www.ip-com.com.cn

User Guide

Multi-WAN Hotspot Router M80

IP-COM
World Wide Wireless

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

Thank you for purchasing IP-COM Multi-WAN Hotspot Router! This user guide helps you configure, manage and maintain the product.

Conventions

This user guide is applicable to IP-COM Multi-WAN Hotspot Router M80.

Unless otherwise specified, “router”, "this router", “product”, or “device” mentioned in this user guide indicates M80.

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

Item	Presentation	Example
Menu	Bold	**System** indicates the "System" menu.
Cascading menus	>	Choose **System** > **Live Users**.

Symbols in this user guide:

Item	Meaning
	This format is used to highlight information of importance or special interest. Ignoring this type of note may result in ineffective configurations, loss of data or damage to device.
	This format is used to highlight a procedure that will save time or resources.

Acronyms and Abbreviations

Acronym or Abbreviation	Full Spelling
ISP	Internet Service Provider
AP	Access Point
DDNS	Dynamic Domain Name System
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone
DNS	Domain Name System

Acronym or Abbreviation	Full Spelling
L2TP	Layer 2 Tunneling Protocol
PPP	Point To Point Protocol
PPPoE	Point-to-Point Protocol over Ethernet
PPTP	Point to Point Tunneling Protocol
SSID	Service Set Identifier
URL	Uniform Resource Locator
VLAN	Virtual Local Area Network
VPN	Virtual Private Network

For more documents

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

Technical support

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

Tel: (86 755) 2765 3089 E-mail: info@ip-com.com.cn Website: http://www.ip-com.com.cn

Contents

1 Product overview

This chapter describes:

1.1 Overview

IP-COM Multi-WAN Hotspot Router M80 is designed for small-and-medium-sized enterprises to implement intelligent network access and management. It supports an AP management system and a multi-authentication management system, and supports various enterprise-oriented functions including filter management, smart bandwidth control, PPTP/L2TP/IPSec VPN, USB sharing and multi-WAN.

1.2 Main features

AP management system

The router is embedded with an AP management system, which is applicable to all IP-COM AP models. Using the system, you can customize SSIDs, transmit power, channels, user capacity, VLANs for APs.

Multiple authentication types

The router supports three authentication types, including captive portal, PPPoE authentication and WiFi via WeChat, letting you to deploy authentication system without investing an authentication server.

- Captive portal: A portal-based authentication mode, allowing you to push advertisement to users.
- PPPoE authentication: This authentication type allows you to establish PPPoE dial-in connections and manage traffic per account, thus effectively addressing network congestion at peak hours.
- WiFi via WeChat: A WeChat-based authentication mode, which allows users to be authenticated by WeChat to increase the number of WeChat fans and broaden your brand visibility.

Smart bandwidth control

This router supports automatic bandwidth control and manual bandwidth control.

- Automatic bandwidth control: Entering the actual bandwidth provided by your ISP, then leave intelligent bandwidth allocation to the router. That is, when the traffic is light, the router allows users to use excessive bandwidth; when the traffic is heavy, the router strictly controls bandwidth usage.
- Manual bandwidth control: You must specify the upper bandwidth limit per accessing equipment and the router controls bandwidth usage accordingly.

VLAN

Compliant with 802.1Q VLAN, the router supports to divide users into different VLANs (max. 15 VLAN policies) to prevent broadcast storm. In a network, it oftently works with devices compliant with IEEE 802Q VLAN, such as switches.

Filter management

This router allows you to control internet and website access of connected devices based on IP groups and time groups. You can either use the pre-defined websites, or manually add URLs.

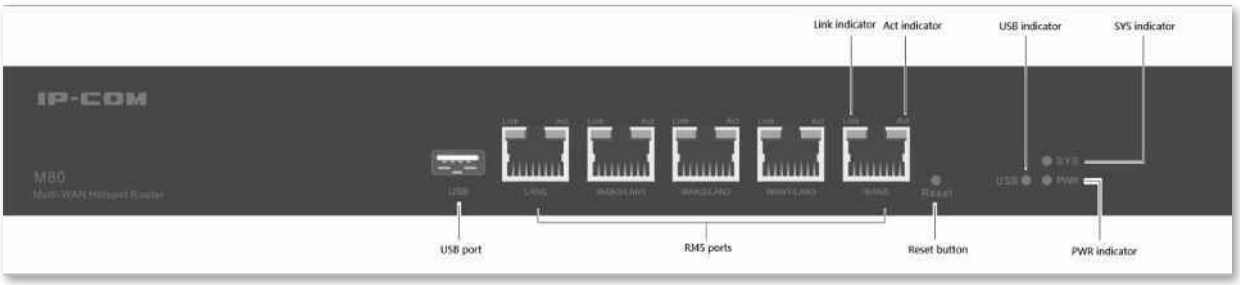
Other useful functions

- VPN: This function enables you to quickly set up IPsec, PPTP, and L2TP VPNs to facilitate remote access to internal resources.
- Multi-WAN: This function allows a maximum of four ISP network connections.
- USB sharing: This function allows USB file sharing to deploy simple enterprise shared file servers.
- Any IP: This function allows all hosts with any IP address on a LAN to access the internet.

1.3 Appearance

1.3.1 Front panel

The front panel includes 13 LED indicators, 1 USB port, 5 RJ45 ports, and 1 RESET button. See the following figure.



LED indicators

There are 1 power (PWR) LED indicator, 1 system (SYS) LED indicator and 1 USB LED indicator. Each RJ45 port has 1 Link LED indicator and 1 Act LED indicator.

LED indicator	Status	Description
PWR	Solid	Power supply is normal.
	Off	Power supply is disconnected or fails.
SYS	Blinking	The system is working properly.
	Solid	The system is faulty.
	Off	System has not completed startup.
USB	Solid	USB port is connected to an USB device.
	Blinking	Reading and writing operation is being done to the USB device.
	Off	USB port is disconnected or the connection is faulty.
Link	Solid	The port is connected.
	Off	The port is not connected or the connection is faulty.
Act	Solid	The port is not transmitting or receiving data.
	Blinking	The port is transmitting or receiving data.

USB port

M80 provides 1 USB port and allows you to share files by plugging USB flash disks, mobile HDDs into it.

RJ45 ports

M80 provides five 10/100/1000 Mbps auto-negotiation RJ45 ports. Each RJ45 port has 1 Link LED indicator and 1 Act LED indicator.

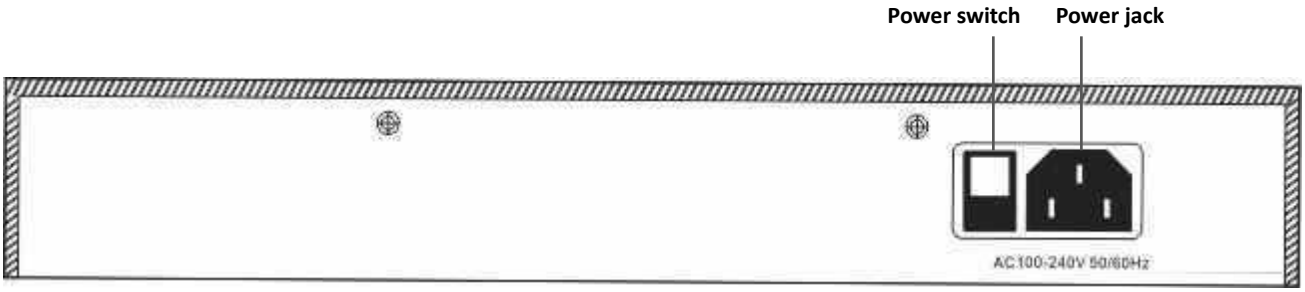
The 5 RJ45 ports include 1 LAN port, 1 WAN port, and 3 WAN/LAN ports. You can set the WAN/LAN ports as LAN or WAN ports as required. By default, the 2 rightmost ports are WAN ports, while the 3 leftmost ports are LAN ports.

RESET button

This button allows you to restore the default factory settings of the router. To restore the settings, use a pin to hold down the button for about 8 seconds, then release, and wait about a minute. When the system (SYS) LED indicator blinks again, the router is restored successfully.

1.3.2 Rear panel

The rear panel includes 1 power switch and 1 power jack. See the following figure.



Power switch

It is used to turn on/off the router.

Power jack

It is used to connect to the power cable included power adapter to supply power to the router.

2 Quick setup

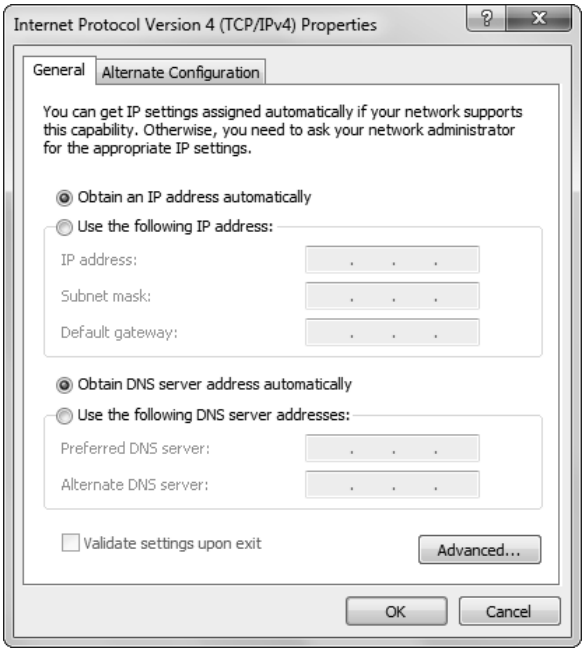
This chapter describes:

- Logging in to the router web UI
- Configuring the router

2.1 Logging in to the router web UI

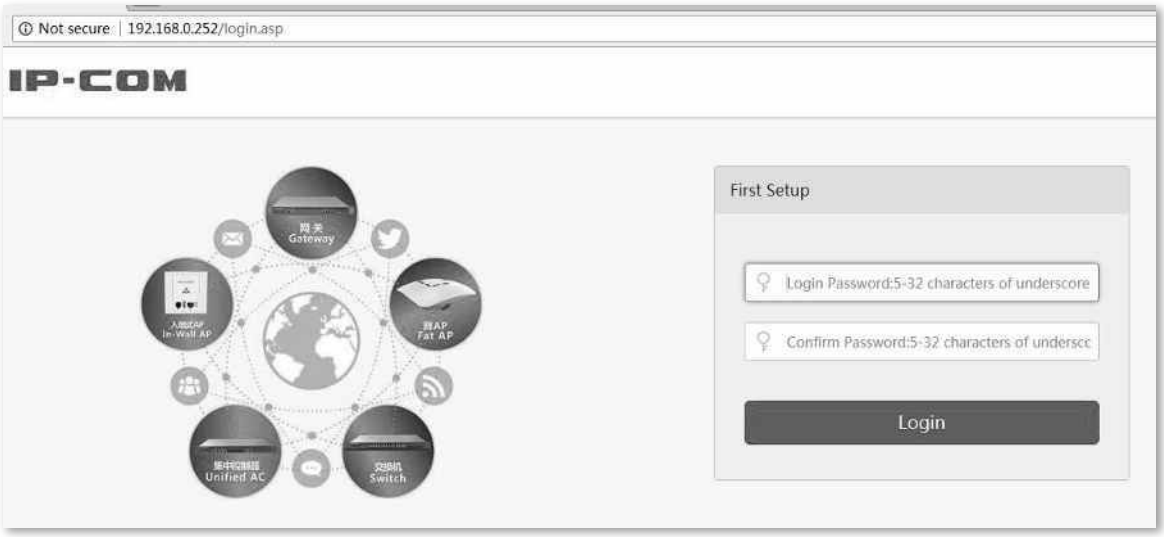
You can use a web browser to log in to the router web UI to perform management. To log in to the web UI, connect a computer to the router (or to a switch connected to the router) using an Ethernet cable and perform the following procedure:

1. Select **Obtain an IP address automatically** and **Obtain DNS server address automatically** options for the local connection.



2. Start a web browser and enter **192.168.0.252** in the address bar.

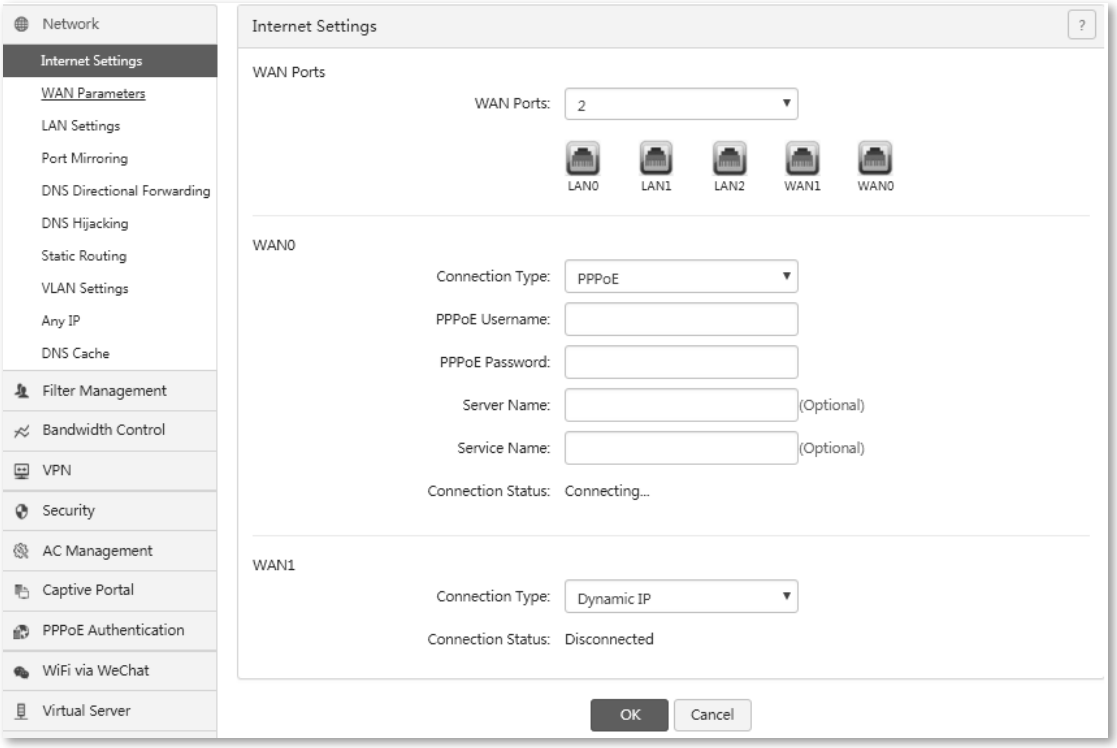
3. Set your login password, and click **Login**.



Note

If the page does not appear, refer to Q1 in Troubleshooting.

After logging in to the web UI, you can configure the router.



2.2 Configuring the router

The router supports three internet connection types. Refer to the following table, or consult your ISP to choose the proper one.

Internet Connection Type	Description
PPPoE	Your internet service provider (ISP) provides a user name and password.
Dynamic IP address	Your ISP provides no internet connection type information or dynamic IP address.
Static IP	Your ISP specifies internet connection information including a static IP address, a subnet mask, a default gateway, and DNS servers for you.

- By default, the router has two WAN ports: WAN0 and WAN1. This User Guide uses WAN0 to illustrate configuration procedures.
- By default, the WAN0 port uses PPPoE, while the WAN1 port uses dynamic IP address to access the internet.
- All parameters for internet access are provided by ISPs. If you are uncertain about the parameters, consult your ISP.

2.2.1 PPPoE

Choose **Network** > **Internet Settings**. The following figure shows the configuration page.

Perform the following procedure to configure your router to access the internet:

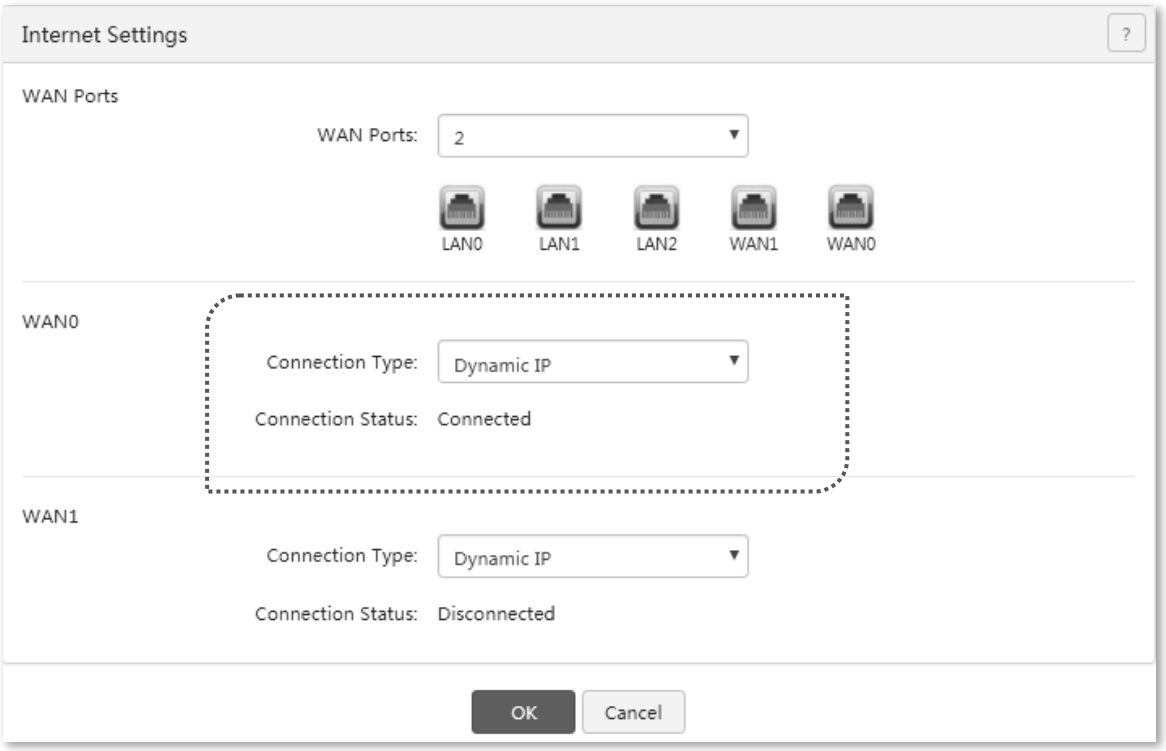
1. Set **Connection Type** to **PPPoE**.
2. Enter **PPPoE Username** and **PPPoE Password** provided by your ISP.
3. Click **OK**.

---End

Wait a moment. After **Connection Status** is changed to **Connected**, you can access the internet. If the internet is inaccessible, choose **Network** > **WAN Parameters**, and change WAN parameters to resolve the problem.

2.2.2 Dynamic IP

Choose **Network** > **Internet Settings**. The following figure shows the configuration page.



Perform the following procedure to configure an internet connection:

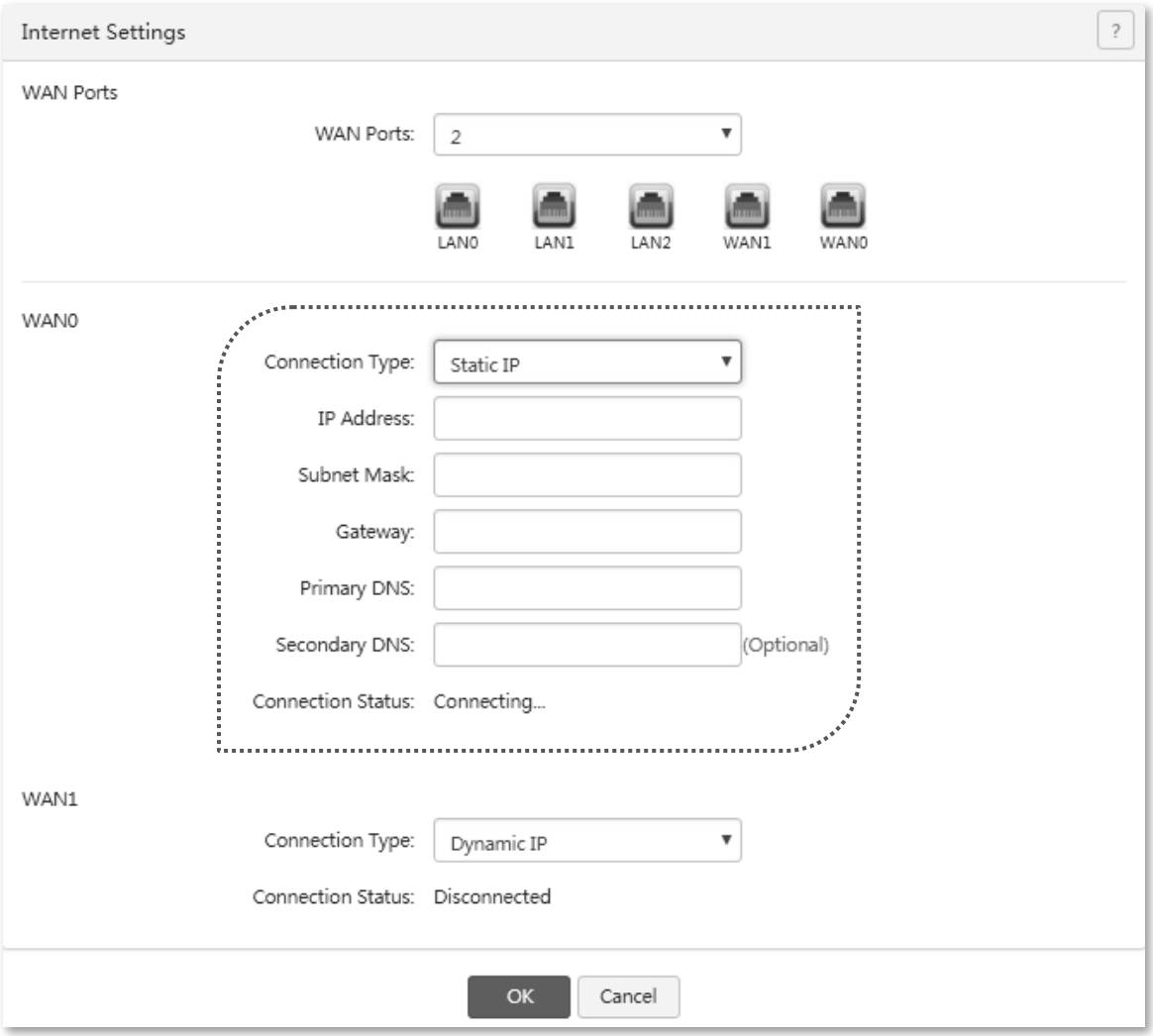
1. Set **Connection Type** to **Dynamic IP**.
2. Click **OK**.

---End

Wait a moment. After **Connection Status** is changed to **Connected**, you can access the internet. If the internet is inaccessible, choose **Network** > **WAN Parameters**, and change WAN parameters to resolve the problem.

2.2.3 Static IP

Choose **Network** > **Internet Settings**. The following figure shows the configuration page.



Perform the following procedure to configure an internet connection:

1. Set **Connection Type** to **Static IP**.
2. Set **IP Address**, **Subnet Mask**, **Gateway**, **Primary DNS**, and **Secondary DNS** provided by your ISP.
3. Click **OK**.

---End

Wait a moment. After **Connection Status** is changed to **Connected**, you can access the internet. If the internet is inaccessible, choose **Network** > **WAN Parameters**, and change WAN parameters to resolve the problem.

3 Login

This chapter describes:

- Logging in to the router web UI
- Logging out of the router web UI
- Web UI layout
- Common buttons on the web UI

3.1 Logging in to the router web UI

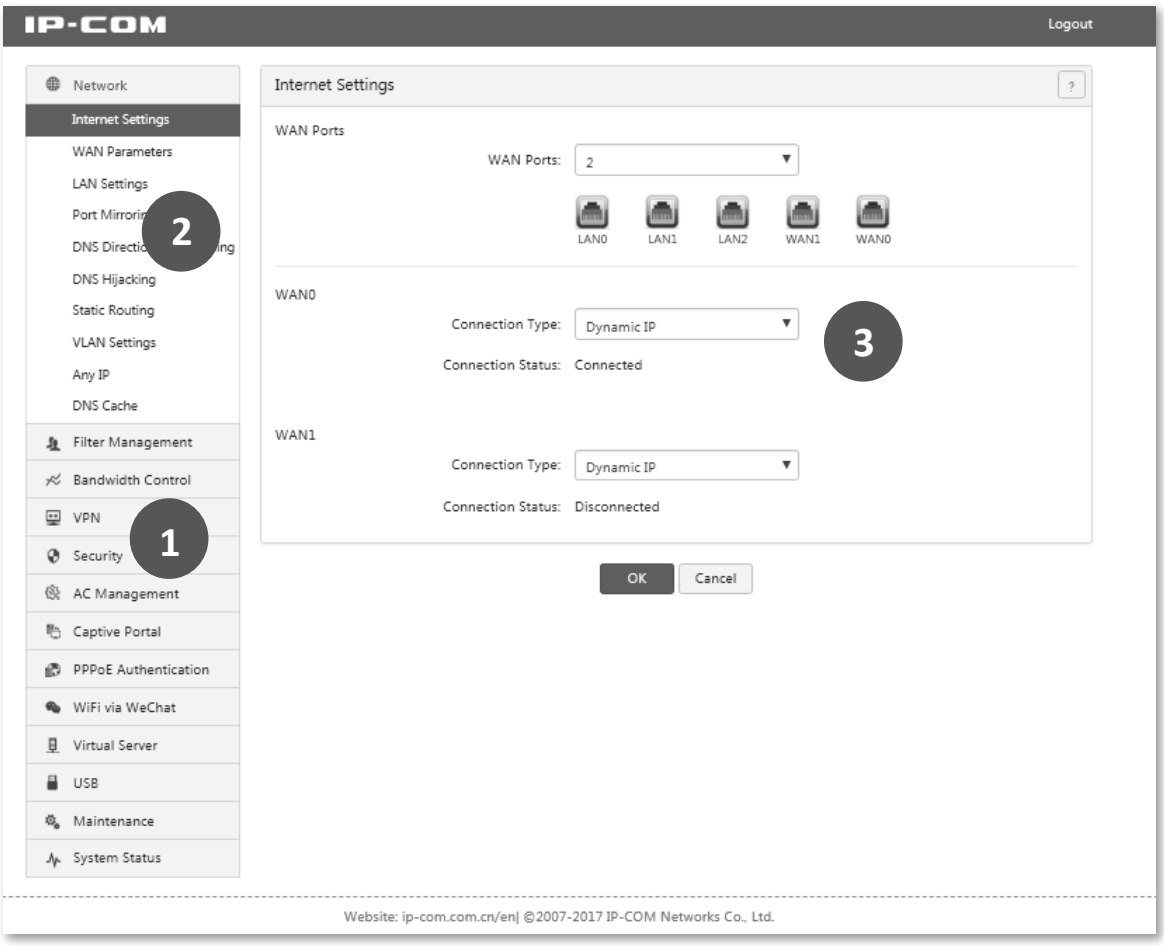
For details, see section 2.1 Logging in to the Router Web UI.

3.2 Logging out of the router web UI

After you log in to the router web UI, the system will log you out if you do not perform any operation within 5 minutes. To log out yourself, click **Logout** in the upper-right corner.

3.3 Web UI layout

The web UI is divided into the level-1 navigation bar, level-2 navigation bar, and configuration area. See the following figure.



SN	Area	Description
❶	Level-1 navigation bar	The navigation bars display router menus. You can easily access functions by choosing items of the menus. When you choose a menu item, information corresponding to the menu item appears in the configuration area.
❷	Level-2 navigation bar	
❸	Configuration area	The configuration area enables you to set or view parameters.

3.4 Common buttons on the web UI

The following table describes the common management buttons.

Button	Description
OK	It is used to save the settings on the current page and enable the settings to take effect.
Cancel	It is used to cancel the settings on the current page and restore the original settings.
?	It provides detailed online help.

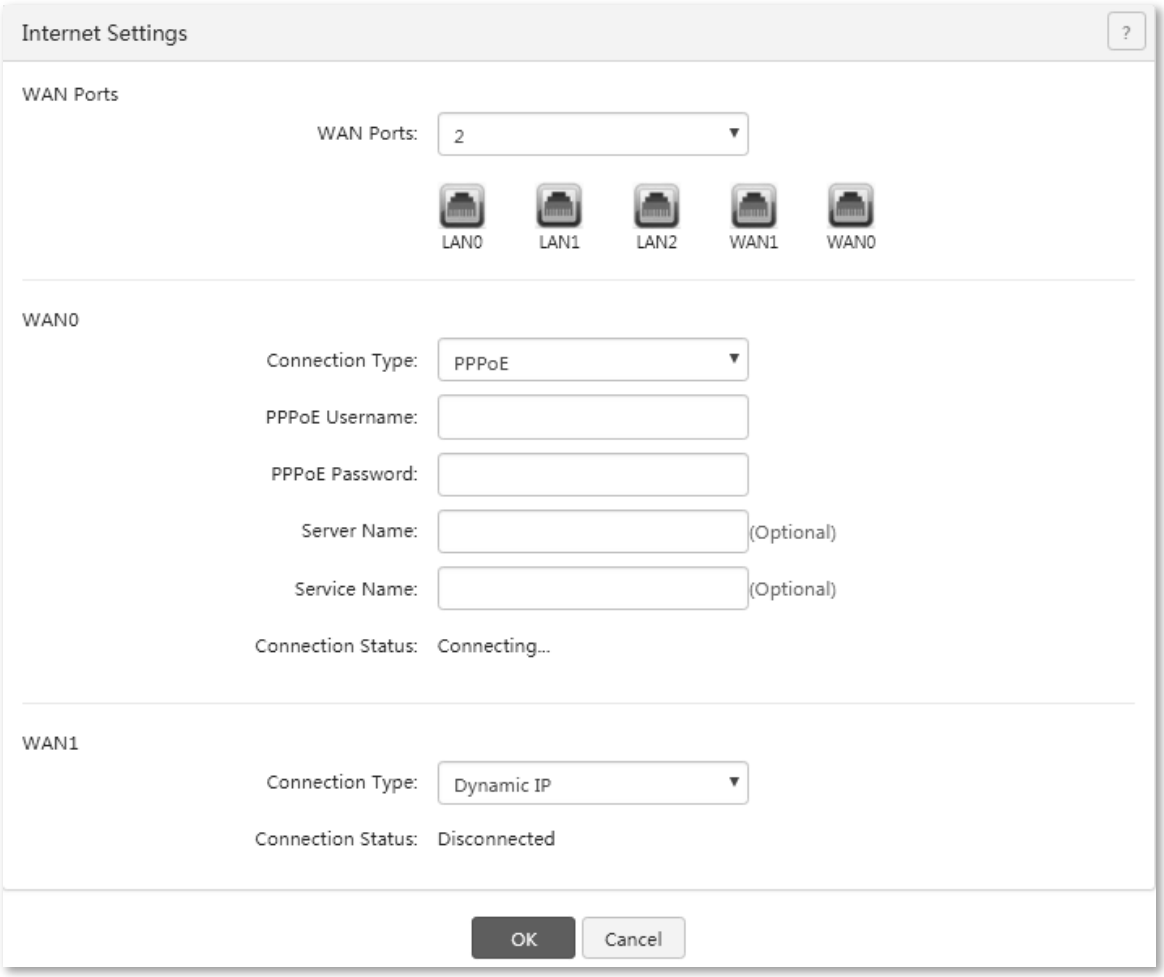
4 Network

This chapter describes:

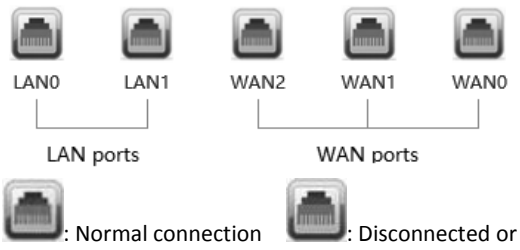
- Setting up an internet connection
- Setting WAN port parameters
- Setting up your LAN
- Configuring port mirroring
- Configuring a static route
- Configuring VLAN
- Configuring any IP
- Configuring the DNS cache

4.1 Setting up an internet connection

This function enables you to share your internet access service among multiple computers on your LAN. To access the page for setting up an internet connection, choose **Network** > **Internet Settings**. See the following figure.



Parameter description

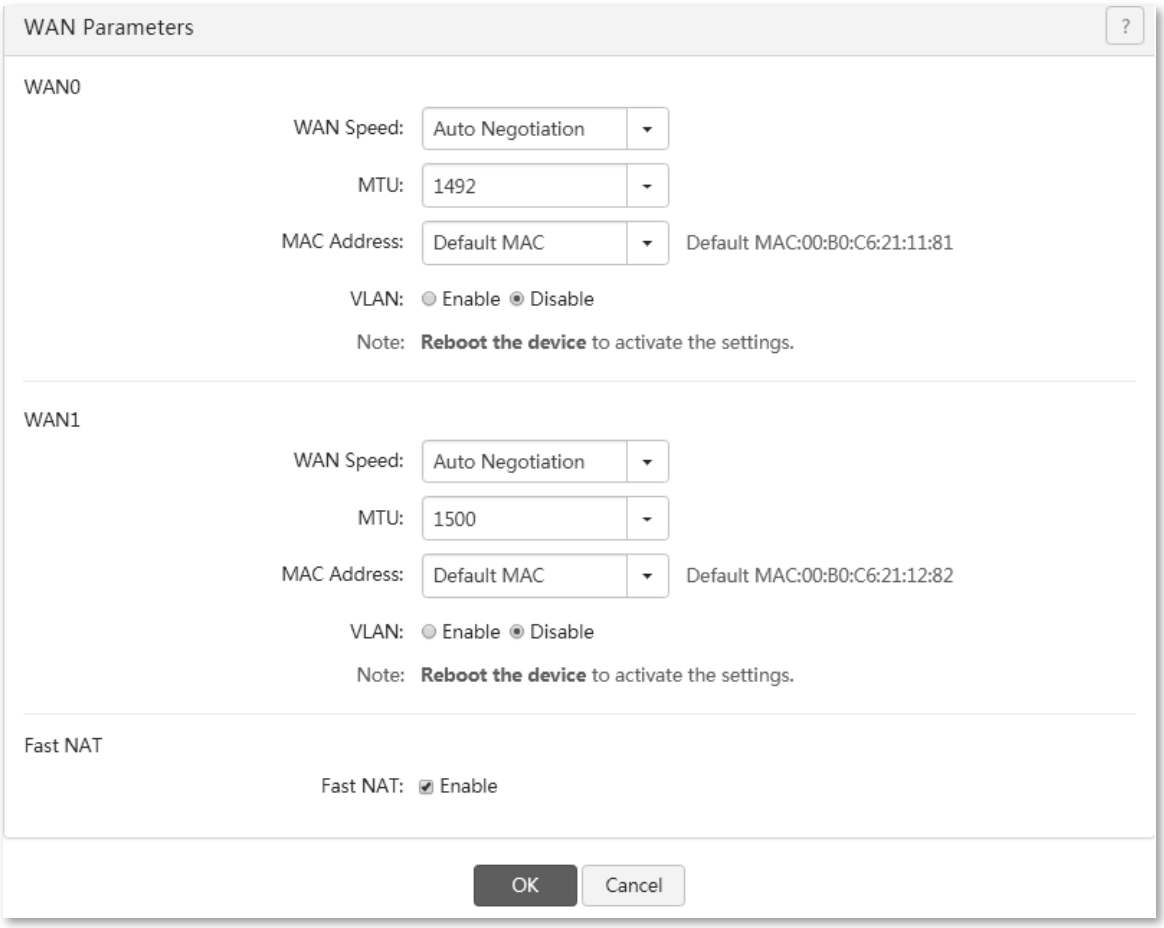
Parameter	Description
WAN Ports	It specifies the number of WAN ports of the router. By default, the router has 2 WAN ports. The router supports a maximum of 4 WAN ports. You can change the number as required. After you change the number of WAN ports, the status of the RJ45 ports changes accordingly. See the following figure.  : Normal connection : Disconnected or connection failure
Connection Type	The router can set up an internet connection using PPPoE, a dynamic IP address, or a static IP address. The connection types are described as follows: – **PPPoE**: It is used if your ISP provides you with a PPPoE user name and password.

Parameter	Description
	– **Dynamic IP**: It is used if your ISP does not provide you with any internet connection information. – **Static IP**: It is used if your ISP provides you with a static IP address.
PPPoE Username	A user name and password are required only after you set **Connection Type** to **PPPoE**. The user name and password may be specified on your broadband service note. If the note does not specify such information, consult your ISP.
PPPoE Password	
IP Address	These parameters are required only after you set **Connection Type** to **Static IP**. The information may be specified on your broadband service note. If the note does not specify such information, consult your ISP.
Subnet Mask	
Default Gateway	
Primary DNS	 If your ISP provides you with only 1 DNS IP address, leave **Secondary DNS** blank.
Secondary DNS	
Connection Status	It displays the WAN port connection status of the WAN port for accessing the internet. – **Connected**: A WAN port of the router is connected using an Ethernet cable and has obtained IP address information. – **Authenticated success**: The router has successfully dialed up and obtained IP address information. – **Connecting…**: The router is connecting to an upstream network device. – **Disconnected**: No connection is set up or connection fails. In this case, verify the cable connection and internet connection information, or consult your ISP. – For other status, troubshooting problems guided by the onscreen instructions.

4.2 Setting WAN port parameters

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

To access the configuration page, choose **Network** > **WAN Parameters**. See the following figure.



4.2.1 WAN speed

If you have correctly connected an Ethernet cable to a WAN port of the router, but the Link LED indicator of the WAN port does not turn on or it takes over 5 seconds for the Link LED indicator to turn on, you can try resolving the problem by changing **WAN Speed** of the port to **10M half duplex** or **10M full duplex**.

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

4.2.2 MTU

Maximum Transmission Unit (MTU) indicates the maximum size of a packet that can be transmitted by a network device. If **Connection Type** is set to **PPPoE**, the default MTU value is **1492**. If **Connection Type** is set to **Dynamic IP** or **Static IP**, the default MTU value is **1500**. The default values are recommended. If you encounter any of the following problems, try gradually decreasing the value (recommended range: 1400 to 1500) to find the proper one:

- Some websites are inaccessible, or secure websites, such as online banking websites and Alipay, cannot be displayed properly.
- Emails service suspends or servers such as FTP and POP servers are not accessible.

MTU Value	Usage
1500	It is the most common value for non-PPPoE connections and non-VPN connections.
1492	It is used for PPPoE connections.
1472	It is the maximum value for the pinging function. (If a greater value is used, packets are splitted.)
1468	It is used for DHCP, which assigns dynamic IP addresses.
1436	It is used for VPNs or PPTP.

4.2.3 MAC address

If your ISP has bound your internet account with the MAC address (physical address) of your computer, the router cannot access the internet despite internet connection parameters have been set on the router. In this case, only the computer can use the account to access the internet. The computer refers to the one used to verify your internet accessibility after your ISP creates the account for you.

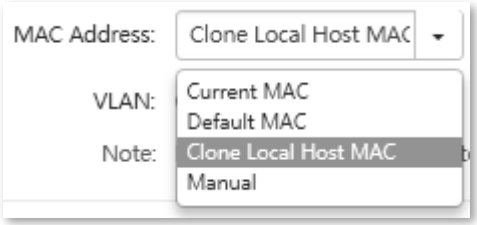
You can try MAC address cloning method 1 or 2 described in the following section to resolve the problem.

Note

Please clone the MAC address of the computer that can normally access to the internet or the MAC address of the WAN port of the router that can normally access to the internet.

Method 1: Clone MAC address of the computer

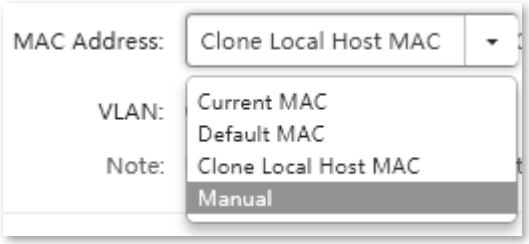
1. Connect the computer that has internet accessibility to the router.
2. Log in to the router web UI on the computer, choose **Network** > **WAN Parameters**.
3. Select **Clone Local Host MAC** from the drop-down list.
4. Click **OK**.



---End

Method 2: Clone WAN MAC address of the rotuer

1. Record the correct WAN MAC address of the router that has internet accessibility.
2. Connect a computer to your new router.
3. Log in to the router web UI on the computer.
4. Choose **Network** > **WAN Parameters**.
5. Select **Manual** from the drop-down list.
6. Enter the MAC address that has internet accessibility.
7. Click **OK**.



---End

Tip

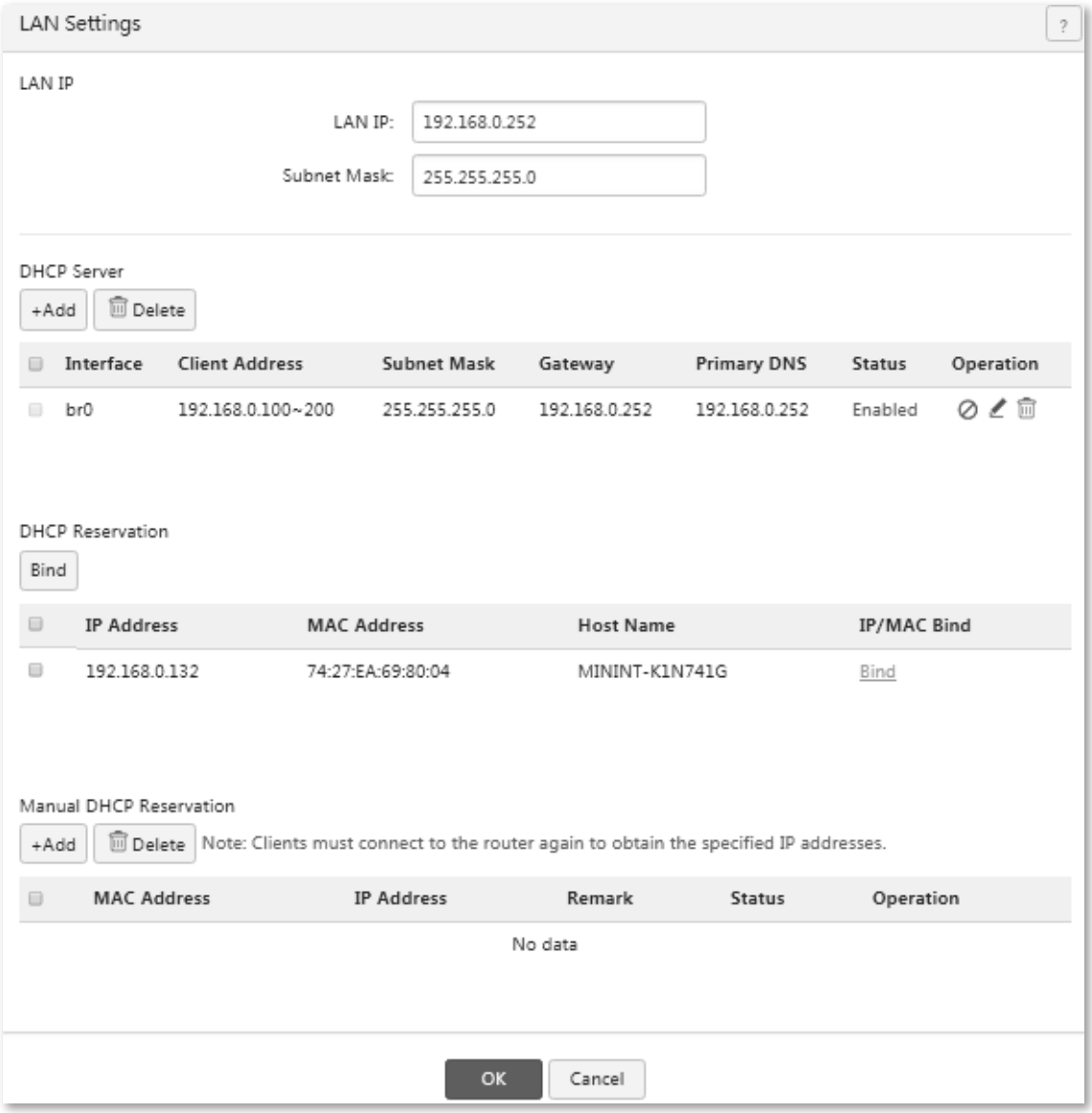
To restore the default MAC address of the WAN port, choose **Network** > **WAN Parameters**, set **MAC Address** corresponding to the WAN port to **Default MAC**, and click **OK**.

4.2.4 Fast NAT

NAT (Network Address Translation) translates private addresses on the internal network to global addresses so as to achieve communication between local network and the public internet. You can enable **Fast NAT** to improve NAT performance of the router.

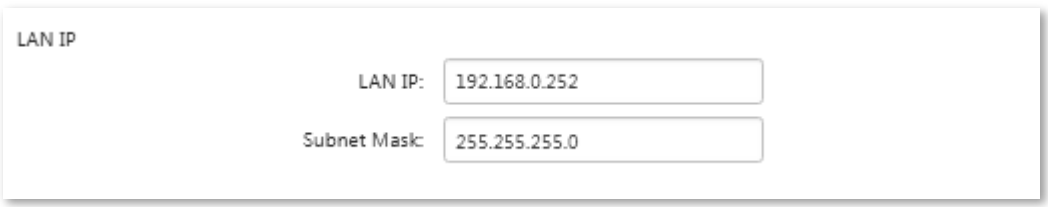
4.3 Setting up your LAN

Choose **Network** > **LAN Settings**. On the page that appears, you can set the LAN IP address and DHCP server parameters for the router.



4.3.1 LAN port IP addresses

The LAN IP address is set for the router to communicate within your LAN and for you to manage the router. The default LAN IP address and subnet mask of the router are **192.168.0.252** and **255.255.255.0** respectively.



Generally, you do not need to change the LAN IP address, unless IP address conflicts. For example, the WAN IP address and LAN IP address of the router may be in the same network segment or the default IP address 192.168.0.252 has been assigned to a device on the LAN.

After the LAN IP address is changed, the following message appears.

When the progress bar completes, you are redirected to the login page. If the login page does not appear, check and ensure that the local connection of your computer is set to **Obtain an IP address automatically**, and try the new LAN IP address to access the web UI of the router.

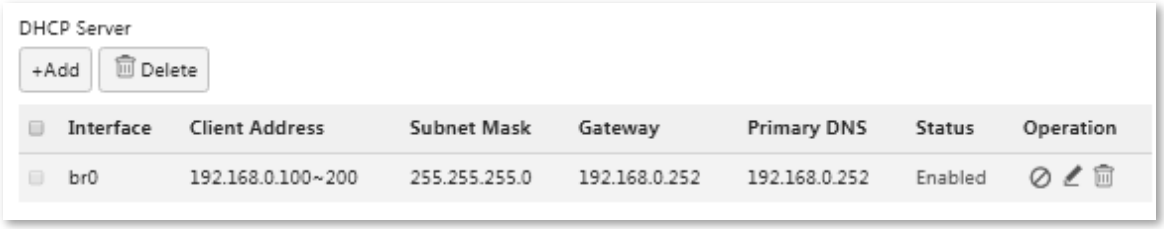
Note

If the new and old LAN IP addresses belong to different network segments, the router automatically changes the DHCP address pool so that the IP addresses in the pool belong to the same network segment as that of new LAN IP address.

4.3.2 DHCP server

The DHCP server automatically assigns IP addresses, subnet masks, gateway IP addresses, and DNS IP addresses to computers on your LAN. With this function disabled, computers can access the internet only when configured with internet connection parameters. Disable this function only when necessary.

The router is pre-configured with one default DHCP server rule. See the following figure:



Parameter description

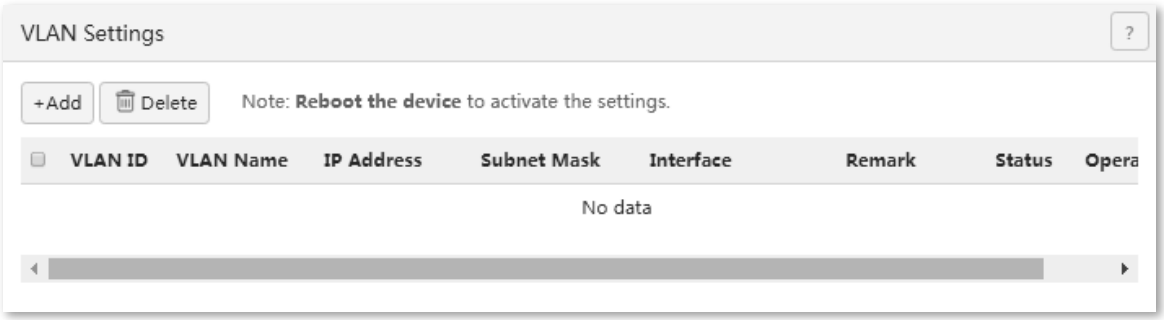
Parameter	Description
Interface	It specifies the interface configured with DHCP server. The default DHCP server rule with the interface named **br0** allocates IP addresses to users on the non-VLAN network.
Client Address	It specifies the IP address range that DHCP server assigns. The default start IP address is **192.168.0.100**, default end IP address is **192.168.0.200**. Note The start and end IP addresses could belong to different network segments.

Parameter	Description
Start IP	It specifies the start IP address of the DHCP address pool. The default value is **192.168.0.100**.
End IP	It specifies the end IP address of the DHCP address pool. The default value is **192.168.0.200**.
Subnet Mask	It specifies the subnet mask assigned to your LAN computers by the DHCP server. It cannot be modified.
Gateway	It specifies the default gateway assigned to your LAN computers by the DHCP server. It cannot be modified.
Primary DNS	It specifies the primary DNS IP address that the DHCP server assigned to computers on your LAN. The router can function as a DNS proxy. Therefore, the LAN IP address of the router is set as the primary DNS IP address by default. Note Generally, the default value is recommended. If you need to change the value, ensure that the new value is the IP address of a correct DNS server or DNS proxy, so that the computers on your LAN can access the internet properly.
Secondary DNS	It specifies the secondary DNS IP address assigned by the DHCP server to computers on your LAN. If the value is blank, the DHCP server does not assign the IP address.
Lease Time	It specifies the validity of an IP address assigned by the DHCP server to a computer. When the IP address expires: – If the computer is connected to the router, the computer automatically updates the lease time to continue using the IP address. – If the computer is not connected to the router (for example, the computer is shut down or the wired or wireless connection of the computer is released), the router releases the IP address. Then, when another computer requests an IP address, the router can assign the released IP address to the computer. Change the default settings only when necessary.

Adding DHCP server

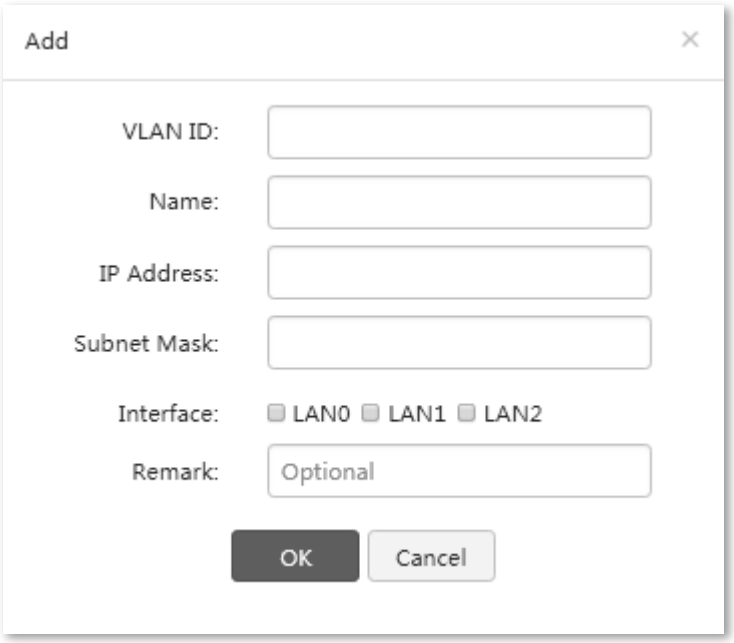
I. Add VLAN interface.

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



3. Set up VLAN rules.

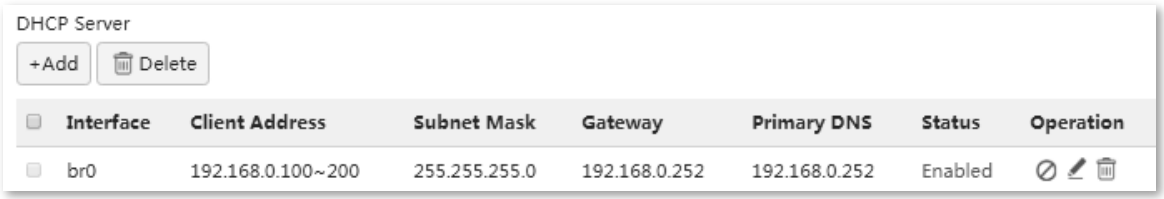
4. Click **OK**.



5. Go back to the page of **VLAN Settings**, click **Reboot the device** to activate the settings.

II. Configure DHCP server.

1. Click **Network** > **LAN Settings**, locate **DHCP Server**.
2. Click +Add.



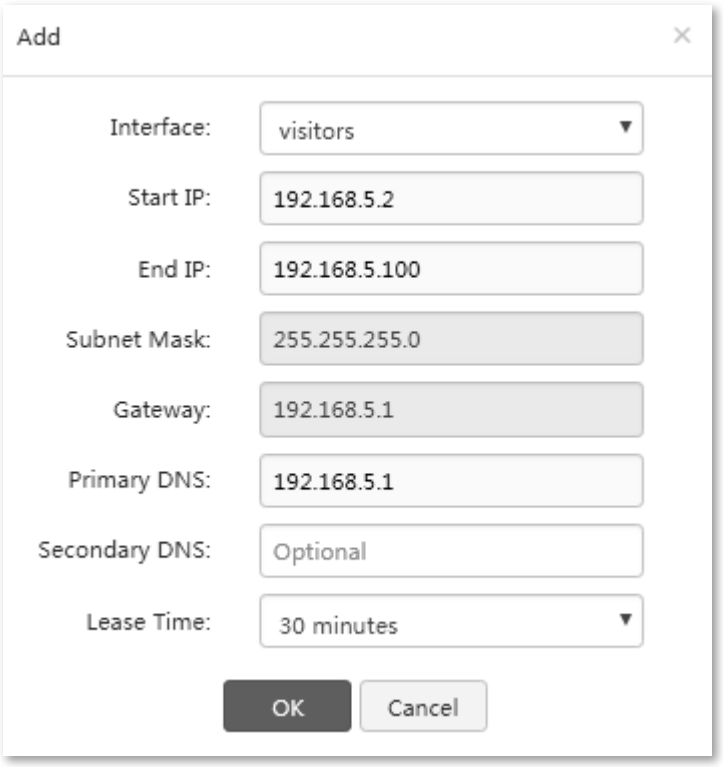
3. Configure DHCP server information on the page that appears.

   (1) **Port**: Choose the VLAN you set from the drop-down list, such as **visitors**.

   (2) **Start/End IP Address**: Enter the IP address range. Network segment of the IP address range shall be the same as that of the gateway, which is **192.168.5.2~192.168.5.100** in this example.

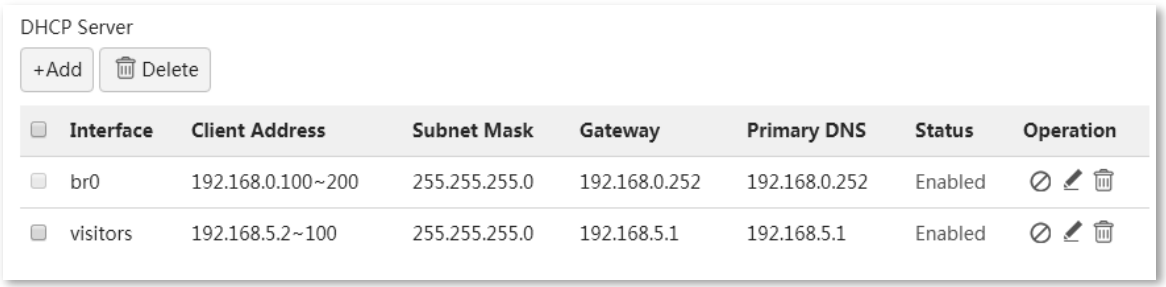
   (3) **Primary DNS**: Enter either the gateway address, or the correct DNS parameter, which is **192.168.5.1** in this example.

(4) Click **OK**.



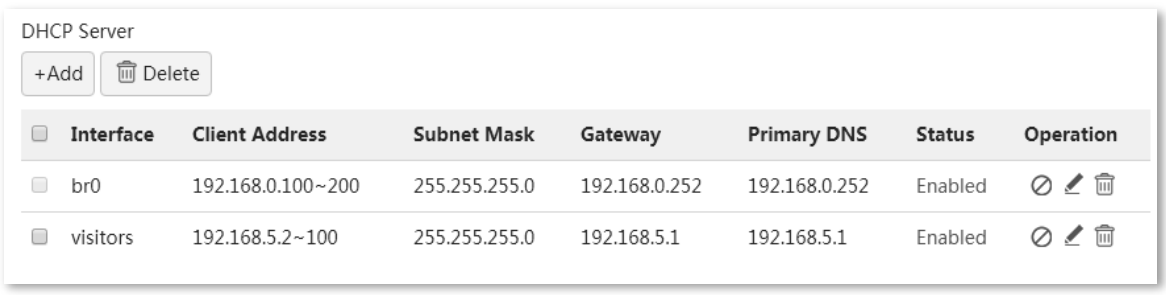
---End

Configuration succeeds.

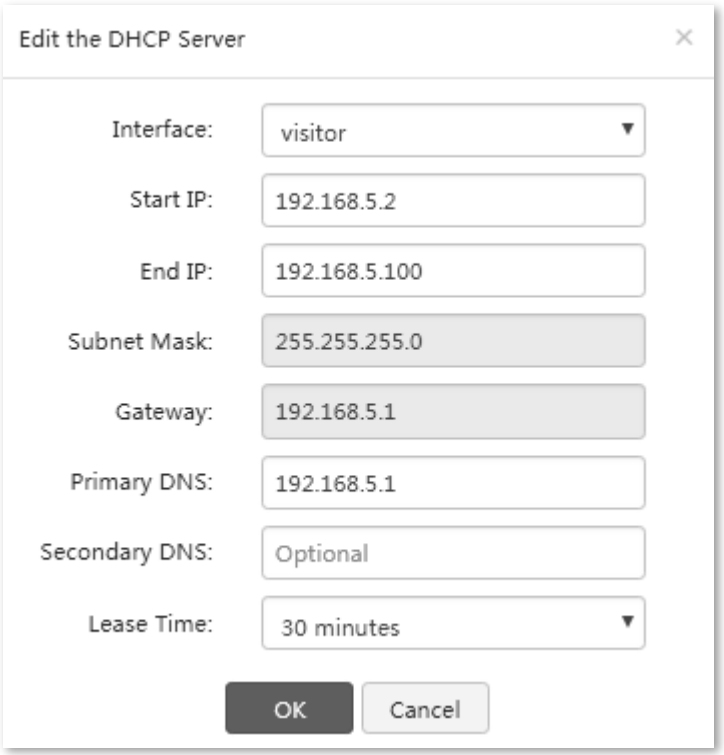


Modifying DHCP server

1. Click **Network** > **LAN Settings**, and locate **DHCP Server** module.
2. Locate the interface you need to modify, and click .



3. Modify related parameters.

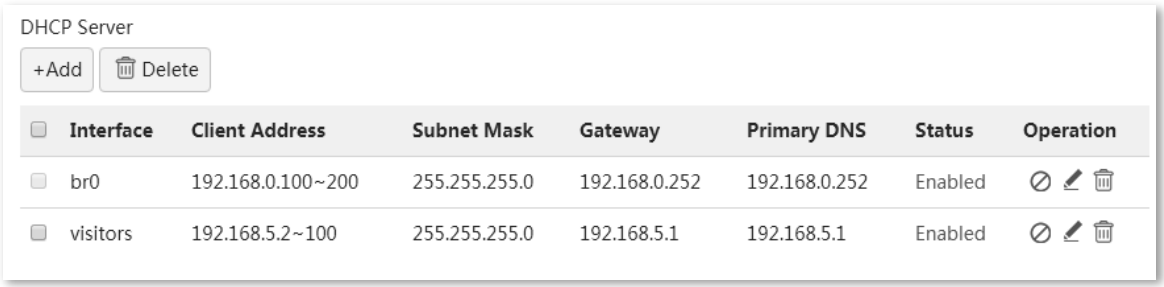


4. Click **OK**.

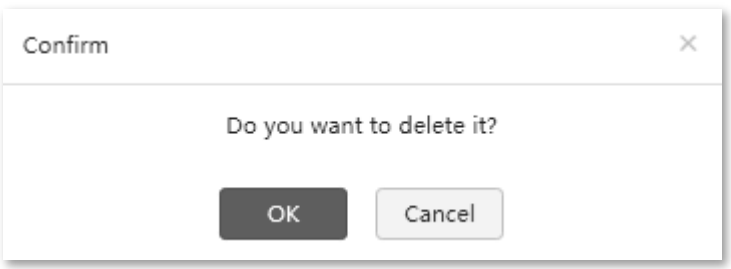
---End

Delete DHCP server

1. Click **Network** > **LAN Settings**, locate **DHCP Server** module.
2. Locate the interface you want to delete, click .



3. Click **OK.**



---End

4.3.3 DHCP reservation

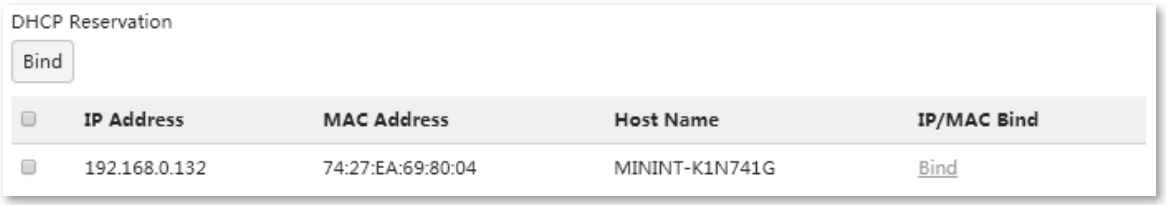
Overview

The DHCP Reservation function enables clients to obtain the same IP addresses every time they connect to the router, making IP address-based functions such as Filter Management, Bandwidth Control, and Virtual Server work properly.

- In **DHCP Reservation** module, it allows you to quickly bind the IP address obtained from the DHCP server and the MAC address of the client.
- In **Manual DHCP Reservation** module, it allows you to bind the client manually so that the DHCP server always assigns a fixed IP address to the same client.

Scenario 1: Clients have connected to the router properly

You are recommended to use DHCP Reservation to perform quick MAC/IP binding. Choose **Network** > **LAN Setting**, and locate **DHCP Reservation** module.

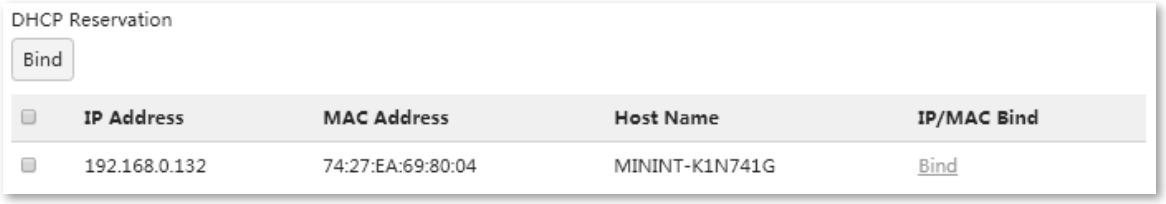


Parameter description

Parameter	Description
Bind	Click it to perform quick MAC/IP binding.
IP Address	It specifies the static IP address assigned by the DHCP server.
MAC Address	It specifies the MAC address bound to the static IP address assigned to a computer.
Host Name	It specifies the name of the clients.
IP/MAC Bind	Click **Bind** to bind the client' IP address and MAC address so that the client always obtain a fixed IP address. It shows bound status after binding successfully.

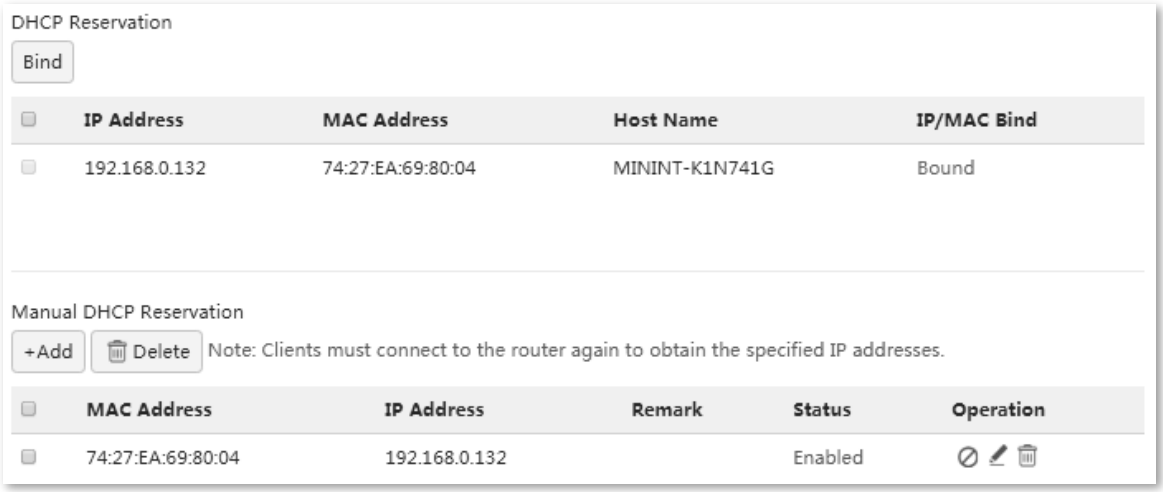
Binding a single client's IP address

1. Choose **Network** > **LAN Settings**, and locate **DHCP Reservation** module.
2. Select the corresponding client in the **DHCP Reservation** list, click Bind.



---End

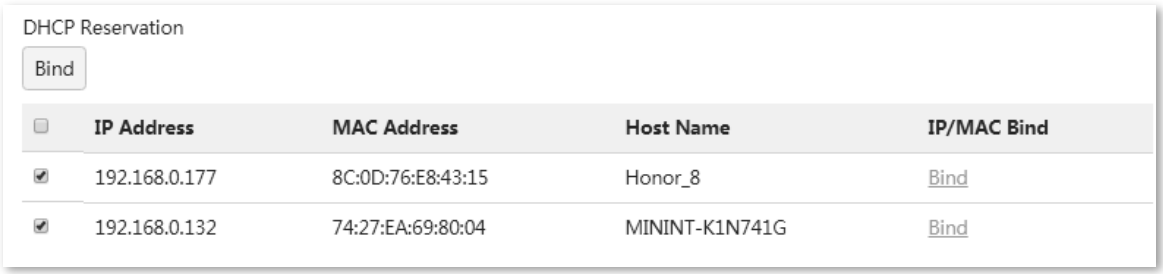
After bound successfully, the following page appears:



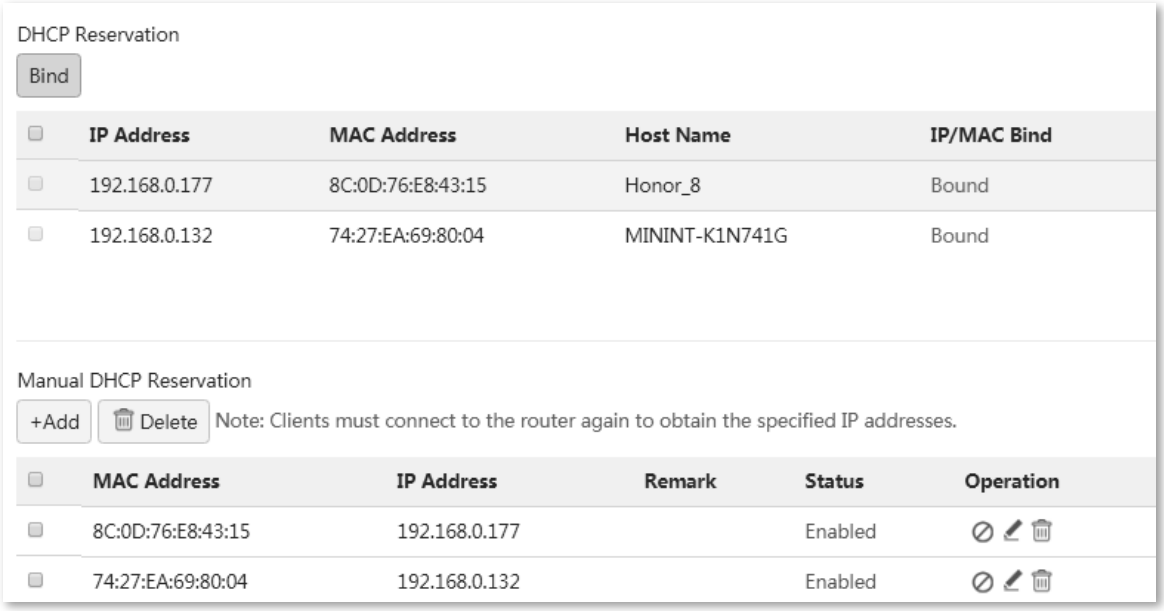
---End

Binding in batch

1. Choose **Network** > **LAN Settings**, locate **DHCP Reservation** module.
2. Select multiple clients in the **DHCP Reservation** list.
3. Click Bind.

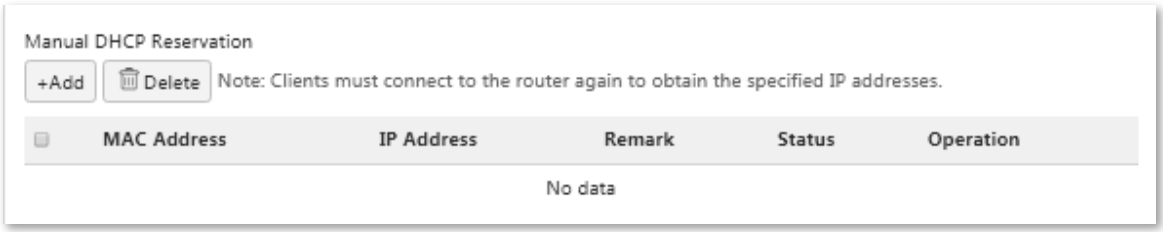


After bound successfully, the following page appears:



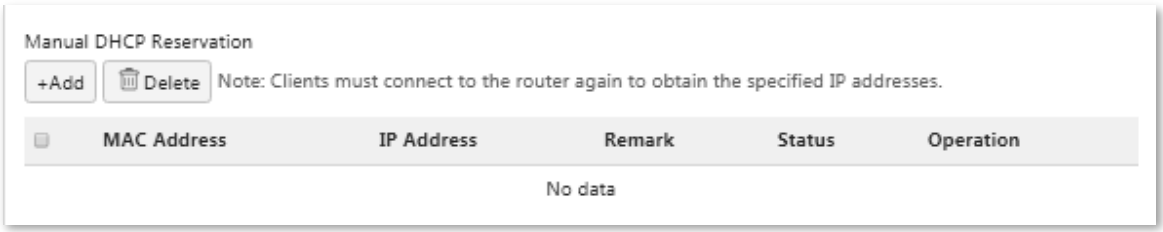
Scenario 2: Clients do not connect to the router

For clients that are not connected to the router, you are recommended to perform manual binding using **Manual DHCP Reservation**. To enter the configuration page, choose **Network** > **LAN Settings**, and move to the **Manual DHCP Reservation** module.

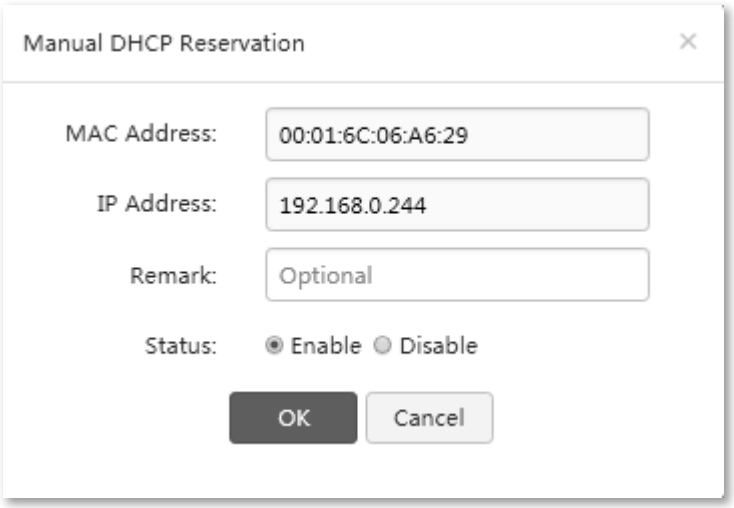


Adding a rule

1. Choose **Network** > **LAN Settings**. Then move to the **Manual DHCP Reservation** module.
2. Click +Add.



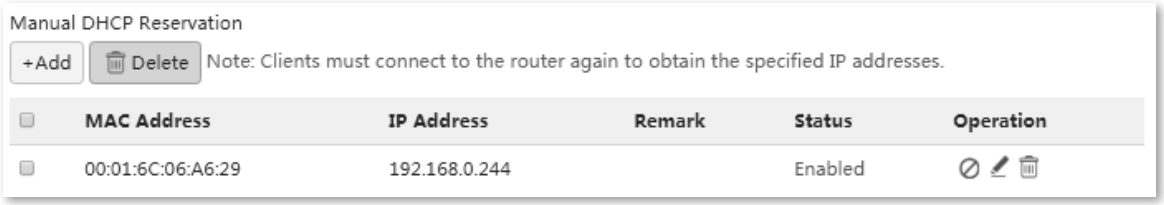
3. Enter **MAC Address**, which is **00:01:6C:06:A6:29** in this example.
4. Enter **IP Address**, which is **192.168.0.244** in this example.



5. Click **OK**.

---End

Add successfully. See the following figure. To bind more clients, repeat above steps 1-4.



Parameter description

Parameter	Description
+Add	Click it to add a rule.
Delete	Click it to delete a rule.
IP Address	It specifies the static IP address assigned by the DHCP server.
MAC Address	It specifies the MAC address bound to the static IP address assigned to a computer.
Remark	It specifies the description of a rule, which is optional.
Status	It specifies whether the rule is enabled. The options include: – **Enabled**: It indicates that the rule is enabled. – **Disabled**: It indicates that the rule is disabled.
Operation	Actions you can perform for a rule. – / : Click it to disable/enable the rule. – : Click it to modify the rule. – : Click it to delete the rule.

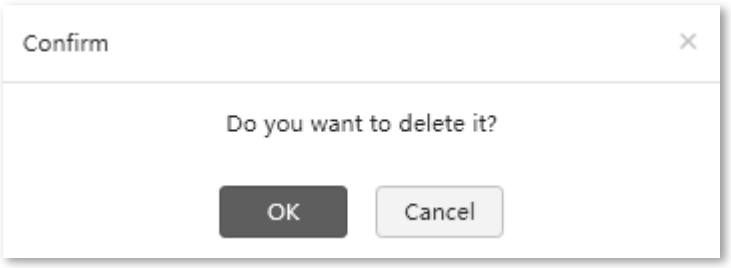
Modifying a rule

1. Choose **Network** > **LAN Settings**.
2. Click corresponding to a rule to be modified.
3. Modify the rule as required.
4. Click to disable a rule.
5. Click to enable a rule.

---End

Deleting a rule

1. Choose **Network** > **LAN Settings**.
2. Click Delete corresponding to a rule to be deleted.
3. Click **OK** on the popup window**.**



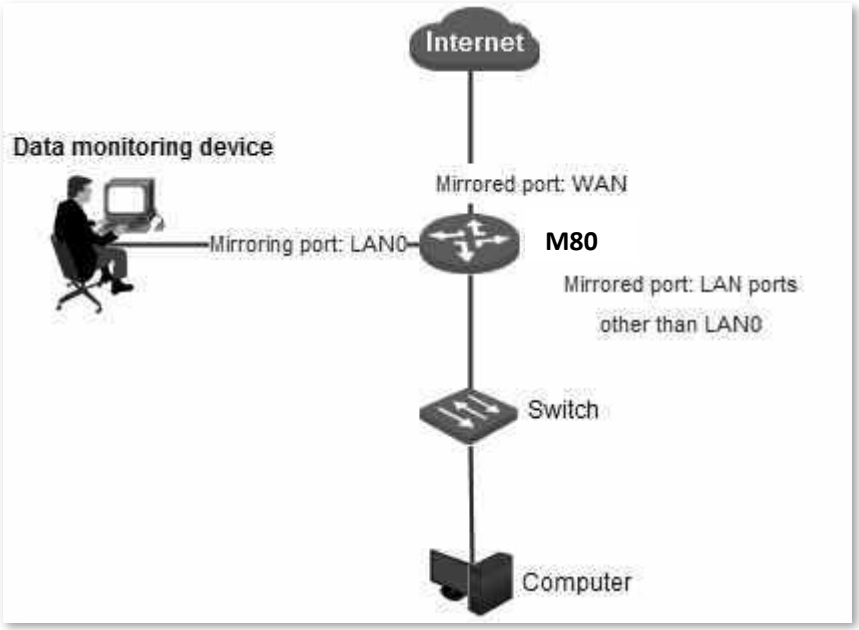
4. To delete multiple rules at the same time, select them and click Delete.

---End

4.4 Port mirroring

4.4.1 Overview

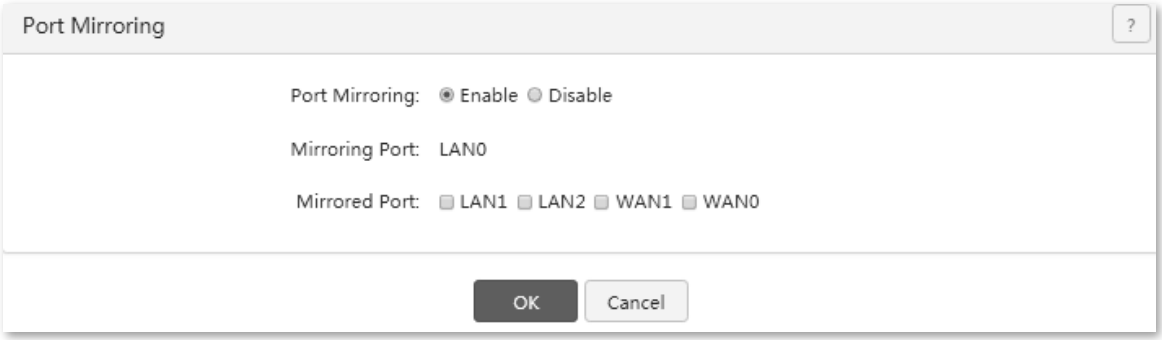
Port mirroring function forwards a copy of data of one or more mirrored ports to the specified mirroring port. The network administrator uses data monitoring devices to monitor traffic, analyze performance and perform network diagnose. The following figure shows the network topology for port mirroring.



The mirroring port of M80 is fixed to LAN0 and cannot be changed.

4.4.2 Configuring port mirroring

1. To access the configuration page, choose **Network** > **Port Mirroring**.
2. Set **Port Mirroring** to **Enable**.
3. Choose **Mirrored Port**.
4. Click **OK**.



---End

Parameter description

Parameter	Description
Port Mirroring	It is used to enable or disable the port mirroring function. The default option is **Disable**.
Mirroring Port	It indicates the monitoring port. Computer connected to this port needs to install monitoring software to perform monitoring. The default mirroring port is **LAN0** and cannot be changed.
Mirrored Port	Port monitored by the mirroring port. With the port mirroring function enabled, incoming and outgoing traffic is visible to the mirroring port.

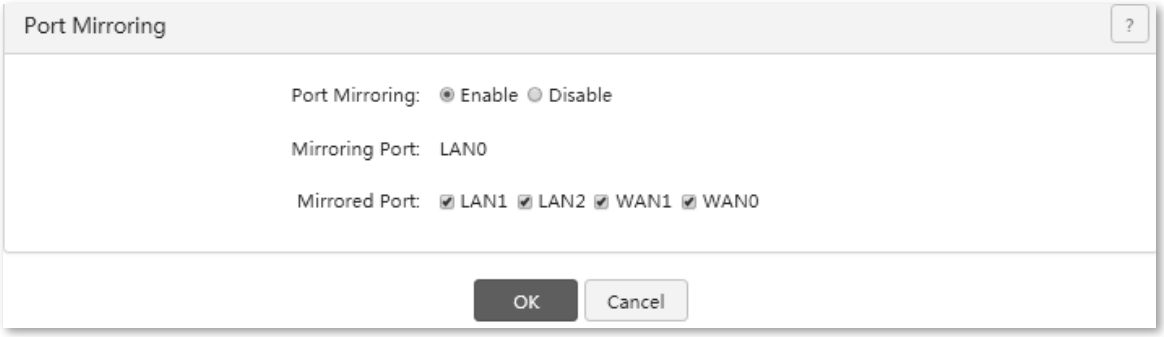
4.4.3 Port mirroring configuration example

Networking requirement

An enterprise has used M80 to set up a LAN. Recently, internet access failures occur frequently and the network administrator needs to capture data packets from the WAN and LAN ports of the router for analysis.

Configuration procedure

1. Choose **Network** > **Port Mirroring.**
2. Set **Port Mirroring** to **Enable**.
3. Select **LAN1**, **LAN2**, **WAN1**, and **WAN0**.
4. Click **OK**.



---End

Verification

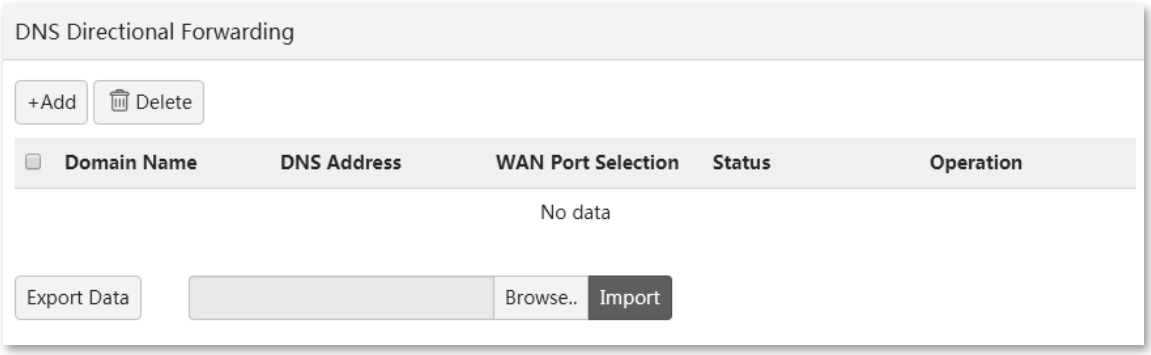
Run monitoring software such as Wireshark on the monitoring computer to verify the software can capture data packets from the mirrored ports.

4.5 DNS Directional Forwarding

4.5.1 Overview

DNS Directional Forwarding function allows you to map a domain name to a DNS server address and specify the egress WAN port to improve the request responsive speed.

To enter the configuration page, choose **Network** > **DNS Directional Forwarding**.

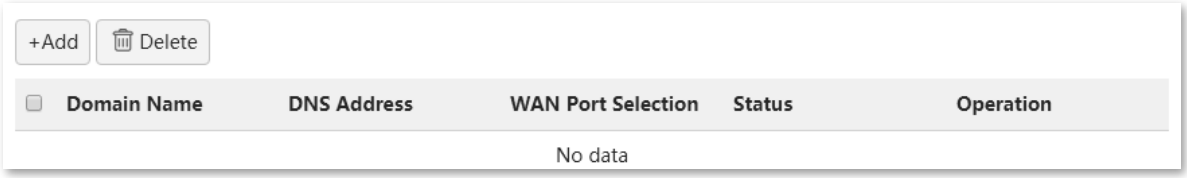


Parameter description

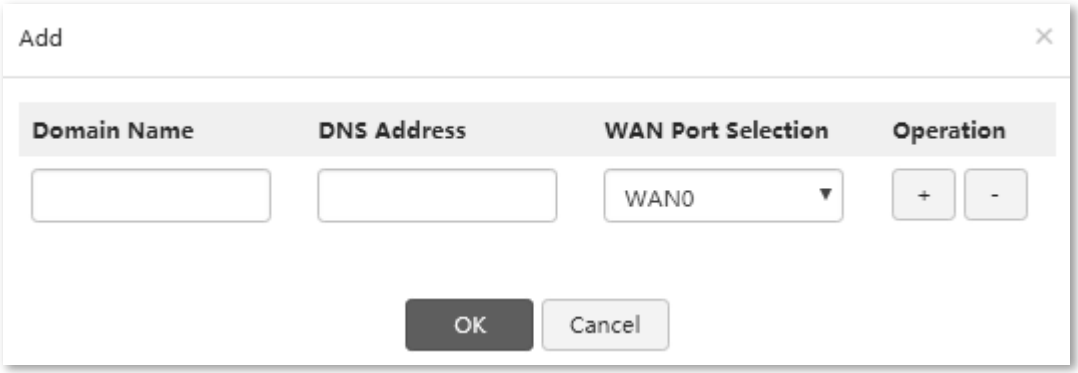
Parameter	Description
Domain Name	It specifies the domain name to be forwarded for resolution.
DNS Address	It specifies the DNS server address.
WAN Port Selection	It specifies the WAN port for data forwarding from the router, set the corresponding WAN port as required.
Status	It specifies the current status of the rule, including **Enabled** and **Disabled**.
Operation	It allows to perform the operations below: – Click to disable a rule. – Click to enable a rule. – Click to modify a rule. – Click to delete a rule.

4.5.2 Adding a DNS Directional Forwarding rule

1. Choose **Network** > **DNS Directional Forwarding**.
2. Click +Add.



3. Set the **Domain Name** to be forwarded for resolution.
4. Set **DNS Address**.
5. Set **WAN Port Selection** to the port for data forwarding.
6. Click **OK**.



---End

4.6 DNS Hijacking

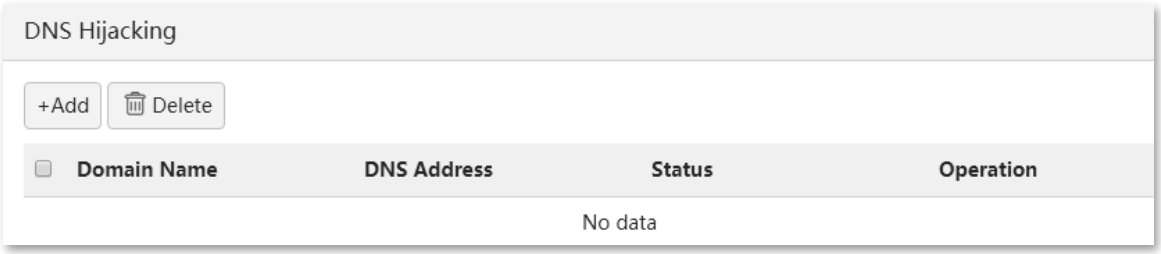
4.6.1 Overview

DNS refers to the process that when a network application requests content from a domain name, it sends the request to the DNS server instead of the real host for a corresponding IP address, and then initiates a request to the service on the specific host.

DNS hijacking means that when the addresses resolved by DNS is tampered with. With this function enabled, it will redirect to a fixed web page whether LAN users visit Google, Wiki, or other web pages.

The DNS hijacking function is only implemented in the LAN, that is, the addresses resolved by the DNS only support the LAN IP address.

To access the configuration page, choose **Network > DNS Hijacking.**

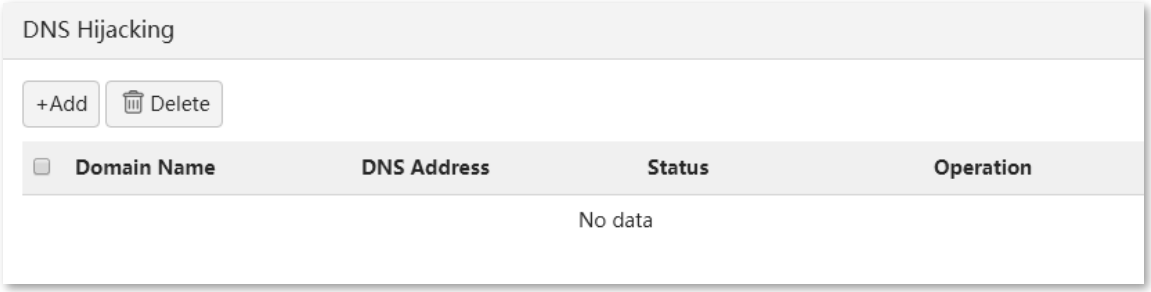


Parameter description

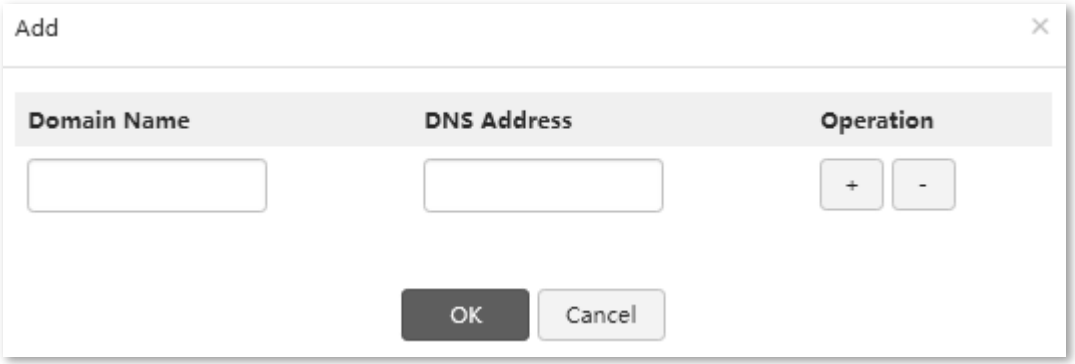
Parameter	Description
Domain Name	It specifies the domain name to be resolve to a fixed IP address on the intranet.
DNS Address	It specifies the IP address for DNS resolution. That is the IP address to resolve when users visit the domain name.
Status	It specifies the current status of the rule, including **Enabled** and **Disabled**.
Operation	It allows you to perform the operations below: Click to disable a rule. Click to enable a rule. Click to modify a rule. Click to delete a rule.

4.6.2 Adding a DNS Hijacking rule

1. Choose **Network** > **DNS Hijacking**.
2. Click +Add.



3. Set **Domain Name** to the IP address to be resolved.
4. Set **DNS Address**.
5. Click **OK.**



---End

4.7 Configuring a static routing

4.7.1 Overview

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

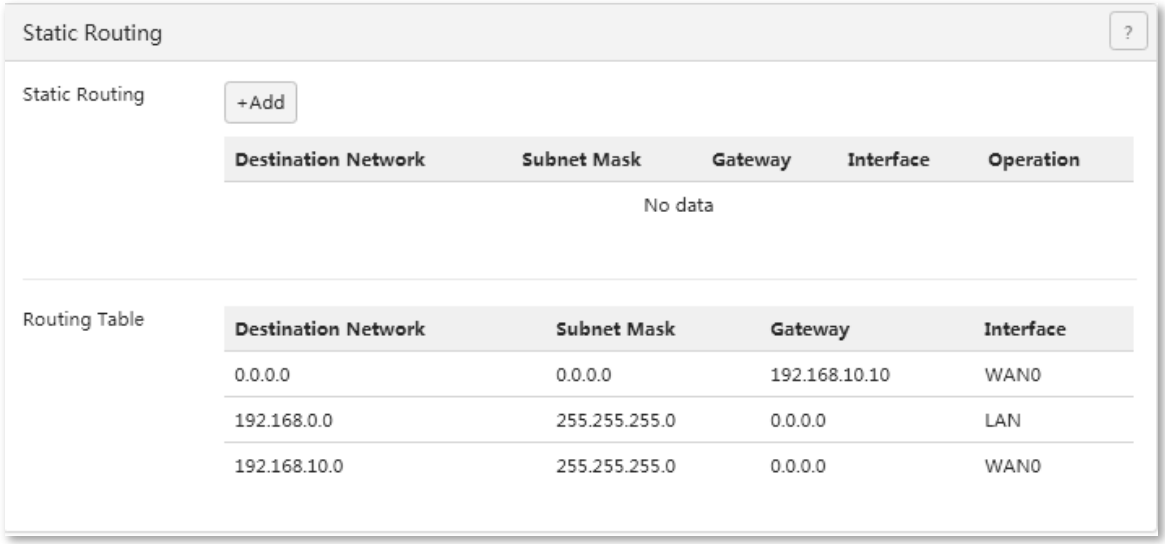
To define a static route, specify the network segment and subnet mask used to identify a destination network or host, the gateway IP address, and the router WAN port for forwarding packets. After a static route is defined, all the packets indented for the destination of the static route are directly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

Note

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

4.7.2 Configuring a static routing

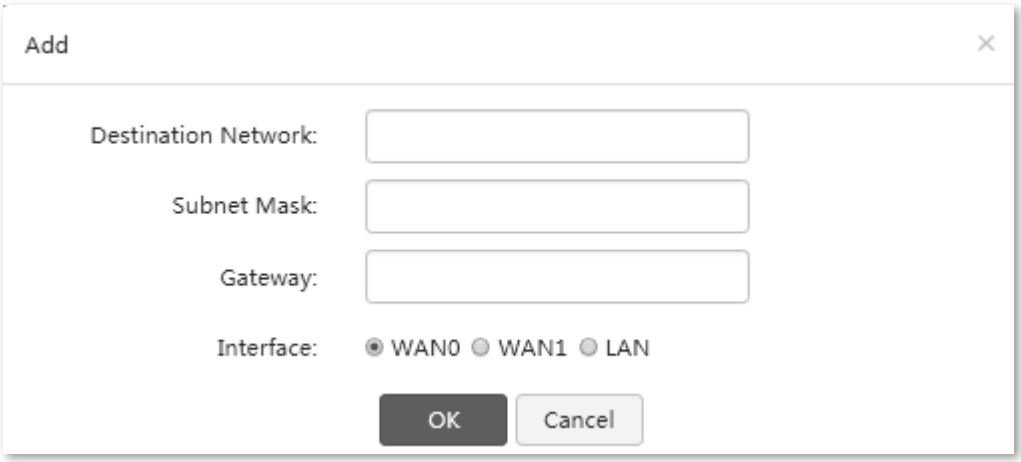
To access the configuration page, choose **Network** > **Static Routing**. See the following figure.



Adding a static routing

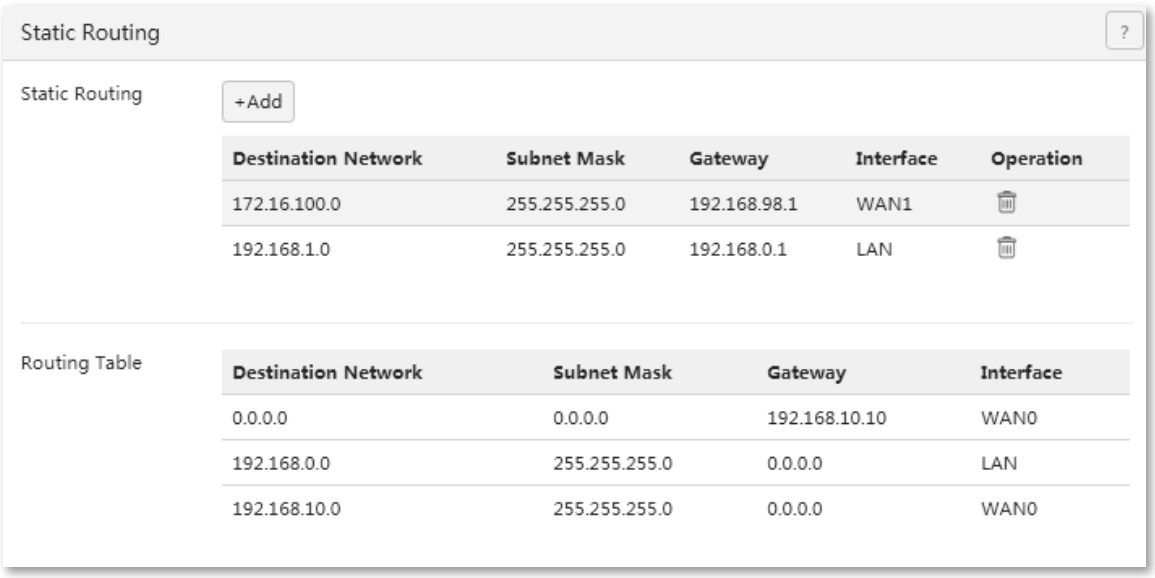
1. Choose **Network** > **Static Routing**.
2. Click +Add.
3. Set related parameters in the **Add** dialog box.

4. Click **OK**.



---End

After configuring static routing successfully, you can check the added static routing rule on page under **Network > Static Routing**. The configured static route is also displayed in the lower routing table, as shown in the following figure.



Parameter description

Parameter	Description
Destination Network	It specifies the IP address or IP address segment of the destination network.
Subnet Mask	It specifies the subnet mask of the IP address of the destination network.
Gateway	It specifies the IP address of the next hop of the packets forwarded from the router WAN port.
Port	It specifies the WAN port that forwards packets.

In the route table, the record where **Destination Network** and **Subnet Mask** are **0.0.0.0** indicates the default route of the router. If no route exactly matching the destination address of a packet is found in the route

table, the router uses the default route to forward the packet. The route containing the gateway IP address **0.0.0.0** is a direct route, which means that the destination network is directly connected to the router using the port specified in the route.

Note

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

Modifying a static routing

1. Choose **Network** > **Static Routing**.
2. Click corresponding to the static route to be modified in the **Static Routing** area.

Deleting a static routing

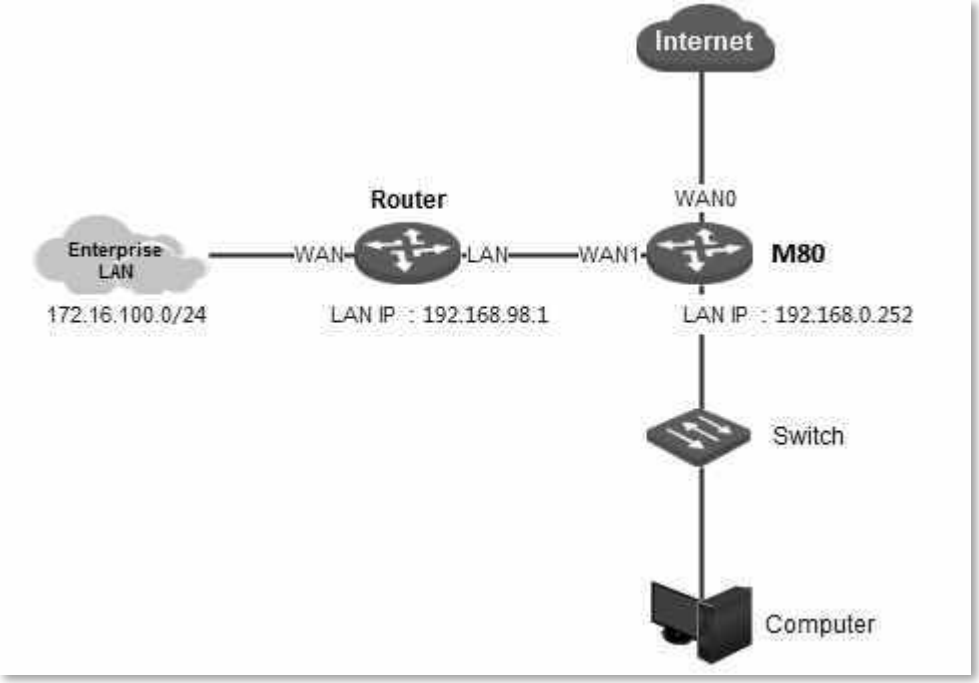
1. Choose **Network** > **Static Routing**.
2. Click corresponding to the static route to be deleted in the **Static Routing** area.

4.7.3 Static route configuration example

Networking requirement

An enterprise uses M80 for network construction. The internet is inaccessible to the enterprise LAN. The WAN0 port of M80 accesses the internet using a PPPoE connection and the WAN1 port of M80 accesses the enterprise LAN using a dynamic IP address. Users on the M80 LAN are allowed to access both the internet and enterprise LAN.

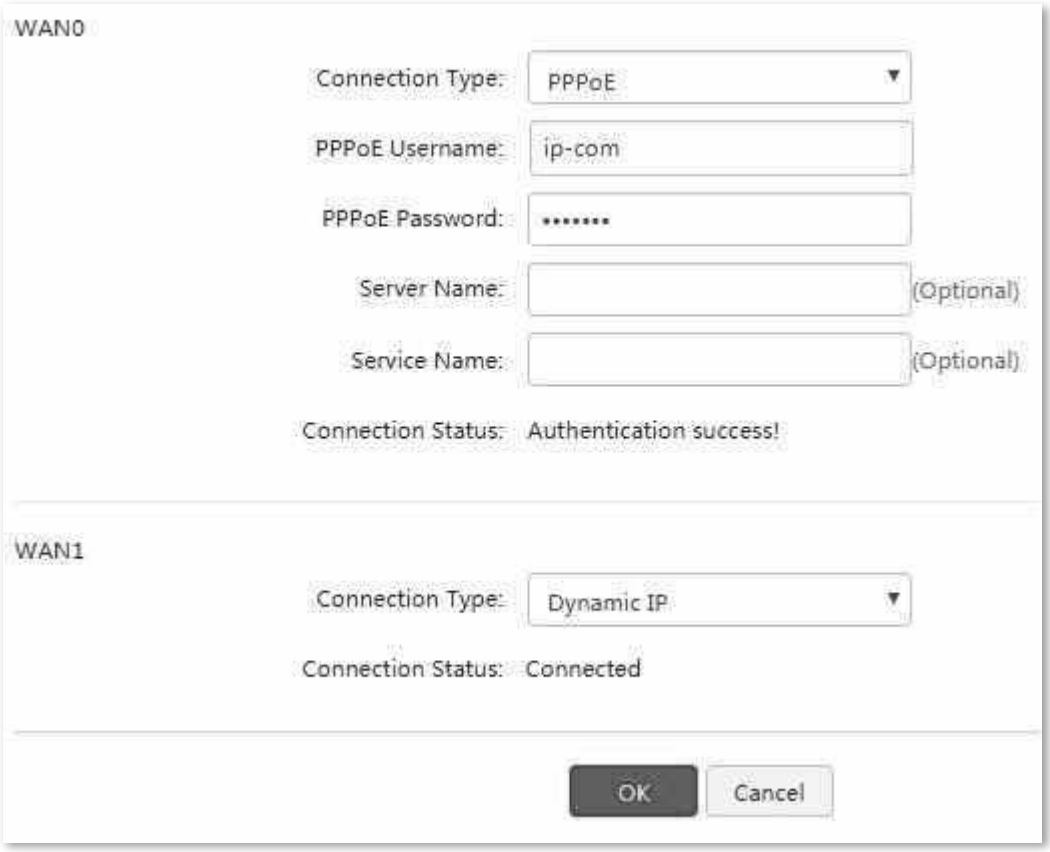
Assume that the PPPoE user name and password are ip-com and the internet bandwidth and LAN bandwidth are 100 Mbps.



Configuration procedure

On the M80 web UI, set up an internet connection and configure a static routing to address the requirement.

1. Set up an internet connection.
   (1) Choose **Network** > **Internet Settings**.
   (2) Set internet connection parameters.
   (3) Click **OK**.

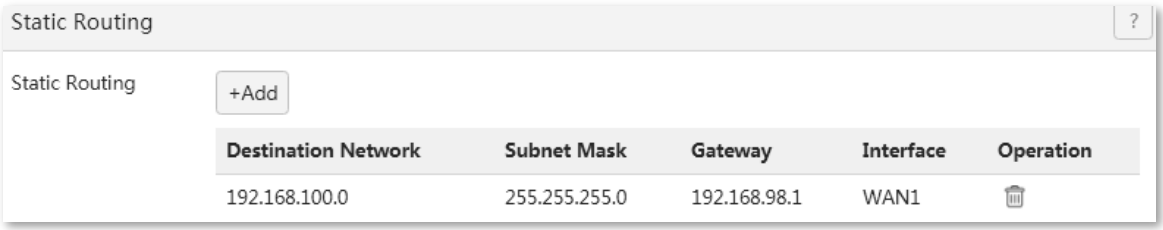


2. Configure a static route.

   (1) Choose **Network** > **Static Routing**.

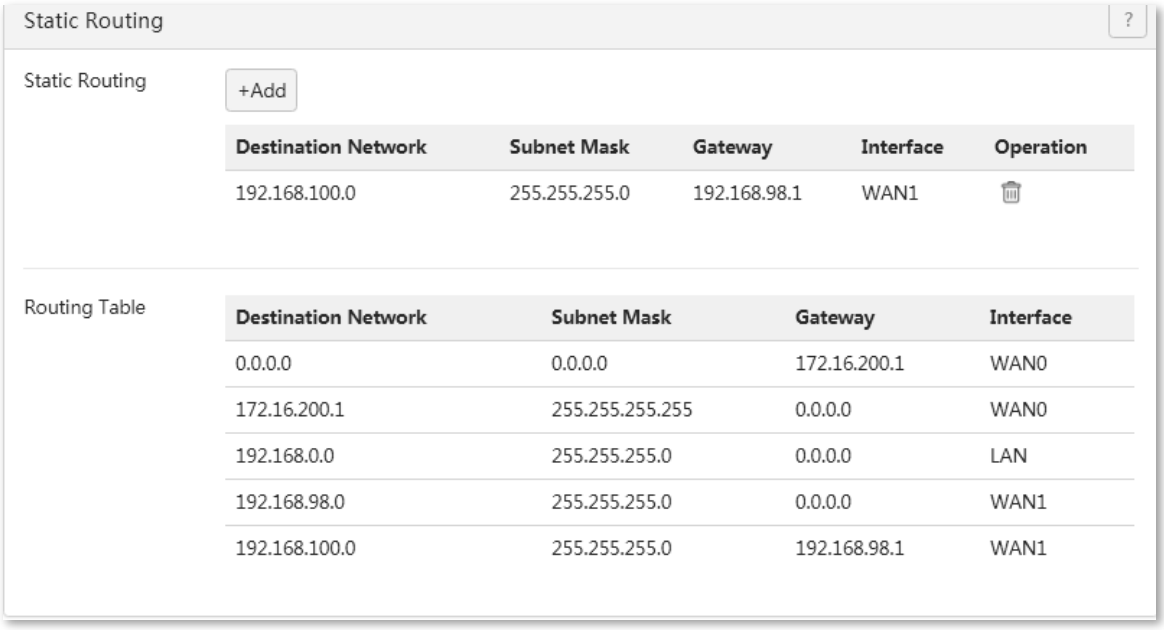
   (2) Click +Add.

   (3) Configure the static route shown in the following figure.



---End

The configured static route appears in the **Route Table** module. See the following figure.



Verification

Access the internet and enterprise LAN using a computer on the LAN.

Note

If the enterprise LAN is connected to the internet, M80 may point its default route to the other router, resulting in incorrect routing. In this case, you can try the following methods:

- Choose **Bandwidth Control** and set **Bandwidth** of the WAN1 port to a value far smaller than the value of **Bandwidth** of the WAN0 port.
- Disable the automatical bandwidth control function of M80 and use a manual multi-WAN policy to ensure that all M80 LAN users access the internet through the WAN0 port of M80.

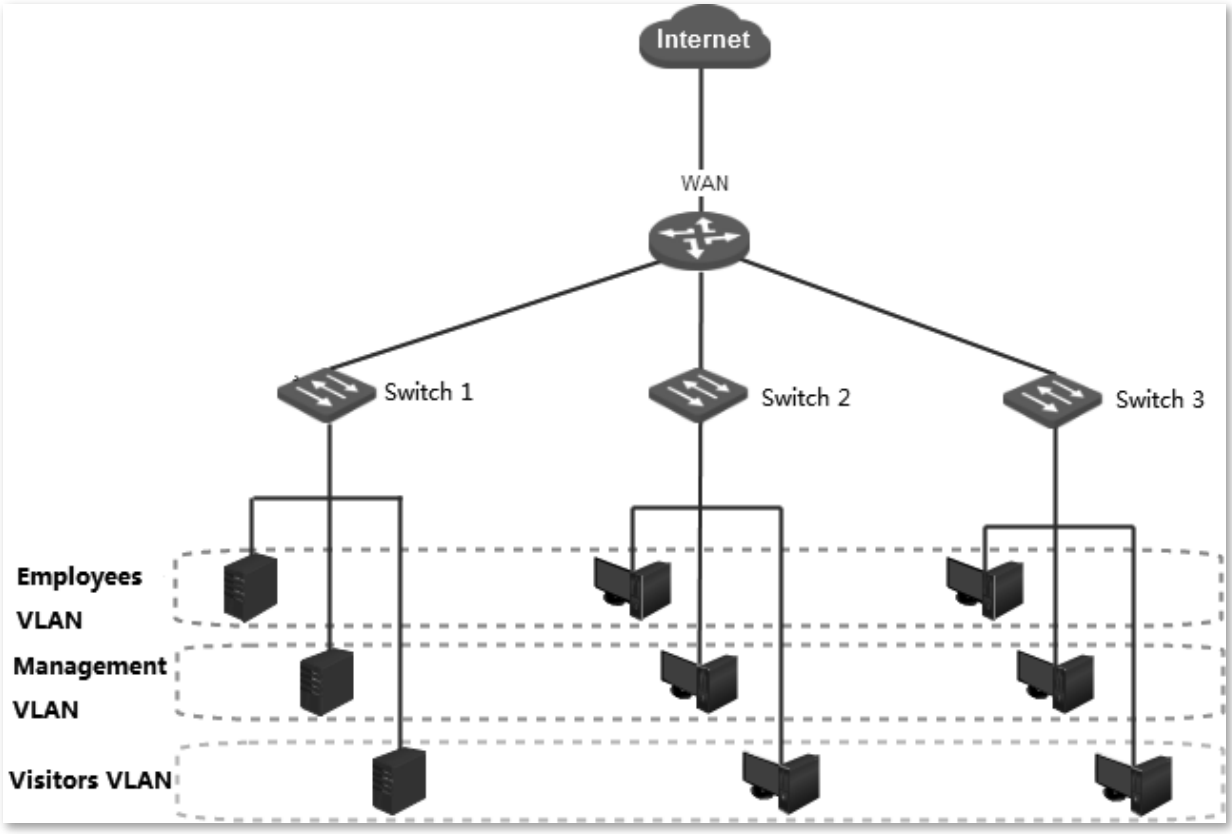
4.8 Configuring VLAN

4.8.1 Overview

In traditional shared media Ethernet and switch Ethernet, all users are in a broadcast domain. With the increasing number of computers in the network, the number of broadcast package grows up dramatically, which adds the data flow between all devices in the network, and then affects the network performance. As the network expands continually, broadcast storms may happen, making the entire network unusable.

VLAN (Virtual Local Area Network) is a technology that divides the devices in a LAN into different network segments logically instead of physically, so as to reach data exchange in a virtual workgroup. It divides a LAN into multiple logical local area networks – VLAN. Hosts in a VLAN are located in the same broadcast domain, which could communicate as if they are connected to the same network segment in any location; There is broadcast isolation between groups, hosts in different VALNs cannot communicate with others directly, must be forwarded by a router or other Layer 3 packet forwarding devices.

VALN application schematic diagram shows as below:



VLAN has the following advantages:

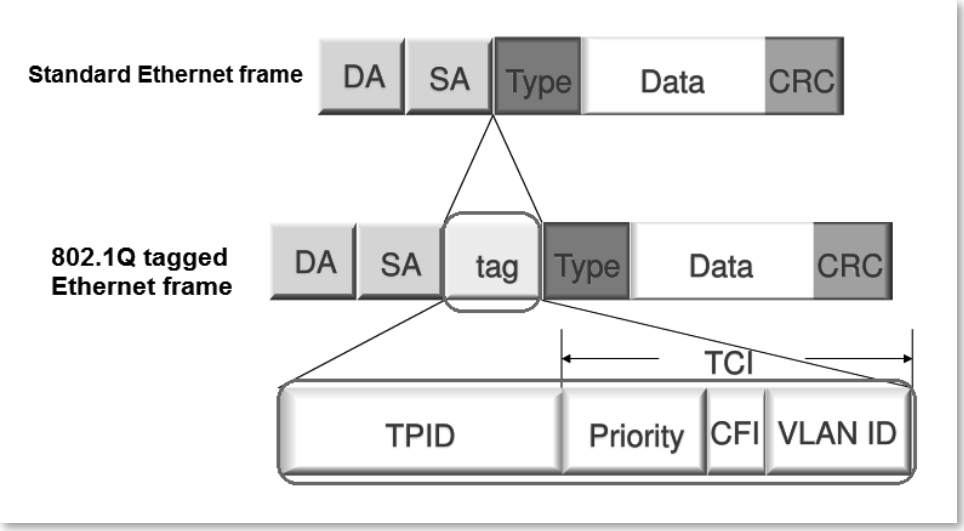
- Performance: Broadcast traffic is transmitted within the VLAN it resides on and cannot reach another VLAN, improving network performance.
- Costdown: VLAN helps reduce investment comparing with using routers or switches to segment LANs.

- Flexibility: VALN can be used to create virtual workgroups across physical network. If the VLANs are deployed properly, devices moved to a new physical place are still in the same VLAN and can access the internet.
- Security: Hosts in different VLANs cannot communicate with each other directly. Layer 3 packets must be forwarded by network devices such as routers or Layer 3 switches, which strengthen the security between different departments in the enterprise network.

This router supports IEEE 802.1Q VLAN. Detailed description is as following:

The IEEE issued the 802.1Q standard in 1999 to specify the implementation of the international standards for VLANs, making it possible to interoperate between devices from different manufacturers.

The 802.1Q protocol specifies that a 4-byte 802.1Q VLAN tag is encapsulated after the destination MAC address and source MAC address of the Ethernet frame to identify the VLAN related information. As shown in the figure below, the standard Ethernet frame becomes an 802.1Q tagged Ethernet frame by adding an 802.1Q VLAN tag after the destination MAC address (DA) and the source MAC address (SA).



The explanation of 802.1Q tag is as below:

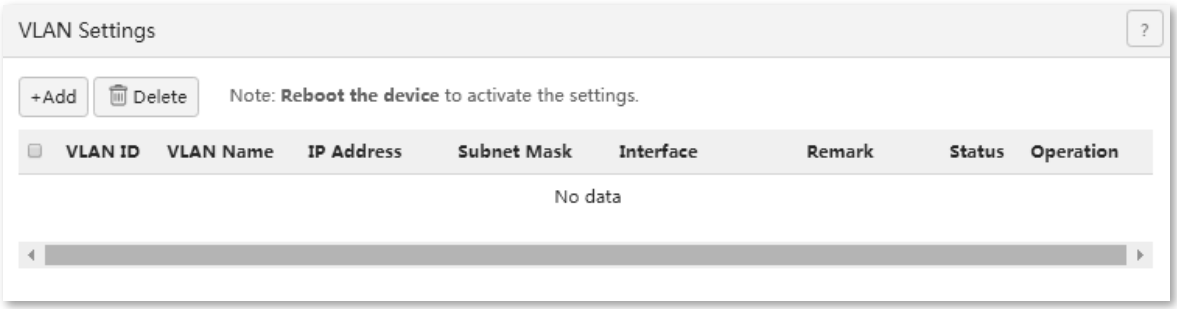
Segment	Description
TPID	Used to identify that the data frame is a data frame with an 802.1Q VLAN tag. The length of this segment is two bytes, which is 16 bits, and the IEEE 802.1Q protocol defines the value as 0x8100.
Priority	Used to identify the priority of data frame, mainly used to send packets with higher priority when the switch is blocked. The length of this segment is 3 bits. The value range is 0~7. 7 is the highest priority and 0 is the lowest priority.
CFI	It is used to identify whether the MAC address is encapsulated in the standard format. The length of this segment is 1 bit. 0 indicates that the MAC address is encapsulated in a standard format, while 1 indicates a non-standard format. For Ethernet switches, it is 0 by default.
VLAN ID	The identifier of VLAN, which is used to identify the 802.1Q VLAN to which the packet belongs. The length of this segment is 12 bits, and the value range is 0~4095. Usually, 0 and 4095 are not used, so the VID value is generally in the range of 1~ 4094.

4.8.2 Adding VLAN

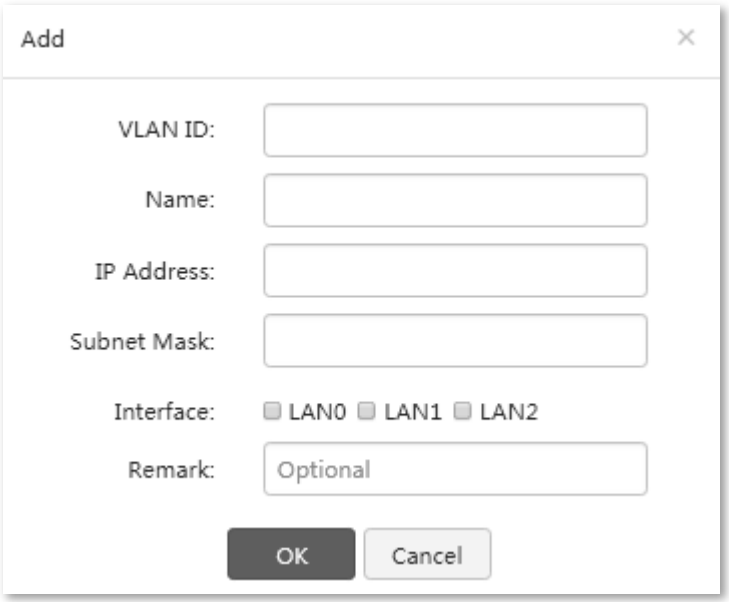
The port would be a Trunk port once VLAN is configured.

Adding VLAN rules

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



3. Set up rules of VLAN on the page that appears.



4. Click **OK**.
5. Go back to the page of **VLAN Settings**, and click **Reboot**. Reboot the device to activate the settings.

---End

Parameters Description

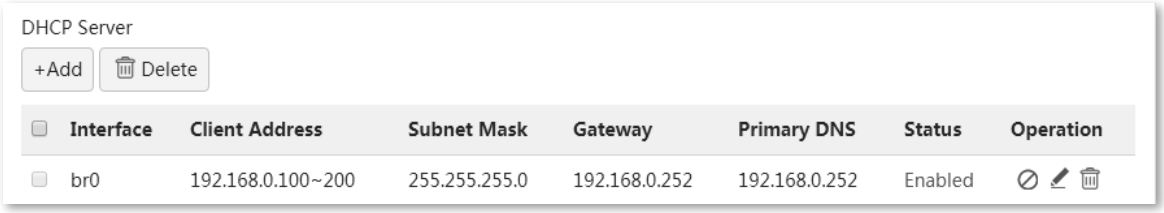
Parameters	Description
VLAN ID	Set up the value of VLAN ID, range is 10~4094.
VLAN Name	Set up the name of VLAN port.

Parameters	Description
IP Address	Set up the IP address of VLAN.
Subnet Mask	Set up the subnet mask of VLAN.
Port	Select the corresponding physical ports of VLAN. 1 VLAN port can correspond to multiple physical ports, 1 physical port can also correspond to multiple VLAN ports.
Remark	Set up the related information of the VLAN rules.
Status	It specifies the current status of the rule, including **Enabled** and **Disabled**. The status is enabled by default after adding a new rule. When it is enabled, click to change status as **Disabled**, click can change the status as **Enabled**.

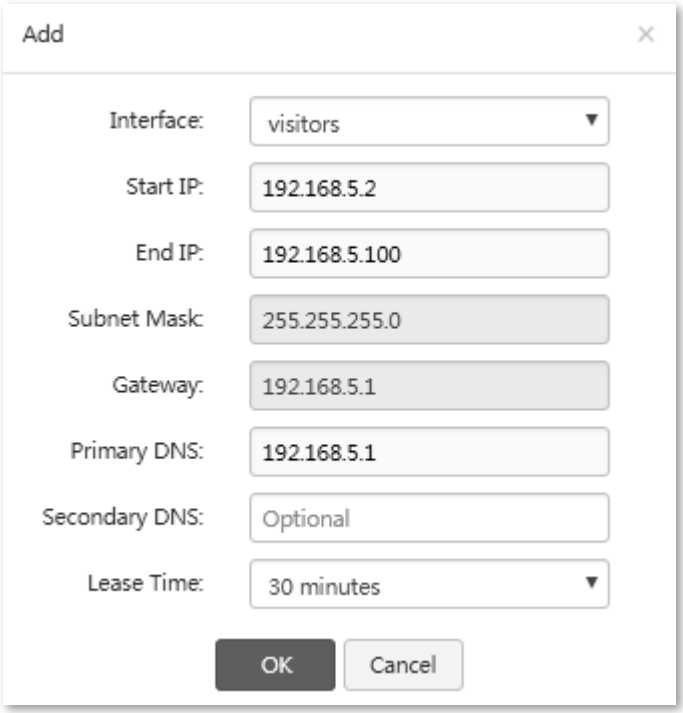
Configuring VLAN DHCP Server

After adding a VLAN rule, you need to set up DHCP server for it. Otherwise, the clients under this VLAN cannot obtain an IP address automatically.

1. Click **Network** > **LAN Settings**, locate **DHCP Server**.
2. Click +Add.

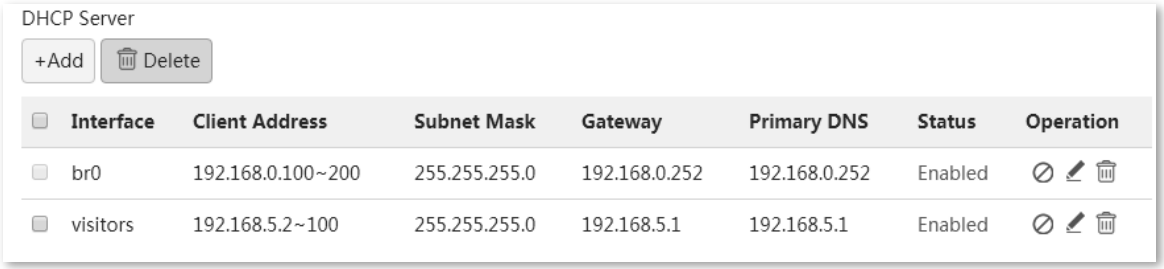


3. Configure DHCP server information on the page that appears.
4. **Port**: Choose the VLAN you set from the drop-down list, such as **visitors**.
5. **Start/End IP Address**: You can assign IP range by configuring DHCP server, IP address segment should be the same as the gateway address, such as **192.168.5.2 - 192.168.5.100**.
6. **Primary DNS**: You can set it as gateway address or a correct DNS, such as **192.168.5.1**.
7. Click **OK**.



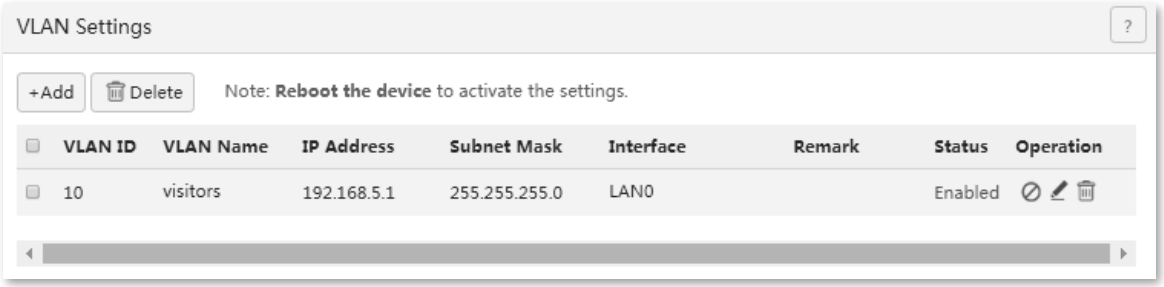
---End

Configuration succeeds.

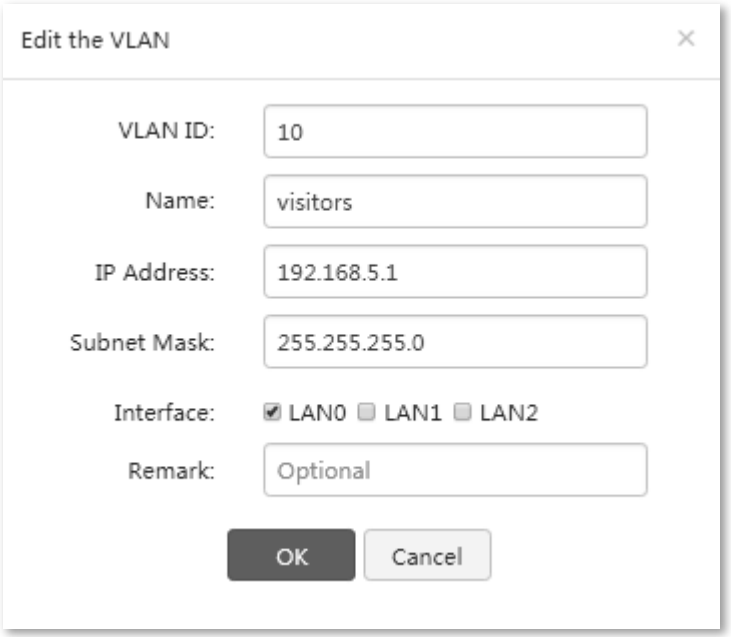


4.8.3 Modifying VLAN rules

1. Click **Network** > **VLAN Settings**.
2. Locate the rule you want to modify, and click .



3. Modify related parameters.
4. Click **OK**.

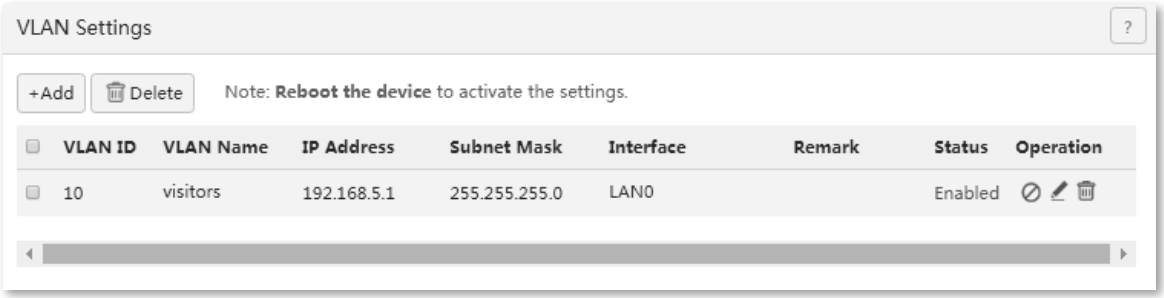


5. Go back to **VLAN Settings** page, and click **Reboot**. Reboot the device to activate the settings.

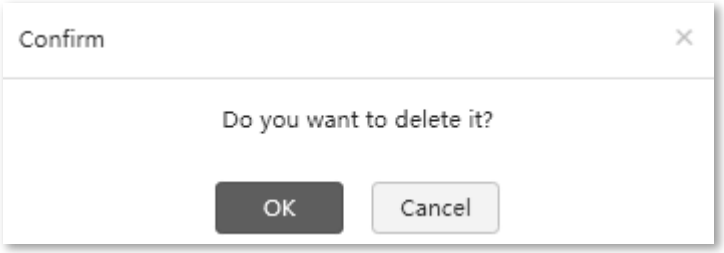
---End

4.8.4 Deleting VLAN rules

1. Click **Network** > **VLAN Settings**.
2. Select the rules you want to delete and click .



3. Click **OK** on the popup window.



4. Go back to **VLAN Settings** page, click **Reboot the device**, to activate the settings.

---End

4.8.5 An example of configuring VLAN settings

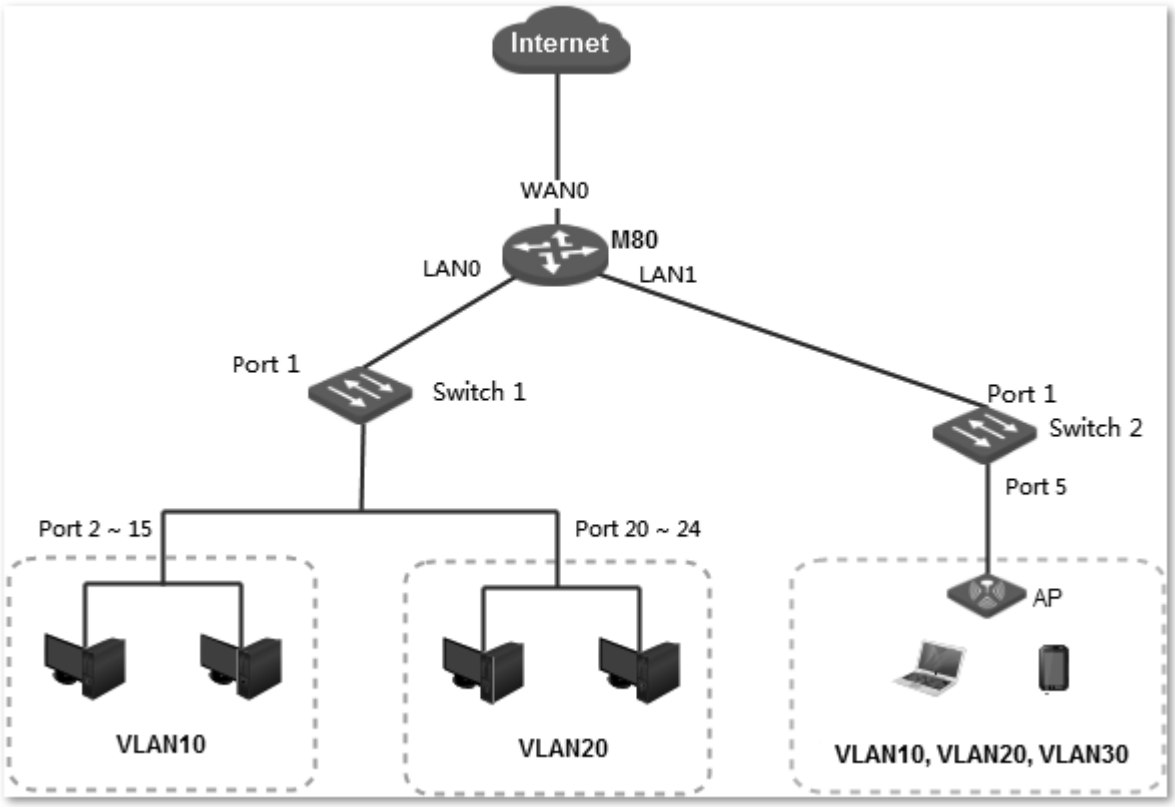
Scenario Requirements

A company adopts M80 + AP to deploy the network environment. Follow the following rules to apply different access permissions for employees, managers, and visitors.

- Employees can access to the internet through wired and wireless connections by a user name and password.
- Managers can access to the internet through wired and wireless access networks without authentication.
- Visitors could access to the internet by wireless connection without authentication.

Solution

You are recommended to combine the router's VLAN function with captive portal function, to make different user groups access to the internet. The employees are assigned to VLAN10, managers to VLAN20, and visitors to VLAN30. Assume that the network topology is as follow:



Procedures:

Set up you router

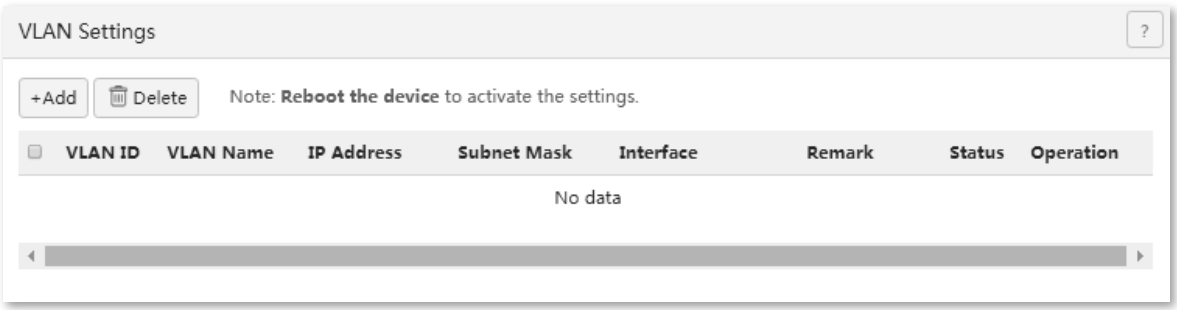
Set up VLAN and DHCP server separately for LAN0 and LAN1.

I. Set up VLAN.

1. Add VLAN10.

   (1) Click **Network** > **VLAN Settings**.

   (2) Click +Add.



   (3) Set **VLAN ID** to **10**.

   (4) Set the name of the rule, which is **employees** in this example.

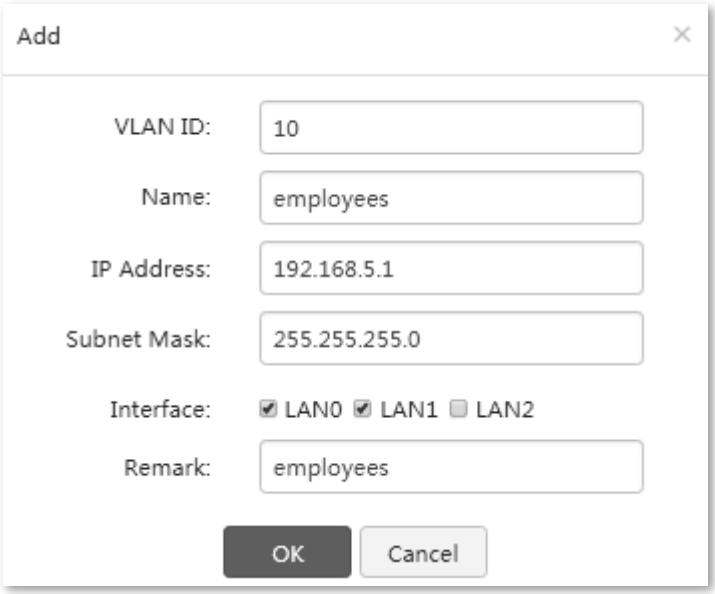
   (5) Set up an IP address, which is **192.168.5.1** in this example.

   (6) Set up a subnet mask, which is **255.255.255.0** in this example.

   (7) Select a VLAN port, which is **LAN0&LAN1** in this example.

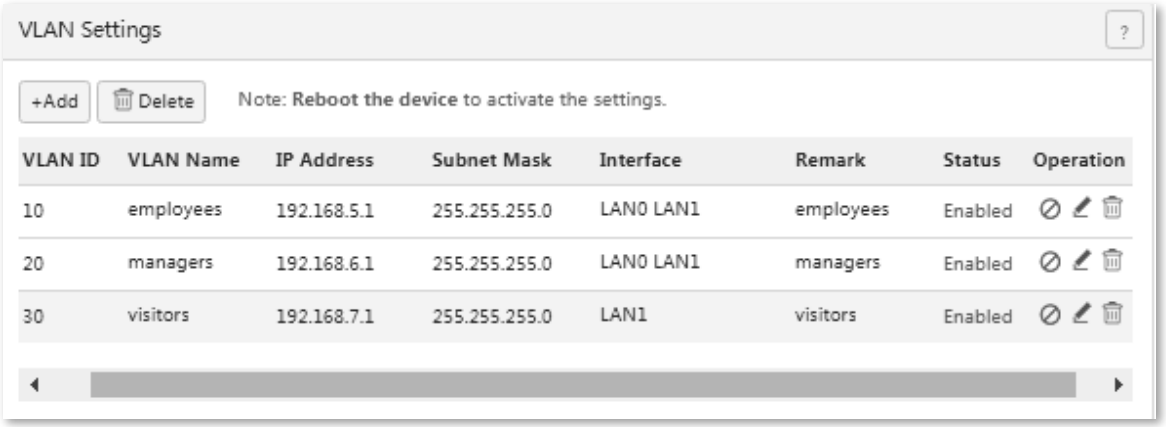
   (8) Set the remark information for this rule, which is **employees** in this example.

   (9) Click **OK**.



2. Repeat the preceding **step 1** to add VLAN20 and VLAN30.

3. Go back to **VLAN Settings** page, click **Reboot the device**, and follow the on-screen instructions to activate the settings.

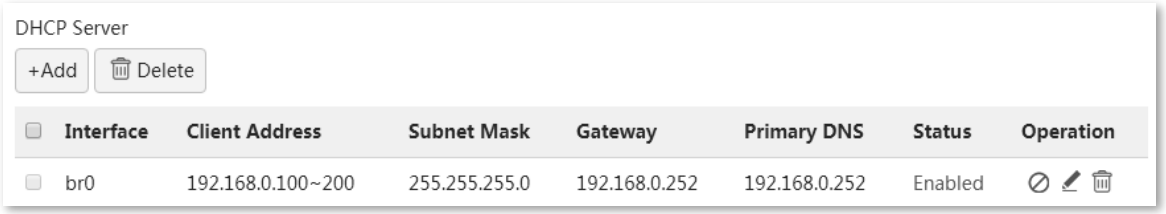


II. Set up DHCP Server for VLAN.

1. Set up DHCP Server for VLAN10.

   (1) Click **Network** > **LAN Settings**, and locate **DHCP Server** section.

   (2) Click +Add.

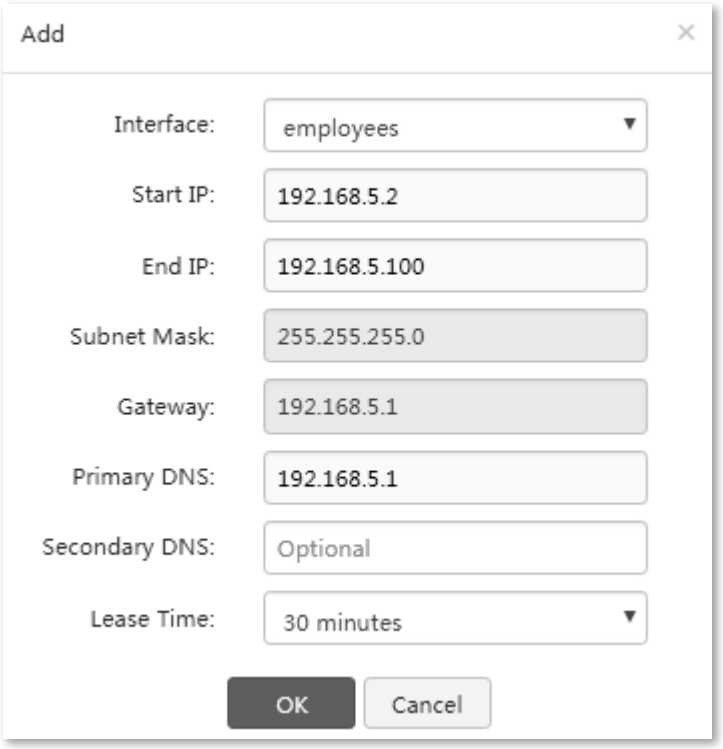


   (3) Select the VLAN you set before, which is **employees** in this example.

   (4) Set **Start/End IP address** to the IP address range assigned to the clients. IP address segment should be the same as gateway, which is **192.168.5.2-192.168.5.100** in this example.

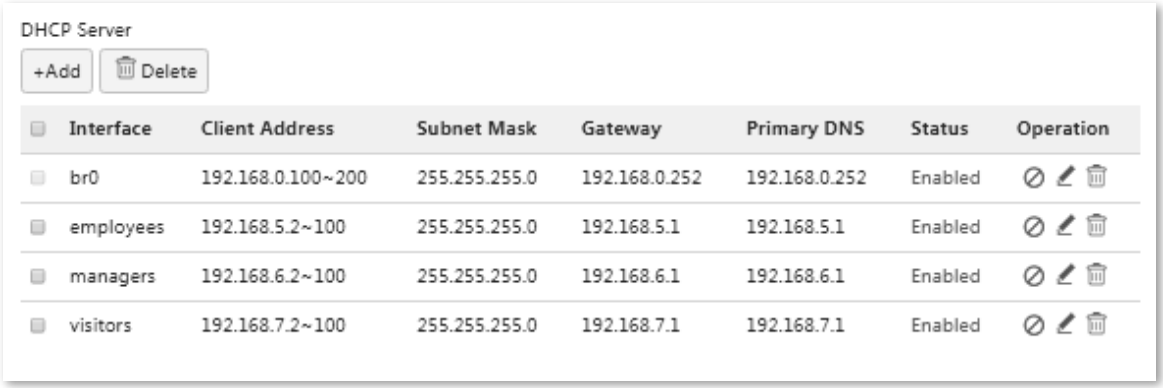
   (5) Set **Primary DNS** to a gateway address or a correct DNS, which is **192.168.5.1** in this example.

   (6) Click **OK**.



2. Repeat the preceding **step 1** to set up DHCP server for VLAN20 and VLAN30.

Added successfully, see the following figure:



III. Set up Captive Portal.

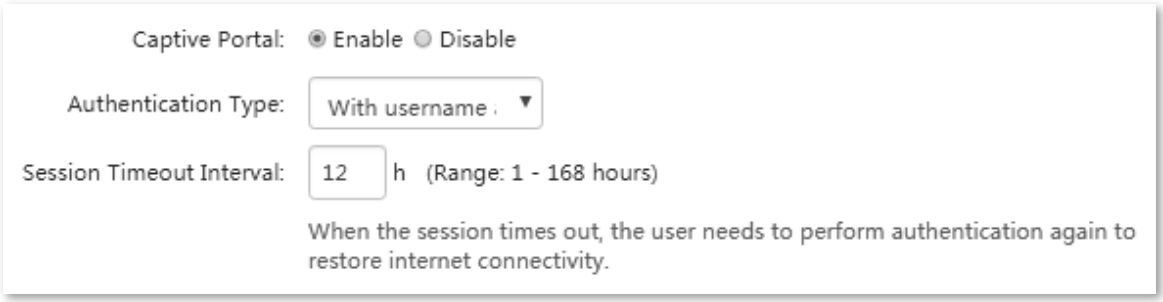
1. Set up Captive Portal basic settings.

   (1) Click **Captive Portal** > **Basic Settings**.

   (2) Set **Captive Portal** to **Enable**.

   (3) Set **Authentication Type** to **With username and password**.

   (4) Set **Session Timeout Interval** to the expiration time, which is **12** in this example.



(5) **Logo**: Click **Change Image** to upload the logo image of the company.

(6) **Title**: Enter the title displayed on the authentication page, which is **Welcome to IP-COM** in this example.

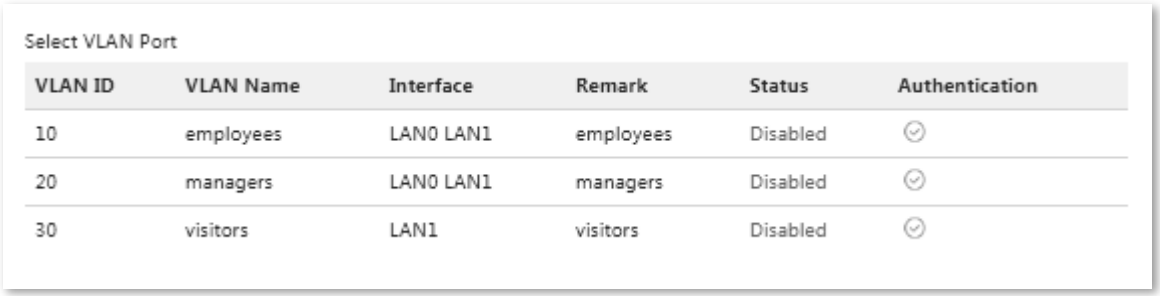
(7) **Background Image**: Click **Change Image** to upload the background image displayed on the authentication page, such as the company's advertising photo.

(8) **Disclaimer**: Set up the company's disclaimer information, which is **@2018 IP-COM Networks Co., Ltd. All rights reserved.** in this example.

(9) **Redirected To**: Select **Specified Page**, and enter the website address where the client is redirected to after authentication completes, which is www.google.com in this example.

2. Enable **Captive Portal** for VLAN10.

(1) Locate the rule for VLAN, click .



(2) Click **OK** on the bottom of this page.

3. Add a Captive Portal account.

(1) Click **Captive Portal** > **User Management**.

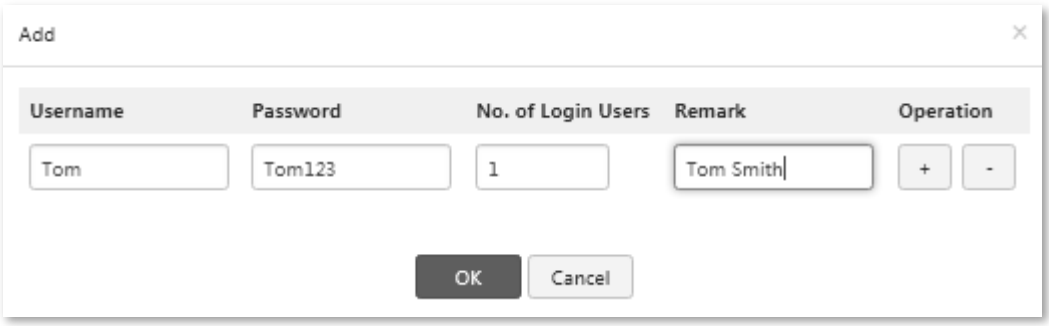
(2) In **User Management** module, click +Add.

(3) Enter the username, which is **Tom** in this example.

(4) Enter the password for authentication, which is **Tom123** in this example.

(5) Set the Remark information of the account, which is **Tom Smith** in this example. If you need to add more users, click +, and repeat the above procedures.

(6) Click **OK**. Repeat **step (2)** to add more accounts as needed.



IV. Set up a policy to AP (Example: IP-COM AP375).

Enable SSIDs for both 2.4 GHz and 5 GHz on AP, and set up VLAN10, VLAN20 and VLAN30 separately, detailed information is shown as below:

Wireless access community	SSID Assignment	VLAN ID
Employees	Office network	VLAN10
Managers	Management network	VLAN20
Visitors	Guest network	VLAN30

1. Log in to the Web UI of M80.
2. Set up wireless information of AP.

(1) Click **AC Management** > **Wireless Settings** to enter the configuration page.

(2) **AC Management**: Click **Enable** to enable this function.

(3) **Status**: Select **Enable**.

(4) **SSID**: Set up the wireless network name to send out for AP, which is **Office network** in this example.

(5) **Frequency band**: Select **2.4G & 5G**.

(6) **Max. user numbers**: Enter the max. user numbers to connect to this SSID, which is **50** in this example.

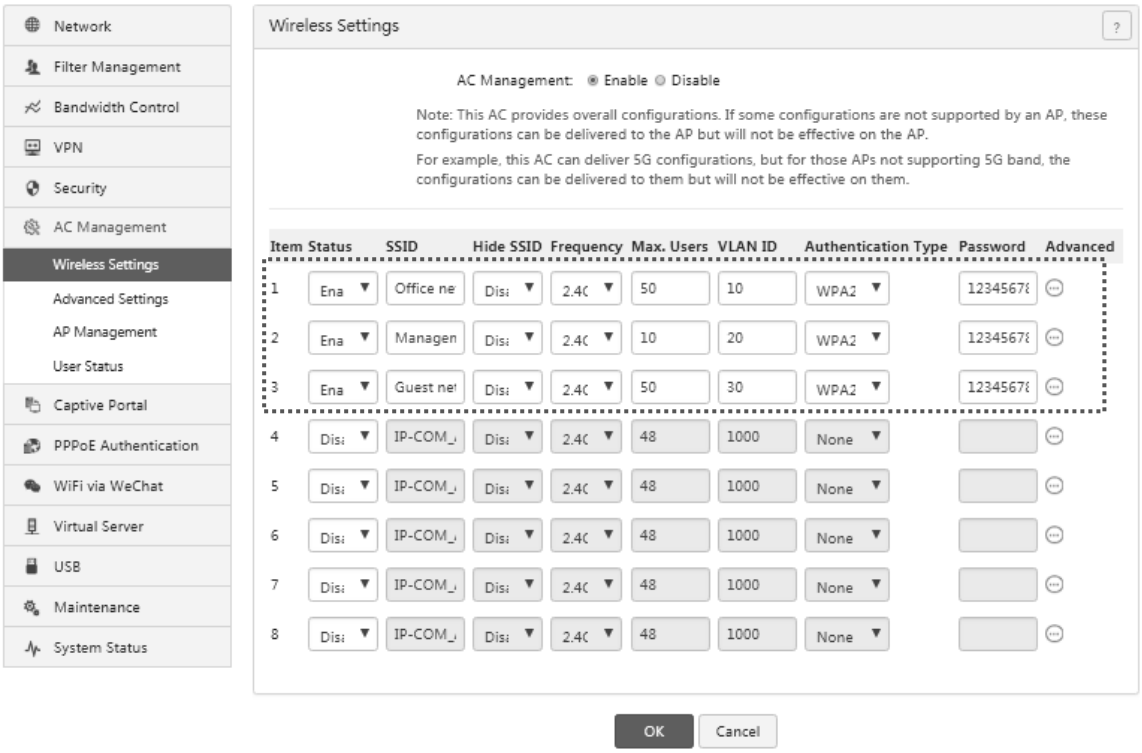
(7) **VLAN ID**: Set a VLAN ID, which is **10** in this example.

(8) **Authentication Type**: Choose authentication type for this SSID, which is **WPA2-PSK** in this example.

(9) **Password**: Enter wireless password, which is **12345678** in this example.

(10) Refer to Step (3)~(9) to add **Management network** and wireless information of **Guest network**.

(11) Click **OK**.

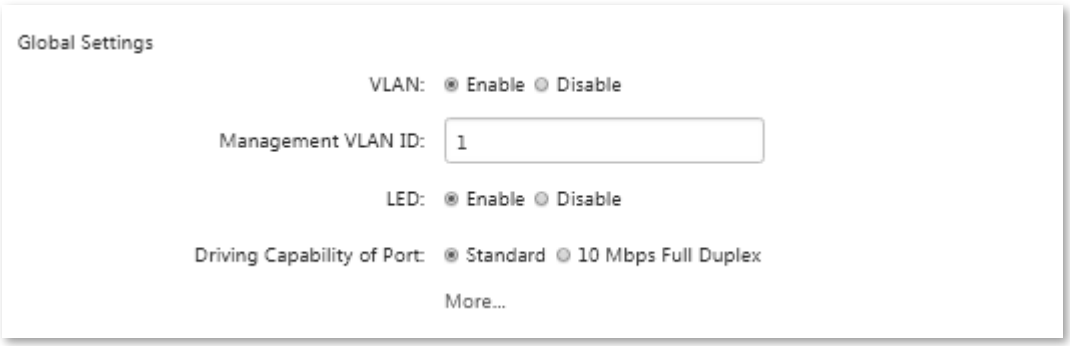


3. Enable the QVLAN function.

(1) Click **AC Management** > **Advance Settings**, and locate **Global Settings** module.

(2) VLAN: Click **Enable**.

(3) Click **OK**.



---End

Configure the switches

Set up 802.1Q VLAN on the switches.

- Set the ports connected by the employees as **Access** ports, allow VLAN10 pass through.

- Set the ports connected by the managers as **Access** ports, allow VLAN20 pass through.
- Set the ports connected to AP as **Trunk** port, allow VLAN10, VLAN20, and VLAN30 pass through.

Settings of Switch 1 are as below:

Port	VLAN ID（VLAN allowed to pass through）	Port Link Type	PVID
Port 1 (connected to M80)	10, 20	Trunk	1
Port 2~15 (connected to the employees)	10	Access	10
Port 20~24 (connected to the managers)	20	Access	20

Settings of Switch 2 are as below:

Port	VLAN ID（VLAN allowed to pass through）	Port Link Type	PVID
Port 1 (connected to M80)	10, 20, 30	Trunk	1
Port 5 (connected to AP)	10, 20, 30	Access	10

As switches are different when deploying the network, please refer to the corresponding user guide for detailed configuration instructions. We take IP-COM F1226P as an example below.

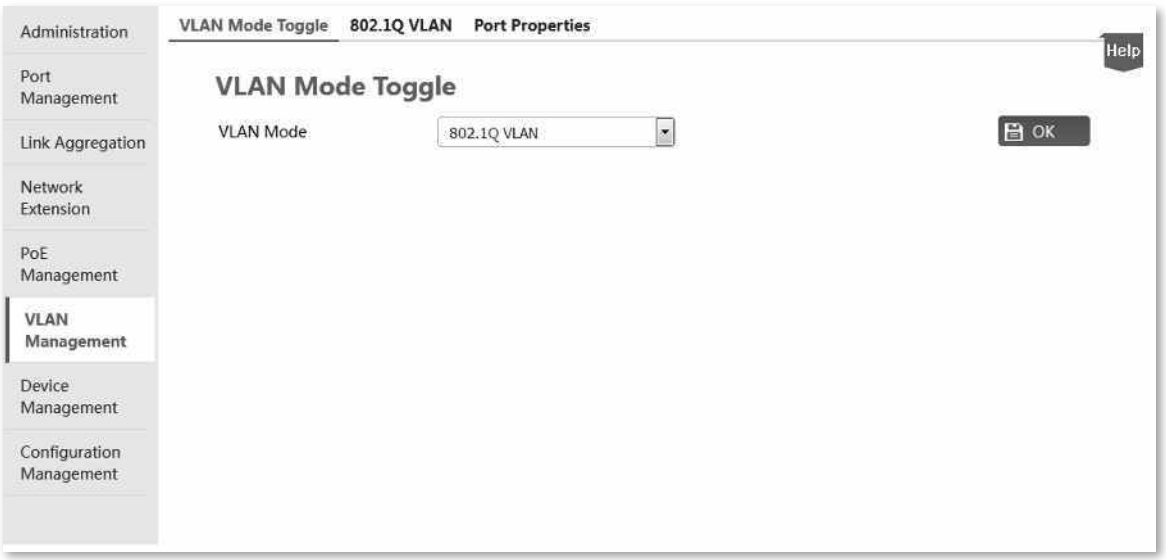
I. Configure Switch 1.

1. Set up the VLAN mode as 802.1Q VLAN.

   (1) Log in to the Web UI of the switch, and click **VLAN Management** to enter the configuration page.

   (2) VLAN Mode: Select **802.1Q VLAN**.

   (3) Click **OK**.



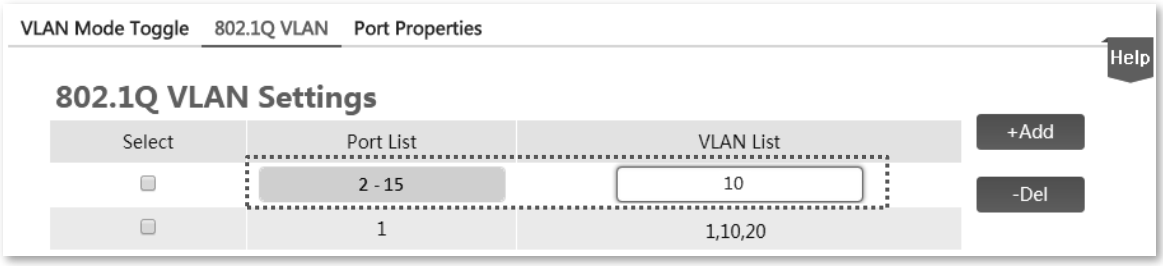
2. Set up 802.1Q VLAN.

   (1) Click **VLAN Management** > **802.1Q VLAN** to enter the configuration page.

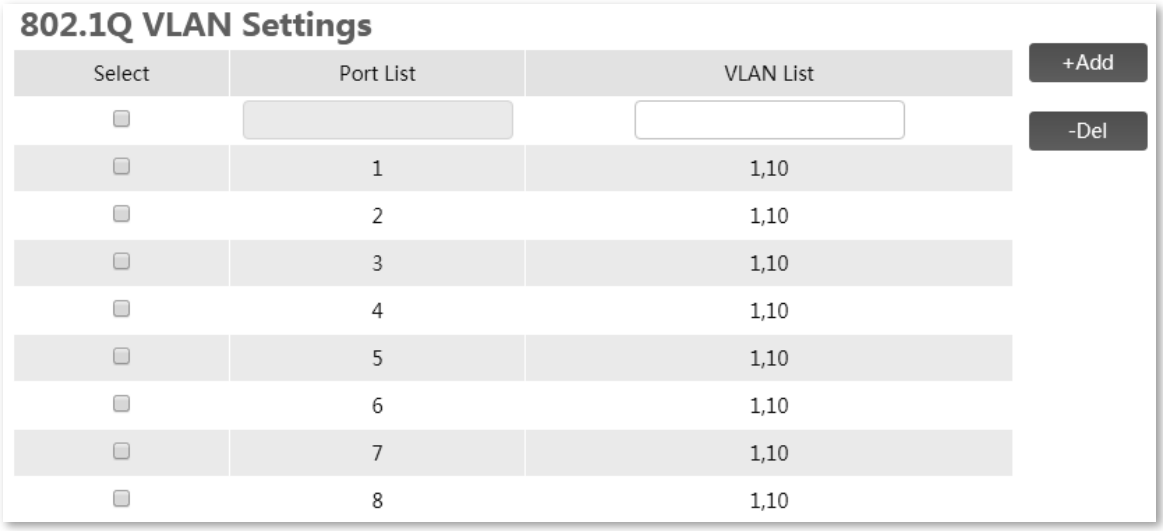
   (2) Choose port **1**, and then enter **10** in the input box under VLAN, click +Add.

   (3) Repeat **step 2** to add VLAN20 to port 1.

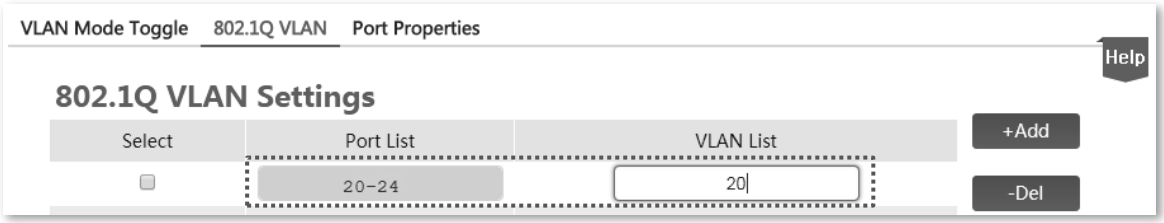
(4) Choose port **2~15**, and then enter **10** in the input box under VLAN, click +Add.



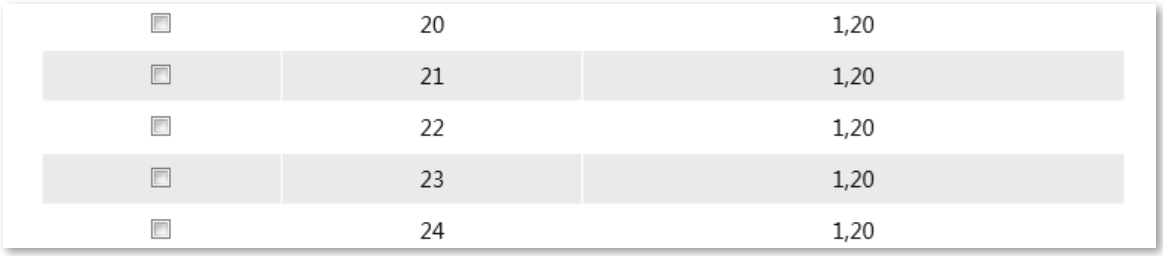
Add successfully.



(5) Choose port **20~24**, and then enter **20** in the input box under VLAN, click +Add.



Add successfully.



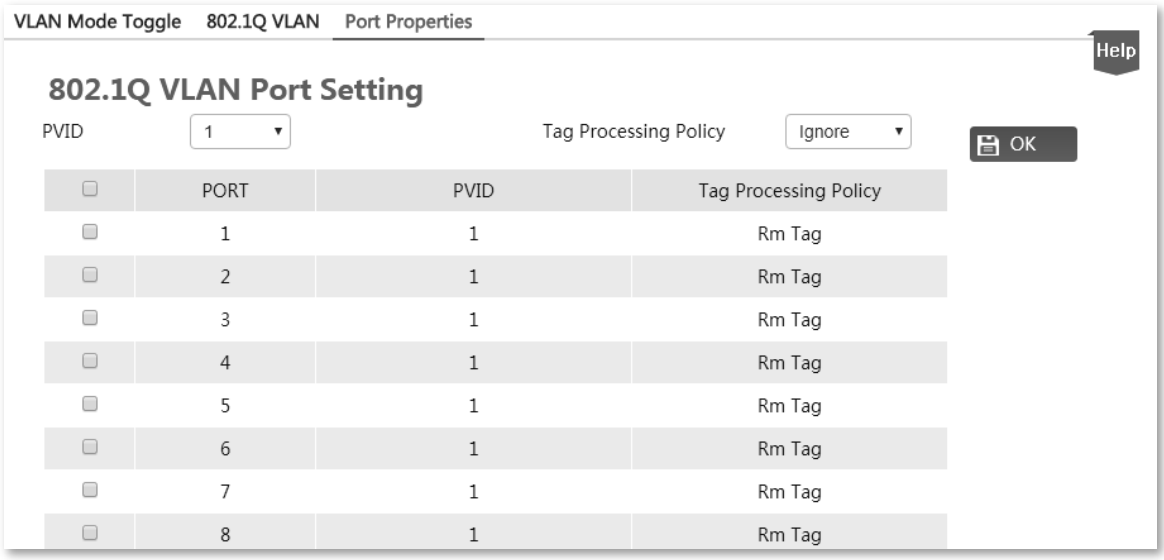
3. Set up port properties.

(1) Click **VLAN Management** > **Port Properties** to enter the configuration page.

(2) Select port **1**, and set **PVID** as **1,** choose **Tag Processing Policy** as **Add Tag**, and click **OK**.

(3) Select port **2~15**, set **PVID** as **10**, choose **Tag Processing Policy** as **Rm Tag**, and click **OK**.

(4) Select port **20~24**, set **PVID** as **20**, choose **Tag Processing Policy** as **Rm Tag**, and click **OK**.



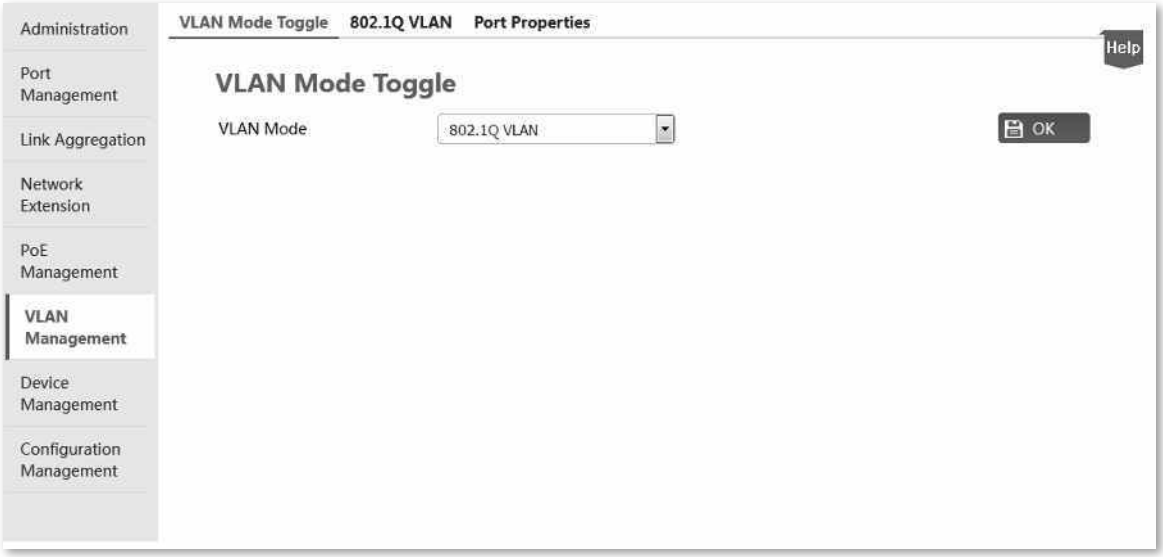
II. Configure Switch 2.

1. Set up the VLAN mode as 802.1Q VLAN.

(1) Log in to the Web UI of the switch, and click **VLAN Management** to enter the configuration page.

(2) **VLAN Mod**e: Select **802.1Q VLAN**.

(3) Click **OK**.

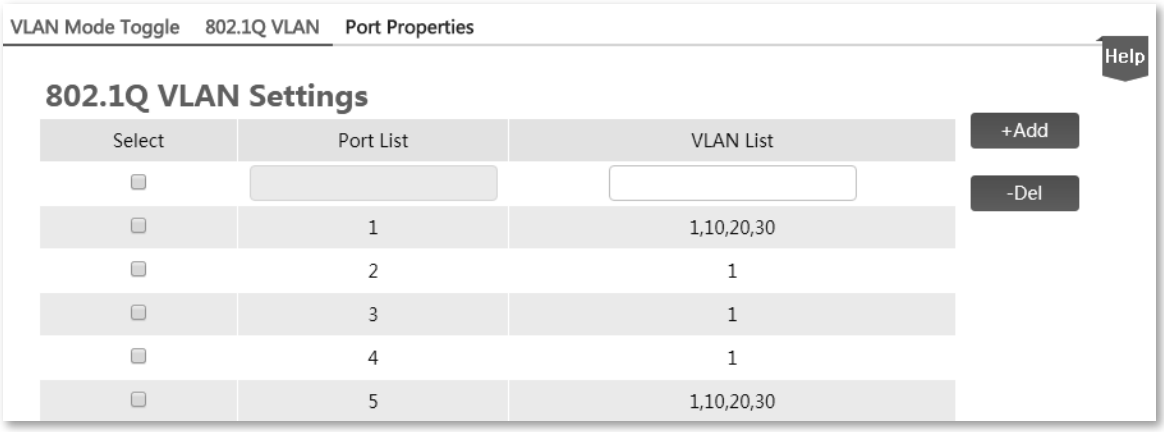


2. Set up 802.1Q VLAN.

(1) Click **VLAN Management** > **802.1Q VLAN** to enter the configuration page.

(2) Choose port **1** and **5**, and then enter **10** in the input box under VLAN, click +Add.

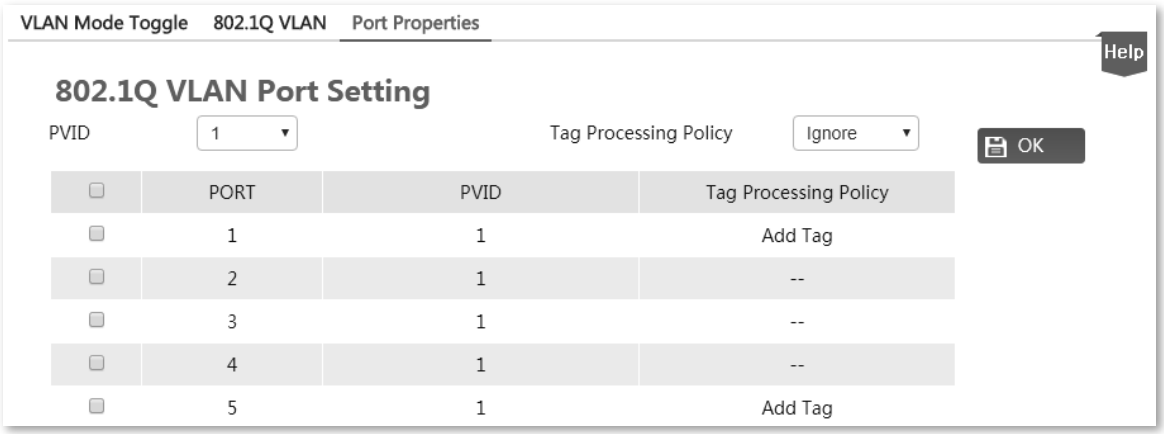
(3) Repeat **step 2** to add **VLAN20**/**VLAN30** for both port **1** and **5**.



3. Set up port properties.

   (1) Click **VLAN Management** > **802.1Q VLAN** to enter the configuration page.

   (2) Select port **1** and **5**, set **PVID** as **1**, choose **Tag Processing Policy** as **Add Tag**, and click **OK**.



---End

Verification

- The employees connected to port 2 ~15 of switch 1 could access to the internet by captive portal.
- The management group connected to port 20~24 could access to the internet directly.
- The devices connected to the SSID named **Office network** could access to the internet by captive portal.
- The devices connected to the SSID named **Management network** could access to the internet directly.
- The devices connected to the SSID named **Guest network** could access to the internet directly.

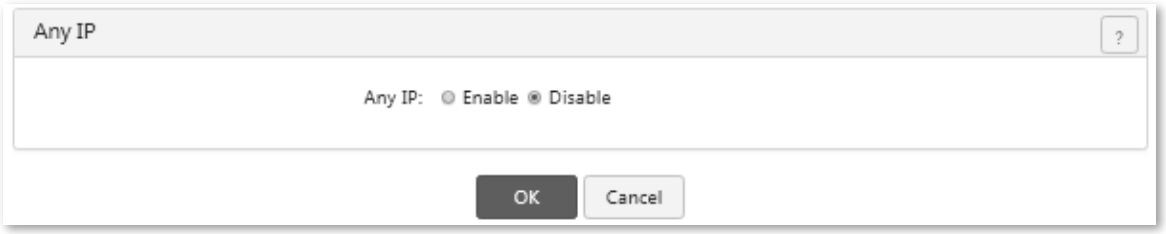
4.9 Configuring Any IP

Any IP, that is, the router allows the client to access the internet by any IP address.

When it is enabled, the client could access to the internet by configuring any IP address, gateway and DNS, no need to check the IP address of the computer network adapter.

Choose **Network** > **Any IP** to enter the configuration page.

This function is disabled by default. You can enable or disable this function as needed.



4.10 Configuring the DNS cache

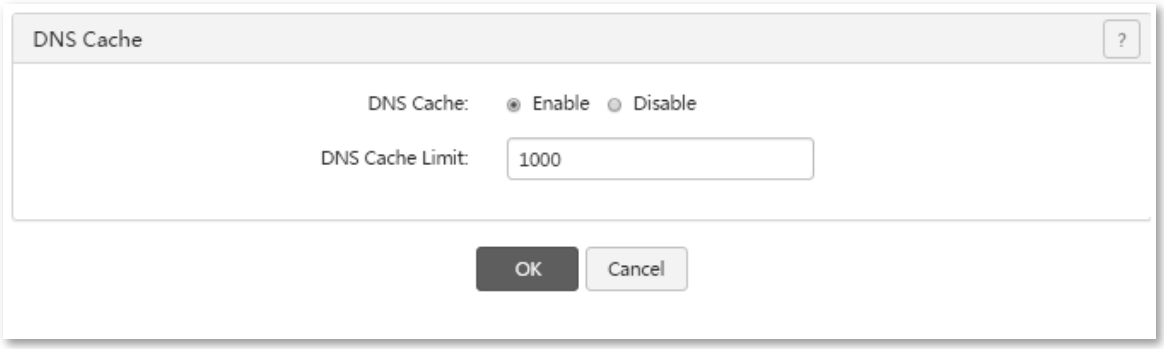
4.10.1 Overview

On the page of **DNS Cache**, you can enable/disable the DNS cache function and set DNS cache limit.

M80 supports the DNS cache function, which enables the router to cache DNS-resolved information about websites accessed by users. When other users access the websites, the router directly uses the information in the cache to direct the users to the websites without accessing the DNS server. This improves the website accessing speed.

4.10.2 Configuring the DNS cache

To access the page for configuring the DNS cache, choose **Network** > **DNS Cache**. See the following figure.



By default, the DNS cache contains 1,000 entries. A maximum of 10,000 entries is allowed.

5 Filter management

5.1 Overview

This chapter describes:

- Setting IP address groups and time groups
- Setting the IP address filter
- Setting the MAC address filter
- Setting the port filter
- Setting the web filter
- Setting multi-WAN policies

5.1.1 Function description

IP address group and time group

This function allows you to set IP address groups and time groups. Time groups are used for the MAC address filter, port filter, web filter, and user-defined bandwidth control, while IP address groups are used for the port filter, web filter, and user-defined multi-WAN policies.

IP address filter

You can set an IP address whitelist and/or an IP blacklist to enable or disable users to access the internet through the router. The whitelist and blacklist are described as follows:

- **Whitelist**: Users in the whitelist are allowed to access the internet.
- **Blacklist**: Users in the blacklist are not allowed to access the internet.

MAC address filter

You can set a MAC address whitelist and/or a MAC address blacklist to enable or disable users to access the internet through the router. The whitelist and blacklist are described as follows:

- **Whitelist**: Users in the whitelist are allowed to access the internet.
- **Blacklist**: Users in the blacklist are not allowed to access the internet.

Port filter

The protocols of various services available over the internet use dedicated port numbers. The common service port numbers range from 0 to 1023 and are generally assigned to specific services.

A port filter prevents LAN users from accessing certain internet services by disabling the users to access the port numbers of the services.

Web filter

A web filter prevents LAN users from accessing specified types of website for controlling internet accessibility of LAN users so that they will not spend time on websites irrelevant to their duties. Before you add web filter rules, add web categories.

Multi-WAN policy

The router has 2 WAN ports by default but allows a maximum of 4 WAN ports. When multiple WAN ports are operational at the same time, an appropriate multi-WAN policy can greatly improve the bandwidth usage of the router. The router supports the following types of multi-WAN policy:

- Smart load balancing (default): If such a policy is applied, the router automatically distributes traffic based on the **bandwidth** on the **Bandwidth Control** page through the WAN ports to achieve load balancing.
- Custom policy: Such a policy is configured by an administrator to distribute data of specified IP address groups to specified WAN ports.

5.1.2 Configuration instruction

Setting an IP filter

Step	Task	Description
1	Set time groups.	Time groups are required when an IP filter is set. Choose **Filter Management** > **IP Group & Time Group** and set time groups.
2	Set IP address groups.	IP address groups are required when an IP filter is set. Choose **Filter Management** > **IP Group & Time Group** and set IP address groups.
3	Set an IP filter.	Choose **Filter Management** > **IP Filter** and set an IP filter.

Setting a MAC address filter

Step	Task	Description
1	Set time groups.	Time groups are required when a MAC address filter is set. Choose **Filter Management** > **IP Group & Time Group** and set time groups.
2	Set a MAC address filter.	Choose **Filter Management** > **MAC Filter** and set a MAC address filter.

Setting a port filter or web filter

Step	Task	Description
1	Set time groups.	Time groups are required when a port filter or web filter is set. Choose **Filter Management** > **IP Group & Time Group** and set time groups.
2	Set IP address groups.	IP address groups are required when a port filter or web filter is set. Choose **Filter Management** > **IP Group & Time Group** and set IP address groups.
3	Set a port filter or a web filter.	Choose **Filter Management** > **Port Filter** and set a port filter. Choose **Filter Management** > **Web Filter** and set a web filter.

Customizing a multi-WAN policy

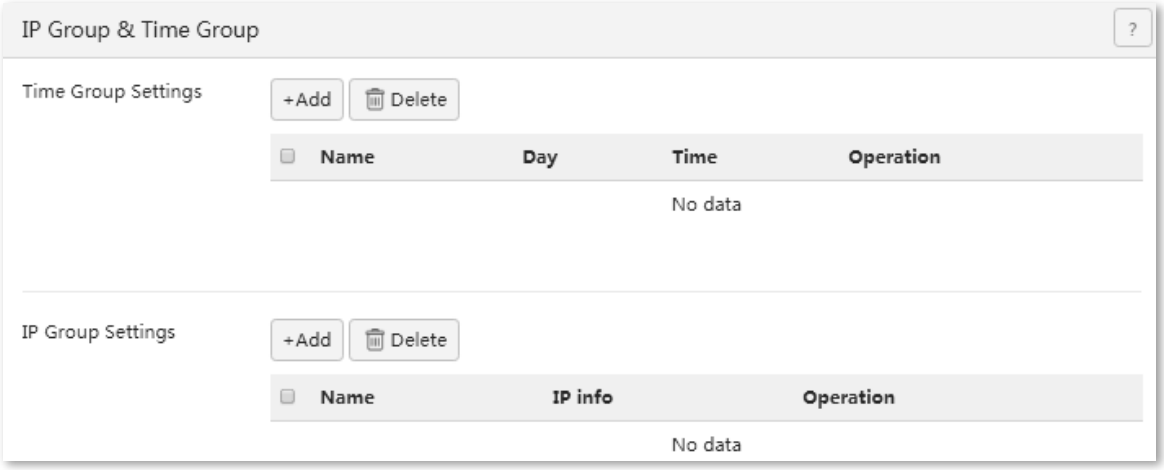
Step	Task	Description
1	Set IP address groups.	IP address groups are required when a multi-WAN policy is customized. Choose **Filter Management** > **IP Group & Time Group** and set IP address groups.
2	Customize a multi-WAN policy.	Choose **Filter Management** > **Multi-WAN Policy** and customize a multi-WAN policy.

Setting a multi-WAN policy for smart load balancing

1. Choose **Filter Management** > **Multi-WAN Policy**.
2. Select **Smart Load Balancing**.

5.2 Setting IP address groups and time groups

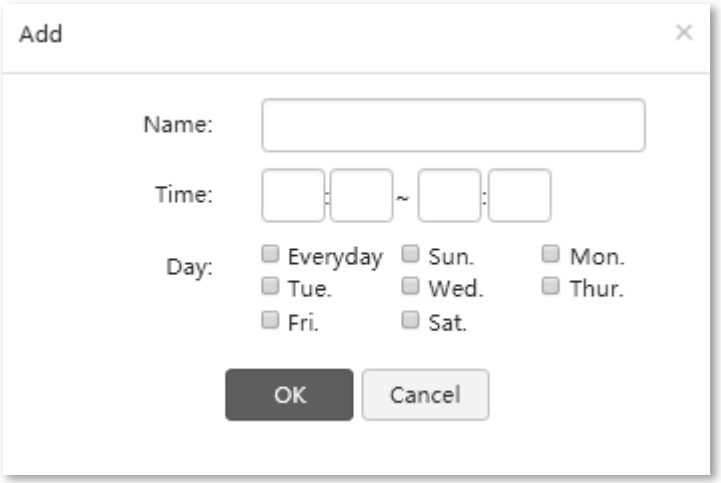
To access the page for setting IP address groups and time groups, choose **Filter Management** > **IP Group & Time Group**. See the following figure.



5.2.1 Setting time groups

Adding a time group

1. Choose **Filter Management** > **IP Group & Time Group**.
2. Click +Add in the **Time Group Settings** area.
3. Set the required parameters.
4. Click **OK.**



---End

Parameter description

Parameter	Description
Name	It specifies the name of a time group. Duplicate group names are not allowed.
Time	It specifies the start time and end time in a day. **00:00~00:00** indicates a whole day.
Day	It specifies the days of week included.

Modifying a time group

1. Choose **Filter Management** > **IP Group & Time Group**.
2. Click corresponding to an available time group.

Note

If a time group that has been referenced, the modified time group will be automatically referenced after the modification.

Deleting a time group

1. Choose **Filter Management** > **IP Group & Time Group**.
2. Click corresponding to a time group to be deleted. To delete multiple time groups at the same time, select them and click Delete.

Note

A time group that has been referenced cannot be deleted.

5.2.2 Setting IP address groups

Adding an IP address group

1. Choose **Filter Management** > **IP Group & Time Group**.
2. Click +Add in the **IP Group Settings** area.
3. Set the required parameters.

4. Click **OK**.

---End

Parameter description

Parameter	Description
Name	It specifies the name of an IP address group. Duplicate group names are not allowed.
IP Range	It specifies the start IP address and end IP address of an IP address group.

Modifying an IP address group

1. Choose **Filter Management** > **IP Group & Time Group**.
2. Click corresponding to an available IP address group.

Note

If a time group that has been referenced, the modified time group will be automatically referenced after the modification.

Deleting an IP address group

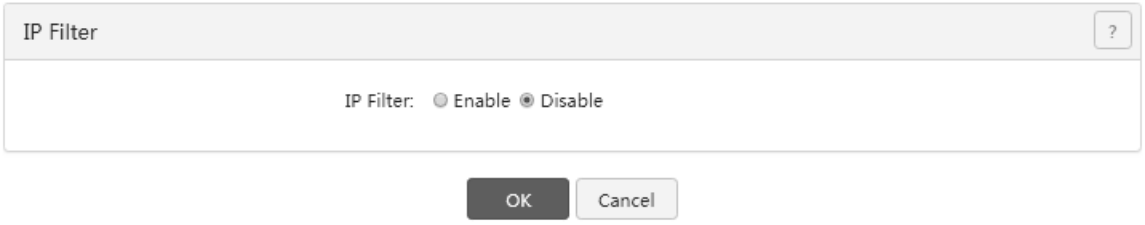
1. Choose **Filter Management** > **IP Group & Time Group**.
2. Click corresponding to an IP address group to be deleted.
   The group is deleted. To delete multiple IP address groups at the same time, select them and click Delete.

Note

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

5.3 Setting the IP address filter

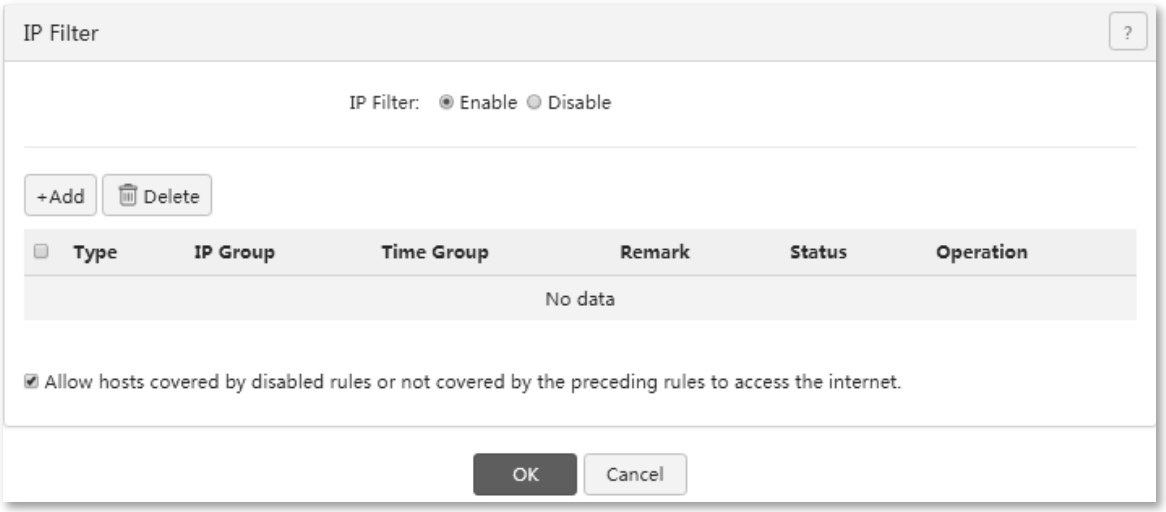
To access the page for setting IP address filter, choose **Filter Management** > **IP Filter**. See the following figure.



5.3.1 Setting IP address filter

Enabling the IP address filter

1. Choose **Filter Management** > **IP Filter**.
2. Set **IP Filter** to **Enable**.
3. Click **OK**.



---End

The IP address filter is enabled. Then, you can set IP address filtering rules.

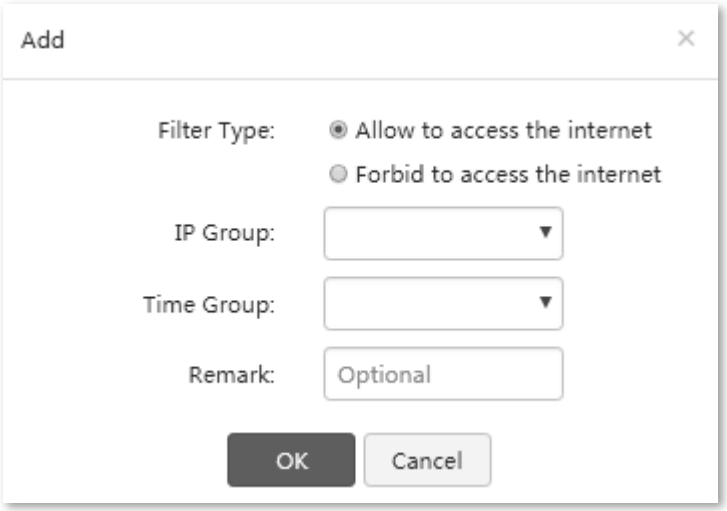
Setting IP address filtering rules

Adding a rule

1. Choose **Filter Management** > **IP Filter**.
2. Click +Add.

3. Set required parameters.

4. Click **OK**.

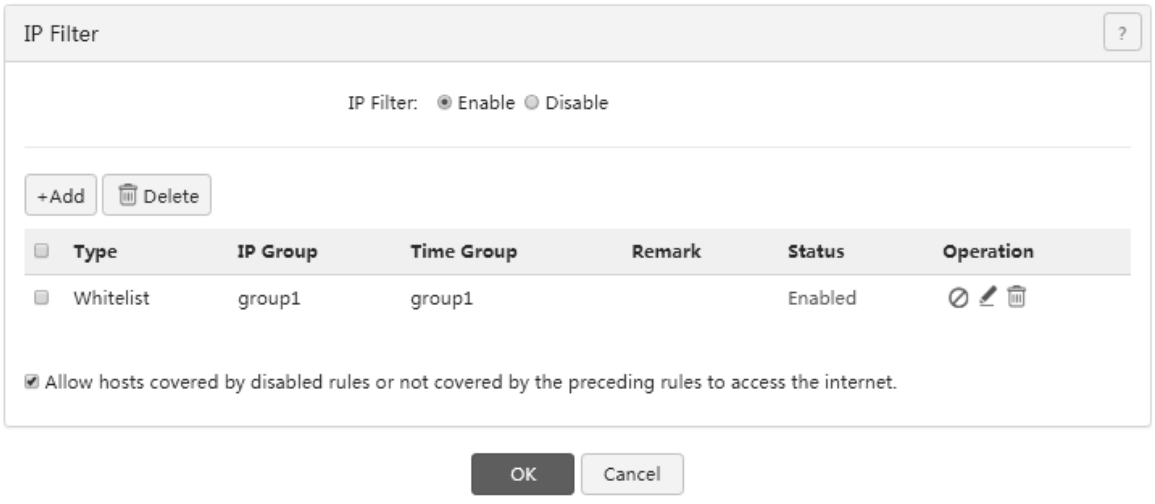


---End

Parameter description

Parameter	Description
Filter Type	It specifies the type of an IP address filter. The options include: – **Allow access to the internet**: This option indicates the whitelist function. If this option is used, users with specified IP addresses can access the internet within specified periods. – **Forbid access to the internet**: This option indicates the blacklist function. If this option is used, users with specified IP addresses cannot access the internet within specified periods.
IP Group	It specifies the referenced IP address group that indicates the corresponding users of a rule. Time groups must be configured in advance on the **Filter Management** > **IP Group & Time Group** page.
Time Group	It specifies the referenced time group that indicates the validity period of a rule. Time groups must be configured in advance on the **Filter Management** > **IP Group & Time Group** page.
Remark	It specifies the description of a rule. This parameter is optional.

The **IP Filter** page appears, showing the added rule. See the following figure.



Parameter description

Parameter	Description
Status	It indicates whether a rule is enabled. After a rule is added, it enters the Enabled state by default. To disable a rule, click corresponding to the rule. To enable a rule, click corresponding to the rule.
Allow hosts covered by disabled rules or not covered by the preceding rules to access the internet.	If it is selected, hosts covered by rules in Disabled state and hosts not covered by rules are allowed to access the internet. If it is not selected, hosts covered by rules in Disabled state and hosts not covered by rules are not allowed to access the internet.

Modifying a rule

1. Choose **Filter Management** > **IP Filter**.
2. Click corresponding to an IP address filtering rule.

Deleting a rule

1. Choose **Filter Management** > **IP Filter**.
2. Click corresponding to an IP address filtering rule to be deleted. To delete multiple MAC address filtering rules at the same time, select them and click Delete.

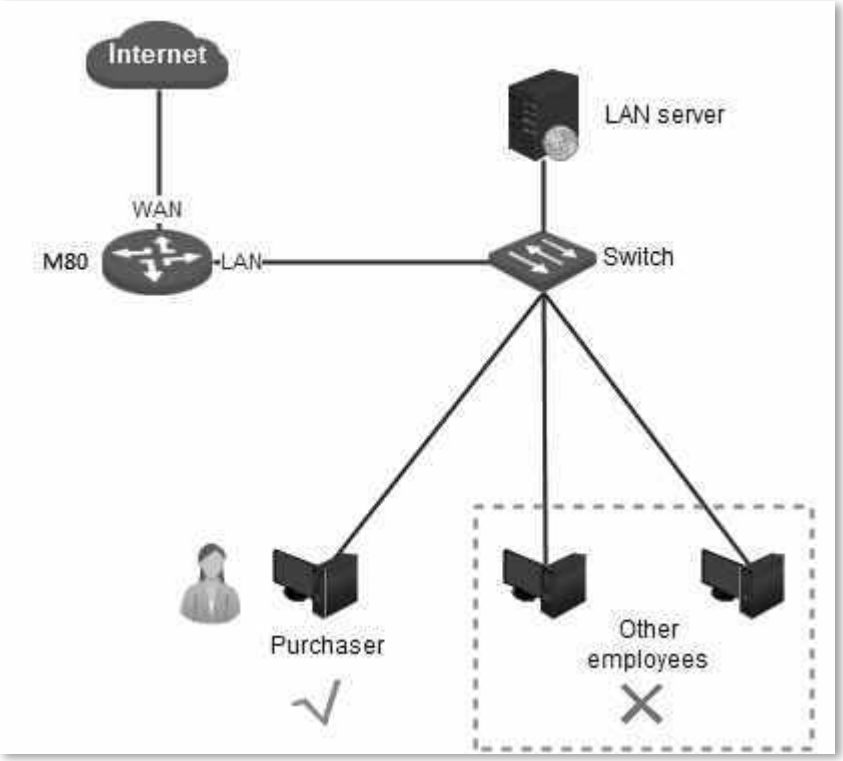
5.3.2 Example of setting the IP address filter

Networking requirement

An enterprise uses M80 to set up a LAN to address the following requirement:

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

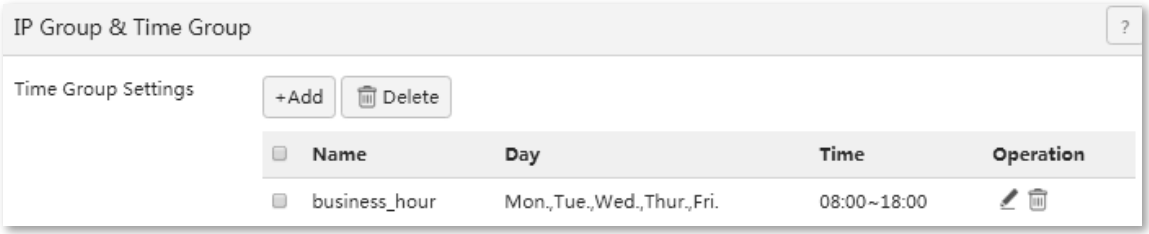
You can use the IP address filter to meet this requirement. Assume that the IP addresses of the purchaser's computers are from 192.168.0.2~192.168.0.100



Configuration procedure

I. Set a time group.

Choose **Filter Management** > **IP Group & Time Group**. Set the time group shown in the following figure.



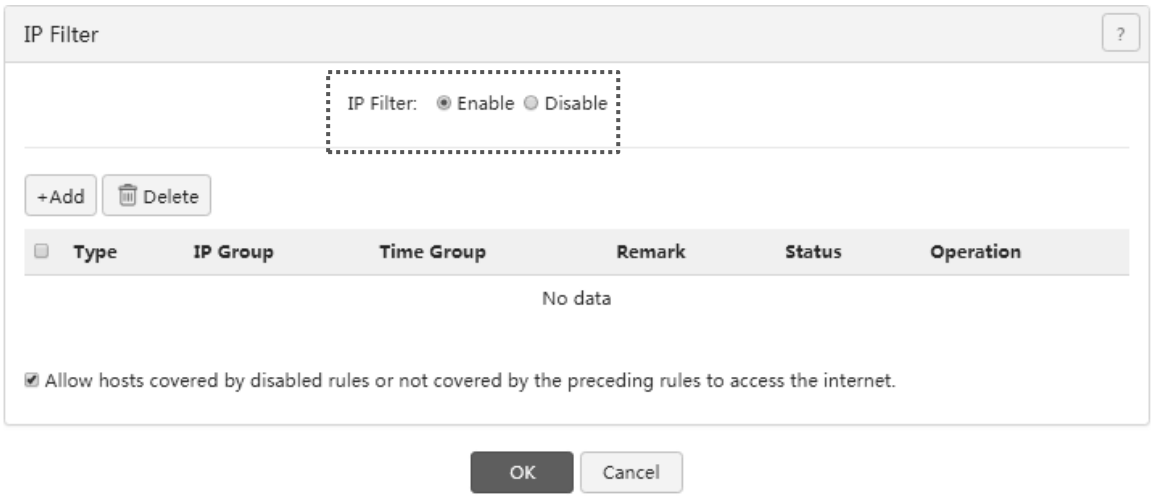
II. Set an IP group.

Choose **Filter Management** > **IP Group & Time Group**. Set the IP group shown in the following figure.

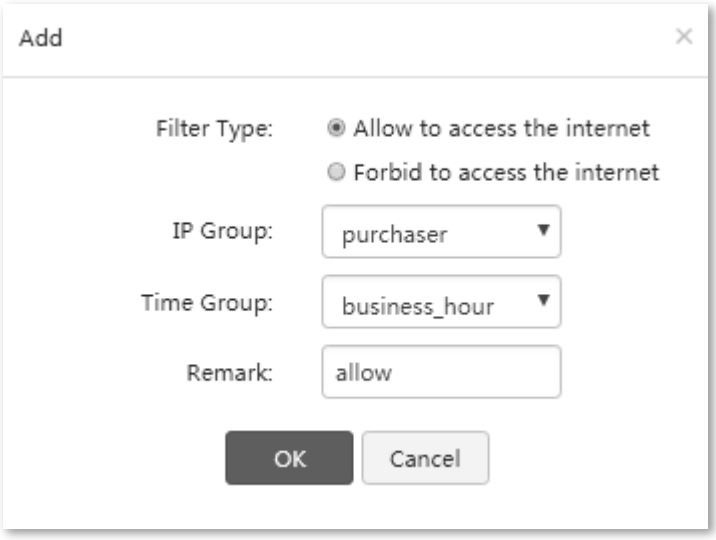
III. Set the IP address filter.

Choose **Filter Management** > **IP Filter**, perform the settings below:

1. Enable the IP address filter.
2. Set **IP Filter** to **Enable**.
3. Click **OK**.



4. Set an IP address filtering rule.
   (1) Click +Add.
   (2) Set Filter Type to Allow to access the internet.
   (3) Set **IP Group** to an available time group. Here takes **purchaser** as an example.
   (4) Set **Time Group** to an available time group. Here takes **Business_hour** as an example.
   (5) Set **Remark** to the description of this rule, such as **allow**.
   (6) Click **OK**.

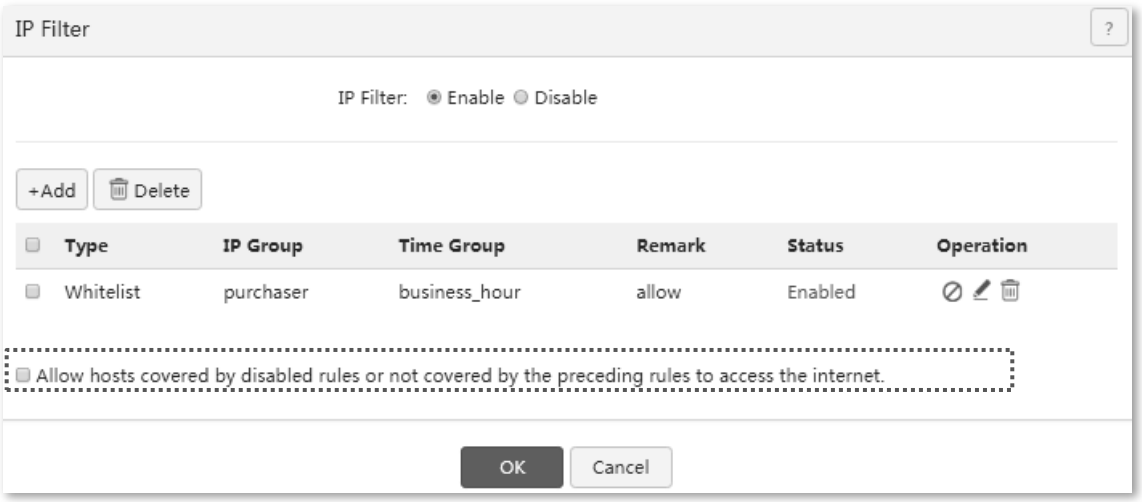


5. Prevent the hosts covered by disabled rules and the hosts not covered by rules to access the internet.

   (1) Choose **Filter Management** > **IP Filter**.

   (2) Deselect **Allow hosts covered by disabled rules or not covered by the preceding rules to access the internet**.

   (3) Click **OK**.



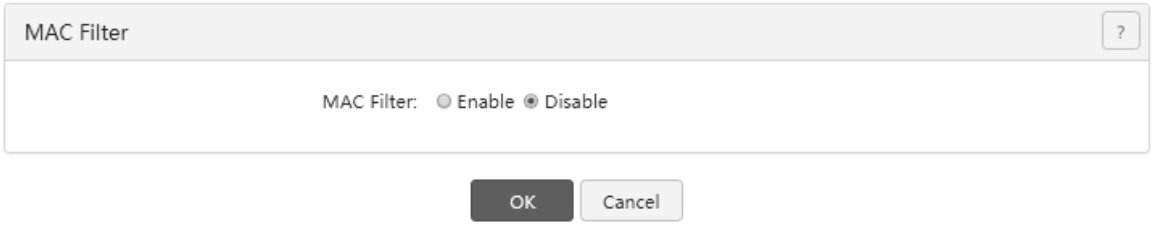
---End

Verification

During 08:00 to 18:00 in weekdays, verify that among the computers on the LAN, only the purchaser's computers can access the internet.

5.4 Setting the MAC address filter

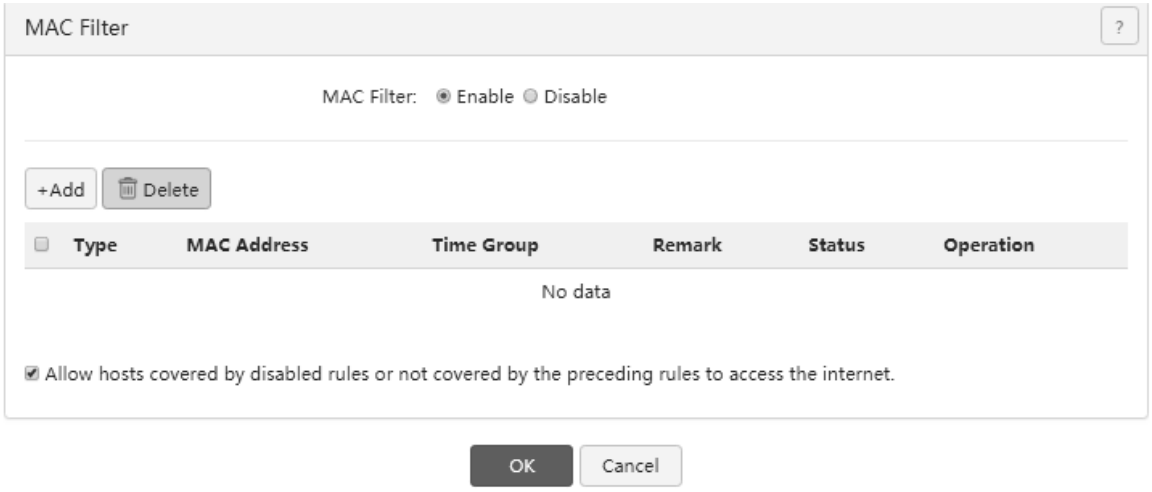
To access the page for setting the MAC address filter, choose **Filter Management** > **MAC Filter**. See the following figure.



5.4.1 Setting the MAC address filter

Enabling the MAC address filter

1. Choose **Filter Management** > **MAC Filter**.
2. Set **MAC Filter** to **Enable**.
3. Click **OK**.



---End

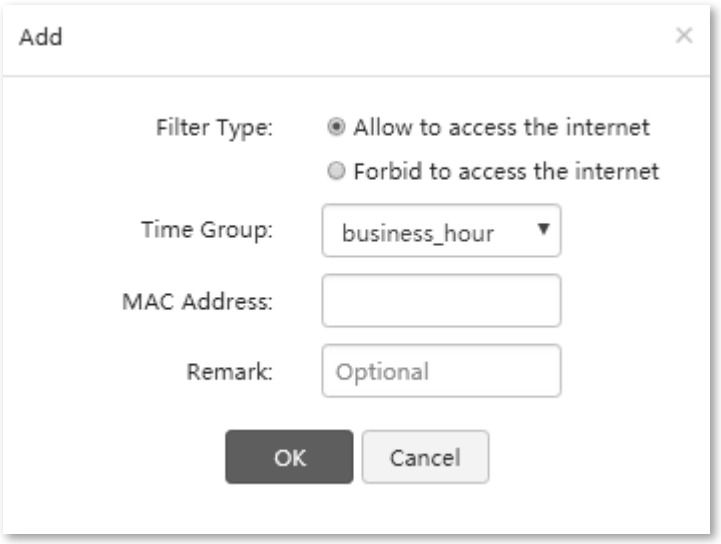
The MAC address filter is enabled. Then, you can set MAC address filtering rules.

Setting MAC address filtering rules

Adding a rule

1. 1. Choose **Filter Management** > **MAC Filter**.
2. Click +Add.
3. Set required parameters.

4. Click **OK**.

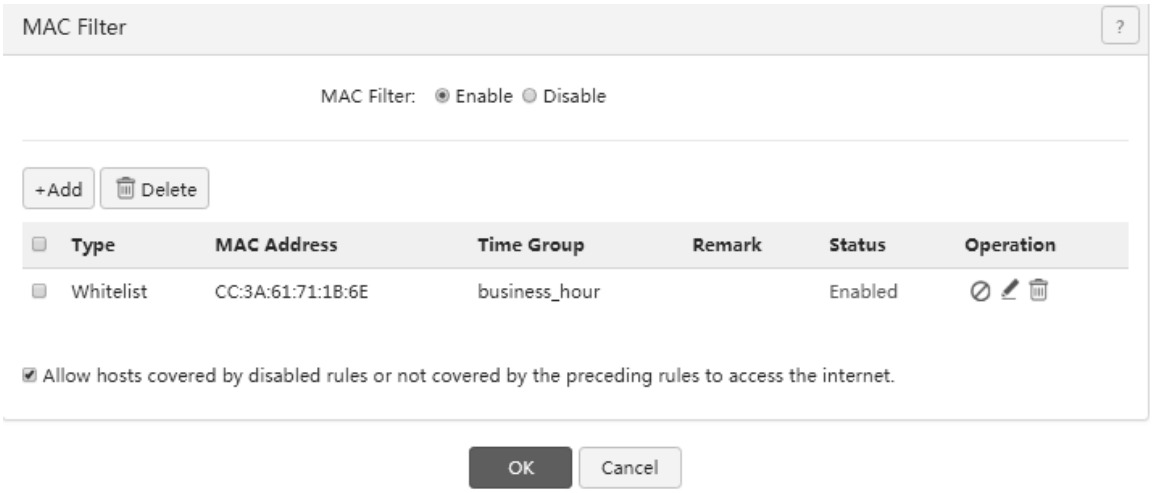


---End

Parameter description

Parameter	Description
Filter Type	It specifies the type of a MAC address filter. The options include **Allow access to the internet**: This option indicates the whitelist function. If this option is used, users with specified MAC addresses can access the internet within specified periods. **Forbid access to the internet**: This option indicates the blacklist function. If this option is used, users with specified MAC addresses cannot access the internet within specified periods.
Time Group	It specifies the referenced time group that indicates the validity period of a rule. Time groups must be configured in advance on the **Filter Management** > **IP Group & Time Group** page.
MAC Address	It specifies the MAC addresses to which a rule is applicable.
Remark	It specifies the description of a rule. This parameter is optional.

The **MAC Filter** page appears, showing the added rule. See the following figure.



Parameter description

Parameter	Description
Status	It indicates whether a rule is enabled. After a rule is added, it enters the Enabled state by default. To disable a rule, click corresponding to the rule. To enable a rule, click corresponding to the rule.
Allow hosts covered by disabled rules or not covered by the preceding rules to access the internet.	If it is selected, hosts covered by rules in Disabled state and hosts not covered by rules are allowed to access the internet. If it is not selected, hosts covered by rules in Disabled state and hosts not covered by rules are not allowed to access the internet.

Modifying a rule

1. Choose **Filter Management** > **MAC Filter**.
2. Click corresponding to a MAC address filtering rule.

Deleting a rule

1. Choose **Filter Management** > **MAC Filter**.
2. Click corresponding to a MAC address filtering rule to be deleted.
   The rule is deleted. To delete multiple MAC address filtering rules at the same time, select them and click Delete.

5.4.2 Example of setting the MAC address filter

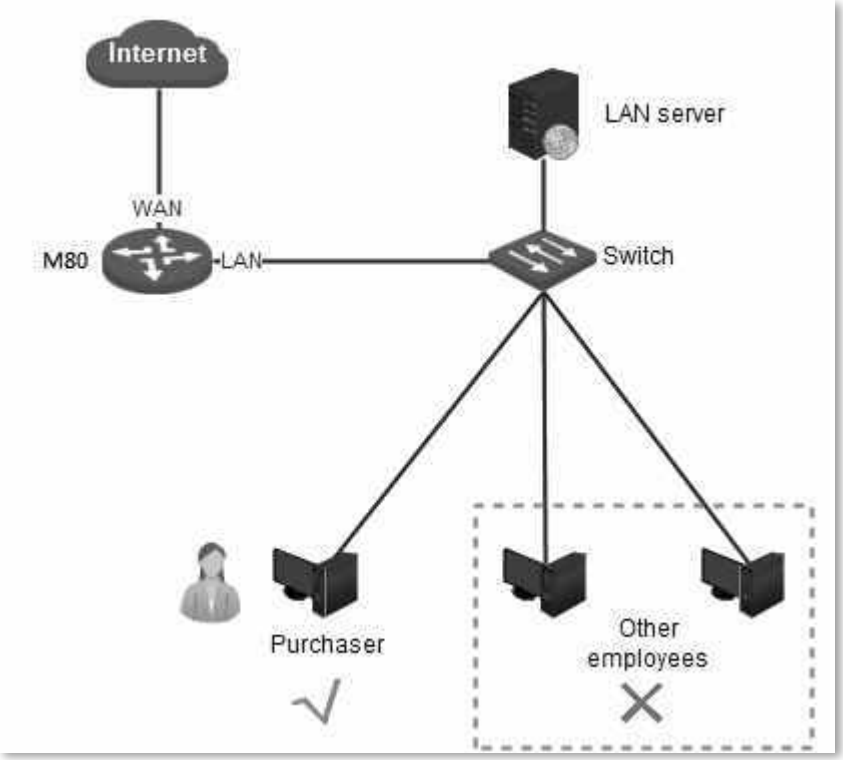
Networking requirement

An enterprise uses M80 to set up a LAN to address the following requirement:

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

You can use the MAC address filter to meet this requirement. Assume that the MAC address of the purchaser's computer is CC:3A:61:71:1B:6E.

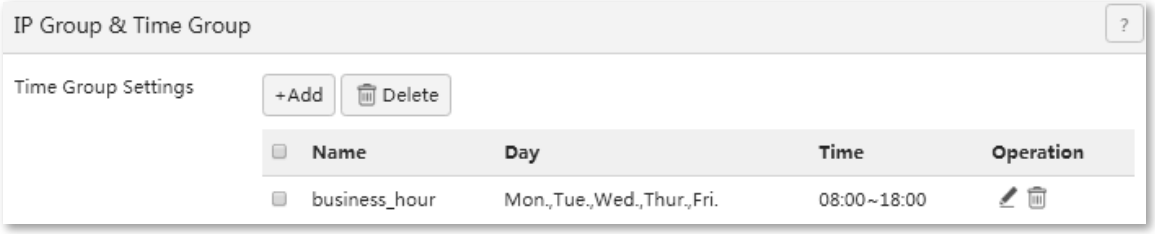
Network topology



Configuration procedure

I. Set a time group.

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



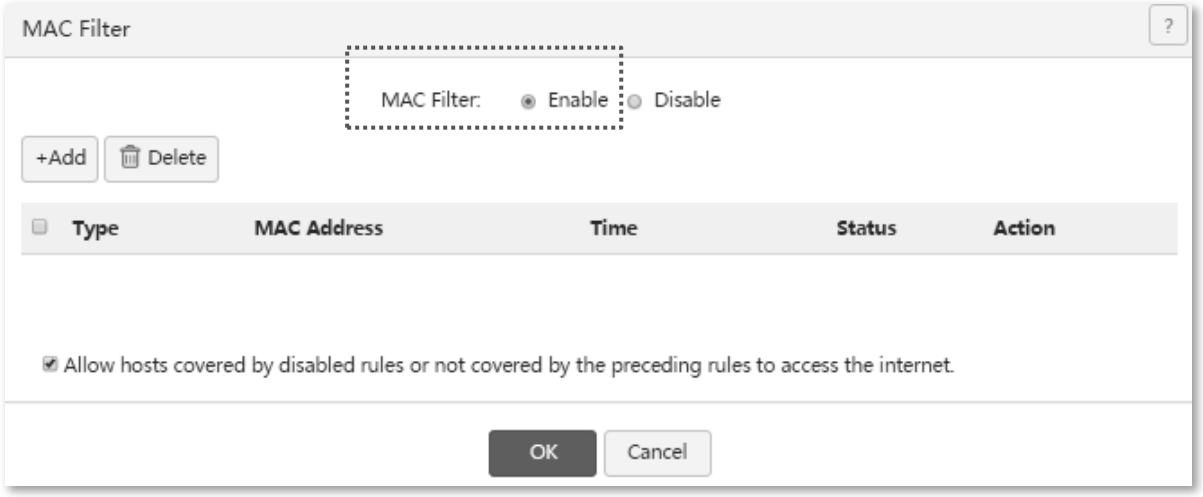
II. Set the MAC address filter.

1. Enable the MAC address filter.

   (1) Choose **Filter Management** > **MAC Filter**.

   (2) Set **MAC Filter** to **Enable**.

   (3) Click **OK**.



2. Set a MAC address filtering rule.

   (1) Click +Add.

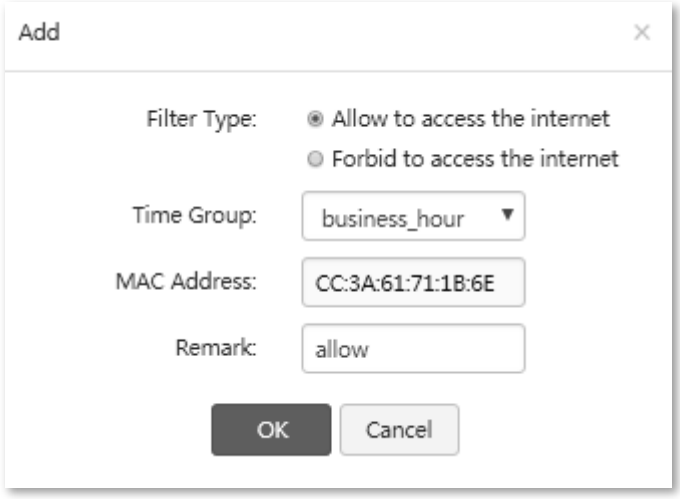
   (2) Set **Filter Type** to **Allow access to the internet**.

   (3) Set **Time Group** to an available time group, which is **business_hour** in this example.

   (4) Set **MAC Address** to the physical address of the purchaser's computer, which is **CC:3A:61:71:1B:6E** in this example.

   (5) Set **Remark** to the description of this rule, such as **allow**.

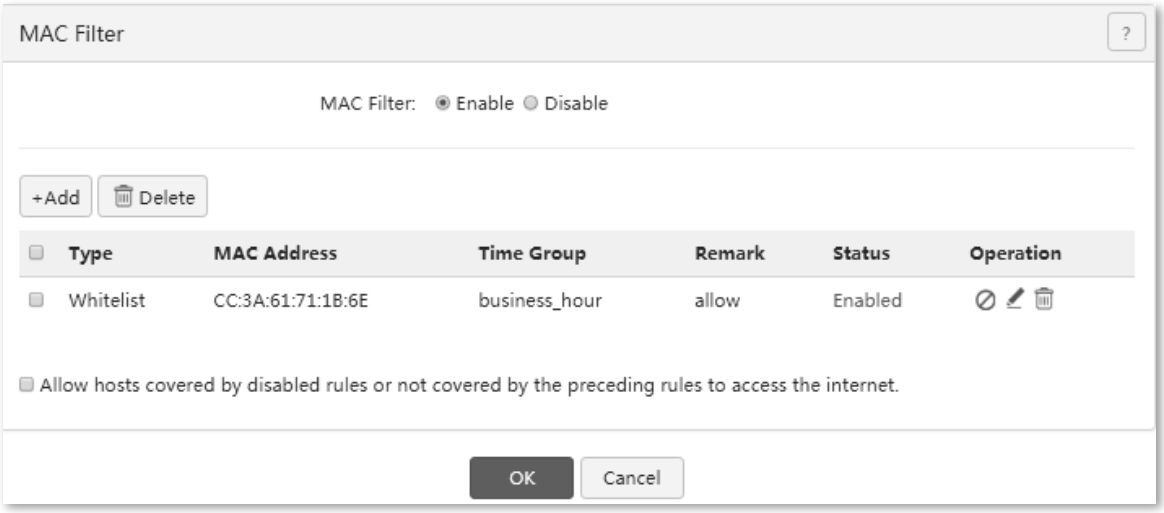
   (6) Click **OK**.



3. Prevent the hosts covered by disabled rules and the hosts not covered by rules to access the internet.

   (1) Deselect **Allow hosts covered by disabled rules or not covered by the preceding rules to access the internet**.

   (2) Click **OK**.



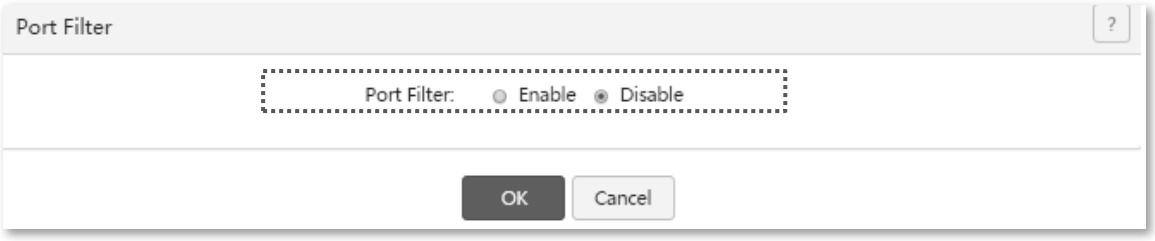
---End

Verification

During 08:00 to 18:00 in weekdays, verify that among the computers on the LAN, only the purchaser's computer can access the internet.

5.5 Setting the port filter

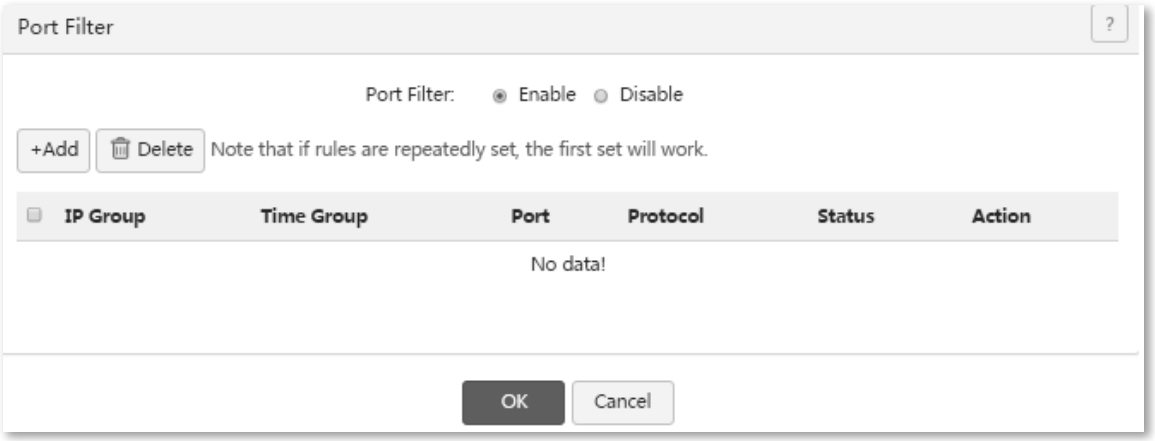
To access the page for setting the port filter, choose **Filter Management** > **Port Filter**. See the following figure.



5.5.1 Setting the port filter

Enabling the port filter

1. Choose **Filter Management** > **Port Filter**.
2. Set **Port Filter** to **Enable**.
3. Click **OK**.

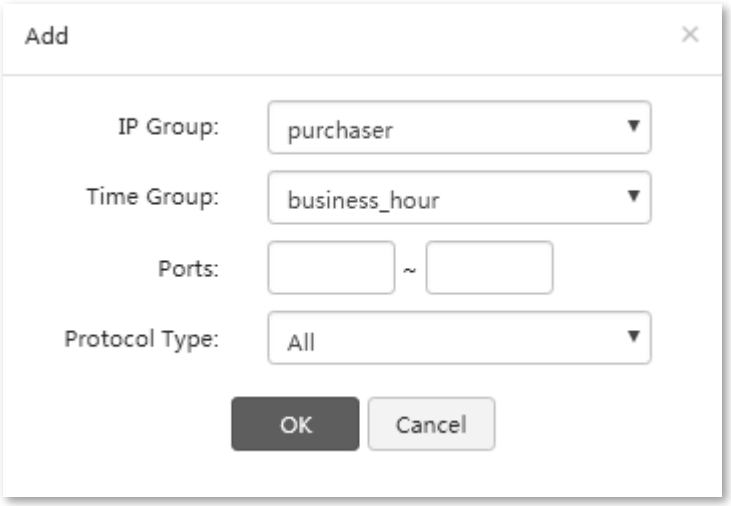


Then, you can set port filtering rules.

Setting port filtering rules

Adding a rule

1. Choose **Filter Management** > **Port Filter**.
2. Click +Add.
3. Set required parameters.
4. Click **OK**.

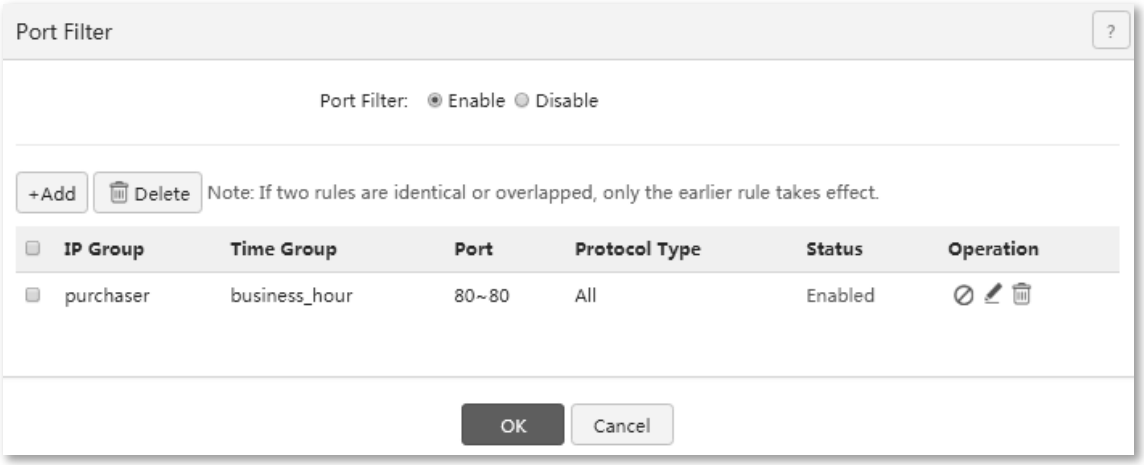


---End

Parameter description

Parameter	Description
IP Group	It specifies a referenced IP address group that indicates the users to which a rule is applicable. IP address groups must be configured in advance on the **Filter Management** > **IP Group & Time Group** page.
Time Group	It specifies a referenced time group that indicates the validity period of a rule. Time groups must be configured in advance on the **Filter Management** > **IP Group & Time Group** page.
Ports	It specifies the TCP or UDP ports of inaccessible services.
Protocol	It specifies the protocol of the inaccessible services. **All** indicates TCP and UDP.

The **Port Filter** page appears, showing the added rule. See the following figure.



Modifying a rule

1. Choose **Filter Management** > **Port Filter**.
2. Click corresponding to a port filtering rule. To disable/enable a rule, click / corresponding to the rule.

Deleting a rule

1. Choose **Filter Management** > **Port Filter**.
2. Click corresponding to a port filtering rule to be deleted. To delete multiple port filtering rules at the same time, select them and click Delete.

5.5.2 Example of setting the port filter

Networking requirement

An enterprise uses M80 to set up a LAN to address the following requirement:

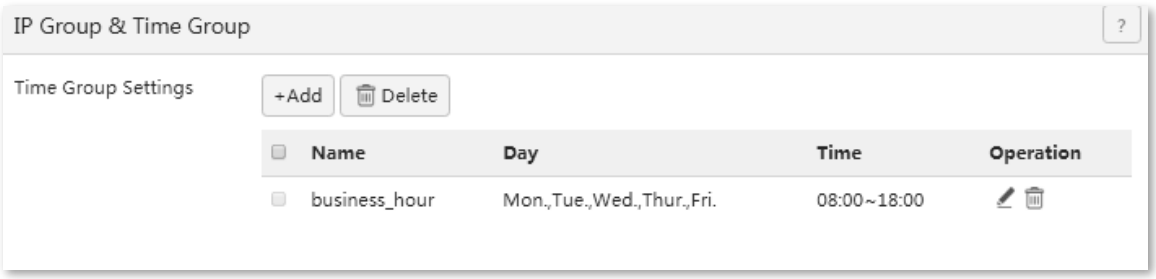
During business hours (08:00 to 18:00 every weekday), computers with IP addresses ranging from 192.168.0.2 to 192.168.0.100 are not allowed to browse web pages. (The default port number of the web service is 80.)

You can use the port filter of the router to meet this requirement.

Configuration procedure

I. Set a time group.

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



II. Set an IP address group.

1. Choose **Filter Management** > **IP Group & Time Group**.
2. Set the IP address group shown in the following figure.

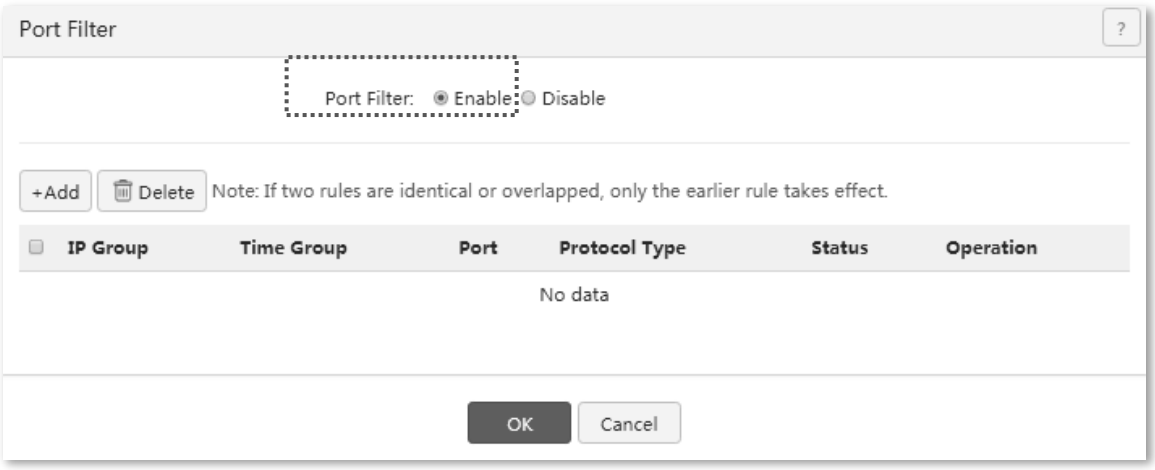
III. Set the port filter.

3. Enable the port filter as follows:

   (1) Choose **Filter Management** > **Port Filter**.

   (2) Set **Port Filter** to **Enable**.

   (3) Click **OK**.



4. Set a port filtering rule.

   (1) Choose **Filter Management** > **Port Filter**.

   (2) Click +Add.

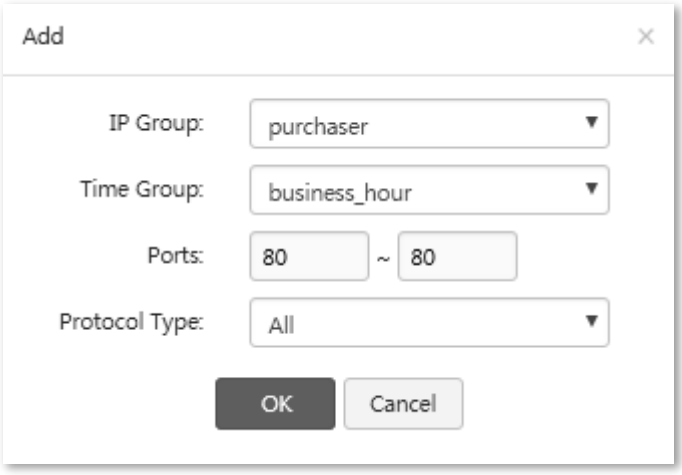
   (3) Set **IP Group** to the IP address group that includes the computers disallowed to browse web pages.

   (4) Set **Time Group** to the time group configured in step I, which is **business_hour** in this example.

   (5) Set **Ports** to port number **80** used to browse web pages.

   (6) Retain the default value **All** of **Protocol**.

   (7) Click **OK**.

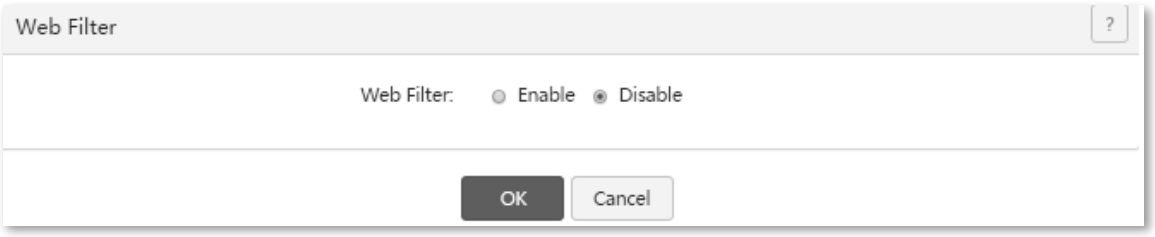


Verification

During 08:00 to 18:00 in weekdays, verify that the computers with IP addresses ranging from 192.168.0.2 to 192.168.0.100 cannot browse web pages, while the other computers with IP addresses ranging from 192.168.0.101 to 192.168.0.254 can.

5.6 Setting the web filter

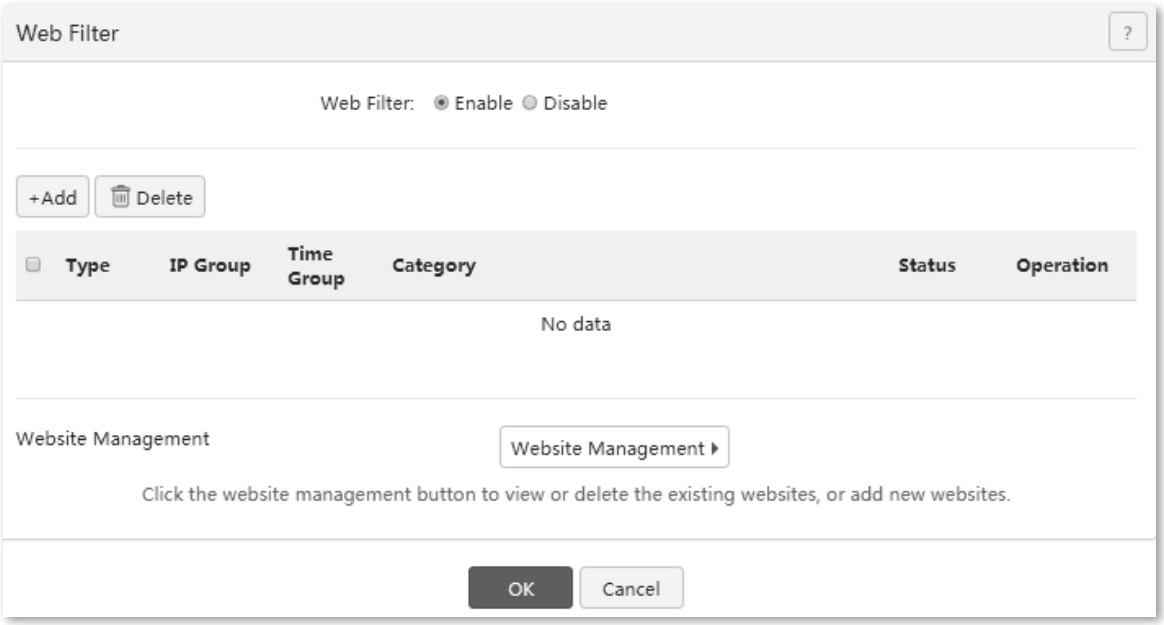
To access the page for setting the web filter, choose **Filter Management** > **Web Filter**. See the following page.



5.6.1 Setting the web filter

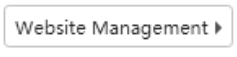
Enabling the web filter

1. Choose **Filter Management** > **Web Filte**r.
2. Set **Web Filter** to **Enable**.
3. Click **OK**.



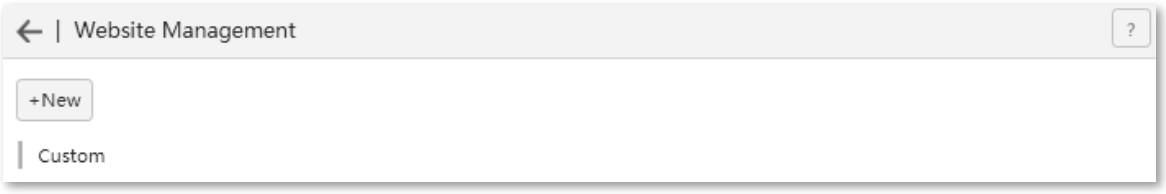
Then, you can set web filtering rules, define website categories, and view websites by category.

Adding a web categories

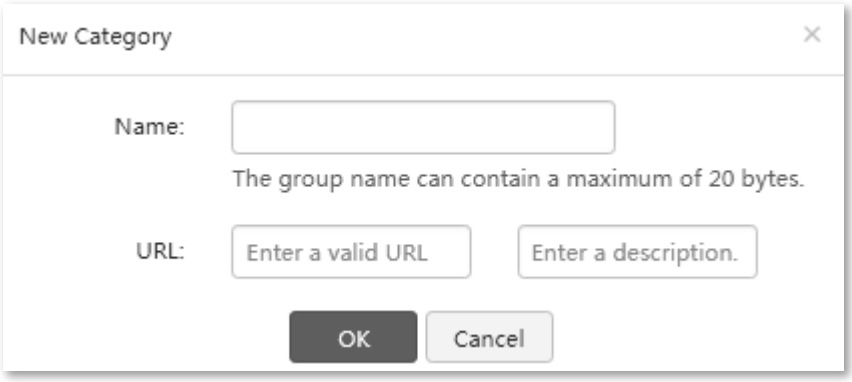
1. Choose **Filter Management** > **Web Filter**.
2. Click 

.

3. Cick +New in the **Web Category** area.



4. Set **Group Name** to the name of a web category.
5. Set **URL** to the URL of a website to be used by web filters and the description of the website.
6. Click **OK**.

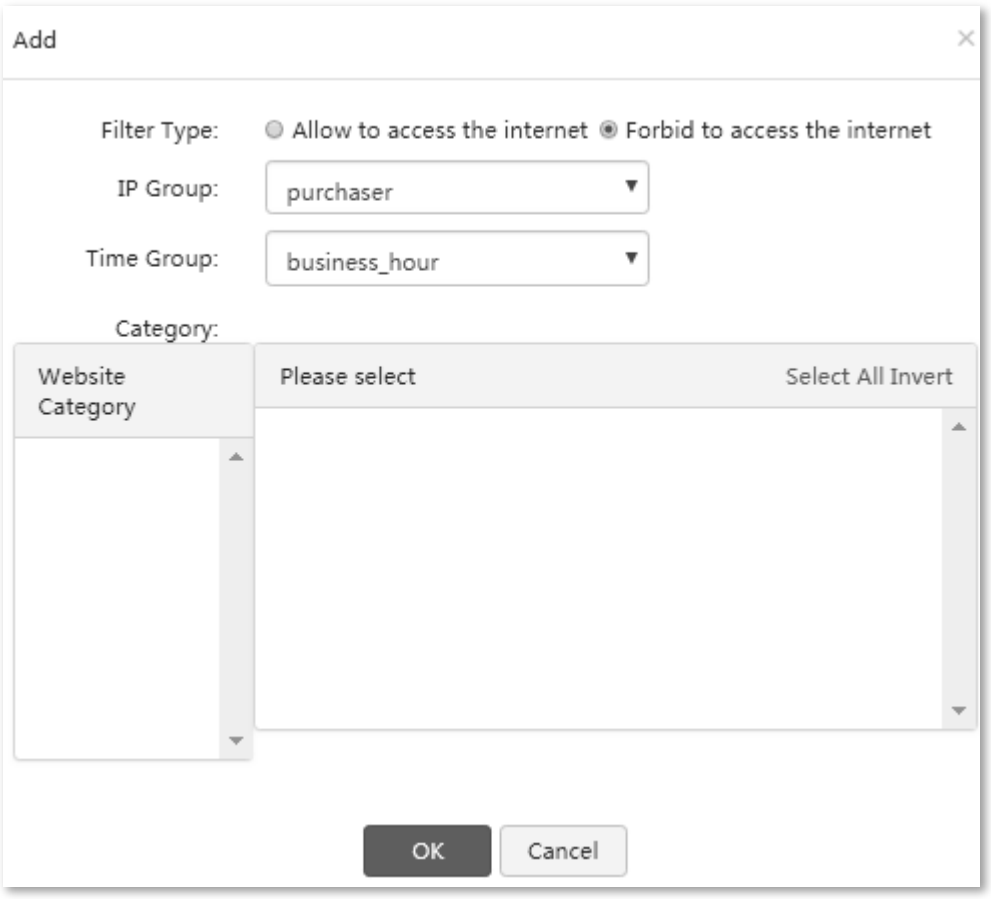


---End

Setting web filtering rules

Adding a rule

1. Choose **Filter Management** > **Web Filter**.
2. Click +Add.
3. Set required parameters.
4. Click **OK**.

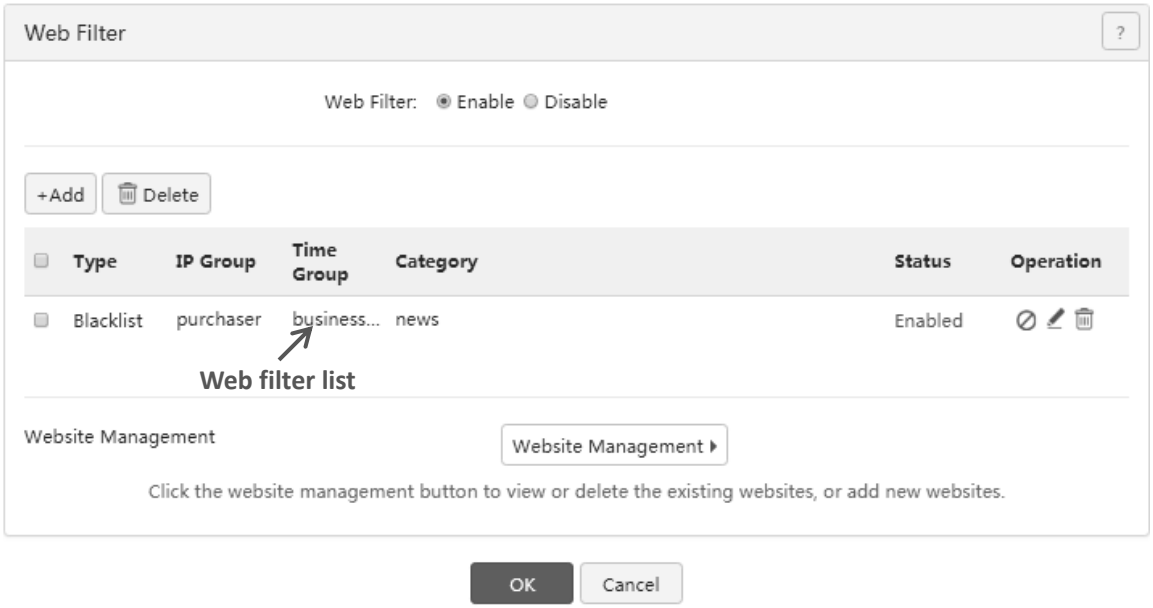


---End

Parameter description

Parameter	Description
IP Group	It specifies a referenced IP address group that indicates the users to which a rule is applicable. IP address groups must be configured in advance on the **Filter Management > IP Group & Time Group** page.
Time Group	It specifies a referenced time group that indicates the validity period of a rule. Time groups must be configured in advance on the **Filter Management** > **IP Group & Time Group** page.
Website Category	It specifies categories of websites inaccessible to specified users.
Please Select	It specifies the application to disable

The **Web Filter** page appears, showing the added rule. See the following figure.



Modifying a rule

1. Choose **Filter Management** > **Web Filter**.
2. Click corresponding to a web filtering rule. To disable/enable a rule, click / corresponding to the rule.

Deleting a rule

1. Choose **Filter Management** > **Web Filter**.
2. Click corresponding to a web filtering rule to be deleted. To delete multiple web filtering rules at the same time, select them and click Delete.

5.6.2 Example of setting the web filter

Networking requirement

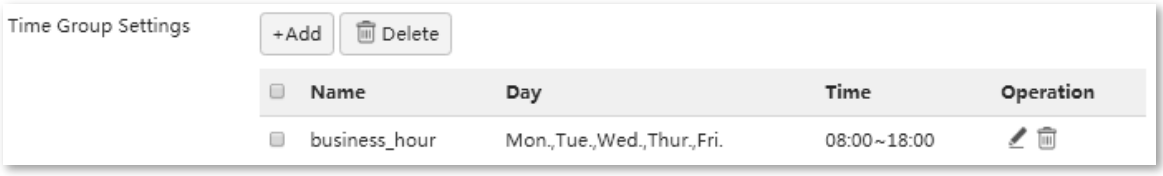
An enterprise uses M80 to set up a LAN to address the following requirement:

During business hours (08:00 to 18:00 every weekday), computers with IP addresses ranging from 192.168.0.2 to 192.168.0.100 are not allowed to browse news websites.

Configuration procedure

I. Set a time group.

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

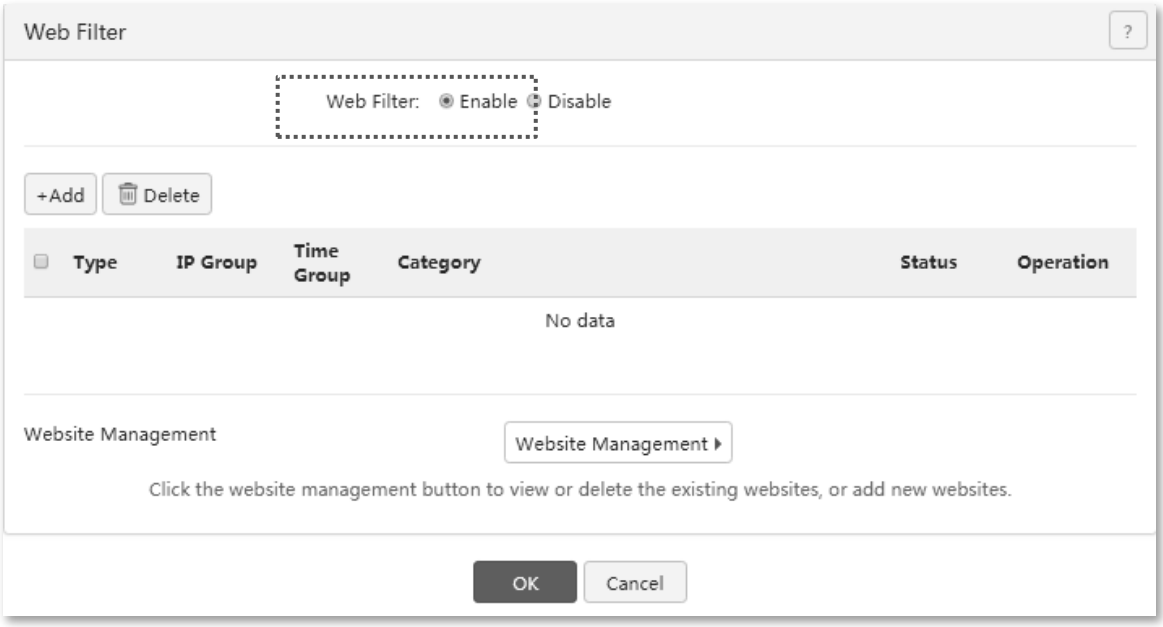


II. Set an IP address group.

1. Choose **Filter Management** > **IP Group & Time Group**.
2. Set the IP address group shown in the following figure.

III. Enable the web filter.

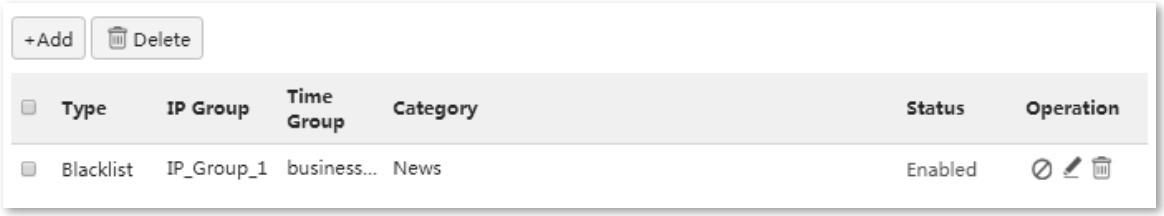
1. Choose **Filter Management** > **Web Filter**.
2. Set **Web Filter** to **Enable**.
3. Click **OK**.



IV. Add a web category.

1. Choose **Filter Management** > **Web Filter**.
2. Click Website Management.
3. Click +New.
4. Set **Group Name** to **News**.

5. Set **URL** to the URL of a news website not accessible to the computers and the description of the website.
6. Click **OK**.

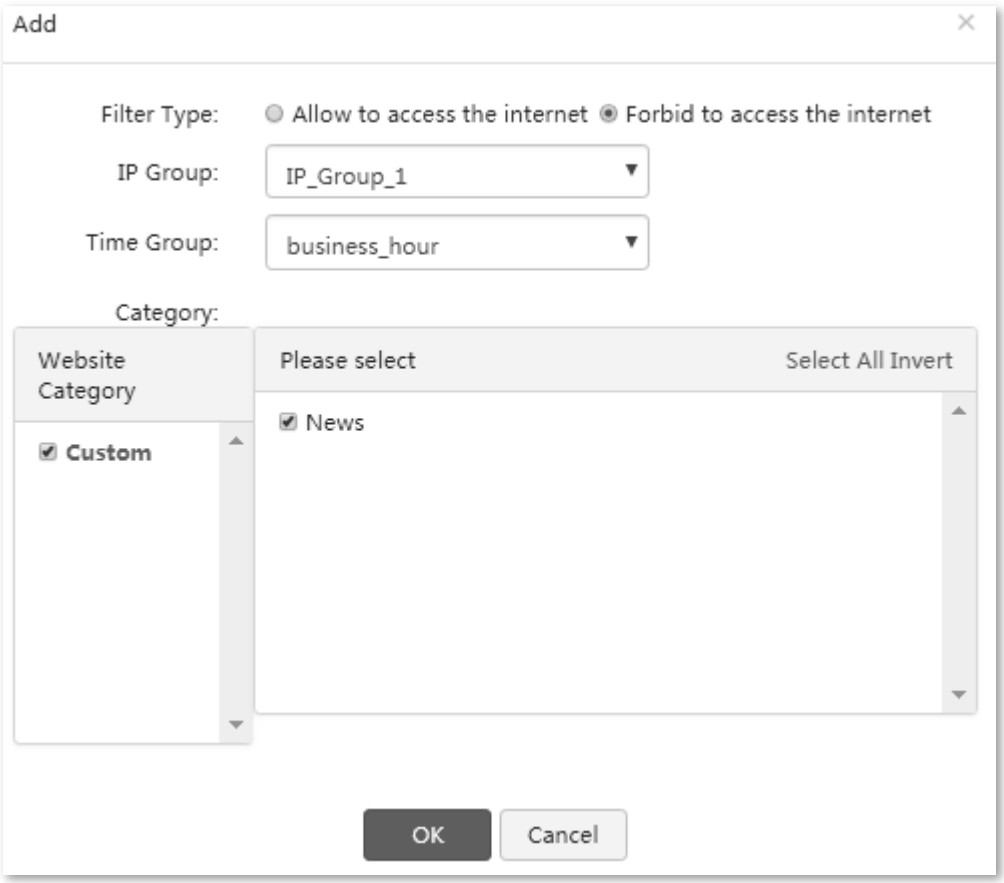


V. Add all the news websites inaccessible to the computers.

1. Click **News** in the **Web Category** area.
2. Enter the URL of another website inaccessible to the computers and the description of the website.
3. Click +Add to the group.
4. Repeat steps 2 and 3 to add the other websites inaccessible to the computers.

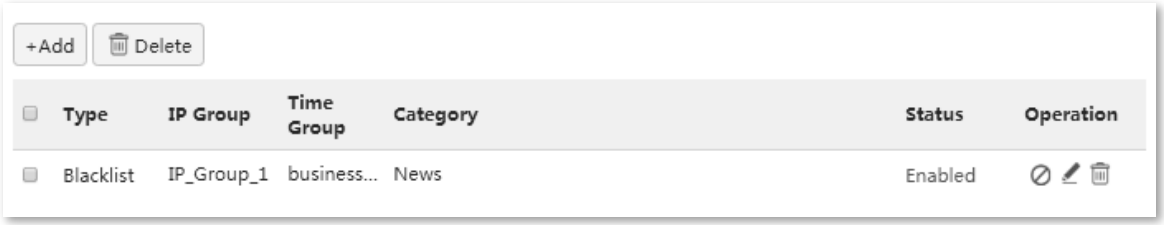
VI. Add a web filtering rule.

1. Choose **Filter Management** > **Web Filter**.
2. Click +Add.
3. Set **IP Group** to the IP address group of the computers allowed to browse only the specified websites.
4. Set **Time Group** to the time group set in **Step I**.
5. Set **Category** to **News**.
6. Click **OK**.



---End

The **Web Filter** page appears, showing the added rule. See the following figure.

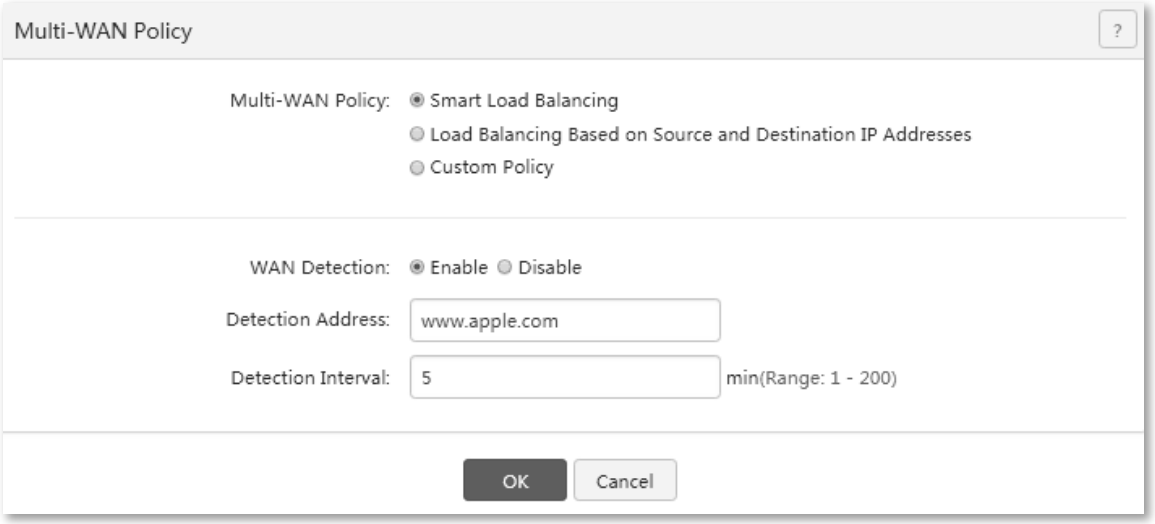


Verification

During 08:00 to 18:00 in weekdays, verify that computers with IP addresses ranging from 192.168.0.2 to 192.168.0.100 are not allowed to browse news websites.

5.7 Setting multi-WAN policies

To access the page for setting multi-WAN policies, choose **Filter Management** > **Multi-WAN Policy**. See the following figure.



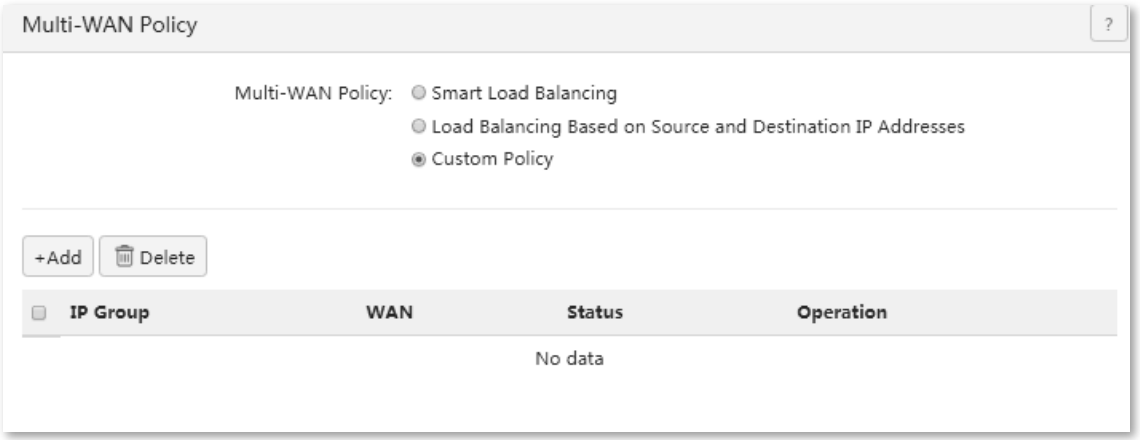
Parameter description

Parameter	Description
Smart Load Balancing	It specifies that the system automatically distributes traffic based on the following rules through the WAN ports to achieve load balancing: If the usage of the bandwidths specified by **Link Speed** preset on the **Network** > **internet Setup** page is lower than 50%, the router distributes traffic proportionately according to the ratio between the bandwidths of the ports. If the usage of the bandwidth on a WAN port specified by **Link Speed** preset on the **Network** > **internet Setup** page reaches or exceeds 50%, the router distributes traffic preferably to the port with more available bandwidth.
Custom	It enables you to assign WAN ports to source IP addresses as required.
Mutil-WAN Policy	It specifies the policy through the WAN ports. – **Smart Load Balancing**: The system automatically distributes traffic through the WAN ports with the smallest amount of traffic. – **Custom Policy**: It enables you to assign WAN ports to source IP addresses as required.
WAN Detection	The router regularly detects the connection status between the WAN ports and **detection address**. – **Detection Address**: The IP address or domain to detect. – **Detection Interval**: The interval of detection, it is 5 minutes by default.

5.7.1 Customizing a multi-WAN policy

Enabling the multi-WAN policy function

1. Choose **Filter Management** > **Multi-WAN Policy**.
2. Set **Multi-WAN Policy** to **Custom**.
3. Click **OK**.



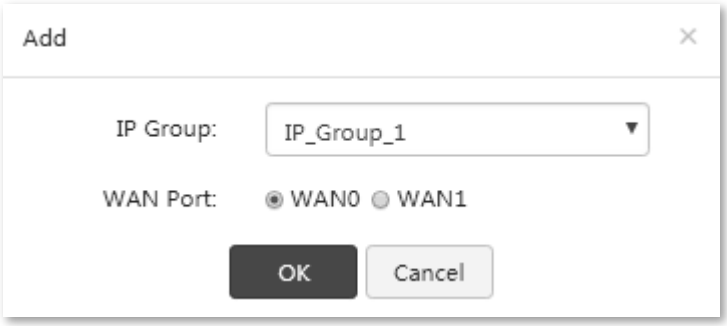
---End

Then, you can customize multi-WAN policies.

Setting multi-WAN rules

Adding a rule

1. Choose **Filter Management** > **Multi-WAN Policy**.
2. Click +Add.
3. Set required parameters.
4. Click **OK**.

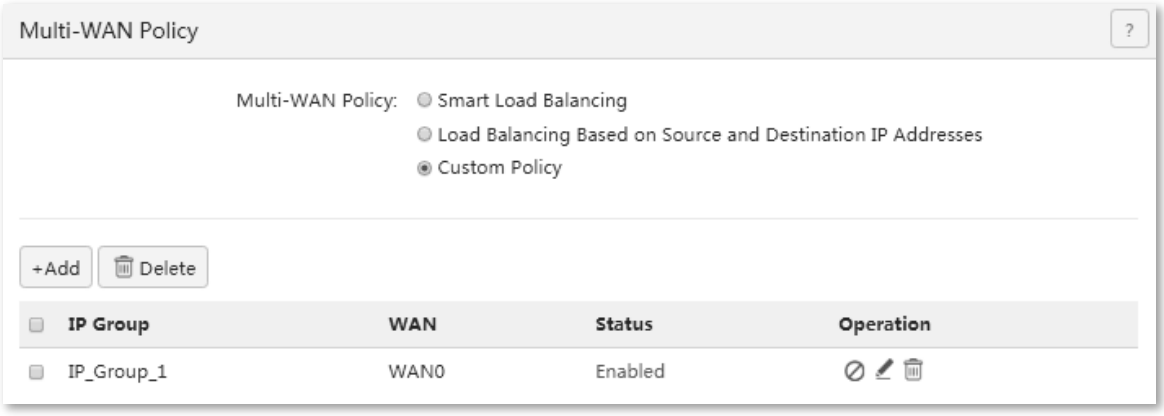


---End

Parameter description

Parameter	Description
IP Group	It specifies the referenced IP address group that indicates the users to which a rule is applicable. IP address groups must be configured in advance on the **Filter Management > IP Group & Time Group** page.
WAN	It specifies the WAN port used for transmitting data traffic of a specified IP address group.

The **Multi-WAN Policy** page appears, showing the added rule. See the following figure.



Modifying a rule

1. Choose **Filter Management** > **Multi-WAN Policy**.
2. Click corresponding to a rule. To disable/enable a rule, click / corresponding to the rule.

Deleting a rule

1. Choose **Filter Management** > **Multi-WAN Policy**.
2. Click corresponding to a rule to be deleted. To delete multiple web filtering rules at the same time, select them and click Delete.

5.7.2 Example of customizing a multi-WAN policy

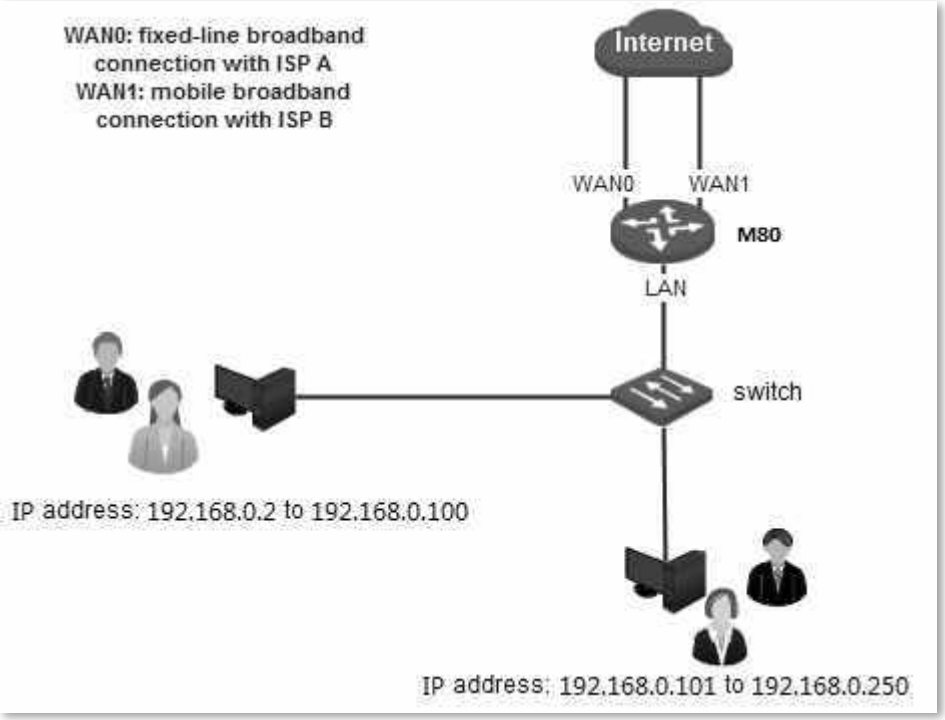
Networking requirement

An enterprise has used M80 to set up a LAN. To meet its internet access requirement, the enterprise has set up two broadband connections with two different ISPs and can now access the internet properly. To achieve load balancing, the enterprise raises the following LAN requirements:

- The computers with IP addresses ranging from 192.168.0.2 to 192.168.0.100 access the Internal through the fixed-line broadband connection with ISP A.
- The computers with IP addresses ranging from 192.168.0.101 to 192.168.0.250 access the Internal through the mobile broadband connection with ISP B.

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

Network topology



Configuration procedure

1. Set an IP address group.
   (1) Choose **Filter Management** > **IP Group & Time Group**.
   (2) Set the IP address group shown in the following figure.

2. Customize a multi-WAN policy.

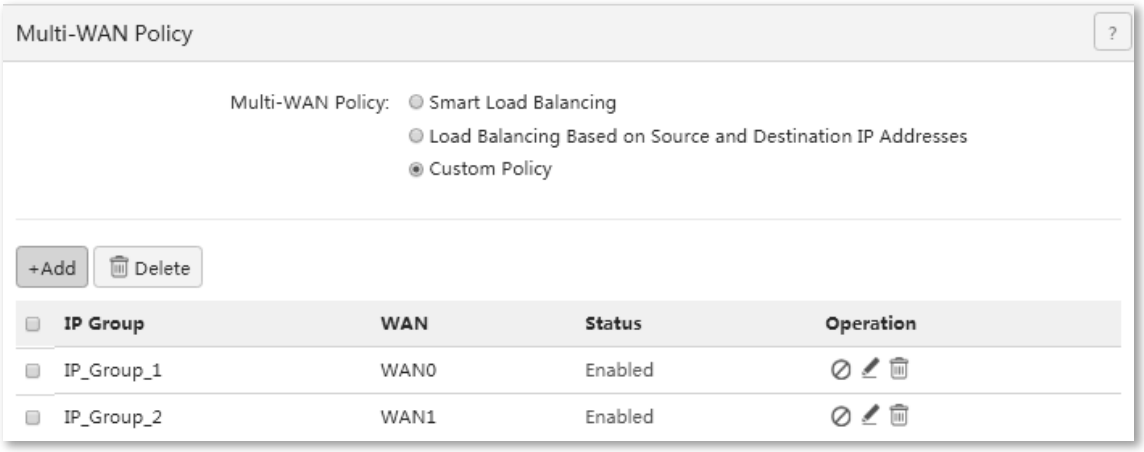
   (1) Choose **Filter Management** > **Multi-WAN Policy**.

   (2) Select **Custom**.

   (3) Click **OK**.

   (4) Click +Add.

   (5) Set the rules shown in the following figure.



---End

Verification

The computers with IP addresses ranging from 192.168.0.2 to 192.168.0.100 access the Internal through WAN0.

The computers with IP addresses ranging from 192.168.0.101 to 192.168.0.250 access the Internal through WAN1.

6 Bandwidth control

6.1 Overview

Internet bandwidth is limited and therefore you must control traffic of users to ensure that the bandwidth is properly used to effectively access resources over the internet.

This chapter describes:

- Setting bandwidth control
- Example of setting manual bandwidth control

6.1.1 Function introduction

M80 supports the following bandwidth control modes:

- **Automatical bandwidth control**

In this mode, the router automatically allocates bandwidth to LAN users based on the upload bandwidth and download bandwidth value that you set on the **Bandwidth Control** page.

Before using automatical bandwidth control, set bandwidth of your broadband connection. Otherwise, automatical bandwidth control may not be accurate.

- **Manual bandwidth control**

In this mode, manually set bandwidth control rules based on the actual environment. Manual bandwidth control allows you to set upload bandwidth and download bandwidth shared among the users in IP address groups or exclusive to specific users in a period. It also allows you to specify the maximum number of concurrent sessions per user device. Comparatively, Manual bandwidth control is more flexible than automatical bandwidth control, while the latter is easier to use.

6.1.2 Configuration instruction

- **Automatical bandwidth control**

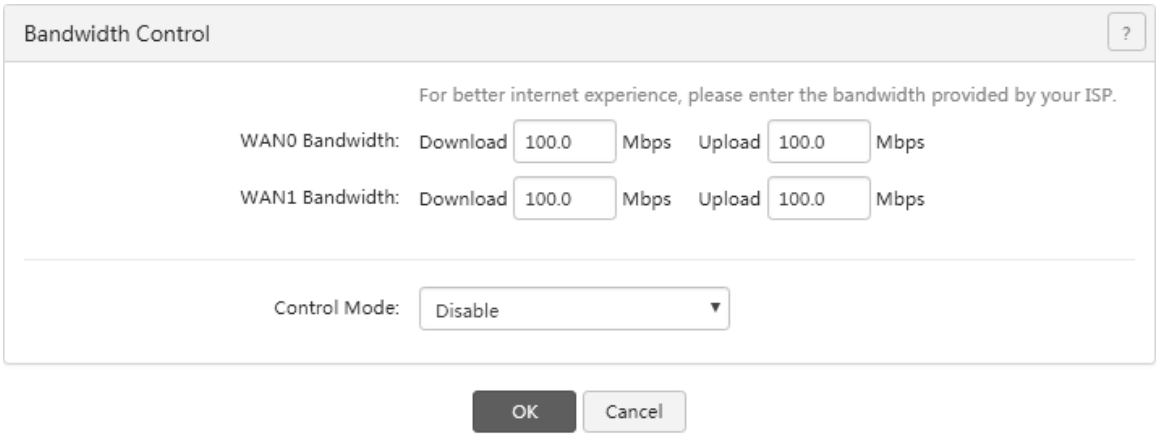
Step	Task	Description
1	Set the bandwidth of your broadband connection.	Set it on the **Bandwidth Control** page. For details, see Setting up an internet connection.
2	Enable automatical bandwidth control.	On the **Bandwidth Control** page, set **Control Mode** to **Automatical Bandwidth Control** and click **OK**.

- **Manual bandwidth control**

Step	Task	Description
1	Set a time group.	When a user-defined bandwidth control rule is set, a time group is required. Set the time group on the **Filter Management** > **IP Group & Time Group page**.
2	Set an IP address group.	When a user-defined bandwidth control rule is set, an IP address group is required. Set the IP address group on the **Filter Management** > **IP Group & Time Group page**.
3	Set a manual bandwidth control rule.	Set a rule on the **Bandwidth Control** page.

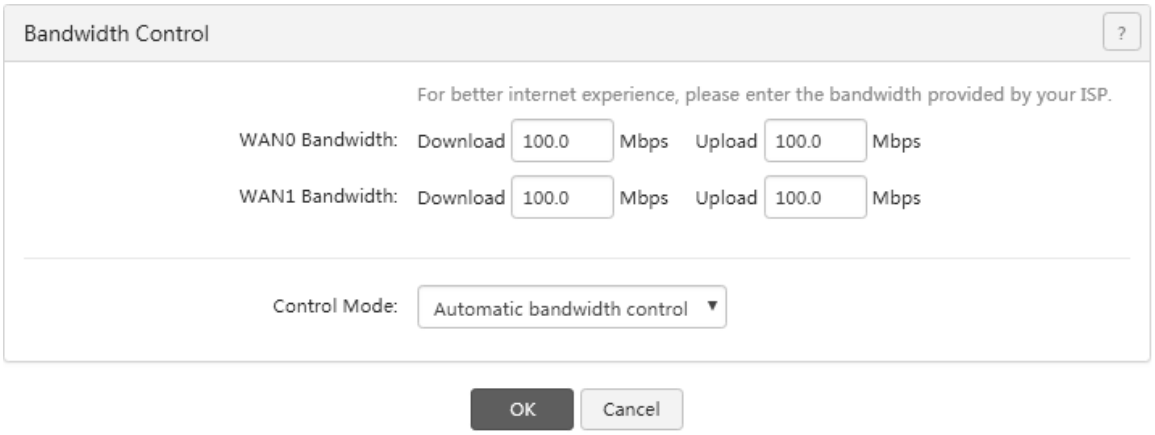
6.2 Setting bandwidth control

To access the page for setting bandwidth control, choose **Bandwidth Control**. See the following figure. This section mainly describes how to set manual bandwidth control.



6.2.1 Enabling automatical bandwidth control

1. Choose **Bandwidth Control**.
2. Set **Control Mode** to **Automatical bandwidth control**.
3. Click **OK**.



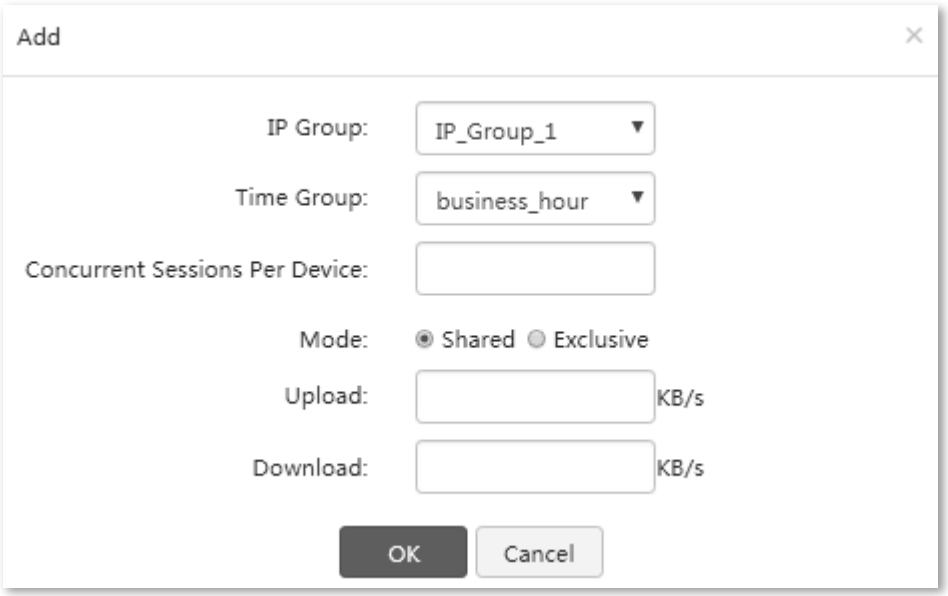
---End

6.2.2 Setting manual bandwidth control rules

Adding a rule

1. Choose **Bandwidth Control**.
2. Set **Control Mode** to **Manual bandwidth control.**

3. Click +Add.
4. Set required parameters.
5. Click **OK**.

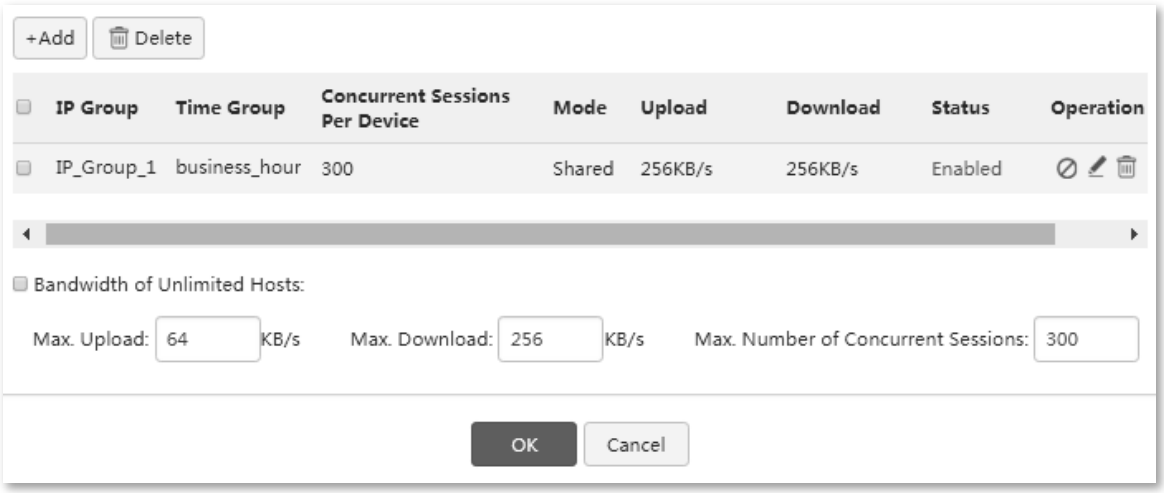


---End

Parameter description

Parameter	Description
IP Group	It specifies a referenced IP group that indicates the users to which a rule is applicable. IP address groups must be configured in advance on the **Filter Management > IP Group & Time Group** page.
Time Group	It specifies a referenced time group that indicates the validity period of a rule. Time groups must be configured in advance on the **Filter Management** > **IP Group & Time Group** page.
Concurrent Session Per Device	It specifies the maximum number of connections allowed for each user device within the IP address group. In normal cases, the value **300** is recommended.
Mode	It specifies the bandwidth control mode. The options include: – **Shared**: In this mode, all the users in specified IP address groups share the specified upload bandwidth and download bandwidth. The available bandwidth may differ across the users. – **Exclusive**: In this mode, the same upload bandwidth and download bandwidth is allocated to the users in specified IP address groups.
Upload	**Upload** specifies the upload bandwidth, while **Download** specifies the download bandwidth.
Download	

The **Bandwidth Control** page appears, showing the added rule. See the following figure.



Modifying a rule

1. Choose **Bandwidth Control**.
2. Click corresponding to a bandwidth control rule. To disable/enable a rule, click / corresponding to the rule.

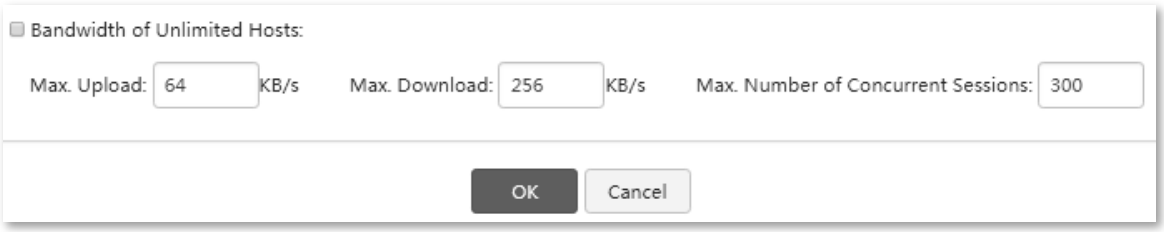
Deleting a rule

1. Choose **Bandwidth Control**.
2. Click corresponding to a rule to be deleted. To delete multiple bandwidth control rules at the same time, select them and click Delete.

6.2.3 Setting bandwidth control parameters for non-specified user devices

When manual bandwidth control is used, you can set bandwidth control parameters for non-specified user devices, which indicate the user devices whose IP addresses are not covered by bandwidth control rules and user devices covered by disabled bandwidth control rules.

If you do not select **Bandwidth of Unlimited Hosts**, the bandwidth and maximum number of concurrent sessions are not limited.



Set the parameters and click **OK**.

6.3 Example of setting manual bandwidth control

Networking requirement

An enterprise uses M80 to set up a LAN to address the following requirement:

During business hours (08:00 to 18:00 every weekday), each computer with an IP address ranging from 192.168.0.2 to 192.168.0.100 is allocated 1 Mbps upload and download bandwidth.

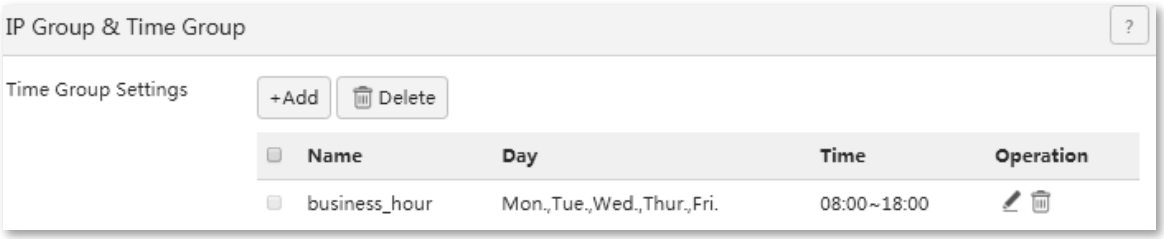
You can use the manual bandwidth control function of the router to meet this requirement. Assume that the maximum number of sessions for user device is 300.

Configuration procedure

1. Set a time group.

   (1) Choose **Filter Management** > **IP Group & Time Group**.

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



2. Set an IP address group.

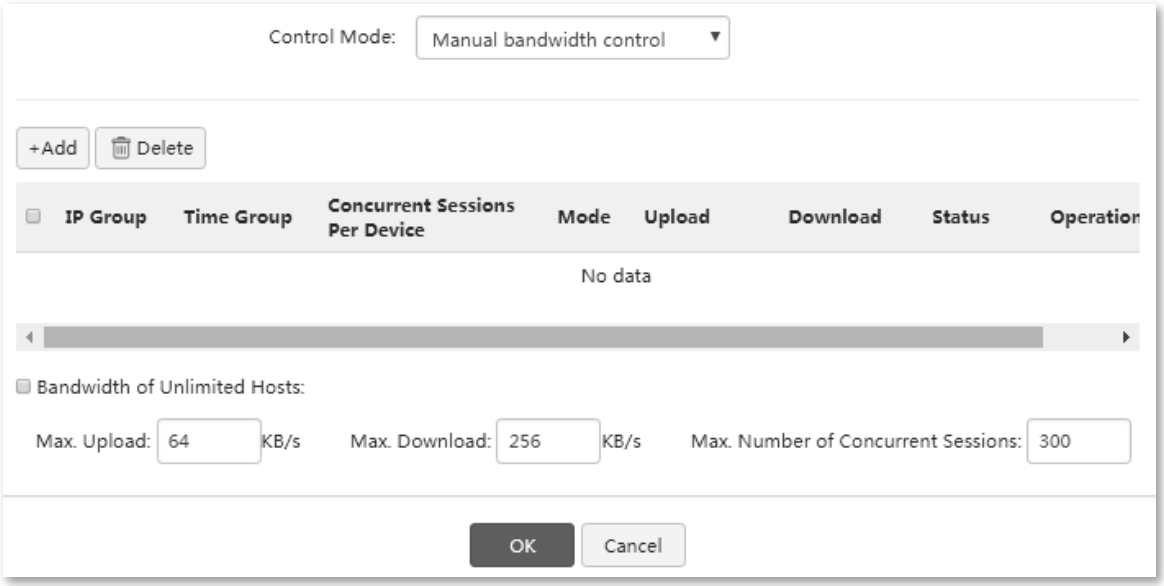
   (1) Choose **Filter Management** > **IP Group & Time Group**.

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

3. Set a manual bandwidth control rule.

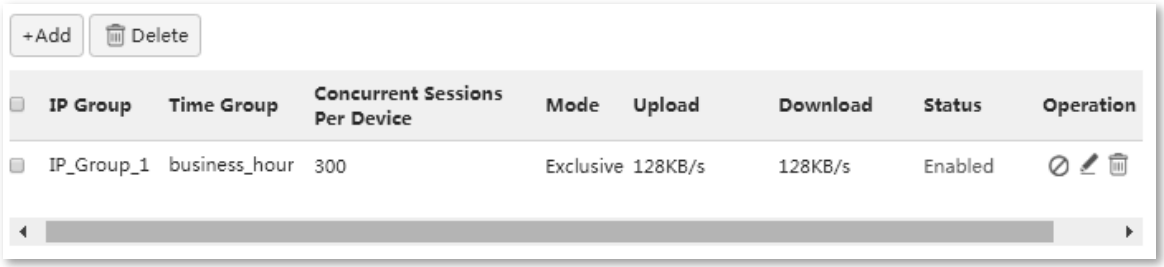
   (1) On the **Bandwidth Control** page, select **Manual bandwidth control**.

   (2) Click **OK**.



(3) On the **Bandwidth Control** page, click +Add.

(4) Create a rule shown in the following figure (1 Mbps = 128 KB/s).



(5) Set the applied **IP Group** to the corresponding rule, which is **IP_Group_1** in this example.

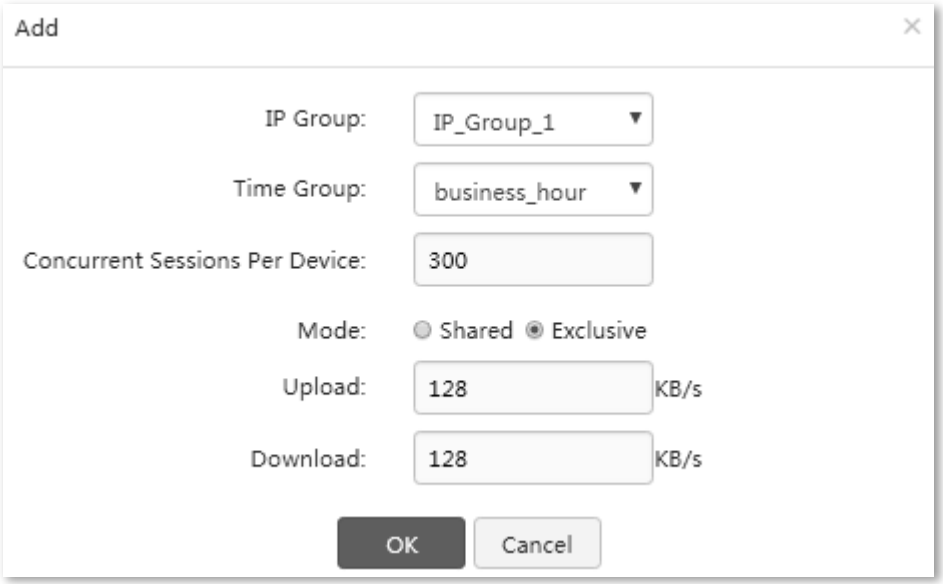
(6) Set the applied **Time Group** to the corresponding rule, which is **business_hour** in this example.

(7) Set the **Concurrent Sessions Per Device** number, which is **300** in this example.

(8) Choose **mode** as **Exclusive**.

(9) Set **Upload/Download** speed, which is **128KB/s** in this example.

(10) Click **OK.**



Verification

During business hours (08:00 to 18:00 every weekday), each computer with an IP address ranging from 192.168.0.2 to 192.168.0.100 is allocated 1 Mbps upload and download bandwidth.

7 VPN

7.1 Overview

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

This chapter describes:

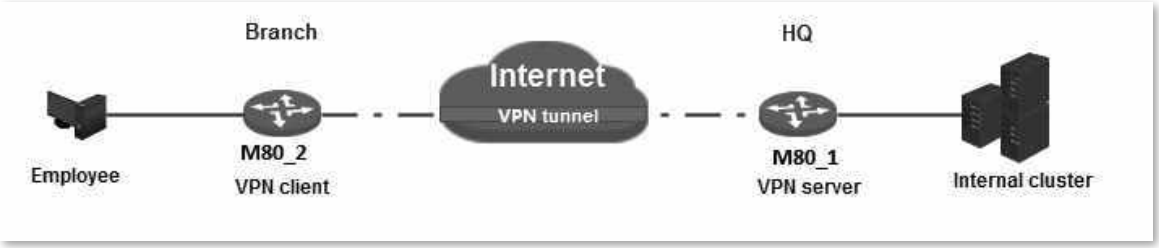
- Configuring a VPN
- Example of configuring a VPN

7.1.1 Function description

A VPN (Virtual Private Network) is a private network built on a public network (usually the internet). It is a private network, instead of a physical network. VPN technology helps employees in branch offices easily share the resources of company headquarters, and ensure that these resources are not exposed to other users on the internet.

7.1.2 Network topology

The following figure shows the typical VPN network topology.



7.1.3 VPN types

M80 supports PPTP, L2TP, and IPSec VPNs.

- **PPTP/L2TP**

The Point to Point Tunneling Protocol (PPTP) and Layer 2 Tunneling Protocol (L2TP) are layer-2 VPN tunnel protocols and the Point to Point Protocol (PPP) is used to encapsulate and add additional headers to data.

M80 can function as a PPTP/L2TP server or client.

- **IPSec**

IP Security (IPSec) is a protocol suite for transmitting data over the internet in a secure and encrypted manner.

7.1.4 IPSec-related concepts

- **Security gateway**

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

- **IPSec peer**

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

- **SA**

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

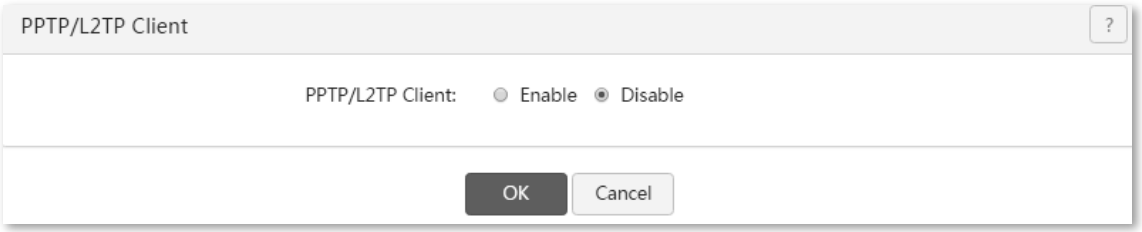
  - A triplet {SPI, Destination IP address, Security protocol identifier} is used as a unique ID.
  - An SA specifies the protocol, algorithm, and key for processing packets.
  - Each IPsec SA is unidirectional with a life cycle.
  - An SA can be created manually or generated automatically using internet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

7.2 Configuring a VPN

7.2.1 Configuring M80 as a PPTP/L2TP client

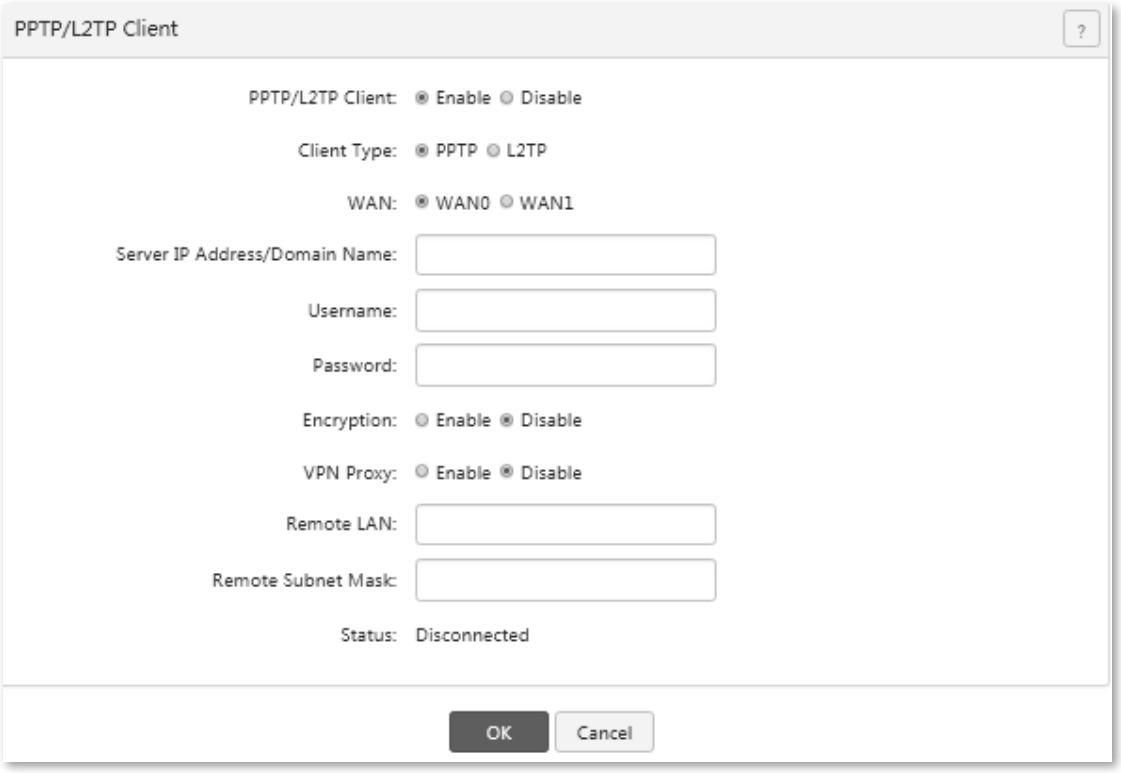
M80 can function as a PPTP/L2TP client to connect to a PPTP/L2TP server. For example, if your branch needs to exchange information with your HQ in a simple and secure manner, you can set up a PPTP/L2TP server at the HQ and configure the egress router of your branch as a PPTP/L2TP client to connect to the server.

To access the page for configuring M80 as a PPTP/L2TP client, choose **VPN** > **PPTP/L2TP Client**. See the following figure.



Configuration procedure

1. Set **PPTP/L2TP Client** to **Enable**.
2. Set the parameters.
3. Click **OK**.



---End

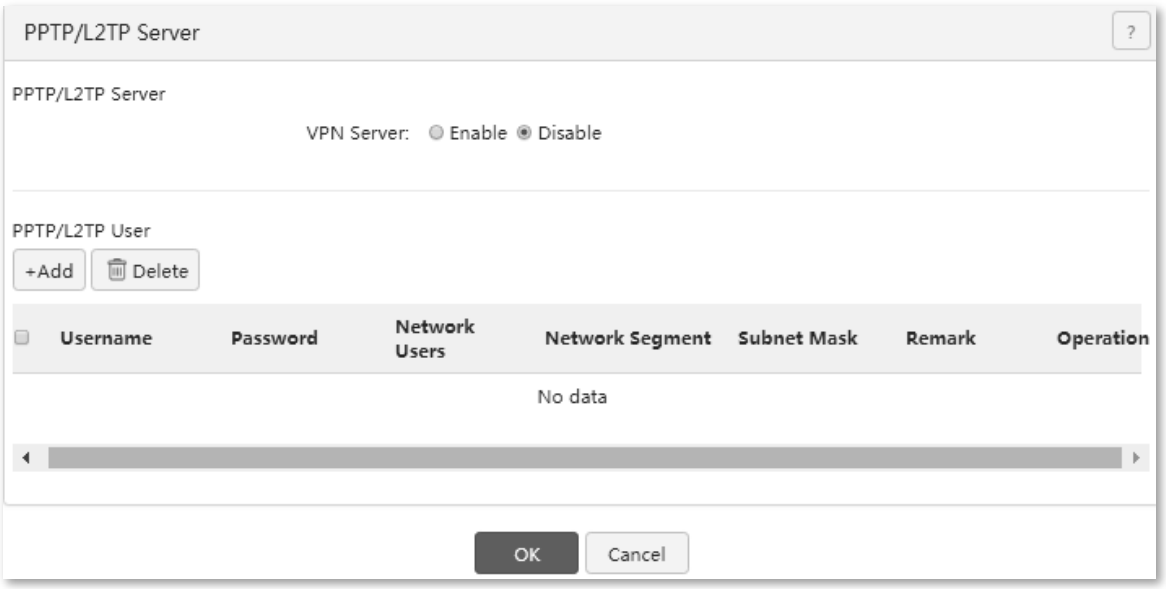
Parameter description

Parameter	Description
PPTP/L2TP Client	It specifies whether the PPTP/L2TP client function is enabled. If this parameter is set to **Enabled**, M80 functions as a PPTP/L2TP VPN client.
Type	It specifies the client type of the router. The router supports the following types: – **PPTP**: Select this option if the VPN server to be connected is a PPTP server. – **L2TP**: Select this option if the VPN server to be connected is an L2TP server.
WAN	It specifies the WAN port of the router for setting up a VPN connection.
Server IP Address/Domain Name	It specifies the IP address or domain name of the VPN server to be connected. Generally, it refers to the IP address or domain name of the WAN port of the peer VPN router that functions as the PPTP/L2TP server.
Username	Username specifies the user name of a PPTP/L2TP account. Password specifies the password for the account. The user name and password are assigned by the VPN server to be connected.
Password	
Encryption	It specifies whether to enable 128-bit data encryption. The value of this parameter must be consistent with that of the server. Otherwise, the client is unable to communicate with the server. Only PPTP VPNs support this parameter.
VPN Proxy	It specifies whether the computers on your LAN access the internet through the router of the PPTP/L2TP server.
Remote LAN	It specifies the network segment of the LAN of the PPTP/L2TP server.
Remote Subnet Mask	It specifies the subnet mask of the LAN of the PPTP/L2TP server.
Status	It specifies the current connection status of the VPN client.

7.2.2 Configuring M80 as a PPTP/L2TP server

M80 can function as a PPTP/L2TP server to connect to PPTP/L2TP clients. For example, if your branch needs to exchange information with your HQ in a simple and secure manner, you can set up a PPTP/L2TP server at the HQ and configure the egress router of your branch as a PPTP/L2TP client to connect to the server.

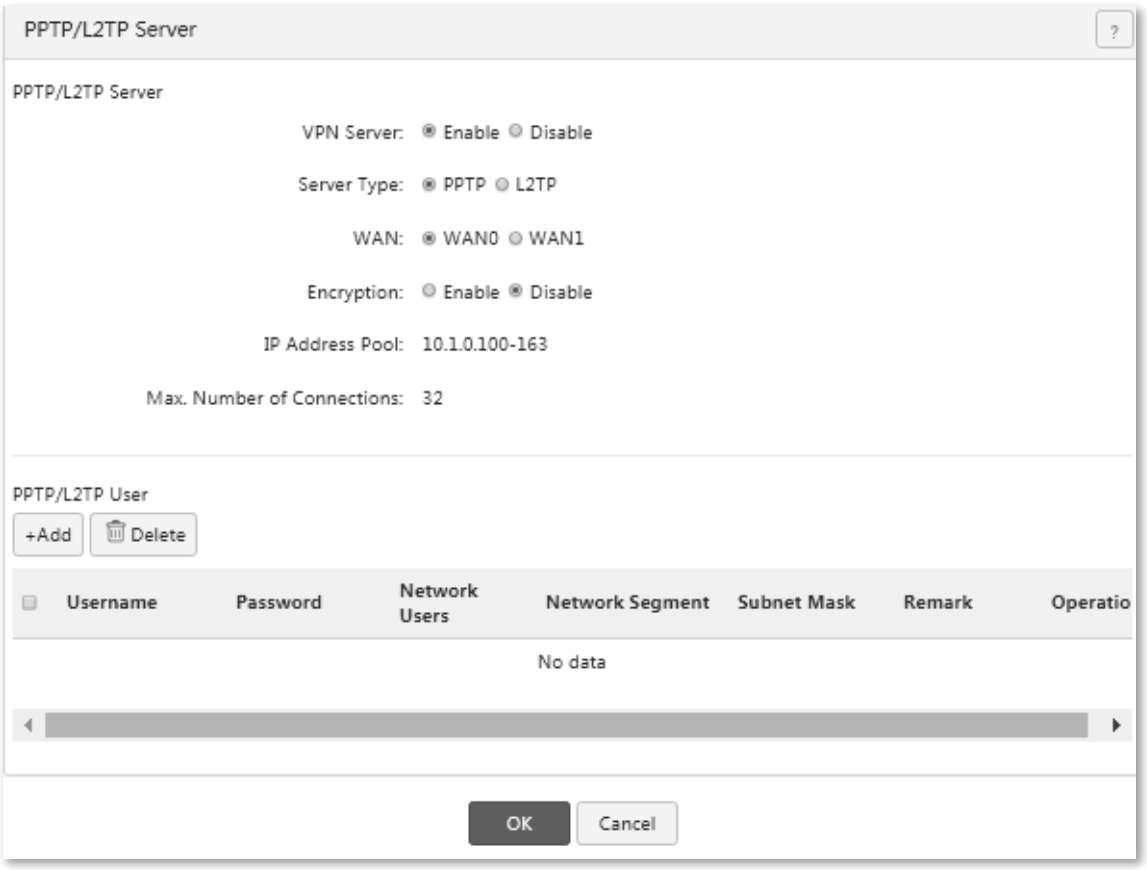
To access the page for configuring M80 as a PPTP/L2TP server, choose **VPN** > **PPTP/L2TP Server**. See the following figure.



To configure M80 as a PPTP/L2TP server, enable the PPTP/L2TP server function and configure a PPTP/L2TP account.

Enabling the PPTP/L2TP server function

1. Choose **VPN** > **PPTP/L2TP Server**.
2. Set **Status** to **Enable**.
3. Set the parameters.
4. Click **OK**.



---End

Parameter description

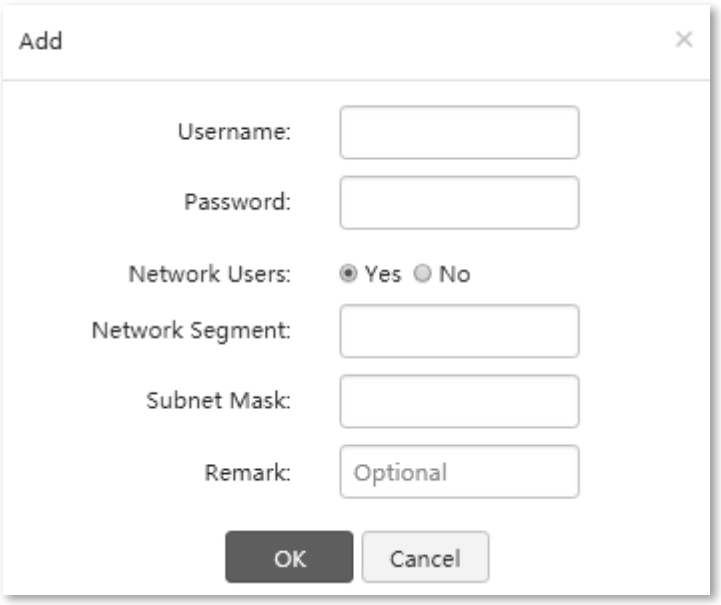
Parameter	Description
VPN Server	It specifies whether to enable the PPTP/L2TP server function. If this parameter is set to **Enabled**, M80 functions as a PPTP/L2TP server.
Type	It specifies the server type of the router. The router supports the following types: – **PPTP**: If this option is selected, the server is accessible only to PPTP clients. – **L2TP**: If this option is selected, the server is accessible only to L2TP clients.
WAN	It specifies the outgoing port of the tunnel between a PPTP/L2TP server and PPTP/L2TP clients.
Encryption	It specifies whether to enable 128-bit data encryption. The value of this parameter must be consistent with that of a client. Otherwise, the client is unable to communicate with the server. Only PPTP VPNs support this parameter.
IP Address Pool	It specifies the range of IP addresses assigned by the server to the PPTP/L2TP VPN clients connected to the server.
Max. Number of Connections	It specifies the maximum VPN clients that can be connected to the PPTP/L2TP server at the same time. The number is fixed at **32**.

Configuring a PPTP/L2TP account

A PPTP/L2TP account is required when a VPN user accesses M80 that functions as a PPTP/L2TP server.

Adding a user

1. Choose **VPN** > **PPTP/L2TP Server**.
2. Click +Add.
3. Set the parameters in the **Add** dialog box.
4. Click **OK**.

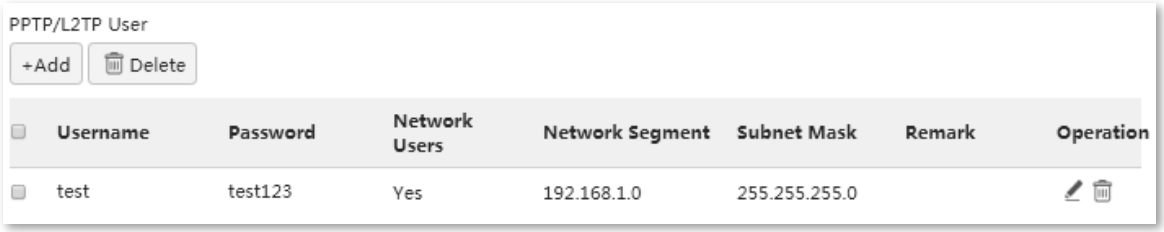


---End

Parameter description

Parameter	Description
Username	It specifies the user name used to set up a PPTP/L2TP VPN connection.
Password	It specifies the password for the user name.
Network Users	– **Yes**: It indicates that a VPN client is a network. If this option is selected, set the **Network Segment** and **Subnet Mask** parameters as well. – **No**: It indicates that there is only one VPN client.
Network Segment	It specifies the LAN network segment of a VPN client in case that the client is a network.
Subnet Mask	It specifies the subnet mask of the LAN of a VPN client in case that the client is a network.
Remark	It specifies the description of a user. This parameter is optional.

The **PPTP/L2TP Server** page appears, showing the added user. See the following figure.



Modifying a user

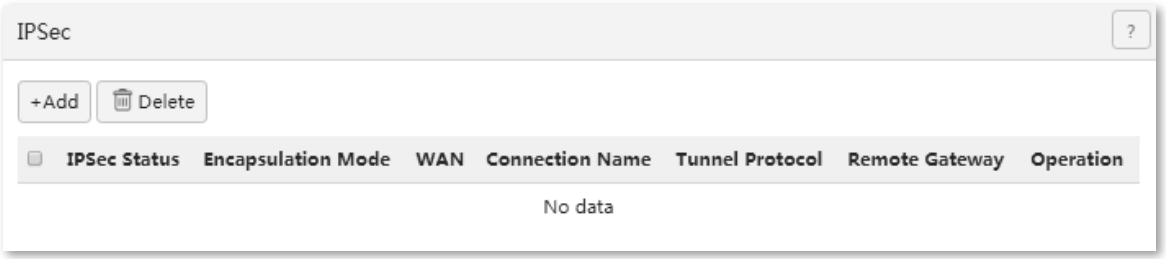
1. Choose **VPN** > **PPTP/L2TP Server**.
2. Click corresponding to a user.
3. Modify the user.

Deleting a user

1. Choose **VPN** > **PPTP/L2TP Server**.
2. Click corresponding to a user to be deleted. To delete multiple users at the same time, select them and click Delete.

7.2.3 Configuring the IPSec function

To access the page for configuring the IPSec function, choose **VPN** > **IPSec**. See the following figure.

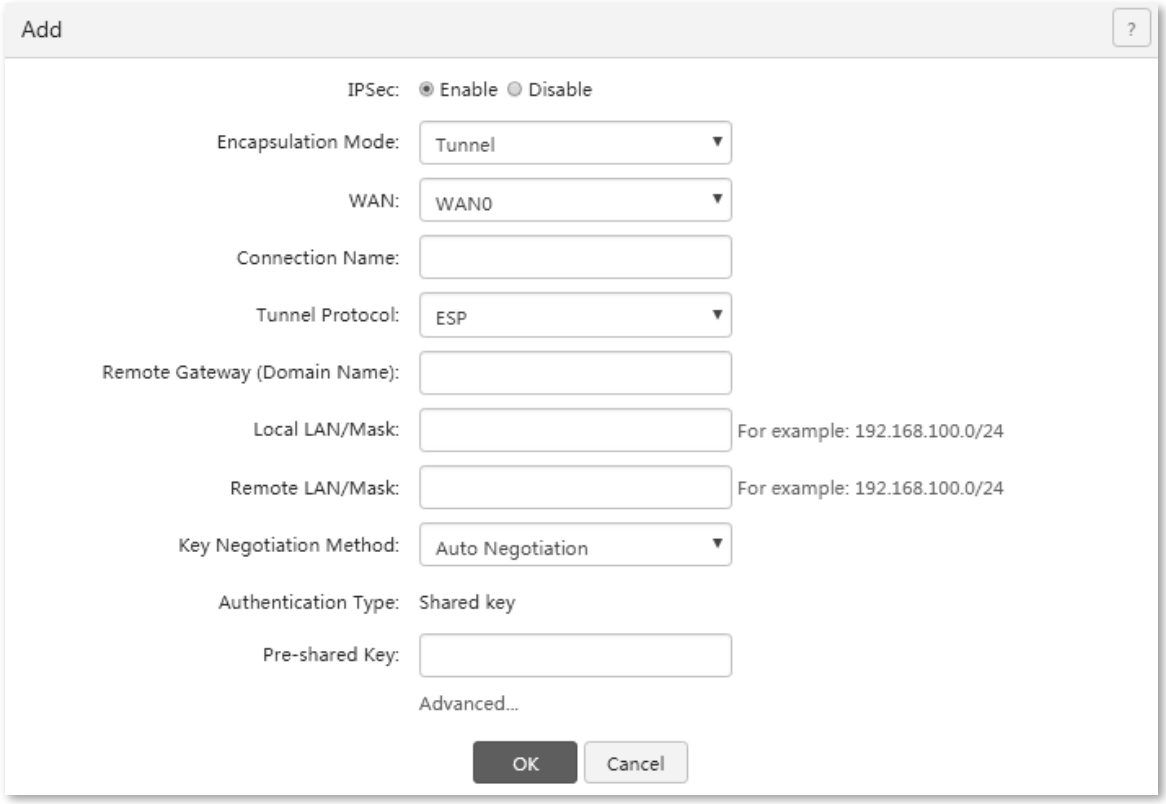


Create IPSec connection

Tunnel Mode

Click +Add to add IPSec tunnel mode.

M80 supports tunnel and transport encapsulation modes. It is tunnel by default. See the following figure.



Parameter description

Parameter	Description
IPSec	It specifies whether to enable the IPSec function.
Encapsulation Mode	It specifies the encapsulation mode of IPSec data. **Tunnel** mode is normally used for the communication between two security gateways. **Transport**

Parameter	Description
	mode is used for communication between host and host, host and gateway.
WAN	It specifies the local WAN port assigned to the IPSec function. The IP address of the WAN port must be set as the value of **Remote Gateway** of the IPSec peer.
Connection Name	It specifies the name of the IPSec connection to be set up.
Tunnel Protocol	It specifies the security service protocol for the IPSec function. M80 supports the following protocols: – **AH**: It indicates the Authentication Header (AH) protocol used for verifying data integrity. If a packet is tampered during transmission, the receiver discards it during data integrity verification. – **ESP**: It indicates the Encapsulating Security Payload (ESP) protocol for verifying data integrity and encrypting data. If a packet processed using this protocol is intercepted during transmission, it is difficult for the intercepting party to obtain the real information contained in the packet. – **AH+ESP**: It indicates both the AH and ESP protocols are used.
Remote Gateway (Domain name)	It specifies the IP address or domain name of the peer gateway of an IPSec tunnel.
Local LAN/Mask	It specifies the network segment and subnet mask of the LAN port of the router. For example, if the IP address of the LAN port of the router is 192.168.0.252 and the subnet mask is 255.255.255.0, set this parameter to **192.168.0.0/24**.
Remote LAN/Mask	It specifies the network segment and subnet mask of the LAN port of the peer gateway, or the IP address and subnet mask of the peer gateway if the gateway is a mobile device. The value format is **Network segment or IP address of the peer gateway/Subnet mask**.
Key Negotiation Method	It specifies the key negotiation mode for an IPSec tunnel. The options include: – **Auto Negotiation**: It indicates that an SA is set up, maintained, and deleted automatically using IKE. This reduces configuration complexity and simplifies IPSec usage and management. Such an SA has a life cycle and is updated regularly, ensuring higher security. – **Manual Setup**: It indicates that an SA is set up by manually specifying encryption and authentication algorithms and keys. Such an SA does not have a life cycle, and therefore it remains valid unless being manually deleted, leading to a security risks. Generally, this mode is used only for commissioning.

Key negotiation mode – Auto negotiation

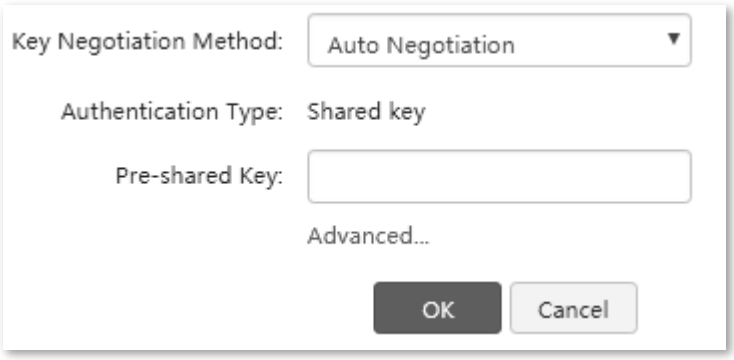
In this mode, the IPSec peers must use information shared between them to encrypt and decrypt data to ensure data confidentiality. Therefore, at the beginning of communication, the peers must negotiate a security key, which is performed by IKE, a combination of ISAKMP, Oakley, and SKEME protocols. The protocols are described as follows:

- ISAKMP: Short for internet Security Association and Key Management Protocol, ISAKMP provides a framework for key exchange and SA negotiation.
- Oakley: It describes a key exchange mechanism.
- SKEME: It describes a key exchange mechanism other than that described by the Oakley protocol.

IKE-based negotiation is divided into the following periods:

- Period 1: The peers negotiate security proposals such as authentication and encryption algorithms for communication, and set up an ISAKMP SA for exchanging more information in period 2 in a secure manner.
- Period 2: The ISAKMP SA set up in period 1 is used as an IPSec security protocol negotiation parameter to set up an IPSec SA for protecting data exchanged between the peers.

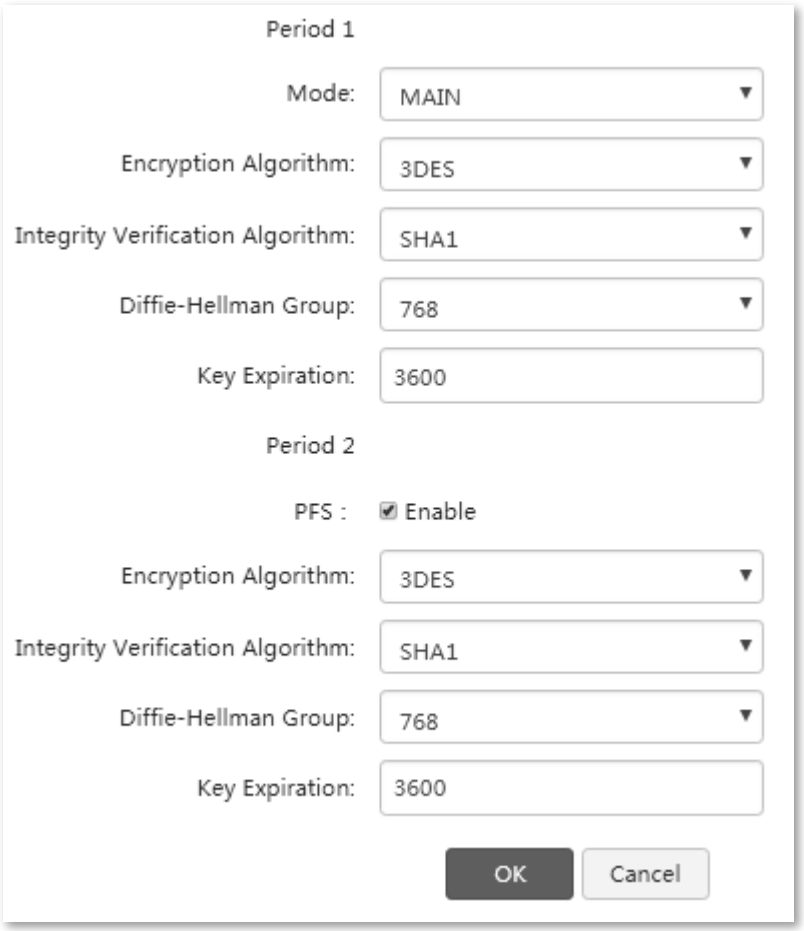
The following figure shows the parameters displayed when **Key Negotiation** is set to **Auto Negotiation**.



Parameter description

Parameter	Description
Authentication Type	It specifies a shared key negotiated by the IPSec peers by a certain means. The value **Shared key** is displayed.
Pre-shared Key	It specifies a pre-shared key used for negotiation. The key consists of a maximum of 128 characters and must be the same as that specified on the peer gateway.
Advanced...	It is a link for you to view advanced parameters for automatic key negotiation. When you click this link, the parameters shown in the following figure appears.

The following figure shows the advanced parameters of auto negotiation when click **Advanced.**

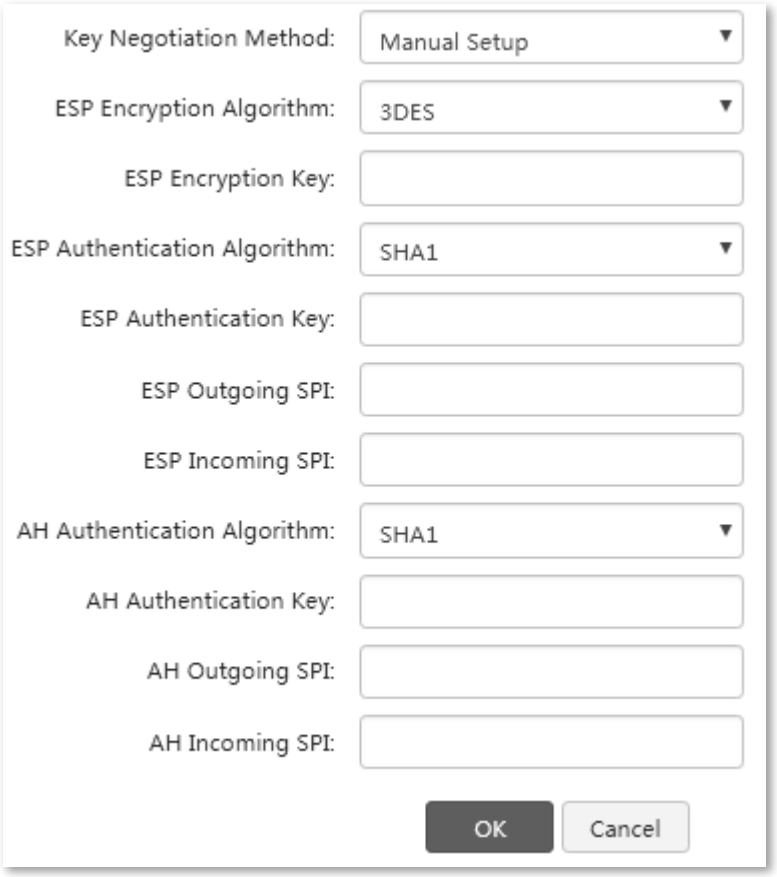


Parameter description

Parameter	Description
Mode	It specifies a packet exchange mode for IKE in period. The exchanged mode must be the same as that specified on the peer. The options include: – **MAIN**: In this mode, the two peers exchange many packets under identity protection, and therefore this mode is more suitable for scenarios where high-level identity protection is required. – **AGGRESSIVE**: In this mode, the two peers exchange only a few packets without identity protection. This mode features quick negotiation and therefore is more suitable for scenarios where high-level identity protection is not required.
Encryption Algorithm	It specifies an IKE session encryption algorithm. M80 supports the following encryption algorithms: – **DES**/**3DES**: The Data Encryption Standard (DES) uses a 56-bit key to encrypt 64-bit data and implements parity check on the last 8 bits of the 64 bits. 3DES indicates triple DES, where three 56-bit keys are used to encrypt data. – **AES-128**/**AES-192**/**AES-256**: The Advanced Encryption Standard (AES)-128/192/256 indicates that a key consisting of 128/192/256 bits is used to encrypt data.
Integrity Verification Algorithm	It specifies an IKE session verification algorithm. M80 supports the following verification algorithms: – **MD5**: Short for Message Digest 5, MD5 generate a 128-bit digest of a message to prevent message tampering. – **SHA1**: Short for Secure Hash Algorithm 1, SHA1 generates a 160-bit digest of a message to prevent message tampering. Therefore, SHA1 offers better security than MD5.
Diffie-Hellman Group	It specifies a Diffie-Hellman group for generating an IKE tunnel key.
Key Expiration	It specifies the validity period of an IPSec SA.
PFS	It specifies whether to enable the Perfect Forward Secrecy (PFS) feature, which generates a new key for IKE in period 2. This new key is not related to the key generated in period 1. In this case, the key generated in period 2 ensures data security when the key generated in period 1 is cracked. If this feature is disabled, the new key is generated in period 2 based on the key generated in period 1. In this case, when the key generated in period 1 is cracked, the new key for ensuring data security is at stake, seriously threatening the security of communication between the two peers.

Key negotiation mode – Manual Setup

The following figure shows the parameters available in this mode. (**Tunnel Protocol** is set to **AH+ESP**.)



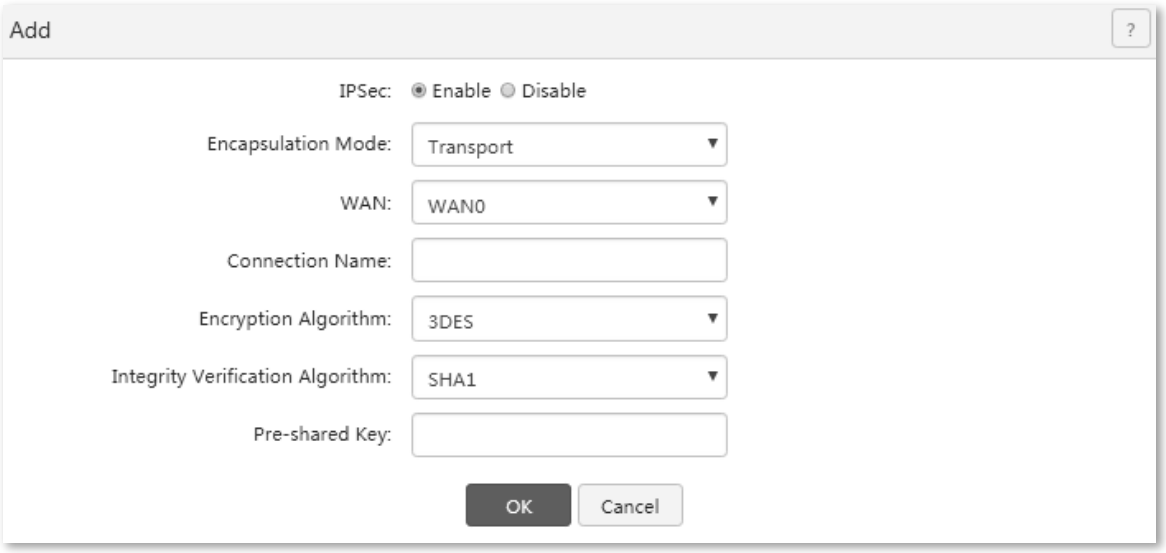
Parameter description

Parameter	Description
ESP Encryption Algorithm	It specifies the ESP encryption algorithm required in case that **Tunnel Protocol** is set to **ESP**. M80 supports the following encryption algorithms: – **DES/3DES**: DES uses a 56-bit key to encrypt 64-bit data and implements parity check on the last 8 bits of the 64 bits. 3DES indicates triple DES, where three 56-bit keys are used to encrypt data. – **AES-128/AES-192/AES-256**: AES-128/192/256 indicates that a key consisting of 128/192/256 bits is used to encrypt data.
ESP Encryption Key	It specifies an ESP encryption key, which must be adopted by the two IPSec peers.
ESP Authentication Algorithm or AH Authentication Algorithm	**ESP Authentication Algorithm** is used in case that **Tunnel Protocol** is set to **ESP**. **AH Authentication Algorithm** is used in case that **Tunnel Protocol** is set to **AH**. M80 provides the following authentication algorithm options: – **NONE**: If this option is selected, no ESP authentication key is required. – **MD5**: If this option is selected, a 128-bit digest of a message is generated to prevent tampering. – **SHA1**: If this option is selected, a 160-bit digest of a message is generated to prevent tampering. **SHA1** offers better security than MD5.
ESP Authentication Key or AH Authentication Key	**ESP Authentication Key** is used in case that **Tunnel Protocol** is set to **ESP**. **AH Authentication Key** is used in case that **Tunnel Protocol** is set to **AH**. The IPSec peers must adopt the same authentication key.
ESP Outgoing SPI or AH Outgoing SPI	It specifies an outgoing Security Parameter Index (SPI). An SPI, the peer gateway address of a tunnel, and a protocol type together identify an IPSec SA. The outgoing SPI specified here must be the same as the incoming SPI of the peer.

Parameter	Description
ESP Incoming SPI or AH Incoming SPI	An SPI, the peer gateway address of a tunnel, and a protocol type together identify an IPSec SA. The incoming SPI specified here must be the same as the outgoing SPI of the peer.

Transport Mode

Click +Add to add IPSec transport mode. The following figure shows the page when it is set to transport mode.



Parameter description

Parameter	Description
IPSec	It specifies whether to enable the IPSec function.
Encapsulation Mode	It specifies the encapsulation mode of IPSec data. Tunnel mode is normally used for the communication between two security gateways. Transport mode is used for communication between host and host, host and gateway.
WAN	It specifies the local WAN port assigned to the IPSec function. The IP address of the WAN port must be set as the value of **Remote Gateway** of the IPSec peer.
Connection Name	It specifies the name of the IPSec connection to be set up.
Encryption Algorithm	It specifies an IKE session encryption algorithm. M80 supports the following encryption algorithms: – **DES**/**3DES**: The Data Encryption Standard (DES) uses a 56-bit key to encrypt 64-bit data and implements parity check on the last 8 bits of the 64 bits. 3DES indicates triple DES, where three 56-bit keys are used to encrypt data. – **AES-128**/**AES-192**/**AES-256**: The Advanced Encryption Standard (AES)-128/192/256 indicates that a key consisting of 128/192/256 bits is used to encrypt data.
Integrity Verification Algorithm	It specifies an IKE session verification algorithm. M80 supports the following verification algorithms: – **MD5**: Short for Message Digest 5, MD5 generates a 128-bit digest of a message to prevent message tampering. – **SHA1**: Short for Secure Hash Algorithm 1, SHA1 generates a 160-bit digest of a message to prevent message tampering. Therefore, SHA1 offers better security than MD5.
Pre-shared Key	It specifies a pre-shared key used for negotiation. The key consists of a maximum of 128 characters and must be the same as that specified on the peer gateway.

7.3 Example of configuring a VPN

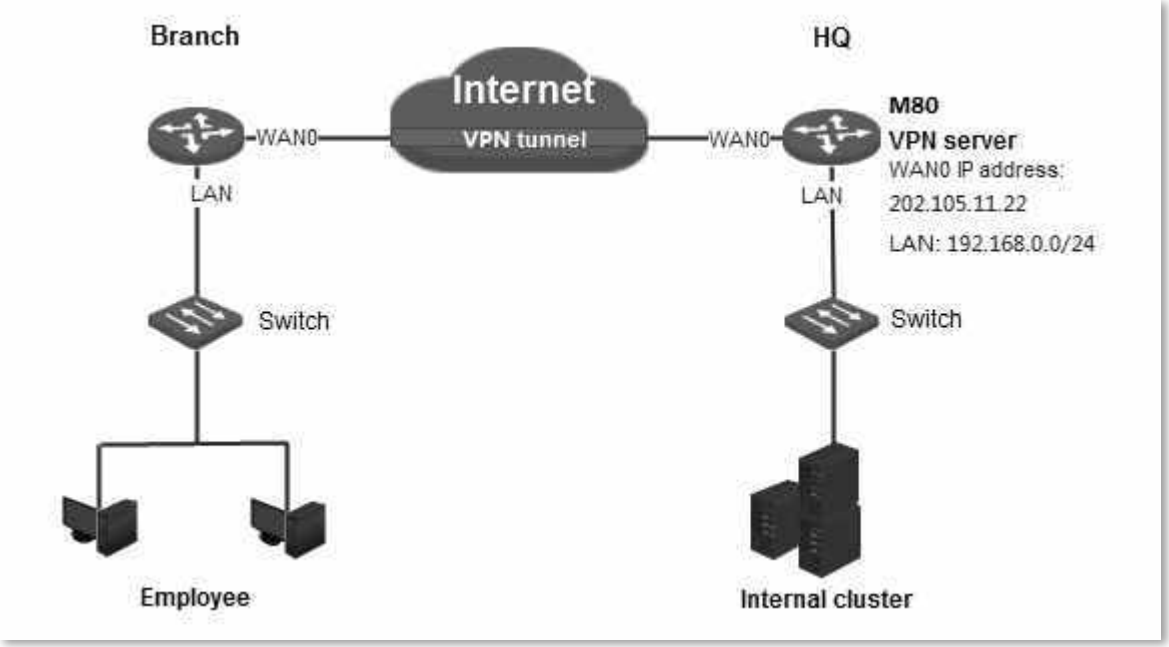
7.3.1 Example of configuring a PPTP/L2TP VPN

Networking requirement

An enterprise has used M80 to set up a LAN and access the internet. Branch employees need to access the HQ's internal resources through the internet, such as internal data, OA, ERP, CRM, project management systems.

PPTP/L2TP VPNs of M80 can address this requirement. The following uses PPTP to illustrate the setup procedure. Set up L2TP VPN in the same way.

Network topology



Configuration procedure

Configure M80_1 as a VPN server and M80_2 as a VPN client as follows:

I. Configure M80_1.

1. Enable the PPTP server function.

   (1) On M80_1, choose **VPN** > **PPTP/L2TP Server**.

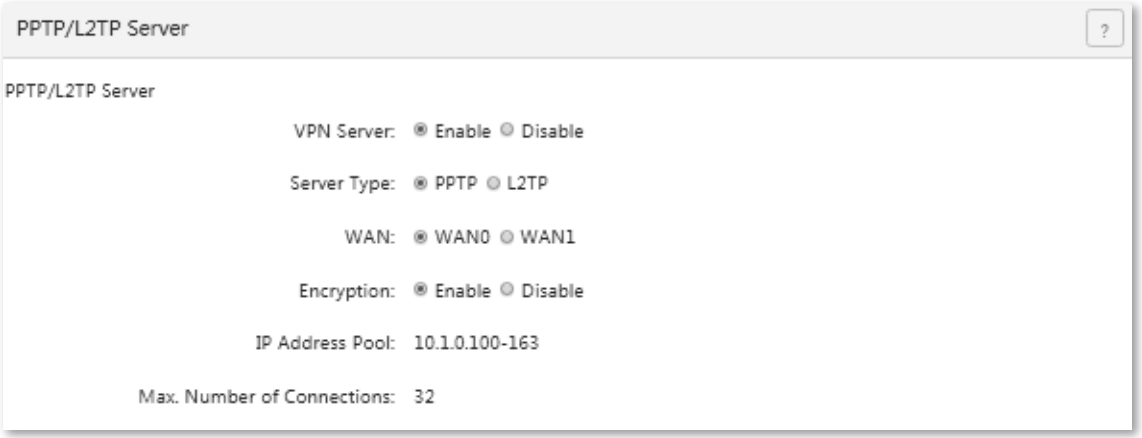
   (2) Set **Status** to **Enable**.

   (3) Set **Type** to the type of the VPN server, which is **PPTP Server** in this example.

(4) Set **WAN** to the outgoing port of the VPN server for setting up a tunnel with the VPN client, which is **WAN0** in this example.

(5) Set **Encryption** to specify whether to enable data encryption. The PPTP server and client must use the same setting.

(6) Click **OK**.



2. Configure a PPTP/L2TP user.

(1) On M80_1, choose **VPN** > **PPTP/L2TP Server**.

(2) Move to **PPTP/L2TP User** module, and click +Add.

(3) Set **Username** to the user name used to connect the VPN client to the VPN server, which is **Branch_1** in this example.

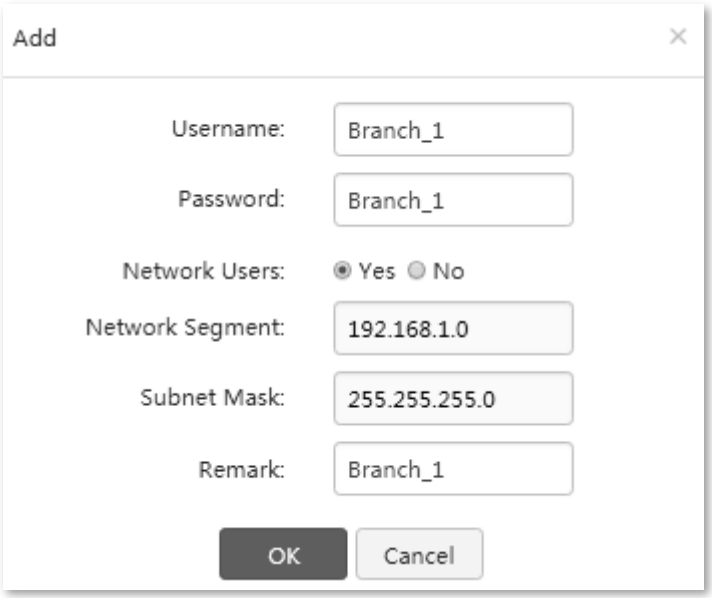
(4) Set **Password** to the password for the user name, which is **Branch_1** in this example.

(5) Set **Network Users** to **Yes**.

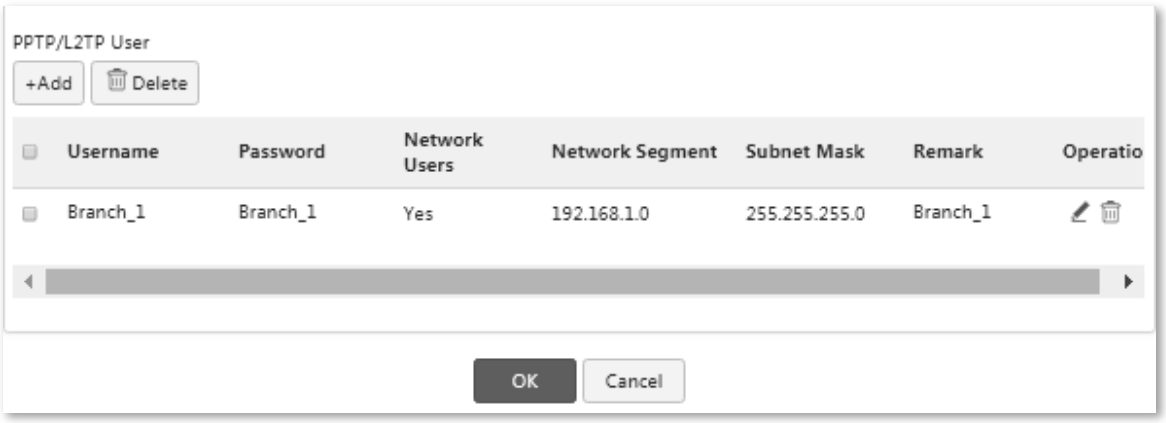
(6) Set **Network Segment** to the LAN IP address of the VPN client, which is **192.168.1.0** in this example.

(7) Set **Subnet Mask** to **255.255.255.0**.

(8) Set **Remark** to the description of the user, which is **Branch_1** in this example.

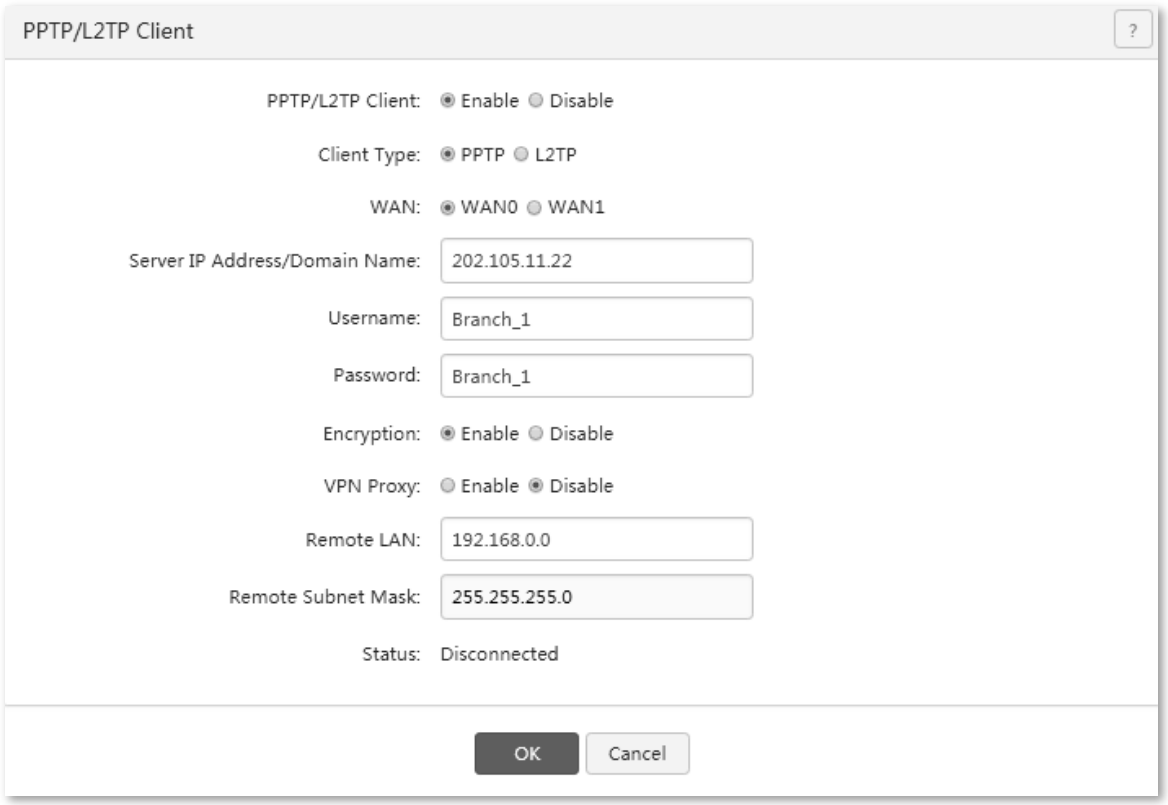


(9) Click **OK**.



II. Configure M80_2.

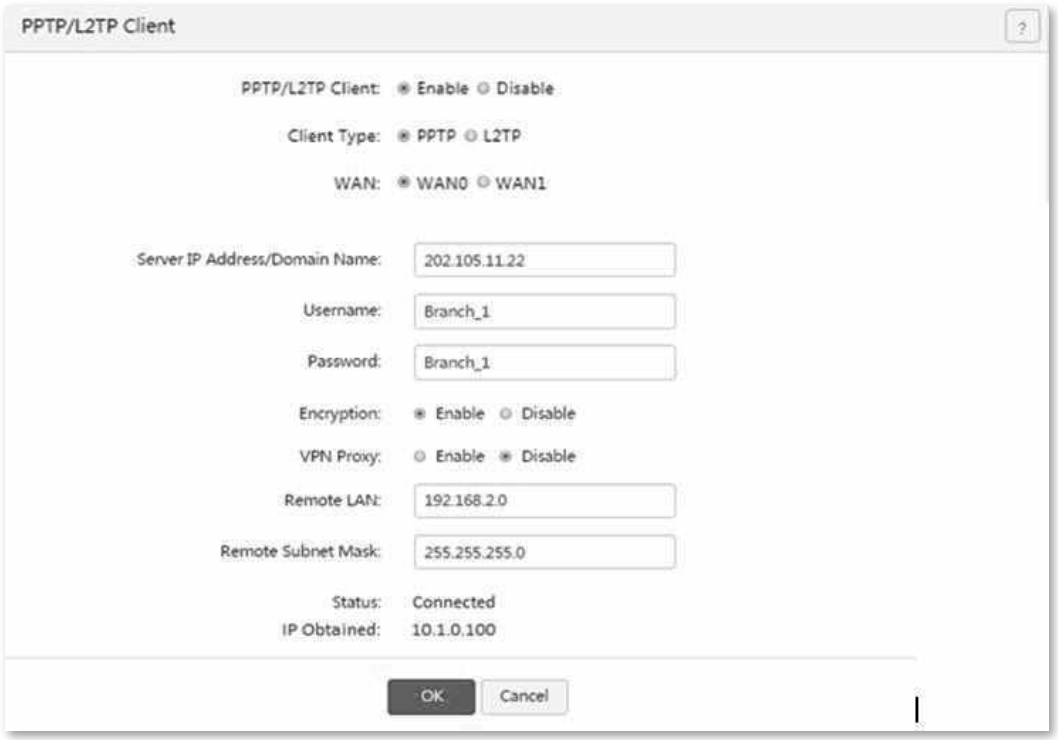
1. On M80_2, choose **VPN** > **PPTP/L2TP Client**.
2. Set **PPTP/L2TP Client** to **Enable**.
3. Set **Type** to the value matching the VPN server, which is **PPTP Client** in this example.
4. Set **WAN** to the outgoing port of the VPN client for setting up a tunnel with the VPN server, which is **WAN0** in this example.
5. Set **Server IP Address/Domain Name** to the IP address of the outgoing port of the VPN server, which is **202.105.11.22** in this example.
6. Set **Username** and **Password** to the user name and password assigned by the VPN server, which are **Branch_1** in this example.
7. Set **Encryption** to **Enable**. This setting must be the same as that on the VPN server.
8. Set **VPN Proxy** to **Disable**.
9. Set **Remote LAN** to the LAN network segment of the VPN server, which is **192.168.0.0** in this example.
10. Set **Remote Subnet Mask** to the LAN subnet mask of the VPN server, which is **255.255.255.0** in this example.
11. Click **OK**.



---End

Verification

1. On M80_2, choose **VPN** > **PPTP/L2TP Client**.
2. Verify that **Status** is **Connected** and an IP address has been obtained.
   See the following figure.



After the preceding configuration, employees at the branch and HQ can remotely access resources on the branch and HQ LANs through the internet in a secure manner. The following is an example of how the employees at branch access the FTP server at the headquarters. The HQ project data is placed on the FTP server. Assume that the server information is as follows:

- IP address of the FTP server is 192.168.0.223
- Server port is 8080.
- Login username and password are both admin.

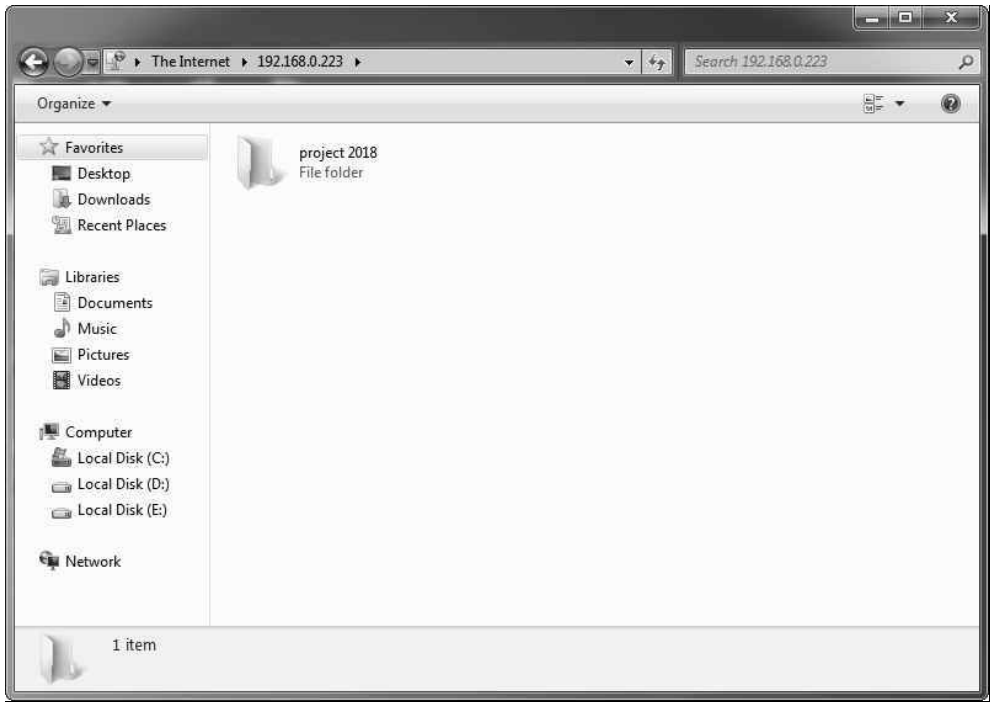
The procedures for employees at the branch access the HQ project data are as follow:

1. Access the link ftp://server IP address:server port on a computer, which is ftp://192.168.0.223:8080 in this example.

2. In the popup window, enter login username and password, which are both **admin** in this example.

3. Click **Logon.**

Access the data successfully.



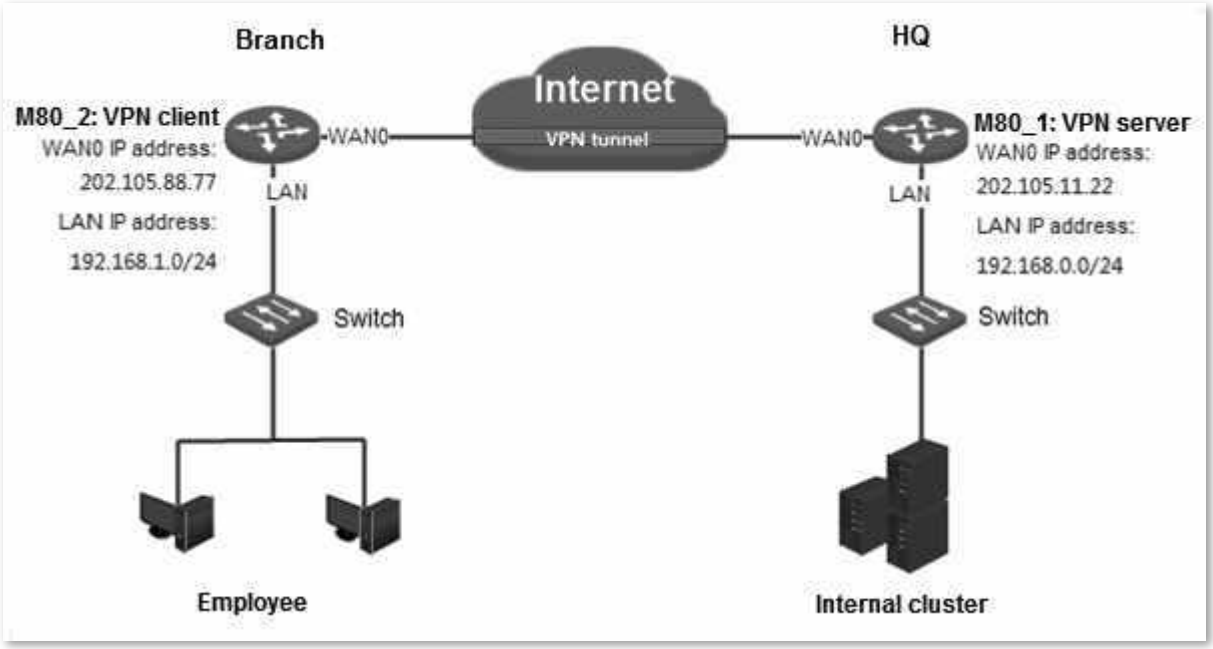
7.3.2 Example of configuring an IPSec VPN

Networking requirement

An enterprise has used M80 to set up a LAN and access the internet. Branch employees need to access the HQ's internal resources through the internet, such as internal data, OA, ERP, CRM, project management systems.

You can set up an IPSec VPN using the router to meet this requirement.

Network topology



Note

- During the configuration, if you need to modify advanced settings for IPSec connections, keep the settings of the two routers consistent.
- When the **Key Negotiation Method** is set to **Manual Setup**, the encryption algorithms, encryption keys, and authentication algorithms at IPSec peers must be the same. The ESP outgoing SPI of M80_1 is the same as the ESP incoming SPI of M80_2, and the ESP incoming SPI of M80_1 and the ESP outgoing of M80_2 are the same.
- You are recommended to turn off the security software such as firewall.

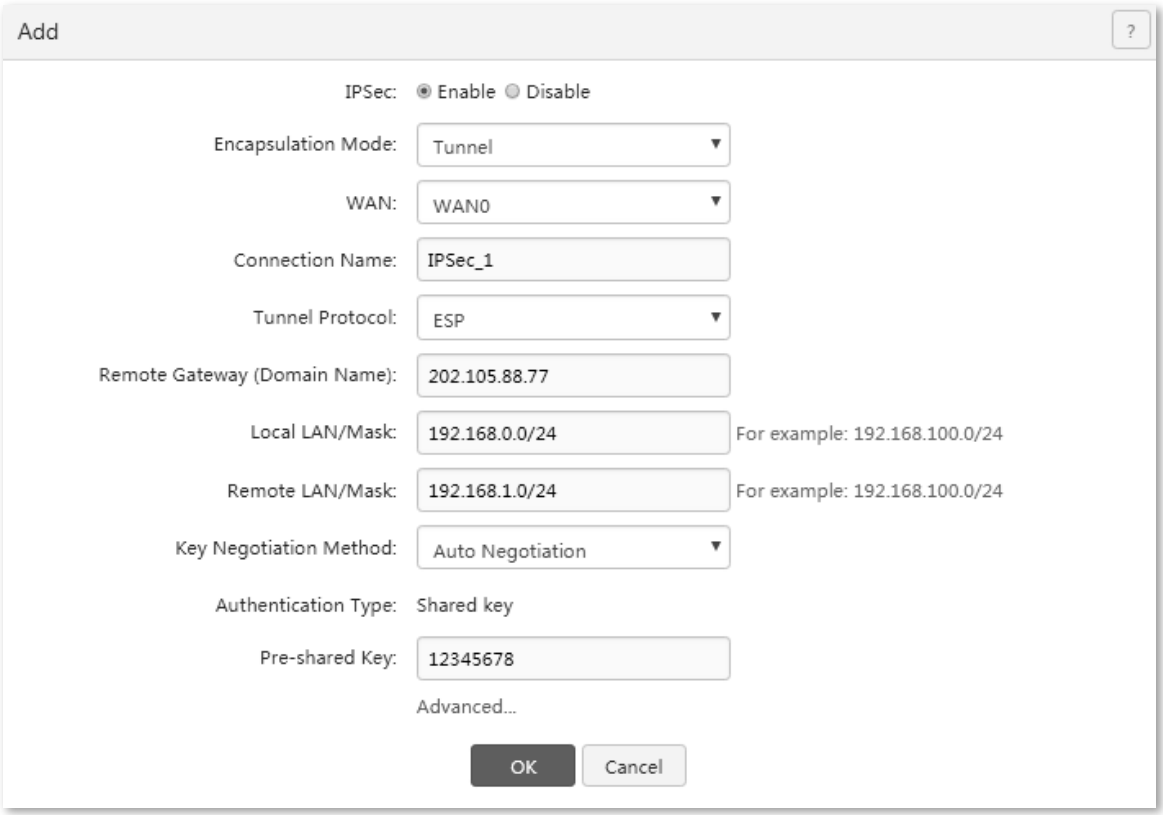
Configuration procedure

Assume that the two routers share the following basic IPSec tunnel information:

- **Encapsulation Mode**: Tunnel
- **Key negotiation method**: Auto Negotiation
- **Pre-shared key**: 12345678

I. Configure M80_1.

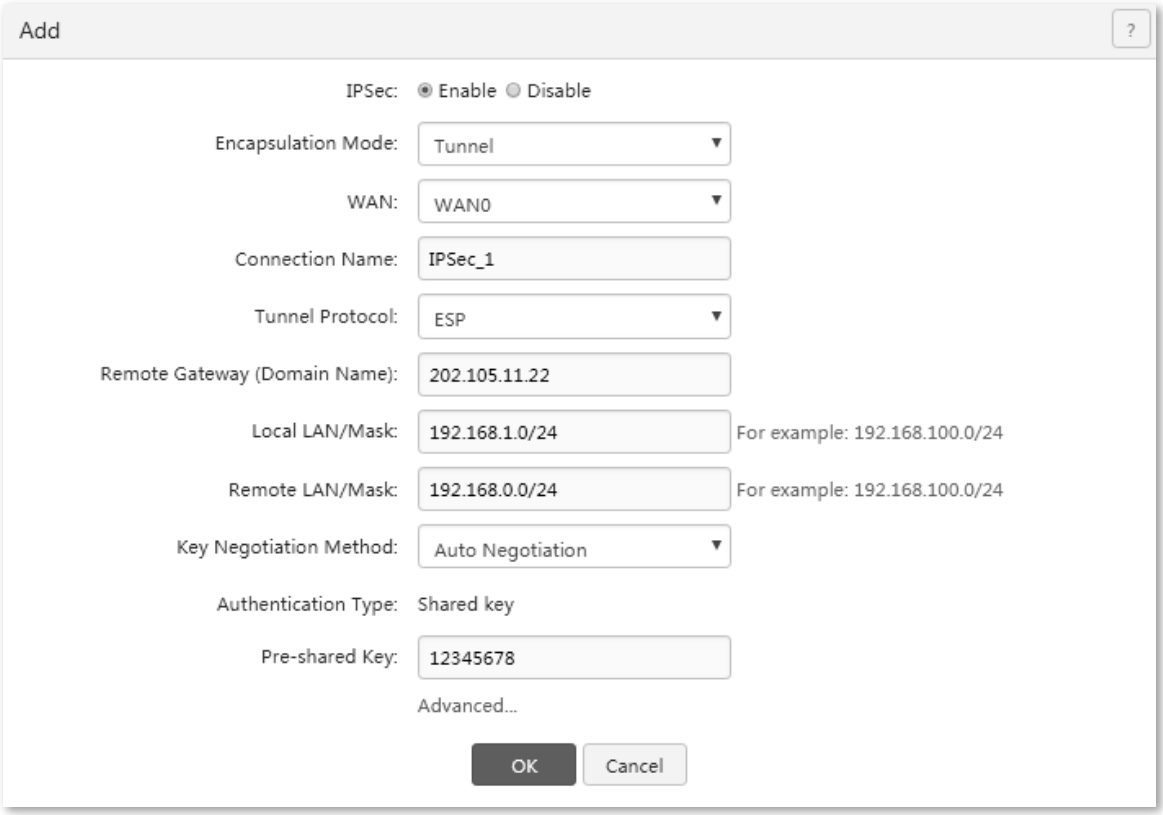
1. On M80_1, choose **VPN** > **IPsec**.
2. Click +Add.
3. Set required parameters.
   (1) Set **IPSec** to **Enable**.
   (2) Set **Encapsulation Mode** to **Tunnel**.
   (3) Set **WAN** to the WAN port bound to the IPSec tunnel, which is **WAN0** in this example.
   (4) Set **Connection Name** to the name of the IPSec tunnel, which is **IPSec_1** in this example.
   (5) Set **Remote Gateway (Domain Name)** to the IP address of the M80_2 WAN port bound to the IPSec tunnel, which is **202.105.88.77** in this example.
   (6) Set **Local LAN/Mask** to the LAN network segment and subnet mask of M80_1, which is **192.168.0.0/24** in this example.
   (7) Set **Remote LAN/Mask** to the LAN network segment and subnet mask of M80_2, which is **192.168.1.0/24** in this example.
   (8) Set **Pre-shared Key** to **12345678**.



4. Click **OK**.

II. Configure M80_2.

1. On M80_2, choose **VPN** > **IPsec**.
2. Click +Add.
3. Follow the M80_1 configuration procedure to set the parameters.



---End

Verification

1. Log in to the routers, choose **System** > **Live Users**.
2. Verify that **IPSec SA** displays the number of connections and related connection information.

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

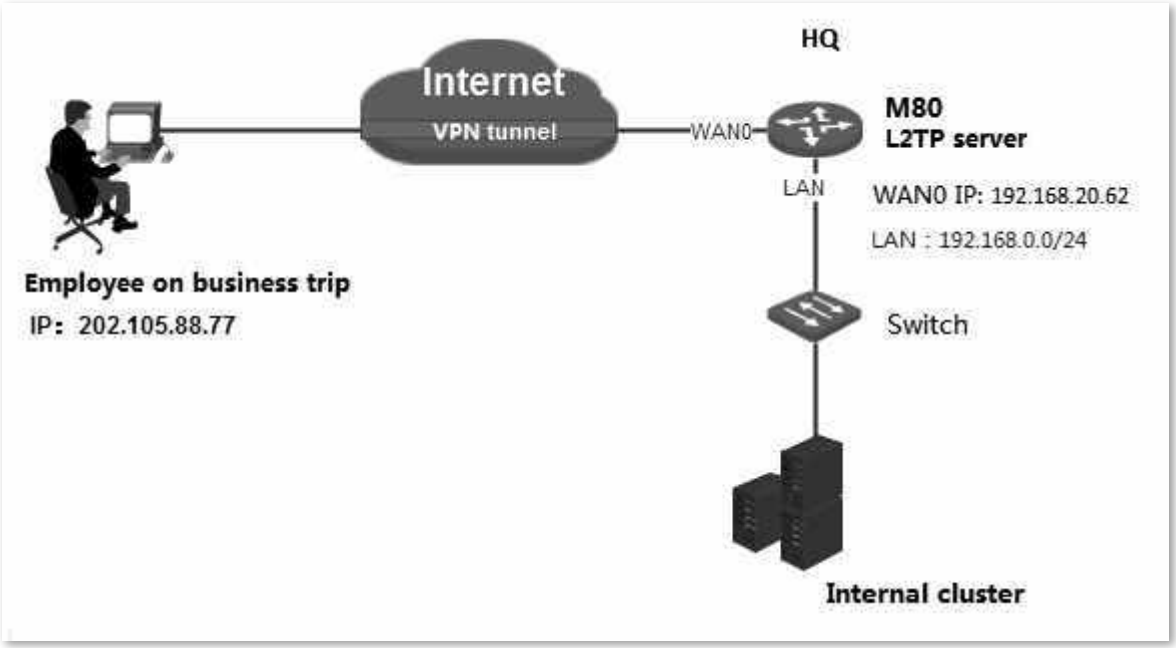
7.3.3 Example of configuring an L2TP over IPSec VPN

Networking requirement

An enterprise has used M80 to set up a LAN and access the internet. Employees of its branch must be allowed to access, through the internet, the HQ's resources over the HQ LAN in a secure manner, including internal materials as well as the OA, ERP, CRM, and project management systems.

You can set up an L2TP over IPSec VPN using the router to meet this requirement.

Network topology



Configuration procedure

Assume that the two routers share the following basic IPSec information:

- **Encapsulation Mode**: Transport
- **Key negotiation Method**: Auto Negotiation
- **Pre-shared Key**: 87654321

I. Configure IPSec connection.

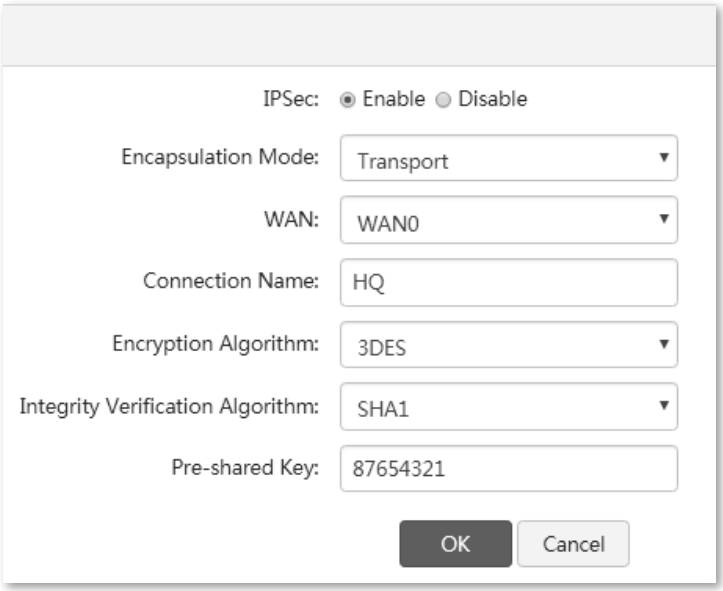
1. Choose **VPN** > **IPsec**.
2. Click +Add .
3. Set required parameters.
   (1) Set **IPSec** to **Enable**.
   (2) Set **Encapsulation Mode** to **Transport**.
   (3) Set **WAN** to the WAN port bound to the IPSec tunnel, which is **WAN0** in this example.

(4) Set **Connection Name** to the name of the IPSec tunnel, which is **HQ** in this example.

(5) Set **Pre-shared Key** to **87654321**.

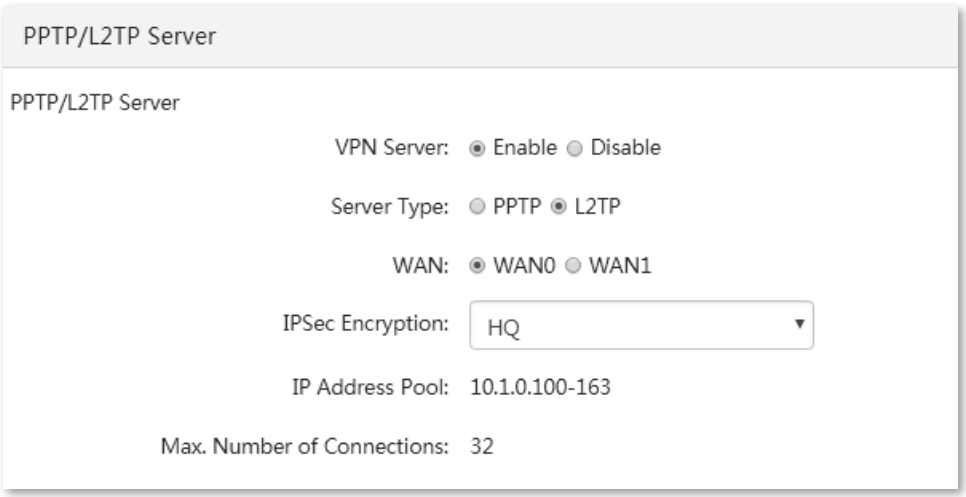
(6) Click **OK**.

The following figure shows the added rule.



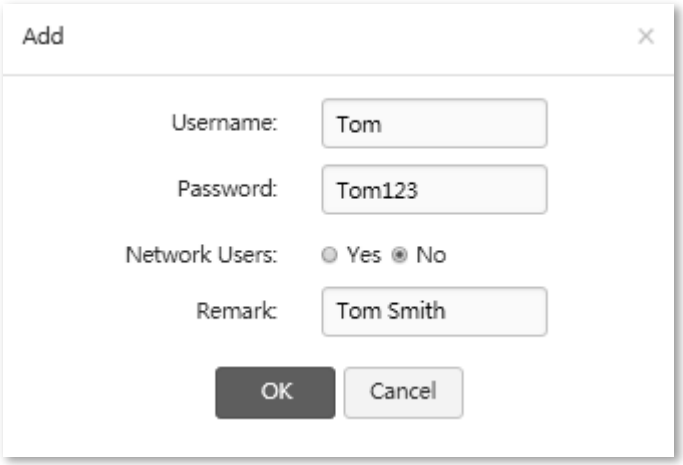
II. Configure L2TP server.

1. Choose **VPN** > **PPTP/L2TP Server**.
2. Set required parameters.
   (1) Set **VPN Server** to **Enable**.
   (2) Set **Server Type** to **L2TP**.
   (3) Set **WAN** to the WAN port bound to the IPSec tunnel, which is **WAN0** in this example.
   (4) Set **IPSec Encryption** to **HQ**.
3. Click **OK.**



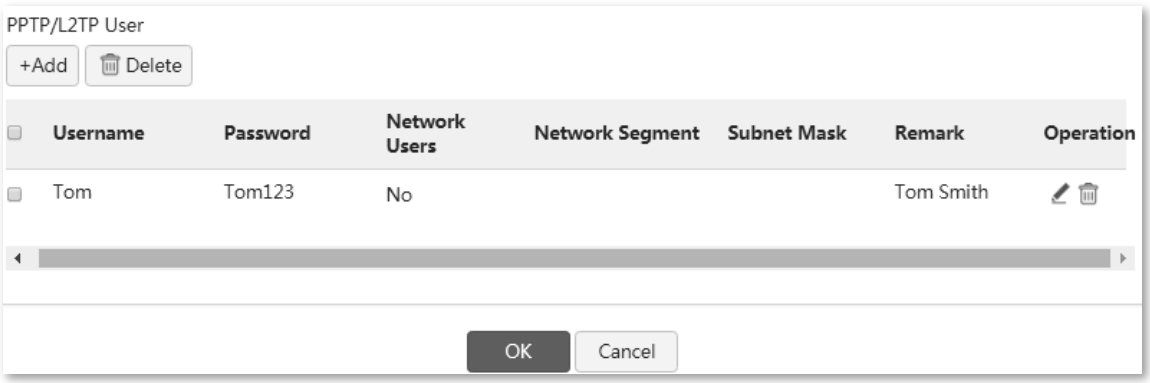
III. Add L2TP users.

1. Choose **VPN** > **PPTP/L2TP Server**, locate **PPTP/L2TP User** module.
2. Click +Add .
3. Set required parameters.
   (1) Set **Username** to the user name used to connect the VPN client to the VPN server, which is **Tom** in this example.
   (2) Set **Password** to the password for the user name, which is **Tom123** in this example.
   (3) Set **Network Uers** to **No**.
   (4) Set **Remark** to the description of the user, which is **Tom Smith** in this example.
   (5) Click **OK.**



---End

The following figure shows the added user.



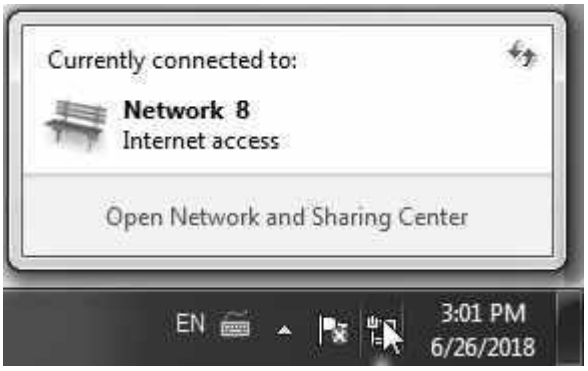
Verification

Creating VPN dialing for employees on business trip

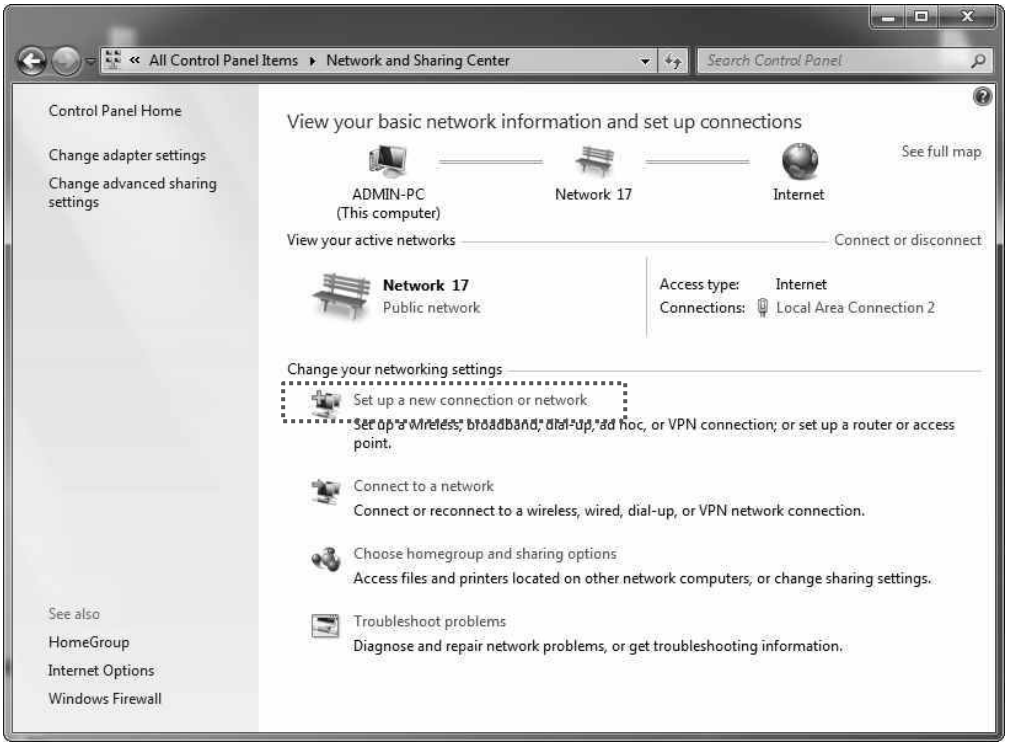
Scenario 1: Create VPN connection on a computer. Here takes Windows 7 as an example.

1. Create VPN connection.

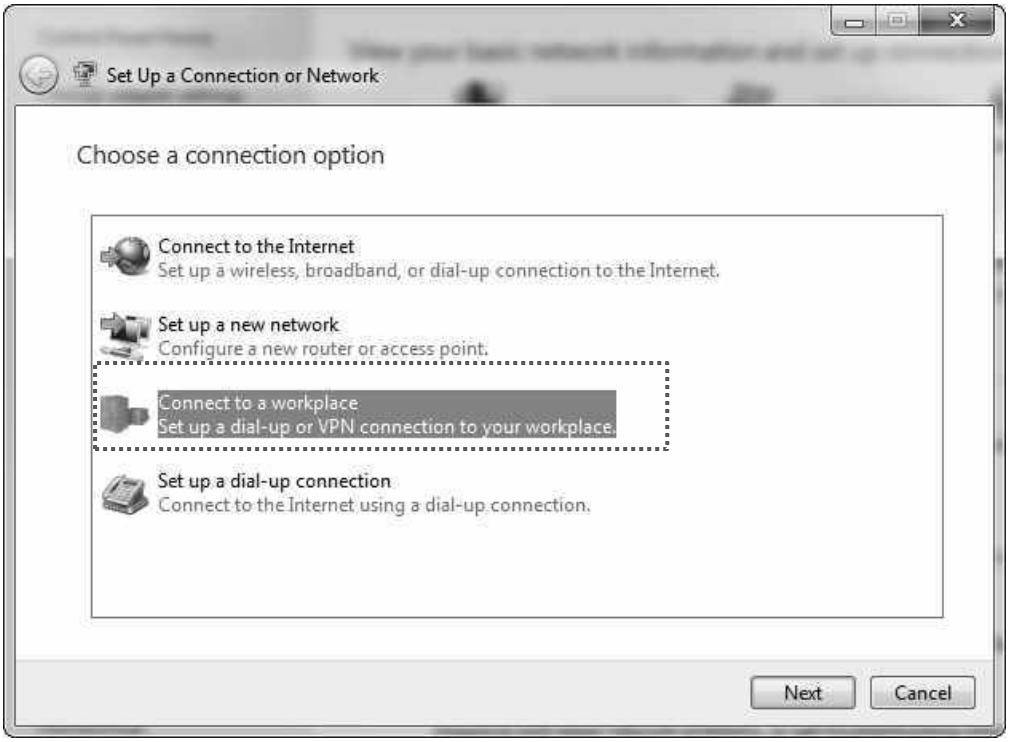
(1) Click in the lower right corner of the desktop, click **Open Network and Sharing Center.**



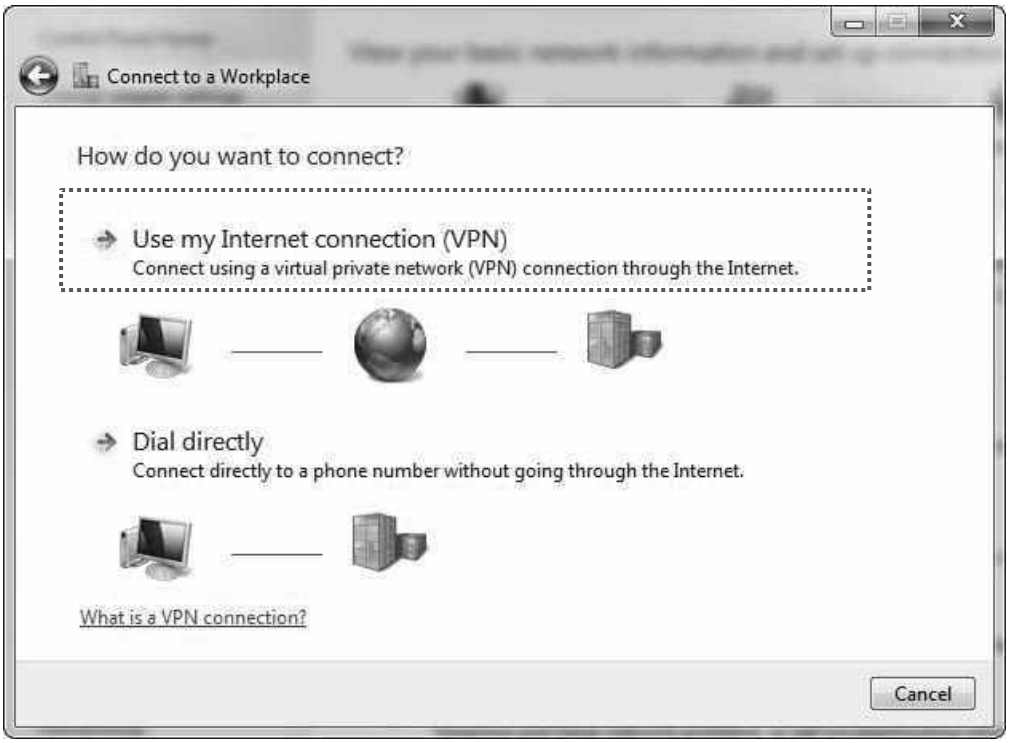
(2) Click **Set up a new connection or network**.



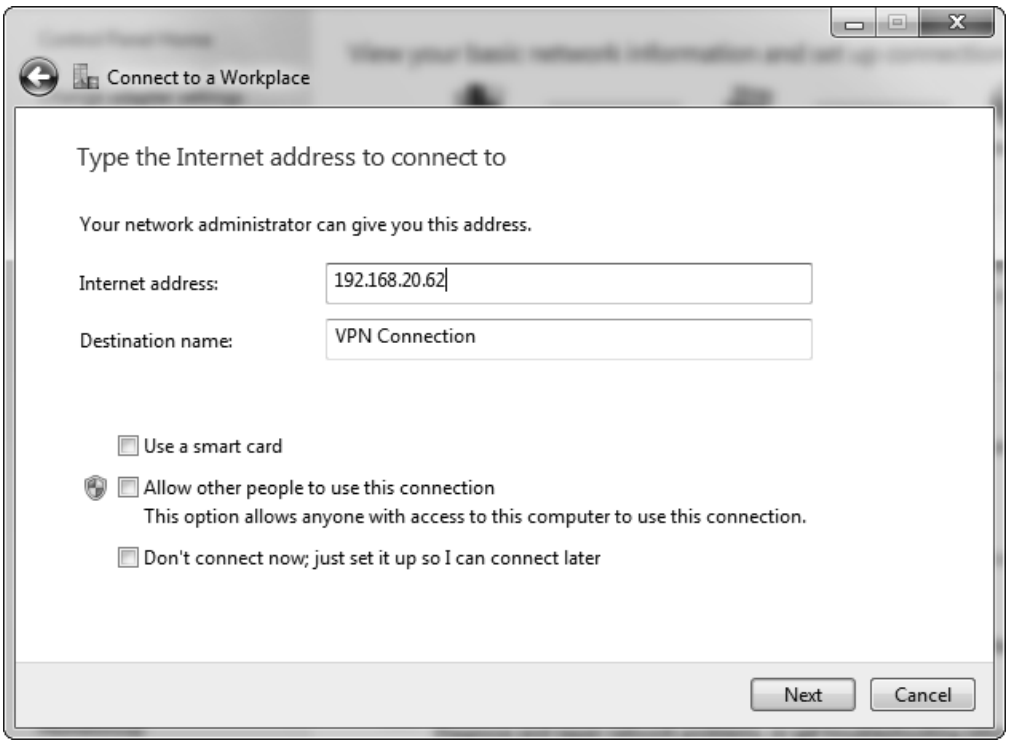
(3) Click **Connect to a workplace**, and then click **Next**.



(4) Click **Use my internet connection (VPN)**. If any other window popup, follow the onscreen instructions.



(5) Set the IP address of the L2TP server, which is **192.168.20.62** in this example. Then click **Next.**

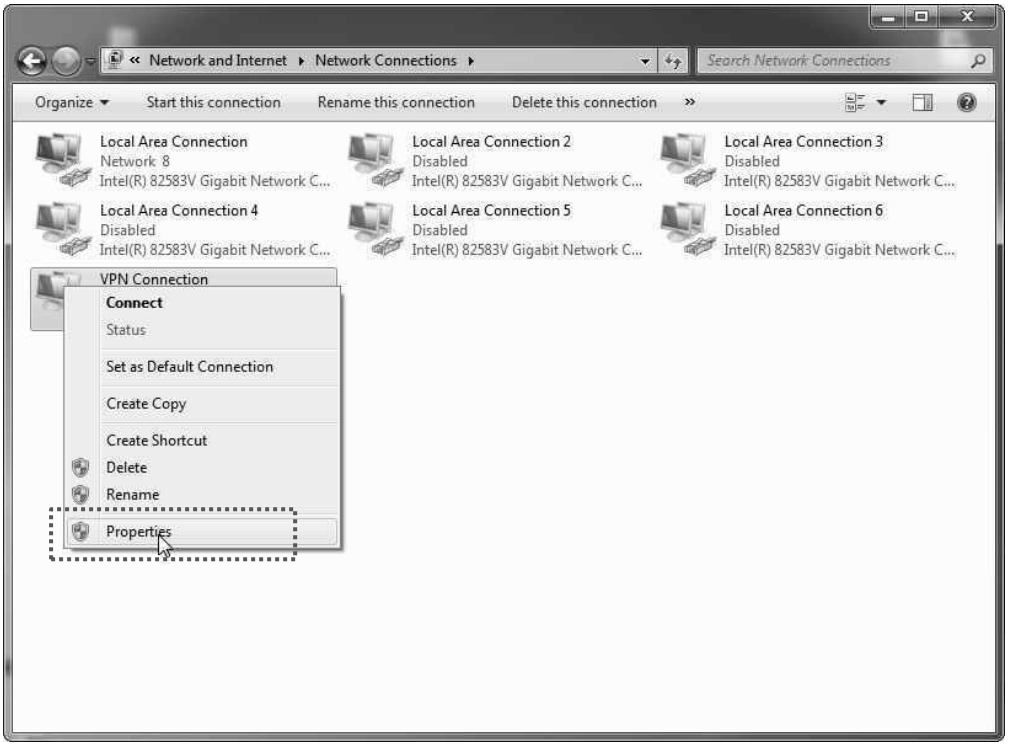


(6) Set the **username** to **Tom**, and **password** to **Tom123**. Then click **Create.**

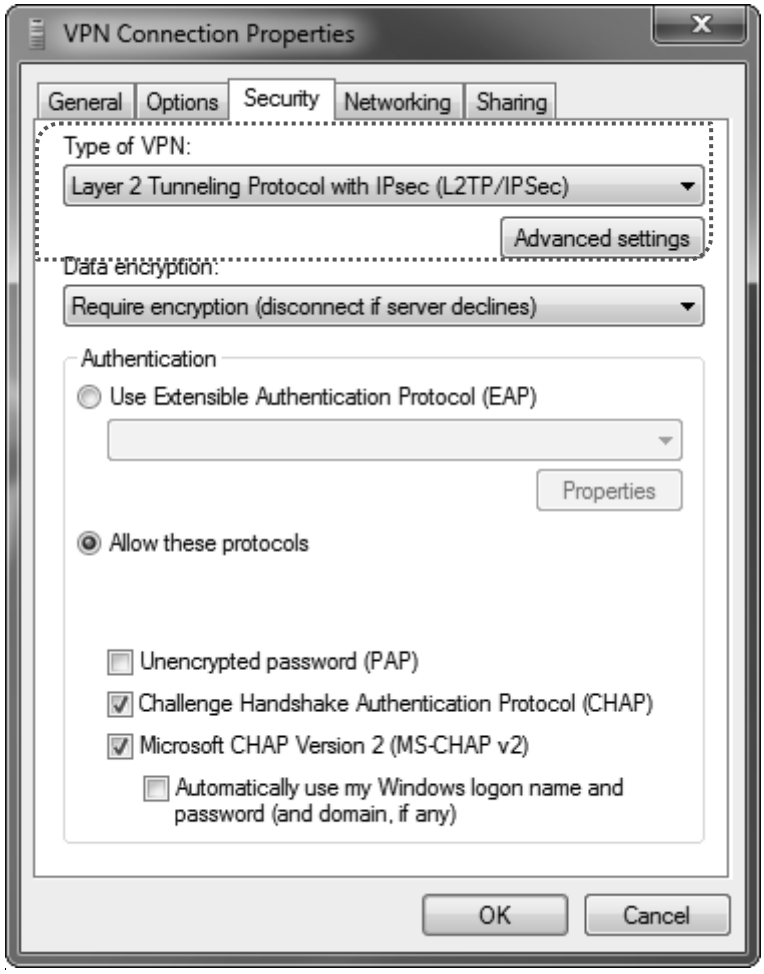
(7) Wait for a moment to establish a connection.

2. Set VPN connection parameters.

(1) Click in the lower right corner of the desktop, choose **Open Network and Sharing Center,** click **Change adapter settings,** right click on **VPN connection,** and choose **Properties.**

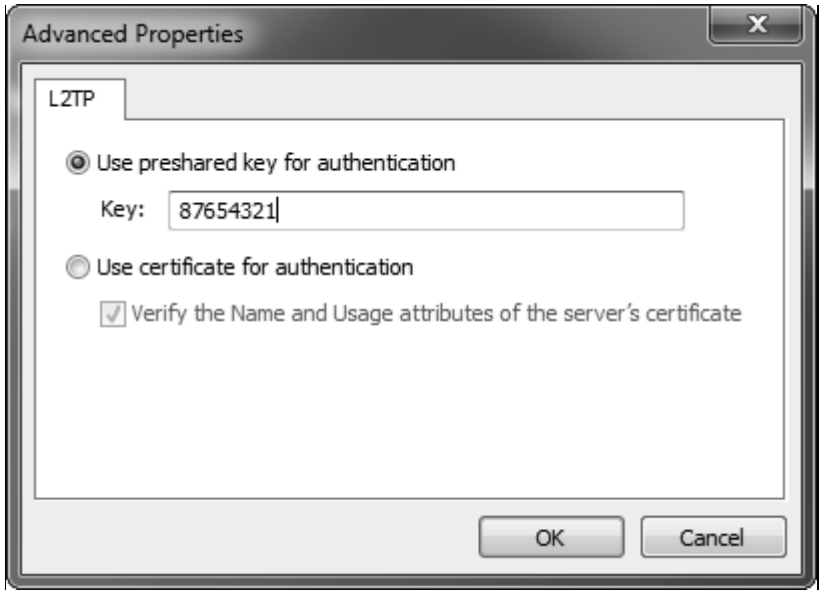


(2) Click **Security** tab, in the **Type of VPN** section, choose **Layer 2 Tunneling Protocol with IPsec (L2TP/IPSec)** and click **Advanced settings**.

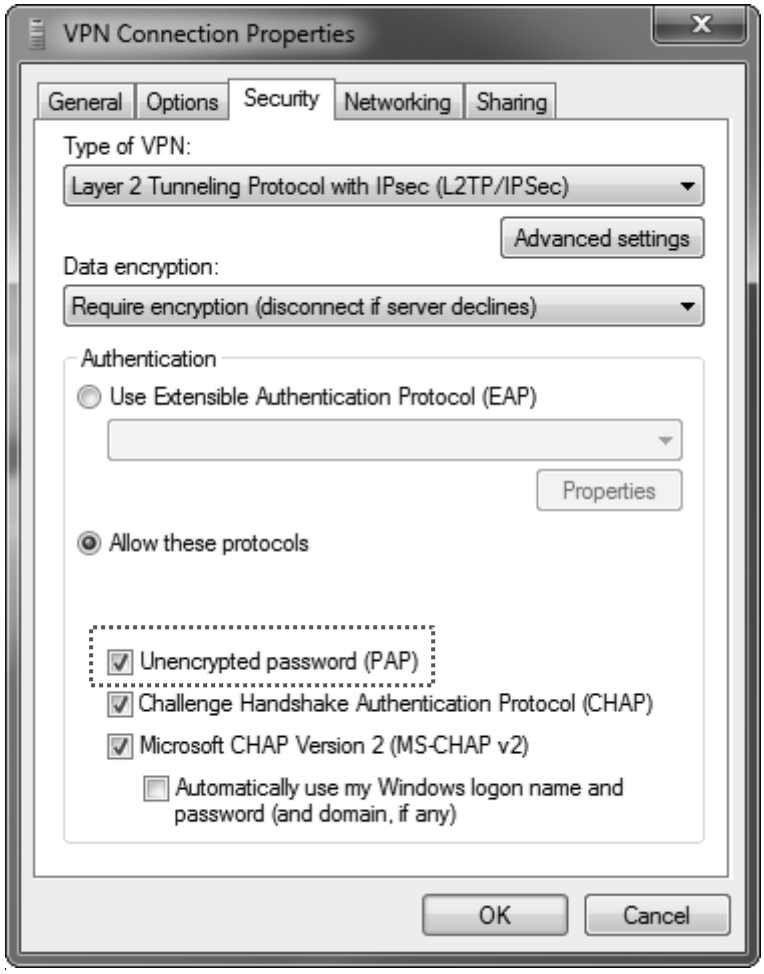


(3) Click **Use preshared key for authentication**, and set the **Key** to **87654321**.

(4) Click **OK.**

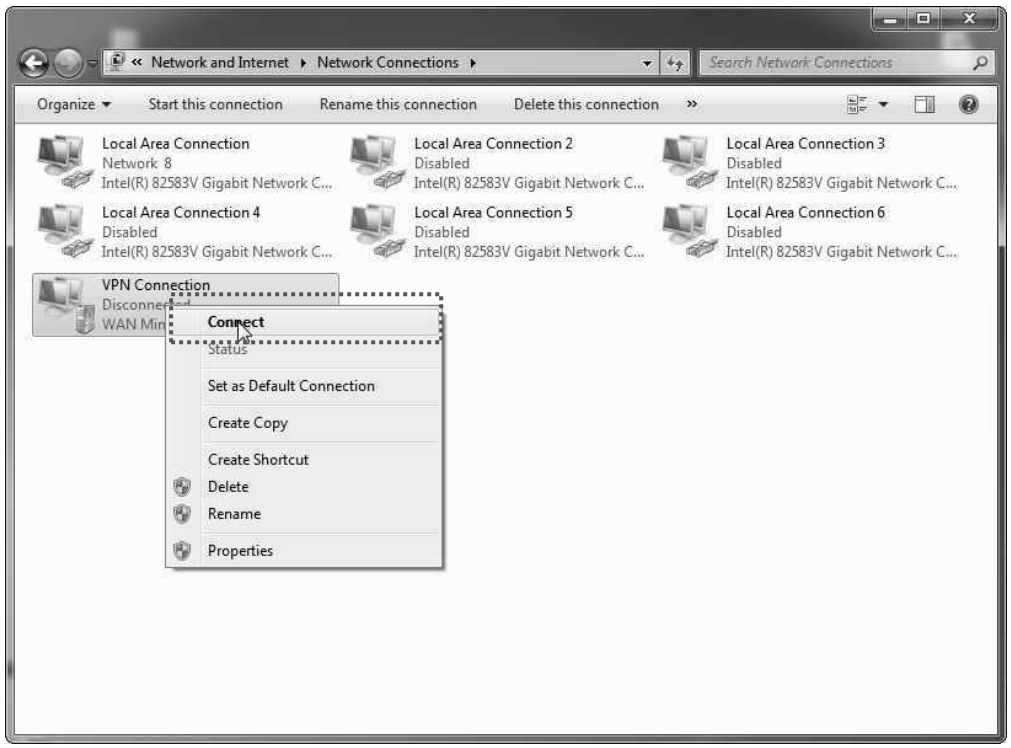


(5) It redirects to the properties page of VPN Connection, tick **Unencrypted password (PAP)**, and then click **OK.**

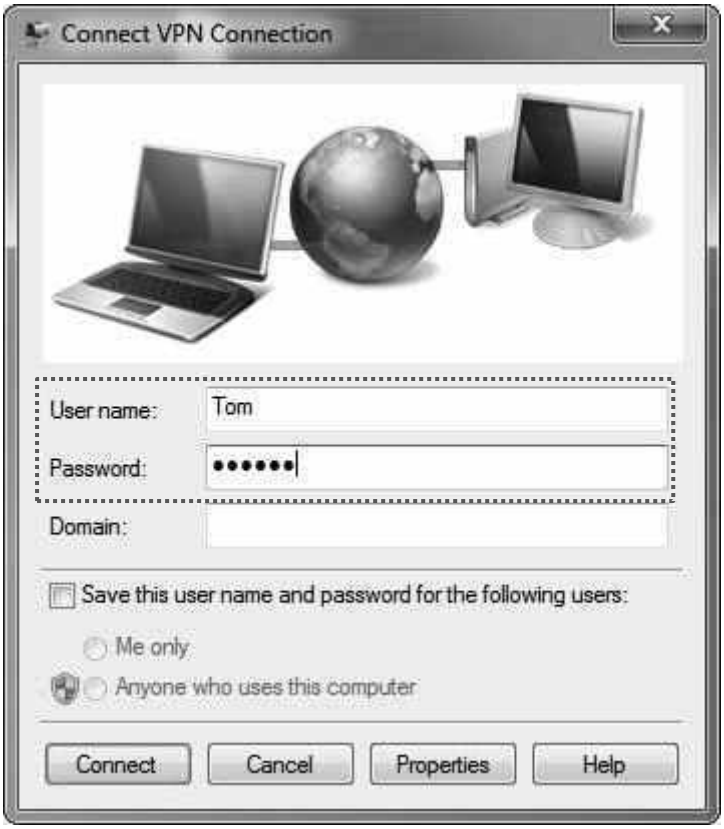


3. Set VPN connection parameters.

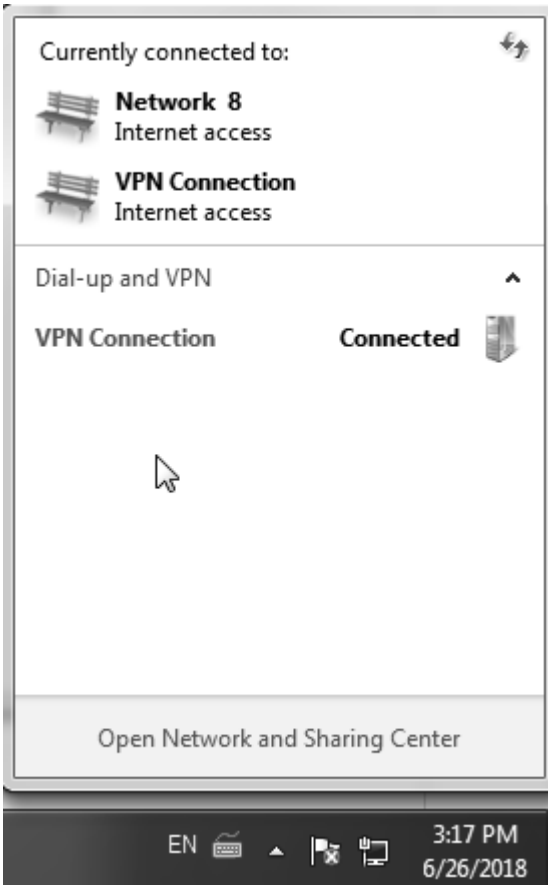
(1) Go to **Network and Sharing Center** page, right click **VPN Connection**, and click **Connect**.



(2) Enter **username** to **Tom**, **password** to **Tom123**, and click **Connect.**

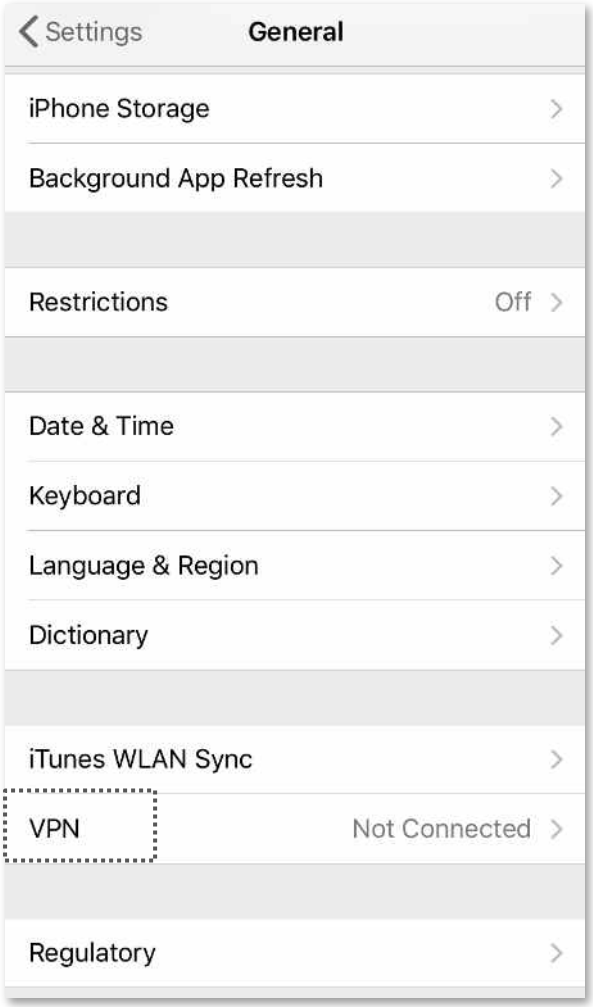


Wait for a moment to establish a connection.

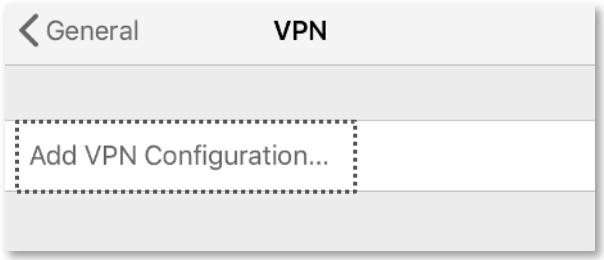


Scenario 2: Create VPN connection on a mobile device, here takes IOS as an example.

1. Click  on the **Settings** page.
2. Click **VPN.**



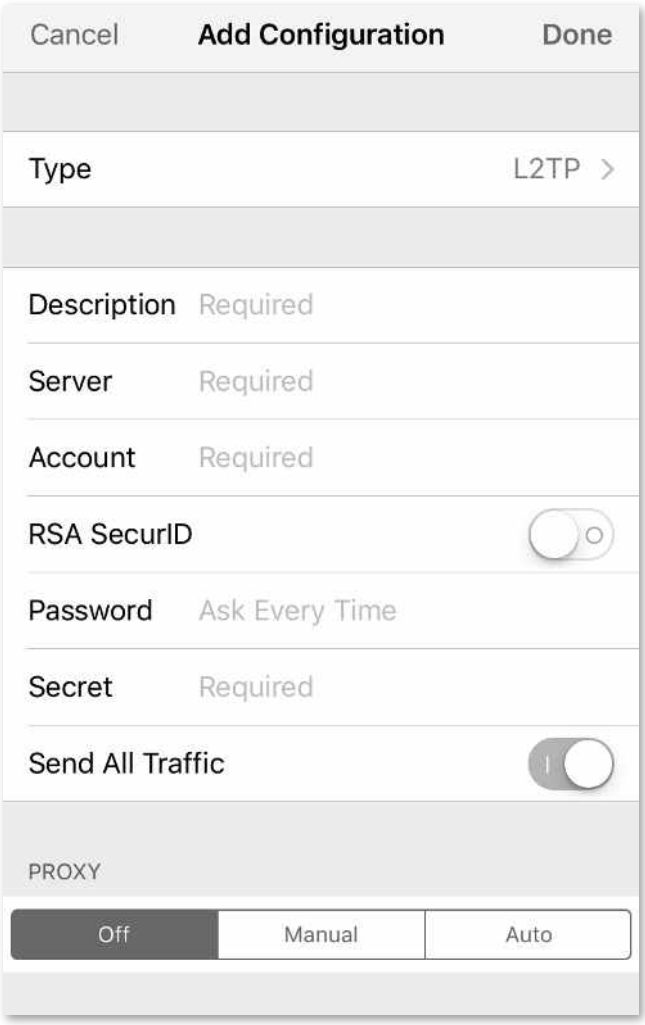
3. Click **Add VPN Configuration.**



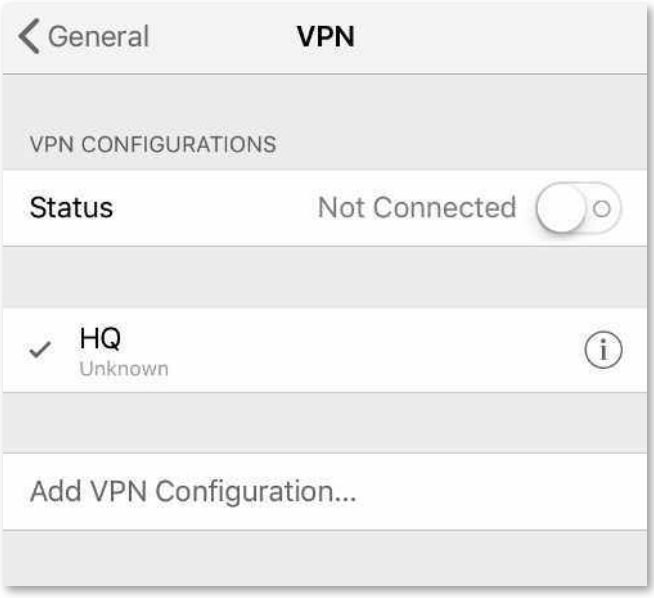
4. Set required parameters.
   (1) Set **Type** to **L2TP.**
   (2) Set **Description** to the name of the VPN connection, which is **HQ** in this example.
   (3) Set **Server** to the IP address of L2TP server, which is **192.168.20.62** in this example.
   (4) Set **Username** to the user name used to connect the VPN client to the VPN server, which is **Tom** in this example.
   (5) Set **Password** to the password for the user name, which is **Tom123** in this example.

(6) Set **Secret** to the **Pre-shared Key** set in IPsec connection, which is **87654321** in this example.

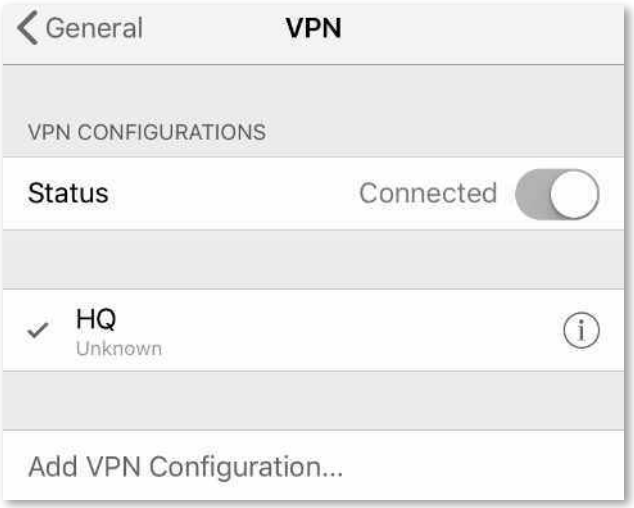
(7) Click **Done.**



5. Click .



Wait for a moment. When the status turns , it indicates a successful connection.



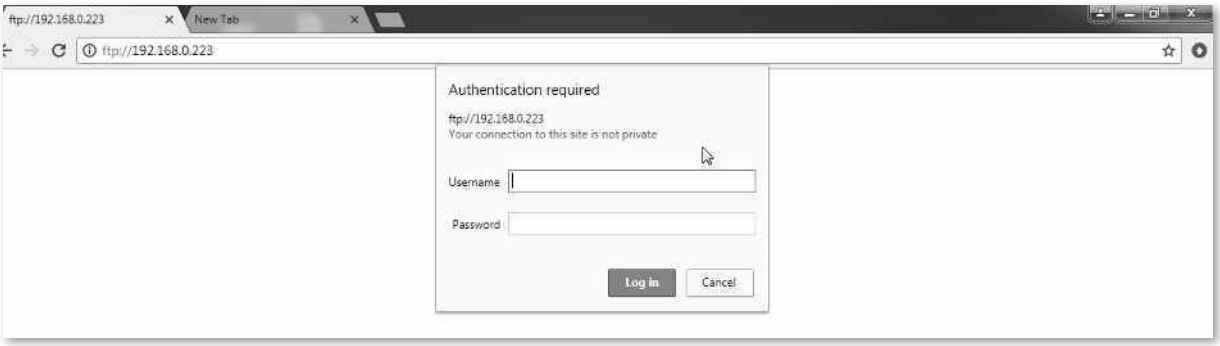
Accessing HQ data for employees on business trip

Here takes accessing web server of HQ as an example. The project data of the HQ is stored on the FTP server. Assume that the server information is as follows:

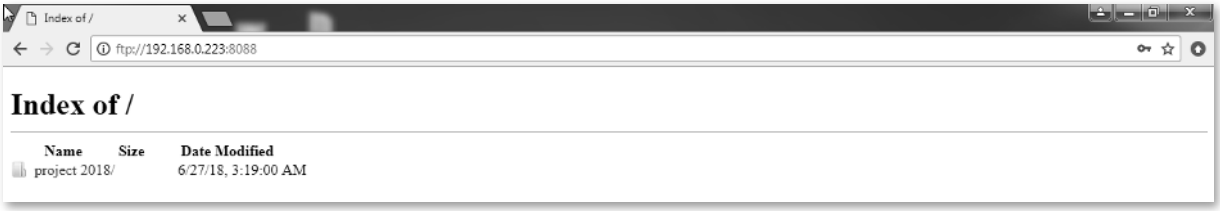
- FTP server IP address: 192.168.0.223
- Server port: 8080

Access procedure:

Open a web browser, access the website ftp://192.168.0.223:8080.



The following figure shows the successful access.



Note

To access the FTP server on a mobile device (smartphone, tablet, etc.), the mobile device needs to install an FTP client.

8 Security

This chapter describes:

8.1 Overview

The Security module of M80 allows you to bind IP addresses with MAC addresses and implement attack protection.

- **IP-MAC binding**

You can use this function to bind IP addresses with MAC addresses for the computers on your LAN. After this function is enabled, only the computers on the Binding List can access the internet. This can effectively prevents unauthorized usage of LAN IP addresses, improving the network security.

M80 supports both manual and dynamic binding modes, which are described as follows:

- **Manual binding**: In this mode, you need to create a binding list. Therefore, the administrator needs to know the MAC addresses of all the computers in your LAN and mapping between the IP addresses and MAC addresses of the computers.
- **Dynamic binding**: In this mode, **Dynamic Binding** on the **Security** > **IP-MAC Binding** page displays the mapping between the IP address and MAC address of a computer after the computer connects to the router. You only need to click **Bind** corresponding to the mapping on the page to bind the IP address with the MAC address.

- **Firewall**

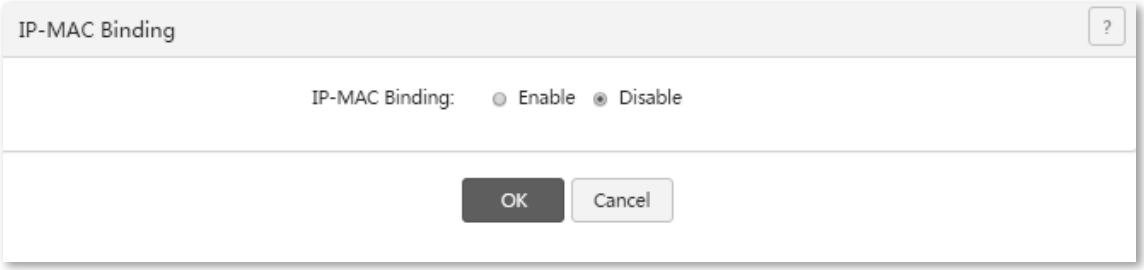
M80 can implement ARP attack defense, DDoS attack defense, IP attack defense, and block WAN pinging, which are described as follows:

- ARP attack defense: This function protects against ARP spoofing and ARP broadcast.
- DDoS attack defense: This function protects against various DDoS attacks, including ICMP flood, UDP flood, and SYN flood attacks, which are used to consume resources of a target system to disable the system to properly provide services.
- IP attack defense: This function blocks the data packets with special IP options as configured. The IP options include the IP timestamp option, IP security option, IP stream option, IP record route option, IP loose source route option, and invalid IP option.
- Block WAN pinging: This function enables the router to ignore ping requests when a computer on a WAN pings the WAN port IP address of the router, so as to prevent exposing the router and protect against ping attacks.

After an attack defense function is enabled, the router logs the attack time, attack type, attack count, and attacker IP address and MAC address on the **System** > **Defense Logs** page when an attack corresponding to the defense function is carried out. This log helps you maintain network security.

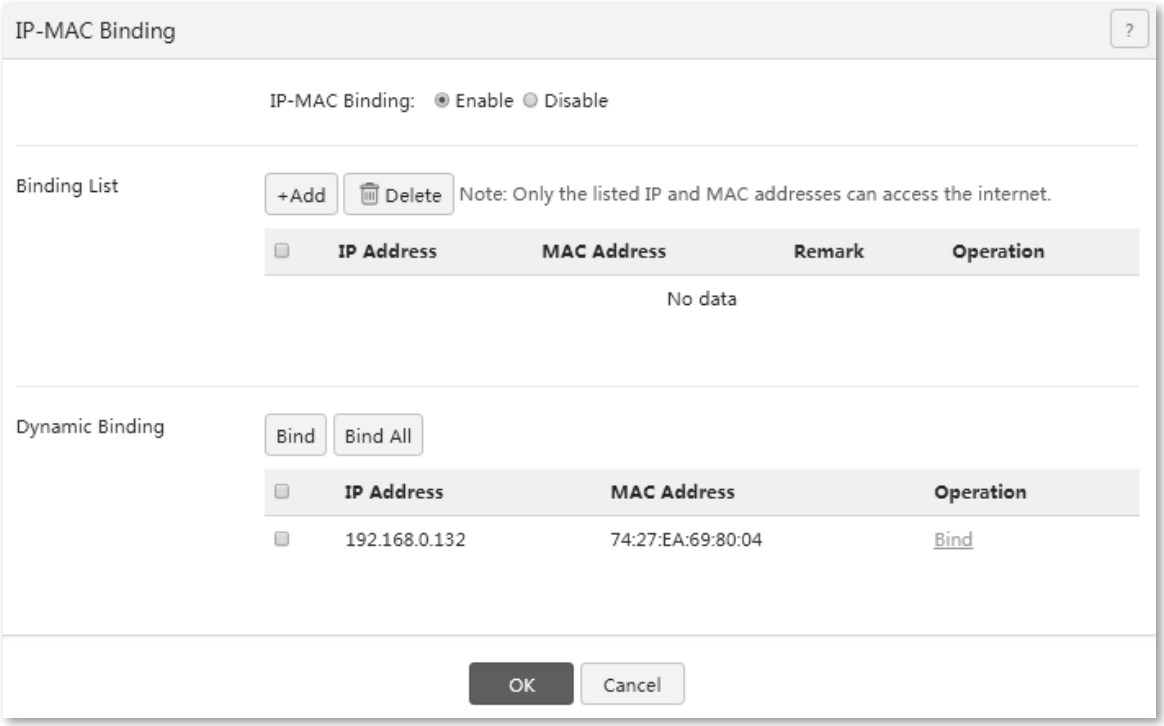
8.2 Binding an IP address with a MAC address

To access the page for binding an IP address with a MAC address, choose **Security** > **IP-MAC Binding**. See the following figure.



8.2.1 Enabling the IP-MAC binding function

1. Click **Security** > **IP-MAC Binding**.
2. Set **IP-MAC Binding** to **Enable**.
3. Click **OK**.



---End

Parameter description

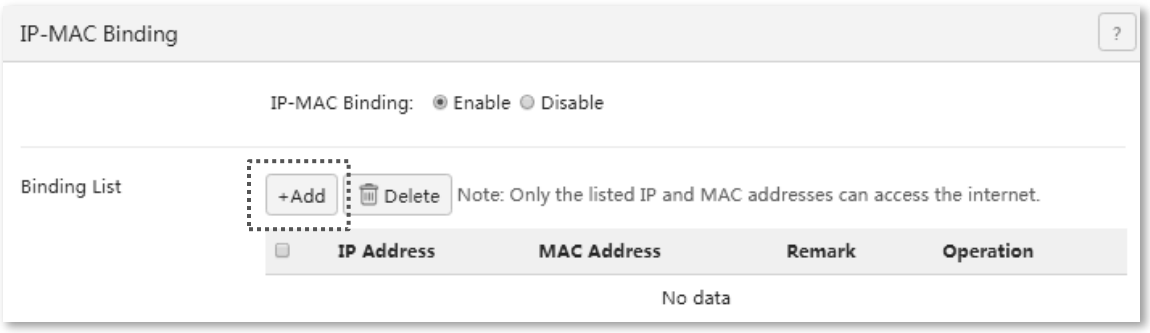
Parameter		Description
IP-MAC Binding		It specifies whether to enable the IP-MAC binding function. The default option is **Disable**. After the function is enabled, only the computers listed on the **Binding List** can access the internet.
Binding List	+Add	It is used to manually bind IP addresses and MAC addresses.
	Delete	It is used to delete IP addresses from MAC addresses.
	IP Address	**IP Address** specifies the IP addresses bound with MAC addresses. **MAC Address** specifies the MAC addresses bound with IP addresses.
	MAC Address	
	Remark	It specifies the description of a binding between an IP address and a MAC address. In a binding entry, this parameter is blank if no description is specified when the entry is created.
	Operation	It specifies the operations that can be performed on binding entries. To modify an entry, click corresponding to the entry. To delete an entry, click corresponding to the entry.
Dynamic Binding	Bind	It is used to add a mapping between an IP address and a MAC address to the binding list. Such mappings are displayed on the dynamic binding list after computers on your LAN connect to the router.
	Bind All	It is used to add all the mappings between IP addresses and MAC addresses from the dynamic binding list to the binding list.
	IP Address	**IP Address** specifies the IP addresses of the computers connected to the router. **MAC Address** specifies the MAC addresses of the computers connected to the router.
	MAC Address	
	Operation	Click **Bind** to add this rule to the binding list quickly.

After enabling the IP-MAC binding function, you can configure an IP-MAC binding entry.

8.2.2 Configuring an IP-MAC binding entry

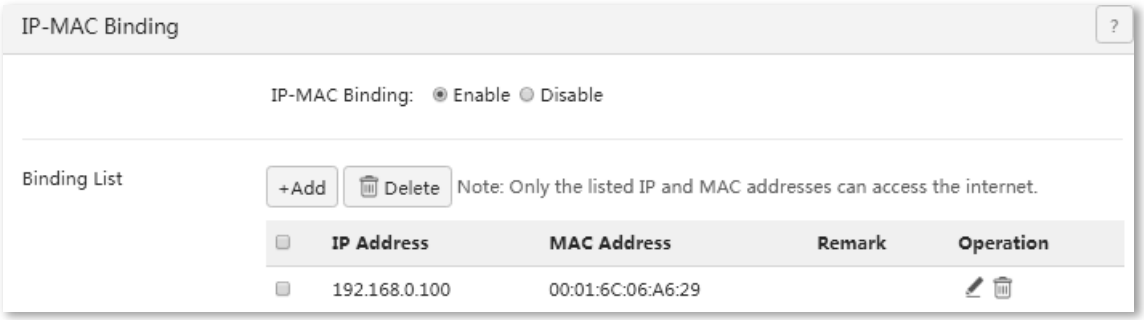
Manually adding an entry

1. Choose **Security** > **IP-MAC Binding**.
2. Click +Add.
3. Set the parameters.



4. Click **OK**.

The **IP-MAC Binding** page appears, showing the added IP-MAC binding entry.



Modifying an entry

1. Choose **Security** > **IP-MAC Binding**.
2. Click corresponding to an entry to be modify.
3. Modify the entry.

Deleting an entry

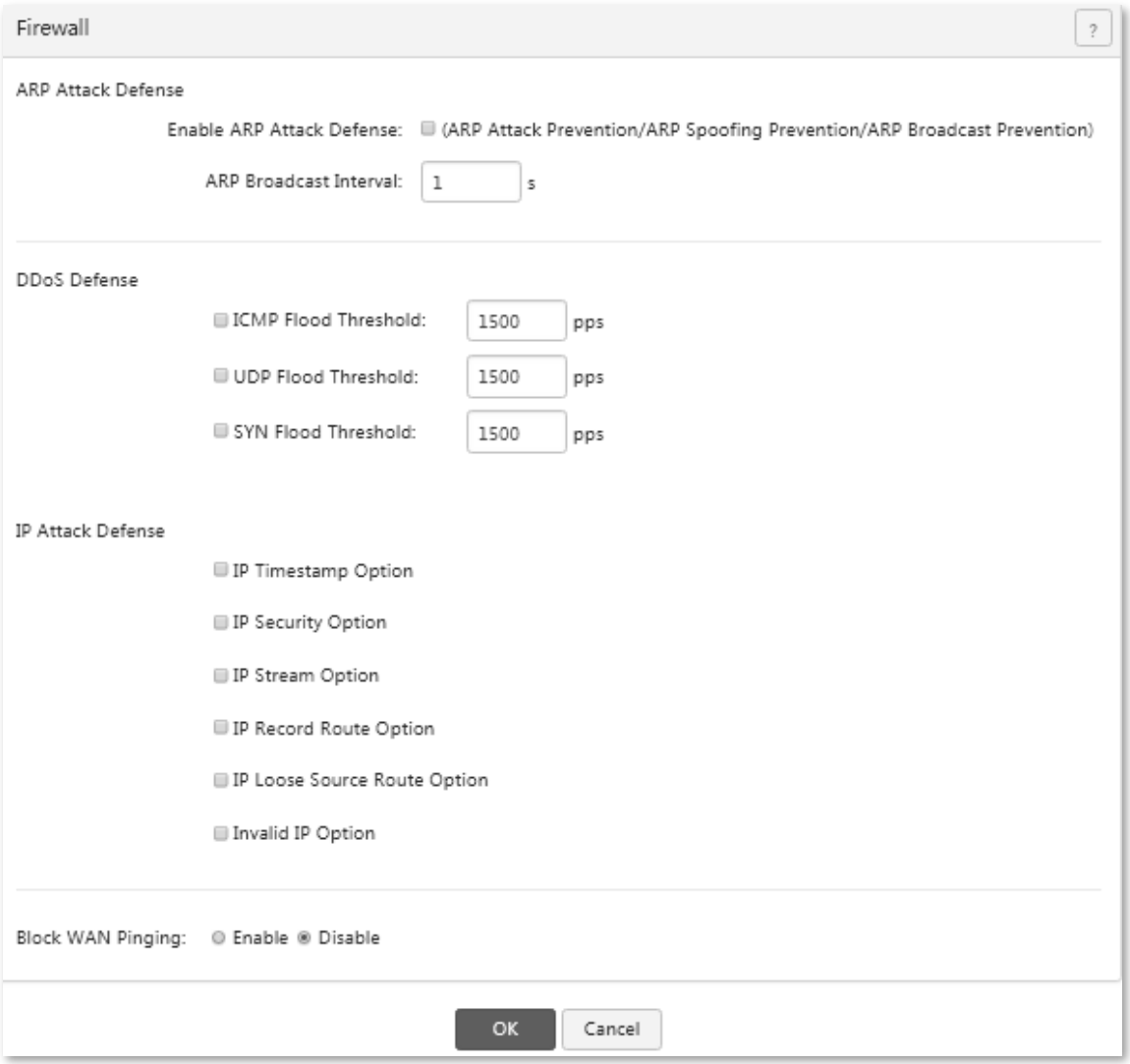
1. Choose **Security** > **IP-MAC Binding**.
2. Click corresponding to an entry to be deleted. To delete multiple entries at the same time, select the entries and click Unbind.

Automatically adding an entry

1. Choose **Security** > **IP-MAC Binding**.
2. Add entries in the dynamic binding list to the binding list.

8.3 Protecting against attacks

To access the page for protecting against attacks, choose **Security** > **Firewall**. See the following figure.



After enabling attack protection, you can view attack information on the **System** > **Defense Logs** page.

Note

Some data packets detected by the attack protection functions, such as some data packets used for network tests, are not attack packets. Therefore, enable the functions only when necessary.

Parameter description

Parameter		Description
ARP Attack Defense	Enable ARP Attack Defense	It specifies whether the ARP attack defense function, which protects against ARP attacks, ARP spoofing, and ARP broadcast, is enabled.
	ARP Broadcast Interval	It specifies the interval at which the router sends ARP broadcast packets.
DDoS Defense	ICMP Flood Threshold	It specifies the maximum number of incoming ICMP packets allowed in one second. If the threshold is exceeded, it is inferred that the router is under ICMP Flood attack.
	UDP Flood Threshold	It specifies the maximum number of incoming UDP packets allowed in one second. If the threshold is exceeded, it is inferred that the router is under UDP Flood attack.
	SYN Flood Threshold	It specifies the maximum number of incoming TCP SYN packets allowed in one second. If the threshold is exceeded, it is inferred that the router is under SYN Flood attack.
IP Attack Defense	IP Timestamp Option	It enables the router to block IP packets with the internet Timestamp option.
	IP Security Option	It enables the router to block IP packets with the Security option.
	IP Stream Option	It enables the router to block IP packets with the Stream ID option.
	IP Record Route Option	It enables the router to block IP packets with the Record Route option.
	IP Loose Source Route Option	It enables the router to block IP packets with the Loose Source Route option.
	Invalid IP Option	It enables the router to block IP packets with integrity or correctness problems.
Block WAN Pinging		It specifies whether to enable the WAN ping attack defense function. The default option is **Disable**. After this function is enabled, devices on a WAN cannot ping the IP address of the WAN port of the router.

9 AC management

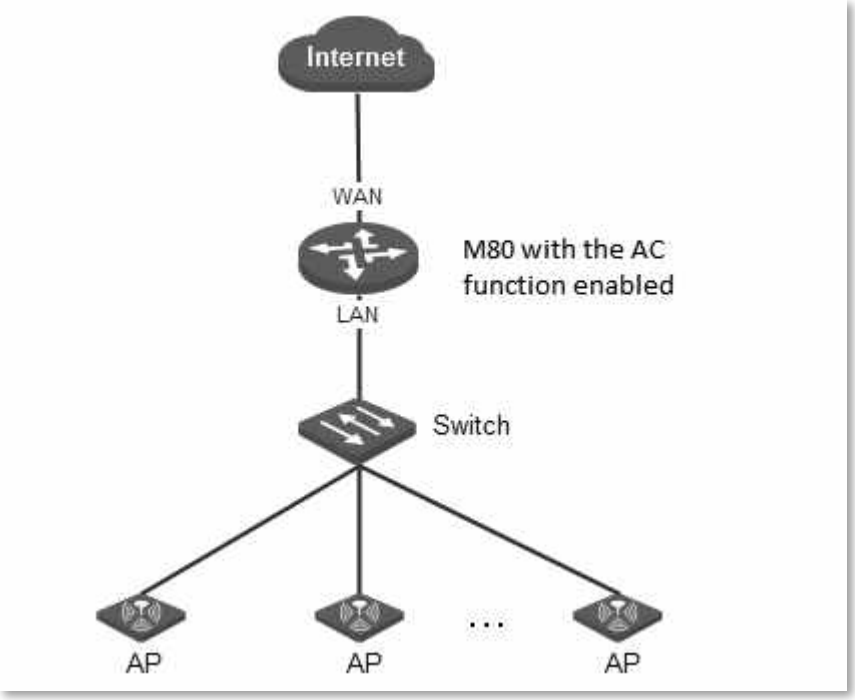
This chapter describes:

- Configuring wireless settings
- Configuring advanced settings
- Managing APs
- Viewing user status

9.1 Overview

M80 can work as an AC to manage IP-COM APs. When VLAN is disabled on M80, only LAN0 supports WiFi via WeChat function. If this function is needed, connect the switch which is connected to the AP to LAN0 of M80.

The following figure shows the network topology where M80 functions as an AC to manage APs.

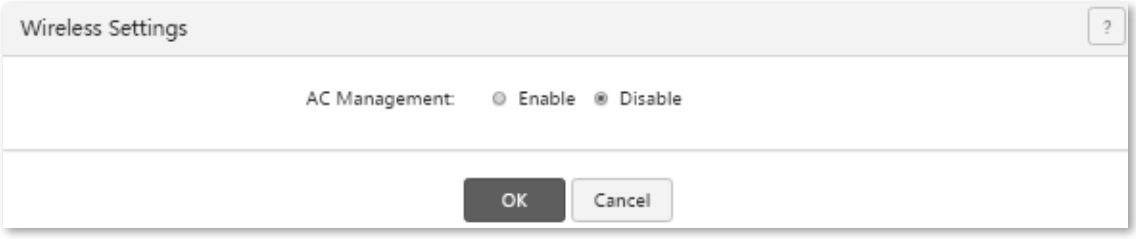


The AC management function of M80 allows you to configure wireless settings, advanced settings, manage APs and view user status.

- Wireless Settings: This module allows you to enable or disable the AC management function of the router and configure SSID-related parameters for the APs on your LAN in a centralized manner. The parameters allow you to specify SSIDs, SSID status, frequencies, maximum number of users, VLAN IDs, authentication types, and passwords, specify whether to hide specific SSIDs, and so on.
- Advanced Settings: This module allows you to configure RF settings and global settings for all the APs on you LAN after the AC management function is enabled.
- AP Management: This module allows you to view information about APs on your LAN after the AC management function is enabled. It also allows you to export, reboot, upgrade, reset, delete, and refresh APs in batches.
- User Status: This module allows you to view, after the AC management function is enabled, information about users connected to the APs managed by the router.

9.2 Configuring wireless settings

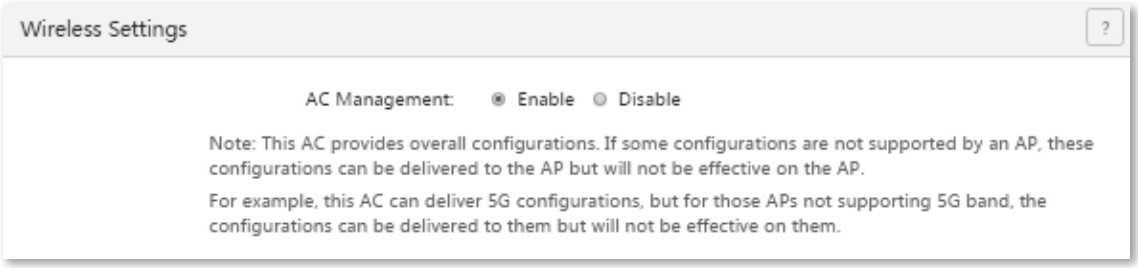
To access the page for configuring wireless settings, choose **AC Management** > **Wireless Settings**. See the following figure.



9.2.1 Enabling the AC management function

1. Choose **AC Management** > **Wireless Settings**.
2. Set **AC Management** to **Enable**.

Then, you can manage all the APs on your LAN in a centralized manner. To view the APs being managed by the router, choose **AC Management** > **AP Management**.



Note

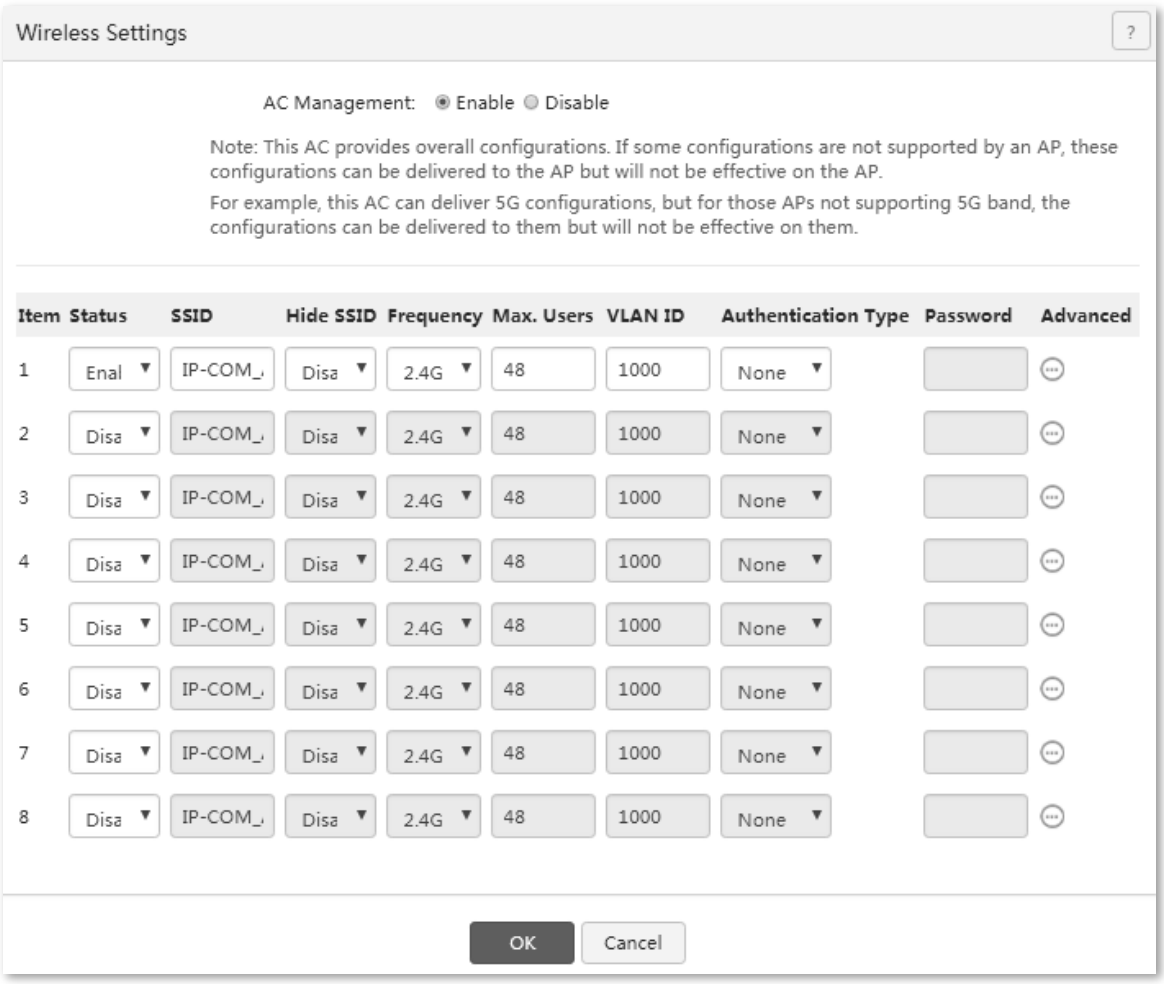
You can use the functions of the AC management module only after setting **AC Management** to **Enable**.

9.2.2 Delivering wireless network policies to APs

1. Choose **AC Management** > **Wireless Settings**.
2. Configure SSID-related policies for APs managed by the router.
3. Click **OK**.

Note

The AC management function allows you to set various AP parameters. Some parameters not supported by APs can be delivered but do not take effect. For example, if you use the AC management function to deliver the 5 GHz frequency parameter to APs that do not support the 5 GHz frequency, the parameter can be delivered successfully to the APs but the APs are not switched to the 5 GHz frequency.



Parameter description

Parameter	Description
Item	It specifies the serial number of a wireless network policy. SNs 1 to 4 correspond to SSIDs 1 to 4 for the 2.4 GHz or 5 GHz frequency respectively, while SNs 5 to 8 correspond to SSIDs 5 to 8 for the 2.4 GHz frequency respectively. The first 4 policies can contain SSID-related parameters applicable to the 2.4 GHz or 5 GHz frequency or both of them. The last 4 policies can contain only the SSID-related parameters applicable to the 2.4 GHz frequency.
Status	It specifies whether a wireless network policy and its corresponding SSID are enabled. By default, wireless network policy 1 is enabled and the other wireless network policies are disabled. Note Disabling wireless network policy 1 may disable the wireless network function of APs. Therefore, it is recommended that you leave wireless network policy 1 enabled. If you disable wireless network policy 1 and then enable it again, the wireless network function of APs may not be enabled as well. In that case, you can enable it on the **AC Management** > **Advanced Settings** page.
SSID	It specifies the SSID for a wireless network policy.
Hide SSID	It specifies whether to hide an SSID. The options include: – **Enable**: It indicates that APs do not broadcast the corresponding SSID and the SSID is not listed among available networks of a user device. To connect a user device to the wireless network with the SSID, enter the SSID manually on the user device. – **Disable**: It indicates that APs broadcast the corresponding SSID and the SSID can be detected by

Parameter	Description
	user devices near the APs.
Frequency	It specifies the operating frequency corresponding to an SSID. – **2.4G**: It indicates that a wireless network policy for the 2.4 GHz frequency is delivered to APs. – **5G**: It indicates that a wireless network policy for the 5 GHz frequency is delivered to APs. – **2.4G&5G**: It indicates that a wireless network policy for both the 2.4 GHz and 5 GHz frequencies is delivered to APs. Note After you configure wireless network policy 1 only for either frequency (2.4 GHz or 5 GHz) and click **OK**, the APs disable the wireless network function for the other frequency. You can enable the function on the **AC Management** > **Advanced Settings** page.
Max. Users	It specifies the maximum number of user devices that can connect concurrently to a wireless network with a specific SSID. By default, 48 user devices are allowed.
VLAN ID	It specifies the ID of the 802.1Q VLAN with a specific SSID. The default VLAN ID is **1000**. If the Q VLAN function of APs is required, set **VLAN** in the global settings on the **AC Management** > **Advanced Settings** page to **Enable**.
Authentication Type	It specifies the authentication type of the wireless network with a specified SSID. The options include: – **None**: It indicates that the wireless network is not encrypted and is accessible to any user devices. This option is not recommended because of network security concern. – **WPA-PSK**: It indicates that WPA-PSK authentication and AES encryption are applied to the wireless network. – **WPA2-PSK**: It indicates that WPA2-PSK authentication and AES encryption are applied to the wireless network.
Password	It specifies a pre-shared WPA-PSK or WPA2-PSK password for authenticating a user device when the user device connects to a WPA-PSK- or WPA2-PSK-protected wireless network.
Advanced	It allows you to specify whether to enable the client isolation function. The options include: – **Enable**: It indicates that wireless clients connected using the same SSID cannot communicate with each other. – **Disable**: It indicates that wireless clients connected using the same SSID can communicate with each other.

9.3 Configuring advanced settings

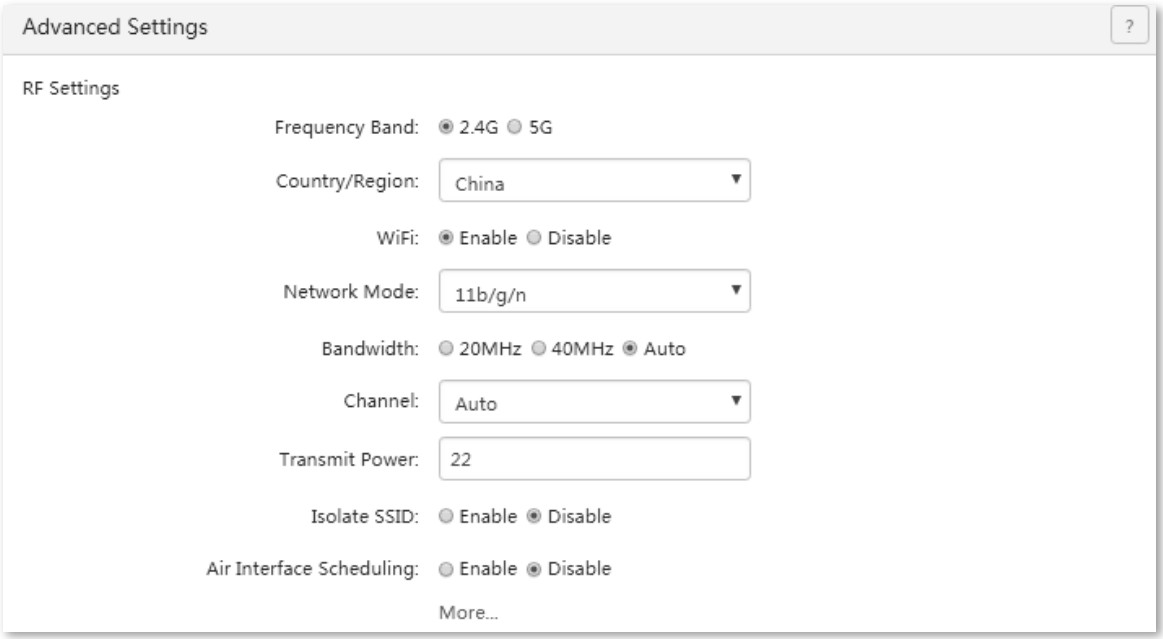
To access the page for configuring advanced settings, choose **AC Management** > **Advanced Settings**. The page includes RF settings and global settings for APs.

Note

When you click **OK** on the page, the settings configured on the page are delivered to APs.

9.3.1 Configuring RF settings

1. Choose **AC Management** > **Advanced Settings**.
2. Set RF parameters for APs, such as frequency, WiFi status, and channel parameters, in the **RF Settings** area.

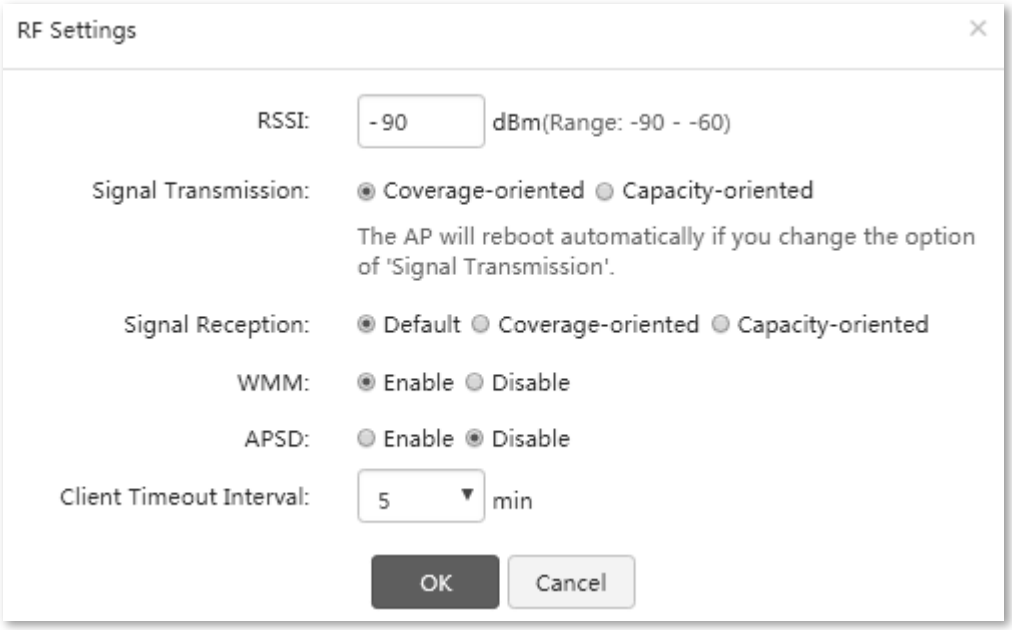


Parameter description

Parameter	Description
Frequency Band	It specifies the intended AP operating frequency of the parameters, 2.4G or 5G. Note The settings are delivered to all APs, including 2.4G and 5G.
Country/Region	It specifies the country/region where the router is used.
WiFi	It specifies whether to enable the wireless network for the specified frequency.
Network Mode	It specifies the wireless network mode of APs. For 2.4 GHz, the 11b, 11g, 11b/g, and 11b/g/n modes are available. For 5 GHz, the 11a, 11ac, and 11a/n modes are available. The modes are described as follows:

Parameter	Description
	– **11b**: In this mode, only 802.11b clients can connect to the APs. – **11g**: In this mode, only 802.11g clients can connect to the APs. – **11b/g**: In this mode, only 802.11b and 802.11g clients can connect to the APs. – **11b/g/n**: In this mode, only 802.11b, 802.11g, and 802.11n clients working at the 2.4 GHz frequency can connect to the APs. – **11a**: In this mode, only 802.11a clients can connect to the APs. – **11ac**: In this mode, only 802.11ac clients can connect to the APs. – **11a/n**: In this mode, only 802.11a and 802.11n clients working at the 5 GHz frequency can connect to the APs.
Bandwidth	It specifies the bandwidth of a wireless network. The options include: – **20MHz**: It indicates that APs can use only the 20 MHz bandwidth. – **40MHz**: It indicates that APs try using the 40 MHz bandwidth first, and switch to the 20 MHz bandwidth under poor bandwidth conditions. – **80MHz** (available only for 5 GHz networks): It indicates that APs switch among the 20 MHz, 40 MHz, and 80 MHz bandwidths based on the ambient environment. – **Auto** (available only for 2.4 GHz networks): It indicates that APs switch between the 20 MHz and 40 MHz bandwidths based on the ambient environment.
Channel	It specifies the operating channel of a wireless network. The available options depend on the settings of **Country** and **Frequency (2.4 G or 5 G)**.
Transmit Power	It specifies the transmit power of an AP. If a transmit power value not supported by an AP is delivered to the AP, a boundary value within the value range supported by the AP takes effect instead of the delivered value. That is, if the value delivered to an AP is greater than the upper limit of the value range of the AP, the maximum value supported by the AP takes effect; if the delivered value is less than the lower limit of the value range, the latter takes effect.
Isolate SSID	It specifies whether to enable the SSID isolation function. If it is enabled, AP clients connected to networks at a specified frequency with different SSIDs cannot communicate with each other.
Air Interface Scheduling	It specifies whether to enable the air interface scheduling function. This function allows all clients to transmit data for the same duration. If a client transmits data at a low speed and does not finish data transmission within the duration, it can continue transmitting data only in its next data transmission duration. This prevents some slow clients from occupying excessive airtime resources, so as to improve the overall AP efficiency and effectively ensure AP connections for a larger number of clients and greater throughputs.
More...	It allows you to access advanced RF parameters. For details about the parameters, see the parameter description in the following table.

3. Click More... in the **RF Settings** area.
   The **RF Settings** dialog box appears.



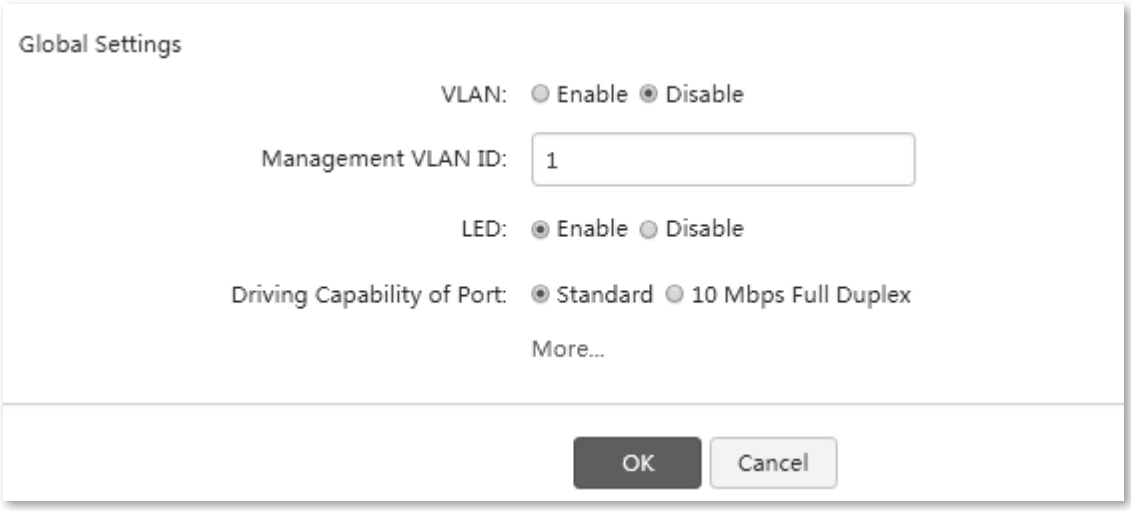
4. Set the parameters, and click **OK**.
   The settings are delivered to APs.

Parameter description

Parameter	Description
RSSI	It specifies the minimum wireless client signal strength acceptable to an AP. A mobile client with signal strength lower than this threshold cannot connect to the AP. You can set this parameter to ensure that mobile clients connect to APs with strong signal strength.
Signal Transmission	It specifies whether the router is suitable for the wide coverage or high density scenario. This parameter is valid only for 2.4 GHz networks. Set this parameter based on the application scenario of the router. The options include: **Coverage-oriented**: This option is used in places with low AP density, such as offices, warehouses, and hospitals, to increase AP coverage. **Capacity-oriented**: This option is used in places with high AP density, such as conference venues, exhibition halls, banquet halls, stadiums, college classrooms, and departure lounges, to reduce mutual interference among APs.
Signal Reception	It specifies the deployment mode of the router. This parameter is valid only for 2.4 GHz networks. Set this parameter based on the application scenario. The options include: **Capacity-oriented**: This option is used in scenarios with high AP density to ensure that clients connect to APs with strong signals. **Coverage-oriented**: This option is used in scenarios with low AP density to better enable clients to connect to APs. **Default**: This option is used to achieve performance between high density and wide coverage.
WMM	It specifies whether to enable the wireless multimedia function. After this function is enabled, audio and video data is forwarded with top priority, so as to enable APs to better transmit multimedia data (such as online video data).
APSD	It specifies whether to enable the Automatic Power Save Delivery (APSD) mode. APSD is a WMM power saving protocol created by Wi-Fi Alliance. Enabling APSD helps reduce power consumption by APs. By default, this mode is disabled.
Client Timeout Interval	It specifies the maximum period before a WiFi client is disconnected from an AP if the client exchanges no data with the AP. When data is exchanged within the period, countdown stops.

9.3.2 Configuring global settings

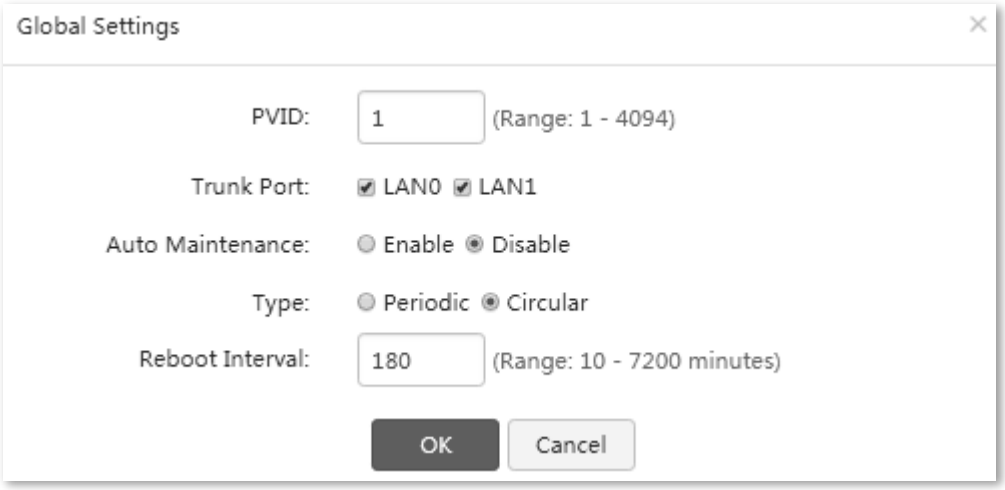
1. Choose **AC Management** > **Advanced Settings**.
2. Set global AP parameters, such as VLAN status, management VLAN ID, LED indicator status, and driving capability of port, in the **Global Settings** area.



Parameter description

Parameter	Description
VLAN	It specifies whether to enable the Q VLAN function of APs. After the function is enabled, the value of **Management VLAN ID** set on the current page and the values of **VLAN ID** set on the **AC Management** > **Wireless Settings** take effect. By default, this function is disabled.
Management VLAN ID	It specifies the management VLAN ID of APs. The default value is **1**. If a new management VLAN ID is delivered to the APs, the router or management computer can manage the APs only after connecting to the new management VLAN network.
LED	It specifies whether to enable or disable the LED indicator function of APs. The options include: – **Enable**: It indicates that the LED indicator functions of APs are enabled. You can check AP operating status based on the LED indicators of the APs. By default, this function is enabled. – **Disable**: It indicates that the LED indicator function of APs is disabled.
Driving Capability of Port	It specifies the transmission mode of Ethernet ports of APs. The options include: – **Standard**: This option is recommended for a scenario that involves a short transmission distance and requires a high transmission speed. – **10 Mbps Full Duplex**: This option is recommended for a scenario that involves a long transmission distance and it results in a low transmission speed. Use the **10 Mbps Full Duplex** option only if the Ethernet cable connecting a peer device to the Ethernet port of an AP is longer than 100 m. If this option is used, ensure that the connected port of the peer device works in auto-negotiation mode. Otherwise, the Ethernet port of the AP may not send or receive data properly.
More...	It allows you to set advanced global parameters. For details about the parameters, see the parameter description in the following table.

3. Click More... in the **Global Settings** area.
   The **Global Settings** dialog box appears.



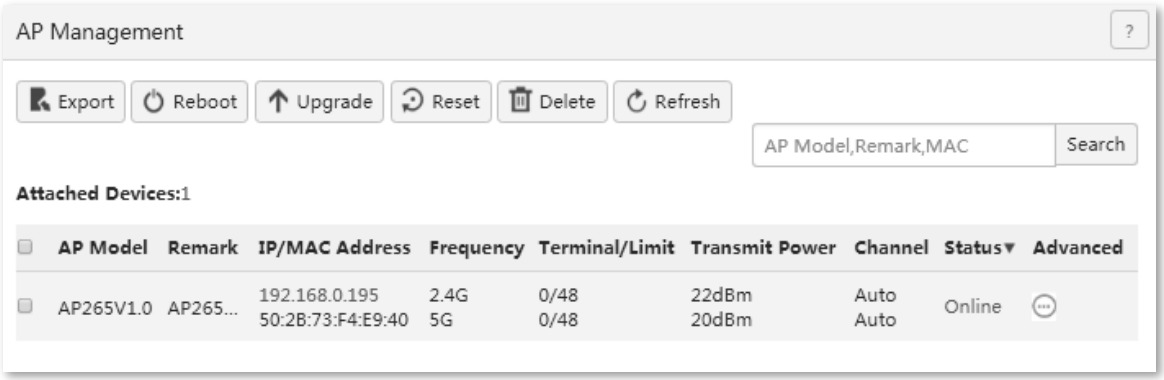
4. Set the parameters and click **OK**.
   The settings are delivered to APs.

Parameter description

Parameter	Description
PVID	It specifies the native VLAN ID of the Trunk ports of APs. This parameter is effective to an AP only after the VLAN function of the AP is enabled.
Trunk Port	It specifies the wired LAN ports used as the Trunk ports of APs. All VLANs can use the Trunk ports to transmit data. Note When enabling the 802.1Q VLAN function, set one or more LAN ports as Trunk ports. If an AP has only one LAN port, set LAN0 as the Trunk port. Otherwise, the configuration may not take effect.
Auto Maintenance	It specifies whether to enable the automatic maintenance function of APs. If the function is enabled, you need to set parameters such as **Type** and **Maintenance Time**/**Reboot Interval**. By default, this function is disabled. Note This function helps prevent degradation of wireless performance or instability of APs that have been working for a long time. During maintenance of an AP, the AP is restarted, resulting in wireless disconnection. Therefore, it is recommended that you set the maintenance time to a time when the wireless traffic is light.
Type	It specifies the type of automatic AP maintenance. The options include: – **Periodic**: It indicates that automatic maintenance is performed at specified times on specified dates. – **Circular**: It indicates that automatic maintenance is performed at an interval.
Maintenance Time	It specifies the time when automatic maintenance is performed.
Reboot Interval	It specifies the interval for circular maintenance.

9.4 Managing APs

To access the page for managing APs, choose **AC Management** > **AP Management**. On this page, you can view and export information about APs managed by the router, reboot, reset, or upgrade online APs in batches, delete offline APs in batches, and modify configuration of APs individually.



9.4.1 Exporting information about APs managed by the router

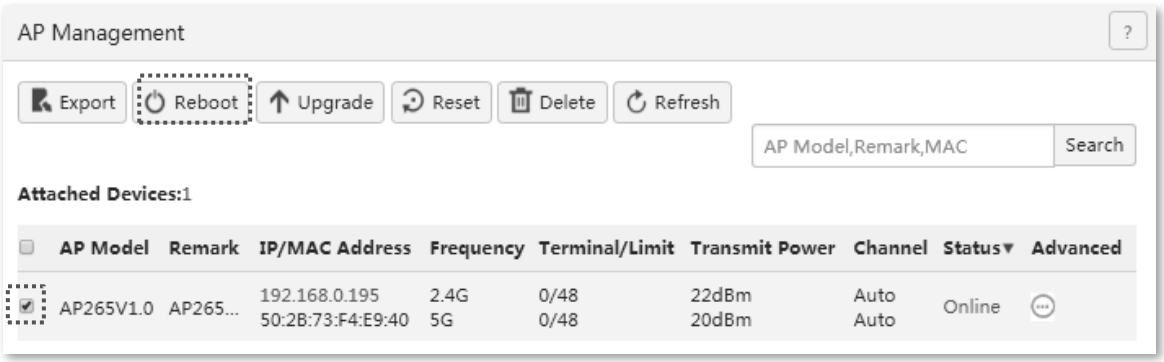
This function enables you to export information about APs managed by the router to an Excel file on your local computer.

1. Choose **AC Management** > **AP Management**.
2. Click **Export** and follow the onscreen instruction to export the information.

9.4.2 Rebooting APs

This function enables you to reboot multiple APs at the same time.

1. Choose **AC Management** > **AP Management** and select the APs to be rebooted.
2. Click **Reboot** and follow the onscreen instruction to reboot the APs.



When the APs are rebooting, they go offline. When rebooting completes, the APs go online automatically. It takes about 1 to 2 minutes to complete this process. You can click **Refresh** to check the status.

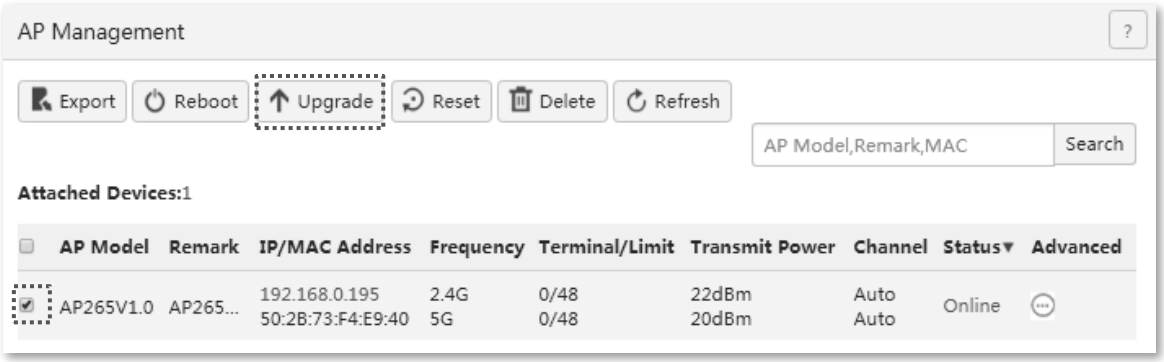
9.4.3 Upgrading APs

This function enables you to upgrade the software of multiple APs at the same time.

Note

When the software of an AP is upgraded, do not turn off the router or AP. Otherwise, the AP may not work properly.

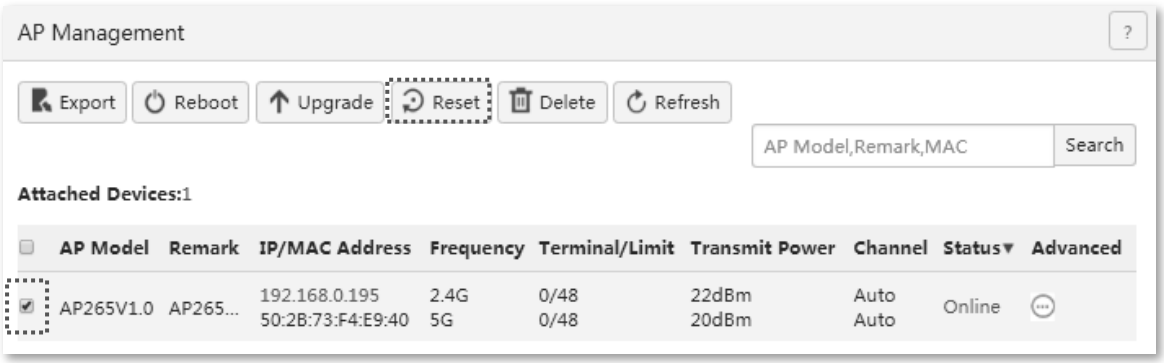
1. Download corresponding AP software from http://www.ip-com.com.cn.
2. Choose **AC Management** > **AP Management** and select the APs to be upgraded.
3. Click **Upgrade** and follow the onscreen instruction to upgrade the APs.



9.4.4 Resetting APs

This function enables you to restore the factory settings of multiple APs at the same time.

1. Choose **AC Management** > **AP Management** and select the APs to be reset.
2. Click **Reset** and follow the onscreen instruction to reset the APs.

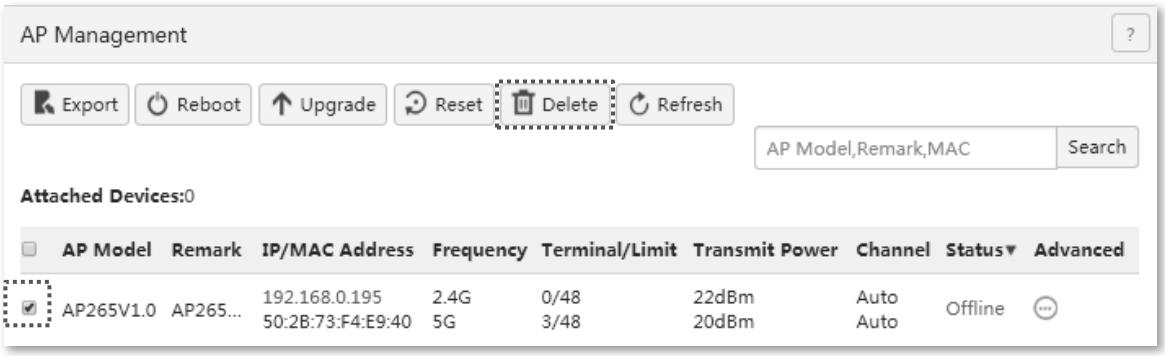


9.4.5 Deleting APs

This function enables you to delete multiple offline APs at the same time.

1. Choose **AC Management** > **AP Management** and select the offline APs to be deleted.

2. Click **Delete** and follow the onscreen instruction to delete the APs.



Note

Online APs cannot be deleted.

9.4.6 Updating AP information

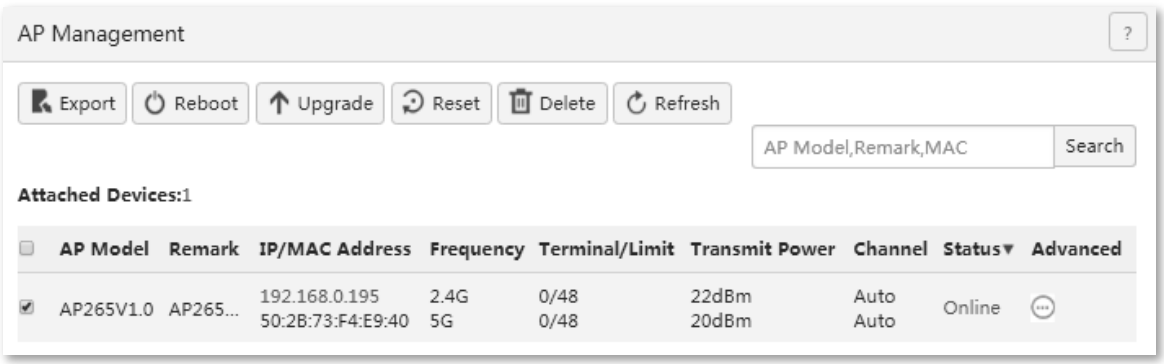
This function enables you to update information about APs.

1. Choose **AC Management** > **AP Management**.
2. Click **Refresh**.

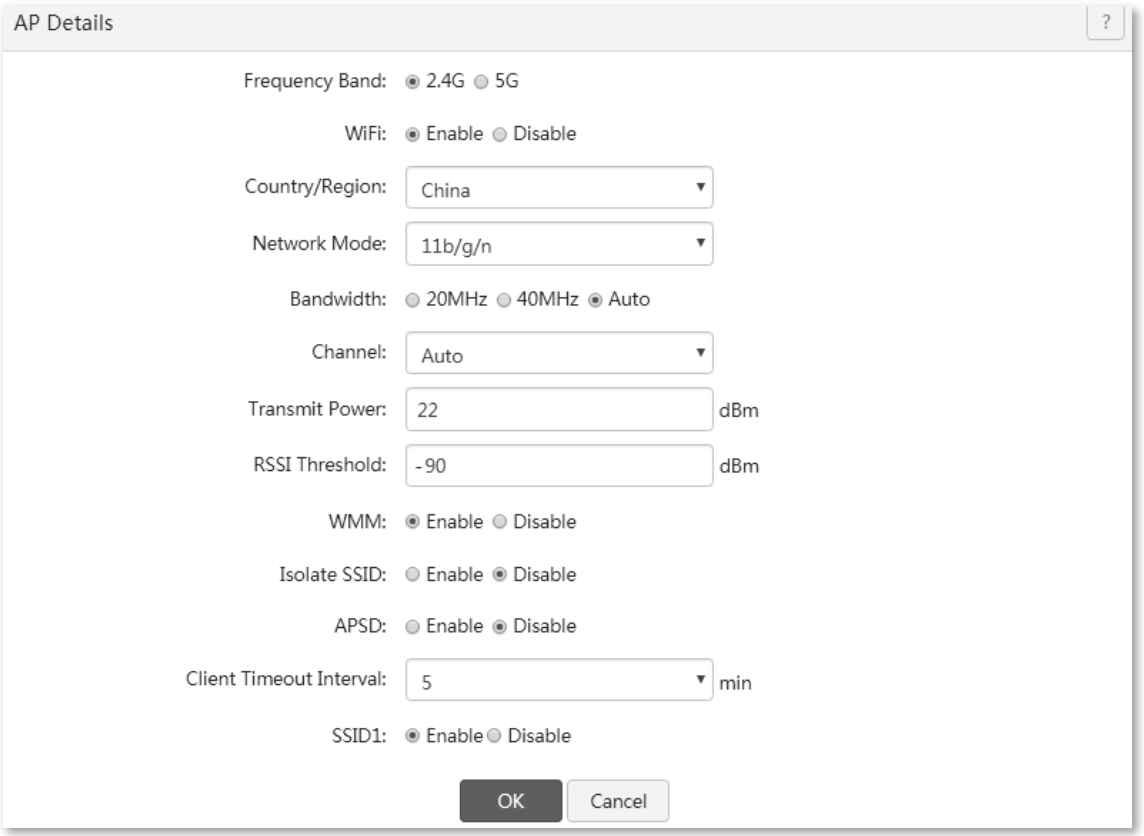
9.4.7 Modifying AP configuration

This function enables you to modify the configuration of an AP, including the remark, wireless network status, country, channel, and transmit power of the AP.

1. Choose **AC Management** > **AP Management**.
2. Select the AP whose configuration is to be modified.
3. Click the corresponding icon.



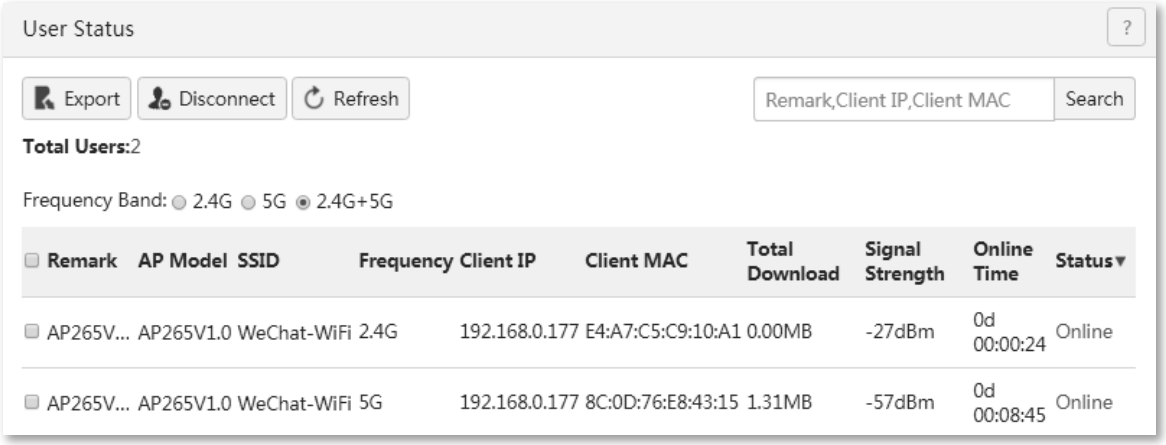
4. Modify the configuration and click **OK**.


AP Details
?
Frequency Band: 2.4G 5G
WiFi: Enable Disable
Country/Region: China
Network Mode: 11b/g/n
Bandwidth: 20MHz 40MHz Auto
Channel: Auto
Transmit Power: 22 dBm
RSSI Threshold: -90 dBm
WMM: Enable Disable
Isolate SSID: Enable Disable
APSD: Enable Disable
Client Timeout Interval: 5 min
SSID1: Enable Disable
OK
Cancel

---End

9.5 Viewing user status

To access the page for viewing user status, choose **AC Management** > **User Status**. On the page, you can view information about users of the APs managed by the router.



Parameter description

Parameter	Description
Frequency Band	It specifies the operating frequency of user devices. The options include **2.4G**, **5G**, and **2.4G+5G**. After an option is selected, the page displays only the user devices operating at the specified frequency or frequencies.
Remark	It specifies the description of APs to which user devices connect.
AP Model	It specifies the models of APs to which user devices connect.
SSID	It specifies SSIDs of networks to which user devices connect.
Frequency	It specifies the operating frequencies of networks to which user devices connect.
Client IP	It specifies the IP addresses assigned to user devices.
Client MAC	It specifies the MAC addresses of user devices.
Total Download	It specifies the total amount of data that user devices download.
Signal Strength	It specifies the radio signal strengths (indicated by RSSI) received by APs from user devices.
Online Time	It specifies the duration of connections to user devices.
Status	It specifies the connection status of user devices.

9.5.1 Exporting user information

1. Choose **AC Management** > **User Status**.
2. Click **Export** and follow the onscreen instruction to export user information.

9.5.2 Disconnecting a user

1. Choose **AC Management** > **User Status**.
2. Select the user to be disconnected.
3. Click **Disconnect**.

To access the network after being disconnected, you need to reconnect to an AP.

9.5.3 Refreshing user information

1. Choose **AC Management** > **User Status**.
2. Click **Refresh.**

10 Captive portal

This chapter describes:

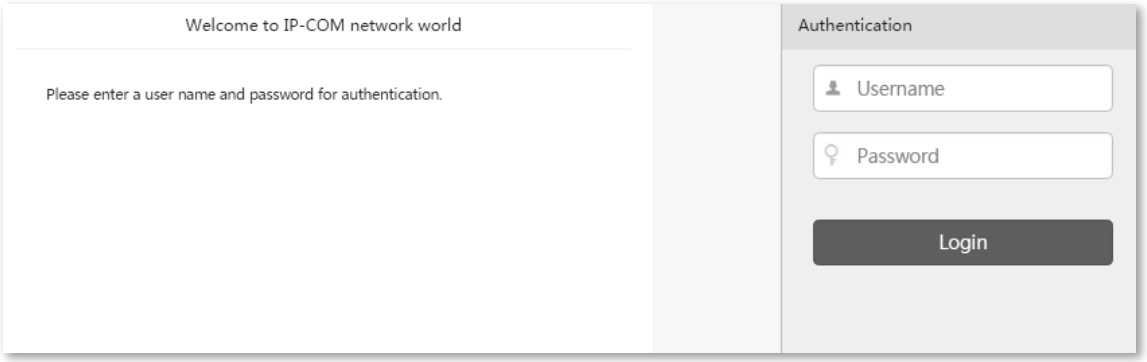
10.1 Overview

M80 supports captive portal, PPPoE authentication and WiFi via WeChat, and only one of them can be enabled on the router. You can select the authentication type referring to the following instructions:

- If the computers connected to your LAN with or without cables must be authenticated for accessing the internet, select captive portal or PPPoE authentication.
- If the computers connected to your LAN with cables must be authenticated for accessing the internet, while no authentication for the computers connected to your LAN without cables, select WiFi via WeChat.

10.1.1 Function description

By default, a computer connected to the router can access the internet after the router sets up an internet connection. To access the internet after captive portal is enabled on the router, a user of the computer must access the authentication web page of the router using a web browser, and enter a user name and password on the page to get authenticated. The following figure shows the authentication web page.



You can modify the title and content of the message on the page as required.

10.1.2 Configuring captive portal

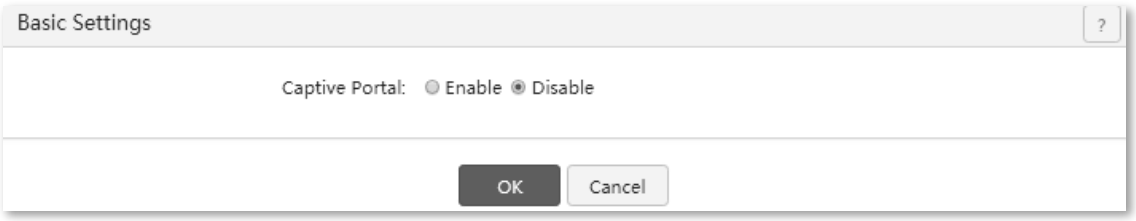
The following table describes the steps for configuring captive portal.

Step	Task	Description
1	Configuring basic settings	Choose **Captive Portal** > **Basic Settings** and set parameters.
2	Managing users	Choose **Captive Portal** > **User Management** and create user accounts for authentication. Only authenticated users can access the internet.

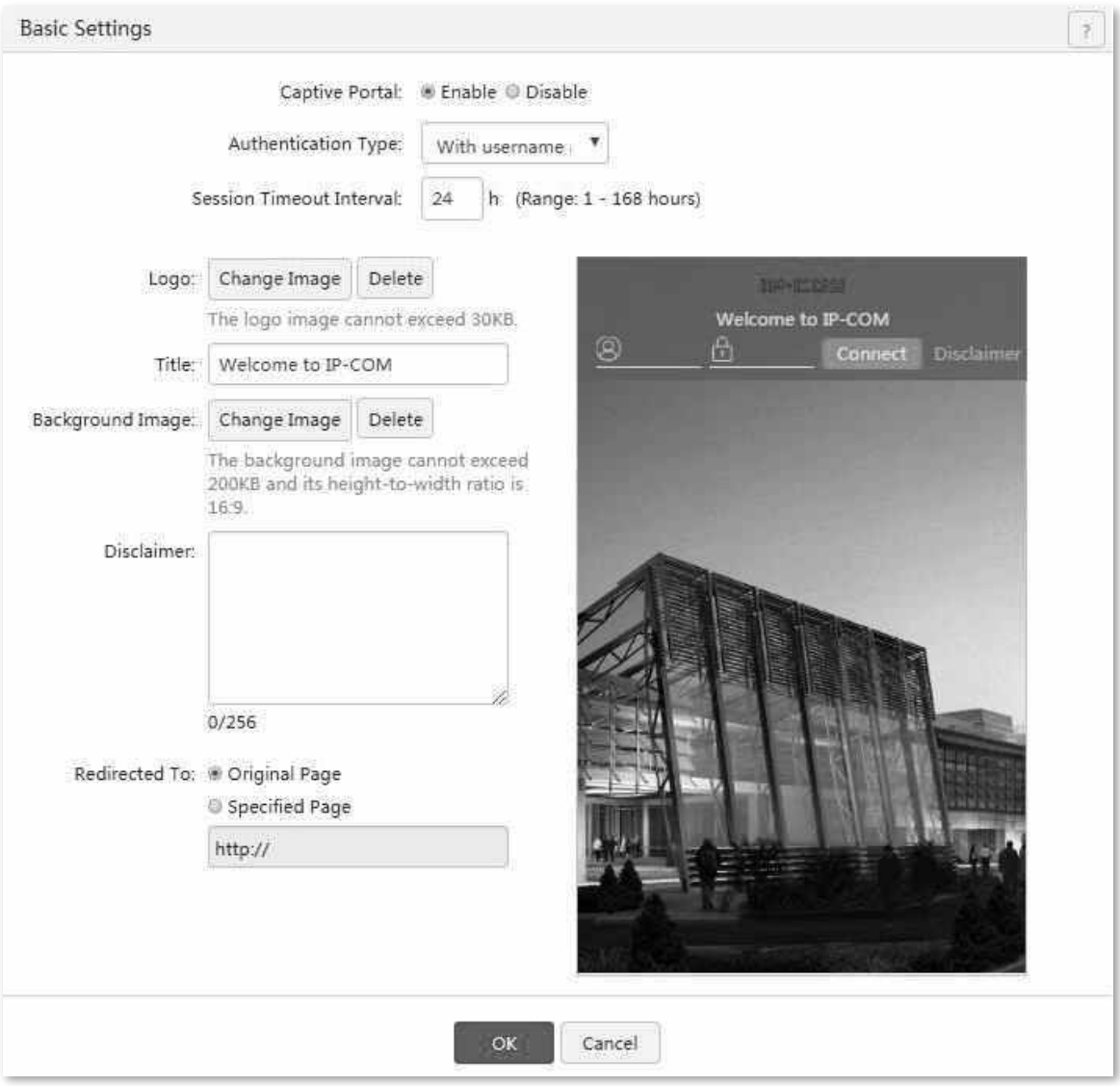
10.2 Configuring captive portal

10.2.1 Configuring basic settings

To access the page for configuring basic settings, choose **Captive Portal** > **Basic Settings**. On the page, you can enable or disable captive portal, set the authentication validity period, specify the computers that do not need to be authenticated, and configure the authentication web page. By default, captive portal is disabled.



Once captive portal is enabled, the following page is displayed.

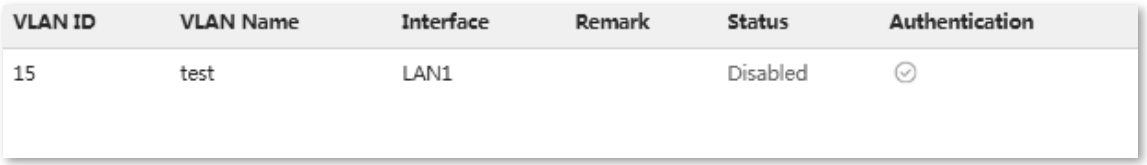


Parameter description

Parameter	Description
Captive Portal	It specifies whether to enable the captive portal function of the router. If the function is enabled, the PPPoE authentication function and WiFi via WeChat function of the router are disabled.
Authentication Type	It specifies the type of the captive portal. – **With username and password**: It allows a user to access the internet with a username and password on the authentication web page. The username and password should be added on page **Captive Portal > User Management**. – **One-key authentication**: It allows a user to access the internet by clicking **Connect** when receiving a captive portal page. – **WiFi via SMS:** It allows a user to access the internet with a verification code sent by SMS when receiving a captive portal page. The code can be set on page **Captive Portal > Basic Settings**.
Session Timeout Interval	It specifies the authentication validity period. A user must be re-authenticated for accessing the internet after the period expires.
Logo	It allows you to modify the logo of captive portal.
Title	It allows you to modify the title of captive portal. It is **Welcome to IP-COM** by default.
Background Image	It allows you to modify the background image of captive portal.
Change Image	Click it to change the image.
Delete	Click it to delete the image.
Disclaimer	It allows you to configure the disclaimer information of captive portal.
Redirected To	It specifies the website that the client automatically redirects to after passing captive portal: – **Original Page**: When the captive portal is passed, the page would redirect to the original page. If the page directs to captive portal when a user is visiting Google search page, after passing the authentication, it will redirect to Google search page. – **Specified Page**: It specifies the website redirected to after passing the captive portal.

This router supports captive portal based on VLAN. VLAN captive portal can be configured on **Captive Portal > Basic Settings** page if VLAN rules are configured on **VLAN Settings** page.

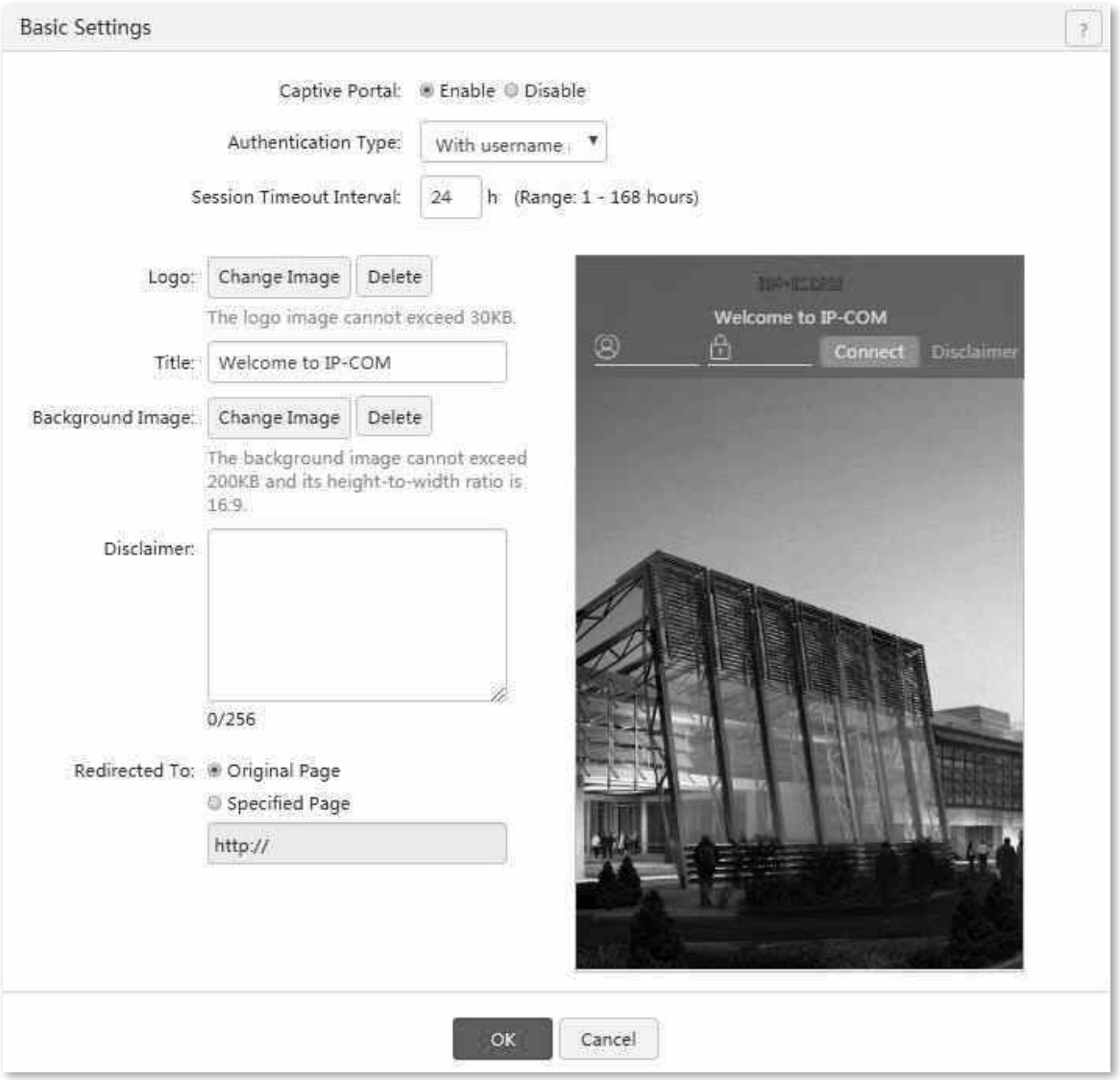
Locate the corresponding VLAN to set up captive portal, click , then the users under this VLAN could access the internet with captive portal.



Configuring captive portal

1. Choose **Captive Portal** > **Basic Settings**.
2. Set **Captive Portal** to **Enable**.
3. Set **Session Timeout Interval** and **Authentication Type** as required.

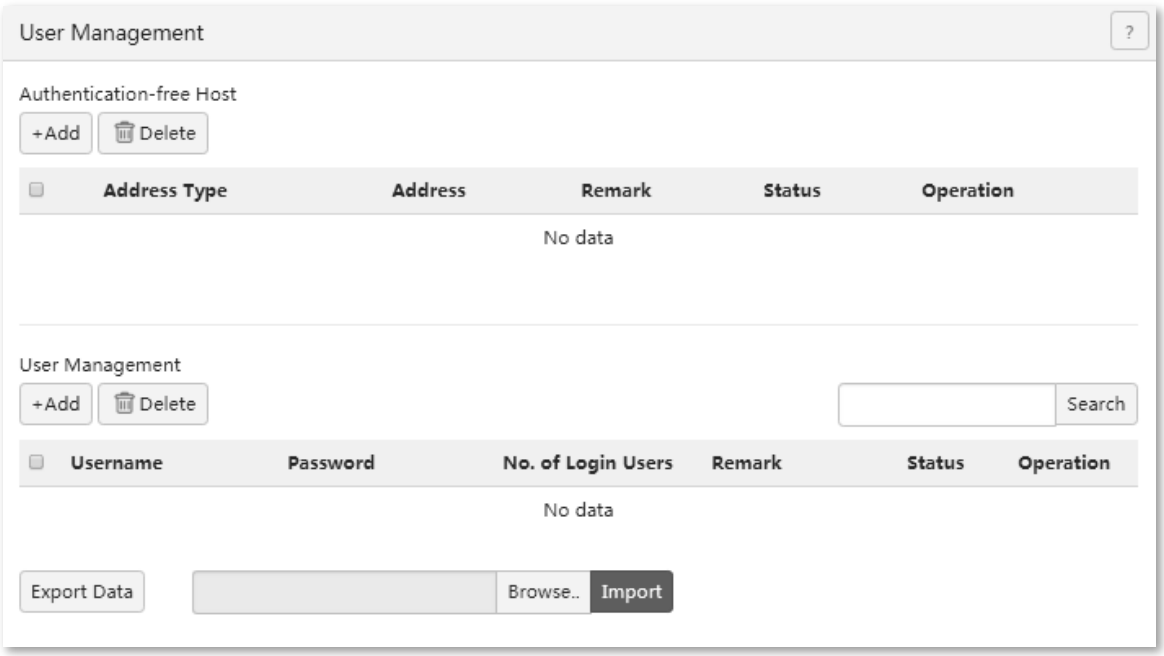
4. Click **OK**.



---End

10.2.2 Managing users

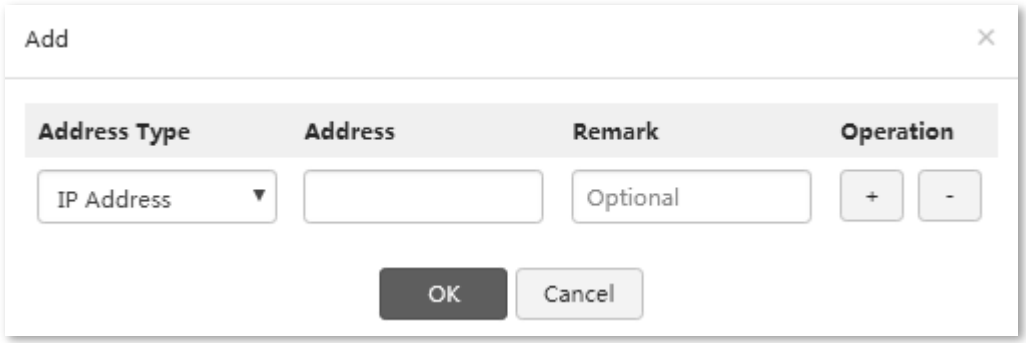
To access the page for managing users, choose **Captive Portal** > **User Management**. See the following figure. On the page, you can create hosts for authentication-free and user accounts for captive portal. If captive portal is enabled, users can access the internet only after being authenticated with the accounts.



Configuring authentication-free host

Adding an authentication-free host

1. Click **Captive Portal** > **User Management**, locate the **Authentication-free Host** module.
2. Click +Add.
3. Set the required parameters.
4. Click **OK**.



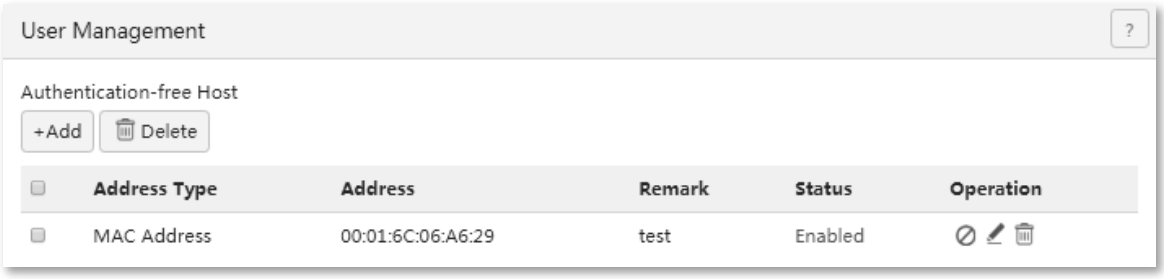
---End

Parameter description

Parameter	Description
Address Type	It allows you to set a device without authentication based on IP address or MAC address.
Address	It specifies the address information for authentication-free. When Address Type is set as IP Address, input the IP address of the authentication-free device. When Address Type is set as MAC Address, input the MAC address of the authentication-free device.

Remark	It specifies the description of an authentication-free host.
Operation	Click + to add a new authentication-free host, and click - to delete the corresponding authentication-free host.

The **User Management** page appears, showing the added hosts. See the following figure.



Modifying an authentication-free host

1. Click **Captive Portal** > **User Management**, locate the **Authentication-free Host** module.
2. Click corresponding to a host to be modified.

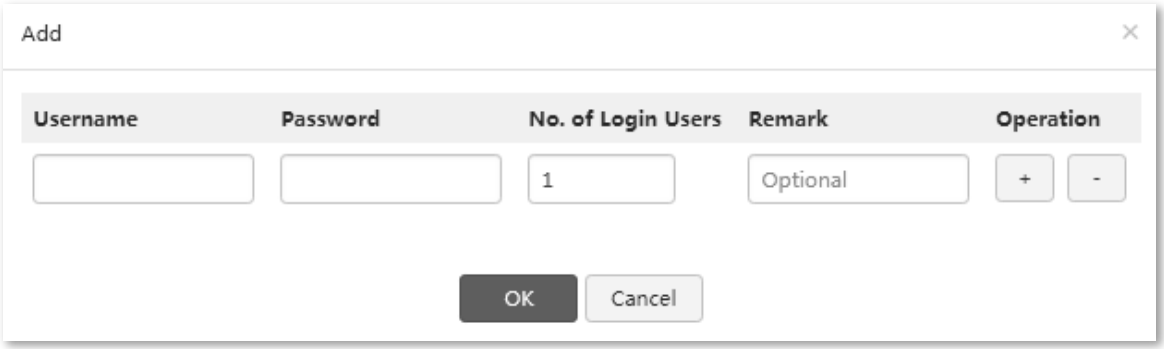
Deleting an authentication-free host

1. Click **Captive Portal** > **User Management**, locate the **Authentication-free Host** module.
2. Click corresponding to an entry to be deleted. To delete multiple entries at the same time, select the entries and click .

Configuring user management

Adding a user account

1. Choose **Captive Portal** > **User Management**.
2. Click +Add.
3. Set required parameters.
4. Click **OK**.

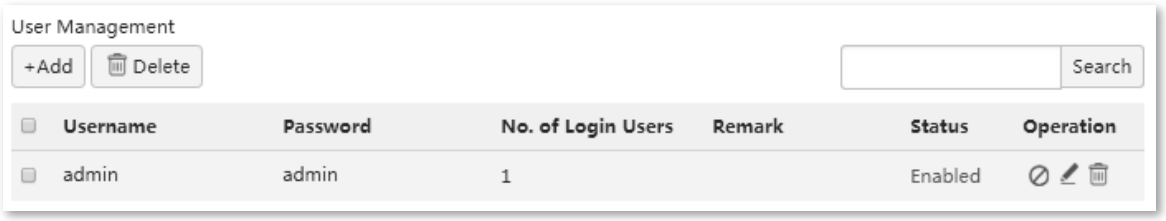


----End

Parameter description

Parameter	Description
Username	**Username** specifies a user name for captive portal. **Password** specifies a password for captive portal. If captive portal is enabled, a user must be authenticated with a correct user name and password before accessing the internet.
Password	
Remark (Optional)	It specifies the description of a user account.
Operation	It provides buttons for adding and deleting entries. The buttons include: + : It is used to add an entry. - : It is used to delete a corresponding entry.

The **User Management** page appears, showing the added user accounts. See the following figure.



Modifying a user account

1. Choose **Captive Portal** > **User Management**.
2. Click corresponding to a user account to be modified.
3. Modify the user account.
4. To disable a user account, click corresponding to the account.
5. To enable a user account, click corresponding to the account.

Deleting a user account

1. Choose **Captive Portal** > **User Management**.
2. Click corresponding to a user account to be deleted. To delete multiple user accounts at the same time, select them and click Delete.

10.3 Example of configuring captive portal

Networking requirement

An enterprise uses M80 to set up a LAN to address the following requirement:

The network administrator can access the internet without being authenticated, while the other employees must be authenticated before accessing the internet.

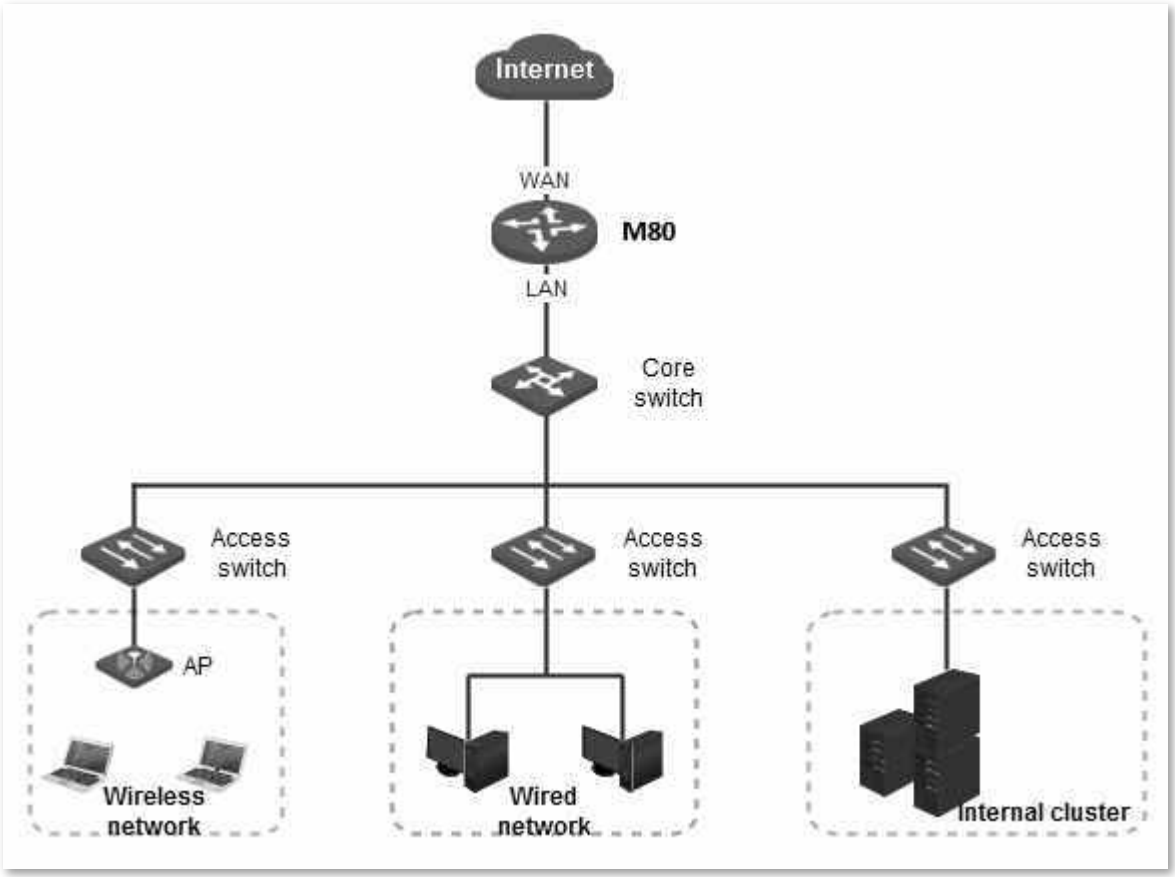
You can use the captive portal function of the router to meet this requirement. Assume that the MAC address of the network administrator's computer is 44:37:E6:12:34:56.

Tip

If you need to set up VLAN in the network, refer to 4.8.5 An example of Configuring VLAN Settings.

Network topology

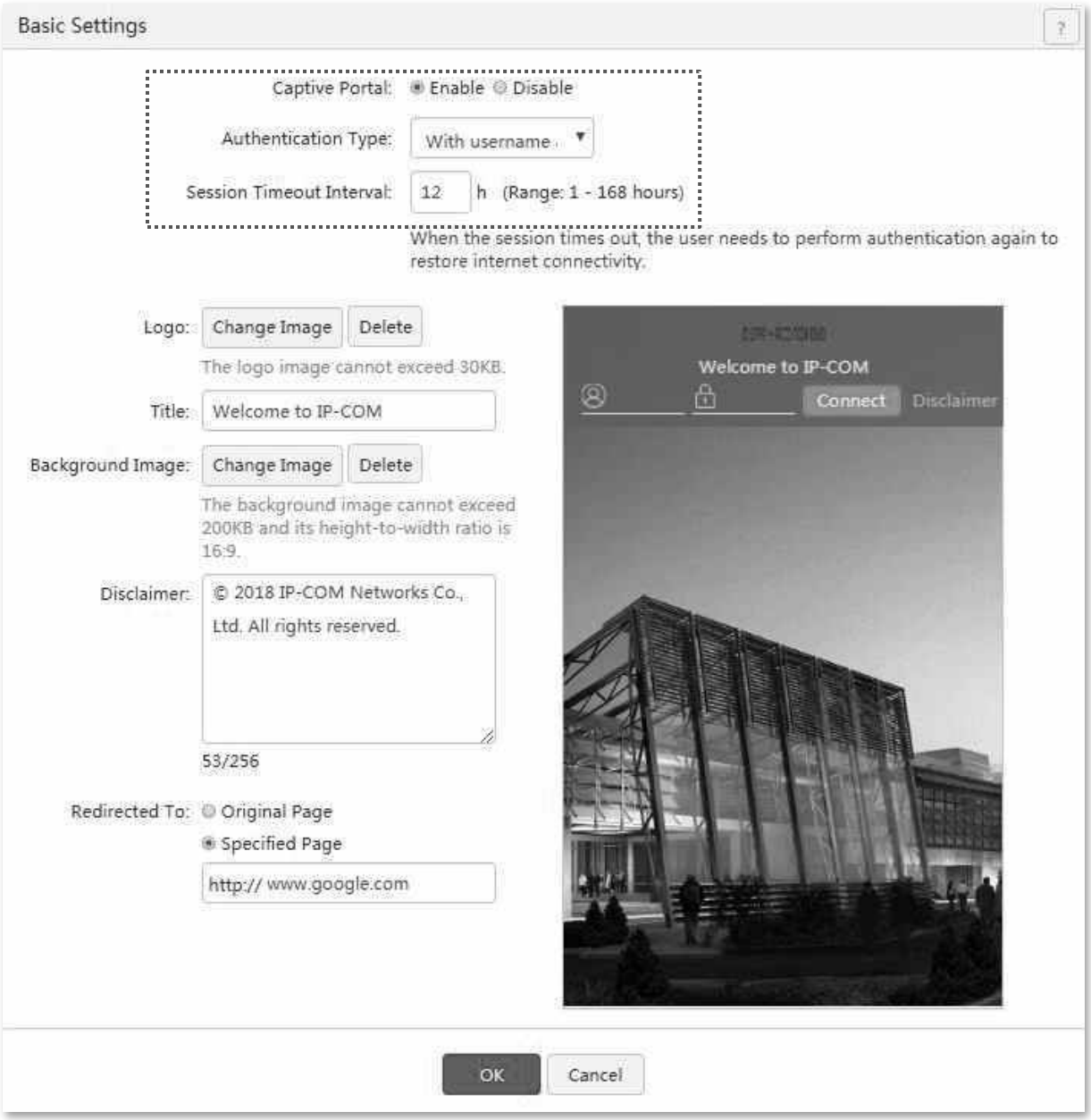
The following figure shows the network topology of the enterprise.



Configuration procedure

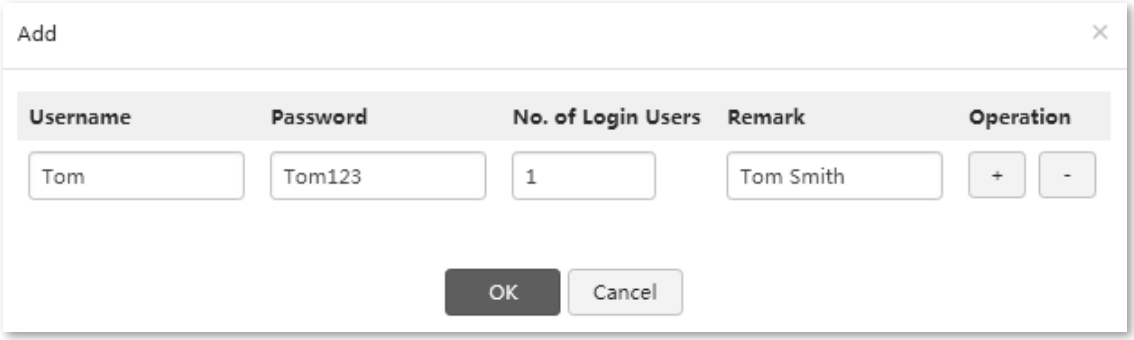
I. Configure basic settings for captive portal.

1. Choose **Captive Portal** > **Basic Settings**.
2. Set **Captive Portal** to **Enable**.
3. Set **Authentication Type** to **With username and password**.
4. Set **Session Timeout Interval** to **12 h**.
5. Click **Change Image** to upload enterprise's logo.
6. Set **Title**, such as **Welcome to IP-COM**.
7. Set **Disclaimer**, such as **© 2018 IP-COM Networks Co., Ltd. All rights reserved**.
8. Set **Redirected To** to **Specified Page**, and then input the website, which is www.google.com in this example.
9. Click **OK**.



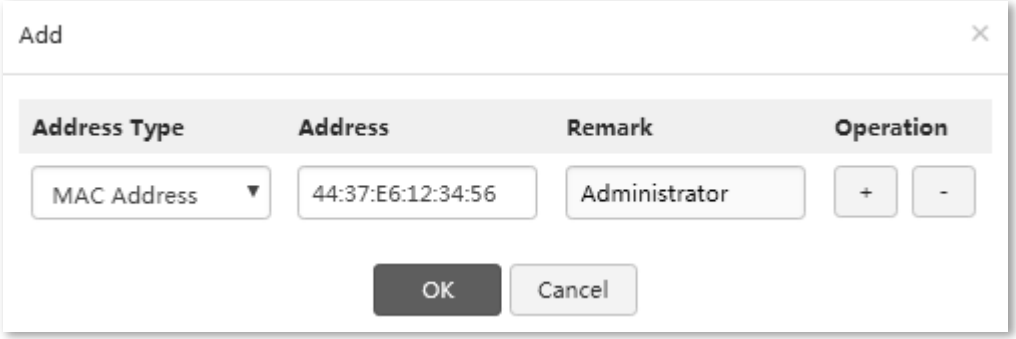
II. Add a user account for captive portal.

1. Choose **Captive Portal** > **User Management**.
2. Click +Add.
3. Set required parameters.
   (1) Set **username** to a user name for captive portal, which is **Tom** in this example.
   (2) Set **Password** to the password of the user Tom, which is **Tom123** in this example.
   (3) Set **Remark (Optional)** to the description of the user Tom, which is **Tom Smith** in this example. You can leave this parameter blank. (To add more user accounts, click + and repeat the preceding steps.)
4. Click **OK**.



III. Add user devices that can access the internet without being authenticated.

1. Choose **Captive Portal** > **Basic Settings**.
2. Click +Add in the **Authentication-free Host** area. The **Add** dialog box appears.
3. Set required parameters.
   (1) Set **Address Type** to **MAC Address** in this example.
   (2) Set **MAC Address** to the MAC address of a user device that can access the internet without being authenticated, which is **44:37:E6:12:34:56** in this example.
   (3) Set **Remark (Optional)** to the description of the user device, which is **Administrator** in this example.
4. Click **OK**.

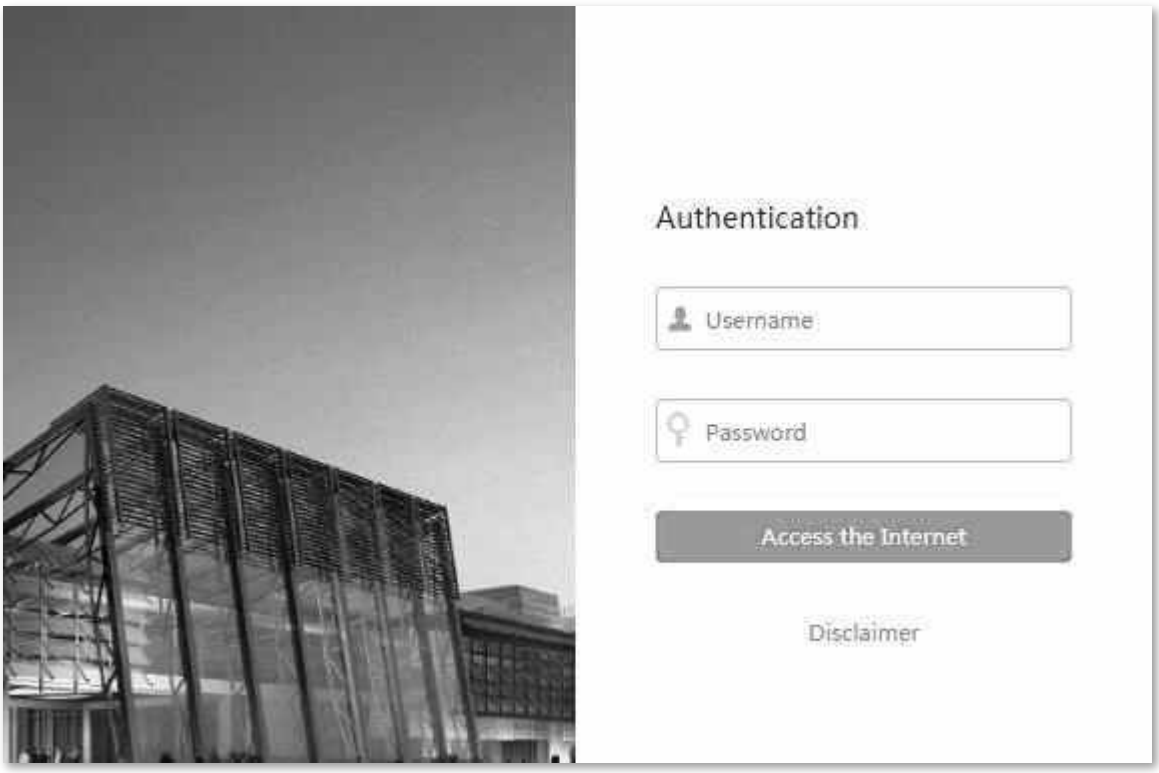


---End

Verification

Verify that the network administrator can access the internet without being authenticated, while the other employees need to perform the following procedure to get authenticated before accessing the internet:

1. Start a web browser and enter the address of any website. The captive portal page appears. See the following figure.



2. Enter a correct user name and password in the **Authentication** page and click Access the Internet.

When the employee is authenticated, the employee is directed to the website www.google.com.

11 PPPoE authentication

11.1 Overview

M80 supports captive portal, PPPoE authentication and WiFi via WeChat, and only one of them can be enabled on the router. You can select the authentication type referring to the following instructions:

- If the computers connected to your LAN with or without cables must be authenticated for accessing the internet, select captive portal or PPPoE authentication.
- If the computers connected to your LAN with cables must be authenticated for accessing the internet, while no authentication for the computers connected to your LAN without cables, select WiFi via WeChat.

This chapter describes:

11.1.1 Function description

By default, a computer connected to the router can access the internet after the router sets up an internet connection. To access the internet after PPPoE authentication is enabled on the router, a user of the computer must set up a PPPoE dial-up connection.

M80 supports account expiration alerts. You can configure the router to alert users within 7 days before account expiration and upon account expiration. This simplifies network administration, improving network administration efficiency. In addition, M80 allows authentication-free hosts and supports flow control policies.

11.1.2 Configuration instruction

The following table describes the procedure for configuring PPPoE authentication.

Step	Task	Description
1	Configuring basic settings	Choose **PPPoE Authentication** > **Basic Settings**, enable PPPoE authentication, and set the parameters.
2	Managing users	Choose **PPPoE Authentication** > **User Management**, create accounts for users to set up PPPoE dial-up connections for accessing the internet.

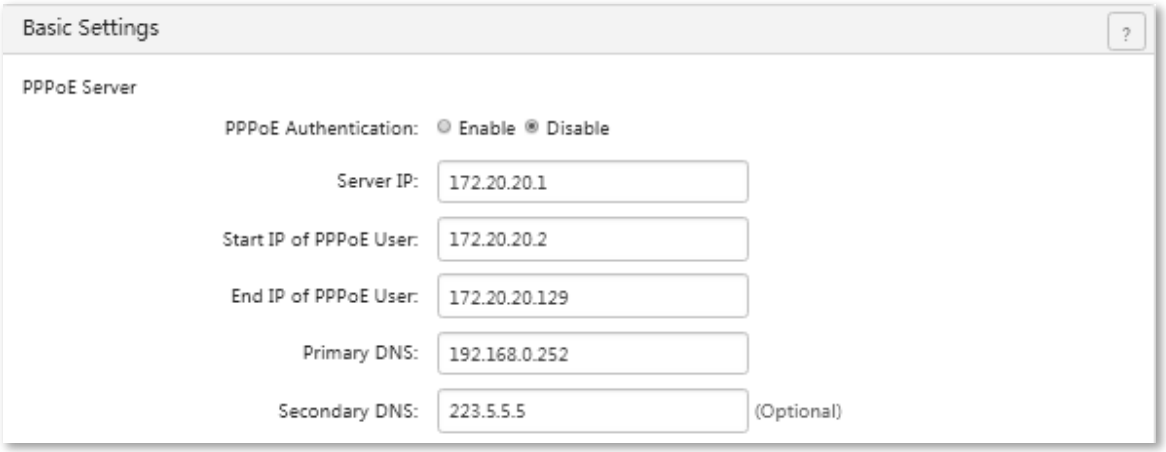
11.2 Configuring PPPoE authentication

11.2.1 Configuring basic settings

To access the page for configuring basic settings, choose **PPPoE Authentication** > **Basic Settings**. On the page, you can set the PPPoE server, account expiration alerts, authentication-free hosts, and flow control policies.

Configuring the PPPoE server

1. Enable **PPPoE Authentication**.
2. Set PPPoE server parameters.

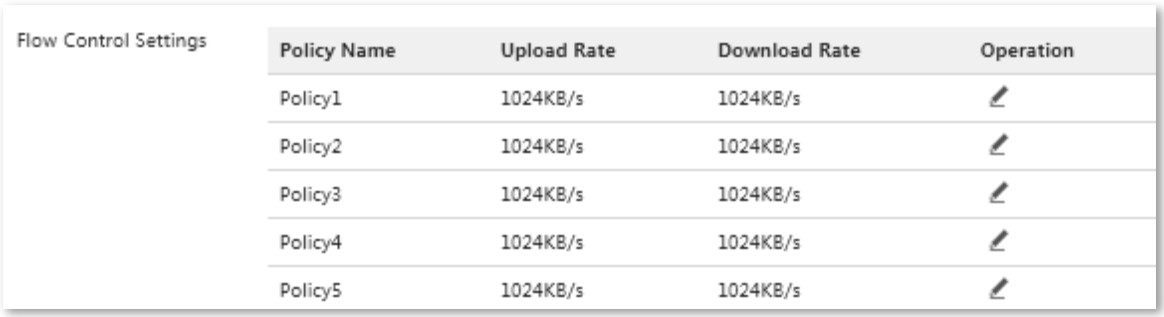


Parameter description

Parameter	Description
PPPoE Authentication	It specifies whether to enable PPPoE authentication. If the function is enabled, the captive portal function of the router is disabled.
Server IP	It specifies the IP address of the PPPoE server. The default value is recommended. If you need to change the default value, set this parameter to a private IP address within the following ranges: – **Class A IP addresses**: 10.0.0.1–10.255.255.254 – **Class B IP addresses**: 172.16.0.1–172.31.255.254
Start IP of PPPoE User and End IP of PPPoE User	These two parameters together specify the IP address range for the PPPoE server to assign an IP address to a user after the user sets up a PPPoE dial-up connection. The start and end IP addresses must belong to the same network segment as the PPPoE server IP address.
Primary DNS and Secondary DNS	These two parameters specify the DNS IP addresses assigned by the router to a user after the user sets up a PPPoE dial-up connection. Generally, these DNS IP addresses are the same as those specified for the WAN port of the router.

Configuring flow control polices

The router supports flow control policies configuration, which effectively control network bandwidths of PPPoE users. This helps prevent some users from using too much bandwidth, which slows down internet connections of other users. The following figure shows the default flow control policies.

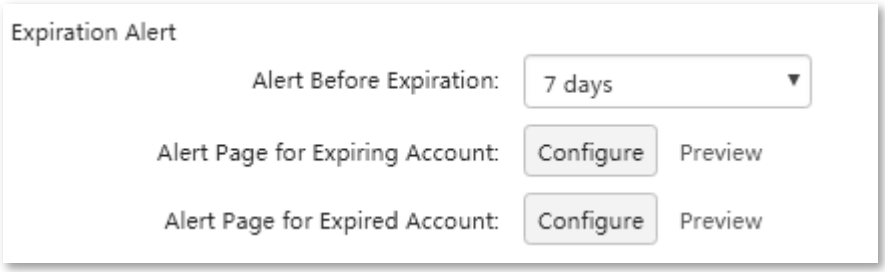


Parameter description

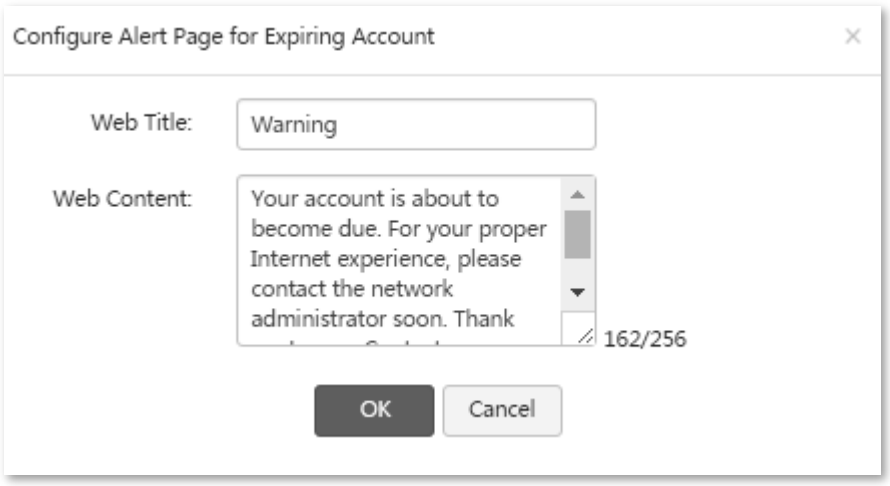
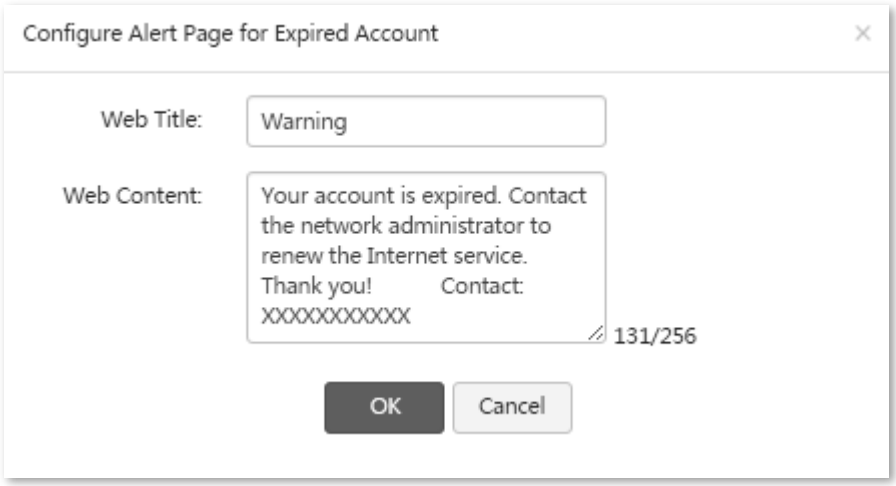
Parameter	Description
Policy Name	It specifies the names of flow control policies. Currently, flow control policy names cannot be modified. If PPPoE authentication is enabled, the bandwidth control function of the router is replaced by the flow control policies for PPPoE users.
Upload and Download Rate	**Upload Rate** specifies the maximum uplink throughputs for policies. **Download Rate** specifies the maximum downlink throughputs for policies. The policies are applied to PPPoE accounts. If the user accounts are used to access the internet, the uplink and downlink throughputs for the accounts are limited according to the policies.
Operation	It allows you to modify flow control policies. To modify a policy, click  corresponding to the policy and change the uplink and downlink throughputs, which are 1024 KB/s (1 Mbps = 128 KB/s = 1024 kb/s; 1 B = 8 b). If a policy applied to a PPPoE account is modified, the account abides by the new policy.

Configuring account expiration alerts

The router can alert users of account expiration. You can configure the router to alert them several days before account expiration and configure alert pages to be displayed before and upon expiration.

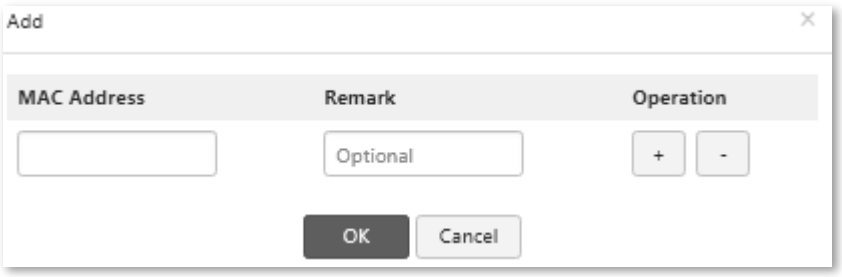


Parameter description

Parameter	Description
Alert Before Expiration	It specifies the number of days before account expiration to alert a user. By default, the router alerts a user 7 days before account expiration.
Alert Page for Expiring Account	It specifies the message on the alert page for expiring accounts. You can click Configure and modify the message. See the following figure.  Set the parameters and click **OK**. The **Basic Setup** page appears. You can click **Preview** to preview the alert page.
Alert Page for Expired Account	It specifies the message on the alert page for expired accounts. You can click Configure. And modify the message. See the following figure.  Set the parameters and click **OK**. The **Basic Setup** page appears. You can click **Preview** to preview the alert page.

Configuring authentication-free hosts

1. Choose **PPPoE Authentication** > **Basic Settings**.
2. Click +Add in the **Authentication-free** area.
3. Set required parameters.
4. Click **OK.**

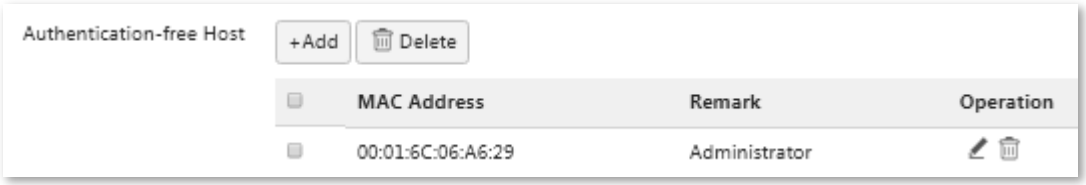


---End

Parameter description

Parameter	Description
MAC Address	It specifies the physical address of the network adapter of the host that can access the internet without being authenticated.
Remark	It specifies the description of a host that can access the internet without being authenticated. It is optional.
Operation	It provides buttons for adding and deleting entries. The buttons include: + : It is used to add an entry. - : It is used to delete a corresponding entry.

The **Basic Setup** page appears, showing the added hosts. See the following figure.



Modifying authentication-free hosts

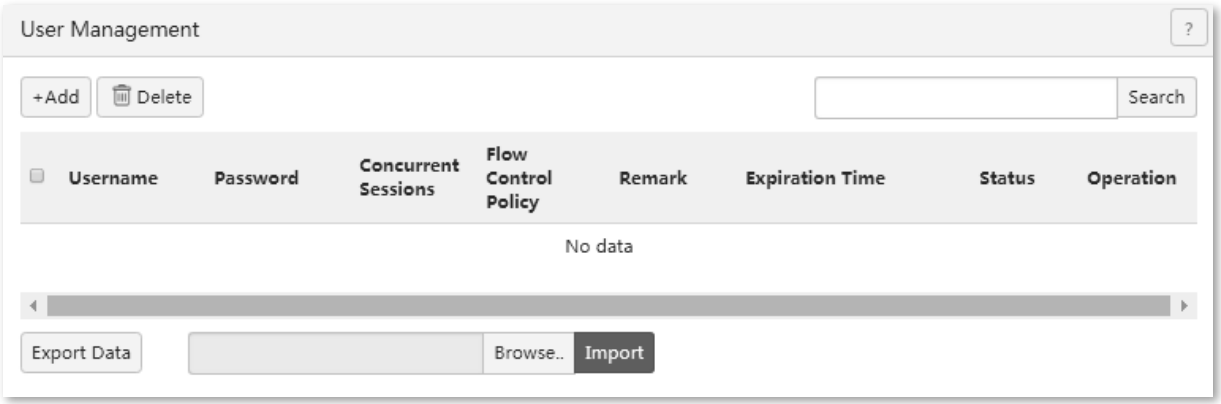
1. Choose **PPPoE Authentication** > **Basic Settings**.
2. Click corresponding to the host and modify the information.

Deleting authentication-free hosts

1. Choose **PPPoE Authentication** > **Basic Settings**.
2. Click corresponding to the host. To delete multiple hosts at the same time, select them and click Delete.

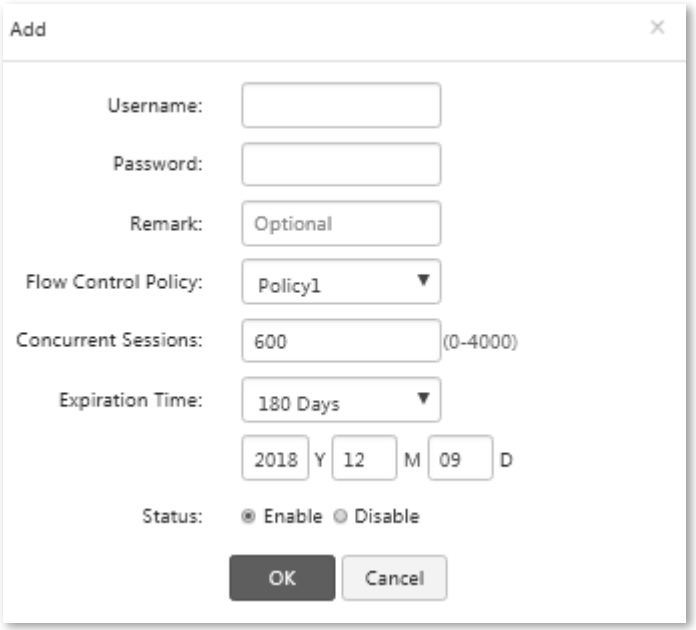
11.2.2 Managing users

To access the page for managing accounts, choose **PPPoE Authentication** > **Account Management**. See the following figure. On the page, you can set PPPoE account information. If PPPoE authentication is enabled, users requiring internet accessibility must use the accounts to set up PPPoE connections. The following figure shows the default account management.



Adding an account

1. Choose **PPPoE Authentication** > **User Management**.
2. Click +Add.
3. Set required parameters.
4. Click **OK**.

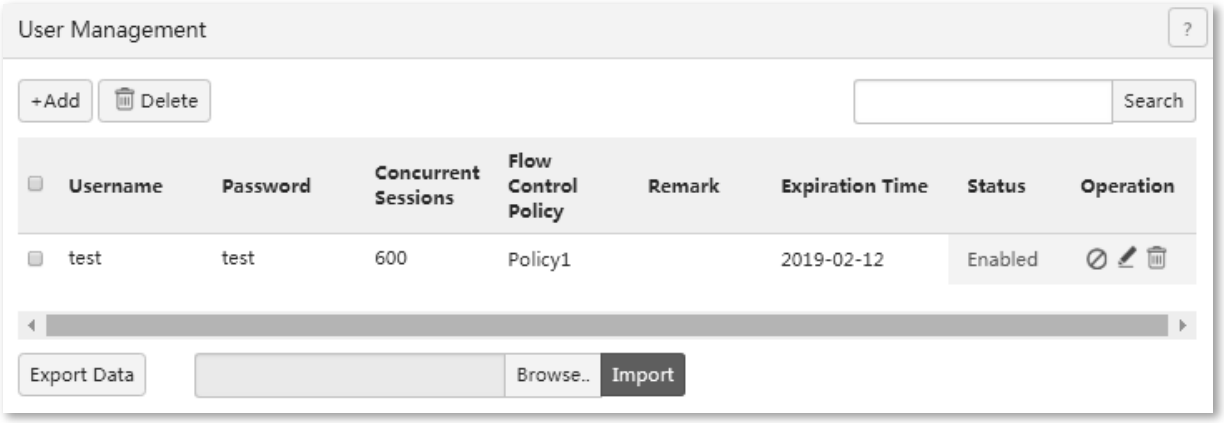


---End

Parameter description

Parameter	Description
Username	**Username** specifies the user name to be entered by a user for authentication when setting by a PPPoE connection. **Password** specifies the password for the user name.
Password	
Remark	It specifies the description of an account. The description is optional.
Flow Control Policy	It specifies the flow control policy applied to an account. You can configure flow control policies in the **Flow Control Settings** area on the **PPPoE Authentication** > **Basic Settings** page.
Expiration	It specifies the expiration date of an account. After the date, the account can be used to set up a PPPoE dial-up connection but cannot access the internet.
Status	It specifies whether an account is enabled.

The **User Management** page appears, showing the added accounts. See the following figure.



Modifying an account

1. Choose **PPPoE Authentication** > **User Management**.
2. Click corresponding to an account to be modified. To disable an account, click corresponding to the account. To enable an account, click corresponding to the account.

Deleting an account

1. Choose **PPPoE Authentication** > **User Management**.
2. Click corresponding to an account to be deleted. To delete multiple accounts at the same time, select them and click Delete.

Exporting or importing PPPoE account data

You can export PPPoE account data to a local computer as a backup. In case that the data on the router is lost, you can import the backup to restore the data.

The procedure for exporting PPPoE account data is as follows:

1. Choose **PPPoE Authentication** > **User Management**.
2. Click Export and follow the onscreen instruction to export the data to a **pppoe_user.cfg** file.

The procedure for importing PPPoE account data is as follows:

1. Choose **PPPoE Authentication** > **User Management**.
2. Click Browse..., select the **pppoe_user.cfg** file, and click Import.

11.3 Example of configuring PPPoE authentication

Networking requirement

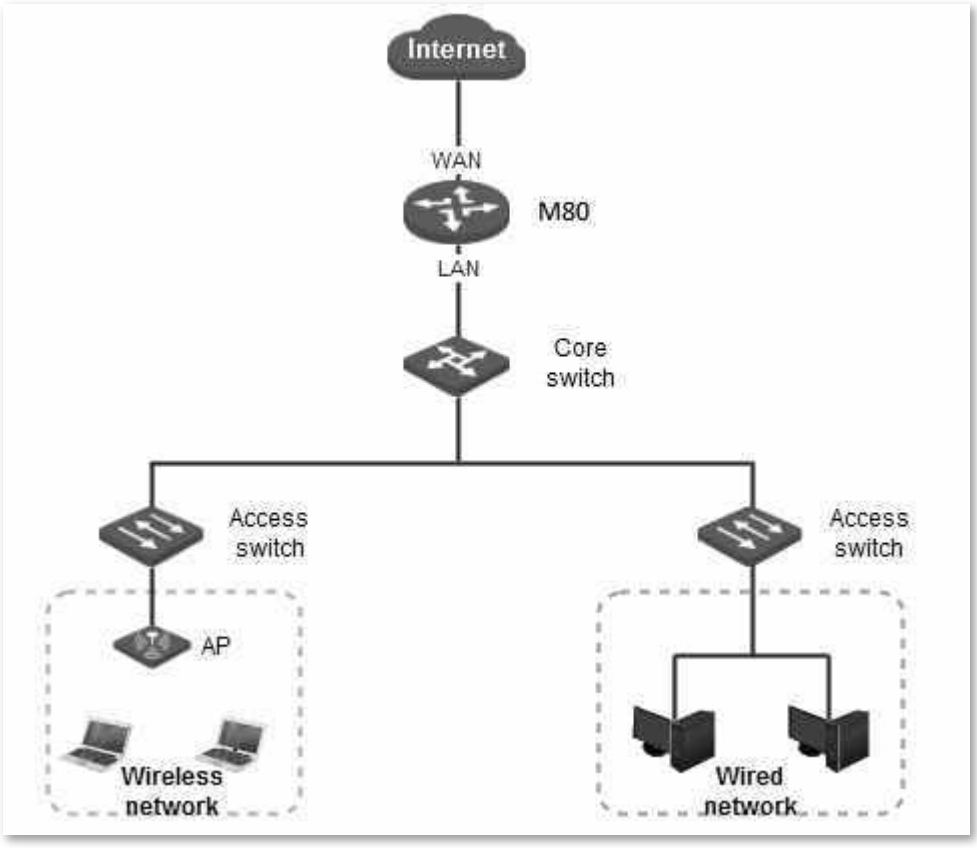
The ISP of a residential estate uses M80 to offer internet accessibility to a building to address the following requirement:

Residents need to set up PPPoE dial-up connections before accessing the internet. The network administrator of the building can access the internet merely with an automatically assigned IP address.

You can use the PPPoE authentication function of the router to meet this requirement. To address the requirement, enable the PPPoE server, add PPPoE user names and passwords for the residents, and set the network administrator's computer as an authentication-free host.

Network topology

The following figure shows the network topology of the residential estate.



Configuration procedure

Note

For the parameters not mentioned in this procedure, retain their default settings.

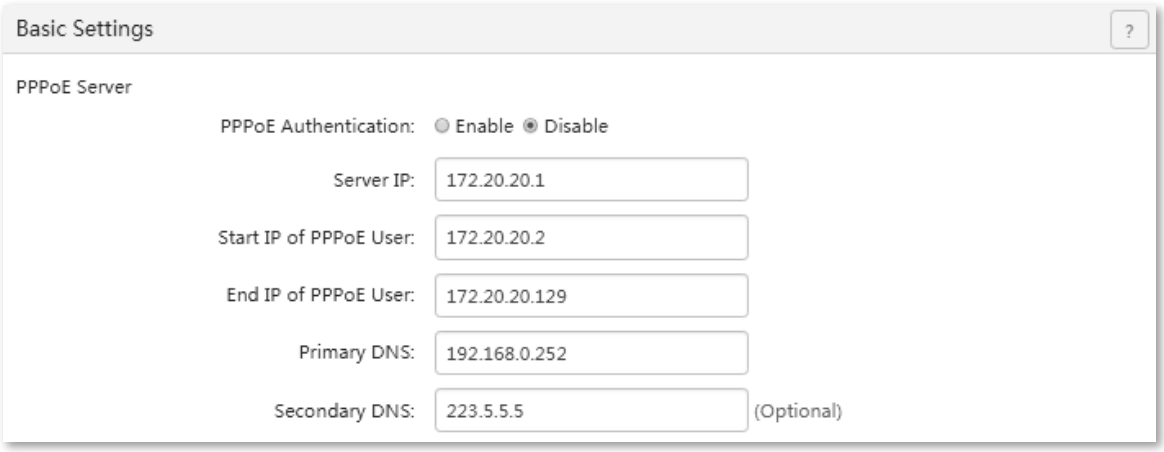
I. Configure basic settings for PPPoE authentication.

Choose **PPPoE Authentication** > **Basic Settings** and perform the following steps:

1. Enable PPPoE authentication and set the account expiration alert time.

   (1) Set **PPPoE Authentication** to **Enable**.

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

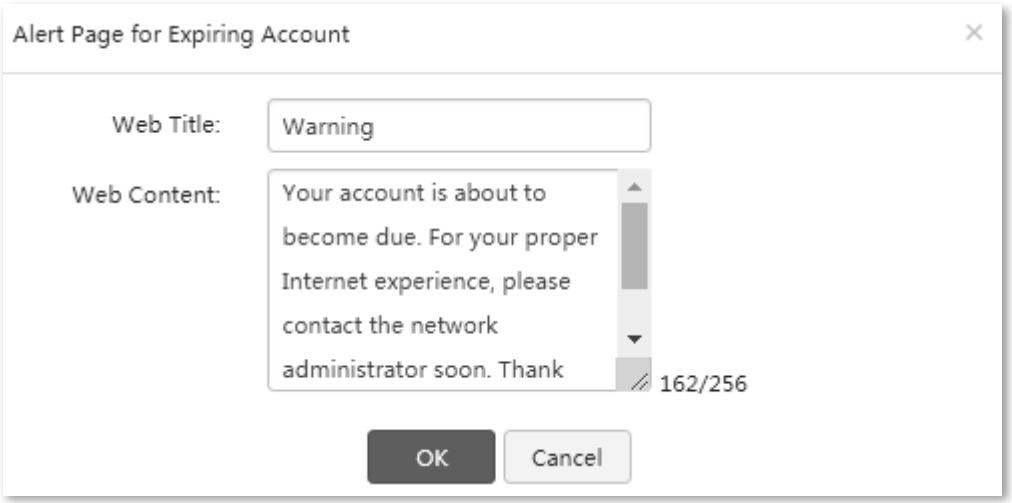


2. Configure the account expiration alert pages.

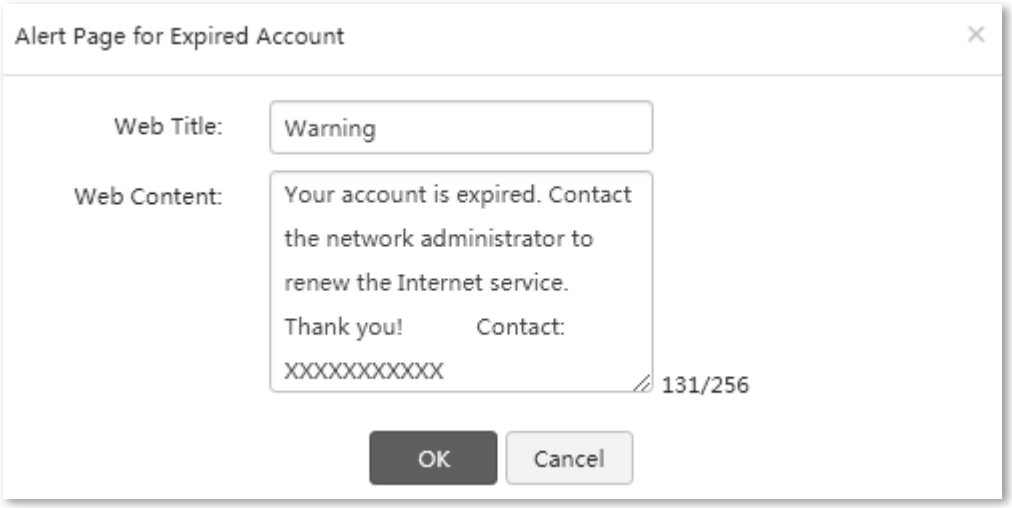
Perform the following steps in the **Expiration Alert** area:

(1) Set **Alert Before Expiration** to the number of days before account expiration to alert users, such as **3** days.

(2) Click Configure to the right of **Alert Page for Expiring Account**, set **Web Title** and **Web Content**, and click **OK**.



(3) Click Configure to the right of **Alert Page for Expired Account**, set **Web Title** and **Web Content**, and click **OK**.



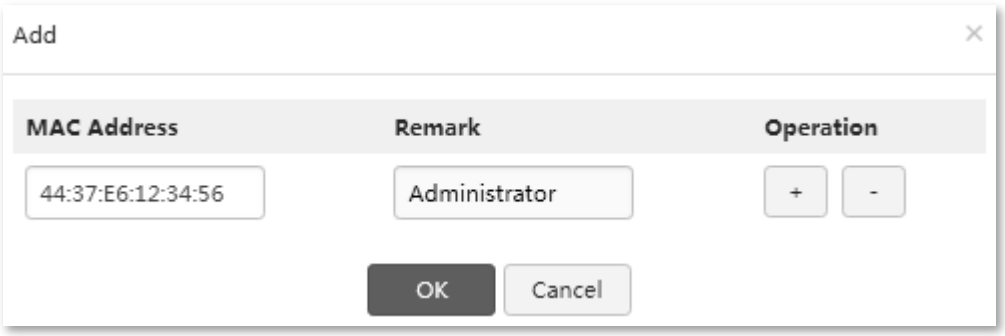
3. Add authentication-free hosts.

(1) In the **Authentication-free** area, click +Add.

(2) Set **MAC Address** to the MAC address of the computer that can access the internet without being authenticated, which is **44:37:E6:12:34:56** in this example.

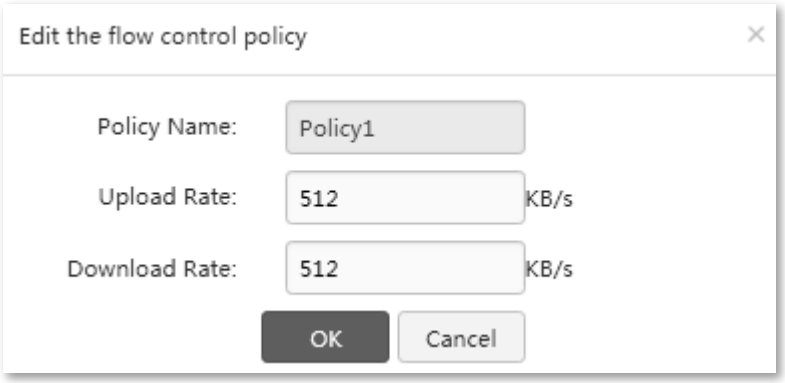
(3) Set **Remark (Optional)** to the description of the computer, which is **Administrator** in this example.

(4) Click **OK**.



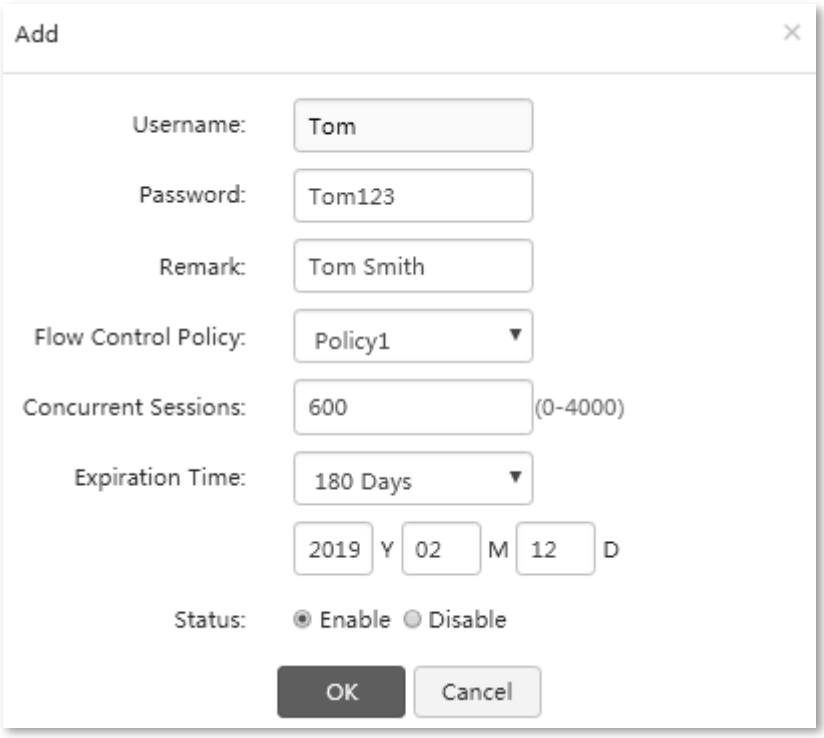
4. Configure flow control policies.

In the **Flow Control Settings** area, click corresponding to **Policy1**, and change the uplink and downlink throughputs. For example, if a resident requests a bandwidth of 4 Mbps, change the throughputs to the values shown in the following figure.



II. Add PPPoE accounts.

1. Choose **PPPoE Authentication** > **User Management**.
2. Click +Add.
3. Set required parameters in the **Add** dialog box.
   (1) Set **Username** to the user name for PPPoE authentication, which is **Tom** is this example.
   (2) Set **Password** to the password for the user Tom, which is **Tom123** in this example.
   (3) Set **Remark** to the description of the user Tom, which is **Tom Smith** in this example. You can leave this parameter blank.
   (4) Set **Flow Control Policy** based on the bandwidth requested by the user.
   (5) Set **Expiration** to the date when the broadband service for the user expires.
   (6) Set **Status** to **Enable**.
   (7) Click **OK**.



---End

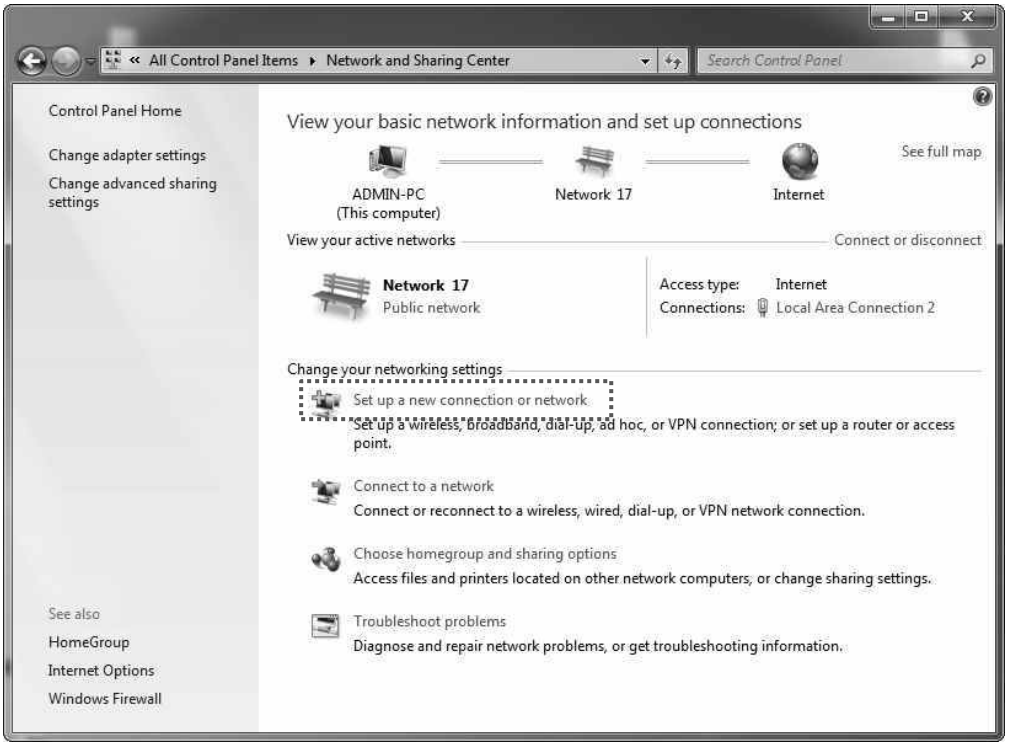
If multiple residents require PPPoE connections, repeat the preceding steps to add an account for each of them.

Verification

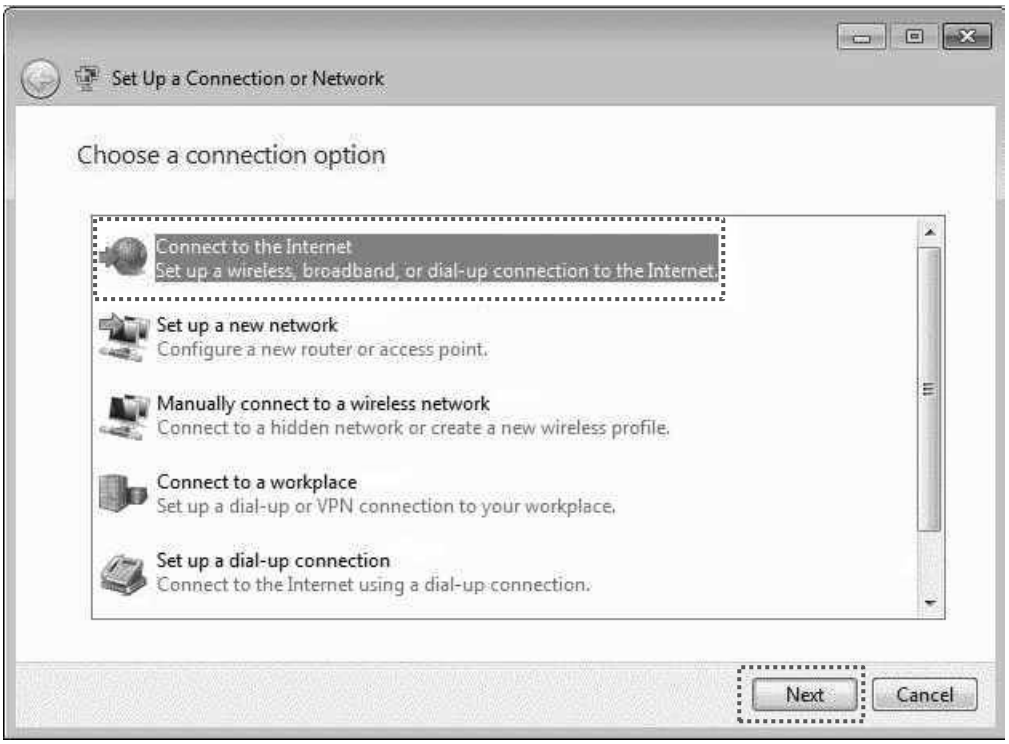
Verify that the network administrator can access the internet without being authenticated, and that the residents can access the internet only after setting up PPPoE connections. To set up a PPPoE connection, a resident must perform the following procedure on his/her computer (Windows 7 is used as an example):

1. Click  in the lower-left corner of the desktop. And then click **Control Panel**.
2. Click **Network and Sharing Center**.

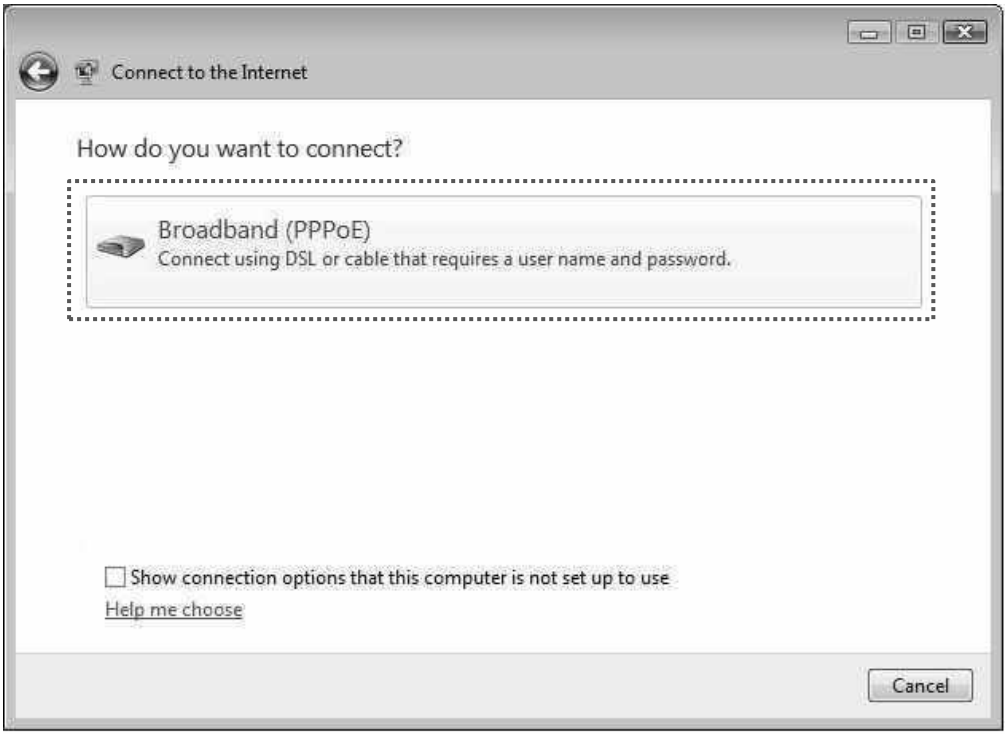
3. Click **Set up a new connection or network**.



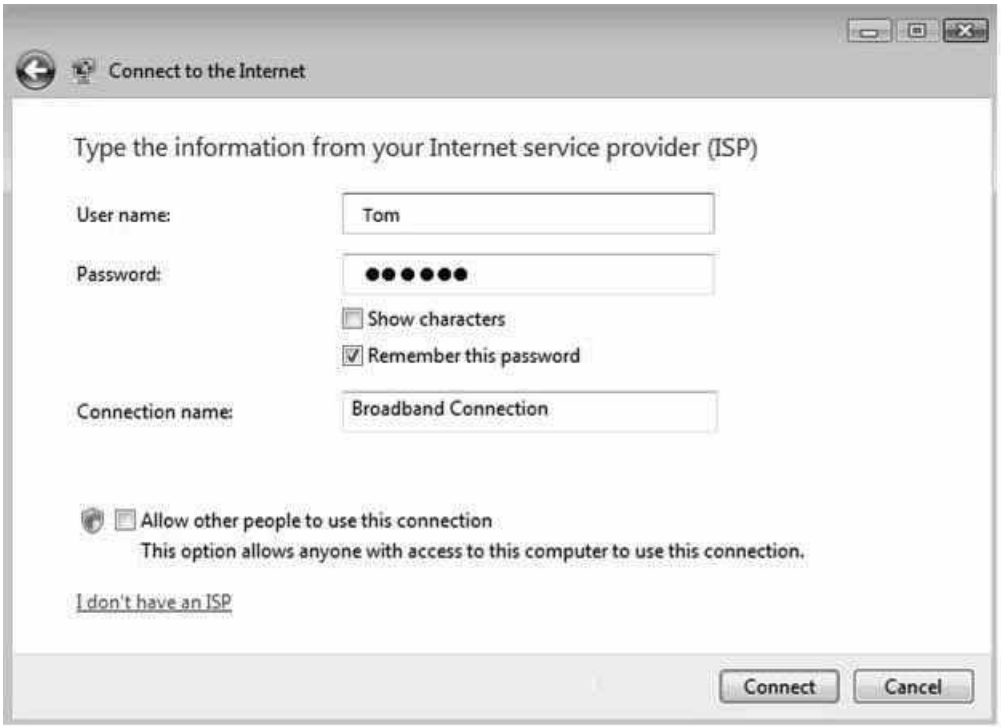
4. Click **Connect to the internet** and click **Next**.



5. Click **Broadband (PPPoE)**.



6. Set **User name** and **Password** to the user name and password of a PPPoE account, which are **Tom** and **Tom123** in this example. Select **Remember this password** if necessary and click **Connect**.



The user can access the internet after a while.

To reconnect the computer to the internet after the computer is restarted, click  in the lower-right corner of the desktop and click **Connect** in the **Broadband Connection** entry.

12 WiFi via WeChat

12.1 Overview

M80 supports captive portal, PPPoE authentication and WiFi via WeChat, and only one of them can be enabled on the router. You can select the authentication type referring to the following instructions:

- If the computers connected to your LAN with or without cables must be authenticated for accessing the internet, select captive portal or PPPoE authentication.
- If the computers connected to your LAN with cables must be authenticated for accessing the internet, while no authentication for the computers connected to your LAN without cables, select WiFi via WeChat.

This chapter describes:

12.1.1 Function description

By default, a computer connected to the router can access the internet after the router sets up an internet connection. To access the internet after WiFi via WeChat is enabled on the router, clients must access authentication web page of the router by WeChat to get authenticated. In this case, here are 3 cases which need authentication:

- Clients connected to LAN0 by cables.
- Clients connected to the wireless of AP which is connected to LAN0 of the router.
- Clients under VLAN with WiFi via WeChat enabled.

12.1.2 Configuration instruction

The following table describes the procedure for configuring WiFi via WeChat.

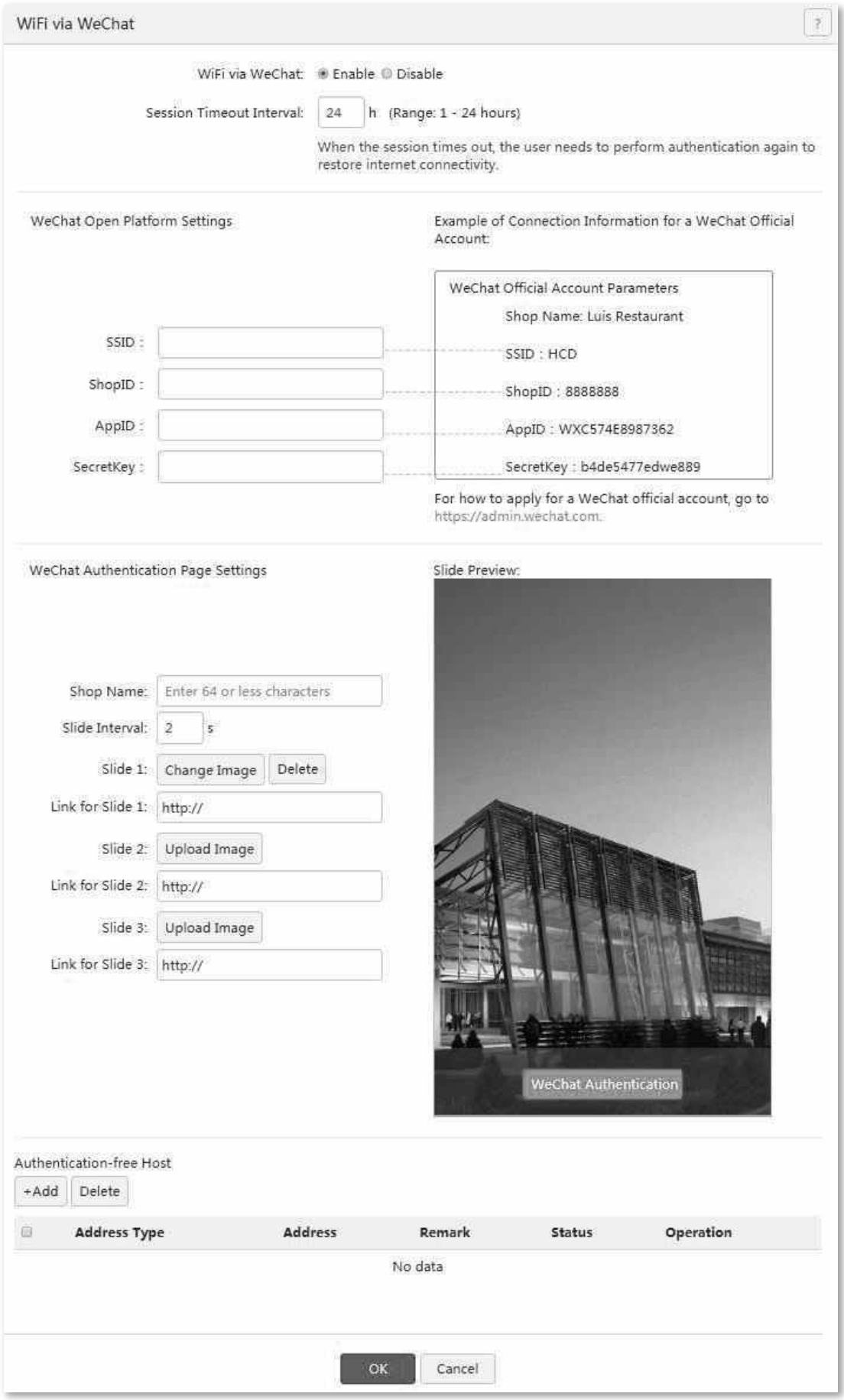
Step	Task	Description
1	Configuring WeChat Open Platform Settings	Log in to the WeChat public platform, prepare and record the information of **SSID**, **ShopID**, **AppID**, and **SecretKey** to configure the router.
2	Configuring WiFi via WeChat	Choose **WiFi via WeChat**, enable **WiFi via WeChat**, and set required parameters.

12.2 Configuring WiFi via WeChat

To access the page for configuring WiFi via WeChat, choose **WiFi via WeChat**. The function is disabled by default.

Configuring WiFi via WeChat

1. Choose **WiFi via WeChat**.
2. Set **WiFi via WeChat** to **Enable**.
3. In **WeChat Open Platform Settings** module, set WeChat official account parameters of **SSID**, **Shop ID**, **AppID**, **SecretKey**.
4. Set WeChat Authentication Page Settings.
5. Add authentication-free hosts.
6. Click **OK**.


WiFi via WeChat
WiFi via WeChat: Enable Disable
Session Timeout Interval: 24 h (Range: 1 - 24 hours)
When the session times out, the user needs to perform authentication again to restore internet connectivity.
WeChat Open Platform Settings
SSID :
ShopID :
AppID :
SecretKey :
Example of Connection Information for a WeChat Official Account:
WeChat Official Account Parameters
Shop Name: Luis Restaurant
SSID : HCD
ShopID : 8888888
AppID : WXC574E8987362
SecretKey : b4de5477edwe889
For how to apply for a WeChat official account, go to https://admin.wechat.com.
WeChat Authentication Page Settings
Shop Name: Enter 64 or less characters
Slide Interval: 2 s
Slide 1: Change Image Delete
Link for Slide 1: http://
Slide 2: Upload Image
Link for Slide 2: http://
Slide 3: Upload Image
Link for Slide 3: http://
Slide Preview:
WeChat Authentication
Authentication-free Host
+Add Delete
Address Type Address Remark Status Operation
No data
OK Cancel

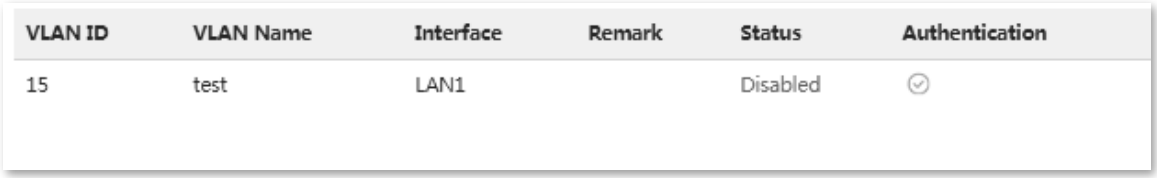
---End

Parameter description

Parameter		Description
WiFi via WeChat		It specifies whether to enable WiFi via WeChat function.
Session Timeout Interval		It specifies the authentication validity period. A user must be re-authenticated for accessing the internet after the period expires.
WeChat Open Platform Settings	SSID	It specifies the wireless network name (AP SSID) of the router that enables WiFi via WeChat, needs to be the same as the SSID in the WeChat open platform.
	ShopID	It specifies the ID of the WeChat open platform shop, needs to be logged in to the WeChat public platform to check.
	AppID	It specifies the unique identifier of the WeChat official account ID. You need to log in to the WeChat open platform to view it.
	SecretKey	It specifies the key used for the encryption in the WeChat official account payment request, which can verify the unique identity of the merchant and must be logged in to the WeChat open platform to check.
WeChat Authentication Page Settings	Shop Name	It allows you to set the shop name.
	Slide Interval	It allows you to set the picture switching period.
	Slide 1/2/3	It specifies the pictures of the authentication page, supports adding up to 3 pictures.
	Link for Slide 1/2/3	It specifies the website to link the picture, which can be an IP address or a domain name.
	Change Image	It allows you to change a picture.
	Delete	It allows you to delete an uploaded picture.
	Upload Image	It allows you to upload a picture.
Authentication-free Host	Address Type	It allows you to set a device without authentication based on IP address or MAC address.
	Address	It specifies the address information for authentication-free. When Address Type is set as IP Address, input the IP address of the authentication-free device. When Address Type is set as MAC Address, input the MAC address of the authentication-free device.
	Remark	It specifies the description of an authentication-free host.
	Status	It specifies whether a rule is enabled.
	Operation	Click + to add a new authentication-free host, and click - to delete the corresponding authentication-free host.

This router supports captive portal based on VLAN. VLAN captive portal can be configured on **Captive Portal > Basic Settings** page if VLAN rules are configured on VLAN Settings page.

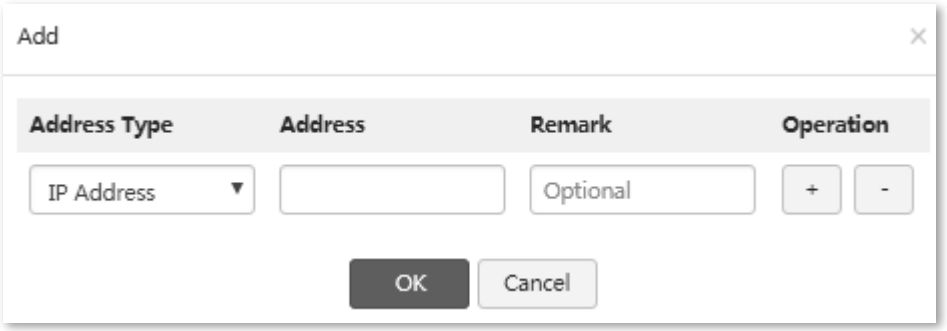
Locate the corresponding VLAN to set up WiFi via WeChat, click , then the users under this VLAN could access the internet with WeChat connection.



Configuring authentication-free host

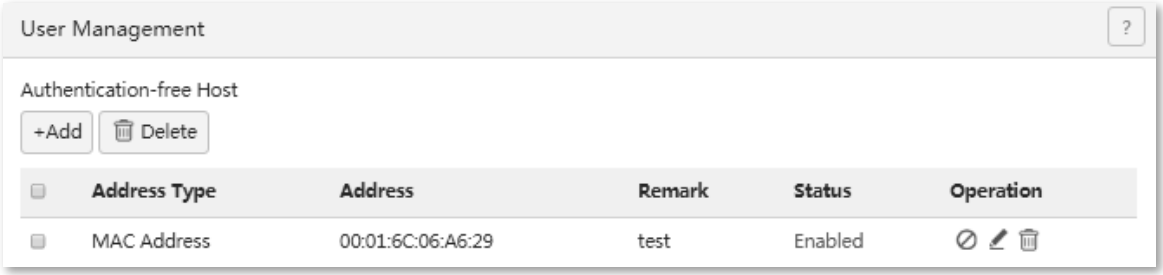
Adding an authentication-free host

1. Choose **WiFi via WeChat** > **User Management**, locate the **Authentication-free Host** module.
2. Click +Add.
3. Set the required parameters.
4. Click **OK**.



---End

The **User Management** page appears, showing the added hosts. See the following figure.



Modifying an authentication-free host

1. Choose **WiFi via WeChat** > **User Management**, locate the **Authentication-free Host** module.
2. Click  corresponding to a host to be modified.

Deleting an authentication-free host

1. Choose **WiFi via WeChat** > **User Management**, locate the **Authentication-free Host** module.
2. Click  corresponding to an entry to be deleted. To delete multiple entries at the same time, select the entries and click  .

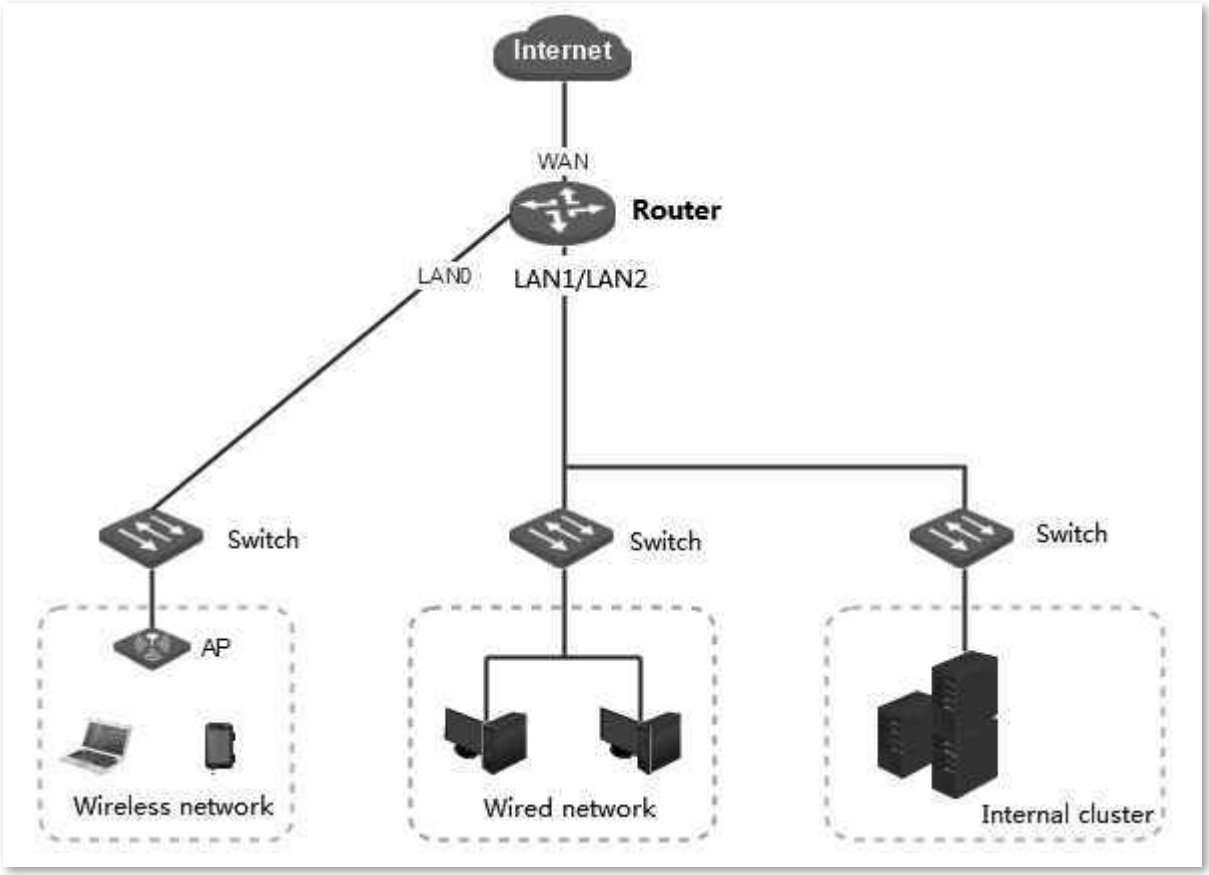
12.3 Example of configuring WiFi via WeChat

Networking requirement

An enterprise uses M80 to set up a LAN with VLAN disabled to address the following requirement:

Hotel managers can access to the wireless network without authentication. Guests need to get authentication via WeChat when connecting to the wireless network. The hotel can send out publicity pictures on the authentication page and ask guests to follow official account ID to realize secondary marketing and increase the number of WeChat fans.

Network topology

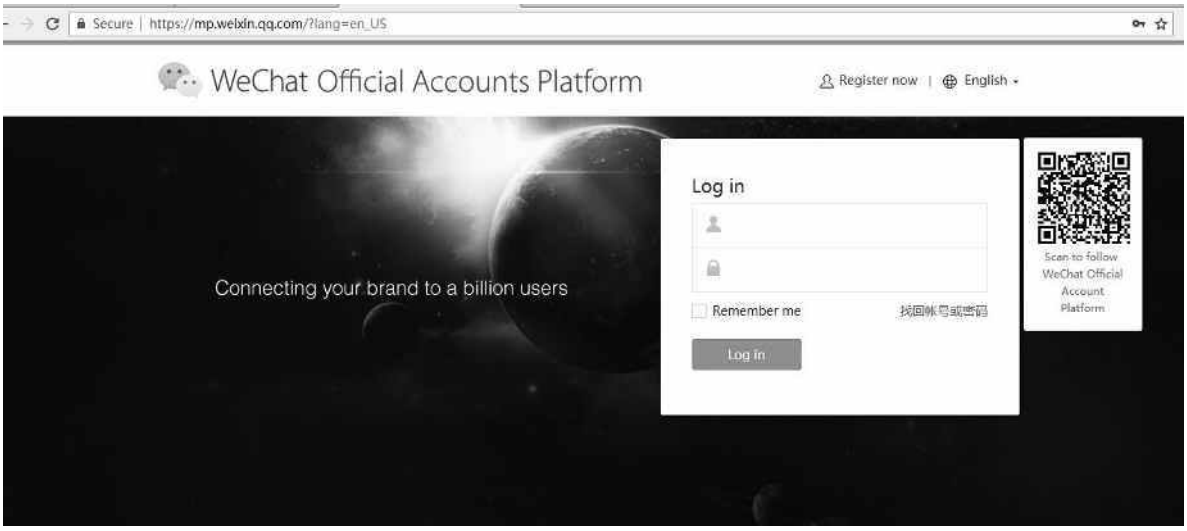


Configuration Procedure

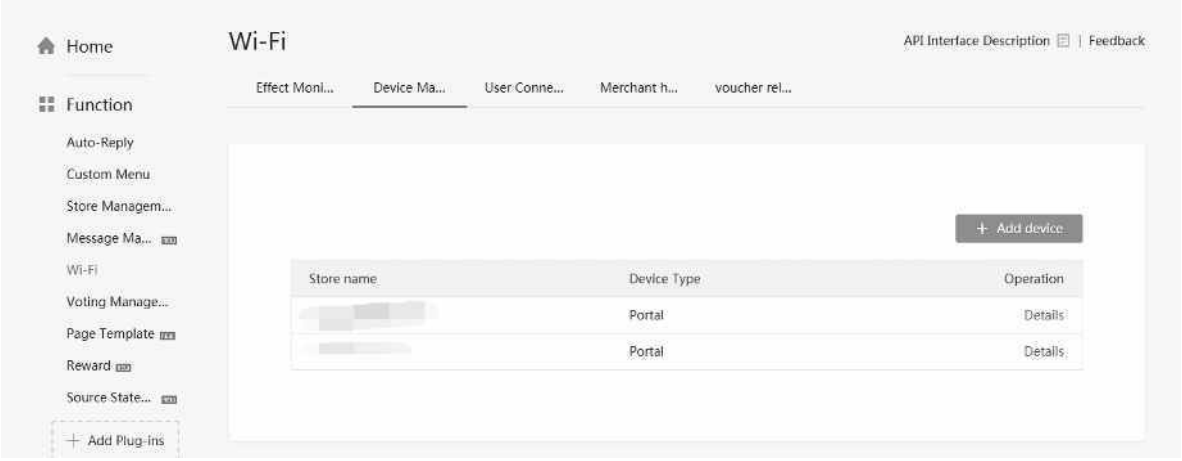
I. Recording WeChat open platform related parameters.

Log in to the WeChat official account to view and record information of SSID, ShopID, AppID, and SecretKey.

1. Start a web browser and visit http://mp.weixin.qq.com, then log in with the WeChat official account and password. If no account, click **Register now** on the following page and follow the on-screen instructions to apply one

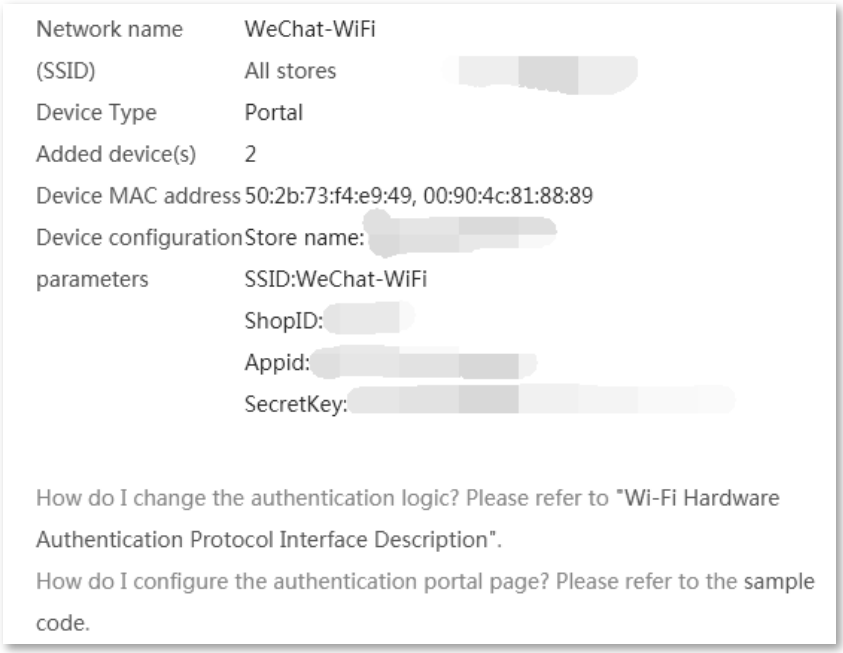


2. Click **WiFi**, and then **Device Management**, click **Details** corresponded to the store name.



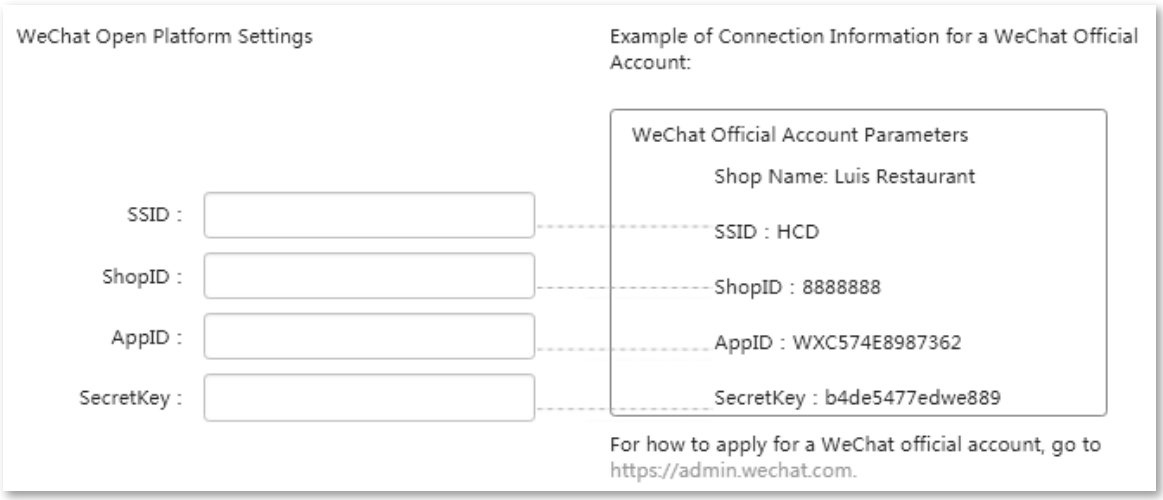
3. Click **Details** corresponded to the store name.

4. Keep parameters of **SSID**, **ShopID**, **Appid** and **SecretKey** to set on the router.

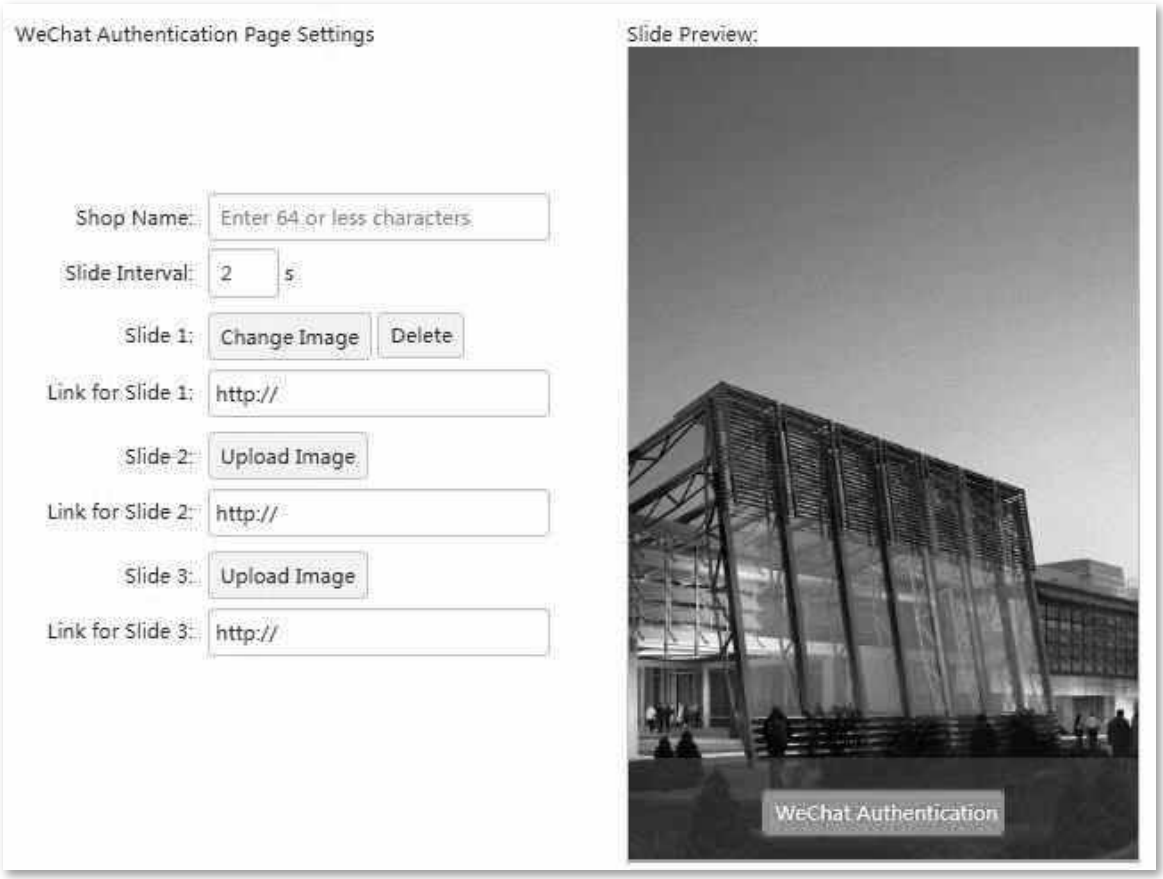


II. Configuring WiFi via WeChat.

1. Choose **WiFi via WeChat**.
2. Set **WiFi via WeChat** to **Enable**.
3. In **WeChat Open Platform Settings** module, set WeChat official account parameters of **SSID**, **Shop ID**, **AppID,** and **SecretKey**.



4. Set **WeChat Authentication Page Settings**.
   (1) Set **Shop Name**.
   (2) Set **Slide Interval**.
   (3) Click Change Image or Upload Image to upload the pictures.
   (4) Set the link for slide 1/2/3.



5. Add Authentication-free Host.

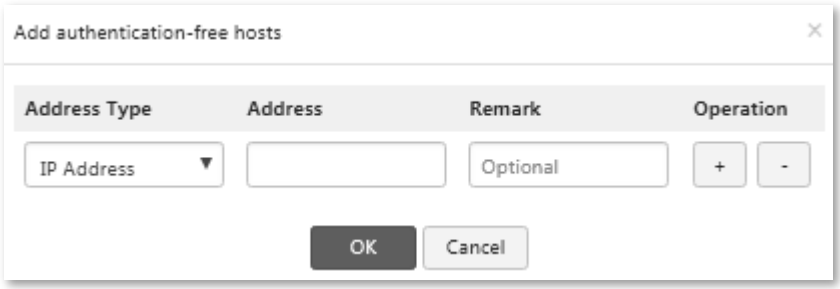
   (1) Click +Add.

   (2) Set **Address Type** to **IP address** or **MAC address** for a device without authentication.

   (3) Set **IP Address** of the client.

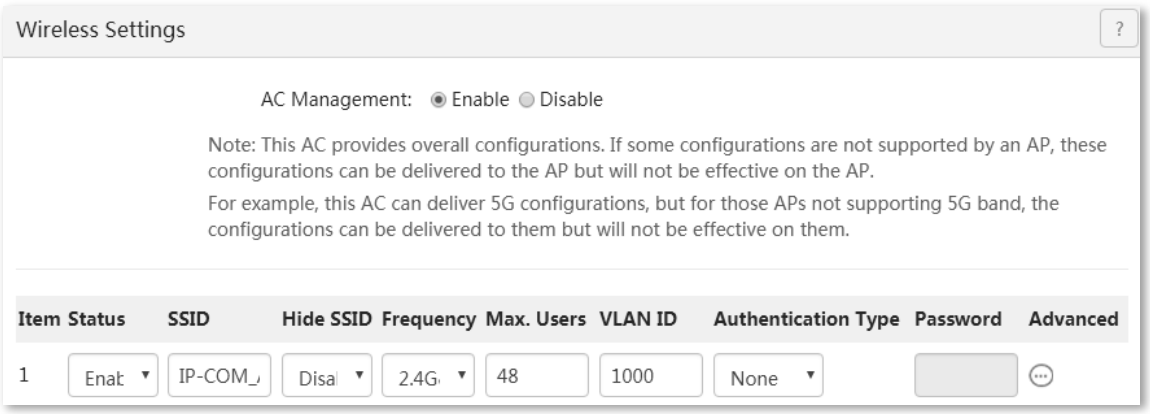
   (4) Set the description of the client.

   (5) Click **OK**.



6. Click **OK** on the **WiFi via WeChat** page.

7. Set **AC Management** to **Enable.** And then set the SSID you want to broadcast. Making sure the **Authentication Type** is set to **None**.



---End

Verification

When wireless clients connect to the wireless network with WiFi via WeChat enabled, users need to get authenticated through WeChat to access the internet.

Procedures for mobile devices (such as smart phones, tablets, etc.) to connect using WiFi via WeChat are as follows:

1. Connect to the wireless network with **WiFi via WeChat** enabled.
2. Open any page on a web browser, it redirects to the user-defined WiFi via WeChat authentication page. For some mobiles, it will automatically display the WiFi via WeChat authentication page when the wireless network is connected. You can force users to follow your Wechat official account so as to increase visibility of your brand and attract fans.

Tip

If the authentication page does not appear, try to access other websites.

3. Click **WeChat Authentication**, and follow the onscreen instructions to access to the internet.

The procedures for a laptop or desktop with a wireless adapter installed to connect WiFi via WeChat are as follows:

1. Connect to the wireless network with **WiFi via WeChat** enabled.
2. Start a web browser and visit any valid website, it redirects you to the authentication page.

Tip

If the authentication page does not appear, try to access other websites.

3. On the WiFi authentication page, click **Connect** to access the internet.

13 Virtual server

13.1 Overview

This chapter describes:

- Port forwarding
- UPnP
- DMZ host
- DDNS

Port forwarding

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

UPnP

UPnP is short for Universal Plug and Play. After you enable this function, the router can detect UPnP-based application programs on local computers and map onto the ports of the programs automatically. In this way, internet users can access these programs. It is generally used for P2P programs, such as BitComet and AnyChat, and helps to increase the download speed.

DMZ host

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

DDNS

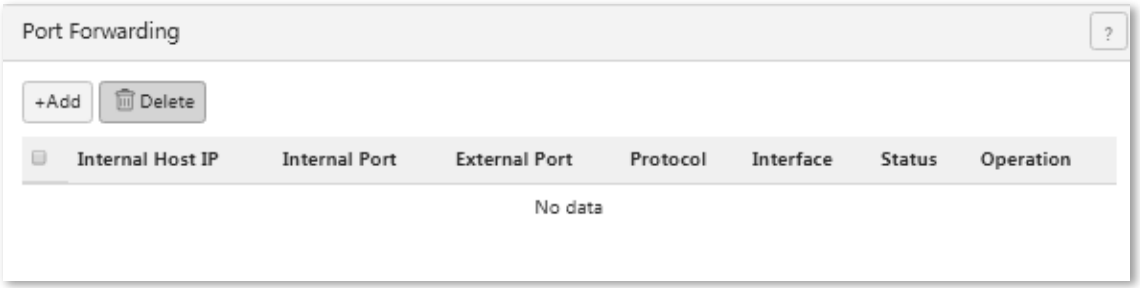
DDNS is short for Dynamic Domain Name Server. When the service is running, the DDNS client on the router sends its current WAN port IP address to the DDNS server. Then the server updates the mapping between the domain name and the IP address in the database to implement dynamic domain name resolution. If you

enable this function, the router sends its WAN IP address to the specified DDNS server when the WAN IP address is changed and the DDNS server maps the changed WAN IP address to a specified static domain name. This enables internet users to access services on your LAN through the static domain name instead of the changeable WAN IP address.

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

13.2 Port forwarding

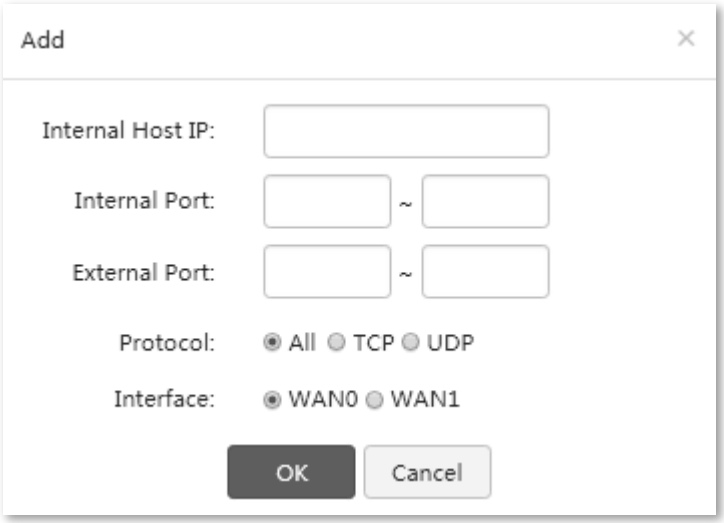
To access the page, choose **Virtual Server** > **Port Forwarding**. The default display is as follows:



13.2.1 Configuring port forwarding

Adding a rule

1. Choose **Virtual Server** > **Port Forwarding**.
2. Click **Add**.
3. Set required parameters.
4. Click **OK**.

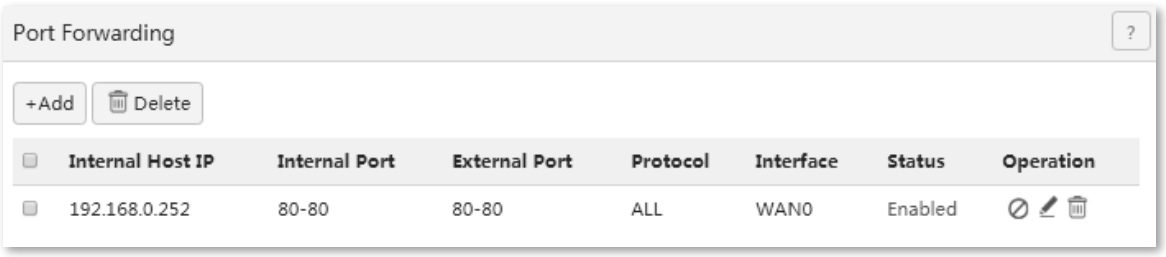


---End

Parameter description

Parameter	Description
Internal Host IP	It specifies the IP address of a local computer that runs a specified service.
Internal Port	It specifies the service port of a server on a local computer.
External Port	It specifies the port for internet users to access a specified service.
Protocol	It specifies the protocol that a specified service uses. **All** indicates that both TCP and UDP are supported. If you are not familiar with the protocols, select **All**.
Interface	It specifies the physical WAN port that internet users use to access the specified service.

The **Port Forwarding** appears, showing the added rule. See the following figure.



Modifying a rule

1. Choose **Virtual Server** > **Port Forwarding**.
2. To modify a rule, click corresponding to the rule.
3. To enable the rule, click . To disable the rule, click .

Deleting a rule

1. Choose **Virtual Server** > **Port Forwarding**.
2. To delete one rule, click corresponding to the rule. To delete multiple rules, select them and click Delete.

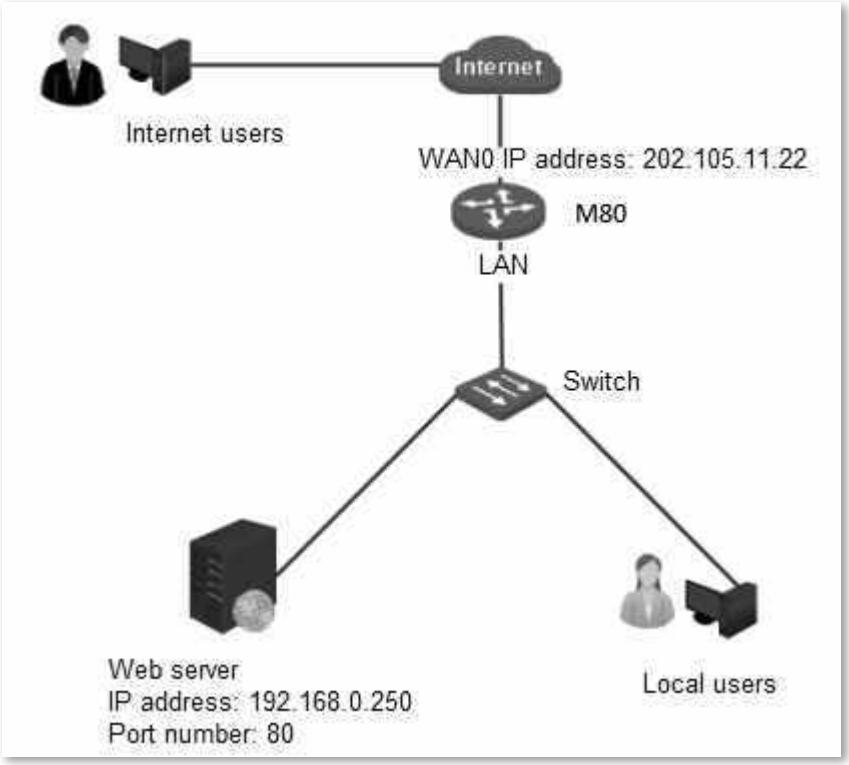
13.2.2 Example of port forwarding

Networking requirement

An enterprise uses M80 to deploy its WLAN network. The router is connected to the internet. Now the enterprise establishes a web server and wants to enable its employees to access the web server through the internet.

You can use the port forwarding function to meet this requirement. Assume that the external port is 80.

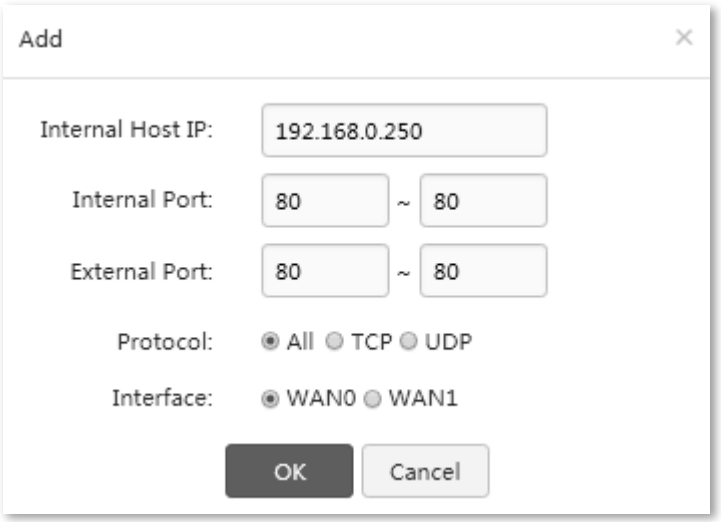
Network topology



Configuration procedure

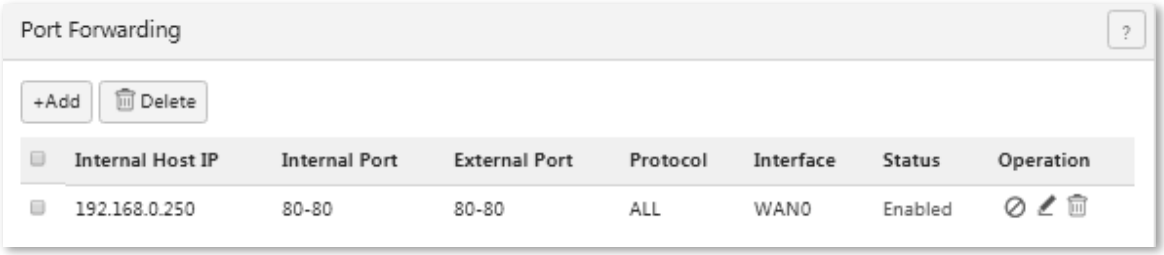
1. Choose **Virtual Server** > **Port Forwarding**.
2. Click **Add**.
3. Set **Internal Host IP** to **192.168.0.250**.
4. Set **Internal Port** to **80**.
5. Set **External Port** to **80**.
6. Set **Protocol** to **TCP** or **All**.
7. Set **Interface** to **WAN0**.

8. Click **OK**.



---End

The following figure shows the added rule.



Verification

Internet users can access the local web server at protocol://WAN IP address:port, which is http://202.105.11.22:80 in this example.

If the router enables the DDNS function, internet users can access the local web server at protocol://WAN domain name:port.

Tip

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

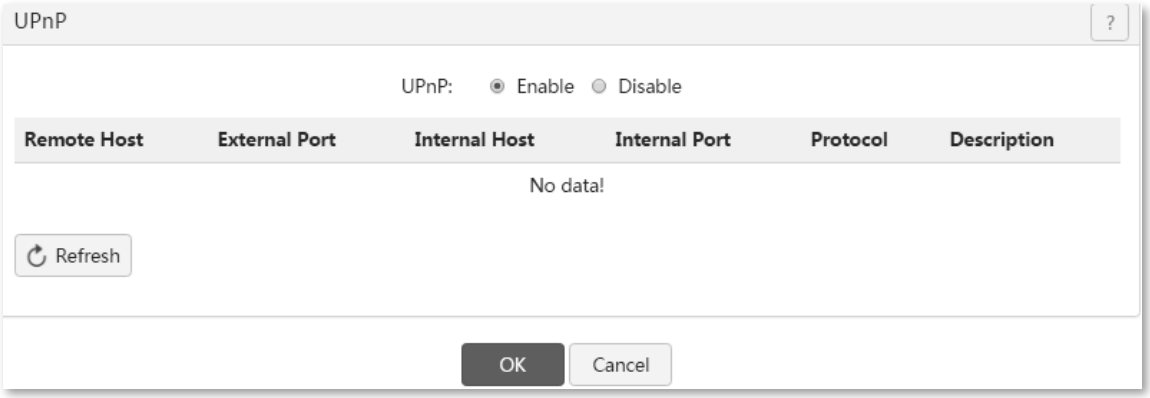
- Make sure that the WAN IP address of the router is a public IP address.
- Make sure that the intranet port number is the service port number on the local host. In this example, it is 80.
- Disable some programs, such as the firewall, anti-virus software, and security guard, which may forbid internet users to access the local service.
- If the IP address of the local host changes, the port forwarding rule is ineffective. To make the rule always effective, set a static IP address for the specified local host.

13.3 UPnP

UPnP is disabled by default of the router.

To enable the function:

1. Choose **Virtual Server** > **UPnP**.
2. Select **Enable** and click **OK**.

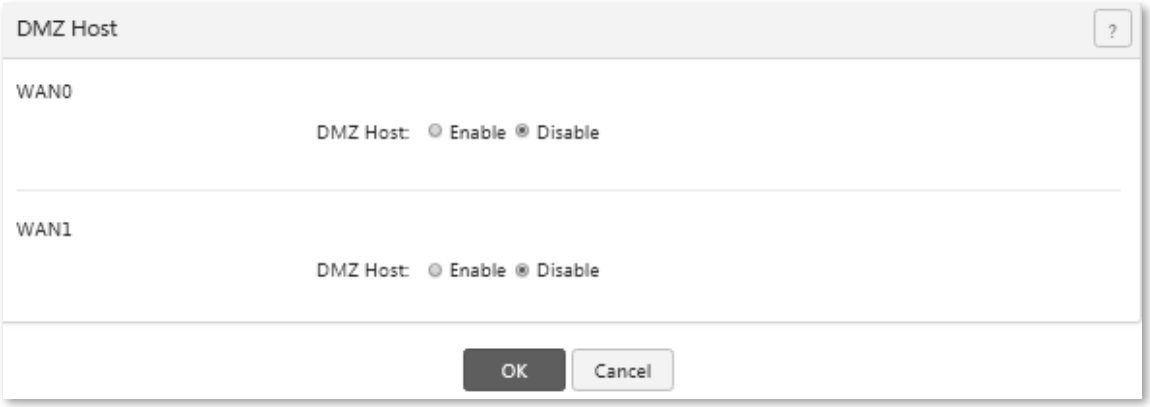


---End

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

13.4 DMZ host

To access the configuring page, choose **Virtual Server** > **DMZ Host**. The default page shows as follows.

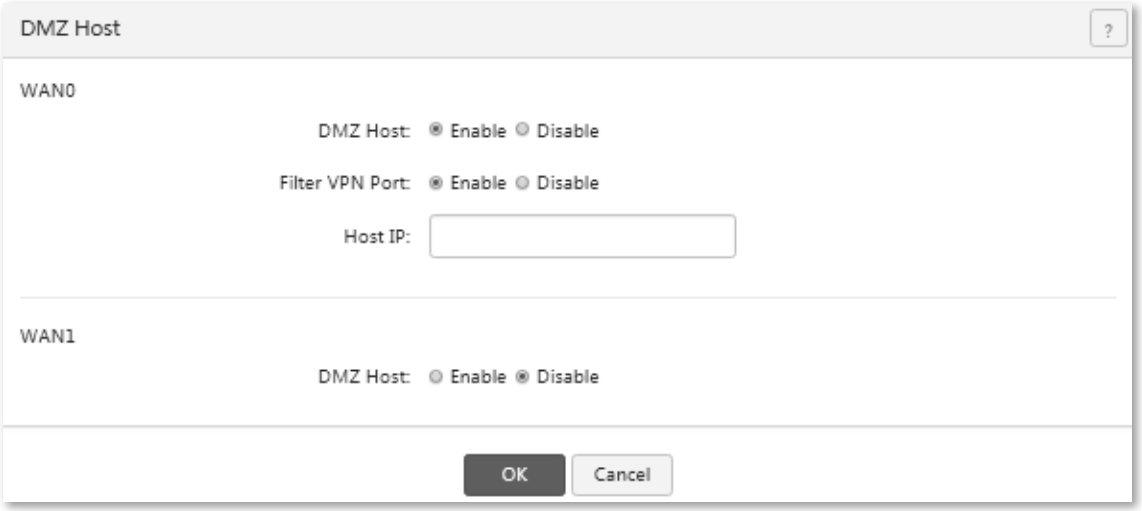


Note

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

13.4.1 Configuring the DMZ host function

1. Choose **Virtual Server** > **DMZ Host**.
2. Set a WAN port to **Enable**.
3. Enter the IP address of the DMZ host accessible to internet users.
4. Click **OK**.



---End

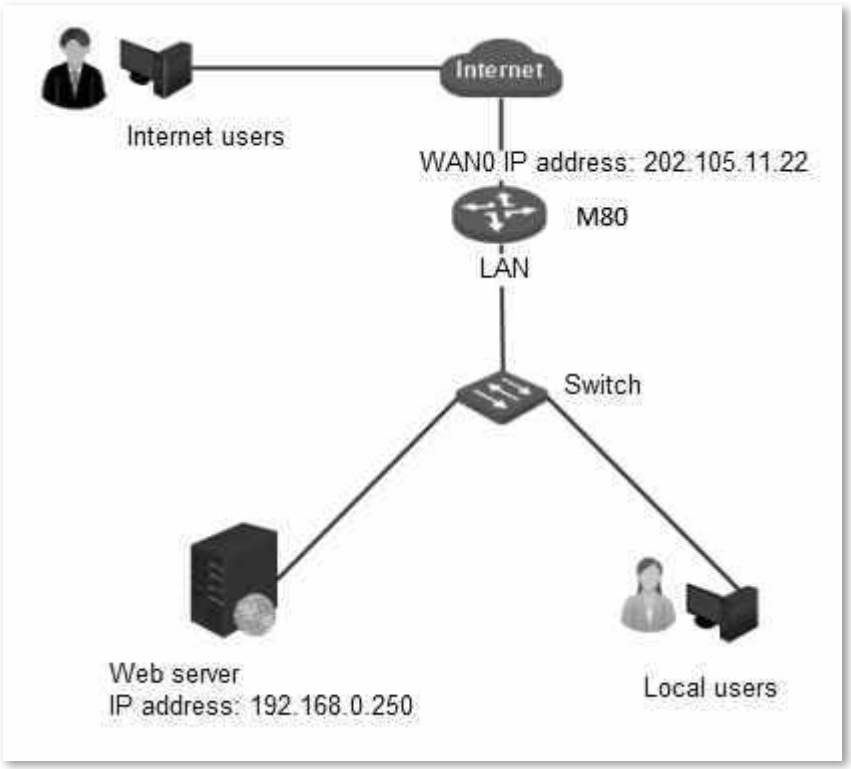
13.4.2 Example of configuring the DMZ host function

Networking requirement

An enterprise uses M80 to deploy its WLAN network. The router is connected to the internet. Now the enterprise establishes a web server and wants to enable its employees to access the web server through the internet.

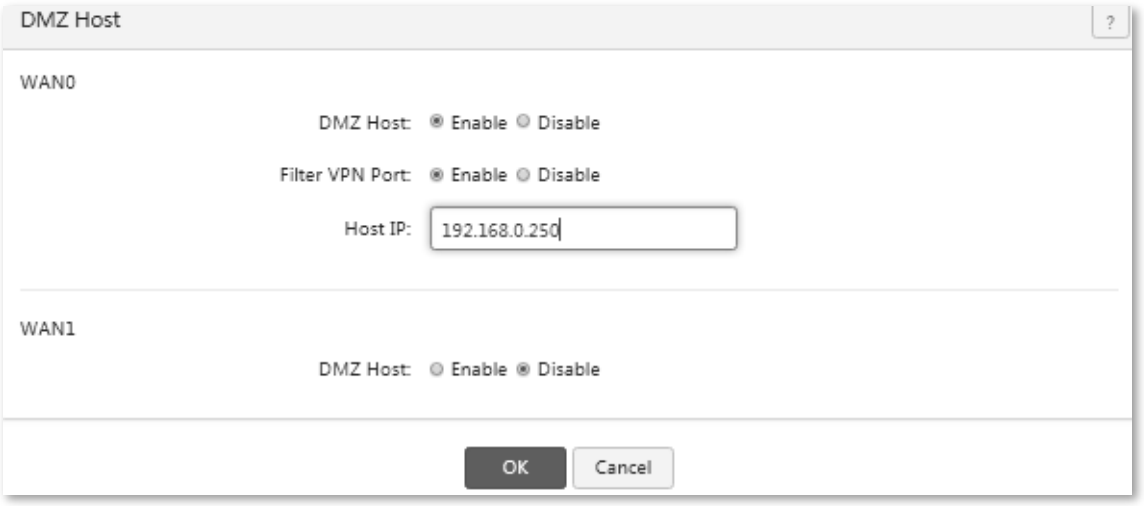
You can use the DMZ function to meet this requirement.

Network topology



Configuration Procedure

1. Choose **Virtual Server** > **DMZ Host**.
2. Set **WAN0** to **Enable**.
3. Set **Host IP** to **192.168.0.250**.
4. Click **OK**.



---End

Verification

Internet users can access the local web server at protocol://WAN IP address:port, which is http://202.105.11.22:80 in this example.

If the router enables the DDNS function and the domain name is ip-com.ddns.net, internet users can access the local web server at protocol://WAN domain name:port.

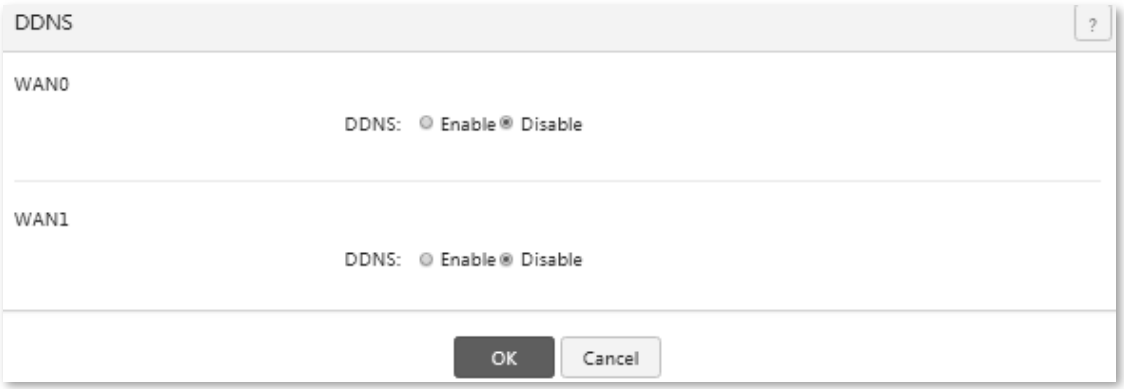
Tip

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

- Make sure that the WAN IP address of the router is a public IP address.
- Disable some programs, such as firewall, anti-virus software, and security guard, which may forbid internet users to access the local service.
- If the IP address of the local host changes, the port forwarding rule is ineffective. To make the rule always effective, set a static IP address for the specified local host.

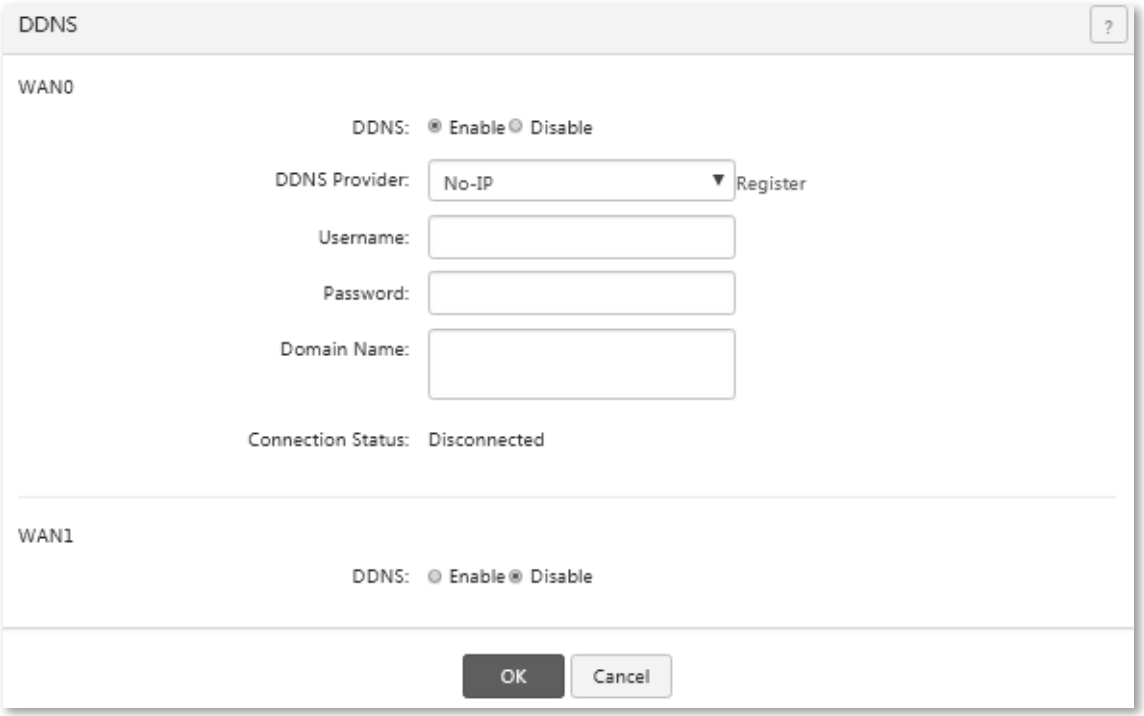
13.5 DDNS

To access the configuring page, choose **Virtual Server** > **DDNS**. The default page shows as follows.



13.5.1 Configuring the DDNS function

1. Choose **Virtual Server** > **DDNS**.
2. Set **DDNS** in the WAN0 or WAN1 area to **Enable**.
3. Set DDNS parameters and click **OK**.



---End

Parameter description

Parameter	Description
DDNS	It specifies whether to enable the DDNS function.
DDNS Provider	It specifies a DDNS provider that can map changeable IP addresses to one static domain name. The router supports the oray.com, gnway.com, DynDNS, and No-IP DDNS providers.
Username	It specifies the login user name of a DDNS provider. You can sign up on a DDNS provider's website to obtain a login user name.
Password	It specifies the login password for a user name assigned by a DDNS provider. You are asked to set a login password when you sign up with the provider.
Domain Name	It specifies the DDNS domain name obtained from a DDNS provider. If your DDNS provider is not oray.com, manually enter the domain name of the DDNS provider. Internet users can use a DDNS domain name to access a specified service.
Connection Status	It indicates whether the router is connected to a DDNS provider.

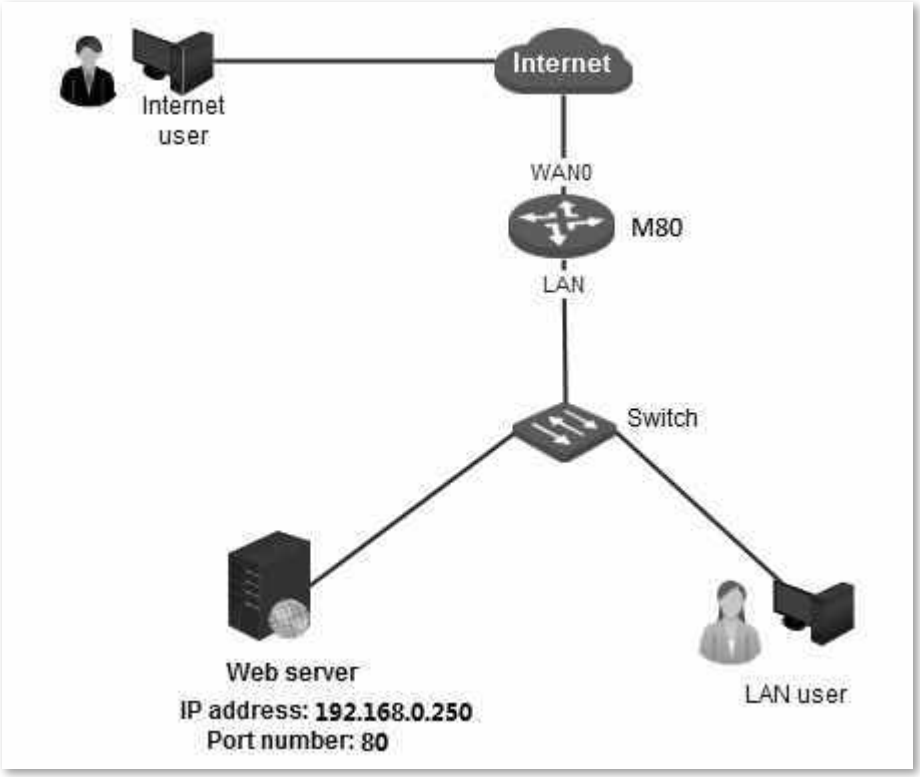
13.5.2 Example of configuring the DDNS function

Networking requirement

An enterprise uses M80 to deploy its WLAN network. The router is connected to the internet. Now the enterprise establishes a web server and wants to be accessed by internet users. Thus when employees are not in the enterprise, they can also access the web server.

You can use Port Forwarding function to meet this requirement (Assume that the external port is 80). In addition, to enable internet users to access the web server using a static domain name instead of a changeable IP address, enable the DDNS function.

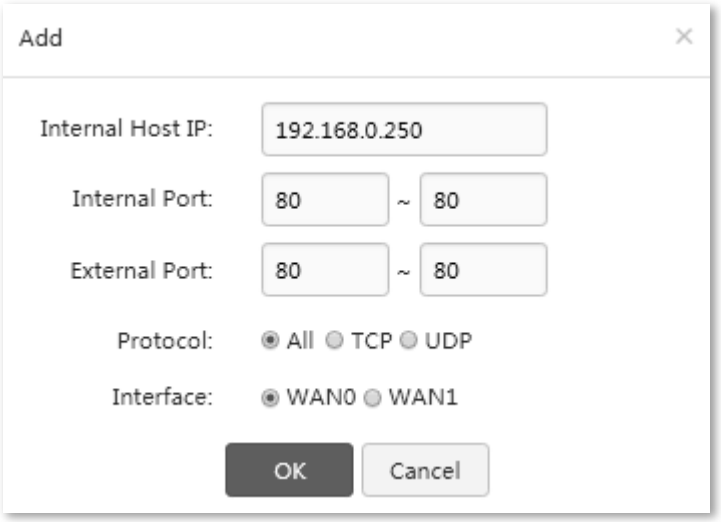
Network topology



Configuration Procedure

I. Configure the port forwarding function.

1. Choose **Virtual Server** > **Port Forwarding**.
2. Click **Add**.
3. Set **Internal Host IP** to **192.168.0.250**.
4. Set **Internal Port** to **80**.
5. Set **External Port** to **80**.
6. Set **Protocol** to **TCP** or **All**.
7. Set **Interface** to **WAN0**.
8. Click **OK**.



II. Configure the DDNS function.

1. Choose **Virtual Server** > **DDNS**.
2. Set **DDNS** to **Enable** in the **WAN0** area and select a DDNS provider, such as **No-IP**.
3. Click **Go to register**, sign up, set a password, and apply for a domain name.

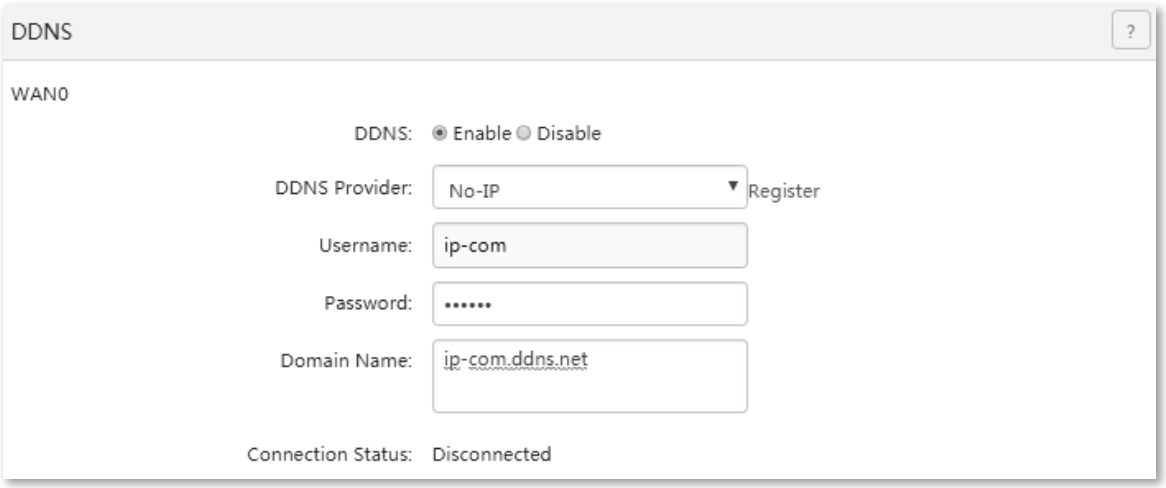
   Assume that the DDNS information is as follows:

   User name: ip-com
   Password: 123456
   Domain name: ip-com.ddns.net
4. Set **Username** to **ip-com**.
5. Set **Password** to **123456**.
6. Set **Domain Name** to **ip-com.ddns.net**.

Tip

If your DDNS provider is **oray.com**, there is no need to set **Domain Name.**

7. Click **OK**.



When you complete the configuration, refresh the page and wait a moment. When the router is connected to the DDNS provider, the connection status changes to **Connected**.

Verification

Verify that internet users can access the local web server at http://ip-com.ddns.net:80.

Tip

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

- Make sure that the WAN IP address of the router is a public IP address.
- Make sure that the intranet port number is the service port number on the local host. In this example, it is 80.
- Disable some programs, such as firewall, antivirus software, and security guard, which may forbid internet users to access the local service.
- If the IP address of the local host changes, the port forwarding rule is ineffective. To make the rule always effective, set a static IP address for the specified local host.

14 USB

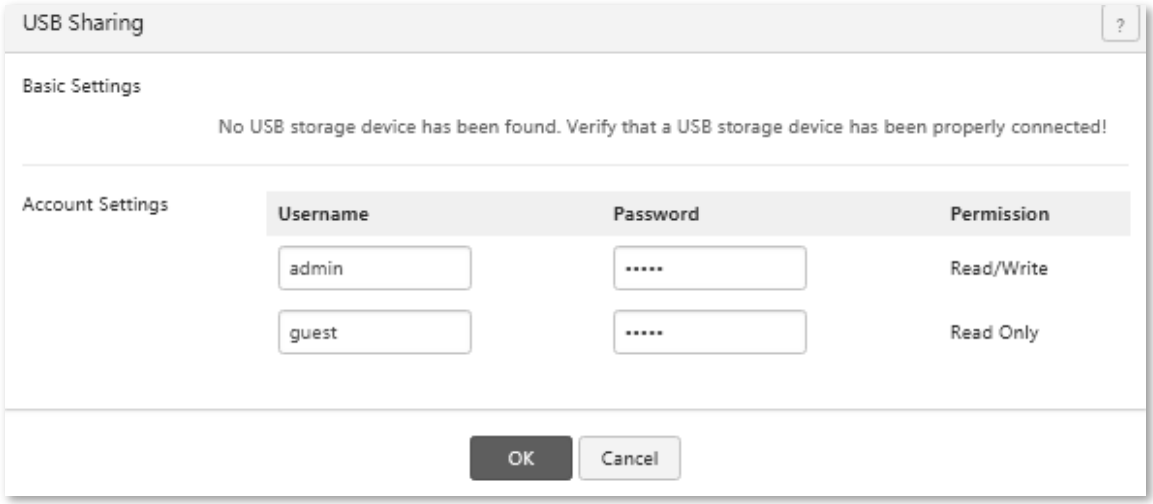
14.1 Overview

The router provides a USB interface that supports USB sharing.

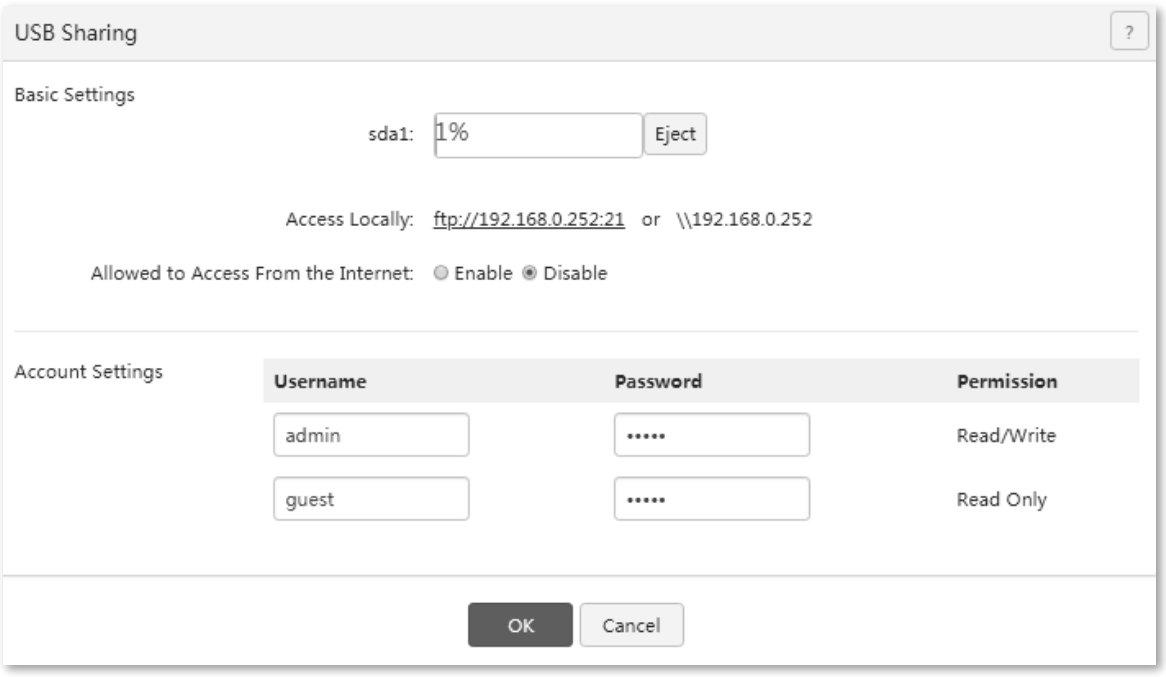
The router can automatically identify the USB storage device that is plugged into its USB interface, and displays information such as the disk usage of the USB device on the web UI. Users in the network can share files on the USB storage device. The router supports file access permission management.

14.2 USB sharing

To access the configuration page, choose **USB > USB Sharing.**



The router can automatically identify the USB disk information when the USB device is plugged in, as shown in the following figure.



Parameter description

Parameter	Description
sda1	It displays usage of the device when a USB storage device is plugged in.
Eject	Click **Eject** before unplugging the USB device in case of losing data.
Access Locally	It specifies the website to access the files of the USB storage device locally. – Click **ftp://192.168.0.252:21** to access the USB storage, or copy the link to a browser. – Copy and paste**\\192.168.0.252** to your computer's **Start > Run** menu to access. – Start a file browser, copy and paste **\\192.168.0.252** to the address bar and press **Enter**, then enter username and password to access. Tip **192.168.0.252** is the current LAN IP address of the router. If the router's LAN IP address changes, the local access address will change accordingly.
Allowed to Access From the internet	It specifies whether to enable allowed to access from the internet. It allows users to access the files of the USB storage device when it is enabled. And the address to access from the internet shows automatically. Accessing the files of the USB storage device is not allowed for internet users when set to disable. It is disabled by default.
Access From the internet	It specifies the address to access the USB storage device from the internet when **Allowed to Access From the internet** is set to **Enable**.
Username/Password	It specifies the username and password to access the USB storage device.
Permission	It specifies the permission for the account to access the USB storage device. It allows users to view and modify the files on the USB storage device when set to **Read/Write**. Default username and password are both **admin**. It allows users to view only the files on the USB storage device when set to **Read Only**. Default username and password are both **guest**.

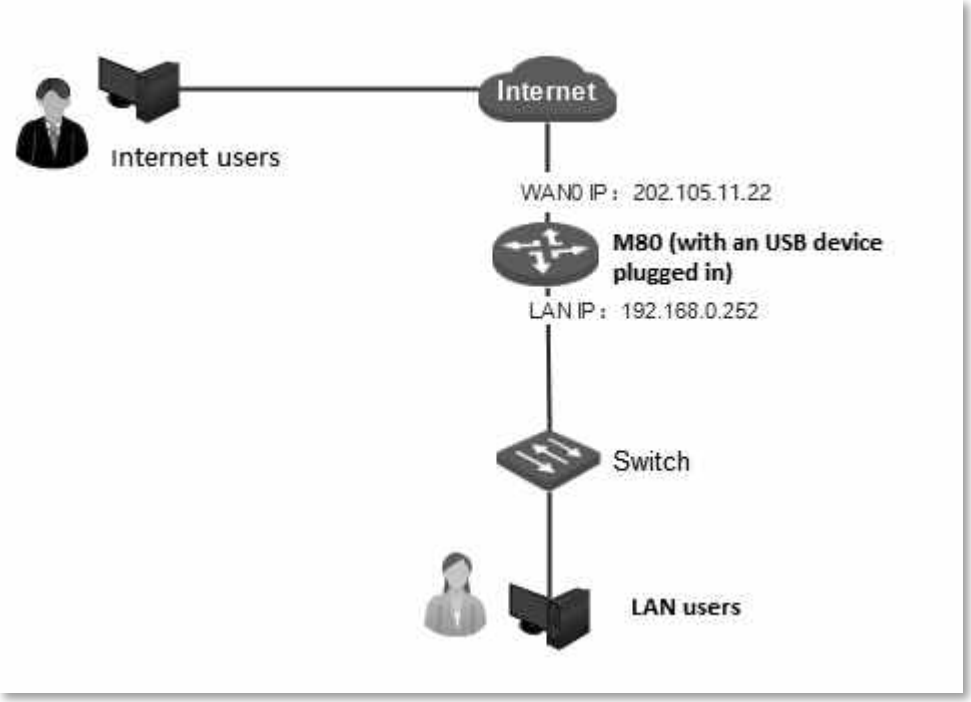
14.3 Example of configuring USB sharing

Networking requirement

An enterprise uses M80 to deploy its LAN network, and connects an USB device to the USB port of M80 as the server, thus both local and internet employees can search and download files via accessing the USB device.

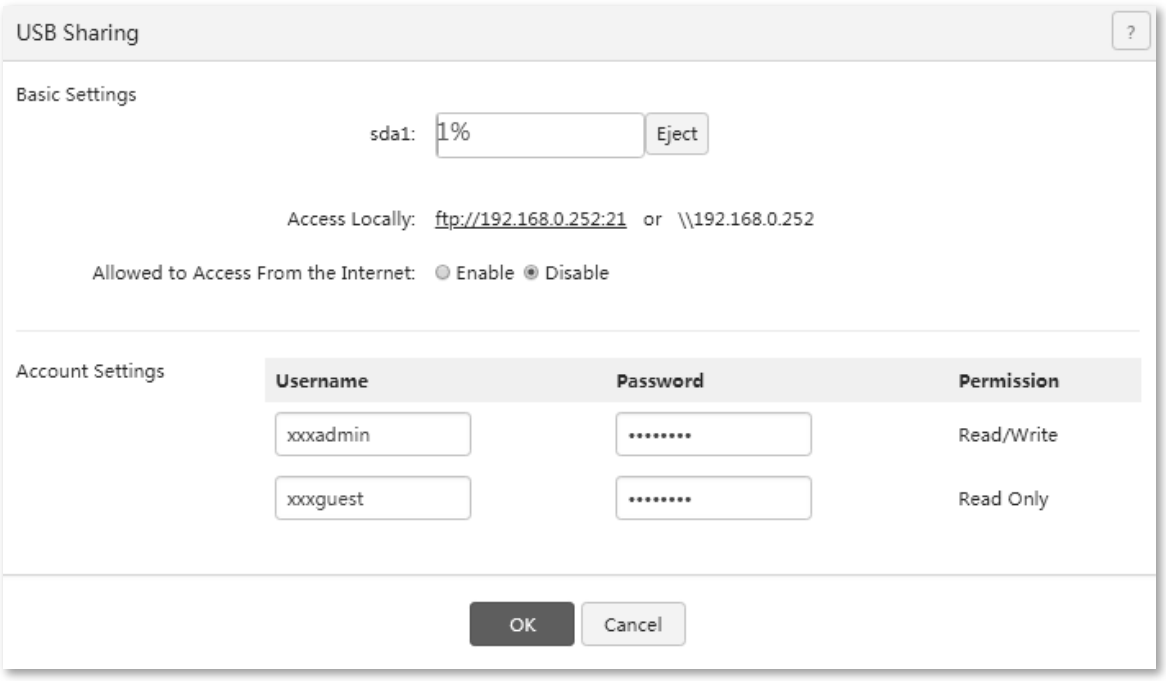
Assume that the username and password of the account with **Read/Write** permission are **xxadmin**/**xxadmin**; while the account with **Read Only** permission are **xxguest/xxguest**.

Network topology



Configuring procedure

1. Choose **USB** > **USB Sharing**.
2. Set **Allowed to Access From the internet** to **Enable.**
3. Set **username** and **password** to **xxxadmin** for read/writer users, and **xxxguest** for read-only users.



---End

Verification

Access the server for local users:

Method 1: Access the link ftp://192.168.0.252:21 on a browser.

Method 2: Access the link \\192.168.0.252 on the lower left corner of the computer. Take windows 10 as an example, click **Windows**, input \\192.168.0.252 in the search bar, and then press **Enter** on your keyboard. Log in to the server with the corresponding username and password.

Access the server for internet users:

Access the link ftp://202.105.11.22:21 on a browser. The username/password authentication page appears, log in to the server with the corresponding username and password.

15 Maintenance

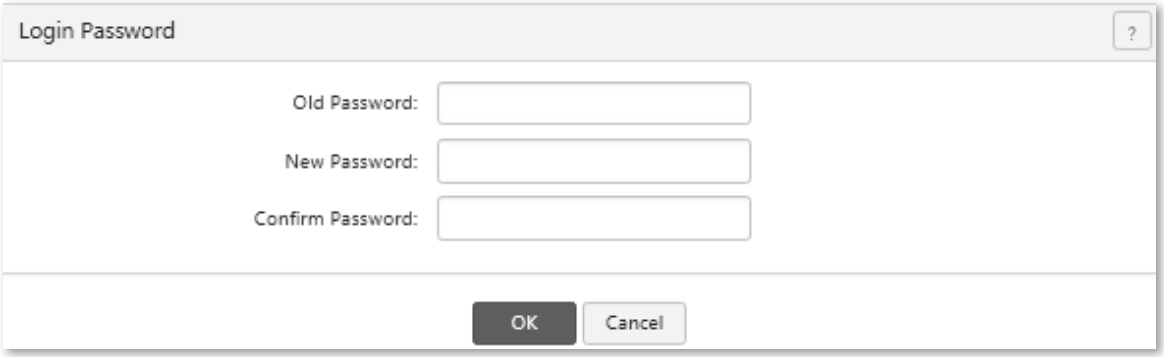
This chapter describes:

- Setting login passwords
- Rebooting the router
- Backing up and restoring configuration
- Upgrading the firmware
- Restoring the factory settings
- Setting the system date and time
- Remotely managing the router using the web UI
- Diagnostics

15.1 Setting login password

You can change the login password on **Login Password** page. When using the router for the first time, you need to set the login password.

To access the page for changing the login password of the router, choose **Maintenance** > **Login Password**.



15.1.1 Modifying login password

1. Click **Maintenance** > **Login Password**.
2. Enter your old password.
3. Set up your new password.
4. Enter the new password again to confirm password.

5. Click **OK**.

---End

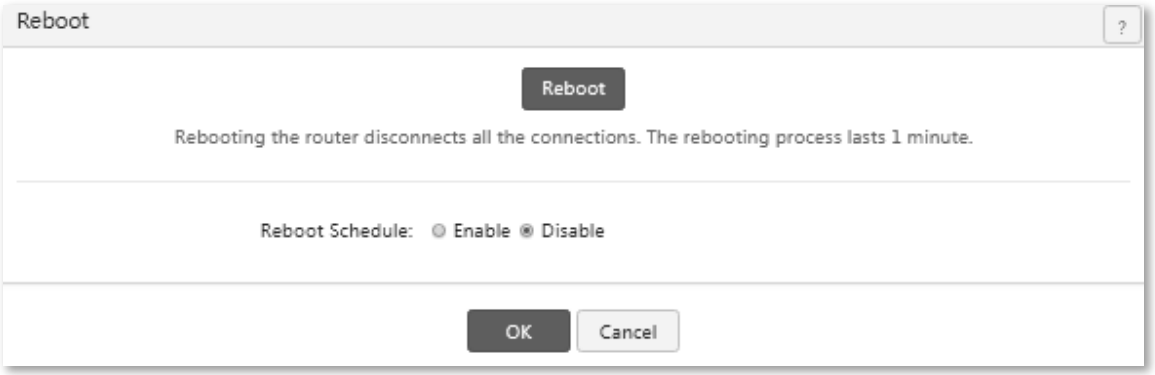
After the configuration completes, the router redirects to the login page. Login to the web UI of the router with the new password you set.

15.2 Rebooting the router

To access the page for rebooting the router, choose **Maintenance** > **Reboot**.

When some manually set parameters do not take effect, try rebooting the router.

In addition, you can enable the Reboot Schedule function to maintain the performance and stability of the router.



15.2.1 Rebooting the router manually

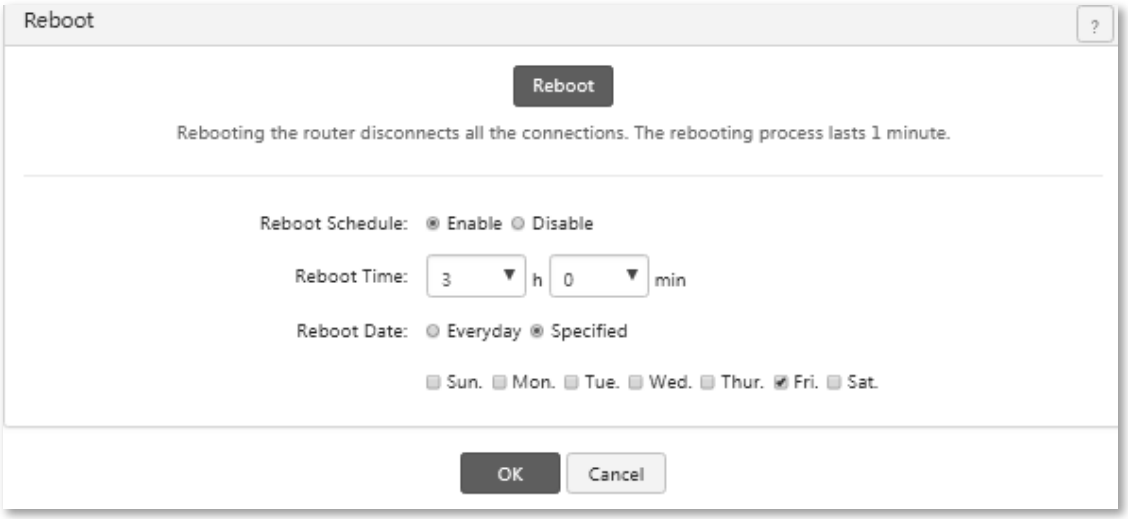
1. Choose **Maintenance** > **Reboot**.
2. Click **Reboot** and follow the onscreen instruction to reboot the router.

15.2.2 Rebooting the router regularly

Configuring procedure

1. Choose **Maintenance** > **Reboot**.
2. Set **Reboot Schedule** to **Enable**.
3. Set **Reboot Time** to a time when the router is rebooted, which is **3:00** in this example.
4. Set **Reboot Date** to **Everyday** or **Specified**, which is **Friday** in this example.

6. Click **OK**.



---End

Verification

The router will reboot at 3:00 every Friday.

Tip

To enable this function to work properly, ensure that the system time of your router is correct. For system time configuration, refer to Setting the system time.

15.3 Backing up and restoring configuration

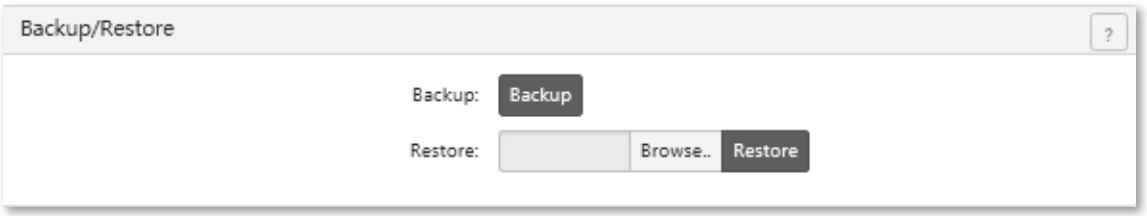
The backup function is used to export the current configuration of the router to your computer.

Restore function is used to import a configuration file to the router.

It is recommended that you 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 a configuration that has been backed up.

To access the configuring page, choose **Maintenance > Backup/Restore.**



15.3.1 Backing up a configuration

1. Choose **Maintenance** > **Backup/Restore**.
2. Click **Backup** and follow the onscreen instruction to back up the configuration.

---End

15.3.2 Restoring a configuration

1. Choose **Maintenance** > **Backup/Restore**.
2. Click **Browse** and upload a configuration file.
3. Click **Restore** and follow the onscreen instruction to restore the configuration.

---End

15.4 Upgrading the firmware

This function enables you to upgrade the firmware to obtain the latest functions or enable the router to perform more stably. The router supports local firmware upgrade and online firmware upgrade. The latter is the default method.

- **Local**: Go to http://www.ip-com.com.cn to download the latest firmware applicable to M80 to your local computer, and upgrade manually.
- **Online**: When the router is connected to the internet, it checks whether there is a later firmware version, and displays the detected information on the page. You can choose whether to upgrade the firmware with the version. If you want to upgrade the firmware, click **Upgrade** and the router upgrades the firmware automatically.

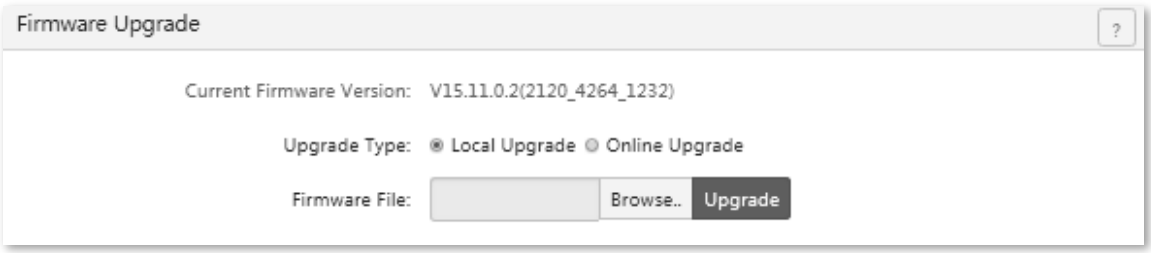
The following section describes local upgrade.

Note

To enable your router to work properly after an upgrade, ensure that the firmware used to upgrade the firmware is applicable to the router. When you are upgrading a firmware, do not power off the router.

To upgrade a firmware:

1. Go to www.ip-com.com.cn and download a firmware version of the router to your computer.
2. Go to the web UI of the router, and choose **Maintenance** > **Firmware Upgrade**.
3. Set **Upgrade Type** to **Local**.
4. Click **Browse** and upload the firmware applicable to the router.
5. Click **Upgrade** and follow the onscreen instruction to upgrade the firmware.



---End

To check if ungrade is successful, go to page **Maintenance** > **Firmware Upgrade** and check the current firmware version.

Tip

For better performance of the new firmware, when the upgrading completes, we recommend that you reset the router to factory default settings and re-configure the router.

15.5 Restoring the factory settings

When you are unable to find a solution to an internet access failure, or forget the login user name or password, you can reset the router to restore its factory settings on the web UI or using the RESET button.

After the router is restored to its factory defaults, you can log in to the router using the following information:

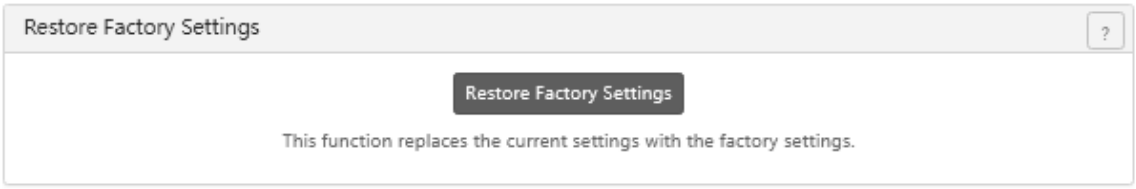
- **IP address**: 192.168.0.252
- **Username**: admin
- **Password**: admin

Note

- You are not recommended to restore the factory settings of the router, as that leads to the loss of the current configuration. After the factory settings are restored, you need to re-configure the router.
- To ensure that the router can work properly after being reset, do not power off the router when it is being reset.

15.5.1 Resetting the router using web UI

1. Choose **Maintenance** > **Restore Factory Settings**.
2. Click **Restore Factory Settings** and follow the onscreen instruction to reset the router.



15.5.2 Resetting the router using the RESET button

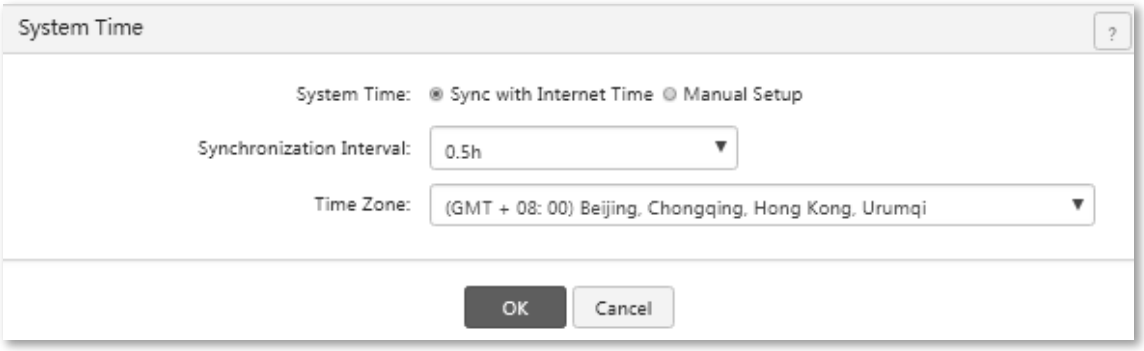
There is no need to log in to the web UI of the router if you use this method.

1. After the router is powered on, use a needle to hold down the RESET button for about 8 seconds.
2. Wait about 1 minute for the router to restore the factory settings.

15.6 Setting the system time

This function is used to set the system time of the router. To make the time-related functions effective, ensure that the system time of the router is set correctly. You can synchronize the system time of the router with the internet or manually set the time. The former is the default method.

To access the configuring page, choose **Maintenance > System Time**.



15.6.1 Synchronizing the system time with the internet

In this method, the system time of the router synchronizes its system time with the time servers on the internet. As long as the router is connected to the internet, the system time is correct, even after the router reboots.

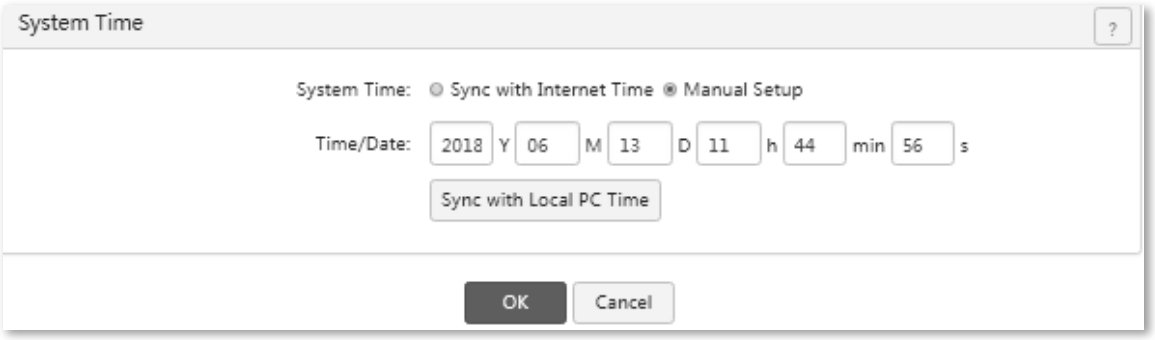
Parameter description

Parameter	Description
Synchronization Interval	It specifies an interval at which the router synchronizes its time with the time server on the internet.
Time Zone	It specifies the time zone where the router is deployed.

After you finish the configuration, you can choose **System Status**> **System Info** and move to **System Info** section to check whether the system time is correct.

15.6.2 Customizing the system time

In this method, you can specify a system time for the router. If the router reboots, you need to re-configure the system time. When you choose **Manual Setup**, the related parameters are shown as follows.



Parameter description

Parameter	Description
Time/Date	It specifies the system time of the router.
Sync with Local PC Time	It allows you to synchronize the system time of the router with the system time of the local PC. If you do not want to enter a system time, click this button to synchronize the time of the router with the management computer to the router.

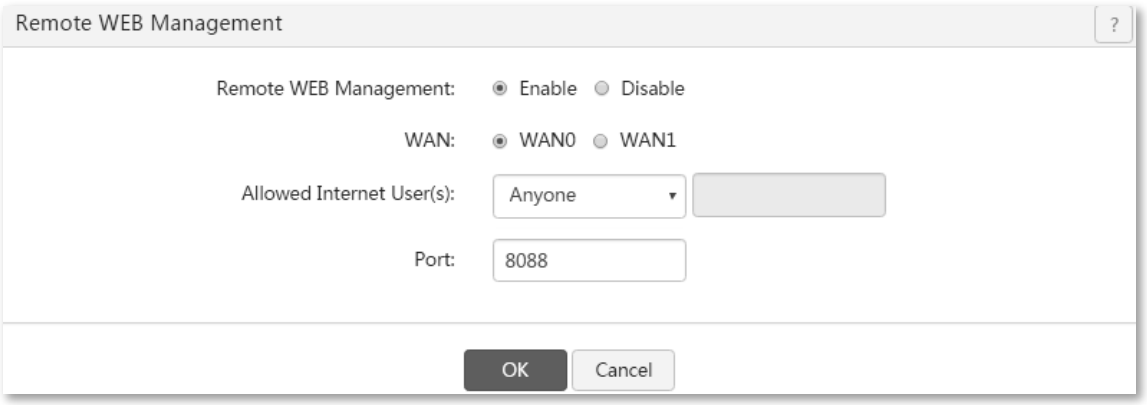
After you finish the configuration, you can choose **System Status** > **System Info** and move to the **System Info** section to check whether the system time is correct.

15.7 Remotly managing the router using the web UI

By default, only local computers that are connected to the router through LAN ports can access the web UI of the router. In special cases, such as remote technical support, you can enable this function and access the web UI through a WAN port.

15.7.1 Configuring remote web management

1. Choose **Maintenance** > **Remote WEB Management**.
2. Set **Remote WEB Management** to **Enable**.
3. Select a WAN port.
4. Set **Allowed internet User(s)** to **Anyone** or **Specified IP**.
5. Set **Port** to a port for accessing the web UI.
6. Click **OK**.



---End

Parameter description

Parameter	Description
Remote WEB Management	It specifies whether to enable the remote management function.
WAN	It specifies a WAN port that is used to access the web UI.
Allowed Internet User(s)	– **Anyone**: It indicates that all internet users can access the web UI. For security of your network, you are not recommended to select this option. – **Specified IP**: It indicates that only the specified public IP address can access the web UI. If you want a computer on a remote network to access the web UI of the router, enter the public IP address of the gateway of the computer.
Port	It specifies a port that is used to access the web UI. By default, it is **8088**. Ports 1 to 1024 are reserved for common services. To avoid port conflicts, it is recommended that

Parameter	Description
	you enter a port number from 1025 to 65535. When you complete the configuration, internet users can access the web UI at http://WAN IP address:Port number. If the DDNS function is enabled for the WAN port, internet users can access the web UI at http://WAN domain name:Port number.

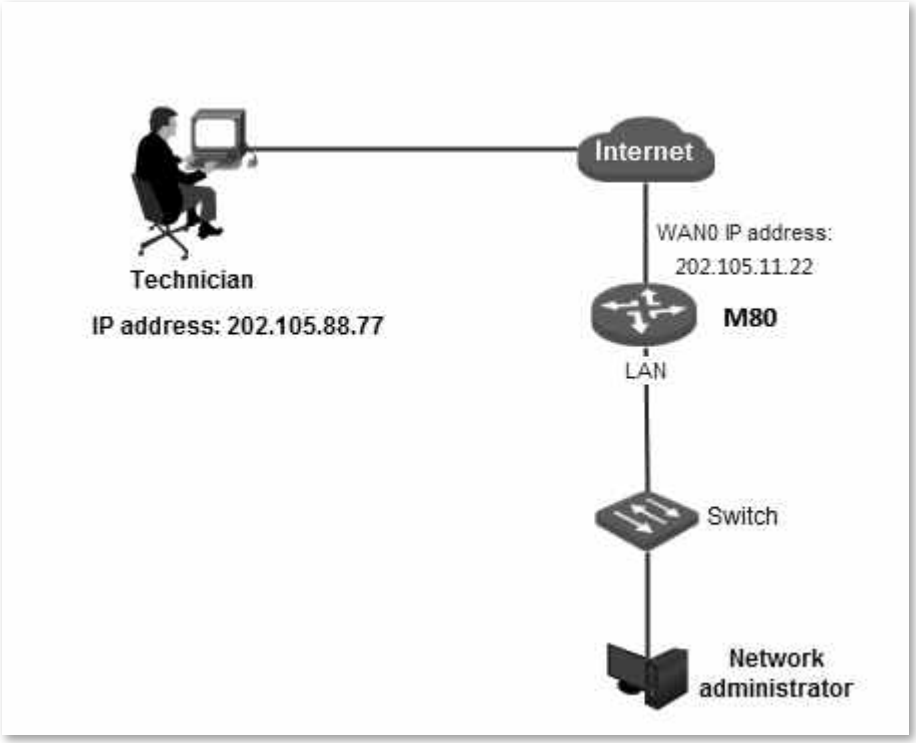
15.7.2 Example of configuring remote web management

Networking requirement

An enterprise uses M80 to deploy its WLAN network. When the network administrator of the enterprise cannot resolve a problem, he/she needs an IP-COM technician to remotely access the web UI of the router to resolve the problem.

You can use the remote web management function to meet this requirement.

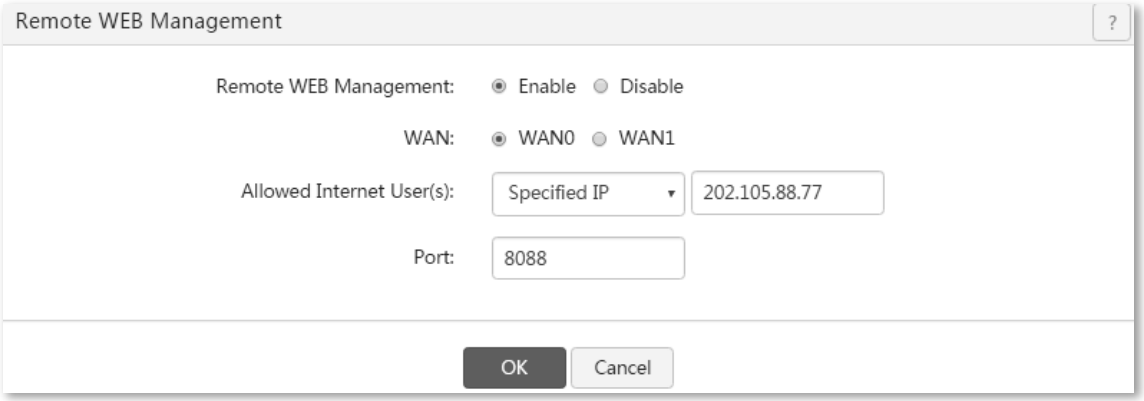
Network topology



Configuration Procedure

1. Choose **Maintenance** > **Remote WEB Management**.
2. Set **Remote WEB Management** to **Enable**.

3. Set **WAN** to **WAN0**.
4. Set **Allowed Internet User(s)** to **Specified IP** and enter the IP address **202.105.88.77** of the technician.
5. Keep the default value of **Port** or enter another value.
6. Click **OK**.

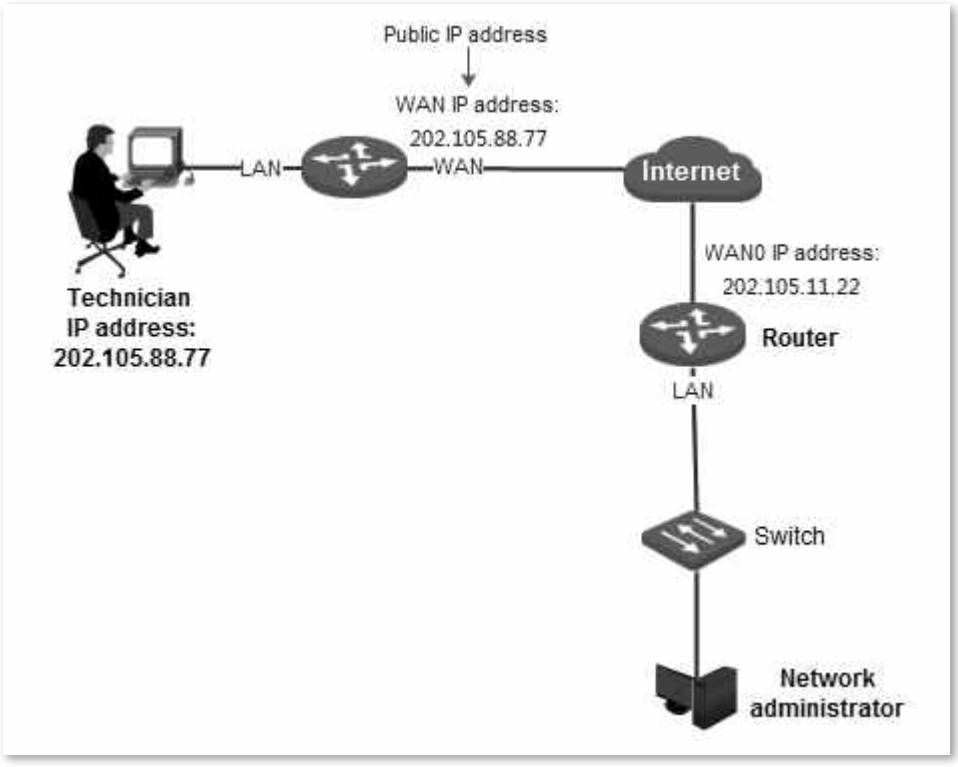


---End

Verification

The IP-COM technician (computer's IP address is 202.105.88.77) can use http:// 202.105.11.22:8088 to access the web UI of the router.

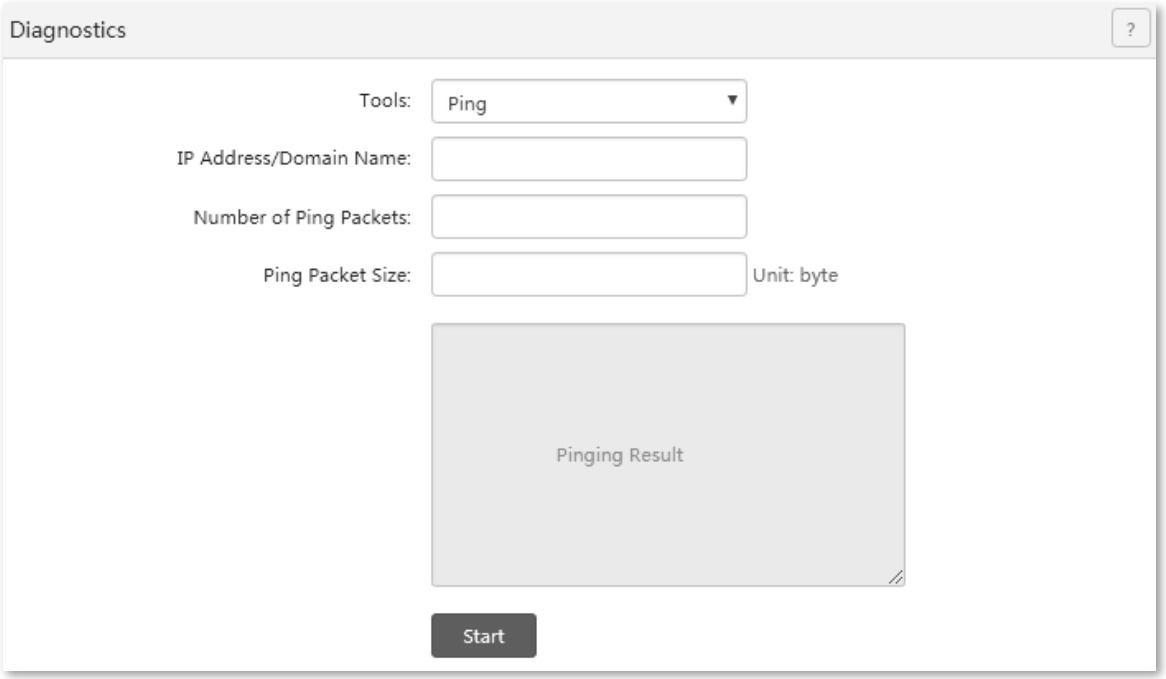
If the technician is on a remote LAN, as shown in the following figure, a public IP address of the router is required for the technician to connect to the router. A private IP address is not applicable. In this case, set **Allowed Internet User(s)** to the WAN IP of M80.



15.8 Diagnostics

15.8.1 Overview

If the network connection fails, you can use the diagnostics tool to check the connection status. To access the page, choose **Maintenance > Diagnostics**.



Parameter description

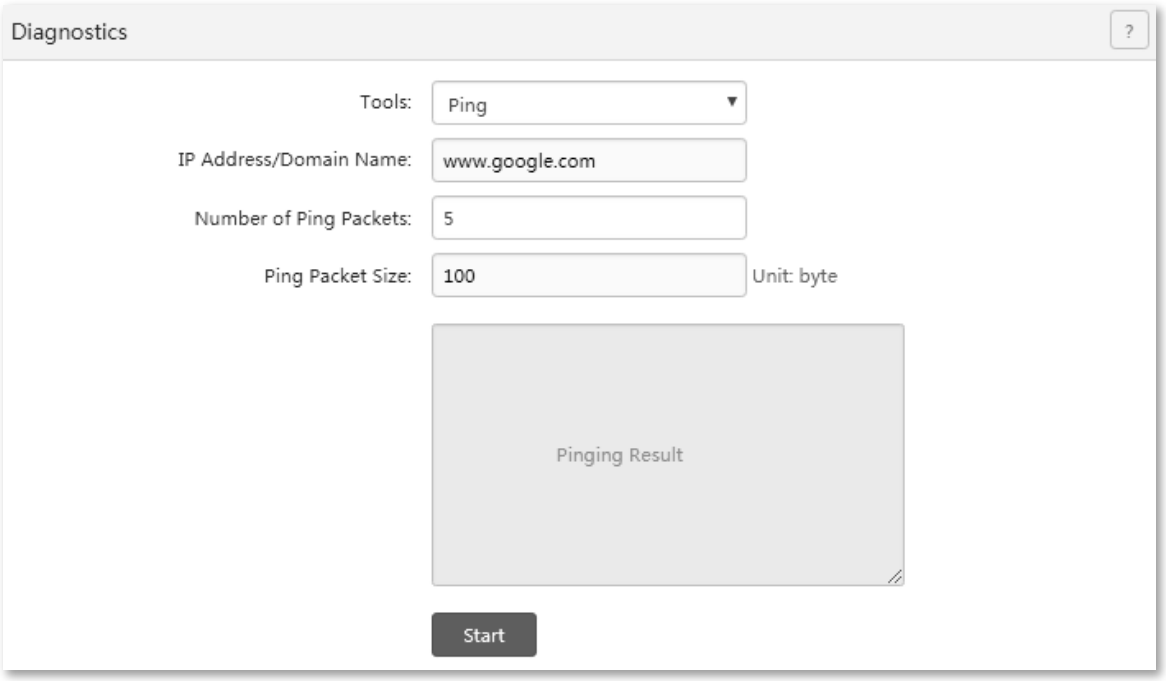
Parameter	Description
Ping	Common commands for troubleshooting. It consists of a set of ICMP echo request messages. If the network is running normally, it will return a set of response reply packets.
Traceroute	A route tracing utility that determines the path taken by the IP data access target.

15.8.2 Ping test procedure

The ping function can detect network connectivity. Assume that you need to detect the connectivity between the router and Google, refer to the following settings.

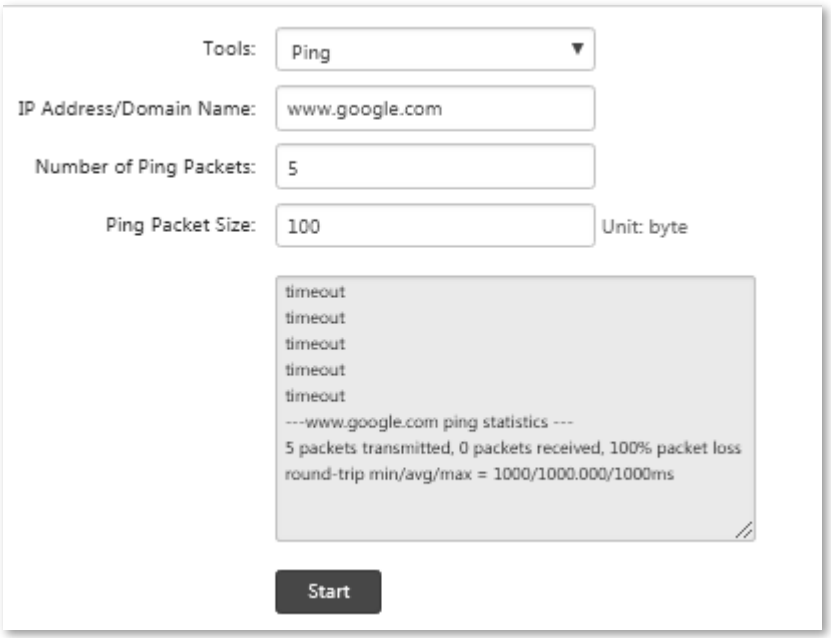
1. Choose **Maintenance** > **Diagnostics**.
2. Choose **Ping** in the drop-down box.
3. Set **IP Address/Domain Name** to www.google.com.
4. Set **Number of Ping Packets** to **5**.
5. Set **Ping Packet Size** to **100**.

6. Click **Start.**



---End

Wait for a moment, the result shows on the bottom of the page.



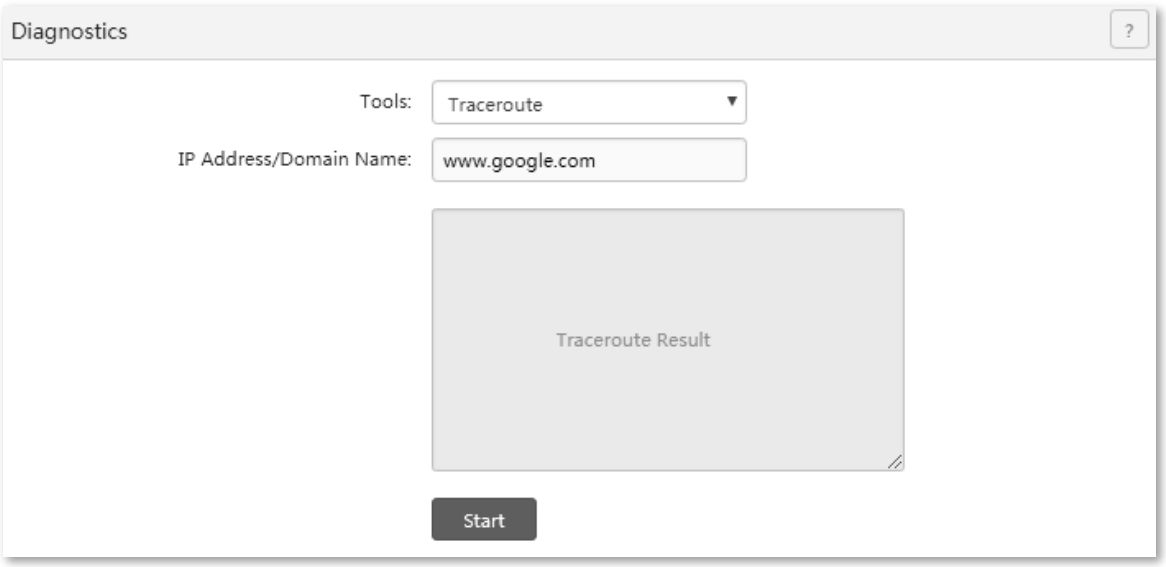
15.8.3 Traceroute dectect procedure

The traceroute function can be used to detect each hop address of destination IP address or domain name process. Assume that you need to detect the path from the router to Google, refer to the following settings.

1. Choose **Maintenance** > **Diagnostics**.
2. Choose **Traceroute** in the drop-down box.

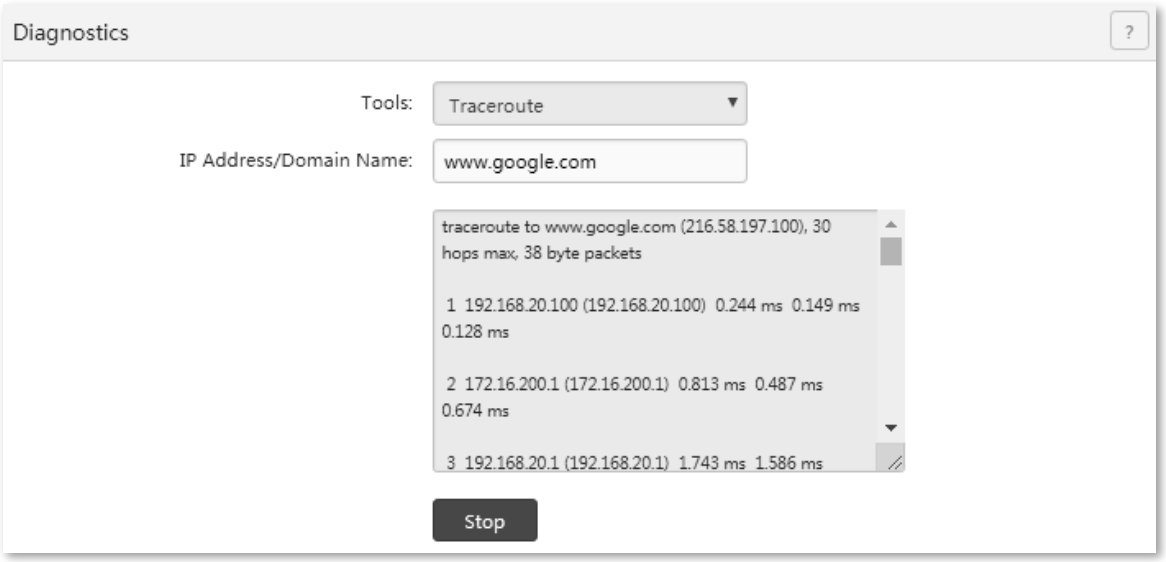
3. Set **IP Address/Domain Name** to **www.google.com**.

4. Click **Start**.



---End

Wait for a moment, the result shows on the bottom of the page. The record of the router starts with sequence number 1, each record is a hop, and each hop stands for a gateway.



16 System

This chapter describes:

- Viewing system info
- Viewing live users
- Viewing traffic statistics
- Viewing defense logs
- Viewing system logs

16.1 Viewing system info

In this area, you can check port status, system info, LAN info, WAN info. To access the page, choose **System Status > System Info**.

16.1.1 Port status

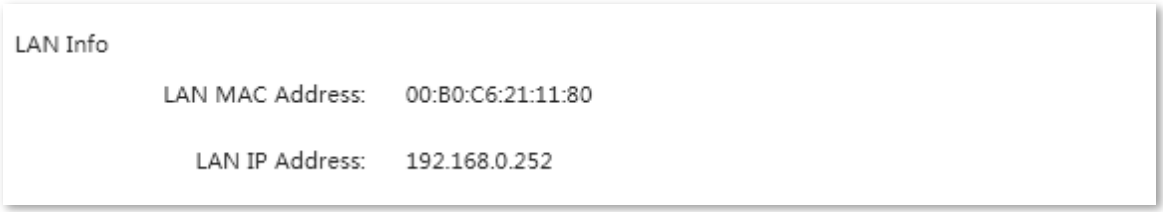
In this area, you can check whether a port is connected, and whether a port is a LAN port or a WAN port. A dimmed port is not connected to any device.

16.1.2 System info

In this area, you can check the device name, system time, uptime of the system after the last reboot, firmware version, CPU usage, and storage usage.

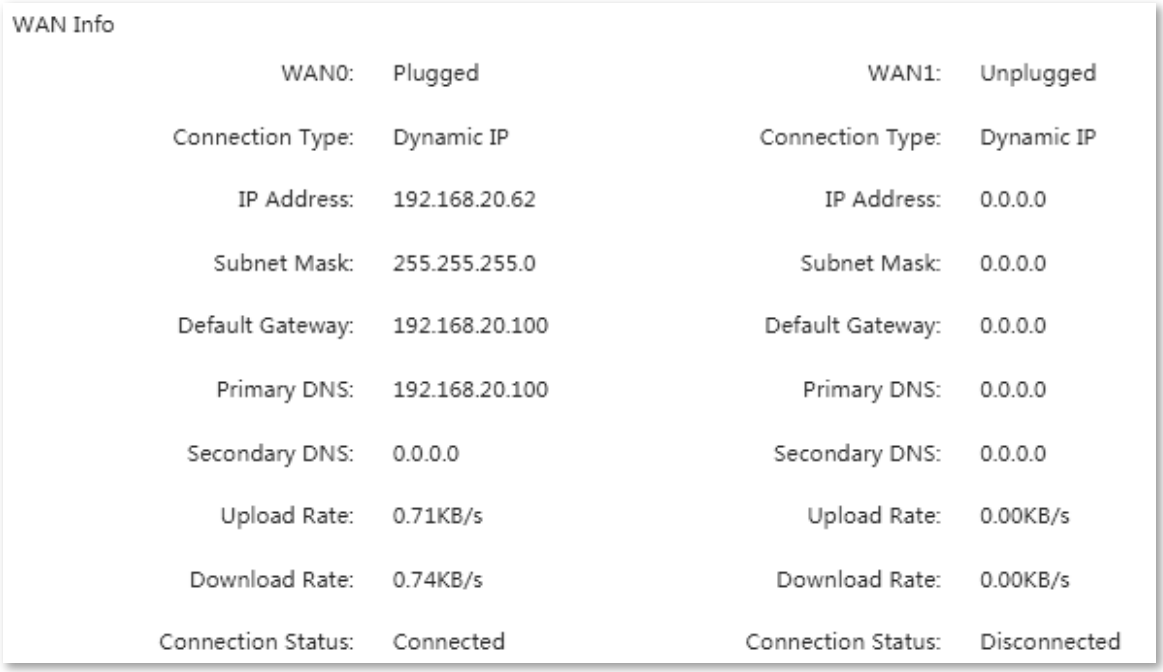
16.1.3 LAN info

In this area, you can check the LAN MAC address and LAN IP address of the router.



16.1.4 WAN info

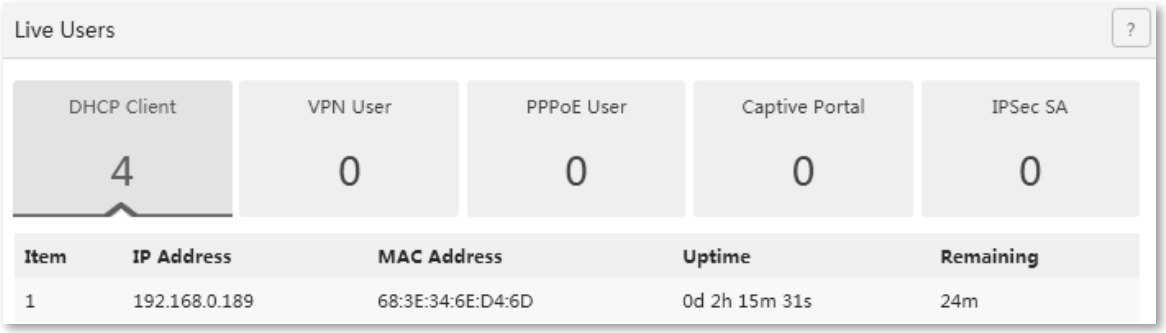
In this area, you can see information about all the WAN ports, including physical connection status, connection types, IP addresses, and so on.



16.2 Viewing live users

16.2.1 DHCP users

To access the page for viewing the information about DHCP clients of the router, choose **System Status**> **Live Users** > **DHCP Client**.

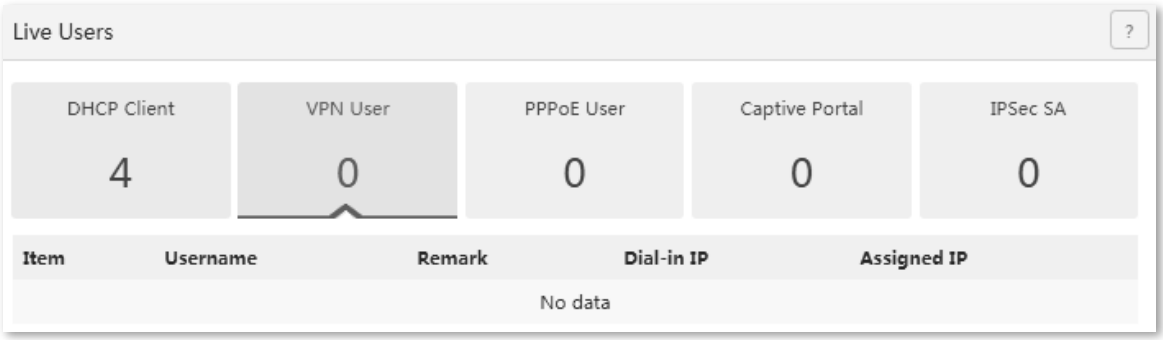


Parameter description

Parameter	Description
IP Address	It specifies the IP address of a DHCP client that is assigned by the DHCP server of the router.
MAC Address	It specifies the MAC address of a DHCP client.
Uptime	It specifies the connection duration of a DHCP client.
Remaining	It specifies the remaining lease time of an IP address.

16.2.2 VPN users

To access the page for viewing the information about PPTP/L2TP clients of the router after you enable the PPTP/L2TP server function, choose **System Status**> **Live Users** > **VPN User**.

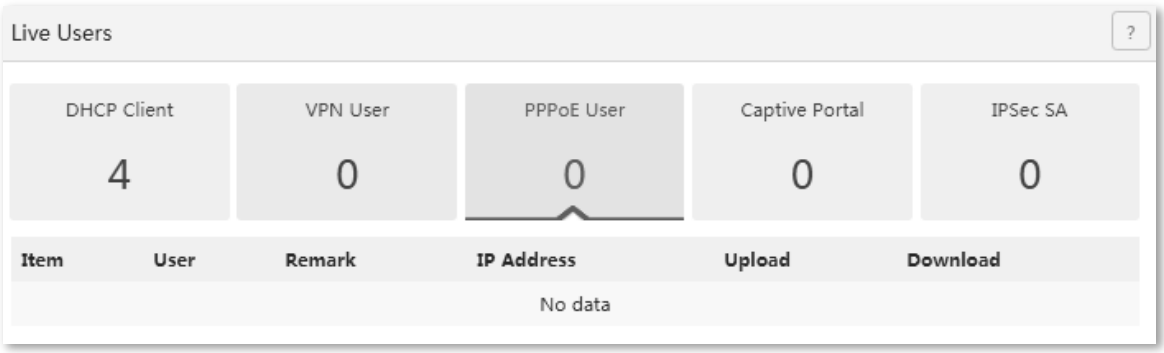


Parameter description

Parameter	Description
Username	It specifies a user name that a VPN client uses to connect to the VPN server of the router.
Remark	It specifies the description of a user name.
Dail-in IP	It specifies the IP address of a VPN client. If the VPN client is a router, this IP address is the WAN IP address of the router for which the VPN client function is enabled.
Assigned IP	It specifies the IP address of a VPN client that is assigned by the VPN serer of the router.

16.2.3 PPPoE users

To access the page for viewing the information about PPPoE clients after you enable PPPoE authentication, choose **System Status**> **Live Users** > **PPPoE User**.



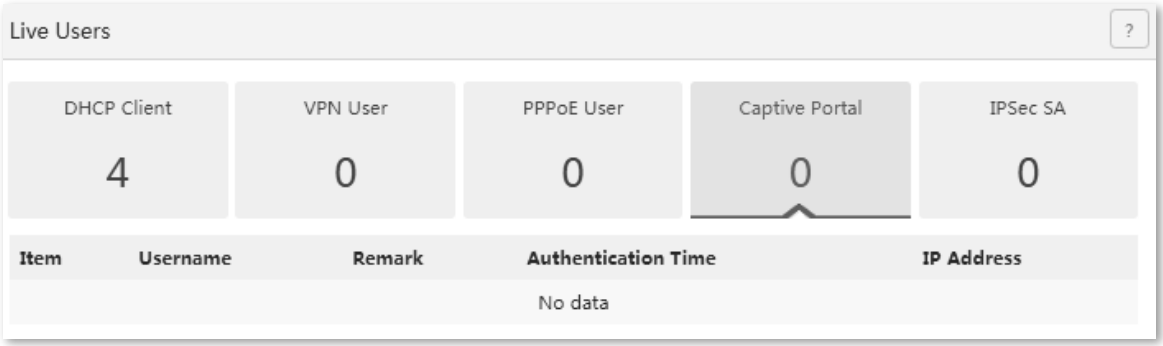
Parameter description

Parameter	Description
User	It specifies the user name of a PPPoE client.
Remark	It specifies the description of a user name.

IP address	It specifies the IP address of a PPPoE client that is assigned by the PPPoE server of the router.
Upload/Download	It specifies the upload or download speed of a PPPoE client.

16.2.4 Captive portal

To access the page for viewing the information about connected clients after you enable the captive portal, choose **System Status**> **Live Users** > **Captive Portal**.

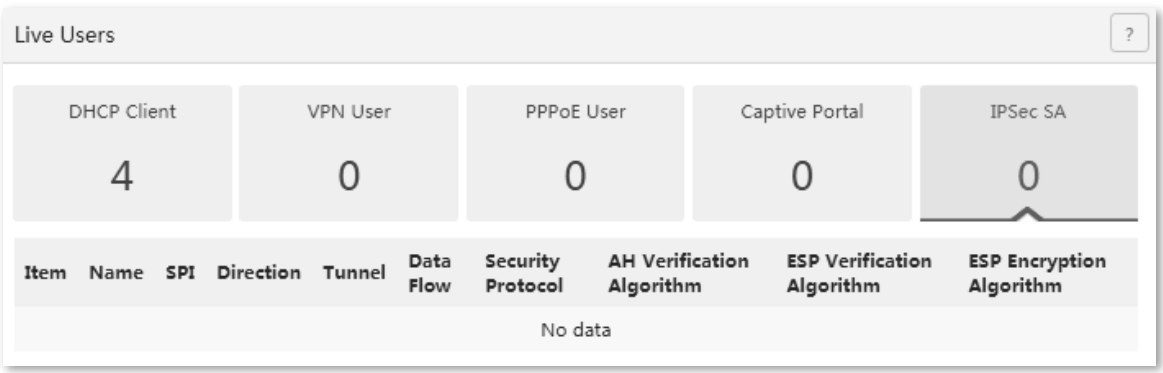


Parameter description

Parameter	Description
Username	It specifies the user name of an authenticated client.
Remark	It specifies the description of a user name.
Authenticated Time	It specifies the authenticated time of a client.
IP Address	It specifies the IP address of an authenticated client.

16.2.5 IPSec SA

To access the page for viewing the information about the IPSec Security Alliance and IPSec tunnel after you add an IPSec tunnel for the router, choose **System Status**> **Live Users** > **IPSec SA**.

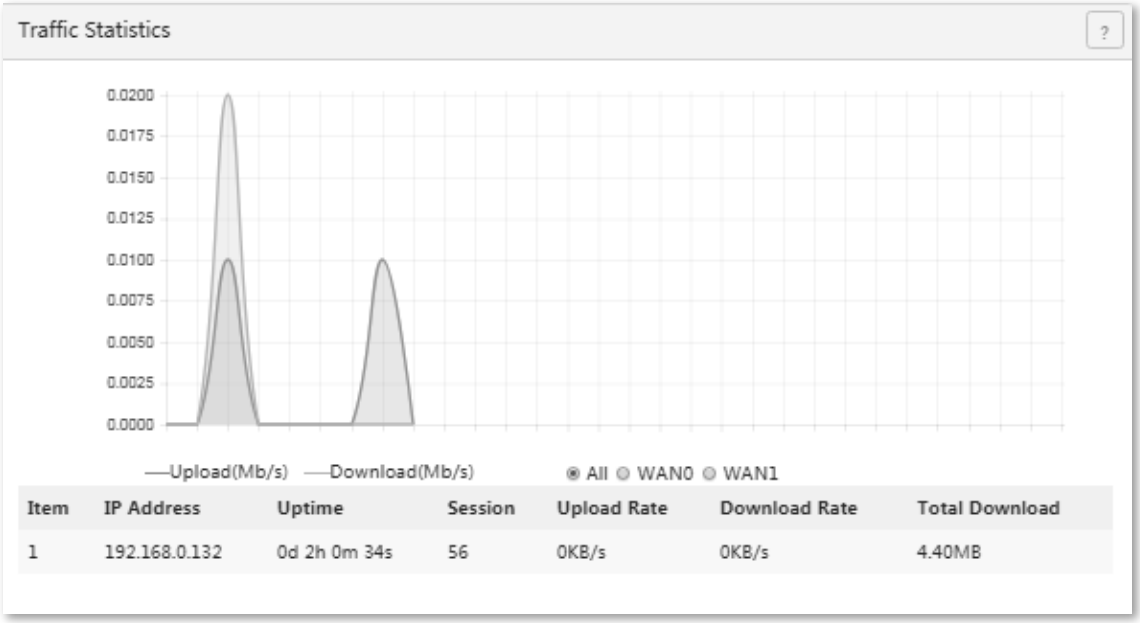


Parameter description

Parameter	Description
Name	It specifies the name of an IPSec tunnel.
SPI	It specifies an SPI value, which is manually set or automatically assigned through negotiation.
Direction	It specifies the data transmission direction of a tunnel. The options include: – **In**: It indicates that data is transmitted from a remote router to this router. – **Out**: It indicates that data is transmitted from this router to a remote router.
Tunnel	It specifies the direction of data transmission over the internet between two routers. – **In**: It indicates that data is transmitted from the WAN IP address of this router to the WAN IP address of a remote router. – **Out**: It indicates that data is transmitted from the WAN IP address of a remote router to the WAN IP address of this router.
Data Flow	It specifies the direction of data transmission over a LAN between two routers. – **In**: It indicates that data is transmitted from the LAN IP address of this router to the LAN IP address of a remote router. – **Out**: It indicates that data is transmitted from the LAN IP address of a remote router to the LAN IP address of this router.
Security Protocol	It specifies the security protocol for an IPSec tunnel.
AH Verification Algorithm	It specifies the AH verification algorithm for an IPSec tunnel.
ESP Verification Algorithm	It specifies the ESP verification algorithm for an IPSec tunnel.
ESP Encryption Algorithm	It specifies the ESP encryption algorithm for an IPSec tunnel.

16.3 Viewing traffic statistics

To access the page for viewing the upload and download speeds of a WAN port or each local IP address, choose **System Status**> **Traffic Statistics**.

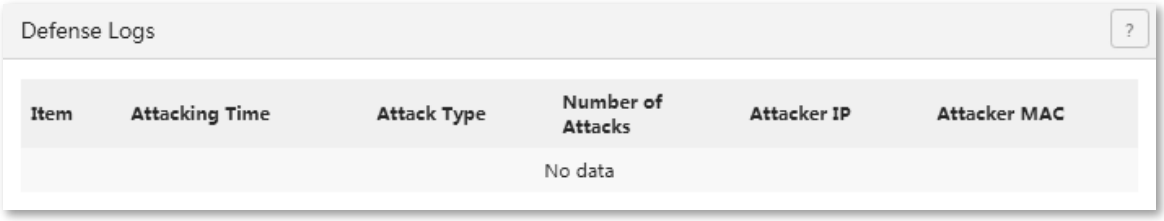


Item	IP Address	Uptime	Session	Upload Rate	Download Rate	Total Download
1	192.168.0.132	0d 2h 0m 34s	56	0KB/s	0KB/s	4.40MB

16.4 Viewing defense logs

If you enable the firewall function, the router logs attacks. According to the attack logs, a network administrator can locate attackers and try resolving problems.

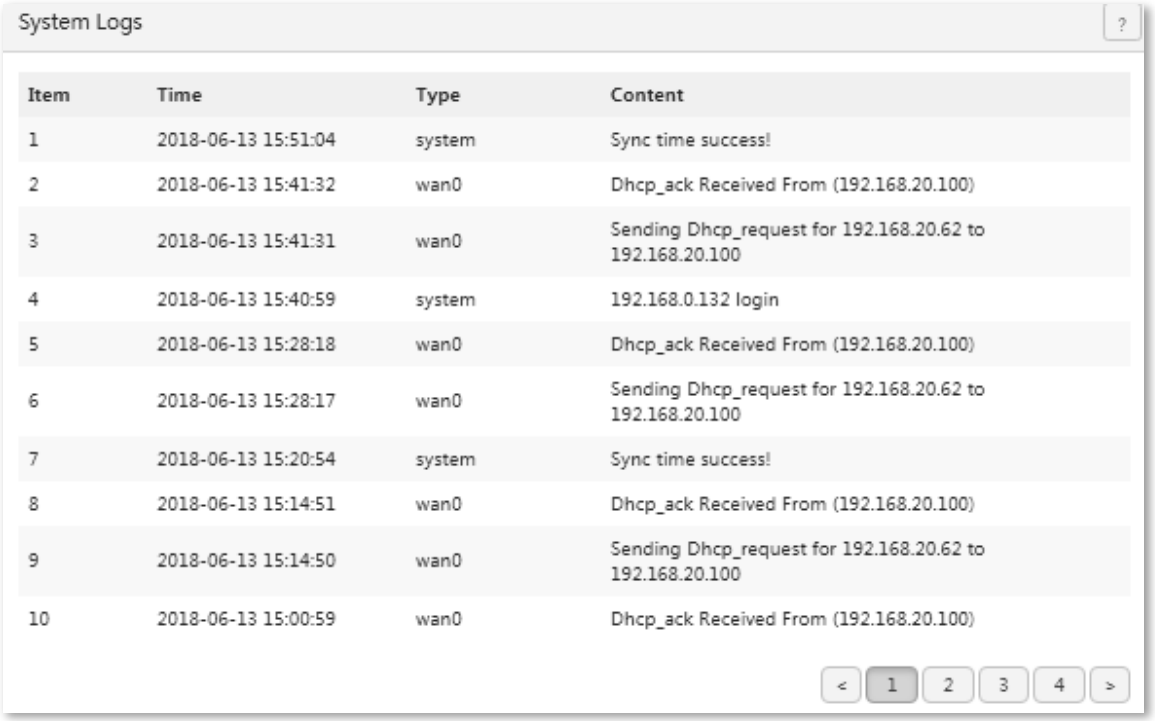
To access the page for viewing attack information, choose **System Status** > **Defense Logs**.



16.5 Viewing system logs

System logs record information about system reboot, PPPoE dial-up connections, time synchronization, device login attempts, WAN connections, and so on. If you encounter a network fault, the system logs are helpful for rectifying the fault.

To access the page for viewing system logs, choose **System Status**> **System Logs**.



The record time of system logs depends on the system time of the router. Ensure that the system time of your router is correct. You can set the time on the **Maintenance** > **System Time** page.

Note

- When the router reboots, the previous system logs are deleted.
- The router reboots when you power on the router after a power failure, upgrade the firmware, back up or restore a router configuration, or restore the factory settings.

Appendix

A Troubleshooting

Q1: When I use the device for the first time, I cannot log in to the web UI of the device after entering 192.168.0.252. What should I do?

A1: Verify that:

- The Ethernet cables are connected correctly and firmly.
- The IP address of your computer is **192.168.0.*X*** (where *x* indicates 2 to 254 except 252).
- Clear the cache of your web browser or use another web browser to log in.
- Disable the firewall of your computer or use another computer to log in.
- The IP address 192.168.0.252 is not assigned to another device on your LAN.
- If the problem persists, please restore the device to the factory settings and try again. For how to restore the factory settings, refer to **Q3**.

Q2: I forget the login user name and password. What should I do?

A2: restore the device to the factory settings and set the username and password. For how to restore the factory settings, refer to **Q3**.

Q3: I cannot log in to the web UI. How can I restore the device to the factory settings?

A3: When the device is powered on, use a needle to press the button for about 8 seconds. Then wait for about 1 minute. If the SYS LED indicator blinks again, the device has been restored to the factory settings. In this case, you need to re-configure the device.

Q4: After I connect to the router, my computer displays the message "IP address is conflicted with another device". What should I do?

Q4: Verify that:

- No other DHCP server on your LAN is enabled.
- The LAN IP address of your router is not assigned to another device on your LAN. The default IP address of the router is 192.168.0.252.
- The IP address of your computer is not assigned to another device on your LAN.

B Safety and emission statement

CE Mark Warning

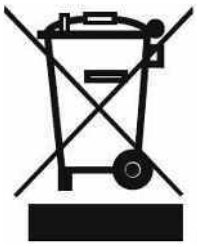
This is a Class A product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

For Pluggable Equipment, the socket-outlet shall be installed near the equipment and shall be easily accessible.

WARNING: The mains plug is used as disconnect device, the disconnect device shall remain readily operable.

The Product is designed for IT Power Distribution System.

NOTE: (1) The manufacturer is not responsible for any radio or TV interference caused by unauthorized modifications to this equipment. (2) To avoid unnecessary radiation interference, it is recommended to use a shielded RJ45 cable.


RECYCLING

This product bears the selective sorting symbol for Waste electrical and electronic equipment (WEEE). This means that this product must be handled pursuant to European directive 2012/19/EU in order to be recycled or dismantled to minimize its impact on the environment.

User has the choice to give his product to a competent recycling organization or to the retailer when he buys new electrical or electronic equipment.

FCC Statement

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this

device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Caution!

Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

NOTE: (1) The manufacturer is not responsible for any radio or TV interference caused by unauthorized modifications to this equipment. (2) To avoid unnecessary radiation interference, it is recommended to use a shielded RJ45 cable.