IP-COM

User Guide

2.5G Cloud Managed VPN Router

www.ip-com.com.cn

Copyright statement

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

This guide describes how to configure each feature of the following IP-COM 2.5G Enterprise router.

- M35
- M50-F
- M80-F

Note

Features available in the router may vary by model and software version. Router availability may also vary by region or ISP. All images, steps, and descriptions in this guide are only examples and may not reflect your actual router experience.

In this guide, unless otherwise specified, all screenshots are taken from M50-F.

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.

More information and support

Visit www.ip-com.com.cn and search for the product model to get your questions answered and get the latest documents.

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 manual was released.

Version	Date	Description
V1.1	2026-01-25	Added: Roaming optimization, External authentication, Custom NAT, USB application, LAN IP scan Updated: LAN settings, Wi-Fi advanced settings, Authentication templates, Authentication types, Group limit, Single user limit, Multi-WAN policy, SSH maintenance, VPN
V1.0	2024-10-31	Original publication.

Contents

1 Set up operating mode

Choose the appropriate mode according to the actual situation. M50-F working in Router mode is taken as an example.

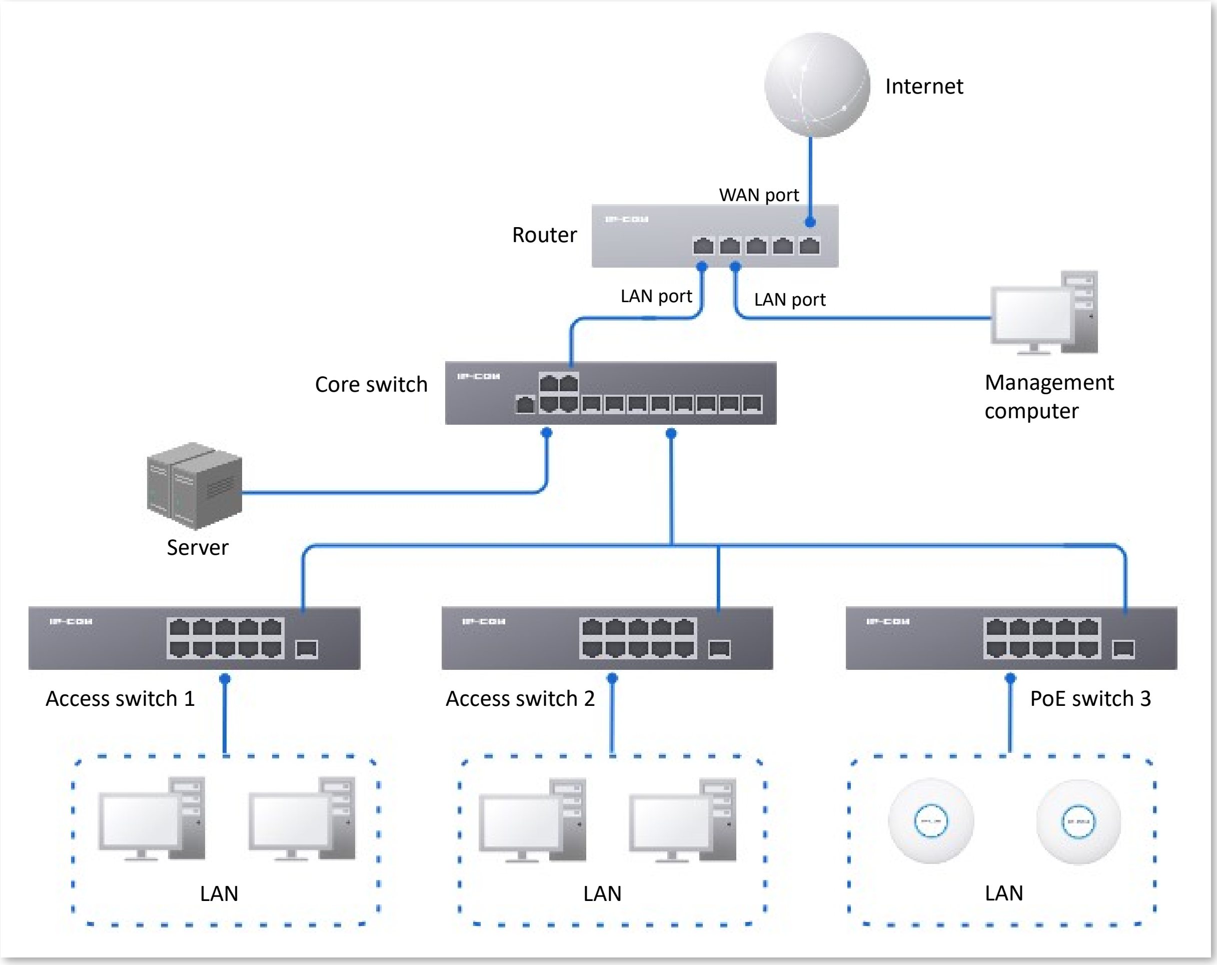
- Router Mode: The device is used as a router and wireless controller, providing internet access, routing forward, AP management, behavior & audit and other functions. In this mode, the device needs to process both control packets and data packets.
- Pure AC Mode: The device is used as a wireless controller to provide functions such as AP management, behavior & audit. 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

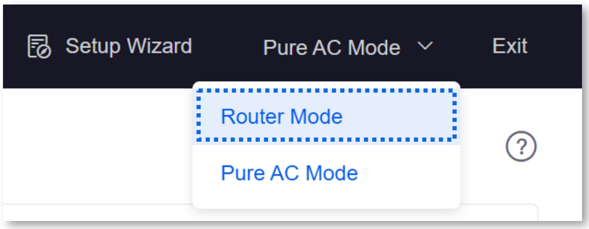
In Router mode, the device is used as a router and wireless controller, which is generally deployed at the egress gateway to proxy the LAN to access the internet.

The application scenario is as follows.

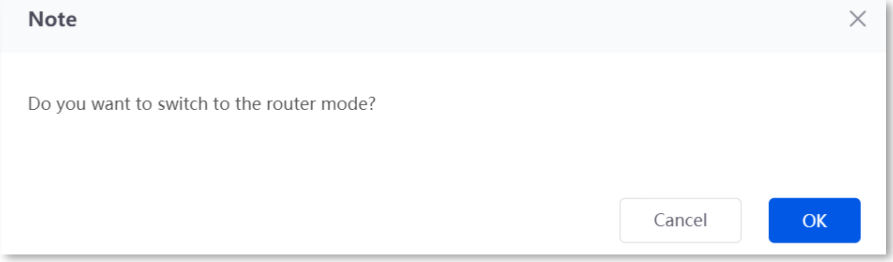


1.1.2 Set the router to Router mode

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**.



Note

Do you want to switch to the router mode?

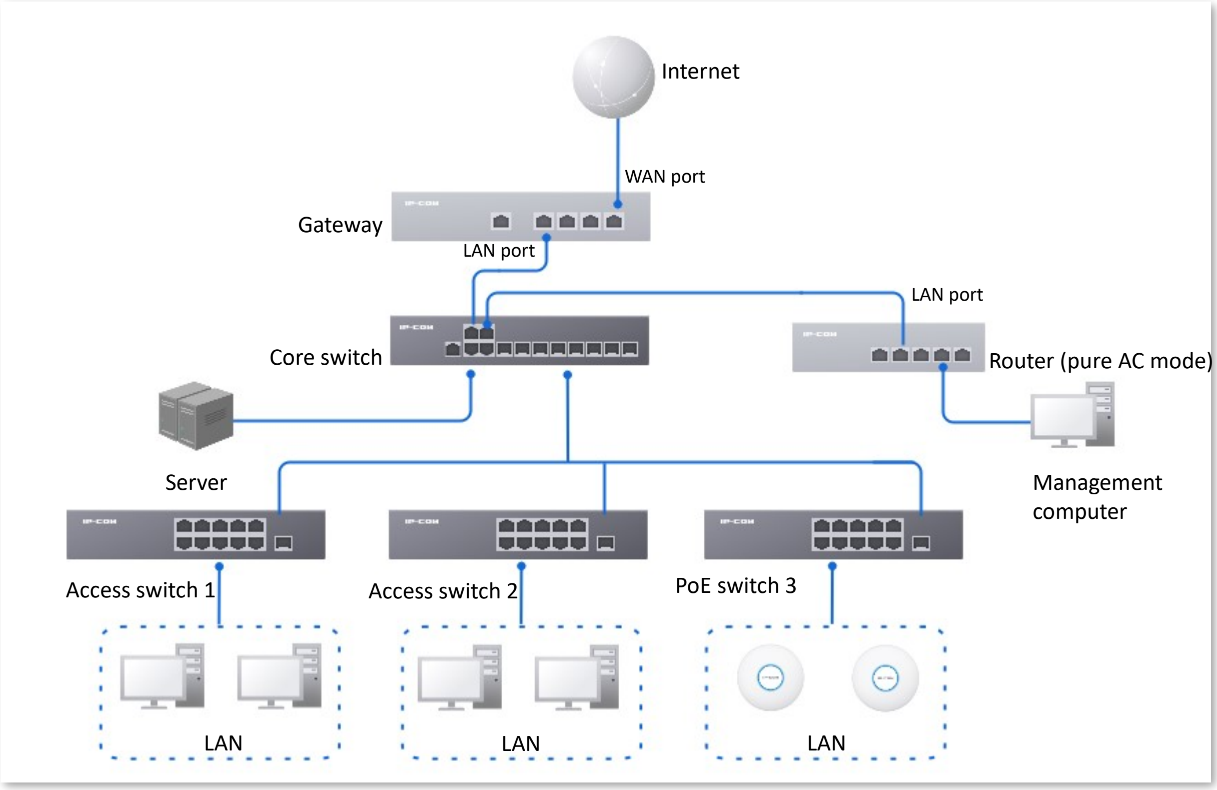
---End

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 scenario is as follows.

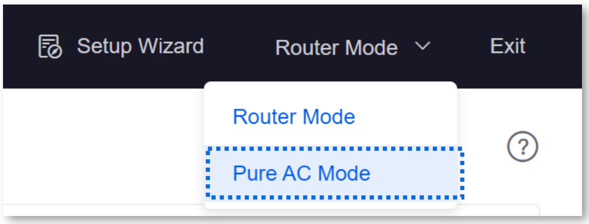


Tip

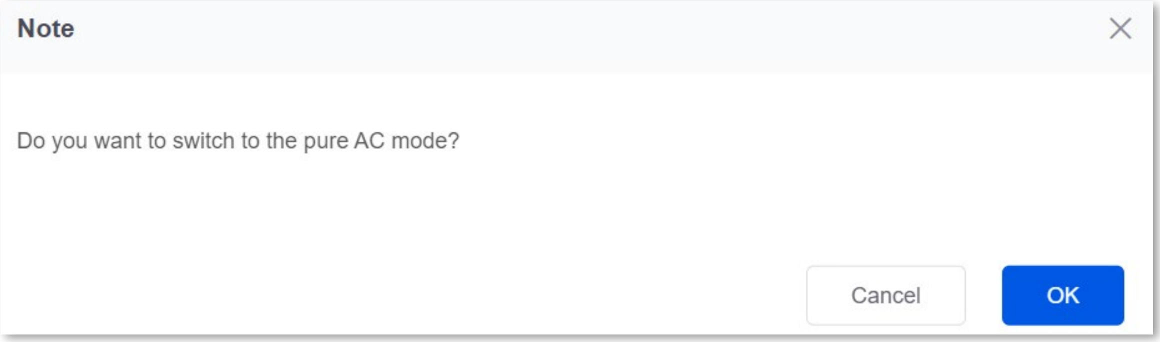
In Pure AC mode, if you want to use the remote web management, cloud maintenance, and SSH maintenance functions of the router, connect the router to the internet first. For details, refer to Connect the router in Pure AC mode.

1.2.2 Set the router to 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**.


Note

Do you want to switch to the pure AC mode?

---End

2 Access the router

2.1 Login

Upon your first use or reset of the router, you can set up the router by referring to the router's quick installation guide (visit www.ip-com.com.cn to download).

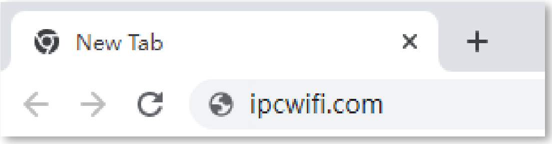
If you want to log in to the web UI of the router, follow the procedures below.

2.1.1 LAN login

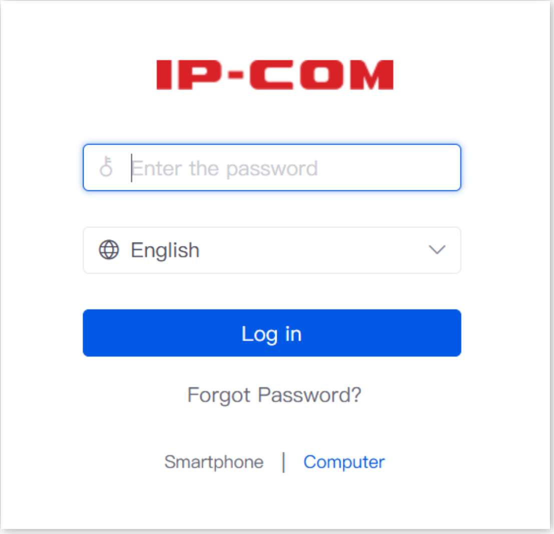
Log in to the web UI in Router mode

Via Computer

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 (such as Chrome) on your computer, and enter **ipcwifi.com** in the address bar to log in to the web UI.



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



---End

Tip

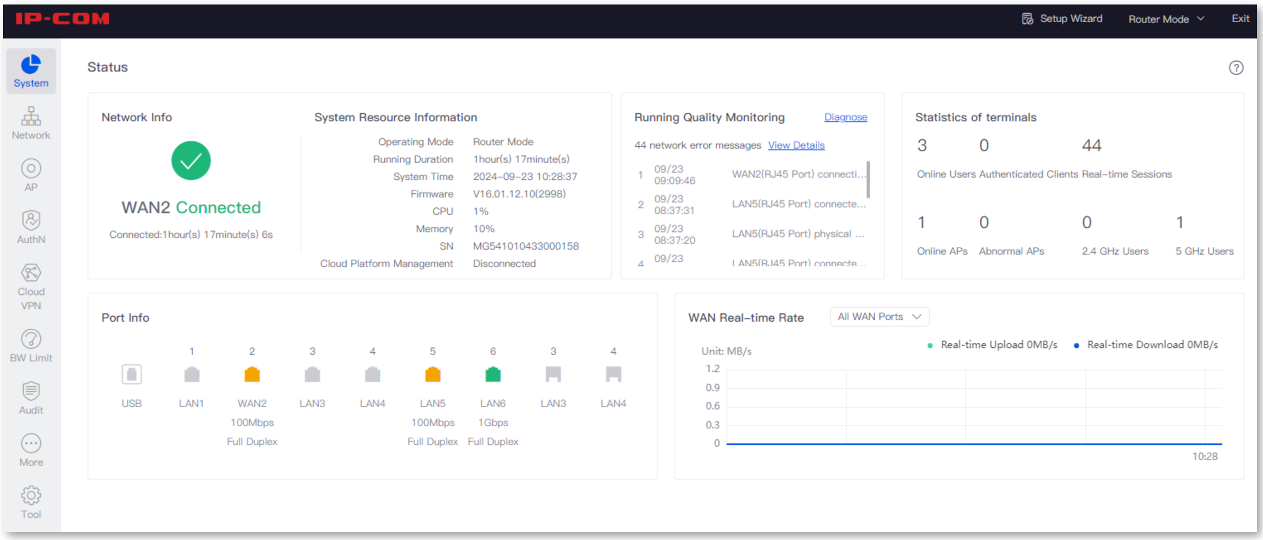
If the wrong password error is displayed on the page, you can:

Restore the router to factory settings, then set up a new password. Note that the router must be configured to connect to the internet again after restoration.

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

- Ensure that the Ethernet port of the router 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**.
- Ensure that you have entered **ipcwifi.com** or **192.168.0.252** in the browser address bar (not the search bar).
- Restore the router to factory settings and try again. Note that the router needs to be configured to connect to the internet again after the reset.

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



Status

Network Info

WAN2 Connected

Connected:1hour(s) 17minute(s) 6s

System Resource Information

Operating Mode	Router Mode
Running Duration	1hour(s) 17minute(s)
System Time	2024-09-23 10:28:37
Firmware	V16.01.12.10(2998)
CPU	1%
Memory	10%
SN	MG541010433000158
Cloud Platform Management	Disconnected

Running Quality Monitoring

44 network error messages

1	09/23 09:09:46	WAN2(RJ45 Port) connecti...
2	09/23 08:37:31	LAN5(RJ45 Port) connecte...
3	09/23 08:37:20	LAN5(RJ45 Port) physical ...
4	09/23	LAN5(RJ45 Port) connecte...

Statistics of terminals

Online Users	Authenticated Clients	Real-time Sessions	
3	0	44	
1	0	0	1
Online APs	Abnormal APs	2.4 GHz Users	5 GHz Users

Port Info

	1	2	3	4	5	6	3	4
USB	LAN1	WAN2 100Mbps Full Duplex	LAN3	LAN4	LAN5 100Mbps Full Duplex	LAN6 1Gbps Full Duplex	LAN3	LAN4

WAN Real-time Rate

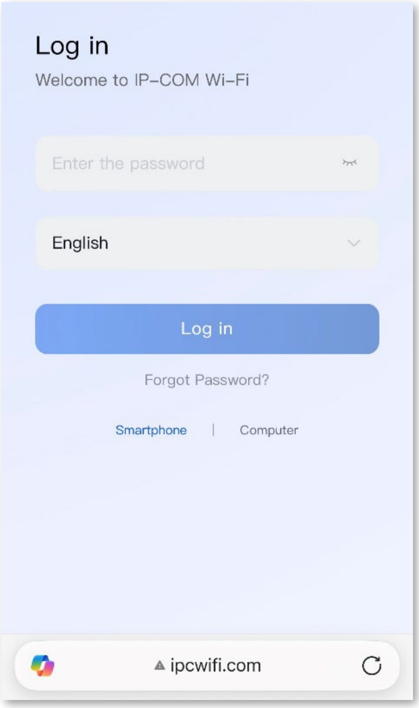
Unit: MB/s

● Real-time Upload 0MB/s ● Real-time Download 0MB/s

Via Wi-Fi Device (Example: Phone)

This option applies when you have an AP connected to the router in the local network.

1. Connect your phone to the AP's wireless network.
   - AP is managed by the router: The wireless name and password are the ones you set. If you haven't set up, the wireless network only has a default Wi-Fi name **IP-COM_*XXXXXX*** (XXXXXX is the last six digits of the MAC address on the label of the router).
   - AP is not managed by the router: The wireless name and password are the AP's original wireless name and password.
2. Start a browser on your phone, then enter **ipcwifi.com** in the address bar.
3. Enter the login password, then click **Log in**.



---End

Tip

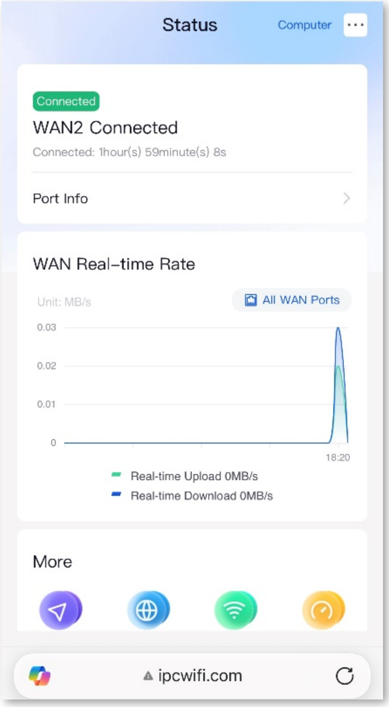
If the wrong password error is displayed on the page, you can:

Restore the router to factory settings, then set up a new password. Note that the router must be configured to connect to the internet again after the reset.

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

- Ensure the AP is working properly and your phone already connects to its Wi-Fi network.
- Disable your cellular data when accessing the router with your phone.
- Restore the router to factory settings and try again. Note that the router needs to be configured to connect to the internet again after the reset.

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



Status

Connected

WAN2 Connected

Connected: 1hour(s) 59minute(s) 8s

Port Info

WAN Real–time Rate

Unit: MB/s

Real-time Upload 0MB/s

Real-time Download 0MB/s

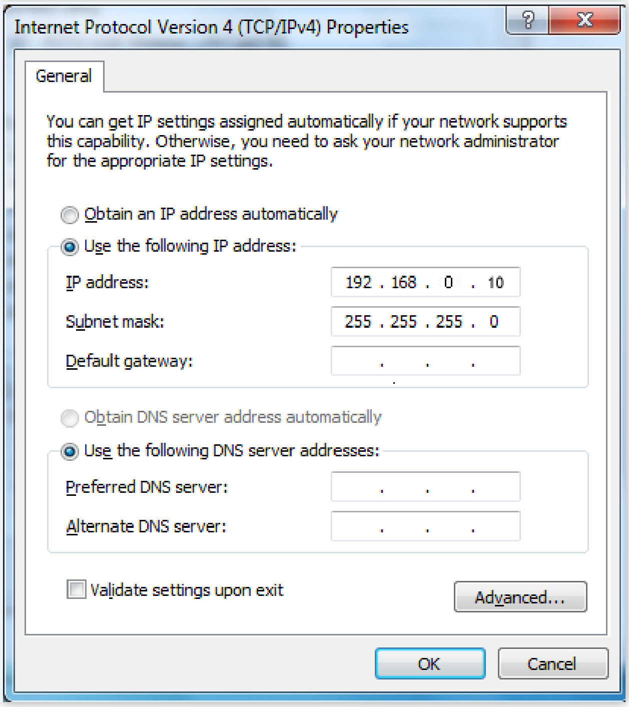
More

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 the same network segment as the router.

   For example, if the IP address of the router is **192.168.0.252**, 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**.



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 0 . 10

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

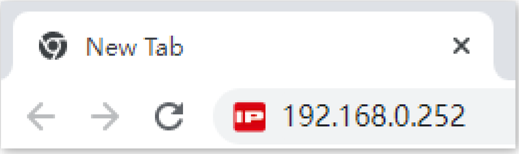
● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

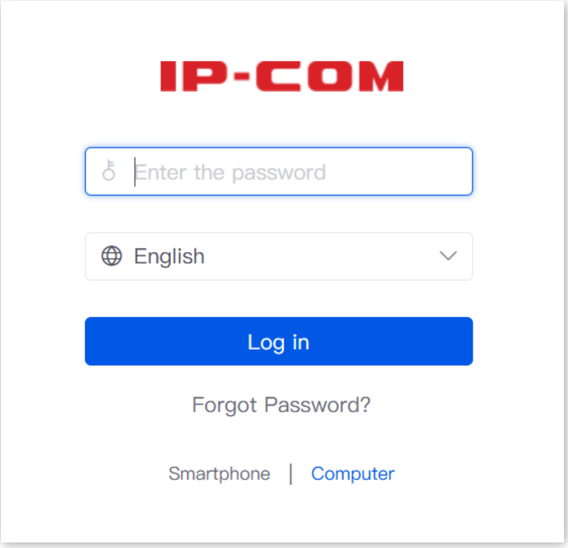
□ Validate settings upon exit

3. Start a browser on the computer, then enter the IP address (**192.168.0.252** by default) of the router.



192.168.0.252

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

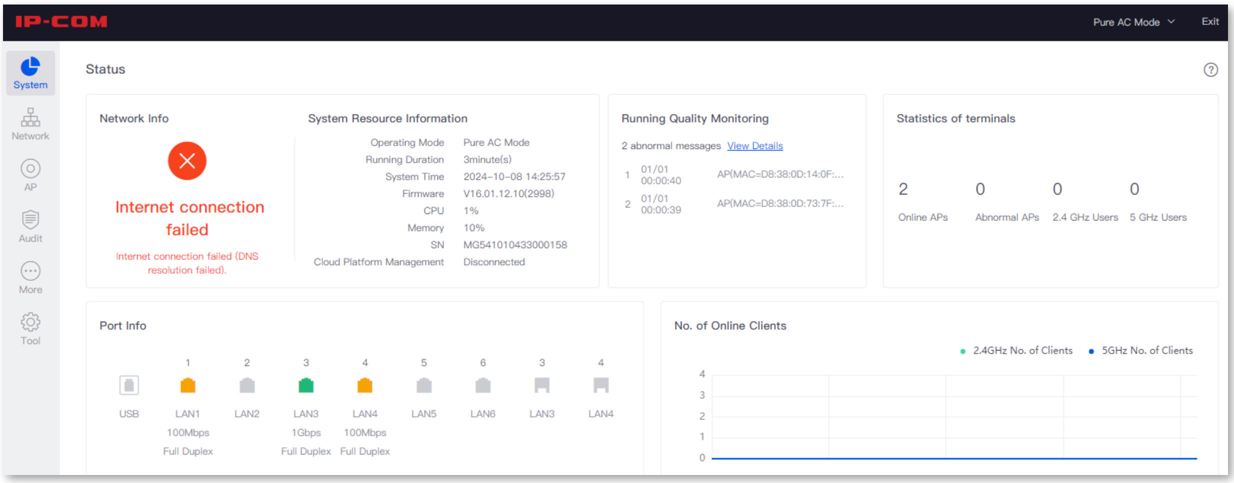


---End

Tip

If the above page does not appear, ensure that the Ethernet port of the router is connected to the computer properly.

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



Network Info

Internet connection failed

Internet connection failed (DNS resolution failed).

System Resource Information

Operating Mode	Pure AC Mode
Running Duration	3minute(s)
System Time	2024-10-08 14:25:57
Firmware	V16.01.12.10(2998)
CPU	1%
Memory	10%
SN	MG541010433000158
Cloud Platform Management	Disconnected

Running Quality Monitoring

2 abnormal messages View Details

1	01/01 00:00:40	AP(MAC=D8:38:0D:14:0F:...
2	01/01 00:00:39	AP(MAC=D8:38:0D:73:7F:...

Statistics of terminals

Online APs	Abnormal APs	2.4 GHz Users	5 GHz Users
2	0	0	0

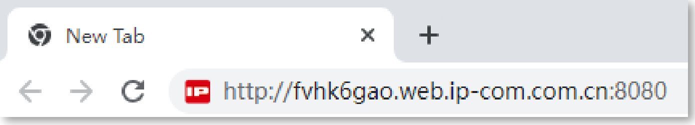
2.1.2 Remote login

The login mode is applicable when the router has connected to the internet and enabled the Remote Web Management function.

Tip

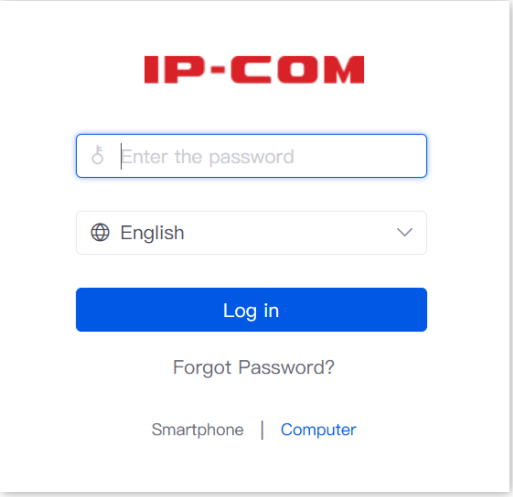
Before using this mode to log in, ensure that your client has been allowed to remotely access the router.

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



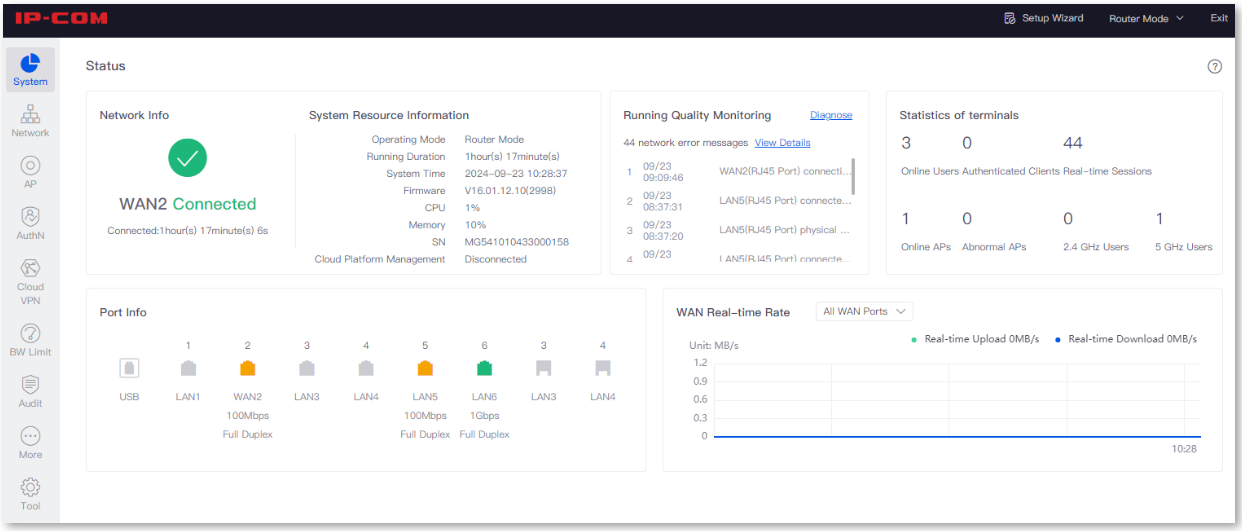
http://fvhk6gao.web.ip-com.com.cn:8080

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.



Status

Network Info

WAN2 Connected

Connected:1hour(s) 17minute(s) 6s

System Resource Information

Operating Mode	Router Mode
Running Duration	1hour(s) 17minute(s)
System Time	2024–09–23 10:28:37
Firmware	V16.01.12.10(2998)
CPU	1%
Memory	10%
SN	MG541010433000158
Cloud Platform Management	Disconnected

Running Quality Monitoring

44 network error messages

1	09/23 09:09:46	WAN2(RJ45 Port) connecti...
2	09/23 08:37:31	LAN5(RJ45 Port) connecte...
3	09/23 08:37:20	LAN5(RJ45 Port) physical ...
4	09/23	LAN5(RJ45 Port) connecte...

Statistics of terminals

Online Users	Authenticated Clients	Real–time Sessions	
3	0	44	

Online APs	Abnormal APs	2.4 GHz Users	5 GHz Users
1	0	0	1

Port Info

	1	2	3	4	5	6	3	4
USB	LAN1	WAN2 100Mbps Full Duplex	LAN3	LAN4	LAN5 100Mbps Full Duplex	LAN6 1Gbps Full Duplex	LAN3	LAN4

WAN Real–time Rate

Real–time Upload 0MB/s   Real–time Download 0MB/s

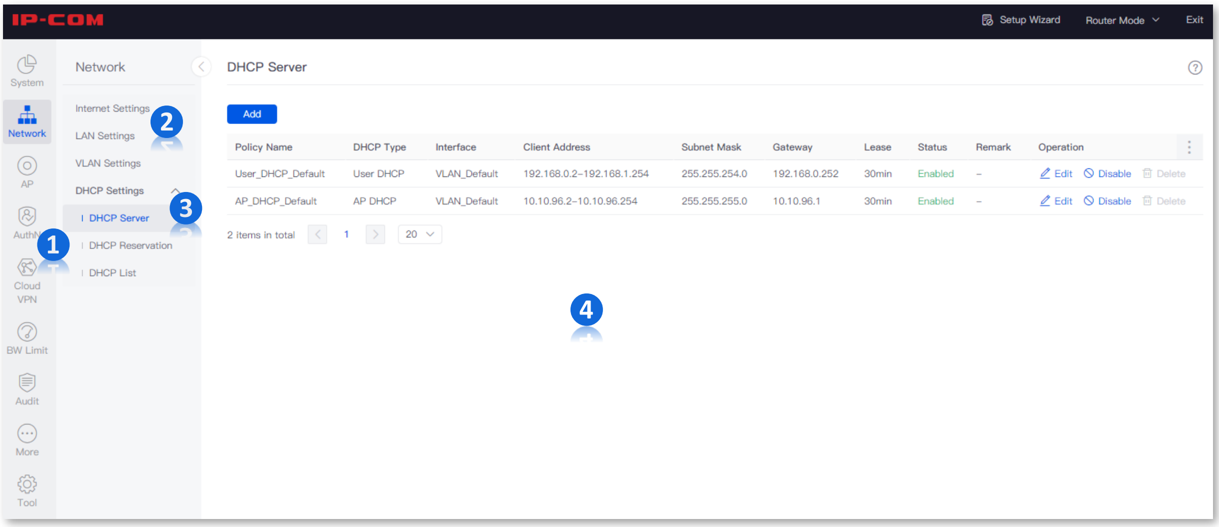
2.2 Logout

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

2.3 Web UI

2.3.1 Web layout

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



Policy Name	DHCP Type	Interface	Client Address	Subnet Mask	Gateway	Lease	Status	Remark	Operation
User_DHCP_Default	User DHCP	VLAN_Default	192.168.0.2–192.168.1.254	255.255.254.0	192.168.0.252	30min	Enabled	–	Edit Disable Delete
AP_DHCP_Default	AP DHCP	VLAN_Default	10.10.96.2–10.10.96.254	255.255.255.0	10.10.96.1	30min	Enabled	–	Edit Disable Delete

Tip

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

NO.	Name	Description
1	Level-1 navigation bar	Used to display menu items of the CPE in the form of a navigation tree that allows you to quickly access functions.
2	Level-2 navigation bar	
3	Level-3 navigation bar	
4	Configuration area	Used to view and modify the configuration.

2.3.2 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 the 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.

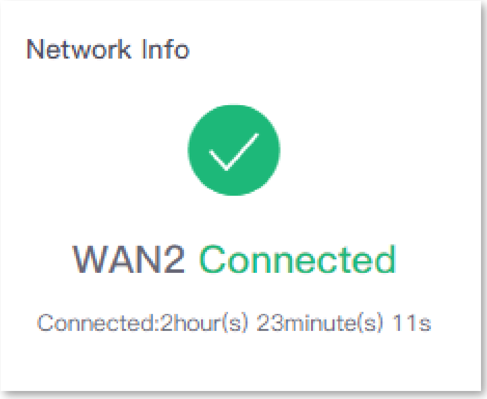
3 Monitor system status

Features available in the router may vary by model and software version. Router availability may also vary by region or ISP. All images, steps, and descriptions in this guide are only examples and may not reflect your actual router experience.

3.1 View network information

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

In the **Network Info** module, you can quickly view the WAN port network status and connection duration of the router. For details, refer to Check connection status.

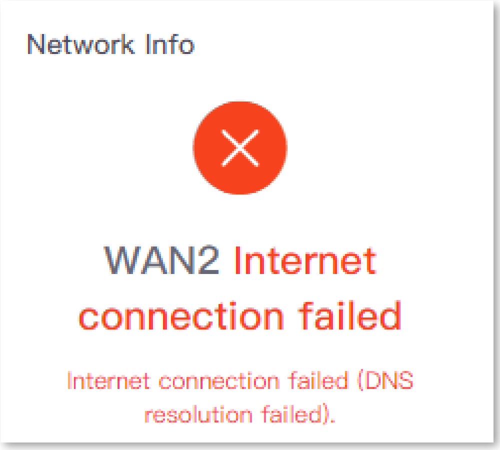


Network Info

WAN2 Connected

Connected:2hour(s) 23minute(s) 11s

If an error message is displayed, you can click ⊗ to redirect to the Internet Settings page and check it. The following figure is for reference only.



Network Info

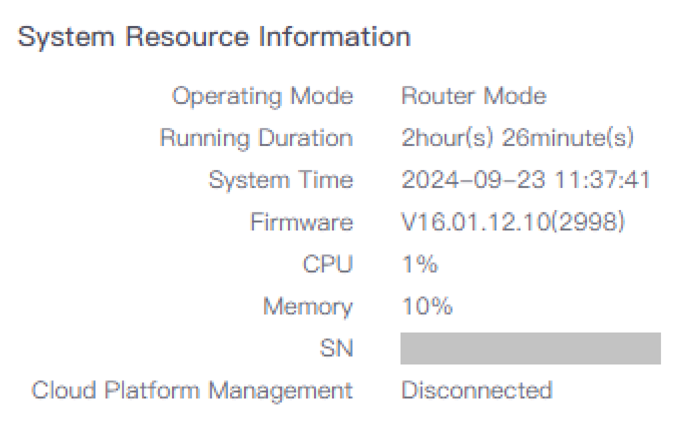
WAN2 Internet connection failed

Internet connection failed (DNS resolution failed).

3.2 View 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. The following figure is for reference only.



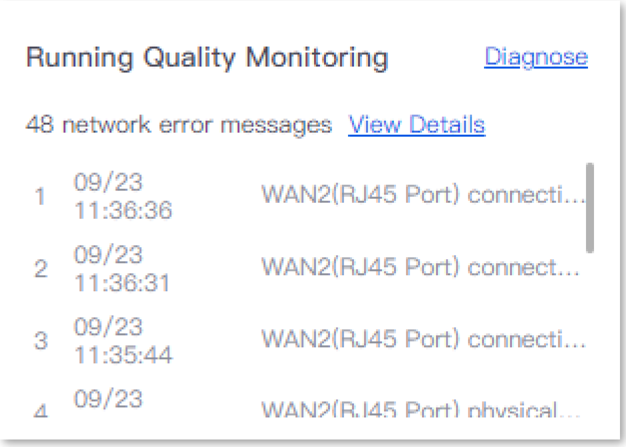
System Resource Information

Operating Mode	Router Mode
Running Duration	2hour(s) 26minute(s)
System Time	2024-09-23 11:37:41
Firmware	V16.01.12.10(2998)
CPU	1%
Memory	10%
SN	[redacted]
Cloud Platform Management	Disconnected

3.3 View running quality monitoring

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

In the **Running Quality Monitoring** module, you can view the error logs of the router. A maximum of 10 latest logs can be displayed. For details, click **View Details** to redirect to Network Monitoring Logs page; click **Diagnose** to redirect to Network Diagnosis page.



Running Quality Monitoring

48 network error messages View Details

1	09/23 11:36:36	WAN2(RJ45 Port) connecti...
2	09/23 11:36:31	WAN2(RJ45 Port) connect...
3	09/23 11:35:44	WAN2(RJ45 Port) connecti...
4	09/23	WAN2(RJ45 Port) physical...

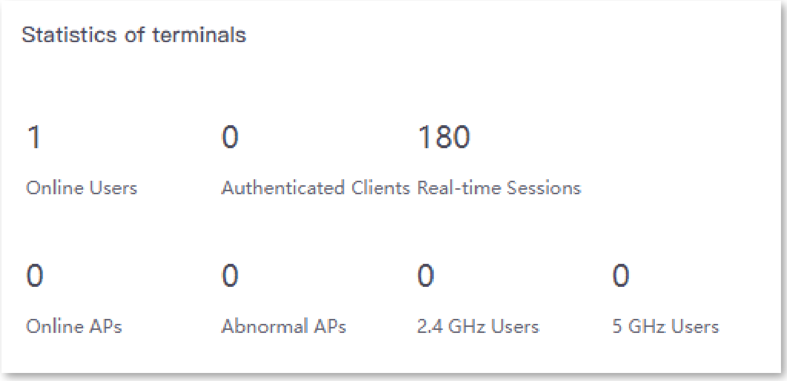
3.4 View statistics of terminals

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

In the **Statistics of terminals** module, you can view the statistics of terminals.

Router mode

In this mode, you can view the number of users and sessions connected to the router, the number of online and offline APs managed by the router, and the number of users currently connected to the 2.4 GHz and 5 GHz network.



Statistics of terminals

1 Online Users

0 Authenticated Clients

180 Real-time Sessions

0 Online APs

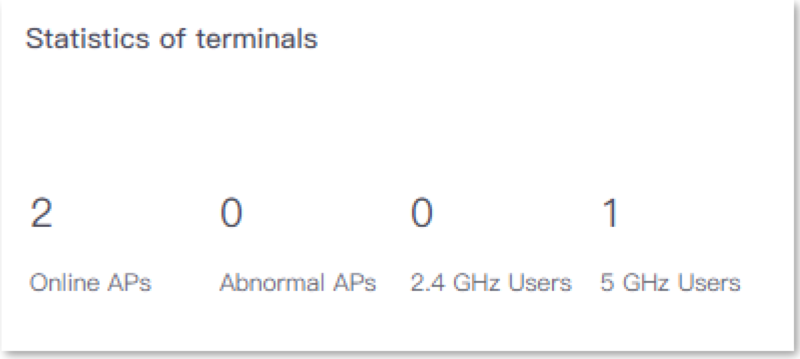
0 Abnormal APs

0 2.4 GHz Users

0 5 GHz Users

Pure AC mode

In this mode, you can view the number of online and offline APs managed by the router and the number of users currently connected to the 2.4 GHz and 5 GHz network.



Statistics of terminals

2 Online APs

0 Abnormal APs

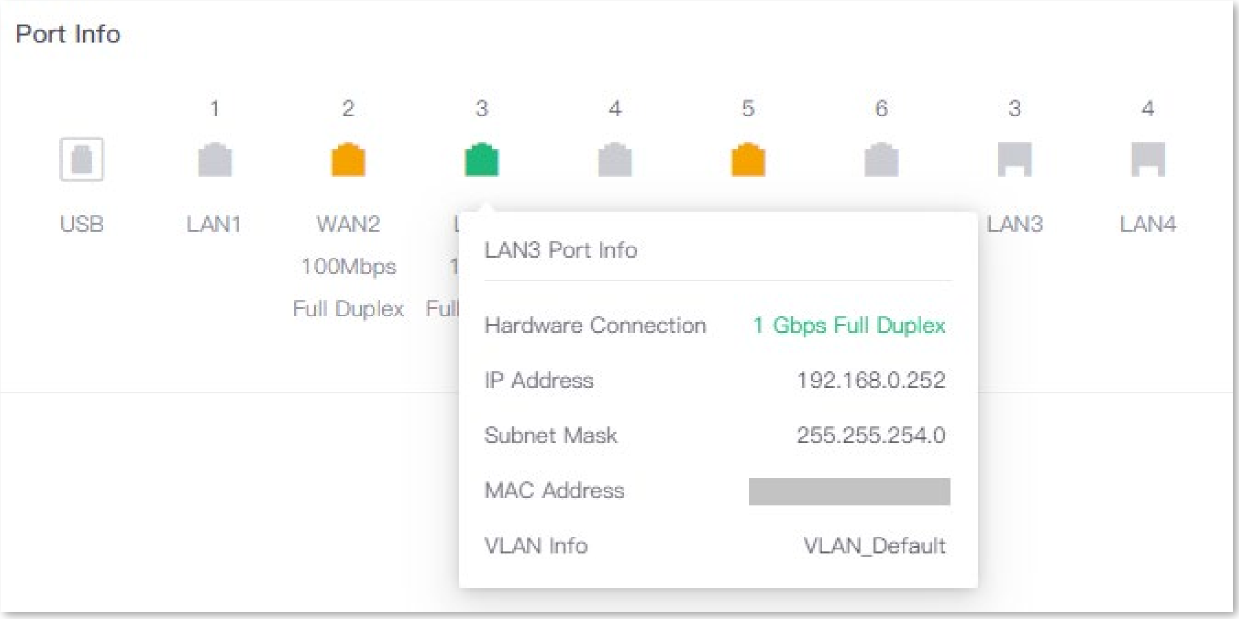
0 2.4 GHz Users

1 5 GHz Users

3.5 View port information

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

In the **Port Info** module, you can view the basic status of each port of the router. Hover the mouse over the port icon to view the physical connection status, IP address and other information of each port.



LAN3 Port Info

Hardware Connection 1 Gbps Full Duplex

IP Address 192.168.0.252

Subnet Mask 255.255.254.0

MAC Address [redacted]

VLAN Info VLAN_Default

Parameter description

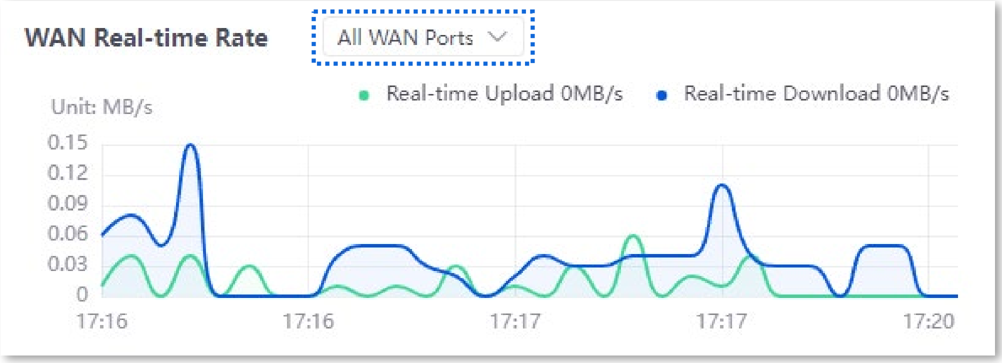
Parameter		Description
Ports		Specifies the roles and connection status of each port of the router. – Green means the port is connected at 1 Gbps or above. – Orange means the port is connected at 100 Mbps/10 Mbps. – Grey means the port is disconnected.
LAN Port Info	Hardware Connection	Specifies the connection status of the LAN port. – **Connection not detected** indicates that the Ethernet cable is not properly connected. – **Connected** indicates that the Ethernet cable is properly connected, and the speed and duplex mode negotiation is in progress.
	IP Address	Specifies the IPv4 address of the LAN port.
	Subnet Mask	Specifies the subnet mask of the LAN port.
	MAC Address	Specifies the MAC address of the LAN port.
	VLAN Info	Specifies the VLAN of the LAN port.
WAN Port Info		Specifies the connection status of the WAN port.

3.6 View 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.

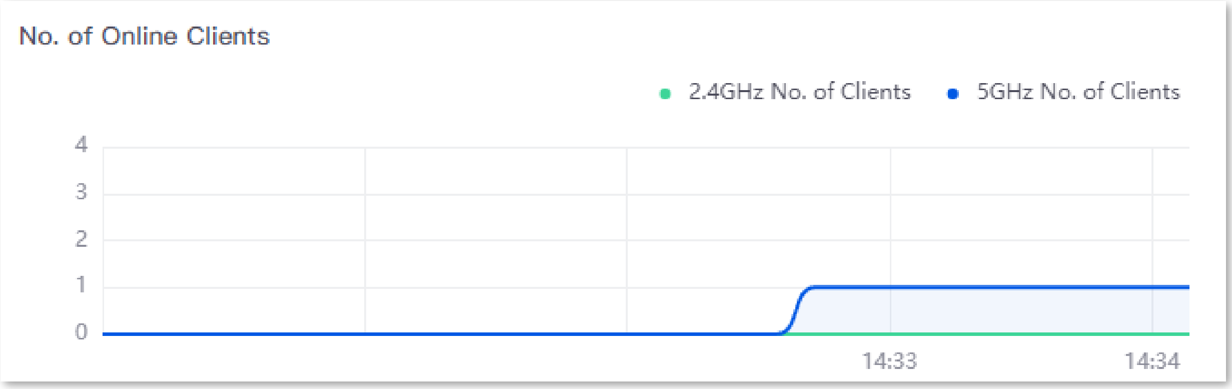
Click the drop-down box next to **WAN Real-time Rate** to select a certain WAN port of the router.



3.7 View online clients (Pure AC mode)

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

In the **No. of Online Clients** module, you can view the real-time changes in the number of users connected to the AP's 2.4 GHz and 5 GHz network.



4 Manage network settings

Features available in the router may vary by model and software version. Router availability may also vary by region or ISP. All images, steps, and descriptions in this guide are only examples and may not reflect your actual router experience.

4.1 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.

4.1.1 No. of WAN ports

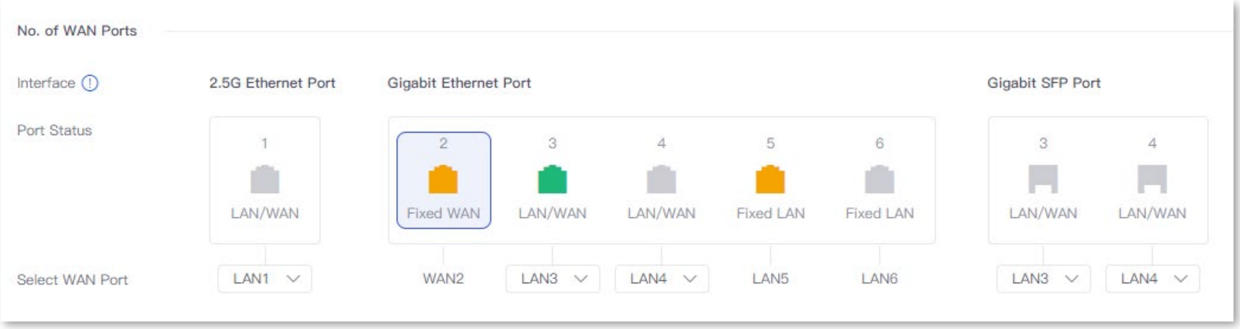
Log in to the web UI of the router, and navigate to **Network** > **Internet Settings** to enter the page.

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 is for reference only.

If the router supports SFP, the port type of SFP port is the same as the RJ45 port with the same number.

– If the RJ45 port with the same number is used after the connection of SFP port, the SFP port takes priority.

– If the SFP port with the same number is used within 30 seconds after the connection of RJ45 port, only the SFP port take priority. Otherwise, the RJ45 port takes priority.



No. of WAN Ports

Interface ⓘ	2.5G Ethernet Port	Gigabit Ethernet Port					Gigabit SFP Port	
Port Status	1 LAN/WAN	2 Fixed WAN	3 LAN/WAN	4 LAN/WAN	5 Fixed LAN	6 Fixed LAN	3 LAN/WAN	4 LAN/WAN
Select WAN Port	LAN1	WAN2	LAN3	LAN4	LAN5	LAN6	LAN3	LAN4

Parameter description

Parameter	Description
Interface	Specifies the interface type and the maximum negotiation rate.
Port Status	Specifies the port type and the connection status. – Green/Orange means the port is connected properly. – Grey means the port is disconnected.
Select WAN Port	Specifies the current type of port. You can change the port type as required.

4.1.2 Configure 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

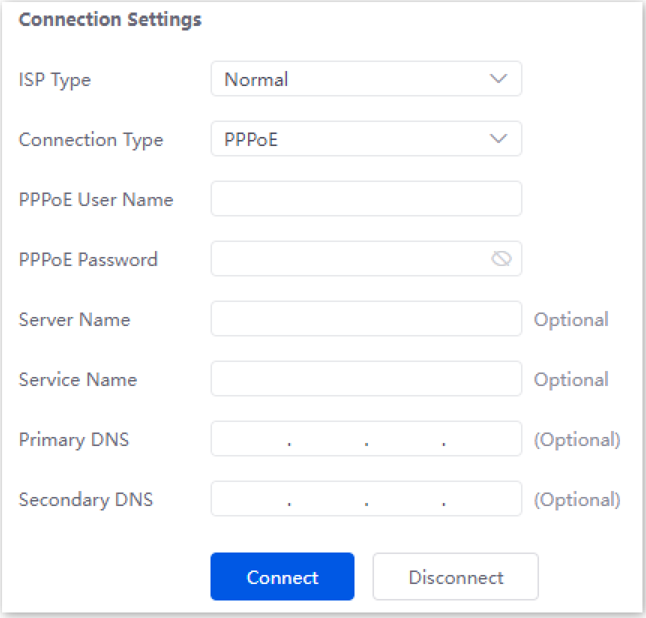
- The number of default WAN ports varies according to Router models. WAN2 is used as an example, and configurations for other WAN ports are similar.
- All internet parameters for accessing the internet are provided by your ISP. If you are not sure, contact your ISP for help.

PPPoE

If the ISP provides you with a PPPoE user name and password, you can choose this connection type to access the internet.

Configuration procedure

1. Log in to the web UI of the router, and navigate to **Network** > **Internet Settings.**
2. Set the **ISP Type**, which is **Normal** in this example.
3. Select **PPPoE** for **Connection Type**.
4. Enter the PPPoE user name and password provided by the ISP.
5. Click **Connect**.


Connection Settings

ISP Type: Normal

Connection Type: PPPoE

PPPoE User Name

PPPoE Password

Server Name — Optional

Service Name — Optional

Primary DNS — (Optional)

Secondary DNS — (Optional)

---End

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

Parameter description

Parameter	Description
ISP Type	Specifies the type of your ISP, such as **Normal**, **Russia**, **Unifi**, **Maxis** and **Manual**. Parameters required for each option may differ. Refer to the following to choose your connection type: – **Normal:** It specifies a common ISP type. Select this option by default. – **Unifi** and **Maxis**: Select these options when your ISP provides specific parameters such as Internet VLAN ID and IPTV VLAN ID. Internet VLAN ID and IPTV VLAN ID cannot be changed. – **Russia:** It is the access type provided by Russia. Select this option when your ISP provides dual access information. – **Manual**: Select this option when your ISP provides VLAN ID information. You can configure the Internet VLAN ID and IPTV VLAN ID as required. If you are not sure, contact your ISP for help.

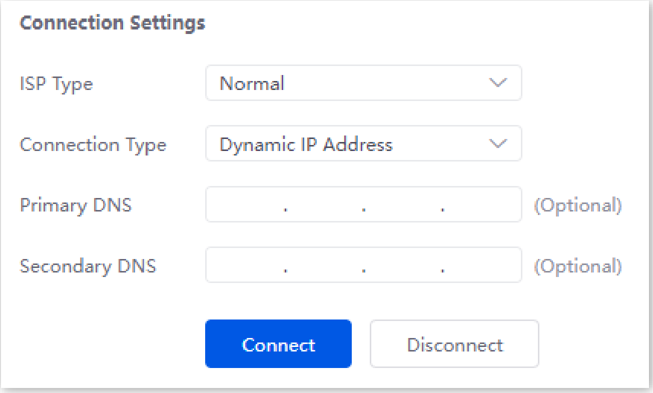
Parameter	Description
Connection Type	Specifies how your router connects to the internet, including: – **PPPoE**: Select this type if you access the internet using the PPPoE user name and PPPoE password. – **Dynamic IP Address**: Select this type if you can access the internet by simply plugging in an Ethernet cable. – **Static IP Address**: Select this type if you want to access the internet using fixed IP information. – **Russia PPPoE**, **Russia PPTP** and **Russia L2TP**: They are available only when you set **ISP Type** to **Russia**. The specific configuration is completed according to the requirements of the ISP. Tip Ports change based on the ISP type: – For **Unifi** or **Manual**, LAN6 changes to an PTV port. – For **Maxis**, all LAN ports that connect network devices support PTV services.
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 or secondary DNS servers. When the DNS server obtained automatically cannot resolve the URL normally, you can manually enter the correct primary or secondary DNS server here. The **Primary DNS** and **Secondary DNS** are optional.
Secondary DNS	

Dynamic IP address

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

Configuration procedure

1. Log in to the web UI of the router, and navigate to **Network** > **Internet Settings.**
2. Set the **ISP Type**, which is **Normal** in this example.
3. Select **Dynamic IP Address** for **Connection Type**.
4. Click **Connect**.



Connection Settings

ISP Type: Normal

Connection Type: Dynamic IP Address

Primary DNS: . . . (Optional)

Secondary DNS: . . . (Optional)

---End

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

Parameter description

Parameter	Description
ISP Type	Specifies the type of your ISP, such as **Normal**, **Russia**, **Unifi**, **Maxis** and **Manual**. Parameters required for each option may differ. Refer to the following to choose your connection type: – **Normal:** It specifies a common ISP type. Select this option by default. – **Unifi** and **Maxis**: Select these options when your ISP provides specific parameters such as Internet VLAN ID and IPTV VLAN ID. Internet VLAN ID and IPTV VLAN ID cannot be changed. – **Russia:** It is the access type provided by Russia. Select this option when your ISP provides dual access information. – **Manual**: Select this option when your ISP provides VLAN ID information. You can configure the Internet VLAN ID and IPTV VLAN ID as required. If you are not sure, contact your ISP for help.
Connection Type	Specifies how your router connects to the internet, including: – **PPPoE**: Select this type if you access the internet using the PPPoE user name and PPPoE password. – **Dynamic IP Address**: Select this type if you can access the internet by simply plugging in an Ethernet cable. – **Static IP Address**: Select this type if you want to access the internet using fixed IP information. – **Russia PPPoE**, **Russia PPTP** and **Russia L2TP**: Available only when you set **ISP Type** to **Russia**. The specific configuration is completed according to the requirements of the ISP.
Primary DNS	Manually enter primary or secondary DNS servers. When the DNS server obtained automatically cannot resolve the URL normally, you can manually enter the correct primary or secondary DNS server here. The **Primary DNS** and **Secondary DNS** are optional.
Secondary DNS	

Static IP address

If the ISP provides you with the fixed IP address, subnet mask, default gateway and DNS server information, you can choose this connection type to access the internet.

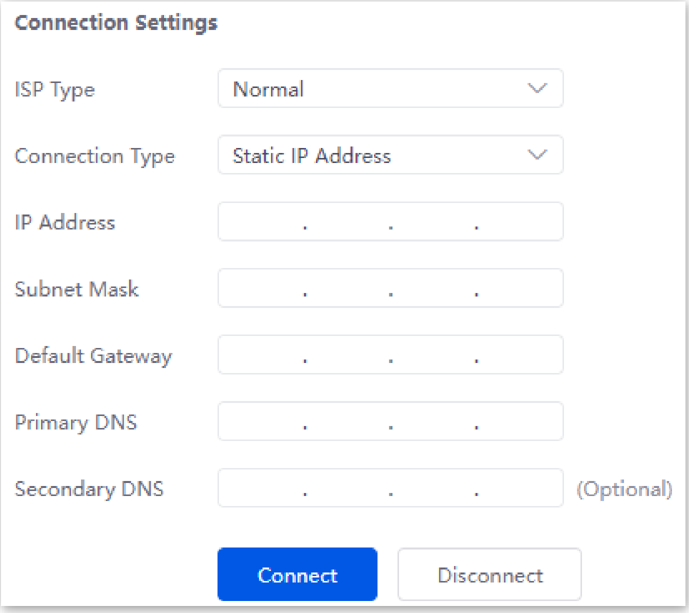
Configuration procedure

1. Log in to the web UI of the router, and navigate to **Network** > **Internet Settings.**
2. Set the **ISP Type**, which is **Normal** in this example.
3. Select **Static IP Address** for **Connection Type**.
4. 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, you can leave the **Secondary DNS** field blank.

5. Click **Connect**.



Connection Settings

ISP Type: Normal

Connection Type: Static IP Address

IP Address: . . .

Subnet Mask: . . .

Default Gateway: . . .

Primary DNS: . . .

Secondary DNS: . . . (Optional)

---End

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

Parameter description

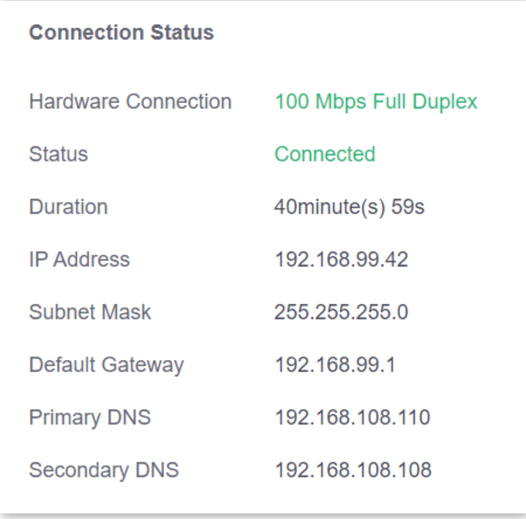
Parameter	Description
ISP Type	Specifies the type of your ISP, such as **Normal**, **Russia**, **Unifi**, **Maxis** and **Manual**. Parameters required for each option may differ. Refer to the following to choose your connection type: – **Normal:** It specifies a common ISP type. Select this option by default. – **Unifi** and **Maxis**: Select these options when your ISP provides specific parameters such as Internet VLAN ID and IPTV VLAN ID. Internet VLAN ID and IPTV VLAN ID cannot be changed. – **Russia:** It is the access type provided by Russia. Select this option when your ISP provides dual access information. – **Manual**: Select this option when your ISP provides VLAN ID information. You can configure the Internet VLAN ID and IPTV VLAN ID as required. If you are not sure, contact your ISP for help.

Parameter	Description
Connection Type	Specifies how your router connects to the internet, including: – **PPPoE**: Select this type if you access the internet using the PPPoE user name and PPPoE password. – **Dynamic IP Address**: Select this type if you can access the internet by simply plugging in an Ethernet cable. – **Static IP Address**: Select this type if you want to access the internet using fixed IP information. – **Russia PPPoE**, **Russia PPTP** and **Russia L2TP**: Available only when you set **ISP Type** to **Russia**. The specific configuration is completed according to the requirements of the ISP.

4.1.3 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 WAN port connection rate and duplex mode, connection status, duration and IP address. The following figure is for reference only.



Connection Status

Hardware Connection	100 Mbps Full Duplex
Status	Connected
Duration	40minute(s) 59s
IP Address	192.168.99.42
Subnet Mask	255.255.255.0
Default Gateway	192.168.99.1
Primary DNS	192.168.108.110
Secondary DNS	192.168.108.108

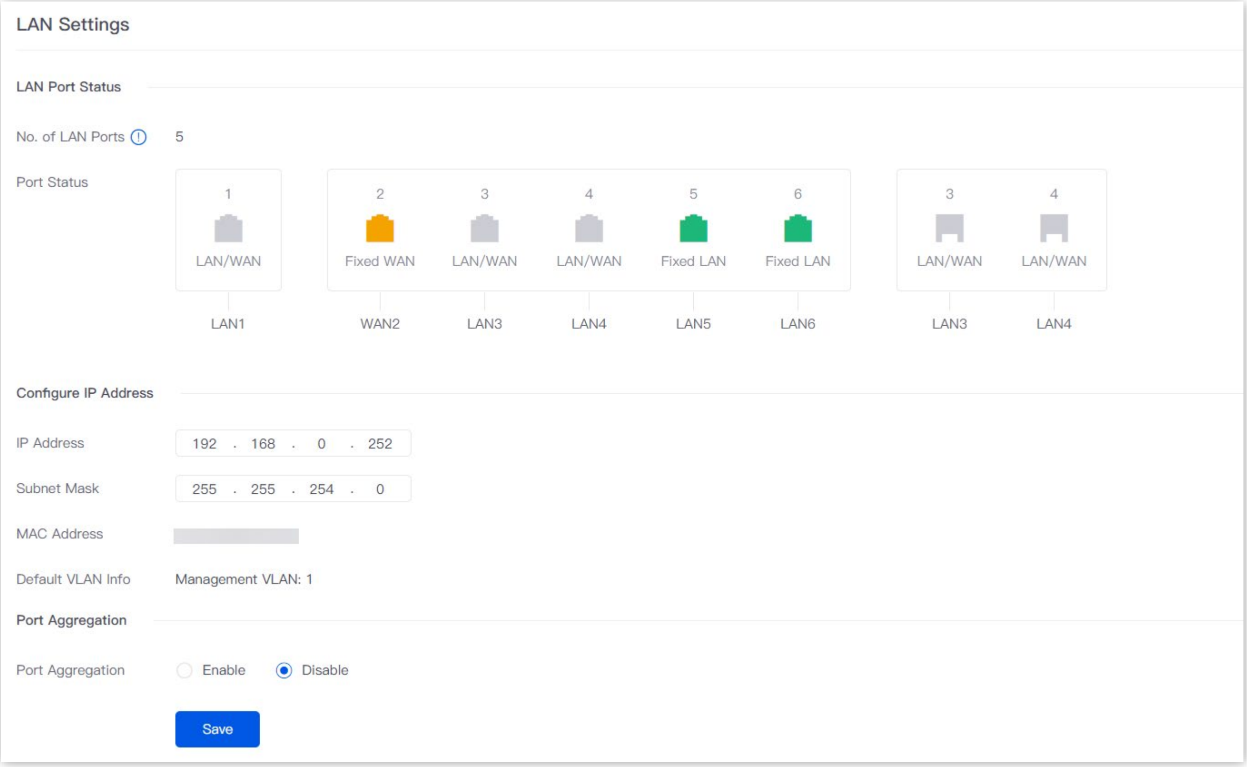
4.2 LAN settings

Port aggregation: Similar to link aggregation on a switch, it combines multiple physical ports into a single logical interface, thereby increasing overall bandwidth, providing link redundancy, and improving network reliability and performance.

- Dynamic aggregation: Uses the Link Aggregation Control Protocol (LACP) to automatically negotiate and manage aggregation groups. Devices exchange LACP packets to detect compatibility and select member ports. It is ideal for complex, high-performance networks that require high reliability and dynamic adaptation, such as large enterprises and cloud data centers.

- Static aggregation: Ports are manually configured into an aggregation group with no automatic negotiation. All port parameters (such as speed, duplex, and VLAN) must match. This mode is best suited for stable, low-change environments such as small business or home networks.

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, specify the IPv4 address of the router's **VLAN_Default**, and configure port aggregation.



LAN Settings

LAN Port Status

No. of LAN Ports ⓘ 5

Port Status

Configure IP Address

IP Address 192 . 168 . 0 . 252

Subnet Mask 255 . 255 . 254 . 0

MAC Address

Default VLAN Info Management VLAN: 1

Port Aggregation

Port Aggregation ○ Enable ● Disable

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. – Green/Orange means the port is connected properly. – Grey means the port is disconnected.

Parameter		Description
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 You need to disable the network adapter of the computer first and then enable the network adapter to obtain the IP address again.
	Subnet Mask	Specifies the subnet mask of the VLAN_Default.
	MAC Address	Specifies the MAC address of the VLAN_Default.
	Default VLAN Info	Specifies the VLAN ID of the VLAN_Default of the router.
Port Aggregation	Interface	After port aggregation is enabled, an aggregation interface is created as AGG1.
	Mode	Specifies the aggregation mode. – **Static**: Administrators need to manually specify the member port on the router and the aggregation port on the peer device to form an aggregation group. – **Dynamic**: The member port specified by the administrator automatically negotiates aggregation groups with the peer device according to the LACP protocol.
	Algorithm	Specifies how to distribute traffic over the aggregation interface. – **Source and Destination MAC**: This algorithm combines source and destination MAC addresses. During data transmission, it considers both the source and destination MAC addresses of the data frame to determine which port in the aggregation group to forward the data frame to. – **Source and Destination IP**: This algorithm combines source and destination IP addresses. During data transmission, it considers both the source and destination IP addresses of the data frame to determine which port in the aggregation group to forward the data frame to. – **Source and Destination MAC-IP-Port**: This algorithm combines five parameters (source MAC, destination MAC, source IP, destination IP, and port number) to accurately allocate data. However, it also places high demands on system performance and may lead to a decrease in device performance.
	MAC Address	After member ports are aggregated as a logical interface, a new MAC address is generated. You can make changes as necessary.
	Member Ports	Specifies RJ45 ports or SFP ports as members of the aggregation interface. All port parameters (such as type, speed and duplex) must match.

Parameter	Description
Rate	Specifies the rate of the aggregation interface AGG1.

4.3 VLAN settings

4.3.1 Overview

VLAN, abbreviated for Virtual Local Area Network, is a technology that divides LAN devices into different network segments logically rather than physically to create virtual work groups. It is used to divide the workstations in the switch-formed network into logical groups among which the broadcast is isolated. Workstations in a group belong to the same VLAN and can communicate like they are connected to the 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.

This router supports 802.1Q VLAN and can communicate with devices that support 802.1Q VLAN in VLAN as well. 802.1Q VLAN is defined by IEEE 802.1q protocol. With 802.1Q VLAN, the router can process packets by identifying the tags in packets.

This router supports two 802.1Q VLAN port types:

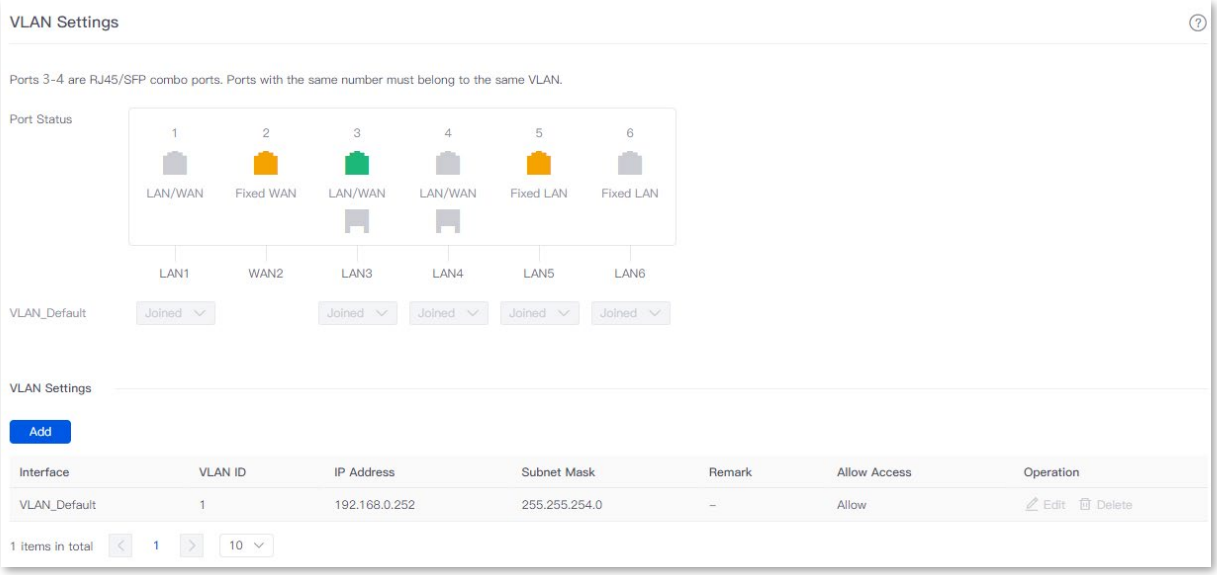
- Access: An access port can join only one VLAN. This type of port is used for connecting the computer.
- Trunk: A trunk port can receive and send packets belonging to multiple VLANs. This type of port is used for connection between switches.

Methods of each port type to process packets are shown as follows.

Port type	Receiving tagged data	Receiving untagged data	Sending data
Access port	Forward data to the ports with VLANs assigned based on the VLAN ID	Forward data to the ports with VLANs assigned based on the PVID	Strip the tag from the packet and then forward it
Trunk port			VLAN ID = PVID of the port, strip the tag from the packet and then forward it VLAN ID ≠ PVID of the port, retain the tag in the packet and then forward it

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.


VLAN Settings

Ports 3-4 are RJ45/SFP combo ports. Ports with the same number must belong to the same VLAN.

VLAN_Default: LAN1 Joined, LAN3 Joined, LAN4 Joined, LAN5 Joined, LAN6 Joined

VLAN Settings

Add

Interface	VLAN ID	IP Address	Subnet Mask	Remark	Allow Access	Operation
VLAN_Default	1	192.168.0.252	255.255.254.0	–	Allow	Edit Delete

1 items in total < 1 > 10

Parameter description

Parameter	Description
Port Status	Specifies the connection status of the port. – Green/Orange means the port is connected properly. – Grey means the port is disconnected.
VLAN Setting	By default, the router has created a VLAN named VLAN_Default, and adds all ports to that VLAN. You can click **Add** to add a new VLAN policy, and select ports to join this VLAN as needed. – Not Join: Forbid the port to join the VLAN to send or receive packets with VLAN ID. – TAG: Allow the port to join multiple VLANs as a trunk port with PVID=1. A trunk port is used for connection between router and switch, or router and AP. For details about packet processing, refer to Methods of each port type to process packets. – UNTAG: Allow the port to join only one VLAN as an access port. An access port is used for connecting the computer. For details about packet processing, refer to Methods of each port type to process packets. Tip If a port contains both tagged and untagged VLANs, it works as a trunk port and uses the VLAN ID of the untagged VLAN as PVID.

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. Tip – If the VLAN ID is 1, it means that there is no VLAN information, and only data without Tag is processed. – All ports within the aggregation group have the same VLAN ID.
IP Address	Specifies the VLAN IP address. Devices connecting to the port can log in to the web UI of the router using the IP address.
Subnet Mask	Specifies the subnet mask 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 the services of this VLAN.

4.3.2 Example of allowing single VLAN on the router

Networking requirements

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

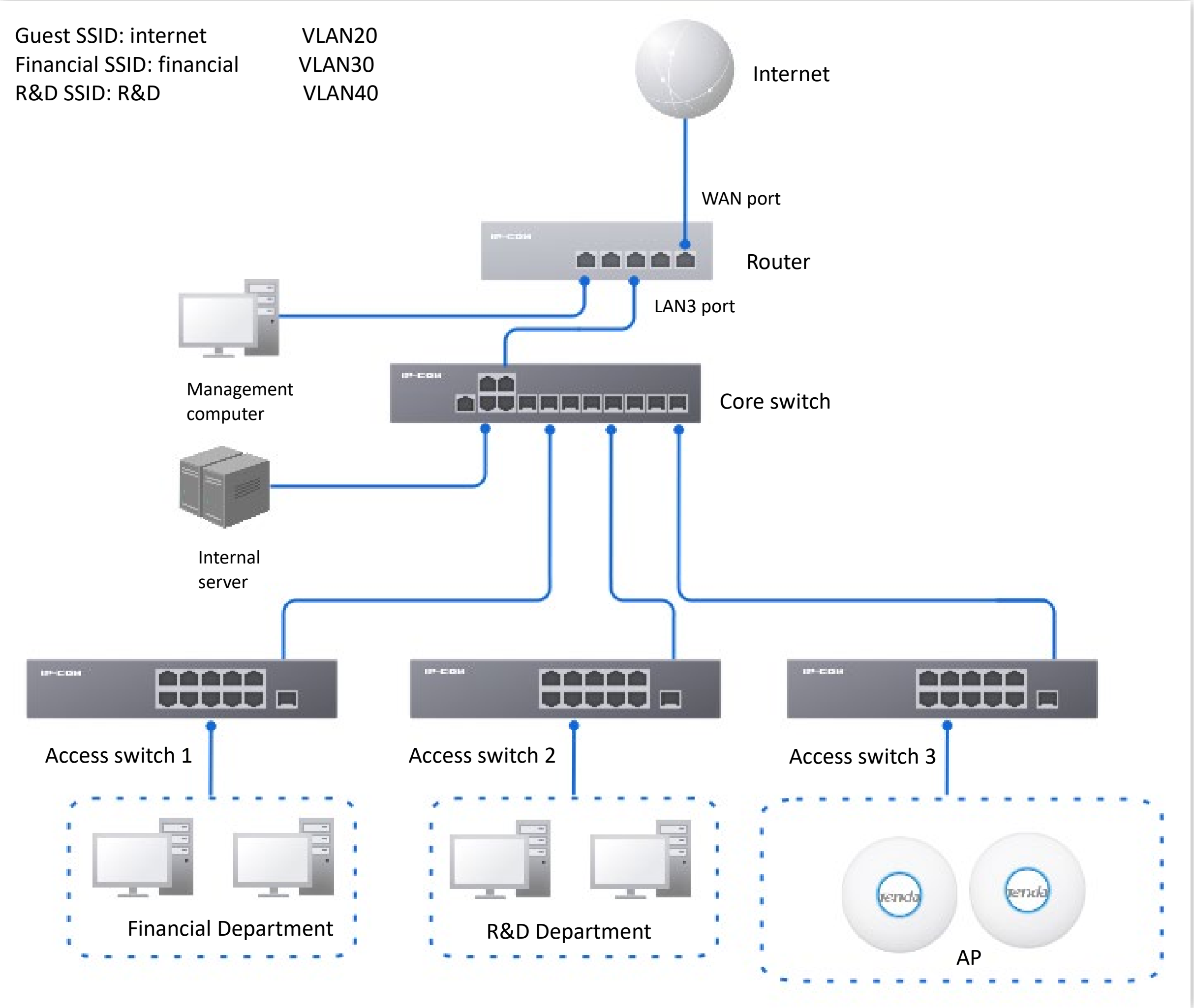
- Guests, departments and staff are required to access networks that are isolated from each other and have different network permissions.
- Guests can only access the internet via wireless connection.
- Staff of the Financial Department can only access the intranet via both wired and wireless connections.
- Staff of the R&D Department can only access the intranet via both wired and wireless connections.

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 application scenario is as follows.



Configuration procedure

Configure the router → Configure the core switch → Configure the internal server

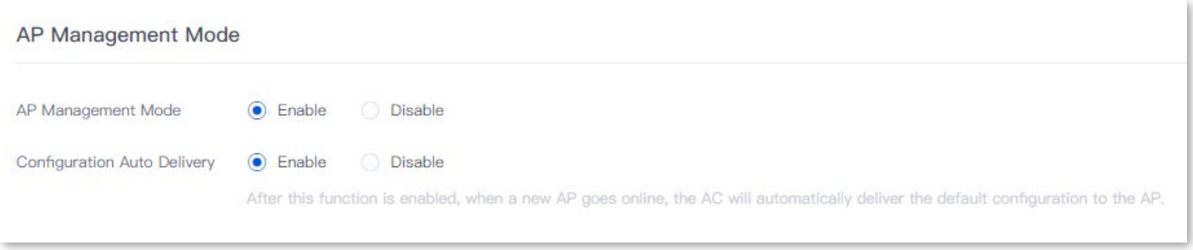
I. Configure the router

1. [Log in to the web UI of the router.]()

2. Manage the AP (skip if done).

   1) Navigate to **AP** > **AP Management Mode**.

   2) Enable the **AP Management Mode** and **Configuration Auto Delivery** function.



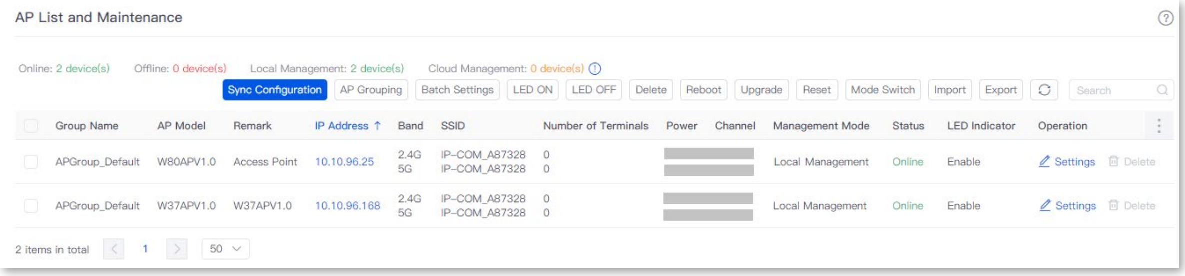
AP Management Mode

AP Management Mode ● Enable ○ Disable

Configuration Auto Delivery ● Enable ○ Disable

After this function is enabled, when a new AP goes online, the AC will automatically deliver the default configuration to the AP.

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



AP List and Maintenance

Online: 2 device(s) Offline: 0 device(s) Local Management: 2 device(s) Cloud Management: 0 device(s)

□	Group Name	AP Model	Remark	IP Address ↑	Band	SSID	Number of Terminals	Power	Channel	Management Mode	Status	LED Indicator	Operation
□	APGroup_Default	W80APV1.0	Access Point	10.10.96.25	2.4G 5G	IP-COM_A87328 IP-COM_A87328	0 0	[redacted]	[redacted]	Local Management	Online	Enable	Settings Delete
□	APGroup_Default	W37APV1.0	W37APV1.0	10.10.96.168	2.4G 5G	IP-COM_A87328 IP-COM_A87328	0 0	[redacted]	[redacted]	Local Management	Online	Enable	Settings Delete

2 items in total < 1 > 50

3. Add the VLAN and configure the DHCP server.

   Examples of VLAN parameters are shown below.

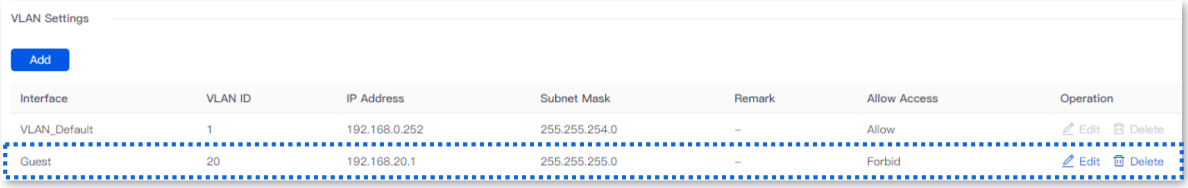
Interface	VLAN ID	IP Address/Subnet·Mask	Allow Access	Physical Port
Guest	20	192.168.20.1/24	Forbid	LAN3 (TAG)

Examples of DHCP server parameters for the VLAN are shown below.

Policy Name	Application Interface	DHCP Type	DHCP Configuration
Guest	[Guest]()	User DHCP	IP Address Pool: 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.

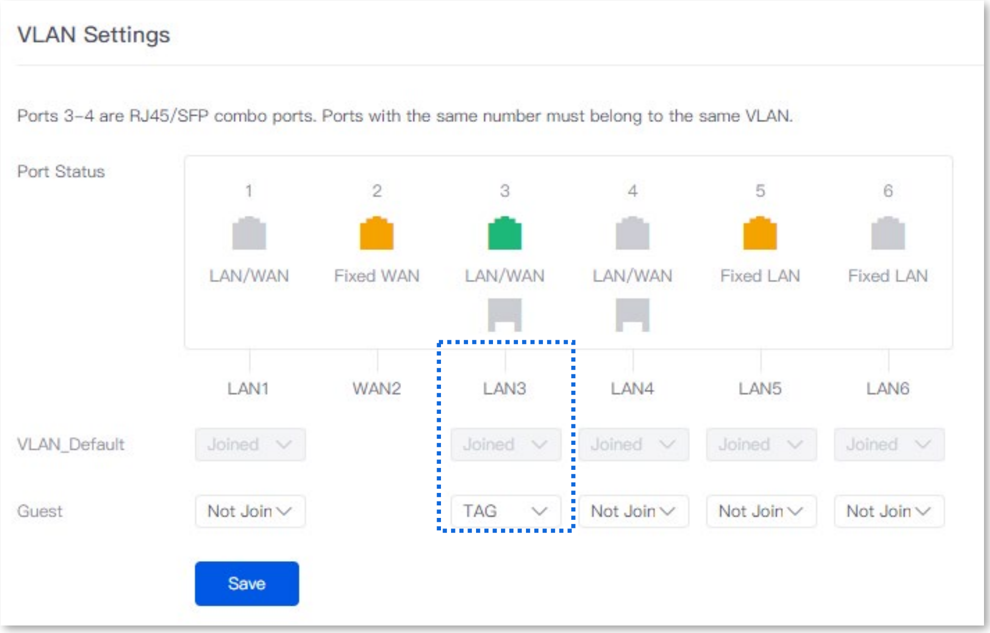
   – Navigate to **Network** > **VLAN Settings,** click **Add** to configure related parameters of the VLAN, and click **Save**.



VLAN Settings

Interface	VLAN ID	IP Address	Subnet Mask	Remark	Allow Access	Operation
VLAN_Default	1	192.168.0.252	255.255.254.0	–	Allow	Edit Delete
Guest	20	192.168.20.1	255.255.255.0	–	Forbid	Edit Delete

– Select LAN port for the **Guest** VLAN, which is **LAN3** in this example, set VLAN policy to **TAG**. Then click **Save**.



VLAN Settings

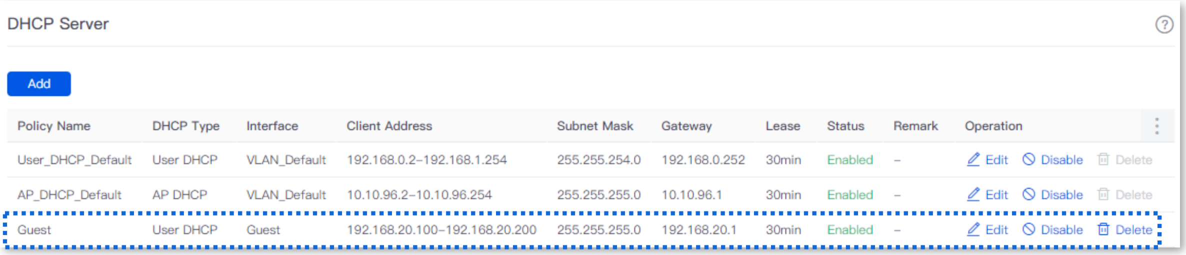
Ports 3–4 are RJ45/SFP combo ports. Ports with the same number must belong to the same VLAN.

Port Status

	LAN1	WAN2	LAN3	LAN4	LAN5	LAN6
VLAN_Default	Joined		Joined	Joined	Joined	Joined
Guest	Not Join		TAG	Not Join	Not Join	Not Join

2) Configure the DHCP server for the VLAN.

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



DHCP Server

Policy Name	DHCP Type	Interface	Client Address	Subnet Mask	Gateway	Lease	Status	Remark	Operation
User_DHCP_Default	User DHCP	VLAN_Default	192.168.0.2–192.168.1.254	255.255.254.0	192.168.0.252	30min	Enabled	–	Edit Disable Delete
AP_DHCP_Default	AP DHCP	VLAN_Default	10.10.96.2–10.10.96.254	255.255.255.0	10.10.96.1	30min	Enabled	–	Edit Disable Delete
Guest	User DHCP	Guest	192.168.20.100–192.168.20.200	255.255.255.0	192.168.20.1	30min	Enabled	–	Edit Disable Delete

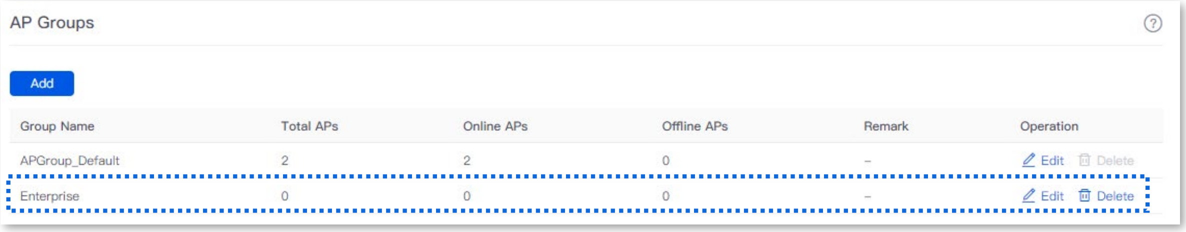
4. Configure the AP policy.

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

AP Group	Wi-Fi	AP VLAN
Enterprise	AP Grouping: Enterprise SSID: internet Security Mode: WPA2-PSK Wi-Fi Password: UmXmL9UK VLAN ID: 20 Maximum Number of Clients: 40	AP Grouping: Enterprise AP VLAN: Enable Trunk port: LAN0
	AP Grouping: Enterprise SSID: Financial Security Mode: WPA2-PSK Wi-Fi Password: CetTLb8T VLAN ID: 30 Maximum Number of Clients: 40	
	AP Grouping: Enterprise SSID: R&D Security Mode: WPA2-PSK Wi-Fi Password: ZeFtub6m VLAN ID: 40 Maximum Number of Clients: 40	

1) Configure the AP Group policy.

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



AP Groups

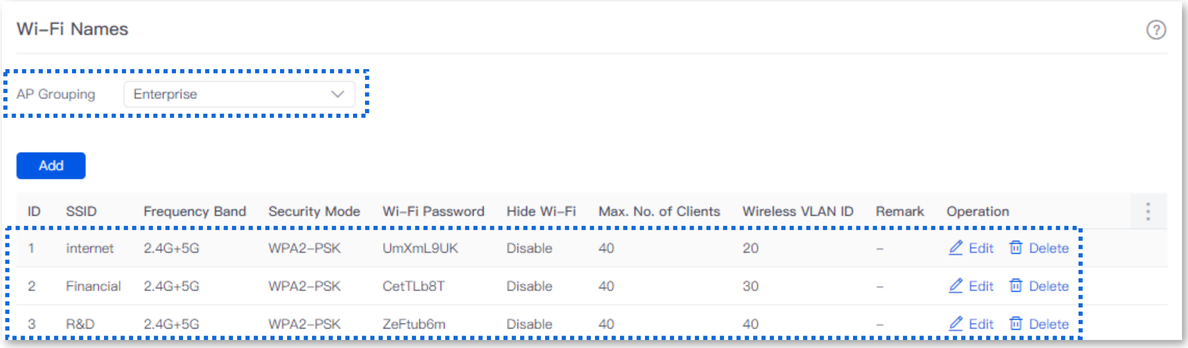
Group Name	Total APs	Online APs	Offline APs	Remark	Operation
APGroup_Default	2	2	0	–	Edit Delete
Enterprise	0	0	0	–	Edit Delete

2) Configure the Wi-Fi policy.

Navigate to **AP** > **Wi-Fi Settings** > **Wi-Fi Names**, select **Enterprise** for **AP Grouping**. Click **Add** to configure related parameters of the Wi-Fi policy, and click **Save**.

Tip

The maximum number of clients supported by the AP is 128. If multiple SSID policies need to be delivered to the same AP, you should plan the maximum number of clients appropriately to ensure that the maximum number of clients for each SSID policy does not exceed 128.



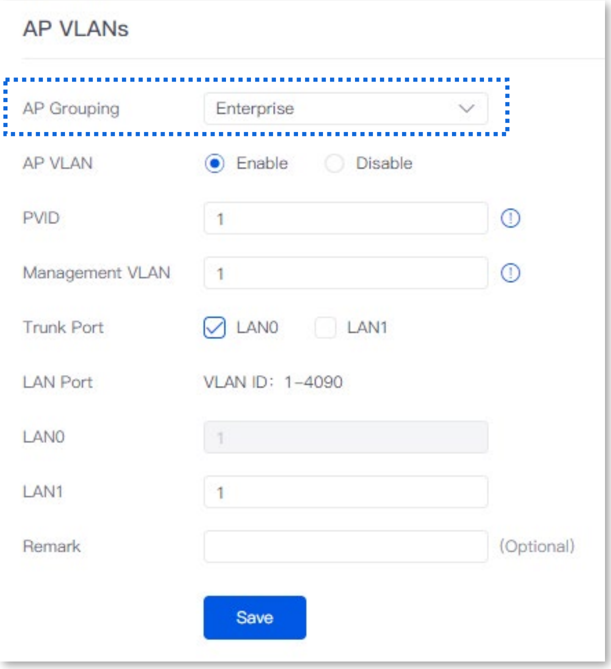
Wi-Fi Names

AP Grouping: Enterprise

ID	SSID	Frequency Band	Security Mode	Wi-Fi Password	Hide Wi-Fi	Max. No. of Clients	Wireless VLAN ID	Remark	Operation
1	internet	2.4G+5G	WPA2-PSK	UmXmL9UK	Disable	40	20	–	Edit Delete
2	Financial	2.4G+5G	WPA2-PSK	CetTLb8T	Disable	40	30	–	Edit Delete
3	R&D	2.4G+5G	WPA2-PSK	ZeFtub6m	Disable	40	40	–	Edit Delete

3) Configure VLAN policy.

Navigate to **AP** > **Wi-Fi Settings** > **AP VLANs**, select **Enterprise** for **AP Grouping**. Enable the **AP VLAN** function and set **Trunk Port** to **LAN0**, and click **Save**.



AP VLANs

AP Grouping: Enterprise

AP VLAN: ● Enable ○ Disable

PVID: 1

Management VLAN: 1

Trunk Port: ☑ LAN0 □ LAN1

LAN Port: VLAN ID: 1–4090

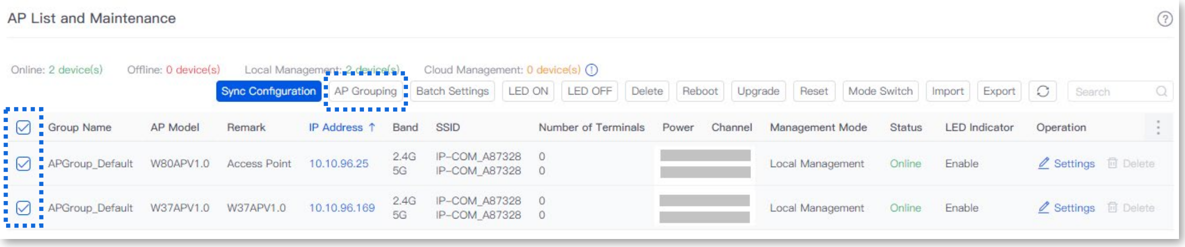
LAN0: 1

LAN1: 1

Remark: (Optional)

5. Deliver the AP group policy.

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

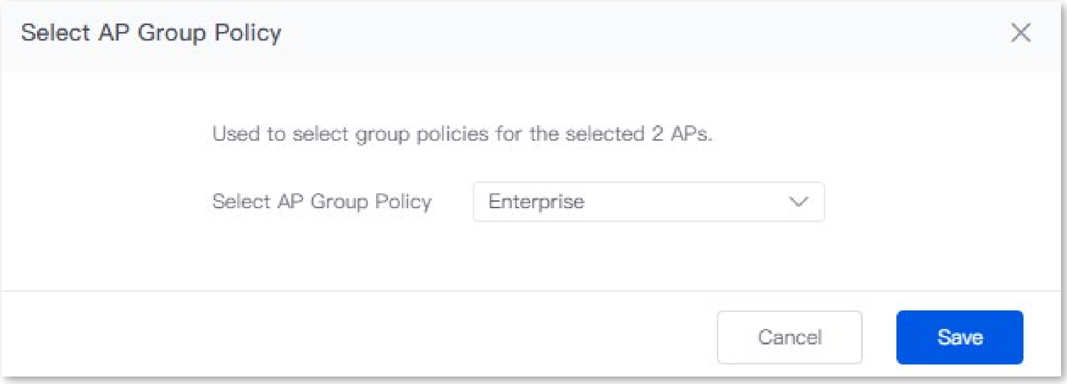


AP List and Maintenance

Online: 2 device(s) Offline: 0 device(s) Local Management: 2 device(s) Cloud Management: 0 device(s)

☑	Group Name	AP Model	Remark	IP Address ↑	Band	SSID	Number of Terminals	Power	Channel	Management Mode	Status	LED Indicator	Operation
☑	APGroup_Default	W80APV1.0	Access Point	10.10.96.25	2.4G 5G	IP-COM_A87328 IP-COM_A87328	0 0	[redacted]	[redacted]	Local Management	Online	Enable	Settings Delete
☑	APGroup_Default	W37APV1.0	W37APV1.0	10.10.96.169	2.4G 5G	IP-COM_A87328 IP-COM_A87328	0 0	[redacted]	[redacted]	Local Management	Online	Enable	Settings Delete

2) Select the AP group policy, and click **Save.** The following figure is for reference only.



Select AP Group Policy

Used to select group policies for the selected 2 APs.

Select AP Group Policy: Enterprise

II. Configure the core switch

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

Port Connected to	VLAN ID (VLAN Allowed)	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 core 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/Subnet·Mask	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 - 192.168.30.200 Subnet Mask: 255.255.255.0 Gateway: 192.168.30.1 Primary DNS: 192.168.30.1

Policy Name	User DHCP
R&D	Client Address: 192.168.40.100 - 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 core switch.

Port Connected to	VLAN ID（VLAN Allowed to Pass）	Port Property	PVID
Core 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.

4.3.3 Example of allowing multiple VLANs on the router

Networking requirements

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

- Guests, 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 via wireless connection.
- Staff of the Sales Department can only access the internet via both wired and wireless connections.
- Staff of the R&D Department can only access the intranet via both wired and wireless connections.
- To facilitate management, assign the management computer, second floor APs and third floor APs into different VLANs.

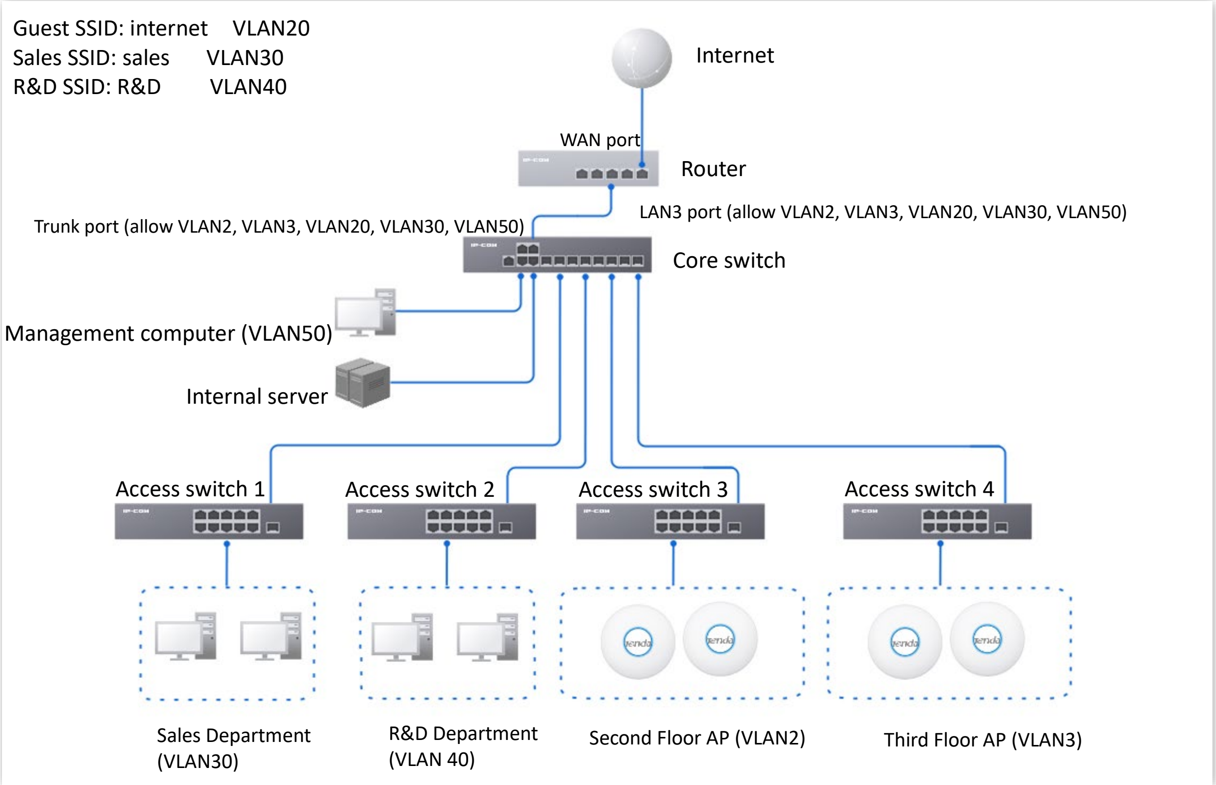
Solution

- 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 Sales Department. The SSID is **Sales**. 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 Sales Department into **VLAN30**.
- Divide the wired network connected by the staff of the R&D Department into **VLAN40**.
- Divide the APs on the second floor into **VLAN2**, and the APs on the third floor into **VLAN3**.
- Divide the management computer into **VLAN50**.
- Configure VLAN forwarding rules on the core switch.
- Configure VLAN forwarding rules on the router and the internal server.

Assume that the information between the ports of the managed switch and other devices is as follows:

Port Connected to	VLAN ID (VLAN Allowed)	Port Property
Router	2,3,20,30,50	Trunk
Management Computer	50	Access
Internal Server	40	Access
Switch1	30	Access
Switch2	40	Access
Switch3, 4	20,30,40	Trunk

The application scenario is as follows.



Configuration procedure

Configure the router → Configure the core switch → Configure the internal server

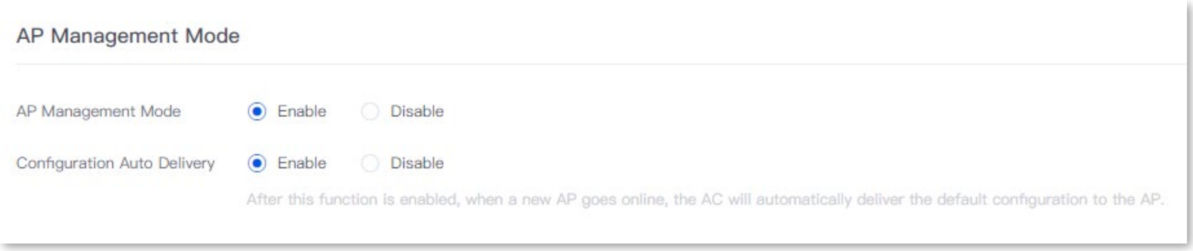
I. Configure the router

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

2. (Skip if done) Manage the AP.

   1) Navigate to **AP** > **AP Management Mode**.

   2) Enable the **AP Management Mode** and **Configuration Auto Delivery** function.



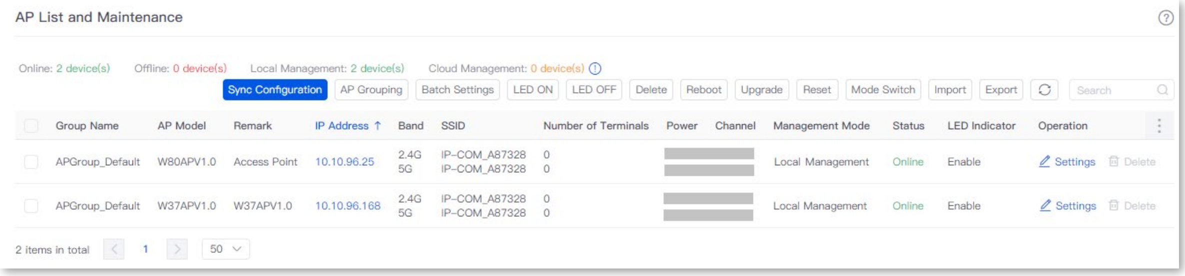
AP Management Mode

AP Management Mode ● Enable ○ Disable

Configuration Auto Delivery ● Enable ○ Disable

After this function is enabled, when a new AP goes online, the AC will automatically deliver the default configuration to the AP.

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



AP List and Maintenance

Online: 2 device(s) Offline: 0 device(s) Local Management: 2 device(s) Cloud Management: 0 device(s)

Group Name	AP Model	Remark	IP Address ↑	Band	SSID	Number of Terminals	Power	Channel	Management Mode	Status	LED Indicator	Operation
APGroup_Default	W80APV1.0	Access Point	10.10.96.25	2.4G 5G	IP-COM_A87328 IP-COM_A87328	0 0	[redacted]	[redacted]	Local Management	Online	Enable	Settings Delete
APGroup_Default	W37APV1.0	W37APV1.0	10.10.96.168	2.4G 5G	IP-COM_A87328 IP-COM_A87328	0 0	[redacted]	[redacted]	Local Management	Online	Enable	Settings Delete

2 items in total 1 50

3. Add the VLAN and configure the DHCP server.

   Examples of VLAN parameters are shown below.

Interface	VLAN ID	IP Address/Subnet·Mask	Allow Access	Physical Port
Guest	20	192.168.20.1/24	Forbid	LAN3 (TAG)
Sales Department	30	192.168.30.1/24	Forbid	LAN3 (TAG)
Management Computer	50	192.168.50.1/24	Forbid	LAN3 (TAG)
Second Floor AP	2	192.168.2.1/24	Forbid	LAN3 (TAG)
Third Floor AP	3	192.168.3.1/24	Forbid	LAN3 (TAG)

Examples of User DHCP server parameters for the VLAN are shown below.

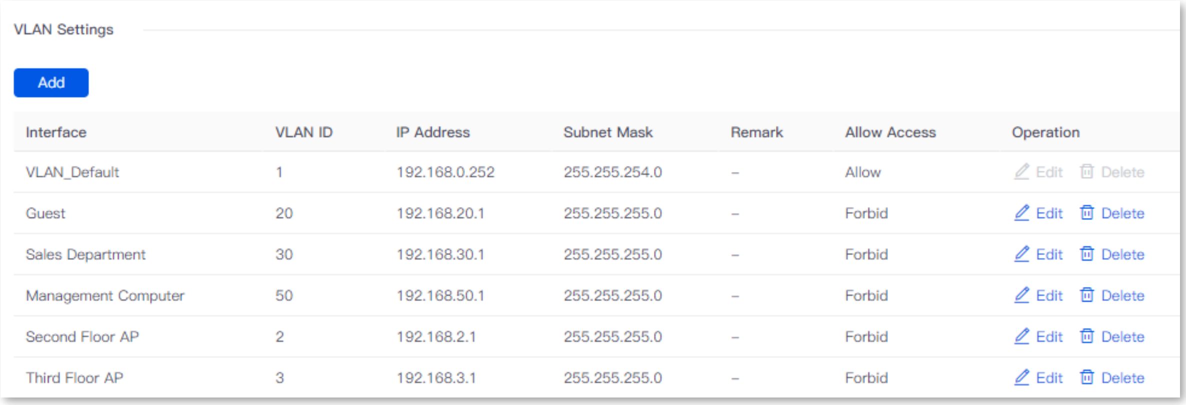
Policy Name	Application Interface	DHCP Type	DHCP Configuration
Guest-User	Guest	User DHCP	Client Address: 192.168.20.100 - 192.168.20.200 Subnet Mask: 255.255.255.0 Gateway: 192.168.20.1 Primary DNS: 192.168.20.1
Sales-User	Sales Department	User DHCP	Client Address: 192.168.30.100 - 192.168.30.200 Subnet Mask: 255.255.255.0 Gateway: 192.168.30.1 Primary DNS: 192.168.30.1
Management VLAN-User	Management Computer	User DHCP	Client Address: 192.168.50.100 - 192.168.50.200 Subnet Mask: 255.255.255.0 Gateway: 192.168.50.1 Primary DNS: 192.168.50.1

Examples of AP DHCP server parameters for the VLAN are shown below.

Policy Name	Application Interface	DHCP Type	DHCP Configuration
2F AP VLAN	Second Floor AP	AP DHCP	Client Address: 172.10.20.100 - 172.10.20.200 Subnet Mask: 255.255.255.0 Gateway: 172.10.20.1 Primary DNS: 172.10.20.1
3F AP VLAN	Third Floor AP	AP DHCP	Client Address: 172.10.30.100 - 172.10.30.200 Subnet Mask: 255.255.255.0 Gateway: 172.10.30.1 Primary DNS: 172.10.30.1

1) Add the VLAN.

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

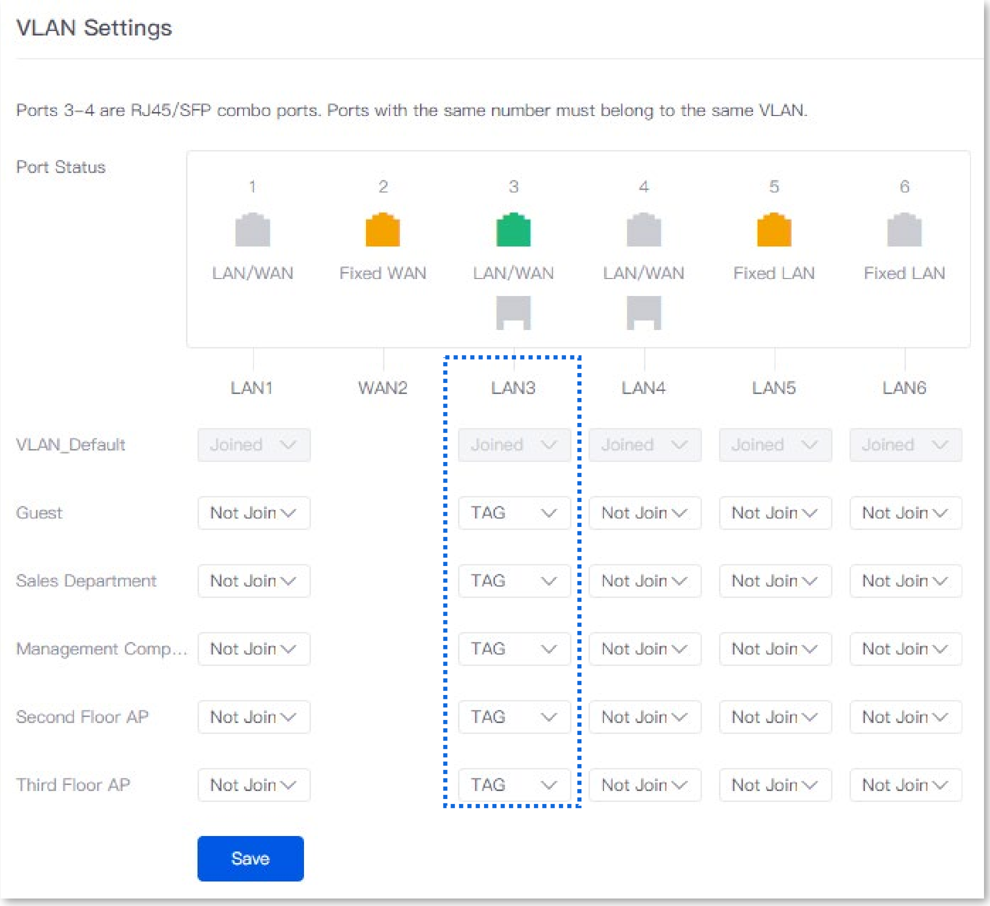


VLAN Settings

Add

Interface	VLAN ID	IP Address	Subnet Mask	Remark	Allow Access	Operation
VLAN_Default	1	192.168.0.252	255.255.254.0	–	Allow	Edit Delete
Guest	20	192.168.20.1	255.255.255.0	–	Forbid	Edit Delete
Sales Department	30	192.168.30.1	255.255.255.0	–	Forbid	Edit Delete
Management Computer	50	192.168.50.1	255.255.255.0	–	Forbid	Edit Delete
Second Floor AP	2	192.168.2.1	255.255.255.0	–	Forbid	Edit Delete
Third Floor AP	3	192.168.3.1	255.255.255.0	–	Forbid	Edit Delete

Select LAN port for the VLAN, which is **LAN3** in this example, set VLAN policy to **TAG**. Then click **Save**.



VLAN Settings

Ports 3–4 are RJ45/SFP combo ports. Ports with the same number must belong to the same VLAN.

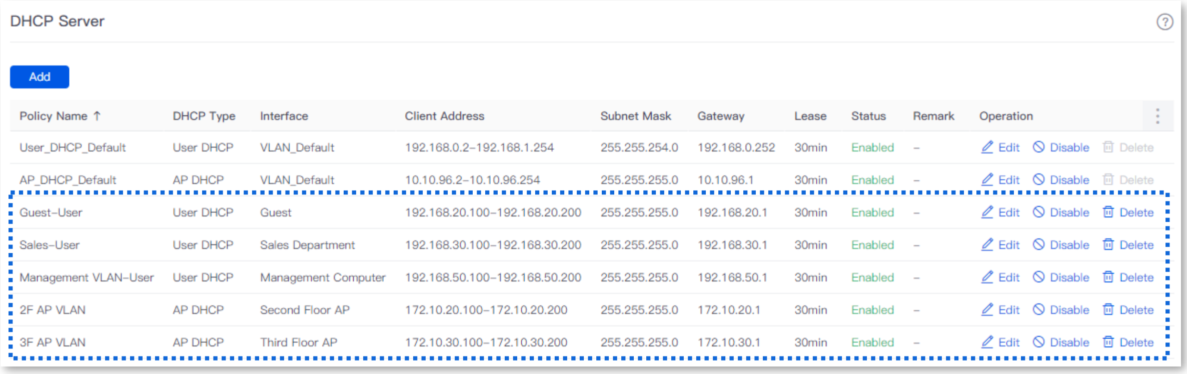
Port Status

	LAN1	WAN2	LAN3	LAN4	LAN5	LAN6
VLAN_Default	Joined		Joined	Joined	Joined	Joined
Guest	Not Join		TAG	Not Join	Not Join	Not Join
Sales Department	Not Join		TAG	Not Join	Not Join	Not Join
Management Comp…	Not Join		TAG	Not Join	Not Join	Not Join
Second Floor AP	Not Join		TAG	Not Join	Not Join	Not Join
Third Floor AP	Not Join		TAG	Not Join	Not Join	Not Join

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 DHCP server for the VLAN, and click **Save**.



Policy Name ↑	DHCP Type	Interface	Client Address	Subnet Mask	Gateway	Lease	Status	Remark	Operation
User_DHCP_Default	User DHCP	VLAN_Default	192.168.0.2–192.168.1.254	255.255.254.0	192.168.0.252	30min	Enabled	–	Edit Disable Delete
AP_DHCP_Default	AP DHCP	VLAN_Default	10.10.96.2–10.10.96.254	255.255.255.0	10.10.96.1	30min	Enabled	–	Edit Disable Delete
Guest–User	User DHCP	Guest	192.168.20.100–192.168.20.200	255.255.255.0	192.168.20.1	30min	Enabled	–	Edit Disable Delete
Sales–User	User DHCP	Sales Department	192.168.30.100–192.168.30.200	255.255.255.0	192.168.30.1	30min	Enabled	–	Edit Disable Delete
Management VLAN–User	User DHCP	Management Computer	192.168.50.100–192.168.50.200	255.255.255.0	192.168.50.1	30min	Enabled	–	Edit Disable Delete
2F AP VLAN	AP DHCP	Second Floor AP	172.10.20.100–172.10.20.200	255.255.255.0	172.10.20.1	30min	Enabled	–	Edit Disable Delete
3F AP VLAN	AP DHCP	Third Floor AP	172.10.30.100–172.10.30.200	255.255.255.0	172.10.30.1	30min	Enabled	–	Edit Disable Delete

4. Configure the AP policy.

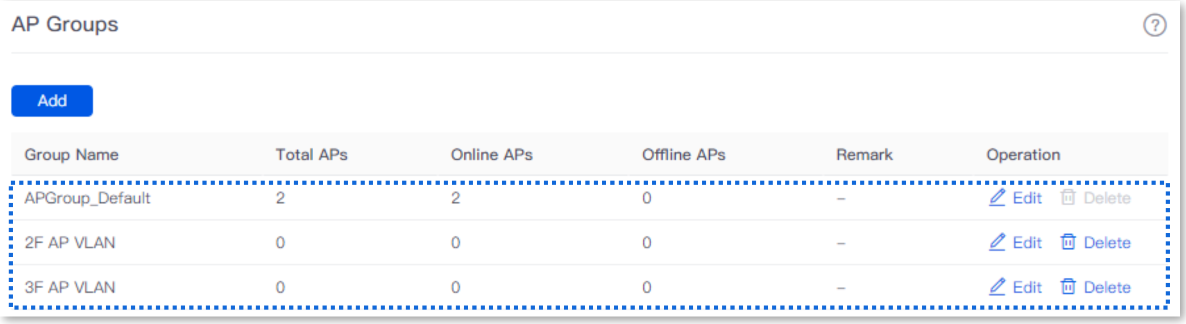
The following table provides examples of AP policy parameters. Retain default values for other parameters that are not mentioned.

AP Group	Wi-Fi	AP VLAN
2F AP VLAN	AP Grouping: 2F AP VLAN SSID: internet Security Mode: WPA2-PSK Wi-Fi Password: UmXmL9UK VLAN ID: 20 Maximum Number of Clients: 40	AP Grouping: 2F AP VLAN AP VLAN: Enable Management VLAN ID: 2 Trunk port: LAN0
	AP Grouping: 2F AP VLAN SSID: Sales Security Mode: WPA2-PSK Wi-Fi Password: CetTLb8T VLAN ID: 30 Maximum Number of Clients: 40	
	AP Grouping: 2F AP VLAN SSID: R&D Security Mode: WPA2-PSK Wi-Fi Password: ZeFtub6m VLAN ID: 40 Maximum Number of Clients: 40	

AP Group	Wi-Fi	AP VLAN
3F AP VLAN	AP Grouping: 3F AP VLAN SSID: internet Security Mode: WPA2-PSK Wi-Fi Password: UmXmL9UK VLAN ID: 20 Maximum Number of Clients: 40	AP Grouping: 3F AP VLAN AP VLAN: Enable Management VLAN ID: 3 Trunk port: LAN0
	AP Grouping: 3F AP VLAN SSID: Sales Security Mode: WPA2-PSK Wi-Fi Password: CetTLb8T VLAN ID: 30 Maximum Number of Clients: 40	
	AP Grouping: 3F AP VLAN SSID: R&D Security Mode: WPA2-PSK Wi-Fi Password: ZeFtub6m VLAN ID: 40 Maximum Number of Clients: 40	

1) Configure the AP Group policy.

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



AP Groups

Add

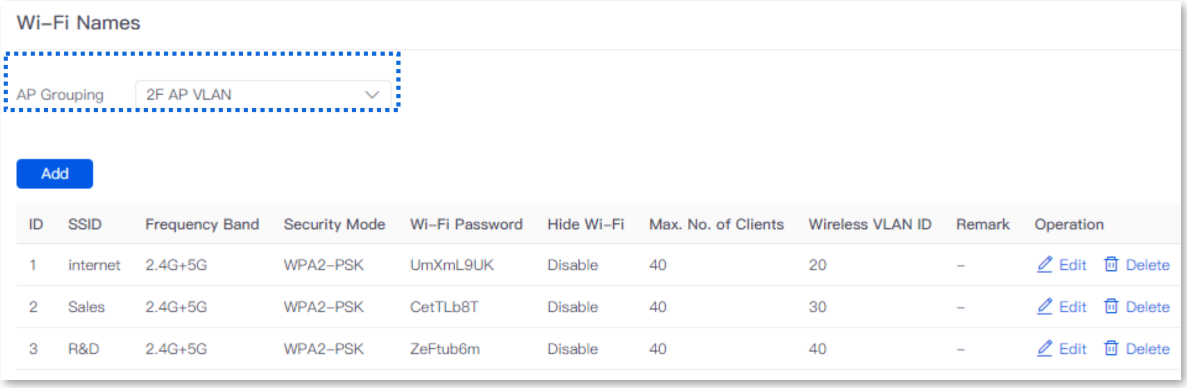
Group Name	Total APs	Online APs	Offline APs	Remark	Operation
APGroup_Default	2	2	0	–	Edit Delete
2F AP VLAN	0	0	0	–	Edit Delete
3F AP VLAN	0	0	0	–	Edit Delete

2) Configure the Wi-Fi policy.

Tip

The maximum number of clients supported by the AP is 128. If multiple SSID policies need to be delivered to the same AP, you should plan the maximum number of clients appropriately to ensure that the maximum number of clients for each SSID policy does not exceed 128.

Navigate to **AP** > **Wi-Fi Settings** > **Wi-Fi Names**, select **2F AP VLAN** for **AP Grouping**. Click **Add** to configure related parameters of the Wi-Fi policy, and click **Save**.

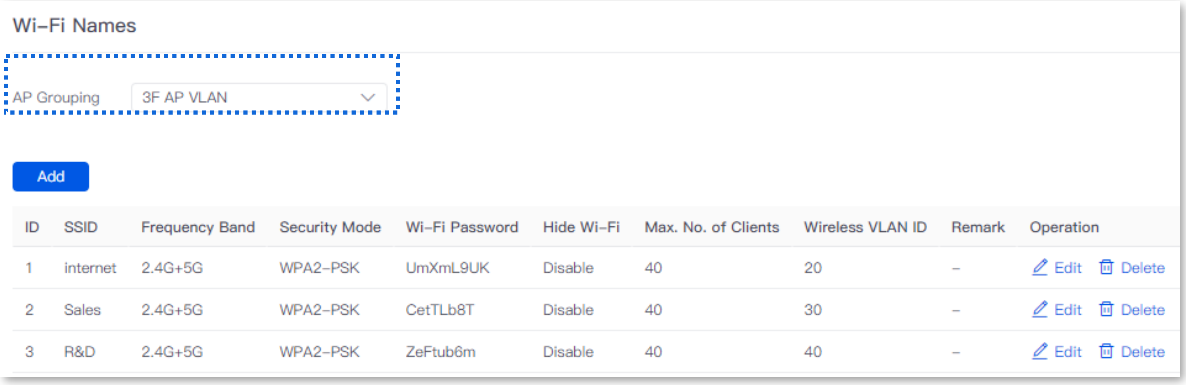


Wi–Fi Names

AP Grouping: 2F AP VLAN

ID	SSID	Frequency Band	Security Mode	Wi–Fi Password	Hide Wi–Fi	Max. No. of Clients	Wireless VLAN ID	Remark	Operation
1	internet	2.4G+5G	WPA2–PSK	UmXmL9UK	Disable	40	20	–	Edit Delete
2	Sales	2.4G+5G	WPA2–PSK	CetTLb8T	Disable	40	30	–	Edit Delete
3	R&D	2.4G+5G	WPA2–PSK	ZeFtub6m	Disable	40	40	–	Edit Delete

Navigate to **AP** > **Wi-Fi Settings** > **Wi-Fi Names**, select **3F AP VLAN** for **AP Grouping**. Click **Add** to configure related parameters of the Wi-Fi policy, and click **Save**.



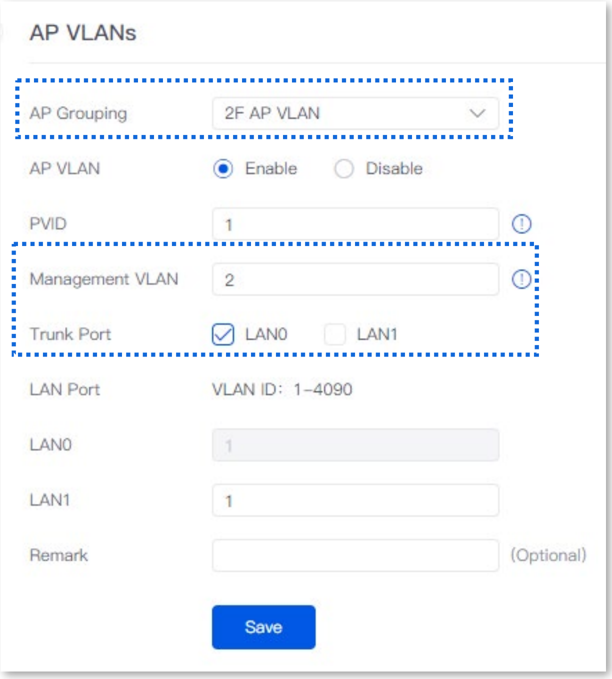
Wi–Fi Names

AP Grouping: 3F AP VLAN

ID	SSID	Frequency Band	Security Mode	Wi–Fi Password	Hide Wi–Fi	Max. No. of Clients	Wireless VLAN ID	Remark	Operation
1	internet	2.4G+5G	WPA2–PSK	UmXmL9UK	Disable	40	20	–	Edit Delete
2	Sales	2.4G+5G	WPA2–PSK	CetTLb8T	Disable	40	30	–	Edit Delete
3	R&D	2.4G+5G	WPA2–PSK	ZeFtub6m	Disable	40	40	–	Edit Delete

3) Configure VLAN policy.

Navigate to **AP** > **Wi-Fi Settings** > **AP VLANs**, select **2F AP VLAN** for **AP Grouping**. Enable the **AP VLAN** function, set **Management VLAN** to **2**, and set **Trunk Port** to **LAN0**. Then click **Save**.



AP VLANs

AP Grouping: 2F AP VLAN

AP VLAN: ● Enable ○ Disable

PVID: 1

Management VLAN: 2

Trunk Port: ☑ LAN0 □ LAN1

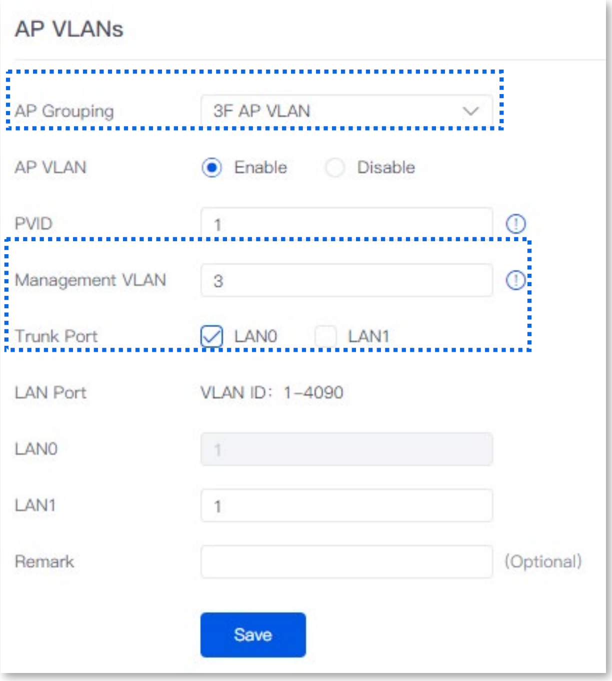
LAN Port: VLAN ID: 1–4090

LAN0: 1

LAN1: 1

Remark: (Optional)

Navigate to **AP** > **Wi-Fi Settings** > **AP VLANs**, select **3F AP VLAN** for **AP Grouping**. Enable the **AP VLAN** function, set **Management VLAN** to **3**, and set **Trunk Port** to **LAN0**. Then click **Save**.



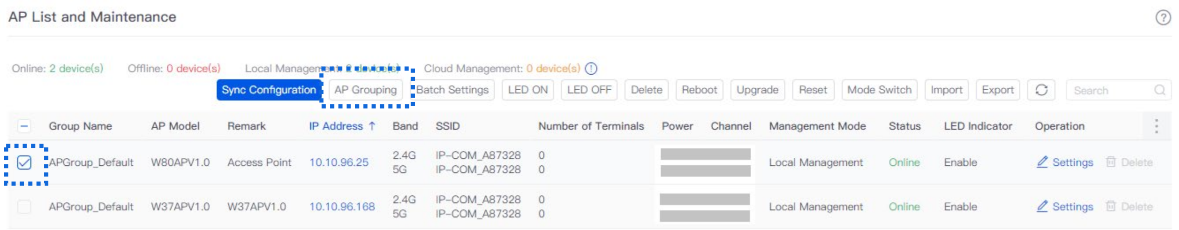
AP VLANs

AP Grouping	3F AP VLAN
AP VLAN	● Enable ○ Disable
PVID	1
Management VLAN	3
Trunk Port	☑ LAN0 □ LAN1
LAN Port	VLAN ID: 1–4090
LAN0	1
LAN1	1
Remark	(Optional)

5. Deliver the AP group policy.

1) Deliver the AP group policy to the APs on the second floor.

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

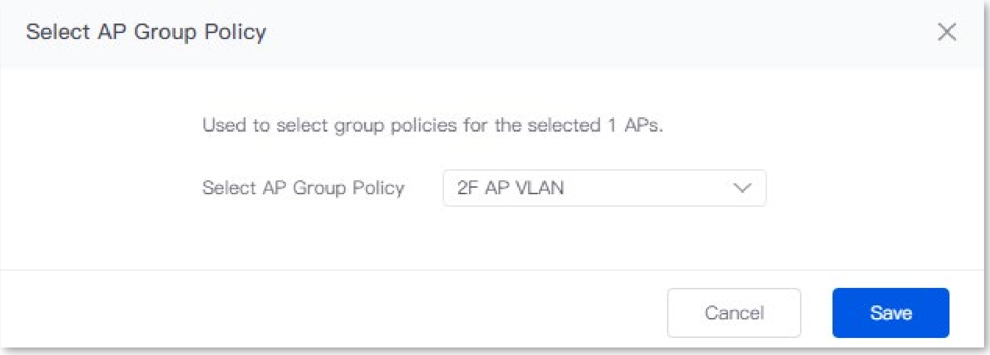


AP List and Maintenance

Online: 2 device(s) Offline: 0 device(s) Local Management: 2 device(s) Cloud Management: 0 device(s)

	Group Name	AP Model	Remark	IP Address ↑	Band	SSID	Number of Terminals	Power	Channel	Management Mode	Status	LED Indicator	Operation
☑	APGroup_Default	W80APV1.0	Access Point	10.10.96.25	2.4G 5G	IP-COM_A87328 IP-COM_A87328	0 0	[redacted]	[redacted]	Local Management	Online	Enable	Settings Delete
□	APGroup_Default	W37APV1.0	W37APV1.0	10.10.96.168	2.4G 5G	IP-COM_A87328 IP-COM_A87328	0 0	[redacted]	[redacted]	Local Management	Online	Enable	Settings Delete

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



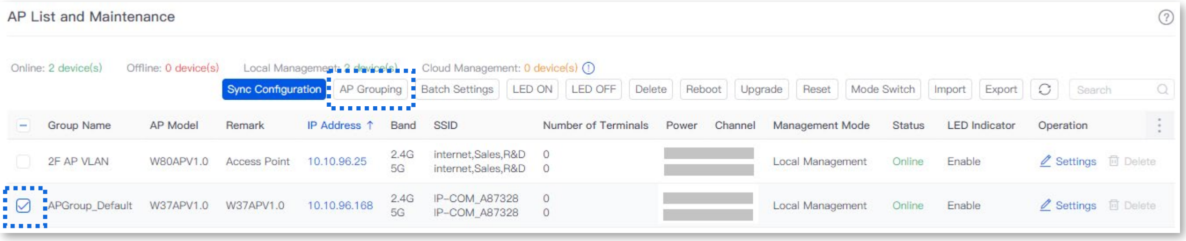
Select AP Group Policy

Used to select group policies for the selected 1 APs.

Select AP Group Policy: 2F AP VLAN

2) Deliver the AP group policy to the APs on the third floor.

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

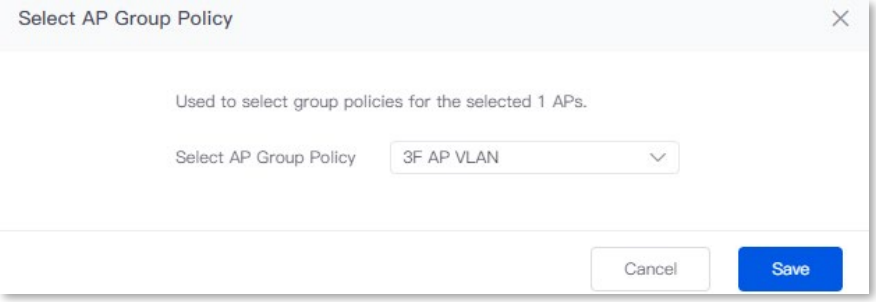


AP List and Maintenance

Online: 2 device(s) Offline: 0 device(s) Local Management: 2 device(s) Cloud Management: 0 device(s)

	Group Name	AP Model	Remark	IP Address ↑	Band	SSID	Number of Terminals	Power	Channel	Management Mode	Status	LED Indicator	Operation
□	2F AP VLAN	W80APV1.0	Access Point	10.10.96.25	2.4G 5G	internet,Sales,R&D internet,Sales,R&D	0 0	[redacted]		Local Management	Online	Enable	Settings Delete
☑	APGroup_Default	W37APV1.0	W37APV1.0	10.10.96.168	2.4G 5G	IP-COM_A87328 IP-COM_A87328	0 0	[redacted]		Local Management	Online	Enable	Settings Delete

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



Select AP Group Policy

Used to select group policies for the selected 1 APs.

Select AP Group Policy: 3F AP VLAN

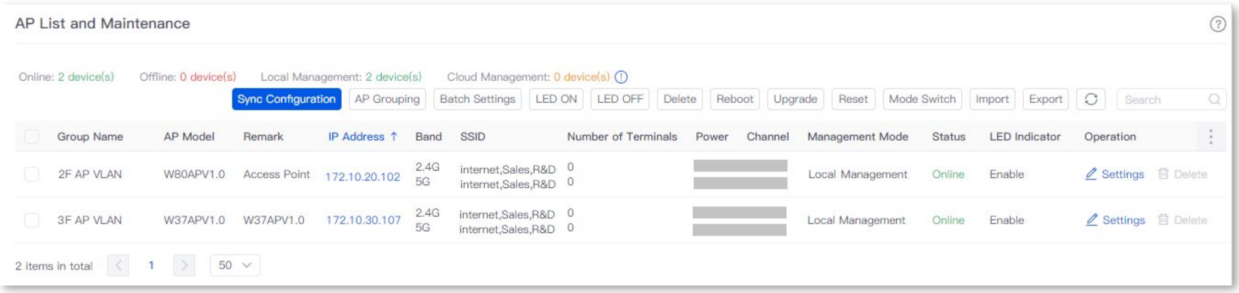
II. Configure the managed switch

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

Port Connected to	VLAN ID (VLAN Allowed)	Port Property	PVID
Router	2,3,20,30,50	Trunk	1
Management computer	50	Access	50
Internal Server	40	Access	40
Switch1 (Sales Department)	30	Access	30
Switch2 (R&D Department)	40	Access	40
Switch3 (2F AP)	2,20,30,40	Trunk	1
Switch4 (3F AP)	3,20,30,40	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.

On the **AP** > **AP List and Maintenance** page of the router, you can find that the AP will go offline, and then go online again.



AP List and Maintenance

Online: 2 device(s) Offline: 0 device(s) Local Management: 2 device(s) Cloud Management: 0 device(s)

	Group Name	AP Model	Remark	IP Address ↑	Band	SSID	Number of Terminals	Power	Channel	Management Mode	Status	LED Indicator	Operation
□	2F AP VLAN	W80APV1.0	Access Point	172.10.20.102	2.4G 5G	internet,Sales,R&D internet,Sales,R&D	0 0	[redacted]		Local Management	Online	Enable	Settings Delete
□	3F AP VLAN	W37APV1.0	W37APV1.0	172.10.30.107	2.4G 5G	internet,Sales,R&D internet,Sales,R&D	0 0	[redacted]		Local Management	Online	Enable	Settings Delete

2 items in total 1 50

III. Configure the internal server

Add VLANs for ports connected to the core 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/Subnet·Mask	Physical Port
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
R&D	Client Address: 192.168.40.100 - 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 core switch.

Port Connected to	VLAN ID (VLAN Allowed)	Port Property	PVID
Core switch	40	Access	40

For details about how to configure the device, see the user guide of the 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 Sales Department connect to the wireless network **Sales**, enter the wireless password **CetTLb8T** to access the internet 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 Sales Department access the wired network, they can access the internet 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.
- The management computer uses the IP address of the VLAN (any VLAN that has been added) to log in to the web UI of the router.

4.4 DHCP settings

4.4.1 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 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.

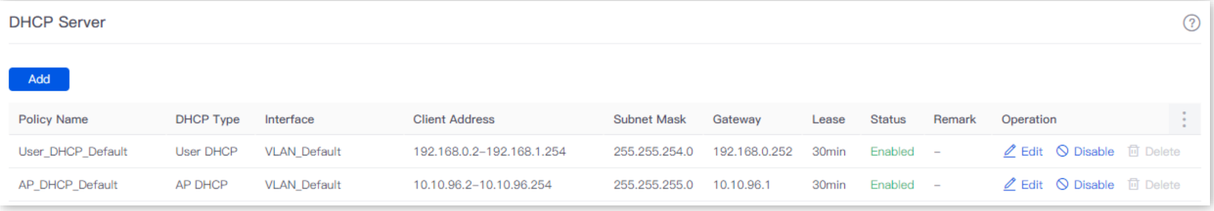
Note

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.

4.4.2 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.



DHCP Server

Add

Policy Name	DHCP Type	Interface	Client Address	Subnet Mask	Gateway	Lease	Status	Remark	Operation
User_DHCP_Default	User DHCP	VLAN_Default	192.168.0.2–192.168.1.254	255.255.254.0	192.168.0.252	30min	Enabled	–	Edit Disable Delete
AP_DHCP_Default	AP DHCP	VLAN_Default	10.10.96.2–10.10.96.254	255.255.255.0	10.10.96.1	30min	Enabled	–	Edit Disable Delete

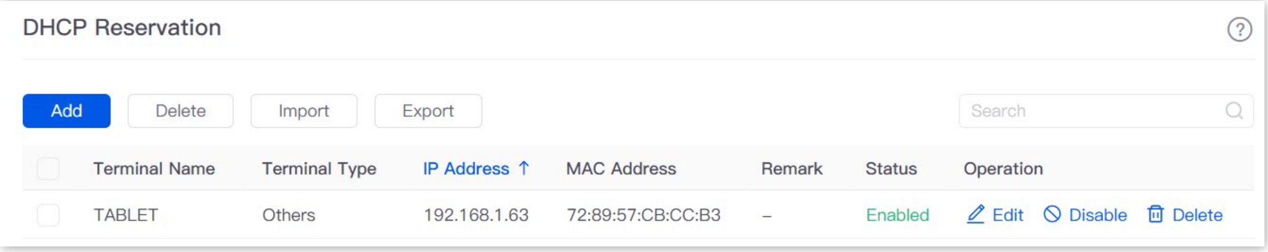
Parameter description

Parameter	Description
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 clients. – **AP DHCP**: Used to assign IP addresses to IP-COM APs.
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.
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 or 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 or 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 clients does not include the excluded address.

4.4.3 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 or export static IP address lists. If the client is already connected to the router, you can quickly add it to the reservation list on the DHCP list page. Otherwise, click **Add** to manually create a reservation rule.



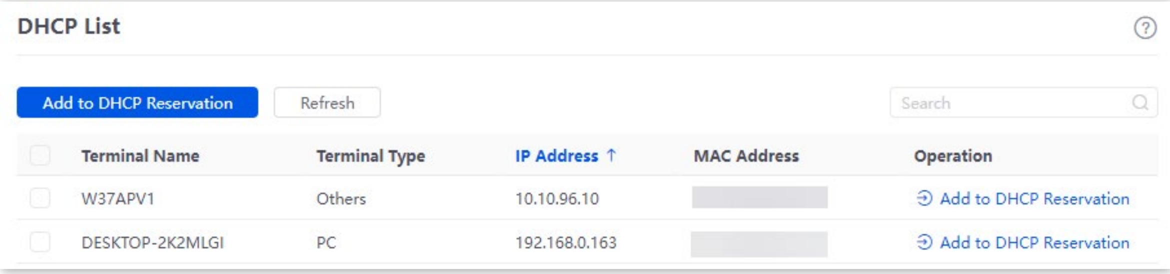
□	Terminal Name	Terminal Type	IP Address ↑	MAC Address	Remark	Status	Operation
□	TABLET	Others	192.168.1.63	72:89:57:CB:CC:B3	–	Enabled	Edit Disable Delete

4.4.4 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 client that obtains the IP address from this router:

- To view device information such as the client name and obtained IP address of the device.
- The clients with assigned IP addresses can be added to the reservation list individually or in batches, so that the DHCP server always assigns the same IP address to the clients. Successfully added clients will appear in the DHCP reservation list.



□	Terminal Name	Terminal Type	IP Address ↑	MAC Address	Operation
□	W37APV1	Others	10.10.96.10	[redacted]	Add to DHCP Reservation
□	DESKTOP-2K2MLGI	PC	192.168.0.163	[redacted]	Add to DHCP Reservation

5 Manage APs

Features available in the router may vary by model and software version. Router availability may also vary by region or ISP. All images, steps, and descriptions in this guide are only examples and may not reflect your actual router experience.

5.1 Overview

The router integrates the functions of a 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 primary router, the AP can be added to the router as follows.

1. Enable the AP to obtain its 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.

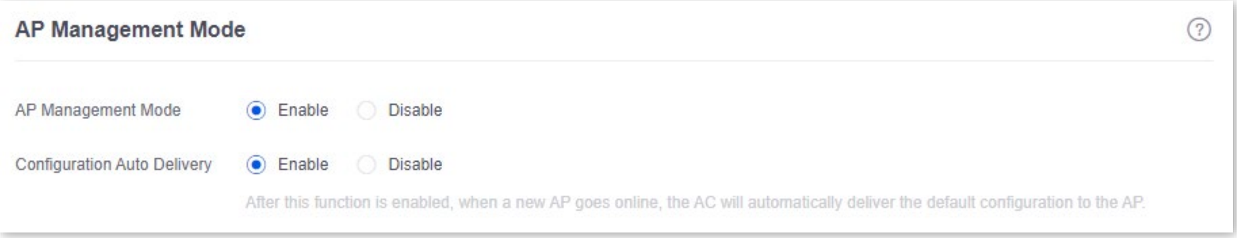
5.2 Configuration wizard

Procedure	Task	Description
1	Configure network	Optional. By default, the router has created a VLAN interface named VLAN_Default. The default IP address of this interface is **192.168.0.252**, and the User_DHCP_Default and AP_DHCP_Default policies are configured.
2	Set AP management mode	Optional. By default, the AP management mode and configuration auto delivery function of the router have been enabled.
3	Configure Wi-Fi	Optional. By default, the router has created an SSID policy for **APGroup_Default**.
4	Configure AP group policy	Optional. By default, the router has created an AP group policy named **APGroup_Default**.
5	Configure AP VLAN	Optional. Disable by default. Enable if you need to configure VLAN of AP.
6	Separate APs to AP groups	Optional. By default, the router has separated the managed APs to **APGroup_Default**. You can modify them based on the actual situation.

5.3 AP management mode

Log in to the web UI of the router, and navigate to **AP** > **AP Management Mode** to enter the page.

On this page, you can set the AP management mode, and configure the auto delivery function. The router only supports IP-COM fat APs.



AP Management Mode

AP Management Mode ● Enable ○ Disable

Configuration Auto Delivery ● Enable ○ Disable

After this function is enabled, when a new AP goes online, the AC will automatically deliver the default configuration to the AP.

Parameter description

Parameter	Description
AP Management Mode	Used to enable or disable the AP management function.
Configuration Auto Delivery	After this function is enabled, when a new AP goes online, or an offline AP goes online, the router will automatically add the AP to **APGroup_Default**, that is, deliver the default configuration to the AP.

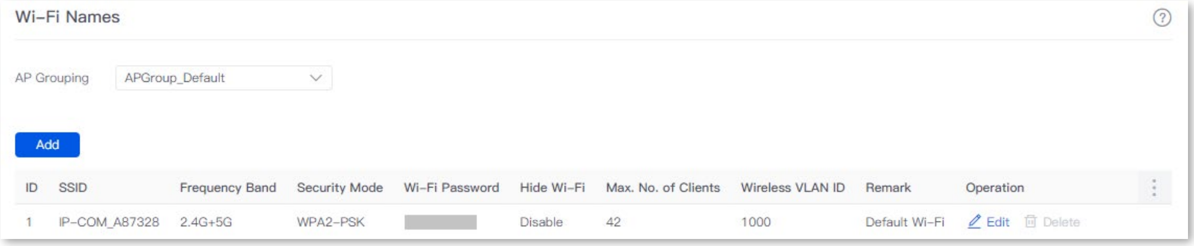
5.4 Wi-Fi setting

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.

5.4.1 Wi-Fi names

Log in to the web UI of the router, and navigate to **AP** > **Wi-Fi Settings** > **Wi-Fi Names** to enter the page.

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



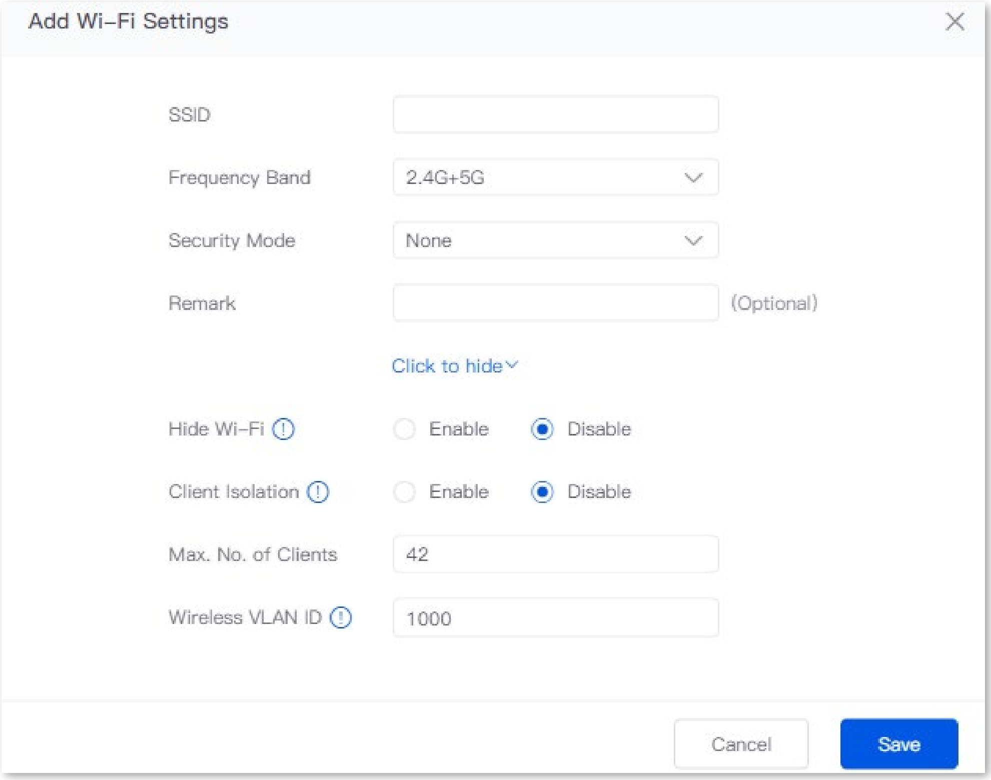
Wi-Fi Names

AP Grouping: APGroup_Default

Add

ID	SSID	Frequency Band	Security Mode	Wi-Fi Password	Hide Wi-Fi	Max. No. of Clients	Wireless VLAN ID	Remark	Operation
1	IP-COM_A87328	2.4G+5G	WPA2-PSK	[redacted]	Disable	42	1000	Default Wi-Fi	Edit Delete

By default, the router has created a Wi-Fi policy. You can click **Add** to add a new Wi-Fi policy.


Add Wi-Fi Settings

SSID

Frequency Band: 2.4G+5G

Security Mode: None

Remark (Optional)

Click to hide

Hide Wi-Fi: ○ Enable ● Disable

Client Isolation: ○ Enable ● Disable

Max. No. of Clients: 42

Wireless VLAN ID: 1000

Parameter description

Parameter	Description
AP Grouping	Specifies the group to which the wireless network belongs. The AP group should be configured at AP Groups in advance.
SSID	Specifies the name of the wireless network.
Frequency Band	Specify the frequency band of the wireless network. Tip If AP only support one band (2.4GHz or 5GHz), when you select **2.4G+5G**, the other band is invalid.

Parameter	Description
Security Mode	Specifies the security modes of the SSID policy. – **None**: The wireless network is not protected by a password. This option is not recommended. – **WPA-PSK**, **WPA2-PSK**, **WPA/WPA2-PSK:** A pre-shared key (PSK) is used for identity authentication. The AP automatically generates the encryption key using TKIP or AES, avoiding WEP's static key vulnerabilities, making it ideal for home or individual use. **WPA/WPA2-PSK** indicates compatibility with both WPA-PSK and WPA2-PSK modes. – **WPA3-SAE**, **WPA3-SAE/WPA2-PSK:** 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**, **WPA2:** 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 (Under Advanced>)	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.
Wi-Fi 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 the wireless password when connecting to the SSID.
Key Update Interval (Under Advanced>)	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. 0 means no update.
Radius Server Address	Specify the IP address, shared key and authentication port of the RADIUS Server. They are required only when **Security Mode** is set to **WPA** or **WPA2**.
Authentication Key	
Authentication Port	
Hide Wi-Fi (Under Advanced>)	Used to enable or disable the hide SSID function. After this function is enabled, the SSID will be hidden and the wireless network will not appear in the available network list of wireless clients (such as smartphones), enhancing the security of the wireless network. If you want to connect to the hidden wireless network, manually enter the SSID on your wireless clients.
Client Isolation (Under Advanced>)	Used to enable or disable the client isolation function. With the **Client Isolation** enabled, clients cannot access each other.

Parameter	Description
Max No. of Clients (Under Advanced>)	Specifies the maximum number of clients allowed to connect to the wireless network. Tip 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 maximum number of clients of the SSID policies does not exceed 128.
Wireless VLAN ID	Specifies the VLAN to which the SSID belongs. The value range is 1, 10 – 4094.

5.4.2 Guest Wi-Fi

Guest Wi-Fi is isolated from other networks. The clients connected to the guest Wi-Fi can access the internet, but cannot access the router's web UI or other networks.

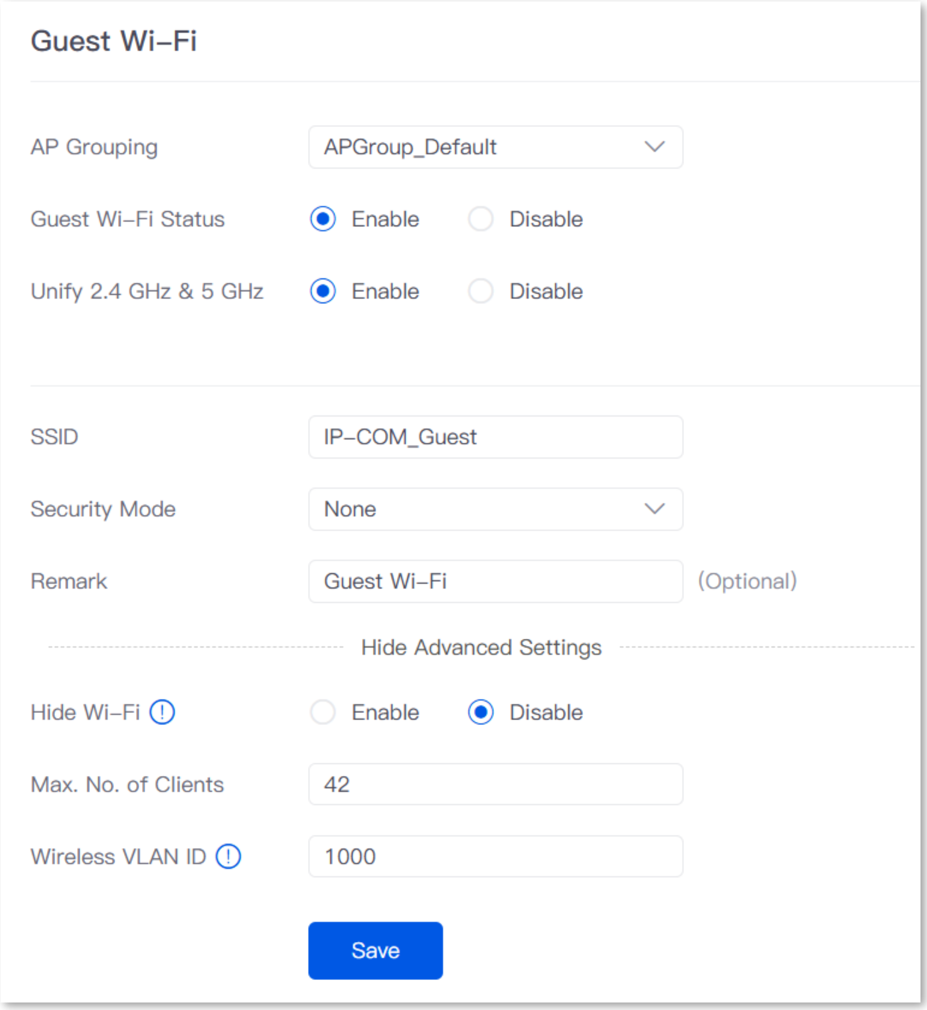
When you need to open a wireless network for guests, you can enable guest Wi-Fi to meet the internet requirements of guests. It protects the security of the main network to prevent personal information disclosure.

Log in to the web UI of the router, and navigate to **AP** > **Wi-Fi Settings** > **Guest Wi-Fi** to enter the page.

By default, the router has created a Wi-Fi policy. You can click **Add** to add a new Wi-Fi policy.

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

- Unify 2.4 GHz & 5 GHz:
  - When enabled: The 2.4 GHz and 5 GHz guest Wi-Fi networks share the same SSID and password. Wi-Fi-enabled clients connected to it will use the frequency with better connection quality.
  - When disabled: The 2.4GHz and 5GHz guest Wi-Fi networks are displayed separately, and you can access the internet by connecting to either one.
- For other parameters, refer to the parameter description for Wi-Fi names.



Guest Wi–Fi

AP Grouping: APGroup_Default

Guest Wi–Fi Status: ● Enable ○ Disable

Unify 2.4 GHz & 5 GHz: ● Enable ○ Disable

SSID: IP–COM_Guest

Security Mode: None

Remark: Guest Wi–Fi (Optional)

Hide Advanced Settings

Hide Wi–Fi: ○ Enable ● Disable

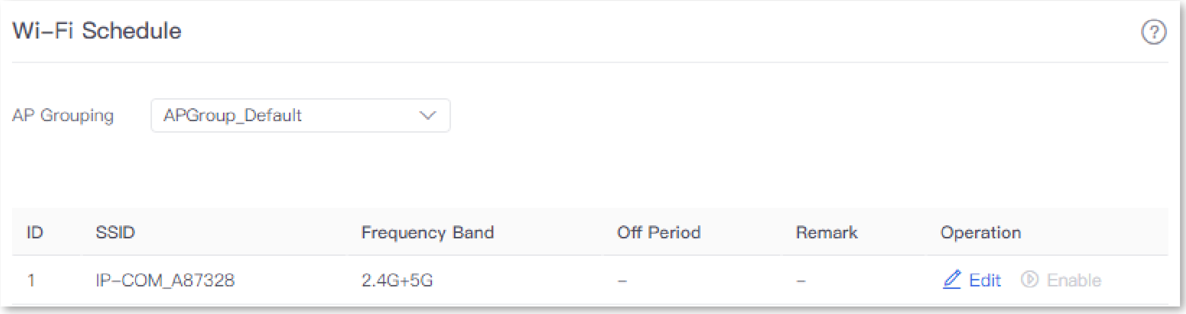
Max. No. of Clients: 42

Wireless VLAN ID: 1000

5.4.3 Wi-Fi schedule

Log in to the web UI of the router, and navigate to **AP** > **Wi-Fi Settings** > **Wi-Fi Schedule** to enter the page.

With this function enabled, you can set the periods for the wireless network to be disabled. Within the period, the router will automatically disable the wireless network of the AP managed by the router. Click ✎ Edit to modify the Wi-Fi schedule policy.



Wi–Fi Schedule

AP Grouping: APGroup_Default

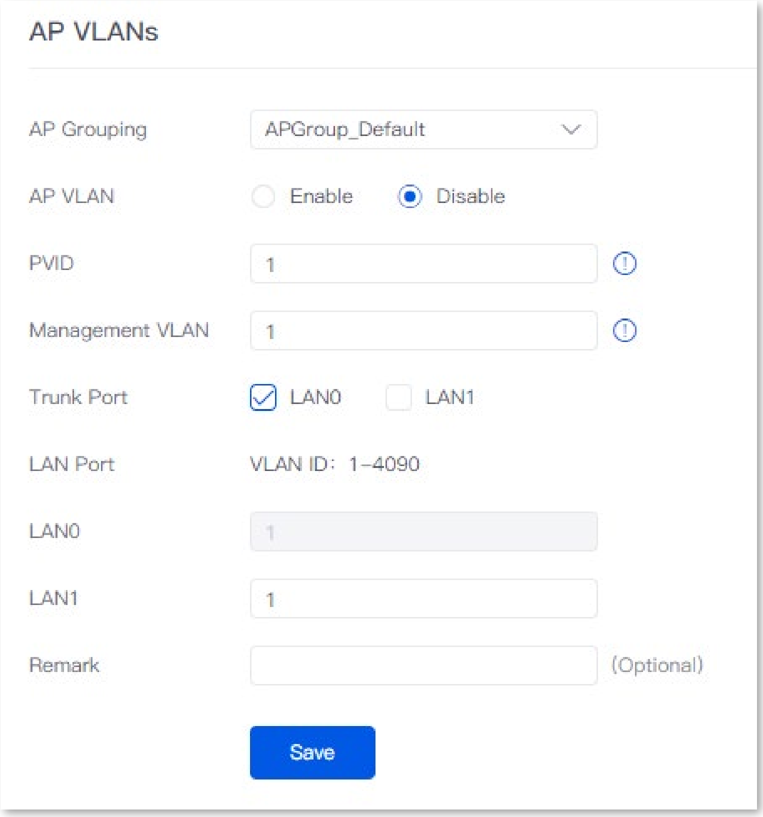
ID	SSID	Frequency Band	Off Period	Remark	Operation
1	IP–COM_A87328	2.4G+5G	–	–	✎ Edit ⊙ Enable

5.4.4 AP VLANs

Log in to the web UI of the router, and navigate to **AP** > **Wi-Fi Settings** > **AP VLANs** to enter the page.

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

You can configure the 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).



AP VLANs

AP Grouping: APGroup_Default

AP VLAN: ○ Enable ● Disable

PVID: 1

Management VLAN: 1

Trunk Port: ☑ LAN0 □ LAN1

LAN Port: VLAN ID: 1–4090

LAN0: 1

LAN1: 1

Remark: (Optional)

Parameter description

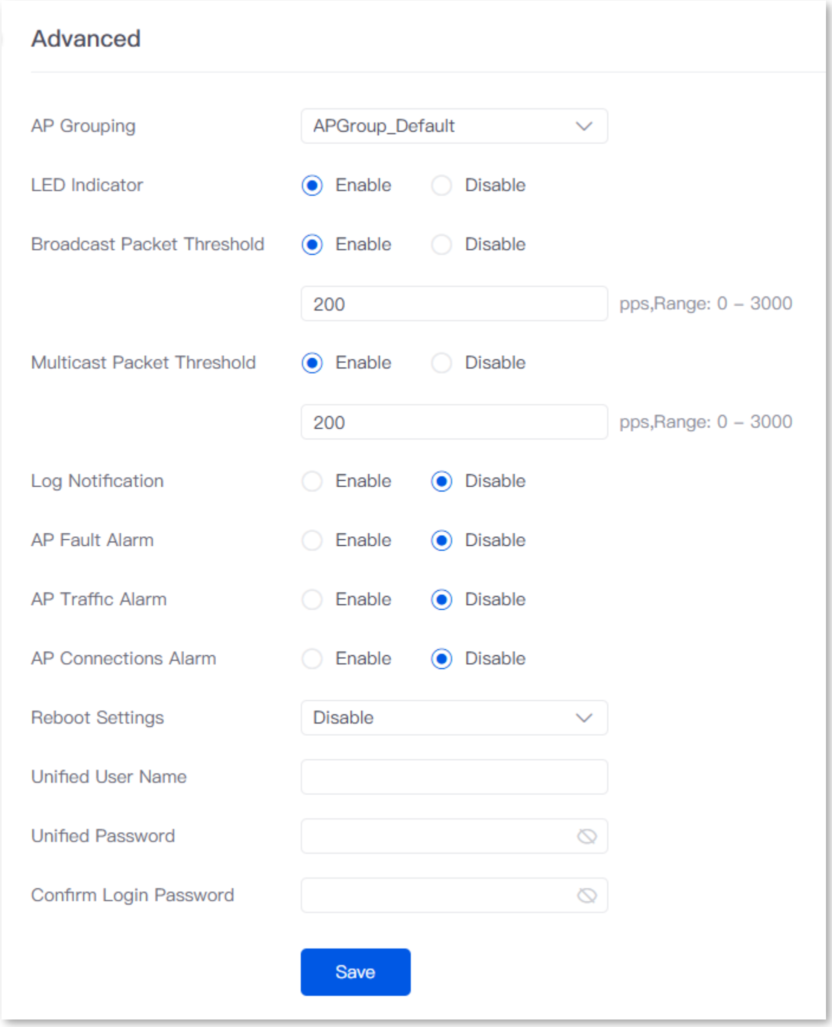
Parameter	Description
AP Grouping	Specifies the group to which the AP VLAN policy belongs. The AP group should be configured at AP Groups in advance.
AP VLAN	Used to enable or disable the AP VLAN function.
PVID	Specifies the ID of the default native VLAN of the trunk port of the AP.
Management VLAN	Specifies the ID of the management VLAN. The default value is 1. After changing the management VLAN, the AP needs to reconnect to the new management VLAN port in order to be managed by the router.

Parameter	Description
Trunk Port	Used to select the trunk ports that allow data of all VLANs to pass. Note 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.

5.4.5 Advanced

Log in to the web UI of the router, and navigate to **AP** > **Wi-Fi Settings** > **Advanced** to enter the page.

On this page, you can configure advanced policies for AP.



Advanced

AP Grouping: APGroup_Default

LED Indicator: ● Enable ○ Disable

Broadcast Packet Threshold: ● Enable ○ Disable

200 pps,Range: 0 – 3000

Multicast Packet Threshold: ● Enable ○ Disable

200 pps,Range: 0 – 3000

Log Notification: ○ Enable ● Disable

AP Fault Alarm: ○ Enable ● Disable

AP Traffic Alarm: ○ Enable ● Disable

AP Connections Alarm: ○ Enable ● Disable

Reboot Settings: Disable

Unified User Name:

Unified Password:

Confirm Login Password:

Parameter description

Parameter	Description
AP Grouping	Specifies the group to which the advanced belongs. The AP group should be configured at AP Groups in advance.
LED Indicator	Turn on or turn off the indicator of AP.
Broadcast Packet Threshold	Specifies the maximum transmission rate of broadcast packets. Default value: 200pps (a maximum of 200 packets per second). Excessive broadcast traffic may cause a broadcast storm, paralyzing the network.
Multicast Packet Threshold	Specifies the maximum transmission rate of multicast packets. Default value: 200pps (a maximum of 200 packets per second). Excessive multicast traffic may affect the overall performance of the network.
Log Notification	Used to enable or disable the log notification function. After it is enabled, the AP alarms will be displayed in **AP Alarm Log** and **AP Running Log** at Running Log.

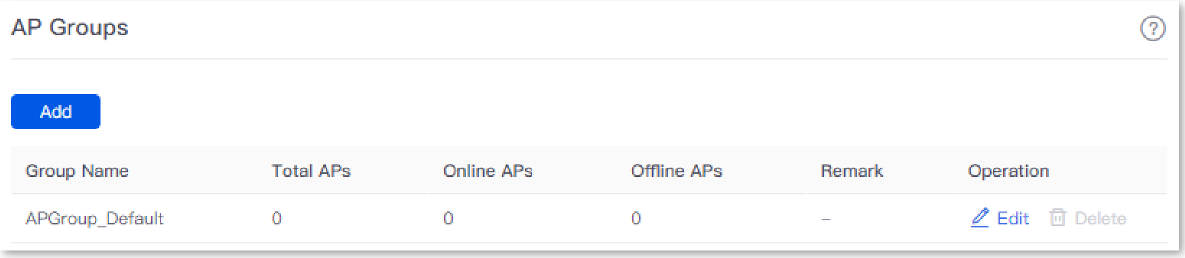
Parameter	Description
AP Fault Alarm	Used to enable or disable the AP fault alarm function. When it is enabled, if the AP is faulty (such as reboot, offline, online), the AP will send an alarm through the Log Notification.
AP Traffic Alarm	Used to enable or disable the AP traffic alarm function. With this function enabled, when the total traffic exceeds the specified threshold, an alarm notification will be triggered. The notification can be sent by Log Notification.
AP Connections Alarm	Used to enable or disable the AP connections alarm function. 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 Notification.
Reboot Settings	Specifies the type of maintenance policy. – **Scheduled Reboot**: The AP reboots once at the specified time point on the specified dates. – **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**.
Unified User Name	Specifies the login user name of the AP.
Unified Password	Specifies the login password of the AP.
Confirm Login Password	Used to confirm the login password of the AP.

5.5 AP groups

Log in to the web UI of the router, and navigate to **AP** > **AP Groups** to enter the page.

With AP group policy, Wi-Fi policy can be associated to different AP groups, making it easy to assign managed APs to different groups and deliver different policies.

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



AP Groups

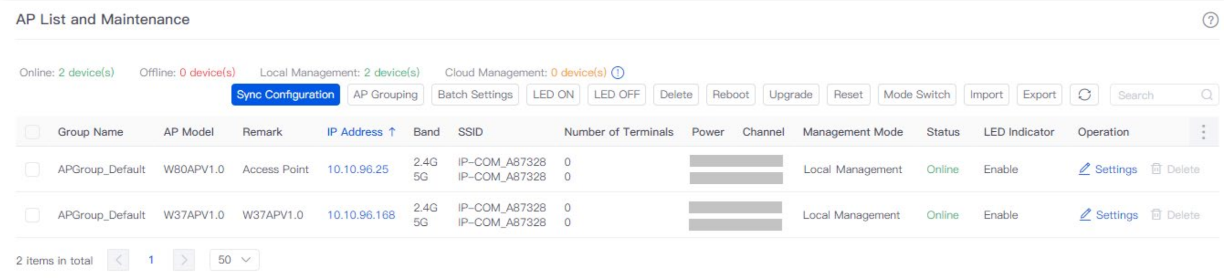
Group Name	Total APs	Online APs	Offline APs	Remark	Operation
APGroup_Default	0	0	0	–	Edit Delete

5.6 AP list and maintenance

5.6.1 Overview

Log in to the web UI of the router, and navigate to **AP** > **AP List and Maintenance** to enter the page.

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. Managed APs will be added to **APGroup_Default** by default.



AP List and Maintenance

Online: 2 device(s) Offline: 0 device(s) Local Management: 2 device(s) Cloud Management: 0 device(s)

□	Group Name	AP Model	Remark	IP Address ↑	Band	SSID	Number of Terminals	Power	Channel	Management Mode	Status	LED Indicator	Operation
□	APGroup_Default	W80APV1.0	Access Point	10.10.96.25	2.4G 5G	IP-COM_A87328 IP-COM_A87328	0 0	[redacted]	[redacted]	Local Management	Online	Enable	Settings Delete
□	APGroup_Default	W37APV1.0	W37APV1.0	10.10.96.168	2.4G 5G	IP-COM_A87328 IP-COM_A87328	0 0	[redacted]	[redacted]	Local Management	Online	Enable	Settings Delete

2 items in total < 1 > 50

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 at AP Groups in advance.
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.

Parameter description

Parameter	Description
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 Wi-Fi of the AP must be enabled and the SSID, encryption mode and Wi-Fi passwords for the 2.4 GHz and 5 GHz Wi-Fi must be consistent.
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.

5.6.2 Deliver policies to APs

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

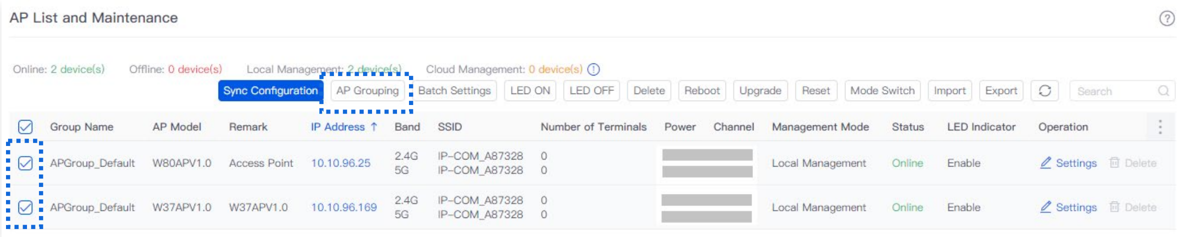
2. (Skip if done) Configure a Wi-Fi policy to be delivered to APs. For details, see Wi-Fi setting in **AP management**.

3. (Skip if done) Configure an AP group. For details, see AP groups in **AP management**.

4. Deliver policies to APs.

   1) Navigate to **AP** > **AP List and Maintenance**.5

   2) Select the APs to which the policies are to be delivered, and click **AP Grouping**. The following figure is for reference only.

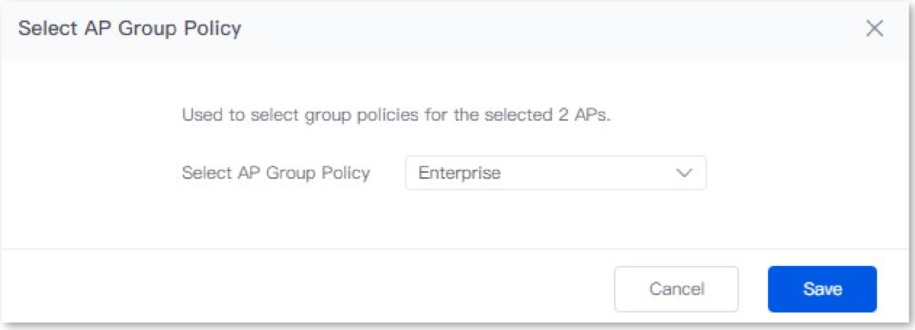


AP List and Maintenance

Online: 2 device(s) Offline: 0 device(s) Local Management: 2 device(s) Cloud Management: 0 device(s)

☑	Group Name	AP Model	Remark	IP Address ↑	Band	SSID	Number of Terminals	Power	Channel	Management Mode	Status	LED Indicator	Operation
☑	APGroup_Default	W80APV1.0	Access Point	10.10.96.25	2.4G 5G	IP-COM_A87328 IP-COM_A87328	0 0	[redacted]	[redacted]	Local Management	Online	Enable	Settings Delete
☑	APGroup_Default	W37APV1.0	W37APV1.0	10.10.96.169	2.4G 5G	IP-COM_A87328 IP-COM_A87328	0 0	[redacted]	[redacted]	Local Management	Online	Enable	Settings Delete

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


Select AP Group Policy

Used to select group policies for the selected 2 APs.

Select AP Group Policy: Enterprise

---End

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

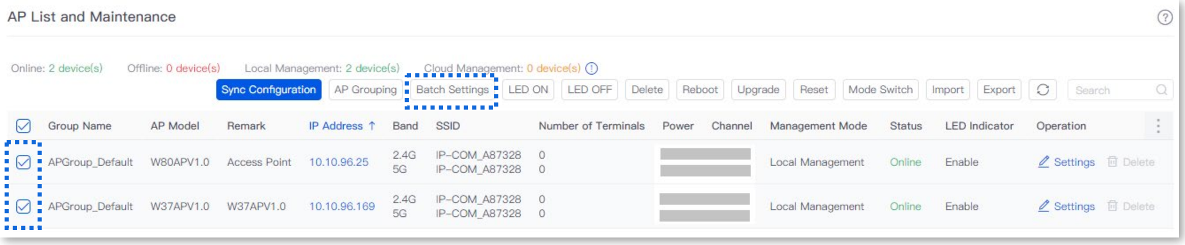
5.6.3 Batch settings

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**. The following figure is for reference only.


AP List and Maintenance

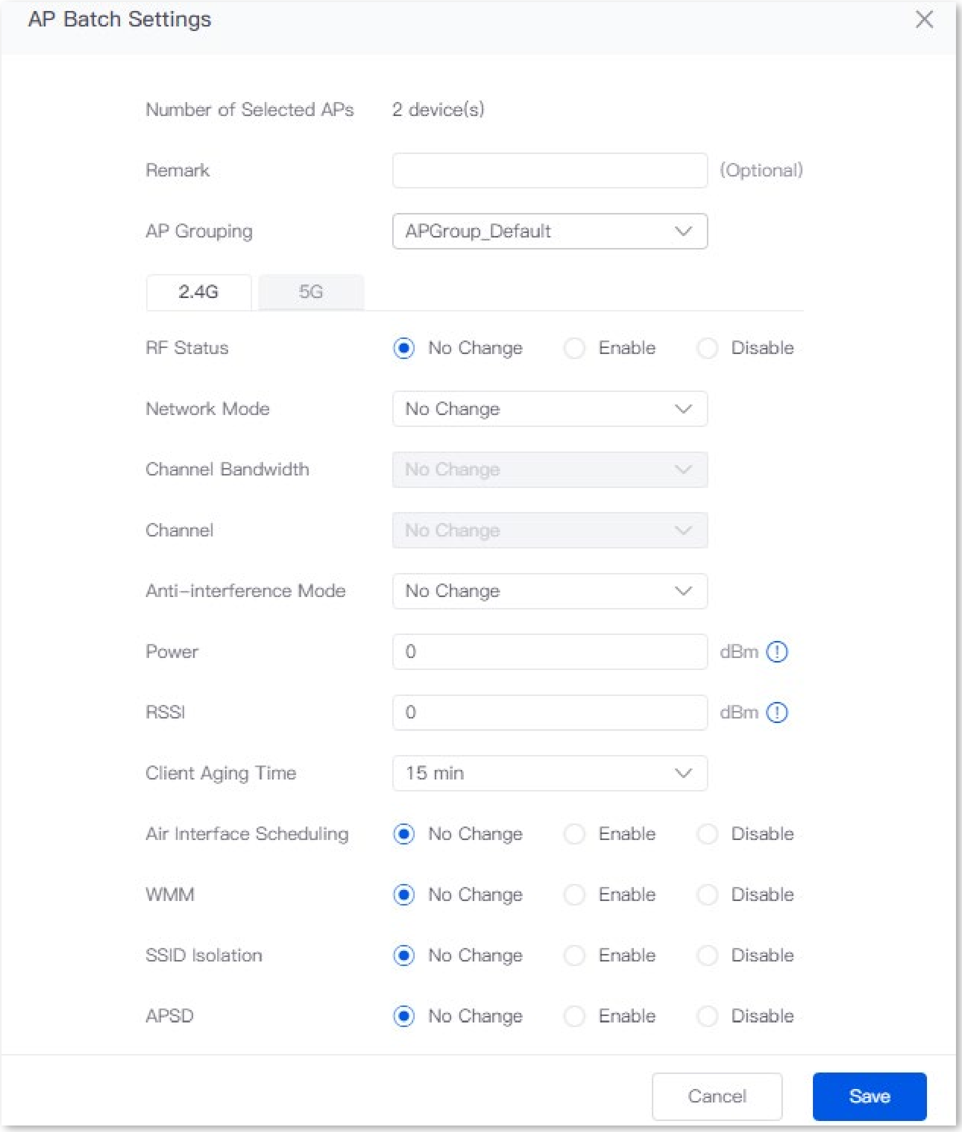
Online: 2 device(s)   Offline: 0 device(s)   Local Management: 2 device(s)   Cloud Management: 0 device(s)

☑	Group Name	AP Model	Remark	IP Address ↑	Band	SSID	Number of Terminals	Power	Channel	Management Mode	Status	LED Indicator	Operation
☑	APGroup_Default	W80APV1.0	Access Point	10.10.96.25	2.4G 5G	IP-COM_A87328 IP-COM_A87328	0 0			Local Management	Online	Enable	Settings Delete
☑	APGroup_Default	W37APV1.0	W37APV1.0	10.10.96.169	2.4G 5G	IP-COM_A87328 IP-COM_A87328	0 0			Local Management	Online	Enable	Settings Delete

4. Set parameters as required, and click **Save**. The following figure is for reference only.

Tip

No Change indicates that the configuration of the AP group to which the AP applies is not modified.



AP Batch Settings

Number of Selected APs: 2 device(s)

Remark: (Optional)

AP Grouping: APGroup_Default

2.4G | 5G

RF Status: ● No Change ○ Enable ○ Disable

Network Mode: No Change

Channel Bandwidth: No Change

Channel: No Change

Anti-interference Mode: No Change

Power: 0 dBm

RSSI: 0 dBm

Client Aging Time: 15 min

Air Interface Scheduling: ● No Change ○ Enable ○ Disable

WMM: ● No Change ○ Enable ○ Disable

SSID Isolation: ● No Change ○ Enable ○ Disable

APSD: ● No Change ○ Enable ○ Disable

---End

Related configurations for the selected APs will be delivered again.

Parameter description

Parameter	Description
AP Grouping	Specifies the AP group policy to be applied for the selected APs. The AP group policy must be configured at AP groups in advance.
2.4G	Used to configure parameters for 2.4 GHz and 5 GHz wireless networks.
5G	
RF Status	Specifies the status of the Wi-Fi function. **No Change** indicates that the RF status of the corresponding frequency band of the AP is not modified. – **Enable**: Select it to enable the Wi-Fi function of the frequency band. – **Disable:** Select it to disable the Wi-Fi function of the frequency band.

Parameter	Description
Network Mode	Specifies the wireless 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.
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. – **No Change**: The router does not deliver the channel bandwidth configuration to the AP. The AP uses the channel bandwidth configured on its web UI.
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. – **No Change:** 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 wireless 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 Wi-Fi analyzer).

Parameter	Description
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. – **No Change**: 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.
Power	Specifies the transmit power of the corresponding band. The higher the transmit power, the wider the Wi-Fi coverage. However, an appropriate reduction of transmit power can improve the performance and security of the wireless 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 wireless network, the AP will cut this client off.
Air Interface Scheduling	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 Wi-Fi 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.
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 Wi-Fi Alliance. Enabling **APSD** can reduce the power consumption of the AP.
5G Preferred	When enabled, the 2.4 GHz and 5 GHz Wi-Fi networks share the same Wi-Fi name and password. When the wireless client supports dual-band Wi-Fi, the client will preferentially access the AP wireless network from the 5GHz band.

5.6.4 Set AP cloud maintenance

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

To enable the cloud maintenance function for APs:

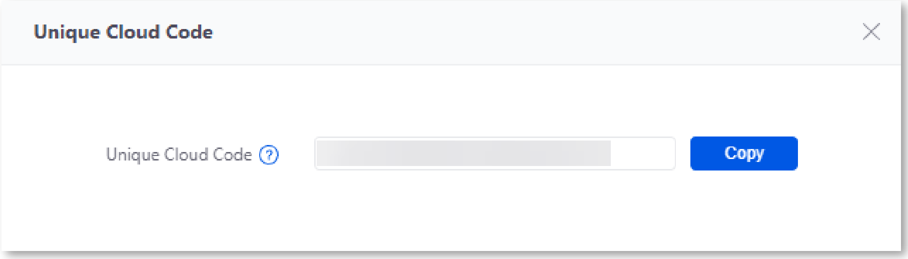
1. Obtain the unique cloud code.

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 Cloud Maintenance.
- Before enabling the cloud maintenance function of the AP, ensure that the AP is connected to the internet.
- The unique loud code can also be obtained from the **Account** entry on the IP-COM Profi App.

1) Access https://imsen.ip-com.com.cn to enter the IP-COM Profi Cloud Platform.

2) Click **Add** in the upper right corner and select **Unique Cloud Code**, and copy the unique cloud code.



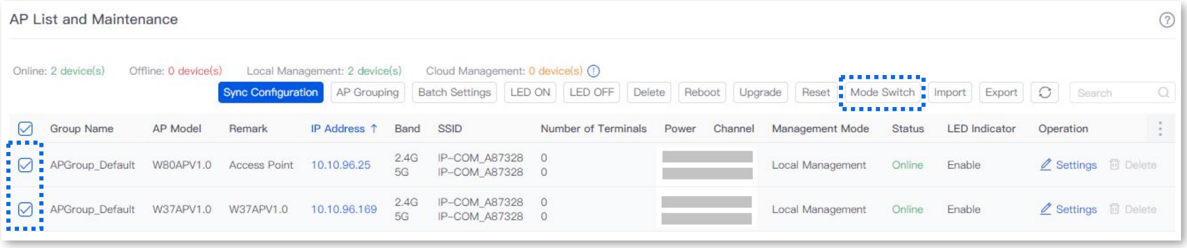
Unique Cloud Code

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**. The following figure is for reference only.



AP List and Maintenance

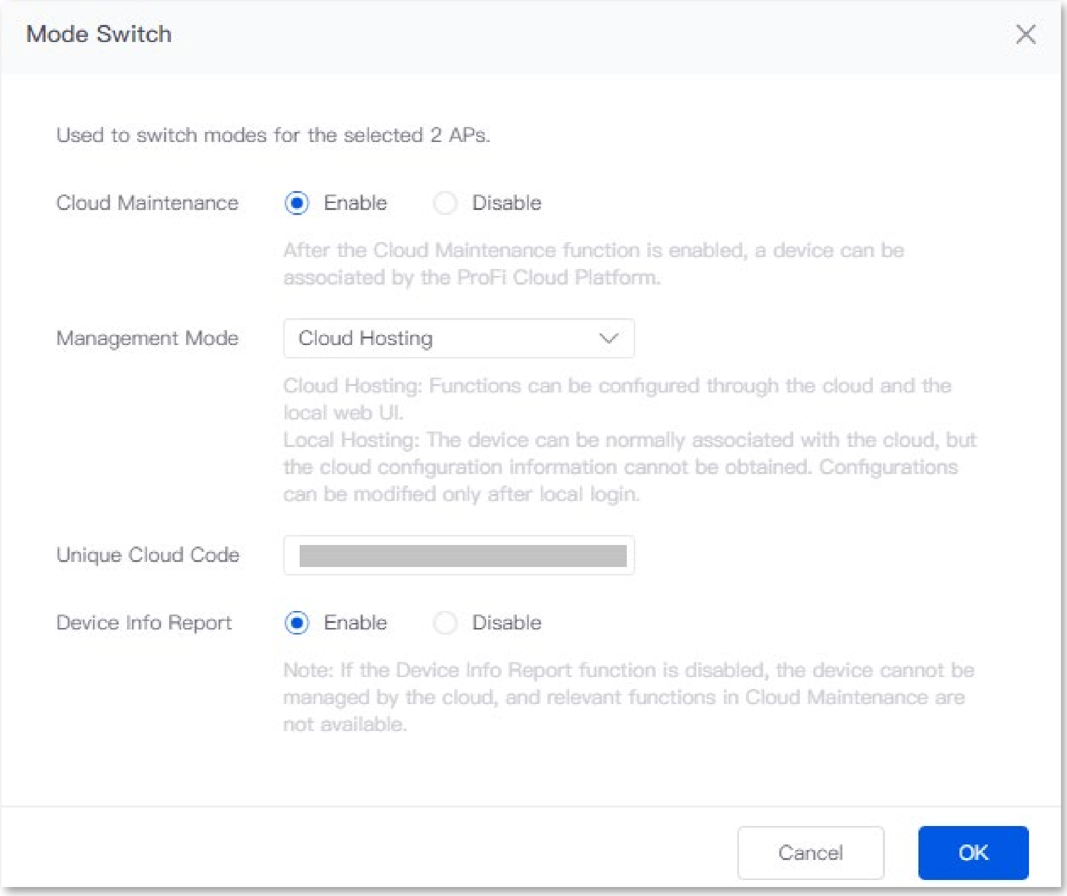
Online: 2 device(s) Offline: 0 device(s) Local Management: 2 device(s) Cloud Management: 0 device(s)

☑	Group Name	AP Model	Remark	IP Address ↑	Band	SSID	Number of Terminals	Power	Channel	Management Mode	Status	LED Indicator	Operation
☑	APGroup_Default	W80APV1.0	Access Point	10.10.96.25	2.4G 5G	IP-COM_A87328 IP-COM_A87328	0 0	[redacted]	[redacted]	Local Management	Online	Enable	Settings Delete
☑	APGroup_Default	W37APV1.0	W37APV1.0	10.10.96.169	2.4G 5G	IP-COM_A87328 IP-COM_A87328	0 0	[redacted]	[redacted]	Local Management	Online	Enable	Settings Delete

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

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

5) Click **OK**.



Mode Switch

Used to switch modes for the selected 2 APs.

Cloud Maintenance ● Enable ○ Disable

After the Cloud Maintenance function is enabled, a device can be associated by the ProFi Cloud Platform.

Management Mode: Cloud Hosting

Cloud Hosting: Functions can be configured through the cloud and the local web UI.
Local Hosting: The device can be normally associated with the cloud, but the cloud configuration information cannot be obtained. Configurations can be modified only after local login.

Unique Cloud Code: [redacted]

Device Info Report ● Enable ○ Disable

Note: If the Device Info Report function is disabled, the device cannot be managed by the cloud, and relevant functions in Cloud Maintenance are not available.

---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.

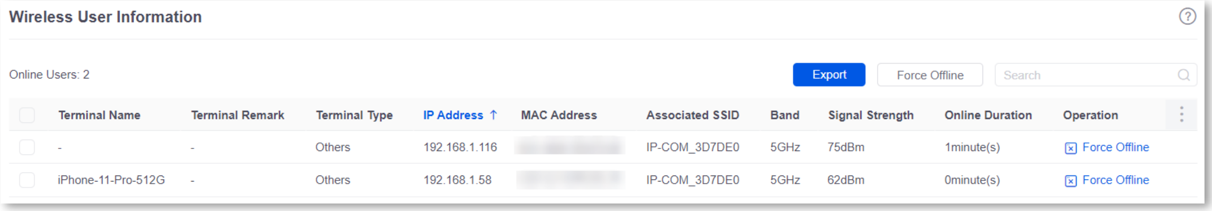
Parameter description

Parameter	Description
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 or ProFi App and all configurations must be performed on the web UI of the router or the APs.
Unique Cloud Code	Used to associate the device to the ProFi Cloud Management System. You can obtain it on the ProFi Cloud Platform (https://imsen.ip-com.com.cn) or the 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.

5.7 Wireless user information

Log in to the web UI of the router, and navigate to **AP** > **Wireless User Information** to enter the page.

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.



Wireless User Information

Online Users: 2

□	Terminal Name	Terminal Remark	Terminal Type	IP Address ↑	MAC Address	Associated SSID	Band	Signal Strength	Online Duration	Operation
□	-	-	Others	192.168.1.116	[redacted]	IP-COM_3D7DE0	5GHz	75dBm	1minute(s)	☒ Force Offline
□	iPhone-11-Pro-512G	-	Others	192.168.1.58	[redacted]	IP-COM_3D7DE0	5GHz	62dBm	0minute(s)	☒ Force Offline

5.8 Example of configuring fat APs

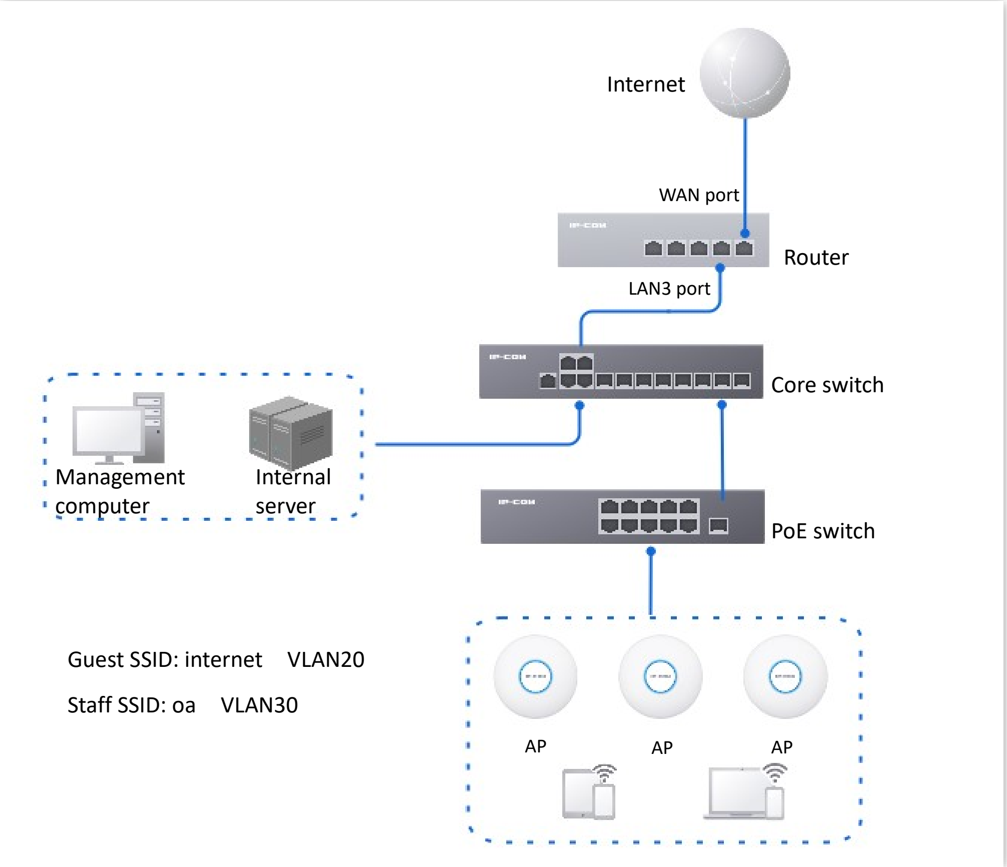
Networking requirements

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 Wi-Fi to the APs.
- Configure a Wi-Fi policy for guests. Assume that the SSID is **internet**, Wi-Fi password is **UmXmL9UK** and VLAN ID is **20**.
- Configure a Wi-Fi policy for staff. Assume that the SSID is **oa**, Wi-Fi password is **CetTLb8T** and VLAN ID is **30**.
- Configure a VLAN forwarding rule on the core switch.
- Configure a VLAN forwarding rule on the router and internal server.

The application scenarios are as follows.

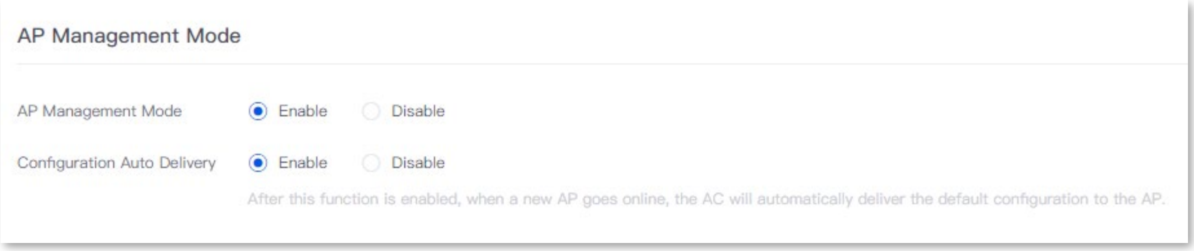


Configuration procedure

Configure the router > Configure the core switch > Configure the internal server

I. Configure the router

1. Log in to the web UI of the router.
2. (Skip if done) Manage APs.
   1) Navigate to **AP** > **AP Management Mode**.
   2) Enable the **AP Management Mode** and **Configuration Auto Delivery** functions.



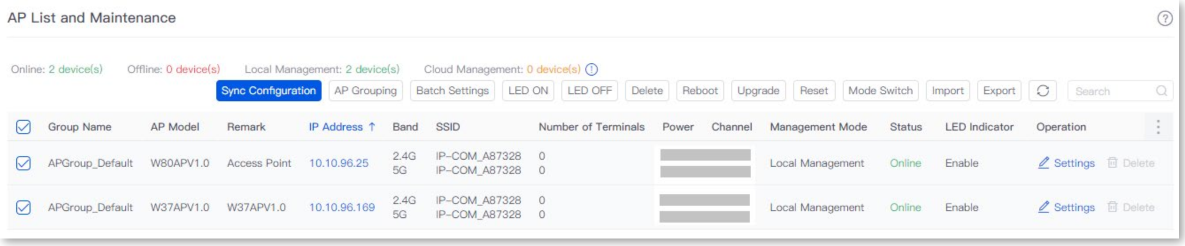
AP Management Mode

AP Management Mode ● Enable ○ Disable

Configuration Auto Delivery ● Enable ○ Disable

After this function is enabled, when a new AP goes online, the AC will automatically deliver the default configuration to the AP.

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



AP List and Maintenance

Online: 2 device(s)   Offline: 0 device(s)   Local Management: 2 device(s)   Cloud Management: 0 device(s)

☑	Group Name	AP Model	Remark	IP Address ↑	Band	SSID	Number of Terminals	Power	Channel	Management Mode	Status	LED Indicator	Operation
☑	APGroup_Default	W80APV1.0	Access Point	10.10.96.25	2.4G 5G	IP-COM_A87328 IP-COM_A87328	0 0	[redacted]		Local Management	Online	Enable	Settings Delete
☑	APGroup_Default	W37APV1.0	W37APV1.0	10.10.96.169	2.4G 5G	IP-COM_A87328 IP-COM_A87328	0 0	[redacted]		Local Management	Online	Enable	Settings Delete

3. Add the VLAN and configure the DHCP server.

Examples of VLAN parameters are shown below.

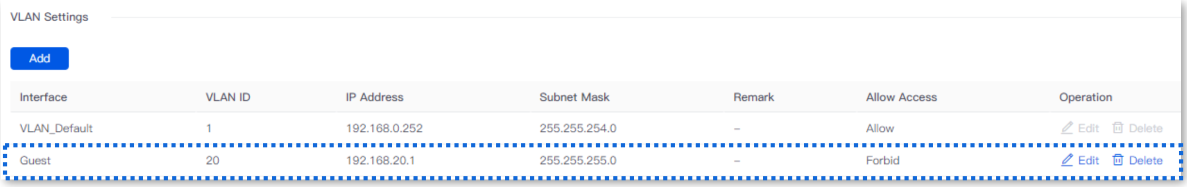
Interface	VLAN ID	IP Address/Subnet·Mask	Allow Access	Physical Port
Guest	20	192.168.20.1/24	Forbid	LAN (TAG)

Examples of DHCP server parameters are shown below.

Policy Name	Application Interface	DHCP Type	DHCP Configuration
Guest	Guest	User DHCP	IP Address Pool: 192.168.20.100 - 192.168.20.200 Subnet Mask: 255.255.255.0 Gateway: 192.168.20.1 Primary DNS: 192.168.20.1

1) Add VLANs.

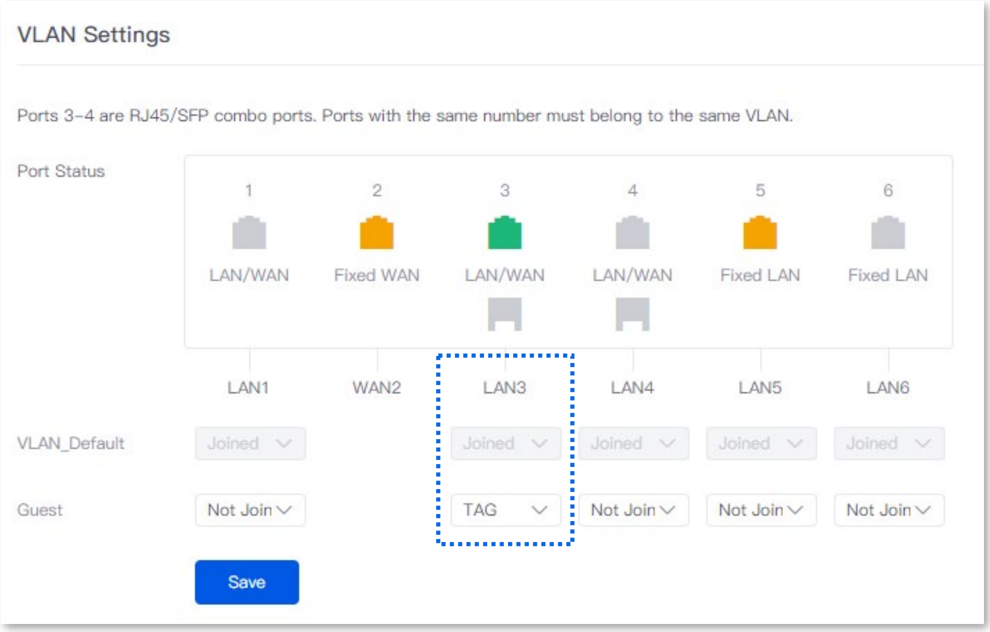
– Navigate to **Network** > **VLAN Settings,** click **Add** to configure related parameters of the VLAN, and click **Save**.



VLAN Settings

Interface	VLAN ID	IP Address	Subnet Mask	Remark	Allow Access	Operation
VLAN_Default	1	192.168.0.252	255.255.254.0	–	Allow	Edit Delete
Guest	20	192.168.20.1	255.255.255.0	–	Forbid	Edit Delete

– Select LAN port for the **Guest** VLAN, which is **LAN3** in this example, set VLAN policy to **TAG**. Then click **Save**.



VLAN Settings

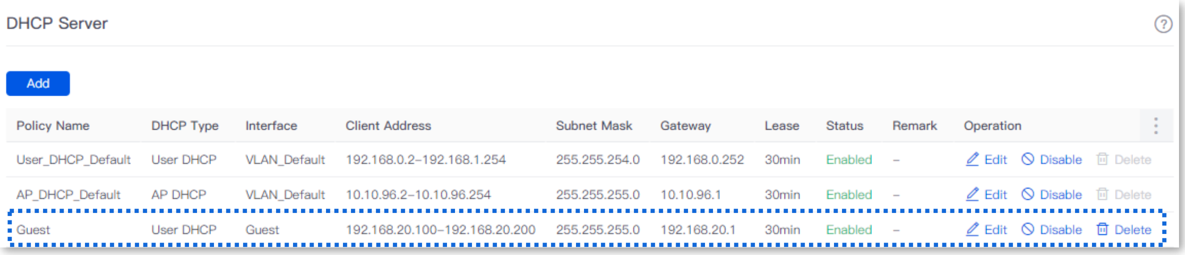
Ports 3–4 are RJ45/SFP combo ports. Ports with the same number must belong to the same VLAN.

Port Status

	LAN1	WAN2	LAN3	LAN4	LAN5	LAN6
VLAN_Default	Joined		Joined	Joined	Joined	Joined
Guest	Not Join		TAG	Not Join	Not Join	Not Join

2) Configure the DHCP server for the VLAN.

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



DHCP Server

Policy Name	DHCP Type	Interface	Client Address	Subnet Mask	Gateway	Lease	Status	Remark	Operation
User_DHCP_Default	User DHCP	VLAN_Default	192.168.0.2–192.168.1.254	255.255.254.0	192.168.0.252	30min	Enabled	–	Edit Disable Delete
AP_DHCP_Default	AP DHCP	VLAN_Default	10.10.96.2–10.10.96.254	255.255.255.0	10.10.96.1	30min	Enabled	–	Edit Disable Delete
Guest	User DHCP	Guest	192.168.20.100–192.168.20.200	255.255.255.0	192.168.20.1	30min	Enabled	–	Edit Disable Delete

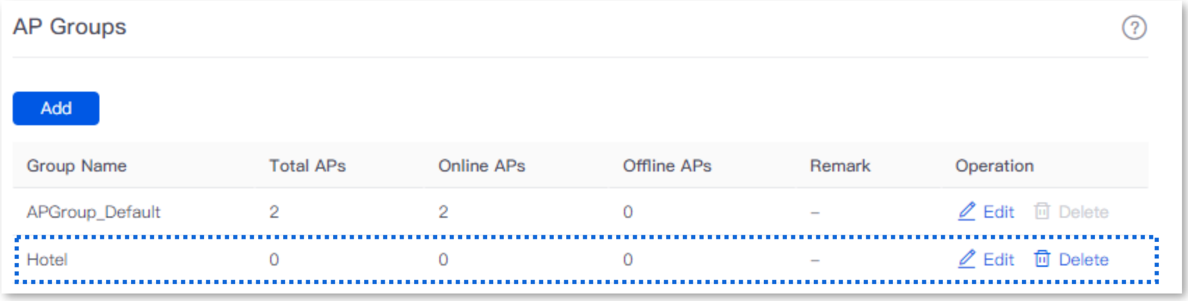
4. Configure the AP policy.

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

AP Group	Wi-Fi	AP VLAN
Hotel	AP Grouping: Hotel SSID: internet Security Mode: WPA2-PSK Wi-Fi Password: UmXmL9UK VLAN ID: 20	AP Grouping: Hotel AP VLAN: Enable Trunk port: LAN0
	AP Grouping: Hotel SSID: oa Security Mode: WPA2-PSK Wi-Fi Password: CetTLb8T VLAN ID: 30	

1) Configure the AP Group policy.

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



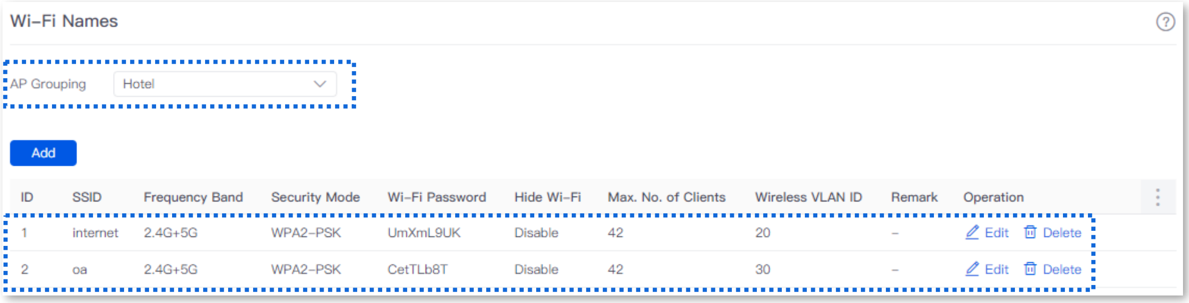
Group Name	Total APs	Online APs	Offline APs	Remark	Operation
APGroup_Default	2	2	0	–	Edit Delete
Hotel	0	0	0	–	Edit Delete

2) Configure the Wi-Fi policy.

Navigate to **AP** > **Wi-Fi Settings** > **Wi-Fi Names**, select **Hotel** for **AP Grouping**. Click **Add** to configure related parameters of the Wi-Fi policy, and click **Save**.

Tip

The maximum number of clients supported by the AP is 128. If multiple SSID policies need to be delivered to the same AP, you should plan the maximum number of clients appropriately to ensure that the maximum number of clients for each SSID policy does not exceed 128.

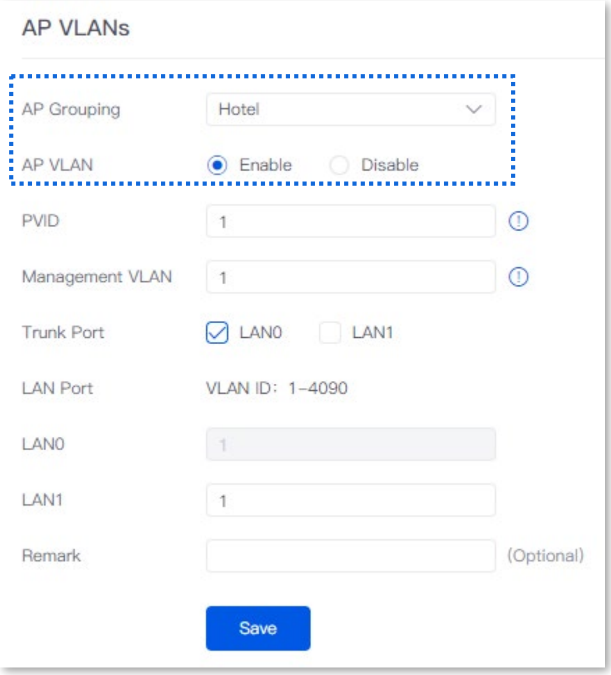


AP Grouping: Hotel

ID	SSID	Frequency Band	Security Mode	Wi-Fi Password	Hide Wi-Fi	Max. No. of Clients	Wireless VLAN ID	Remark	Operation
1	internet	2.4G+5G	WPA2-PSK	UmXmL9UK	Disable	42	20	–	Edit Delete
2	oa	2.4G+5G	WPA2-PSK	CetTLb8T	Disable	42	30	–	Edit Delete

3) Configure VLAN policy.

Navigate to **AP** > **Wi-Fi Settings** > **AP VLANs**, select **Hotel** for **AP Grouping**. Enable the **AP VLAN** function and set **Trunk Port** to **LAN0**, and click **Save**.



AP VLANs

AP Grouping: Hotel

AP VLAN: ● Enable ○ Disable

PVID: 1

Management VLAN: 1

Trunk Port: ☑ LAN0 □ LAN1

LAN Port: VLAN ID：1–4090

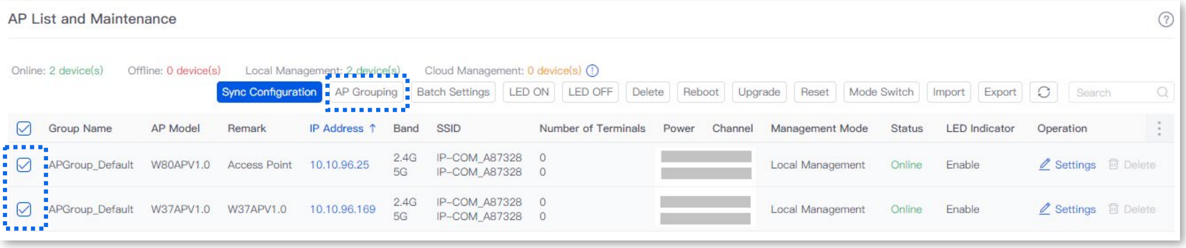
LAN0: 1

LAN1: 1

Remark: (Optional)

5. Deliver the AP group policy.

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

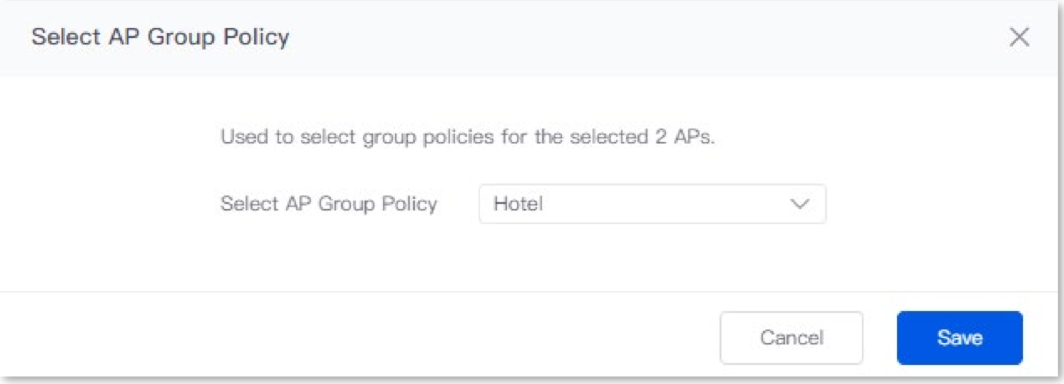


AP List and Maintenance

Online: 2 device(s) Offline: 0 device(s) Local Management: 2 device(s) Cloud Management: 0 device(s)

☑	Group Name	AP Model	Remark	IP Address ↑	Band	SSID	Number of Terminals	Power	Channel	Management Mode	Status	LED Indicator	Operation
☑	APGroup_Default	W80APV1.0	Access Point	10.10.96.25	2.4G 5G	IP-COM_A87328 IP-COM_A87328	0 0	[redacted]	[redacted]	Local Management	Online	Enable	Settings Delete
☑	APGroup_Default	W37APV1.0	W37APV1.0	10.10.96.169	2.4G 5G	IP-COM_A87328 IP-COM_A87328	0 0	[redacted]	[redacted]	Local Management	Online	Enable	Settings Delete

   2) Select the AP group policy, and click **Save.** The following figure is for reference only.



Select AP Group Policy

Used to select group policies for the selected 2 APs.

Select AP Group Policy: Hotel

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
AP	20,30	Trunk	1
Router	20	Trunk	1
Internal Server	30	Access	30

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 core switch and configure the DHCP server.

1. Add VLANs. The parameters shown below are for reference only.

VLAN Name	VLAN ID	IP Address/Subnet·Mask	Physical Port
Staff	30	192.168.30.1/24	LAN

2. Configure the user DHCP server for the VLAN. The parameters shown below are for reference only.

Policy Name	User DHCP
Staff	Client Address: 192.168.30.100 - 192.168.30.200 Subnet Mask: 255.255.255.0 Gateway: 192.168.30.1 Primary DNS: 192.168.30.1

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

Port Connected to	VLAN ID（VLAN Allowed to Pass）	Port Property	PVID
Switch	30	Access	30

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

---End

Verification

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

5.9 IPTV

5.9.1 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.

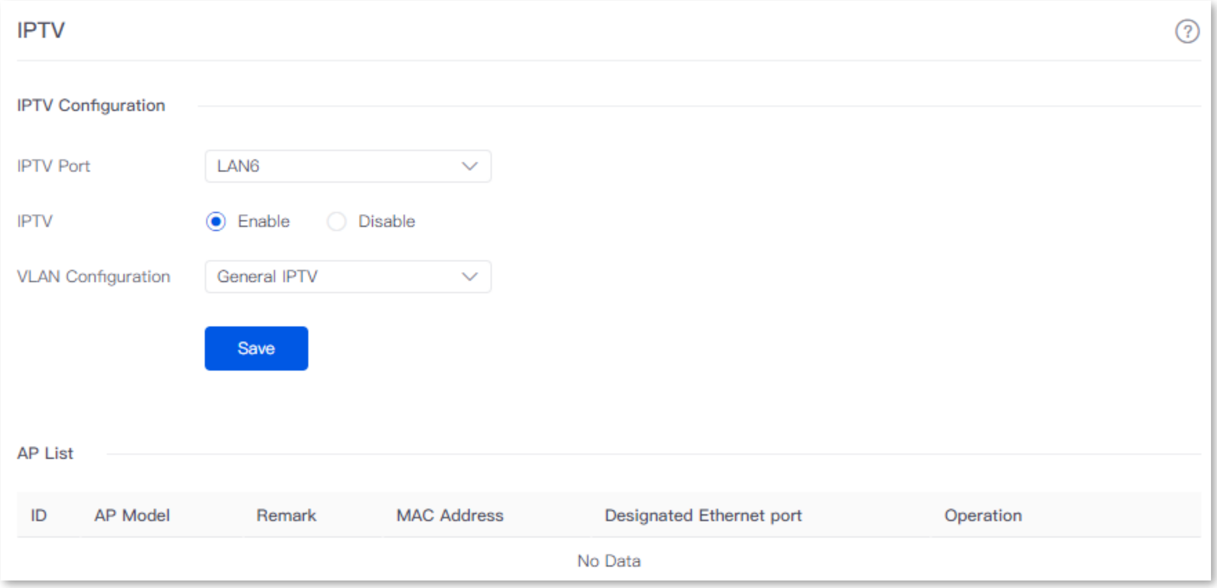
With the IPTV function, you can set up an IPTV data pass-through channel between the device and the AP to solve the difficult connection problem caused by the long distance between the IPTV set-top box and the optical modem.

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 the IPTV function.

Log in to the web UI of the router, and navigate to **AP** > **IPTV** to enter the page. This function is disabled by default. The following displays the page when the function is enabled.



IPTV

IPTV Configuration

IPTV Port: LAN6

IPTV: ● Enable ○ Disable

VLAN Configuration: General IPTV

Save

AP List

ID	AP Model	Remark	MAC Address	Designated Ethernet port	Operation
No Data					

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 Port Information on the **System** page for the LAN port number.

Parameter		Description
	IPTV	Used to enable or disable the IPTV data pass-through function.
	VLAN Configuration	Specifies the VLAN ID of the IPTV service. – If the broadband service provider does not provide VLAN-related information when activating the IPTV service, select **General IPTV**, or select **Customize VLAN** and select **Without VLAN Tag**. – If the broadband service provider provides a **VLAN ID** when activating the IPTV service, select **Customize VLAN** and **With VLAN Tag**, and enter the corresponding **VLAN ID**.
AP List	AP Model	Specifies the product model of the AP. Only APs that support IPTV are displayed in the AP list.
	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 **LAN1**.

5.9.2 Watch IPTV programs

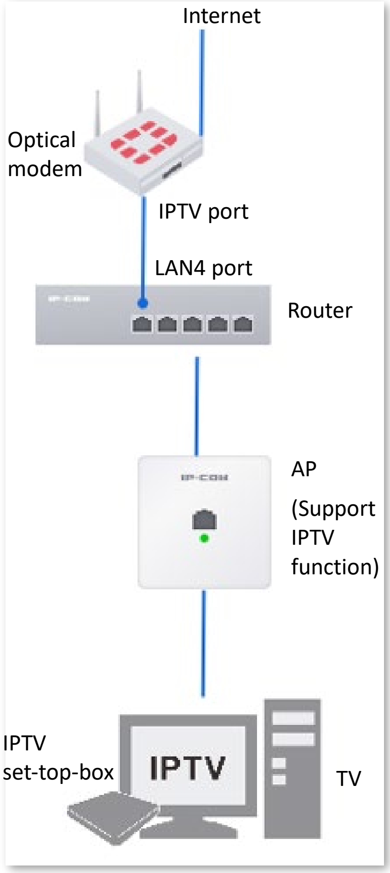
Networking requirements

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

Requirements: Watching IPTV programs.

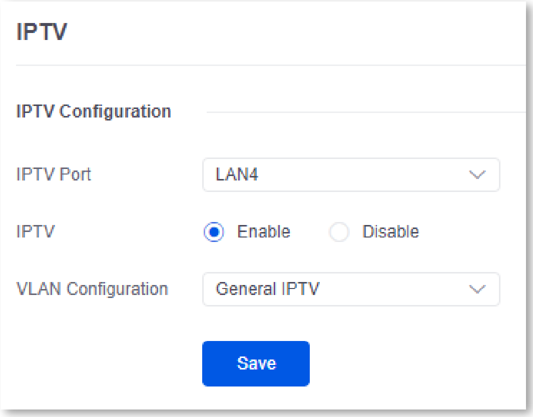
Solution

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.
   4) Select the router as the LAN port of IPTV, which is **LAN4** in this example.
   5) Enable the **IPTV** function.
   6) Set **VLAN Configuration**, which is **General IPTV** in this example.
   7) Click **Save**.



IPTV

IPTV Configuration

IPTV Port: LAN4

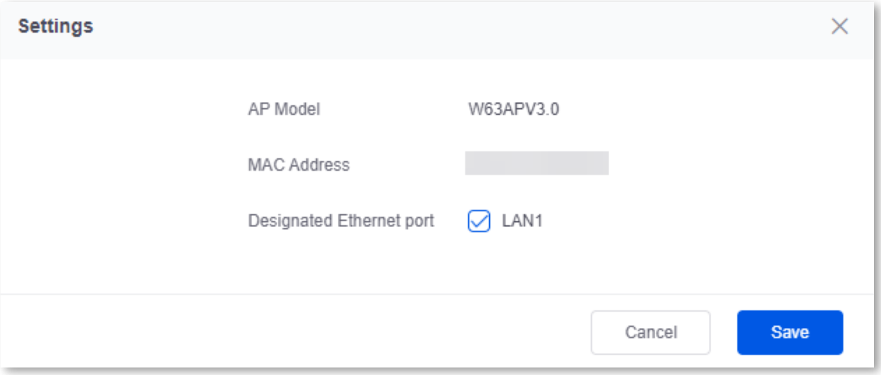
IPTV: ● Enable ○ Disable

VLAN Configuration: General IPTV

2. Designate AP as the wired Ethernet port of the IPTV port. The following figure is for reference only.

   1) Choose the AP to be connected to the IPTV set-top box and click ✎ .

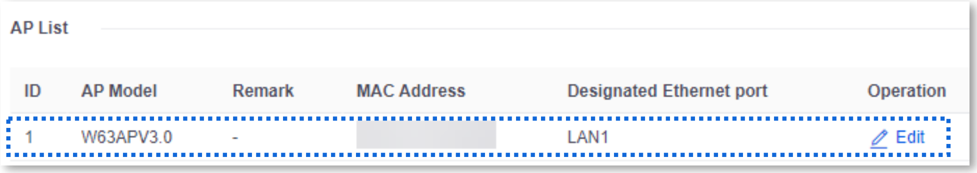
   2) Tick the **Designated Ethernet Port** and click **Save**.



Settings

AP Model	W63APV3.0
MAC Address	
Designated Ethernet port	☑ LAN1

The LAN1 port of the AP is designated successfully.



AP List

ID	AP Model	Remark	MAC Address	Designated Ethernet port	Operation
1	W63APV3.0	-		LAN1	✎ Edit

3. Set your IPTV set-top box.

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

---End

Verification

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

5.9.3 Access the internet & Watch IPTV programs

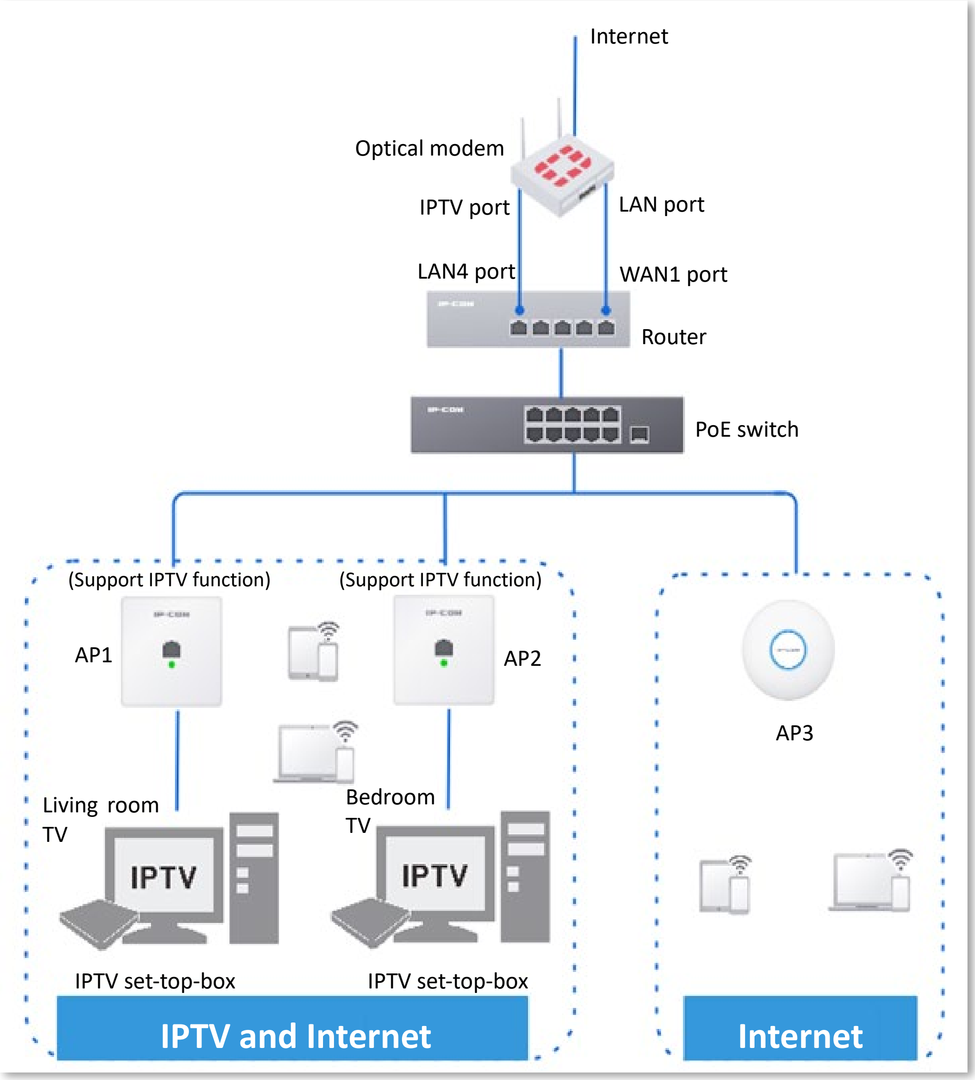
Networking requirements

The IPTV service is included in a hotel broadband service. The ISP provides an IPTV user name and password, and the VLAN ID of the IPTV service (VLAN ID 10 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 the VLAN function of the switch to achieve the above requirements.

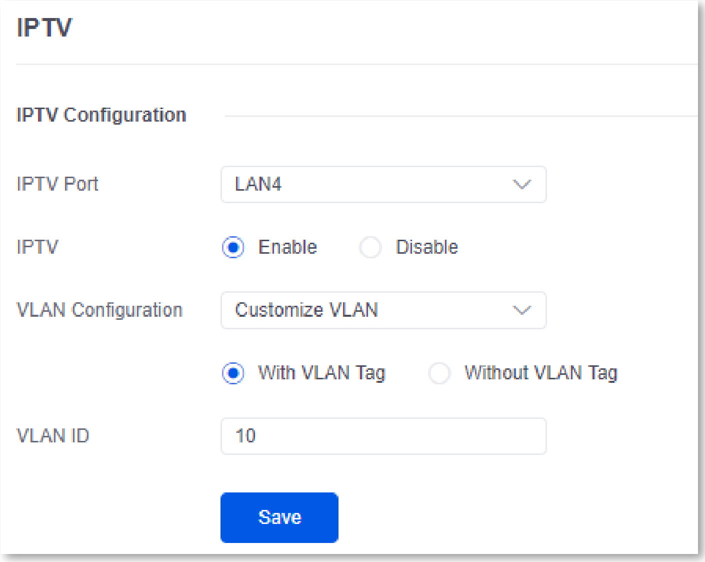

Internet
Optical modem
IPTV port
LAN port
LAN4 port
WAN1 port
Router
PoE switch
(Support IPTV function)
(Support IPTV function)
AP1
AP2
AP3
Living room TV
Bedroom TV
IPTV
IPTV
IPTV set-top-box
IPTV set-top-box
IPTV and Internet
Internet

Configuration procedure

I. Set up IPTV

1. 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 the IPTV IN port.
   4) Select the router as the LAN port of the IPTV IN port, which is LAN4 in this example.
   5) Enable the **IPTV** function.
   6) Select **Customize VLAN** for **VLAN Configuration**, select **With VLAN Tag**, and enter 10 for **VLAN ID**.
   7) Click **Save**.



IPTV

IPTV Configuration

IPTV Port: LAN4

IPTV: ● Enable ○ Disable

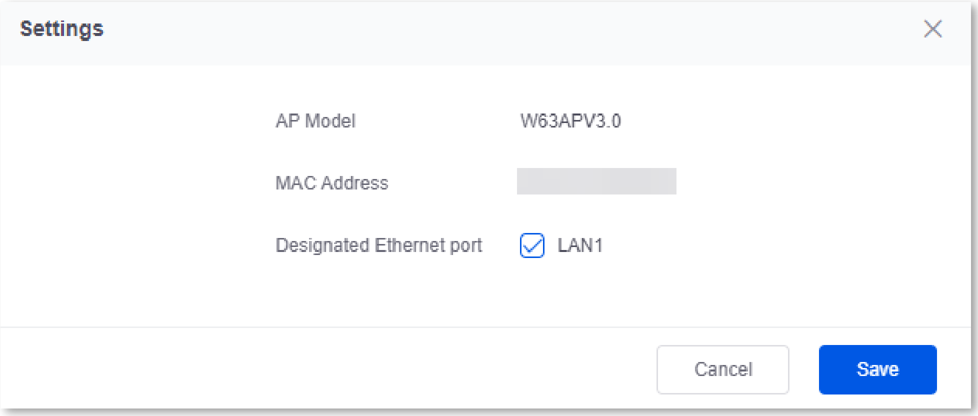
VLAN Configuration: Customize VLAN

● With VLAN Tag ○ Without VLAN Tag

VLAN ID: 10

2. Designate a wired Ethernet port of the AP1 (support IPTV function).

   1) Select the AP1 to be connected to the IPTV set-top box and click ✎ .
   2) Tick the **Designated Ethernet Port** and click **Save**.



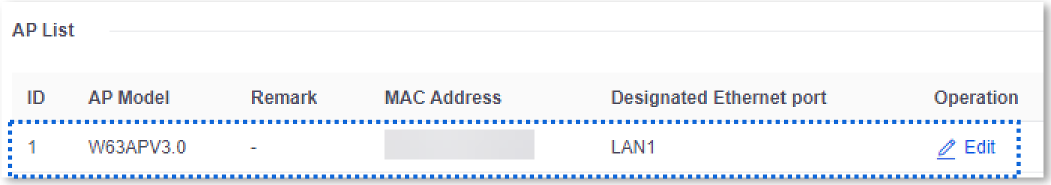
Settings

AP Model: W63APV3.0

MAC Address: [redacted]

Designated Ethernet port: ☑ LAN1

The LAN1 port of the AP is designated successfully.



AP List

ID	AP Model	Remark	MAC Address	Designated Ethernet port	Operation
1	W63APV3.0	-	[redacted]	LAN1	Edit

3) Repeat sub-step 4 of step **1** to designate other wired Ethernet port of AP2 (support IPTV function).

3. Set your IPTV set-top box.

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

---End

II. Set up internet

Refer to the internet settings to connect your router online.

Verification

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

5.10 Wi-Fi optimization

Log in to the web UI of the router, and navigate to **AP** > **Wi-Fi Optimization** to enter the page.

On this page, you can improve wireless network performance for an AP either by adjusting its power, channel and band or enabling auto/scheduled optimization.

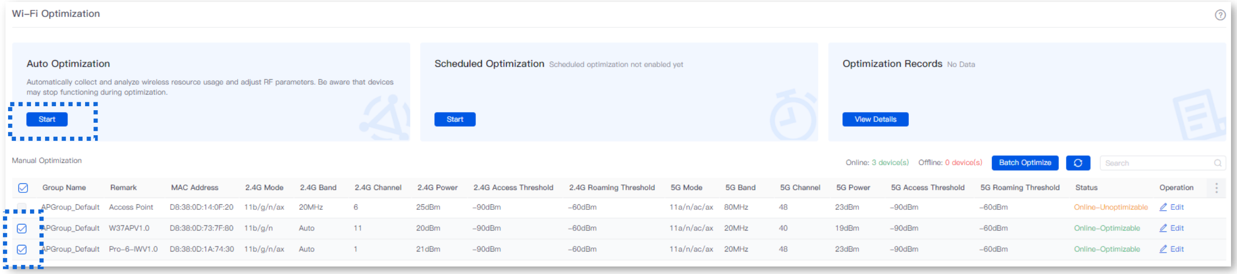
Tip

- There must be at least 2 APs in the AP group that support the Wi-Fi optimization function
- During optimization, wireless connection may be interrupted. Operate when APs are idle.

5.10.1 Run instant auto optimization on wireless networks

Auto optimization allows network administrators to assess the performance of the wireless network and employ optimization strategies accordingly.

In the **Auto Optimization** module, click **Start**.



Automatically collect and analyze wireless resource usage and adjust RF parameters. Be aware that devices may stop functioning during optimization.

Scheduled optimization not enabled yet

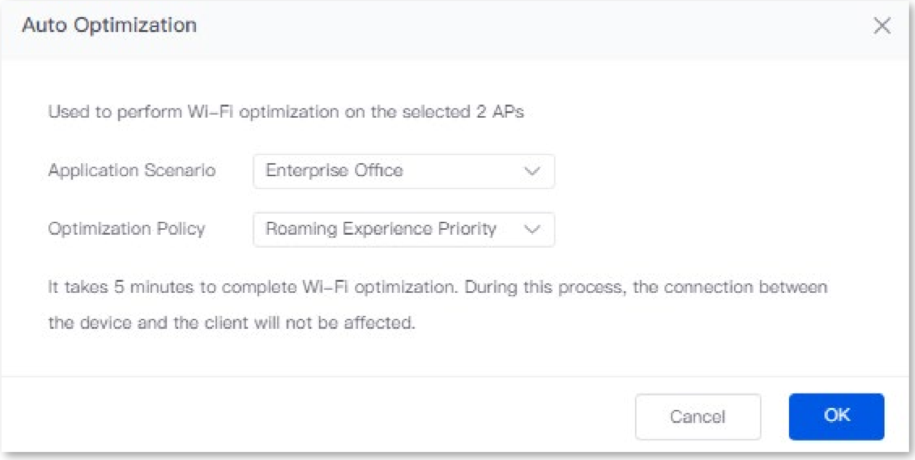
No Data

Manual Optimization

Online: 3 device(s) Offline: 0 device(s)

☑	Group Name	Remark	MAC Address	2.4G Mode	2.4G Band	2.4G Channel	2.4G Power	2.4G Access Threshold	2.4G Roaming Threshold	5G Mode	5G Band	5G Channel	5G Power	5G Access Threshold	5G Roaming Threshold	Status	Operation
□	APGroup_Default	Access Point	D8:38:0D:14:0F:20	11b/g/n/ax	20MHz	6	25dBm	-90dBm	-60dBm	11a/n/ac/ax	80MHz	48	23dBm	-90dBm	-60dBm	Online-Unoptimizable	Edit
☑	APGroup_Default	W37APV1.0	D8:38:0D:73:7F:80	11b/g/n	Auto	11	20dBm	-90dBm	-60dBm	11a/n/ac/ax	20MHz	40	19dBm	-90dBm	-60dBm	Online-Optimizable	Edit
☑	APGroup_Default	Pro-6-IWV1.0	D8:38:0D:1A:74:30	11b/g/n/ax	Auto	1	21dBm	-90dBm	-60dBm	11a/n/ac/ax	20MHz	48	23dBm	-90dBm	-60dBm	Online-Optimizable	Edit

Configure **Application Scenario** and **Optimization Policy**, click **OK**.



Used to perform Wi-Fi optimization on the selected 2 APs

Application Scenario: Enterprise Office

Optimization Policy: Roaming Experience Priority

It takes 5 minutes to complete Wi-Fi optimization. During this process, the connection between the device and the client will not be affected.

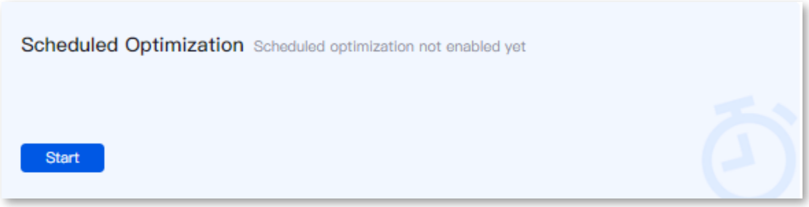
Parameter description

Parameter	Description
Application Scenario	Select the application scenario as required.
Optimization Policy	Used to select an appropriate optimization policy. – **Roaming Experience Priority**: Prioritize roaming experience. It can be used in scenarios with high AP deployment density, maximizing the roaming experience and ensuring that clients connect to APs with good signals, which may reduce the maximum coverage of the wireless network. – **Coverage Priority**: Prioritize Wi-Fi coverage. It can be used in scenarios with low AP deployment density, maximizing coverage and ensuring that clients successfully connect to APs as much as possible, which may reduce the roaming sensitivity.

5.10.2 Run scheduled auto optimization on wireless networks

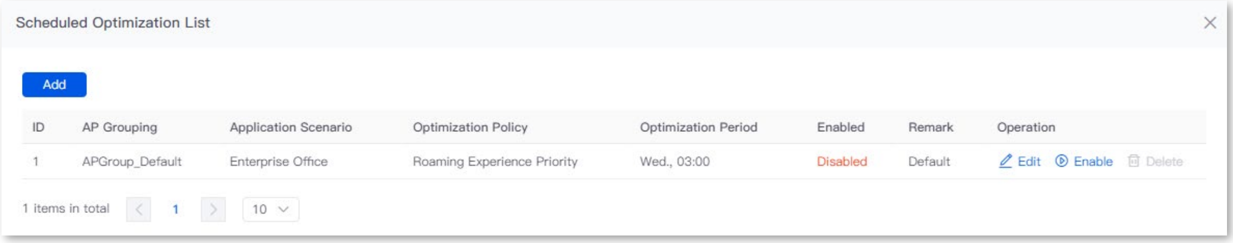
Scheduled optimization allows network administrators to perform wireless network optimization at the scheduled time.

In the **Scheduled Optimization** module, click **Start**.



Scheduled Optimization Scheduled optimization not enabled yet

By default, the router has created an optimization policy named **APGroup_Default** that is disabled. You can click **Add** to add a new policy.



Scheduled Optimization List

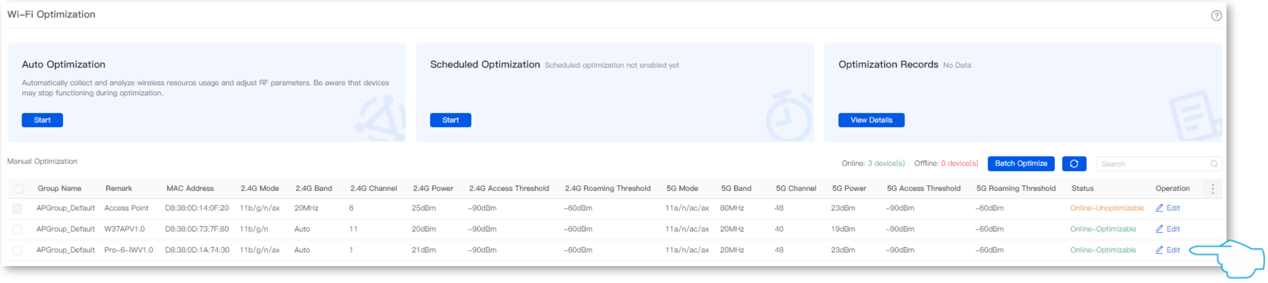
ID	AP Grouping	Application Scenario	Optimization Policy	Optimization Period	Enabled	Remark	Operation
1	APGroup_Default	Enterprise Office	Roaming Experience Priority	Wed., 03:00	Disabled	Default	Edit Enable Delete

1 items in total < 1 > 10

5.10.3 Enable manual optimization on wireless networks

Log in to the web UI of the router, and navigate to **AP** > **Wi-Fi Optimization** to enter the page.

On this page, you can manually configure wireless parameters such as channel, bandwidth and transmit power to optimize wireless network.



Wi-Fi Optimization

Auto Optimization

Automatically collect and analyze wireless resource usage and adjust RF parameters. Be aware that devices may stop functioning during optimization.

Scheduled Optimization Scheduled optimization not enabled yet

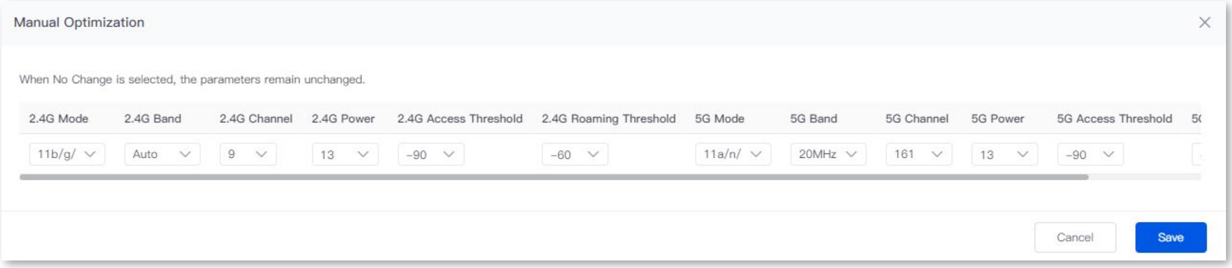
Optimization Records No Data

Manual Optimization

Online: 3 device(s) Offline: 0 device(s)

□	Group Name	Remark	MAC Address	2.4G Mode	2.4G Band	2.4G Channel	2.4G Power	2.4G Access Threshold	2.4G Roaming Threshold	5G Mode	5G Band	5G Channel	5G Power	5G Access Threshold	5G Roaming Threshold	Status	Operation
□	APGroup_Default	Access Point	D8:38:0D:14:0F:20	11b/g/n/ax	20MHz	6	25dBm	-90dBm	-60dBm	11a/n/ac/ax	80MHz	48	23dBm	-90dBm	-60dBm	Online-Unoptimizable	Edit
□	APGroup_Default	W37APV1.0	D8:38:0D:73:7F:80	11b/g/n	Auto	11	20dBm	-90dBm	-60dBm	11a/n/ac/ax	20MHz	40	19dBm	-90dBm	-60dBm	Online-Optimizable	Edit
□	APGroup_Default	Pro-6-IWV1.0	D8:38:0D:1A:74:30	11b/g/n/ax	Auto	1	21dBm	-90dBm	-60dBm	11a/n/ac/ax	20MHz	48	23dBm	-90dBm	-60dBm	Online-Optimizable	Edit

Click **Edit** of the AP you want to manually optimize wireless network. Modify the wireless parameters such as channel, bandwidth and transmit power as required, and click **Save**. The following figure is for reference only.



Manual Optimization

When No Change is selected, the parameters remain unchanged.

2.4G Mode	2.4G Band	2.4G Channel	2.4G Power	2.4G Access Threshold	2.4G Roaming Threshold	5G Mode	5G Band	5G Channel	5G Power	5G Access Threshold	5(
11b/g/	Auto	9	13	-90	-60	11a/n/	20MHz	161	13	-90	

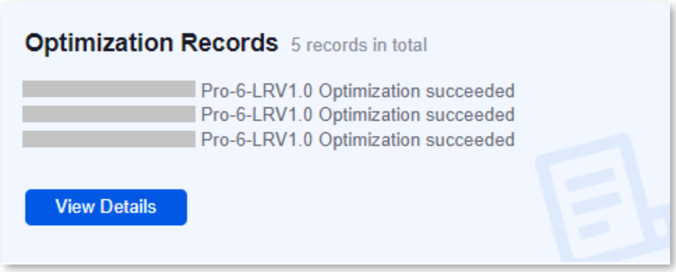
Parameter description

Parameter	Description
2.4G Access Threshold	When the 5G Preferred function is enabled, if the AP's 5GHz signal strength is below this value, dual-band clients are steered to the 2.4GHz network.
2.4G Disconnect Threshold	The minimum 2.4 GHz signal strength required to maintain a connection. If the signal falls below this value, the client disconnects and roams to an AP with a stronger signal.
5G Access Threshold	When the 5G Preferred function is enabled, dual-band clients connect to the 5 GHz band if the AP's received 5 GHz signal strength meets or exceeds this value.
5G Disconnect Threshold	The minimum 5 GHz signal strength required to maintain the current AP connection. If the signal falls below this value, the client disconnects and roams to an AP with a stronger signal.

5.10.4 View optimization records

In the **Optimization Record** module, you can view records that contain detailed information about each optimization task you performed.

Up to 3 records are displayed. To view more records, click **View Details**.



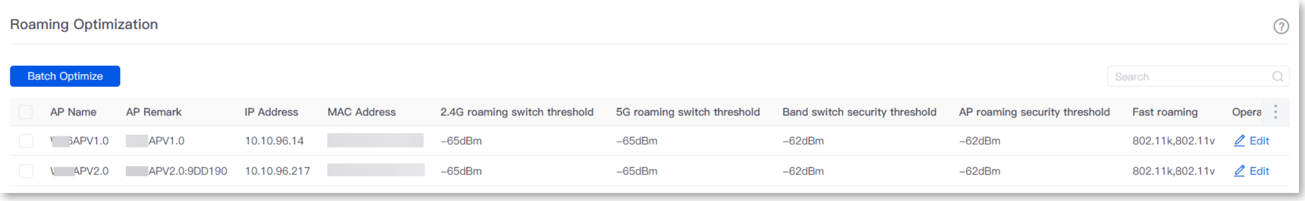
Optimization Records 5 records in total

[redacted] Pro-6-LRV1.0 Optimization succeeded
[redacted] Pro-6-LRV1.0 Optimization succeeded
[redacted] Pro-6-LRV1.0 Optimization succeeded

5.11 Roaming optimization

Log in to the web UI of the router, and navigate to **AP** > **Roaming Optimization** to enter the page.

On this page, you can optimize the roaming performance of the AP by adjusting the roaming threshold between the AP and the client to achieve a better roaming experience and create a high-quality wireless network.



Roaming Optimization

□	AP Name	AP Remark	IP Address	MAC Address	2.4G roaming switch threshold	5G roaming switch threshold	Band switch security threshold	AP roaming security threshold	Fast roaming	Opera
□	[redacted]APV1.0	[redacted]APV1.0	10.10.96.14	[redacted]	-65dBm	-65dBm	-62dBm	-62dBm	802.11k,802.11v	Edit
□	[redacted]APV2.0	[redacted]APV2.0:9DD190	10.10.96.217	[redacted]	-65dBm	-65dBm	-62dBm	-62dBm	802.11k,802.11v	Edit

Parameter description

Parameter	Description
2.4G Roaming Switch Threshold	The signal strength level at which a client roams from the current AP to a nearby AP with a stronger signal on the 2.4 GHz or 5 GHz band.
5G Roaming switch Threshold	
Band switch security threshold	If the AP's received signal strength on the current band (2.4 GHz or 5 GHz) falls below this value, the client automatically switches to the other band.
AP roaming security threshold	The signal strength threshold at which a connected client roams from the current AP to another AP with a stronger signal.
Fast Roaming	Wireless roaming refers to a client device automatically connecting to the AP with the better signal and disconnecting from the original AP when it moves to a border area between the coverage areas of two or more APs. This is provided that the APs have the same Wi-Fi name, security mode, and Wi-Fi password. – **802.11k**: Wireless LAN Spectrum Resource Measurement Protocol. When enabled, it assists clients in scanning for potential APs in the environment, resolving the question of whether and when roaming is necessary. – **802.11v**: Wireless Network Management Protocol. When enabled, it assists clients in selecting target APs, resolving the issue of which AP to roam to. – **802.11r**: Fast BSS Switching Protocol. Enabling it eliminates the handshake overhead during wireless reassociation, reduces roaming time, and solves the problem of how to roam quickly.

6 Configure authentication

Features available in the router may vary by model and software version. Router availability may also vary by region or ISP. All images, steps, and descriptions in this guide are only examples and may not reflect your actual router experience.

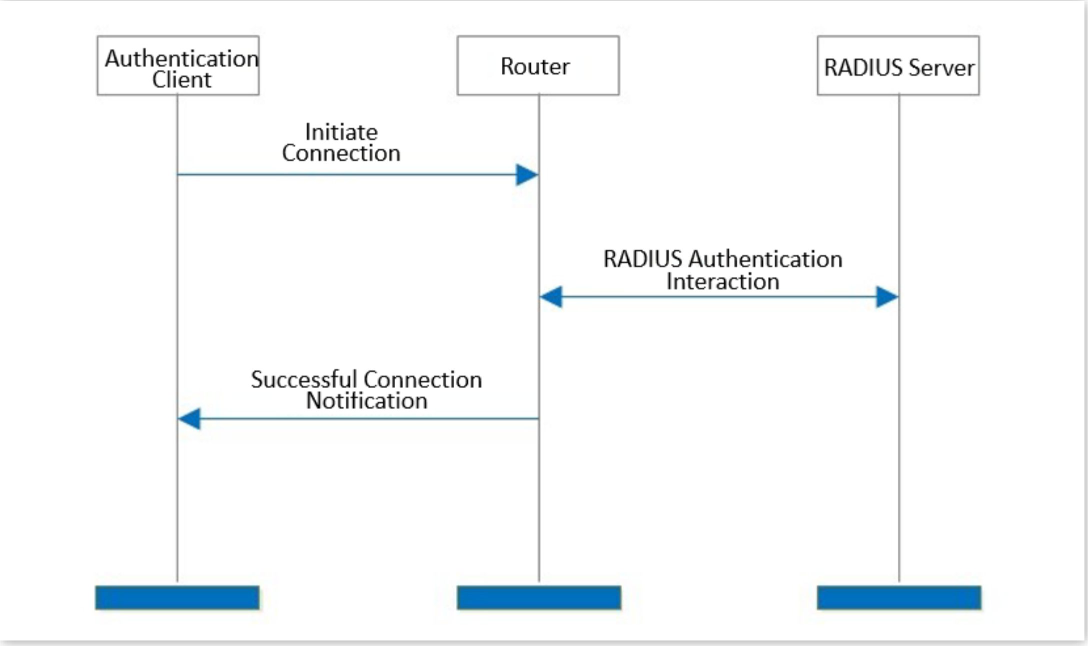
6.1 Overview

By default, when the router is connected to the internet, the LAN users can access the internet. With the Authentication function enabled, clients connected to the authentication network can access the internet only after successful authentication. If a client is reconnected to the router after successful authentication, the client may be required to perform authentication again. The guest policies of this router take effect based on the VLAN interface.

The router supports authentication using both the local server and external server.

- Local authentication: When enabled, the user authentication is completed on the local router. The authentication users are saved on the local router and the portal customization is also generated on the local router.
- External authentication: When enabled, the external RADIUS server completes user authentication and billing.

The external server works as follows:


Authentication Client
Router
RADIUS Server
Initiate Connection
RADIUS Authentication Interaction
Successful Connection Notification

1. The authentication client uses HTTP to initiate a connection request.
2. The router will request redirection to the local portal customization, and the user enters the user name and password on the portal customization.
3. Based on the user name and password, the router performs RADIUS authentication interaction with RADIUS server for user authentication and charging.
4. The router notifies the authentication client that the online connection is successful.

6.2 Configuration wizard

6.2.1 Local authentication

Procedure	Task	Description
1	Configure authentication templates	Required. Manually create a portal customization.
2	Configure authentication type	Required. Configure one or multiple authentication types based on actual requirements.
3	Configure time policy	Required. Configure the time policy based on actual requirements.
4	Configure guest policy	Required.
5	Configure charging policy	Optional. When configuring an authenticated account, you can select a charging policy to charge for traffic as needed.
6	Configure authentication account	Optional. If the **Authentication Type** is **Account** or **Random Code**, the authentication account must be configured.
7	Configure authentication-free hosts	Optional. To enable the devices to connect to the internet without authentication, the authentication-free host must be configured.

Tip

To use PPPoE authentication, configure the PPPoE server and enable captive portal (required), configure charging policy (optional), configure authentication account (required), configure authentication-free hosts (optional), and disable DHCP server under the PPPoE server interface (required).

6.2.2 External authentication

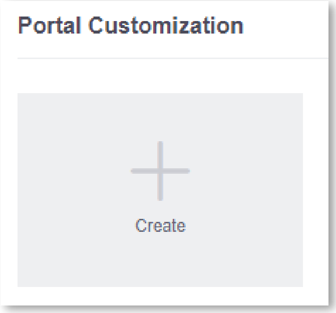
Procedure	Task	Description
1	Configure VPN client	Required. Configure the router as a VPN client to dial into the RADIUS server.
2	Configure authentication templates	Required. Manually create a portal customization.
3	Configure account authentication	Required. Configure account authentication based on actual requirements.
4	Configure time policy	Required. Configure the time policy based on actual requirements.
5	Configure Radius server	Required. Configure the authentication and accounting policies for the external server based on actual requirements.
6	Configure guest policy	Required.
7	Configure authentication-free hosts	Optional. To enable the devices to connect to the internet without authentication, the authentication-free host must be configured.

6.3 Configure authentication templates

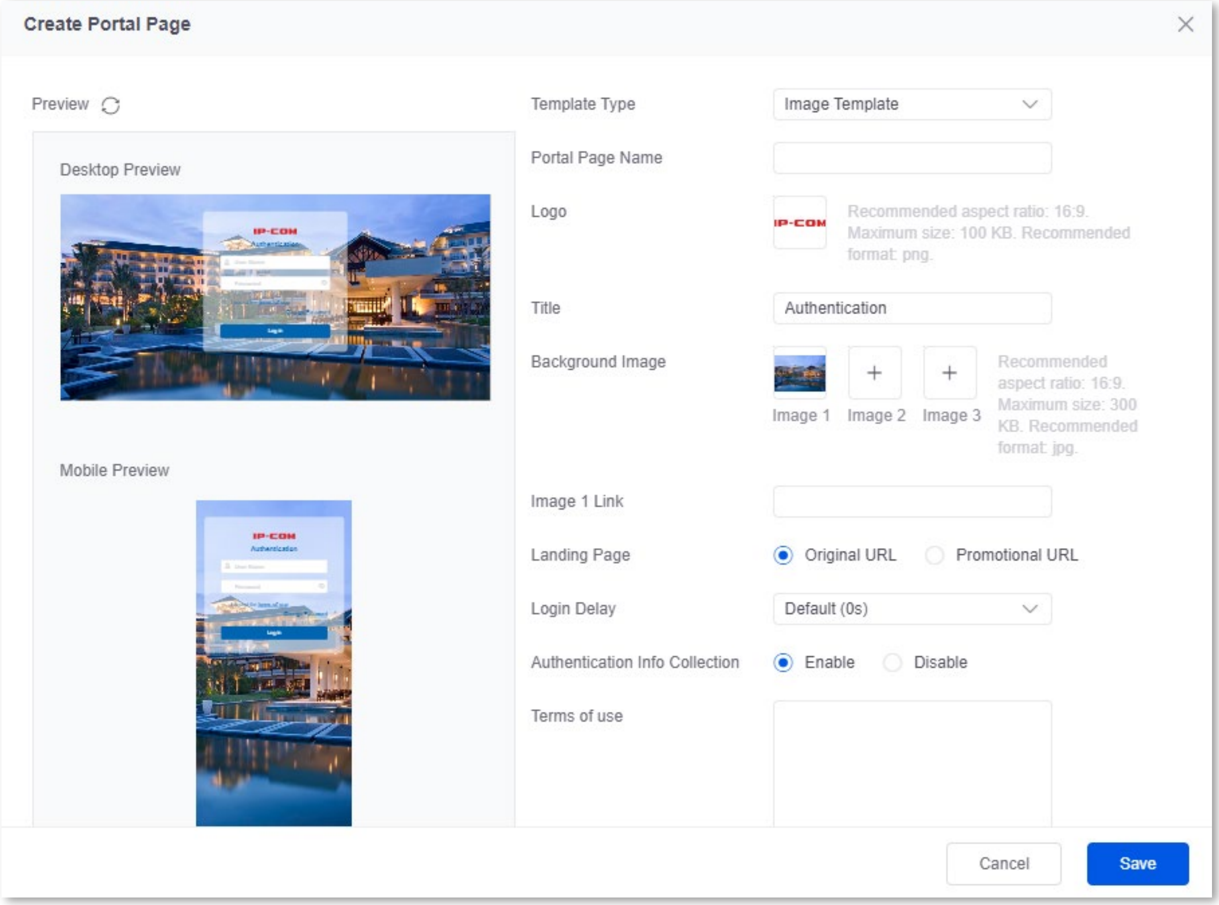
6.3.1 Image template

The image template can be used for SMS authentication, email authentication, account authentication, no authentication and random code authentication. An image template has been preset in the system. You can edit based on the preset template or create a new one.

To add an image template, log in to the web UI of the router, navigate to **AuthN** > **Authentication Template** > **Portal Customization**, and click **Create**.



Portal Customization



Create Portal Page

Template Type: Image Template

Portal Page Name:

Logo: IP-COM Recommended aspect ratio: 16:9. Maximum size: 100 KB. Recommended format: png.

Title: Authentication

Background Image: Image 1 Image 2 Image 3 Recommended aspect ratio: 16:9. Maximum size: 300 KB. Recommended format: jpg.

Image 1 Link:

Landing Page: ● Original URL ○ Promotional URL

Login Delay: Default (0s)

Authentication Info Collection: ● Enable ○ Disable

Terms of use:

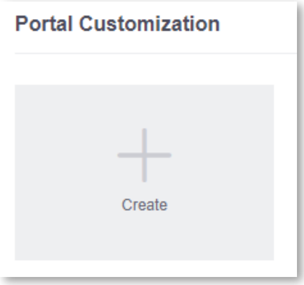
Parameter description

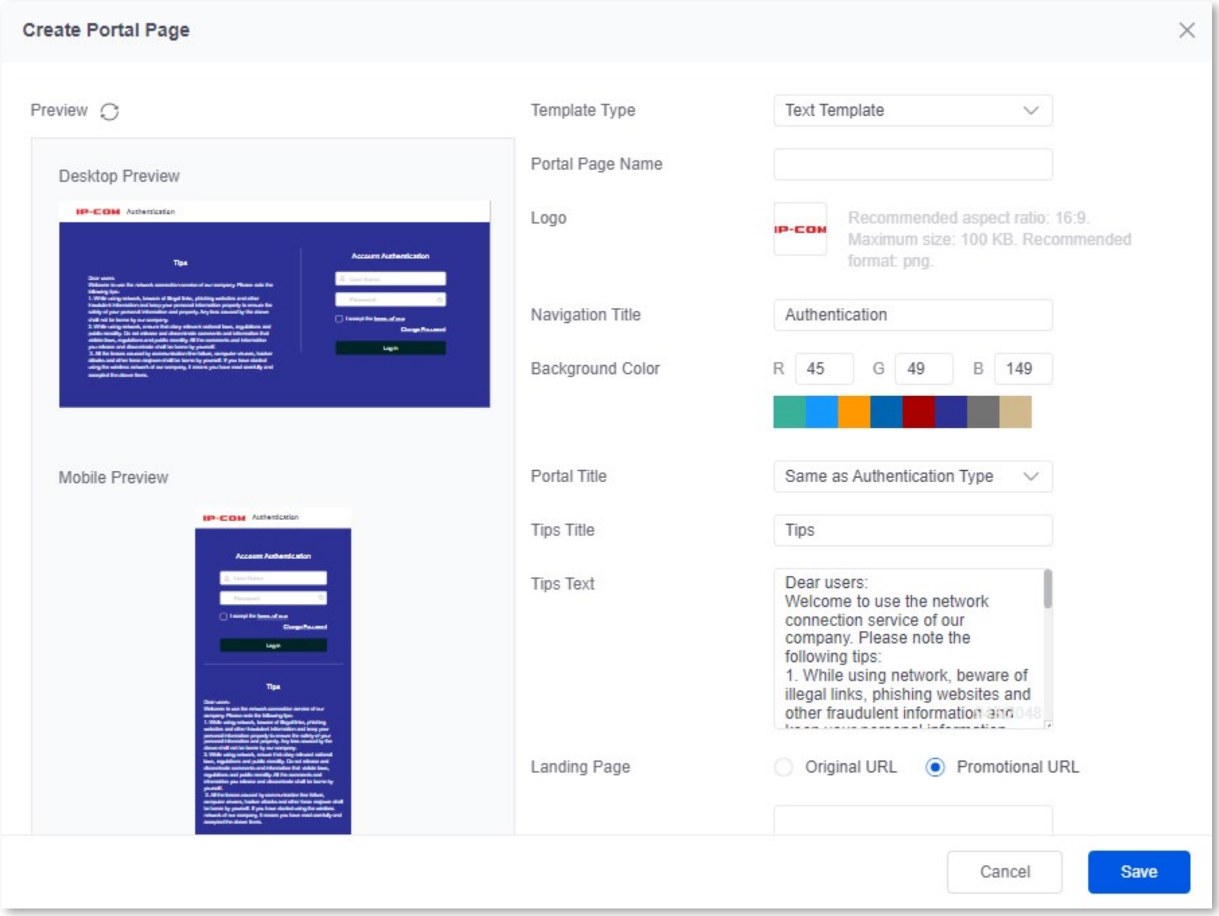
Parameter	Description
Background Image	Specifies the background images of the portal page. You can upload at most three images. 💡 Tip – This parameter is available only when the **Template Type** is set to **Image Template**. – When two or three background images are uploaded, the images will be displayed in turn on the portal page.
Image 1 Link/ Image 2 Link/ Image 3 Link	Specifies the URL linked to the corresponding background image. After the configuration is completed, you can access the website by clicking the corresponding background image on the portal page. 📝 Note – This parameter is available only when the **Template Type** is set to **Image Template**. – The link must be an http URL, otherwise, the function will not take effect.
Landing Page	Specifies the web address that users are automatically redirected to after passing the authentication. – **Original URL**: After users pass the authentication, the browser redirects to the website that users visited before the authentication. For example, if the user is visiting Google when being redirected to the portal page, the user will be redirected back to Google after passing the authentication. – **Promotional URL**: After users pass the authentication, the browser redirects to the address specified here.
Login Delay	Specifies the delay time before login. By default, the delay time is **Default (0s).**
Authentication Info Collection	Used to enable or disable the authentication information collection function.
Terms of use	Specifies the disclaimer information on the web portal page. Users must agree and tick the disclaimer before logging in.

6.3.2 Text template

The text template can be used for SMS authentication, email authentication, account authentication, no authentication and random code authentication. You can create a text template for authentication as required.

To add a text template, log in to the web UI of the router, navigate to **AuthN** > **Authentication Template** > **Portal Customization**, and click **Create**.





Template Type: Text Template

Portal Page Name:

Logo: Recommended aspect ratio: 16:9. Maximum size: 100 KB. Recommended format: png.

Navigation Title: Authentication

Background Color: R 45 G 49 B 149

Portal Title: Same as Authentication Type

Tips Title: Tips

Tips Text: Dear users:
Welcome to use the network connection service of our company. Please note the following tips:
1. While using network, beware of illegal links, phishing websites and other fraudulent information and

Landing Page: ○ Original URL ● Promotional URL

Parameter description

Parameter	Description
Portal Page Name	Specifies the name of the portal page. The name is required.
Background Color	Specifies the background color. You can enter an RGB value or select one from the given colors. Tip This parameter is available only when the **Template Type** is set to **Text Template**.

Parameter	Description
Portal Title	Specifies the title of the portal page, including **Same as Authentication Type** and **Customize**. – **Same as Authentication Type**: The name is the same as the authentication type. For example, if this template is used for account authentication, the authentication title will be **Account.** – **Customize**: You can customize a portal title here.
Tips Title	Specifies the tip title on the portal page. By default, the title is **Tips**. Tip This parameter is available only when the **Template Type** is set to **Text Template**.
Tips Text	Specifies the tip content on the portal page. Tip This parameter is available only when the **Template Type** is set to **Text Template**.
Landing Page	Specifies the web address that users are automatically redirected to after passing the authentication. – **Original URL**: After users pass the authentication, the browser redirects to the website that users visited before the authentication. For example, if the user is visiting Google when being redirected to the portal page, the user will be redirected back to Google after passing the authentication. – **Promotional URL**: After users pass the authentication, the browser redirects to the address specified here.
Login Delay	Specifies the delay time before login. By default, the delay time is **Default (0s).**
Authentication Info Collection	Used to enable or disable the authentication information collection function.
Terms of use	Specifies the disclaimer information on the web portal page. Users must agree and tick the disclaimer before logging in.

6.4 Configure authentication type

6.4.1 SMS

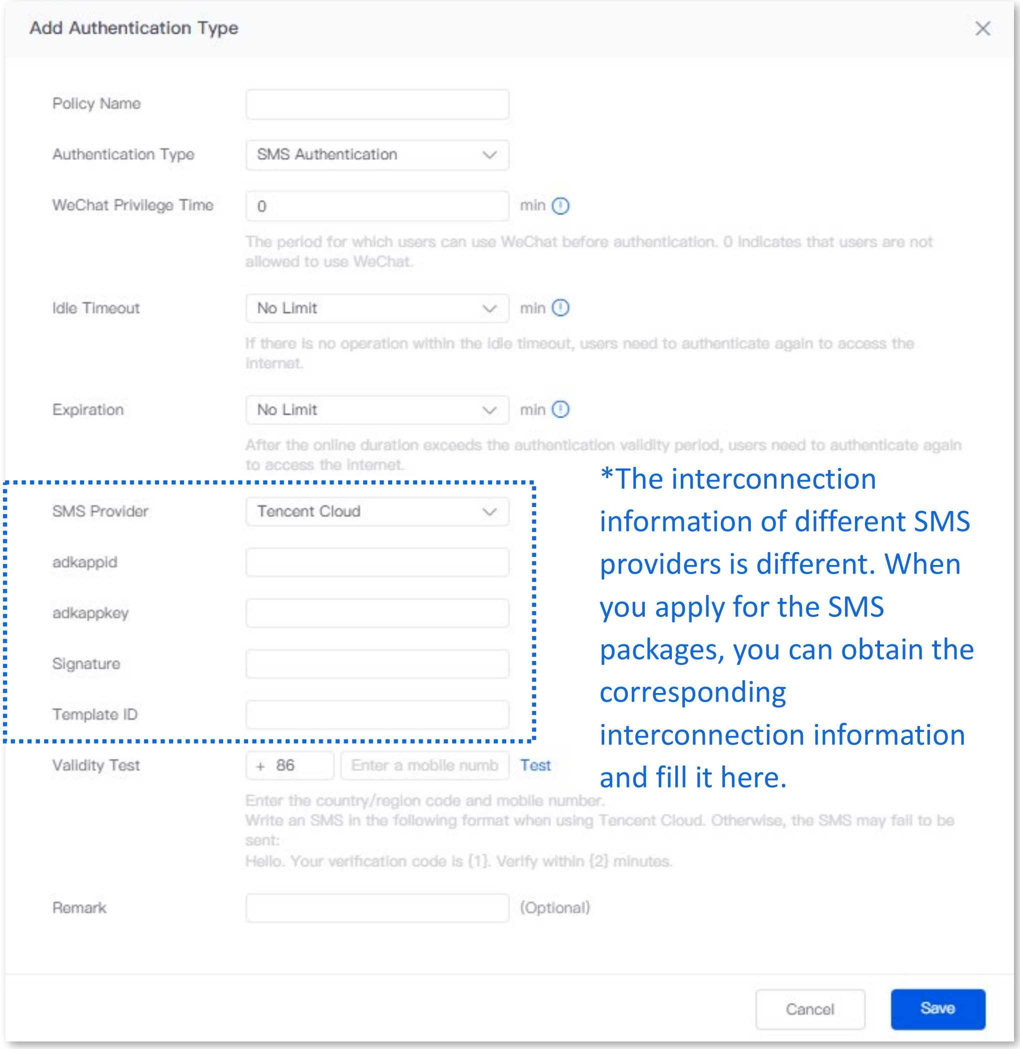
After the **SMS** authentication is enabled, you need to enter a valid mobile phone number on the portal customization to obtain a verification code for authentication. After successful authentication, you can access the internet.

The SMS providers issues the authorization verification code to the specified mobile phone number. Currently, the preset SMS providers include **Tencent Cloud**, **AliCloud**, **Jixintong** and **NEXMO**. Meanwhile, **Customize HTTP Interconnection** is also supported if you want to use other SMS providers.

Note

You need to subscribe to an SMS package from an SMS provider before performing corresponding configurations on the router.

To add an SMS authentication type, log in to the web UI of the router, navigate to **AuthN** > **Authentication Template** > **Authentication Type**, and click **Add**.



Add Authentication Type

Policy Name

Authentication Type: SMS Authentication

WeChat Privilege Time: 0 min

The period for which users can use WeChat before authentication. 0 indicates that users are not allowed to use WeChat.

Idle Timeout: No Limit min

If there is no operation within the idle timeout, users need to authenticate again to access the internet.

Expiration: No Limit min

After the online duration exceeds the authentication validity period, users need to authenticate again to access the internet.

SMS Provider: Tencent Cloud

adkappid

adkappkey

Signature

Template ID

Validity Test: + 86 Enter a mobile numb Test

Enter the country/region code and mobile number.
Write an SMS in the following format when using Tencent Cloud. Otherwise, the SMS may fail to be sent:
Hello. Your verification code is {1}. Verify within {2} minutes.

Remark (Optional)

*The interconnection information of different SMS providers is different. When you apply for the SMS packages, you can obtain the corresponding interconnection information and fill it here.

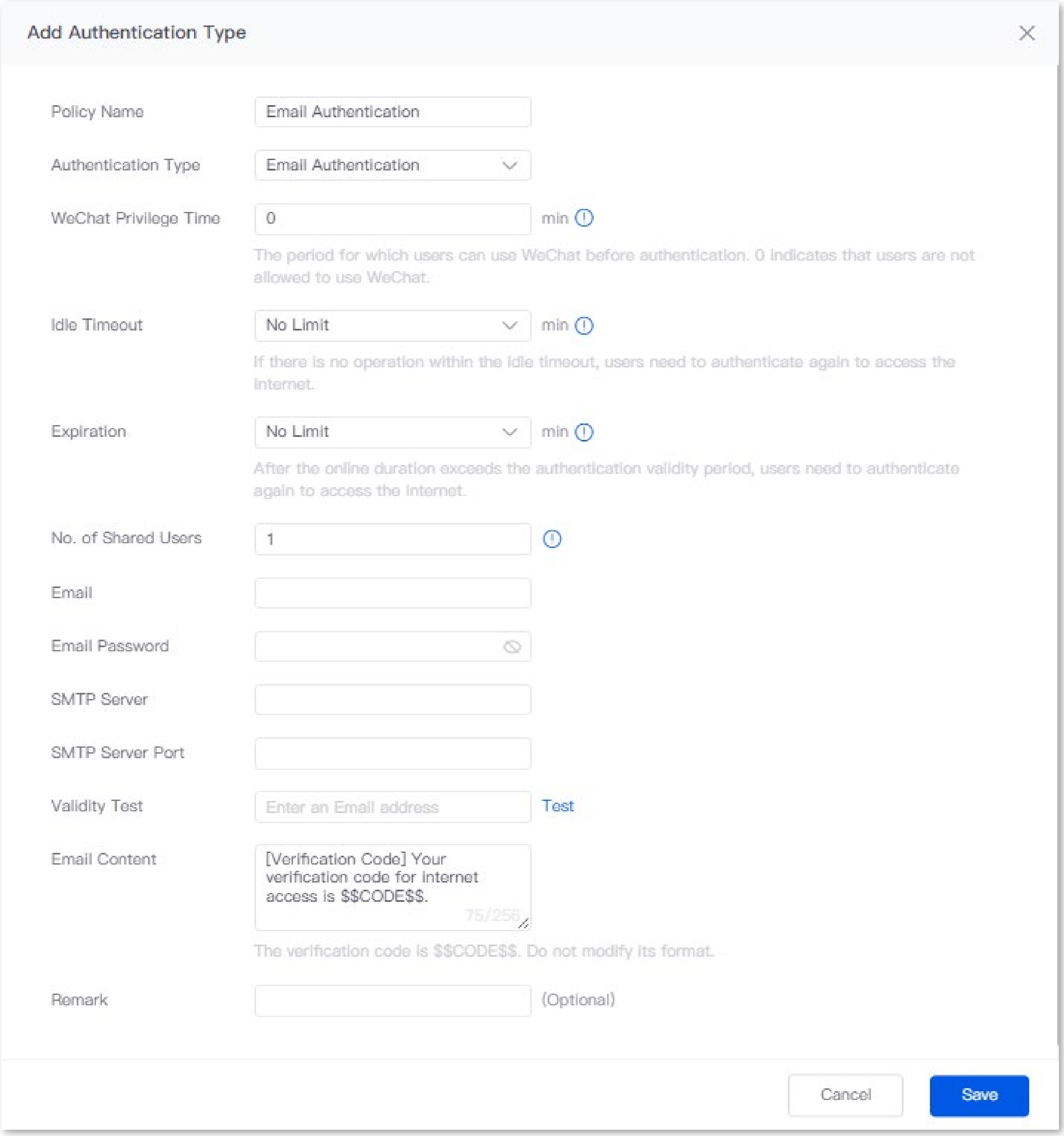
Parameter description

Parameter	**Description**
WeChat Privilege Time	Specifies the duration for which users can use WeChat before authentication. **0** indicates that users are not allowed to use WeChat before authentication.
Idle Timeout	Specifies the idle timeout of the authentication. If there is no operation within the **Idle Timeout** after successful authentication, you need to authenticate again to access the internet.
Expiration	Specifies the validity period of authentication. If the internet access expires after successful authentication, you need to re-authenticate to access the internet.
Validity Test	Used to check whether the router is connected to the SMS provider. Enter the mobile phone number and click Test . If the connection is successful, the mobile phone number will receive a message with the verification code.

6.4.2 Email

After the **Email** authentication is enabled, you need to enter an Email address on the portal customization to obtain a verification code for authentication. After successful authentication, you can access the internet.

To add an Email authentication type, log in to the web UI of the router, navigate to **AuthN** > **Authentication Template** > **Authentication Type**, and click **Add**.



Add Authentication Type

Policy Name	Email Authentication
Authentication Type	Email Authentication
WeChat Privilege Time	0 min The period for which users can use WeChat before authentication. 0 indicates that users are not allowed to use WeChat.
Idle Timeout	No Limit min If there is no operation within the idle timeout, users need to authenticate again to access the Internet.
Expiration	No Limit min After the online duration exceeds the authentication validity period, users need to authenticate again to access the Internet.
No. of Shared Users	1
Email	
Email Password	
SMTP Server	
SMTP Server Port	
Validity Test	Enter an Email address Test
Email Content	[Verification Code] Your verification code for internet access is $$CODE$$. 75/256 The verification code is $$CODE$$. Do not modify its format.
Remark	(Optional)

Parameter description

Parameter	Description
WeChat Privilege Time	Specifies the duration for which users can use WeChat before authentication. **0** indicates that users are not allowed to use WeChat before authentication.
Idle Timeout	Specifies the idle timeout of the authentication. If there is no operation within the **Idle Timeout** after successful authentication, you need to authenticate again to access the Internet.
Expiration	Specifies the validity period of authentication. If the internet access expires after successful authentication, you need to re-authenticate to access the internet.

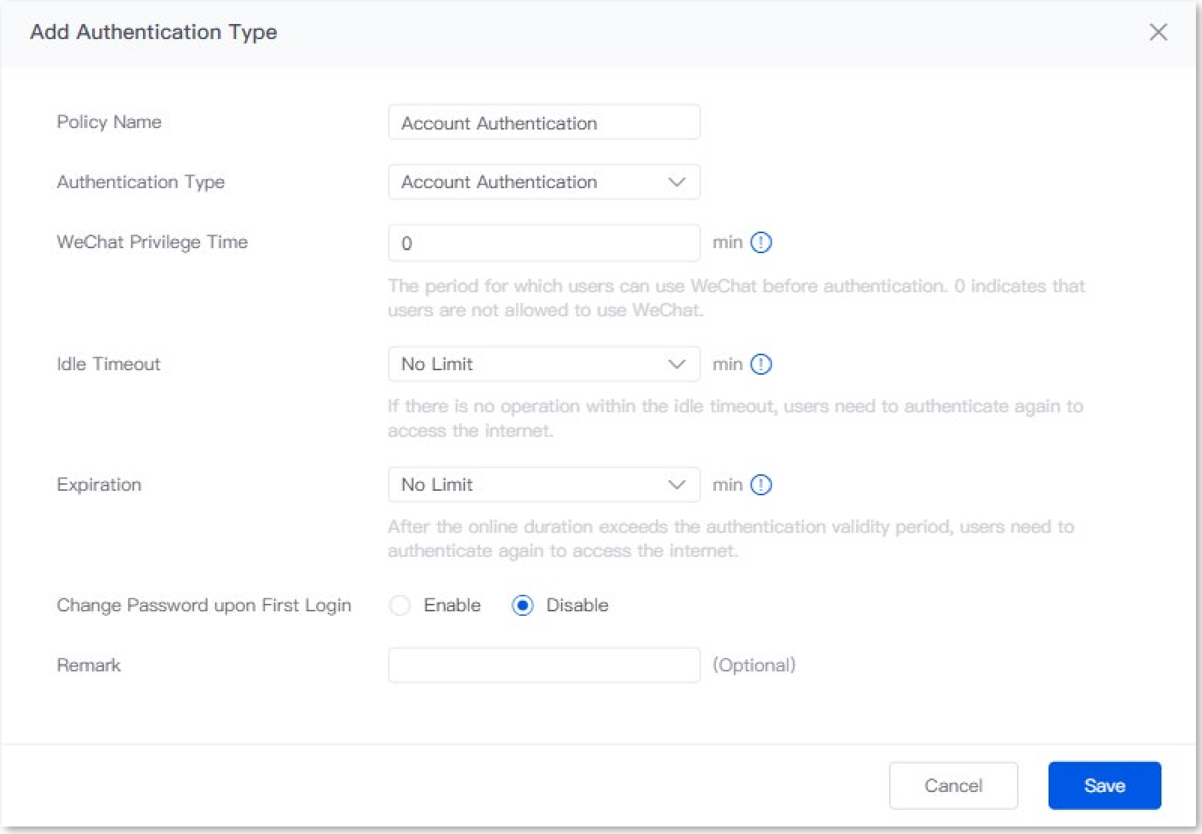
)

Parameter	Description
No. of Shared Users	Specifies the number of shared users allowed to access the internet through Email authentication at the same time.
Email	Specify the account and password used to send verification code mails.
Email Password	
SMTP Server	Specify the SMTP server address or port. The Simple Mail Transfer Protocol (SMTP) server is a proxy server for sending mails. The SMTP server addresses and ports of each mail server provider are different, so the user needs to query them by themselves.
SMTP Server Port	
Validity Test	Used to check whether the router is connected to the mail server. Enter the Email address and click Test . If the connection is successful, the Email box will receive a verification code.
Email Content	Specifies the content of the verification code Email.

6.4.3 Account

After **Account** is enabled, you need to enter the user name and password on the portal customization. After successful authentication, you can access the internet. The user name and password should be configured at Account Management in advance.

To add an Account type, log in to the web UI of the router, navigate to **AuthN** > **Authentication Template** > **Authentication Type**, and click **Add**.



Add Authentication Type

Policy Name: Account Authentication

Authentication Type: Account Authentication

WeChat Privilege Time: 0 min

The period for which users can use WeChat before authentication. 0 indicates that users are not allowed to use WeChat.

Idle Timeout: No Limit min

If there is no operation within the idle timeout, users need to authenticate again to access the internet.

Expiration: No Limit min

After the online duration exceeds the authentication validity period, users need to authenticate again to access the internet.

Change Password upon First Login: ○ Enable ● Disable

Remark: (Optional)

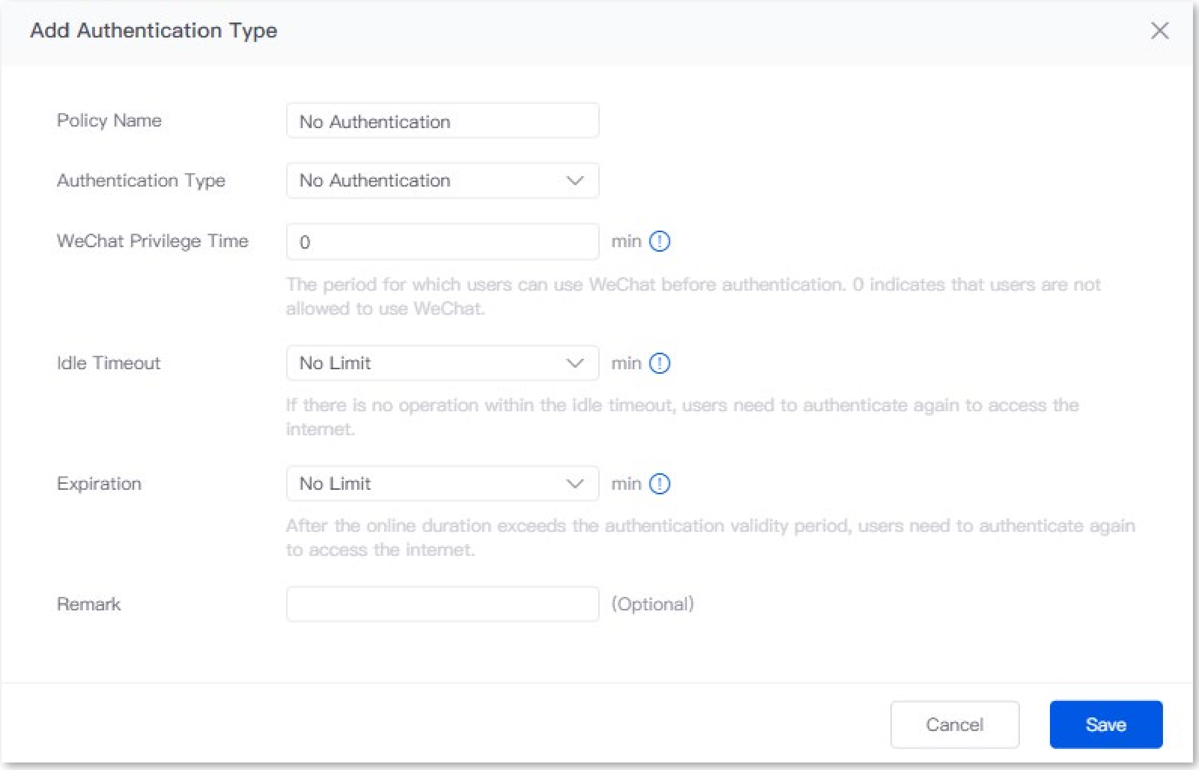
Parameter description

Parameter	Description
WeChat Privilege Time	Specifies the duration for which users can use WeChat before authentication. **0** indicates that users are not allowed to use WeChat before authentication.
Idle Timeout	Specifies the idle timeout of the authentication. If there is no operation within the **Idle Timeout** after successful authentication, you need to authenticate again to access the internet.
Expiration	Specifies the validity period of authentication. If the internet access expires after successful authentication, you need to re-authenticate to access the internet.
Change Password upon First Login	Used to enable or disable the change password upon first login function. After this function is enabled, the user needs to change the password to access the internet after the first successful authentication.

6.4.4 No authentication

After **No Authentication** is enabled, you only need to click **Connect** on the pop-up portal customization to access the internet.

To allow no authentication, log in to the web UI of the router, navigate to **AuthN** > **Authentication Template** > **Authentication Type**, and click **Add**.



Add Authentication Type

Policy Name: No Authentication

Authentication Type: No Authentication

WeChat Privilege Time: 0 min

The period for which users can use WeChat before authentication. 0 indicates that users are not allowed to use WeChat.

Idle Timeout: No Limit min

If there is no operation within the idle timeout, users need to authenticate again to access the internet.

Expiration: No Limit min

After the online duration exceeds the authentication validity period, users need to authenticate again to access the internet.

Remark: (Optional)

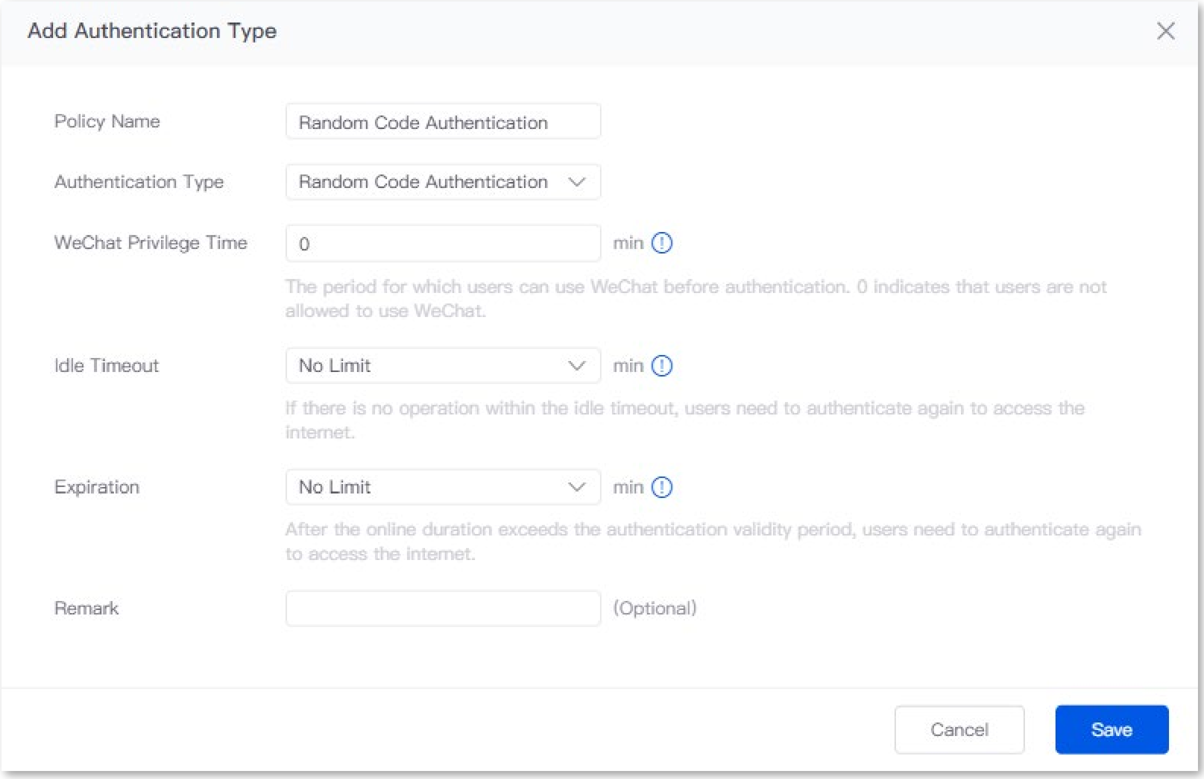
Parameter description

Parameter	Description
WeChat Privilege Time	Specifies the duration for which users can use WeChat before authentication. **0** indicates that users are not allowed to use WeChat before authentication.
Idle Timeout	Specifies the idle timeout of the authentication. If there is no operation within the **Idle Timeout** after successful authentication, you need to authenticate again to access the internet.
Expiration	Specifies the validity period of authentication. If the internet access expires after successful authentication, you need to re-authenticate to access the internet.

6.4.5 Random code

After the **Random Code** authentication is enabled, you need to enter the random code on the portal customization to obtain a verification code for authentication. After successful authentication, you can access the internet. The random codes need to be configured in random code account in advance.

To add a random code authentication type, log in to the web UI of the router, navigate to **AuthN** > **Authentication Template** > **Authentication Type**, and click **Add**.


Add Authentication Type

Policy Name: Random Code Authentication

Authentication Type: Random Code Authentication

WeChat Privilege Time: 0 min

The period for which users can use WeChat before authentication. 0 indicates that users are not allowed to use WeChat.

Idle Timeout: No Limit min

If there is no operation within the idle timeout, users need to authenticate again to access the internet.

Expiration: No Limit min

After the online duration exceeds the authentication validity period, users need to authenticate again to access the internet.

Remark: (Optional)

Parameter description

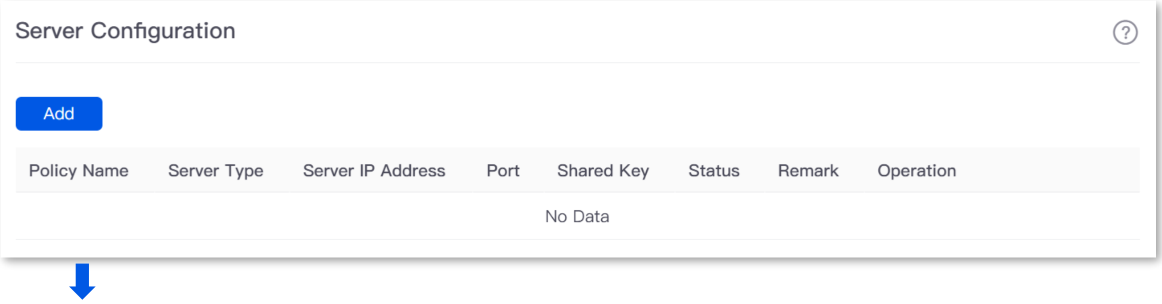
Parameter	Description
WeChat Privilege Time	Specifies the duration for which users can use WeChat before authentication. **0** indicates that users are not allowed to use WeChat before authentication.
Idle Timeout	Specifies the idle timeout of the authentication. If there is no operation within the **Idle Timeout** after successful authentication, you need to authenticate again to access the Internet.
Expiration	Specifies the validity period of authentication. If the internet access expires after successful authentication, you need to re-authenticate to access the internet.

6.5 Configure server

When the router enables external authentication, accounting policies and user information are stored on the Radius server. User authentication is also performed on the Radius server.

Log in to the web UI of the router, and navigate to **AuthN** > **Server Configuration** to enter the page.

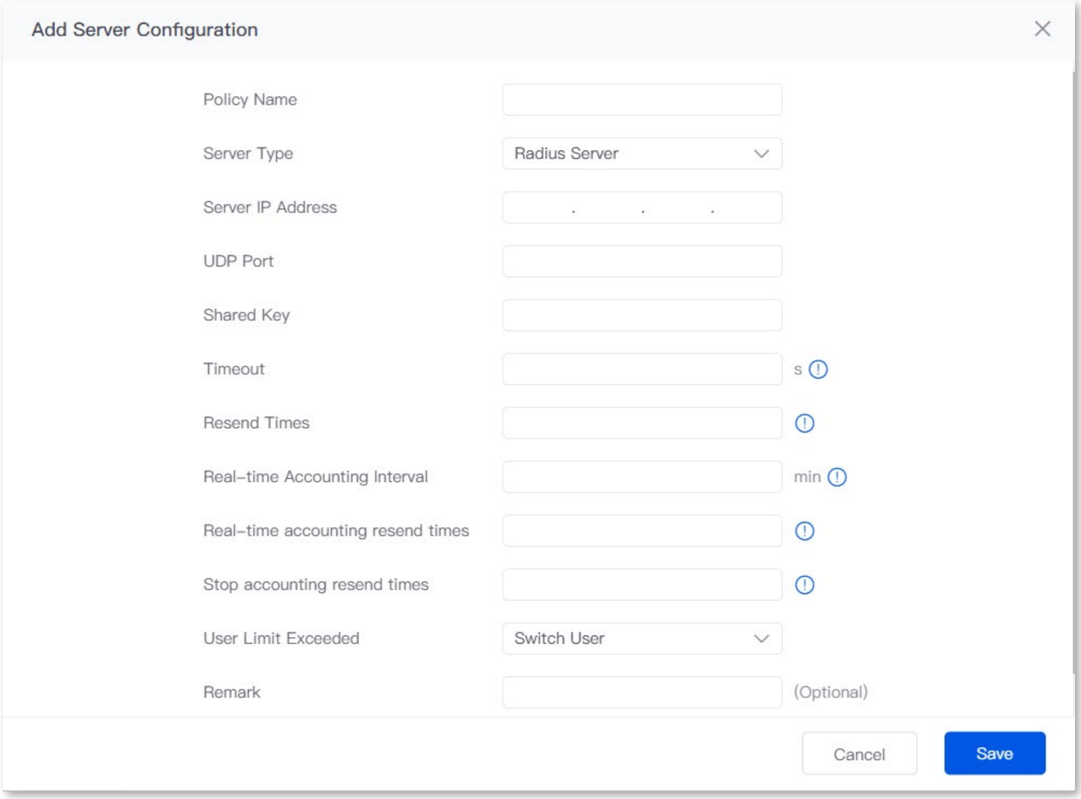
Click **Add** to add a Radius server. The figure below is for reference only. Each Radius server requires one Radius authentication policy and one Radius accounting policy.



Server Configuration

Policy Name	Server Type	Server IP Address	Port	Shared Key	Status	Remark	Operation

No Data



Add Server Configuration

Policy Name	
Server Type	Radius Server
Server IP Address	. . .
UDP Port	
Shared Key	
Timeout	s
Resend Times	
Real–time Accounting Interval	min
Real–time accounting resend times	
Stop accounting resend times	
User Limit Exceeded	Switch User
Remark	(Optional)

Parameter description

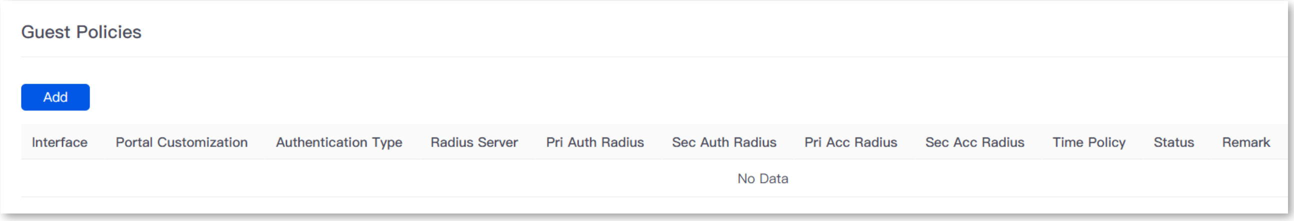
Parameter	Description
Server Type	Specifies the Radius server.
Server IP Address	Specifies the IP address of the Radius server.
UDP Port	Specifies the Radius server's port, which must match the authentication port of the Radius server. Generally, the authentication port number is 1812, and the accounting port is 1813.
Shared Key	The shared key configured on the Radius authentication server.
Timeout	Specifies the duration to wait for a response from the Radius server. If the timeout period expires, the client automatically resends the request.
Resend Times	Specifies the number of times the client resends the request after the Radius server response times out.

Parameter	Description
Real-time Accounting Interval	Specifies the real-time accounting interval of the Radius server. At each interval, the router sends online-user accounting data to the Radius server. Shorter intervals increase load on both the NAS and the RADIUS server.
Real-time Accounting Resend Times	Specifies the number of times the client resends the real-time accounting request after the Radius server response times out.
Stop Accounting Resend Times	Specifies the number of times the client resends the stop accounting request after the Radius server response times out.
User Limit Exceeded	When the number of users using a Radius server account exceeds the shared account limit, the Radius server can take action: – **Switch User**: Users who were authenticated earliest will be logged out first, allowing newly authenticated users to log in. – **Restrict Login**: Prevents new users from logging in. Existing authenticated users remain unaffected. New users can only log in once an existing user has logged out.

6.6 Configure guest policy

Log in to the web UI of the router, and navigate to **AuthN** > **Guest Policies** to enter the page.

On this page, you can configure the corresponding guest policies based on the VLAN interface.



Guest Policies

Interface	Portal Customization	Authentication Type	Radius Server	Pri Auth Radius	Sec Auth Radius	Pri Acc Radius	Sec Acc Radius	Time Policy	Status	Remark
					No Data					

Parameter description

Parameter	Description
Interface	Specifies the interface that the guest policy is used to. Configure the VLAN interface in advance.
Portal Customization	Specifies the portal customization of the guest policy. The portal customization should be configured at Portal Customization in advance.
Authentication Type	Specifies the authentication type of the guest policy. The authentication type should be configured at Authentication Type in advance.

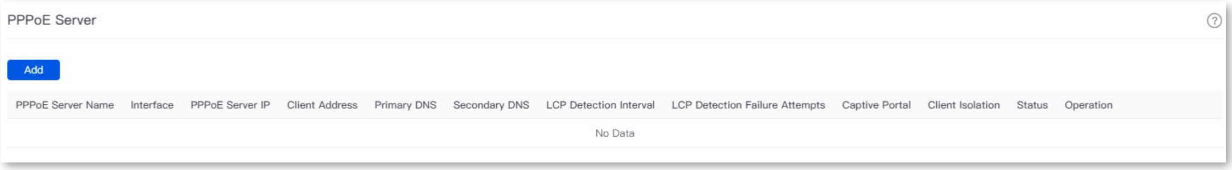
Parameter	Description
Radius Server	Specifies the Radius server for authentication.
Pri Auth Radius	Specifies the primary RADIUS server for user authentication. The primary authentication server should be configured at Server Configuration in advance.
Sec Auth Radius	Specifies the secondary RADIUS server for fallback authentication. The secondary authentication server should be configured at Server Configuration in advance.
Pri Acc Radius	Specifies the primary accounting RADIUS server for real-time accounting after authentication. The primary accounting server should be configured at Server Configuration in advance.
Sec Acc Radius	Specifies the secondary accounting RADIUS server for fallback accounting. The secondary accounting server should be configured at Server Configuration in advance.
Time Policy	Specifies the period during which guest policy takes effect. The time policy should be configured at Time Group in advance.

6.7 PPPoE server

Log in to the web UI of the router, and navigate to **AuthN** > **PPPoE Server** to enter the page.

On this page, you can configure the PPPoE Server based on the VLAN interface.

After the **PPPoE Server** is enabled, the router is configured as a PPPoE server. You need to access the internet through broadband dial-up authentication. The PPPoE user name and password need to be configured at Account Management in advance.

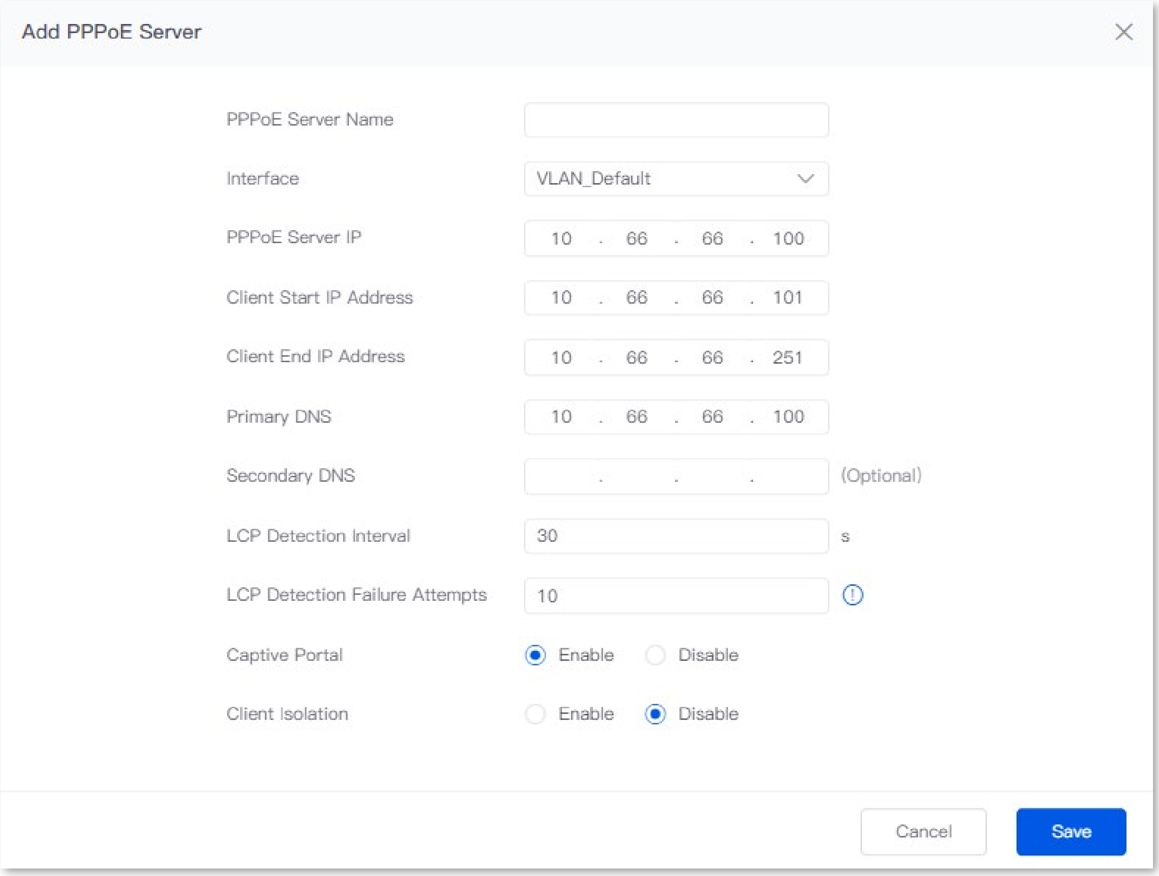


PPPoE Server

Add

PPPoE Server Name	Interface	PPPoE Server IP	Client Address	Primary DNS	Secondary DNS	LCP Detection Interval	LCP Detection Failure Attempts	Captive Portal	Client Isolation	Status	Operation

No Data



Add PPPoE Server ×

PPPoE Server Name	
Interface	VLAN_Default
PPPoE Server IP	10 . 66 . 66 . 100
Client Start IP Address	10 . 66 . 66 . 101
Client End IP Address	10 . 66 . 66 . 251
Primary DNS	10 . 66 . 66 . 100
Secondary DNS	. . . (Optional)
LCP Detection Interval	30 s
LCP Detection Failure Attempts	10 ⓘ
Captive Portal	● Enable ○ Disable
Client Isolation	○ Enable ● Disable

Cancel Save

Parameter description

Parameter	Description
PPPoE Server Name	Specifies the name of the customized PPPoE server.
Interface	Specifies the VLAN interface upon which the customized PPPoE server takes effect.
PPPoE Server IP	Specifies the IP address of the customized PPPoE server. It is also the gateway address of the client and must be in the same network segment with the address pool of the client.
Client Start IP Address	Specify the start or end IP address that the PPPoE server assigns to clients.
Client End IP Address	
Primary DNS	Specify the IP addresses of primary and secondary DNS servers assigned by the PPPoE server to users. **Secondary DNS** is optional. Tip To provide normal internet access, ensure that **Primary DNS** is set to the IP address of a correct DNS server or proxy.
Secondary DNS	

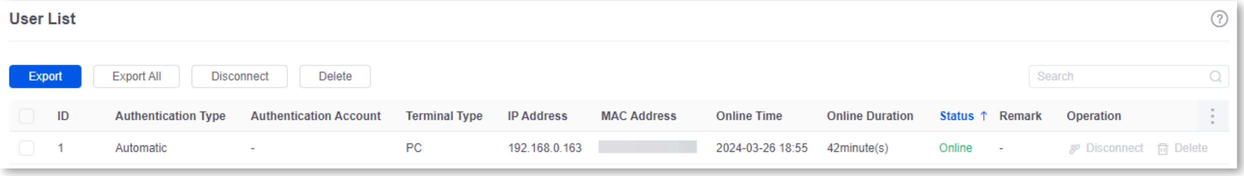
Parameter	Description
LCP Detection Interval	Specifies the interval at which PPPoE sends Link Control Protocol (LCP) packets.
LCP Detection Failure Attempts	Specifies the limit of failure attempts of the LCP Detection. When the number of unreplied LCP packets reaches the limit, the PPPoE server will disconnect the connection automatically.
Captive Portal	Used to enable or disable the captive portal function. With **Captive Portal** enabled, the clients connected to authenticated VLAN interface need to make a broadband dial-up authentication for internet access.
Client Isolation	Used to enable or disable the client isolation function. With **Client Isolation** enabled, clients cannot access each other.

6.8 Account

6.8.1 User list

Log in to the web UI of the router, and navigate to **AuthN** > **Account** > **User List** to enter the page.

On this page, you can check and export the authentication user information, kick authenticated accounts offline in batches and delete the authentication information of offline users in batches.



ID	Authentication Type	Authentication Account	Terminal Type	IP Address	MAC Address	Online Time	Online Duration	Status ↑	Remark	Operation
1	Automatic	-	PC	192.168.0.163	[redacted]	2024-03-26 18:55	42minute(s)	Online	-	Disconnect Delete

Button & parameter description

Name	Description
Disconnect	Used to disconnect the selected online users who have authenticated successfully. After being disconnected, an online user that has been authenticated before needs to re-authenticate to access the internet and an authentication-free online user will automatically connect to the internet again.
Delete	Used to delete information of selected offline users.

Name	Description
Authentication Type	Specifies the authentication type of the current authenticated user. The user configured as the authentication-free host is displayed as **Authentication-free** and the user whose guest policy is not configured is displayed as **Automatic**.
Authentication Account	Specifies the account, Email, mobile phone number, real name or random code used by the user.
Authentication Interface	Specifies the VLAN interface that the guest policy is used.

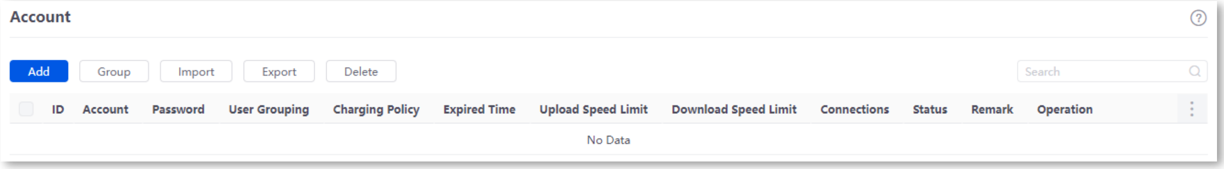
6.8.2 Account management

Overview

Log in to the web UI of the router, and navigate to **AuthN** > **Account** > **Account** to enter the page.

On this page, you can add a user account for account authentication or PPPoE authentication to access the internet.

You can configure the account charging strategy and upload or download speed to complete the authentication charging and the flow control function. You can also recharge the existing accounts and check the charging records.



ID	Account	Password	User Grouping	Charging Policy	Expired Time	Upload Speed Limit	Download Speed Limit	Connections	Status	Remark	Operation
No Data											

Button & parameter description

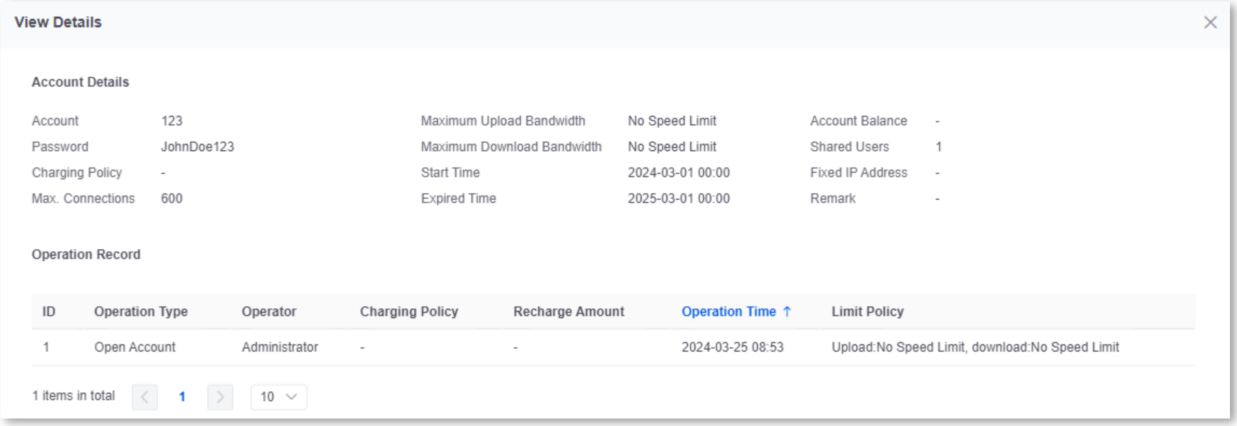
Name	Description
Group	Used to add selected users to user groups.
Account	Specify the user name and password used for authentication.
Password	
User Grouping	Specifies the user group of the account.
Charging Policy	Specifies the charging policy of the account, which should be configured in Charging Policy in advance. **Unused** specifies that the charging function is disabled for this account.

Name	Description
Upload Speed Limit/Maximum Upload Speed	Specify the maximum upload and download rate of the account. Tip If a charging policy is selected, the maximum upload and download rate configured in the charging policy will be used automatically. If no charging policy is selected, you can manually configure the parameters here.
Download Speed Limit/Maximum Download Speed	
Account Balance	Specifies the balance of the account. It needs to be entered after the charging policy is selected.
Charging Start Time	Specifies the time when the account becomes valid. Note If no charging policy is selected, you can manually configure this parameter.
End Time/Expired Time	Specifies the validity period of internet access of the account. If the internet access period of the account expires after successful authentication, you need to recharge to access the internet again. Note The parameter value will be calculated automatically by the router after the charging policy is selected and the account balance is entered. If no charging policy is selected, the parameter needs to be configured manually.
Connections/Max. Connections	Specifies the maximum number of concurrent connections allowed for the account, which is also the maximum number of conversations that the router can deal with simultaneously. When the account is used by multiple persons at the same time, the number of concurrent connections per person is the set value.
No. of Shared Users	Specifies the number of users that are allowed to use this account to authenticate and access the internet at the same time. Note If the Bind MAC Address function is enabled and the number of devices allowed to be concurrently connected under a single account has reached the shared user limit, other MAC devices cannot use this account to authenticate and access the internet.
Bind MAC Address	When enabled, the router will bind the MAC address that successfully use this account to authenticate and access the internet.

Name	Description
Fixed IP Address	Specifies the fixed IP address of the router. After it is configured, only the device with this IP address can use the account to authenticate and access the internet. By default, the fixed IP address is not configured. Note The fixed IP address does not take effect in the PPPoE authentication type.

Account details and operation records

Click Details of the corresponding account to check the account details and operation records in the pop-up window. The following figure is for reference only.



View Details

Account Details

Account	123	Maximum Upload Bandwidth	No Speed Limit	Account Balance	-
Password	JohnDoe123	Maximum Download Bandwidth	No Speed Limit	Shared Users	1
Charging Policy	-	Start Time	2024-03-01 00:00	Fixed IP Address	-
Max. Connections	600	Expired Time	2025-03-01 00:00	Remark	-

Operation Record

ID	Operation Type	Operator	Charging Policy	Recharge Amount	Operation Time ↑	Limit Policy
1	Open Account	Administrator	-	-	2024-03-25 08:53	Upload:No Speed Limit, download:No Speed Limit

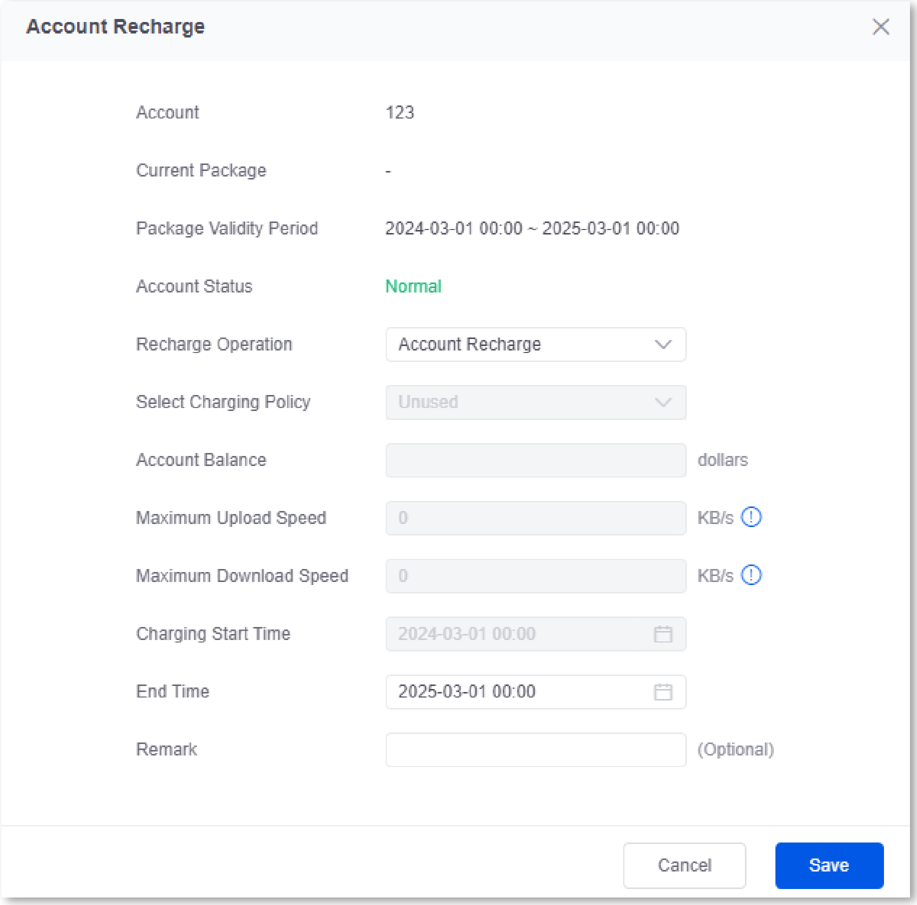
1 items in total

Recharge the account

Click Recharge of the corresponding account to recharge the account in the pop-up window or change the charging policy.

Note

If no charging policy is used in the account, you can change the expiration time manually to recharge the account.



Account Recharge

Account	123
Current Package	-
Package Validity Period	2024-03-01 00:00 ~ 2025-03-01 00:00
Account Status	Normal
Recharge Operation	Account Recharge
Select Charging Policy	Unused
Account Balance	dollars
Maximum Upload Speed	0 KB/s
Maximum Download Speed	0 KB/s
Charging Start Time	2024-03-01 00:00
End Time	2025-03-01 00:00
Remark	(Optional)

Parameter description

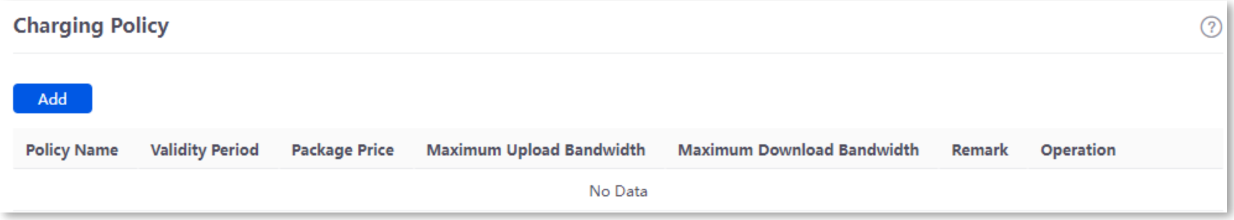
Parameter	Description
Recharge Operation	Used to select the recharge operation. You can select **Account Recharge** to renew the current package or **Charging Policy Modification** to change the current package. Note Changing the charging policy will clear the account balance and validity period.
Select Charging Policy	Used to select the charging policy of the account. When **Recharge Operation** is set to **Charging Policy Modification**, you can select a new charging policy here.
Account Balance	Specifies the balance of the charging. Tip If no charging policy is used on the account, which means that **Select Charging Policy** is set to **Unused**, account balance cannot be set.
Maximum Upload Speed	Specify the maximum upload and download speed of the current account.

Parameter	Description
Maximum Download Speed	Tip If no charging policy is used on the account, which means that **Recharge Operation** is set to **Charging Policy Modification** and **Select Charging Policy** is set to **Unused**, these parameters need to be set manually.
Charging Start Time	Specifies the time when the account starts to take effect.
End Time	Specifies the validity end time for using the account to access the internet. After this account is authenticated and connected to the internet successfully, if the online time exceeds the end time, you need to recharge to access the internet. Tip If no charging policy is used on the account, which means that **Select Charging Policy** is set to **Unused**, the parameter needs to be set manually.

6.8.3 Charging policy

Log in to the web UI of the router, and navigate to **AuthN** > **Account** > **Charging Policy** to enter the page.

On this page, you can configure charging policies based on actual charging requirements.



Charging Policy

Policy Name	Validity Period	Package Price	Maximum Upload Bandwidth	Maximum Download Bandwidth	Remark	Operation
No Data						

Parameter description

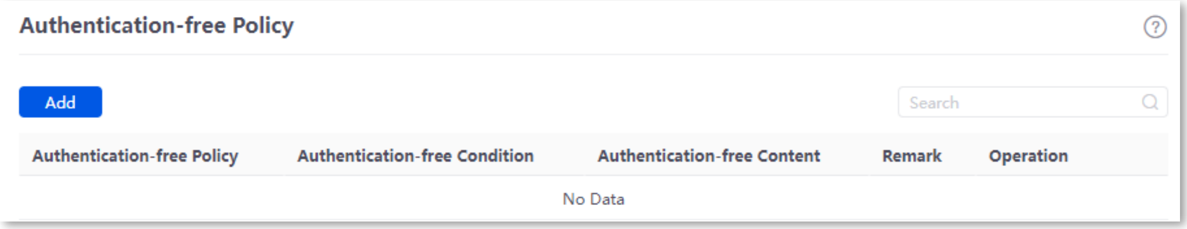
Parameter	Description
Validity Period	Specifies the charging cycle of a charging policy.
Package Price	Specifies the package amount of a charging cycle. For example, if the charging cycle is 1 hour, and the package price is $2, then it costs $2 per hour to access the internet using this charging policy.

Parameter	Description
Maximum Upload Bandwidth	Specify the maximum upload and download rate of the account. **0** indicates no limit.
Maximum Download Bandwidth	

6.8.4 Authentication-free policy

Log in to the web UI of the router, and navigate to **AuthN** > **Account** > **Authentication-free Policy** to enter the page.

On this page, you can configure the authentication-free policies for special devices such as network cameras. After configuration, these devices can connect to the internet without authentication.



Authentication-free Policy

Authentication-free Policy	Authentication-free Condition	Authentication-free Content	Remark	Operation
No Data				

Parameter description

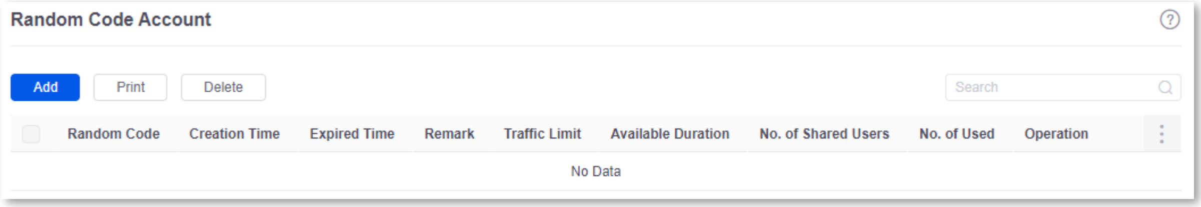
Parameter	Description
Authentication-free Policy	Specifies the authentication-free policy type of the router, including **Terminal Type** and **Terminal Unique Information**.

Parameter	Description
Authentication-free Condition	Specifies the condition of the authentication-free policy. Only the clients that meet the condition can access the internet without authentication. When **Authentication-free Policy** is set to **Terminal Unique Information**, the following authentication-free conditions are available: – **Mobile Number**: When SMS authentication is enabled, set mobile numbers that do not require authentication to enable them to access the internet without obtaining verification codes. – **IP Address**: Devices with the configured IP addresses can access the internet without authentication. – **MAC Address**: Devices with the configured MAC addresses can access the internet without authentication. When **Authentication-free Policy** is set to **Terminal Type**, the following authentication-free conditions are available: – **Wired Terminals**: Devices that are connected to the LAN of the router in a wired manner can access the internet without authentication. – **Wireless Terminals**: Devices that are connected to the LAN of the router in a wireless manner can access the internet without authentication. – **Mobile Phone**: Devices that are identified as mobile phones can access the internet without authentication.
Authentication-free Content	Specifies the content of the authentication-free policy. When a device meets both the authentication-free policy and content, it can access the internet without authentication. **“–“** indicates no authentication contents.

6.8.5 Random code account

Log in to the web UI of the router, and navigate to **AuthN** > **Account** > **Random Code Account** to enter the page.

On this page, you can add the random codes used in random code authentication.



Parameter description

Parameter	Description
Random Code	Specifies the random code used for authentication.
Creation Time	Specifies the time when the random code is created.

Parameter	Description
No. of Created Codes	Specifies the number of random codes to be created.
Account Validity Period	Specifies the validity period of the random code, ranging from 0 to 87600. **0** indicates no limit.
Expired Time	Specifies the time point when the random code expires. Expired accounts cannot be used again. The expiration time point is calculated based on the creation time of the random code and the validity period of the configured account.
Remark	Specifies the introduction to the random code. The remark is optional.
Traffic Limit	Specifies the total download traffic that the random code is allowed to use. Once this value is exceeded, the random code will be denied internet access.
Available Duration	Specifies the longest duration this random code is allowed to stay online at a time. When the random code expires, the user needs to log in again.
No. of Shared Users	Specifies the number of users who are allowed to access the internet using this random code at the same time. Note The Bind MAC Address function is enabled by default in Random Code guest policies. For example, if the number of shared users is 2, the router will bind the first two MAC addresses that successfully use this random code to authenticate. Devices with other MAC addresses cannot use this random code to authenticate and access the internet.
No. of Used	Specifies the number of users who are using the random code to access the internet.
Random Code Title	Specifies the title of the random code. It appears on the central upper part of the page. You can use it for advertising promotion. For example, “Welcome to *XX*”.

6.9 Example of local authentication for tenants

6.9.1 Networking requirements

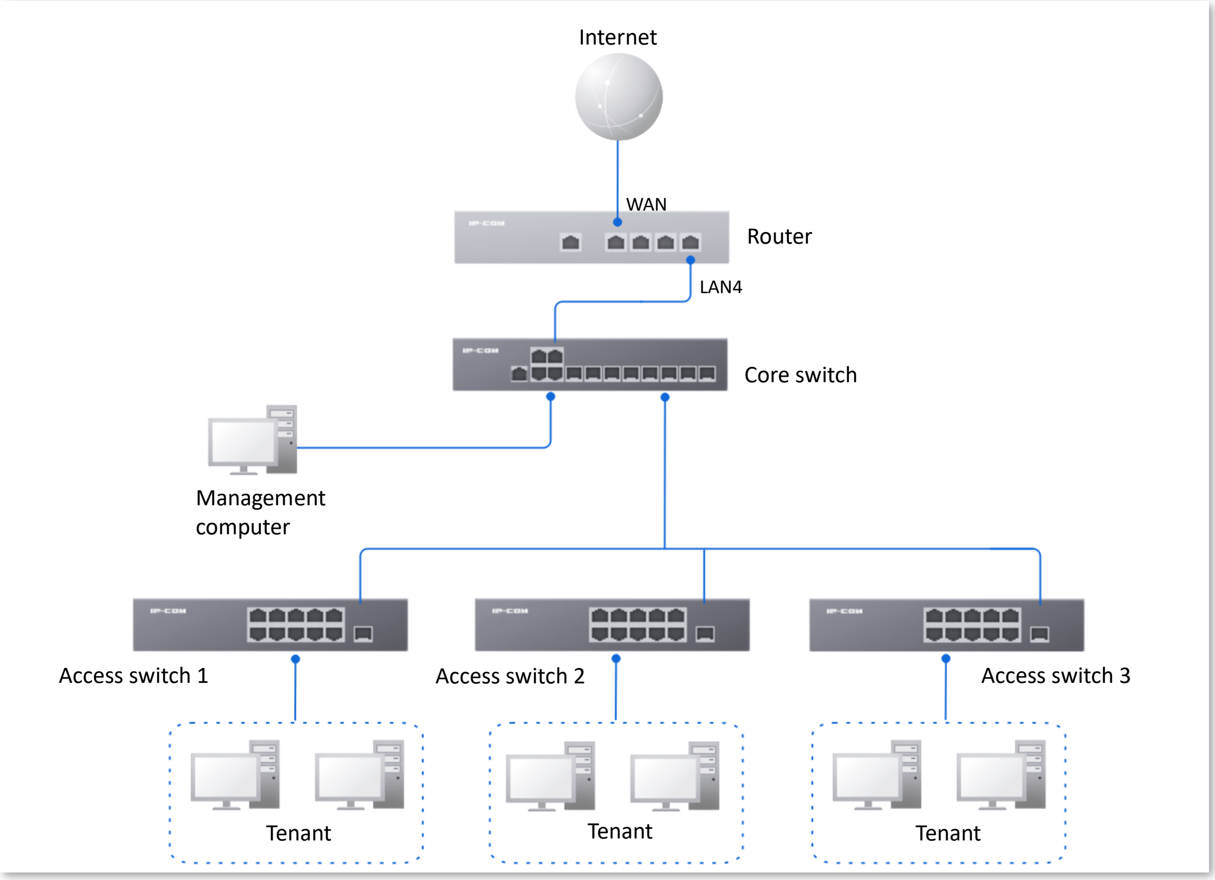
An owner of rented flats uses a router as the egress gateway. Tenants need to pay by month to get internet access when connecting to the flat network.

To manage the network usage, the following requirements are raised for the flat network:

- All tenants have to access the internet using the PPPoE connection mode.

- Two internet access packages ($15 per month with 20 MHz bandwidth and $50 per month with 100 MHz bandwidth) are provided for tenants.
- The flat manager's computer can access the internet without authentication for convenient management.

The following figure shows the network topology.



6.9.2 Solution

- Configure the PPPoE server based on the VLAN interface.
- Configure an authentication-free policy for the manager's computer.
- Configure authentication accounts.

6.9.3 Configuration procedure

Configure the router → Configure the core switch

I. Configure the router

1. Log in to the web UI of the router.
2. Add VLANs and configure a DHCP server.

Example of configuring the VLAN:

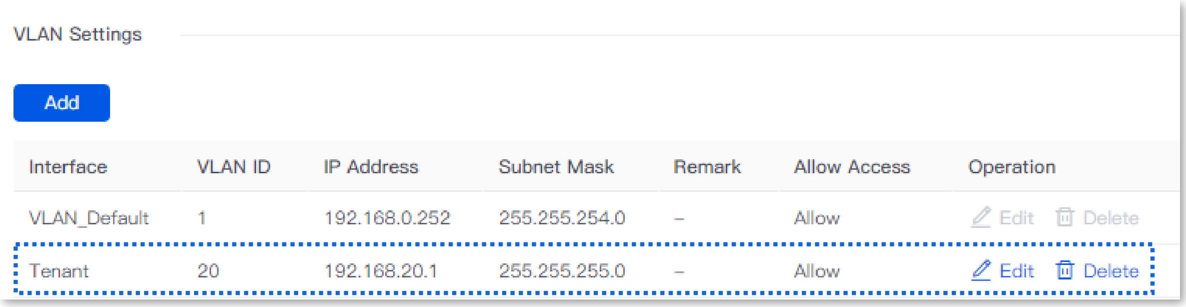
Interface	VLAN ID	IP Address/Subnet·Mask	Physical Port
Tenant	20	192.168.20.1/24	LAN4 (UNTAG)

Example of configuring the DHCP server:

Policy Name	Interface	User DHCP	AP DHCP
Tenant	Tenant	IP address pool: 192.168.20.100 - 192.168.20.200 Subnet mask: 255.255.255.0 Default gateway: 192.168.20.1 Primary DNS: 192.168.20.1	/

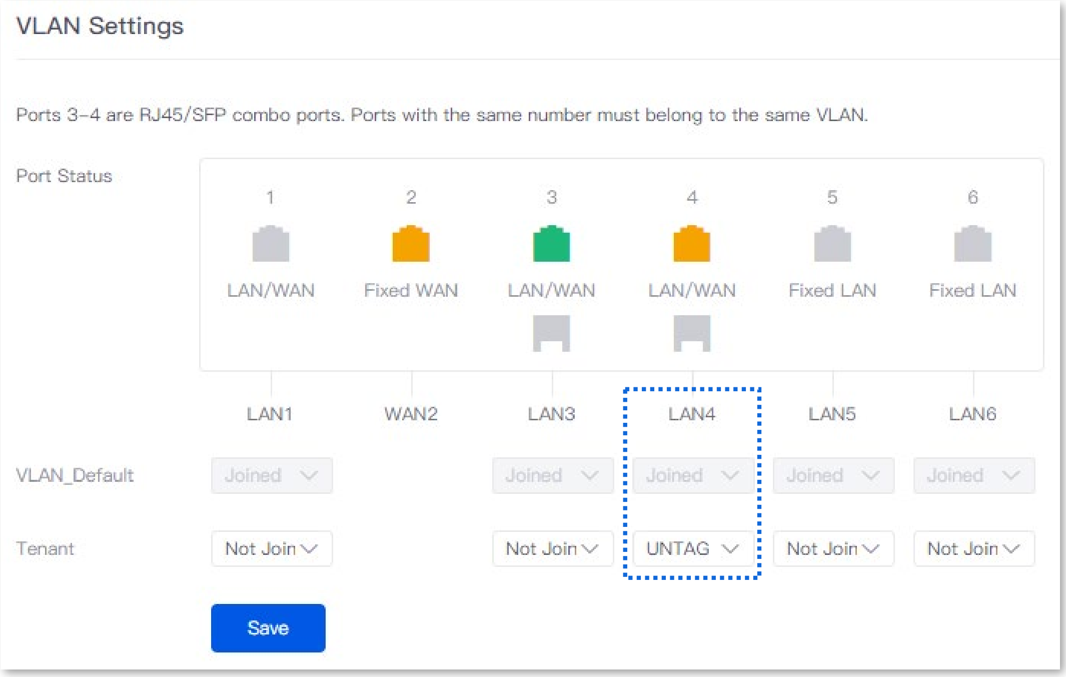
1) Add VLANs.

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



Interface	VLAN ID	IP Address	Subnet Mask	Remark	Allow Access	Operation
VLAN_Default	1	192.168.0.252	255.255.254.0	–	Allow	Edit Delete
Tenant	20	192.168.20.1	255.255.255.0	–	Allow	Edit Delete

- Select LAN port for the **Tenant** VLAN, which is **LAN4** in this example, set VLAN policy to **UNTAG**. Then click **Save**.



VLAN Settings

Ports 3–4 are RJ45/SFP combo ports. Ports with the same number must belong to the same VLAN.

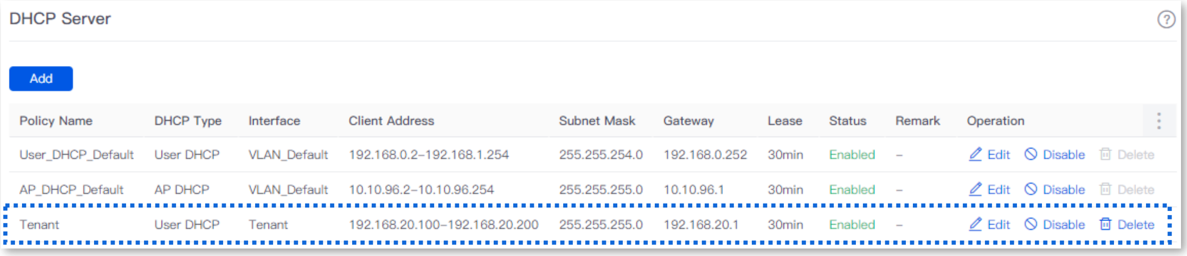
Port Status

1	2	3	4	5	6
LAN/WAN	Fixed WAN	LAN/WAN	LAN/WAN	Fixed LAN	Fixed LAN

	LAN1	WAN2	LAN3	LAN4	LAN5	LAN6
VLAN_Default	Joined		Joined	Joined	Joined	Joined
Tenant	Not Join		Not Join	UNTAG	Not Join	Not Join

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 Tenant VLAN and click **Save.**



DHCP Server

Policy Name	DHCP Type	Interface	Client Address	Subnet Mask	Gateway	Lease	Status	Remark	Operation
User_DHCP_Default	User DHCP	VLAN_Default	192.168.0.2–192.168.1.254	255.255.254.0	192.168.0.252	30min	Enabled	–	Edit Disable Delete
AP_DHCP_Default	AP DHCP	VLAN_Default	10.10.96.2–10.10.96.254	255.255.255.0	10.10.96.1	30min	Enabled	–	Edit Disable Delete
Tenant	User DHCP	Tenant	192.168.20.100–192.168.20.200	255.255.255.0	192.168.20.1	30min	Enabled	–	Edit Disable Delete

3. Configure the PPPoE server.

Example:

PPPoE server configuration

PPPoE Server Name: PPPoE_1

Interface: Tenant

PPPoE Server IP: 10.66.66.100

Client IP Address: 10.66.66.101~10.66.66.251

Primary DNS: 10.66.66.100

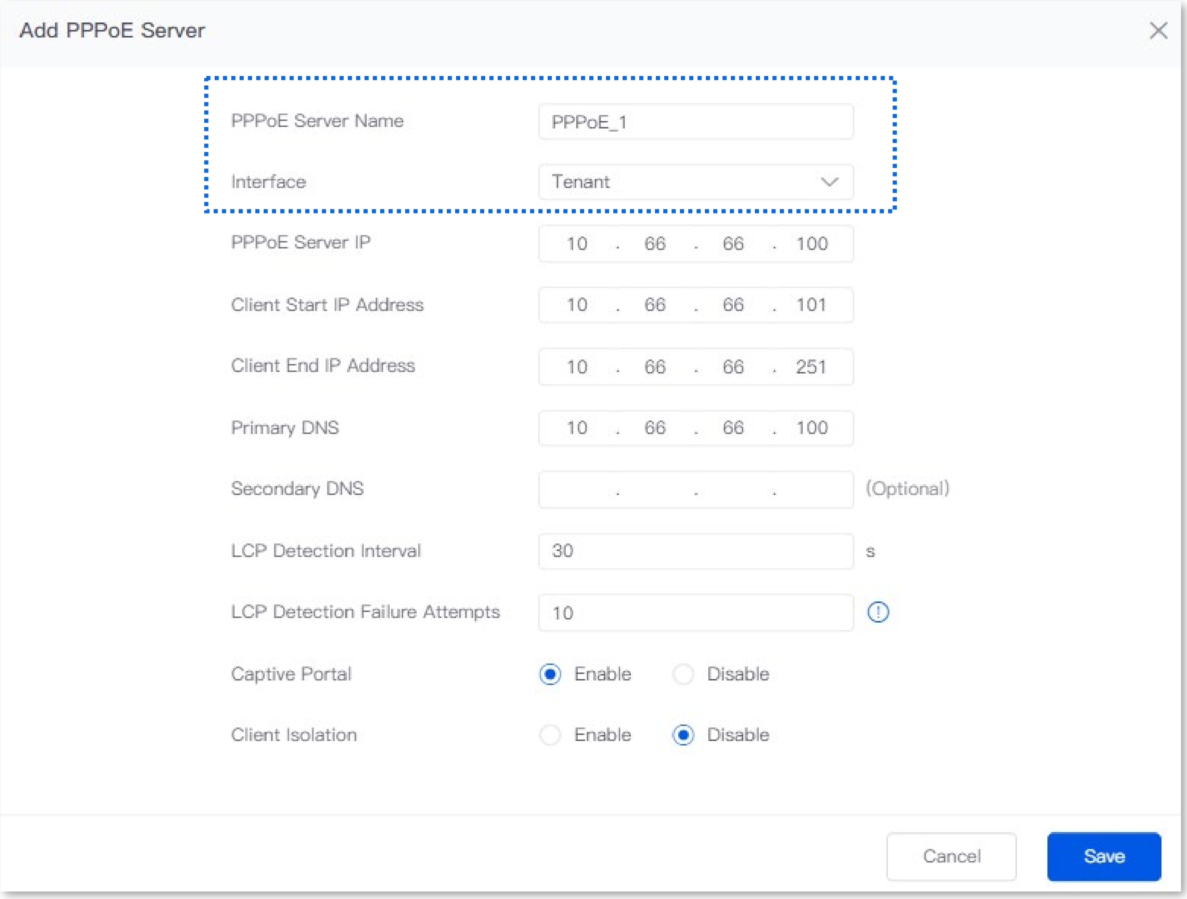
LCP Detection Interval: 30s

LCP Detection Failure Attempts: 10

Captive Portal: Enable

Other parameters: Use defaults

Navigate to **AuthN** > **PPPoE Server**, and click **Add**. Configure parameters as required, and click **Save**. The following figure is for reference only.



Add PPPoE Server

PPPoE Server Name: PPPoE_1

Interface: Tenant

PPPoE Server IP: 10 . 66 . 66 . 100

Client Start IP Address: 10 . 66 . 66 . 101

Client End IP Address: 10 . 66 . 66 . 251

Primary DNS: 10 . 66 . 66 . 100

Secondary DNS: . . . (Optional)

LCP Detection Interval: 30 s

LCP Detection Failure Attempts: 10

Captive Portal: ● Enable ○ Disable

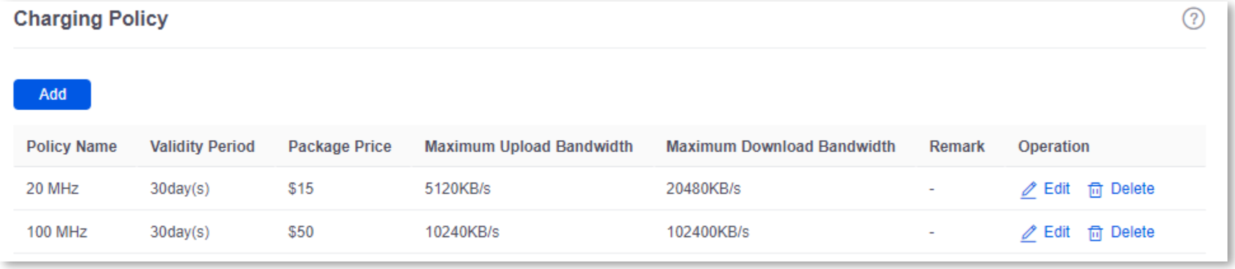
Client Isolation: ○ Enable ● Disable

4. Configure the PPPoE service package.

Example:

20 MHz Package	100 MHz Package
Policy Name: 20 MHz Validity Period: 30 days Package Price: 15 dollars Maximum Upload Bandwidth: 5120 KB/s Maximum Download Bandwidth: 20480 KB/s	Policy Name: 100 MHz Validity Period: 30 days Package Price: 50 dollars Maximum Upload Bandwidth: 10240 KB/s Maximum Download Bandwidth: 102400 KB/s

Navigate to **AuthN** > **Account** > **Charging Policy**, and click **Add**. Configure parameters as required, and click **Save**. The following figure is for reference only.



Charging Policy

Policy Name	Validity Period	Package Price	Maximum Upload Bandwidth	Maximum Download Bandwidth	Remark	Operation
20 MHz	30day(s)	$15	5120KB/s	20480KB/s	-	Edit Delete
100 MHz	30day(s)	$50	10240KB/s	102400KB/s	-	Edit Delete

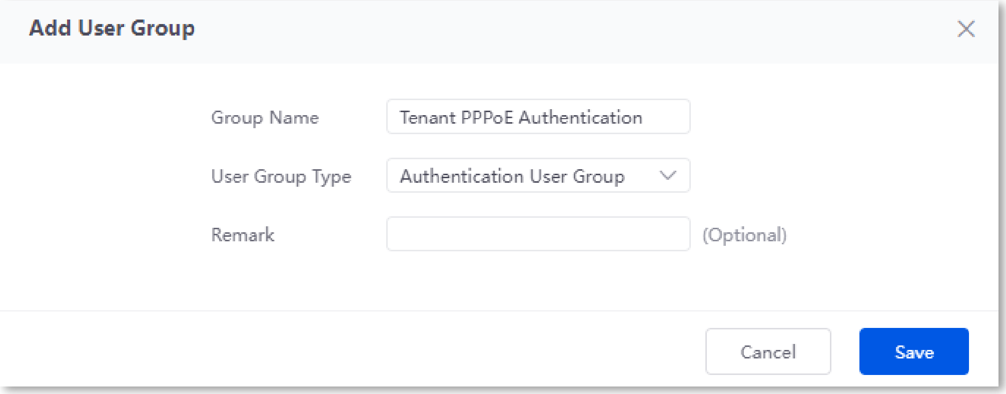
5. Configure authentication accounts for tenants.

The values shown below are examples only. For other parameters not mentioned, the default settings are used.

User Group	Authentication Account
Group Name: Tenant PPPoE Authentication User Group Type: Authentication User Group	Account: Room number Password: Room number+Mobile number User Grouping: Tenant PPPoE Authentication Select Charging Policy: 20 MHz or 100 MHz Account Balance: Set as required No. of Shared Users: 1

1) Add the user group.

Navigate to **Audit** > **Group Policy** > **User Group**, and click **Add**. Configure parameters as required, and click **Save**. The following figure is for reference only.



Add User Group

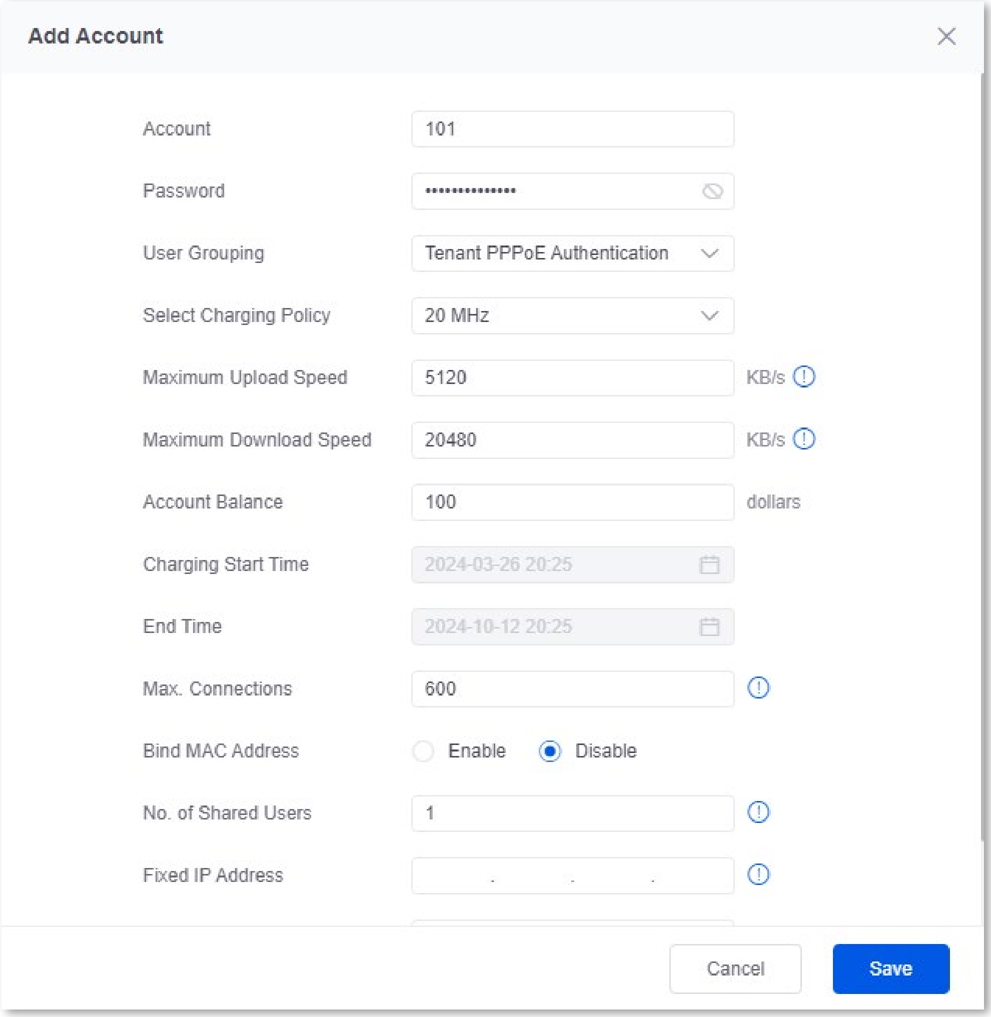
Group Name: Tenant PPPoE Authentication

User Group Type: Authentication User Group

Remark: (Optional)

2) Add an authentication account and add it to the user group.

Navigate to **AuthN** > **Account** > **Account**, and click **Add**. Configure parameters as required, and click **Save**. The following figure is for reference only.



Add Account

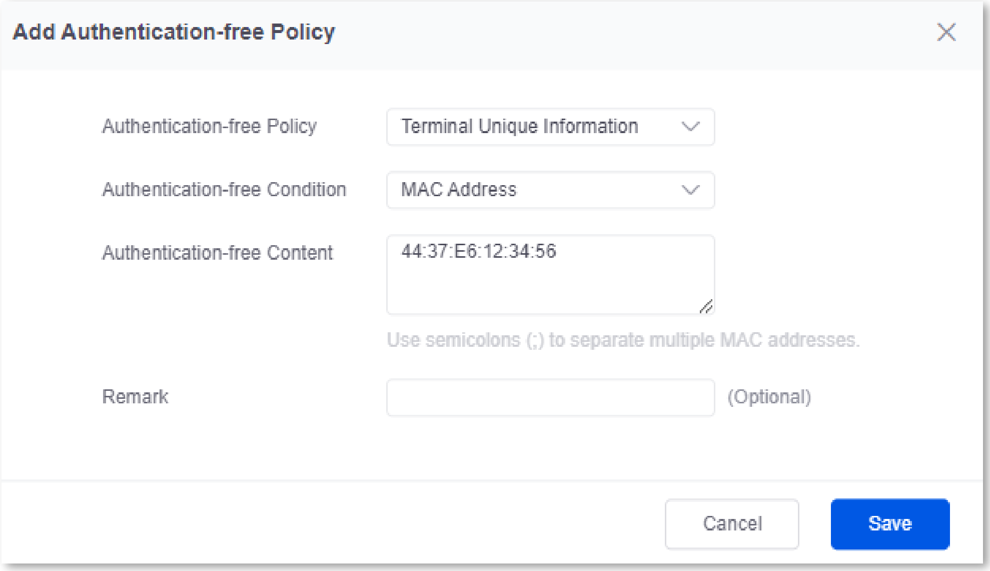
Account	101
Password	••••••••••••••
User Grouping	Tenant PPPoE Authentication
Select Charging Policy	20 MHz
Maximum Upload Speed	5120 KB/s
Maximum Download Speed	20480 KB/s
Account Balance	100 dollars
Charging Start Time	2024-03-26 20:25
End Time	2024-10-12 20:25
Max. Connections	600
Bind MAC Address	○ Enable ● Disable
No. of Shared Users	1
Fixed IP Address	. . .

3) Repeat the substep 2) to configure authentication accounts for other tenants.

6. Configure the authentication-free policy.

Assume that the MAC address of the computer to which the authentication-free policy applies is 44:37:E6:12:34:56.

Navigate to **AuthN** > **Account** > **Authentication-free Policy**, and click **Add**. Configure parameters as required, and click **Save**.



Authentication-free Policy: Terminal Unique Information

Authentication-free Condition: MAC Address

Authentication-free Content: 44:37:E6:12:34:56

Use semicolons (;) to separate multiple MAC addresses.

Remark: (Optional)

II. Configure the core switch

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

Port Connected to	VLAN ID (VLAN Allowed)	Port Property	PVID
Router	20	Trunk	20
Access switch	20	Access	20
Management computer	20	Access	20

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.

---End

6.9.4 Verification

The flat manager’s computer (MAC address: 44:37:E6:12:34:56) can access the internet without authentication.

Tenants need to dial in when accessing the internet.

Dial-up from the router

This method is applicable for scenarios where the tenant uses a router to connect to the broadband Ethernet port of the flat network. For details about the router settings, see the user guide of the corresponding router.

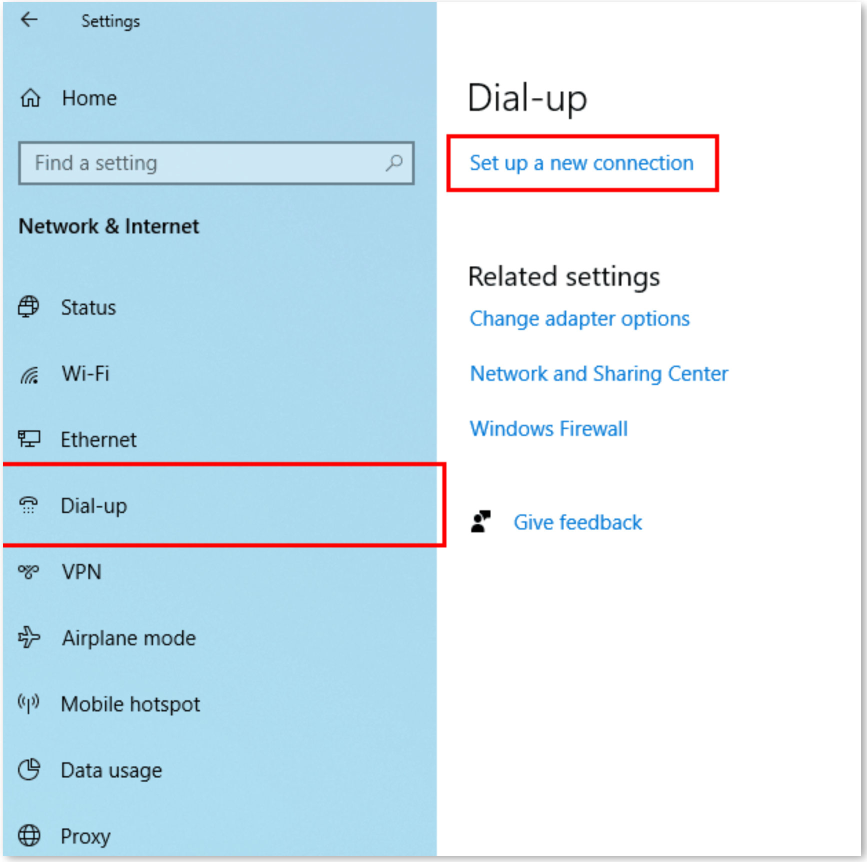
1. Log in to the web UI of the router of the tenant.
2. Set the internet connection type to PPPoE, enter the PPPoE user name and password, and save the settings.

After the settings, the tenant can access the internet through the router.

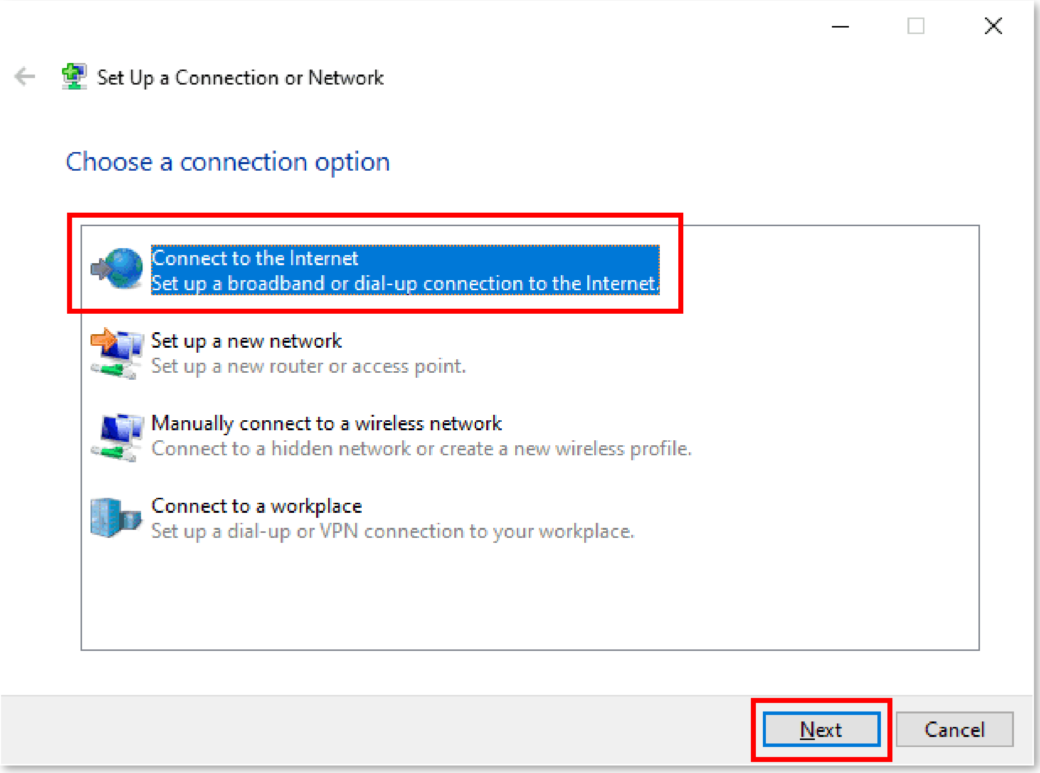
Dial-up from the computer

It is suitable for scenarios where the tenant uses the computer to connect to the broadband Ethernet port of the flat network. Windows 10 is used for example in the following steps.

1. Right-click 🌐 in the lower-right corner of your desktop. Then click **Network & Internet**.
2. Click **Dial-up** in the left navigation bar. Then click **Set up a new connection**.



3. Select **Connect to the Internet**, and click **Next**.



Set Up a Connection or Network

Choose a connection option

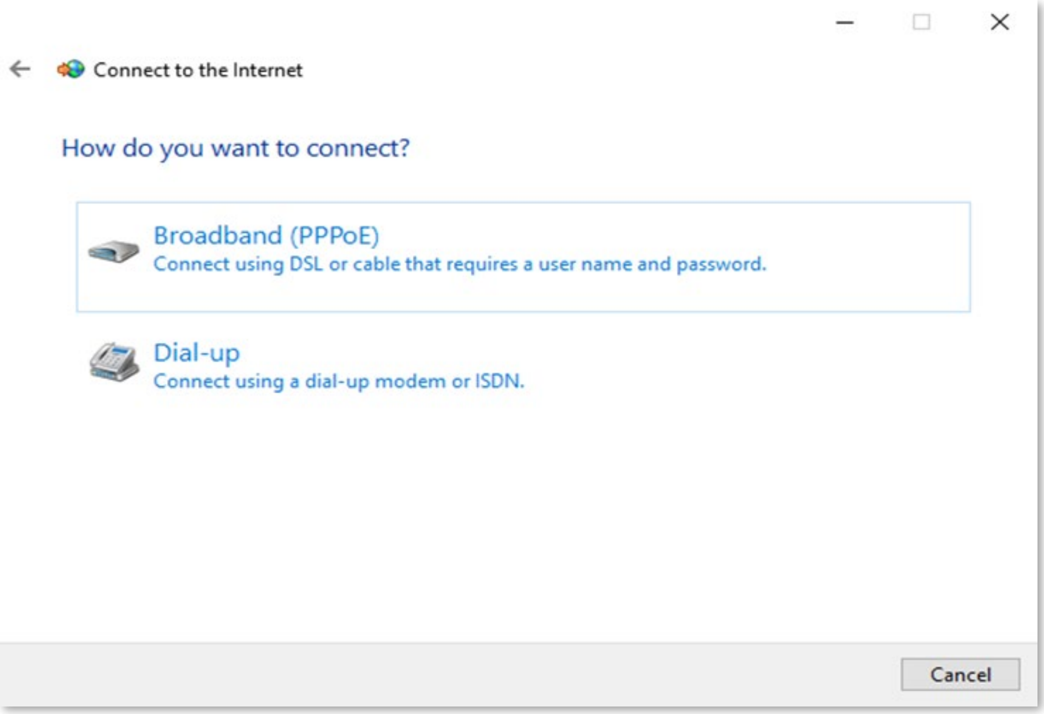
Connect to the Internet
Set up a broadband or dial-up connection to the Internet.

Set up a new network
Set up a new router or access point.

Manually connect to a wireless network
Connect to a hidden network or create a new wireless profile.

Connect to a workplace
Set up a dial-up or VPN connection to your workplace.

4. Select **Broadband (PPPoE)**.



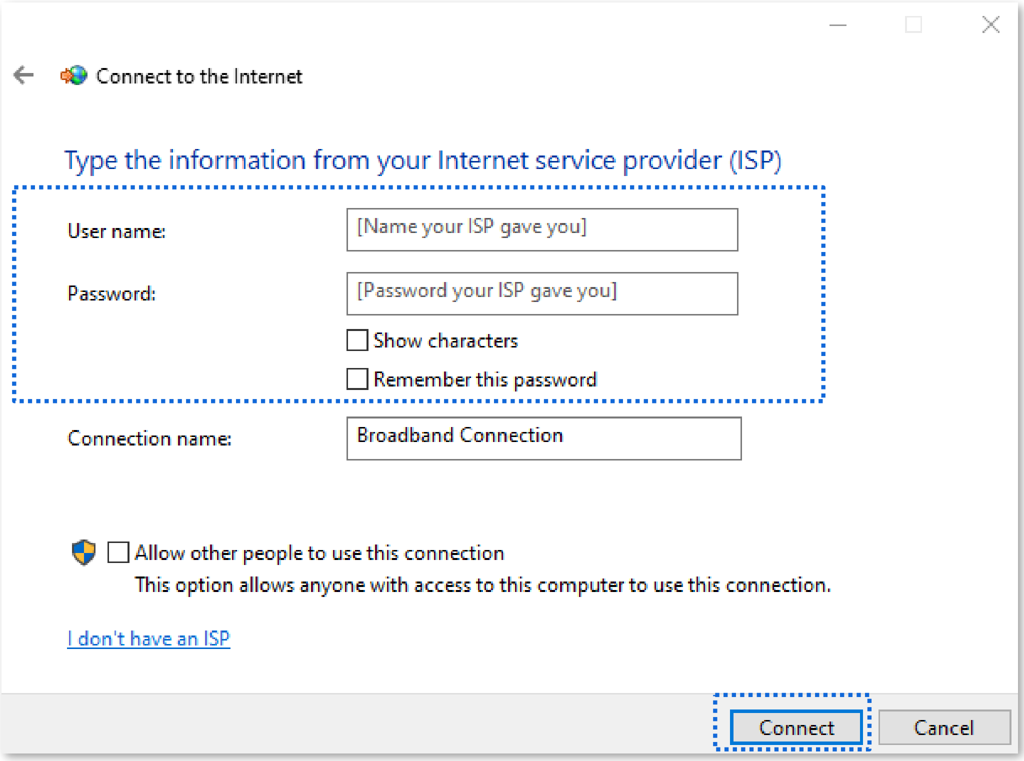
Connect to the Internet

How do you want to connect?

Broadband (PPPoE)
Connect using DSL or cable that requires a user name and password.

Dial-up
Connect using a dial-up modem or ISDN.

5. Enter the PPPoE user name and password, select **Remember this password**, and click **Connect**.



Connect to the Internet

Type the information from your Internet service provider (ISP)

User name: [Name your ISP gave you]

Password: [Password your ISP gave you]

□ Show characters

□ Remember this password

Connection name: Broadband Connection

□ Allow other people to use this connection

This option allows anyone with access to this computer to use this connection.

I don't have an ISP

Wait until the dial-up completes successfully. Then the tenant can access the internet.

To access the internet after the tenant's computer is restarted, click 🖳 and then **Broadband Connection** to perform dial-up again.

6.10 Example of external authentication for tenants

6.10.1 Networking requirements

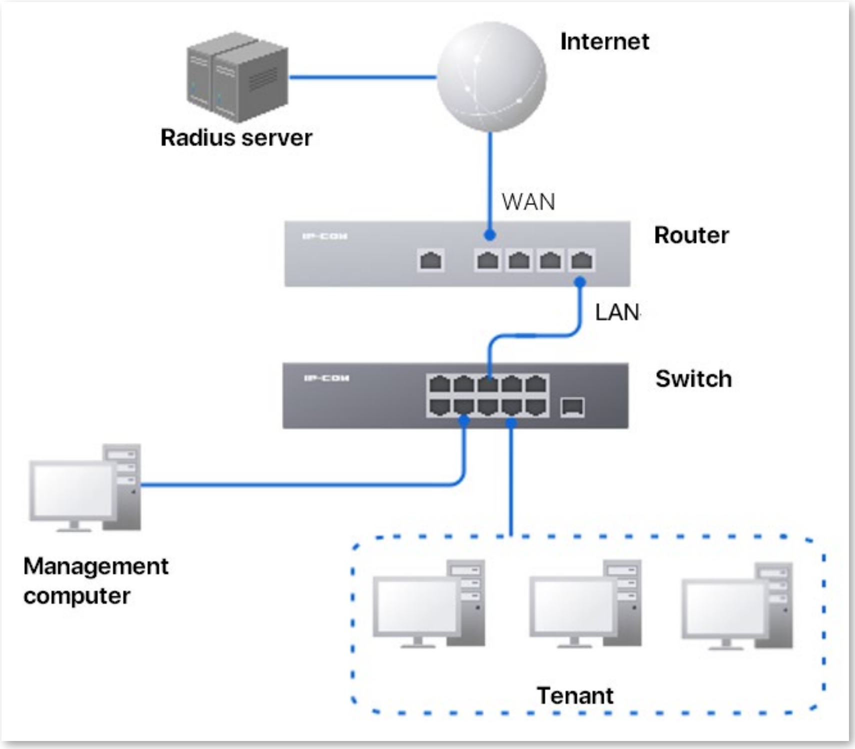
An owner of rented flats uses a router as the egress gateway. Tenants need to pay by month and authenticate using their account and password to get internet access when connecting to the flat network. Assuming the fee payment system is deployed on a Radius server, the configuration parameters are:

- The Radius server is a PPTP server. WAN IP address: 1.10.10.1, Internal IP address: 10.150.0.0/24
- Radius server login username/password: admin
- Radius server shared password: UmXmL9UK
- Radius server authentication username/password: internet-auth

To access the flat network, tenants are required to:

- Authenticate using their account and password
- The flat manager’s computer can access the internet without authentication for convenient management.

The following figure shows the network topology.



6.10.2 Solution

- Configure the router as a PPTP client to access the Radius server.
- Configure account and password authentication.
- Configure the authentication-free policy for the management computer.

6.10.3 Configuration procedure

Configure the Radius server → Configure the router

I. Configure the Radius server

1. Configure a VPN server on the Radius server and configure the username and password for dial-in VPN.

   The VPN values shown below are examples only.

VPN Type	Server Address (Use default settings)	Username/Password	IP Address
PPTP	10.150.0.1	admin	10.150.0.90

2. Configure the corresponding NAS device information on the Radius server. Note that the IP address must be the same as the IP address of the VPN created.

   The NAS values shown below are examples only.

Name	IP Address	Shared Secret
PPTP	10.150.0.90	UmXmL9UK

3. Configure the authentication username and password on the Radius server, for example "internet-auth".

   For detailed instructions, refer to the manual for the Radius server.

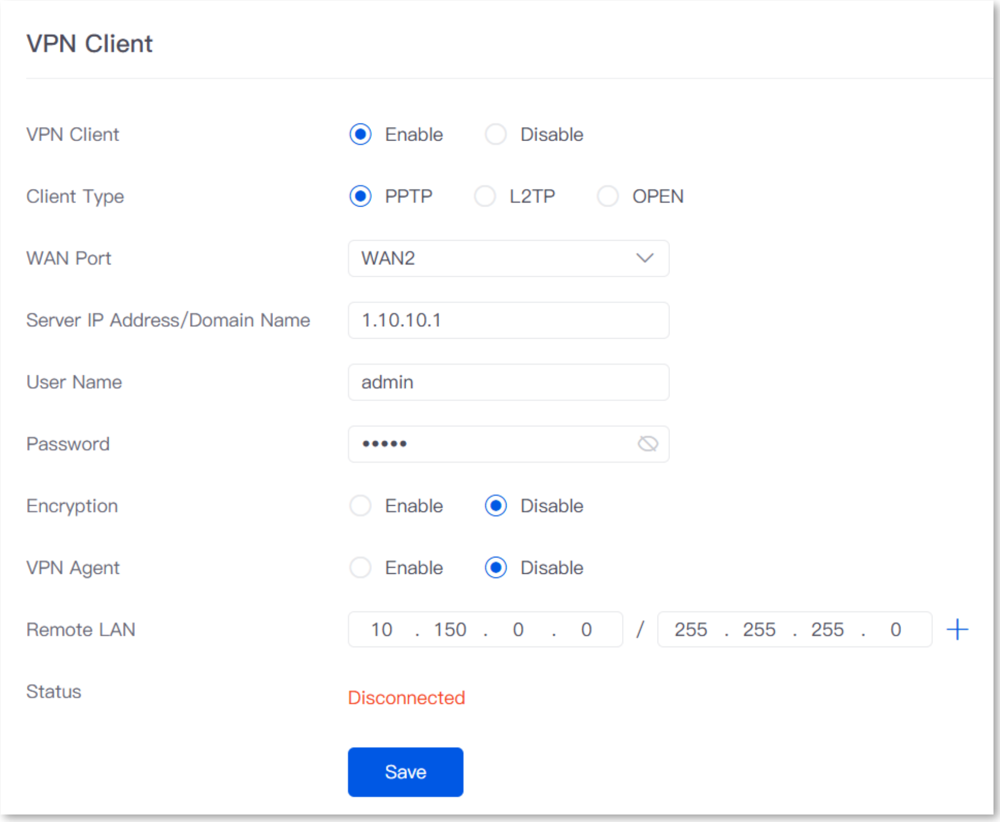
II. Configure the router

1. Log in to the web UI of the router.
2. Configure the router as a PPTP client to connect to the Radius server.

   The PPTP client values shown below are examples only. Keep default settings for other parameters.

PPTP Server Settings
Server WAN IP Address: 1.10.10.1 Server Internal IP Address: 10.150.0/24 Login Username/Password: admin

Navigate to **More** > **VPN Client** and enable the VPN client function. Then configure parameters for the PPTP client and click **Save**.



VPN Client

VPN Client ● Enable ○ Disable

Client Type ● PPTP ○ L2TP ○ OPEN

WAN Port WAN2

Server IP Address/Domain Name 1.10.10.1

User Name admin

Password •••••

Encryption ○ Enable ● Disable

VPN Agent ○ Enable ● Disable

Remote LAN 10 . 150 . 0 . 0 / 255 . 255 . 255 . 0 +

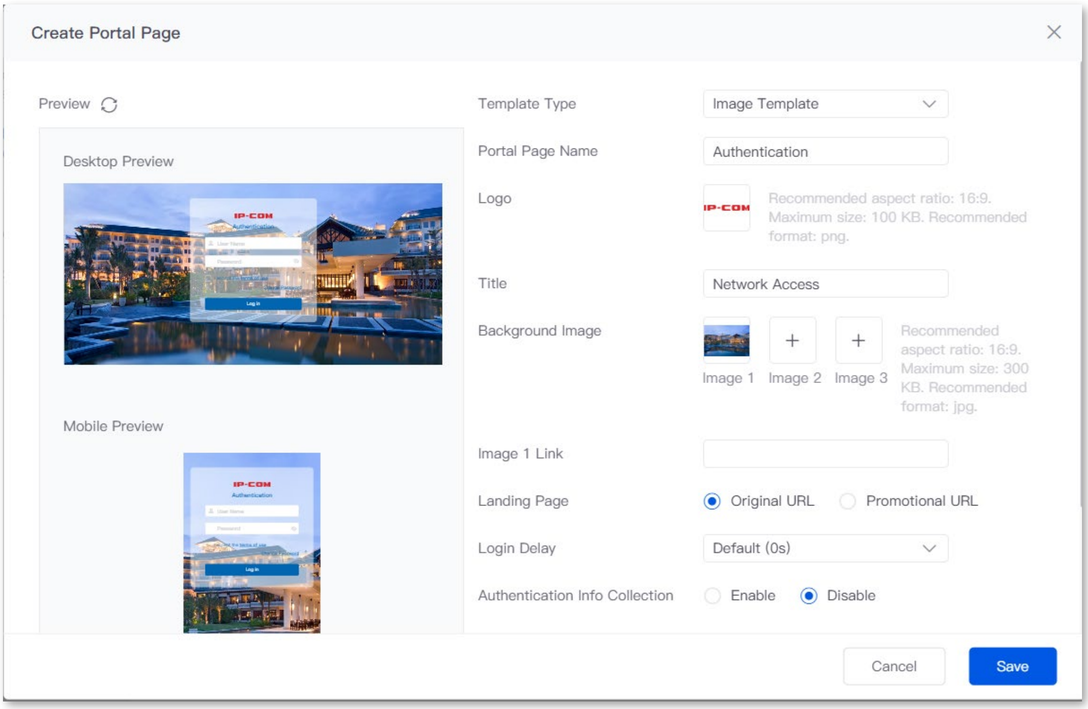
Status Disconnected

When the status shows "Connected," the router has successfully established a VPN connection and can access the Radius server.

3. Configure the Radius server authentication.

   1) Set up the image template.

   Navigate to **AuthN** > **Authentication Template** > **Portal Customization**, then click **Create** to create an image template. The following figure is for reference only.



Create Portal Page

Template Type Image Template

Portal Page Name Authentication

Logo — Recommended aspect ratio: 16:9. Maximum size: 100 KB. Recommended format: png.

Title Network Access

Background Image Image 1 Image 2 Image 3 — Recommended aspect ratio: 16:9. Maximum size: 300 KB. Recommended format: jpg.

Image 1 Link

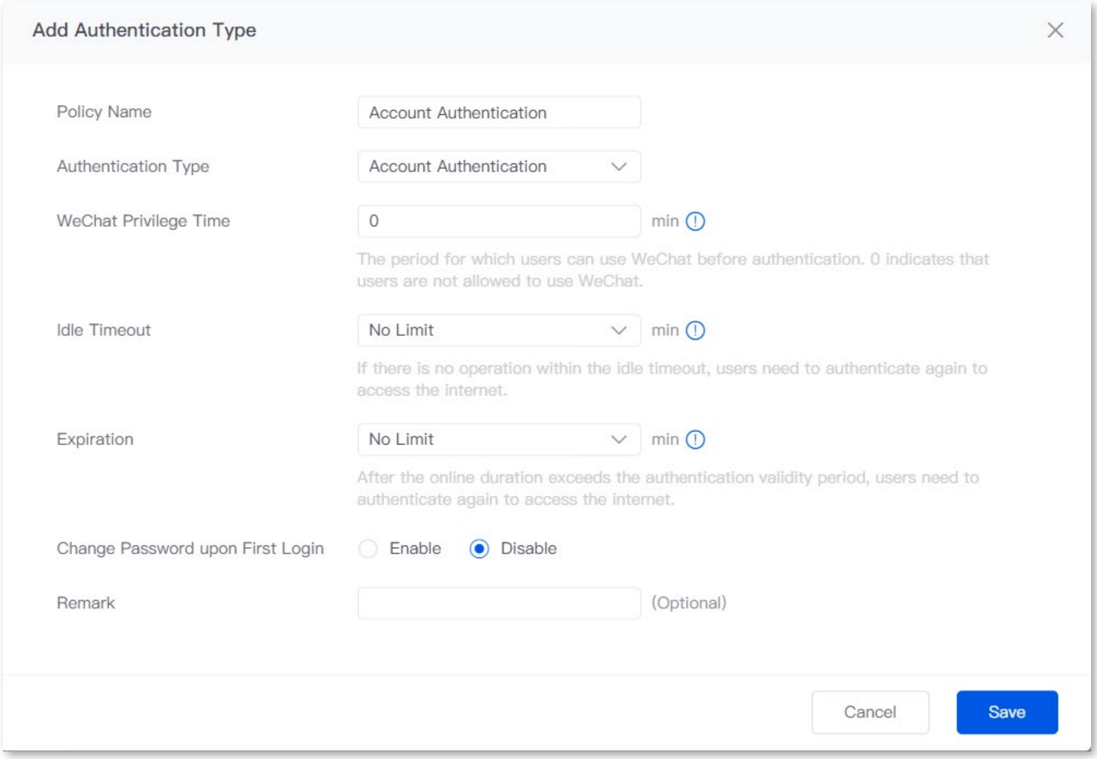
Landing Page ● Original URL ○ Promotional URL

Login Delay Default (0s)

Authentication Info Collection ○ Enable ● Disable

2) Set up the account authentication type.

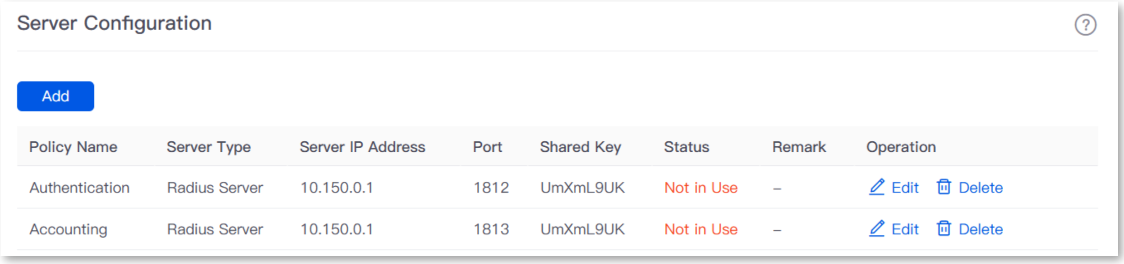
Navigate to **AuthN** > **Authentication Template** > **Authentication Type**, then click **Add** to add an authentication type. The following figure is for reference only.



Policy Name	Account Authentication
Authentication Type	Account Authentication
WeChat Privilege Time	0 min The period for which users can use WeChat before authentication. 0 indicates that users are not allowed to use WeChat.
Idle Timeout	No Limit min If there is no operation within the idle timeout, users need to authenticate again to access the internet.
Expiration	No Limit min After the online duration exceeds the authentication validity period, users need to authenticate again to access the internet.
Change Password upon First Login	○ Enable ● Disable
Remark	(Optional)

3) Set up the Radius server.

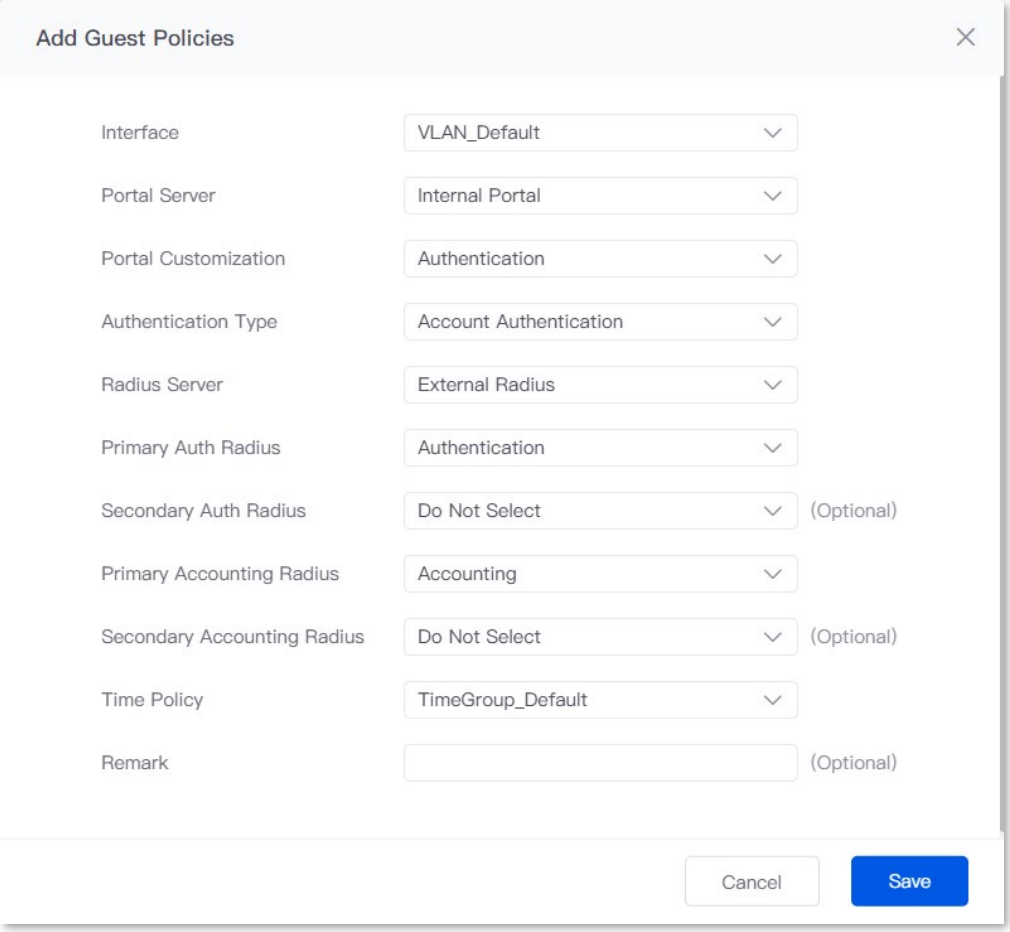
Navigate to the **AuthN** > **Server Configuration**. Click **Add** and add an authentication policy (port 1812) and an accounting policy (port 1813). The following figure is for reference only.



Policy Name	Server Type	Server IP Address	Port	Shared Key	Status	Remark	Operation
Authentication	Radius Server	10.150.0.1	1812	UmXmL9UK	Not in Use	–	Edit Delete
Accounting	Radius Server	10.150.0.1	1813	UmXmL9UK	Not in Use	–	Edit Delete

4) Set up the authentication policy.

Navigate to the **AuthN** > **Guest Policies**. Click **Add** and add a guest policy. Note that for **Primary Auth Radius** and **Primary Accounting Radius**, select the authentication and policies configured on the **Server Configuration** page, respectively.



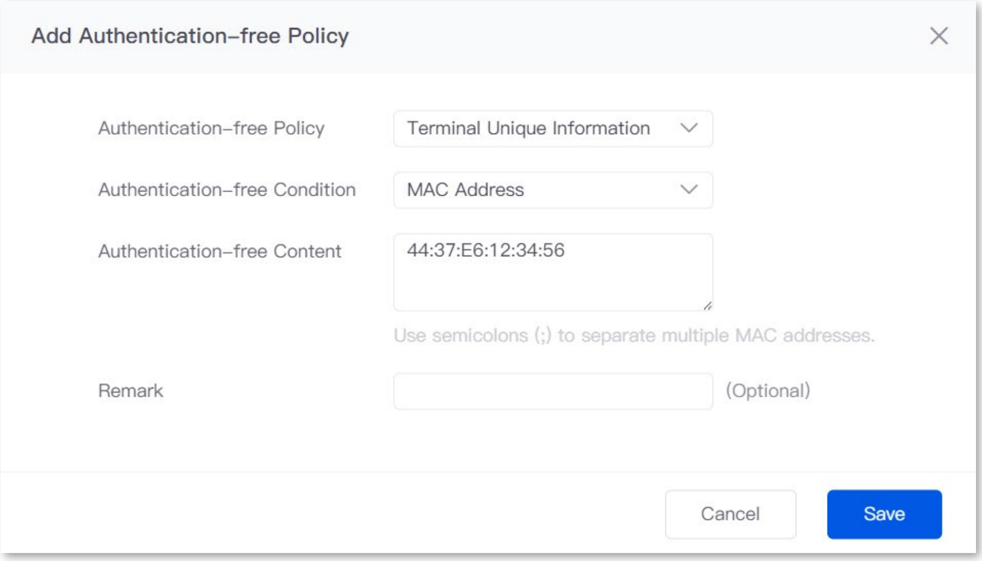
Add Guest Policies

Interface	VLAN_Default	
Portal Server	Internal Portal	
Portal Customization	Authentication	
Authentication Type	Account Authentication	
Radius Server	External Radius	
Primary Auth Radius	Authentication	
Secondary Auth Radius	Do Not Select	(Optional)
Primary Accounting Radius	Accounting	
Secondary Accounting Radius	Do Not Select	(Optional)
Time Policy	TimeGroup_Default	
Remark		(Optional)

4. Set up the authentication-free policy.

   Assume the MAC address of the computer that does not require authentication is 44:37:E6:12:34:56.

   Navigate to the **AuthN** > **Account** > **Authentication-free Policy**. Click **Add**, add an authentication-free policy, then click **Save**.



Add Authentication–free Policy

Authentication–free Policy	Terminal Unique Information	
Authentication–free Condition	MAC Address	
Authentication–free Content	44:37:E6:12:34:56 Use semicolons (;) to separate multiple MAC addresses.	
Remark		(Optional)

---End

6.10.4 Verification

The flat manager's computer (MAC address 44:37:E6:12:34:56) can access the internet without authentication. Tenants need to authenticate with an account and password to access the network.

Access internet via router

This option is suitable when tenants use a router to connect to the flat network’s broadband port. For configuration details, refer to the user manual for the specific router model.

1. Access the management page of the tenant router.
2. Select dynamic IP as the connection type and save the settings.

Connect your phones and tablets to the router’s Wi-Fi and open any webpage. When the authentication page appears, enter your username and password (**internet-auth**) to log in. After authentication, you can access the internet.

Connect your computer to the router via Wi-Fi or an Ethernet cable. Open any webpage to trigger the authentication page, enter your username and password (**internet-auth**) to log in. After authentication, you can access the internet.

Access internet via computer

This option is suitable when tenants connect their computers directly to the flat's broadband network. After connecting, open any web page. When the authentication page appears, enter your authentication username and password (**internet-auth**) to log in. Once authentication is successful, internet access is available.

7 Limit bandwidth usage

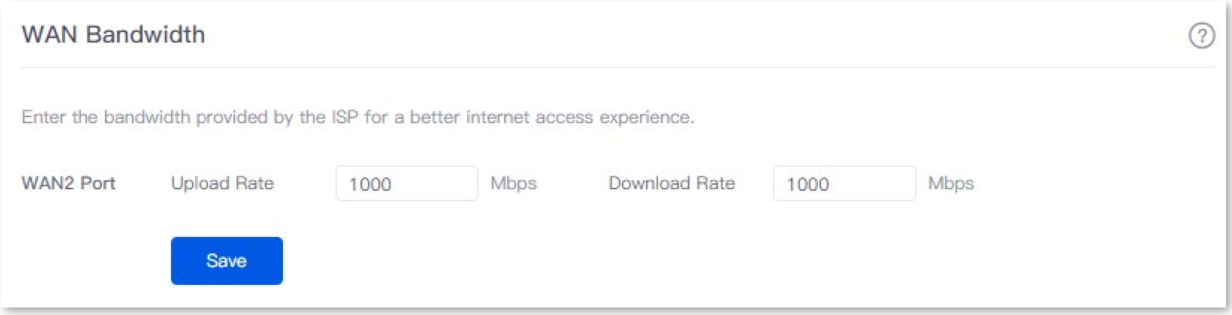
Features available in the router may vary by model and software version. Router availability may also vary by region or ISP. All images, steps, and descriptions in this guide are only examples and may not reflect your actual router experience.

7.1 WAN bandwidth

Log in to the web UI of the router, and 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 Group Speed Limit policy.



WAN Bandwidth

Enter the bandwidth provided by the ISP for a better internet access experience.

WAN2 Port Upload Rate 1000 Mbps Download Rate 1000 Mbps

Parameter description

Parameter	Description
Upload Rate	Specify the bandwidth values of the broadband. If you are not sure, contact your ISP for help.
Download Rate	

7.2 Group limit

Group limit policies are provided for administrators to prioritize network resources for critical operations while meeting your organization's specific bandwidth requirements. By configuring a group limit, you can enable each user within a group to share the total bandwidth.

7.2.1 Example of configuring group limit

Networking requirements

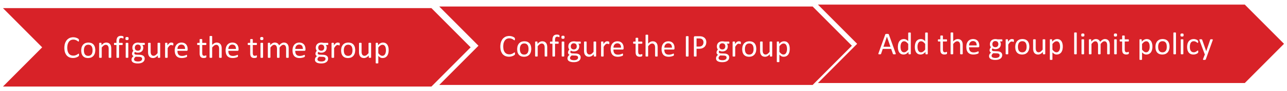
An enterprise uses the enterprise router to deploy a network.

Requirements: Each purchasing staff in the network (IP range: 192.168.0.2 – 192.168.0.50) can share a maximum upload and download bandwidth of 1 Mbps (1 Mbps = 128 KB/s) during working hours (8:00 - 18:00) from Monday to Friday, while users outside the specified IP range are not restricted.

Solution

Configure a group limit based on IP range. Assume that the concurrent connections of each user are 600.

Configuration procedure



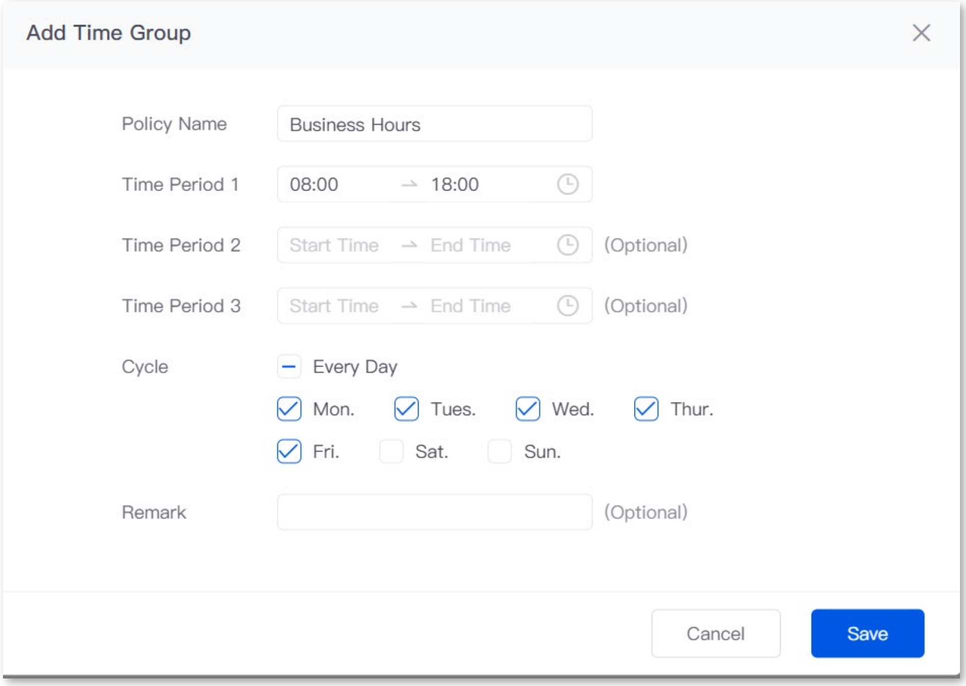
Configure the time group

Configure the IP group

Add the group limit policy

1. [Log in to the web UI of the router](#).
2. Configure the time group.

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



Add Time Group

Policy Name: Business Hours

Time Period 1: 08:00 → 18:00

Time Period 2: Start Time → End Time (Optional)

Time Period 3: Start Time → End Time (Optional)

Cycle: − Every Day

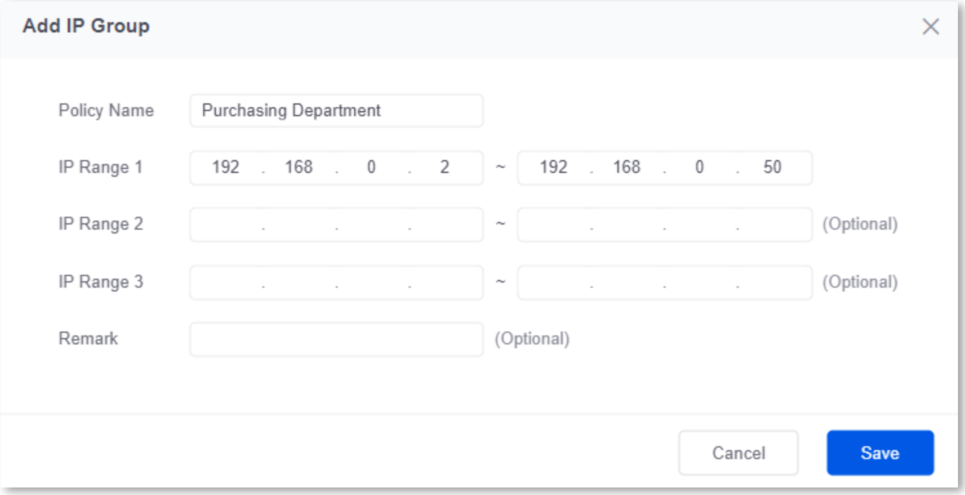
☑ Mon. ☑ Tues. ☑ Wed. ☑ Thur.

☑ Fri. □ Sat. □ Sun.

Remark: (Optional)

3. Configure the IP group.

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

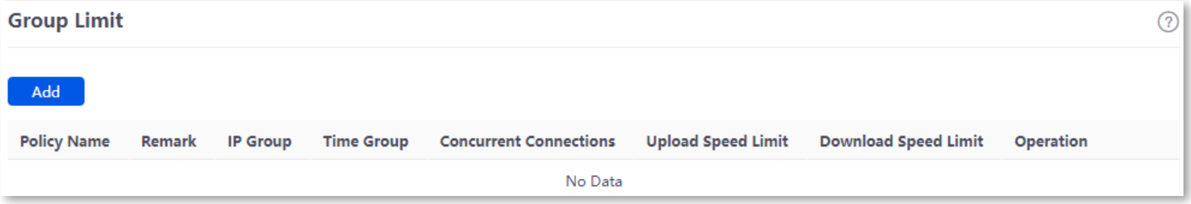


Add IP Group

Policy Name	Purchasing Department		
IP Range 1	192 . 168 . 0 . 2	~	192 . 168 . 0 . 50
IP Range 2	. . .	~	. . . (Optional)
IP Range 3	. . .	~	. . . (Optional)
Remark	(Optional)		

4. Add the group limit policy.

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

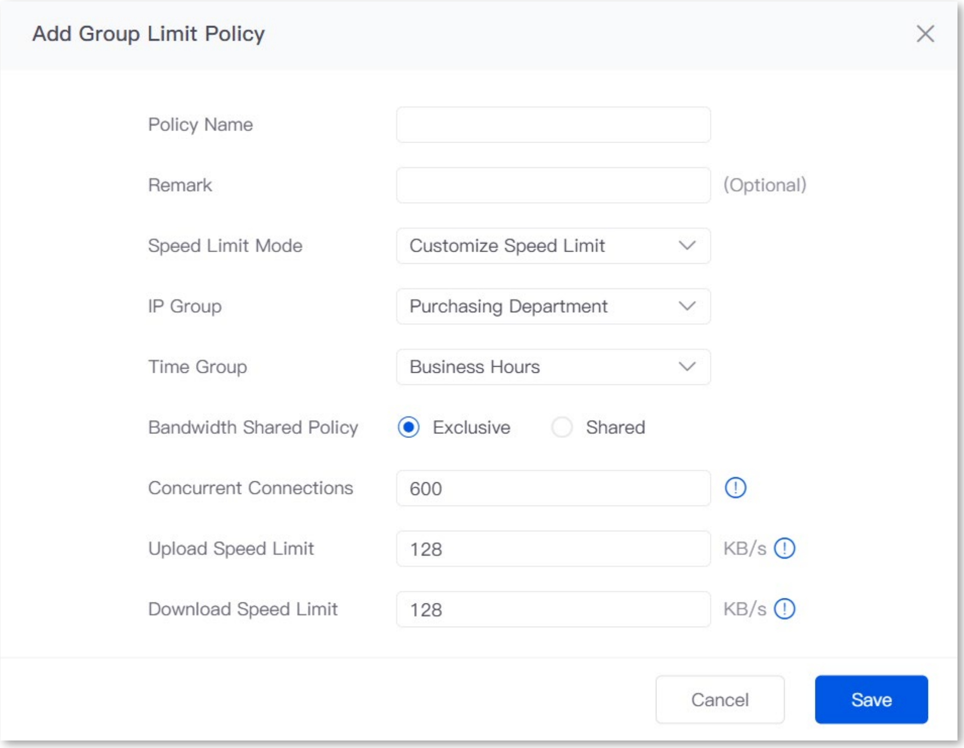


Group Limit

Policy Name	Remark	IP Group	Time Group	Concurrent Connections	Upload Speed Limit	Download Speed Limit	Operation
No Data							

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

- Set the **Policy Name**, which is **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.
- Set the **Concurrent Connections** per client, which is **600** in this example.
- Set the **Upload Speed Limit** and **Download Speed Limit** of client devices, which are both **128** KB/s.



Add Group Limit Policy

Policy Name

Remark (Optional)

Speed Limit Mode: Customize Speed Limit

IP Group: Purchasing Department

Time Group: Business Hours

Bandwidth Shared Policy: ● Exclusive ○ Shared

Concurrent Connections: 600

Upload Speed Limit: 128 KB/s

Download Speed Limit: 128 KB/s

---End

Verification

For users within the IP range 192.168.0.2 - 192.168.0.50, each shares a maximum upload speed and download speed of 128 KB/s during 8:00 - 18:00 from Monday to Friday.

7.2.2 Parameter description

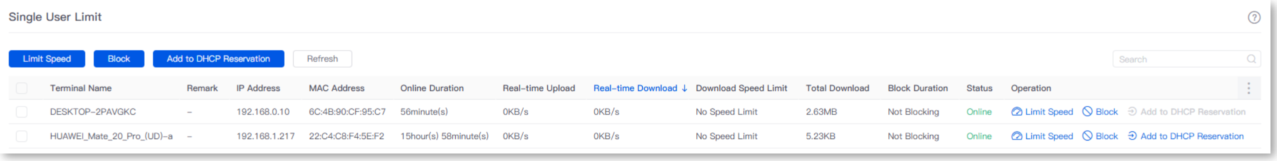
Parameter	Description
IP Group	Specifies the IP address group upon which the group speed limit policy takes effect. The group speed limit policy takes effect only when the device IP addresses are in the IP address group. Configure the IP group at IP Group first.
Time Group	Specifies the time group upon which the group speed limit policy takes effect. The group speed limit policy takes effect only in such configured time. Configure the time group at Time Group first.
Bandwidth Shared Policy	Specifies the bandwidth allocation methods for users within an IP group: – **Shared**: All users within the IP group share the allocated bandwidth. – **Exclusive**: Each user enjoys the allocated bandwidth independently.

Parameter	Description
Concurrent Connections	Specifies the maximum connections for a single use device in the controlled IP group. Tip **0** indicates no limit.
Upload Speed Limit	Specify the maximum upload or download rate of the controlled user. Tip **0** indicates no limit.
Download Speed Limit	

7.3 Single user limit

[Log in to the web UI of the router](), and navigate to **BW Limit** > **Single User Limit**.

You can restrict the upload/download speed, assign static IP addresses, or block internet access for certain users. Blocked devices regain access automatically when the block period ends or is removed. The following figure is for reference only.



Terminal Name	Remark	IP Address	MAC Address	Online Duration	Real-time Upload	Real-time Download ↓	Download Speed Limit	Total Download	Block Duration	Status	Operation
DESKTOP-2PAVGKC	-	192.168.0.10	6C:4B:90:CF:95:C7	56minute(s)	0KB/s	0KB/s	No Speed Limit	2.63MB	Not Blocking	Online	Limit Speed Block Add to DHCP Reservation
HUAWEI_Mate_20_Pro_(UD)-a	-	192.168.1.217	22:C4:C8:F4:5E:F2	15hour(s) 58minute(s)	0KB/s	0KB/s	No Speed Limit	5.23KB	Not Blocking	Online	Limit Speed Block Add to DHCP Reservation

Button description

Button	Description
Limit Speed	Specifies the maximum upload/download speed for the user.
⊘ Block	Used to block a user for a specified duration, or unblock the user.
Add to DHCP Reservation	Used to assign the obtained IP address to the user.
Limit Speed	Specifies the maximum upload/download speed for selected users.
Block	Used to block selected users for a specified duration, or unblock the users.
Add to DHCP Reservation	Used to assign the obtained IP address to selected users.

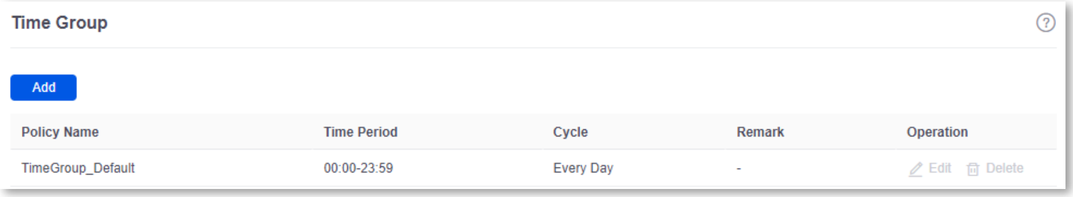
8 Manage behavior & audit

Features available in the router may vary by model and software version. Router availability may also vary by region or ISP. All images, steps, and descriptions in this guide are only examples and may not reflect your actual router experience.

8.1 Group policy

8.1.1 Configure time group

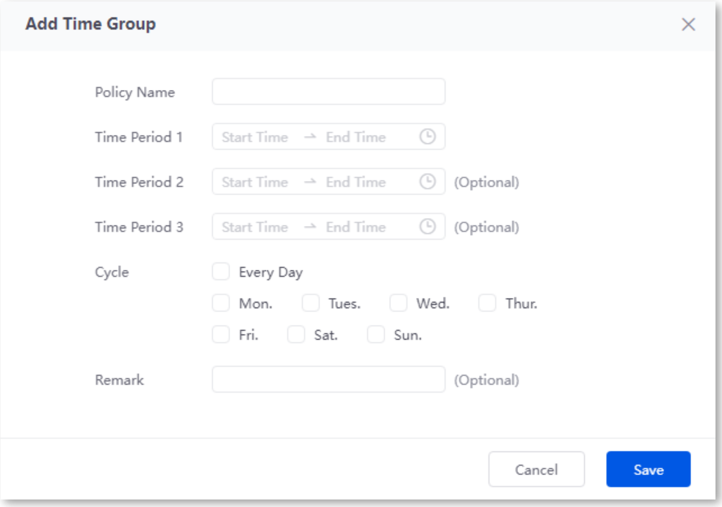
1. Log in to the web UI of the router, then navigate to **Audit** > **Group Policy** > **Time Group**.
2. Click **Add**.



Time Group

Policy Name	Time Period	Cycle	Remark	Operation
TimeGroup_Default	00:00-23:59	Every Day	-	Edit Delete

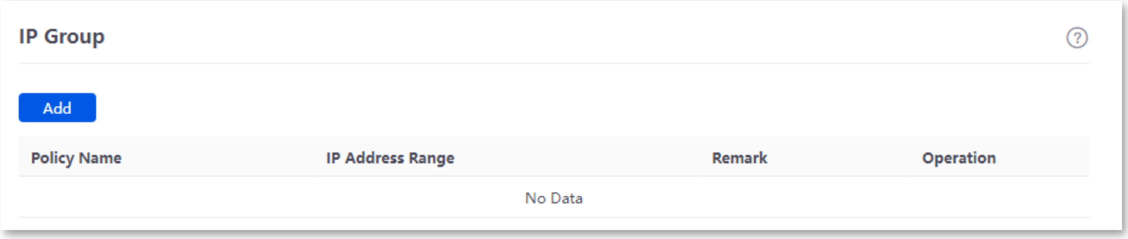
3. Configure the parameters in the **Add Time Group** window, and click **Save**.
   - **Time Period**: Specifies the periods included in the time group. One policy supports at most 3 periods, and the periods cannot be repeated.
   - **Cycle**: Specifies the cycle upon which the time group policy takes effect.



---End

8.1.2 Configure IP group

1. Log in to the web UI of the router, then navigate to **Audit** > **Group Policy** > **IP Group**.
2. Click **Add**.



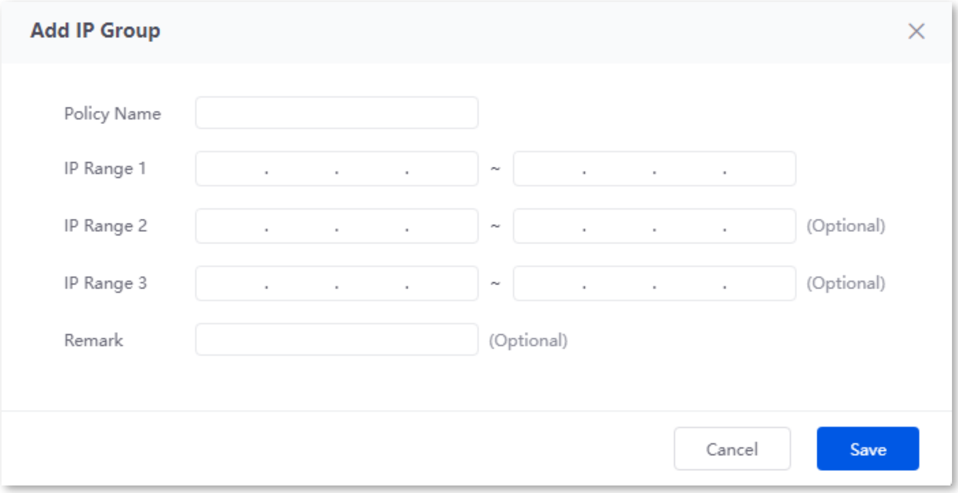
IP Group

Add

Policy Name	IP Address Range	Remark	Operation
No Data			

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

   IP Range: Specifies the IP ranges included in the IP group. One policy supports at most 3 IP ranges, and the IP ranges cannot be repeated.



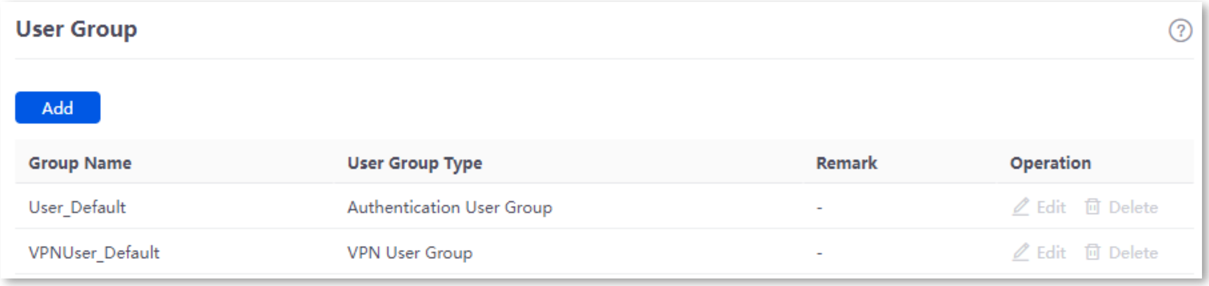
---End

8.1.3 Configure user group

Tip

Two user groups named **User_Default** and **VPNUser_Default** have been added by default. The default user group cannot be deleted or edited.

1. Log in to the web UI of the router, then navigate to **Audit** > **Group Policy** > **User Group**.
2. Click **Add**.



User Group

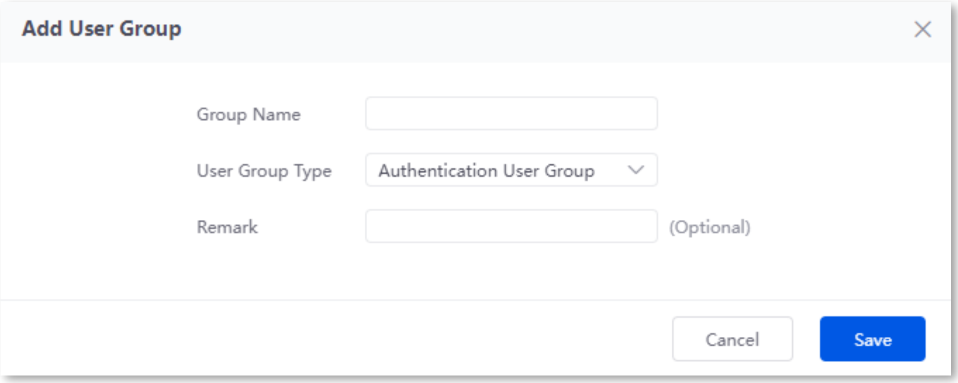
Add

Group Name	User Group Type	Remark	Operation
User_Default	Authentication User Group	-	Edit Delete
VPNUser_Default	VPN User Group	-	Edit Delete

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

   – When **User Group Type** is **Authentication User Group**: The user group is referenced by account management.

   – When **User Group Type** is **VPN User Group**: The user group is referenced by user management.



Add User Group

Group Name

User Group Type: Authentication User Group

Remark (Optional)

---End

8.2 Filtering

8.2.1 IP address filtering

Log in to the web UI of the router, and 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 the internet.

Example of configuring IP address filtering

Networking requirements

An enterprise uses the enterprise router to deploy a network.

Requirements: During 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

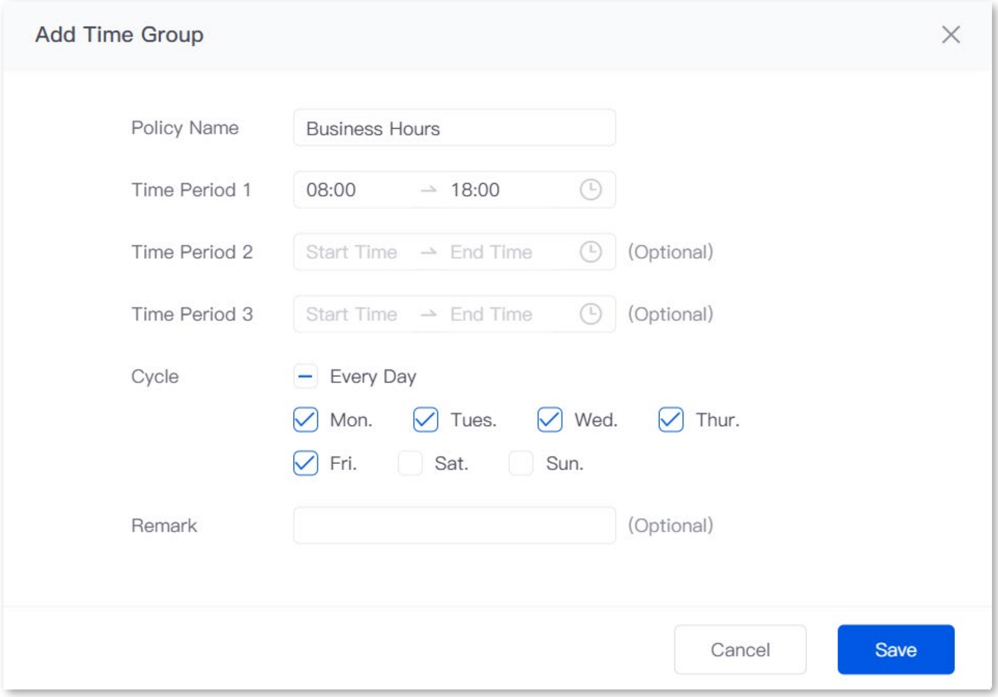
The router’s IP address filtering function can achieve the requirements. Assume that the IP addresses of the purchasing staff’s computers range from 192.168.0.2 - 192.168.0.50.

Configuration procedure

Configure the time group → Configure the IP group → Add the IP address filtering policy

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

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



Add Time Group ×

Policy Name: Business Hours

Time Period 1: 08:00 → 18:00

Time Period 2: Start Time → End Time (Optional)

Time Period 3: Start Time → End Time (Optional)

Cycle: ⊟ Every Day

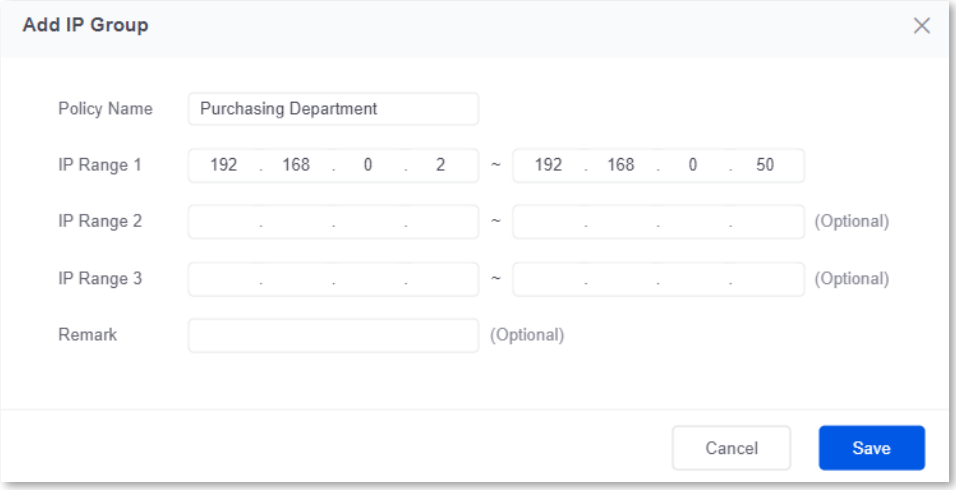
☑ Mon. ☑ Tues. ☑ Wed. ☑ Thur.

☑ Fri. □ Sat. □ Sun.

Remark: (Optional)

3. Configure the IP group.

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



Policy Name: Purchasing Department

IP Range 1: 192 . 168 . 0 . 2 ~ 192 . 168 . 0 . 50

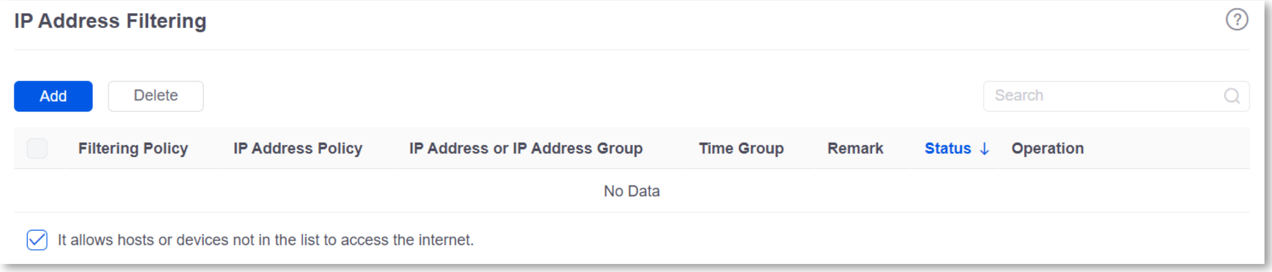
IP Range 2: . . . ~ . . . (Optional)

IP Range 3: . . . ~ . . . (Optional)

Remark: (Optional)

4. Add the IP address filtering policy.

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



Filtering Policy	IP Address Policy	IP Address or IP Address Group	Time Group	Remark	Status ↓	Operation
No Data						

☑ It allows hosts or devices not in the list to access the internet.

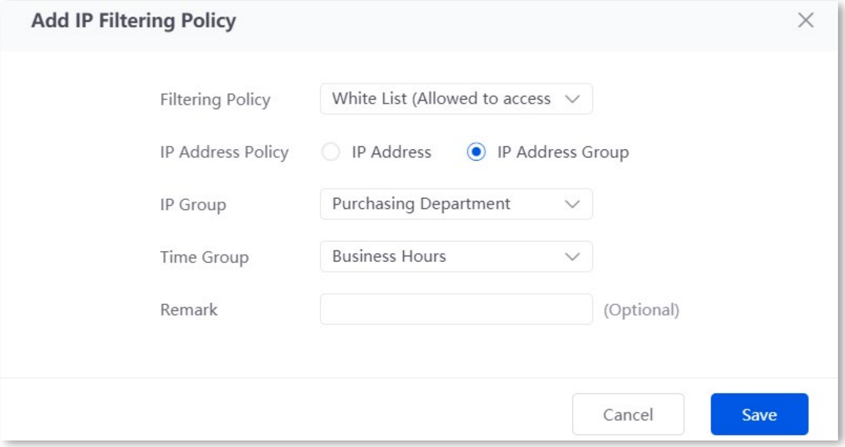
   2) Configure the parameters in the **Add IP Filtering Policy** window, and click **Save**.

      – Select the **Filtering Policy**, which is **White List (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.



Filtering Policy: White List (Allowed to access

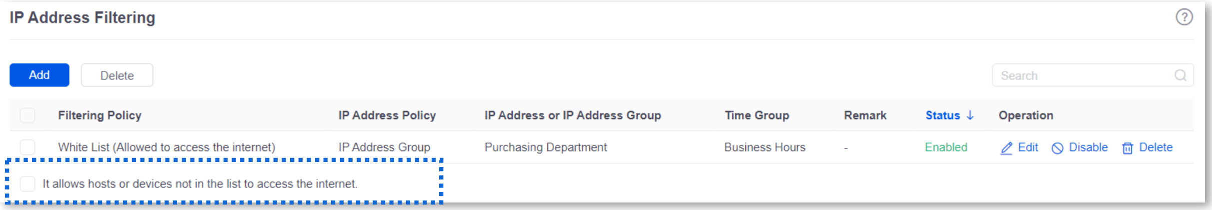
IP Address Policy: ○ IP Address ● IP Address Group

IP Group: Purchasing Department

Time Group: Business Hours

Remark: (Optional)

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



IP Address Filtering

□	Filtering Policy	IP Address Policy	IP Address or IP Address Group	Time Group	Remark	Status ↓	Operation
□	White List (Allowed to access the internet)	IP Address Group	Purchasing Department	Business Hours	-	Enabled	Edit Disable Delete

□ It allows hosts or devices not in the list to access the internet.

---End

Verification

Only the computers of the 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 at 8:00 – 18:00 from Monday to Friday.

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 period, and is allowed to access the internet during other times. – **White List (Allowed to access the internet)**: The user with the specified IP address is allowed to access the internet during the specified period, and is blocked from accessing the internet during other times.
IP Address Policy	To filter one IP address, select **IP Address** and enter the IP address. To filter one or more IP ranges, select **IP Address Group** and select the corresponding IP group policy you set. Tip The IP group should be configured at IP Group in advance.
IP Address or IP Address Group	
Time Group	Used to select the time group policy upon which the IP address filtering policy takes effect. Tip The time group should be configured at Time Group in advance.
It allows hosts or devices not in the list to access the internet.	– When Selected: The devices not in the filtering list or devices with the filtering policy disabled can access the internet. – When Deselected: The devices not in the filtering list or devices with the filtering policy disabled cannot access the internet. Tip To deselect this function, configure a whitelist first.

8.2.2 MAC address filtering

Log in to the web UI of the router, and 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 the internet.

Example of configuring MAC address filtering

Networking requirements

An enterprise uses the enterprise router to deploy a network.

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

Solution

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

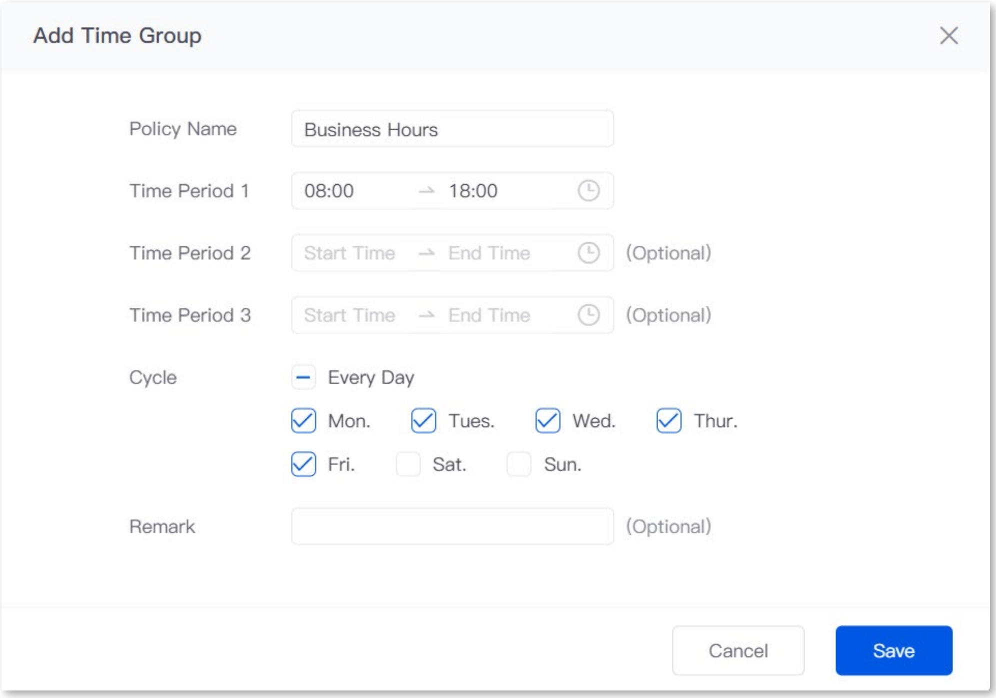
Configuration procedure

Configure the time group

Add the MAC address filtering policy

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

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



Add Time Group

Policy Name: Business Hours

Time Period 1: 08:00 → 18:00

Time Period 2: Start Time → End Time (Optional)

Time Period 3: Start Time → End Time (Optional)

Cycle: − Every Day

☑ Mon. ☑ Tues. ☑ Wed. ☑ Thur.

☑ Fri. □ Sat. □ Sun.

Remark: (Optional)

Cancel Save

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**.

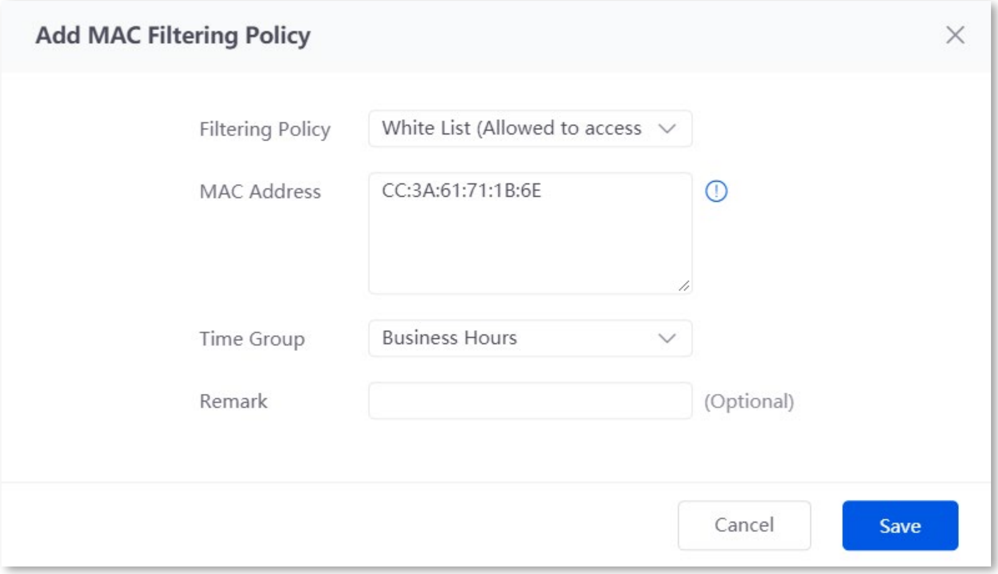
      – Select the **Filtering Policy**, which is **White List (Allowed to access the internet)** in this example.

      – 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.



Add MAC Filtering Policy

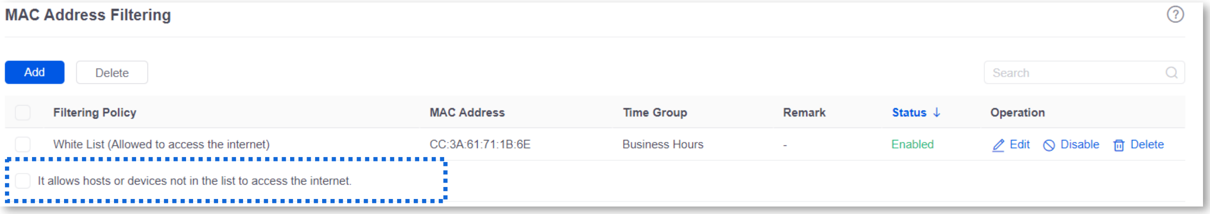
Filtering Policy: White List (Allowed to access

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

Time Group: Business Hours

Remark: (Optional)

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



MAC Address Filtering

	Filtering Policy	MAC Address	Time Group	Remark	Status ↓	Operation
□	White List (Allowed to access the internet)	CC:3A:61:71:1B:6E	Business Hours	-	Enabled	Edit Disable Delete

□ It allows hosts or devices not in the list to access the internet.

---End

Verification

Only the 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 at 8:00 – 18:00 from Monday to Friday.

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 period, and is allowed to access the internet during other times. – **White List (Allowed to access the internet)**: The user with the specified MAC address is allowed to access the internet during the specified period, and is blocked from accessing the internet during other times.
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. Tip The time group should be configured at Time Group in advance.
Remark	(Optional) Specifies the remark of the MAC address filtering policy.
Status	Specifies the status of the MAC address filtering policy including **Enabled** or **Disabled**.
It allows hosts or devices not in the list to access the internet.	– When Selected: The devices not in the filtering list or devices with the filtering policy disabled can access the internet. – When Deselected: The devices not in the filtering list or devices with the filtering policy disabled cannot access the internet. Tip To deselect this function, configure a whitelist first.

8.2.3 Port filtering

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.

Log in to the web UI of the router, and 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.

Example of configuring port filtering

Networking requirements

An enterprise uses the enterprise router to deploy a network.

Requirements: During 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 requirements. Assume that the IP address of the purchasing staff's computers ranges from 192.168.0.2 – 192.168.0.50.

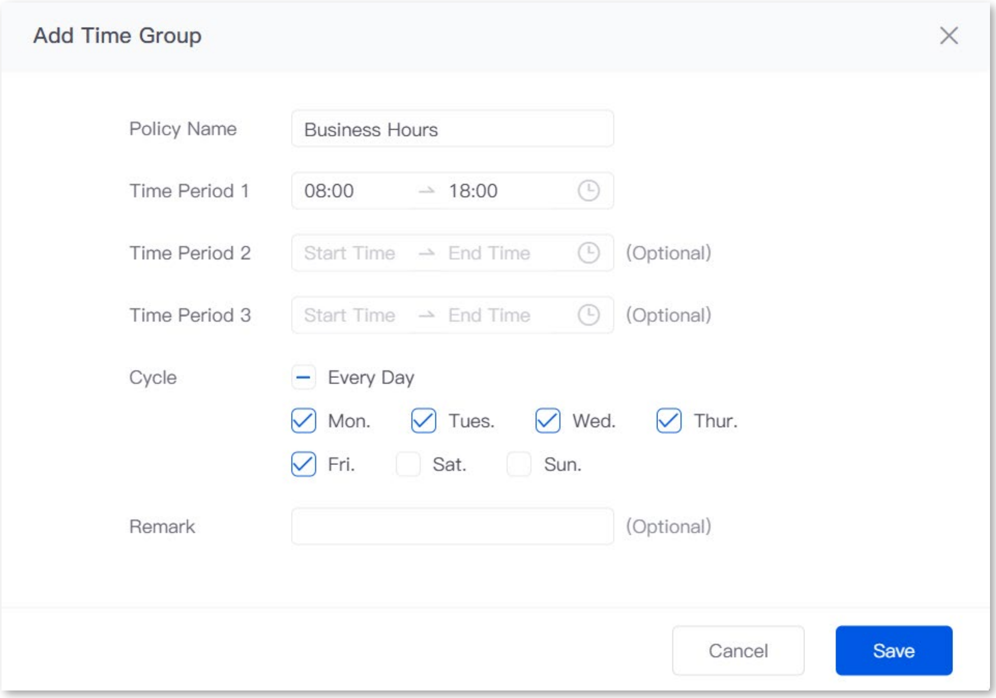
Configuration procedure

Configure the time group → Configure the IP group → Add the port filtering policy

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

2. Configure the time group.

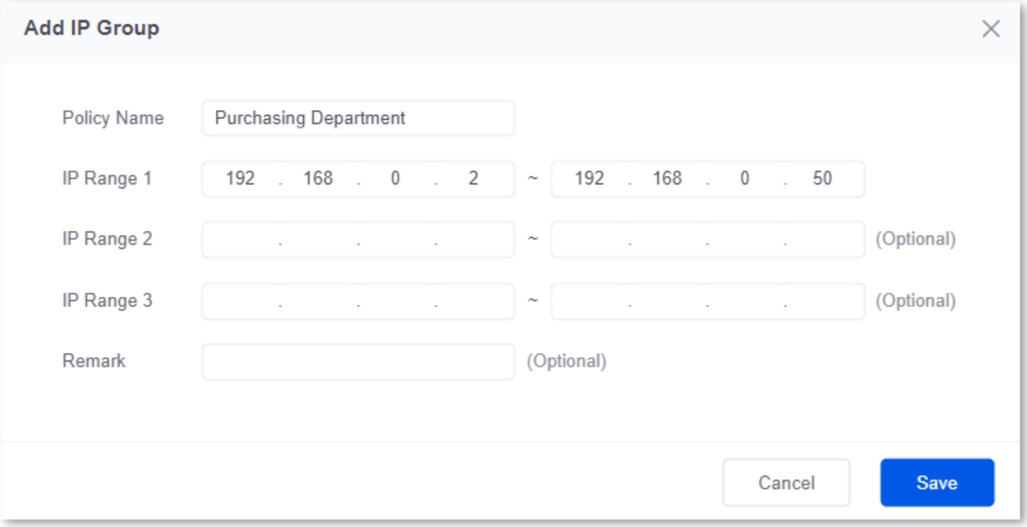
   Navigate to **Audit** > **Group Policy** > **Time Group**, and click **Add** to configure the following time group.


Add Time Group

Policy Name	Business Hours
Time Period 1	08:00 → 18:00
Time Period 2	Start Time → End Time (Optional)
Time Period 3	Start Time → End Time (Optional)
Cycle	☐ Every Day ☑ Mon. ☑ Tues. ☑ Wed. ☑ Thur. ☑ Fri. ☐ Sat. ☐ Sun.
Remark	(Optional)

3. Configure the IP group.

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



Add IP Group

Policy Name: Purchasing Department

IP Range 1: 192 . 168 . 0 . 2 ~ 192 . 168 . 0 . 50

IP Range 2: . . . ~ . . . (Optional)

IP Range 3: . . . ~ . . . (Optional)

Remark: (Optional)

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.

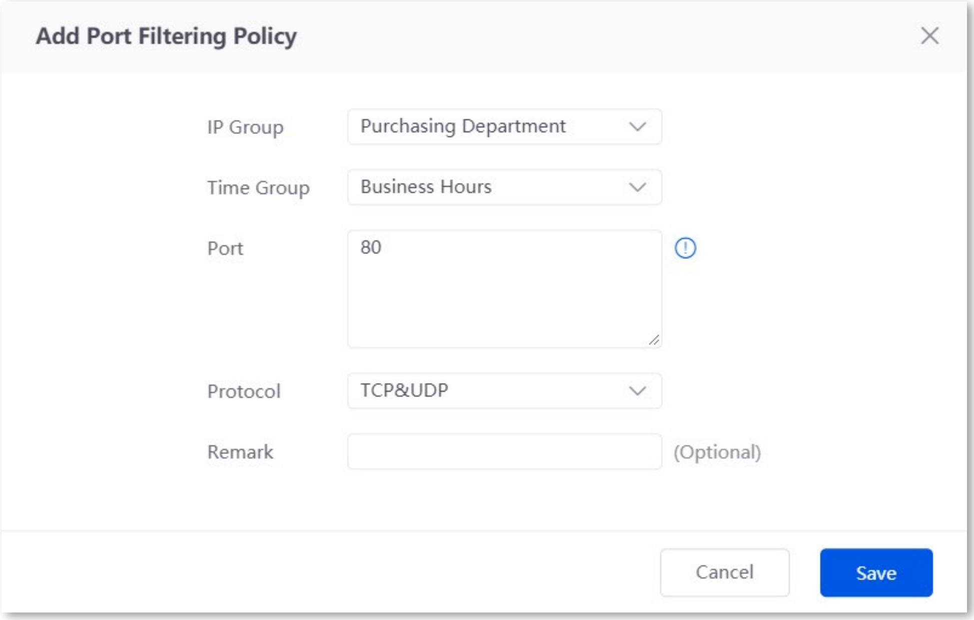
      – Enter the **Port** number for webpage browsing, which is **80** in this example.

      – 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**.



Add Port Filtering Policy

IP Group: Purchasing Department

Time Group: Business Hours

Port: 80

Protocol: TCP&UDP

Remark: (Optional)

---End

Verification

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

Parameter description

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

8.2.4 URL filtering

Log in to the web UI of the router, and 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.

Example of configuring URL filtering

Networking requirements

An enterprise uses the enterprise router to deploy a network.

Requirements: During 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

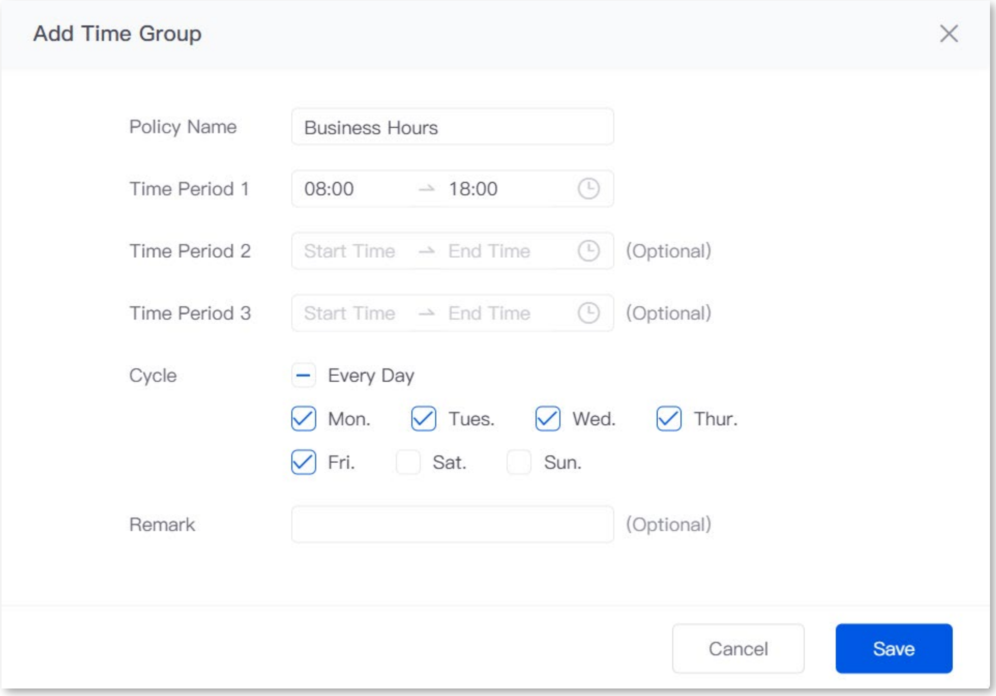
The router's URL filtering function can achieve the requirements. Assume that the IP addresses of designers' computers range from 192.168.0.60 - 192.168.0.100.

Configuration procedure

Configure the time group → Configure the IP group → Add the URL filtering policy

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

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



Add Time Group

Policy Name: Business Hours

Time Period 1: 08:00 → 18:00

Time Period 2: Start Time → End Time (Optional)

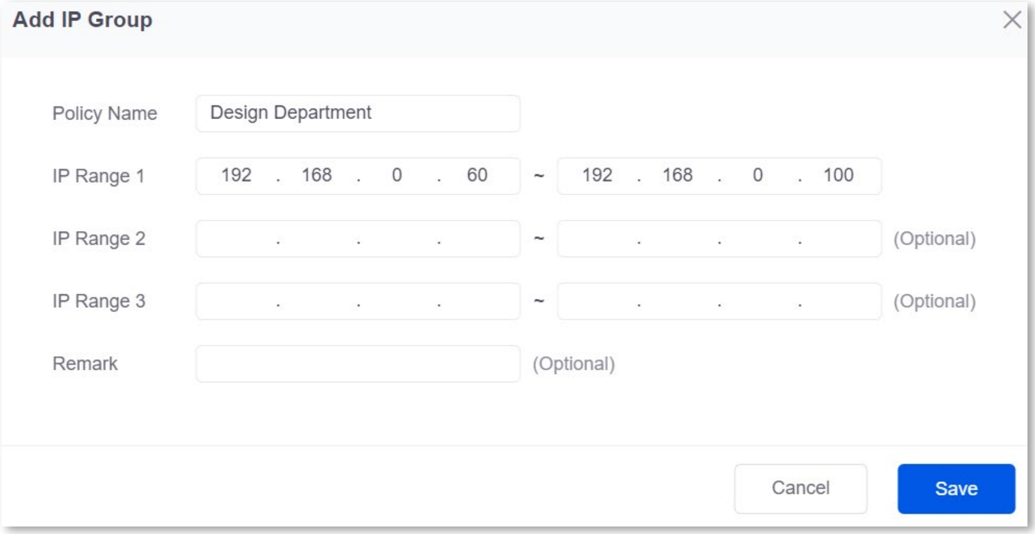
Time Period 3: Start Time → End Time (Optional)

Cycle: ▣ Every Day
☑ Mon. ☑ Tues. ☑ Wed. ☑ Thur.
☑ Fri. □ Sat. □ Sun.

Remark: (Optional)

3. Configure the IP group.

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



Add IP Group

Policy Name	Design Department	
IP Range 1	192 . 168 . 0 . 60 ~ 192 . 168 . 0 . 100	
IP Range 2	. . . ~ . . .	(Optional)
IP Range 3	. . . ~ . . .	(Optional)
Remark		(Optional)

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**.

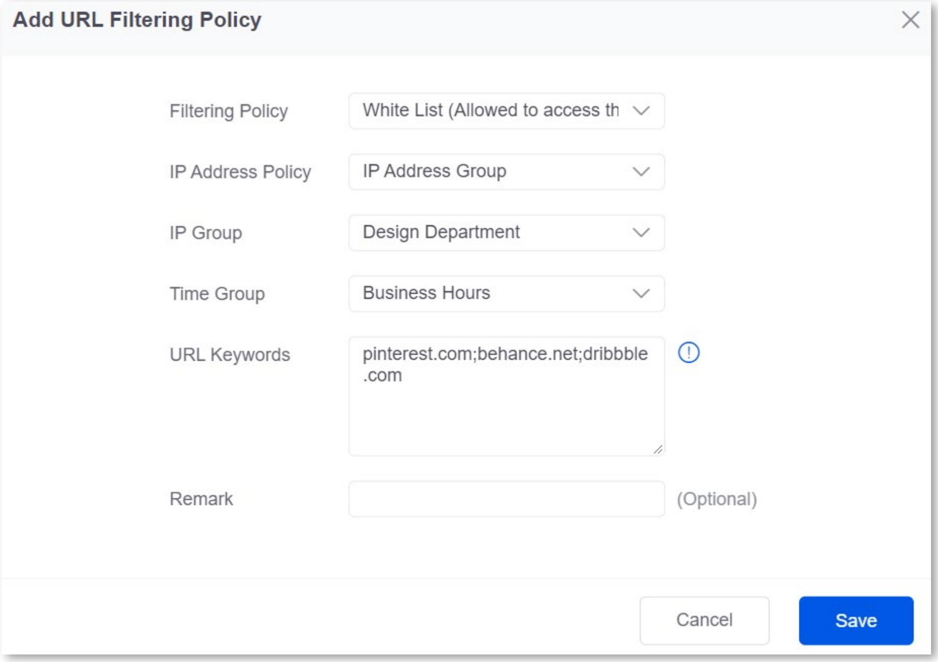
      – Select the **Filtering Policy**, which is **White List (Allowed to access the internet)** in this example.

      – 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.

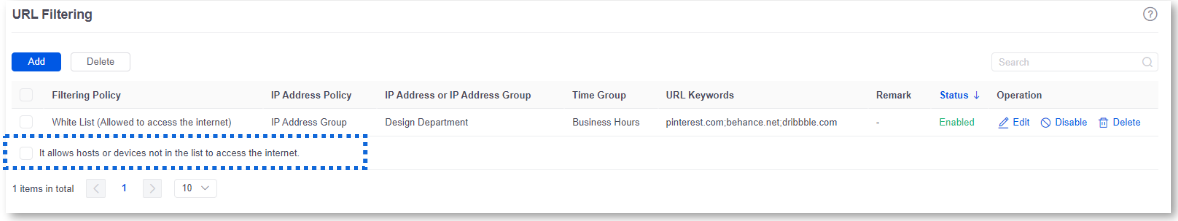
      – Specify the **URL Keywords**, which are **pinterest.com;behance.net;dribbble.com** in this example.



Add URL Filtering Policy

Filtering Policy	White List (Allowed to access th	
IP Address Policy	IP Address Group	
IP Group	Design Department	
Time Group	Business Hours	
URL Keywords	pinterest.com;behance.net;dribbble .com	
Remark		(Optional)

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



□	Filtering Policy	IP Address Policy	IP Address or IP Address Group	Time Group	URL Keywords	Remark	Status ↓	Operation
□	White List (Allowed to access the internet)	IP Address Group	Design Department	Business Hours	pinterest.com;behance.net;dribbble.com	-	Enabled	Edit Disable Delete

□ It allows hosts or devices not in the list to access the internet.

1 items in total < 1 > 10

---End

Verification

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 at 8:00 – 18:00 from Monday to Friday.

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 period, and is allowed to access all websites during other times. – **White List (Allowed to access the internet)**: The user with the specified IP address is only allowed to access specified websites during the specified period, and is allowed to access all websites during other times.
IP Address Policy	To filter one IP address, select **IP Address** and enter the IP address. To filter one or more IP ranges, select **IP Address Group** and select the corresponding IP group policy you set. Tip The IP group should be configured at IP Group in advance.
IP Address or IP Address Group	
Time Group	Used to select the time group policy upon which the URL filtering policy takes effect. Tip The time group should be configured at Time Group in advance.
URL Keywords	Specifies the keywords of the URL forbidden or allowed to access.

Parameter	Description
It allows hosts or devices not in the list to access the internet.	– When Selected: The devices not in the filtering list or devices with the filtering policy disabled can access the specified websites. – When Deselected: The devices not in the filtering list or devices with the filtering policy disabled cannot access the specified websites. Tip To deselect this function, configure a whitelist first.

8.2.5 Wireless MAC filtering

Log in to the web UI of the router, and navigate to **Audit** > **Filtering** > **Wireless MAC Filtering** to enter the page.

On this page, you can allow or block mobile users in the LAN to connect to specified wireless networks based on their wireless MAC addresses.

Example of configuring wireless MAC filtering

Networking requirements

An enterprise uses the router to set up a network. The router is connected to an AP (managed by the router), and already delivers the wireless network named VIP to the AP.

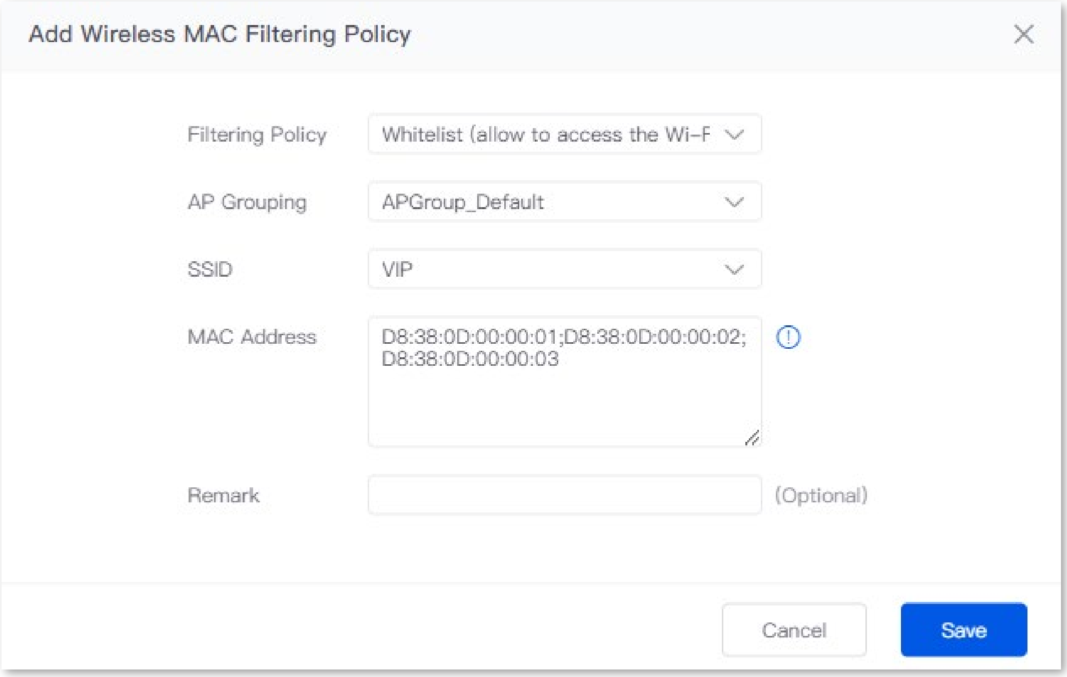
Requirement: The wireless network of VIP only opens access to several devices.

Solution

The router’s wireless MAC filtering function can achieve the requirements. Assume that only 3 wireless devices are allowed to connect to the wireless network of VIP during business hours. The MAC addresses are D8:38:0D:00:00:01, D8:38:0D:00:00:02 and D8:38:0D:00:00:03.

Configuration procedure

1. Log in to the web UI of the router.
2. Add the wireless MAC filtering policy.
   1) Navigate to **Audit** > **Filtering** > **Wireless MAC Filtering**, and click **Add**.
   2) Configure the parameters in the **Add Wireless MAC Filtering Policy** window, and click **Save**.
      – Select the **Filtering Policy**, which is **Whitelist (allow to access the Wi-Fi network)** in this example.
      – Select the **AP Grouping**, which is **APGroup_Default** in this example.
      – Select the applied **SSID**, which is **VIP** (set in advance) in this example.
      – Enter the **MAC Addresses** upon which the policy takes effect, which are **D8:38:0D:00:00:01;D8:38:0D:00:00:02;D8:38:0D:00:00:03** in this example.


Add Wireless MAC Filtering Policy

Filtering Policy: Whitelist (allow to access the Wi-F

AP Grouping: APGroup_Default

SSID: VIP

MAC Address: D8:38:0D:00:00:01;D8:38:0D:00:00:02;
D8:38:0D:00:00:03

Remark: (Optional)

---End

Verification

Only the above wireless devices can connect to the network of VIP while other devices cannot.

Parameter description

Parameter	Description
Filtering Policy	Specifies the mode of the wireless MAC address filtering policy. – **Blacklist (prohibit to access the Wi-Fi network)**: The user with the specified MAC address is blocked to access the internet through the specified SSID during the specified period, and is allowed to access the internet through the SSID during other times. – **Whitelist (allow to access the Wi-Fi network)**: The user with the specified MAC address is allowed to access the internet through the specified SSID during the specified period, and is blocked from accessing the internet through the SSID during other times.
AP Grouping	Specifies the group upon which wireless MAC address filtering policy takes effect. The AP group should be configured at AP Groups in advance.
SSID	Used to select the SSID policy upon which the wireless MAC address filtering policy takes effect. The SSID policy should be configured at Wi-Fi Policy in advance.
MAC Address	Specifies the MAC address to be filtered.

8.2.6 User filtering

Log in to the web UI of the router, and navigate to **Audit** > **Filtering** > **User Filtering** to enter the page.

On this page, you can allow or block authenticated users in the LAN to connect to the internet based on users and user groups.

Example of configuring user filtering

Networking requirements

An enterprise uses the router to set up a network. The enterprise has configured the account authentication, and the account has been added to the authenticated user group of R&D Department. Refer to Authentication for specific instructions.

Requirement: During business hours (8:00 -18:00 from Monday to Friday), only one R&D employee authenticated through the user name and password can access the internet while other employees cannot.

Solution

The router's user filtering function can achieve the requirements.

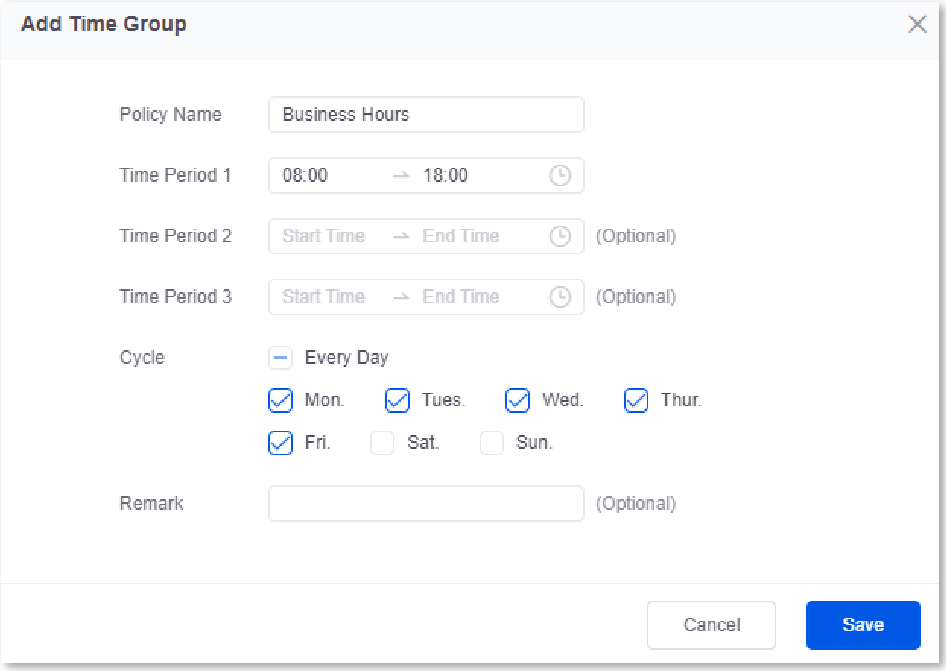
Configuration procedure

Configure the time group

Add the user filtering policy

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

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



Add Time Group

Policy Name: Business Hours

Time Period 1: 08:00 → 18:00

Time Period 2: Start Time → End Time (Optional)

Time Period 3: Start Time → End Time (Optional)

Cycle: ▣ Every Day

☑ Mon. ☑ Tues. ☑ Wed. ☑ Thur.

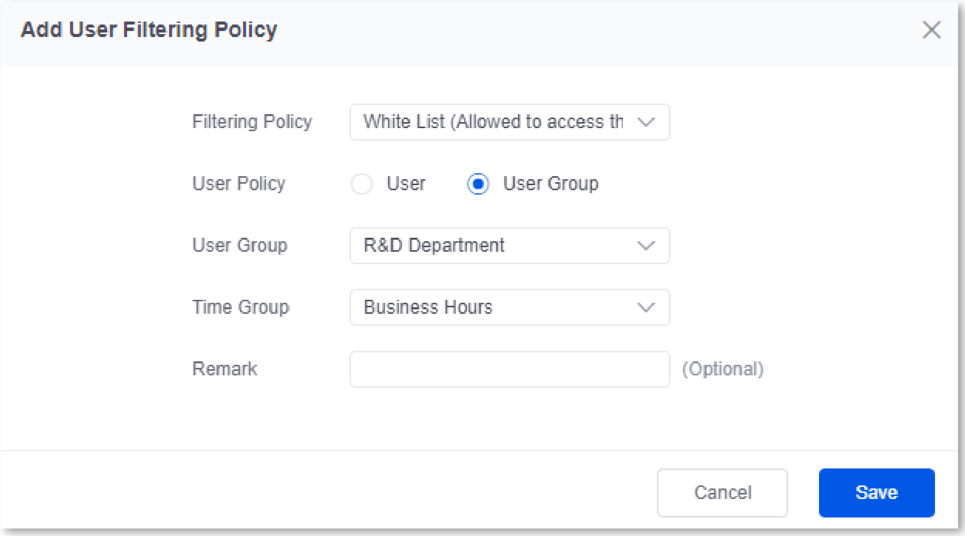
☑ Fri. □ Sat. □ Sun.

Remark: (Optional)

Cancel | Save

3. Add the user filtering policy.

   1) Navigate to **Audit** > **Filtering** > **User Filtering**, and click **Add**.
   2) Configure the parameters in the **Add User Filtering Policy** window, and click **Save**.
      - Select the **Filtering Policy**, which is **White List (Allowed to access the internet)** in this example.
      - Select **User Group** for **User Policy**.
      - Select the **User Group** upon which the policy takes effect, which is **R&D Department** (set in advance) in this example.
      - Select the **Time Group** upon which the policy takes effect, which is **Business Hours** in this example.



Add User Filtering Policy

Filtering Policy: White List (Allowed to access th

User Policy: ○ User ● User Group

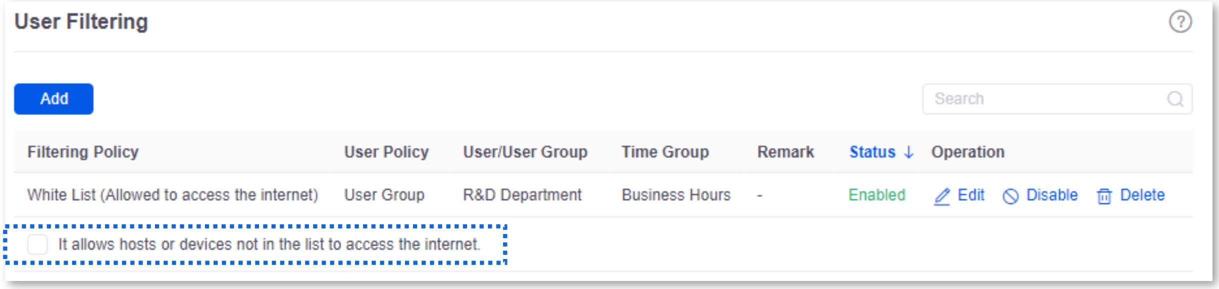
User Group: R&D Department

Time Group: Business Hours

Remark: (Optional)

Cancel | Save

   3) Deselect **It allows hosts or devices not in the list to access the internet**. In the pop-up window, click **OK**.



User Filtering

Add

Search

Filtering Policy	User Policy	User/User Group	Time Group	Remark	Status ↓	Operation
White List (Allowed to access the internet)	User Group	R&D Department	Business Hours	-	Enabled	Edit Disable Delete

□ It allows hosts or devices not in the list to access the internet.

---End

Verification

During business hours (8:00 -18:00 from Monday to Friday), only the staff of R&D Department authenticated through the user name and password can access the internet while other staff cannot.

Parameter description

Parameter	Description
Filtering Policy	Specifies the mode of the user filtering policy. – **Blacklist (Blocked to access the internet)**: The specified user or user group is blocked to access the internet during the specified period, and is allowed to access the internet during other times. – **White List (Allowed to access the internet)**: The specified user or user group is allowed to access the internet during the specified period, and is blocked from accessing the internet during other times.
User Policy	Used to select the user policy (authenticated user or user group) upon which the user filtering policy takes effect. The authenticated user should be configured at Account Management in advance, and the authenticated user group should be configured at User Group in advance.
User/User Group	Specifies the authenticated user or user group to be filtered.
User Name	Specifies the user name of the authenticated user.
Time Group	Used to select the time group upon which the user filtering policy takes effect. The time group should be configured at Time Group in advance.
It allows hosts or devices not in the list to access the internet.	– When Selected: The devices not in the filtering list or devices with the filtering policy disabled can access the internet. – When Deselected: The devices not in the filtering list or devices with the filtering policy disabled cannot access the internet. Tip To deselect this function, configure a whitelist first.

8.2.7 VPN access permission

Log in to the web UI of the router, and navigate to **Audit** > **Filtering** > **VPN Access Permission** to enter the page.

On this page, you can configure VPN access permissions rules to allow or block VPN users from accessing servers in the LAN.

Example of configuring VPN access permission

Networking requirements

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

The enterprise has established a PPTP VPN connection between its headquarters and subsidiary 1 via the router. The headquarters has created the VPN user group named **Subsidiary 1 Staff** on the router, and has added the user names and passwords of subsidiary 1 staff to the VPN user group. If you want to check the specific configuration of VPN, refer to VPN service.

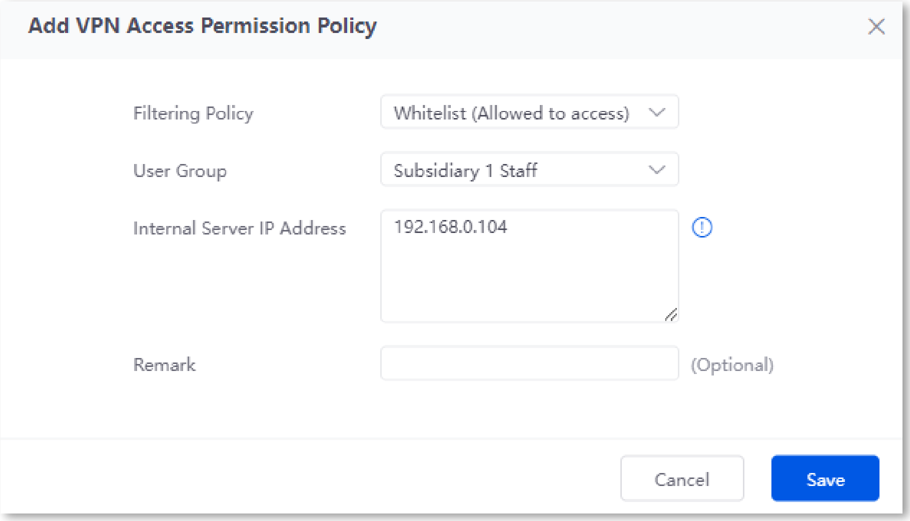
Requirements: Only subsidiary 1 staff are allowed to access the headquarters FTP server through PPTP VPN, and other staff cannot access it.

Solution

The router's VPN access permission function can achieve the requirements. Assume that the IP address of the headquarters FTP server is 192.168.0.104.

Configuration procedure

1. Log in to the web UI of the router.
2. Add the VPN access permission policy.
   1) Navigate to **Audit** > **Filtering** > **VPN Access Permission**, and click **Add**.
   2) Configure the parameters in the **Add VPN Access Permission Policy** window, and click **Save**.
      - Select the **Filtering Policy**, which is **Whitelist (Allowed to access)** in this example.
      - Select the **User Group**, which is **Subsidiary 1 Staff** in this example.
      - Set **Internal Server IP Address**, which is **192.168.0.104** in this example.



Add VPN Access Permission Policy

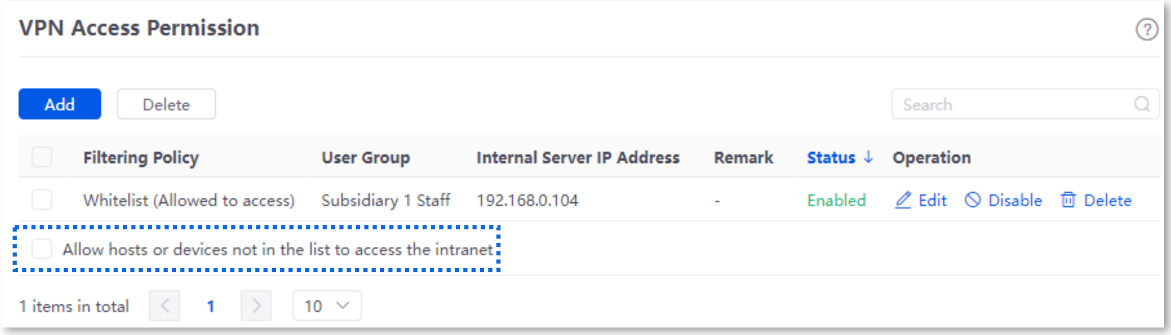
Filtering Policy: Whitelist (Allowed to access)

User Group: Subsidiary 1 Staff

Internal Server IP Address: 192.168.0.104

Remark: (Optional)

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



VPN Access Permission

	Filtering Policy	User Group	Internal Server IP Address	Remark	Status ↓	Operation
□	Whitelist (Allowed to access)	Subsidiary 1 Staff	192.168.0.104	-	Enabled	Edit Disable Delete

□ Allow hosts or devices not in the list to access the intranet

1 items in total < 1 > 10

---End

Verification

Only the subsidiary 1 staff can access the FTP server with the headquarters IP address 192.168.0.104 through PPTP VPN, and other staff cannot access it.

Parameter description

Parameter	Description
Filtering Policy	Specifies the mode of the VPN access permission policy. – **Blacklist (Blocked to access)**: The specified VPN user group is blocked to access specified servers in the LAN. – **Whitelist (Allowed to access)**: The specified VPN user group is allowed to access the specified servers in the LAN.
User Group	Specifies the VPN user group for which the VPN access permission policy takes effect.
Internal Server IP Address	Specifies the internal server IP address for which the VPN access permission policy takes effect.

Parameter	Description
Allow hosts or devices not in the list to access the intranet	– When Selected: The devices not in the list or devices with the policy disabled can access the intranet server. – When Deselected: The devices not in the list or devices with the policy disabled cannot access the intranet server. Tip To deselect this function, configure a whitelist first.

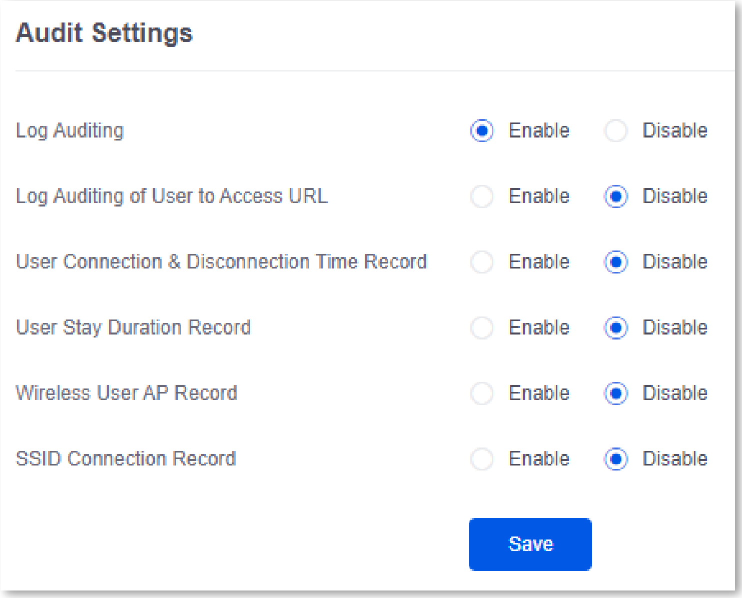
8.3 Log auditing

8.3.1 Audit settings

Log in to the web UI of the router, and 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. The following displays the page when the function is enabled.



Audit Settings

Log Auditing	● Enable	○ Disable
Log Auditing of User to Access URL	○ Enable	● Disable
User Connection & Disconnection Time Record	○ Enable	● Disable
User Stay Duration Record	○ Enable	● Disable
Wireless User AP Record	○ Enable	● Disable
SSID Connection Record	○ Enable	● Disable

Parameter description

Parameter	Description
Log Auditing	Used to enable or disable the log auditing function.

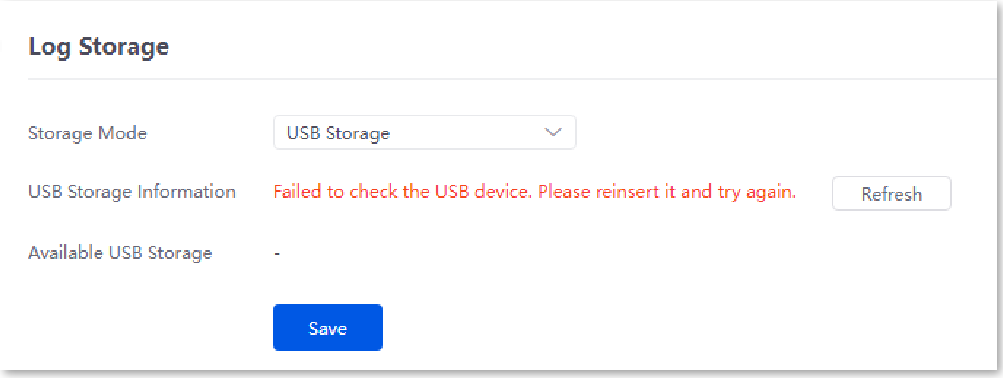
Parameter	Description
Log Auditing of User to Access URL	Used to enable or disable the function to record the information of web pages accessed by users.
User Connection & Disconnection Time Record	Used to enable or disable the function to record the time at which a user obtains an IP address from the 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.

8.3.2 Log storage

Log in to the web UI of the router, and 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 on the local PC or a USB disk. A log tool is required to be installed in the local computer, such as **Syslog**.

USB storage is enabled by default. The following displays the page when the function is enabled.



Log Storage

Storage Mode: USB Storage

USB Storage Information: Failed to check the USB device. Please reinsert it and try again.

Available USB Storage: -

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.

Parameter	Description
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.**

9 More

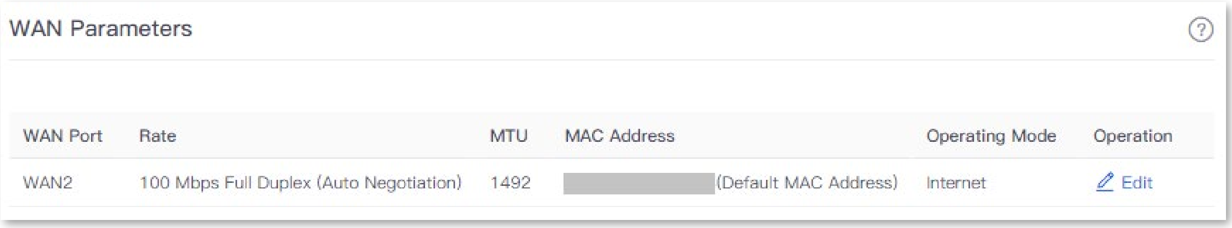
Features available in the router may vary by model and software version. Router availability may also vary by region or ISP. All images, steps, and descriptions in this guide are only examples and may not reflect your actual router experience.

9.1 Advanced routing

9.1.1 WAN parameters

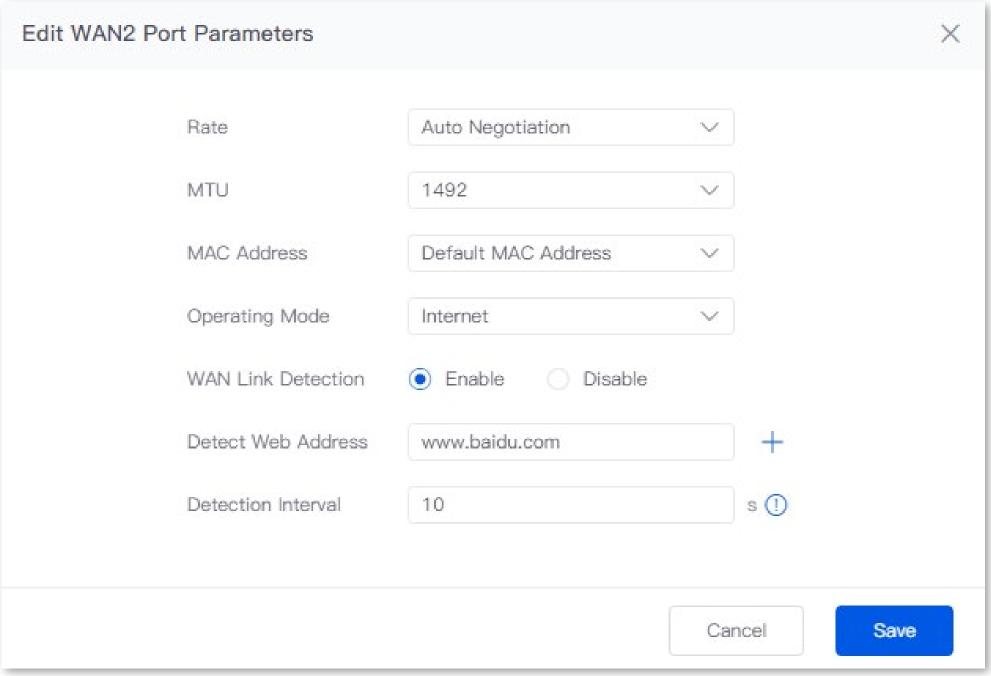
Log in to the web UI of the router, and navigate to **More** > **Advanced Routing** > **WAN Parameters** to enter the page. On this page, you can configure the parameters of the WAN port.

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.



WAN Parameters

WAN Port	Rate	MTU	MAC Address	Operating Mode	Operation
WAN2	100 Mbps Full Duplex (Auto Negotiation)	1492	[redacted] (Default MAC Address)	Internet	Edit


Edit WAN2 Port Parameters

Rate: Auto Negotiation

MTU: 1492

MAC Address: Default MAC Address

Operating Mode: Internet

WAN Link Detection: ● Enable ○ Disable

Detect Web Address: www.baidu.com

Detection Interval: 10 s

Parameter description

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

Parameter	**Description**
MTU	Maximum Transmission Unit (**MTU**) is the largest data packet that a network device transmits, and is related to the WAN port's connection type. Generally, keep the default value. If you cannot access some websites or cannot send and receive emails, you can try to modify the MTU value. The recommended modification range is 1400 to 1500. The following are scenarios where commonly used MTU apply: – **1500**: Used for the most common settings in non-PPPoE connections and non-VPN connections. – **1492**: Used for PPPoE connections. – **1480**: It is the maximum value for the Ping function (packets larger than this value will be broken down). – **1450**: Used for DHCP, which assigns dynamic IP addresses to connected devices. – **1400**: Used for VPN or PPTP.
MAC Address	Specifies the MAC address of the WAN port, which can be customized. After the networking is set up, if the router still cannot connect to the internet, the ISP may have bound the account to a certain MAC address. You can try to solve the problem by modifying the MAC address of the WAN port. – **Default MAC Address**: The default value can be changed if the MAC address is set to **Customize**. – **Customize**: You can customize the MAC address 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.
Detect Web Address	Specifies the domain name that needs to be detected. Tip When the **WAN Link Detection** function is enabled, **Detect Web Address** can be configured.

Parameter	Description
Detection Interval	Specifies the interval to perform detections. Tip When the **WAN Link Detection** function is enabled, **Detection Interval** can be configured.

9.1.2 Multi-WAN policy

Log in to the web UI of the router, and 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 utilisation 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.

  – **Connection Load Balancing**: Distributes LAN connections across WAN ports based on assigned weights, optimizing performance for multi-user concurrent access.

  – **Customize**: Users can designate a WAN port for forwarding traffic of a source IP address according to actual needs.

  – **Disable**: Disable the multi-WAN policy.

- **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.

Example of configuring multi-WAN policy

Networking requirements

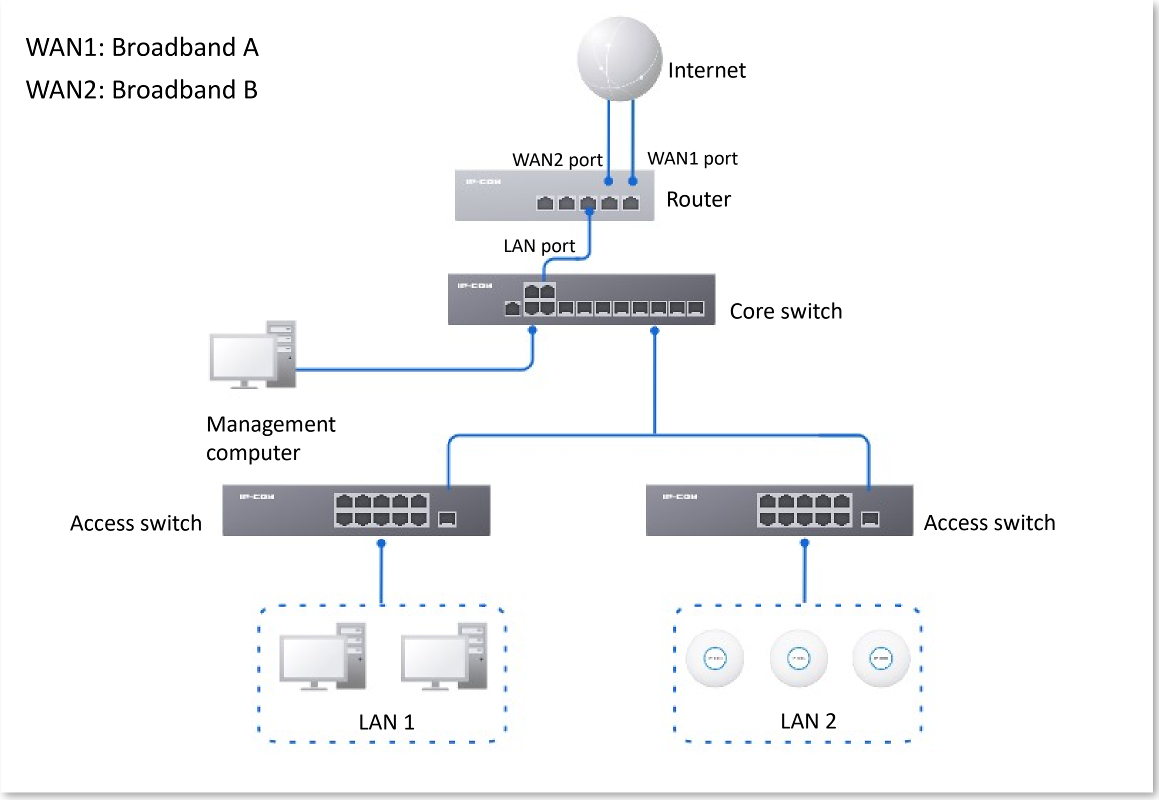
An enterprise uses the enterprise router to set up a network. To meet the requirements of the enterprise network, two broadband lines have been handled and the internet has been successfully accessed.

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

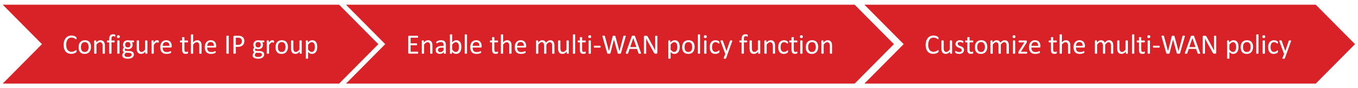
- Computers with IP addresses 192.168.0.2 - 192.168.0.100 access the internet through Broadband A.
- Computers with IP addresses 192.168.0.101 - 192.168.0.250 access the internet through Broadband B.

Solution

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



Configuration procedure

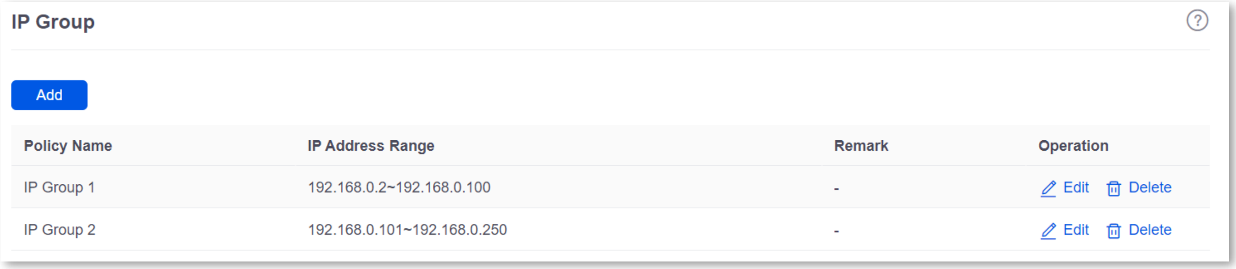

Configure the IP group

Enable the multi-WAN policy function

Customize the multi-WAN policy

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

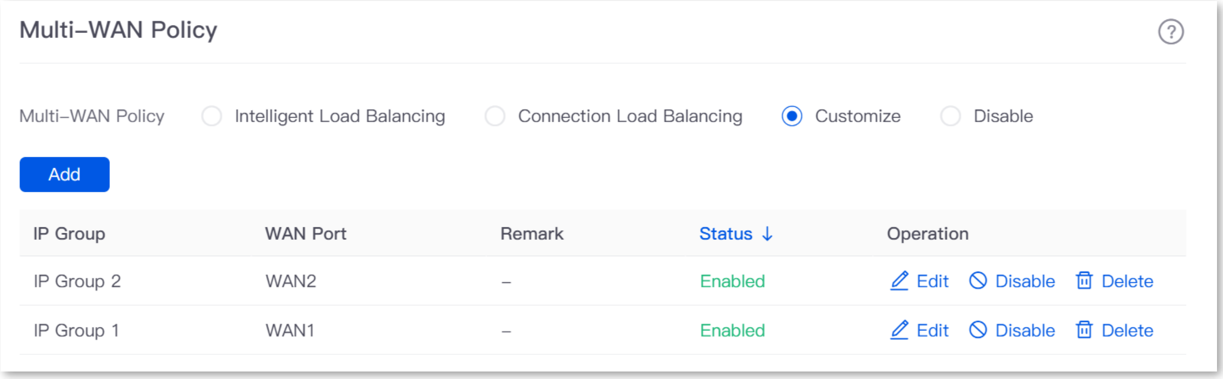
   Navigate to **Audit** > **Group Policy** > **IP Group**, and click **Add** to configure the following two IP groups.


IP Group

Add

Policy Name	IP Address Range	Remark	Operation
IP Group 1	192.168.0.2~192.168.0.100	-	Edit Delete
IP Group 2	192.168.0.101~192.168.0.250	-	Edit Delete

3. Customize the multi-WAN policy.
   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) Click **Add** to create the following two multi-WAN policies.


Multi–WAN Policy

Multi–WAN Policy ○ Intelligent Load Balancing ○ Connection Load Balancing ● Customize ○ Disable

Add

IP Group	WAN Port	Remark	Status ↓	Operation
IP Group 2	WAN2	–	Enabled	Edit Disable Delete
IP Group 1	WAN1	–	Enabled	Edit Disable Delete

---End

Verification

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

Parameter description

Parameter	Description
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 at 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.

9.1.3 Static routing

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.

Log in to the web UI of the router, and 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.

Example of configuring static routing

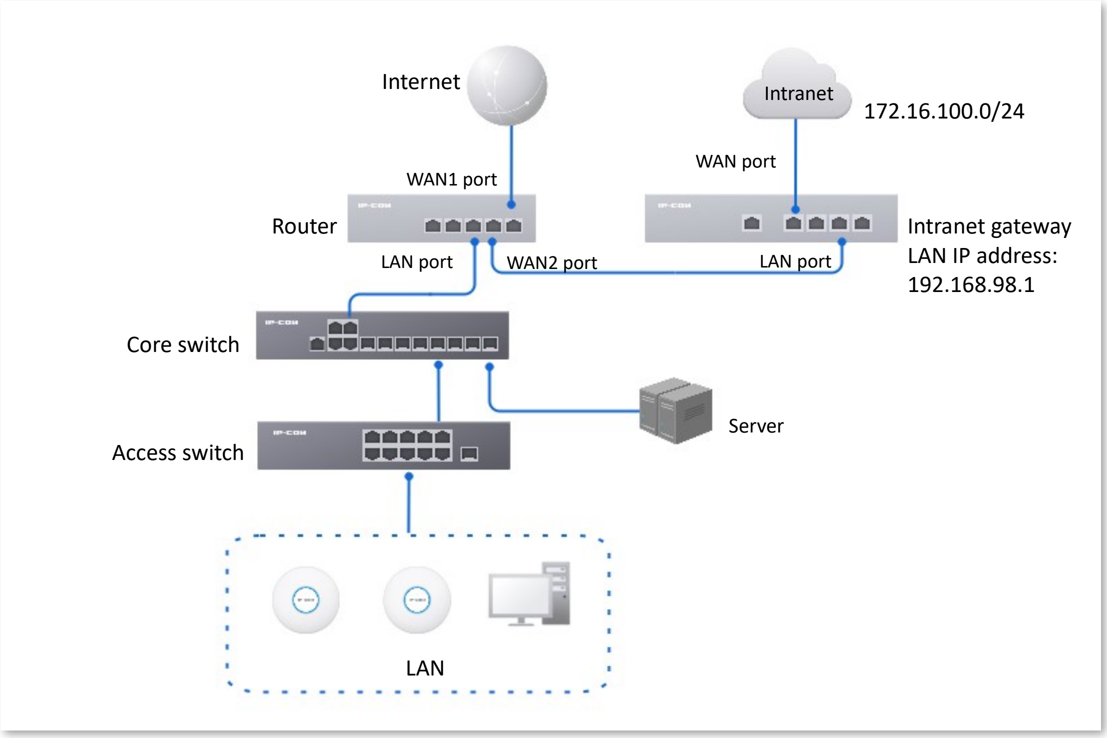
Networking requirements

An enterprise uses the enterprise router to set up a network. The WAN2 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 WAN1 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

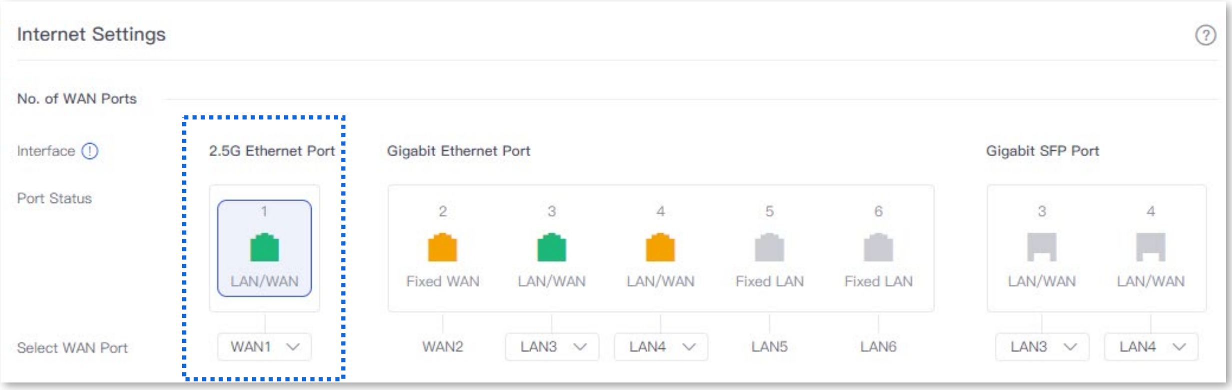
Connect the WAN port to the internet > Configure the static routing

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

2. Enable two WAN ports and connect WAN1 port to the internet.

   1) Navigate to **Network** > **Internet Settings**.

   2) Set **WAN1** for Ethernet port1.

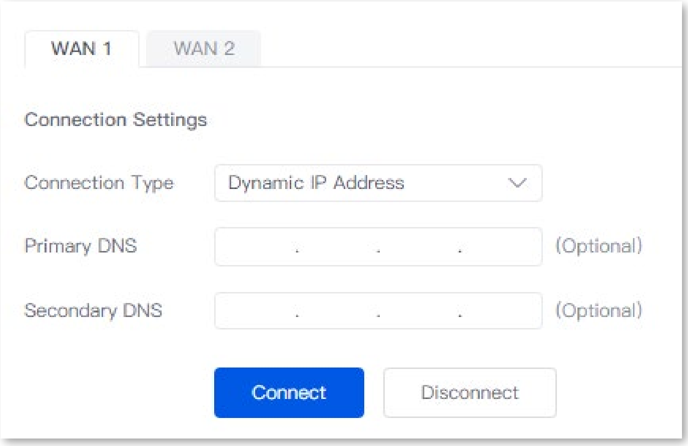


Internet Settings

No. of WAN Ports

Interface	2.5G Ethernet Port	Gigabit Ethernet Port					Gigabit SFP Port	
	1	2	3	4	5	6	3	4
Port Status	LAN/WAN	Fixed WAN	LAN/WAN	LAN/WAN	Fixed LAN	Fixed LAN	LAN/WAN	LAN/WAN
Select WAN Port	WAN1	WAN2	LAN3	LAN4	LAN5	LAN6	LAN3	LAN4

   3) Under **WAN1**, select **Dynamic IP Address** for **Connection Type**, and click **Connect**.



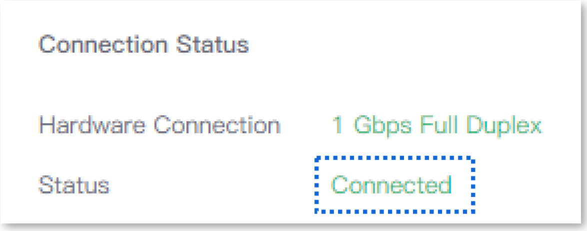
Connection Settings

Connection Type: Dynamic IP Address

Primary DNS: . . . (Optional)

Secondary DNS: . . . (Optional)

When the **Status** is **Connected**, the WAN1 port is successfully connected to the network.



Connection Status

Hardware Connection: 1 Gbps Full Duplex

Status: Connected

3. Configure the static routing.

1) Obtain the IP address information of the WAN1 port.

Navigate to **Network** > **Internet Settings,** and view the IP address information obtained by WAN1 under **Connection Status**, assuming the following:

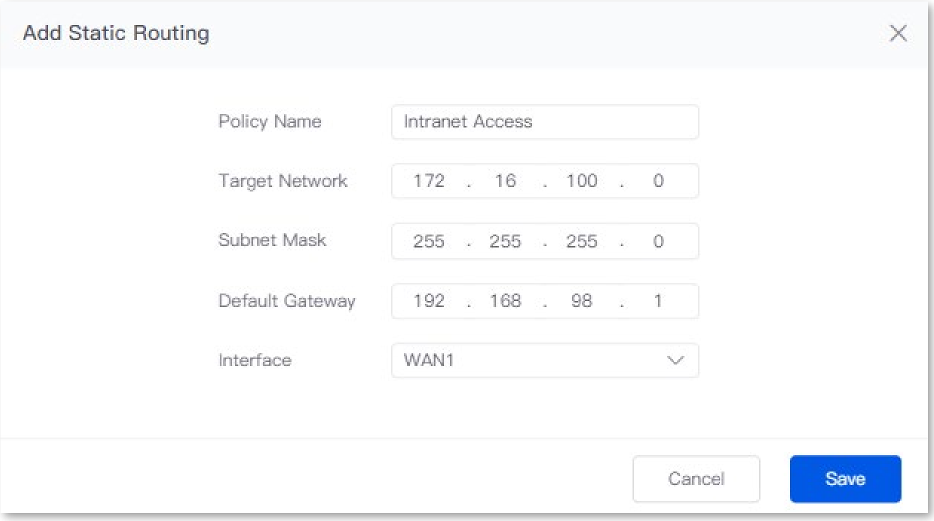
WAN1 IP Address	Subnet Mask	Default Gateway	Primary DNS
192.168.98.190	255.255.255.0	192.168.98.1	192.168.98.1

2) Configure parameters of the static routing.

Example:

Policy Name	Target Network	Subnet Mask	Default Gateway	Interface
Intranet Access	172.16.100.0	255.255.255.0	192.168.98.1	WAN1

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


Add Static Routing

Policy Name: Intranet Access

Target Network: 172 . 16 . 100 . 0

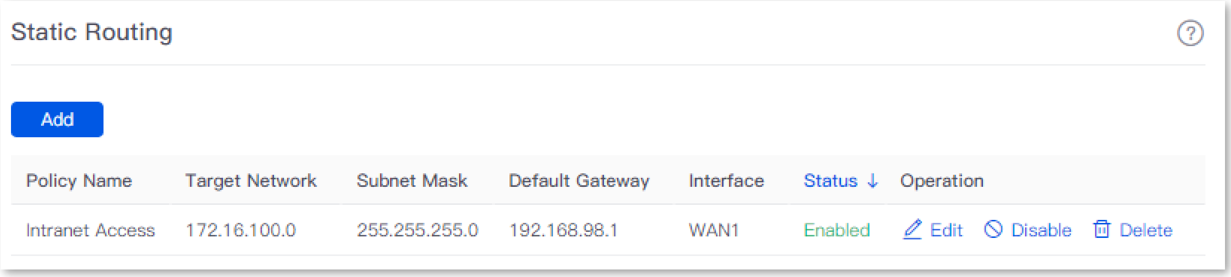
Subnet Mask: 255 . 255 . 255 . 0

Default Gateway: 192 . 168 . 98 . 1

Interface: WAN1

---End

The static route is added successfully.


Static Routing

Policy Name	Target Network	Subnet Mask	Default Gateway	Interface	Status ↓	Operation
Intranet Access	172.16.100.0	255.255.255.0	192.168.98.1	WAN1	Enabled	Edit Disable Delete

Verification

LAN users can access both the internet and the intranet.

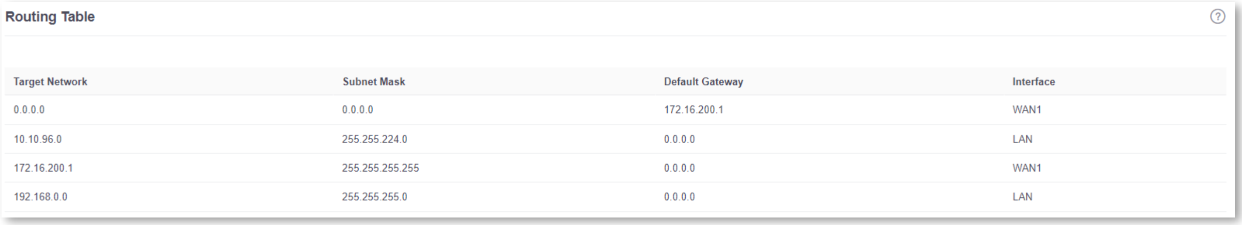
Parameter description

Parameter	Description
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 default route will be chosen for router 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.

Parameter	Description
Interface	Specifies the interface from which packets egress. Select it as required.

9.1.4 Routing table

[Log in to the web UI of the router](), and navigate to **More** > **Advanced Routing** > **Routing Table** to enter the page. On this page, you can view the detailed routing information of the router.



Routing Table

Target Network	Subnet Mask	Default Gateway	Interface
0.0.0.0	0.0.0.0	172.16.200.1	WAN1
10.10.96.0	255.255.224.0	0.0.0.0	LAN
172.16.200.1	255.255.255.255	0.0.0.0	WAN1
192.168.0.0	255.255.255.0	0.0.0.0	LAN

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.

9.1.5 Policy routing

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.

[Log in to the web UI of the router](), and navigate to **More** > **Advanced Routing** > **Policy Routing** to enter the page. On this page, you can configure the policy routing according to your needs.

Example of configuring policy routing

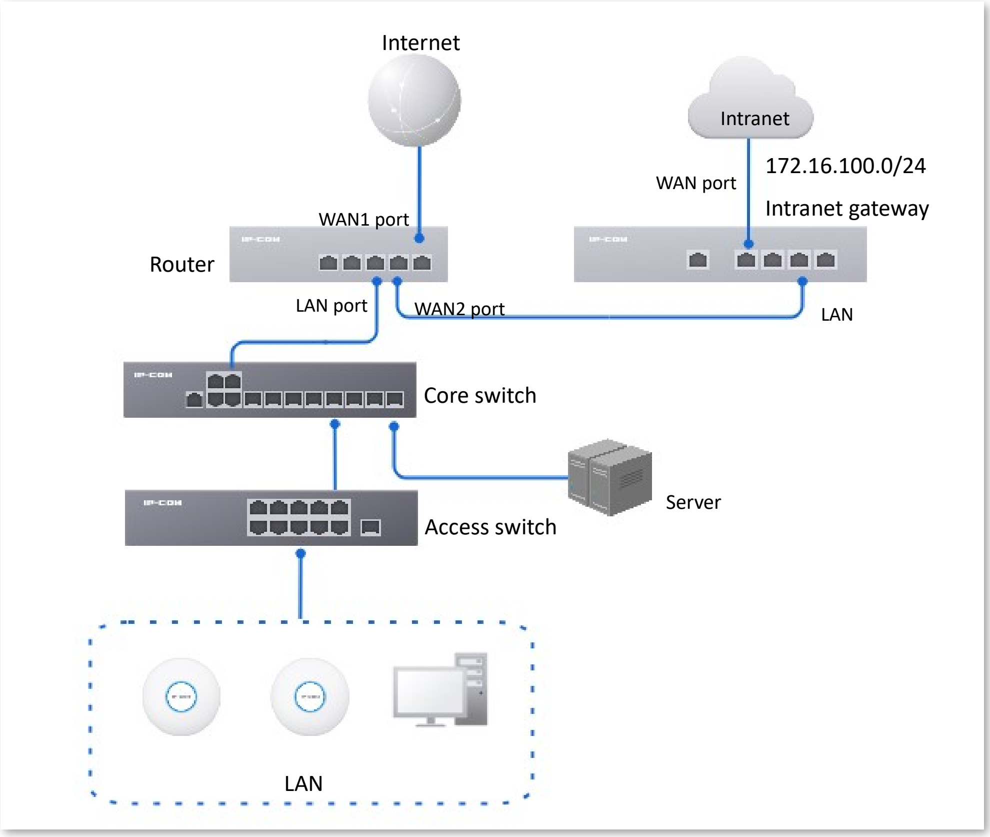
Networking requirements

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 - 192.168.0.254 can access both the internet and the web server of the enterprise's intranet (the port number is 9999).

Solution

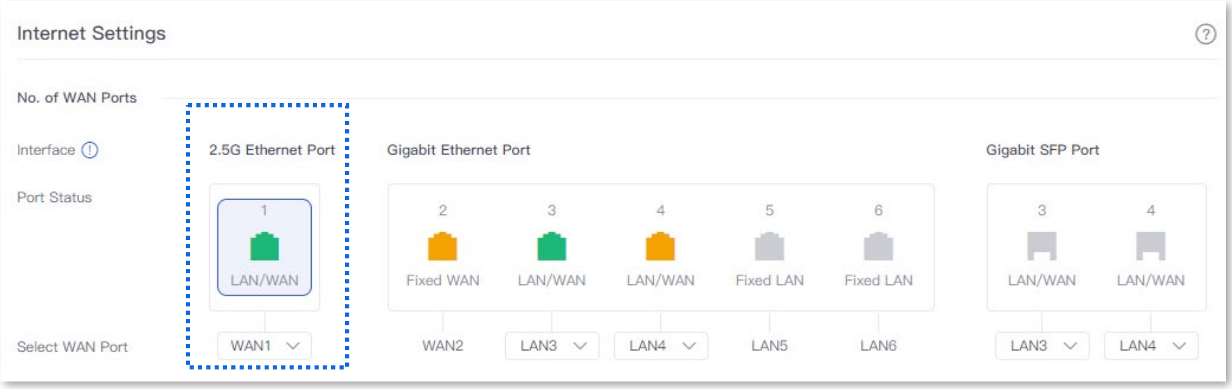
You can use the Policy Routing function to meet the requirements.



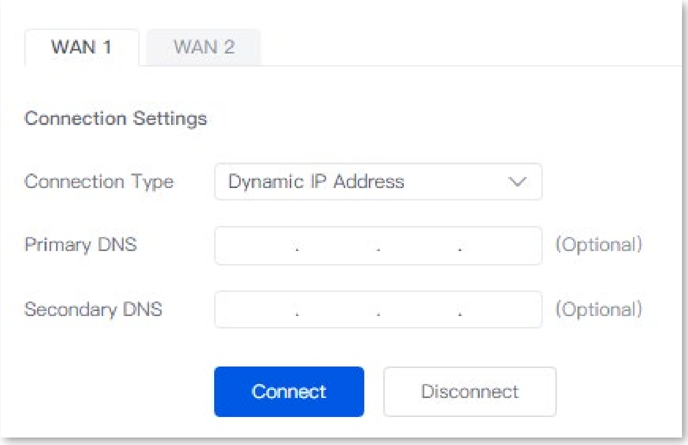
Configuration procedure

Configure the WAN1 port to access the internet → Configure the policy routing

1. Log in to the web UI of the router.
2. Configure the WAN1 port to access the internet.
   1) Navigate to **Network** > **Internet Settings**.
   2) Set **WAN1** for Ethernet port1.



   3) Under **WAN1**, select **Dynamic IP Address** for **Connection Type**, and click **Connect**.


WAN 1 | WAN 2

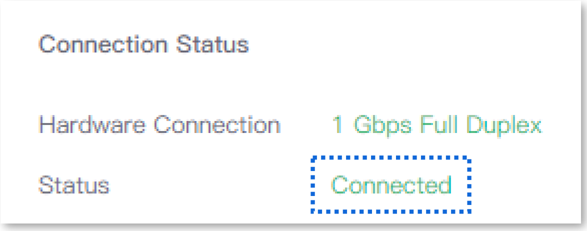
Connection Settings

Connection Type: Dynamic IP Address

Primary DNS: . . . (Optional)

Secondary DNS: . . . (Optional)

When the **Status** is **Connected**, the WAN1 port is successfully connected to the network.


Connection Status

Hardware Connection: 1 Gbps Full Duplex

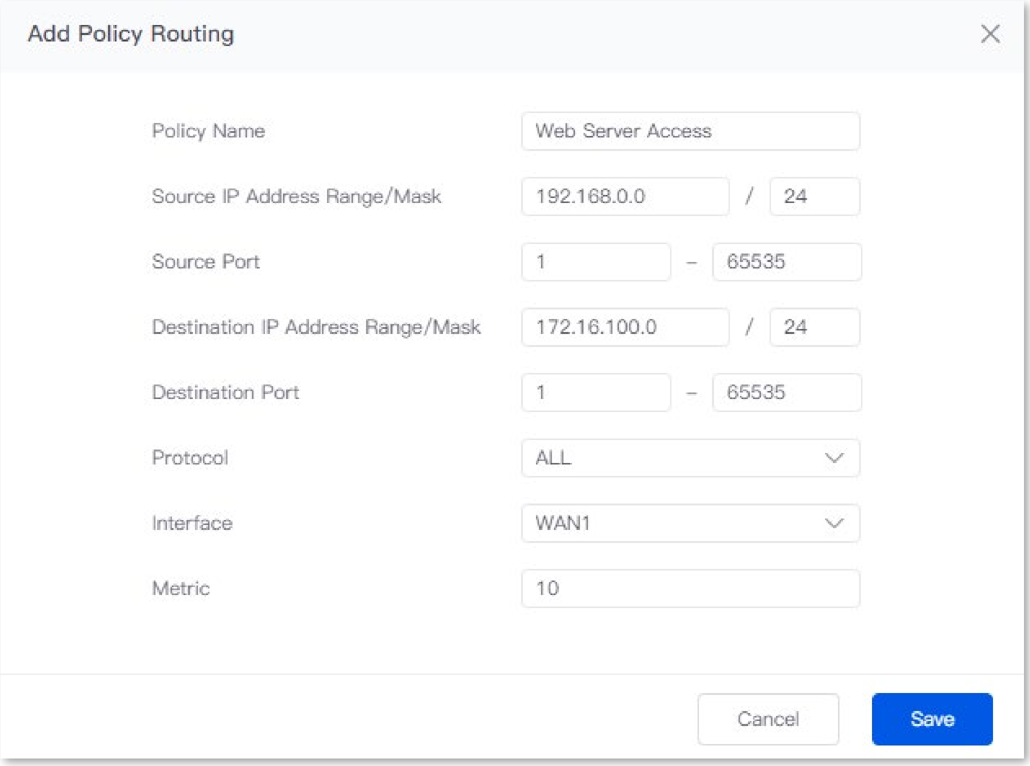
Status: Connected

3. Configure the policy routing.

The following table provides 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	WAN1	10

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

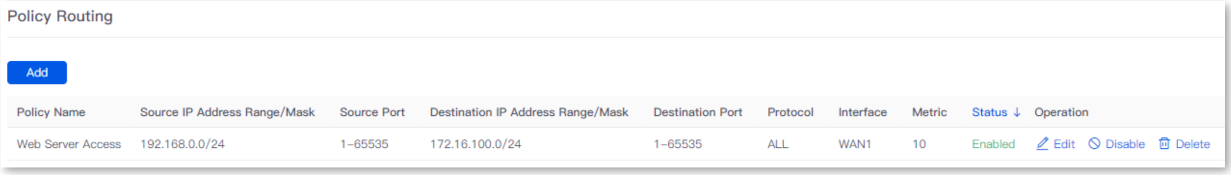


Add Policy Routing

Policy Name	Web Server Access
Source IP Address Range/Mask	192.168.0.0 / 24
Source Port	1 – 65535
Destination IP Address Range/Mask	172.16.100.0 / 24
Destination Port	1 – 65535
Protocol	ALL
Interface	WAN1
Metric	10

---End

The policy routing is added successfully.



Policy Routing

Policy Name	Source IP Address Range/Mask	Source Port	Destination IP Address Range/Mask	Destination Port	Protocol	Interface	Metric	Status ↓	Operation
Web Server Access	192.168.0.0/24	1–65535	172.16.100.0/24	1–65535	ALL	WAN1	10	Enabled	Edit Disable Delete

Verification

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

Parameter description

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

9.1.6 Custom NAT

NAT (Network Address Translation) allows multiple devices on a local area network (LAN) to share one or more public IP addresses to access the internet, while simultaneously hiding the LAN devices and preventing direct access from the wide area network (WAN), thus providing a certain level of security for the local network.

This router supports NAT and works as follows:

- When a device within the router's LAN IP range needs to access the internet through this router, the router automatically translates its IP address into a valid public IP address.
- When a device outside the router's LAN IP range needs to access the internet through this router, you can customize the NAT function to allow the router to translate its IP address into a valid public IP address.

Log in to the web UI of the router, and navigate to **More** > **Advanced Routing** > **Custom NAT** to enter the page. On this page, you can configure custom NAT policies.

Example of using NAT for internet access

Network requirements

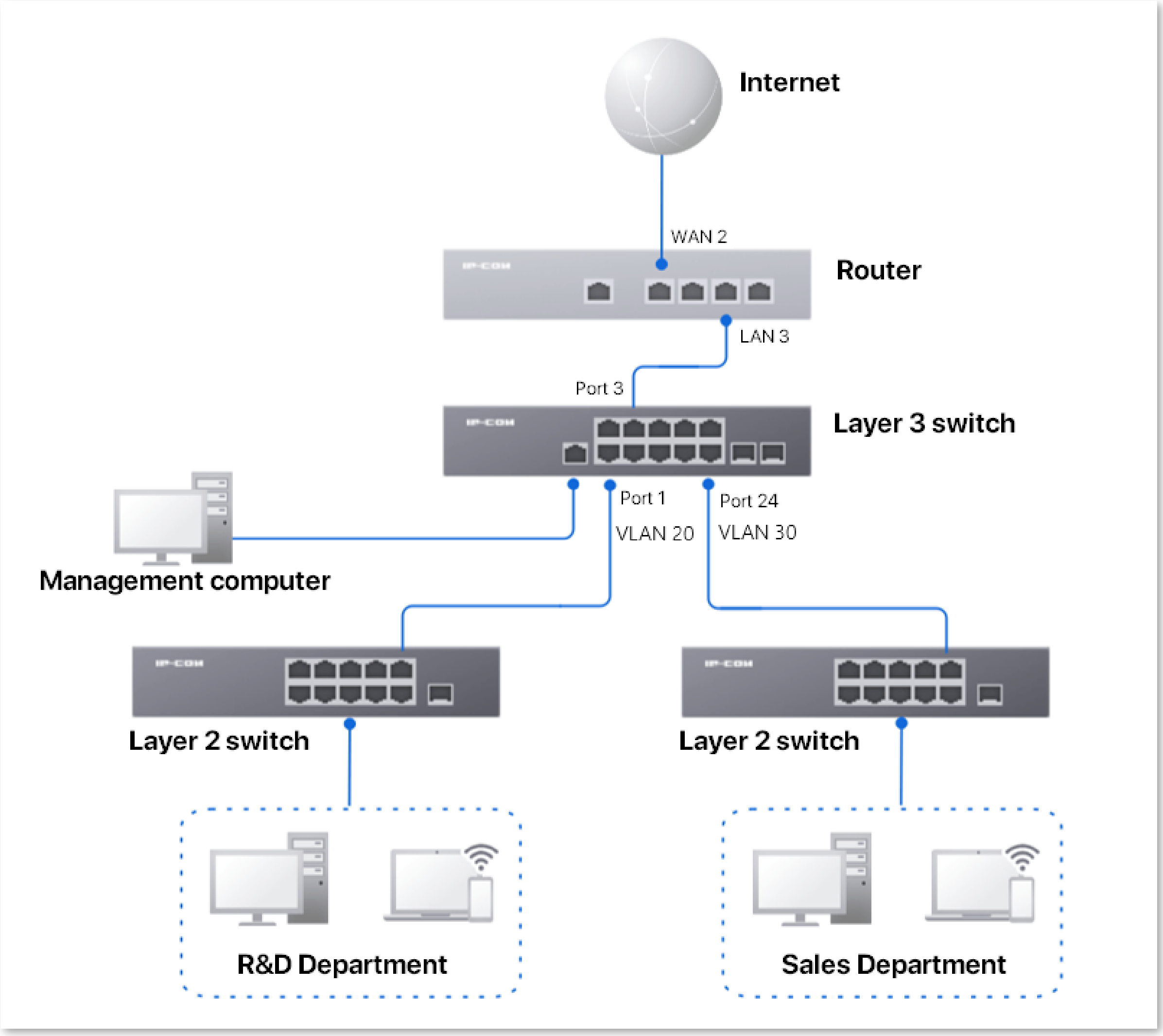
A company uses a router and a G5328XP-24-410W Layer 3 switch to build its network. The router's LAN3 port connects to port 3 of the switch. The company's internal network uses the switch to divide the R&D department and sales department into different VLANs. The specific network topology is described below:

- R&D Department: VLAN 20, connected to port 1 of the switch.
- Sales Department: VLAN 30, connected to port 24 of the switch.
- Layer 3 switch & Router: Port 3 on the switch is assigned to the default VLAN 1. Port LAN 3 on the router is assigned to the default VLAN. The IP addresses of the switch's port 3 and the router's LAN 3 must be in the same subnet. In this example, the router's LAN 3 remains at its default value of **192.168.0.252**, and the switch's port 3 is configured to **192.168.0.2**.

Requirement: Both the R&D and Sales departments should have internet access.

Solution

Configure the by custom NAT function on the router to provide internet access.



Configuration procedure

1. Set up the Layer 3 switch.

   1) Assign VLANs for ports 1 and 24 on the switch, and configure a DHCP server.

   The VLAN values shown below are examples only:

VLAN ID	DHCP Pool	Subnet Mask	VLAN ID (Allowed)	Port Type	PVID
20	192.168.20.1	255.255.255.0	20	Access	20
30	192.168.30.1	255.255.255.0	30	Access	30

   The DHCP values shown below are examples only:

VLAN ID	DHCP Pool	Subnet Mask	Default Gateway	DNS
20	192.168.20.2~192.168.20.250	255.255.255.0	192.168.20.1	223.5.5.5
30	192.168.30.2~192.168.30.250	255.255.255.0	192.168.20.1	223.5.5.5

   2) Set up the IP address of port 3 on the switch (Default to the IP address of the switch's default VLAN).

Port	IP Address	VLAN ID (Allowed)	Port Type	PVID
3	192.168.0.2	1	Access	1

   Leave other ports at their default settings. For detailed instructions, refer to the user manual for the switch.

   3) Set up the default route on the switch.

Destination Address	Subnet Mask	Next Hop (Default Gateway)
0.0.0.0	0.0.0.0	192.168.0.252

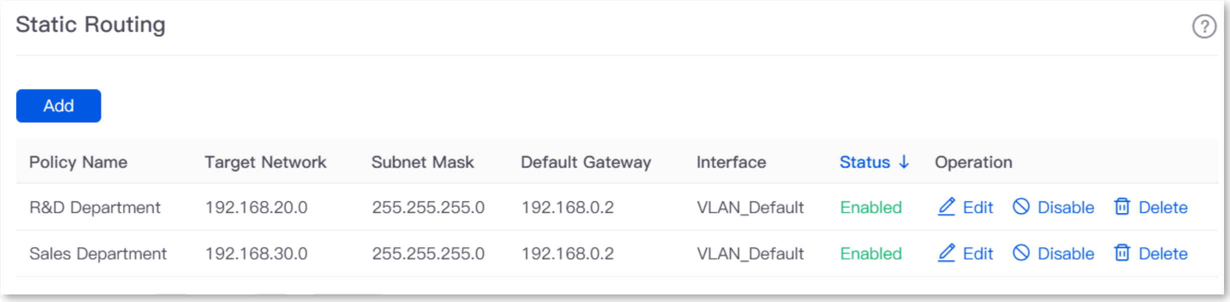
2. Set up the router.

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

   2) Add the static routing rules shown below.

Policy Name	IP Address	Subnet Mask	Default Gateway	Interface
R&D Department	192.168.20.0	255.255.255.0	192.168.0.2	VLAN Default
Sales Department	192.168.30.0	255.255.255.0	192.168.0.2	VLAN Default

   Navigate to **More** > **Advanced Routing** > **Static Routing**. Click **Add**, then configure the static routes as follows.



Static Routing

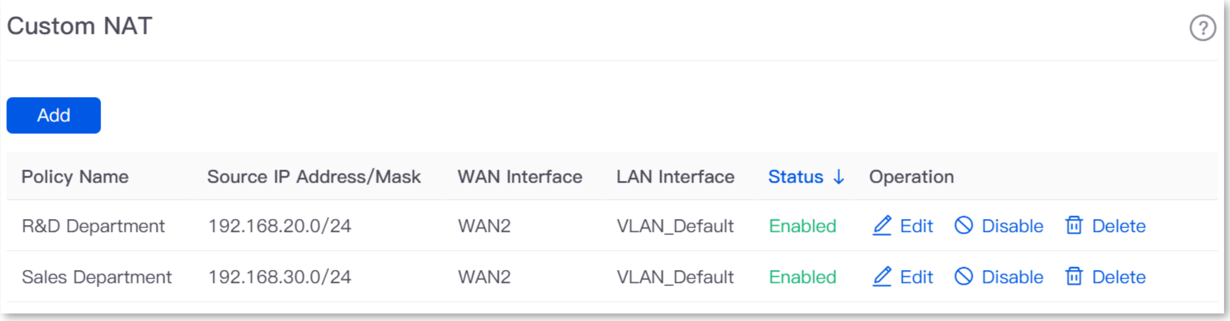
Add

Policy Name	Target Network	Subnet Mask	Default Gateway	Interface	Status ↓	Operation
R&D Department	192.168.20.0	255.255.255.0	192.168.0.2	VLAN_Default	Enabled	Edit Disable Delete
Sales Department	192.168.30.0	255.255.255.0	192.168.0.2	VLAN_Default	Enabled	Edit Disable Delete

3) Set up the custom NAT rules shown below.

Policy Name	Source IP Address/Mask	WAN Interface	LAN Interface
R&D Department	192.168.20.0/24	WAN 2	VLAN Default
Sales Department	192.168.30.0/24	WAN 2	VLAN Default

Navigate to **More** > **Advanced Routing** > **Custom NAT**. Click **Add**, then configure the NAT rules as follows.



Custom NAT

Add

Policy Name	Source IP Address/Mask	WAN Interface	LAN Interface	Status ↓	Operation
R&D Department	192.168.20.0/24	WAN2	VLAN_Default	Enabled	Edit Disable Delete
Sales Department	192.168.30.0/24	WAN2	VLAN_Default	Enabled	Edit Disable Delete

---End

Verification

Employees in both the R&D and Sales departments can access the internet.

Parameter description

Parameter	Description
Source IP Address/Mask	Specifies the source IP addresses to be translated into a network address.
WAN Interface	Specifies the internet port that performs network address translation.
LAN Interface	Specifies the LAN port connected to the Source IP Address/Mask.
Add to SD-WAN Routing	Reserved for future use.

9.2 Virtual service

9.2.1 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 meetings 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 the local network by using the DMZ host. Exercise caution to using 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.

Log in to the web UI of the router, and 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.

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 changes.

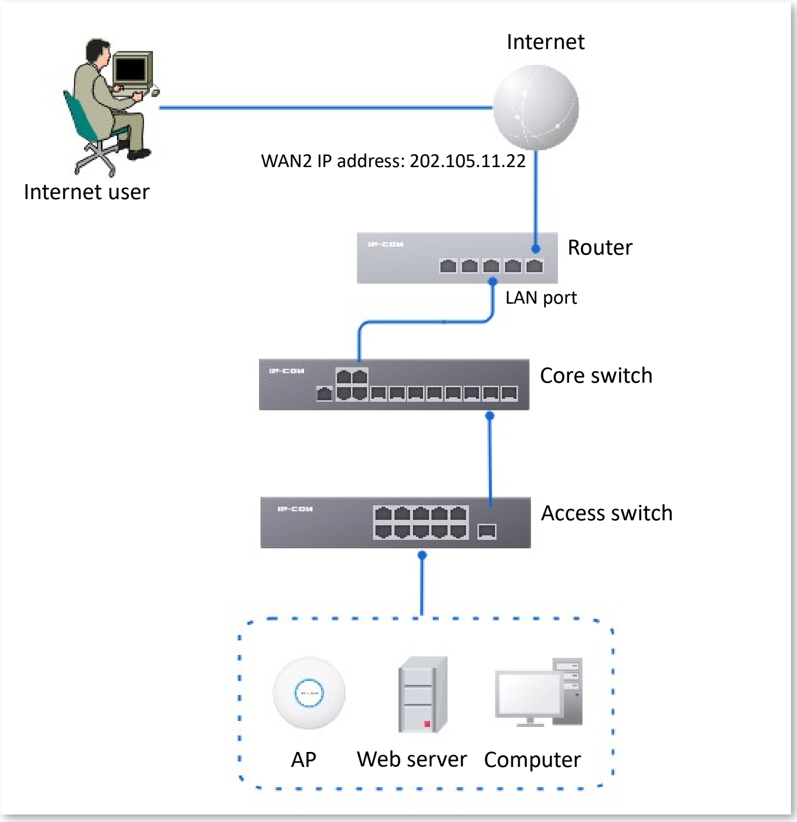
Assume that the information on the web server is shown below:

- IP address of the web server: 192.168.0.250

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

Tip

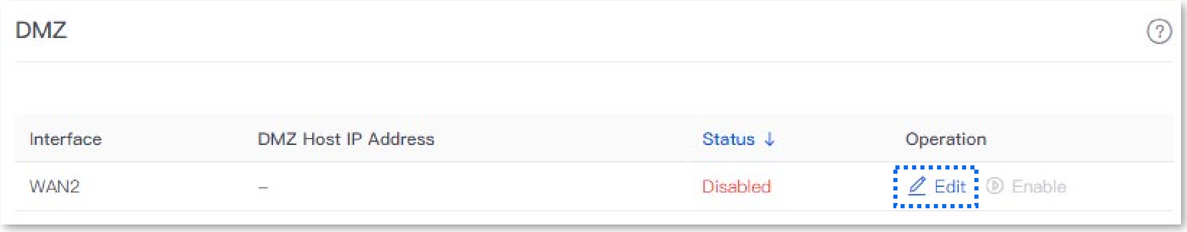
- Before the configuration, ensure that the WAN port of the router obtains a public IP address. If the WAN port obtains a private IP address or an intranet IP address assigned by the ISP, the DMZ function may not take effect. Common IPv4 addresses are classified into class A, class B and class C. Private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



Configuration procedure

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

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.**

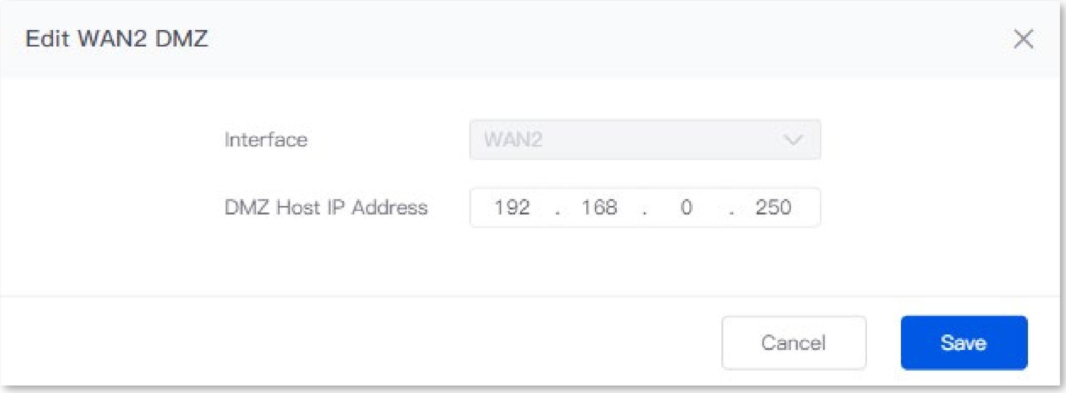


DMZ

Interface	DMZ Host IP Address	Status ↓	Operation
WAN2	–	Disabled	Edit Enable

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**.

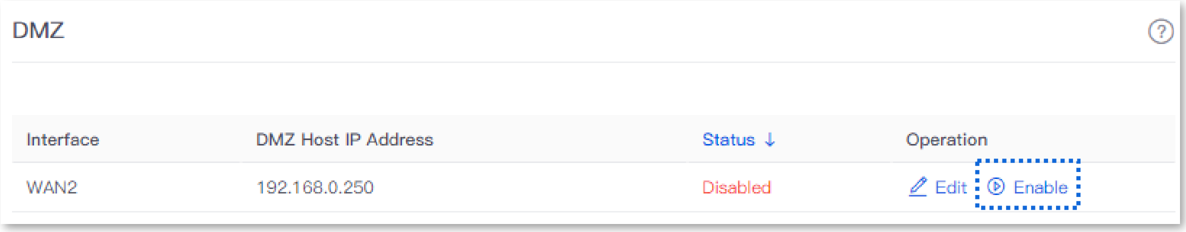


Edit WAN2 DMZ

Interface: WAN2

DMZ Host IP Address: 192 . 168 . 0 . 250

5) Click **Enable**.

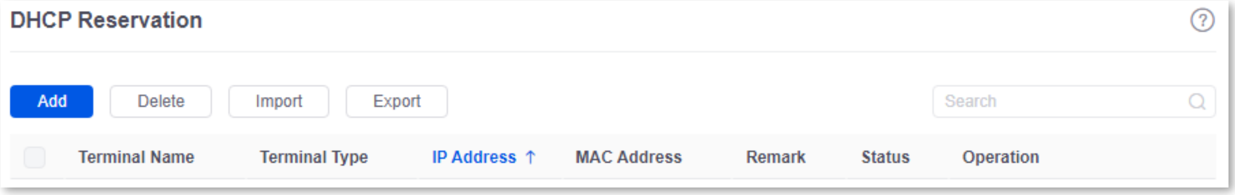


DMZ

Interface	DMZ Host IP Address	Status ↓	Operation
WAN2	192.168.0.250	Disabled	Edit Enable

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

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



DHCP Reservation

□	Terminal Name	Terminal Type	IP Address ↑	MAC Address	Remark	Status	Operation

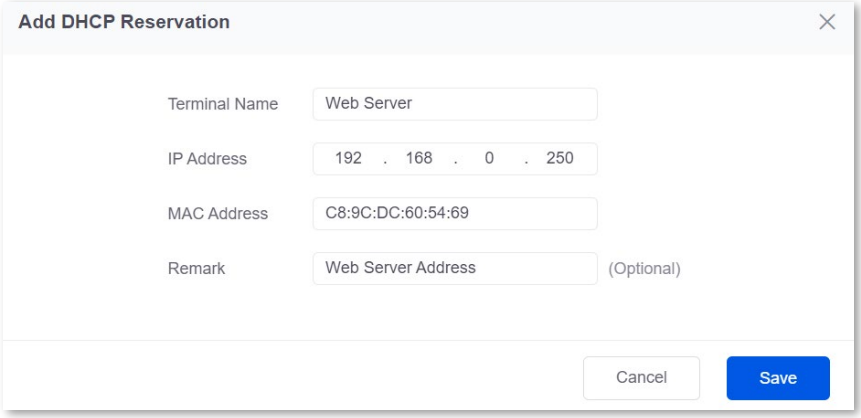
2) Set the following rules, and click **Save**.

– 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.


Add DHCP Reservation

Terminal Name: Web Server

IP Address: 192 . 168 . 0 . 250

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

Remark: Web Server Address (Optional)

---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**.

Parameter description

Parameter	**Description**
Interface	Specifies the port whose DMZ service will be enabled.
DMZ Host IP Address	Specifies the IP address of the device to be set as a DMZ host within the LAN.

9.2.2 DDNS

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.

Log in to the web UI of the router, and navigate to **More** > **Virtual Service** > **DDNS** to enter the page. The router has created a corresponding DMZ policy for each WAN port by default, and the status is **Disabled**. On this page, you can modify the DDNS policies according to your needs. The DDNS function is disabled by default.

Example of configuring DDNS

Networking requirements

An enterprise uses the enterprise router to set up a network. The router is 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

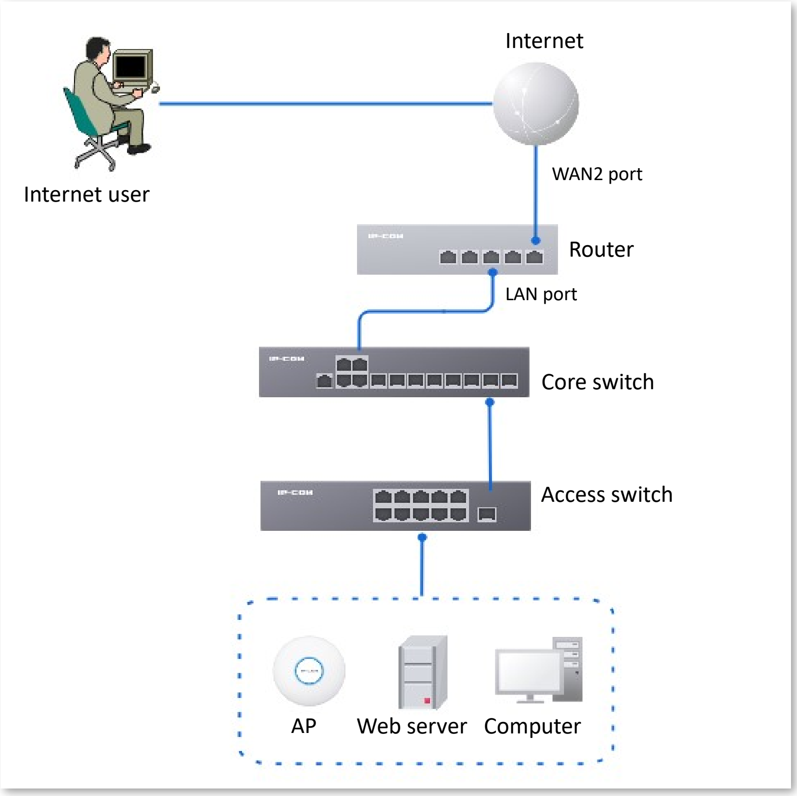
- You can use the Port Mapping function to enable internet users to access the intranet web server.
- You can use the DDNS function to enable internet users to access the intranet web server through a fixed domain name, avoiding access failures caused by WAN IP address change.
- You can use the DHCP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

Assume that the information on the web server is shown below:

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

Tip

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

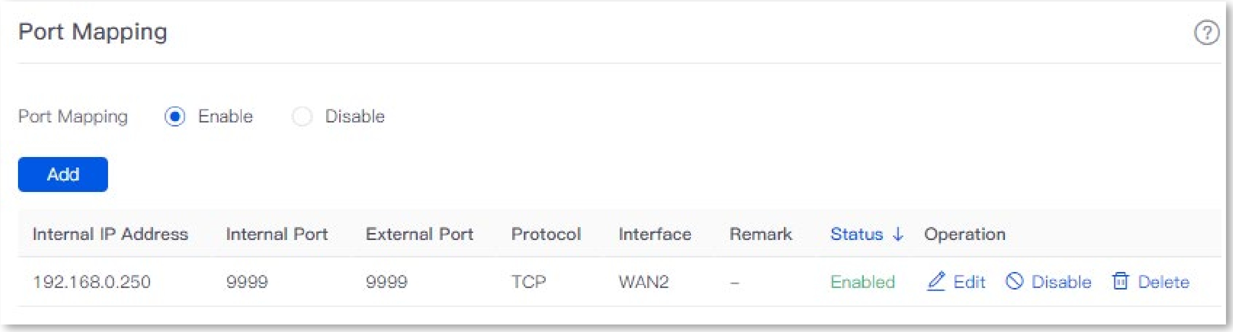


Configuration procedure

Set port mapping > Set the fixed IP address assigned to the server host > Set DDNS

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.



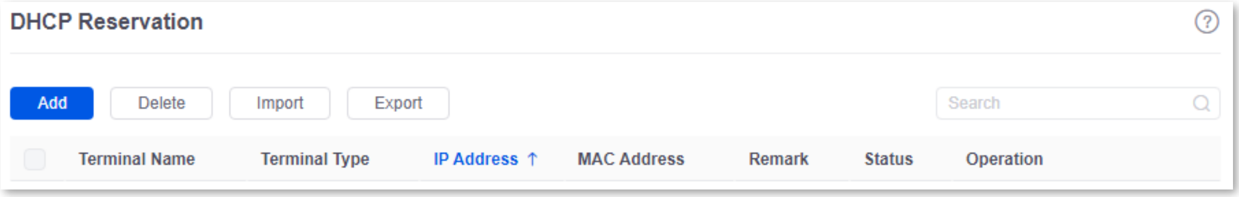
Port Mapping

Port Mapping ● Enable ○ Disable

Add

Internal IP Address	Internal Port	External Port	Protocol	Interface	Remark	Status ↓	Operation
192.168.0.250	9999	9999	TCP	WAN2	–	Enabled	Edit Disable Delete

3. Set the fixed IP address assigned to the server host.
   1) Navigate to Network > DHCP Settings > DHCP Reservation, and click Add.


DHCP Reservation

□	Terminal Name	Terminal Type	IP Address ↑	MAC Address	Remark	Status	Operation

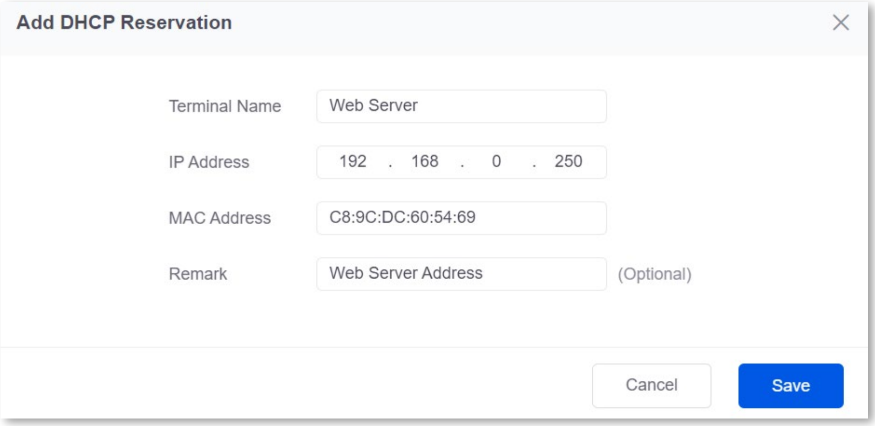
2) Set the following rules, and click **Save**.

– 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.


Add DHCP Reservation

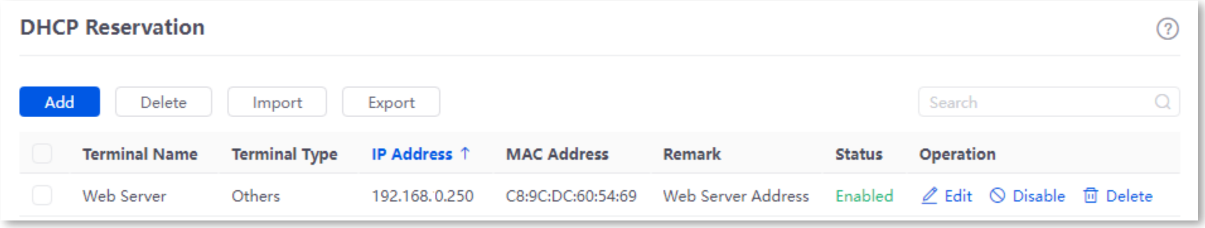
Terminal Name: Web Server

IP Address: 192 . 168 . 0 . 250

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

Remark: Web Server Address (Optional)

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


DHCP Reservation

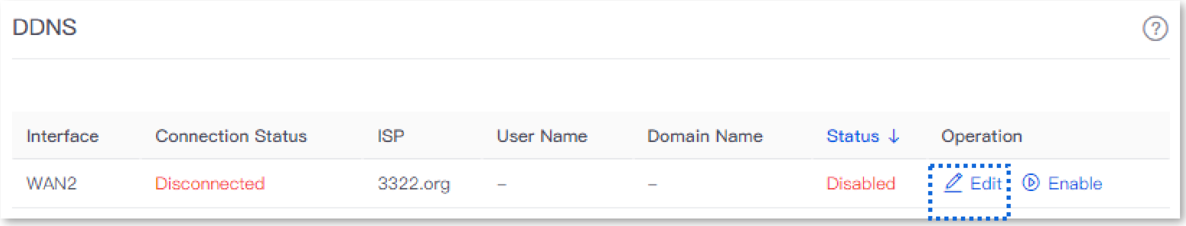
□	Terminal Name	Terminal Type	IP Address ↑	MAC Address	Remark	Status	Operation
□	Web Server	Others	192.168.0.250	C8:9C:DC:60:54:69	Web Server Address	Enabled	Edit Disable Delete

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 **WAN2** in this example.


DDNS

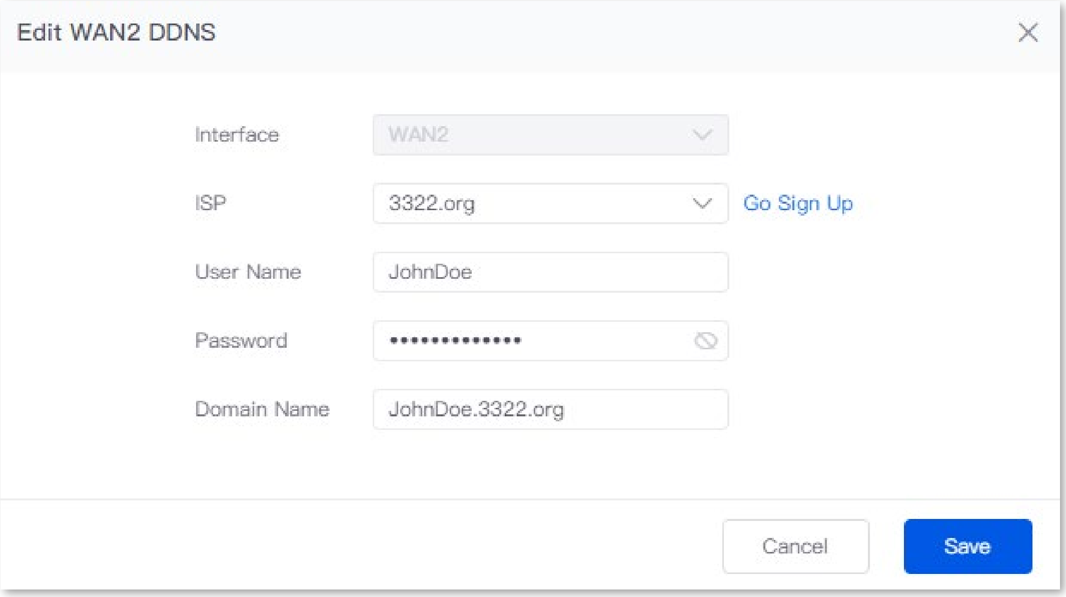
Interface	Connection Status	ISP	User Name	Domain Name	Status ↓	Operation
WAN2	Disconnected	3322.org	–	–	Disabled	Edit Enable

2) Configure the following parameters in the pop-up **Edit WAN2 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.

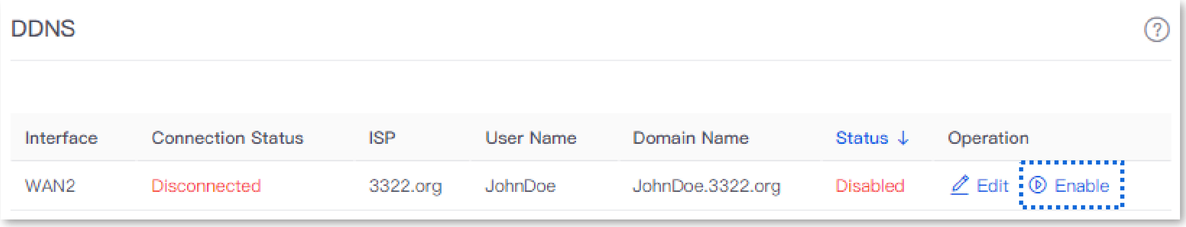
– Set **User Name** and **Password**, which are **JohnDoe** and **JohnDoe123456** in this example.

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


Edit WAN2 DDNS

Interface	WAN2
ISP	3322.org
User Name	JohnDoe
Password	••••••••••••••
Domain Name	JohnDoe.3322.org

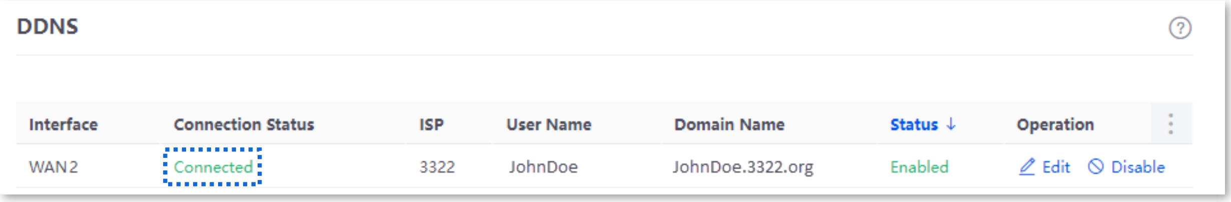
3) Click **Enable**.


DDNS

Interface	Connection Status	ISP	User Name	Domain Name	Status ↓	Operation
WAN2	Disconnected	3322.org	JohnDoe	JohnDoe.3322.org	Disabled	Edit Enable

---End

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



DDNS

Interface	Connection Status	ISP	User Name	Domain Name	Status ↓	Operation
WAN2	Connected	3322	JohnDoe	JohnDoe.3322.org	Enabled	Edit Disable

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 is completed, try the following methods one by one:

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

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.

9.2.3 DNS hijacking

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.

Log in to the web UI of the router, and navigate to **More** > **Virtual Service** > **DNS Hijacking** to enter the page. On this page, you can configure the DNS hijacking policy as required.

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:

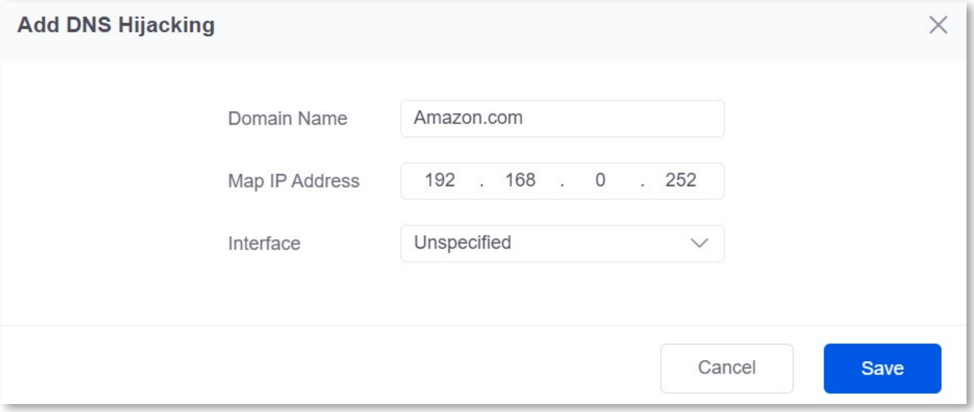
When LAN users visit Amazon (Amazon.com), eBay (eBay.com) and other websites, they can access the web UI of the router.

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**.
   1) Set **Domain Name** of Amazon, which is **Amazon.com** in this example.
   2) Set **Map IP Address** of the router, which is **192.168.0.252** in this example.



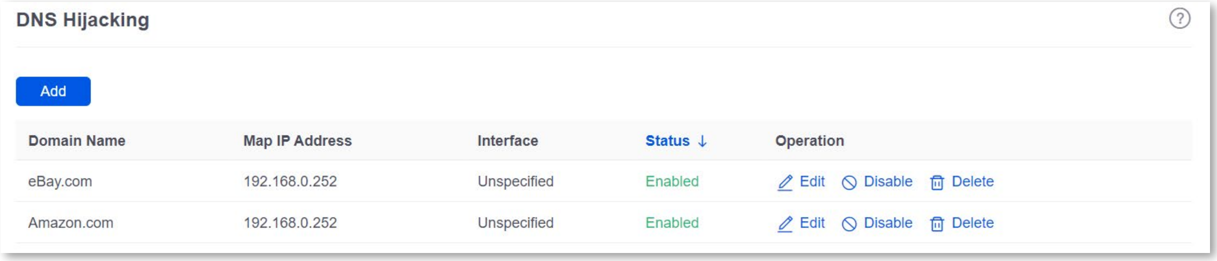
Add DNS Hijacking

Domain Name: Amazon.com

Map IP Address: 192 . 168 . 0 . 252

Interface: Unspecified

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



DNS Hijacking

Domain Name	Map IP Address	Interface	Status ↓	Operation
eBay.com	192.168.0.252	Unspecified	Enabled	Edit Disable Delete
Amazon.com	192.168.0.252	Unspecified	Enabled	Edit Disable Delete

---End

Verification

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

Parameter description

Parameter	Description
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.

9.2.4 IP hijacking

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

Log in to the web UI of the router, and navigate to **More** > **Virtual Service** > **IP Hijacking** to enter the page. On this page, you can configure the IP hijacking policy as required.

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

Example of configuring IP hijacking

Networking requirements

An enterprise uses the enterprise-class router to set up a network. The router is 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.

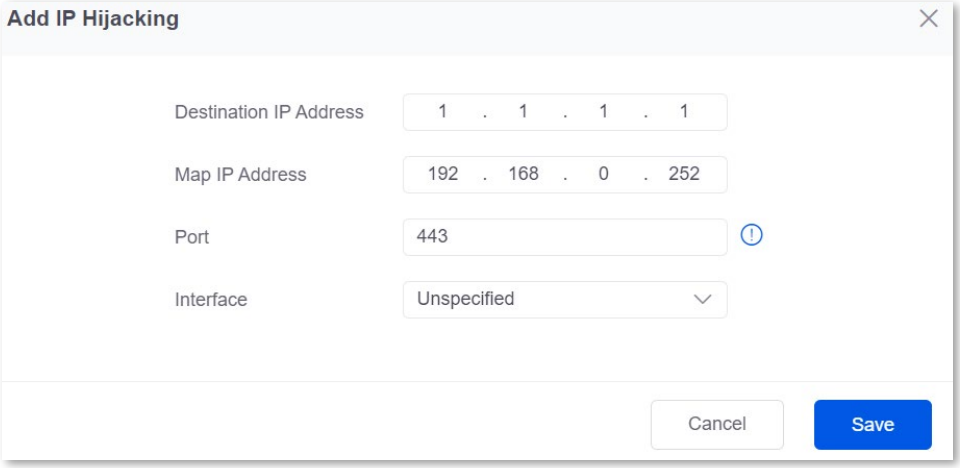
Solution

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 number of the HTTPS web service 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**.
   1) Set **Destination IP Address**, which is **1.1.1.1** in this example.
   2) Set **Map IP Address**, which is **192.168.0.252** in this example.
   3) Set **Port**, which is **443** in this example.



Add IP Hijacking

Destination IP Address: 1 . 1 . 1 . 1

Map IP Address: 192 . 168 . 0 . 252

Port: 443

Interface: Unspecified

---End

Verification

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

Parameter description

Parameter	Description
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.

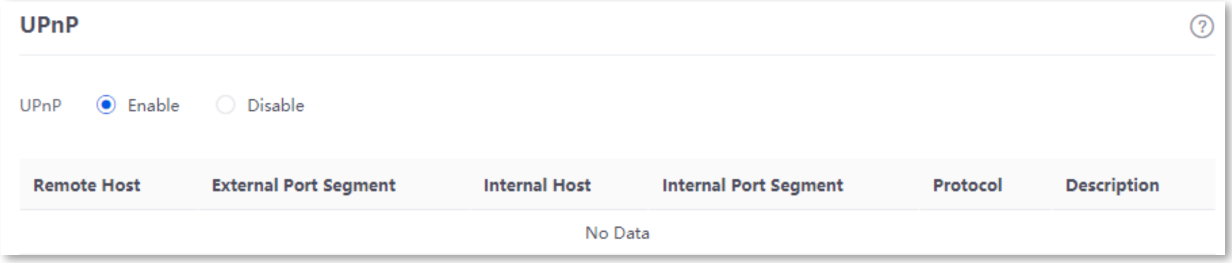
Parameter	Description
Port	Specifies the port to which the IP hijacking policy applies. The IP addresses will be hijacked only when specified ports are accessed. Tip The value 0 indicates all ports.
Interface	Specifies the specified egress of the IP hijacking policy.

9.2.5 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.

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

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



UPnP

UPnP ● Enable ○ Disable

Remote Host	External Port Segment	Internal Host	Internal Port Segment	Protocol	Description
No Data					

9.2.6 Port mirroring

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.

Log in to the web UI of the router, and navigate to **More** > **Virtual Service** > **Port Mirroring** to enter the page. On this page, you can configure the port mirroring according to your needs.

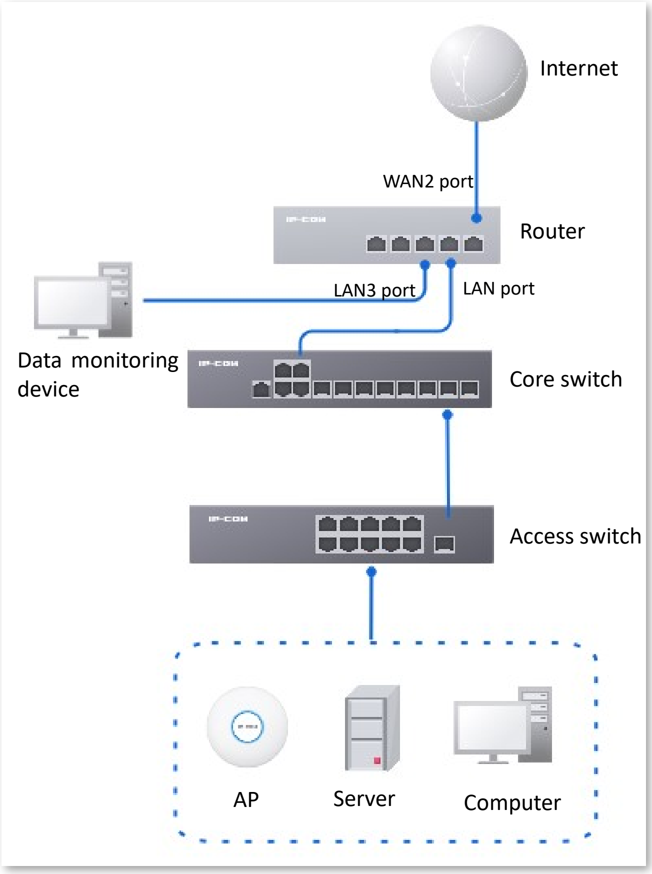
Example of configuring port mirroring

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.

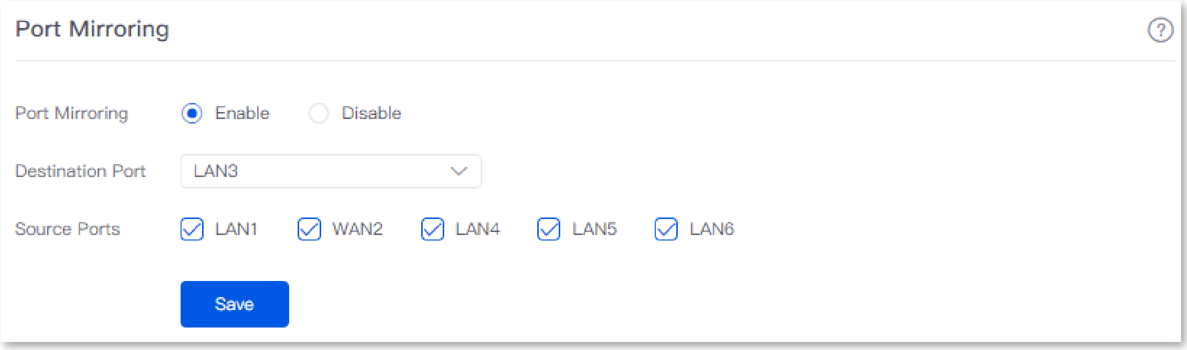
Solution

- 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. Enable the **Port Mirroring** function.
4. Select **Destination Port**, which is **LAN3** in this example.
5. Select **Source Ports**, which is **LAN1**, **WAN2**, **LAN4**, **LAN5** and **LAN6** in this example.
6. Click **Save**.



Port Mirroring

Port Mirroring ● Enable ○ Disable

Destination Port LAN3

Source Ports ☑ LAN1 ☑ WAN2 ☑ LAN4 ☑ LAN5 ☑ LAN6

---End

Verification

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

Parameter description

Parameter	Description
Port Mirroring	Used to enable or disable 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.

9.2.7 Port mapping

By default, users on the internet cannot access devices on 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.

Log in to the web UI of the router, and 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.

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

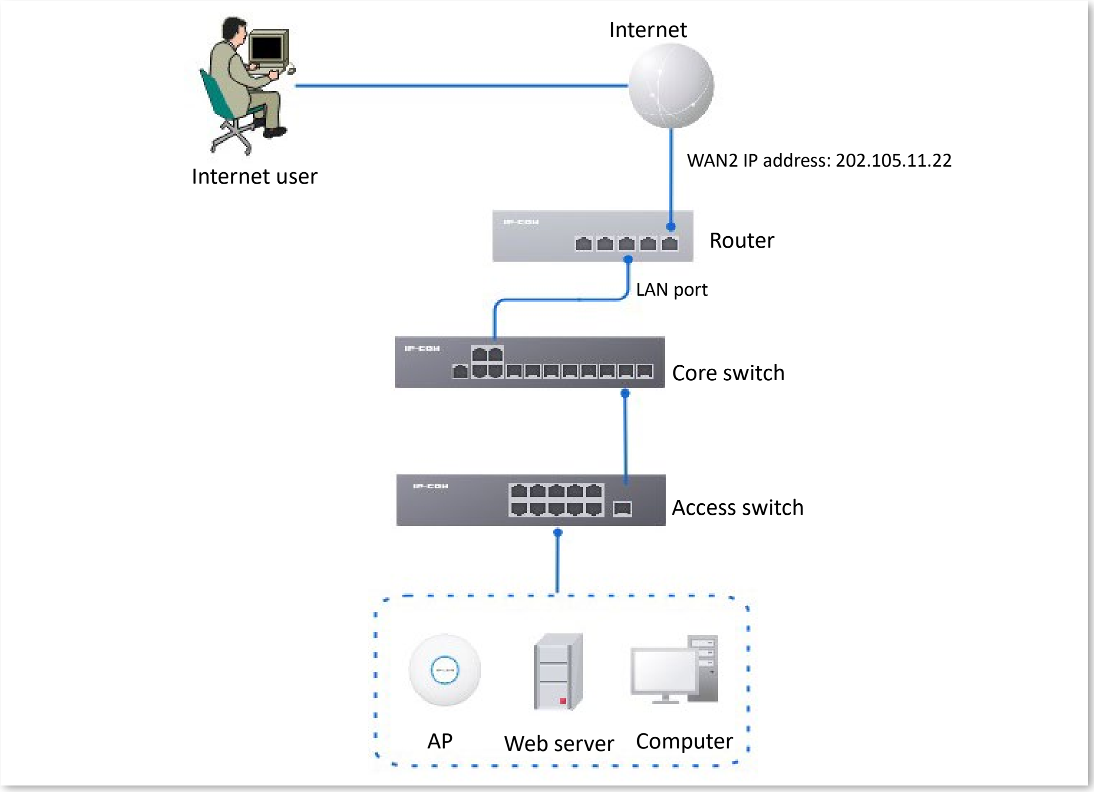
- You can use the Port Mapping function to enable internet users to access the intranet web server. Assume that the external network port opened by the router is 9999.
- You can use the DHCP Reservation function to avoid access failures caused by web server address changes.

Assume that the information on the web server is shown below:

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

Tip

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



Configuration procedure

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

1. Log in to the web UI of the router.
2. Set port mapping.
   1) Navigate to **More** > **Virtual Service** > **Port Mapping**.
   2) Enable the **Port Mapping** function, and click **Add**.
   3) Configure parameters in the **Add** window, and click **Save**.

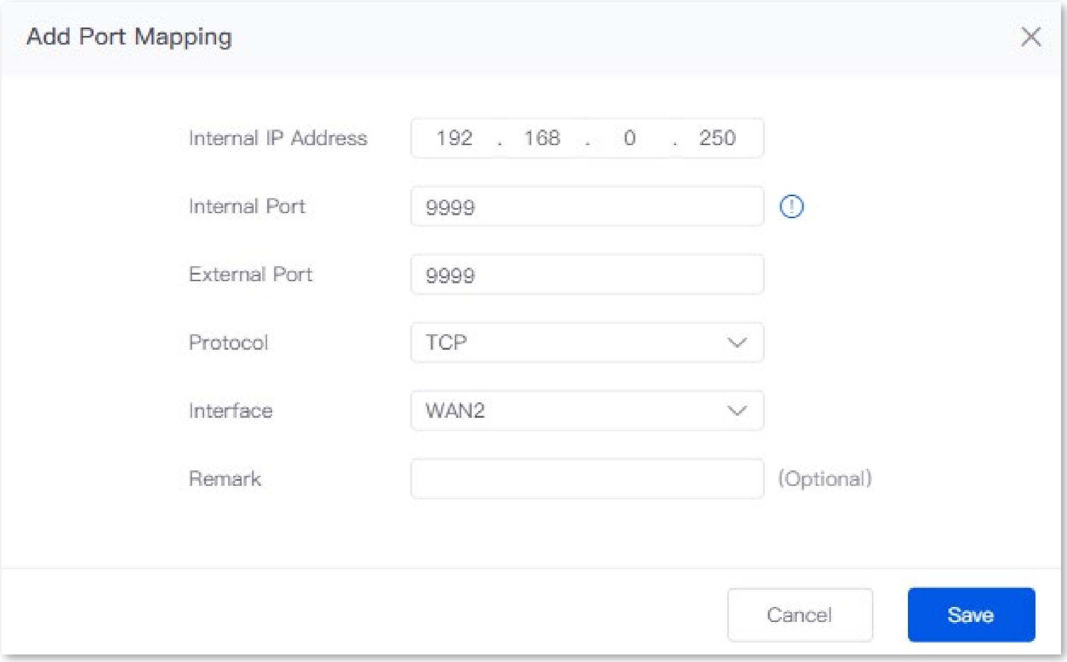
   – Set **Internal IP Address** (the IP address of the web server), which is **192.168.0.250** in this example.

   – 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.

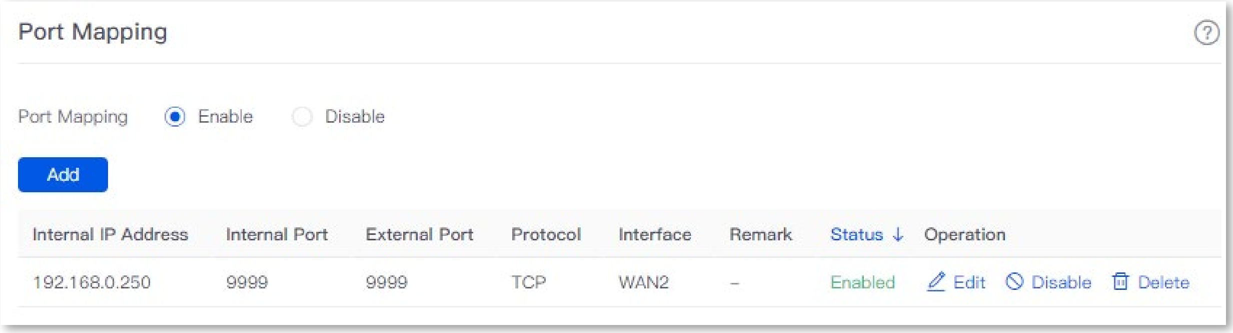
   – Set **Interface** (the WAN port used by Internet users to access the LAN server), which is **WAN2** in this example.



Add Port Mapping

Internal IP Address	192 . 168 . 0 . 250
Internal Port	9999
External Port	9999
Protocol	TCP
Interface	WAN2
Remark	(Optional)

The port mapping policy has been added successfully. See the following figure.



Port Mapping

Port Mapping ● Enable ○ Disable

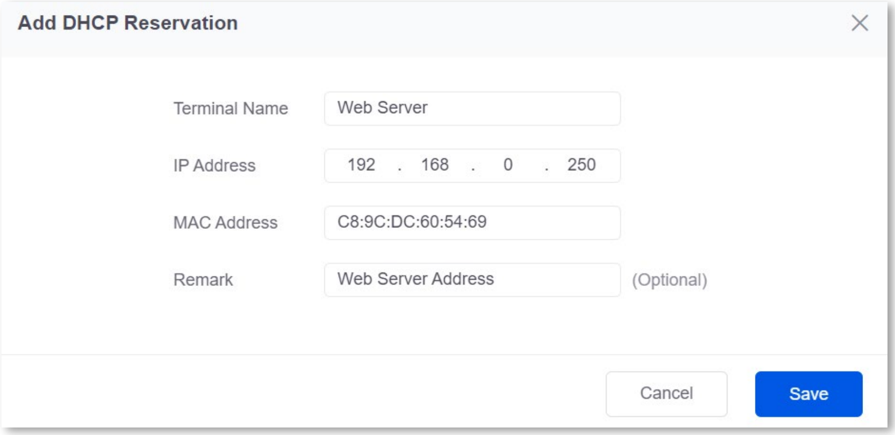
Internal IP Address	Internal Port	External Port	Protocol	Interface	Remark	Status ↓	Operation
192.168.0.250	9999	9999	TCP	WAN2	–	Enabled	Edit Disable Delete

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.

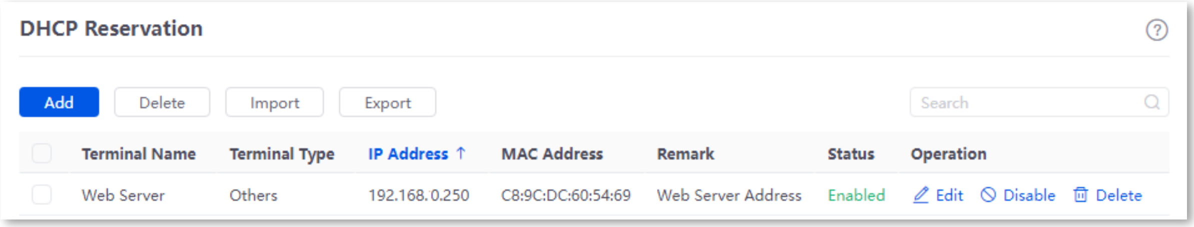


Add DHCP Reservation

Terminal Name	Web Server
IP Address	192 . 168 . 0 . 250
MAC Address	C8:9C:DC:60:54:69
Remark	Web Server Address (Optional)

---End

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



DHCP Reservation

□	Terminal Name	Terminal Type	IP Address ↑	MAC Address	Remark	Status	Operation
□	Web Server	Others	192.168.0.250	C8:9C:DC:60:54:69	Web Server Address	Enabled	Edit Disable Delete

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 is completed, try the following methods one by one:

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

Parameter description

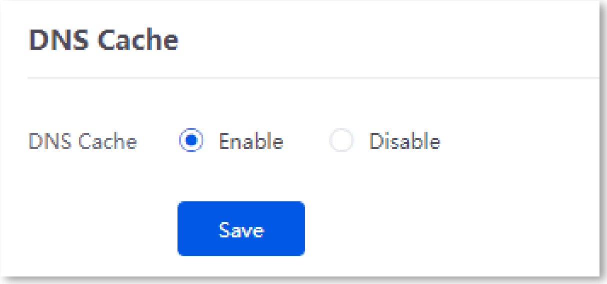
Parameter	Description
Internal IP Address	Specifies the IP address of the internal server.
Internal Port	Specifies the service port of the LAN host.
External Port	Specifies the port opened by the router for access from internet users.
Protocol	Specifies the protocol type used by the LAN host. If you 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.

9.2.8 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 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.

Log in to the web UI of the router, and navigate to **More** > **Virtual Service** > **DNS Cache** to access the page. The DNS cache function is enabled by default.



DNS Cache

DNS Cache ● Enable ○ Disable

9.3 Maintenance service

9.3.1 Remote web management

Generally, you can log in to the web UI of the router only when you connect to the LAN port or the wireless 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).

Log in to the web UI of the router, and 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.

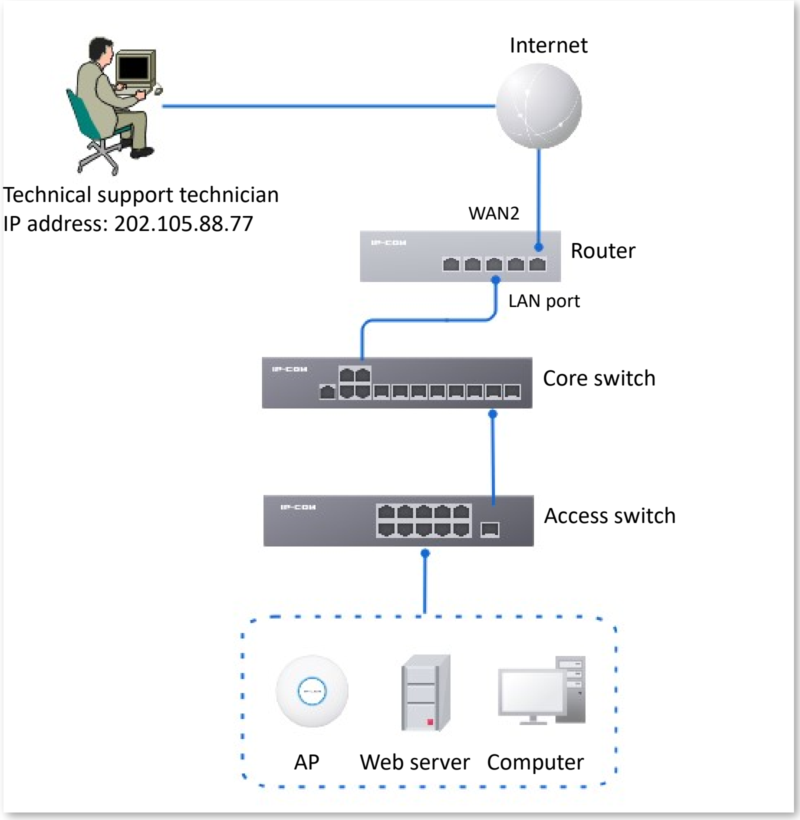
Example of configuring remote web management

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.

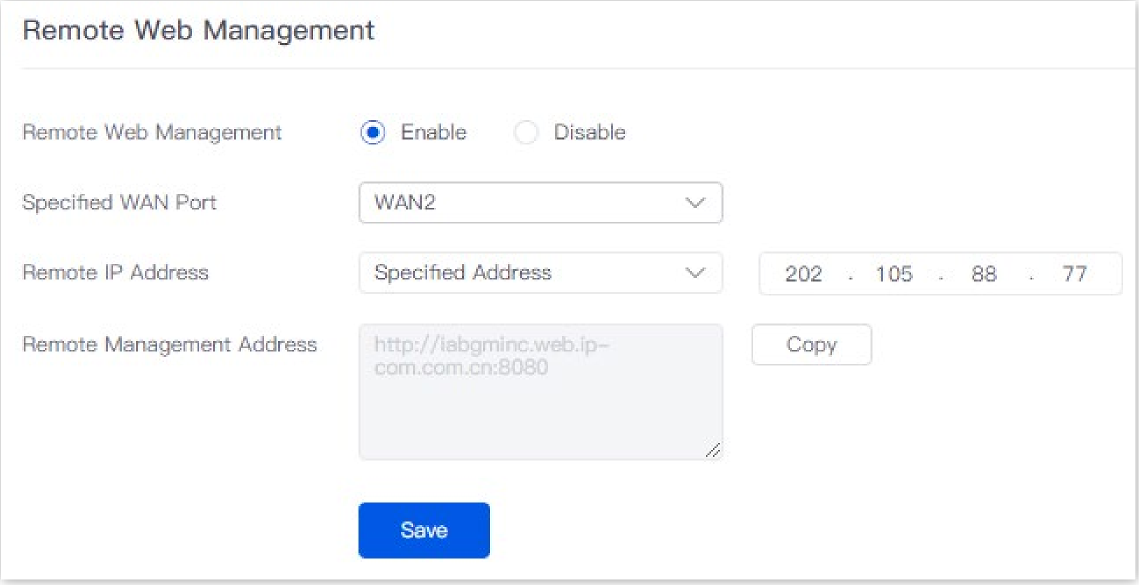
Solution

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. Enable the **Remote Web Management** function.
3. Set **Specified WAN Port**, which is **WAN2** 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**.



Remote Web Management

Remote Web Management: ● Enable ○ Disable

Specified WAN Port: WAN2

Remote IP Address: Specified Address 202 . 105 . 88 . 77

Remote Management Address: http://iabgminc.web.ip-com.com.cn:8080

---End

Verification

The IP-COM technical support technician can log in to the web UI of the router by visiting **Remote Management Address** on the computer (the IP address of the computer is 202.105.88.77).

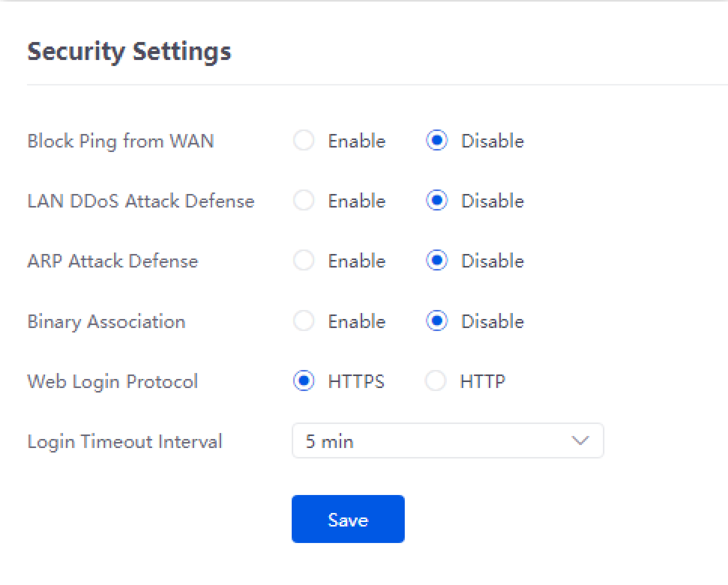
Parameter description

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.

9.3.2 Security settings

Log in to the web UI of the router, and 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.



Security Settings

Block Ping from WAN ○ Enable ● Disable

LAN DDoS Attack Defense ○ Enable ● Disable

ARP Attack Defense ○ Enable ● Disable

Binary Association ○ Enable ● Disable

Web Login Protocol ● HTTPS ○ HTTP

Login Timeout Interval 5 min

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.

Parameter	Description
LAN DDoS Attack Defense	Used to enable or disable the LAN DDoS attack defense function. DDoS is abbreviated for Distributed Denial of Service. The DDoS 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.
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.

9.3.3 Cloud maintenance

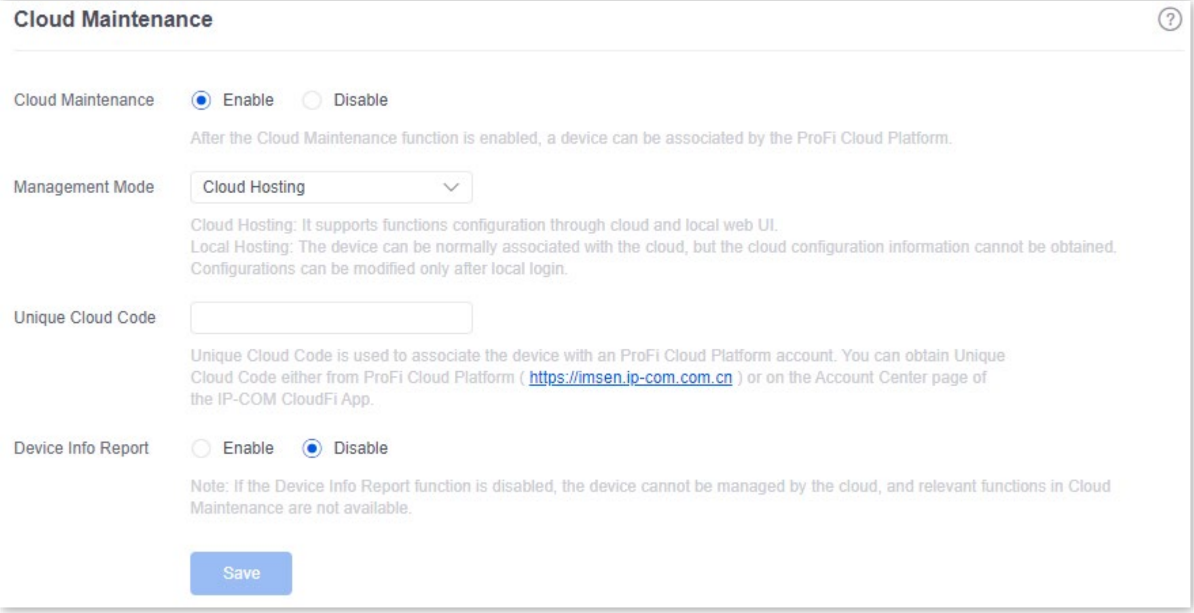
Tip

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

The IP-COM ProFi Cloud Management system is a cloud platform providing central management for IP-COM devices that support cloud management.

The router can be managed by the IP-COM ProFi Cloud platform. You can configure and check the parameters of the router on the web UI of the IP-COM ProFi cloud platform (https://imsen.ip-com.com.cn) or IP-COM ProFi App.

Log in to the web UI of the router, and navigate to **More** > **Maintenance Service** > **Cloud Maintenance** to enter the page. On this page, you can configure the Cloud Maintenance function of the router.



Cloud Maintenance

Cloud Maintenance ● Enable ○ Disable

After the Cloud Maintenance function is enabled, a device can be associated by the ProFi Cloud Platform.

Management Mode: Cloud Hosting

Cloud Hosting: It supports functions configuration through cloud and local web UI.
Local Hosting: The device can be normally associated with the cloud, but the cloud configuration information cannot be obtained. Configurations can be modified only after local login.

Unique Cloud Code:

Unique Cloud Code is used to associate the device with an ProFi Cloud Platform account. You can obtain Unique Cloud Code either from ProFi Cloud Platform (https://imsen.ip-com.com.cn) or on the Account Center page of the IP-COM CloudFi App.

Device Info Report ○ Enable ● Disable

Note: If the Device Info Report function is disabled, the device cannot be managed by the cloud, and relevant functions in Cloud Maintenance are not available.

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 (web portal or 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 IP-COM ProFi cloud platform account associated with the device. You can obtain it from the IP-COM ProFi cloud platform (https://imsen.ip-com.com.cn) or the IP-COM ProFi App.
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 IP-COM ProFi Cloud platform. The configuration information of the router will be reported to the cloud platform.

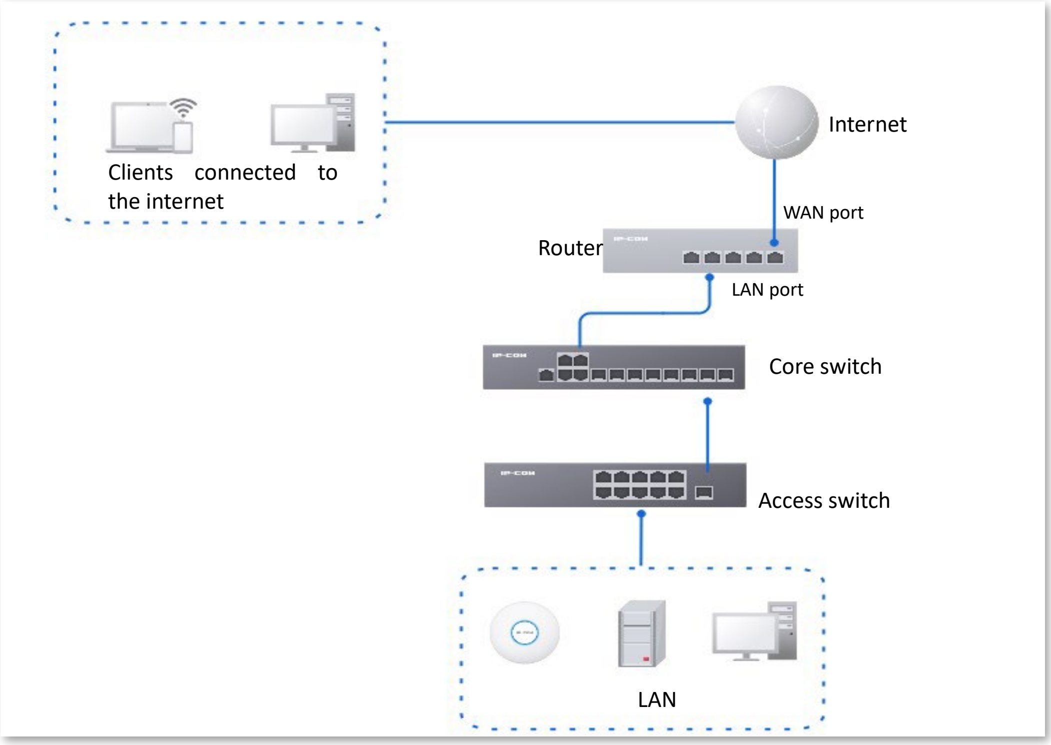
Example of configuring cloud maintenance on IP-COM ProFi Cloud platform

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 IP-COM ProFi Cloud platform to meet the requirements.



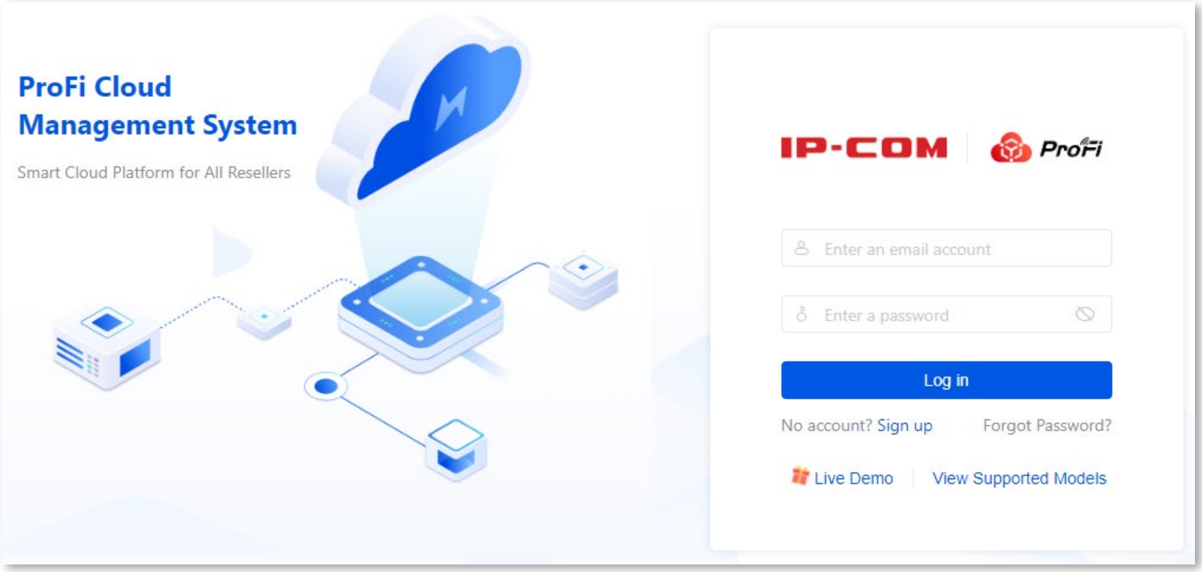
Configuration procedure

Tip

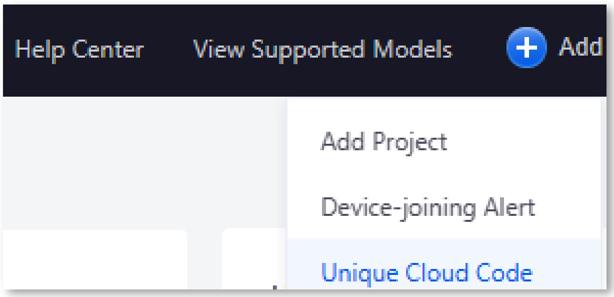
- Before configuring the cloud maintenance function of the router, ensure that the router is connected to the internet.
- The system version V1.5.6 of the IP-COM ProFi cloud management is used as an example. The actual operation and UI interface of the system version prevail.

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

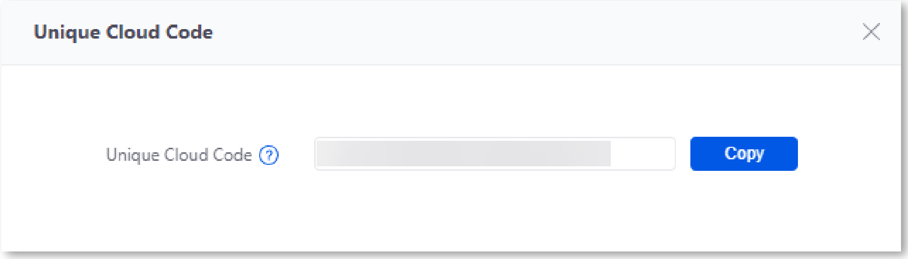
   1) On a computer that has connected to the Internet, start a web browser, visit https://imsen.ip-com.com.cn, and access the IP-COM ProFi cloud platform.



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



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

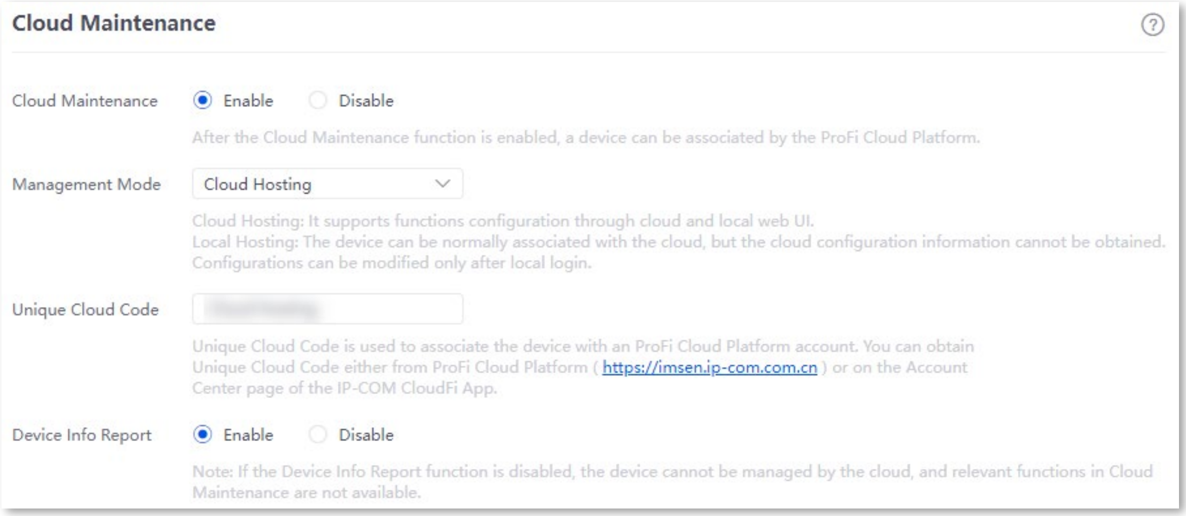


2. Enable the cloud maintenance function for the router.

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**.



Cloud Maintenance

Cloud Maintenance ● Enable ○ Disable

After the Cloud Maintenance function is enabled, a device can be associated by the ProFi Cloud Platform.

Management Mode: Cloud Hosting

Cloud Hosting: It supports functions configuration through cloud and local web UI.
Local Hosting: The device can be normally associated with the cloud, but the cloud configuration information cannot be obtained. Configurations can be modified only after local login.

Unique Cloud Code: [redacted]

Unique Cloud Code is used to associate the device with an ProFi Cloud Platform account. You can obtain Unique Cloud Code either from ProFi Cloud Platform (https://imsen.ip-com.com.cn) or on the Account Center page of the IP-COM CloudFi App.

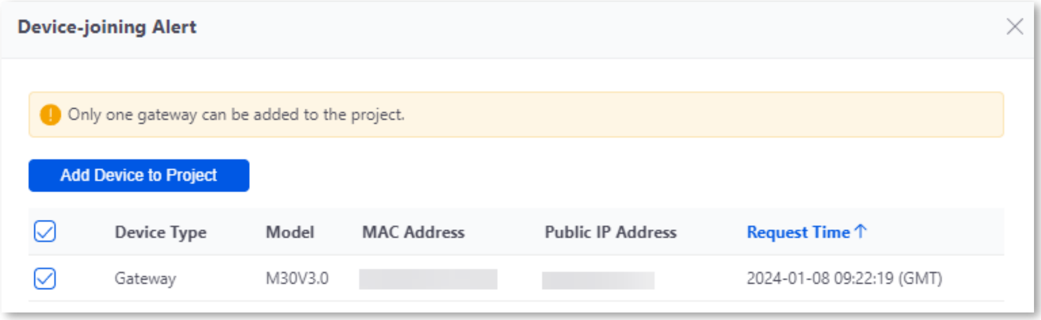
Device Info Report ● Enable ○ Disable

Note: If the Device Info Report function is disabled, the device cannot be managed by the cloud, and relevant functions in Cloud Maintenance are not available.

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

   1) Log in to the IP-COM ProFi cloud platform. Click **Add** in the upper right corner and select **Device-joining Alert**.

   2) Select the router to be added to the project and click **Add Device to Project**. The following figure is for reference only.



Device-joining Alert

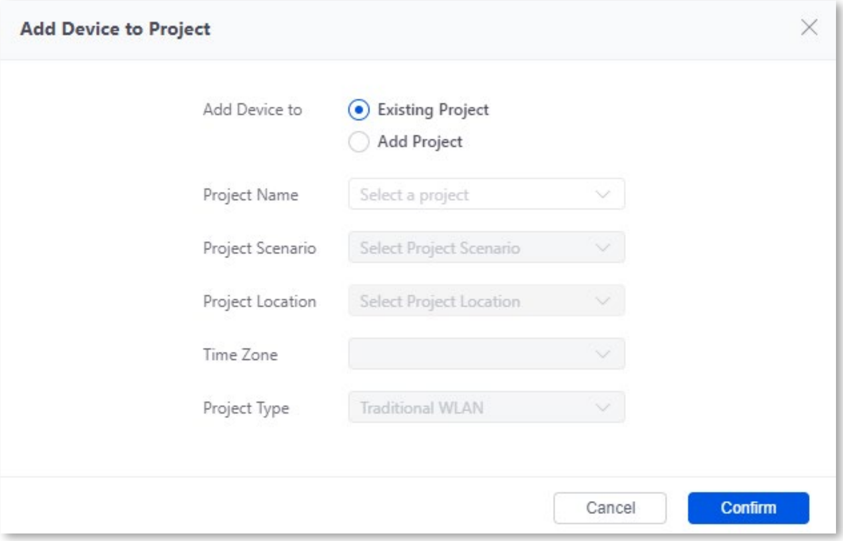
Only one gateway can be added to the project.

Add Device to Project

☑	Device Type	Model	MAC Address	Public IP Address	Request Time ↑
☑	Gateway	M30V3.0	[redacted]	[redacted]	2024-01-08 09:22:19 (GMT)

   3) Select the project to which you want to add the router. The following figure is for reference only.

If the project has already been created, select **Existing Project,** select the corresponding project in the **Project Name** drop-down menu, and then click **Confirm**.



Add Device to Project

Add Device to: ● Existing Project ○ Add Project

Project Name: Select a project

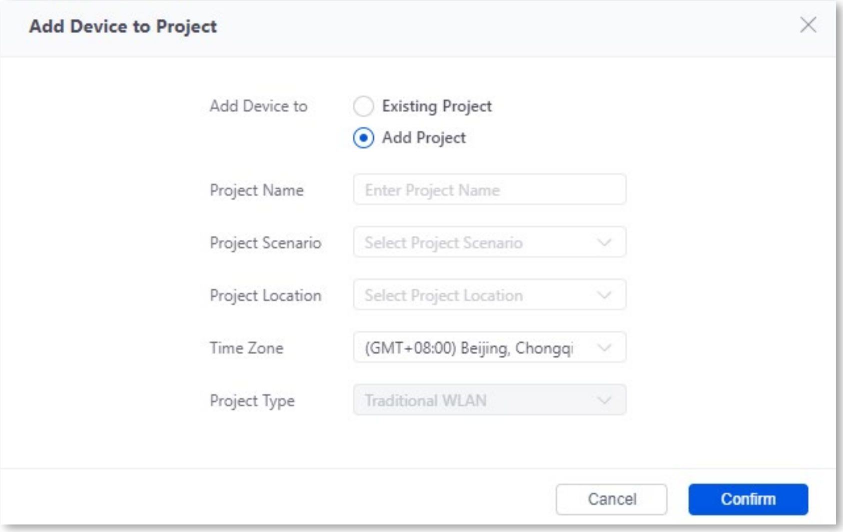
Project Scenario: Select Project Scenario

Project Location: Select Project Location

Time Zone:

Project Type: Traditional WLAN

If you want to create a new project, select **Add Project**, set the **Project Name**, **Project Scenario** and **Project Location**, and then click **Confirm**.



Add Device to Project

Add Device to: ○ Existing Project ● Add Project

Project Name: Enter Project Name

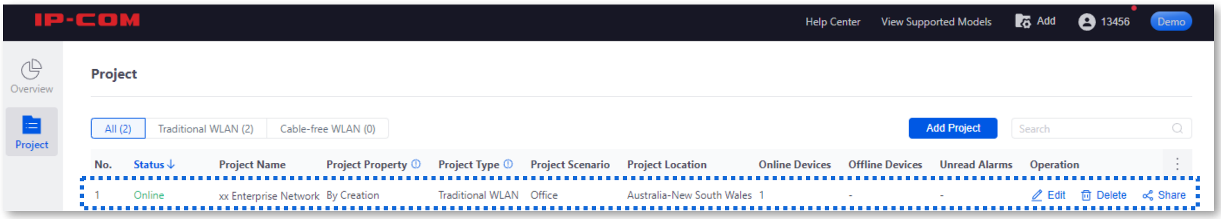
Project Scenario: Select Project Scenario

Project Location: Select Project Location

Time Zone: (GMT+08:00) Beijing, Chongqi

Project Type: Traditional WLAN

Added successfully. You can enter the **Project** page to view details. The following figure is for reference only.



No.	Status	Project Name	Project Property	Project Type	Project Scenario	Project Location	Online Devices	Offline Devices	Unread Alarms	Operation
1	Online	xx Enterprise Network	By Creation	Traditional WLAN	Office	Australia-New South Wales	1	-	-	Edit Delete Share

---End

Verification

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

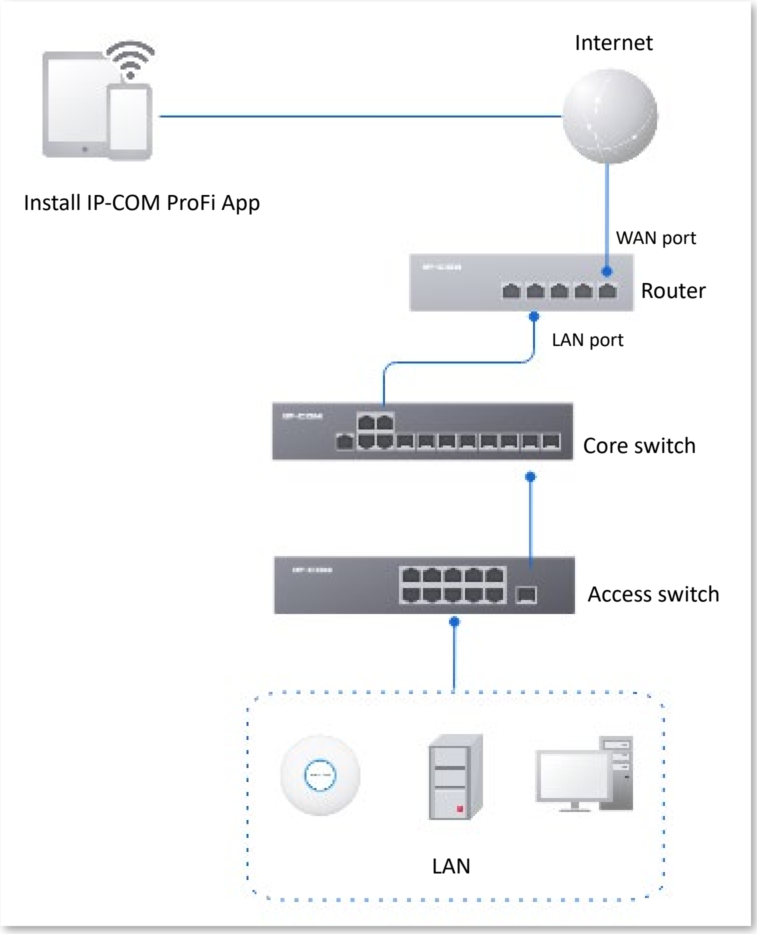
Example of configuring cloud maintenance on IP-COM ProFi App

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 IP-COM ProFi App to meet the requirements.



Configuration procedure (method 1)

Tip

Before configuring the cloud maintenance function of the router, ensure that the router is connected to the Internet.

1. Scan the QR code to download the IP-COM ProFi App. Then log in to the App

2. Connect your mobile device such as smartphone to the Wi-Fi of the AP.

3. Run the IP-COM ProFi App, and add the router to the project.

   1) (Skip if done) Add a project.

   2) Enter the project you want to add the router. The pop-up window will show the detected router. Then add the router to the project by following the instruction.

   You can view the **Help Documentation** of the IP-COM ProFi App on the **Help Center** page of the IP-COM ProFi App for specific methods.

   Configuration procedure (method 2)

Tip

Before configuring the cloud maintenance function of the router, ensure that the router is connected to the Internet.

1. Scan the QR code to download the IP-COM ProFi App.

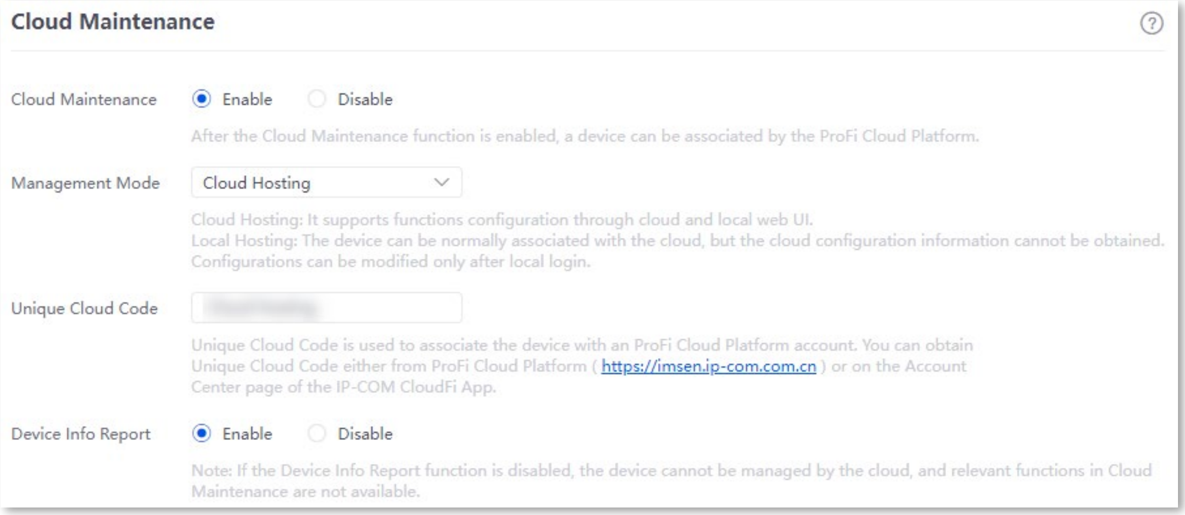
2. Log in to the IP-COM ProFi App and obtain **Unique Cloud Code**.

3. 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) Enable the **Cloud Maintenance** function, 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**.



Cloud Maintenance

Cloud Maintenance ● Enable ○ Disable

After the Cloud Maintenance function is enabled, a device can be associated by the ProFi Cloud Platform.

Management Mode: Cloud Hosting

Cloud Hosting: It supports functions configuration through cloud and local web UI.
Local Hosting: The device can be normally associated with the cloud, but the cloud configuration information cannot be obtained. Configurations can be modified only after local login.

Unique Cloud Code: [redacted]

Unique Cloud Code is used to associate the device with an ProFi Cloud Platform account. You can obtain Unique Cloud Code either from ProFi Cloud Platform (https://imsen.ip-com.com.cn) or on the Account Center page of the IP-COM CloudFi App.

Device Info Report ● Enable ○ Disable

Note: If the Device Info Report function is disabled, the device cannot be managed by the cloud, and relevant functions in Cloud Maintenance are not available.

4. (Skip if done) Add a project on the IP-COM ProFi App.

5. Add the router to the project.

   You can view the **Help Documentation** of the IP-COM ProFi App on the **Help Center** page of the IP-COM ProFi App for specific methods.

   ---End

   Verification

   After the configuration is completed, the router can be managed through the IP-COM ProFi App, and all its configuration information is delivered by the cloud platform.

9.3.4 SSH maintenance

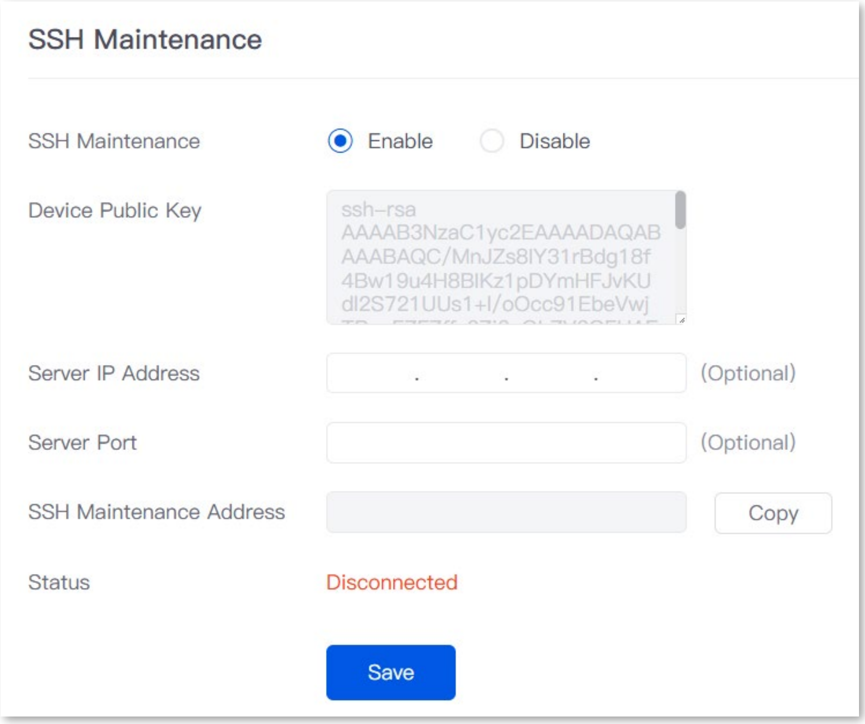
This function can be used for remote network debugging by professional engineers. After enabling this function, professional engineers can remotely connect to the router through Secure Shell (SSH) and perform remote debugging.

Log in to the web UI of the router, and navigate to **More** > **Maintenance Service** > **SSH Maintenance** to enter this page. On this page, you can configure the remote debugging function.

Remotely connect to the router using an SSH tool

Enable the SSH maintenance function

1. Log in to the web UI of the router.
2. Navigate to **More** > **Maintenance Service** > **SSH Maintenance**.
3. Enable the **SSH Maintenance** function. Retain default settings for other parameters and click **Save**.



SSH Maintenance

SSH Maintenance ● Enable ○ Disable

Device Public Key
ssh–rsa
AAAAB3NzaC1yc2EAAAADAQAB
AAABAQC/MnJZs8lY31rBdg18f
4Bw19u4H8BlKz1pDYmHFJvKU
dl2S721UUs1+l/oOcc91EbeVwj

Server IP Address . . . (Optional)

Server Port (Optional)

SSH Maintenance Address Copy

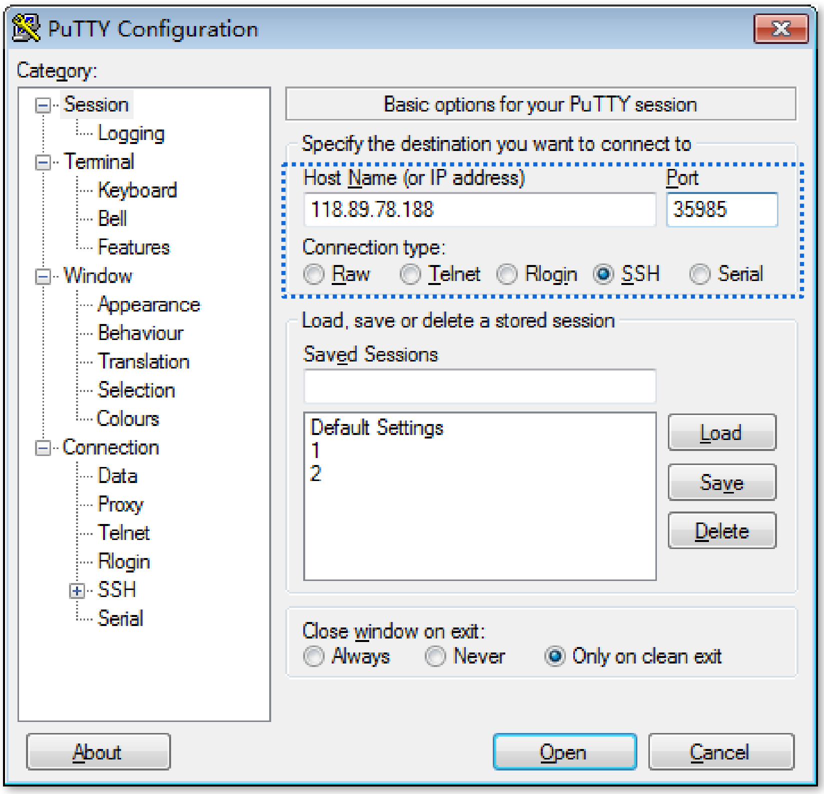
Status Disconnected

Save

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

Remotely connect to the router using an SSH tool

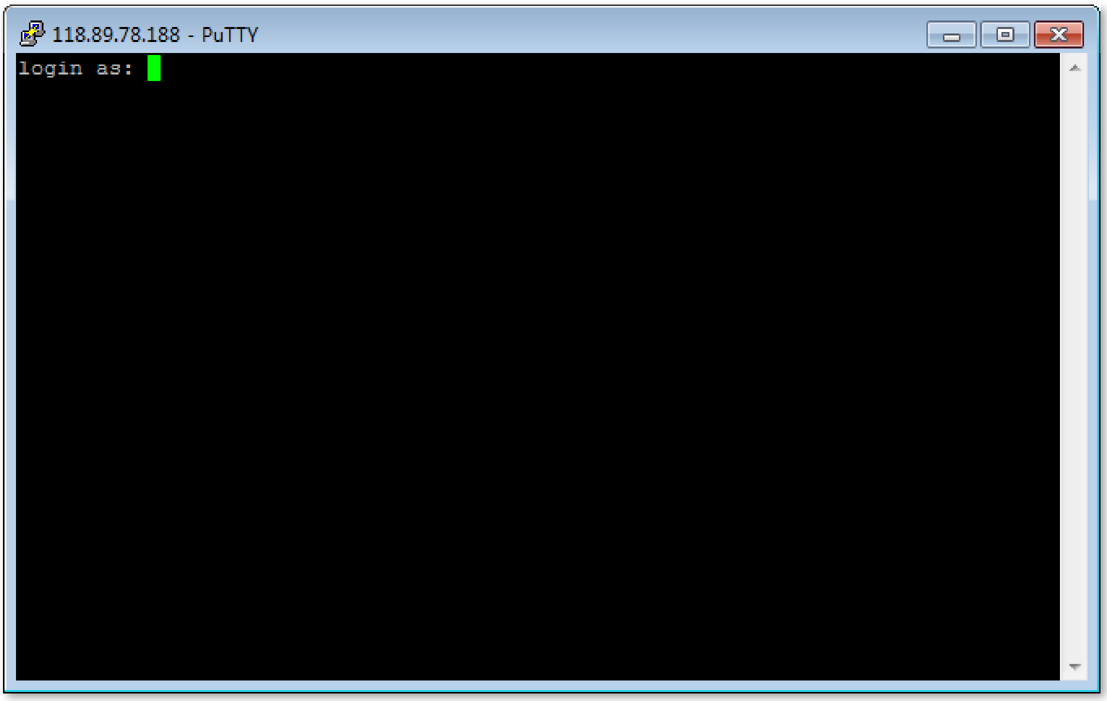
1. Run an SSH client tool (PuTTY used for example here) on a computer connected to the network.
2. Set **Connection Type** to **SSH**.
3. Set **Host Name (or IP address)** to the remote debugging address and port to be accessed. The following figure shows an example.
4. Click **Open**.



Host Name (or IP address): 118.89.78.188
Port: 35985
Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial
Close window on exit: ○ Always ○ Never ● Only on clean exit

---End

If the following figure is displayed, the router is connected successfully.



```
login as:
```

Parameter description

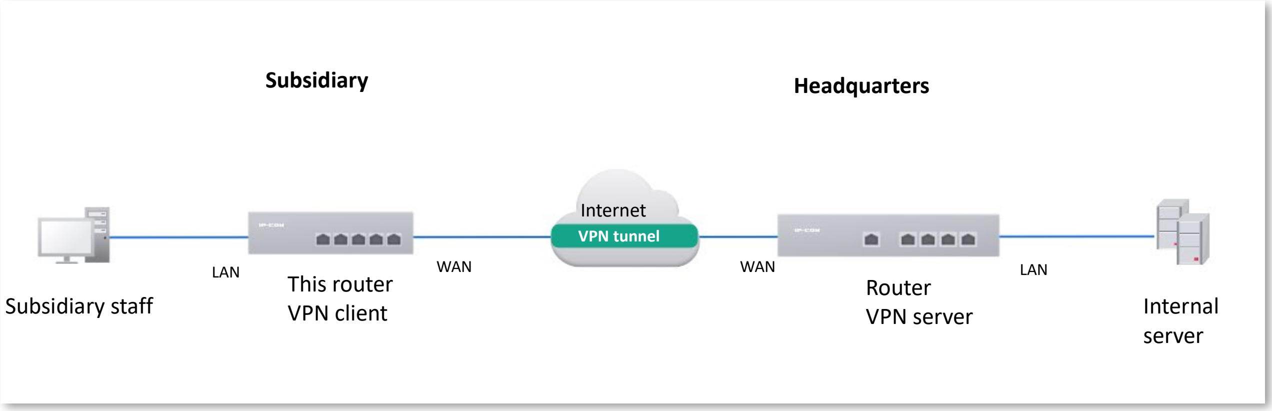
Parameter	Description
SSH Maintenance	Used to enable or disable the SSH maintenance function.
Device Public Key	Specifies the RSA public key of the device. The device's public key has been preset in the authorization list in the default server. If the default server is not used, you need to add the device 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.
SSH Maintenance Address	Specifies the address for remotely accessing this device using SSH.

9.4 VPN

9.4.1 Overview

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

The typical network topology of VPN is as follows:



This router supports Point to Point Tunneling Protocol (PPTP) server, Layer 2 Tunneling Protocol (L2TP) server and IP Security (IPSec).

- **Layer-2 VPN channel protocol: PPTP, L2TP**

Layer-2 VPN channel protocol is used to transmit Layer-2 (data link layer) network protocol, where frames at the data link layer are transmitted in the tunnel.

PPTP encapsulates Point to Point Protocol (PPP) frames into IP data packets and transmits data over the internet. L2TP encapsulates PPP frames into different data packets for transmission according to different network types.

- **Layer-3 VPN channel protocol: IPSec**

Layer-3 VPN channel protocol is used to transmit Layer-3 (network layer) network protocol, where groups at the network layer are transmitted in the tunnel.

IPSec encapsulates data in a tunneling protocol and relies on the third layer to transmit the networks only for TCP/IP.

Compared with the Layer-2 VPN channel protocol, the Layer-3 VPN channel protocol has better security and reliability. The second-layer tunnel is generally terminated on the user-side device, which has high requirements for the security of the client and firewall technology. While the third-layer tunnel is generally terminated at the Internet Service Provider (ISP) gateway, which does not have high requirements for the security of the client.

- **OpenVPN**

OpenVPN is based on the Secure Sockets Layer/Transport Layer Security (SSL/TLS) framework and operates between the application and transport layers. It uses application-layer mechanisms to establish and manage VPN connections, while relying on Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) at the transport layer for data transmission.

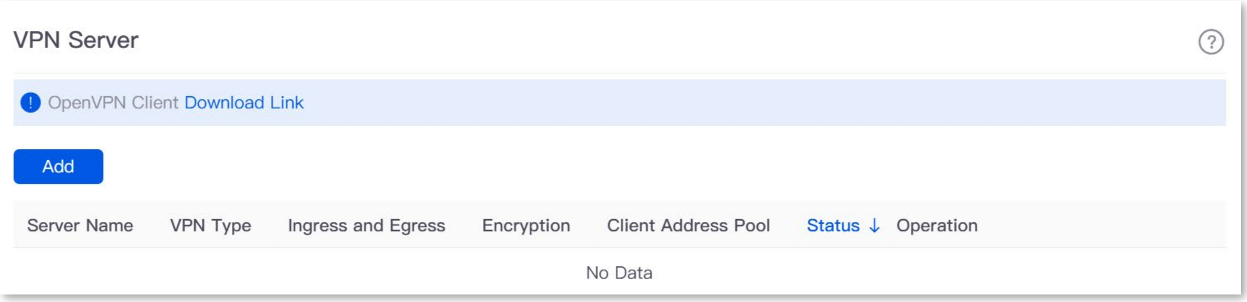
In terms of security architecture, OpenVPN sits between Layer 2 tunneling protocols (such as PPTP and L2TP) and Layer 3 tunneling protocols (such as IPsec), providing a balance of flexibility and security.

9.4.2 PPTP/L2TP/OpenVPN

Configure PPTP/L2TP/OpenVPN server

The router works as a PPTP, L2TP or OpenVPN server and can connect to PPTP, L2TP or OpenVPN clients.

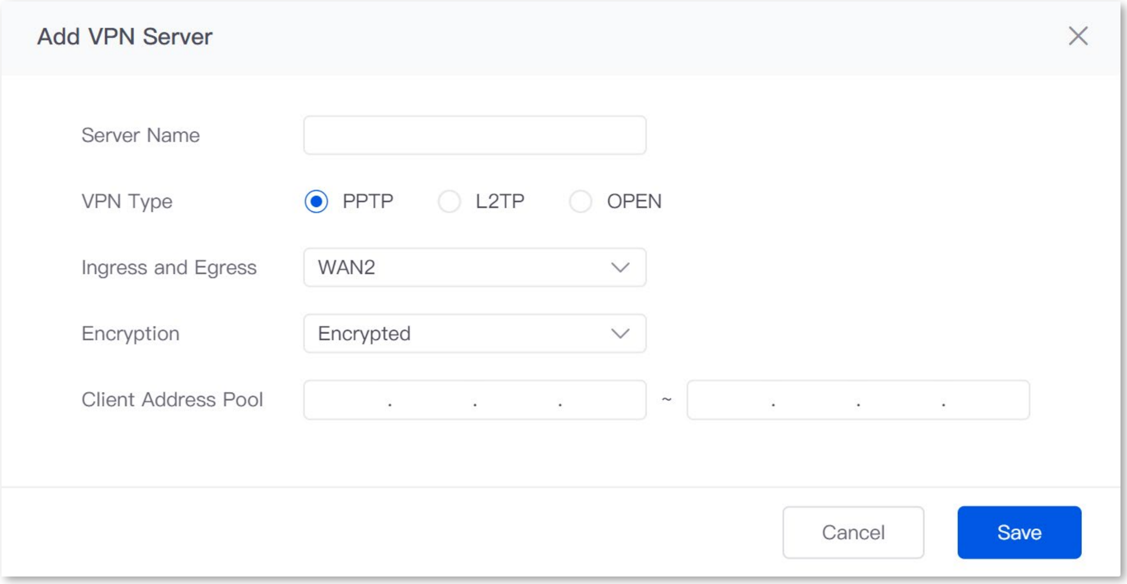
Log in to the web UI of the router, and navigate to **More** > **VPN Service > VPN Server** to enter the page.



VPN Server

OpenVPN Client Download Link

Server Name	VPN Type	Ingress and Egress	Encryption	Client Address Pool	Status ↓	Operation
No Data						



Add VPN Server

Server Name:

VPN Type: ● PPTP ○ L2TP ○ OPEN

Ingress and Egress: WAN2

Encryption: Encrypted

Client Address Pool: . . . ~ . . .

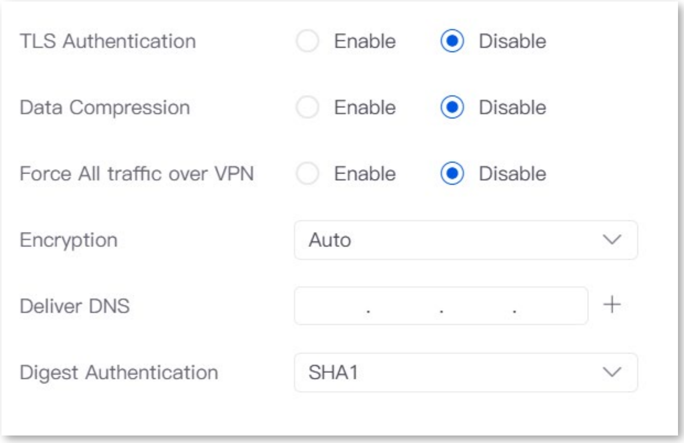
Parameter description

Parameter	Description
Server Name	Specifies the name of the VPN server.
VPN Type	Specifies the VPN server type of the router. – **PPTP**: The router works as a PPTP server and can connect to PPTP clients. – **L2TP**: The router works as a L2TP server and can connect to L2TP clients. – **OPEN**: The router works as an OpenVPN server and can connect to OpenVPN clients.
Ingress and Egress	Specifies the WAN port used for the connection between the VPN server and VPN client. The IP address or domain name of the WAN port is the **Server IP Address/Domain Name** of the VPN client.

Parameter	Description
Encryption	Only PPTP and L2TP servers are supported. – **PPTP**: Specifies whether to enable the 128-bit data encryption. The encryption settings of PPTP server and PPTP client must be consistent. Otherwise, communications cannot be conducted normally. – **L2TP**: Specifies whether to encrypt data packets by enabling the IPSec. The encryption settings of L2TP server and L2TP client must be consistent. Otherwise, communications cannot be conducted normally.
Pre-shared Key	Specifies the pre-shared key of the L2TP server and the L2TP client. When the L2TP tunnel uses IPSec for encryption, both the L2TP client and the L2TP server use this pre-shared key to authenticate each other. The pre-shared key of the L2TP client and the L2TP server should be the same. Used with the L2TP server only.
IKE Policy	Used to establish a secure control channel for negotiating subsequent IPsec SA (Security Association) during the first phase of the VPN connection. Used with the L2TP server only.
Transform Set	Used to define the encryption parameters that protect user data during the second phase of the VPN connection. In this phase, IPsec SAs are created. Used with the L2TP server only.
Exchange Mode	The negotiation mode must be the same as the peer's settings. Used with the L2TP server only. – **Main**: This mode involves the exchange of numerous messages between the two parties and provides identity protection. It is suitable for connections with greater security. – **Aggressive**: This mode provides fast negotiation speed due to fewer messages exchanged and sending identities unprotected. It is suitable for faster connections.
Local ID Type	Local gateway identifier. Used with the L2TP server only. – **IP Address**: The local router negotiates with the peer gateway using the corresponding WAN port IP address. – **NAME**: When selecting this option, you need to enter any string in the **Local ID** field for negotiation with the peer gateway. The local ID must be the same as the peer ID of the remote gateway.
Client Address Pool	Specifies the IP address range within which the VPN server can assign IP addresses to VPN clients. Used with the PPTP and L2TP servers only.

Parameter	Description
Server Mode	Specifies the authentication mode of the OpenVPN server. Used with the OpenVPN server only. – **User/Password**: OpenVPN clients need to use the account and password provided by the OpenVPN server to connect to the OpenVPN server. The server account and password are configured at User Management. – **Certificate**: Uses a Public Key Infrastructure (PKI)–based authentication mechanism. Both the server and the client use digital certificates containing public keys and identity information. During authentication, the server verifies the client certificate by checking the issuing Certificate Authority (CA), certificate validity period, and digital signature. The client also verifies the server certificate. A VPN connection is established only after both certificates are successfully validated. – **User+Certificate**: Both User/Password and Certificate authentication modes are used.
Protocol	Data transmission protocol. Used with the OpenVPN server only. – **TCP**: Data transmission offers reliable performance, ensuring orderly data reception and retransmission of lost data, although the transmission speed is relatively slow. It is suitable for scenarios requiring high data accuracy. – **UDP**: Data transmission is more efficient and suitable for scenarios with high real-time requirements but low sensitivity to data loss, such as video calls.
Port ID	It is recommended to use a registered port (1024~65535) for the OpenVPN service to ensure that the service starts normally.
IP Address	Specifies the OpenVPN address pool. The first available address in the address pool is allocated to the server, and the remaining addresses are allocated to clients. For example, if the address range is set to 10.10.99.0/24, then the server-side VPN virtual address will be 10.10.99.1. Used with the OpenVPN server only.
Deliver Route	The VPN server sends routing configurations to the VPN client, instructing the client on which path to send data packets to the target network.

Click **Show Advanced Settings**. The following figure is for reference only.



TLS Authentication ○ Enable ● Disable

Data Compression ○ Enable ● Disable

Force All traffic over VPN ○ Enable ● Disable

Encryption: Auto

Deliver DNS: . . .

Digest Authentication: SHA1

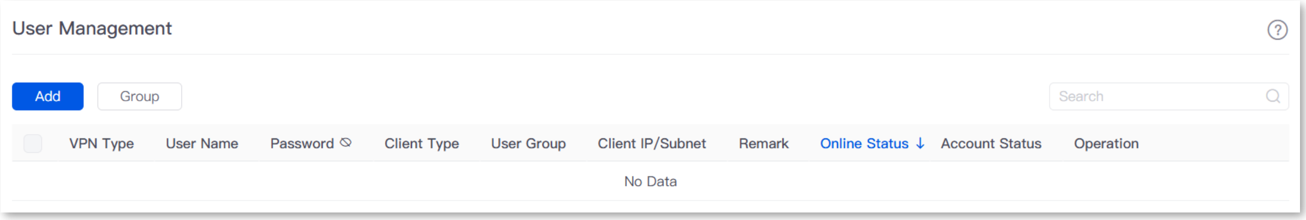
Parameter description

Parameter	Description
TLS Authentication	When enabled, TLS authentication is applied at the transport layer. During the establishment of a secure channel (such as an SSL/TLS–encrypted connection) between the OpenVPN server and client, it performs authentication and protects data during transmission. This may increase system resource usage and network latency. Requires OpenVPN client version 2.4.0 or later.
Data Compression	When enabled, OpenVPN compresses transmitted data to reduce bandwidth usage and improve transmission efficiency. The server and client must use the same settings.
Force All Traffic over VPN	When enabled, the OpenVPN client routes all traffic through the VPN tunnel to the OpenVPN server, except traffic destined for the local network.
Encryption	Specifies the method of data encryption. If this parameter is set to **Auto** on the server side, it can be set to any option on the client side. If a specific encryption algorithm is configured on the server side, the client must select the same encryption algorithm; otherwise, the connection will fail.
Deliver DNS	Specifies whether the OpenVPN server pushes DNS settings to the client, allowing the client to correctly resolve domain names when accessing network resources through the VPN.
Digest Authentication	A security mechanism that uses a hash function to convert data of arbitrary length into a fixed-length message digest. The digest acts as a unique fingerprint to verify data integrity and authenticity during authentication.

Configure user management

Log in to the web UI of the router, and navigate to **More** > **VPN Service > User Management** to enter the page.

On this page, you can configure PPTP or L2TP user accounts. When the PPTP or L2TP server is enabled, VPN users need to use accounts to dial up the VPN on the router.

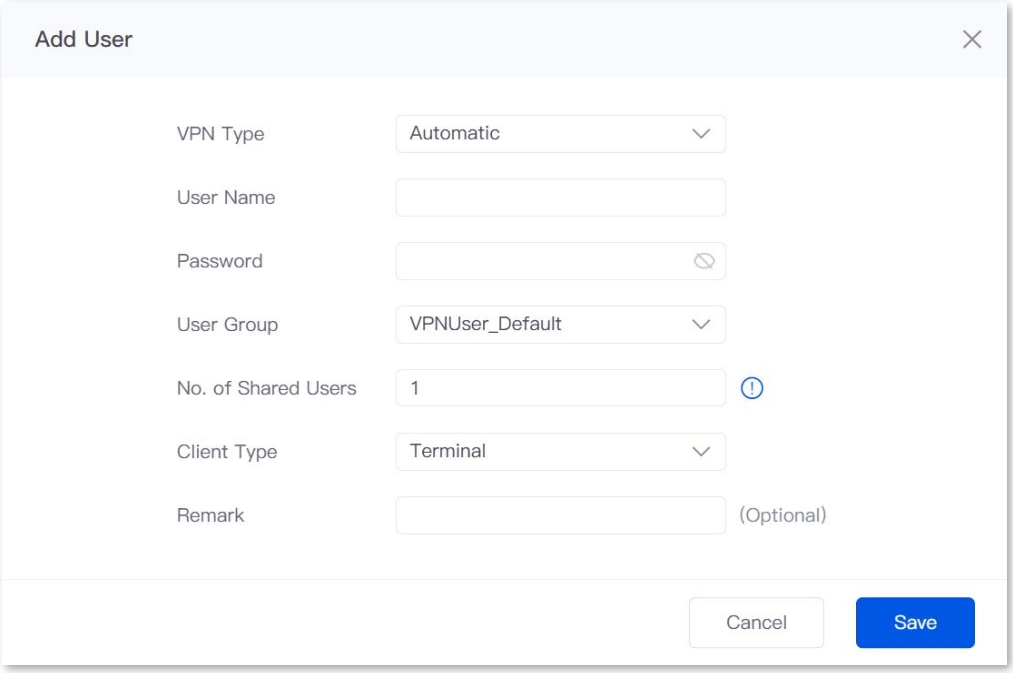


User Management

Add Group Search

☐	VPN Type	User Name	Password	Client Type	User Group	Client IP/Subnet	Remark	Online Status ↓	Account Status	Operation

No Data



Add User

VPN Type: Automatic

User Name:

Password:

User Group: VPNUser_Default

No. of Shared Users: 1

Client Type: Terminal

Remark: (Optional)

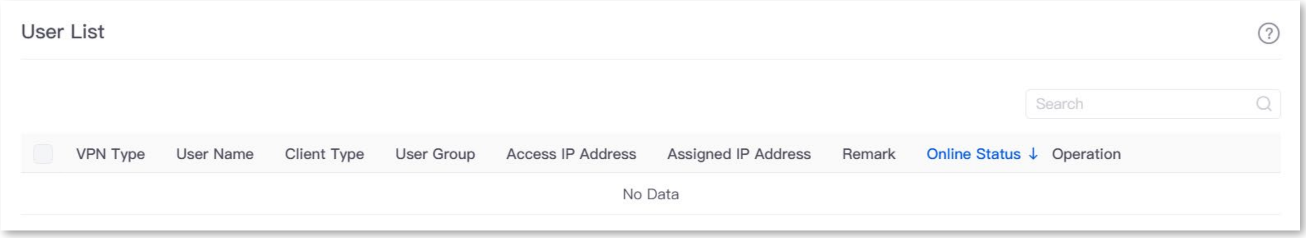
Parameter description

Parameter	Description
VPN Type	Specifies the service type of the client.
User Name	Specifies the user name required for the VPN connection.
Password	Specifies the password required for the VPN connection.
User Group	Specifies the user group that the VPN client is added. After the VPN account is added to a user group, the access permission of subsequent users on the internal server is controlled. The user group must be configured at User Group. Used with the PPTP and L2TP servers only.
No. of Shared Users	Specifies the user limit on sharing the same VPN account.
Client Type	Specifies the type of the VPN client. Used with the PPTP and L2TP servers only. – Select **Terminal** when the VPN client is a single host. – Select **Network Device** when the VPN client is a network.
Client IP/Subnet	Specifies the IP address range of the client intranet. It is available only when the **Client Type** is set to **Network Device**. Used with the PPTP and L2TP servers only.

Configure user list

Log in to the web UI of the router, and navigate to **More** > **VPN Service** to enter the page.

On this page, you can view the VPN client details dialed into the router's VPN server.



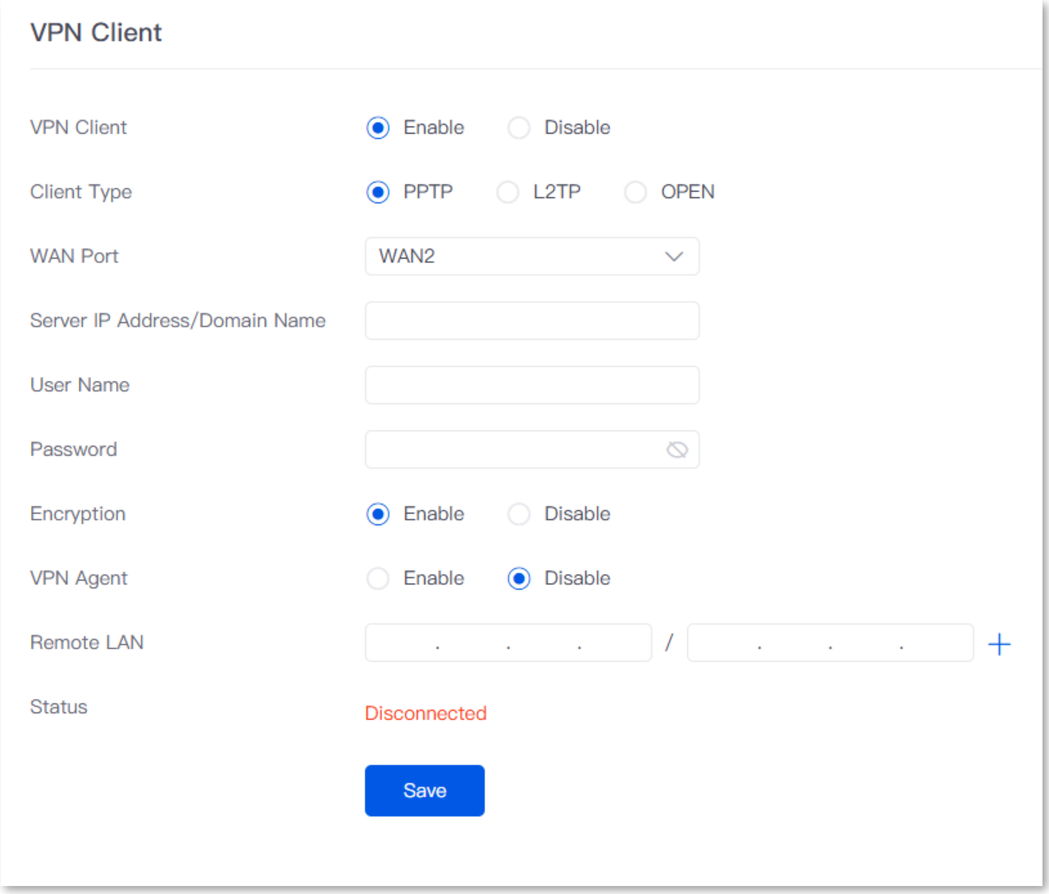
User List

□	VPN Type	User Name	Client Type	User Group	Access IP Address	Assigned IP Address	Remark	Online Status ↓	Operation
No Data									

Configure PPTP/L2TP/OpenVPN client

The router works as a PPTP, L2TP or OpenVPN client and can connect to the PPTP, L2TP, or OpenVPN server.

Log in to the web UI of the router, and navigate to **More** > **VPN Client** to enter the page. Set **VPN Client** to **Enable** and configure parameters. Then click **Save**.



VPN Client

VPN Client: ● Enable ○ Disable

Client Type: ● PPTP ○ L2TP ○ OPEN

WAN Port: WAN2

Server IP Address/Domain Name:

User Name:

Password:

Encryption: ● Enable ○ Disable

VPN Agent: ○ Enable ● Disable

Remote LAN: . . . / . . . +

Status: Disconnected

Parameter description

Parameter	Description
VPN Client	Used to enable or disable the VPN client function. After this function is enabled, the router works as a VPN client.

Parameter	Description
Client Type	Specifies the VPN server type of the router, including **PPTP**, **L2TP** and **OPEN**. Both PPTP and L2TP are Layer 2 VPN tunneling protocols, use Point-to-Point Protocol (PPP) for data encapsulation, and add additional headers to the data. – **PPTP**: Select **PPTP** when the VPN server is a PPTP server. – **L2TP**: Select **L2TP** when the VPN server is a L2TP server. – **OPEN**: Select **OPEN** when the VPN server is an OpenVPN server.
WAN Port	Specifies the WAN port of the PPTP or L2TP client for setting up a connection with the PPTP or L2TP server.
Server IP Address/Domain Name	Specifies the IP address or domain name of the VPN server. Generally, it is the IP address or domain name of the WAN port with the PPTP/L2TP server function enabled on the peer VPN router.
User Name	Specify the user name and password assigned by the VPN server to the VPN client.
Password	
Encryption	Specifies whether to enable 128-bit data encryption. The value of this parameter must be consistent with that of the server. Otherwise, the client is unable to communicate with the server. Only PPTP VPNs support this parameter.
Pre-shared Key	Used when the client type is L2TP and encryption is enabled. The configuration must be consistent with that of the peer server.
IKE Policy	
Transform Set	
Exchange Mode	
Local ID Type	
VPN Agent	With this function enabled, clients in the LAN can obtain IP addresses from the VPN server to access the internet.
Remote LAN	Specifies the network segment and subnet mask of the LAN of the PPTP or L2TP server.
Client Config	Used when the client type is OPEN. – **File Import**: Import the configuration file sent by the OpenVPN server, and all parameters will be automatically filled in. – **Web Setup**: Manually configure all parameters.
Server Mode	The authentication mode must be consistent with that of the peer OpenVPN server.
Client Config	When **File Import** is selected for **Client Config**, import the configuration file of the peer OpenVPN server.

9.4.3 Example of configuring a PPTP/L2TP VPN

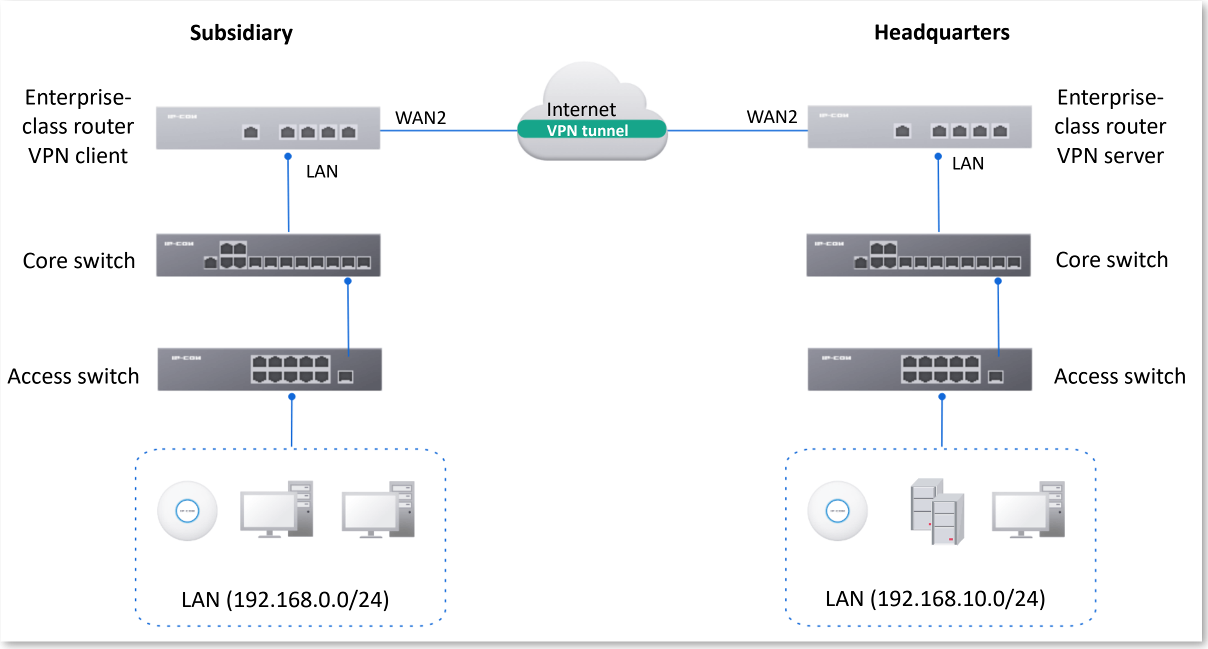
Networking requirements

The headquarters and subsidiary used enterprise-class routers to set up a network and successfully access the internet. The subsidiary staff need to access intranet resources through the internet, such as internal documents, office OA, ERP system, CRM system, and project management system.

Solution

Configure the enterprise-class router of the headquarters as the VPN server and the enterprise-class router of the subsidiary as the VPN client to enable remote users to securely access the intranet through the internet. PPTP VPN is taken for example here and the configuration of L2TP VPN is similar.

Assume that the WAN2 IP address of the headquarters' enterprise-class router is 202.105.11.22.



Configuration procedure

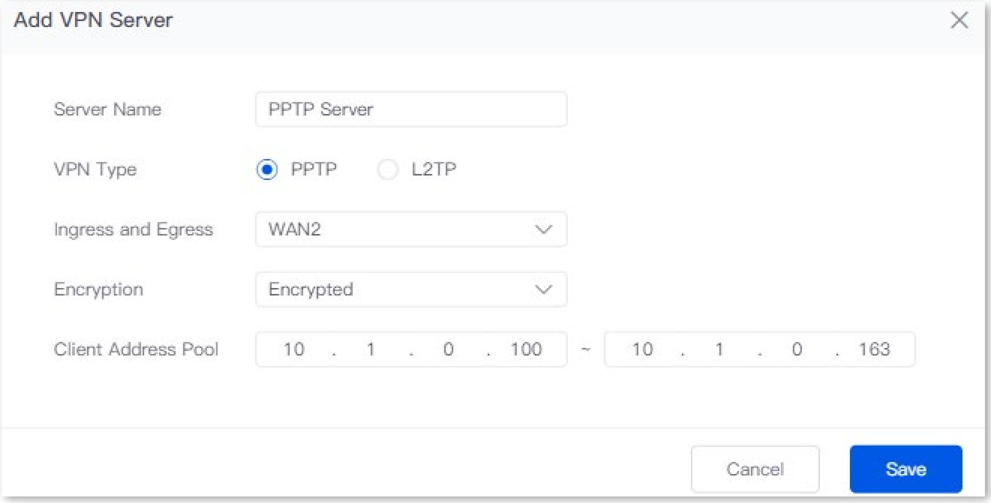
Configure a router as the VPN server → Configure the other router as the VPN client

I. Configure the enterprise-class router of the headquarters as the VPN server

1. Log in to the web UI of the router.
2. Configure the PPTP server.

Server Name	VPN Type	Ingress and Egress	Encryption	Client Address Pool
PPTP Server	PPTP	WAN2	Encrypted	10.1.0.100-10.1.0.163

Navigate to **More** > **VPN Service** > **VPN Server**, click **Add** to configure parameters of the PPTP server, and click **Save**.



Server Name: PPTP Server

VPN Type: ● PPTP ○ L2TP

Ingress and Egress: WAN2

Encryption: Encrypted

Client Address Pool: 10 . 1 . 0 . 100 ~ 10 . 1 . 0 . 163

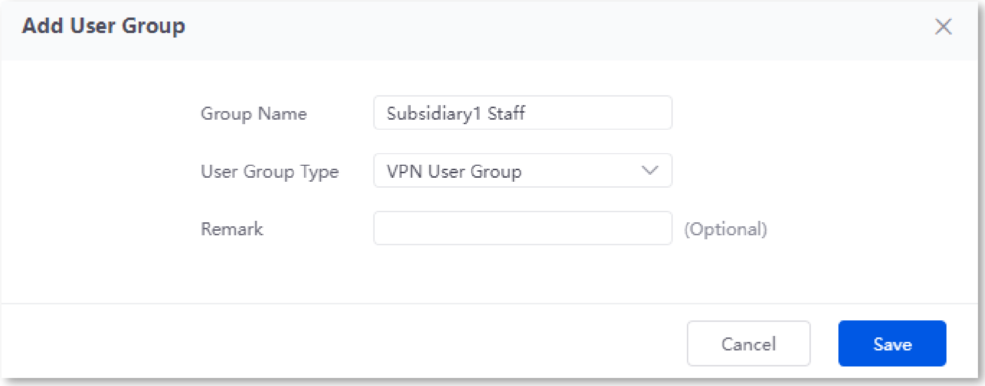
3. Configure the PPTP user.

The following table provides the examples of PPTP user parameters.

VPN Type	User Name	Password	User Group	Client Type	Client Subnet
PPTP	Subsidiary1	Subsidiary1	Subsidiary1 Staff	Network Device	192.168.0.0/24

1) Configure VPN user groups.

Navigate to **Audit** > **Group Policy** > **User Group**, click **Add** to configure VPN user groups for the subsidiary, and click **Save**.



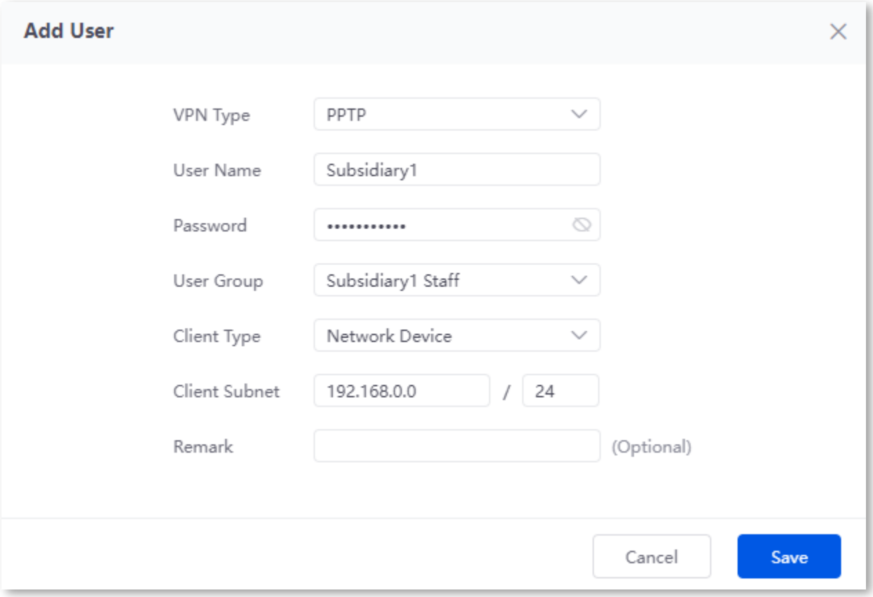
Group Name: Subsidiary1 Staff

User Group Type: VPN User Group

Remark: (Optional)

2) Configure the PPTP user.

Navigate to **More** > **VPN Service** > **User Management**, click **Add** to configure the relevant parameters of the PPTP user, and click **Save**.



Add User

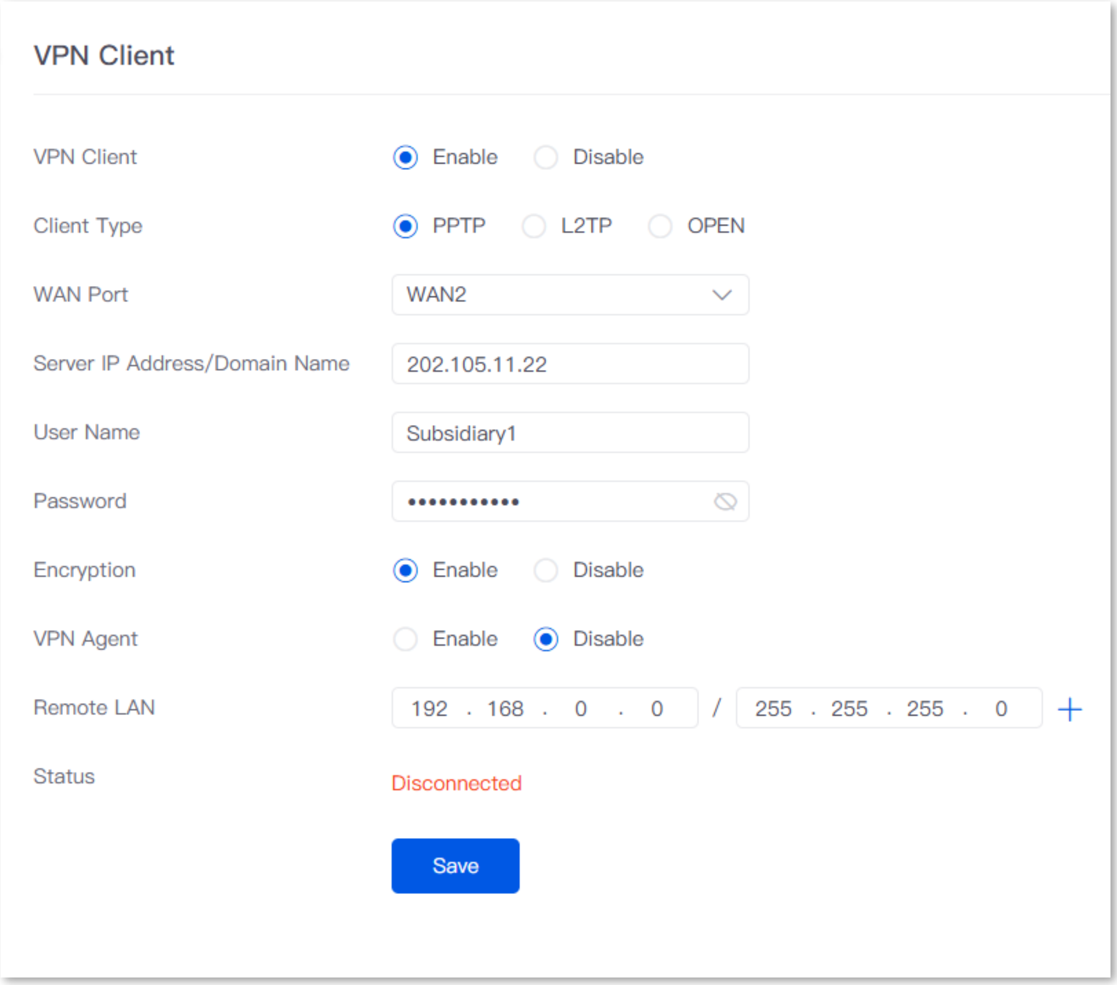
VPN Type	PPTP
User Name	Subsidiary1
Password	•••••••••••
User Group	Subsidiary1 Staff
Client Type	Network Device
Client Subnet	192.168.0.0 / 24
Remark	(Optional)

II. Configure the enterprise-class router of the subsidiary as the VPN client

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

2. Configure the PPTP client.

   1) Navigate to **More** > **VPN Client**, and enable the **VPN Client** function.
   2) Set **Client Type** to be consistent with the VPN server, which is **PPTP** in this example.
   3) Set **WAN** Port, which is **WAN2** in this example.
   4) Set **Server IP Address/Domain Name**, which is **202.105.11.22** in this example.
   5) Set **User Name and Password**, which both are **Subsidiary1** in this example.
   6) Enable the **Encryption** function.
   7) Set **Remote LAN**, which is **192.168.0.0/255 255.255.0** in this example.
   8) Click **Save**.



VPN Client

VPN Client	● Enable ○ Disable
Client Type	● PPTP ○ L2TP ○ OPEN
WAN Port	WAN2
Server IP Address/Domain Name	202.105.11.22
User Name	Subsidiary1
Password	•••••••••••
Encryption	● Enable ○ Disable
VPN Agent	○ Enable ● Disable
Remote LAN	192 . 168 . 0 . 0 / 255 . 255 . 255 . 0 +
Status	Disconnected

---End

When **Connected** is shown under **Status**, the VPN connection is successful.

Staff in the subsidiary and headquarters can securely access each other's LAN resources through the internet.

Verification

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

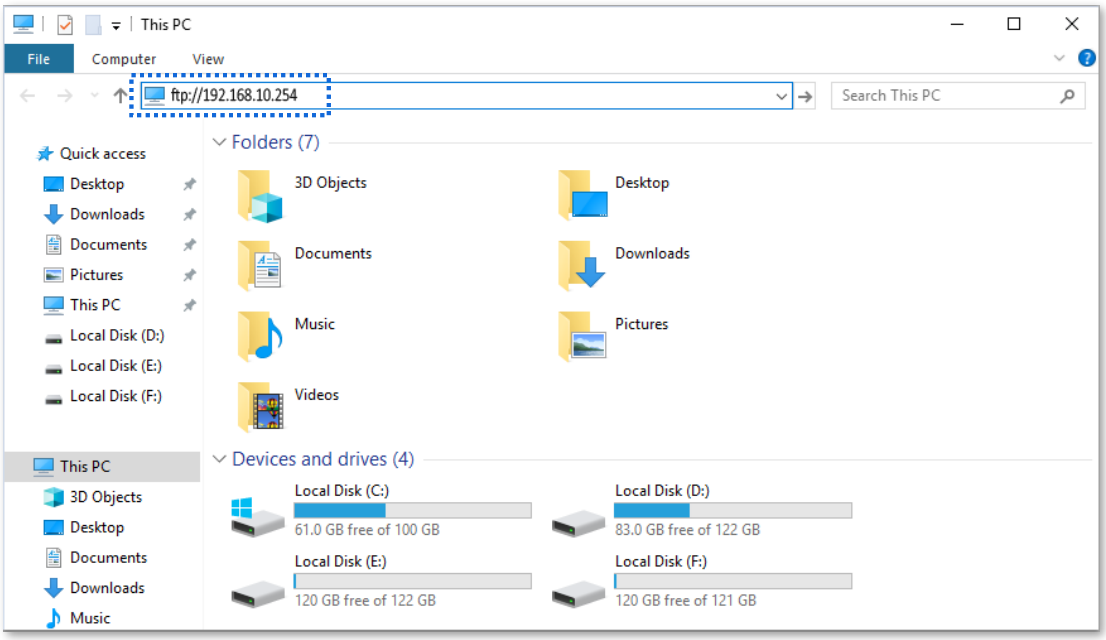
- FTP server IP address: 192.168.10.254
- FTP service port: 21
- Login user name/password: Tom123/Tom123

When the subsidiary staff access the headquarters project materials, perform the following procedure:

1. Enter **ftp://server IP address** in a browser or **This PC**, which is **ftp://192.168.10.254** in this example.

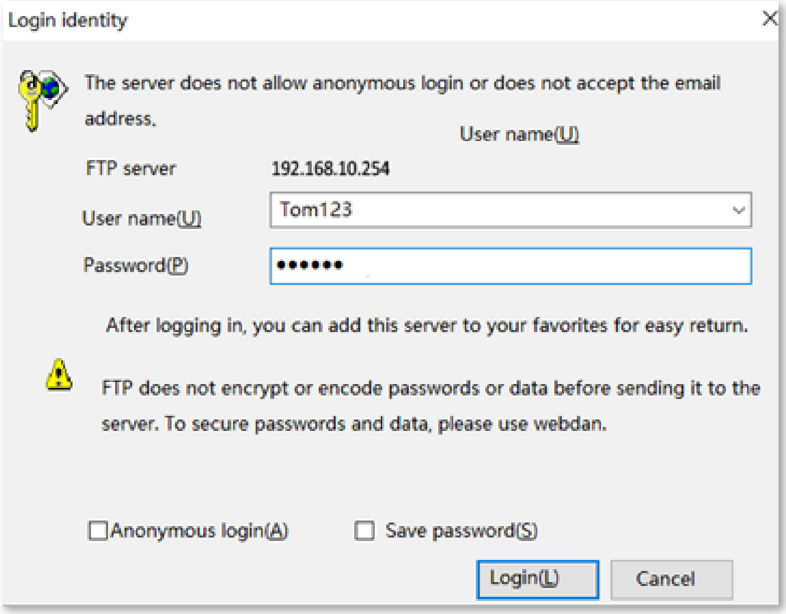
Tip

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



ftp://192.168.10.254

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



Login identity

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

User name(U)

FTP server 192.168.10.254

User name(U) Tom123

Password(P) ••••••

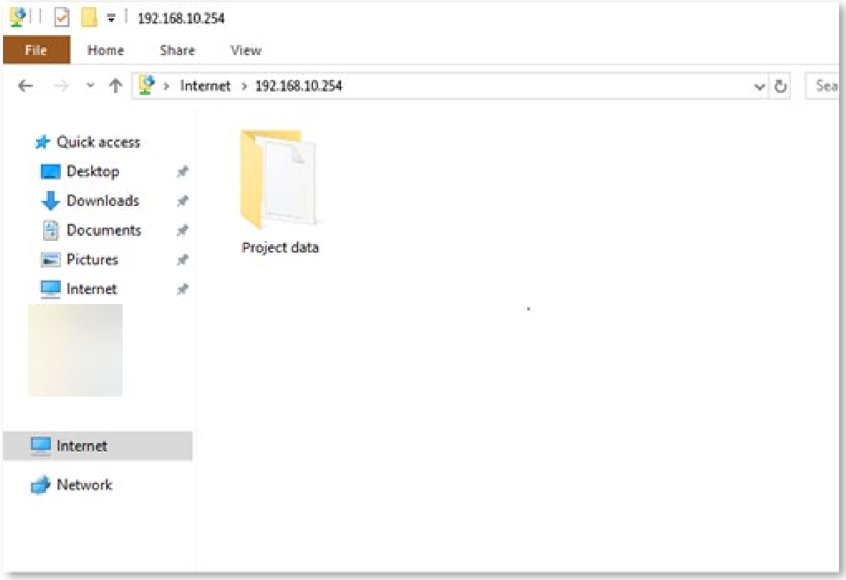
After logging in, you can add this server to your favorites for easy return.

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

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

---End

Access is successful. See the following figure.



9.4.4 Example of configuring an L2TP over IPSec VPN

Networking requirements

An enterprise uses the enterprise router to set up a network and successfully access the internet. The staff on business trip need to access internal resources through the internet, such as internal documents, office OA, ERP system, CRM system, project management system and so on.

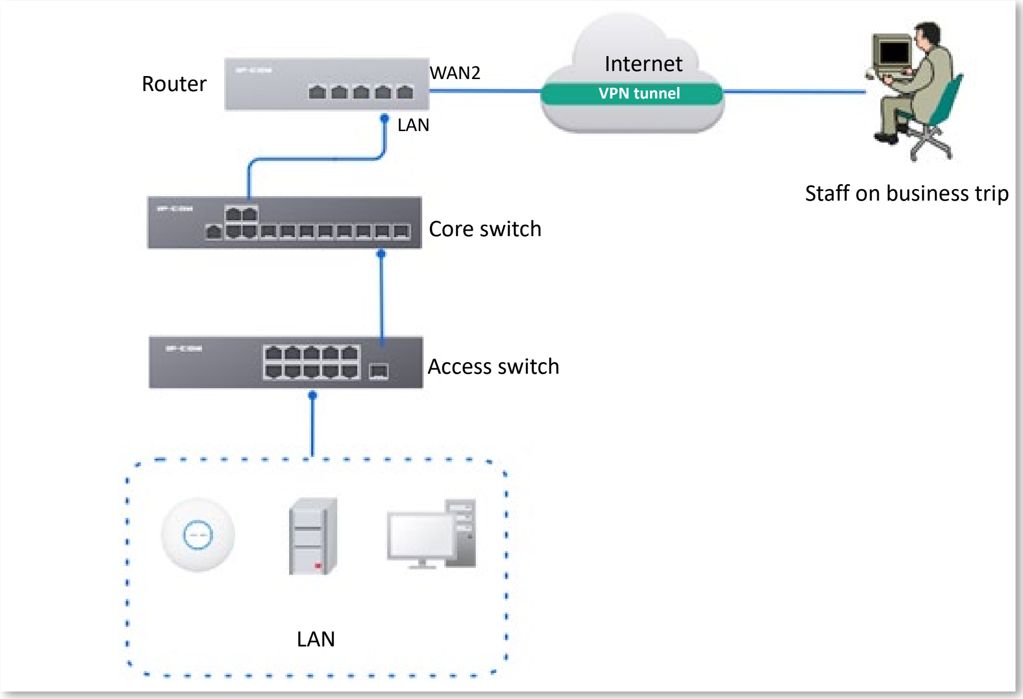
Solution

Configure an L2TP server on the router, and enable IPSec to encrypt data packets, so that remote users can securely access the intranet through the internet.

Assume that the basic information of the L2TP server is as follows:

- The user name and password assigned by the L2TP server are both **Tom123**.
- The L2TP server IP address is **202.105.11.22**.
- L2TP server enables encryption of data.
- The intranet of the L2TP server is **192.168.10.0/24**.
- The port through which the L2TP server establishes the VPN tunnel is **WAN2**.

Assume that when the L2TP server establishes a connection with the L2TP client, the pre-shared key used to authenticate the identity is **JohnDoe123**.



Configuration procedure

Configure the L2TP server → Configure the L2TP user

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

2. Configure the L2TP server.

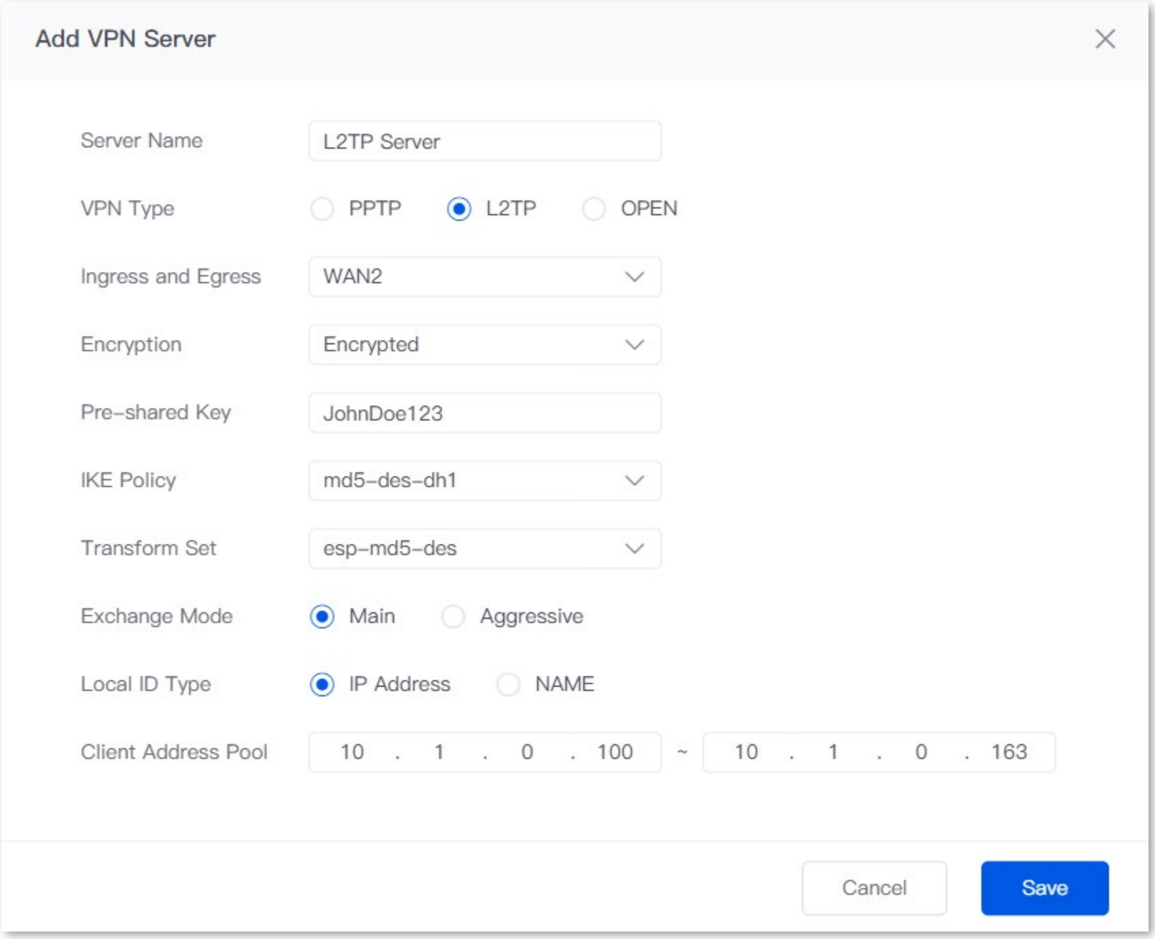
   The L2TP server parameters shown below are examples only.

Server Name	VPN Type	Ingress and Egress	Encryption	Pre-shared Key	Client Address Pool
L2TP Server	L2TP	WAN2	Encrypted	JohnDoe123	10.1.0.100–10.1.0.163

   Navigate to **More** > **VPN Service** > **VPN Server**. Click **Add** to configure L2TP server parameters, and click **Save**.

   Tip

   The **Encryption** is set to **Encrypted**, which means the L2TP server uses the IPSec to encrypt.



Add VPN Server

Server Name: L2TP Server

VPN Type: ○ PPTP ● L2TP ○ OPEN

Ingress and Egress: WAN2

Encryption: Encrypted

Pre-shared Key: JohnDoe123

IKE Policy: md5-des-dh1

Transform Set: esp-md5-des

Exchange Mode: ● Main ○ Aggressive

Local ID Type: ● IP Address ○ NAME

Client Address Pool: 10 . 1 . 0 . 100 ~ 10 . 1 . 0 . 163

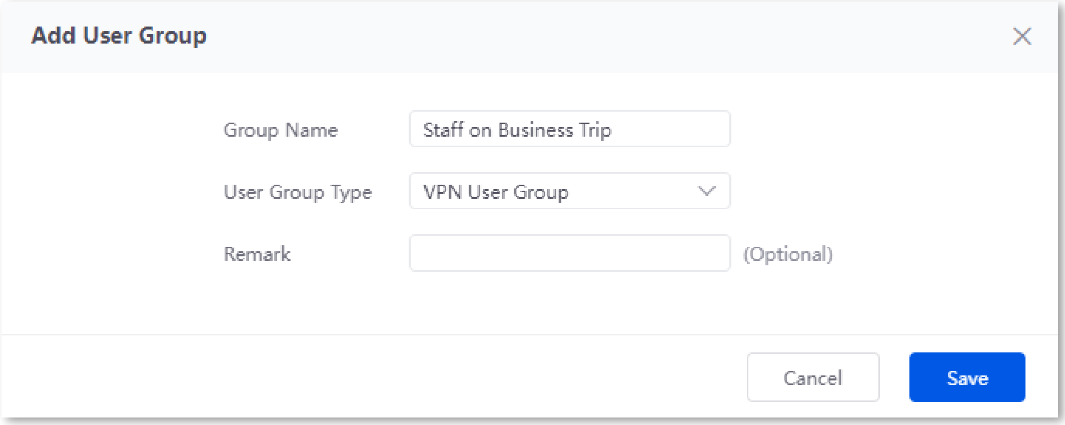
3. Configure the L2TP user.

The L2TP user parameters shown below are examples only.

VPN Type	User Name	Password	User Group	Client Type
L2TP	Tom123	Tom123	Staff on Business Trip	Terminal

1) Configure VPN user group.

Navigate to **Audit** > **Group Policy** > **User Group**, click **Add** to configure VPN user group for VPN client, and click **Save**.



Add User Group

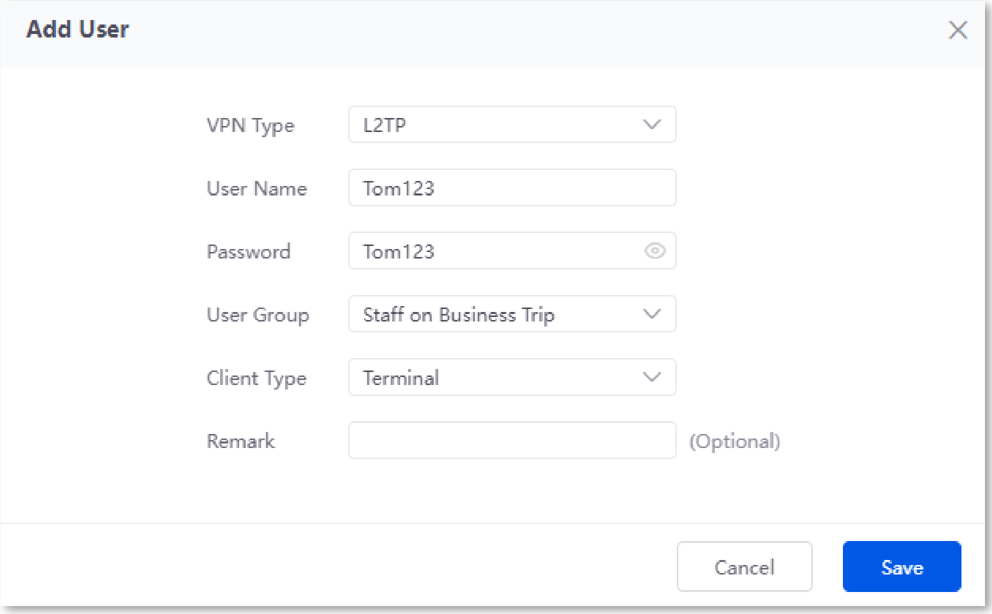
Group Name: Staff on Business Trip

User Group Type: VPN User Group

Remark: (Optional)

2) Configure the L2TP user.

Navigate to **More** > **VPN Service** > **User Management**. Click **Add** to configure the relevant parameters of the L2TP user, and click **Save**.



Add User

VPN Type	L2TP
User Name	Tom123
Password	Tom123
User Group	Staff on Business Trip
Client Type	Terminal
Remark	(Optional)

---End

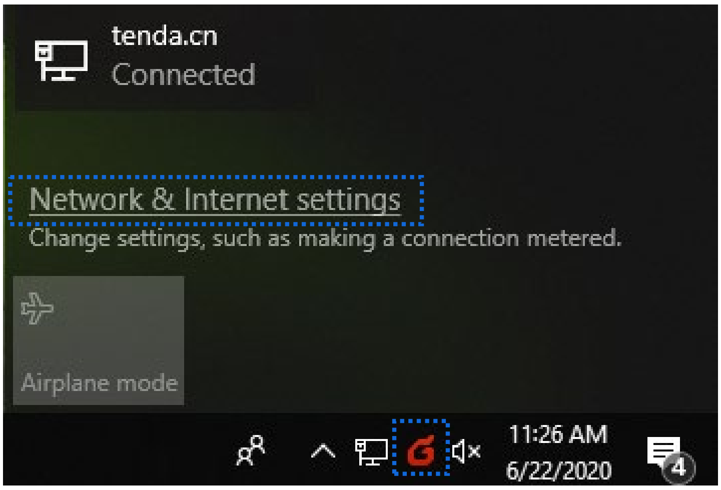
Verification

Staff on business trip use VPN dial-up to access headquarters resources.

Scenario 1: Staff on business trip access headquarters resources on a computer (Example: Windows 10).

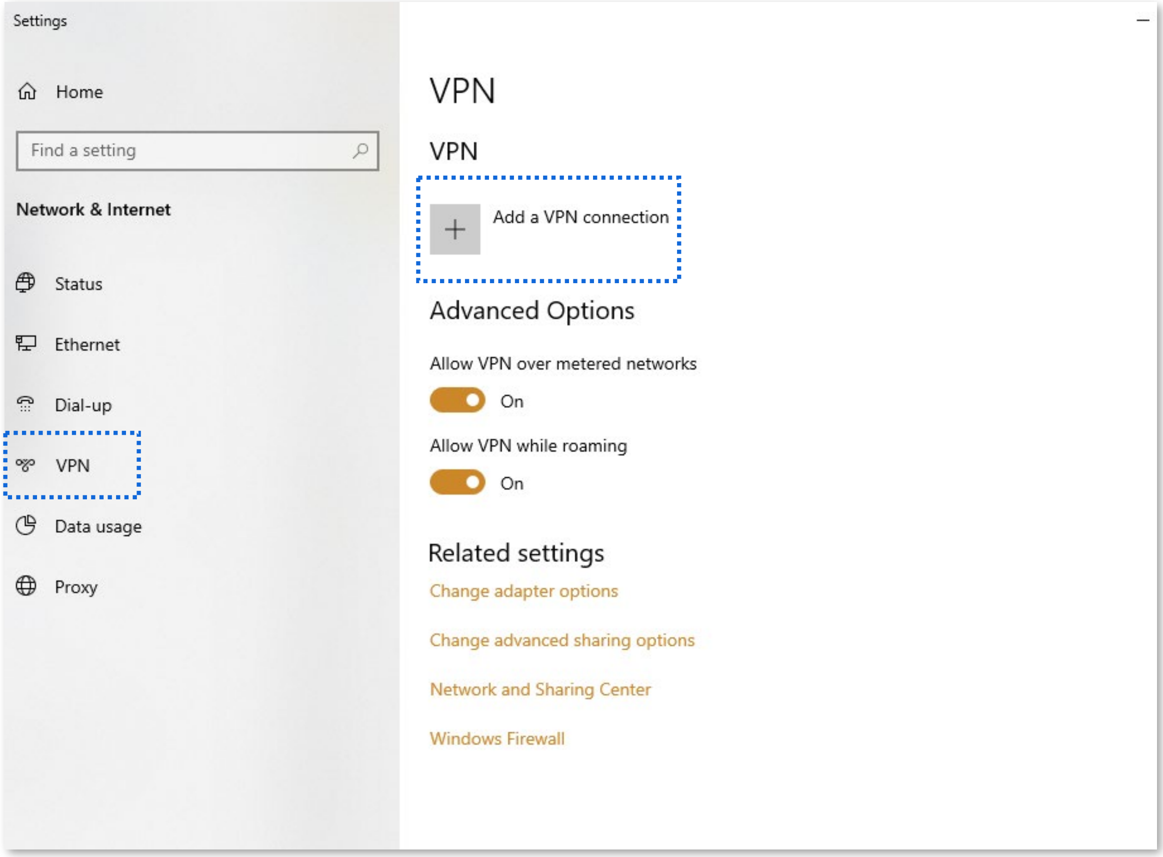
I. Staff creating VPN connection on business trip

1. Click 🖳 in the lower right corner of the desktop, click **Network & Internet settings**.



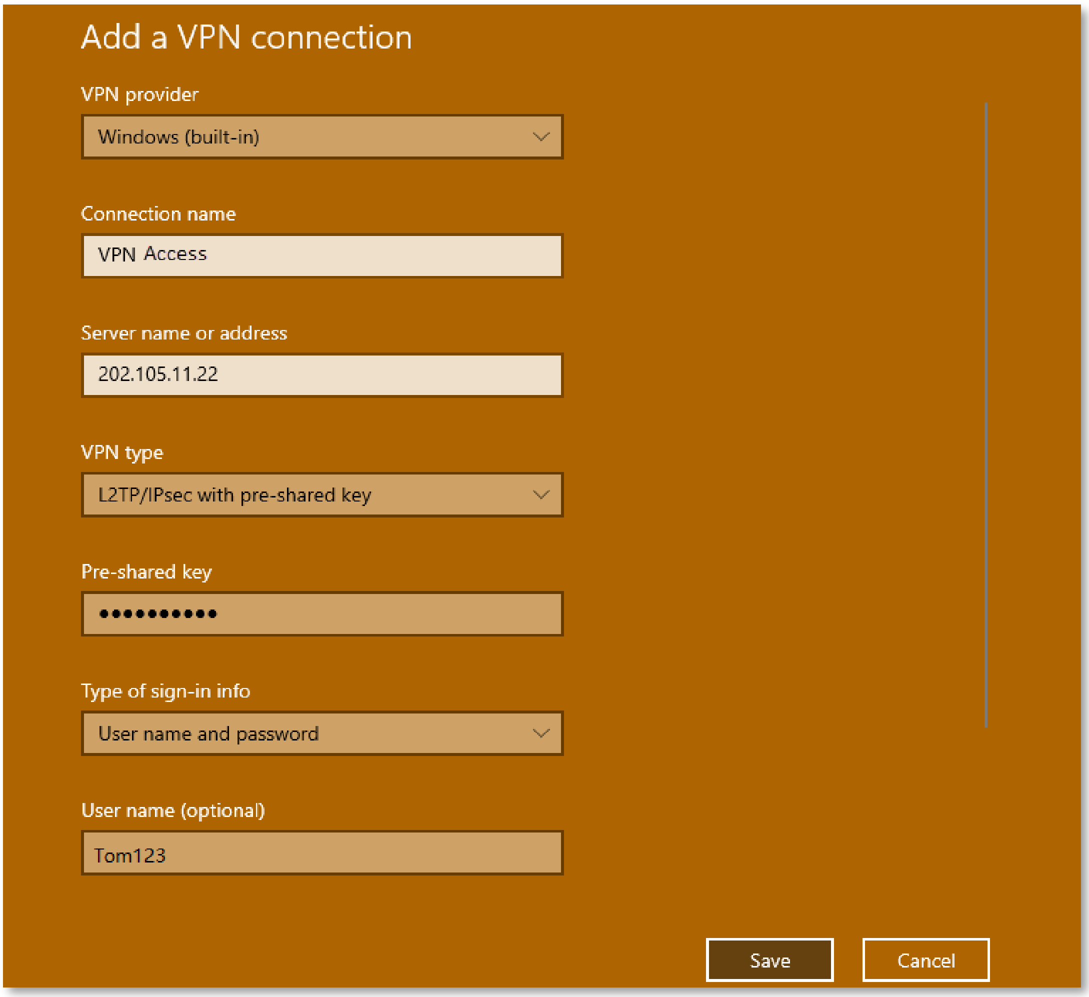
tenda.cn
Connected
Network & Internet settings
Change settings, such as making a connection metered.
Airplane mode
11:26 AM
6/22/2020
4

2. Click **VPN** and then **Add a VPN connection**.



3. Set VPN connection parameters, and then click **Save**.

   1) Select **VPN provider**, which is **Windows (built-in)** in this example.
   2) Set the **Connection name** of VPN, which is **VPN Access** in this example.
   3) Set **Server name or address**, which is **202.105.11.22** in this example.
   4) Select **VPN type**, which is **L2TP/IPsec with pre-shared key** in this example.
   5) Set **Pre-shared key** of the IPSec tunnel, which is **JohnDoe123** in this example.
   6) Pull down the scroll bar, select **Type of sign-in info**, which is **User name and password** in this example.
   7) Set **User name** and **Password**, which are both **Tom123** in this example.



Add a VPN connection

VPN provider: Windows (built-in)

Connection name: VPN Access

Server name or address: 202.105.11.22

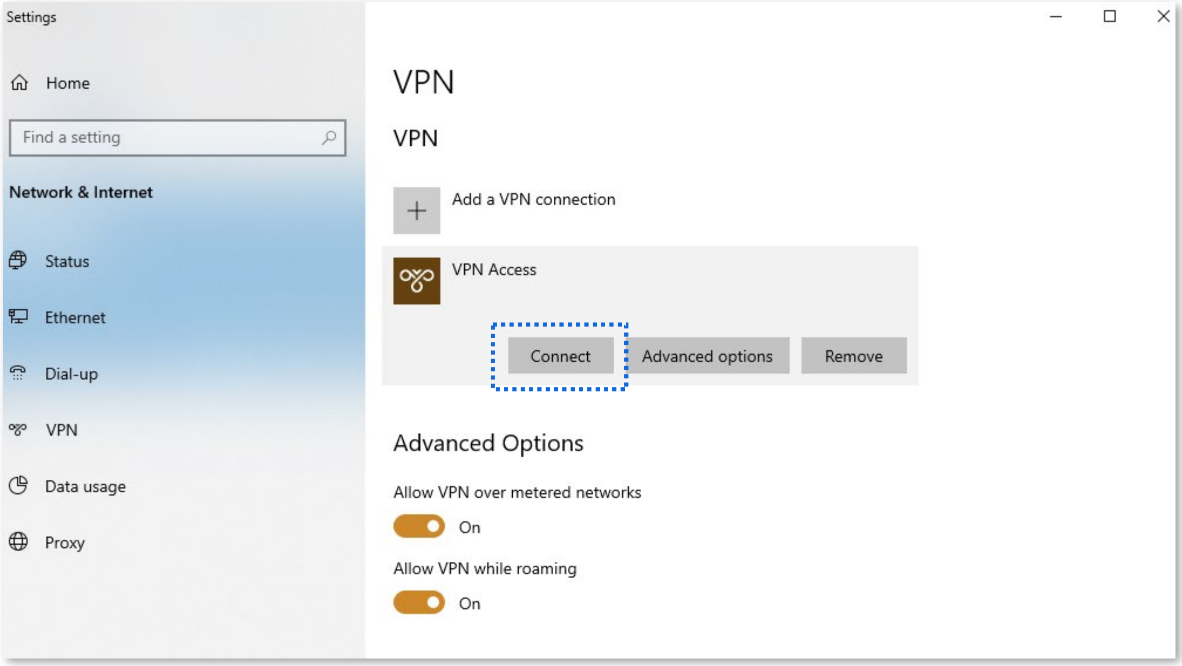
VPN type: L2TP/IPsec with pre-shared key

Pre-shared key: ●●●●●●●●●●

Type of sign-in info: User name and password

User name (optional): Tom123

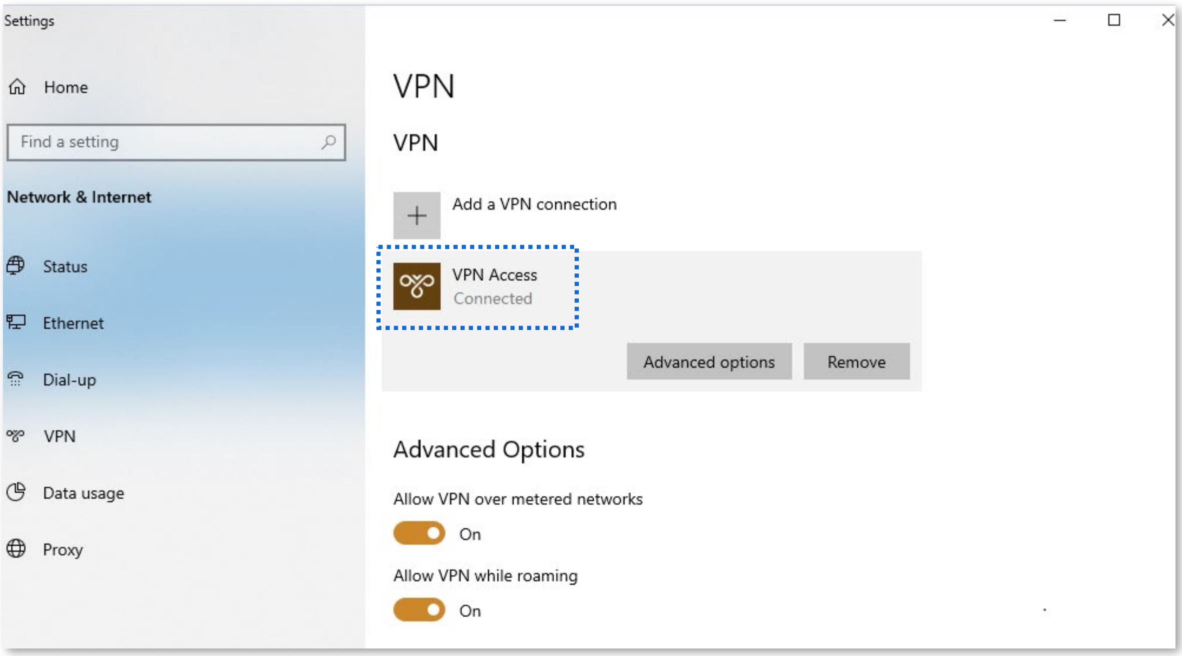
4. Click **VPN Access,** then click **Connect**.



Allow VPN over metered networks: On

Allow VPN while roaming: On

Wait until a connection is established, which can access VPN according to the account information provided by the headquarters.



II. Staff accessing headquarters resources on business trip

Assume that the staff on business trip need to access the FTP server of headquarters. The server information is as follows:

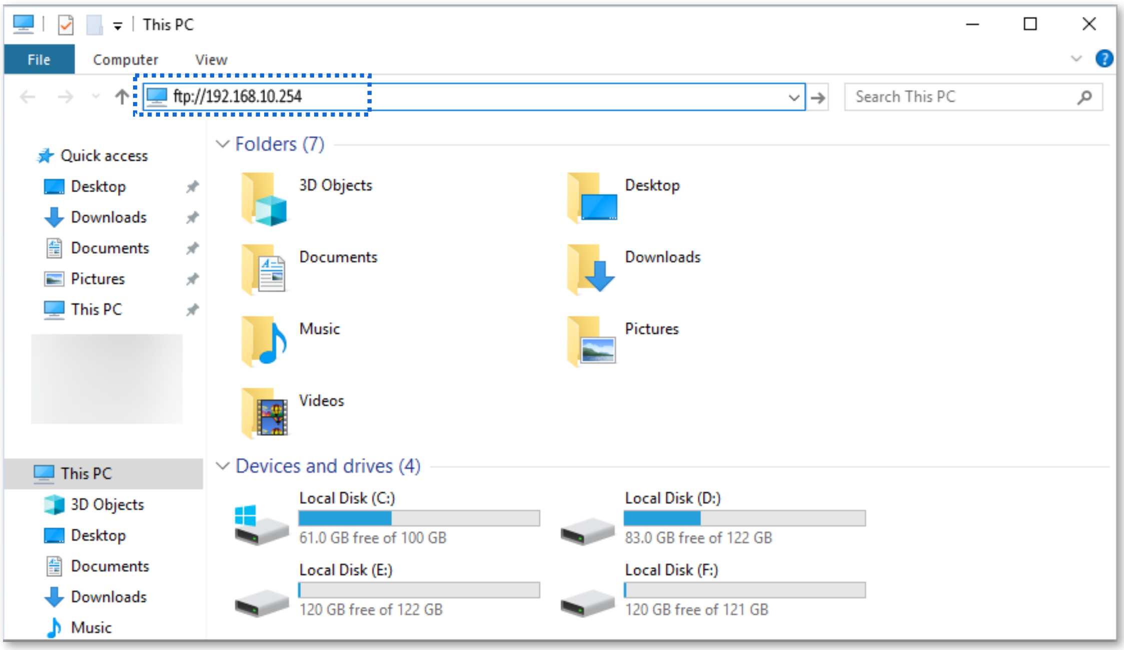
- FTP server IP address: **192.168.10.254**
- FTP service port: **21**
- Login user name/password: **Tom123/Tom123**

When the staff on business trip access the headquarters project materials, perform the following procedures:

1. Enter **ftp://server IP address** in a browser or **This PC**, which is **ftp://192.168.10.254** in this example.

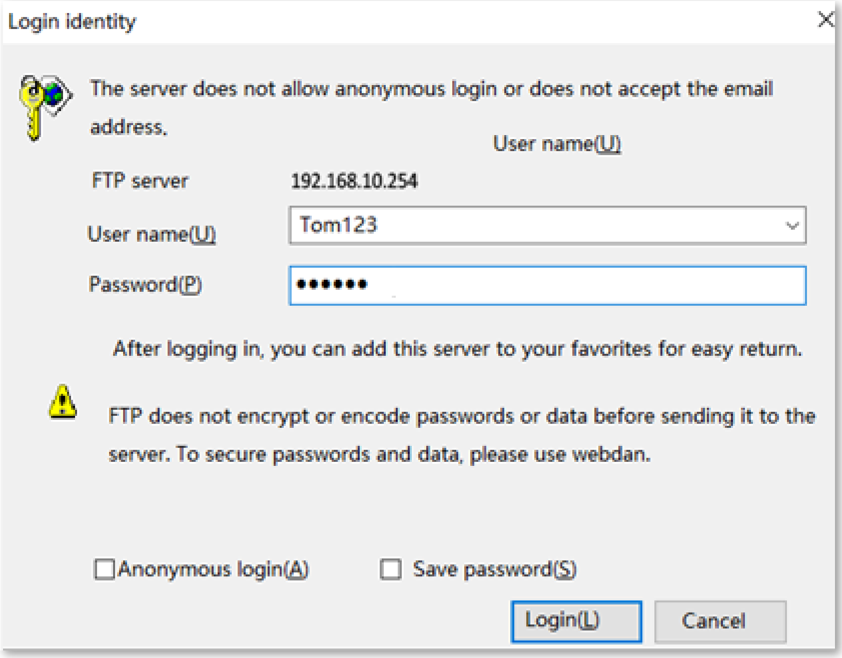
Tip

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



ftp://192.168.10.254

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



Login identity

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

User name(U)

FTP server 192.168.10.254

User name(U) Tom123

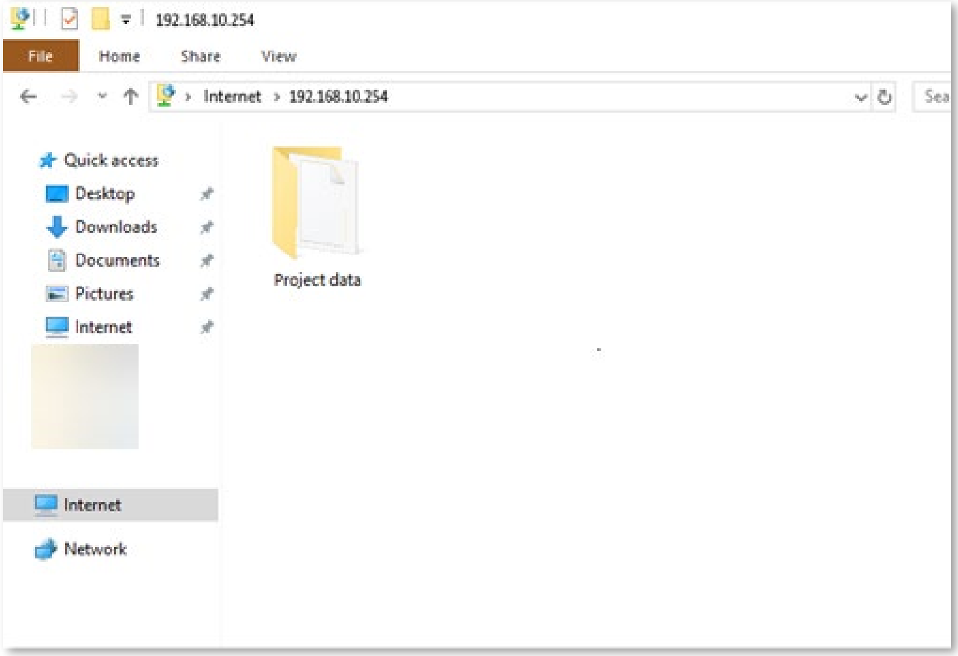
Password(P) ••••••

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

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

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

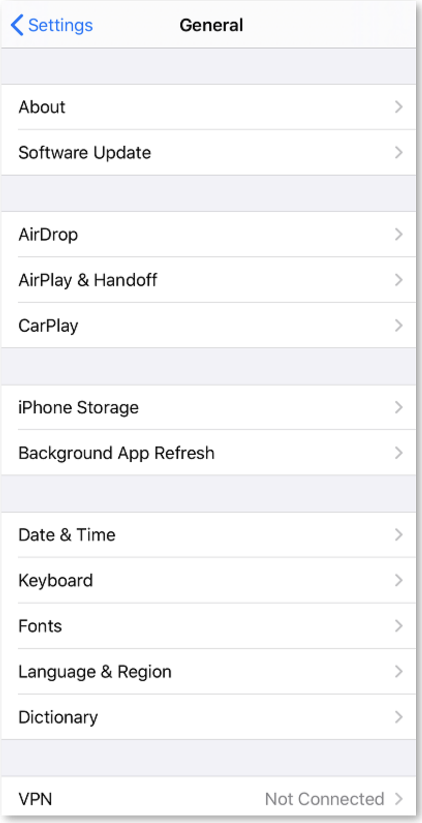
Access is successful.



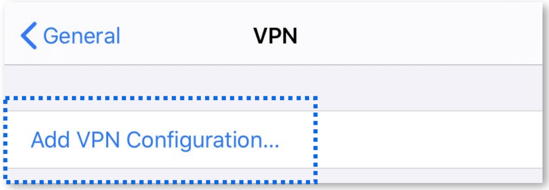
Scenario 2: Staff on business trip access headquarters resources on mobile devices (Example: iOS system)

I. Staff creating VPN connection on business trip

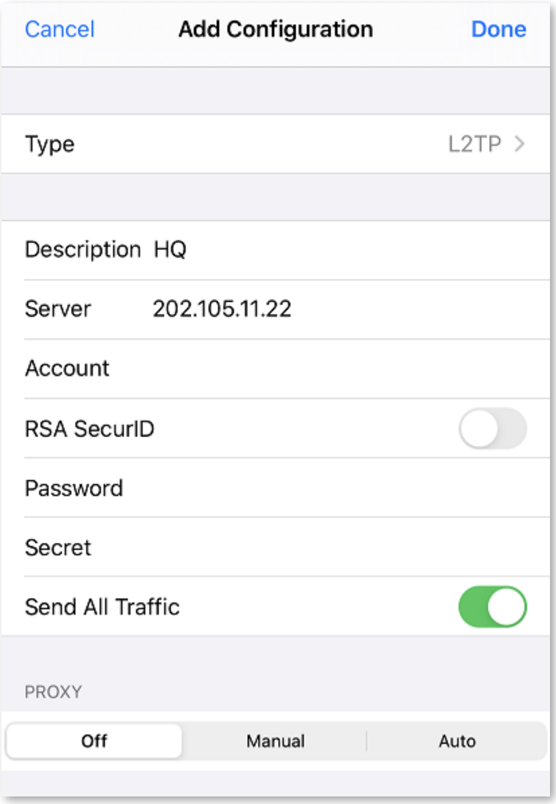
1. Click ⚙ (Settings) on your smartphone.
2. Tap **VPN.**



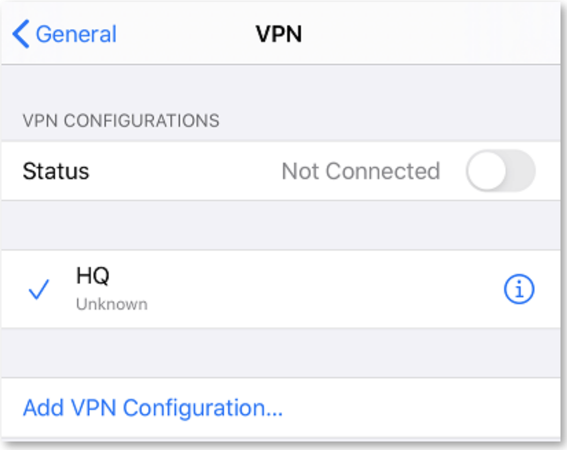
3. Tap **Add VPN Configuration...**



4. Set the VPN connection parameters.
   1) Select the **Type**, which is **L2TP** in this example.
   2) Set the name of VPN connection in **Description**, which is **HQ** in this example.
   3) Set **Server** (the IP address of L2TP server), which is **202.105.11.22** in this example.
   4) Set **Account** and **Password** of L2TP VPN, which are both **Tom123** in this example.
   5) Set **Secret** of IPSec tunnel, which is **JohnDoe123** in this example.
   6) Tap **Done**.

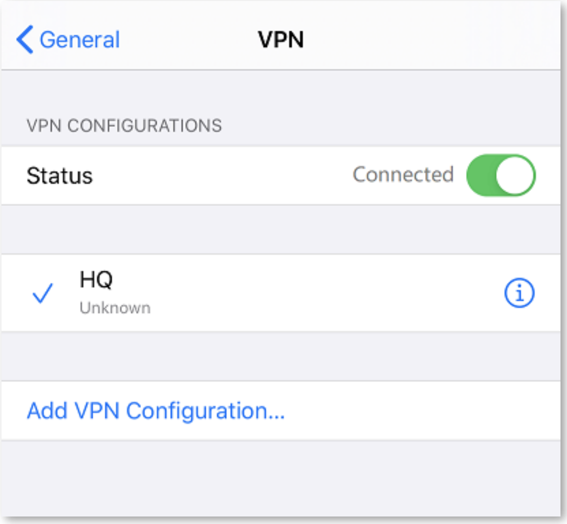

Type L2TP
Description HQ
Server 202.105.11.22
RSA SecurID ○
Send All Traffic ●
PROXY Off

5. Tap ○.



Status Not Connected

Wait until the **Status** turns to **Connected** , the IPSec connection is created successfully.



Status Connected

II. Staff accessing headquarters resources on business trip

If you want to use the mobile device (such as smartphone and tablet) to access the FTP server, you should install an FTP client on your mobile device first.

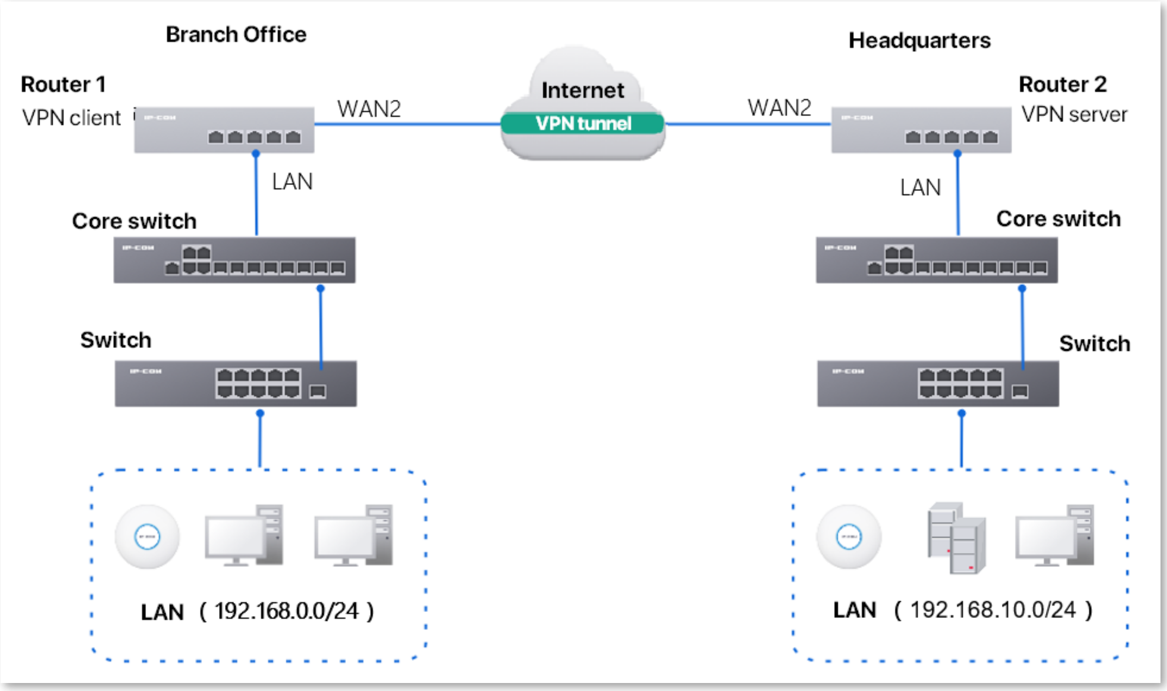
9.4.5 Example of configuring an OpenVPN as router

Networking requirements

An enterprise uses the M80-F enterprise router to set up a network and successfully access the internet. Staff in the branch office need to access internal resources through the internet, such as internal documents, office OA, ERP system, CRM system, project management system and so on.

Solution

By configuring the headquarters router as a VPN server and the branch office routers as a VPN client, remote users can securely access the company's internal LAN over the Internet. This example uses OpenVPN.



Configuration procedure

Configure headquarters router as VPN server → Configure branch office router as VPN client

I. Configure the headquarters router as VPN server

1. Log in to the web UI of the headquarters' router.
2. Set up the OpenVPN server.

   Example (leave other parameters at default settings):

   Server Name: OpenVPN

   VPN Type: OPEN

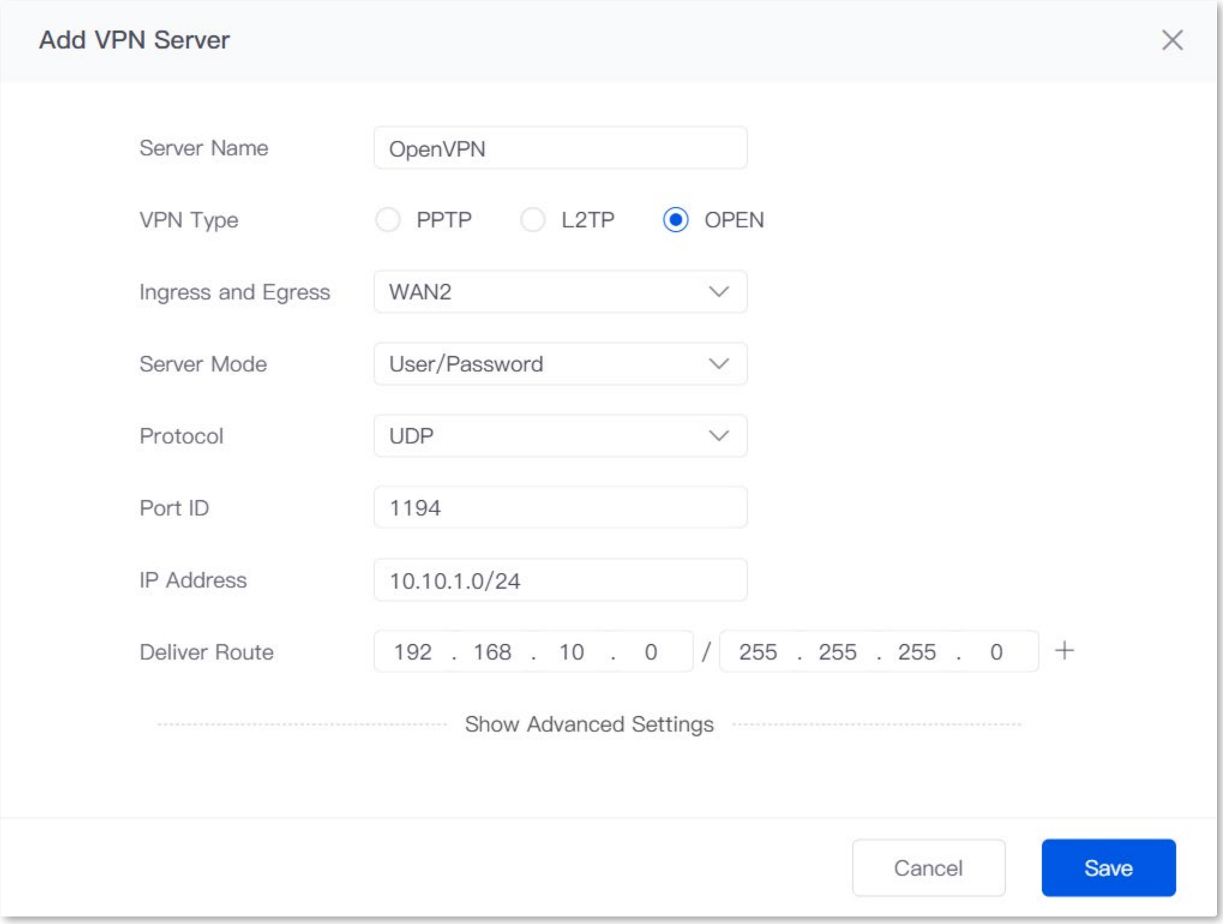
   Ingress and Egress: WAN2

   Server Mode: User/Password

   IP Address: 10.10.1.0/24

   Deliver Route: 192.168.10.0/255.255.255.0

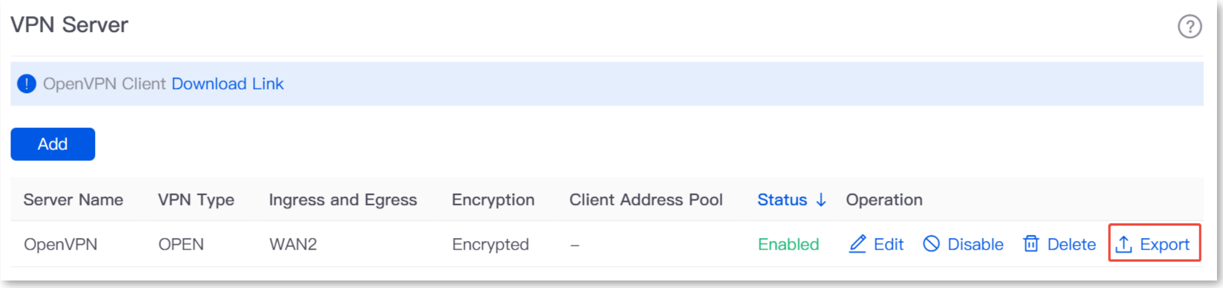
   Navigate to **More** > **VPN Service** > **VPN Server**. Click **Add**, configure parameters, and click **Save**.



Add VPN Server

Server Name	OpenVPN
VPN Type	○ PPTP ○ L2TP ● OPEN
Ingress and Egress	WAN2
Server Mode	User/Password
Protocol	UDP
Port ID	1194
IP Address	10.10.1.0/24
Deliver Route	192 . 168 . 10 . 0 / 255 . 255 . 255 . 0 +

After configuration, click Export and send the downloaded **xxxxxxxx_openvpn-client-cfg.tar** file to the OpenVPN client's management computer.



VPN Server

OpenVPN Client Download Link

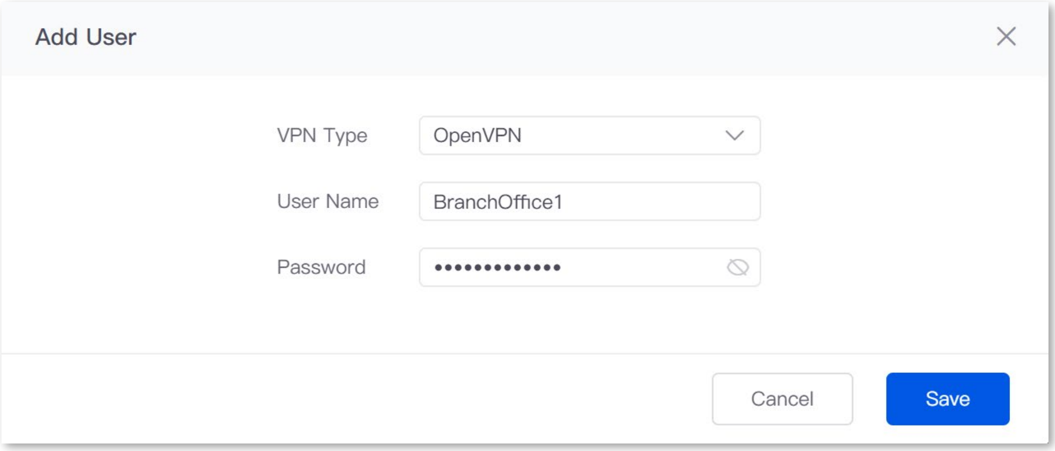
Server Name	VPN Type	Ingress and Egress	Encryption	Client Address Pool	Status ↓	Operation
OpenVPN	OPEN	WAN2	Encrypted	–	Enabled	Edit Disable Delete Export

3. Set up the OpenVPN user.

The values shown below are examples only:

VPN Type	Username	Password
OpenVPN	BranchOffice1	BranchOffice1

Navigate to **More** > **VPN Service** > **User Management**. Click **Add**, configure parameters, and click **Save**.



Add User

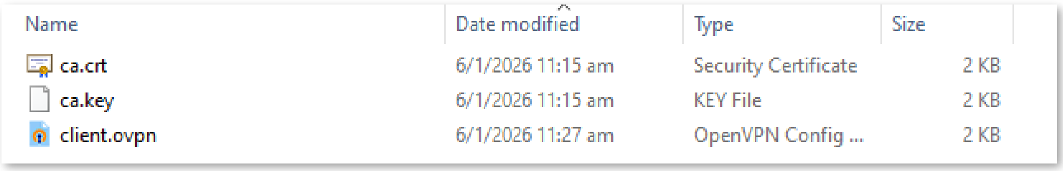
VPN Type: OpenVPN

User Name: BranchOffice1

Password: •••••••••••••

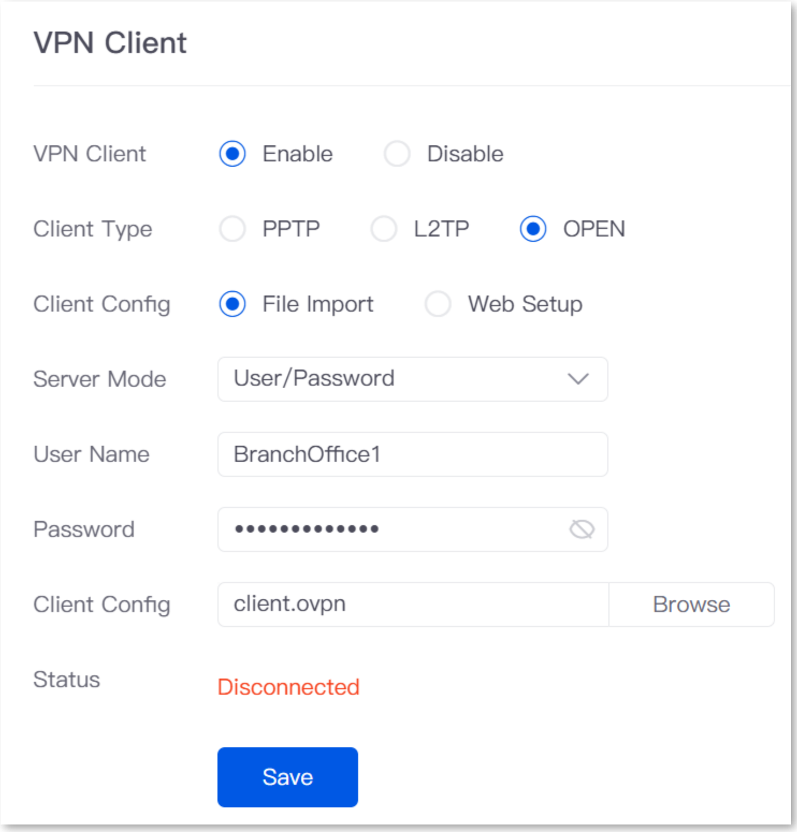
II. Configure the branch office router as VPN client

1. Download the file **xxxxxxxx_openvpn-client-cfg.tar** sent by the OpenVPN server and decompress it.



Name	Date modified	Type	Size
ca.crt	6/1/2026 11:15 am	Security Certificate	2 KB
ca.key	6/1/2026 11:15 am	KEY File	2 KB
client.ovpn	6/1/2026 11:27 am	OpenVPN Config ...	2 KB

2. Log in to the web UI of the branch office's router.
3. Set up the OpenVPN client.
   1) Enable VPN client at **More** > **VPN Client**.
   2) Select **OPEN** as the client type.
   3) Select **File Import** to configure the client.
   4) Select **User/Password** for server authentication.
   5) Enter the user name assigned by the VPN server. Example: BranchOffice1.
   6) Enter the password assigned by the VPN server. Example: BranchOffice1.
   7) Click **Browse** to import the **client.ovpn** file.
   8) Click **Save**.


VPN Client

VPN Client ● Enable ○ Disable

Client Type ○ PPTP ○ L2TP ● OPEN

Client Config ● File Import ○ Web Setup

Server Mode: User/Password

User Name: BranchOffice1

Password: •••••••••••••

Client Config: client.ovpn Browse

Status: Disconnected

---End

When "Connected" is shown under **Status**, the VPN connection is successful. Staff at both the branch office and headquarters can securely access each other's local area network resources via the internet.

Verification

Assume that a branch office is accessing the headquarters FTP server. Project materials at headquarters is stored on the FTP server. The server information is as follows:

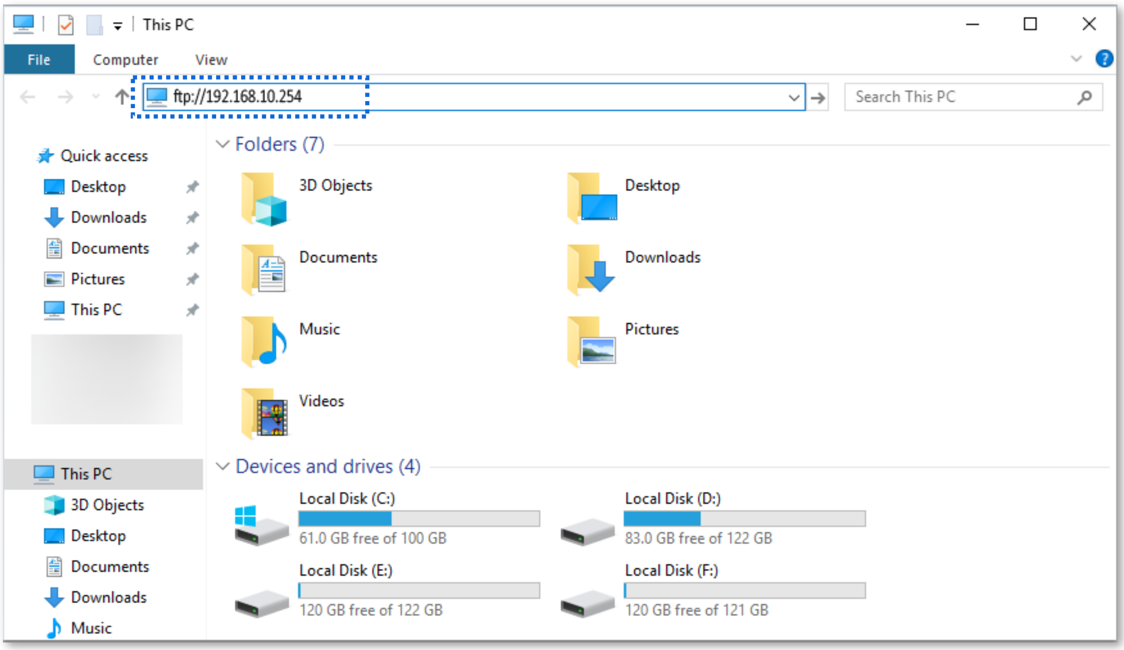
- FTP server IP address: **192.168.10.254**
- FTP service port: **21**
- Login user name/password: **Tom123/Tom123**

When a branch office employee accesses the headquarters project materials, perform the following procedures:

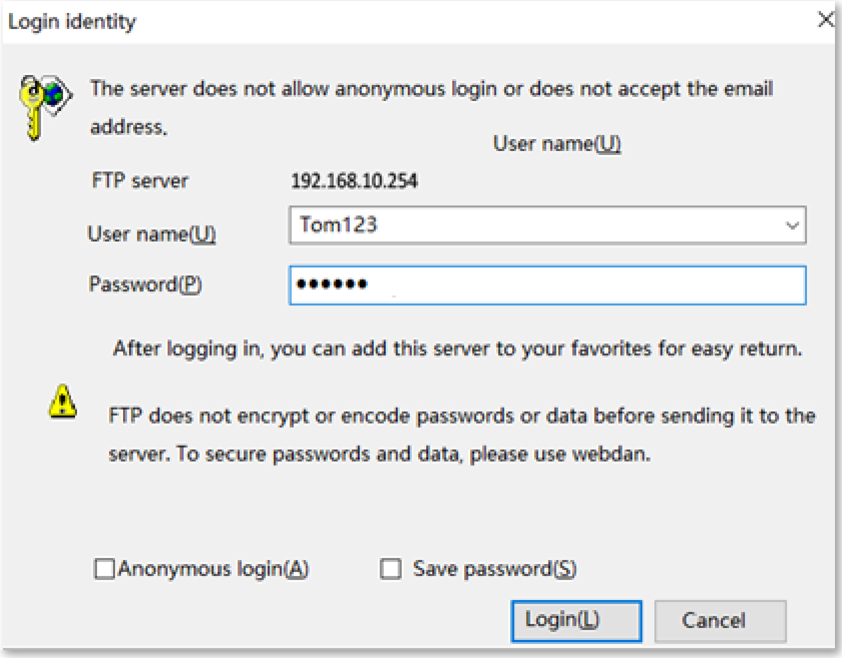
1. Enter **ftp://server IP address** in a browser or **This PC**, which is **ftp://192.168.10.254** in this example.

Tip

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


ftp://192.168.10.254

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


Login identity

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

User name(U)

FTP server 192.168.10.254

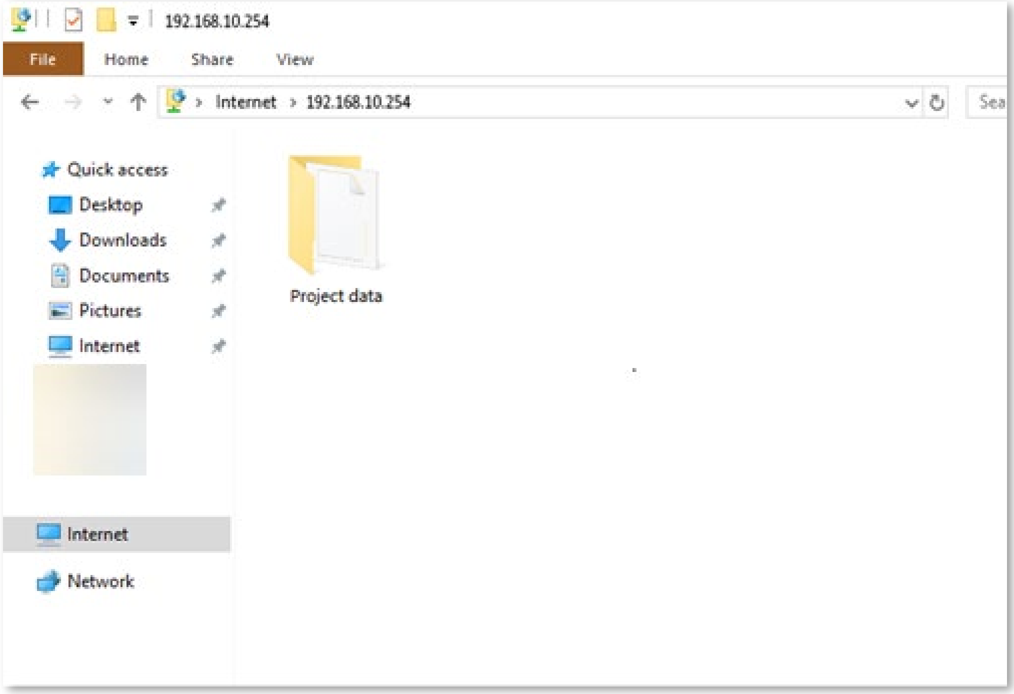
User name(U) Tom123

Password(P) ••••••

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

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

Access is successful.



9.4.6 Example of configuring an OpenVPN as terminal

Networking requirements

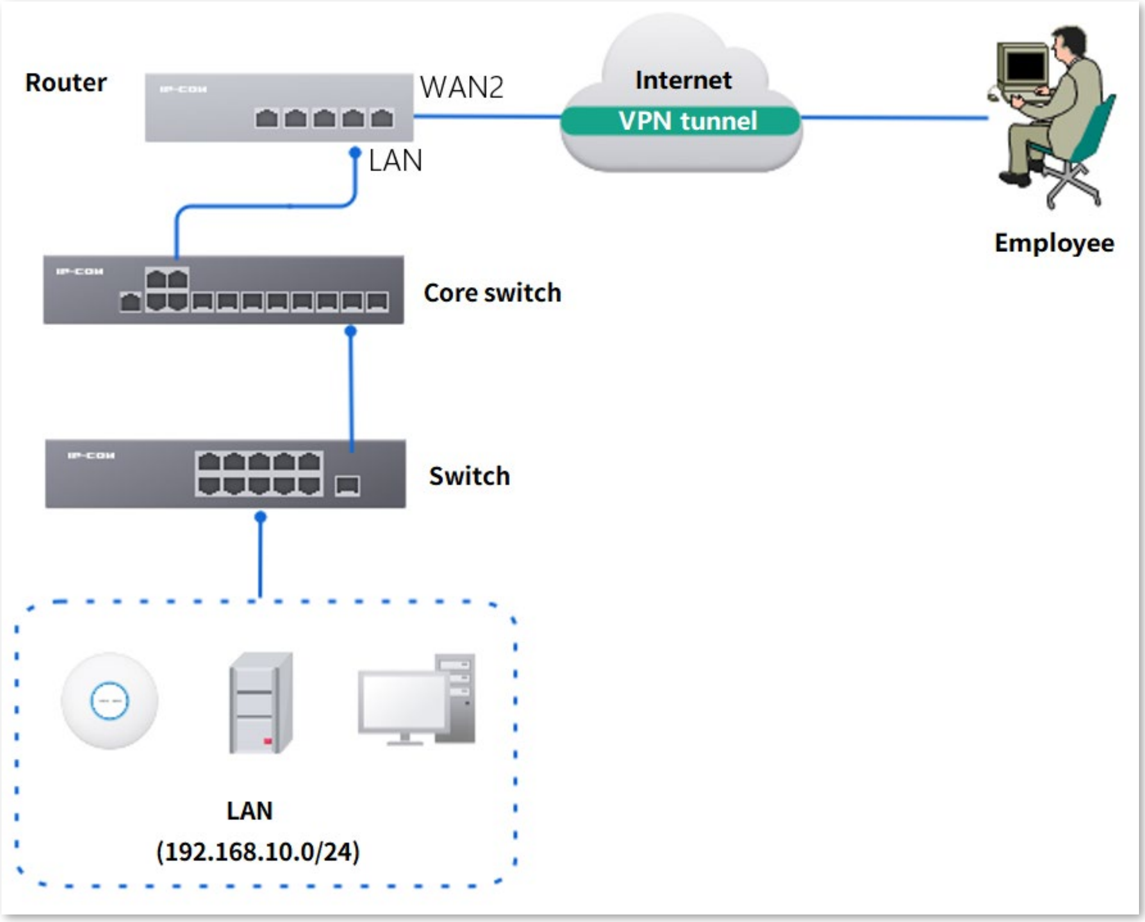
An enterprise uses the router to set up a network and successfully access the internet. Staff on a business trip need to access internal resources through the internet, such as internal documents, office OA, ERP system, CRM system, project management system and so on.

Solution

Configure an OpenVPN server on the router to enable remote users to securely access the company's internal network via the Internet.

Assume the OpenVPN server information is as follows:

- Username/Password assigned: **DavidWells**
- OpenVPN server IP address: **10.10.1.0/24**
- Route configuration to the client: **192.168.10.0/255.255.254.0**
- Interface to establish the VPN tunnel: **WAN2**



Configuration procedure

1. Log in to the web UI of the router.
2. Set up the OpenVPN server.

   Example (Leave other parameters at default settings):

   Server Name: OpenVPN

   VPN Type: OPEN

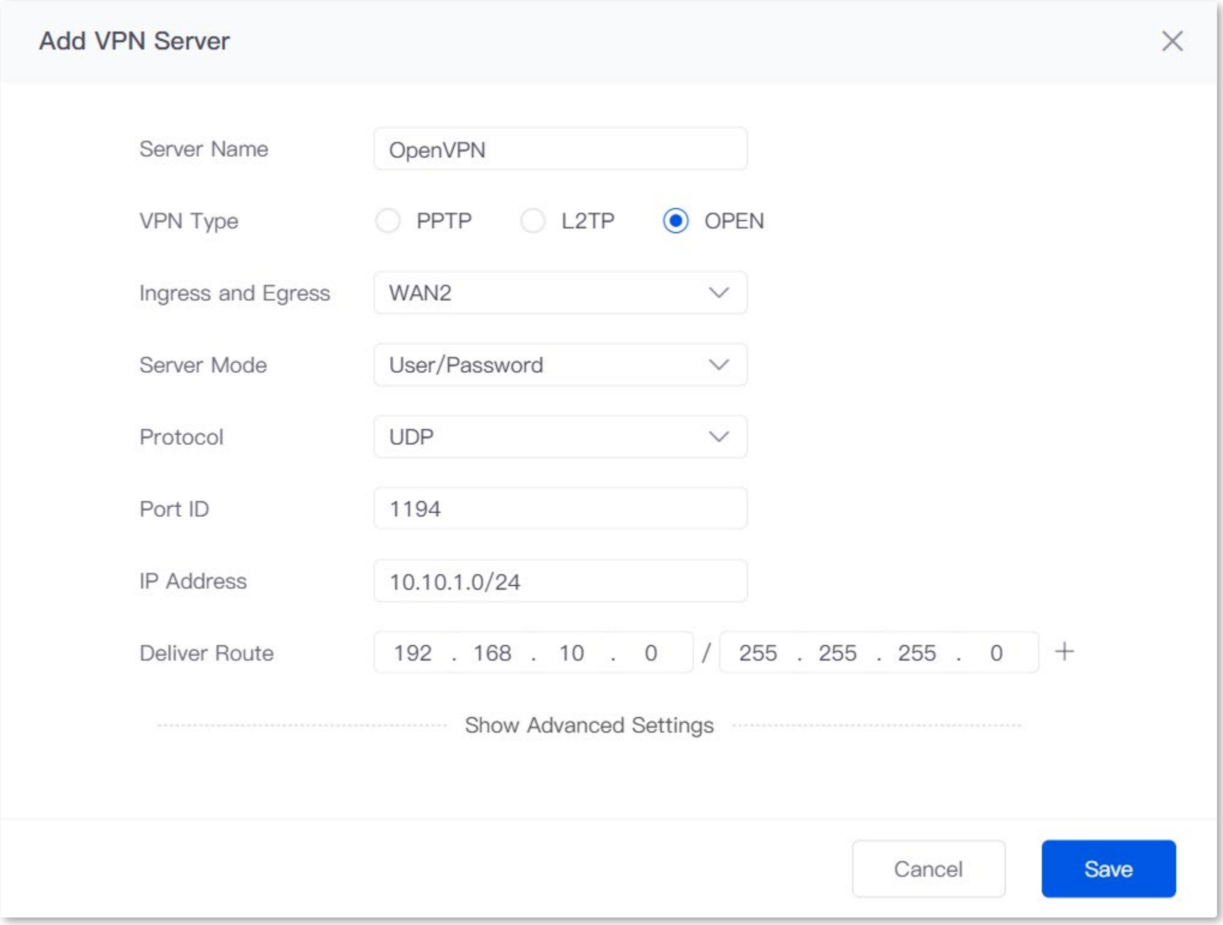
   Ingress and Egress: WAN2

   Server Mode: User/Password

   IP Address: 10.10.1.0/24

   Deliver Route: 192.168.10.0/255.255.255.0

   Navigate to **More** > **VPN Service** > **VPN Server**. Click **Add**, configure parameters, and click **Save**.



Add VPN Server

Server Name: OpenVPN

VPN Type: ○ PPTP ○ L2TP ● OPEN

Ingress and Egress: WAN2

Server Mode: User/Password

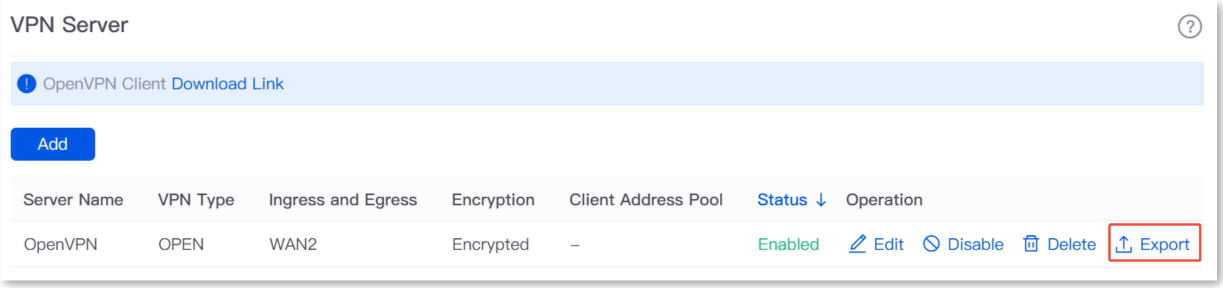
Protocol: UDP

Port ID: 1194

IP Address: 10.10.1.0/24

Deliver Route: 192 . 168 . 10 . 0 / 255 . 255 . 255 . 0

After configuration, click Export and send the downloaded **xxxxxxxx_openvpn-client-cfg.tar** file to the employee.



VPN Server

OpenVPN Client Download Link

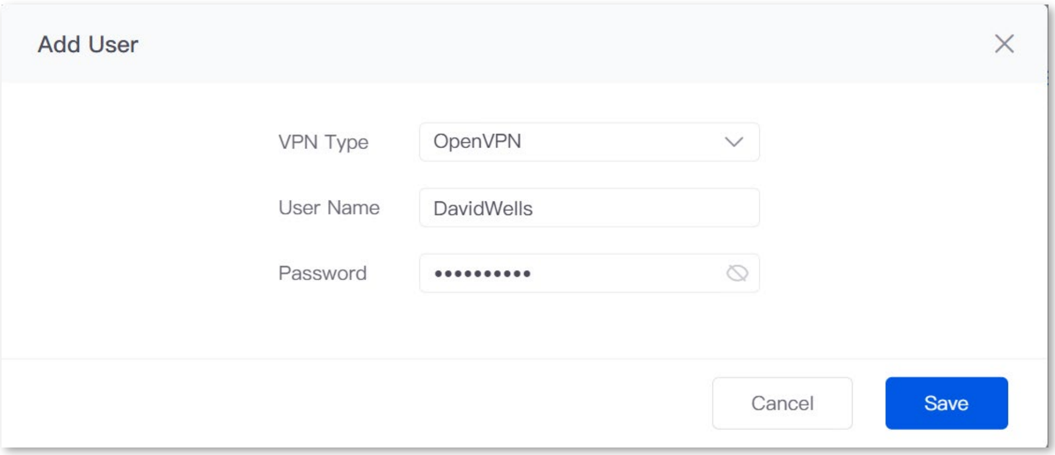
Server Name	VPN Type	Ingress and Egress	Encryption	Client Address Pool	Status ↓	Operation
OpenVPN	OPEN	WAN2	Encrypted	–	Enabled	Edit Disable Delete Export

3. Set up the OpenVPN user.

The values shown below are examples only:

VPN Type	Username	Password
OpenVPN	DavidWells	DavidWells

Navigate to **More** > **VPN Service** > **User Management**. Click **Add**, configure parameters, and click **Save**.



Add User

VPN Type: OpenVPN

User Name: DavidWells

Password: ••••••••••

---End

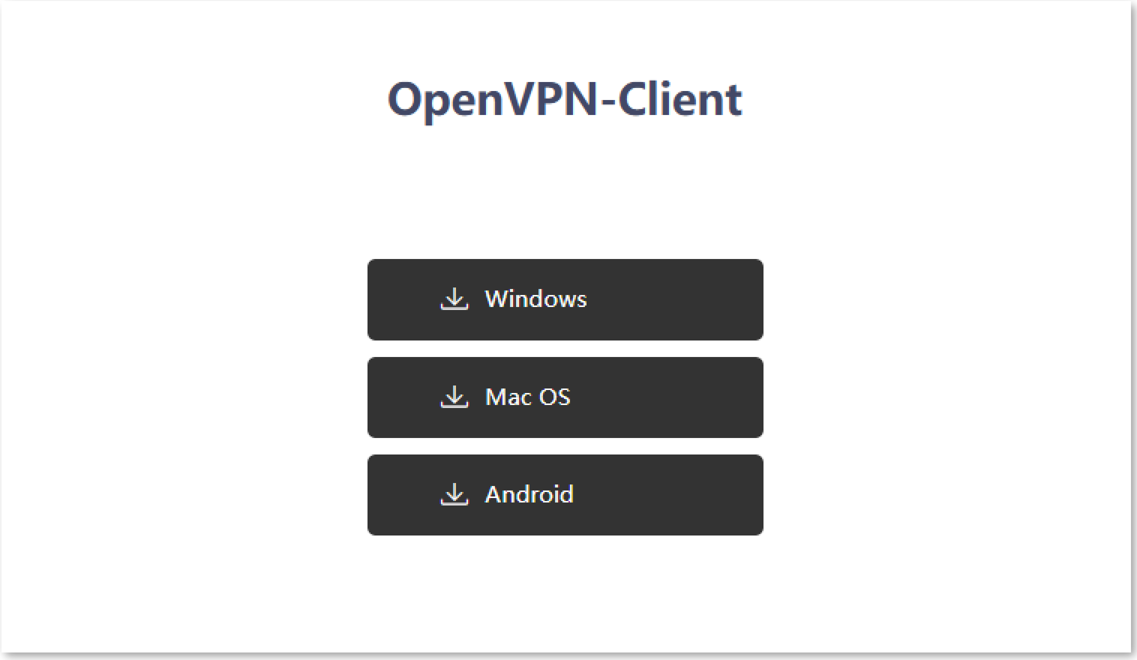
Verification

The employee on business trips uses VPN dial-up to access the headquarters resources.

Scenario 1: Accessing Headquarters Resources Remotely (Example: Windows 10)

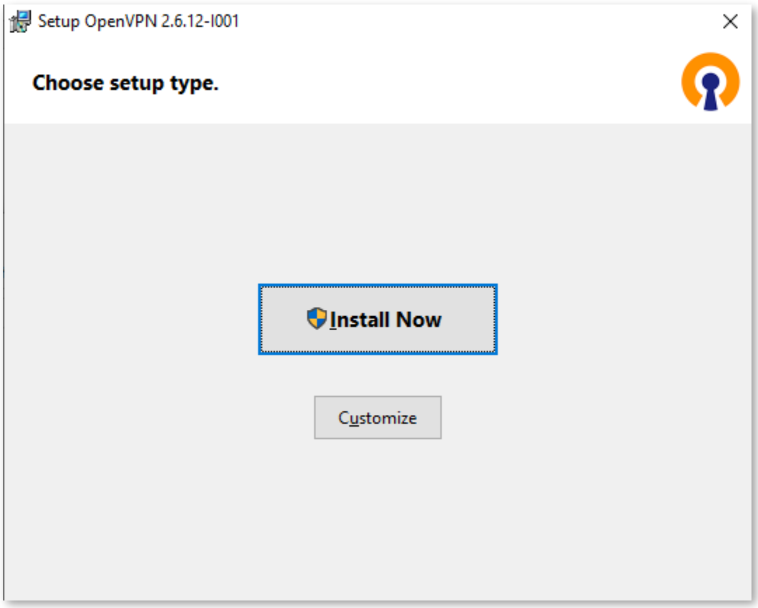
I. Install the OpenVPN client

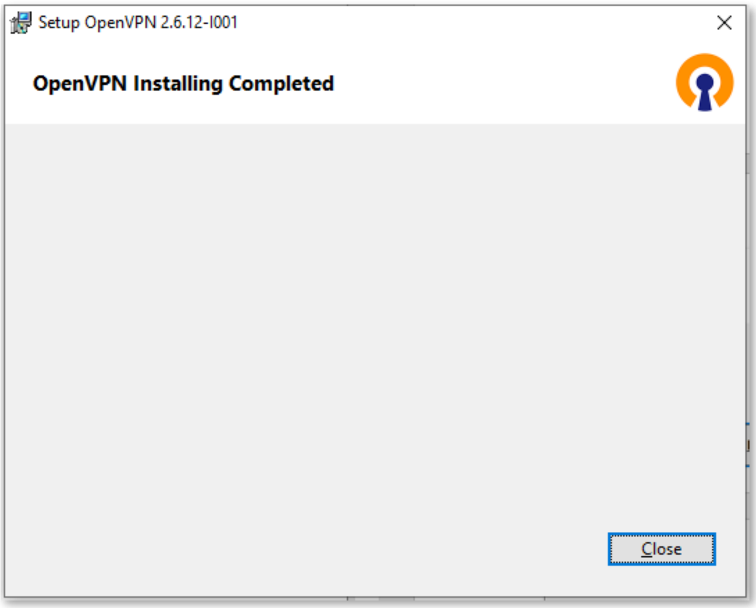
1. Download the OpenVPN client installer from ip-com.com.cn/en to the employee's computer.



OpenVPN-Client

2. Unpack the OpenVPN_Client-Win.rar file to obtain the OpenVPN-x.x.x-Ixxx-amd64.msi installer.
3. Double-click the installer and start installing the OpenVPN client.
4. Click **Install Now**, then wait until the installation completes. Click **Close**.

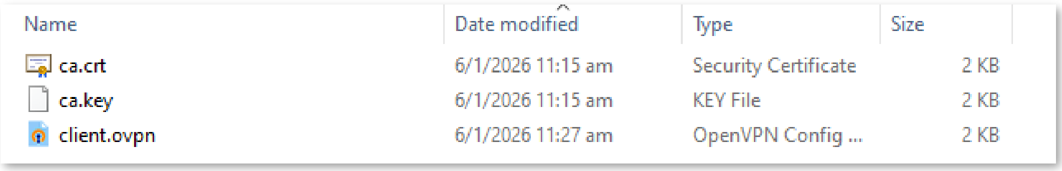




You can see the icon in the taskbar at the bottom right of your computer.

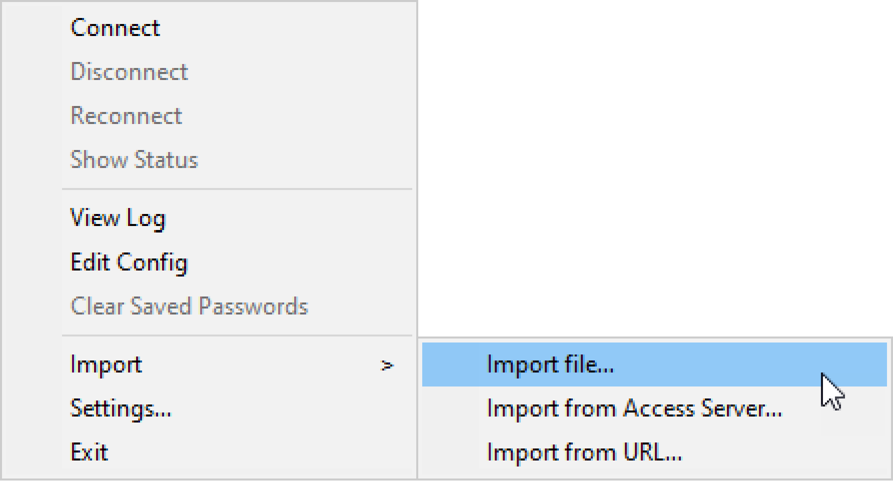
II. Establish an OpenVPN connection

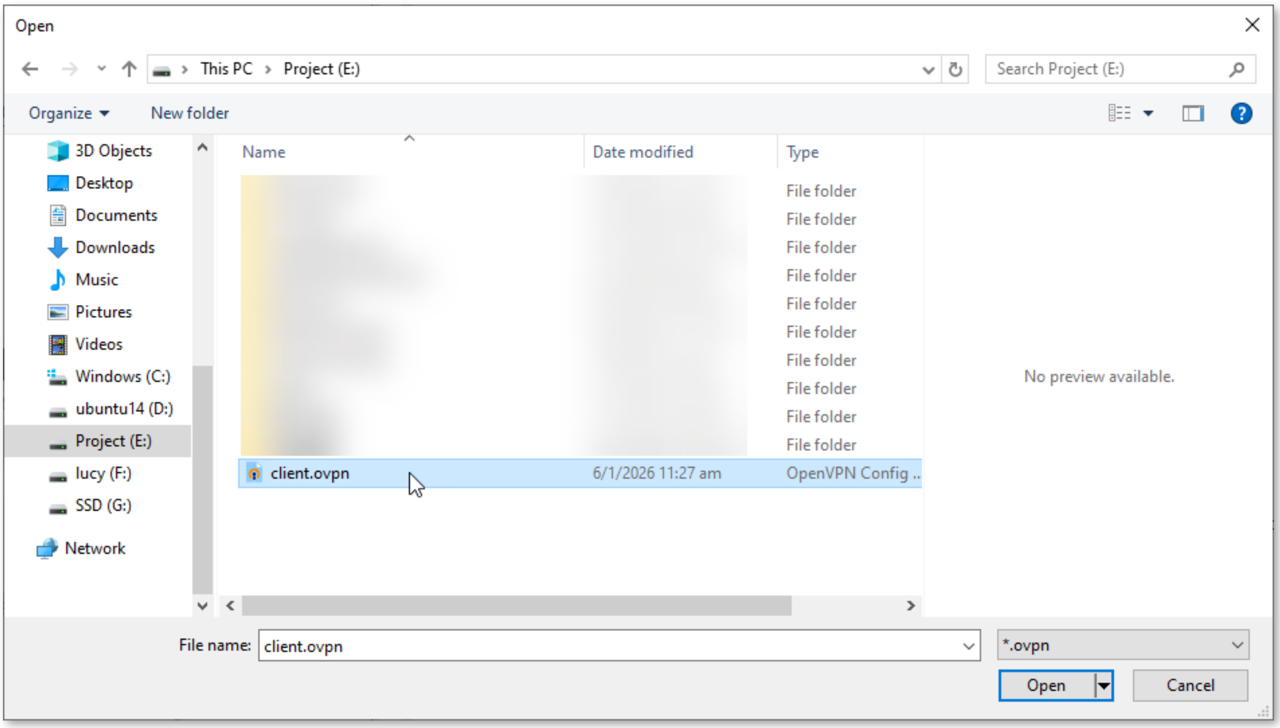
1. Download the **xxxxxxxx_openvpn-client-cfg.tar** file sent by the OpenVPN server and unpack it.



Name	Date modified	Type	Size
ca.crt	6/1/2026 11:15 am	Security Certificate	2 KB
ca.key	6/1/2026 11:15 am	KEY File	2 KB
client.ovpn	6/1/2026 11:27 am	OpenVPN Config ...	2 KB

2. Right-click the icon, select **Import** > **Import file...**, then locate and import the client.ovpn file.



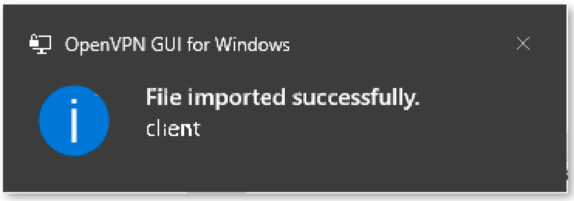


Name	Date modified	Type
		File folder
		File folder
		File folder
		File folder
		File folder
		File folder
		File folder
		File folder
		File folder
		File folder
client.ovpn	6/1/2026 11:27 am	OpenVPN Config ..

File name: client.ovpn

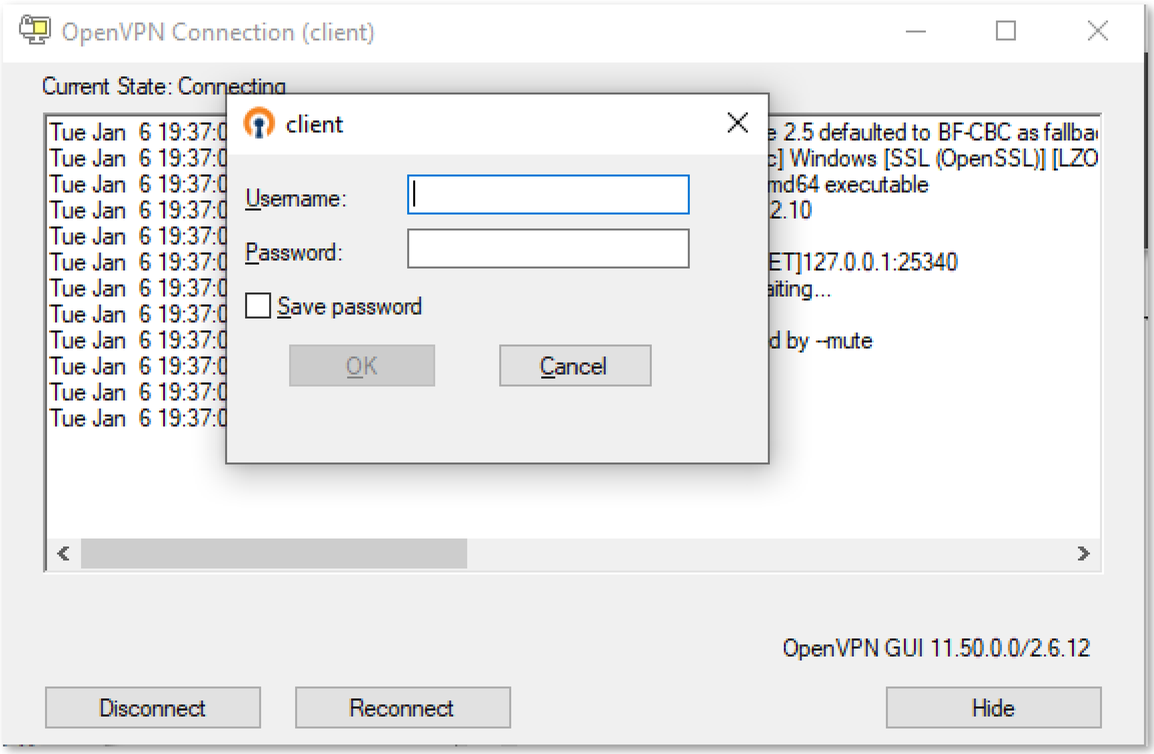
*.ovpn

File imported successfully.



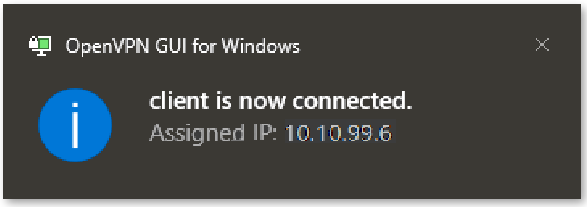
File imported successfully.
client

3. Double-click the icon, enter the username and password assigned by the VPN server, and click **OK**.


OpenVPN Connection (client)
Current State: Connecting
client
Username:
Password:
☐ Save password
OK
Cancel
OpenVPN GUI 11.50.0.0/2.6.12
Disconnect
Reconnect
Hide

```
Tue Jan  6 19:37:0     e 2.5 defaulted to BF-CBC as fallba
Tue Jan  6 19:37:0     c] Windows [SSL (OpenSSL)] [LZO
Tue Jan  6 19:37:0     md64 executable
Tue Jan  6 19:37:0     2.10
Tue Jan  6 19:37:0
Tue Jan  6 19:37:0     ET]127.0.0.1:25340
Tue Jan  6 19:37:0     aiting...
Tue Jan  6 19:37:0
Tue Jan  6 19:37:0     d by --mute
Tue Jan  6 19:37:0
Tue Jan  6 19:37:0
Tue Jan  6 19:37:0
```

Connected successfully.


OpenVPN GUI for Windows

client is now connected.

Assigned IP: 10.10.99.6

III. Access the headquarters resources

Assume that the employee on a business trip is accessing the headquarters FTP server. The server information is as follows:

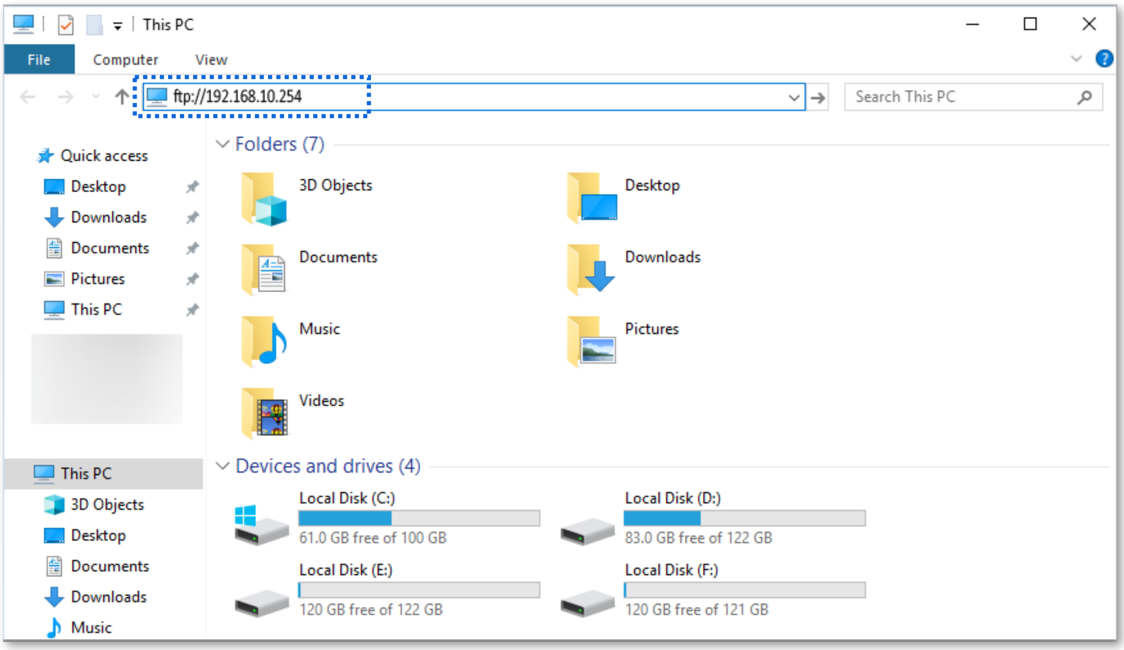
- FTP server IP address: **192.168.10.254**
- FTP service port: **21**
- Login user name/password: **Tom123/Tom23**

When a branch office employee accesses the headquarters project materials, perform the following procedures:

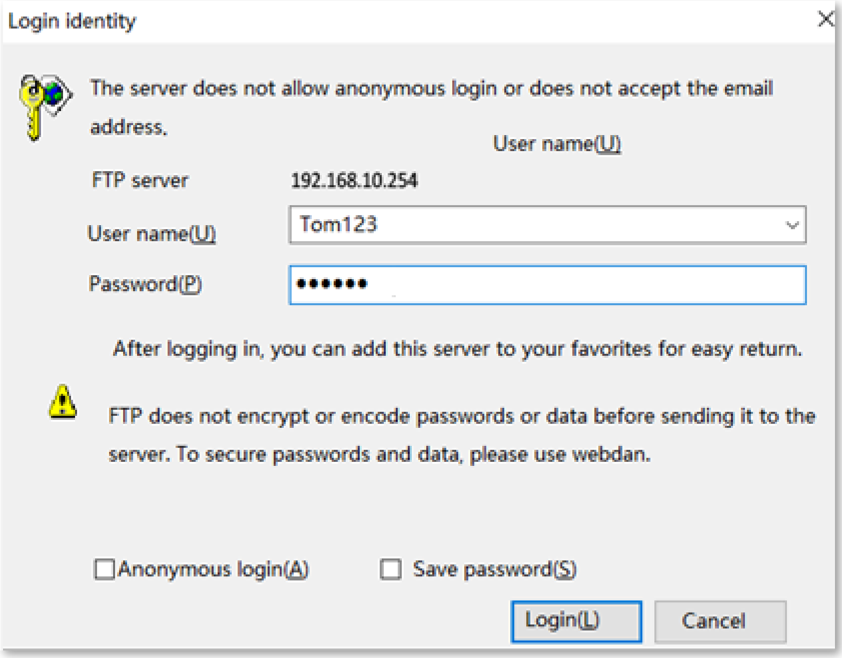
1. Enter **ftp://server IP address** in a browser or **This PC**, which is **ftp://192.168.10.254** in this example.

Tip

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



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



Login identity

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

User name(U)

FTP server 192.168.10.254

User name(U) Tom123

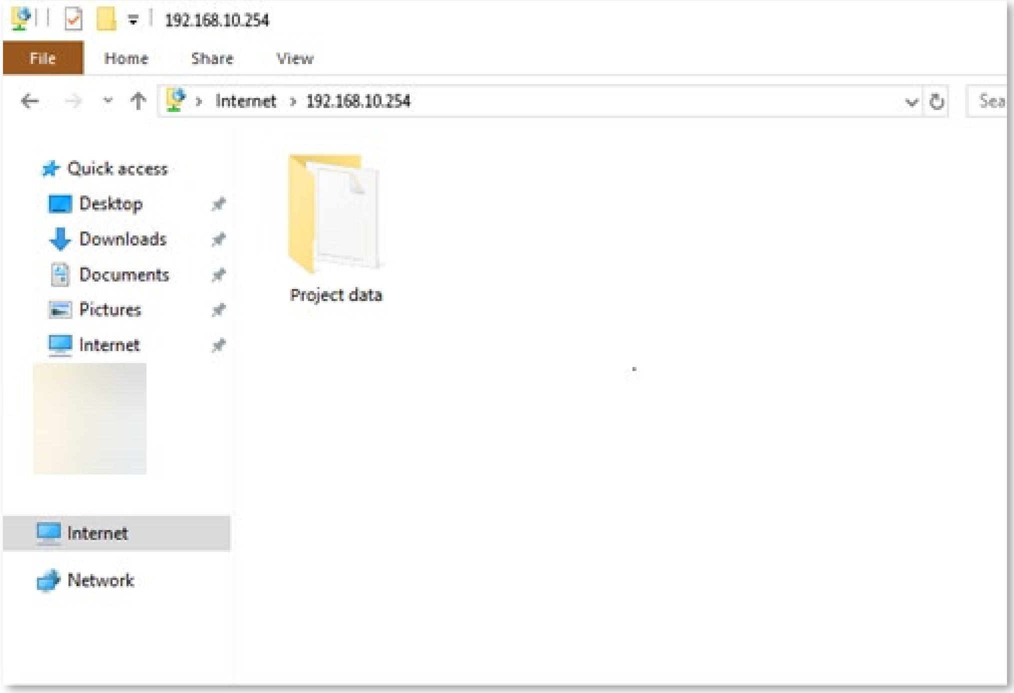
Password(P) ••••••

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

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

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

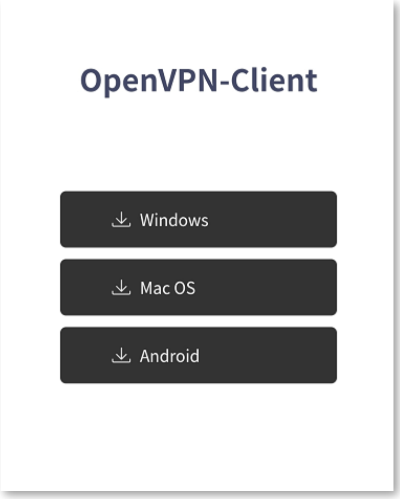
Access is successful.



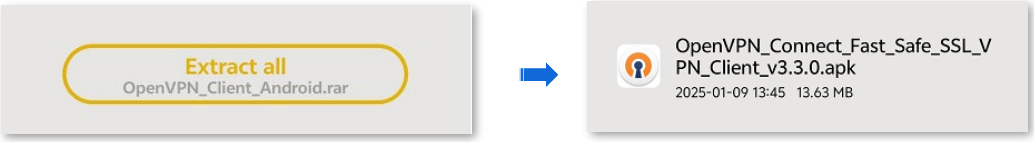
Scenario 2: Accessing Headquarters Resources Remotely (Example: Android device)

I. Install the OpenVPN client

1. Download the OpenVPN client installer from the App Store to the employee's phone.



2. Unpack the OpenVPN_Client-Android.rar file to get the .apk file. The figure below is for reference only.


Extract all
OpenVPN_Client_Android.rar
OpenVPN_Connect_Fast_Safe_SSL_VPN_Client_v3.3.0.apk
2025-01-09 13:45 13.63 MB

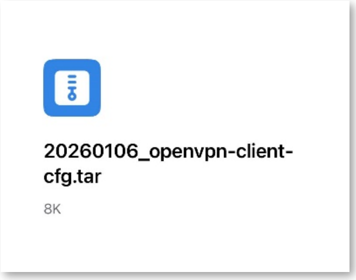
3. Tap the .apk file and start installation.

Tip

Ignore "This application poses a risk" during installation if the message appears.

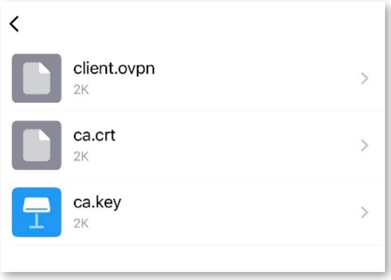
II. Establish an OpenVPN connection

1. Download the **xxxxxxxx_openvpn-client-cfg.tar** file sent by the OpenVPN server and unpack it.



20260106_openvpn-client-cfg.tar

8K



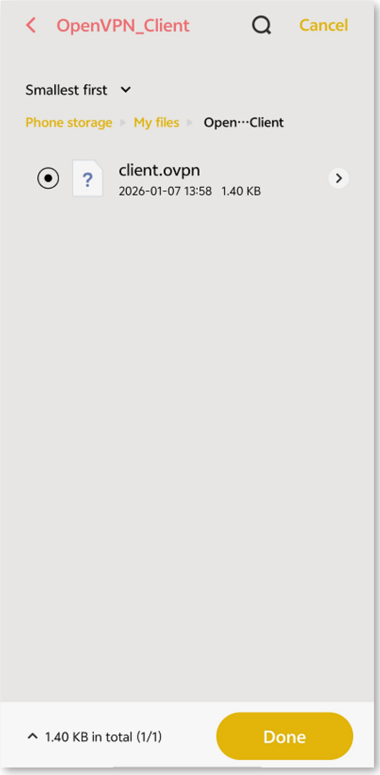
client.ovpn 2K

ca.crt 2K

ca.key 2K

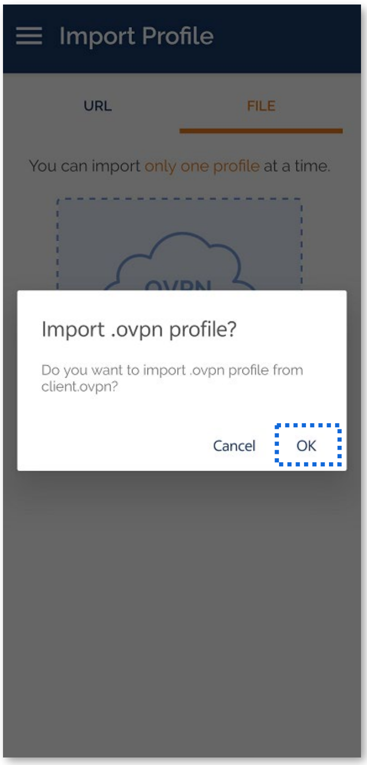
2. Tap **client.ovpn** and open with the OpenVPN Connect app.

3. Tap **OK**.



client.ovpn 2026-01-07 13:58 1.40 KB

1.40 KB in total (1/1)



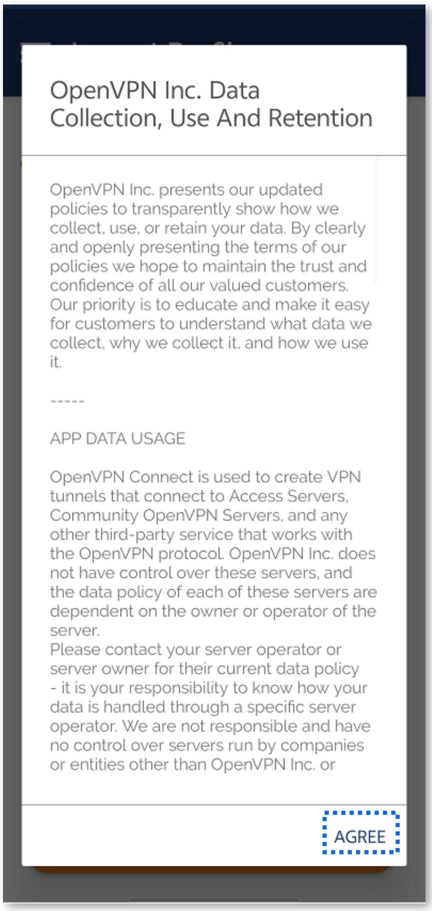
You can import only one profile at a time.

Import .ovpn profile?

Do you want to import .ovpn profile from client.ovpn?

4. The phone automatically runs the OpenVPN client. Tap **AGREE**.

5. Enter the username assigned by the VPN server. Tap **ADD**.

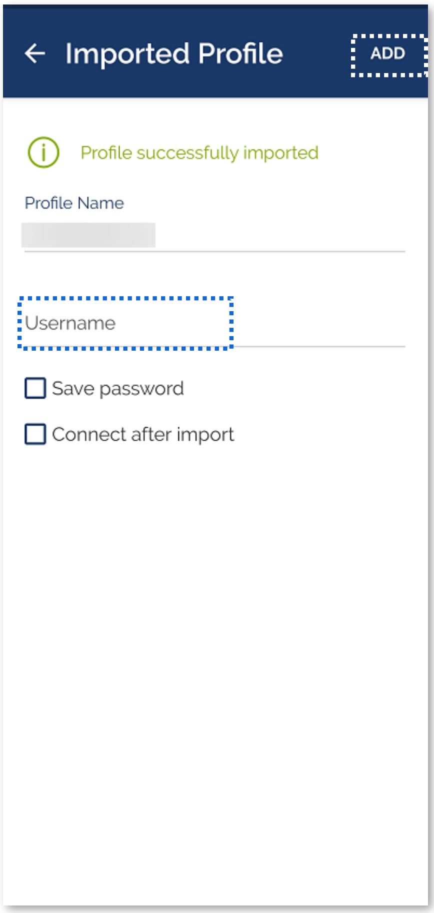


OpenVPN Inc. Data Collection, Use And Retention

OpenVPN Inc. presents our updated policies to transparently show how we collect, use, or retain your data. By clearly and openly presenting the terms of our policies we hope to maintain the trust and confidence of all our valued customers. Our priority is to educate and make it easy for customers to understand what data we collect, why we collect it, and how we use it.

APP DATA USAGE

OpenVPN Connect is used to create VPN tunnels that connect to Access Servers, Community OpenVPN Servers, and any other third-party service that works with the OpenVPN protocol. OpenVPN Inc. does not have control over these servers, and the data policy of each of these servers are dependent on the owner or operator of the server.
Please contact your server operator or server owner for their current data policy - it is your responsibility to know how your data is handled through a specific server operator. We are not responsible and have no control over servers run by companies or entities other than OpenVPN Inc. or



Profile successfully imported

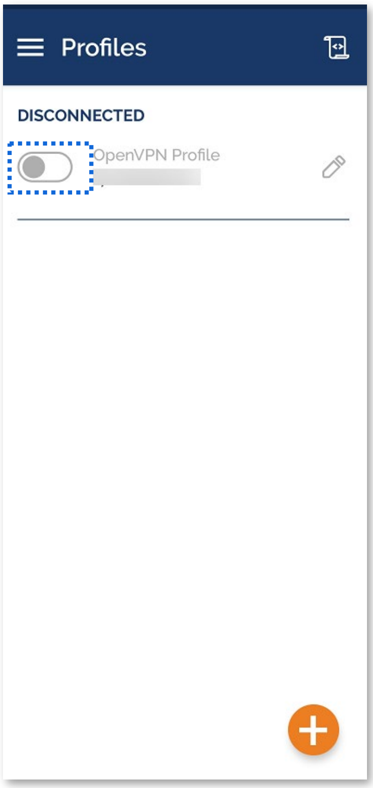
Profile Name

Username

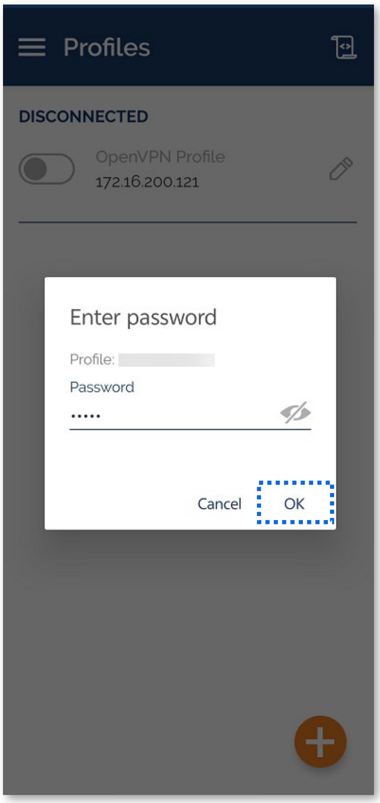
□ Save password

□ Connect after import

6. Tap ○ . Enter the password assigned by the VPN server, then tap **OK**.



OpenVPN Profile



OpenVPN Profile
172.16.200.121

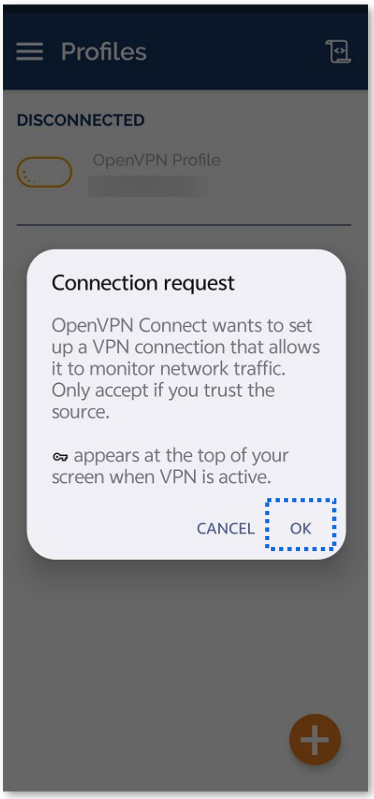
Enter password

Profile:

Password
•••••

7. Tap **OK**.

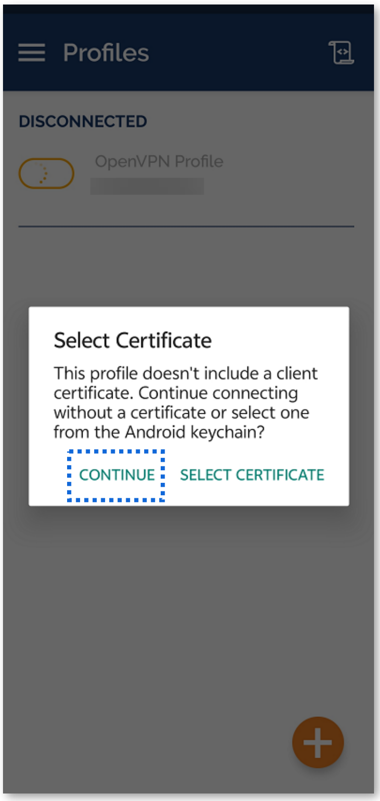
8. Tap **CONTINUE**.



Connection request

OpenVPN Connect wants to set up a VPN connection that allows it to monitor network traffic. Only accept if you trust the source.

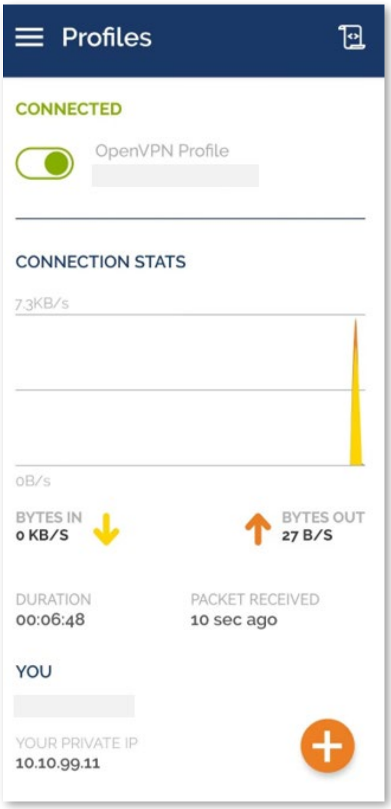
🔑 appears at the top of your screen when VPN is active.



Select Certificate

This profile doesn't include a client certificate. Continue connecting without a certificate or select one from the Android keychain?

9. Wait until a connection to the VPN server is established.



BYTES IN 0 KB/S

BYTES OUT 27 B/S

DURATION 00:06:48

PACKET RECEIVED 10 sec ago

YOU

YOUR PRIVATE IP 10.10.99.11

III. Access the headquarters resources

If you want to access the FTP server using a mobile device (smartphone, tablet, etc.), you need to have an FTP client successfully installed on your device.

9.4.7 IPSec

Overview

IP Security (IPSec) is a protocol suite for transmitting data over the internet in a secure and encrypted manner.

- **Encapsulation mode**

The Encapsulation mode specifies the encapsulation mode of the data transmitted by IPSec.

- **Tunnel Mode**: This mode adds an additional IP head and is most commonly used between gateways. The whole IP data packet of the user is used to calculate the Authentication Header (AH) or Encapsulating Security Payload (ESP) head. The AH or ESP head and the user data encrypted by ESP are encapsulated in a new IP data packet.
- **Transport Mode**: This mode does not change the original IP head and is most commonly used between hosts. Only the data at the transmission layer is used to calculate the AH or ESP head. The AH or ESP head or the user data encrypted by ESP are placed behind the original IP packet head.

Mode Protocol	Tunnel Mode	Transport Mode
AH	IP AH Data	IP AH IP Data
ESP	IP ESP Data ESP-T	IP ESP IP Data ESP-T
AH +ESP	IP AH ESP Data ESP-T	IP AH ESP IP Data ESP-T

- **Security gateway**

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

- **IPSec peer**

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

- **SA**

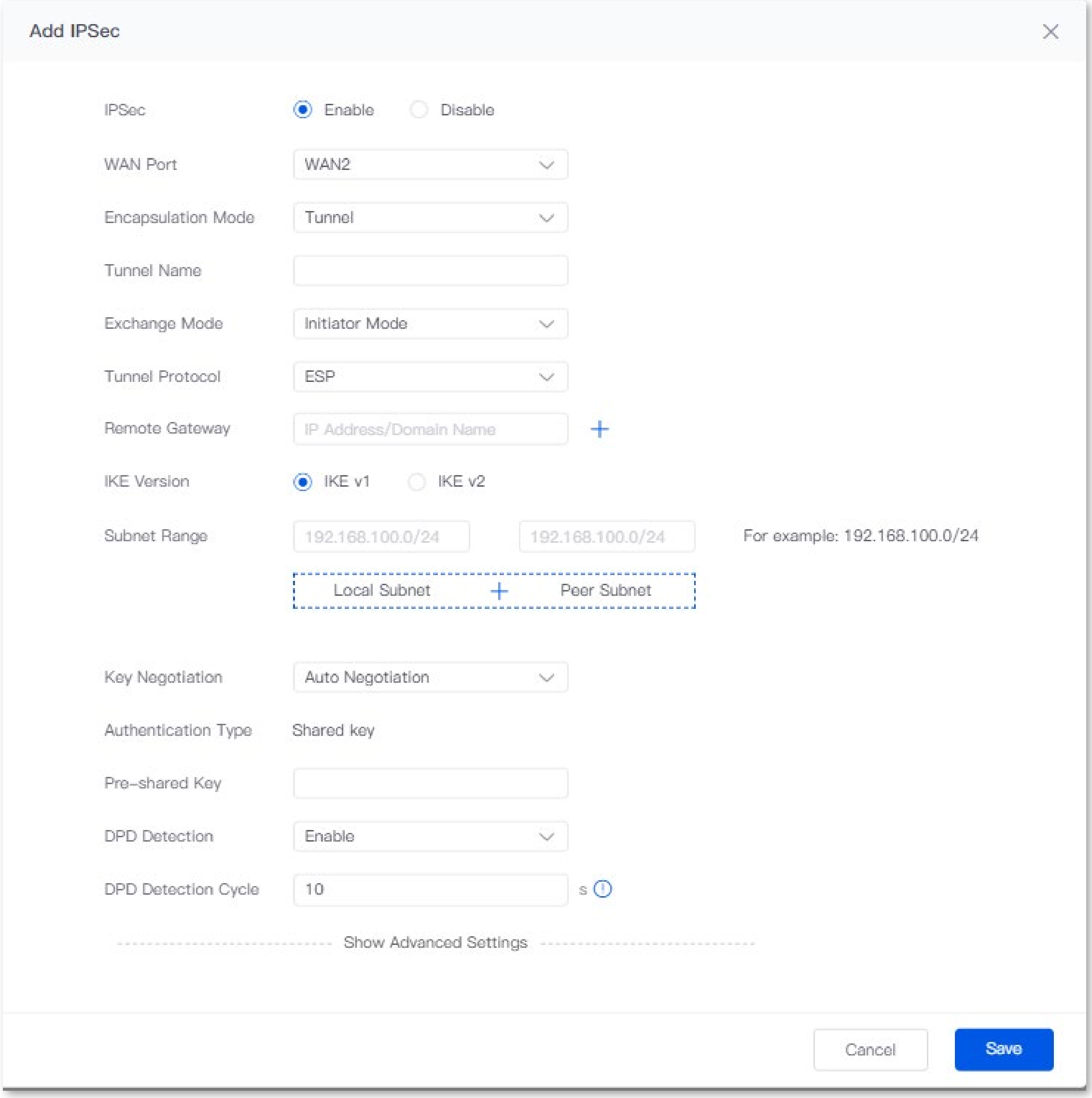
SA specifies some elements of the peers, such as the base protocol (AH, ESP or both), encapsulation mode (transport or tunnel), encryption algorithm (DES, 3DES or AES), shared key for data protection in specified flows and life cycle of the key.

SA has the following features:

- A triplet {SPI, Destination IP address, Security protocol identifier} is used as a unique ID.
- An SA specifies the protocol, algorithm and key for processing packets.
- An SA is unidirectional. At least two SAs are needed to protect data flows in bidirectional communication. If two peers want to use both AH and ESP to protect data flows between them, each peer will construct an independent SA for each protocol.
- An SA can be created manually or generated automatically using Internet Key Exchange (IKE).
  - Manually: The configuration is complex. All the information required to create an SA must be manually configured, and some advanced features (such as regular key update) are not supported. At this time, the SA has no life cycle limit and never expires unless it is manually deleted, which has certain security risks. Typically used in small and static environments, or when the number of peer devices communicating is less.
  - IKE Auto-Negotiation: Simple configuration, which you only need to configure the information of IKE negotiation security policy, and IKE Auto-Negotiation will create and maintain the SA. At this time, the SA has a life cycle and will be updated regularly to enhance security. Generally used in medium and large dynamic network environments.

Configure IPSec-tunnel mode

Log in to the web UI of the router, and navigate to **More** > **VPN Service** > **IPSec** to enter the page. On this page, you can configure the IPSec policy.



Add IPSec

IPSec ● Enable ○ Disable

WAN Port: WAN2

Encapsulation Mode: Tunnel

Tunnel Name:

Exchange Mode: Initiator Mode

Tunnel Protocol: ESP

Remote Gateway: IP Address/Domain Name +

IKE Version ● IKE v1 ○ IKE v2

Subnet Range: 192.168.100.0/24 192.168.100.0/24 For example: 192.168.100.0/24

Local Subnet + Peer Subnet

Key Negotiation: Auto Negotiation

Authentication Type: Shared key

Pre-shared Key:

DPD Detection: Enable

DPD Detection Cycle: 10 s

Show Advanced Settings

Cancel Save

Parameter description

Parameter	Description
IPSec	Used to enable or disable the IPSec function.
WAN Port	Specifies the local WAN port assigned to the IPSec function. The IP address of the WAN port must be set as the value of remote gateway of the IPSec peer.
Encapsulation Mode	– **Tunnel**: Used to protect the whole IP data packet (including IP head and data load), usually used for secure communication between two gateways. – **Transport**: Used to protect data load of the IP data packet, but not the IP head. This mode is generally used for secure communication between hosts and hosts or between hosts and gateways.
Tunnel Name	Specifies the name of the IPSec tunnel.

Parameter	Description
Exchange Mode	Specifies the negotiation mode of the IPSec tunnel. – **Initiator Mode**: The router initiates connection proactively and asks for access to the peer gateway. – **Responder Mode:** The router waits for the connection request. Note Do not set both sides of the IPSec tunnel to **Responder Mode.** Otherwise, you will fail to establish the IPSec tunnel.
Tunnel Protocol	Specifies the protocol which offers the security service for IPSec. – **AH**: It is abbreviated for Authentication Header. This protocol is used for verifying data integrity. If a packet is tampered during transmission, the receiver discards it during data integrity verification. – **ESP**: It is abbreviated for Encapsulating Security Payload. This protocol is used for verifying data integrity and encrypting data. If a packet processed using this protocol is intercepted during transmission, it is difficult for the intercepting party to obtain the real information contained in the packet. This compatible protocol is widely used in gateway products.
Remote Gateway	Specifies the WAN port IP address or domain name set by the IPSec tunnel peer gateway. Note When it is set to a domain name, the DDNS function has to be configured in the remote gateway to ensure that the use of IPSec tunnel is not affected by the changeable WAN port IP address of the remote gateway.
IKE Version	– **IKE v1**: Provides basic VPN functionality and broad compatibility, but with lower security. When configuring subnet ranges, each local–remote subnet pair must be configured manually. Any subnet mismatch will cause Security Association (SA) establishment to fail. – **IKE v2**: Offers an optimized negotiation process with improved security and flexibility. It supports multiple subnets and dynamic subnet negotiation. If subnets do not match exactly, the peers automatically negotiate the overlapping subnet range.
Subnet Range	– **Local Subnet**: Specifies the network segment and prefix length of the LAN network of the router. For example: Assume that the LAN IP address and subnet mask of this router are 192.168.0.1 and 255.255.255.0 respectively, enter 192.168.0.0/24. – **Peer Subnet**: Specifies the network segment and prefix length of the IPsec tunnel peer gateway LAN. If the peer is a single host, set this parameter to the device IP address with a /32 prefix.

Parameter	Description
Key Negotiation	The key negotiation method to establish an IPSec tunnel. **Auto Negotiation**: It indicates that an SA is set up, maintained, and deleted automatically using IKE (Internet Key Exchange). This reduces configuration complexity and simplifies IPSec usage and management. Such an SA (Security Association) has a life cycle and is updated regularly, leading to higher security.

Key negotiation-auto negotiation

During the auto-negotiation, to ensure the privacy of information, both parties to the IPSec communication need to use information known to each other to encrypt and decrypt the data, so the two parties need to negotiate the security key at the beginning of the communication, and this process is completed by IKE.

IKE is a hybrid of ISAKMP, Oakley and SKEME protocols.

- ISAKMP: Internet Security Association and Key Management Protocol (ISAKMP) provides a framework for exchanging keys and SA negotiation.
- Oakley: Oakley Key Determination Protocol is a key-agreement protocol that describes the specific mechanism for key exchange.
- SKEME: Secure Key Exchange Mechanism (SKEME) describes another key exchange mechanism that differs from Oakley.

IKE negotiation process is divided into two phases:

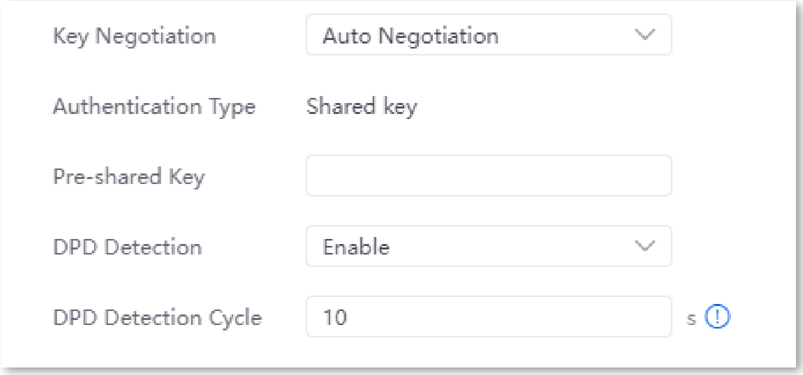
- **Phase 1**

The communicating parties will negotiate and exchange security proposals such as authentication algorithms and encryption algorithms, and establish an ISAKMP SA for the secure exchange of more information in Phase 2.

- **Phase 2**

This stage mainly negotiates a specific SA for IPSec on the ISAKMP SA established in Phase 1, and establishes an IPSec SA for the secure transmission of IP data.

When **Key Negotiation** is set to **Auto Negotiation**, the following figure is for reference only.



Key Negotiation: Auto Negotiation

Authentication Type: Shared key

Pre-shared Key:

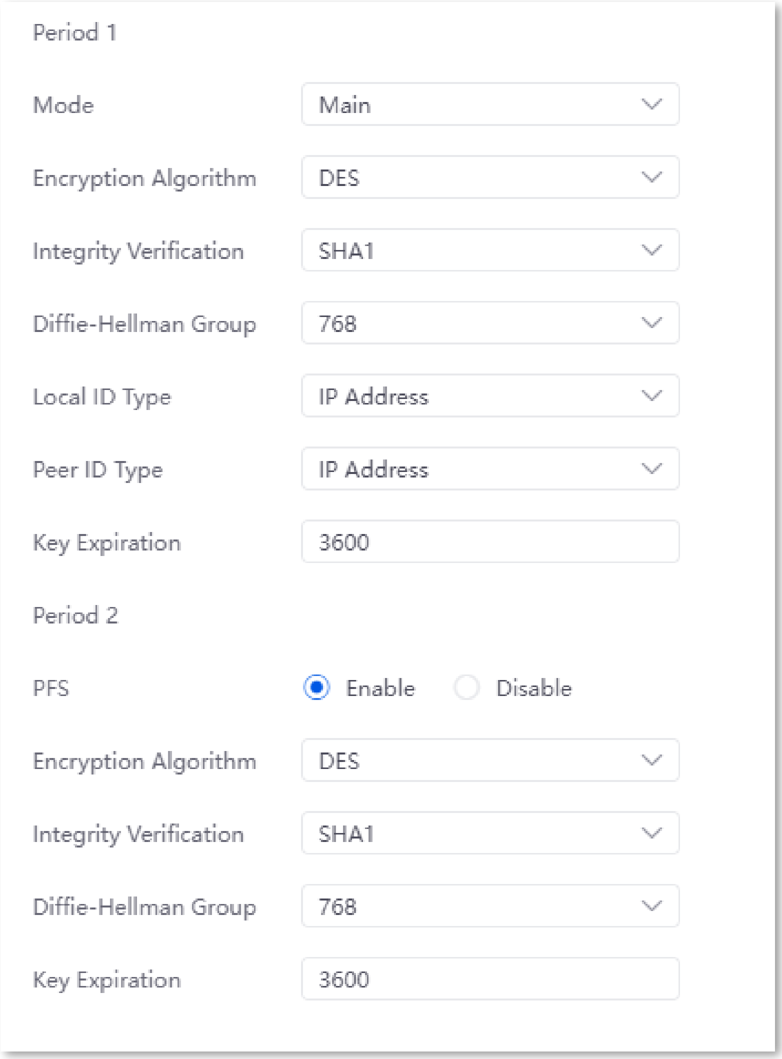
DPD Detection: Enable

DPD Detection Cycle: 10 s

Parameter description

Parameter	Description
Authentication Type	When **Shared key** is displayed on the page, it indicates that IPSec peers negotiated a key string shared between them.
Pre-shared Key	Specifies the pre-shared key used for negotiation. The key consists of a maximum of 128 characters and must be the same as that specified on the peer gateway.
DPD Detection	Used to enable or disable the Dead Peer Detection (DPD) function. When the DPD function is enabled, the router will periodically send DPD packets to the remote tunnel site to confirm whether the remote site is valid.
DPD Detection Cycle	Specifies the interval at which the router sends DPD frames. The default value is 10. If the router does not receive the confirmation of DPD frames within the valid period, it will initialize the IPSec SA from the local to the remote device.

Click **Show Advanced Settings** to display the advanced parameters of auto negotiation.



Period 1

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

Period 2

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

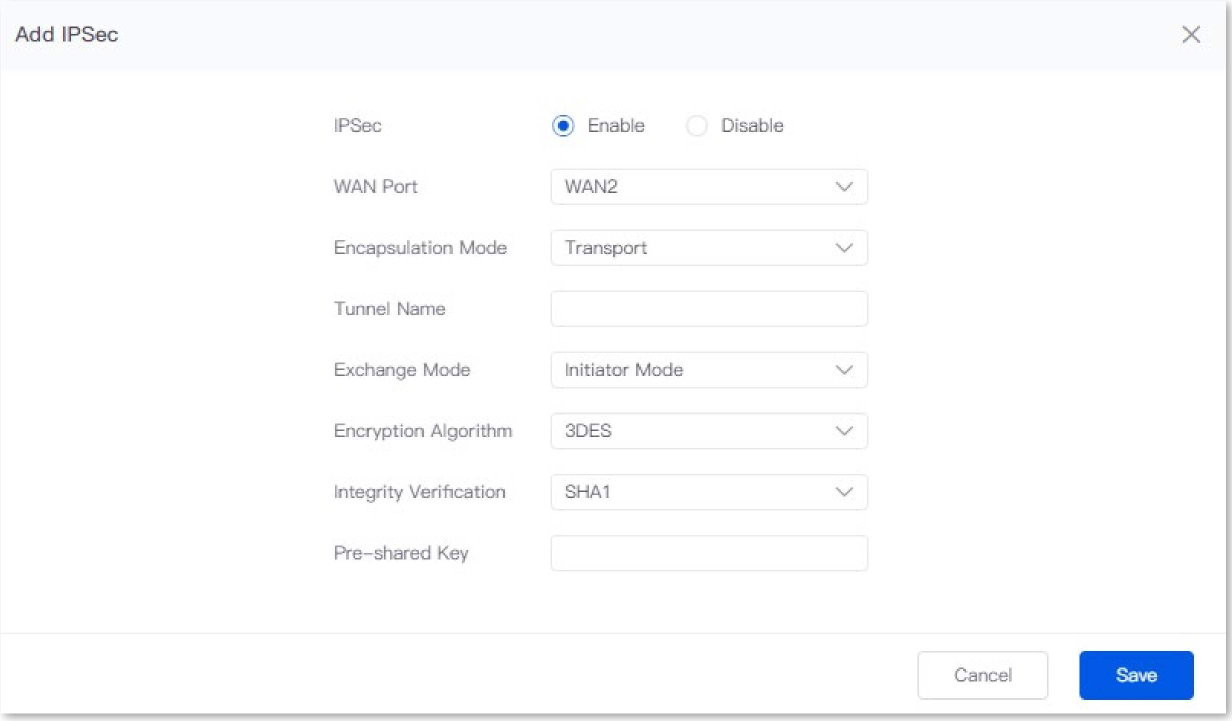
Parameter description

Parameter	Description
Mode	Specifies the mode supported by IKEv1. The mode selected should be consistent with that of the peer device. – **Main**: Under this mode, packet exchanges are frequent and identity protection is provided. Therefore, this mode is applicable for scenarios that require high level of identity protection. – **Aggressive:** Under this mode, identity protection is not provided and packet exchanges are less with high negotiation speed. Therefore, this mode is applicable for scenarios that require low level of identity protection.
Encryption Algorithm	Specifies the IKE session encryption algorithm. – **DES**: It is abbreviated for Data Encryption Standard. A 56-bit key is used to encrypt 64-bit data. The last 8 bits of the 64-bit data are used for parity check. 3DES indicates that three 56-bit keys are used for encryption. – **AES**: It is abbreviated for Advanced Encryption Standard. AES 128/192/256 indicates that 128/192/256-bit keys are used for encryption respectively.
Integrity Verification	Specifies the IKE session verification algorithm. – **MD5**: It is abbreviated for Message Digest Algorithm. A 128-bit message digest is generated to prevent message tampering. – **SHA1**: It is abbreviated for Secure Hash Algorithm. A 160-bit message digest is generated to prevent message tampering, leading to higher security than MD5.
Diffie-Hellman Group	Specifies the group information for the Diffie-Hellman algorithm for generating a session key used to encrypt an IKE tunnel. The information should be the same as that of the remote gateway.
Local ID Type	Specifies the ID of local gateway. – **IP Address**: Local router uses the WAN IP address of the remote gateway for negotiation with it. – **FQDN**: It is abbreviated for Fully Qualified Domain Name. You have to manually set a string of characters in the **Local ID.** Local ID should be identical with the peer ID of the remote gateway. Note Local ID type should be identical with the peer ID type. And you are recommended to modify the **Mode** to **Aggressive** in this case.

Parameter	Description
Peer ID Type	Specifies the ID of peer gateway. – **IP Address**: The router uses the IP address of the specified WAN port for negotiation with the remote gateway. – **FQDN**: It is abbreviated for Fully Qualified Domain Name. You have to manually set a string of characters in the **Peer ID.** Peer ID should be identical with the local ID of the remote gateway. Note Local ID type should be identical with the peer ID type. And you are recommended to modify the **Mode** to **Aggressive** in this case.
Key Expiration	Specifies the survival time of IPSec SA.
PFS	Specifies the Perfect Forward Secrecy (PFS) property of the IPSec session key. The PFS property must be consistent with the local PFS property. – **Enable**: Phase 2 negotiates to generate a new key material that is not associated with the key material negotiated by Phase 1, even if the IKE1 Phase 1 key is cracked, the Phase 2 key remains secure. – **Disable**: The key of Phase 2 will be generated according to the key material generated by Phase 1. Once the key of Phase 1 is cracked, the Phase 2 key used to protect the communication data is also at risk, which will seriously threaten the communication security of both parties.

Configure IPSec-transport mode

Log in to the web UI of the router, and navigate to **More** > **VPN Service** > **IPSec** to enter the page. Click **Add**, select **Transport** for **Encapsulation Mode** on the **Add IPSec** pop-up window, configure other parameters as required, and click **Save**.


Add IPSec

IPSec	● Enable ○ Disable
WAN Port	WAN2
Encapsulation Mode	Transport
Tunnel Name	
Exchange Mode	Initiator Mode
Encryption Algorithm	3DES
Integrity Verification	SHA1
Pre-shared Key	

Parameter description

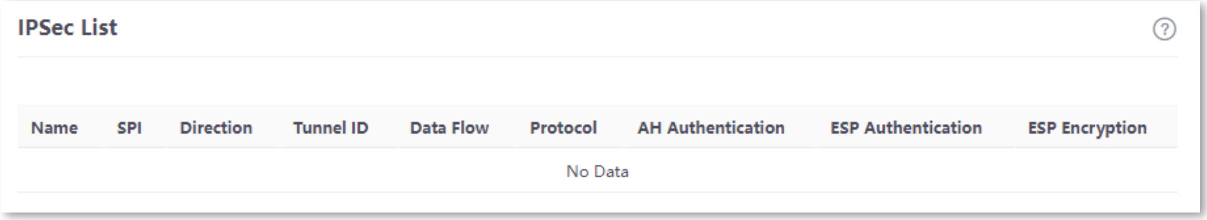
Parameter	Description
IPSec	Used to enable or disable the IPSec function.
WAN Port	Specifies the local WAN port assigned to the IPSec function. The IP address of the WAN port must be set as the value of remote gateway of the IPSec peer.
Encapsulation Mode	Specifies the encapsulation mode of IPSec data. – **Tunnel**: Used to protect the whole IP data packet (including IP head and data load), usually used for secure communication between two gateways. – **Transport**: Used to protect data load of the IP data packet, but not the IP head. This mode is generally used for secure communication between hosts and hosts or between hosts and gateways.
Tunnel Name	Specifies the name of the IPSec tunnel.
Exchange Mode	Specifies the negotiation mode of the IPSec tunnel. – **Initiator Mode**: The router initiates connection proactively and asks for access to the peer gateway. – **Responder Mode:** The router waits for the connection request. Note Do not set both sides of the IPSec tunnel to **Responder Mode.** Otherwise, you will fail to establish the IPSec tunnel.

Parameter	Description
Encryption Algorithm	Specifies the IKE session encryption algorithm. The router supports the following algorithms: – **DES**: A 56-bit key is used to encrypt 64-bit data. The last 8 bits of the 64-bit data are used for parity check. 3DES indicates that three 56-bit keys are used for encryption. – **AES**: A 128/192/256-bit key is used for encryption. AES 128/192/256 indicates that 128/192/256-bit keys are used for encryption respectively.
Integrity Verification	Specifies the IKE session verification algorithm. – **MD5**: It is abbreviated for Message Digest Algorithm. A 128-bit message digest is generated to prevent message tampering. – **SHA1**: It is abbreviated for Secure Hash Algorithm. A 160-bit message digest is generated to prevent message tampering, leading to higher security than MD5.
Pre-shared Key	Specifies the pre-shared key used for negotiation. The key consists of a maximum of 128 characters and must be the same as that specified on the peer gateway.

View IPSec SA

Log in to the web UI of the router, and navigate to **More** > **VPN Service** > **IPSec List** to enter the page.

After the devices at both ends of the IPSec tunnel are configured, you can view the IPSec SA in the IPSec list.


IPSec List

Name	SPI	Direction	Tunnel ID	Data Flow	Protocol	AH Authentication	ESP Authentication	ESP Encryption
No Data								

Parameter description

Parameter	Description
Name	Specifies the name of the IPSec tunnel policy.
SPI	Specifies the Security Parameter Index (SPI) of the current tunnel, which is obtained through automatic IKE negotiation.
Direction	Specifies the direction of the tunnel (in: flow in, out: flow out). Because IPSec rules are one-way, when an IPSec tunnel is successfully established, each tunnel will generate a pair of “in and out” IPSec rules with the same name.

Parameter	Description
Tunnel ID	Specifies the gateway addresses of two sides of the tunnel.
Data Flow	Specifies the subnet masks of two sides of the tunnel.
Protocol	Specifies the protocol which offers the security service for IPSec. – **AH**: It is abbreviated for Authentication Header. This protocol is used for verifying data integrity. If a packet is tampered during transmission, the receiver discards it during data integrity verification. – **ESP**: It is abbreviated for Encapsulating Security Payload. This protocol is used for verifying data integrity and encrypting data. If a packet processed using this protocol is intercepted during transmission, it is difficult for the intercepting party to obtain the real information contained in the packet. This compatible protocol is widely used in gateway products.
AH Authentication	Specifies the AH authentication algorithm used by the tunnel, which is determined by the proposal of the second phase of IKEv1.
ESP Authentication	Specifies the ESP authentication algorithm used by the tunnel, which is determined by the proposal of the second phase of IKEv1.
ESP Encryption	Specifies the ESP encryption algorithm used by the security protocol, which is determined by the security proposal in the second phase of IKEv1.

9.4.8 Example of configuring an IPSec VPN

Networking requirements

The headquarters and subsidiary use enterprise-class routers to set up a network and successfully access the internet. The subsidiary staff need to access intranet resources through the internet, such as internal documents, office OA, ERP system, CRM system, project management system and so on.

Solution

Set up an IPSec tunnel through the two routers (such as M30) to enable remote users to securely access the intranet through the internet.

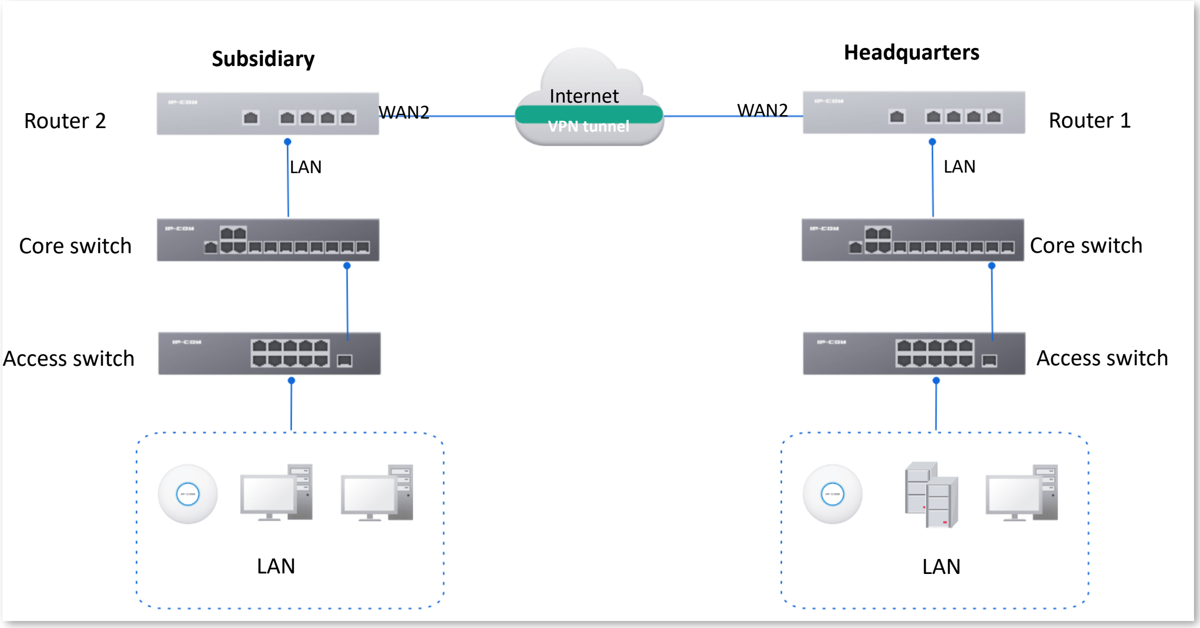
Assume that router 1 is deployed at the headquarters, the basic information is shown as follows:

- The port on which the IPSec tunnel is established is WAN2.
- The WAN2 IP address is 202.105.11.22.
- The LAN network is 192.168.10.0/24.

Assume that router 2 is deployed in the subsidiary, the basic information is shown as follows:

- The port on which the IPSec tunnel is established is WAN2.
- The WAN2 IP address is 202.105.88.77.
- The LAN network is 192.169.1.0/24.

Assume that two routers make the IPSec connection, the pre-shared key used to verify the identity is UmXmL9UK.



Configuration procedure

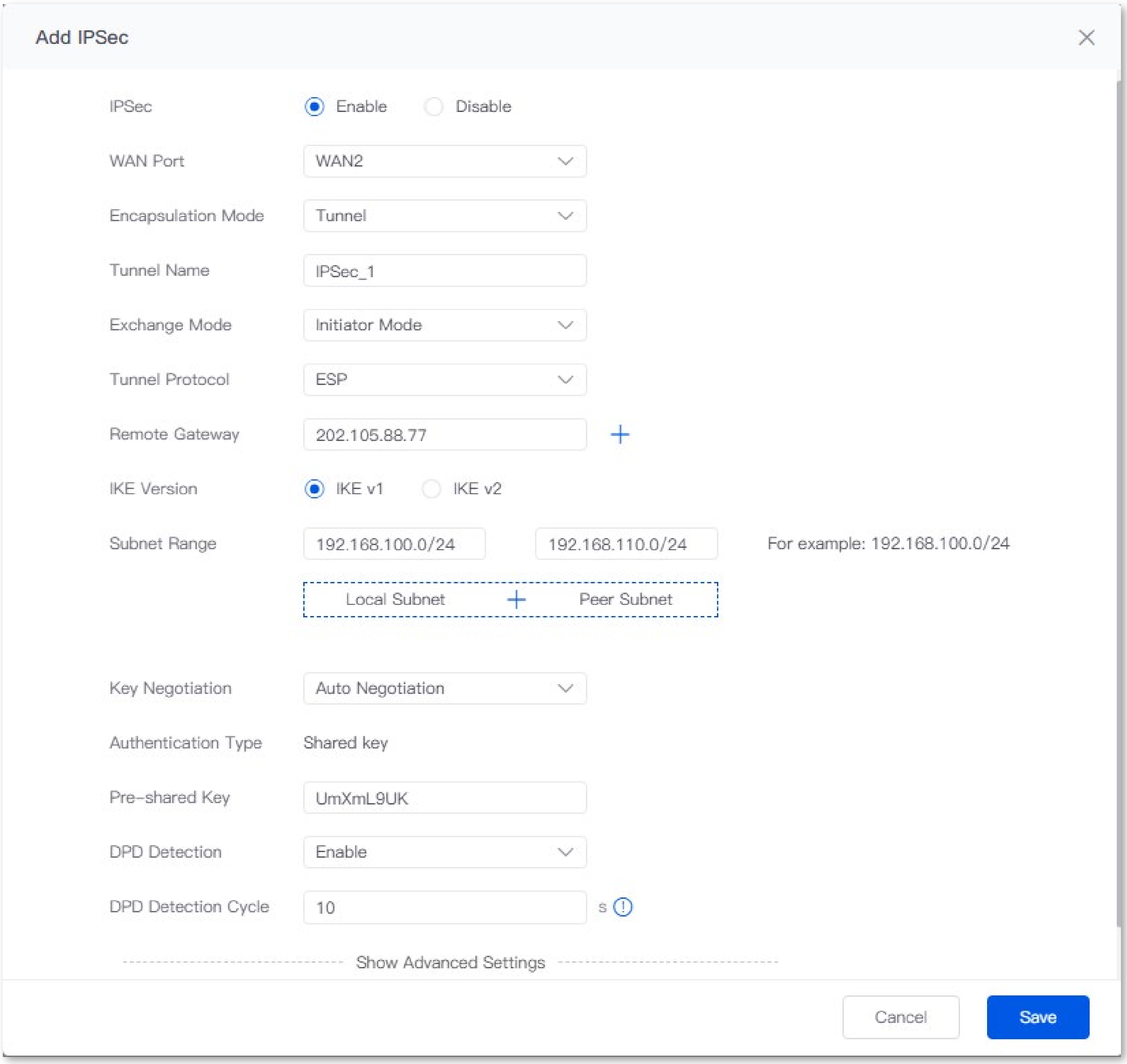
Configure the router 1 → Configure the router 2

Note

During the configuration process, if you need to set the advanced options of IPSec connection, keep the setting parameters of the two routers the same.

I. Configure the router 1

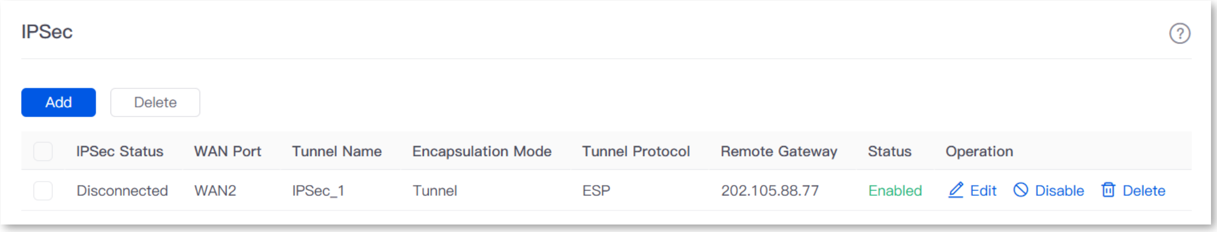
Log in to the web UI of the router 1. Navigate to **More** > **VPN Service** > **IPSec**, and click **Add** to configure the following IPSec. The parameter settings are for reference only.



Add IPSec

- IPSec: ● Enable ○ Disable
- WAN Port: WAN2
- Encapsulation Mode: Tunnel
- Tunnel Name: IPSec_1
- Exchange Mode: Initiator Mode
- Tunnel Protocol: ESP
- Remote Gateway: 202.105.88.77
- IKE Version: ● IKE v1 ○ IKE v2
- Subnet Range: 192.168.100.0/24 192.168.110.0/24 For example: 192.168.100.0/24
  Local Subnet + Peer Subnet
- Key Negotiation: Auto Negotiation
- Authentication Type: Shared key
- Pre-shared Key: UmXmL9UK
- DPD Detection: Enable
- DPD Detection Cycle: 10 s

The IPSec policy of router 1 is added successfully.

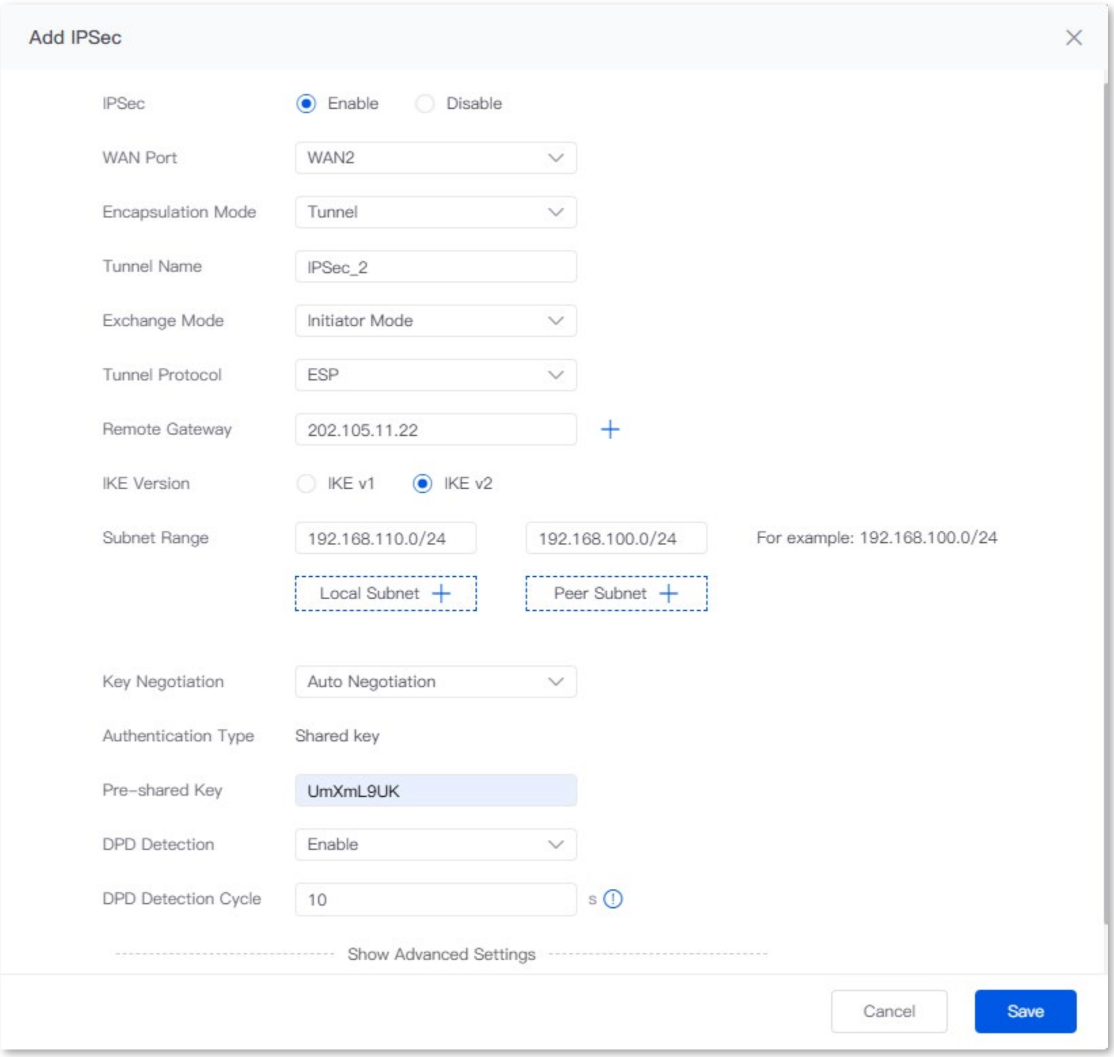


IPSec

IPSec Status	WAN Port	Tunnel Name	Encapsulation Mode	Tunnel Protocol	Remote Gateway	Status	Operation
Disconnected	WAN2	IPSec_1	Tunnel	ESP	202.105.88.77	Enabled	Edit Disable Delete

II. Configure the router 2

Log in to the web UI of the router 2. Navigate to **More** > **VPN Service** > **IPSec**, and click **Add** to configure the following IPSec. The parameter settings are for reference only.



Add IPSec

IPSec: ● Enable ○ Disable

WAN Port: WAN2

Encapsulation Mode: Tunnel

Tunnel Name: IPSec_2

Exchange Mode: Initiator Mode

Tunnel Protocol: ESP

Remote Gateway: 202.105.11.22 +

IKE Version: ○ IKE v1 ● IKE v2

Subnet Range: 192.168.110.0/24 192.168.100.0/24 For example: 192.168.100.0/24

Local Subnet + Peer Subnet +

Key Negotiation: Auto Negotiation

Authentication Type: Shared key

Pre-shared Key: UmXmL9UK

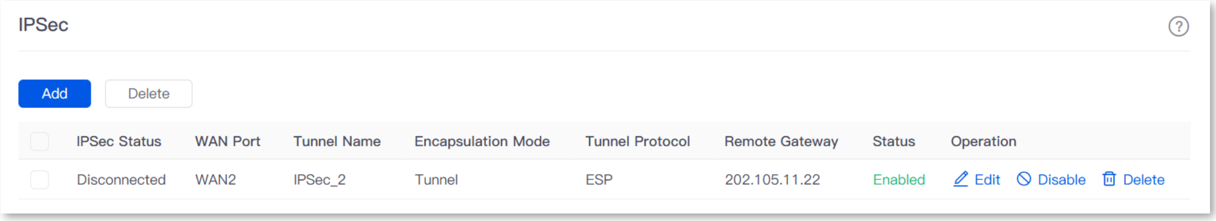
DPD Detection: Enable

DPD Detection Cycle: 10 s

Show Advanced Settings

Cancel Save

The IPSec policy of router 2 is added successfully.



IPSec

Add Delete

□	IPSec Status	WAN Port	Tunnel Name	Encapsulation Mode	Tunnel Protocol	Remote Gateway	Status	Operation
□	Disconnected	WAN2	IPSec_2	Tunnel	ESP	202.105.11.22	Enabled	Edit Disable Delete

---End

Verification

When there are two IPSec SA entries appearing under **IPSec List**, the VPN tunnel is set up. The headquarters and subsidiary can securely access each other's LAN resources through the internet.

9.5 IPv6

9.5.1 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).

9.5.2 Internet

Log in to the web UI of the router, and 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 user name and password that supports IPv6 service.	

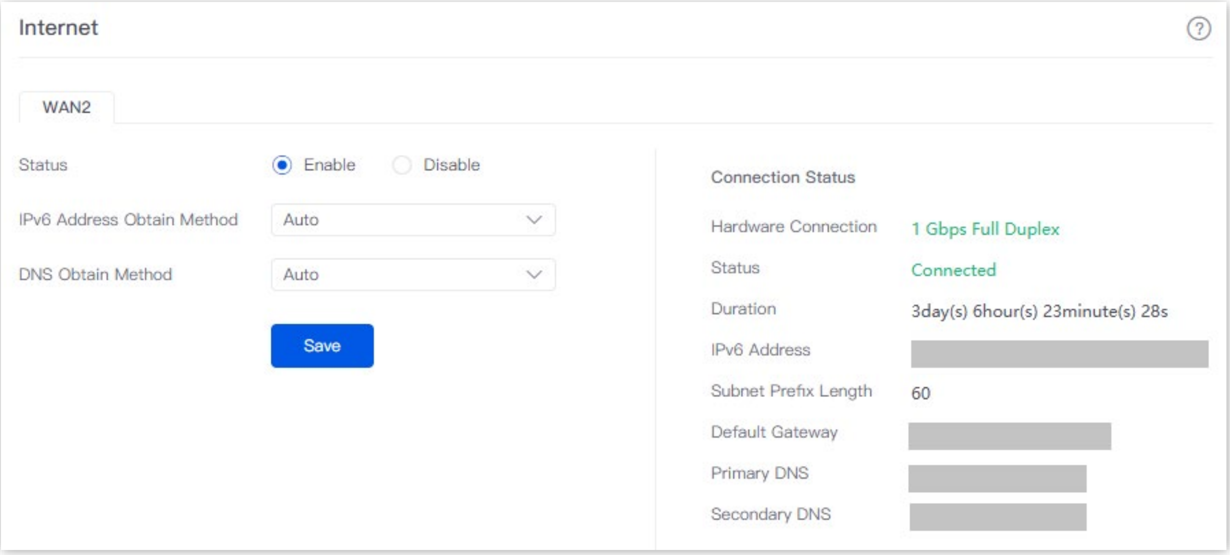
Condition	Selection
The upstream device is the ISP device, and the ISP does not provide specific network parameters.	
The upstream device does not assign IP addresses.	Manual
The upstream device is the ISP device, and the ISP provides a group of fixed IPv6 addresses for internet access, including the 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 for help.

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.



Internet

WAN2

Status ● Enable ○ Disable

IPv6 Address Obtain Method: Auto

DNS Obtain Method: Auto

Save

Connection Status

Hardware Connection	1 Gbps Full Duplex
Status	Connected
Duration	3day(s) 6hour(s) 23minute(s) 28s
IPv6 Address	[redacted]
Subnet Prefix Length	60
Default Gateway	[redacted]
Primary DNS	[redacted]
Secondary DNS	[redacted]

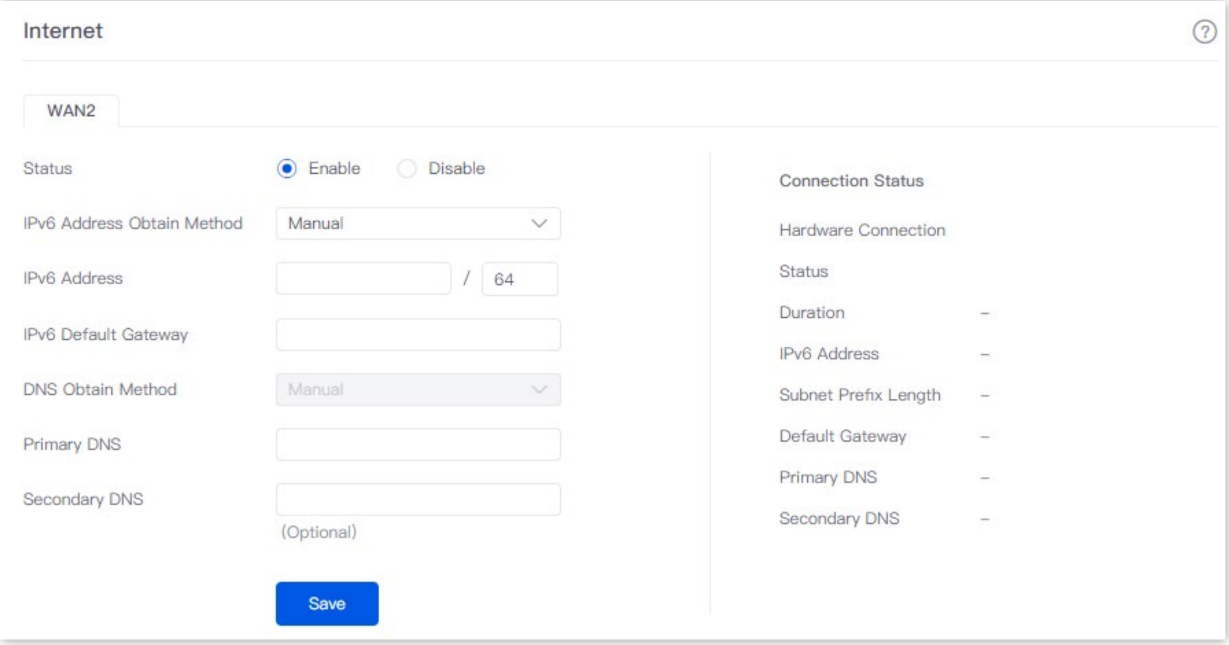
Parameter description

Parameter		Description
Mode	Status	Used to enable or disable the IPv6 function of the corresponding WAN port.
	IPv6 Address Obtain Method	Select **Auto**.

Parameter		Description
	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 contact the corresponding ISP for help.
	Duration	Specifies the duration of the WAN port access to the IPv6 network.
	IPv6 Address	Specifies the IPv6 global unicast address of the WAN port.
	Subnet Prefix Length	Specifies the network prefix number of the IPv6 address.
	Default Gateway	Specifies the IPv6 default gateway of the WAN port.
	Primary DNS	Specify the primary or secondary IPv6 DNS server address of the WAN port.
	Secondary DNS	

Manual

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



Internet

WAN2

Status ● Enable ○ Disable

IPv6 Address Obtain Method: Manual

IPv6 Address: / 64

IPv6 Default Gateway:

DNS Obtain Method: Manual

Primary DNS:

Secondary DNS: (Optional)

Save

Connection Status

Hardware Connection

Status

Duration –

IPv6 Address –

Subnet Prefix Length –

Default Gateway –

Primary DNS –

Secondary DNS –

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	
	Hardware Connection	Specifies the current rate and duplex mode of the WAN port.

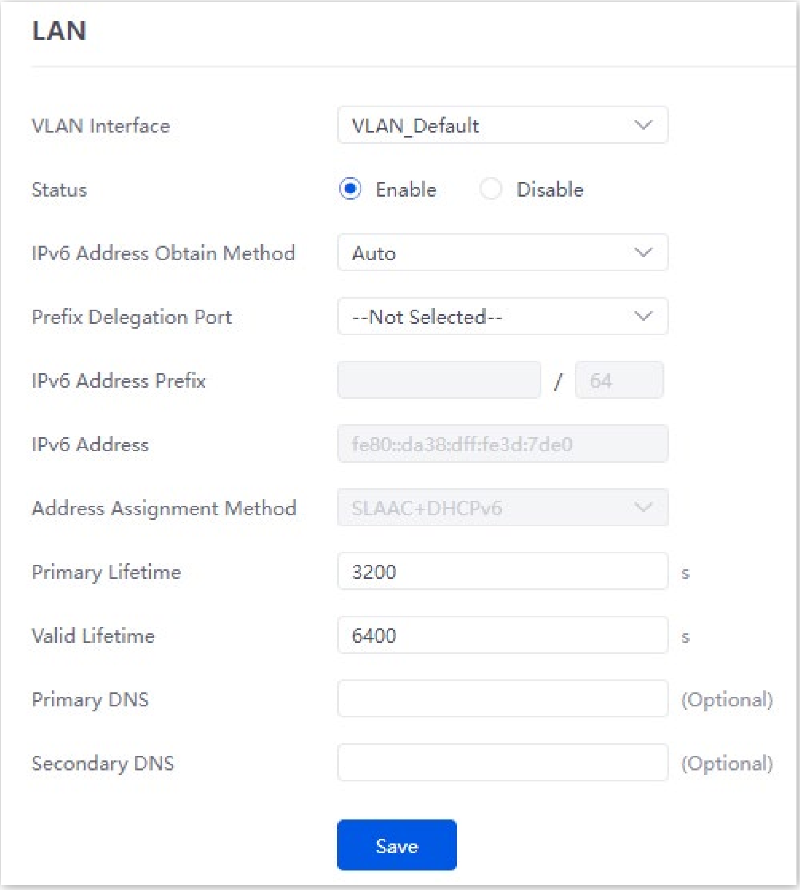
Parameter		Description
Connection Status	Status	Specifies the connection status of the WAN port of the router. – **Connected**: The WAN port of the router has been plugged into the Ethernet cable, and the IPv6 address information has been obtained. – **Connecting...**: The router is connecting to the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

9.5.3 LAN

Log in to the web UI of the router, and 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 in the LAN can share the broadband server.

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



LAN

VLAN Interface	VLAN_Default
Status	● Enable ○ Disable
IPv6 Address Obtain Method	Auto
Prefix Delegation Port	--Not Selected--
IPv6 Address Prefix	/ 64
IPv6 Address	fe80::da38:dff:fe3d:7de0
Address Assignment Method	SLAAC+DHCPv6
Primary Lifetime	3200 s
Valid Lifetime	6400 s
Primary DNS	(Optional)
Secondary DNS	(Optional)

Parameter description

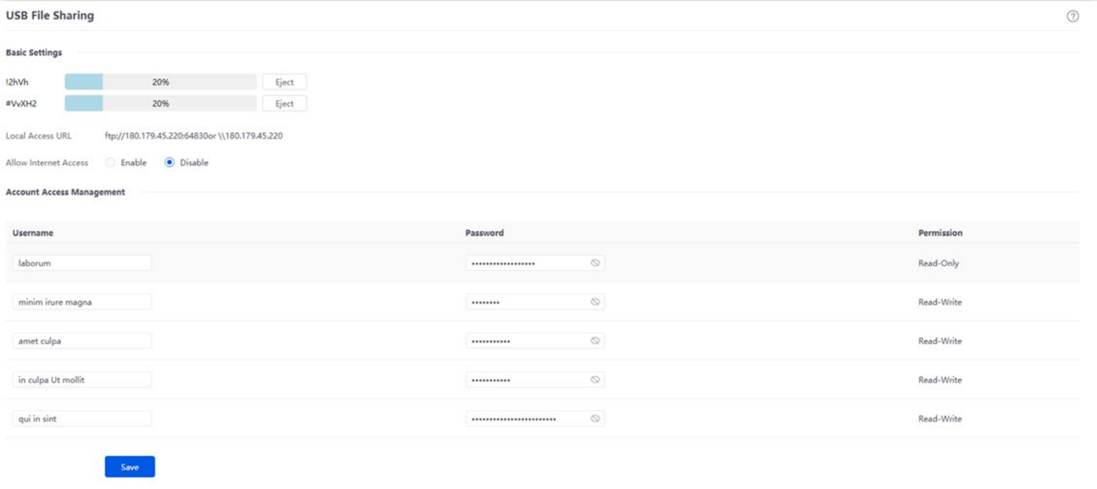
Parameter	Description
VLAN Interface	Specifies the VLAN interface for IPv6.
Status	Used to enable or disable the IPv6 function of the corresponding VLAN.
IPv6 Address Obtain Method	Specifies the method to obtain IPv6 addresses. – **Auto:** The IPv6 address prefix of the VLAN is automatically obtained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

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

9.6 USB application

Log in to the web UI of the router, and navigate to **More** > **USB Application** to enter the page.

When a USB storage device (such as a USB flash drive) is connected to the router's USB port, LAN or Internet users can access the device resources via a sharing link with a username and password.



USB File Sharing

Basic Settings

I2hVh 20% Eject

#VvXH2 20% Eject

Local Access URL ftp://180.179.45.220:64830or \\180.179.45.220

Allow Internet Access ○ Enable ● Disable

Account Access Management

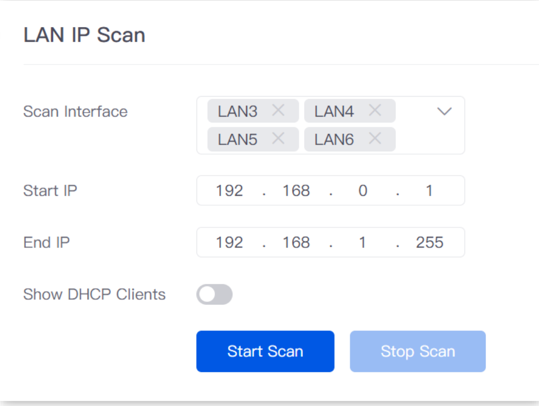
Username	Password	Permission
laborum	••••••••••••••••••	Read-Only
minim irure magna	•••••••••	Read-Write
amet culpa	••••••••••••	Read-Write
in culpa Ut mollit	••••••••••••	Read-Write
qui in sint	••••••••••••••••••••••••	Read-Write

9.7 LAN IP scan

With the LAN IP scanning function, you can scan and view all devices within a specified IP rang under the router's LAN port, including devices that obtain IPs from the router's DHCP server (which can be scanned after enabling Show DHCP Clients) and devices for which you have manually set static IPs.

Configuration procedure:

1. Log in to the web UI of the router.
2. Navigate to **More** > **LAN IP Scan**.
3. Select the scan interface.
4. Enter the start and end IP addresses.
5. (Optional) To display devices that have obtained IP addresses from the router’s DHCP server, enable **Show DHCP Clients**.
6. Click **Start Scan**.



LAN IP Scan

Scan Interface: LAN3, LAN4, LAN5, LAN6

Start IP: 192 . 168 . 0 . 1

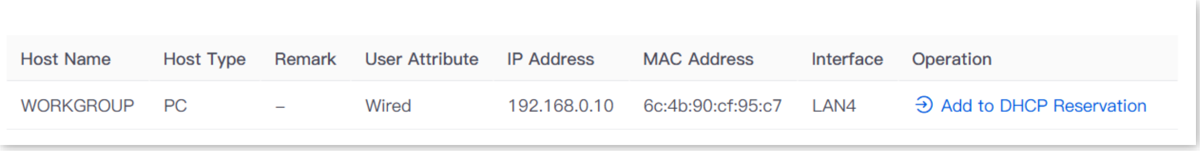
End IP: 192 . 168 . 1 . 255

Show DHCP Clients: off

---End

Wait while the router processes the settings. The page will then display devices connected to the router’s LAN port that have manually configured static IP addresses.

Click **Add to DHCP Reservation** to add the device to the DHCP reservation list. The router will assign the IP address accordingly, and the assignment result will be shown under **Status** on the **DHCP Reservation** page. The figure below is for reference only.



Host Name	Host Type	Remark	User Attribute	IP Address	MAC Address	Interface	Operation
WORKGROUP	PC	–	Wired	192.168.0.10	6c:4b:90:cf:95:c7	LAN4	Add to DHCP Reservation

10 Handle maintenance tasks

Features available in the router may vary by model and software version. Router availability may also vary by region or ISP. All images, steps, and descriptions in this guide are only examples and may not reflect your actual router experience.

10.1 System time

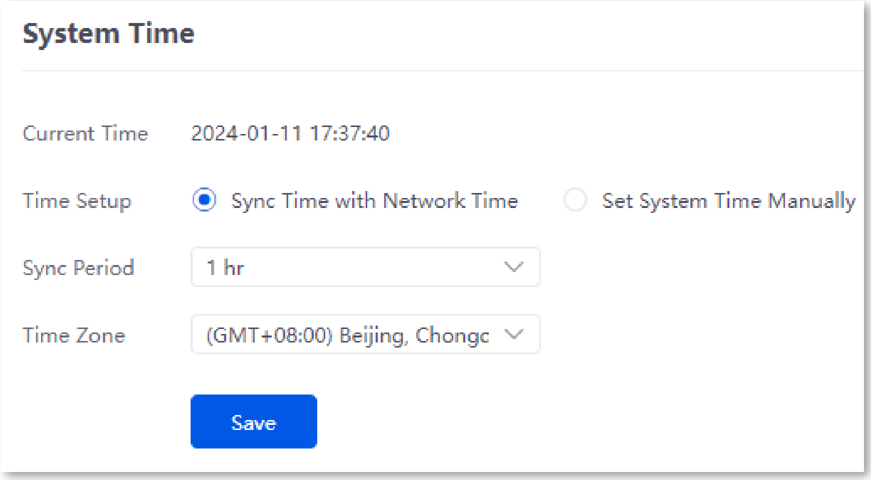
Log in to the web UI of the router, and navigate to **Tool** > **System Time** to enter the page. On this page, you can configure the system time of the router.

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.

10.1.1 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.



System Time

Current Time 2024-01-11 17:37:40

Time Setup ● Sync Time with Network Time ○ Set System Time Manually

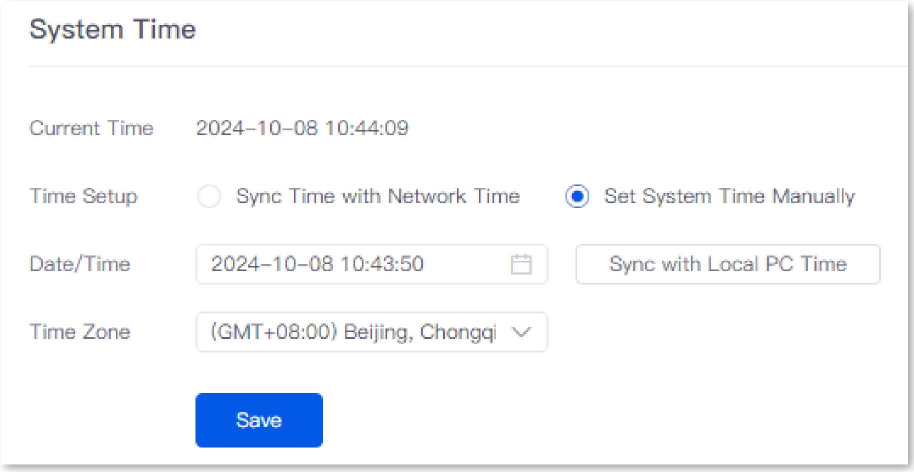
Sync Period 1 hr

Time Zone (GMT+08:00) Beijing, Chongc

10.1.2 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.



System Time

Current Time 2024-10-08 10:44:09

Time Setup ○ Sync Time with Network Time ● Set System Time Manually

Date/Time 2024-10-08 10:43:50

Time Zone (GMT+08:00) Beijing, Chongqi

10.2 Diagnostic tool

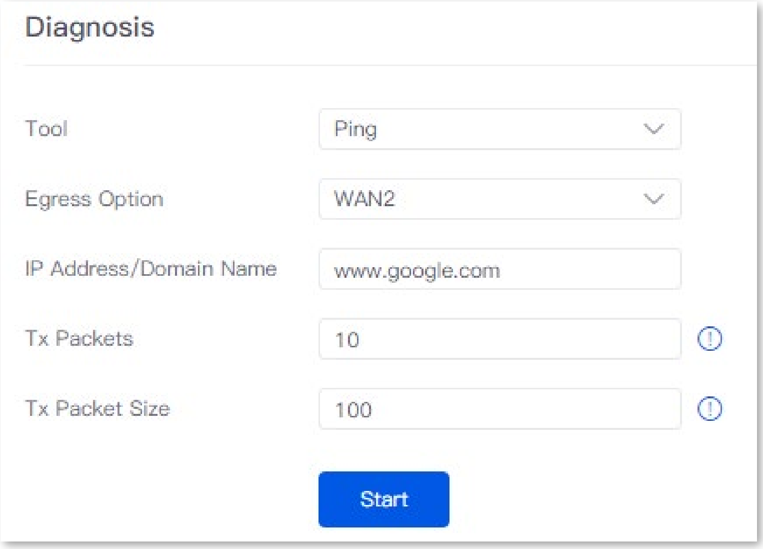
10.2.1 Ping

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

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 **WAN2** 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 **100** in this example.
7. Click **Start**.



Diagnosis

Tool: Ping

Egress Option: WAN2

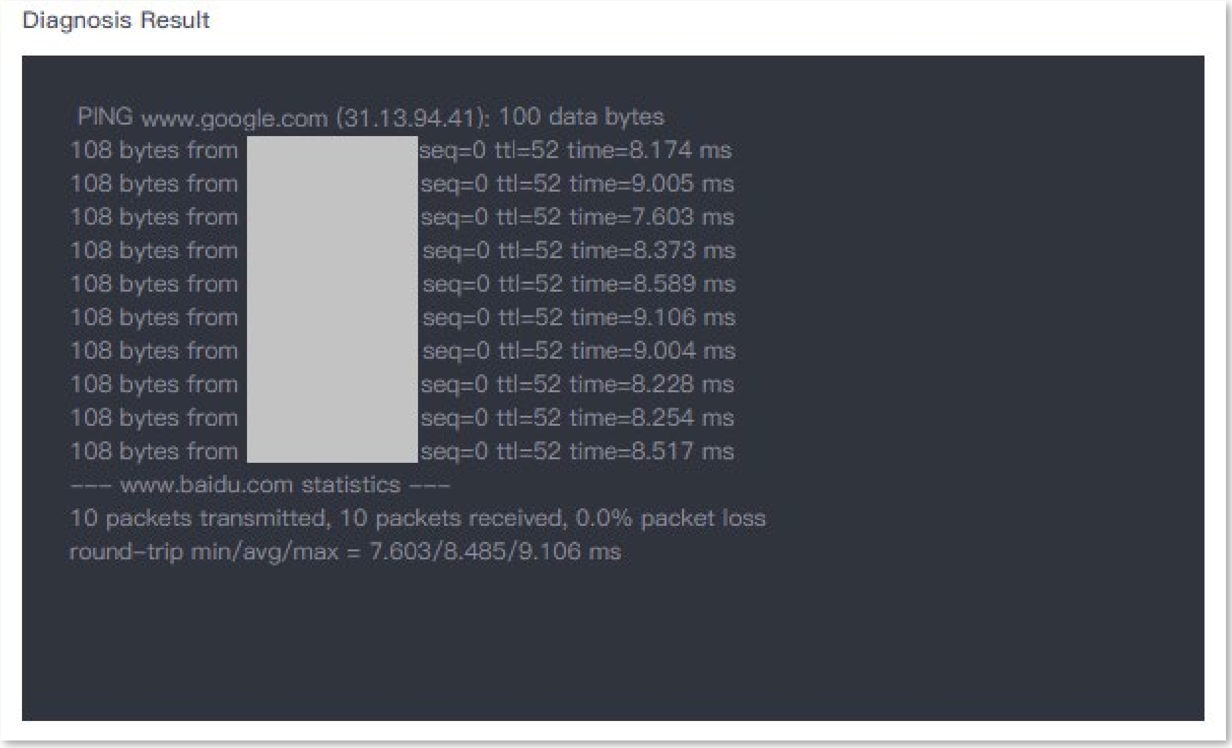
IP Address/Domain Name: www.google.com

Tx Packets: 10

Tx Packet Size: 100

---End

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



Diagnosis Result

```
 PING www.google.com (31.13.94.41): 100 data bytes
108 bytes from [redacted] seq=0 ttl=52 time=8.174 ms
108 bytes from seq=0 ttl=52 time=9.005 ms
108 bytes from seq=0 ttl=52 time=7.603 ms
108 bytes from seq=0 ttl=52 time=8.373 ms
108 bytes from seq=0 ttl=52 time=8.589 ms
108 bytes from seq=0 ttl=52 time=9.106 ms
108 bytes from seq=0 ttl=52 time=9.004 ms
108 bytes from seq=0 ttl=52 time=8.228 ms
108 bytes from seq=0 ttl=52 time=8.254 ms
108 bytes from seq=0 ttl=52 time=8.517 ms
--- www.baidu.com statistics ---
10 packets transmitted, 10 packets received, 0.0% packet loss
round-trip min/avg/max = 7.603/8.485/9.106 ms
```

10.2.2 Tracert

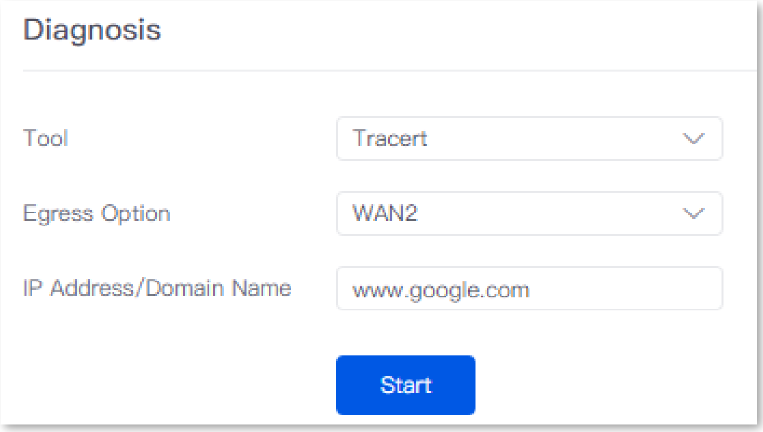
Tracert is used to detect the routes that a packet takes from a router to a destination host.

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 **WAN2** 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**.



Diagnosis

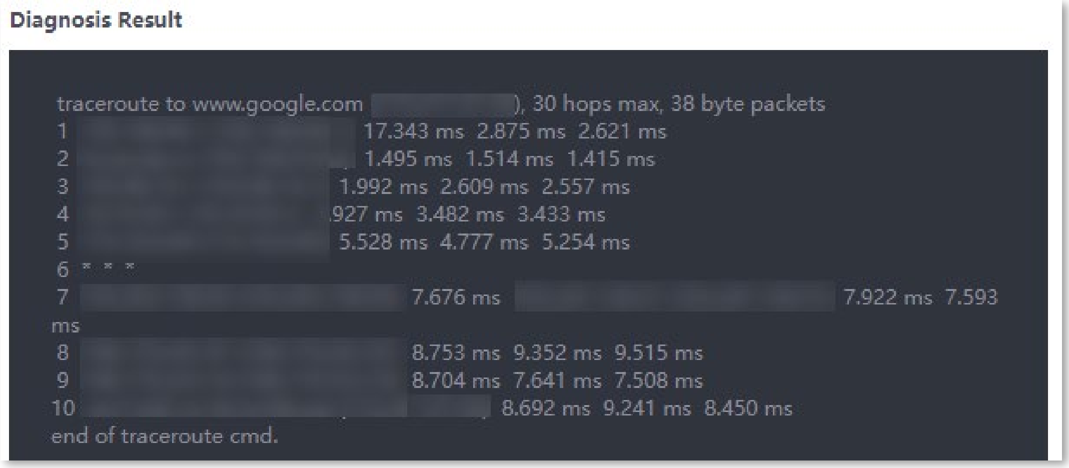
Tool: Tracert

Egress Option: WAN2

IP Address/Domain Name: www.google.com

---End

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



Diagnosis Result

```
traceroute to www.google.com [redacted]), 30 hops max, 38 byte packets
1 [redacted] 17.343 ms  2.875 ms  2.621 ms
2 [redacted] 1.495 ms  1.514 ms  1.415 ms
3 [redacted] 1.992 ms  2.609 ms  2.557 ms
4 [redacted]927 ms  3.482 ms  3.433 ms
5 [redacted] 5.528 ms  4.777 ms  5.254 ms
6 * * *
7 [redacted] 7.676 ms [redacted] 7.922 ms  7.593
ms
8 [redacted] 8.753 ms  9.352 ms  9.515 ms
9 [redacted] 8.704 ms  7.641 ms  7.508 ms
10 [redacted] 8.692 ms  9.241 ms  8.450 ms
end of traceroute cmd.
```

10.2.3 Packet capture tool

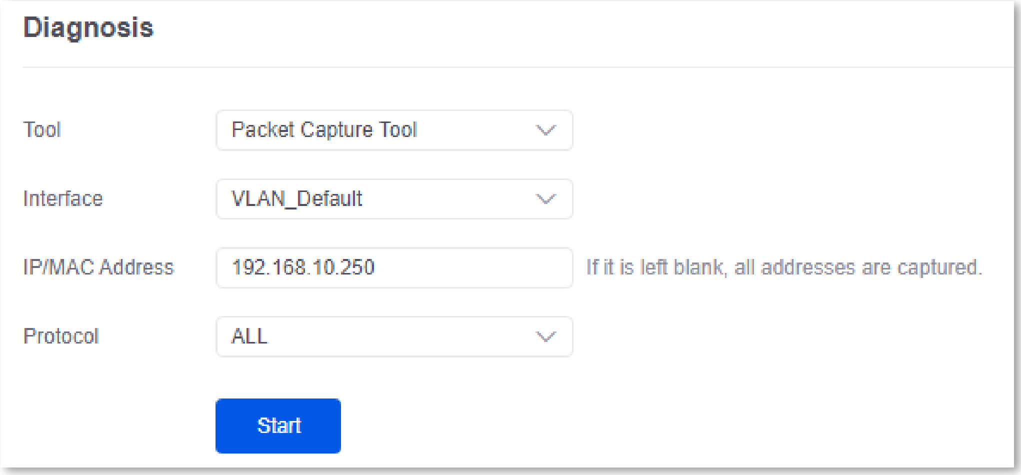
Packet Capture Tool is a network data collection and analysis tool, which can completely intercept the specified data packets in the network to provide analysis.

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**.



Diagnosis

Tool: Packet Capture Tool

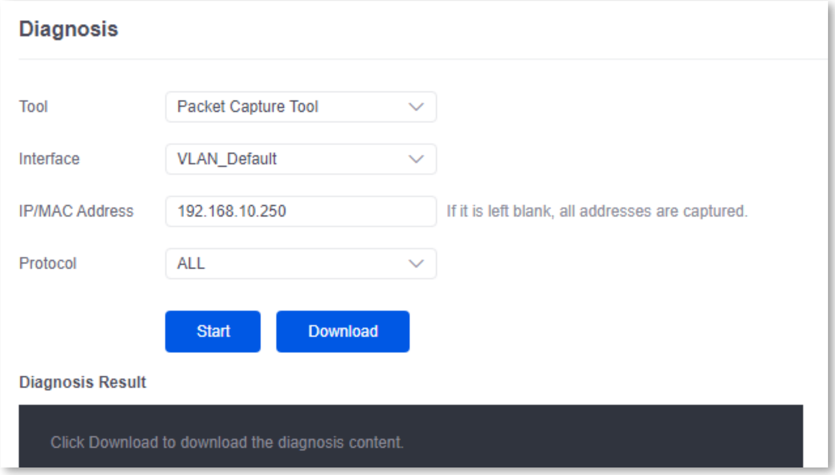
Interface: VLAN_Default

IP/MAC Address: 192.168.10.250 If it is left blank, all addresses are captured.

Protocol: ALL

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**).



Diagnosis

Tool: Packet Capture Tool

Interface: VLAN_Default

IP/MAC Address: 192.168.10.250 If it is left blank, all addresses are captured.

Protocol: ALL

Diagnosis Result

Click Download to download the diagnosis content.

---End

Parameter description

Parameter	Description
Interface	Specifies the VLAN interface whose data will be intercepted.

Parameter	Description
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.

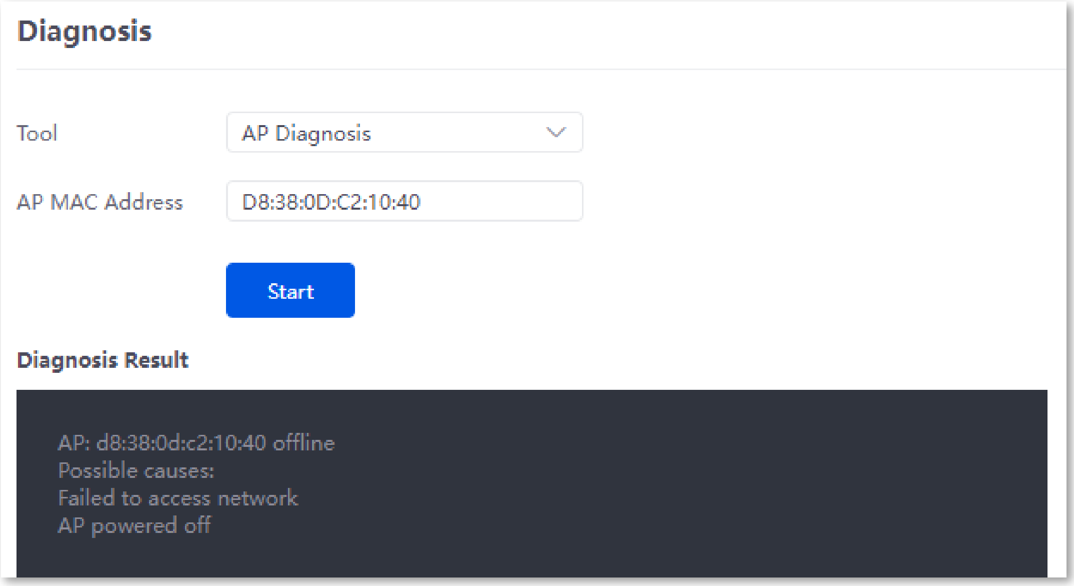
10.2.4 AP diagnosis

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.



```
AP: d8:38:0d:c2:10:40 offline
Possible causes:
Failed to access network
AP powered off
```

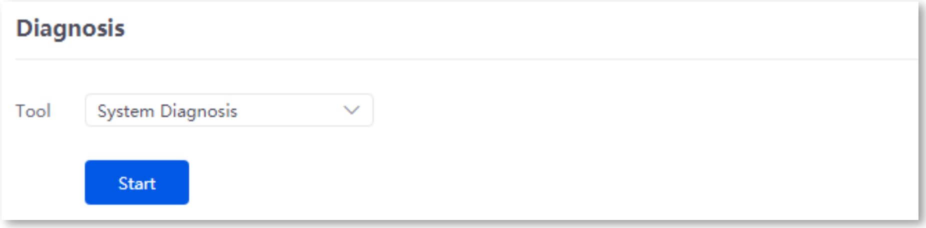
---End

10.2.5 System diagnosis

You can view the status information of all processes in the system.

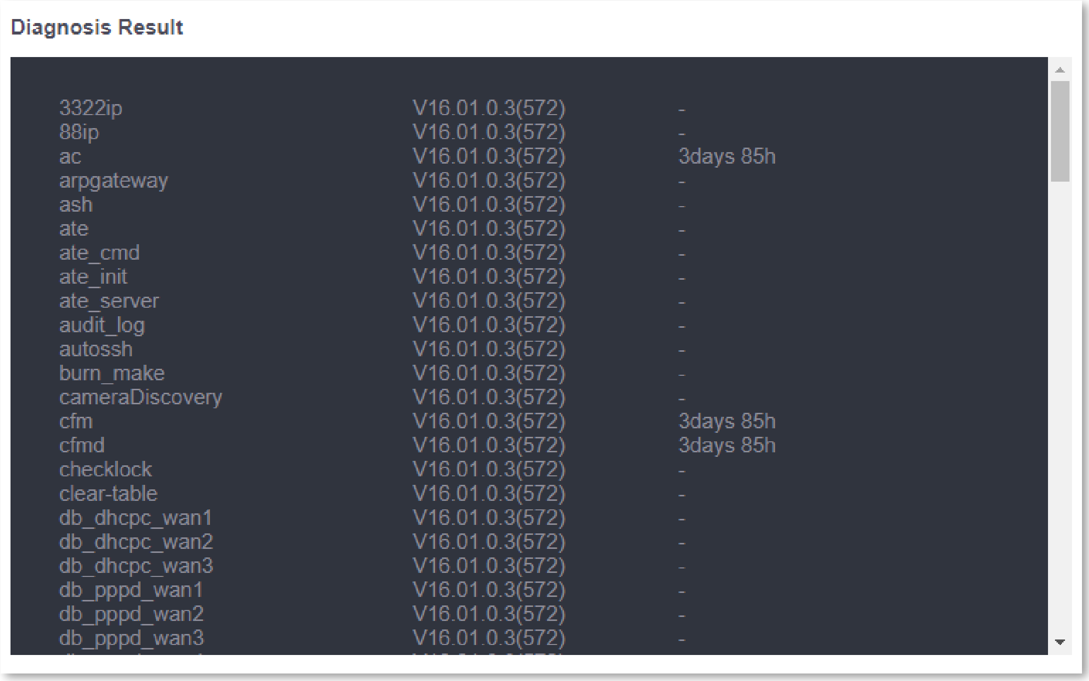
To perform system diagnosis:

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.



Diagnosis Result

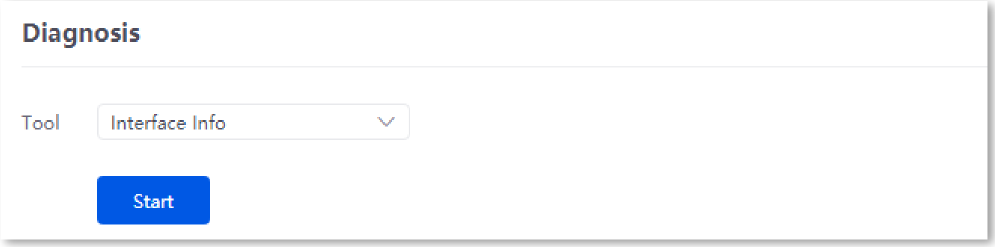
```
3322ip               V16.01.0.3(572)     -
88ip                 V16.01.0.3(572)     -
ac                   V16.01.0.3(572)     3days 85h
arpgateway           V16.01.0.3(572)     -
ash                  V16.01.0.3(572)     -
ate                  V16.01.0.3(572)     -
ate_cmd              V16.01.0.3(572)     -
ate_init             V16.01.0.3(572)     -
ate_server           V16.01.0.3(572)     -
audit_log            V16.01.0.3(572)     -
autossh              V16.01.0.3(572)     -
burn_make            V16.01.0.3(572)     -
cameraDiscovery      V16.01.0.3(572)     -
cfm                  V16.01.0.3(572)     3days 85h
cfmd                 V16.01.0.3(572)     3days 85h
checklock            V16.01.0.3(572)     -
clear-table          V16.01.0.3(572)     -
db_dhcpc_wan1        V16.01.0.3(572)     -
db_dhcpc_wan2        V16.01.0.3(572)     -
db_dhcpc_wan3        V16.01.0.3(572)     -
db_pppd_wan1         V16.01.0.3(572)     -
db_pppd_wan2         V16.01.0.3(572)     -
db_pppd_wan3         V16.01.0.3(572)     -
```

10.2.6 Interface info

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**.

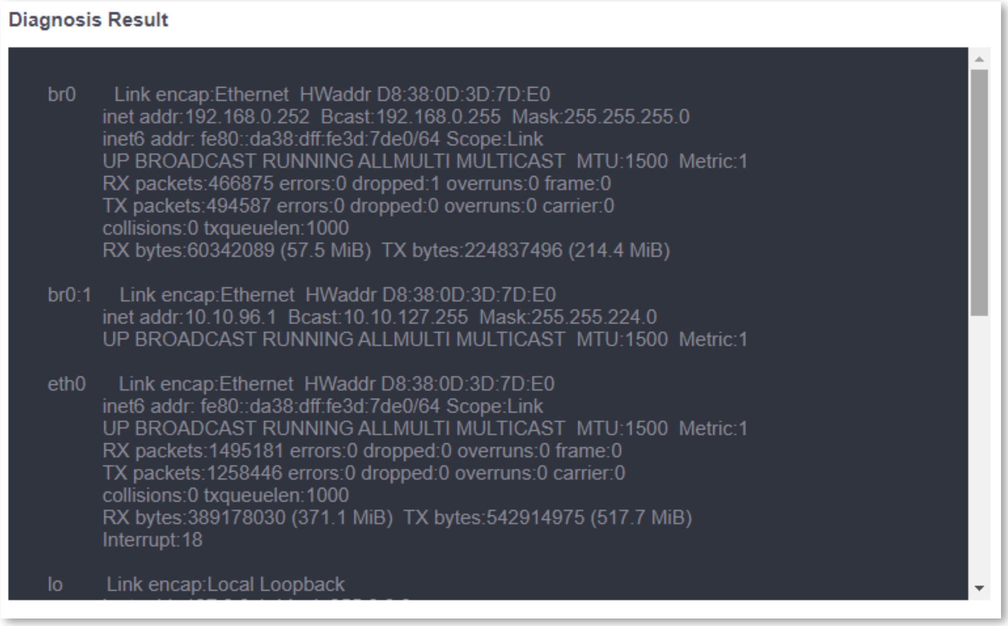


Diagnosis

Tool: Interface Info

---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.



Diagnosis Result

```
br0       Link encap:Ethernet  HWaddr D8:38:0D:3D:7D:E0
          inet addr:192.168.0.252  Bcast:192.168.0.255  Mask:255.255.255.0
          inet6 addr: fe80::da38:dff:fe3d:7de0/64 Scope:Link
          UP BROADCAST RUNNING ALLMULTI MULTICAST  MTU:1500  Metric:1
          RX packets:466875 errors:0 dropped:1 overruns:0 frame:0
          TX packets:494587 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:60342089 (57.5 MiB)  TX bytes:224837496 (214.4 MiB)

br0:1     Link encap:Ethernet  HWaddr D8:38:0D:3D:7D:E0
          inet addr:10.10.96.1  Bcast:10.10.127.255  Mask:255.255.224.0
          UP BROADCAST RUNNING ALLMULTI MULTICAST  MTU:1500  Metric:1

eth0      Link encap:Ethernet  HWaddr D8:38:0D:3D:7D:E0
          inet6 addr: fe80::da38:dff:fe3d:7de0/64 Scope:Link
          UP BROADCAST RUNNING ALLMULTI MULTICAST  MTU:1500  Metric:1
          RX packets:1495181 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1258446 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:389178030 (371.1 MiB)  TX bytes:542914975 (517.7 MiB)
          Interrupt:18

lo        Link encap:Local Loopback
```

10.3 Log center

Log in to the web UI of the router, and navigate to **Tool** > **Log Center** to enter the page. On this page, you can view the log information recorded by the router.

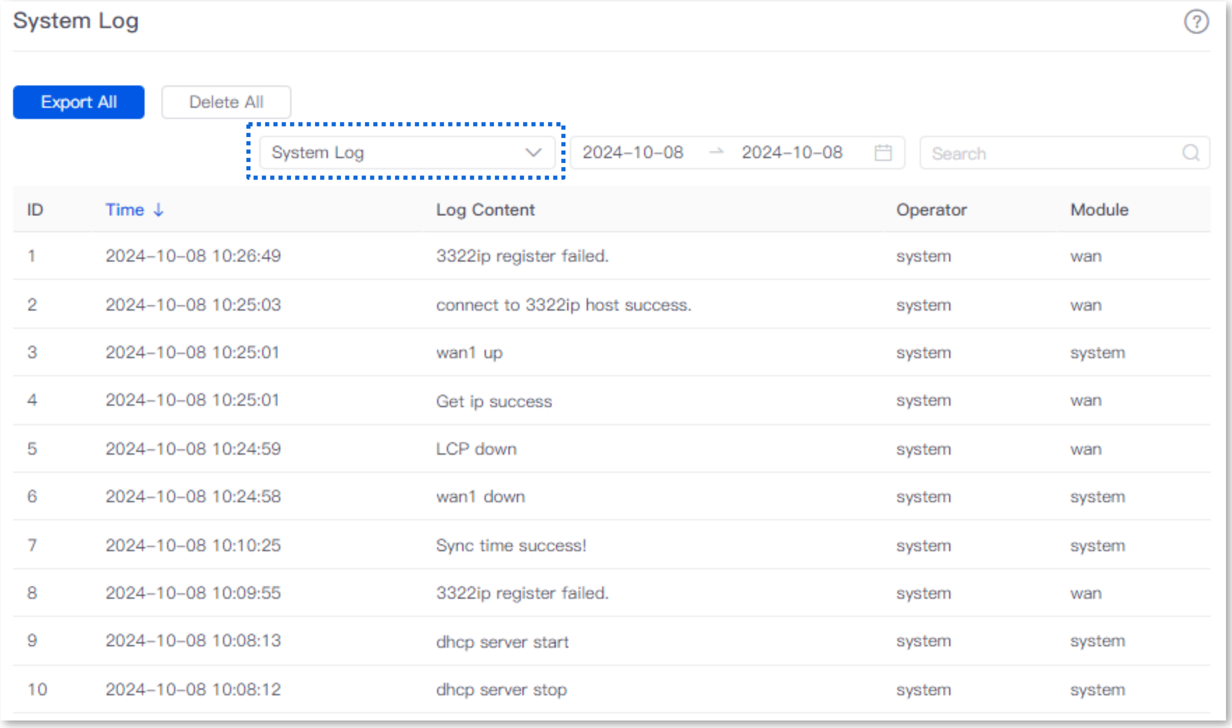
The log center records the **System Log**, **Operating Log** and **Running Log** of the router. In case of network failure, you can use the router's log center to troubleshoot the problem.

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

10.3.1 System log

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

Click the drop-down list box on this page. You can view certain log information of the router.

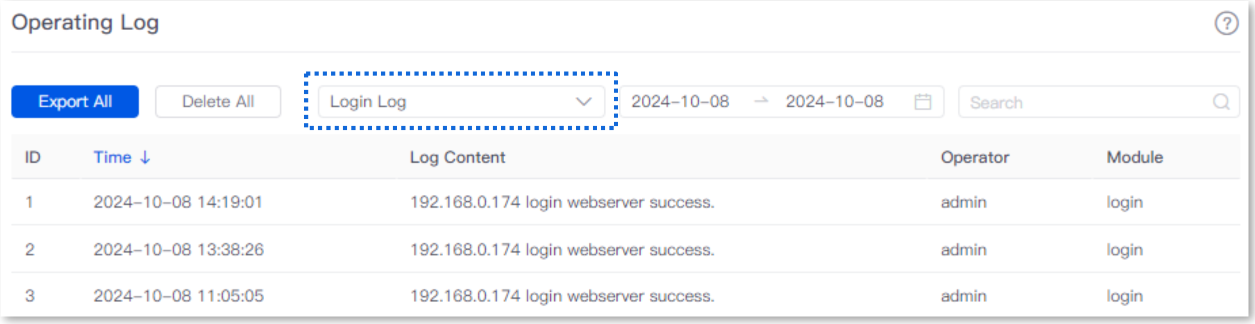

System Log

ID	Time ↓	Log Content	Operator	Module
1	2024-10-08 10:26:49	3322ip register failed.	system	wan
2	2024-10-08 10:25:03	connect to 3322ip host success.	system	wan
3	2024-10-08 10:25:01	wan1 up	system	system
4	2024-10-08 10:25:01	Get ip success	system	wan
5	2024-10-08 10:24:59	LCP down	system	wan
6	2024-10-08 10:24:58	wan1 down	system	system
7	2024-10-08 10:10:25	Sync time success!	system	system
8	2024-10-08 10:09:55	3322ip register failed.	system	wan
9	2024-10-08 10:08:13	dhcp server start	system	system
10	2024-10-08 10:08:12	dhcp server stop	system	system

10.3.2 Operating log

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

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

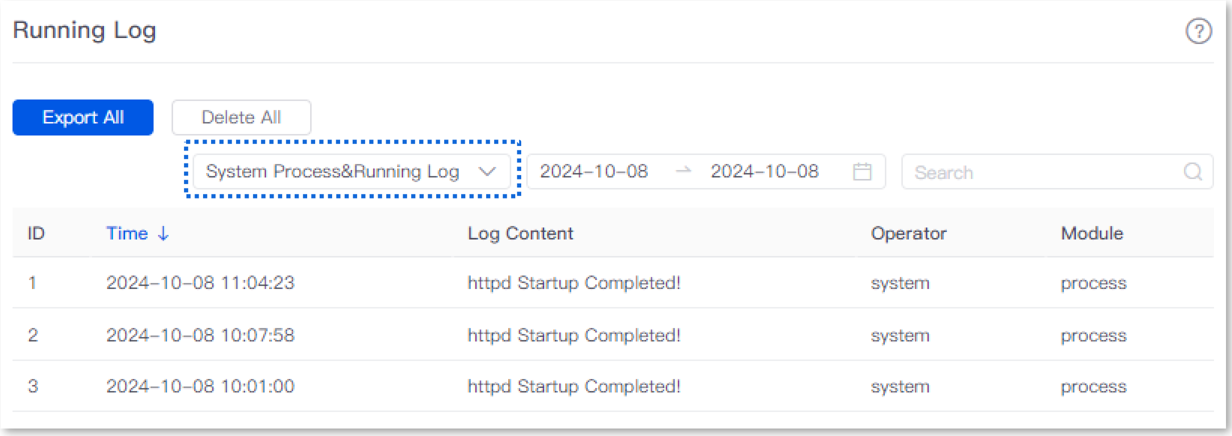

Operating Log

ID	Time ↓	Log Content	Operator	Module
1	2024-10-08 14:19:01	192.168.0.174 login webserver success.	admin	login
2	2024-10-08 13:38:26	192.168.0.174 login webserver success.	admin	login
3	2024-10-08 11:05:05	192.168.0.174 login webserver success.	admin	login

10.3.3 Running log

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

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.

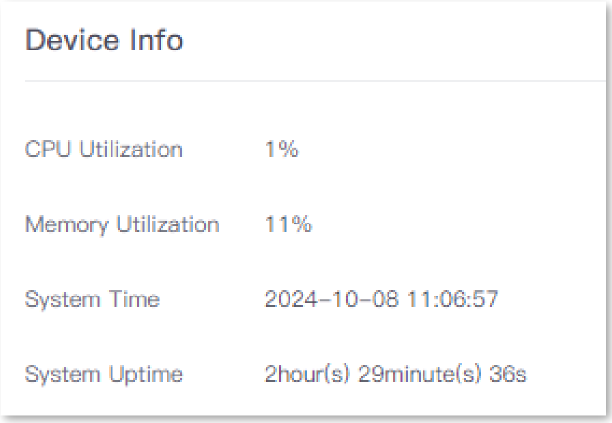


ID	Time ↓	Log Content	Operator	Module
1	2024-10-08 11:04:23	httpd Startup Completed!	system	process
2	2024-10-08 10:07:58	httpd Startup Completed!	system	process
3	2024-10-08 10:01:00	httpd Startup Completed!	system	process

10.4 Maintenance

10.4.1 Device information

Log in to the web UI of the router, and 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.



CPU Utilization	1%
Memory Utilization	11%
System Time	2024-10-08 11:06:57
System Uptime	2hour(s) 29minute(s) 36s

10.4.2 Restore & Backup

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.

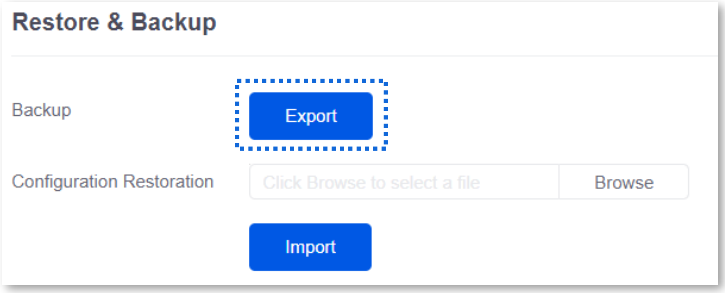
You are recommended to back up the configuration after it is significantly changed. When the performance of your router decreases because of an improper configuration, or after you restore the router to factory settings, you can use this function to restore the configuration that has been backed up.

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

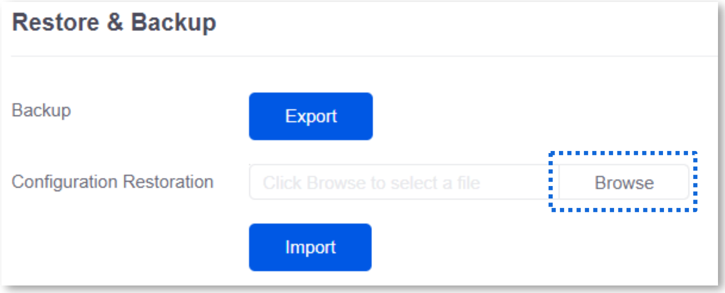
If the message “This type of file can harm your computer. Do you want to keep RouterCfm.cfg anyway?” appears on the page, click “Keep”.

Restore

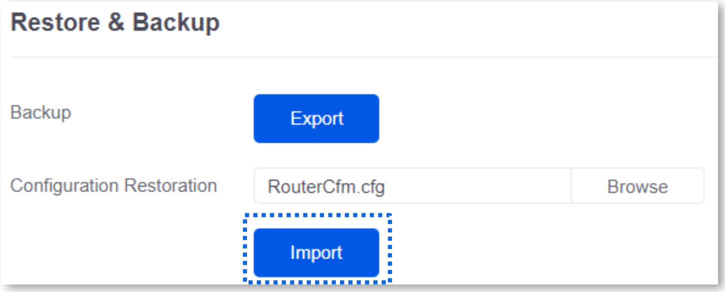
1. Log in to the web UI of the router.

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.

10.4.3 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

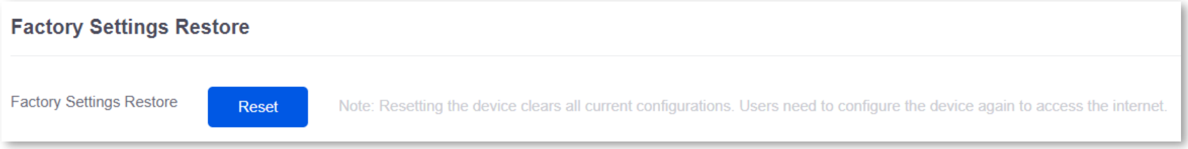
After the reset, the default LAN IP address of the router is 192.168.0.252.

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**.



Factory Settings Restore

Factory Settings Restore Reset Note: Resetting the device clears all current configurations. Users need to configure the device again to access the internet.

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 blinks, 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 lights solid green. When the **SYS** LED indicator blinks again, the router is reset successfully.

10.5 Upgrade service

10.5.1 Overview

Log in to the web UI of the router, and 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**.

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 suffixed with **.bin**.

Parameter	Description
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.

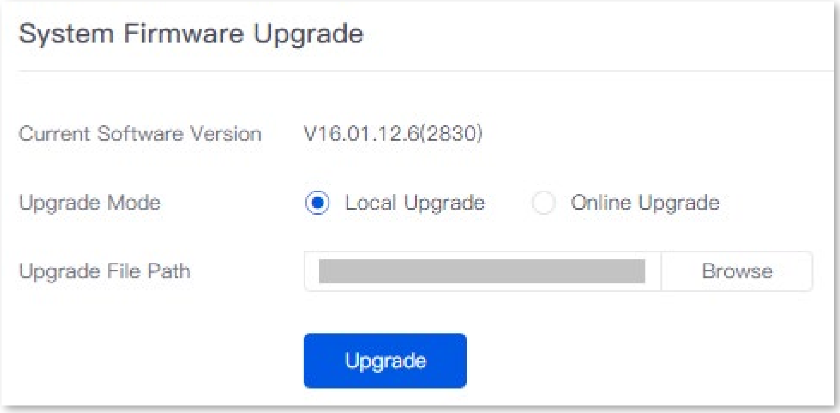
10.5.2 System firmware upgrade

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.

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**.



System Firmware Upgrade

Current Software Version V16.01.12.6(2830)

Upgrade Mode ● Local Upgrade ○ Online Upgrade

Upgrade File Path

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

---End

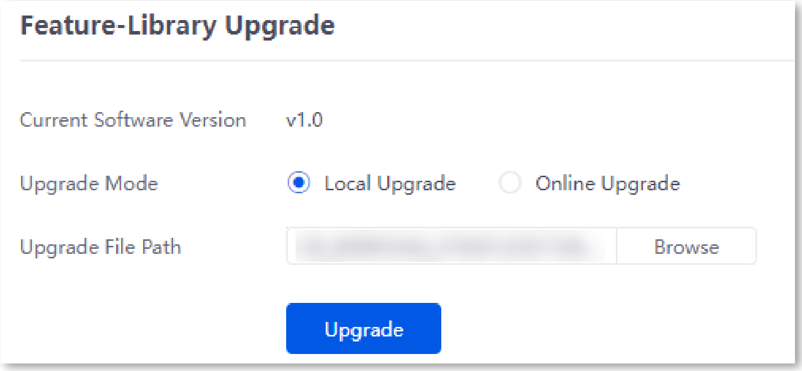
After the progress bar completes, you can log in to the router again and check whether **Current Software Version** in **Tool** > **Upgrade Service** > **System Firmware Upgrade** is the one that you upgraded. If yes, the upgrade is successful.

10.5.3 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.

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**.


Feature-Library Upgrade

Current Software Version v1.0

Upgrade Mode ● Local Upgrade ○ Online Upgrade

Upgrade File Path

---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.

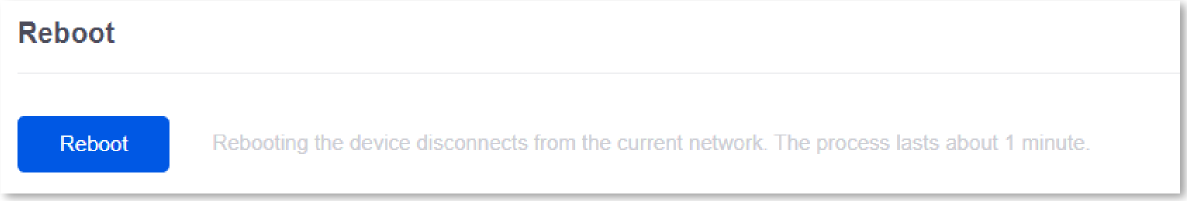
10.6 Reboot services

10.6.1 Reboot

You can reboot the router to 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:

Log in to the web UI of the router, and navigate to **Tool** > **Reboot Services** > **Reboot**, and click **Reboot**.



Reboot

Reboot

Rebooting the device disconnects from the current network. The process lasts about 1 minute.

10.6.2 Scheduled reboot

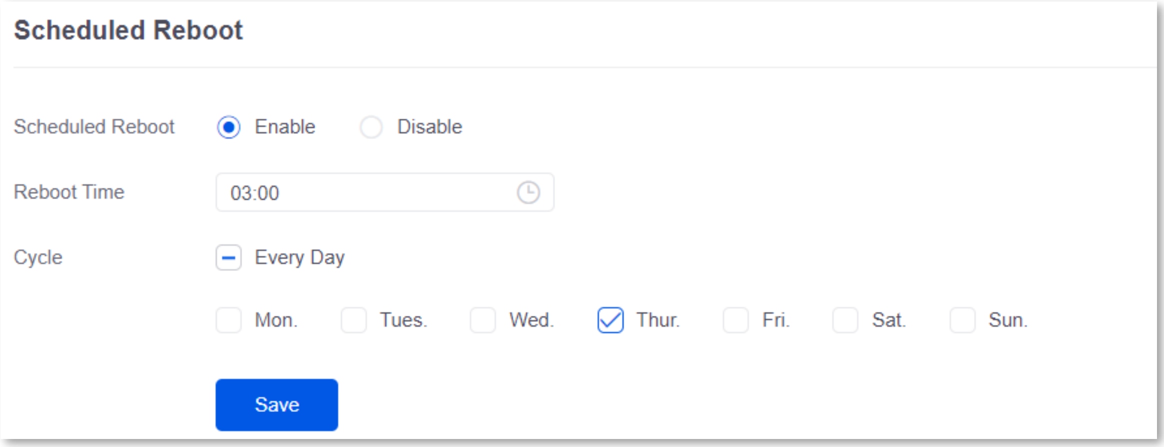
By setting the router to reboot periodically during leisure time, you can prevent the decreasing of performance and instability of the router after running for a long period.

Tip

The time of reboot depends on the system time of the router. To ensure 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. Enable the **Scheduled Reboot** function.
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**.



Scheduled Reboot

Scheduled Reboot ● Enable ○ Disable

Reboot Time 03:00

Cycle ⊟ Every Day

□ Mon. □ Tues. □ Wed. ☑ Thur. □ Fri. □ Sat. □ Sun.

Save

---End

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

10.7 Network diagnosis

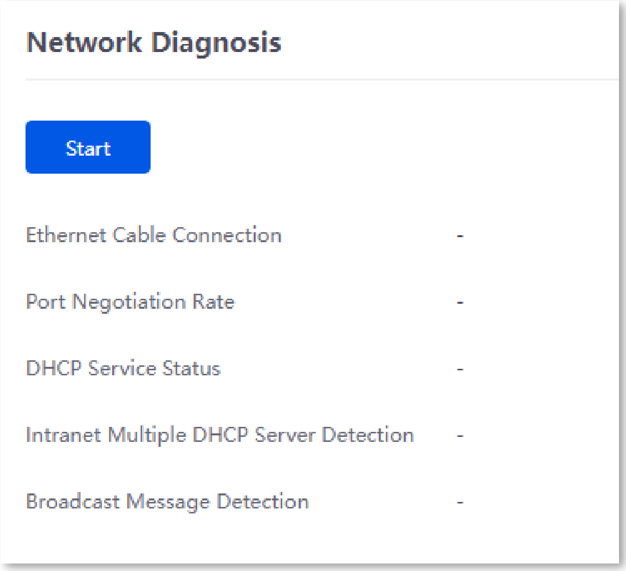
10.7.1 Configure network diagnosis

Log in to the web UI of the router, and navigate to **Tool** > **Network Diagnosis** > **Network Diagnosis** to enter the page.

On this page, you can detect the network status of the router. If a network abnormality is detected, it will be reported to the network monitoring logs.

Note

After **Start** is clicked, the process may last for a period of time and cannot be paused or ended manually. Operate during idle periods.



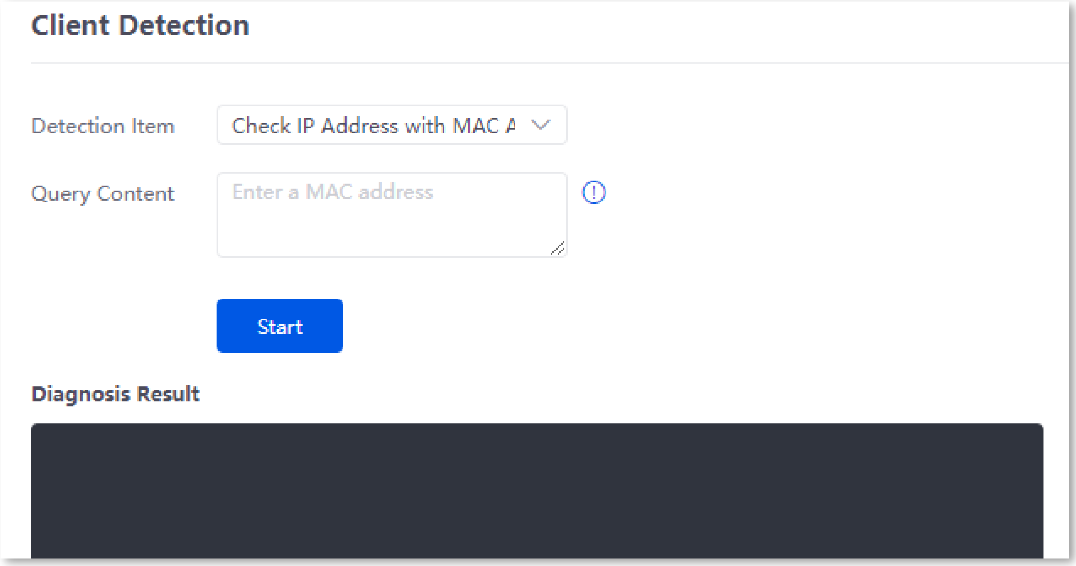
Network Diagnosis

Ethernet Cable Connection	-
Port Negotiation Rate	-
DHCP Service Status	-
Intranet Multiple DHCP Server Detection	-
Broadcast Message Detection	-

10.7.2 Client detection

Log in to the web UI of the router, and navigate to **Tool** > **Network Diagnosis** > **Client Detection** to enter the page.

On this page, you can check the IP address of a client through its MAC address. The following figure is for reference only.



Client Detection

Detection Item: Check IP Address with MAC A

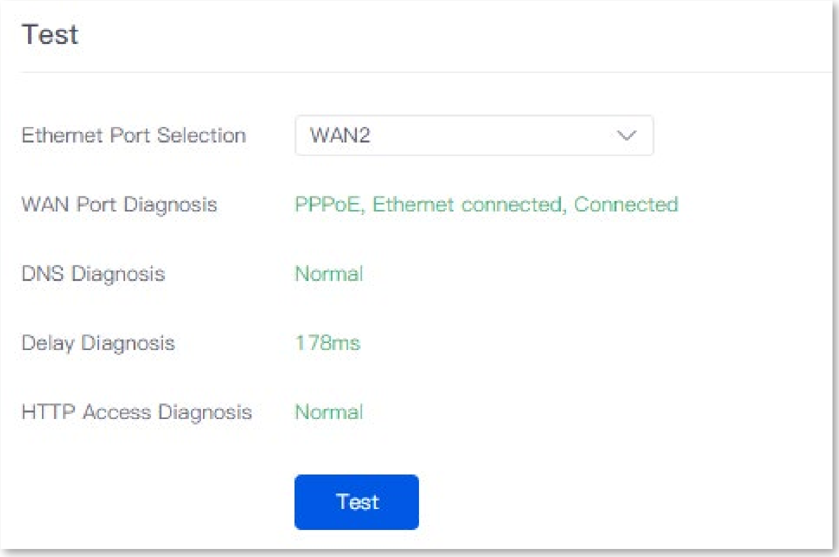
Query Content: Enter a MAC address

Diagnosis Result

10.7.3 WAN port diagnosis

Log in to the web UI of the router, and navigate to **Tool** > **Network Diagnosis** > **WAN Port Diagnosis**.

On this page, you can perform a network test on the WAN port of the router.



Test

Ethernet Port Selection: WAN2

WAN Port Diagnosis: PPPoE, Ethernet connected, Connected

DNS Diagnosis: Normal

Delay Diagnosis: 178ms

HTTP Access Diagnosis: Normal

Parameter description

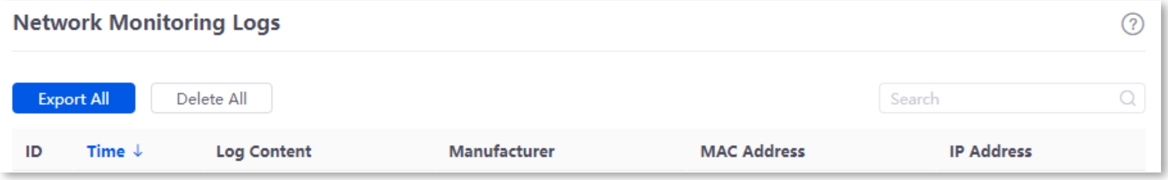
Parameter	Description
Ethernet Port Selection	Specifies the WAN port to be tested.
WAN Port Diagnosis	Used to test the WAN port's connection type, Ethernet cable connection status and internet connection status.
DNS Diagnosis	Used to test whether the WAN port can resolve the domain name properly.

Parameter	Description
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.

10.7.4 Network monitoring logs

Log in to the web UI of the router, and navigate to **Tool** > **Network Diagnosis** > **Network Monitoring Logs**.

On this page, you can check the network monitoring logs recorded by the router on this page. If the network is faulty, you can perform troubleshooting using these logs.


Network Monitoring Logs

ID	Time ↓	Log Content	Manufacturer	MAC Address	IP Address

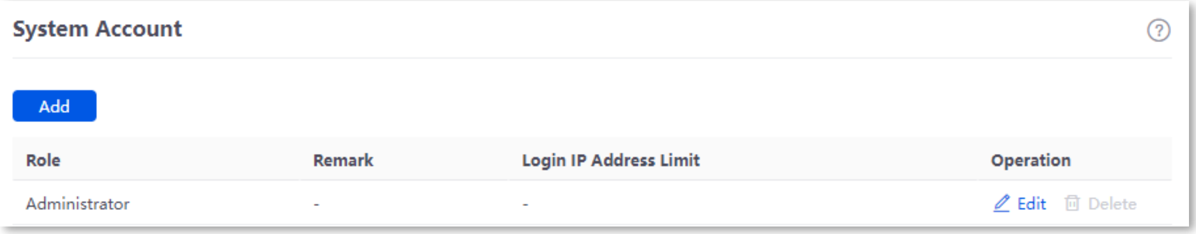
Parameter description

Parameter	Description
Time	Specifies the time when the log is generated.
Log Content	Specifies the content of the abnormal log.
Manufacturer	Specifies the manufacturer of the DHCP server detected in the LAN.
MAC Address	Specifies the MAC address of the DHCP server detected in the LAN.
IP Address	Specifies the IP address of the DHCP server detected in the LAN.

10.8 System account

Log in to the web UI of the router, and navigate to **Tool** > **System Account** to enter the page.

On this page, you can add, modify or delete the administrator and visitor accounts.


System Account

Role	Remark	Login IP Address Limit	Operation
Administrator	-	-	Edit Delete

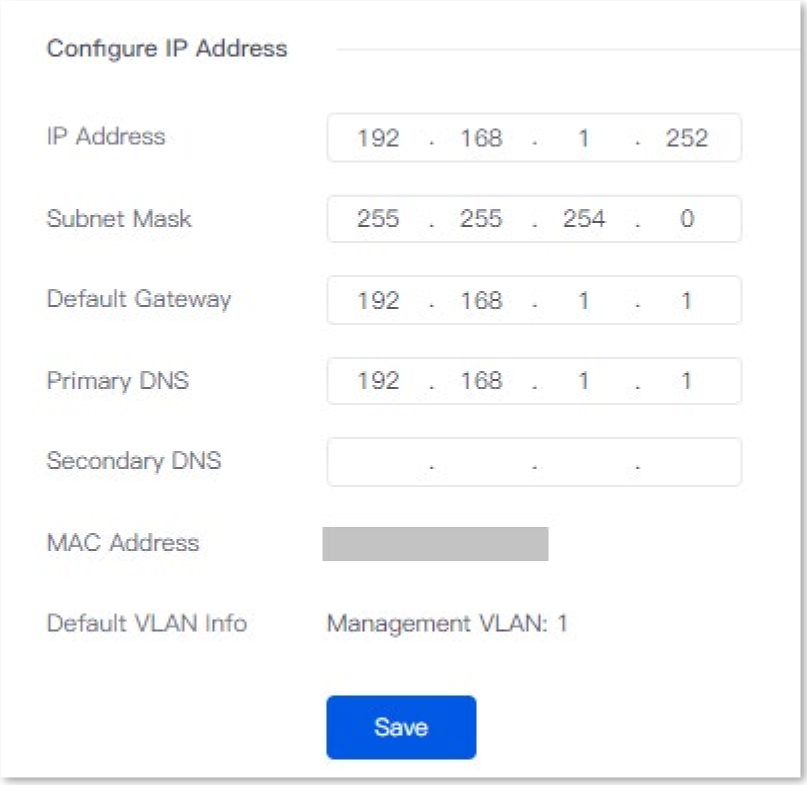
Parameter description

Parameter	Description
Role	Specifies the user role in managing the web UI. There is an administrator account by default. The operation authority of corresponding user roles is described as follows: – **Administrator**: Able to view and configure all functions of the router. – **Visitor**: Only able to view configurations of the router except system account information.
Password	Used to set the login password of the account.
Confirm Password	
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 is completed, only users with the IP address or within the IP address range can use the account to access the web UI.

Appendix

A.1 Connect the router in Pure AC mode

1. Log in to the web UI in Pure AC mode.
2. Navigate to **Network** > **LAN Settings**, on the **Configure IP Address** module, configure the LAN port information of the router and click **Save**. The following figure is for reference only.
   1) Set **IP Address** of the router to one on the same network segment as the LAN IP address of the gateway, and is not occupied by other devices.
   2) Retain **Subnet Mask** to default settings, which is **255.255.254.0**.
   3) Set **Default Gateway** to the LAN IP address of the gateway.
   4) Set **Primary DNS** to the correct IP address of DNS server or DNS proxy.

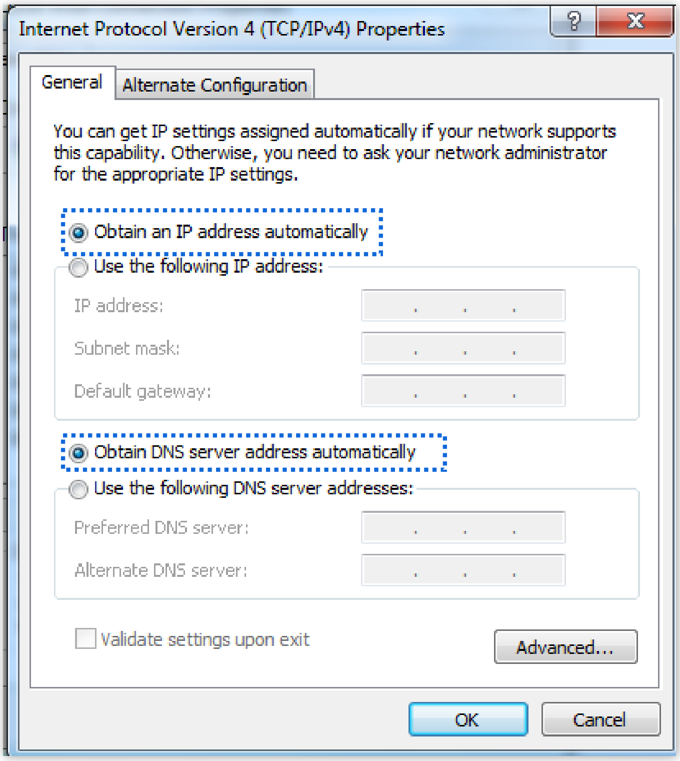


Configure IP Address

IP Address	192 . 168 . 1 . 252
Subnet Mask	255 . 255 . 254 . 0
Default Gateway	192 . 168 . 1 . 1
Primary DNS	192 . 168 . 1 . 1
Secondary DNS	. . .
MAC Address	[redacted]
Default VLAN Info	Management VLAN: 1

---End

To log in to the web UI of the router, set the management computer to **Obtain an IP address automatically** and **Obtain DNS server address automatically**.


Internet Protocol Version 4 (TCP/IPv4) Properties

General | Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address:

Subnet mask:

Default gateway:

● Obtain DNS server address automatically

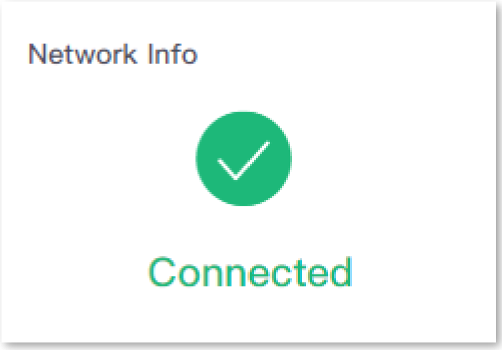
○ Use the following DNS server addresses:

Preferred DNS server:

Alternate DNS server:

□ Validate settings upon exit

Start a web browser and enter the newly set IP address in the address bar to log in to the web UI of the router again. In the **Network Info** module of the **System** page, you can view that the router is connected to the internet.


Network Info

Connected

A.2 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
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
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
FQDN	Fully Qualified Domain Name

Acronym or Abbreviation	Full Spelling
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
ISP	Internet Service Provider
L2TP	Layer 2 Tunneling Protocol
LAN	Local Area Network
LCP	Link Control Protocol
LED	Light Emitting Diode
MAC	Medium Access Control
MPDU	MAC Protocol Data Unit
MPPE	Microsoft Point-to-Point Encryption
MSDU	MAC Service Data Unit
MTU	Maximum Transmission Unit
NAT	Network Address Translation
NTS	Network time server
PAP	Password Authentication Protocol
PFS	Perfect Forward Secrecy

Acronym or Abbreviation	Full Spelling
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
RTS	Request to Send
RX	Receive
SA	Security Association
SDN	Software Defined Network
SLAAC	Stateless Address Autoconfiguration
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
SN	Serial Number
SNMP	Simple Network Management Protocol
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

Acronym or Abbreviation	Full Spelling
URL	Uniform Resource Locator
USB	Universal Serial Bus
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