www.ip-com.com.cn

User Guide

AC3000 Tri-band Cable-Free WiFi Router

IP-COM

World Wide Wireless

Copyright Statement

©2021 IP-COM Networks Co., Ltd. All rights reserved.

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 CompFi 6 AC3000 Tri-band Cable-Free WiFi Router.

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.

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

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

Revision History

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

Version	Date	Description
V1.0	2021-12-27	Original publication

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 UI.

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

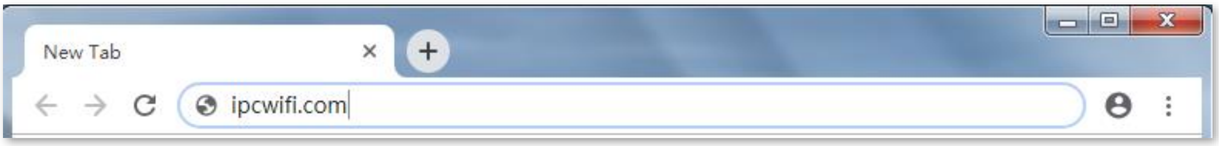
1.1.1 Log in to the Cable-Free (Router Mode) device

Tip

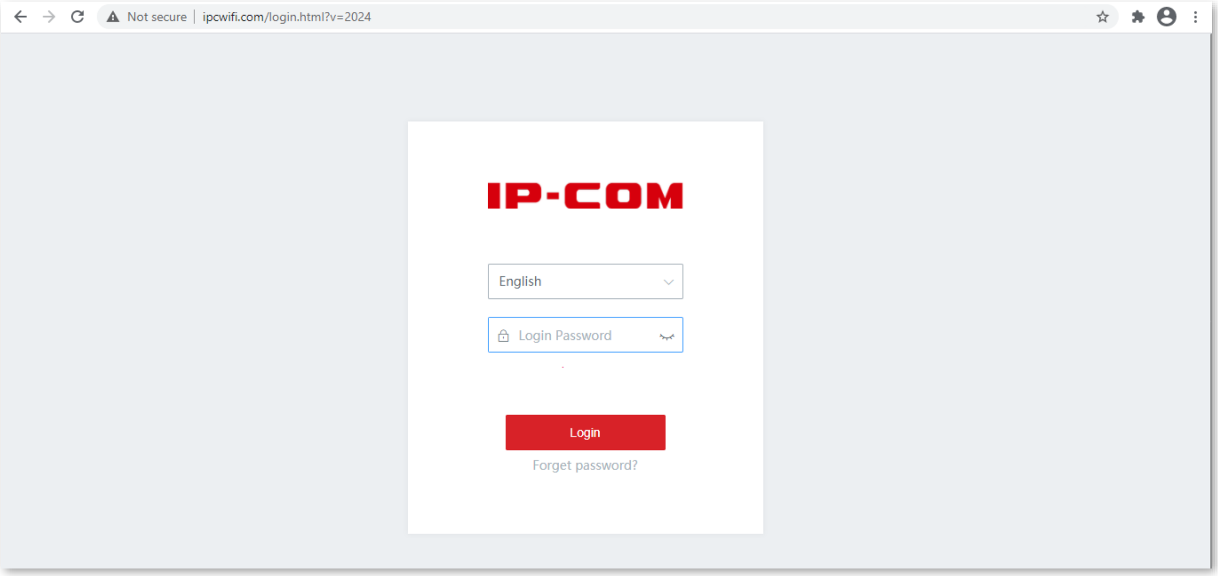
- In **Cable-Free (Router Mode)**, the **PoE WAN/LAN1** and **WAN/LAN2** ports of the device serve as WAN ports.
- The device works in **Cable-Free (Router Mode)** by default.

Log in with your computer

1. Connect the computer to the **WAN/LAN3** or **LAN4** port of the device with an Ethernet cable.
2. Start a browser on the computer, such as Google Chrome, and visit **www.ipcwifi.com**



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



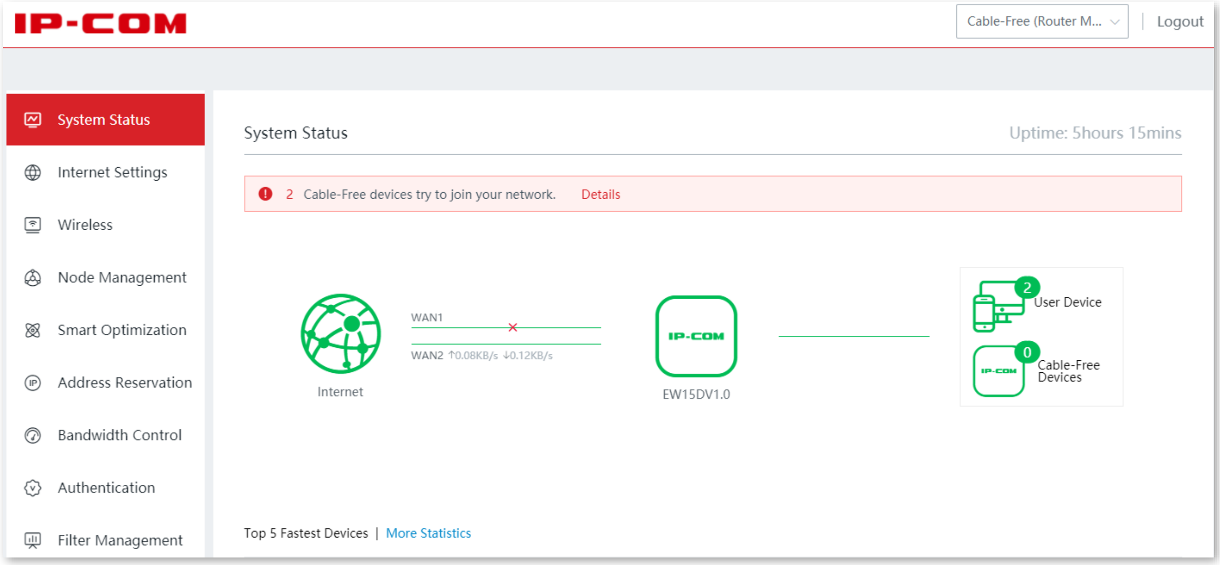
----End

Tip

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

- Ensure that the device is powered on.
- Ensure that your computer is connected to the LAN port of the device, and is set to **Obtain an IP address automatically** and **Obtain DNS server address automatically**.
- Reset the device and log in again. How to reset: When the **SYS** LED indicator is blinking, hold down the **RESET** button with a needle-like object for about 8 seconds and release it when all the LED indicators light solid green. When the **SYS** LED indicator blinks again, the device is reset successfully.

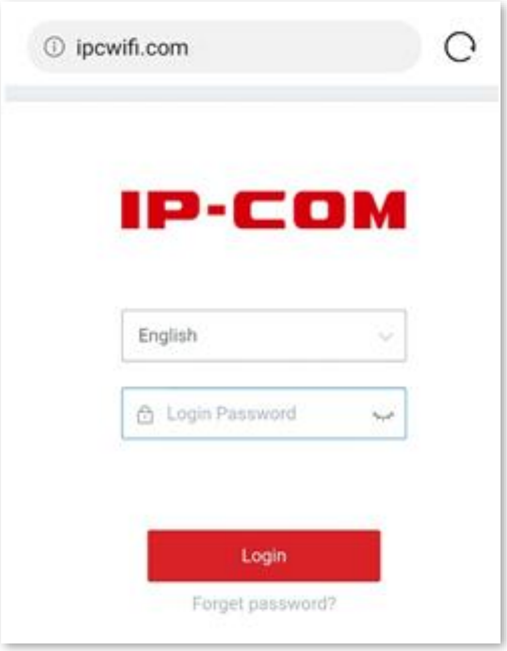
Log in to the web UI successfully. See the following figure.



- **Log in with your smartphone/iPad**

Take smartphone as an example.

1. Connect your smartphone to the WiFi network of the device.
2. Start a browser on the smartphone, 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 solutions:

- Ensure that your smartphone is connected to the WiFi network of the device.
- Ensure that the mobile data is disabled.
- Reset the device and log in again. How to reset: When the **SYS** LED indicator is blinking, hold down the **RESET** button with a needle-like object for about 8 seconds and release it when all the LED indicators light solid green. When the **SYS** LED indicator blinks again, the device is reset successfully.

----End

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

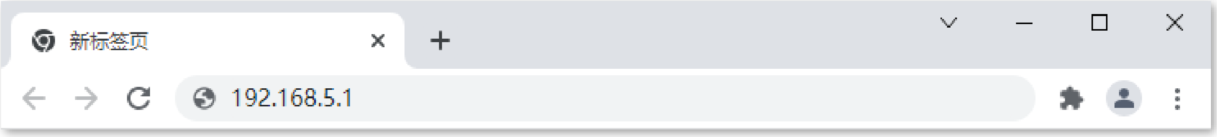
Tip

In **Cable-Free (AP Mode)**, the **PoE WAN/LAN1** port of the device serves as a LAN port generally connecting to an upstream router, and the **WAN/LAN2** port serves as a LAN port connecting to a LAN device.

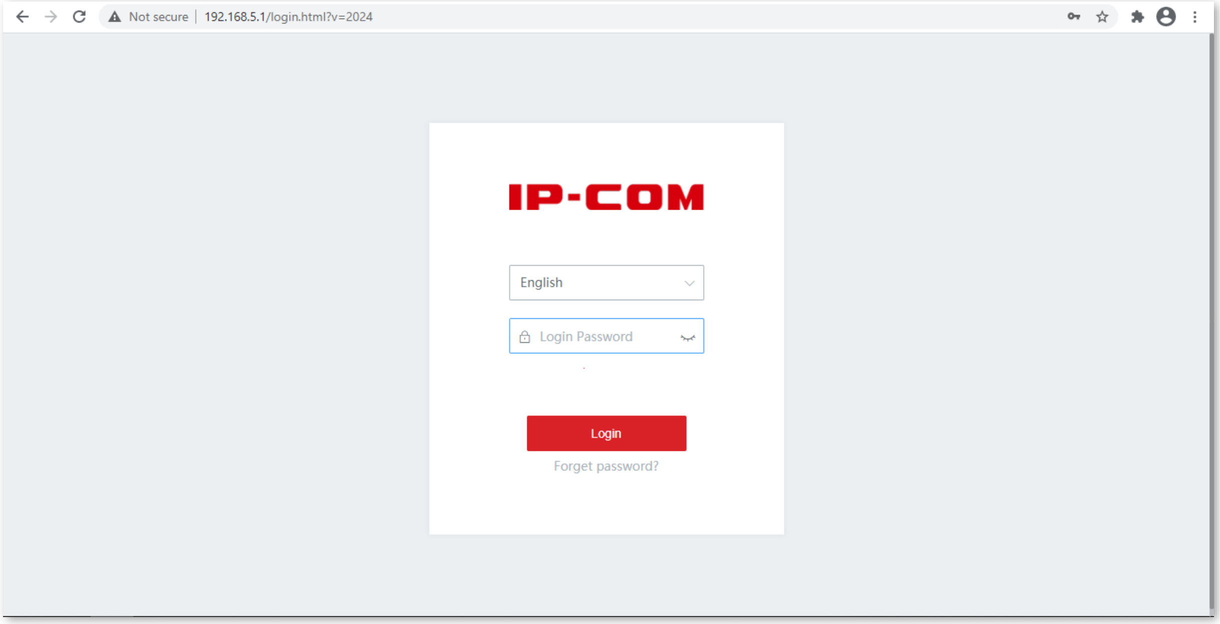
Log in with your computer

1. Connect the computer to the **WAN/LAN2**, **WAN/LAN3**, or **LAN4** port of the device with an Ethernet cable.
2. Set the IP address of the computer to make sure the computer and the device are on the same segment. By default, the IP address of the device is **192.168.5.1**. If the device connects to an upstream router or AC, its IP address can be obtained from the connected upstream router or AC.

   For example, if the IP address of the device is **192.168.5.1**, set the IP address of the computer to **192.168.5.*X*** (*X* ranges from 2 to 254 and is not occupied by other devices), and the subnet mask to **255.255.255.0**.
3. Start a browser on 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**.



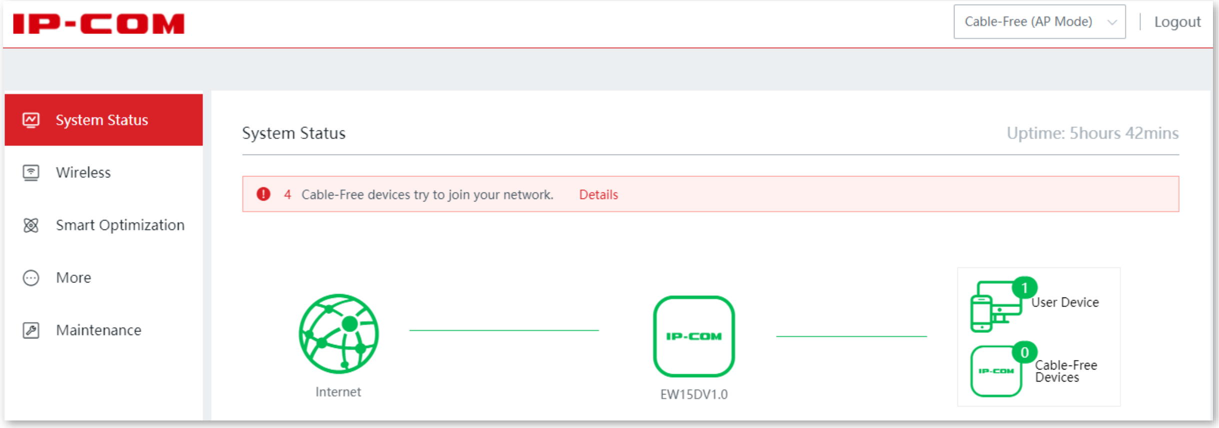
----End

Tip

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

- Ensure the device is powered on.
- Ensure that the computer is connected to the LAN port of the device, and the computer and the device are on the same network segment.

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



Cable-Free (AP Mode) | Logout

System Status

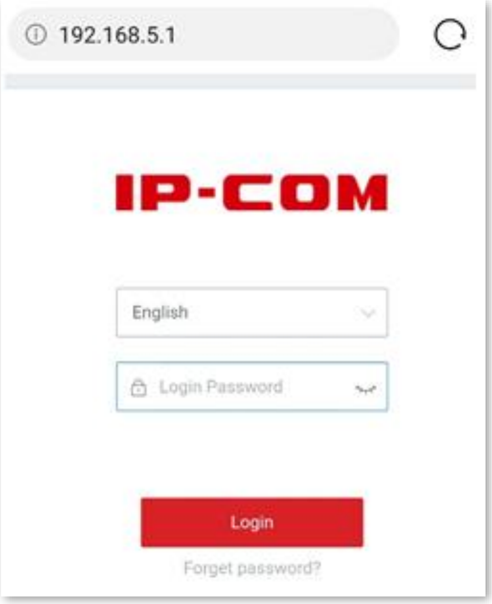
Uptime: 5hours 42mins

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

Log in with your smartphone/iPad

Take smartphone as an example.

1. Connect your smartphone to the WiFi network of the device.
2. Configure the IP address of the smartphone to make sure the smartphone and the device are on the same network segment.
   For example, if the IP address of the device is **192.168.5.1**, configure the IP address of the smartphone to **192.168.5.*X*** (*X* ranges from 2 to 254 and is not occupied by other devices), and the subnet mask to **255.255.255.0**.
3. Start a browser on the smartphone, and visit **192.168.5.1**
4. Enter the login password, and click **Login**.



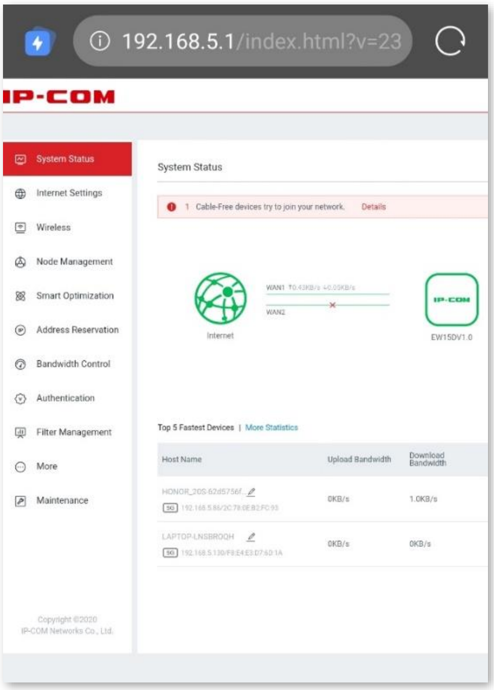
Tip

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

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

----End

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



System Status

1 Cable-Free devices try to join your network. Details

Top 5 Fastest Devices | More Statistics

Host Name	Upload Bandwidth	Download Bandwidth
HONOR_20S-62d5756f... 5G 192.168.5.86/2C:78:0E:B2:FC:93	0KB/s	1.0KB/s
LAPTOP-LNSBROQH 5G 192.168.5.130/F8:E4:E3:D7:60:1A	0KB/s	0KB/s

1.2 Log out of the web UI

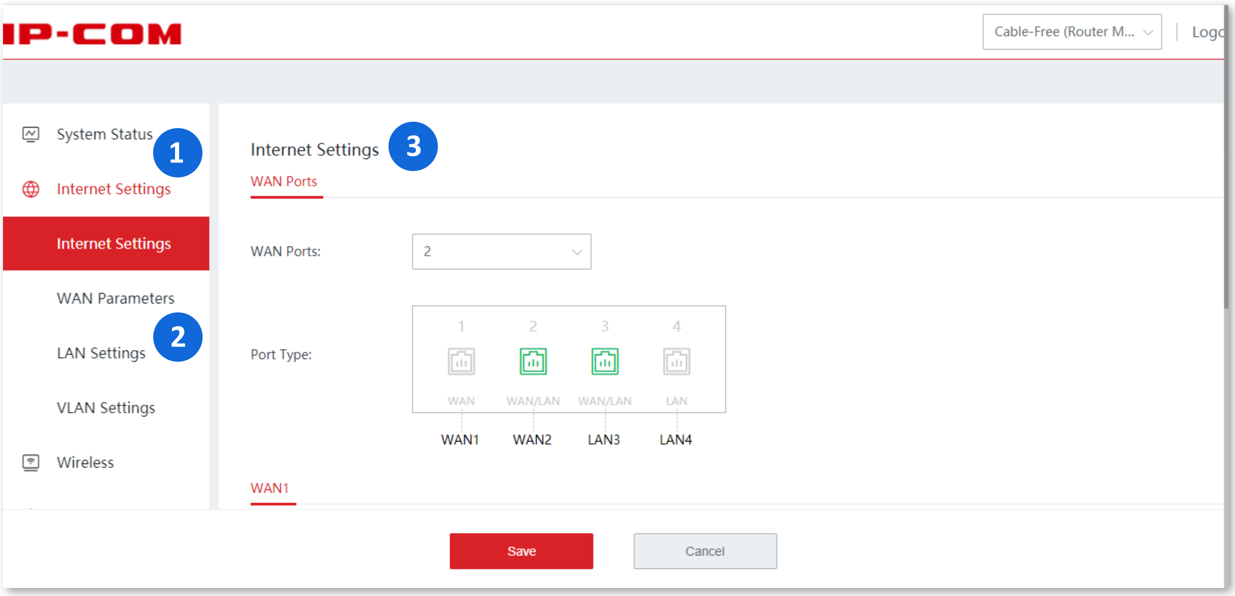
If you log in to the web UI of the device and perform no operation within 20 minutes, the device logs you out automatically.

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.



WAN Ports: 2

Port Type:

Tip

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

NO.	Name	Description
1	Level-1 navigation bar	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.

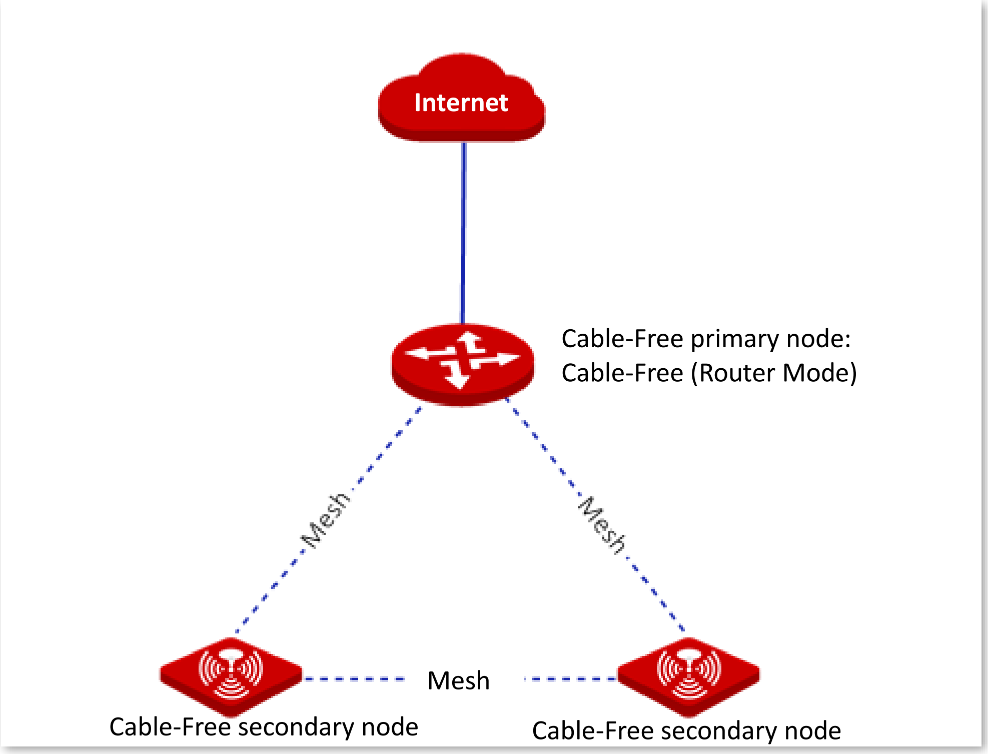
2.2 Frequently-used elements

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 made.
Refresh	It is used to refresh the current page to check the latest configuration.
?	It is used to view help information for the current page.
Cable-Free (Router M... ⌄	Click the drop-down list to select and switch the work mode of the cable-free device. You can switch 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 displays the status of the function, including enabled and disabled. ● specifies the function is enabled and ○ specifies the function is disabled.
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)

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



3.1 System status

In this section, you can:

- Check physical connections and device info
- Add secondary nodes
- Monitor traffic
- Manage online devices

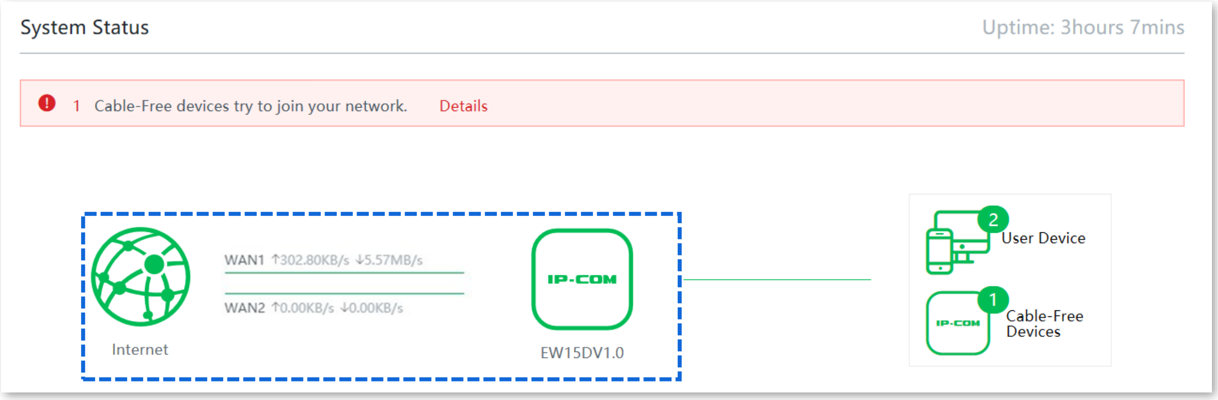
3.1.1 Check physical connections and device info

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

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

Check physical connections

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

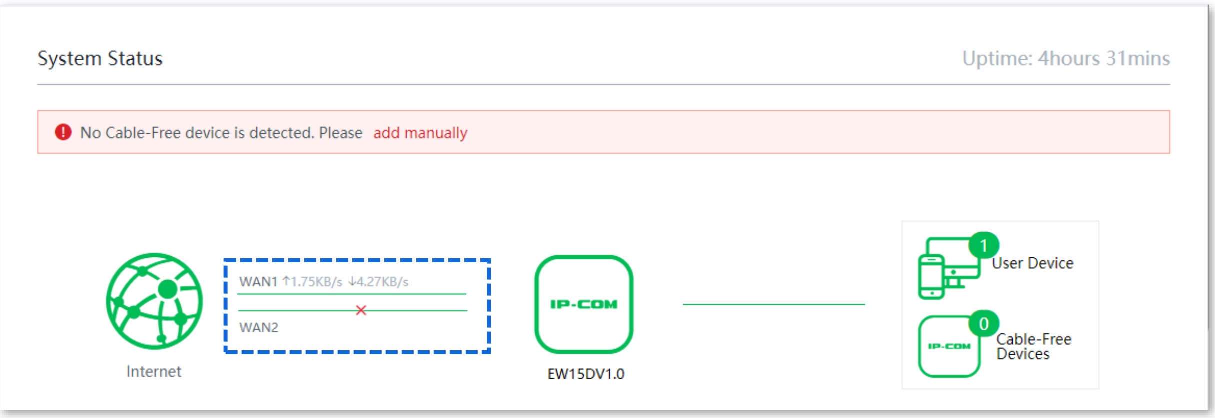


System Status

Uptime: 3hours 7mins

1 Cable-Free devices try to join your network. Details

The following figure indicates that the Cable-Free (Router Mode) node is not connected to the internet properly through a WAN port. Please check whether that WAN port of the device is connected to the internet properly, or the internet connection parameters you set are correct.



System Status

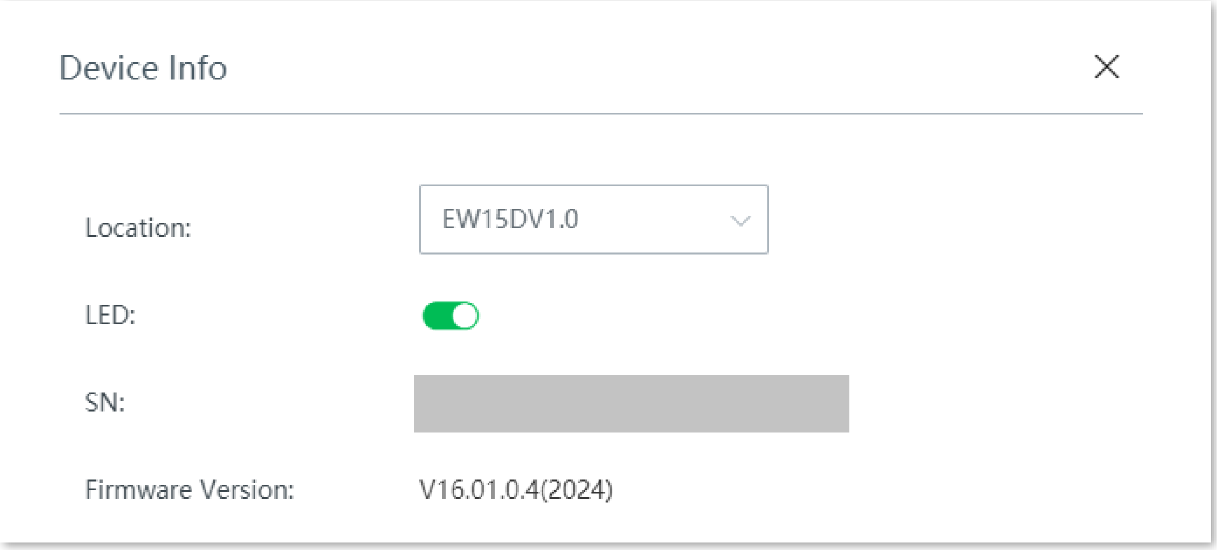
Uptime: 4hours 31mins

No Cable-Free device is detected. Please add manually

Check the information of the cable-free primary node

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

Device info



Device Info

Location: EW15DV1.0

LED: ●

SN:

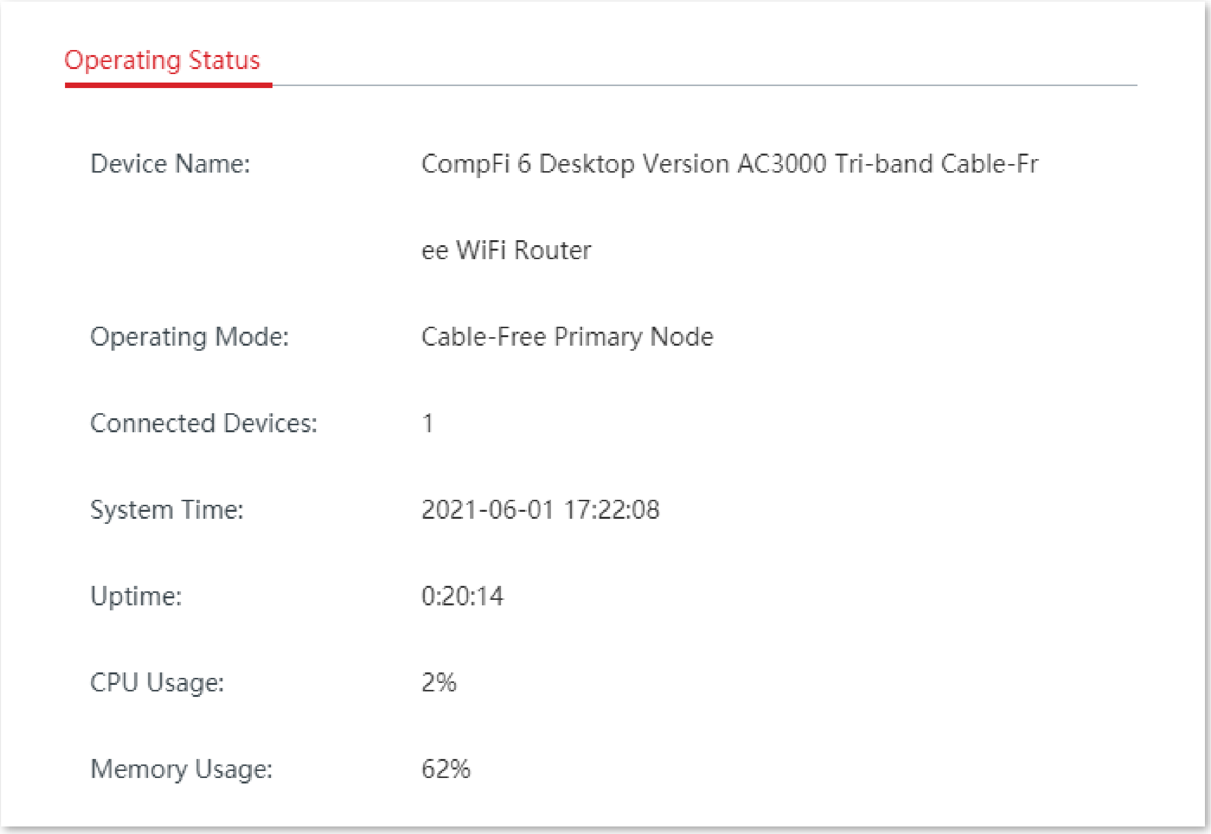
Firmware Version: V16.01.0.4(2024)

Parameter description

Parameter	Description
Location	It specifies the location information of the node, which helps you easily locate it. You can select a location description from the drop-down list or customize one as required.

Parameter	Description
LED	It specifies the status of the LED indicators of the node. 🟢: It indicates that the LED indicators are turned on. You can judge the operating status of the device based on the LED indicators. ⚪: It indicates that the LED indicators are turned off.
SN	It specifies the serial number of the node, which is used to manually add the node into a mesh network.
Firmware Version	It specifies the current version of the node.

Operating status



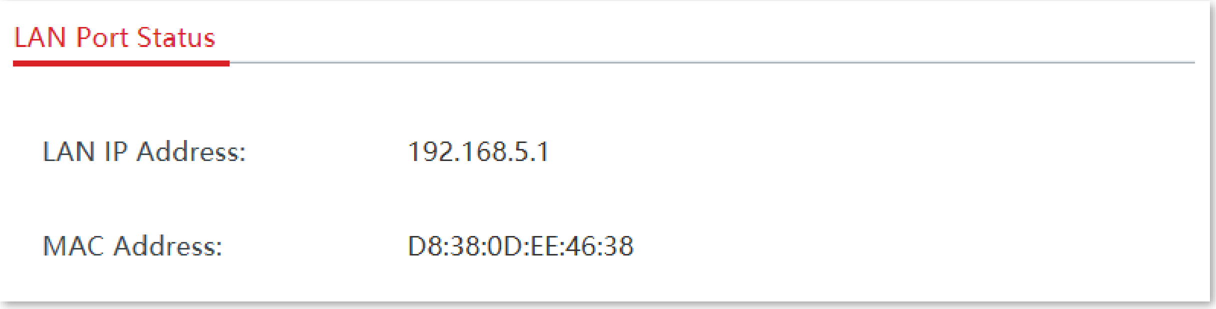
Operating Status

Device Name:	CompFi 6 Desktop Version AC3000 Tri-band Cable-Free WiFi Router
Operating Mode:	Cable-Free Primary Node
Connected Devices:	1
System Time:	2021-06-01 17:22:08
Uptime:	0:20:14
CPU Usage:	2%
Memory Usage:	62%

Parameter description

Parameter	Description
Device Name	It specifies the name of your node.
Operating Mode	It specifies the current operating mode of the node. – **Cable-Free Primary Node**: The node serves as a primary node in the cable-free network and connects to a wired network. The node is the only exit to the external network in the cable-free network and transforms data between the Mesh network and the wired network. – **Cable-Free Secondary Node**: The node serves as a secondary node in the cable-free network and is used to extend the coverage of the existing cable-free network through Mesh technology. Tip If the node serves as a cable-free secondary node, the **PoE WAN/LAN1** port and the **WAN/LAN2** port are LAN ports.
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 duration the node has been running.
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

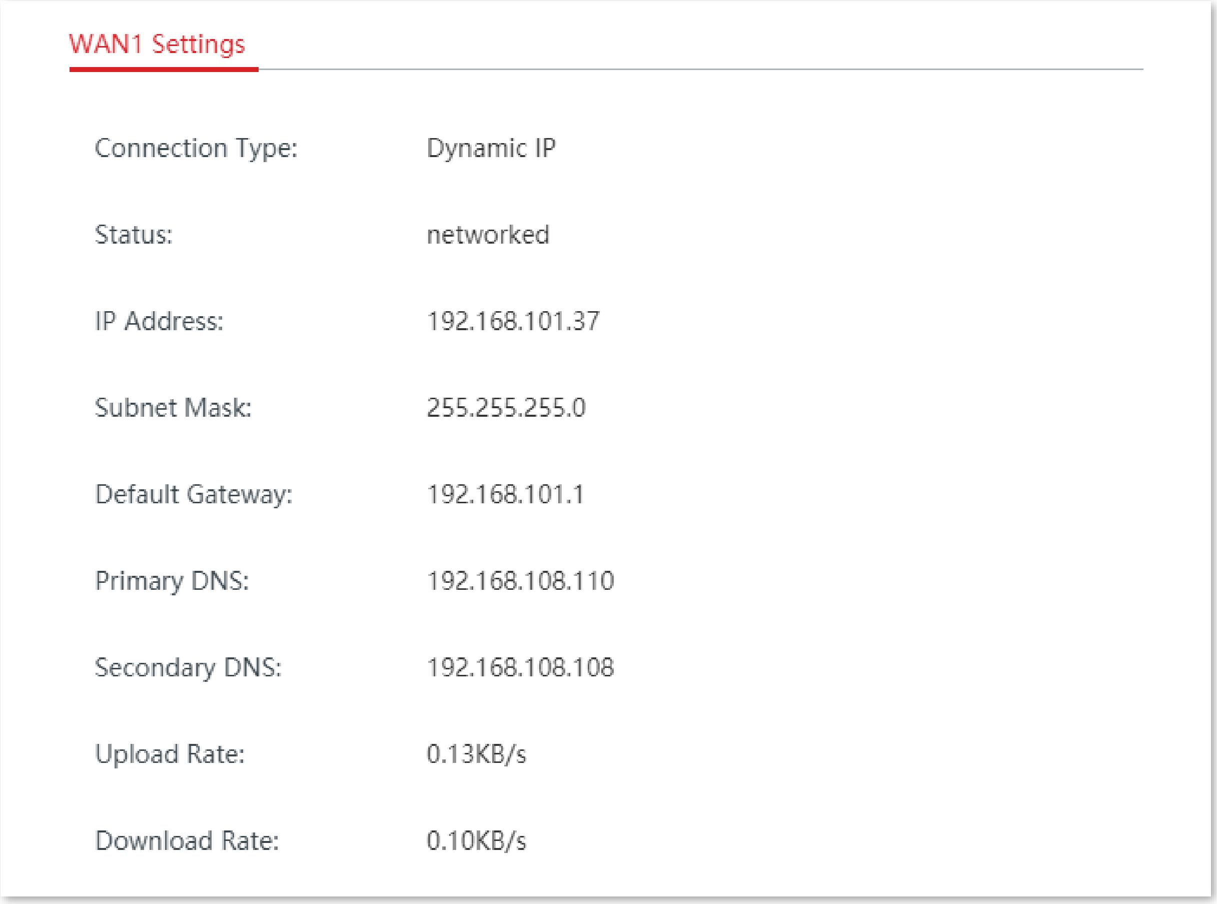
MAC Address: D8:38:0D:EE:46:38

Parameter description

Parameter	Description
LAN IP Address	It specifies the IP address of the LAN port of the node and is also the management IP address of the node, which is **192.168.5.1** by default. LAN users can visit this IP address to log in to the management web UI of the node. The IP address of the secondary node is automatically obtained from the DHCP server of the primary node.

Parameter	Description
MAC Address	It specifies the physical address of the LAN port of the node.

WAN settings



WAN1 Settings

Connection Type: Dynamic IP

Status: networked

IP Address: 192.168.101.37

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.101.1

Primary DNS: 192.168.108.110

Secondary DNS: 192.168.108.108

Upload Rate: 0.13KB/s

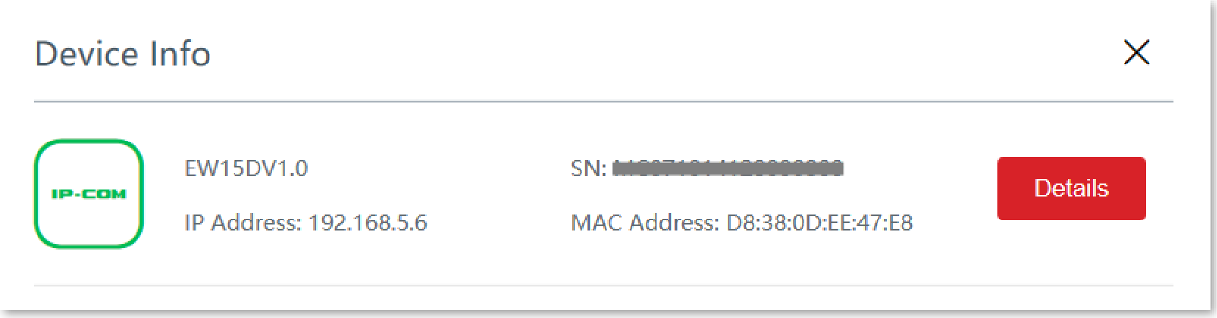
Download Rate: 0.10KB/s

Parameter description

Parameter	Description
Connection Type	It specifies the internet connection type of the WAN port of the node.
Status	It specifies the connection status of the WAN port of the node. If **Disconnected** appears, please check the physical connection of the WAN port.
IP Address	It specifies the IP address of the WAN port of the node.
Subnet Mask	It specifies the subnet mask of the WAN port of the node.
Default Gateway	It specifies the gateway IP address of the WAN port of the node.
Primary DNS	It specifies the primary/secondary DNS server address of the WAN port of the node.
Secondary DNS	
Upload Rate	It specifies the real-time upload/download rate of the WAN port of the node.
Download Rate	

Check the information of the cable-free secondary nodes

On the **System Status** page, click the cable-free devices icon next to the user device icon, you can check the device info of the cable-free secondary nodes.



Device Info

EW15DV1.0

SN: [redacted]

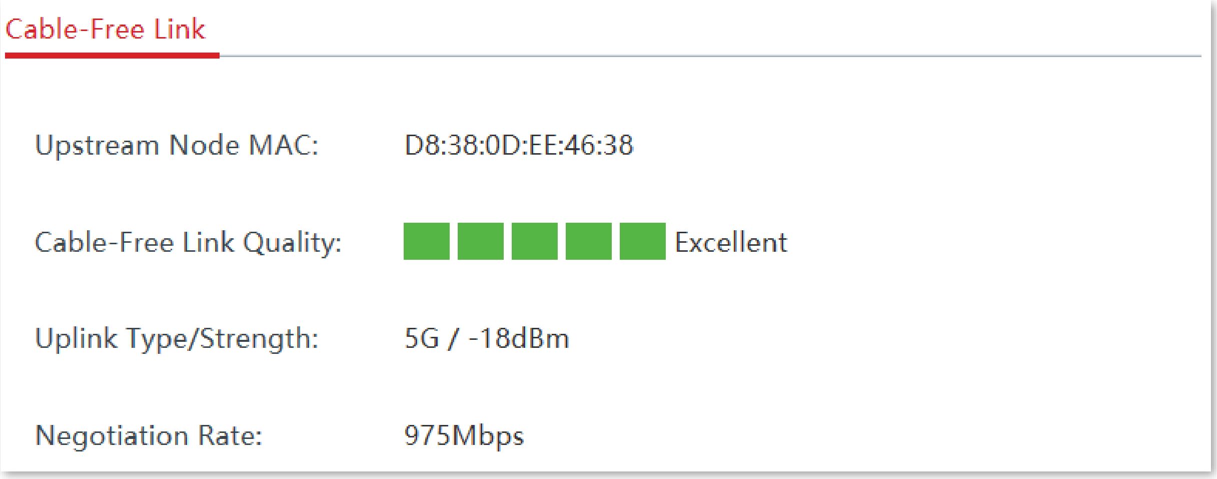
IP Address: 192.168.5.6

MAC Address: D8:38:0D:EE:47:E8

For more information, please click Details on the page of the target node.

Here, you can check or set the device info of the node, check its operating status, LAN port status, cable-free link quality, and restart or delete the node.

Cable-free link quality



Cable-Free Link

Upstream Node MAC: D8:38:0D:EE:46:38

Cable-Free Link Quality: 🟩🟩🟩🟩🟩 Excellent

Uplink Type/Strength: 5G / -18dBm

Negotiation Rate: 975Mbps

Parameter description

Parameter	Description
Upstream Node MAC	It specifies the physical address of the interface used by the upstream node in the Mesh network to form the Mesh link.
Cable-Free Link Quality	It specifies the connection quality of the cable-free links.
Uplink Type/Strength	It specifies the mode in which the node and its upstream node form a network and the strength of the signal of the upstream node received by the node.
Negotiation Rate	It specifies the rate at which the node performs negotiation with its upstream node.

Reboot the node

Click **Reboot** to reboot the node.

Delete the node

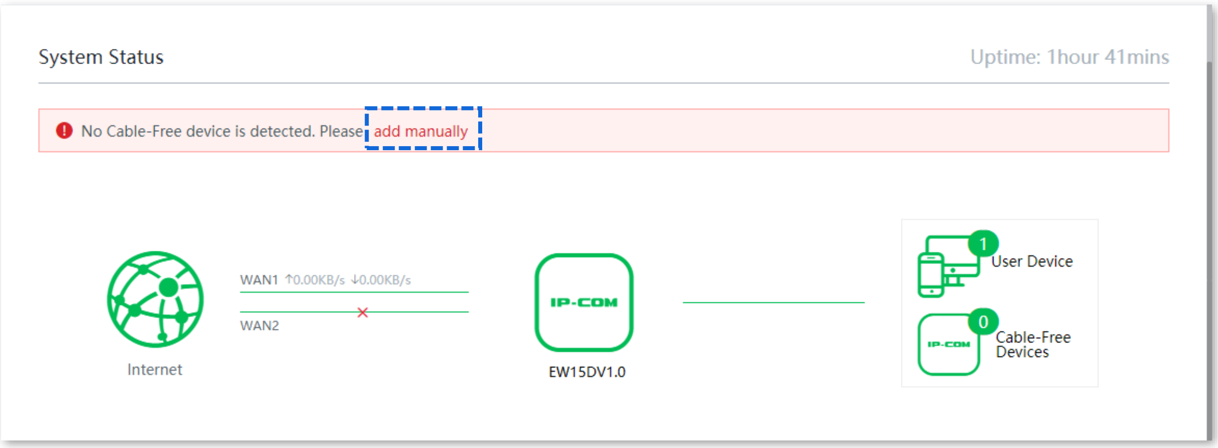
Click **Delete** to delete the node from the cable-free network. Nodes deleted from the cable-free network will be restored to factory settings.

3.1.2 Add secondary nodes

Generally, the primary node device can automatically detect secondary node devices in factory settings. If your secondary node device fails to be detected, you can also log in to the web UI of the primary node device to manually add secondary node devices.

Configuration procedures (add manually)

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

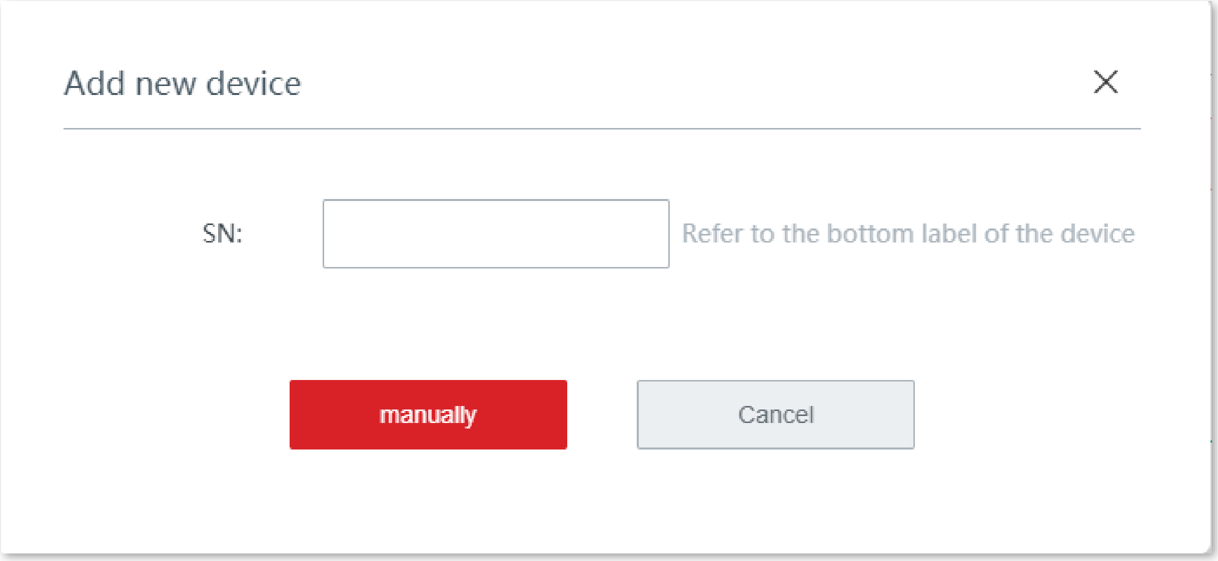


System Status

Uptime: 1hour 41mins

No Cable-Free device is detected. Please add manually

3. Enter the SN (on the surface label) of the Mesh device to be added.
4. Click **manually**.

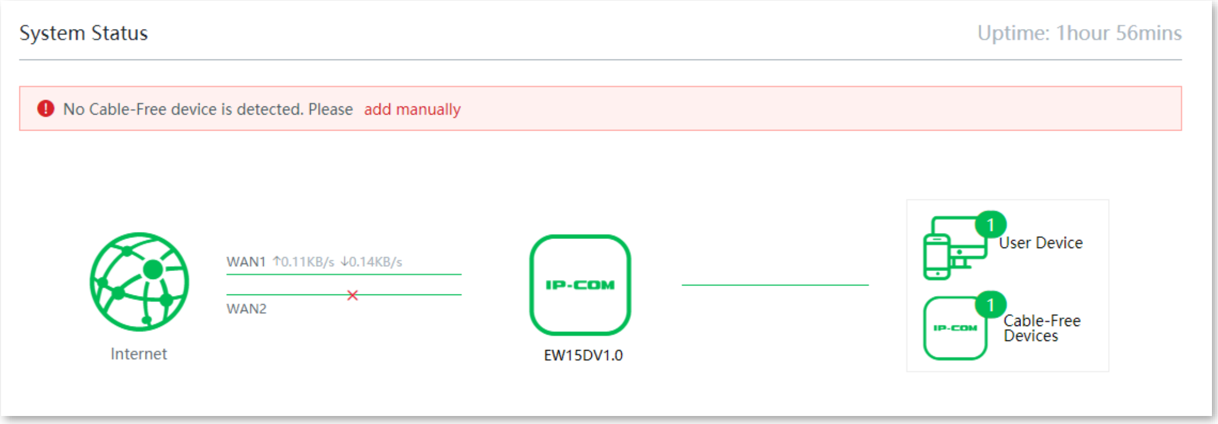


Add new device

SN: Refer to the bottom label of the device

----End

After the secondary node device is added successfully, you can click the cable-free devices icon on the right side of the **System Status** page to check its details.



System Status

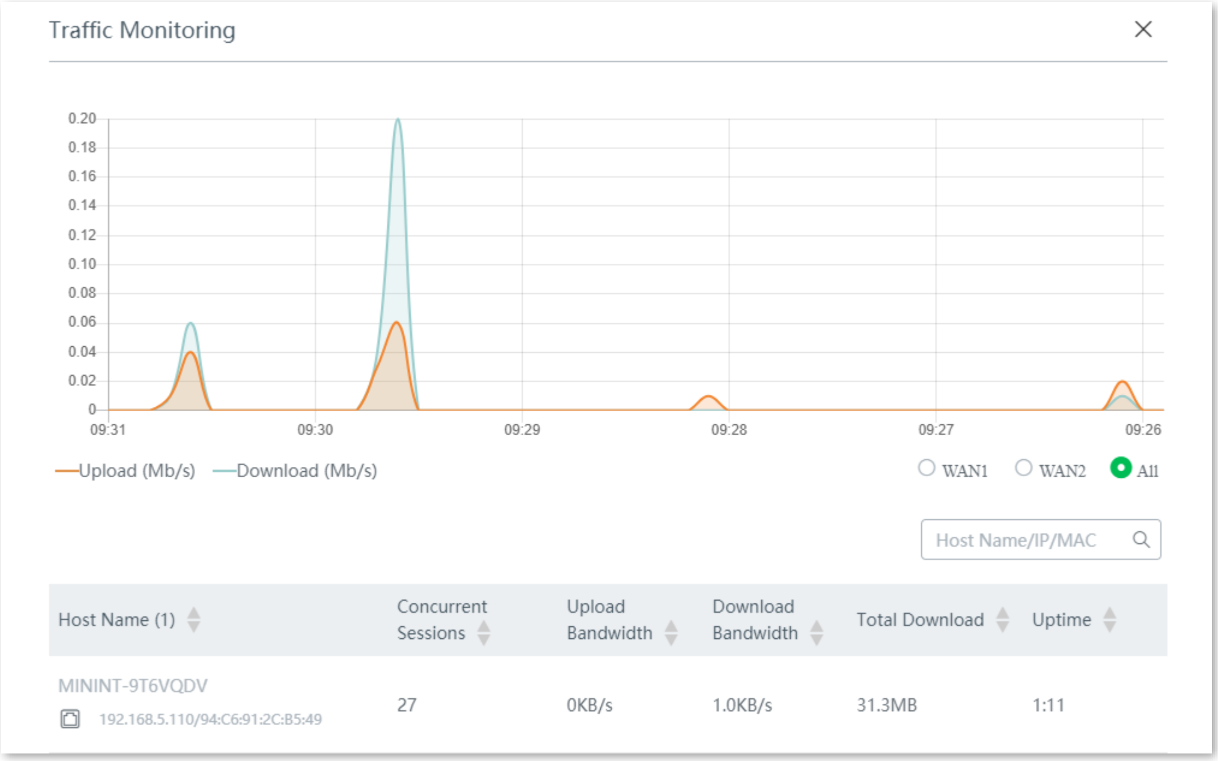
Uptime: 1hour 56mins

No Cable-Free device is detected. Please add manually

3.1.3 Monitor traffic

You can view the real-time upload and download bandwidth of the WAN ports, 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 (1)	Concurrent Sessions	Upload Bandwidth	Download Bandwidth	Total Download	Uptime
MININT-9T6VQDV □ 192.168.5.110/94:C6:91:2C:B5:49	27	0KB/s	1.0KB/s	31.3MB	1:11

Parameter description

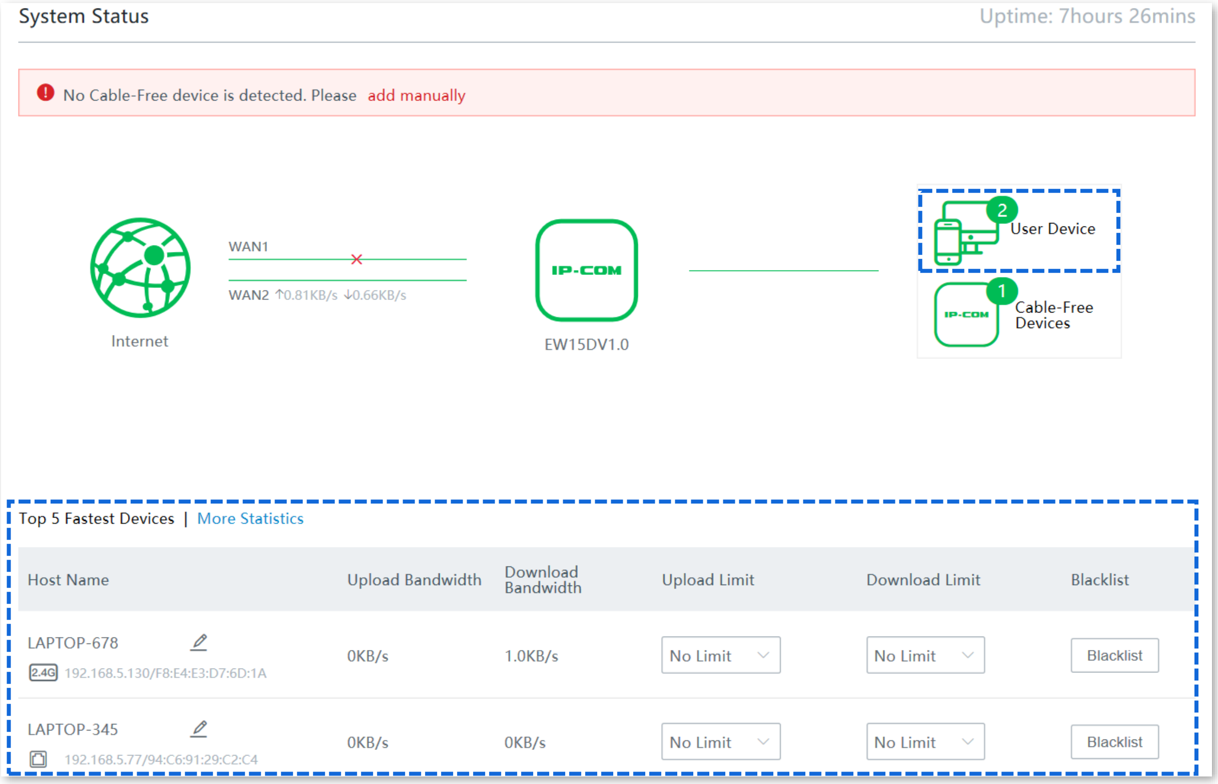
Parameter	Description
Host Name	It displays the name, IP address, and MAC address of the connected client. Tip If you want to add host name-based rules, such as adding an authentication-free host using host name, you need to use the host name here. □ : The client connects to the device in a wired manner. 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 the concurrent sessions established by the client.
Upload Bandwidth	It displays the current upload/download bandwidth of the client. You can set the maximum upload/download bandwidth for a client. For details, refer to Manage online devices.
Download Bandwidth	
Total Download	It specifies the total download traffic generated by the client.
Uptime	It specifies the duration the client has been connected.

3.1.4 Manage online devices

You can edit the name of user devices, set the upload and download bandwidth separately or in batches, or block a device from accessing your network.

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

The **System Status** page displays the top 5 clients with the highest speed. Click the **User Device** icon to manage all connected user devices.



System Status

Uptime: 7hours 26mins

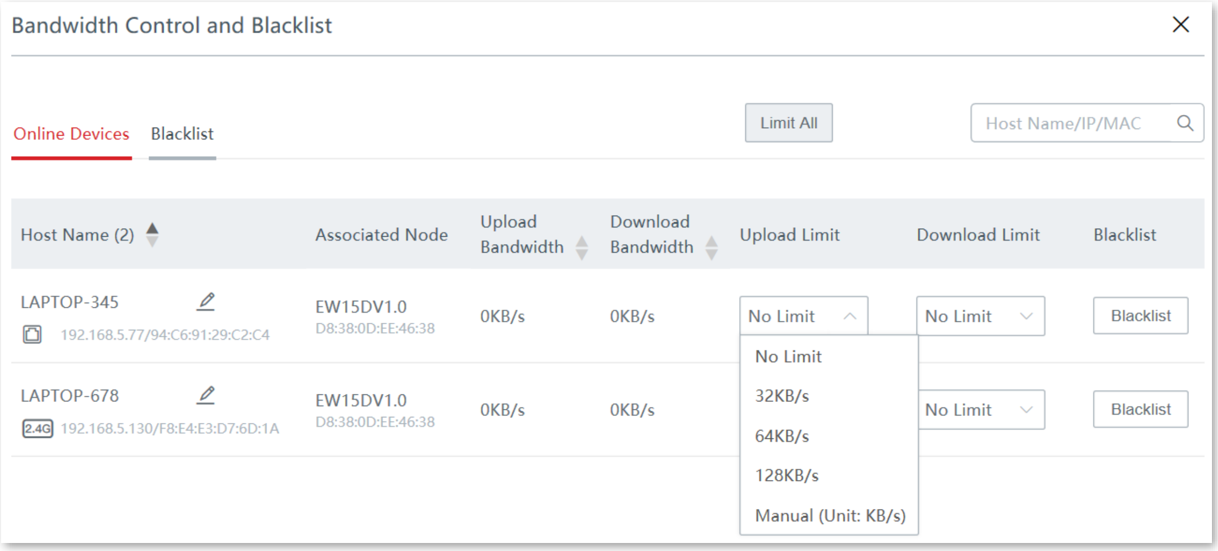
! No Cable-Free device is detected. Please add manually

Top 5 Fastest Devices | More Statistics

Host Name	Upload Bandwidth	Download Bandwidth	Upload Limit	Download Limit	Blacklist
LAPTOP-678 2.4G 192.168.5.130/F8:E4:E3:D7:6D:1A	0KB/s	1.0KB/s	No Limit	No Limit	Blacklist
LAPTOP-345 192.168.5.77/94:C6:91:29:C2:C4	0KB/s	0KB/s	No Limit	No Limit	Blacklist

Set bandwidth limit for connected clients

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



Bandwidth Control and Blacklist

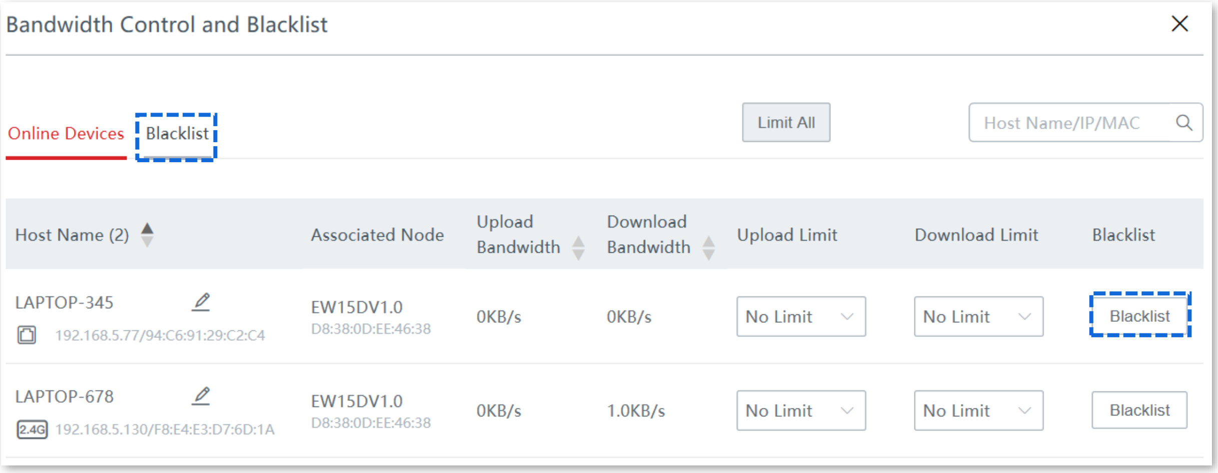
Online Devices | Blacklist | Limit All | Host Name/IP/MAC

Host Name (2)	Associated Node	Upload Bandwidth	Download Bandwidth	Upload Limit	Download Limit	Blacklist
LAPTOP-345 192.168.5.77/94:C6:91:29:C2:C4	EW15DV1.0 D8:38:0D:EE:46:38	0KB/s	0KB/s	No Limit	No Limit	Blacklist
LAPTOP-678 2.4G 192.168.5.130/F8:E4:E3:D7:6D:1A	EW15DV1.0 D8:38:0D:EE:46:38	0KB/s	0KB/s		No Limit	Blacklist

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

Add devices into the blacklist

To block unknown devices from accessing your network, click the **Blacklist** button to blacklist them. The blocked devices will be moved to the **Blacklist** tab page and cannot access the internet through the device.



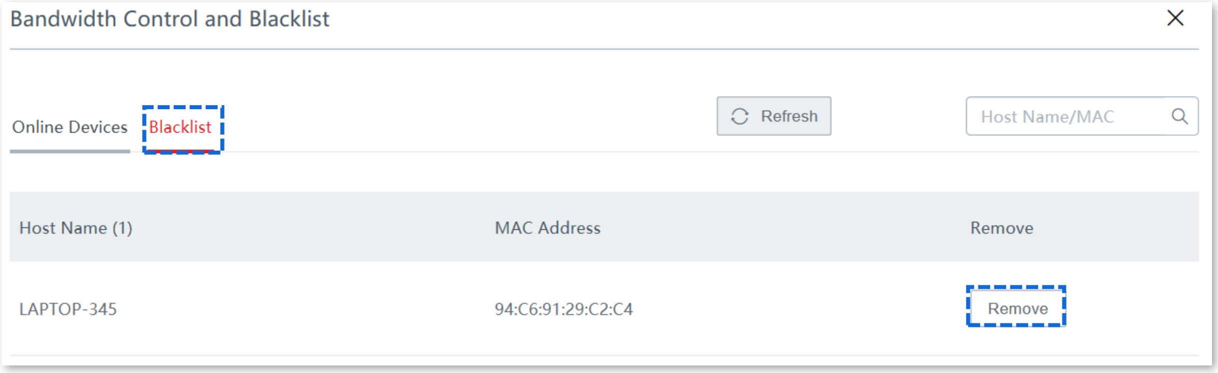
Bandwidth Control and Blacklist

Online Devices | Blacklist | Limit All | Host Name/IP/MAC

Host Name (2)	Associated Node	Upload Bandwidth	Download Bandwidth	Upload Limit	Download Limit	Blacklist
LAPTOP-345 192.168.5.77/94:C6:91:29:C2:C4	EW15DV1.0 D8:38:0D:EE:46:38	0KB/s	0KB/s	No Limit	No Limit	Blacklist
LAPTOP-678 2.4G 192.168.5.130/F8:E4:E3:D7:6D:1A	EW15DV1.0 D8:38:0D:EE:46:38	0KB/s	1.0KB/s	No Limit	No Limit	Blacklist

Remove devices from the blacklist

To remove devices from the blacklist, click the **User Device** icon on the **System Status** page, click **Blacklist**, then click **Remove** to remove the target device.



Bandwidth Control and Blacklist

Host Name (1)	MAC Address	Remove
LAPTOP-345	94:C6:91:29:C2:C4	Remove

3.2 Internet settings

In this section, you can configure:

- Internet settings
- WAN parameters
- LAN settings
- VLAN settings

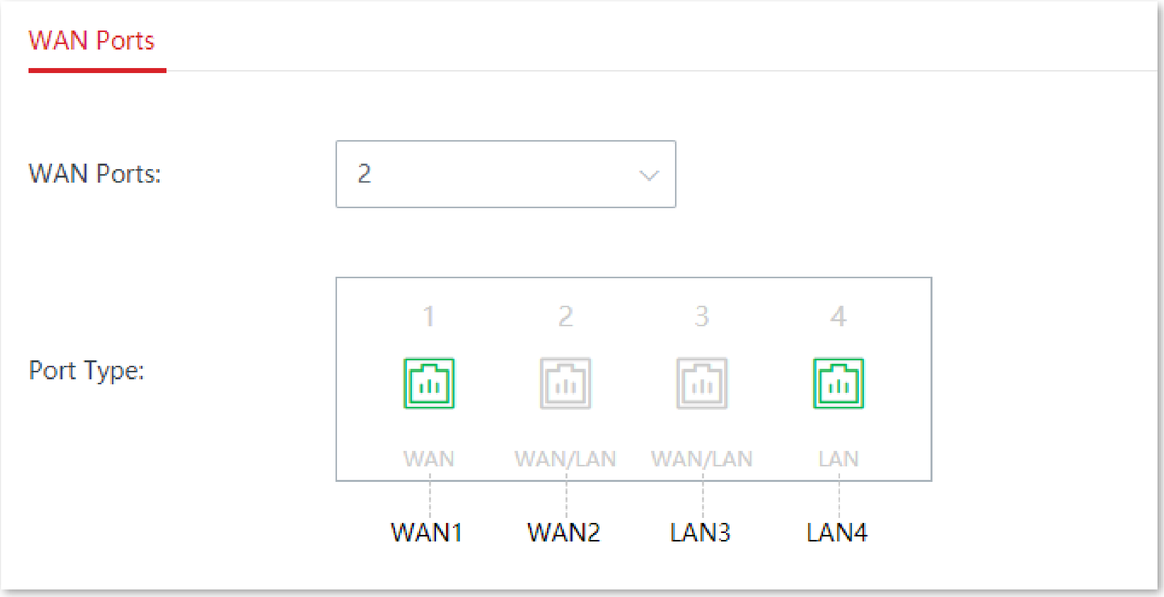
3.2.1 Internet settings

Overview

On this page, you can configure or change the internet settings to enable the device to access the internet.

If you are using the device for the first time or you restored 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.



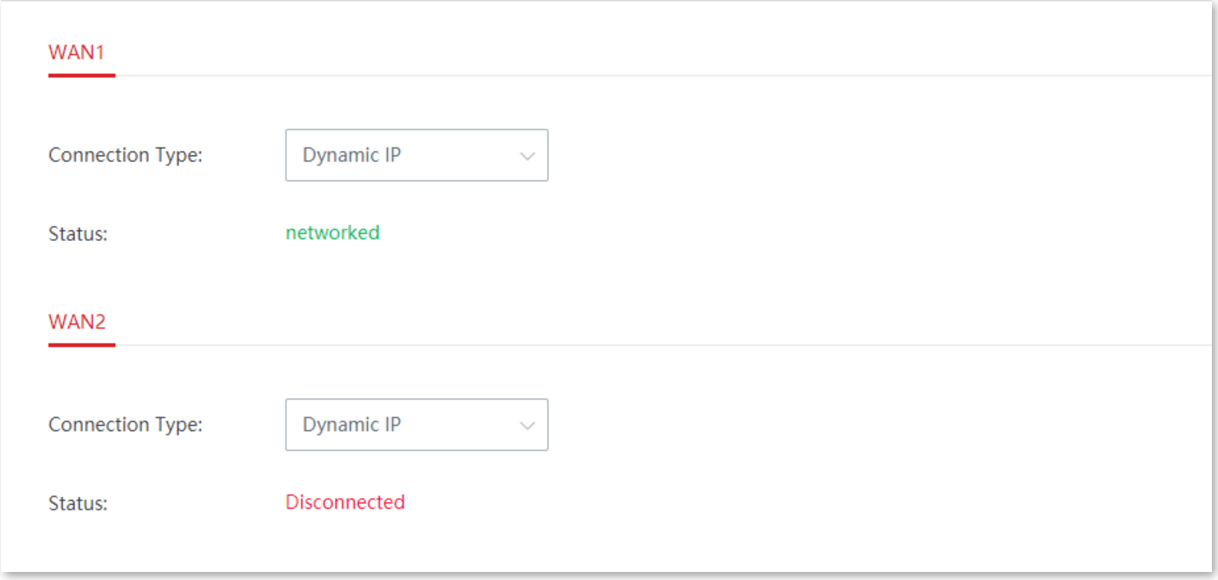
WAN Ports

WAN Ports: 2

Port Type:

Parameter description

Parameter	Description
WAN Ports	It specifies the number of WAN ports. By default, the device has 2 WAN ports (**PoE WAN/LAN1** and **WAN/LAN2**). You can change the WAN port number as needed. You can set 3 WAN ports at most.
Port Type	It specifies whether a port is connected. 🟩: The port is connected properly. ⬜: The port is disconnected or not connected properly.



WAN1

Connection Type: Dynamic IP

Status: networked

WAN2

Connection Type: Dynamic IP

Status: Disconnected

Parameter description

Parameter	Description
Connection Type	It specifies in what way the device connects to the internet. The options include **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**. You can obtain them from your ISP.
PPPoE Password	
Server Name	These two parameters are required only when your internet connection type is **PPPoE** or **PPPoE Russia**. You can obtain them from your ISP. These two parameters are optional.
Service Name	
PPTP Server Address	This parameter is required only when your internet connection type is **PPTP/PPTP Russia**. You can obtain it from your ISP.
L2TP Server Address	This parameter is required only when your internet connection type is **L2TP/L2TP Russia**. You can obtain it from your ISP.
User Name	These two parameters are required only when your internet connection type is

Parameter	Description
Password	**PPTP/PPTP Russia** or **L2TP/L2TP Russia**. You can obtain them from your ISP.
Obtain an IP address	This parameter appears when your internet connection type is **PPPoE Russia**, **PPTP/PPTP Russia**, or **L2TP/L2TP Russia**. If there is no DHCP server in the network, select **Manual** and enter the IP address and related parameters. If there is a DHCP server in the network, select **Auto**, and the device will obtain these parameters from the DHCP server.
IP Address	These parameters are required only when your internet connection type is **Static IP** or if you set **Obtain an IP address** to **Manual** when your internet connection type is **PPPoE Russia**, **PPTP/PPTP Russia**, or **L2TP/L2TP Russia**. The **Secondary DNS** parameter is optional. You can obtain them from your ISP.
Subnet Mask	
Default Gateway	
Primary DNS	
Secondary DNS	
Status	It specifies the internet connection status of the WAN port. – **Authenticated successfully/networked**: 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 whether the physical connection is proper, or the parameters you entered are correct.

Set up internet connection

Tip

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

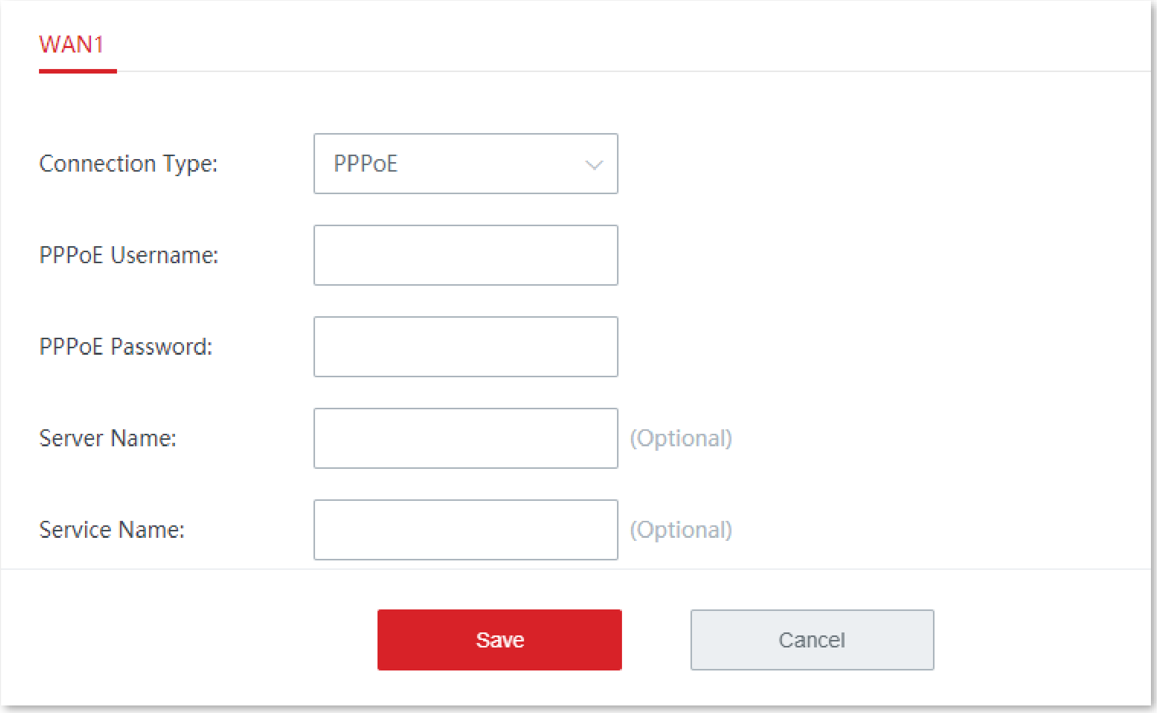
Choose your connection type

Available parameters	Connection type
PPPoE username, 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 has its DHCP server enabled.	Dynamic IP

Available parameters	Connection type
PPPoE username, PPPoE password, service name, and server name. If the DHCP server of the upstream device is disabled (means you have to select **Manual** for **Obtain an IP address**), then the IP address, subnet mask, default gateway, and primary DNS are required.	PPPoE Russia
PPTP server address, user name, and password. If the DHCP server of the upstream device is disabled (means you have to select **Manual** for **Obtain an IP address**), then the IP address, subnet mask, default gateway, and primary DNS are required.	PPTP/PPTP Russia
L2TP server address, user name, and password. If the DHCP server of the upstream device is disabled (means you have to select **Manual** for **Obtain an IP address**), then the IP address, subnet mask, default gateway, and primary DNS are required.	L2TP/L2TP Russia

PPPoE

1. Click **Internet Settings** to enter the page.
2. Set **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**.



Connection Type: PPPoE

PPPoE Username:

PPPoE Password:

Server Name: (Optional)

Service Name: (Optional)

----End

The device connects to the internet successfully when the **Status** is displayed as Authenticated successfully.

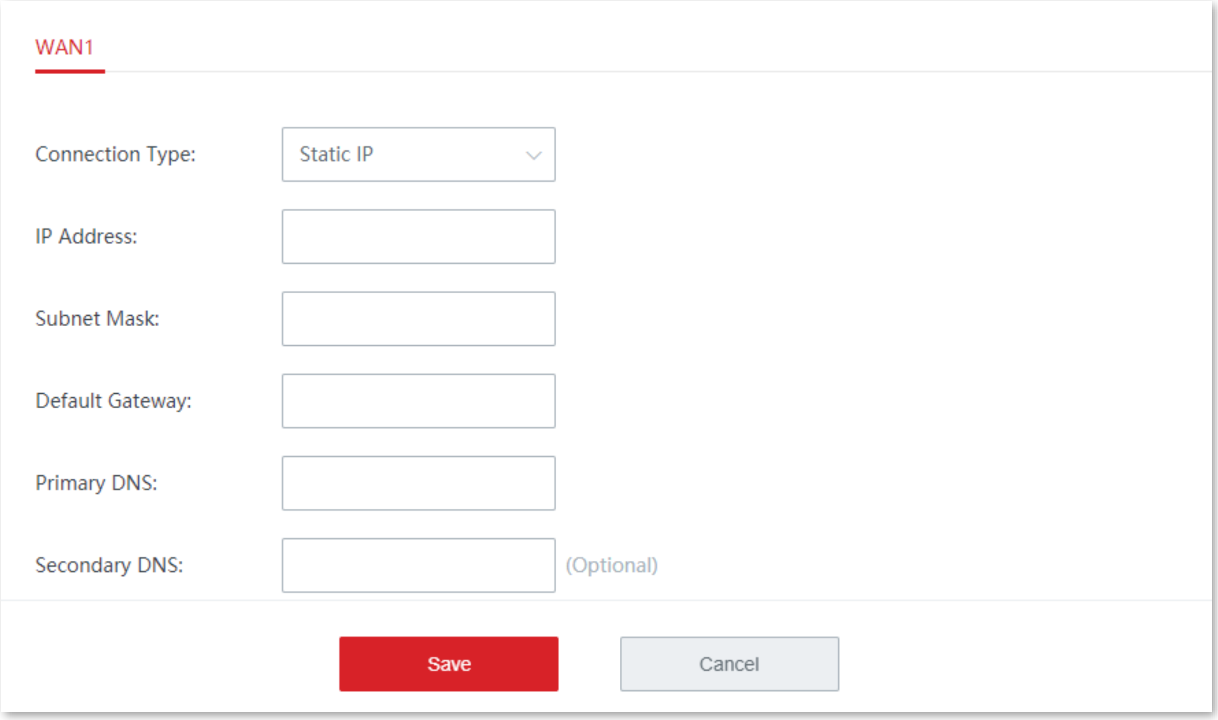
Tip

If you fail to access the internet, please try the following solutions:

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

Static IP

1. Click **Internet Settings** to enter the page.
2. Set **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**.



WAN1

Connection Type: Static IP

IP Address:

Subnet Mask:

Default Gateway:

Primary DNS:

Secondary DNS: (Optional)

----End

The device connects to the internet successfully when the **Status** is displayed as networked.

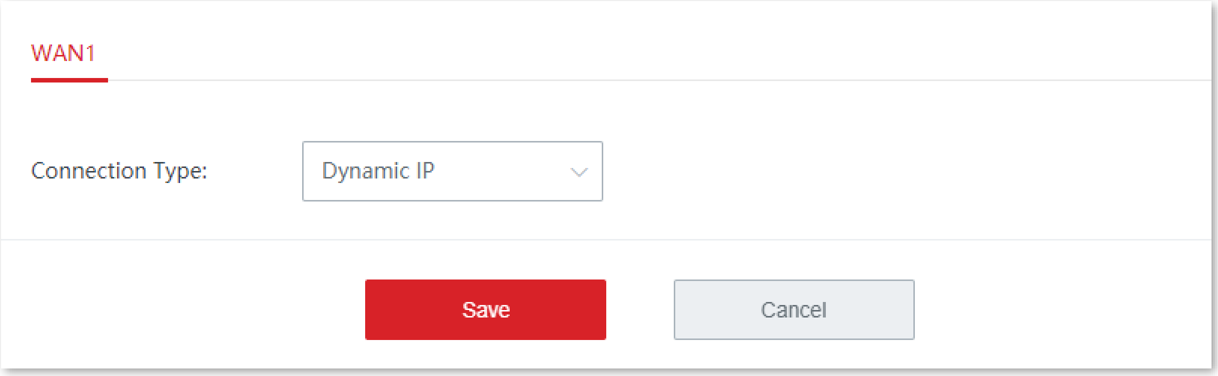
Tip

If you fail to access the internet, please try the following solutions:

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

Dynamic IP

1. Click **Internet Settings** to enter the page.
2. Set **Connection Type** to **Dynamic IP**.
3. Click **Save**.

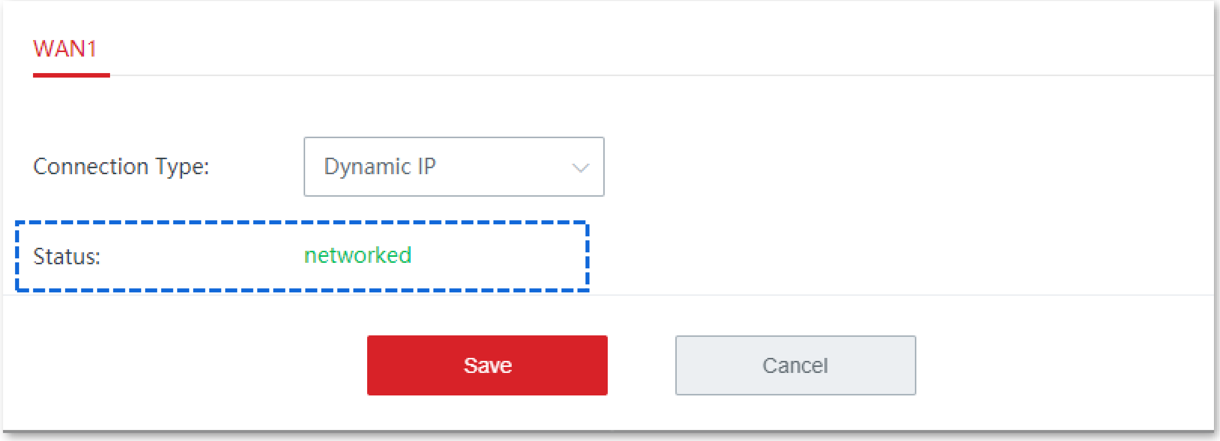


WAN1

Connection Type: Dynamic IP

----End

The device connects to the internet successfully when the **Status** is displayed as networked.



WAN1

Connection Type: Dynamic IP

Status: networked

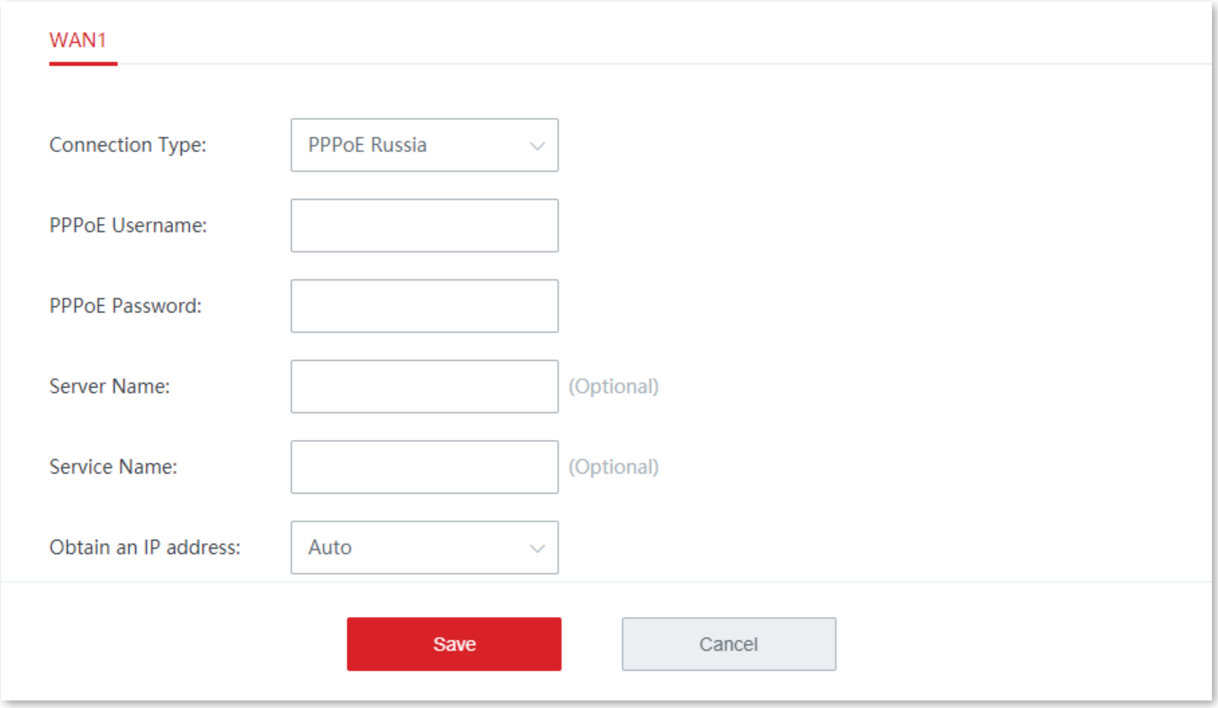
Tip

If you fail to access the internet, please try the following solutions:

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

PPPoE Russia

1. Click **Internet Settings** to enter the page.
2. Set **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 other related parameters are also provided, enter them in the corresponding input box as well.
4. Click **Save**.


WAN1

Connection Type: PPPoE Russia

PPPoE Username:

PPPoE Password:

Server Name: (Optional)

Service Name: (Optional)

Obtain an IP address: Auto

----End

The device connects to the internet successfully when the **Status** is displayed as networked.

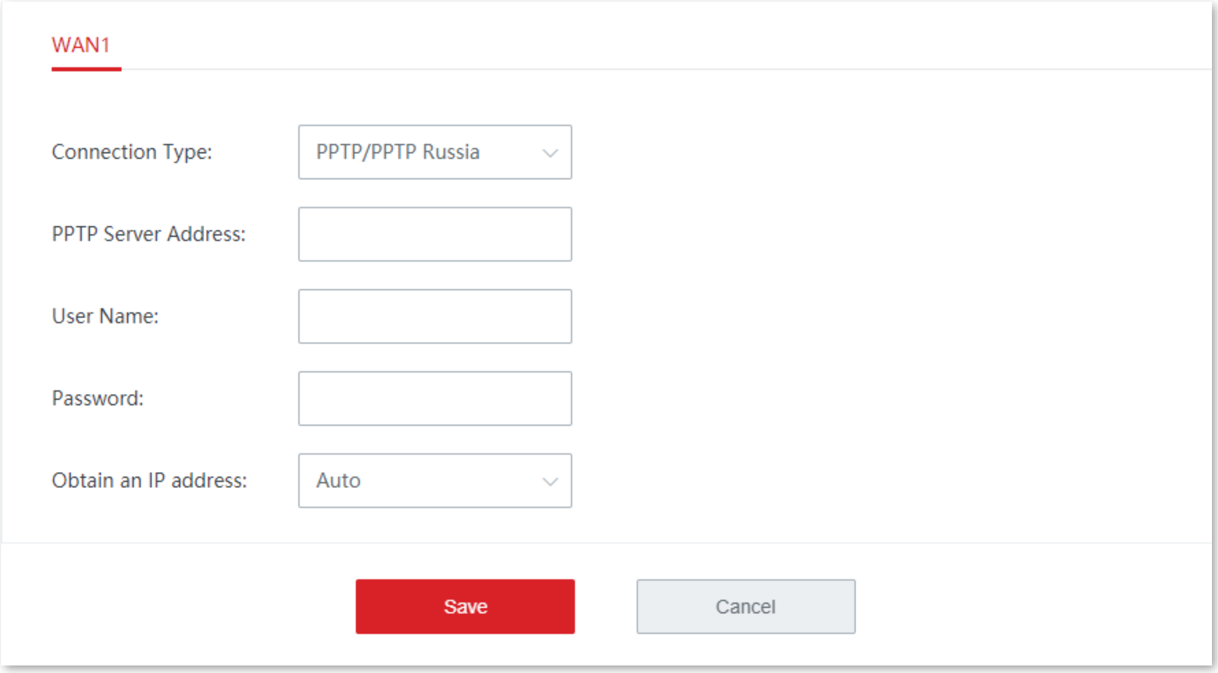
Tip

If you fail to access the internet, please try the following solutions:

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

PPTP/PPTP Russia

1. Click **Internet Settings** to enter the page.
2. Set **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**.



WAN1

Connection Type: PPTP/PPTP Russia

PPTP Server Address:

User Name:

Password:

Obtain an IP address: Auto

----End

The device connects to the internet successfully when the **Status** is displayed as networked.

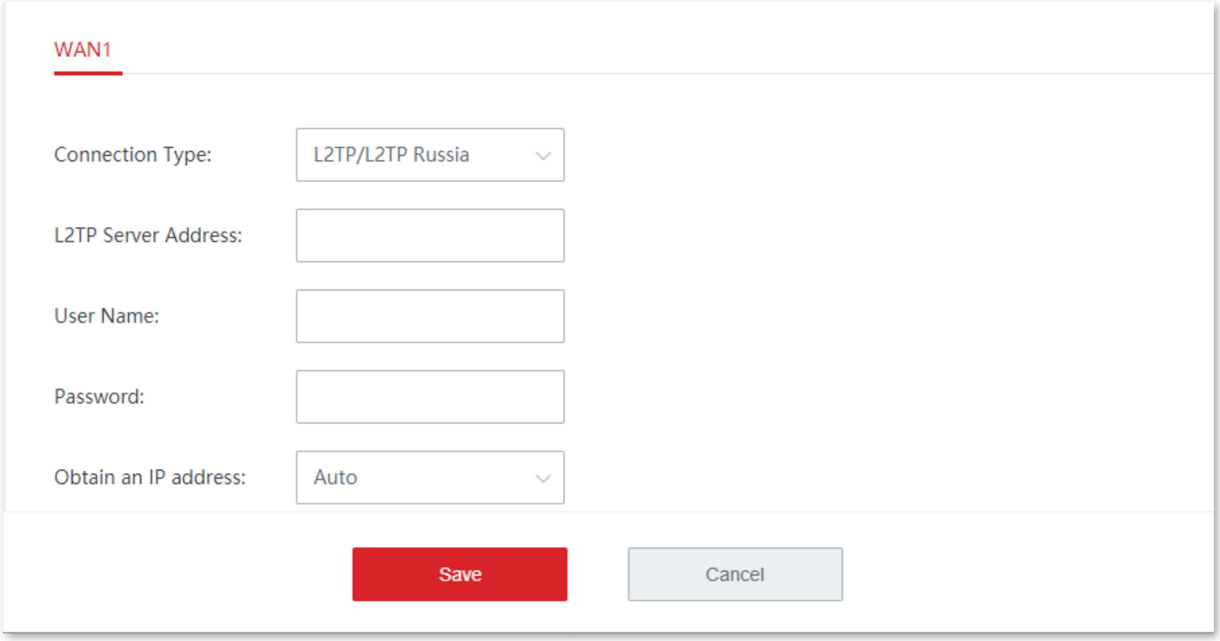
Tip

If you fail to access the internet, please try the following solutions:

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

L2TP/L2TP Russia

1. Click **Internet Settings** to enter the page.
2. Set **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**.



WAN1

Connection Type: L2TP/L2TP Russia

L2TP Server Address:

User Name:

Password:

Obtain an IP address: Auto

----End

Wait for the device to complete rebooting. The device connects to the internet successfully when the **Status** is displayed as networked.

Tip

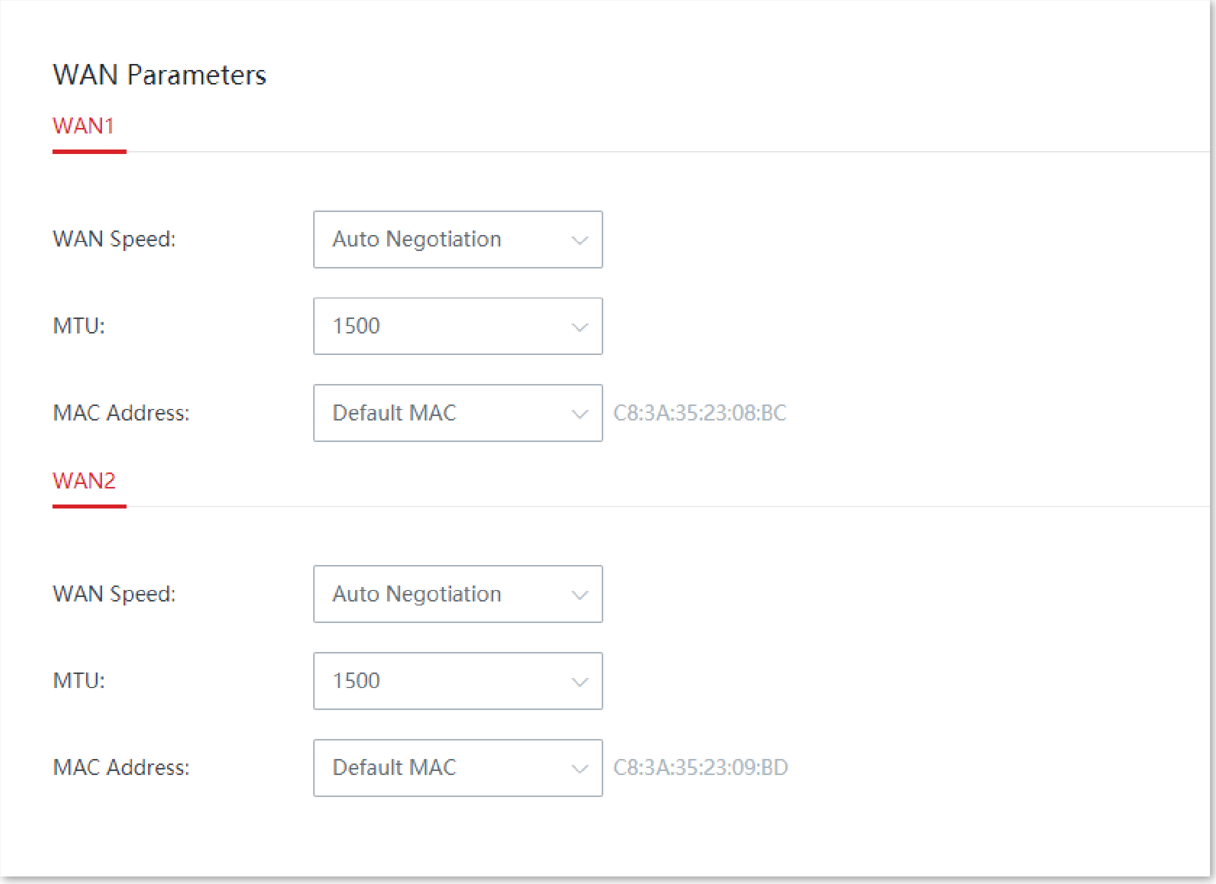
If you fail to access the internet, please try the following solutions:

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

3.2.2 WAN parameters

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

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



WAN Parameters

WAN1

WAN Speed: Auto Negotiation

MTU: 1500

MAC Address: Default MAC C8:3A:35:23:08:BC

WAN2

WAN Speed: Auto Negotiation

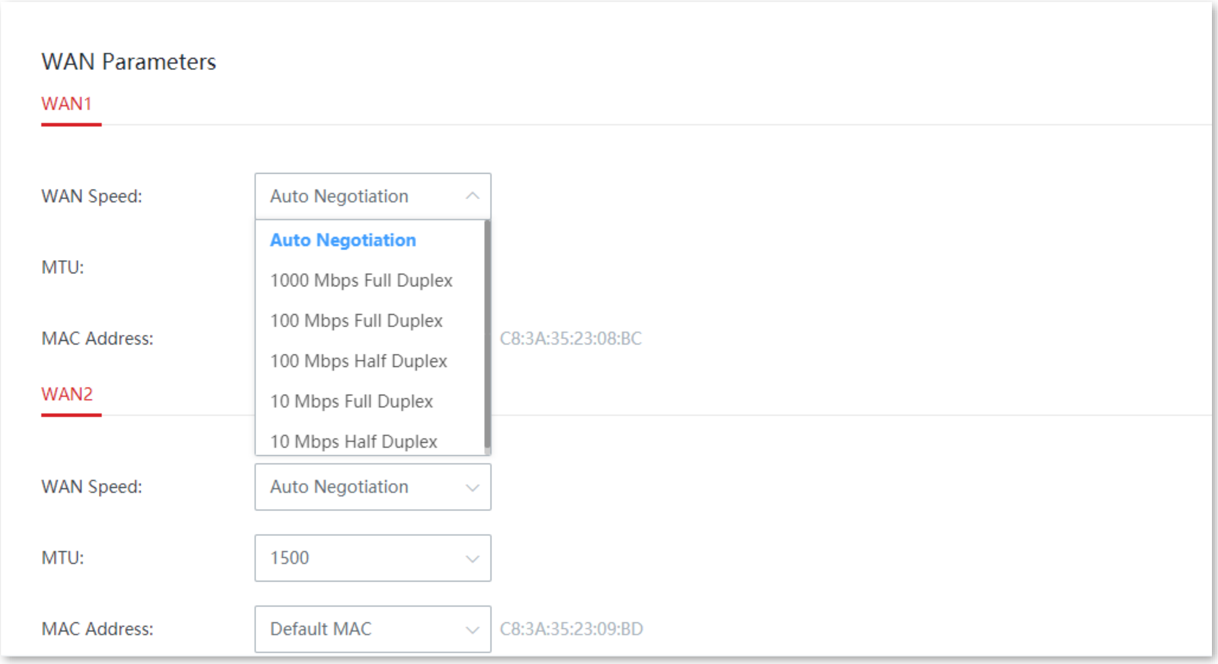
MTU: 1500

MAC Address: Default MAC C8:3A:35:23:09:BD

WAN speed

By default, the WAN speed of cable-free nodes is set to **Auto Negotiation**, which is appropriate for almost all cases. If the WAN port is properly connected and the Ethernet cable is not damaged, but in the Internet Settings module, the WAN port is still in grey color. In this case, you can change the WAN speed to **10 Mbps Full Duplex** or **10 Mbps Half Duplex** to fix the problem.

Otherwise, you are recommended to retain the default option **Auto Negotiation**.



WAN Parameters

WAN1

WAN Speed: Auto Negotiation

MTU:

MAC Address: C8:3A:35:23:08:BC

WAN2

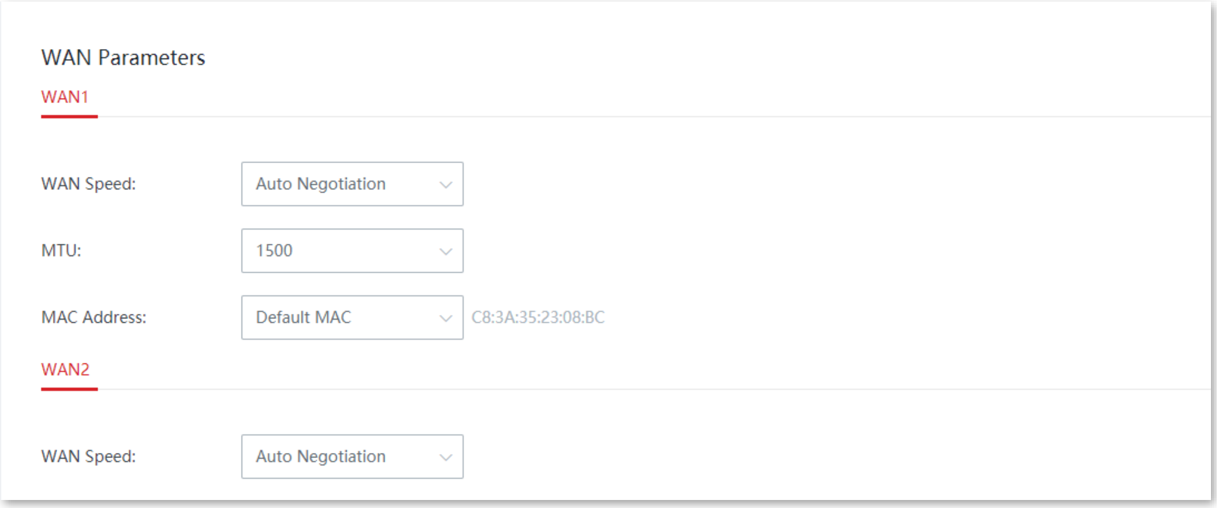
WAN Speed: Auto Negotiation

MTU: 1500

MAC Address: Default MAC C8:3A:35:23:09:BD

MTU

MTU is abbreviated for Maximum Transmission Unit. It specifies the maximum size of a packet that can be transmitted by a network device. If your connection type is PPPoE or PPPoE Russia, the default MTU value is 1492. If your connection type is Static IP or Dynamic IP, the default MTU value is 1500.



WAN Parameters

WAN1

WAN Speed: Auto Negotiation

MTU: 1500

MAC Address: Default MAC C8:3A:35:23:08:BC

WAN2

WAN Speed: Auto Negotiation

In general, it is recommended to retain the default option for the MTU value unless you encounter the following conditions:

- You can neither access some websites nor open security sites (such as online banking websites or PayPal).

– You can neither send nor receive Emails, or access servers such as FTP and POP servers.

In this case, you can try gradually reducing the MTU value (recommended range: 1400 to 1500) to fix the problem.

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

MAC address

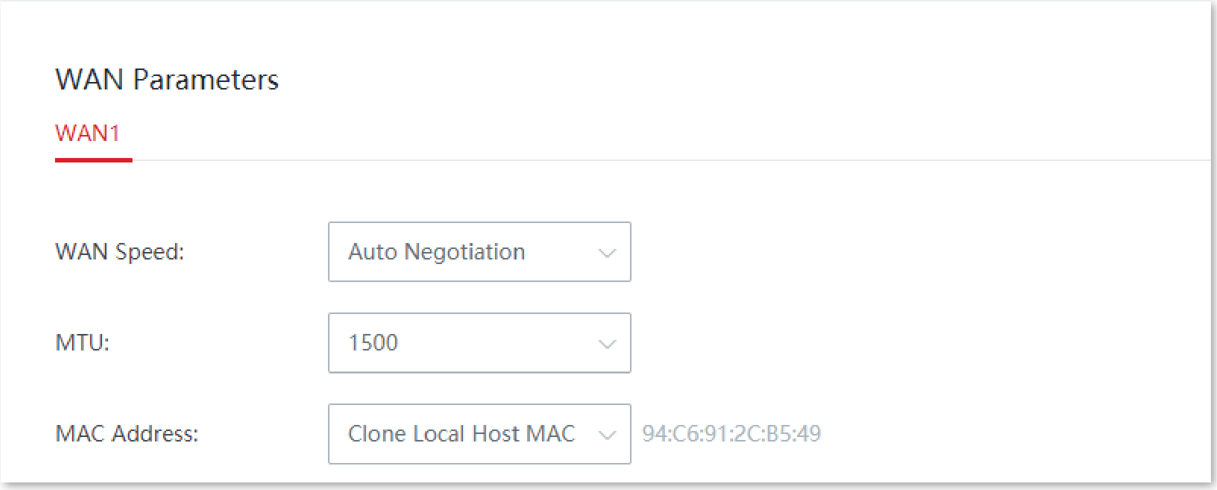
If the device still fails to access the internet after you completed internet settings configurations, probably the ISP bound the internet account with a MAC address (physical address). In this case, you can try MAC address cloning (method 1 or method 2) to fix the problem.

Note

Please clone the MAC address of the computer or the MAC address of the WAN port of the router on which you set up the dial up internet connection.

Method 1: Use the computer on which you set up the dial up internet connection for cloning

1. Use an Ethernet cable to connect the computer on which you set up the dial up internet connection to the cable-free network.
2. Start a web browser on the computer, and visit **192.168.5.1**.
3. Log in to the web UI of the cable-free node (router mode) and navigate to **Internet Settings** > **WAN Parameters**.
4. Select **Clone Local Host MAC** for **MAC Address**.
5. Click **Save**.



WAN Parameters

WAN1

WAN Speed: Auto Negotiation

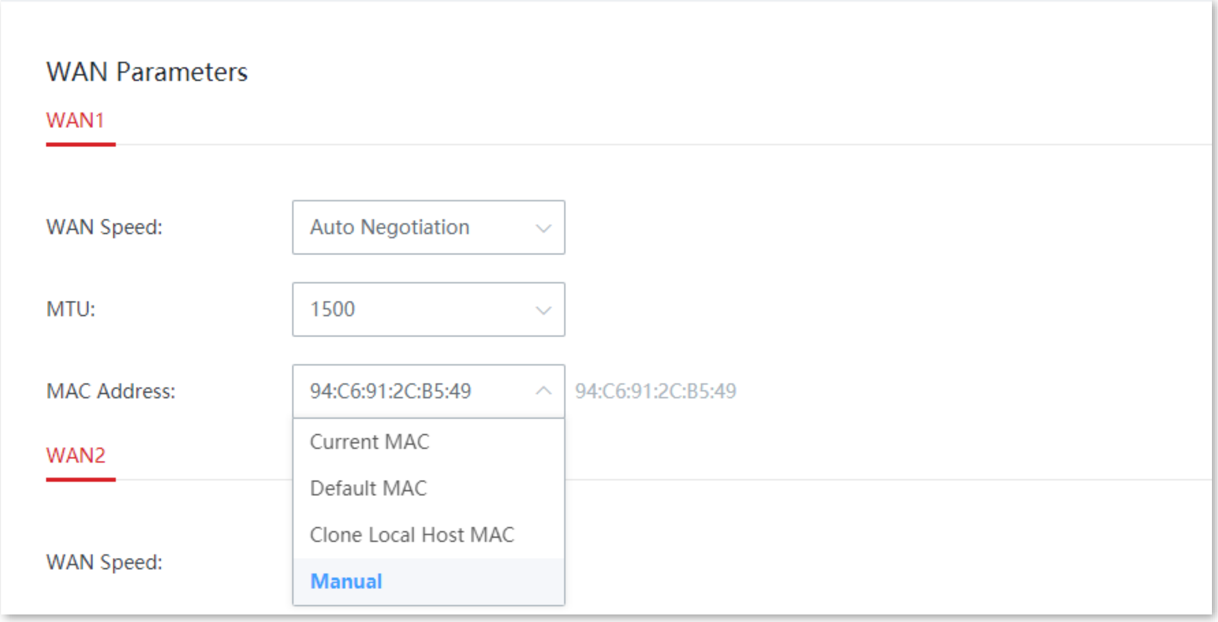
MTU: 1500

MAC Address: Clone Local Host MAC 94:C6:91:2C:B5:49

----End

Method 2: Use another device for cloning

1. Record the correct MAC address.
2. Log in to the web UI of the cable-free node (router mode) and navigate to **Internet Settings** > **WAN Parameters**.
3. Click the **MAC Address** drop-down list and select **Manual**, enter the correct MAC address ("the MAC address of the computer which directly connects to the Ethernet jack and has internet availability" or "the MAC address of the WAN port of the router on which you set up the dial up internet connection").
4. Click **Save**.



WAN Parameters

WAN1

WAN Speed: Auto Negotiation

MTU: 1500

MAC Address: 94:C6:91:2C:B5:49 94:C6:91:2C:B5:49

WAN2

WAN Speed:

----End

Tip

If you want to restore the MAC address of the WAN port to the default MAC address, navigate to **Internet Settings** > **WAN Parameters**, click the **MAC Address** drop-down list, select **Default MAC**, and click **Save**.

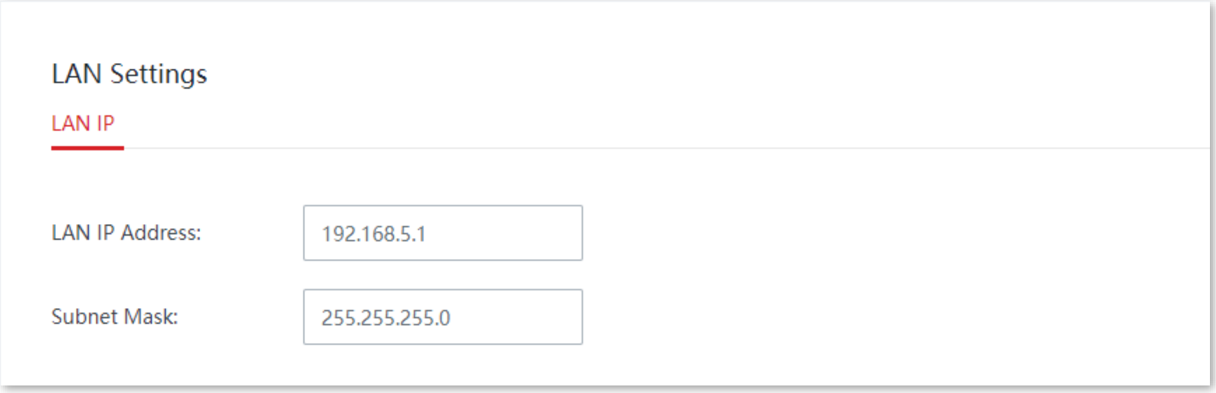
3.2.3 LAN settings

On the **Internet Settings** > **LAN Settings** page, you can check the LAN IP configuration of the device and configure the DHCP server.

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

LAN IP

The LAN IP is the LAN IP address of the node and also the management IP address of the node. The default LAN IP is 192.168.5.1 and the subnet mask is 255.255.255.0



LAN Settings

LAN IP

LAN IP Address: 192.168.5.1

Subnet Mask: 255.255.255.0

Generally, you do not need to modify LAN settings unless an IP address conflict occurs. For example, if the WAN port IP address obtained by the node and its LAN port IP address are on the same network segment; or, the IP address of another device in the LAN is also 192.168.5.1.

After the LAN port IP address is modified, you will be automatically redirected to the login page. If not, please verify that the IP address of the management host is set to **Obtain an IP address automatically** and **Obtain DNS server address automatically**, and then try again to access the new LAN port IP address.

Tip

If the new LAN port IP address is not on the same network segment as the original LAN port IP address, the system will automatically match and modify the DHCP address pool to make it on the same network segment as the new LAN port IP address.

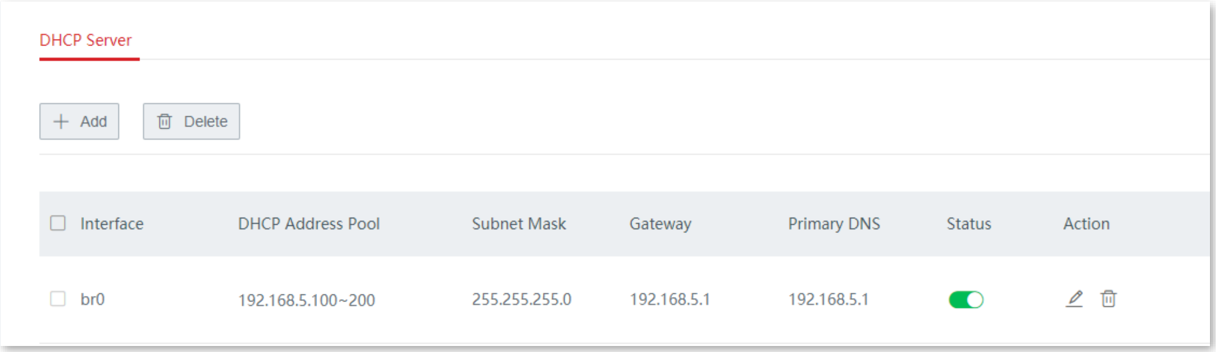
Parameter description

Parameter	Description
LAN IP Address	It specifies the IP address of the LAN port of the device, which can be used to log in to its web UI. The default IP address is **192.168.5.1**.
Subnet Mask	It specifies the subnet mask of the LAN port of the device. The default subnet mask is **255.255.255.0**.

DHCP server

DHCP server can automatically assign IP address, subnet mask, gateway address, DNS and other Internet information to user devices of the LAN.

If you disable DHCP server, you need to manually configure the IP address information on the LAN device to access the Internet. Please keep the DHCP server enabled if there is no special case.



□ Interface	DHCP Address Pool	Subnet Mask	Gateway	Primary DNS	Status	Action
□ br0	192.168.5.100~200	255.255.255.0	192.168.5.1	192.168.5.1	●	✎ 🗑

Click **+ Add** to add a DHCP server and click **Delete** to delete a DHCP server.

Parameter description

Parameter	Description
Interface	It specifies the interface of the DHCP server.
Start IP	It specifies the start IP address of the DHCP address pool. By default, it is 192.168.5.31.
End IP	It specifies the end IP address of the DHCP address pool. By default, it is 192.168.5.200.
DHCP Address Pool	It specifies the address range of the DHCP address pool (the assignable addresses).
Subnet Mask	It specifies the subnet mask assigned by the DHCP server to clients.
Gateway	It specifies the default gateway address assigned by the DHCP server to clients.
Primary DNS	It specifies the primary DNS server IP address assigned by the DHCP server to clients. The cable-free node (router mode) supports DNS proxy function, and the primary DNS address is the LAN IP address of the node by default. Tip Generally, you are recommended to keep the default setting. If it is necessary to change the default setting, please set this parameter to a correct DNS server IP address or DNS proxy IP address, to enable clients to access the internet.
Secondary DNS	It specifies the secondary DNS server IP address assigned by the DHCP server to clients. This parameter is optional. If it is empty, the DHCP server does not assign it to clients.
Lease Time	It specifies the validity period of the assigned IP address, which is 30 minutes by default. 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.
Status	It specifies the status of the DHCP server. You can toggle it on or off as required.
Action	It specifies the operations you can perform on the DHCP server. ✎: Click it to edit the DHCP server. 🗑 : Click it to delete the DHCP server. The default DHCP server cannot be deleted.

3.2.4 VLAN settings

Overview

VLAN, abbreviated for Virtual Local Area Network, is a technology which divides LAN devices into different network segments logically rather than physically to create virtual work groups. It is used to divide the work stations in the switch-formed network into logical groups among which broadcast is isolated. Work stations in a group belong to a same VLAN and can communicate like they are connected to a same network segment no matter where they physically are. However, due to the isolation of broadcast packets, the VLAN cannot communicate with each other and packets must be forwarded by a router or other layer 3 packet forwarding devices.

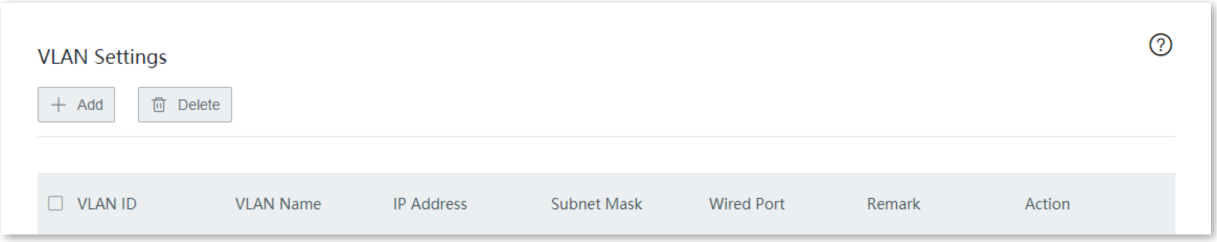
Compared with the traditional Ethernet, VLAN has the following advantages:

- Control the range of broadcast domain: Broadcast messages in the LAN are restricted in a VLAN, which saves bandwidth and improves network processing capability.
- Enhance the security of the LAN: Because messages are isolated in the data link layer by the broadcast domain divided by VLAN, the host in each VLAN cannot directly communicate with each other and messages have to be forwarded by a router or other layer 3 network devices.
- Create virtual work groups freely: VLAN can create virtual work groups irrespective of physical network range. A user can still access the network without having to change network configurations as long as he or she remains within the virtual work group even if his or her physical location changed.

Add VLAN

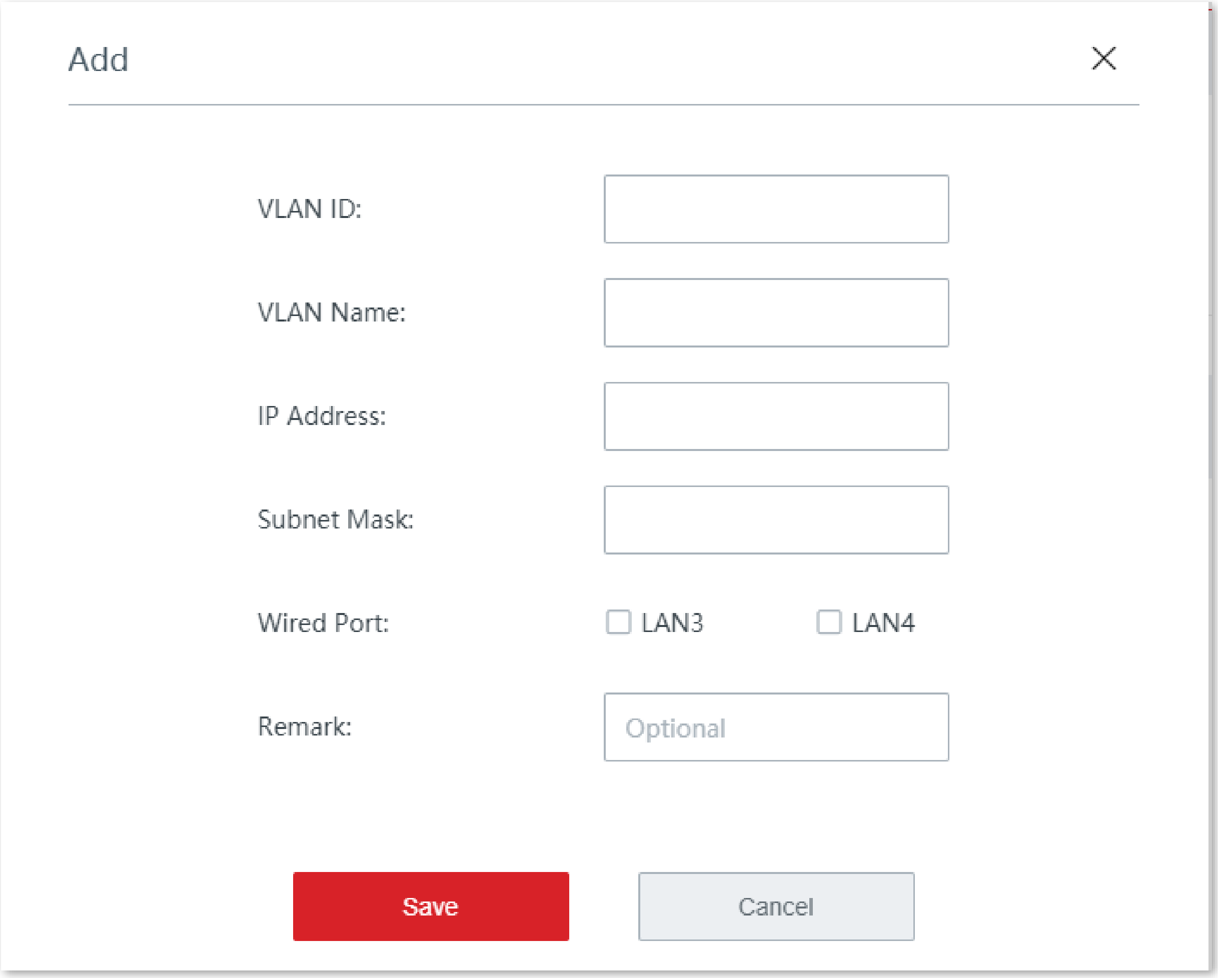
The cable-free device supports IEEE 802.1q VLAN, which can be used in the network environment where QVLAN is divided.

1. Click **Internet Settings** > **VLAN Settings**.
2. Click **+ Add**.



□ VLAN ID	VLAN Name	IP Address	Subnet Mask	Wired Port	Remark	Action

3. Configure a VLAN rule in the pop-up window.
4. Click **Save**.

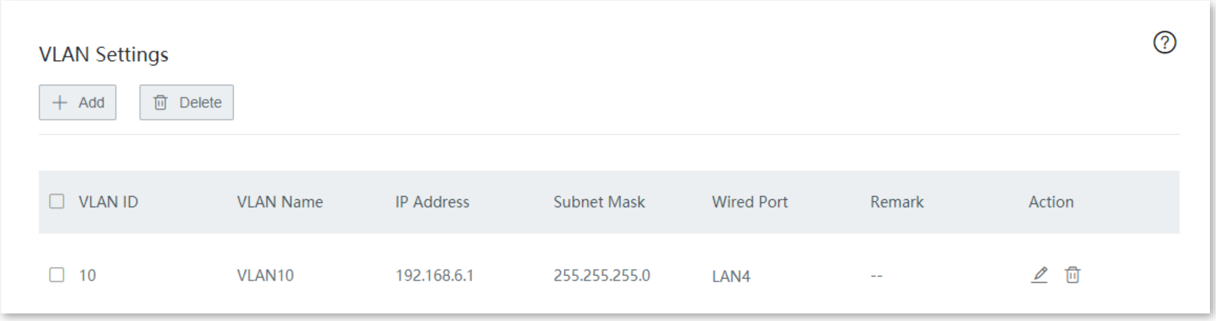


----End

Parameter description

Parameter	Description
VLAN ID	It specifies the identifier of the VLAN, which is used to divide separate VLANs in a LAN. Different IDs stand for different VLANs.
VLAN Name	It specifies the name of the VLAN interface.
IP Address	It specifies the IP address of the VLAN interface and devices connected to the interface can use this IP address to log in to the web UI of the router.
Subnet Mask	It specifies the subnet mask of the VLAN interface.
Wired Port	It specifies the physical port supported by the VLAN.
Remark	It specifies the remarks of the VLAN.
Action	It specifies the operations you can perform on the rule. ✎: Click it to edit the rule. 🗑 : Click it to delete the rule.

After the VLAN is added successfully, you can view the added VLAN on the **Internet Settings** > **VLAN Settings** page. See the following figure.



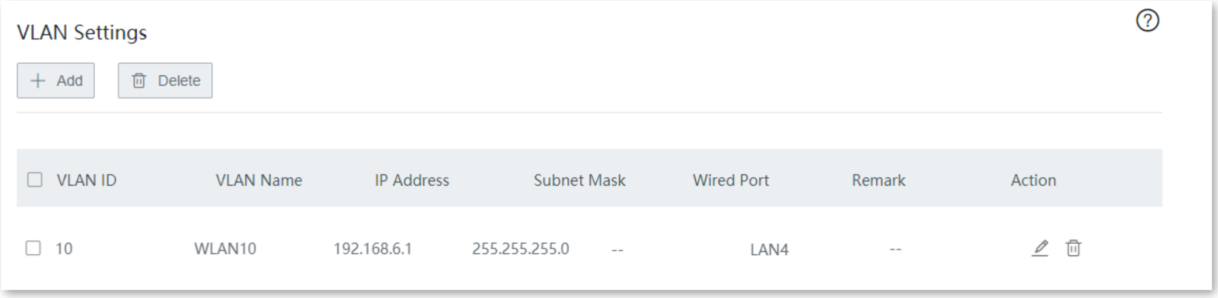
VLAN Settings

☐ VLAN ID	VLAN Name	IP Address	Subnet Mask	Wired Port	Remark	Action
☐ 10	VLAN10	192.168.6.1	255.255.255.0	LAN4	--	✎ 🗑

Besides, you need to set a DHCP server for the VLAN, so as to enable clients under the VLAN to automatically obtain IP address from the node to access the internet.

Modify VLAN

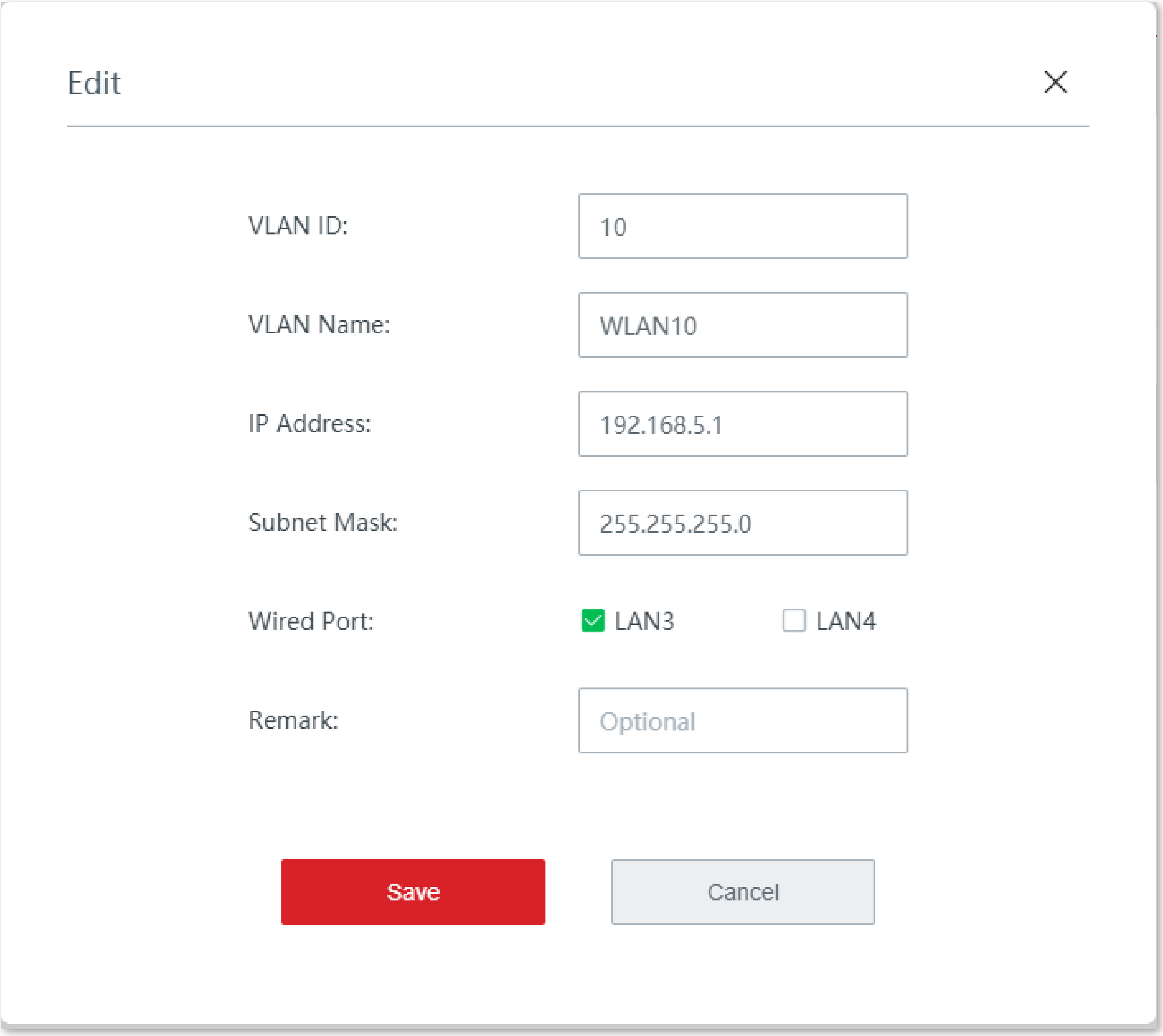
1. Click **Internet Settings** > **VLAN Settings**.
2. Locate the VLAN rule to be modified and click ✎.



VLAN Settings

☐ VLAN ID	VLAN Name	IP Address	Subnet Mask	Wired Port	Remark	Action
☐ 10	WLAN10	192.168.6.1	255.255.255.0 --	LAN4	--	✎ 🗑

3. Modify parameters.
4. Click **Save**.



Edit

VLAN ID: 10

VLAN Name: WLAN10

IP Address: 192.168.5.1

Subnet Mask: 255.255.255.0

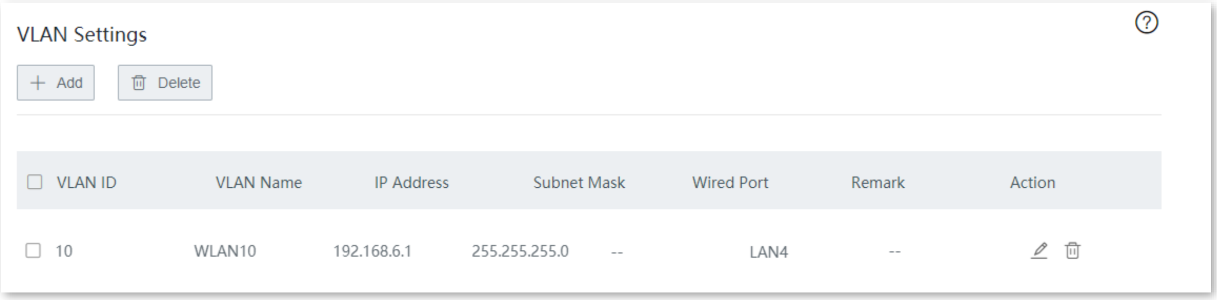
Wired Port: ☑ LAN3 □ LAN4

Remark: Optional

----End

Delete VLAN

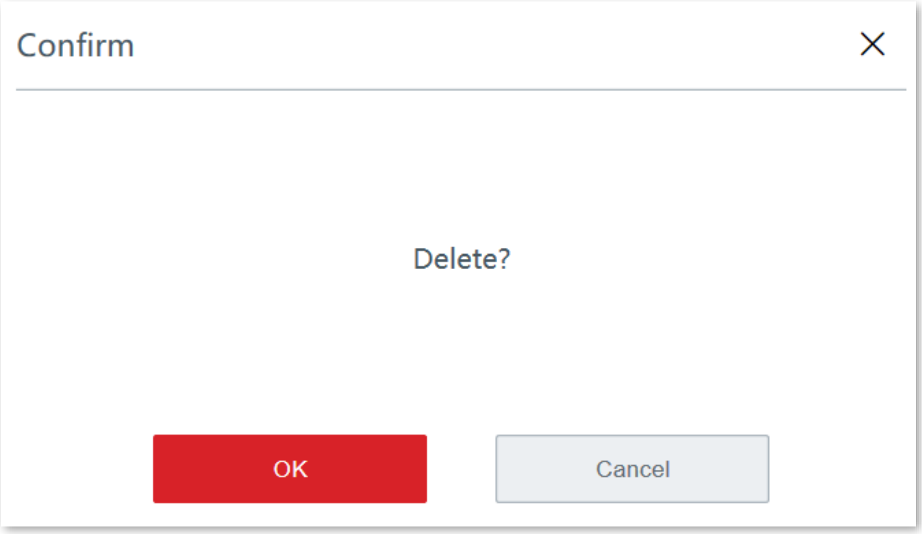
1. Click **Internet Settings** > **VLAN Settings**.
2. Locate the VLAN rule to be deleted and click 🗑.



VLAN Settings

□ VLAN ID	VLAN Name	IP Address	Subnet Mask	Wired Port	Remark	Action
□ 10	WLAN10	192.168.6.1	255.255.255.0 --	LAN4	--	✎ 🗑

3. Click **OK** after confirming the pop-up reminder.



Confirm

Delete?

----End

3.3 Wireless

On this page, you can change the wireless configurations of the cable-free primary node.

The device supports tri-band WiFi networks at most. By default, the device adopts wireless networking with one 5 GHz band exclusively used to establish a cable-free link, and the 2.4 GHz band and the other 5 GHz band used for client access.

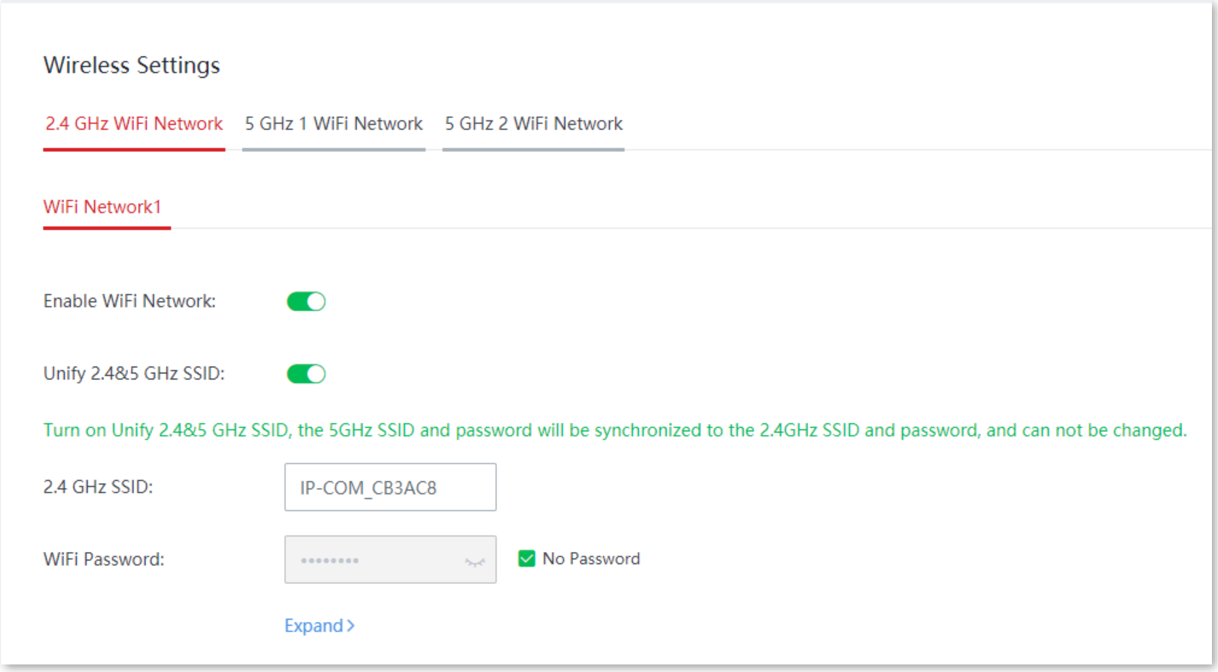
3.3.1 Wireless settings

On this page, you can configure the basic wireless parameters, including enable/disable WiFi networks, change the WiFi network name, set the WiFi password and other parameters.

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

Tip

The 2.4 GHz WiFi network 1 SSID (WiFi name) and WiFi password have been set as the default SSID policy. The configuration of 2.4 GHz WiFi network 1 SSID and WiFi password will be synchronized to other nodes applied with the default SSID policy (By default, all secondary nodes are applied with the default SSID policy in the cable-free network).



Wireless Settings

2.4 GHz WiFi Network | 5 GHz 1 WiFi Network | 5 GHz 2 WiFi Network

WiFi Network1

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_CB3AC8

WiFi Password: •••••••• ☑ No Password

Expand >

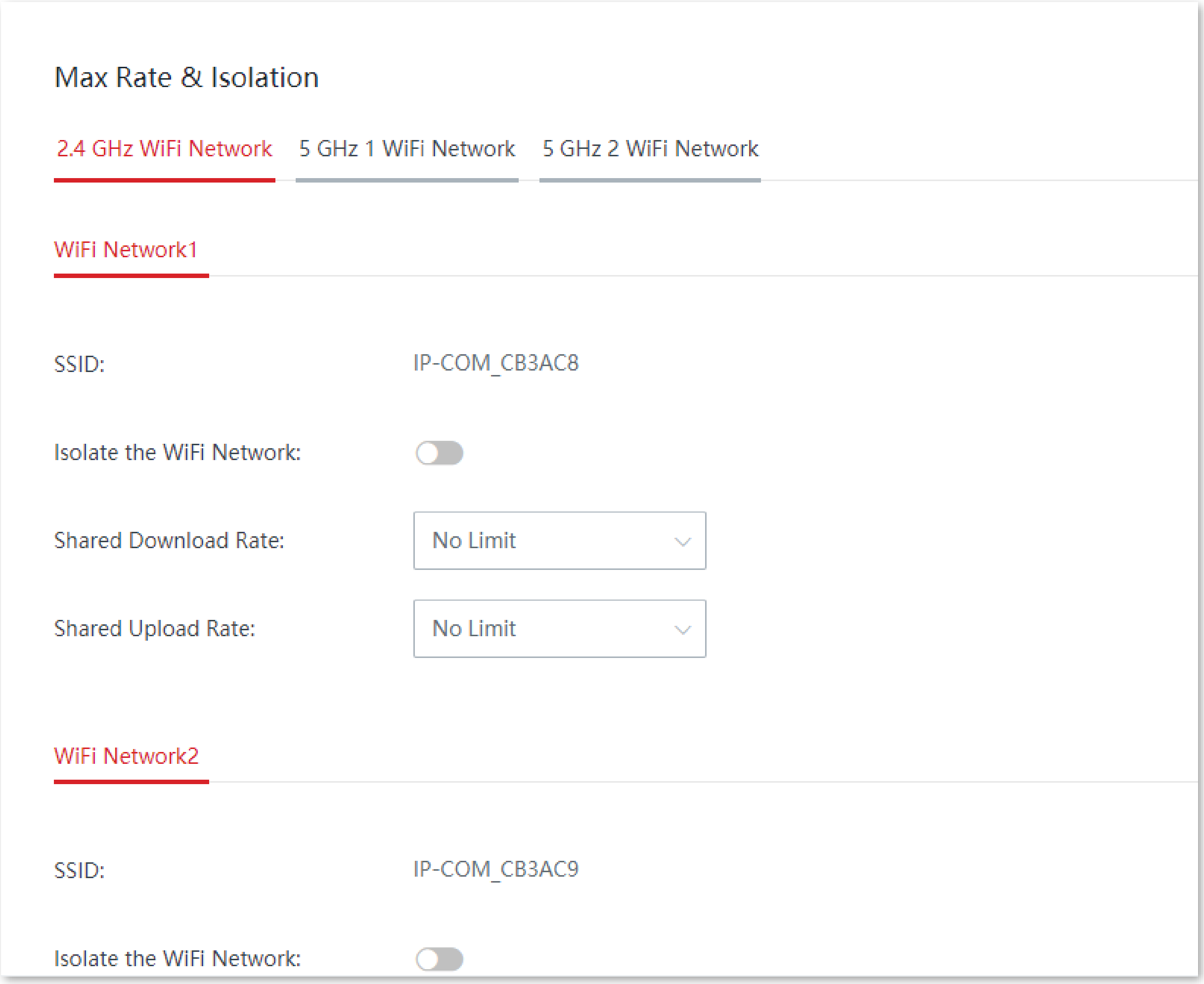
Parameter description

Parameter	Description
WiFi Network1/2/3/4	Every band of the node supports 4 WiFi networks and only WiFi network 1 is enabled by default.
Enable WiFi Network	It is used to enable/disable the corresponding WiFi network.
Unify 2.4&5 GHz SSID	After this function is enabled, the 2.4 GHz WiFi network shares the same SSID (WiFi network name) and WiFi password with the 5 GHz WiFi network, and the parameters of the 5 GHz WiFi network on the **Wireless Settings** and **Max Rate & Isolation** module automatically synchronize with those of the 2.4 GHz WiFi network and cannot be changed separately. When a wireless client connects to the cable-free device, it will be automatically connected to the WiFi network with the best network quality. Tip If there are clients in your network which supports only the 2.4 GHz WiFi network, to guarantee these devices can normally connect to the WiFi network as well, you are recommended not to enable this function.
SSID	It specifies the WiFi network name of the corresponding WiFi network.
WiFi Password	It specifies the password of the corresponding WiFi network. For WiFi network security, it is strongly recommended that you set a WiFi password.
No Password	It specifies that no WiFi password is set. Under such circumstances, the corresponding WiFi network is open.
Hide SSID	After this function is enabled, the SSID will be hidden and will not appear in the available network list of clients (such as smartphones), which enhances the security of the WiFi network. If you want to connect to a hidden WiFi network, manually enter the SSID on your client.
Max. Clients	It specifies the maximum number of clients allowed to connect to the WiFi network. If this value is reached, new clients cannot connect to the WiFi network unless some clients are disconnected.
VLAN ID	It specifies the VLAN ID of the WiFi network.

3.3.2 Max rate & isolation

On this page, you can configure the maximum rate and isolation. This function is disabled by default.

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



Max Rate & Isolation

2.4 GHz WiFi Network | 5 GHz 1 WiFi Network | 5 GHz 2 WiFi Network

WiFi Network1

SSID: IP-COM_CB3AC8

Isolate the WiFi Network:

Shared Download Rate: No Limit

Shared Upload Rate: No Limit

WiFi Network2

SSID: IP-COM_CB3AC9

Isolate the WiFi Network:

Parameter description

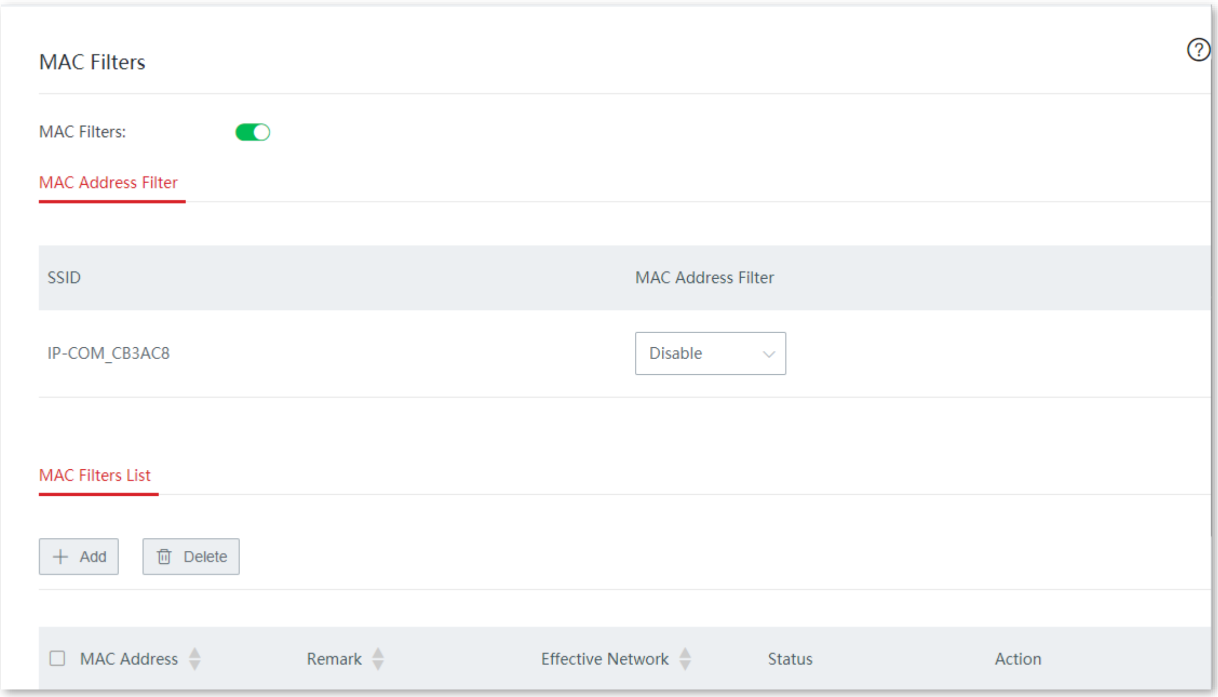
Parameter	Description
SSID	It specifies the WiFi network name of the node.
Isolate the WiFi Network	After this function is enabled, clients connected to this WiFi network cannot communicate with clients connected to other WiFi networks of the cable-free system, thus enhancing the security of WiFi networks.
Shared Upload/Download Rate	It specifies the maximum upload/download rate shared by clients connected to the WiFi network. **No Limit** means to set no limit on the maximum upload/download rate of the WiFi network.
No Access to LAN	This function is valid only for **WiFi Network2/3/4**. After this function is enabled, clients connected to the WiFi network can access only the internet, and can access neither the LAN nor the web UI of the node.

3.3.3 MAC filters

Overview

On this page, you can allow or forbid WiFi network access from specified clients by setting MAC filter rules. By default, this function is disabled.

Click **Wireless** > **MAC Filters** to enter the page. The following displays the page when the function is enabled.



MAC Filters

MAC Filters: ●

MAC Address Filter

SSID	MAC Address Filter
IP-COM_CB3AC8	Disable

MAC Filters List

□ MAC Address	Remark	Effective Network	Status	Action

Click **+ Add** to add a MAC filters rule and click **Delete** to delete a MAC filters rule.

Parameter description

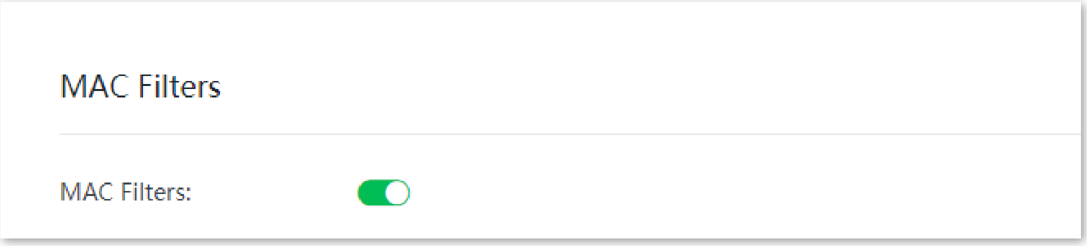
Parameter	Description	
MAC Filters	○ specifies the MAC filters function is disabled and ● specifies the MAC filters function is enabled.	
MAC Address Filter	SSID	It specifies the name of the enabled WiFi network of the node. Tip By default, the SSID of 2.4 GHz WiFi network, 5 GHz 1 WiFi network, and 5 GHz 2 WiFi network is the same. Therefore, only one SSID is displayed by default.

Parameter		Description
	MAC Address Filter	It specifies the MAC address filter mode. – **Disable**: It specifies that the MAC address filter function is not enabled on the WiFi network and all wireless clients are allowed to connect to the WiFi network. – **Only Allow**: It specifies that only the wireless clients in the **MAC Filters List** are allowed to connect to the WiFi network. – **Only Forbid**: It specifies that only the wireless clients in the **MAC Filters List** are forbidden to connect to the WiFi network. Other wireless clients can connect to the WiFi network.
MAC Filters List	MAC Address	It specifies the MAC address of the wireless client.
	Remark	It specifies the remarks of the MAC address.
	Effective Network	It specifies the WiFi network on which the rule takes effect.
	Status	It specifies the status of the rule. You can enable or disable the rule as required.
	Action	It specifies the operations you can perform on the rule. ✎: Click it to edit the rule. 🗑 : Click it to delete the rule.

Set MAC filters rule

Enable the MAC filters function

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

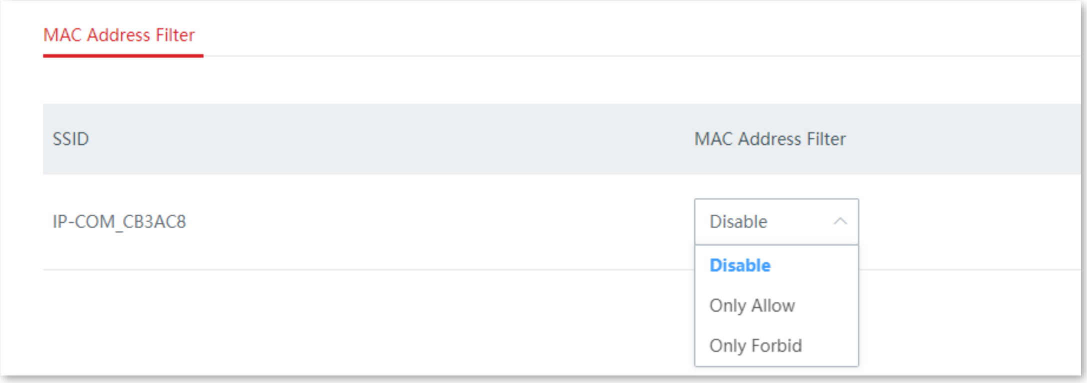


MAC Filters

MAC Filters: ●

Set MAC address filter mode

1. Select the appropriate **MAC Address Filter** mode as required.
2. Click **Save**.



SSID	MAC Address Filter
IP-COM_CB3AC8	Disable

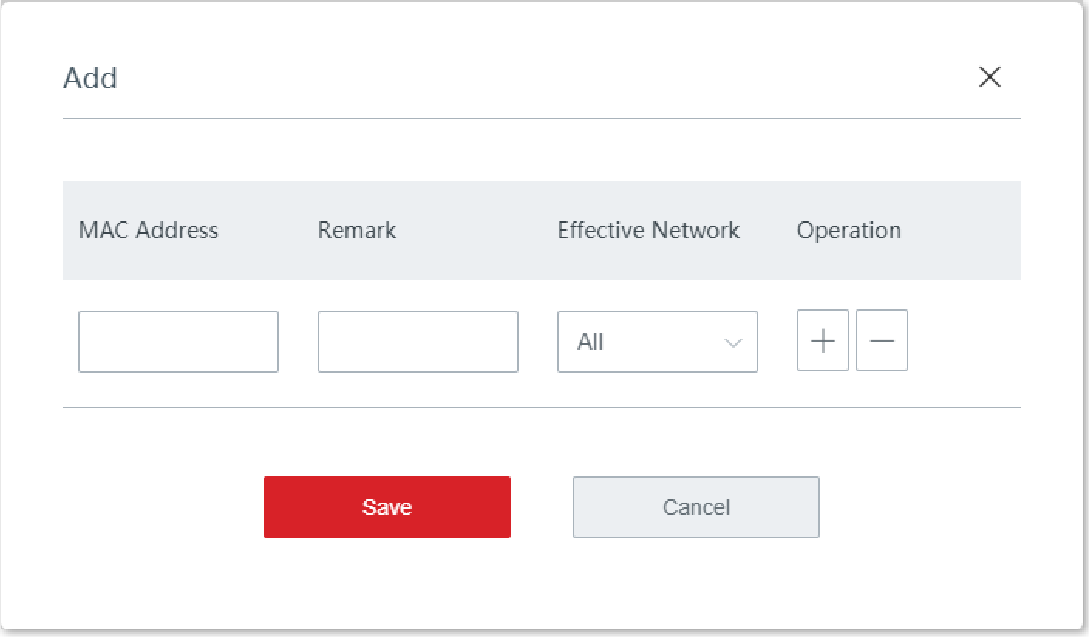
Add a MAC filter rule

1. Click **+ Add** to enter the configuration page.
2. Add a MAC filter rule.
   (1) Enter the MAC address of the wireless client on which the MAC filter rule applies.
   (2) (Optional) Set a remark for the MAC address.
   (3) Select a WiFi network on which the MAC filter rule takes effect.

Tip

Click + to add a MAC filter rule and click – to delete an unsaved MAC filter rule.

3. Click **Save**.



MAC Address	Remark	Effective Network	Operation
		All	+ –

----End

You can check the newly added MAC filter rule on the **Wireless** > **MAC Filters** page.

Example of configuring MAC filters rule

Network requirement

An enterprise uses cable-free devices to set up a network.

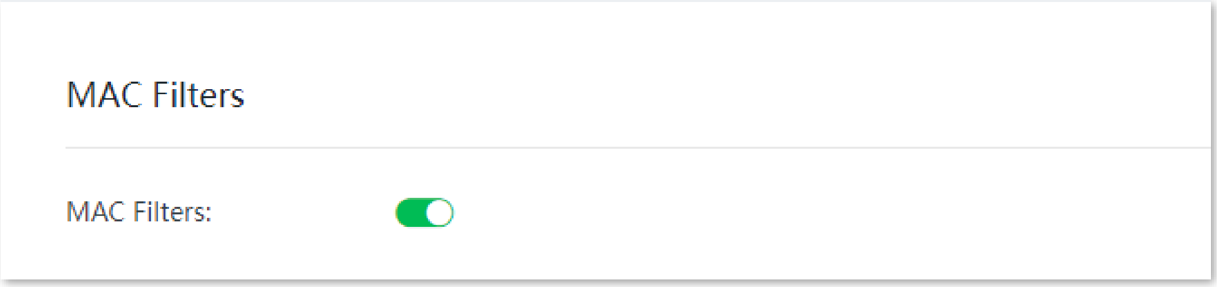
Requirement: Only a procurement personnel is allowed to connect to the WiFi network (Procurement) of the cable-free primary node for internet access.

Solution

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

Configuration procedures

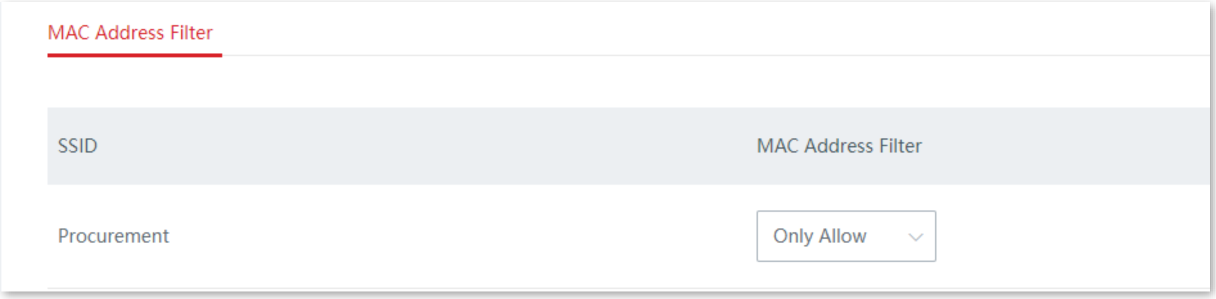
1. Click **Wireless** > **MAC Filters**.
2. Enable the MAC filters function.
   (1) Toggle on **MAC Filters**.
   (2) Click **Save**.



MAC Filters

MAC Filters:

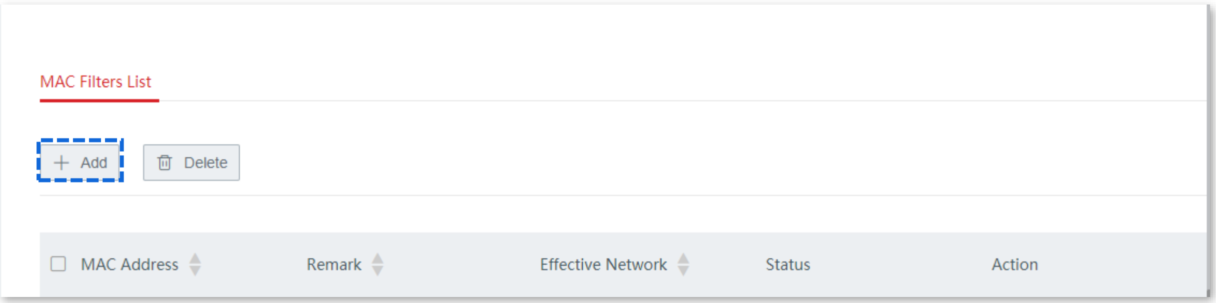
3. Set the MAC address filter mode.
   (1) Select a **MAC Address Filter** mode for the WiFi network "Procurement", which is "**Only Allow**" in this example.
   (2) Click **Save**.



MAC Address Filter

SSID	MAC Address Filter
Procurement	Only Allow

4. Add a MAC filter rule.
   (1) Click **+ Add**.

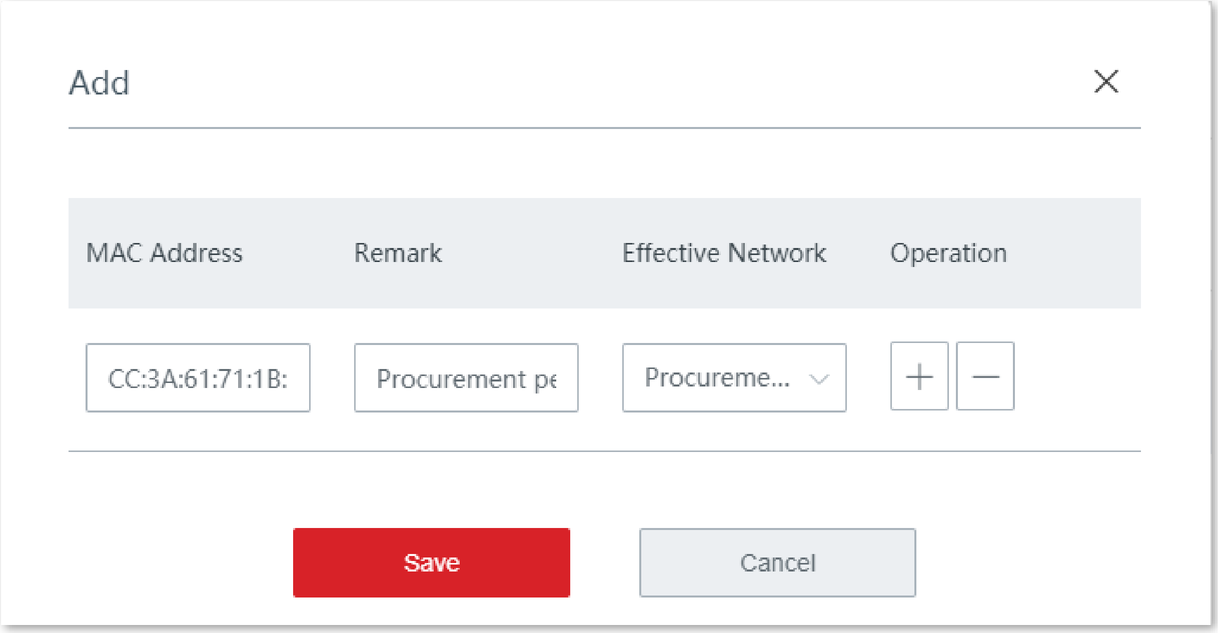


□ MAC Address	Remark	Effective Network	Status	Action

(2) On the **Add** configuration window, set the following parameters:

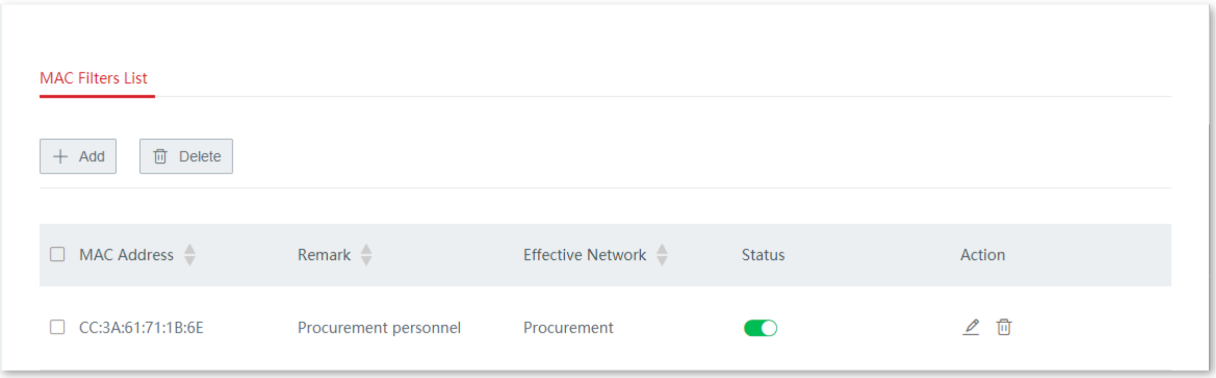
- Enter **CC:3A:61:71:1B:6E** in the **MAC Address** input box.
- Enter **Procurement personnel** in the **Remark** input box.
- Select **Procurement** from the drop-down list of **Effective Network**.

(3) Click **Save**.



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

Added successfully. See the following figure.



□ MAC Address	Remark	Effective Network	Status	Action
□ CC:3A:61:71:1B:6E	Procurement personnel	Procurement	●	✎ 🗑

----End

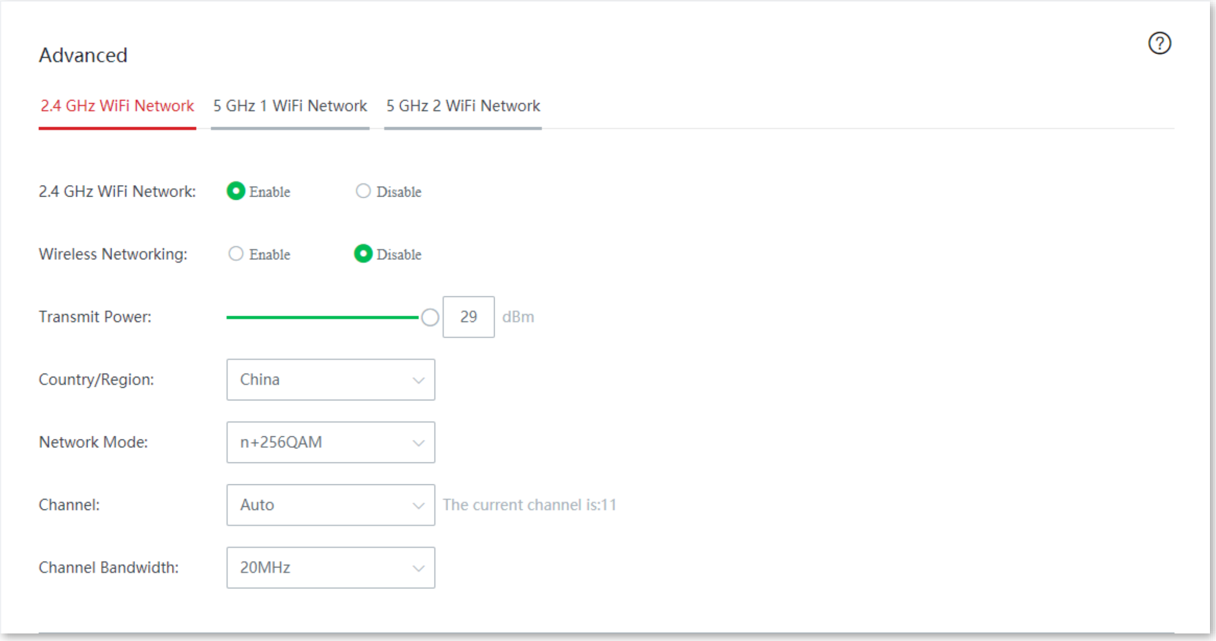
Verification

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

3.3.4 Advanced

On this page, you can set the advanced wireless settings, such as transmit power, network mode, channel, and channel bandwidth.

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



Advanced

2.4 GHz WiFi Network: ● Enable ○ Disable

Wireless Networking: ○ Enable ● Disable

Transmit Power: 29 dBm

Country/Region: China

Network Mode: n+256QAM

Channel: Auto The current channel is:11

Channel Bandwidth: 20MHz

Parameter description

Parameter	Description
2.4 GHz/5 GHz WiFi Network	It is used to enable or disable the WiFi function of the corresponding band.
Wireless Networking	After this function is enabled, the router can use this band to perform wireless networking. Note If the wireless networking function is enabled on more than one band, the router will perform load balancing and network accordingly; therefore, the networking performance of the cable-free system is improved, but the capacity is reduced. Please choose the appropriate band to enable the wireless networking function. Below are some suggestions: – **Capacity-oriented**: Enable the function only on the 5 GHz 2 band. – **Coverage-oriented**: Enable the function on both the 2.4 GHz and 5 GHz 1 bands.
Transmit Power	It specifies the transmit power of the corresponding band. The higher the transmit power, the wider the WiFi coverage. However, an appropriate reduction of transmit power can help improve the performance and security of the WiFi network.
Country/Region	It specifies the country or region where the node is located. Please select the correct country or region.

Parameter	Description
Network Mode	It specifies the WiFi network mode of the corresponding band. Network modes of the 2.4 GHz WiFi network include 11b, 11g, 11b/g, 11b/g/n, and n+256QAM. By default, the router works in the n+256QAM mode. – **11b**: In this mode, only 802.11b wireless clients are allowed to access the 2.4 GHz WiFi network. – **11g**: In this mode, only 802.11g wireless clients are allowed to access the 2.4 GHz WiFi network. – **11b/g**: In this mode, 802.11b and 802.11g wireless clients can access the 2.4 GHz WiFi network. – **11b/g/n**: In this mode, wireless clients compliant with 802.11b or 802.11g and wireless clients working at 2.4 GHz and compliant with 802.11n can access the 2.4 GHz WiFi network. – **n+256QAM**: Wireless clients compliant with 802.11b or 802.11g and wireless clients working at 2.4 GHz and compliant with 802.11n can access the 2.4 GHz WiFi network. QAM, abbreviated for Quadrature Amplitude Modulation, is a modulation scheme that moderates amplitude on two orthogonal carriers. Using the orthogonality of sine wave and cosine wave, it moderates two signals at the same time, improving the modulation efficiency. In the n+256QAM network mode, the 256-QAM modulation mode compliant with the IEEE 802.11ac standard can be used under the IEEE 802.11n standard in the 2.4GHz band, which improves the single stream rate from 150 Mbps to 200 Mbps. Note: Such improvement can be realized only when the band is 2.4 GHz band, and the transmitting an d receiving ends both support the n+256QAM network mode. If any one end does not support n+256QAM, the single stream rate under the 2.4 GHz band is still 150 Mbps at most. Moreover, after the network mode is set to n+256QAM, the stability and anti-interference capability of the network will be reduced compared with the stability and anti-interference capability under other modes. Network modes of the 5 GHz WiFi network include 11a, 11ac, and 11a/n mixed. By default, the router works in the 11ac mode. – **11a**: In this mode, only 802.11a wireless clients are allowed to access the 5 GHz WiFi network. – **11ac**: In this mode, only 802.11ac wireless clients are allowed to access the 5 GHz WiFi network. – **11a/n mixed**: In this mode, wireless clients compliant with 802.11a and wireless clients working at 5 GHz and compliant with 802.11n can access the 5 GHz WiFi network.

Parameter	Description
Channel	It specifies the channel in which the wireless data is transmitted and received. The available channels are determined by the current country/region and wireless band. **Auto**: The node automatically detects the occupation rate of channels and selects the appropriate working channel accordingly. If connection drop, freeze or slow internet occurs frequently when you are using the WiFi network, you can try changing the working channel. You can check the channels with low occupation rate and little interference using software tools (such as WiFi analyzer).
Channel Bandwidth	It specifies the bandwidth of the working channel. A high channel bandwidth means a higher transmission rate, but the penetration capability is reduced and the transmission distance is shortened. – **20MHz**: The node uses the 20MHz channel bandwidth. – **40MHz**: The node uses the 40MHz channel bandwidth. – **20MHz/40MHz**: This channel bandwidth is available only for the 2.4 GHz only. The node automatically adjusts the channel bandwidth to 20MHz or 40MHz based on the surrounding environment. – **80MHz**: This channel bandwidth is available only for the 5 GHz only. The node uses the 80MHz channel bandwidth.
RSSI Threshold	It specifies the minimum wireless signal strength can be received by the band. Clients with a lower signal strength value cannot connect to the node. When there are multiple nodes in the surroundings, an appropriate RSSI value helps ensure wireless clients connects to the nodes with a stronger signal.
Air Interface Scheduling	After this function is enabled, the node fairly allocates download transmission time to clients, which guarantees that high-speed clients and low-speed clients obtain the same download transmission time. In this way, high-speed clients can transmit more data, achieving higher system throughput and a larger number of accessed clients.
APSD	It is abbreviated for Automatic Power Save Delivery, which is the WMM power-saving certification protocol of the WiFi Alliance. Enabling APSD can reduce the power consumption of the node. By default, this function is enabled.
Short GI	It specifies short guard interval for preventing data block interference. This parameter is available only for the 2.4 GHz WiFi network. When wireless signal is transmitted in space, delays may occur on the receiving end due to multipath and other factors. If the succeeding data block is transmitted too fast, it will cause interference to the preceding data block, and short GI can be used to avoid this interference. When short GI is enabled, wireless throughput is improved.

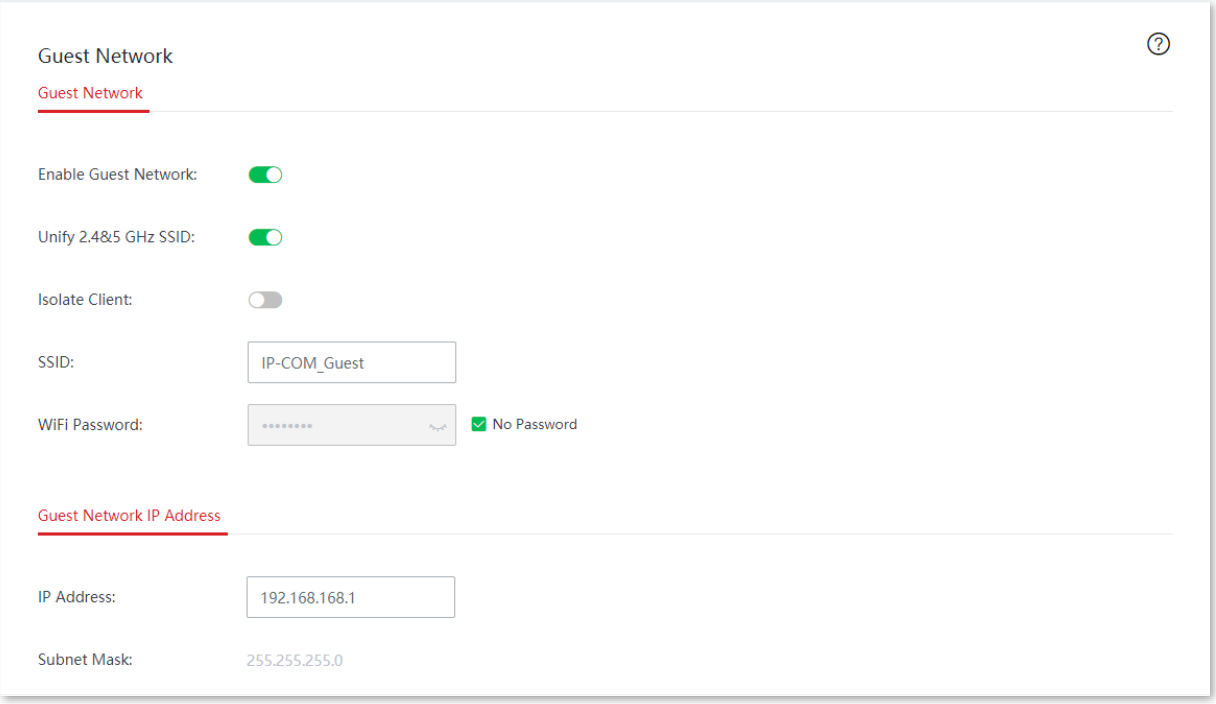
Parameter	Description
Deployment Mode	Choose a deployment mode based on the deployment intensity of nodes. – **Capacity-oriented**: This deployment mode is generally used in scenarios where nodes are deployed intensively, such as meeting hall, exhibition hall, banquet hall, gym, university classroom, and airport. This mode can effectively reduce interferences between nodes. – **Coverage-oriented**: This deployment mode is generally used in scenarios where nodes are deployed loosely, such as office, warehouse, and hospital. This mode can expand the coverage of nodes.
Client Timeout Interval	If a client generates no data communication within this interval after connecting to the WiFi network, the node will cut this client off.
Mandatory Rate	By adjusting the mandatory rate and optional rate, you can limit access from low-speed clients, thus improving the internet experience of other clients. – **Mandatory Rate**: It is a group of mandatory rates of the node. Clients must support these mandatory rates; otherwise, the clients will fail to access the WiFi network. – **Optional Rate**: It is a collection of other rates supported by the node except for mandatory rates. These optional rates help clients realize connection with the node at a higher rate.
Optional Rate	

3.3.5 Guest network

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

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

Click **Wireless** > **Guest Network** to enter the page. By default, this function is disabled. The following displays the page when guest network is enabled.



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

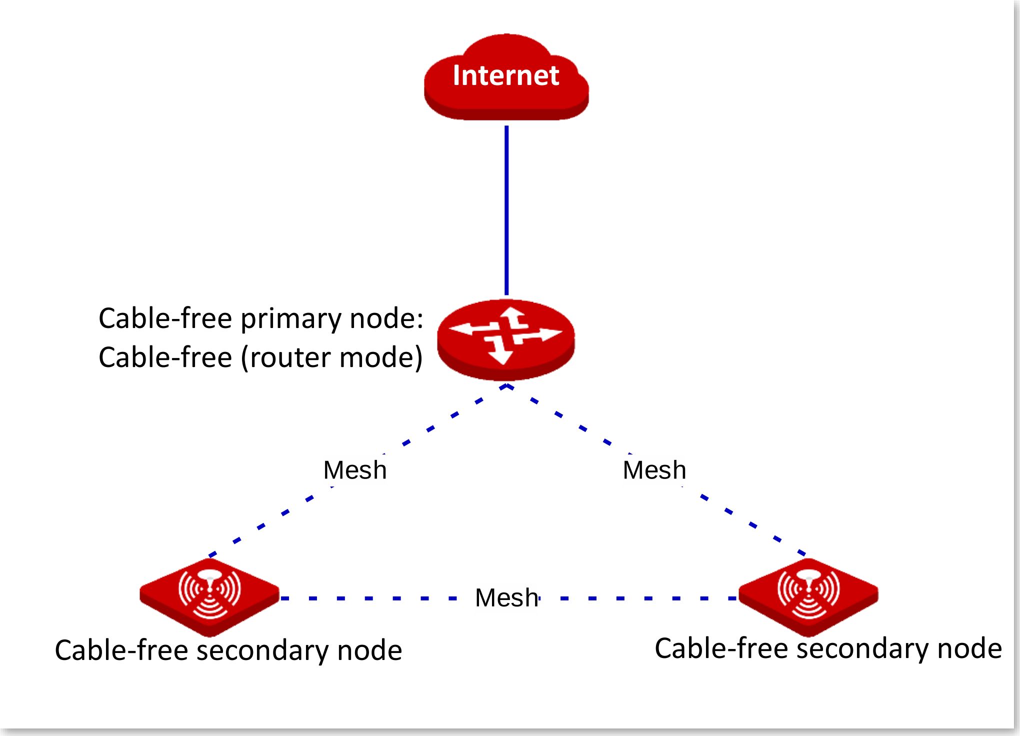
Parameter		Description
Guest Network	Enable Guest Network	It is used to enable or disable the guest network function.
	Unify 2.4&5 GHz SSID	After this function is enabled, the 2.4 GHz guest network and the 5 GHz guest network share the same WiFi network name and password. A wireless client will be automatically connected to the WiFi network with the best network quality when connecting to the guest network. Tip If there are guest clients which support only the 2.4 GHz network in your network, to avoid connection failure of these clients, you are recommended not to enable this function.
	Isolate Client	It specifies the isolation status of the wireless clients connected to the guest network. After this function is enabled, clients connected to the guest network cannot communicate with each other, enhancing the security of the WiFi network.

Parameter		Description
	SSID	It specifies the WiFi network name of the guest network. Tip To help you identify the primary network, you are recommended to set a different name for the guest network.
	WiFi Password	It specifies the WiFi password of the guest network.
	No Password	It specifies that no password is set for the guest network. The corresponding WiFi network is open.
Guest Network IP Address	IP Address	The default IP address of the guest network is **192.168.168.1**. After wireless clients connect to the guest network, they will obtain such an IP address (**192.168.168.***X*). Generally, you are recommended to retain the default settings.
	Subnet Mask	It specifies the subnet mask of the guest network, which is used to define the address space of the guest network.

3.4 Node management

3.4.1 Overview

The cable-free (router mode) node features the node management function which can centrally manage other IP-COM cable-free devices in a network. See the following network topology.



- **Configuration wizard**

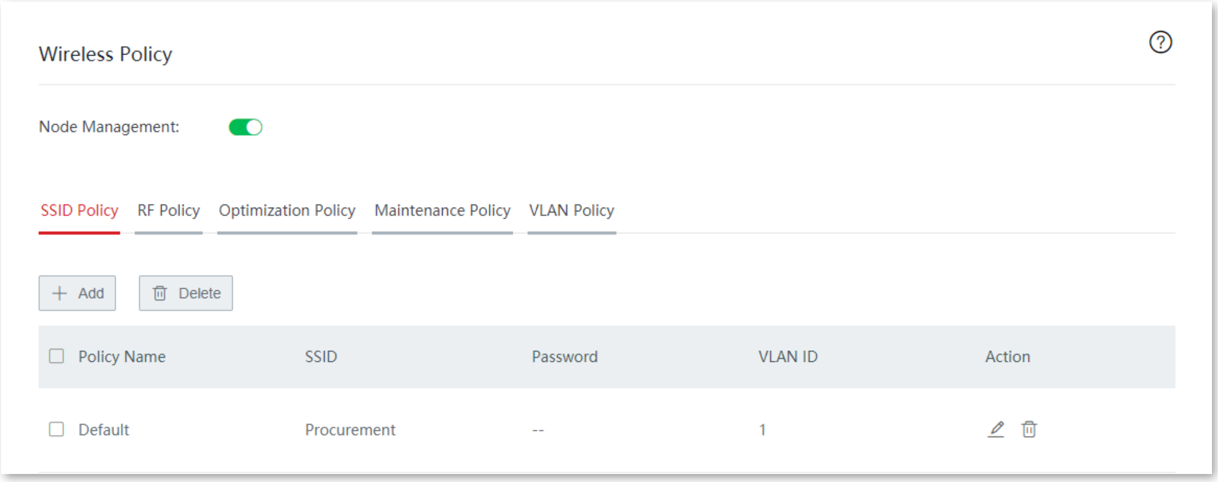
After a cable-free device joins the cable-free network, it can be managed centrally. See the following table for configuration procedures and tasks.

Procedure	Task	Description
1	Enable the node management function	Optional. This function is enabled by default.
2	Configure wireless policy	Required. Configure the configuration information of the node in the form of policy.
3	Maintain node	Required. Deliver configurations to the node.

Procedure	Task	Description
4	Topology routing	Optional. View the current network topology, manually specify the preferred transmission path between two nodes.

- **Enable the node management function**

The node management function is enabled by default. If you want to change its status, click **Node Management** > **Wireless Policy** to enter the page.



Node Management: ●

□ Policy Name	SSID	Password	VLAN ID	Action
□ Default	Procurement	--	1	✎ 🗑

3.4.2 Wireless policy

On this page, you can configure the configuration information of a node, such as SSID policy, RF policy, optimization policy, maintenance policy, and VLAN policy. You can use these policies in **Wireless** > **Maintenance** > **Policy Delivery**.

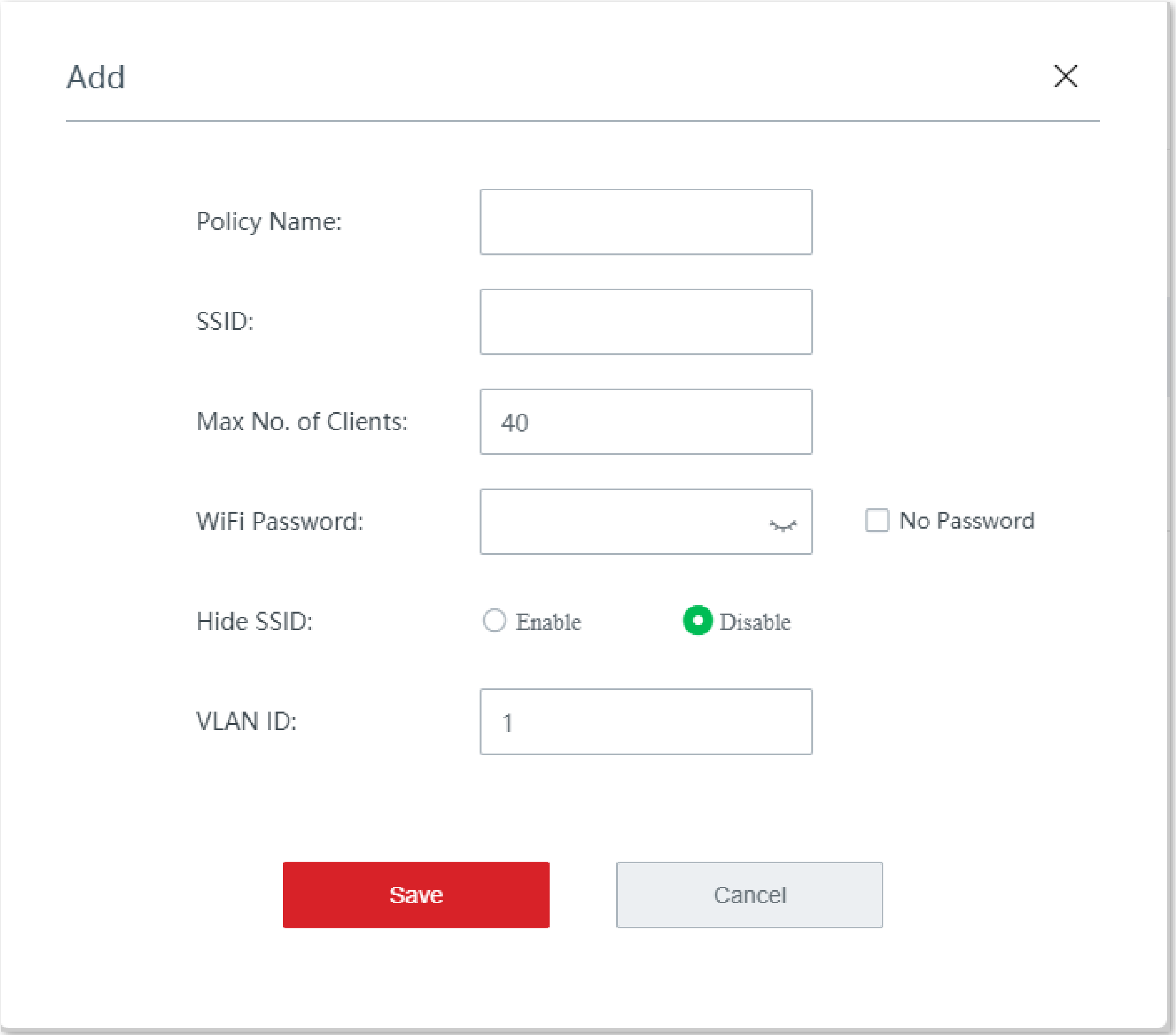
Click **Node Management** > **Wireless Policy** to enter the page.

SSID policy

SSID policy is used to configure the SSID-related parameters of the node.

Add a policy

On the **Node Management** > **Wireless Policy** > **SSID Policy** page, click **+ Add** to enter the configuration window.



Add

Policy Name:

SSID:

Max No. of Clients: 40

WiFi Password: □ No Password

Hide SSID: ○ Enable ● Disable

VLAN ID: 1

Parameter description

Parameter	Description
Policy Name	It specifies the name of the SSID policy. Note The SSID policy name cannot be duplicated.
SSID	It specifies the name of the WiFi network.
Max No. of Clients	It specifies the maximum number of clients allowed to connect to the WiFi network.
WiFi Password	It specifies the WPA-PSK or WPA2-PSK, which is also the WiFi password users need to enter when connecting the WiFi network. **No Password**: It specifies that no WiFi password is set for the WiFi network and the WiFi network is open.

Parameter	Description
Hide SSID	After this function is enabled, the SSID will be hidden and the WiFi network will not appear in the available network list of wireless clients (such as smartphones), enhancing the security of the WiFi network. If you want to connect to the hidden WiFi network, manually enter the SSID on your wireless clients.
VLAN ID	It specifies the VLAN to which the WiFi network belongs. The default VLAN ID is 1. Tip The VLAN ID takes effect only when you enable the VLAN function for the node.

Modify the policy

On the **Node Management** > **Wireless Policy** > **SSID Policy** page, click ✎ in the **Action** column to modify the corresponding policy.

Delete the policy

You can delete a policy that has not been used (not been delivered to online nodes yet).

Delete one policy: On the **Node Management** > **Wireless Policy** > **SSID Policy** page, click 🗑 in the **Action** column of the corresponding policy.

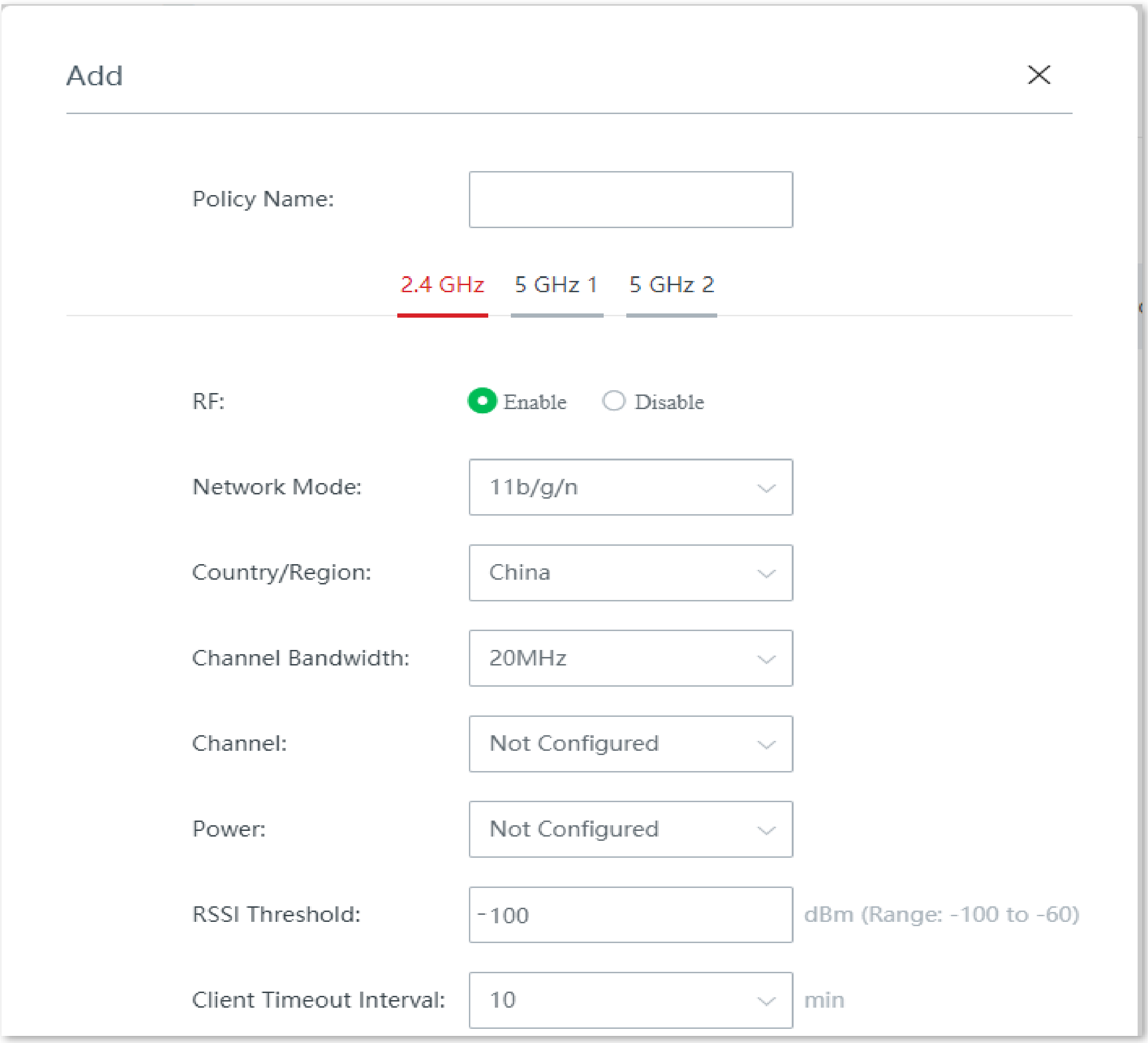
Delete policies in batches: On the **Node Management** > **Wireless Policy** > **SSID Policy** page, check the policies to be deleted and click **Delete**.

RF policy

RF policy is used to configure the basic RF parameters of the node.

Add a policy

On the **Node Management** > **Wireless Policy** > **RF Policy** page, click **+ Add** to enter the configuration window.



Add

Policy Name:

2.4 GHz 5 GHz 1 5 GHz 2

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

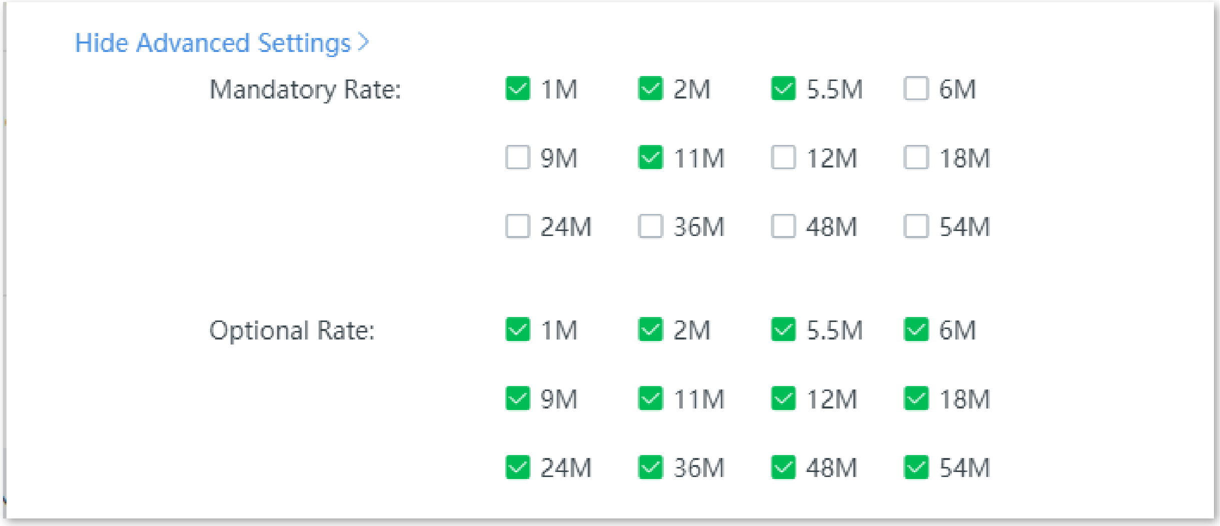
Parameter description

Parameter	Description
Policy Name	It specifies the name of the RF policy. Note The RF policy name cannot be duplicated.
2.4 GHz 5 GHz 1 5 GHz 2	It is for you to choose the frequency band to be configured. If you only choose one frequency band, the other two frequency bands retain the default settings.
RF	It specifies the status of the WiFi function. – **Enable**: Choose it to enable the WiFi function of the frequency band. – **Disable**: Choose it to disable the WiFi function of the frequency band.

Parameter	Description
Network Mode	It specifies the WiFi network mode of the corresponding band. Network modes of the 2.4 GHz frequency band include 11b, 11g, 11b/g, 11b/g/n, and n+256QAM. – **11b**: In this mode, only 802.11b wireless clients are allowed to access the 2.4 GHz WiFi network. – **11g**: In this mode, only 802.11g wireless clients are allowed to access the 2.4 GHz WiFi network. – **11b/g**: In this mode, 802.11b and 802.11g wireless clients can access the 2.4 GHz WiFi network. – **11b/g/n**: In this mode, wireless clients compliant with 802.11b or 802.11g and wireless clients working at 2.4 GHz and compliant with 802.11n can access the 2.4 GHz WiFi network. – **n+256QAM**: Wireless clients compliant with 802.11b or 802.11g and wireless clients working at 2.4 GHz and compliant with 802.11n can access the 2.4 GHz WiFi network. QAM, abbreviated for Quadrature Amplitude Modulation, is a modulation scheme that moderates amplitude on two orthogonal carriers. Using the orthogonality of sine wave and cosine wave, it moderates two signals at the same time, improving the modulation efficiency. In the n+256QAM network mode, the 256-QAM modulation mode compliant with the IEEE 802.11ac standard can be used under the IEEE 802.11n standard in the 2.4GHz band, which improves the single stream rate from 150 Mbps to 200 Mbps. Note: Such improvement can be realized only when the band is 2.4 GHz band, and the transmitting an d receiving ends both support the n+256QAM network mode. If any one end does not support n+256QAM, the single stream rate under the 2.4 GHz band is still 150 Mbps at most. Moreover, after the network mode is set to n+256QAM, the stability and anti-interference capability of the network will be reduced compared with the stability and anti-interference capability under other modes. Network modes of the 5 GHz 1 frequency band and the 5 GHz 2 frequency band include 11a, 11ac, and 11a/n. – **11a**: In this mode, only 802.11a wireless clients are allowed to access the 5 GHz WiFi network. – **11ac**: In this mode, only 802.11ac wireless clients are allowed to access the 5 GHz WiFi network. – **11a/n**: In this mode, wireless clients compliant with 802.11a and wireless clients working at 5 GHz and compliant with 802.11n can access the 5 GHz WiFi network.
Country/Region	It specifies the country or region where the node is located. Please select the correct country or region.

Parameter	Description
Channel Bandwidth	It specifies the bandwidth of the working channel. A high channel bandwidth means a higher transmission rate, but the penetration capability is reduced and the transmission distance is shortened. – **20MHz**: The node uses the 20MHz channel bandwidth. – **40MHz**: The node uses the 40MHz channel bandwidth. – **20MHz/40MHz**: This channel bandwidth is available only for the 2.4 GHz only. The node automatically adjusts the channel bandwidth to 20MHz or 40MHz based on the surrounding environment. – **80MHz**: This channel bandwidth is available only for the 5 GHz only. The node uses the 80MHz channel bandwidth.
Channel	It specifies the channel in which the wireless data is transmitted and received. The available channels are determined by the current country/region and wireless band. – **Not Configured:** Retain the current configurations of the node. – **Auto**: The node automatically detects the occupation rate of channels and selects the appropriate working channel accordingly. If connection drop, freeze or slow internet occurs frequently when you are using the WiFi network, you can try changing the working channel. You can check the channels with low occupation rate and little interference using software tools (such as WiFi analyzer).
Power	It specifies the transmit power of the corresponding band. The higher the transmit power, the wider the WiFi coverage. However, an appropriate reduction of transmit power can help improve the performance and security of the WiFi network. **Not Configured:** Retain the current configurations of the node.
RSSI Threshold	It specifies the minimum wireless signal strength can be received by the band. Clients with a lower signal strength value cannot connect to the node. When there are multiple nodes in the surroundings, an appropriate RSSI value helps ensure wireless clients connects to the nodes with a stronger signal.
Client Timeout Interval	If a client generates no data communication within this interval after connecting to the WiFi network, the node will cut this client off.
Show/Hide Advanced Settings	Click to expand/collapse the advanced parameters: mandatory rate and optional rate.
Mandatory Rate	By adjusting the mandatory rate and optional rate, you can limit access from low-speed clients, thus improving the internet experience of other clients. – **Mandatory Rate**: It is a group of mandatory rates of the node. Clients must support these mandatory rates; otherwise, the clients will fail to access the WiFi network. – **Optional Rate**: It is a collection of other rates supported by the node except for mandatory rates. These optional rates help clients realize connection with the node at a higher rate.
Optional Rate	

Refer to the following figure for the advanced parameters.



Hide Advanced Settings >

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

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

Modify the policy

On the **Node Management** > **Wireless Policy** > **RF Policy** page, click ✎ in the **Action** column to modify the corresponding policy.

Delete the policy

You can delete a policy that has not been used (not been delivered to online nodes yet).

Delete one policy: On the **Node Management** > **Wireless Policy** > **RF Policy** page, click 🗑 in the **Action** column of the corresponding policy.

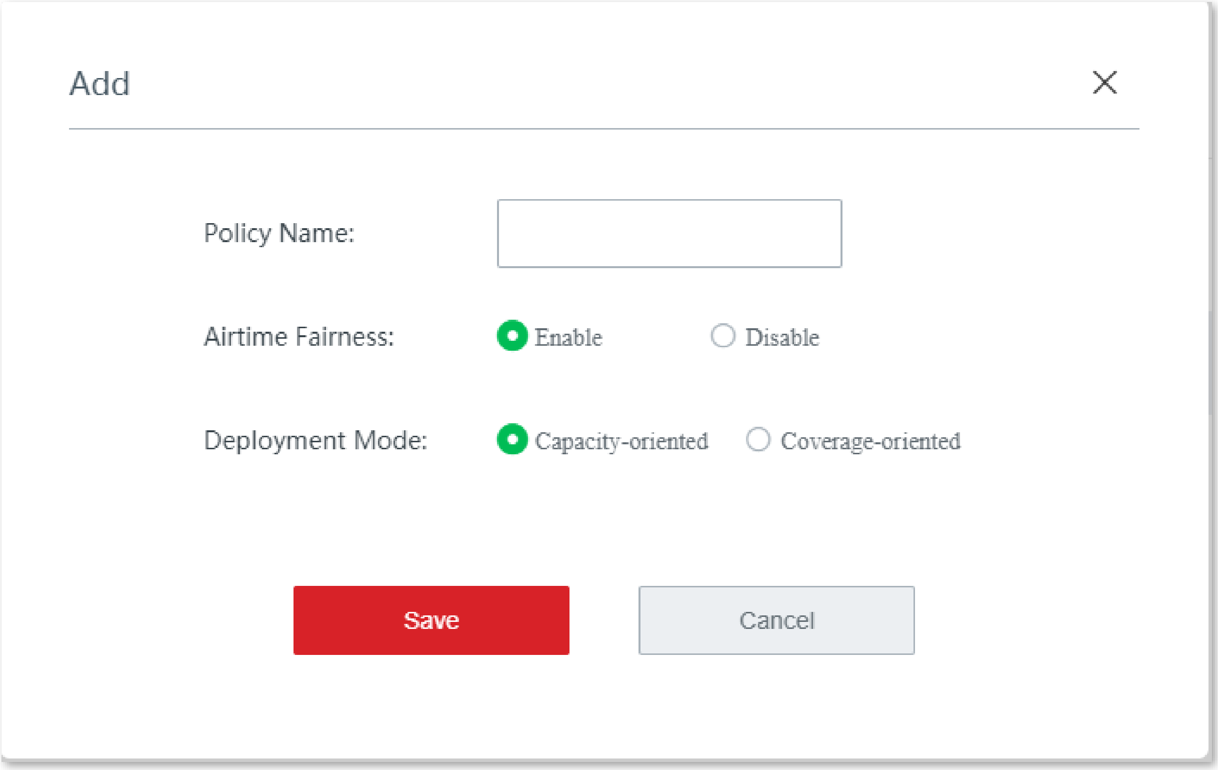
Delete policies in batches: On the **Node Management** > **Wireless Policy** > **RF Policy** page, check the policies to be deleted and click **Delete**.

Optimization policy

Optimization policy is used to configure the optimization parameters of the node.

Add a policy

On the **Node Management** > **Wireless Policy** > **Optimization Policy** page, click **+ Add** to enter the configuration window.



Add

Policy Name:

Airtime Fairness: ● Enable ○ Disable

Deployment Mode: ● Capacity-oriented ○ Coverage-oriented

Parameter description

Parameter	Description
Policy Name	It specifies the name of the optimization policy. Note The optimization policy name cannot be duplicated.
Airtime Fairness	After this function is enabled, the node fairly allocates download transmission time to clients, which guarantees that high-speed clients and low-speed clients obtain the same download transmission time. In this way, high-speed clients can transmit more data, achieving higher system throughput and a larger number of accessed clients.
Deployment Mode	Choose a deployment mode based on the deployment intensity of nodes. – **Capacity-oriented**: This deployment mode is generally used in scenarios where nodes are deployed intensively, such as meeting hall, exhibition hall, banquet hall, gym, university classroom, and airport. This mode can effectively reduce interferences between nodes. – **Coverage-oriented**: This deployment mode is generally used in scenarios where nodes are deployed loosely, such as office, warehouse, and hospital. This mode can expand the coverage of nodes.

Modify the policy

On the **Node Management** > **Wireless Policy** > **Optimization Policy** page, click ✎ in the **Action** column to modify the corresponding policy.

Delete the policy

You can delete a policy that has not been used (not been delivered to online nodes yet).

Delete one policy: On the **Node Management** > **Wireless Policy** > **Optimization Policy** page, click 🗑 in the **Action** column of the corresponding policy.

Delete policies in batches: On the **Node Management** > **Wireless Policy** > **Optimization Policy** page, check the policies to be deleted and click **Delete**.

Maintenance policy

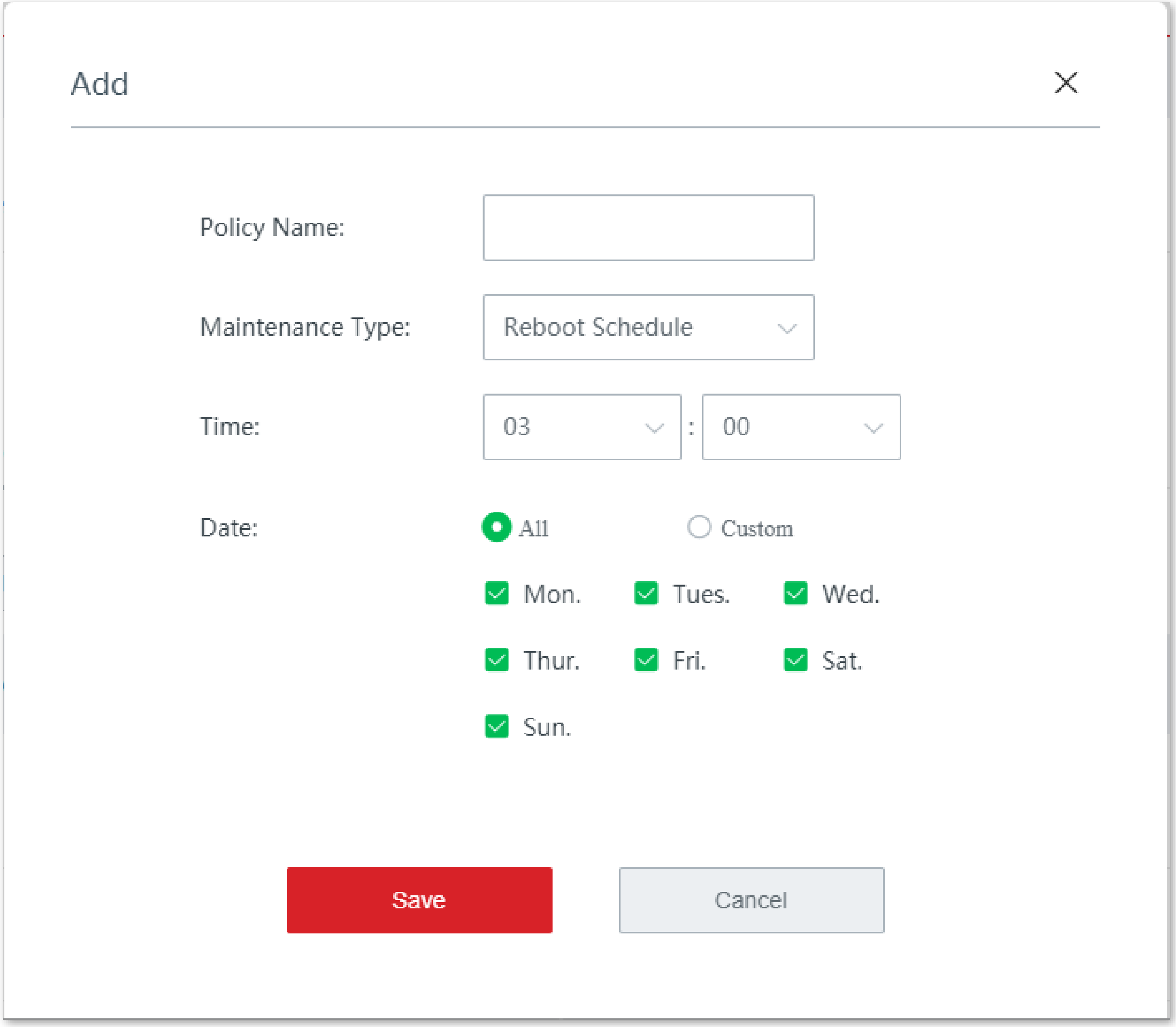
Maintenance policy is used to configure the customized reboot parameters of the node. An appropriate maintenance policy helps avoid such phenomena as deteriorating performance and instability of the cable-free network caused by long time operation.

Tip

- Maintenance policies take effect for managed nodes and the time point when the maintenance policies start being effective is counted based on the system time of the managed nodes. Please make sure that the system time of the managed nodes is correct.
- During the reboot, all connections will be cut off; therefore, you are recommended to schedule the maintenance time at an idle period to minimize its effect on your businesses.

Add a policy

On the **Node Management** > **Wireless Policy** > **Maintenance Policy** page, click **+ Add** to enter the configuration window.



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 the maintenance policy. Note The maintenance policy name cannot be duplicated.
Maintenance Type	It specifies the maintenance type of the node. You can choose between reboot schedule and cyclic reboot. – **Reboot Schedule**: The node reboots once at the specified time point on the specified date(s). – **Cyclic Reboot**: The node reboots once every specified interval.
Time	If the **Maintenance Type** is set to **Reboot Schedule**, set these two parameters to set the time point and dates when the node reboots.
Date	

Parameter	Description
Interval	If the **Maintenance Type** is set to **Cyclic Reboot**, set this parameter to set the reboot interval.

Modify the policy

On the **Node Management** > **Wireless Policy** > **Maintenance Policy** page, click ✎ in the **Action** column to modify the corresponding policy.

Delete the policy

You can delete a policy that has not been used (not been delivered to online nodes yet).

Delete one policy: On the **Node Management** > **Wireless Policy** > **Maintenance Policy** page, click 🗑 in the **Action** column of the corresponding policy.

Delete policies in batches: On the **Node Management** > **Wireless Policy** > **Maintenance Policy** page, check the policies to be deleted and click **Delete**.

VLAN policy

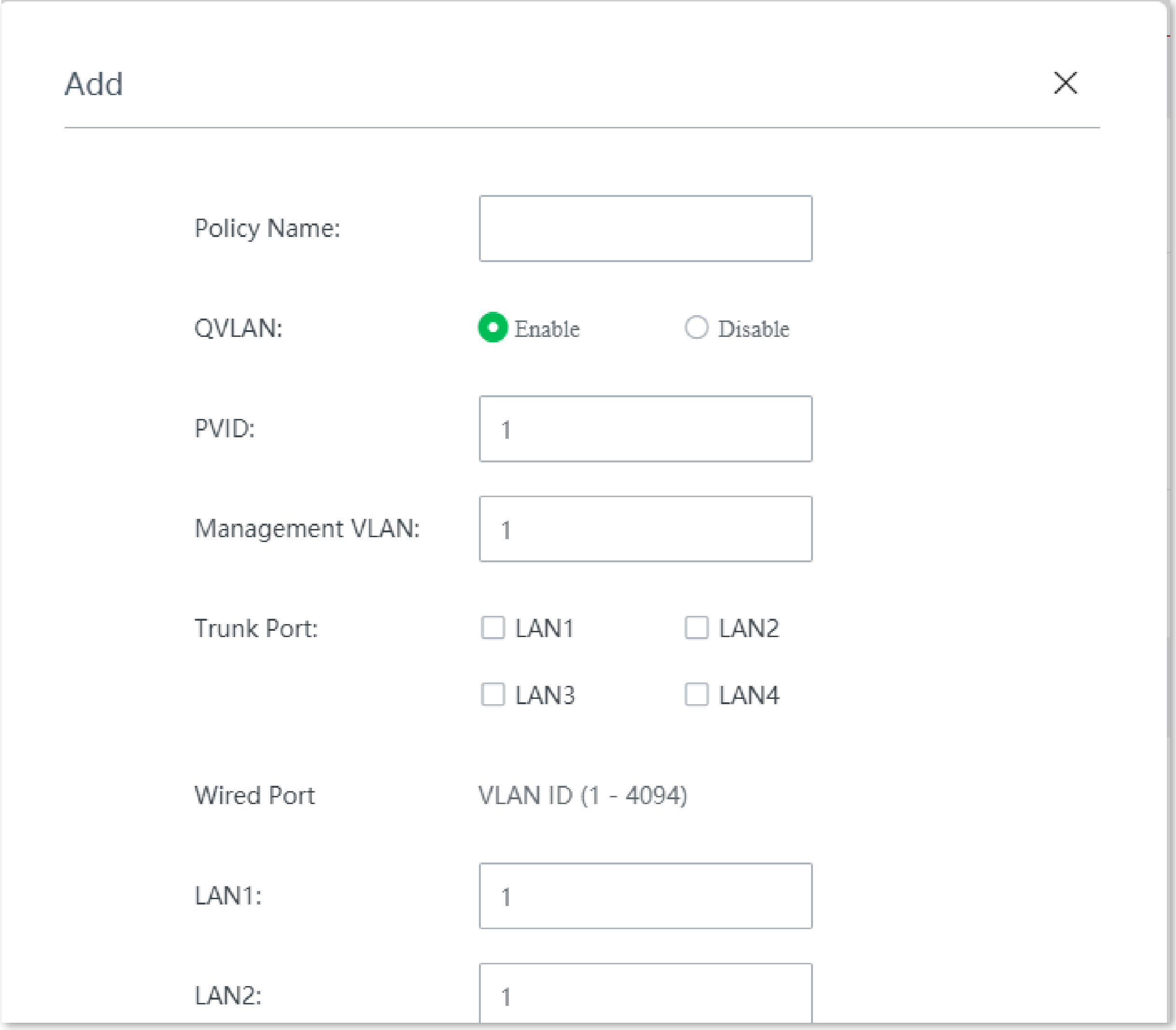
VLAN policy is used to configure the VLAN-related parameters of the node.

Tip

If you need to view the default values for each parameter in VLAN policy, refer to the default settings for each parameter when a new VLAN policy is being added.

Add a policy

On the **Node Management** > **Wireless Policy** > **VLAN Policy** page, click **+ Add** to enter the configuration window.



Add

Policy Name:	
QVLAN:	● Enable ○ Disable
PVID:	1
Management VLAN:	1
Trunk Port:	□ LAN1 □ LAN2 □ LAN3 □ LAN4
Wired Port	VLAN ID (1 - 4094)
LAN1:	1
LAN2:	1

Parameter description

Parameter	Description
Policy Name	It specifies the name of the VLAN policy. Note The VLAN policy name cannot be duplicated.
QVLAN	It specifies whether to enable the QVLAN function. By default, this function is enabled.
PVID	It specifies the ID of the default native VLAN of the trunk port of the node. After the QVLAN function is enabled, the LAN port is the trunk port. Traffic of all VLANs can pass through a trunk port. Its default value is **1**.
Management VLAN	It specifies the ID of the management VLAN. The default value is **1**. After changing the management VLAN, you can manage the node only after connecting your computer to the new management VLAN.
Trunk Port	Select the trunk port(s). The trunk port allows data of all VLANs to pass.

Parameter	Description
Wired Port	It specifies the wired LAN port of the node.
VLAN ID	It specifies the VLAN ID of the port. The default value is **1**.

Modify the policy

On the **Node Management** > **Wireless Policy** > **VLAN Policy** page, click ✎ in the **Action** column to modify the corresponding policy.

Delete the policy

You can delete a policy that has not been used (not been delivered to online nodes yet).

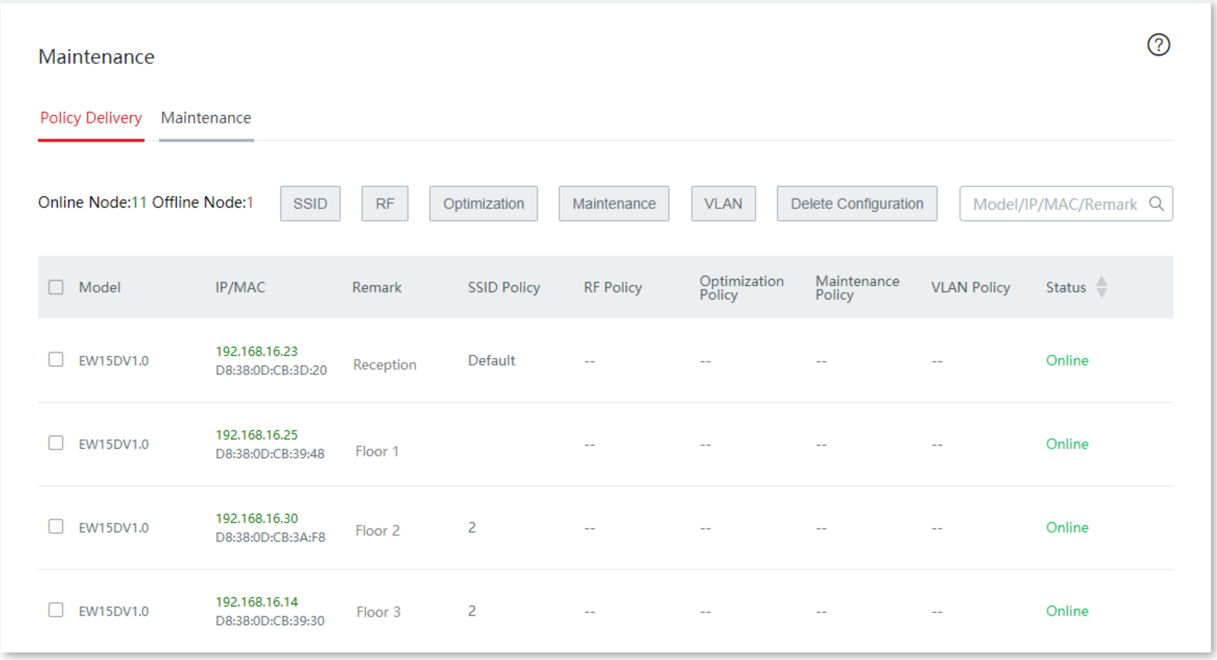
Delete one policy: On the **Node Management** > **Wireless Policy** > **VLAN Policy** page, click 🗑 in the **Action** column of the corresponding policy.

Delete policies in batches: On the **Node Management** > **Wireless Policy** > **VLAN Policy** page, check the policies to be deleted and click **Delete**.

3.4.3 Maintenance

On this page, you can deliver the wireless policies you configured to online nodes, delete the configurations of nodes, reboot/reset online nodes in batches, delete offline nodes in batches, modify the configuration of a node separately, and check/export the information of managed nodes.

Click **Node Management** > **Maintenance** to enter the page.



Maintenance

Online Node:11 Offline Node:1

□	Model	IP/MAC	Remark	SSID Policy	RF Policy	Optimization Policy	Maintenance Policy	VLAN Policy	Status
□	EW15DV1.0	192.168.16.23 D8:38:0D:CB:3D:20	Reception	Default	--	--	--	--	Online
□	EW15DV1.0	192.168.16.25 D8:38:0D:CB:39:48	Floor 1		--	--	--	--	Online
□	EW15DV1.0	192.168.16.30 D8:38:0D:CB:3A:F8	Floor 2	2	--	--	--	--	Online
□	EW15DV1.0	192.168.16.14 D8:38:0D:CB:39:30	Floor 3	2	--	--	--	--	Online

Policy delivery

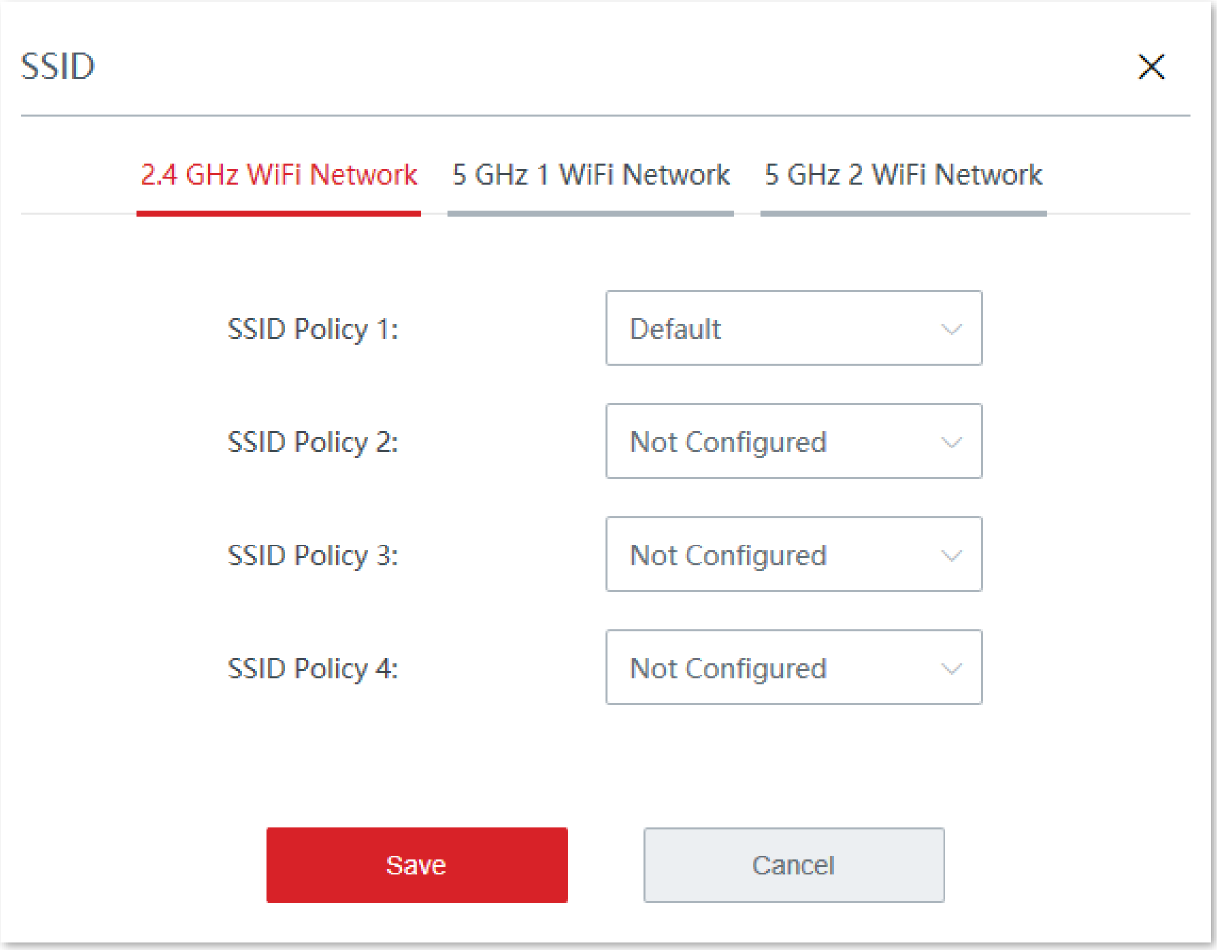
Policy delivery is used to deliver configured policies to online nodes.

SSID

Click **SSID** to deliver SSID policies to one or multiple online nodes.

Deliver SSID policies:

1. On the **Node Management** > **Maintenance** > **Policy Delivery** page, select the nodes to which you deliver SSID policies.
2. Click **SSID** and configure the parameters.
3. Click **Save**.



SSID

2.4 GHz WiFi Network | 5 GHz 1 WiFi Network | 5 GHz 2 WiFi Network

SSID Policy 1: Default

SSID Policy 2: Not Configured

SSID Policy 3: Not Configured

SSID Policy 4: Not Configured

Parameter description

Parameter	Description
2.4 GHz WiFi Network 5 GHz 1 WiFi Network 5 GHz 2 WiFi Network	Select the wireless frequency band on which the SSID policy takes effect. Available SSID bands depend on the secondary node. If the secondary node does not support 5 GHz, 5GHz settings won’t be allowed. – If both 2.4 GHz and 5 GHz bands are needed at the same time, please

Parameter	Description
	configure them one after the other, and then click **Save**. – If some selected secondary nodes only support 2.4 GHz, and some selected secondary nodes support both 2.4 GHz and 5 GHz, the AC will automatically issue wireless settings to secondary nodes according to their actual supported wireless bands.
SSID Policy 1/2/3/4	Select the SSID policy to be delivered. SSID policies must be configured in the SSID policy module in advance. If the node enables multiple wireless networks, each network must be configured with a unique SSID policy. Not Configured: Current configuration of the node remains unchanged.

----End

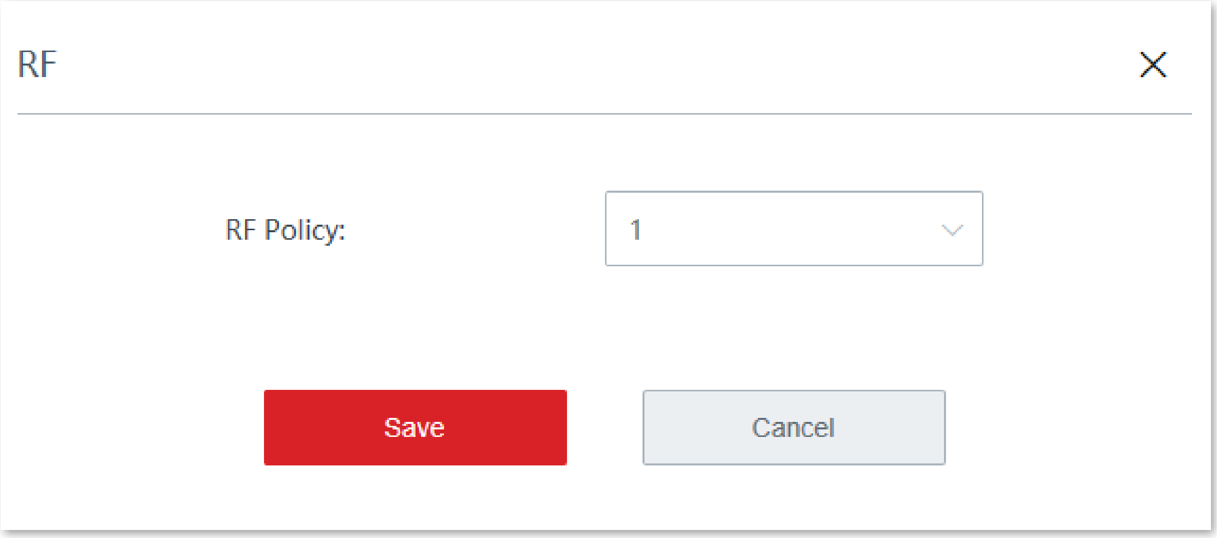
The SSID policies will be delivered to the selected nodes.

RF

Click **RF** to deliver RF policies to one or multiple online nodes.

Deliver an RF policy:

1. On the **Node Management** > **Maintenance** > **Policy Delivery** page, select the nodes to which you deliver an RF policy.
2. Click **RF** and select the target RF policy.
3. Click **Save**.


RF

RF Policy: 1

Parameter description

Parameter	Description
RF Policy	Select the RF policy to be delivered. RF policies must be configured in the RF policy module in advance. Not Configured: Current configuration of the node remains unchanged.

----End

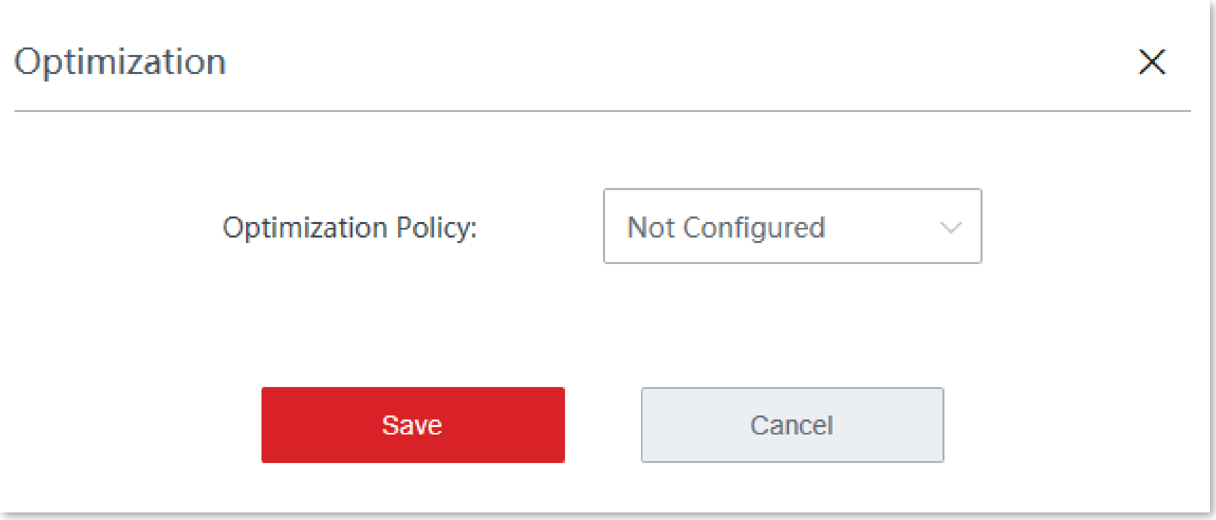
The RF policy will be delivered to the selected nodes.

Optimization

Click **Optimization** to deliver optimization policies to one or multiple online nodes.

Deliver an optimization policy:

1. On the **Node Management** > **Maintenance** > **Policy Delivery** page, select the nodes to which you deliver an optimization policy.
2. Click **Optimization** and select the target optimization policy.
3. Click **Save**.



Optimization

Optimization Policy: Not Configured

Parameter description

Parameter	Description
Optimization Policy	Select the optimization policy to be delivered. Optimization policies must be configured in the Optimization policy module in advance. Not Configured: Current configuration of the node remains unchanged.

----End

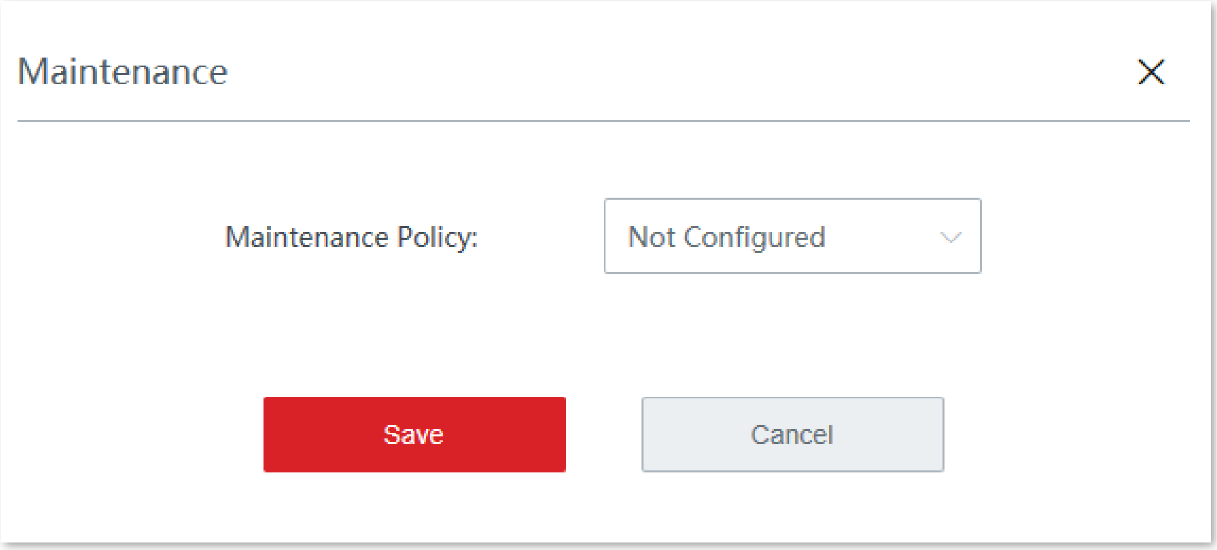
The optimization policy will be delivered to the selected nodes.

Maintenance

Click **Maintenance** to deliver maintenance policies to one or multiple online nodes.

Deliver a maintenance policy:

1. On the **Node Management** > **Maintenance** > **Policy Delivery** page, select the nodes to which you deliver a maintenance policy.
2. Click **Maintenance** and select the target maintenance policy.
3. Click **Save**.



Maintenance

Maintenance Policy: Not Configured

Parameter description

Parameter	Description
Maintenance Policy	Select the maintenance policy to be delivered. Maintenance policies must be configured in the Maintenance policy module in advance. Not Configured: Current configuration of the node remains unchanged.

----End

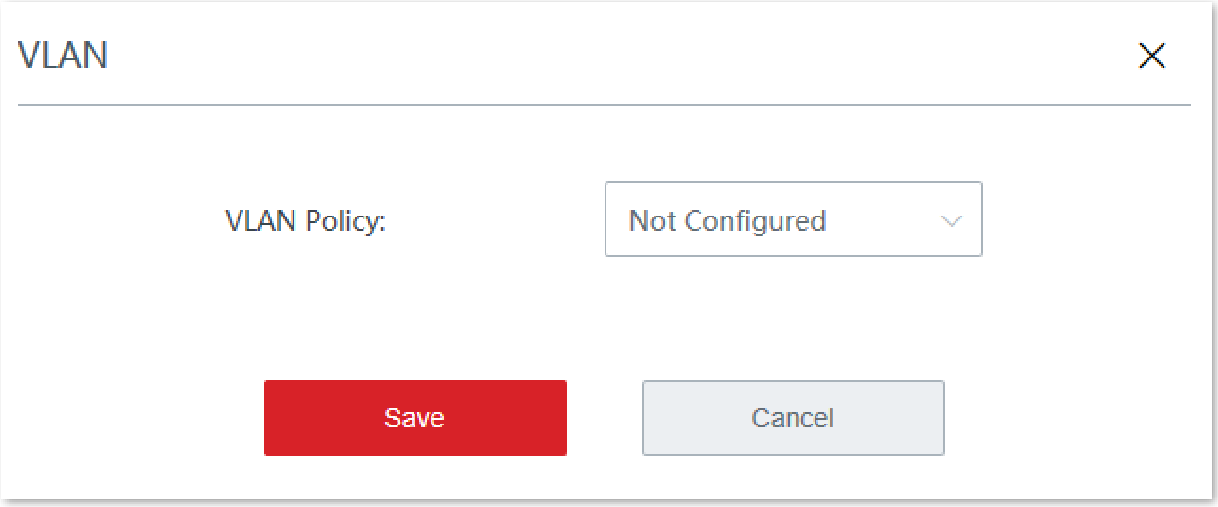
The maintenance policy will be delivered to the selected nodes.

VLAN

Click **VLAN** to deliver VLAN policies to one or multiple online nodes.

Deliver a VLAN policy:

1. On the **Node Management** > **Maintenance** > **Policy Delivery** page, select the nodes to which you deliver a VLAN policy.
2. Click **VLAN** and select the target VLAN policy.
3. Click **Save**.



VLAN

VLAN Policy: Not Configured

Parameter description

Parameter	Description
VLAN Policy	Select the VLAN policy to be delivered. VLAN policies must be configured in the VLAN policy module in advance. Not Configured: Current configuration of the node remains unchanged.

----End

The VLAN policy will be delivered to the selected nodes.

Delete configuration

Click **Delete Configuration** to delete the configurations delivered to one or multiple online nodes.

Delete configurations of one node: On the **Node Management** > **Maintenance** > **Policy Delivery** page, check the target node and click **Delete Configuration**.

Delete configurations in batches: On the **Node Management** > **Maintenance** > **Policy Delivery** page, check the nodes whose configurations you want to delete and click **Delete Configuration**.

After you click **Delete Configuration**, all the policy configuration of the target node will be restored to factory settings.

Maintenance

Click **Node Management** > **Maintenance** > **Maintenance** to enter the page.

Maintenance is used to reboot or reset online nodes in batches, check or export the information of managed nodes, delete the information of offline nodes, and refresh the displayed node information.

Reboot

Click **Reboot** to reboot one or multiple nodes.

Reboot node:

1. On the **Node Management** > **Maintenance** > **Maintenance** page, select the nodes to be rebooted.
2. Click **Reboot** and follow the on-screen instructions.

----End

After the nodes are rebooted, they are offline for a while and then automatically get online after the reboot completes. This whole process may take 1 to 2 minutes. Please wait with patience. You can click **Refresh** on the same page to check the latest status of the node.

Reset

Click **Reset** to restore one or multiple nodes to factory settings.

Reset node:

1. On the **Node Management** > **Maintenance** > **Maintenance** page, select the nodes to be reset.
2. Click **Reset** and follow the on-screen instructions.

----End

Export

Click **Export** to export the node information in the Excel form and save it to the management computer.

On the **Node Management** > **Maintenance** > **Maintenance** page, click **Export** and follow the on-screen instructions.

Delete

Click **Delete** to delete the information of one or multiple offline nodes.

Delete one node: On the **Node Management** > **Maintenance** > **Maintenance** page, click 🗑 on the row where the target node resides.

Delete nodes in batches: On the **Node Management** > **Maintenance** > **Maintenance** page, check the nodes to be deleted and click **Delete**.

Refresh

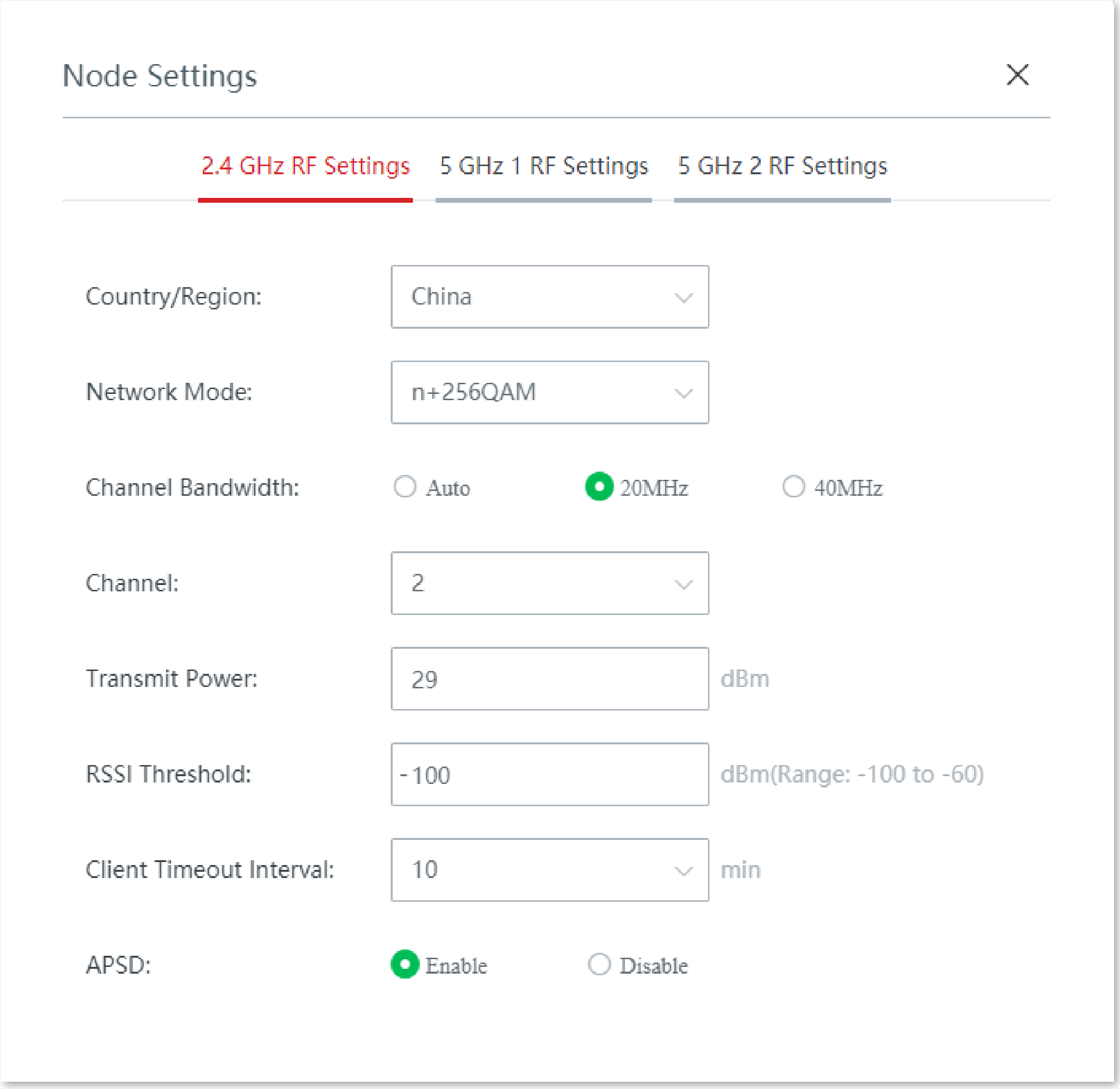
Click **Refresh** on the **Node Management** > **Maintenance** > **Maintenance** page to refresh the displayed node information.

Edit

Click **Edit** to edit separately the configurations of a node, such as its country/region, channel, transmit power and other parameters.

Edit the configurations of a node:

1. On the **Node Management** > **Maintenance** > **Maintenance** page, locate the node whose configurations you want to edit, and click ✎ on the row where the node resides.
2. Modify the parameters as required.



Node Settings

Country/Region: China

Network Mode: n+256QAM

Channel Bandwidth: ○ Auto ● 20MHz ○ 40MHz

Channel: 2

Transmit Power: 29 dBm

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

Client Timeout Interval: 10 min

APSD: ● Enable ○ Disable

3. Click **Save**.

----End

The new configurations are automatically delivered to the target node.

Parameter description

Parameter	Description
Country/Region	It specifies the country or region where the node locates. Please select the correct country/region to comply with the regulations of different countries or regions have on channel or transmit power.
Network Mode	It specifies the WiFi network mode of the corresponding band. Network modes of the 2.4 GHz WiFi network include 11b, 11g, 11b/g, 11b/g/n, and n+256QAM. By default, the router works in the n+256QAM mode. – **11b**: In this mode, only 802.11b wireless clients are allowed to access the 2.4 GHz WiFi network. – **11g**: In this mode, only 802.11g wireless clients are allowed to access the 2.4 GHz WiFi network. – **11b/g**: In this mode, 802.11b and 802.11g wireless clients can access the 2.4 GHz WiFi network. – **11b/g/n**: In this mode, wireless clients compliant with 802.11b or 802.11g and wireless clients working at 2.4 GHz and compliant with 802.11n can access the 2.4 GHz WiFi network. – **n+256QAM**: Wireless clients compliant with 802.11b or 802.11g and wireless clients working at 2.4 GHz and compliant with 802.11n can access the 2.4 GHz WiFi network. QAM, abbreviated for Quadrature Amplitude Modulation, is a modulation scheme that moderates amplitude on two orthogonal carriers. Using the orthogonality of sine wave and cosine wave, it moderates two signals at the same time, improving the modulation efficiency. In the n+256QAM network mode, the 256-QAM modulation mode compliant with the IEEE 802.11ac standard can be used under the IEEE 802.11n standard in the 2.4GHz band, which improves the single stream rate from 150 Mbps to 200 Mbps. Note: Such improvement can be realized only when the band is 2.4 GHz band, and the transmitting an d receiving ends both support the n+256QAM network mode. If any one end does not support n+256QAM, the single stream rate under the 2.4 GHz band is still 150 Mbps at most. Moreover, after the network mode is set to n+256QAM, the stability and anti-interference capability of the network will be reduced compared with the stability and anti-interference capability under other modes. Network modes of the 5 GHz WiFi network include 11a, 11ac, and 11a/n. By default, the router works in the 11ac mode. – **11a**: In this mode, only 802.11a wireless clients are allowed to access the 5 GHz WiFi network. – **11ac**: In this mode, only 802.11ac wireless clients are allowed to access the 5 GHz WiFi network. – **11a/n**: In this mode, wireless clients compliant with 802.11a and wireless clients working at 5 GHz and compliant with 802.11n can access the 5 GHz WiFi network.

Parameter	Description
Channel Bandwidth	It specifies the bandwidth of the working channel. A high channel bandwidth means a higher transmission rate, but the penetration capability is reduced and the transmission distance is shortened. – **20MHz**: The node uses the 20MHz channel bandwidth. – **40MHz**: The node uses the 40MHz channel bandwidth. – **Auto**: This channel bandwidth is available only for the 2.4 GHz only. The node automatically adjusts the channel bandwidth to 20MHz or 40MHz based on the surrounding environment. – **80MHz**: This channel bandwidth is available only for the 5 GHz only. The node uses the 80MHz channel bandwidth.
Channel	It specifies the channel in which the wireless data is transmitted and received. The available channels are determined by the current country/region and wireless band. **Auto**: The node automatically detects the occupation rate of channels and selects the appropriate working channel accordingly. If connection drop, freeze or slow internet occurs frequently when you are using the WiFi network, you can try changing the working channel. You can check the channels with low occupation rate and little interference using software tools (such as WiFi analyzer).
Transmit Power	It specifies the transmit power of the corresponding band. The higher the transmit power, the wider the WiFi coverage. However, an appropriate reduction of transmit power can help improve the performance and security of the WiFi network.
RSSI Threshold	It specifies the minimum wireless signal strength can be received by the band. Clients with a lower signal strength value cannot connect to the node. When there are multiple nodes in the surroundings, an appropriate RSSI value helps ensure wireless clients connects to the nodes with a stronger signal.
Client Timeout Interval	If a client generates no data communication within this interval after connecting to the WiFi network, the node will cut this client off.
APSD	It is abbreviated for Automatic Power Save Delivery, which is the WMM power-saving certification protocol of the WiFi Alliance. Enabling APSD can reduce the power consumption of the node.

3.4.4 Topology routing

On this page, you can check the network topology routes currently available and manually set preferred routes between nodes. In the **Network Topology** module, you can check the current topology, the status of the route, and select the nodes whose topology routes you want to check. In the **Communication Routing** module, you can customize the preferred route between two nodes.

Click **Node Management** > **Topology Routing** to enter the page.

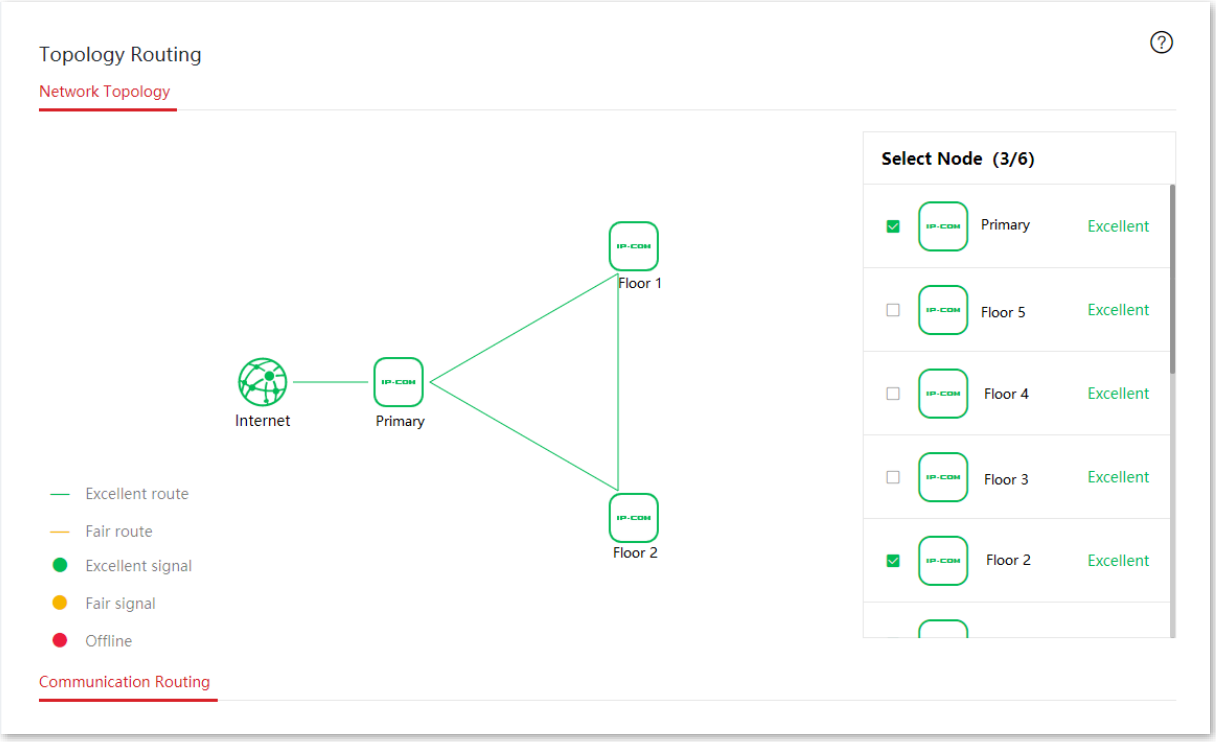
Network topology

Click **Node Management** > **Topology Routing** to enter the page. In this module, you can:

- check the current network topology.
- check the connection status of the link between nodes.
- check the internet connection status of each node.

Check the current network topology

You can select the secondary nodes you want to display in the topology in the right column and check the current network topology of the selected node. See the following figure.



Topology Routing

Network Topology

Select Node (3/6)

☑ Primary Excellent

□ Floor 5 Excellent

□ Floor 4 Excellent

□ Floor 3 Excellent

☑ Floor 2 Excellent

Communication Routing

Tip

At most 6 nodes can be displayed. You can select 6 or fewer than 6 nodes to check their network topology.

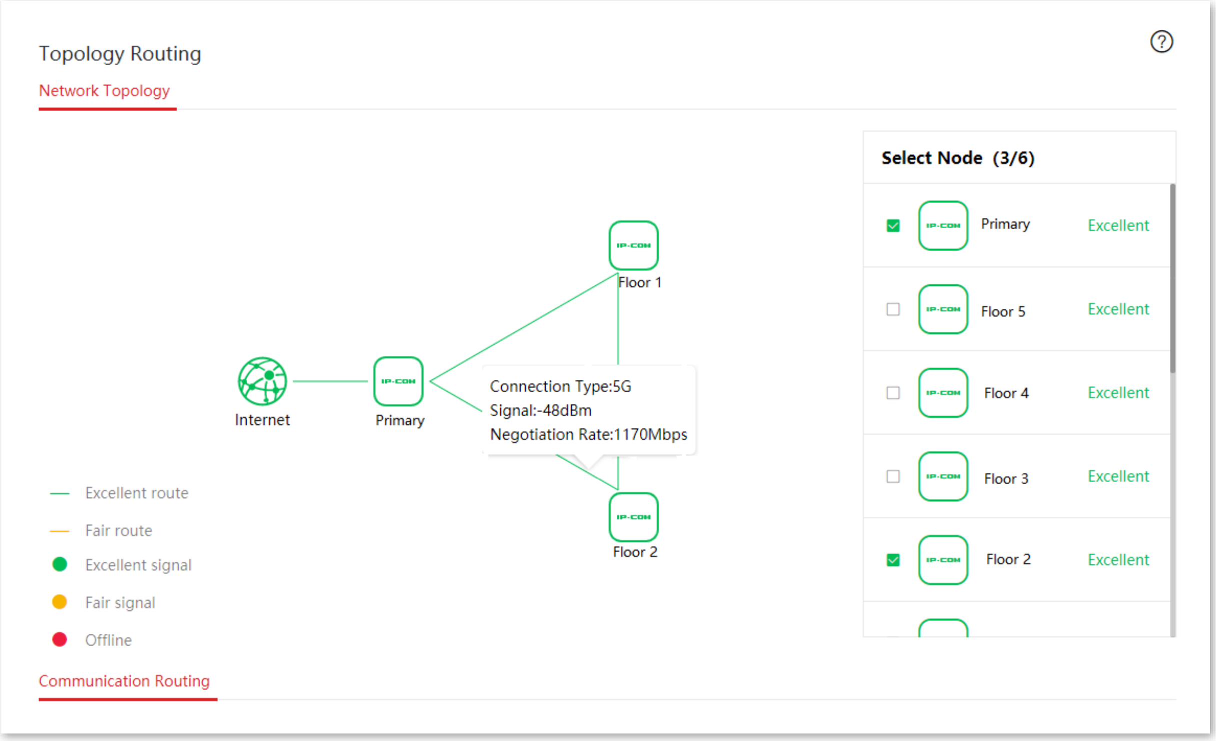
Check the connection status of the link between nodes

You can learn the link quality between two nodes according to the line color in the network topology.

- 🟩 indicates that the quality of the link between two nodes is excellent.
- 🟨 indicates that the quality of the link between two nodes is fair.

Check the internet connection status of each node

You can view the internet connection status of each node by hovering the mouse to the node icon in the network topology.



Connection Type:5G
Signal:-48dBm
Negotiation Rate:1170Mbps

Parameter description

Parameter	Description
Connection Type	It specifies the way by which the node connects with the upstream node.
Signal	It specifies the strength of the signal this node received from the upstream node.
Negotiation Rate	It specifies the wireless negotiation rate between this node and the upstream node.

Communication routing

Click **Node Management** > **Topology Routing** to enter the page. In this module, you can:

– add the preferred transmission path for two nodes.

– display the preferred transmission path between two nodes.

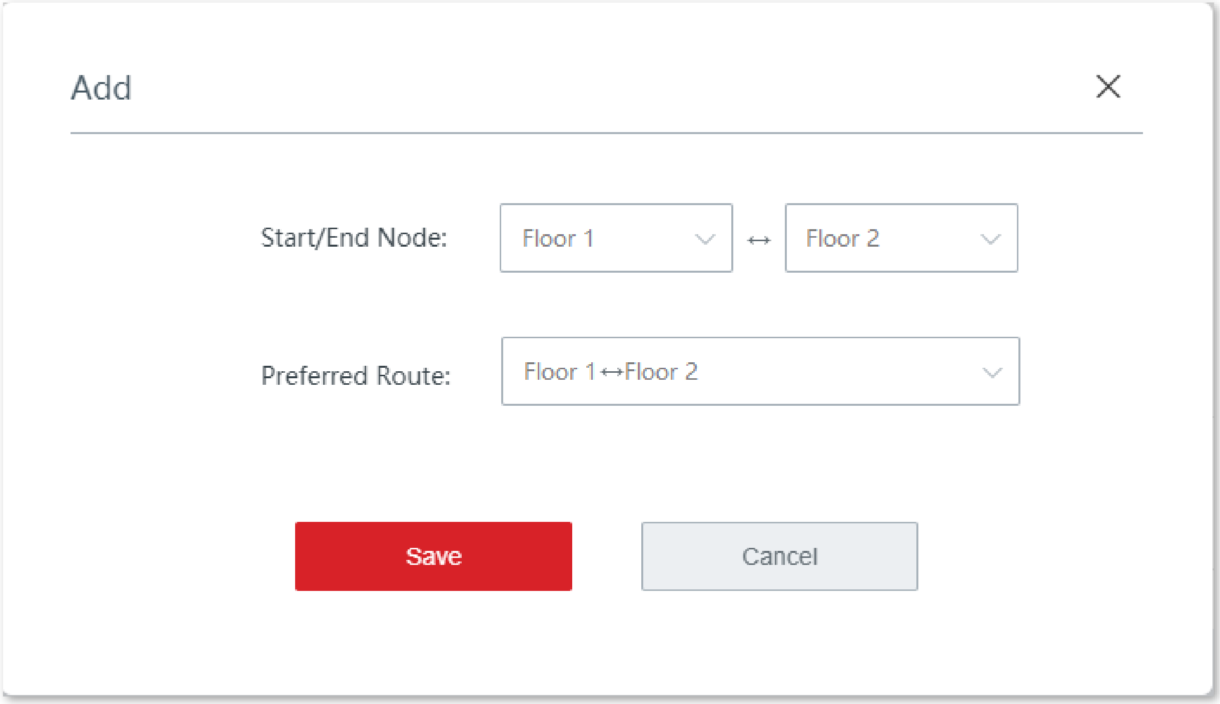
– modify the preferred transmission path between two nodes.

– delete the preferred transmission path between two nodes.

Add the preferred transmission path for two nodes

You can manually specify the preferred transmission path between two nodes.

1. In the **Communication Routing** module on the **Node Management** > **Topology Routing** page, click **+ Add**.
2. When the configuration completes, click **Save**.

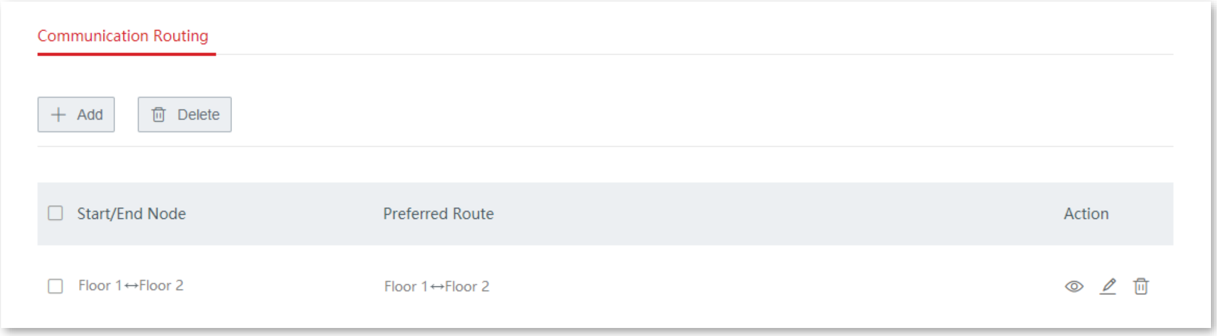


Start/End Node: Floor 1 ↔ Floor 2

Preferred Route: Floor 1↔Floor 2

----End

After the rule of the preferred transmission path is added successfully, you can check the added rule on the **Node Management** > **Topology Routing** > **Communication Routing** page. See the following figure.



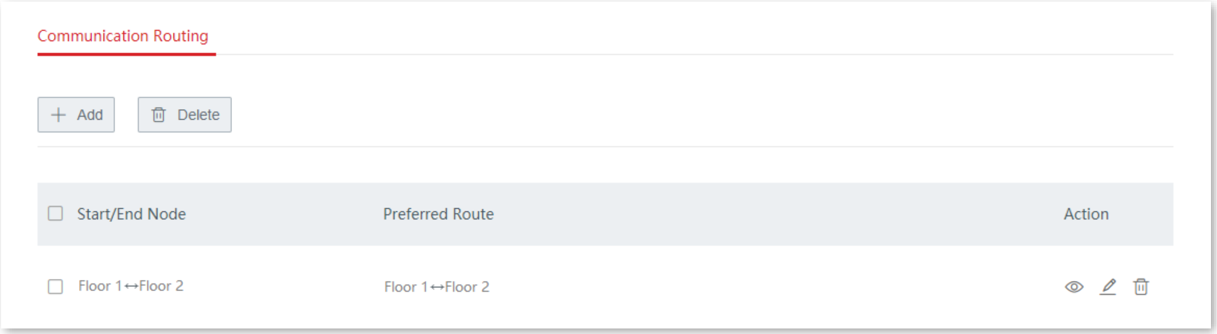
□ Start/End Node	Preferred Route	Action
□ Floor 1↔Floor 2	Floor 1↔Floor 2	

Parameter description

Parameter	Description
Start/End Node	Click the drop-down list to select the start and end node. The start node and end node cannot be the same.
Preferred Route	Click the drop-down list to select the preferred transmission path between the two nodes.
Action	It specifies the operations you can perform on the rule. 👁 : Click it to display the preferred transmission path between two nodes in the network topology. ✎: Click it to edit the rule. 🗑 : Click it to delete the rule.

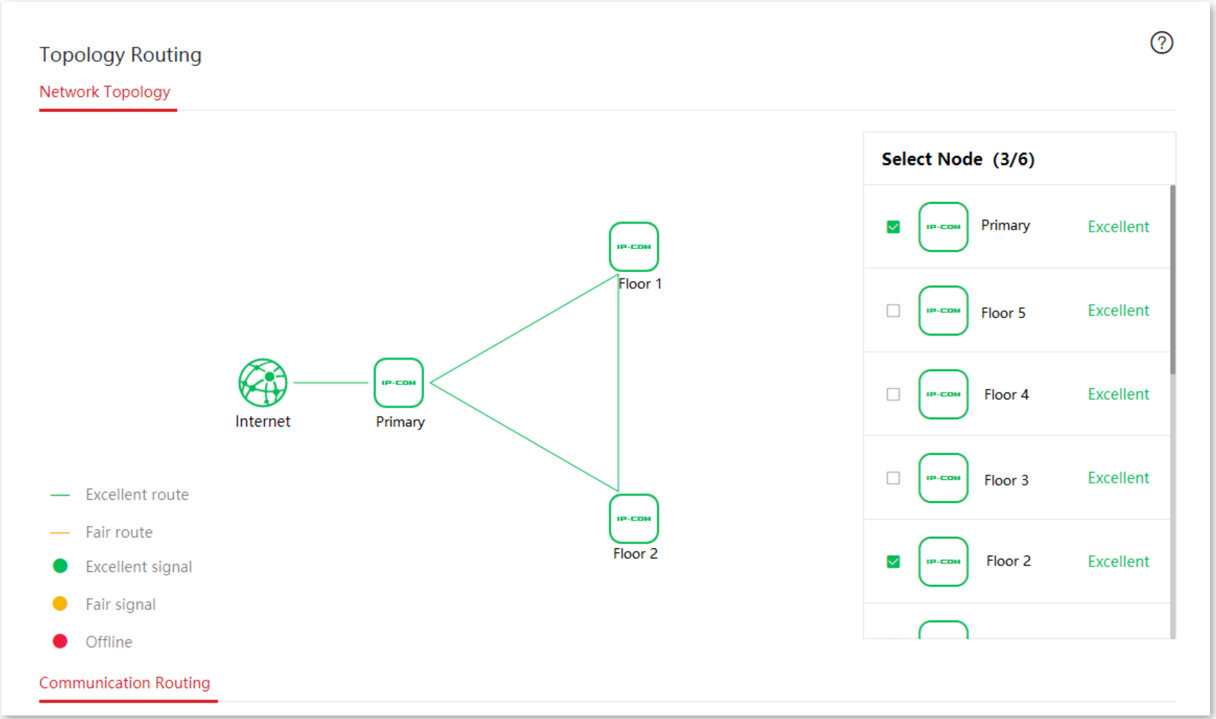
Display the preferred transmission path between two nodes

In the **Communication Routing** module on the **Node Management** > **Topology Routing** page, locate the rules you want to display in the network topology and click 👁 .



□ Start/End Node	Preferred Route	Action
□ Floor 1↔Floor 2	Floor 1↔Floor 2	👁 ✎ 🗑

After clicking 👁 , you can see the preferred transmission path between two nodes in the network topology.



Topology Routing

Network Topology

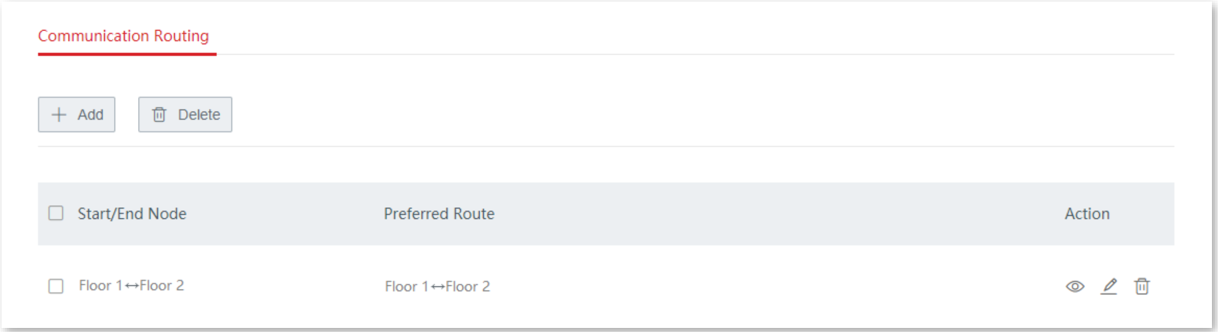
Select Node (3/6)

	Node	Signal
☑	Primary	Excellent
□	Floor 5	Excellent
□	Floor 4	Excellent
□	Floor 3	Excellent
☑	Floor 2	Excellent

Communication Routing

Modify the preferred transmission path between two nodes

1. In the **Communication Routing** module on the **Node Management** > **Topology Routing** page, locate the rule you want to modify and click ✎.



Communication Routing

+ Add   🗑 Delete

□ Start/End Node	Preferred Route	Action
□ Floor 1↔Floor 2	Floor 1↔Floor 2	👁 ✎ 🗑

2. Modify the rule and click **Save**.

----End

After the modification is saved, the new preferred transmission path rule is generated between the two nodes.

Delete the preferred transmission path between two nodes

Delete one path: In the **Communication Routing** module on the **Node Management** > **Maintenance** page, click 🗑 on the row where the target path resides.

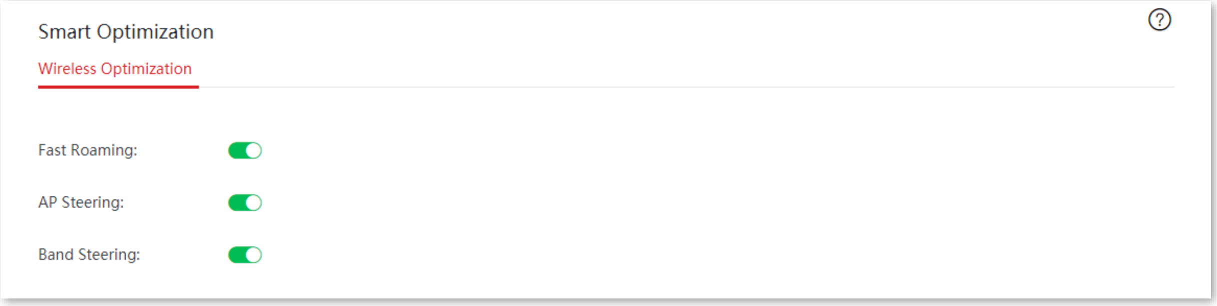
Delete paths in batches: In the **Communication Routing** module on the **Node Management** > **Maintenance** page, select the paths to be deleted and click **Delete**.

3.5 Smart optimization

On this page, you can optimize the whole cable-free system network to enhance the user experience.

Click **Smart Optimization** to enter the page.

On this page, you can control the enabling status of fast roaming, AP steering and band steering to optimize the WiFi experience of the cable-free system.



Smart Optimization

Fast Roaming: ●

AP Steering: ●

Band Steering: ●

Parameter description

Parameter	Description
Fast Roaming	After this function is enabled, clients with 802.11r capabilities are automatically switched to other nodes if the WiFi signal they received from the current node decreases to the threshold value for triggering fast roaming. This process takes only milliseconds. Enabling this function to minimize the effects on services when users are moving across nodes. Note This function requires that all nodes share the same SSID and WiFi password.
AP Steering	After this function is enabled, clients with 802.11k and 802.11v capabilities can obtain the network information of all the nodes and decide whether to switch to other nodes with better network quality accordingly. Enabling this function to disperse clients and ensure that clients connect to more appropriate nodes. Note This function requires that all nodes share the same SSID and WiFi password.
Band Steering	After this function is enabled, the node will guide dual-band clients to connect to the frequency band with the better network quality based on the network quality of all frequency bands. Note This function requires that the 2.4 GHz frequency band and the 5 GHz frequency band of the node share the same SSID and WiFi password.

3.6 Address reservation

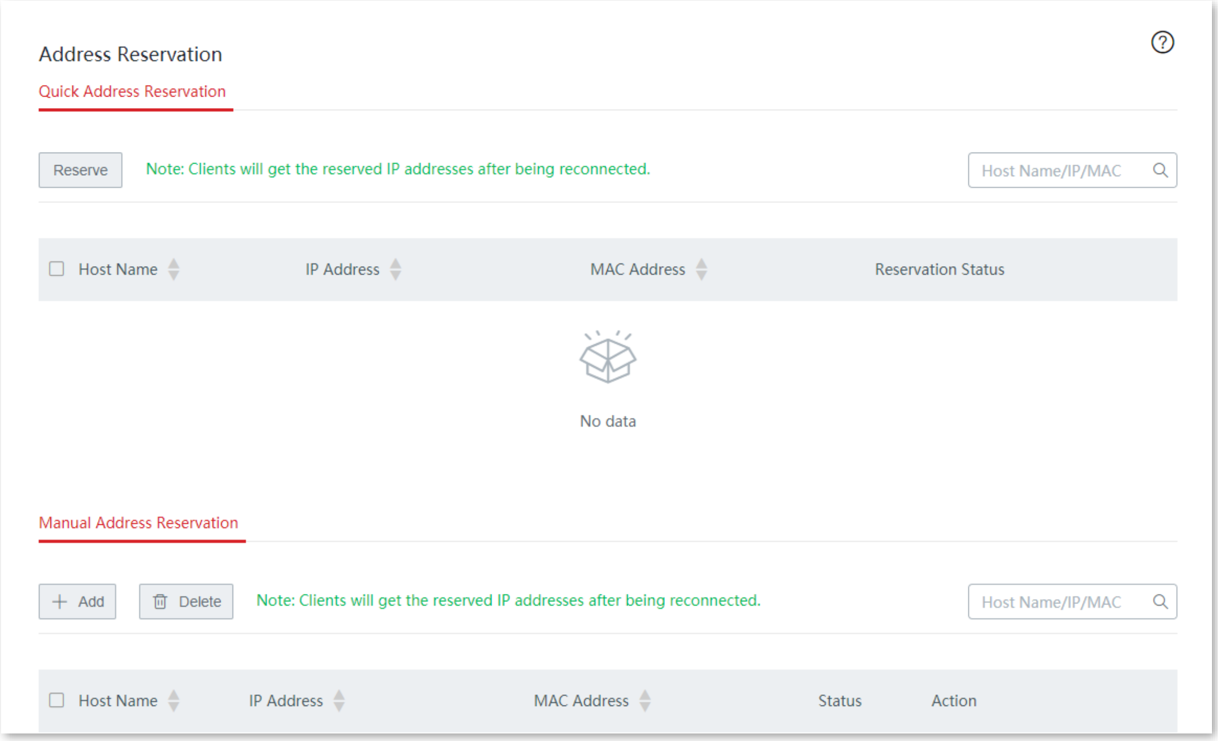
3.6.1 Overview

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

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

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

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



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

□ Host Name	IP Address	MAC Address	Reservation Status

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

□ Host Name	IP Address	MAC Address	Status	Action

Parameter description

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

3.6.2 Configure address reservation

If you want to assign IP address for clients already connecting to the cable-free network, it is recommended that you configure on the **Quick Address Reservation** module. Otherwise, configure on the **Manual Address Reservation** module.

Quick address reservation

Reserve IP address for one client:

On the **Address Reservation** > **Quick Address Reservation** page, locate the client to which you assign a fixed IP address and click **Reserve**.

Reserve IP addresses for multiple clients:

On the **Address Reservation** > **Manual Address Reservation** page, select the clients to which you assign fixed IP addresses and click **Reserve**.

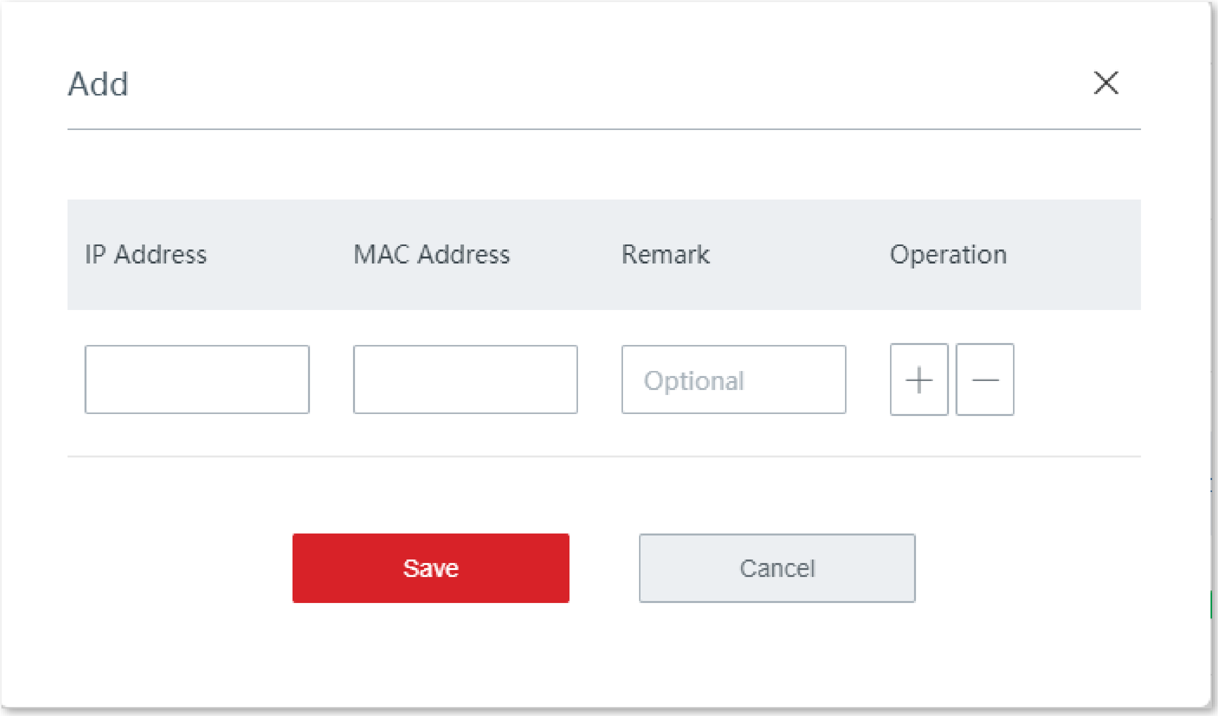
After IP address is reserved successfully, you can check the added rules on the **Address Reservation** > **Manual Address Reservation** page. The rules will take effect the next time when client requests for IP address.

Manual address reservation

On the **Address Reservation** > **Manual Address Reservation** page, click **+ Add**, configure parameters in the pop-up configuration window, and click **Save**.

Tip

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



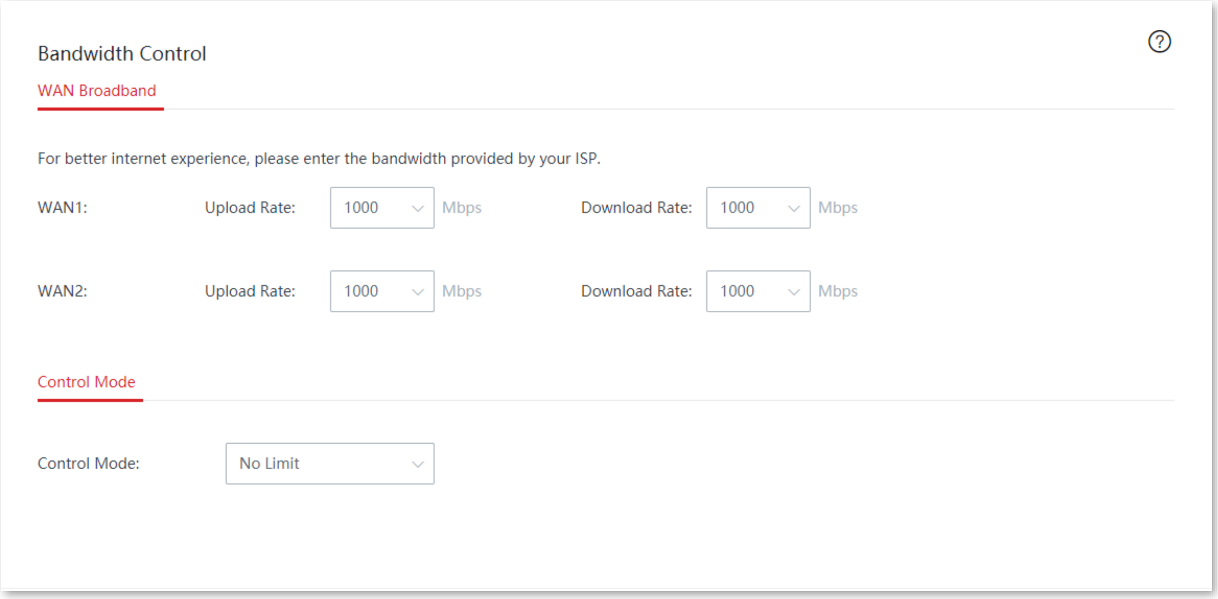
After the rule is added successfully, you can check the added rule on the **Address Reservation** > **Manual Address Reservation** page. The rule will take effect the next time when client requests for IP address.

3.7 Bandwidth control

3.7.1 Overview

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

Click **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

WAN2: Upload Rate: 1000 Mbps Download Rate: 1000 Mbps

Control Mode

Control Mode: No Limit

Parameter description

Parameter		Description
WAN Broadband	Upload Rate	Enter your bandwidth value. If you do not know for sure, please contact your ISP.
	Download Rate	
Control Mode	No Limit	No limitations are set on the upload/download rate of LAN users.
	Manual	The network administrator, based on the actual conditions, set the maximum upload/download rate for each connected client, or set an upload/download rate for all the connected clients. The manual control mode is more flexible compared with the limit by group control mode.
	Auto	The system, based on the WAN upload/download rate set on the **Bandwidth Control** page, evenly distributes bandwidth to LAN users.

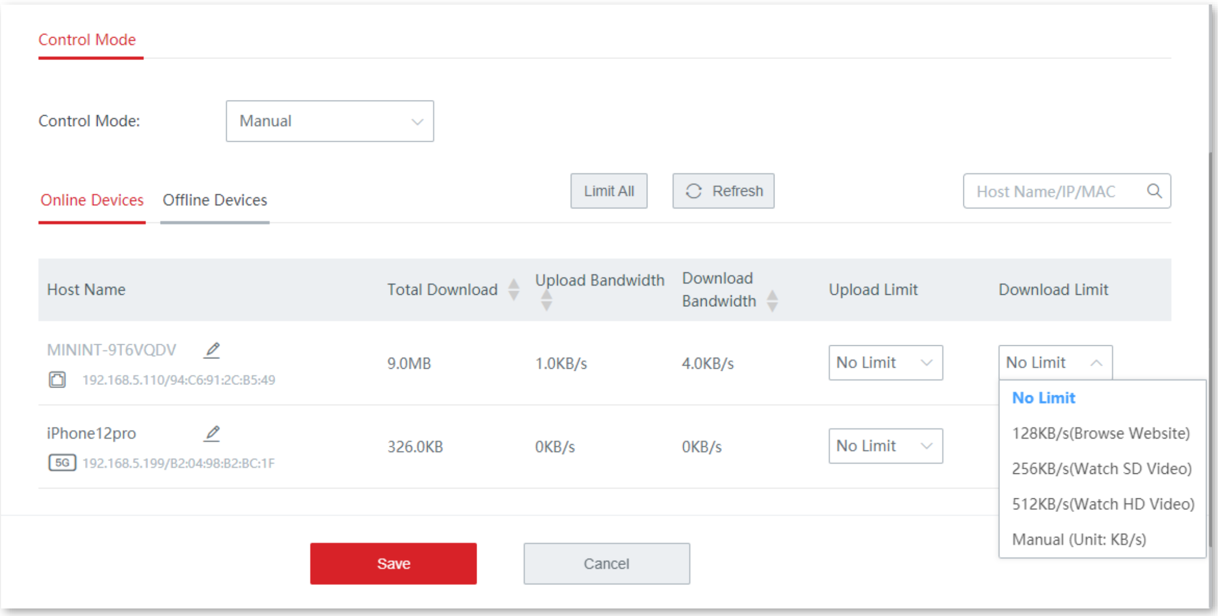
Parameter	Description
Limit By Group	The network administrator, based on the actual conditions, sets rate limit rules for different groups. The network administrator controls the dedicated or shared upload/download rate for users in the specified IP group in the specified time group, and also, sets the concurrent sessions for each client.

3.7.2 Manual

- **Scenario 1: Assume that you want to separately set the maximum upload/download rate for connected clients**

Configuration procedures:

1. Click **Bandwidth Control**.
2. Set **Control Mode** to **Manual**.
3. Choose **Online Devices** or **Offline Devices** as required. **Online Devices** is used for illustration in the following figure.
4. Set the maximum upload/download rate for the target client.
5. Click **Save**.



Control Mode: Manual

Host Name	Total Download	Upload Bandwidth	Download Bandwidth	Upload Limit	Download Limit
MININT-9T6VQDV 192.168.5.110/94:C6:91:2C:B5:49	9.0MB	1.0KB/s	4.0KB/s	No Limit	No Limit
iPhone12pro 5G 192.168.5.199/B2:04:98:B2:BC:1F	326.0KB	0KB/s	0KB/s	No Limit	

----End

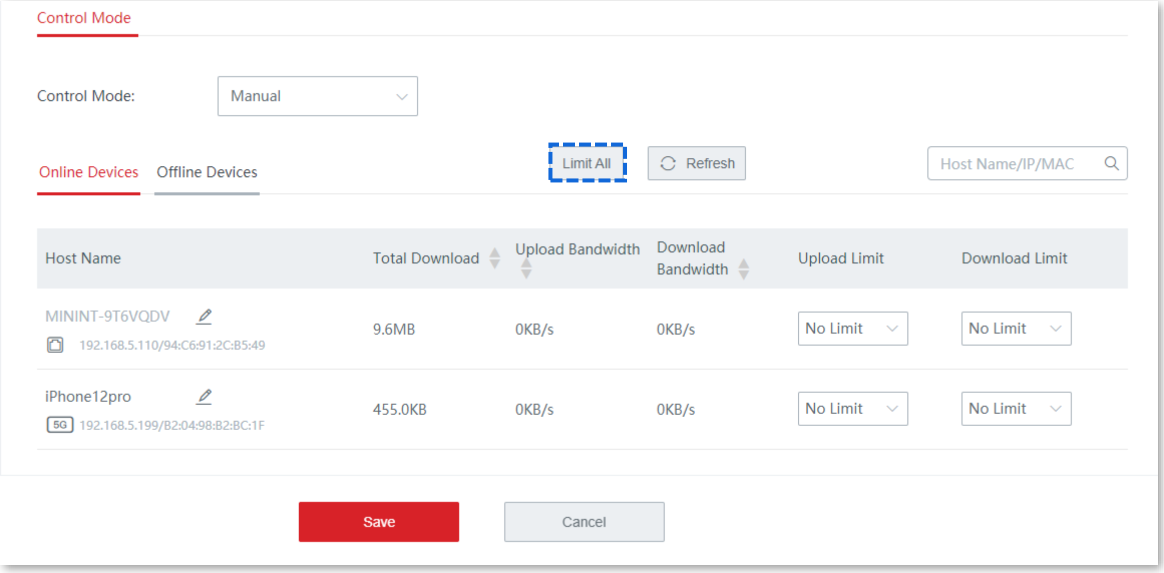
Parameter description

Parameter	Description
Host Name	It specifies the basic information of the client, including the reported client name, the way the client connects to the cable-free network, IP address, and MAC address. You can modify the host name by clicking ✎ as required.
Total Download	It specifies the total volume of the download data.
Offline Time	It specifies the time when the client got offline. This parameter Is available only when you choose **Offline Devices**.
Upload Bandwidth	It specifies the real-time upload/download rate of the client. 1 Mbps=128 KB/s=1024 kb/s.
Download Bandwidth	
Upload Limit	It specifies the maximum upload/download rate the client can use.
Download Limit	

- **Scenario 2: Assume that you want to set a maximum upload/download rate for all the online or offline clients in the LAN**

Configuration procedures:

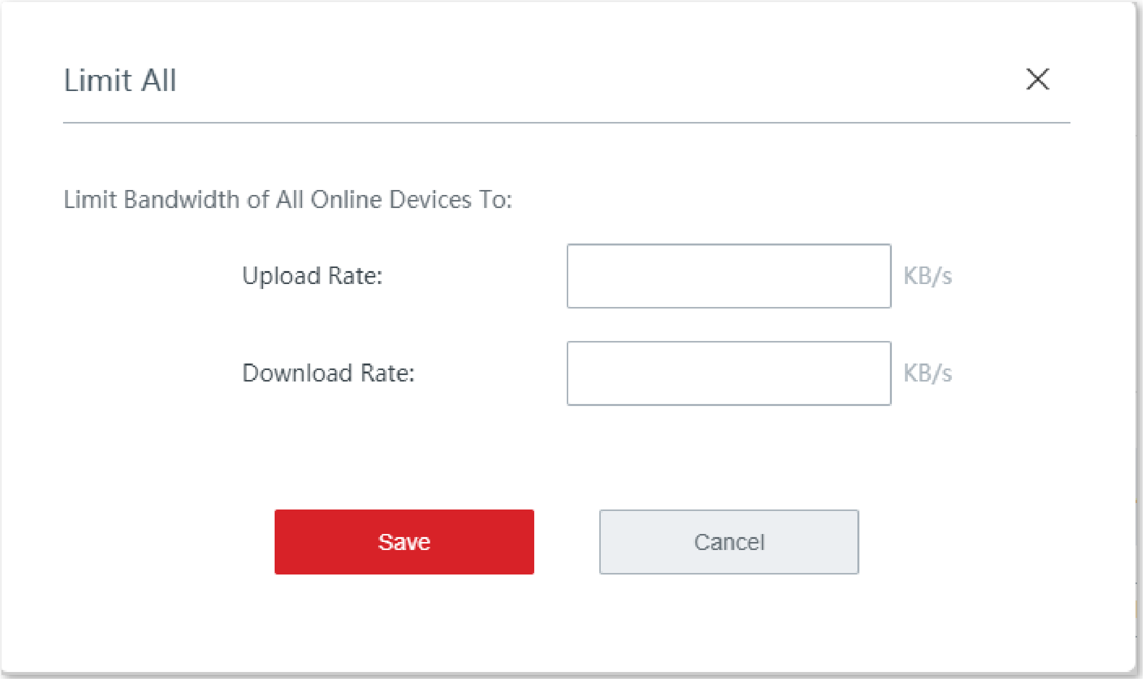
1. Click **Bandwidth Control**.
2. Set **Control Mode** to **Manual**.
3. Choose **Online Devices** or **Offline Devices** as required. **Online Devices** is used for illustration in the following figure.
4. Click **Limit All**.



Control Mode: Manual

Host Name	Total Download	Upload Bandwidth	Download Bandwidth	Upload Limit	Download Limit
MININT-9T6VQDV 192.168.5.110/94:C6:91:2C:B5:49	9.6MB	0KB/s	0KB/s	No Limit	No Limit
iPhone12pro 5G 192.168.5.199/B2:04:98:B2:BC:1F	455.0KB	0KB/s	0KB/s	No Limit	No Limit

5. Set a maximum upload and download rate for all the online (offline) clients in the LAN, and click **Save**.



Limit All

Limit Bandwidth of All Online Devices To:

Upload Rate: KB/s

Download Rate: KB/s

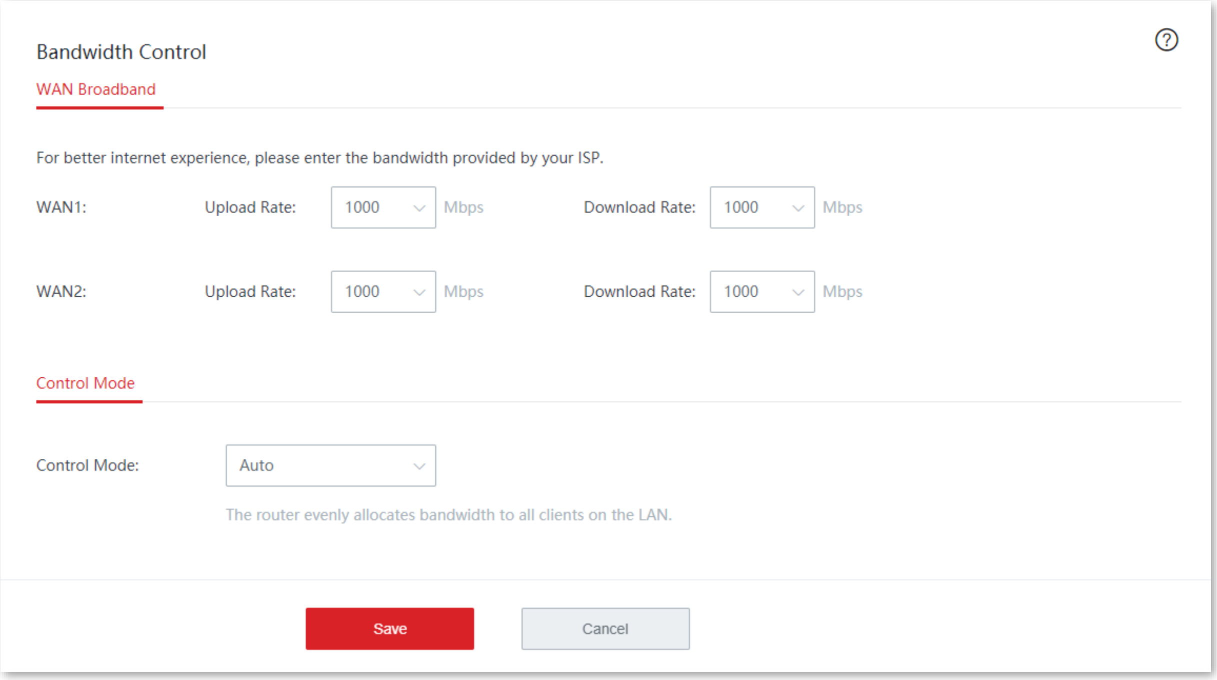
----End

3.7.3 Auto

Distribute bandwidth evenly to the online clients connecting to the cable-free network.

Configuration procedures:

1. Click **Bandwidth Control**.
2. Set the upload/download rate of the target WAN port based on the bandwidth provided by your ISP.
3. Set **Control Mode** to **Auto**.
4. Click **Save**.



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

WAN2: Upload Rate: 1000 Mbps Download Rate: 1000 Mbps

Control Mode

Control Mode: Auto

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

----End

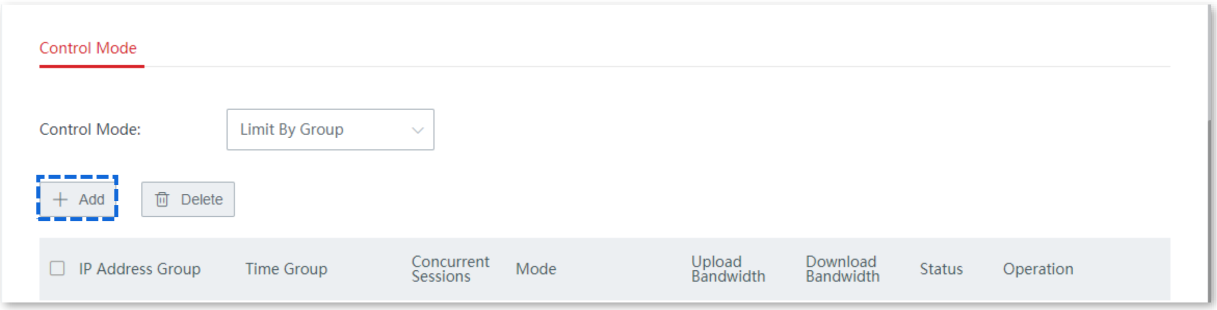
3.7.4 Limit by group

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

Tip

Before configuring limit by group rules, first configure the target IP group and time group.

1. Click **Bandwidth Control**.
2. Set **Control Mode** to **Limit By Group**.
3. Click **+ Add**.

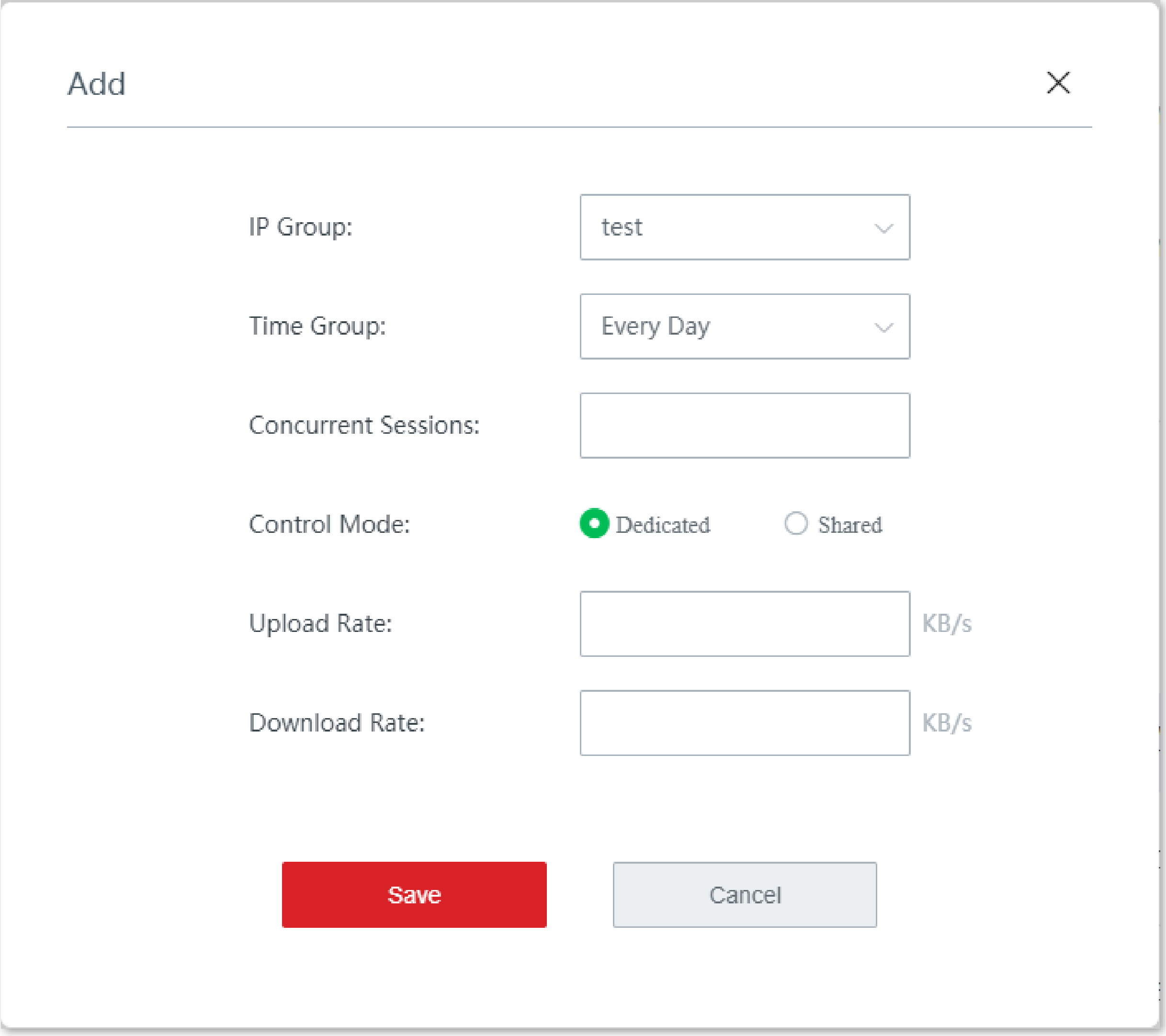


Control Mode

Control Mode: Limit By Group

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

4. Configure parameters in the **Add** window.
5. Click **Save**.



Add

IP Group: test

Time Group: Every Day

Concurrent Sessions:

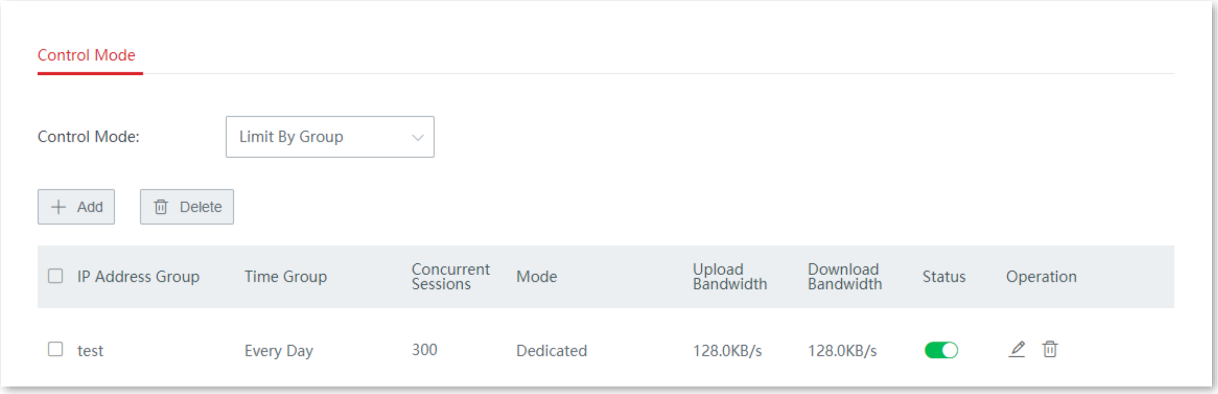
Control Mode: ● Dedicated ○ Shared

Upload Rate: KB/s

Download Rate: KB/s

----End

You can check the added rule on the **Bandwidth Control** page. 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
□	test	Every Day	300	Dedicated	128.0KB/s	128.0KB/s	●	✎ 🗑

Parameter description

Parameter	Description
IP Address Group	It specifies the IP group to be used, which is used to designate the clients with these IP addresses. IP group should be configured in advance on the **Filter Management** > **IP Group/Time Group** page.
Time Group	It specifies the time group to be used, which is used to designate the validity period of the rule. Time group should be configured in advance on the **Filter Management** > **IP Group/Time Group** page.
Concurrent Sessions (concurrent sessions of each client)	It specifies the maximum number of connections each client within the specified IP address range can use. Unless you have any special requirements, it is recommended to set the parameter to no less than **300**.
Control Mode (bandwidth control method)	It specifies the mode of bandwidth control rules. – **Dedicated**: It specifies that every client within the specified IP address range uses the set upload/download rate. Under this mode, every client obtains the same bandwidth. – **Shared**: It specifies that all clients within the specified IP address range use the set upload/download rate together. Under this mode, every client may obtain different bandwidths.
Upload Rate	It specifies the maximum upload/download rate you set.
Download Rate	
Status	It specifies the status of the rule. You can enable or disable the rule as required.
Operation	It specifies the operations you can perform on the rule. ✎: Click it to edit the rule. 🗑 : Click it to delete the rule.

3.7.5 Example of configuring limit by group rules

Networking requirement

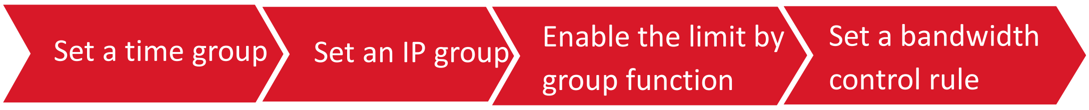
An enterprise uses cable-free devices to set up a network. The enterprise has the following requirements:

During business hours (08:00 to 18:00 every workday), computers with an IP address ranging from 192.168.5.2 to 192.168.5.10 can use a fixed upload and download bandwidth of 1 Mbps. For other clients in the LAN, no bandwidth control rules are added.

Solution

You can use the **Limit By Group** function to meet this requirement. Assume that the concurrent sessions of each client is 300.

Configuration procedures


Set a time group

Set an IP group

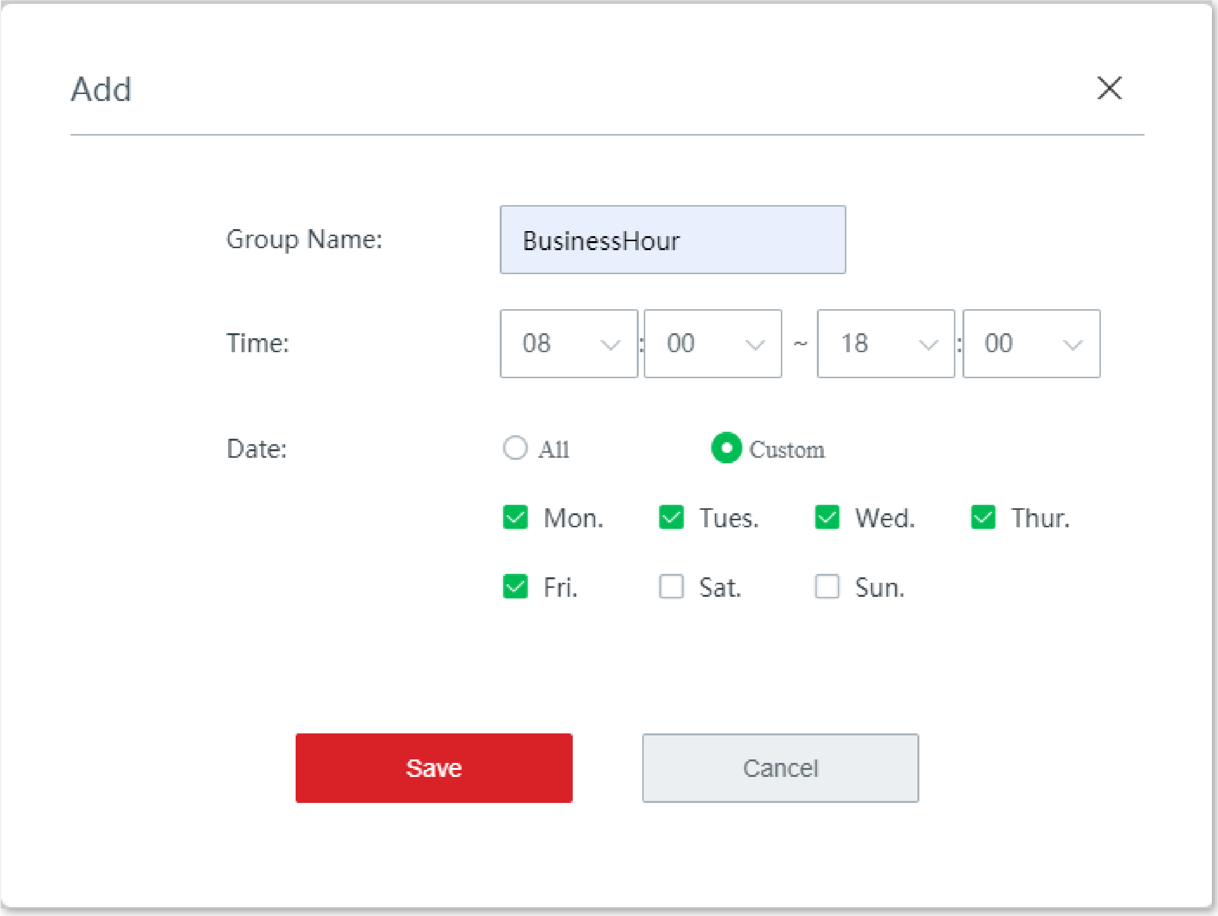
Enable the limit by group function

Set a bandwidth control rule

1. Set a time group.

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

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


Add

Group Name: BusinessHour

Time: 08 : 00 ~ 18 : 00

Date: ○ All ● Custom

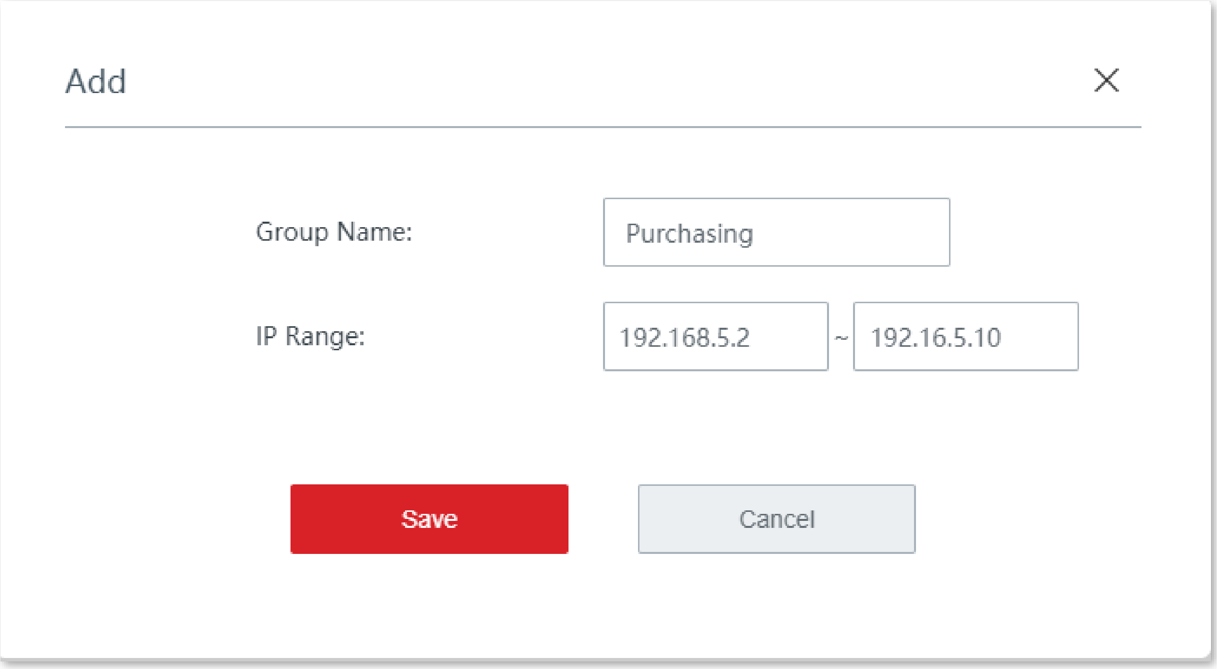
☑ Mon. ☑ Tues. ☑ Wed. ☑ Thur.

☑ Fri. □ Sat. □ Sun.

2. Set an IP group.

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

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

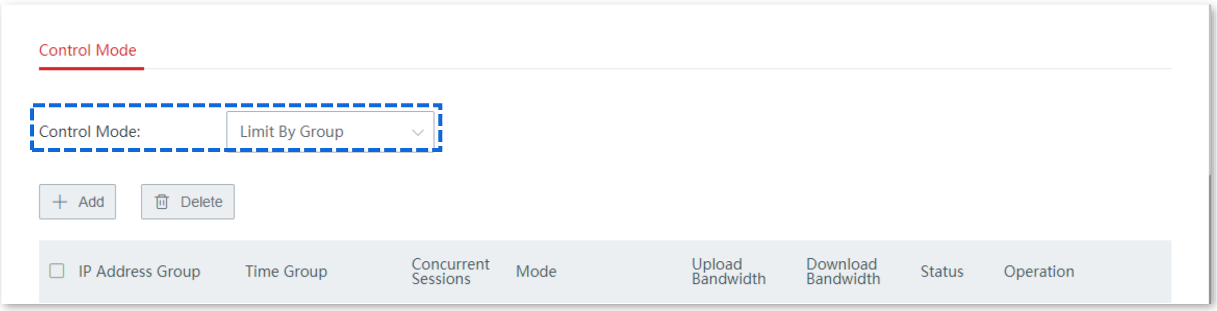


Add

Group Name: Purchasing

IP Range: 192.168.5.2 ~ 192.16.5.10

3. Enable the limit by group function.
   (1) Click **Bandwidth Control** and set **Control Mode** to **Limit By Group**.
   (2) Click **Save**.

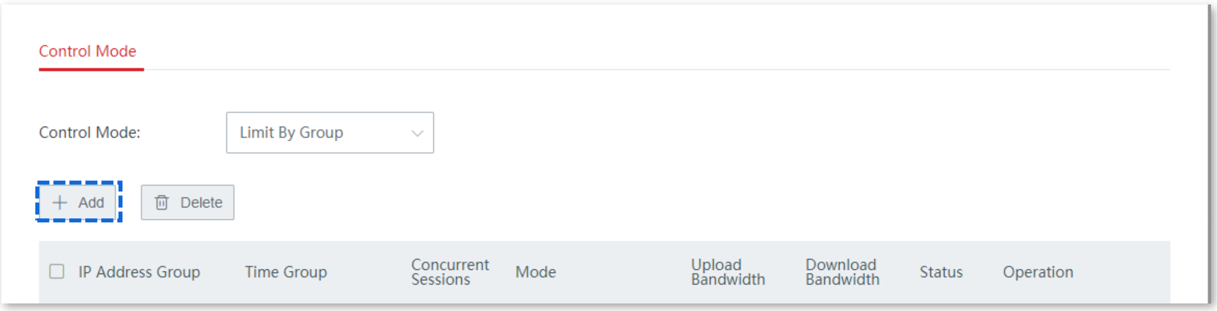


Control Mode

Control Mode: Limit By Group

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

4. Set a bandwidth control rule.
   (1) Click **Bandwidth Control**, and click **+Add**.



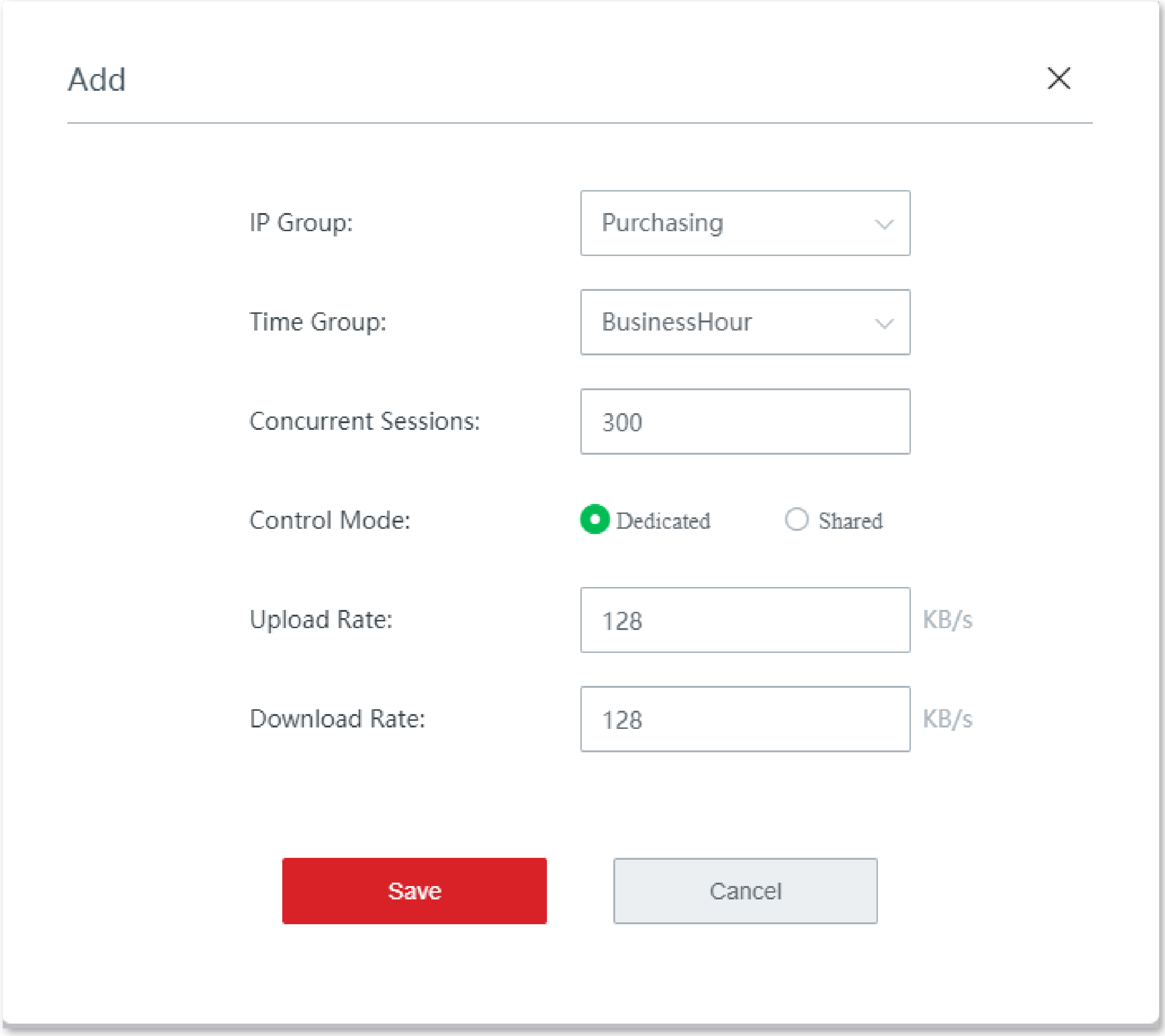
Control Mode

Control Mode: Limit By Group

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

   (2) Configure parameters in the **Add** window, and click **Save**.
      - Click the drop-down list and select the IP group to which this rule applies, which is **Purchasing** in this example.

- Click the drop-down list and select the time group to which this rule applies, which is **BusinessHour** in this example.
- Set the concurrent sessions of each client, which is **300** in this example.
- Set **Control Mode** to **Dedicated**.
- Set the maximum upload/download rate of clients, which are both **128KB/s** in this example.



Add

IP Group: Purchasing

Time Group: BusinessHour

Concurrent Sessions: 300

Control Mode: ● Dedicated ○ Shared

Upload Rate: 128 KB/s

Download Rate: 128 KB/s

----End

Verification

Clients with an IP address ranging from 192.168.5.2 to 192.168.5.10, during 8:00 to 18:00 from Monday to Friday, can use a maximum upload and download rate of 128 KB/s.

3.8 Authentication

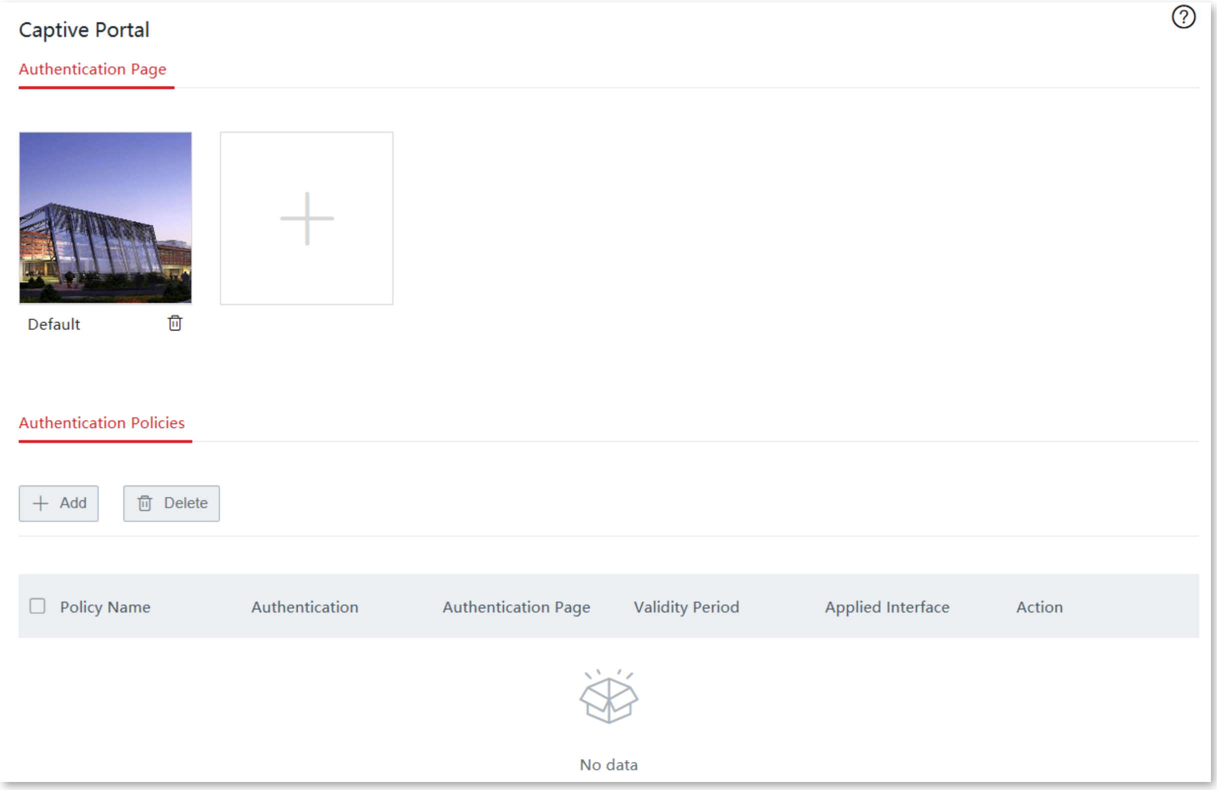
3.8.1 Captive portal

Overview

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

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

Here, you can configure authentication page and authentication policy.



□ Policy Name	Authentication	Authentication Page	Validity Period	Applied Interface	Action

No data

Authenticaiton page

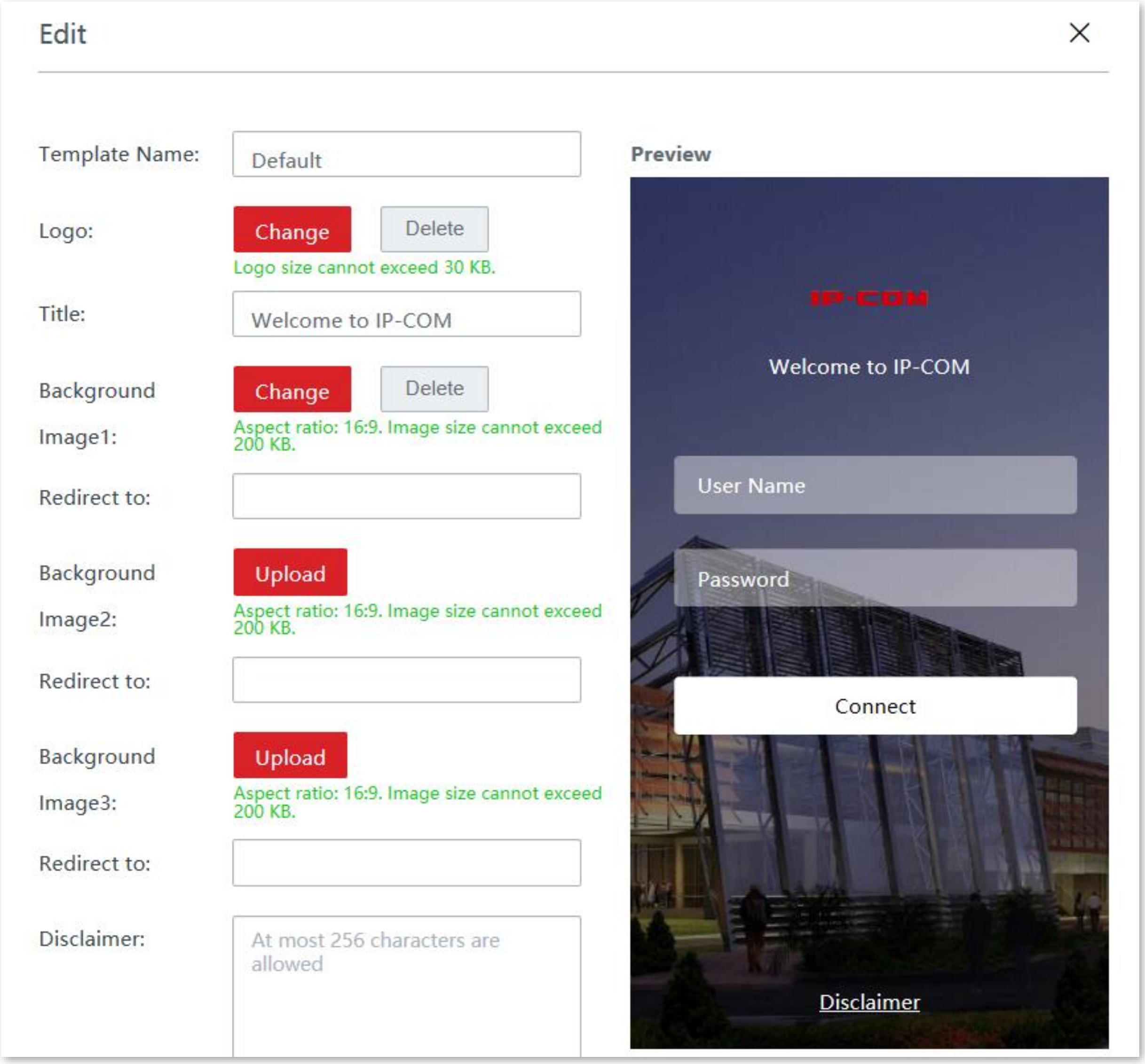
In the **Authentication Page** module on the **Authentication** > **Captive Portal** page, you can:

- Configure authentication page based on default template.
- Create authentication page manually.

Configure authentication page based on default template

Here, you can configure the captive portal authentication page based on the default template.

1. Click **Authentication**, click **Default** in the **Authentication Page** module to enter the configuration window.
2. Configure related parameters, and click **Save**.



Edit

Template Name: Default

Logo: Change Delete

Logo size cannot exceed 30 KB.

Title: Welcome to IP-COM

Background Image1: Change Delete

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

Redirect to:

Background Image2: Upload

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

Redirect to:

Background Image3: Upload

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

Redirect to:

Disclaimer: At most 256 characters are allowed

Preview

IP-COM

Welcome to IP-COM

User Name

Password

Connect

Disclaimer

----End

Parameter description

Parameter	Description
Template Name	It specifies the name of the web authentication page template. By default, the name is **Default**.
Logo	It specifies the logo image of the web authentication page. Click **Change** to change the logo picture, and click **Delete** to delete the uploaded picture.
Title	It specifies the title information of the web authentication page. By default, the title is **Welcome to IP-COM**.
Background Image	It specifies the background image of the web authentication page. Click **Change** to change the picture, and click **Delete** to delete the uploaded picture. Tip When two background images are uploaded, those two images will be displayed in turn on the web authentication page.
Redirect to	It specifies the URL linked to the background image. After the configuration completes, you can access the website by clicking the background image on the authentication page. Tip The URL should be an HTTP website; otherwise, the function does not take effect.
Disclaimer	It specifies the disclaimer information on the web authentication page.
Redirect to	It specifies the web address users are automatically redirected to after passing the authentication. – Previous Page: After users pass the authentication, the browser redirects to the web address users visited before the authentication. For example, if the user is visiting Google when being redirected to the authentication page, he will be redirected back to Google after he passed the authentication. – Specified Page: After users pass the authentication, the browser redirects to the address specified here.

Create authentication page manually

Here, you can also create an authentication page manually.

1. Click **Authentication** > **Captive Portal**, and click + in the **Authentication Page** module to enter the configuration window.
2. Configure related parameters, and click **Save**.

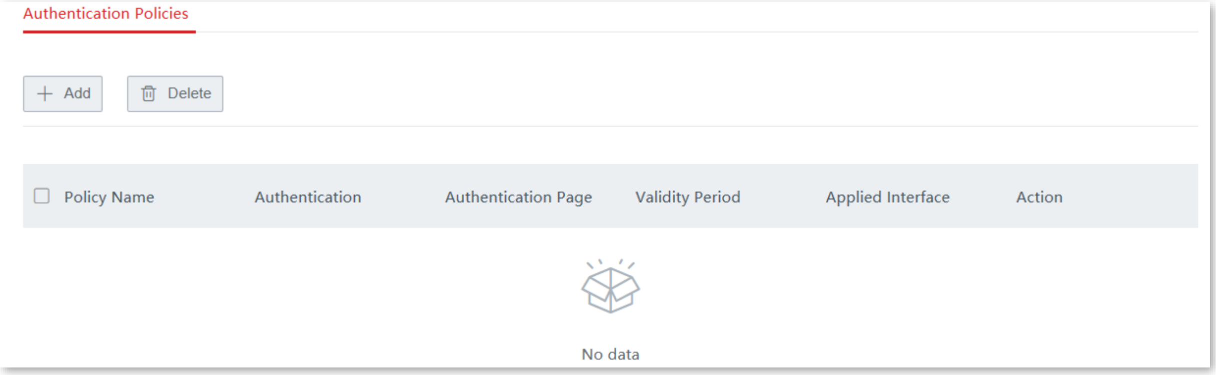
----End

Authentication policies

Click **Authentication** > **Captive Portal** to enter the page. In the **Authentication Policies** module, you can configure web authentication policy based on VLAN interface or SSID policy. You can set Authentication, Valid Duration and Authentication Page and other parameters.

Configuration procedures:

1. Click **Authentication** > **Captive Portal**, in the **Authentication Policies** module, click **+ Add**, and configure parameters in the pop-up window.
2. Configure related parameters, and click **Save**.



□ Policy Name	Authentication	Authentication Page	Validity Period	Applied Interface	Action

----End

Parameter description

Parameter	Description
Policy Name	It specifies the name of the authentication policy.
Authentication	It specifies the authentication method adopted by the authentication policy. – With username and password: Users enter the username and password on the prompted captive portal page. The username and password should be added to the Authentication > User Management page. – One-key Authentication: Users gain internet access simply by clicking **Connect** on the prompted captive portal page. – WiFi via SMS: Users enter mobile phone number on the prompted captive portal page and obtain a verification code to access the internet. For detailed parameter description, refer to SMS authentication settings. – Email Authentication: Users enter email account on the prompted captive portal page and obtain a verification code to access the internet. For detailed parameter description, refer to the Email authentication settings.
Authentication Page	It specifies the authentication page adopted by the authentication policy.
Validity Period	It specifies the length of time that internet access lasts after users pass the authentication. When the period expires, users need to perform authentication again to gain internet access.

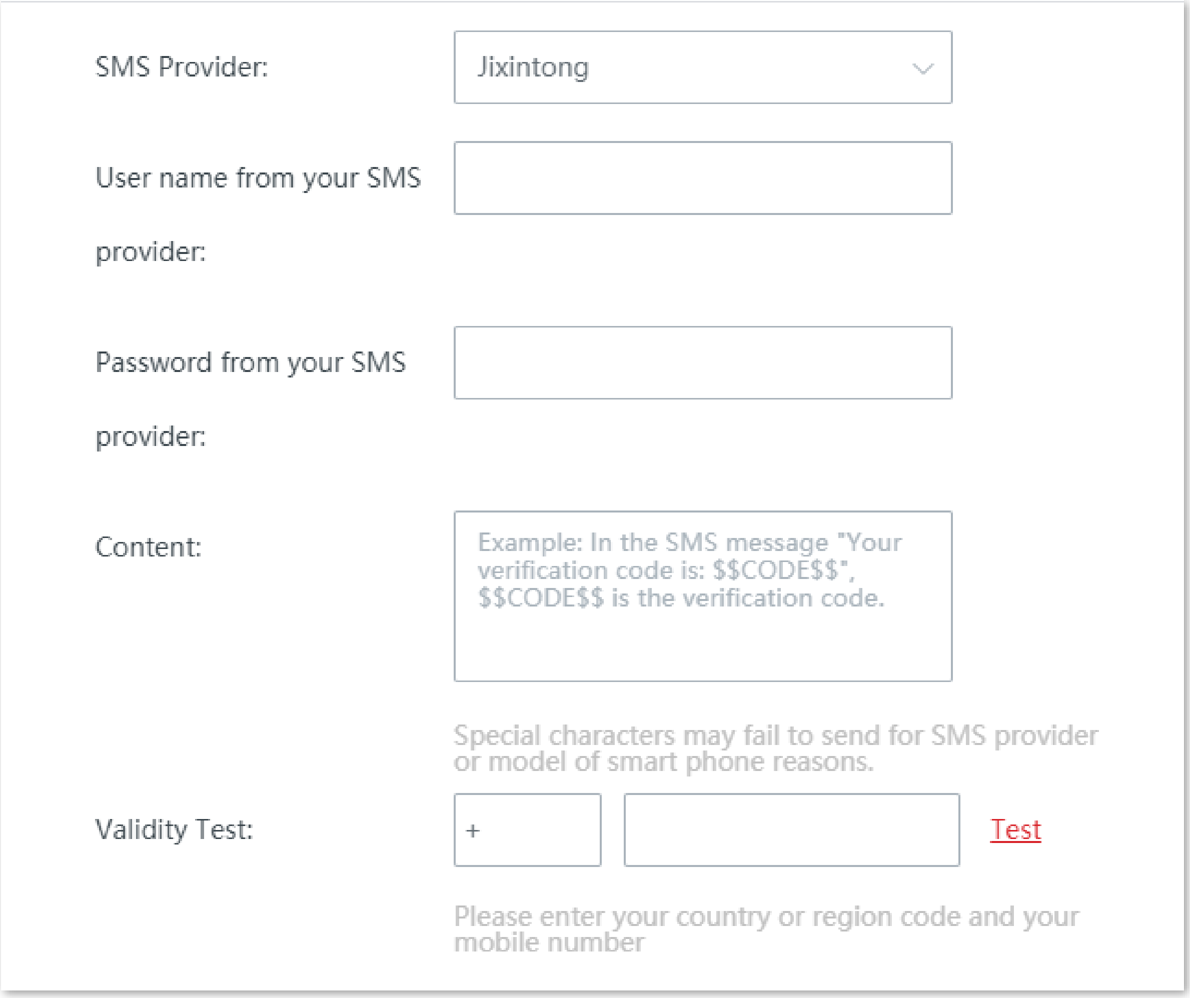
Parameter	Description
Applied Interface	It specifies the interface on which the authentication policy takes effect. It can be a VLAN interface or SSID policy.
Action	It specifies the operations you can perform on the authentication policy. ✎: Click it to edit the authentication policy. 🗑 : Click it to delete the authentication policy.

SMS authentication settings

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

Note

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



SMS Provider: Jixintong

User name from your SMS provider:

Password from your SMS provider:

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

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

Validity Test: + Test

Please enter your country or region code and your mobile number

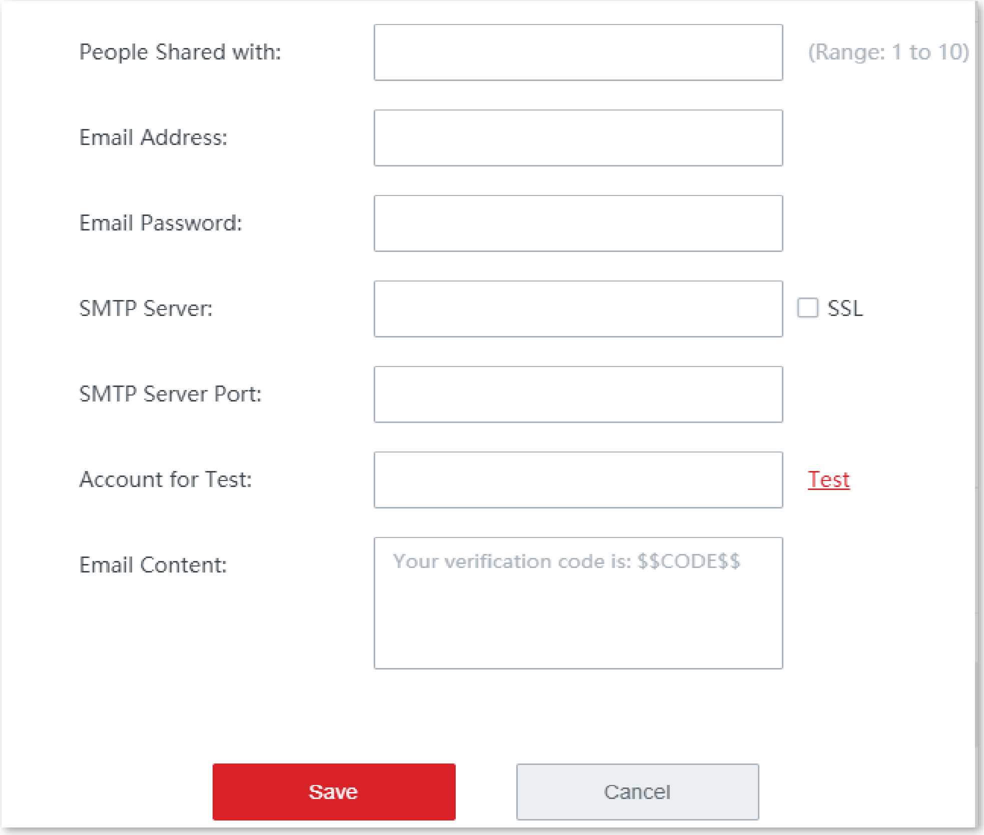
Parameter description

Parameter		Description
Jixintong	User name from your SMS provider	It specifies the user name you applied in Jixintong.
	Password from your SMS provider	It specifies the password of the user name you applied in Jixintong.
	Content	It specifies the SMS content sent to mobile phone through the Jixintong SMS platform. Tip "$$CODE$$" is the format of the SMS verification code and cannot be modified.
	Validity Test	It is used to check whether the interconnection between this cable-free device and SMS provider is successful. Enter the phone number here, and then click the **Test** button. If the interconnection is successful, the phone number will receive a SMS message containing a verification code.
NEXMO	api_key	It specifies the api_key you applied in NEXMO.
	api_secret	It specifies the api_secret you applied in NEXMO.
	Content	It specifies the SMS content sent to mobile phone through the NEXMO SMS platform. Tip "$$CODE$$" is the format of the SMS verification code and cannot be modified.
	Validity Test	It is used to check whether the interconnection between this cable-free device and SMS provider is successful. Enter the phone number here, and then click the **Test** button. If the interconnection is successful, the phone number will receive a SMS message containing a verification code.
Customize HTTP Interconnection	Encoding	It specifies the coding format of SMS content. Please select the coding format supported by the corresponding SMS service provider.
	SMS Gateway URL Interface	Enter the URL interface address of SMS gateway provided by SMS service provider. In general, SMS service providers provide the format of SMS Gateway URL Interface and users need to complete the URL interface address of SMS gateway according to the information applied for in SMS service providers.

Parameter		Description
	Content	It specifies the SMS content sent to mobile phone through the SMS platform. Tip "$$CODE$$" is the format of the SMS verification code and cannot be modified.
	SMS Error Code	Enter the SMS error code of SMS service provider. After the SMS platform fails to send an SMS message, it will send the message to this cable-free device. Users can consult the corresponding SMS service provider based on relevant information. For the specific content of the SMS error code, consult the corresponding SMS service provider.
	Validity Test	It is used to check whether the interconnection between this cable-free device and SMS provider is successful. Enter the phone number here, and then click the **Test** button. If the interconnection is successful, the phone number will receive an SMS message containing a verification code.

Email authentication settings

This cable-free device supports email authentication. Related parameters are as follows.



People Shared with: (Range: 1 to 10)

Email Address:

Email Password:

SMTP Server: □ SSL

SMTP Server Port:

Account for Test:

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

Parameter description

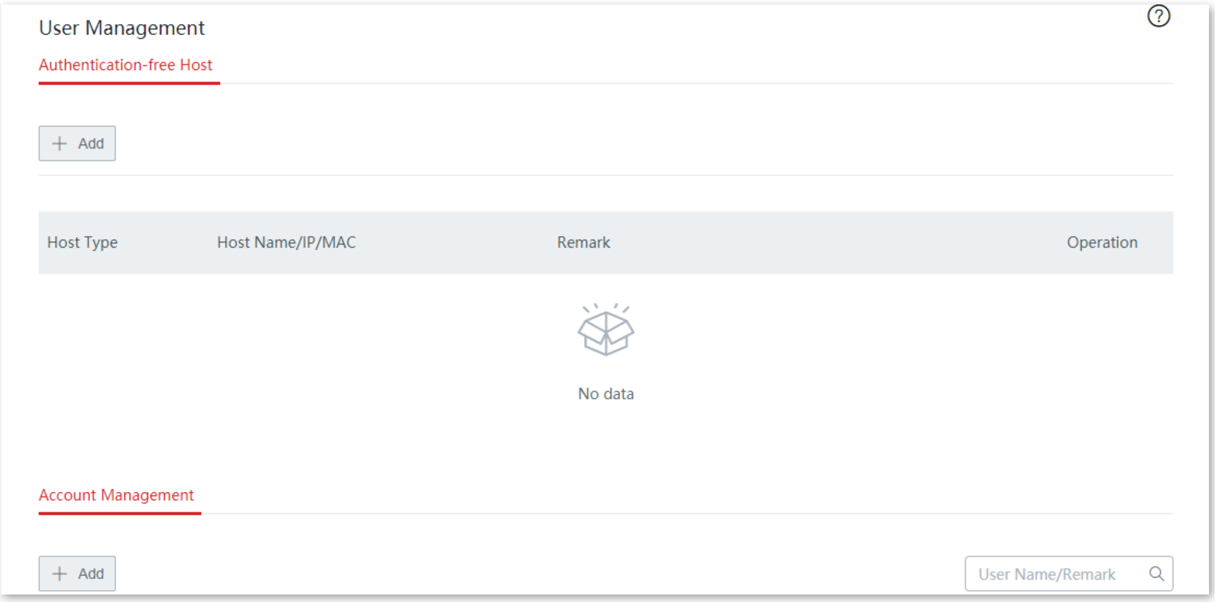
Parameter	Description
People Shared with	It specifies the number of users allowed to access the internet using a same email address.
Email Address	It specifies the email account that sends email.
Email Password	It specifies the password or authorization code of the email account.
SMTP Server	It specifies the SMTP server address. Tip The SMTP (Simple Mail Transfer Protocol) server is a mail delivery server. The address and port of the SMTP server of each mail service provider are different. Please check on your own.
SSL	Secure Sockets Layer, a security protocol. It uses data encryption, identity authentication and message integrity verification mechanism to ensure the security of network data transmission.
SMTP Server Port	It specifies SMTP service port. Tip The SMTP (Simple Mail Transfer Protocol) server is a mail delivery server. The address and port of the SMTP server of each mail service provider are different. Please check on your own.
Account for Test	It specifies the email account, which is used to test whether the email server settings are valid.
Email Content	It specifies the content of the verification code email.

3.8.2 User management

Overview

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

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



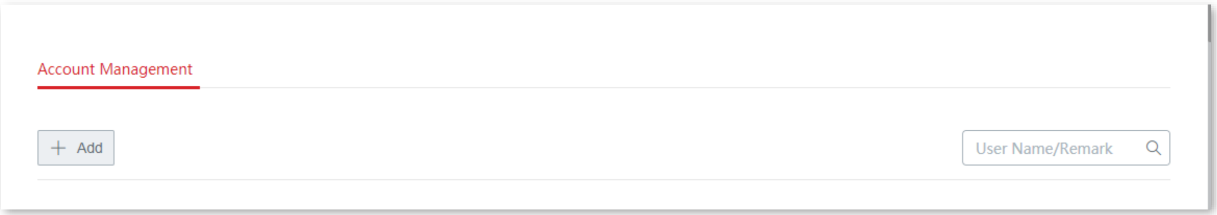
Parameter description

Parameter		Description
Authentication-free Host	Host Type	It specifies by which method you specify an authentication-free host. The cable-free device supports host name, IP address and MAC address.
	Host Name/IP Address/MAC Address	It specifies the information of the authentication-free host. – If you select **Host Name**, enter the host name of the authentication-free device. Please fill in the host name on the System Status page here. If the host name is modified, modify the host name here as well. – If you select **IP Address**, enter the IP address of the authentication-free device. You are recommended to bind the IP address for the device on the **Address Reservation** page. – If you select **MAC Address**, enter the MAC address of the authentication-free device.
	Remark	It specifies the description of the authentication-free device.
	Operation	It specifies the operations you can perform on the rule. ✎: Click it to edit the rule. 🗑 : Click it to delete the rule.
Account Management	User Name	It specifies the user name and password of the authentication account. After the account authentication function is enabled, users need to use this user name and password for authentication on the browser page before gaining internet access.
	Password	

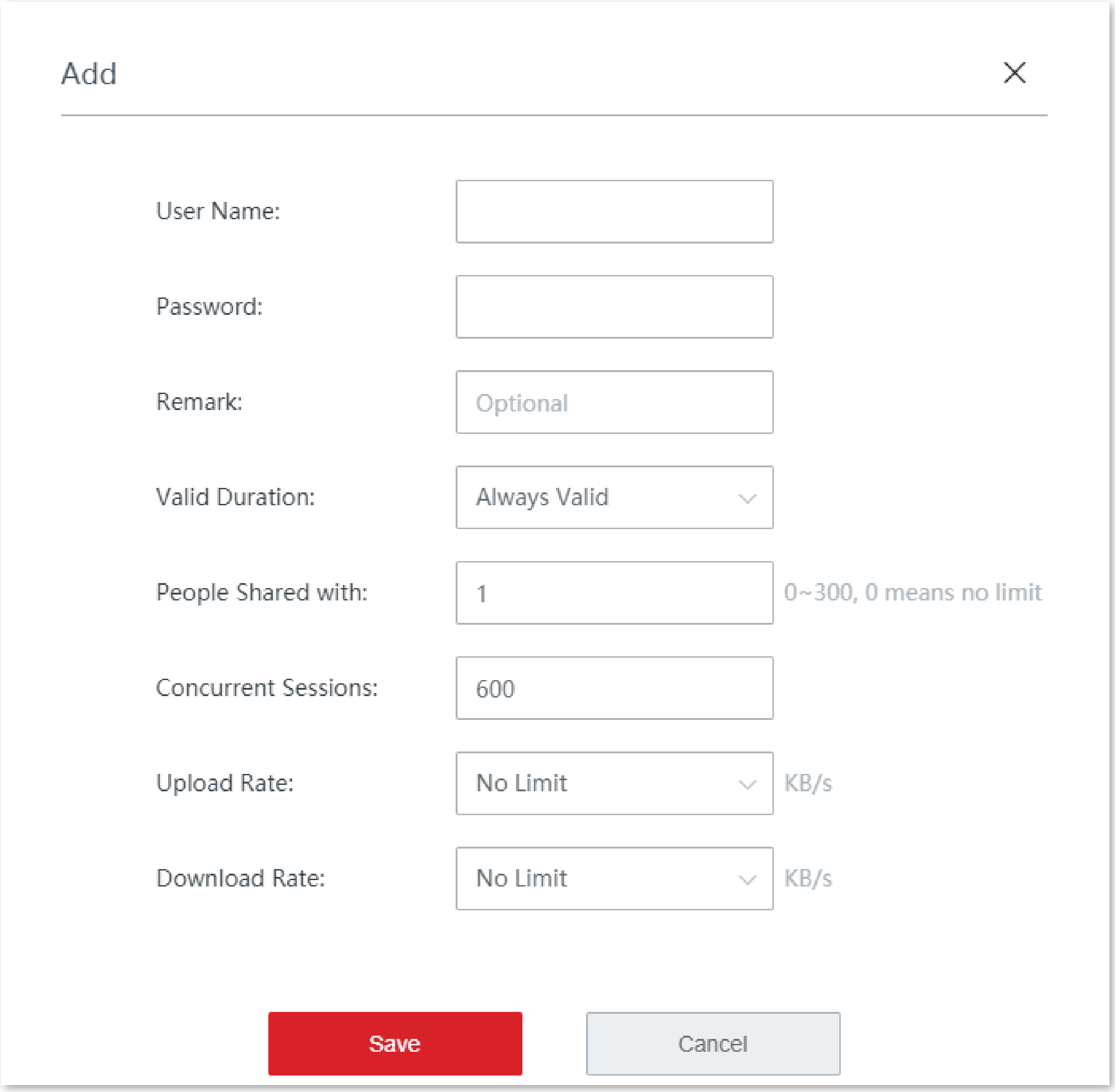
Parameter		Description
	Remark	It specifies the account description information.
	Client Status	It specifies the status of the account (being used or not).
	Valid Duration	It specifies the valid duration of the account. After the duration expires, users cannot use this account for internet access authentication.
	Status	It specifies the status of the rule. You can enable it or disable it as needed.
	Operation	It specifies the operations you can perform on the rule. ✎: Click it to edit the rule. 🗑 : Click it to delete the rule.
	Export	It is used to export the data of the configured authentication user account to the local computer.
	Import	It is used to import the previously exported authentication user account data to the cable-free device.

Add authentication account

1. Click **Authentication** > **User Management**.
2. Click **+ Add**.



3. Set the required parameters in the **Add** window.
4. Click **Save**.



Add

User Name:		
Password:		
Remark:	Optional	
Valid Duration:	Always Valid	
People Shared with:	1	0~300, 0 means no limit
Concurrent Sessions:	600	
Upload Rate:	No Limit	KB/s
Download Rate:	No Limit	KB/s

----End

Description of some parameters

Parameter	Description
People Shared with	It specifies the number of users allowed to access the internet using the same account.
Concurrent Sessions	It specifies the maximum number of concurrent connections each device can set up.
Upload Rate	It specifies the maximum upload/download rate of this account.
Download Rate	

3.8.3 Example of configuring user management

Example of configuring WiFi via SMS

Networking requirement

An enterprise uses the cable-free device to build a network.
In order to standardize the use of network, the requirements are as below.

- Employees connecting to the device’s WiFi network "IP-COM_EE47E8" need authentication when accessing the internet.
- After passing the authentication, employees are redirected to Bing.
- Network administrator does not need authentication when accessing the internet.

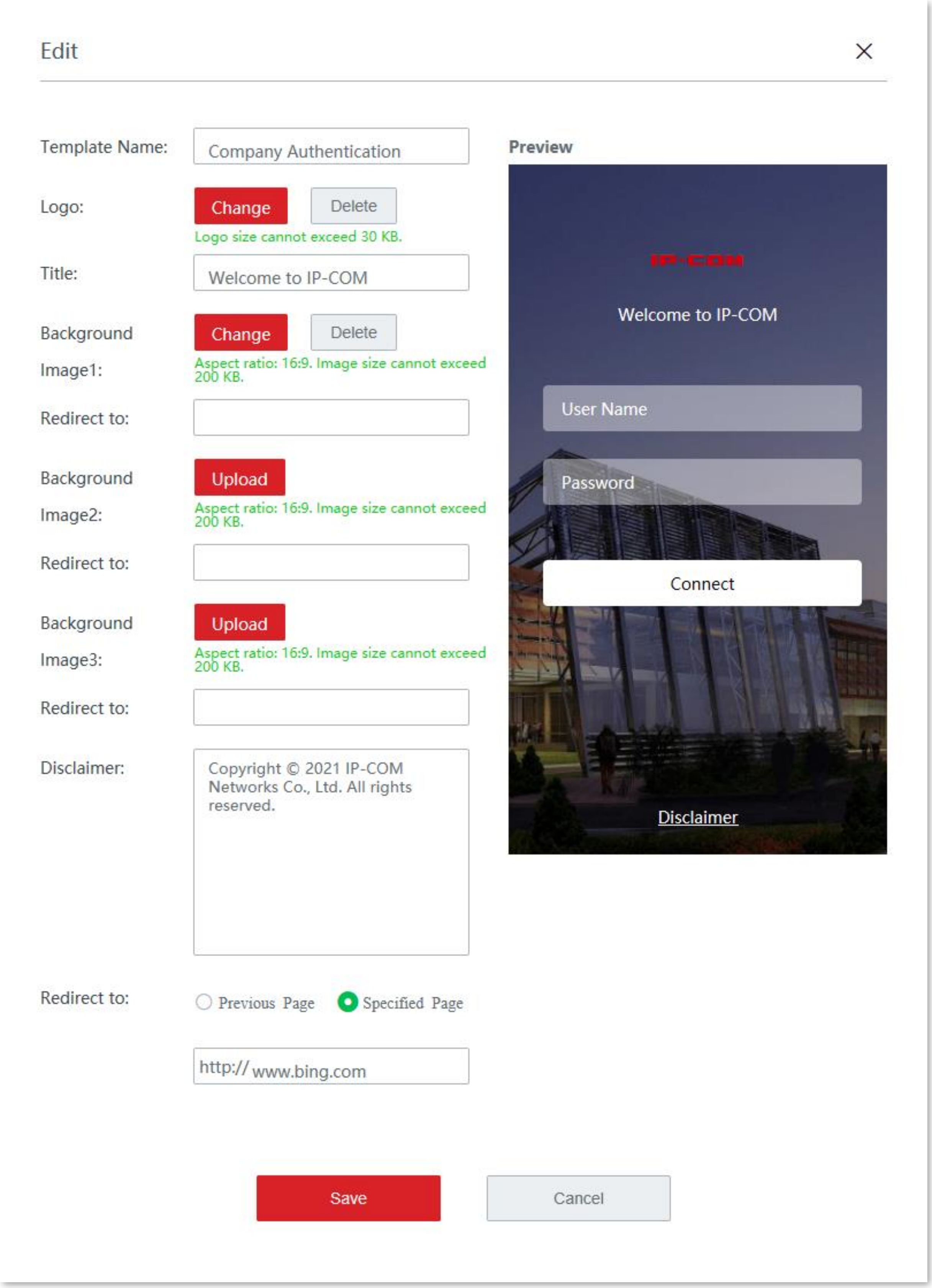
Solution

The above requirements can be achieved through the WiFi via SMS function of the router. Assume that:

- The physical address of the network administrator computer is 94:C6:91:29:C2:C4.
- The account applied by the enterprise in Jixintong is Tom123.
- The password of the account applied by the enterprise in Jixintong is Tom123.

Configuration procedures

1. Configure authentication page information.
   (1) Click **Authentication** > **Captive Portal**.
   (2) In the **Authentication Page** module, click **Default**.
   (3) Modify the following parameters in the pop-up window, and click **Save**.
   - Template Name: Set the name of the template of the authentication page, such as **Company Authentication**.
   - Logo: Click **Change** and upload the company logo image.
   - Title: Set the title of the captive portal page, such as **Welcome to XX**.
   - Background Image: Click **Change** and upload the background image of the captive portal page, such as the enterprise promotion photo.
   - Disclaimer: Set the disclaimer information of the enterprise, such as **Copyright © 2021 XX. All rights reserved**.
   - Redirect to: Choose **Specified Page**, and enter the URL to which the client jumps after passing authentication, which is www.bing.com in this example.



Edit

Template Name: Company Authentication

Logo: Change Delete

Logo size cannot exceed 30 KB.

Title: Welcome to IP-COM

Background Image1: Change Delete

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

Redirect to:

Background Image2: Upload

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

Redirect to:

Background Image3: Upload

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

Redirect to:

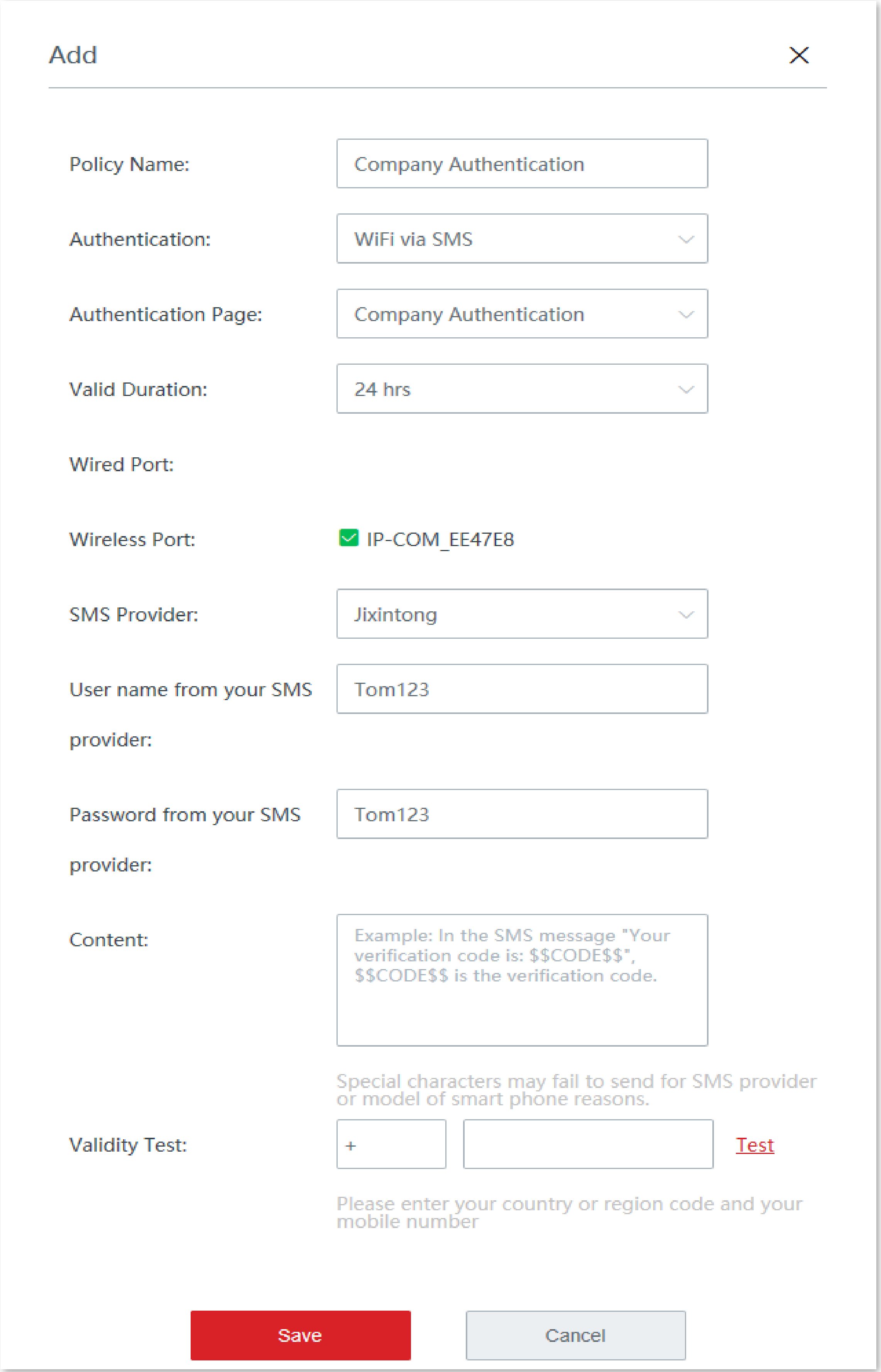
Disclaimer: Copyright © 2021 IP-COM Networks Co., Ltd. All rights reserved.

Redirect to: ○ Previous Page ● Specified Page

http:// www.bing.com

Save Cancel

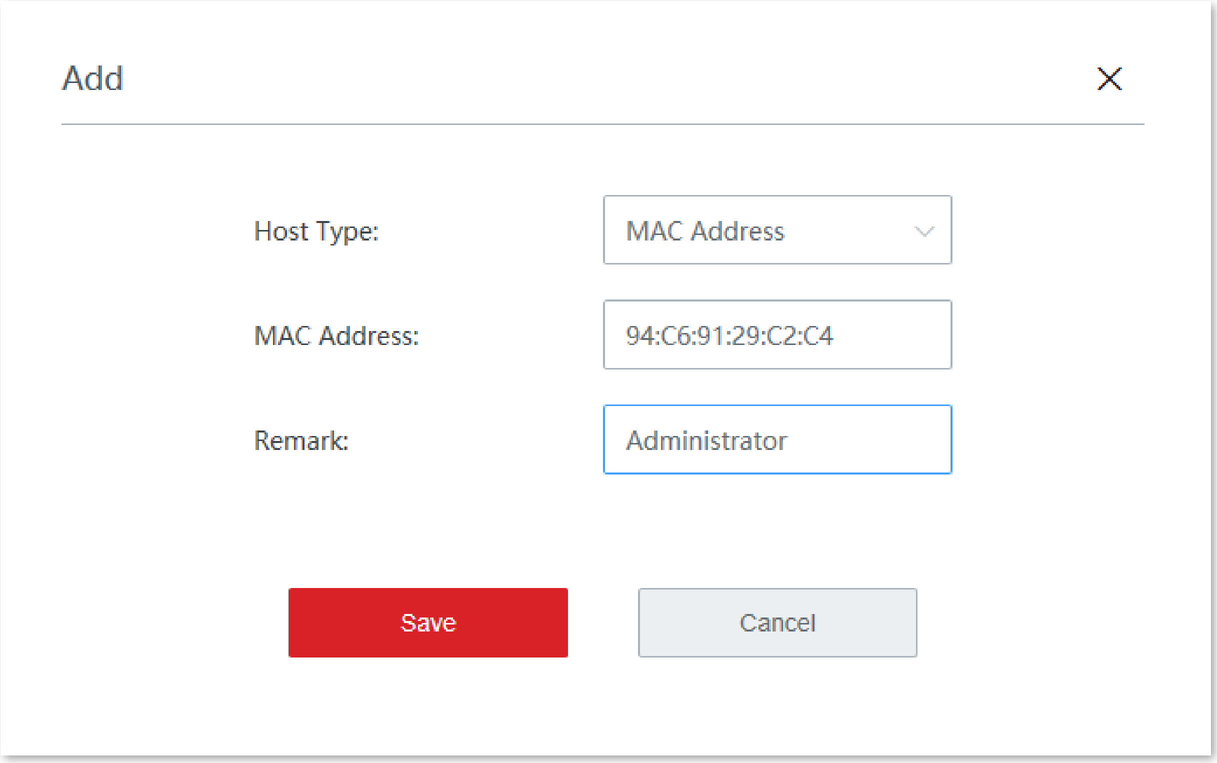
2. Configure WiFi via SMS.
   (1) Click **Authentication** > **Captive Portal**.
   (2) In the **Authentication Policies** module, click **+ Add**.
   (3) Configure the parameters in the pop-up window, and then click **Save** at the bottom of the page.
      - Policy Name: Set the policy name, such as **WiFi via SMS**.
      - Authentication: Set **Authentication** to **WiFi via SMS**.
      - Authentication Page: Set **Authentication Page** to **Company Authentication**.
      - Valid Duration: Set the valid duration for SMS authentication, such as **24 hrs**.
      - Wireless Port: Select the WiFi network requiring SMS authentication, which is **IP-COM_EE47E8** in this example.
      - SMS Provider: Select the SMS provider from which you have purchased an SMS package, which is **Jixintong** in this example.
      - User name from your SMS provider: Enter the user name applied from Jixintong, which is **Tom123** in this example.
      - Password from your SMS provider: Enter the password corresponding to the user name, which is **Tom123** in this example.
      - Content: Set the SMS content sent to the user through the Jixintong SMS platform, such as **Your verification code is $$CODE$$**.
      - Validity test: Used to check whether the interconnection between this cable-free device and SMS provider is successful. Enter the mobile phone number here, and then click the **Test** button. If the interconnection is successful, the phone number will receive an SMS message containing a verification code.



Add

Policy Name:	Company Authentication
Authentication:	WiFi via SMS
Authentication Page:	Company Authentication
Valid Duration:	24 hrs
Wired Port:	
Wireless Port:	☑ IP-COM_EE47E8
SMS Provider:	Jixintong
User name from your SMS provider:	Tom123
Password from your SMS provider:	Tom123
Content:	Example: In the SMS message "Your verification code is: $$CODE$$", $$CODE$$ is the verification code. Special characters may fail to send for SMS provider or model of smart phone reasons.
Validity Test:	+ Test Please enter your country or region code and your mobile number

3. Add authentication-free hosts.
   (1) Click **Authentication** > **User Management**.
   (2) Click **+ Add** in the **Authentication-free Host** module.
   (3) Configure the following parameters in the **Add** window.
      - Host Type: Select the method by which you specify an authentication-free host, which is **MAC Address** in this example.
      - MAC Address: Enter the MAC address of the client, which is **94:C6:91:29:C2:C4** in this example.
      - Remark: Enter a remark of the user, which is **Administrator** in this example.
   (4) Click **save**.



Add

Host Type: MAC Address

MAC Address: 94:C6:91:29:C2:C4

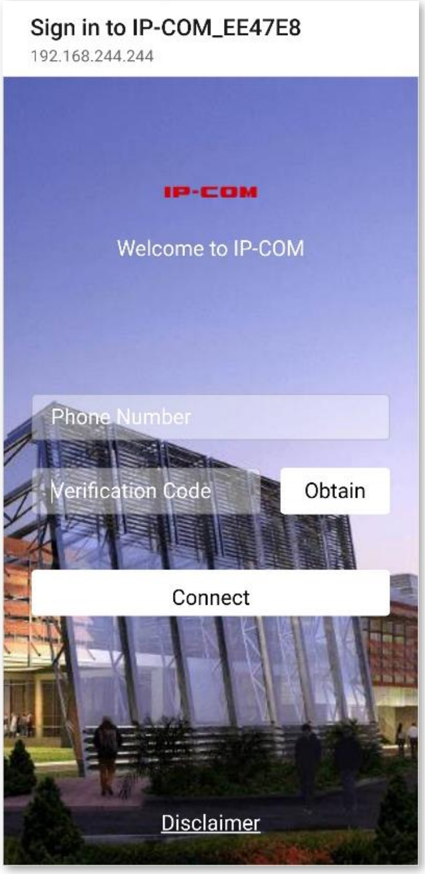
Remark: Administrator

----End

Verification

The network administrator does not need SMS authentication when accessing the internet. Employees need SMS authentication when accessing the internet. The steps are as follows:

1. Visit any website and the browser will automatically redirect to the SMS authentication page.
2. Enter a valid mobile phone number.
3. Click **Obtain** to get verification code.
4. Check the verification code received by your mobile phone.
5. Enter the verification code, and then click **Connect**.


Sign in to IP-COM_EE47E8
192.168.244.244

----End

If the authentication is successful, the browser will automatically redirect to **Bing**.

Example of configuring account authentication

Networking requirement

An enterprise uses the cable-free device to build a network.
In order to standardize the use of network, the requirements are as below:

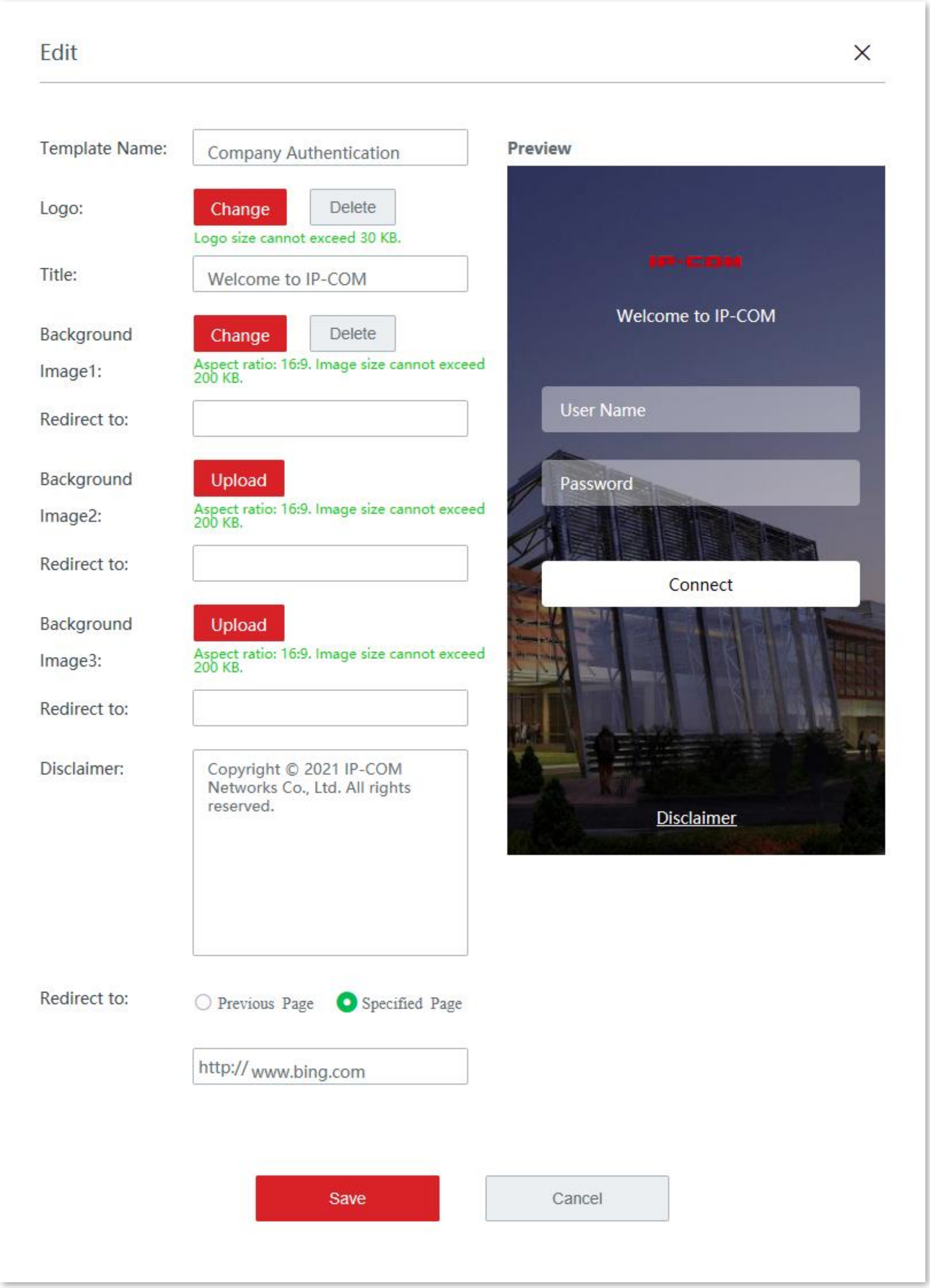
- Employees (10 persons) connecting to the device's WiFi network "IP-COM_EE47E8" need authentication when accessing the internet.
- No limit is set on the upload/download rate for employees.
- After passing the authentication, employees are redirected to Bing.
- Network administrator do not need authentication when accessing the internet.

Solution

The above requirements can be achieved through the account authentication function of the router. Assume that the physical address of the network administrator computer is 94:C6:91:29:C2:C4.

Configuration procedures

1. Configure authentication page information.
   (1) Click **Authentication** > **Captive Portal**.
   (2) In the **Authentication Page** module, click **Default**.
   (3) Modify the following parameters in the pop-up window, and click **Save**.
      - Template Name: Set the name of the template of the authentication page, such as **Company Authentication**.
      - Logo: Click **Change** and upload the company logo image.
      - Title: Set the title of the captive portal page, such as **Welcome to XX**.
      - Background Image: Click **Change** and upload the background image of the captive portal page, such as the enterprise promotion photo.
      - Disclaimer: Set the disclaimer information of the enterprise, such as **Copyright © 2021 XX. All rights reserved**.
      - Redirect to: Choose **Specified Page**, and enter the URL to which the client jumps after passing authentication, which is www.bing.com in this example.



Edit

Template Name: Company Authentication

Logo: Change Delete

Logo size cannot exceed 30 KB.

Title: Welcome to IP-COM

Background Image1: Change Delete

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

Redirect to:

Background Image2: Upload

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

Redirect to:

Background Image3: Upload

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

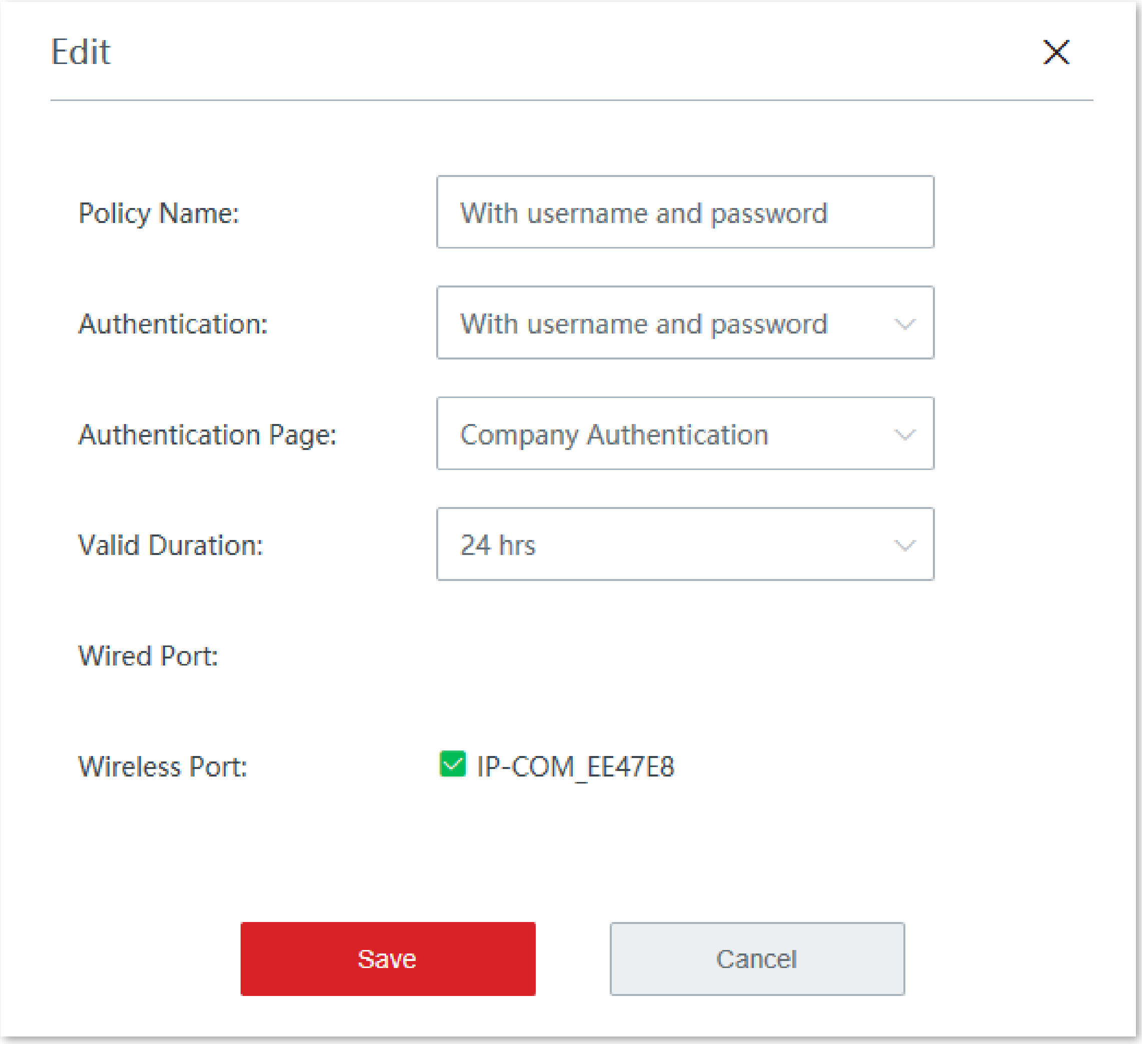
Redirect to:

Disclaimer: Copyright © 2021 IP-COM Networks Co., Ltd. All rights reserved.

Redirect to: ○ Previous Page ● Specified Page

http:// www.bing.com

2. Configure account authentication.
   (1) Click **Authentication** > **Captive Portal**.
   (2) In the **Authentication Policies** module, click **+ Add**.
   (3) Configure the parameters in the pop-up window, and then click **Save** at the bottom of the page.
      - Policy Name: Set the policy name, such as **With username and password.**
      - Authentication: Set **Authentication** to **With username and password**.
      - Authentication Page: Set **Authentication Page** to **Company Authentication**.
      - Valid Duration: Set the valid duration for account authentication, such as **24 hrs**.
      - Wireless Port: Select the WiFi network requiring account authentication, which is **IP-COM_EE47E8** in this example.



Edit

Policy Name: With username and password

Authentication: With username and password

Authentication Page: Company Authentication

Valid Duration: 24 hrs

Wired Port:

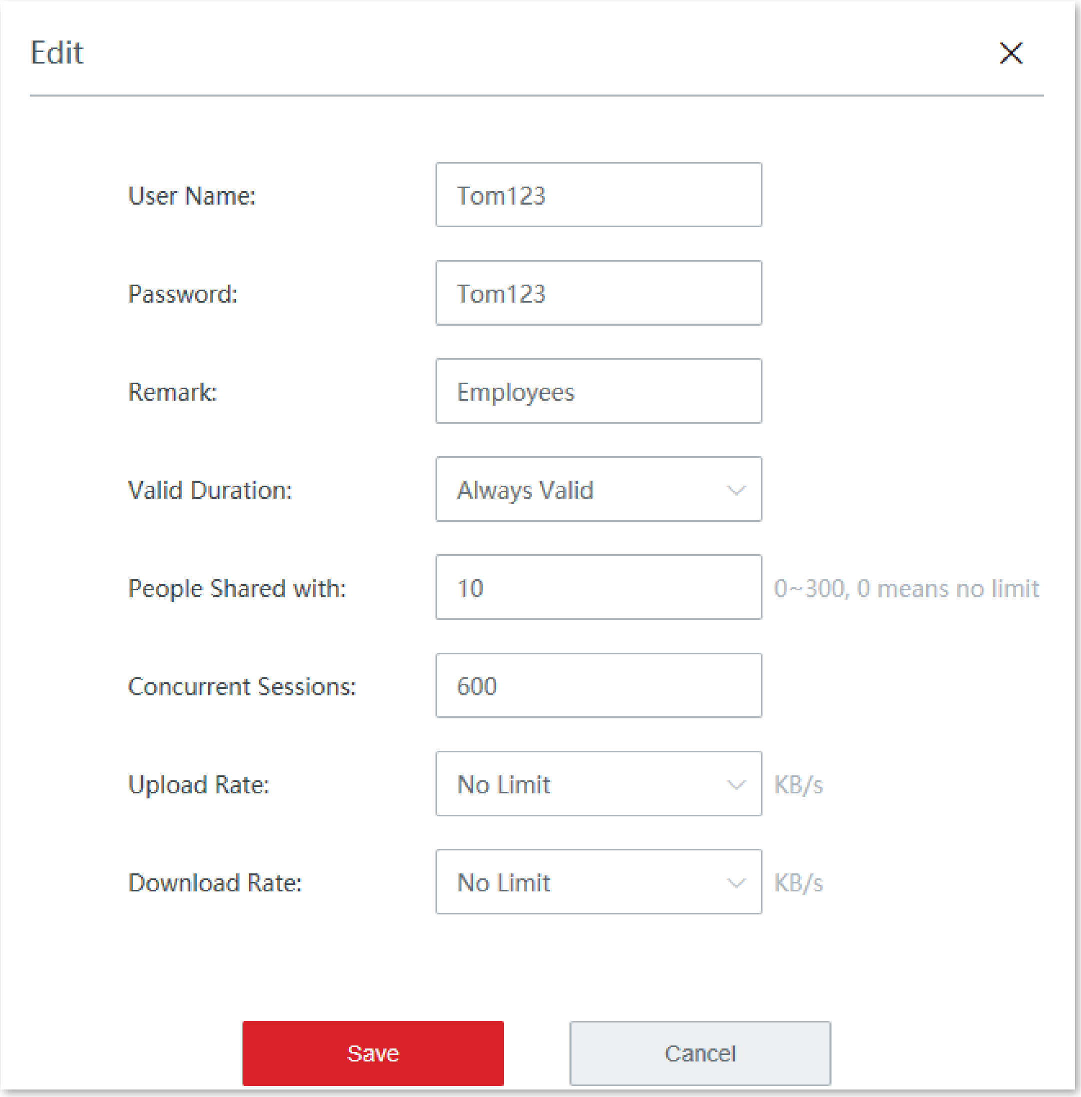
Wireless Port: ☑ IP-COM_EE47E8

3. Add authentication accounts.
   (1) Click **Authentication** > **User Management**.
   (2) Click **+ Add** in the **Account Management** module.

(3) Configure the following parameters in the **Add** window.

- User name: Set the user name for account authentication, such as **Tom123**.
- Password: Set the password corresponding to the user name, such as **Tom123**.
- Remark: Enter the description of the user, such as **Employees**.
- Valid Duration: Set the valid duration for the account, such as **Always Valid**.
- People Shared with: Set the number of users allowed to connect to the internet using this account at the same time, such as **10**.
- Concurrent Sessions: Set the concurrent sessions established by the account device. You are recommended to keep the default settings.
- Upload Rate: Set the maximum upload rate for the account, which is **No Limit** in this example.
- Download Rate: Set the maximum download rate for the account, which is **No Limit** in this example.

(4) Click **save**.



Edit

User Name: Tom123

Password: Tom123

Remark: Employees

Valid Duration: Always Valid

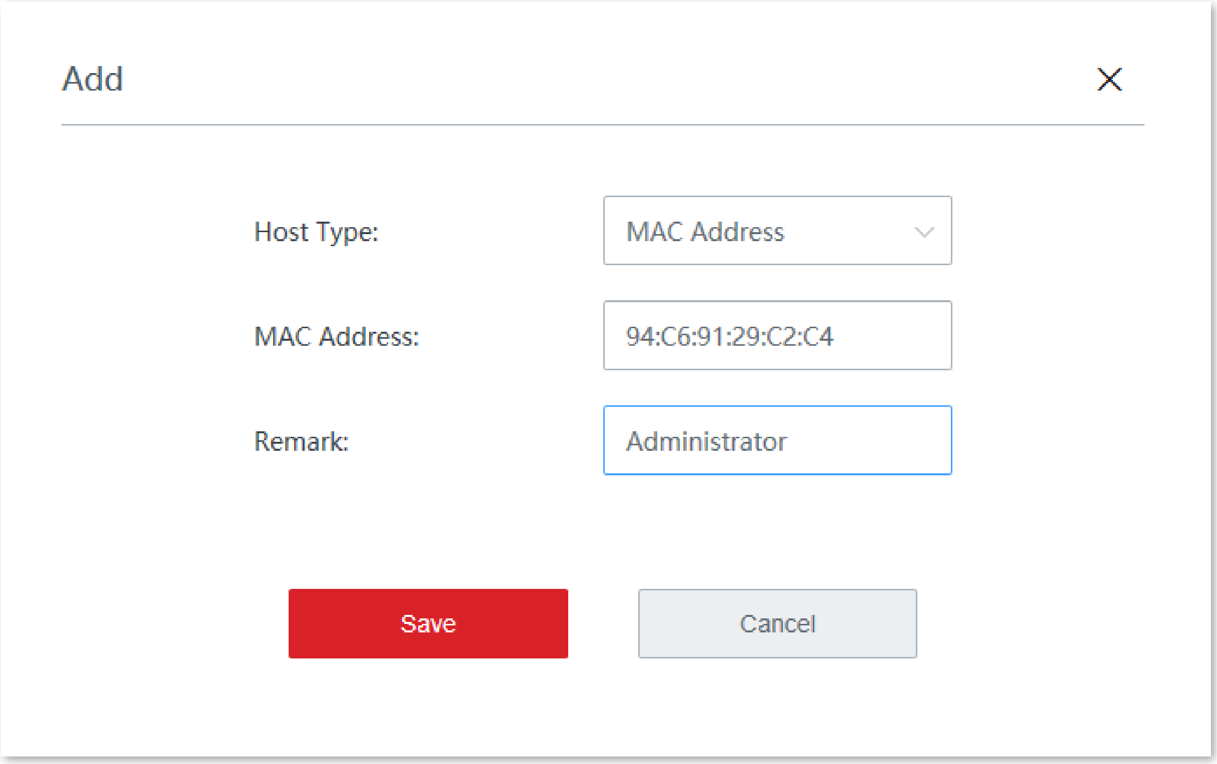
People Shared with: 10 0~300, 0 means no limit

Concurrent Sessions: 600

Upload Rate: No Limit KB/s

Download Rate: No Limit KB/s

4. Add authentication-free hosts.
   (1) Click **Authentication** > **User Management**.
   (2) Click **+ Add** in the **Authentication-free Host** module.
   (3) Configure the following parameters in the **Add** window.
       - Host Type: Select the method by which you specify an authentication-free host, which is **MAC Address** in this example.
       - MAC Address: Enter the MAC address of the client, which is **94:C6:91:29:C2:C4** in this example.
       - Remark: Enter a remark of the user, which is **Administrator** in this example.
   (4) Click **save**.



Add

Host Type: MAC Address

MAC Address: 94:C6:91:29:C2:C4

Remark: Administrator

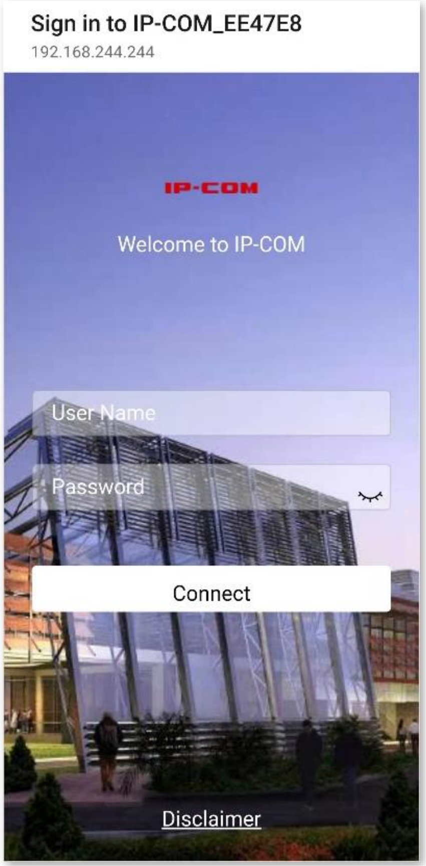
----End

Verification

The network administrator does not need authentication when accessing the internet.

Employees need account authentication when accessing the internet. The steps are as follows:

1. Visit a website and the browser will automatically redirect to the account authentication page.
2. Enter the user name and password.
3. Click **Connect**.



Sign in to IP-COM_EE47E8
192.168.244.244

----End

If the authentication is successful, the browser will automatically redirect to Bing.

Example of configuring email authentication

Networking requirement

An enterprise uses the cable-free device to build a network.
In order to standardize the use of network, the requirements are as below:

- Employees (10 persons) connecting to the device’s WiFi network “IP-COM_EE47E8” need authentication when accessing the internet.
- No limit is set on the upload/download rate for employees.
- After passing the authentication, employees are redirected to Bing.
- Network administrator does not need authentication when accessing the internet.

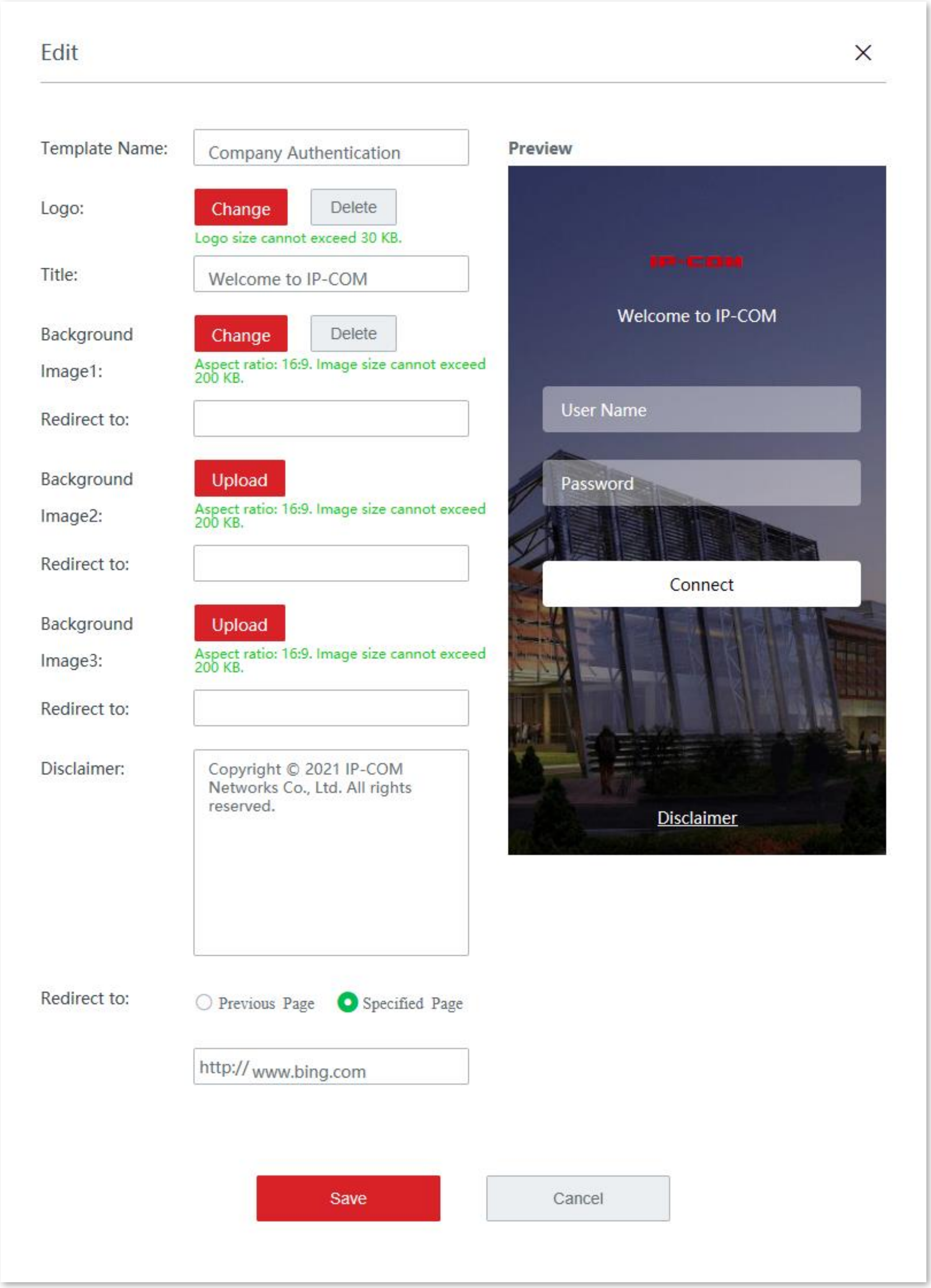
Solution

The above requirements can be achieved through the email authentication function of the device.
Assume that the physical address of the network administrator computer is 94:C6:91:29:C2:C4.
Assume that the basic parameters of the email server are as follows:

- Email Address: Tom@gmail.com
- Email Password: abc123456
- SMTP Server: smtp.gmail.com (SSL enabled)
- SMTP Server Port: 465
- Account for Test: lisi@gmail.com

Configuration procedures

1. Configure authentication page information.
   (1) Click **Authentication** > **Captive Portal**.
   (2) In the **Authentication Page** module, click **Default**.
   (3) Modify the following parameters in the pop-up window, and click **Save**.
      - Template Name: Set the name of the template of the authentication page, such as **Company Authentication**.
      - Logo: Click **Change** and upload the company logo image.
      - Title: Set the title of the captive portal page, such as **Welcome to XX**.
      - Background Image: Click **Change** and upload the background image of the captive portal page, such as the enterprise promotion photo.
      - Disclaimer: Set the disclaimer information of the enterprise, such as **Copyright © 2021 XX. All rights reserved**.
      - Redirect to: Choose **Specified Page**, and enter the URL to which the client jumps after passing authentication, which is www.bing.com in this example.



Edit

Template Name: Company Authentication

Logo:

Logo size cannot exceed 30 KB.

Title: Welcome to IP-COM

Background Image1:

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

Redirect to:

Background Image2:

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

Redirect to:

Background Image3:

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

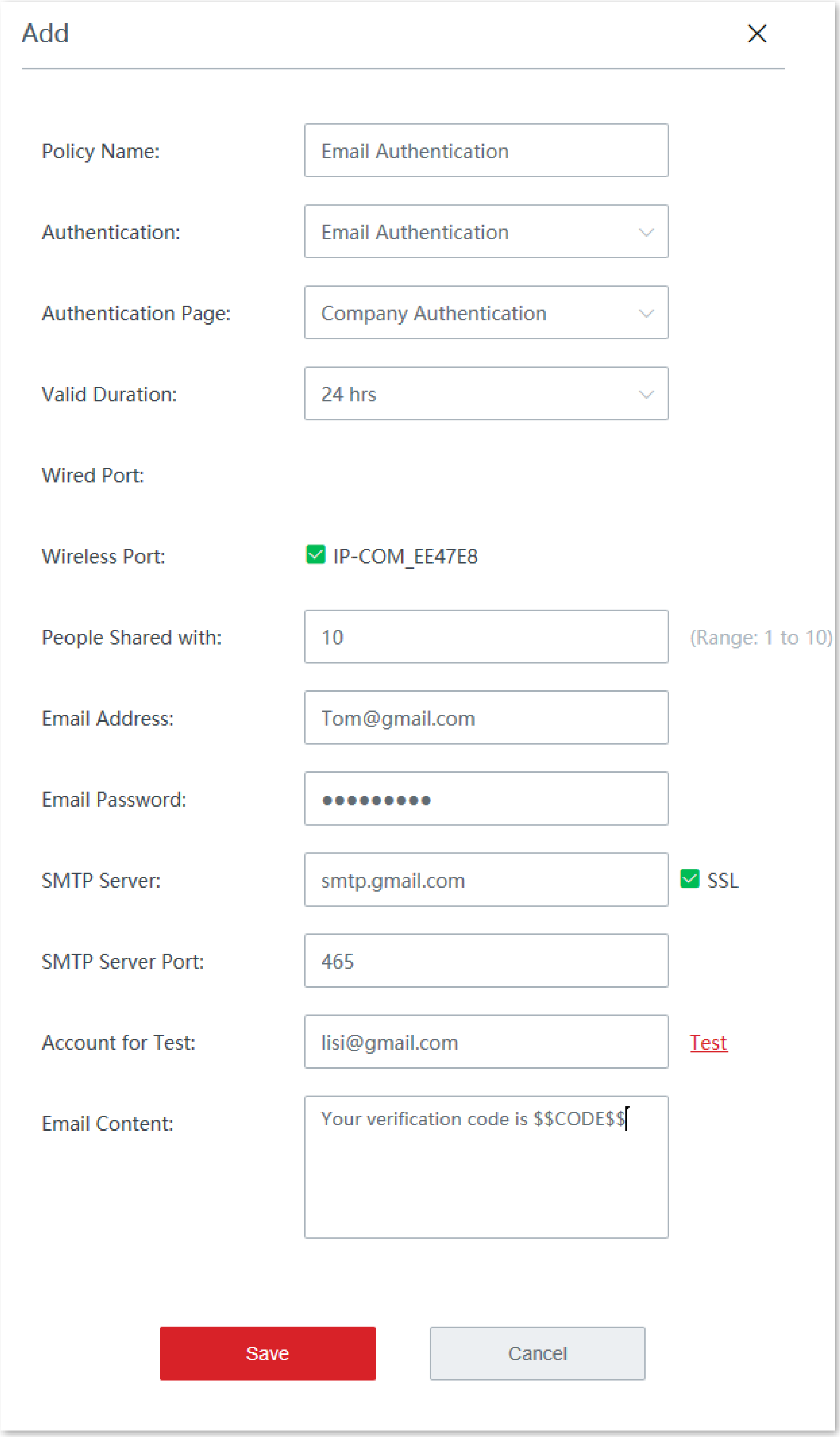
Redirect to:

Disclaimer: Copyright © 2021 IP-COM Networks Co., Ltd. All rights reserved.

Redirect to: ○ Previous Page ● Specified Page

http:// www.bing.com

2. Configure email authentication.
   (1) Click **Authentication** > **Captive Portal**.
   (2) In the **Authentication Policies** module, click **+ Add**.
   (3) Configure the parameters in the pop-up window, and then click **Save** at the bottom of the page.
      - Policy Name: Set the policy name, such as **Email Authentication.**
      - Authentication: Set **Authentication** to **Email Authentication**.
      - Authentication Page: Set **Authentication Page** to **Company Authentication**.
      - Valid Duration: Set the valid duration for email authentication, such as **24 hrs**.
      - Wireless Port: Select the WiFi network requiring email authentication, which is **IP-COM_EE47E8** in this example.
      - People Shared with: Set the number of users allowed to connect to the internet using email at the same time, such as **10**.
      - Email Address: Enter the email address, which is **Tom@gmail.com** in this example.
      - Email Password: Enter the password corresponding to the email address, which is **abc123456** in this example.
      - SMTP Server: Enter the SMTP server address, which is **smtp.gmail.com** in this example.
      - Tick **SSL**.
      - SMTP Server Port: Enter the SMTP server port, which is **465** in this example.
      - Account for Test: Enter a valid email address, which is **lisi@gmail.com** in this example.
      - Email Content: Set the email content sent to users ("$$CODE$$" is the format of the email verification code and cannot be modified).



Add

Policy Name:	Email Authentication
Authentication:	Email Authentication
Authentication Page:	Company Authentication
Valid Duration:	24 hrs
Wired Port:	
Wireless Port:	☑ IP-COM_EE47E8
People Shared with:	10 (Range: 1 to 10)
Email Address:	Tom@gmail.com
Email Password:	●●●●●●●●●
SMTP Server:	smtp.gmail.com ☑ SSL
SMTP Server Port:	465
Account for Test:	lisi@gmail.com Test
Email Content:	Your verification code is $$CODE$$

(4) To check whether the configuration is correct, click the **Test** button besides **Account for Test**.

Tip

If the test fails, please try the following solutions:

- Ensure that the email address has enabled SMTP service.
- Ensure that the account for test is real and valid.
- Adjust email content.

3. Add authentication-free hosts.

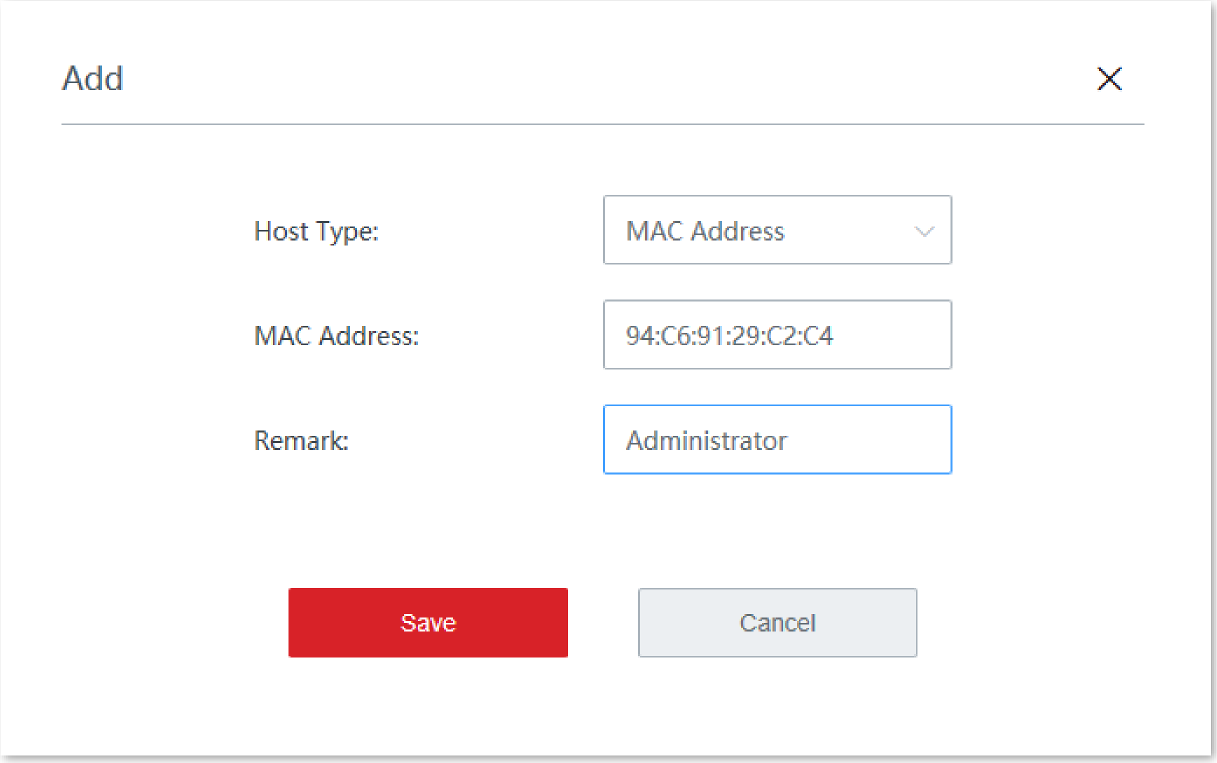
(1) Click **Authentication** > **User Management**.

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

(3) Configure the following parameters in the **Add** window.

- Host Type: Select the method by which you specify an authentication-free host, which is **MAC Address** in this example.
- MAC Address: Enter the MAC address of the client, which is **94:C6:91:29:C2:C4** in this example.
- Remark: Enter a remark of the user, which is **Administrator** in this example.

(4) Click **save**.



Add

Host Type: MAC Address

MAC Address: 94:C6:91:29:C2:C4

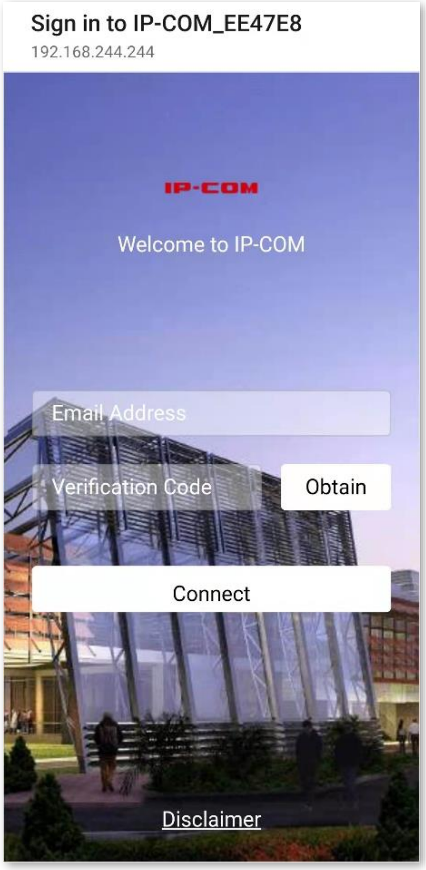
Remark: Administrator

----End

Verification

The network administrator does not need authentication when accessing the internet. Employees need email authentication when accessing the internet. The steps are as follows:

1. Visit a website and the browser will automatically redirect to the email authentication page.
2. Enter a valid email address.
3. Click **Obtain** to get verification code.
4. Log in to the email and check the received verification code.
5. Enter the verification code on the page and click **Connect**.



Sign in to IP-COM_EE47E8

192.168.244.244

----End

If the authentication is successful, the browser will automatically redirect to Bing.

3.9 Filter management

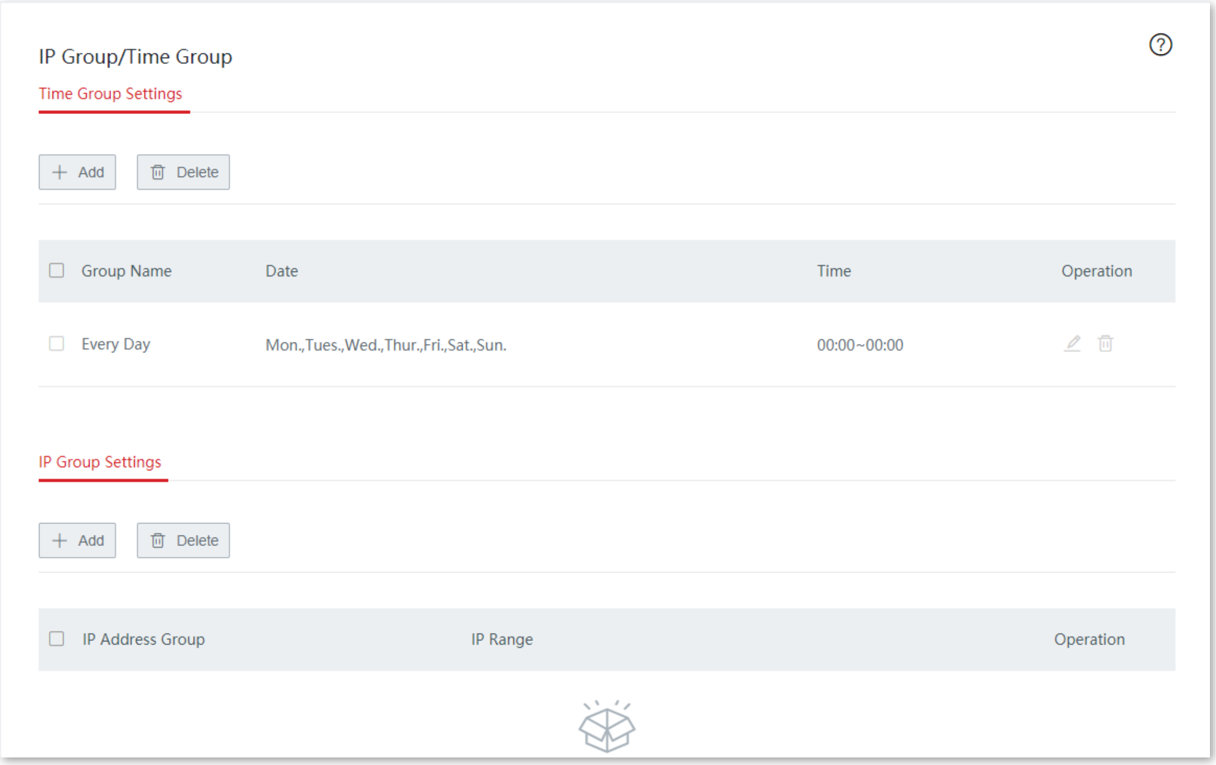
3.9.1 IP group/time group

Overview

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

By default, a time group has been added on the node, and the default time group cannot be deleted or edited.

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



IP Group/Time Group

Time Group Settings

+ Add   Delete

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

IP Group Settings

+ Add   Delete

□ IP Address Group	IP Range	Operation

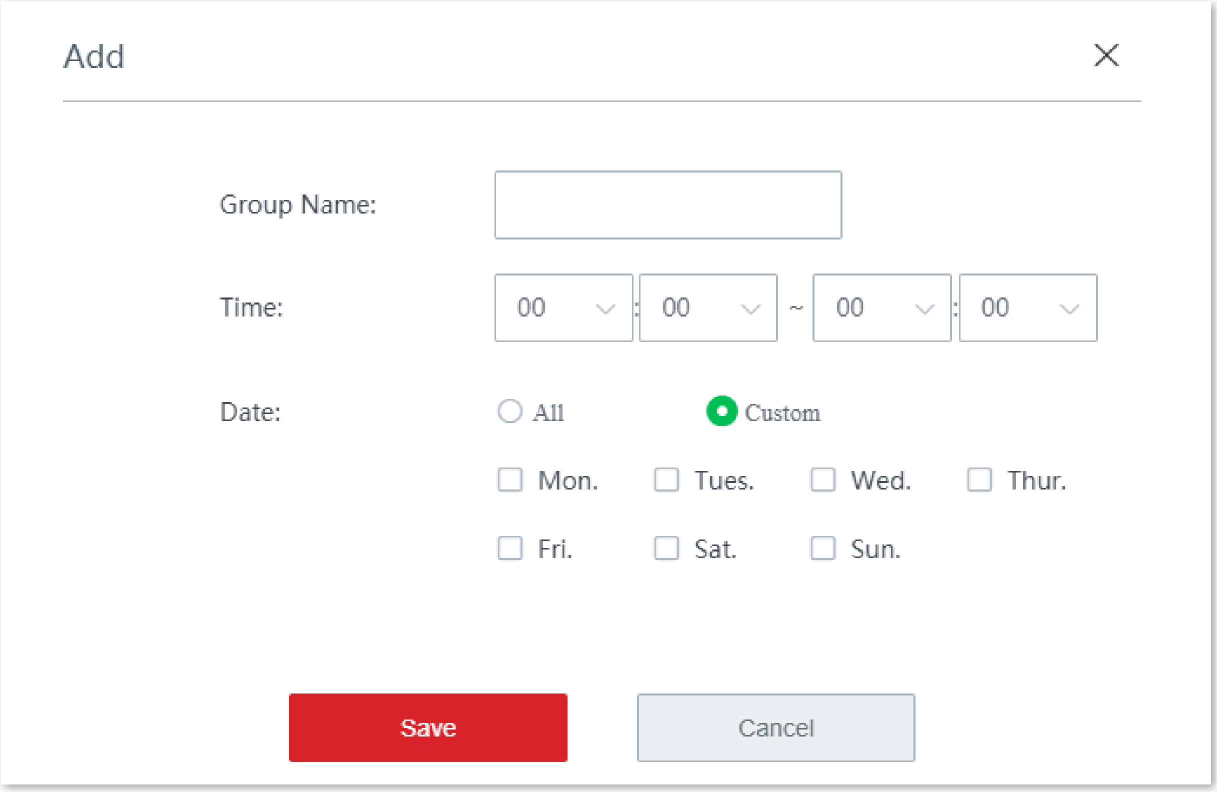
Parameter description

Parameter		Description
Time Group Settings	Group Name	It specifies the name of the time group.
	Date	It specifies the dates included in the time group.
	Time	It specifies the start and end time of the time group. **00:00~00:00** indicates a whole day.

Parameter		Description
	Operation	It specifies the operations you can perform on the rule. ✎: Click it to edit the rule. 🗑 : Click it to delete the rule.
IP Group Settings	IP Address Group	It specifies the name of the IP group.
	IP Range	It specifies the start and end IP address of the IP group.
	Operation	It specifies the operations you can perform on the rule. ✎: Click it to edit the rule. 🗑 : Click it to delete the rule.

Add a time group

1. Click **Filter Management** > **IP Group/Time Group**, and locate the **Time Group Settings** configuration area.
2. Click **+ Add**.
3. Set the required parameters in the **Add** window.
4. Click **Save**.



Add ✕

Group Name:

Time: 00 : 00 ~ 00 : 00

Date: ○ All ● Custom

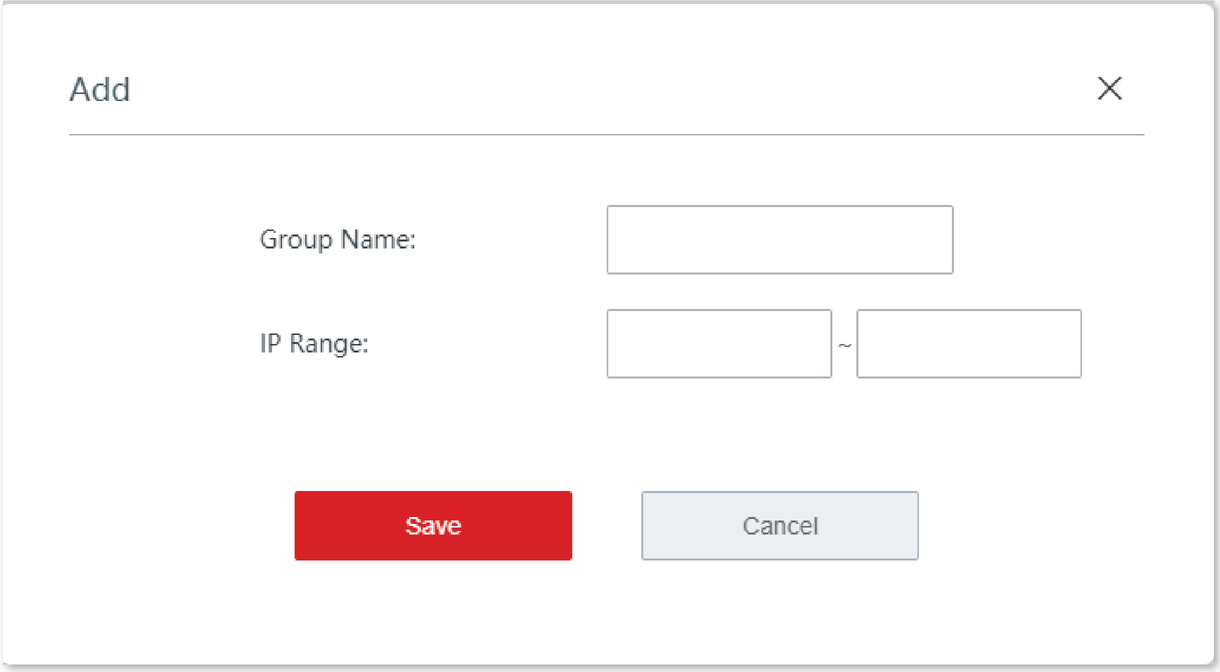
□ Mon. □ Tues. □ Wed. □ Thur.

□ Fri. □ Sat. □ Sun.

----End

Add an IP group

1. Click **Filter Management** > **IP Group/Time Group**, and locate the **IP Group Settings** configuration area.
2. Click **+ Add**.
3. Set the required parameters in the **Add** window.
4. Click **Save**.



Add

Group Name:

IP Range: ~

----End

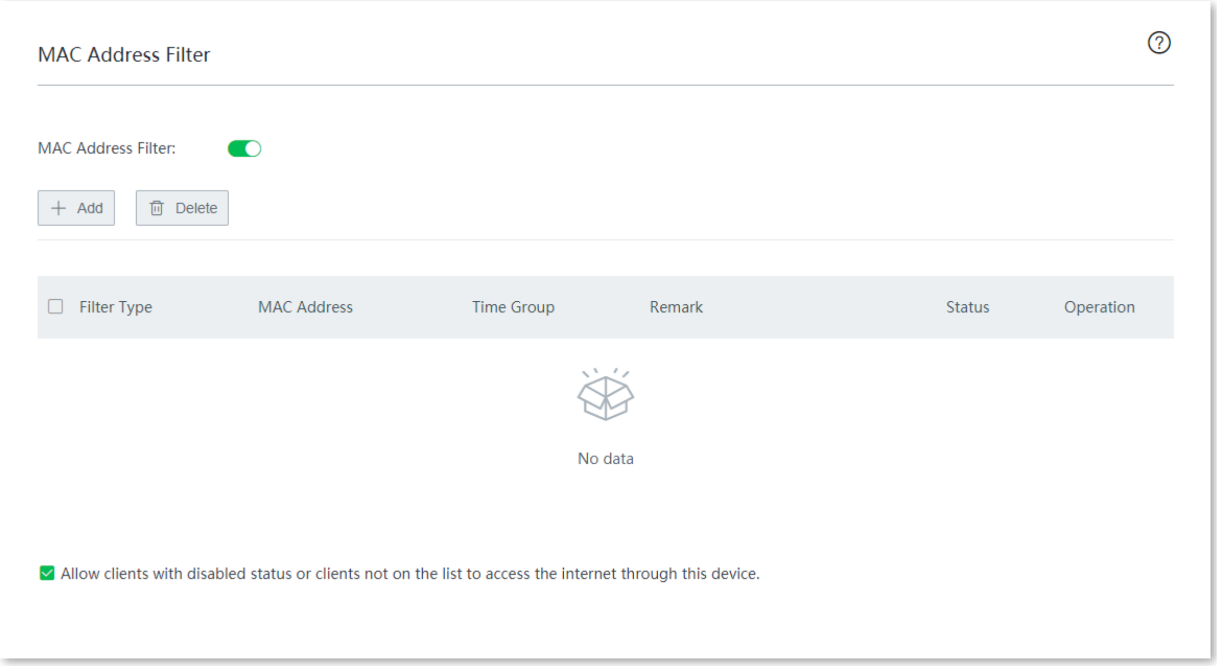
3.9.2 MAC address filter

Overview

On this page, you can allow or block internet access through this node for specified clients.

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

The MAC address filter function is disabled by default. The following displays the page when the function is enabled.



MAC Address Filter

MAC Address Filter: ●

＋ Add 🗑 Delete

□ Filter Type	MAC Address	Time Group	Remark	Status	Operation

No data

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

Parameter description

Parameter	Description
MAC Address Filter	It specifies whether to enable the MAC address filter function. ○ indicates the function is disabled and ● indicates the function is enabled.
Filter Type	It specifies the MAC address filter types. – **Whitelist**: It specifies that internet access is allowed. In this mode, clients with the specified MAC address can access the internet only within the specified time period. – **Blacklist**: It specifies that internet access is blocked. In this mode, clients with the specified MAC address cannot access the internet only within the specified time period.
MAC Address	It specifies the MAC address of the client to which the rule applies.
Time Group	Select the time group rule, which is used to specify the time period during which the MAC address filter rule takes effect. The time group rule should be configured in advance in the **Time Group Settings** module on the **Filter Management** > **IP Group/Time Group** page.
Remark	It specifies the remark of the MAC address filter rule.
Status	It specifies the status of the MAC address filter rule. You can enable or disable the rule as required.
Operation	It specifies the operations you can perform on the rule. ✎: Click it to edit the rule. 🗑 : Click it to delete the rule.

Parameter	Description
Allow clients with disabled status or clients not on the list to access the internet through this device.	– If this option is selected, clients to which the disabled rules in the list apply and clients not in the list can both access the internet. – If this option is not selected, clients to which the disabled rules in the list apply and clients not in the list can neither access the internet.

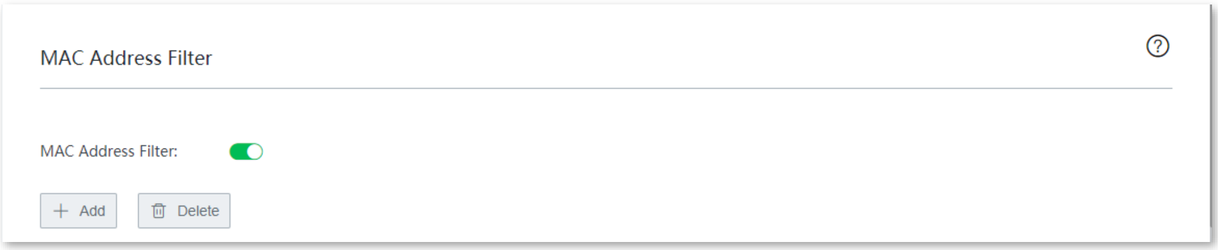
Configure a MAC address filter rule

Tip

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

Enable the MAC address filter function

On the **Filter Management** > **MAC Address Filter** page, toggle on **MAC Address Filter**, and click **Save**.

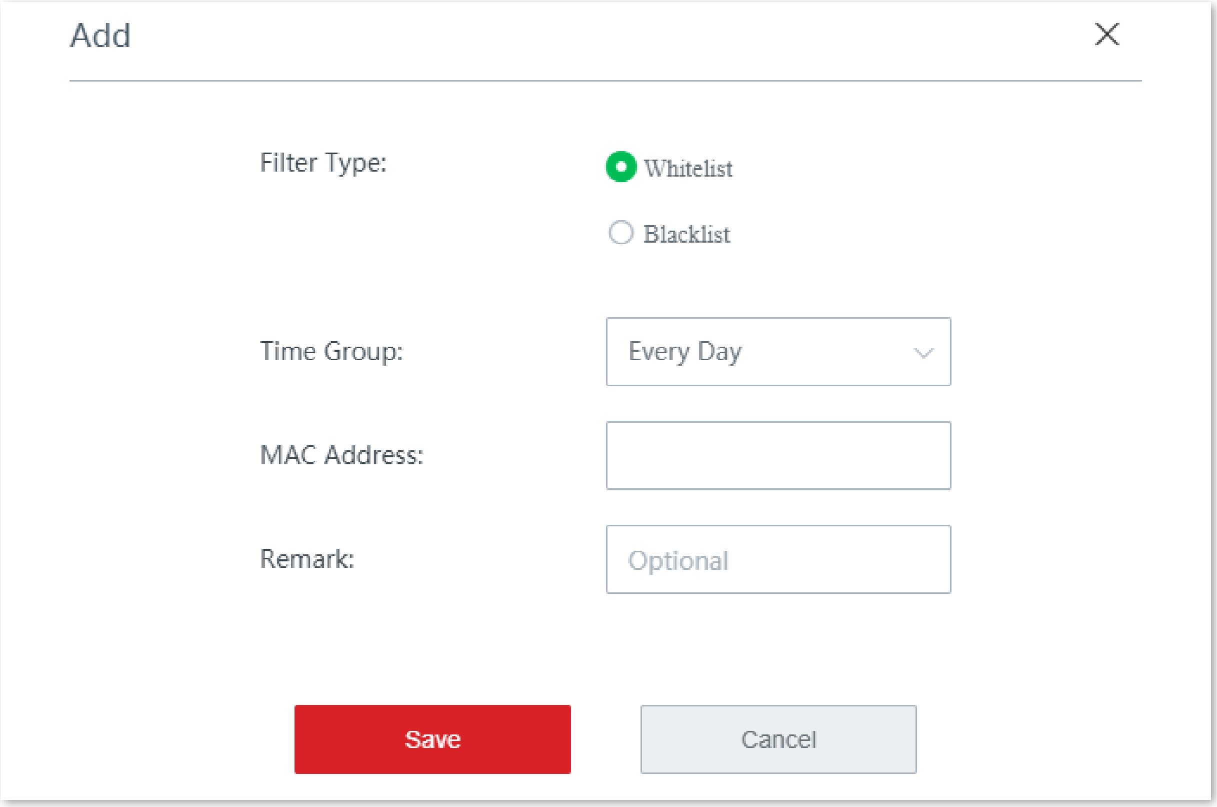


MAC Address Filter

MAC Address Filter: on

Add a MAC address filter rule

On the **Filter Management** > **MAC Address Filter** page, click **+ Add**, configure parameters in the pop-up configuration window, and click **Save**.



Add

Filter Type: ● Whitelist ○ Blacklist

Time Group: Every Day

MAC Address:

Remark: Optional

Example of configuring a MAC address filter rule

Networking requirement

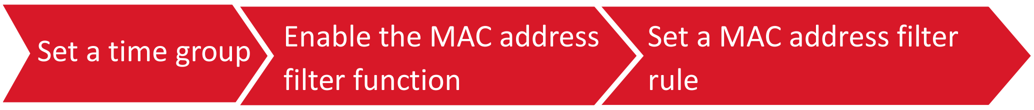
An enterprise uses cable-free devices to set up a network. The enterprise has the following requirements:

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

Solution

You can use the **MAC Address Filter** function to meet this requirement. Assume that the MAC address of the purchaser is CC:3A:61:71:1B:6E.

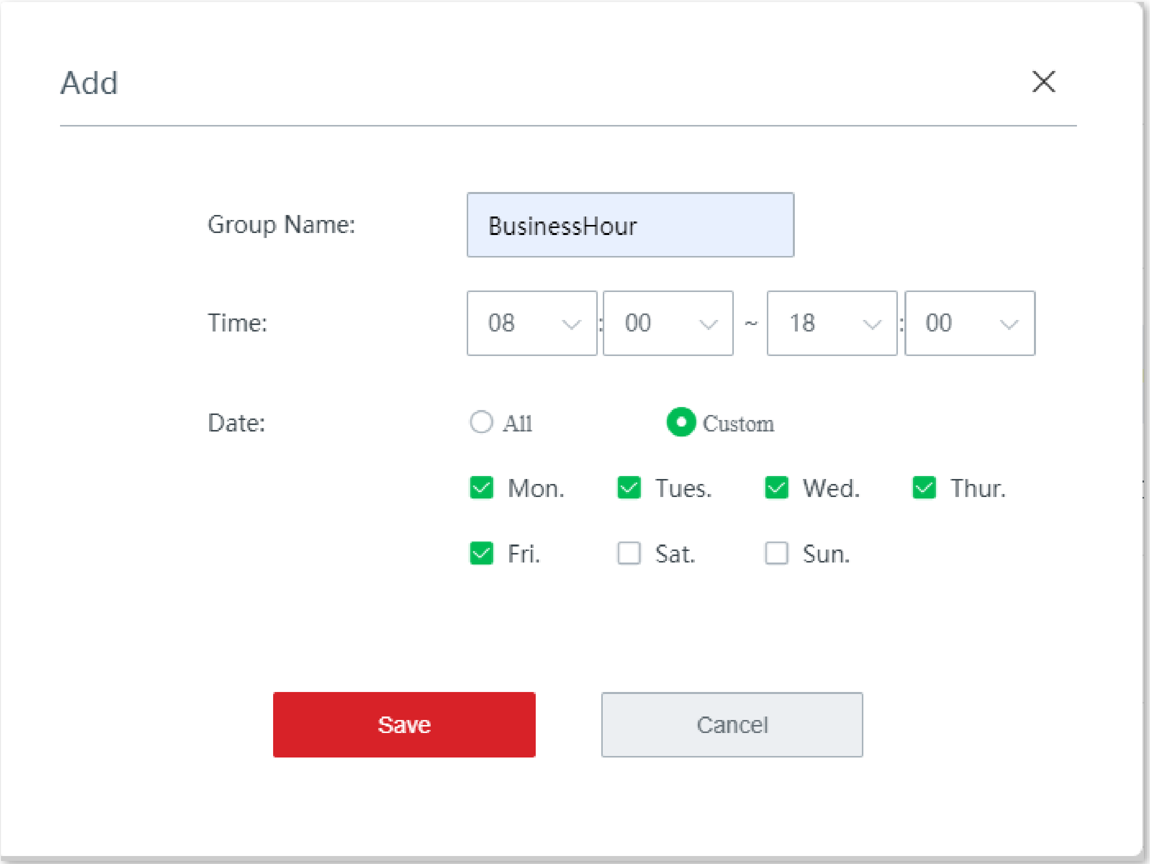
Configuration procedures



Set a time group → Enable the MAC address filter function → Set a MAC address filter rule

I. **Set a time group.**

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



Add

Group Name: BusinessHour

Time: 08 : 00 ~ 18 : 00

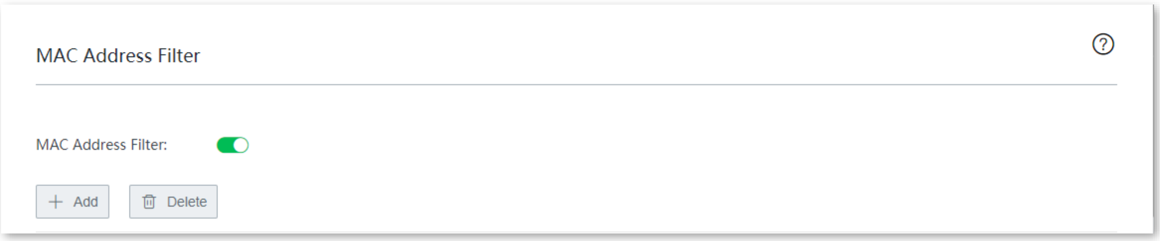
Date: ○ All ● Custom

☑ Mon. ☑ Tues. ☑ Wed. ☑ Thur.

☑ Fri. □ Sat. □ Sun.

II. Enable the MAC address filter function.

1. On the **Filter Management** > **MAC Address Filter** page, toggle on **MAC Address Filter**.
2. Click **Save**.



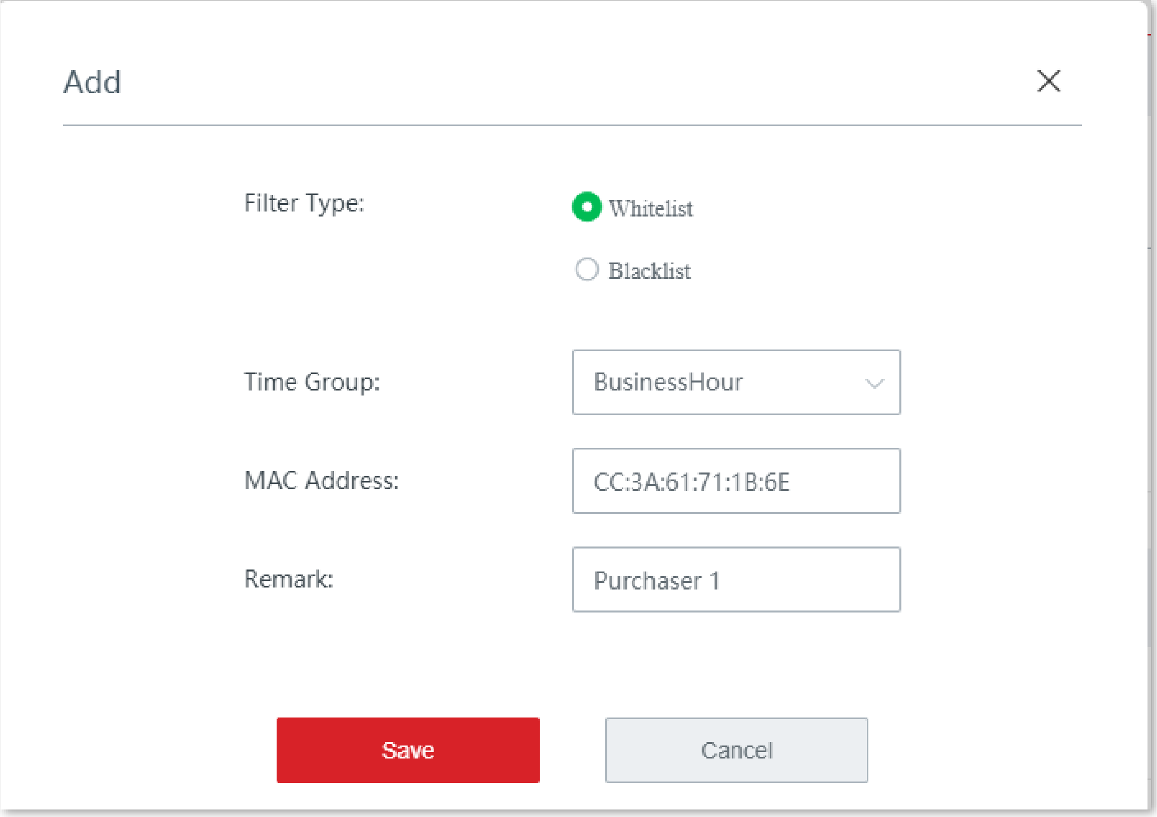
MAC Address Filter

MAC Address Filter: ●

III. Set a MAC address filter rule.

1. Add a MAC address filter rule.
   (1) On the **Filter Management** > **MAC Address Filter** page, click **+ Add**.
   (2) Configure parameters in the **Add** window, and click **Save**.
      – Choose **Filter Type**, which is **Whitelist** in this example.
      – Select the target time group, which is **BusinessHour** in this example.
      – Enter the physical address of the computer of the purchaser, which is **CC:3A:61:71:1B:6E** in this example.

- (Optional) Set the remarks of the rule, for example, **Purchaser 1**.



Add

Filter Type: ● Whitelist ○ Blacklist

Time Group: BusinessHour

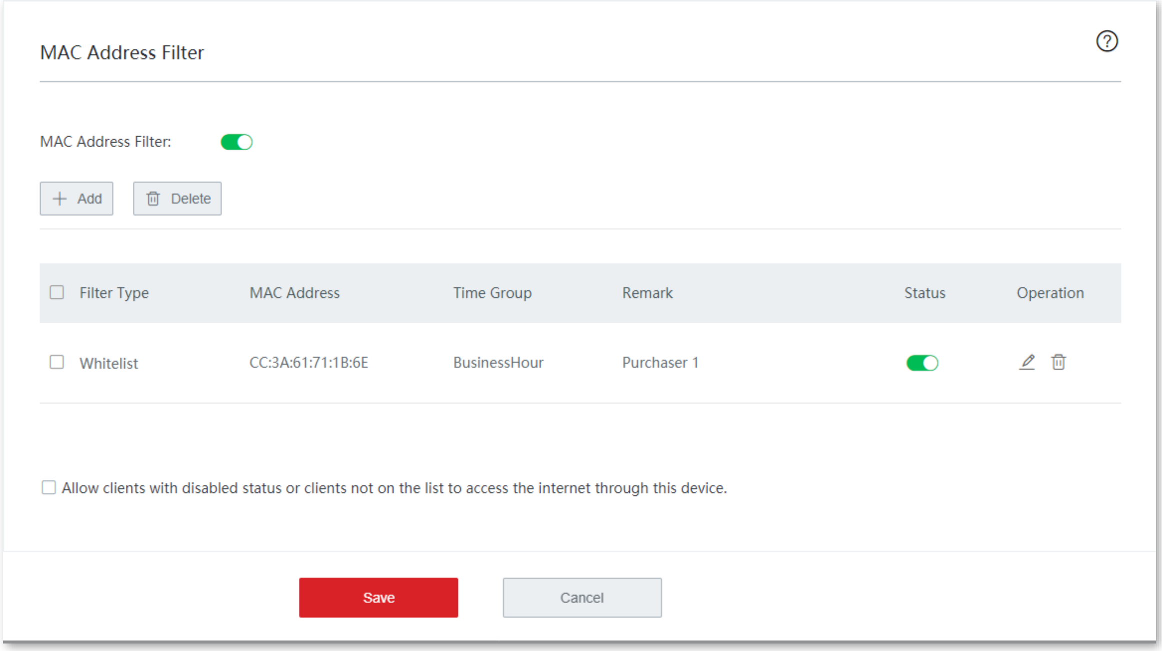
MAC Address: CC:3A:61:71:1B:6E

Remark: Purchaser 1

2. Block clients to which disabled rules apply and clients not in the list.

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

(2) Click **Save**.



MAC Address Filter

MAC Address Filter: on

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

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

----End

Verification

In the LAN during 8:00 to 18:00 from Monday to Friday, only the computer with the MAC address of CC:3A:61:71:1B:6E can access the internet.

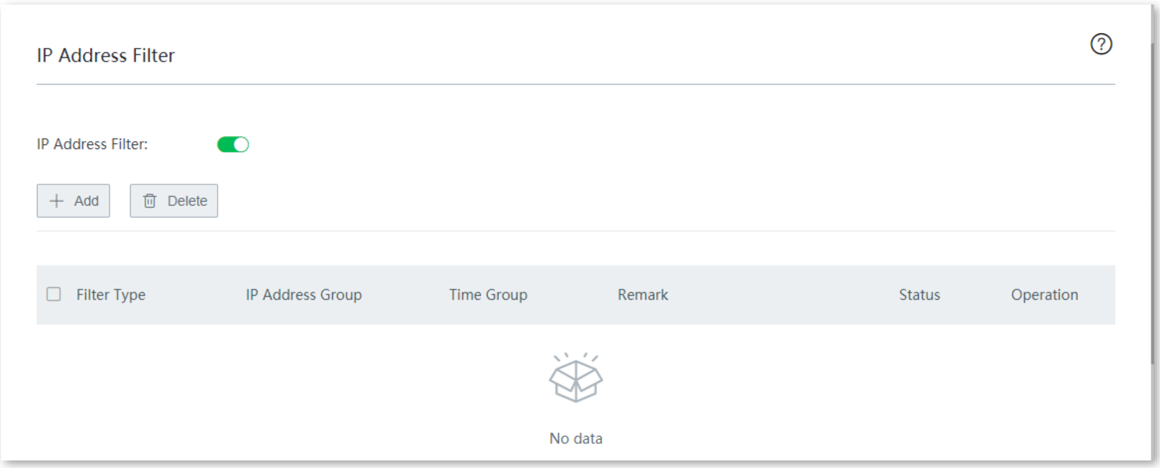
3.9.3 IP address filter

Overview

On this page, you can allow or block internet access through this node for specified clients.

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

The IP address filter function is disabled by default. The following displays the page when the function is enabled.



IP Address Filter: ●

□ Filter Type	IP Address Group	Time Group	Remark	Status	Operation

No data

Parameter description

Parameter	Description
IP Address Filter	It specifies whether to enable the IP address filter function. ○ indicates the function is disabled and ● indicates the function is enabled.
Filter Type	It specifies the IP address filter types. – **Whitelist**: It specifies that internet access is allowed. In this mode, clients with the specified IP address can access the internet only within the specified time period. – **Blacklist**: It specifies that internet access is blocked. In this mode, clients with the specified IP address cannot access the internet only within the specified time period.

Parameter	Description
IP Address Group	It specifies the IP group the rule uses, which is used to specify the client to which the rule applies. The IP group rule should be configured in advance in the **IP Group Settings** module on the **Filter Management** > **IP Group/Time Group** page.
Time Group	It specifies the time group the rule uses, which is used to specify the time period during which the rule is effective. The time group rule should be configured in advance in the **Time Group Settings** module on the **Filter Management** > **IP Group/Time Group** page.
Remark	It specifies the remark of the IP address filter rule.
Status	It specifies the status of the IP address filter rule. You can enable or disable the rule as required.
Operation	It specifies the operations you can perform on the rule. ✎: Click it to edit the rule. 🗑 : Click it to delete the rule.
Allow clients with disabled status or clients not on the list to access the internet through this device.	– If this option is selected, clients to which the disabled rules in the list apply and clients not in the list can both access the internet. – If this option is not selected, clients to which the disabled rules in the list apply and clients not in the list can neither access the internet.

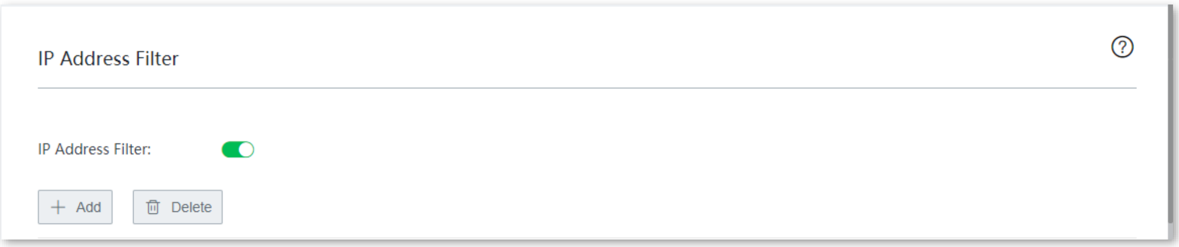
Configure an IP address filter rule

Tip

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

Enable the IP address filter function

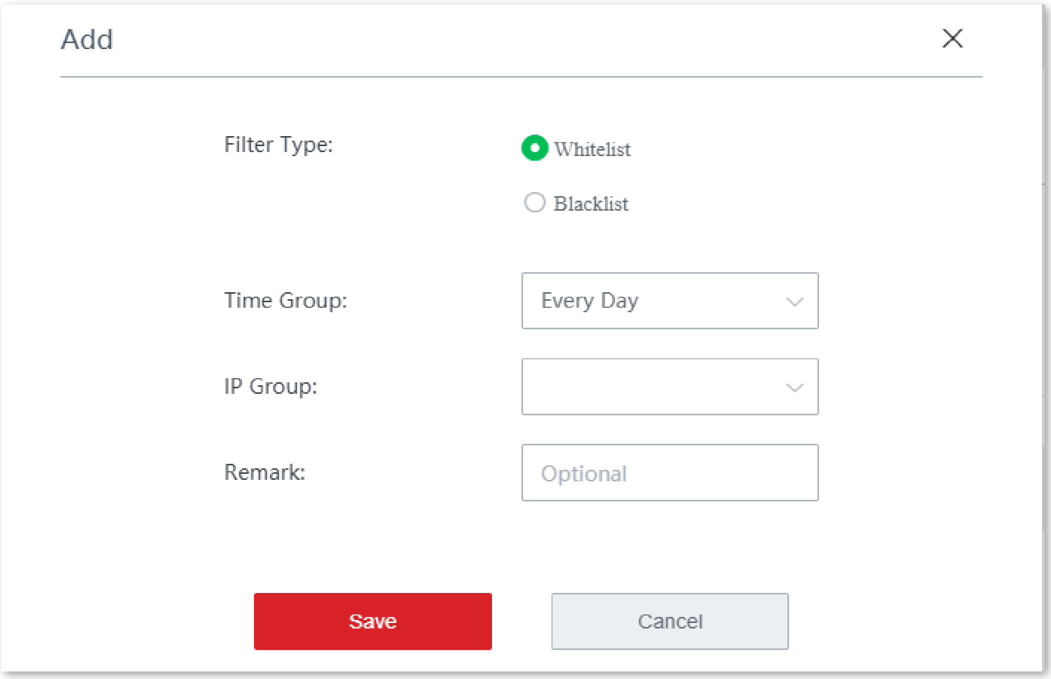
On the **Filter Management** > **IP Address Filter** page, toggle on **IP Address Filter**, and click **Save**.


IP Address Filter

IP Address Filter: ●

Add an IP address filter rule

On the **Filter Management** > **IP Address Filter** page, click **+ Add**, configure parameters in the pop-up configuration window, and click **Save**.



Add

Filter Type: ● Whitelist ○ Blacklist

Time Group: Every Day

IP Group:

Remark: Optional

Example of configuring an IP address filter rule

Networking requirement

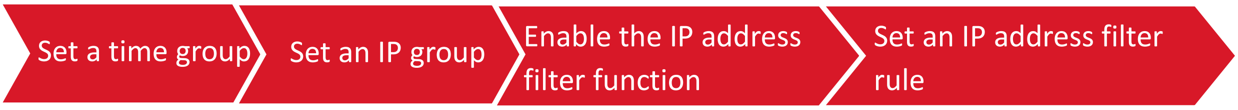
An enterprise uses cable-free devices to set up a network. The enterprise has the following requirements:

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

Solution

You can use the **IP Address Filter** function to meet this requirement. Assume that the IP addresses of purchasers range from 192.168.5.2 to 192.168.5.10.

Configuration procedures

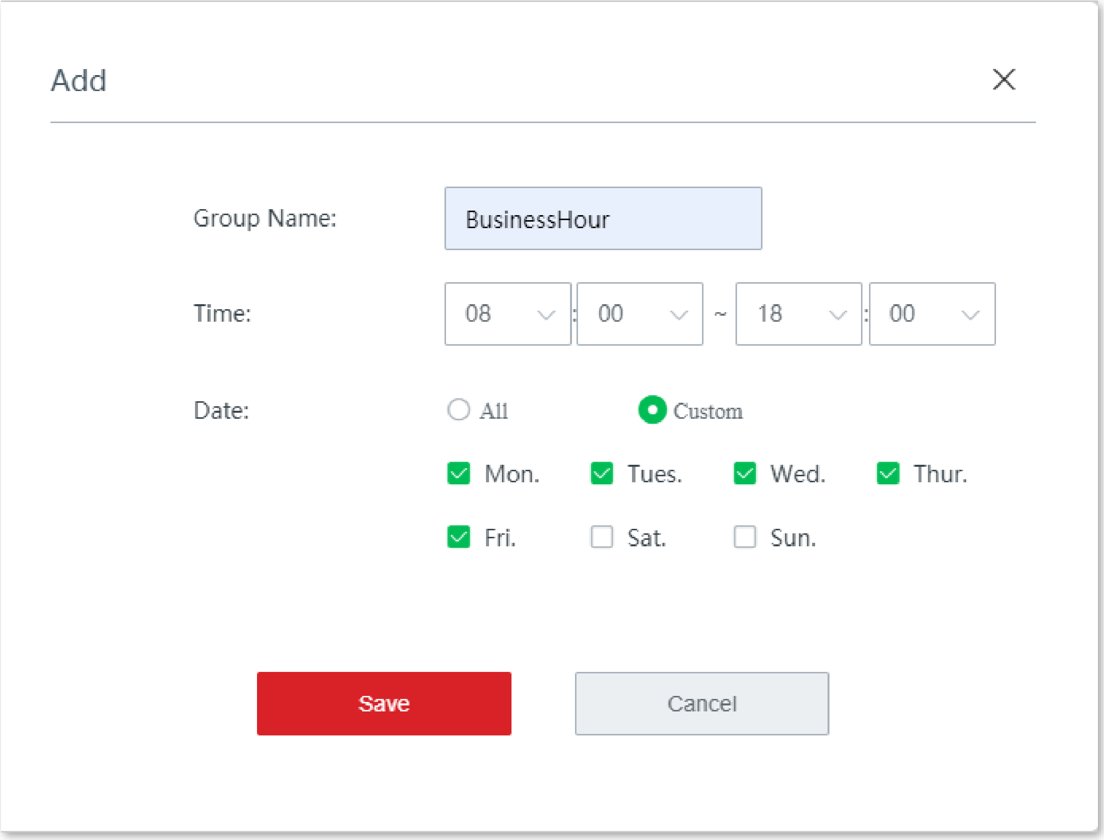


Set a time group → Set an IP group → Enable the IP address filter function → Set an IP address filter rule

I. Set a time group.

1. Click **Filter Management** > **IP Group/Time Group**.

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



Add

Group Name: BusinessHour

Time: 08 : 00 ~ 18 : 00

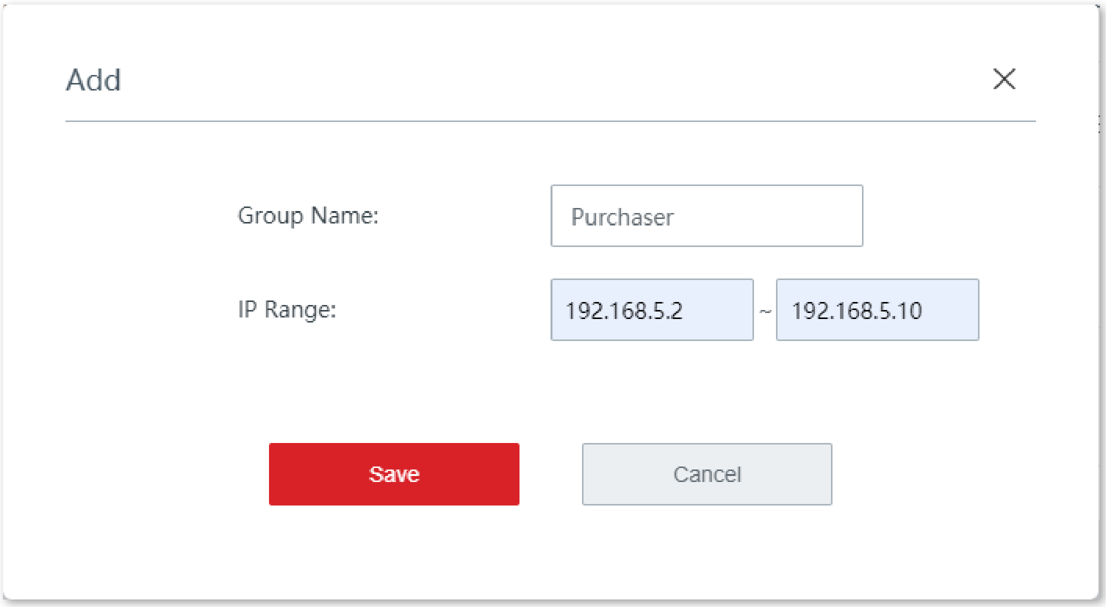
Date: ○ All ● Custom

☑ Mon. ☑ Tues. ☑ Wed. ☑ Thur.

☑ Fri. □ Sat. □ Sun.

II. Set an IP group.

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



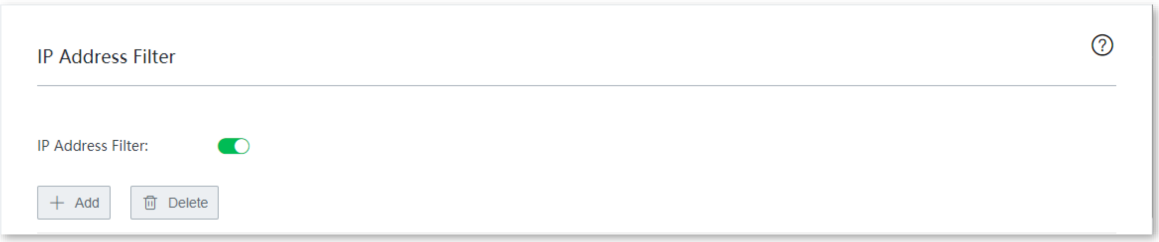
Add

Group Name: Purchaser

IP Range: 192.168.5.2 ~ 192.168.5.10

III. Enable the IP address filter function.

1. On the **Filter Management** > **IP Address Filter** page, toggle on **IP Address Filter**.
2. Click **Save**.

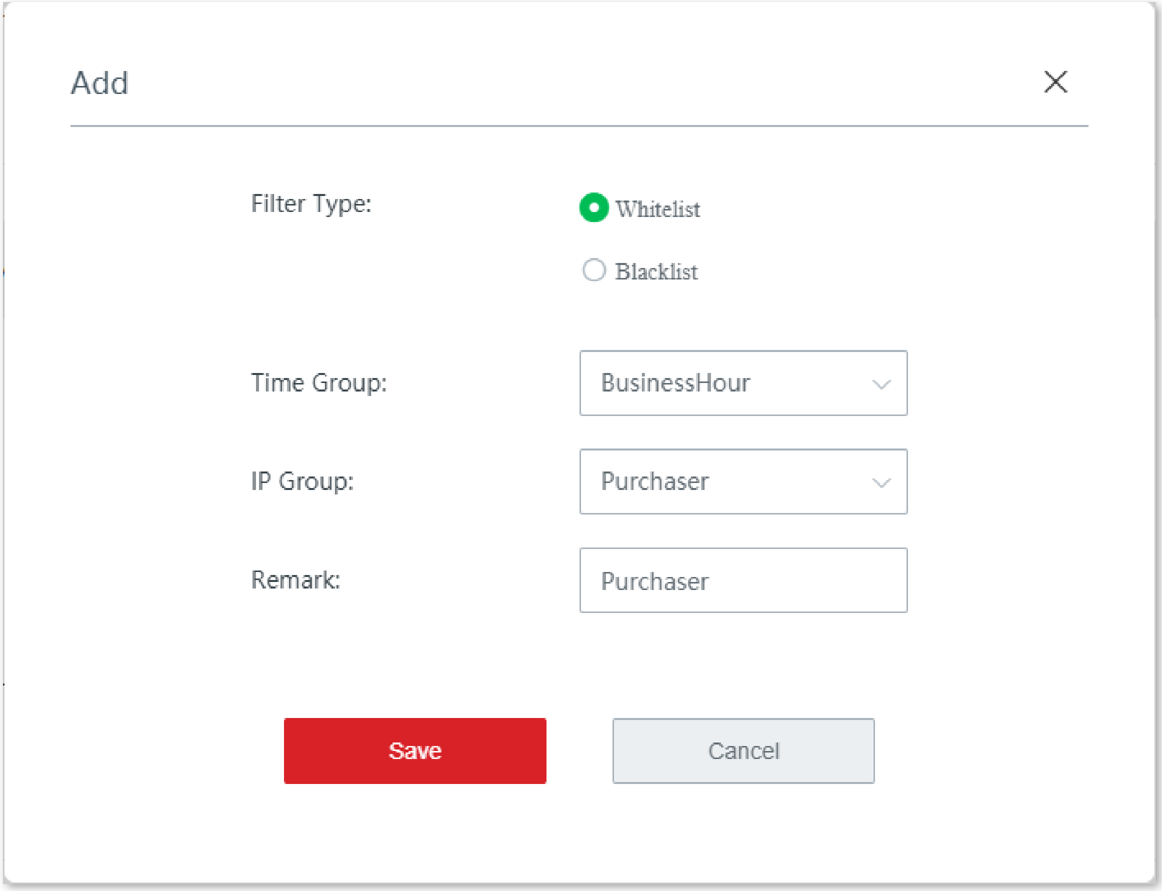


IP Address Filter

IP Address Filter: ●

IV. Set an IP address filter rule.

1. Add an IP address filter rule.
   (1) On the **Filter Management** > **IP Address Filter** page, click **+ Add**.
   (2) Configure parameters in the **Add** window, and click **Save**.
   - Choose **Filter Type**, which is **Whitelist** in this example.
   - Select the target time group, which is **BusinessHour** in this example.
   - Select the target IP group, which is **Purchaser** in this example.
   - (Optional) Set the remarks of the rule, for example, **Purchaser**.



Add

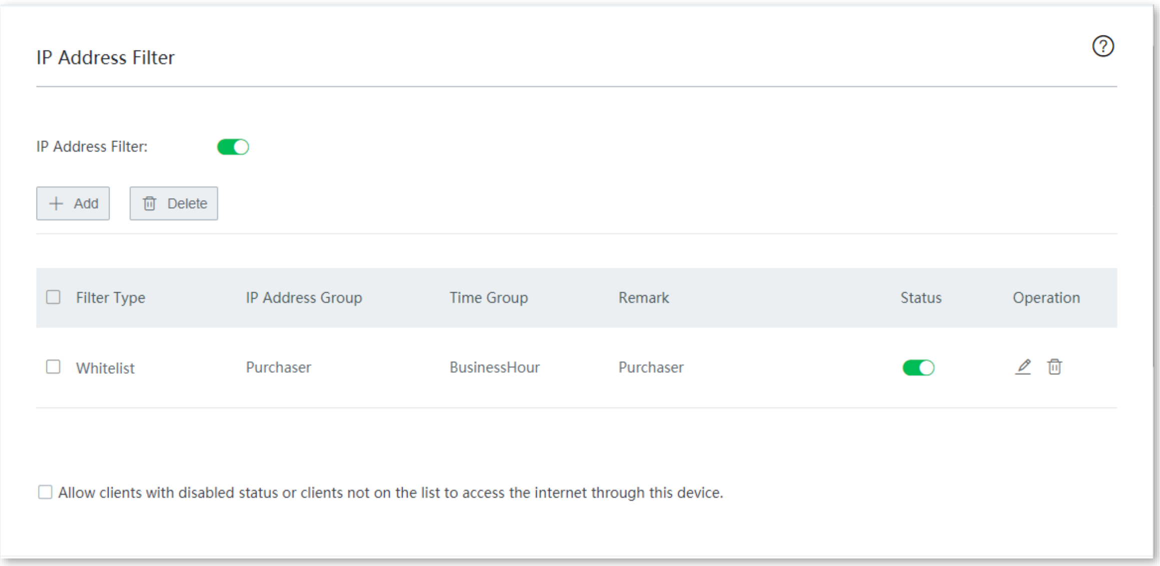
Filter Type: ● Whitelist ○ Blacklist

Time Group: BusinessHour

IP Group: Purchaser

Remark: Purchaser

2. Block clients to which disabled rules apply and clients not in the list.
   (1) Deselect **Allow clients with disabled status or clients not on the list to access the internet through this device**.
   (2) Click **Save**.



□ Filter Type	IP Address Group	Time Group	Remark	Status	Operation
□ Whitelist	Purchaser	BusinessHour	Purchaser	●	

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

----End

Verification

In the LAN during 8:00 to 18:00 from Monday to Friday, only the computers of purchasers (IP address range: 192.168.5.2 to 192.168.5.10) can access the internet.

3.9.4 Port filter

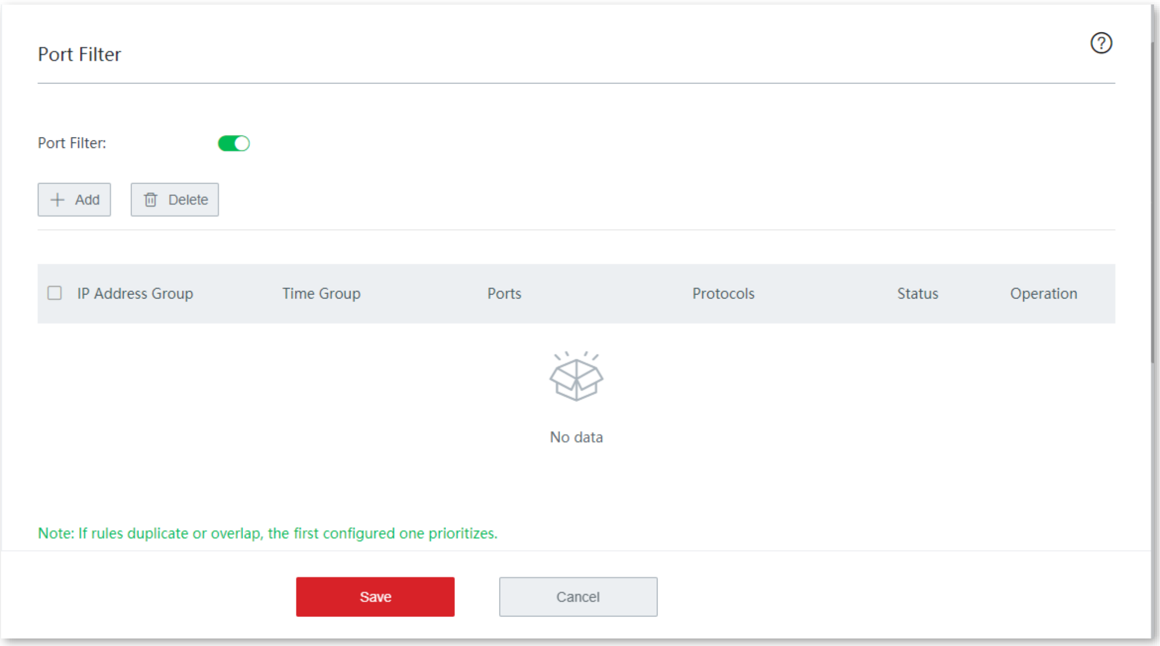
Overview

The application protocols used by various services on the internet have specified ports assigned to them. Among these ports, ports 0 to 1023 are used by common services and are generally assigned to fixed services.

On this page, you can control the types of internet services users can access by blocking the access to specified ports.

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

The port filter function is disabled by default. The following displays the page when the function is enabled.



Port Filter

Port Filter:

□ IP Address Group	Time Group	Ports	Protocols	Status	Operation

No data

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

Parameter description

Parameter	Description
Port Filter	It specifies whether to enable the port filter function. ○ indicates the function is disabled and ● indicates the function is enabled.
IP Address Group	It specifies the IP group the rule uses, which is used to specify the client to which the rule applies. The IP group rule should be configured in advance in the **IP Group Settings** module on the **Filter Management** > **IP Group/Time Group** page.
Time Group	It specifies the time group the rule uses, which is used to specify the time period during which the rule is effective. The time group rule should be configured in advance in the **Time Group Settings** module on the **Filter Management** > **IP Group/Time Group** page.
Ports	It specifies the TCP or UDP port number used by the service to be blocked.
Protocols	It specifies the protocol used by the service to be blocked. **All** indicates TCP and UDP.
Status	It specifies the status of the port filter rule. You can enable or disable the rule as required.
Operation	It specifies the operations you can perform on the rule. ✎: Click it to edit the rule. 🗑 : Click it to delete the rule.

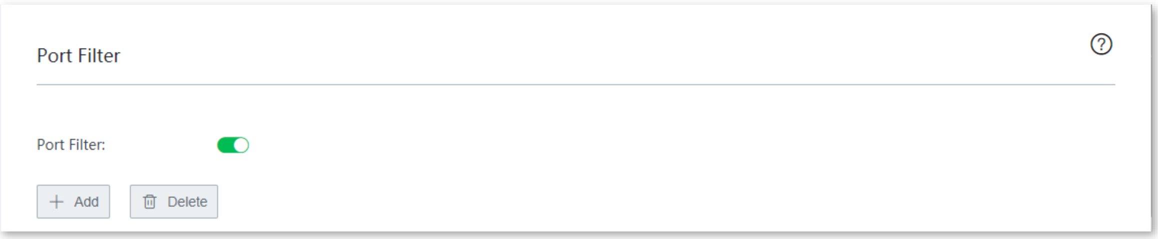
Configure a port filter rule

Tip

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

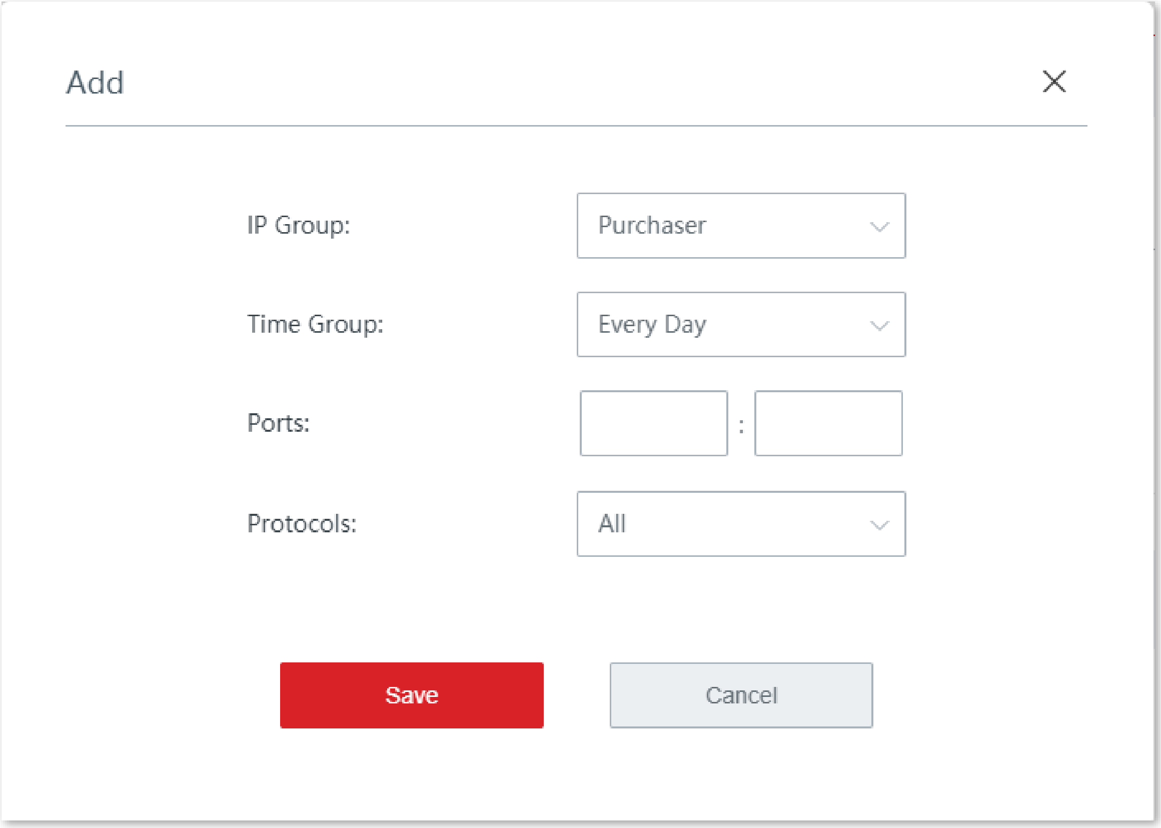
Enable the port filter function

On the **Filter Management** > **Port Filter** page, toggle on **Port Filter**, and click **Save**.



Add a port filter rule

On the **Filter Management** > **Port Filter** page, click **+ Add**, configure parameters in the pop-up configuration window, and click **Save**.



IP Group: Purchaser

Time Group: Every Day

Ports: :

Protocols: All

Example of configuring a port filter rule

Networking requirement

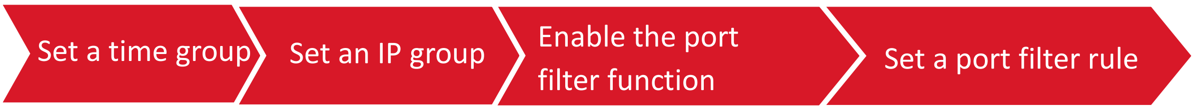
An enterprise uses cable-free devices to set up a network. The enterprise has the following requirements:

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

Solution

You can use the **Port Filter** function to meet this requirement. Assume that the IP addresses of the finance department staff range from 192.168.5.2 to 192.168.5.10.

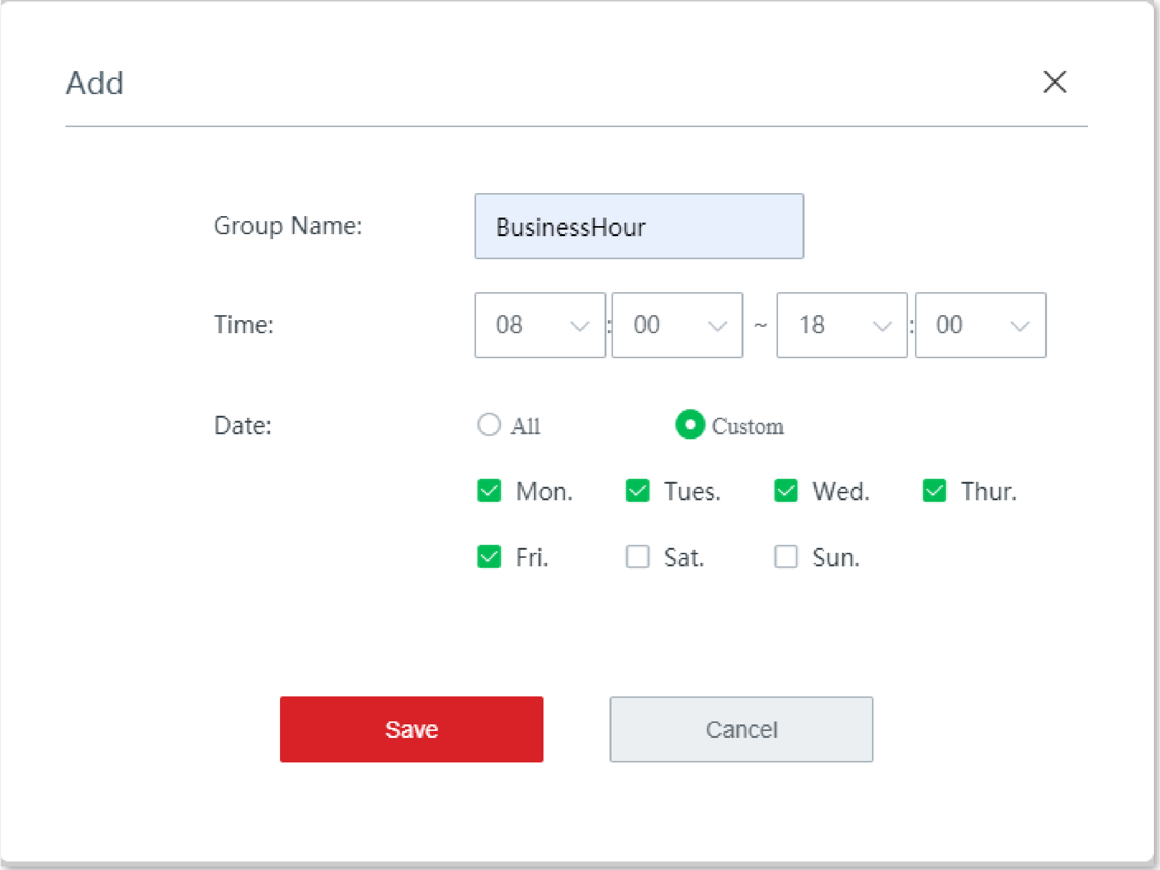
Configuration procedures



Set a time group → Set an IP group → Enable the port filter function → Set a port filter rule

I. **Set a time group.**

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



Group Name: BusinessHour

Time: 08 : 00 ~ 18 : 00

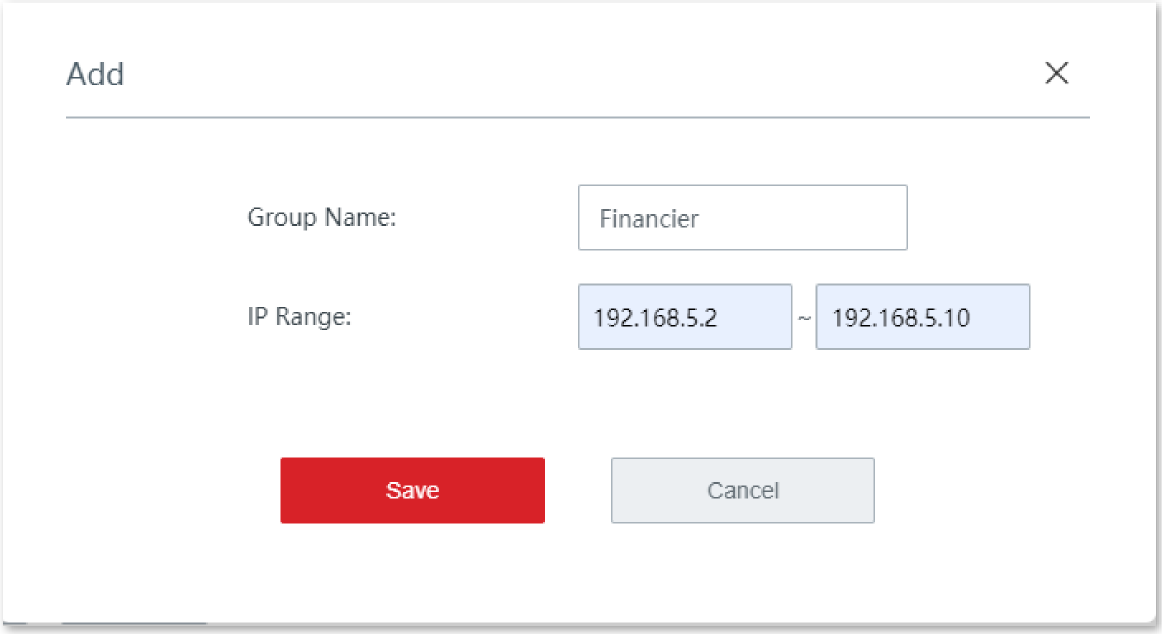
Date: ○ All ● Custom

☑ Mon. ☑ Tues. ☑ Wed. ☑ Thur.

☑ Fri. □ Sat. □ Sun.

II. Set an IP group.

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



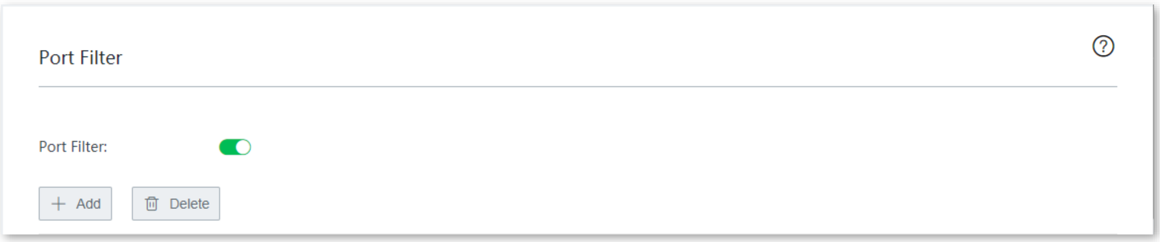
Add

Group Name: Financier

IP Range: 192.168.5.2 ~ 192.168.5.10

III. Enable the port filter function.

1. On the **Filter Management** > **Port Filter** page, toggle on **Port Filter**.
2. Click **Save**.

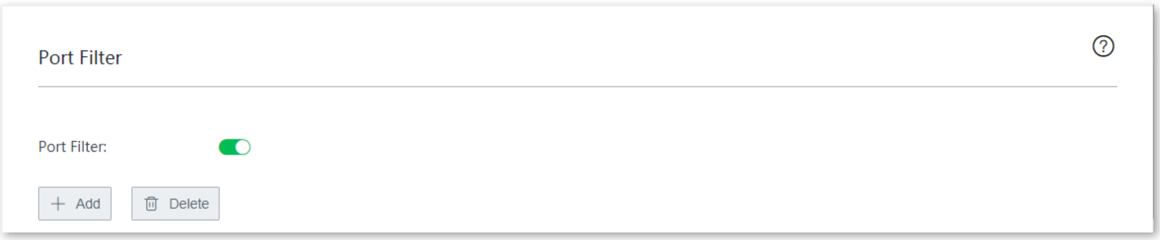


Port Filter

Port Filter: ●

IV. Set a port filter rule.

1. On the **Filter Management** > **Port Filter** page, click **+ Add**.



Port Filter

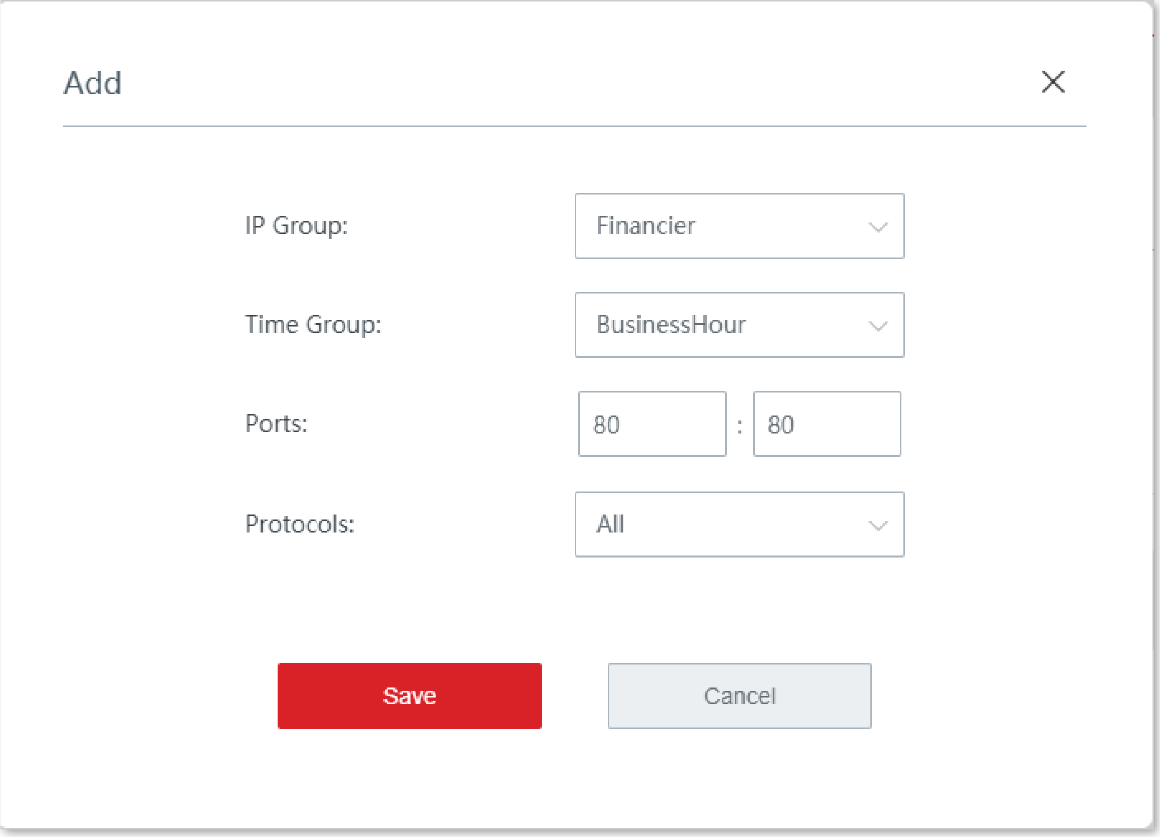
Port Filter: ●

2. Configure parameters in the **Add** window, and click **Save**.
   (1) Select the target IP group, which is **Financier** in this example.

(2) Select the target time group, which is **BusinessHour** in this example.

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

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



Add

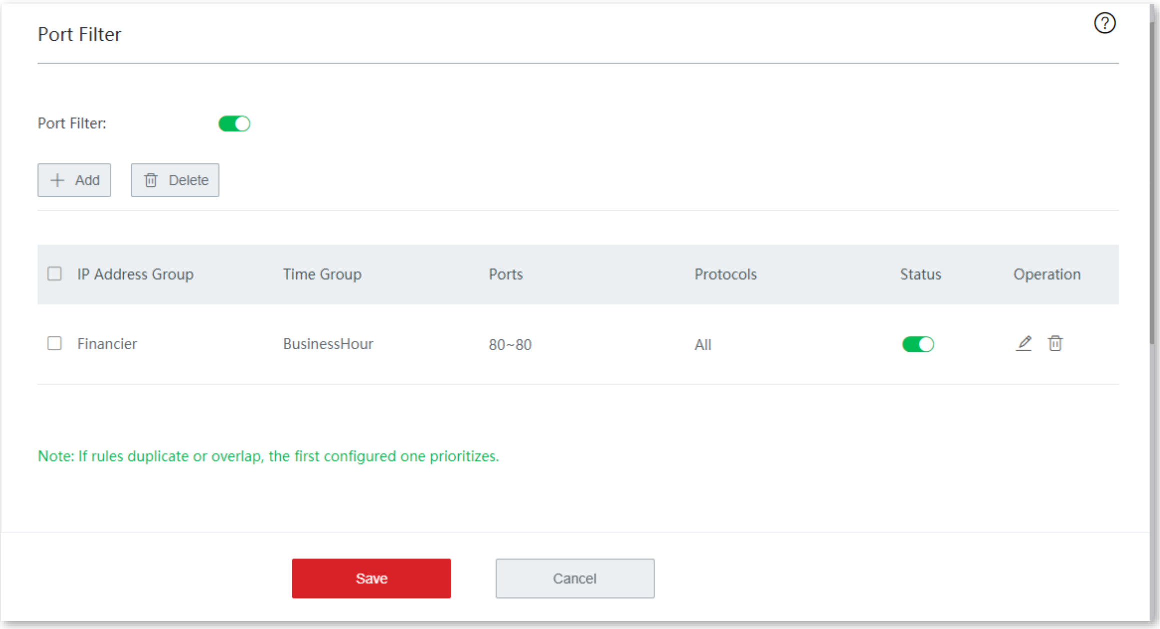
IP Group: Financier

Time Group: BusinessHour

Ports: 80 : 80

Protocols: All

The port filter rule is added successfully. See the following figure.



Port Filter

Port Filter: ●

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

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

----End

Verification

In the LAN during 8:00 to 18:00 from Monday to Friday, computers with an IP address ranging from 192.168.5.2 to 192.168.5.10 cannot use the webpage browsing service.

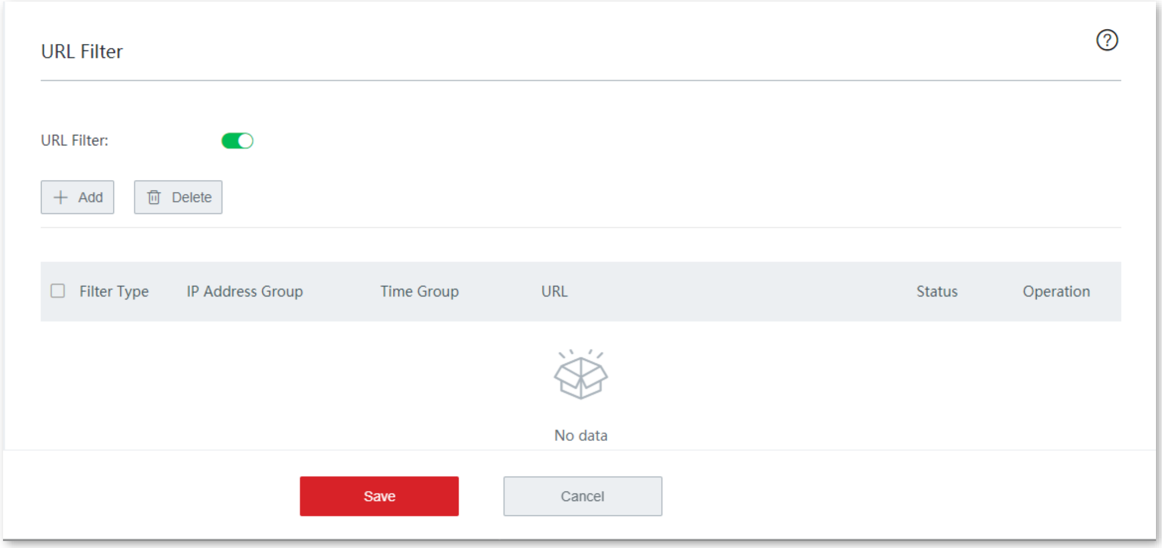
3.9.5 URL filter

Overview

On this page, you can allow or block users' access to specified website categories to control the internet behavior of LAN users.

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

The URL filter function is disabled by default. The following displays the page when the function is enabled.



URL Filter

URL Filter: ●

□ Filter Type	IP Address Group	Time Group	URL	Status	Operation

No data

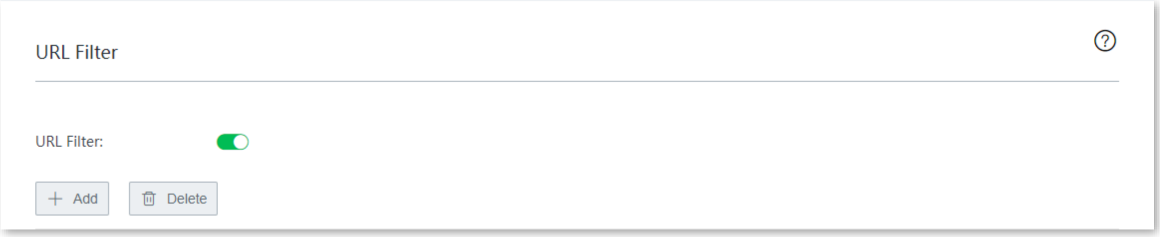
Parameter description

Parameter	Description
URL Filter	It specifies whether to enable the URL filter function. ○ indicates the function is disabled and ● indicates the function is enabled.
Filter Type	It specifies the URL filter types. – **Allow access only**: It specifies that internet access is allowed. In this mode, clients in the IP group can access only the specified website and cannot access other websites during the specified time period. During other time periods, the clients can access all the websites. – **Block access only**: It specifies that internet access is blocked. In this mode, clients in the IP group cannot access only the specified website and can access other websites during the specified time period. During other time periods, the clients can access all the websites.
IP Address Group	It specifies the IP group the rule uses, which is used to specify the client to which the rule applies. The IP group rule should be configured in advance in the **IP Group Settings** module on the **Filter Management** > **IP Group/Time Group** page.
Time Group	It specifies the time group the rule uses, which is used to specify the time period during which the rule is effective. The time group rule should be configured in advance in the **Time Group Settings** module on the **Filter Management** > **IP Group/Time Group** page.
URL	It specifies the URL category the rule uses. The URL category should be configured in advance.
Status	It specifies the status of the URL filter rule. You can enable or disable the rule as required.
Operation	It specifies the operations you can perform on the rule. ✎: Click it to edit the rule. 🗑 : Click it to delete the rule.
URL Management	It specifies the customized URL category. Tip The device does not have a pre-set default URL category.

Configure a URL filter rule

Enable the URL filter function

On the **Filter Management** > **URL Filter** page, toggle on **URL Filter**, and click **Save**.

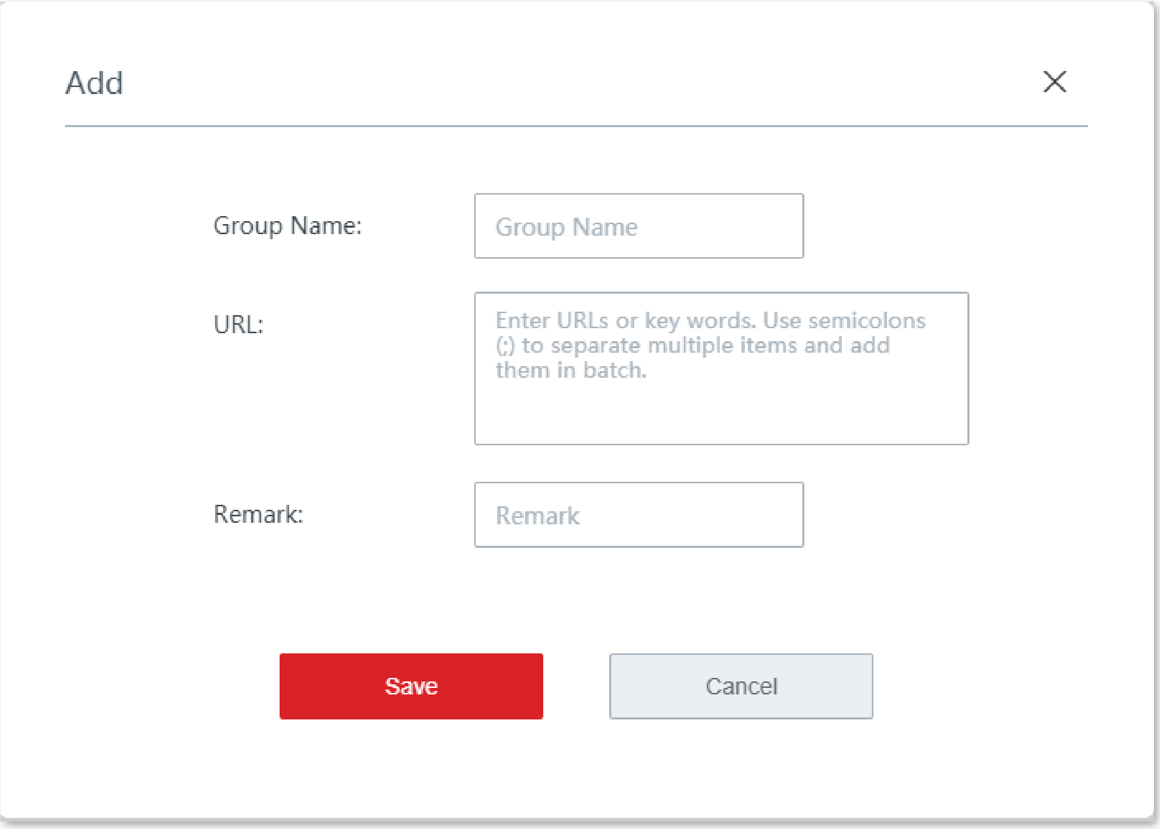


URL Filter

URL Filter: ●

Add a customized URL group

1. On the **Filter Management** > **URL Filter** page, click **URL Management**.
2. Click **New**.
3. Configure parameters in the **Add** window.
4. Click **Save**.



Add

Group Name: Group Name

URL: Enter URLs or key words. Use semicolons (;) to separate multiple items and add them in batch.

Remark: Remark

----End

Parameter description

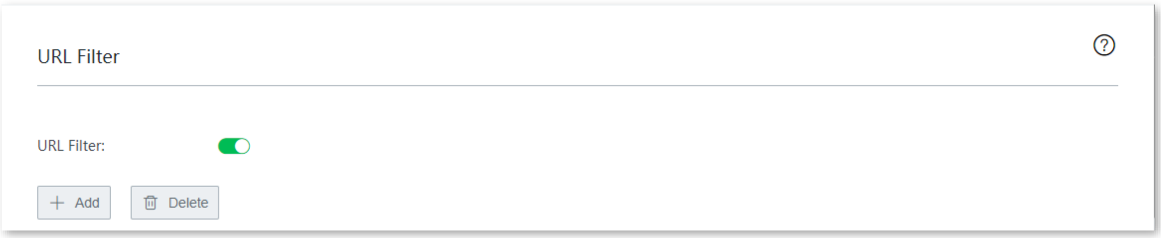
Parameter	Description
Group Name	It specifies the name of the URL group. The name cannot be duplicated.
URL	It specifies the domain name or the keywords of the domain name of the website to be blocked. Use semicolons (;) to separate multiple domain names or keywords of domain names. Tip When you enter keywords of the domain name, make sure the keywords unchanged. For example, for www.facebook.com, you should enter **facebook** rather than **Facebook**.
Remark	It specifies the remark of the URL group.

Add a URL filter rule

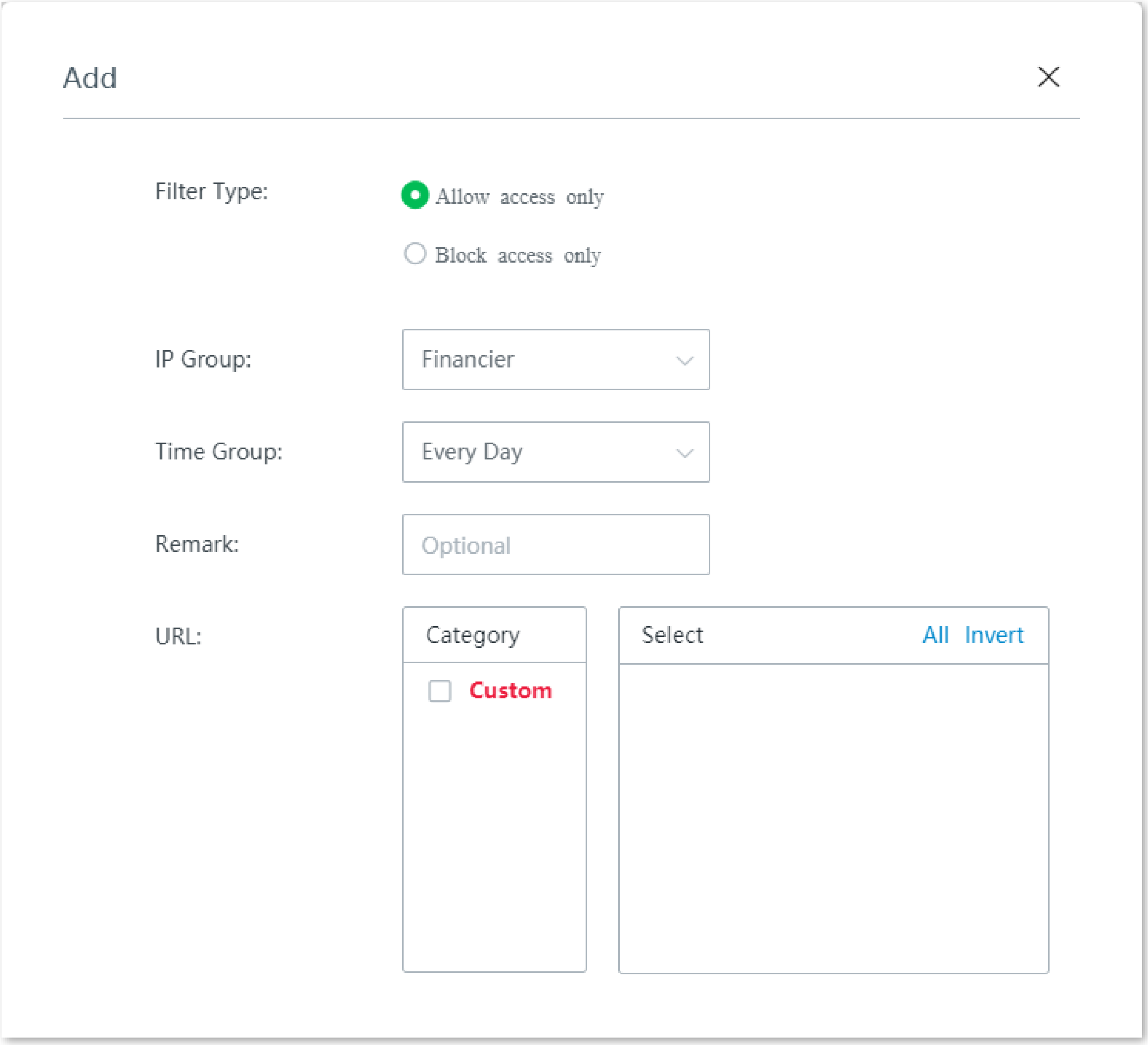
Tip

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

1. On the **Filter Management** > **URL Filter** page, click **+ Add**.



2. Configure parameters in the **Add** window.
3. Click **Save**.



Add

Filter Type: ● Allow access only ○ Block access only

IP Group: Financier

Time Group: Every Day

Remark: Optional

URL:

----End

Example of configuring a URL filter rule

Networking requirement

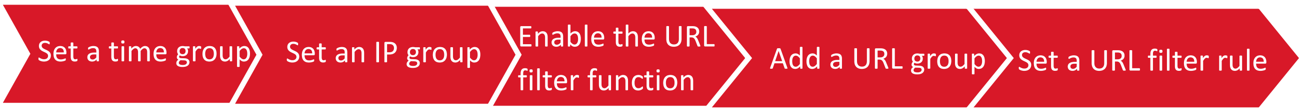
An enterprise uses cable-free devices to set up a network. The enterprise has the following requirements:

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

Solution

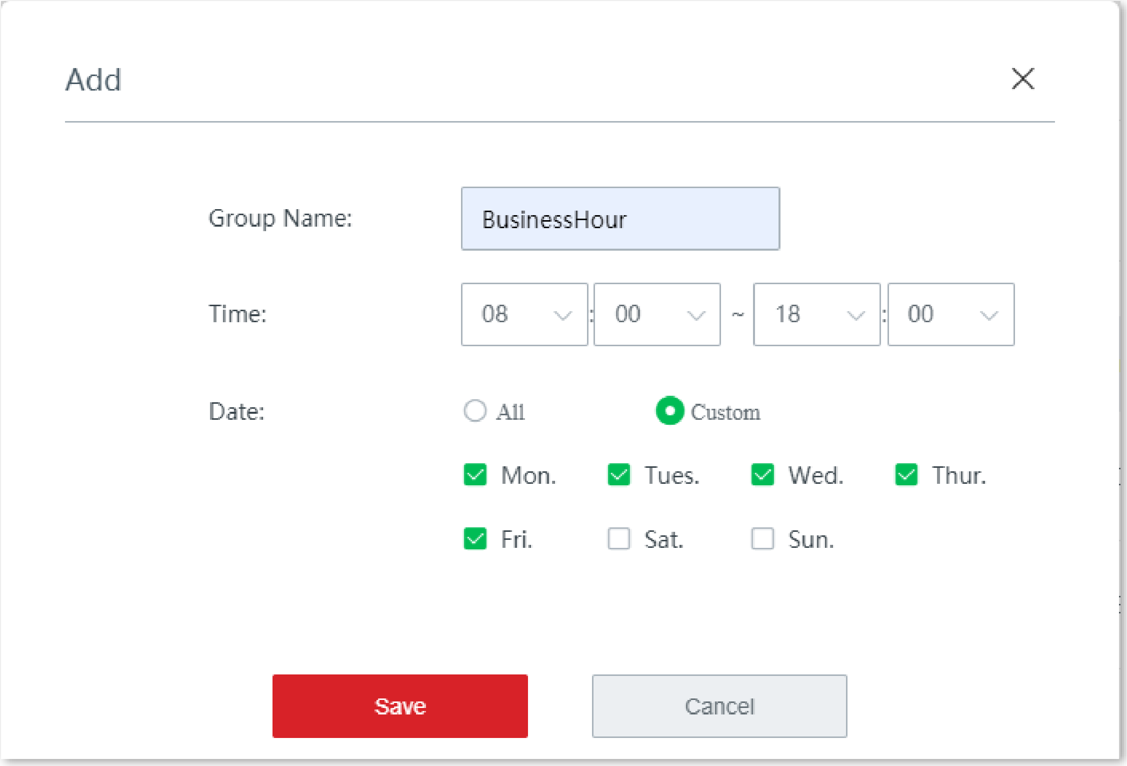
You can use the **URL Filter** function to meet this requirement. Assume that the IP addresses of the designing department staff range from 192.168.5.2 to 192.168.5.10.

Configuration procedures


Set a time group → Set an IP group → Enable the URL filter function → Add a URL group → Set a URL filter rule

I. Set a time group.

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



Group Name: BusinessHour

Time: 08 : 00 ~ 18 : 00

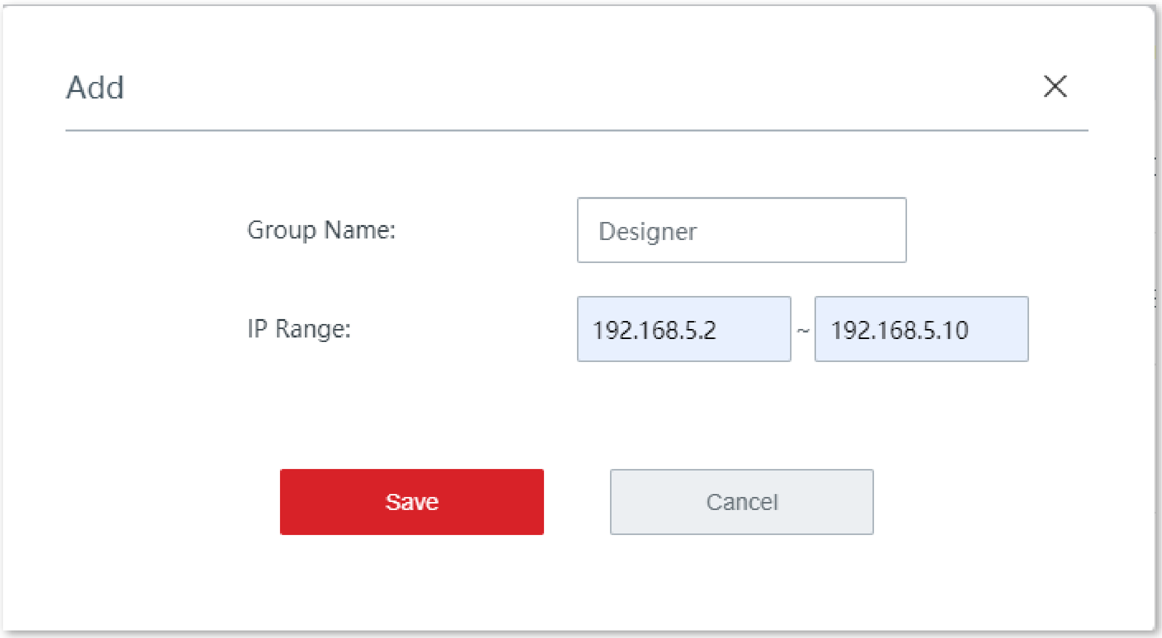
Date: ○ All ● Custom

☑ Mon. ☑ Tues. ☑ Wed. ☑ Thur.

☑ Fri. □ Sat. □ Sun.

II. Set an IP group.

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



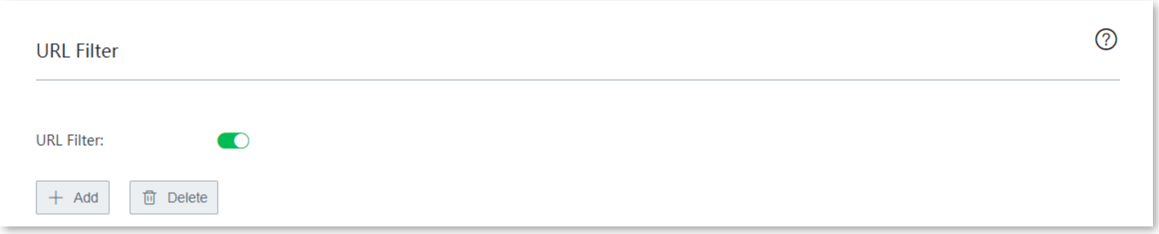
Add

Group Name: Designer

IP Range: 192.168.5.2 ~ 192.168.5.10

III. Enable the URL filter function.

1. On the **Filter Management** > **URL Filter** page, toggle on **URL Filter**.
2. Click **Save**.

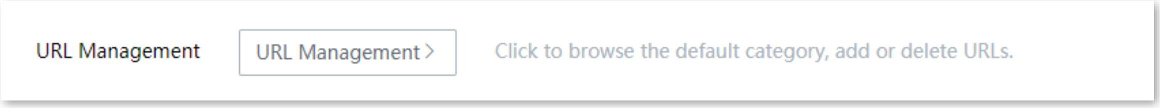


URL Filter

URL Filter: ●

IV. Add a URL group.

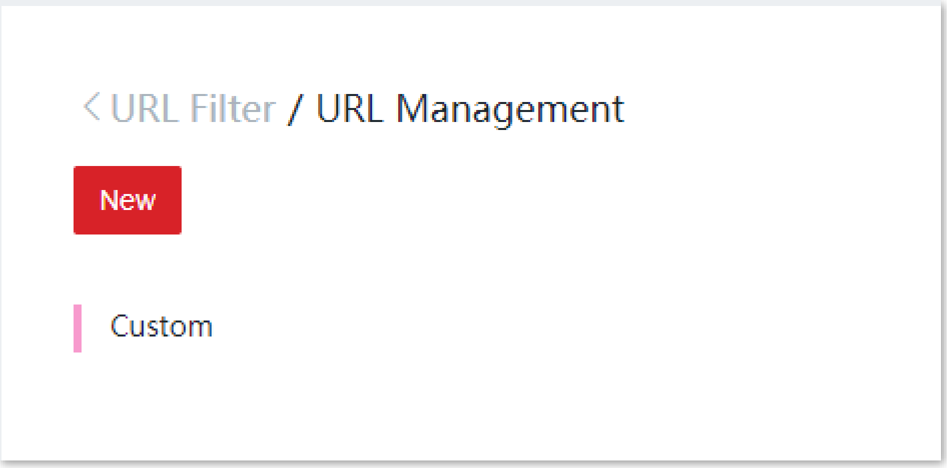
1. On the **Filter Management** > **URL Filter** page, click **URL Management**.



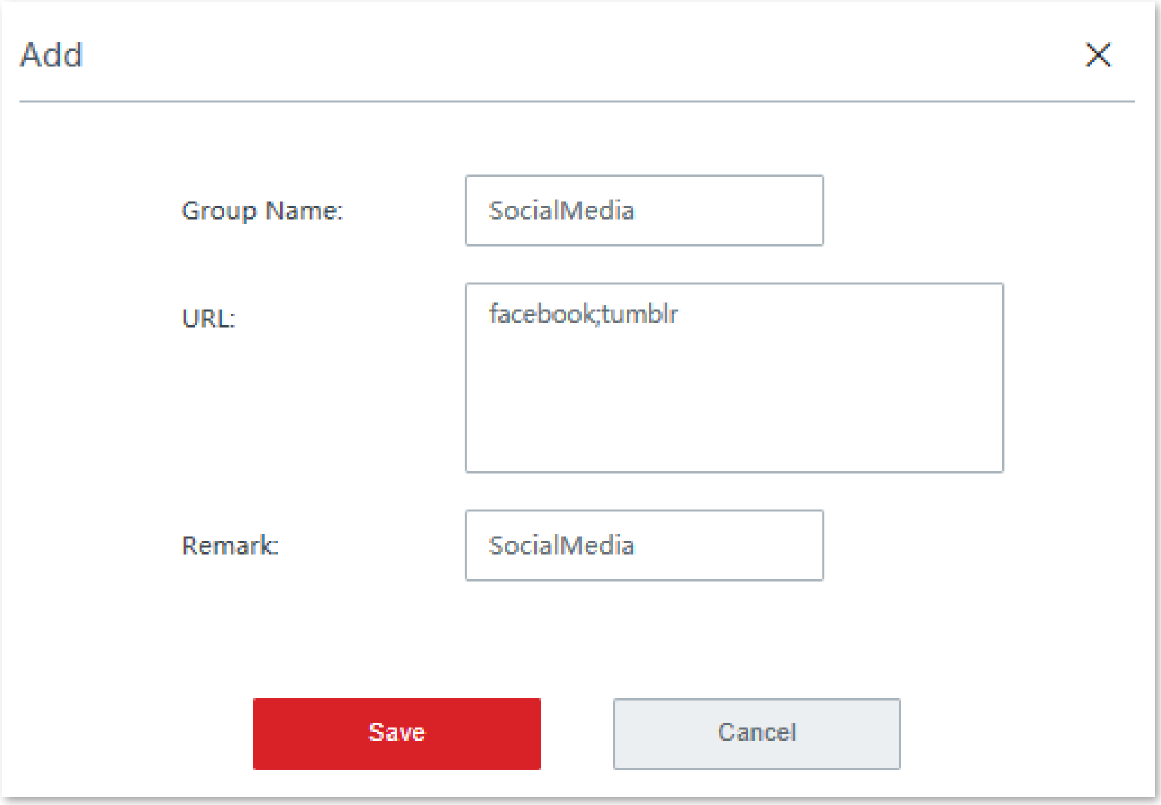
URL Management

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

2. Click **New**.



3. Configure parameters in the **Add** window, and click **Save**.
   (1) Set **Group Name**, which is **SocialMedia** in this example.
   (2) Enter the keywords of the domain name of the website to be blocked, which is **facebook;tumblr** in this example.
   (3) Set the remarks of the URL group, for example, **SocialMedia**.



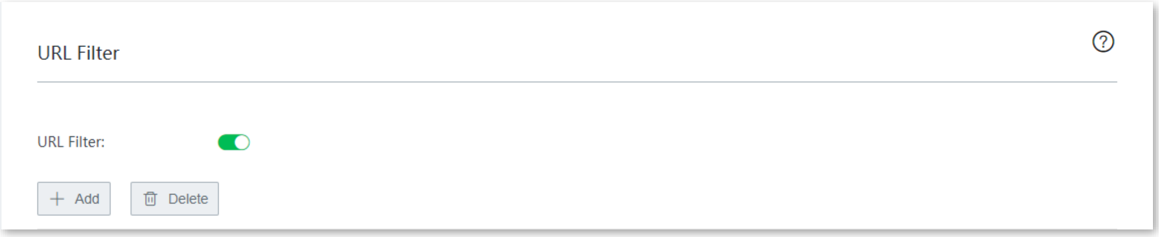
Group Name: SocialMedia

URL: facebook;tumblr

Remark: SocialMedia

V. Set a URL filter rule.

1. On the **Filter Management** > **URL Filter** page, click **+ Add**.



URL Filter

URL Filter: ●

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

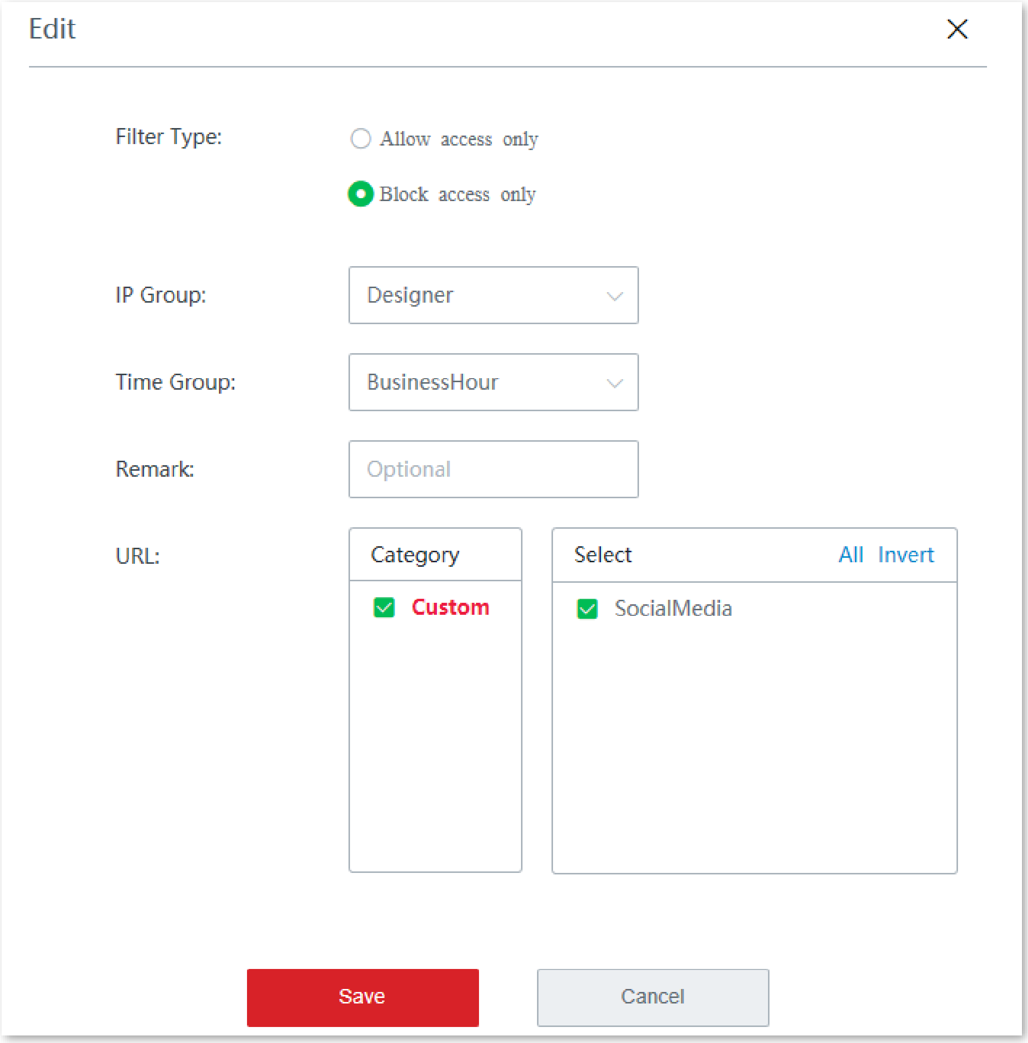
(1) Choose **Block access only** for **Filter Type**.

(2) Select the target IP group, which is **Designer** in this example.

(3) Select the target time group, which is **BusinessHour** in this example.

(4) (Optional) Set the remarks of the URL filter rule. You can also choose to leave it blank.

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



Edit

Filter Type: ○ Allow access only ● Block access only

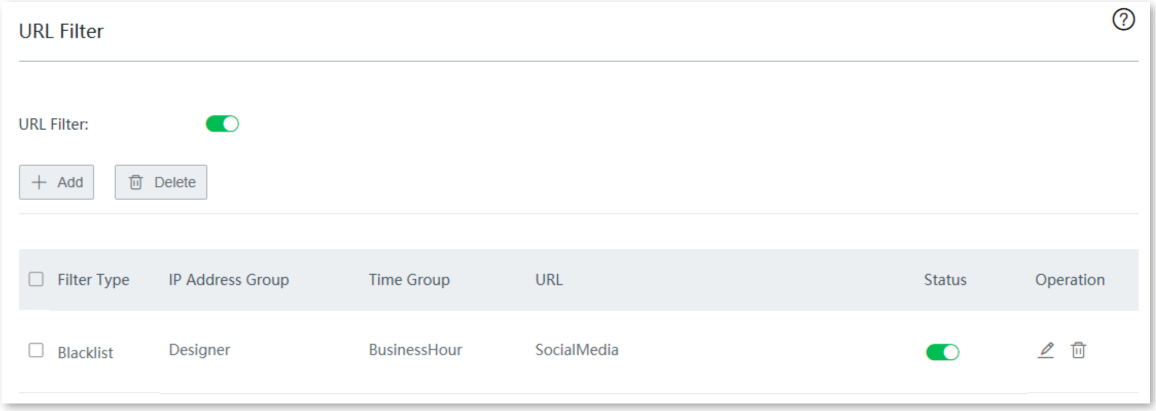
IP Group: Designer

Time Group: BusinessHour

Remark: Optional

URL: Category: ☑ Custom; Select: ☑ SocialMedia

The URL filter rule is added successfully. See the following figure.



URL Filter

URL Filter:

□ Filter Type	IP Address Group	Time Group	URL	Status	Operation
□ Blacklist	Designer	BusinessHour	SocialMedia	●	

----End

Verification

In the LAN during 8:00 to 18:00 from Monday to Friday, computers with an IP address ranging from 192.168.5.2 to 192.168.5.10 cannot access the websites specified in the SocialMedia URL group.

3.10 More

3.10.1 Static routing

Overview

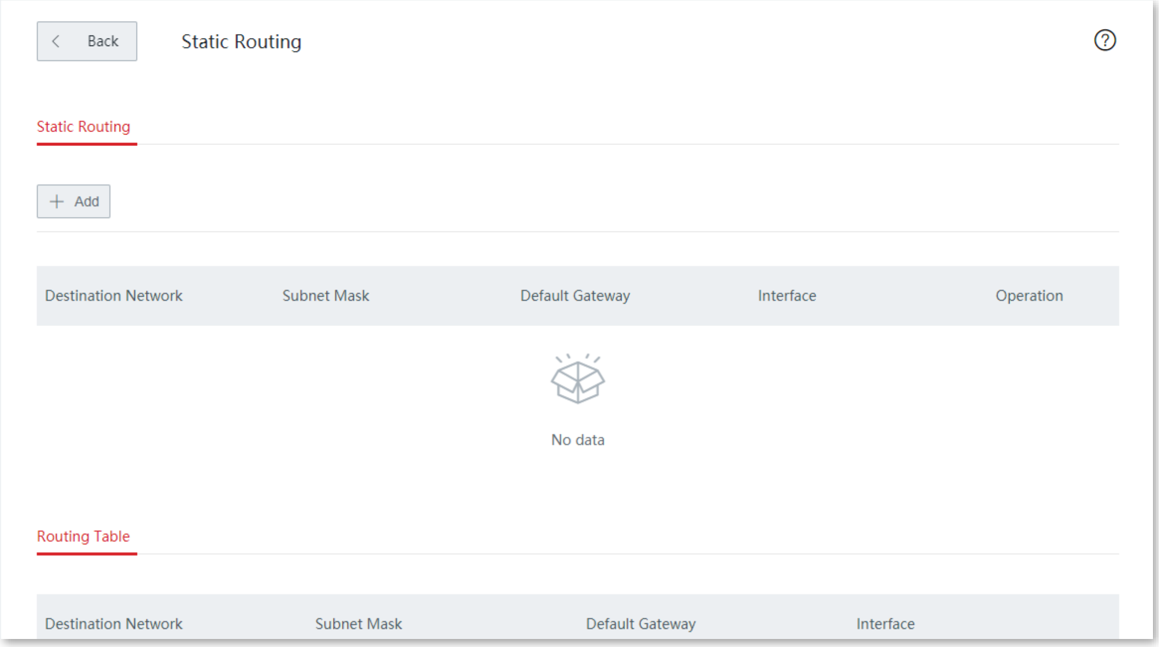
Routing is an operation to choose an optimum path to convey data from the source address to the target address. Static route is a manually-configured special route and is simpler, more efficient, and more reliable. An appropriate static route can reduce issues arising from route selection and ease the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

You can specify a static route by setting **Destination Network**, **Subnet Mask**, **Default Gateway**, and **Interface**. Among these parameters, **Destination Network** and **Subnet Mask** are used to specify a destination network or host. After the static route is configured successfully, all the data whose destination address is the destination network of the static route is directly forwarded to the gateway address through the interface of the static route.

Note

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

Click **More** > **Static Routing** to enter the page. See the following figure.



Parameter description

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

Example of configuring static routing

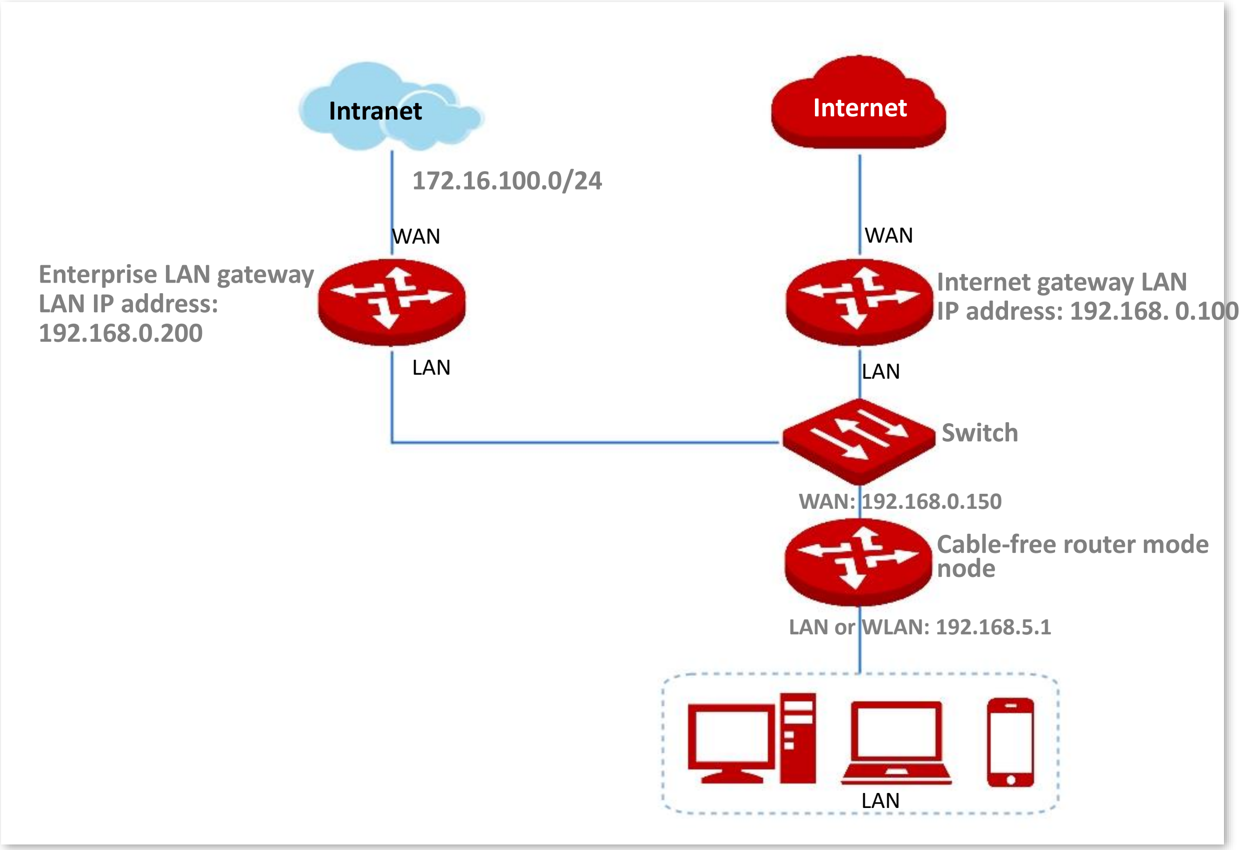
Networking requirement

An enterprise uses cable-free devices to set up a network. The enterprise has the following requirements:

The internet and the intranet are deployed on different networks and the node accesses the internet by automatically obtaining an IP address from the internet gateway. LAN users can access both the internet and the intranet.

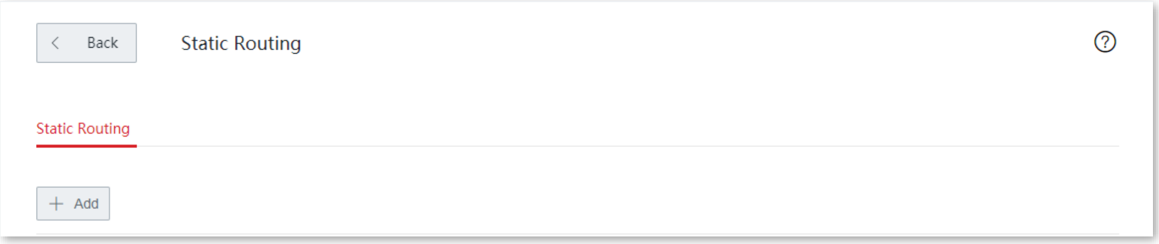
Solution

You can use the **Static Routing** function to meet this requirement. See the following topology.

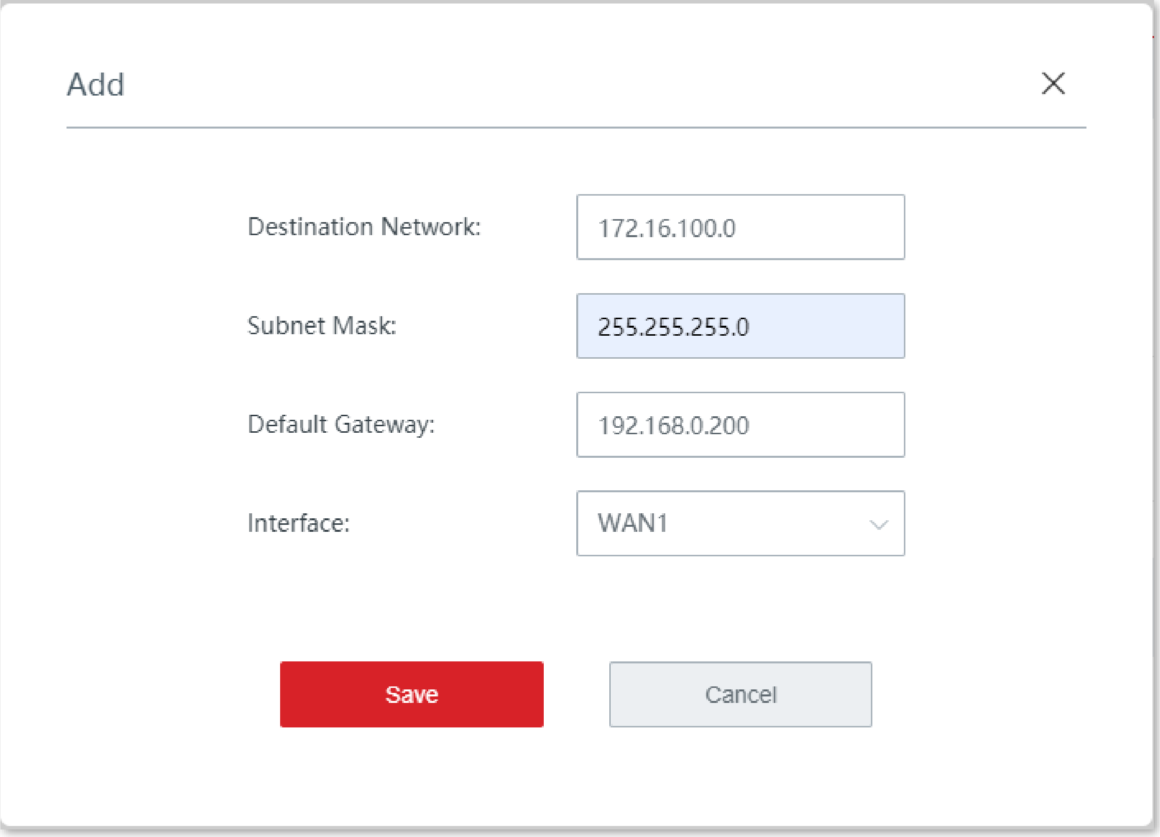


Configuration procedures

1. On the **More** > **Static Routing** page, click **+ Add**.



2. Configure parameters in the **Add** window.
   (1) Enter **Destination Network** (the IP address of the target network), which is **172.16.100.0** in this example.
   (2) Enter **Subnet Mask** (the subnet mask of the target network), which is **255.255.255.0** in this example.
   (3) Enter **Default Gateway** (the ingress port IP address of the next hop route), which is **192.168.0.200** in this example.
   (4) Select **Interface** (the interface over which the node communicates with the target network), which is **WAN1** in this example.
3. Click **Save**.



Add

Destination Network: 172.16.100.0

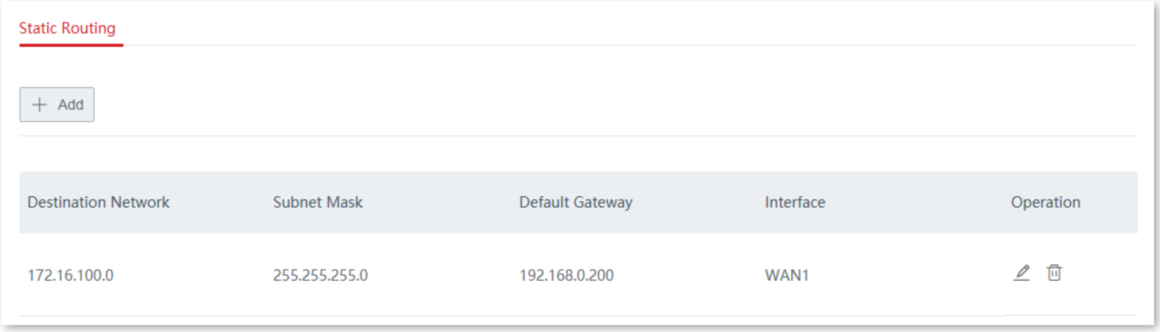
Subnet Mask: 255.255.255.0

Default Gateway: 192.168.0.200

Interface: WAN1

----End

The static route is added successfully. See the following figure.



Static Routing

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

Verification

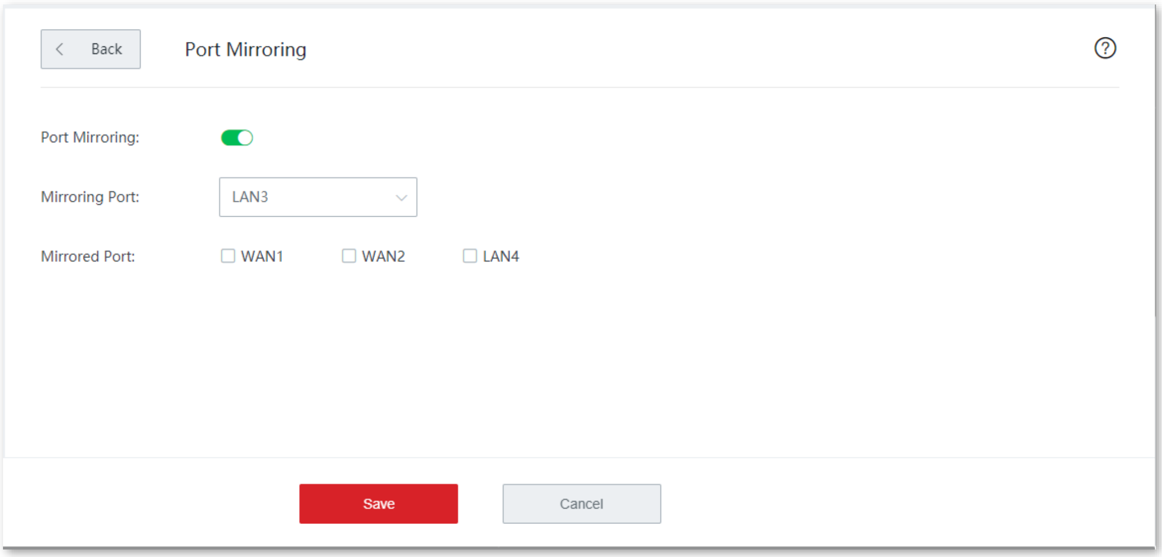
LAN users can access both the internet and the intranet.

3.10.2 Port mirroring

On this page, you can copy the data of the mirrored port to the specified port (mirroring port). Generally, the mirroring port is connected with a data monitoring device for the network administrator to perform real-time flow monitoring, performance analysis, and fault diagnosis.

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

The port mirroring function is disabled by default. The following displays the page when the function is enabled.



Port Mirroring: ●

Mirroring Port: LAN3

Mirrored Port: □ WAN1 □ WAN2 □ LAN4

Parameter description

Parameter	Description
Port Mirroring	It specifies whether to enable the port mirroring function. ○ indicates the function is disabled and ● indicates the function is enabled.
Mirroring Port	It specifies the monitoring port. Devices connected to this port should be installed with monitoring software. By default, the mirroring port is LAN3.
Mirrored Port	It specifies the port to be monitored. After the port mirroring function is enabled, the data of the mirrored port will be copied to the mirroring port.

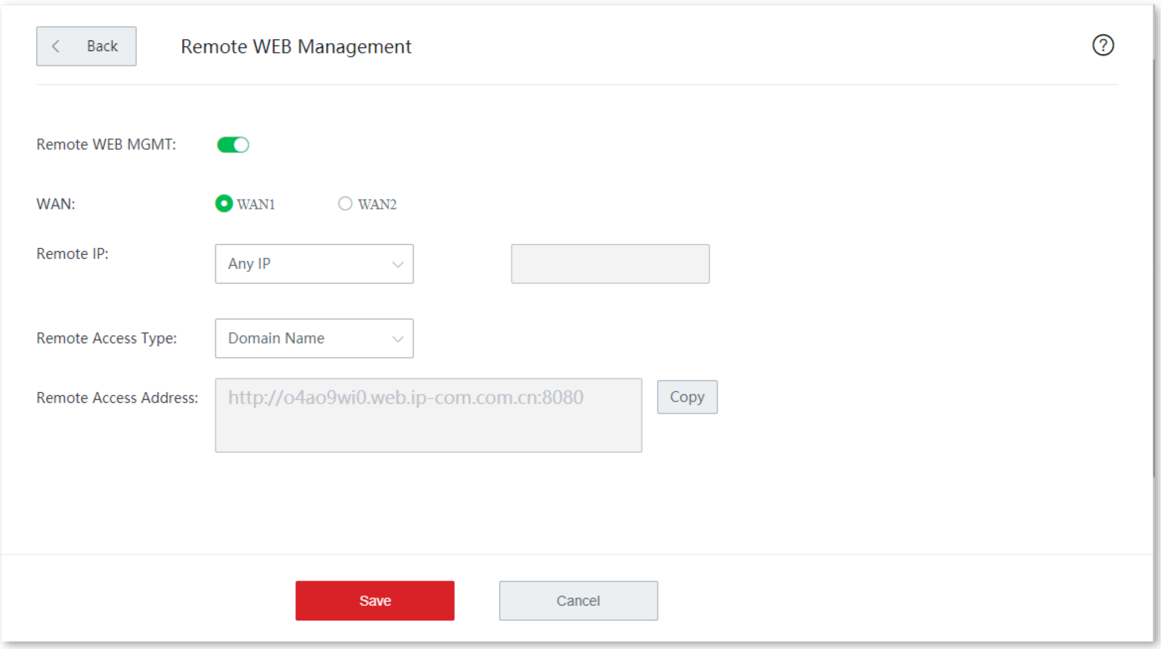
3.10.3 Remote WEB management

Overview

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

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

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



Remote WEB MGMT: ●

WAN: ● WAN1 ○ WAN2

Remote IP: Any IP

Remote Access Type: Domain Name

Remote Access Address: http://o4ao9wi0.web.ip-com.com.cn:8080

Parameter description

Parameter	Description
Remote WEB MGMT	It specifies whether to enable the remote web management function. ○ indicates the function is disabled and ● indicates the function is enabled.
WAN	It specifies the WAN port of the node, which is also the WAN port used to remotely access the web UI of the node.
Remote IP	It specifies the IP address of the device to remotely access the web UI of the node. – **Any IP**: It indicates that devices with any IP addresses on the internet can access the web UI of the node. For network security, this option is not recommended. – **Specified IP**: It indicates that only the device with the specified IP address can remotely access the web UI of the node. If the device is deployed in the LAN, enter the IP address of the gateway of the device (the public IP address).
Remote Access Type	It specifies the way in which the remote access is achieved. – **Domain Name**: The domain name type is the default type. The node automatically generates a unique remote management address and internet users can visit this address to log in to the web UI of the node. – **IP Address**: Internet users enter **http://the IP address of the WAN port of the node:port number** in the address bar of a browser to access the web UI of the node.

Parameter	Description
Remote Access Address	This parameter appears when **Remote Access Type** is set to **Domain Name**. It specifies the domain name used to remotely access the node. After you enabled **Remote WEB MGMT** and selected **Domain Name** for **Remote Access Type**, internet users can use this domain name to log in to the web UI of the node.
Port	This parameter appears when **Remote Access Type** is set to **IP Address**. It specifies the port used to remotely access the node. The default port is **8088** and you can change it as needed. Ports 1 to 1024 are occupied by well-known services and, to avoid port conflict, you are recommended to change the port to one between port 1025 to 65535.

Example of configuring remote web management

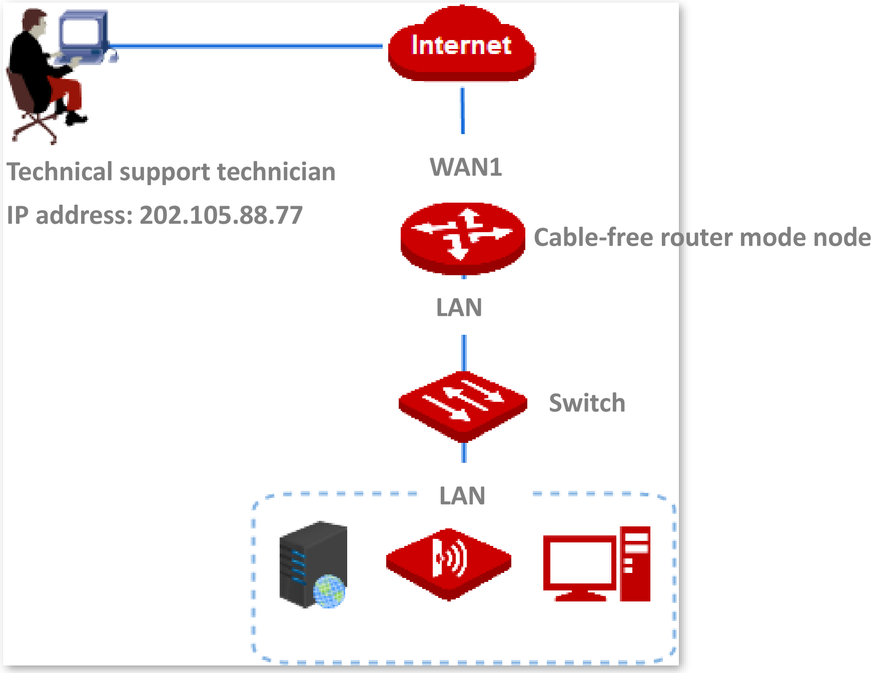
Networking requirement

An enterprise uses cable-free devices to set up a network. The enterprise has the following requirements:

If the network administrator encountered a problem during network setup and is in need of the IP-COM technical support, the IP-COM technical support technician can remotely log in to the web UI of the device to perform analysis and troubleshooting.

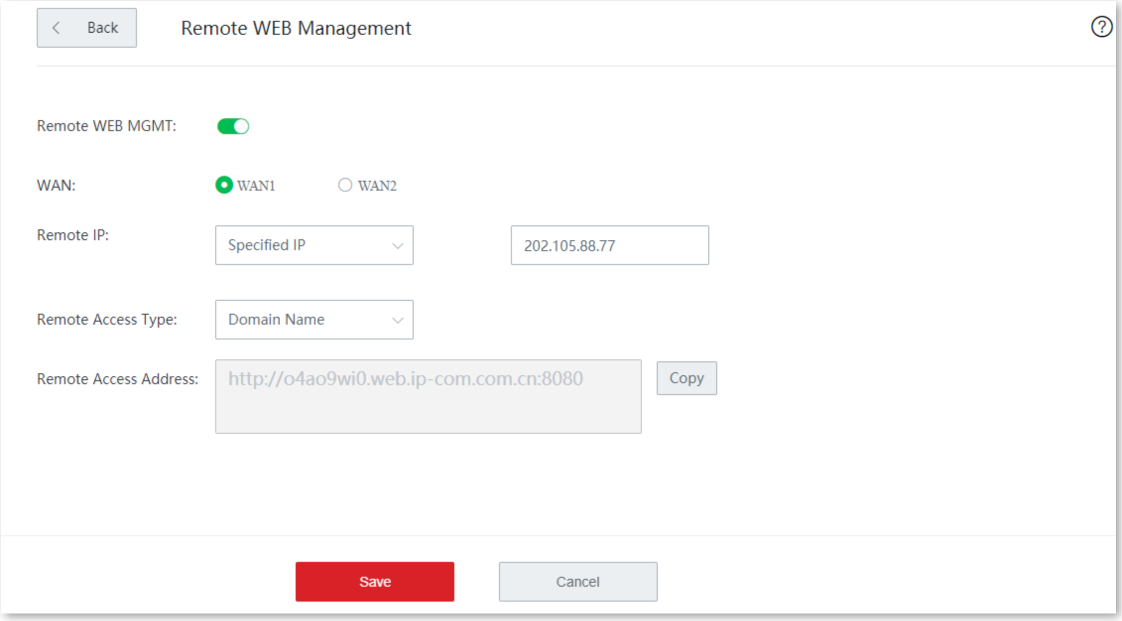
Solution

You can use the **Remote WEB Management** function to meet this requirement. See the following figure.


Internet
Technical support technician
IP address: 202.105.88.77
WAN1
Cable-free router mode node
LAN
Switch
LAN

Configuration procedures

1. Click **More** > **Remote WEB Management**.
2. Toggle on **Remote WEB MGMT**.
3. Click the **Remote IP** drop-down list, select **Specified IP**, and enter the IP address of the computer of the IP-COM technical support technician, which is **202.105.88.77** in this example.
4. Click **Save**.



Remote WEB MGMT: ●

WAN: ● WAN1 ○ WAN2

Remote IP: Specified IP 202.105.88.77

Remote Access Type: Domain Name

Remote Access Address: http://o4ao9wi0.web.ip-com.com.cn:8080

----End

Verification

The IP-COM technical support technician can log in to the web UI of the cable-free device by visiting http://o4ao9wi0.web.ip-com.com.cn:8080 on his or her computer (the IP address of the computer is 202.105.88.77).

3.10.4 DDNS

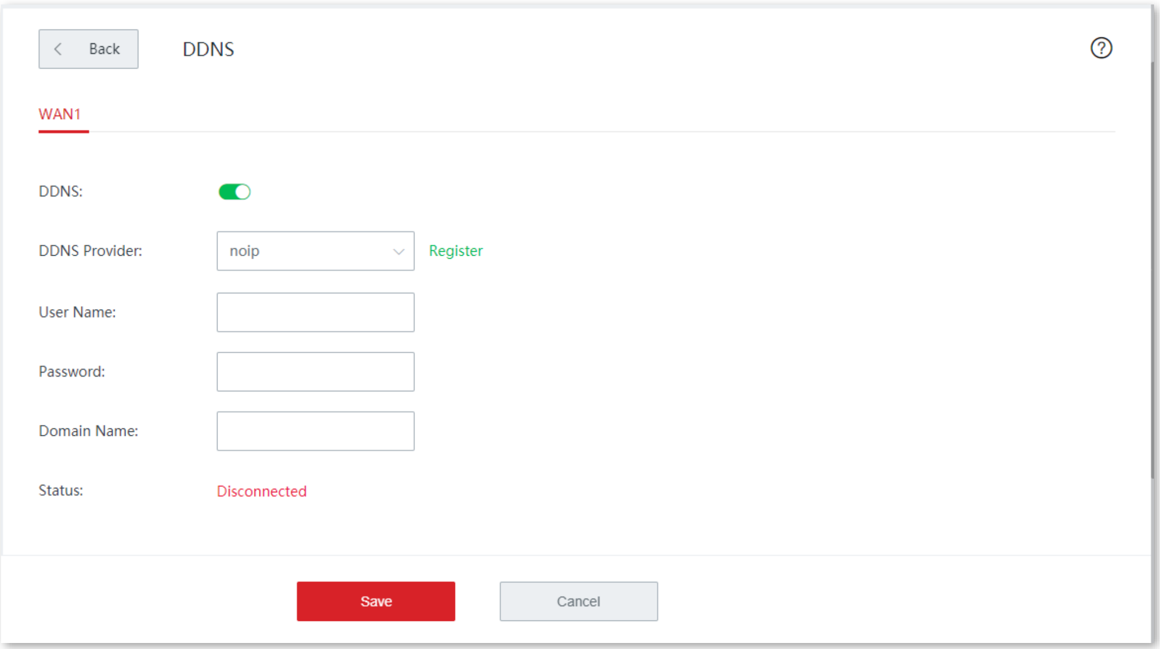
Overview

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

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

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

The DDNS function is disabled by default. The following displays the page when the function is enabled.



DDNS: ●

DDNS Provider: noip Register

User Name:

Password:

Domain Name:

Status: Disconnected

Parameter description

Parameter	Description
DDNS	It specifies whether to enable the DDNS function. ○ indicates the function is disabled and ● indicates the function is enabled.
DDNS Provider	It specifies the DDNS provider. The node supports **noip**, **dyndns**, **oray**, and **gnway**.
Service Type	It specifies the type of the DDNS account. This parameter appears when **DDNS Provider** is set to **oray**. Only common services are supported for now.
User Name Password	It specifies the user name/password used to log in to the DDNS service. It is the login username and password applied from the DDNS provider.
Domain Name	It specifies the domain name obtained from the DDNS provider. If **DDNS Provider** is set to other DDNS provider other than **oray**, you need to manually enter the domain name applied from the target website.
Status	It specifies the DDNS service status.

Example of configuring DDNS

Networking requirement

An enterprise uses a cable-free device to set up a network. The device has connected to the internet and can offer internet service to LAN users. The enterprise has the following requirements:

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

Solution

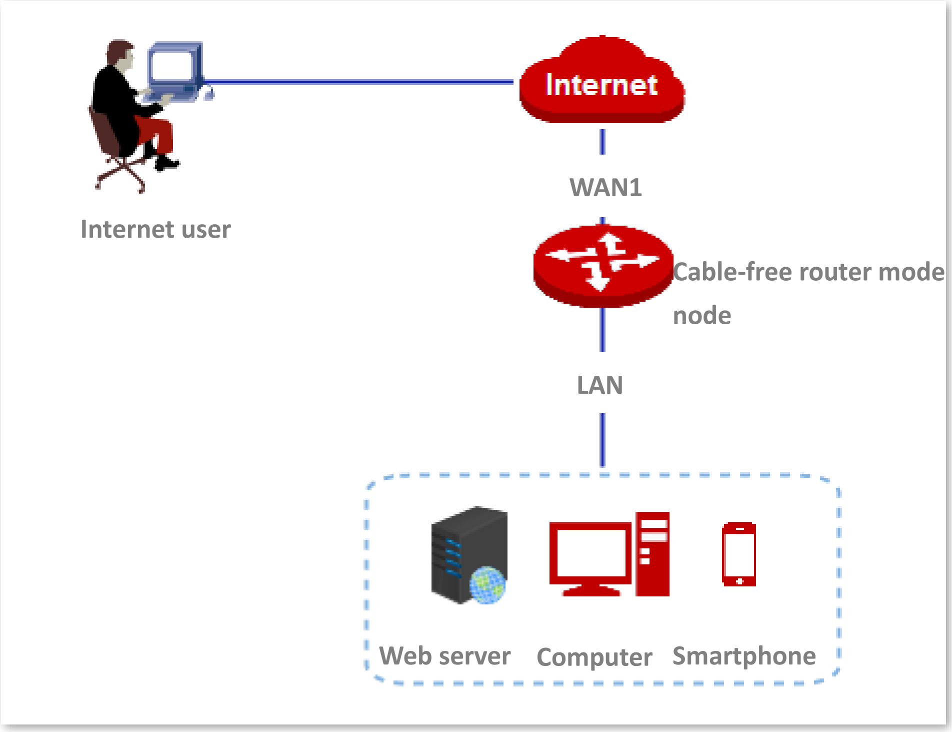
- You can use the **Port Forwarding** function to enable internet users to access the intranet web server.
- You can use the **DDNS** function to enable internet users to access the intranet web server through a fixed domain name, avoiding access failure caused by WAN IP address change.
- You can use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

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

- IP address of the web server: 192.168.5.250
- MAC address of the host that runs the web server: C8:9C:DC:60:54:69
- Service port: 9999

Tip

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



Configuration procedures

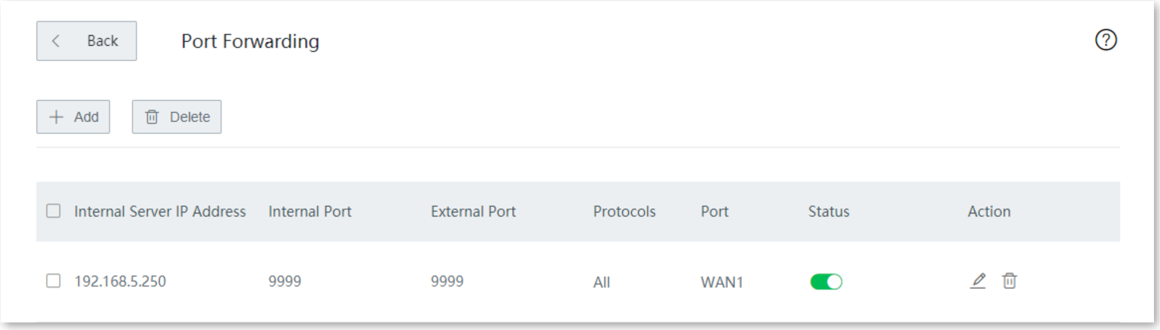
Set port forwarding

Reserve a fixed IP address for the server host

Set DDNS

I. Set port forwarding.

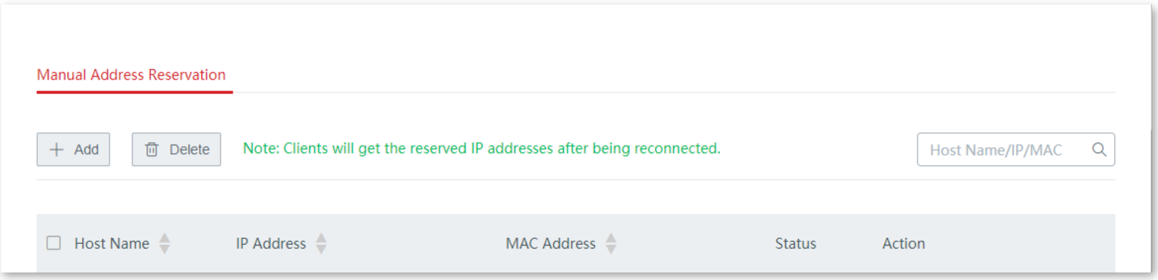
On the **More** > **Port Forwarding** page, set the following rule. See configuring port forwarding.



□ Internal Server IP Address	Internal Port	External Port	Protocols	Port	Status	Action
□ 192.168.5.250	9999	9999	All	WAN1	●	

II. Reserve a fixed IP address for the server host.

1. Click **Address Reservation** and locate the **Manual Address Reservation** module.
2. Click **+ Add**.

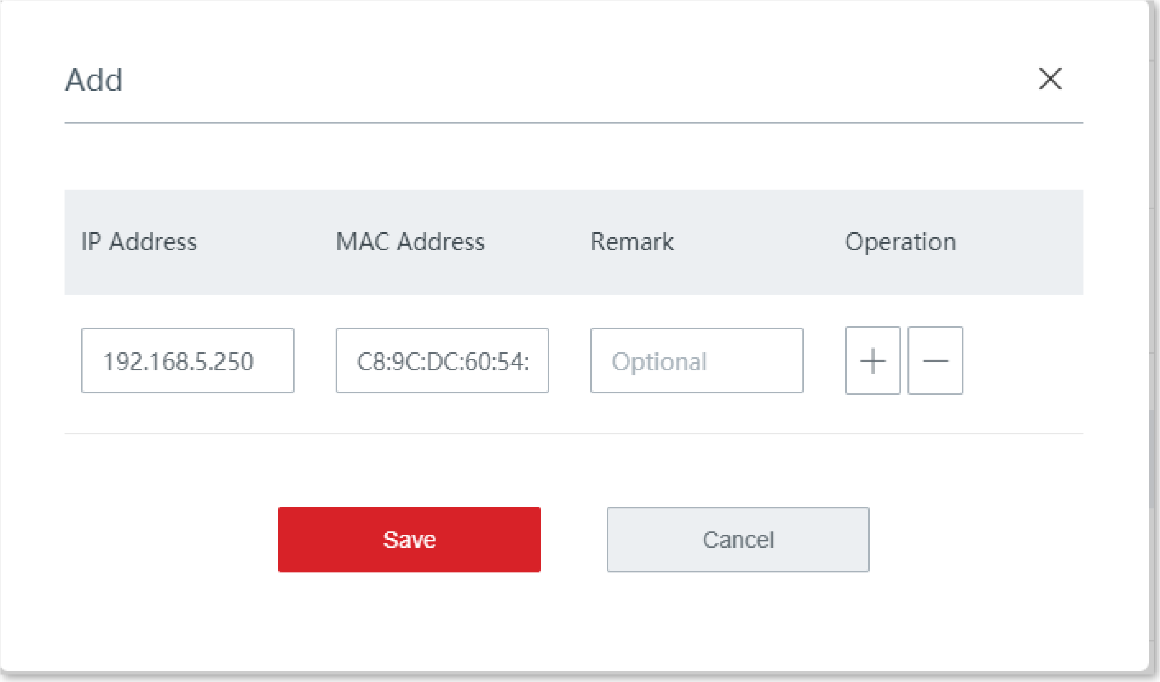


Manual Address Reservation

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

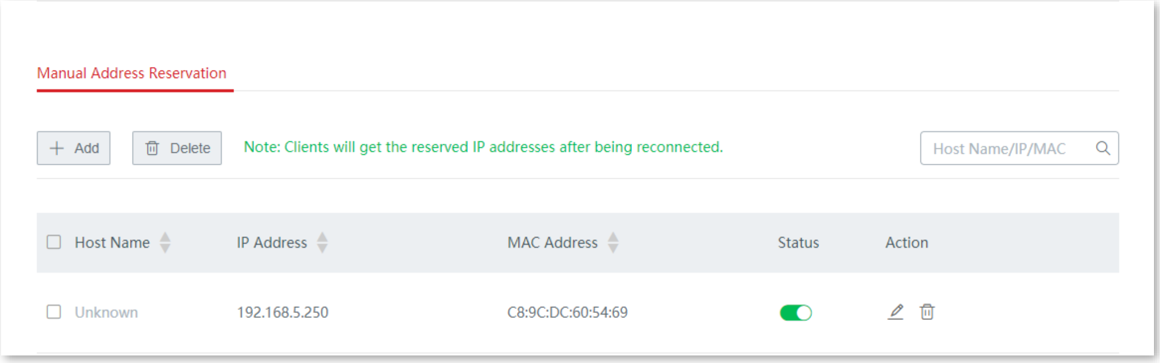
□ Host Name	IP Address	MAC Address	Status	Action

3. Configure parameters in the **Add** window, and click **Save**.
   (1) Set the fixed IP address assigned to the server host, which is **192.168.5.250** in this example.
   (2) Enter the MAC address of the server host, which is **C8:9C:DC:60:54:69** in this example.



IP Address	MAC Address	Remark	Operation
192.168.5.250	C8:9C:DC:60:54:	Optional	+ —

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



Manual Address Reservation

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

□ Host Name	IP Address	MAC Address	Status	Action
□ Unknown	192.168.5.250	C8:9C:DC:60:54:69	●	✎ 🗑

III. Set DDNS.

1. Register a domain name.

   Log in to the DDNS provider website. Assume that the DDNS provider where you applied the domain name is **noip**, the user name you registered is **IP-COM**, the password is **123456**, and the domain name is **ip-com.ddns.net**

2. Log in to the web UI of the node and set DDNS.

   (1) Click **More** > **DDNS** to enter the configuration page.

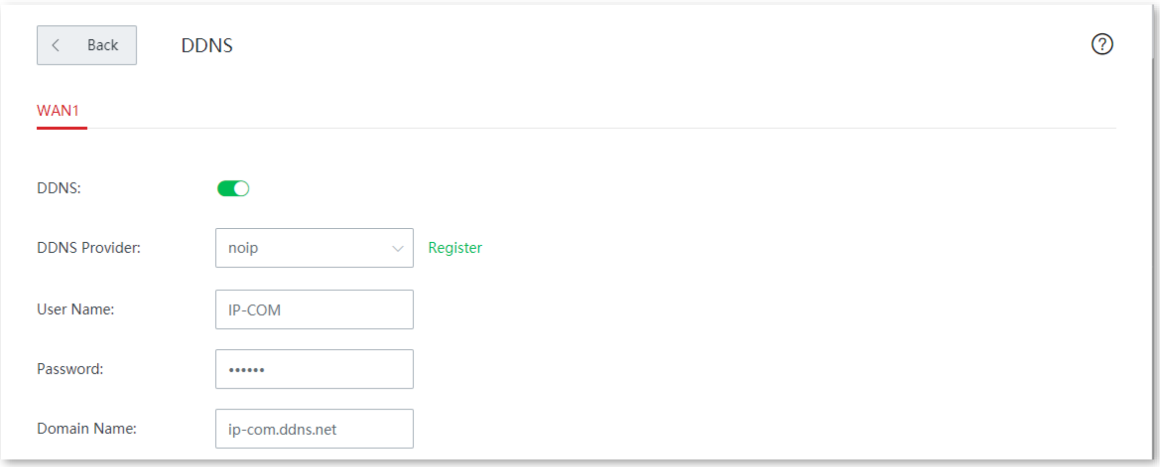
   (2) Toggle on **DDNS**.

   (3) Click the **DDNS Provider** drop-down list and select **noip**.

   (4) Enter the user name and password, which is **IP-COM** and **123456** in this example.

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

   (6) Click **Save**.



DDNS:

DDNS Provider: noip

User Name: IP-COM

Password: ••••••

Domain Name: ip-com.ddns.net

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

----End

Verification

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

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

Tip

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

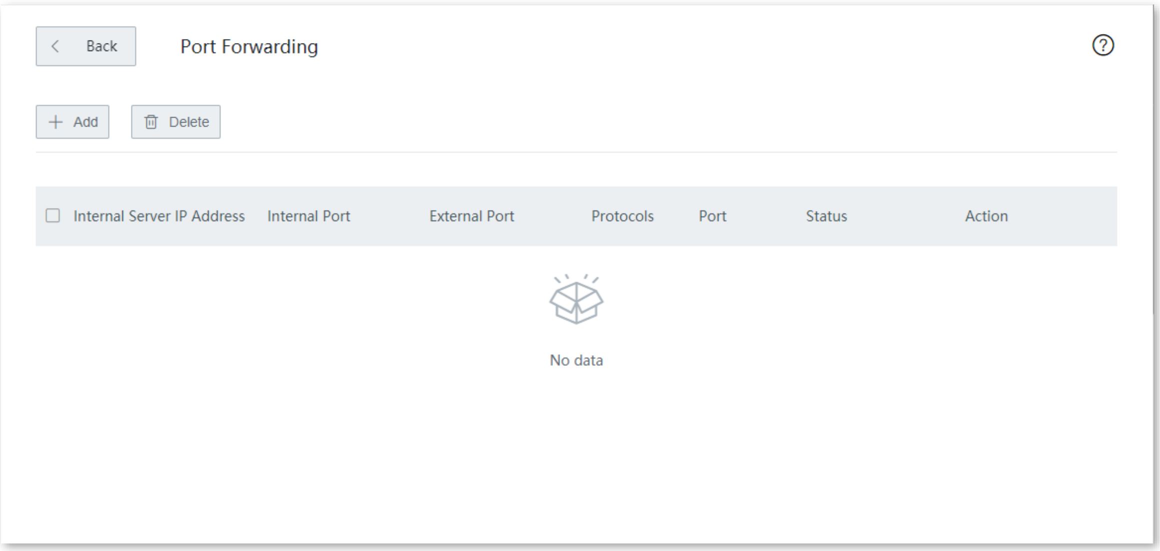
- Make sure that the internal port you entered is correct.
- Maybe the system firewall, anti-virus software and security guard on the LAN server blocked internet user access. Please disable these programs and try again.

3.10.5 Port forwarding

Overview

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

Click **More** > **Port Forwarding** to enter the page. See the following figure.



□ 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 the internal server.
Internal Port	It specifies the service port of the internal server.
External Port	It specifies the port opened to internet users to access.

Parameter	Description
Protocols	It specifies the type of the transfer layer protocol used by the LAN service. **All** indicates both TCP and UDP. Select **All** if you are uncertain about the service type.
Port	It specifies the WAN port internet users use to access the LAN service.
Status	It specifies the status of the rule. You can enable or disable the rule as required.
Action	It specifies the operations you can perform on the rule. ✎: Click it to edit the rule. 🗑 : Click it to delete the rule.

Example of configuring port forwarding

Networking requirement

An enterprise uses a cable-free device to set up a network. The device has connected to the internet and can offer internet service to LAN users. The enterprise has the following requirements:

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

Solution

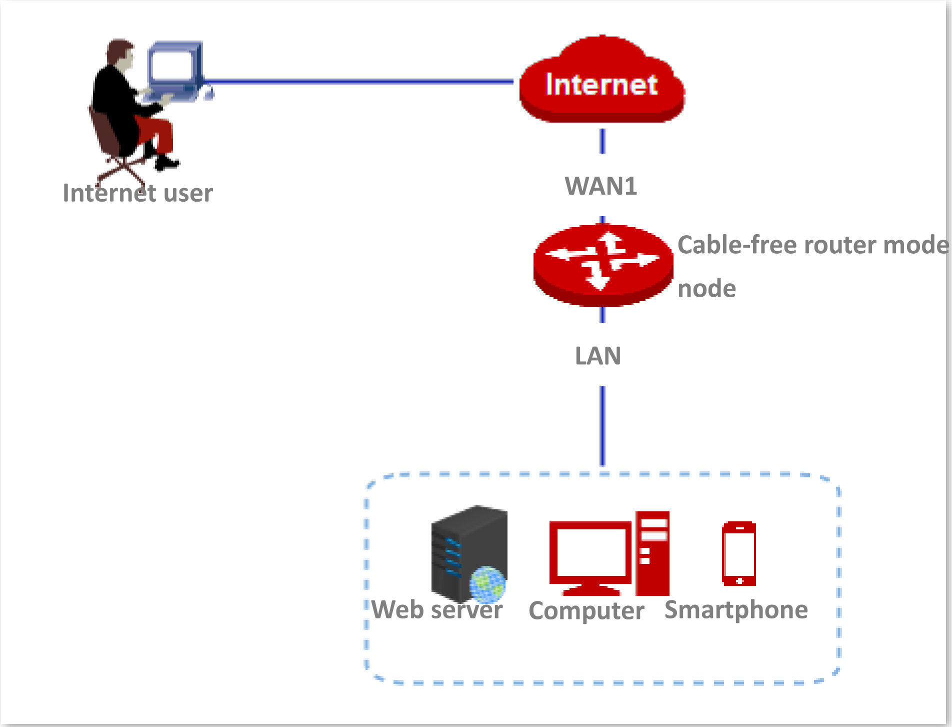
- You can use the **Port Forwarding** function to enable internet users to access the intranet web server. Assume that the open port of the cable-free device is 9999.
- You can use the **Address Reservation** function to avoid access failure caused by web server address change.

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

- IP address of the web server: 192.168.5.250
- MAC address of the host that runs the web server: C8:9C:DC:60:54:69
- Service port: 9999

Tip

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

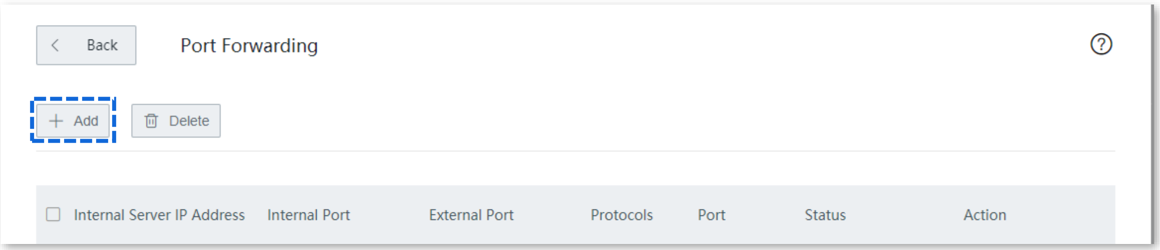


Configuration procedures

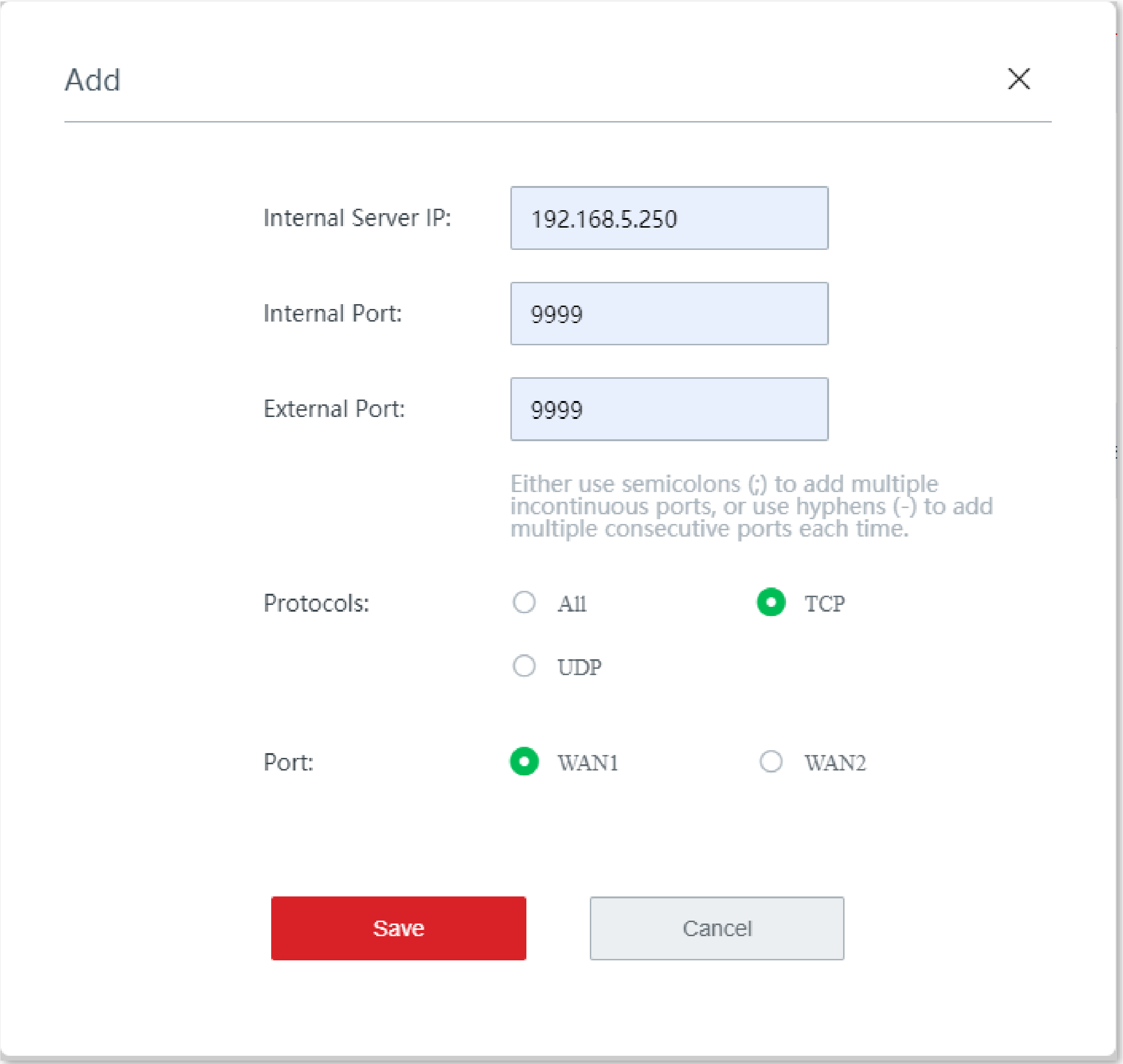
Set port forwarding → Reserve a fixed IP address for the server host

I. Set port forwarding.

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



3. Configure parameters in the **Add** window, and click **Save**.
   (1) Enter the **Internal Server IP**, which is **192.168.5.250** in this example.
   (2) Enter the **Internal Port**, which is **9999** in this example.
   (3) Enter the **External Port**, which is **9999** in this example.
   (4) Choose the protocol used by the web server, which is **TCP** in this example.
   (5) Select **WAN1** as the port through which WAN users get access to the LAN server.



Add

Internal Server IP: 192.168.5.250

Internal Port: 9999

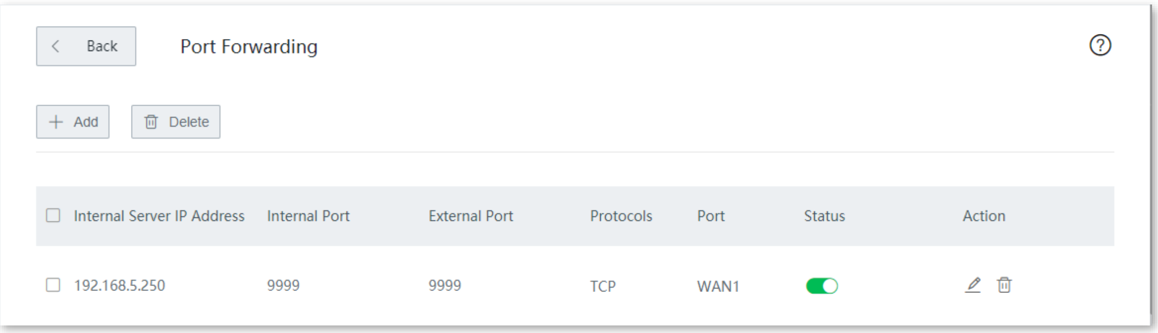
External Port: 9999

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

Protocols: ○ All ● TCP ○ UDP

Port: ● WAN1 ○ WAN2

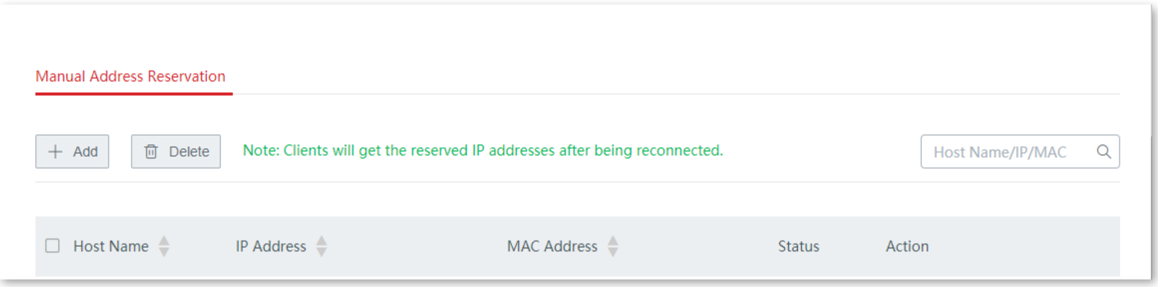
The port forwarding rule is configured successfully. See the following figure.



□ Internal Server IP Address	Internal Port	External Port	Protocols	Port	Status	Action
□ 192.168.5.250	9999	9999	TCP	WAN1	●	

II. Reserve a fixed IP address for the server host.

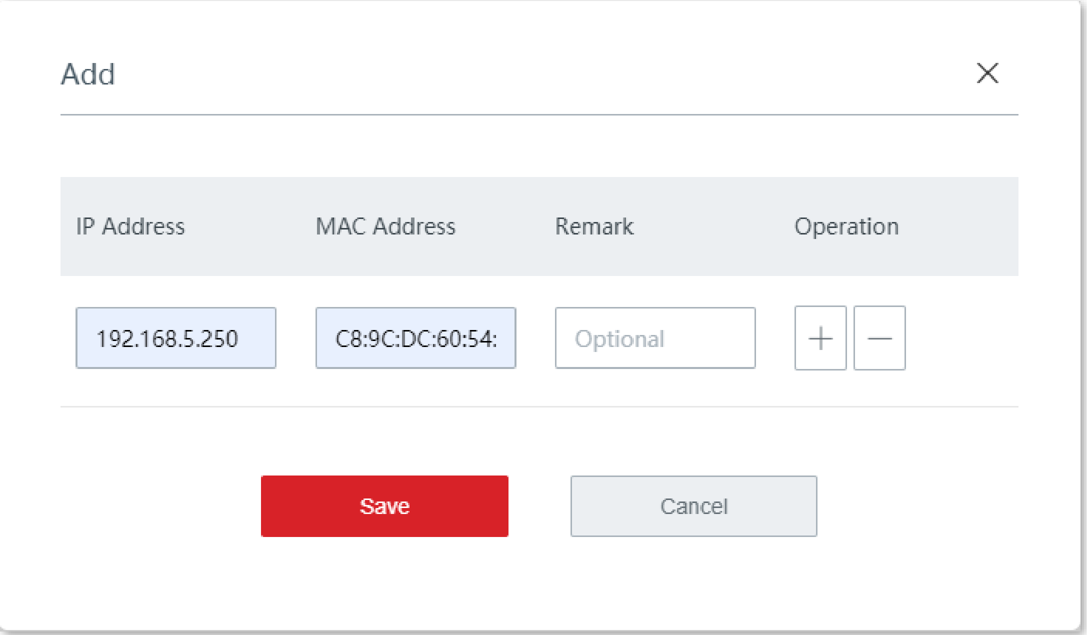
1. Click **Address Reservation** and locate the **Manual Address Reservation** module.
2. Click **+ Add**.



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

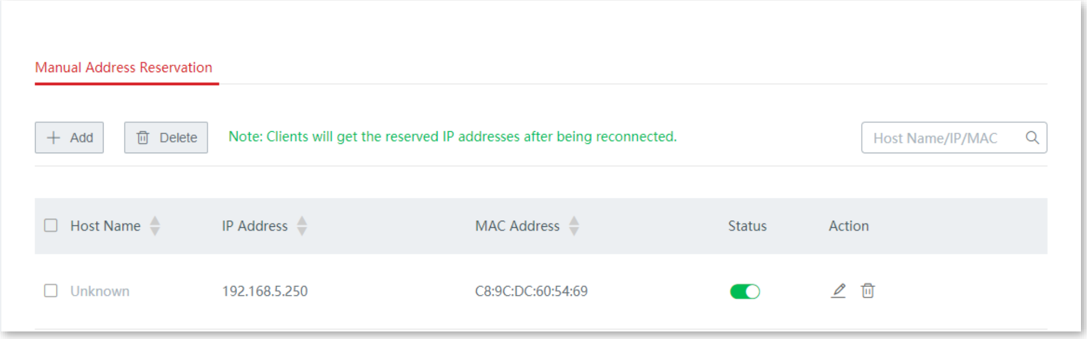
□ Host Name	IP Address	MAC Address	Status	Action

3. Configure parameters in the **Add** window, and click **Save**.
   (1) Set the fixed IP address assigned to the server host, which is **192.168.5.250** in this example.
   (2) Enter the MAC address of the server host, which is **C8:9C:DC:60:54:69** in this example.



IP Address	MAC Address	Remark	Operation
192.168.5.250	C8:9C:DC:60:54:	Optional	+ —

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



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

□ Host Name	IP Address	MAC Address	Status	Action
□ Unknown	192.168.5.250	C8:9C:DC:60:54:69	●	

----End

Verification

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

In this example, assume that the IP address of the WAN1 port is 202.105.11.22, the access address is http://202.105.11.22:9999

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

Tip

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

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

3.10.6 DMZ host

Overview

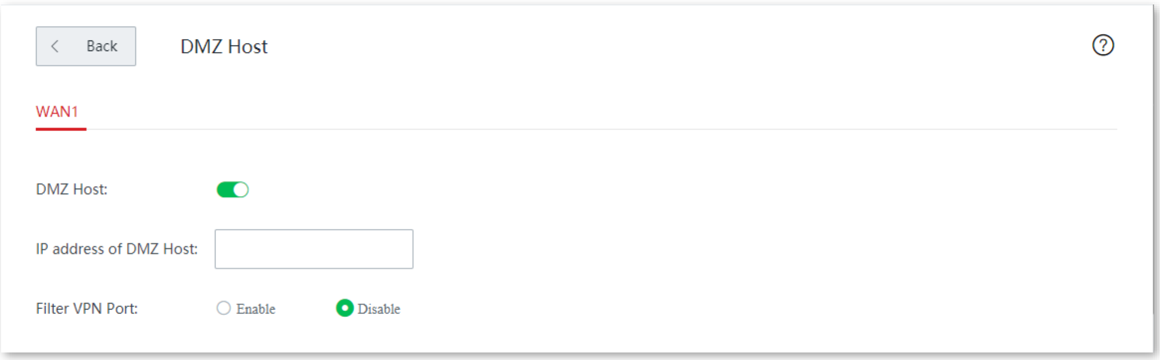
After setting a device in the LAN as the DMZ host, it enjoys no limitations when communicating with the internet. For example, if video meeting or online games are under way on a computer, you can set that computer as the DMZ host to make the video meeting and online games go smoother. In addition, you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

Note

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

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

The DMZ function is disabled by default. The following displays the page when the function is enabled.



DMZ Host: ●

IP address of DMZ Host:

Filter VPN Port: ○ Enable ● Disable

Parameter description

Parameter	Description
DMZ Host	It specifies whether to enable the DMZ host function. ○ indicates the function is disabled and ● indicates the function is enabled.
IP address of DMZ Host	It specifies the IP address of the LAN device to be set as the DMZ host.

Parameter	Description
Filter VPN Port	It specifies whether to enable the filter VPN port function. After this function is enabled and you enabled the DMZ host function at the same time, the VPN service on the cable-free router mode node will respond to the VPN requests from the internet. Note If the node has already enabled the VPN server function and is about to enable the DMZ host function, to ensure the validity of the VPN server on the node, please enable the filter VPN port function as well.

Example of configuring DMZ host

Networking requirement

An enterprise uses a cable-free device to set up a network. The device has connected to the internet and can offer internet service to LAN users. The enterprise has the following requirements:

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

Solution

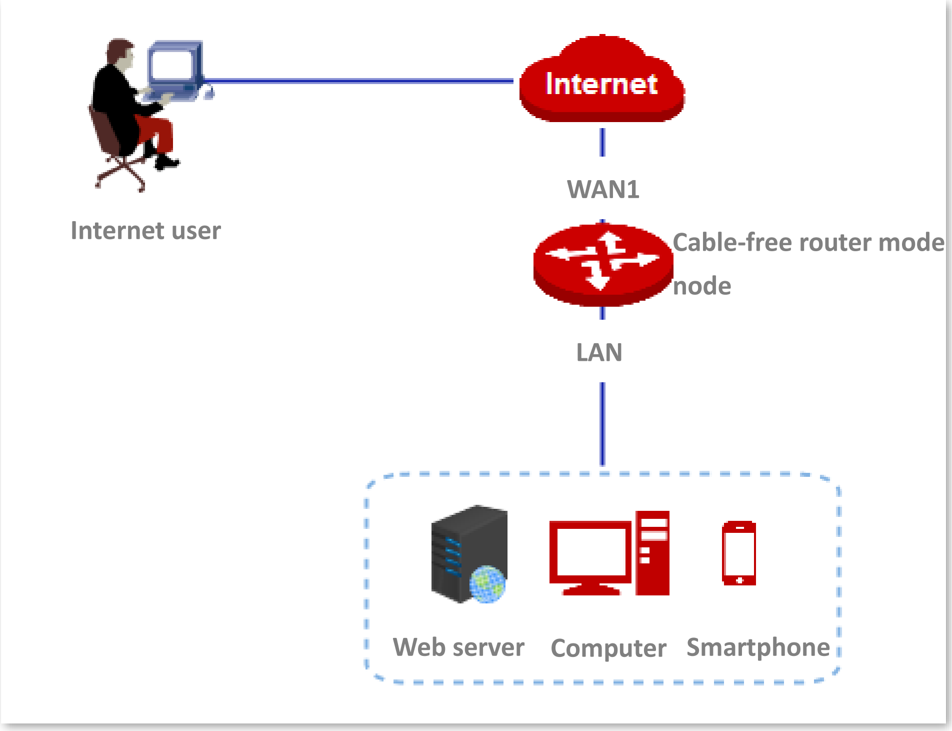
- You can use the **DMZ Host** function to enable internet users to access the intranet web server.
- You can use the **Address Reservation** function to avoid access failure caused by web server address change.

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

- IP address of the web server: 192.168.5.250
- MAC address of the host that runs the web server: C8:9C:DC:60:54:69
- Service port: 9999

Tip

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

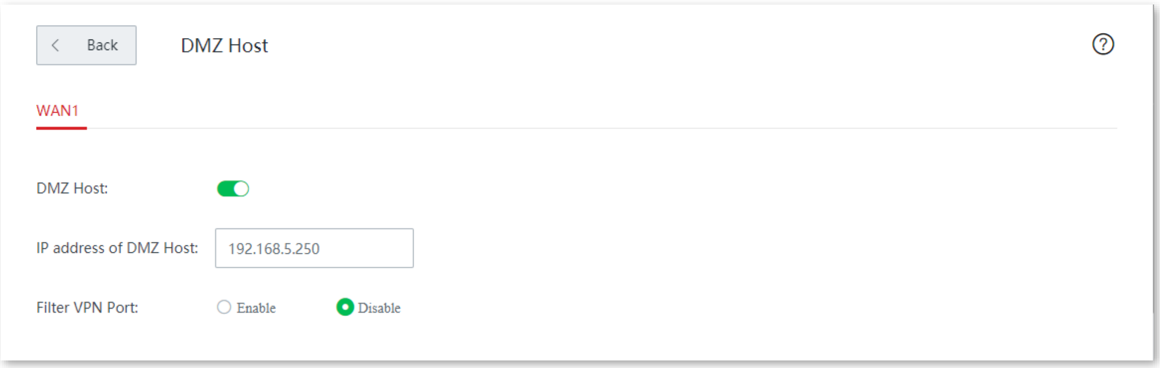


Configuration procedures

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

I. **Set the DMZ host.**

1. Click **More** > **DMZ Host**.
2. Toggle on **DMZ Host**.
3. Enter the IP address of the LAN device to be set as the DMZ host, which is **192.168.5.250** in this example.
4. Click **Save**.



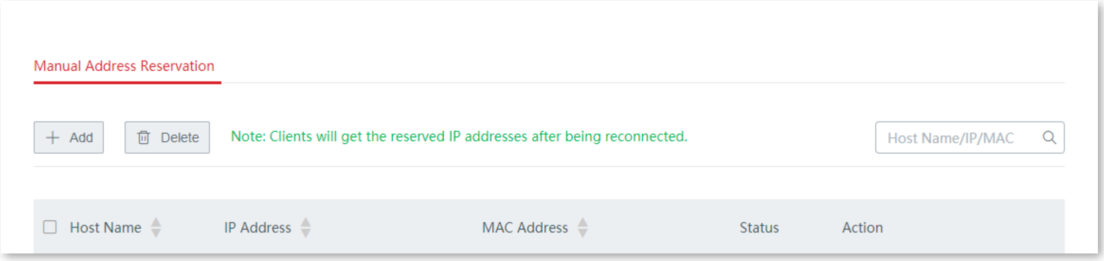
DMZ Host: ●

IP address of DMZ Host: 192.168.5.250

Filter VPN Port: ○ Enable ● Disable

II. Reserve a fixed IP address for the DMZ host.

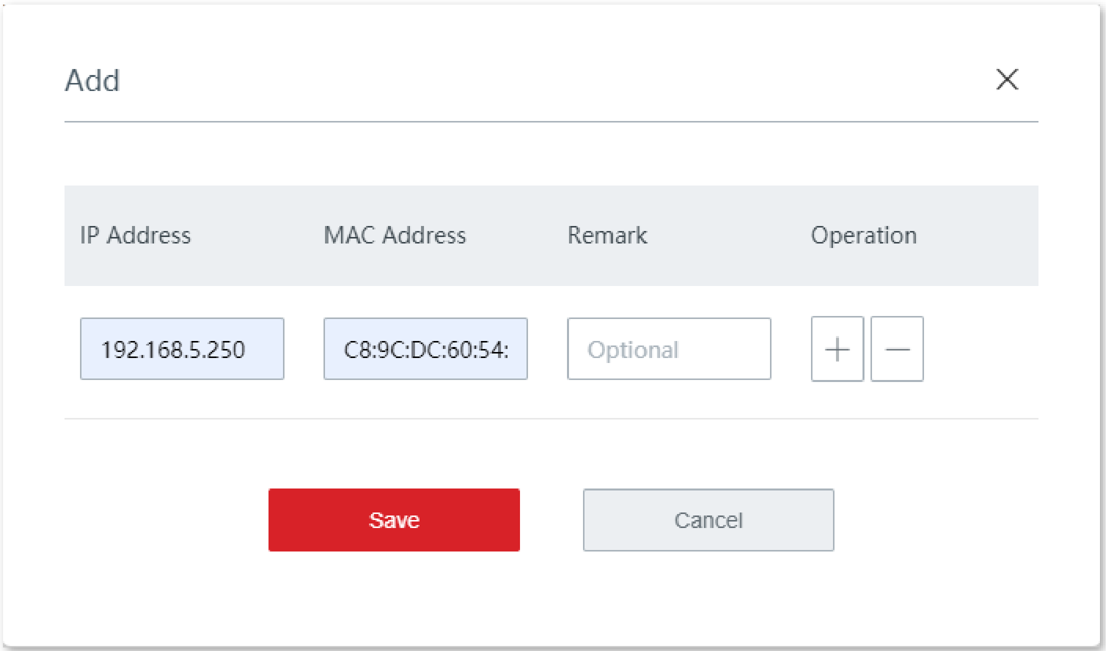
1. Click **Address Reservation** and locate the **Manual Address Reservation** module.
2. Click **+ Add**.



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

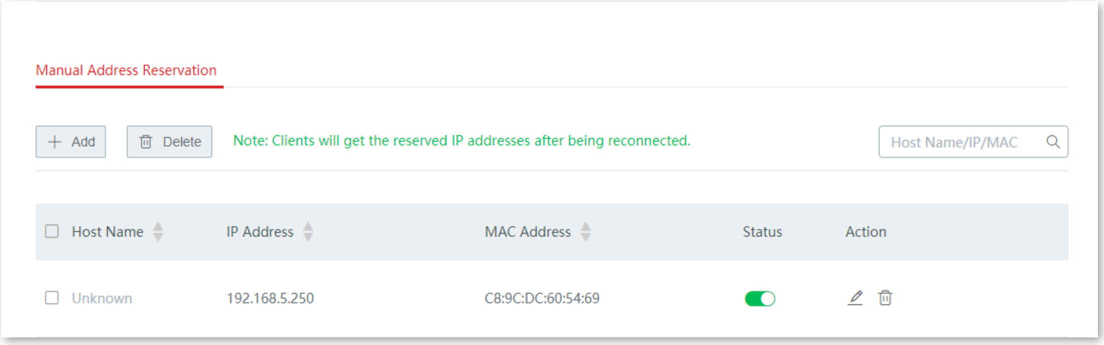
□ Host Name	IP Address	MAC Address	Status	Action

3. Configure parameters in the **Add** window, and click **Save**.
   (1) Set the fixed IP address assigned to the server host, which is **192.168.5.250** in this example.
   (2) Enter the MAC address of the server host, which is **C8:9C:DC:60:54:69** in this example.



IP Address	MAC Address	Remark	Operation
192.168.5.250	C8:9C:DC:60:54:	Optional	+ —

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



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

□ Host Name	IP Address	MAC Address	Status	Action
□ Unknown	192.168.5.250	C8:9C:DC:60:54:69	●	

----End

Verification

Internet users can successfully access the intranet server by using **intranet service application layer protocol name**://**WAN port IP address**:**internal service port**. If you use the default port for the intranet service, the intranet service port number can be excluded from the access address. Under such circumstances, the access address is **intranet service application layer protocol name**://**WAN port IP address**.

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

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

Tip

After the configuration, if internet users still cannot access the LAN server, disable the system firewall, anti-virus software or security guard on the DMZ host and try again.

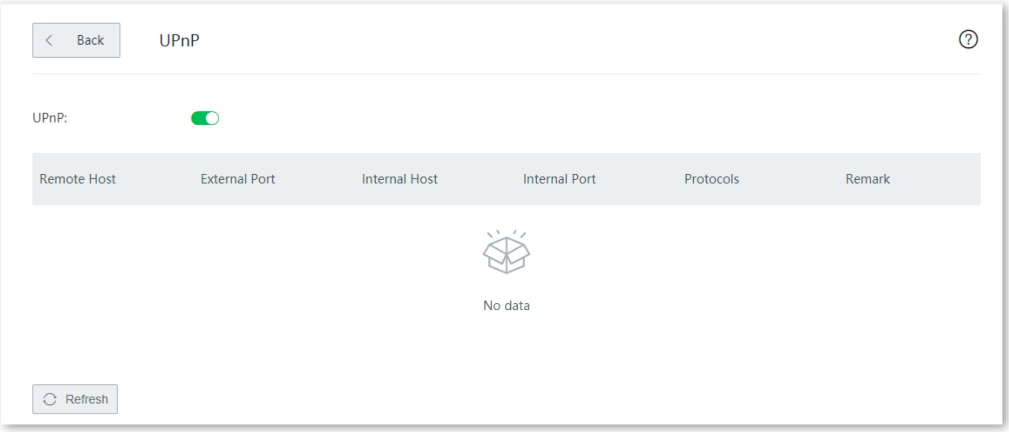
3.10.7 UPnP

Overview

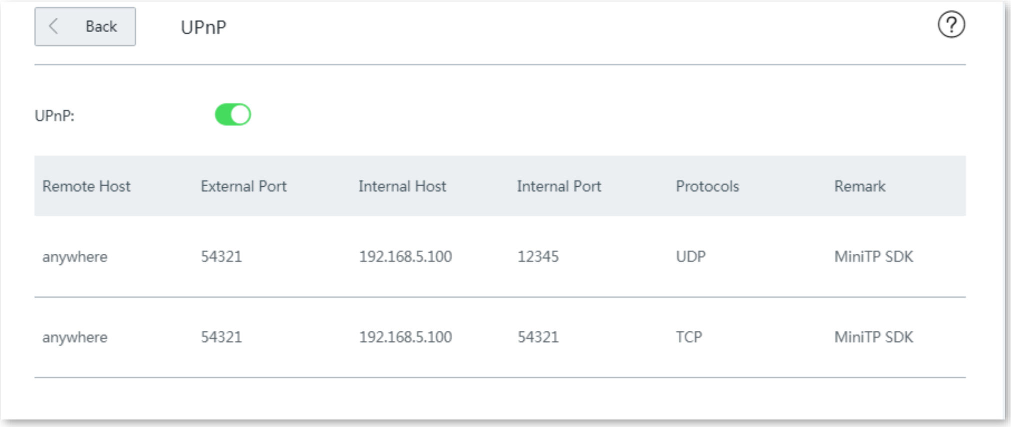
UPnP is abbreviated for Universal Plug and Play. After the UPnP function is enabled, the cable-free router mode node can automatically open port for UPnP-supporting programs in the LAN (such as Xunlei, BitComet, and AnyChat) and make these applications run smoother.

Enable UPnP

On the **More** > **UPnP** page, toggle on **UPnP**.



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



UPnP: ●

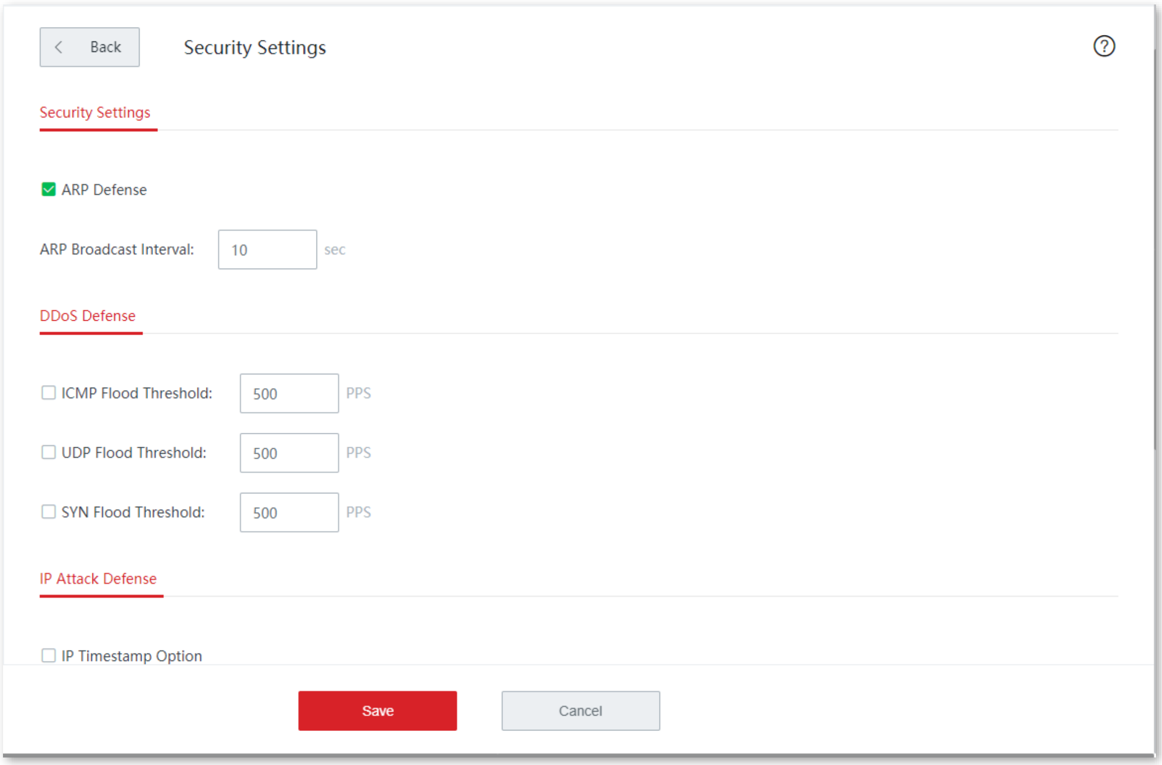
Remote Host	External Port	Internal Host	Internal Port	Protocols	Remark
anywhere	54321	192.168.5.100	12345	UDP	MiniTP SDK
anywhere	54321	192.168.5.100	54321	TCP	MiniTP SDK

3.10.8 Security settings

The cable-free router mode node supports ARP Defense, DDoS Defense, IP Attack Defense, and Block WAN Ping security settings.

- ARP Defense: This function can identify the ARP spoofing in the local network, and record the MAC addresses of the attacker.
- DDoS Defense: DDoS attack, abbreviated for Distributed Denial of Service Attack, makes network resource unavailable to its intended users. The node can block DDoS attack, including ICMP Flood, UDP Flood, and SYN Flood attacks.
- IP Attack Defense: With this function enabled, the node can intercept some packets with specified IP options. These IP options include IP Timestamp Option, IP Security Option, IP Stream Option, IP Record Route Option, IP Loose Source Route Option and illegal IP options.
- Block WAN Ping: With this function enabled, the node automatically ignores WAN IP address ping requests from internet hosts; therefore, the node avoids exposing itself and defends the external ping attacks.

Click **More** > **Security Settings** to enter the page. See the following figure.



Security Settings

Security Settings

☑ ARP Defense

ARP Broadcast Interval: 10 sec

DDoS Defense

□ ICMP Flood Threshold: 500 PPS

□ UDP Flood Threshold: 500 PPS

□ SYN Flood Threshold: 500 PPS

IP Attack Defense

□ IP Timestamp Option

Parameter description

Parameter		Description
Security Settings	ARP Defense	It specifies whether to enable the ARP defense function.
	ARP Broadcast Interval	It specifies the interval at which the node sends ARP broadcast messages.
DDoS Defense	ICMP Flood Threshold	If ICMP request packets from a same host in LAN received by the node exceed this threshold within 1 second, the node suffers ICMP flood attack.
	UDP Flood Threshold	If UDP request packets from a same host in LAN received by the node exceed this threshold within 1 second, the node suffers UDP flood attack.
	SYN Flood Threshold	If TCP SYN request packets from a same host in LAN received by the node exceed this 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.

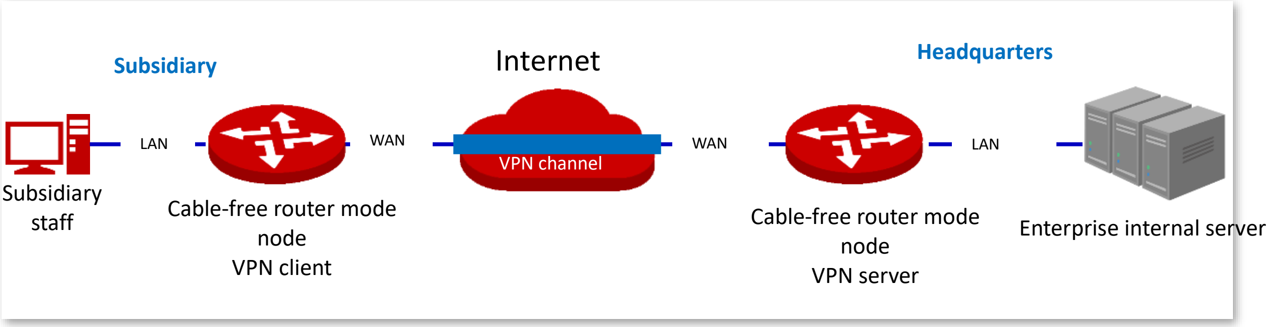
Parameter		Description
	IP Record Route Option	With this function enabled, the node blocks IP packets that contain the Record Route option in the local network.
	IP Loose Source Route Option	With this function enabled, the node blocks IP packets that contain the Loose Source Route option in the local 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, this function is disabled. After the block WAN ping function is enabled, the node automatically ignores WAN IP address ping requests from internet hosts; therefore, the node avoids exposing itself and defends external ping attacks.

3.10.9 VPN server

Overview

VPN, abbreviated for Virtual Private Network, is a special network set up on the public network (generally the internet). It exists only logically, and does not have any physical lines. The VPN technology is widely used in enterprise networks and is used to achieve resource sharing between a subsidiary and the headquarters, and at the same time, protects these resources from being exposed to other users in the internet.

The typical network topology is shown as below.



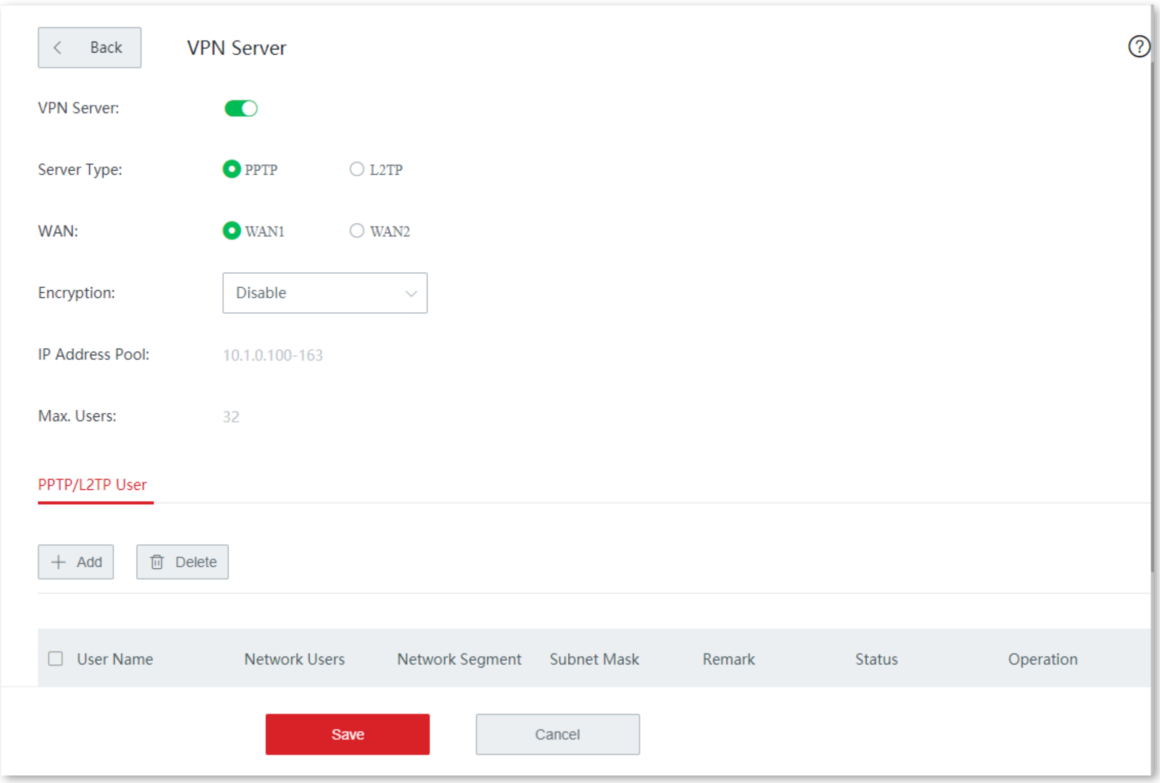
The cable-free router mode node can be used as a PPTP/L2TP server to accept connections from PPTP/L2TP clients.

Configure VPN server

Click **More** > **VPN Server** to enter the page.

Enable the VPN server

The VPN server is disabled by default. The following displays the page when the function is enabled.



< Back VPN Server

VPN Server: ●

Server Type: ● PPTP ○ L2TP

WAN: ● WAN1 ○ WAN2

Encryption: Disable

IP Address Pool: 10.1.0.100-163

Max. Users: 32

PPTP/L2TP User

+ Add Delete

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

Save Cancel

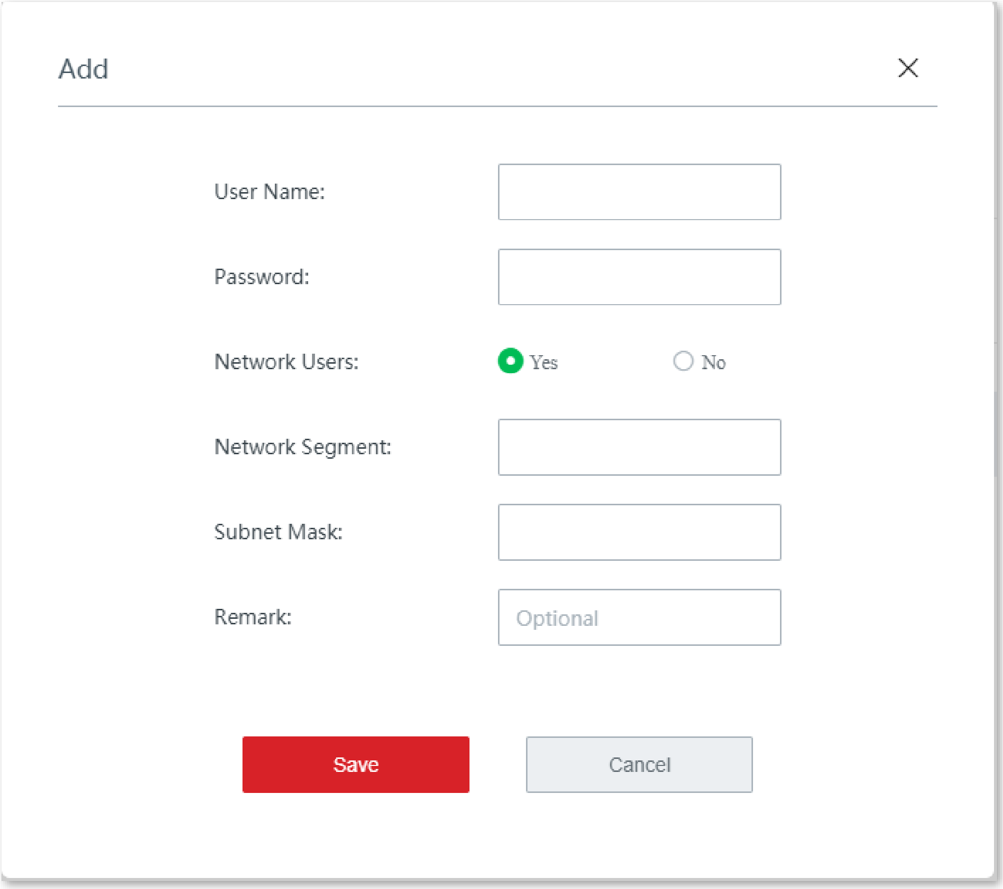
Parameter description

Parameter	Description
VPN Server	It specifies whether to enable the VPN server function. ○ indicates the function is disabled and ● indicates the function is enabled. After this function is enabled, the node serves as a VPN server.
Server Type	It specifies the VPN protocol type the node uses, including PPTP and L2TP. Both PPTP and L2TP are layer-2 VPN channel protocol and use the PPP to encapsulate data, and both add an additional head for data. – **PPTP:** The node serves as a PPTP server and accepts connections from PPTP clients. – **L2TP:** The node serves as an L2TP server and accepts connections from L2TP clients.
WAN	It specifies the WAN port for setting up a VPN channel between the VPN server and the clients. The IP address or domain name of the WAN port is the server IP address/domain name of VPN client.

Parameter	Description
Encryption	It specifies whether to enable 128-bit data encryption. This parameter only appears when PPTP is selected. The encryption configuration of the client and server must be the same. Otherwise, the communication cannot be performed properly.
IPSec Encryption	It specifies whether to enable the IPSec encryption. This parameter only appears when L2TP is selected. If you want to configure IPSec encryption, select the IPSec rules whose encapsulation mode is transport mode.
IP Address Pool	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 connect to the PPTP/L2TP server. The value is fixed to **32**.

Add PPTP/L2TP user account

On the **More** > **VPN Server** page, locate the **PPTP/L2TP User** module, click **+ Add**, configure parameters in the pop-up window, and click **Save**.



Add

User Name:

Password:

Network Users: ● Yes ○ No

Network Segment:

Subnet Mask:

Remark: Optional

Parameter description

Parameter	Description
User Name	It specifies the VPN user name and password, which is the user name/password VPN users need to enter when performing PPTP/L2TP dial-ups (VPN connection).
Password	
Network Users	It specifies the type of the VPN client. – Yes: Choose this option when the VPN client is a network. Under such circumstances, you need to set the network segment, subnet mask of the VPN client. – No: Choose this option when the VPN client is a host.
Network Segment	When the VPN client is a network, enter the private network prefix of the client.
Subnet Mask	When the VPN client is a network, enter the subnet mask of the client.
Remark	It specifies the remarks of the account.

Example of configuring PPTP/L2TP VPN service

Networking requirement

An enterprise and its subsidiary both use cable-free devices to set up network and the cable-free devices have connected to the internet. The enterprise has the following requirements:

Subsidiary staff can access the LAN resources through the internet, such as documents, OA, ERP system, CRM system, project management system and other resources.

Solution

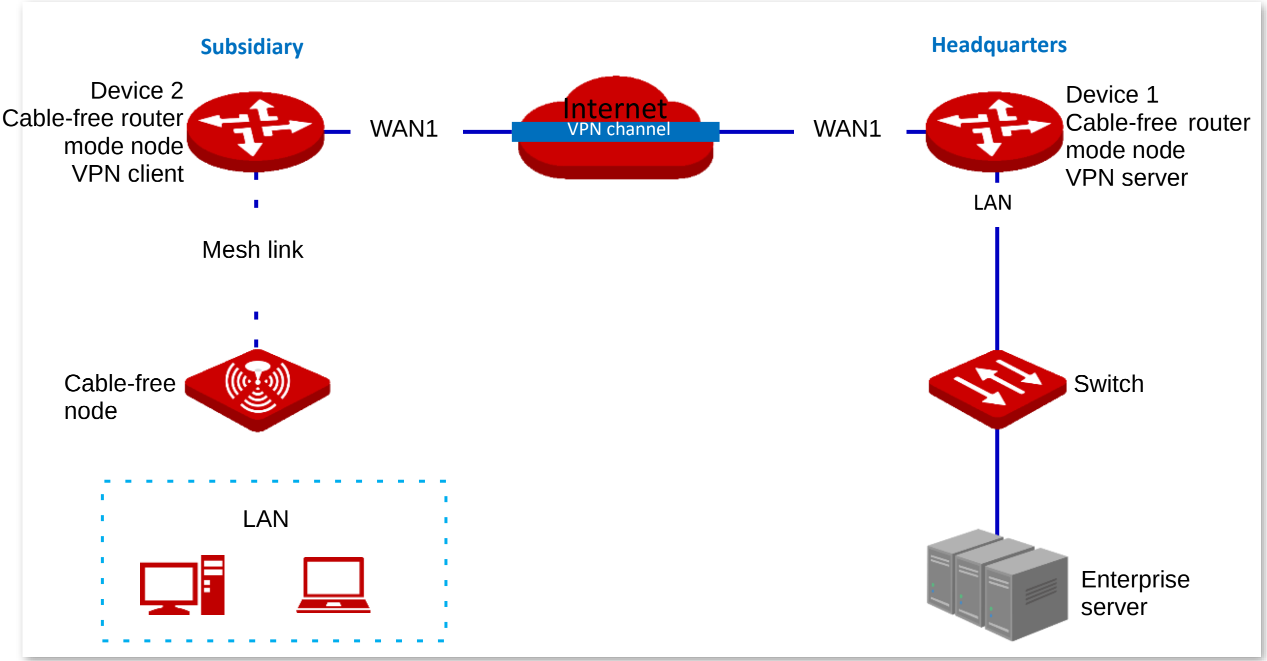
Set a cable-free device as the VPN server and the other as the VPN client to enable remote users to securely access the LAN through the internet. PPTP VPN is taken as an example here and configurations for L2TP VPN are the same.

Assume that device 1 is set as the PPTP server and its basic information is as follows:

- User name and password assigned by the PPTP server: subsidiary 1
- IP address of the PPTP server: 202.105.11.22
- Data encryption is enabled on the PPTP server.
- Intranet of the PPTP server: 192.168.5.0/24

Assume that device 2 is set as the PPTP client and its basic information is as follows:

Network prefix of the PPTP client: 192.168.1.0/24

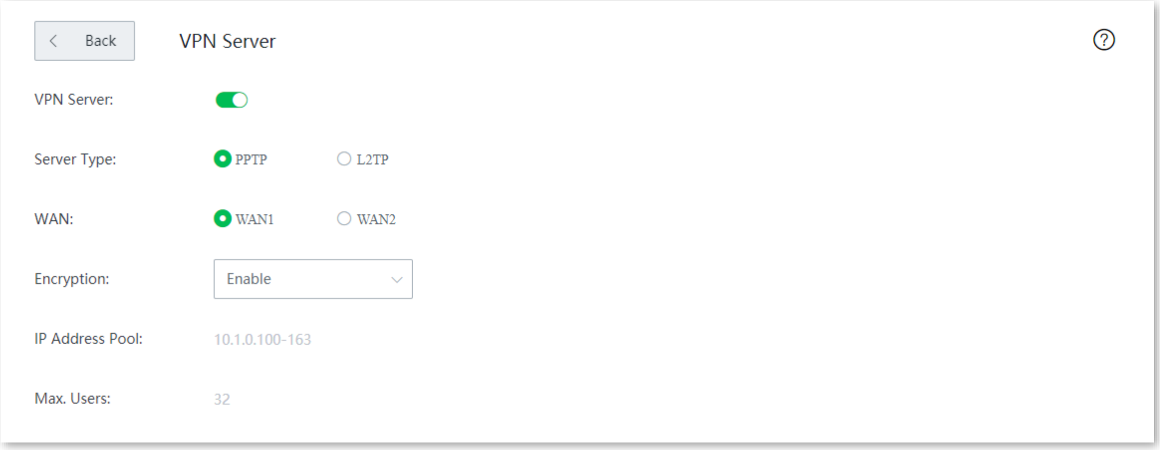


Configuration procedures

Set device 1 as the VPN server → Set device 2 as the VPN client

I. Set device 1 as the VPN server.

1. Log in to the web UI of device 1.
2. Enable the PPTP server.
   (1) Click **More** > **VPN Server**.
   (2) Toggle on **VPN Server**.
   (3) Perform the following configurations, and click **Save**.
      – Choose **Server Type**, which is **PPTP** in this example.
      – Select **Enable** for **Encryption**.



VPN Server: on

Server Type: ● PPTP ○ L2TP

WAN: ● WAN1 ○ WAN2

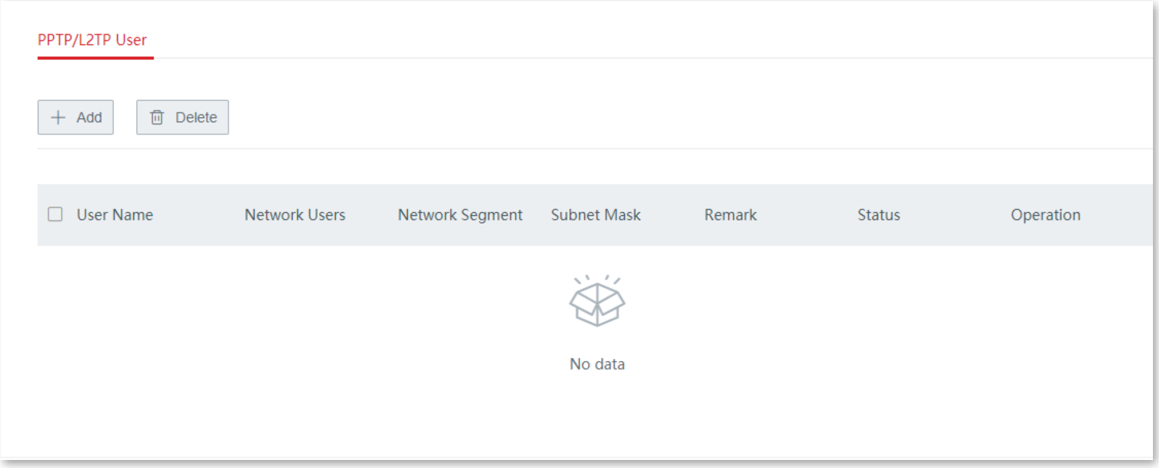
Encryption: Enable

IP Address Pool: 10.1.0.100-163

Max. Users: 32

3. Configure PPTP/L2TP user.

   (1) On the **More** > **VPN Server** page, locate the **PPTP/L2TP User** module, and click **+ Add**.

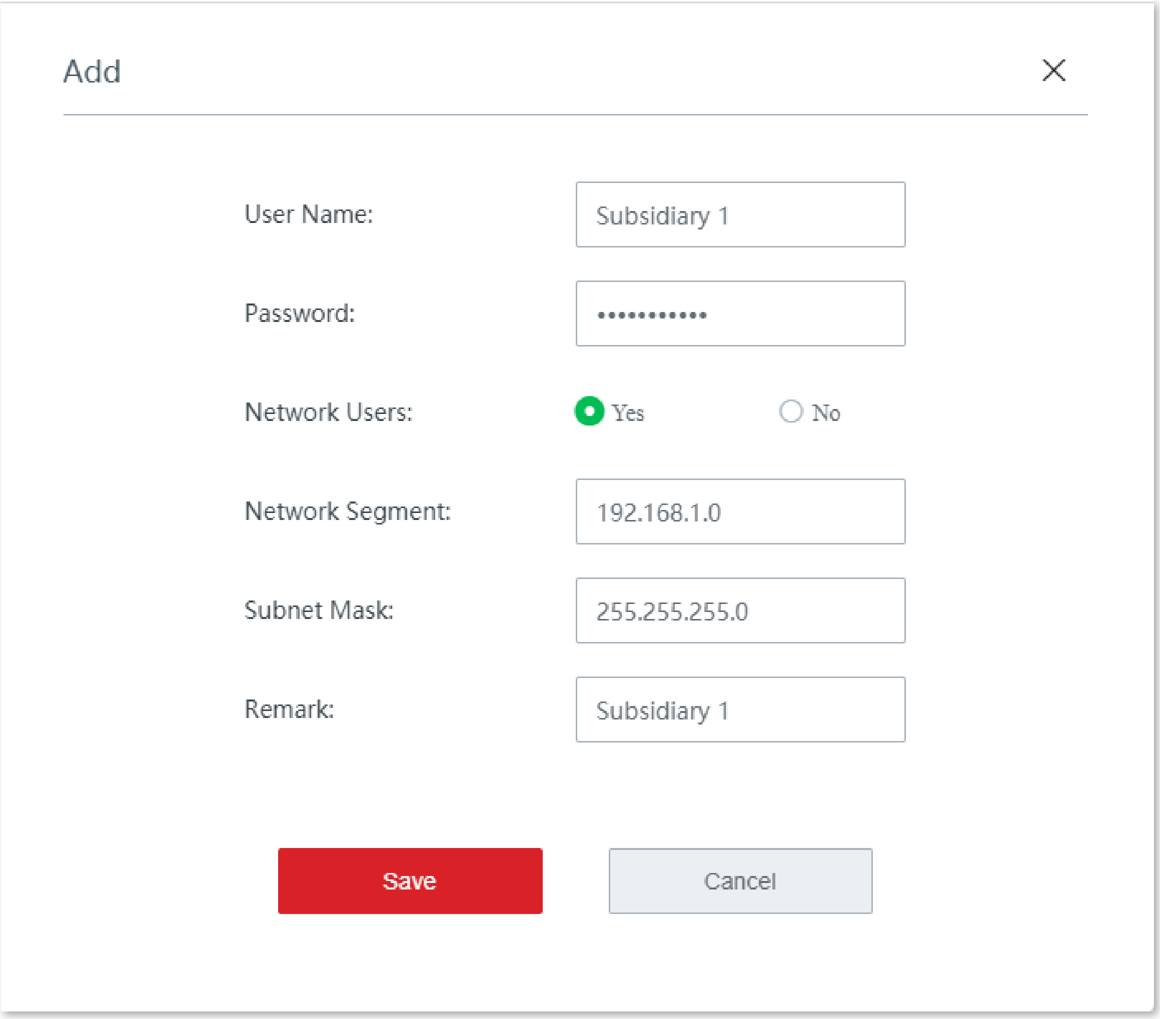


□ User Name	Network Users	Network Segment	Subnet Mask	Remark	Status	Operation

No data

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

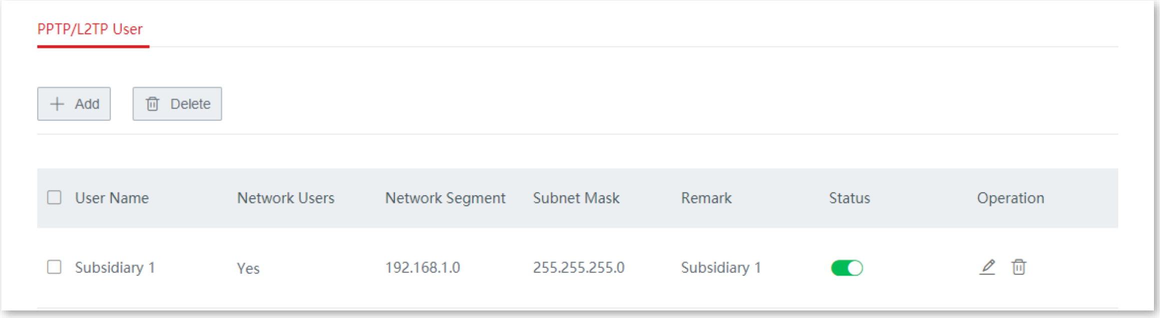
   - Enter the user name the VPN client uses for VPN connection, which is **Subsidiary 1** in this example.
   - Enter the password, which is **Subsidiary1** in this example.
   - Choose **Yes** for **Network Users**.
   - Enter the network segment of the VPN client LAN, which is **192.168.1.0** in this example.
   - Enter the subnet mask, which is **255.255.255.0** in this example.
   - Enter the remark for the user account, which is **Subsidiary 1** in this example.



Add

User Name:	Subsidiary 1
Password:	•••••••••••
Network Users:	● Yes ○ No
Network Segment:	192.168.1.0
Subnet Mask:	255.255.255.0
Remark:	Subsidiary 1

The PPTP/L2TP user is added successfully. See the following figure.



□ User Name	Network Users	Network Segment	Subnet Mask	Remark	Status	Operation
□ Subsidiary 1	Yes	192.168.1.0	255.255.255.0	Subsidiary 1	●	✎ 🗑

II. Set device 2 as the VPN client.

1. Log in to the web UI of device 2 and click **More** > **VPN Client**.
2. Toggle on **VPN Client**.
3. Perform the following configurations, and click **Save**.
   (1) Choose the **Client Type**, which is **PPTP** in this example.

(2) Enter the IP address/domain name of the WAN port which serves as the egress at the VPN server side, which is **202.105.11.22** in this example.

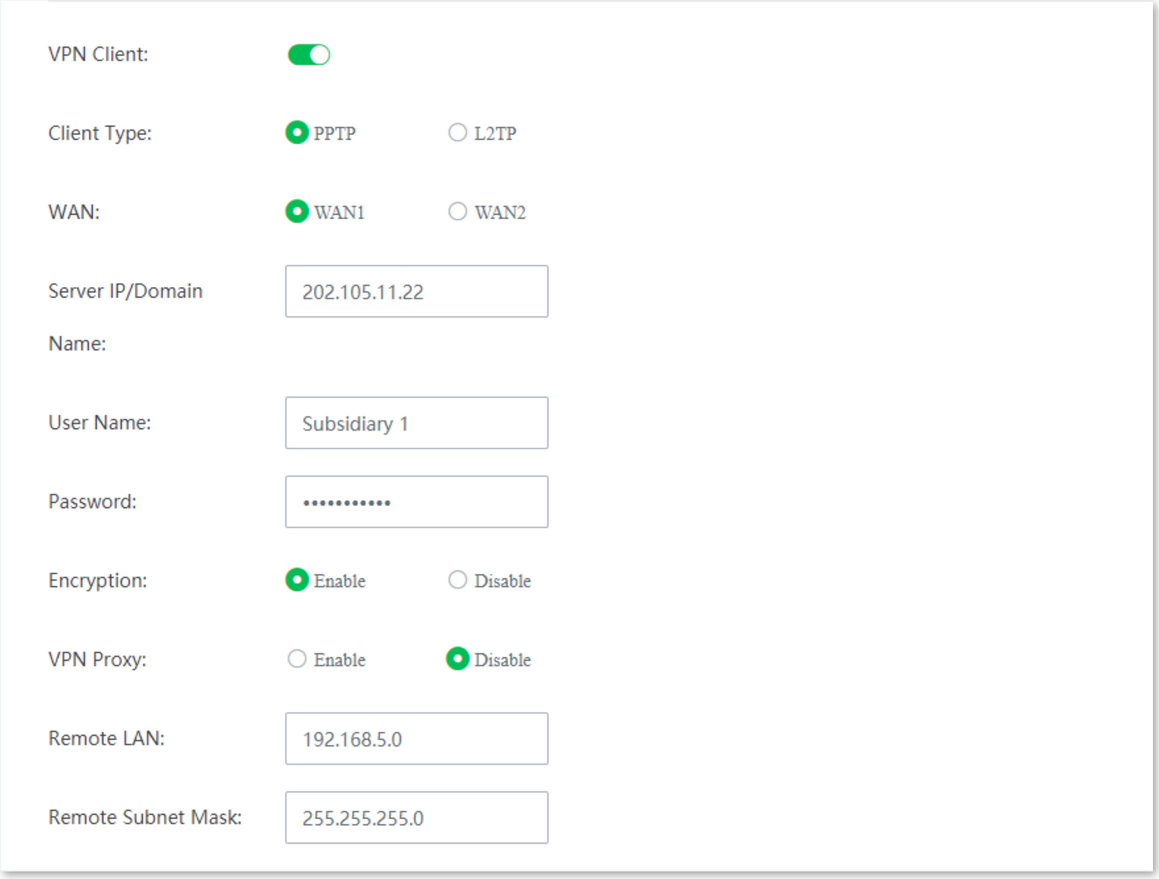
(3) Enter the user name assigned by the VPN server, which is **Subsidiary 1** in this example.

(4) Enter the password, which is **Subsidiary1** in this example.

(5) Choose **Enable** for **Encryption**.

(6) Enter the **Remote LAN**, which is **192.168.5.0** in this example.

(7) Enter the **Remote Subnet Mask**, which is **255.255.255.0** in this example.



VPN Client: ●

Client Type: ● PPTP ○ L2TP

WAN: ● WAN1 ○ WAN2

Server IP/Domain Name: 202.105.11.22

User Name: Subsidiary 1

Password: •••••••••••

Encryption: ● Enable ○ Disable

VPN Proxy: ○ Enable ● Disable

Remote LAN: 192.168.5.0

Remote Subnet Mask: 255.255.255.0

When **Connected** is displayed on **Status**, the VPN connection is successful.

----End

Staff of the headquarters and the subsidiary can securely access the LAN resources through the internet.

Verification

Assume that the subsidiary is about to access the FTP server of the headquarters. The headquarters project data is stored on an FTP server and the server information is as follows:

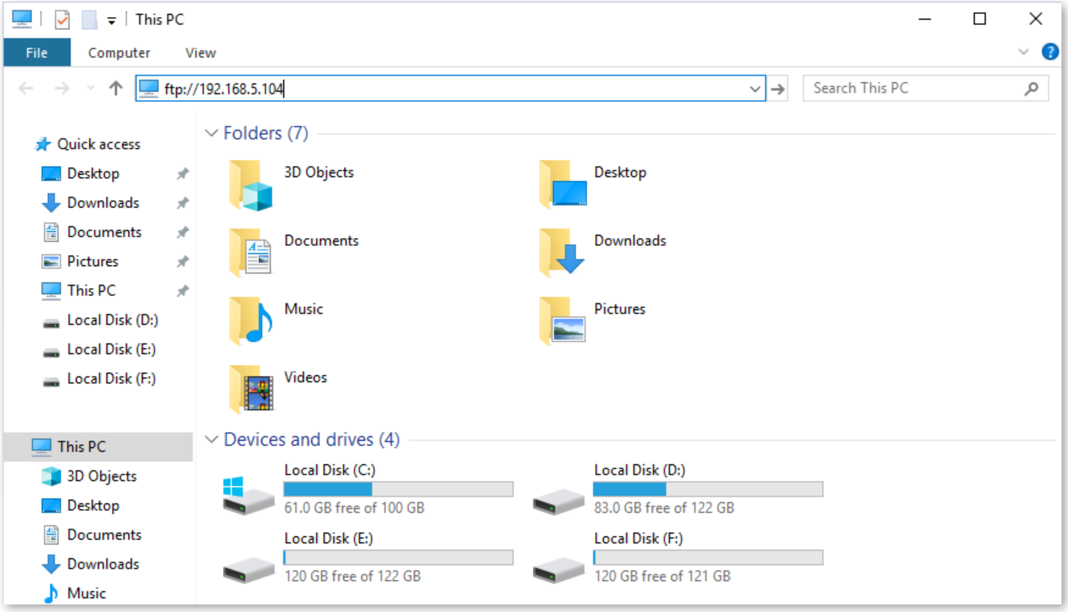
- FTP server IP address: 192.168.5.104
- Server port: 21
- Login username/password: Tom123/Tom123

When subsidiary staff accesses the headquarters project materials, perform the following procedures:

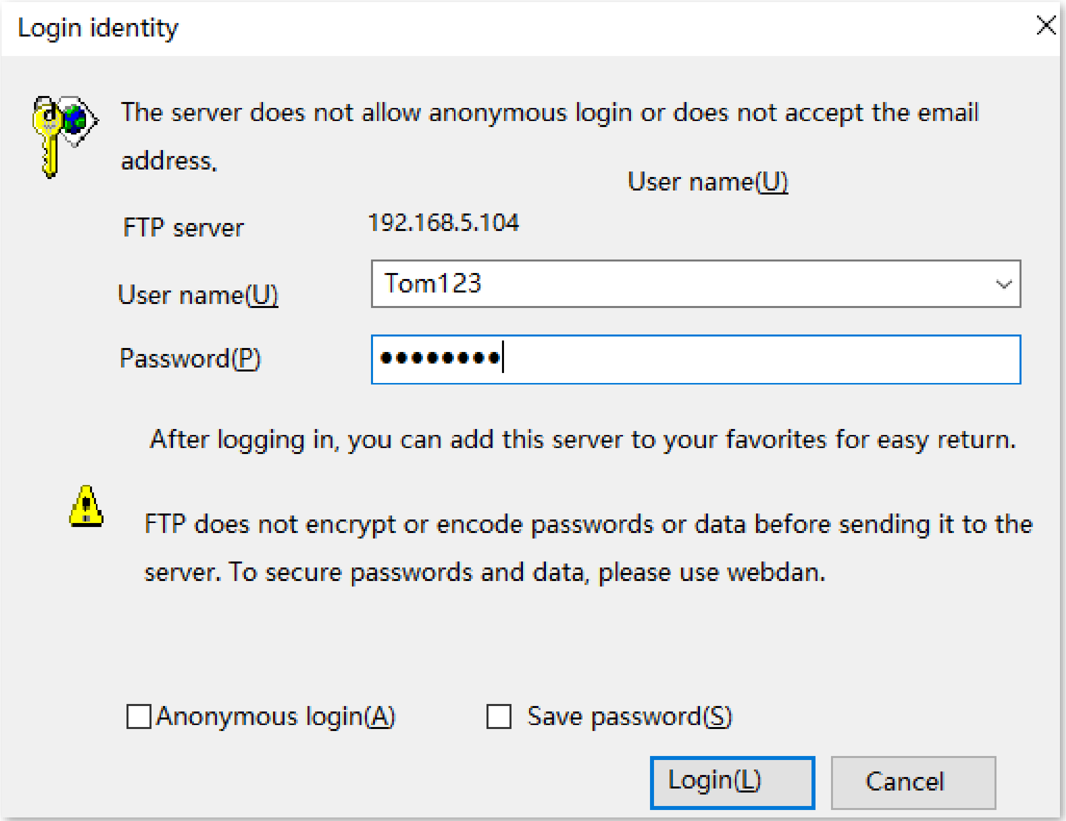
1. Enter **ftp://server IP address** in a browser or **This PC**, which is **ftp://192.168.5.104** in this example.

Tip

If the LAN service port is not the default port number, the access format is **LAN service application layer protocol name://server IP address:LAN service port**.



2. Enter the user name and password, which are both **Tom123** in this example, and click **Login**.



Login identity

The server does not allow anonymous login or does not accept the email address.

User name(U)

FTP server 192.168.5.104

User name(U) Tom123

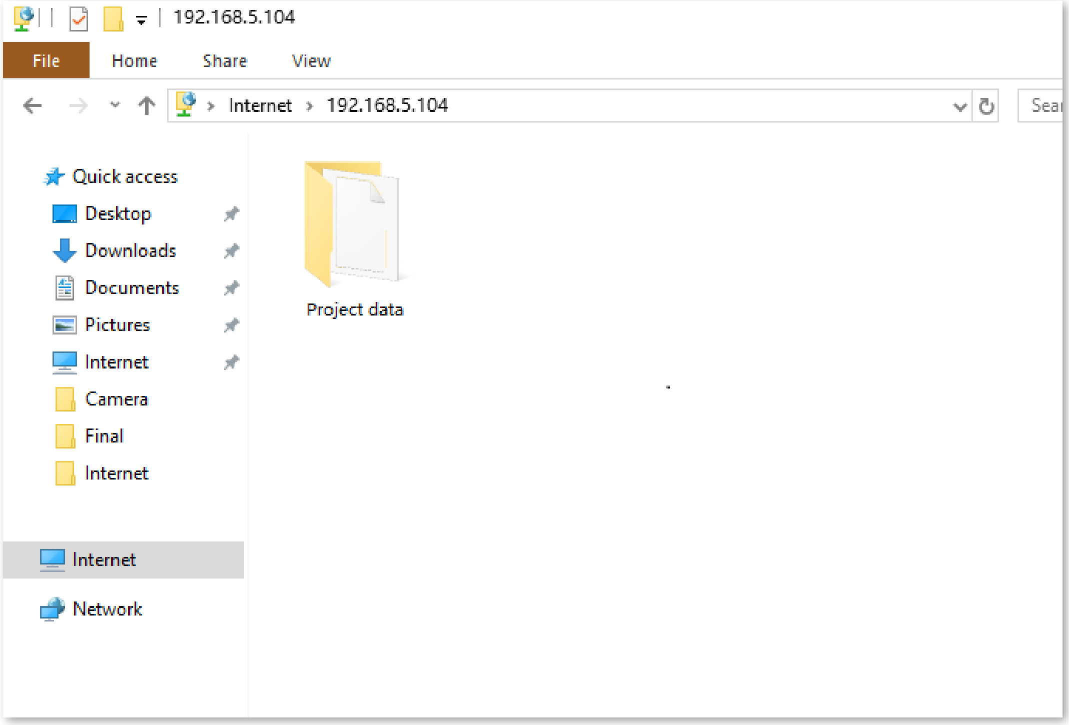
Password(P) ●●●●●●●●

After logging in, you can add this server to your favorites for easy return.

FTP does not encrypt or encode passwords or data before sending it to the server. To secure passwords and data, please use webdan.

□Anonymous login(A) □ Save password(S)

The access is successful. See the following figure.

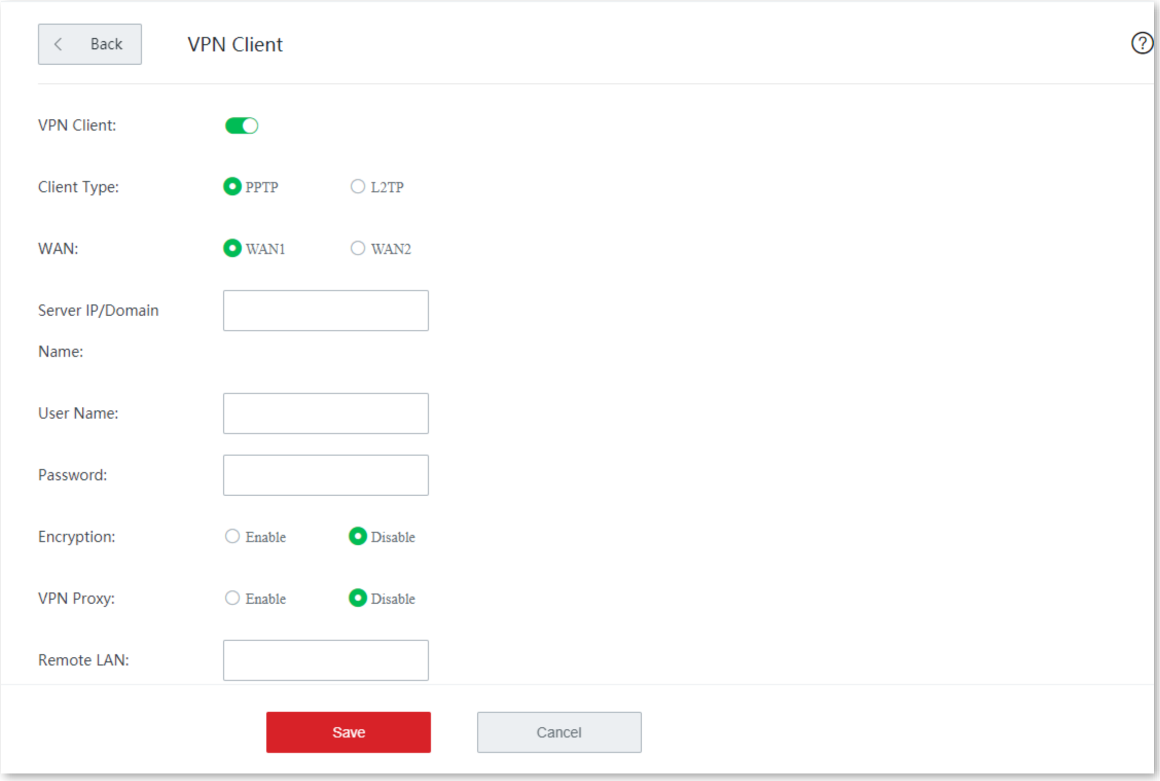


3.10.10 VPN client

Cable-free router mode node can be used as a PPTP/L2TP client connected to the PPTP/L2TP server.

Click **More** > **VPN Client** to enter the page.

The VPN client function is disabled by default. The following displays the page when the function is enabled.



VPN Client: ●

Client Type: ● PPTP ○ L2TP

WAN: ● WAN1 ○ WAN2

Server IP/Domain Name:

User Name:

Password:

Encryption: ○ Enable ● Disable

VPN Proxy: ○ Enable ● Disable

Remote LAN:

Parameter description

Parameter	Description
VPN Client	It specifies whether to enable the VPN client function. ○ indicates the function is disabled and ● indicates the function is enabled. After this function is enabled, the node serves as a VPN client.
Client Type	It specifies the VPN protocol type the node uses, including PPTP and L2TP. Both PPTP and L2TP are layer-2 VPN channel protocol and use the PPP to encapsulate data, and both add an additional head for data. – **PPTP:** Choose this option if the VPN server to be connected is a PPTP server. – **L2TP:** Choose this option if the VPN server to be connected is an L2TP server.

Parameter	Description
WAN	It specifies the WAN port the node uses for VPN dial-up.
Server IP/Domain Name	It specifies the IP address or domain name of the VPN server to be connected, which is generally the IP address or domain name of the WAN port enabling the PPTP/L2TP server function of the peer VPN router.
User Name	It specifies the PPTP/L2TP user account, which is the user name and password assigned by the VPN server.
Password	
Encryption	It specifies whether to enable data encryption. This parameter only appears when PPTP is selected. The encryption configuration of the client and server must be the same. Otherwise, the communication cannot be performed properly.
VPN Proxy	After this function is enabled, LAN users access the internet through the VPN server-side router.
Remote LAN	It specifies the network segment of the LAN of the VPN server.
Remote Subnet Mask	It specifies the subnet mask of the LAN of the VPN server.
Status	It specifies the current connection status of the VPN.

3.10.11 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 subsidiary employees to remotely share resources and access your headquarters 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 data transmitted by IPSec. IPSec supports **Tunnel** and **Transport** modes.

  - **Tunnel**: This mode adds an additional IP head and is most commonly used between gateways. The whole IP data packet of the user is used to calculate the AH or ESP head. AH or ESP head and the user data encrypted by ESP are encapsulated in a new IP data packet.

- **Transport**: This mode does not change the original IP head and is most commonly used between hosts. Only the data at the transmission layer is used to calculate AH or ESP head. AH or ESP head or user data encrypted by ESP are placed behind the original IP packet head.

− **Security gateway**

It refers to a gateway (secure and encrypted router) with the IPSec functionality. IPSec is used to protect data exchanged between such gateways from being tampered and peeped.

− **IPSec peer**

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

− **SA**

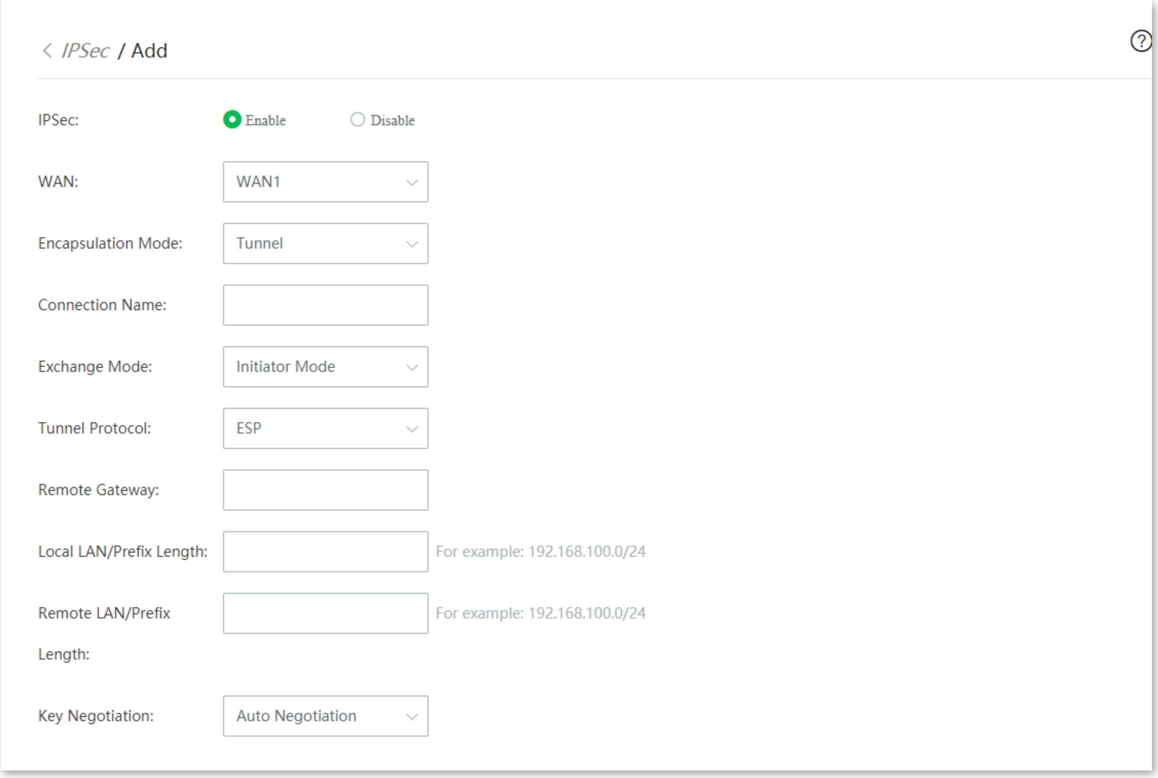
SA specifies some elements of the peers, such as the base protocol (AH, ESP, or both), encapsulation mode (transport or tunnel), encryption algorithm (DES, 3DES, or AES), shared key for data protection in specified flows, and life cycle of the key. SA has the following features:

- A triplet {SPI, Destination IP address, Security protocol identifier} is used as a unique ID.
- An SA specifies the protocol, algorithm, and key for processing packets.
- Each IPsec SA is unidirectional with a life cycle.
- An SA can be created manually or generated automatically using internet Key Exchange (IKE). The IKE protocol has two versions of IKEv1 and IKEv2. The device supports IKEv1 and the IKE hereinafter stands for IKEv1.

Configure IPSec connection

Add an IPSec connection

On the **More** > **IPSec** page, click **+ Add**, configure parameters in the pop-up window, and click **Save**.



< *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

Parameter description

Parameter	Description
IPSec	It specifies whether to enable the IPSec function.
WAN	It specifies the WAN port over which the IPSec function takes effect. The remote gateway address of the IPSec peer device should be the IP address or domain name of this interface.
Encapsulation Mode	It specifies the IPSec data encapsulation mode. – **Tunnel**: This mode is generally used between two security gateways. – **Transport:** This mode is generally used between hosts or host and gateway.
Connection Name	It specifies the name of the IPSec connection.
Exchange Mode	It specifies the exchange mode of the IPSec tunnel. – **Initiator Mode**: The device sends a connection request to the peer device. – **Responder Mode**: The device waits for the peer device to send a connection request. Note Do not set both ends of the IPSec tunnel as **Responder Mode**; otherwise, the IPSec tunnel setup fails.

Parameter	Description
Tunnel Protocol	It specifies the protocol which offers the security service for IPSec. – **AH**: It is abbreviated for Authentication Header. This protocol is used for verifying data integrity. If a packet is tampered during transmission, the receiver discards it during data integrity verification. – **ESP**: It is abbreviated for Encapsulating Security Payload. This protocol is used for verifying data integrity and encrypting data. If a packet processed using this protocol is intercepted during transmission, it is difficult for the intercepting party to obtain the real information contained in the packet. This compatible protocol is widely used in gateway products. – **AH+ESP**: It indicates that the function features both AH and ESP.
Remote Gateway	It specifies the IP address or domain name of the peer gateway of the IPSec tunnel.
Local LAN/Prefix Length	It specifies the network segment/prefix length of the LAN of the device. For example, if the IP address of the LAN port of the device is 192.168.5.1 and the subnet mask is 255.255.255.0, the local LAN/prefix length can be 192.168.5.0/24.
Remote LAN/Prefix Length	It specifies the network segment/prefix length of the LAN of the peer gateway of the IPSec tunnel. If the peer device is a host, this parameter can be set as "the IP address of the device/32".
Key Negotiation	It specifies the key negotiation mode of the IPSec security tunnel. By default, **Auto Negotiation** is selected. – **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 mode--Auto negotiation**

To ensure the information privacy, both IPSec communicating parties use the information known to both for encryption and decryption. Therefore, at the beginning of the communication, both parties need to negotiate a security key and the key is generated by IKE. 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) offers an architecture for key exchange and SA negotiation.

- Oakley: It describes the detailed mechanism of key exchange.
- SKEME: It describes another key exchange mechanism different from Oakley.

IKE negotiation can be divided into phase I and phase II.

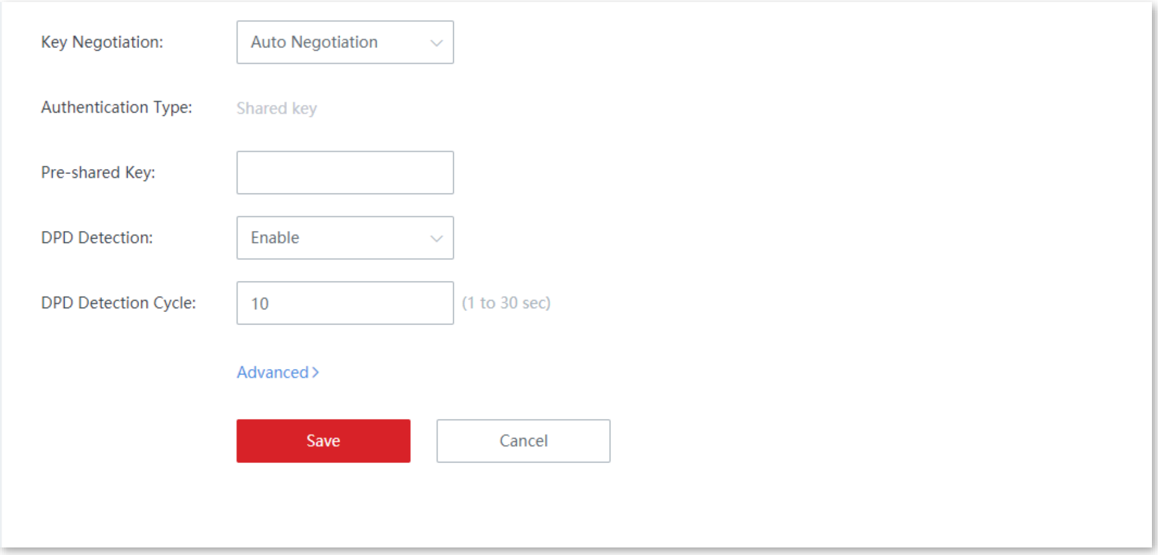
During IKE Phase I:

The communicating parties negotiate exchange and authentication algorithm, encryption algorithm and other security protocols, and generate an ISAKMP SA which is used to exchange more information in phase II.

During IKE phase II:

The ISAKMP SA set up in phase I is used as the security agreement negotiation parameter of IPSec to create IPSec SA, which is used to protect the communication data of both parties.

The following displays the page when **Auto Negotiation** is selected for **Key Negotiation**.



Key Negotiation: Auto Negotiation

Authentication Type: Shared key

Pre-shared Key:

DPD Detection: Enable

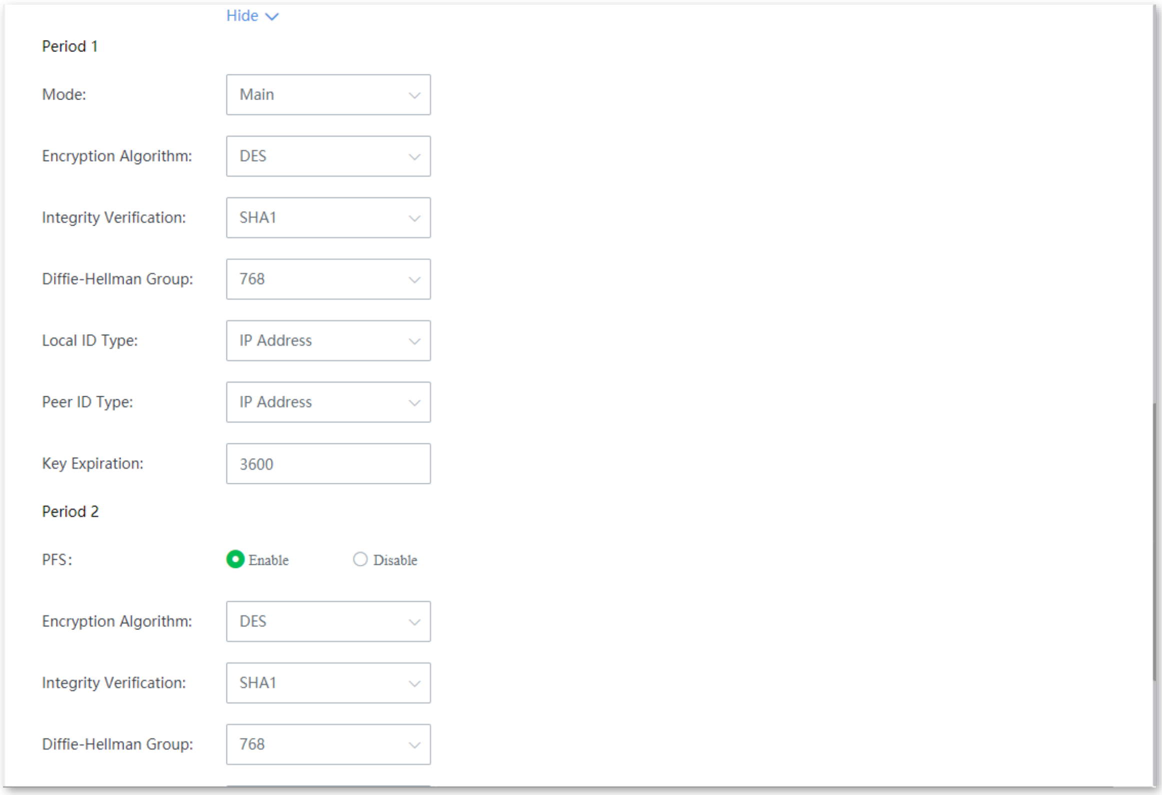
DPD Detection Cycle: 10 (1 to 30 sec)

Parameter description

Parameter	Description
Authentication Type	It specifies the shared key mode, which indicates a shared key string negotiated by IPSec parties with some way in advance.
Pre-shared Key	It specifies the pre-shared key used during negotiation. This parameter must be the same with that of the peer gateway. A maximum of 128 characters are allowed.
DPD Detection	It specifies whether to enable the DPD Detection. This function can detect whether the remote tunnel site is valid.

Parameter	Description
DPD Detection Cycle	It specifies the cycle of transmitting DPD packets. The device transmits DPD packets based on the cycle set here. If the DPD packets are not confirmed by the remote peer device during the cycle period, the device re-initializes the IPSec SA between the both sides.

Click **Advanced** to display the advanced parameters of auto negotiation. The following displays the page when the advanced parameters are displayed.



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

Parameter description

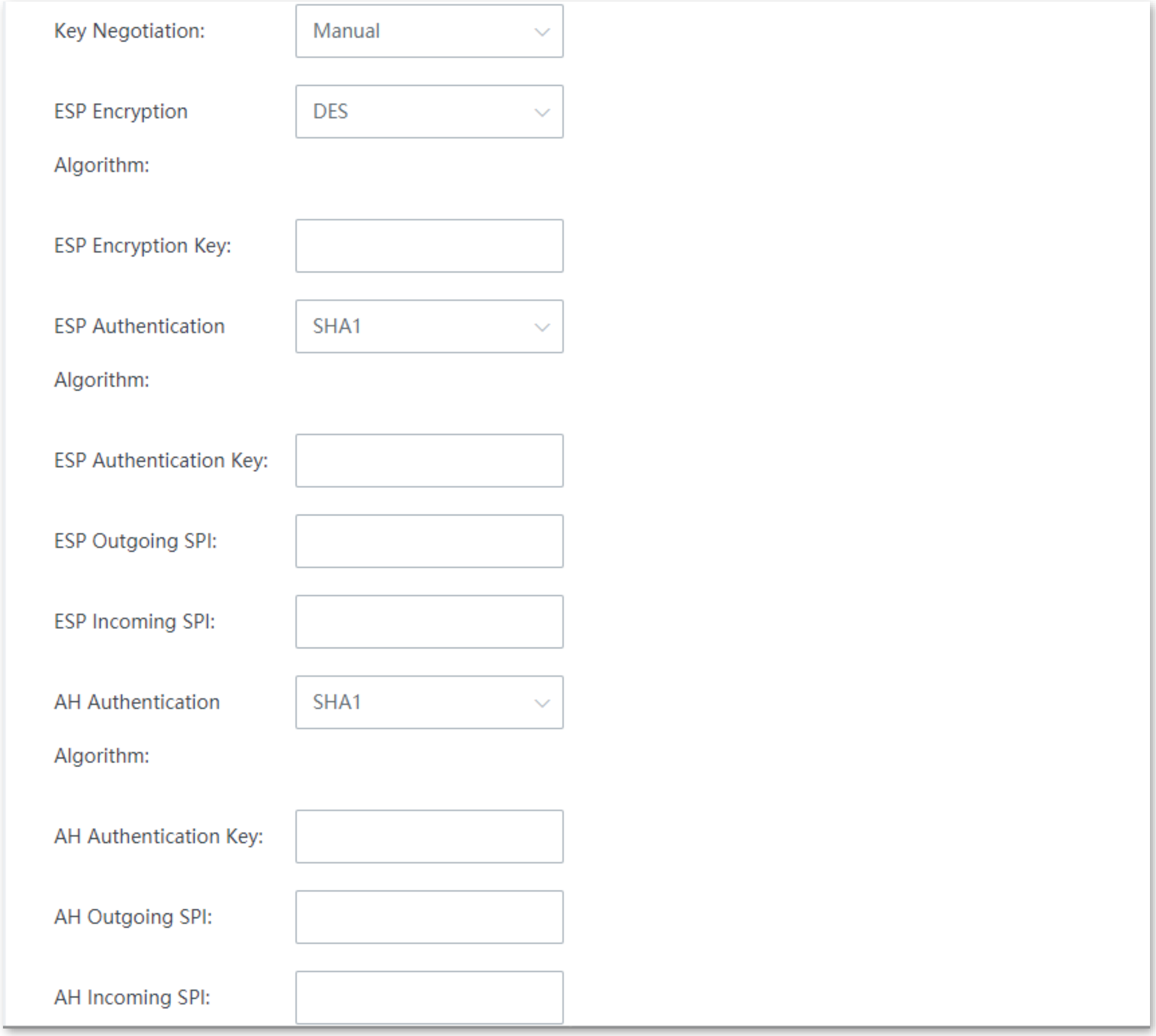
Parameter	Description
Mode	It specifies the exchange mode in IKE phase I, which should be the same as that of peer gateway. – Main: This mode is the primary mode. In this mode, exchanged packets are huge to offer identity protection, which is applicable to scenarios where identity protection is rigorous. – Aggressive: This mode does not offer identity protection. In this mode, the exchanged packets are few in number and negotiation rate is high, which is applicable to scenarios where identity protection is loose.

Parameter	Description
Encryption Algorithm	It specifies the IKE session encryption algorithm. The router supports the following algorithms: – DES (Data Encryption Standard): A 56-bit key is used to encrypt 64-bit data. The last 8 bits of the 64-bit data are used for parity check. **3DES** indicates that three 56-bit keys are used for encryption. – AES (Advanced Encryption Standard): **AES 128/192/256** indicates that 128/192/256-bit keys are used for encryption respectively.
Integrity Verification	It specifies the IKE session verification algorithm. The router supports the following algorithms: – MD5 (Message Digest Algorithm): A 128-bit message digest is generated to prevent message tampering. – SHA1 (Secure Hash Algorithm): A 160-bit message digest is generated to prevent message tampering, leading to higher security than MD5.
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.
Local ID Type	It specifies the ID of the local gateway. – IP Address: The router uses the IP address of the specified WAN port for negotiation with the remote gateway. – FQDN: Fully Qualified Domain Name. If you select FQDN, you need to manually set a string of characters, which should be identical with the remote ID. Note **Local ID Type** and **Peer ID Type** should be the same. Under such circumstances, you are recommended to modify the **Mode** to **Aggressive**.
Peer ID Type	It specifies the ID of the remote gateway. – IP Address: By default, the remote gateway uses the WAN IP address of the router for negotiation. – FQDN: Fully Qualified Domain Name. If you select FQDN, you need to manually set a string of characters, which should be identical with the local ID. Note **Local ID Type** and **Peer ID Type** should be the same. Under such circumstances, you are recommended to modify the **Mode** to **Aggressive**.
Key Expiration	It specifies the life cycle of ISAKMP SA.

Parameter	Description
PFS	This feature generates a new key in IKE Phase II, which is unrelated to the key generated in IKE Phase I, ensuring that the key generated in Phase II is secure even if the key generated in IKE1 Phase I is cracked. With the PFS disabled, generation of the new key in IKE Phase II depends on the key in Phase I. Once the key generated in IKE Phase I is cracked, the key generated in Phase II will suffer threats, and further threatens the communication security.
Key Expiration	It specifies the life cycle of IPSec SA.

Key negotiation mode--Manual

The following displays the page when **Manual** is selected for **Key Negotiation** (Tunnel protocol AH+ESP is used for illustration here).



Key Negotiation:	Manual
ESP Encryption Algorithm:	DES
ESP Encryption Key:	
ESP Authentication Algorithm:	SHA1
ESP Authentication Key:	
ESP Outgoing SPI:	
ESP Incoming SPI:	
AH Authentication Algorithm:	SHA1
AH Authentication Key:	
AH Outgoing SPI:	
AH Incoming SPI:	

Parameter description

Parameter	Description
ESP Encryption Algorithm	When the **Tunnel Protocol** is set to **ESP**, the **ESP** encryption algorithm is required. The router supports the following algorithms: – DES: A 56-bit key is used to encrypt 64-bit data. The last 8 bits of the 64-bit data are used for parity check. **3DES** indicates that three 56-bit keys are used for encryption. – AES: A 128/192/256-bit key is used for encryption.
ESP Encryption Key	It specifies the ESP encryption key. Both IPSec communication parties should have the same key.
ESP/AH Authentication Algorithm	When the **Tunnel Protocol** is set to **ESP** or **AH**, the corresponding encryption algorithm is required. The router supports the following algorithms: – MD5: A 128-bit message digest is generated to prevent message tampering. – SHA1: A 160-bit message digest is generated to prevent message tampering.
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	It specifies the outgoing SPI. SPI, remote gateway address, protocol type identify an IPSec security community. This parameter must be the same with the incoming SPI of the peer device.
ESP/AH Incoming SPI	It specifies the incoming SPI. SPI, remote gateway address, protocol type identify an IPSec security community. This parameter must be the same with the outgoing SPI of the peer device.

Modify IPSec connection

On the **More** > **IPSec** page, click ✎ under the **Operation** column to modify the IPSec connection.

Delete IPSec connection

On the **More** > **IPSec** page, click 🗑 under the **Operation** column to delete the IPSec connection.

Example of configuring an IPSec VPN

Networking requirement

An enterprise and its subsidiary both use cable-free devices to set up network and the cable-free devices have connected to the internet. The enterprise has the following requirements:

Subsidiary staff can access the LAN resources through the internet, such as documents, OA, ERP system, CRM system, project management system and other resources.

Solution

Set up IPSec tunnel on the two cable-free devices for the remote users to securely access the LAN through the internet.

Assume that device 1 is deployed in the headquarters and its basic information is as follows:

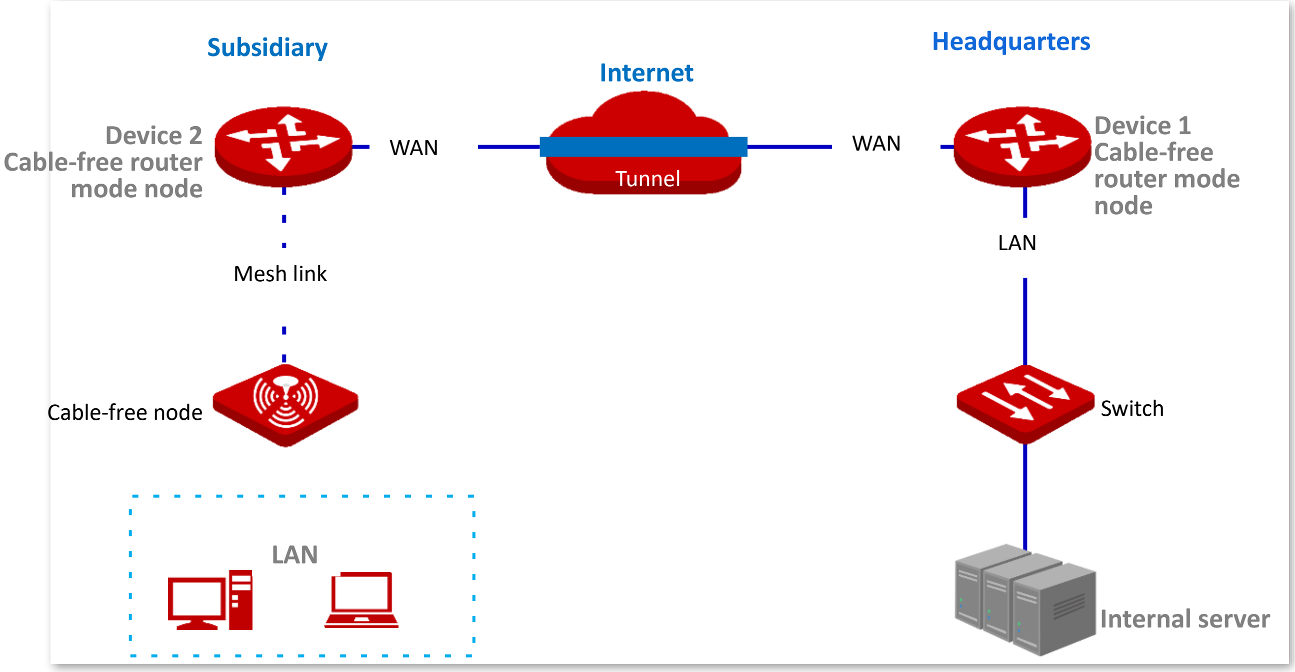
- WAN IP address: 202.105.11.22
- IP address of the LAN: 192.168.5.0/24

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

- WAN IP address: 202.105.88.77
- IP address of the LAN: 192.168.1.0/24

Assume that the basic information of the IPSec connection between the two routers is:

- Encapsulation mode: Tunnel
- Key negotiation mode: Auto negotiation
- Pre-shared key: 12345678



Configuration procedures

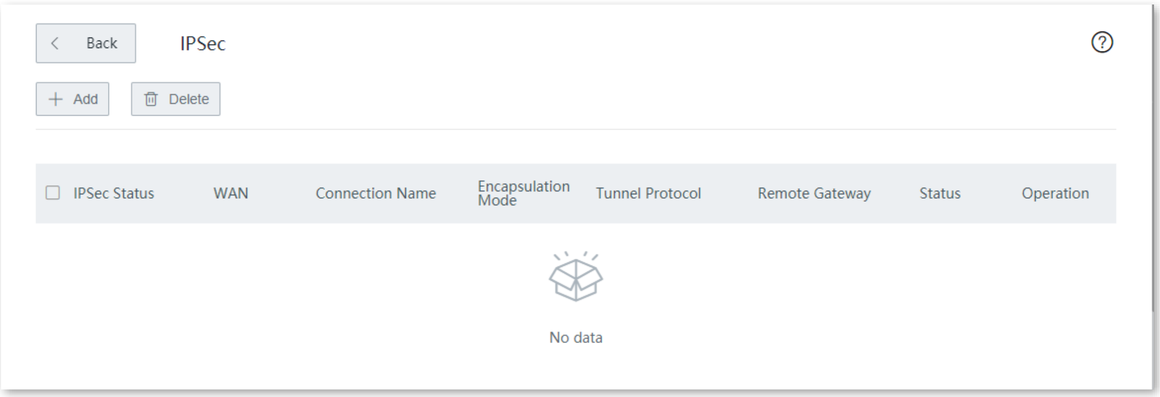
Note

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

If **Manual** is set for **Key Negotiation**, the encryption algorithm, encryption key, and authentication algorithm of the two IPSec parties should be the same. The outgoing SPI of device 1 should be the same with the incoming SPI of device 2 and the incoming SPI of device 1 should be the same with the outgoing SPI of device 2.

I. Set device 1.

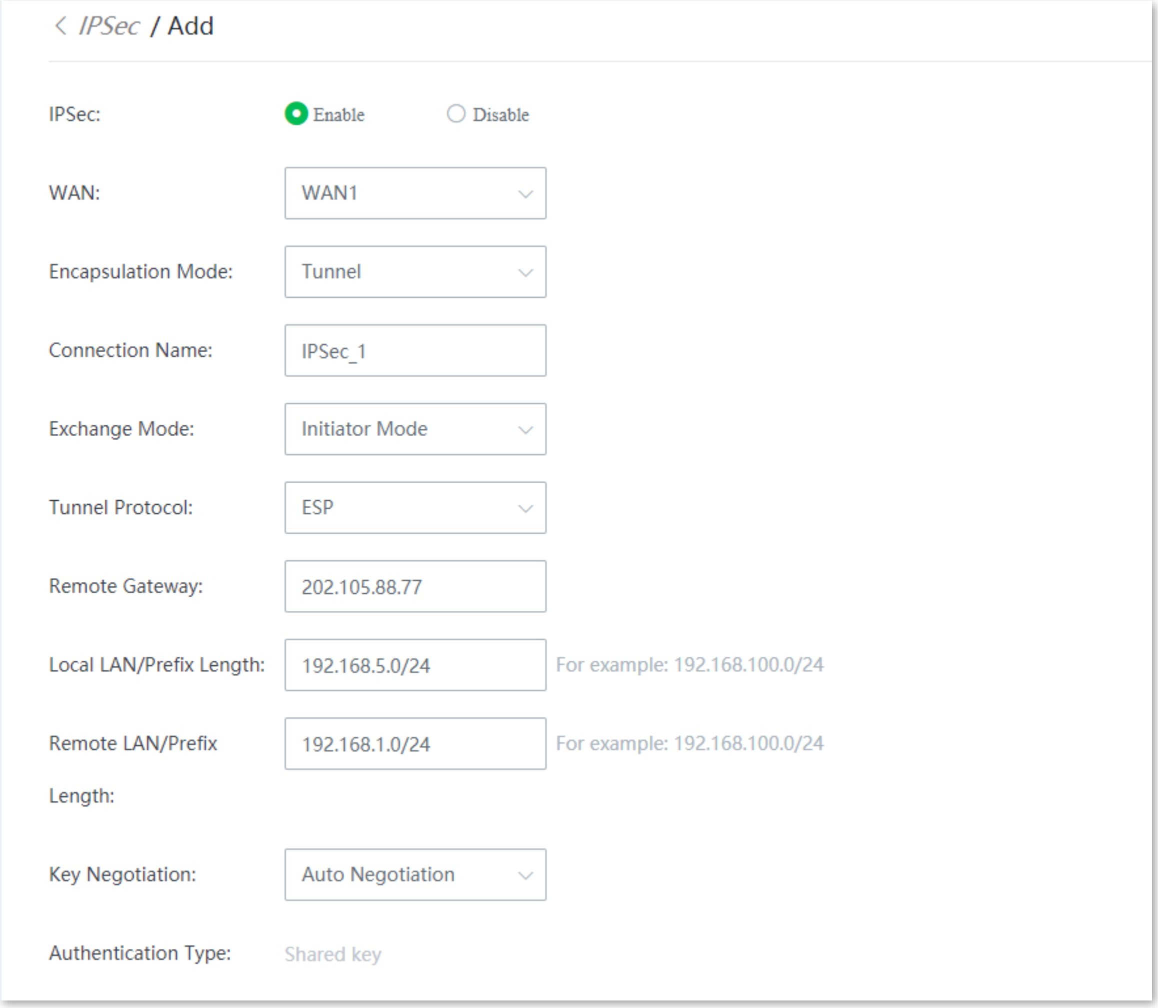
1. Log in to the web UI of the cable-free device 1 and click **More** > **IPSec**.
2. Click **+ Add**.



□ IPSec Status	WAN	Connection Name	Encapsulation Mode	Tunnel Protocol	Remote Gateway	Status	Operation

No data

3. Configure parameters in the **Add** window, and click **Save**.
   (1) Set **Connection Name**, which is **IPSec_1** in this example.
   (2) Enter **Remote Gateway**, which is **202.105.88.77** in this example.
   (3) Enter **Local LAN/Prefix Length**, which is **192.168.5.0/24** in this example.
   (4) Enter **Remote LAN/Prefix Length**, which is **192.168.1.0/24** in this example.
   (5) Set **Pre-shared Key**, which is **12345678** 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

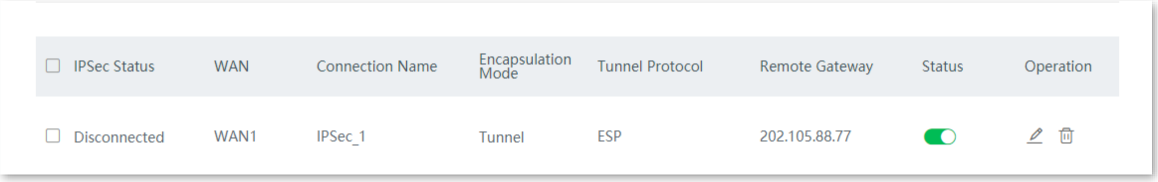
Local LAN/Prefix Length: 192.168.5.0/24 For example: 192.168.100.0/24

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

Key Negotiation: Auto Negotiation

Authentication Type: Shared key

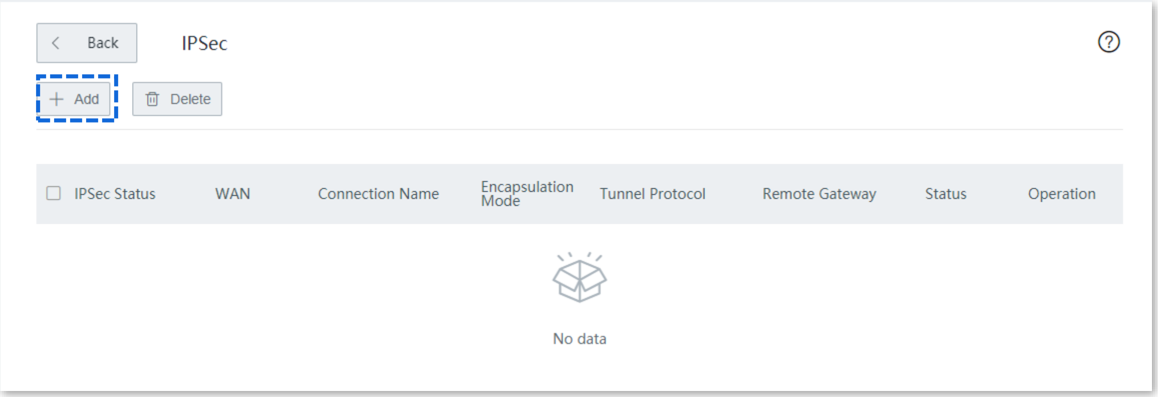
The IPSec is added successfully. See the following figure.



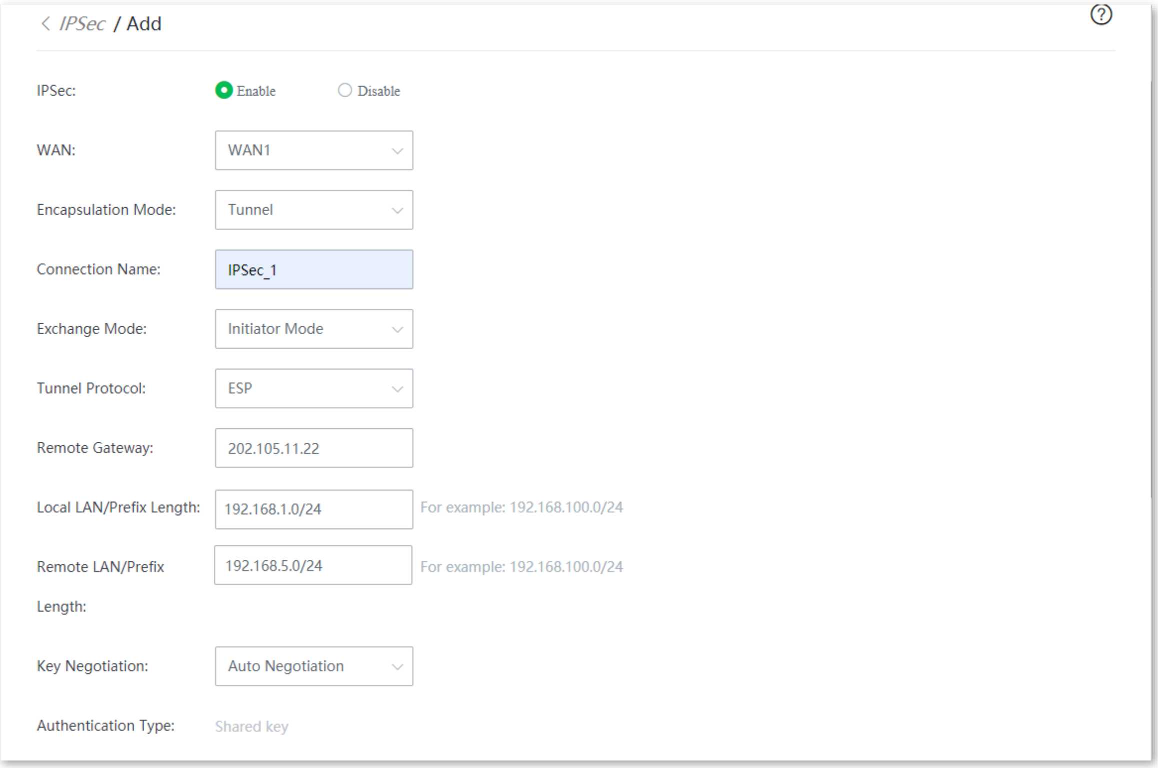
□ IPSec Status	WAN	Connection Name	Encapsulation Mode	Tunnel Protocol	Remote Gateway	Status	Operation
□ Disconnected	WAN1	IPSec_1	Tunnel	ESP	202.105.88.77	●	✎ 🗑

II. Set device 2.

1. Log in to the web UI of the cable-free device 2 and click **More** > **IPSec**.
2. Click **+ Add**.

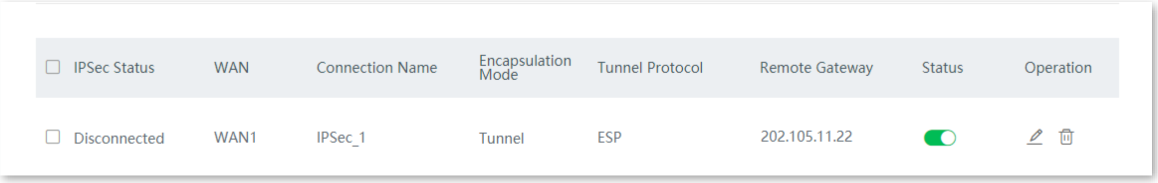


3. Configure parameters in the **Add** window, and click **Save**.
   (1) Set **Connection Name**, which is **IPSec_1** in this example.
   (2) Enter **Remote Gateway**, which is **202.105.11.22** in this example.
   (3) Enter **Local LAN/Prefix Length**, which is **192.168.1.0/24** in this example.
   (4) Enter **Remote LAN/Prefix Length**, which is **192.168.5.0/24** in this example.
   (5) Set **Pre-shared Key**, which is **12345678** 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

The IPSec is added successfully. See the following figure.



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

----End

Verification

When **Connected** is displayed in **IPSec Status**, the IPSec tunnel is set up successfully and headquarters and subsidiary staff can securely access the LAN resources of each other through internet.

3.10.12 Multi-WAN policy

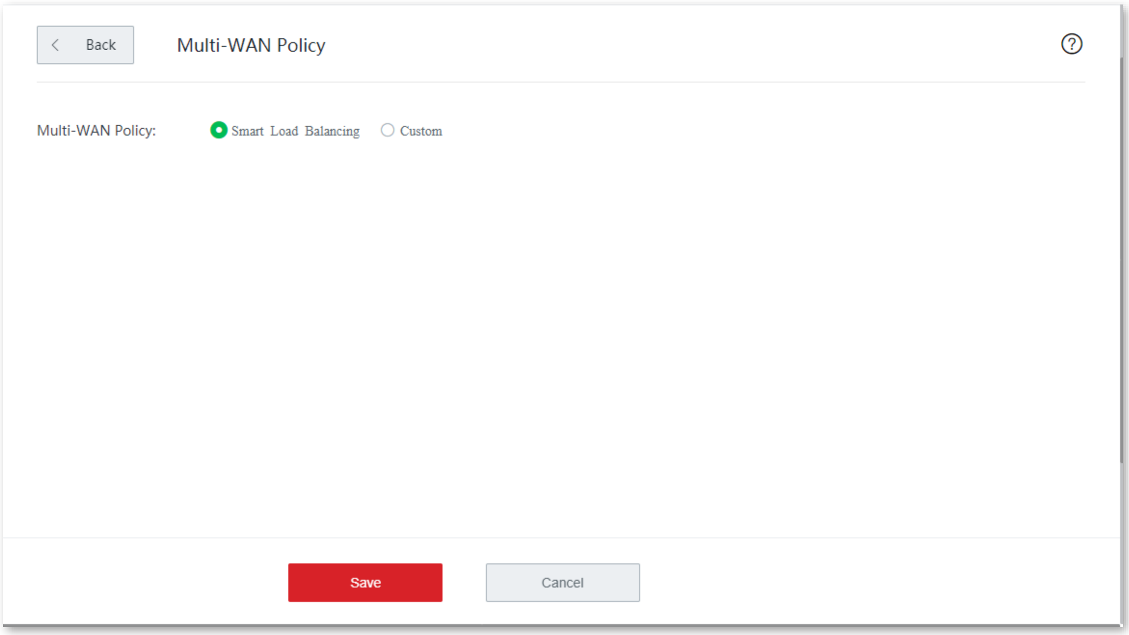
Overview

The cable-free device supports the following types of multi-WAN policy:

- **Smart load balancing** (default): If such a policy is applied, the device automatically distributes traffic based on the bandwidth on the **Bandwidth Control** page through the WAN ports to achieve load balancing.
- **Custom**: Such a policy is configured by an administrator to distribute traffic of specified IP address groups to specified WAN ports.

Click **More** > **Multi-WAN Policy** to enter the page.

By default, the cable-free device enables two WAN ports.



Multi-WAN Policy

Multi-WAN Policy: ● Smart Load Balancing ○ Custom

Parameter description

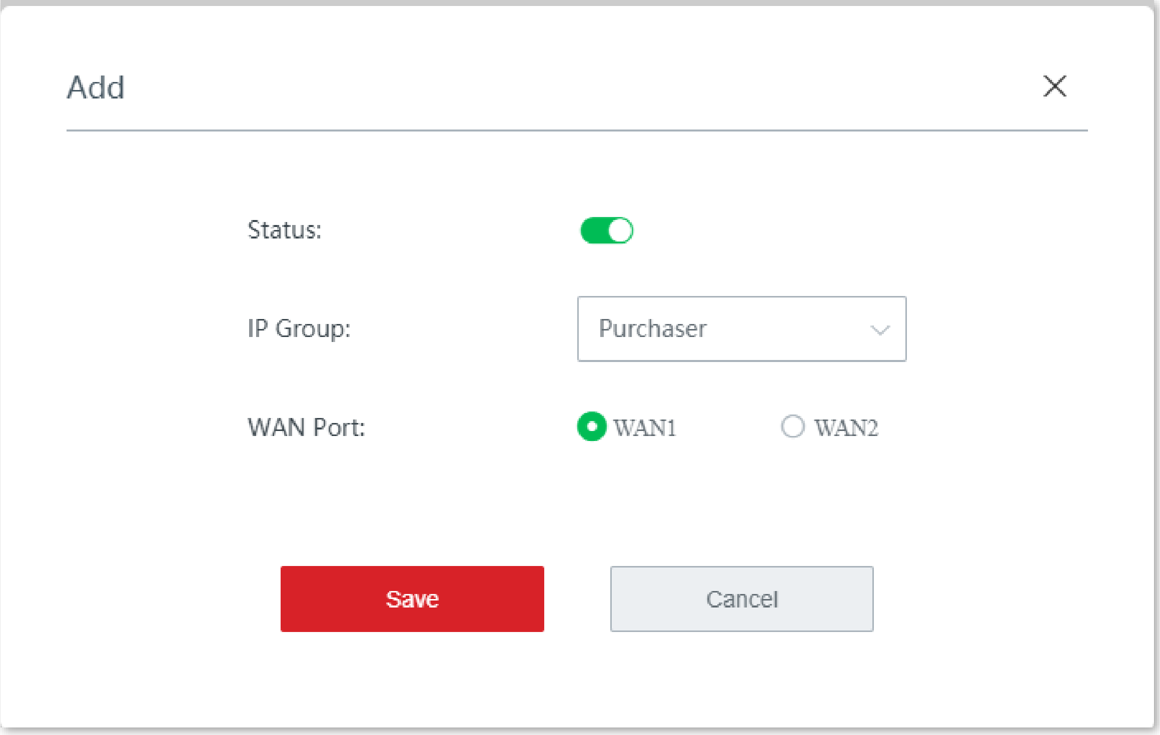
Parameter	Description
Multi-WAN Policy	It specifies the policy through the WAN ports. - **Smart Load Balancing**: The system automatically distributes traffic to the WAN ports with the smallest amount of traffic. - **Custom**: It enables you to assign WAN ports to source IP addresses as required.

Customize a Multi-WAN Policy

Tip

Before configuring the multi-WAN policy, go to **Filter Management** > **IP Group/Time Group** to add an IP group first.

1. Choose **More** > **Multi-WAN Policy**, select **Custom** and click **+Add**.
2. Select the **IP Group** you set.
3. Select the **WAN Port** to which the policy applies.
4. Click **Save**.



Add

Status: ●

IP Group: Purchaser

WAN Port: ● WAN1 ○ WAN2

----End

Parameter description

Parameter	Description
Status	It specifies whether to enable the rule.
IP Group	Create or select the IP group to which the rule applies. To create an IP group, choose **Filter Management** > **IP Group/Time Group**. One IP group matches one rule.
WAN	It specifies the WAN port for incoming and outgoing traffic.

Example of customizing multi-WAN policy

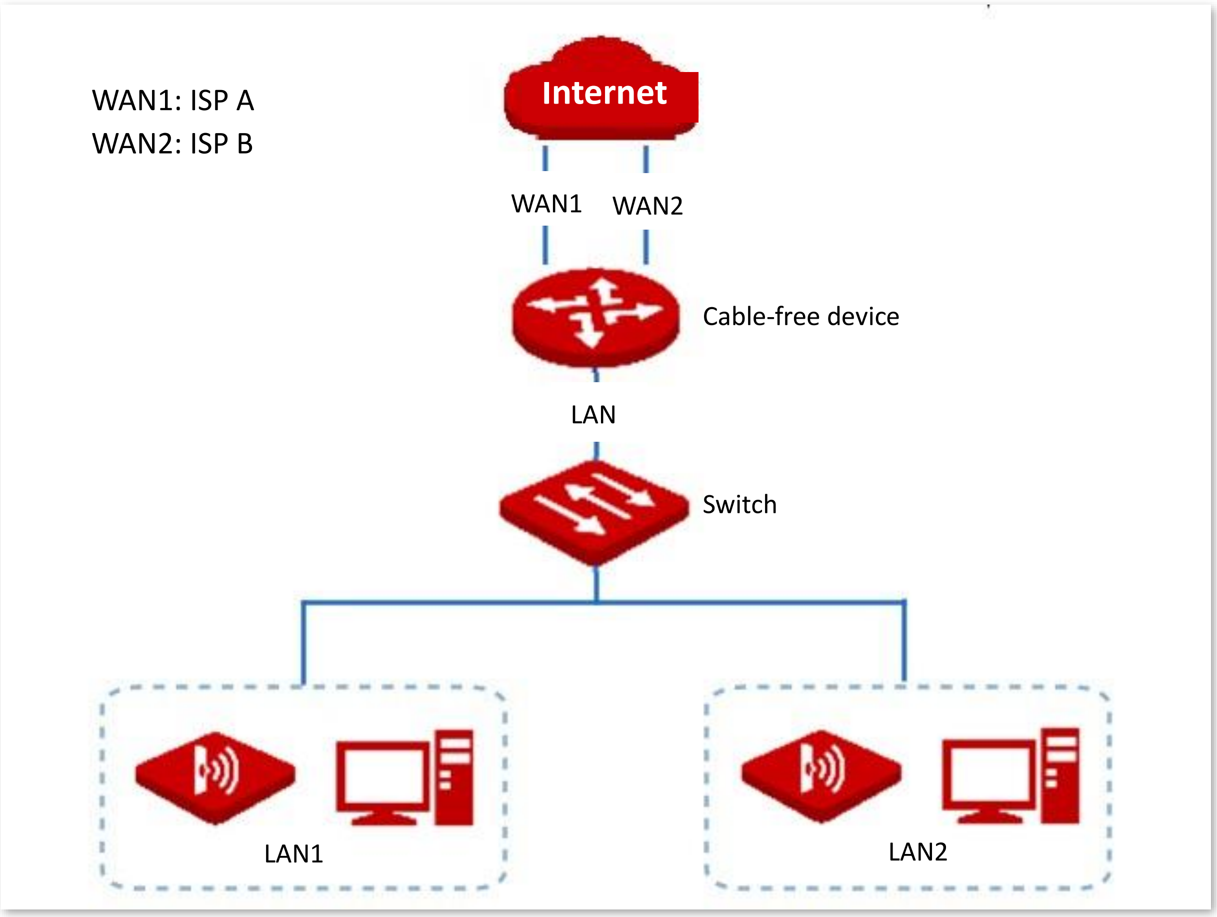
Networking Requirement

An enterprise and its subsidiary both use cable-free devices to set up network and the cable-free devices have connected to the internet. To meet its internet access requirement, the enterprise has set up two broadband connections with two different ISPs and can now access the Internet properly. To achieve load balancing, the enterprise has the following requirements:

- The devices with IP addresses ranging from 192.168.5.2 to 192.168.5.100 access the internet through the fixed-line broadband connection with ISP A.
- The devices with IP addresses ranging from 192.168.5.101 to 192.168.5.250 access the internet through the mobile broadband connection with ISP B.

Solution

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



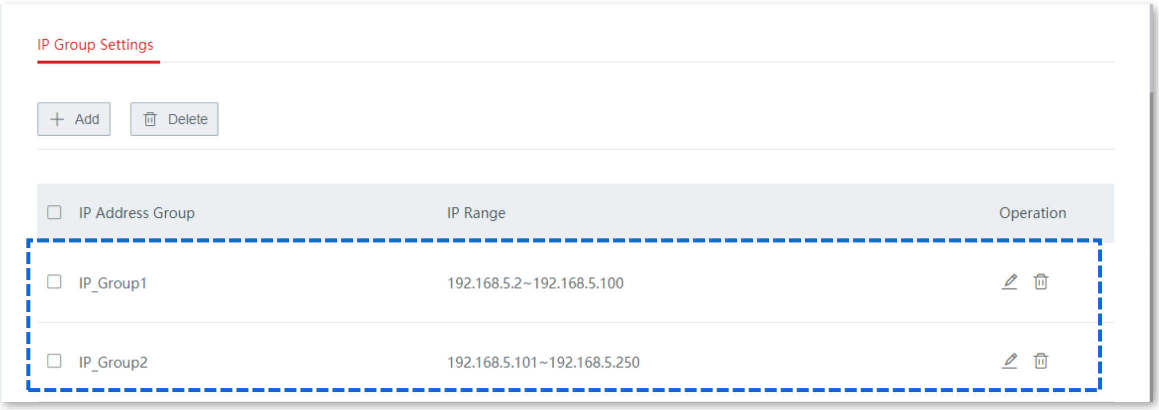
Configuration procedures

Set IP address group > Enable custom multi-WAN policy > Customize multi-WAN policy rule

1. Set IP address groups.

   (1) Click **Filter Management** > **IP Group/Time Group** and locate the **IP Group Settings** configuration area.

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



IP Group Settings

＋ Add   Delete

□ IP Address Group	IP Range	Operation
□ IP_Group1	192.168.5.2~192.168.5.100	
□ IP_Group2	192.168.5.101~192.168.5.250	

2. Enable custom multi-WAN policy.

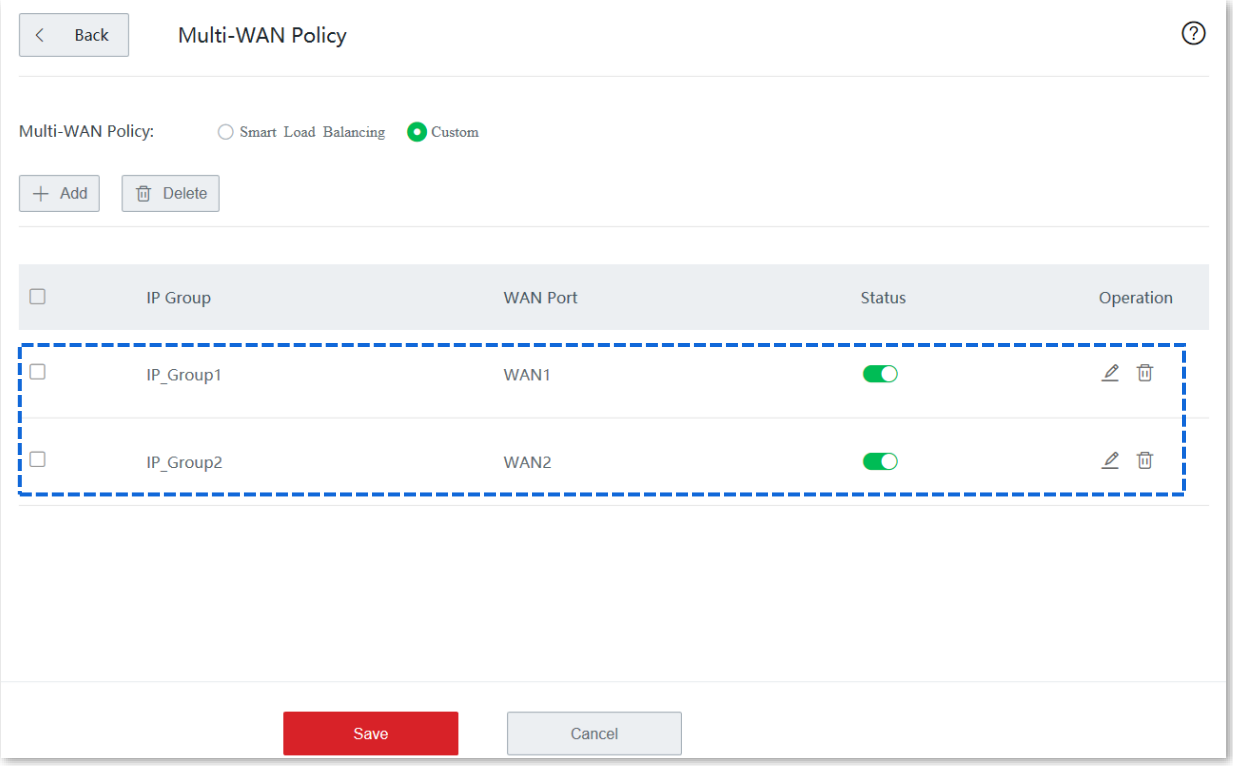
(1) Click **More** > **Multi-WAN Policy**.

(2) Choose **Custom**, and click **Save**.

3. Customize multi-WAN policy rules.

(1) Select the **IP Group** you set and the **WAN Port** to which the policy applies.

(2) Click **Save**.



Multi-WAN Policy: ○ Smart Load Balancing ● Custom

□	IP Group	WAN Port	Status	Operation
□	IP_Group1	WAN1	●	
□	IP_Group2	WAN2	●	

----End

Verification

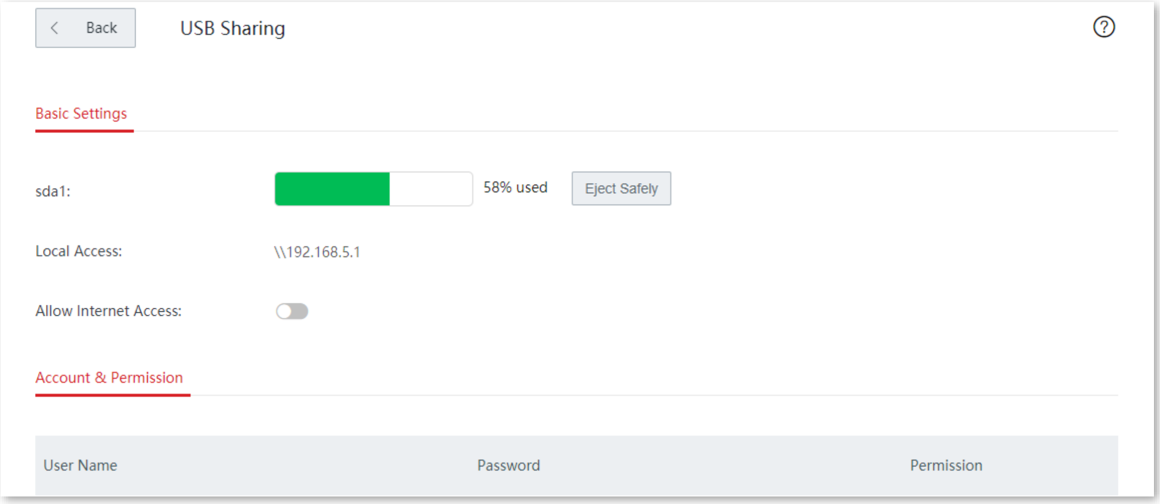
The computers with IP addresses ranging from 192.168.5.2 to 192.168.5.100 access the internet through WAN1.

The computers with IP addresses ranging from 192.168.5.101 to 192.168.5.250 access the internet through WAN2.

3.10.13 USB sharing

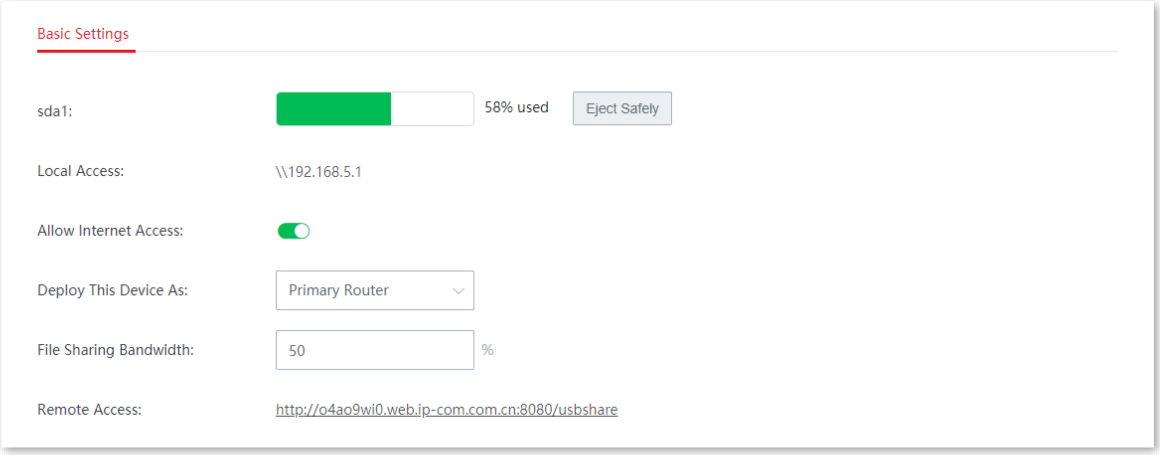
On this page, you can rapidly set up a company-exclusive file server by connecting a USB device to the cable-free device.

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



Basic settings

In this module, you can check the details of the USB disk and the access address of local users, and choose whether to allow internet users to access the USB disk.



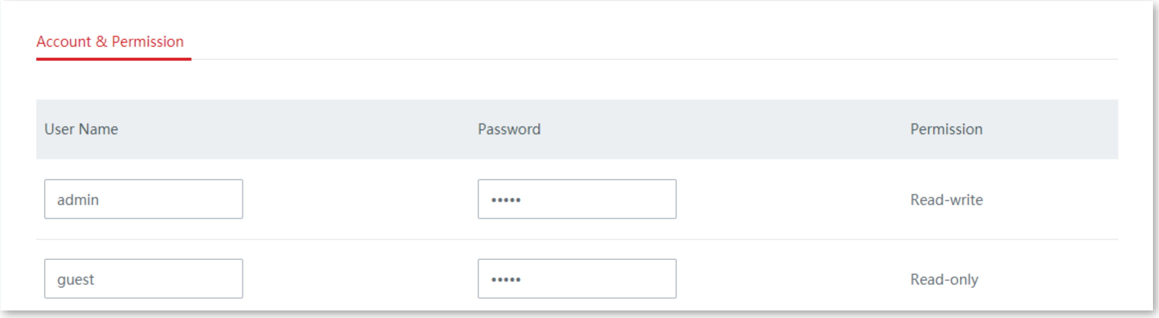
Parameter description

Parameter	Description
sda1	It specifies the status and occupation percentage of the USB disk device.
Eject Safely	Click it to safely eject the USB disk device.
Local Access	It specifies the access address LAN users use to access the USB disk device. \\192.168.5.1: You can type this address into the **Start > Run** menu on your computer to get local access. 192.168.5.1 is the default LAN IP address of the router. If the address is changed, you need to type in the new address to get local access.

Parameter	Description
Allow Internet Access	Toggle it on to enable internet users to access the USB disk device. Tip After it is enabled, you can remotely access the files of USB storage device plugged in the cable-free device through IP-COM INAS App. For details, please refer to the user guide of IP-COM INAS App.
Deploy This Device As	It specifies the role the cable-free device plays in the network. The options include **Primary Router** and **Secondary or Multi-Level Router**. Note This parameter must be set to the role the cable-free device actually plays in the network. Otherwise, internet user may fail to access the USB disk device.
File Sharing Bandwidth	It specifies the bandwidth ratio assigned to internet users to access the USB disk device. Please set a proper value so that resource conflict between internet users and LAN users will not occur.
File Sharing Port	This parameter appears only when **Secondary or Multi-Level Router** is selected for **Deploy This Device As**. It specifies the port used for file sharing.
External Port on Primary Router	This parameter appears only when **Secondary or Multi-Level Router** is selected for **Deploy This Device As**. It specifies the external port on the primary router used for port forwarding. Tip If the cable-free device is deployed as Secondary or Multi-Level Router, you need to configure a port forwarding rule on the primary router to this device to realize internet access to the company file server.
Remote Access	It specifies the domain name internet users use to access the USB disk device.

Account & permission

In this module, you can modify the user name and password for both the read-write and read-only users of the USB disk device.



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

Parameter description

Parameter	Description
User Name	It specifies the user name of the read-write or the read-only user.
Password	It specifies the password of the read-write or the read-only user.
Permission	It specifies the permission of the target user. The options include **Read-write** and **Read-only**. – Read-write: The user can read, add, or delete files on the USB disk device. – Read-only: The user can only read files on the USB disk device.

Example of configuring USB sharing

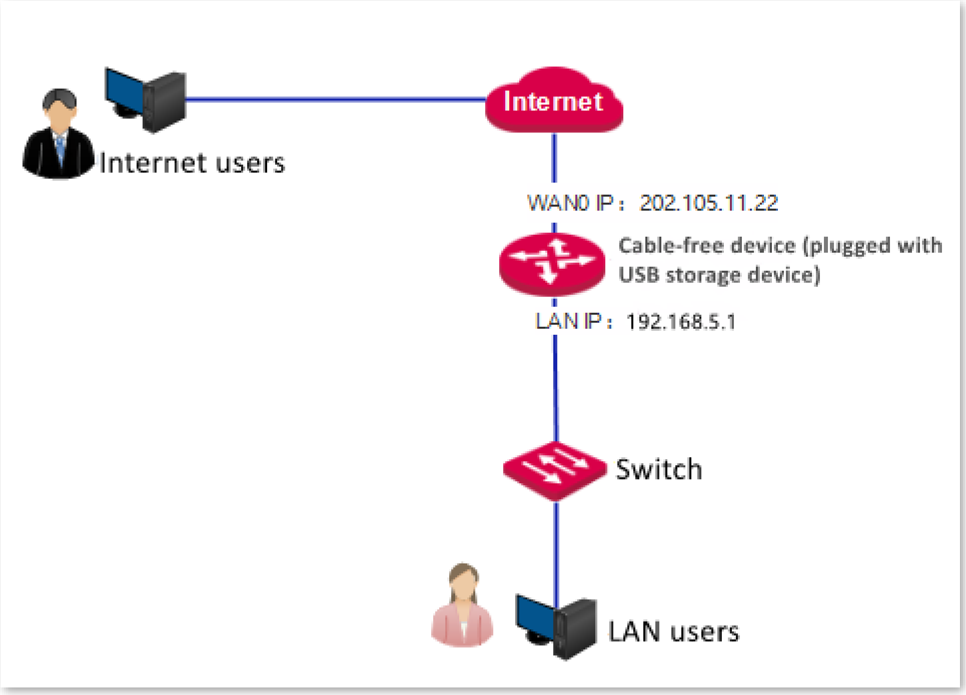
Networking requirement

An enterprise uses the cable-free device to build a network.

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

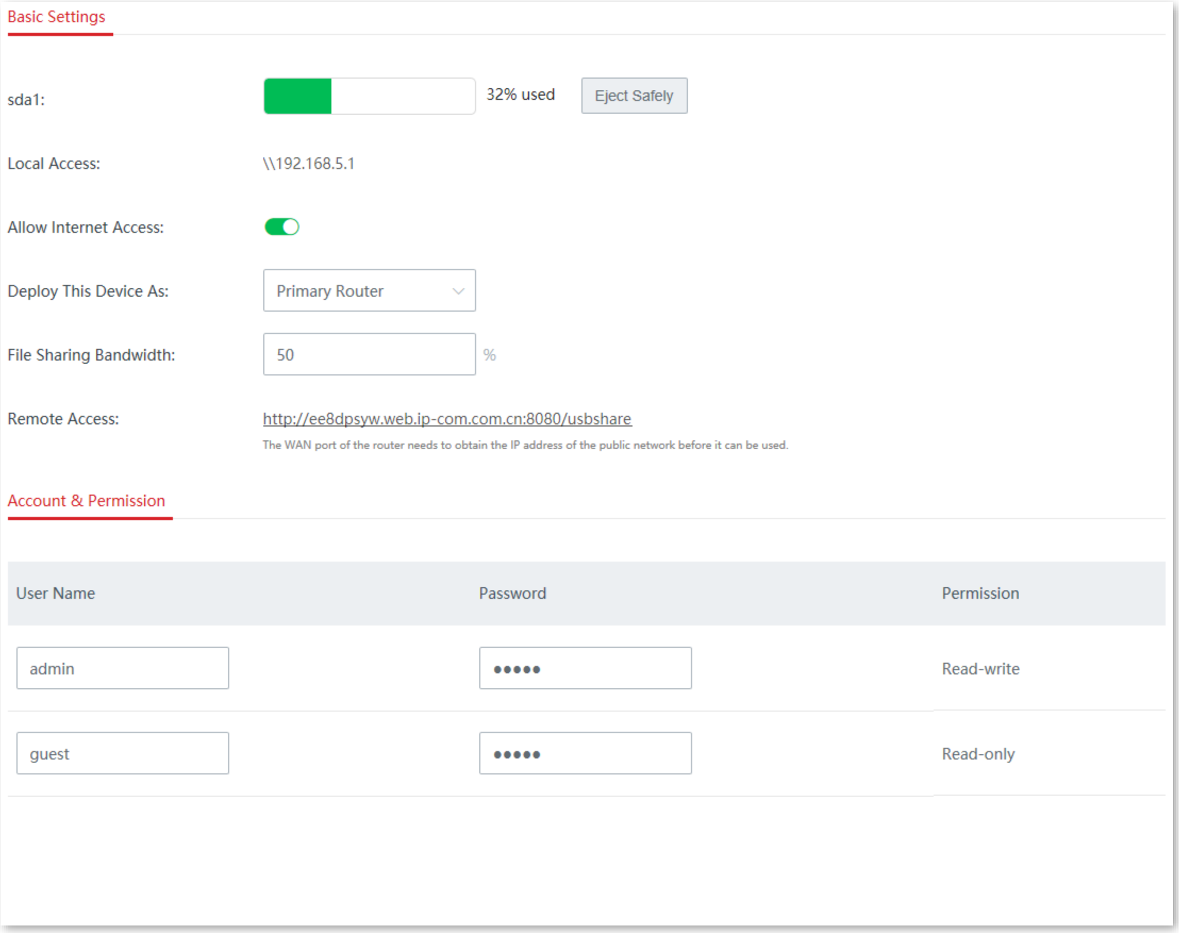
Assume that the read-write user name/password are both “xxadmin”, and the read-only user name/password are both “xxguest”.

Network Topology



Configuration Procedures

1. Plug the mobile storage device into the cable-free device.
2. Log in to the web UI of the cable-free device and click **More** > **USB Sharing.**
3. Toggle on **Allow Internet Access**.
4. Set the read-write user name/password as “**xxadmin**”, and the read-only user name/password as “**xxguest**”.
5. Click **Save**.



Basic Settings

sda1: 32% used

Local Access: \\192.168.5.1

Allow Internet Access:

Deploy This Device As: Primary Router

File Sharing Bandwidth: 50 %

Remote Access: http://ee8dpsyw.web.ip-com.com.cn:8080/usbshare

The WAN port of the router needs to obtain the IP address of the public network before it can be used.

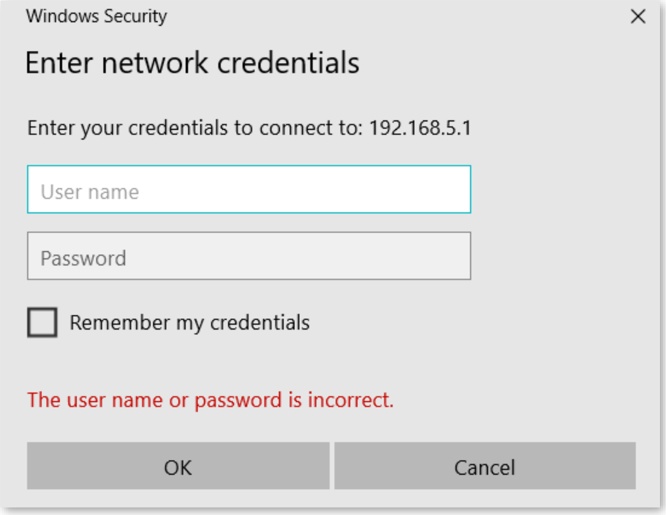
Account & Permission

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

Verification

LAN users access the server:

Take Windows 10 as an example: Enter **\\192.168.5.1** in the search bar at the lower-left of your computer screen. Then, the following page appears. Enter authorized user name and password, and click **Ok**.



Windows Security

Enter network credentials

Enter your credentials to connect to: 192.168.5.1

□ Remember my credentials

The user name or password is incorrect.

Internet users access the server:

Method one (through computer):

Start a browser, enter the **Remote Access** domain name. Then, the authorization page appears. Enter authorized user name and password in the authorization page.

Method two (through IP-COM INAS App):

Log in to the IP-COM INAS App, click **File > Add System**. Enter the Remark, remote access Domain Name, authorized user name and password, click **Save**, and the file share system is successfully added. For details, please refer to the user guide of IP-COM INAS App.

3.11 Maintenance

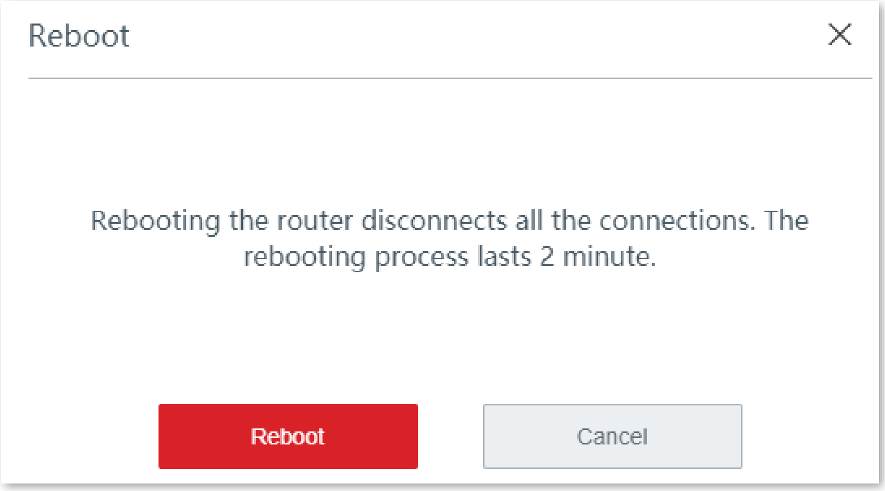
3.11.1 Reboot

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

Tip

When you reboot the primary node, secondary nodes reboot too.

Click **Maintenance** > **Reboot** to enter the page. The prompt window appears. Confirm the message and click **Reboot**.



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

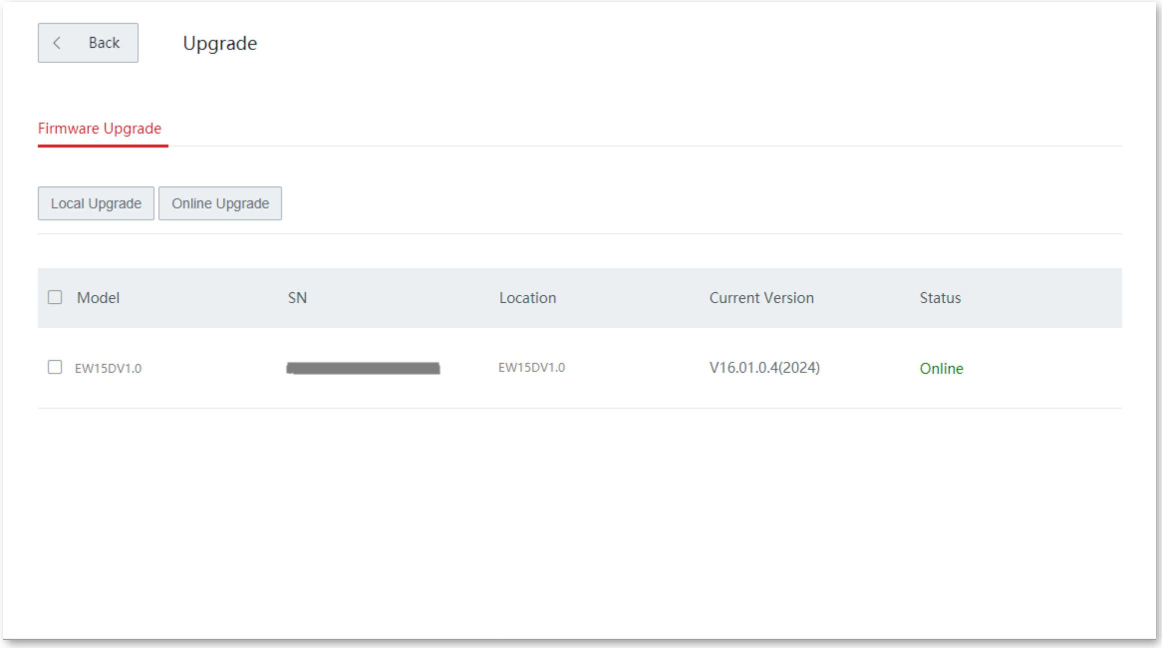
3.11.2 Upgrade

Overview

Click **Maintenance** > **Upgrade** to enter the page.

On this page, you can upgrade the firmware of the cable-free device, so as to experience more functions and get a better user experience.

The cable-free device supports local upgrade and online upgrade.



□ Model	SN	Location	Current Version	Status
□ EW15DV1.0	[redacted]	EW15DV1.0	V16.01.0.4(2024)	Online

Parameter description

Parameter	Description
Local Upgrade	Go to www.ip-com.com.cn to download the latest firmware to your local computer, and upgrade the cable-free device manually.
Online Upgrade	When the cable-free device is connected to the internet, you can select the device to be upgraded and click **Online Upgrade**. The device will download the firmware and upgrade the firmware automatically.

Local upgrade

Note

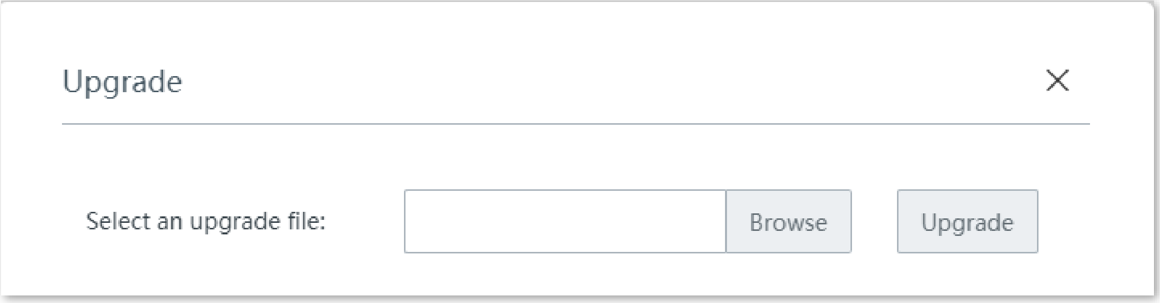
To make sure the upgrade is performed properly and the cable-free device is not damaged, ensure that:

- The correct upgrade file is used. Generally, a firmware upgrade file has a suffix of .bin
- During the upgrade, do not power off the device.

1. Visit www.ip-com.com.cn, download the upgrade firmware of the model to your computer, and unzip it.
2. Log in to the web UI of your device, click **Maintenance** > **Upgrade**, and locate the **Firmware Upgrade** module.
3. Select the cable-free device 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.

Tip

The file loading button of different browsers may differ. Chrome is taken for illustration here.



----End

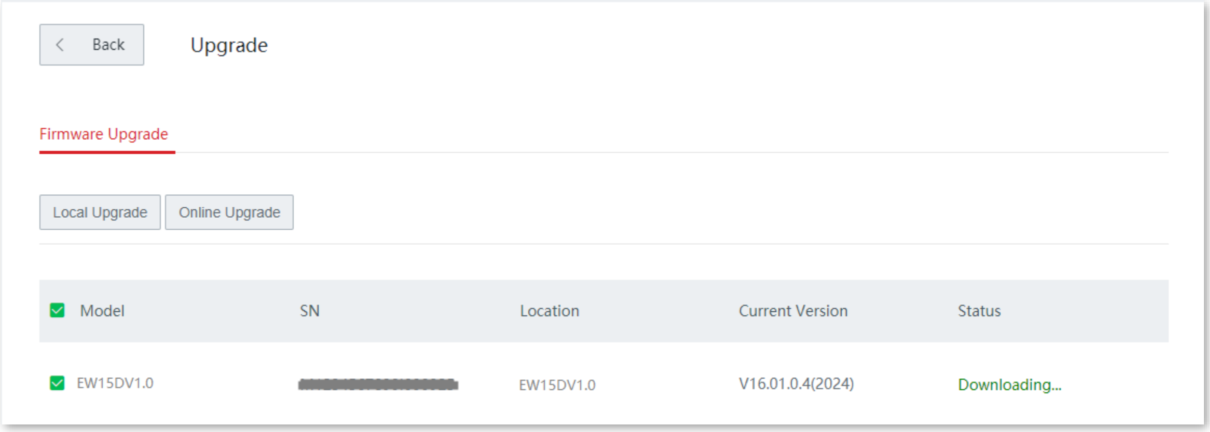
After the progress bar completes, you can log in again and check the current software version number of the device on the Upgrade or System Status page to confirm whether the upgrade is successful.

Tip

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

Online upgrade

When the device is connected to the internet, you can select the device to be upgraded and click **Online Upgrade**. The device will download the firmware and upgrade the firmware automatically.



☑ Model	SN	Location	Current Version	Status
☑ EW15DV1.0	[redacted]	EW15DV1.0	V16.01.0.4(2024)	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

After the reset, the default LAN IP address of the cable-free device is 192.168.5.1

Note

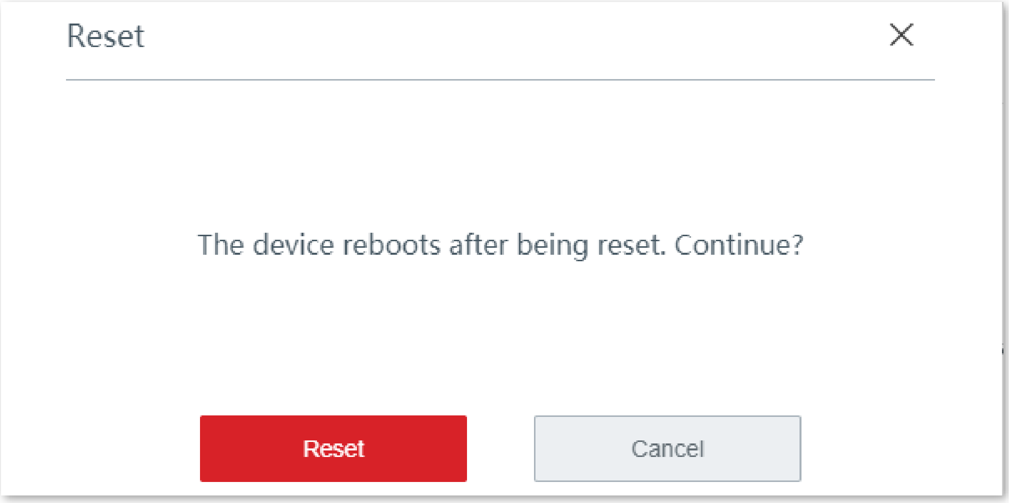
- After the reset, the cable-free device will be restored to factory settings and you can access the internet only after you reconfigure it. Reset device with caution.
- To avoid damaging the device, ensure that the device is powered on throughout the reset.

Reset the device using web UI

Tip

When you reset the primary node using web UI, secondary nodes are also reset and restored to factory settings.

On the **Maintenance > Reset** page, confirm the information 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.

When the **SYS** LED indicator is blinking, hold down the **RESET** button with a needle-like object for about 8 seconds and release it when all the LED indicators light solid green. When the **SYS** LED indicator blinks again, the device is reset successfully.

3.11.4 Password manager

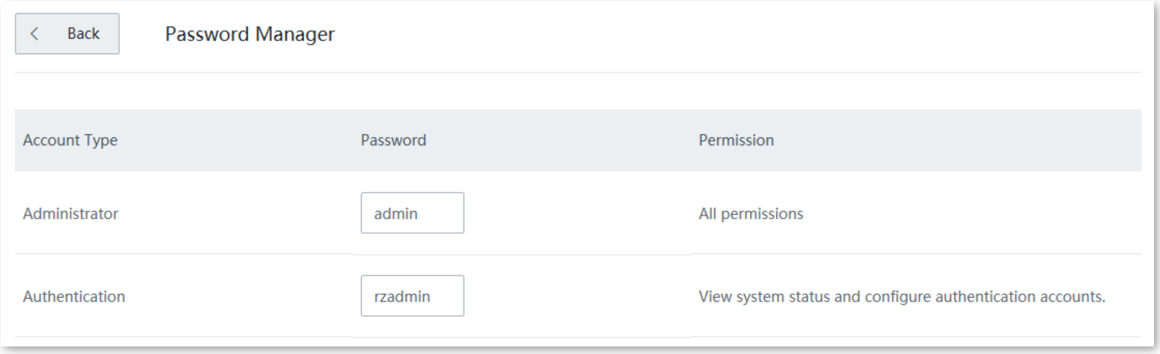
Overview

Click **Maintenance** > **Password Manager** to enter the page.

On this page, you can modify the password of the administrator. You need to set the password the first time you use the cable-free device.

Modify login password

1. Click **Maintenance** > **Password Manager** to enter the page.
2. Locate the target account type and modify the password.
3. Click **Save**.



Password Manager

Account Type	Password	Permission
Administrator	admin	All permissions
Authentication	rzadmin	View system status and configure authentication accounts.

----End

You will be redirected to the login page. Enter the password you set, and click **Login** to log in to the web UI of the device.

3.11.5 Custom reboot

Overview

On this page, you can set the cable-free device to automatically reboot periodically to avoid such phenomena as deteriorating performance and instability caused by long time operation.

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

The device supports cyclic reboot and reboot schedule.

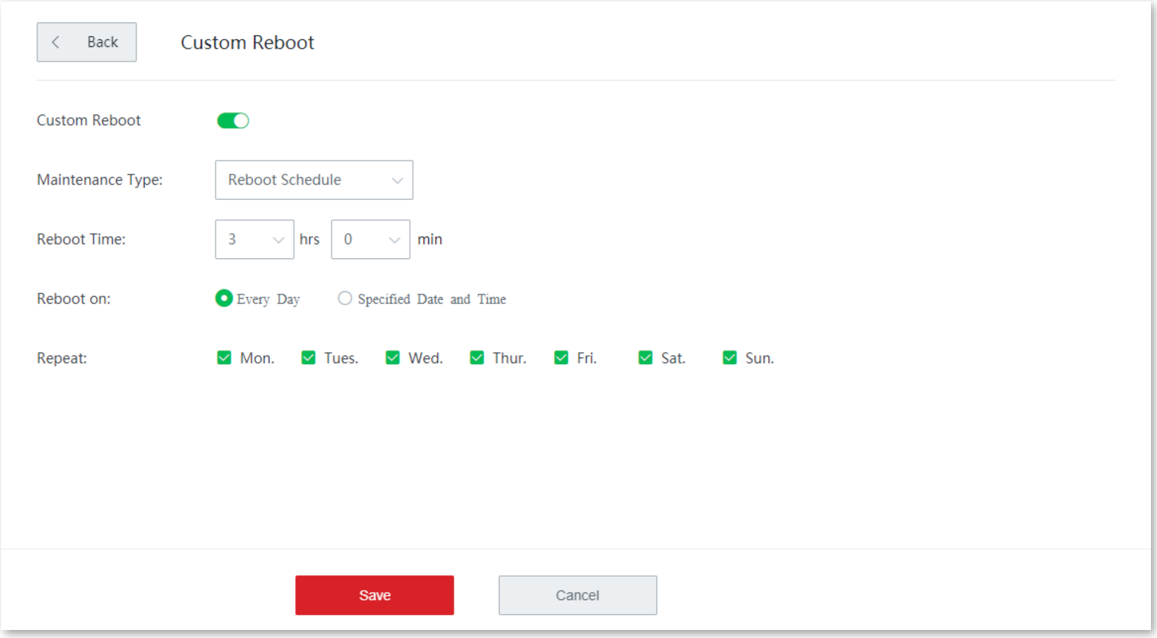
- Cyclic Reboot: The device automatically reboots every specified interval.
- Reboot Schedule: The device automatically reboots on the specified time and date.

Reboot schedule

Tip

To enable reboot schedule function to work properly, ensure that the System time of your cable-free device is correct.

1. Click **Maintenance** > **Custom Reboot** to enter the page.
2. Toggle on **Custom Reboot**.
3. Set the time, which is **3 hrs 0 min** in this example.
4. Set the date, which is **Every Day** in this example.
5. Click **Save**.



Custom Reboot: on

Maintenance Type: Reboot Schedule

Reboot Time: 3 hrs 0 min

Reboot on: ● Every Day ○ Specified Date and Time

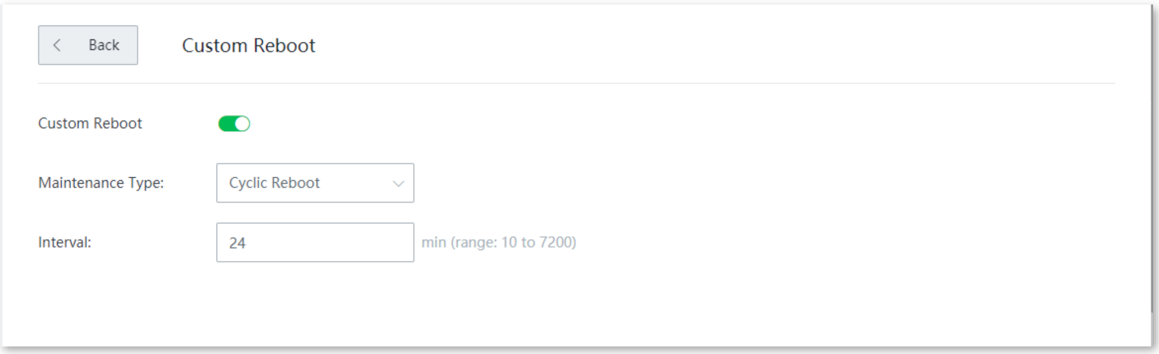
Repeat: ☑ Mon. ☑ Tues. ☑ Wed. ☑ Thur. ☑ Fri. ☑ Sat. ☑ Sun.

----End

The device automatically reboots every 3 am in the morning.

Cyclic reboot

1. Click **Maintenance** > **Custom Reboot**.
2. Toggle on **Custom Reboot**.
3. Select **Cyclic Reboot**.
4. Set the interval.
5. Click **Save**.



Custom Reboot ●

Maintenance Type: Cyclic Reboot

Interval: 24 min (range: 10 to 7200)

----End

The device automatically reboots every specified interval.

3.11.6 Backup/restore

Overview

You can use the backup function to copy the current configurations of the cable-free device to the local computer and use the restore function to restore the configurations of the cable-free device to the backed up configurations.

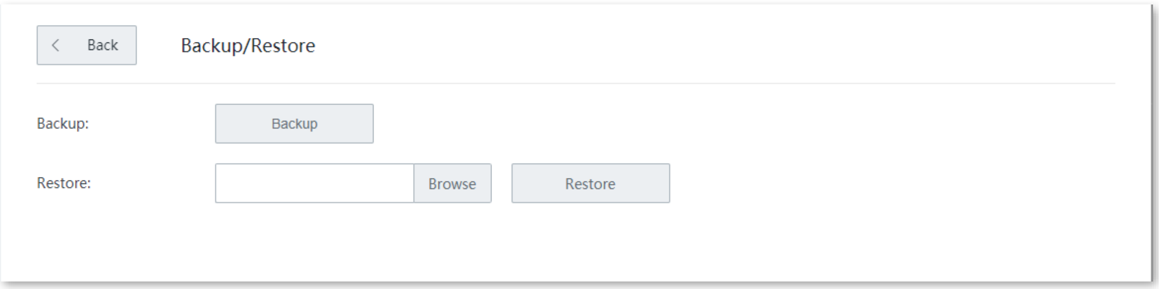
You are recommended to back up the configuration after it is significantly changed. When the performance of your device decreases because of an improper configuration, or after you restore the device to factory settings, you can use this function to restore the configuration that has been backed up.

Click **Maintenance** > **Backup/Restore** to enter the page.

Backup

1. Click **Maintenance** > **Backup/Restore**.

2. Click **Backup**. The system exports a **RouterCfm.cfg** file to your local computer.



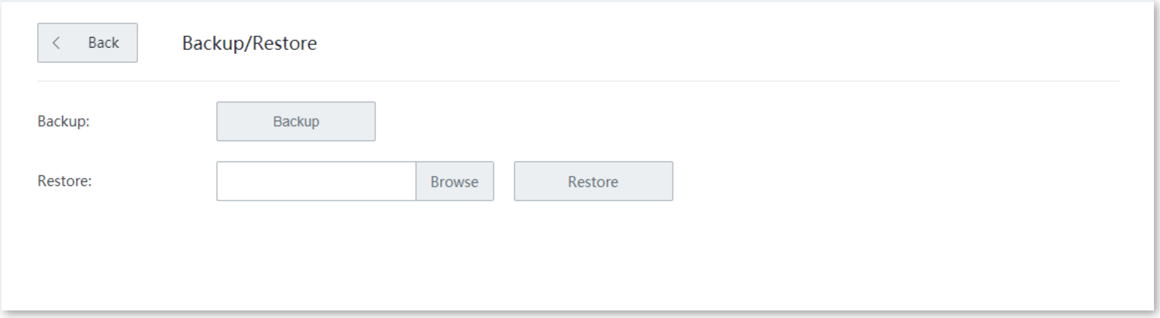
----End

Restore

1. Click **Maintenance** > **Backup/Restore**.
2. Click **Browse**, and upload the configuration file ending with **.cfg**.
3. Click **Restore**.

Tip

The file loading button of different browsers may differ. Chrome is taken for illustration here.



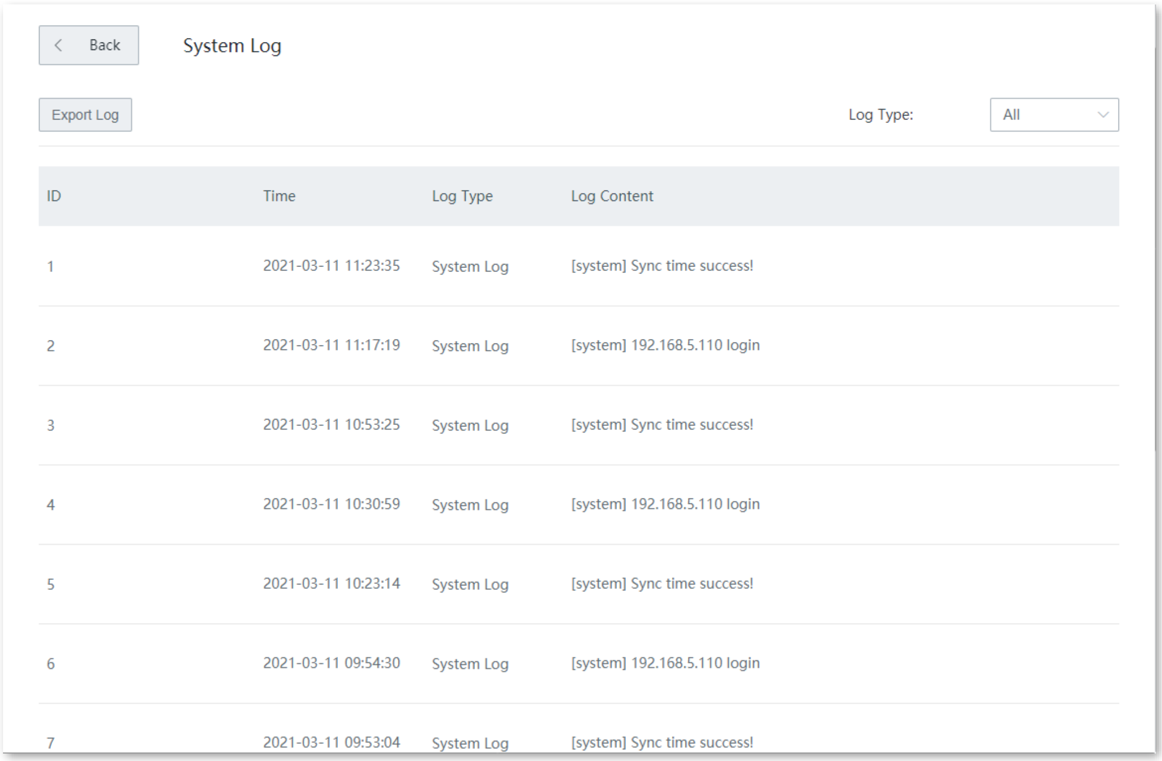
----End

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

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.

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



ID	Time	Log Type	Log Content
1	2021-03-11 11:23:35	System Log	[system] Sync time success!
2	2021-03-11 11:17:19	System Log	[system] 192.168.5.110 login
3	2021-03-11 10:53:25	System Log	[system] Sync time success!
4	2021-03-11 10:30:59	System Log	[system] 192.168.5.110 login
5	2021-03-11 10:23:14	System Log	[system] Sync time success!
6	2021-03-11 09:54:30	System Log	[system] 192.168.5.110 login
7	2021-03-11 09:53:04	System Log	[system] Sync time success!

The time of the logs depend on the system time of the cable-free device. To make sure the time of the logs are correct, please set correctly the system time of the cable-free device first.

Note

- The cable-free device records only the logs occurred after the last reboot.
- After a power cutoff, such operations as power-on again, firmware upgrade, backup/restore, and reset will all cause the cable-free device to reboot.

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 cable-free device to the destination IP address or domain name.

Click **Maintenance** > **Diagnostic Tool** to enter the page.

Execute Ping command

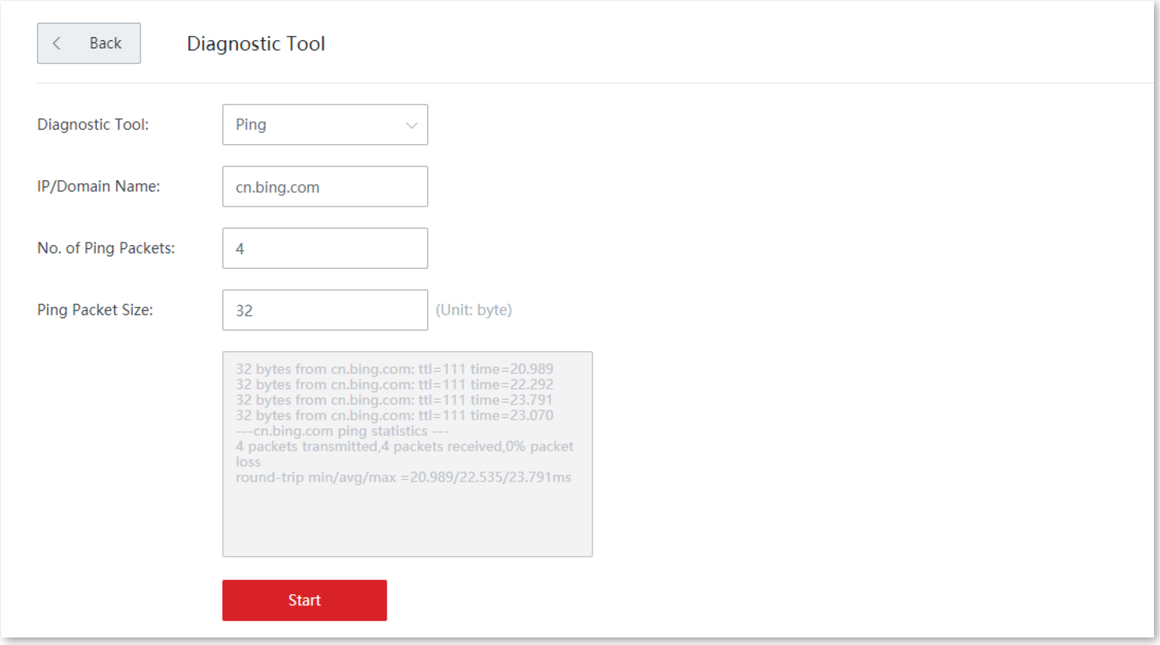
Assume that you need to detect the connectivity between the device and the **Bing** website.

Configuration procedures:

1. Click **Maintenance** > **Diagnostic Tool**.
2. Select **Ping** from the drop-down list of **Diagnostic Tool**.
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**. You are recommended to retain the default settings.
5. Set **Ping Packet Size**. You are recommended to retain the default settings.
6. Click **Start**.

----End

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



Diagnostic Tool: Ping

IP/Domain Name: cn.bing.com

No. of Ping Packets: 4

Ping Packet Size: 32 (Unit: byte)

```
32 bytes from cn.bing.com: ttl=111 time=20.989
32 bytes from cn.bing.com: ttl=111 time=22.292
32 bytes from cn.bing.com: ttl=111 time=23.791
32 bytes from cn.bing.com: ttl=111 time=23.070
---cn.bing.com ping statistics ---
4 packets transmitted,4 packets received,0% packet
loss
round-trip min/avg/max =20.989/22.535/23.791ms
```

Execute Traceroute command

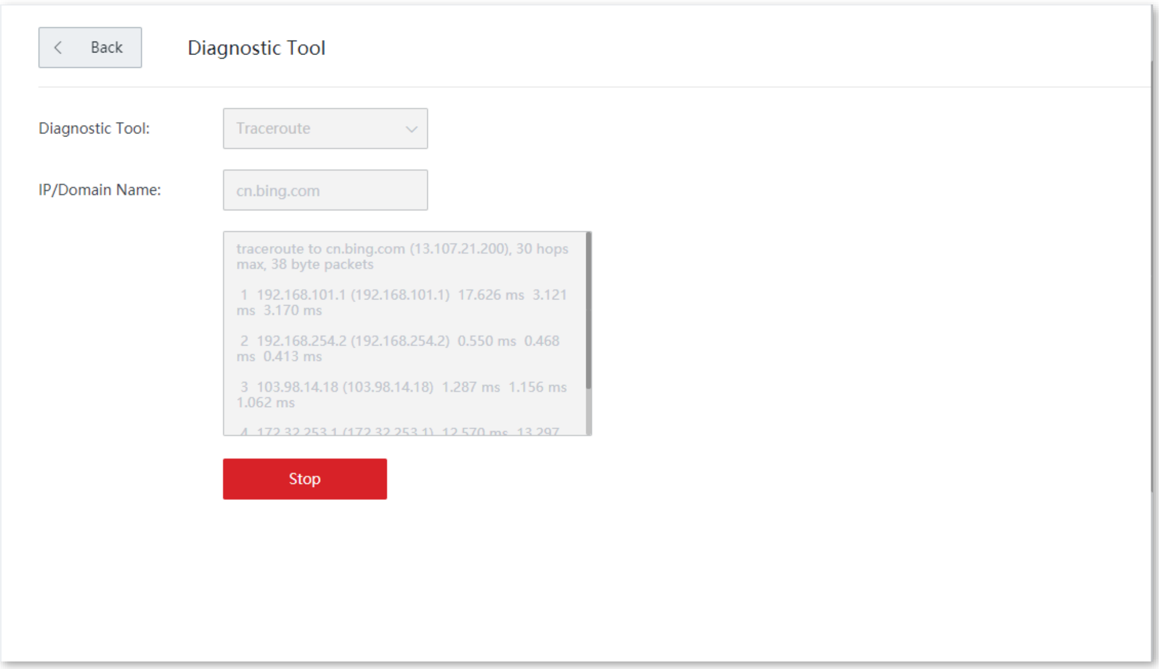
Assume that you need to detect the path from the device to **Bing** website.

Configuration procedures:

1. Click **Maintenance** > **Diagnostic Tool**.
2. Select **Traceroute** from the drop-down list of **Diagnostic Tool**.
3. Enter the IP address or domain name of the traceroute target, which is **cn.bing.com** in this example.
4. Click **Start**.

----End

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



Diagnostic Tool: Traceroute

IP/Domain Name: cn.bing.com

```
traceroute to cn.bing.com (13.107.21.200), 30 hops
max, 38 byte packets

 1  192.168.101.1 (192.168.101.1)  17.626 ms  3.121
ms  3.170 ms

 2  192.168.254.2 (192.168.254.2)  0.550 ms  0.468
ms  0.413 ms

 3  103.98.14.18 (103.98.14.18)  1.287 ms  1.156 ms
1.062 ms

 4  172.32.253.1 (172.32.253.1)  12.570 ms  13.297
```

3.11.9 System time

To make the time-related functions effective, ensure that the system time of the device is set correctly.

The device supports:

- Sync with internet time
- Manual

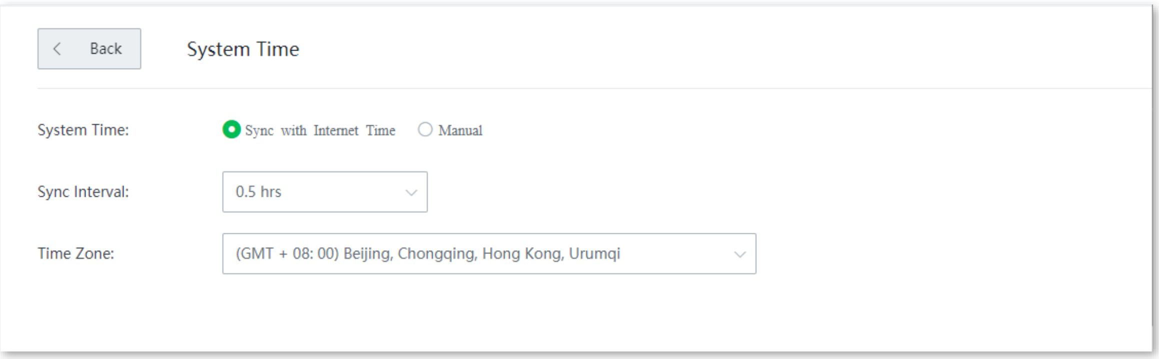
By default, sync with internet time is chosen.

Click **Maintenance** > **System Time** to enter the page.

Sync with internet time

If you choose 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.

After the configuration, you can enter the System Status page to check whether the system time of the cable-free device is correct.



Back

System Time

System Time: ● Sync with Internet Time ○ Manual

Sync Interval: 0.5 hrs

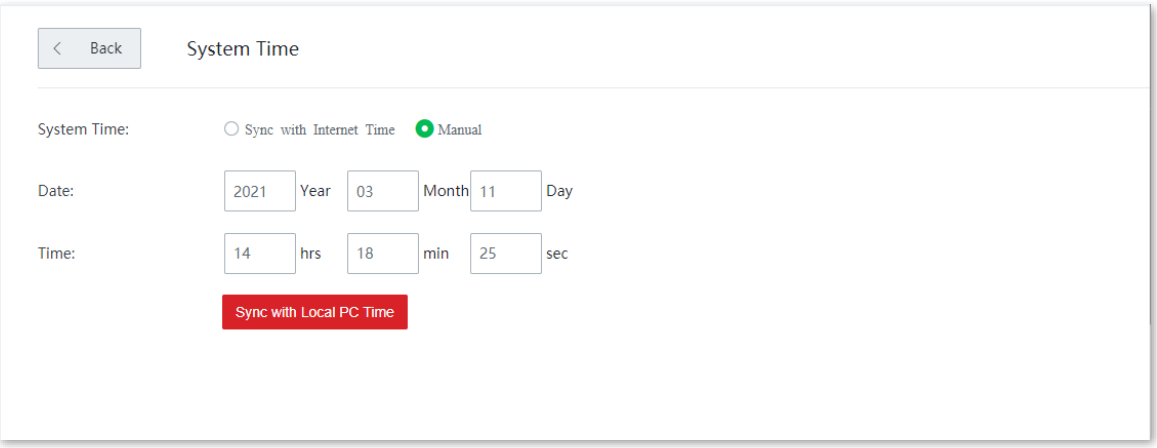
Time Zone: (GMT + 08: 00) Beijing, Chongqing, Hong Kong, Urumqi

Parameter description

Parameter	Description
System Time	It is used to choose the configuration method of the system time. The options include sync with internet time and manual.
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.

Manual

If you choose this method, you can manually specify a system time for the device. Every time the cable-free device reboots, you have to reconfigure the system time. The following displays the page when **Manual** is chosen.



Back

System Time

System Time: ○ Sync with Internet Time ● Manual

Date: 2021 Year 03 Month 11 Day

Time: 14 hrs 18 min 25 sec

Parameter description

Parameter	Description
System Time	It is used to choose the configuration method of the system time. The options include sync with internet time and manual.
Date	You can directly enter the correct time here. Or, you can click **Sync with Local PC Time** to synchronize the time of the cable-free device with that of the computer managing the cable-free device.
Time	

After the configuration, you can enter the System Status page to check whether the system time of the cable-free device is correct.

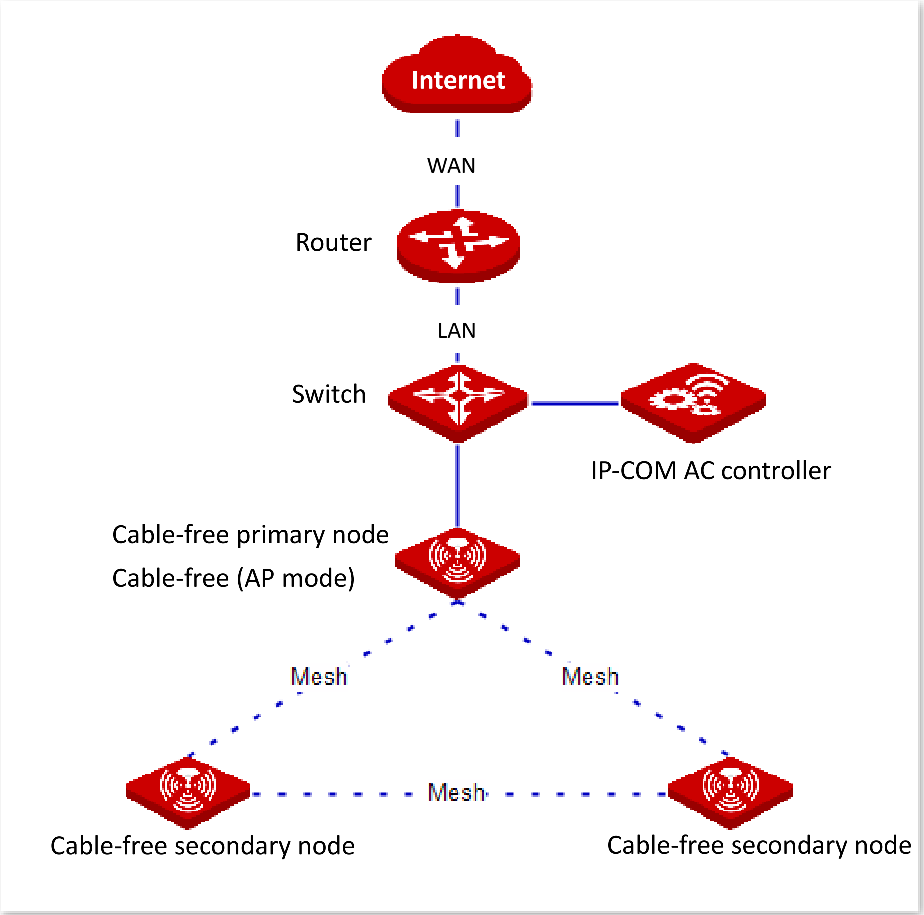
3.11.10 Function center

On this page, you can view the **Enabled Function** and **Disabled Function** of the cable-free device. You can enter the configuration page of a function after clicking it.

Click **Maintenance** > **Function Center** to enter the page.

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.



Tip

The **PoE WAN/LAN1** port of the cable-free AP mode node is a LAN port which connects to the upstream switch or router to connect to the internet.

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 the page.

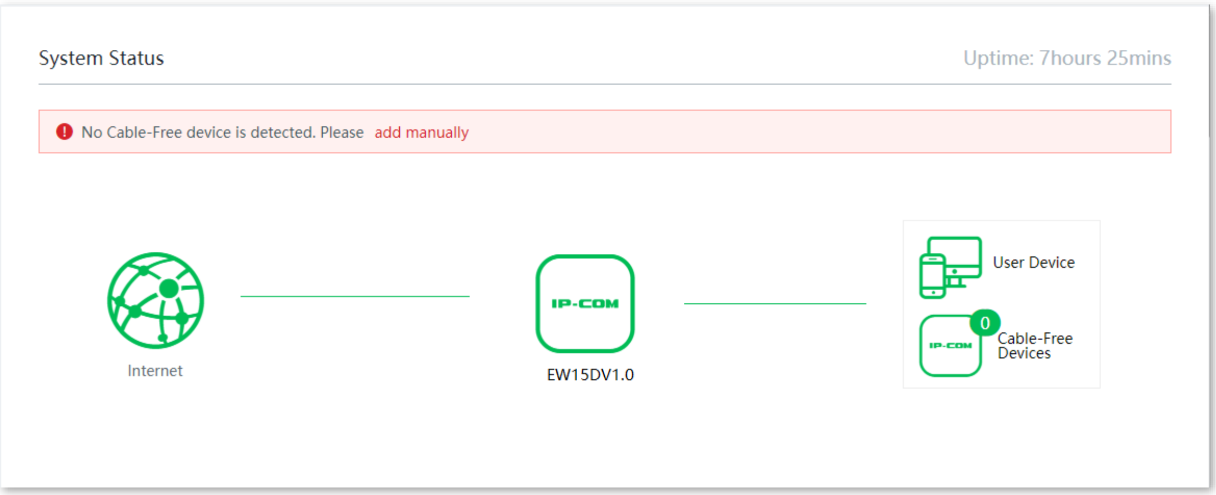
4.1.1 Add secondary node devices

The cable-free primary node can detect the secondary node devices in factory settings automatically. You can add cable-free secondary nodes as needed.

Add cable-free device:

If the system has already detected the new cable-free device, directly click **Details** on the **System Status** page to add the cable-free device. Otherwise, perform the following procedures:

1. On the **System Status** page, click **add manually**.

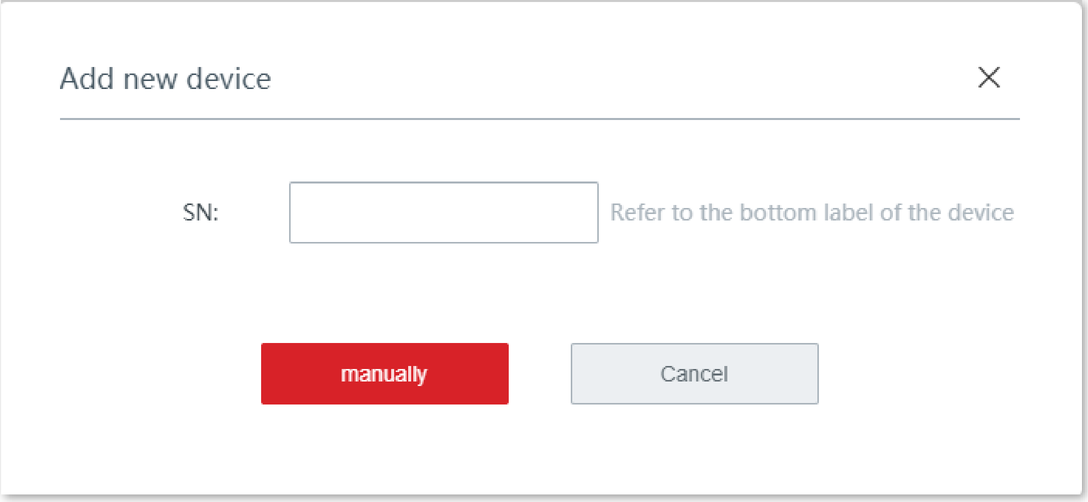


System Status

Uptime: 7hours 25mins

No Cable-Free device is detected. Please add manually

2. Enter the SN of the cable-free device to be added. You can find the SN on the product label of the device.
3. Click **manually**.



Add new device

SN: Refer to the bottom label of the device

----End

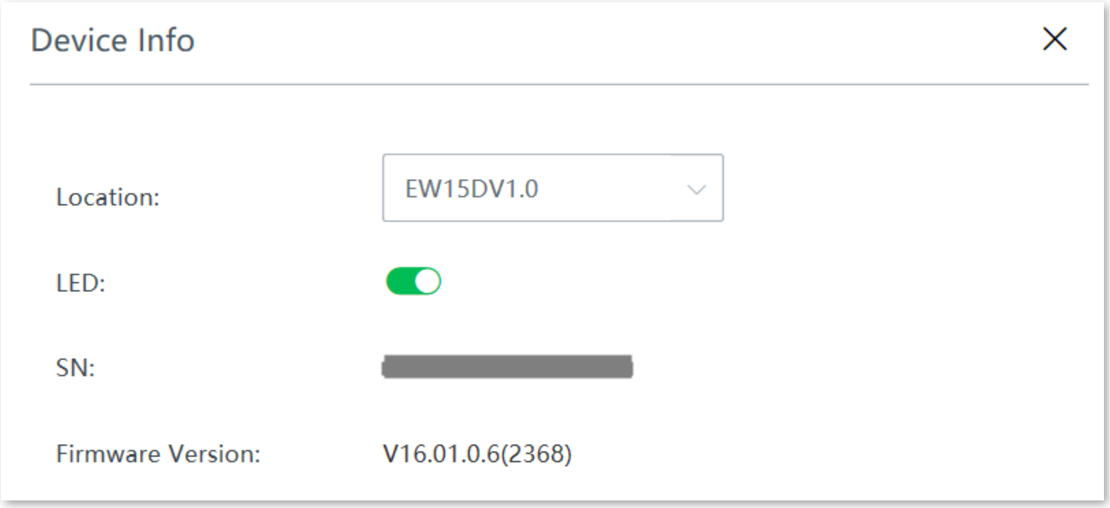
After the cable-free device is added successfully, you can click **Cable-Free Devices** on the right side of the **System Status** page to check the details of the device.

4.1.2 Check device info

Check the cable-free primary node info

On the **System Status** page, click the cable-free device directly connecting to the internet to enter the device info window. There, you can check the basic information of the cable-free primary node, operating status and LAN port status.

Device info



Device Info

Location: EW15DV1.0

LED: ●

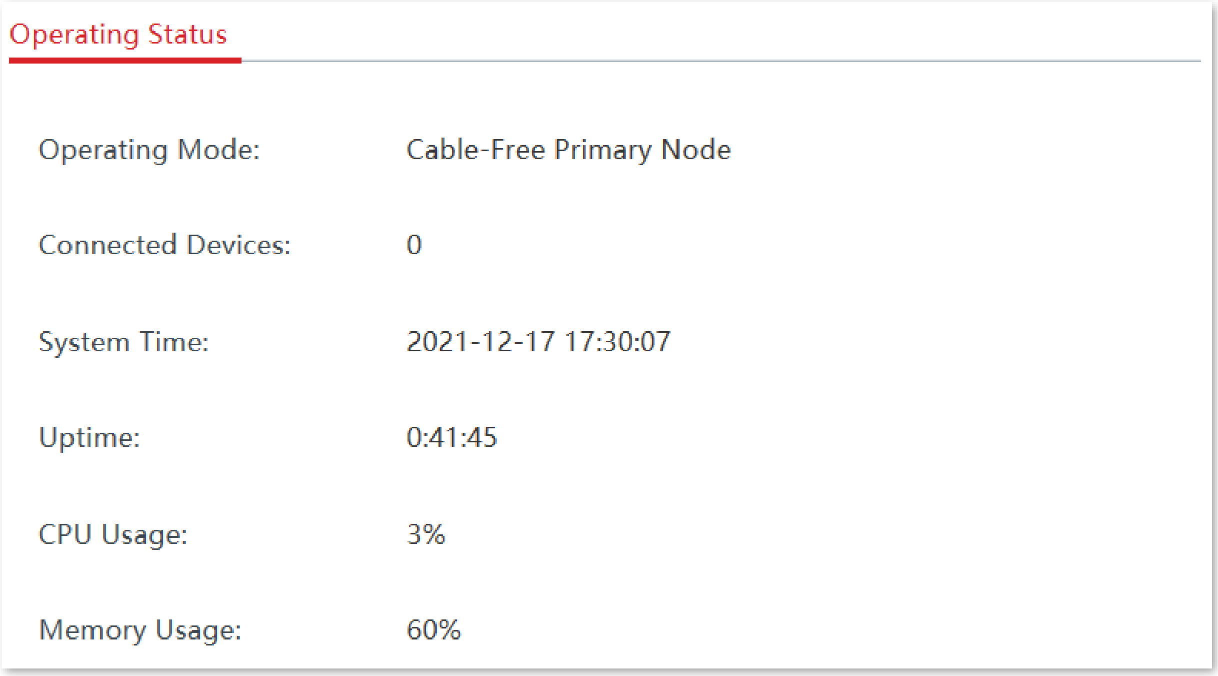
SN: [redacted]

Firmware Version: V16.01.0.6(2368)

Parameter description

Parameter	Description
Location	It specifies the location of the device. You are recommended to set this parameter to the description of the installation position of the node. In this way, you can rapidly locate the node when managing nodes.
LED	It specifies whether to turn on/off the LED indicator of the device. After you enabled the LED, you can judge the working status of the node by referring to the LED indicator. By default, the LED indicator is enabled.
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: 0

System Time: 2021-12-17 17:30:07

Uptime: 0:41:45

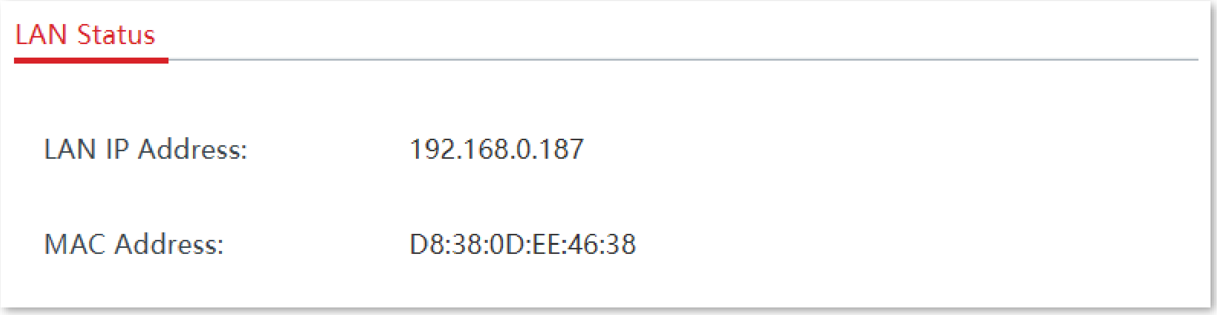
CPU Usage: 3%

Memory Usage: 60%

Parameter description

Parameter	Description
Operating Mode	It specifies the current working mode of the device. – Cable-Free Primary Node: The node serves as the primary node in the cable-free network and connects to the upstream wired network. The node is the only egress to the outer network, which realizes data transformation between the mesh network and wired network. – Cable-Free Node: The node serves as the secondary node in the cable-free network and through mesh, extends the coverage of the current cable-free network. Tip The **PoE WAN/LAN1** port of the cable-free secondary node is a LAN port.
Connected Devices	It specifies the number of devices connected to the device currently.
System Time	It specifies the current system time of the device.
Uptime	It specifies the time that has elapsed since the device started up the last time.
CPU Usage	It specifies the current CPU usage of the device.
Memory Usage	It specifies the current memory usage of the device.

LAN port status


LAN Status

LAN IP Address: 192.168.0.187

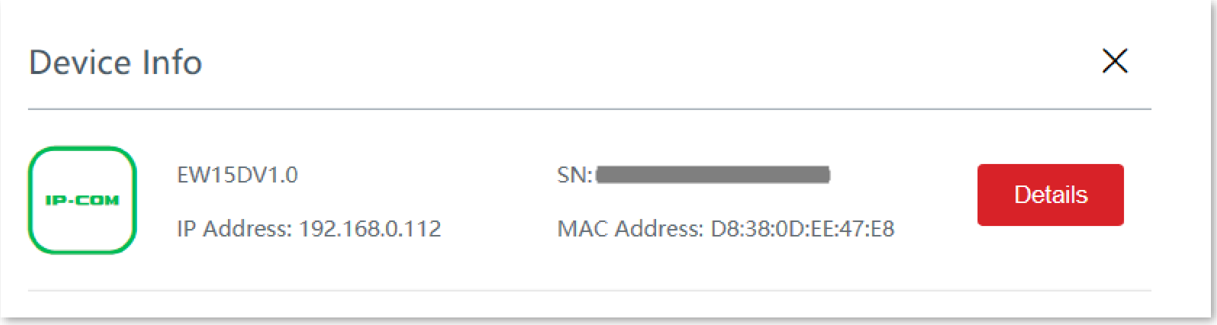
MAC Address: D8:38:0D:EE:46:38

Parameter description

Parameter	Description
LAN IP Address	It specifies the LAN IP address of the device which is also the management IP address of the device. LAN users can log in to the web UI of the device by visiting this IP address. The default LAN IP address of the primary node is 192.168.5.1. The LAN IP address of the secondary node is automatically obtained from the DHCP server at the LAN. Tip In the cable-free AP mode, if there is a DHCP server in the network, the node automatically obtains an IP address from the DHCP server. The next time you log in to the web UI of the node, you should check the IP address the node obtained at the client list of the DHCP server, and then use this IP address to log in.
MAC Address	It specifies the physical address of the LAN port of the device.

Check the cable-free secondary node info

On the **System Status** page, click the cable-free device near the user device to check the device info of the secondary node in the pop-up window.



Device Info

EW15DV1.0

SN: [redacted]

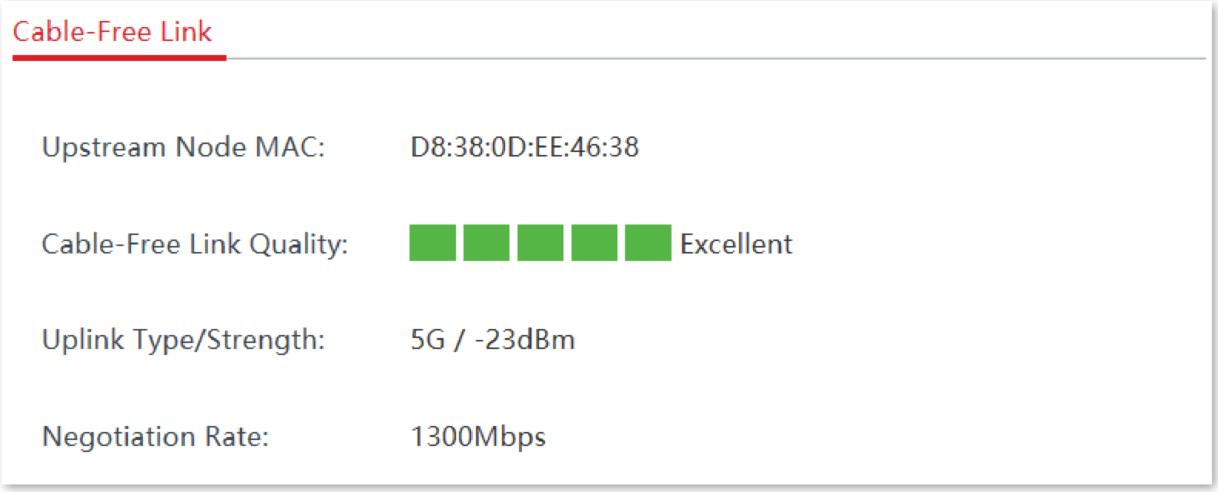
IP Address: 192.168.0.112

MAC Address: D8:38:0D:EE:47:E8

To learn more information, click **Details** to expand the details page.

On the details page, you can check or set the basic information of the node, check its operating status, LAN port status, cable-free link information, reboot or delete the node.

Cable-free link



Upstream Node MAC: D8:38:0D:EE:46:38

Cable-Free Link Quality: 🟩🟩🟩🟩🟩 Excellent

Uplink Type/Strength: 5G / -23dBm

Negotiation Rate: 1300Mbps

Parameter description

Parameter	Description
Upstream Node MAC	It specifies the physical address of the port the upstream node of the mesh link used to set up the mesh link.
Cable-Free Link Quality	It specifies the connection quality of the cable-free link between cable-free nodes.
Uplink Type/Strength	It specifies the type by which the node sets up a network with the upstream node and the strength of the signal the node receives from the upstream node.
Negotiation Rate	It specifies the rate at which the node negotiates with the upstream node.

Reboot the node

Click **Reboot** to reboot the node.

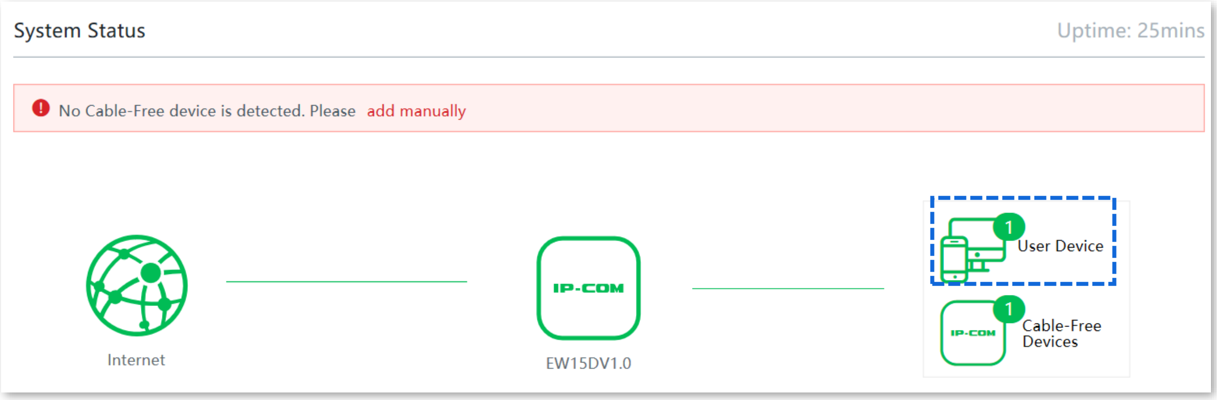
Delete the node

Click **Delete** to remove the node from the cable-free network. Removed nodes will be restored to factory settings.

4.1.3 Manage online devices

On this page, you can click **User Device** to check all the online clients.

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

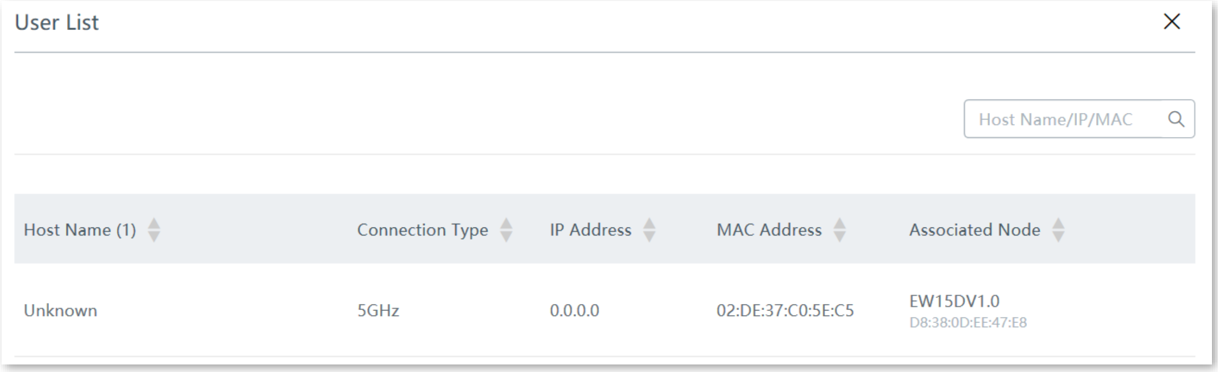


System Status

Uptime: 25mins

No Cable-Free device is detected. Please add manually

↓



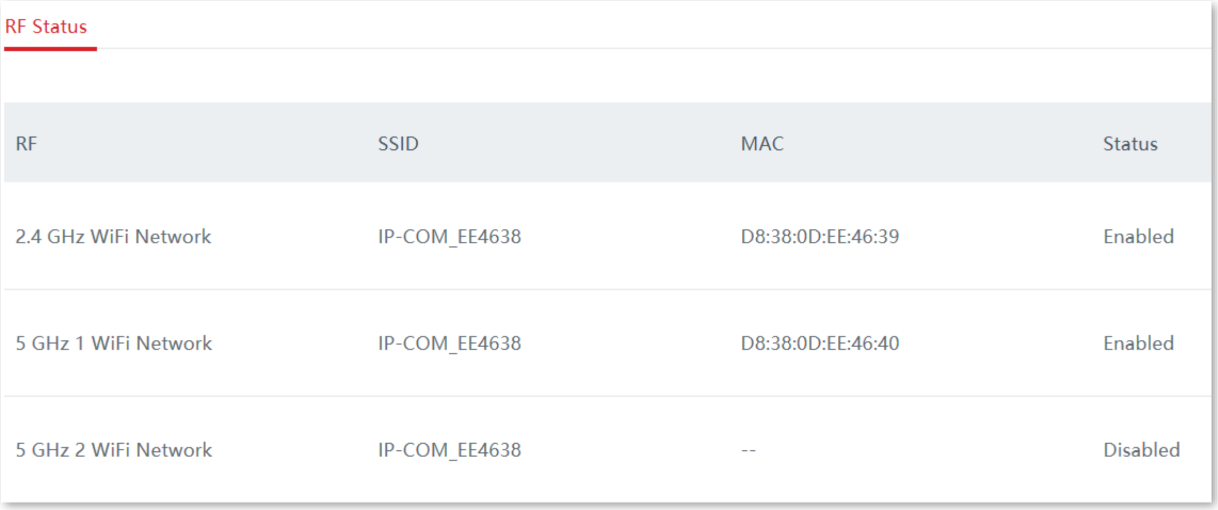
User List

Host Name/IP/MAC

Host Name (1)	Connection Type	IP Address	MAC Address	Associated Node
Unknown	5GHz	0.0.0.0	02:DE:37:C0:5E:C5	EW15DV1.0 D8:38:0D:EE:47:E8

4.1.4 Check the RF status

On the **RF Status** module of the **System Status** page, 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_EE4638	D8:38:0D:EE:46:39	Enabled
5 GHz 1 WiFi Network	IP-COM_EE4638	D8:38:0D:EE:46:40	Enabled
5 GHz 2 WiFi Network	IP-COM_EE4638	--	Disabled

4.2 Wireless

On this page, you can change the wireless configurations of the cable-free primary node.

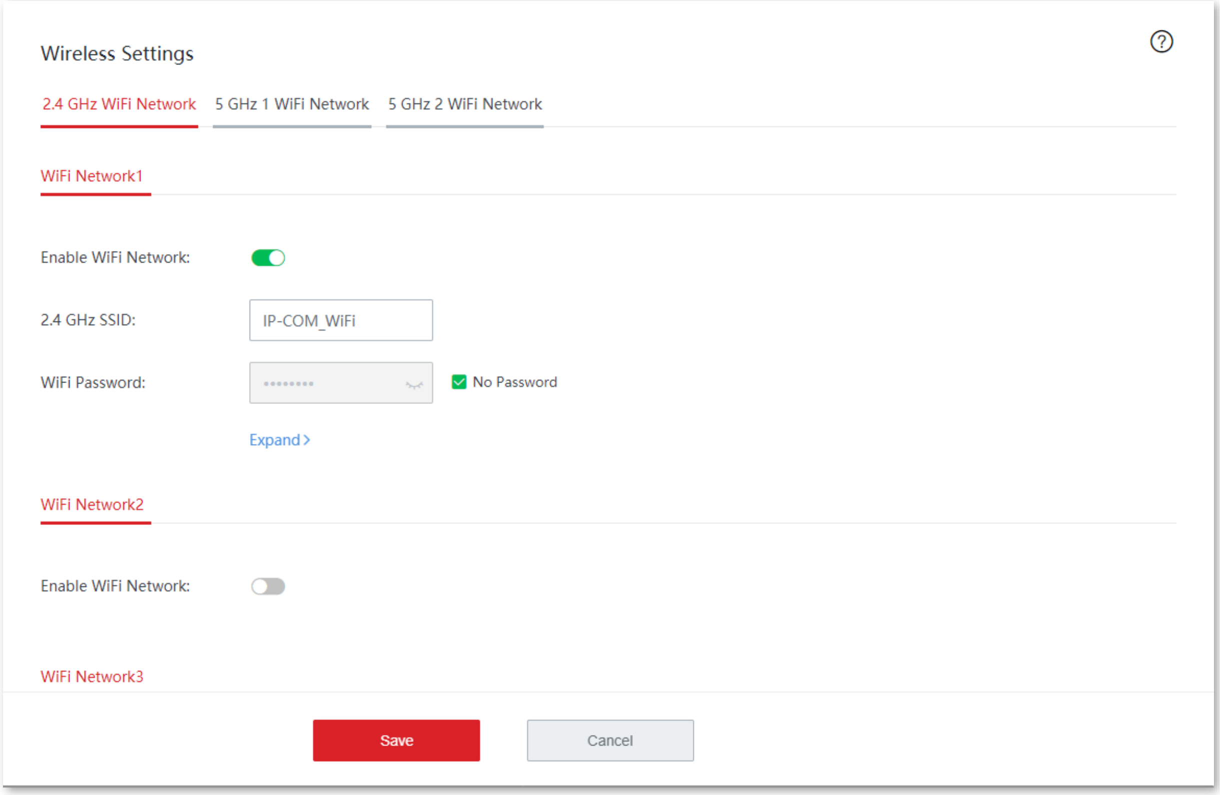
Tip

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

4.2.1 Wireless settings

On this page, you can configure the basic wireless parameters, including enable/disable WiFi networks, change the WiFi network name, set the WiFi password and other parameters.

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



Wireless Settings

WiFi Network1

Enable WiFi Network: ●

2.4 GHz SSID: IP-COM_WiFi

WiFi Password: •••••••• ☑ No Password

WiFi Network2

Enable WiFi Network: ○

WiFi Network3

Parameter description

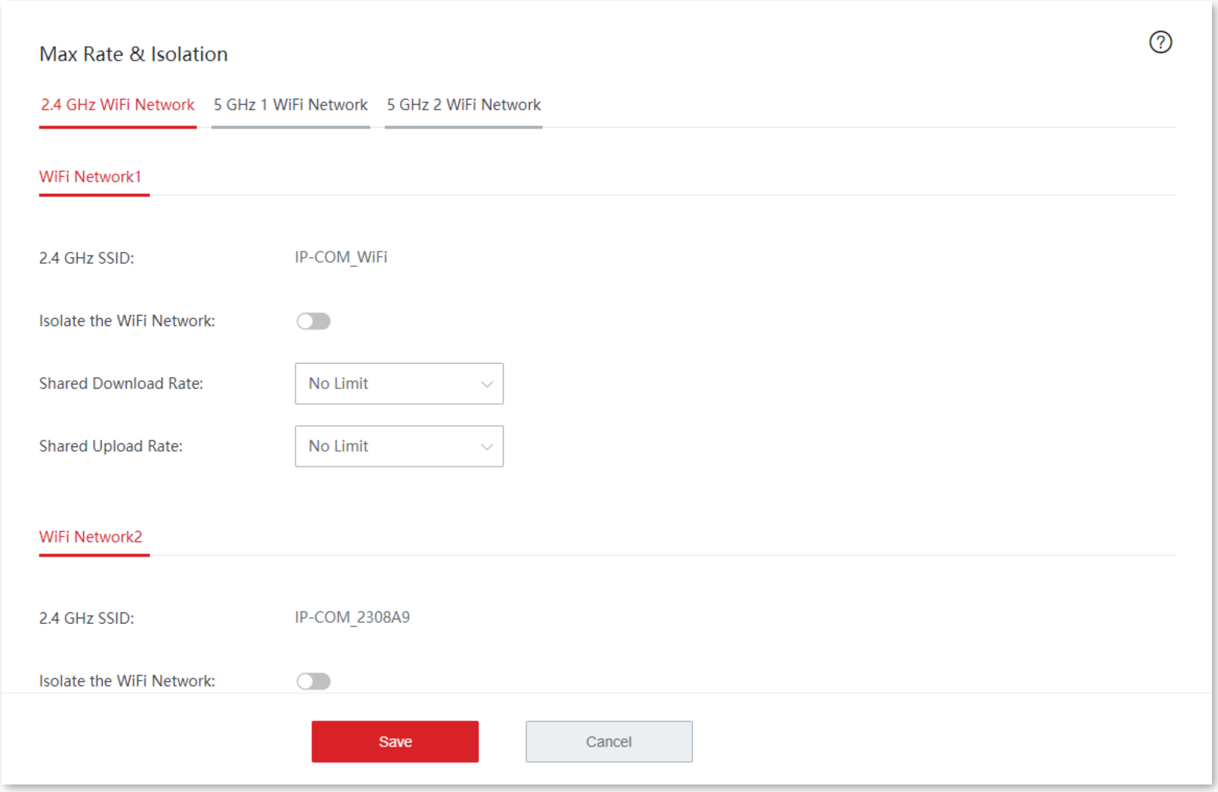
Parameter	Description
WiFi Network1/2/3/4	Every band of the node supports 4 WiFi networks and only WiFi network 1 is enabled by default.
Enable WiFi Network	It is used to enable/disable the corresponding WiFi network.
SSID	It specifies the WiFi network name of the corresponding WiFi network.

Parameter	Description
WiFi Password	It specifies the password of the corresponding WiFi network. For WiFi network security, it is strongly recommended that you set a WiFi password.
No Password	It specifies that no WiFi password is set. Under such circumstances, the corresponding WiFi network is open.
Hide SSID	After this function is enabled, the SSID will be hidden and will not appear in the available network list of clients (such as smartphones), which enhances the security of the WiFi network. If you want to connect to a hidden WiFi network, manually enter the SSID on your client.
Max. Clients	It specifies the maximum number of clients allowed to connect to the WiFi network. If this value is reached, new clients cannot connect to the WiFi network unless some clients are disconnected.

4.2.2 Max rate & isolation

On this page, you can configure the maximum rate and isolation. This function is disabled by default.

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



Max Rate & Isolation

WiFi Network1

2.4 GHz SSID: IP-COM_WiFi

Isolate the WiFi Network:

Shared Download Rate: No Limit

Shared Upload Rate: No Limit

WiFi Network2

2.4 GHz SSID: IP-COM_2308A9

Isolate the WiFi Network:

Parameter description

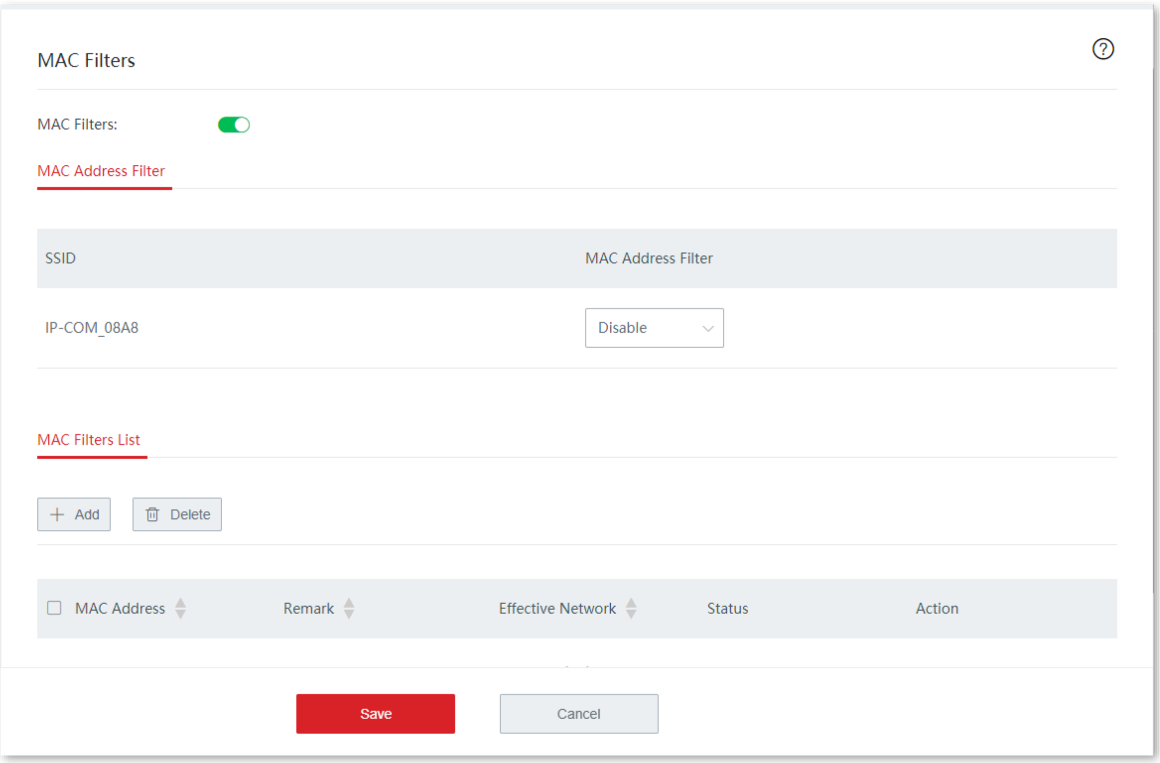
Parameter	Description
SSID	It specifies the WiFi network name of the node.
Isolate the WiFi Network	After this function is enabled, clients connected to this WiFi network cannot communicate with clients connected to other WiFi networks of the cable-free system, thus enhancing the security of WiFi networks.
Shared Upload/Download Rate	It specifies the maximum upload/download rate shared by clients connected to the WiFi network. **No Limit**: It indicates that to set no limit on the maximum upload/download rate of the WiFi network.

4.2.3 MAC filters

Overview

On this page, you can allow or forbid WiFi network access from specified clients by setting MAC filter rules. By default, this function is disabled.

Click **Wireless** > **MAC Filters** to enter the page. The following displays the page when the function is enabled.



MAC Filters

MAC Filters: ●

MAC Address Filter

SSID	MAC Address Filter
IP-COM_08A8	Disable

MAC Filters List

□ MAC Address	Remark	Effective Network	Status	Action

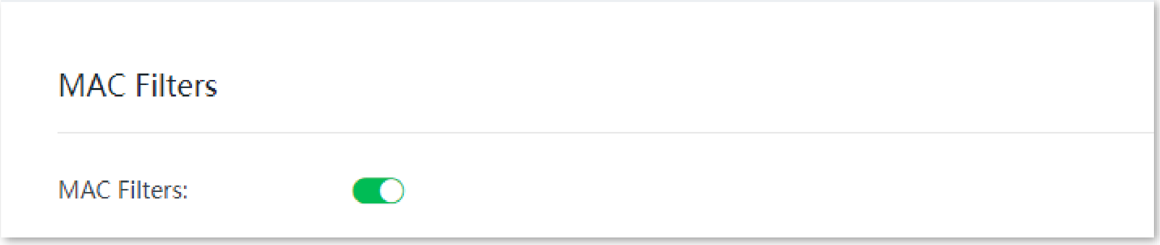
Parameter description

Parameter	Description	
MAC Filters	It specifies the status of the MAC filter function. ○ specifies the function is disabled and ● specifies the function is enabled.	
MAC Address Filter	SSID	It specifies the name of the enabled WiFi network of the node.
	MAC Address Filter	It specifies the MAC address filter mode. – **Disable**: It specifies that the MAC address filter function is not enabled on the WiFi network and all wireless clients are allowed to connect to the WiFi network. – **Only Allow**: It specifies that only the wireless clients in the **MAC Filters List** are allowed to connect to the WiFi network. – **Only Forbid**: It specifies that only the wireless clients in the **MAC Filters List** are forbidden to connect to the WiFi network. Other wireless clients can connect to the WiFi network.
MAC Filters List	MAC Address	It specifies the MAC address of the wireless client.
	Remark	It specifies the remarks of the MAC address.
	Effective Network	It specifies the WiFi network on which the rule takes effect.
	Status	It specifies the status of the rule. You can enable or disable the rule as required.
	Action	It specifies the operations you can perform on the rule. ✎: Click it to edit the rule. 🗑 : Click it to delete the rule.

Set a MAC filters rule

Enable the MAC filters function

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

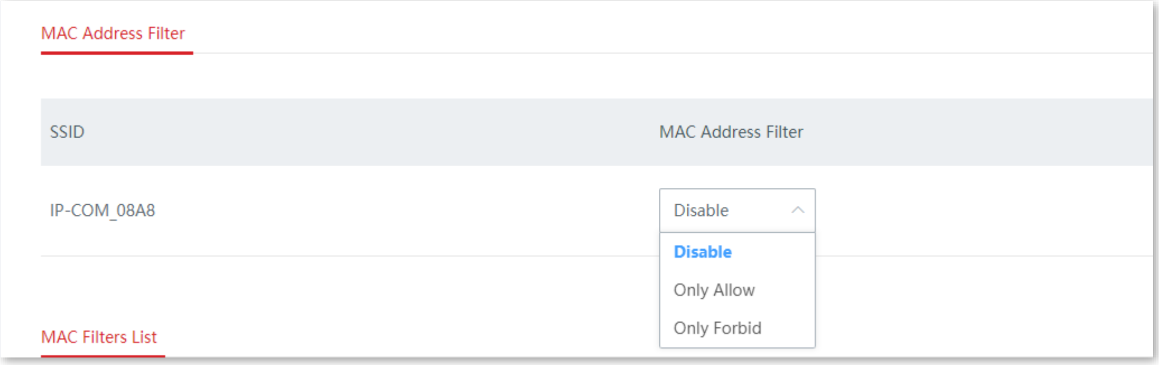


MAC Filters

MAC Filters: ●

Set MAC address filter mode

1. Click **Wireless** > **MAC Filters**.
2. Select the appropriate **MAC Address Filter** mode as required.
3. Click **Save**.



MAC Address Filter

SSID	MAC Address Filter
IP-COM_08A8	Disable

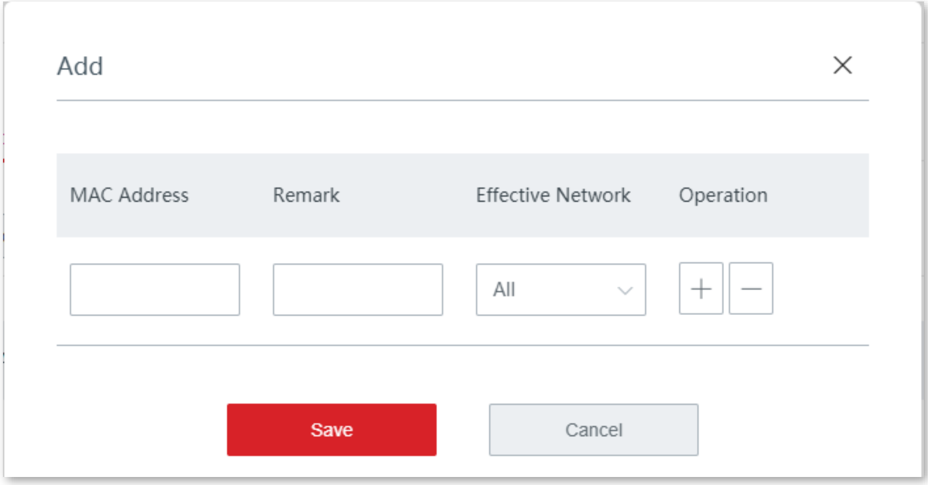
Add a MAC filter rule

1. On the **Wireless** > **MAC Filters** page, click **+ Add** to enter the configuration page.
2. Add a MAC filter rule.
   (1) Enter the MAC address of the wireless client on which the MAC filter rule applies.
   (2) (Optional) Set a remark for the MAC address.
   (3) Select a WiFi network on which the MAC filter rule takes effect.

Tip

Click + to add a MAC filter rule and click – to delete an unsaved MAC filter rule.

3. Click **Save**.



Add

MAC Address	Remark	Effective Network	Operation
		All	+ –

----End

You can check the newly added MAC filter rule on the **Wireless** > **MAC Filters** page.

Example of configuring MAC filters rule

Networking requirement

An enterprise uses cable-free devices to set up a network.

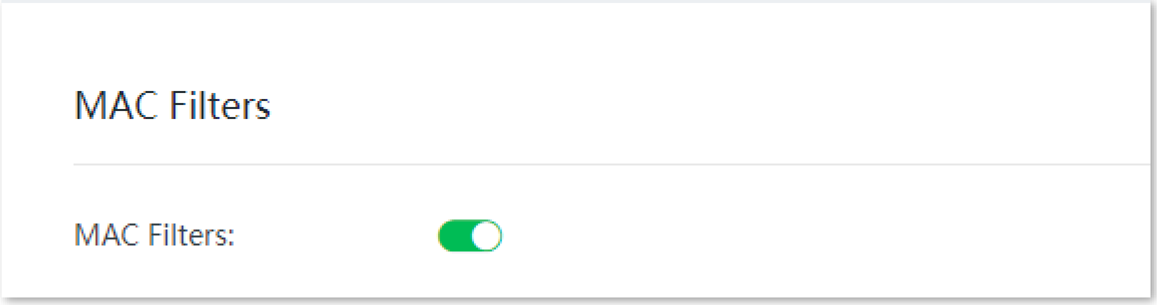
Requirement: Only a procurement personnel is allowed to connect to the WiFi network (Procurement) of the cable-free primary node for internet access.

Solution

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

Configuration procedures

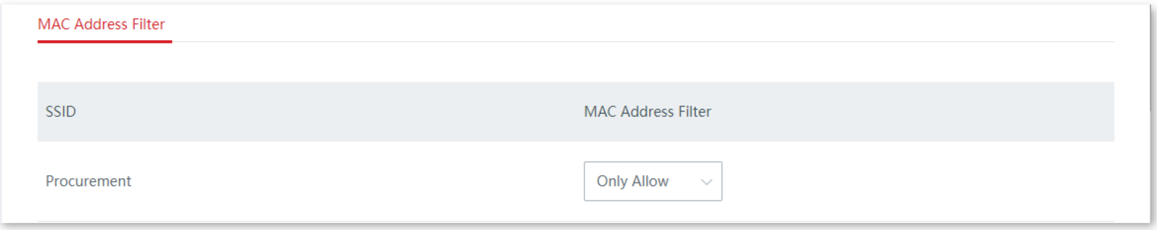
1. Click **Wireless** > **MAC Filters**.
2. Enable the MAC filters function.
   (1) Toggle on **MAC Filters**.
   (2) Click **Save**.



MAC Filters

MAC Filters: ●

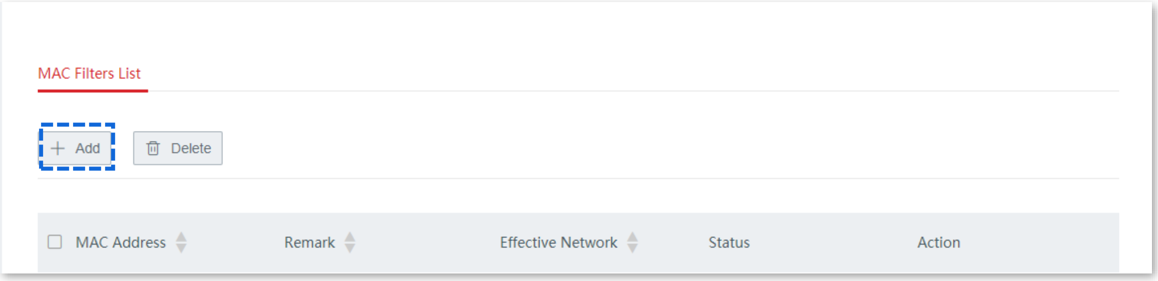
3. Set the MAC address filter mode.
   (1) Select a **MAC Address Filter** mode for the WiFi network "Procurement", which is "**Only Allow**" in this example.
   (2) Click **Save**.



MAC Address Filter

SSID	MAC Address Filter
Procurement	Only Allow

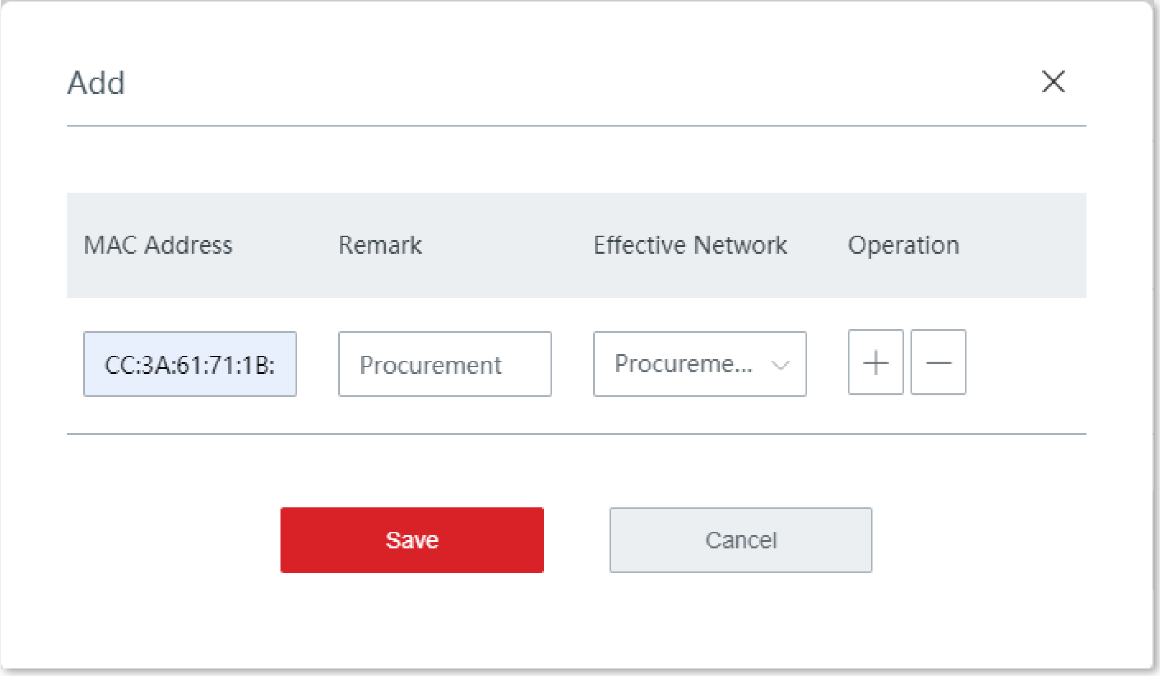
4. Add a MAC filter rule.
   (1) Click **+ Add**.



□ MAC Address	Remark	Effective Network	Status	Action

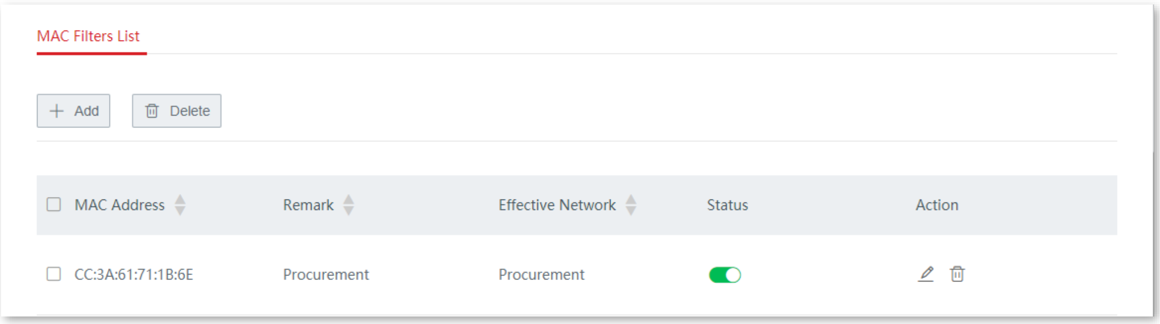
(2) Configure parameters in the **Add** window, and click **Save**.

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



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

The MAC filters rule is added successfully. See the following figure.



□ MAC Address	Remark	Effective Network	Status	Action
□ CC:3A:61:71:1B:6E	Procurement	Procurement	●	✎ 🗑

----End

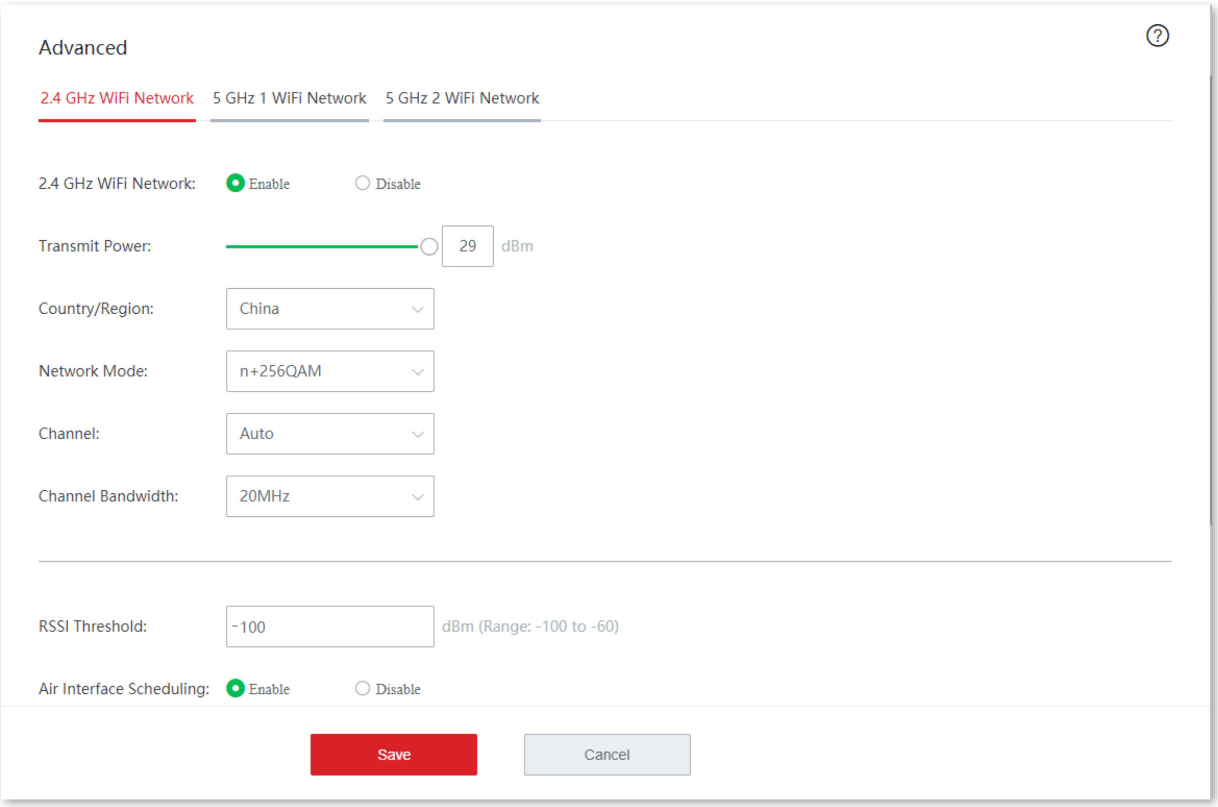
Verification

Only the above-mentioned wireless client can connect to the WiFi network “Procurement” while others are blocked.

4.2.4 Advanced

On this page, you can configure the advanced parameters such as transmit power, network mode, deployment mode, channel, channel bandwidth, and air interface scheduling.

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



Advanced

2.4 GHz WiFi Network: ● Enable ○ Disable

Transmit Power: 29 dBm

Country/Region: China

Network Mode: n+256QAM

Channel: Auto

Channel Bandwidth: 20MHz

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

Air Interface Scheduling: ● Enable ○ Disable

Parameter description

Parameter	Description
2.4 GHz/5 GHz WiFi Network	It specifies whether to enable the wireless function of the corresponding wireless band.
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.
Country/Region	It specifies the 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 of the corresponding band. Network modes of the 2.4 GHz WiFi network include 11b, 11g, 11b/g, 11b/g/n, and n+256QAM. By default, the router works in the n+256QAM mode. – **11b**: In this mode, only 802.11b wireless clients are allowed to access the 2.4 GHz WiFi network. – **11g**: In this mode, only 802.11g wireless clients are allowed to access the 2.4 GHz WiFi network. – **11b/g**: In this mode, 802.11b and 802.11g wireless clients can access the 2.4 GHz WiFi network. – **11b/g/n**: In this mode, wireless clients compliant with 802.11b or 802.11g and wireless clients working at 2.4 GHz and compliant with 802.11n can access the 2.4 GHz WiFi network. – **n+256QAM**: Wireless clients compliant with 802.11b or 802.11g and wireless clients working at 2.4 GHz and compliant with 802.11n can access the 2.4 GHz WiFi network. QAM, abbreviated for Quadrature Amplitude Modulation, is a modulation scheme that moderates amplitude on two orthogonal carriers. Using the orthogonality of sine wave and cosine wave, it moderates two signals at the same time, improving the modulation efficiency. In the n+256QAM network mode, the 256-QAM modulation mode compliant with the IEEE 802.11ac standard can be used under the IEEE 802.11n standard in the 2.4GHz band, which improves the single stream rate from 150 Mbps to 200 Mbps. Note: Such improvement can be realized only when the band is 2.4 GHz band, and the transmitting an d receiving ends both support the n+256QAM network mode. If any one end does not support n+256QAM, the single stream rate under the 2.4 GHz band is still 150 Mbps at most. Moreover, after the network mode is set to n+256QAM, the stability and anti-interference capability of the network will be reduced compared with the stability and anti-interference capability under other modes. Network modes of the 5 GHz WiFi network include 11a, 11ac, and 11a/n mixed. By default, the router works in the 11ac mode. – **11a**: In this mode, only 802.11a wireless clients are allowed to access the 5 GHz WiFi network. – **11ac**: In this mode, only 802.11ac wireless clients are allowed to access the 5 GHz WiFi network. – **11a/n mixed**: In this mode, wireless clients compliant with 802.11a and wireless clients working at 5 GHz and compliant with 802.11n can access the 5 GHz WiFi network.

Parameter	Description
Channel	It specifies the channel in which the wireless data is transmitted and received. The available channels are determined by the current country/region and wireless band. **Auto**: The node automatically detects the occupation rate of channels and selects the appropriate working channel accordingly. If connection drop, freeze or slow internet occurs frequently when you are using the WiFi network, you can try changing the working channel. You can check the channels with low occupation rate and little interference using software tools (such as WiFi analyzer).
Channel Bandwidth	It specifies the bandwidth of the working channel. A high channel bandwidth means a higher transmission rate, but the penetration capability is reduced and the transmission distance is shortened. – **20MHz**: The node uses the 20MHz channel bandwidth. – **40MHz**: The node uses the 40MHz channel bandwidth. – **20MHz/40MHz**: This channel bandwidth is available only for the 2.4 GHz only. The node automatically adjusts the channel bandwidth to 20MHz or 40MHz based on the surrounding environment. – **80MHz**: This channel bandwidth is available only for the 5 GHz only. The node uses the 80MHz channel bandwidth.
RSSI Threshold	It specifies the minimum wireless signal strength can be received by the band. Clients with a lower signal strength value cannot connect to the node. When there are multiple nodes in the surroundings, an appropriate RSSI value helps ensure wireless clients connects to the nodes with a stronger signal.
Air Interface Scheduling	After this function is enabled, the node fairly allocates download transmission time to clients, which guarantees that high-speed clients and low-speed clients obtain the same download transmission time. In this way, high-speed clients can transmit more data, achieving higher system throughput and a larger number of accessed clients.
APSD	It is abbreviated for Automatic Power Save Delivery, which is the WMM power-saving certification protocol of the WiFi Alliance. This parameter is available only for the 5 GHz WiFi network. Enabling APSD can reduce the power consumption of the node. By default, this function is enabled.
Short GI	It specifies short guard interval for preventing data block interference. This parameter is available only for the 2.4 GHz WiFi network. When wireless signal is transmitted in space, delays may occur on the receiving end due to multipath and other factors. If the succeeding data block is transmitted too fast, it will cause interference to the preceding data block, and short GI can be used to avoid this interference. When short GI is enabled, wireless throughput is improved.

Parameter	Description
Deployment Mode	Choose a deployment mode based on the deployment intensity of nodes. – **Capacity-oriented**: This deployment mode is generally used in scenarios where nodes are deployed intensively, such as meeting hall, exhibition hall, banquet hall, gym, university classroom, and airport. This mode can effectively reduce interferences between nodes. – **Coverage-oriented**: This deployment mode is generally used in scenarios where nodes are deployed loosely, such as office, warehouse, and hospital. This mode can expand the coverage of nodes.
Client Timeout Interval	If a client generates no data communication within this interval after connecting to the WiFi network, the node will cut this client off.
Mandatory Rate	By adjusting the mandatory rate and optional rate, you can limit access from low-speed clients, thus improving the internet experience of other clients. – **Mandatory Rate**: It is a group of mandatory rates of the node. Clients must support these mandatory rates; otherwise, the clients will fail to access the WiFi network. – **Optional Rate**: It is a collection of other rates supported by the node except for mandatory rates. These optional rates help clients realize connection with the node at a higher rate.
Optional Rate	

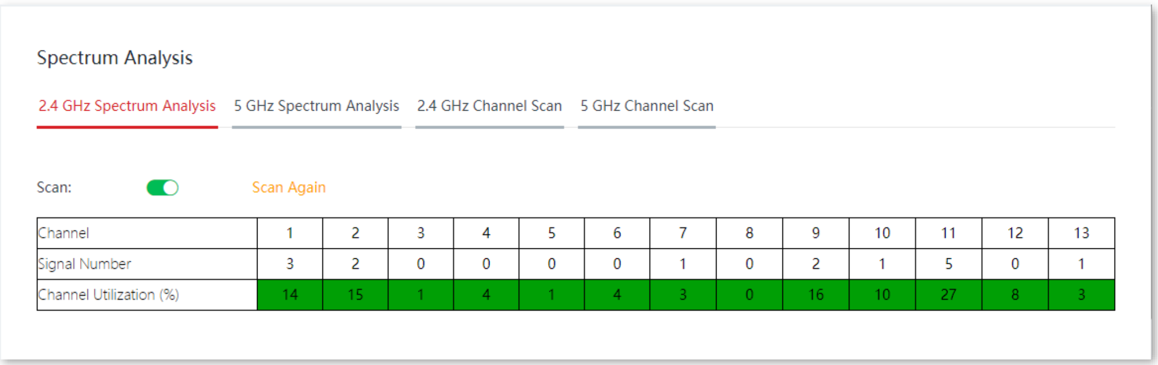
4.2.5 Spectrum analysis

Specturm analysis

On this page, 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.

Click **Wireless** > **Spectrum Analysis** > **Spectrum Analysis** to enter the page.

The following figure takes the 2.4 GHz band for illustration.



Scan: ●

Channel	1	2	3	4	5	6	7	8	9	10	11	12	13
Signal Number	3	2	0	0	0	0	1	0	2	1	5	0	1
Channel Utilization (%)	14	15	1	4	1	4	3	0	16	10	27	8	3

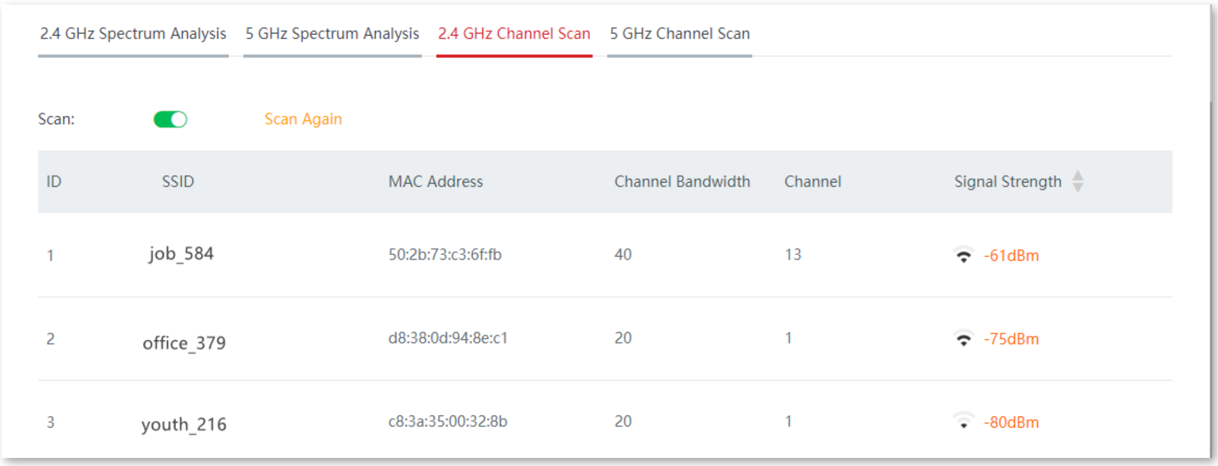
- A channel utilization under green paint indicates an idle channel.
- A channel utilization under yellow paint indicates a crowded channel.
- A channel utilization under red paint indicates an extremely crowded and unavailable channel.

Channel scan

On this page, you can check the basic information of other WiFi networks in the ambient environment, such as the WiFi network name, MAC address, channel bandwidth, signal strength, and other information.

Click **Wireless** > **Spectrum Analysis** > **Channel Scan** to enter the page.

The following figure takes the 2.4 GHz band for illustration.

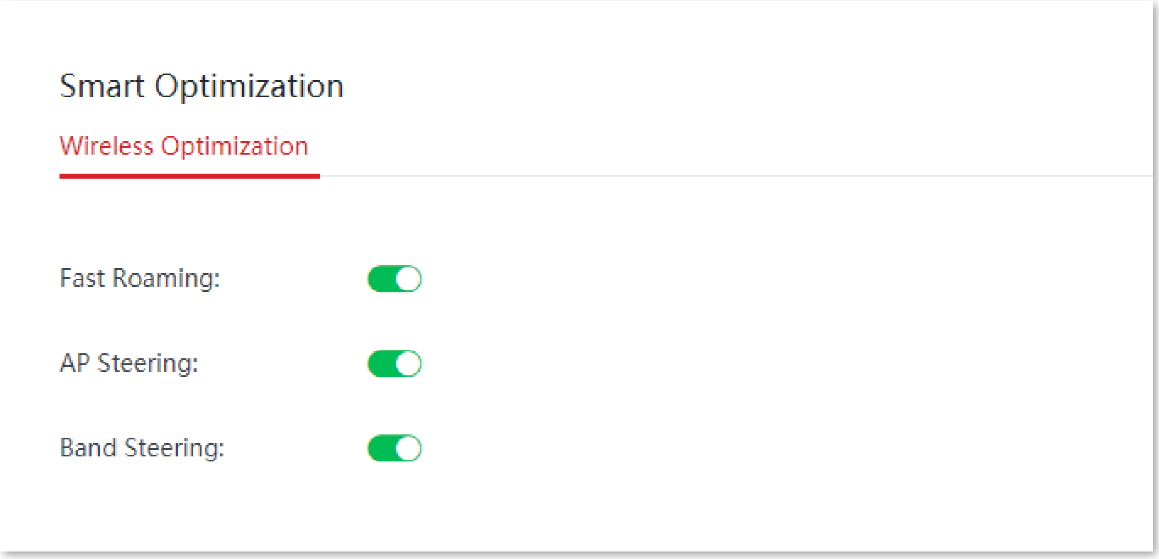


ID	SSID	MAC Address	Channel Bandwidth	Channel	Signal Strength
1	job_584	50:2b:73:c3:6f:fb	40	13	-61dBm
2	office_379	d8:38:0d:94:8e:c1	20	1	-75dBm
3	youth_216	c8:3a:35:00:32:8b	20	1	-80dBm

4.3 Smart optimization

On this page, you can optimize the entire cable-free network to enjoy a better user experience. Click **Smart Optimization** to enter the page.

On this page, you can optimize the WiFi experience of the cable-free system by adjusting the status of fast roaming, AP steering, and band steering.



Smart Optimization

Fast Roaming: ●

AP Steering: ●

Band Steering: ●

Parameter description

Parameter	Description
Fast Roaming	After this function is enabled, clients with 802.11r capabilities are automatically switched to other nodes if the WiFi signal they received from the current node decreases to the threshold value for triggering fast roaming. This process takes only milliseconds. Enabling this function to minimize the effects on services when users are moving across nodes. Note: This function requires that all nodes share the same SSID and WiFi password.
AP Steering	After this function is enabled, clients with 802.11k and 802.11v capabilities can obtain the network information of all the nodes and decide whether to switch to other nodes with better network quality accordingly. Enabling this function to disperse clients and ensure that clients connect to more appropriate nodes. Note: This function requires that all nodes share the same SSID and WiFi password.
Band Steering	After this function is enabled, the node will guide dual-band clients to connect to the frequency band with the better network quality based on the network quality of all frequency bands. Note: This function requires that the 2.4 GHz frequency band and the 5 GHz frequency band of the node share the same SSID and WiFi password.

4.4 More

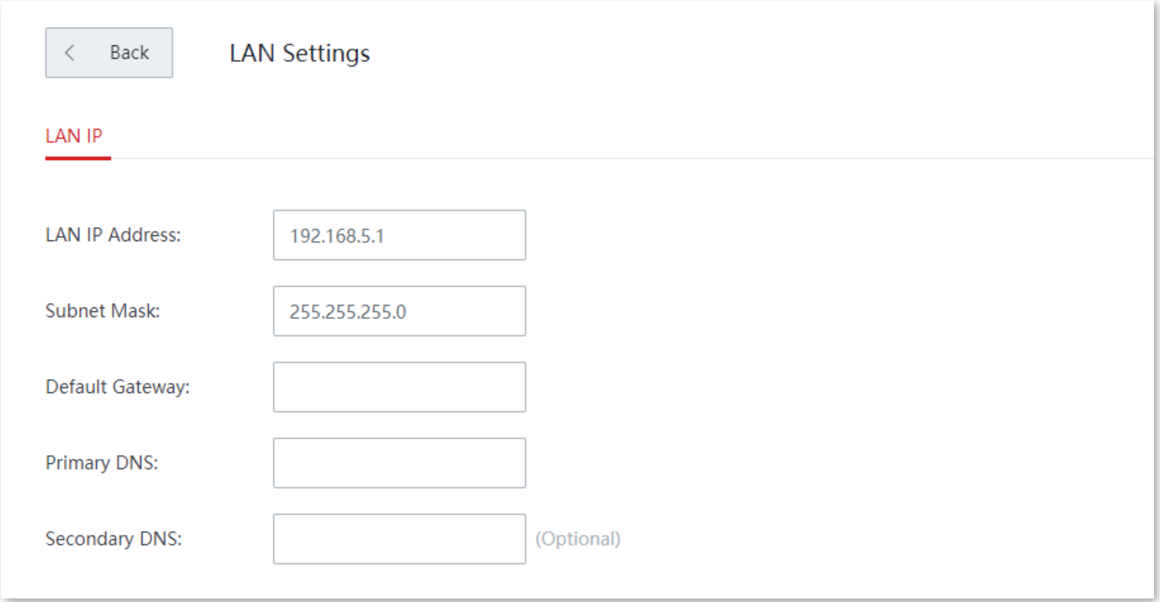
4.4.1 LAN settings

On this page, you can set the LAN IP address and the DHCP server.

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

LAN settings

The LAN IP address is the IP address of the LAN of the node, which is also the management IP address of the node. By default, the LAN IP address is 192.168.5.1 and the subnet mask is 255.255.255.0.



LAN IP Address: 192.168.5.1

Subnet Mask: 255.255.255.0

Default Gateway:

Primary DNS:

Secondary DNS: (Optional)

Generally, you do not need to change the LAN settings unless IP address conflict occurs, for example, the IP address of another device in the LAN is also 192.168.5.1.

After the LAN IP address is changed successfully, you will be redirected to the login page. If you are not redirected, verify that the IP address of the management computer and the new LAN IP address are on the same network segment, and visit the new LAN IP address to try again.

Parameter description

Parameter	Description
LAN IP Address	It specifies the IP address of the LAN port of the device, which is also the management IP address of the device. LAN users can log in to the web UI of the

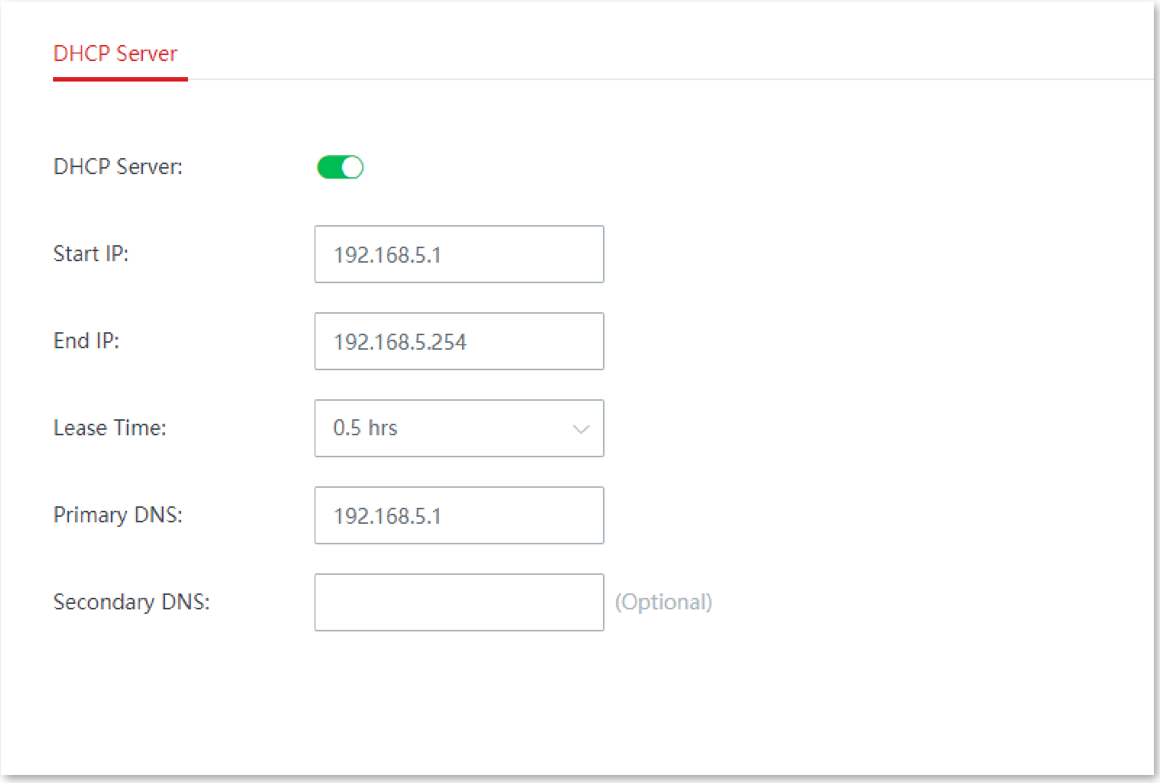
Parameter	Description
	device by visiting this IP address.
Subnet Mask	It specifies the subnet mask of the device, which is 255.255.255.0 by default. It is used to define the address space of the network segment.
Default Gateway	It specifies the default gateway of the device. If the device needs to connect to the internet, the default gateway is generally set to the LAN IP address of the exit router.
Primary DNS	It specifies the primary DNS server address of the device. If the exit router has DNS proxy function, enter the LAN port IP address of the exit router here. Otherwise, enter the IP address of the correct DNS server.
Secondary DNS	It specifies the secondary DNS server address of the device. This parameter is optional. 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.

In the **Cable-Free (AP Mode),** the DHCP server is disabled by default.

The following displays the page when DHCP server is enabled.



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)

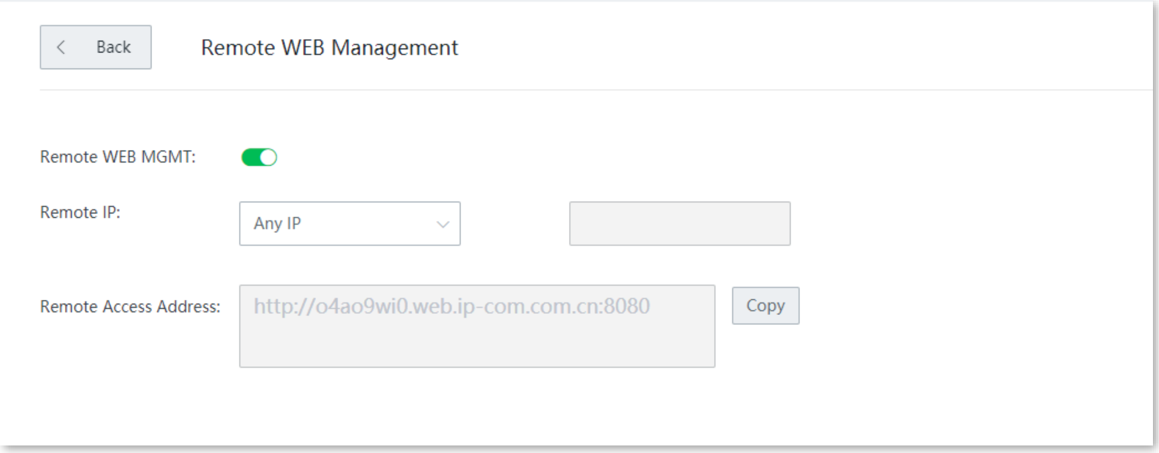
Parameter description

Parameter	Description
DHCP Server	It specifies whether to enable the DHCP server function. ○ indicates the function is disabled and ● indicates the function is enabled.
Start IP	It specifies the range of IP addresses that the 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 After the LAN IP address is changed, if the new LAN IP address and the previous LAN IP address are not in the same network segment, the system will automatically match and modify the DHCP address pool to make the address pool in the same network segment with the new LAN IP address.
End IP	
Lease Time	It specifies the validity period of the IP address assigned by the DHCP server to LAN devices. By default, the time is 30 minutes. When the IP address expires: – If the device is still connected to the 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 this IP address to other devices. You are recommended to keep the default settings unless in special circumstances.
Primary DNS	It specifies the primary DNS server IP address assigned by the DHCP server to LAN devices. By default, the primary DNS server address is the LAN IP address of the device. Tip If you enabled the DHCP server, to ensure LAN devices can access the internet properly, please make sure that the primary DNS you set is the correct DNS server address or DNS proxy IP address.
Secondary DNS	It specifies the secondary DNS server IP address assigned by the DHCP server to LAN devices. If this parameter is left blank, the DHCP server does not assign the secondary DNS server IP address.

4.4.2 Remote WEB management

In general, only the devices which are connected to the node’s LAN port or WiFi network can log in to the node's web UI. However, the remote web management function enables you to access the web UI of the node remotely through the Internet when you have special requirements (such as remote technical support). By default, this function is disabled.

Click **More** > **Remote WEB Management** to enter the page. The following displays the page when the function is enabled.



Remote WEB MGMT: ●

Remote IP: Any IP

Remote Access Address: http://o4ao9wi0.web.ip-com.com.cn:8080

Parameter description

Parameter	Description
Remote WEB MGMT	It specifies whether to enable the remote web management function. ○ indicates the function is disabled and ● indicates the function is enabled.
Remote IP	It specifies the IP address of the device that can remotely access the web UI of the router. – Any IP: It specifies that any devices with any IP addresses on the internet can access the web UI of the cable-free (AP mode) node. For network security, this option is not recommended. – Specified IP: It specifies that only the device with the specified IP address can remotely access the web UI of the cable-free (AP mode) node. If the device is in a LAN, enter the IP address of its gateway (public IP address).
Remote Access Address	It specifies the domain name used to remotely manage the cable-free (AP mode) node. After you enabled the remote web management function, internet users can visit this domain name to log in to the web UI of the cable-free (AP mode) node.

4.4.3 QVLAN

Overview

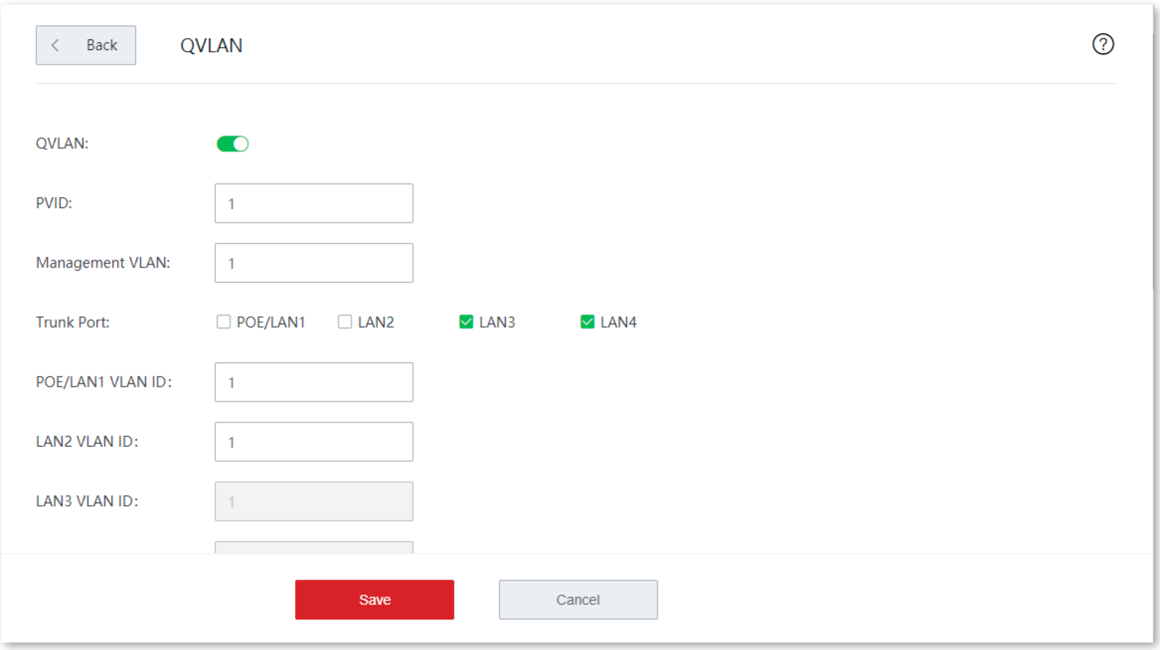
The cable-free (AP mode) nodes support IEEE 802.1q VLAN and can be used in network environments where QVLANs are partitioned. By default, the QVLAN function is disabled.

After the QVLAN function is enabled, the Tag data is forwarded to other ports in the corresponding VLAN according to the VID. The Untag data is forwarded to other ports in the corresponding VLAN according to the PVID. Refer to the following table for how different link ports receive and transmit data.

Link type	Receiving data		Transmitting data
	Receiving Tag data	Receiving Untag data	
Access	Forward the Tag data to other port in the corresponding VLAN according to the VID.	Forward the Tag data to other port in the corresponding VLAN according to the PVID.	Transmit it after removing the Tag from the message.
Trunk			VID = port PVID, remove the Tag and transmit the data. VID ≠ port PVID, keep the Tag and transmit the data.

Configure QVLAN

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



QVLAN: ●

PVID: 1

Management VLAN: 1

Trunk Port: □ POE/LAN1 □ LAN2 ☑ LAN3 ☑ LAN4

POE/LAN1 VLAN ID: 1

LAN2 VLAN ID: 1

LAN3 VLAN ID: 1

Parameter description

Parameter	Description
QVLAN	It specifies whether to enable the QVLAN function. ○ indicates the function is disabled and ● indicates the function is enabled.
PVID	It specifies the ID of the VLAN to which the trunk port belongs by default, which is **1** here.
Management VLAN	It specifies the management VLAN ID of the node. The default value is **1** here. After the management VLAN is modified, the management computer can manage the node only after re-connecting to the new management VLAN.
Trunk Port	Choose the Ethernet port (wired LAN port) serving as the trunk port of the node. The trunk port allows all VLANs to pass through. Note When you enable the QVLAN function, choose at least one LAN port to serve as the trunk port. If the node has only one Ethernet port, this Ethernet port serves as the trunk port by default.
PoE/LAN1 VLAN ID	If the Ethernet port is not set as the trunk port, it serves as an access port and its VLAN ID can be set here.
LAN2 VLAN ID	
LAN3 VLAN ID	
LAN4 VLAN ID	
VLAN ID	It specifies the WiFi network currently enabled on the 2.4 GHz/5 GHz band of the node, and the VLAN of the WiFi network. Tip After you enabled VLAN, the WiFi network serves as an access port and its PVID is the same with VLAN ID.

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 hotel has the following requirements:

- 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.

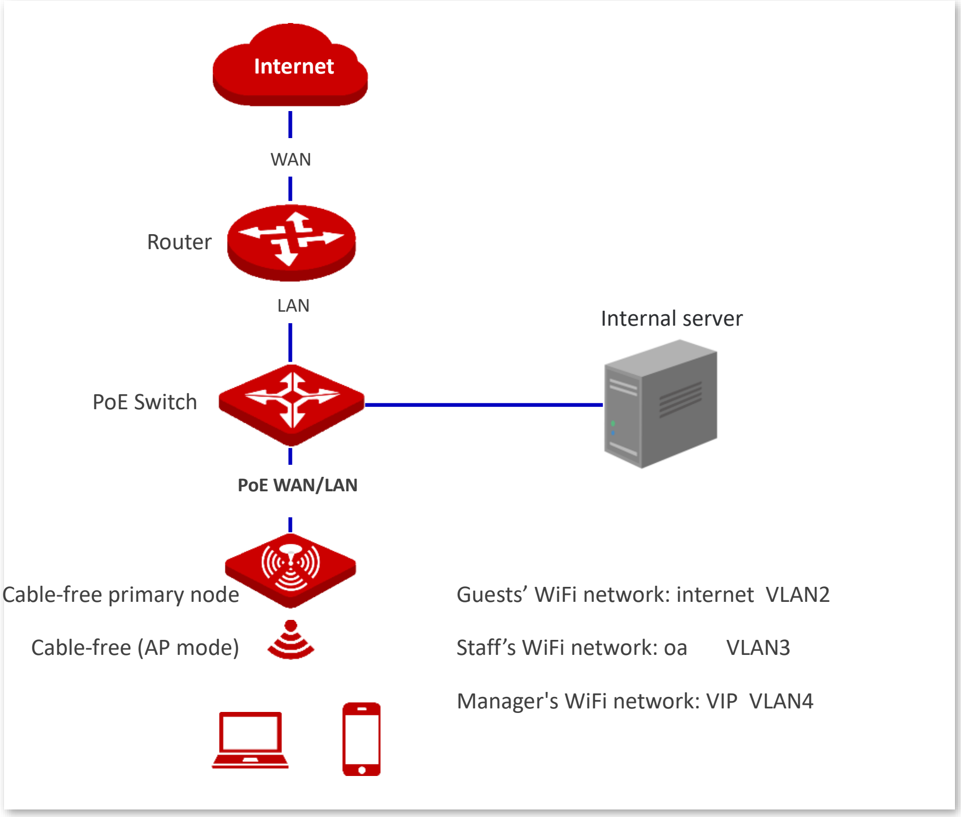
- Hotel managers can access both the internet and the intranet when they are connected to the WiFi network.

Solution

Assign different WiFi networks for guests, staff and managers, and use VLAN to give all users their own access rights.

Assume that:

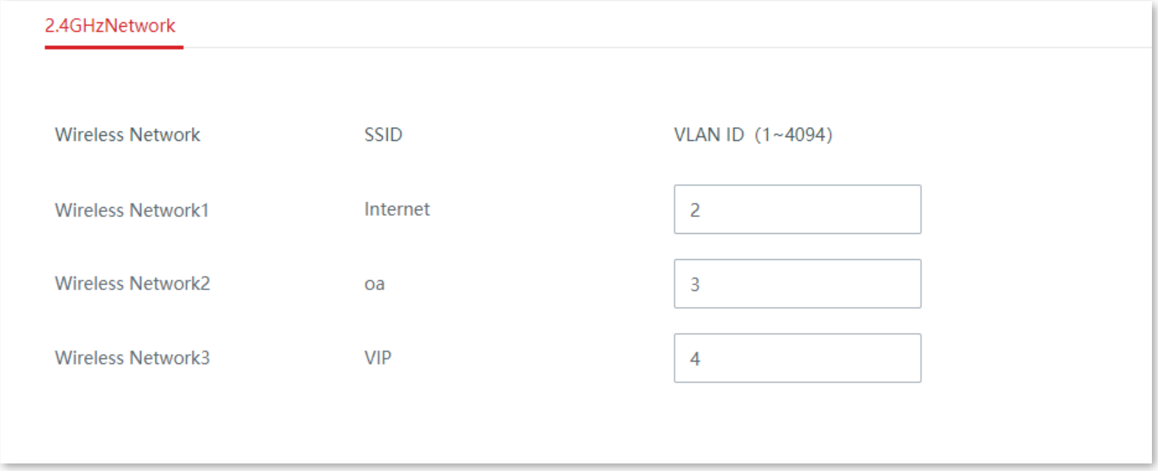
- The 2.4 GHz band is used to deploy WiFi networks.
- The WiFi network for guests is **Internet** and belongs to VLAN 2.
- The WiFi network for staff is **oa** and belongs to VLAN 3.
- The WiFi network for managers is **VIP** and belongs to VLAN 4.


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

Configuration procedures

I. Configure cable-free device.

1. Log into the web UI of cable-free device, click **More** > **QVLAN**.
2. Toggle on **QVLAN**.
3. Modify the VLAN ID of each WiFi network on the 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**.



Wireless Network	SSID	VLAN ID (1~4094)
Wireless Network1	Internet	2
Wireless Network2	oa	3
Wireless Network3	VIP	4

II. Configure the switch.

Deploy IEEE 802.1q VLAN on the switch. See the following table.

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

Keep default settings for other unmentioned ports. Refer to the user guide of switch for detailed configurations.

III. Configure the router and internal server.

To ensure that wireless clients connected to the cable-free device can access the internet properly, the router and the internal server should support QVLAN and have QVLAN configured. See the following table.

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

Refer to the user guide of the target device for detailed configurations.

----End

Verication

Users connected to **Internet** can only access the internet, users connected to **oa** can only access the intranet, and users connected to **VIP** can access both the internet and the intranet.

4.5 Maintenance

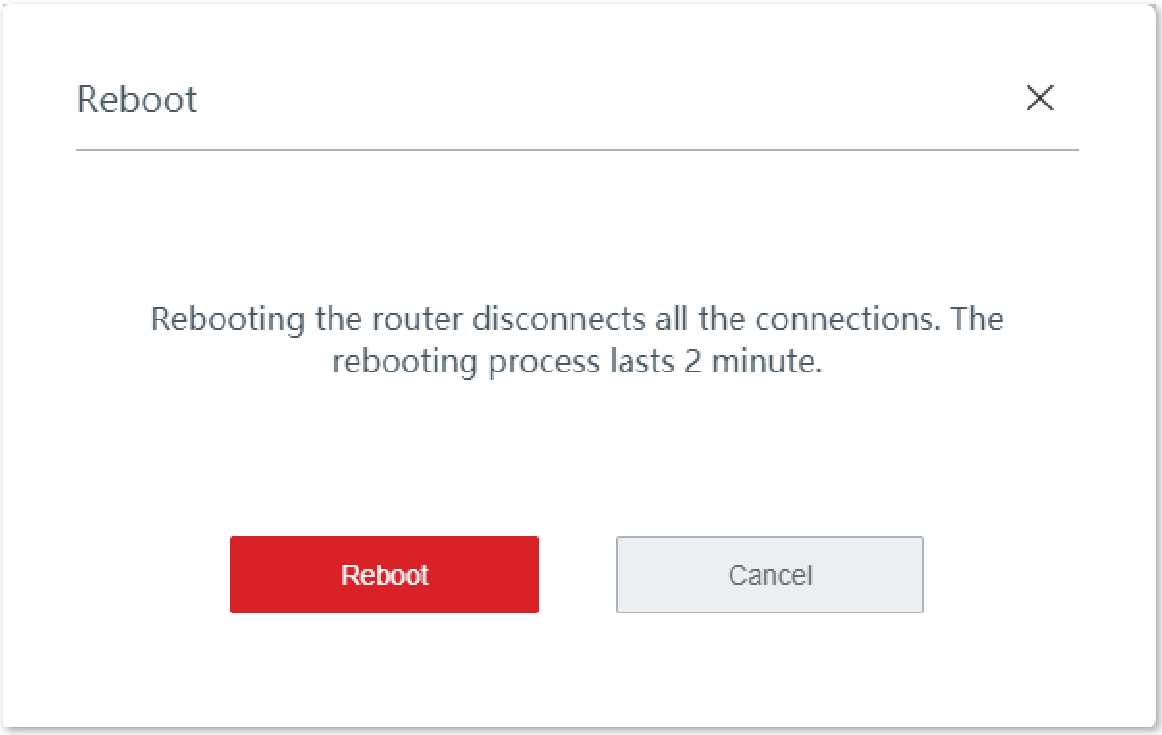
4.5.1 Reboot

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

Tip

When you reboot the primary node, secondary nodes reboot too.

Click **Maintenance** > **Reboot** to enter the page. The prompt window appears. Confirm the message and click **Reboot**.



Reboot

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

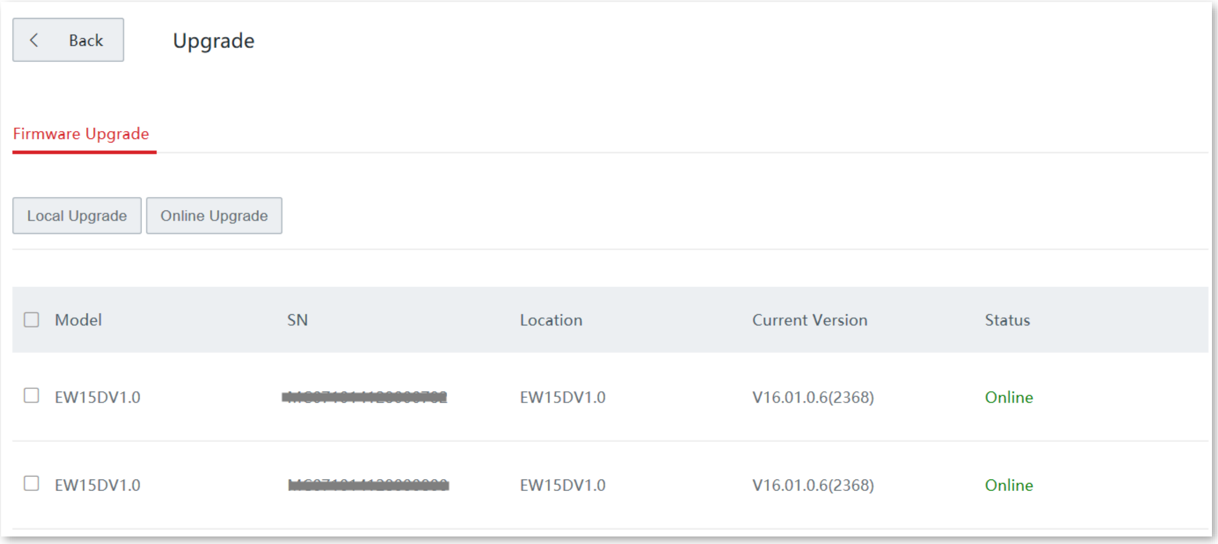
4.5.2 Upgrade

Overview

Click **Maintenance** > **Upgrade** to enter the page.

On this page, you can upgrade the firmware of the cable-free device, so as to experience more functions and get a better user experience.

The cable-free device supports local upgrade and online upgrade.



□ Model	SN	Location	Current Version	Status
□ EW15DV1.0	[redacted]	EW15DV1.0	V16.01.0.6(2368)	Online
□ EW15DV1.0	[redacted]	EW15DV1.0	V16.01.0.6(2368)	Online

Parameter description

Parameter	Description
Local Upgrade	Go to www.ip-com.com.cn to download the latest firmware to your local computer, and upgrade the router manually.
Online Upgrade	When the router is connected to the internet, you can select the device to be upgraded and click **Online Upgrade**. The device will download the firmware and upgrade the firmware automatically.

Local upgrade

Note

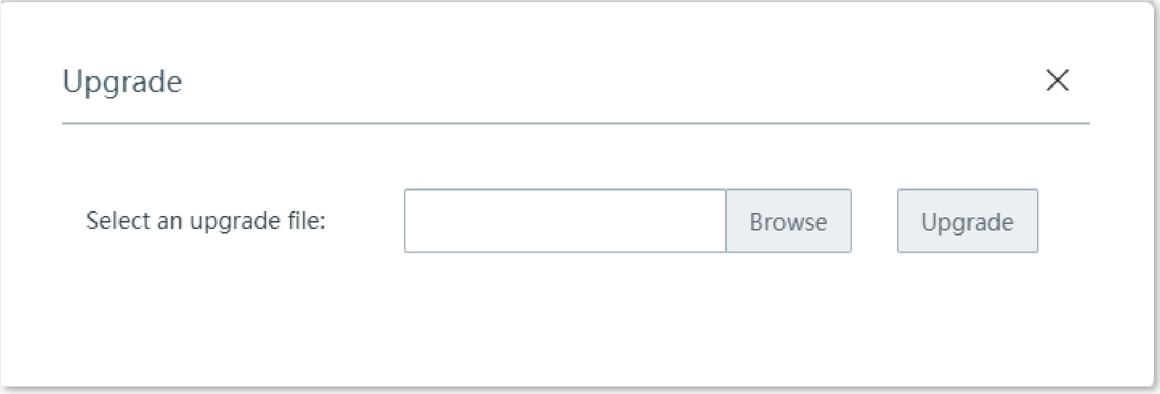
To make sure the upgrade is performed properly and the cable-free device is not damaged, ensure that:

- The correct upgrade file is used. Generally, a firmware upgrade file has a suffix of .bin
- During the upgrade, do not power off the device.

1. Visit www.ip-com.com.cn, download the upgrade firmware of the model to your computer, and unzip it.
2. Log in to the web UI of your device, click **Maintenance** > **Upgrade**, and locate the **Firmware Upgrade** module.
3. Select the cable-free device 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.

Tip

The file loading button of different browsers may differ. Chrome is taken for illustration here.



Upgrade

Select an upgrade file:

----End

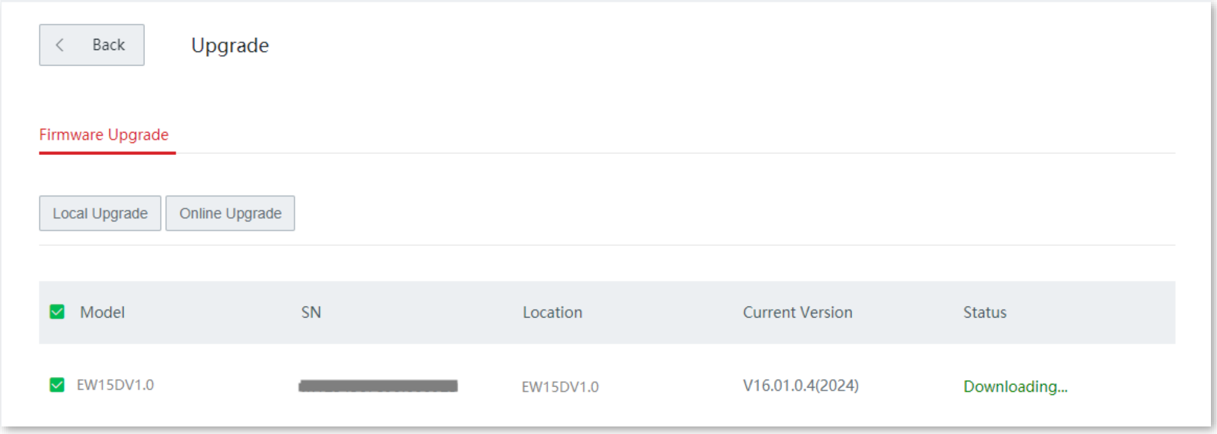
After the progress bar completes, you can log in again and check the current software version number of the device on the Upgrade or System Status page to confirm whether the upgrade is successful.

Tip

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

Online upgrade

When the device is connected to the internet, you can select the device to be upgraded and click **Online Upgrade**. The device will download the firmware and upgrade the firmware automatically.



☑ Model	SN	Location	Current Version	Status
☑ EW15DV1.0	[redacted]	EW15DV1.0	V16.01.0.4(2024)	Downloading...

4.5.3 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

After the reset, the default LAN IP address of the cable-free device is 192.168.5.1

Note

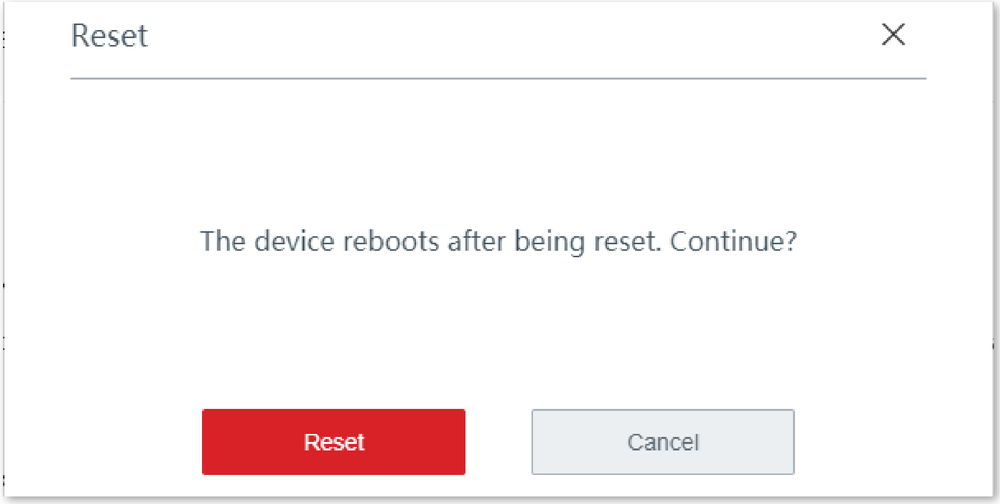
- After the reset, the cable-free device will be restored to factory settings and you can access the internet only after you reconfigure it. Reset device with caution.
- To avoid damaging the device, ensure that the device is powered on throughout the reset.

Reset the device using web UI

Tip

When you reset the primary node using web UI, secondary nodes are also reset and restored to factory settings.

On the **Maintenance > Reset** page, confirm the information 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.

When the **SYS** LED indicator is blinking, hold down the **RESET** button with a needle-like object for about 8 seconds and release it when all the LED indicators light solid green. When the **SYS** LED indicator blinks again, the device is reset successfully.

4.5.4 Password manager

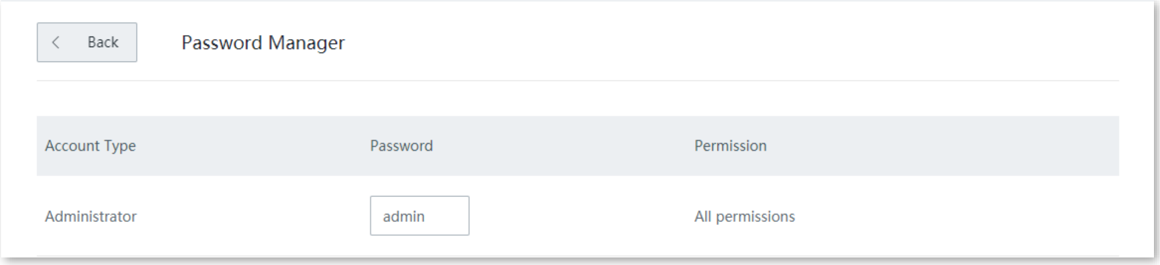
Overview

Click **Maintenance** > **Password Manager** to enter the page.

On this page, you can modify the password of the administrator. You need to set the password the first time you use the cable-free device.

Modify login password

1. Click **Maintenance** > **Password Manager** to enter the page.
2. Locate the target account type and modify the password.
3. Click **Save**.



Password Manager

Account Type	Password	Permission
Administrator	admin	All permissions

----End

You will be redirected to the login page. Enter the password you set, and click **Login** to log in to the web UI of the device.

4.5.5 Custom reboot

Overview

On this page, you can set the cable-free device to automatically reboot periodically to avoid such phenomena as deteriorating performance and instability caused by long time operation.

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

The device supports cyclic reboot and reboot schedule.

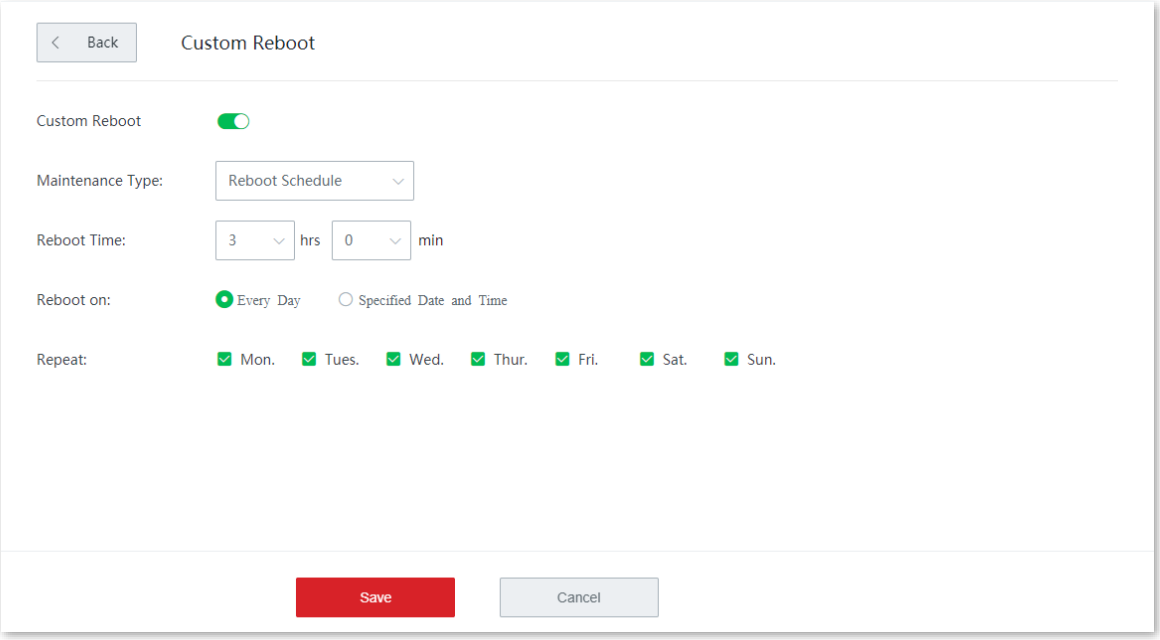
- Cyclic Reboot: The device automatically reboots every specified interval.
- Reboot Schedule: The device automatically reboots on the specified time and date.

Reboot schedule

Tip

To enable reboot schedule function to work properly, ensure that the System time of your cable-free device is correct.

1. Click **Maintenance** > **Custom Reboot** to enter the page.
2. Toggle on **Custom Reboot**.
3. Set the time, which is **3 hrs 0 min** in this example.
4. Set the date, which is **Every Day** in this example.
5. Click **Save**.



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.

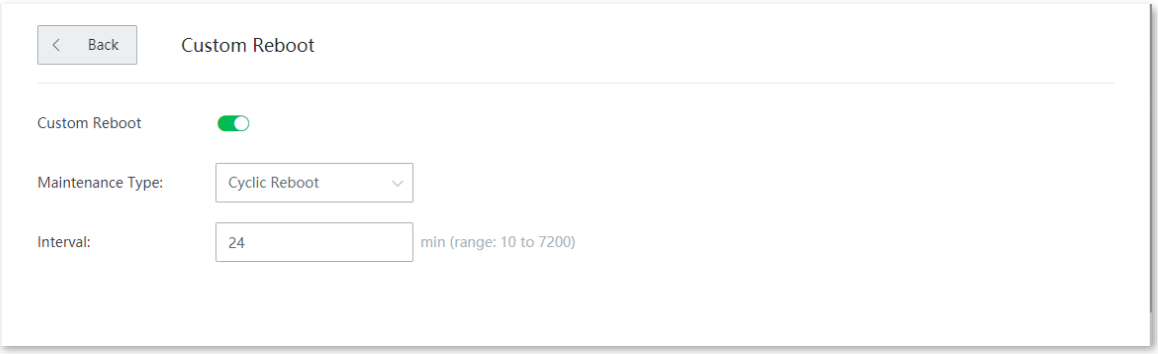
----End

The device automatically reboots every 3 am in the morning.

Cyclic reboot

1. Click **Maintenance** > **Custom Reboot**.

2. Toggle on **Custom Reboot**.
3. Select **Cyclic Reboot**.
4. Set the interval.
5. Click **Save**.



Custom Reboot

Maintenance Type: Cyclic Reboot

Interval: 24 min (range: 10 to 7200)

----End

The device automatically reboots every specified interval.

4.5.6 Backup/restore

Overview

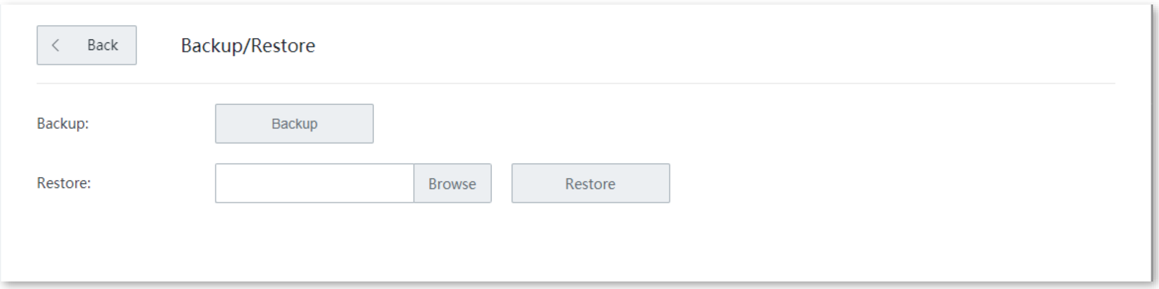
You can use the backup function to copy the current configurations of the cable-free device to the local computer and use the restore function to restore the configurations of the cable-free device to the backed up configurations.

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.

Click **Maintenance** > **Backup/Restore** to enter the page.

Backup

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



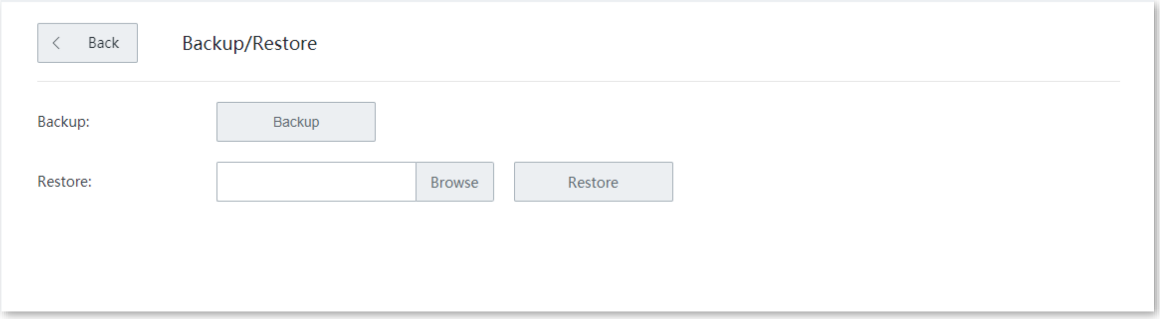
----End

Restore

1. Click **Maintenance** > **Backup/Restore**.
2. Click **Browse**, and upload the configuration file ending with **.cfg**.
3. Click **Restore**.

Tip

The file loading button of different browsers may differ. Chrome is taken for illustration here.



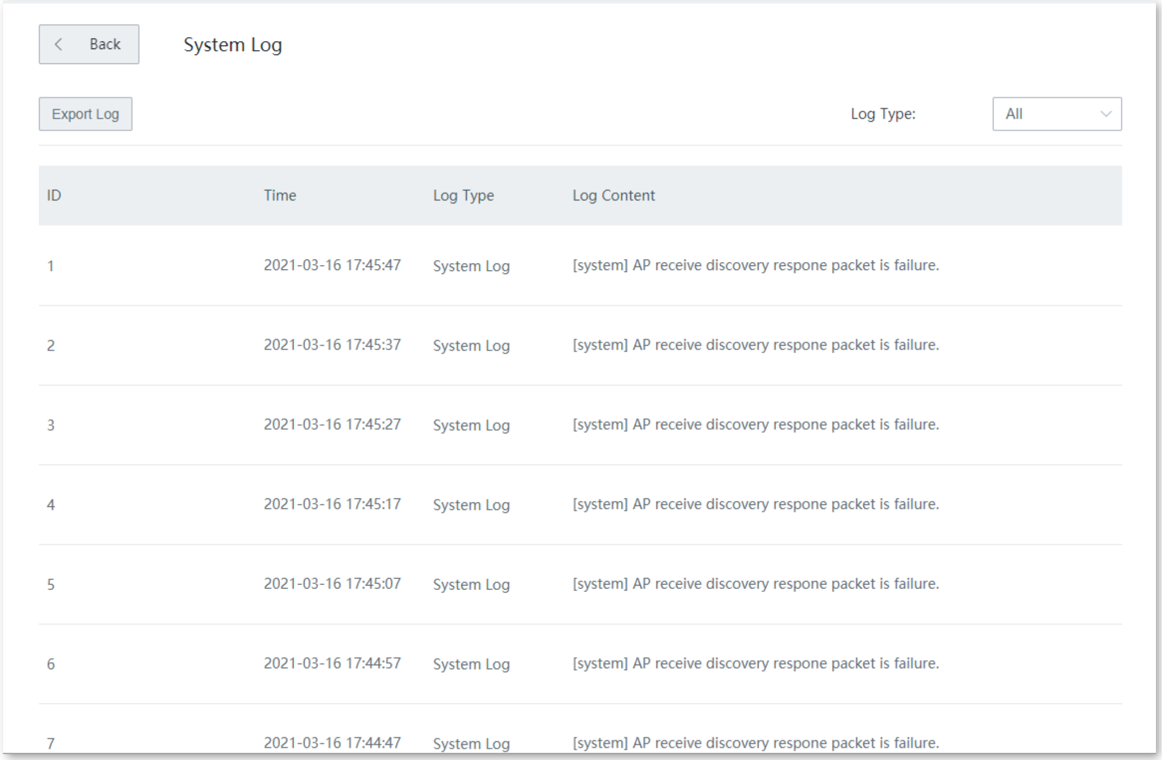
----End

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

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.

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



ID	Time	Log Type	Log Content
1	2021-03-16 17:45:47	System Log	[system] AP receive discovery respone packet is failure.
2	2021-03-16 17:45:37	System Log	[system] AP receive discovery respone packet is failure.
3	2021-03-16 17:45:27	System Log	[system] AP receive discovery respone packet is failure.
4	2021-03-16 17:45:17	System Log	[system] AP receive discovery respone packet is failure.
5	2021-03-16 17:45:07	System Log	[system] AP receive discovery respone packet is failure.
6	2021-03-16 17:44:57	System Log	[system] AP receive discovery respone packet is failure.
7	2021-03-16 17:44:47	System Log	[system] AP receive discovery respone packet is failure.

The time of the logs depend on the system time of the cable-free device. To make sure the time of the logs are correct, please set correctly the system time of the cable-free device first.

Note

- The cable-free device records only the logs occurred after the last reboot.
- After a power cutoff, such operations as power-on again, firmware upgrade, backup/restore, and reset will all cause the cable-free device to reboot.

4.5.8 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 cable-free device to the destination IP address or domain name.

Click **Maintenance** > **Diagnostic Tool** to enter the page.

Execute Ping command

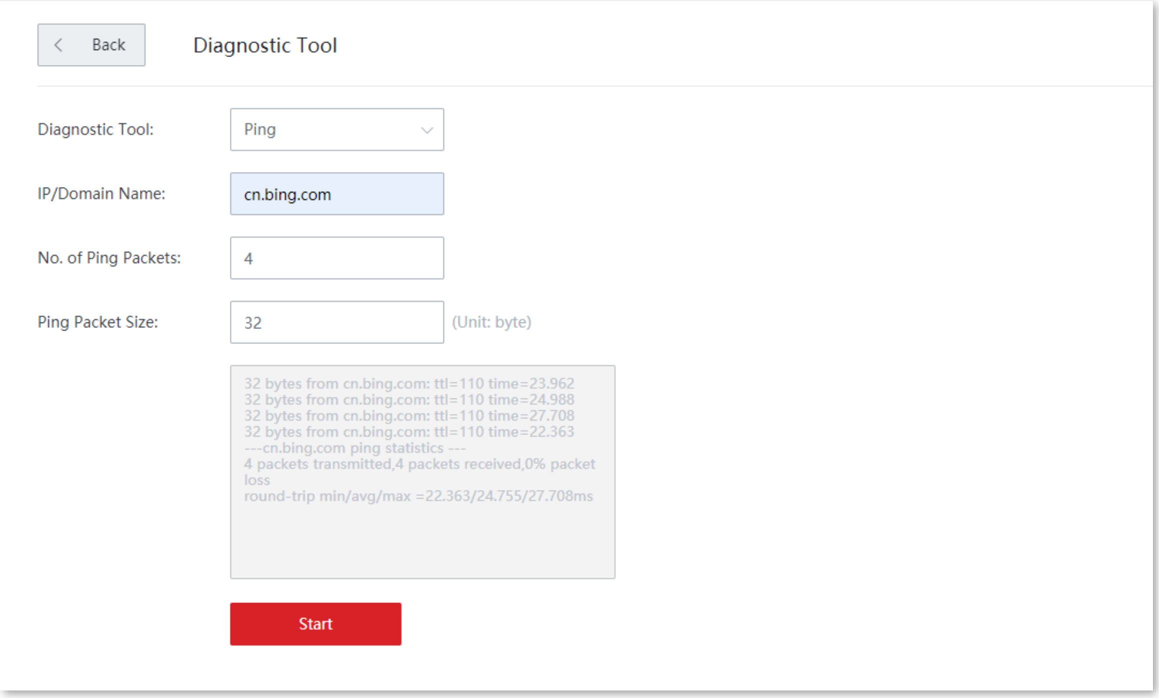
Assume that you need to detect the connectivity between the device and the **Bing** website.

Configuration procedures:

1. Click **Maintenance** > **Diagnostic Tool**.
2. Select **Ping** from the drop-down list of **Diagnostic Tool**.
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**. You are recommended to retain the default settings.
5. Set **Ping Packet Size**. You are recommended to retain the default settings.
6. Click **Start**.

----End

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



Diagnostic Tool: Ping

IP/Domain Name: cn.bing.com

No. of Ping Packets: 4

Ping Packet Size: 32 (Unit: byte)

```
32 bytes from cn.bing.com: ttl=110 time=23.962
32 bytes from cn.bing.com: ttl=110 time=24.988
32 bytes from cn.bing.com: ttl=110 time=27.708
32 bytes from cn.bing.com: ttl=110 time=22.363
---cn.bing.com ping statistics ---
4 packets transmitted,4 packets received,0% packet
loss
round-trip min/avg/max =22.363/24.755/27.708ms
```

Execute Traceroute command

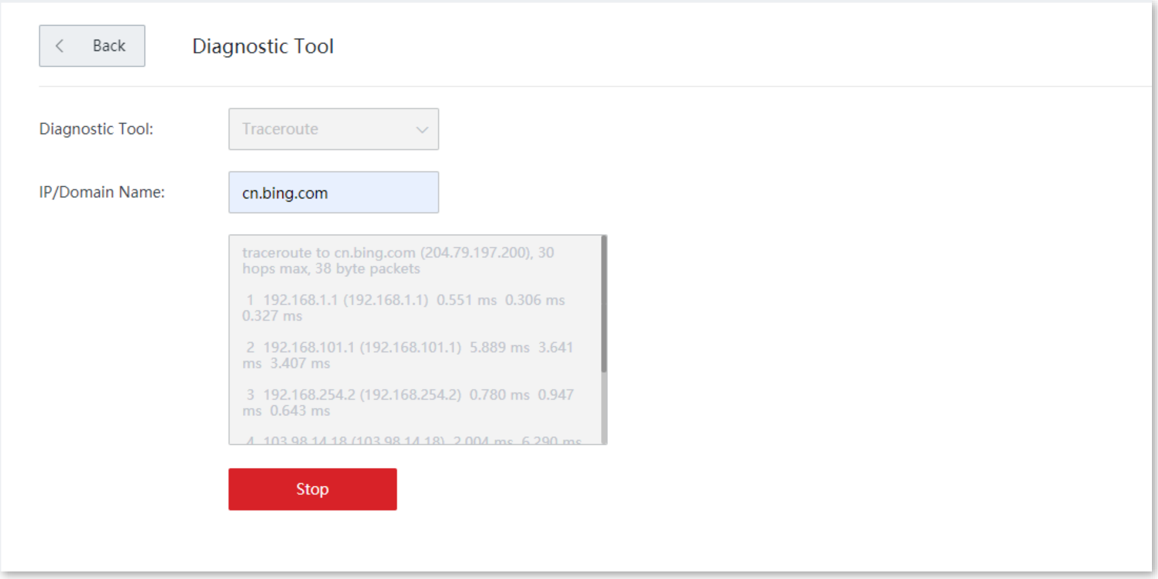
Assume that you need to detect the path from the device to **Bing** website.

Configuration procedures:

1. Click **Maintenance** > **Diagnostic Tool**.
2. Select **Traceroute** from the drop-down list of **Diagnostic Tool**.
3. Enter the IP address or domain name of the traceroute target, which is **cn.bing.com** in this example.
4. Click **Start**.

----End

The diagnosis result is shown in the lower part of the page. 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  192.168.1.1 (192.168.1.1)  0.551 ms  0.306 ms
0.327 ms

 2  192.168.101.1 (192.168.101.1)  5.889 ms  3.641
ms  3.407 ms

 3  192.168.254.2 (192.168.254.2)  0.780 ms  0.947
ms  0.643 ms

 4  103.98.14.18 (103.98.14.18)  2.004 ms  6.290 ms
```

4.5.9 System time

To make the time-related functions effective, ensure that the system time of the device is set correctly.

The device supports:

- Sync with internet time
- Manual

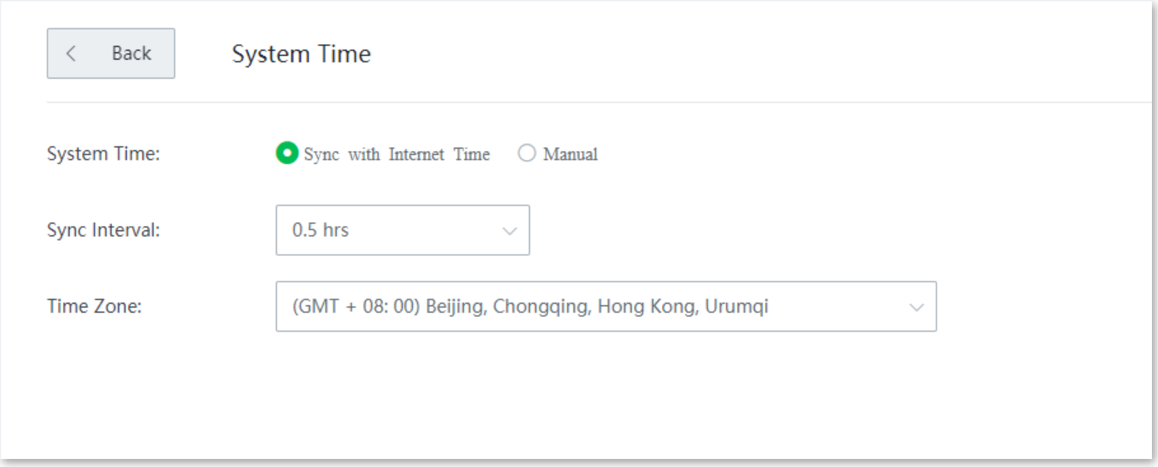
By default, sync with internet time is chosen.

Click **Maintenance** > **System Time** to enter the page.

Sync with internet time

If you choose 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.

After the configuration, you can enter the **System Status** page to check whether the system time of the cable-free device is correct.



System Time: ● Sync with Internet Time ○ Manual

Sync Interval: 0.5 hrs

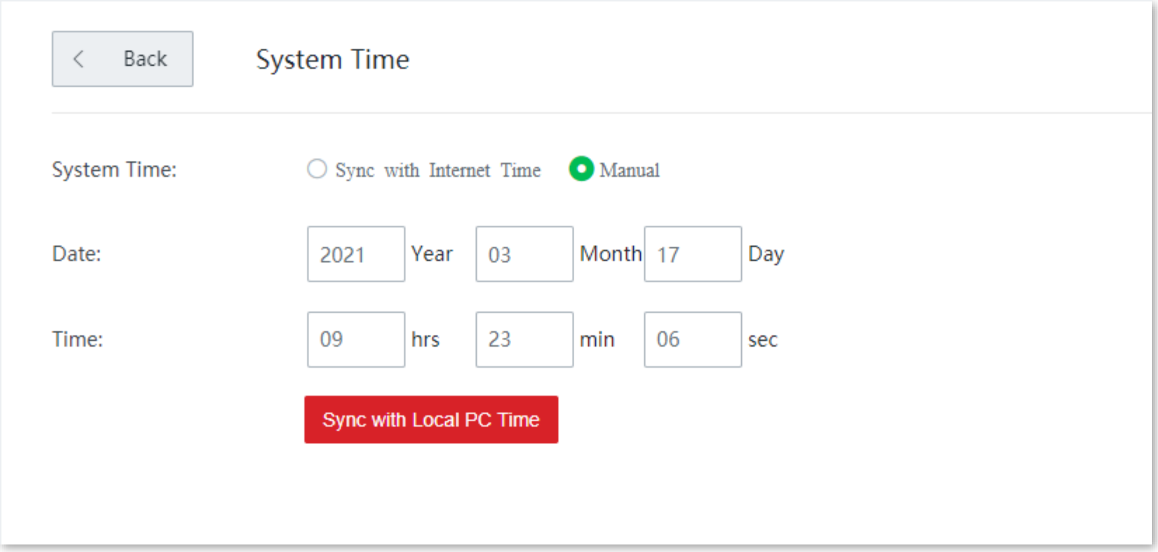
Time Zone: (GMT + 08: 00) Beijing, Chongqing, Hong Kong, Urumqi

Parameter description

Parameter	Description
System Time	It is used to choose the configuration method of the system time. The options include sync with internet time and manual.
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.

Manual

If you choose this method, you can manually specify a system time for the device. Every time the cable-free device reboots, you have to reconfigure the system time. The following displays the page when **Manual** is chosen.



System Time: ○ Sync with Internet Time ● Manual

Date: 2021 Year 03 Month 17 Day

Time: 09 hrs 23 min 06 sec

Parameter description

Parameter	Description
System Time	It is used to choose the configuration method of the system time. The options include sync with internet time and manual.
Date	You can directly enter the correct time here. Or, you can click **Sync with Local PC Time** to synchronize the time of the cable-free device with that of the computer managing the cable-free device.
Time	

After the configuration, you can enter the **System Status** page to check whether the system time of the cable-free device is correct.

Appendix

A.1 Default parameters

Parameter		**Default**
Login	Management domain name	www.ipcwifi.com
	Management IP address	192.168.5.1
	Login password	No password
Working mode		Cable-free (Router mode)
Mesh networking mode		Wireless networking
LAN settings	IP address	192.168.5.1
	Subnet mask	255.255.255.0
DHCP server	DHCP server	Enabled in router mode, disabled in AP mode
	Start IP address	192.168.5.31
	End IP address	192.168.5.200
	Lease time	0.5 hrs
	Primary DNS	192.168.5.1
Wireless	Primary WiFi network	Enabled SSID for the 2.4/5 GHz bands are the same SSID: IP-COM_*XXXXXX*, in which *XXXXXX* indicates the last 6 characters of the LAN MAC address of the cable-free device. WiFi password: no password
	Guest network	Disabled
Node management		Enabled
System time		Sync with internet time

A.2 Acronyms and abbreviations

Acronym or Abbreviation	Full Spelling
AC	Access Controller
AES	Advanced Encryption Standard
AH	Authentication Header
AP	Access Point
APSD	Automatic Power Save Delivery
ARP	Address Resolution Protocol
CPU	Central Processing Unit
CRM	Customer Relationship Management
DDNS	Dynamic Domain Name Service
DDoS	Distributed Denial of Service
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone
DNS	Domain Name System
DPD	Dead Peer Detection
ERP	Enterprise Resource Planning
ESP	Encapsulating Security Payload
FQDN	Fully Qualified Domain Name
FTP	File Transfer Protocol
GI	Guard Interval
GMT	Greenwich Mean Time
HTTP	Hyper Text Transfer Protocol
ICMP	Internet Control Message Protocol
ID	Identity Document
IEEE	Institute of Electrical and Electronic Engineers
IKE	Internet Key Exchange
IP	Internet Protocol
IPsec	Internet Protocol Security

Acronym or Abbreviation	Full Spelling
ISAKMP	Internet Security Association Key Management Protocol
ISP	Internet Service Provider
L2TP	Layer 2 Tunneling Protocol
LAN	Local Area Network
MAC	Medium Access Control
MGMT	Management
MTU	Maximum Transmission Unit
NAT	Network Address Translation
NTS	Network Time Server
OA	Office Automation
PFS	Perfect Forward Secrecy
PoE	Power over Ethernet
POP	Post Office Protocol
PPP	Point to Point Protocol
PPPoE	Point-to-Point Protocol over Ethernet
PPTP	Point to Point Tunneling Protocol
PSK	Pre-shared Key
PVID	Port-base VLAN ID
QAM	Quadrature Amplitude Modulation
RF	Radio Frequency
RSSI	Received Signal Strength Indicator
SA	Security Association
SHA	Secure Hash Algorithm
SMS	Short Messaging Service
SMTP	Simple Mail Transfer Protocol
SN	Serial Number
SPI	Security Parameter Index
SSID	Service Set Identifier
SSL	Secure Sockets Layer
SYN	Synchronize Sequence Numbers

Acronym or Abbreviation	Full Spelling
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
UI	User Interface
UPnP	Universal Plug and Play
URL	Uniform Resource Locator
VID	VLAN Identity Document
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WAN	Wide Area Network
WLAN	Wireless Local Area Network
WMM	Wi-Fi Multi-media