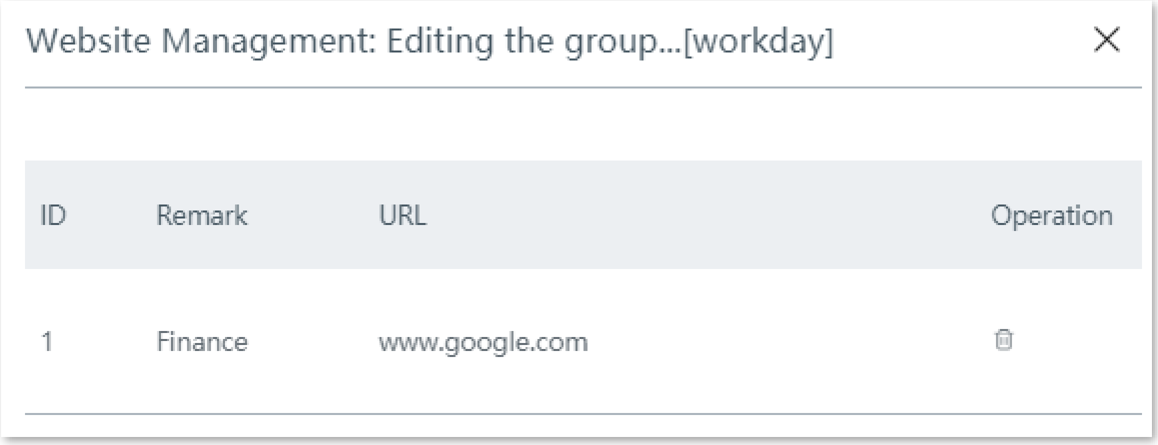


URL Filter

URL Filter: ●

□ Filter Type	IP Address Group	Time Group	URL	Status	Operation
□ Blacklist	Finance	Every Day	workday	●	

To remove an added URL category, move the cursor to the name of the group, click 🗑 , and click **OK** on the pop-up window. The category in use cannot be removed.



Website Management: Editing the group...[workday]

ID	Remark	URL	Operation
1	Finance	www.google.com	🗑

Example of configuring URL filter

Networking requirement

An enterprise uses EW12 to set up a LAN to meet the following requirement:

During business hours (08:30 to 18:00 on workday), staff are disallowed to access social medias including Facebook, YouTube, and Tumblr.

Solutions

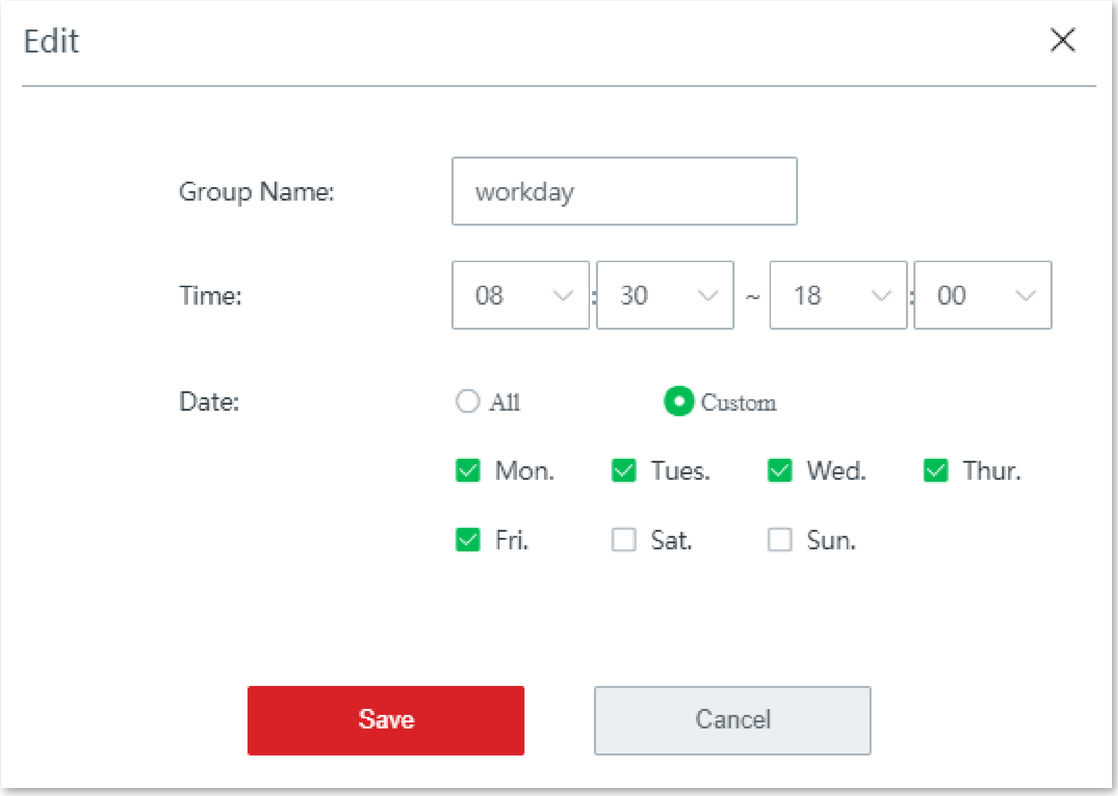
The URL filter can meet this requirement.

Configuration procedure

1. Add a time group.

   (1) Navigate to **Filter Management** > **IP Group/Time Group**.

   (2) Add a time group as shown in the following figure.



Group Name: workday

Time: 08 : 30 ~ 18 : 00

Date: ○ All ● Custom

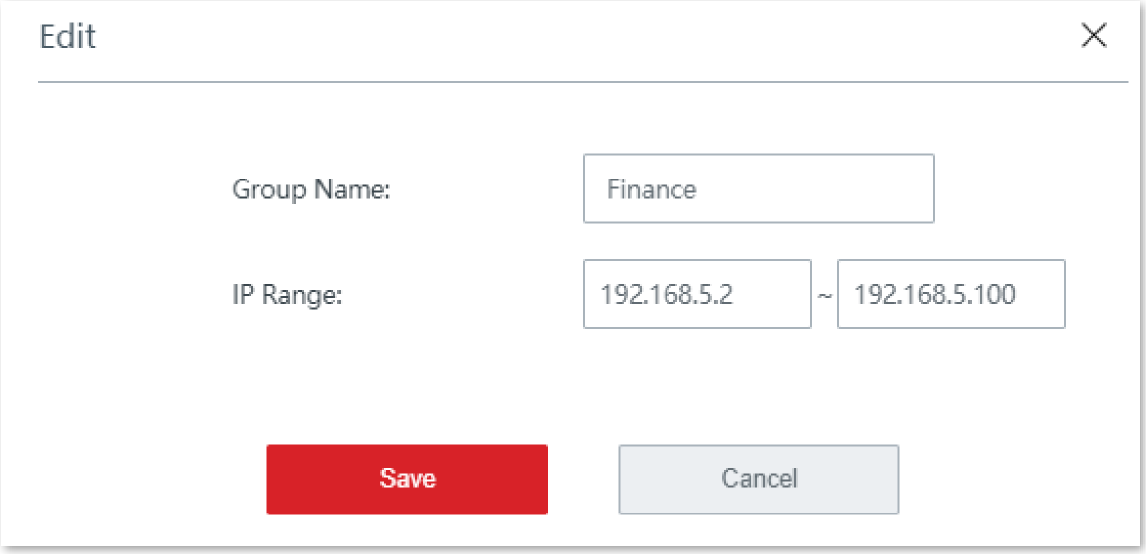
☑ Mon. ☑ Tues. ☑ Wed. ☑ Thur.

☑ Fri. □ Sat. □ Sun.

2. Add an IP group.

   (1) Navigate to **Filter Management** > **IP Group/Time Group**.

   (2) Add an IP group as shown in the following figure.



Group Name: Finance

IP Range: 192.168.5.2 ~ 192.168.5.100

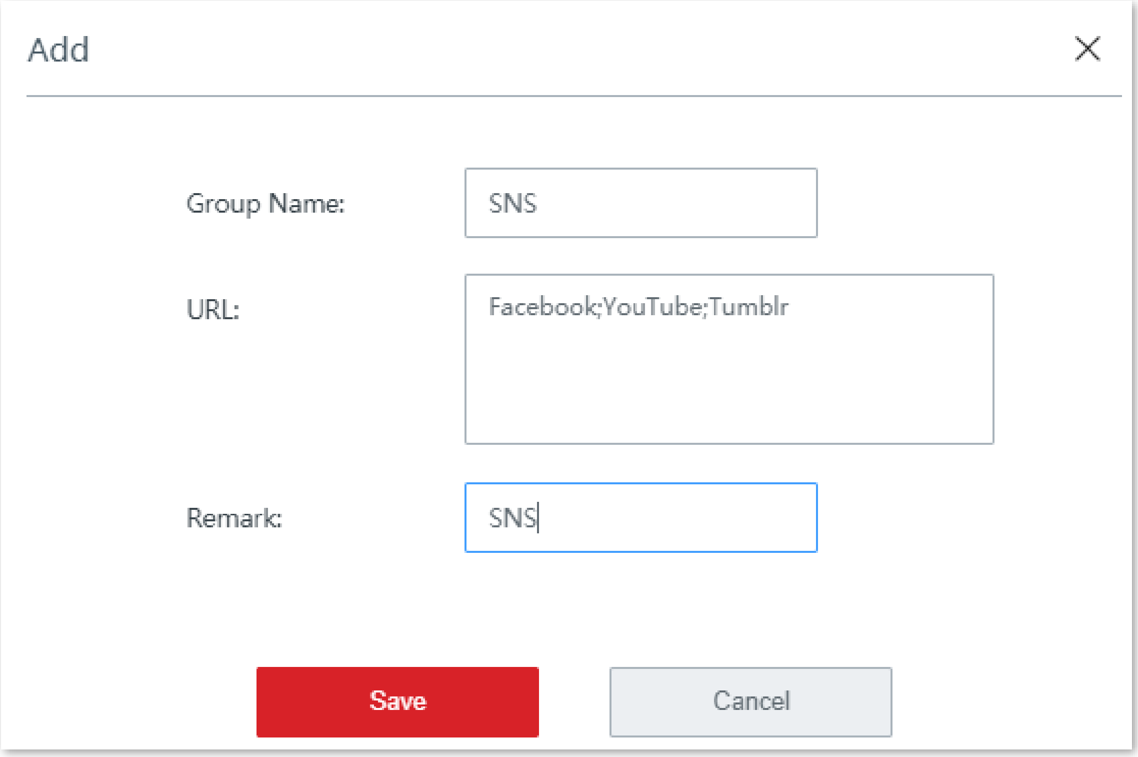
3. Add a URL rule.

   (1) Navigate to **Filter Management** > **URL Filter**, enable the function and click **Save**.

   (2) Click the **URL Management** button. The **URL Management** configuration page appears.

   (3) Click **New**. The **Add** window appears.

   (4) Set the required parameters, and click **Save**. See the following figure.



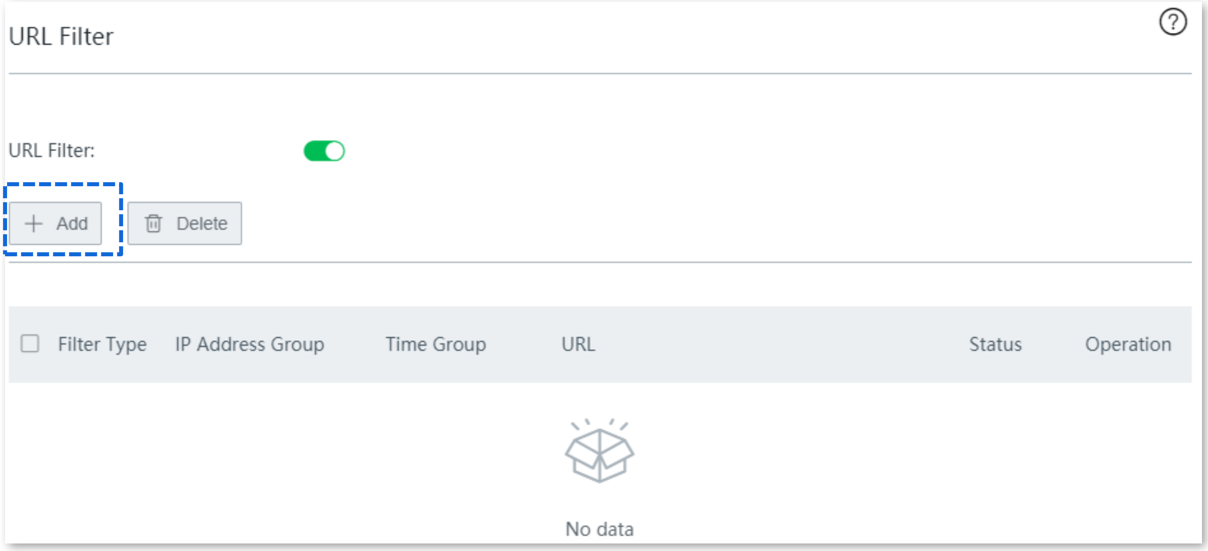
Group Name: SNS

URL: Facebook;YouTube;Tumblr

Remark: SNS

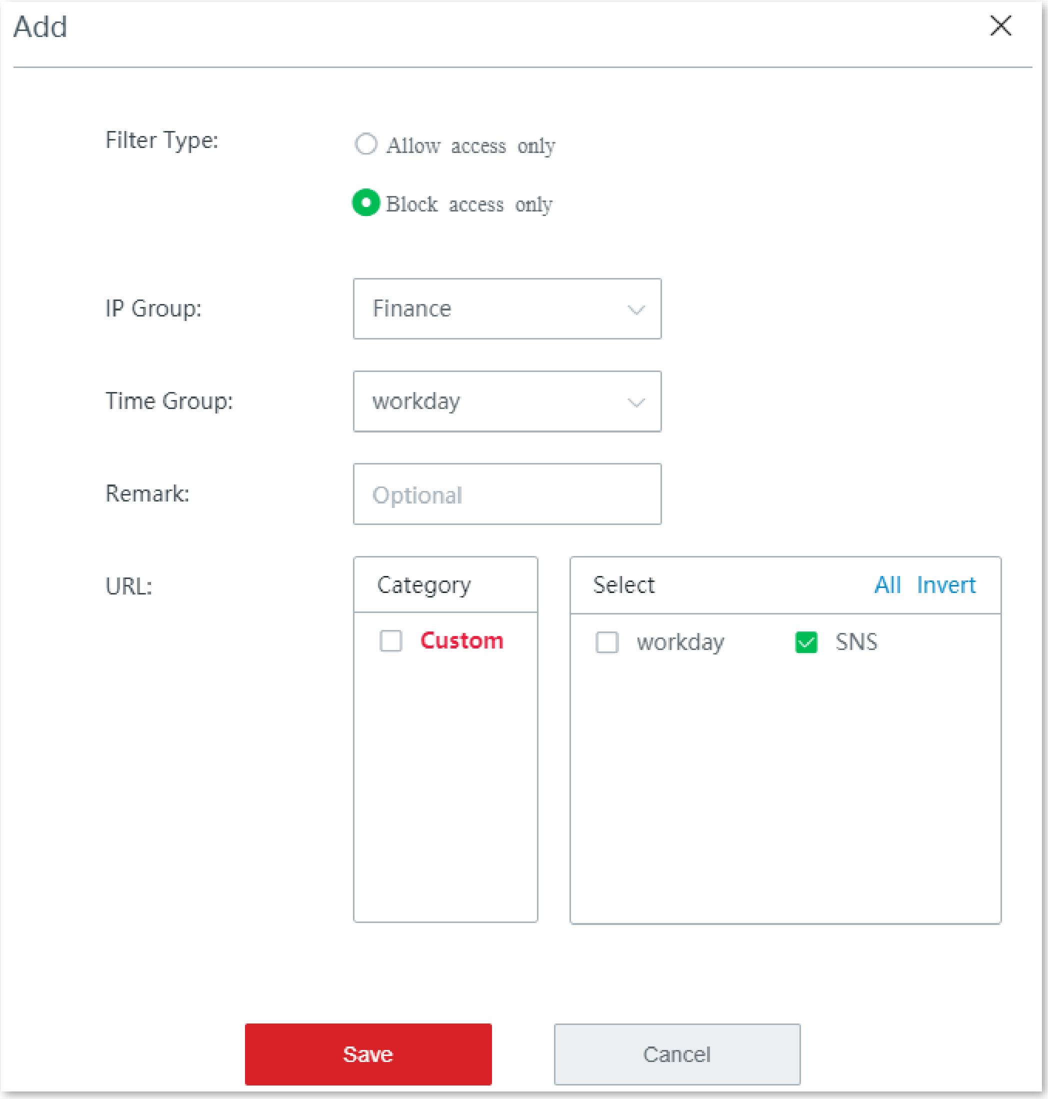
4. Create a URL filter rule.

(1) Click **+Add**. The configuration window appears.



□	Filter Type	IP Address Group	Time Group	URL	Status	Operation

- Select **Block access only**.
- Select the IP Group, which is **Finance** in this example.
- Select the Time Group, which is **workday** in this example.
- (Optional) Specify a description for the rule in the Remark input box.
- Select a URL category, which is **SNS** in this example.
- Click **Save**.



Add

Filter Type: ○ Allow access only ● Block access only

IP Group: Finance

Time Group: workday

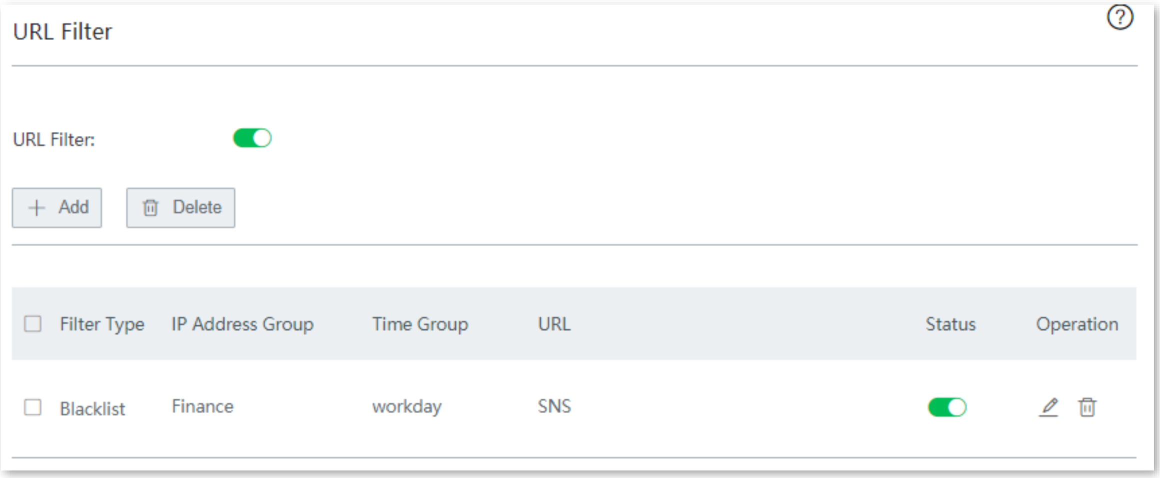
Remark: Optional

URL:

Category	Select All Invert
□ Custom	□ workday ☑ SNS

----End

The rule is added successfully. See the following figure.



URL Filter

URL Filter: ●

□	Filter Type	IP Address Group	Time Group	URL	Status	Operation
□	Blacklist	Finance	workday	SNS	●	

Verification

During 08:30 to 18:00 on workdays, clients with the IP address ranging from 192.168.5.2 to 192.168.5.100 cannot access Facebook, YouTube, and Tumblr.

3.10 More

3.10.1 LAN settings

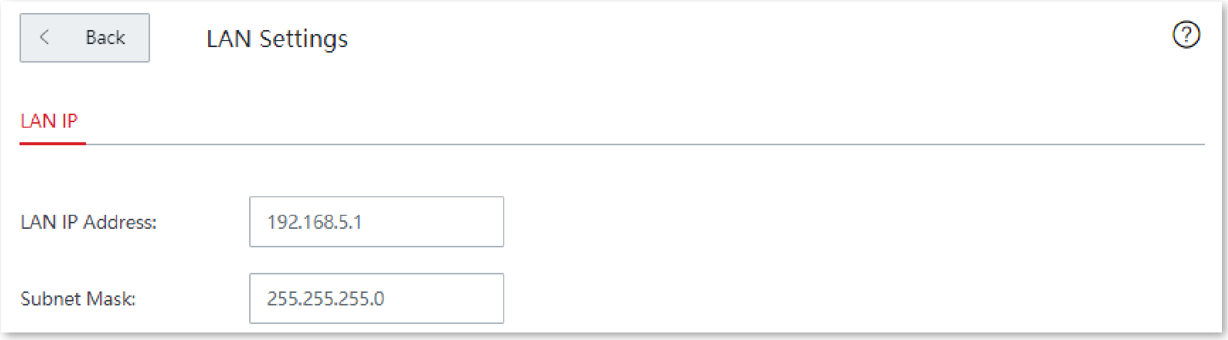
You can view and modify the LAN IP address of the node, and configure DHCP server here.

Navigate to **More** > **LAN Settings** to enter this page.

The LAN IP address is also the login IP address of the node. The default LAN IP address is **192.168.5.1**.

Change LAN IP address

Generally, you do not need to modify the LAN IP address of the node unless an IP conflict happens.

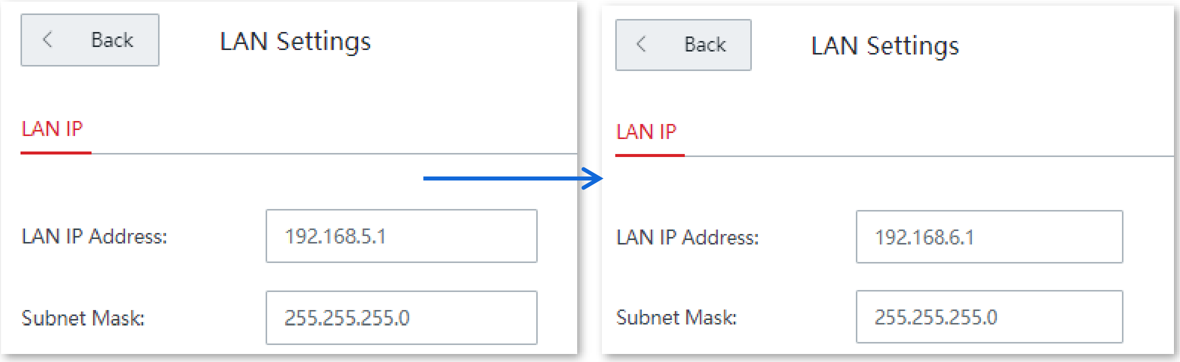


LAN IP Address: 192.168.5.1

Subnet Mask: 255.255.255.0

Configuration procedure

1. Navigate to **More** > **LAN Settings** to enter the page.
2. Modify the LAN IP address as required, which is **192.168.6.1** in this example.



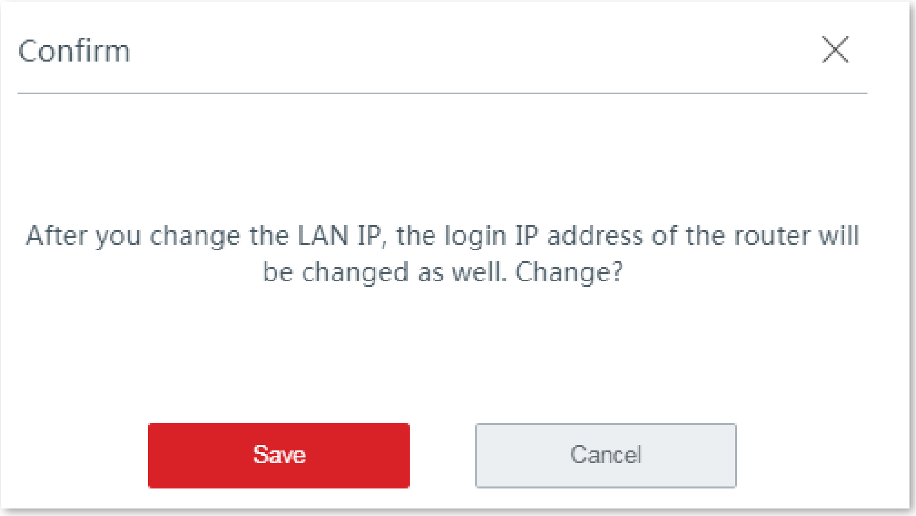
LAN IP Address: 192.168.5.1

Subnet Mask: 255.255.255.0

LAN IP Address: 192.168.6.1

Subnet Mask: 255.255.255.0

3. Click **Save**, the following message appears.



Confirm

After you change the LAN IP, the login IP address of the router will be changed as well. Change?

4. Confirm the message in the pop-up window, and click **Save**.

----End

Wait until the progress bar completes. You will be redirected to the login page.

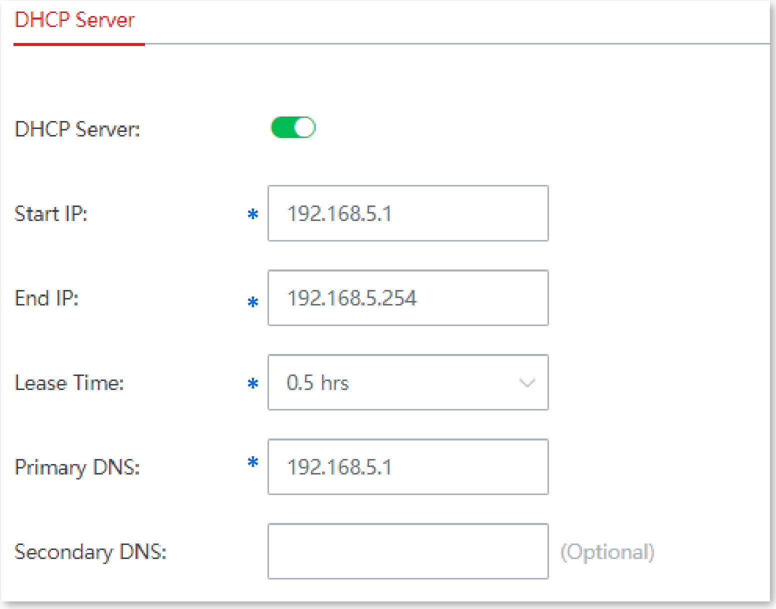
Use the new LAN IP address or domain name (www.ipcwifi.com) log in to the web UI of node later.

Change the DHCP server settings

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

Configuration procedure

1. Navigate to **More** > **LAN Settings** to enter the page.
2. Change the settings as required.



DHCP Server

DHCP Server: ●

Start IP: * 192.168.5.1

End IP: * 192.168.5.254

Lease Time: * 0.5 hrs

Primary DNS: * 192.168.5.1

Secondary DNS: (Optional)

3. Click **Save**.

----End

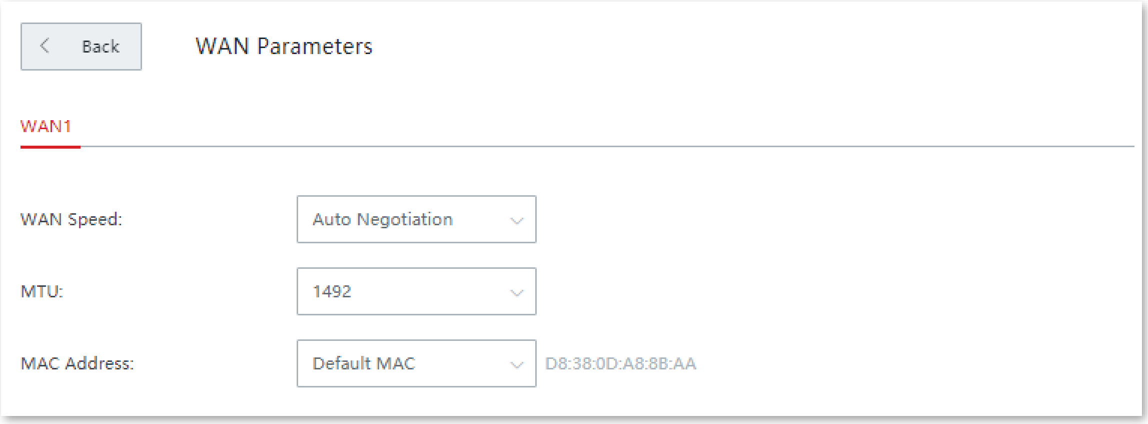
Parameter description

Parameter	Description
Start IP	It specifies the start/end IP address of the IP address pool of the DHCP server.
End IP	
Lease Time	It specifies the validity period of an IP address assigned by the DHCP server to a client. When half of the lease time has elapsed, the client sends a DHCP request to the DHCP server to renew the lease time. If the request succeeds, the lease time is extended according to the request. Otherwise, the client sends the request again when 7/8 of the lease time has elapsed. If the request succeeds, the lease time is extended according to the request. Otherwise, the client must request an IP address from the DHCP server after the lease time expires. It is recommended that you retain the default value.
Primary DNS	It specifies the primary DNS server IP address assigned by the DHCP server to clients.
Secondary DNS	It specifies the secondary DNS server IP address assigned by the DHCP server to clients. This parameter is optional.

3.10.2 WAN parameters

If you have set internet connection parameters but your LAN devices cannot access the internet, try modifying WAN port parameters here.

Navigate to **More** > **WAN Parameters** to enter the page.



WAN Parameters

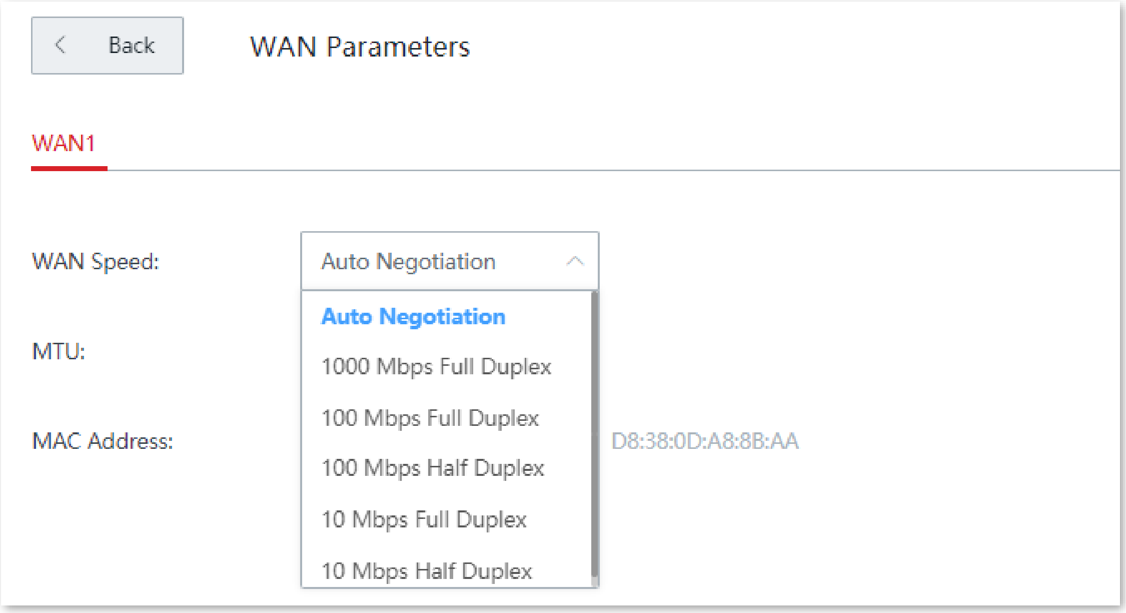
WAN Speed: Auto Negotiation

MTU: 1492

MAC Address: Default MAC D8:38:0D:A8:8B:AA

WAN speed

By default, the cable-free node uses **Auto Negotiation**, which is appropriate for almost all cases. If the node's WAN port is correctly connected to the Ethernet cable and the Ethernet cable works normally, but the corresponding WAN port indicator is not on. Or after being connected to the Ethernet cable, the WAN port lights on after a while (more than 5 seconds). Then the WAN port speed of the node can be set to **10 Mbps Half Duplex** or **10 Mbps Full Duplex** to solve the problem.



WAN Parameters

WAN Speed: Auto Negotiation

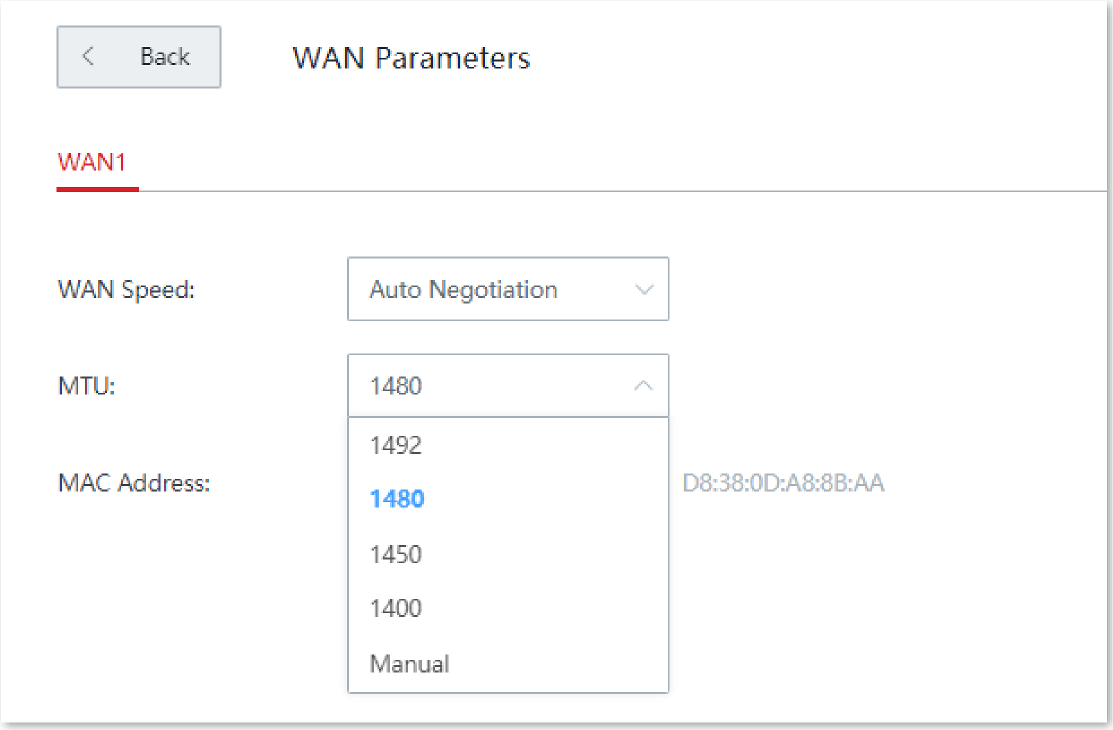
MTU:

MAC Address: D8:38:0D:A8:8B:AA

MTU

MTU is abbreviated for Maximum Transmission Unit. It specifies the maximum size of a packet that can be transmitted by a network device. Either larger or smaller MTU value affects the network performance. Do not modify the default settings unless the following situations happen:

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



WAN Speed: Auto Negotiation

MTU: 1480

MAC Address: D8:38:0D:A8:8B:AA

Commonly-used MTU value in different scenarios:

MTU (Bytes)	Scenario
1500	It is the most common value for non-PPPoE connections and non-VPN connections.
1492	It is used for PPPoE connections.
1480	It is the maximum value for the pinging function.
1450	It is used for DHCP, which assigns dynamic IP addresses to connected devices.
1400	It is used for VPN.

Tip

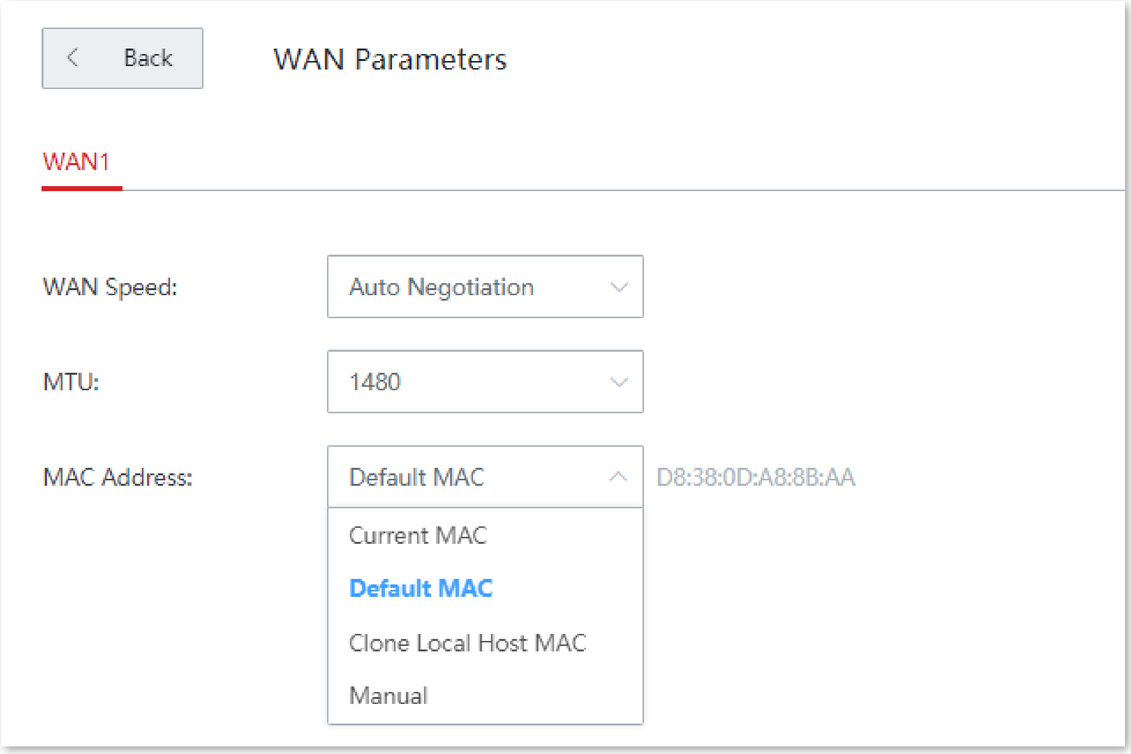
In general, it is recommended to leave the MTU value as the default, unless in the following conditions:

- Unable to access some sites, or open security sites.
- Unable to send or receive mail, or to access servers such as FTP and POP.

At this point, you can try to gradually reduce the MTU value from the maximum until the problem disappears.

MAC address

If the node still cannot connect to the internet when the network is set up, it is possible that the ISP has tied the internet account information to a MAC address (physical address). You can try to solve the problem with MAC address cloning (method 1 or method 2).



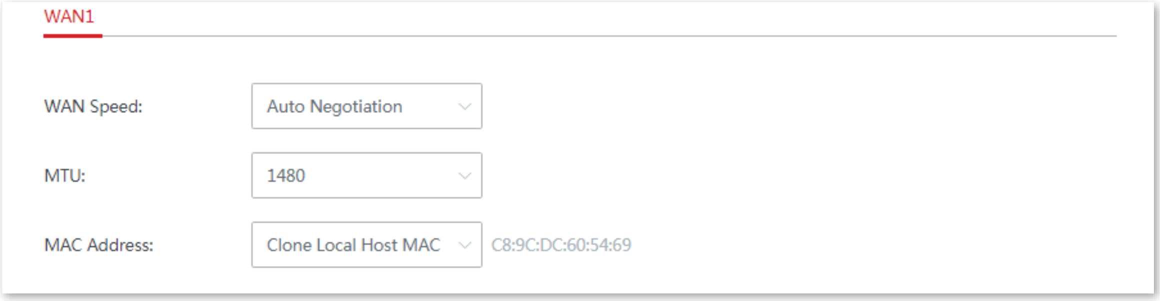
WAN Speed: Auto Negotiation

MTU: 1480

MAC Address: Default MAC D8:38:0D:A8:8B:AA

Method 1: Use the computer which can access the internet for cloning

1. Connect the computer which can access the internet with an Ethernet cable.
2. Start a web browser on the computer, and visit **192.168.5.1**.
3. Log in to the web UI, and navigate to **More** > **WAN Parameters**.
4. Set **MAC Address** to **Clone Local Host MAC**.
5. Click **Save**.



WAN Speed: Auto Negotiation

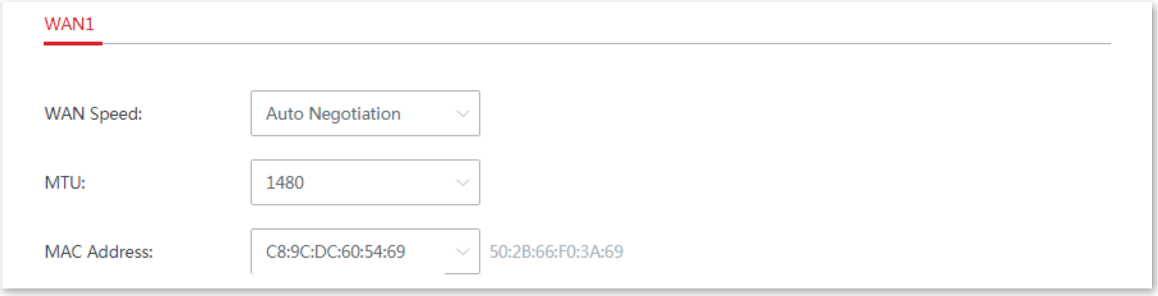
MTU: 1480

MAC Address: Clone Local Host MAC C8:9C:DC:60:54:69

----End

Method 2: Use another computer for cloning

1. Check the MAC address of the computer that can access the internet, which is **C8:9C:DC:60:54:69** in this example, and note it down.
2. Connect a computer to the node.
3. Start a web browser on the computer, and visit **192.168.5.1**.
4. Log in to the web UI, and navigate to **More** > **WAN Parameters**.
5. Set **MAC Address** to **Manual**, and change the MAC address.
6. Click **Save**.



WAN1

WAN Speed: Auto Negotiation

MTU: 1480

MAC Address: C8:9C:DC:60:54:69 50:2B:66:F0:3A:69

----End

3.10.3 Static routing

Overview

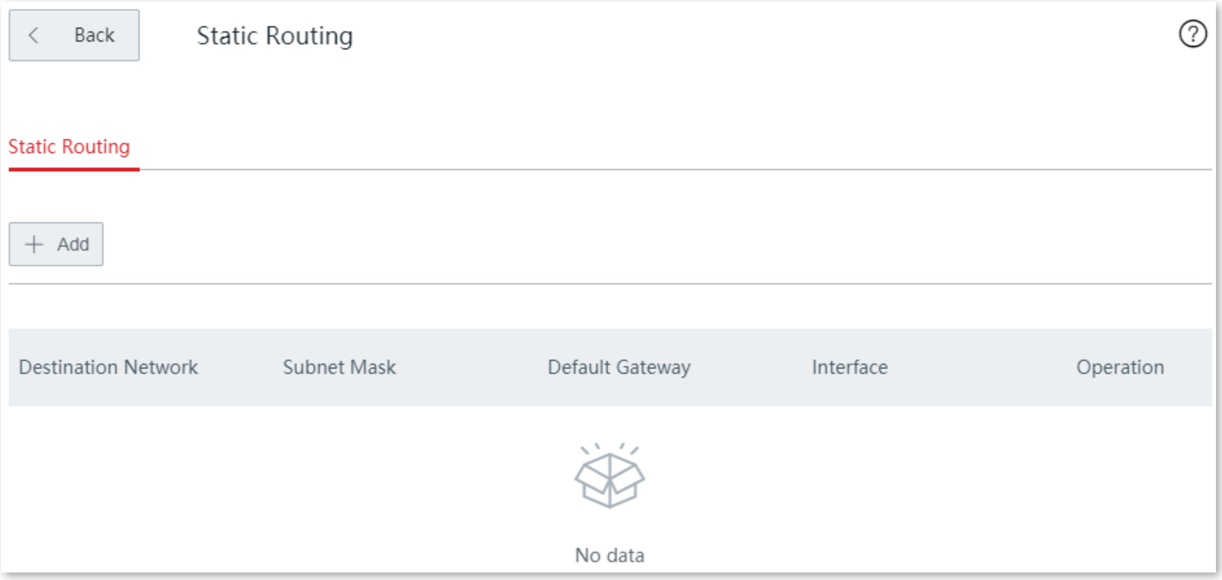
Routing is an operation to select the optimal route for delivering data from a source to a destination. A static route is a special route configured manually, which is simple, efficient, and reliable. Proper static routes help reduce route selection issues and prevent overload caused by route selection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

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

Tip

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

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



Destination Network	Subnet Mask	Default Gateway	Interface	Operation

Parameter description

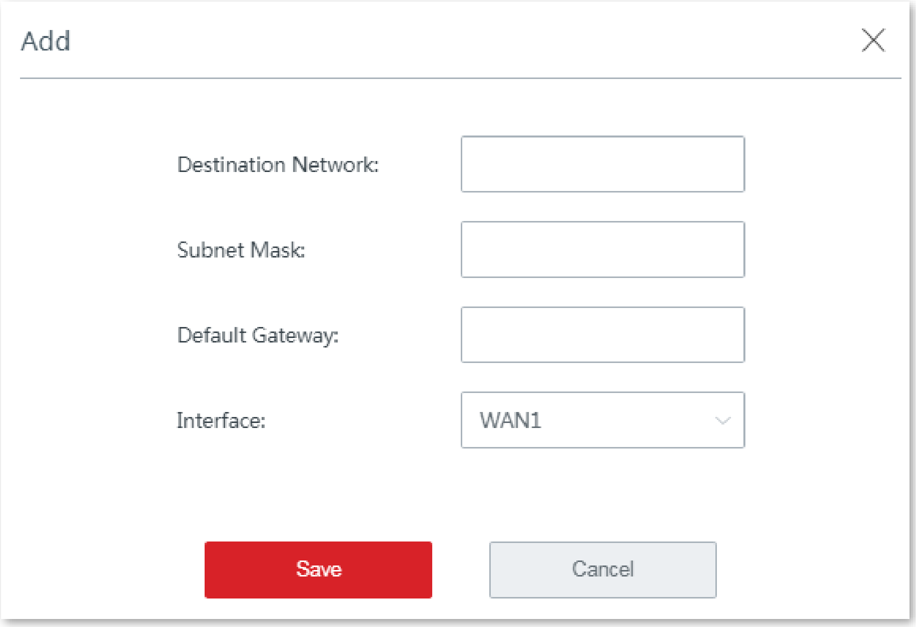
Parameter	Description
Destination Network	It specifies the IP address of the destination network. The default is **0.0.0.0**. **0.0.0.0** indicates the default route. Tip If the destination address of a packet cannot be found in the route table, the node uses the default route to forward the packet.
Subnet Mask	It specifies the subnet mask of the destination network. The default is **0.0.0.0**. **0.0.0.0** indicates the default route.
Default Gateway	It specifies the ingress port IP address of the next hop route after packets egress from the node. Tip **0.0.0.0** indicates that the destination network is directly connected to the node using the port specified in the route.
Interface	It specifies the interface from which packets egress. Select it as required.
Operation	It is used to edit or delete the rule. ✎: Click it to edit the rule. 🗑: Click it to delete the rule.

Configure static routing

Tip

If a static route conflicts with a user-defined multi-WAN policy, the static route takes preference over the policy.

1. Navigate to **More** > **Static Routing** to enter the page.
2. Click **+Add**. The configuration page appears.
3. Set the parameters and click **Save**.



Add

Destination Network:

Subnet Mask:

Default Gateway:

Interface: WAN1

----End

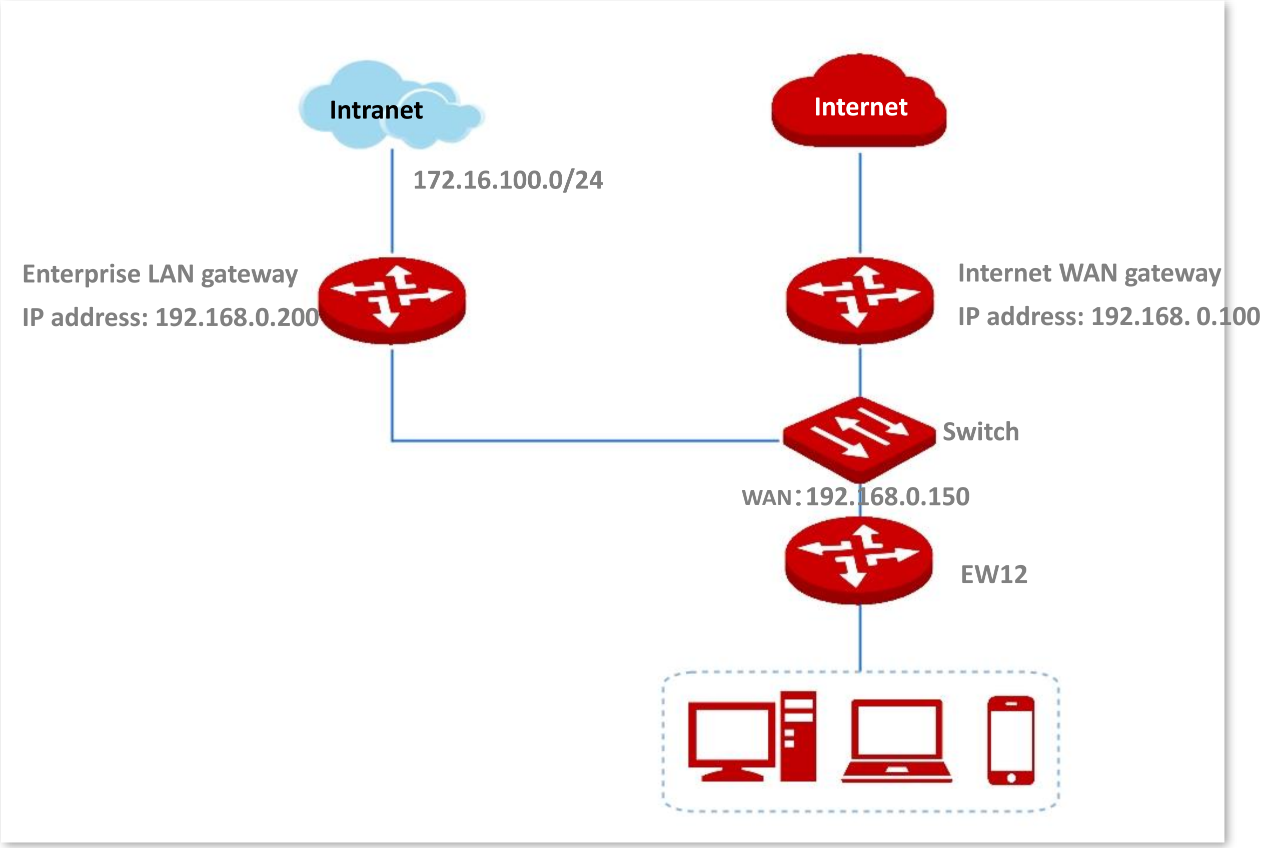
Example of configuring static routing

Network requirement

An enterprise uses EW12 and another two routers to deploy its network. Router1 is connected to the internet and its DHCP server is enabled. Router2 is connected to an intranet and its DHCP server is disabled. Users are able to access both the internet and intranet at the same time. Assume that the PPPoE user name and password are admin/admin.

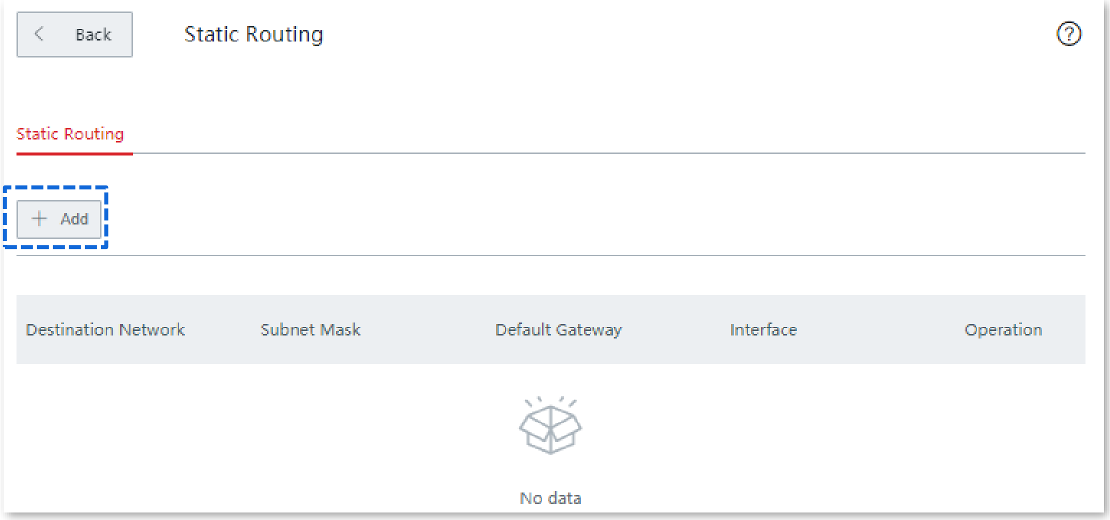
Solutions

The static routing function can address this requirement.



Configuration procedure

1. Navigate to **More** > **Static Routing**, and click **+Add**.



Destination Network	Subnet Mask	Default Gateway	Interface	Operation

No data

2. Set the parameters in the **Add** window as follows.

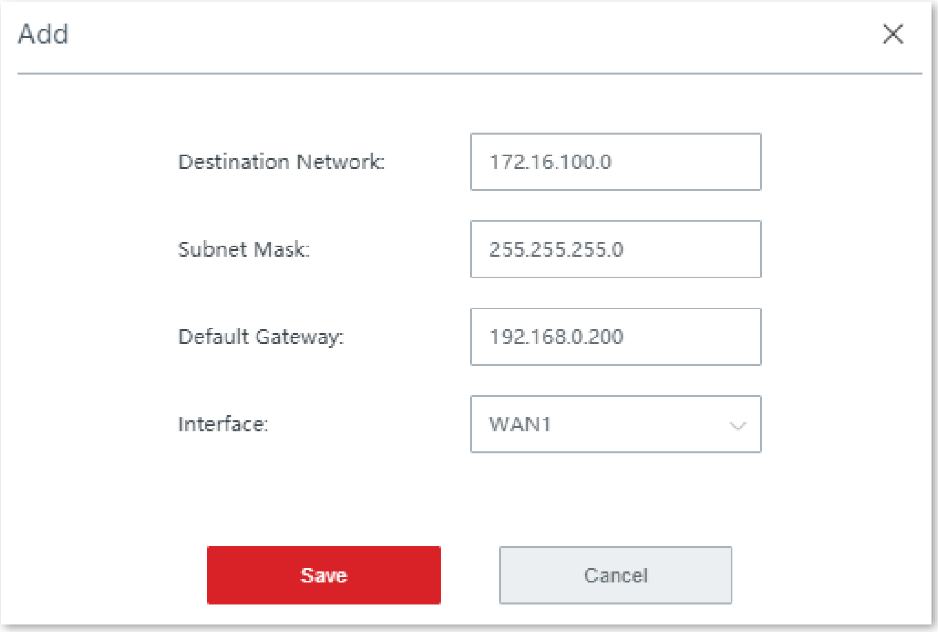
Enter the **Destination Network**, which is 172.16.100.0 in this example.

Enter the **Subnet Mask**, which is 255.255.255.0 in this example.

Enter the **Default Gateway**, which is 192.168.0.200 in this example.

Select the **Interface**, which is WAN1 in this example.

3. and click **Save**.



Add

Destination Network: 172.16.100.0

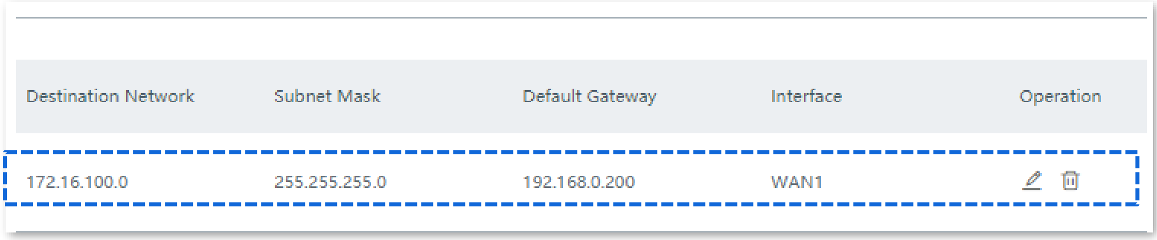
Subnet Mask: 255.255.255.0

Default Gateway: 192.168.0.200

Interface: WAN1

----End

The rule is added successfully. See the following figure.



Destination Network	Subnet Mask	Default Gateway	Interface	Operation
172.16.100.0	255.255.255.0	192.168.0.200	WAN1	

Veification

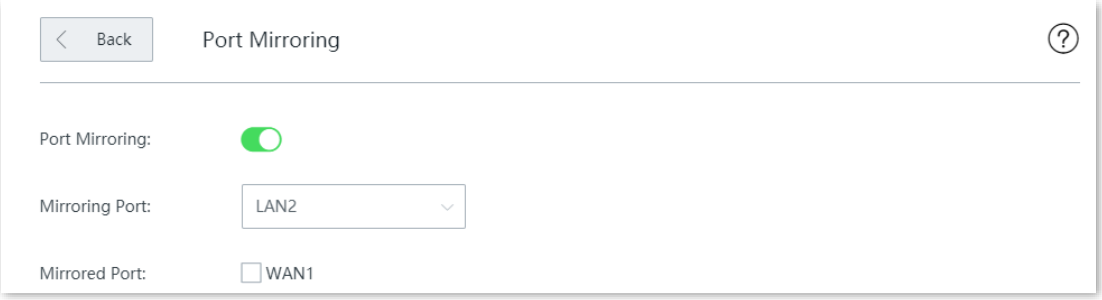
Computers in the LAN can access the internet and the intranet simultaneously.

3.10.4 Port mirroring

Overview

Port mirroring enables data from the node WAN port (mirrored port) to be copied to the specified port (mirroring port). Mirroring port is usually connected with data monitoring devices to enable network administrators to perform real-time traffic monitoring, performance analysis and fault diagnosis.

Navigate to **More** > **Port Mirroring** to enter the page. By default, this function is disabled.



Port Mirroring: ●

Mirroring Port: LAN2

Mirrored Port: □ WAN1

Configure port mirroring

1. Navigate to **More** > **Port Mirroring** to access the configuration page.
2. Set **Port Mirroring** to ● .
3. Choose **Mirroring Port** and **Mirrored Port** as required.
4. Click **Save** to apply your settings.

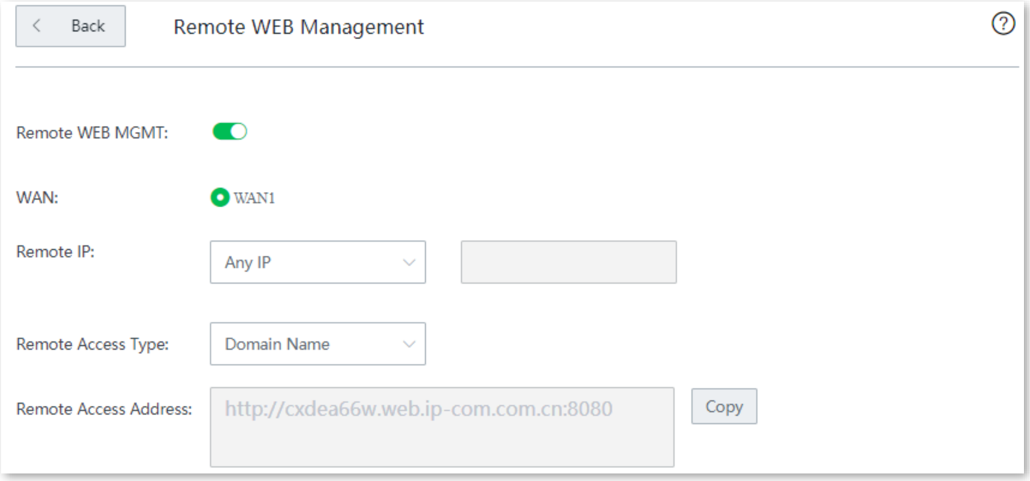
----End

3.10.5 Remote WEB management

Overview

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

Navigate to **More** > **Remote WEB Management** to enter the page. By default, this function is disabled.



Remote WEB MGMT: ●

WAN: ● WAN1

Remote IP: Any IP

Remote Access Type: Domain Name

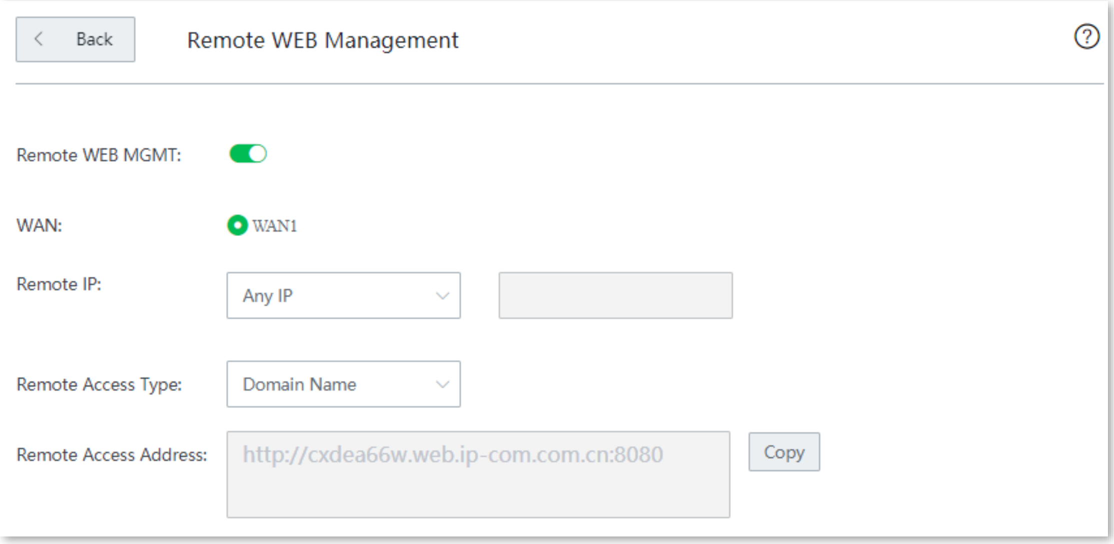
Remote Access Address: http://cxdea66w.web.ip-com.com.cn:8080

Parameter description

Parameter	Description
Remote WEB MGMT	It specifies whether or not to enable the remote WEB MGMT function.
Remote IP	It specifies the IP address of the remote host which is allowed to access the web UI of the node. – **Any IP**: It indicates that all internet users can access the web UI of the node. For security of your network, select this option only when necessary. – **Specified IP**: It indicates that only the host with the specified public IP address is allowed to access the web UI of node remotely. If the host for remote access is in an intranet, enter the public IP address of the computer's gateway here.
Remote Access Address	It specifies the domain name used by the remote host for accessing the web UI of the node.

Configure remote WEB managemnent

1. Navigate to **More** > **Remote WEB Management**, and enable this function.
2. Set the **Remote IP** to either of **Any IP** or **Specified IP**.
3. Select **Remote Access Type** to either of **Domain Name** or **IP Address**.
4. Click **Save** to apply your settings.



Remote WEB Management

Remote WEB MGMT: ●

WAN: ● WAN1

Remote IP: Any IP

Remote Access Type: Domain Name

Remote Access Address: http://cxdea66w.web.ip-com.com.cn:8080

----End

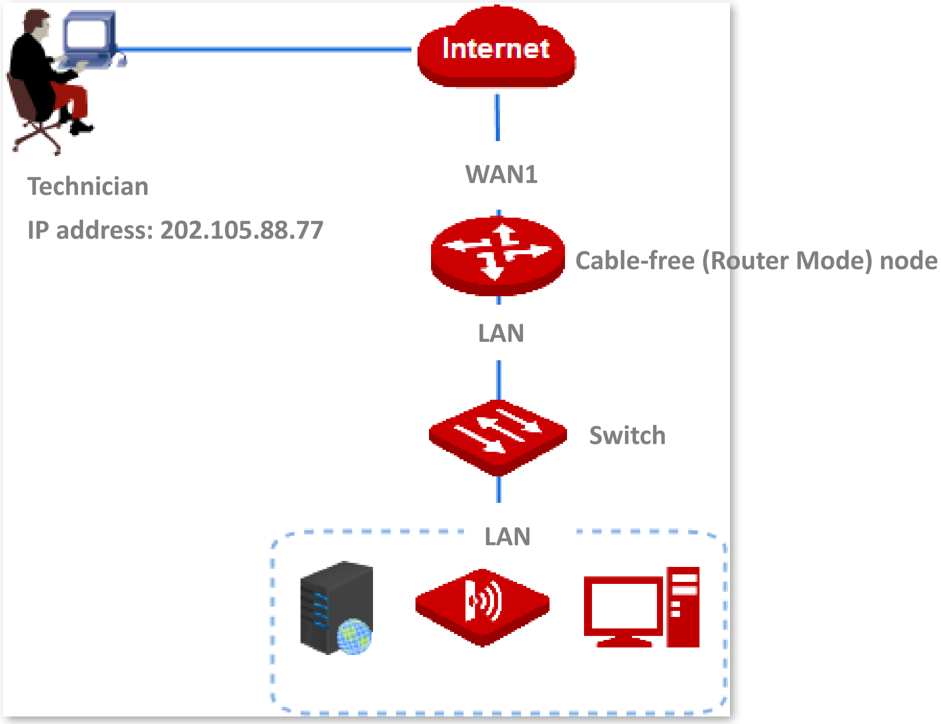
Example of configuring remote web management

Networking requirement

An enterprise uses EW12 to deploy its network. And its network administrator needs to seek an IP-COM technician to solve a problem remotely.

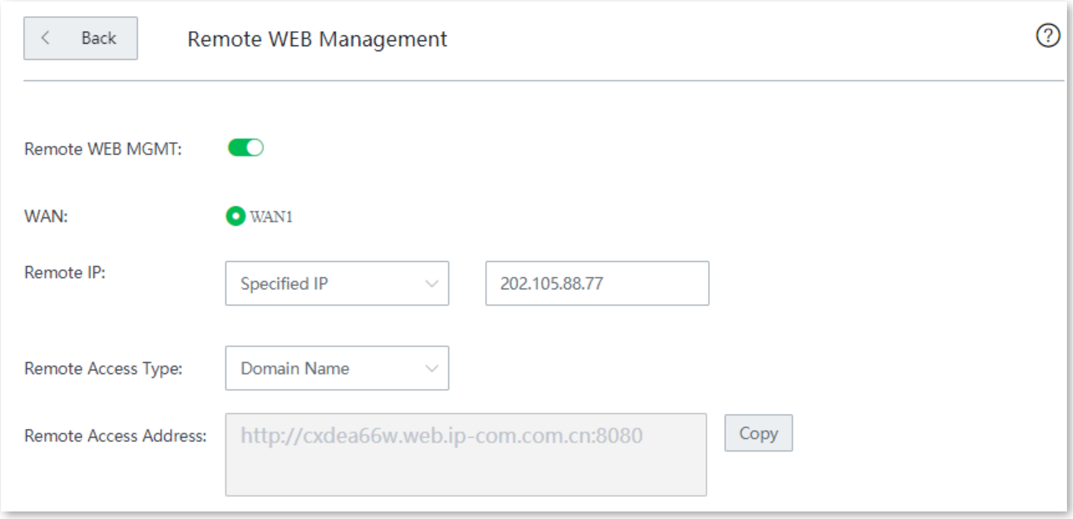
Solutions

Remote web management function can meet this requirement.



Configuration procedure

1. Navigate to **More** > **Remote WEB Management**, and enable this function.
2. Select **Specific IP** in the Remote IP bar. Enter the IP address of the technician's computer, which is **202.105.88.77** in this example.
3. Select **Remote Access Type** to **Domain Name**.
4. Click **Save** to apply your settings.
5. Click **Copy** and send the **Remote Access Address** to the IP-COM technician.



Remote WEB Management

Remote WEB MGMT: ●

WAN: ● WAN1

Remote IP: Specified IP 202.105.88.77

Remote Access Type: Domain Name

Remote Access Address: http://cxdea66w.web.ip-com.com.cn:8080

----End

Verification

IP-COM technician with a computer IP address 202.105.88.77 can use http://cxdea66w.web.ip-com.com.cn:8080 to access the web UI of the node remotely.

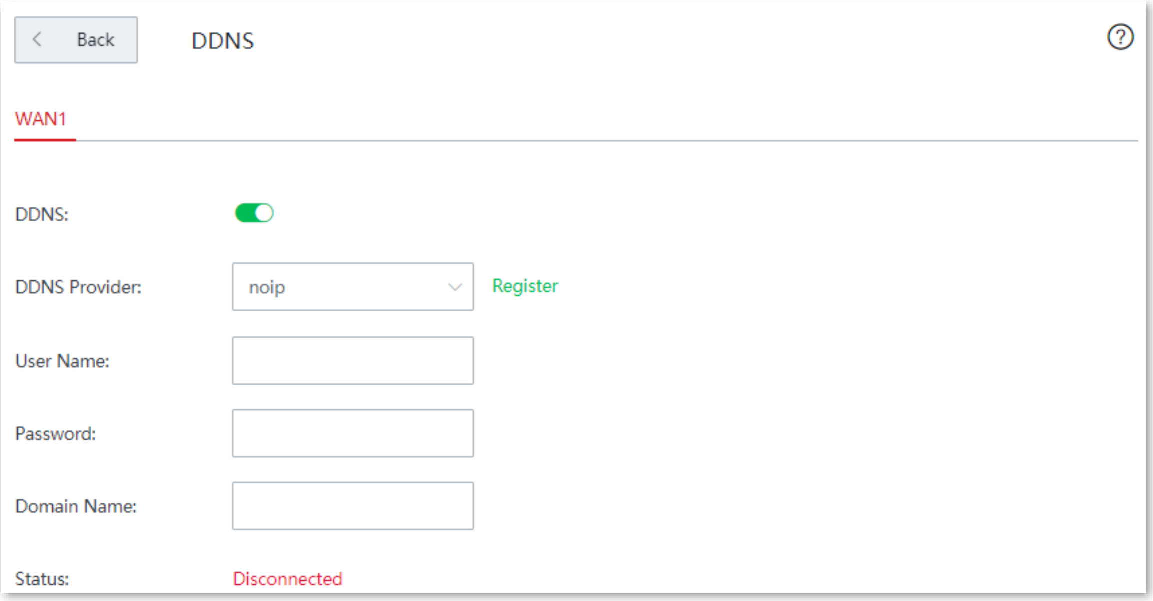
3.10.6 DDNS

Overview

DDNS is short for Dynamic Domain Name Server. It detects when your IP address changes and maps your dynamic IP address to a static domain name. When the service is running, the DDNS client on the node sends its current WAN port IP address to the DDNS server. Then the server updates the mapping between the domain name and the IP address in the database to implement dynamic domain name resolution. If you enable this function, the node sends its WAN IP address to the specified DDNS server when the WAN IP address is changed and the DDNS server maps the changed WAN IP address to a specified static domain name. This enables internet users to access services on your LAN through the static domain name instead of the changeable WAN IP address.

This function always interworks with other functions, such as Port Forwarding, and DMZ Host.

Navigate to **More** > **DDNS** to enter the page. By default, this function is disabled. Click ○ to ● and enable the function. See the following figure.



DDNS: ●

DDNS Provider: noip

User Name:

Password:

Domain Name:

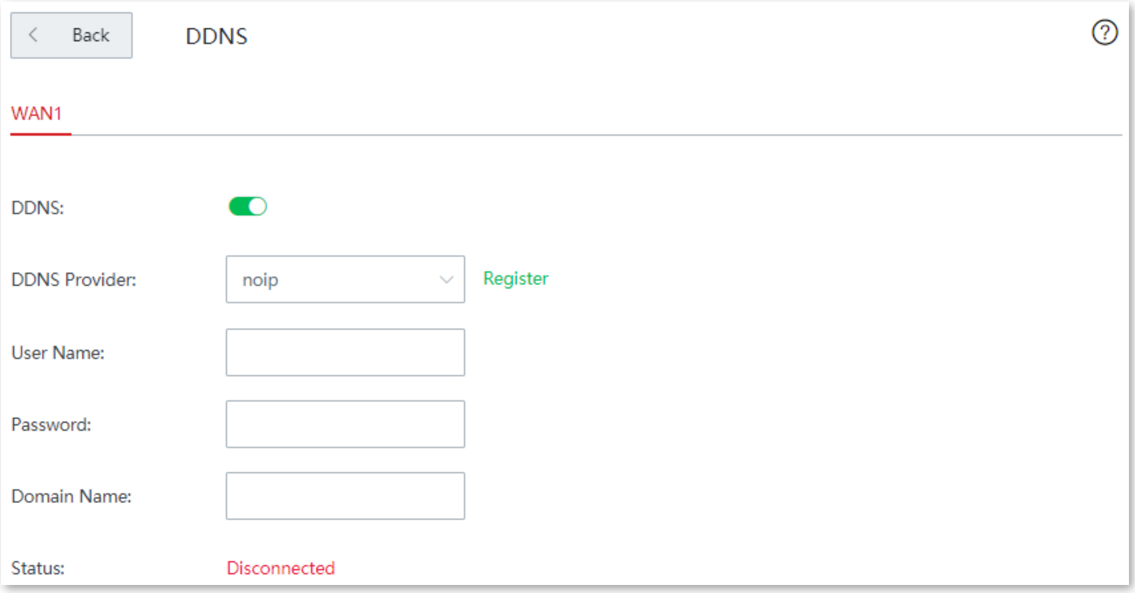
Status: Disconnected

Parameter description

Parameter	Description
DDNS	It specifies whether or not to enable the DDNS function.
DDNS Provider	It specifies the DDNS provider. The node supports **noip**, **dyndns**, **oray**, and **gnway**.
User Name	It specifies the user name used to log in to a DDNS provider. It is registered on the website of the provider.
Password	It specifies the password used to log in to a DDNS provider.
Domain Name	It specifies the domain name obtained from a DDNS provider.
Status	It specifies the DDNS service status.

Configure DDNS

1. Navigate to **More** > **DDNS** to enter the page.
2. Set **DDNS** to ●.
3. Set the related parameters.
4. Click **Save**.



DDNS: ●

DDNS Provider: noip

Register

User Name:

Password:

Domain Name:

Status: Disconnected

----End

Example of configuring DDNS

Networking requirement

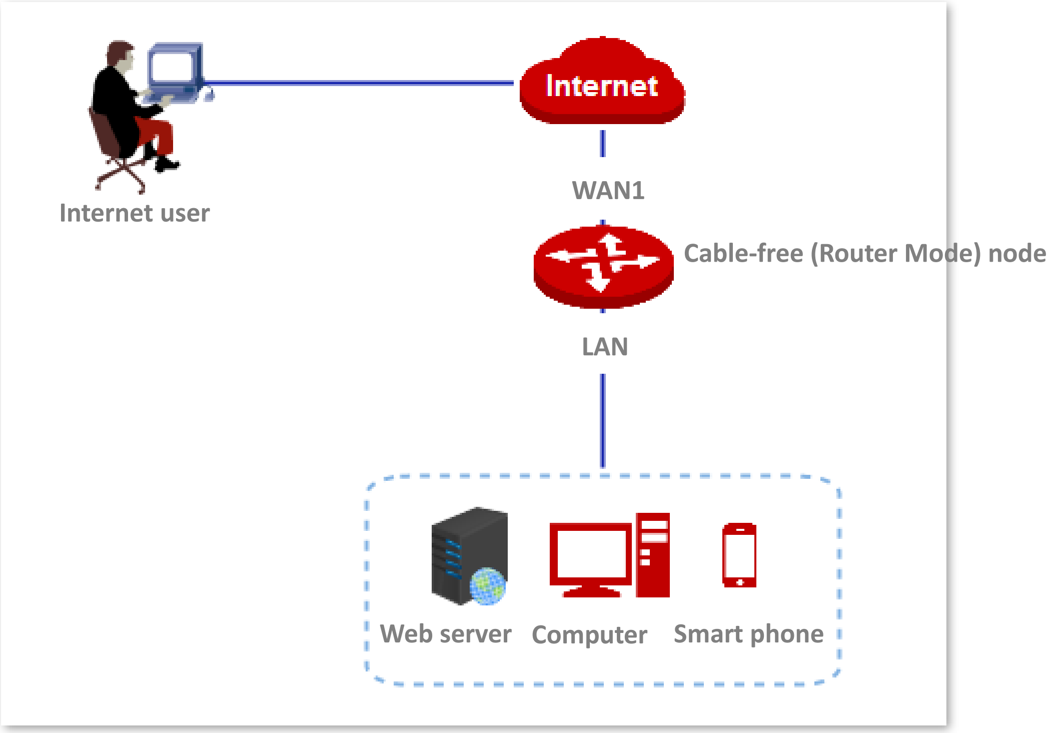
An enterprise uses EW12 to deploy its WLAN network. The node is connected to the internet. Now the enterprise establishes a web server and wants to be accessed by internet users. Thus, when employees are not in the enterprise, they can also access the web server. Assume that the external port is 80.

Solutions

The DDNS in combination with address reservation and port forwarding can meet this requirement.

Assume that the related information is shown as below:

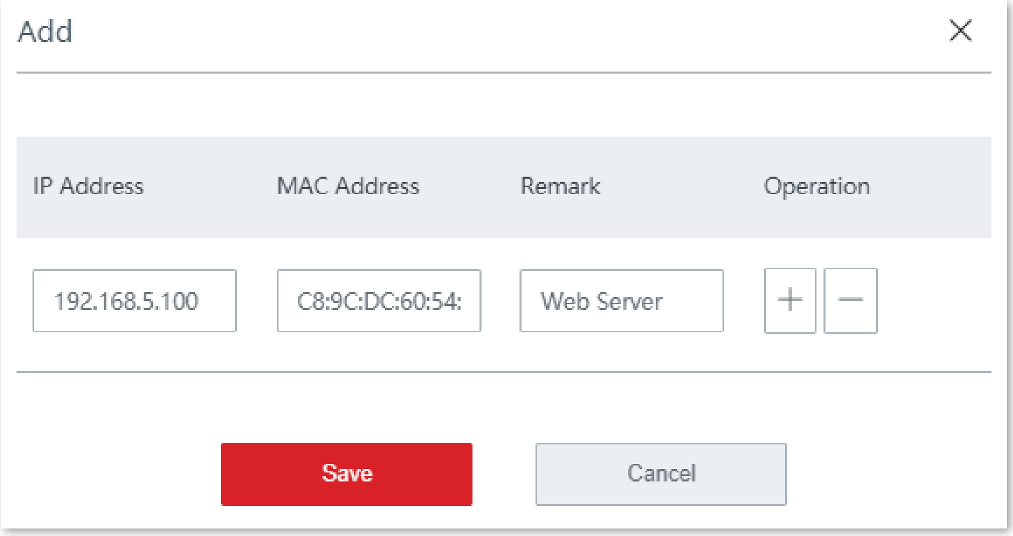
- IP address of the web server: 192.168.5.100
- MAC address of the host that runs the web server: C8:9C:DC:60:54:69
- Service port: 80
- IP address of WAN1 port: 202.105.11.22



Configuration procedure

1. Reserve an IP address for the host of the web server.

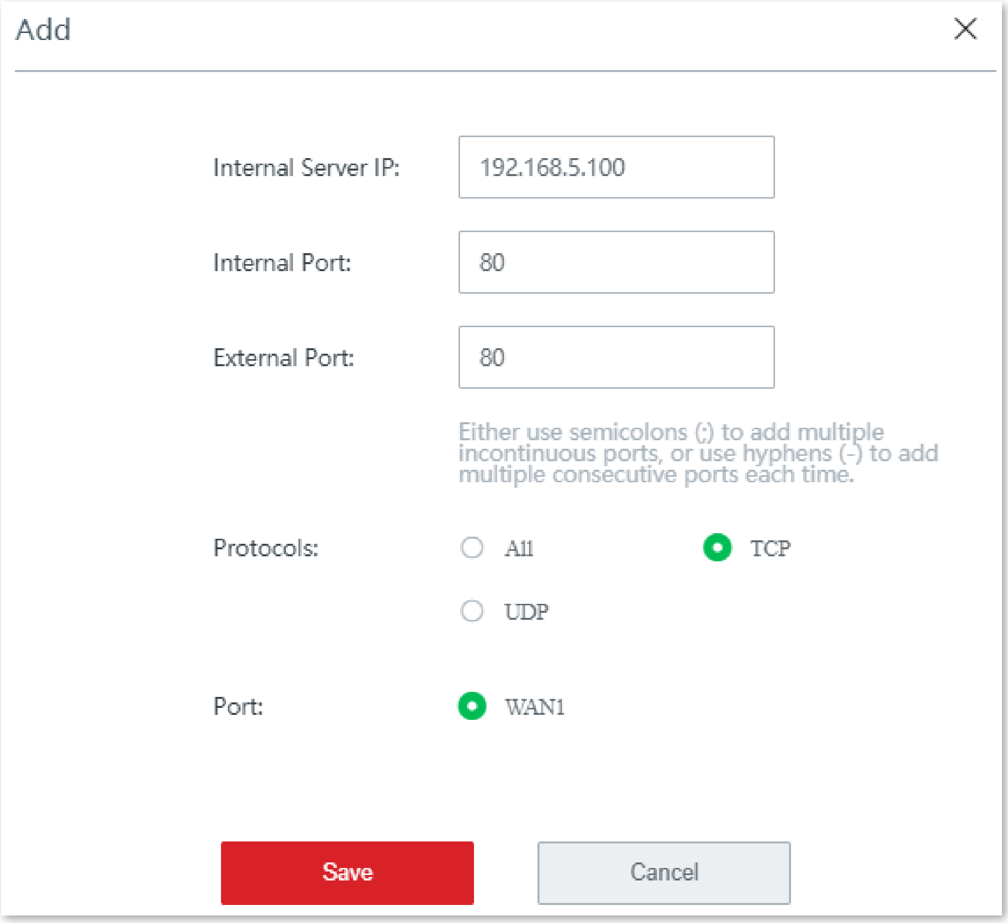
   Click **Address Reservation** to reserve the IP address. Refer to Address reservation for detailed configuration procedures.


Add

IP Address	MAC Address	Remark	Operation
192.168.5.100	C8:9C:DC:60:54:	Web Server	+ −

2. Configure port forwarding.

   Navigate to **More** > **Port Forwarding**, and add a rule. Refer to Port forwarding for detailed configuration procedures.



Internal Server IP: 192.168.5.100

Internal Port: 80

External Port: 80

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

Protocols: ○ All ● TCP ○ UDP

Port: ● WAN1

3. Configure DDNS.

(1) Register a domain name.

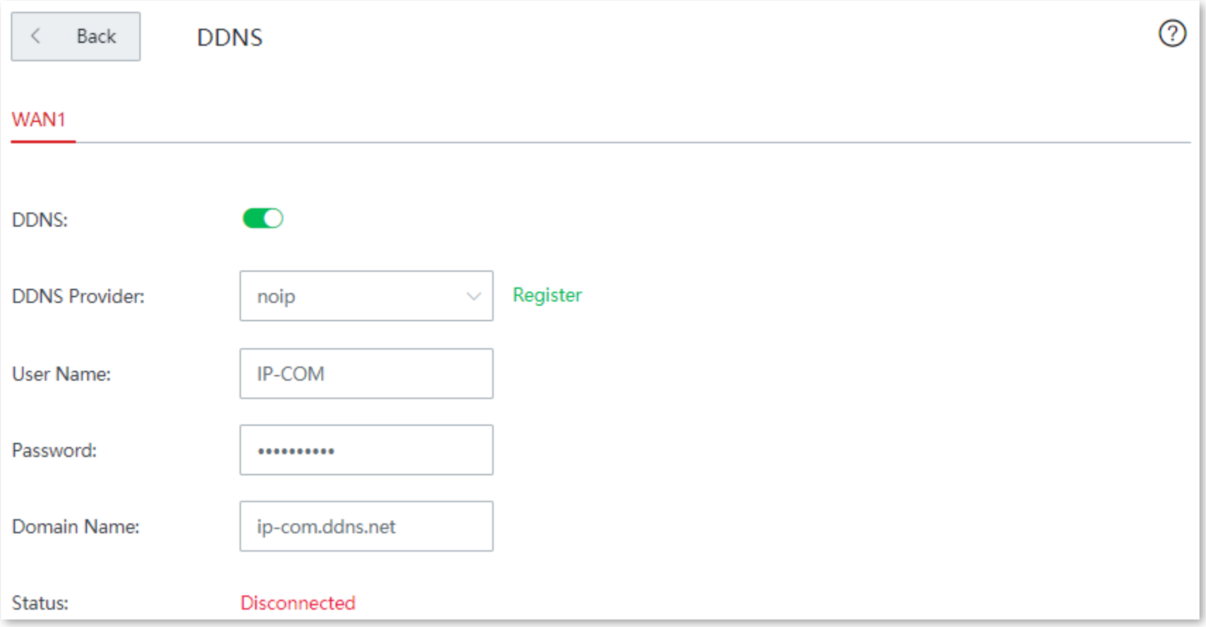
Select the DDNS provider from the drop-down list menu, which is **noip** in this example, and click Register next to the menu to register a domain name.

(2) Set the DDNS-related parameters.

Log in to the web UI of the node, navigate to **More** > **DDNS**, and enable this DDNS function.

Enter the DDNS-related parameters you registered on your DDNS provider’s website.

(3) Click **Save** to apply your settings.



DDNS: ●

DDNS Provider: noip Register

User Name: IP-COM

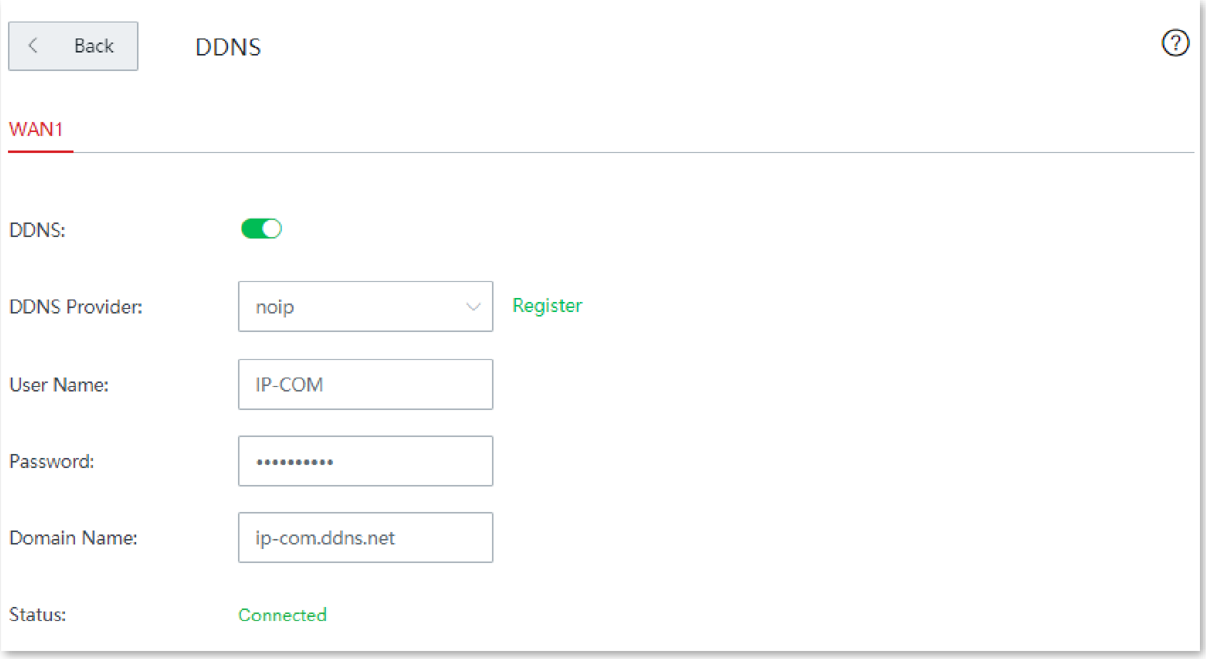
Password: ••••••••••

Domain Name: ip-com.ddns.net

Status: Disconnected

----End

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



DDNS: ●

DDNS Provider: noip Register

User Name: IP-COM

Password: ••••••••••

Domain Name: ip-com.ddns.net

Status: Connected

Verification

Users on the internet can successfully access the Intranet server by using **Intranet Service Application Layer Protocol Name**://**WAN port domain name**: **extranet port**, which is http://cxdea66w.web.ip-com.com.cn:8080 in this example. If the outer network port is remained default when users configure port forwarding, the access address does not have to add the outer network port number.

Tip

If you cannot access the web server after configuration, try the following methods to resolve the problem:

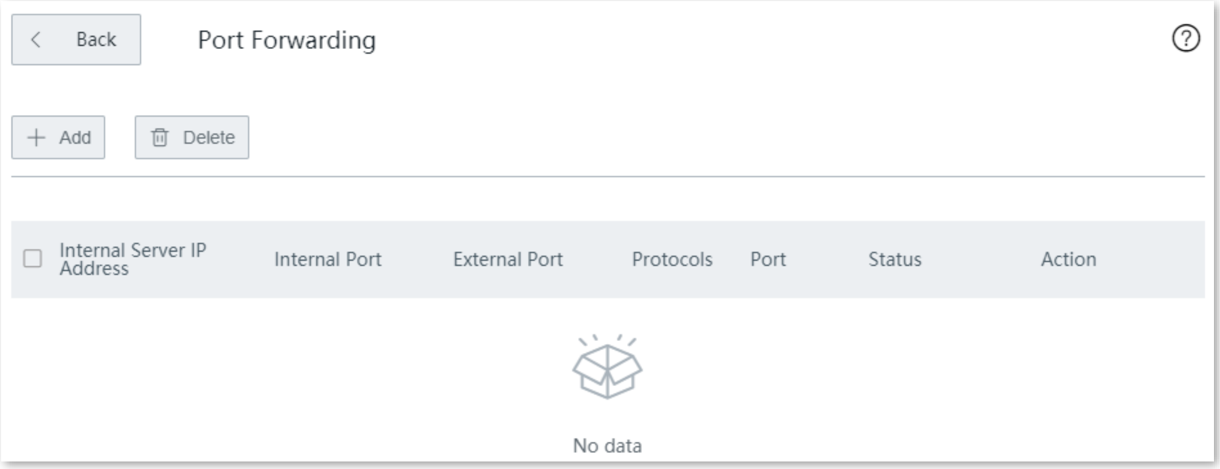
- Make sure the node's WAN port gets the public network IP address. The commonly used address categories of IPV4 include A, B and C. The private network addresses of A are 10.0.0.0-10.255.255.255. The private network address of class B address is 172.16.0.0-172.31.255.255; The private network addresses of class C addresses are 192.168.0.0-192.168.255.255.
- Make sure that the Intranet port you filled in is the correct service port.
- It may be that the system firewall, anti-virus software and security guard on the LAN server block the access of internet users. Please disable these programs and try again.

3.10.7 Port forwarding

Overview

By default, internet users cannot access any service on any of your local hosts. If you want to enable internet users to access a particular service on a local host, enable this function and specify the IP address and service port of the local host. This can also prevent local network from being attacked.

Navigate to **More** > **Port forwarding**. See the following figure.



Port Forwarding

□ Internal Server IP Address	Internal Port	External Port	Protocols	Port	Status	Action

No data

Parameter description

Parameter	Description
Internal Server IP Address	It specifies the IP address of a local computer that runs a specified service.
Internal Port	It specifies the service port of the LAN server.
External Port	It specifies the port for internet users to access a specified service.
Protocol	It specifies the service protocol. All indicates both TCP and UDP. Select All if you are uncertain about the service type.
Port	It specifies the physical WAN port that internet users use to access the specified service.
Status	It specifies whether the rule is enabled or not.
Operation	You can perform the following operations to the corresponding rule: ✎: Click it to edit the rule. 🗑: Click it to delete the rule.

Configure port forwarding

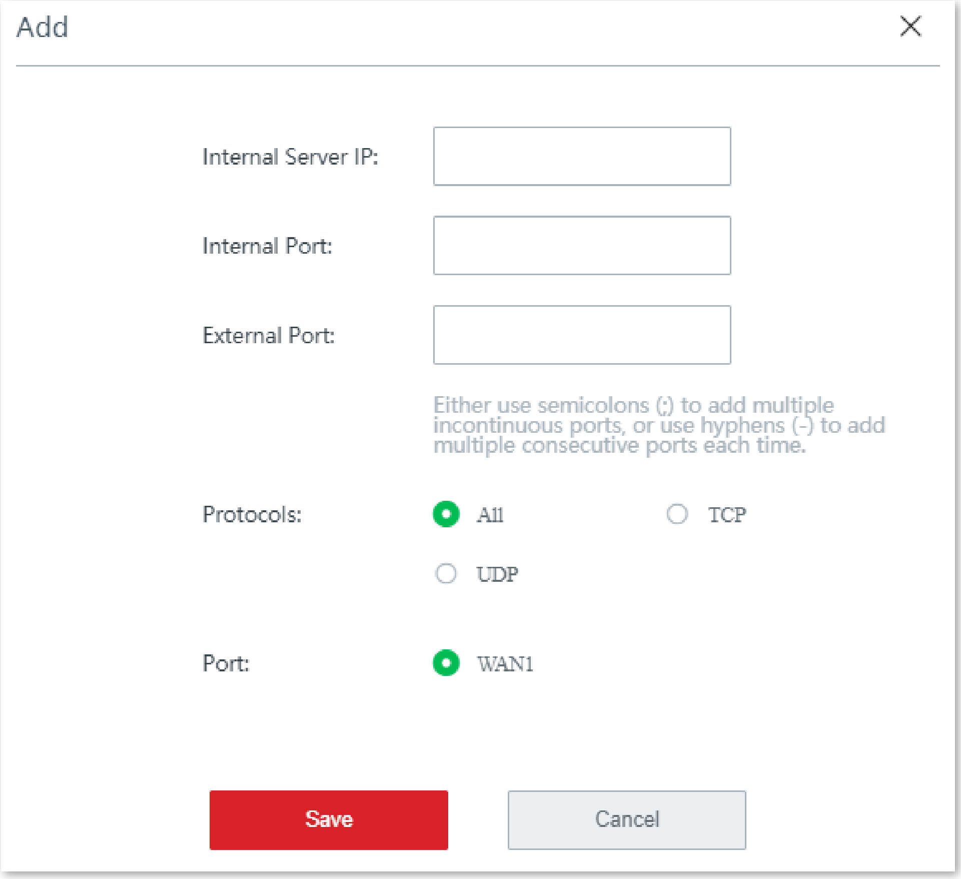
Tip

A dynamic IP address will disable the port forwarding rule. To use this function and make the rule always effective, set a reserved IP address for the specified local host.

Some programs, such as firewall, antivirus software, and security guard, may hinder internet users to access the local service. Disable them when necessary.

The WAN IP address of the node must be a public IP address. If it is a private IP address, the function does not take effect. Commonly-used IPv4 private IP addresses include 10.0.0.0 to 10.255.255.255, 172.16.0.0 to 172.31.255.255, and 192.168.0.0 to 192.168.255.255.

1. Navigate to **More** > **Port Forwarding** to enter the page.
2. Click **+Add**. The **Add** configuration window appears.
3. Set required parameters.
4. Click **Save** to apply your settings.



Internal Server IP:

Internal Port:

External Port:

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

Protocols: ● All ○ TCP ○ UDP

Port: ● WAN1

----End

Example of configuring a port forwarding rule

Networking requirement

An enterprise uses EW12 to deploy its WLAN network. The node is connected to the internet. Now the enterprise establishes a web server and wants to enable its employees to access the web server through the internet.

Solutions

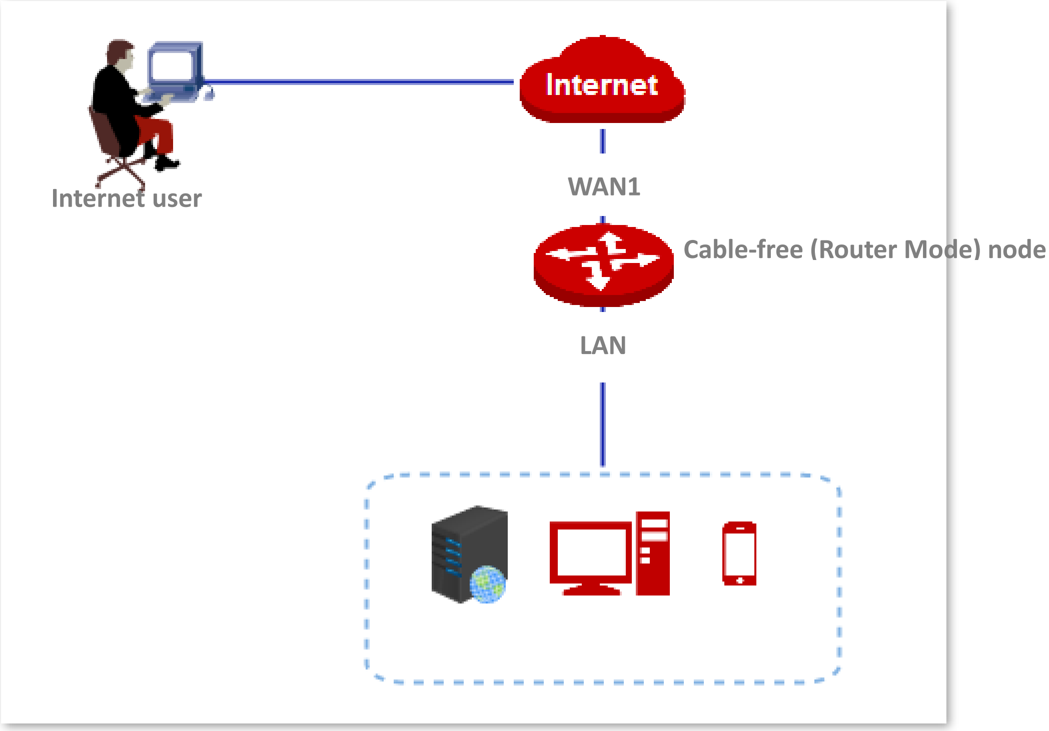
The port forwarding function in combination with the address reservation function can meet this requirement.

Assume that the related information is shown as below:

- IP address of the web server: 192.168.5.100
- MAC address of the host that runs the web server: C8:9C:DC:60:54:69
- Service port: 80
- IP address of WAN1: 202.105.11.22:80

Tip

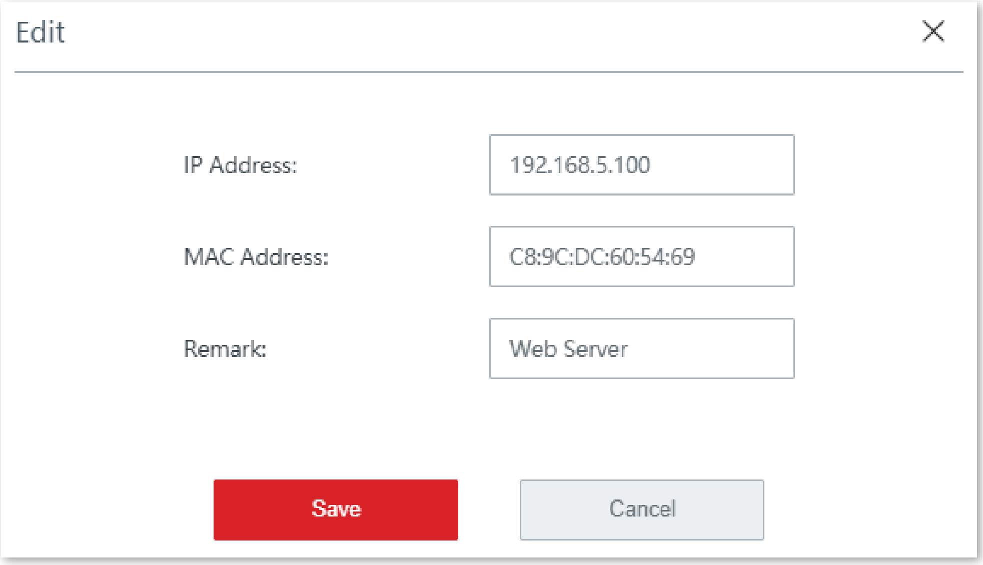
The WAN IP address of the node must be a public IP address. If it is a private IP address, the function does not take effect. Commonly-used IPv4 private IP addresses include 10.0.0.0 to 10.255.255.255, 172.16.0.0 to 172.31.255.255, and 192.168.0.0 to 192.168.255.255.



Configuration procedure

1. Reserve the IP address to the host.

   Navigate to **Address Reservation** to reserve the IP address. Refer to Address reservation for detailed configuration procedures.



Edit

IP Address: 192.168.5.100

MAC Address: C8:9C:DC:60:54:69

Remark: Web Server

2. Configuring port forwarding.

   (1) Navigate to **More** > **Port Forwarding** to enter the configuration page.

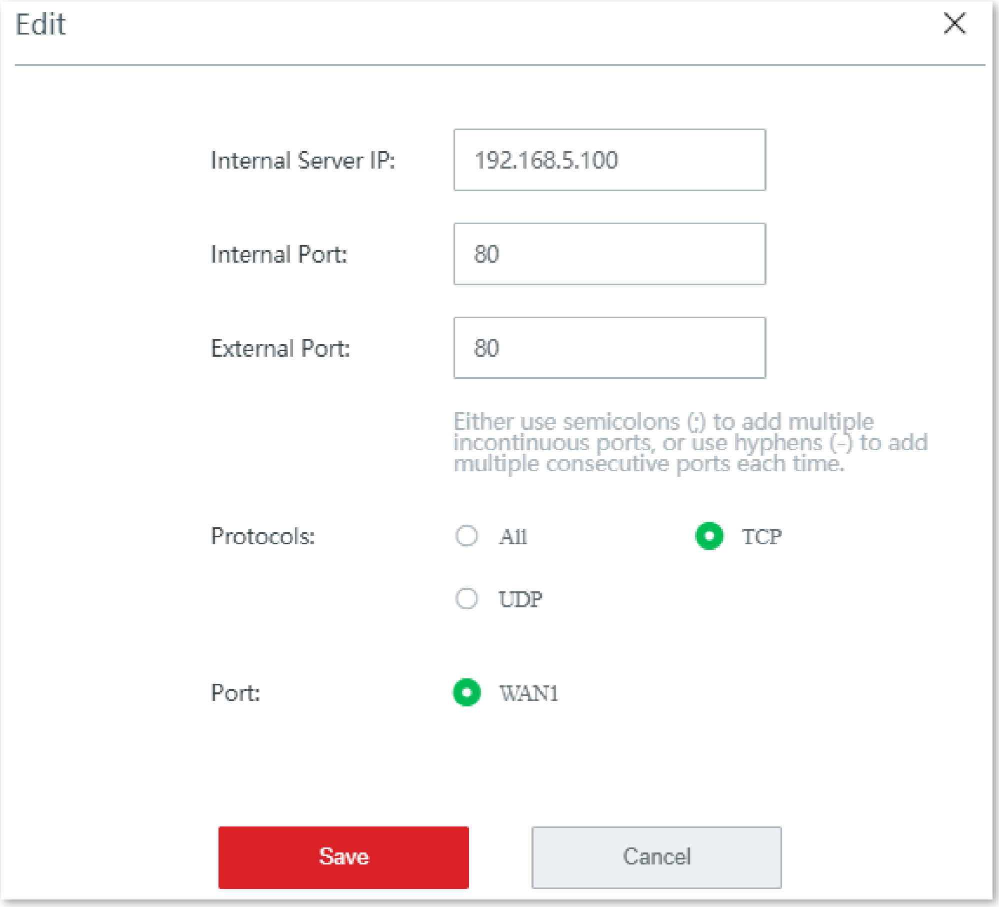
   (2) Click **+Add**. The **Add** configuration window appears.

   (3) Set the **Internal Server IP** to **192.168.5.100**.

   (4) Set both the **Internal Port** and **External Port** to **80** respectively.

   (5) Set the **Protocols** to **TCP**.

   (6) Click **Save**.



Internal Server IP: 192.168.5.100

Internal Port: 80

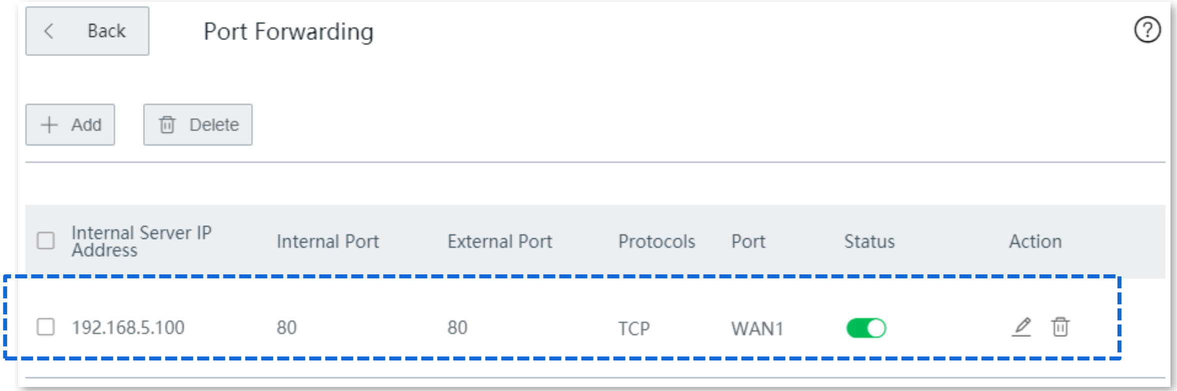
External Port: 80

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

Protocols: ○ All ● TCP ○ UDP

Port: ● WAN1

The rule is added successfully. See the following figure.



□	Internal Server IP Address	Internal Port	External Port	Protocols	Port	Status	Action
□	192.168.5.100	80	80	TCP	WAN1	●	✎ 🗑

Verification

Internet users can use http://202.105.11.22:80 to access the web server.

- **http** indicates intranet service protocol name.
- **202.105.11.22** is the IP address of the WAN1 port.
- **80** is the external port number.

In addition, If the WAN port is configured with DDNS, you can use intranet service protocol name://domain name:external port to access the web server.

Tip

If you cannot access the web server after configuration, try the following methods to resolve the problem:

– Make sure the router WAN port gets the public network IP address. The commonly used address categories of IPV4 include A, B and C. The private network addresses of A are 10.0.0.0-10.255.255.255. The private network address of class B address is 172.16.0.0-172.31.255.255; The private network addresses of class C addresses are 192.168.0.0-192.168.255.255.
– Make sure that the Intranet port you filled in is the correct service port.
– It may be that the system firewall, anti-virus software and security guard on the LAN server block the access of internet users. Please disable these programs and try again.

3.10.8 DMZ host

Overview

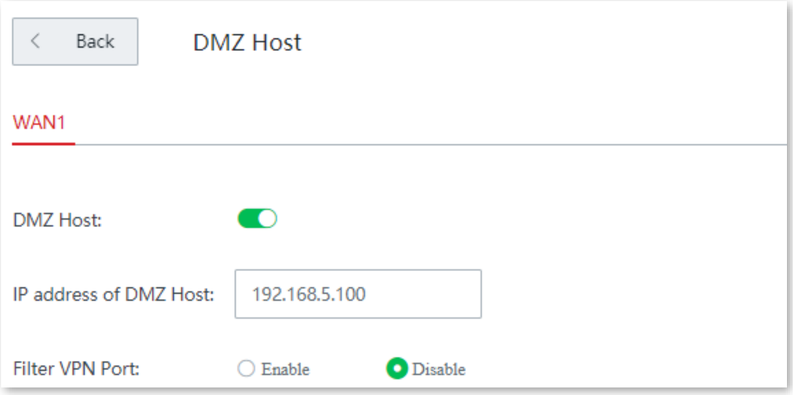
By default, internet users cannot access any service on any local host. If you want internet users to access all services on a local host, enable this function. It is especially used for video conferences and online games. You can set a local computer running these programs to be a DMZ host for better video conferencing and online gaming experience.

Note

If you set a local computer as a DMZ host, the computer is not protected by the firewall of the router and may be easily attacked by internet users. Therefore, enable the DMZ host function only when necessary.

Navigate to **More** > **DMZ Host** to enter the page. By default, this function is disabled.

To enable the function, switch ○ to ●.



DMZ Host: ●

IP address of DMZ Host: 192.168.5.100

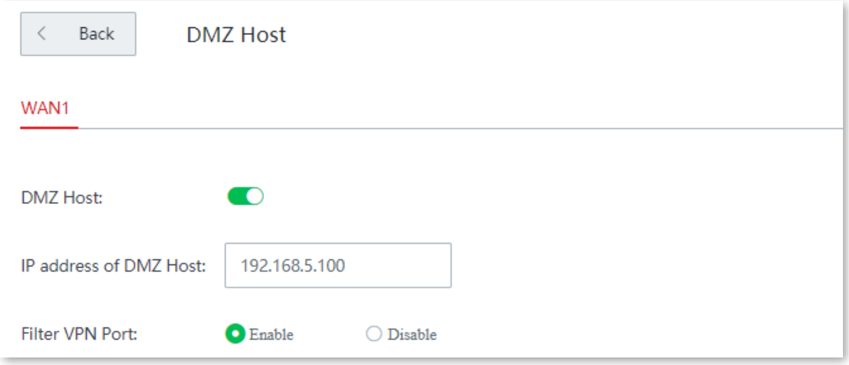
Filter VPN Port: ○ Enable ● Disable

Parameter description

Parameter	Description
DMZ Host	It specifies whether to enable the DMZ function.
IP address of DMZ Host	It specifies the IP address of the DMZ host.
Filter VPN Port	It is used to specify whether to filter the VPN port if DMZ is enabled for a host. By default, it is disabled. – **Enable**: When the DMZ host and Filter VPN Port are enabled, VPN requests are responded by the router. – **Disable**: When the DMZ host and Filter VPN Port are disabled, VPN requests are not responded by the router.

Configure DMZ host

1. Navigate to **More** > **DMZ Host**, and enable this function of WAN port.
2. Enter the IP address of the DMZ host.
3. Enable **Filter VPN Port** as required.
4. Click **Save** to apply your settings.



DMZ Host: ●

IP address of DMZ Host: 192.168.5.100

Filter VPN Port: ● Enable ○ Disable

----End

Example of configuring DMZ host

Networking requirement

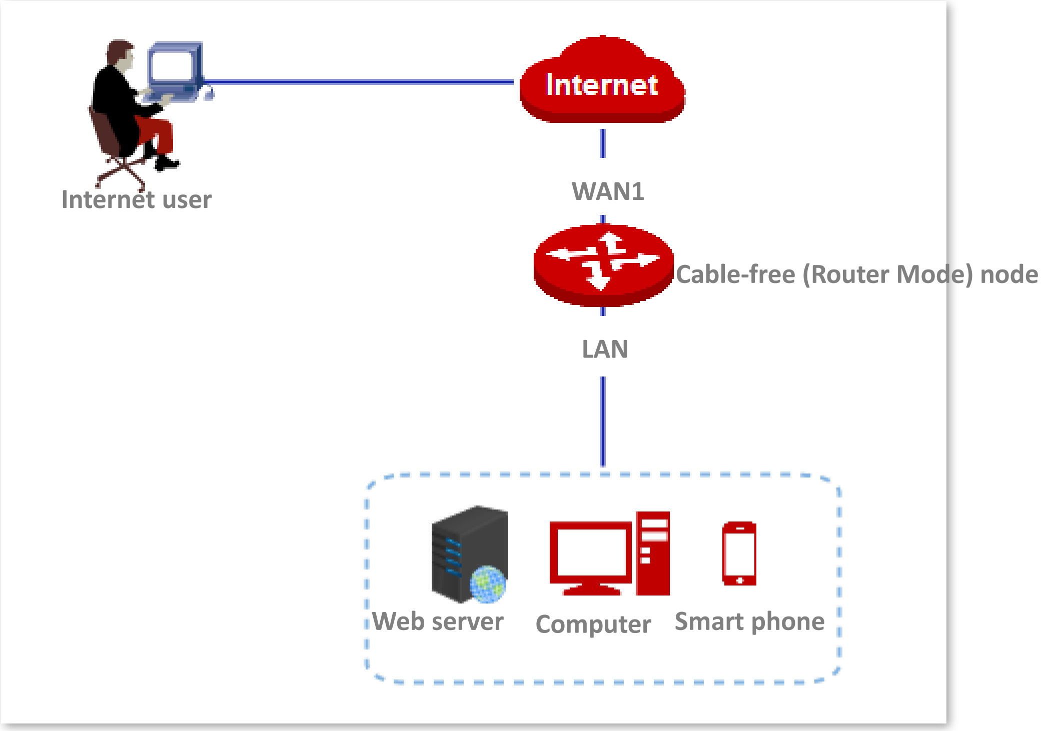
An enterprise uses EW12 to deploy its WLAN network. The device is connected to the internet. Now the enterprise establishes a web server and wants to enable its employees to access the web server through the internet.

Solutions

You can use the DMZ host and address reservation to meet this requirement.

Assume that the related information is shown as below:

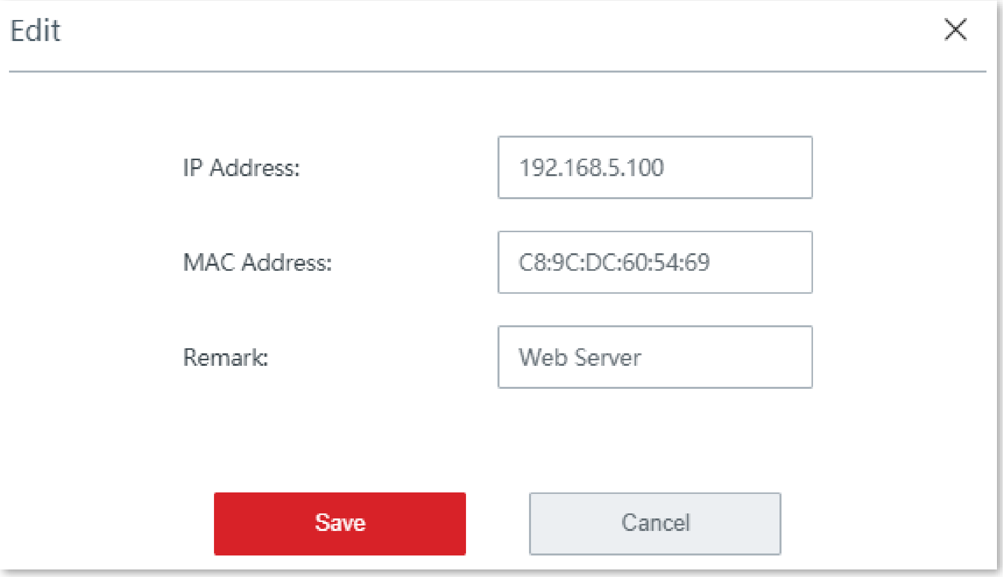
- IP address of the web server: 192.168.5.100
- MAC address of the host that runs the web server: C8:9C:DC:60:54:69
- Port: 80
- WAN IP address of the device is 202.105.11.22



Configuration procedure

1. Reserve the IP address to the host

   Navigate to **Address Reservation** to reserve the IP address. Refer to Address reservation for detailed configuration procedures.



IP Address: 192.168.5.100

MAC Address: C8:9C:DC:60:54:69

Remark: Web Server

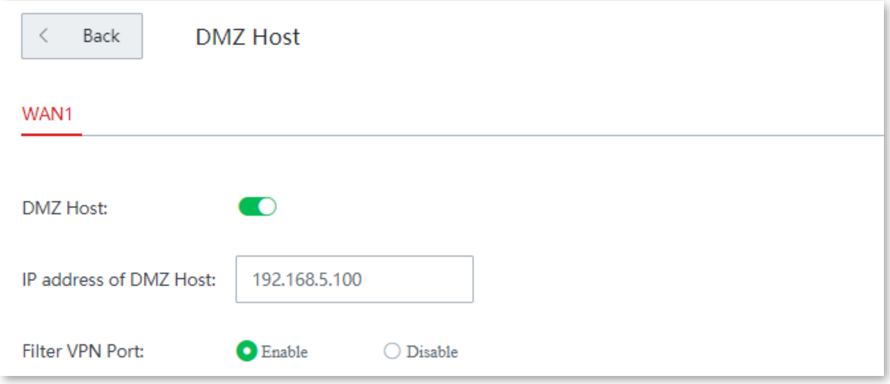
2. Configure DMZ host.

   (1) Navigate to **More** > **DMZ Host**, and enable this function of the corresponding WAN port.

   (2) Enter the IP address of the DMZ host, which is **192.168.5.100** in this example.

   (3) Enable **Filter VPN Port**.

   (4) Click **Save** to apply your settings.



DMZ Host: ●

IP address of DMZ Host: 192.168.5.100

Filter VPN Port: ● Enable ○ Disable

----End

Verification

Internet users can use http://202.105.11.22:80 to access the web server.

- **http** indicates intranet service protocol name.
- **202.105.11.22** is the IP address of the WAN1 port.
- **80** is the external port number.

In addition, If the corresponding WAN port is configured with DDNS, you can use intranet service protocol name://domain name:external port to access the web server.

Tip

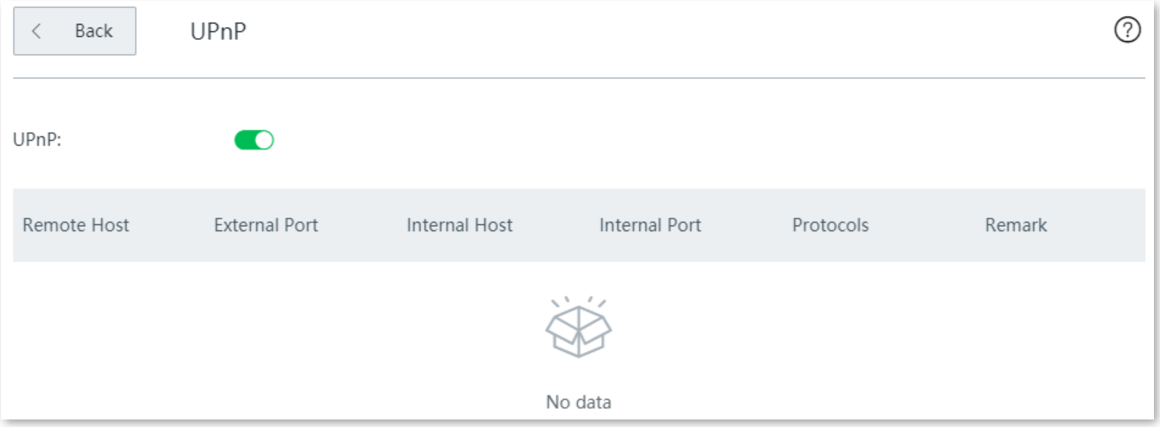
If you cannot access the web server after configuration, try the following methods to resolve the problem:

- Make sure the device’s WAN port gets the public network IP address. The commonly used address categories of IPV4 include A, B and C. The private network addresses of A are 10.0.0.0-10.255.255.255. The private network address of class B address is 172.16.0.0-172.31.255.255; The private network addresses of class C addresses are 192.168.0.0-192.168.255.255.
- It may be that the system firewall, anti-virus software and security guard on the LAN server block the access of internet users. Please disable these programs and try again.

3.10.9 UPnP

This function enables the cable-free node to implement automatic port forwarding by automatically detecting UPnP-based application programs and enabling ports on the router for the applications.

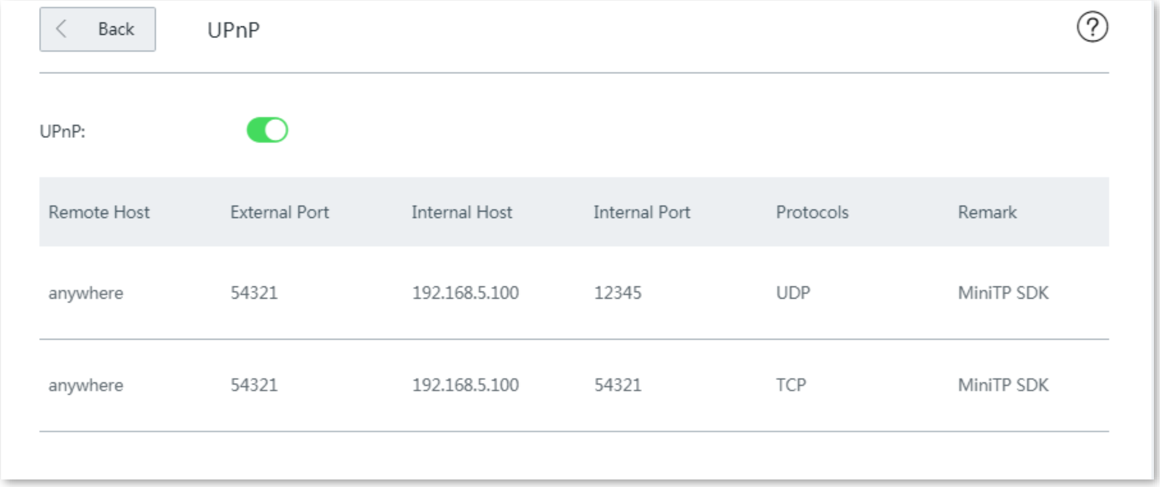
Navigate to **More** > **UPnP** to enter the page. By default, this function is enabled. See the following figure.



Remote Host	External Port	Internal Host	Internal Port	Protocols	Remark

No data

With this function enabled, when UPnP-based programs, such as BitComet and AnyChat, are running on the local network, the external and internal mapping relationships are displayed on the page.

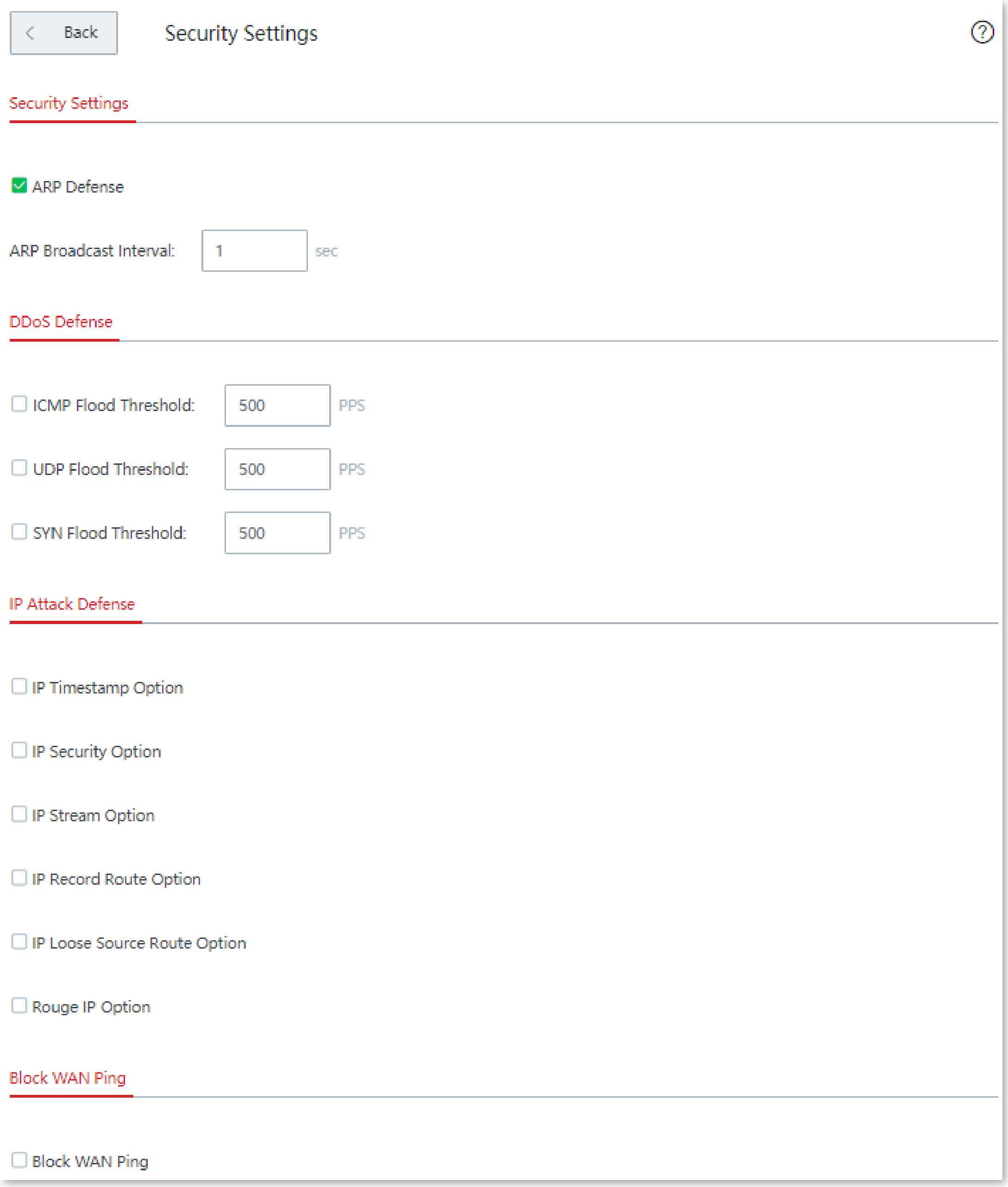


Remote Host	External Port	Internal Host	Internal Port	Protocols	Remark
anywhere	54321	192.168.5.100	12345	UDP	MiniTP SDK
anywhere	54321	192.168.5.100	54321	TCP	MiniTP SDK

3.10.10 Security settings

The Cable-Free (Router Mode) supports ARP Defense, DDoS Defense, IP Attack Defense, and Block WAN Ping.

- **ARP Defense:** This function can identify the ARP spoofing in the local network, and record the MAC addresses of the attack.
- **DDoS Defense**: DDoS attack, that is Distributed Denial of Service Attack, makes network resource unavailable to its intended users. The node can block DDoS attack, including ICMP Flood, UDP Flood, and SYN Flood attackers.
- **IP Attack Defense**: With this function enabled, the node can intercept some packets with specified IP options as required. These IP options include IP Timestamp Option, IP Security Option, IP Stream Option, IP Record Route Option, IP Loose Source Route Option and illegal IP options.
- **Block WAN Ping:** With this function enabled, users cannot ping the WAN IP address of the node over the internet.



Security Settings

Security Settings

☑ ARP Defense

ARP Broadcast Interval: 1 sec

DDoS Defense

□ ICMP Flood Threshold: 500 PPS

□ UDP Flood Threshold: 500 PPS

□ SYN Flood Threshold: 500 PPS

IP Attack Defense

□ IP Timestamp Option

□ IP Security Option

□ IP Stream Option

□ IP Record Route Option

□ IP Loose Source Route Option

□ Rouge IP Option

Block WAN Ping

□ Block WAN Ping

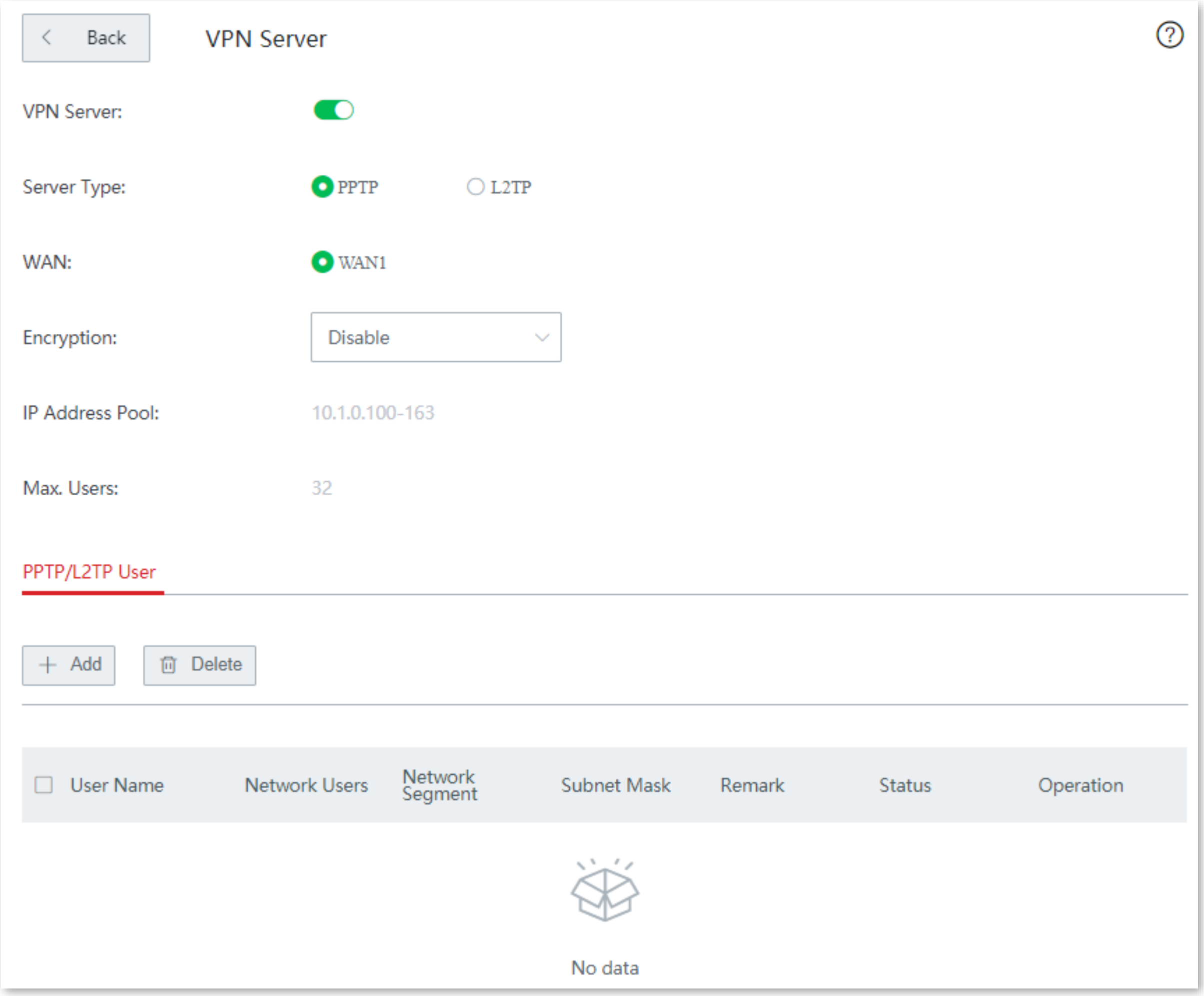
Parameter description

Parameter		Description
ARP Defense	ARP Defense	It specifies whether to enable the ARP defense function.
	ARP Broadcast Interval	It specifies the interval for sending ARP inquiry messages.
DDoS Defense	ICMP Flood Threshold	It specifies that if ICMP request packets from a same host in LAN received by the node exceed the threshold within 1 second, the node suffers ICMP flood attack.
	UDP Flood Threshold	It specifies that If UDP request packets from a same host in LAN received by the node exceed the threshold within 1 second, the node suffers UDP flood attack.
	SYN Flood Threshold	SYN Flood Attack. If SYN request packets from a same host in LAN received by the node exceed the threshold within 1 second, the node suffers SYN flood attack.
IP Attack Defense	IP Timestamp Option	With this function enabled, the node blocks IP packets that contain the internet timestamp option in the local network.
	IP Security Option	With this function enabled, the node blocks IP packets that contain the Security option in the local network.
	IP Stream Option	With this function enabled, the node blocks IP packets that contain the Stream ID option in the local network.
	IP Record Route Option	With this function enabled, the node blocks IP packets that contain the Record Route option in the local network.
	IP Loose Source Route Option	With this function enabled, the node blocks IP packets that contain the Loose Source Route option in the local network.
	Rouge IP Option	With this function enabled, the node blocks IP packets that fail to pass integrity and correctness check in the local network.
Block WAN Ping		It specifies whether to enable the Block WAN Ping function. By default, it is disabled.

3.10.11 VPN server

Overview

The Cable-Free (Router Mode) node supports PPTP server and L2TP server. To enter the configuration page, navigate to **More** > **VPN Server** and enable this function.



VPN Server

VPN Server: ●

Server Type: ● PPTP ○ L2TP

WAN: ● WAN1

Encryption: Disable

IP Address Pool: 10.1.0.100-163

Max. Users: 32

PPTP/L2TP User

□ User Name	Network Users	Network Segment	Subnet Mask	Remark	Status	Operation

No data

Parameter description

Parameter	Description
VPN Server	It is used to enable or disable the PPTP/L2TP VPN server function.
Server Type	It specifies the VPN server type that the Cable-Free (Router Mode) node supports, including: – **PPTP:** The Point to Point Tunneling Protocol. If PPTP is selected, the peer VPN client should be set to PPTP client. – **L2TP:** Layer 2 Tunneling Protocol. If L2TP is selected, the peer VPN client should be set to L2TP client.

Parameter	Description
WAN	It specifies the WAN port of the node for setting up a VPN connection.
Encryption	It specifies whether to enable 128-bit data encryption. This parameter only appears when PPTP is selected. The value of this parameter must be consistent with that of the client. Otherwise, the client is unable to communicate with the server.
IP Address Pool	It specifies IP address range that the PPTP/L2TP clients can obtain from the VPN server to be connected.
Max. Users	It specifies the maximum number of VPN clients allowed to be connected to the PPTP/L2TP server. The value is fixed to **32**.
User Name	It specifies the user name and password used to dial in a PPTP/L2TP VPN connection.
Password	
Network Users	It specifies the password for the user name used to dial in PPTP/L2TP VPN connection.
Network Segment	It specifies whether a VPN client is a network. – **Yes**: The network segment and subnet mask of the VPN client are required. – **No**: The VPN client is a computer.
Subnet Mask	It specifies subnet mask of the LAN of a VPN client in case that the client is a network.
Remark	It specifies a short description about the corresponding account. You are recommended to add a remark to your VPN account for later management.
Status	It specifies whether or the corresponding rule is enabled.

Configure the node as a PPTP/L2TP VPN server

Tip

To establish a VPN connection, the VPN server and VPN client should be configured consistently on **Client Type**, **WAN** and **Encryption**.

1. Enable the PPTP/L2TP server function.

(1) Navigate to **More** > **VPN Server**, enable **VPN Server**, and click **Save**.

(2) Set the VPN server to **PPTP** or **L2TP** as required.

Tip

The peer VPN client should use the same type.

(3) Select the egress WAN port of the tunnel between a PPTP/L2TP server and PPTP/L2TP clients.

Tip

If the egress WAN port you selected is set to a DMZ host, enable the port's **Filter VPN Port** first by navigating to **More** > **DMZ Host**.

The IP address of the egress WAN port must be a public IP address. The following lists private IP address range of IPv4. IP addresses that are not in the range are public IP addresses.

– Category A: 10.0.0.0-10.255.255.255

– Category B: 172.16.0.0—172.31.255.255

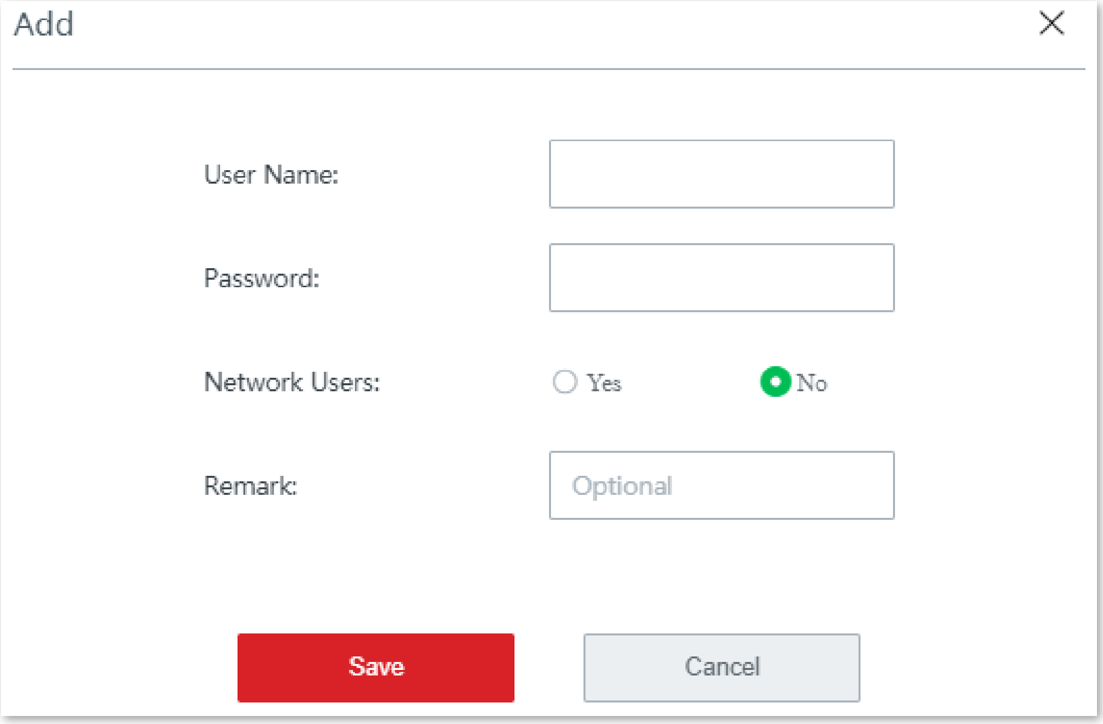
– Category C: 192.168.0.0-192.168.255.255

2. Add a PPTP/L2TP user.

(1) Navigate to **More** > **VPN Server**, and go to the **PPTP/L2TP User** module.

(2) Click **+Add**. The **Add** page appears.

(3) Set required parameters, and click **Save**.



Add

User Name:

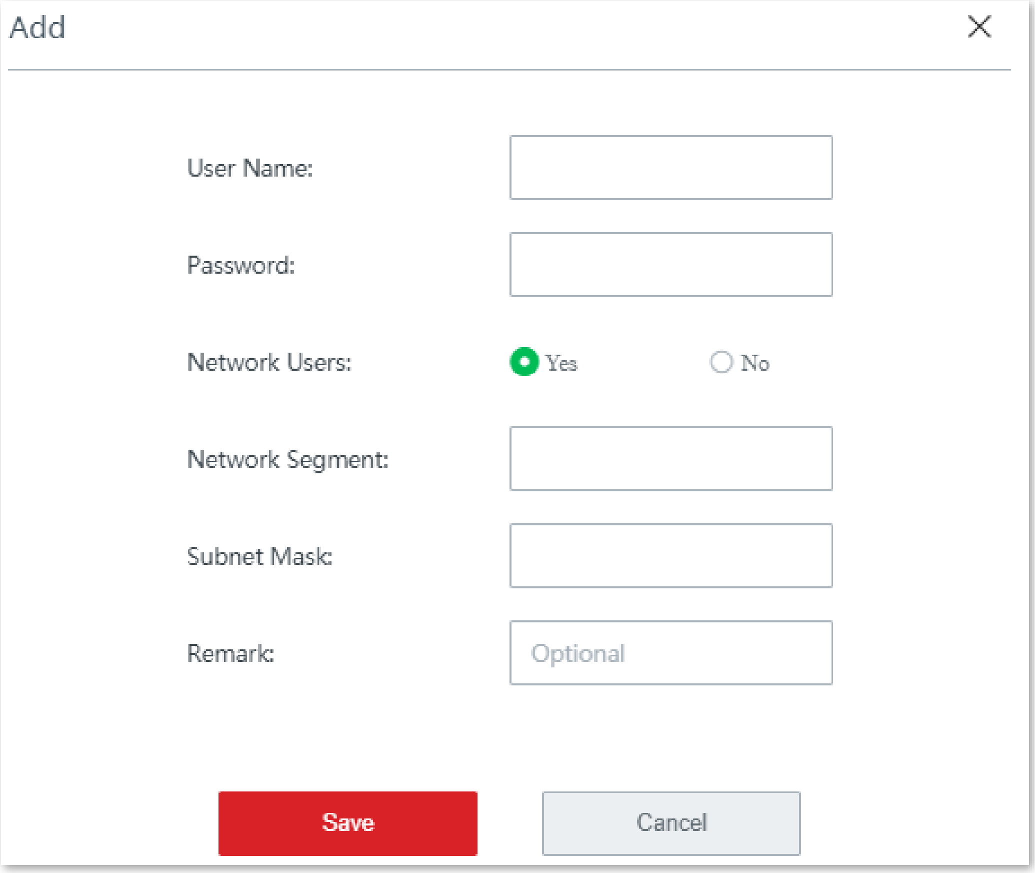
Password:

Network Users: ○ Yes ● No

Remark: Optional

3. Choose **Yes** and set the parameters.

4. Click **Save**.



Add

User Name:

Password:

Network Users: ● Yes ○ No

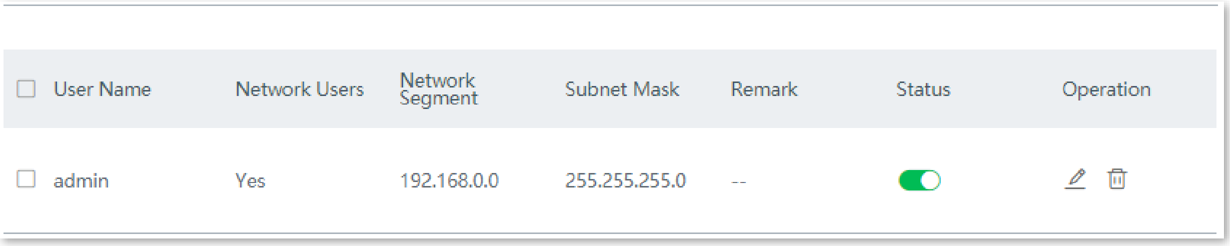
Network Segment:

Subnet Mask:

Remark: Optional

----End

Added successfully. See the following figure.



□	User Name	Network Users	Network Segment	Subnet Mask	Remark	Status	Operation
□	admin	Yes	192.168.0.0	255.255.255.0	--	●	✎ 🗑

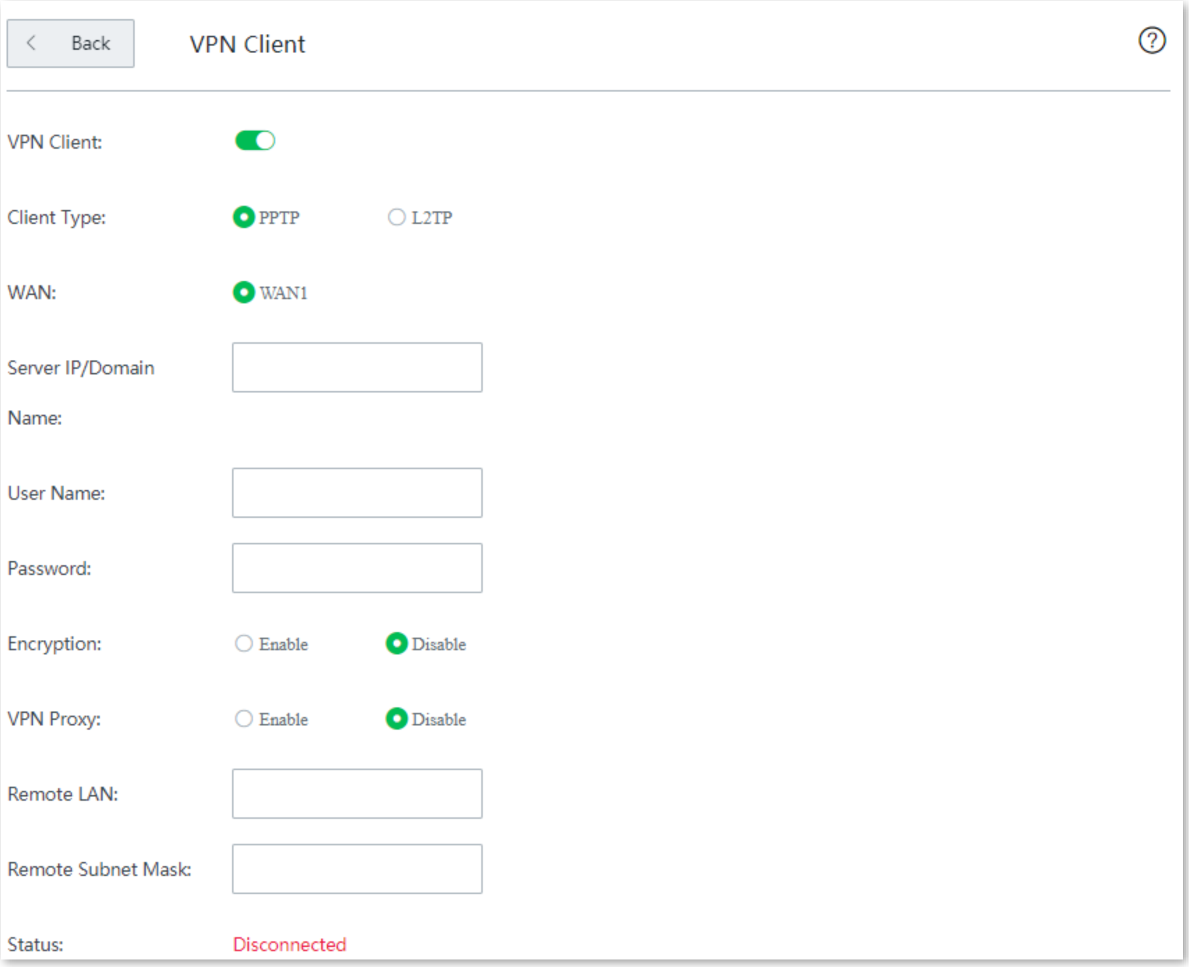
Parameter description

Parameter		Description
PPTP/L2TP Server	Server Status	It specifies whether the PPTP/L2TP server of the device is enabled.
	Type	It specifies the VPN server type of the node. PPTP and L2TP are supported.
	WAN Port	It specifies the WAN port of the node for setting up a VPN connection.
	Encryption	It 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.
	IPSec	It specifies that only L2TP server supports this parameter. Whether the IPSec is enabled. To enable the IPSec, you have to create an IPSec tunnel first by choosing VPN > IPSec, and set the Encapsulation Mode to Transmission.
	Address Pool	It specifies the IP address range of PPTP/L2TP clients assigned by the VPN server to be connected.
	Max. Users	It specifies the maximum number of VPN clients allowed to be connected to the PPTP/L2TP server. The value is fixed to 32.
PPTP/L2TP User	User Name	It specifies the user name used to dial in a VPN (PPTP/L2TP) connection.
	Password	It specifies the password for the user name used to dial in VPN connection.
	Network	It specifies whether a VPN client is a network. – - **Yes**: The network segment and subnet mask of the VPN client are required. – - **No**: The VPN client is a computer.
	Network Segment	It specifies the LAN network segment of a VPN client in case that the client is a network.
	Subnet Mask	It specifies the subnet mask of the LAN of a VPN client in case that the client is a network.
	Remark	It is used to add remark to your VPN account for later management.

3.10.12 VPN client

Overview

To enter the configuration page, navigate to **More** > **VPN Client**. By default, this function is disabled. After you enable the function, the following page appears.



< Back

VPN Client

VPN Client: ●

Client Type: ● PPTP ○ L2TP

WAN: ● WAN1

Server IP/Domain Name:

User Name:

Password:

Encryption: ○ Enable ● Disable

VPN Proxy: ○ Enable ● Disable

Remote LAN:

Remote Subnet Mask:

Status: Disconnected

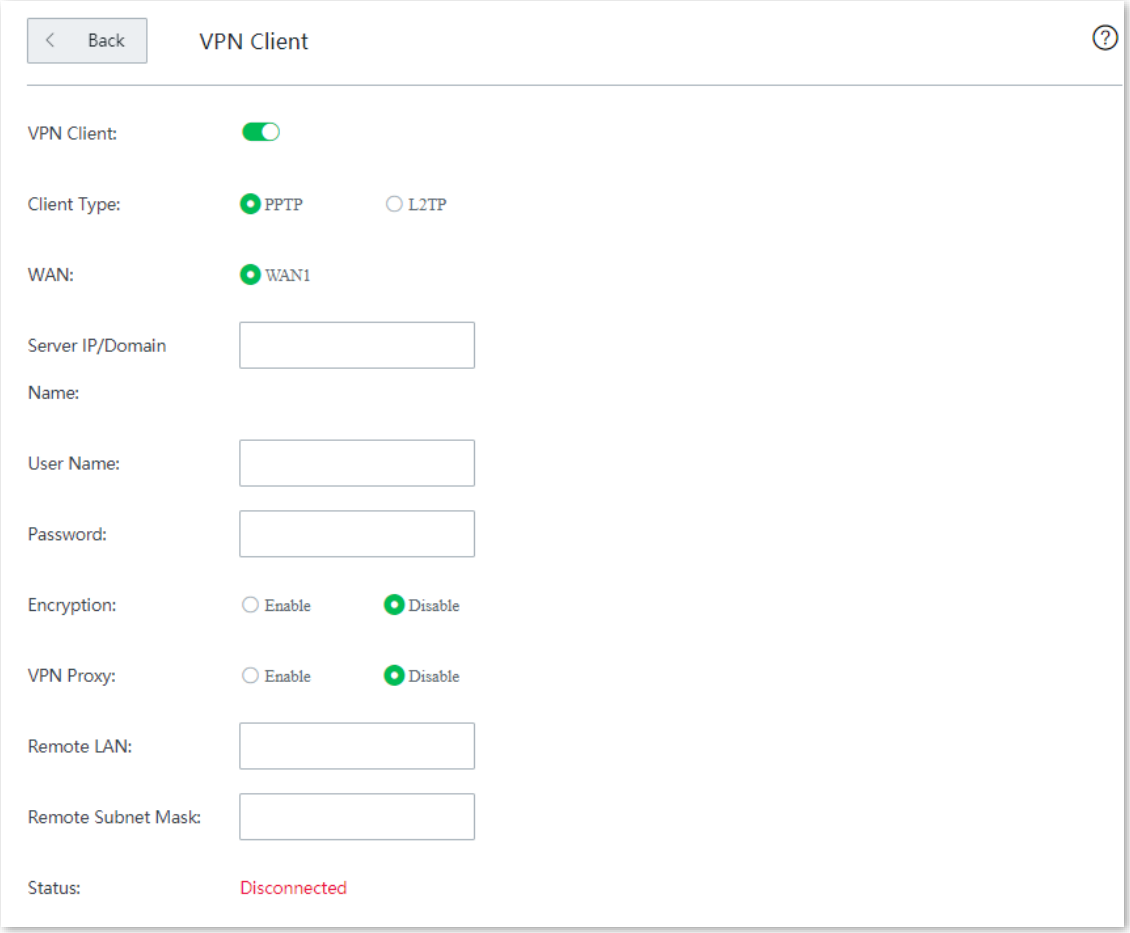
Parameter description

Parameter	Description
Client Type	It specifies VPN server type of the node. PPTP and L2TP are supported.
WAN	It specifies WAN port of the PPTP/L2TP client for setting up a connection with the PPTP/L2TP server.
Server IP Address/Domain Name	It specifies IP address or domain name of the VPN server.
User Name	It specifies username of the PPTP/L2TP account. It is assigned by the VPN server to be connected.

Parameter	Description
Password	It specifies password for the corresponding PPTP/L2TP account. It is assigned by the VPN server to be connected.
Encryption	It 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 Proxy	With this function enabled, clients on the LAN can obtain IP addresses from the VPN server to access the internet.
Remote LAN	It specifies the network segment of the LAN of the PPTP/L2TP server.
Remote Subnet Mask	It specifies the subnet mask of the LAN of the PPTP/L2TP server.
Status	It specifies the current connection status of the VPN client.
Obtained IP Address	It specifies the IP address obtained by the VPN client.

Configure the node as a PPTP/L2TP VPN client

1. Navigate to **More** > **VPN Client**, and enable the function.



VPN Client: ●

Client Type: ● PPTP ○ L2TP

WAN: ● WAN1

Server IP/Domain Name:

User Name:

Password:

Encryption: ○ Enable ● Disable

VPN Proxy: ○ Enable ● Disable

Remote LAN:

Remote Subnet Mask:

Status: Disconnected

2. Set required parameters.

Tip

– **Client Type**, **WAN**, and **Encryption** should be identical with its peer VPN server.
– Click ? on the upper-right corner on the page to get the detailed explanation to the parameters here.

3. Click **Save** to apply your settings.

----End

3.10.13 IPSec

Overview

A Virtual Private Network (VPN) is a dedicated network set up on a public network (usually the internet). A VPN is a logically network without physical connections. Using the VPN technology, you can enable your branch employees to remotely share resources and access your HQ LAN, and meanwhile ensure that the resources are not accessible to other public network users. The device supports IPSec VPN.

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 IPSec transmission data. IPSec supports **Tunnel** mode.

Tunnel mode is most commonly used between gateways. With tunnel mode, the entire original IP packet is protected by IPSec. This means IPSec wraps the original packet, encrypts it, adds a new IP header and sends it to the other side of the VPN tunnel (IPSec peer).

- **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 tampering and peeping.

- **IPSec peer**

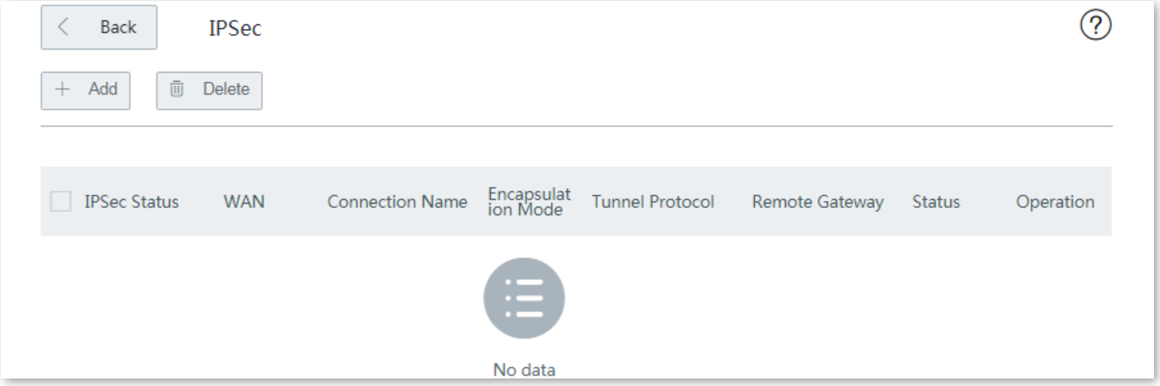
The two IPSec terminals are called IPSec peers. The two peers (security gateways) can securely exchange data only after a Security Association (SA) is set up between them.

- **SA**

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

- A triplet {SPI, Destination IP address, Security protocol identifier} is used as a unique ID.
- An SA specifies the protocol, algorithm, and key for processing packets.
- Each IPsec SA is unidirectional with a life cycle.
- An SA can be created manually or generated automatically using internet Key Exchange (IKE).

Navigate to **More** > **IPSec** to enter the page.



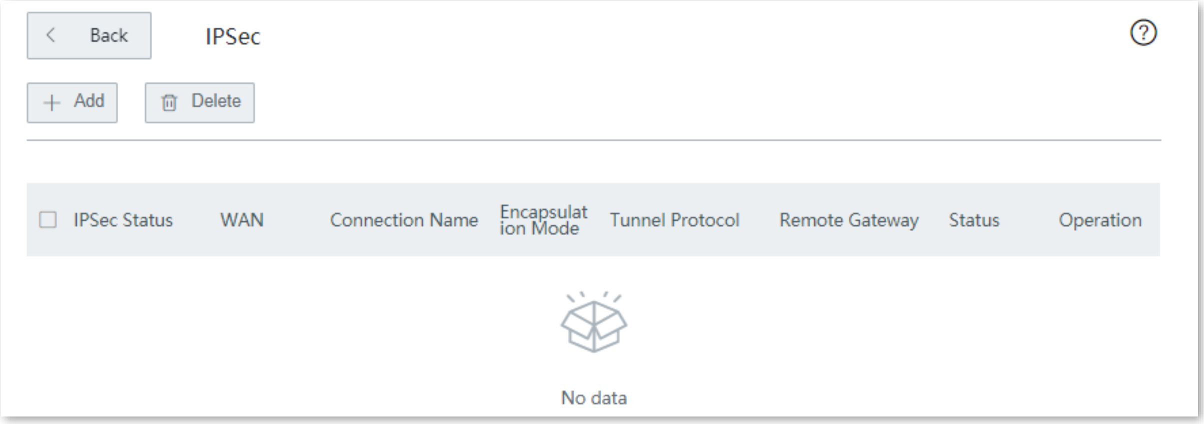
Parameter description

Parameters	Description
IPSec Status	It specifies whether the IPSec connection is connected or not.
WAN	It specifies the local WAN port assigned to the IPSec function. The IP address of the WAN port must be set as the value of Remote Gateway of the IPSec peer.
Connection Name	It specifies the name of the IPSec connection.
Encapsulation Mode	It specifies the IPSec data encapsulation mode.
Tunnel Protocol	It specifies the tunnel protocol of the IPSec rule. By default, it is ESP. ESP: It indicates the Encapsulating Security Payload (ESP) protocol 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: It indicates the Authentication Header (AH) protocol used for verifying data integrity. If a packet is tampered during transmission, the receiver discards it during data integrity verification. AH+ESP: It indicates that the function features both AH and ESP.

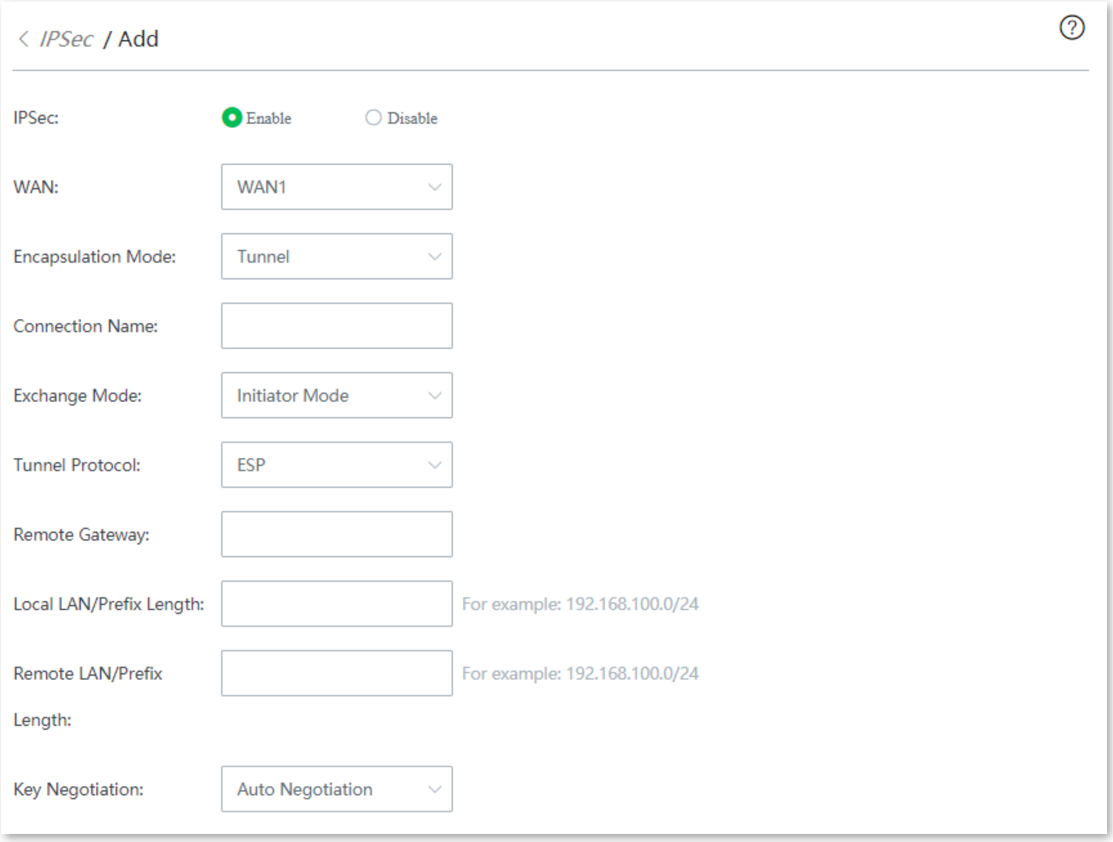
Parameters	Description
Remote Gateway	It specifies the WAN port IP address or domain name of the remote gateway of the IPSec tunnel. 💡 Tip When it is set to be a domain name, DDNS should be configured on the remote gateway so that the IPSec tunnel is not affected when the WAN port IP address of the remote gateway changes.
Status	It specifies whether the rule is enabled or not.
Operation	It is used to perform the following operations to the corresponding rule: ✎: Click it to edit the rule. 🗑: Click it to delete the rule.

Create an IPSec connection

1. Navigate to **More** > **IPSec** to enter the page.
2. Click **Add**. The configuration window appears.



3. Set the related parameters as required, and click **Save** on the bottom of the page.



< IPSec / Add

IPSec:	● Enable ○ Disable
WAN:	WAN1
Encapsulation Mode:	Tunnel
Connection Name:	
Exchange Mode:	Initiator Mode
Tunnel Protocol:	ESP
Remote Gateway:	
Local LAN/Prefix Length:	For example: 192.168.100.0/24
Remote LAN/Prefix Length:	For example: 192.168.100.0/24
Key Negotiation:	Auto Negotiation

----End

Parameter description

Parameters	Description
IPSec	It specifies whether to enable the IPSec function.
WAN	It specifies the local WAN port assigned to the IPSec function. The IP address of the WAN port must be set as the value of Remote Gateway of the IPSec peer.
Encapsulation Mode	It specifies the encapsulation mode for IPSec data. – Tunnel: It is usually used for communication between two secured gateways. – Transport: It is usually used for communication between hosts and hosts, and between hosts and gateways.
Connection Name	It specifies the name of the IPSec connection.
Exchange Mode	It is used to select the negotiation mode of IPSec tunnel. – Initiator Mode: Positively initiate connection request with peer gateway. It requires that the peer gateway is reachable. – Responder Mode: Wait for the connection request from peer gateway. Note Do not set the Exchange Mode of both sides to Responder Mode. Otherwise, you will be failed to create an IPSec tunnel.

Parameters	Description
Tunnel Protocol	It specifies the tunnel protocol of the IPSec rule. By default, it is ESP. – ESP: It indicates the Encapsulating Security Payload (ESP) protocol 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: It indicates the Authentication Header (AH) protocol used for verifying data integrity. If a packet is tampered during transmission, the receiver discards it during data integrity verification. – AH+ESP: It indicates that the function features both AH and ESP.
Remote Gateway	It specifies the WAN port IP address or domain name of the remote gateway of the IPSec tunnel. Note When it is set to be a domain name, DDNS should be configured on the remote gateway so that the IPSec tunnel is not affected when the WAN port IP address of the remote gateway changes.
Local LAN/Prefix Length	It specifies the local network segment and prefix length of the node. For example, the LAN IP address of the node is 192.168.5.1, and subnet mask is 255.255.255.0, so the local network segment/prefix length is 192.168.5.0/24.
Remote LAN/Prefix Length	It specifies the local network segment/prefix length of opposite gateway. If opposite device is a single host, not a network, this parameter should be set to the IP address of the host/32.
Key Negotiation	It specifies the key negotiation method to establish an IPSec tunnel. The default mode is Auto Negotiation. – Auto Negotiation: It indicates that an SA is set up, maintained, and deleted automatically using IKE (Internet Key Exchange). This reduces configuration complexity and simplifies IPSec usage and management. Such an SA (Security Association) has a life cycle and is updated regularly, leading to higher security. – Manual: It indicates that an SA is set up by manually specifying encryption and authentication algorithms and keys. Such an SA does not have a life cycle, and therefore it remains valid unless being manually deleted, leading to security risks. Generally, this mode is used only for commissioning.

- **Key Negotiation: Auto Negotiation**

To ensure the information privacy, both IPSec communicating parties use the same key for encryption and decryption. The material used to build these keys must be exchanged in a secure fashion. Information can be securely exchanged only if the key belongs exclusively to the IPSec communicating parties.

The goal of the Internet Key Exchange (IKE) is for both sides to independently produce the same symmetrical key. IKE is a combination of ISAKMP (Internet Security Association and Key

Management Protocol), SKEME and Oakley protocols.

- ISAKMP: ISAKMP (Internet Security Association and Key Management Protocol) is a key exchange architecture or framework used within IPSec, which manages the exchange of keys between both endpoints.
- SKEME: A secure and versatile key exchange protocol for key management over internet is presented. SKEME constitutes a compact protocol that supports a variety of realistic scenarios and security models over internet.
- Oakley: is a protocol to carry out the key exchange negotiation process for both peers, in which both ends after being authenticated can agree on secure and secret keying material.

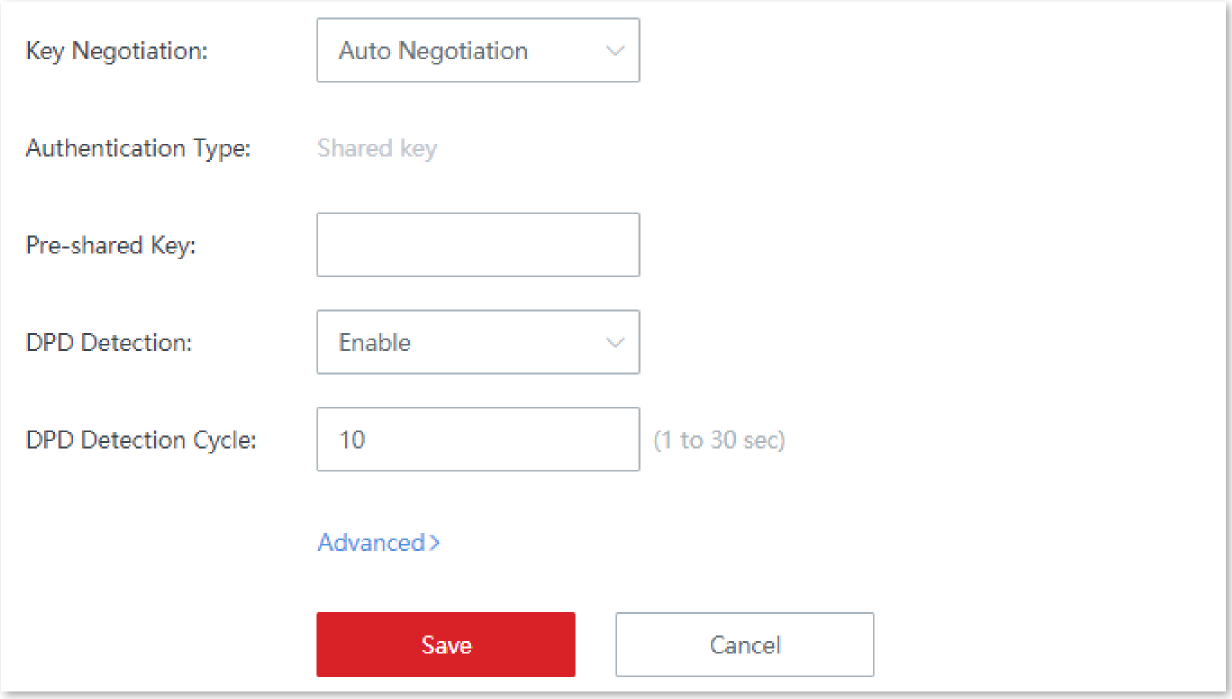
IKE operates in phase 1 and phase 2.

During IKE Phase I:

- The peers authenticate, either by certificates or via a pre-shared secret.
- A Diffie-Hellman key is created. The nature of the Diffie-Hellman protocol means that both sides can independently create the shared secret, a key which is known only to the peers.
- Key material (random bits and other mathematical data) as well as an agreement on methods for IKE phase II are exchanged between the peers.

IKE phase II is encrypted according to the keys and methods agreed upon in IKE phase I. The key material exchanged during IKE phase II is used for building the IPsec keys. The outcome of phase II is the IPsec Security Association. The IPsec SA is an agreement on keys and methods for IPsec, thus IPsec takes place according to the keys and methods agreed upon in IKE phase II.

When the **Key Negotiation** is set to **Auto Negotiation**, you can see the following page.



Key Negotiation: Auto Negotiation

Authentication Type: Shared key

Pre-shared Key:

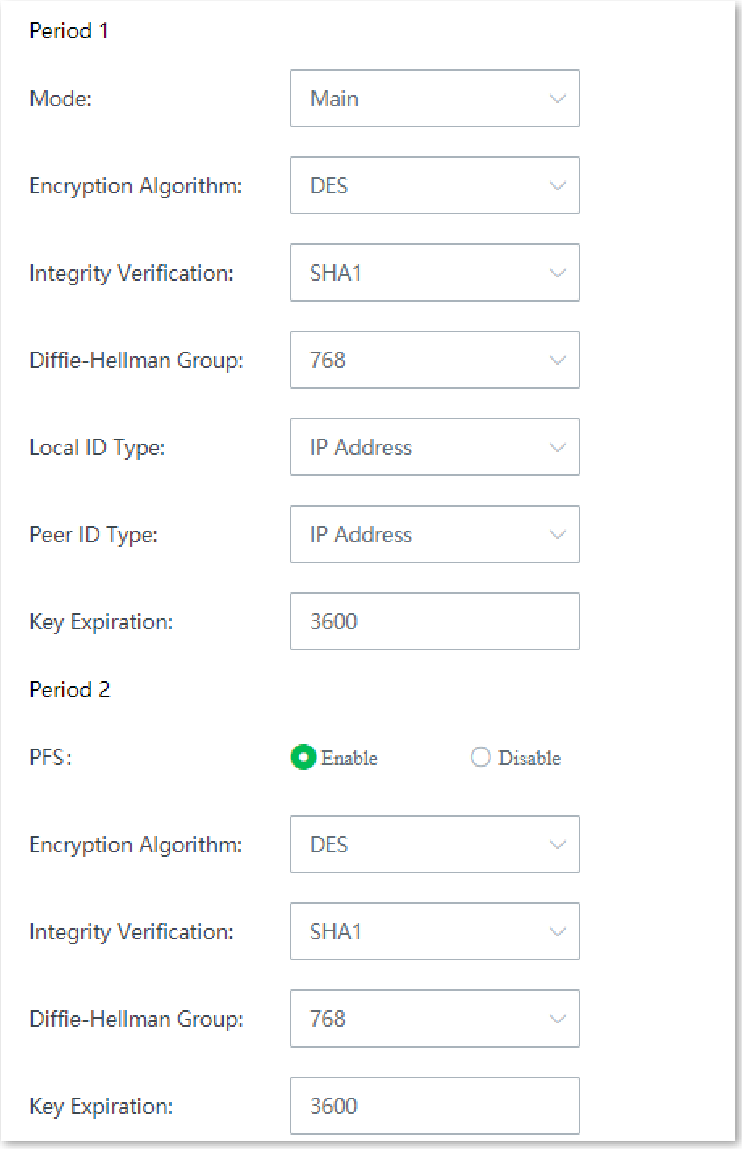
DPD Detection: Enable

DPD Detection Cycle: 10 (1 to 30 sec)

Parameter description

Parameters	Description
Authentication Type	It displays Shared key, indicating that IPSec peers negotiated a key string shared between them.
Pre-shared Key	It specifies a pre-shared key used for negotiation. The key consists of a maximum of 128 characters and must be the same as that specified on the peer gateway.
DPD Detection	It specifies whether to enable the DPD Detection. This function can detect whether the remove tunnel site is valid.
DPD Detection Cycle	It specifies the period of transmitting DPD packets. The node transmits DPD packets based on the period set here. If the DPD packets do not be confirmed by the remote peer during the period, the node re-initializes the IPSec SA between the both sides.

Click **Advanced** to see the advanced parameters.



Period 1

Mode:	Main
Encryption Algorithm:	DES
Integrity Verification:	SHA1
Diffie-Hellman Group:	768
Local ID Type:	IP Address
Peer ID Type:	IP Address
Key Expiration:	3600

Period 2

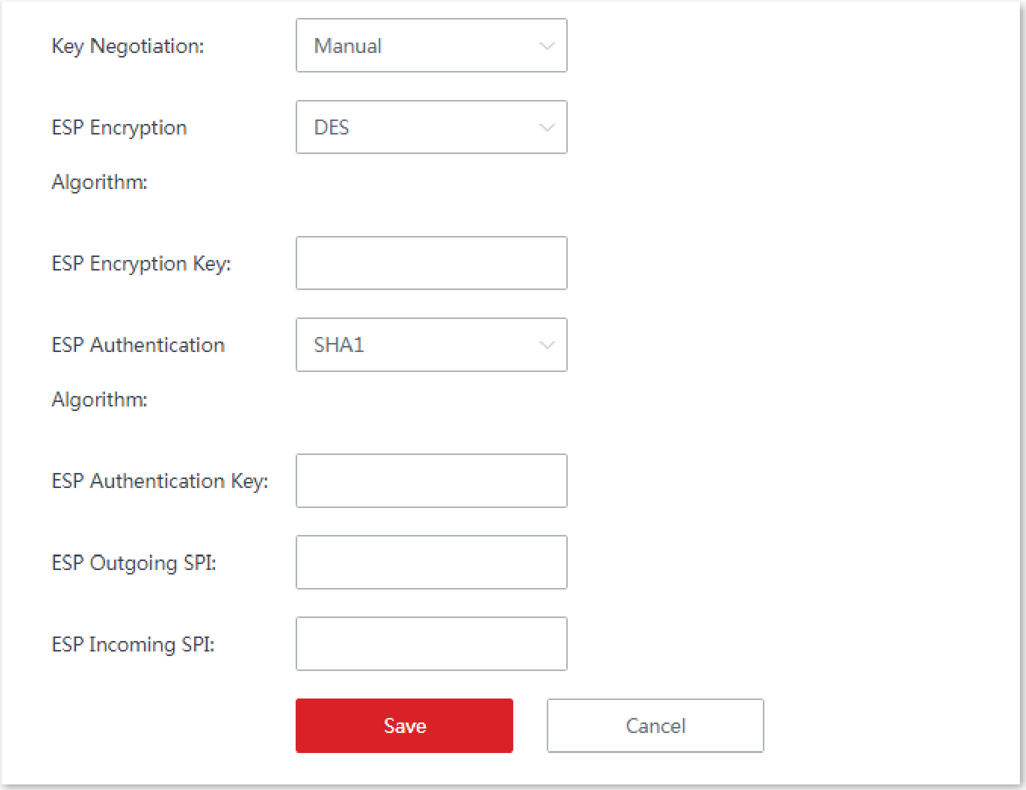
PFS:	● Enable ○ Disable
Encryption Algorithm:	DES
Integrity Verification:	SHA1
Diffie-Hellman Group:	768
Key Expiration:	3600

Parameter description

Parameters	Description
Mode	It used to select the exchange mode in IKE phase I, which should be the same as that of peer gateway. Main: In this mode, the Phase 1 parameters are exchanged in multiple rounds with encrypted authentication information Aggressive: In Aggressive mode, the Phase 1 parameters are exchanged in a single message with unencrypted authentication information. Tip Although Main mode is more secure, you must select Aggressive mode if there is more than one dialup Phase 1 configuration for the interface IP address, and the remote VPN peer or client is authenticated using an identifier local ID. Aggressive mode might not be as secure as Main mode, but the advantage to Aggressive mode is that it is faster than Main mode (since fewer packets are exchanged). Aggressive mode is typically used for remote access VPNs. But you would also use aggressive mode if one or both peers have dynamic external IP addresses.
Encryption Algorithm	It specifies the IKE session encryption algorithm. The device 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: 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	It specifies the IKE session verification algorithm. The device 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.
Diffie-Hellman Group	It specifies the group information for the Diffie-Hellman algorithm for generating a session key used to encrypt an IKE tunnel. The information should be the same as that of the remote gateway.
Key Expiration	It specifies the life cycle of IKE SA.
PFS	This feature generates a new key in IKE Period 2, which is unrelated to the key generated in IKE Period 1, leaving the key generated in Period 2 security even if the key generated in IKE1 Period 1 is cracked. With the PFS disabled, generation of the new key in IKE Period 2 depends on the key in Period 1. Once the key generated in IKE Period 1 is cracked, the key generated in Period 2 will suffer threats, and further threatens the communication security.

- **Key Negotiation: Manual**

When the **Key Negotiation** is set to **Manual**, you can see the following page.



Key Negotiation: Manual

ESP Encryption Algorithm: DES

ESP Encryption Key:

ESP Authentication Algorithm: SHA1

ESP Authentication Key:

ESP Outgoing SPI:

ESP Incoming SPI:

Parameter description

Parameters	Description
ESP Encryption Algorithm	When the Tunnel Protocol is set to ESP, the ESP encryption algorithm is required. The device 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. A key of 8 ASCII characters or 16 hexadecimal characters is required. 3DES indicates that three 56-bit keys are used for encryption. A key of 24 ASCII characters or 48 hexadecimal characters is required. – AES: A 128/192/256-bit key is used for encryption. A key of 16/24/32 ASCII characters or 32/48/64 hexadecimal characters is required.
ESP Encryption Key	It is used to set 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 device supports the following algorithms: – MD5: A 128-bit message digest is generated to prevent message tampering. The authentication key must be 16 ASCII characters or 32 hexadecimal characters. – SHA1: A 160-bit message digest is generated to prevent message tampering. The authentication key must be 20 ASCII characters or 40 hexadecimal characters.

Parameters	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	SPI (Security Parameter Index) is used to identify an IPSec SA with the IP address and security protocol of the remote gateway. – ESP Outgoing SPI: Keep this value same as the ESP incoming SPI value of the remote gateway. – ESP Incoming SPI: Keep this value same as the ESP outgoing SPI value of the remote gateway. – AH Outgoing SPI: Keep this value same as the AH incoming SPI value of the remote gateway. – AH Incoming SPI: Keep this value same as the AH outgoing SPI value of the remote gateway.
ESP/AH Incoming SPI	

Example of configuring an IPSec VPN

Network requirement

An enterprise and its branch use EW12 to set up LANs and access the internet. Branch employees need to access the HQ's internal resources through the internet, such as internal data, OA, ERP, CRM, project management systems.

Solutions

You can use two routers to establish an IPSec VPN connection to meet this requirement.

Assume that:

The enterprise and its branch use Router1 and Router2 to establish networks respectively.

The related information of **Router1** is shown as below:

- IP address of WAN1: 202.105.11.22
- LAN: 192.168.5.0/24

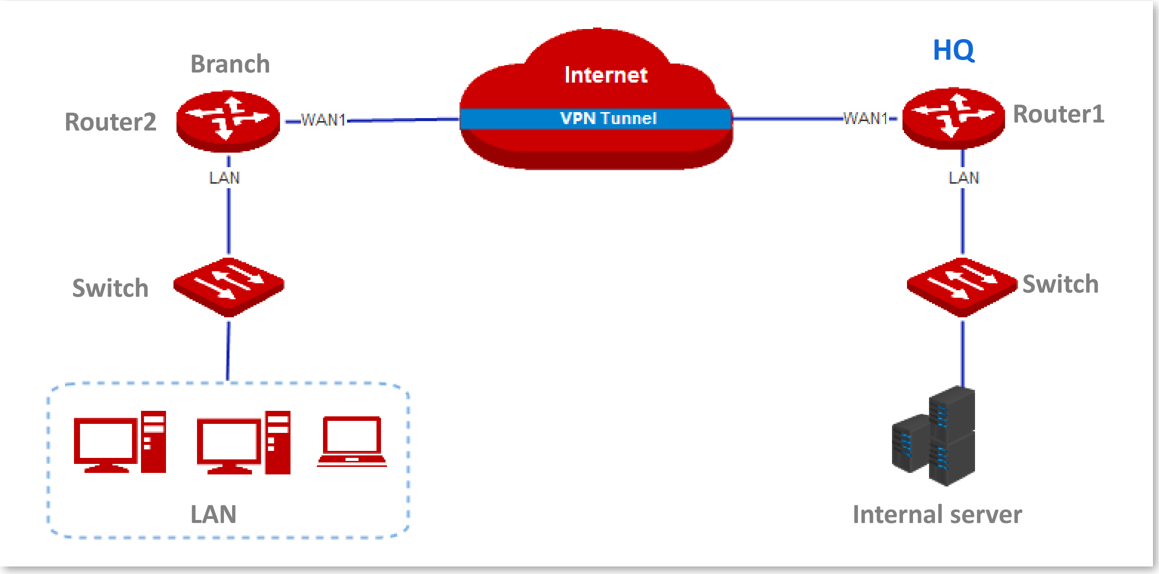
The related information of **Router2** is shown as below:

- IP address of WAN1: 202.105.88.77
- LAN: 192.168.1.0/24

The IPSec connection information of the two routers is shown as below:

- Encapsulation Mode: Tunnel mode
- Key Negotiation: Auto negotiation
- Pre-shared Key: 12345678

Network topology



Configuration procedure

Tip

During the configuration, if you need to modify advanced settings for IPSec connections, keep the settings of the two routers consistent.

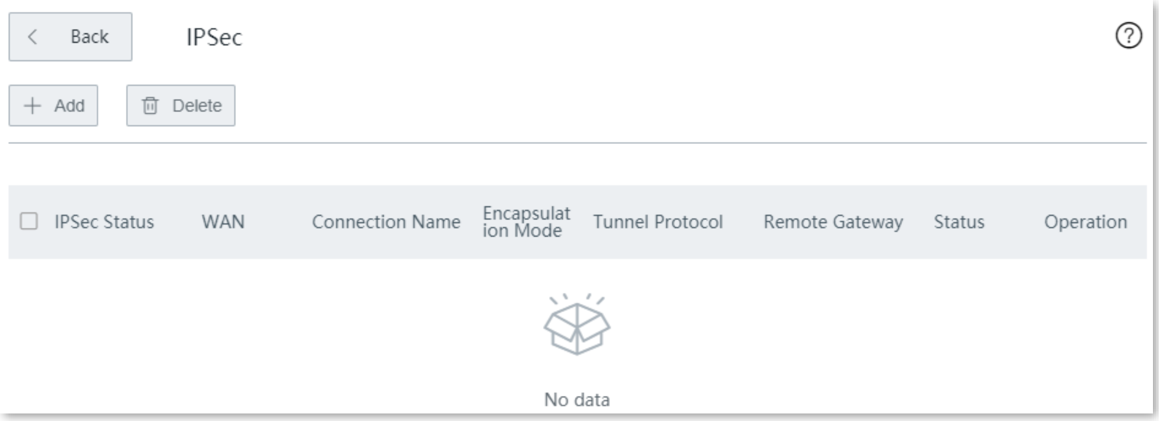
When the Key Negotiation Method is set to Manual Setup, the encryption algorithms, encryption keys, and authentication algorithms at IPSec peers must be the same. The ESP outgoing SPI of EW12_HQ is the same as the ESP incoming SPI of EW12_Branch, and the ESP incoming SPI of EW12_HQ and the ESP outgoing of EW12_Branch are the same.

For the security software such as firewall may prevent the internet users from access the VPN tunnel, so you are recommended to turn off the security software such as firewall.

1. Set Router1.

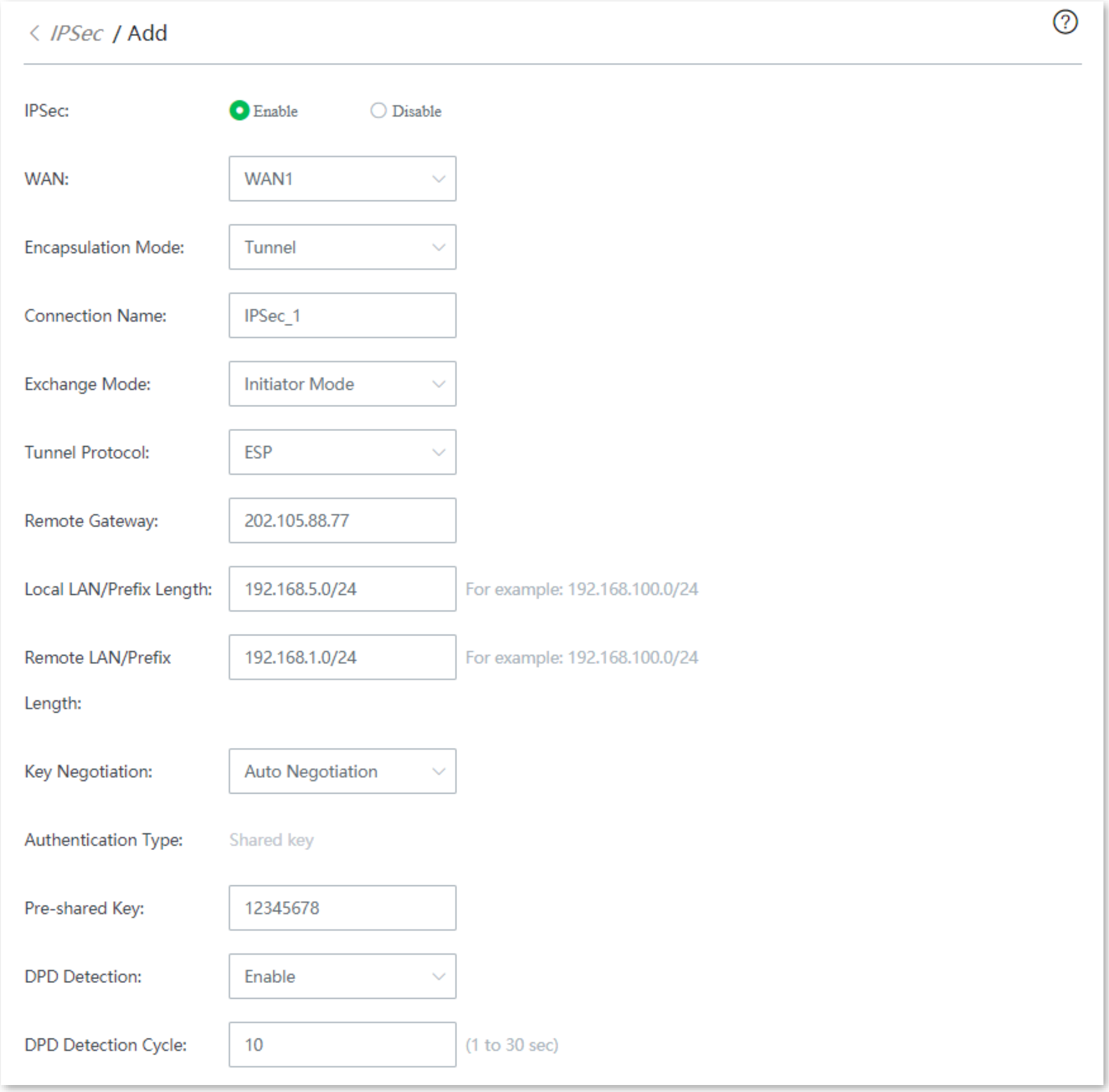
(1) Navigate to **More** > **IPSec** to enter the page.

(2) Click **Add**. The configuration area appears.



(3) Set the related parameters, and click **Save**.

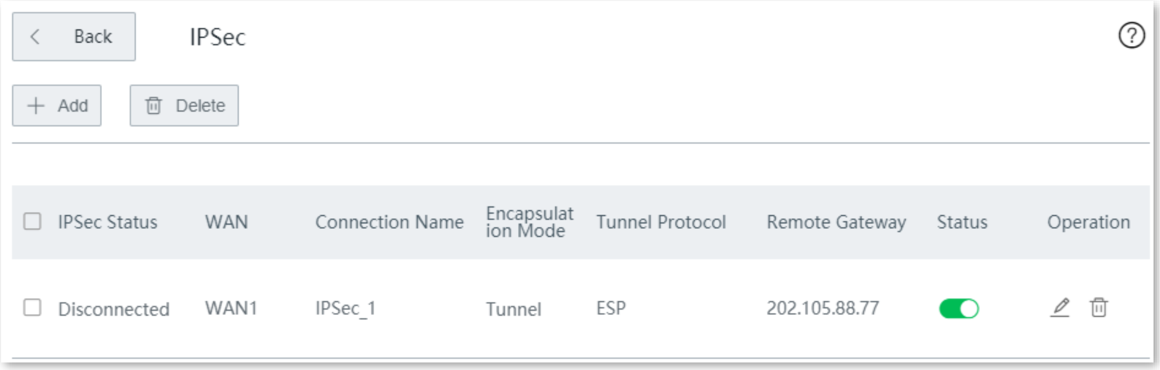
- Select an encapsulation mode, which is **Tunnel** in this example.
- Enter a tunnel name, which is **IPSec_1** in this example.
- Enter the remote gateway IP address, which is **202.105.88.77** in this example.
- Enter the local LAN/prefix length, which is **192.168.5.0/24** in this example.
- Enter the remote LAN/prefix length, which is **192.168.1.0/24** in this example.
- Enter the Pre-shared key, which is **123458678** in this example.



IPSec / Add

IPSec:	● Enable ○ Disable	
WAN:	WAN1	
Encapsulation Mode:	Tunnel	
Connection Name:	IPSec_1	
Exchange Mode:	Initiator Mode	
Tunnel Protocol:	ESP	
Remote Gateway:	202.105.88.77	
Local LAN/Prefix Length:	192.168.5.0/24	For example: 192.168.100.0/24
Remote LAN/Prefix Length:	192.168.1.0/24	For example: 192.168.100.0/24
Key Negotiation:	Auto Negotiation	
Authentication Type:	Shared key	
Pre-shared Key:	12345678	
DPD Detection:	Enable	
DPD Detection Cycle:	10	(1 to 30 sec)

It is added successfully. See the following figure.



□	IPSec Status	WAN	Connection Name	Encapsulation Mode	Tunnel Protocol	Remote Gateway	Status	Operation
□	Disconnected	WAN1	IPSec_1	Tunnel	ESP	202.105.88.77	●	

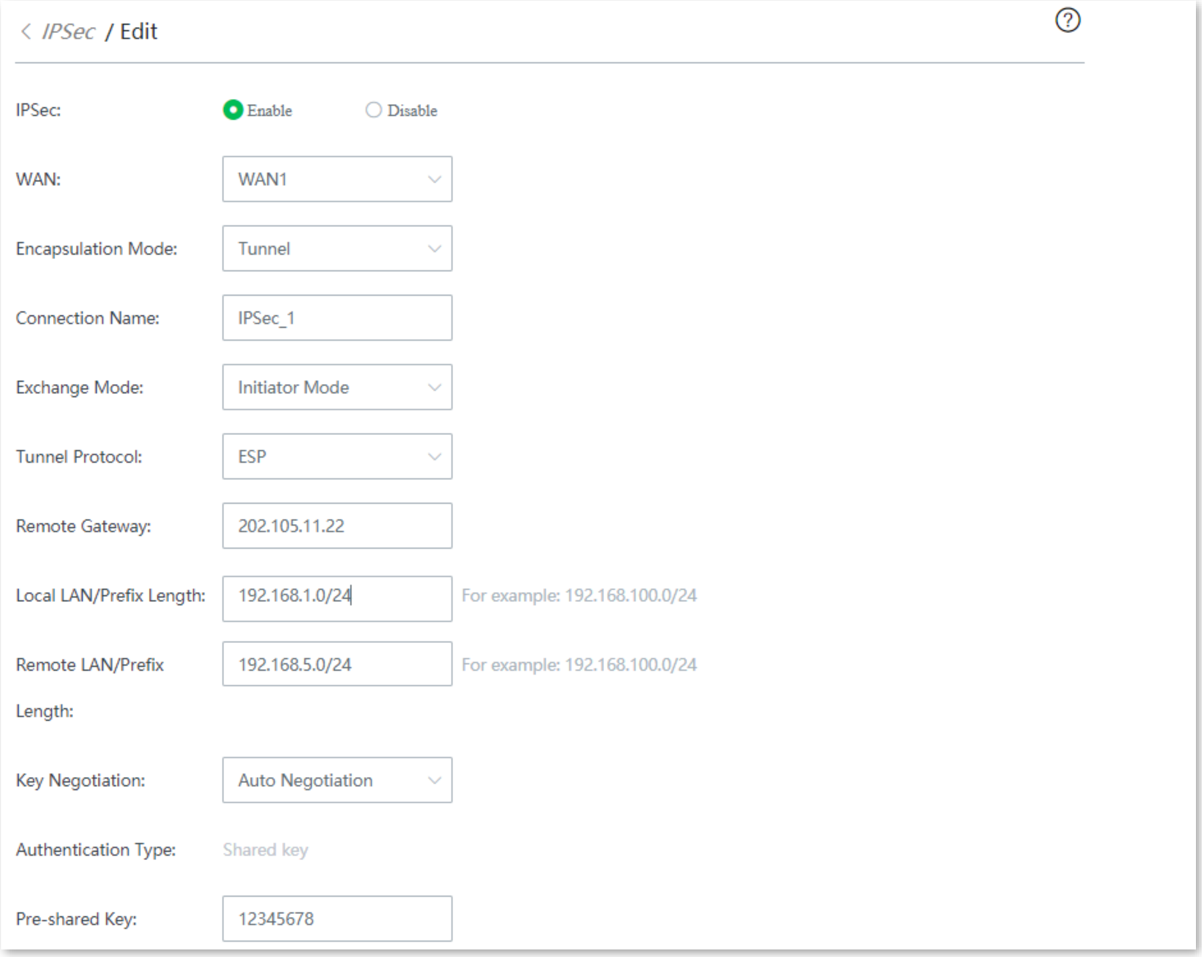
2. Set the Router2.

(1) Navigate to **More** > **IPSec** to enter the page.

(2) Click **+Add**. The configuration area appears.

(3) Set the related parameters, and click **Save**.

- Select an encapsulation mode, which is **Tunnel** in this example.
- Enter a tunnel name, which is **IPSec_1** in this example.
- Enter the remote gateway IP address, 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 **192.168.5.0/24** in this example.
- Enter the Pre-shared key, which is **123458678** in this example.



IPSec: ● Enable ○ Disable

WAN: WAN1

Encapsulation Mode: Tunnel

Connection Name: IPSec_1

Exchange Mode: Initiator Mode

Tunnel Protocol: ESP

Remote Gateway: 202.105.11.22

Local LAN/Prefix Length: 192.168.1.0/24 For example: 192.168.100.0/24

Remote LAN/Prefix Length: 192.168.5.0/24 For example: 192.168.100.0/24

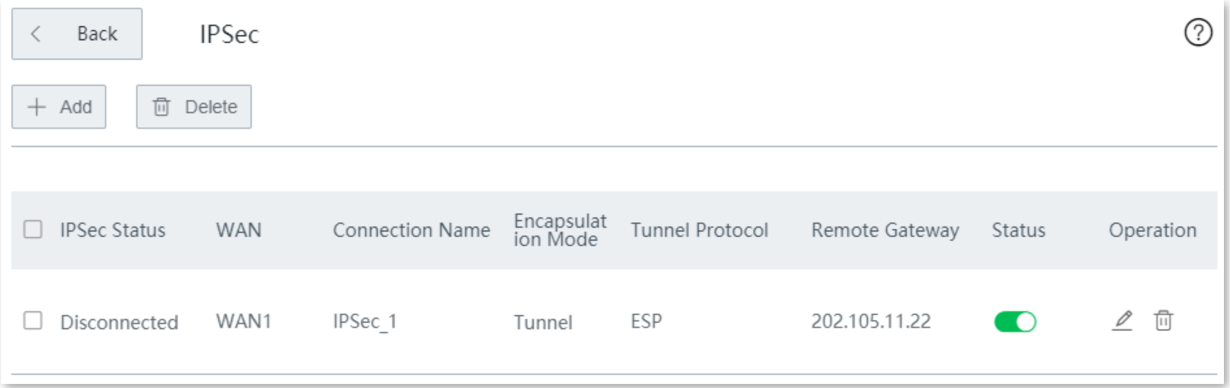
Key Negotiation: Auto Negotiation

Authentication Type: Shared key

Pre-shared Key: 12345678

----End

It is added successfully. See the following figure.



□ IPSec Status	WAN	Connection Name	Encapsulation Mode	Tunnel Protocol	Remote Gateway	Status	Operation
□ Disconnected	WAN1	IPSec_1	Tunnel	ESP	202.105.11.22	●	

Verification

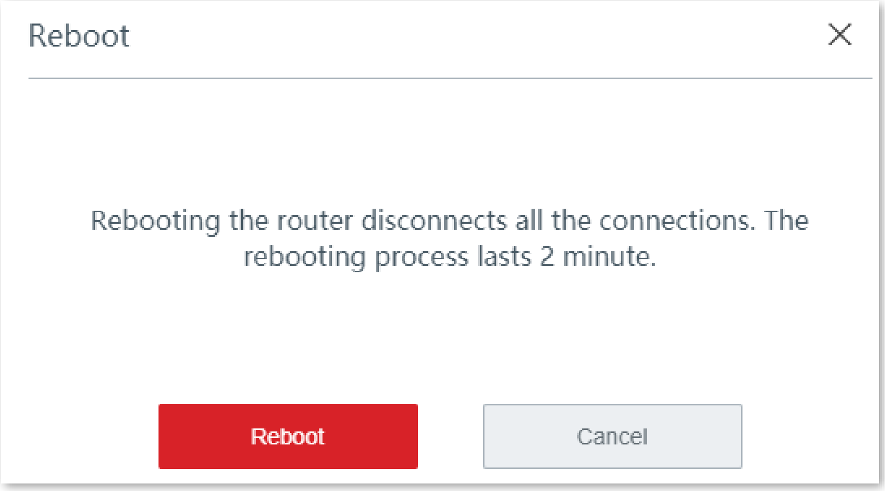
After the preceding configuration, employees at the branch and HQ can remotely access resources on the branch and HQ LAN resources through the internet in a secure manner.

3.11 Maintenance

3.11.1 Reboot

If a parameter does not take effect or the device does not work properly, you can try rebooting the device to resolve the problem.

Navigate to **Maintenance** > **Reboot**. The prompt window appears. Confirm the message and click **Reboot**.



Reboot

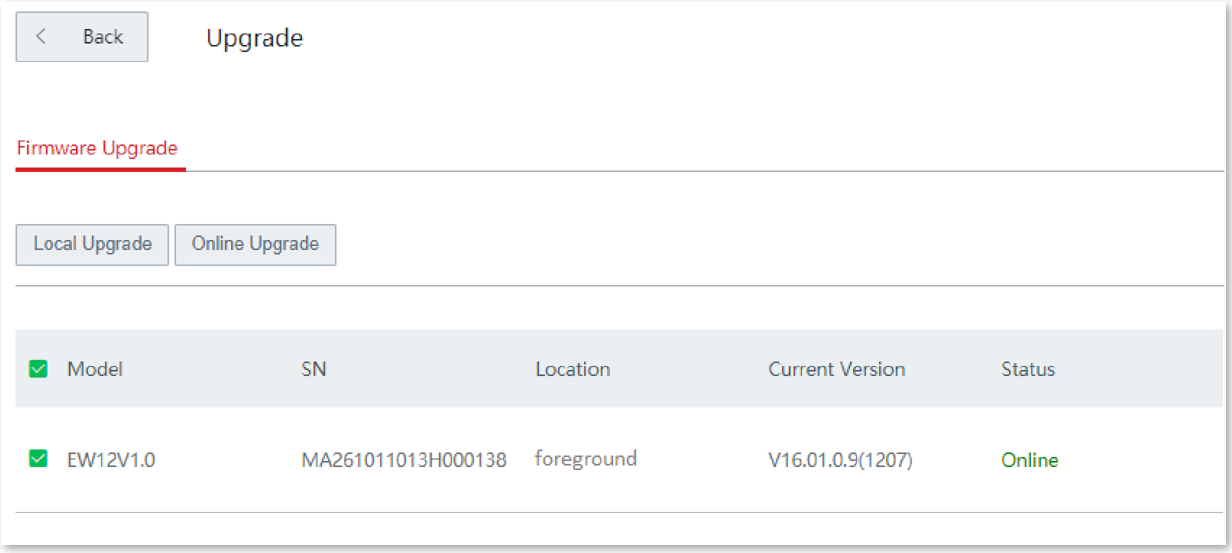
Rebooting the router disconnects all the connections. The rebooting process lasts 2 minute.

3.11.2 Upgrade

Overview

The device supports **local** and **online** upgrades.

Navigate to **Maintenance** > **Upgrade** to enter the configuration page. See the following figure.



☑	Model	SN	Location	Current Version	Status
☑	EW12V1.0	MA261011013H000138	foreground	V16.01.0.9(1207)	Online

Upgrade the device locally

Tip

To enable your device to work properly after an upgrade, ensure that the firmware used to upgrade complies with your product model.

When upgrading, do not power off the device.

1. Download the upgrade file to your local computer.

   (1) Visit www.ip-com.com.cn, and search the product model in the searching bar to enter the product details page.

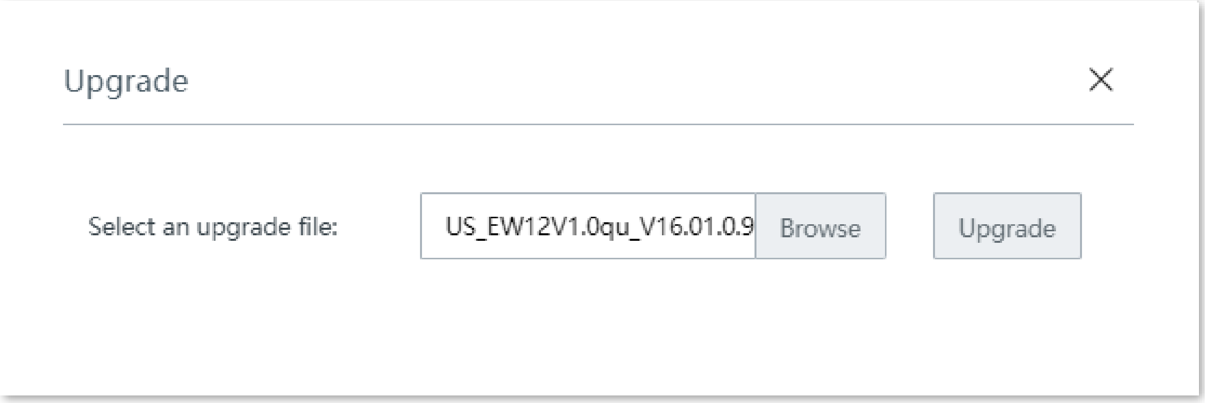
   (2) Locate the latest firmware, download it to your computer, and unzip it.

2. Log in to the web UI of your device, click **Maintenance** > **Upgrade** to enter the configuration page.

3. Select the cable-free device which needs to be upgraded, and click **Local Upgrade**.

4. Click **Browse**, select and upload the firmware that has been downloaded to your computer. Ensure that the suffix of the firmware is ".bin".

5. Click **Upgrade**. Wait until the progress bar completes.



Upgrade

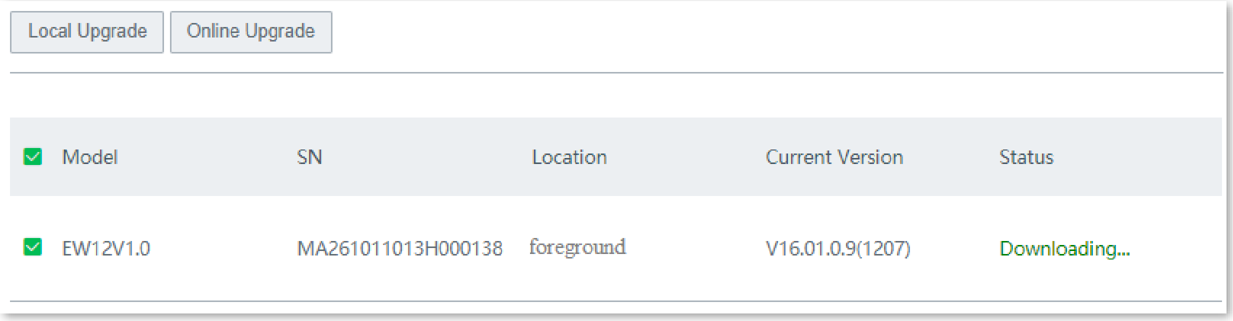
Select an upgrade file: US_EW12V1.0qu_V16.01.0.9

----End

After the progress bar completes, you can login in again and check the current software version number of the device on the **Upgrade** or **System Status** page to confirm whether the upgrade is successful.

Upgrade the device online

When the device is connected to the internet, it checks whether there is a later firmware version, and displays the detected information on the page. You can choose whether to upgrade, and click **Online Upgrade**.



☑	Model	SN	Location	Current Version	Status
☑	EW12V1.0	MA261011013H000138	foreground	V16.01.0.9(1207)	Downloading...

3.11.3 Reset

Overview

If the internet is inaccessible for unknown reasons, or you forget the login password, you can reset the device to resolve the problems.

The device supports two resetting methods:

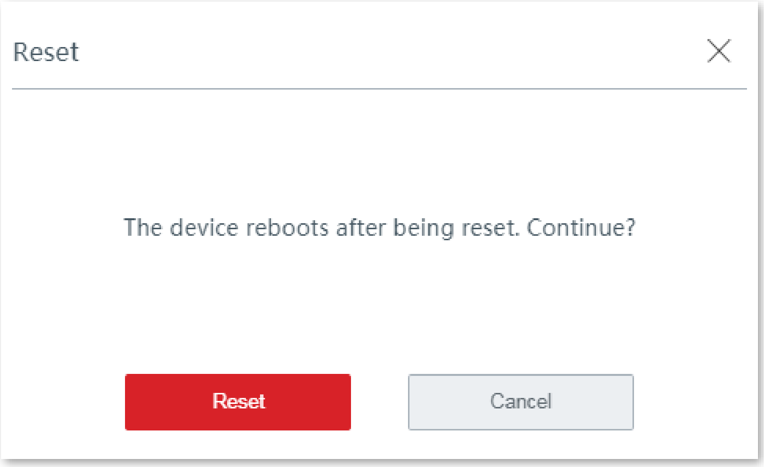
- Reset the device using web UI
- Reset the device using the Reset button

Reset the device using web UI

Tip

- Resetting the device deletes all your current configurations and you need to reconfigure the device to access the internet.
- If it is necessary to reset the device, back up your current configuration first.
- When resetting, do not power off the device.

Navigate to **Maintenance > Reset**, and follow the on-screen instruction to reset the device.



Reset

The device reboots after being reset. Continue?

Reset the device using the Reset button

If you forget your login password, but need to log in to the web UI of the device, you can use the hardware Reset button on the device to reset it, and configure it again.

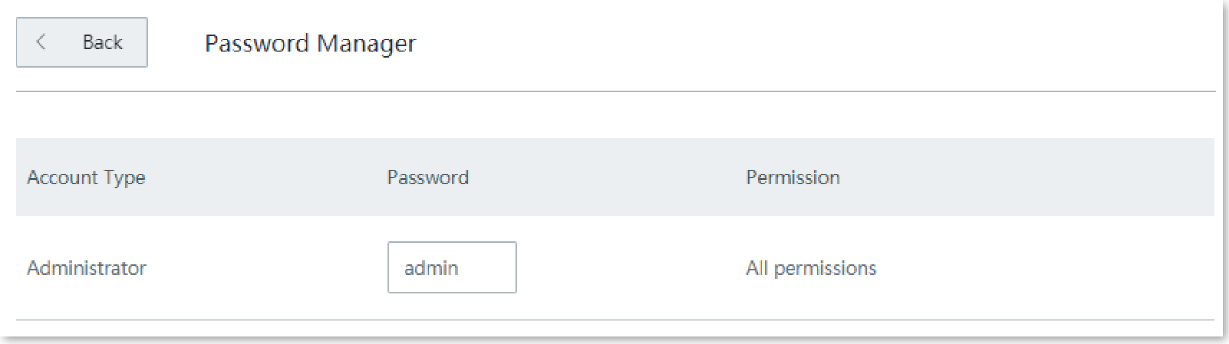
With the LED indicator blinking, hold down the Reset button using a paper clip (or something with a pointed end) for about 8 seconds, then release it when the LED indicator lights solid on. The device is reset to the factory settings successfully when the LED indicator blinks again.

3.11.4 Password manager

Overview

Navigate to **Maintenance** > **Password Manager** to enter the configuration page

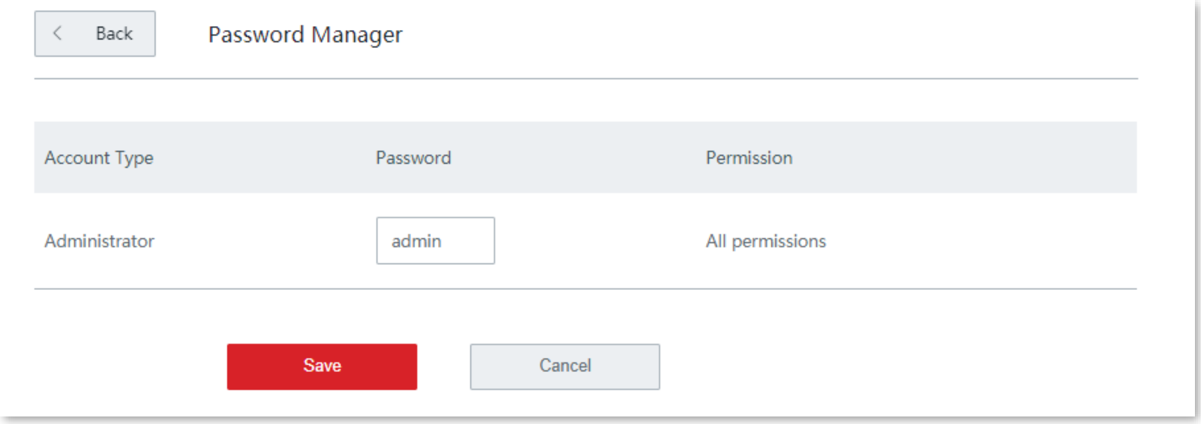
This function allows you to modify the password of the administrator. You need to set the password.



Account Type	Password	Permission
Administrator	admin	All permissions

Modify login password

1. Navigate to **Maintenance** > **Password Manager** to enter the configuration page.
2. Locate the account type and modify the password.
3. Click **Save** on the bottom of the page to apply your settings.



Account Type	Password	Permission
Administrator	admin	All permissions

----End

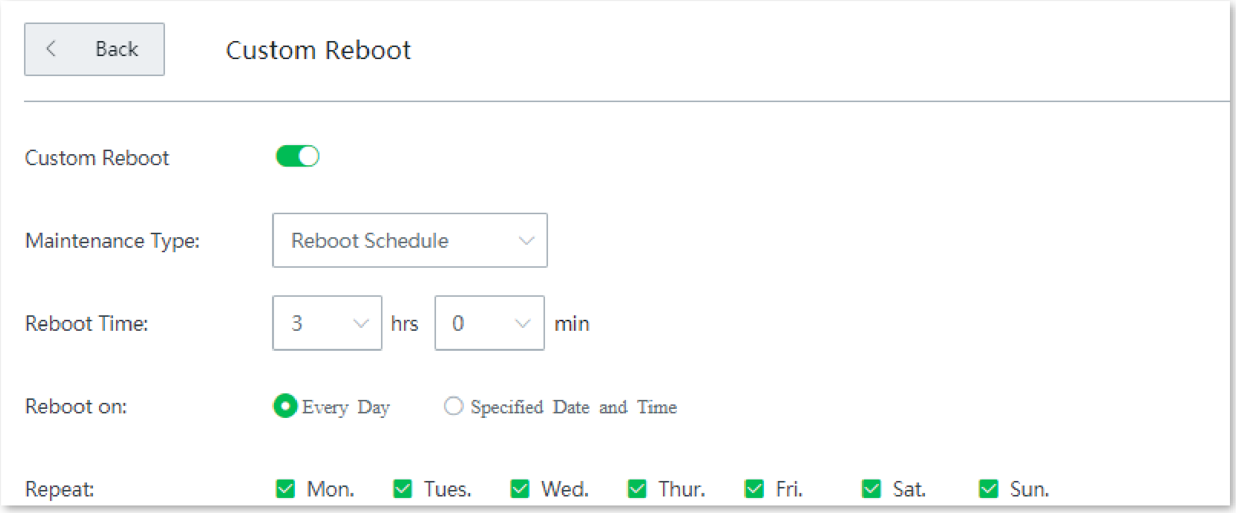
Then you will be redirected to the login page. Enter the password corresponding to the administrator account you set just now, and click **Login** to log in to the device.

3.11.5 Custom reboot

Overview

This device allows you to reboot it on schedule to maintain its performance.

Navigate to **Maintenance** > **Custom Reboot** to enter the page.



< Back   Custom Reboot

Custom Reboot

Maintenance Type: Reboot Schedule

Reboot Time: 3 hrs 0 min

Reboot on: ● Every Day ○ Specified Date and Time

Repeat: ☑ Mon. ☑ Tues. ☑ Wed. ☑ Thur. ☑ Fri. ☑ Sat. ☑ Sun.

Parameter description

Parameters	Description
Reboot Schedule	It specifies whether to enable the Reboot Schedule function.
Reboot Time	It specifies the time at which the device reboots.
Reboot on	It specifies the repeat rule.
Repeat	It specifies the dates on which the device reboots.

Reboot the device on schedule

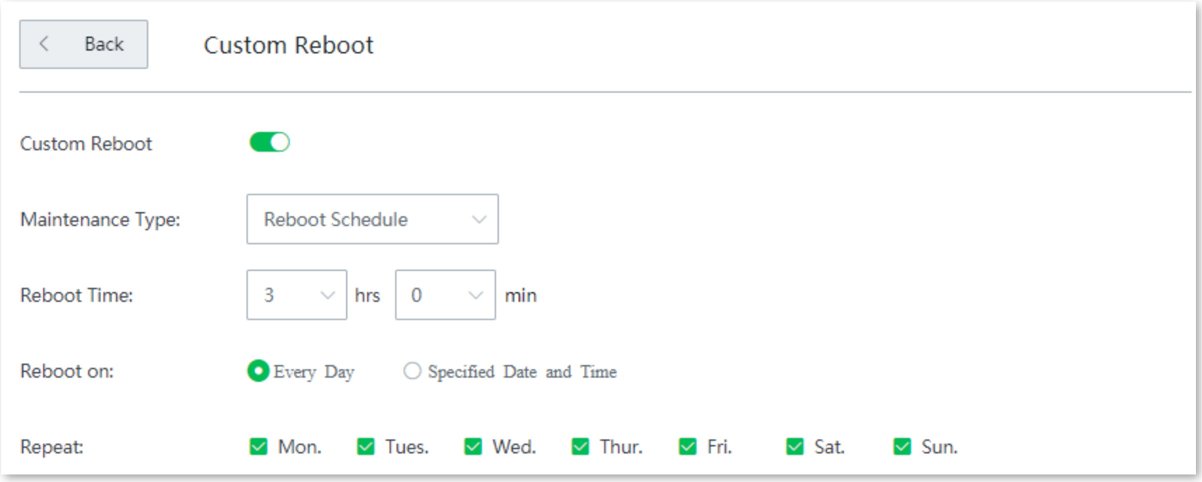
Tip

To enable reboot schedule function to work properly, ensure that the System time of your router is correct.

1. Navigate to **Maintenance** > **Custom Reboot** to enter the configuration page, and enable this function.

2. Set the time and date when the device performs rebooting.

3. Click **Save** to apply your settings.



Custom Reboot

Custom Reboot: on

Maintenance Type: Reboot Schedule

Reboot Time: 3 hrs 0 min

Reboot on: ● Every Day ○ Specified Date and Time

Repeat: ☑ Mon. ☑ Tues. ☑ Wed. ☑ Thur. ☑ Fri. ☑ Sat. ☑ Sun.

----End

The device performs rebooting regularly on the time and date you set here.

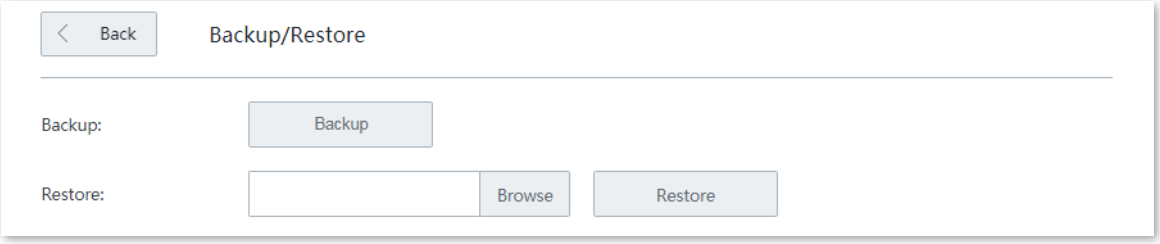
3.11.6 Backup/Restore

Overview

The **Backup** function is used to export the current configuration of the device to your computer. The **Restore** function is used to import a configuration file to the device.

You are recommended to back up the configuration after it is significantly changed. When the performance of your device decreases because of an improper configuration, or after you restore the device to factory settings, you can use this function to restore the configuration that has been backed up.

Navigate to **Maintenance** > **Backup/Restore** to enter the configuration page.



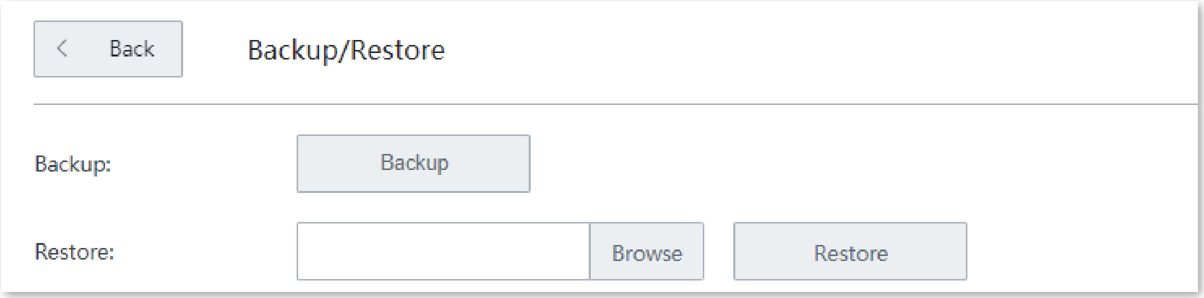
Backup/Restore

Backup:

Restore:

Back up your current configuration

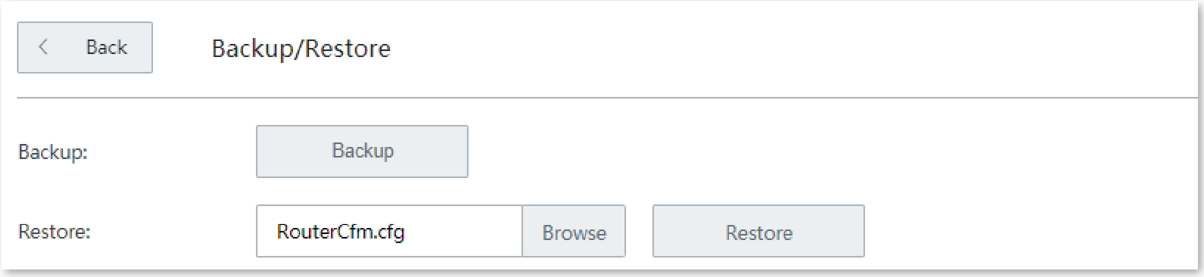
1. Navigate to **Maintenance** > **Backup/Restore** to enter the configuration page.
2. Click **Backup**. The system exports a **RouterCfm.cfg** file to your local computer.



----End

Restore your previous configuraiton

1. Navigate to **Maintenance** > **Backup/Restore** to enter the configuration page.
2. Click **Browse**, and upload the configuration file ending with **.cfg**.
3. Click **Restore** and follow the on-screen instruction to restore the configuration.



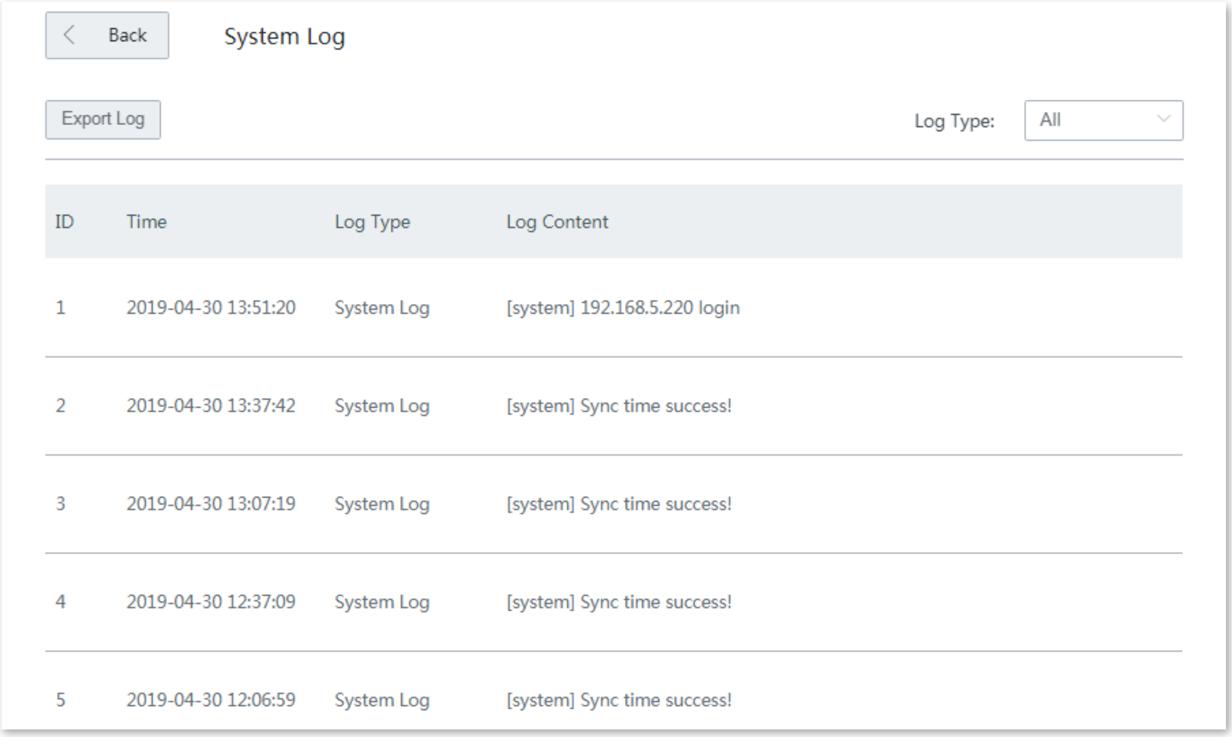
Restore: RouterCfm.cfg

----End

3.11.7 System log

System logs record information about system running status and the operation you performed on it. When system malfunctions occur, you can use system log for troubleshooting.

Navigate to **Maintenance** > **System Log** to enter the page.



Log Type: All

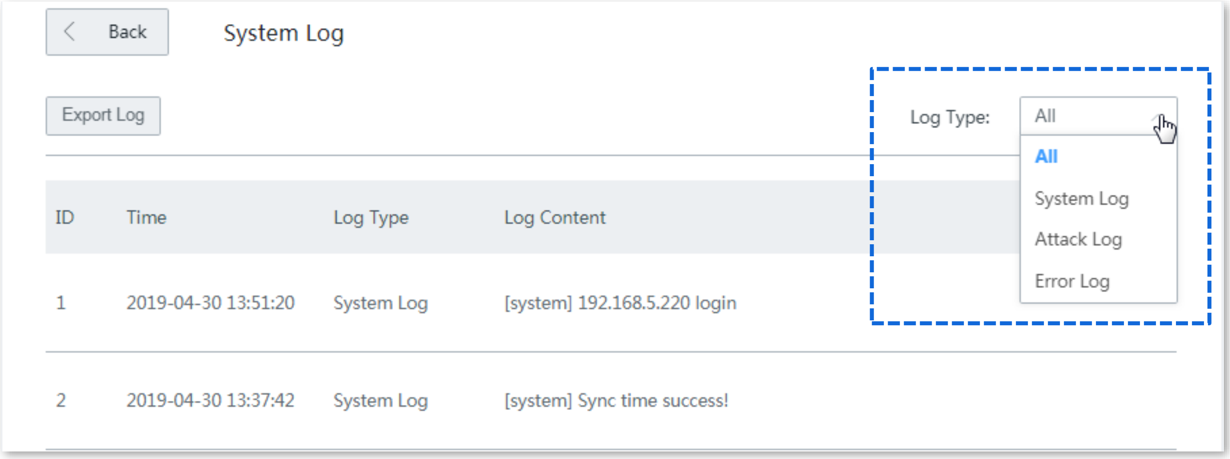
ID	Time	Log Type	Log Content
1	2019-04-30 13:51:20	System Log	[system] 192.168.5.220 login
2	2019-04-30 13:37:42	System Log	[system] Sync time success!
3	2019-04-30 13:07:19	System Log	[system] Sync time success!
4	2019-04-30 12:37:09	System Log	[system] Sync time success!
5	2019-04-30 12:06:59	System Log	[system] Sync time success!

View system log

Tip

- System logs will be cleared each time the device reboots or resets.
- A maximum of 300 logs will be recorded.
- The system only keeps 300 logs that are generated the most recently.

The device records three log types: **System Log**, **Attack Log**, and **Error Log**. You can view all logs or filter the logs to view as needed.

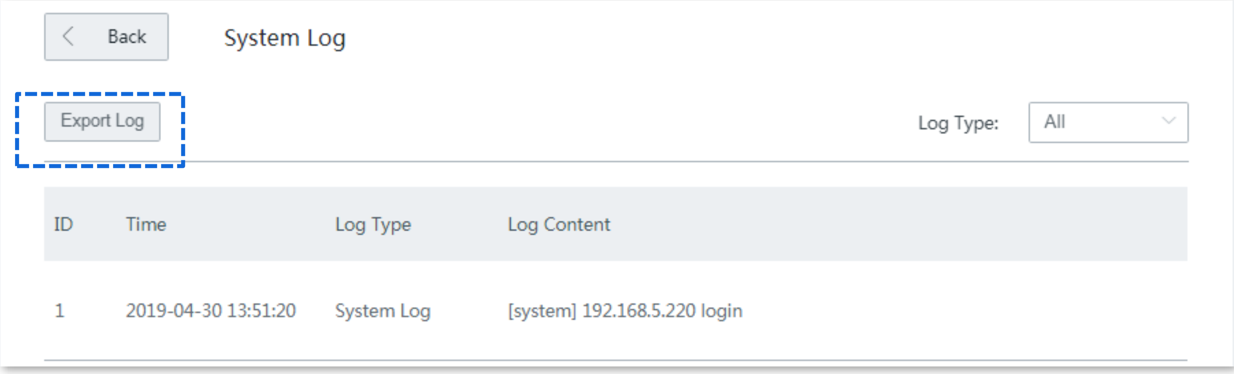


Log Type: All

ID	Time	Log Type	Log Content
1	2019-04-30 13:51:20	System Log	[system] 192.168.5.220 login
2	2019-04-30 13:37:42	System Log	[system] Sync time success!

Export system log

Click Export Log, the log file will be downloaded to your local computer.



ID	Time	Log Type	Log Content
1	2019-04-30 13:51:20	System Log	[system] 192.168.5.220 login

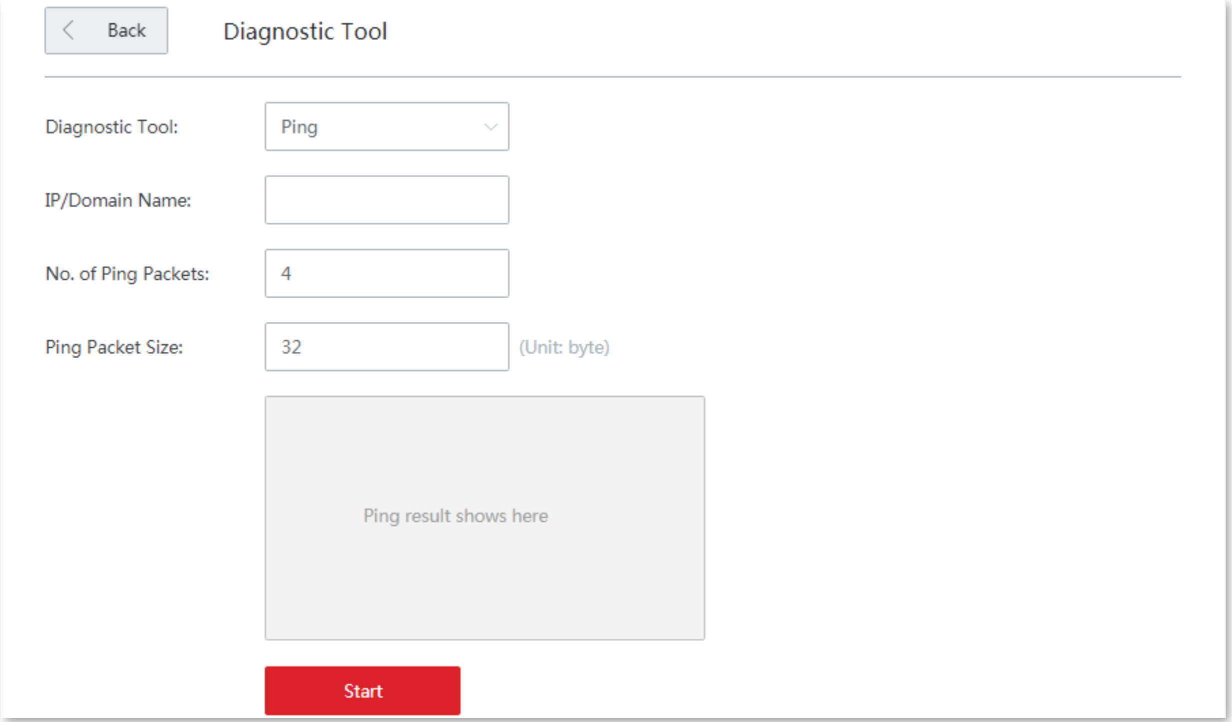
3.11.8 Diagnostic tool

Overview

You can execute Ping/Traceroute command on this page.

- **Ping**: Used to check whether the connection is correct and the connection quality.
- **Traceroute**: Used to detect the route from the bridge to the destination IP address or domain name.

Navigate to **Maintenance** > **Diagnosis Tool** to enter the page.



Diagnostic Tool: Ping

IP/Domain Name:

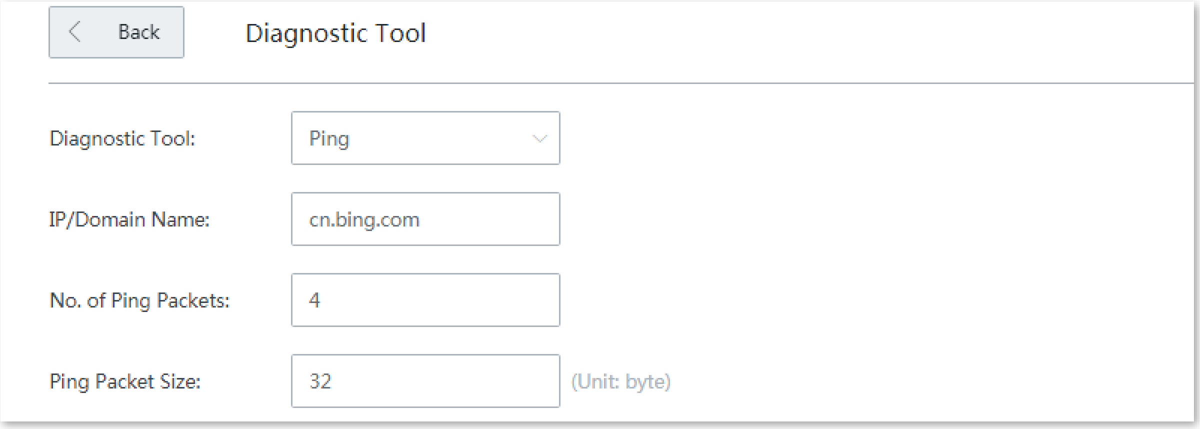
No. of Ping Packets: 4

Ping Packet Size: 32 (Unit: byte)

Execut Ping command to detect connection quality

Assume that you need to detect the connectivity between the device and the **Bing** website.

1. Navigate to **Maintenance** > **Diagnosis Tool** to enter the configuration page.
2. Select **Ping** from the drop-down list menu of the Tools.
3. Enter the IP address or domain name of the ping target, which is **cn.bing.com** in this example.
4. Set **No. of Ping Packets** as required.
5. Set **Ping Packet Size** as required.
6. Click **Start**.



Diagnostic Tool: Ping

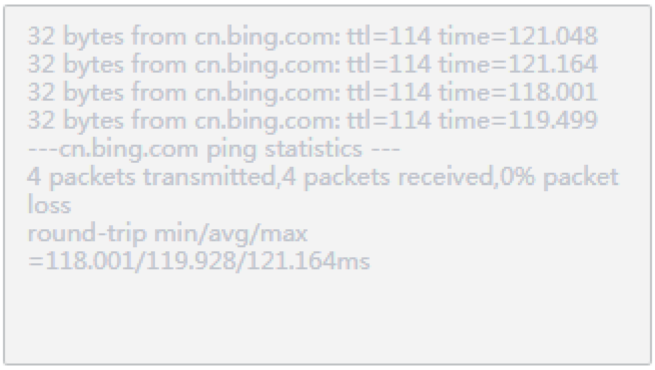
IP/Domain Name: cn.bing.com

No. of Ping Packets: 4

Ping Packet Size: 32 (Unit: byte)

----End

Wait a moment. The ping result will be displayed in the result box. See the following figure.



```
32 bytes from cn.bing.com: ttl=114 time=121.048
32 bytes from cn.bing.com: ttl=114 time=121.164
32 bytes from cn.bing.com: ttl=114 time=118.001
32 bytes from cn.bing.com: ttl=114 time=119.499
---cn.bing.com ping statistics ---
4 packets transmitted,4 packets received,0% packet
loss
round-trip min/avg/max
=118.001/119.928/121.164ms
```

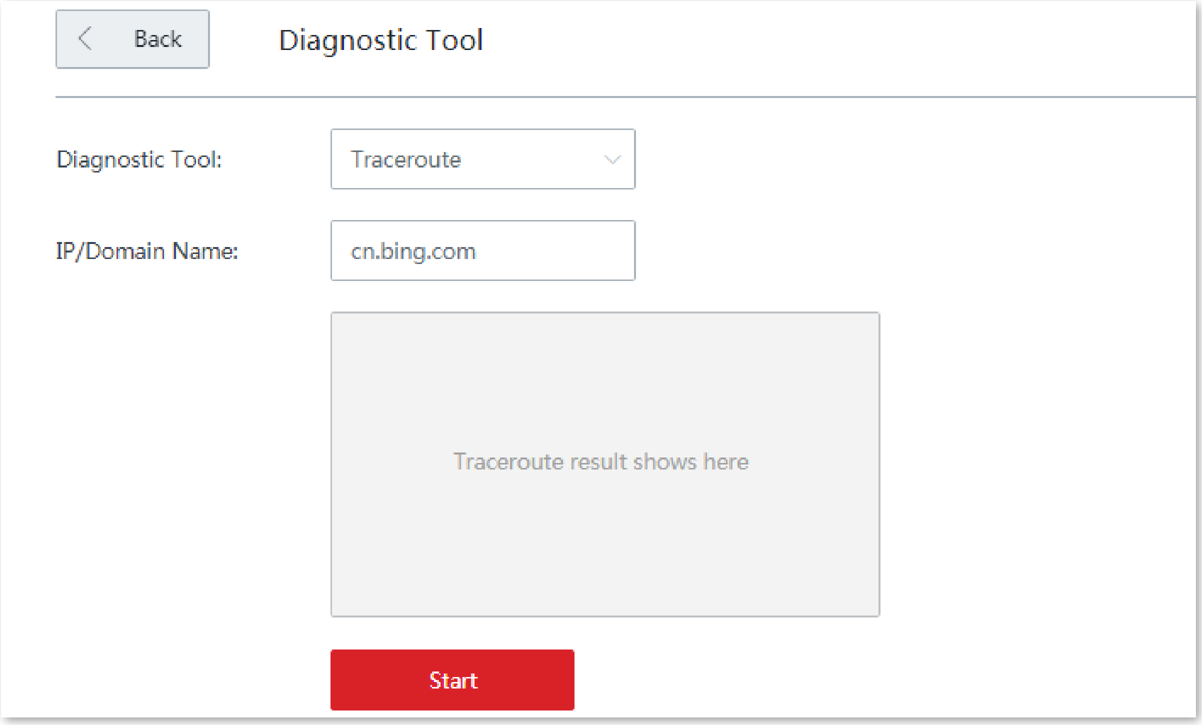
Execut Traceroute command to detect the route selection

Assume that You need to detect the path from the device to **Bing** website.

1. Navigate to **Maintenance** > **Diagnosis Tool** to enter the configuration page.
2. Select **Traceroute** from the drop-down list menu of the Tools menu.

3. Enter the IP address or domain name of the traceroute target, which is **cn.bing.com** in this example.

4. Click **Start**.

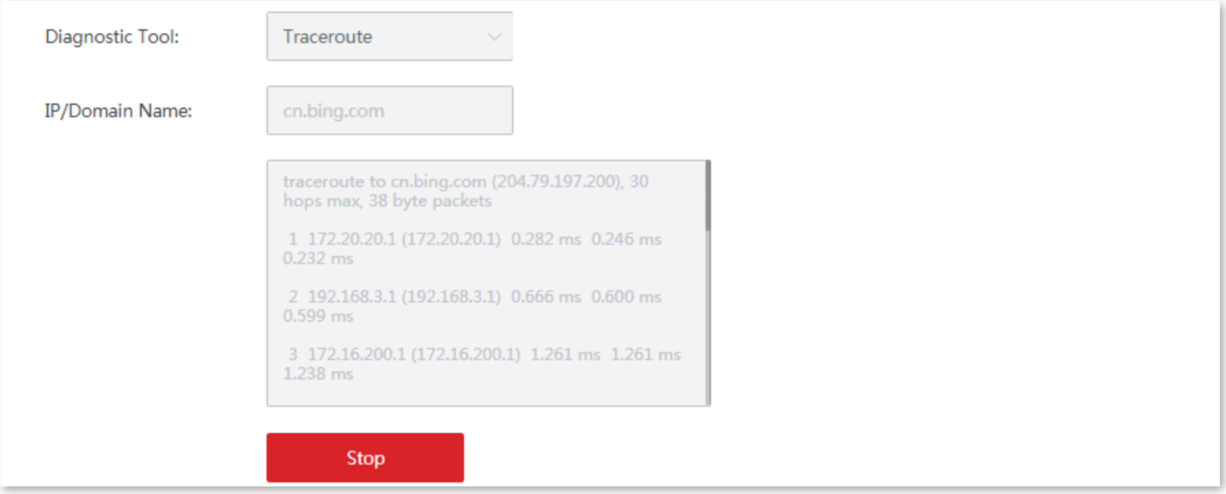


Diagnostic Tool: Traceroute

IP/Domain Name: cn.bing.com

----End

Wait a moment. The traceroute result will be displayed in the result box. See the following figure.



Diagnostic Tool: Traceroute

IP/Domain Name: cn.bing.com

```
traceroute to cn.bing.com (204.79.197.200), 30
hops max, 38 byte packets

 1  172.20.20.1 (172.20.20.1)  0.282 ms  0.246 ms
0.232 ms

 2  192.168.3.1 (192.168.3.1)  0.666 ms  0.600 ms
0.599 ms

 3  172.16.200.1 (172.16.200.1)  1.261 ms  1.261 ms
1.238 ms
```

Click **Stop** to end the process as required.

3.11.9 System time

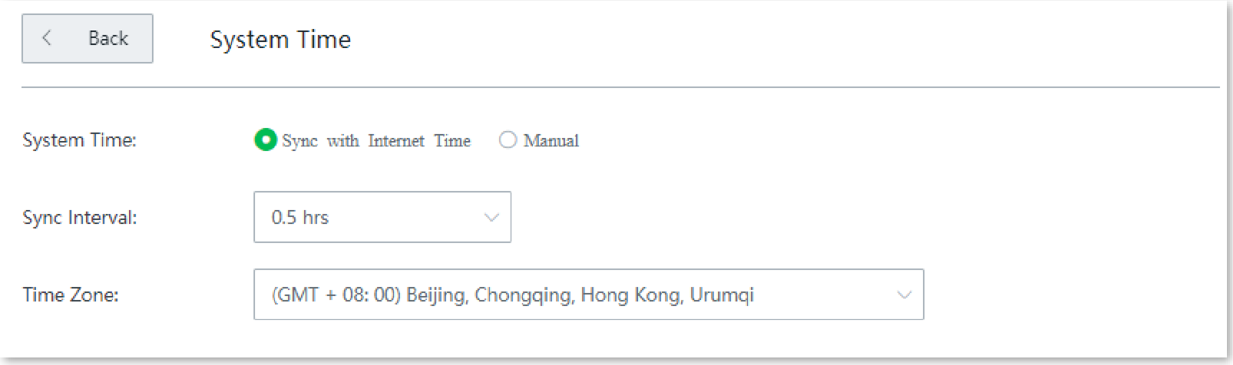
Overview

This function is used to set the system time of your device. To make the time-related functions effective, ensure that the system time of the device is set correctly.

The device supports:

- Synchronize with internet time (default)
- Set system time manually

Navigate to **Maintenance** > **System Time** to enter the page. See the following figure.



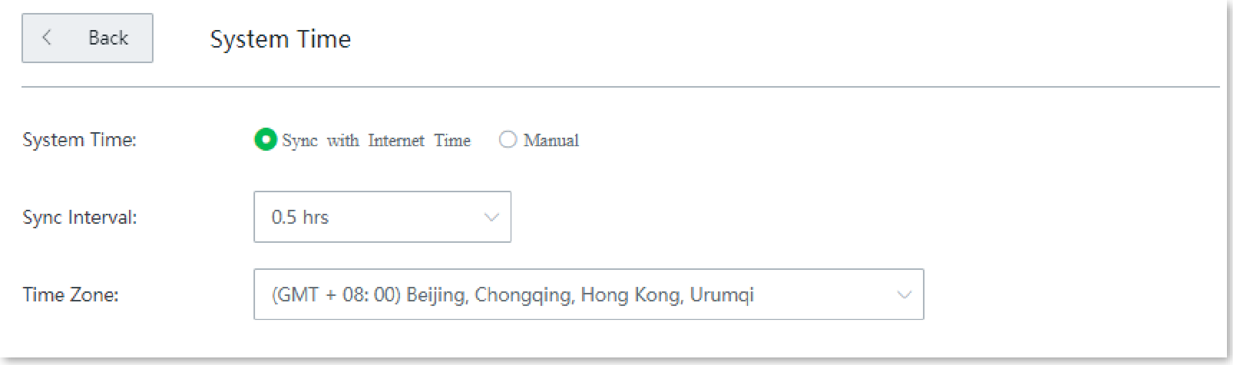
System Time: ● Sync with Internet Time ○ Manual

Sync Interval: 0.5 hrs

Time Zone: (GMT + 08: 00) Beijing, Chongqing, Hong Kong, Urumqi

Synchronize with internet time

In this method, the device automatically synchronizes its system time with the network time server (NTS). As long as the device is connected to the internet, the system time is correct.



System Time: ● Sync with Internet Time ○ Manual

Sync Interval: 0.5 hrs

Time Zone: (GMT + 08: 00) Beijing, Chongqing, Hong Kong, Urumqi

Parameter description

Parameters	Description
Sync Interval	It specifies an interval at which the device synchronizes its system time with the time server on the internet. By default, the device performs synchronization every 0.5 hours.

Parameters	Description
Time Zone	It specifies the time zone where the device is deployed.

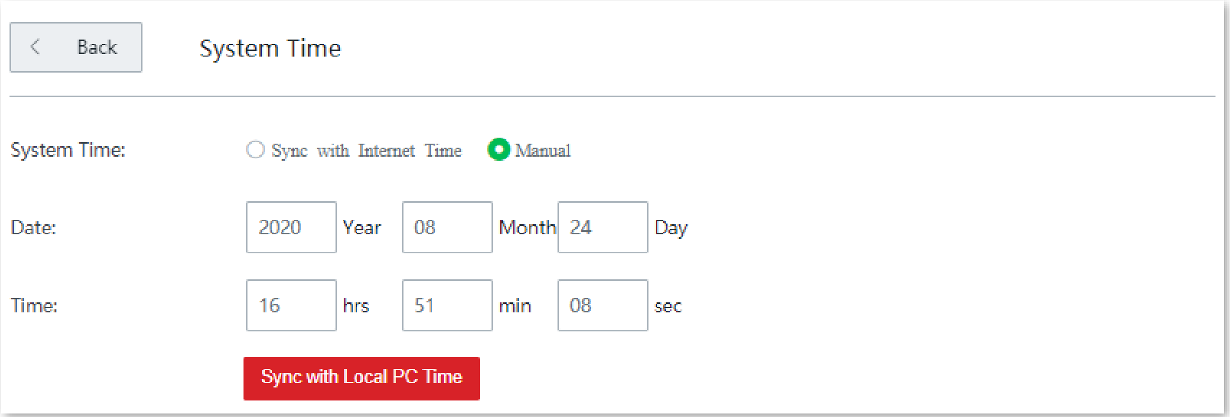
After configuration, navigate to the System status page to check whether it is synchronized.

Set system time manually

In this method, you can manually specify a system time for the device. When **Manual option** is selected**,** the related parameters are shown as follows.

Tip

In this method, you need to manually reconfigure the system time each time the device reboots.



System Time: ○ Sync with Internet Time ● Manual

Date: 2020 Year 08 Month 24 Day

Time: 16 hrs 51 min 08 sec

Parameter description

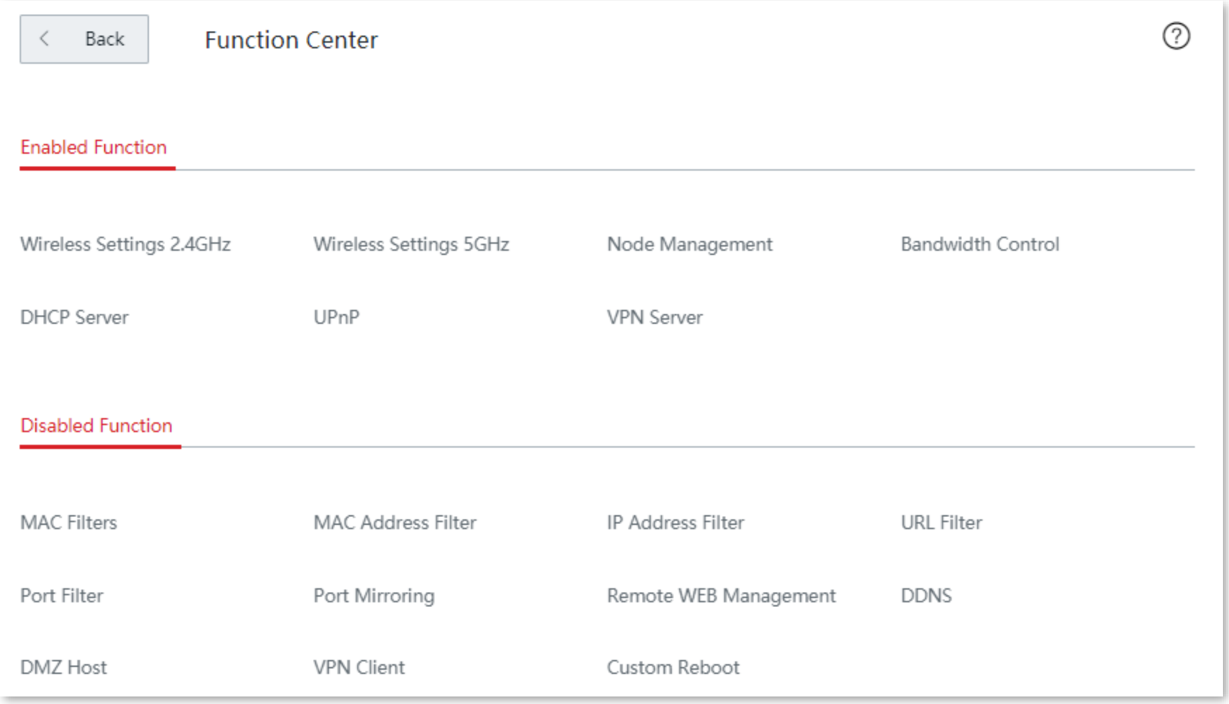
Parameters	Description
Date	Manually enter the date and time as needed.
Time	
Sync with Local PC Time	It allows you to synchronize the system time of the device with the system time of the management computer. Click this button, the device auto-fills the system time of your management computer.

After configuration, navigate to the System status page to check whether it is synchronized.

3.11.10 Function center

The function center groups all functions of the device into **Enabled Function** and **Disabled Function**, giving you a clearly insight into the functions that are enabled or disabled.

In addition, move the mouse pointer to a specific function and click it, you will be directed to the corresponding configuration page.



Enabled Function

Wireless Settings 2.4GHz   Wireless Settings 5GHz   Node Management   Bandwidth Control

DHCP Server   UPnP   VPN Server

Disabled Function

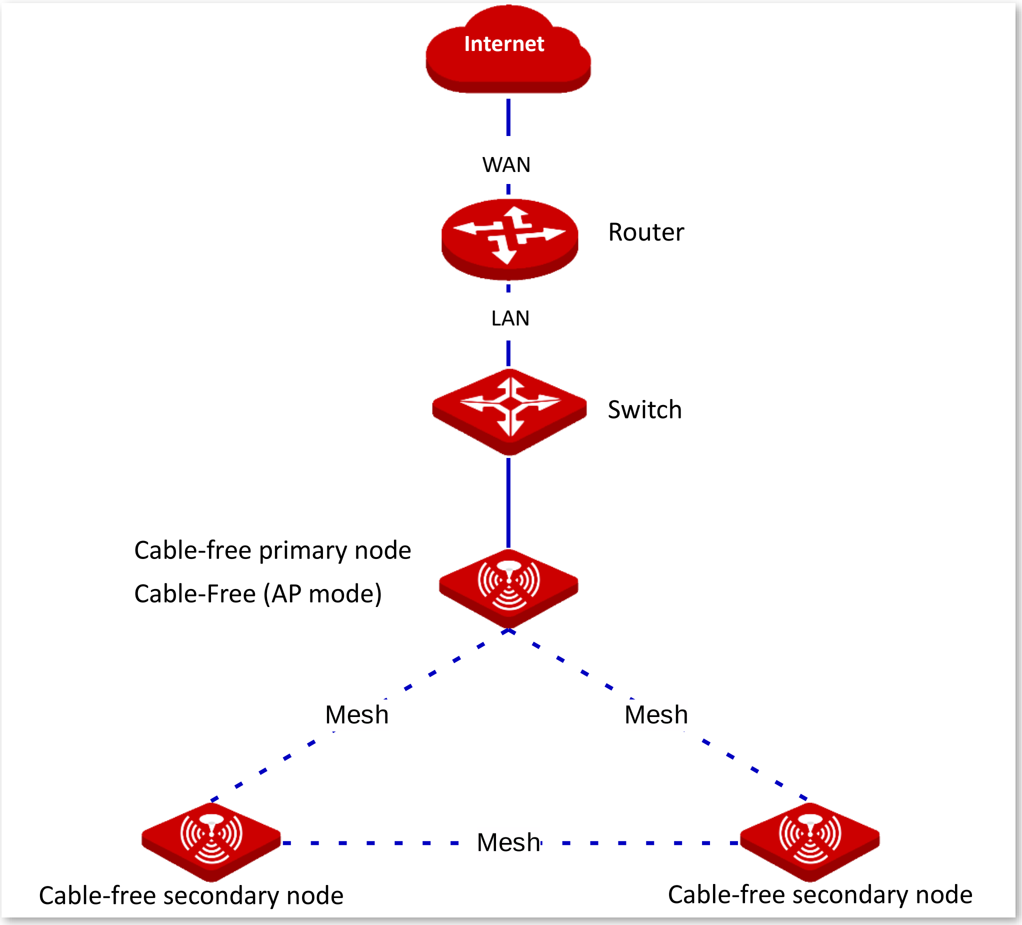
MAC Filters   MAC Address Filter   IP Address Filter   URL Filter

Port Filter   Port Mirroring   Remote WEB Management   DDNS

DMZ Host   VPN Client   Custom Reboot

4 Cable-free (AP mode)

When working in Cable-free (AP mode), the device serves as an AP. It can provide Mesh wireless network coverage with other cable-free devices. See the following topology.



4.1 System status

In this section, you can:

- Add secondary node devices.
- Check device info.
- Manage online devices.
- Check the RF status.

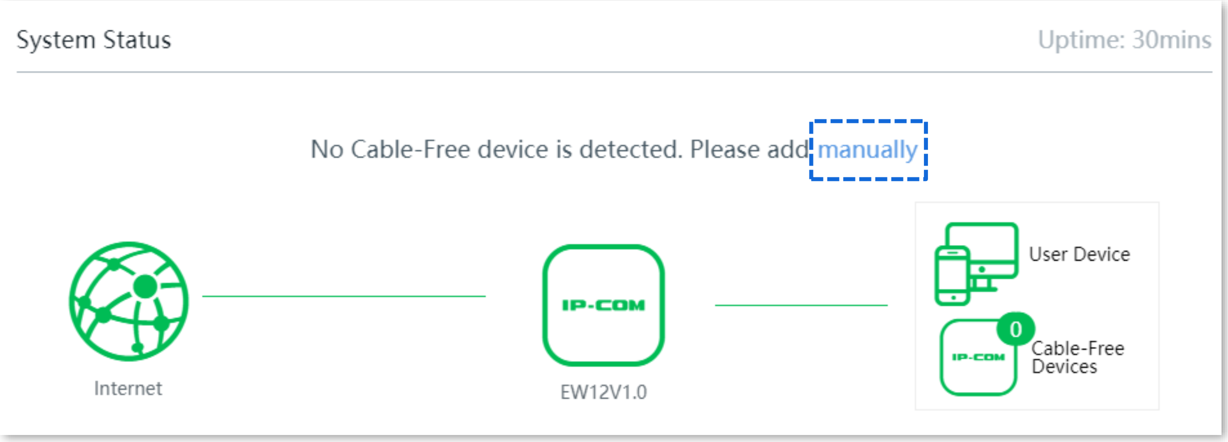
Click **System Status** to enter this page.

4.1.1 Add secondary node devices

The cable-free primary node can detect the secondary node devices in factory settings automatically. If not, you can also add them by logging in to the web UI of the device. You can add cable-free secondary nodes as needed.

Configuration procedure

1. Click manually.

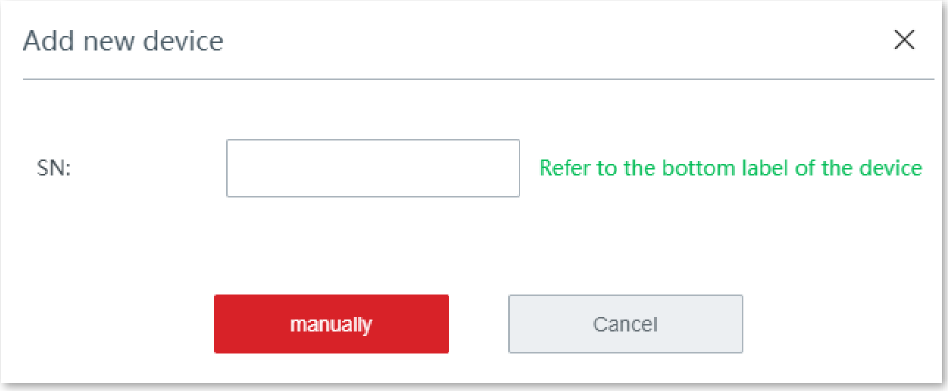


System Status

Uptime: 30mins

No Cable-Free device is detected. Please add manually

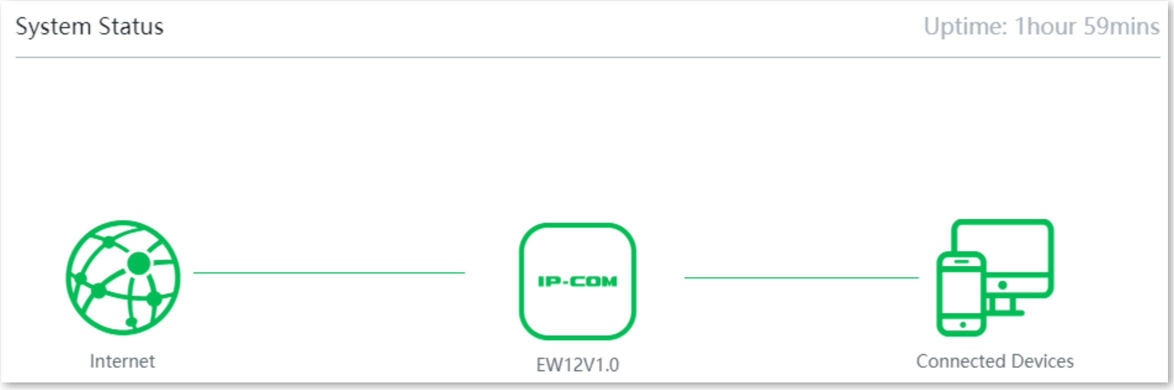
2. Enter the SN number of the secondary node device to be added, which can be found on the product label of the device.
3. Click manually.



Add new device

SN: Refer to the bottom label of the device

Wait a moment. The secondary node device is added to the mesh network successfully.



System Status

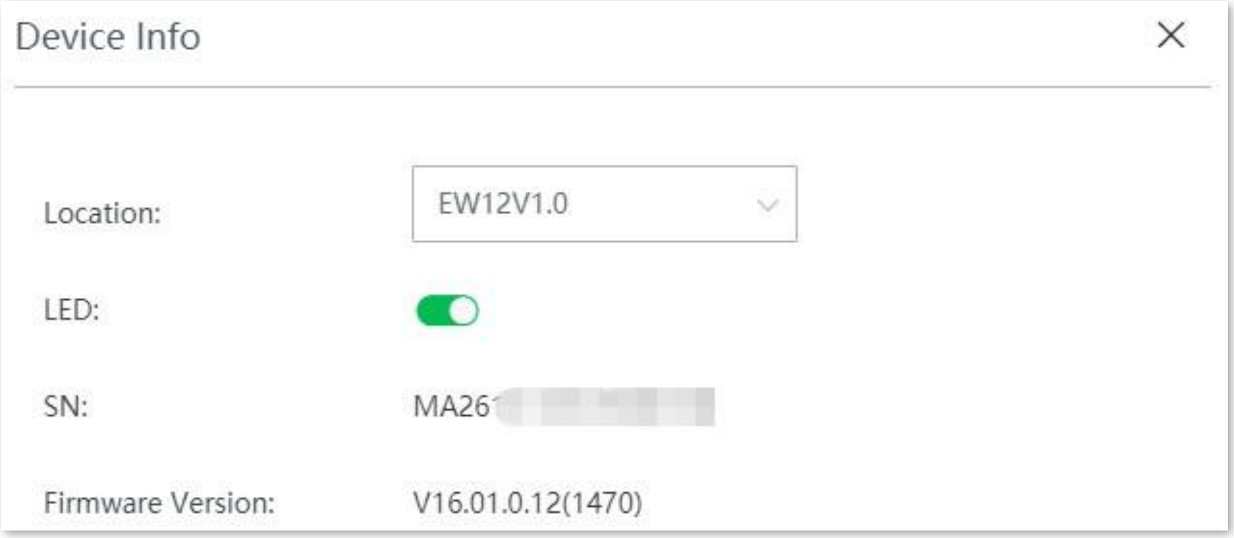
Uptime: 1hour 59mins

4.1.2 Check the device info

On the **System Status** page, click the icon , the **Device Info** window pops up.

The Device Info window consists of two parts: device information and operating status.

Device info



Device Info

Location: EW12V1.0

LED:

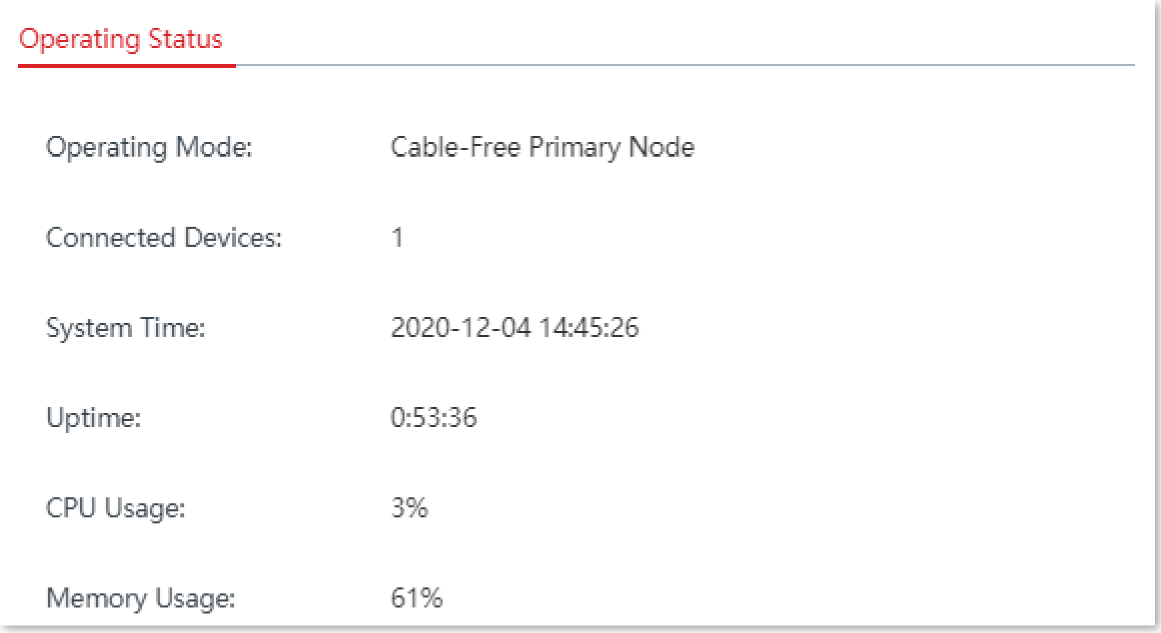
SN: MA26[redacted]

Firmware Version: V16.01.0.12(1470)

Parameter description

Parameter	Description
Device Name	It specifies the name of your device.
Location	It specifies the location information of your device. You can select a location description from the dropdown list or customize one as required.
LED	It specifies whether to turn on/off the LED indicator of the device. Enable: It indicates that the LED indicators are on. You can check the operating status of the device based on the LED indicators. Disable: It indicates that the LED indicators are off.
SN	It specifies the serial number of the device.
Firmware Version	It specifies the firmware version number of the device.

Operating status



Operating Status

Operating Mode: Cable-Free Primary Node

Connected Devices: 1

System Time: 2020-12-04 14:45:26

Uptime: 0:53:36

CPU Usage: 3%

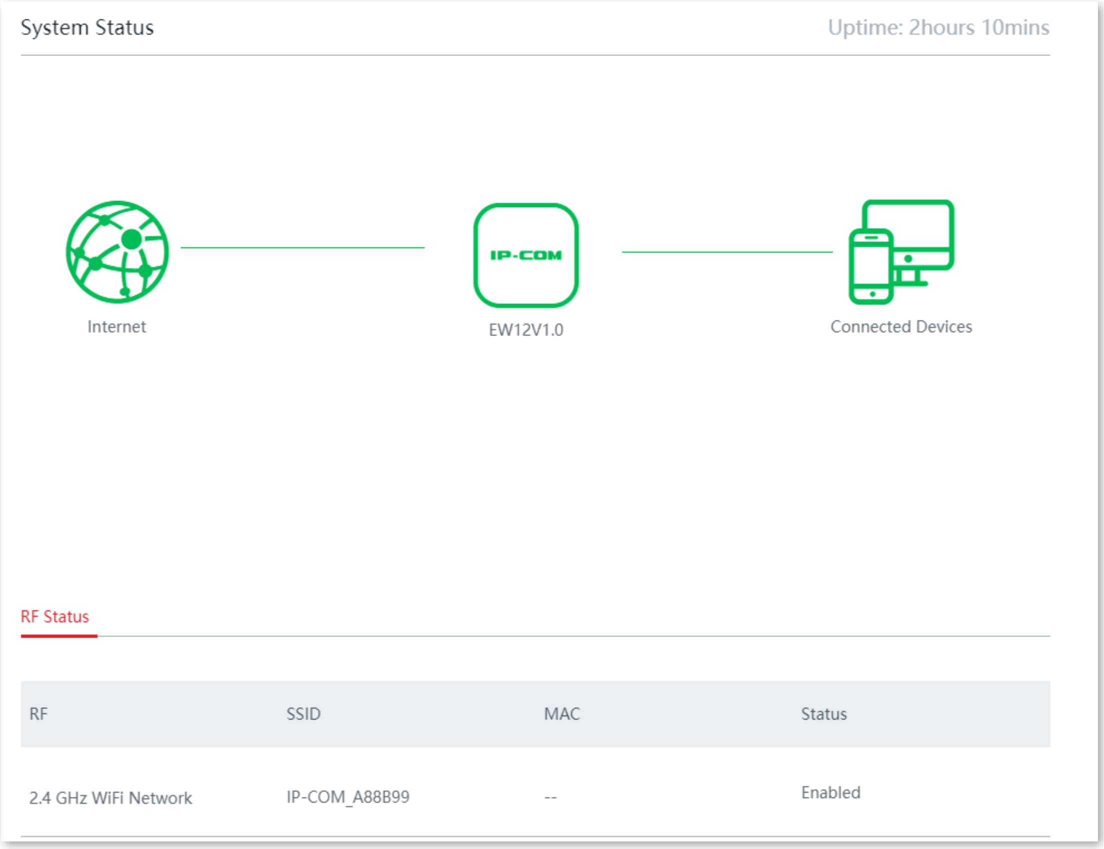
Memory Usage: 61%

Parameter description

Parameter	Description
Uptime	It specifies the time that has elapsed since the device was started last time.
Operating Mode	It specifies the current working mode of the device.
Connected Devices	It specifies the number of devices connected to the device currently.
LAN IP Address	It specifies the IP address of the AP, which is managed IP address as well. Users in LAN can use this IP address to log in to the web UI of the device. The default is 192.168.5.1.
MAC Address	It specifies the MAC address of the LAN port of the device.
System Time	It specifies the current system time of the device. You can set system time by navigating to Maintenance > System time.
CPU Usage	It specifies the current CPU usage of the device.
Memory Usage	It specifies the current memory usage of the device.

4.1.3 Manage the online devices

The **System Status** page directly presents the top 5 clients with the highest speed. Click the **Connected Devices** icon 🖥 to view all connected clients.



System Status

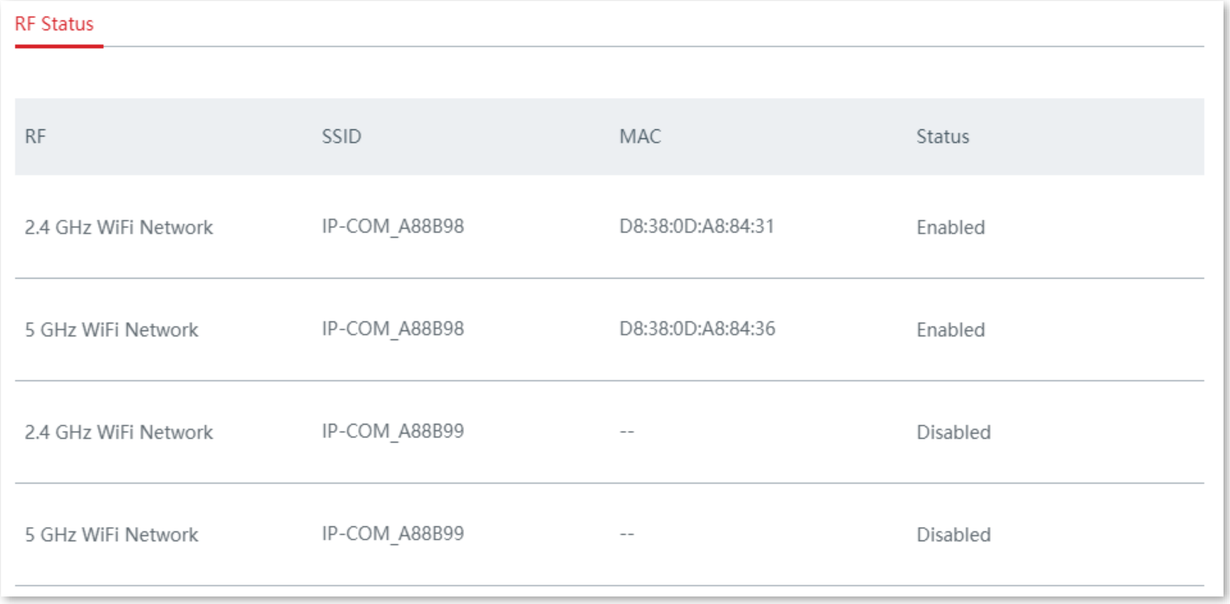
Uptime: 2hours 10mins

RF Status

RF	SSID	MAC	Status
2.4 GHz WiFi Network	IP-COM_A88B99	--	Enabled

4.1.4 Check the RF status

In this section, you can check the name, MAC address, and network enabled status of each WiFi network on the node.



RF Status

RF	SSID	MAC	Status
2.4 GHz WiFi Network	IP-COM_A88B98	D8:38:0D:A8:84:31	Enabled
5 GHz WiFi Network	IP-COM_A88B98	D8:38:0D:A8:84:36	Enabled
2.4 GHz WiFi Network	IP-COM_A88B99	--	Disabled
5 GHz WiFi Network	IP-COM_A88B99	--	Disabled

4.2 Wireless

In this module, you are allowed to view and edit SSIDs (WiFi names) and WiFi passwords, configure other settings of 2.4 GHz and 5 GHz WiFi networks separately, hide your WiFi networks so that nearby wireless clients cannot detect them, and specify how many wireless clients can connect to a WiFi network.

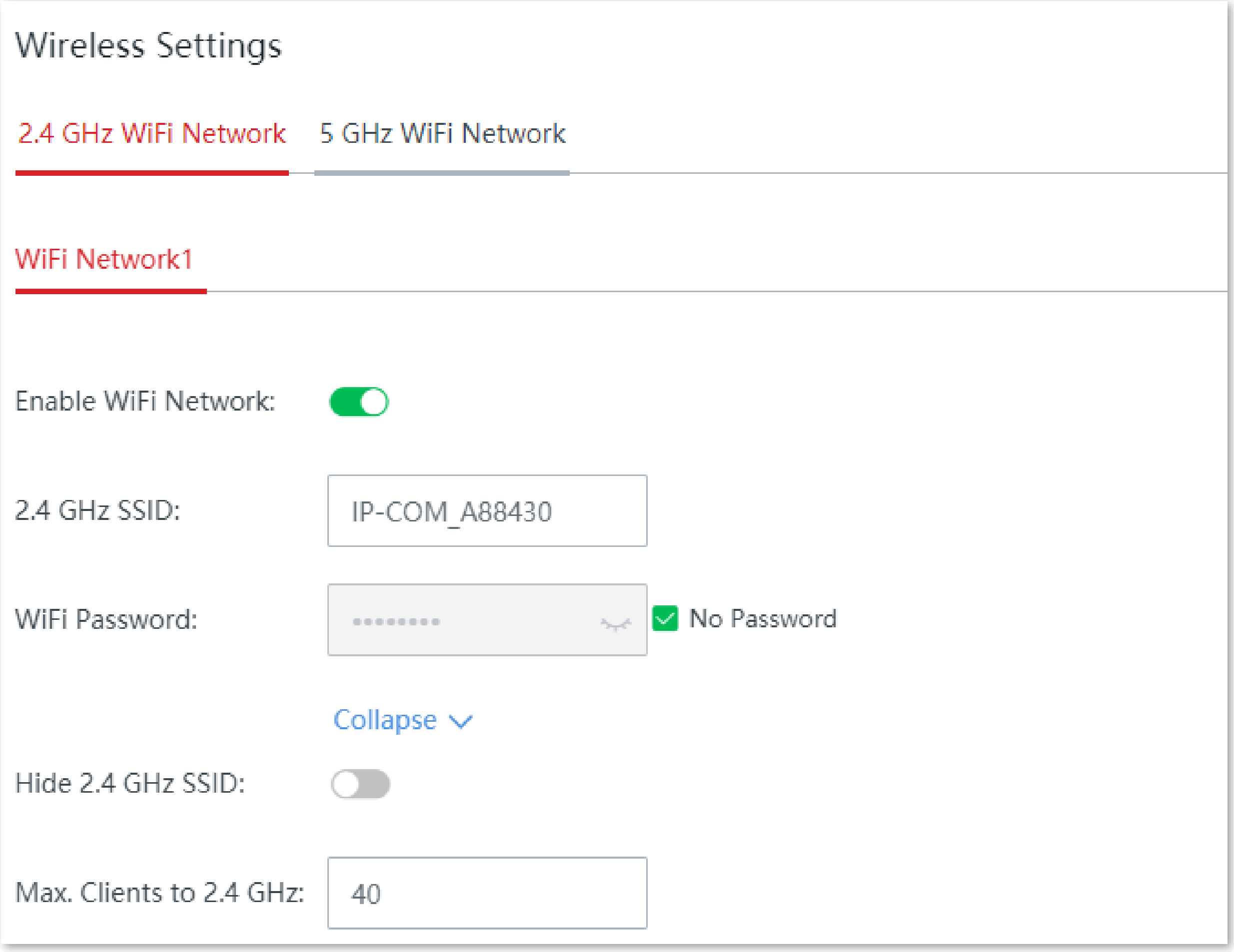
This dual-band device supports at most three 2.4 GHz WiFi networks, and three 5 GHz WiFi networks. By default, the SSIDs for 2.4 GHz WiFi Network 1 and 5 GHz WiFi Network 1 are unified, and only **WiFi Network1** is enabled.

Tip

The configuration of this module will be applied synchronously to other nodes in the cable-free network.

4.2.1 Wireless settings

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


Wireless Settings

Enable WiFi Network: ●

2.4 GHz SSID: IP-COM_A88430

WiFi Password: ••••••••• ☑ No Password

Hide 2.4 GHz SSID: ○

Max. Clients to 2.4 GHz: 40

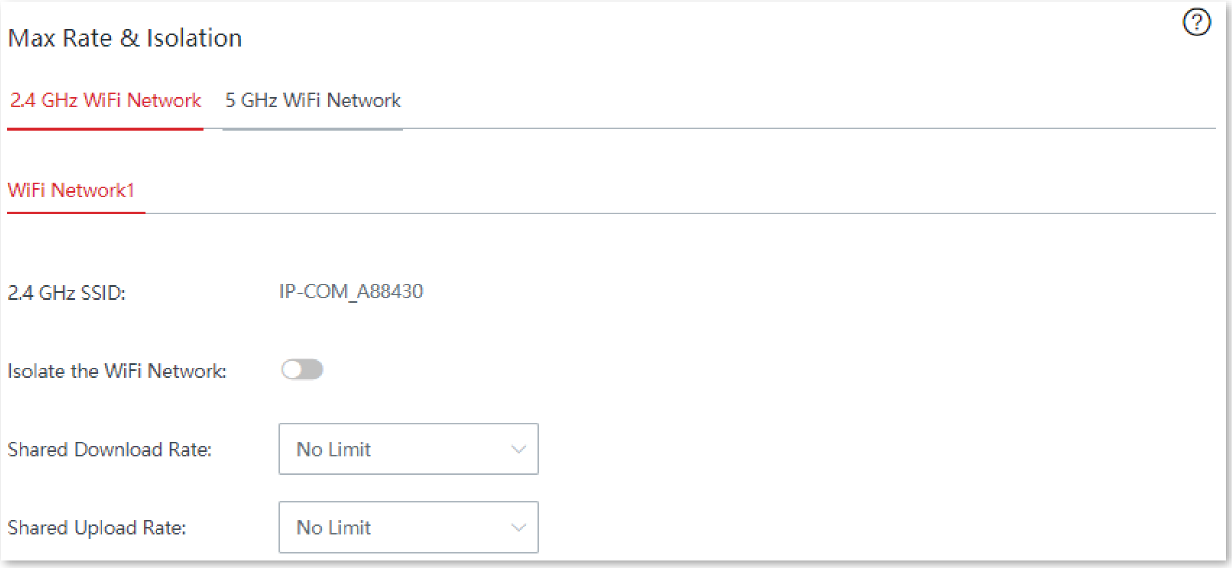
Parameter description

Parameter	Description
Enable WiFi Network1/2/3	It is used to enable/disable the corresponding WiFi network of the device.
SSID	It specifies the WiFi name of the corresponding WiFi network.
WiFi Password	It specifies the password for wireless internet connection. You are recommended to use the combination of digits, letters and special characters for higher security. Selecting **No Password** indicates that wireless clients can connect to the WiFi network without a password. Select this option only when necessary since it leads to weak network security.
Hide SSID	With this function enabled, nearby wireless clients cannot detect the SSID and you need to manually enter the SSID on the wireless client to access the WiFi network. Disable indicates that nearby wireless clients can detect the SSID. By default, this function is disabled.
Max. Clients	It specifies maximum number of wireless clients that can be connected to the WiFi network at each frequency band. After the value is reached, this WiFi network denies new connection requests.

4.2.2 Max rate & isolation

Network isolation makes clients connected to different networks of the device cannot communicate with each other.

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



2.4 GHz SSID: IP-COM_A88430

Isolate the WiFi Network: ○

Shared Download Rate: No Limit

Shared Upload Rate: No Limit

Parameter description

Parameter	Description
SSID	It specifies the WiFi name of the corresponding WiFi network.
Isolate this network	With this function enabled, clients connected to different WiFi networks of this device cannot communicate with each other, leading to higher WiFi network security. By default, this function is disabled.
No Access to LAN	With this function enabled, clients connected to this WiFi network cannot access the Web UI and private network (LAN) of this node, protecting your LAN network security.
Shared Upload/Download Rate	It specifies the upload/download rate shared by clients connected to this WiFi network. Upload and download rate allocated to individual client may vary.

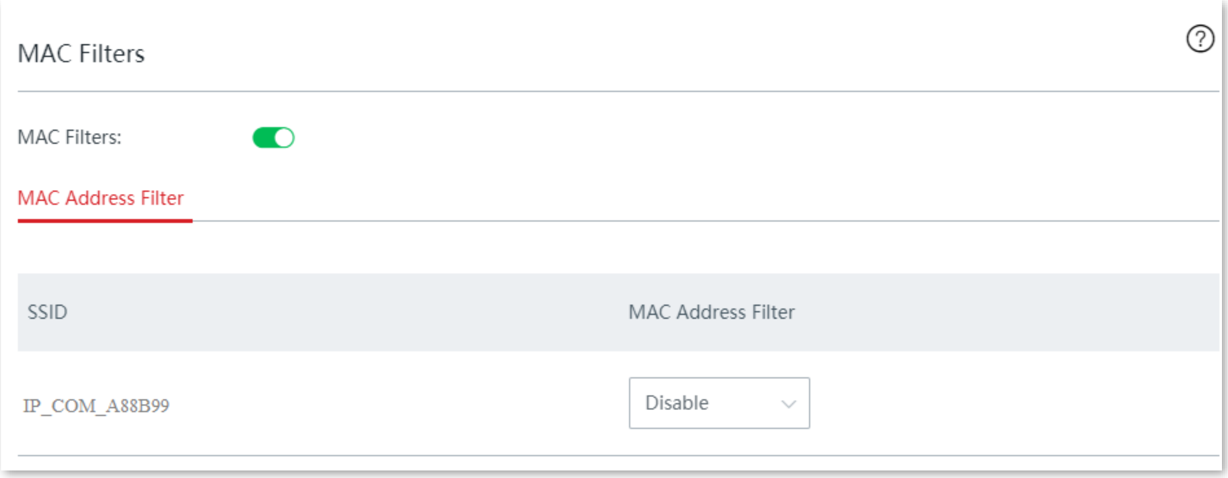
4.2.3 MAC filters

Overview

This module allows you to configure MAC address-based wireless access control rules. By default, this function is disabled.

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

To enable this function, set the MAC Filters from ○ to ● , and click **Save**. See the following figure.



MAC Filters

MAC Filters: ●

MAC Address Filter

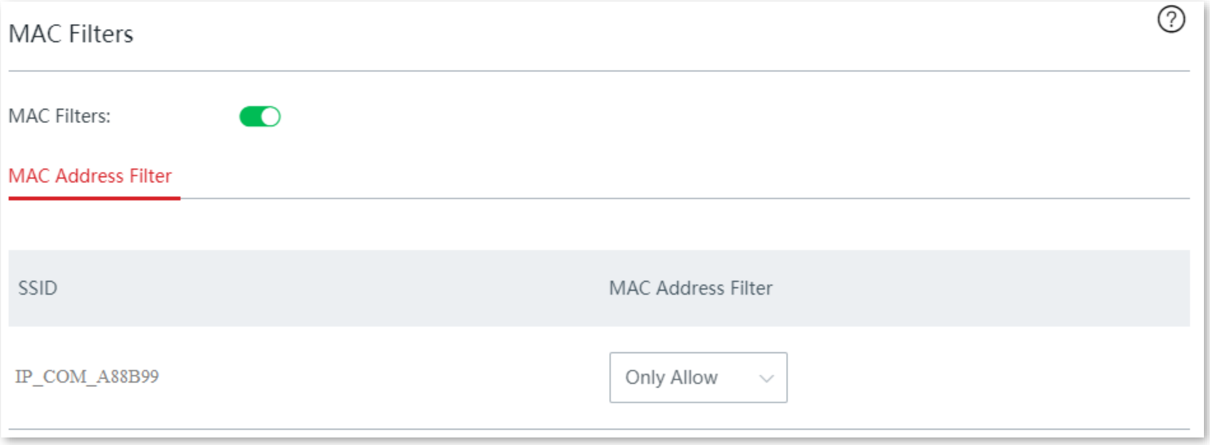
SSID	MAC Address Filter
IP_COM_A88B99	Disable

Parameter description

Parameter		Description
MAC Address Filter	SSID	It lists all the WiFi networks that the device supports. 💡 Tip If you unify the SSIDs of 2.4 GHz and 5 GHz bands, the corresponding WiFi networks only display one SSID here.
	MAC Address Filter	It specifies the modes you can perform on the corresponding WiFi network. There are three modes for selection: – **Disable**: This function is disabled, and all wireless clients can connect to this WiFi network. – **Only Allow**: Only wireless clients with the specified MAC address can connect to this WiFi network. – **Only Forbid**: Only wireless clients with the specified MAC address cannot connect to this WiFi network.
MAC Filters List	MAC Filters List	It specifies the wireless access control list you configured.
	MAC Address	It specifies the MAC address of the client to which the rule applies.
	Remark	Optional. It specifies the brief description you set for the corresponding MAC address.
	Effective Network	It specifies the WiFi network(s) to which the wireless client with this MAC address applies.
	Status	It specifies whether the rule is enabled or not. ○: This rule is disabled. ● : This rule is enabled.
	Action	It specifies the operations you can do on the rule. ✎: Click it to edit the rule. 🗑 : Click it to delete the rule.

Create a MAC filter rule

1. Set the **MAC Filters** from ○ to ● , select MAC address filter mode for the corresponding SSID from the **MAC Address Filter** drop-down list menu, and click **Save**.



MAC Filters

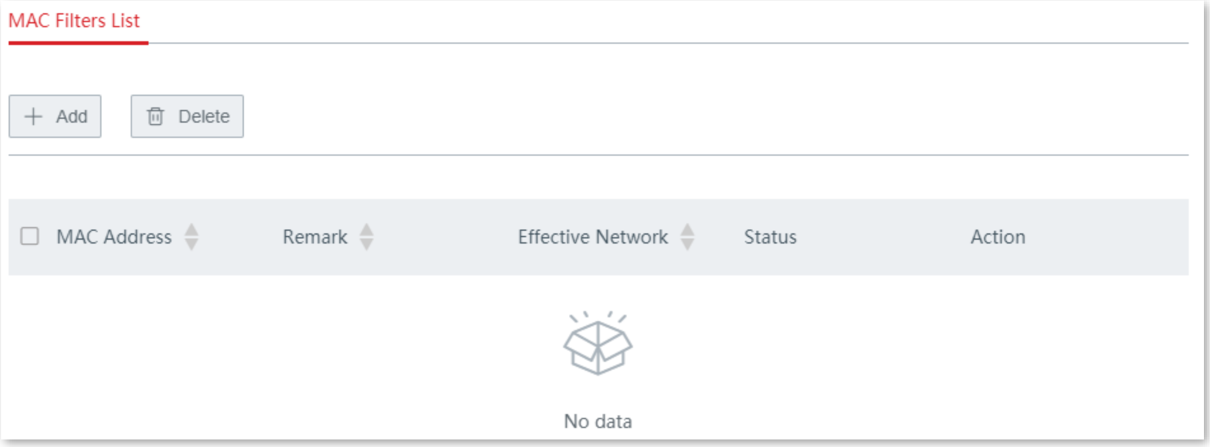
MAC Filters: ●

MAC Address Filter

SSID	MAC Address Filter
IP_COM_A88B99	Only Allow

2. Create a MAC filter rule.

(1) Click **Add**. The **Add** configuration window appears.



MAC Filters List

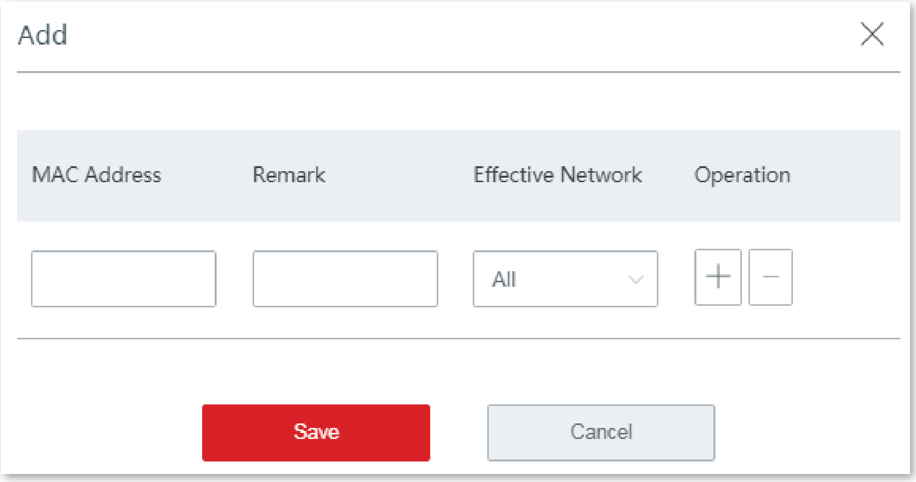
□ MAC Address	Remark	Effective Network	Status	Action

No data

(2) Set up the following parameters.

- Enter the MAC address of the client in **MAC Address** input box.
- Specify a description for the client in **Remark** input box.
- Select the WiFi network from the drop-down list menu of the **Effective Network**.

(3) Click **Save**.



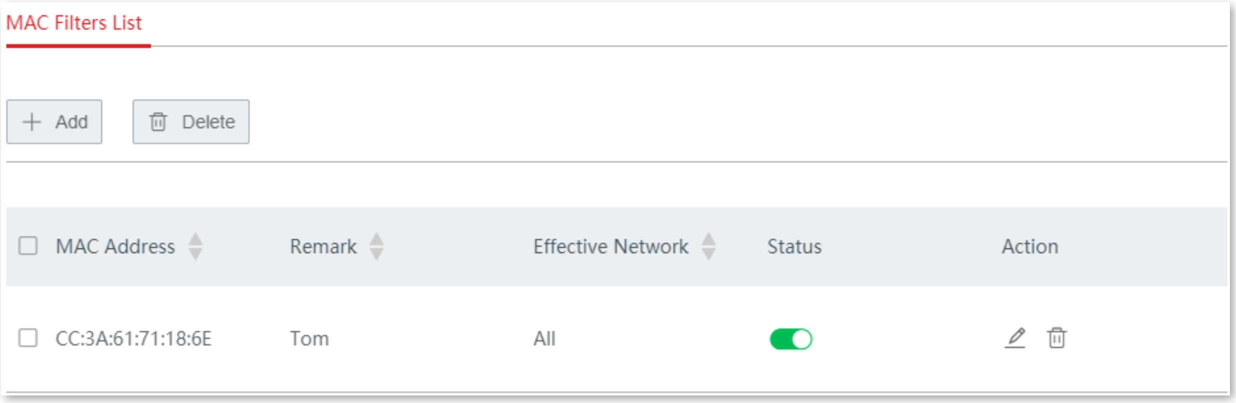
Add ×

MAC Address	Remark	Effective Network	Operation
		All	+ −

Save Cancel

----End

After it is saved successfully, you can see it in the MAC Filters List.



MAC Filters List

+ Add Delete

□ MAC Address	Remark	Effective Network	Status	Action
□ CC:3A:61:71:18:6E	Tom	All	●	✎ 🗑

Example of configuring MAC filters

Network requirement

An enterprise uses EW12 to set up a LAN to meet the following requirement:

Only the purchasing staff is allowed to connect to the WiFi network (Purchase) to access the internet.

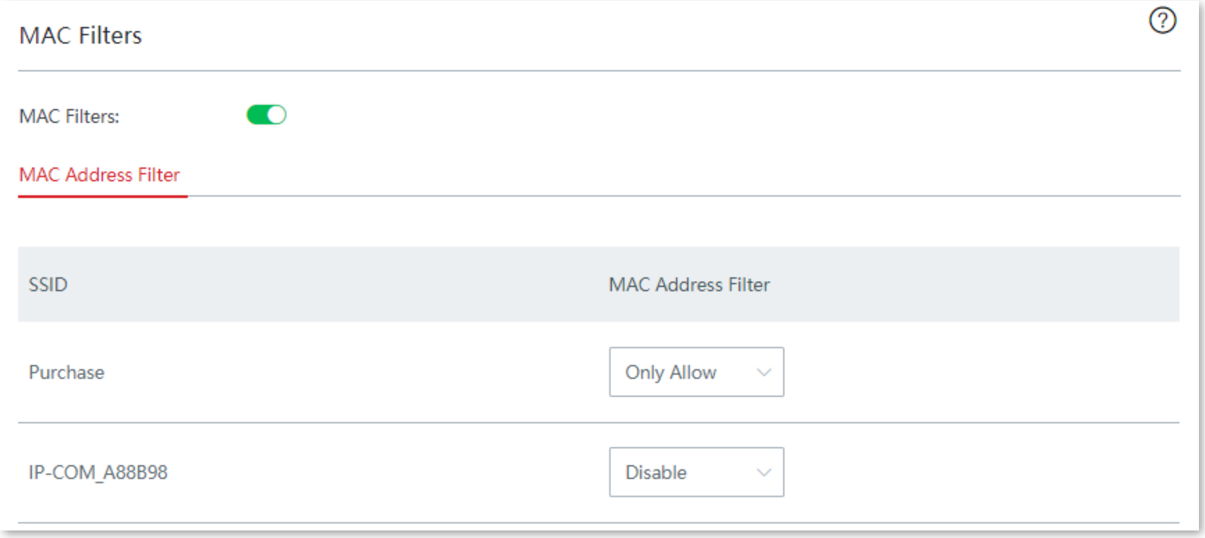
Assume that the MAC address of the purchasing staff's computer is CC:3A:61:71:1B:6E.

Solutions

The MAC filters can meet this requirement.

Configuration procedure

1. Set the **MAC Filters** from ○ to ●, select **Only Allow** for **Purchase** from the **MAC Address Filter** drop-down list menu, and click **Save**.



MAC Filters

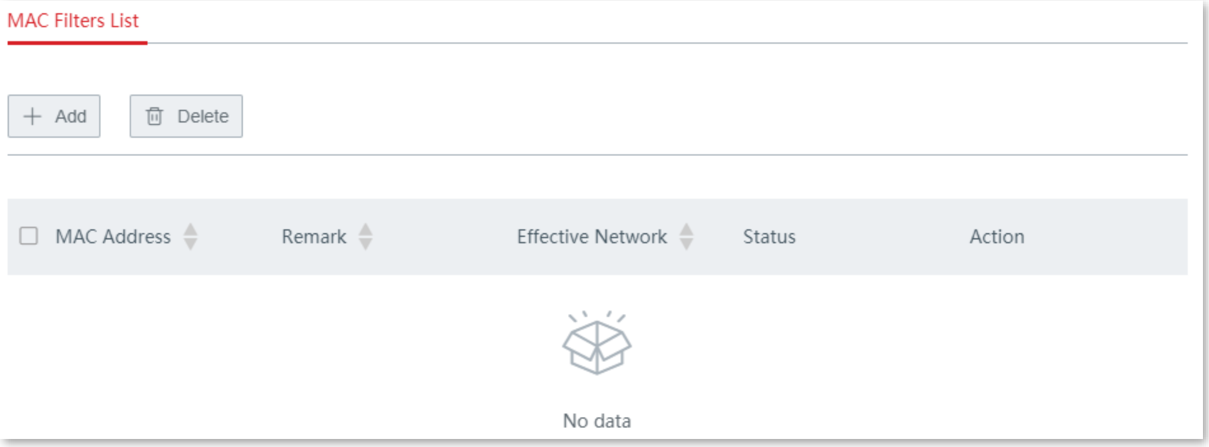
MAC Filters:

MAC Address Filter

SSID	MAC Address Filter
Purchase	Only Allow
IP-COM_A88B98	Disable

2. Create a MAC filter rule.

(1) Click **Add**. The **Add** configuration window appears.



MAC Filters List

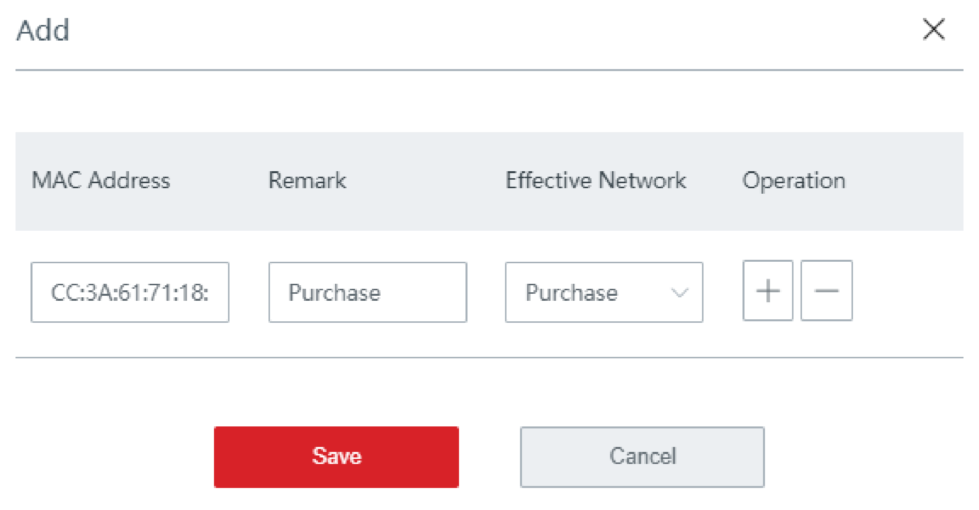
□ MAC Address	Remark	Effective Network	Status	Action

No data

(2) Set the following parameters.

- Enter **CC:3A:61:71:1B:6E** in the **MAC Address** input box.
- Enter **Purchase** in the **Remark** input box.
- Select **Purchase** from the drop-down list menu of the **Effective Network**.

(3) Click **Save**.

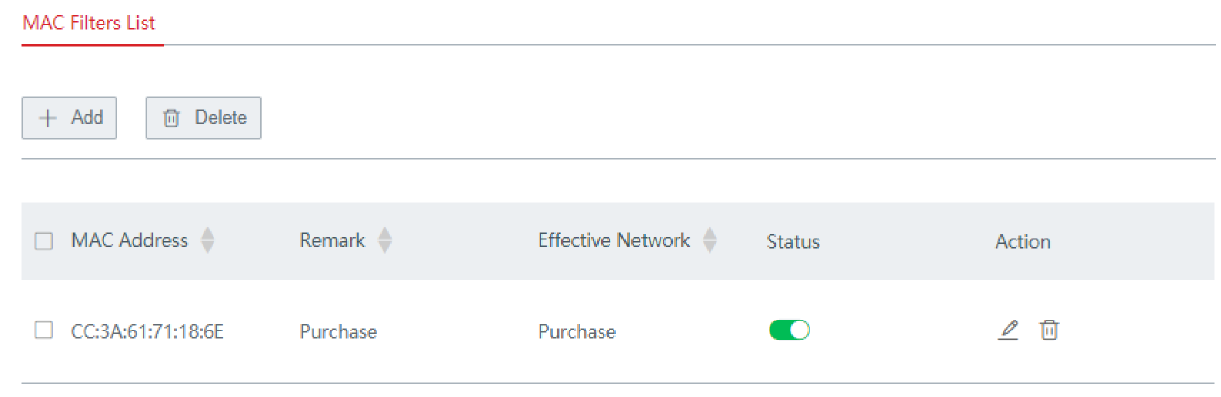


Add

MAC Address	Remark	Effective Network	Operation
CC:3A:61:71:18:	Purchase	Purchase	+ −

----End

After the rule is saved, you can see it in the **MAC Filters List**.



MAC Filters List

□ MAC Address	Remark	Effective Network	Status	Action
□ CC:3A:61:71:18:6E	Purchase	Purchase	●	

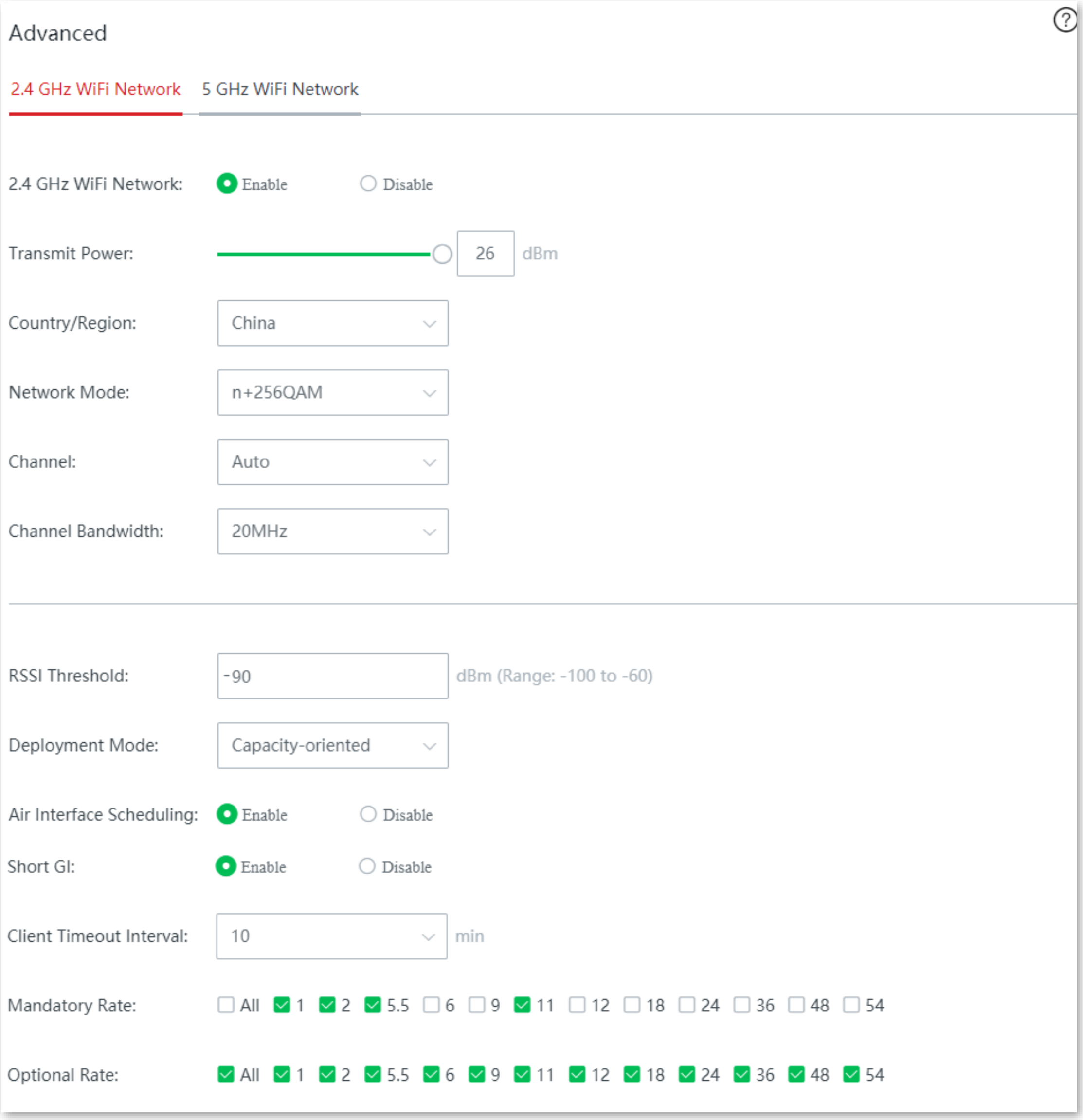
Verification

Only the computer with the MAC address of CC:3A:61:71:1B:6E can connect to the WiFi network (**Purchase**), and other devices are blocked.

4.2.4 Advanced

This page allows you to configure the advanced parameters such as transmit power, network mode, deployment mode, and air interface scheduling.

Navigate to **Wireless** > **Advanced** to enter the configuration page.



Advanced

2.4 GHz WiFi Network | 5 GHz WiFi Network

2.4 GHz WiFi Network: ● Enable ○ Disable

Transmit Power: 26 dBm

Country/Region: China

Network Mode: n+256QAM

Channel: Auto

Channel Bandwidth: 20MHz

RSSI Threshold: -90 dBm (Range: -100 to -60)

Deployment Mode: Capacity-oriented

Air Interface Scheduling: ● Enable ○ Disable

Short GI: ● Enable ○ Disable

Client Timeout Interval: 10 min

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

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

Parameter description

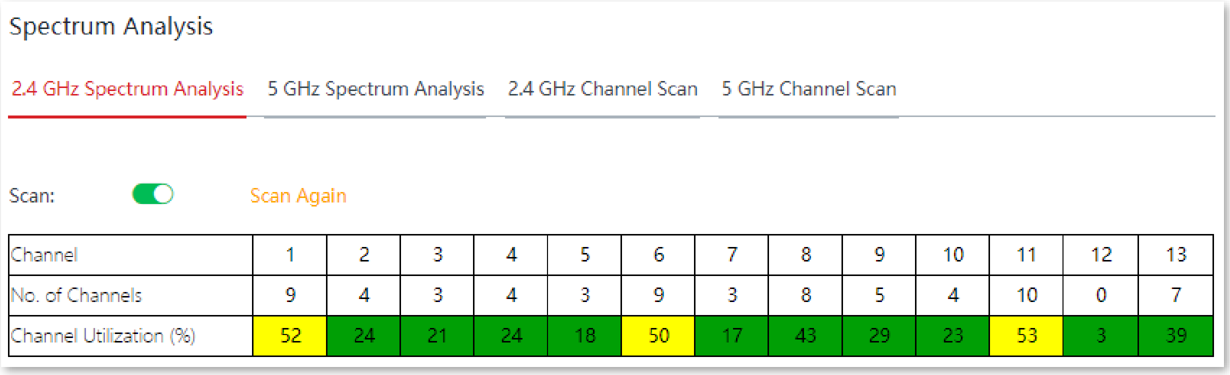
Parameter	Description
Transmit Power	It specifies transmit power of this device. Unit: dBm. A higher value leads to wider WiFi coverage. However, decreasing the value properly increases performance and security of the WiFi network.
Country/Region	It specifies country or region where this device is located. Select your country or region to ensure that this device complies with the channel regulations.

Parameter	Description
Network Mode	It specifies the WiFi network mode (also called 802.11 mode, radio mode, or wireless mode) of the node. A proper network mode enables the clients to get the maximum transmission rate and compatibility. Available options for 2.4 GHz band: – 11b: In this mode, only 802.11b wireless devices are allowed to access the node's 2.4 GHz WiFi network. – 11g: In this mode, only 802.11g wireless devices are allowed to access the node's 2.4 GHz WiFi network. – 11b/g: In this mode, 802.11b and 802.11g wireless devices can access the node's 2.4 GHz WiFi network. – 11b/g/n (default): In this mode, 802.11b, 802.11g and 802.11n wireless devices operating at 2.4 GHz can access the node's 2.4 GHz WiFi network. – n+256QAM: In this mode, 802.11b, 802.11g and 802.11n wireless devices operating at 2.4 GHz can access the node's 2.4 GHz WiFi network. QAM is known as Quadrature Amplitude Modulation, which is a modulation method of amplitude modulation on two orthogonal carriers. It modulates signals simultaneously by using the orthogonality of sine wave and cosine wave to improve the modulation efficiency. n+256QAM is at the 2.4 GHz band. Switch the IEEE 802.11n standard to the 256-QAM modulation mode of IEEE 802.11ac, and the single-stream rate also increases from 150 Mbps of IEEE 802.11n standard to 200 Mbps of IEEE 802.11ac standard. This enhancement is only effective when the 2.4 GHz band is supported by both the transmitter and the receiver. If either part does not support n+256QAM, the highest single-stream rate in the 2.4 GHz band is still 150 Mbps. After the modulation mode is changed to n+256QAM, the network stability and anti-interference performance are inferior to other modes. Available options for 5 GHz band: – 11a: In this mode, only 802.11a wireless devices are allowed to access the node's 5 GHz WiFi network. – 11ac (default): In this mode, only 802.11ac wireless devices are allowed to access the node's 5 GHz WiFi network. – 11a/n mixed: In this mode, 802.11a and 802.11n wireless devices operating in 5 GHz can access the node's 5 GHz WiFi network. It cannot be modified when the device works in Cable-Free (Router mode).

Parameter	Description
Channel	It specifies the channel in which this device operates. Select one idle channel in the ambient environment to prevent interference. Auto indicates that this device automatically changes to a channel rarely used in the ambient environment to prevent interference.
Channel Bandwidth	It is used to select the channel bandwidth to accommodate higher transmission speed. Available options for 2.4 GHz band: 20MHz, 40MHz, and 20/40MHz. Available options for 5 GHz band: 20MHz, 40MHz, and 80MHz.
RSSI Threshold	It is used to set the minimum strength of received signals acceptable to this device. If the strength of the signals transmitted by a wireless client is weaker than this threshold, the wireless client cannot connect to this device.
Deployment Mode	It is used to select a mode that address your application scenario. – **Coverage-oriented**: Apply to scenarios with large area, multiple walls, decentralized users and less than 10 SSIDs in ambient environment. – **Capacity-oriented**: Apply to scenarios with intensive users, open and large areas, and more than 25 SSIDs in ambient environment.
Air Interface Scheduling	With this function, you can allocate time equally among clients, preventing low-speed clients from consuming too much resources, thus increasing performance and throughput of the device.
Short GI	It specifies short guard interval for preventing data block interference. Propagation delays may occur on the receiver side due to factors such as multipath wireless signal transmission. If a data block is transmitted at an overly high speed, it may interfere with the previous data block. The short GI helps prevent such interference. Enabling the short GI can yield a 10% improvement in wireless data throughput.
Client Timeout Interval	If a wireless client does not exchange data with the node within the specified period, the device disconnects the client.
APSD	It specifies Automatic Power Save Delivery. This function enables the device to reduce power consumption after a specified period during which no traffic is transmitted or received. By default, it is disabled.
Mandatory Rate	It specifies the basic rate sets for normal operation of the node. You can adjust the mandatory rates to restrict low-rate clients accessing the WiFi network and improve the internet experience of other clients. – **Mandatory Rate**: The clients can connect to the node only when they meet the mandatory rate required by the router. – **Optional Rate**: The clients meeting the mandatory requirement can connect to the node with higher rate.
Optional Rate	

4.2.5 Spectrum analysis

In this section, you can check the number of WiFi networks and channel utilization of each channel, and select a channel with low utilization as the working channel of the node to improve the wireless transmission efficiency.



Spectrum Analysis

Scan: ●

Channel	1	2	3	4	5	6	7	8	9	10	11	12	13
No. of Channels	9	4	3	4	3	9	3	8	5	4	10	0	7
Channel Utilization (%)	52	24	21	24	18	50	17	43	29	23	53	3	39

- A channel utilization under green paint indicates an idle channel.
- A channel utilization under yellow paint indicates a crowded channel.
- A channel utilization under red paint indicates an extremely crowded channel and the channel cannot be used.

4.3 Smart optimization

The Smart Optimization function is used to optimize the entire mesh network. Click **Smart Optimization** to enter this page.

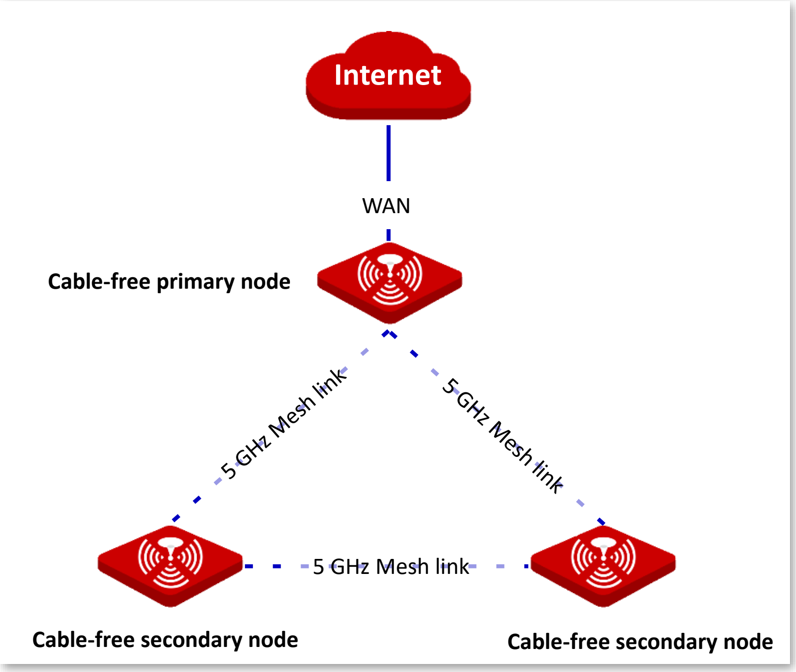
4.3.1 Wired networking

Overview

The cable-free device supports two networking modes: cable-free networking and wired networking. Cable-free networking is adopted by default.

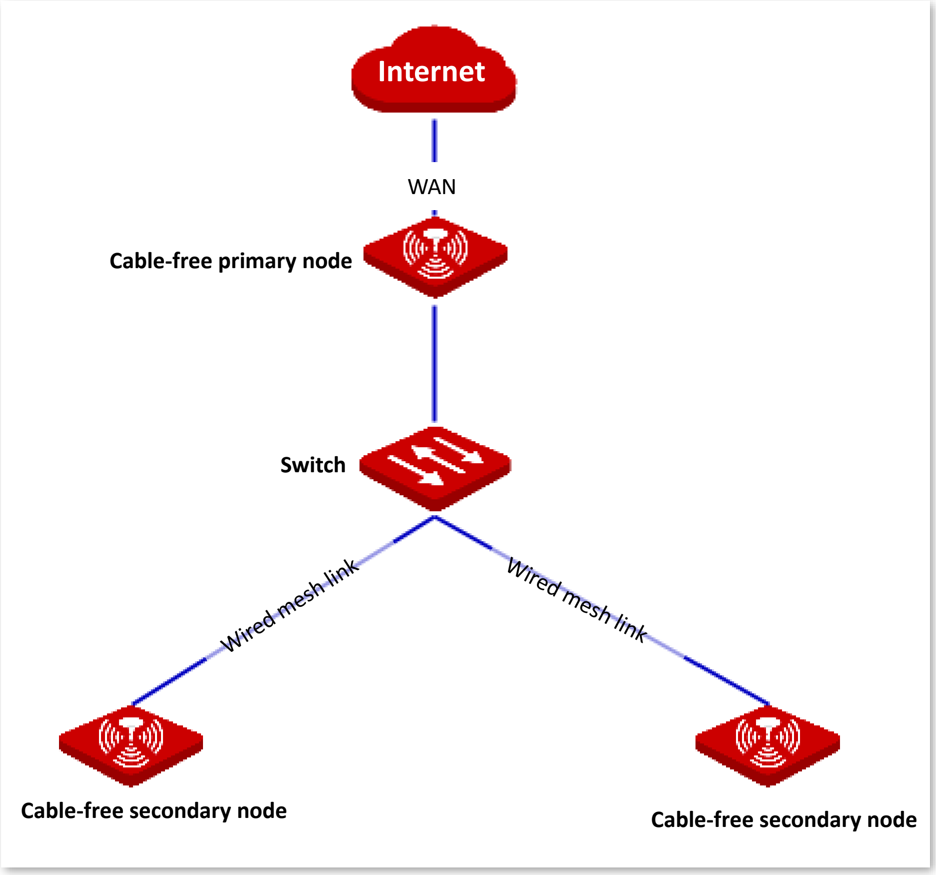
- **Cable-free networking**

The cable-free network system is set up in a wired manner, and each cable-free device is connected wirelessly. The cable-free device will use one of the 5 GHz wireless frequency bands specially for establishing the wireless mesh link. The 2.4 GHz wireless frequency band and another 5 GHz wireless frequency band will be used for terminal devices' access.



- **Wired networking**

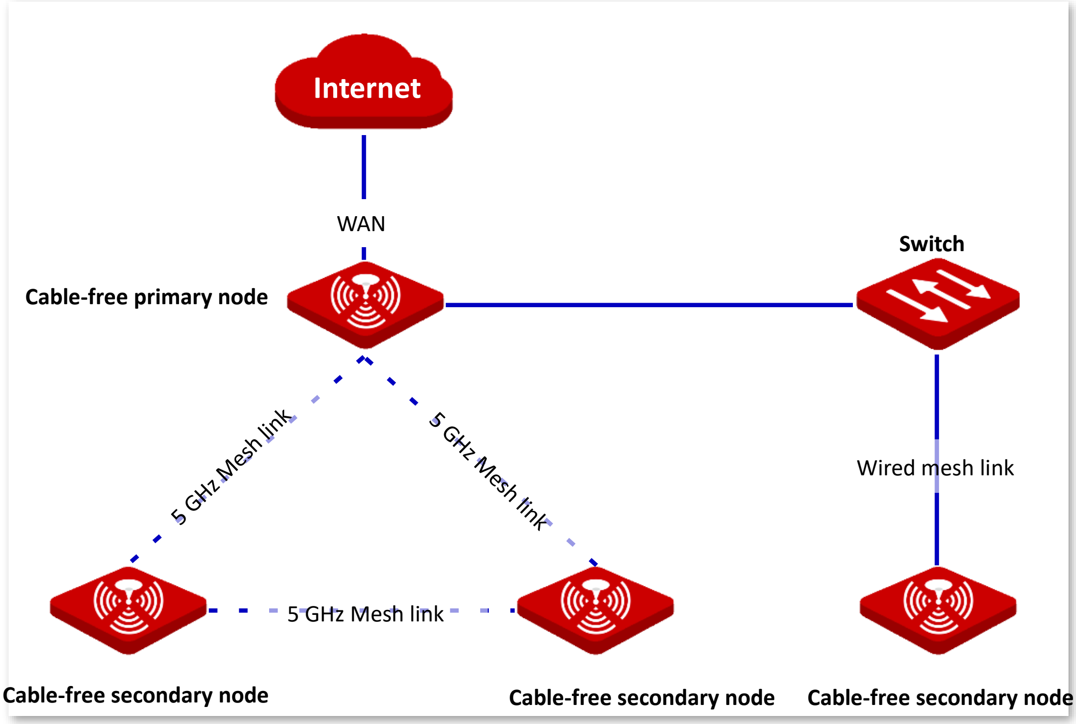
The wired network system is established by wired mode, and each cable-free device is connected by Ethernet cable. The three wireless bands of cable-free device are used for terminal devices' access.



Cable-free networking is simpler and faster. Network wiring of a wired network should meet some requirements. There are still some advantages as follows.

- The mesh links are more stable with higher speed and longer transmission distance.
- The cable-free device capacity is larger.

In actual networking, you can also adopt mixed networking mode according to your needs. The network connection diagram is shown below as an example.

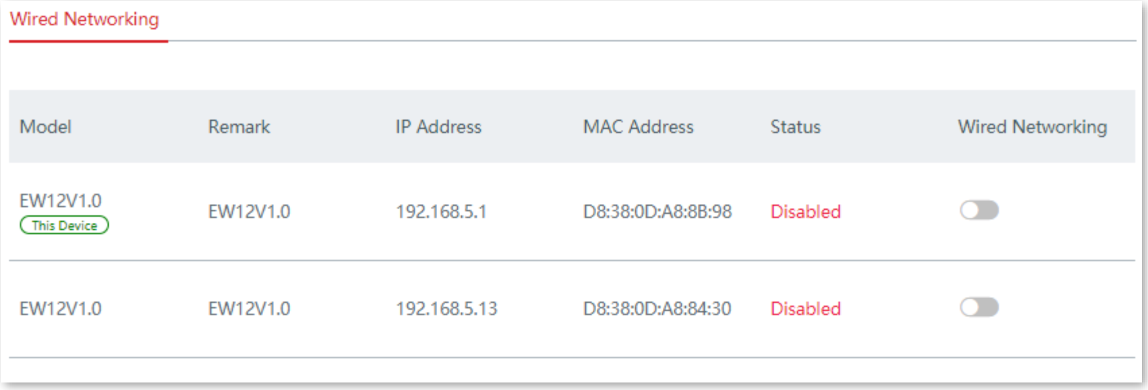


Configure wired networking

Tip

When the wired networking is enabled, the wireless networking function will be disabled automatically. Cable-free device that has connected to the network wirelessly will be disconnected.

1. Navigate to **Wired Networking** in **Smart Optimization** page. Select the node whose networking mode you want to change, and switch ○ to ●.



Wired Networking

Model	Remark	IP Address	MAC Address	Status	Wired Networking
EW12V1.0 This Device	EW12V1.0	192.168.5.1	D8:38:0D:A8:8B:98	Disabled	○
EW12V1.0	EW12V1.0	192.168.5.13	D8:38:0D:A8:84:30	Disabled	○

Parameter description

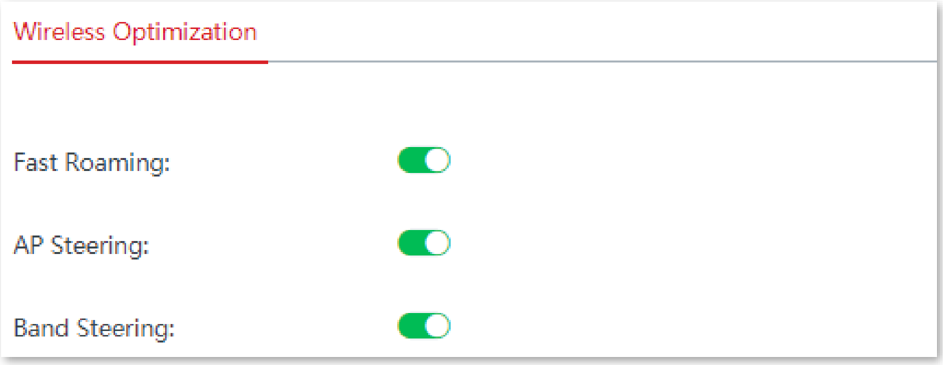
Parameter	Description
Model	It specifies the model and version of the node.
Remark	It specifies the remark for nodes. You can change it in the **Node Management** > **Maintenance** page.
IP Address	It specifies the IP address of the node.
MAC Address	It specifies the physical address of the node.
Status	It specifies the status of the wired networking function.
Wired Networking	It is used to enable/disable the wired networking function. After this function is enabled, the networking mode of nodes changes from cable-free networking to wired networking. And the three wireless bands of nodes are used for terminal access.

2. Connect nodes above with Ethernet cables.

----End

4.3.2 Wireless optimization

With this function, you can optimize the wireless experience in cable-free networking by adjusting the enabling states for fast roaming, AP steering, and band steering.



Fast Roaming: ●

AP Steering: ●

Band Steering: ●

Parameter description

Parameter	Description
Fast Roaming	With this function enabled, the device enables IEEE 802.11r fast roaming protocol, improving the user experience.
AP Steering	With this function enabled, the device leads a client to switch to another node for the higher connection quality when the current connection quality of the client is poor (week signal strength and high channel occupation ratio).

Parameter	Description
Band Steering	With this function enabled, the node leads a client to connect to the WiFi network at the frequency band with better quality (strong signal strength and low channel occupation ratio) when the current 5 GHz or 2.4 GHz connection quality of the client is poor (week signal strength and high channel occupation ratio).

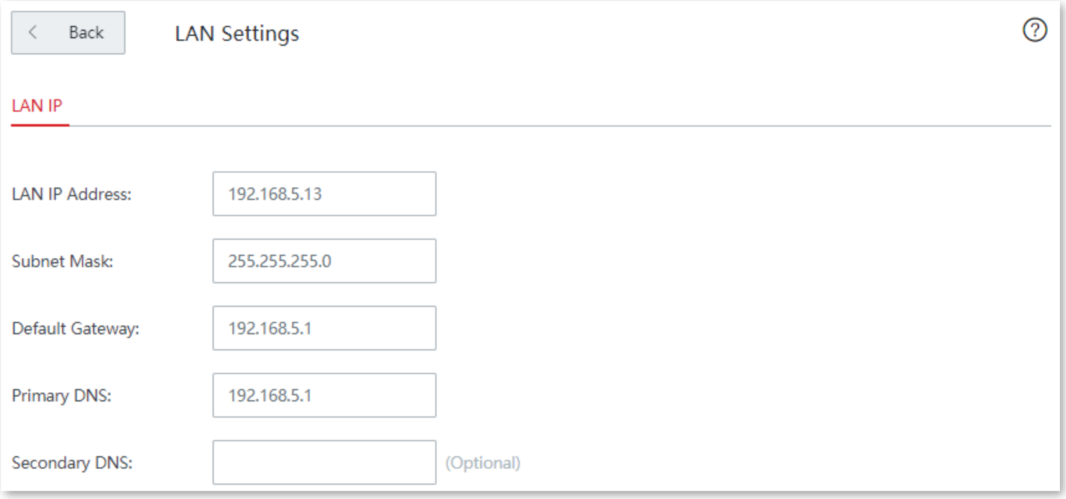
4.4 More

This chapter describes how to configure LAN settings and QVLAN.

4.4.1 LAN settings

LAN IP

In this section, you can configure LAN settings.



LAN IP Address: 192.168.5.13

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.5.1

Primary DNS: 192.168.5.1

Secondary DNS: (Optional)

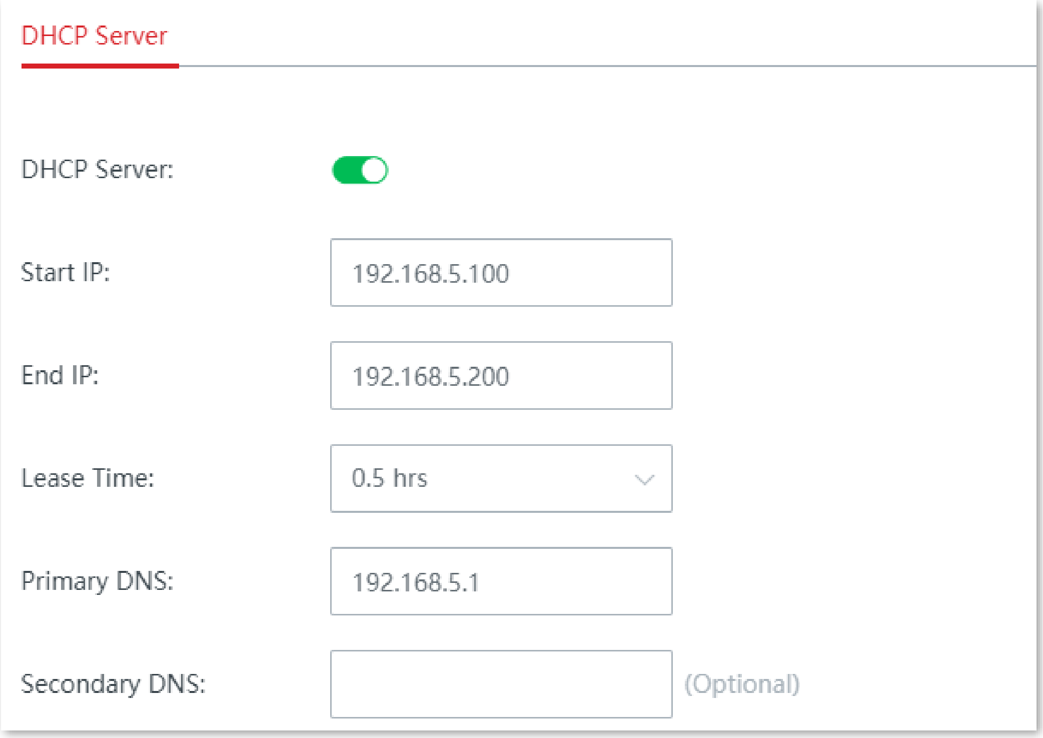
Parameter description

Parameter	Description
LAN IP Address	It specifies the IP address of the LAN port of the device. If you change this IP address, you can log in again only with the new IP address.
Subnet Mask	It specifies the LAN subnet mask of the device, which is 255.255.255.0 by default. It should be applied to all the PCs on the LAN.
Default Gateway	With this function enabled, the node automatically assigns IP addresses to clients to be connected.
Primary DNS	It specifies the primary DNS server address for the node. If the exit node has DNS proxy function, enter the LAN port IP address of the exit node here. Otherwise, enter the IP address of the correct DNS server.
Secondary DNS	It specifies the secondary DNS server address for the node. If you have two DNS server IP addresses, enter the other IP address here.

DHCP server

DHCP server can automatically assign IP address, subnet mask, gateway address, DNS and other internet access information to LAN user devices. The DHCP server is disabled by default in **Cable-Free (AP Mode)**.

When the DHCP server is enabled, the page appears as follows.



DHCP Server: ●

Start IP: 192.168.5.100

End IP: 192.168.5.200

Lease Time: 0.5 hrs

Primary DNS: 192.168.5.1

Secondary DNS: (Optional)

Parameter description

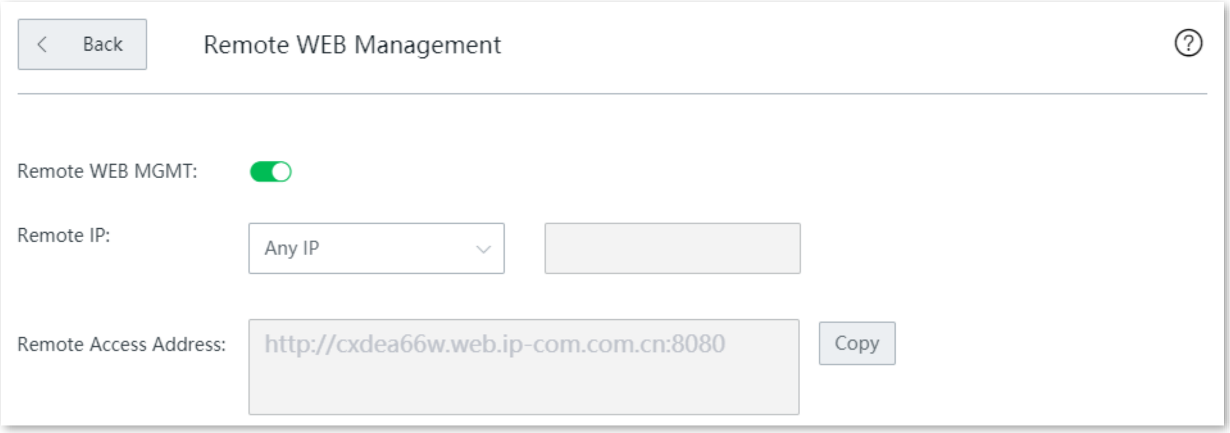
Parameter	Description
DHCP Server	It specifies the switch of the function. ● specifies to enable the function, ○ specifies to disable the function.
Start IP	It specifies the range of IP addresses that a DHCP server can assign. The start IP address is 192.168.5.100 and the end IP address is 192.168.5.200 by default. Tip With the LAN port IP address modified, if the new LAN port IP address and the original LAN port IP address are not in the same network segment, the system will automatically match and modify the DHCP address pool to make it in the same network segment with the new LAN port IP address.
End IP	
Lease Time	It specifies the effective time the DHCP server assigns IP addresses to LAN devices, which is 30 minutes by default. When the IP address expires: – If the device is still connected to the cable-free network, the device will automatically renew and continue to occupy the IP address. – If the device is not connected to the cable-free network, the node will release the IP address. If other devices later request IP address information, the node can assign the IP to other devices. If there is no special need, it is recommended to keep the default setting.

Parameter	Description
Primary DNS	It specifies the primary DNS server address for the node. If the exit node has DNS proxy function, enter the LAN port IP address of the exit node here. Otherwise, enter the IP address of the correct DNS server.
Secondary DNS	It specifies the secondary DNS server address for the node. If you have two DNS server IP addresses, enter the other IP address here.

4.4.2 Remote WEB management

In general, only the devices which connected to the node’s LAN port or WiFi network can log in to the node's management page. This function enables you to access the management page of the node remotely through the WAN port when you have special needs (such as remote technical support).

Navigate to **More** > **Remote WEB Management** to enter this page, this function is disabled by default.



Remote WEB MGMT: ●

Remote IP: Any IP

Remote Access Address: http://cxdea66w.web.ip-com.com.cn:8080

Parameter description

Parameter	Description
Remote WEB MGMT	It specifies the switch of the function. ● specifies to enable the function, ○ specifies to disable the function.
Remote IP	It specifies IP addresses of devices that can remotely access node management pages. – Any IP: It specifies that any device with any IP address on the internet can access the node's management page. For the sake of network security, this option is not recommended. – Specified IP: Only devices with a specified IP address can remotely access the node's management page. If the device is on LAN area, enter the IP address of the device's gateway (public network IP address).

Parameter	Description
Lease Time	It specifies the effective time the DHCP server assigns IP addresses to LAN devices, which is 30 minutes by default. When the IP address expires: – If the device is still connected to the cable-free network, the device will automatically renew and continue to occupy the IP address. – If the device is not connected to the cable-free network, the node will release the IP address. If other devices later request IP address information, the node can assign the IP to other devices. If there is no special need, it is recommended to keep the default setting.
Primary DNS	It specifies the primary DNS server address for the node. If the exit node has DNS proxy function, enter the LAN port IP address of the exit node here. Otherwise, enter the IP address of the correct DNS server.

4.4.3 QVLAN

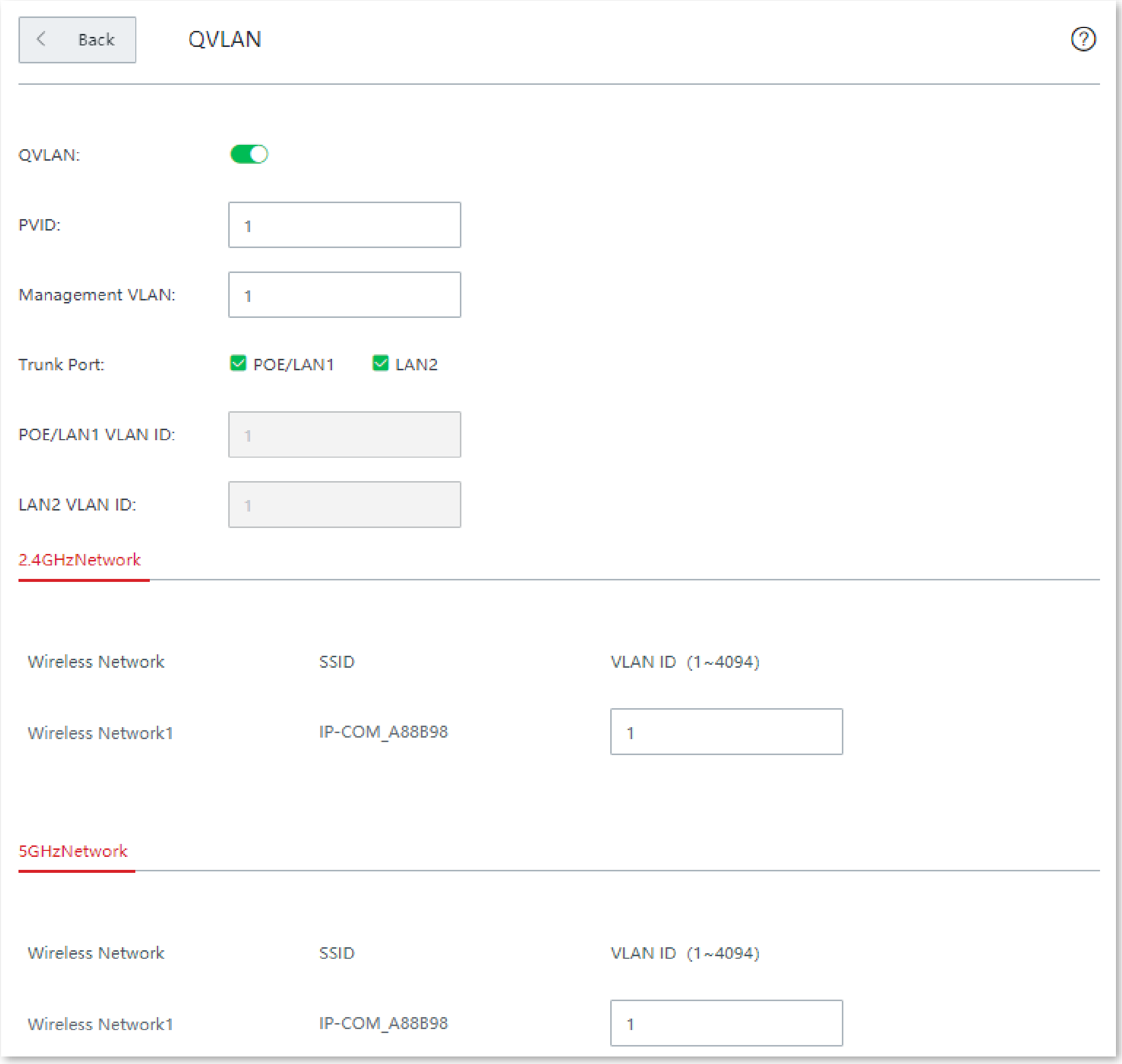
Cable-free (AP Mode) nodes support IEEE 802.1Q VLAN and can be used in network environments where QVLANs are partitioned. By default, the QVLAN is disabled.

With this function, the Tag data is forwarded to other ports in the corresponding VLAN according to the VID. And the Untag is forwarded to the other port of the corresponding VLAN according to the PVID. The process methods of port of each link type upon receiving and sending data are shown in the following table.

link type	Receiving data		Sending data
	Receiving Tag data	Receiving Untag data	
Access	Forward the Tag data to other port of the corresponding VLAN according to the VID in it.	Forward the Tag data to other port of the corresponding VLAN according to the PVID in it.	Send it after removing the Tag from the message.
Trunk			VID = port PVID, remove the Tag and send. VID ≠ port PVID, keep the Tag and send.

Configure QVLAN

Navigate to **More** > **QVLAN** to enter the page.



Back QVLAN

QVLAN: ●

PVID: 1

Management VLAN: 1

Trunk Port: ☑ POE/LAN1 ☑ LAN2

POE/LAN1 VLAN ID: 1

LAN2 VLAN ID: 1

2.4GHzNetwork

Wireless Network	SSID	VLAN ID（1~4094）
Wireless Network1	IP-COM_A88B98	1

5GHzNetwork

Wireless Network	SSID	VLAN ID（1~4094）
Wireless Network1	IP-COM_A88B98	1

Parameter description

Parameter	Description
QVLAN	It is used to enable or disable the VLAN function.
PVID	It specifies the VLAN ID of a trunk port by default, which is 1 here.
Management VLAN	It specifies the management VLAN ID of the node. The default value is 1 in here. After the management VLAN is modified, your computer is required to be connected to the new management VLAN to manage the node.

Parameter	Description
Trunk Port	It is used to select the Ethernet port (wired LAN port) that will be the trunk port of the node, which is POE/LAN1 and LAN2 by default. The trunk port allows all VLANs to pass through it. Note When you want to enable the QVLAN, select at least one LAN port as the trunk port. If the node has only one Ethernet port, the Ethernet port serves as the trunk port by default.
PoE/LAN1 VLAN ID	If the Ethernet port is not set as a trunk port, it serves as an access port and its VLAN ID can be set here.
LAN2 VLAN ID	
SSID	It specifies the WiFi network name. This page only displays the SSIDs of the enabled WiFi networks.
VLAN ID	It is used to divide the physical ports and WiFi networks into specified VLANs. By default, the VLAN of physical ports is 1.

Example of configuring QVLAN

Networking requirement

A hotel uses cable-free device for wireless coverage. The cable-free device has been set to work in the Cable-Free (AP Mode) and has been connected to the internet. The current requirements are as follows:

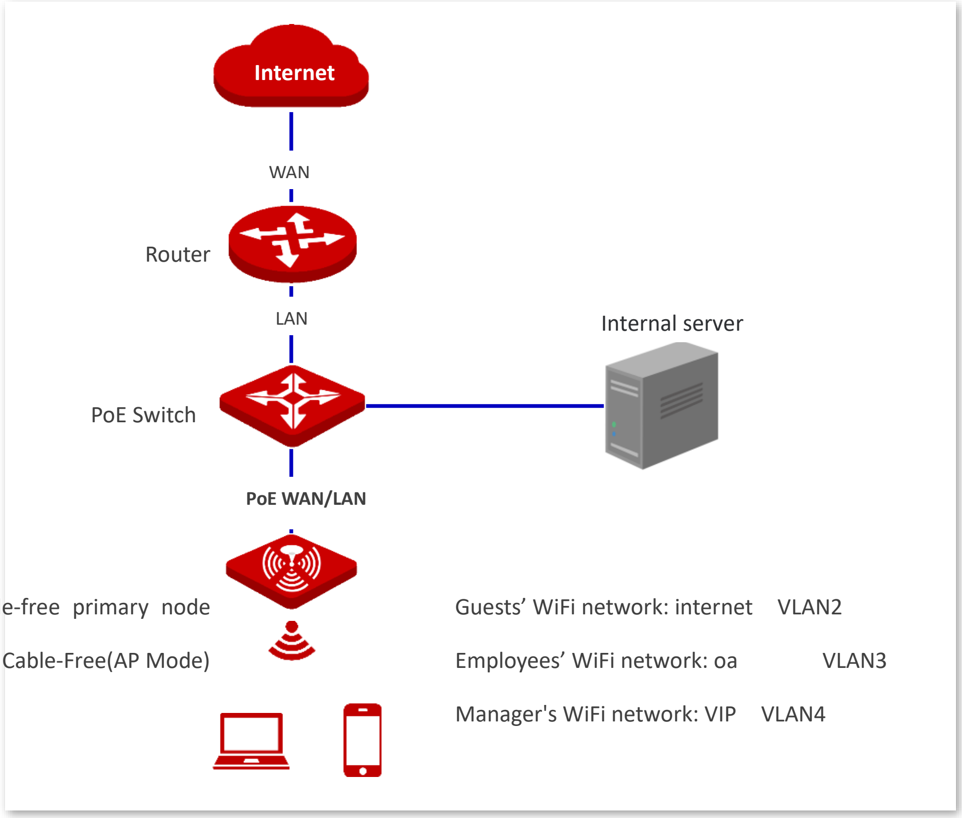
- Hotel guests can only access the internet when they are connected to the WiFi network.
- Hotel staff can only access the hotel intranet when they are connected to the WiFi network.
- Hotel managers can access both the internet and the hotel intranet when they access the WiFi network.

Solution

Assign different WiFi networks for guests, employees and managers, and divide VLAN, so that all users can get their own corresponding accessing authority

Assumption:

- Deploy WiFi networks in the 2.4 GHz band.
- The WiFi network for guests is **Internet** and belongs to VLAN 2.
- The WiFi network for employees is **oa** and belongs to VLAN 3.
- The WiFi network for manager is **VIP** and belongs to VLAN 4.


Internet
WAN
Router
LAN
Internal server
PoE Switch
PoE WAN/LAN
Cable-free primary node
Cable-Free(AP Mode)
Guests' WiFi network: internet VLAN2
Employees' WiFi network: oa VLAN3
Manager's WiFi network: VIP VLAN4

Configuration procedure

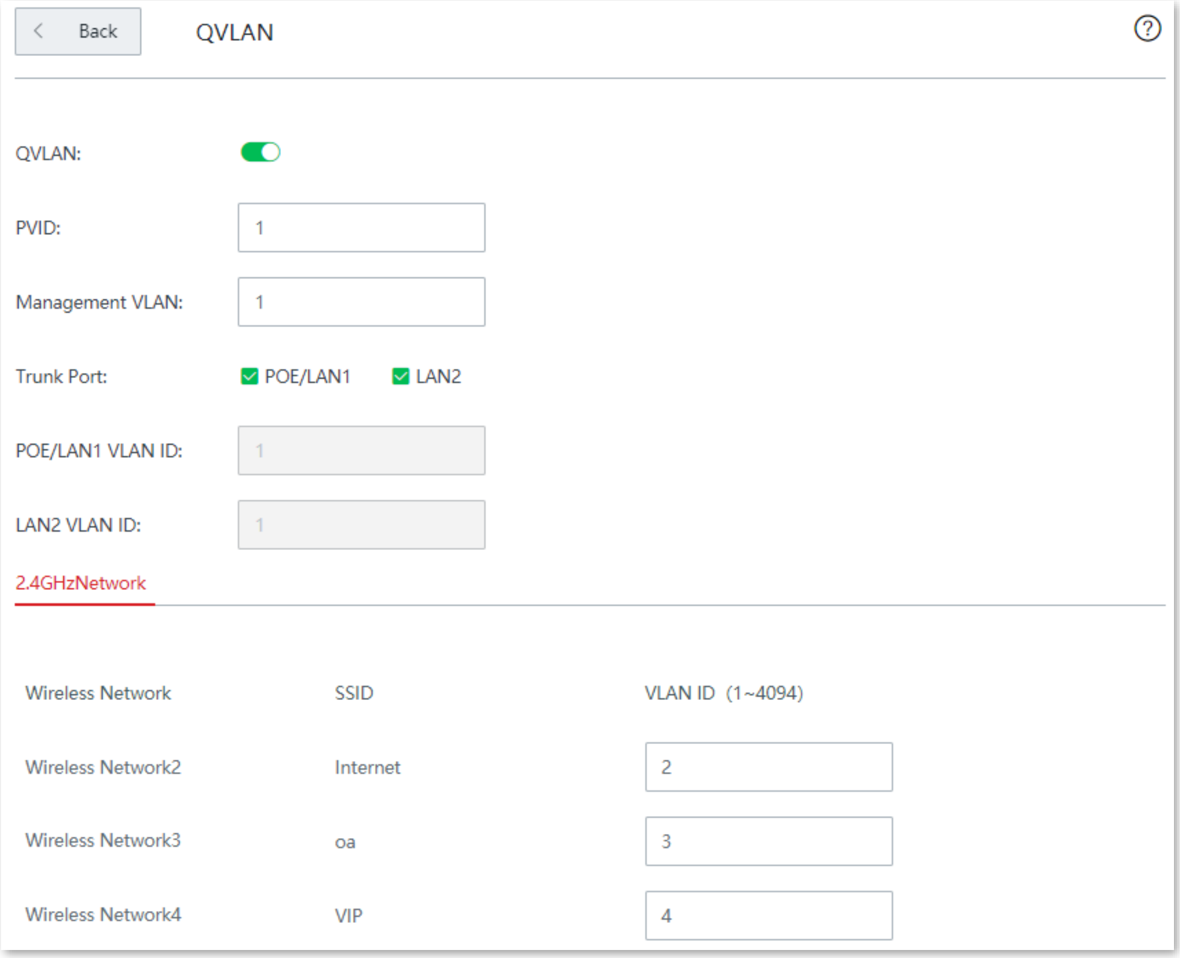
1. Configure cable-free devices.

   (1) Log into the web UI of cable-free devices, navigate to **More** > **QVLAN** to enter this page.

   (2) Switch ○ to ●.

   (3) Modify the VLAN ID of each WiFi network in 2.4 GHz band. The VLAN ID of Internet is 2, the VLAN ID of oa is 3, and the VLAN ID of VIP is 4.

   (4) Click **Save**.



QVLAN: ●

PVID: 1

Management VLAN: 1

Trunk Port: ☑ POE/LAN1 ☑ LAN2

POE/LAN1 VLAN ID: 1

LAN2 VLAN ID: 1

Wireless Network	SSID	VLAN ID (1~4094)
Wireless Network2	Internet	2
Wireless Network3	oa	3
Wireless Network4	VIP	4

2. Configure the switch.

Divide IEEE 802.1q VLANs through the switch.

Port connected to	VLAN ID	Port Properties	PVID
Cable-free primary node	1,2,3,4	Trunk	1
Internal server	3,4	Trunk	1
Router	2,4	Trunk	1

Any other ports not mentioned can be left at the default settings. Please refer to the operation instruction of the switch for the specific configuration method.

3. Configure the router and internal server.

To ensure that wireless clients connected to cable-free devices can access the internet properly, routers and internal servers need to support QVLAN and be configured in this module.

Router:

Port connected to	VLAN ID	Port Properties	PVID
Switch	2,4	Trunk	1

Internal server:

Port connected to	VLAN ID	Port Properties	PVID
Switch	3,4	Trunk	1

Please refer to the operation instructions of the corresponding equipment for specific configuration methods.

----End

Verication

Users connected to the **Internet** can only access the internet. Users connected to **oa** can only access the Intranet. Users connected to the **VIP** can access both the internet and the intranet.

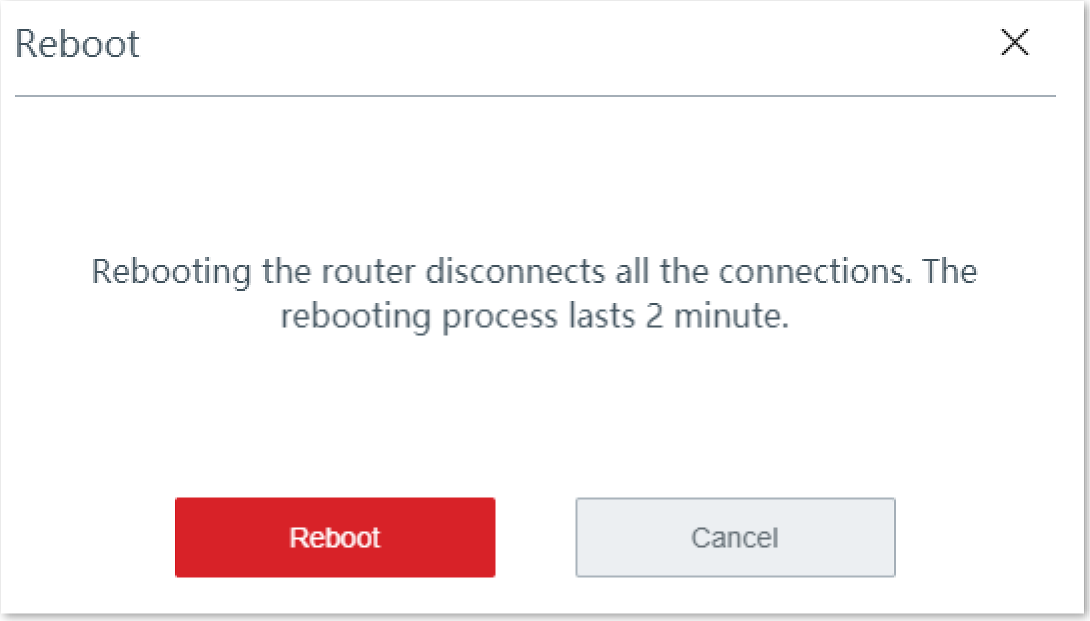
4.5 Maintenance

This chapter describes how to reboot, reset, and upgrade the device, how to modify the login password, how to back up your current configuration and restore the device to previous configuration, how to view the system logs and functions that are enabled or disabled, how to set up system time, and how to use the Ping and Traceroute commands.

4.5.1 Reboot

If a parameter does not take effect or the device does not work properly, you can try rebooting the device to resolve the problem.

Navigate to **Maintenance** > **Reboot**. The prompt window appears. Confirm the message and click **Reboot**.



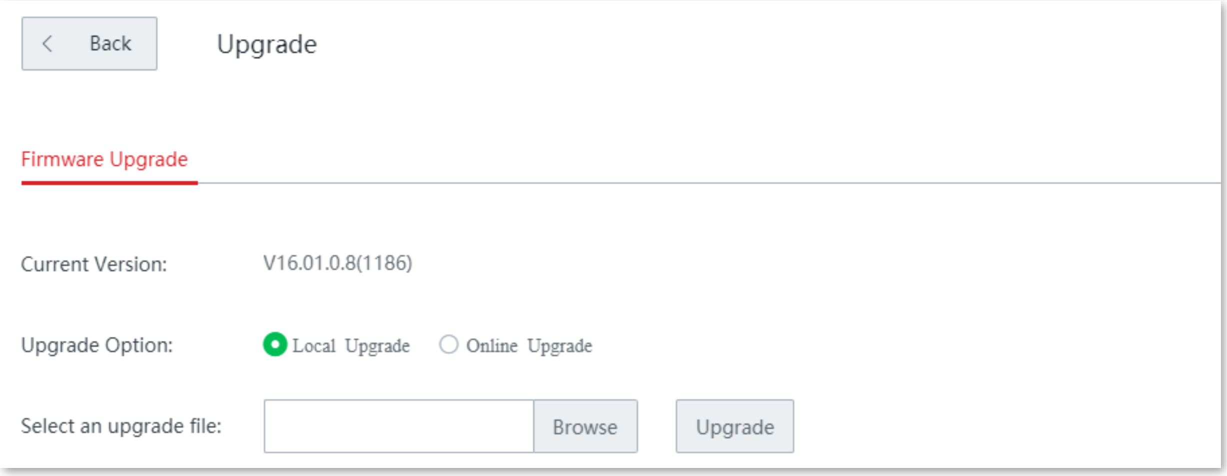
Rebooting the router disconnects all the connections. The rebooting process lasts 2 minute.

4.5.2 Upgrade

Overview

The device supports **local** and **online** upgrades.

Navigate to **Maintenance** > **Upgrade** to enter the configuration page. See the following figure.



Current Version: V16.01.0.8(1186)

Upgrade Option: ● Local Upgrade ○ Online Upgrade

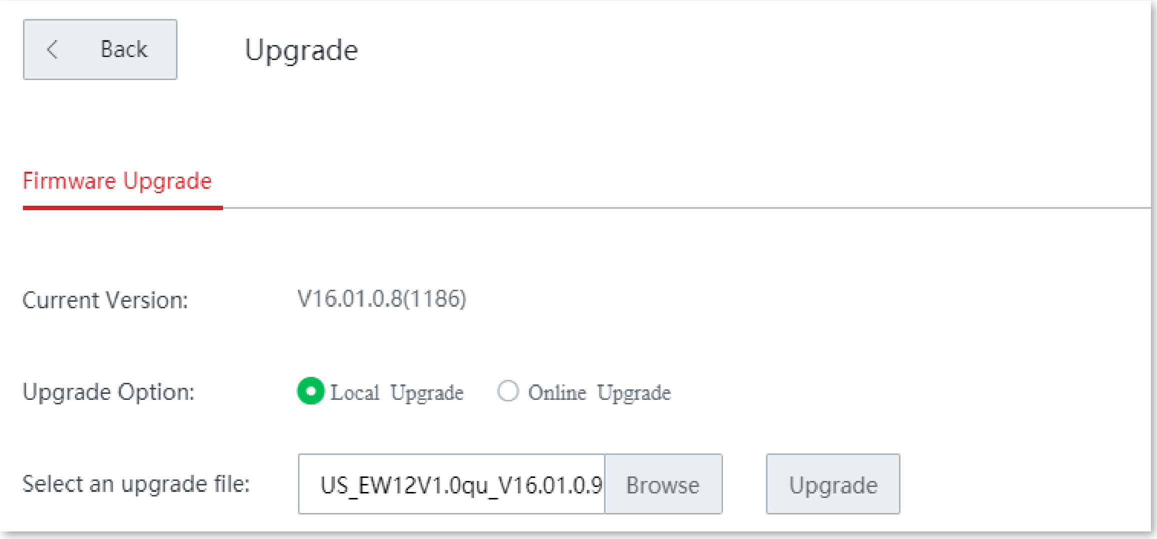
Select an upgrade file:

Upgrade the rotuer locally

Tip

- To enable your device to work properly after an upgrade, ensure that the firmware used to upgrade complies with your product model.
- When upgrading, do not power off the device.

1. Download the upgrade file to your local computer.
   (1) Visit www.ip-com.com.cn, and search the product model in the searching bar to enter the product details page.
   (2) Locate the latest firmware, download it to your computer, and unzip it.
2. Log in to the web UI of your device, navigate to **Maintenance** > **Upgrade** to enter the configuration page.
3. Set **Upgrade Option** to **Local Upgrade**.
4. Click **Browse**, select and upload the firmware that has been downloaded to your computer. Ensure that the suffix of the firmware is **.bin**.
5. Click **Upgrade**. Wait until the progress bar completes.
6. Reset the device to apply your settings.



Current Version: V16.01.0.8(1186)

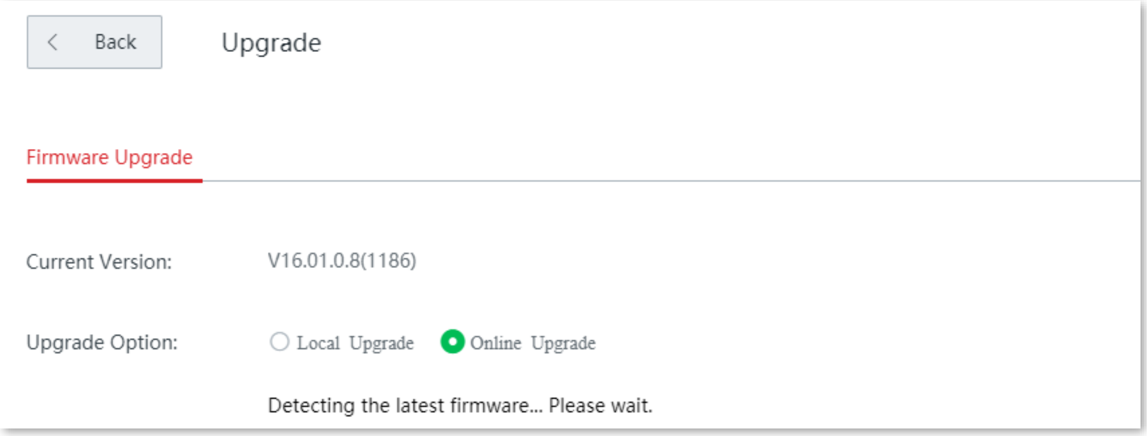
Upgrade Option: ● Local Upgrade ○ Online Upgrade

Select an upgrade file: US_EW12V1.0qu_V16.01.0.9

----End

Upgrade the rotuer online

When the device is connected to the internet, it checks whether there is a later firmware version, and displays the detected information on the page. You can choose whether to upgrade. If you want to upgrade the firmware, click **Upgrade**.



Current Version: V16.01.0.8(1186)

Upgrade Option: ○ Local Upgrade ● Online Upgrade

Detecting the latest firmware... Please wait.

4.5.3 Reset

Overview

If the internet is inaccessible for unknown reasons, or you forget the login password, you can reset the cable-free device to resolve the problems.

The device supports two resetting methods:

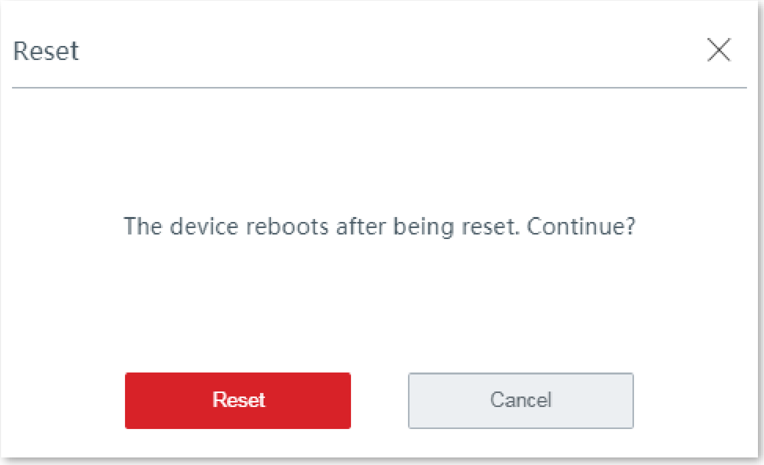
- Reset the device by using web UI
- Reset the device by using the Reset button

Reset the device by using web UI

Tip

- Resetting the device deletes all your current configurations and you need to reconfigure the device to access the internet.
- If it is necessary to reset the device, backing up your current configuration first.
- When resetting, do not power off the device.

Navigate to **Maintenance > Reset**, and follow the on-screen instruction to reset the device.


Reset

The device reboots after being reset. Continue?

Reset the device by using the Reset button

If you forget your login password, but need to log in to the web UI of the device, you can use the hardware **RESET** button on the device to reset it, and configure it again.

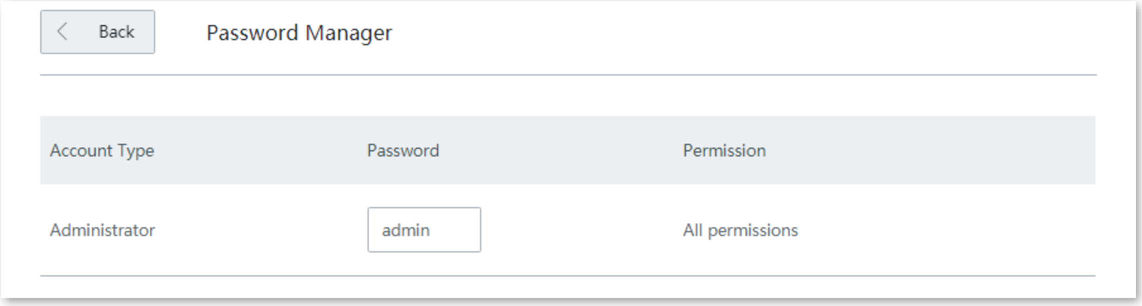
With the LED indicator blinking, hold down the Reset button using a paper clip (or something with a pointed end) for about 8 seconds, then release it when the LED indicator lights solid on. The device is reset to the factory settings successfully when the LED indicator blinks again.

4.5.4 Password manager

Overview

On this page, you can change the Administrator account information of the device to prevent unauthorized login. Password for the account is the login password you set during initial setup. You can view and modify it here.

Navigate to **Maintenance** > **Password Manager** to enter the configuration page.



Account Type	Password	Permission
Administrator	admin	All permissions

Modify login password

1. Navigate to **Maintenance** > **Password Manager** to enter the configuration page.
2. Modify the password.
3. Click **Save** on the bottom of the page to apply your settings.

----End

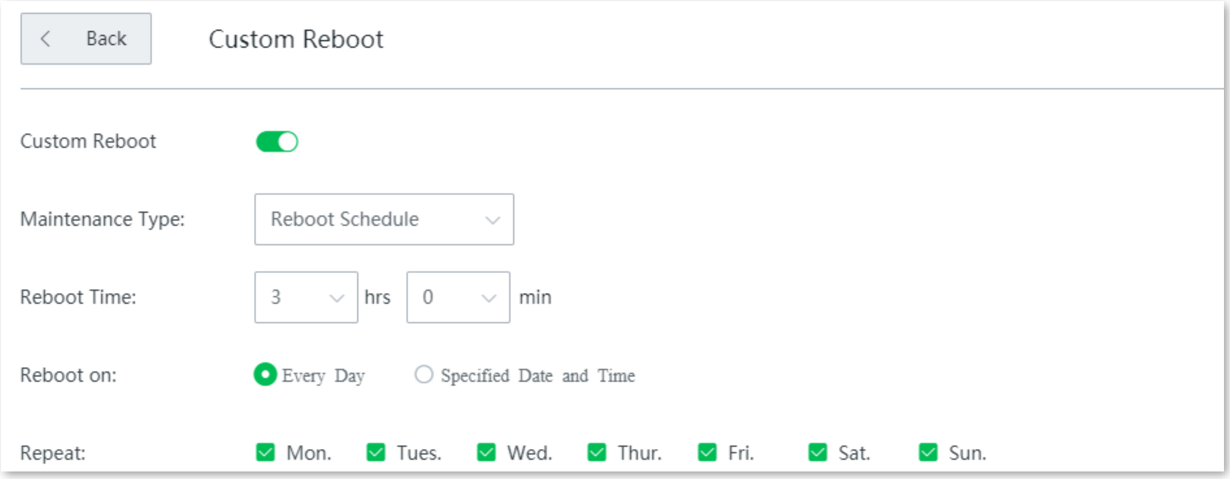
Then you will be redirected to the login page. Enter the password corresponding to the administrator account you set just now, and click **Login** to log in to the device.

4.5.5 Custom reboot

Overview

This device will reboot on schedule automatically to maintain its performance.

Navigate to **Maintenance** > **Custom Reboot** to enter the page.



Custom Reboot

Custom Reboot: On

Maintenance Type: Reboot Schedule

Reboot Time: 3 hrs 0 min

Reboot on: ● Every Day ○ Specified Date and Time

Repeat: ☑ Mon. ☑ Tues. ☑ Wed. ☑ Thur. ☑ Fri. ☑ Sat. ☑ Sun.

Parameter description

Parameters	Description
Custom Reboot	It specifies whether to enable the Custom Schedule function.
Maintenance Type	It specifies the method of rebooting the device.
Reboot Time	It specifies the time at which the device reboots.
Reboot on	It specifies the repeat rule.
Repeat	It specifies the dates on which the device reboots.

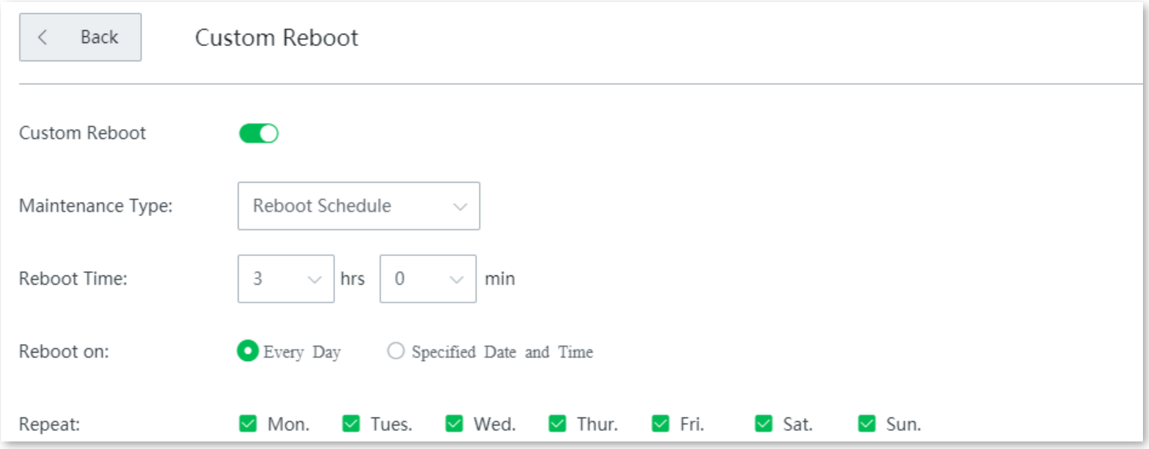
Reboot the AP on schedule

Tip

To enable reboot schedule function to work properly, ensure that the System time of your device is correct.

1. Navigate to **Maintenance** > **Custom Reboot** to enter the configuration page, and enable this function.
2. Set the time and date when the device performs rebooting.

3. Click **Save** to apply your settings.



Custom Reboot

Maintenance Type: Reboot Schedule

Reboot Time: 3 hrs 0 min

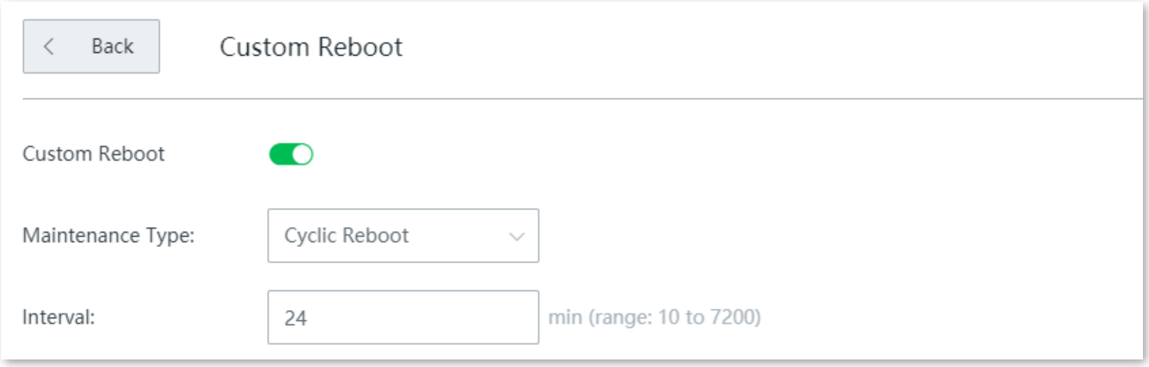
Reboot on: ● Every Day ○ Specified Date and Time

Repeat: ☑ Mon. ☑ Tues. ☑ Wed. ☑ Thur. ☑ Fri. ☑ Sat. ☑ Sun.

----End

Reboot the device on cyclic

1. Navigate to **Maintenance** > **Custom Reboot** to enter the configuration page.
2. Set the cyclic when the device performs rebooting.
3. Click **Save** to apply your settings.



Custom Reboot

Maintenance Type: Cyclic Reboot

Interval: 24 min (range: 10 to 7200)

----End

The device performs rebooting regularly on the time and date you set here.

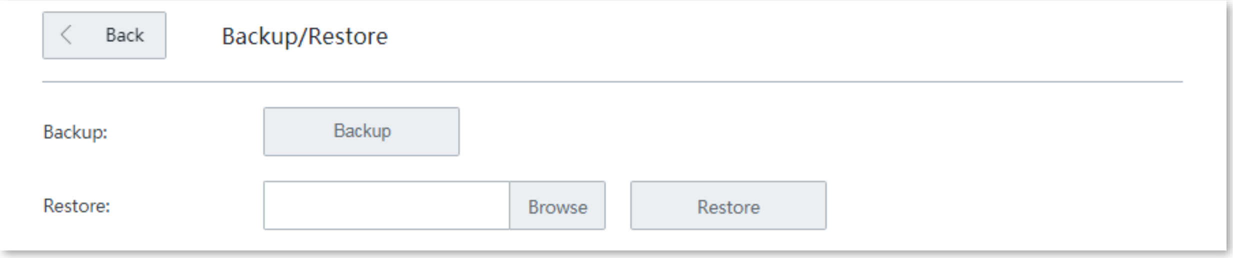
4.5.6 Backup/Restore

Overview

The **Backup** function is used to export the current configuration of the device to your computer. The **Restore** function is used to import a configuration file to the device.

You are recommended to back up the configuration after it is significantly changed. When the performance of your device decreases because of an improper configuration, or after you restore the device to factory settings, you can use this function to restore the configuration that has been backed up.

Navigate to **Maintenance** > **Backup/Restore** to enter the configuration page.

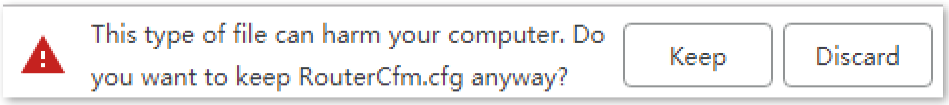


Back up your current configuration

1. Navigate to **Maintenance** > **Backup/Restore** to enter the configuration page.
2. Click **Backup**. The system exports a **RouterCfm.cfg** file to your local computer.

Tip

If the following warning message appears, click **Keep**.


This type of file can harm your computer. Do you want to keep RouterCfm.cfg anyway?

----End

Restore your previous configuraiton

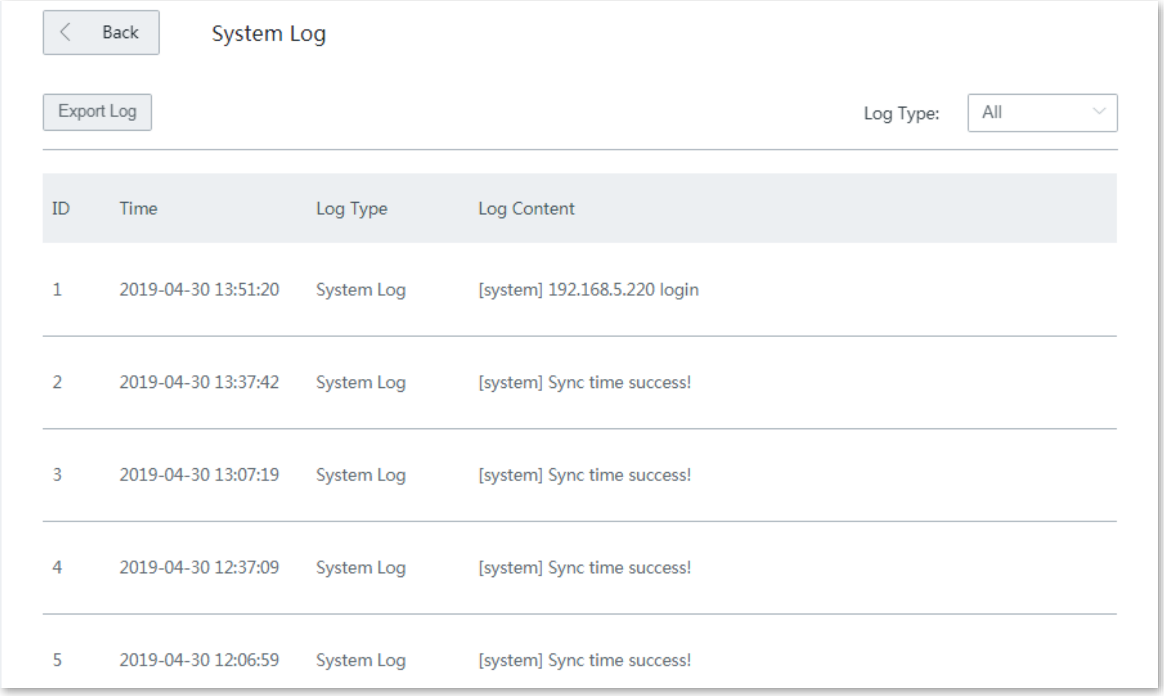
1. Navigate to **Maintenance** > **Backup/Restore** to enter the configuration page.
2. Click **Browse**, and upload the configuration file ending with **.cfg**.
3. Click **Restore** and follow the on-screen instruction to restore the configuration.

----End

4.5.7 System log

System logs record information about system running status and the operation you performed on it. When system malfunctions occur, you can use system log for troubleshooting.

Navigate to **Maintenance** > **System Log** to enter the page.



Log Type: All

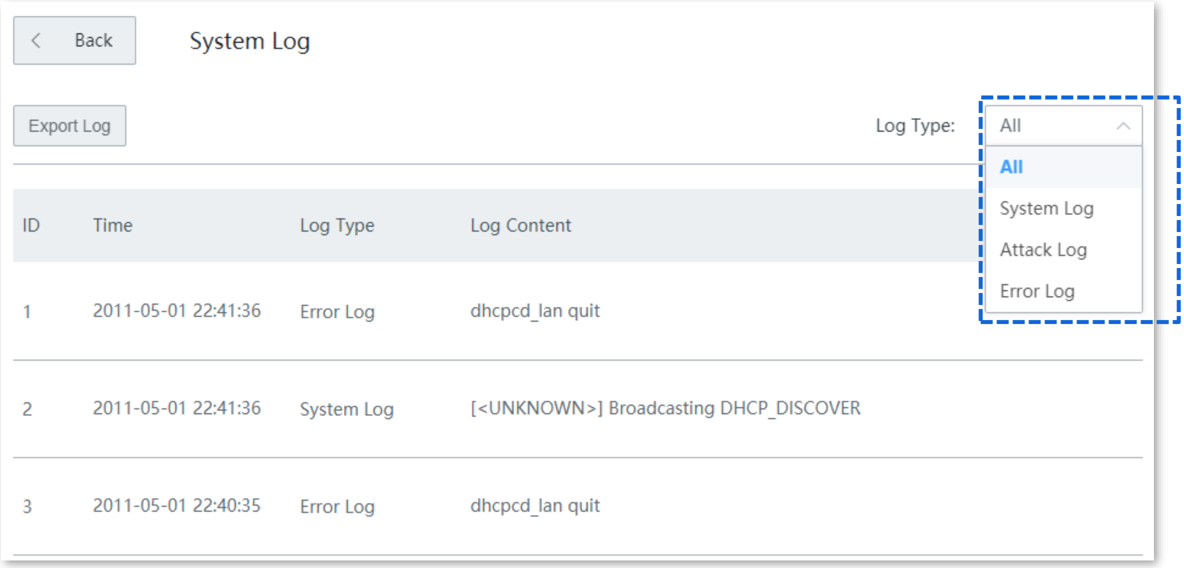
ID	Time	Log Type	Log Content
1	2019-04-30 13:51:20	System Log	[system] 192.168.5.220 login
2	2019-04-30 13:37:42	System Log	[system] Sync time success!
3	2019-04-30 13:07:19	System Log	[system] Sync time success!
4	2019-04-30 12:37:09	System Log	[system] Sync time success!
5	2019-04-30 12:06:59	System Log	[system] Sync time success!

View system log

Tip

- System logs will be cleared each time the device reboots or resets.
- A maximum of 300 logs will be recorded.
- The system only keeps 300 logs that are generated the most recently.

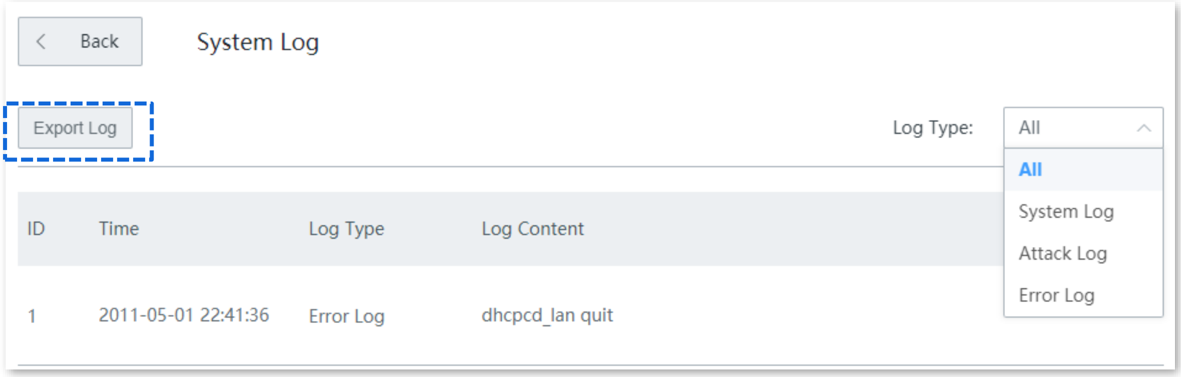
The device records three log types: **System Log**, **Attack Log**, and **Error Log**. You can view all logs or filter the logs to view as needed.



ID	Time	Log Type	Log Content
1	2011-05-01 22:41:36	Error Log	dhcpcd_lan quit
2	2011-05-01 22:41:36	System Log	[<UNKNOWN>] Broadcasting DHCP_DISCOVER
3	2011-05-01 22:40:35	Error Log	dhcpcd_lan quit

Export system log

Click Export Log, the log file will be downloaded to your local computer.



ID	Time	Log Type	Log Content
1	2011-05-01 22:41:36	Error Log	dhcpcd_lan quit

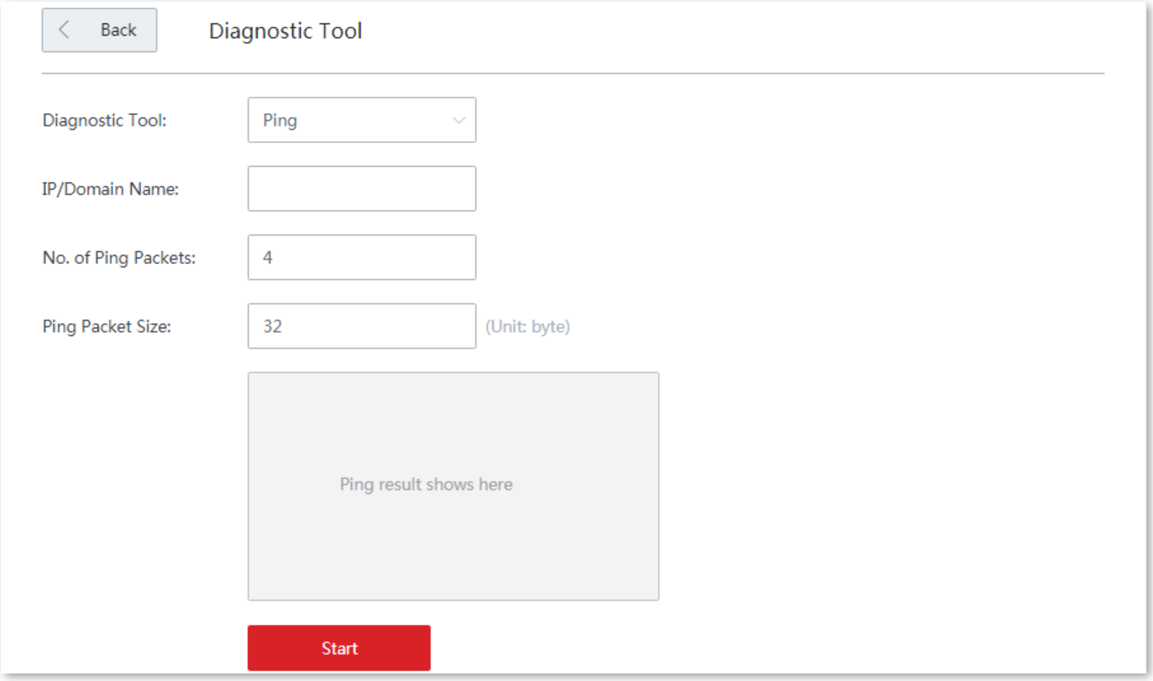
4.5.8 Diagnostic tool

Overview

You can execute Ping/Traceroute command on this page.

- **Ping**: It is used to check whether the connection is correct and the connection quality.
- **Traceroute**: It is used to detect the route from the bridge to the destination IP address or domain name.

Navigate to **Maintenance** > **Diagnosis Tool** to enter the page.



Diagnostic Tool: Ping

IP/Domain Name:

No. of Ping Packets: 4

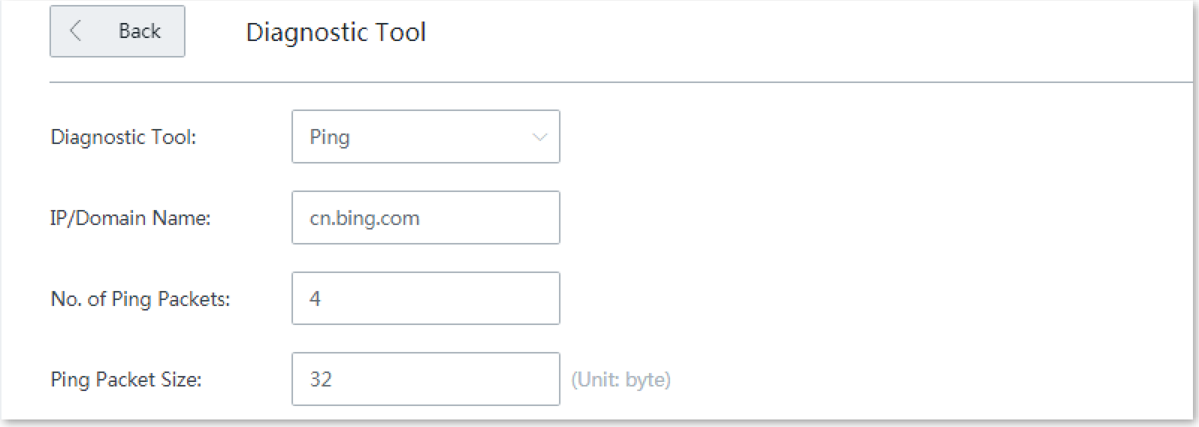
Ping Packet Size: 32 (Unit: byte)

Ping result shows here

Execut Ping command to detect connection quality

Assume that you need to detect the connectivity between the device and the **Bing** website.

1. Navigate to **Maintenance** > **Diagnosis Tool** to enter the configuration page.
2. Select **Ping** from the drop-down list menu of the Tools.
3. Enter the IP address or domain name of the ping target, which is **cn.bing.com** in this example.
4. Set **Number of Ping Packets** as required.
5. Set **Ping Packet Size** as required.
6. Click **Start**.



Diagnostic Tool: Ping

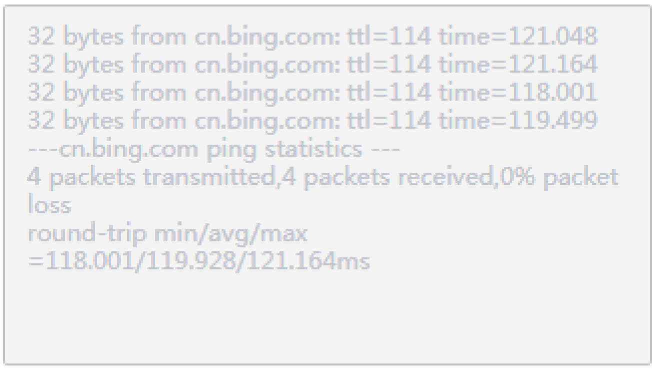
IP/Domain Name: cn.bing.com

No. of Ping Packets: 4

Ping Packet Size: 32 (Unit: byte)

----End

Wait a moment. The ping result will be displayed in the result box. See the following figure.

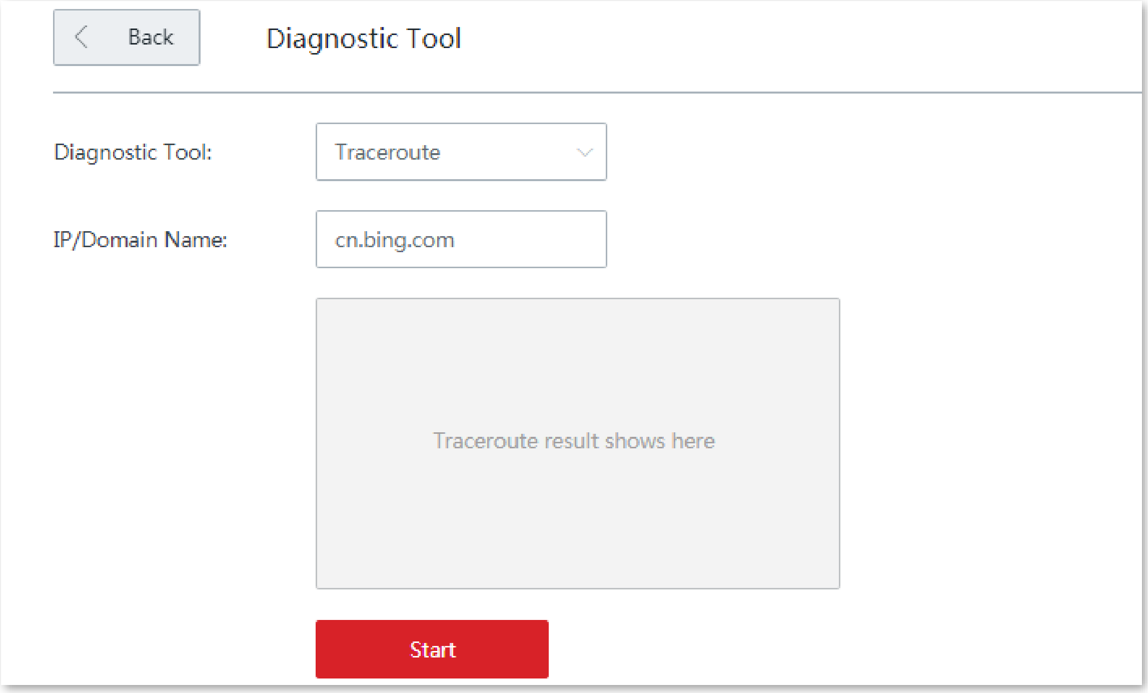


```
32 bytes from cn.bing.com: ttl=114 time=121.048
32 bytes from cn.bing.com: ttl=114 time=121.164
32 bytes from cn.bing.com: ttl=114 time=118.001
32 bytes from cn.bing.com: ttl=114 time=119.499
---cn.bing.com ping statistics ---
4 packets transmitted,4 packets received,0% packet
loss
round-trip min/avg/max
=118.001/119.928/121.164ms
```

Execut Traceroute command to detect the route selection

Assume that you need to detect the path from the device to **Bing** website.

1. Navigate to **Maintenance** > **Diagnosis Tool** to enter the configuration page.
2. Select **Traceroute** from the drop-down list menu of the Tools menu.
3. Enter the IP address or domain name of the traceroute target, which is **cn.bing.com** in this example.
4. Click **Start**.



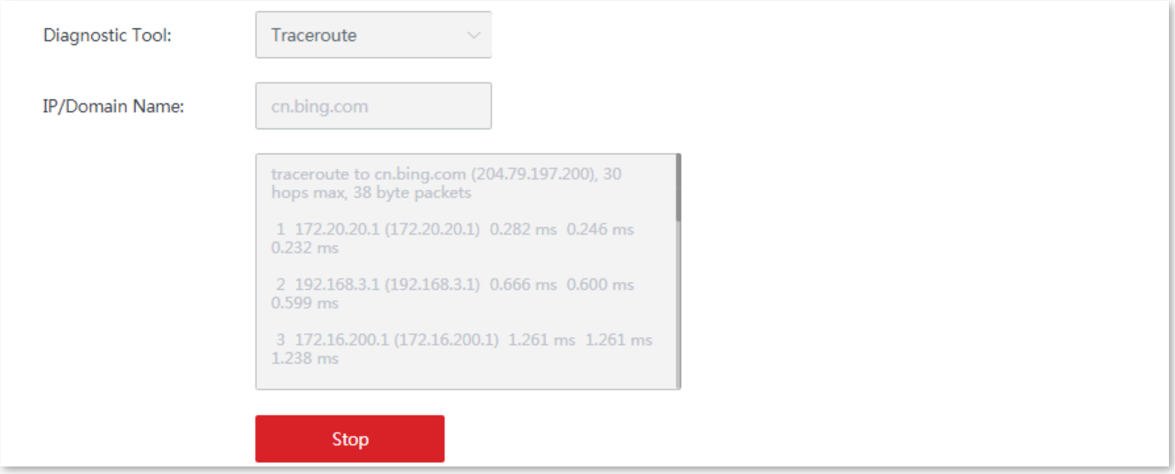
Diagnostic Tool

Diagnostic Tool: Traceroute

IP/Domain Name: cn.bing.com

----End

Wait a moment. The traceroute result will be displayed in the result box. See the following figure.



Diagnostic Tool: Traceroute

IP/Domain Name: cn.bing.com

```
traceroute to cn.bing.com (204.79.197.200), 30
hops max, 38 byte packets

 1  172.20.20.1 (172.20.20.1)  0.282 ms  0.246 ms
0.232 ms

 2  192.168.3.1 (192.168.3.1)  0.666 ms  0.600 ms
0.599 ms

 3  172.16.200.1 (172.16.200.1)  1.261 ms  1.261 ms
1.238 ms
```

Click **Stop** to end the process as required.

4.5.9 System time

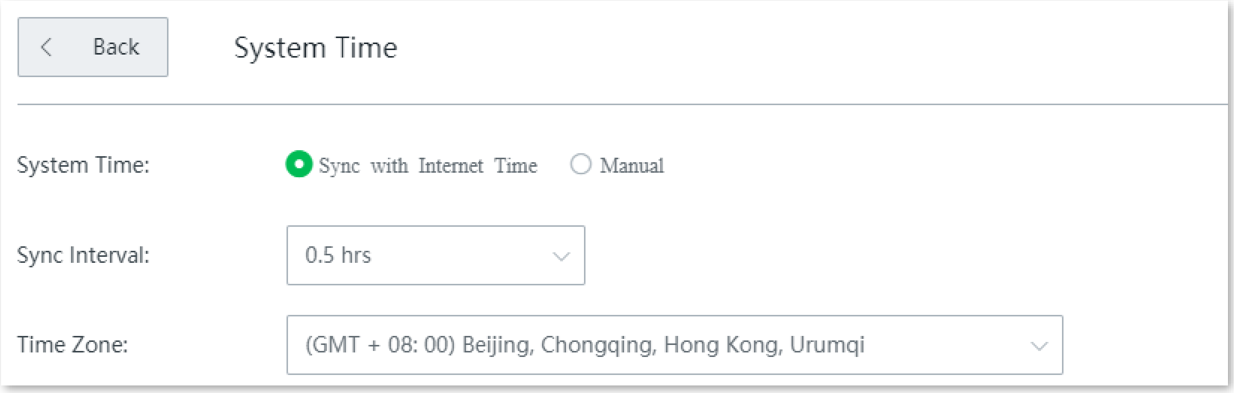
Overview

This function is used to set the system time of your device. To make the time-related functions effective, ensure that the system time of the device is set correctly.

The device supports:

- Synchroniz with internet time (default)
- Set system time manually

Navigate to **Maintenance** > **System Time** to enter the page. See the following figure.



System Time: ● Sync with Internet Time ○ Manual

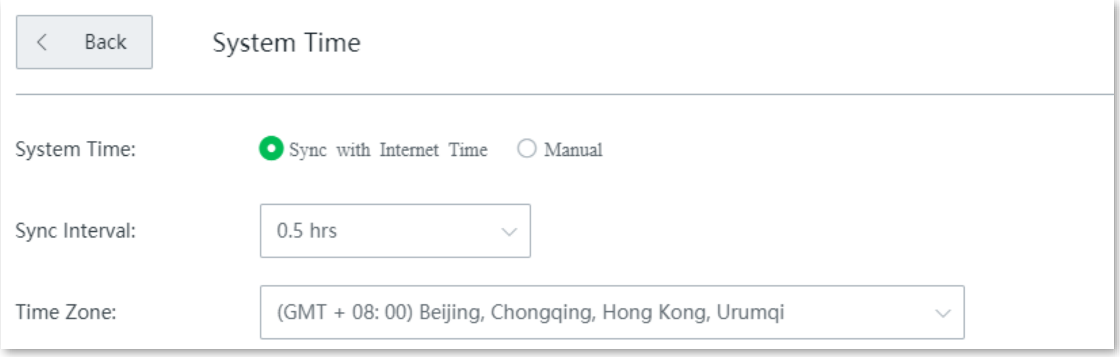
Sync Interval: 0.5 hrs

Time Zone: (GMT + 08: 00) Beijing, Chongqing, Hong Kong, Urumqi

Synchroniz with internet time

In this method, the device automatically synchronizes its system time with the network time server (NTS). As long as the device is connecting to the internet, the system time is correct.

After configuration, navigate to the System status to check whether it is synchronized.



System Time

System Time: ● Sync with Internet Time ○ Manual

Sync Interval: 0.5 hrs

Time Zone: (GMT + 08: 00) Beijing, Chongqing, Hong Kong, Urumqi

Parameter description

Parameters	Description
Sync Interval	It specifies an interval at which the device synchronizes its system time with the time server on the internet. By default, the device performs synchronization every 0.5 hours.
Time Zone	It specifies the time zone where the device is deployed.

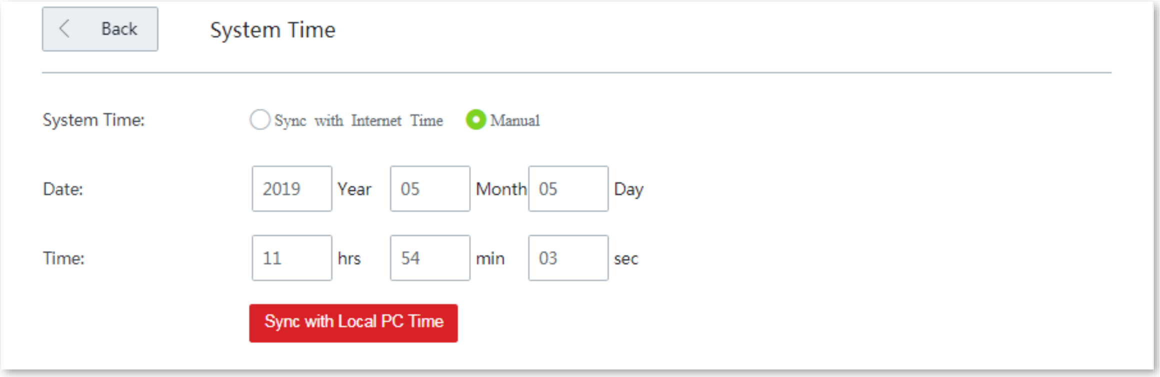
Set system time manually

In this method, you can manually specify a system time for the device. When **Manual option** is selected**,** the related parameters are shown as follows.

Tip

In this method, you need to manually reconfigure the system time each time the device reboots.

After configuration, navigate to the System status page to check whether it is synchronized.



System Time

System Time: ○ Sync with Internet Time ● Manual

Date: 2019 Year 05 Month 05 Day

Time: 11 hrs 54 min 03 sec

Parameter description

Parameters	Description
Date	Manually enter the date and time as needed.
Time	
Sync with Local PC Time	It allows you to synchronize the system time of the device with the system time of the management computer. Click this button, the device auto-fills the system time of your management computer.

Appendix

A.1 Default parameters

Parameters			Default
Login	Login IP address		192.168.5.1
	Administrator password		admin
Working mode			Cable-free (Router Mode)
LAN settings	IP address		192.168.5.1
	Subnet mask		255.255.255.0
DHCP server	DHCP server		Enable
	Start IP address		192.168.5.31
	End IP address		192.168.5.254
	Lease time		0.5 hrs
	Primary DNS		192.168.5.1
Wireless	SSID	2.4/5 GHz	Support 3 SSIDs at each band. The default SSID is IP-COM_*XXXXXX*, *XXXXXX* indicates the last 6 characters of the LAN MAC address with a range of XXXXXX to XXXXXX + 2.
	WiFi password		No password
	RSSI threshold		-100 dBm
	Prioritize 5 GHz		Enable
	Prioritize 5 GHz threshold		-80 dBm
	Guest network		Disable
Any IP			Disable

Parameters	**Default**
Capacity-oriented mode	Enable
Fast roaming	Disable
System time	Sync with internet time

A.2 Acronyms and abbreviations

Acronym or Abbreviation	Full Spelling
AES	Advanced Encryption Standard
APSD	Automatic Power Save Delivery
ARP	Address Resolution Protocol
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DDNS	Dynamic Domain Name Server
DDoS	Distributed Denial of Service
DPD	Dead Peer Detection
GMT	Greenwich Mean Time
HTTP	Hyper Text Transfer Protocol
IP	Internet Protocol
ICMP	Internet Control Message Protocol
ISP	Internet Service Provider
LAN	Local Area Network
L2TP	Layer 2 Tunneling Protocol
MAC	Medium Access Control
NAT	Network Address Translation
PPP	Point to Point Protocol
PPTP	Point to Point Tunneling Protocol
SMTP	Simple Mail Transfer Protocol
SSID	Service Set Identifier
SPI	Security Parameter Index
SSL	Secure Sockets Layer

Acronym or Abbreviation	Full Spelling
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
URL	Uniform Resource Locator
UPnP	Universal Plug and Play
WAN	Wide Area Network
WMM	Wi-Fi multi-media