IP-COM



User Guide

Enterprise Router

www.ip-com.com.cn

Copyright statement

Copyright © 2023 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 a warranty of any kind, express or implied.

Preface

Thank you for choosing IP-COM. Please read this user guide before you start.

This user guide is applicable to the IP-COM Enterprise Routers. All screenshots herein, unless otherwise specified, are taken from M30V3.0.

Tip

Web UI of different models may vary. Please refer to the actual product.

Conventions

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

Item	Presentation	Example
Cascading menus	>	Choose **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.

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.

Product document overview

Document	Description
Datasheet	It introduces the basic information of the device, including product overview, selling points and specifications.
User Manual	It introduces how to set up the device quickly for internet access, including the appearance of the router, installation, connection, configuration, safety precaution and so on.
Quick Installation Guide	It introduces how to use the device quickly, including package contents, the appearance of the router, installation methods, 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

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

Email address: info@ip-com.com.cn

Website: 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	2023-1-29	Original publication

Contents

1 Operating mode 1

1.1 Router mode 2

1.1.1 Overview 2

1.1.2 Set the router to operate in router mode 3

1.2 Pure AC mode 4

1.2.1 Overview 4

1.2.2 Set the router to operate in pure AC mode 5

2 Login and logout 6

2.1 Login 6

2.1.1 LAN login 6

2.1.2 Remote login 10

2.2 Logout 11

3 Web UI introduction 12

3.1 Web layout 12

3.2 Common buttons 13

4 System status 14

4.1 System resource information 14

4.2 Interface info 15

4.3 WAN real-time rate 16

4.4 AP management 17

5 Networks 18

5.1 Internet settings 18

5.1.1 No. of WAN ports 18

5.1.2 Set the internet 19

5.1.3 Check connection status....23
5.2 LAN settings....25
5.3 LAN configuration info....26
5.4 VLAN settings....27
5.4.1 Overview....27
5.4.2 Example of configuring the VLAN....29
5.5 DHCP settings....36
5.5.1 Overview....36
5.5.2 DHCP server....37
5.5.3 DHCP reservation....38
5.5.4 DHCP list....40
6 AP Management....41
6.1 Overview....41
6.2 Configuration wizard....42
6.3 Wireless policy....43
6.3.1 SSID policy....43
6.3.2 RF policy....46
6.3.3 VLAN policy....49
6.3.4 Advanced policy....51
6.4 AP group policy....58
6.5 AP list and maintenance....60
6.5.1 Overview....60
6.5.2 Deliver policies to APs....63
6.5.3 Batch settings....64
6.5.4 Set the AP cloud maintenance function....66
6.6 Wireless user information....69
6.7 Exmaple of configuring fat APs....71
6.8 IPTV....77
6.8.1 Overview....77

6.8.2 Watch IPTV programs (scenario 1) 78
6.8.3 Watch IPTV programs (scenario 2) 80
7 Cloud VPN 83
7.1 Overview 83
7.2 Configure cloud VPN operating mode 85
8 Bandwidth limit 86
8.1 WAN bandwidth 86
8.2 Group limit 87
8.3 Single user limit 89
8.3.1 Overview 89
8.3.2 Configure single user limit 90
8.4 Example of configuring group speed limit 91
9 Behavior&Audit 94
9.1 Group policy 94
9.1.1 Time group 94
9.1.2 IP group 96
9.2 Filtering 97
9.2.1 IP address filtering 97
9.2.2 MAC address filtering 101
9.2.3 Port filtering 104
9.2.4 URL filtering 108
9.3 Log auditing 113
9.3.1 Audit settings 113
9.3.2 Log storage 114
10 More 115
10.1 Advanced routing 115
10.1.1 WAN parameters 115
10.1.2 Multi-WAN policy 117
10.1.3 Static routing 121

10.1.4 Routing table 126
10.1.5 Policy routing 127
10.2 Virtual Service 132
10.2.1 DMZ 132
10.2.2 DDNS 136
10.2.3 DNS hijacking 141
10.2.4 IP hijacking 143
10.2.5 UPnP 146
10.2.6 Port mirroring 146
10.2.7 Port mapping 149
10.2.8 DNS cache 154
10.3 Maintenance service 155
10.3.1 Remote web management 155
10.3.2 AP management mode 158
10.3.3 Security settings 159
10.3.4 Cloud maintenance 160
10.3.5 Remote debugging 173
10.4 IPv6 177
10.4.1 Overview 177
10.4.2 Internet 177
10.4.3 LAN 182
11 System maintenance 184
11.1 System time 184
11.1.1 Sync time with network time 184
11.1.2 Set system time manually 185
11.2 Diagnostic tool 186
11.2.1 Ping 186
11.2.2 Tracert 187
11.2.3 Packet capture tool 189

11.2.4 AP diagnosis....191
11.2.5 System diagnosis....192
11.2.6 Interface info....193
11.3 Log center....194
11.3.1 System log....194
11.3.2 Operating log....194
11.3.3 Running log....195
11.4 System maintenance....196
11.4.1 Device info....196
11.4.2 Restore & Backup....196
11.4.3 Factory settings restore....198
11.5 Upgrade service....200
11.5.1 Overview....200
11.5.2 System firmware upgrade....201
11.5.3 Feature-Library upgrade....202
11.6 Reboot services....203
11.6.1 Reboot....203
11.6.2 Scheduled reboot....203
11.7 System account....205
11.8 Test....206
Appendix....207

1 Operating mode

This router supports two operating modes. Choose the appropriate mode according to the actual situation. The text description takes router mode as an example.

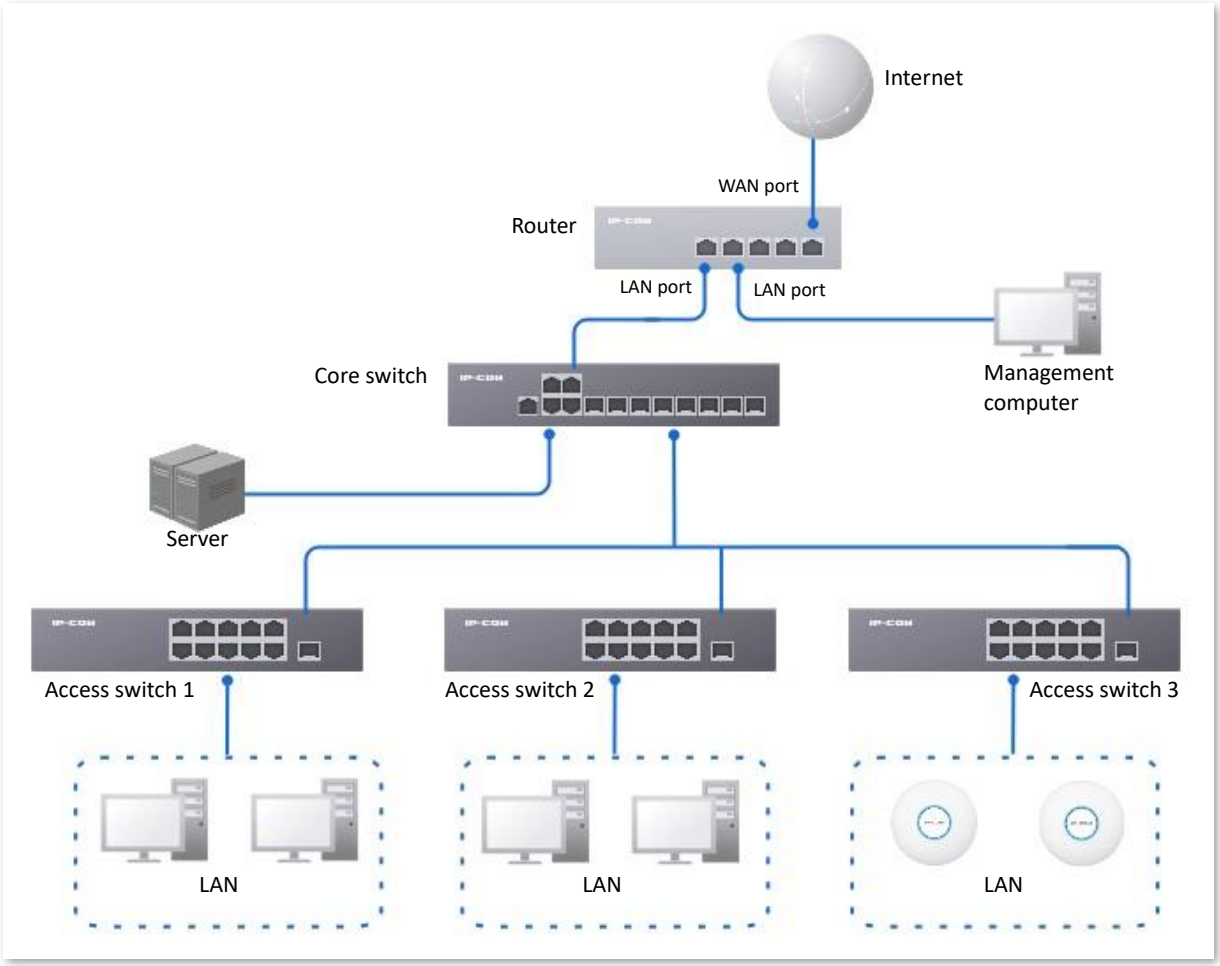
- Router Mode: The device is used as a router and wireless controller, providing internet access, routing forward, AP management, behavior & audit and other functions. In this mode, the device needs to process both control packets and data packets.
- Pure AC Mode: The device is used as a wireless controller to provide functions such as AP management, behavior & audit. Refer to the page display. In this mode, data packets no longer pass through the device, and the device only needs to process control packets.

1.1 Router mode

1.1.1 Overview

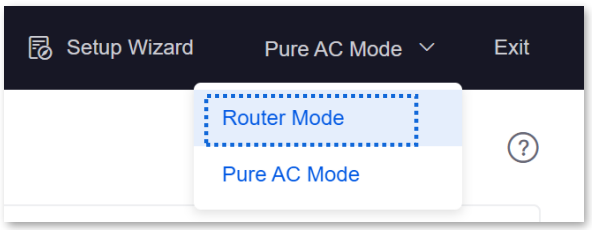
In router mode, the device is used as a router and wireless controller, which is generally deployed at the egress gateway to proxy the LAN to access the internet.

The application scenarios are as follows.

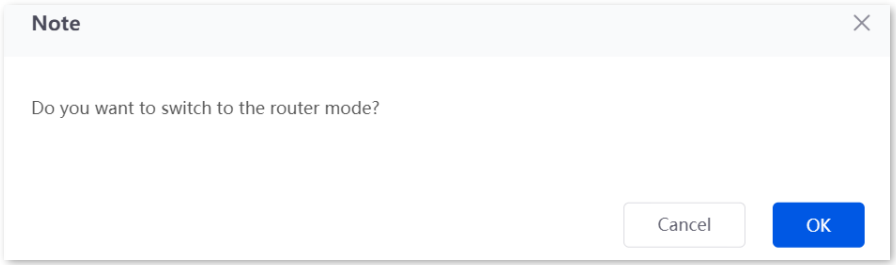


1.1.2 Set the router to operate in router mode

1. Log in to the web UI of the router, and select **Router Mode** from the mode selection drop-down menu at the top right of the page. The following figure is for reference only.



2. Confirm the prompt information and click **OK**.



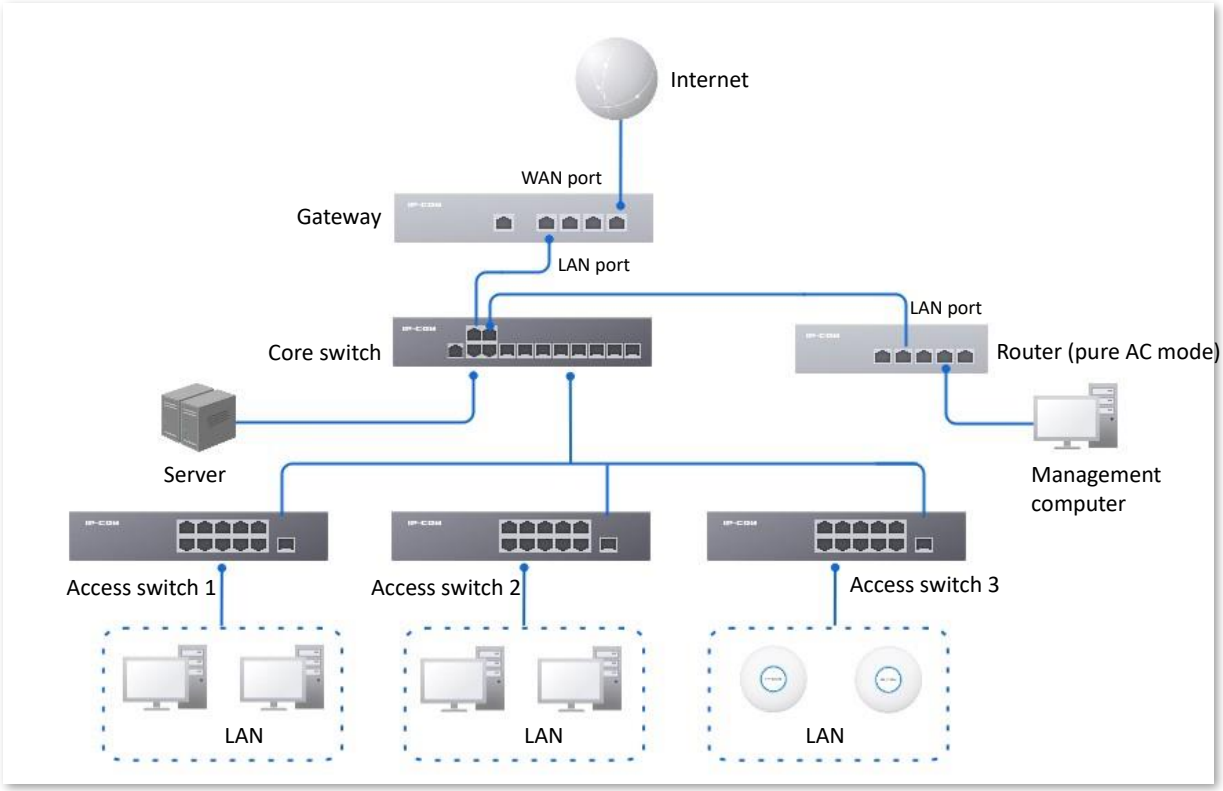
----End

1.2 Pure AC mode

1.2.1 Overview

In pure AC mode, the device is used as a wireless controller, which can be deployed under the core switch. Only some functions are supported.

The application scenarios are as follows.

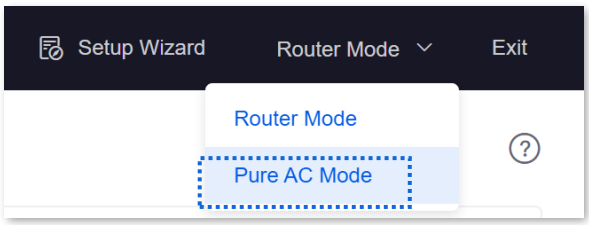


Tip

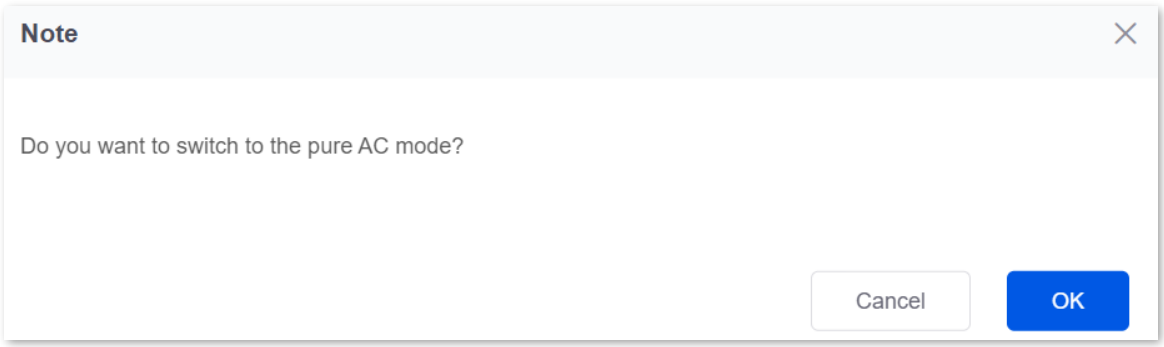
In pure AC mode, if you want to use the remote web management, cloud maintenance, and remote debugging functions of the router, connect the router to another internet through the WAN port, and set the router to the internet through **Dynamic IP Address** or **Static IP Address**. Otherwise, the configuration is invalid.

1.2.2 Set the router to operate in pure AC mode

1. Log in to the web UI of the router, and select **Pure AC Mode** from the mode selection drop-down menu at the top right of the page. The following figure is for reference only.



2. Confirm the prompt information and click **OK**.



----End

2 Login and logout

2.1 Login

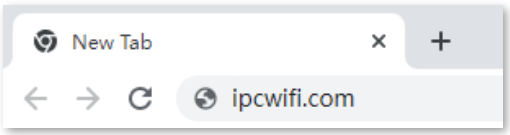
For initial use or having restored to factory settings of this device, you can refer to the quick installation guide (download it from www.ip-com.com.cn).

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

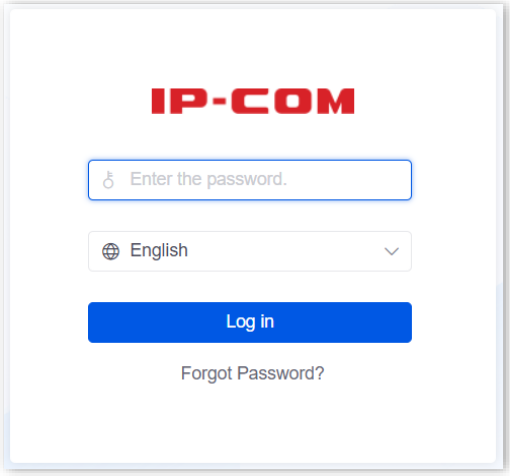
2.1.1 LAN login

Login to the web UI in router mode

1. Use an Ethernet cable to connect the management computer to the LAN port of the router, or a switch connected to the LAN port of the router.
2. Start a web browser (Chrome as an example) on your computer, and enter the IP address of the router (**ipcwifi.com**).



3. Enter the login password, and click **Log in**.



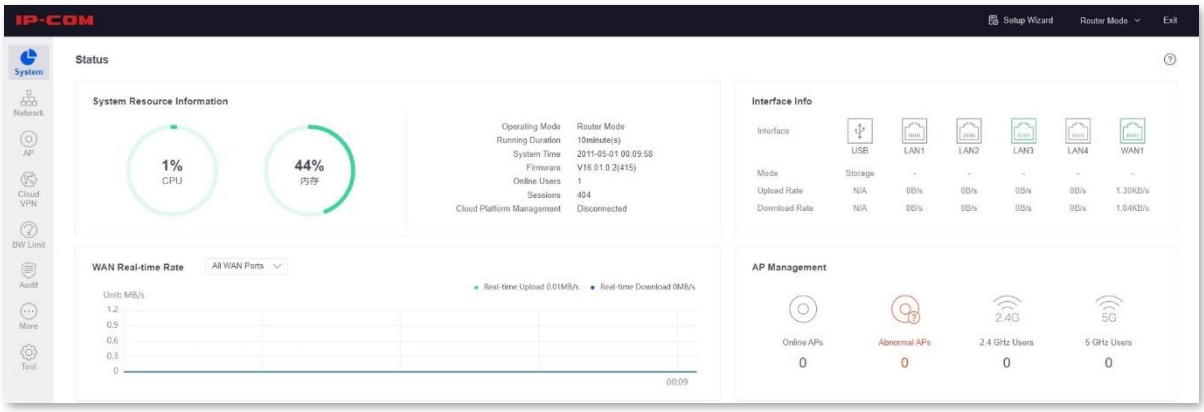
----End

Tip

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

- Ensure that the management computer is properly connected and the Ethernet cable is not loose.
- Set your computer to **Obtain an IP address automatically** and **Obtain DNS server address automatically**.
- Restore the router to factory settings and retry. Note that the router needs to be connected to the internet again after restoration.

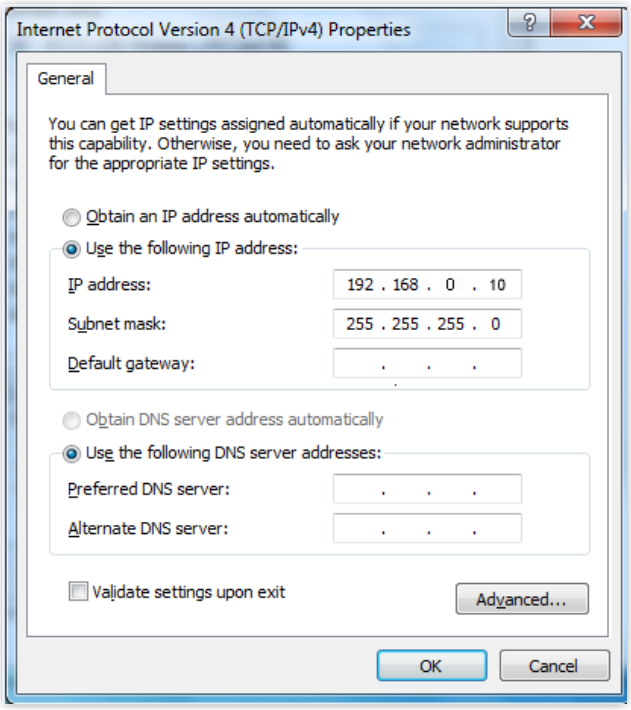
If the following page is displayed, you have logged in to the web UI successfully.



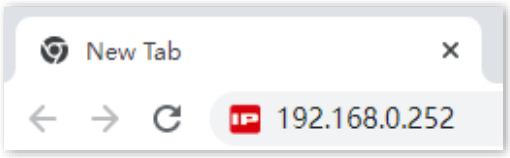
Log in to the web UI in pure AC mode

1. Use an Ethernet cable to connect the management computer to the LAN port of the router, or a switch connected to the LAN port of the router.
2. Configure the IP address of the management computer to one in a same network segment with the router.

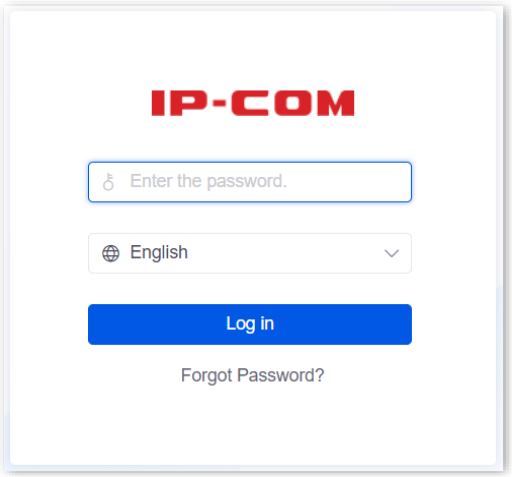
   For example, if the IP address of the router is **192.168.0.252**, then you can set the IP address of the computer to **192.168.0.*X*** (*X* ranges from 2 to 251 and is not occupied by other devices), and subnet mask to **255.255.255.0**.



3. Start a browser on the computer and visit the IP address of the router (**192.168.0.252** by default).



4. Enter the login password, and click **Log in**.

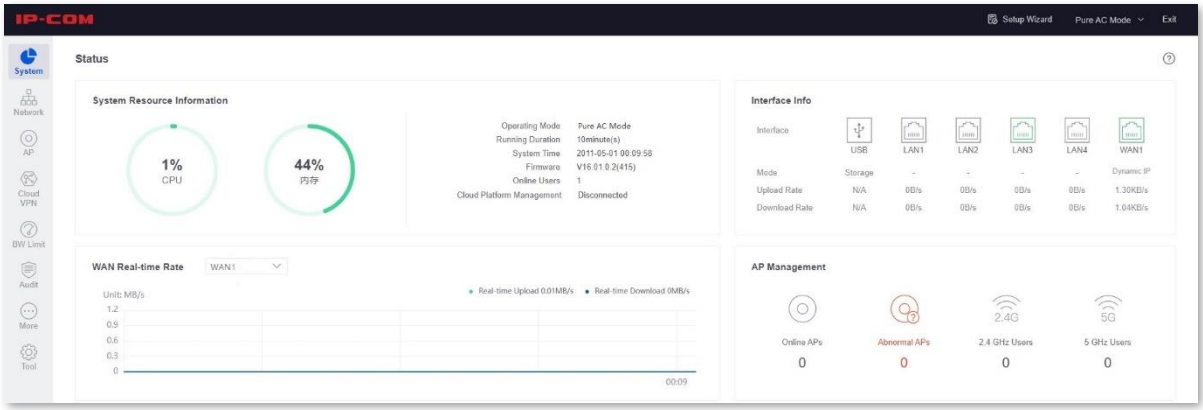


---End

Tip

If the above page does not appear, ensure that the management computer is properly connected and the Ethernet cable is not loose.

If the following page is displayed, you have logged in to the web UI successfully.



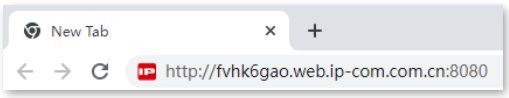
2.1.2 Remote login

The login mode is applicable when the router has enabled the Remote Web Management function.

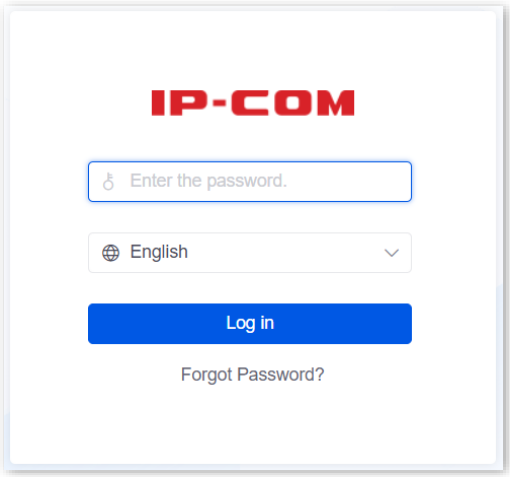
Tip

Before using this mode to log in, ensure that your terminal device has been allowed to remotely access the router.

1. Start a web browser (Chrome as an example) on a terminal connected to the internet, and access the router's remote management address. The following figure is for reference only.

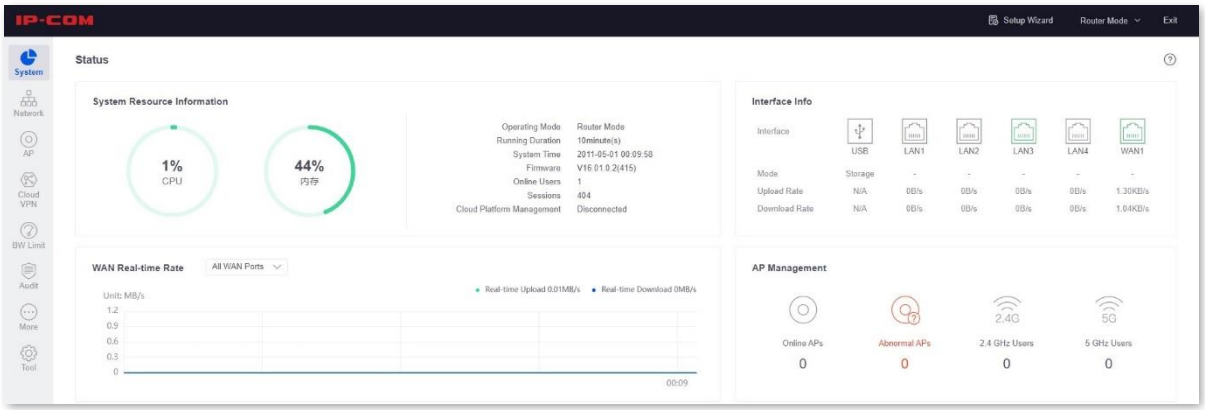


2. Enter the login password, and click **Log in**.



----End

If the following page is displayed, you have logged in to the web UI successfully.



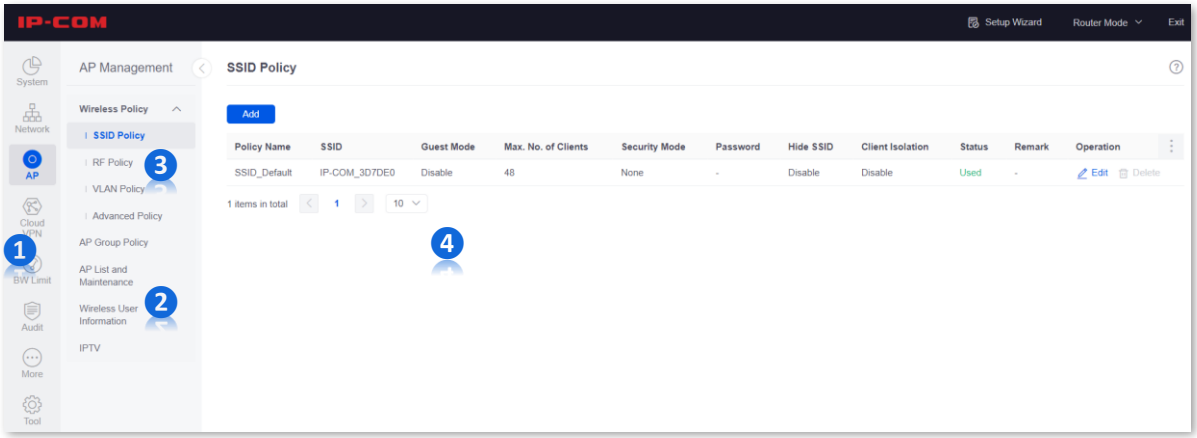
2.2 Logout

After you log in to the router's web UI page, the system will automatically log you out if there is no operation within the Login Timeout. Alternatively, you can directly click **Exit** on the upper right corner to exit the web UI page.

3 Web UI introduction

3.1 Web layout

The web UI page can be divided into four parts: level-1 navigation bar, level-2 navigation bar, level-3 navigation bar and the configuration area. See the following figure.



Tip

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

NO.	Name	Description
1	Level-1 navigation bar	The navigation bars and tab pages display the function menu of the router. Users can select functions in the navigation bars and the configuration appears in the configuration area.
2	Level-2 navigation bar	
3	Level-3 navigation bar	
4	Configuration area	This area enables you to view and modify the configuration.

3.2 Common buttons

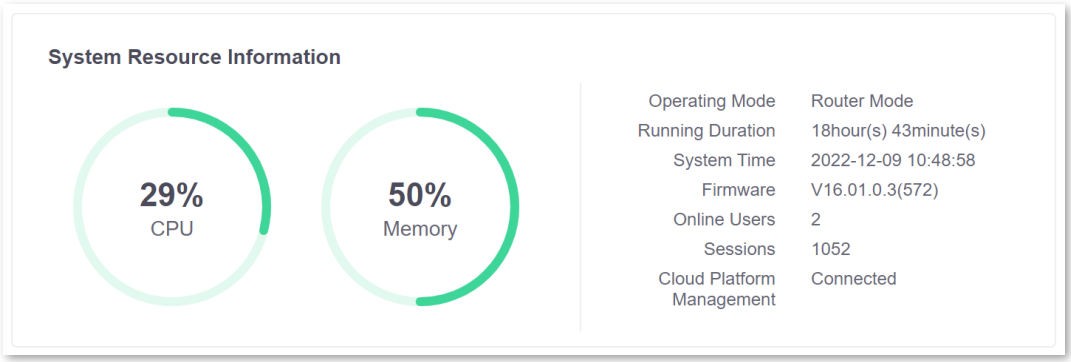
The following table describes the common buttons available on the web UI of the device.

Common buttons	Description
Add	Used to add new rules on the current page.
Save	Used to save the configuration on the current page and enable the configuration to take effect.
Cancel	Used to restore the original configuration without saving the configuration on the current page.
Edit	Used to edit corresponding rules, policies or information.
Delete	Used to delete the rules on the current page.
	Used to view the help information for the current page.
	Used to view the help information of the corresponding setting.
	Used to customize the list parameters to be displayed, or restore the list parameters display to the default state.

4 System status

4.1 System resource information

Log in to the web UI of the router, and click **System** to enter the page. In the **System Resource Information** module, you can view the system information of the router.

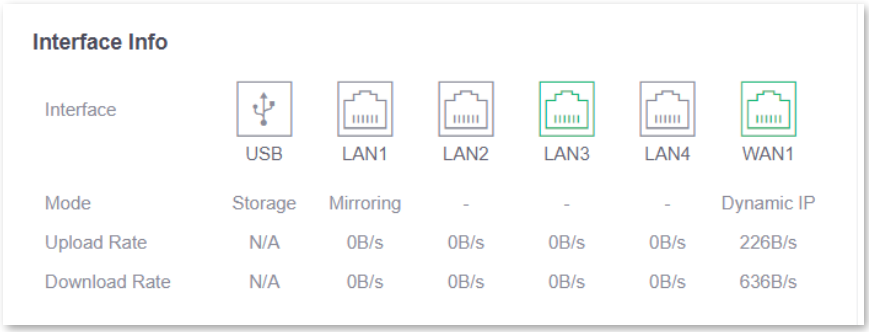


Parameter description

Parameter	Description
CPU	Specifies the CPU usage of the router.
Memory	Specifies the memory usage of the router.
Operating Mode	Specifies the current operating mode of the router.
Running Duration	Specifies the time during which this router is operating since the last reboot.
System Time	Specifies the current system time of the router.
Firmware	Specifies the current firmware version of the router.
Online Users	Specifies the number of current connected users of the router.
Sessions	Specifies the number of concurrent connections of the router.
Cloud Platform Management	Specifies whether the router is connected to the cloud platform.

4.2 Interface info

Log in to the web UI of the router, and click **System** to enter the page. In the **Interface Info** module, you can view the basic status of each port of the router.



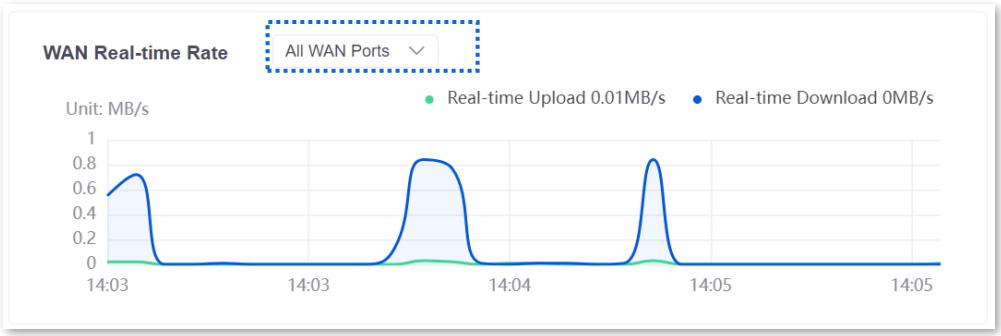
Parameter description

Parameter	Description
Interface	Specifies the roles and connection status of each port of the router. – Green means connected. – Grey means disconnected.
Mode	Specifies the operating mode of each port of the router. Supports displaying the connection type of WAN port, the port mirroring mode **Mirroring** (with Port mirroring enabled) of the port. Some routers support plugging in USB devices, and displaying the operating mode **Storage** of the USB devices.
Upload Rate	Specify the real-time upload/download rate of each port of the router.
Download Rate	

4.3 WAN real-time rate

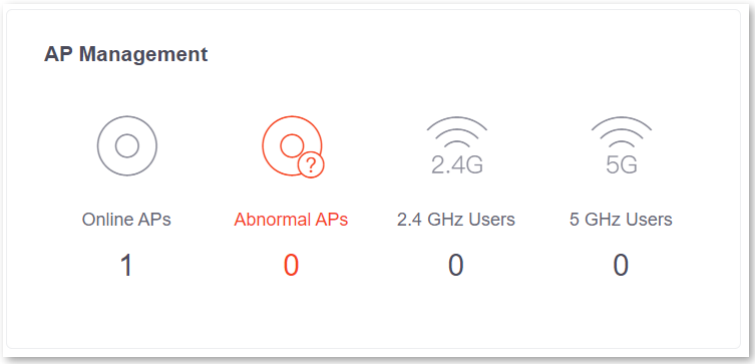
Log in to the web UI of the router, and click **System** to enter the page. In the **WAN Real-time Rate** module, you can view the upload and download rates of all WAN ports or a certain WAN port of the router.

Click the drop-down box next to **WAN Real-time Rate** to select a certain WAN port of the router.



4.4 AP management

Log in to the web UI of the router, and click **System** to enter the page. In the **AP Management** module, you can view the basic information of APs managed by the router.



Parameter description

Parameter	Description
Online APs	Specifies the number of online APs.
Abnormal APs	Specifies the number of offline APs.
2.4 GHz Users	Specifies the number of users connected to the 2.4 GHz network.
5 GHz Users	Specifies the number of users connected to the 5 GHz network.

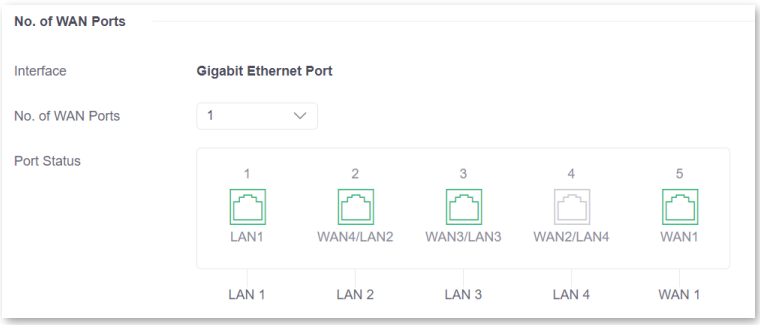
5 Networks

5.1 Internet settings

Here, you can configure the internet access parameters of the WAN port of the router, so that multiple devices in the LAN can share the broadband service.

5.1.1 No. of WAN ports

Log in to the web UI of the router, and navigate to **Network** > **Internet Settings** to enter the page. In the **No. of WAN Ports** module, you can view the rate type of the WAN port and set the number of WAN ports. You can also view the connection status and the properties of each Ethernet port. The following figure takes M30 router as an example.



Parameter description

Parameter	Description
Interface	Specifies the rate type of the port.
No. of WAN Ports	Specifies the number of WAN ports. The number of default WAN ports varies according to router models. You can change the WAN port number as needed.
Port Status	Specifies the port type and the connection status.  : The port is connected properly.  : The port is disconnected or not connected properly.

5.1.2 Set the internet

Log in to the web UI of the router, and navigate to **Network** > **Internet Settings** to enter the page. In the **Connection Settings** module, you can set the internet parameters of the WAN port. Connection types of the router include **PPPoE**, **Dynamic IP Address** and **Static IP Address**.

Tip

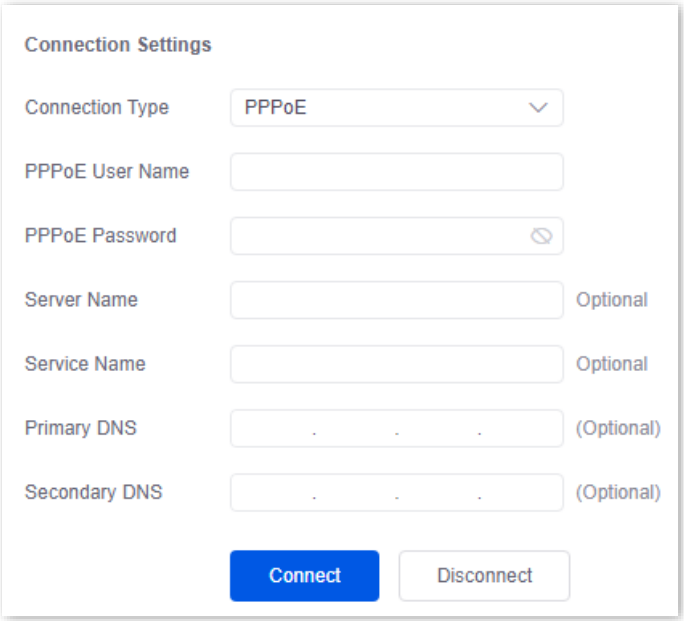
- The number of default WAN ports varies according to router models. WAN1 is used as an example, and configurations for other WAN ports are similar.
- All internet parameters for accessing the internet are provided by your ISP. Consult your ISP if you are not clear.

PPPoE

The router uses the PPPoE user name and password provided by the ISP to access the internet with PPPoE.

Configuration procedure

1. Log in to the web UI of the router, and navigate to **Network** > **Internet Settings.**
2. In the **Connection Settings** module, select **PPPoE** for **Connection Type**.
3. Enter the PPPoE user name and password provided by the ISP.
4. Click **Connect**.



----End

Wait for a moment. You can view related internet information in the **Connection Status** module.

Parameter description

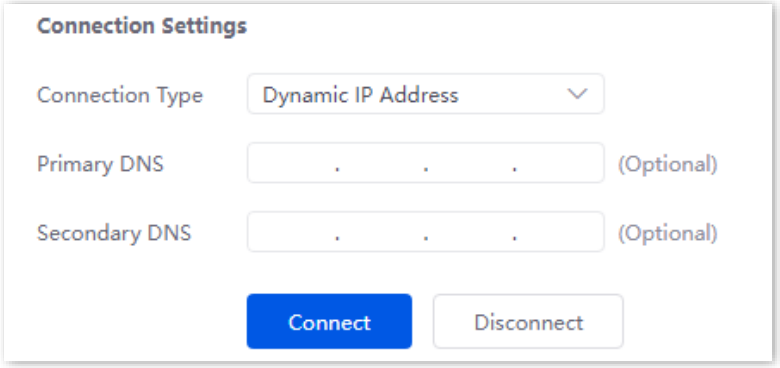
Parameter	Description
PPPoE User name	Specify the PPPoE user name and password provided by the ISP.
PPPoE Password	
Server Name	Specifies the name of the PPPoE server, also called the AC name. Used by the router to verify the validity of the PPPoE server. The **Server Name** is optional. Note To avoid dialing failures, do not set this parameter if your ISP does not provide the server name.
Service Name	Specifies the name of the PPPoE service. Used by the PPPoE server to verify the validity of the router. The **Service Name** is optional. Note To avoid dialing failures, do not set this parameter if your ISP does not provide the service name.
Primary DNS	Manually enter primary/secondary DNS servers. When the DNS server obtained automatically cannot resolve the URL normally, you can manually enter a correct primary/secondary DNS server here. The **Primary DNS** and **Secondary DNS** are optional.
Secondary DNS	

Dynamic IP address

The router uses the IP address information dynamically assigned by the ISP to access the internet.

Configuration procedure

1. Log in to the web UI of the router, and navigate to **Network** > **Internet Settings.**
2. In the **Connection Settings** module, select **Dynamic IP Address** for **Connection Type**.
3. Click **Connect**.



----End

Wait for a moment. You can view related internet information in the **Connection Status** module.

Parameter description

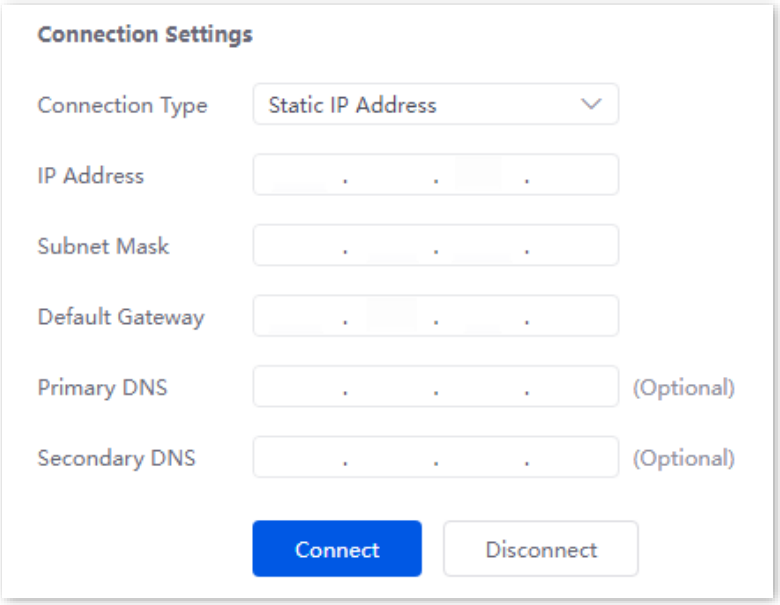
Parameter	Description
Primary DNS	Manually enter primary/secondary DNS servers. When the DNS server obtained automatically cannot resolve the URL normally, you can manually enter a correct primary/secondary DNS server here. The **Primary DNS** and **Secondary DNS** are optional.
Secondary DNS	

Static IP address

The router uses the fixed IP address, subnet mask, default gateway and DNS server information provided by the ISP to access the internet.

Configuration procedure

1. Log in to the web UI of the router, and navigate to **Network** > **Internet Settings.**
2. In the **Connection Settings** module, select **Static IP Address** for **Connection Type**.
3. Enter the **IP Address**, **Subnet Mask**, **Default Gateway**, **Primary DNS** and **Secondary DNS** provided by the ISP.
4. Click **Connect**.



----End

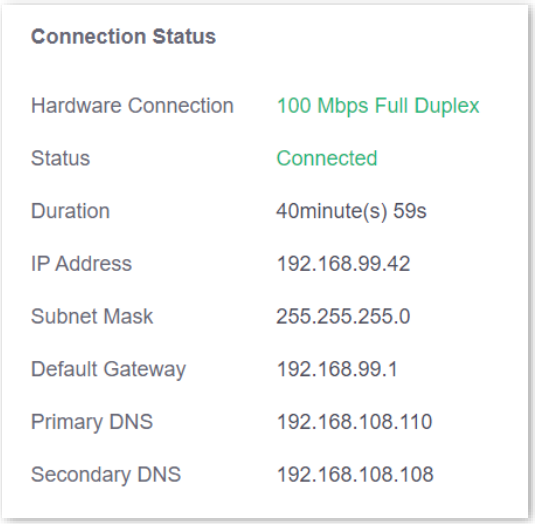
Wait for a moment. You can view related internet information in the **Connection Status** module.

Parameter description

Parameter	Description
IP Address	Enter the **IP Address**, **Subnet Mask**, **Default Gateway**, **Primary DNS** and **Secondary DNS** provided by the ISP. Tip If the ISP only provides one DNS address, the **Secondary DNS** is not required.
Subnet Mask	
Default Gateway	
Primary DNS	
Secondary DNS	

5.1.3 Check connection status

Log in to the web UI of the router, and navigate to **Network** > **Internet Settings** to enter the page. In the **Connection Status** module, you can view the network status of the corresponding WAN port IPv4, including the Ethernet port connection rate and duplex mode, connection status, duration and IP address. The following figure is for reference only.



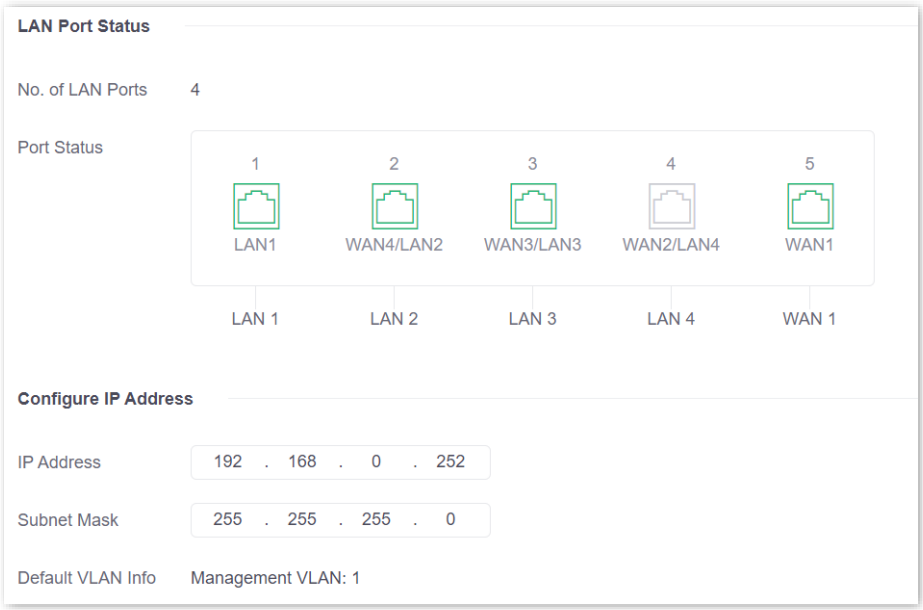
Parameter description

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

Parameter	Description
Default Gateway	Specifies the IPv4 gateway address of the WAN port.
Primary DNS	Specifies the primary DNS server address of the WAN port.
Secondary DNS	Specifies the secondary DNS server address of the WAN port.

5.2 LAN settings

Log in to the web UI of the router, and navigate to **Network** > **LAN Settings** to enter the page. You can view the router's LAN port connection status and configuration information on this page. And you can also set the IPv4 address information of the router's **VLAN_Default**.

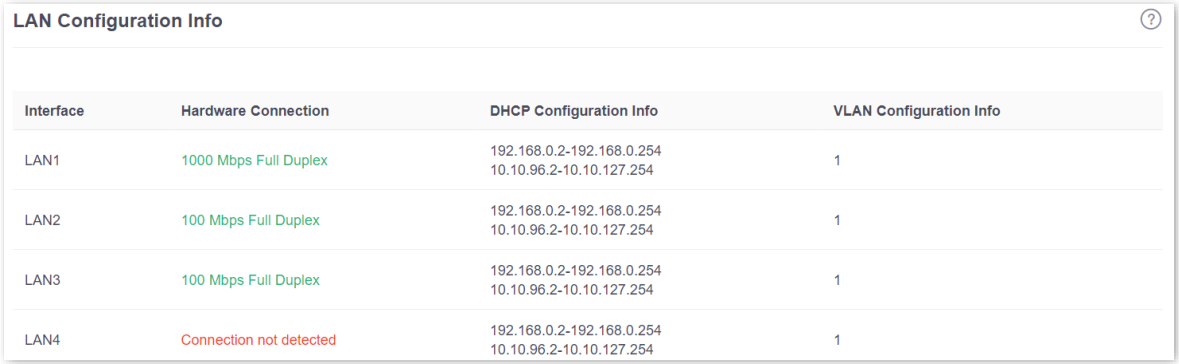


Parameter description

Parameter		Description
LAN Port Status	No. of LAN Ports	Specifies the number of current LAN ports.
	Port Status	Specifies the connection status of the port. : The port is connected properly. : The port is disconnected or not connected properly.
Configure IP Address	IP Address	Specifies the IPv4 address of the **VLAN_Default**. Devices connected to the **VLAN_Default** can access the IPv4 address to log in to the web UI of the router through the **http** (default) or **https** protocol. The default address is **192.168.0.252**. Tip After modifying the IP address, you need to disable and then enable the network adapter of your computer to enable the network adapter to obtain the IP address again.
	Subnet Mask	Specifies the subnet mask of the **VLAN_Default**.
	Default VLAN Info	Specifies the VLAN ID of the **VLAN_Default** of the router.

5.3 LAN configuration info

Log in to the web UI of the router, and navigate to **Network** > **LAN Configuration Info** to enter the page. On this page, you can view the configuration of the LAN port.



Parameter description

Parameter	Description
Interface	Specifies the LAN port of the router.
Hardware Connection	Specifies the connection status of the LAN port. – **Connection not detected** in red indicates that the Ethernet cable is not properly connected. – The description in green indicates that the Ethernet cable is properly connected. – **Obtaining** in yellow indicates that the Ethernet cable is connected and the rate is being negotiated.
DHCP Configuration Info	Specifies the IP address range that the DHCP server of the LAN port allocates to its clients. You can modify the IP address range in Network > DHCP Settings > **DHCP Server**.
VLAN Configuration Info	Specifies the VLAN to which the LAN port belongs.

5.4 VLAN settings

5.4.1 Overview

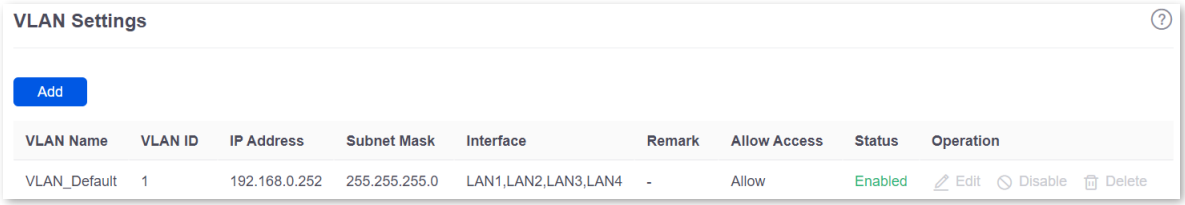
VLAN, abbreviated for Virtual Local Area Network, is a technology which divides LAN devices into different network segments logically rather than physically to create virtual work groups. It is used to divide the work stations in the switch-formed network into logical groups among which broadcast is 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: Users can create virtual work groups irrespective of physical network range with VLAN. Users can still access the network without having to change network configurations as long as they remain within the virtual work group even if his or her physical location changed.

Log in to the web UI of the router, and navigate to **Network** > **VLAN Settings** to enter the page. On this page, you can configure VLAN rules.

By default, the router has created a VLAN named **VLAN_Default**, and its VLAN ID is **1**, which cannot be deleted. If VLAN=1, there is no VLAN information, only the data of the LAN port without VLAN is processed. If VLAN≠1, only the data of the LAN port with VLAN is processed.



Parameter description

Parameter	Description
VLAN Name	Specifies the name of each added VLAN ID.

Parameter	Description
VLAN ID	Specifies the identifier of virtual local area network (VLAN) and is used to separate subordinate LANs inside a LAN. Each ID represents a LAN.  If the VLAN ID is **1**, it means that there is no VLAN information, and only data without Tag is processed.
IP Address	Specifies the VLAN IP address. Devices connecting to the port can access the web UI of the router using the IP address.
Subnet Mask	Specifies the subnet mask of the VLAN.
Interface	Specifies the physical ports that belong to the VLAN. Select at least one port.
Remark	Specifies the description of the VLAN.
Allow Access	Specifies whether clients from other VLANs can access services of this VLAN. – **Allow** indicates that clients from other VLANs can access services of this VLAN. – **Forbid** indicates that clients from other VLANs cannot access services of this VLAN.
Status	Specifies the current status of the VLAN, including **Enabled** and **Disabled**.
Operation	Used to edit, enable, disable or delete the VLAN. Edit: Used to modify the VLAN. Enable: Used to enable the VLAN. Disable: Used to disable the VLAN. Delete: Used to delete the VLAN.

5.4.2 Example of configuring the VLAN

Networking requirements

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

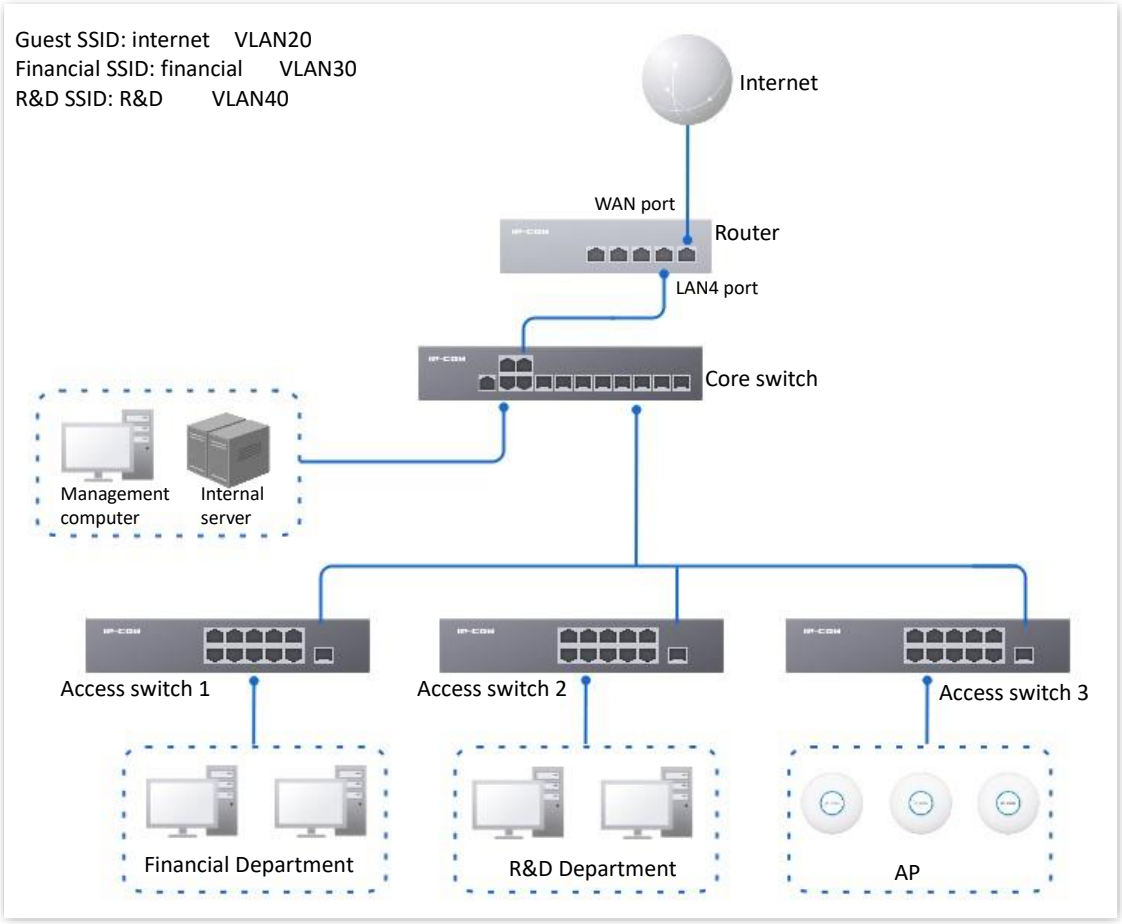
Visitors, departments and staff are required to access networks that are isolated from each other and have different network permissions.

- Guests can only access the internet and are isolated from other networks when accessing the wireless network.
- Staff of the Financial Department support access to wired and wireless networks, which can only access the intranet and are isolated from other networks.
- Staff of the R&D Department support access to wired networks and wireless networks, which can only access the intranet and are isolated from other networks.

Solution

- Successfully manage the AP on the router, and deliver different wireless policies to the AP.
- Configure the SSID policy for guest connection. The SSID is **internet**. The wireless password is **UmXmL9UK**, and the VLAN ID is **20**.
- Configure the SSID policy for staff of the Financial Department. The SSID is **Financial**. The wireless password is **CetTLb8T**, and the VLAN ID is **30**.
- Configure the SSID policy for staff of the R&D Department. The SSID is **R&D**. The wireless password is **ZeFtub6m**, and the VLAN ID is **40**.
- Divide the wired network connected by the staff of the Financial Department into VLAN30.
- Divide the wired network connected by the staff of the R&D Department into VLAN40.
- Configure VLAN forwarding rules on the switch.
- Configure VLAN forwarding rules on the router and the internal server.

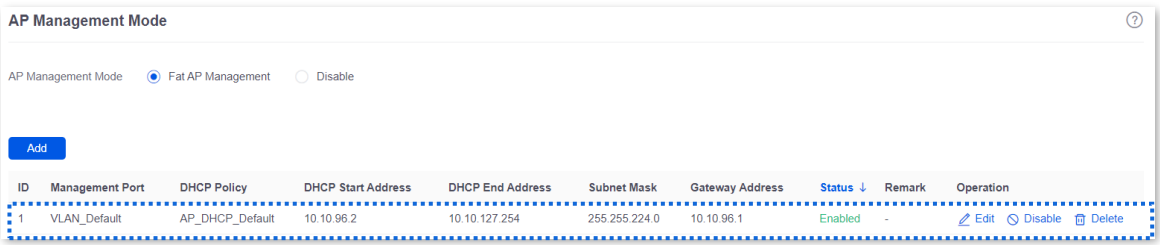
The network topology is as follows.



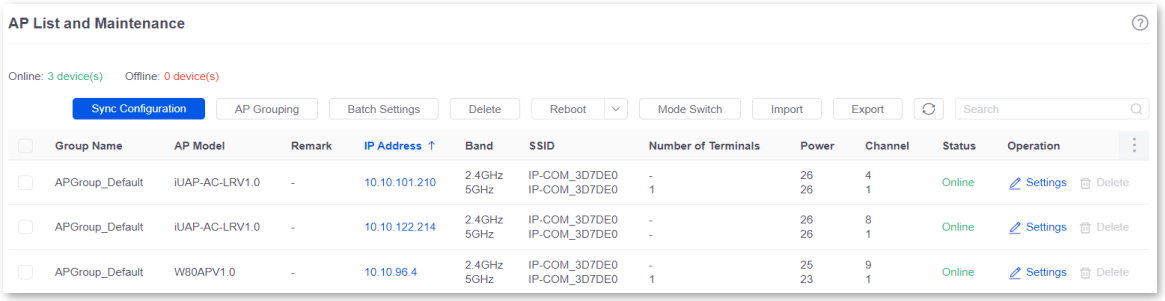
Configuration procedure

I. Set the router.

1. Log in to the web UI of the router.
2. Manage the AP (Skip if performed).
   1) Navigate to **More** > **Maintenance Service** > **AP Management Mode**.
   2) Set **AP Management Mode** to **Fat AP Management** .
   3) Click **Add** to add the DHCP policy **AP_DHCP_Default** for the management port **VLAN_Default.**



Navigate to **AP** > **AP List and Maintenance,** you can view whether the router successfully manages the AP.



3. Add the VLAN and configure the DHCP server.

Examples of VLAN parameters are shown in the table below.

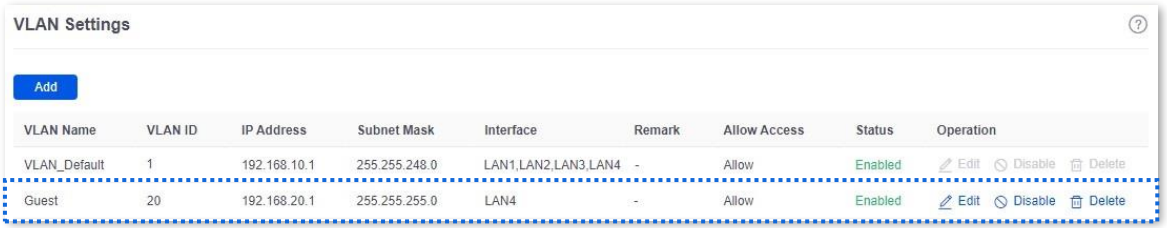
VLAN Name	VLAN ID	IP Address/Network Segment	Interface
Guest	20	192.168.20.1/24	LAN4

Examples of DHCP server parameters for the VLAN are shown in the following table.

Policy Name	Application Interface	User DHCP	AP DHCP
Guest	Guest	Client Address: 192.168.20.100 to 192.168.20.200 Subnet Mask: 255.255.255.0 Gateway: 192.168.20.1 Primary DNS: 192.168.20.1	/

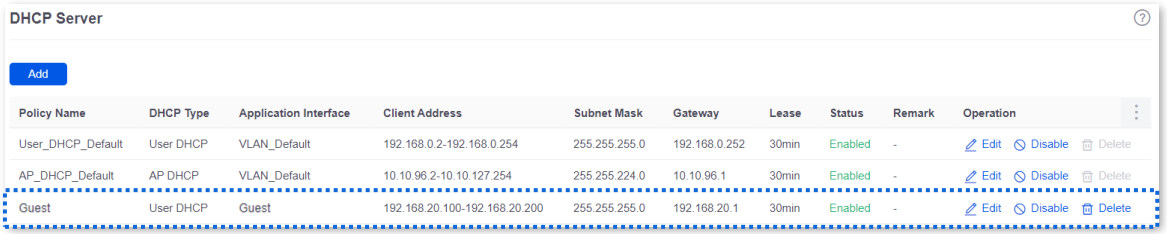
1) Add the VLAN.

Navigate to **Network** > **VLAN Settings,** click **Add** to configure related parameters of the VLAN, and click **Save**.



2) Configure the DHCP server for the VLAN.

Navigate to **Network** > **DHCP Settings** > **DHCP Server**, and click **Add** to configure related parameters of the user DHCP server for the VLAN **Guest**.



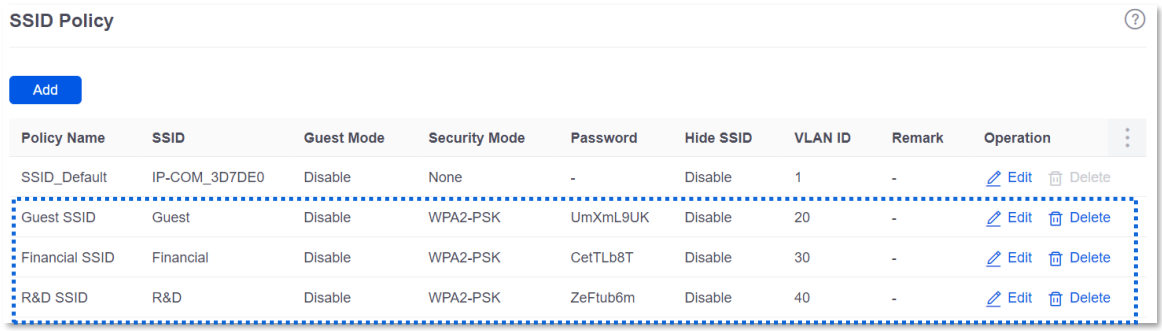
4. Configure the AP policy.

The following table provides the examples of AP policy parameters. Retain default values for other parameters that are not mentioned.

SSID Policy	RF Policy	AP Group Policy
Policy Name: Guest SSID SSID: internet Security Mode/ Encryption: WPA2-PSK/AES Password: UmXmL9UK VLAN ID: 20	RF_Default	Policy Name: Enterprise No. of SSIDs: 3 2.4G/5G SSID1 Policy: Guest SSID 2.4G/5G SSID2 Policy: Financial SSID 2.4G/5G SSID3 Policy: R&D SSID RF Policy: RF_Default VLAN policy: AP VLAN
Policy Name: Financial SSID SSID: Financial Security Mode/ Encryption: WPA2-PSK/AES Password: CetTLb8T VLAN ID: 30	RF_Default	
Policy Name: R&D SSID SSID: R&D Security Mode/ Encryption: WPA2-PSK/AES Password: ZeFtub6m VLAN ID：40	RF_Default	

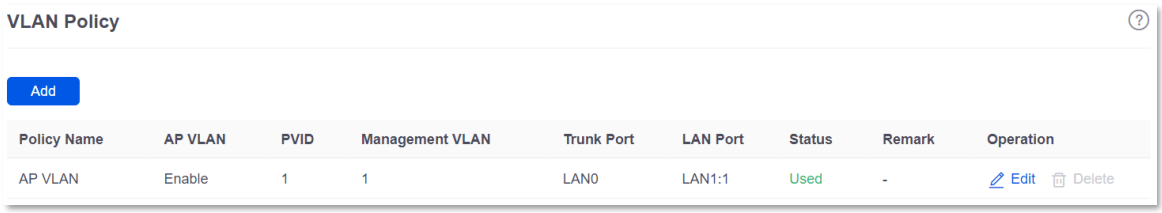
1) Configure the SSID policy.

Navigate to **AP** > **Wireless Policy** > **SSID Policy**, click **Add** to configure related parameters of the SSID policy, and click **Save**.



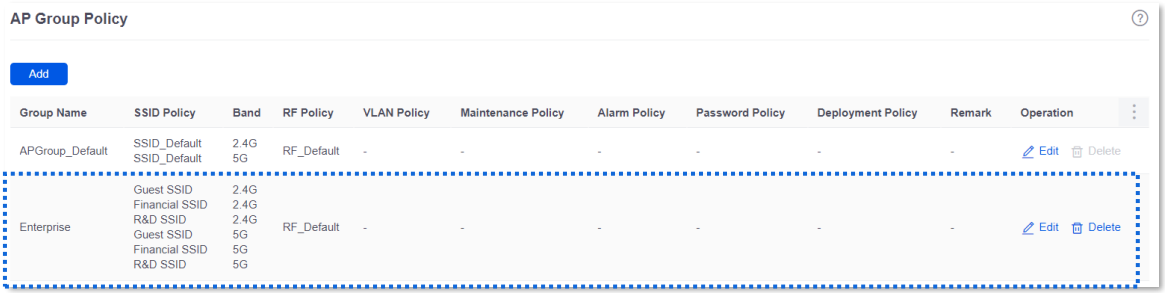
2) Configure VLAN policy.

Navigate to **AP** > **Wireless Policy** > **VLAN Policy**, click **Add**, enable **AP VLAN** and set **Trunk Port** to **LAN0**, and click **Save**.



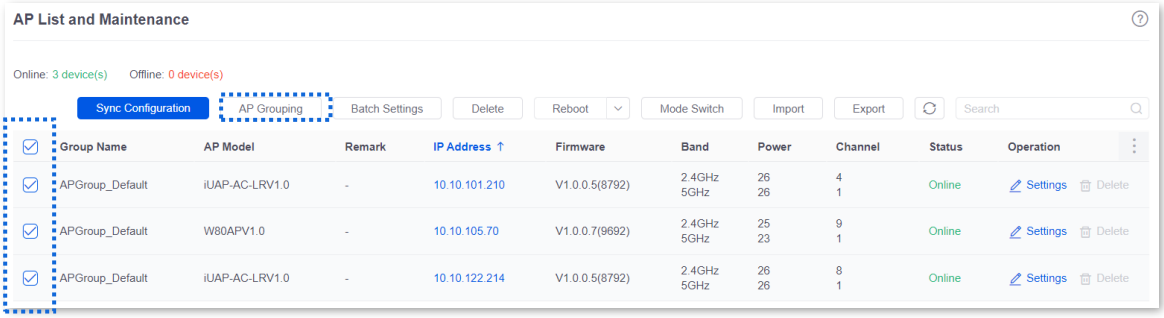
3) Configure the AP group policy.

Navigate to **AP** > **AP Group Policy**, click **Add** to configure related parameters of the AP group policy, and click **Save**.

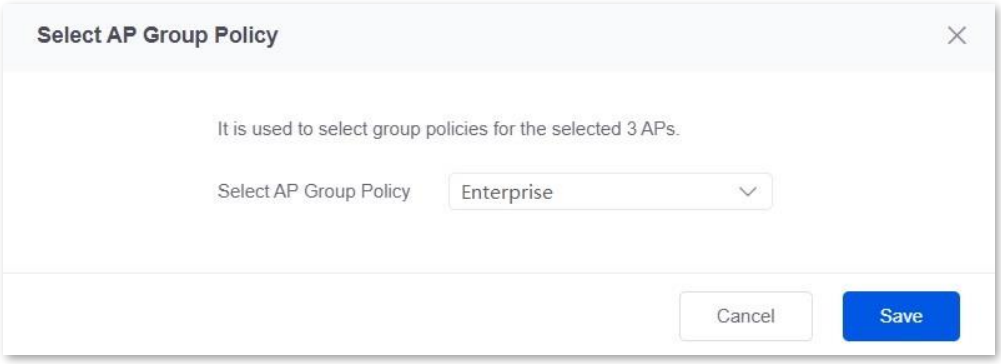


5. Deliver the AP group policy.

1) Navigate to **AP** > **AP List and Maintenance**, select the APs to which the AP group policy is to be delivered, and click **AP Grouping**.



2) Select the AP group policy, and click **Save.**



II. Configure the core switch.

Divide the IEEE 802.1q VLAN on the core switch as follows.

Port connected to	VLAN ID (VLAN allowed to pass)	Port Property	PVID
Router	20	Trunk	1
Internal Server	30,40	Trunk	1
Switch1 (Financial Department)	30	Access	30
Switch2 (R&D Department)	40	Access	40
Switch3 (AP)	20,30,40	Trunk	1

Retain the default settings for other ports that are not mentioned. For details about how to configure the switch, see the user guide of the switch.

III. Configure the internal server.

Add VLANs for ports connected to the switch and configure the DHCP server.

1. Add VLANs. The parameters in the following table are for reference only.

VLAN Name	VLAN ID	IP Address/Network Segment	Physical Port
Financial	30	192.168.30.1/24	LAN
R&D	40	192.168.40.1/24	LAN

2. Configure the user DHCP server for the VLAN. The parameters in the following table are for reference only.

Policy Name	User DHCP
Financial	Client Address: 192.168.30.100 to 192.168.30.200 Subnet Mask: 255.255.255.0 Gateway: 192.168.30.1 Primary DNS: 192.168.30.1
R&D	Client Address: 192.168.40.100 to 192.168.40.200 Subnet Mask: 255.255.255.0 Gateway: 192.168.40.1 Primary DNS: 192.168.40.1

3. Set the VLAN of the port connected to the switch.

Port connected to	VLAN ID（VLAN allowed to pass）	Port Property	PVID
Switch	30,40	Trunk	1

For details about how to configure the device, see the user guide of the corresponding device.

----End

Verification

- When the guests connect to the wireless network **internet**, enter the wireless password **UmXmL9UK** to access the internet and be isolated from other networks.
- When the staff of the Financial Department connect to the wireless network **Financial**, enter the wireless password **CetTLb8T** to access the intranet and be isolated from other networks.
- When the staff of the R&D Department connect to the wireless network **R&D**, enter the wireless password **ZeFtub6m** to access the intranet and be isolated from other networks.
- When the staff of the Financial Department access the wired network, they can access the intranet and are isolated from other networks
- When the staff of the R&D Department access the wired network, they can access the intranet and are isolated from other networks

5.5 DHCP settings

5.5.1 Overview

When users have the following network requirements, the IP address configuration of the network device can be completed through the DHCP server.

- The network scale is large, and the workload of manually configuring network parameters for each network device is also large.
- The number of devices on the network is far greater than the number of IP addresses that can be used by the network, while the number of devices accessing the internet at the same time is less.
- Only a few hosts in the network need fixed IP addresses.

The router provides a DHCP server, which can automatically assign IP address information to DHCP clients.

DHCP server

The IP address allocation mechanism is as follows:

1) When the router receives an IP address allocation request sent by the DHCP client, it queries the DHCP static allocation table according to the MAC address of the DHCP client. If the DHCP client is in the static allocation table, the corresponding IP address is assigned to the DHCP client; otherwise, the router will take the next step.
2) The router identifies the DHCP client type (user or AP) and the VLAN to which it belongs from the request message, and then selects the type of DHCP server policy corresponding to the VLAN according to the identified information to assign an IP address.

DHCP reservation

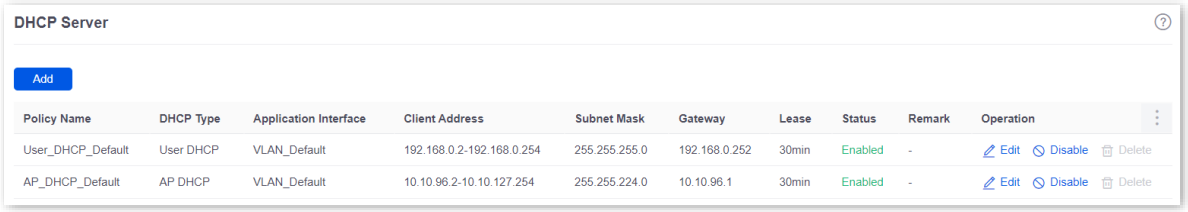
With the DHCP Reservation function, you can make the specified client always obtain the preset IP address, and avoid the functions such as **Internet Speed Control** and **Port Mapping** that take effect based on the IP address from becoming invalid due to the change of the client IP address.

Note

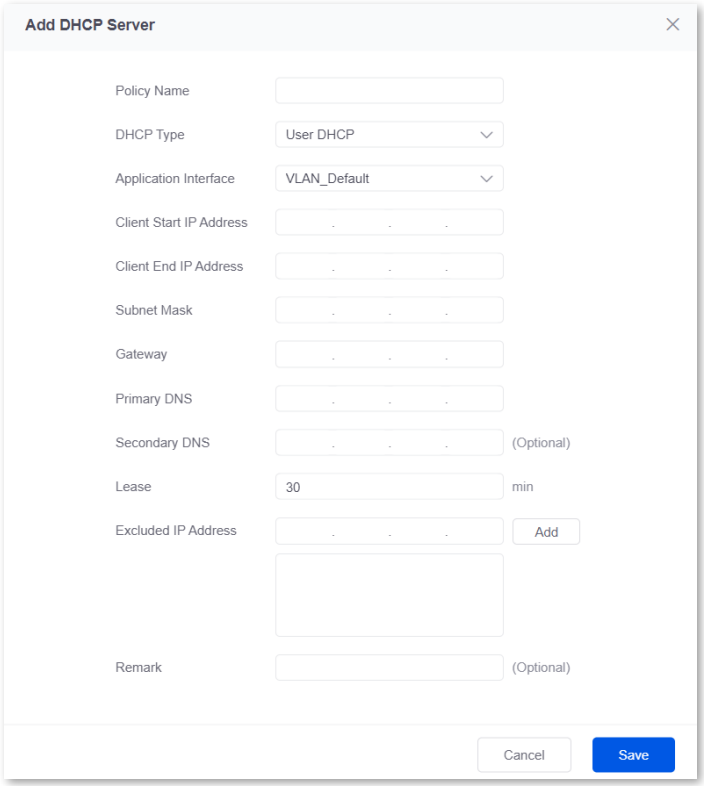
The DHCP Reservation function is mainly for users. If the AP is added to the DHCP reservation, the AP may obtain an IP address abnormally. To ensure the normal operation of the AP, do not add the AP to the DHCP reservation.

5.5.2 DHCP server

Log in to the web UI of the router, and navigate to **Network** > **DHCP Settings** > **DHCP Server** to enter the page. On this page, you can configure the DHCP server based on the VLAN. You can click ⋮ to select parameters to be displayed.



By default, the router has created two DHCP server policies named **User_DHCP_Default** and **AP_DHCP_Default**. You can click **Add** to add a new DHCP server policy.



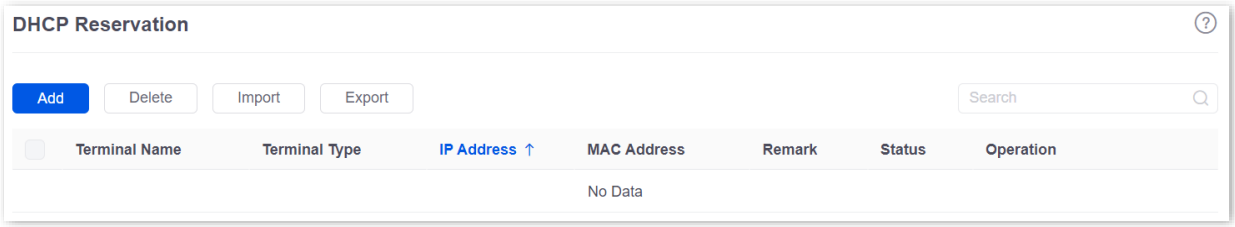
Parameter description

Parameter	Description
Policy Name	Specifies the name of the DHCP policy.
DHCP Type	Specifies the DHCP type of the router. The router supports two types of DHCP: User DHCP and AP DHCP. – **User DHCP**: Used to assign IP address to terminal devices. – **AP DHCP**: Used to assign IP addresses to IP-COM Aps.

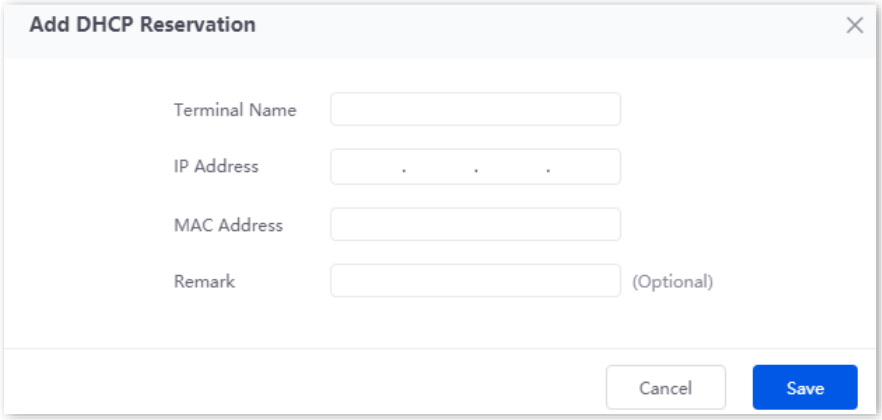
Parameter	Description
Application Interface	Specifies the VLAN for which the DHCP server rule takes effect. You can configure the VLAN on the VLAN settings page.
Client Address	Specifies the range of the DHCP address pool (range of IP addresses assigned by the DHCP server to its clients).
Client Start IP Address	Specifies the start IP address of the DHCP IP address pool (the IP address range that the DHCP server can assign to its clients).
Client End IP Address	Specifies the end IP address of the DHCP IP address pool.
Subnet Mask	Specifies the subnet mask that the DHCP server assigns to its clients.
Gateway	Specifies the gateway address that the DHCP server assigns to its clients.
Primary DNS	Specify the IP addresses of the primary and secondary DNS servers that are assigned to the device in the LAN by the DHCP server. Note For the LAN devices to access the internet properly, ensure that the primary/secondary DNS you entered is the correct IP address of the DNS server or proxy. Secondary DNS can be left blank.
Secondary DNS	
Lease	Specifies the validity period of the IP address the DHCP server assigns to clients. – When the IP address of a client expires but the client is still connected to the router, auto-renewal happens and the client continues to occupy that IP address. – If the client is disconnected (turned off, Ethernet cable disconnected or wireless network disconnected) from the router, the router will release the IP address and make it available for other clients in case they request IP address information as well.
Excluded IP Address	Specifies the IP address assigned to terminals does not include the excluded address.
Status	Specifies the status of the DHCP server, including **Enabled**, **Disabled** and **Expired**.
Remark	Specifies the description of the DHCP server policy.

5.5.3 DHCP reservation

Log in to the web UI of the router, and navigate to **Network** > **DHCP Settings** > **DHCP Reservation** to enter the page. On this page, you can configure the DHCP static assignment rules and also import/export static IP address lists.



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



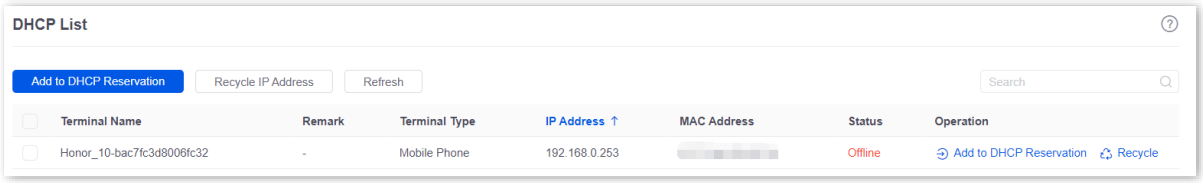
Parameter description

Parameter	Description
Terminal Name	Specifies the name of the terminal.
Terminal Type	Specifies the terminal types such as Mobile Phone, PAD and PC. If the terminal type is not recognized, **Others** will be displayed.
IP Address	Specifies the fixed IP address to be assigned to the terminal.
MAC Address	Specifies the MAC address of the terminal. A MAC address can be specified in the following format: 00:23:24:E8:14:5A, 00-23-24-E8-14-5A or 002324E8145A.
Remark	Specifies the description of the assigned static IP address.
Status	Specifies the status of the DHCP reservation, including **Enabled**, **Disabled** and **Expired**.
Import	Used to import CSV files for adding DHCP static assignment rules.
Export	Used to export DHCP static assignment rules to your local computer as a CSV file. Tip To modify the exported file, open the file as a txt file.

5.5.4 DHCP list

Log in to the web UI of the router, and navigate to **Network** > **DHCP Settings** > **DHCP List** to enter the page. On this page, you can perform the following operations on the terminal device that obtains the IP address from this router:

- To view device information such as the terminal name and obtained IP address of the device.
- The terminal devices with assigned IP addresses can be added to the static allocation list individually or in batches, so that the DHCP server always assigns the same IP address to the terminal devices.
- When the device is offline and the lease has not expired, you can manually reclaim the IP address to the address pool for allocation to other devices.



Parameter description

Parameter	Description
Terminal Name	Specifies the name of the terminal.
Remark	Specifies the description of the DHCP list.
Terminal Type	Specifies the terminal types such as Mobile Phone, PAD and PC. If the terminal type is not recognized, **Others** will be displayed.
IP Address	Specifies the IP address of the terminal.
MAC Address	Specifies the MAC address of the terminal.
Status	Specifies the status of the device, including **Online** and **Offline**.
Operation	Used to add to DHCP reservation and recycle. Add to DHCP Reservation : Used to assign the current IP address as a static IP address to the client. Recycle: Used to recycle IP addresses whose lease has not expired to the address pool for offline devices.

6 AP Management

6.1 Overview

The router integrates the functions of wireless controller to manage IP-COM fat APs, configure wireless networks for APs and maintain APs in batches. The workload of managing large-scale wireless networks can be greatly reduced.

To add an AP to the router

To be managed by the router, the AP needs to be found and added to the router. When the router is used as the main router, the AP can be added to the router as follows.

1. Enable the AP to obtain its own IP address.

   IP-COM fat APs support the DHCP client function. When the AP is enabled, the AP automatically obtains its own IP address, gateway IP address and IP address of the DNS server.

2. Enable the AP to obtain the IP address of the router.

   The router periodically broadcasts its IP address on the network. By monitoring the broadcast, the AP can obtain the IP address of the router.

3. Enable the AP to send a join request to the router.

   After obtaining the IP address of the router, the AP sends a join request to the IP address.

4. Enable the router to respond to the join request.

   After the router responds to the join request, the AP joins the router successfully.

6.2 Configuration wizard

Procedure	Task	Description
1	Set AP management mode	Optional. By default, the AP management mode of the router has been set to **Fat AP Management**, and the **AP_DHCP_Default** policy has been added to the **VLAN_Default** interface.
2	Configure network	Optional. By default, the router has created a VLAN interface named **VLAN_Default**. The IP address of this interface is **192.168.0.252** and the user DHCP and AP DHCP service are enabled.
3	Configure wireless policies	Optional. By default, the router has created an SSID policy named **SSID_Default**, an RF policy named **RF_Default**.
4	Configure AP group policy	Optional. By default, the router has created an AP group policy named **APGroup_Default**.
5	Separate APs to AP groups	Optional. By default, the router has separated the managed APs to **APGroup_Default**. You can modify them based on actual situation.

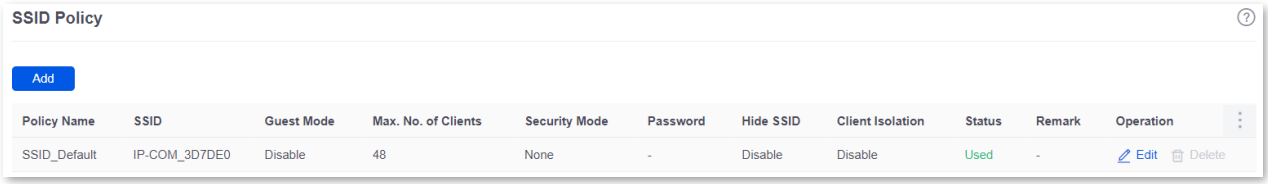
6.3 Wireless policy

On this page, you can configure policies for APs to be used in AP Group Policy in advance. The policies include the SSID policy, RF policy, VLAN policy and advanced policy.

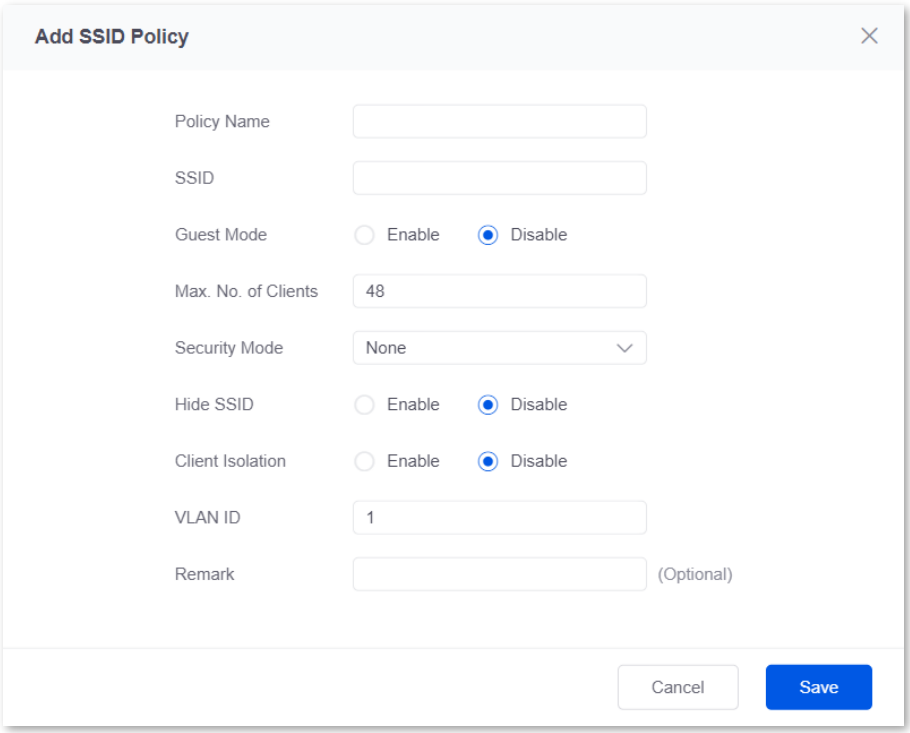
6.3.1 SSID policy

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

You can configure the SSID policy in **AP Management** > **Wireless Policy** > **SSID Policy**. You can click ⋮ to select parameters to be displayed.



By default, the router has created an SSID policy named **SSID_Default**. You can click **Add** to add a new SSID policy.



Parameter description

Parameter	Description
Policy Name	Specifies the name of the SSID policy.
SSID	Specifies the name of the WiFi network.

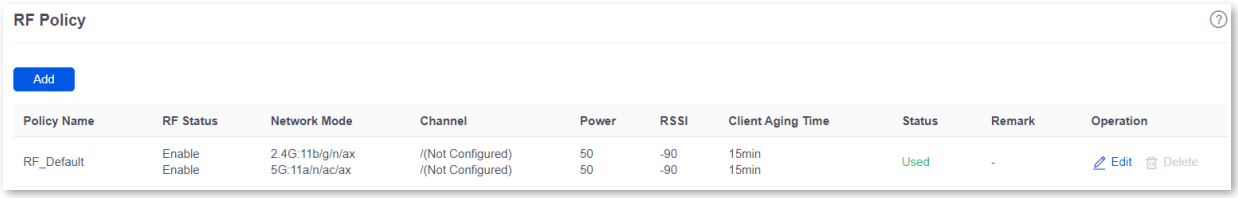
Parameter	Description
Guest Mode	After enabling, the SSID is used as guest network. Users connected to the SSID can only access the internet, but cannot access each other or LAN.
Max No. of Clients	Specifies the maximum number of clients allowed to connect to the WiFi network.  Generally, the maximum number of IP-COM clients is **128**. If you want to deliver multiple SSID policies to the same AP, you need to plan the maximum number of clients of each policy in advance. Ensure the sum of maximum number of clients of the SSID policies does not exceed 128.
Security Mode	Specifies the security modes of the SSID policy. – **None**: It indicates that the wireless network has no password. For the security of the network, this option is not recommended. – **WPA-PSK** and **WPA2-PSK:** They indicate that WPA pre-shared keys are used for network authentication, which is ideal for individual and domestic scenarios. – **WPA3-SAE** and **WPA3-SAE/WPA2-PSK:** They indicate that the wireless network is authenticated with a WPA pre-shared key, which is more secure than WPA2. Some smartphones do not support WPA3, so **WPA3-SAE/WPA2-PSK** is recommended. – **WPA** and **WPA2:** They indicate that 802.1x is used for network authentication and generating root keys to encrypt data, which is suitable for scenarios with high security requirements such as enterprises.
Encryption	Specifies the encryption when the security mode is WPA-PSK, WPA2-PSK, WPA3-SAE, WPA3-SAE/WPA2-PSK, WPA and WPA2. – **AES**: Specifies the Advanced Encryption Standard. – **TKIP**: Specifies the Temporal Key Integrity Protocol. Under **TKIP** mode, the AP can only use a lower rate (maximum 54 Mbps) than under **AES** mode. – **TKIP&AES**: Specifies that both the **AES** and **TKIP** are compatible.  **WPA3-SAE** only supports **AES**.
Password	Specifies the pre-shared keys when the security modes are WPA-PSK, WPA2-PSK, WPA3-SAE and WPA3-SAE/WPA2-PSK. The users need to enter wireless password when connecting to the SSID.
Key Update Interval	Specifies the key update interval when the security mode is WPA-PSK, WPA2-PSK, WPA3-SAE and WPA3-SAE/WPA2-PSK. A short key update interval can enhance the security of WPA data.

Parameter	Description
Radius Server Address	Specify the IP address, shared key and authentication port of RADIUS Server. They are required only when **Security Mode** is set to **WPA** or **WPA2**.
Authentication Key	
Authentication Port	
Hide SSID	Used to enable or disable the function of hiding 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.
Client Isolation	Used to enable or disable the function of **Client Isolation**. With the **Client Isolation** enabled, terminals cannot access each other.
VLAN ID	Specifies the VLAN to which the SSID belongs. The default **VLAN ID** is **1**, which means no VLAN is configured.
Status	Specifies the status of the SSID policy.
Remark	Specifies the introduction to the SSID policy. The remark is optional.
Operation	Used to edit or delete an SSID policy. Edit **:** Used to modify the policy. Delete **:** Used to delete the policy. Tip Generally, keep at least one SSID policy, so the last policy cannot be deleted. The policy in use cannot be deleted. Remove the policy reference before deleting a policy in use.

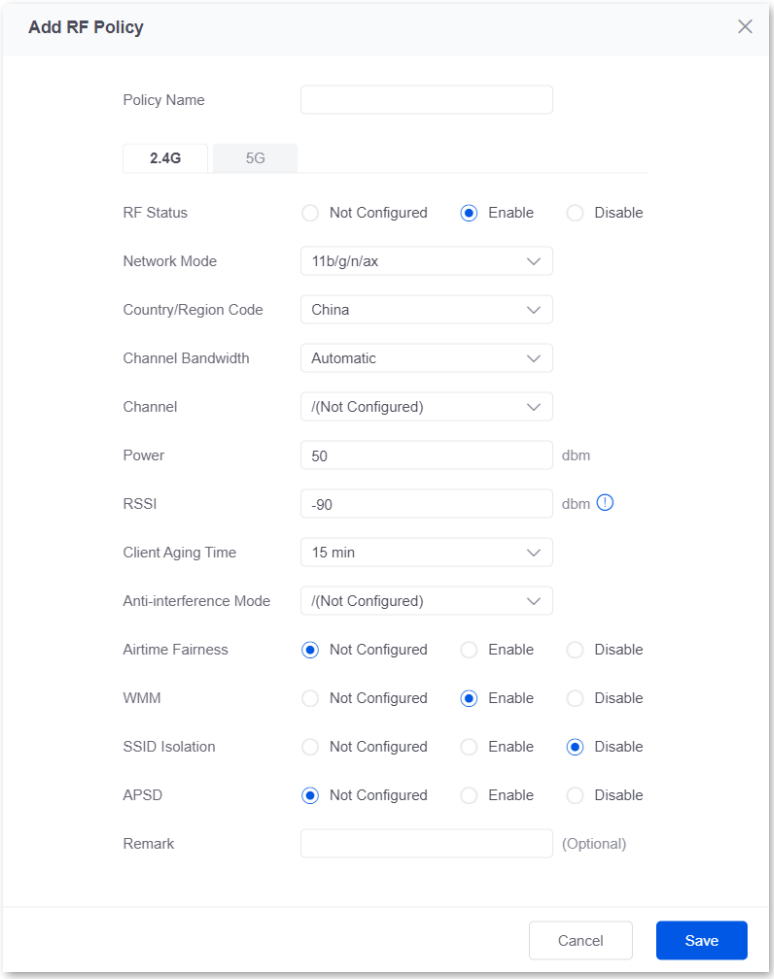
6.3.2 RF policy

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

You can configure the RF policy in **AP Management** > **Wireless Policy** > **RF Policy**.



By default, the router has created an RF policy named **RF_Default**. You can click **Add** to add a new RF policy.



Parameter description

Parameter	Description
Policy Name	Specifies the name of the RF policy.
2.4G	Specify the parameters for RF policies under 2.4 GHz and 5 GHz WiFi networks.

Parameter	Description
5G	
RF Status	Specifies the status of the WiFi function. **Not Configured** indicates that the RF status of the corresponding frequency band of the AP is not modified. – **Enable**: Select it to enable the WiFi function of the frequency band. – **Disable:** Select it to disable the WiFi function of the frequency band.
Network Mode	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 **11b/g/n/ax**. – **11b**: The AP works in 802.11b wireless network mode. – **11g**: The AP works in 802.11g wireless network mode. – **11b/g**: The AP works in 802.11b/g wireless network mode. – **11b/g/n**: The AP works in 802.11b/g/n wireless network mode. – **11b/g/n/ax**: The AP works in 802.11b/g/n/ax wireless network mode. Network modes of the 5 GHz frequency band include **11a**, **11a/n**, **11ac**, and **11a/n/ac/ax**. – **11a**: The AP works in 802.11a wireless network mode. – **11a/n**: The AP works in 802.11a/n wireless network mode. – **11ac**: The AP works in 802.11ac wireless network mode. – **11a/n/ac/ax**: The AP works in 802.11a/n/ac/ax wireless network mode.
Country/Region Code	Specifies the country or region where the AP is located. Please select the correct country or region.
Channel Bandwidth	Specifies the bandwidth of the working channel. A high channel bandwidth means a higher transmission rate, but the penetration capability is reduced and the transmission distance is shortened. – **Automatic**: The AP automatically adjusts the channel bandwidth based on the surrounding environment. – **20M**: The AP uses the 20 MHz channel bandwidth. – **40M**: The AP uses the 40 MHz channel bandwidth. – **80M:** This channel bandwidth is available for the 5 GHz only. The AP uses the 80 MHz channel bandwidth. – **160M:** This channel bandwidth is available for the 5 GHz only. The AP uses the 160 MHz channel bandwidth. Tip **20M** is available for each network mode. **40M** is available for **11b/g/n**, **11b/g/n/ax**, **11a/n**, **11ac** and **11a/n/ac/ax**. **80M** is available for **11ac** and **11a/n/ac/ax**. **160M** is only available for **11a/n/ac/ax**.

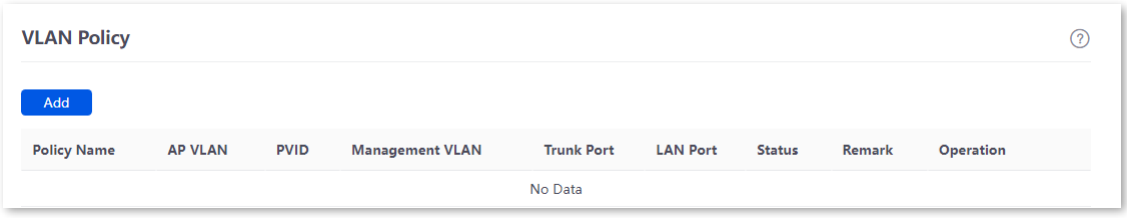
Parameter	Description
Channel	Specifies the channel in which the wireless data is transmitted and received. The available channels are determined by the current country/region and wireless band. – **/(Not Configured):** Retain the current configurations of the AP. – **Automatic**: The AP automatically detects the occupation rate of channels and selects the appropriate working channel accordingly. If the connection drops, freezes 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 a low occupation rate and little interference using software tools (such as WiFi analyzer).
Power	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	Specifies the minimum wireless signal strength can be received by the band. Clients with a lower signal strength value cannot connect to the AP. When there are multiple APs in the surroundings, an appropriate **RSSI** value helps ensure wireless clients connect to the APs with a stronger signal.
Client Aging Time	If a client generates no data communication within this time after connecting to the WiFi network, the AP will cut this client off.
Anti-interference Mode	Interference mitigation mode of this device. Only supported in 2.4 GHz. – **0**: Interference suppression measures are disabled. – **1**: Suppress same frequency interference for weak radio environment, such as the same frequency interference caused by microwave ovens, smartphones and bluetooth devices. – **2**: Forcibly suppress moderate interference for bad radio environment when the number of wireless signal interference sources is less than 30. – **3**: Automatically suppress critical interference for heavy loading radio environment. – **4:** Automatically suppress critical interference and reduce noise when the number of wireless signal interference sources is more than 30, such as high-density scenarios. – **/(Not Configured)**: The router does not deliver the anti- interference mode configuration to the AP. The AP uses the anti-interference mode configured on its web UI.
Airtime Fairness	If this function is enabled, the same download time is assigned to users experiencing different download rates, ensuring a better experience for high-rate users.
WMM	Specifies the WiFi Multi-media, which provides basic solutions for wireless QoS. When this function is enabled, audio and video data are forwarded in priority. To improve the performance of AP in wireless multimedia data transmission (for example, online videos), this function is enabled by default.

Parameter	Description
SSID isolation	Used to enable or disable the SSID isolation function. When it is enabled, devices under different SSIDs cannot communicate with each other.
APSD	Specifies the 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 AP.
5G Preferred	If the client supports 2.4 GHz and 5 GHz, with this function enabled, 5 GHz is used in priority when the 5 GHz signal strength is not less than the RSSI value. Tip – This function is only available for the 5 GHz band. To use this function, the 2.4 GHz and 5 GHz bands of the AP must be enabled and the SSID, encryption mode and passwords for the 2.4 GHz and 5 GHz bands must be consistent. – 5GHz Priority Threshold is configured on the web UI of the AP.
Status	Specifies the status of the RF policy.
Remark	Specifies the introduction to the RF policy. The remark is optional.
Operation	Used to edit or delete an RF policy. Edit: Used to modify the policy. Delete: Used to delete the policy. Tip Generally, keep at least one RF policy, so the last policy cannot be deleted. The policy in use cannot be deleted. Remove the policy reference before deleting a policy in use.

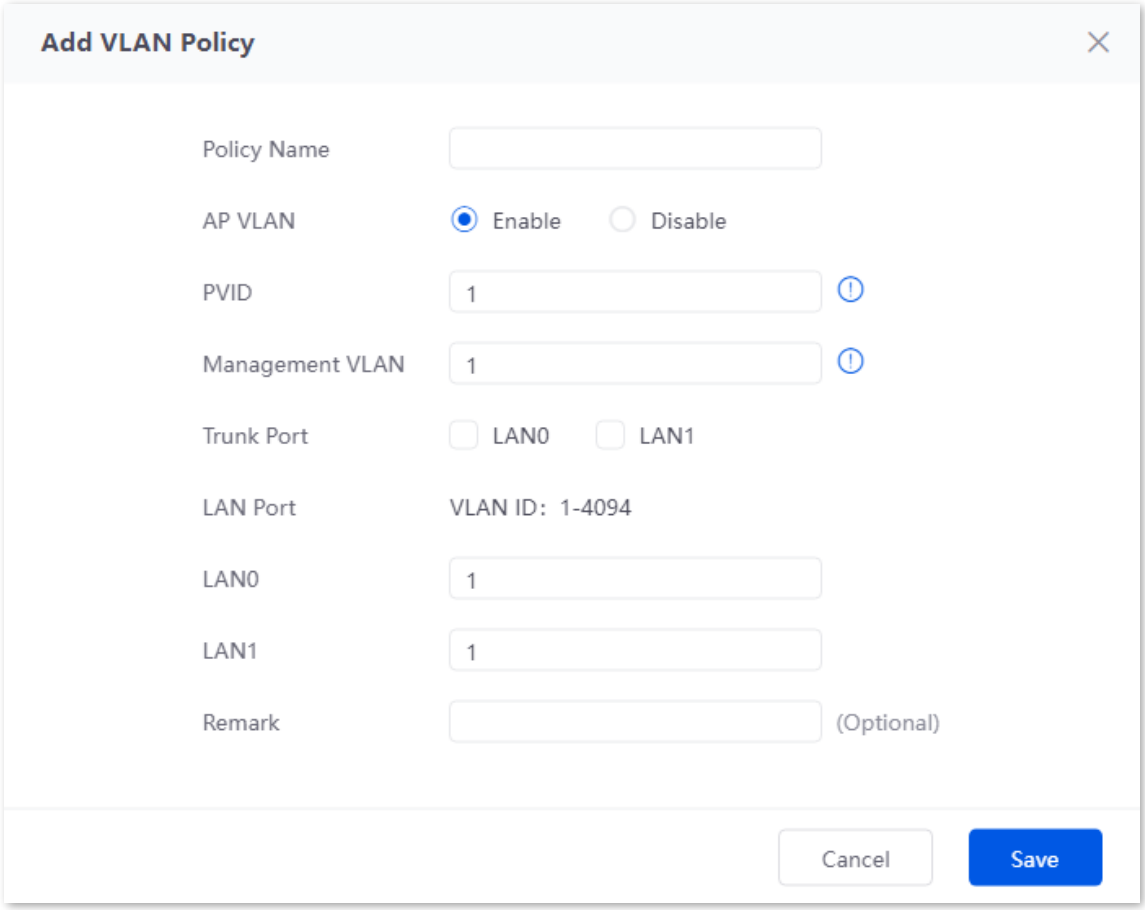
6.3.3 VLAN policy

VLAN policy is used to configure the basic VLAN parameters of the AP.

You can configure the VLAN policy in **AP Management** > **Wireless Policy** > **VLAN Policy** to associate the VLAN-related settings of the AP (such as the enabling status of the AP VLAN, management VLAN and Trunk port).



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



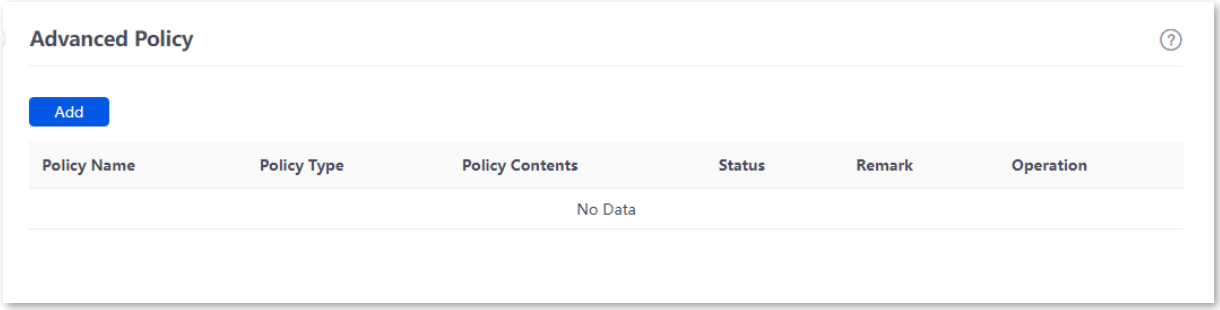
Parameter description

Parameter	Description
Policy Name	Specifies the name of the VLAN policy.
AP VLAN	Used to enable the 802.1Q VLAN function of the AP.
PVID	Specifies the ID of the default native VLAN of the trunk port of the AP. After the QVLAN function is enabled, the LAN port is the trunk port. The traffic of all VLANs can pass through a trunk port. Its default value is 1.
Management VLAN	Specifies the ID of the management VLAN. The default value is 1. After changing the management VLAN, you can manage the AP only after connecting the router to the new management VLAN and you can log in to the web UI of the AP again only after connecting your client (such as the management computer) to the new management VLAN.

Parameter	Description
Trunk Port	Used to select the trunk port(s) that allow data of all VLANs to pass. Tip After the 802.1Q VLAN function is enabled, at least one LAN port needs to be selected as the Trunk port. If this policy is applied for only one LAN port, set LAN0 as the Trunk port. Otherwise, the configuration may fail.
LAN Port	Specifies the VLAN ID of the wired LAN port (non-Trunk port) of the AP. This parameter is required only when the AP that uses the current policy has two LAN ports. The wired LAN port that cannot be modified is the Trunk port. Tip After the 802.1Q VLAN function is enabled, the wired LAN port (non-Trunk port) and wireless port of the SSID are Access ports. Their PVIDs are the same as their own VLAN IDs.
Status	Specifies the status of the VLAN policy.
Remark	Specifies the introduction to the VLAN policy. The remark is optional.
Operation	Used to edit or delete a VLAN policy. Edit: Used to modify the policy. Delete: Used to delete the policy. Tip Generally, keep at least one VLAN policy, so the last policy cannot be deleted. The policy in use cannot be deleted. Remove the policy reference before deleting a policy in use.

6.3.4 Advanced policy

You can configure advanced policies (including maintenance policies, alarm policies, password policies and deployment policies) in **AP Management** > **Wireless Policy** > **Advanced Policy**.



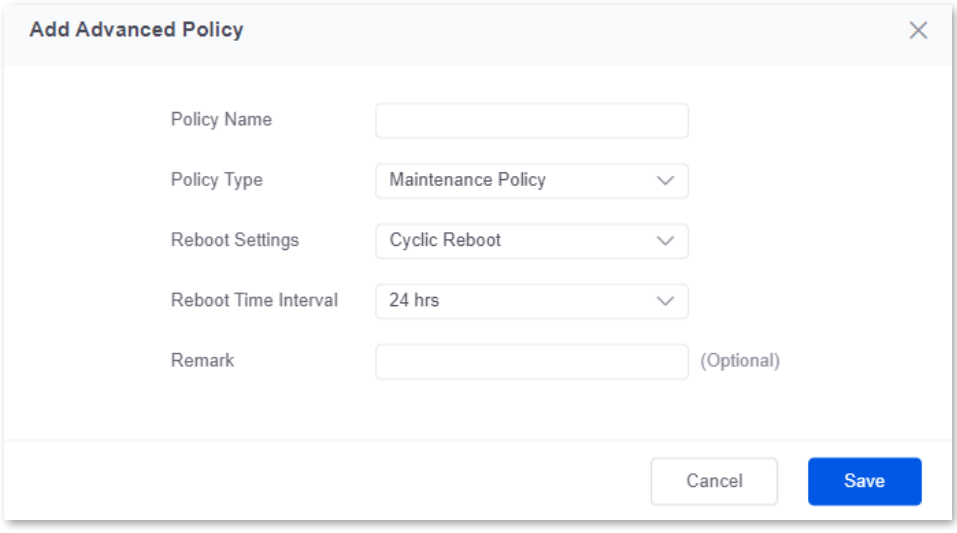
Parameter description

Parameter	Description
Policy Name	Specifies the name of the advanced policy.
Policy Type	Specifies the type of advanced policy, including **Maintenance Policy**, **Alarm Policy**, **Password Policy** and **Deployment Policy**.
Policy Contents	Specifies the contents of the policy.
Status	Specifies the status of the advanced policy.
Remark	Specifies the introduction to the advanced policy. The remark is optional.
Operation	Used to edit or delete an advanced policy. Edit: Used to modify the policy. Delete: Used to delete the policy. Tip The policy in use cannot be deleted. Remove the policy reference before deleting a policy in use.

Maintenance policy

This policy is used to configure the customized reboot parameters of the AP. Rebooting the AP can make it work with high performance. It is recommended that the AP be automatically rebooted during idle periods.

To enter the page, navigate to **AP** > **Wireless Policy** > **Advanced Policy**. You can click **Add** to add a new maintenance policy.



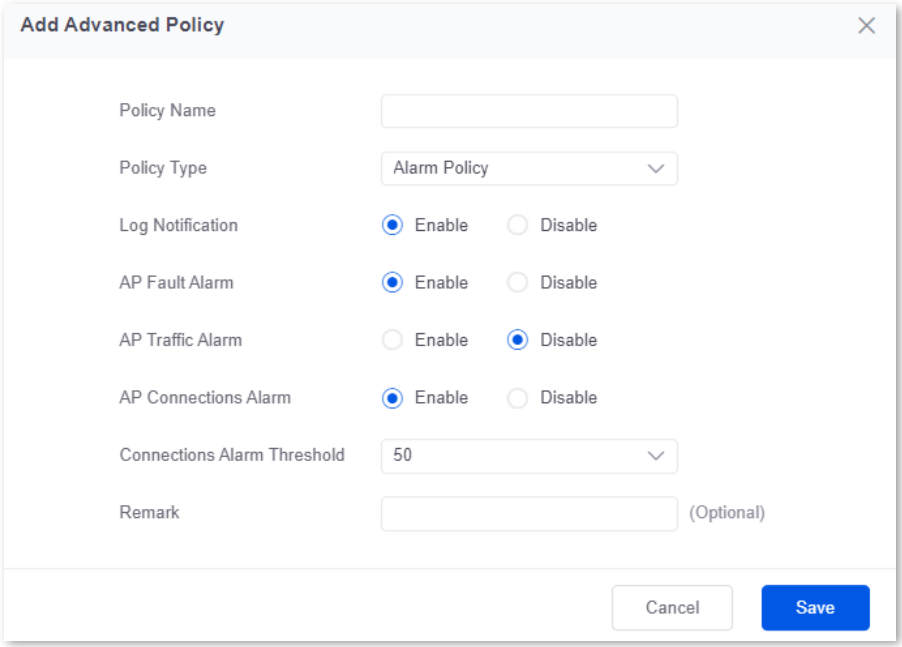
Parameter description

Parameter	Description
Policy Name	Specifies the name of the maintenance policy.
Policy Contents	Specifies the contents of the policy.
Reboot Settings	Specifies the type of maintenance policy. – **Scheduled Reboot**: The AP reboots once at the specified time point on the specified date(s). – **Cyclic Reboot:** The AP reboots once at the interval specified by **Reboot Time Interval**.
Time	Specify the reboot time of the AP when **Reboot Settings** is set to **Scheduled Reboot**.
Repeat	
Reboot Time Interval	Specifies the interval at which the AP reboots when **Reboot Settings** is set to **Cyclic Reboot**.
Status	Specifies the status of the policy.
Remark	Specifies the introduction to the policy. The remark is optional.

Alarm policy

On this page, you can configure alarm policies for the AP, so that the router will generate alarms after alarm events occur on the AP. The administrator can view such alarms to monitor the network status in real time.

To enter the page, navigate to **AP** > **Wireless Policy** > **Advanced Policy**. You can click **Add** to add a new alarm policy.



Parameter description

Parameter	Description
Policy Name	Specifies the name of the alarm policy.
Policy Contents	Specifies the contents of the policy.
Log Notification	Used to enable or disable the log notification. After it is enabled, the AP alarms will be displayed in **AP Alarm Log** and **Fat AP Running Log** in **Tool** > **Log Center** > **Running Log**.
AP Fault Alarm	Used to enable or disable the function of **AP Fault Alarm**. When it is enabled, if the AP is faulty (such as reboot, offline, online), the AP will send an alarm through the log.
AP Traffic Alarm	Used to enable or disable the function of **AP Traffic Alarm**. With this function enabled, when the total traffic exceeds the specified threshold, an alarm notification will be triggered. The notification can be sent by log.
Traffic Alarm Threshold	Specifies the threshold of the AP traffic alarm. When the total AP traffic exceeds the threshold, an alarm notification will be triggered.
AP Connections Alarm	Used to enable or disable the function of **AP Connections Alarm**. With this function enabled, when the number of AP connections exceeds the specified threshold, an alarm notification will be triggered. The notification can be sent by log.
Connections Alarm Threshold	Specifies the threshold of connections alarm. When the number of AP connections exceeds the threshold, an alarm notification will be triggered.

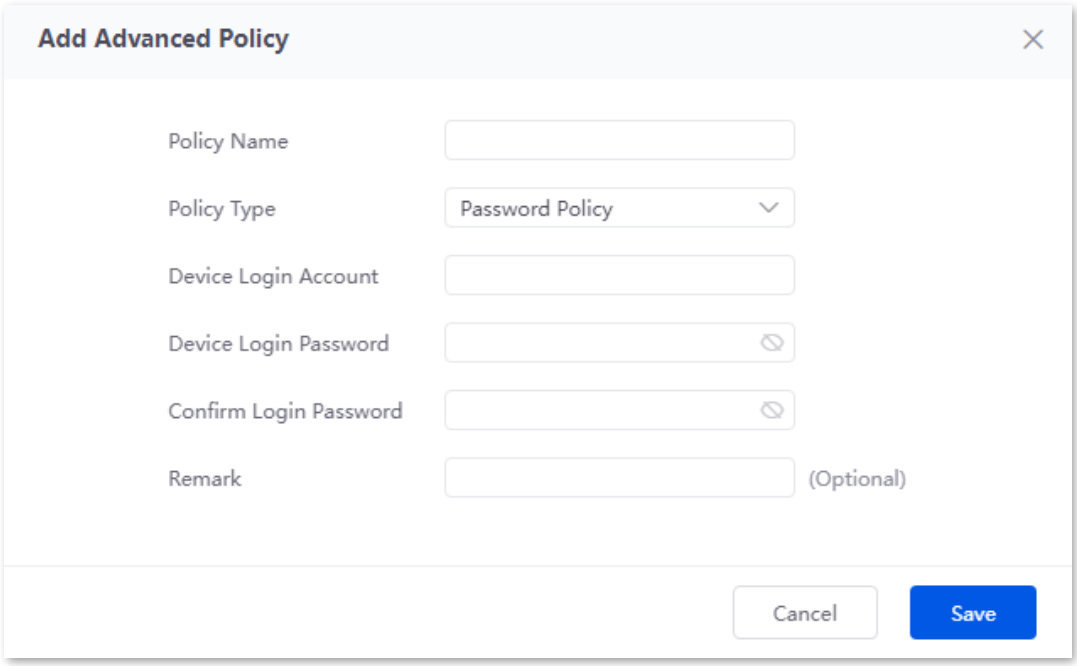
Parameter	Description
Status	Specifies the status of the policy.
Remark	Specifies the introduction to the policy. The remark is optional.

Password policy

On this page, you can configure password policies for the AP to preset the account and password used to log in to the web UI of the AP.

The default login account and password are **admin**. To prevent unauthorized users from entering the web UI of the AP and modifying settings, change the login account and password immediately upon your first login.

To enter the page, navigate to **AP** > **Wireless Policy** > **Advanced Policy**. You can click **Add** to add a new password policy.



Parameter description

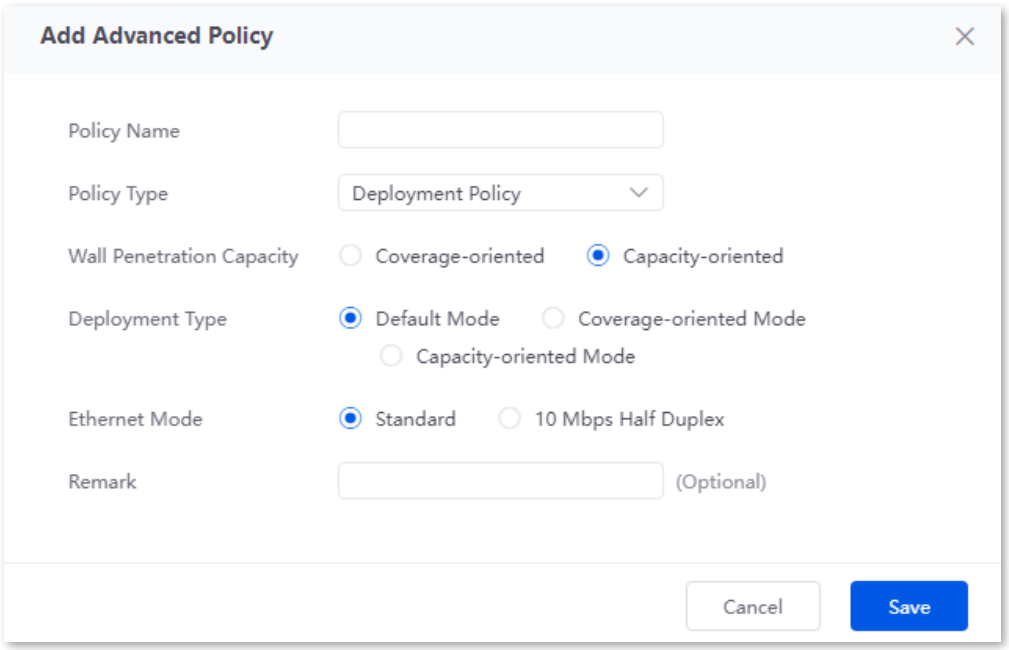
Parameter	Description
Policy Name	Specifies the name of the password policy.
Policy Contents	Specifies the contents of the policy.
Device Login Account	Specifies the login account of the AP.

Parameter	Description
Device Login Password	Specifies the login password of the AP.
Confirm Login Password	Used to confirm the login password of the AP.
Status	Specifies the status of the policy.
Remark	Specifies the introduction to the policy. The remark is optional.

Deployment policy

On this page, you can configure deployment policies for the AP to meet coverage requirements of different wireless network scenarios.

To enter the page, navigate to **AP** > **Wireless Policy** > **Advanced Policy**. You can click **Add** to add a new deployment policy.



Parameter description

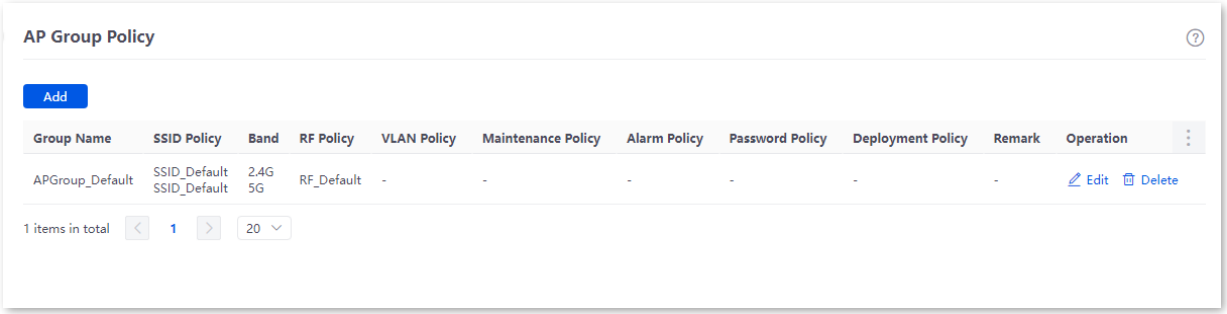
Parameter	Description
Policy Name	Specifies the name of the deployment policy.
Policy Contents	Specifies the contents of the policy.

Parameter	Description
Wall Penetration Capacity	Used to configure the wall penetration capacity of the AP. – **Coverage-oriented**: It is used to enhance the wall penetration capacity. It is applicable to scenarios with more walls. – **Capacity-oriented**: It is used to enhance the AP capacity in high-density scenarios. It is applicable to scenarios with few walls and more single users.
Deployment Type	Specifies the deployment type of the AP. – **Coverage-oriented Mode**: It is applicable to scenarios that require extensive coverage. – **Capacity-oriented Mode**: It is applicable to scenarios that require high density. – **Default Mode:** Used in environments between **Capacity-oriented** and **Coverage-oriented**.
Ethernet Mode	Used to configure the **Ethernet Mode** of the AP. – **Standard**: This mode indicates the auto-adaptive mode. – **10 Mbps Half Duplex**: When this mode is selected, the internet access mode is forced to 10 Mbps half duplex. – **10 Mbps Half Duplex** is recommended only when the length of the Ethernet cable between the AP PoE port and the peer device exceeds 100m to promote the driving distance of the Ethernet cable. Meanwhile, the working mode of the port of the peer device must be Auto-negotiation; otherwise, the AP PoE port may be unable to receive and send data normally.
Status	Specifies the status of the policy.
Remark	Specifies the introduction to the policy. The remark is optional.

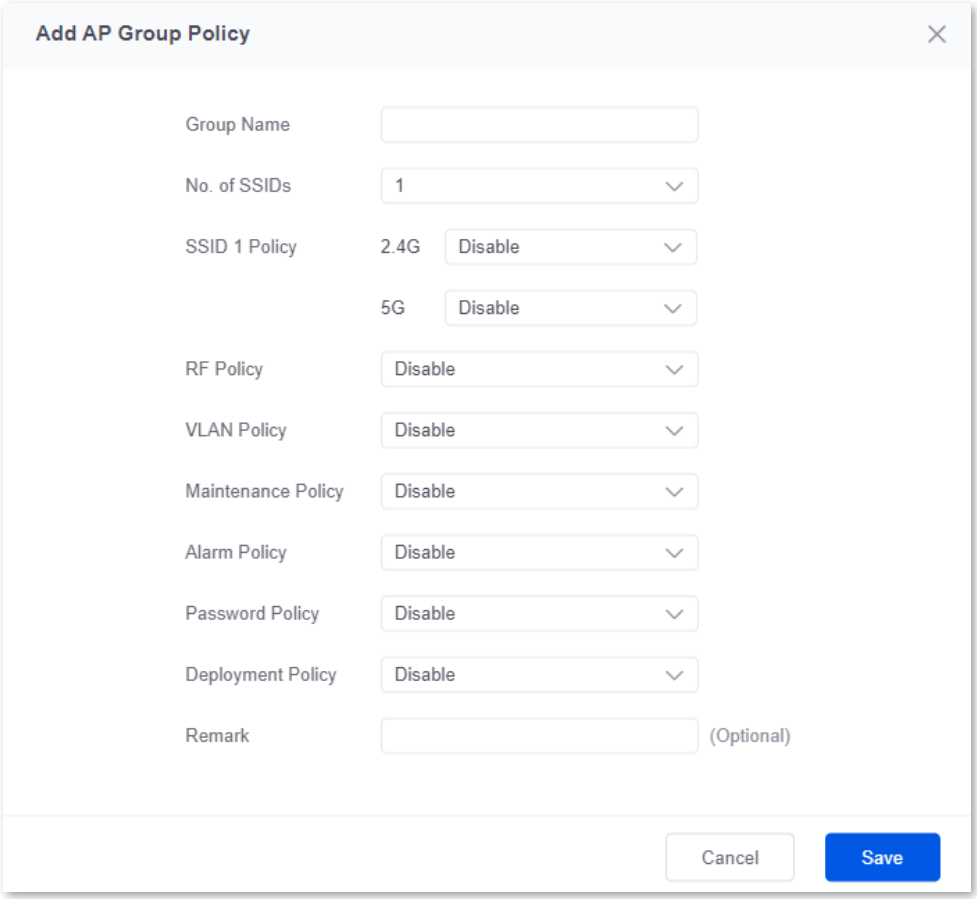
6.4 AP group policy

AP group policy is used to combine wireless policies and deliver them to corresponding APs.

You can configure the AP group policy in **AP Management** > **Wireless Policy** > **AP Group Policy**. You can click ⋮ to select parameters to be displayed.



By default, the router has created an AP group policy named **APGroup_Default**. You can click **Add** to add a new AP group policy.



Parameter description

Parameter	Description
Group Name	Specifies the name of the AP group policy.

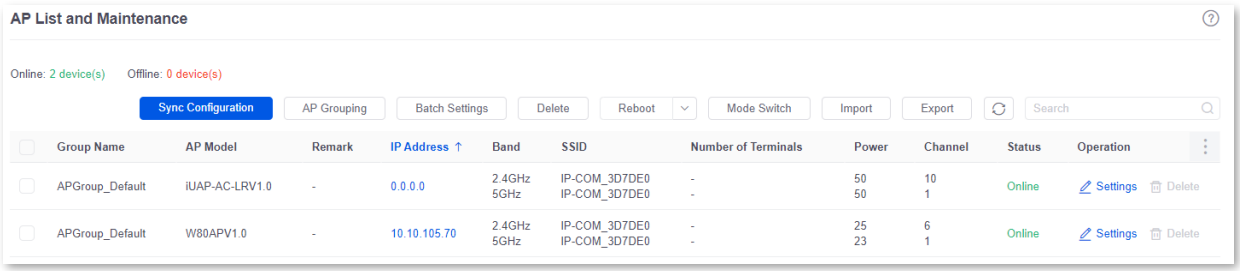
Parameter	Description
No. of SSIDs	Specifies the number of the SSIDs.
SSID Policy	Specifies the SSID policy to be used in the AP group policy. The SSID policy should be configured in **Wireless Policy** > **SSID Policy** in advance. If multiple SSIDs are configured, each SSID should be used with a different SSID policy.
Band	Specifies the working frequency band of the AP. – **2.4 GHz:** The frequency band of the AP is **2.4 GHz**. – **5 GHz:** The frequency band of the AP is **5 GHz**. Tip If your AP only supports 2.4 GHz, select 2.4 GHz or 2.4 GHz&5 GHz. If you select 5 GHz, the configuration is invalid.
RF Policy	Specifies the RF policy to be used in the AP group policy. The RF policy should be configured in **Wireless Policy** > **RF Policy** in advance.
VLAN Policy	Specifies the VLAN policy to be used in the AP group policy. The VLAN policy should be configured in **Wireless Policy** > **VLAN Policy** in advance.
Maintenance Policy	Specifies the maintenance policy to be used in the AP group policy. The maintenance policy should be configured in **Wireless Policy** > **Advanced Policy** in advance.
Alarm Policy	Specifies the alarm policy to be used in the AP group policy. The alarm policy should be configured in **Wireless Policy** > **Advanced Policy** in advance.
Password Policy	Specifies the password policy to be used in the AP group policy. The password policy should be configured in **Wireless Policy** > **Advanced Policy** in advance.
Deployment Policy	Specifies the deployment policy to be used in the AP group policy. The deployment policy should be configured in **Wireless Policy** > **Advanced Policy** in advance.
Remark	Specifies the introduction to the AP group policy. The remark is optional.
Operation	Used to edit or delete an AP group policy. Edit: Used to modify the policy. Delete: Used to delete the policy. Tip Generally, keep at least one AP group policy, so the last policy cannot be deleted. The policy in use cannot be deleted. Remove the policy reference before deleting a policy in use.

6.5 AP list and maintenance

6.5.1 Overview

On this page, you can scan the AP list, deliver the AP group policies to corresponding APs and configure the maintenance operations such as upgrading and restarting APs.

To enter the page, navigate to **AP** > **AP List and Maintenance**. You can click ⋮ to select parameters to be displayed.



Button description

Button	Description
Sync Configuration	Used to synchronize the configuration of the selected APs.
AP Grouping	Specifies the AP group policy to be used on the selected APs. The AP group policy should be configured in **Wireless Policy** > AP Group Policy in advance.
Batch Settings	Used to deliver the configuration to the selected APs in batches.
Delete	Used to delete the information of offline APs that are selected.
Reboot	Used to reboot the selected APs.
Upgrade	Used to upgrade the firmware of the selected APs. Tip Click ⌄ beside **Reboot** and you can see this function.
Reset	Used to reset the selected APs to factory settings. Tip Click ⌄ beside **Reboot** and you can see this function.

Button	Description
Mode Switch	Used to enable or disable the cloud maintenance function of the AP or switch the management mode of cloud maintenance. For details, refer to set the AP cloud maintenance function. Tip The cloud maintenance function may be unavailable for some APs.
Import	Used to import the configuration information of the selected APs. After importing, only remarks of devices with the same MAC address are replaced. Other information will not synchronize.
Export	Used to export the configuration information of the selected APs.

Parameter description

Parameter	Description
Online	Specifies the number of online devices.
Offline	Specifies the number of offline devices.
Group Name	Specifies the AP group name.
AP Model	Specifies the AP model.
Remark	Specifies the introduction to the AP.
IP Address	Specifies the IP address that the AP obtains from the AP DHCP server. It is also the login address of the AP.
MAC Address	Specifies the wireless MAC address of the AP.
Firmware	Specifies the current firmware version of the AP.
Band	Specifies the working frequency band of the AP, including **2.4 GHz** and **5 GHz**.
SSID	Specifies the current SSID of the AP.
Number of Terminals	Specifies the number of the terminals that the AP connects to.
Power	Specifies the wireless transmission power of the AP. **Policy Delivery** indicates that the transmission power of the AP is consistent with the setting in the AP group selected. You can click **Settings** under **Operation** to modify it.

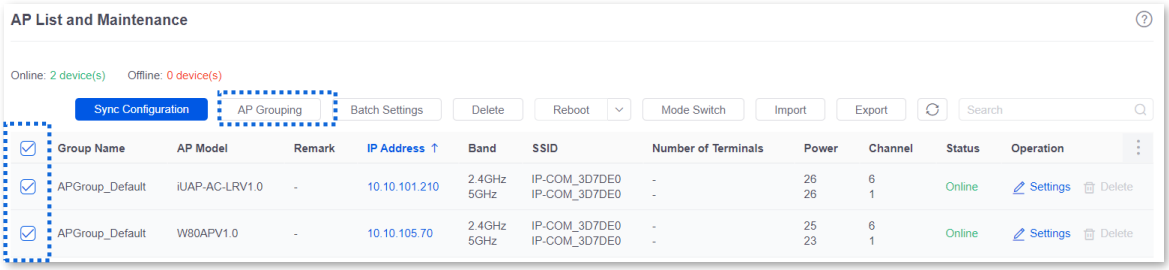
Parameter	Description
Channel	Specifies the wireless channel of the SSID that the client connects to. **Policy Delivery** indicates that the channel is consistent with the setting in the AP group selected. You can click **Settings** under **Operation** to modify it.
5G Preferred	If the client supports 2.4 GHz and 5 GHz, with this function enabled, 5 GHz is used in priority when the 5 GHz signal strength is not less than the RSSI value. Tip This function is only available for the 5 GHz band.
Management Mode	Specifies the management mode of the AP. For details about the cloud maintenance function, see Set the AP cloud maintenance function. Tip The cloud maintenance function may be unavailable for some APs.
Management VLAN	Specifies the management VLAN ID of the AP to differentiate it from data VLAN. If this parameter is not set, - is displayed by default.
Wired Port VLAN	Specifies the default VLAN ID of the wired port of the AP.
RF	Specifies the current RF status of the AP.
Online Duration	Specifies the online duration of the online AP.
Offline Duration	Specifies the offline duration of the offline AP.
Status	Specifies the current status of the AP.
Operation	It is used to edit or delete the corresponding AP group policy. Settings : Used to modify the corresponding policy. Delete : Used to delete the corresponding policy. Tip Generally, keep at least one AP group policy, so the last policy cannot be deleted. The policy in use cannot be deleted. Remove the policy reference before deleting a policy in use.

6.5.2 Deliver policies to APs

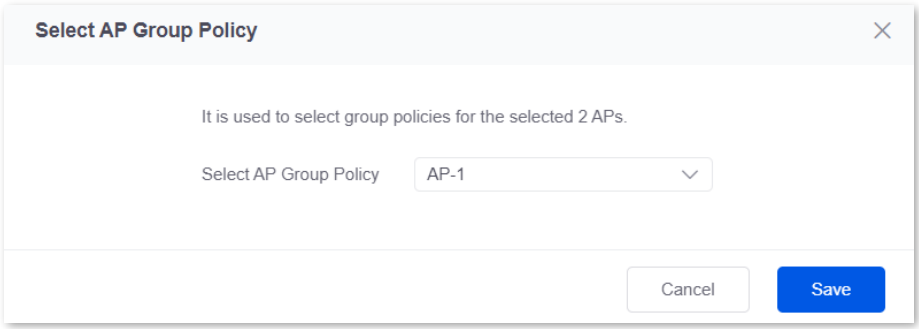
Tip

When an AP goes online, it will be added to the **APGroup_Default** group by default.

1. Log in to the web UI of the router.
2. (Skip if performed) Configure a wireless policy to be delivered to APs. For details, see **Wireless policy** in **AP management**.
3. (Skip if performed) Configure an AP group and add the wireless policy configured in step **2** to an AP group. For details, see **AP group policy** in **AP management**.
4. Deliver policies to APs.
   1) Navigate to **AP** > **AP List and Maintenance**.
   2) Select the APs to which the policies are to be delivered, and click **AP Grouping**. See the following figure for example.



   3) Select an AP group from the **Select AP Group Policy** drop-down list box, and click **Save**. See the following figure for example.



---End

After the APs are added to an AP group, the policies associated to the AP group will be applied to the APs.

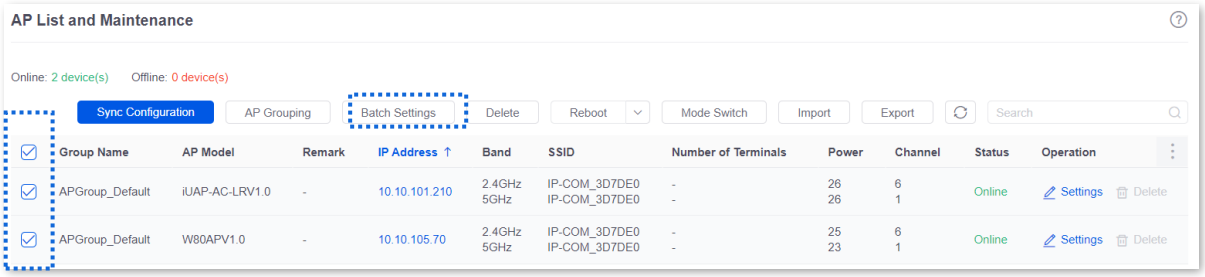
6.5.3 Batch settings

You can use **Batch Settings** to perform detailed settings for multiple selected APs in a unified manner.

Tip

This operation can only be performed on non-offline devices.

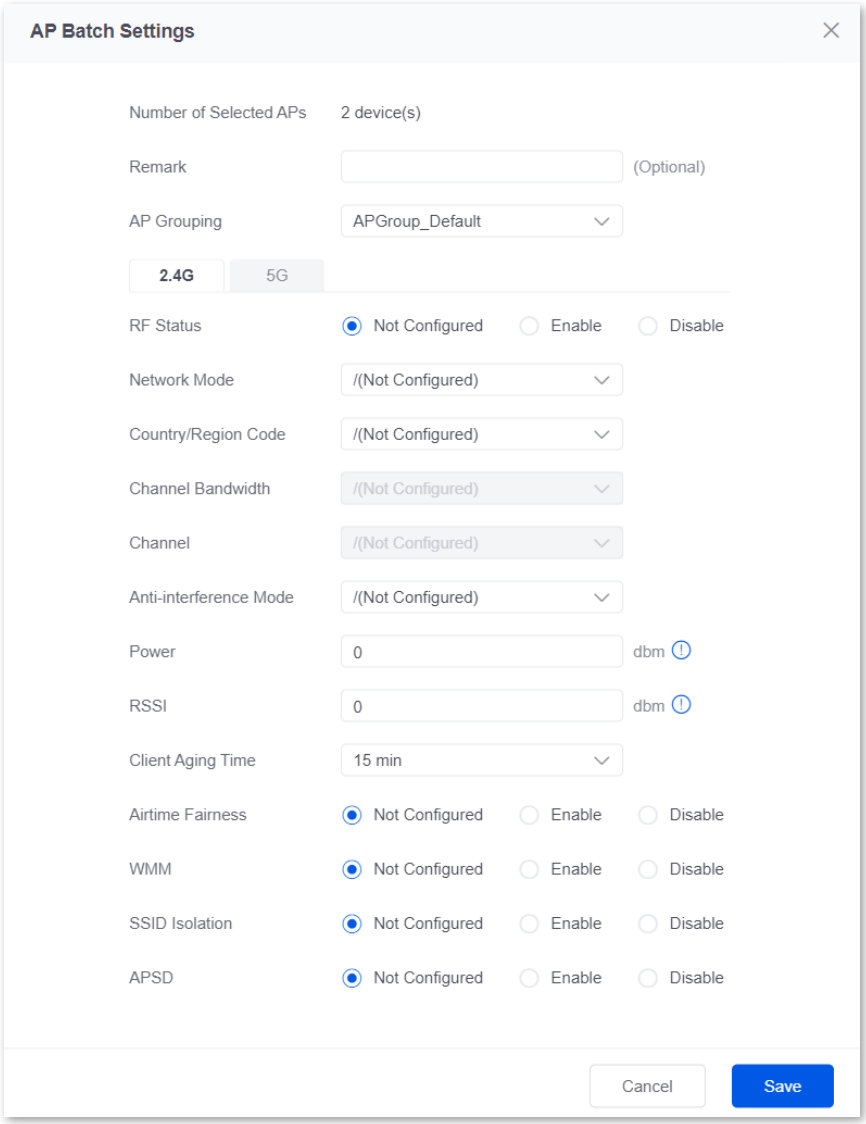
1. Log in to the web UI of the router.
2. Navigate to **AP** > **AP List and Maintenance**.
3. Select the APs for which detailed settings are to be performed, and click **Batch Settings**. See the following figure for example.



4. Set parameters as required, and click **Save**. See the following figure for example.

Tip

/(Not configured) indicates that the configuration of the AP group to which the AP applies is not modified.



---End

Related configurations for the selected APs will be delivered again.

Parameter description

Parameter	Description
Number of Selected APs	Specifies the number of APs that are selected currently. It cannot be modified.
Remark	Specifies the introduction of the APs. The remark is optional.
AP Grouping	Specifies the AP group policy to be applied for the selected APs. The AP group policy must be configured in **AP group policy** in advance.
2.4G	Used to configure parameters for 2.4 GHz and 5 GHz WiFi networks. Refer to Parameter description in RF policy.
5G	

6.5.4 Set the AP cloud maintenance function

You can use **Mode Switch** to enable the cloud maintenance function or switch the cloud management mode for selected APs.

To add APs and the router to the same project, keep their **Unique Cloud Code** consistent when enabling the cloud maintenance function.

Tip

This operation can only be performed on non-offline devices.

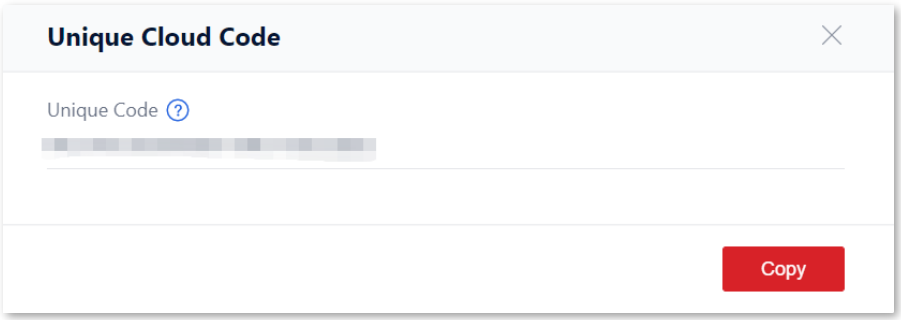
To enable the cloud maintenance function for APs:

1. Obtain the unique cloud code.

Tip

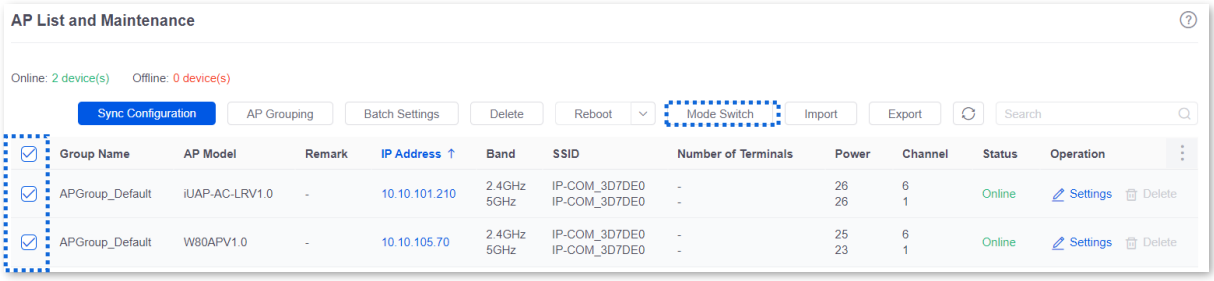
- If the cloud maintenance function has been enabled for the router and you need to add the AP and router to the same project, you can obtain the unique cloud code in **More** > **Maintenance Service** > **Cloud Maintenance**.
- Before enabling the cloud maintenance function of the AP, check that the AP is connected to the internet.

1) Access https://imsen.ip-com.com.cn to enter the Profi Cloud Platform.
2) Navigate to **Account Management** > **Unique Cloud Code** on the upper-right corner of the page, and copy the unique cloud code.



2. Enable the cloud maintenance function for the APs.

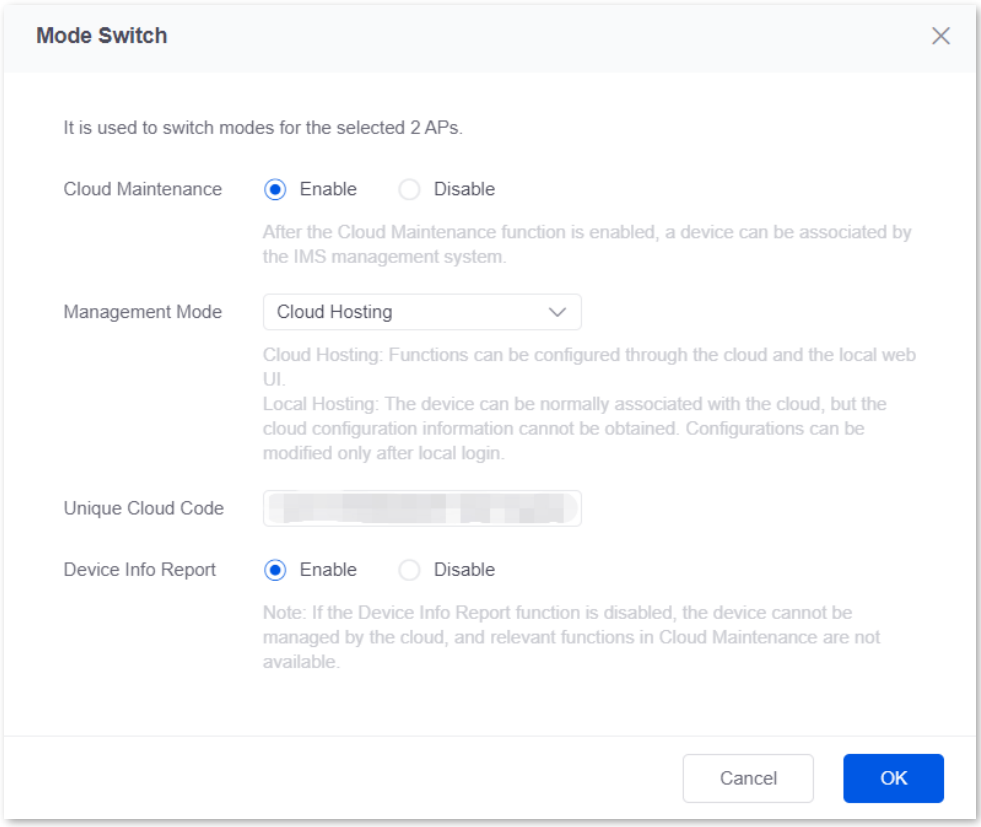
1) Log in to the web UI of the router, and navigate to **AP** > **AP List and Maintenance**.
2) Select the APs for which the cloud maintenance function is to be enabled, and click **Mode Switch**. See the following figure for example.



3) Set **Cloud Maintenance** to **Enable**, and set **Management Mode** as required (**Cloud Hosting** for example here).

4) Enter the unique cloud code obtained in step **1** in **Unique Cloud Code** and set **Device Info Report** to **Enable**.

5) Click **Save**.



---End

After the cloud maintenance function is enabled for the APs, you can manage them on the ProFi Cloud Platform (https://imsen.ip-com.com.cn) or ProFi App.

Parameter description

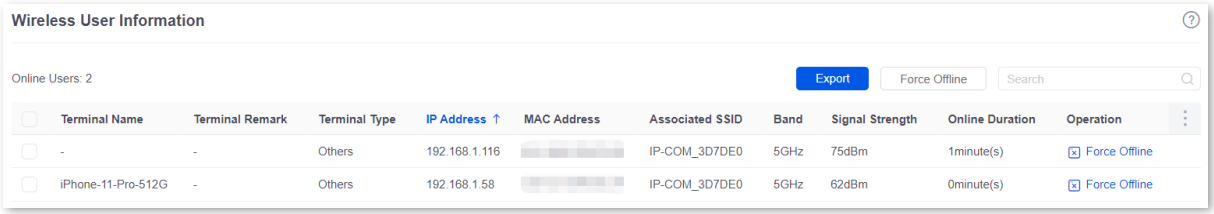
Parameter	Description
Cloud Maintenance	Used to enable or disable the **Cloud Maintenance** function.

Parameter	Description
Management Mode	Specifies the cloud maintenance management mode. – **Cloud Hosting**: Suitable for projects that are managed in a unified manner and the ProFi Cloud Platform or ProFi App is used for maintenance. APs can be managed in the ProFi Cloud Platform and configurations can be delivered to APs through the ProFi Cloud Platform. You can also configure APs by logging in to their web UI locally. – **Local Hosting**: Suitable for projects that are managed and viewed in a unified manner. APs can be managed in the ProFi Cloud Platform and all configurations must be performed on the web UI of the APs.
Unique Cloud Code	Used to associate the device to the ProFi Cloud Management System. You can obtain it from: – **Account Management** > **Unique Cloud Code** in ProFi Cloud Platform – **Account Center** in ProFi App
Device Info Report	Used to enable or disable the Device Info Report function. After this function is enabled, APs can be managed on the ProFi Cloud Platform and AP configurations will be uploaded to the ProFi Cloud Platform.

6.6 Wireless user information

On this page, you can view basic information about the users connected to the APs and configure the operations such as forcing the users offline.

To enter the page, navigate to **AP** > **Wireless User Information**. You can click ⋮ to select parameters to be displayed.



Parameter description

Parameter	Description
Online Users	Specifies the number of online device(s).
Export	Used to back up uses' information to the local computer in batches.
Force Offline	Used to kick online users offline in batches.
Terminal Name	Specifies the name of the terminal.
Terminal Remark	Specifies the introduction to the terminal.
Terminal Type	Specifies the type of the terminal such as Mobile Phone, PAD and PC. If the terminal type is not recognized, **Others** will be displayed.
IP Address	Specifies the IP address of the client.
MAC Address	Specifies the MAC address of the client.
Associated Device	Specifies the information of the AP that the client connects to.
Associated Device Remark	Specifies the remark of the AP that the client connects to.
Associated Device IP Address	Specifies the IP address of the wireless network belonging to the AP that the client connects to.
Associated Device MAC Address	Specifies the MAC address of the wireless network belonging to the AP that the client connects to.
Associated SSID	Specifies the name of the wireless network to which the client connects, or the SSID.

Parameter	Description
Band	Specifies the frequency band of the wireless network to which the client connects. – **2.4 GHz:** The frequency band of the AP is **2.4 GHz**. – **5 GHz:** The frequency band of the AP is **5 GHz**.
Real-time Upload	Specifies the real-time upload rate of the client.
Real-time Download	Specifies the real-time download rate of the client.
Total Traffic	Specifies the total download traffic during total client connection.
Signal Strength	Specifies the signal strength of the wireless network to which the client connects.
Online Duration	Specifies the duration during which the client is connected to the wireless network.
Operation	Force Offline : Used to kick the users offline.

6.7 Exmaple of configuring fat APs

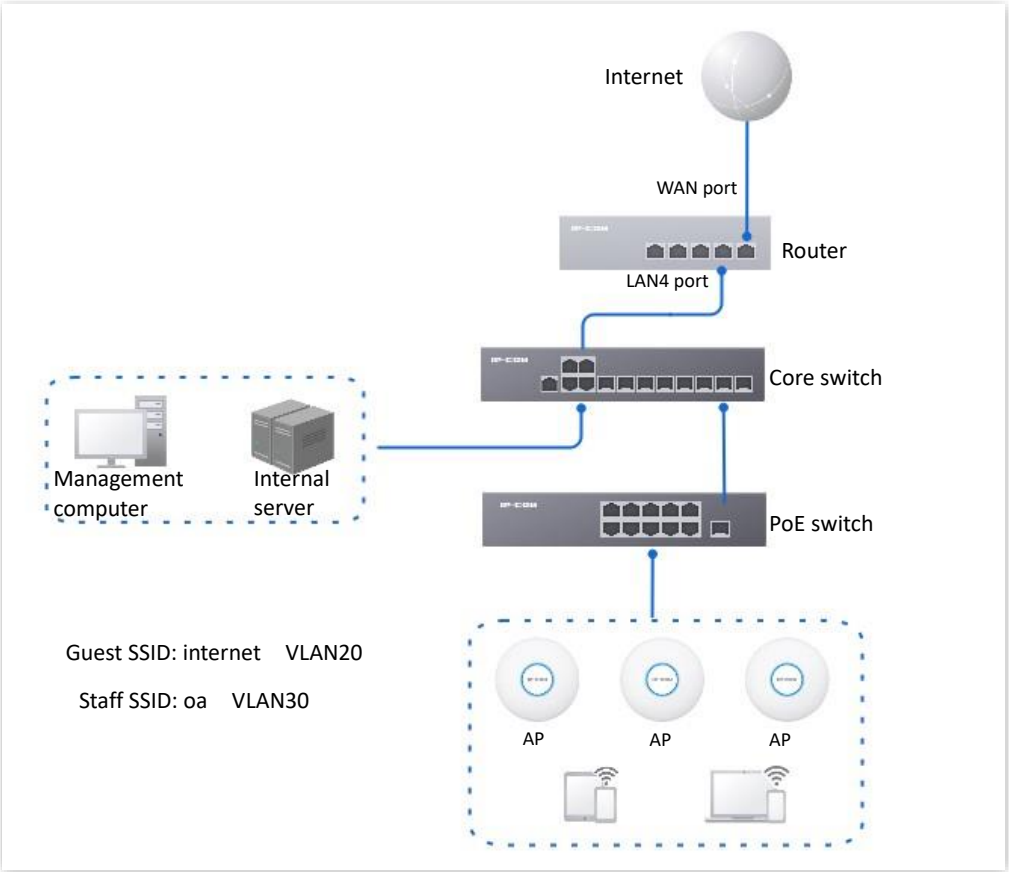
Networking requirements

A hotel uses the enterprise router and fat AP to construct networks, in which they require that the networks accessed by guests and staff are isolated. Guests can access only the internet and staff can access only the intranet.

Solution

- Successfully manage APs on the router and deliver different wireless policies to the APs.
- Configure an SSID policy for guests. Assume that the SSID is **internet**, wireless password is **UmXmL9UK** and VLAN ID is **20**.
- Configure an SSID policy for staff. Assume that the SSID is **oa**, wireless password is **CetTLb8T** and VLAN ID is **30**.
- Configure a VLAN forwarding rule on the switch.
- Configure a VLAN forwarding rule on the router and internal server.

The network topology is as follows.



Configuration procedure

I. Configure the router.

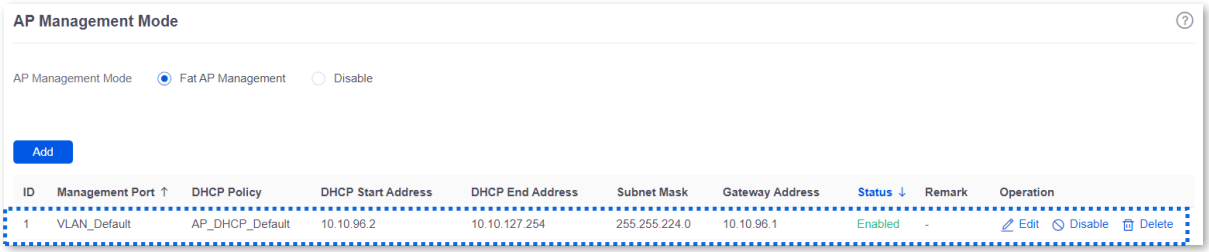
1. Log in to the web UI of the router.

2. Manage APs.

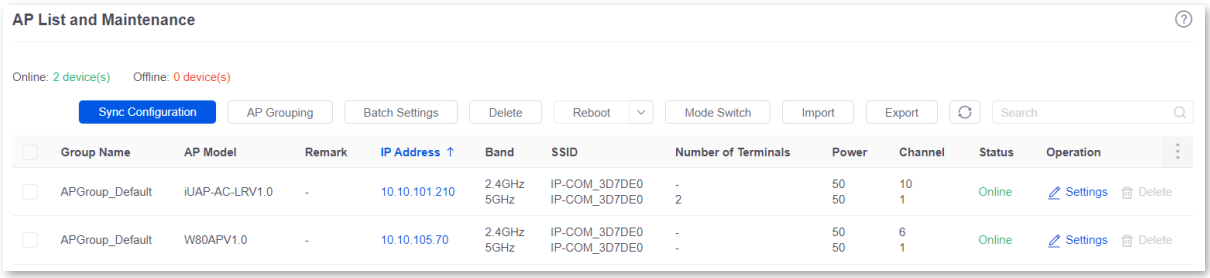
   1) Navigate to **More** > **Maintenance Service** > **AP Management Mode**.

   2) Set **AP Management Mode** to **Fat AP Management** and click **OK** in the pop-up window.

   3) Click **Add**. Add the **AP_DHCP_Default** DHCP policy for the **VLAN_Default** management port.



Navigate to **AP** > **AP List and Maintenance** to check whether the router manages the AP successfully.



3. Add the VLAN and configure the DHCP server.

   The following table lists the VLAN parameters for example.

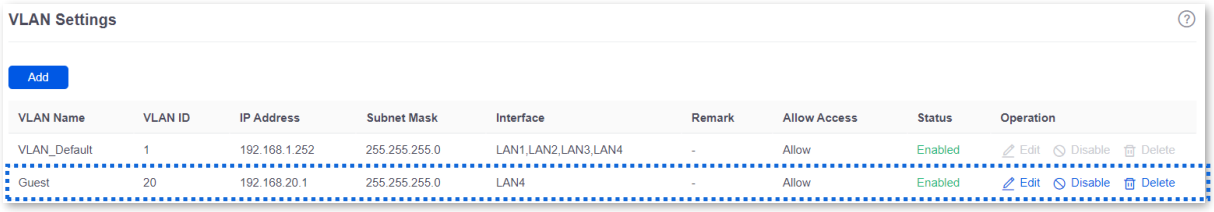
VLAN name	VLAN ID	IP address/Network segment	Physical Port
Guest	20	192.168.20.1/24	LAN4

The following table lists the DHCP server parameters of the VLAN for example.

Policy Name	Application Interface	User DHCP	AP DHCP
Guest	Guest	Client Address: 192.168.20.100 to 192.168.20.200 Subnet Mask: 255.255.255.0 Gateway: 192.168.20.1 Primary DNS: 192.168.20.1	/

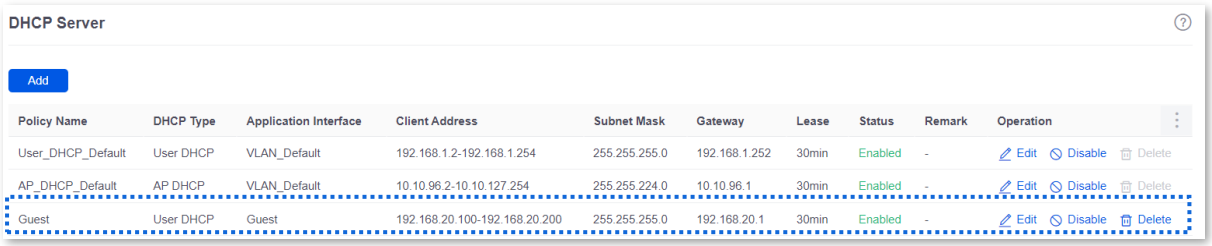
1) Add VLANs.

Navigate to **Network** > **VLAN Settings**. Click **Add**, configure VLAN parameters and click **Save.**



2) Configure the DHCP server for the VLAN.

Navigate to **Network** > **DHCP Settings** > **DHCP Server**. Click **Add**, configure parameters for user DHCP server of the Guest VLAN and click **Save.**



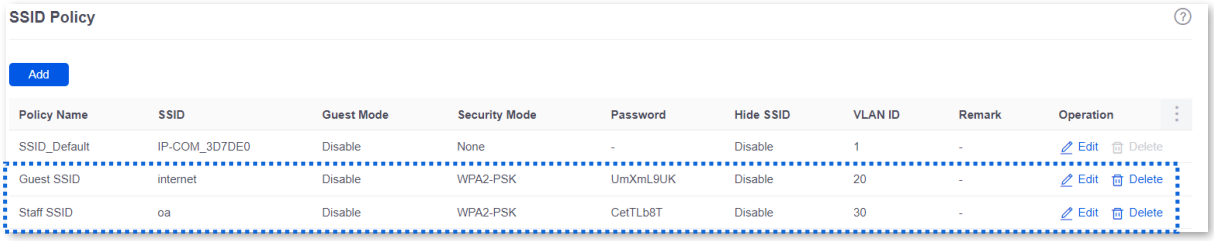
4. Set AP policies.

The following table lists the AP policies for example. Retain default values for other parameters that are not mentioned.

SSID policy	RF policy	VLAN policy	AP group policy
Policy name: Guest SSID SSID: internet Encryption type: WPA2-PSK/AES Password: UmXmL9UK VLAN ID: 20	RF_Default	VLAN enabled	Policy name: Hotel SSID Number of SSIDs: 2 2.4G/5G SSID1 policy: Guest SSID 2.4G/5G SSID2 policy: Staff SSID RF policy: RF_Default VLAN policy: AP VLAN
Policy name: Staff SSID SSID: oa Encryption type: WPA2-PSK/AES Password: CetTLb8T VLAN ID: 30	RF_Default	VLAN enabled	

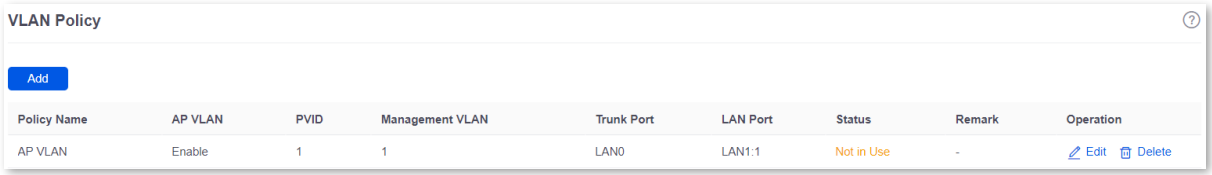
1) Configure SSID policies.

Navigate to **AP** > **Wireless Policy** > **SSID Policy**, and click **Add**. Configure parameters as required, and click **Save**.



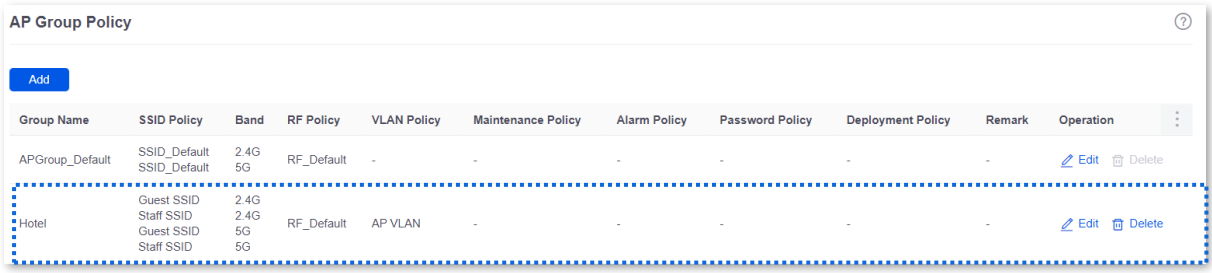
2) Configure the VLAN policy.

Navigate to **AP** > **Wireless Policy** > **VLAN Policy**, and click **Add**. Enable **AP VLAN**, set **Trunk Port** and click **Save**.



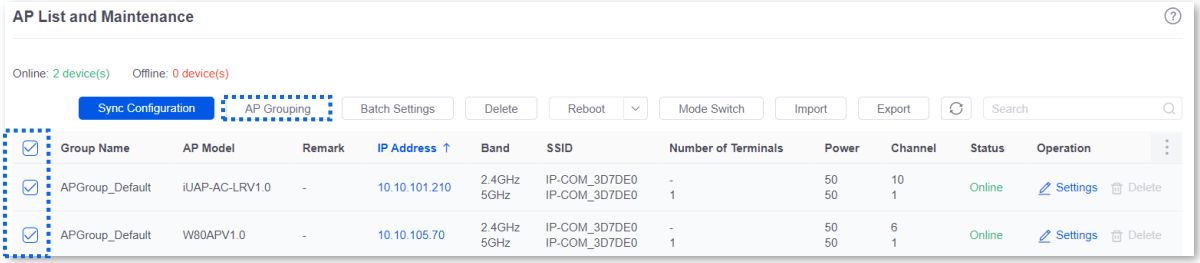
3) Configure the AP group policy.

Navigate to **AP** > **AP Group Policy**, and click **Add**. Configure parameters as required, and click **Save**.

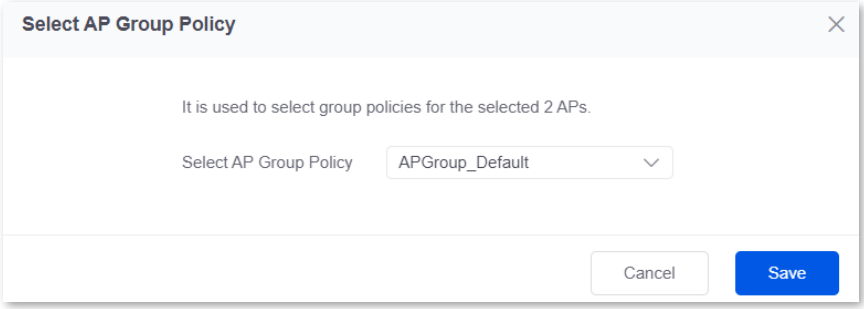


5. Deliver the AP group policy.

1) Navigate to **AP** > **AP List and Maintenance**. Select the APs to which the AP group policy is to be delivered, and click **AP Grouping**.



2) Select an AP group policy, which is **Hotel** in this example. Then, click **Save**.



II. Configure the core switch.

Divide the IEEE 802.1q VLAN on the VLAN as follows.

Port connected to	VLAN ID (VLAN allowed to pass)	Port property	PVID
AP	20,30	Trunk	1
Router	20	Trunk	1
Internal server	30	Access	30

For other ports that are not mentioned, keep the default settings. For details about the configuration procedure, see the user guide of the corresponding switch.

III. Configure the internal server.

Add the VLAN for the port connected to the switch and configure the DHCP server.

1. Add the VLAN. The following table lists the parameters for example.

VLAN name	VLAN ID	IP address/Network Segment	Physical port	Port property
Staff	30	192.168.30.1/24	LAN	Access

2. Configure the DHCP server for the VLAN. The following table lists the parameters for example.

VLAN name	User DHCP
Staff	IP address pool: 192.168.30.100 to 192.168.30.200 Subnet mask: 255.255.255.0 Default gateway: 192.168.30.1 Primary DNS: 192.168.30.1

3. Set the VLAN connected to the port of the switch.

Port connected to	VLAN ID (VLAN allowed to pass)	Port property	PVID
Switch	30	Access	30

For details about the configuration procedure, see the user guides of the corresponding devices.

---End

Verification

Users who connect to **internet** can access only the internet and users who connect to **oa** can access only the intranet.

6.8 IPTV

6.8.1 Overview

Internet Protocol Television (IPTV) is the technology integrating internet, multimedia, telecommunication and many other technologies to provide interactive services, including digital TV, for family users by internet broadband lines.

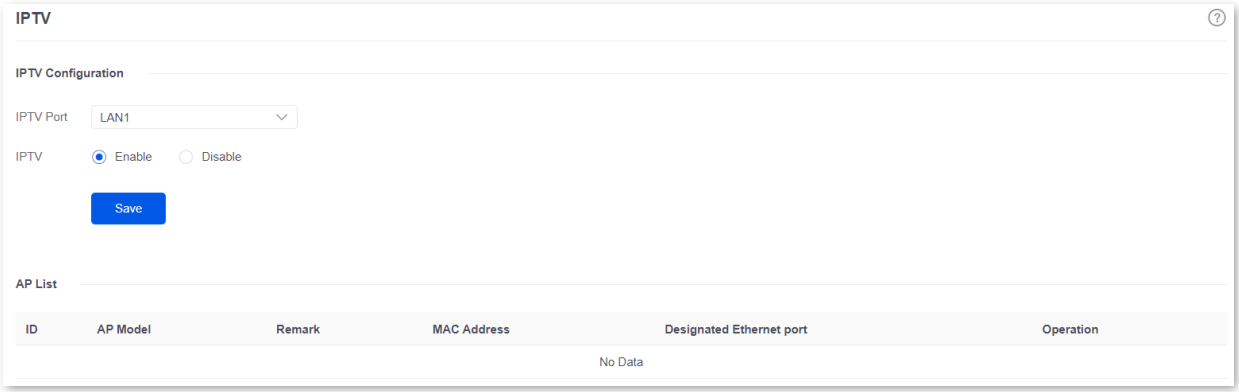
With the IPTV function, you can set up an IPTV data pass-through channel between the device and the AP to solve the difficult connection problem caused by the long distance between the IPTV set-top box and the optical modem.

If the IPTV service is included in your broadband service, you can enable the IPTV function of the router, then you can enjoy both internet access through the router and rich IPTV programs with a set-top box and TV.

Tip

This function needs to be used with IP-COM APs that support IPTV function.

To enter the page, navigate to **AP** > **IPTV**. This function is disabled by default. After it is enabled, the following information is displayed.



Parameter description

Parameter		Description
IPTV Configuration	IPTV Port	Used to designate a LAN port as the IPTV port to connect to the IPTV port of the modem. Refer to Interface Info on the **System** page for the LAN port number.
	IPTV	Used to enable/disable the IPTV data pass-through function of this device.

Parameter		Description
AP List	AP Model	Specifies the product model of the AP. Only APs that support IPTV are displayed in the AP list.
	MAC Address	Specifies the MAC address of the AP.
	Remark	Specifies the description of the AP.
	Designated Ethernet port	Specifies the wired Ethernet port on the AP to set up a transparent IPTV data transmission channel with the router. The designated Ethernet port needs to be connected to the IPTV set-top box. Tip The designated Ethernet port of the AP is **LAN0**.

6.8.2 Watch IPTV programs (scenario 1)

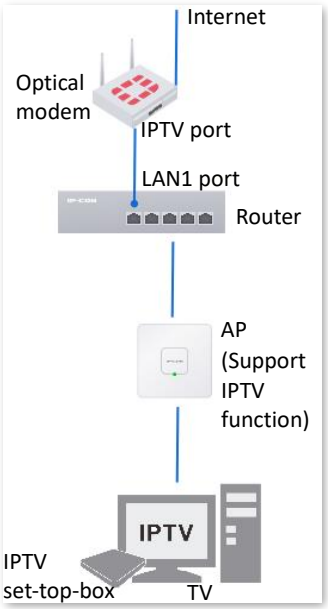
Networking requirements

The IPTV service is included in your broadband service. The ISP provides an IPTV account and password, but no VLAN information.

Requirements: Watching IPTV programs.

Solution

You can configure the IPTV function of the router to achieve the above requirements.



Configuration procedure

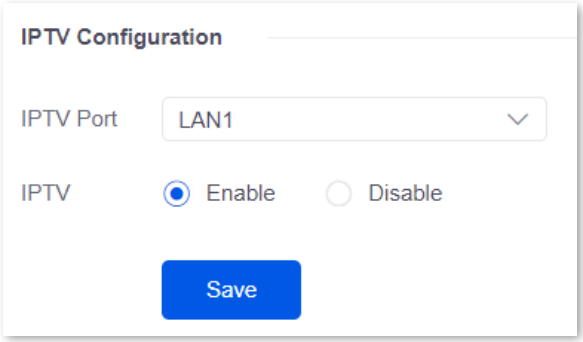
1. Configure the router.

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

   2) Navigate to **AP** > **IPTV**.

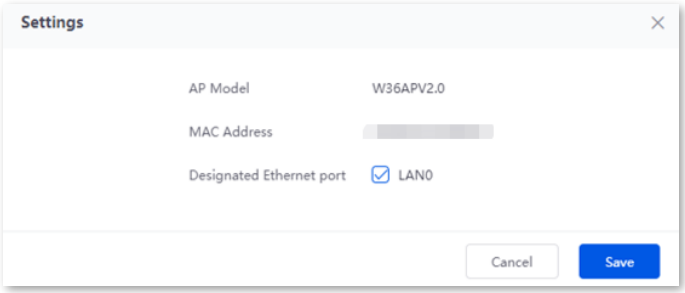
   3) Enable the IPTV function and designate IPTV port.

      - Select the router as the LAN port of IPTV. In this example, select **LAN1** for **IPTV Port**.
      - Set **IPTV** to **Enable**.
      - Click **Save**.

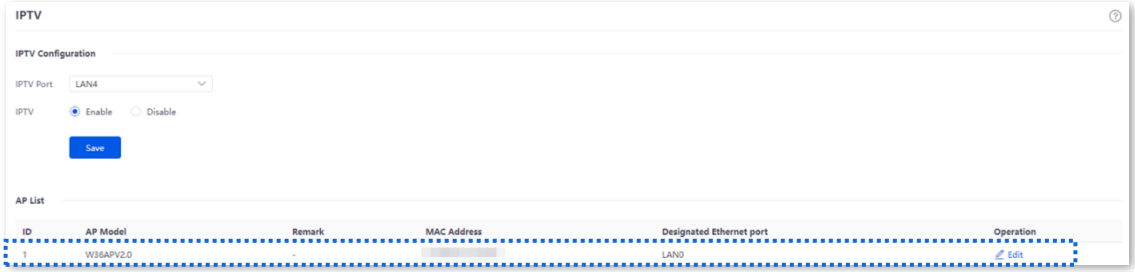


   4) Designate AP1 as the wired Ethernet port of IPTV port. The following figure is for reference only.

      - Choose the AP to be connected to the IPTV set-top box and click ✎.
      - Check the **Designated Ethernet Port** and click **Save**.



   The IPTV port of the AP is designated successfully.



2. Set your IPTV set-top box.

   Use the IPTV account and password provided by your ISP to dial up on your IPTV set-top box.

   ---End

Verification

After completing the configuration, you can watch IPTV programs on your TV.

6.8.3 Watch IPTV programs (scenario 2)

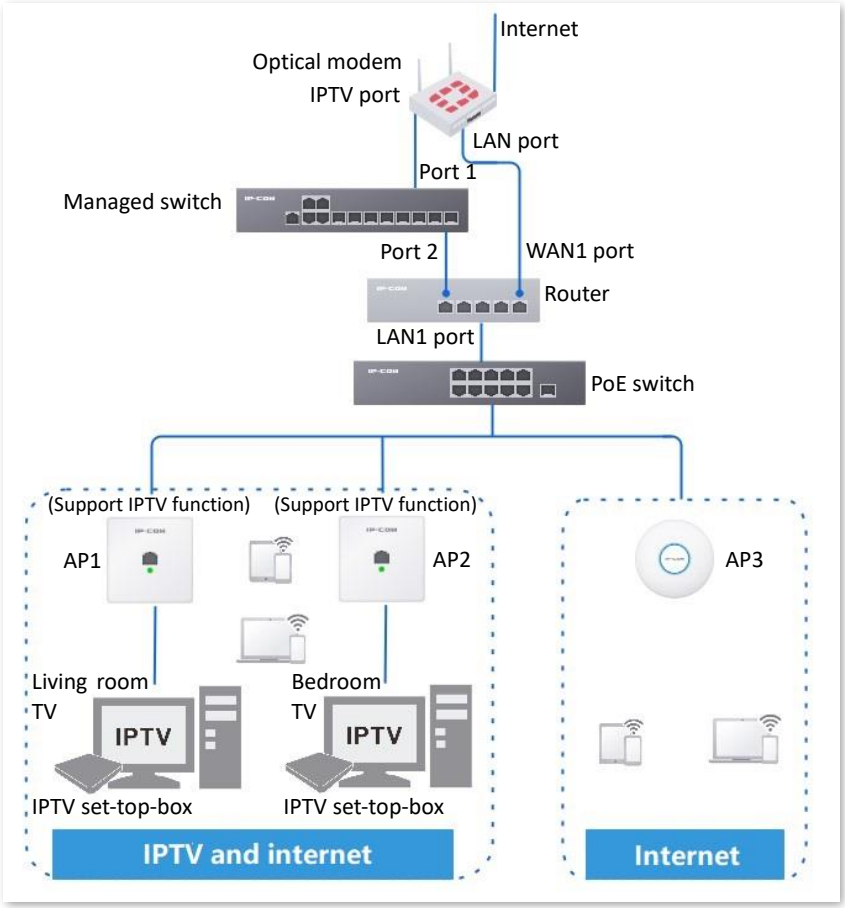
Networking requirements

The IPTV service is included in a hotel broadband service. The ISP provides an IPTV account and password, and the VLAN ID of the IPTV service (VLAN ID 2 is taken as an example here).

Requirements: Watching IPTV programs and accessing the internet at the same time.

Solution

You can configure the IPTV function of the router, and VLAN function of the switch to achieve the above requirements.



Configuration procedure

1. Configure the switch (IP-COM layer-2 managed switch G3328FV1.0 is taken as an example here).

   1) Add VLAN.

      - Navigate to **Basics** > **VLAN** > **802.1Q VLAN**.
      - Click **Add**.
      - Set **VLAN ID** to **2**, **VLAN Description** to **IPTV** on the pop-out window. Then click **Confirm**.

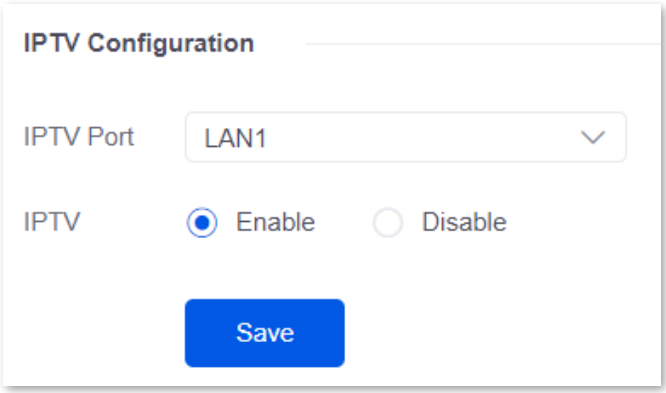
   2) Configure port property.

      - Click **Basics** > **VLAN** > **Port Member**.
      - Click the button behind port 1 and set **PVID** to **2**.
      - Click the button behind port 2 and set **PVID** to **2**.

2. Configure the router.

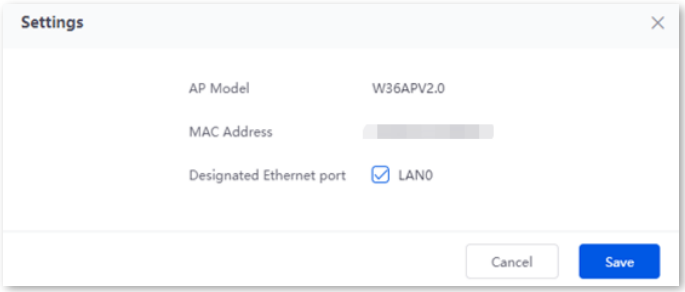
   1) Log in to the web UI of the router.
   2) Navigate to **AP** > **IPTV**.
   3) Enable the IPTV function of the router and designate IPTV port.

      - Select the router as the LAN port of IPTV. In this example, select **LAN1** for **IPTV Port**.
      - Set **IPTV** to **Enable**.
      - Click **Save**.

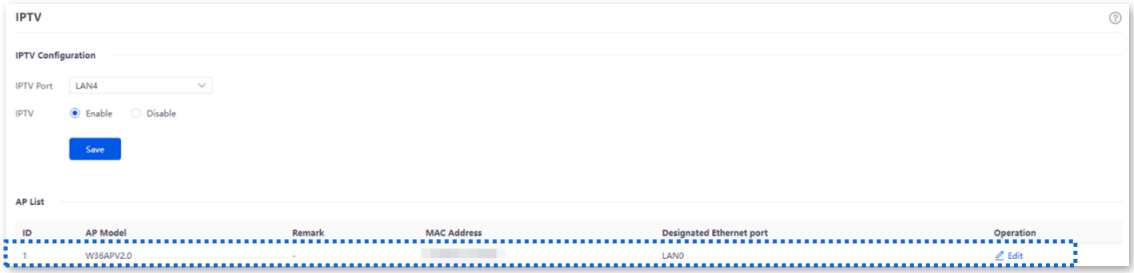
      

   4) Designate a wired Ethernet port of the AP1.

      - Choose the AP1 to be connected to the IPTV set-top box and click .
      - Check the **Designated Ethernet Port** and click **Save**.



The IPTV port of the AP is designated successfully.



5) Repeat 4) of step 2 to designate other wired Ethernet port of AP2 (supporting IPTV function).

3. Connect the IPTV cable connected to the optical modem to port 1 of the switch.
4. Use an Ethernet cable to connect port 2 of the switch to the IPTV port of the router.
5. Connect the IPTV set-top box to the designated Ethernet port of the AP.
6. Set your IPTV set-top box.

   Use the IPTV account and password provided by your ISP to configure network settings on your IPTV set-top box.

---End

Verification

You can watch IPTV programs and access the internet at the same time.

7 Cloud VPN

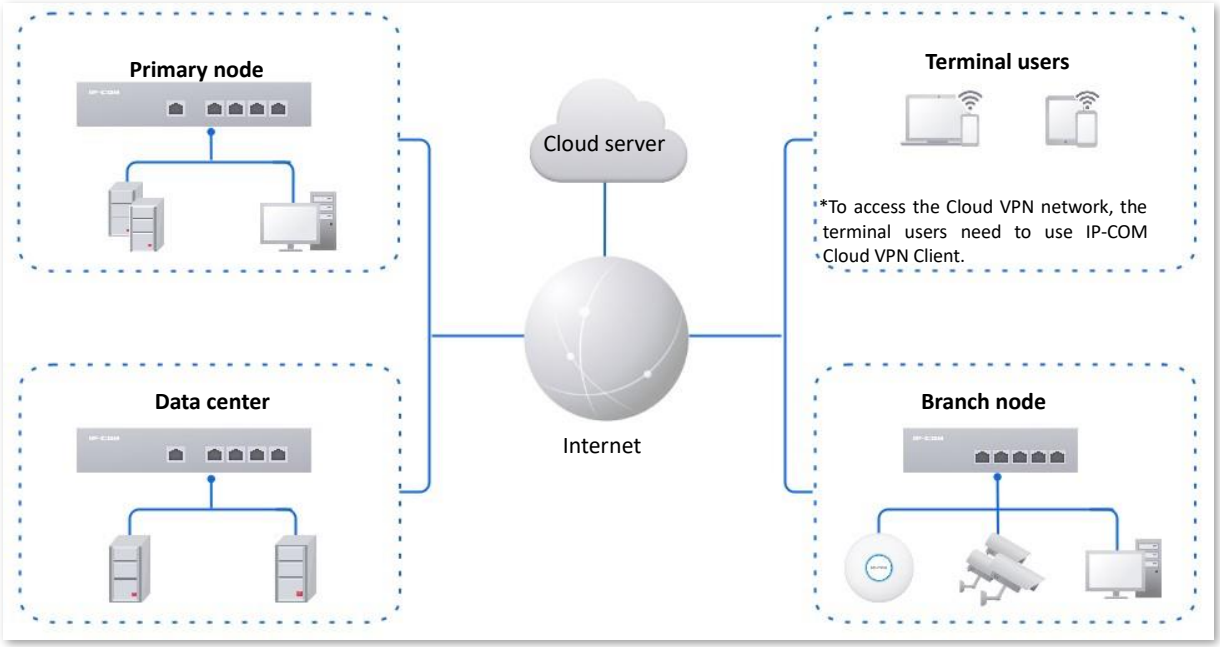
7.1 Overview

Cloud VPN is a service formed by applying Software Defined Network (SDN) technology to WAN scenarios. It can provide wide area interconnection for employees on business trips, branch offices, headquarters and data centers.

Advantages of Cloud VPN:

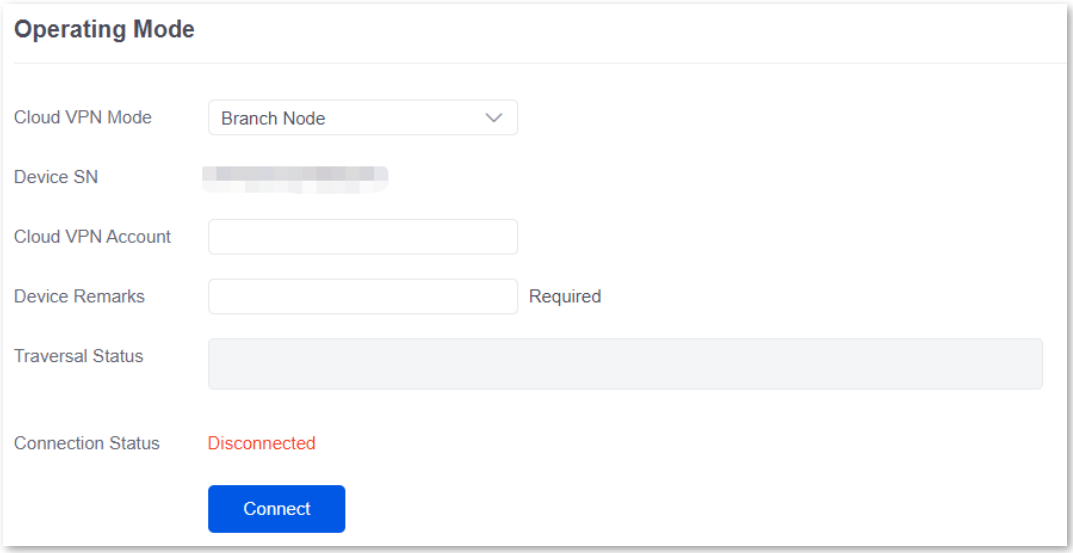
- Simple networking. One-click interconnection can be realized by the cloud server.
- Permission management. The primary node can configure different access policies for branch nodes, terminal accounts and data centers.
- Unified management. The primary node can manage WiFi and video surveillance on branch nodes in a unified way.

The typical topology of Cloud VPN networking solution is as follows.



Log in to the web UI of the router, and click **Cloud VPN** to enter the page.

You can configure the Cloud VPN mode and related parameters. Only **Branch Node** is supported. The Cloud VPN function of the router is disabled by default. The following figure displays when **Branch Node** is selected.

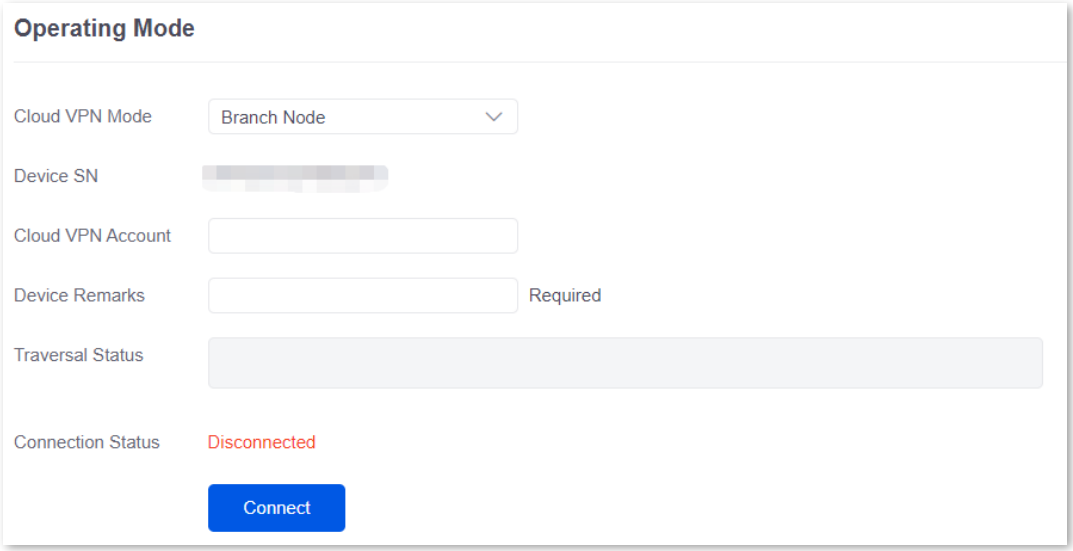


Parameter description

Parameter	Description
Cloud VPN Mode	Specifies the Cloud VPN mode of the router. Only **Branch Node** is supported. – **Branch Node**: In this mode, the router is the branch node in the Cloud VPN and can receive the access policies delivered by the primary node and data center. – **Disable**: It specifies that the Cloud VPN function is disabled.
Device SN	Specifies the serial number of the router.
Cloud VPN Account	Specify the account used to connect to the Cloud VPN service, that is, the Cloud VPN account of the primary node.
Device Remarks	Specifies the remarks of the router, which facilitate the identification of the primary node.
Traversal Status	Specifies the traversal connection status between the current node and other nodes in the Cloud VPN network.
Connection Status	Specifies the connection status between the router and the primary node in the Cloud VPN network, including **Connected**, **Disconnected** and **Connecting**.
Connect	Used to connect to or disconnect from the primary node.
Disconnect	

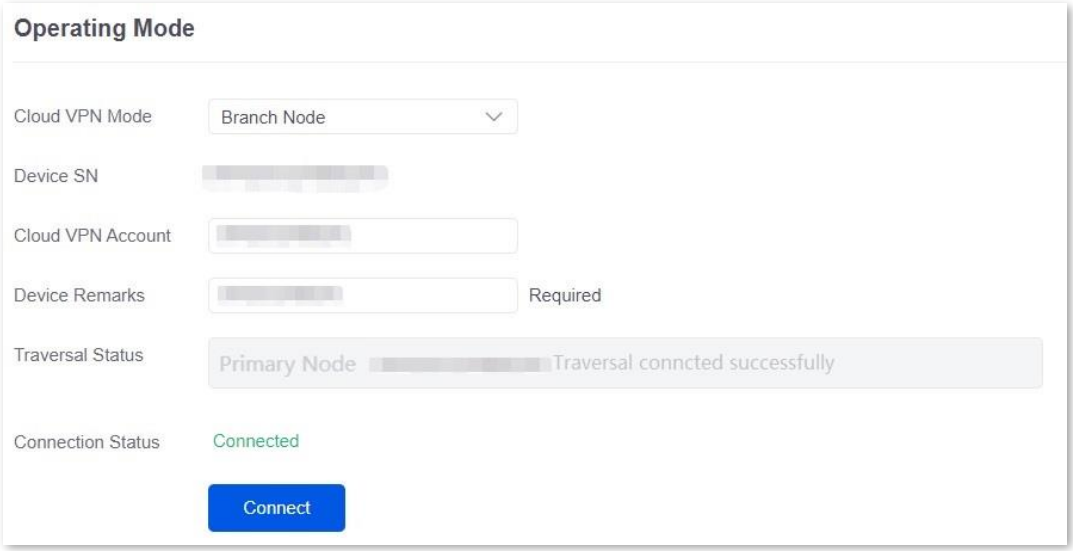
7.2 Configure cloud VPN operating mode

1. Log in to the web UI of the router and click **Cloud VPN**.
2. Select **Branch Node** from the drop-down list box of **Cloud VPN Mode**.
3. Enter **Cloud VPN Account** of the primary node.
4. Enter **Device Remarks** that can be easily identified.
5. Click **Connect**.



---End

The primary node will receive a join request from the router. After the primary node adds the router to the Cloud VPN, the **Connection Status** will be displayed as **Connected**. The following figure is for reference only.



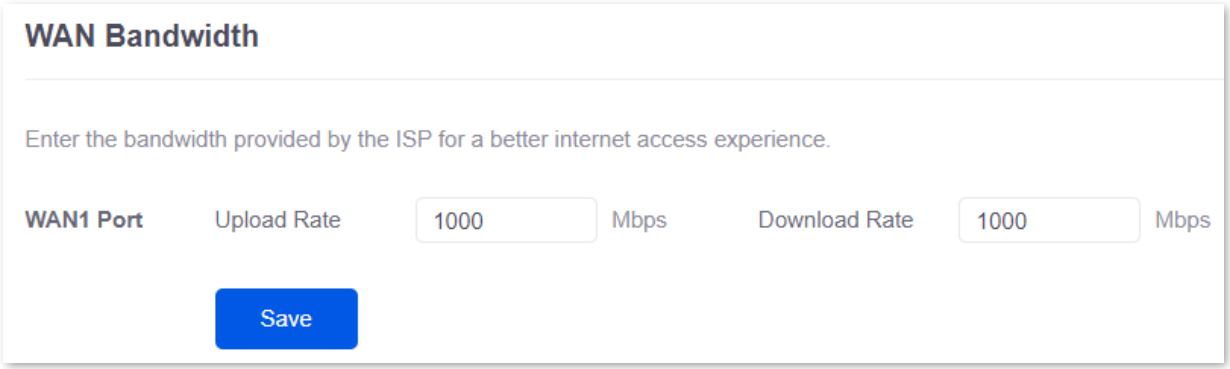
8 Bandwidth limit

8.1 WAN bandwidth

Navigate to **BW Limit** > **WAN Bandwidth** to enter the page.

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

By properly configuring the WAN port bandwidth, you can allocate bandwidth to LAN users more accurately when using the **Intelligent Speed Limit** policy.



Parameter description

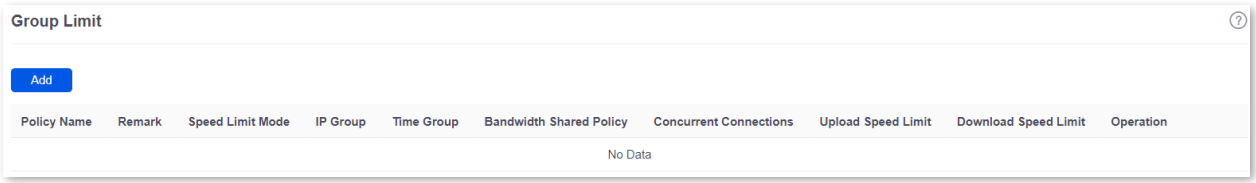
Parameter	Description
Upload Rate	Specify the bandwidth values of the broadband. If you are not clear about them, consult your ISP.
Download Rate	

8.2 Group limit

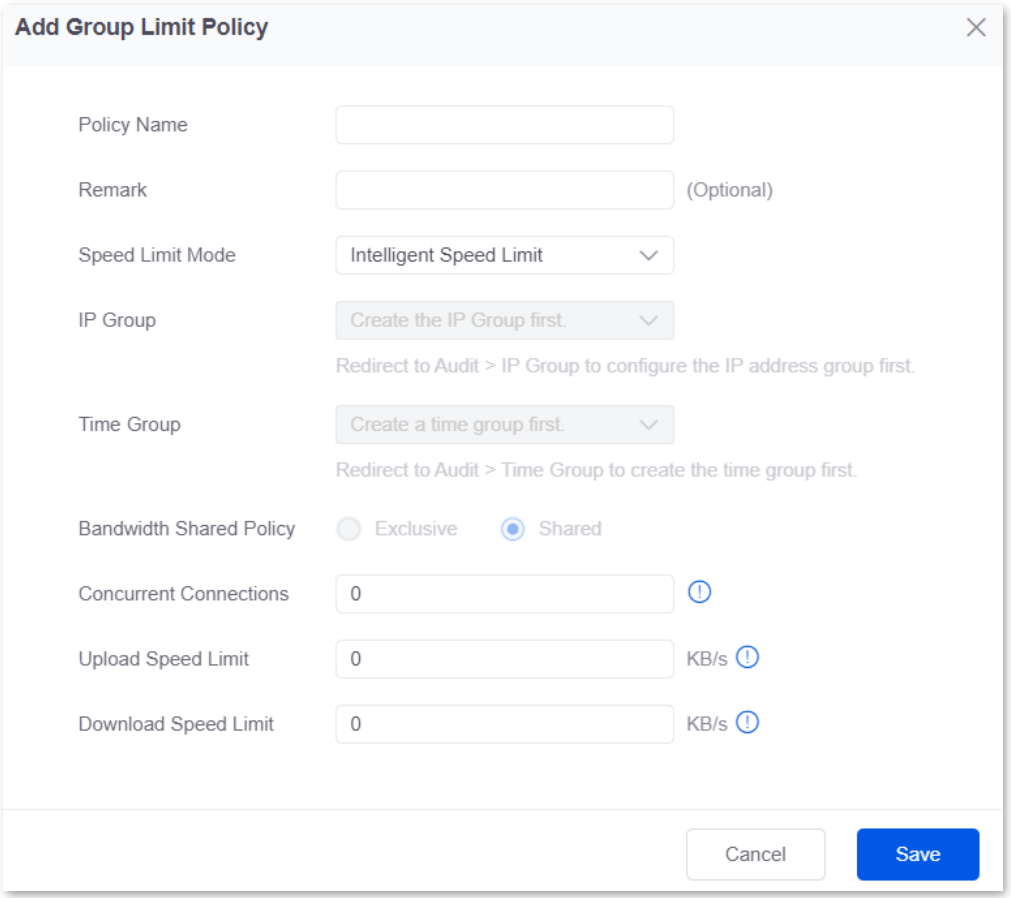
The extranet bandwidth is always limited, so the network administrator needs to control users' network speed to reasonably allocate the limited bandwidth resources, utilizing the extranet resources effectively.

Navigate to **BW Limit** > **Group Limit** to enter the page.

On this page, you can configure the group speed limit policy of the router.



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



Parameter description

Parameter	Description
Policy Name	Specifies the name of the group limit policy.

Parameter	Description
Remark	Specifies the remark of the group limit policy. The remark is optional.
Speed Limit Mode	Specifies the speed limit modes of the router. – **Intelligent Speed Limit**: The router evenly allocates bandwidth to users of certain IP group during the time period, based on the upload/download rate of the WAN port on the WAN Bandwidth page. Thus, before using this mode, the network administrator needs to enter the correct bandwidth of the network on the WAN Bandwidth page. – **Customize Speed Limit**: You can set the maximum upload/download rate for users connected to the router separately or in a unified manner according to the actual requirements.
IP Group	Specifies the IP address group upon which the group speed limit policy takes effect. The group speed limit policy takes effect only when the device IP addresses are in the IP address group. Configure the IP group in **Audit** > **Group Policy** > **IP Group** first.
Time Group	Specifies the time group upon which the group speed limit policy takes effect. The group speed limit policy takes effect only in such configured time. Configure the time group in **Audit** > **Group Policy** > **Time Group** first.
Bandwidth Shared Policy	Specifies the bandwidth shared policy. – **Shared**: All users in the controlled IP group share the upload/download rate that you set. In this mode, the bandwidth of each controlled user may be different. – **Exclusive**: Each user in the controlled IP group has an exclusive upload/download rate. In this mode, each controlled user gets the same bandwidth. In the **Intelligent Speed Limit** mode, only **Shared** is supported.
Concurrent Connections	Specifies the maximum connections for a single use device in the controlled IP group. Tip **0** indicates no limit.
Upload Speed Limit Download Speed Limit	Specify the maximum upload/download rate of the controlled user. Tip **0** indicates no limit.

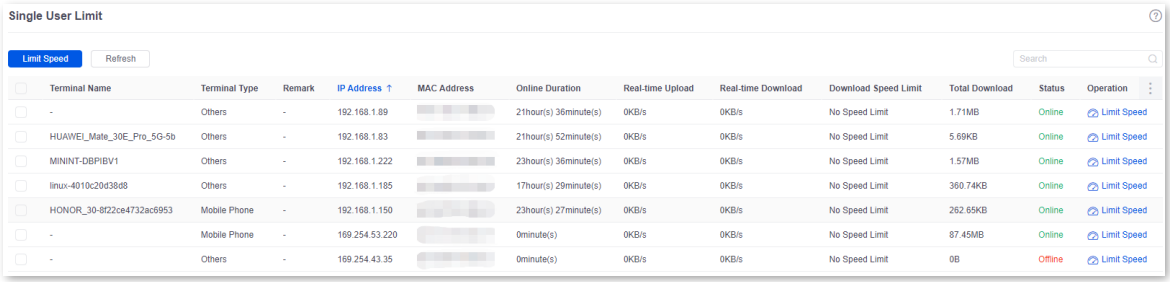
8.3 Single user limit

8.3.1 Overview

Navigate to **BW Limit** > **Single User Limit** to enter the page.

On this page, you can configure the maximum upload or download rates for users connected to the router separately or in a unified way, according to the actual requirements.

You can click ⋮ to select parameters to be displayed.



Parameter description

Parameter	Description
Terminal Name	Specifies the name of the terminal device.
Terminal Type	Specifies the type of the terminal device.
Remark	Specifies the remark of the terminal device.
IP Address	Specifies the IP address of the terminal device.
MAC Address	Specifies the MAC address of the terminal device.
Online Duration	Specifies the online duration of the terminal device.
Real-time Upload	Specifies the real-time upload rate of the terminal device.
Real-time Download	Specifies the real-time download rate of the terminal device.
Upload Speed Limit	Specifies the maximum upload rate of the terminal device.
Total Upload	Specifies the total upload traffic of the terminal device.
Download Speed Limit	Specifies the maximum download rate of the terminal device.

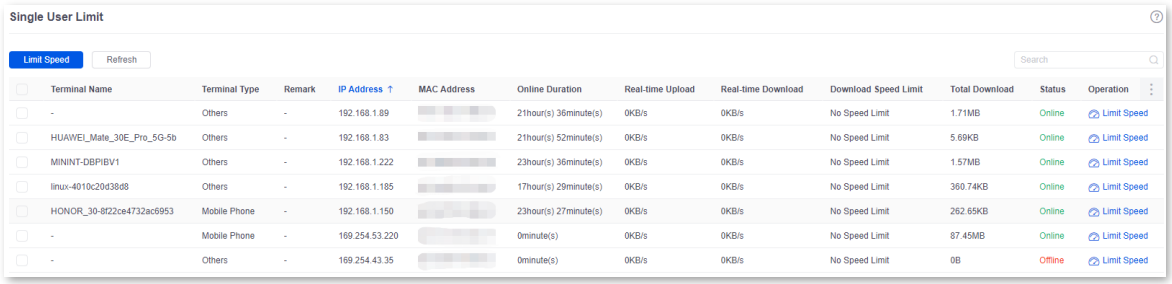
Parameter	Description
Total Download	Specifies the total download traffic of the terminal device.
Status	Specifies the status of the device, including **Online** and **Offline**.
Limit Speed	Used to limit the speed of the selected devices.
Refresh	Used to refresh the current list.

8.3.2 Configure single user limit

1. Log in to the web UI of the router, and navigate to **BW Limit** > **Single User Limit**.
2. Select the terminal device to be limited and click **Limit Speed**.

Tip

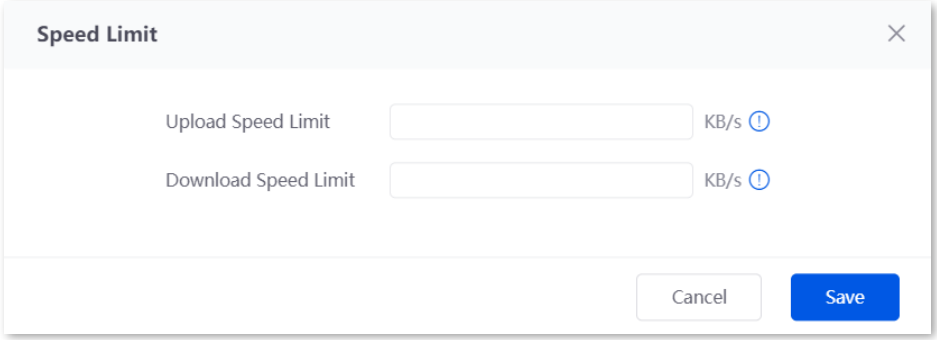
You can select multiple terminal devices and click **Limit Speed** to set speed limits for the devices at a time.



3. Set the **Upload Speed Limit** and **Download Speed Limit** for the selected terminal device, and click **Save**.

Tip

0 indicates no limit. By default, terminal devices are set with no speed limit.



----End

8.4 Example of configuring group speed limit

Networking requirements

An enterprise uses the enterprise router to deploy a network.

Requirement: Each purchasing employee (IP address range: 192.168.0.2 – 192.168.0.50) in the LAN can use the fixed upload and download bandwidth of 1 Mbps (1 Mbps = 128 KB/s) during working hours (8:00 to 18:00) from Monday to Friday while other devices in the LAN are not restricted for bandwidth.

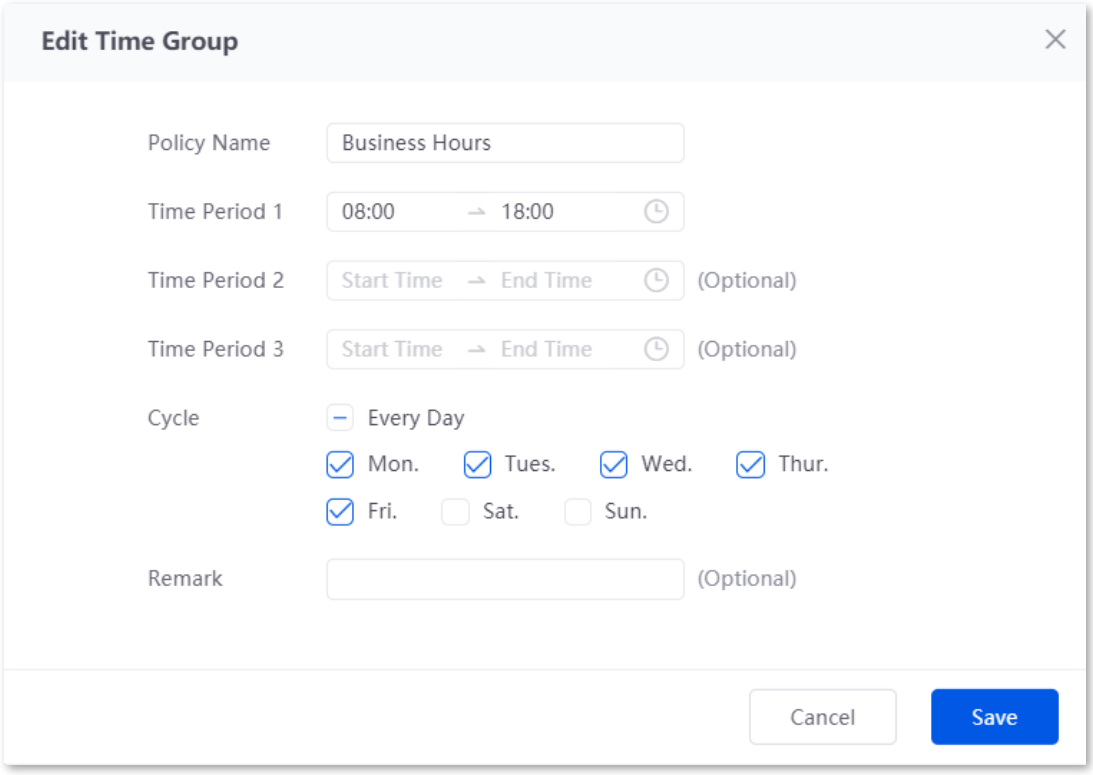
Solution

The **BW Limit > Group Limit** function of the router can achieve the requirement. Assume that the concurrent connections of each user device are 600.

Configuration procedure

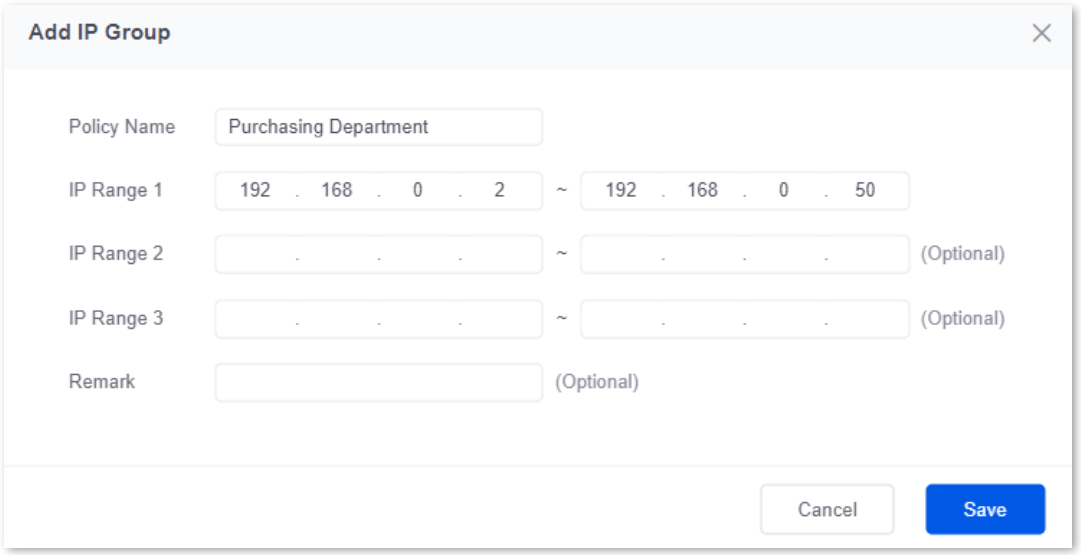
1. Log in to the web UI of the router.
2. Configure the time group.

   Navigate to **Audit** > **Group Policy** > **Time group**, and configure the following time group.



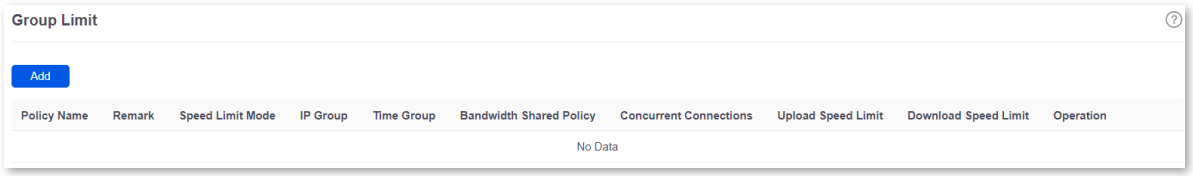
3. Configure the IP group.

Navigate to **Audit** > **Group Policy** > **IP group**, and configure the following IP group.



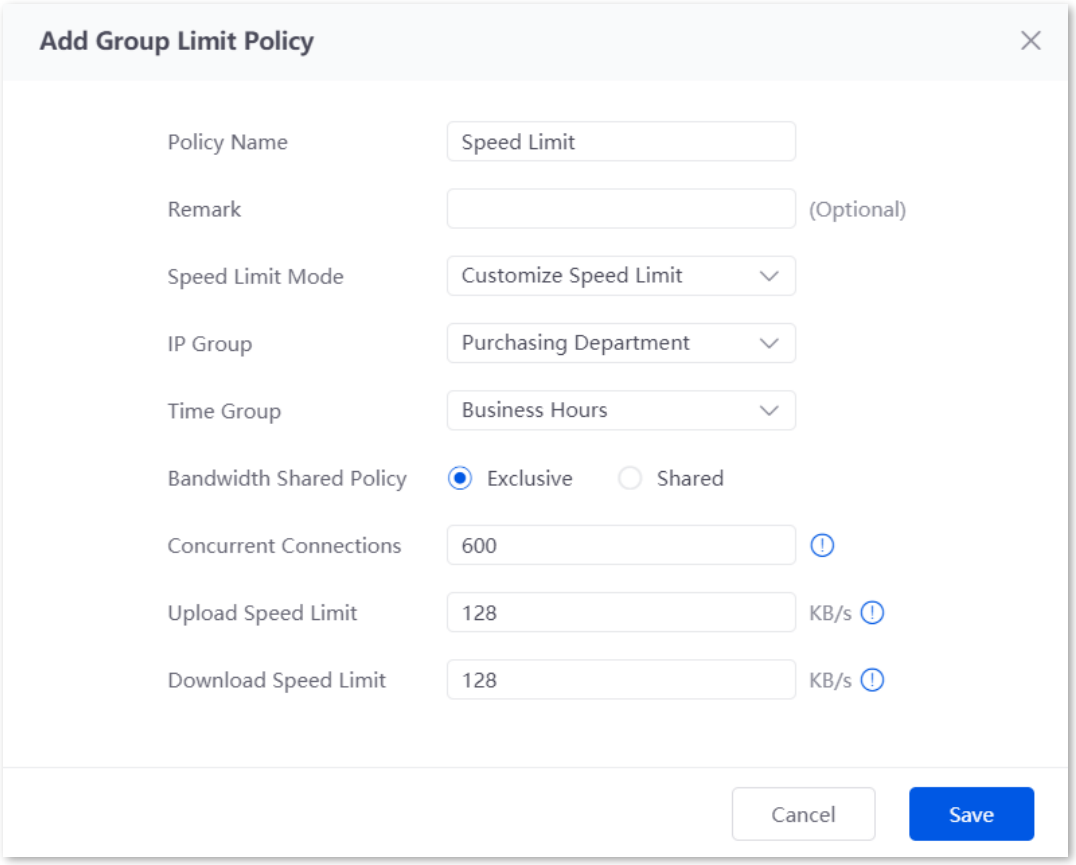
4. Add the group limit policy.

1) Navigate to **BW Limit** > **Group Limit**, and click **Add**.



2) Configure the parameters in the **Add Group Limit Policy** window, and click **Save**.

- Set the **Policy Name**, such as **Speed Limit**.
- Select the **Speed Limit Mode**, which is **Customize Speed Limit** in this example.
- Select the **IP Group** to which the policy applies, which is **Purchasing Department** in this example.
- Select the **Time Group** to which the policy applies, which is **Business Hours** in this example.
- Select the **Bandwidth Shared Policy**, which is **Exclusive** in this example.
- Set the **Concurrent Connections** per client, which is **600** in this example.
- Set the **Upload Speed Limit** and **Download Speed Limit** of terminal devices, which are both **128** KB/s.



----End

Verification

For users with IP addresses ranging from 192.168.0.2 to 192.168.0.50, the maximum upload speed and download speed are both 128 KB/s at 8:00 - 18:00 from Monday to Friday.

9 Behavior&Audit

9.1 Group policy

When configuring the functions such as various kinds of filtering, group limit and multi-WAN policy, you need to configure the IP group, time group in advance.

9.1.1 Time group

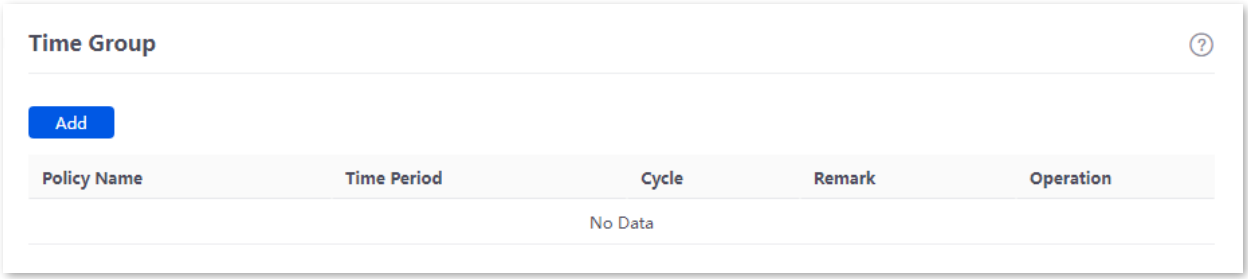
The time group policy is used to divide time into different groups and combine different groups together randomly.

Navigate to **Audit** > **Group Policy** > **Time Group** to enter the page.

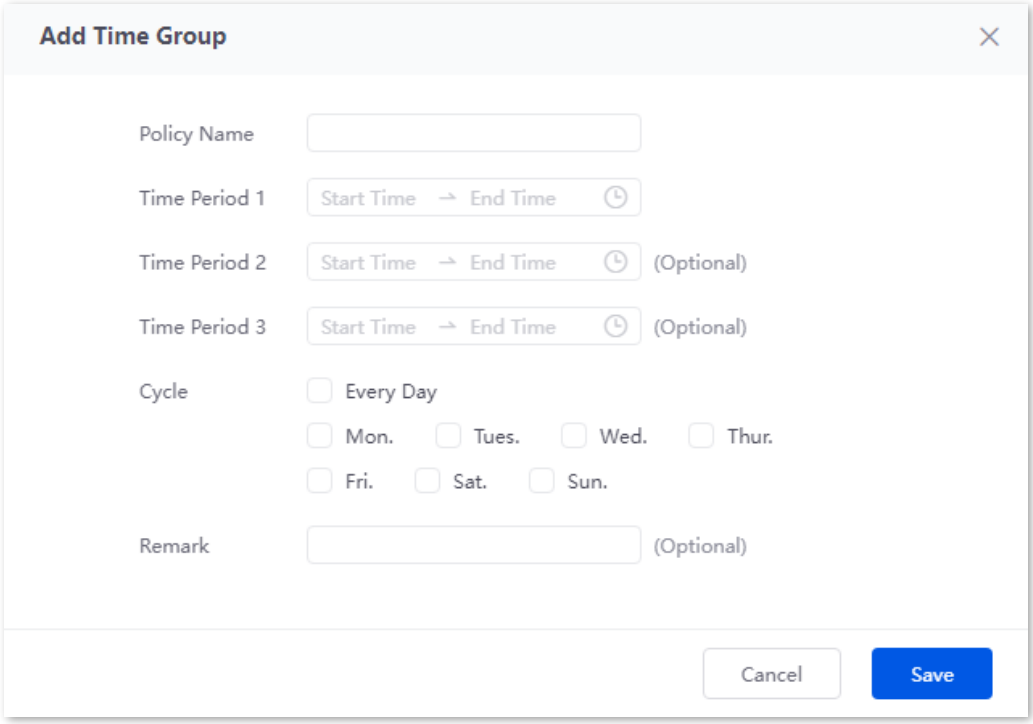
On this page, you can configure the time group policy according to the actual requirements.

Configuration procedure:

1. Log in to the web UI of the router.
2. Navigate to **Audit** > **Group Policy** > **Time Group**.
3. Click **Add**.



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



----End

Parameter description

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

9.1.2 IP group

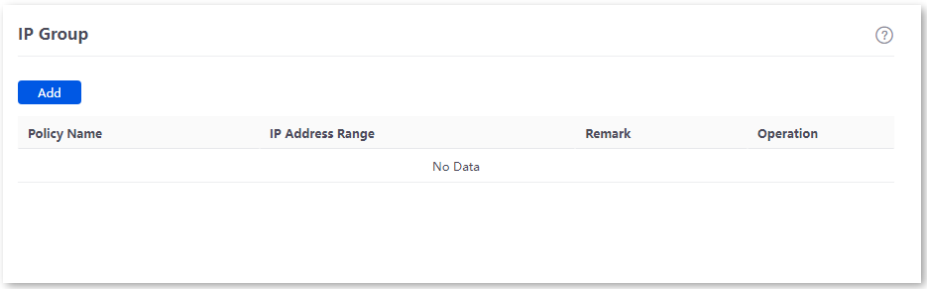
The IP group policy is used to set the hosts within the LAN into different groups based on their IP addresses.

Navigate to **Audit** > **Group Policy** > **IP Group** to enter the page.

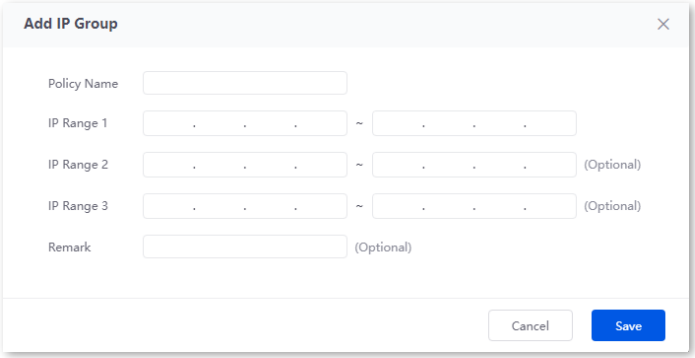
On this page, you can configure the IP group policy according to the actual requirements.

Configuration procedure:

1. Log in to the web UI of the router.
2. Navigate to **Audit** > **Group Policy** > **IP Group**.
3. Click **Add**.



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



----End

Parameter description

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

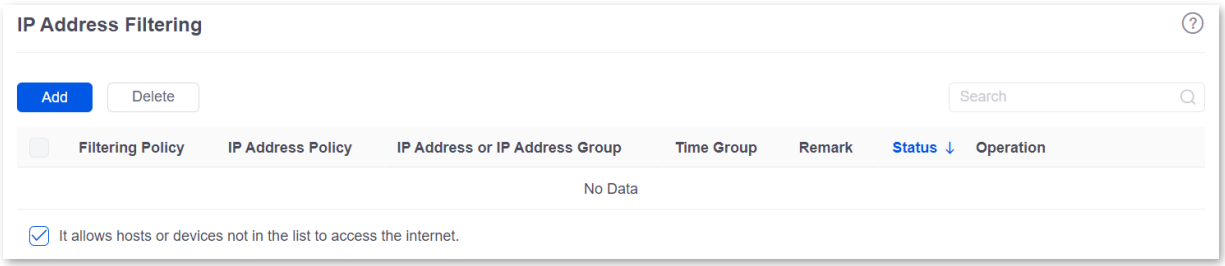
9.2 Filtering

9.2.1 IP address filtering

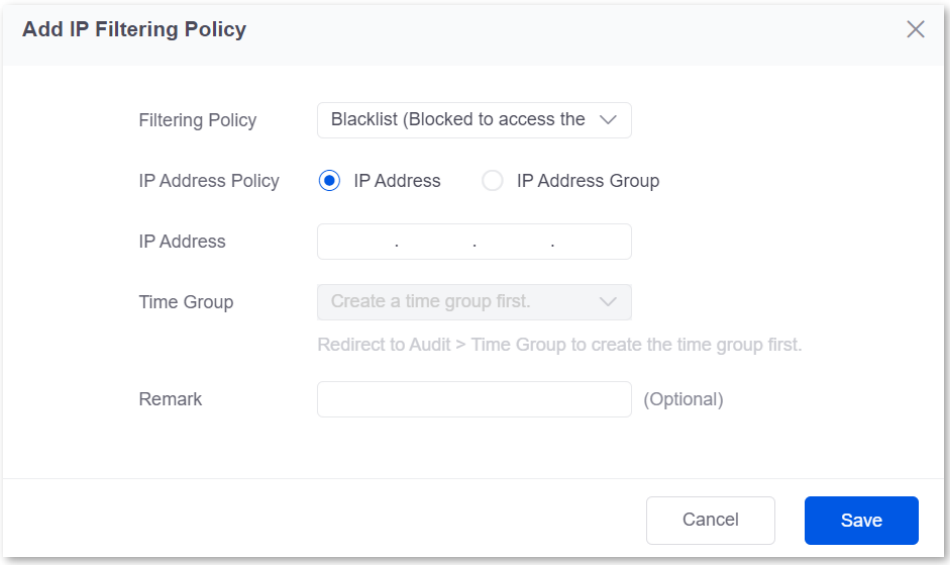
Overview

Navigate to **Audit** > **Filtering** > **IP address Filtering** to enter the page.

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



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



Parameter description

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

Example of configuring IP address filtering

Networking requirements

An enterprise uses the enterprise router to deploy a network.

Requirement: During the business hours (8:00 – 18: 00 from Monday to Friday), only purchasing staff can access the internet while other staff cannot access the internet.

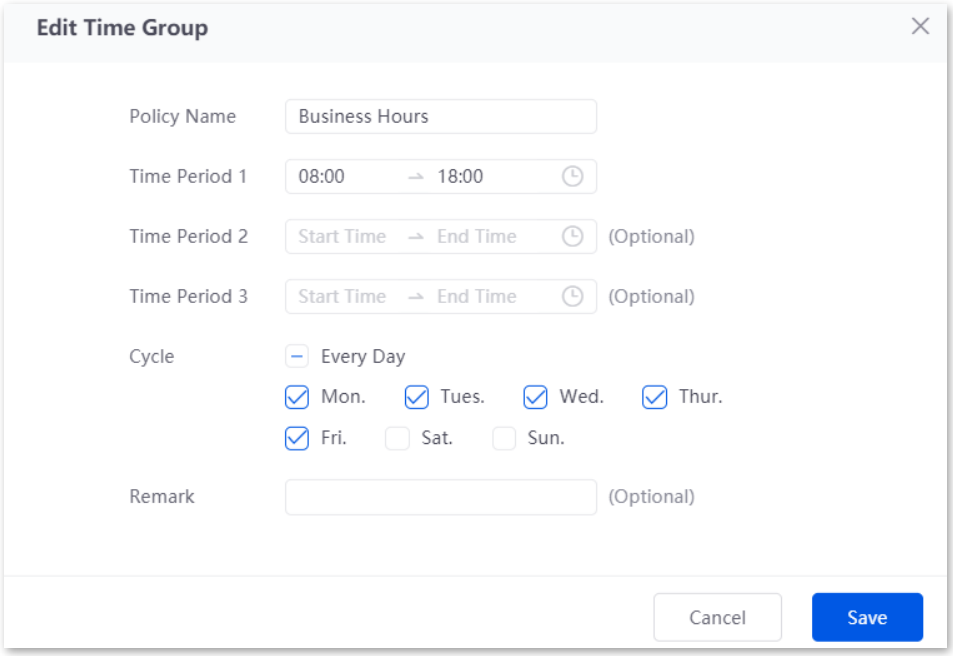
Solution

The router's IP address filtering function can achieve the requirement. Assume that the IP addresses of purchasing staff's computers range from 192.168.0.2 to 192.168.0.50.

Configuration procedure

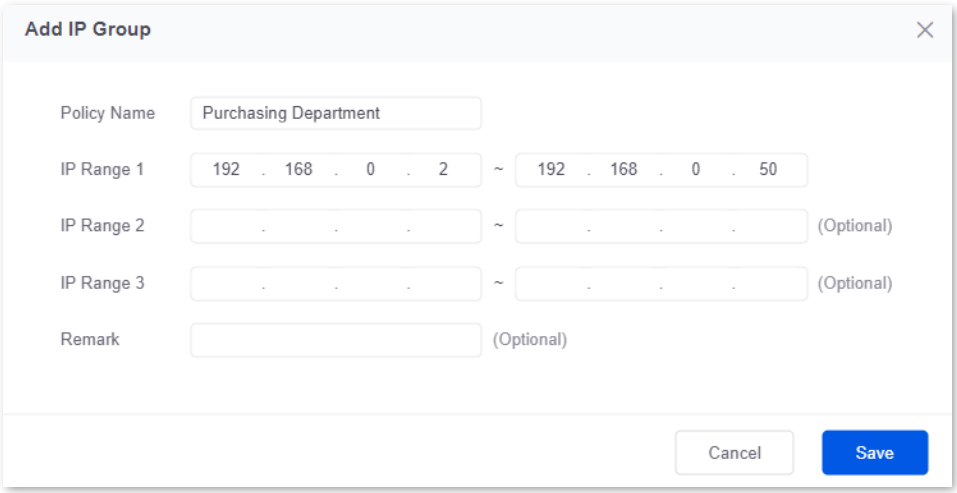
1. Log in to the web UI of the router.
2. Configure the time group.

   Navigate to **Audit** > **Group Policy** > **Time Group**, and configure the following time group.



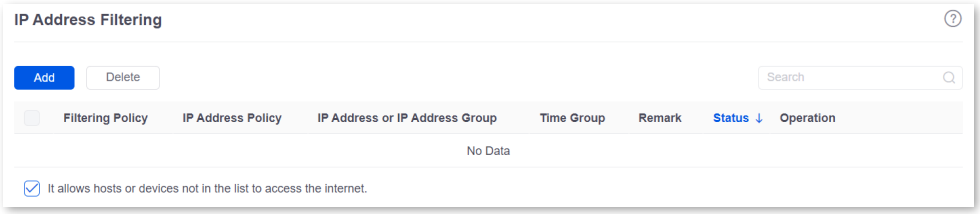
3. Configure the IP group.

   Navigate to **Audit** > **Group Policy** > **IP Group**, and configure the following IP group.



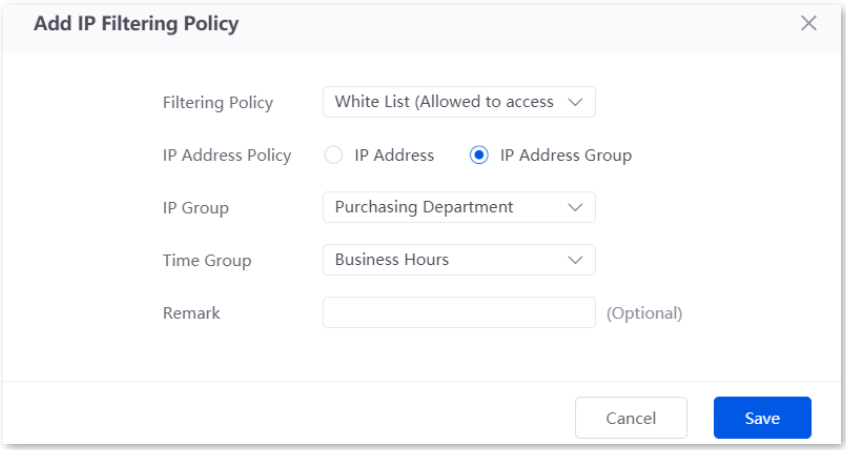
4. Add the IP address filtering policy.

   1) Navigate to **Audit** > **Filtering** > **IP Address Filtering**, and click **Add**.

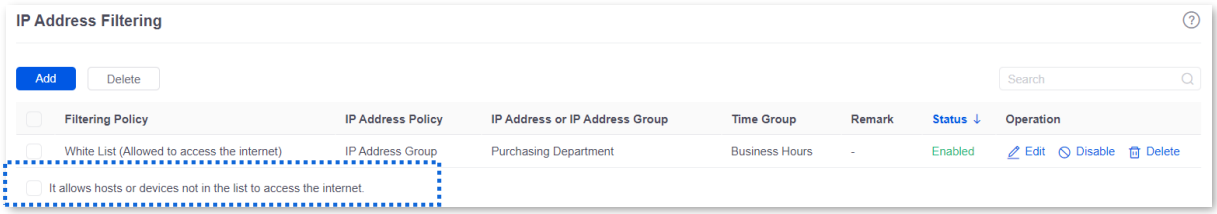


2) Configure the parameters in the **Add IP Filtering Policy** window, and click **Save**.

- Select the **Filtering Policy**, which is **Whitelist (Allowed to access the internet)** in this example.
- Select **IP Address Group** for **IP Address Policy**.
- Select the **IP Group** upon which the policy takes effect, which is **Purchasing Department** in this example.
- Select the **Time Group** upon which the policy takes effect, which is **Business Hours** in this example.



3) Deselect **Allow hosts or devices not in the list to access the internet**. In the displayed dialog box, click **OK**.



----End

Verification

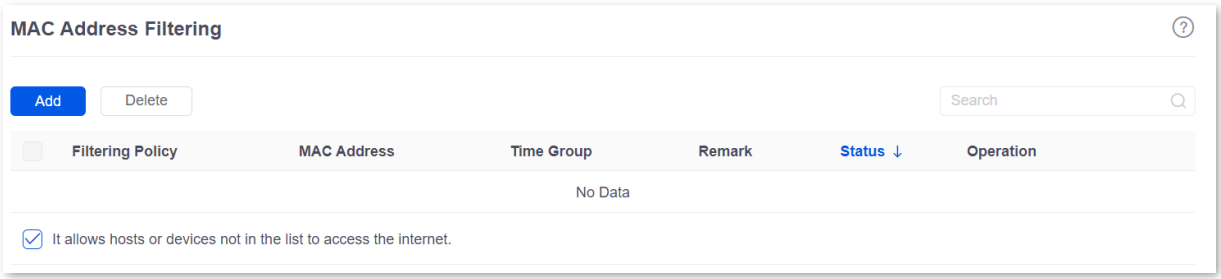
At 8:00 – 18:00 from Monday to Friday, only computers of purchasing staff (IP address range: 192.168.0.2 – 192.168.0.50) in the LAN can access the internet while other staff cannot access the internet.

9.2.2 MAC address filtering

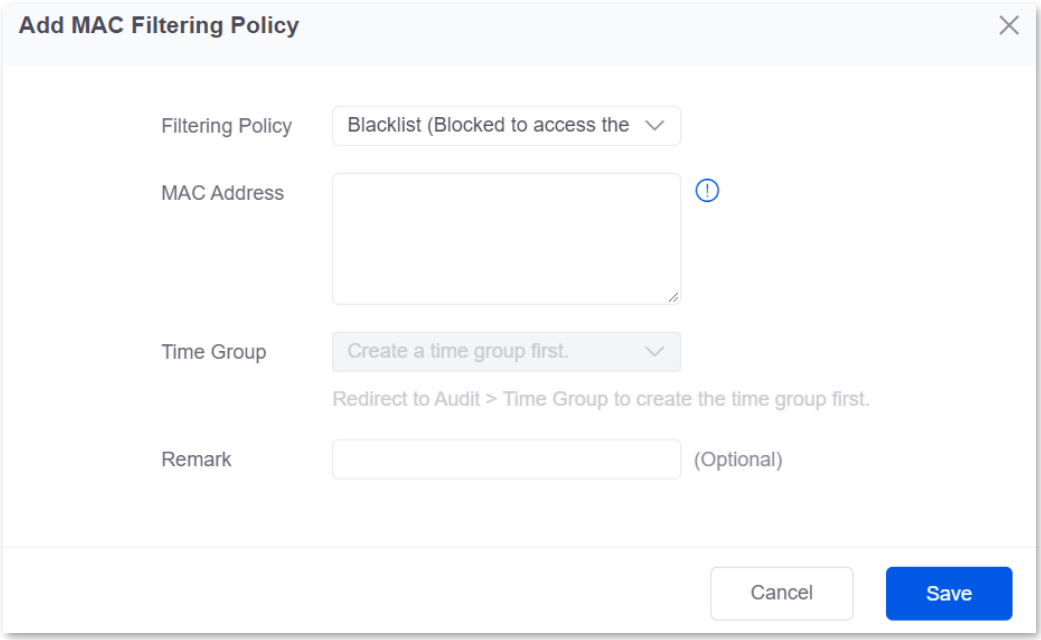
Overview

Navigate to **Audit** > **Filtering** > **MAC Address Filtering** to enter the page.

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



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



Parameter description

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

Parameter	Description
MAC Address	Specifies the MAC address in the **Blacklist** or **Whitelist.**
Time Group	Used to select the time group policy upon which the MAC address filtering policy takes effect. Note The time group should be configured in **Audit** > **Group Policy** > **Time Group** in advance.
Remark	Specifies the remark of the MAC address filtering policy. The remark is optional.
Status	Specifies the status of the MAC address filtering policy, **Enabled** or **Disabled**.
Allow hosts or devices not in the list to access the internet	– When Selected: The devices not in the filtering list or devices with the filtering policy disabled can access the internet. – When Deselected: The devices not in the filtering list or devices with the filtering policy disabled cannot access the internet. Note To deselect this function, configure a whitelist first.

Example of configuring MAC address filtering

Networking requirements

An enterprise uses the enterprise router to deploy a network.

Requirement: During the business hours (8:00 – 18: 00 from Monday to Friday), only a purchasing employee can access the internet while other staff cannot access the internet.

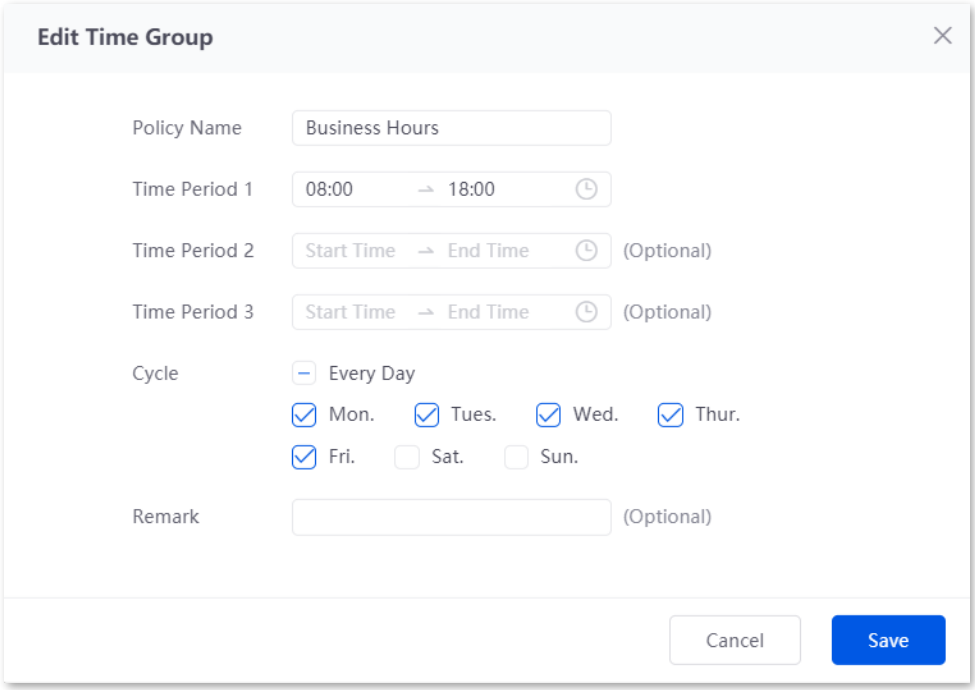
Solution

The router's MAC address filtering function can achieve the requirement. Assume that the MAC address of the purchasing employee's computer is CC:3A:61:71:1B:6E.

Configuration procedure

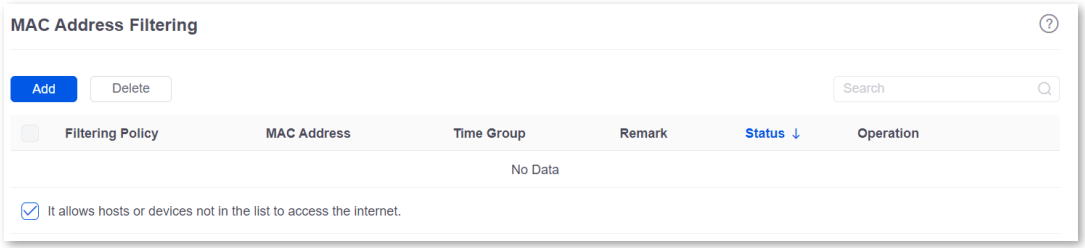
1. Log in to the web UI of the router.
2. Configure the time group.

   Navigate to **Audit** > **Group Policy** > **Time Group**, and configure the following time group.



3. Add the MAC address filtering policy.

1) Navigate to **Audit** > **Filtering** > **MAC Address Filtering**, and click **Add**.

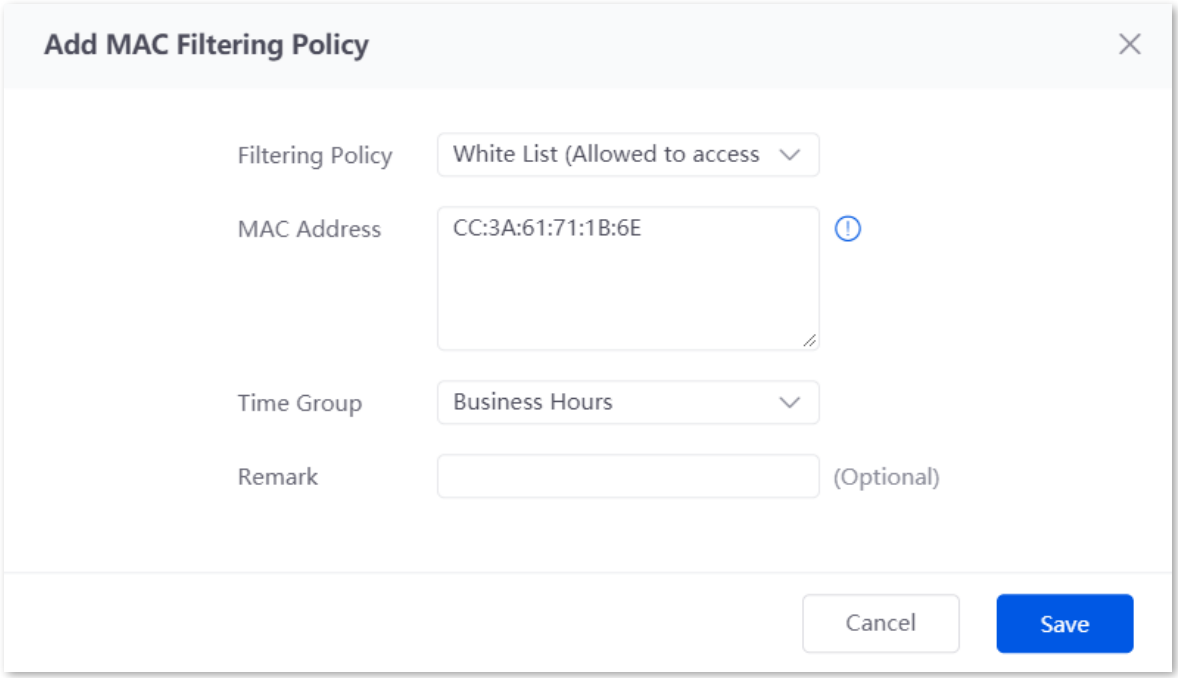


2) Configure the parameters in the **Add MAC Filtering Policy** window, and click **Save**.

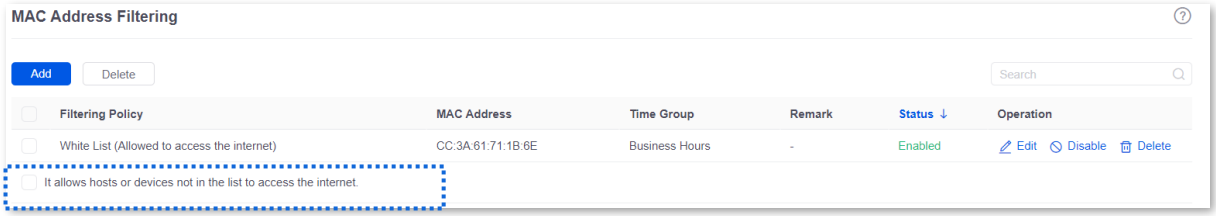
- Select the **Filtering Policy**, which is **Whitelist (Allowed to access the internet)** in this example.
- Enter the **MAC Address** allowed to access the internet, which is **CC:3A:61:71:1B:6E** in this example.
- Select the **Time Group** upon which the policy takes effect, which is **Business Hours** in this example.

Tip

If you need to filter multiple MAC addresses, use semicolons (;) to separate them.



3) Deselect **Allow hosts or devices not in the list to access the internet**. In the displayed dialog box, click **OK**.



----End

Verification

At 8:00 – 18:00 from Monday to Friday, only a purchasing employee using the computer with a MAC address of CC:3A:61:71:1B:6E in the LAN can access the internet while other staff cannot access the internet.

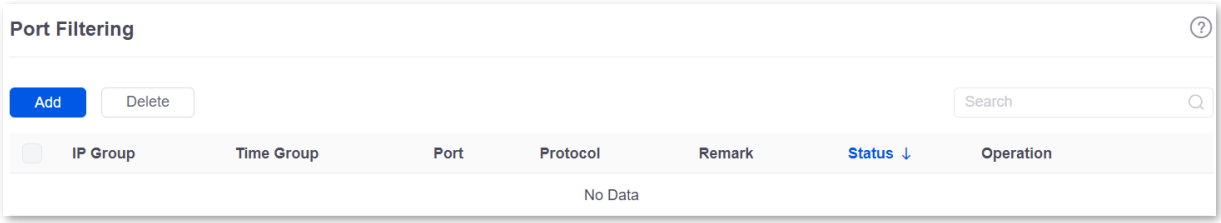
9.2.3 Port filtering

Overview

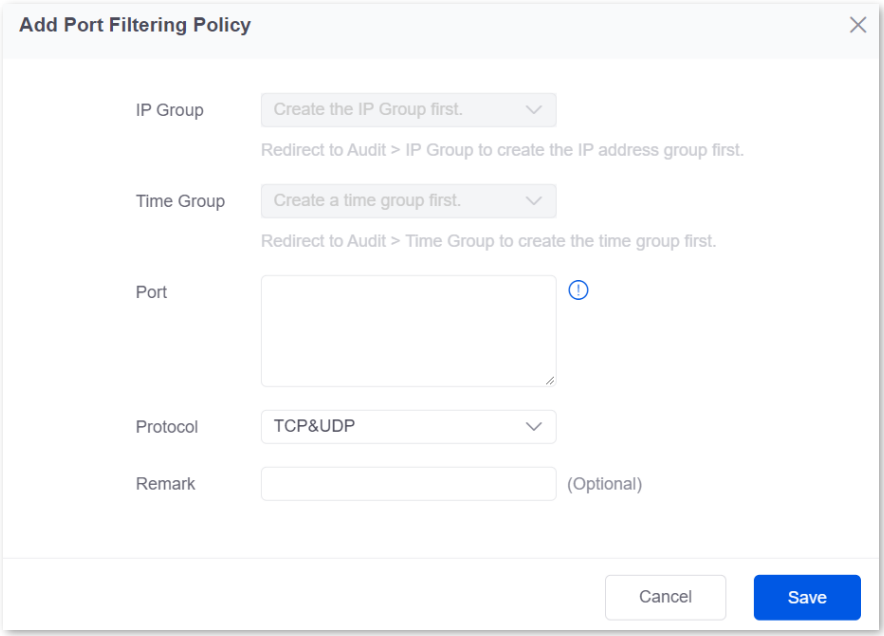
Application protocols for internet services have specific port numbers. 0 to 1023 are port numbers for some common services. These ports are generally fixed to specific services.

Navigate to **Audit** > **Filtering** > **Port Filtering** to enter the page.

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



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



Parameter description

Parameter	Description
IP Group	Used to select the IP address group policy upon which the port filtering policy takes effect. Note The IP address group should be configured in **Audit** > **Group Policy** > IP Group in advance.
Time Group	Used to select the time group policy upon which the port filtering policy takes effect. Note The time group should be configured in **Audit** > **Group Policy** > Time Group in advance.
Port	Specifies the service port forbidden to access.
Protocol	Specifies the service protocol forbidden to access.

Parameter	Description
Remark	Specifies the remark of the port filtering policy. The remark is optional.
Status	Specifies the status of the port filtering policy, **Enabled** or **Disabled**.

Example of configuring port filtering

Networking requirements

An enterprise uses the enterprise router to deploy a network.

Requirement: During the business hours (8:00 – 18: 00 from Monday to Friday), purchasing staff are forbidden to browse webpages (The default port number for webpage browsing is 80.).

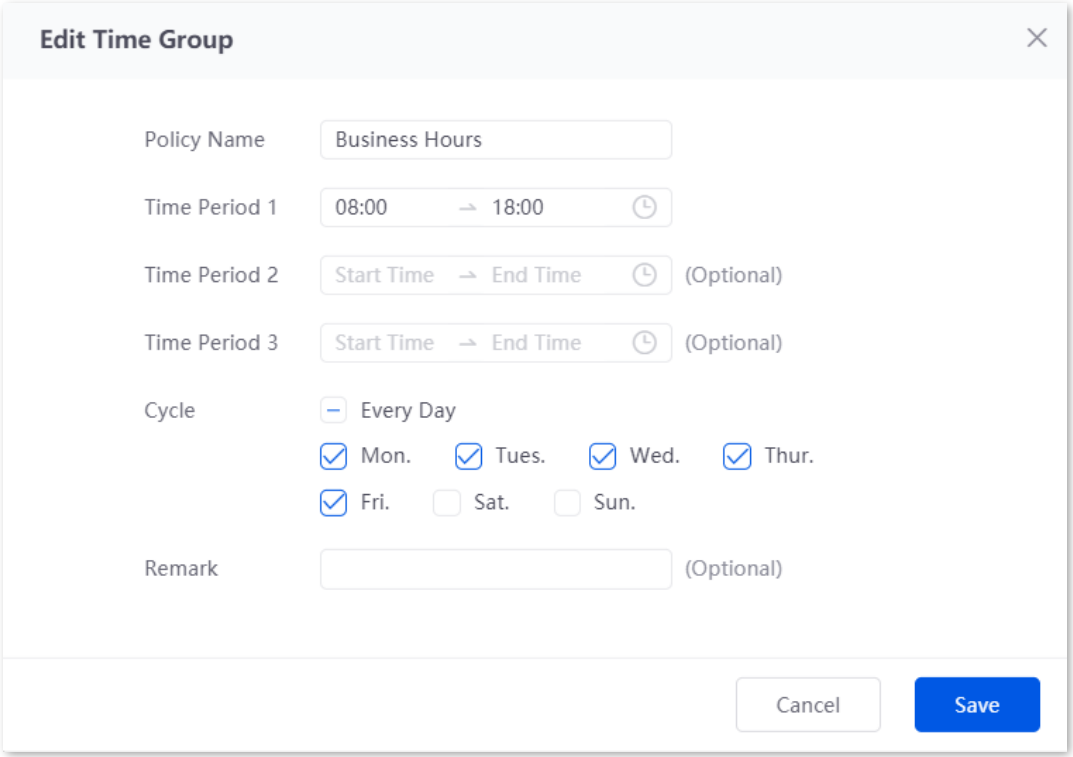
Solution

The router's port filtering function can achieve the requirement. Assume that the IP address of the purchasing staff's computers range from 192.168.0.2 – 192.168.0.50.

Configuration procedure

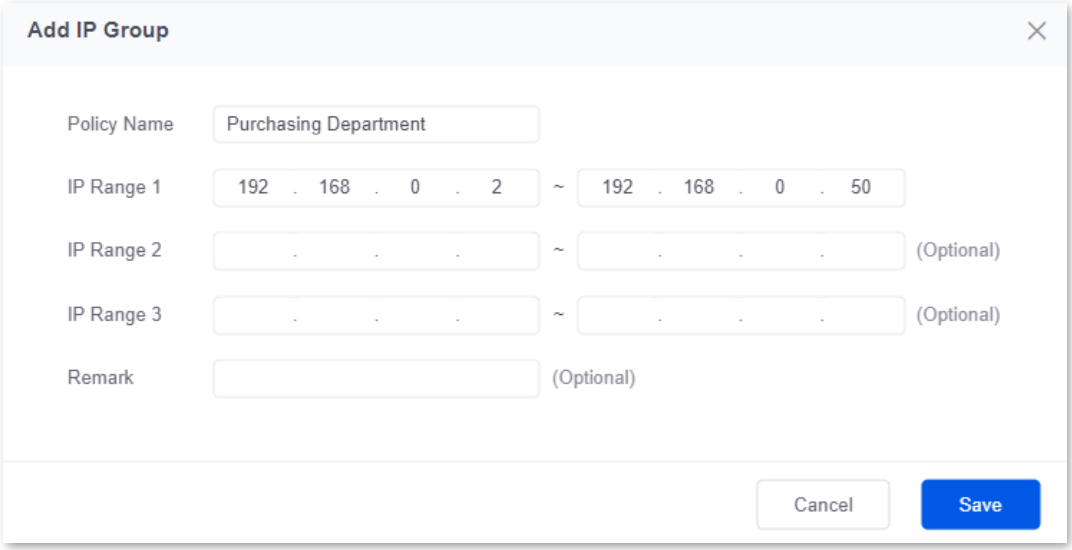
1. Log in to the web UI of the router.
2. Configure the time group.

   Navigate to **Audit** > **Group Policy** > **Time Group**, and configure the following time group.



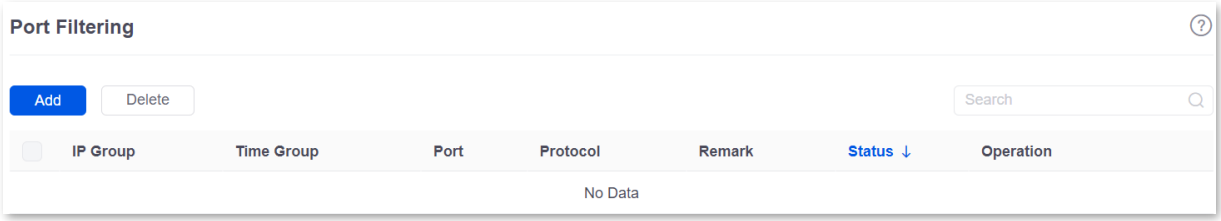
3. Configure the IP group.

   Navigate to **Audit** > **Group Policy** > **IP Group**, and configure the following IP group.



4. Add the port filtering policy.

   1) Navigate to **Audit** > **Filtering** > **Port Filtering**, and click **Add**.

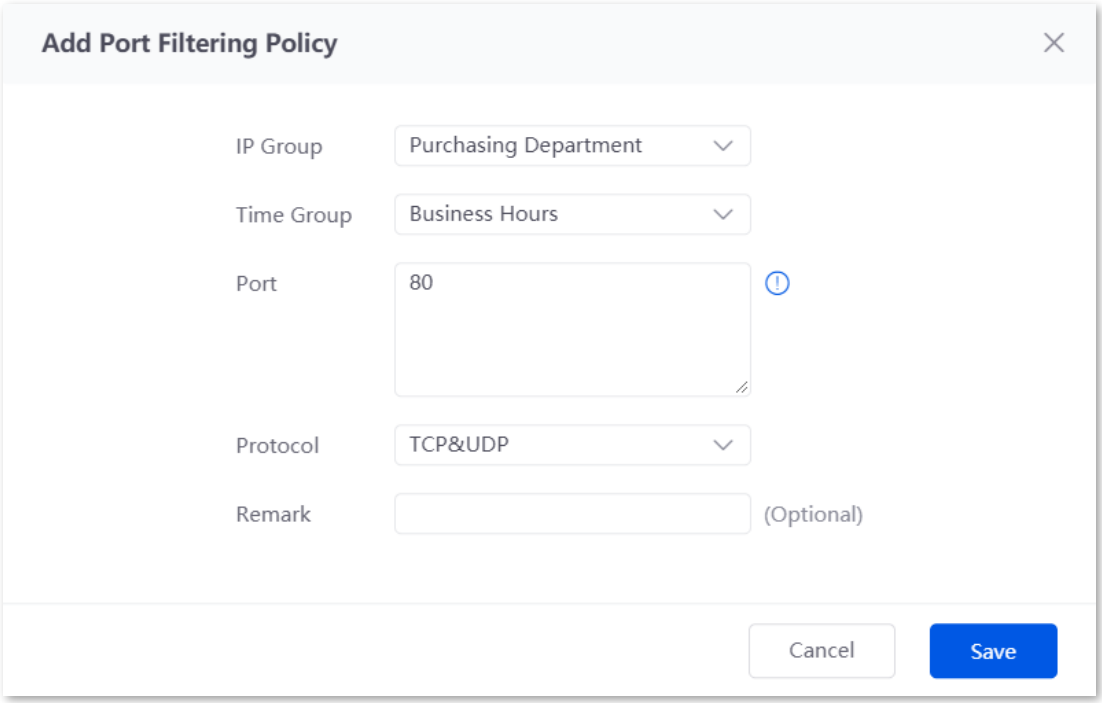


   2) Configure the parameters in the **Add Port Filtering Policy** window, and click **Save**.

      - Select the **IP Group** upon which the policy takes effect, which is **Purchasing Department** in this example.
      - Select the **Time Group** upon which the policy takes effect, which is **Business Hours** in this example.
      - Enter the **Port** number for webpage browsing, which is **80** in this example.
      - Select the **Protocol** used by the service. It is recommended to keep the default **TCP&UDP**.

Tip

- If you need to filter multiple non-consecutive ports, use semicolons (;) to separate them, such as **80;20**.
- If you need to filter multiple consecutive ports, use tildes (~) to connect them, such as **75~80**.



----End

Verification

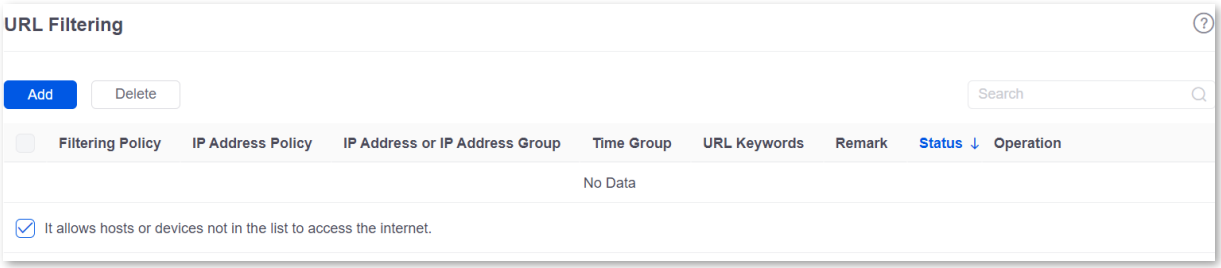
At 8:00 – 18:00 from Monday to Friday, purchasing staff using computers with IP addresses ranging from 192.168.0.2 – 192.168.0.50 in the LAN cannot browse webpages.

9.2.4 URL filtering

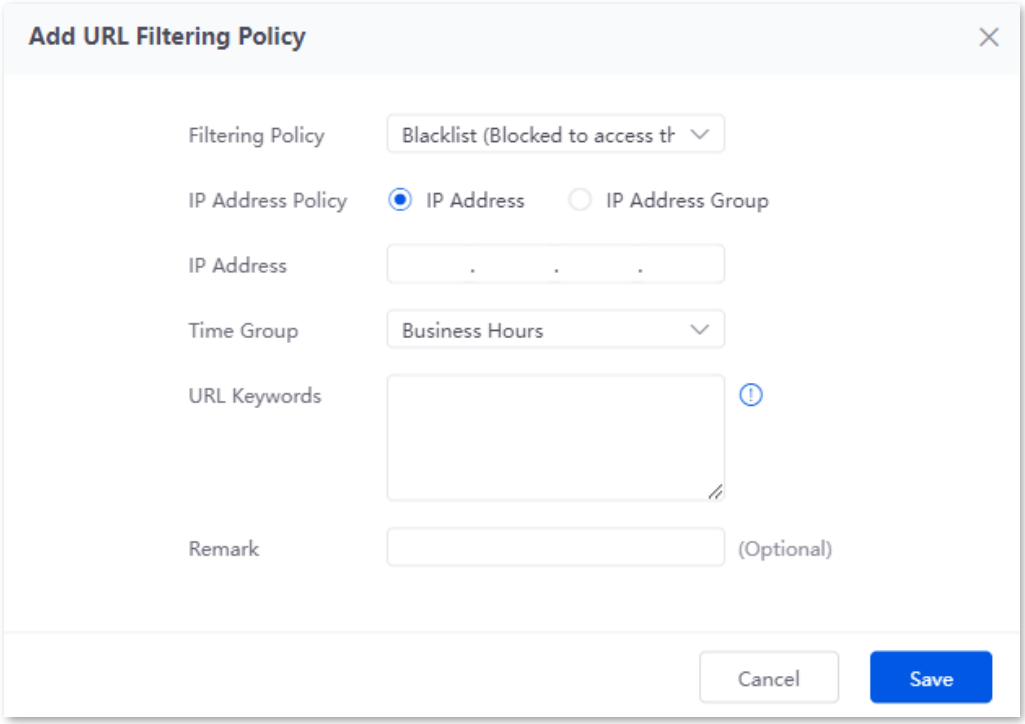
Overview

Navigate to **Audit** > **Filtering** > **URL Filtering** to enter the page.

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



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



Parameter description

Parameter	Description
Filtering Policy	Specifies the mode of the URL filtering policy. – **Blacklist (Blocked to access the internet)**: The user with the specified IP address is only blocked to access specified websites during the specified time period, and is allowed to access all websites during other time. – **Whitelist (Allowed to access the internet)**: The user with the specified IP address is only allowed to access specified websites during the specified time period, and is allowed to access all websites during other time.
IP Address Policy	To filter one IP address, select **IP Address** and enter the IP address.
IP Address or IP Address Group	To filter one or more IP address groups, select **IP Address Group** and select the corresponding IP group policy you set. Note The IP group should be configured in **Audit** > **Group Policy** > **IP Group** in advance.
Time Group	Used to select the time group policy upon which the URL filtering policy takes effect. Note The time group should be configured in **Audit** > **Group Policy** > **Time Group** in advance.
URL Keywords	Specifies the keywords of the URL forbidden/allowed to access.

Parameter	Description
Remark	Specifies the remark of the URL filtering policy. The remark is optional.
Status	Specifies the status of the URL filtering policy, **Enabled** or **Disabled**.
Allow hosts or devices not in the list to access the internet	– When Selected: The devices not in the filtering list or devices with the filtering policy disabled can access the specified websites. – When Deselected: The devices not in the filtering list or devices with the filtering policy disabled cannot access the specified websites. Note To deselect this function, configure a whitelist first.

Example of configuring URL filtering

Networking requirements

An enterprise uses the enterprise router to deploy a network.

Requirement: During the business hours (8:00 – 18: 00 from Monday to Friday), only designers can access some websites for designing, such as Pinterest (pinterest.com), Behance (behance.net) and Dribbble (dribbble.com), while other staff cannot access the internet.

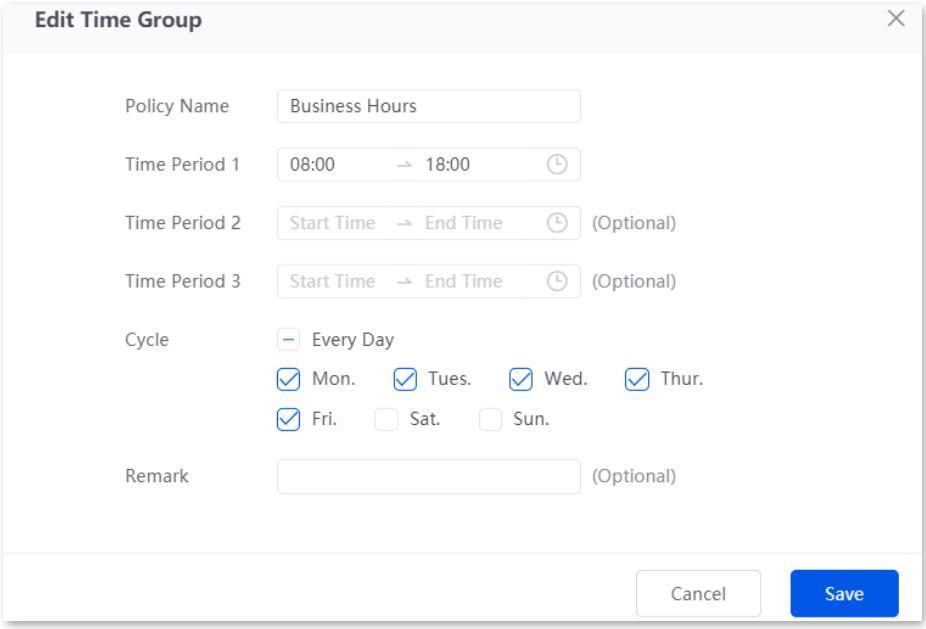
Solution

The router's URL filtering function can achieve the requirement. Assume that the IP addresses of designers' computers range from 192.168.0.60 to 192.168.0.0.

Configuration procedure

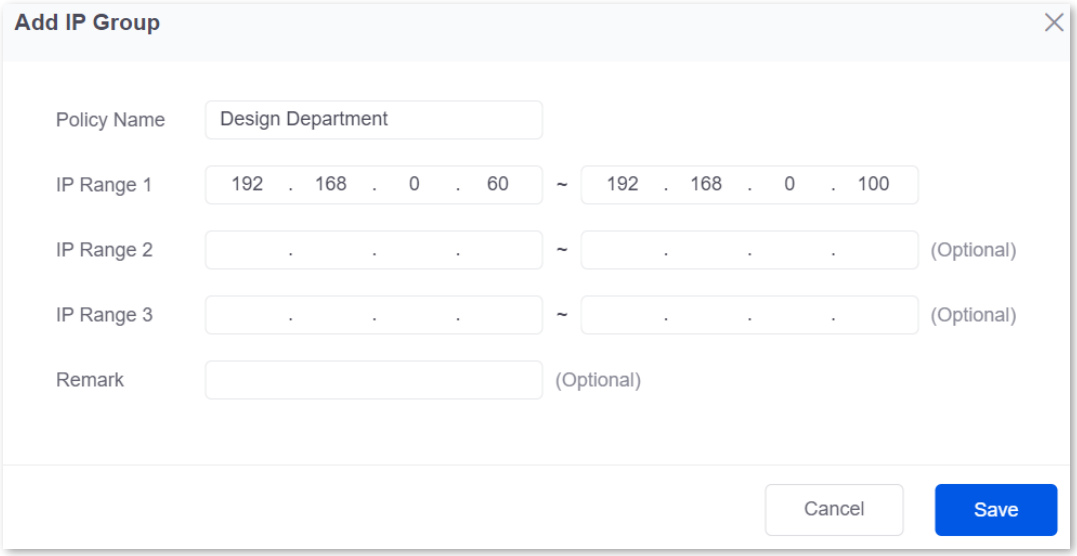
1. Log in to the web UI of the router.
2. Configure the time group.

   Navigate to **Audit** > **Group Policy** > **Time Group**, and configure the following time group.



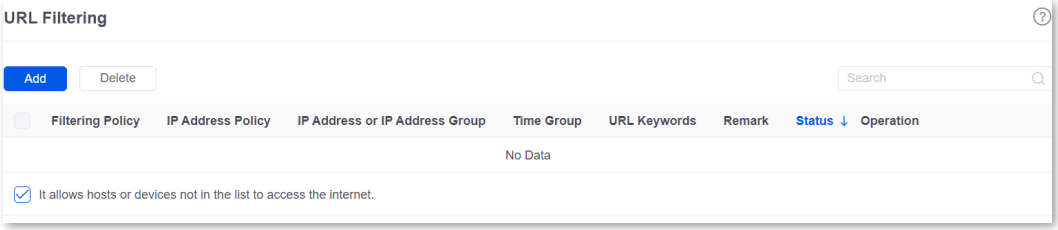
3. Configure the IP group.

   Navigate to **Audit** > **Group Policy** > **IP Group**, and configure the following IP group.



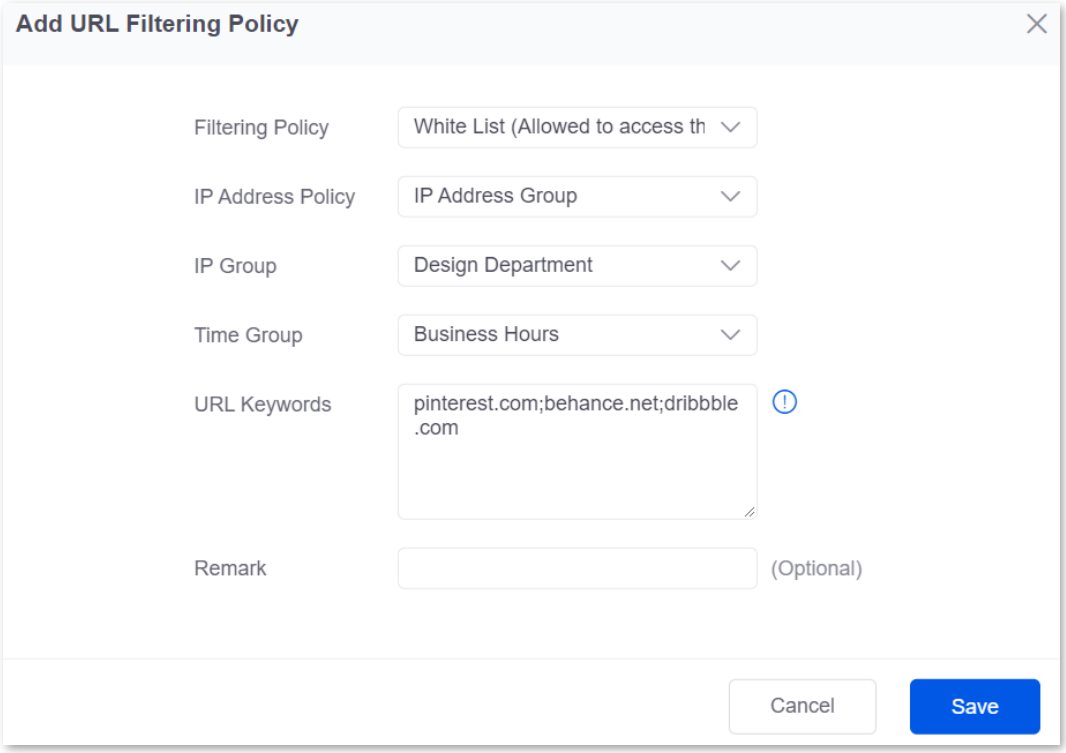
4. Add the URL filtering policy.

   1) Navigate to **Audit** > **Filtering** > **URL Filtering**, and click **Add**.

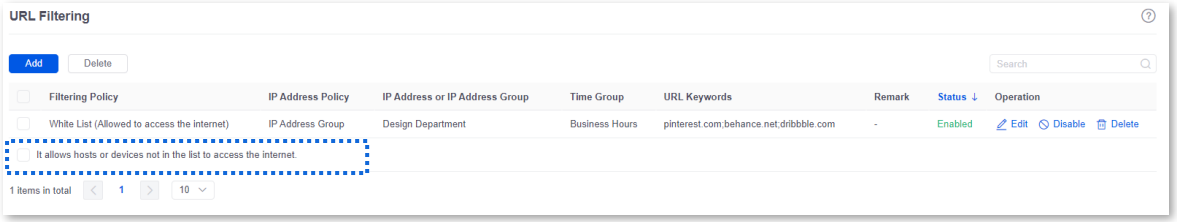


   2) Configure the parameters in the **Add URL Filtering Policy** window, and click **Save**.

- Select the **Filtering Policy**, which is **Whitelist (Allowed to access the internet)** in this example.
- Select **IP Address Group** for **IP Address Policy**.
- Select the **IP Group** upon which the policy takes effect, which is **Design Department** in this example.
- Select the **Time Group** upon which the policy takes effect, which is **Business Hours** in this example.
- Enter the **URL Keywords**, which are **pinterest.com;behance.net;dribbble.com** in this example.



3) Deselect **Allow hosts or devices not in the list to access the internet**. In the displayed dialog box, click **OK**.



----End

Verification

At 8:00 – 18:00 from Monday to Friday, only computers of designers (IP address range: 192.168.0.60 – 192.168.0.100) in the LAN can access the websites of pinterest.com, behance.net and dribbble.com while other computers cannot access the internet.

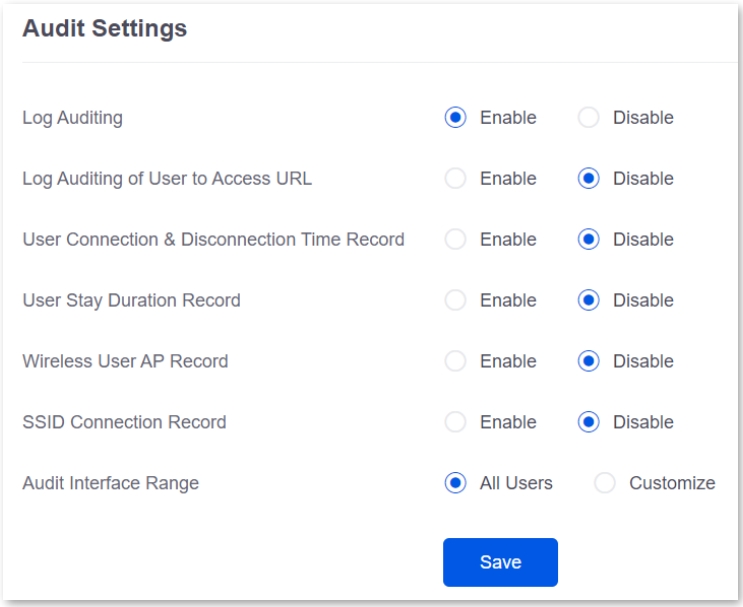
9.3 Log auditing

9.3.1 Audit settings

Navigate to **Audit** > **Log Audit** > **Audit Settings** to enter the page.

On this page, you can collect specified types of logs from the specified port as required.

This function is disabled by default. After it is enabled, the following information is displayed.



Parameter description

Parameter	Description
Log Auditing	Used to enable or disable the log auditing function.
Log Auditing of User to Access URL	Used to enable or disable the function to record the information of web pages accessed by users.
User Connection & Disconnection Time Record	Used to enable or disable the function to record the time at which a user obtains an IP address from the user DHCP server.
User Stay Duration Record	Used to enable or disable the function to record the users' online duration.
Wireless User AP Record	Used to enable or disable the function to record the information about the AP connected to the wireless user.
SSID Connection Record	Used to enable or disable the function to record the name of the SSID connected to the wireless user.

Parameter	Description
Audit Interface Range	Specifies the interface on which the log audit takes effect. – **All Users**: Audit the logs of all VLAN interfaces and wireless interfaces. – **Customize**: Audit the logs of selected VLAN interfaces and wireless interfaces.

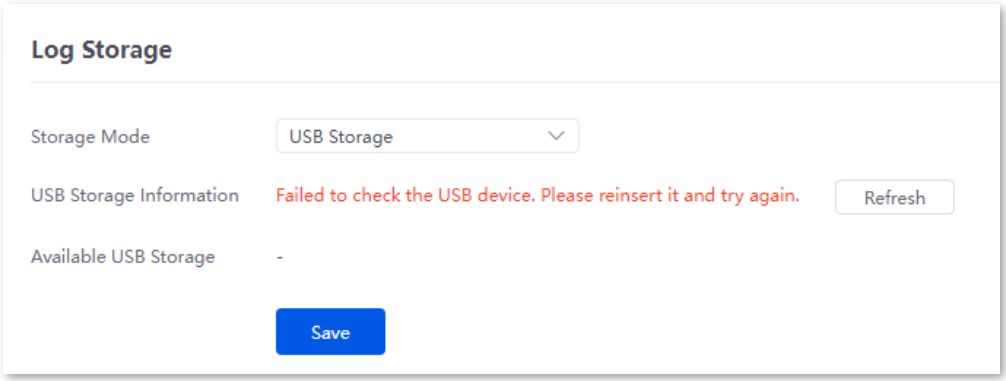
9.3.2 Log storage

Navigate to **Audit** > **Log Audit** > **Log Storage** to enter the page.

When the log auditing function is enabled, the result of log auditing can only be stored to the local PC or a USB disk. A log tool is required to be installed in the local computer, such as **Syslog**.

Only some routers support this function. Please refer to the actual product.

USB storage is enabled by default, as shown in the following figure.



Parameter description

Parameter	Description
Storage Mode	Specifies the mode of storage. – **USB Storage**: Store the result of log auditing to other USB storage devices through USB ports. – **Local Computer Storage**: Store the result of log auditing on the local computer.
USB Storage Information	Specifies the basic information of the USB storage device. When the **Storage Mode** is **USB Storage**, the system will automatically obtain the information.
Available USB Storage	Specifies the available storage space of the USB storage device. When the **Storage Mode** is **USB Storage**, the system will automatically scan the device.
Local Computer IP Address	Specifies the IP address of the local computer where the result of log auditing is stored. It is needed when the **Storage Mode** is **Local Computer Storage**

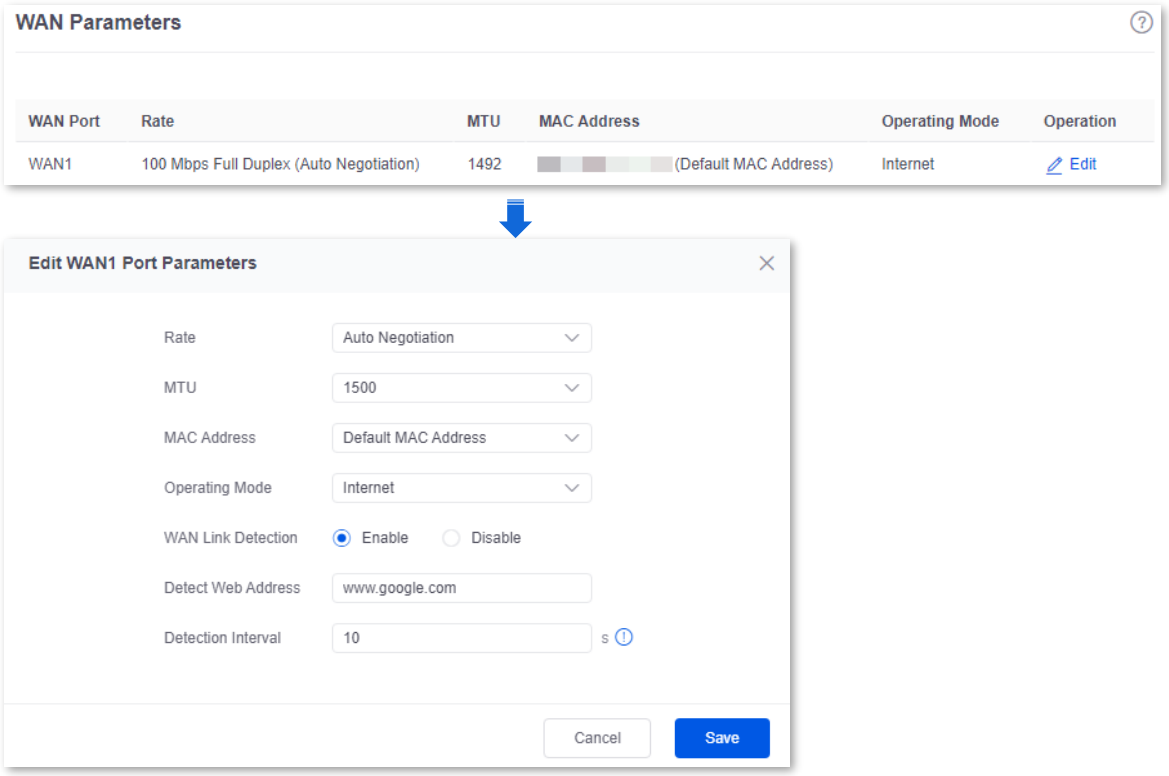
10 More

10.1 Advanced routing

10.1.1 WAN parameters

Navigate to **More** > **Advanced Routing** > **WAN Parameters** to enter the page. On this page, you can configure the parameters of the WAN port.

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



Parameter description

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

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

Parameter	Description
Detect Web Address	Specifies the domain name that needs to be detected. Note When the WAN Link Detection function is enabled, **Detect Web Address** can be configured.
Detection Interval	Specifies the interval to perform detections. Note When the WAN Link Detection function is enabled, **Detection Interval** can be configured.
Operation	Edit: Used to modify the WAN parameters.

10.1.2 Multi-WAN policy

Overview

Navigate to **More** > **Advanced Routing** > **Multi-WAN Policy** to enter the page. On this page, you can configure the multi-WAN policy and E-bank data based on source in&out.

- **Multi-WAN policy**

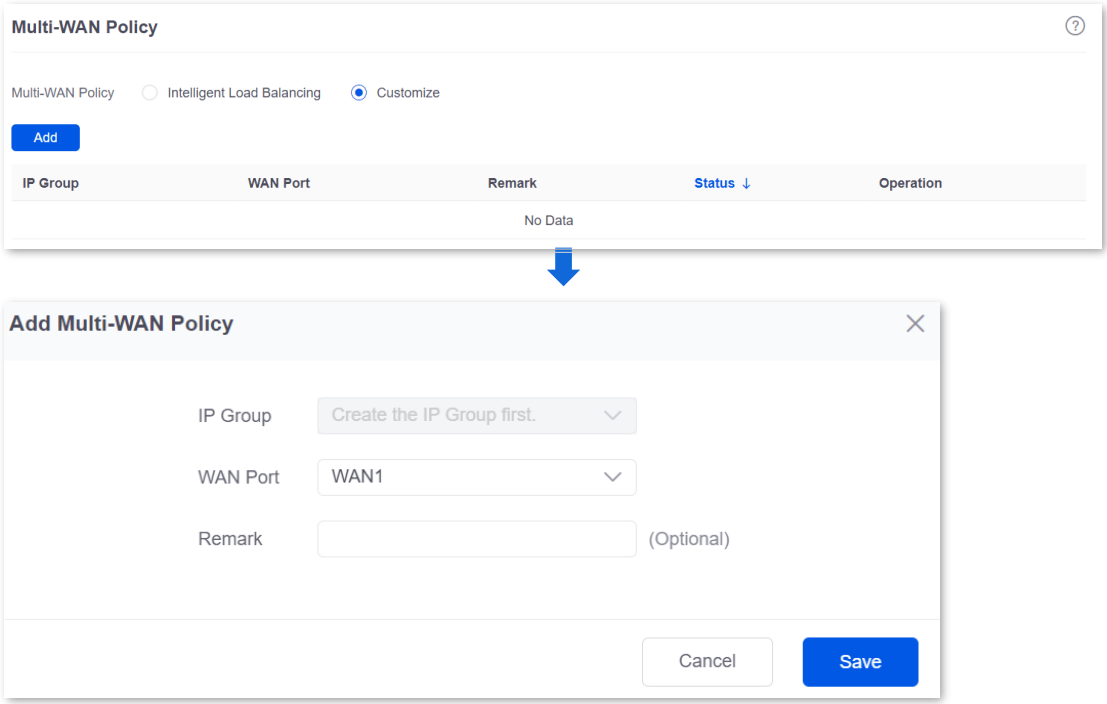
  After the router enables multiple WAN ports, it can allow multiple broadband access at the same time to achieve bandwidth superposition. When multiple WAN ports are working at the same time, setting a reasonable multi-WAN policy can greatly improve the bandwidth utilization of the router.

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

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

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

  By default, the router's multi-WAN policy is **Intelligent Load Balancing**. When **Customize** is selected, the page is as follows. You can click **Add** to customize the multi-WAN policy.



Parameter description

Parameter	Description
Add	Used to add a new multi-WAN policy.
IP Group	Specifies the IP group of the multi-WAN policy. Data traffic from this IP group which can only be forwarded through the specified WAN port. Only one rule can be configured for an IP group. You can configure the IP group in **Audit** > **Group Policy** > **IP Group**.
WAN Port	Specifies the WAN port of the multi-WAN policy. Data traffic from the specified IP group will only be forwarded through this WAN port.
Remark	Specifies the description of the multi-WAN policy.
Status	Specifies the status of the customized multi-WAN policy, including **Enabled**, **Disabled**.
Operation	Used to edit, enable, disable or delete the multi-WAN policy. Edit: Used to modify the multi-WAN policy. Enable: Used to enable the multi-WAN policy. Disable: Used to disable the multi-WAN policy. Delete: Used to delete the multi-WAN policy.

Example of configuring multi-WAN policy

Networking requirements

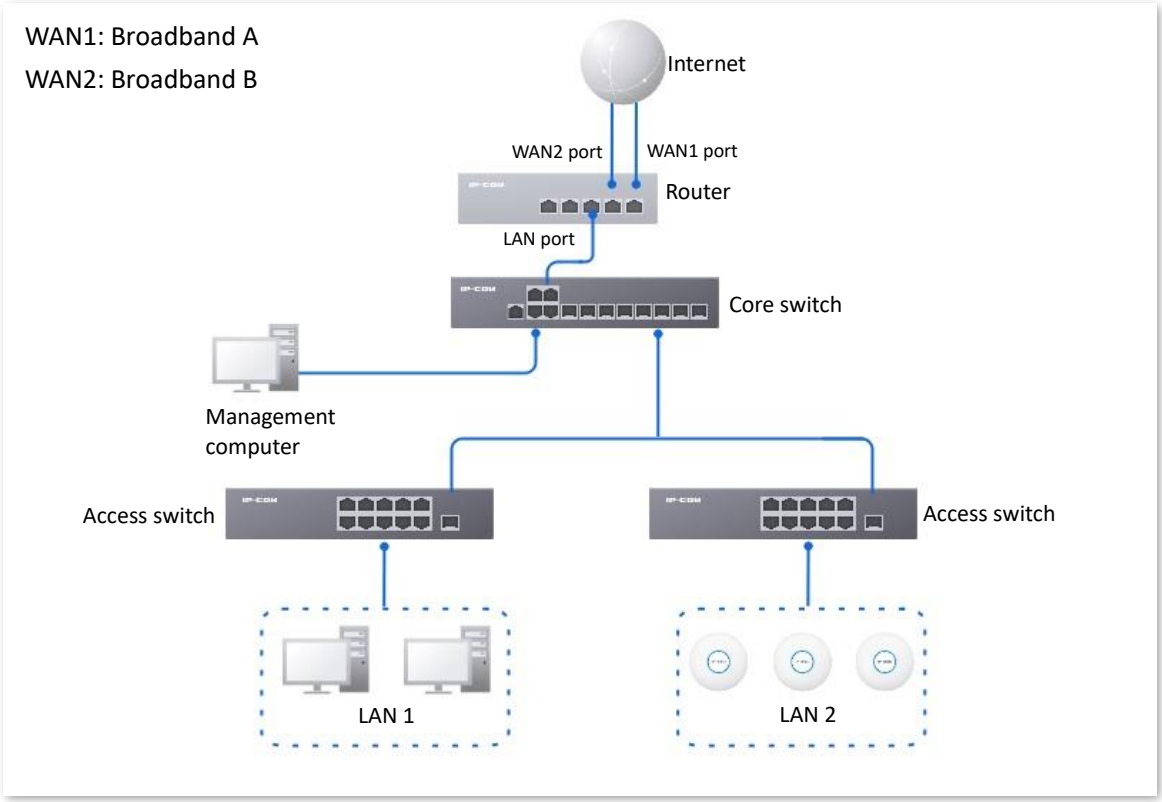
An enterprise uses the enterprise router to set up a network. To meet the requirements of the enterprise network, two broadband lines have been handled and the internet has been successfully accessed.

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

- Computers with IP addresses 192.168.0.2 to 192.168.0.100 access the internet through Broadband A.
- Computers with IP addresses 192.168.0.101 to 192.168.0.250 access the internet through Broadband B.

Solution

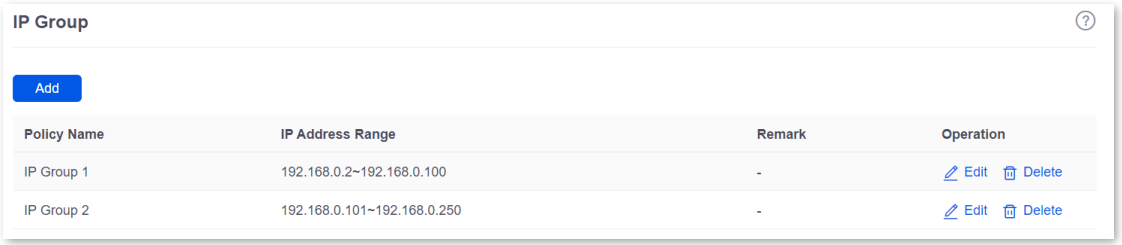
You can use the multi-WAN policy function of the router to meet the requirements.



Configuration procedure

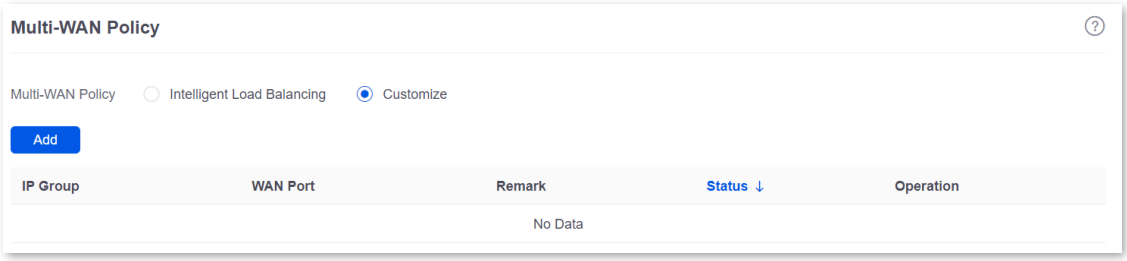
1. Log in to the Web UI of the router.
2. Configure the IP group.

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



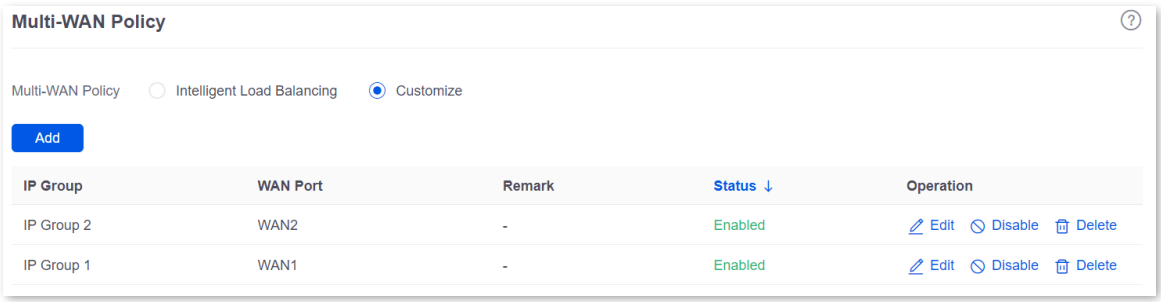
3. Enable the multi-WAN policy function.

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



4. Customize the multi-WAN policy.

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



----End

Verification

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

10.1.3 Static routing

Overview

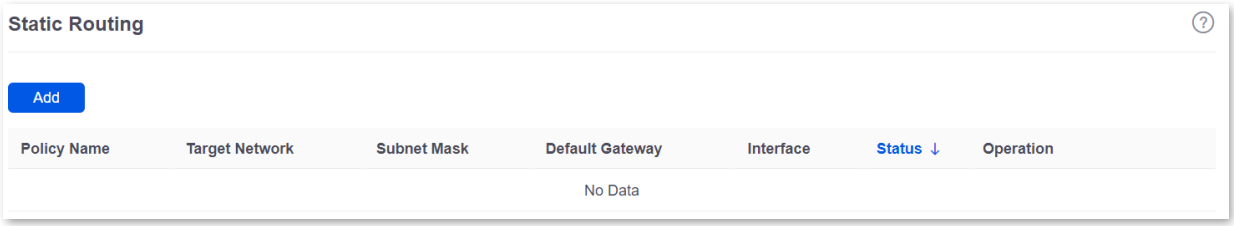
Routing is an operation to choose an optimum path to convey data from the source address to the target address. A static route is a manually configured special route and is simpler, more efficient, and more reliable. An appropriate static route can reduce issues arising from route selection and ease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

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

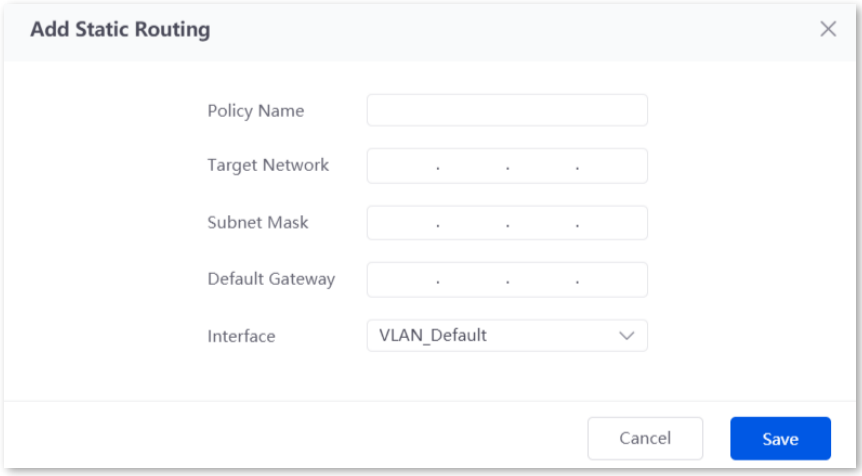
Note

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

Navigate to **More** > **Advanced Routing** > **Static Routing** to enter the page. On this page, you can configure the corresponding static routing according to actual network conditions. You can click ⋮ to select parameters to be displayed.



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



Parameter description

Parameter	Description
Policy Name	Specifies the name of the static routing policy.
Target Network	Specifies the IP address of the target network. **0.0.0.0** target network and **0.0.0.0** subnet mask indicate the default route. Tip If no accurate route is found in the route table, the router chooses the default route to forward data packets.
Subnet Mask	Specifies the subnet mask of the target network.
Default Gateway	Specifies the ingress port IP address of the next hop route after data packets egress from the router. **0.0.0.0** indicates direct routing, which means that the target network is directly connected to the interface of the router.
Interface	Specifies the interface from which packets egress. Select it as required.
Status	Specifies the current policy status, including **Enabled** and **Disabled**.
Operation	Used to edit, enable, disable or delete the static routing policy. Edit: Used to modify the static routing policy. Enable: Used to enable the static routing policy. Disable: Used to disable the static routing policy. Delete: Used to delete the static routing policy.

Example of configuring static routing

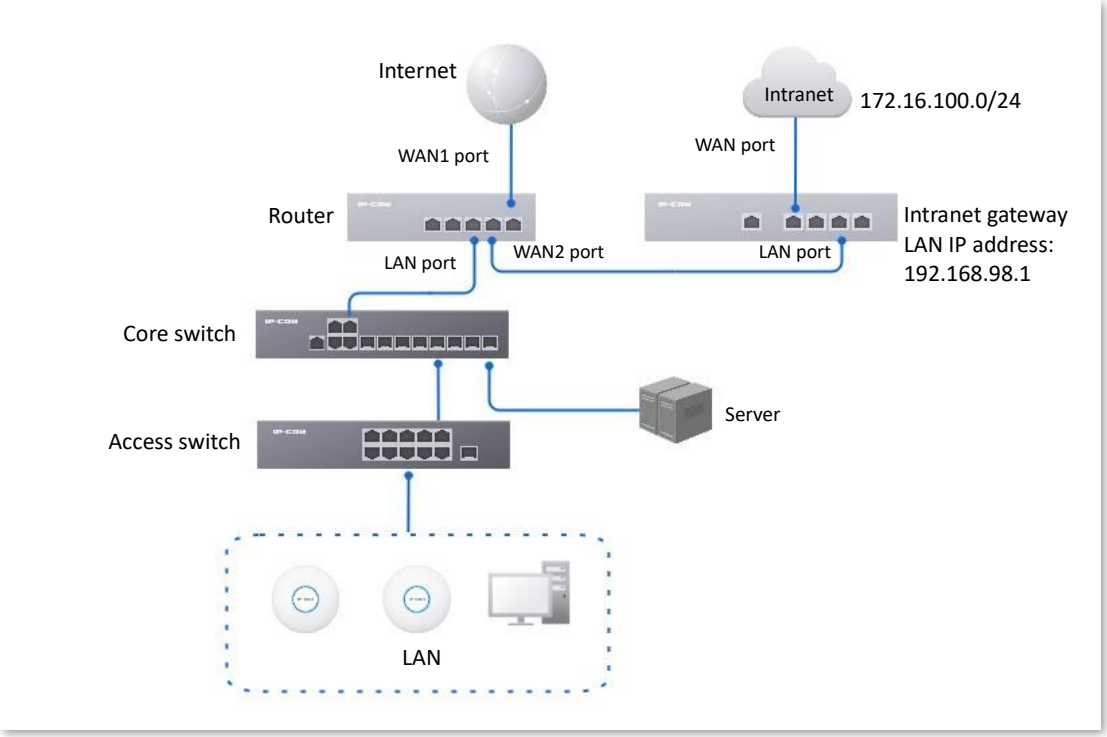
Networking requirements

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

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

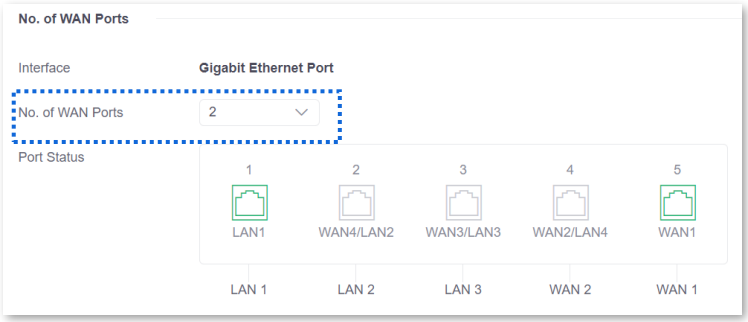
Solution

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

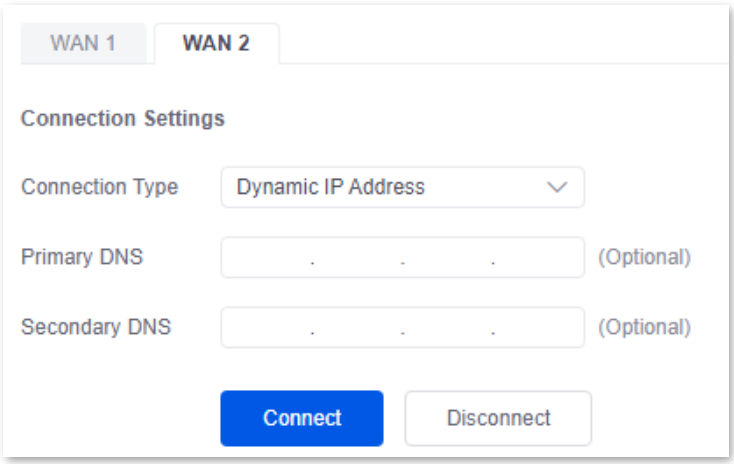


Configuration procedure

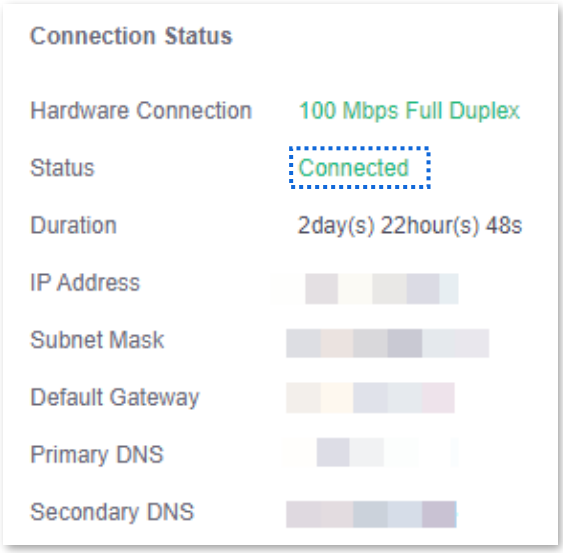
1. Log in to the Web UI of the router.
2. Enable two WAN ports and connect WAN2 port to the internet.
   1) Navigate to **Network** > **Internet Settings**.
   2) Set **No. of WAN Ports** to **2**.



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



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



3. Configure the static routing.

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

Navigate to **Network > Internet Settings,** and view the IP address information obtained by WAN2 under **Connection Status**, assuming the following:

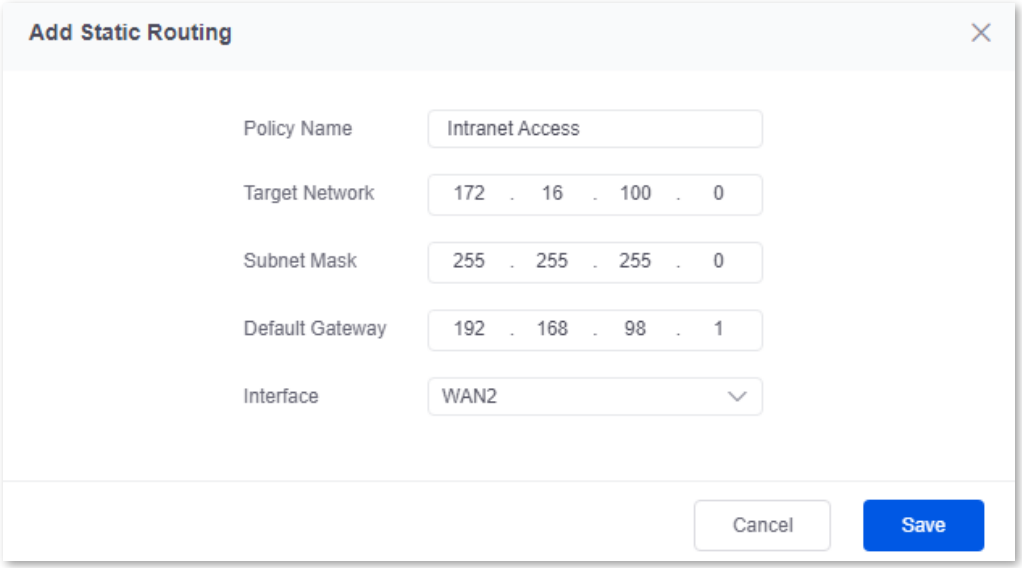
WAN2 IP Address	Subnet Mask	Default Gateway	Primary DNS
192.168.98.190	255.255.255.0	192.168.98.1	192.168.98.1

2) Configure parameters of the static routing.

The following table lists the static routing parameters for example:

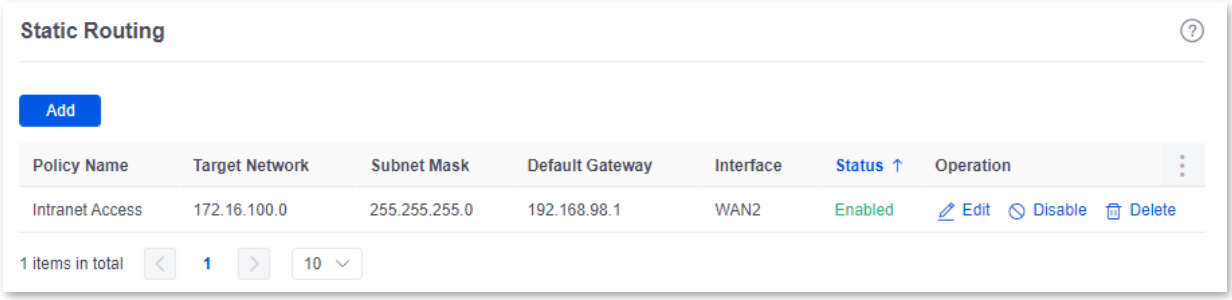
Policy Name	Target Network	Subnet Mask	Default Gateway	Interface
Intranet Access	172.16.100.0	255.255.255.0	192.168.98.1	WAN2

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



----End

The static route is added successfully.

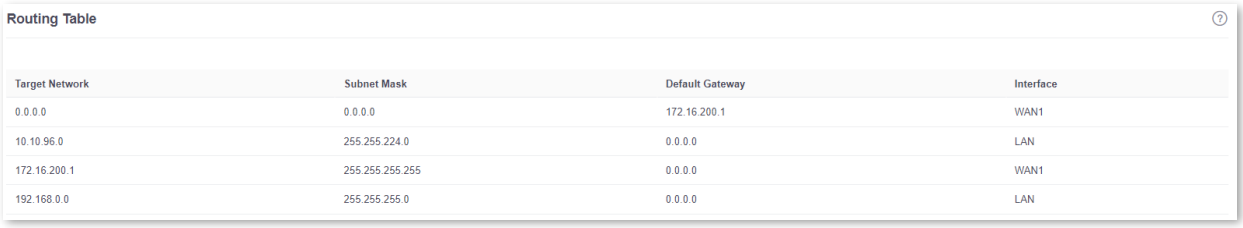


Verification

LAN users can access both the internet and the intranet.

10.1.4 Routing table

Navigate to **More** > **Advanced Routing** > **Routing Table** to enter the page. On this page, you can view the detailed routing information of the router.



Parameter description

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

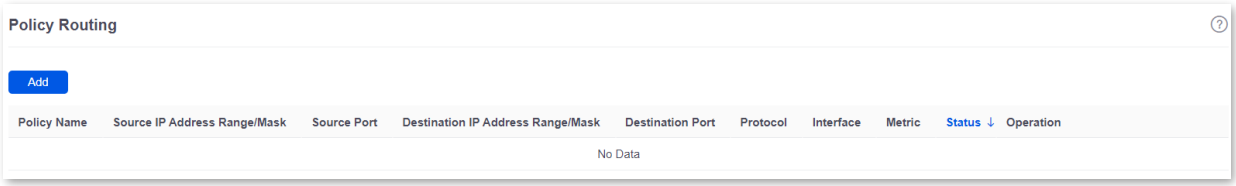
10.1.5 Policy routing

Overview

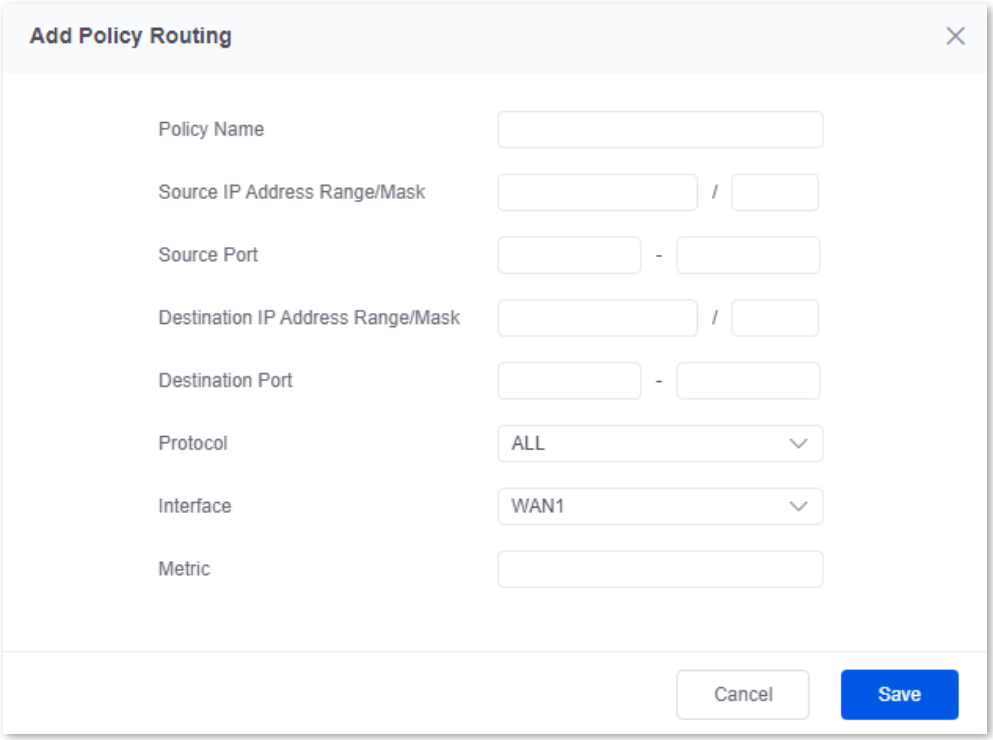
Policy routing, also known as policy-based routing, means that the next hop forwarding address of an IP packet is determined by a comprehensive consideration of multiple factors, rather than the destination or source IP address. You can set the source network, target network, destination port, protocol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

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

Navigate to **More** > **Advanced Routing** > **Policy Routing** to enter the page. On this page, you can configure the policy routing according to your needs.



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



Parameter description

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

Example of configuring policy routing

Networking requirements

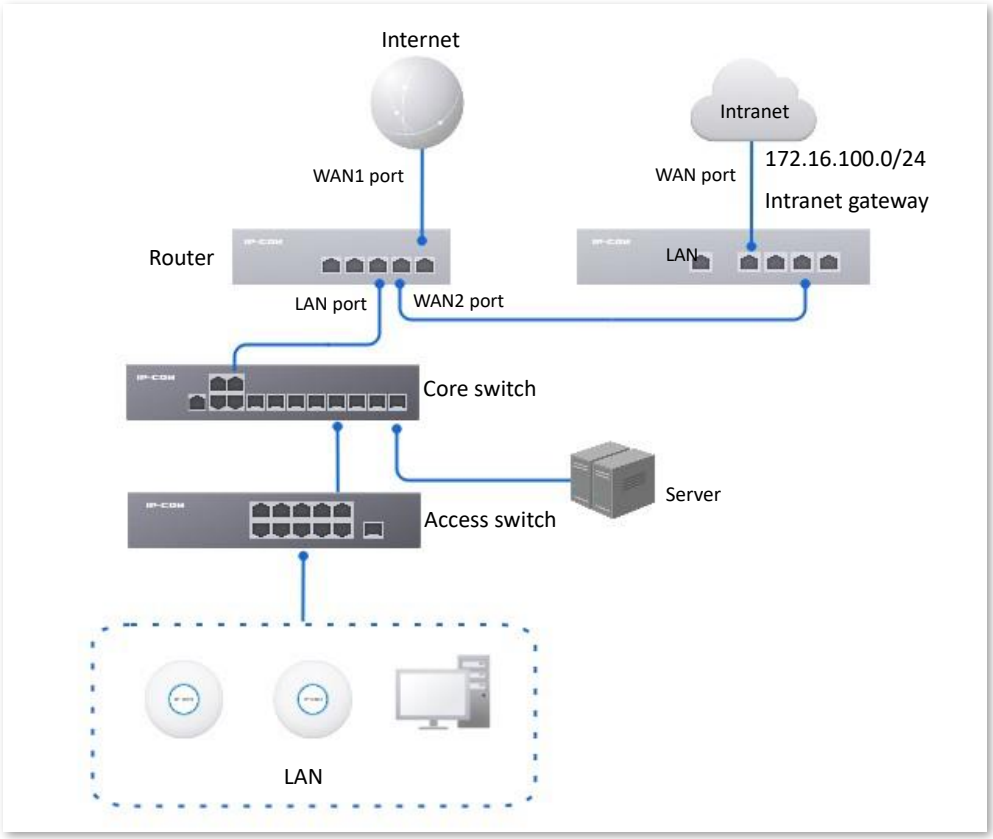
An enterprise uses the enterprise router to set up a network. The router is connected to the internet through PPPoE. The enterprise has built a Web server on the intranet, which is in a

different network from the internet. The access mode of the enterprise's intranet is dynamic IP address.

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

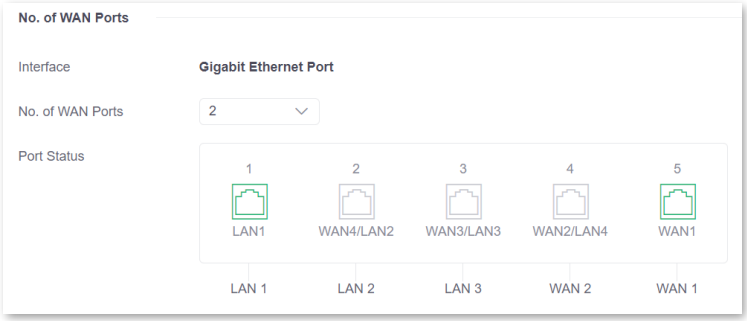
Solution

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

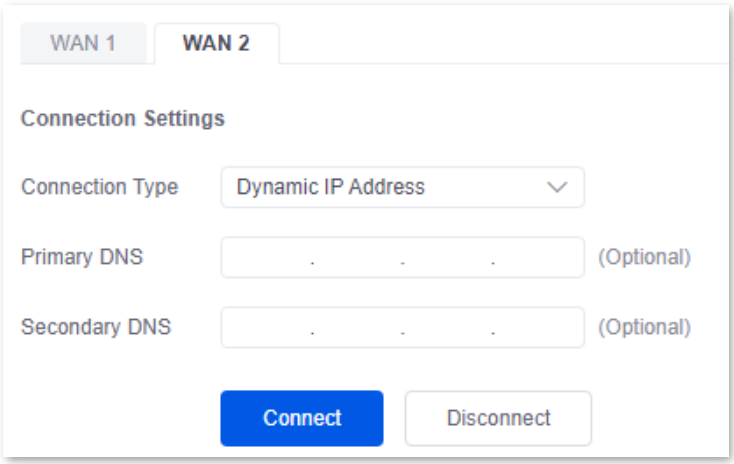


Configuration procedure

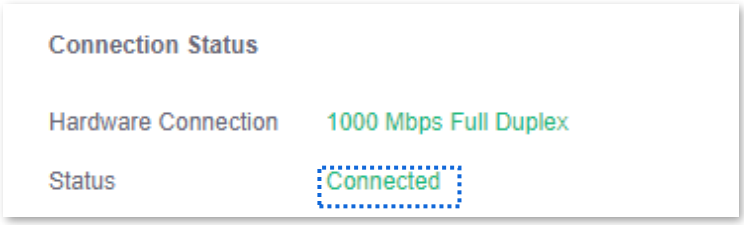
1. Log in to the Web UI of the router.
2. Configure the WAN2 port to access the internet.
   1) Navigate to **Network** > **Internet Settings**.
   2) Set **No. of WAN Ports** to **2**.



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



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

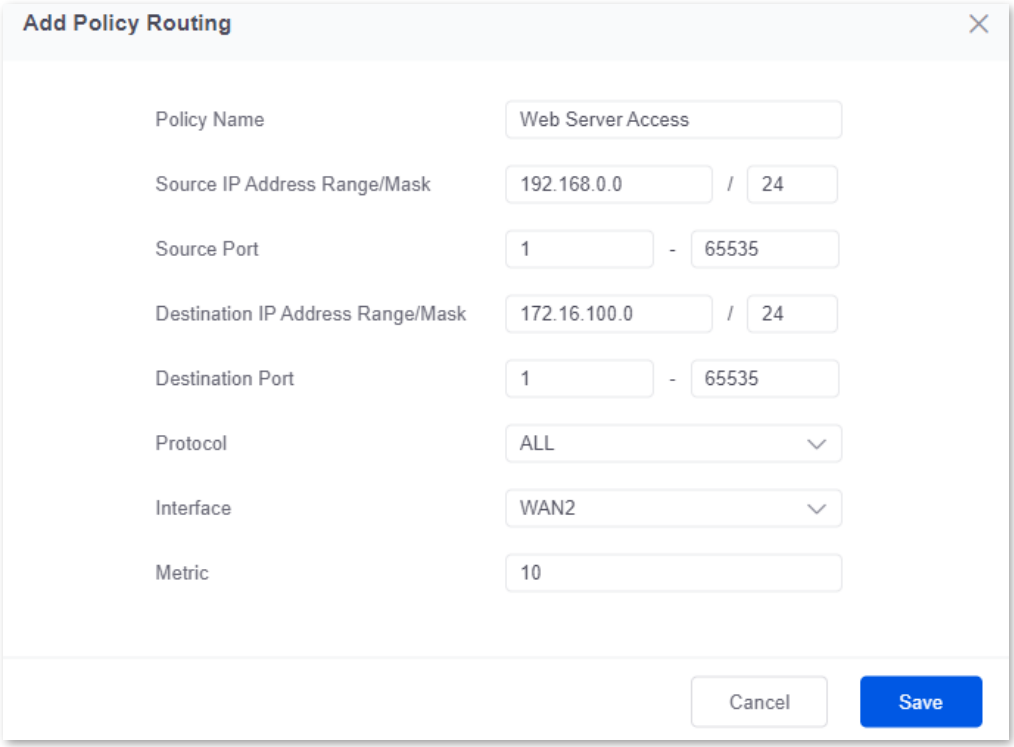


3. Configure the policy routing.

The following table provides the examples of policy routing parameters.

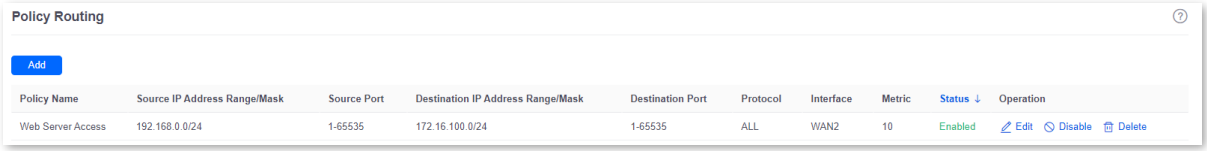
Policy Name	Source IP Address Range/Mask	Source Port	Destination IP Address Range/Mask	Destination Port	Protocol	Interface	Metric
Web Server Access	192.168.0.0/24	1–65535	172.16.100.0/24	1–65535	ALL	WAN2	10

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



----End

The policy routing is added successfully.



Verification

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

10.2 Virtual Service

10.2.1 DMZ

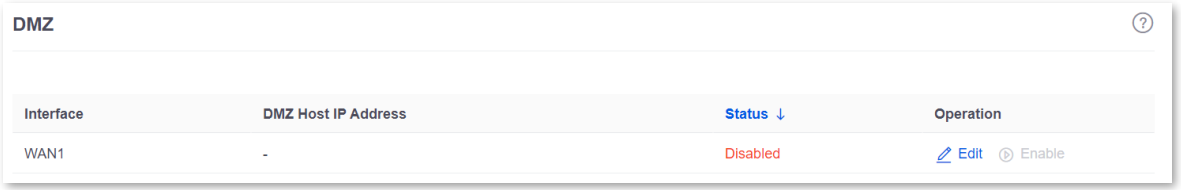
Overview

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

Note

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

Navigate to **More** > **Virtual Service** > **DMZ** to enter the page. On this page, you can modify the corresponding DMZ policy according to your needs. The DMZ function is disabled by default. You can click ⋮ to select parameters to be displayed.



Parameter description

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

Parameter	Description
Operation	Used to edit, enable or disable the DMZ policy. Edit : Used to modify the DMZ policy. Enable : Used to enable the DMZ policy. Disable : Used to disable the DMZ policy.

Example of configuring DMZ

Networking requirements

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

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

Solution

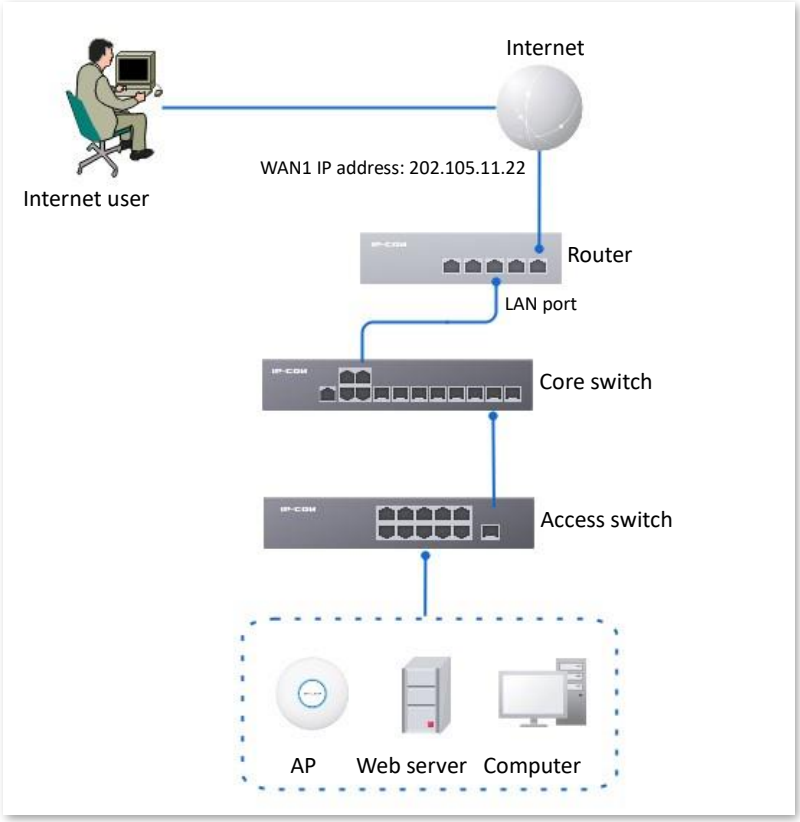
- You can use the DMZ function to enable internet users to access the intranet web server.
- You can use the DHCP Reservation function to avoid access failures caused by web server address change.

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

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

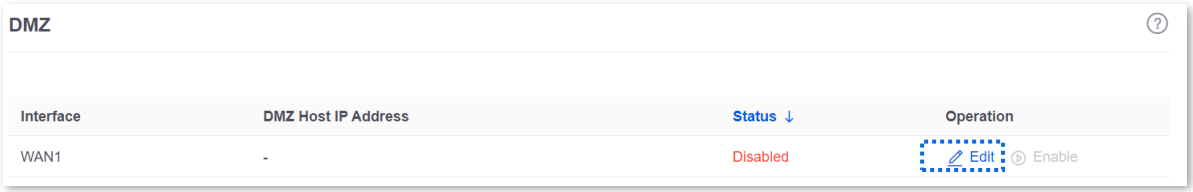
Tip

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

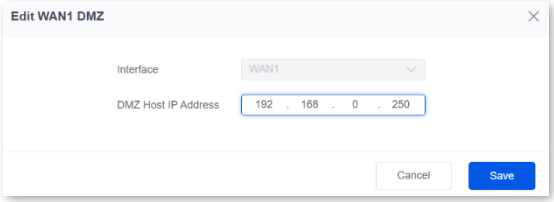


Configuration procedure

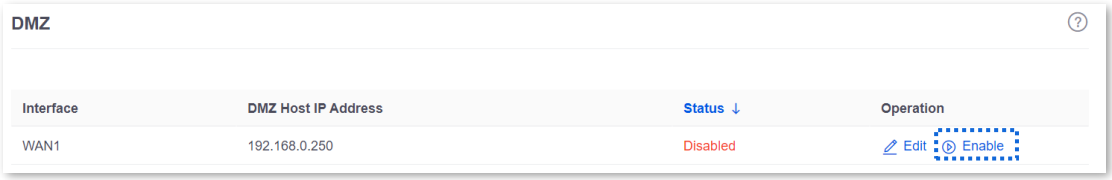
1. Log in to the Web UI of the router.
2. Set the DMZ host.
   1) Navigate to **More** > **Virtual Service** > **DMZ**.
   2) Locate the corresponding WAN port, and click **Edit.**



   3) Set **DMZ Host IP Address** (the IP address of the LAN device to be set as the DMZ host), which is **192.168.0.250** in this example.
   4) Click **Save**.

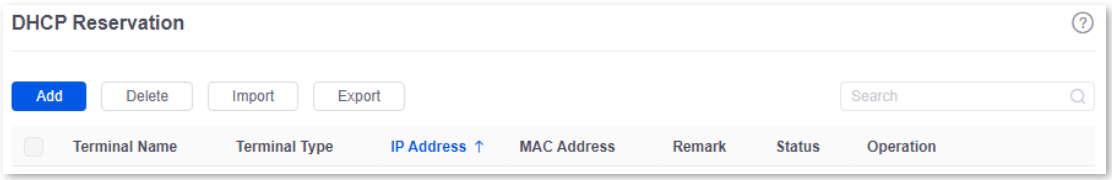


   5) Click **Enable**.



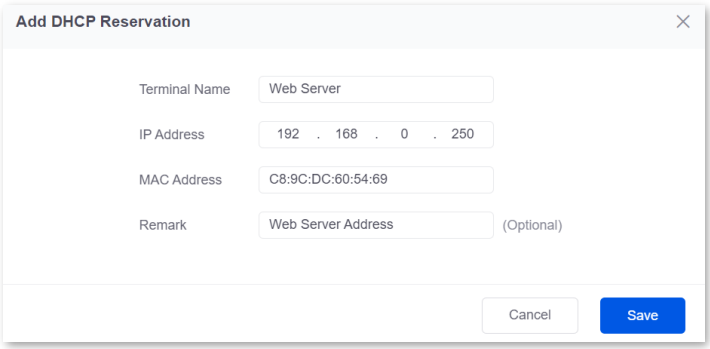
3. Reserve a fixed IP address for the DMZ host.

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



2) Set the following rules, and click **Save**.

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



----End

Verification

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

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

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

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

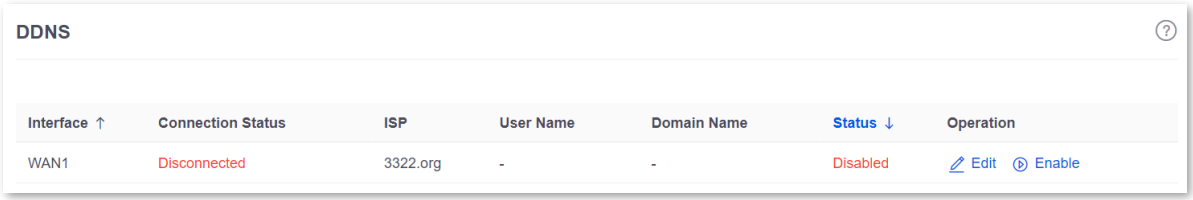
10.2.2 DDNS

Overview

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

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

Navigate to **More** > **Virtual Service** > **DDNS** to enter the page. The router has created a corresponding DMZ policy for each WAN port by default, and the status is **Disabled**. On this page, you can modify the DDNS policies according to your needs. The DDNS function is disabled by default. You can click ⋮ to select parameters to be displayed.



Parameter description

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

Parameter	Description
Status	Specifies the status of the DDNS service policy, including **Enabled**, **Disabled** and **Expired**.

Example of configuring DDNS

Networking requirements

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

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

Solution

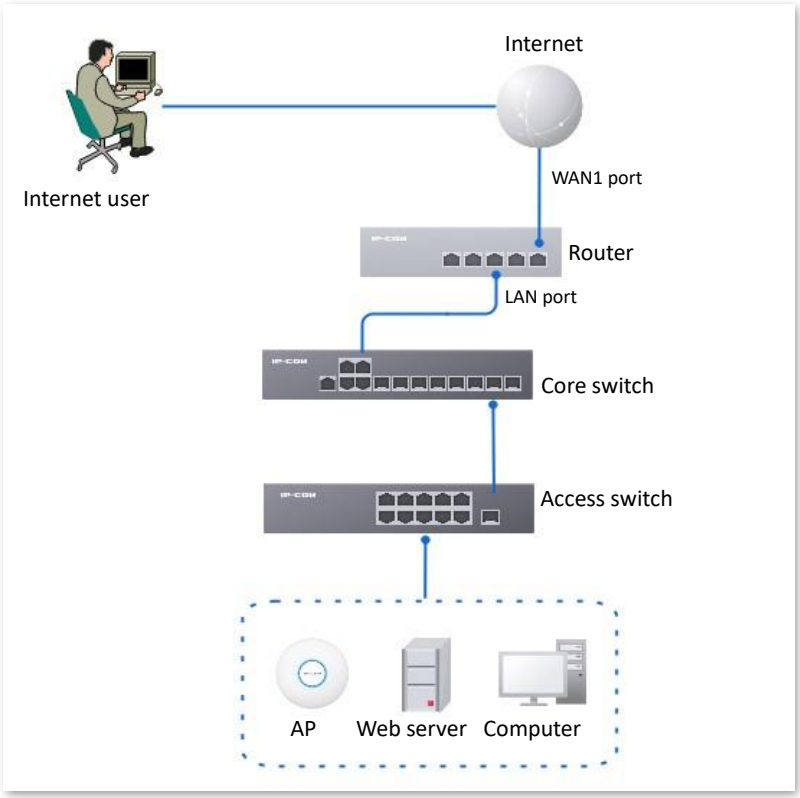
- You can use the Port Mapping function to enable internet users to access the intranet web server.
- You can use the DDNS function to enable internet users to access the intranet web server through a fixed domain name, avoiding access failures caused by WAN IP address change.
- You can use the DHCP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

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

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

Tip

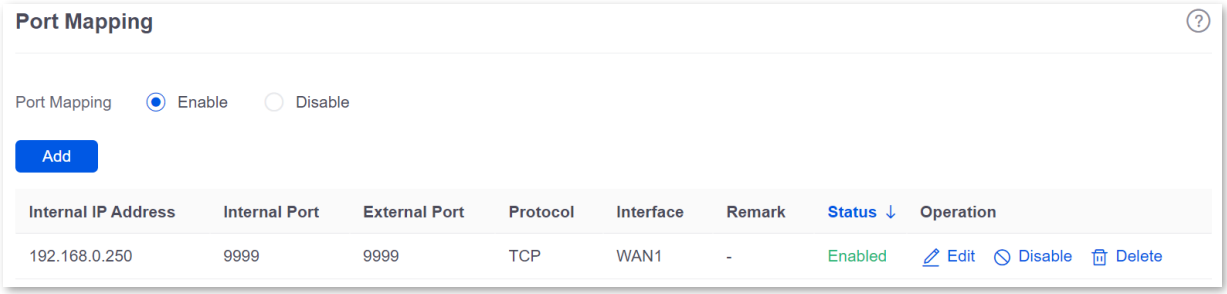
- Before the configuration, ensure that the WAN port of the router obtains a public IP address. If the WAN port obtains a private IP address or an intranet IP address assigned by the ISP, the DDNS function may not take effect. Common IPv4 addresses are classified into class A, class B and class C. Private IP addresses of class A range from 10.0.0.0 to 10.255.255.255. Private IP addresses of class B range from 172.16.0.0 to 172.31.255.255. Private IP addresses of class C range from 192.168.0.0 to 192.168.255.255.
- ISPs may not support unreported web service accessed using the default port number 80. Therefore, when setting port mapping, you are recommended to set the external port as a non-familiar port (1024 to 65535), such as 9999, to ensure normal access.
- Internal and external ports can be different.



Configuration procedure

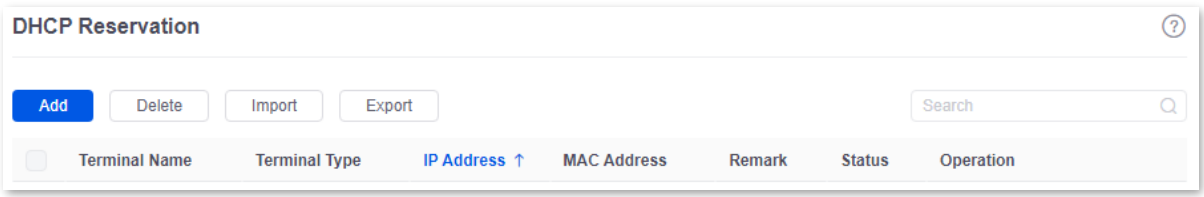
1. Log in to the Web UI of the router.
2. Set port mapping.

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



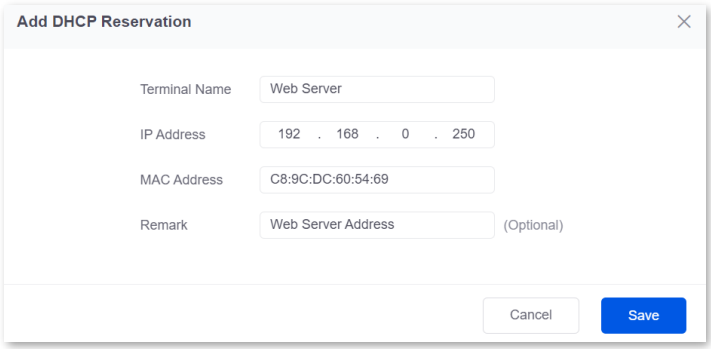
3. Reserve a fixed IP address for the DMZ host.

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

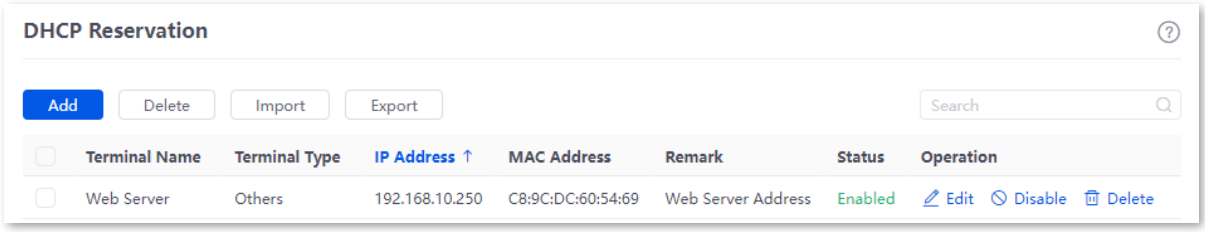


   2) Set the following rules, and click **Save**.

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



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

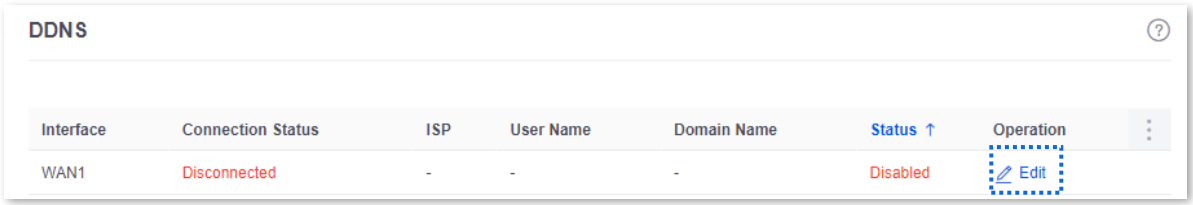


4. Register a domain name.

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

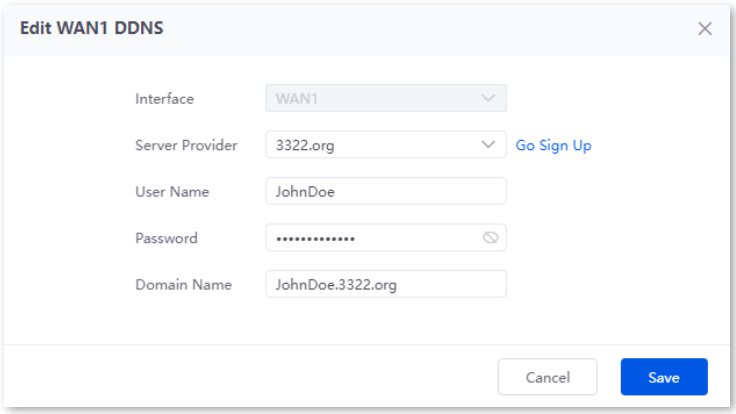
5. Set DDNS.

   1) Navigate to **More** > **Virtual Service** > **DDNS** to enter the configuration page. Click **Edit** after the corresponding WAN port rule, which is **WAN1** in this example.

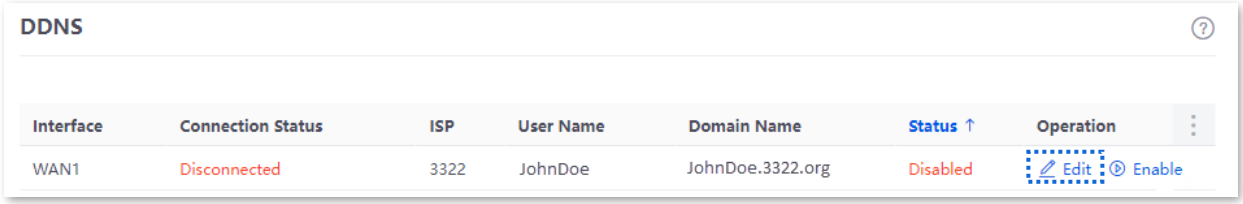


   2) Configure the following parameters in the pop-up **Edit WAN1 DDNS** window, and then click **Save**.
      - Set **Server Provider** (the DDNS provider where you applied the domain name), which is **3322.org** in this example.
      - Set **User Name** and **Password**, which are **JohnDoe** and **JohnDoe123456**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

- Set **Domain Name**, which is **JohnDoe.3322.org** in this example.

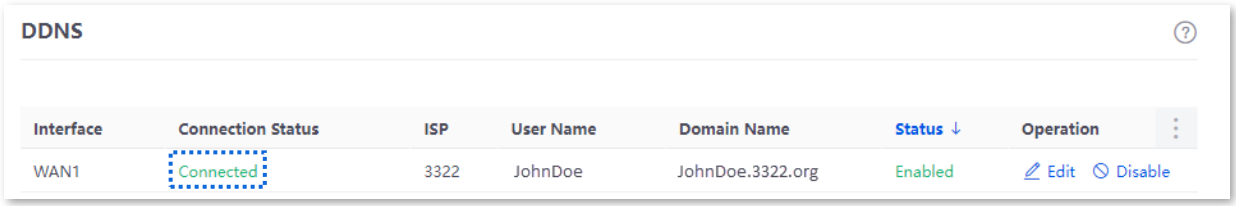


3) Click **Enable**.



----End

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



Verification

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

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

Tip

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

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

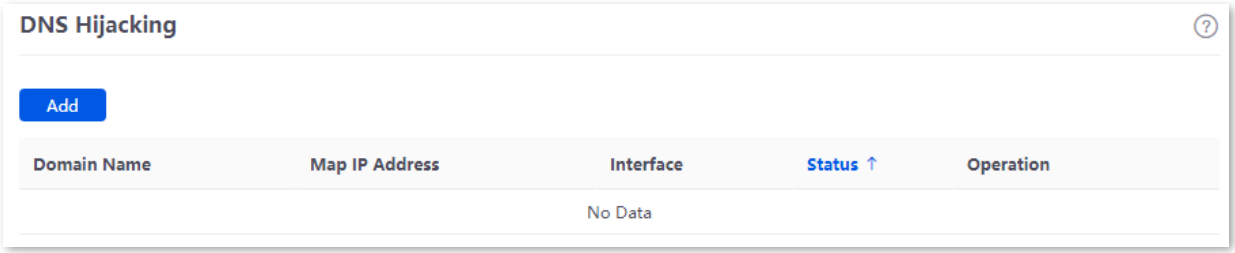
10.2.3 DNS hijacking

Overview

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

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

Navigate to **More** > **Virtual Service** > **DNS Hijacking** to enter the page. On this page, you can configure the DNS hijacking policy according to your needs.



Parameter description

Parameter	Description
Add	Used to add a new DNS hijacking policy.
Domain Name	Specifies the domain name to be hijacked.
Map IP Address	Specifies the IP address to be accessed after the hijacking.
Interface	Specifies the specified egress of the DNS hijacking policy.
Status	Specifies the current status of the DNS hijacking policy, including **Enabled** and **Disabled**.
Operation	Used to edit, enable, disable or delete the DNS hijacking policy. Edit: Used to modify the DNS hijacking policy. Enable: Used to enable the DNS hijacking policy. Disable: Used to disable the DNS hijacking policy. Delete: Used to delete the DNS hijacking policy.

Example of configuring DNS hijacking

Networking requirements

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

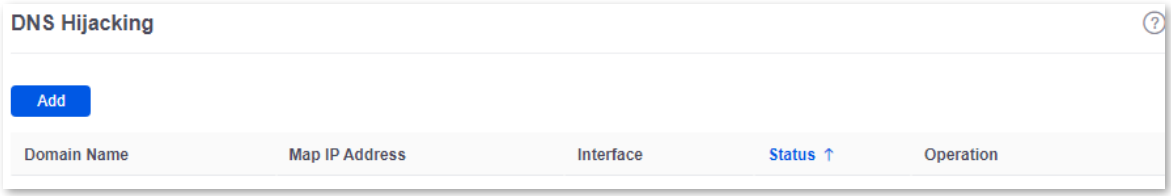
When LAN users visit Amazon (Amazon.com), eBay (eBay.com) and other websites, they can access the web UI of the router.

Solution

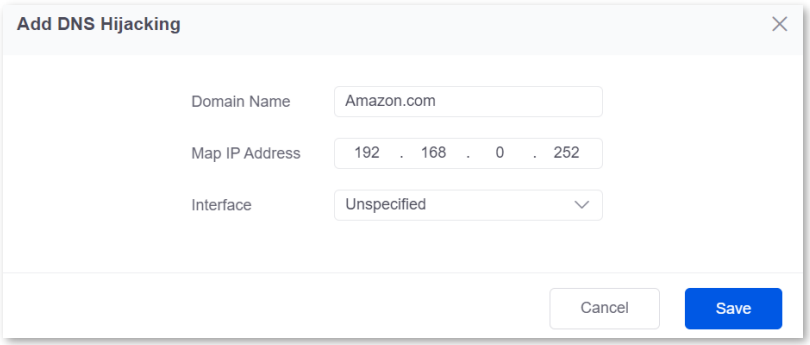
The above requirements can be achieved using the DNS hijacking function of the router. Assume that the IP address of the router is 192.168.0.252.

Configuration procedure

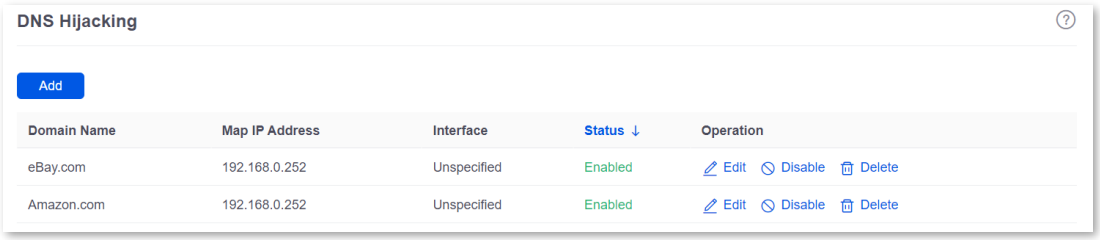
1. Log in to the web UI of the router.
2. Navigate to **More** > **Virtual Service** > **DNS Hijacking**, and click **Add**.



3. Set the following rules of the DNS hijacking policy, and click **Save**.
   - Set **Domain Name** of Amazon, which is **Amazon.com** in this example.
   - Set **Map IP Address** of the router, which is **192.168.0.252** in this example.



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



----End

Verification

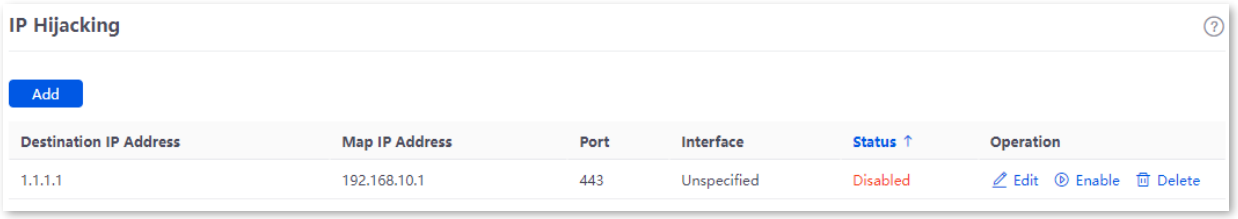
When LAN users visit Amazon (Amazon.com) and eBay (eBay.com) websites, they always visit the web UI of the router.

10.2.4 IP hijacking

Overview

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

Navigate to **More** > **Virtual Service** > **IP Hijacking** to enter the page. On this page, you can configure the IP hijacking policy according to your needs.



Parameter description

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

Parameter	Description
Operation	Used to edit, enable, disable or delete the IP hijacking policy. Edit: Used to modify the IP hijacking policy. Enable : Used to enable the IP hijacking policy. Disable : Used to disable the IP hijacking policy. Delete : Used to delete the IP hijacking policy.

Example of configuring IP hijacking

Networking requirements

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

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

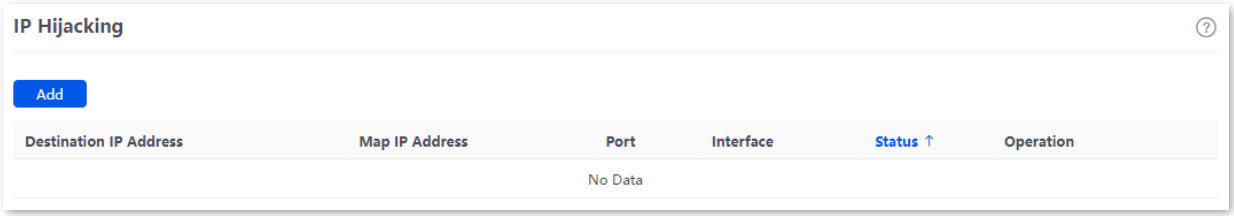
Solution

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

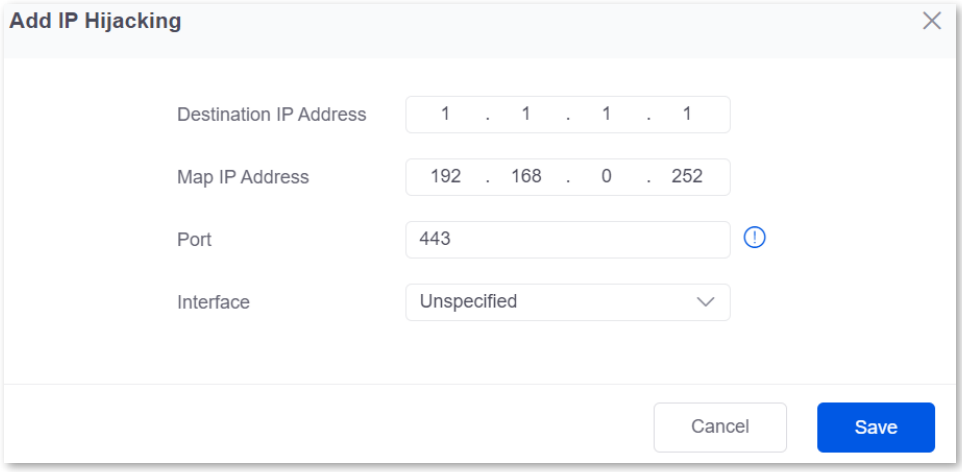
Assume that the management IP address of the router is 192.168.0.252 and the port to be accessed is 443.

Configuration procedure

1. Log in to the web UI of the router.
2. Navigate to **More** > **Virtual Service** > **IP Hijacking**, and click **Add**.



3. Configure parameters in the **Add IP Hijacking** window, and click **Save**.
   - Set **Destination IP Address**, which is **1.1.1.1** in this example.
   - Set **Map IP Address**, which is **192.168.0.252** in this example.
   - Set **Port**, which is **443** in this example.



----End

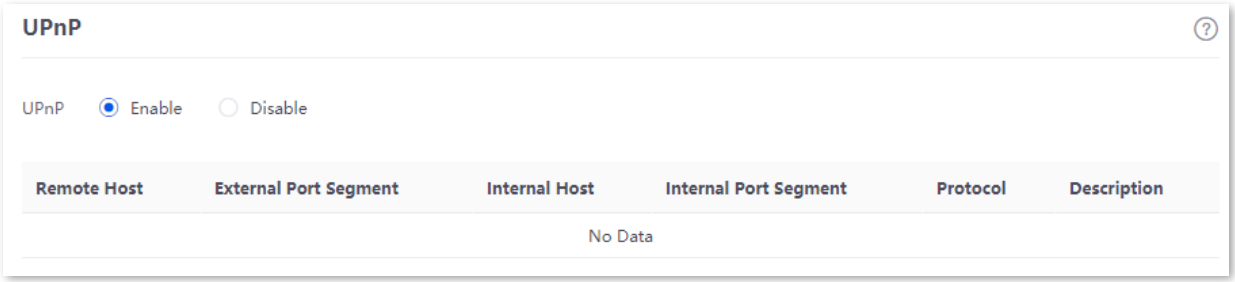
Verification

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

10.2.5 UPnP

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

Navigate to **More** > **Virtual Service** > **UPnP** to enter the page. The UPnP function is disabled by default. After this function is enabled, when UPnP-supporting programs (such as BitComet) are running in the LAN, you can check the port switching information generated when application programs send requests.



Parameter description

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

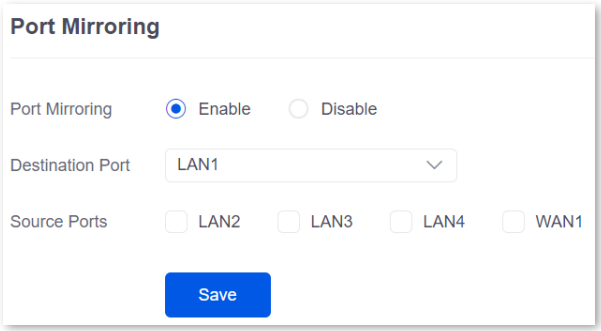
10.2.6 Port mirroring

Overview

On this page, you can copy the data from one or multiple ports (source ports) to a specified port (destination port) with the Port Mirroring function. Generally, the mirroring port is connected to a data monitoring device for the network administrator to perform real-time traffic monitoring, performance analysis and fault diagnosis.

Navigate to **More** > **Virtual Service** > **Port Mirroring** to enter the page. On this page, you can configure the port mirroring according to your needs.

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



Parameter description

Parameter	Description
Port Mirroring	Specifies whether to enable the Port Mirroring function.
Destination Port	Specifies the destination port, to which the data from the source ports is copied. Generally, the router connected to this port is installed with monitoring firmware. Note When the Port Mirroring function is enabled, **Destination Port** can be configured.
Source Ports	Specifies the source port, whose data is copied to the destination port. Note When the Port Mirroring function is enabled, **Source Ports** can be configured.

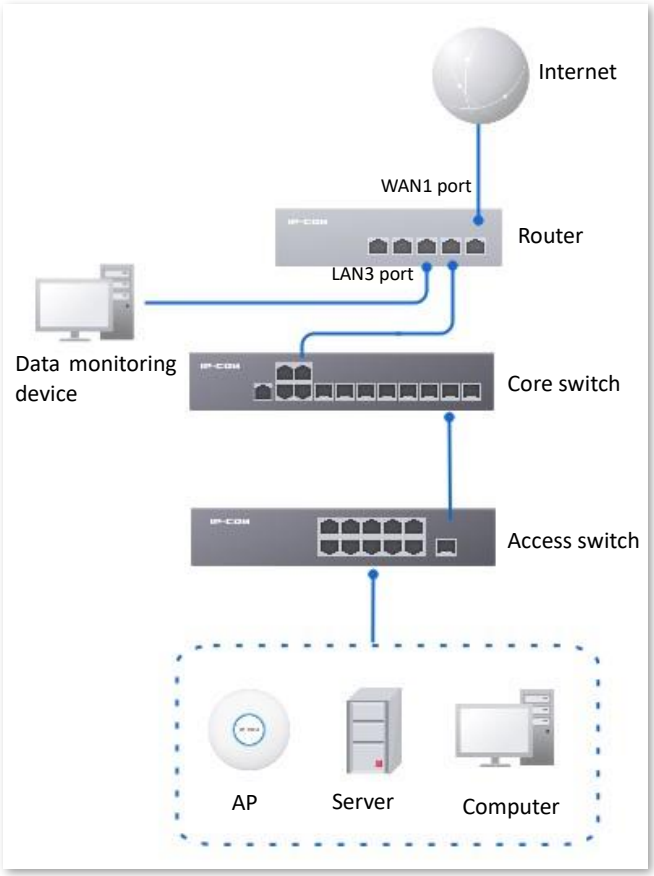
Example of configuring port mirroring

Networking requirements

An enterprise uses the enterprise router to set up a network. Recently, the enterprise's network is abnormal and often cannot access the internet. The network administrator needs to capture the data of the router's WAN port and LAN port for analysis.

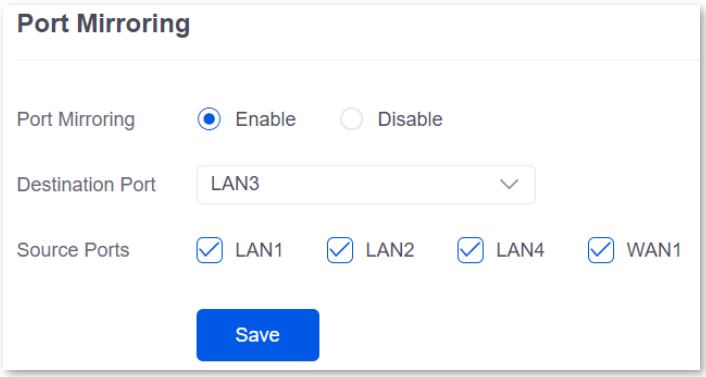
Solution

- The above requirements can be achieved using the Port Mirroring function of the router.
- Assume that the monitoring device is connected to the LAN3 port. The device needs to monitor the data of other ports.



Configuration procedure

1. Log in to the Web UI of the router.
2. Navigate to **More** > **Virtual Service** > **Port Mirroring**.
3. Select **Enable** for **Port Mirroring**.
4. Select **Destination Port**, which is **LAN3** in this example.
5. Select **Source Ports**, which is **WAN1**, **LAN2** and **LAN4** in this example.
6. Click **Save**.



----End

Verification

Running monitoring software on the monitoring computer, such as Wireshark, to capture the data packets of the source ports.

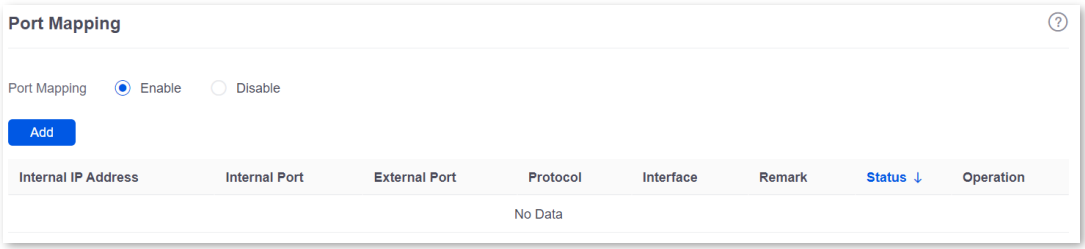
10.2.7 Port mapping

Overview

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

Navigate to **More** > **Virtual Service** > **Port Mapping** to enter the page. On this page, you can configure the port mapping policy according to your needs.

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



Parameter description

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

Example of configuring port mapping

Networking requirements

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

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

Solution

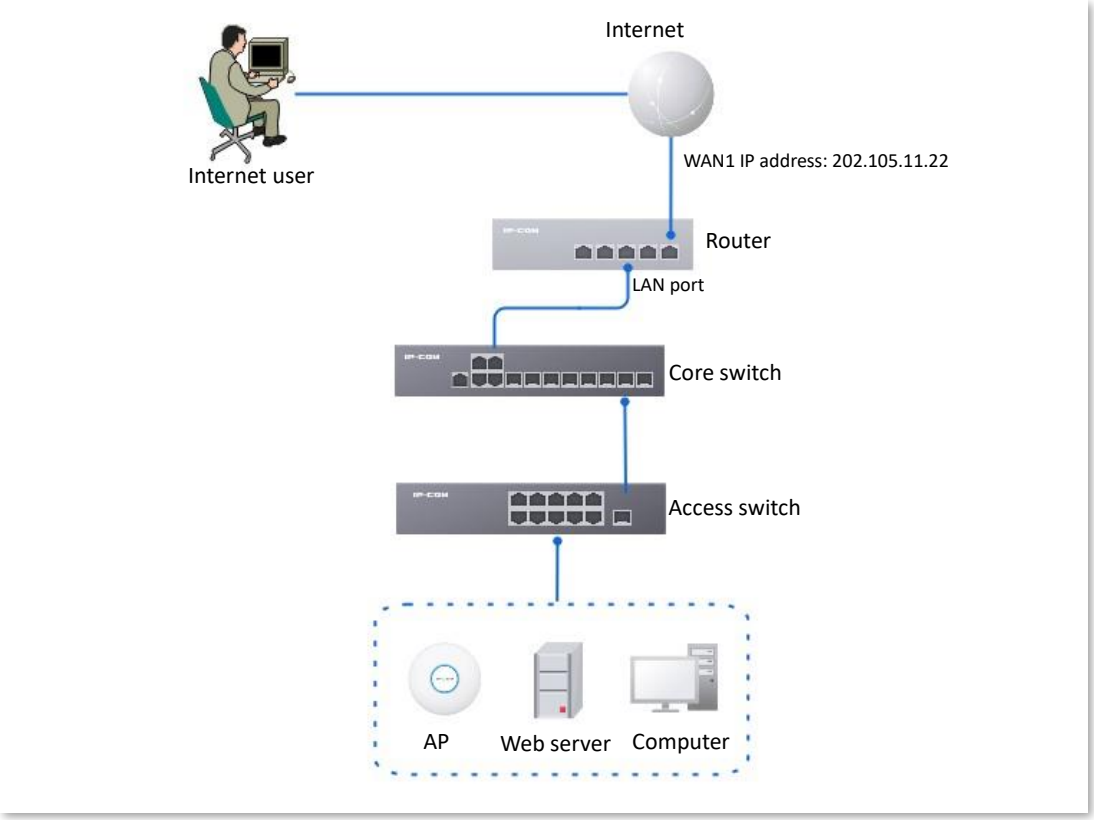
- You can use the Port Mapping function to enable internet users to access the intranet web server. Assume that the external network port opened by the router is 9999.
- You can use the DHCP Reservation function to avoid access failures caused by web server address change.

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

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

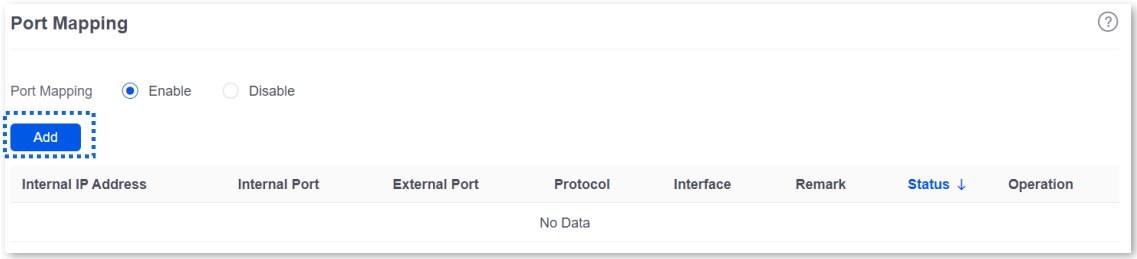
Tip

- Before the configuration, ensure that the WAN port of the router obtains a public IP address. If the WAN port obtains a private IP address or an intranet IP address assigned by the ISP, the Port Mapping function may not take effect. Common IPv4 addresses are classified into class A, class B and class C. Private IP addresses of class A range from 10.0.0.0 to 10.255.255.255. Private IP addresses of class B range from 172.16.0.0 to 172.31.255.255. Private IP addresses of class C range from 192.168.0.0 to 192.168.255.255.
- ISPs may not support unreported web service accessed using the default port number 80. Therefore, when setting port mapping, you are recommended to set the external port as a non-familiar port (1024 to 65535), such as 9999, to ensure normal access.
- Internal and external ports can be different.



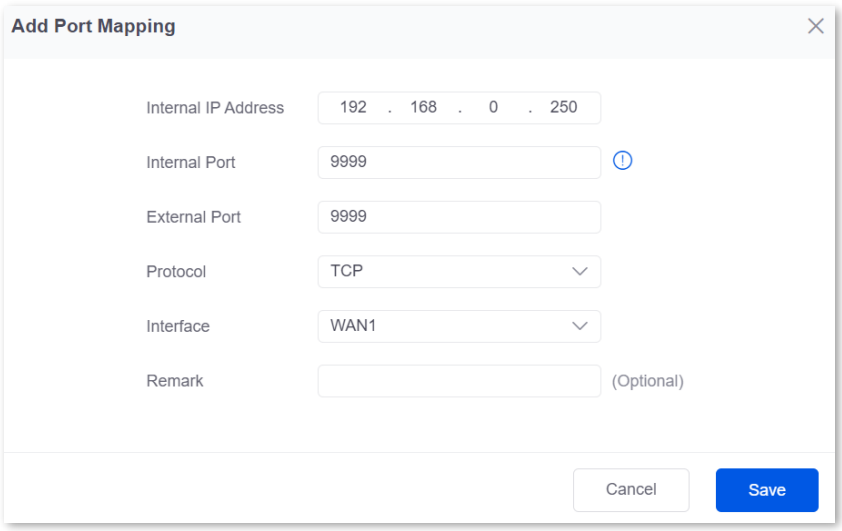
Configuration procedure

1. Log in to the Web UI of the router.
2. Set port mapping.
   1) Navigate to **More** > **Virtual Service** > **Port Mapping**.
   2) Select **Enable** for **Port Mapping**, and click **Add**.

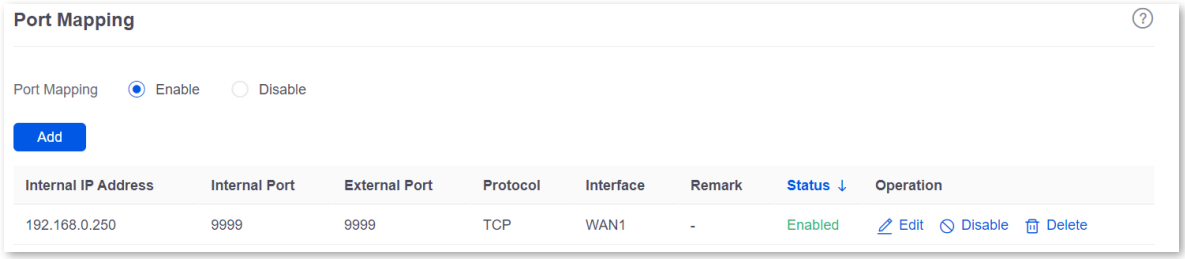


   3) Configure parameters in the **Add** window, and click **Save**.
      - Set **Internal IP Address** (the IP address of the web server), which is **192.168.0.250** in this example.
      - Set **Intranet Port** (the port used by the web server), which is **9999** in this example.
      - Set **External Port** (the port that the router opens to WAN users), which is **9999** in this example.
      - Set **Protocol**, which is **TCP** in this example. If you are not sure about the protocol type of the service, **TCP&UDP** is recommended.

- Set **Interface** (the WAN port used by Internet users to access the LAN server), which is **WAN1** in this example.

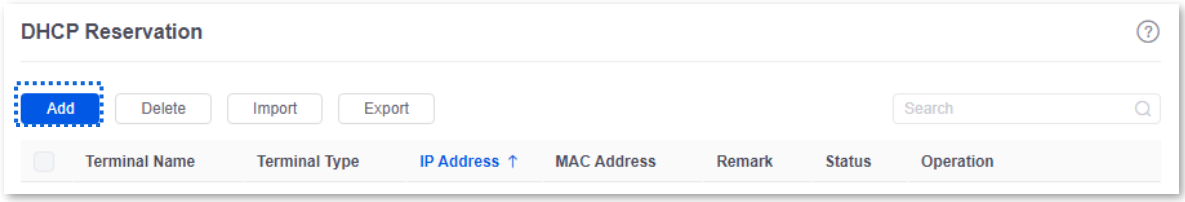


The port mapping policy is added successfully. See the following figure.



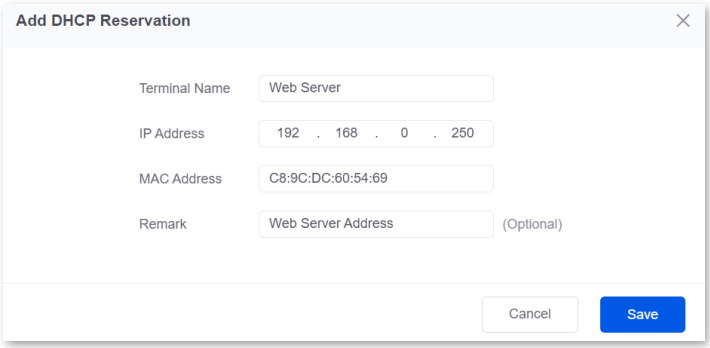
3. Set the fixed IP address assigned to the server host.

1) Navigate to **Network** > **DHCP Settings** > **DHCP Reservation**, and Click **Add**.



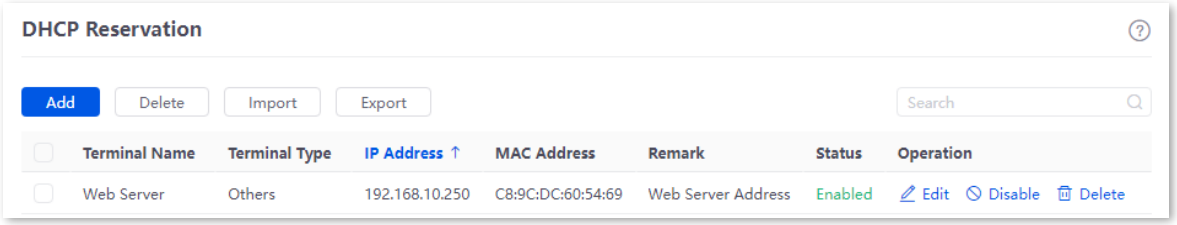
2) Set the following rules, and click **Save**.

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



----End

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



Verification

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

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

You can find the router's current WAN port IP address on the **Internet Settings** page.

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

Tip

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

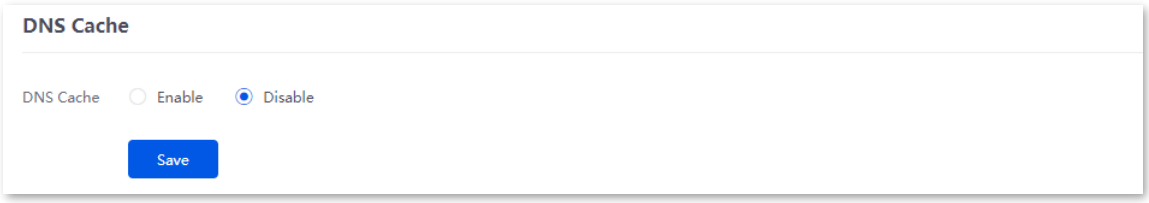
- Make sure that the internal port you entered is correct.
- Maybe the system firewall, anti-virus software and security guard on the LAN server blocked internet user access. Disable these programs and try again.

10.2.8 DNS cache

The Domain Name Server (DNS) is used to manage the relationships between domain names and IP addresses so that domain names can be mapped with corresponding IP addresses. Users accessing domain names are actually accessing the mapped IP addresses through DNS domain name parsing.

The DNS cache function enables the router to cache DNS-resolved information about websites visited by users. When other users access the websites, the router directly uses the information in the cache to direct users to the websites without accessing the DNS server. This improves the website accessing speed.

To access the page, navigate to **More** > **Virtual Service** > **DNS Cache**. The DNS cache function is enabled by default.



10.3 Maintenance service

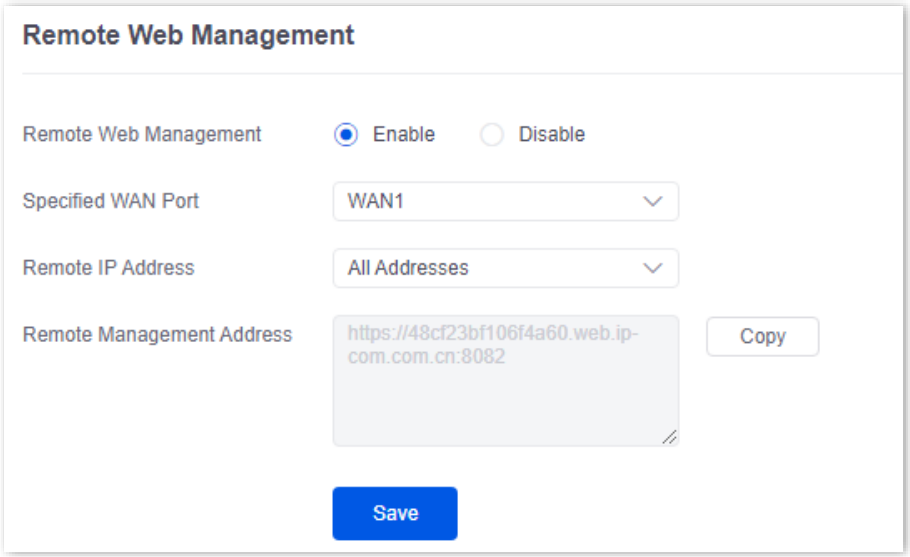
10.3.1 Remote web management

Overview

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

Navigate to **More** > **Maintenance Service** > **Remote Web Management** to enter the page. On this page, you can enable or disable the remote web management and restrict the hosts that can remotely log in to the local router.

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



Parameter description

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

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

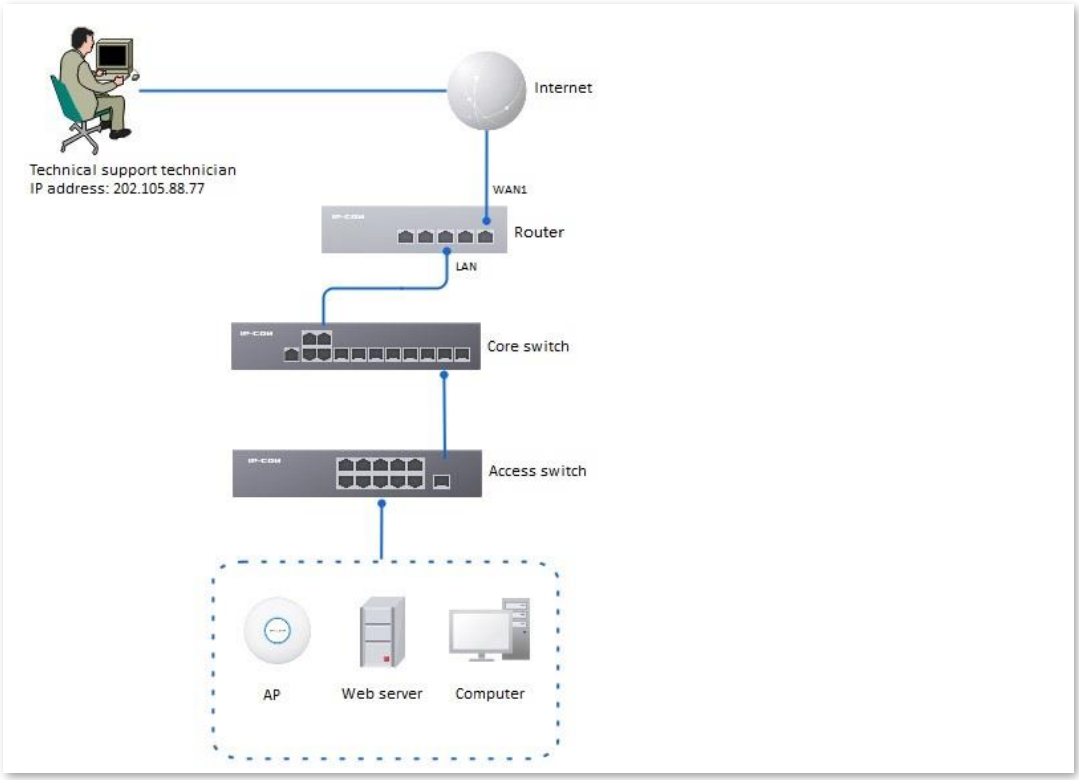
Example of configuring remote web management

Networking requirements

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

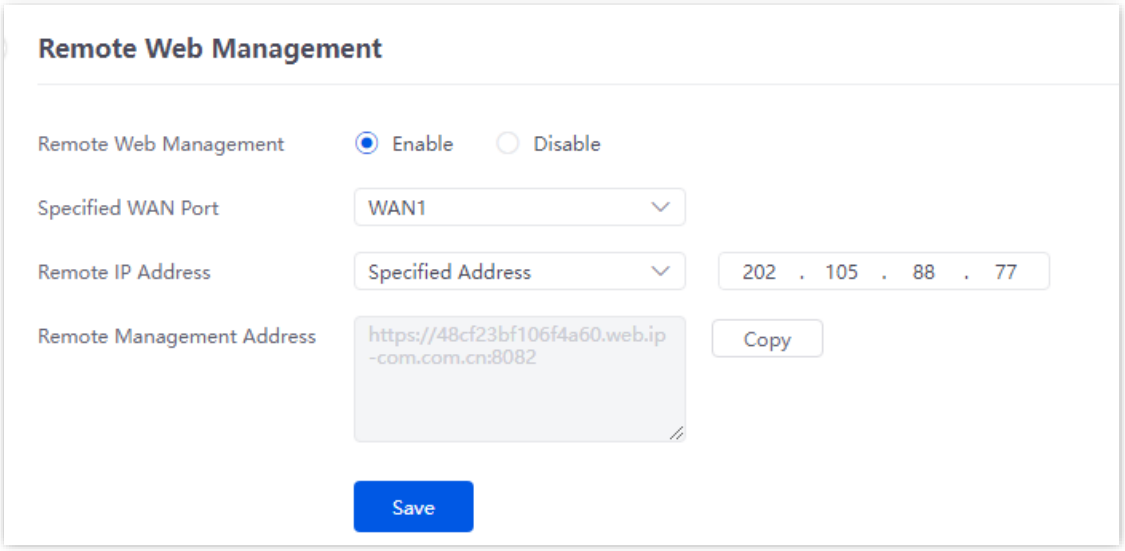
Solution

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



Configuration procedure

1. Log in to the Web UI of the router, and navigate to **More** > **Maintenance Service** > **Remote Web Management**.
2. Select **Enable** for **Remote Web Management**.
3. Set **Specified WAN Port**, which is **WAN1** in this example.
4. Set **Remote IP Address** as **Specified Address.** And enter the IP address of the computer supported by IP-COM technology, which is **202.105.88.77** in this example**.**
5. Click **Save**.



----End

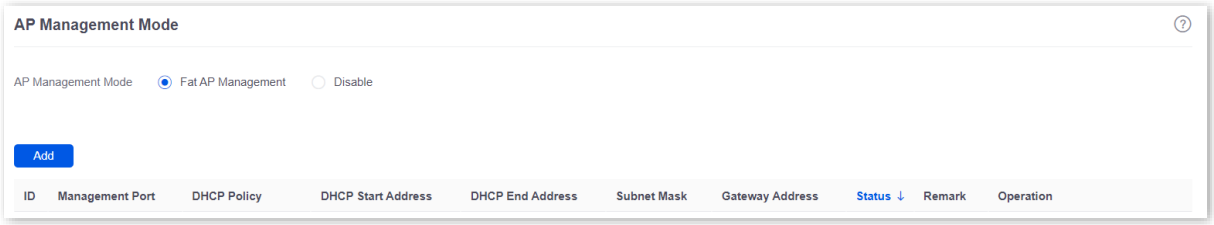
Verification

The IP-COM technical support technician can log in to the web UI of the router by visiting https://48cf23bf106f4a60.web.ip-com.com.cn:8082 on the computer (the IP address of the computer is 202.105.88.77).

10.3.2 AP management mode

Navigate to **More** > **Maintenance Service** > **AP Management Mode** to enter the page. On this page, you can set the AP management mode and add AP DHCP policy for the VLAN. The router only supports IP-COM fat APs.

The AP management mode function is disabled by default. You can click **Add** to add AP DHCP policy for the VLAN interface and assign IP address to the AP.

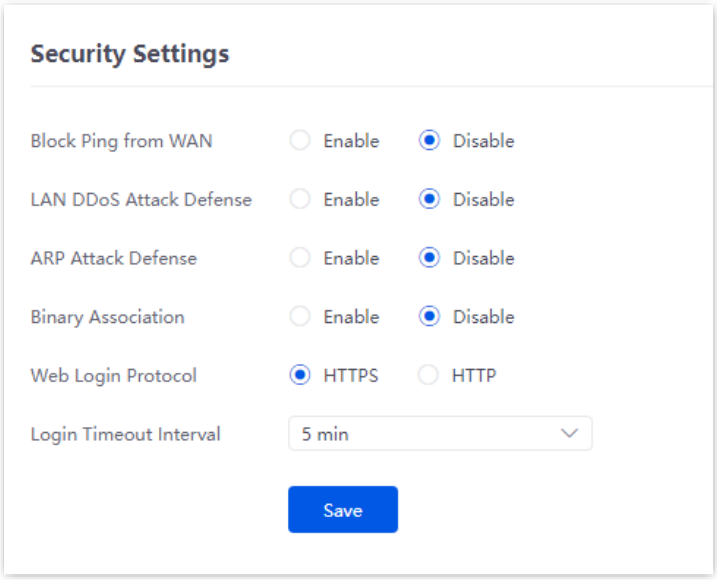


Parameter description

Parameter	Description
AP Management Mode	Used to set the AP management mode. – **Fat AP Management**: In this mode, you can manage fat APs. – **Disable**: Specifies that the AP cannot be managed.
ID	Specifies the number of the policy.
Management Port	Specifies the VLAN. Only APs connected to the management port can be managed.
DHCP Policy	Specifies the DHCP policy delivered to the managed AP. Tip If it is a new VLAN, you need to add an AP DHCP policy in **Network** > **DHCP Settings** > DHCP Server.
DHCP Start Address	Specifies the start address of the DHCP address pool delivered to the AP.
DHCP End Address	Specifies the end address of the DHCP address pool delivered to the AP.
Subnet Mask	Specifies the subnet mask of the DHCP.
Gateway Address	Specifies the gateway address of the DHCP.
Status	Specifies the current AP DHCP policy status, including **Enabled**, **Disabled** and **Expired**.
Remark	Specifies the introduction to the AP DHCP policy. The remark is optional.

10.3.3 Security settings

Navigate to **More** > **Maintenance Service** > **Security Settings** to enter the page. On this page, you can enable corresponding attack defense functions according to the actual network conditions.



Parameter description

Parameter	Description
Block Ping from WAN	Used to enable or disable the Block Ping from WAN function. With this function enabled, when a WAN host pings the IP address of the WAN port on the router, the router automatically ignores the Ping request to prevent itself from being exposed and defend against external Ping attacks.
LAN DDoS Attack Defense	Used to enable or disable the LAN DDoS Attack Defense function. DDoS attack indicates the distributed denial of service attack. The attack allows an attacker to exhaust the resources of a system, making the system unable to properly provide services. With this function enabled, the router can defend common DDoS attacks from the internal network.
ARP Attack Defense	Used to enable or disable the ARP Attack Defense function. With this function enabled, the router can identify ARP spoofing in the LAN and record the MAC address of the attacker.
Binary Association	Used to enable or disable the Binary Association function. With this function enabled, only devices whose IP addresses are bound with MAC addresses in the list to access the internet.

Parameter	Description
Web Login Protocol	Specifies the mode to log in to the web UI of the router, including **HTTPS** and **HTTP**. The default mode is **HTTPS**. – **HTTPS**: Hyper Text Transfer Protocol Secure (HTTPS) uses SSL/TLS to encrypt data packets based on HTTP and establishes a secure channel, thus ensuring the security of the data transmission process. It ensures the security of data transmission and the authenticity of the website via HTTPS Access. – **HTTP**: Hyper Text Transfer Protocol (HTTP) is a specification for communication between browsers and servers.
Login Timeout Interval	Used to set the login timeout interval. After logging in to the web UI of the router, you will be automatically logged out when no operation is performed within the defined time period.

10.3.4 Cloud maintenance

Overview

Tip

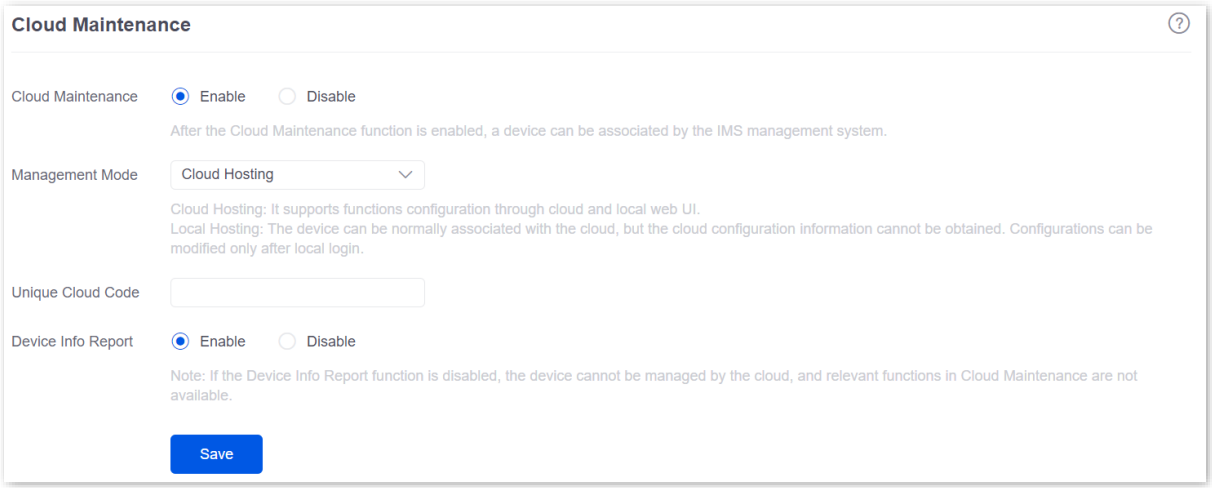
The cloud maintenance function may be unavailable for some versions. Please refer the actual product.

The ProFi cloud platform is a cloud platform established by IP-COM, providing central management for IP-COM devices that support cloud management.

With this router managed by the ProFi cloud platform, you can configure and check the parameters of the router on the ProFi cloud platform. You can also configure and check these parameters on the web UI of the router.

Navigate to **More** > **Maintenance Service** > **Cloud Maintenance** to enter the page. On this page, you can configure the Cloud Maintenance function of the router.

The Cloud Maintenance function is disabled by default. The following figure is for reference only.



Parameter description

Parameter	Description
Cloud Maintenance	Used to enable or disable the Cloud Maintenance function.
Management Mode	Specifies the management mode of cloud maintenance. – **Cloud Hosting**: It is applicable to unified managed projects that are maintained on the IP-COM ProFi cloud platform (ProFi Cloud web UI or ProFi App). The router can be managed by the IP-COM ProFi cloud platform and the configuration information of relevant functions is delivered by the ProFi cloud platform. When logging in to the web UI of the router locally, you can also configure the functions. – **Local Hosting**: It is applicable for scenarios where the project is centrally managed and viewed. The router can be managed on the IP-COM ProFi cloud platform, but all function configurations need to be set on the web UI of the router.
Unique Cloud Code	Specifies the ProFi cloud platform account associated with the device. You can obtain it as follows. – On the IP-COM ProFi Cloud web UI, you can click the account in the upper right corner to obtain the unique cloud code in the drop-down menu. – In the IP-COM ProFi App, you can obtain the unique cloud code in the personal center.
Device Info Report	Used to enable or disable the Device Info Report function. If the Device Info Report function is enabled, the router can be managed by the ProFi cloud platform. The configuration information of the router will be reported to the cloud platform.

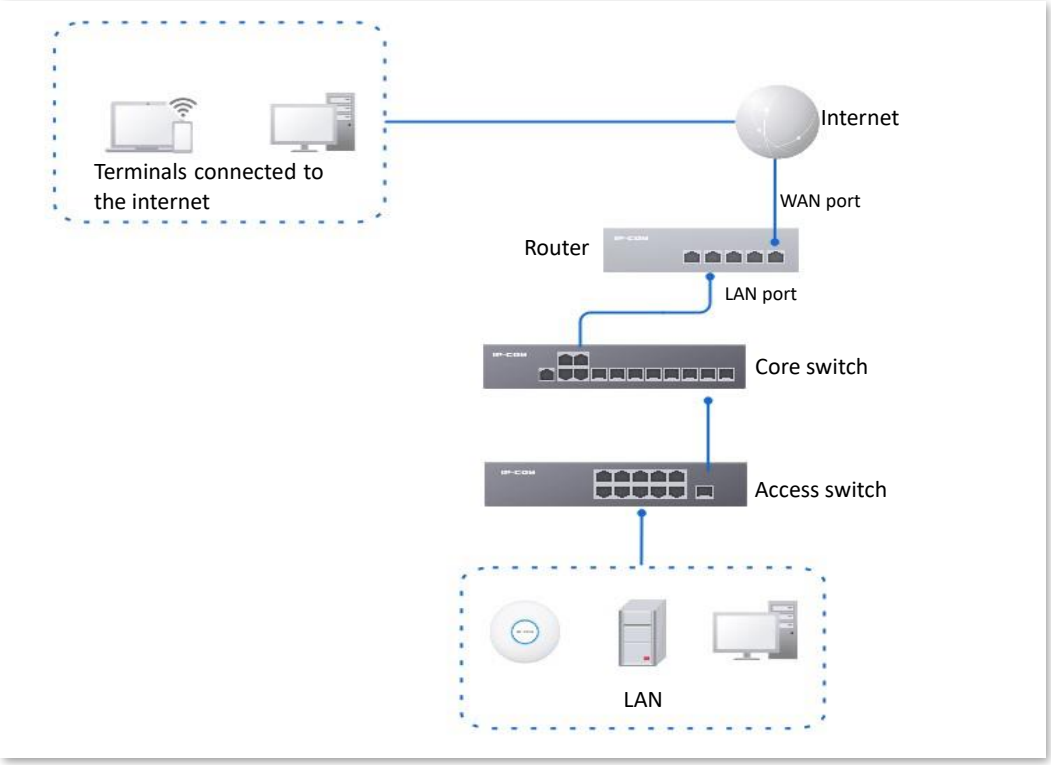
Example of configuring cloud maintenance on ProFi Cloud platform

Networking requirements

An enterprise uses the enterprise router to set up a network and has successfully connected to the Internet. The requirements are managing the router remotely and delivering related configurations.

Solution

You can use the Cloud Management function of the router and ProFi Cloud platform to meet the requirements.



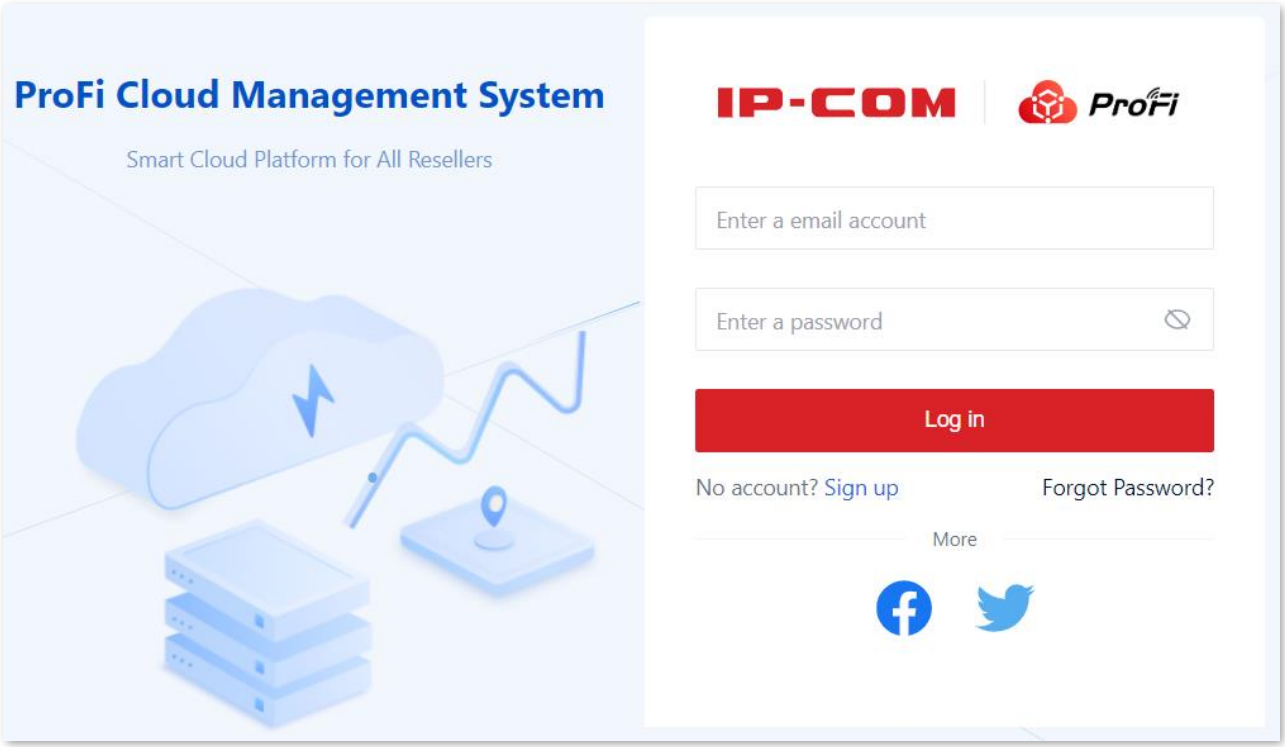
Configuration procedure

Tip

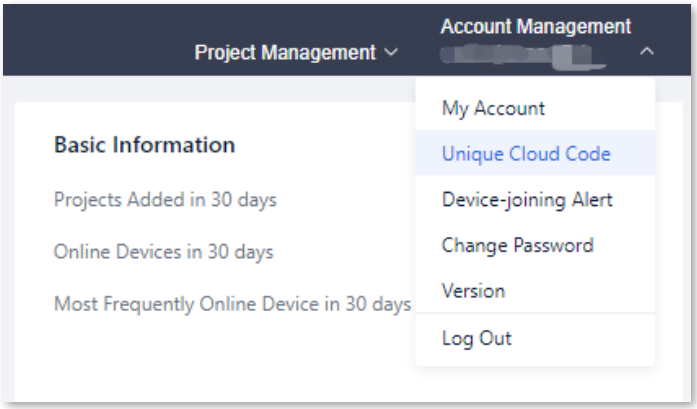
Before configuring the cloud maintenance function of the router, make sure that the router is successfully connected to the Internet.

1. Log in to IP-COM ProFi Cloud platform and obtain unique cloud code.

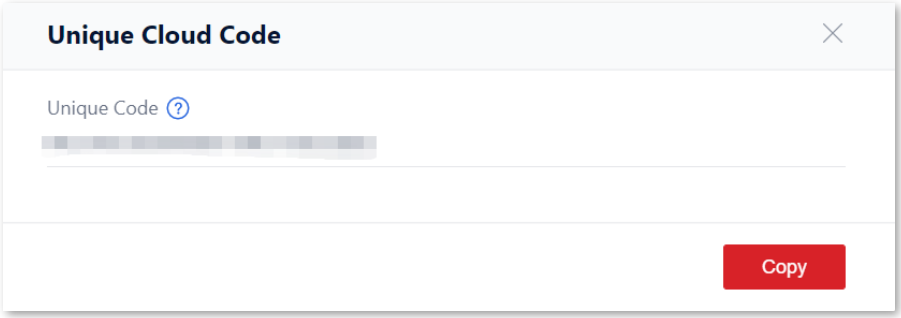
   1) On a computer that has connected to the Internet, start a web browser, visit https://imsen.ip-com.com.cn, and log in to IP-COM ProFi cloud platform.



2) Click the personal avatar at the upper right corner and select **Unique Cloud Code**.



3) Click **Copy** to copy the **Unique Cloud Code**.

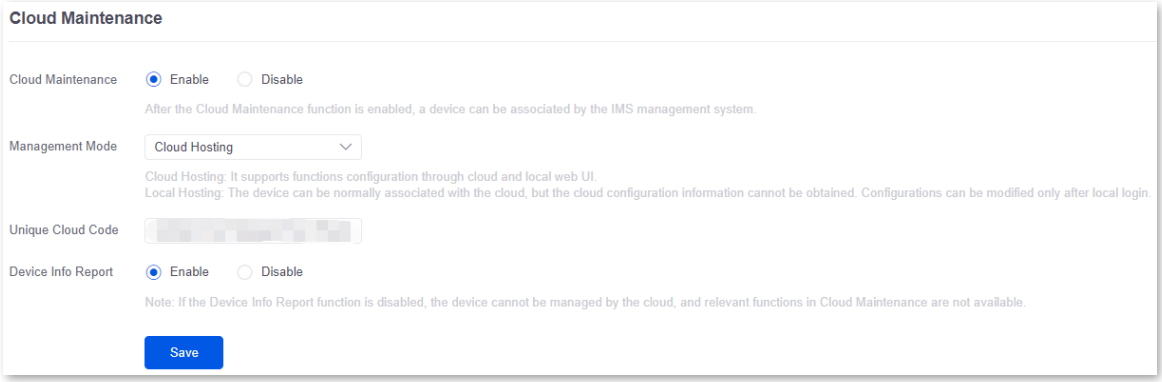


2. Enable the cloud maintenance function for the router.

1) Log in to the web UI of the router, and navigate to **More** > **Maintenance Service** > **Cloud Maintenance**.

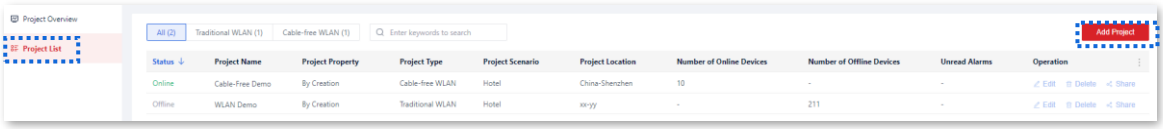
2) Set **Cloud Maintenance** to **Enable**, and set **Management Mode** as required (**Cloud Hosting** for example here).

3) Enter the **Unique Cloud Code** and set **Device Info Report** to **Enable**. Confirm the prompt information (if it pops up) and click **OK**. Then click **Save**.

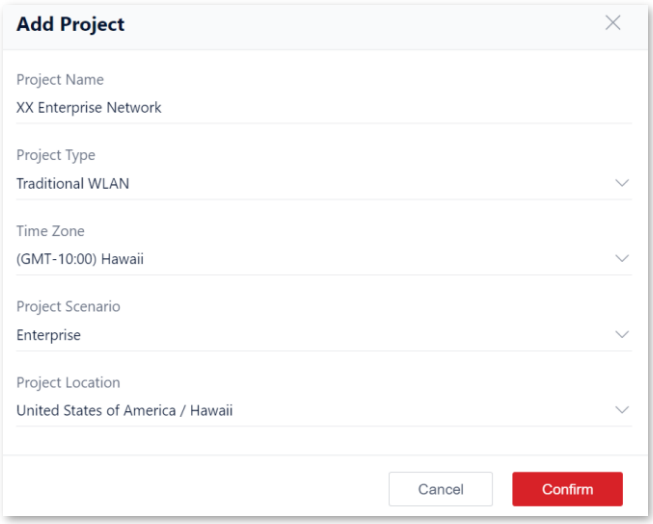


3. Add a project on the ProFi Cloud platform and add the router to the project.

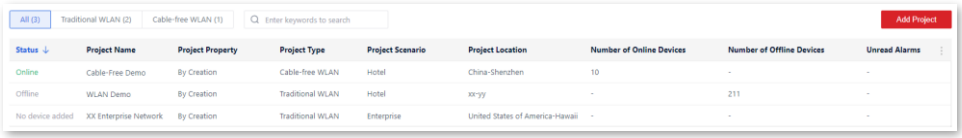
1) Log in to ProFi cloud platform. Click **Project List** and click **Add Project**.



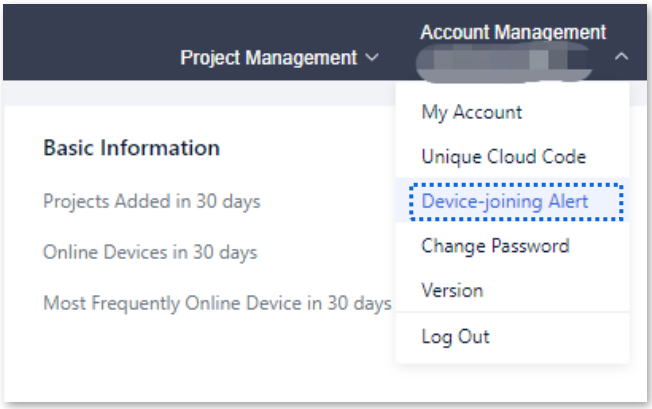
2) Configure project parameters and click **Confirm**. The following figure is for reference only.



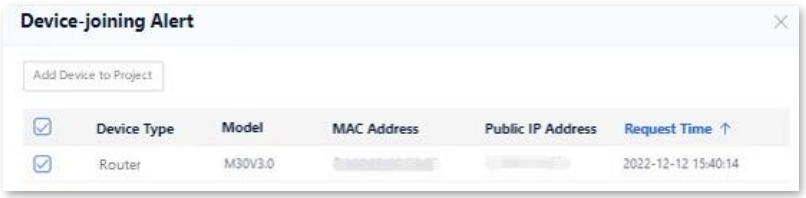
Added successfully.



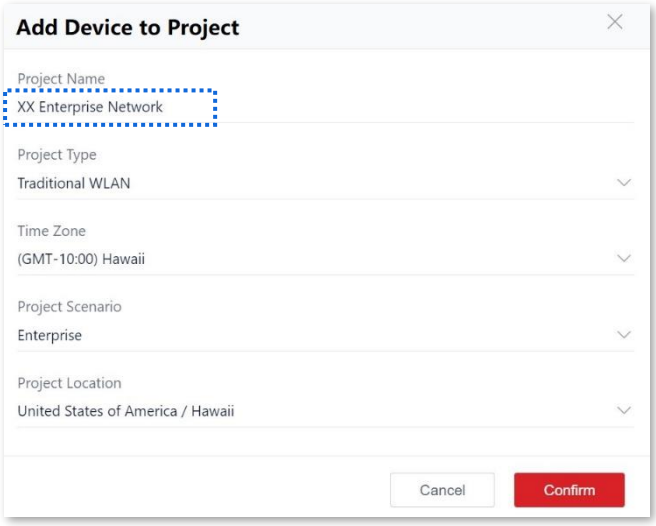
3) Click the personal avatar at the upper right corner and select **Device-joining Alert**.



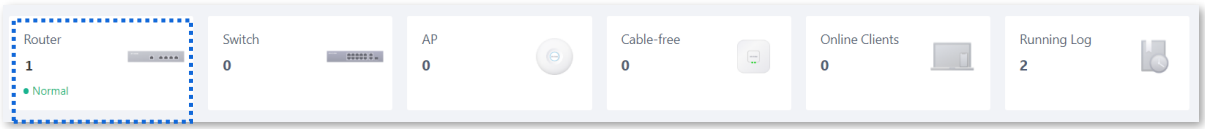
4) Select the router to be added to the project and click **Add Device to Project**.



5) Select the project to which you want to add the router and click **Confirm**. The following figure is for reference only.



Added successfully. You can enter the management page of the project to view details.



---End

Verification

After the configuration, the router can be managed through the ProFi Cloud platform, and all its configuration information is delivered by the ProFi Cloud platform.

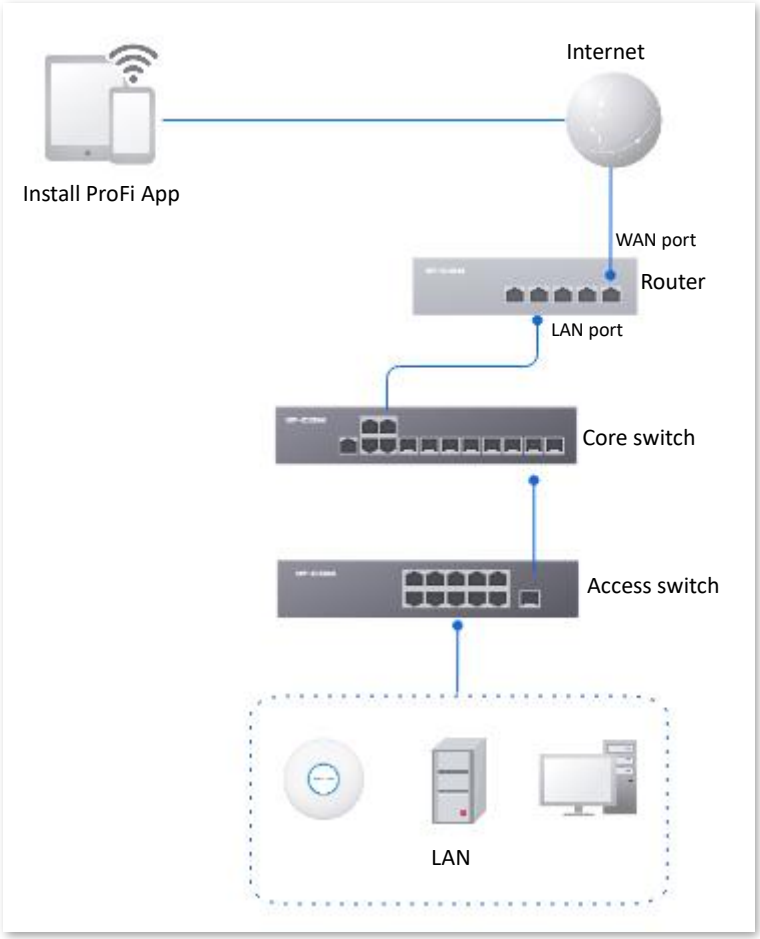
Example of configuring cloud maintenance on ProFi App

Networking requirements

An enterprise uses the enterprise router to set up a network and has successfully connected to the Internet. The requirements are managing the router remotely and delivering related configurations.

Solution

You can use the Cloud Management function of the router and ProFi App to meet the requirements.



Configuration procedure (method 1)

Tip

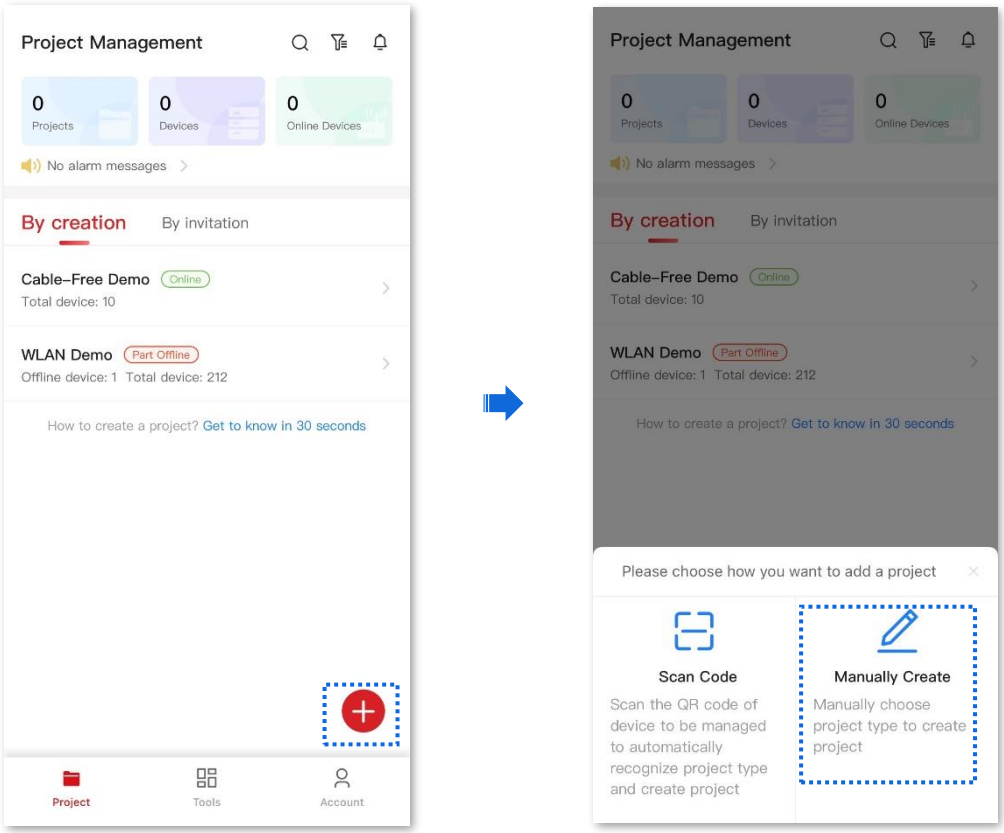
- Before configuring the cloud maintenance function of the router, make sure that the router is successfully connected to the Internet.
- V1.4.3 App version is taken as an example here. The actual operation and interface display of the corresponding App version shall prevail.

1. Scan the following QR code or search for the **ProFi** App in **App Store** or **Google Play** to download and install the **ProFi** App on your mobile phone.

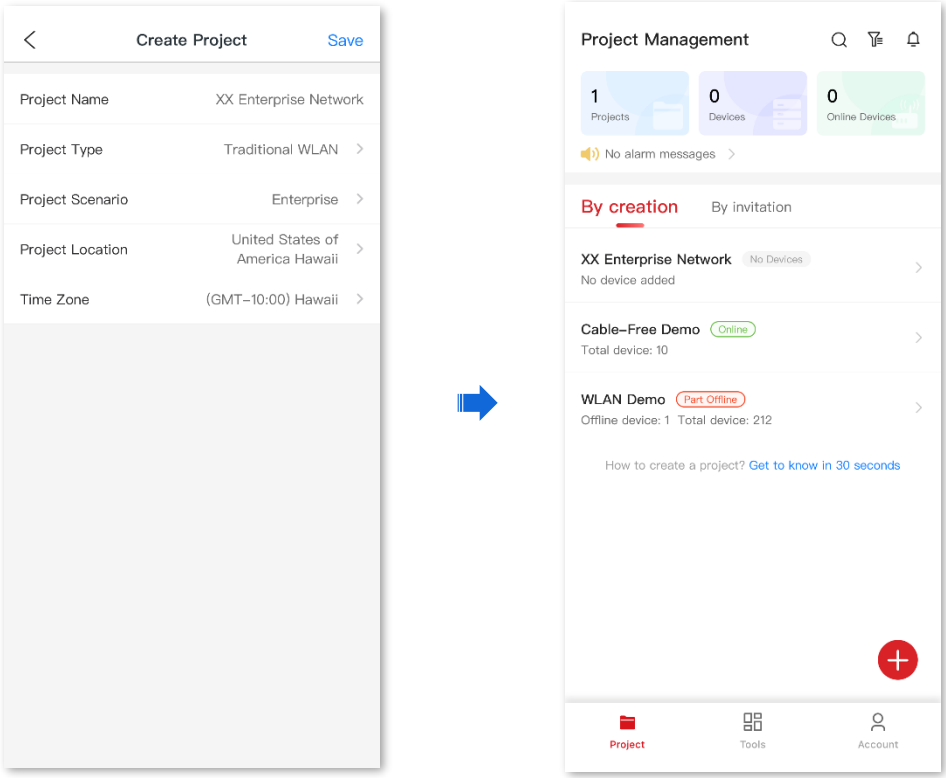
Scan to download ProFi App

2. Add a project on the ProFi App.

1) Enter **Project** page on the ProFi App and tap ⊕. Select a method to add a project. The following figure is for reference only.

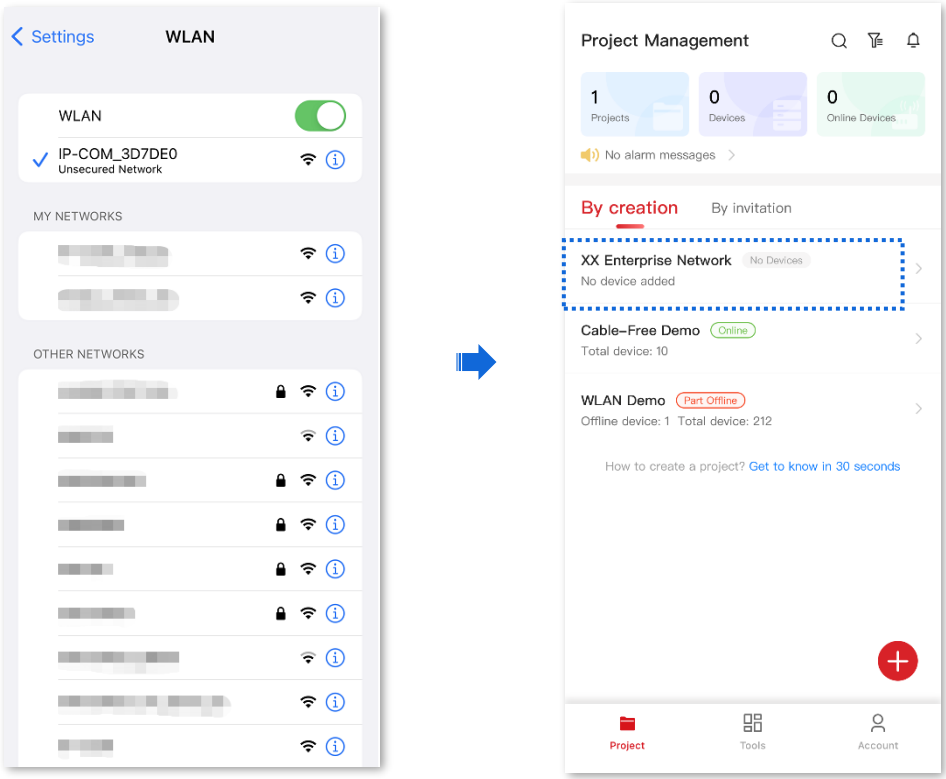


2) Configure project parameters and tap **Save**. The following figure is for reference only.

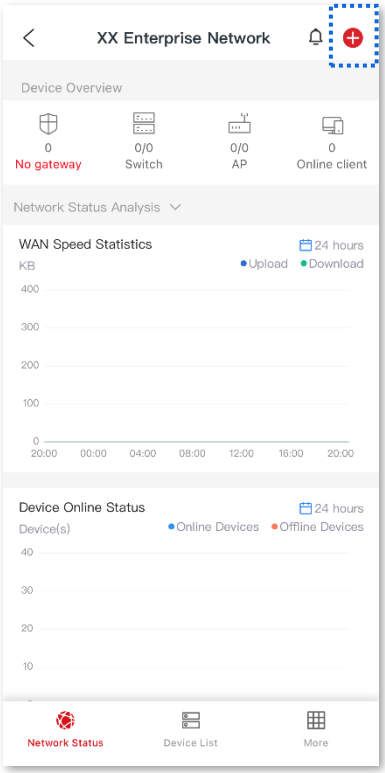


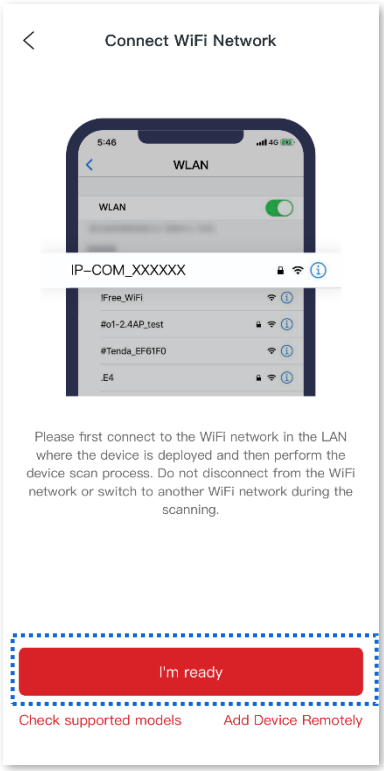
3. Add the router to the project.

1) Connect to the WiFi network in the LAN where the router is deployed (The WiFi provides internet access). Enter the management page of the ProFi App. The following figure is for reference only.

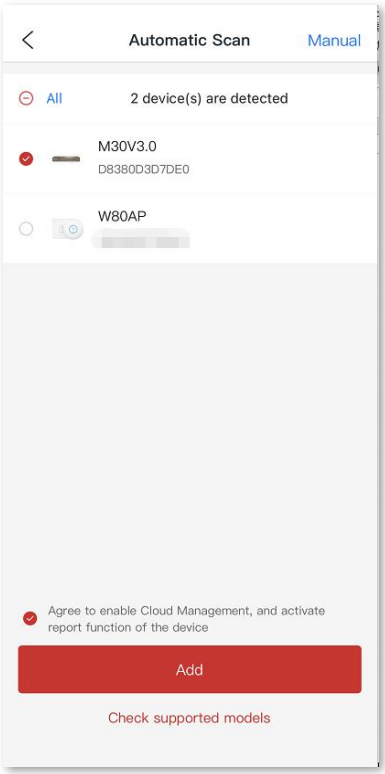


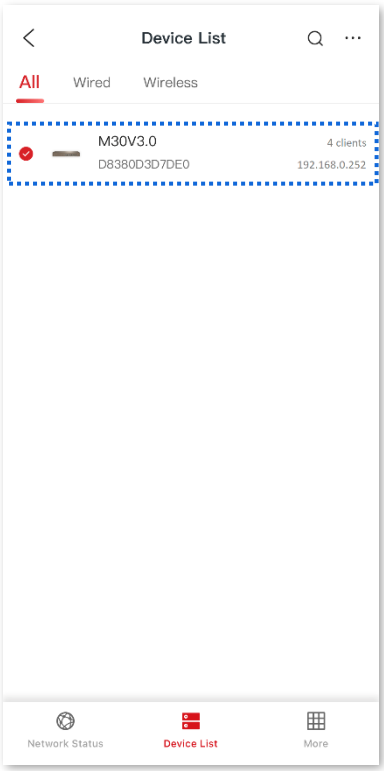
2) Tap ⊕ and tap **I'm ready**.





3) The App starts scanning devices in the LAN and the router will be detected automatically. Tick the device. Then tick **Agree to enable Cloud Management, and activate report function of the device**. Tap **Add** to add the device.





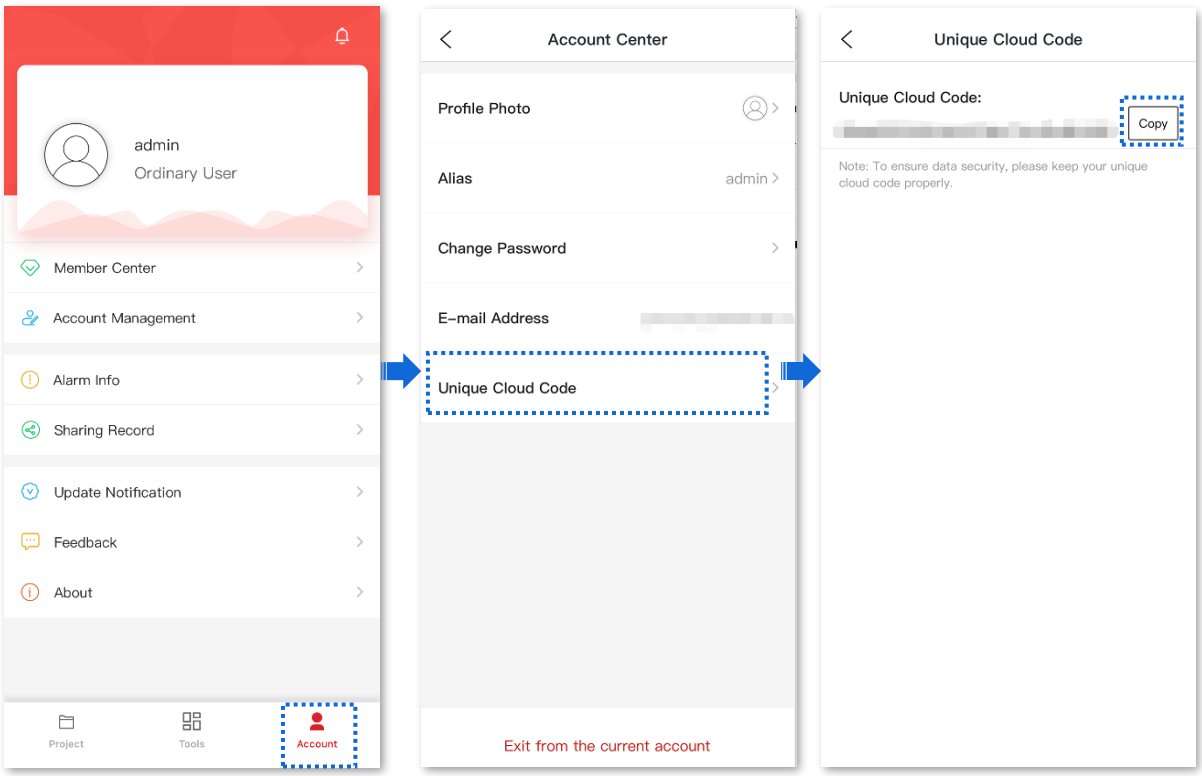
Configuration procedure (method 2)

Tip

- Before configuring the cloud maintenance function of the router, make sure that the router is successfully connected to the Internet.
- V1.4.3 App version is taken as an example here. The actual operation and interface display of the corresponding App version shall prevail.

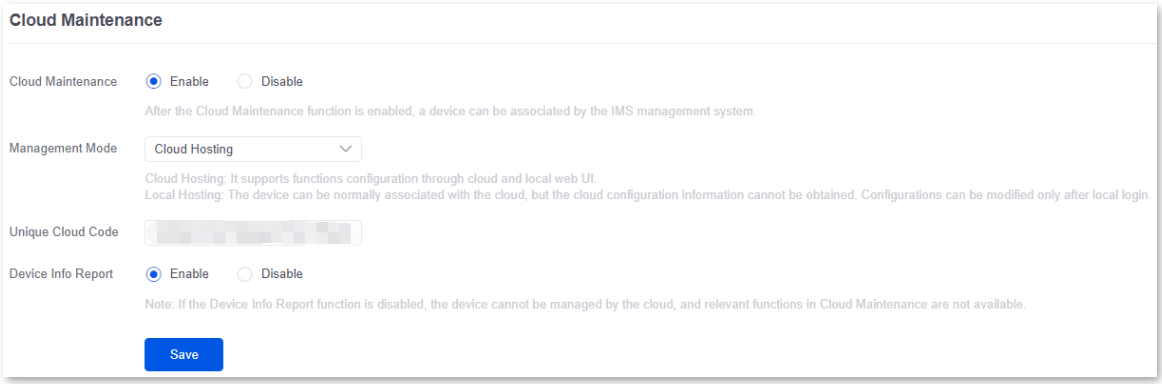
1. Log in to ProFi App and obtain **Unique Cloud Code**.

1) Run ProFi App on your phone and tap **Account** > . Then tap **Unique Cloud Code**.
2) Tap **Copy** to copy the unique cloud code.



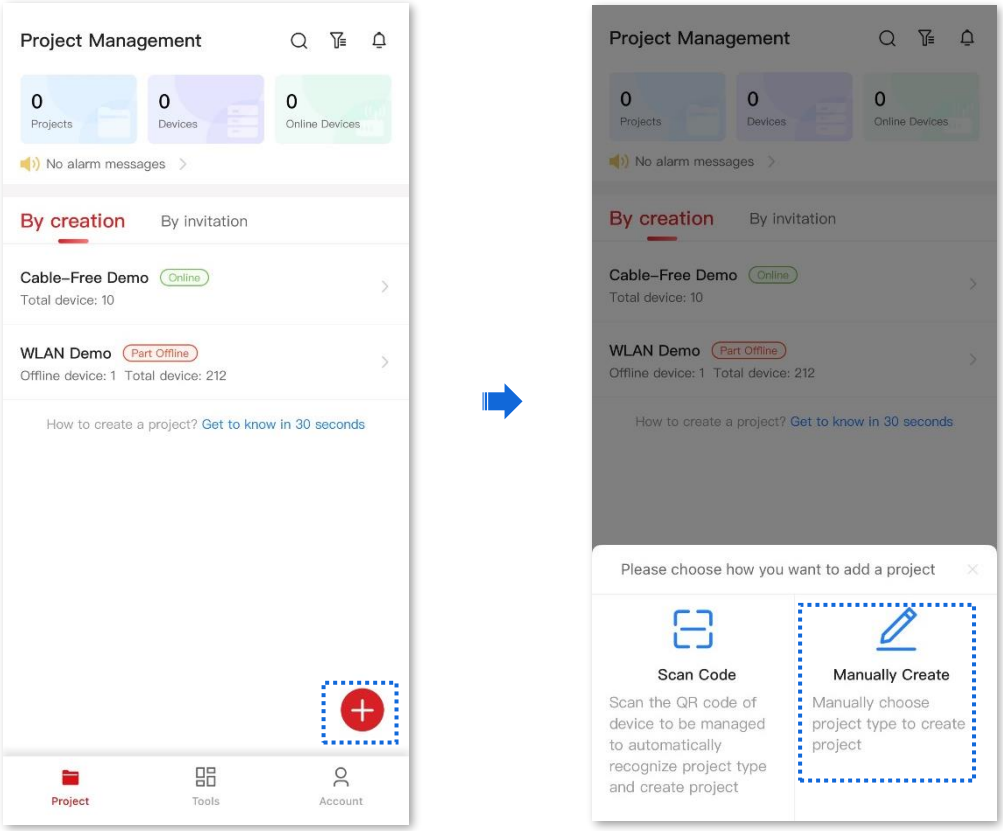
2. Enable the cloud maintenance function for the router.

1) Log in to the web UI of the router, and navigate to **More** > **Maintenance Service** > **Cloud Maintenance**.
2) Set **Cloud Maintenance** to **Enable**, and set **Management Mode** as required (**Cloud Hosting** for example here).
3) Enter the **Unique Cloud Code** and set **Device Info Report** to **Enable**. Confirm the prompt information (if it pops up) and click **OK**. Then click **Save**.

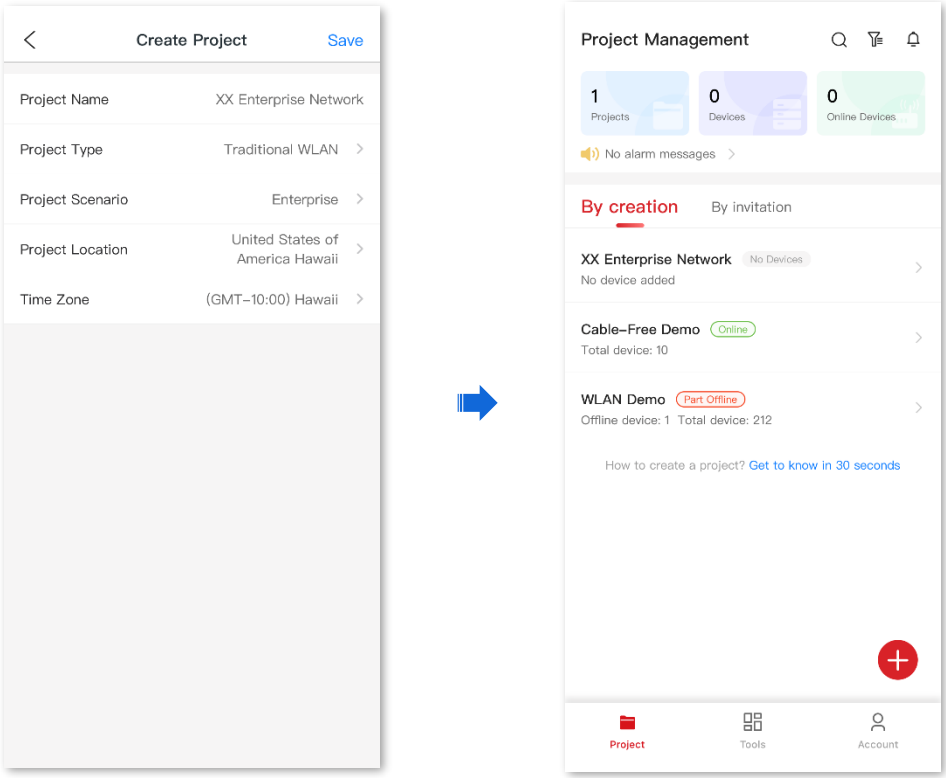


3. Add a project on the ProFi App.

1) Enter **Project** page on the ProFi App and tap ⊕. Select a method to add a project. The following figure is for reference only.



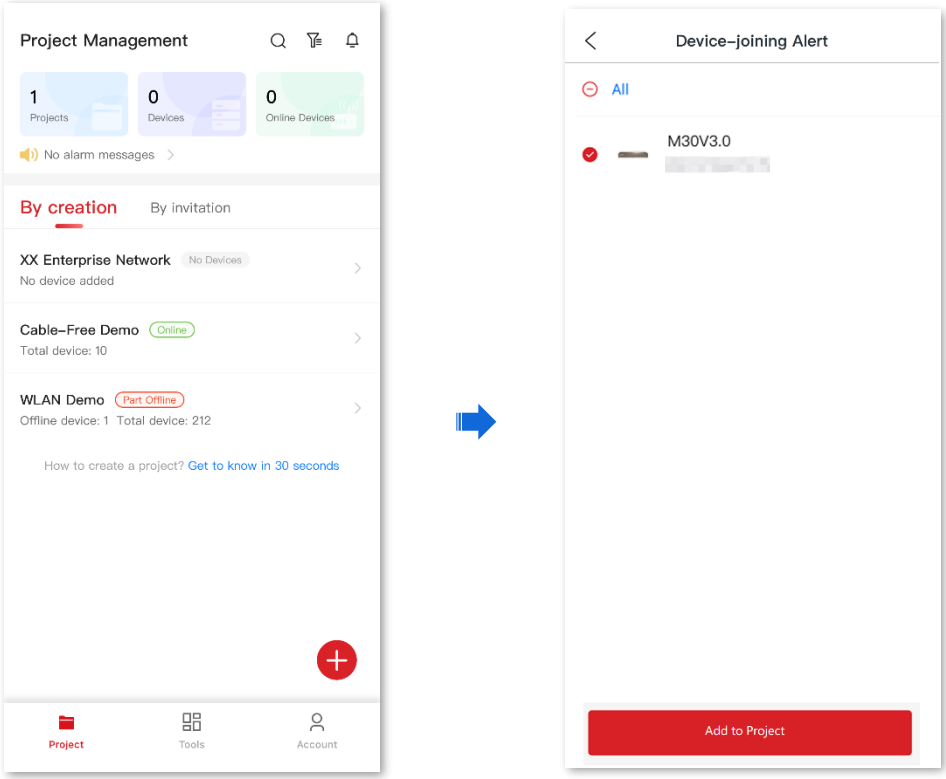
2) Configure project parameters and tap **Save**. The following figure is for reference only.



4. Add the router to the project.

1) Return to the App and tap  to view **Device-joining Alert** on the upper right corner.

2) Find this router and tap **Add to Project**.



3) Select the project to which you want to add the router and tap **Confirm**. Added successfully. You can return to the project list or enter the project as required.

---End

Verification

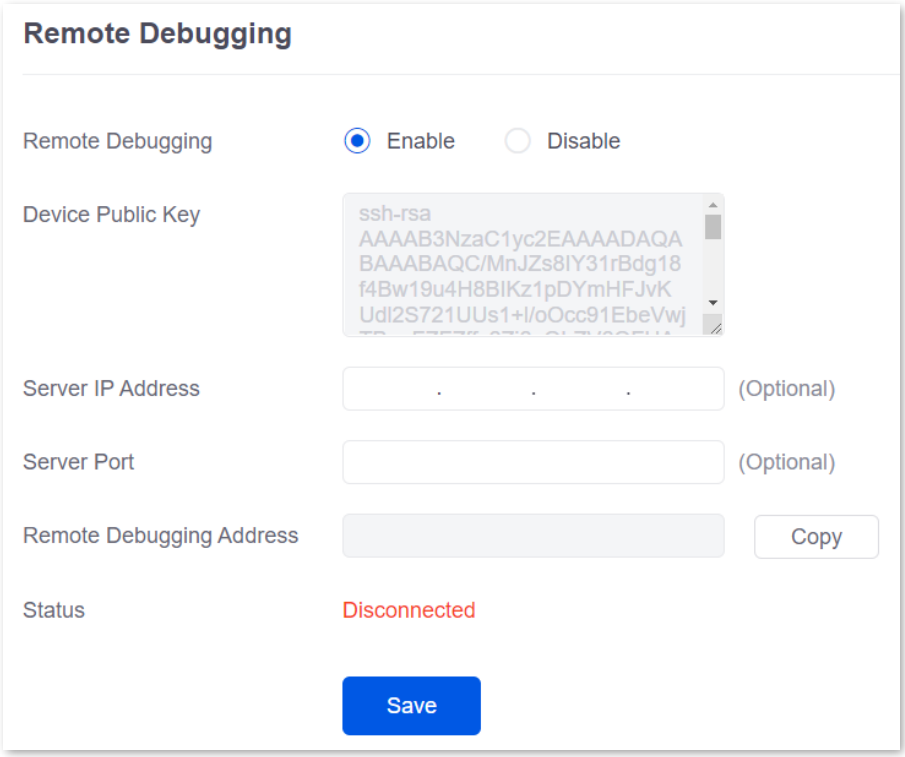
After the configuration, the router can be managed through the ProFi App, and all its configuration information is delivered by the ProFi App.

10.3.5 Remote debugging

Overview

This function can be used for remote network debugging by professional engineers. After enabling this function, professional engineers can remotely connect to the router through SSH and perform remote debugging.

Navigate to **More** > **Maintenance Service** > **Remote Debugging** to enter this page. On this page, you can configure the remote debugging function. By default, this function is disabled and the following figure shows an example with the function enabled.



Parameter description

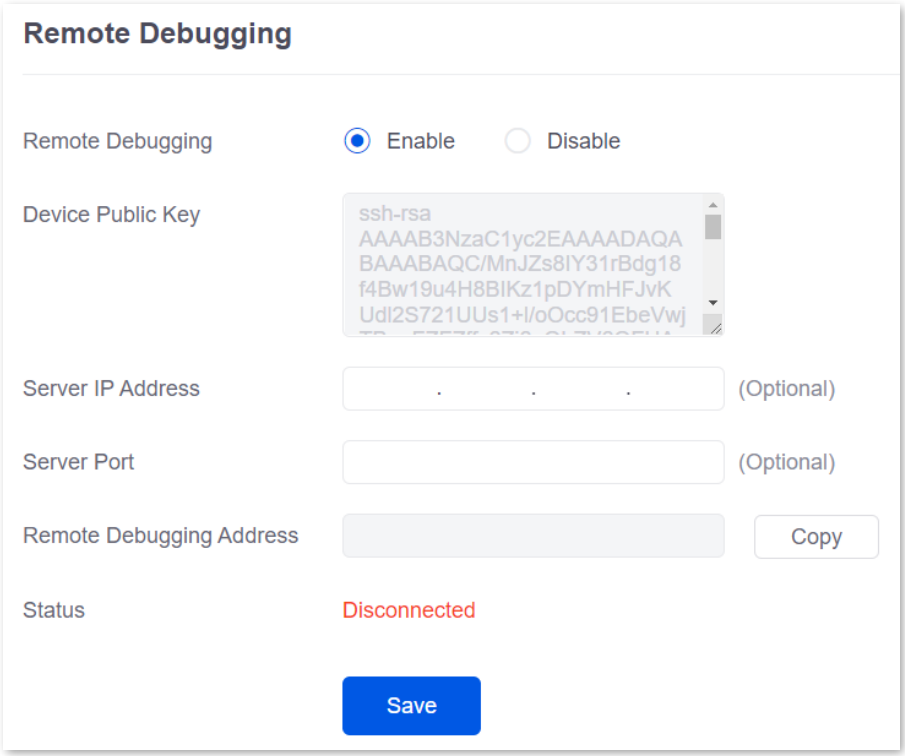
Parameter	Description
Remote Debugging	Used to enable or disable the remote debugging function.

Parameter	Description
Device Public Key	Specifies the RSA public key of the device. The device public key has been preset in the authorization list in the default server. If the default server is not used, you need to add the device public key on the customized server.
Server IP Address	Specifies the IP address of the external server, which must be a public IP address. When it is left blank, the default server is used.
Server Port	Specifies the service port of the external server. When it is left blank, the default server port is used.
Remote Debugging Address	Specifies the address for remotely accessing this device using SSH.
Status	Specifies the connection status between this device and the server.

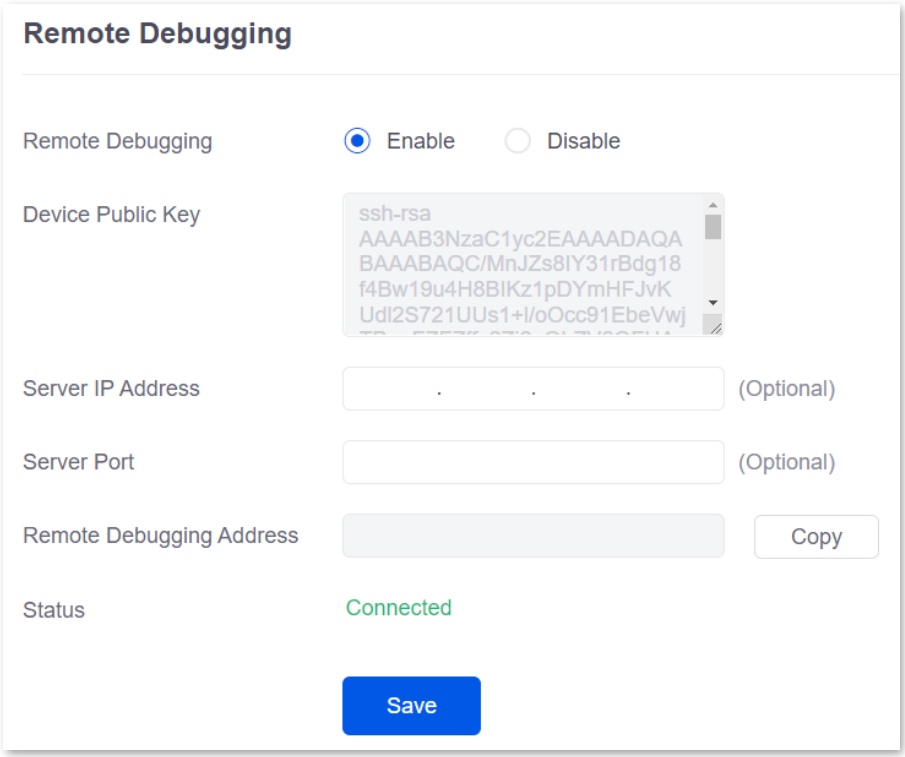
Remotely connect to the router using an SSH tool

Enable the remote debugging function

1. Log in to the Web UI of the router.
2. Navigate to **More** > **Maintenance Service** > **Remote Debugging**.
3. Set **Remote Debugging** to **Enable**. Retain default settings for other parameters and click **Save**.



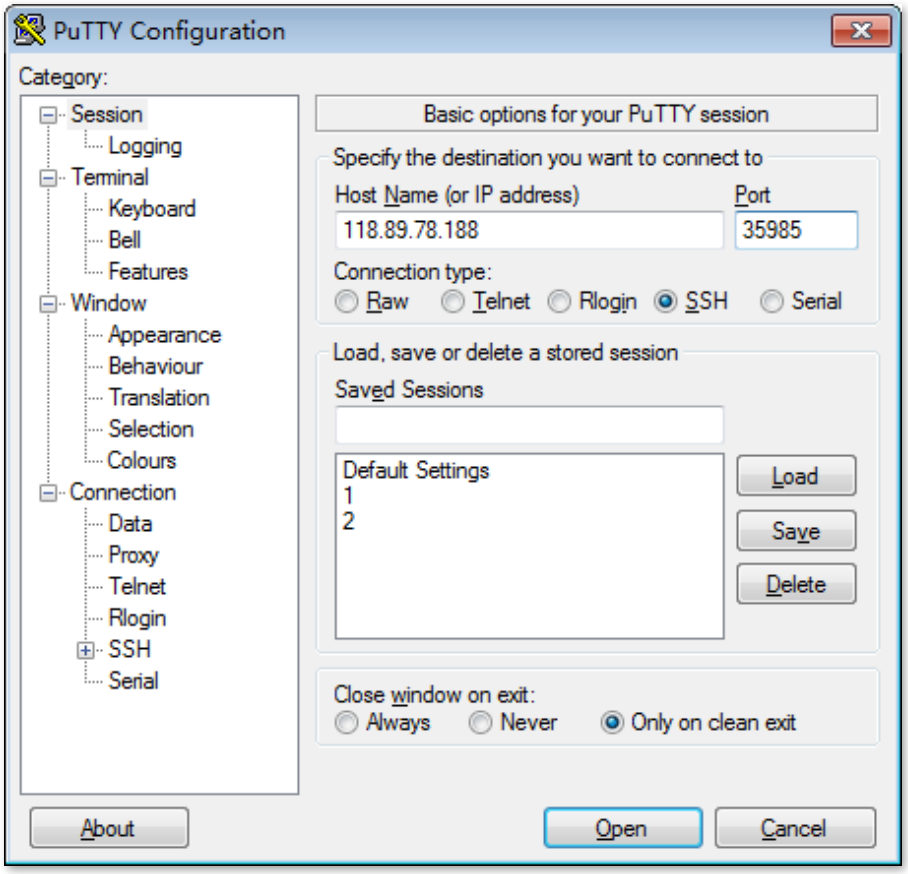
Wait a while. When **Status** is displayed as **Connected**, you can remotely connect to the router by entering destination IP address in the SSH tool.



Remotely connect to the router using an SSH tool

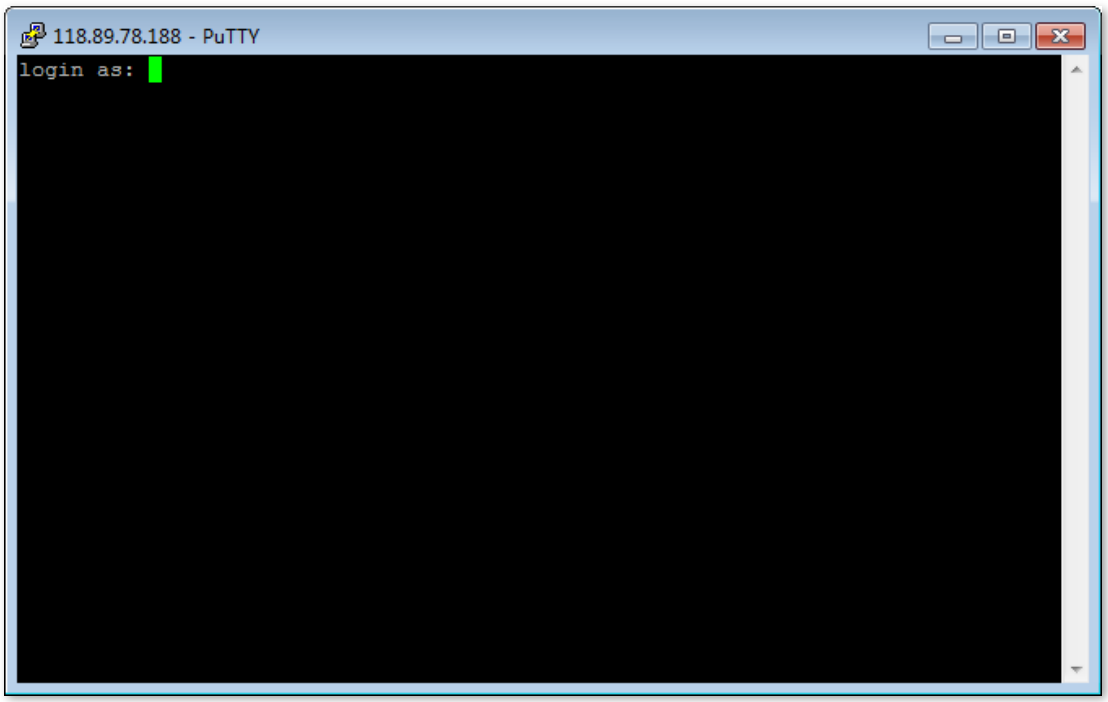
1. Run an SSH terminal tool (PuTTY used for example here) on a computer connected to the network.
2. Set **Connection Type** to **SSH**.
3. Set **Host Name (or IP address)** to the remote debugging address and port to be accessed.

   The following figure shows an example.
4. Click **Open**.



----End

If the following figure is displayed, you connect to the router successfully.



10.4 IPv6

10.4.1 Overview

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

IPv6 address

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

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

Basic concept

- **DHCPv6**

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

- **SLAAC**

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

10.4.2 Internet

Navigate to **More** > **IPv6** > **Internet** to enter the page. On this page, you can configure the IPv6 address of the corresponding WAN port.

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

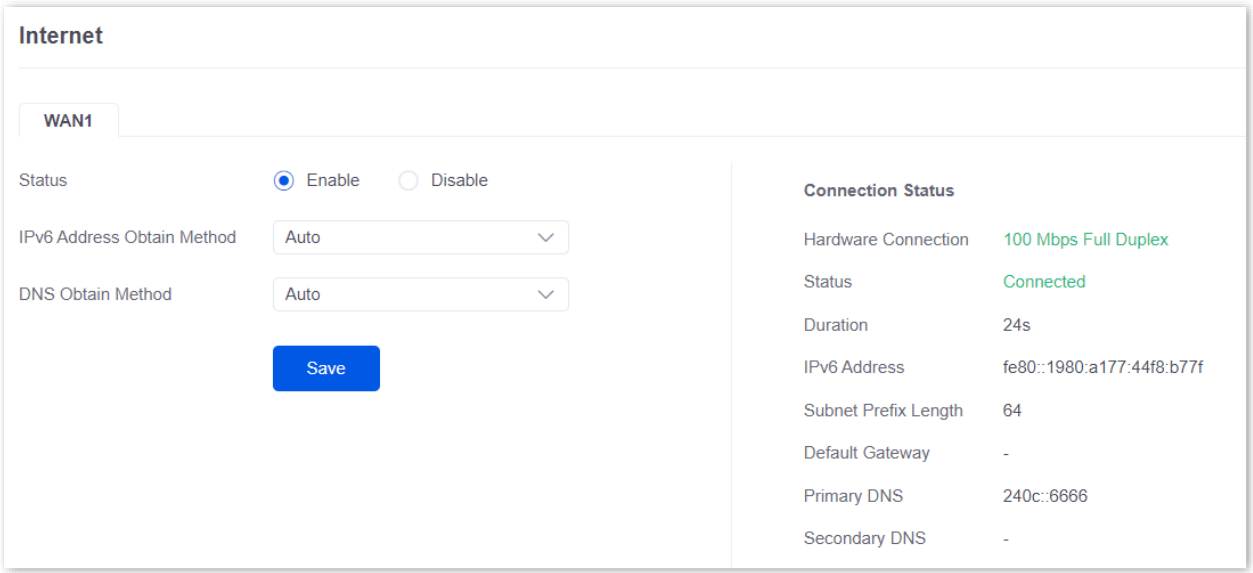
Condition	Selection
The IP address assignment modes of the LAN port on the upstream device are DHCPv6, SLAAC or DHCPv6+SLAA.	Auto
The upstream device is the ISP device, and the ISP provides a PPPoE account and password that supports IPv6 service.	
The upstream device is the ISP device, and the ISP does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

Note

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

Auto

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

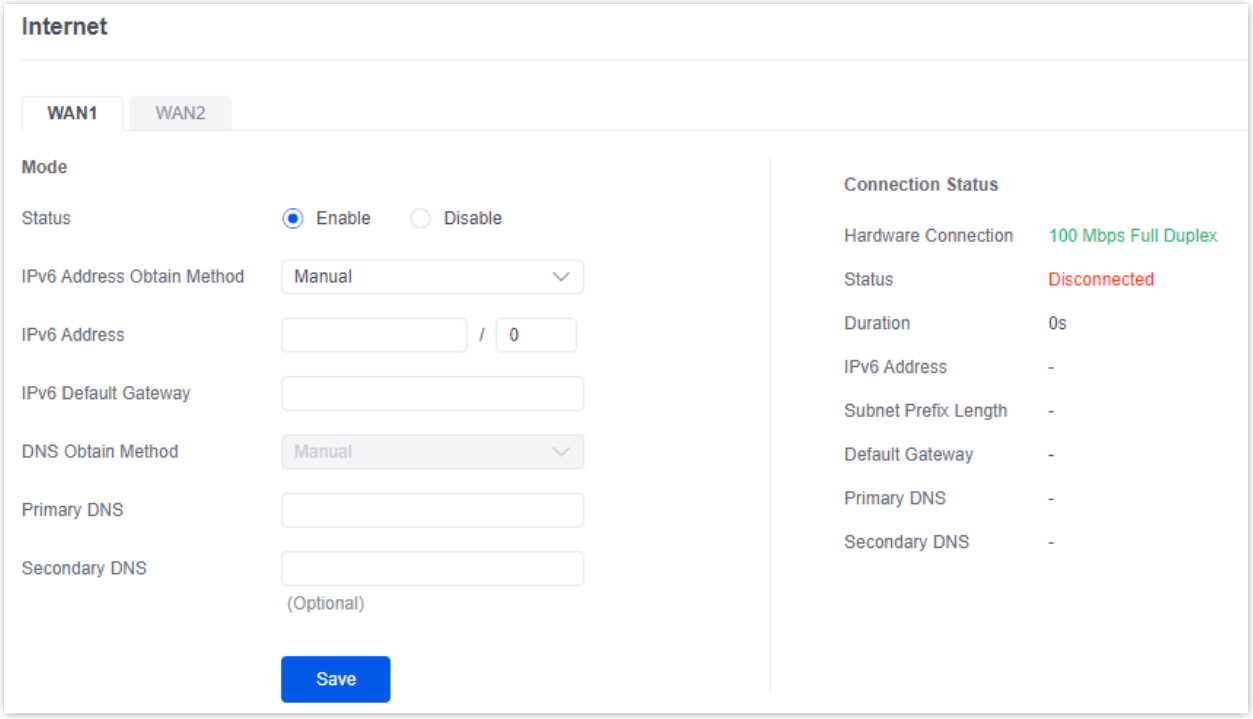


Parameter description

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

Manual

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



Parameter description

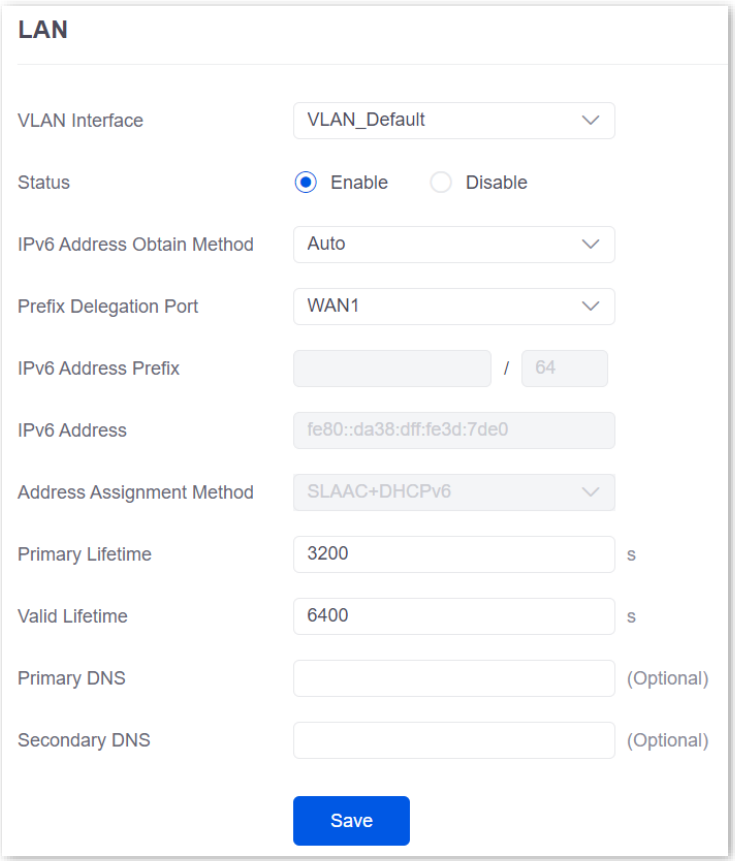
Parameter		Description
Mode	Status	Used to enable or disable the IPv6 function of the corresponding WAN port.
	IPv6 Address Obtain Method	Select **Manual**.
	IPv6 Address	Enter the IPv6 global unicast address provided by ISP.
	IPv6 Default Gateway	Enter the IPv6 default gateway provided by ISP.
	DNS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

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

10.4.3 LAN

Navigate to **More** > **IPv6** > **LAN** to enter the page. On this page, you can configure the IPv6 address of the corresponding VLAN so that multiple devices on the LAN can share the broadband server.

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



Parameter description

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

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

11 System maintenance

11.1 System time

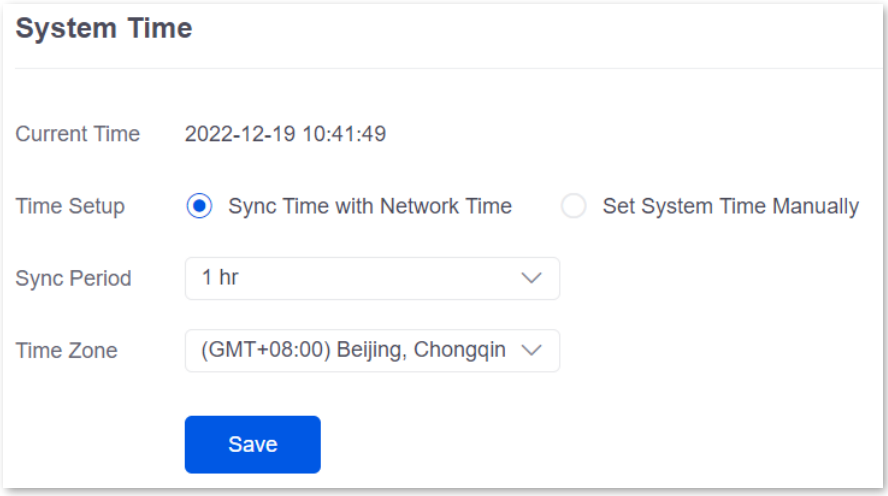
Navigate to **Tool** > **System Time** to enter the page. On this page, you can configure the system time of the router.

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

11.1.1 Sync time with network time

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

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



Parameter description

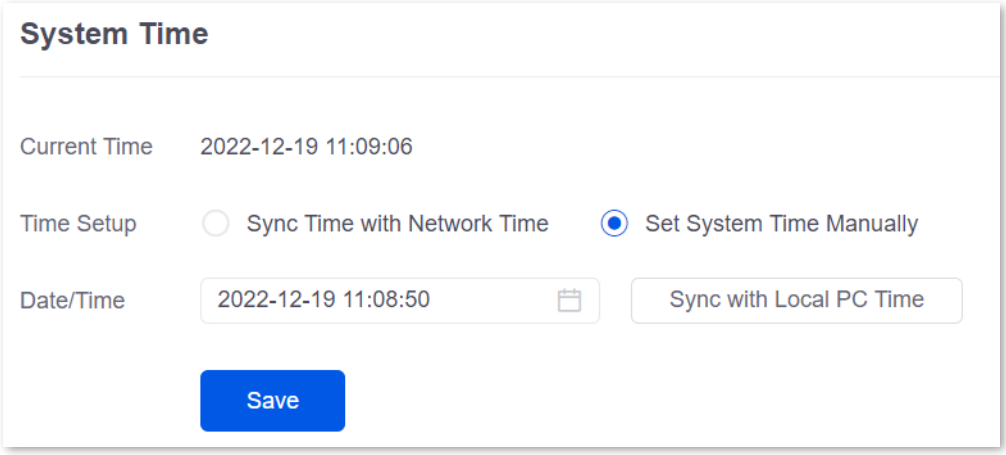
Parameter	Description
Current Time	Specifies the current system time of the router.

Parameter	Description
Time Setup	Specifies the setting mode of the system time. Select **Sync Time with Network Time**.
Sync Period	Specifies the interval at which the router synchronizes the system time with a time server on the internet.
Time Zone	Specifies the standard time zone in which the router is currently located.

11.1.2 Set system time manually

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

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



Parameter description

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

11.2 Diagnostic tool

11.2.1 Ping

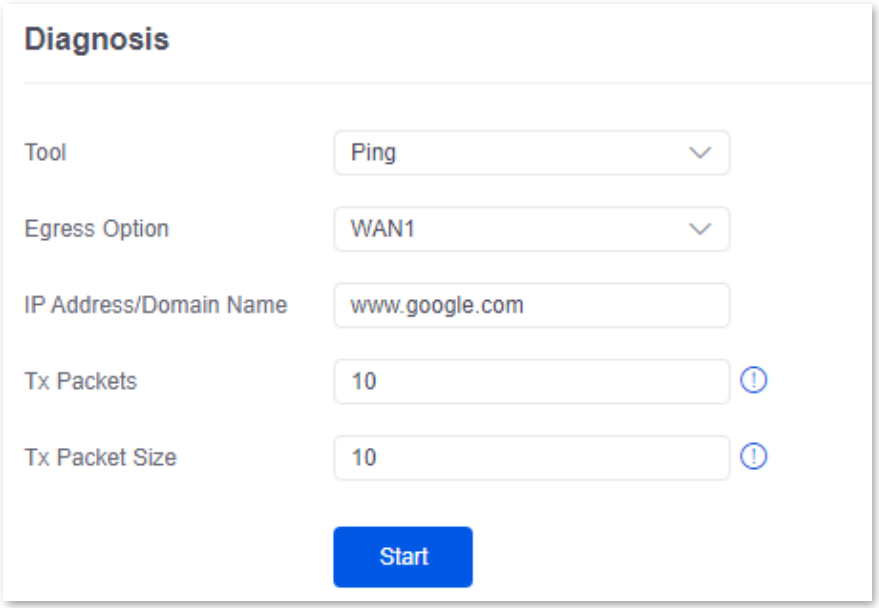
Ping is used to check whether the connection is correct and the connection quality.

Navigate to **Tool** > **Diagnosis** to enter the page. On this page, you can check whether the connection is correct and the connection quality with **Ping**.

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

To perform Ping test:

1. Log in to the Web UI of the router, and navigate to **Tool** > **Diagnosis**.
2. Select **Ping** from the **Tool** drop-down list box.
3. Set **Egress Option** to the interface for the test, which is **WAN1** in this example.
4. Enter the IP address or domain name of the ping target, which is **www.google.com** in this example.
5. Set **Tx Packets** to the number of packets sent in the Ping test, which is **10** in this example.
6. Set **Tx Packet Size** to the size of packets sent in the Ping test, which is **10** in this example.
7. Click **Start**.

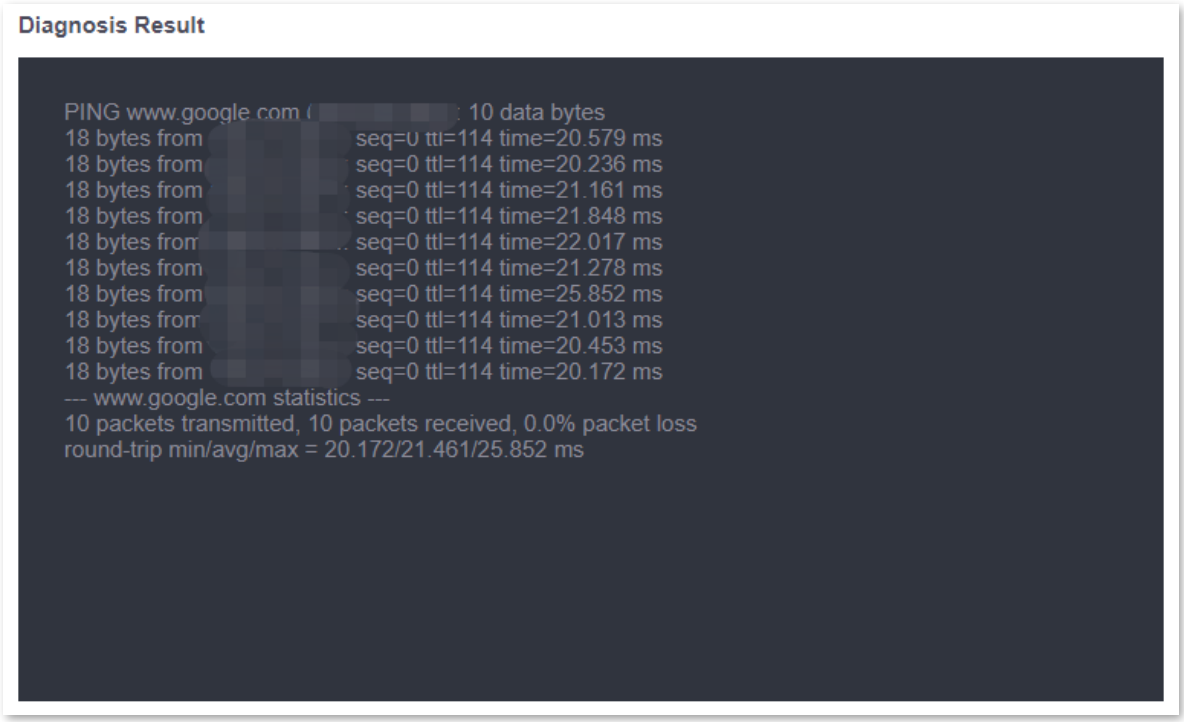


----End

Parameter description

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

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



11.2.2 Tracert

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

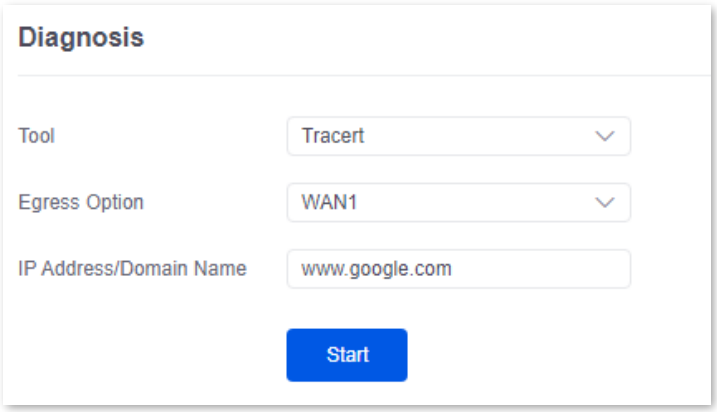
Navigate to **Tool** > **Diagnosis** to enter the page. On this page, you can detect the routes that a packet takes from a router to a destination host with **Tracert**.

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

To perform Tracert test:

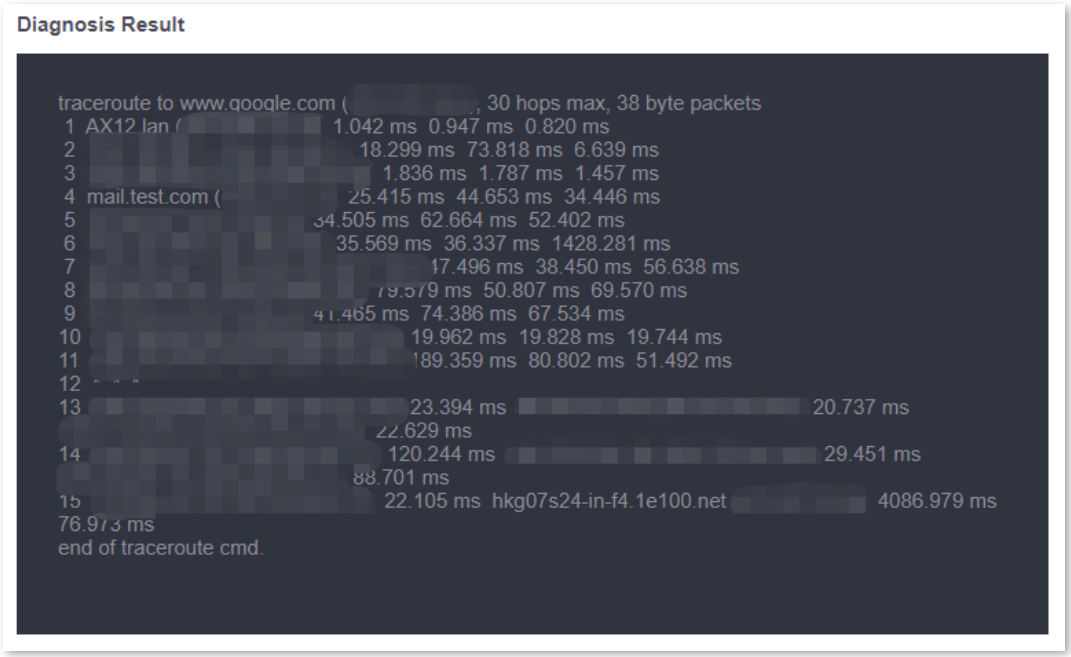
1. Log in to the Web UI of the router, and navigate to **Tool** > **Diagnosis**.
2. Select **Tracert** from the **Tool** drop-down list box.
3. Set **Egress Option** to the interface for the test, which is **WAN1** in this example.

4. Enter the IP address or domain name of the tracert target, which is **www.google.com** in this example.
5. Click **Start**.



----End

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



Parameter description

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

11.2.3 Packet capture tool

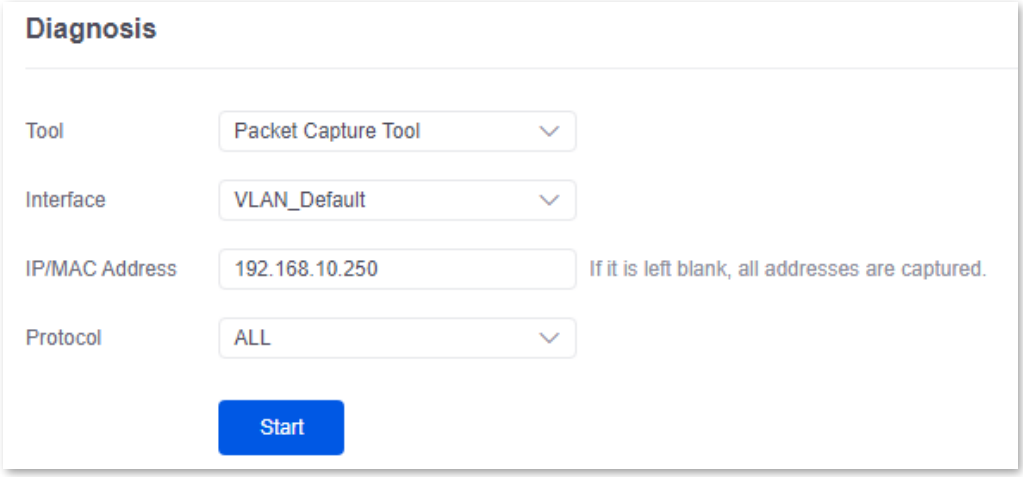
Packet Capture Tool is a network data collection and analysis tool, which can completely intercept the specified data packets in the network to provide analysis.

Navigate to **Tool** > **Diagnosis** to enter the page. On this page, you can intercept the specified data packets of an interface with **Packet Capture Tool**.

Assume that you want to intercept all types of data packets from the router's LAN4 port. The IP address of the LAN4 port is 192.168.10.250, which belongs to VLAN_Default.

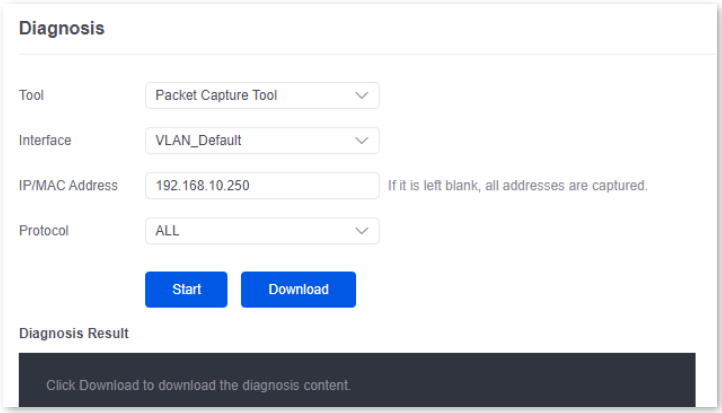
Configuration procedure:

1. Log in to the Web UI of the router, and navigate to **Tool** > **Diagnosis**.
2. Select **Packet Capture Tool** from the **Tool** drop-down list box.
3. Set **Interface** to the VLAN interface to intercept data, which is **VLAN_Default** in this example.
4. Set **IP/MAC Address** of the LAN4 port, which is **192.168.10.250** in this example.
5. Set **Protocol**, which is **ALL** in this example.
6. Click **Start**.



7. (Optional) During packet capture, click **End** as required.
8. Click **Download**.

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



----End

Parameter description

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

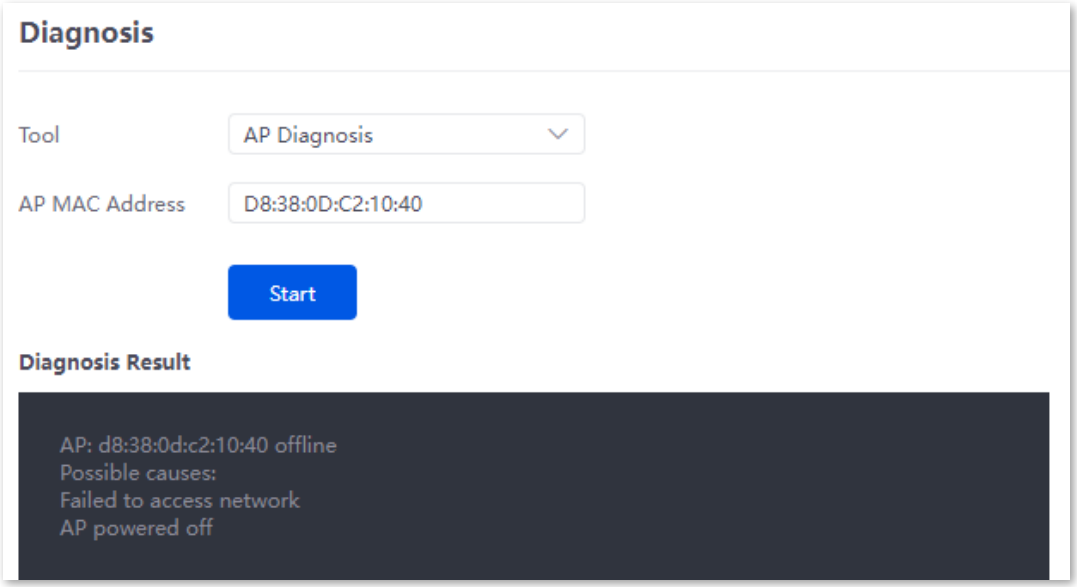
11.2.4 AP diagnosis

Navigate to **Tool** > **Diagnosis** to enter the page. On this page, you can view the AP status based on the MAC address, including online status, IP address, and AP group to which it belongs.

Assume that you want to perform diagnosis on an AP (MAC address: D8:38:0D:C2:10:40) in the network, follow the steps below:

1. Log in to the web UI of the router, and navigate to **Tool** > **Diagnosis**.
2. Select **AP Diagnosis** for **Tool**.
3. Set **AP MAC Address** to the MAC address of the AP, which is **D8:38:0D:C2:10:40** in this example.
4. Click **Start**.

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



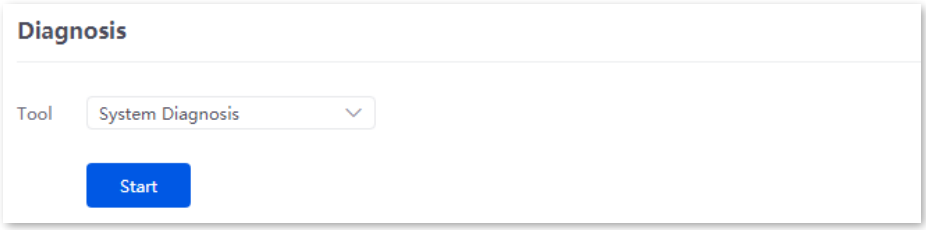
---End

11.2.5 System diagnosis

Navigate to **Tool** > **Diagnosis** to enter the page. On this page, you can view the status information of all processes in the system.

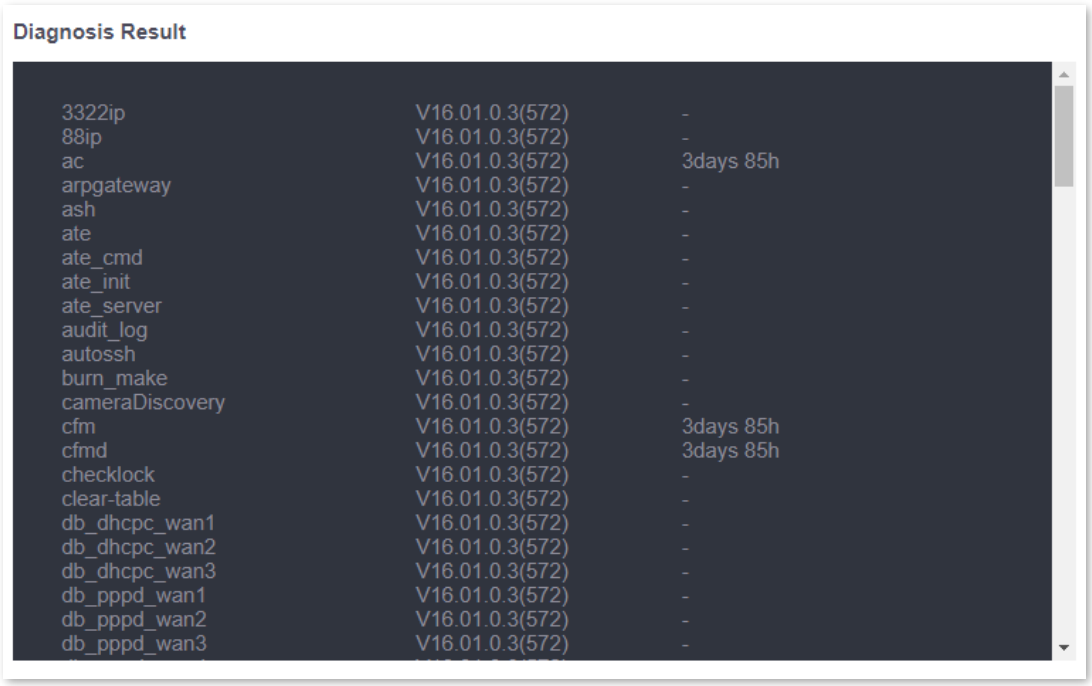
To perform system diagnosis:

1. Log in to the web UI of the router, and navigate to **Tool** > **Diagnosis**.
2. Select **System Diagnosis** for **Tool**.
3. Click **Start**.



---End

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

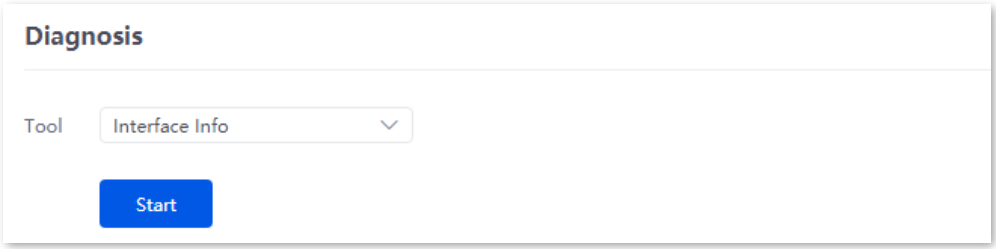


11.2.6 Interface info

Navigate to **Tool** > **Diagnosis** to enter the page. On this page, you can view the interface information of the router, including the physical interface, bridging interface, tunnel interface and VLAN virtual interface. The bridging interface and the VLAN virtual interface are generated when the VLAN is created, but no VLAN virtual interface is generated when the VLAN is 0. The tunnel interface is generated when the SSID policy is created.

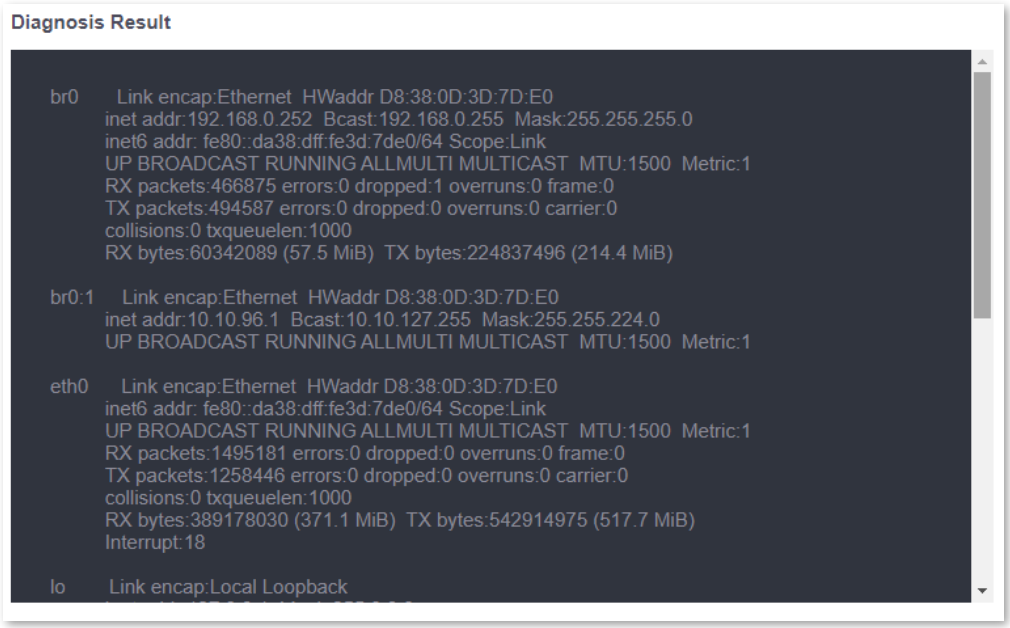
To check the interface information:

1. Log in to the web UI of the router, and navigate to **Tool** > **Diagnosis**.
2. Select **Interface Info** for **Tool**.
3. Click **Start**.



---End

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



11.3 Log center

Navigate to **Tool** > **Log Center** to enter the page. On this page, you can view the log information recorded by the router.

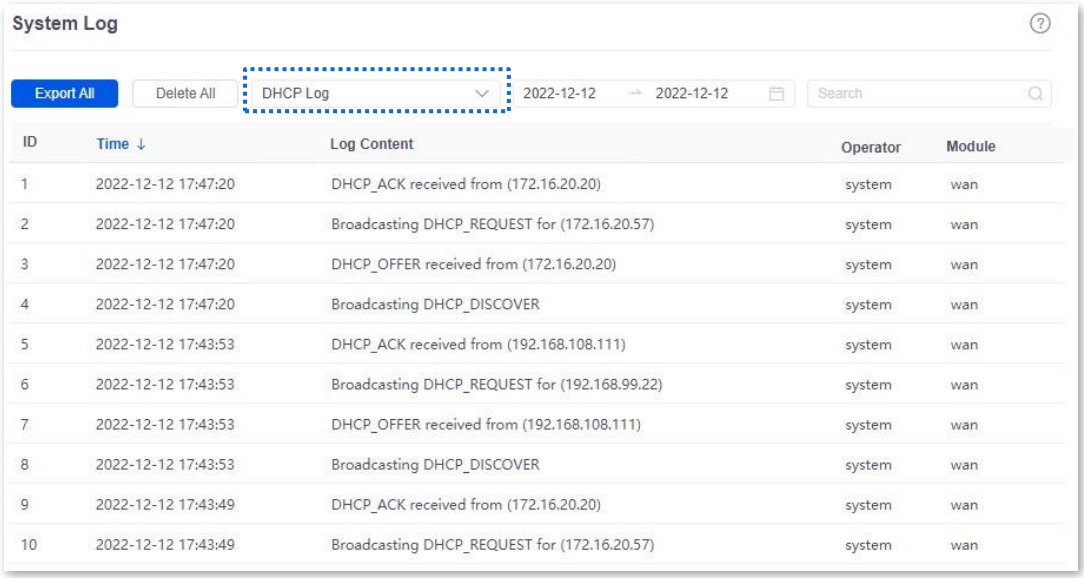
The log center records the **System Log**, **Operating Log** and **Running Log** of the router. In case of network failure, you can use the router's log center to troubleshoot the problem.

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

11.3.1 System log

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

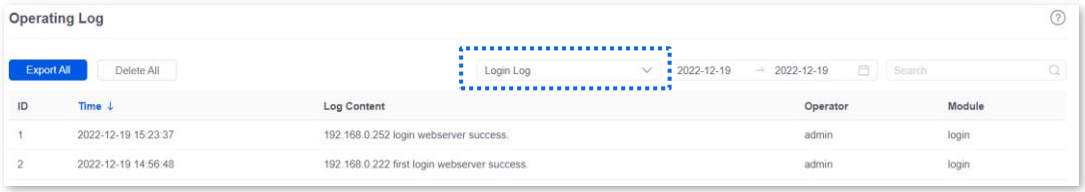
Navigate to **Tool** > **Log Center** > **System Log** to enter the page. Click the drop-down list box on this page. You can view certain log information of the router.



11.3.2 Operating log

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

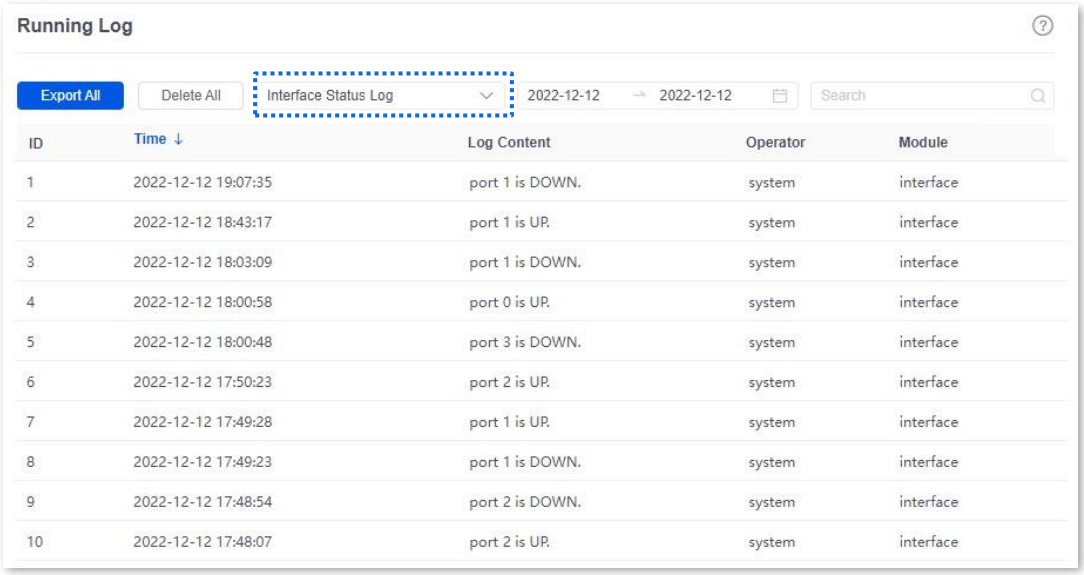
Navigate to **Tool** > **Log Center** > **Operating Log** to enter the page. You can view certain operation information of the router by selecting log types from the drop-down list box highlighted on the following figure.



11.3.3 Running log

The **Running Log** records the information of the system process running and the AP report.

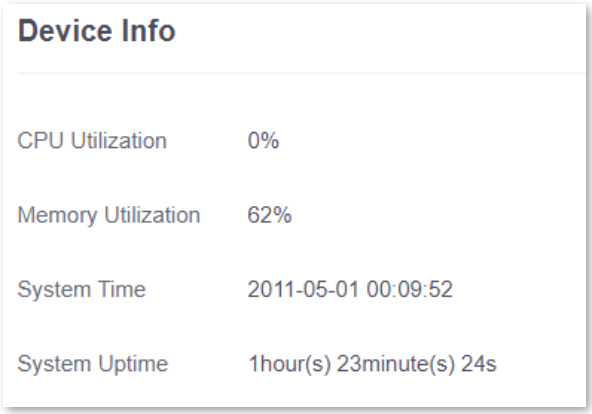
Navigate to **Tool** > **Log Center** > **Running Log** to enter the page. You can view certain information of the system process running and the AP report of the router by selecting log types from the drop-down list box highlighted on the following figure.



11.4 System maintenance

11.4.1 Device info

Navigate to **Tool** > **Maintenance** > **Device Info**. On this page, you can view the basic composition and usage of current system hardware, as well as system time and running time.



11.4.2 Restore & Backup

Overview

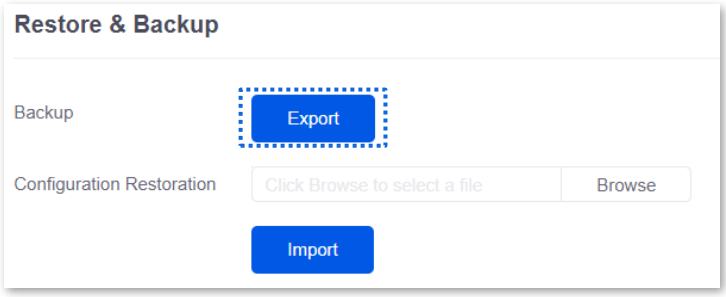
You can use the Backup function to copy the current configurations of the router to the local computer and use the Configuration Restoration function to restore the configurations of the router to the backed-up configurations.

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

Navigate to **Tool** > **Maintenance** > **Restore & Backup**. On this page, you can use the Backup and Restore function.

Backup

1. Log in to the Web UI of the router.
2. Navigate to **Tool** > **Maintenance** > **Restore & Backup**.
3. Click **Export**.



----End

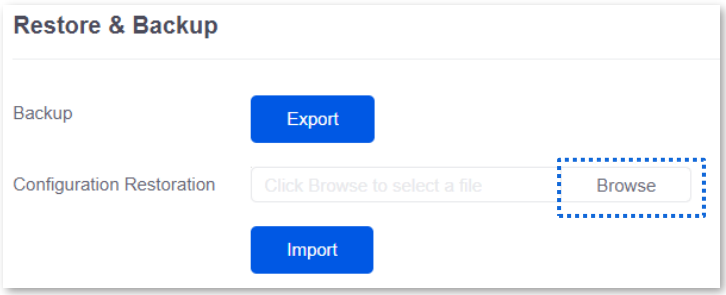
The browser will download a configuration file named **RouterCfm.cfg**.

Tip

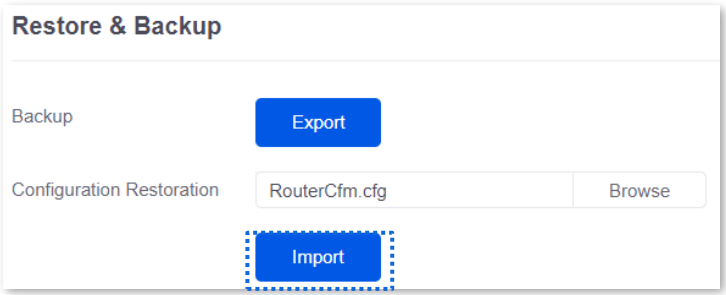
If the message “This type of file can harm your computer. Do you want to keep RouterCfm.cfg anyway?” appears on the page, click “Keep”.

Restore

1. Log in to the Web UI of the router.
2. Navigate to **Tool** > **Maintenance** > **Restore & Backup**.
3. Click **Browse**, and select the configuration file you have backed up.



4. Click **Import**.



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

----End

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

11.4.3 Factory settings restore

Overview

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

The router supports two resetting methods:

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

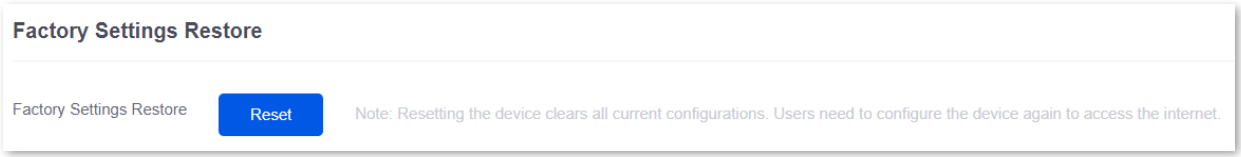
After the reset, the default LAN IP address of the router is 192.168.0.252.

Note

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

Reset the device using web UI

1. Log in to the Web UI of the router.
2. Navigate to **Tool** > **Maintenance** > **Factory Settings Restore**.
3. click **Reset**.



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

----End

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

Reset the device using the RESET button

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

When the **SYS** LED indicator is blinking, hold down the reset button (**RESET** or **Reset**) with a needle-like object for about 8 seconds and release it when the **SYS** LED indicator light is solid green. When the **SYS** LED indicator blinks again, the router is reset successfully.

11.5 Upgrade service

11.5.1 Overview

Navigate to **Tool** > **Upgrade Service**. On this page, you can upgrade the router's firmware and feature-library.

- System firmware upgrade: You can upgrade the firmware of the router to experience more functions and get a better user experience. The router supports **Local Upgrade** and **Online Upgrade**. The default upgrade mode is **Local Upgrade**.
- Feature-Library upgrade: You can update the router's feature-library. The upgrading of feature-library does not incur the upgrading of the system. The router supports **Local Upgrade** and **Online Upgrade**. The default upgrade mode is **Local Upgrade**.

Parameter description

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

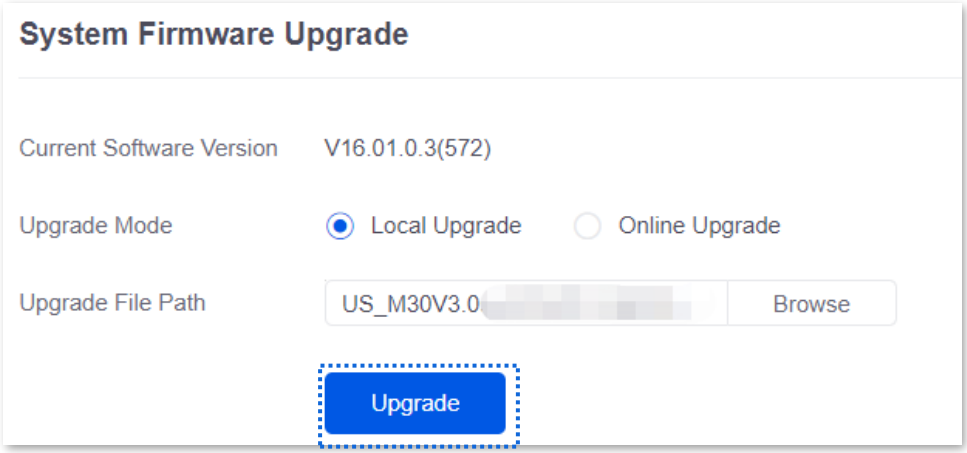
11.5.2 System firmware upgrade

Note

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

Navigate to **Tool** > **Upgrade Service** > **System Firmware Upgrade**. On this page, you can upgrade the firmware of the router.

1. Visit www.ip-com.com.cn, download the upgrade firmware of the corresponding model to your computer and unzip it.
2. Log in to the web UI of your router, and navigate to **Tool** > **Upgrade Service** > **System Firmware Upgrade**.
3. Select **Local Upgrade** for **Upgrade Mode**.
4. Click **Browse**. Select and upload the firmware that has been downloaded to your computer in step 1, and click **Upgrade**.



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

----End

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

Tip

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

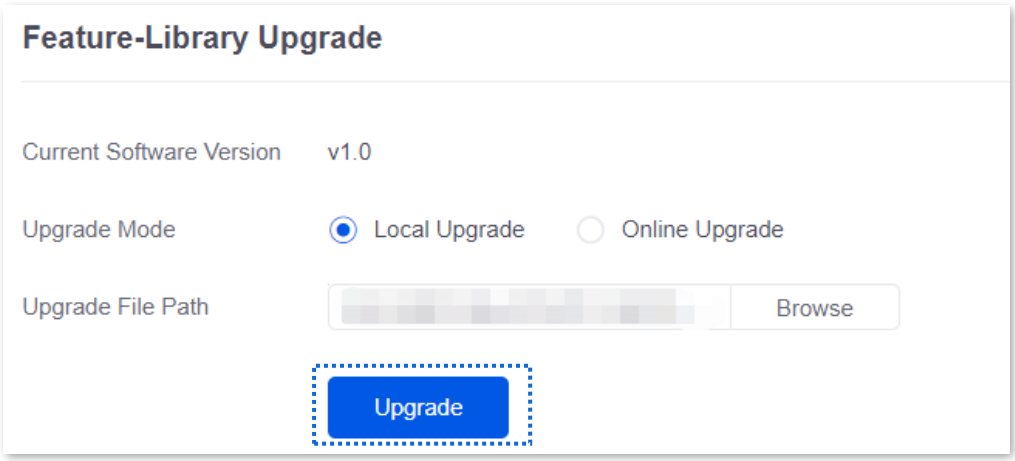
11.5.3 Feature-Library upgrade

Note

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

Navigate to **Tool** > **Upgrade Service** > **Feature-Library Upgrade**. On this page, you can upgrade the router's feature-library.

1. Visit www.ip-com.com.cn, download the latest feature-library file of the corresponding model and save it to your computer.
2. Log in to the web UI of your router, and navigate to **Tool** > **Upgrade Service** > **Feature-Library Upgrade**.
3. Select **Local Upgrade** for **Upgrade Mode**.
4. Click **Browse**. Select and upload the feature-library file that has been downloaded to your computer in step 1, and Click **Upgrade**.



----End

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

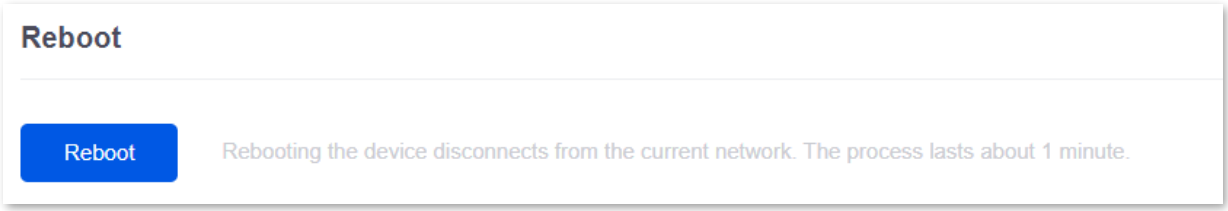
11.6 Reboot services

11.6.1 Reboot

Navigate to **Tool** > **Reboot Services** > **Reboot**. On this page, you can reboot the router to make certain settings take effect and improve the performance of the router. Rebooting the device disconnects from the current network. The process lasts about 1 minute. It is recommended to reboot the device when the network is relatively idle.

Reboot steps:

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



11.6.2 Scheduled reboot

Navigate to **Tool** > **Reboot Services** > **Scheduled Reboot**. On this page, by setting the router to reboot periodically during leisure time, you can prevent the decreasing of performance and instability of the router after running for a long period.

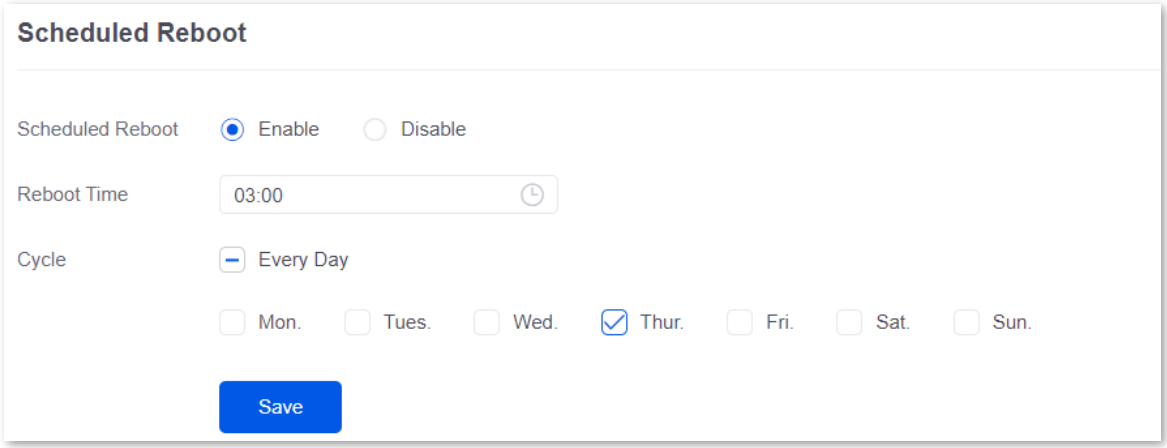
Tip

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

Scheduled reboot steps:

1. Log in to the Web UI of the router.
2. Navigate to **Tool** > **Reboot Services** > **Scheduled Reboot**.
3. Select **Enable** for **Scheduled Reboot**.
4. Select the time when the router will automatically reboot, which is **03:00** in this example.
5. Select the reboot date, which is **Thur.** in this example.

6. Click **Save**.

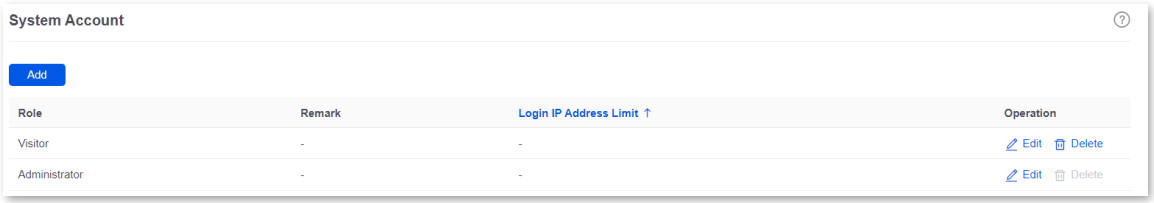


----End

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

11.7 System account

Navigate to **Tool** > **System Account**. On this page, you can add, modify or delete the administrator and visitor accounts.

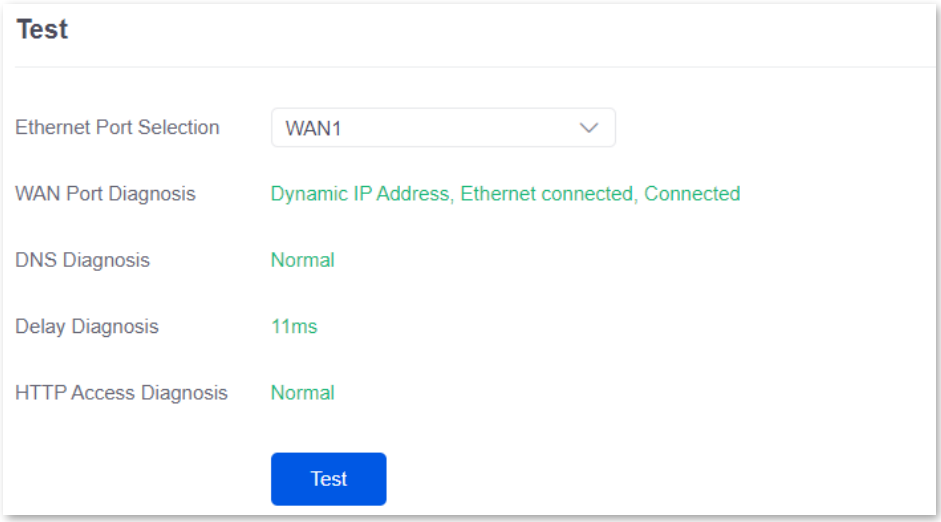


Parameter description

Parameter	Description
Add	Used to add a new system account.
Role	Specifies the user role in managing the web UI. There is an administrator account by default. The operation authority of corresponding user roles is described as follows: – **Administrator**: Able to view and configure all functions of the router. – **Visitor**: Only able to view configurations of the router except system account information.
Password Confirm Password	Used to set the login password of the account.
Remark	Specifies the remark for the account. You can enter the description for the operation permission of the account.
Login IP Address Limit	Specifies the IP addresses of the users of the account. After the configuration, only users with the IP address or within the IP address range can use the account to access the web UI.
Operation	Used to edit or delete account information. The super-administrator account cannot be added or deleted. Edit: Used to modify the account information. Delete: Used to delete the account information.

11.8 Test

Navigate to **Tool** > **Test**. On this page, you can perform a network test on the WAN port of the router.



Parameter description

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

Appendix

Acronyms and abbreviations

Acronym or Abbreviation	Full Spelling
ACK	Acknowledge
AES	Advanced Encryption Standard
AH	Authentication Header
AP	Access Point
APSD	Automatic Power Save Delivery
ARP	Address Resolution Protocol
ASCII	American Standard Code for Information Interchange
AuthN	Authentication
BW	Bandwidth
CHAP	Challenge Handshake Authentication Protocol
CPU	Central Processing Unit
DDNS	Dynamic Domain Name Service
DDoS	Distributed Denial of Service
DES	Data Encryption Standard
DH	Diffie-Hellman
DHCP	Dynamic Host Configuration Protocol
DHCPv6	Dynamic Host Configuration Protocol for IPv6
DMZ	Demilitarized Zone

Acronym or Abbreviation	Full Spelling
DNS	Domain Name System
DPD	Dead Peer Detection
DTIM	Delivery Traffic Indication Map
EDCA	Enhanced Distributed Channel Access
ERP	Enterprise Resource Planning
ESP	Encapsulating Security Payload
FTP	File Transfer Protocol
GRE	Generic Routing Encapsulation
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ICMP	Internet Control Message Protocol
ID	Identity Document
IEEE	Institute of Electrical and Electronics Engineers
IKE	Internet Key Exchange
IP	Internet Protocol
IPsec	Internet Protocol Security
IPTV	Internet Protocol Television
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
ISAKMP	Internet Security Association and Key Management Protocol
ISP	Internet Service Provider
L2TP	Layer 2 Tunneling Protocol
LAN	Local Area Network

Acronym or Abbreviation	Full Spelling
LCP	Link Control Protocol
LDAP	Lightweight Directory Access Protocol
LED	Light Emitting Diode
MAC	Medium Access Control
MPDU	Message Protocol Data Unit
MPPE	Microsoft Point-to-Point Encryption
MS-CHAP	Microsoft Challenge Handshake Authentication Protocol
MSDU	Multiple MAC Service Data Units
MTU	Maximum Transmission Unit
NAT	Network Address Translation
NTS	Network time server
ONVIF	Open Network Video Interface Forum
PAP	Password Authentication Protocol
PFS	Perfect Forward Secrecy
PPP	Point to Point Protocol
PPPoE	Point-to-Point Protocol over Ethernet
PPTP	Point to Point Tunneling Protocol
PVID	Port-based VLAN ID
PoE	Power over Ethernet
QoS	Quality of Service
RA	Router Advertisement
RADIUS	Remote Authentication Dial In User Service
RSSI	Received Signal Strength Indicator

Acronym or Abbreviation	Full Spelling
RTS	Request to Send
RX	Receive
SA	Security Association
SDN	Software Defined Network
SKEME	Security Key Exchange Mechanism
SLAAC	Stateless Address Autoconfiguration
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
SN	Serial Number
SNMP	Simple Network Management Protocol
SPI	Security Parameter Index
SSH	Secure Shell
SSID	Service Set Identifier
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TKIP	Temporal Key Integrity Protocol
TX	Transmit
UDP	User Datagram Protocol
UI	User Interface
UPnP	Universal Plug and Play
URL	Uniform Resource Locator
USB	Universal Serial Bus
UTF-8	8-bit Unicode Transformation Format

Acronym or Abbreviation	Full Spelling
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
VoIP	Voice over Internet Protocol
WAN	Wide Area Network
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network
WMM	Wi-Fi Multi-Media
WPA	Wi-Fi Protected Access
WPA-PSK	WPA-Preshared Key