www.ip-com.com.cn

User Manual

Multi-WAN Hotspot Router M50

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 manual helps you configure, manage and maintain the product.

Conventions

This user manual is applicable to IP-COM Multi-WAN Hotspot Router M50.

Unless otherwise specified, “router”, "this router", “product”, or “device” mentioned in this user manual indicates M50.

Typographical conventions in this user manual:

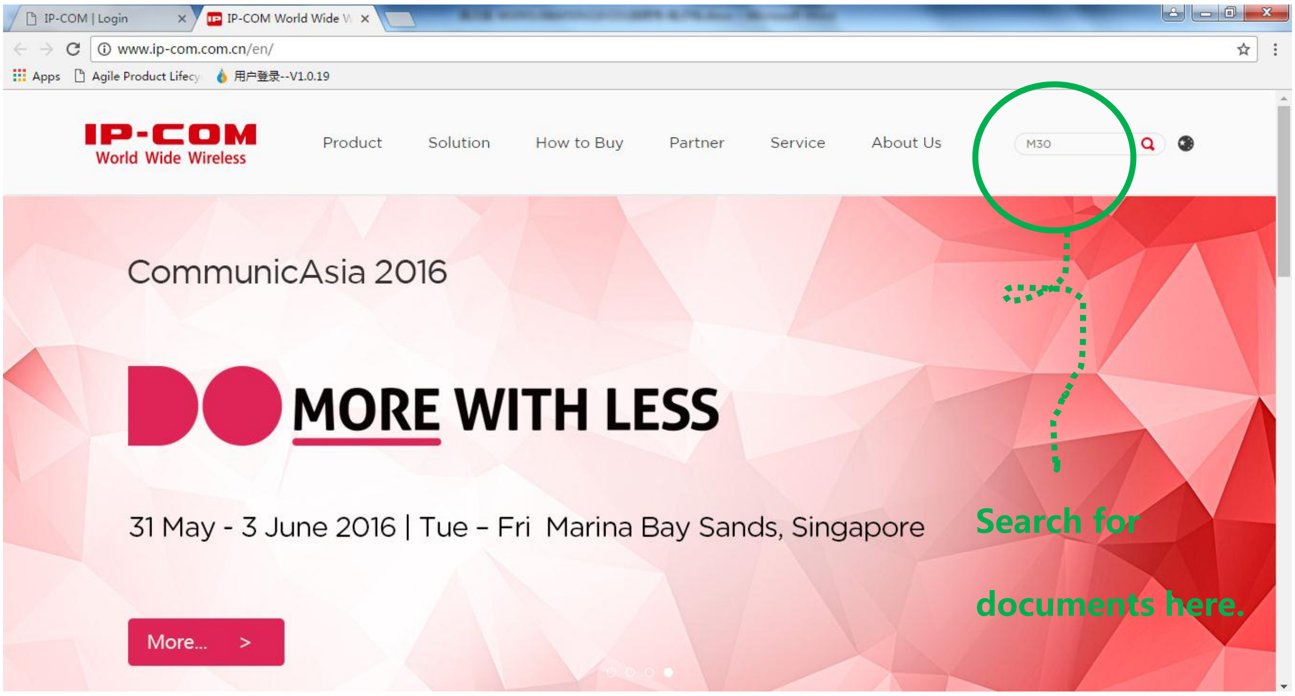
Item	Presentation	Example
Menu	Bold	**System** indicates the "System" menu.
Cascading menus	>	Choose **System** > **Live Users**.

Symbols in this user manual:

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

For more documents

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



Search for documents here.

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

Table of contents

Chapter 1 Product overview

This chapter describes:

- Main features
- Appearance

1.1 Overview

IP-COM Multi-WAN Hotspot Router M50 is designed for small- and medium-sized enterprises to implement intelligent network access and management. It offers an AP management system and a multi-authentication management system, and supports various enterprise-oriented functions including filter management, smart bandwidth management, PPTP/L2TP/IPSec VPN, 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 and can manage up to 16 APs at the same time. Using the system, you can customize SSIDs, power, channels, user capacity, reboot policies, and alarm policies for APs.

Multi-authentication management system

The router is embedded with a multi-authentication management system, which supports web authentication, and PPPoE authentication. This system authenticates, without an additional authentication server, users who request internet access, which helps reduce enterprise costs.

- Web authentication: a portal-based authentication mode, which allows you to add advertisements to the push page.
- PPPoE authentication: a PPPoE server–based authentication mode, which allows users to be authenticated with PPPoE accounts. This mode enables you to control traffic by account to effectively address network congestion at peak hours.

Smart bandwidth management

This router supports smart bandwidth control and user-defined bandwidth control.

- Smart bandwidth control: You can specify only the actual access bandwidth and leave the router to manage bandwidth based on bandwidth usage. 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.
- User-defined bandwidth control: You must specify the upper bandwidth limit per accessing equipment and the router controls bandwidth usage accordingly.

Filter management

You can configure URL-related filter management policies and application-related filter management policies by IP address group or time group.

The router allows you to add URLs to the database.

Other useful functions

VPN: This function enables you to quickly set up IPsec, PPTP, and L2TP VPNs to facilitate remote access to internal resources.

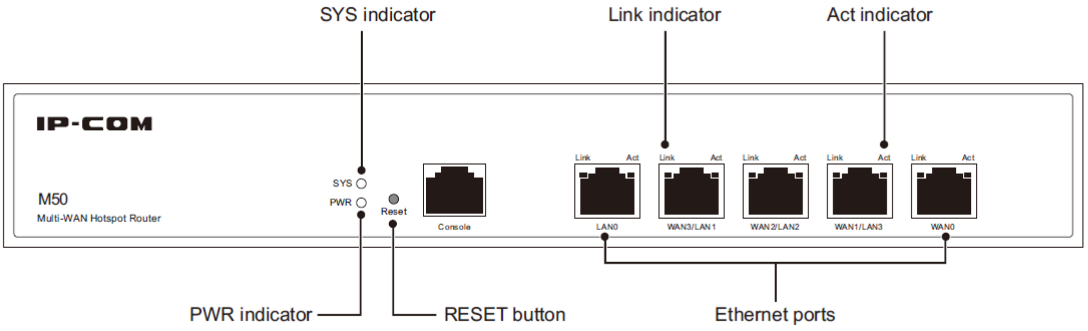
Multi-WAN: This function allows a maximum of four ISP network connections.

Hotel mode: This function allows all hosts in a LAN to access the internet with any IP address.

1.3 Appearance

1.3.1 Front panel

The front panel includes 12 LED indicators, 5 RJ45 ports, and 1 RESET button. See the following figure, which indicates the front panel of M50.



Indicators

There are 1 PWR indicator and 1 SYS indicator. Each RJ45 port has 1 Link indicator and 1 Act indicator.

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 startup is not complete yet.
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.

RJ45 ports

M50 provides five 10/100/1000 Mbps auto-negotiation RJ45 ports. Each RJ45 port has 1 Link indicator and 1 Act indicator.

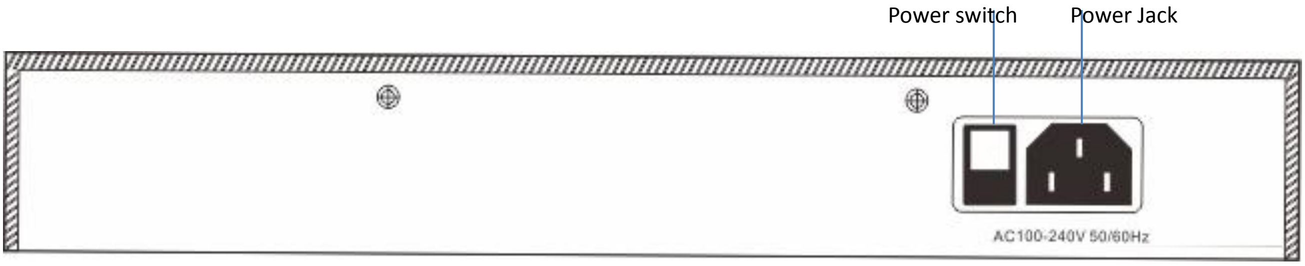
The 5 RJ45 ports include 1 LAN port, 1 WAN port, and 3 LAN/WAN ports. You can set the LAN/WAN ports as LAN or WAN ports as required. By default, the 2 rightmost ports are WAN ports, while the 3 leftmost ports are LAN ports.

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 at least 8 seconds and wait about a minute. When the SYS indicator flashes again, you can infer that the settings are 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 the power cable contained in the product package to the router.

Chapter 2 Quick internet connection setup

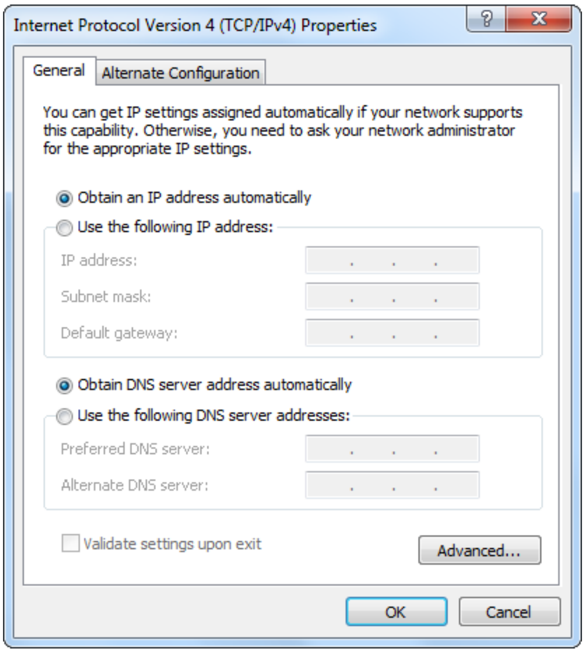
This chapter describes:

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

2.1 Logging in to the router web UI

You can use a 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 the switch connected to the router) using an Ethernet cable and perform the following procedure:

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



Internet Protocol Version 4 (TCP/IPv4) Properties

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

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

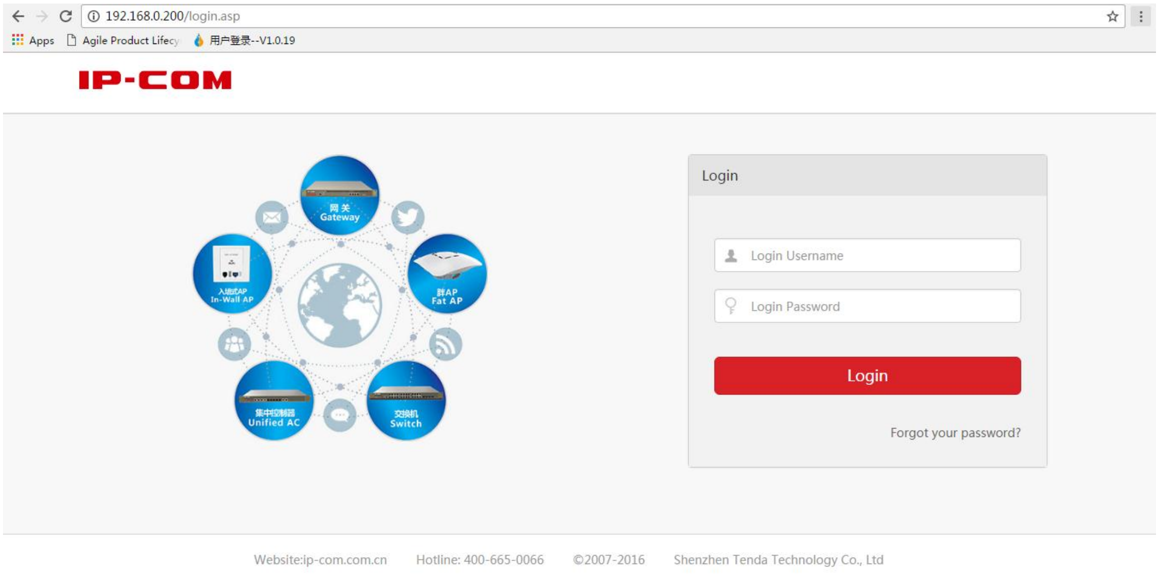
Preferred DNS server: . . .

Alternate DNS server: . . .

□ Validate settings upon exit

2. Start a browser (such as Internet Explorer) and enter **192.168.0.252** to access the router login page.

3. Enter your user name and password (the default user name and password are **admin**) and click **Login**.

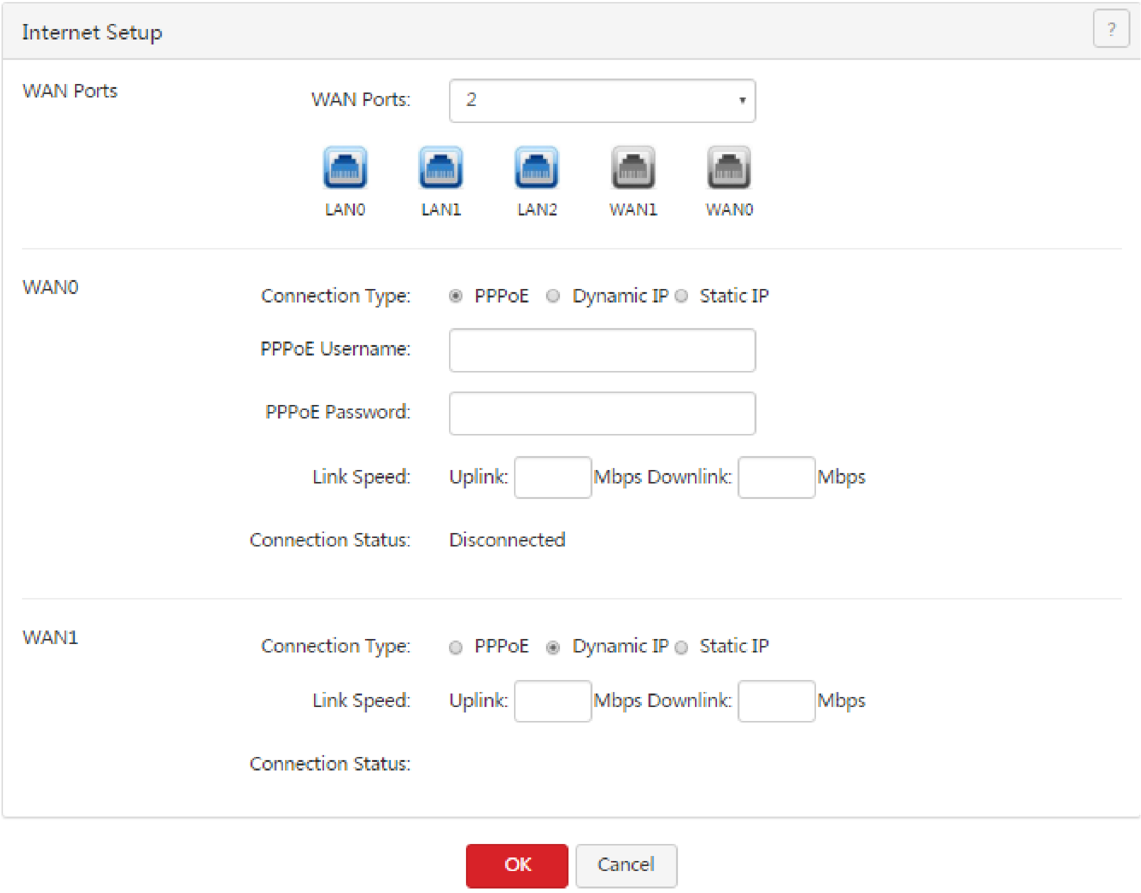


Website:ip-com.com.cn Hotline: 400-665-0066 ©2007-2016 Shenzhen Tenda Technology Co., Ltd

Note

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

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



Internet Setup

WAN Ports

WAN Ports: 2

WAN0

Connection Type: ● PPPoE ○ Dynamic IP ○ Static IP

PPPoE Username:

PPPoE Password:

Link Speed: Uplink: Mbps Downlink: Mbps

Connection Status: Disconnected

WAN1

Connection Type: ○ PPPoE ● Dynamic IP ○ Static IP

Link Speed: Uplink: Mbps Downlink: Mbps

Connection Status:

2.2 Configuring the router

By configuring the router, you can enable multiple computers in your LAN to access the internet. Before configuring the router, consult your ISP on your internet connection type.

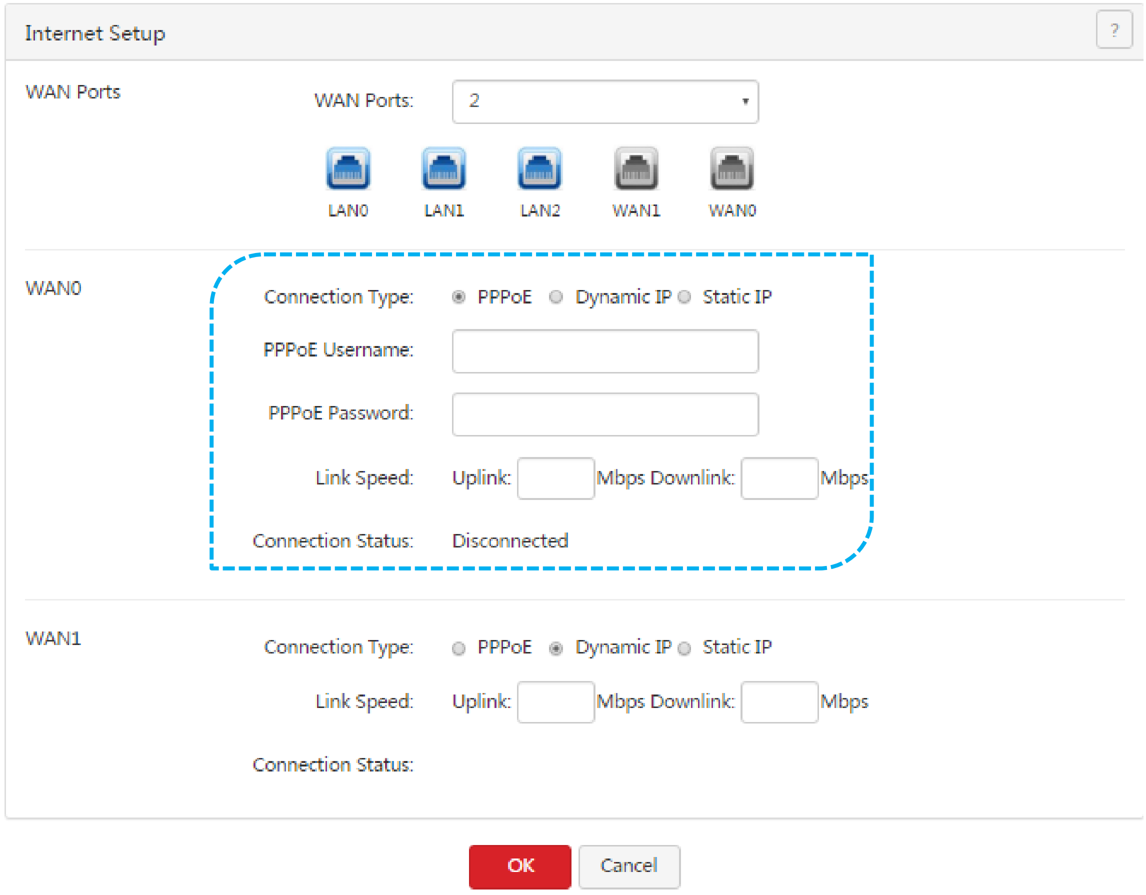
Internet Connection Type	Description
PPPoE	Your internet service provider (ISP) provides a user name and password for you to access the internet.
Dynamic IP address	Your ISP does not provide any internet connection type information for you or specifies that you can access the internet using a dynamic IP address.
Static IP address	Your ISP specifies internet connection information including a fixed IP address, a subnet mask, a default gateway, and DNS servers for you.

Note

- The router provides 2 WAN ports. In the following sections, the WAN0 port is used as an example to describe the configuration method, which is also applicable to the WAN1 port.
- By default, the WAN0 port is connected to the internet using PPPoE, while the WAN1 port is connected to the internet using a dynamic IP address.
- All internet access parameters are specified by ISPs. If you are uncertain about the parameters, consult your ISP.
- If a dialog box appears when you configure the router, take measures according to the message in the dialog box.

2.2.1 PPPoE

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



Internet Setup

WAN Ports

WAN Ports: 2

WAN0

Connection Type: ● PPPoE ○ Dynamic IP ○ Static IP

PPPoE Username:

PPPoE Password:

Link Speed: Uplink: Mbps Downlink: Mbps

Connection Status: Disconnected

WAN1

Connection Type: ○ PPPoE ● Dynamic IP ○ Static IP

Link Speed: Uplink: Mbps Downlink: Mbps

Connection Status:

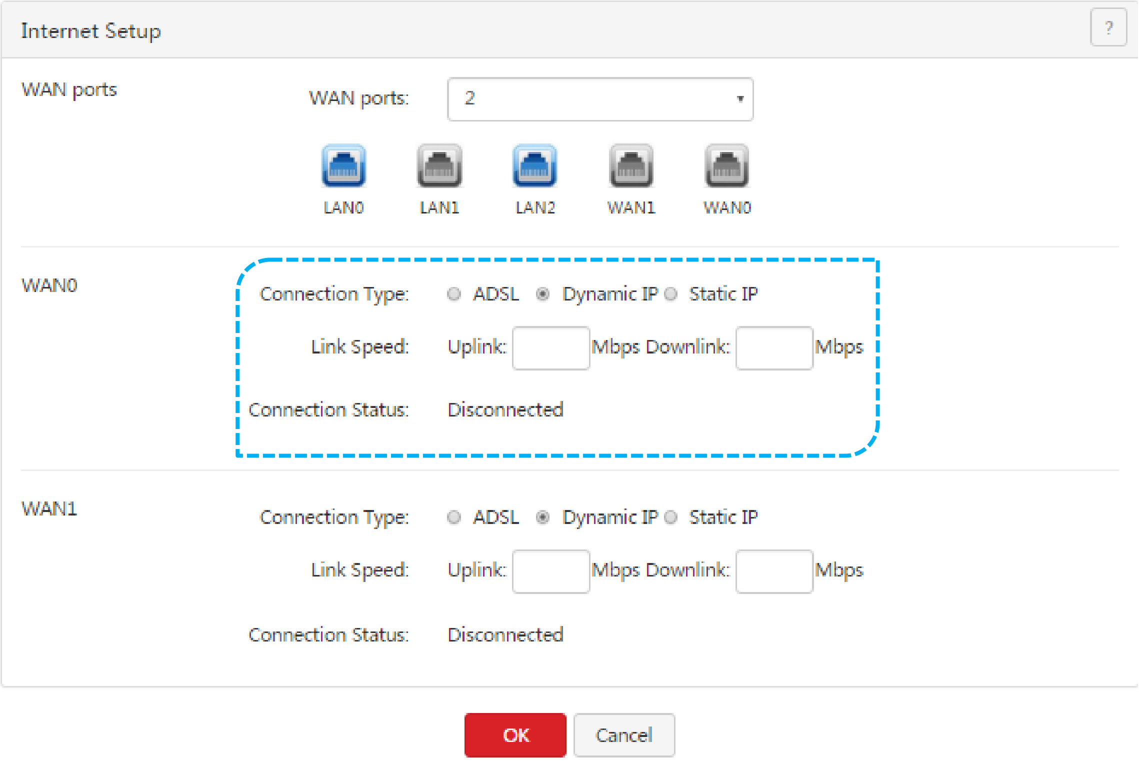
Perform the following procedure to configure an internet connection:

1. Set **Connection Type** to **PPPoE**.
2. Set **PPPoE Username** and **PPPoE Password** to the broadband service user name and password provided by your ISP.
3. Set **Link Speed** to the bandwidth of your broadband connection. If you are uncertain about the bandwidth, consult your ISP.
4. Click **OK**.

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 address

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



Internet Setup

WAN ports

WAN ports: 2

WAN0

Connection Type: ○ ADSL ● Dynamic IP ○ Static IP

Link Speed: Uplink: Mbps Downlink: Mbps

Connection Status: Disconnected

WAN1

Connection Type: ○ ADSL ● Dynamic IP ○ Static IP

Link Speed: Uplink: Mbps Downlink: Mbps

Connection Status: Disconnected

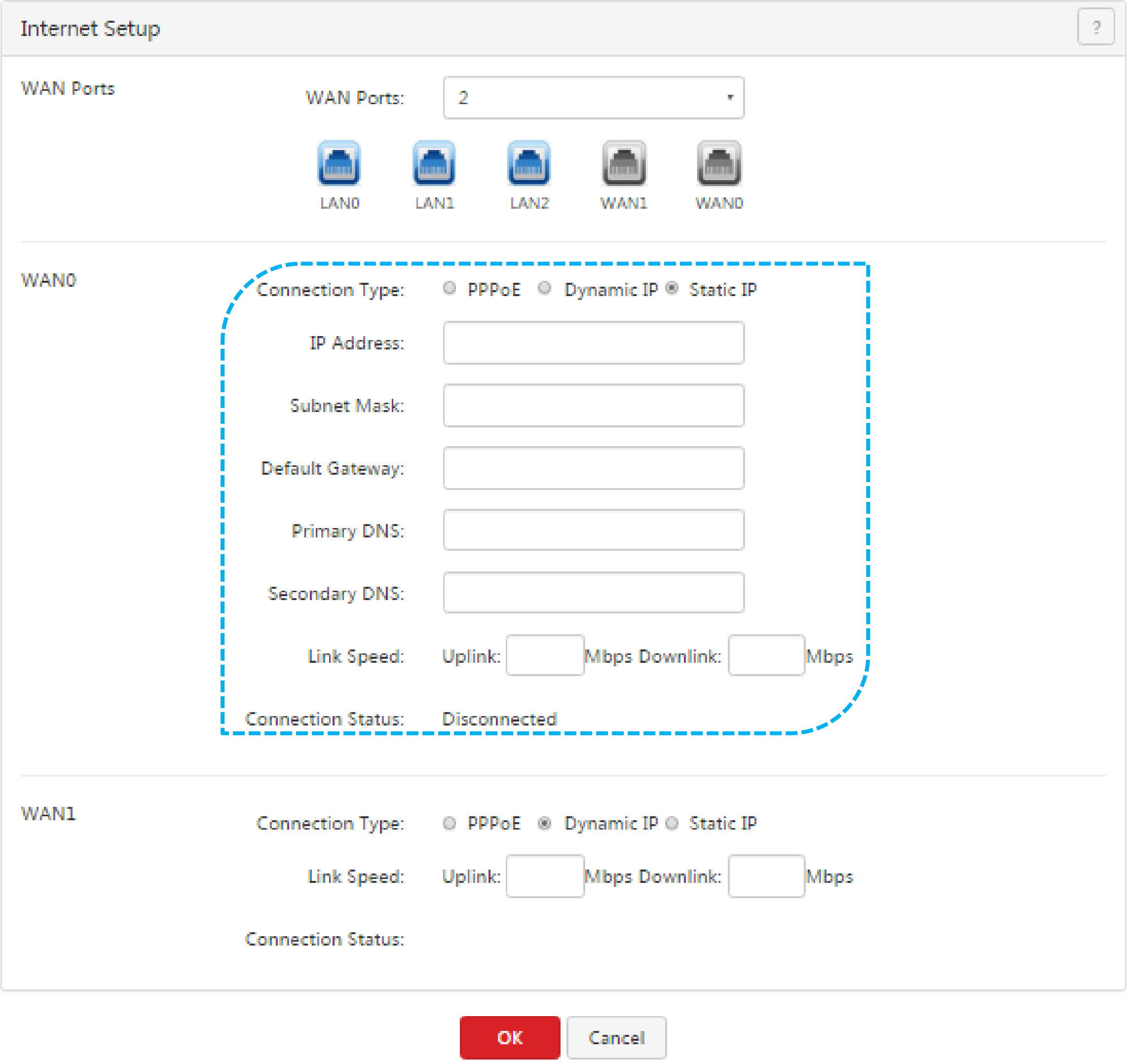
Perform the following procedure to configure an internet connection:

1. Set **Connection Type** to **Dynamic IP**.
2. Set **Link Speed** to the bandwidth of your broadband connection. If you are uncertain about the bandwidth, consult your ISP.
3. Click **OK**.

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 address

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



Internet Setup

WAN Ports

WAN Ports: 2

WAN0

Connection Type: ○ PPPoE ○ Dynamic IP ● Static IP

IP Address:

Subnet Mask:

Default Gateway:

Primary DNS:

Secondary DNS:

Link Speed: Uplink: Mbps Downlink: Mbps

Connection Status: Disconnected

WAN1

Connection Type: ○ PPPoE ● Dynamic IP ○ Static IP

Link Speed: Uplink: Mbps Downlink: Mbps

Connection Status:

Perform the following procedure to configure an internet connection:

1. Set **Connection Type** to **Static IP**.
2. Set **IP Address**, **Subnet Mask**, **Default Gateway**, **Primary DNS**, and **Secondary DNS** to those provided by your ISP.
3. **Link Speed** to the bandwidth of your broadband connection. If you are uncertain about the bandwidth, consult your ISP.
4. Click **OK**.

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.

Chapter 3 Login

This chapter describes:

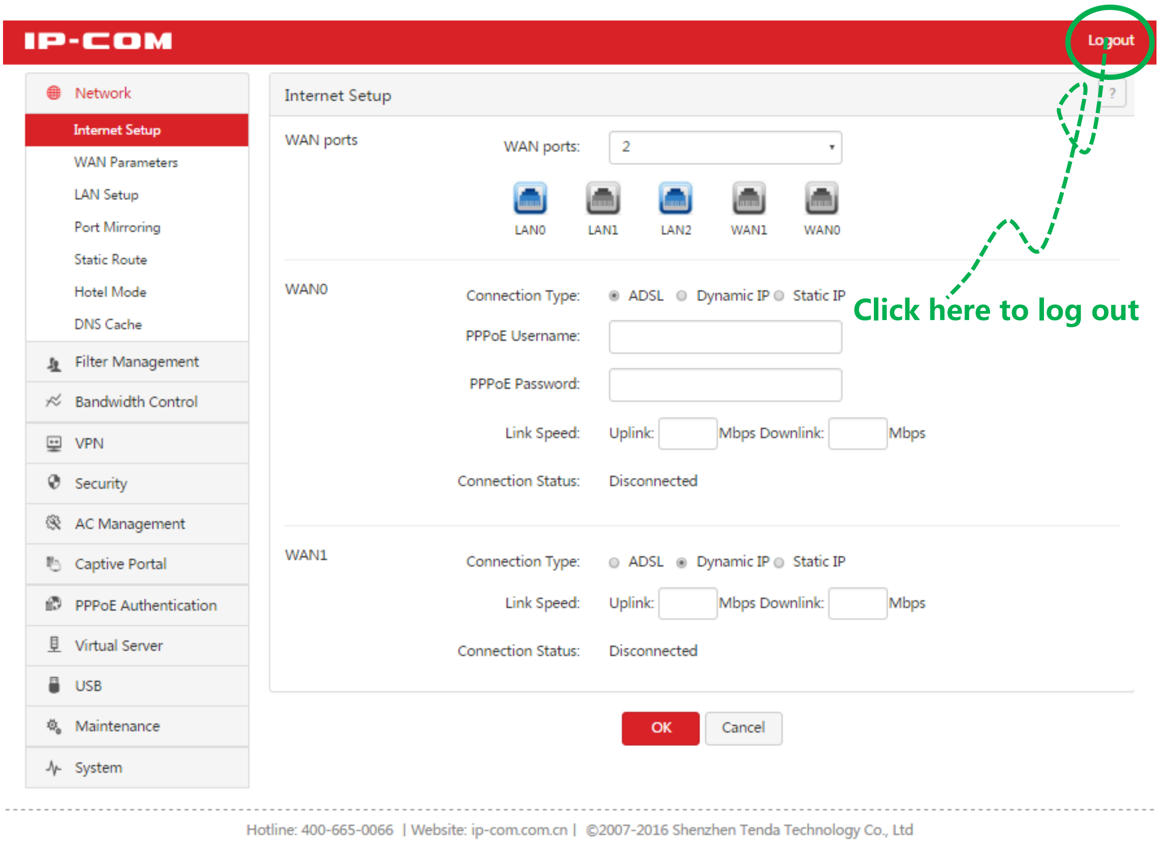
- Logging in to the router web UI
- Logging out of the router web UI
- Web UI layout
- Common buttons on the web UI

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.



Internet Setup

WAN ports

WAN ports: 2

WAN0

Connection Type: ● ADSL ○ Dynamic IP ○ Static IP

PPPoE Username:

PPPoE Password:

Link Speed: Uplink: Mbps Downlink: Mbps

Connection Status: Disconnected

WAN1

Connection Type: ○ ADSL ● Dynamic IP ○ Static IP

Link Speed: Uplink: Mbps Downlink: Mbps

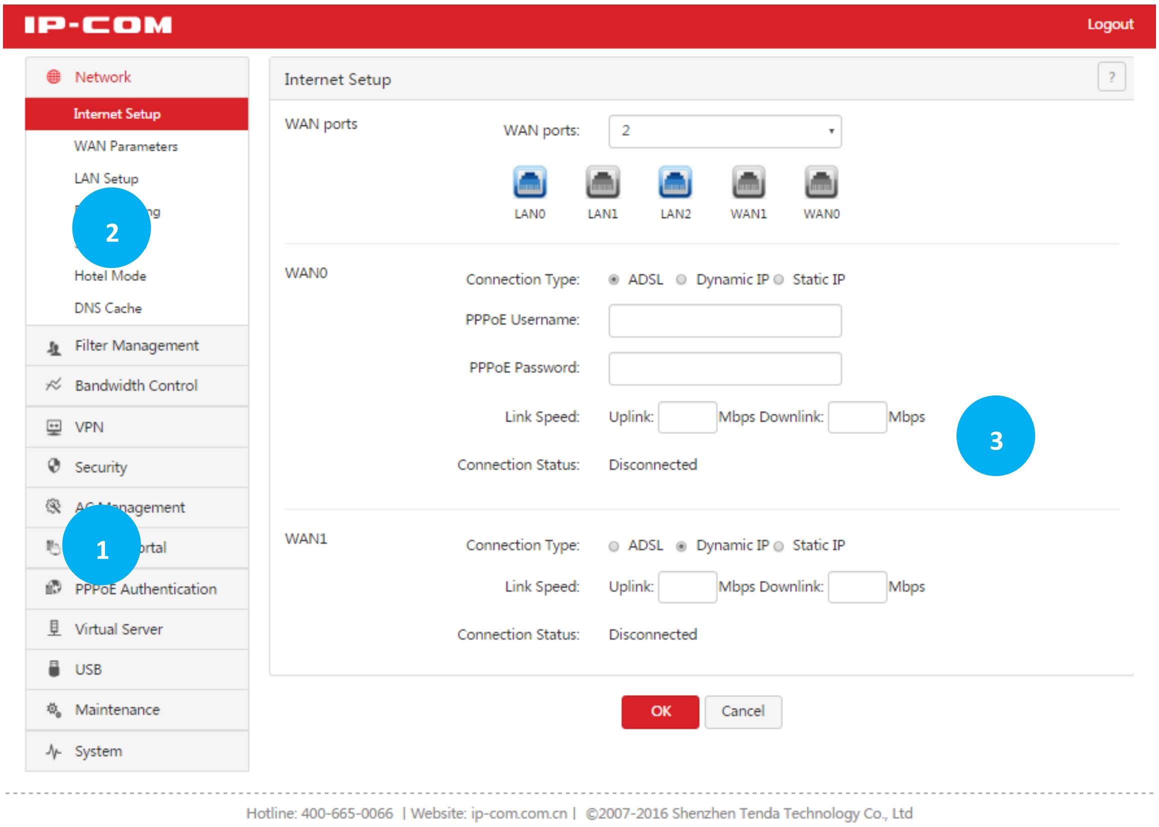
Connection Status: Disconnected

Hotline: 400-665-0066 | Website: ip-com.com.cn | ©2007-2016 Shenzhen Tenda Technology Co., Ltd

Click here to log out

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.



Internet Setup

WAN ports

WAN ports: 2

WAN0

Connection Type: ● ADSL ○ Dynamic IP ○ Static IP

PPPoE Username:

PPPoE Password:

Link Speed: Uplink: Mbps Downlink: Mbps

Connection Status: Disconnected

WAN1

Connection Type: ○ ADSL ● Dynamic IP ○ Static IP

Link Speed: Uplink: Mbps Downlink: Mbps

Connection Status: Disconnected

Hotline: 400-665-0066 | Website: ip-com.com.cn | ©2007-2016 Shenzhen Tenda Technology Co., Ltd

Note

The dimmed functions and parameters on the web UI are functions and parameters not supported by the router or unavailable for the current configuration.

SN	Area	Description
1	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.
2	Level-2 navigation bar	
3	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 is located in the upper-right corner and used to view help information of the parameters on the current page.

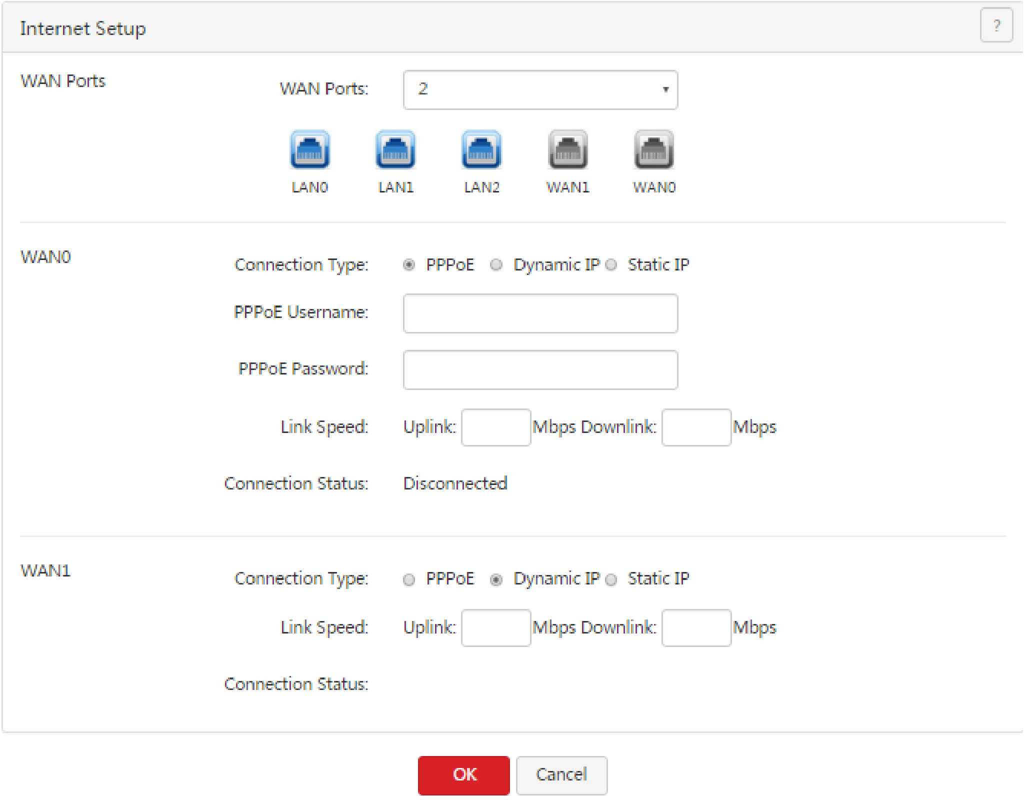
Chapter 4 Network

This chapter describes:

- Setting up an internet connection
- Setting WAN port parameters
- Setting up your LAN
- Configuring port mirroring
- Configuring a static route
- Using the Hotel mode
- 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 Setup**. See the following figure.



Internet Setup

WAN Ports

WAN Ports: 2

WAN0

Connection Type: ● PPPoE ○ Dynamic IP ○ Static IP

PPPoE Username:

PPPoE Password:

Link Speed: Uplink: Mbps Downlink: Mbps

Connection Status: Disconnected

WAN1

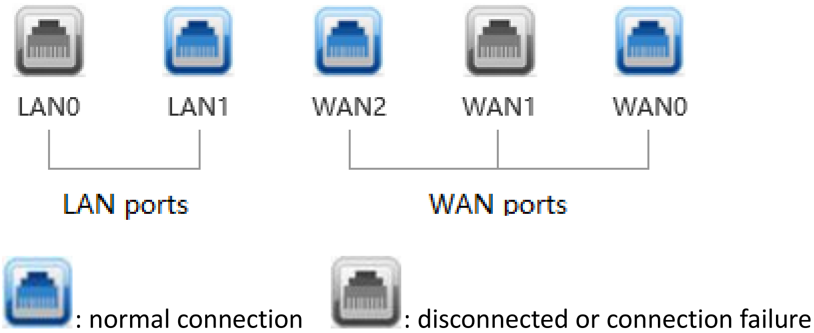
Connection Type: ○ PPPoE ● Dynamic IP ○ Static IP

Link Speed: Uplink: Mbps Downlink: Mbps

Connection Status:

The following table describes the parameters.

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.

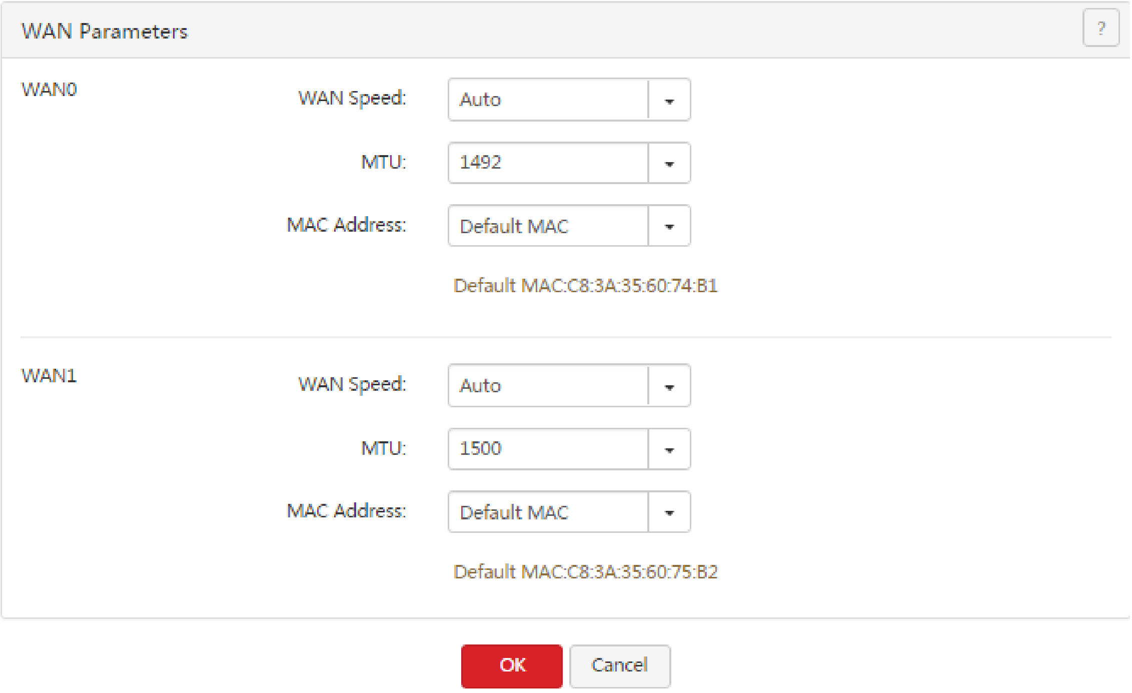
Parameter	Description
	After you change the number of WAN ports, the status of the RJ45 ports changes accordingly. See the following figure.  LAN0 LAN1 WAN2 WAN1 WAN0 LAN ports WAN ports : normal connection : disconnected or connection failure
Connection Type	The router can set up an internet connection 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. ● **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 fixed 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. ⚠ **Note** If your ISP provides you with only 1 DNS IP address, leave **Secondary DNS** blank.
Subnet Mask	
Default Gateway	
Primary DNS	
Secondary DNS	
Link Speed	It specifies the bandwidth of your broadband connection. If you are uncertain about the bandwidth, consult your ISP. ⚠ **Note** If you leave this parameter blank, the smart bandwidth control and smart load balacing functions cannot take effect. Therefore, it is recommended that you set this parameter.
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.

Parameter	Description
	● **Disconnected**: No connection is set up or connection fails. In this case, verify the cable connection and internet connection information, or consult your ISP. If a state not specified here appears, take measures based on the message corresponding to the state.

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 page for modifying WAN port parameters, choose **Network** > **WAN Parameters**. See the following figure.



WAN Parameters

WAN0

WAN Speed: Auto

MTU: 1492

MAC Address: Default MAC

Default MAC:C8:3A:35:60:74:B1

WAN1

WAN Speed: Auto

MTU: 1500

MAC Address: Default MAC

Default MAC:C8:3A:35:60:75:B2

4.2.1 WAN speed

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

Otherwise, it is recommended that you retain the default setting **Auto** of **WAN Speed**.

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**. In normal cases, the default values are recommended. If you encounter any of the following problems, try gradually reducing the value (recommended range: 1400 to 1500) to find the suitable value that does not lead to the problem:

- Some websites are not accessible or some secure websites cannot be displayed properly (such as the login pages of online banking websites and Alipay’s website).
- Emails cannot be received 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.

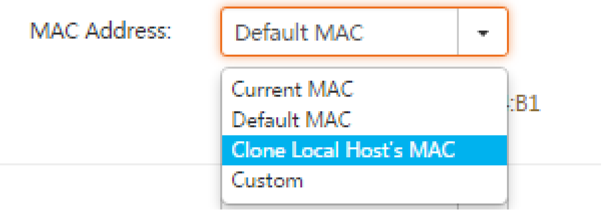
4.2.3 MAC address

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.

Method 1:

1. Connect the computer to the router.
2. Log in to the router web UI on the computer.
3. Choose **Network** > **WAN Parameters**.
4. Set **MAC Address** corresponding to the WAN port used to access the internet to **Clone Local Host’s MAC**.
5. Click **OK**.


MAC Address: Default MAC

Method 2:

1. Connect a computer other than the above-mentioned computer to the router.
2. Log in to the router web UI on the computer.
3. Choose **Network** > **WAN Parameters**.
4. Set **MAC Address** corresponding to the WAN port used to access the internet to **Custom**.

5. Enter the MAC address of the computer with internet accessibility.

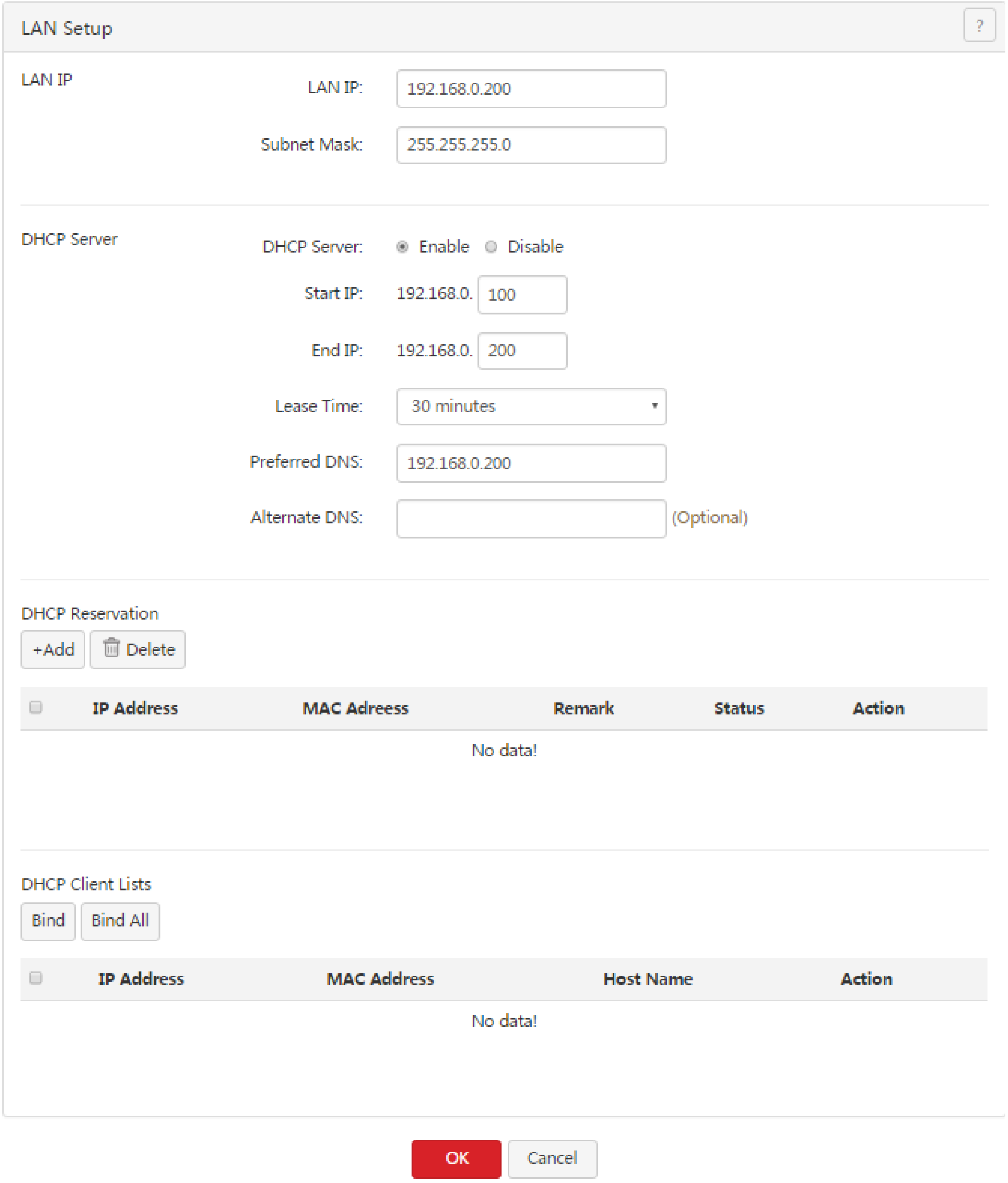
6. Click **OK**.

MAC Address:

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**.

4.3 Setting up your LAN

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



LAN Setup

LAN IP

LAN IP: 192.168.0.200

Subnet Mask: 255.255.255.0

DHCP Server

DHCP Server: ● Enable ○ Disable

Start IP: 192.168.0. 100

End IP: 192.168.0. 200

Lease Time: 30 minutes

Preferred DNS: 192.168.0.200

Alternate DNS: (Optional)

DHCP Reservation

+Add Delete

□	IP Address	MAC Adreess	Remark	Status	Action

No data!

DHCP Client Lists

Bind Bind All

□	IP Address	MAC Address	Host Name	Action

No data!

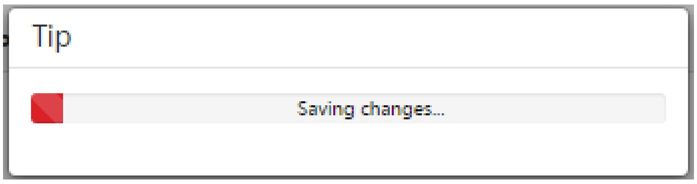
OK Cancel

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 it is in conflict with another IP address. 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 message shown in the following figure appears.



Tip

Saving changes...

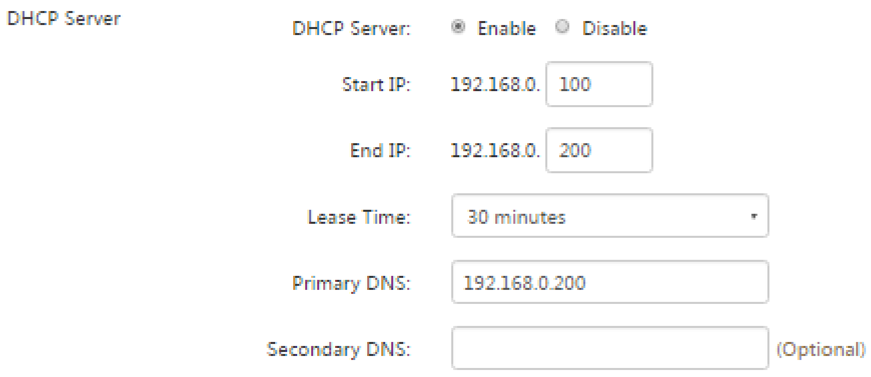
When the progress bar is complete, the login page appears. If the page does not appear, verify that the **Obtain an IP address automatically** option is selected for the local connection of your computer and an IP address is assigned from the router to your computer. Then, try accessing the login page with the new LAN IP address.

Note

If the new and old LAN IP addresses belong to different network segments, the router changes the DHCP address pool accordingly so that the IP addresses in the pool belong to the same network segment as the 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. If you disable the DHCP function, you need to manually configure this information on the computers so that the computers can access the internet. Disable this function only when necessary.



DHCP Server

DHCP Server: ● Enable ○ Disable

Start IP: 192.168.0. 100

End IP: 192.168.0. 200

Lease Time: 30 minutes

Primary DNS: 192.168.0.200

Secondary DNS: (Optional)

The following table describes the parameters.

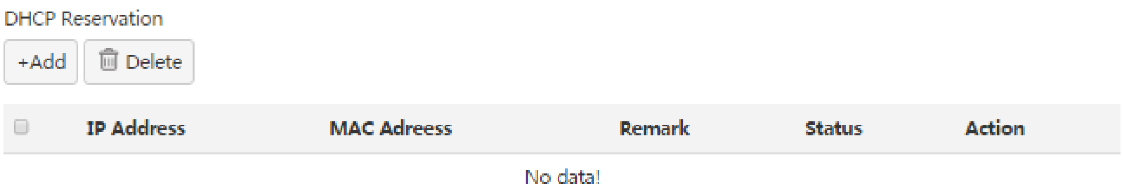
Parameter	Description
DHCP Server	It is used to enable or disable the DHCP function of the router.

Parameter	Description
Start IP	It specifies the start IP address of the DHCP address pool (range of IP addresses that can be assigned by the DHCP server). 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**. ⚠ **Note** The start and end IP addresses must belong to the same network segment as the LAN IP address of the router.
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.
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.

4.3.3 Static IP addresses assignment using DHCP

The filter management, flow control, and virtual server functions of the router are implemented based on IP addresses assigned to computers. These functions fail when the IP addresses change and as a result you need to update rules for the functions accordingly.

The function of static IP address assignment using DHCP helps address this problem. It allows the DHCP server to assign a fixed IP address to a computer, enabling the filter management, flow control, and virtual server functions to work properly.



DHCP Reservation

+Add | Delete

□	IP Address	MAC Adreess	Remark	Status	Action

No data!

Note

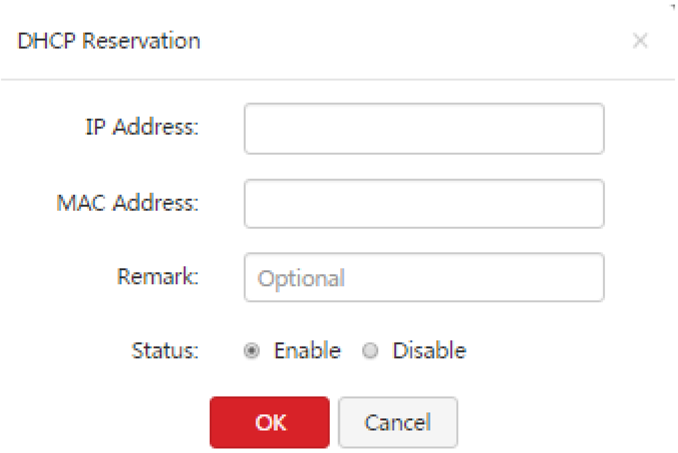
When using this function, ensure that the DHCP server function of the router has been enabled.

Adding a rule

1. Choose **Network** > **LAN Setup**.

2. Click +Add in the **DHCP Reservation** area.

   The **DHCP Reservation** dialog box appears.



DHCP Reservation

IP Address:

MAC Address:

Remark: Optional

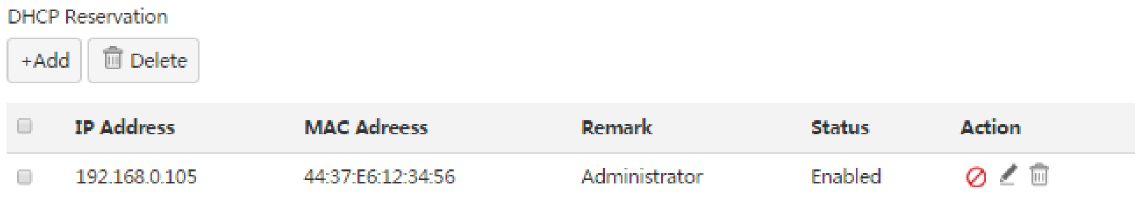
Status: ● Enable ○ Disable

The following table describes the parameters.

Parameter	Description
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. This parameter is optional.
Status	It specifies whether to enable a rule. The options include: ● **Enable**: It indicates that a rule is enabled. ● **Disable**: It indicates that a rule is disabled.

3. Set the parameters and click **OK**.

The LAN Setup page appears, showing the added rule. See the following figure.



DHCP Reservation

□	IP Address	MAC Adress	Remark	Status	Action
□	192.168.0.105	44:37:E6:12:34:56	Administrator	Enabled	⊘ ✎ 🗑

Modifying a rule

1. Choose **Network** > **LAN Setup**.
2. Click ✎ corresponding to a rule to be modified.
3. Modify the rule.
4. To disable a rule, click ⊘ corresponding to the rule.
5. To enable a rule, click ✓ corresponding to the rule.

Deleting a rule

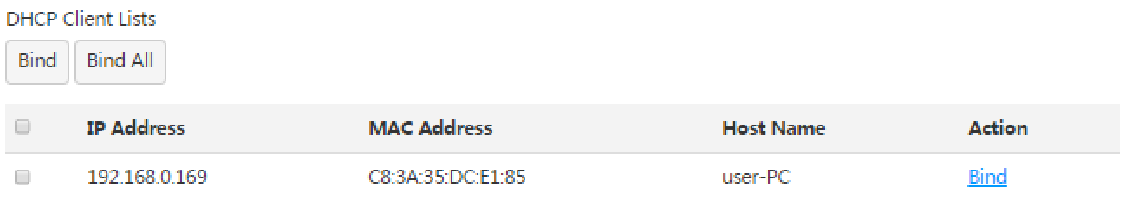
1. Choose **Network** > **LAN Setup**.
2. Click 🗑 corresponding to a rule to be deleted.

   The rule is deleted.
3. To delete multiple rules at the same time, select them and click 🗑 Delete.

4.3.4 DHCP Client List

If the DHCP server function of the router is enabled, you can refer to the DHCP client list for details (including IP addresses, MAC addresses, and host names) of the clients that obtain IP addresses from the DHCP server.

In addition, you can quickly bind clients with their current IP addresses so that the DHCP server always assigns the IP addreses to the clients.



DHCP Client Lists

□	IP Address	MAC Address	Host Name	Action
□	192.168.0.169	C8:3A:35:DC:E1:85	user-PC	Bind

Binding a client

1. Choose **Network** > **LAN Setup**.
2. Click Bind corresponding to the client to the bound in the **DHCP Client Lists** area.
   The client is bound with its current IP address.

Binding clients in batches

1. Choose **Network** > **LAN Setup**.

2. Select the clients to be bound in the **DHCP Client Lists** area and click Bind.

   The clients are bound with their current IP addresses.

Binding all clients

1. Choose **Network** > **LAN Setup**.

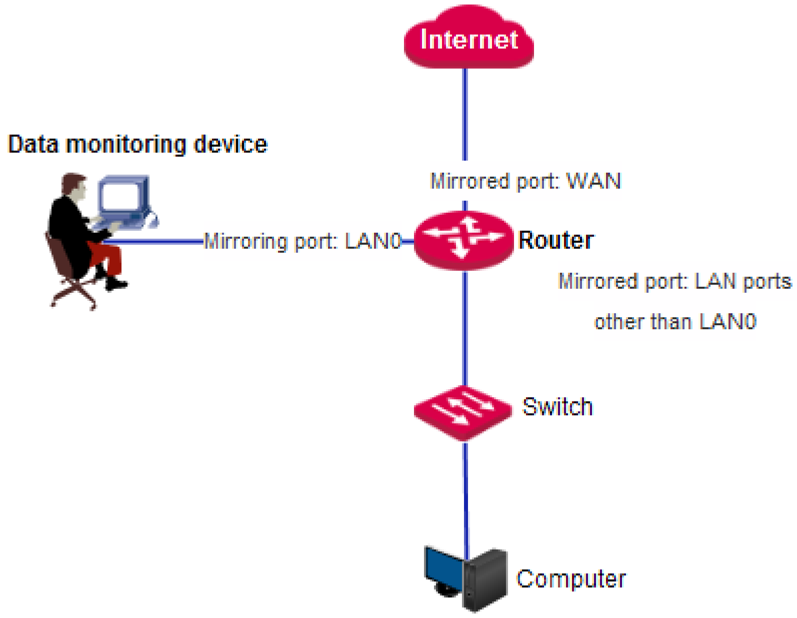
2. Click Bind All in the **DHCP Client Lists** area.

   All the clients are bound with their current IP addresses.

4.4 Configuring port mirroring

4.4.1 Overview

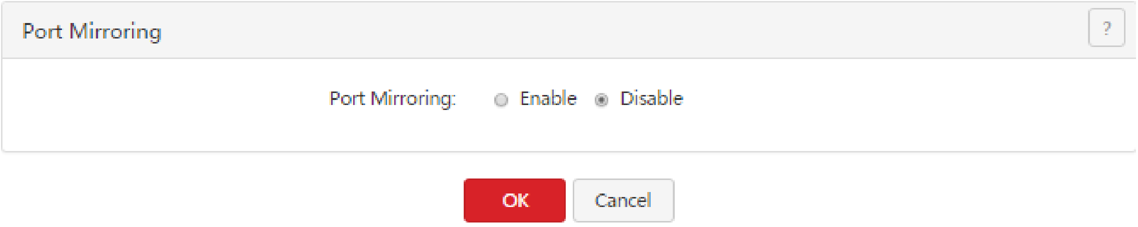
M50 provides the port mirroring function, which enables you to replicate data from one or more ports of the router (mirrored ports) to a specified port (mirroring port). Generally, a data monitoring device is deployed at the mirroring port so that network an administrator can monitor traffic, analyze performance, and diagnose faults in real time. The following figure shows the network topology for port mirroring.



The mirroring port of M50 is fixed to LAN0 and cannot be changed in the current version.

4.4.2 Configuring port mirroring

To access the port mirroring page, choose **Network** > **Port Mirroring**. The following figure shows the default setting.



Port Mirroring

Port Mirroring: ○ Enable ● Disable

If this function is required, set **Port Mirroring** to **Enable**, select mirrored ports, and click **OK**.

The following table describes the parameters.

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. A piece of monitoring software must be installed on the computer with this port to perform monitoring. The default mirroring port is LAN0 and cannot be changed in the current version.
Mirrored Port	It specifies the monitored ports. After the port mirroring function is enabled, packets of the mirrored ports are replicated to the mirroring port for monitoring.

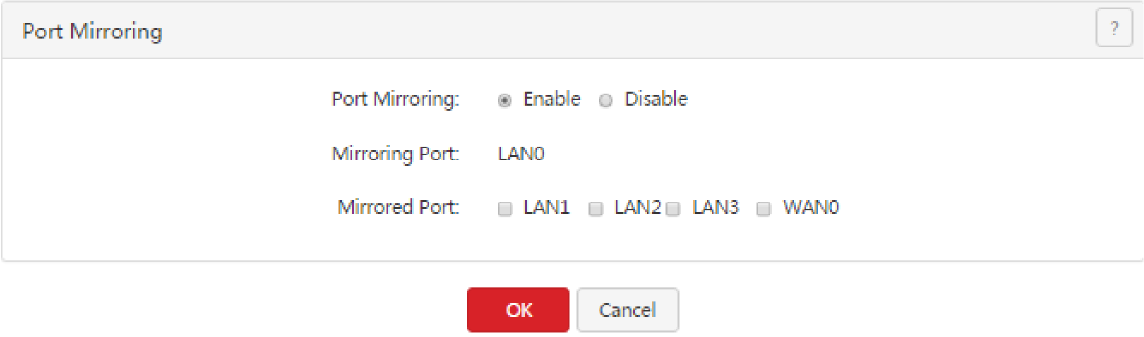
4.4.3 Port mirroring configuration example

Networking requirement

An enterprise has used M50 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** and set **Port Mirroring** to **Enable**.
2. Set **Mirrored Port** to **LAN1**, **LAN2**, **WAN1**, and **WAN0**.
3. Click **OK**.



Port Mirroring

Port Mirroring: ● Enable ○ Disable

Mirroring Port: LAN0

Mirrored Port: □ LAN1 □ LAN2 □ LAN3 □ WAN0

Verification

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

4.5 Configuring a static route

4.5.1 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.

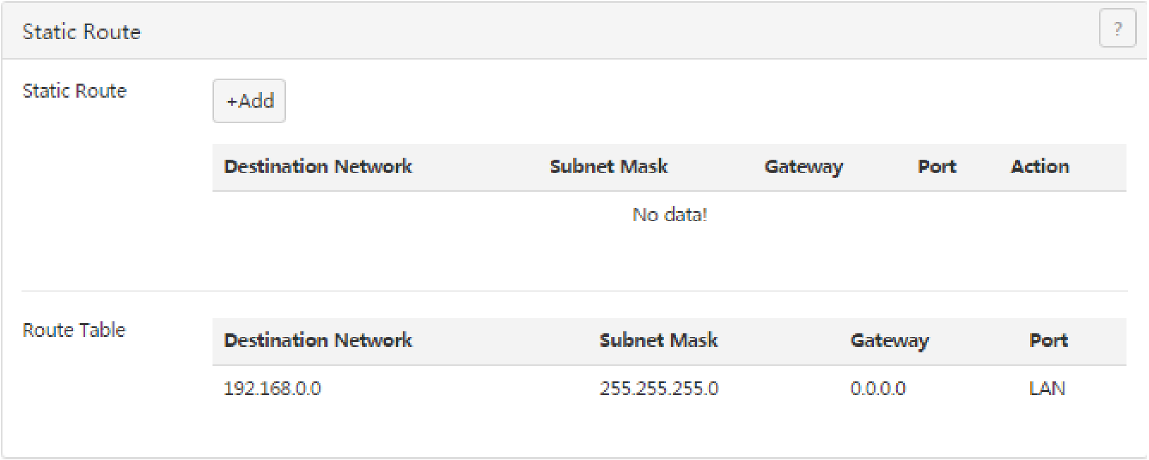
To define a static route, specify the network segment and subnet mask used to identify a destination network or host, the gateway IP address, and the router WAN port for forwarding packets. After a static route is defined, all the packets indented for the destination of the static route are directly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

4.5.2 Configuring a static route

To access the page for configuring a static route, choose **Network** > **Static Route**. See the following figure.



Static Route

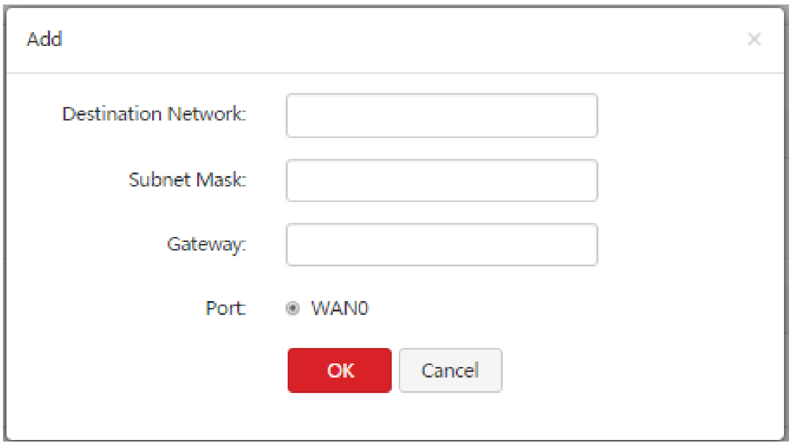
Destination Network	Subnet Mask	Gateway	Port	Action
No data!				

Route Table

Destination Network	Subnet Mask	Gateway	Port
192.168.0.0	255.255.255.0	0.0.0.0	LAN

Adding a static route

1. Choose **Network** > **Static Route** and click +Add. The **Add** dialog box appears.



Add

Destination Network:

Subnet Mask:

Gateway:

Port: ● WAN0

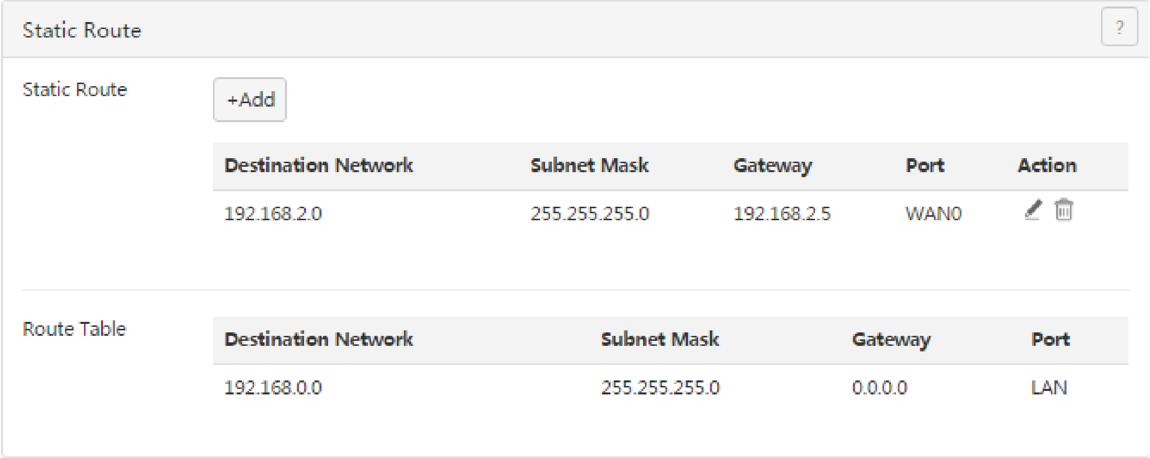
The following table describes the parameters.

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.

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

3. Choose **Network** > **Static Route** and view the added static route.

The available static routes are displayed in the **Route Table** module on the page. See the following figure.



Static Route

Static Route

Destination Network	Subnet Mask	Gateway	Port	Action
192.168.2.0	255.255.255.0	192.168.2.5	WAN0	✎ 🗑

Route Table

Destination Network	Subnet Mask	Gateway	Port
192.168.0.0	255.255.255.0	0.0.0.0	LAN

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 is in conflict with a user-defined multi-WAN policy, the static route takes preference over the policy**.**

Modifying a static route

1. Choose **Network** > **Static Route**.
2. Click ✎ corresponding to the static route to be modified in the **Static Route** area.
3. Modify the static route.

Deleting a static route

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

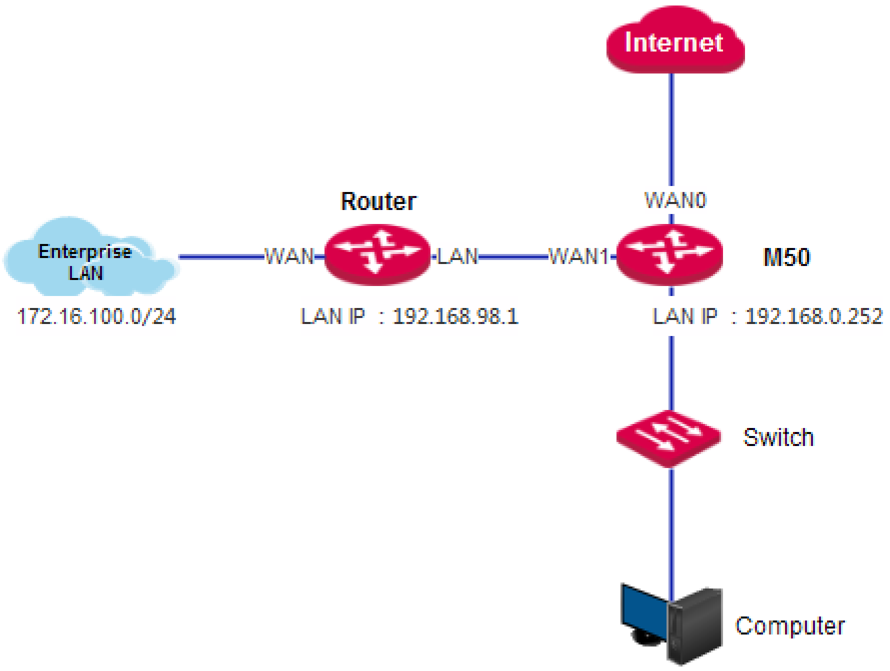
   The static route is deleted.

4.5.3 Static route configuration example

Networking requirement

An enterprise uses M50 for network construction. The internet is inaccessible to the enterprise LAN. The WAN0 port of M50 accesses the internet using a PPPoE connection and the WAN1 port of M50 accesses the enterprise LAN using a dynamic IP address. Users on the M50 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.

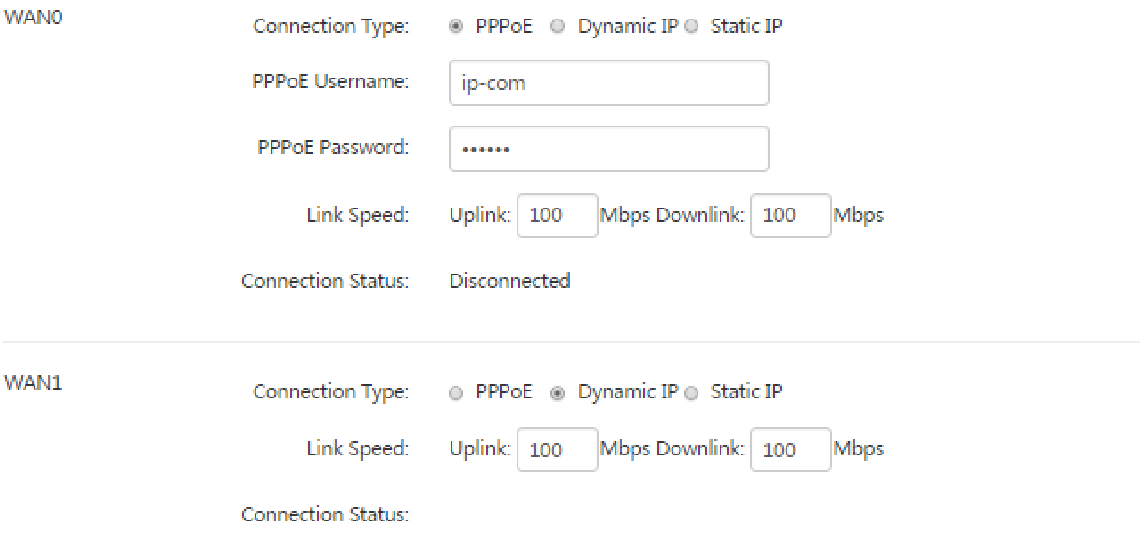


Configuration procedure

On the M50 web UI, set up an internet connection and configure a static route to address the requirement.

I. Set up an internet connection.

1. Choose **Network** > **Internet Setup**.
2. Set internet connection parameters.
3. Click **OK**.



WAN0

Connection Type: ● PPPoE ○ Dynamic IP ○ Static IP

PPPoE Username: ip-com

PPPoE Password: ••••••

Link Speed: Uplink: 100 Mbps Downlink: 100 Mbps

Connection Status: Disconnected

WAN1

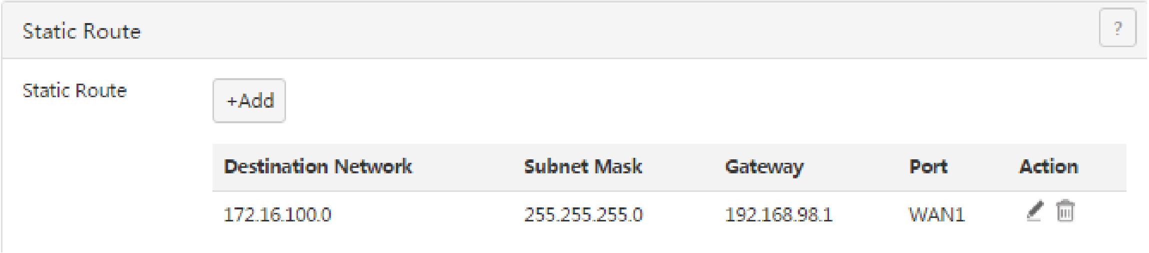
Connection Type: ○ PPPoE ● Dynamic IP ○ Static IP

Link Speed: Uplink: 100 Mbps Downlink: 100 Mbps

Connection Status:

II. Configure a static route.

1. Choose **Network** > **Static Route**.
2. Click +Add.
3. Configure the static route shown in the following figure.

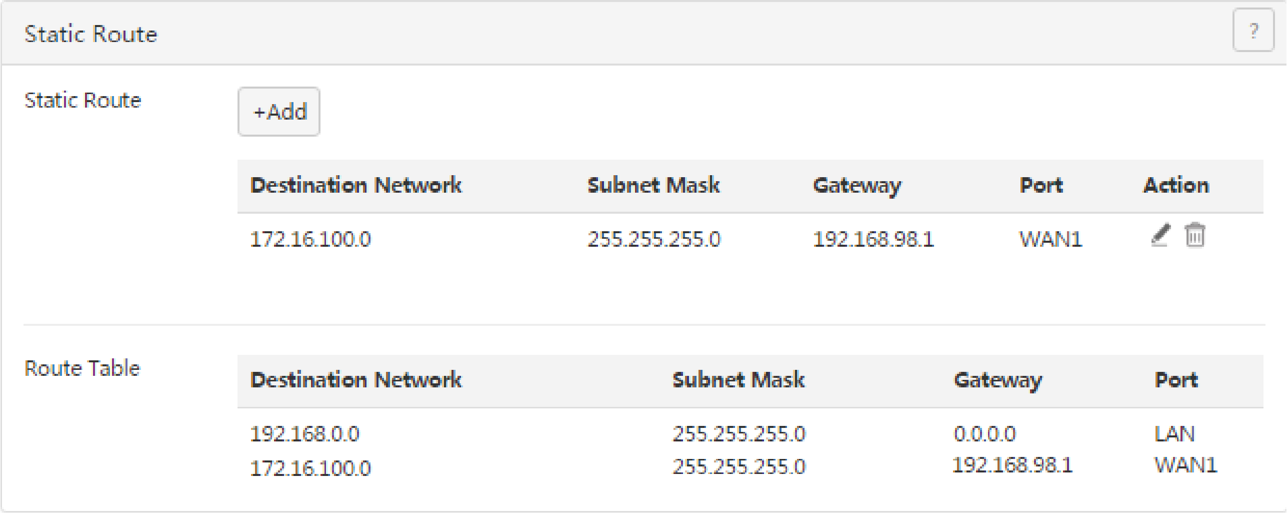


Static Route

Static Route +Add

Destination Network	Subnet Mask	Gateway	Port	Action
172.16.100.0	255.255.255.0	192.168.98.1	WAN1	✎ 🗑

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



Static Route

Static Route +Add

Destination Network	Subnet Mask	Gateway	Port	Action
172.16.100.0	255.255.255.0	192.168.98.1	WAN1	✎ 🗑

Route Table

Destination Network	Subnet Mask	Gateway	Port
192.168.0.0	255.255.255.0	0.0.0.0	LAN
172.16.100.0	255.255.255.0	192.168.98.1	WAN1

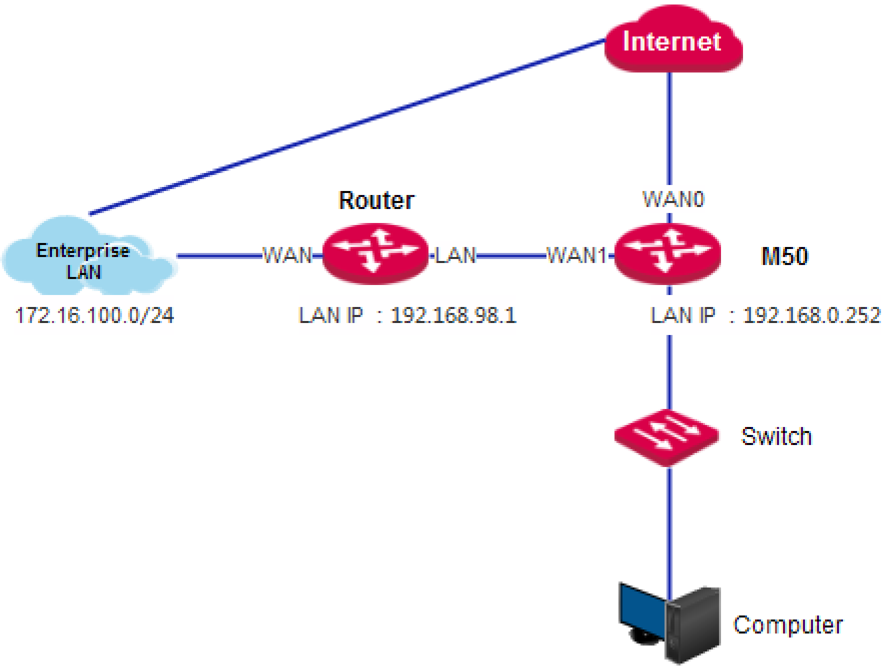
Verification

Access the internet and enterprise LAN using a computer on the M50 LAN.

Note

If the enterprise LAN is connected to the internet, as shown in the following figure, M50 may point its default route to the other router, resulting in incorrect routing. In this case, choose **Network** > **Internet Setup** and set **Link Speed** of the WAN1 port to a value far smaller than the value of **Link Speed** of the WAN0 port.

If the preceding case occurs, it is recommended that you disable the smart bandwidth control function of M50 and use a user-defined multi-WAN policy to ensure that all M50 LAN users access the internet through the WAN0 port of M50. Otherwise, a network exception may occur.



4.6 Using the Hotel mode

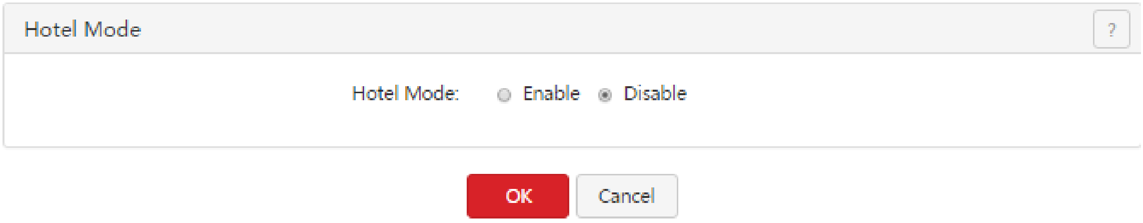
4.6.1 Overview

Generally, IP addresses are assigned automatically an M50 LAN for accessing the internet. In addition, IP addresses, gateway IP addresses, and DNS IP addresses can be manually configured for an M50 LAN to access the internet. Usually, a hotel has heavy traffic. Some of its guests configure their network adapters to obtain IP addresses automatically, some assign static IP addresses to their network adapters, and still some do not know how to configure their network adapters. In this case, hotel employees often need to help their guests configure network adapters, which bothers both the employees and guests.

To address this issue, M50 offers the Hotel mode. After a hotel enables this mode, computers in the LAN of the hotel can access the internet using any IP addresses (including IP addresses out of the IP address groups configured on M50), gateway IP addresses, and DNS IP addresses. Therefore, a guest of the hotel can access the internet through the hotel LAN without changing the network configuration of his/her network adapter.

4.6.2 Configuring the Hotel mode

To access the page for configuring the Hotel mode, choose **Network** > **Hotel Mode**. The following figure shows the default Hotel mode setting.



Hotel Mode

Hotel Mode: ○ Enable ● Disable

To enable the Hotel mode, select **Enable** and click **OK**.

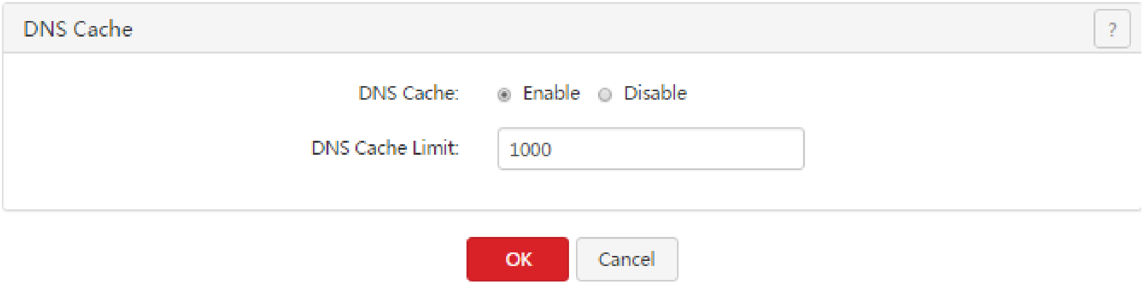
4.7 Configuring the DNS cache

4.7.1 Overview

M50 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.

4.7.2 Configuring the DNS cache

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



DNS Cache

DNS Cache: ● Enable ○ Disable

DNS Cache Limit: 1000

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

Chapter 5 Filter management

5.1 Overview

This chapter describes:

- Setting IP address groups and time groups
- 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 sets 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.

Note

If you set an IP address group, the LAN devices not included in the group cannot access the internet. In this case, add the devices that require internet accessibility to the group.

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 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 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 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

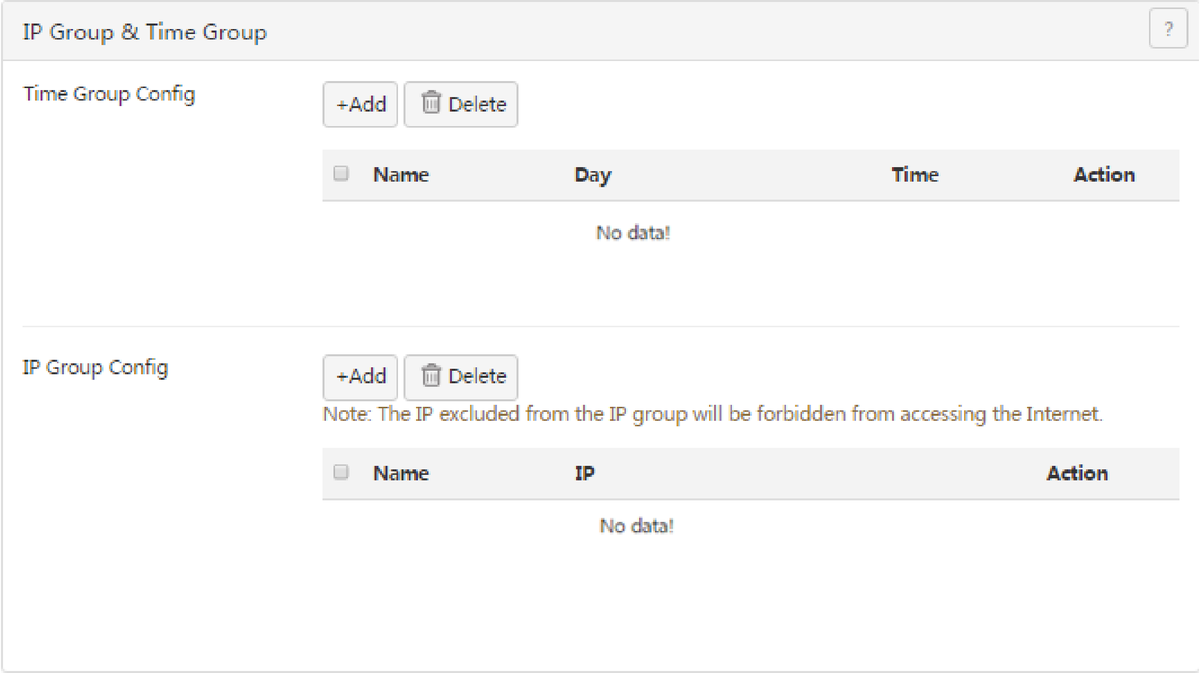
Step	Task	Description
1	Set IP address groups.	IP address groups are required when a multi-WAN policy is customized. Choose **Filter Management** > **IP Group & Time Group** and set IP address groups.
2	Customize a multi-WAN policy.	Choose **Filter Management** > **Multi-WAN Policy** and customize a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



IP Group & Time Group

Time Group Config

+Add | Delete

□	Name	Day	Time	Action

No data!

IP Group Config

+Add | Delete

Note: The IP excluded from the IP group will be forbidden from accessing the Internet.

□	Name	IP	Action

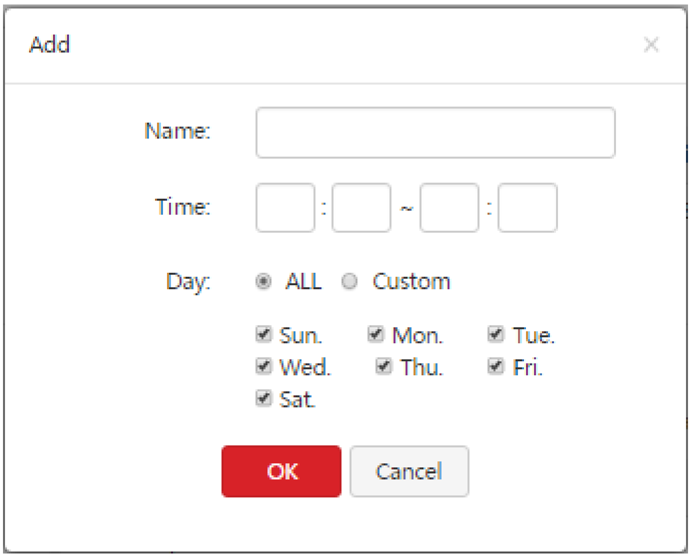
No data!

5.2.1 Setting time groups

Adding a time group

1. On the **Filter Management** > **IP Group & Time Group** page.
2. Click +Add in the **Time Group Config** area.

   The **Add** dialog box appears.



Add

Name:

Time: __ : __ ~ __ : __

Day: ● ALL ○ Custom

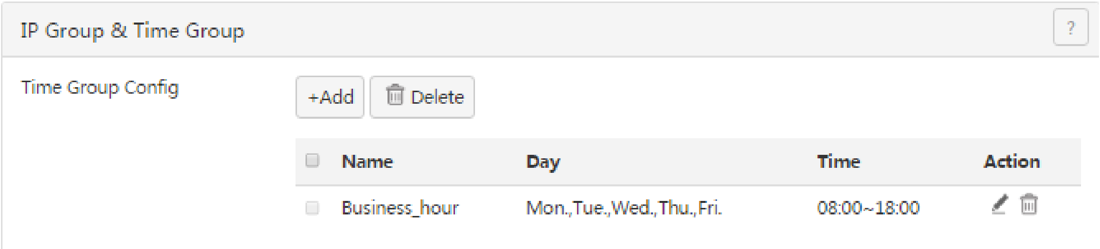
☑ Sun. ☑ Mon. ☑ Tue.
☑ Wed. ☑ Thu. ☑ Fri.
☑ Sat.

The following table describes the parameters.

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.

3. Set the parameters and click **OK**.

The **IP Group & Time Group** page appears, showing the added time group. See the following figure.



IP Group & Time Group

Time Group Config

□	Name	Day	Time	Action
□	Business_hour	Mon.,Tue.,Wed.,Thu.,Fri.	08:00~18:00	✎ 🗑

Modifying a time group

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

2. Click ✎ corresponding to an available time group.

3. Modify the group.
   If the time group has been referenced, the reference is updated when group modification is complete.

Deleting a time group

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

2. Click 🗑 corresponding to a time group to be deleted.

   The group is deleted.

3. 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

Note

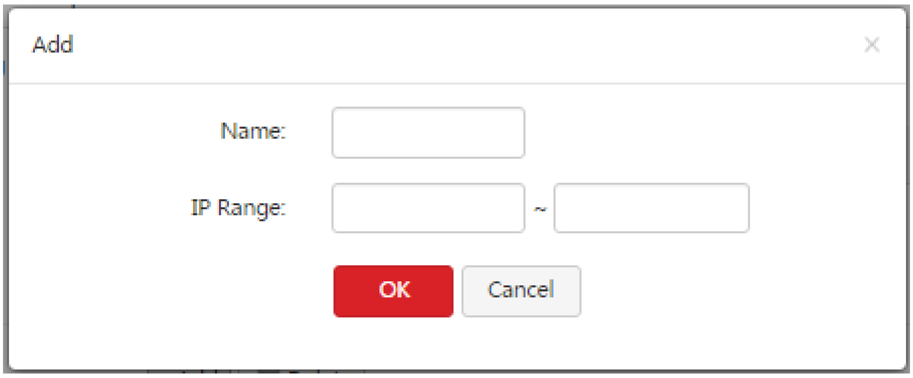
If you set an IP address group, the LAN devices not included in the group cannot access the internet. In this case, add the devices that require internet accessibility to the group.

Adding an IP address group

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

2. Click +Add in the **IP Group Config** area.

   The **Add** dialog box appears.

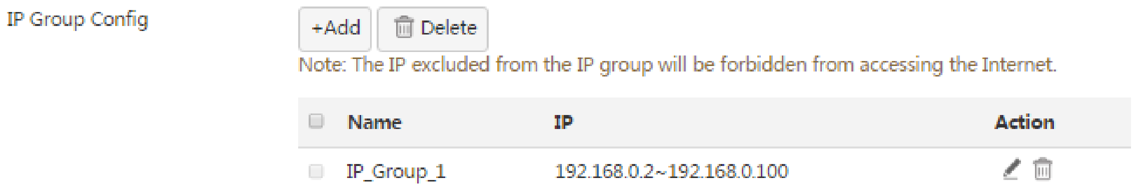


The following table describes the parameters.

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.

3. Set the parameters and click **OK**.

The **IP Group & Time Group** page appears, showing the added IP address group. See the following figure.



Note: The IP excluded from the IP group will be forbidden from accessing the Internet.

□	Name	IP	Action
□	IP_Group_1	192.168.0.2~192.168.0.100	✎ 🗑

Modifying an IP address group

1. Choose **Filter Management** > **IP Group & Time Group**.
2. Click ✎ corresponding to an available IP address group.
3. Modify the group.
   If the IP address group has been referenced, the reference is updated when group modification is complete.

Deleting an IP address group

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

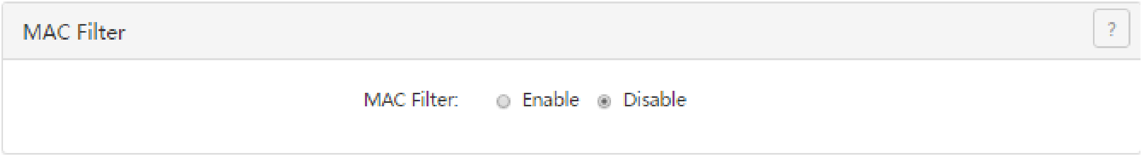
   The group is deleted.
3. To delete multiple IP address groups at the same time, select them and click 🗑 Delete.

⚠ **Note**

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

5.3 Setting the MAC address filter

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



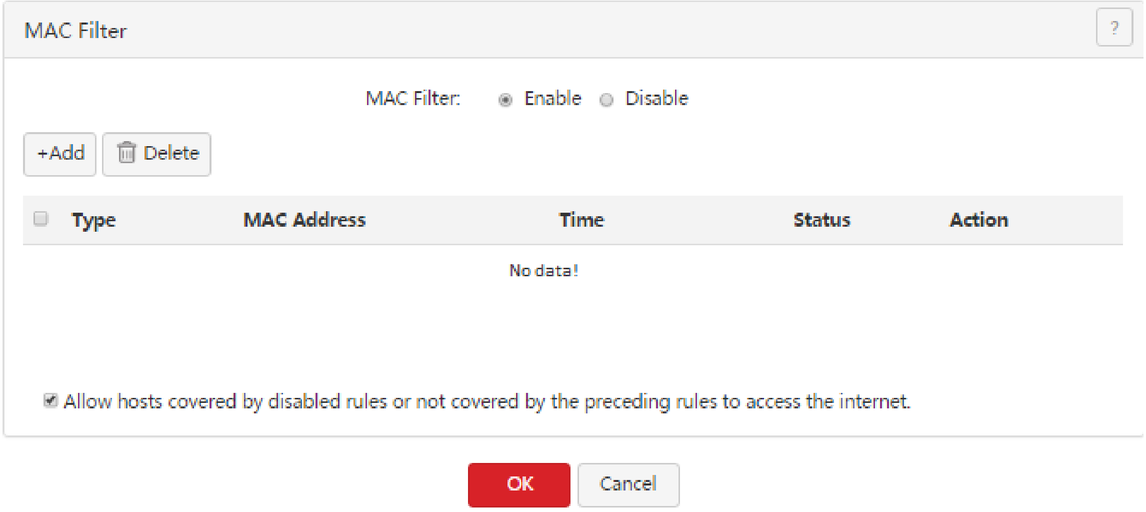
MAC Filter ?

MAC Filter: ○ Enable ● Disable

5.3.1 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**.
   The MAC address filter is enabled. Then, you can set MAC address filtering rules.



MAC Filter

MAC Filter: ● Enable ○ Disable

☐	Type	MAC Address	Time	Status	Action
			No data!		

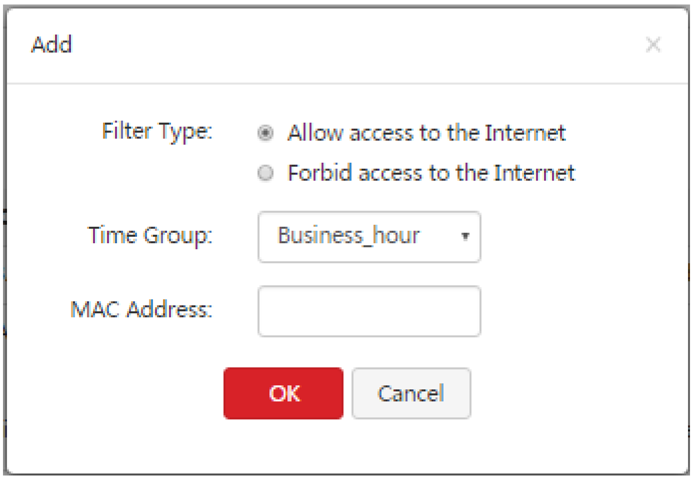
☑ Allow hosts covered by disabled rules or not covered by the preceding rules to access the internet.

Setting MAC address filtering rules

- Adding a rule

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

The **Add** dialog box appears.



Add

Filter Type: ● Allow access to the Internet
○ Forbid access to the Internet

Time Group: Business_hour

MAC Address:

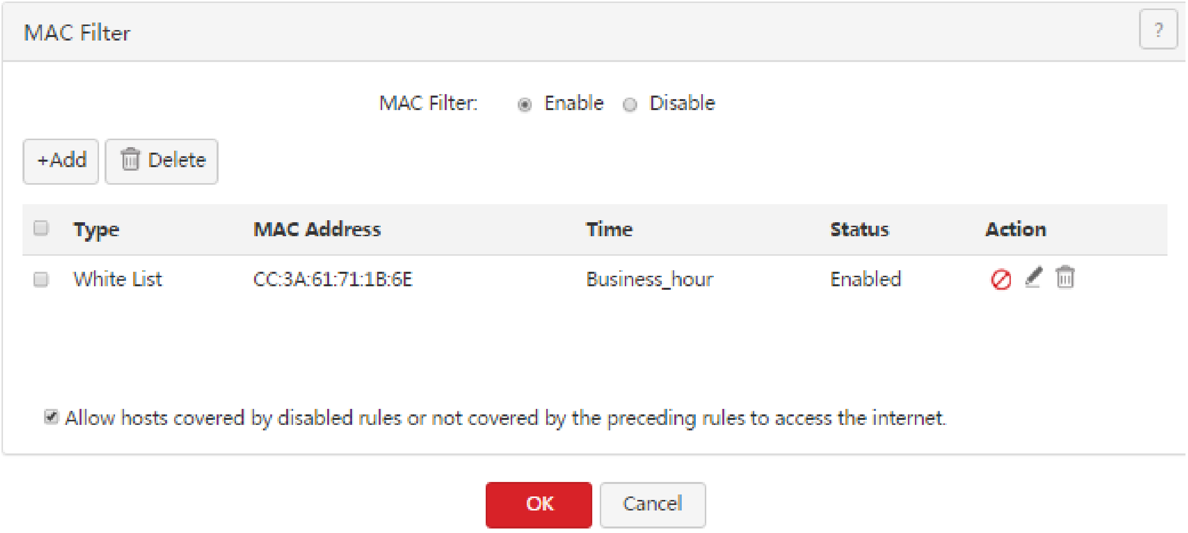
The following table describes the parameters.

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.

Parameter	Description
MAC Address	It specifies the MAC addresses to which a rule is applicable.

3. Set the parameters and click **OK**.

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



MAC Filter: ● Enable ○ Disable

□	Type	MAC Address	Time	Status	Action
□	White List	CC:3A:61:71:1B:6E	Business_hour	Enabled	⊘ ✎ 🗑

☑ Allow hosts covered by disabled rules or not covered by the preceding rules to access the internet.

The following table describes the parameters.

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.
3. Modify the 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.

3. To delete multiple MAC address filtering rules at the same time, select them and click 🗑 Delete .

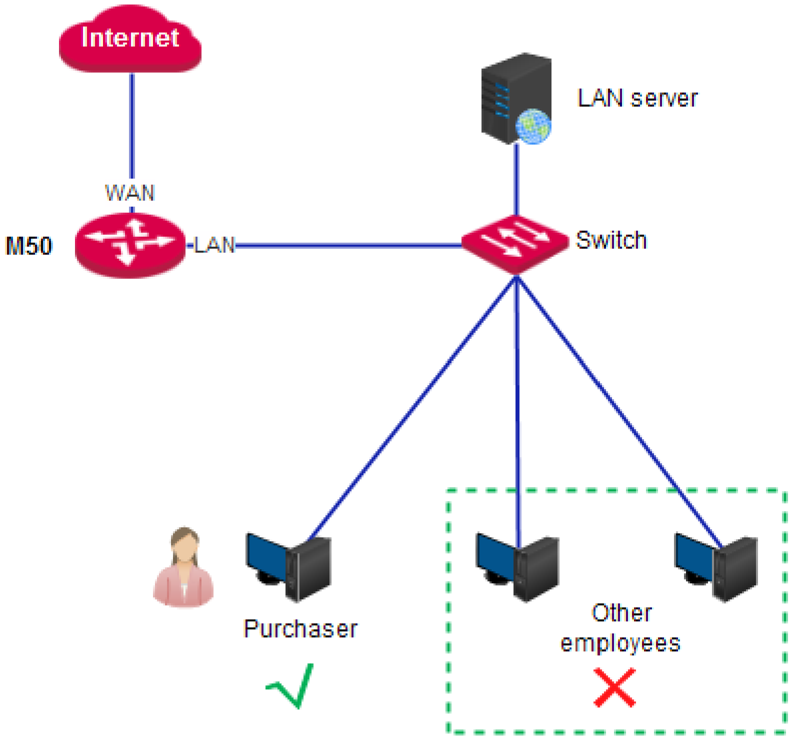
5.3.2 Example of setting the MAC address filter

Networking requirement

An enterprise uses M50 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.

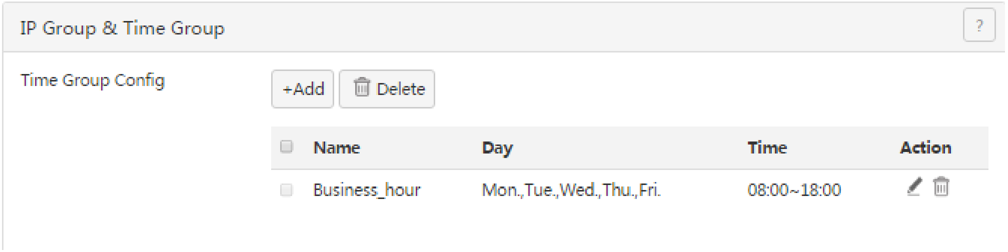


Configuration procedure

I. Set a time group.

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

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


IP Group & Time Group

Time Group Config

+Add | 🗑 Delete

□	Name	Day	Time	Action
□	Business_hour	Mon.,Tue.,Wed.,Thu.,Fri.	08:00~18:00	✎ 🗑

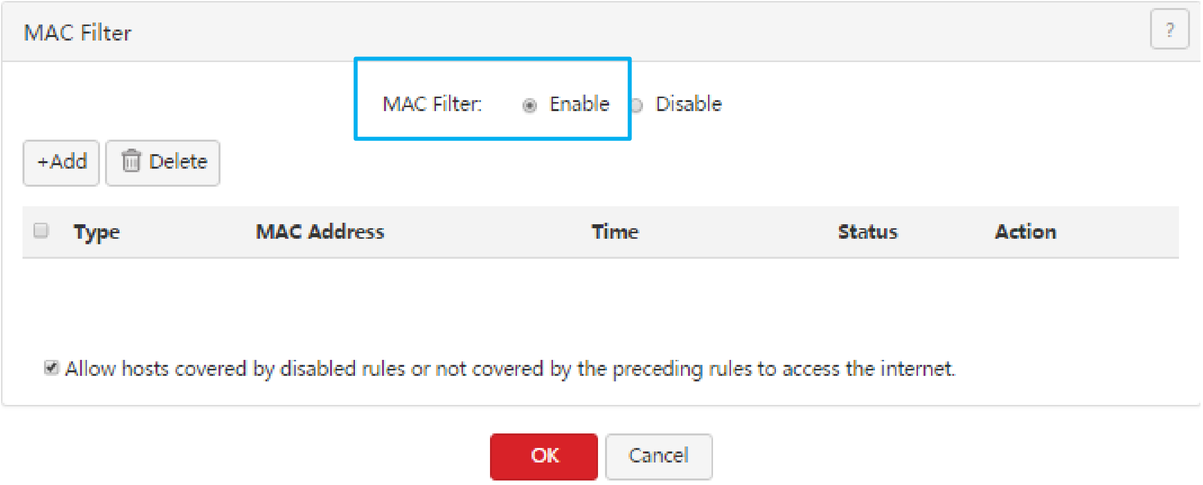
II. Set the MAC address filter.

1. Enable the MAC address filter.

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

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

(3) Click **OK**.



MAC Filter: ● Enable ○ Disable

□	Type	MAC Address	Time	Status	Action

☑ Allow hosts covered by disabled rules or not covered by the preceding rules to access the internet.

2. Set a MAC address filtering rule.

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

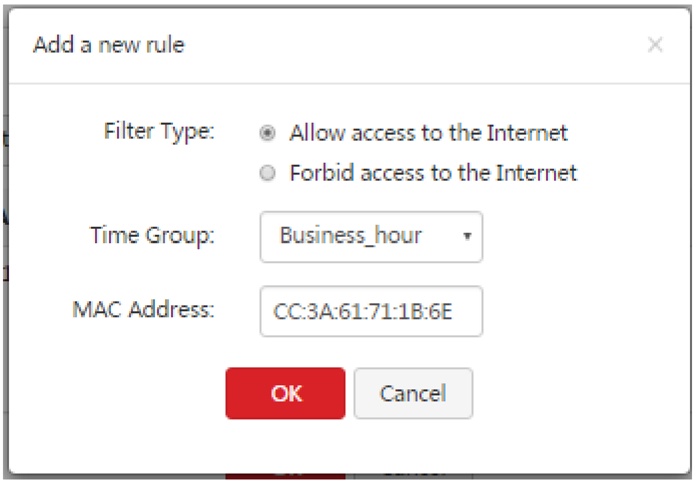
(2) Click +Add.

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

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

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

(6) Click **OK**.



Filter Type: ● Allow access to the Internet
○ Forbid access to the Internet

Time Group: Business_hour

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

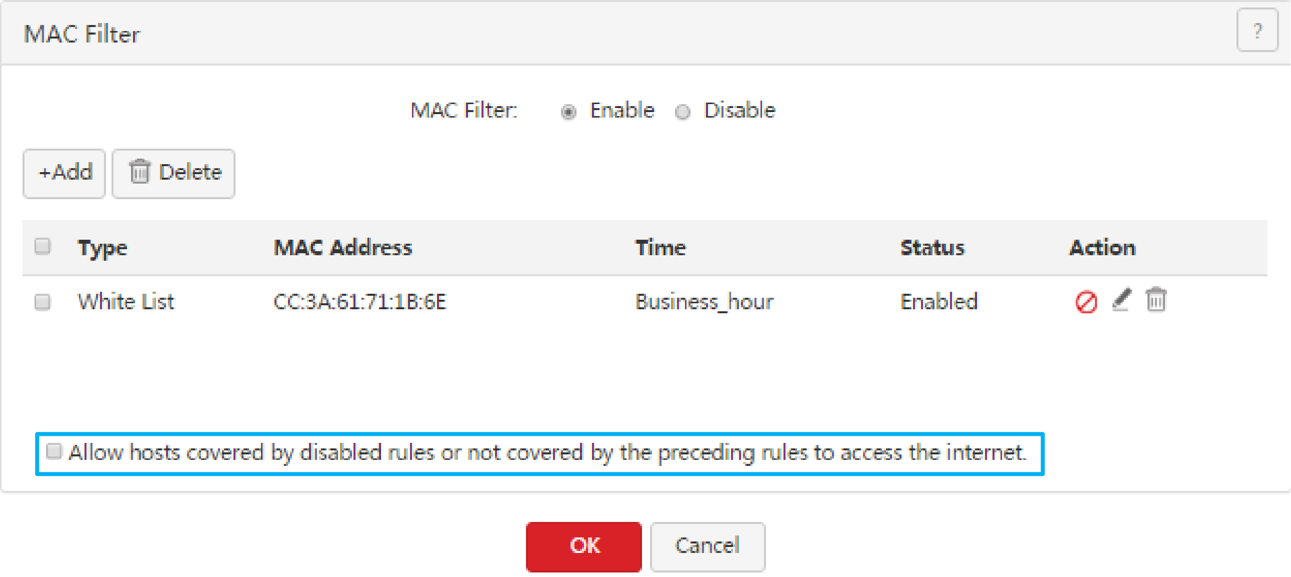
3. Prevent the hosts covered by disabled rules and the hosts not covered by rules to access the internet.

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

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

internet.

(3) Click **OK**.



MAC Filter

MAC Filter: ● Enable ○ Disable

□	Type	MAC Address	Time	Status	Action
□	White List	CC:3A:61:71:1B:6E	Business_hour	Enabled	

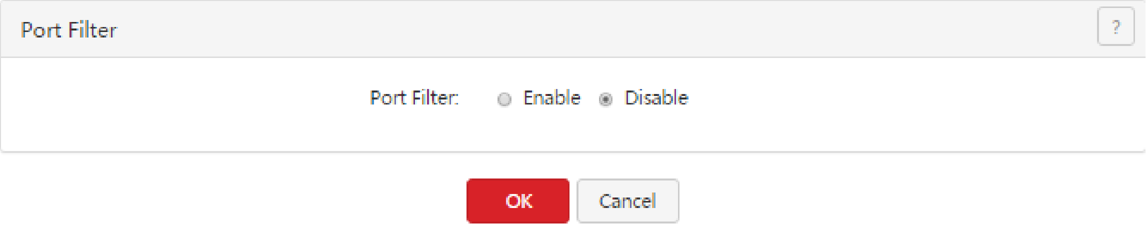
□ Allow hosts covered by disabled rules or not covered by the preceding rules to access the internet.

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.

5.4 Setting the port filter

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



Port Filter

Port Filter: ○ Enable ● Disable

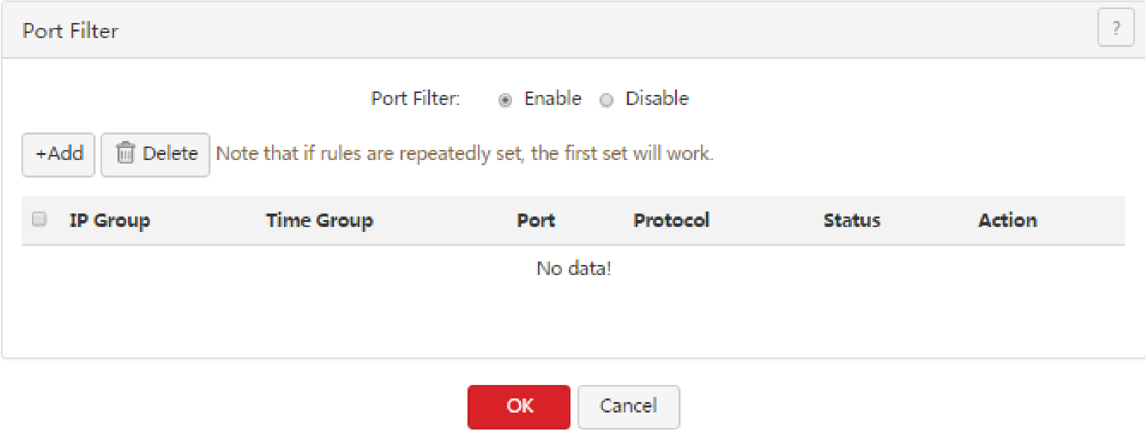
5.4.1 Setting the port filter

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.



Port Filter

Port Filter: ● Enable ○ Disable

+Add | Delete | Note that if rules are repeatedly set, the first set will work.

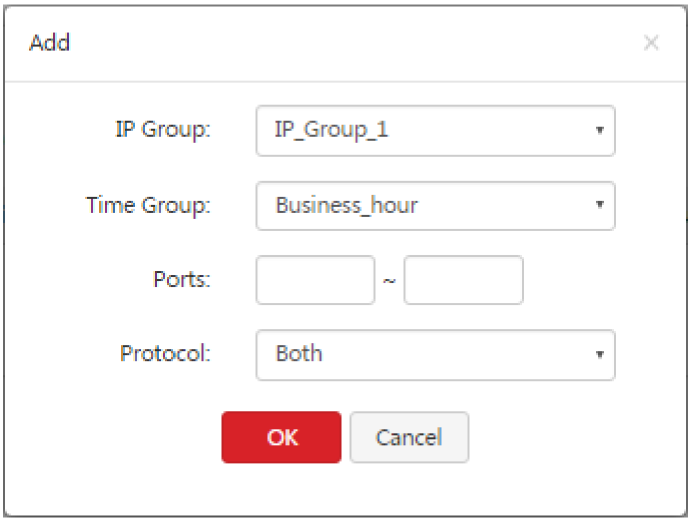
□	IP Group	Time Group	Port	Protocol	Status	Action
No data!						

Setting port filtering rules

- Adding a rule

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

The **Add a new rule** dialog box appears.



Add

IP Group: IP_Group_1

Time Group: Business_hour

Ports: ~

Protocol: Both

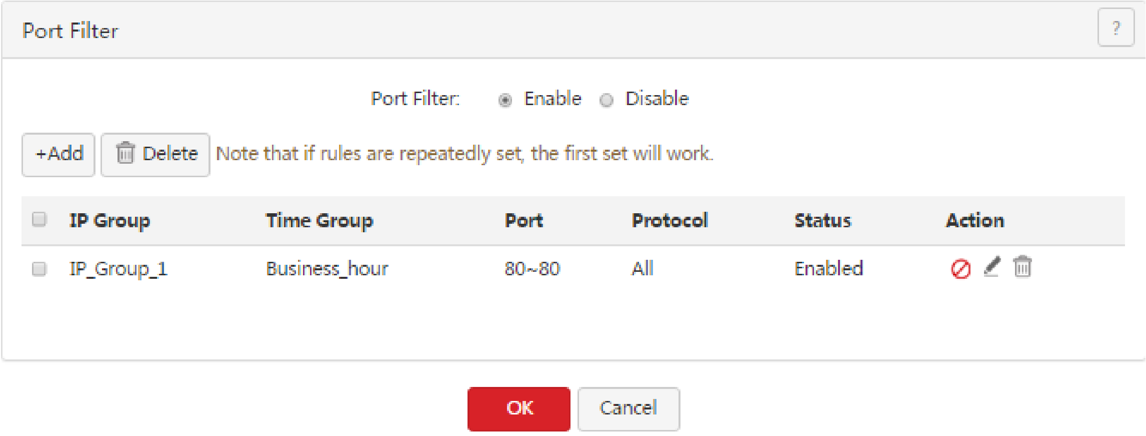
The following table describes the parameters.

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.

Parameter	Description
Protocol	It specifies the protocol of the inaccessible services. **Both** indicates TCP and UDP.

3. Set the parameters and click **OK**.

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



Port Filter

Port Filter: ● Enable ○ Disable

+Add | 🗑 Delete | Note that if rules are repeatedly set, the first set will work.

□	IP Group	Time Group	Port	Protocol	Status	Action
□	IP_Group_1	Business_hour	80~80	All	Enabled	⊘ ✎ 🗑

OK Cancel

- Modifying a rule

1. Choose **Filter Management** > **Port Filter**.
2. Click ✎ corresponding to a port filtering rule.
3. Modify the rule.
4. To disable a rule, click ⊘ corresponding to the rule.
5. To 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.

   The rule is deleted.

3. To delete multiple port filtering rules at the same time, select them and click 🗑 Delete.

5.4.2 Example of setting the port filter

Networking requirement

An enterprise uses M50 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.)

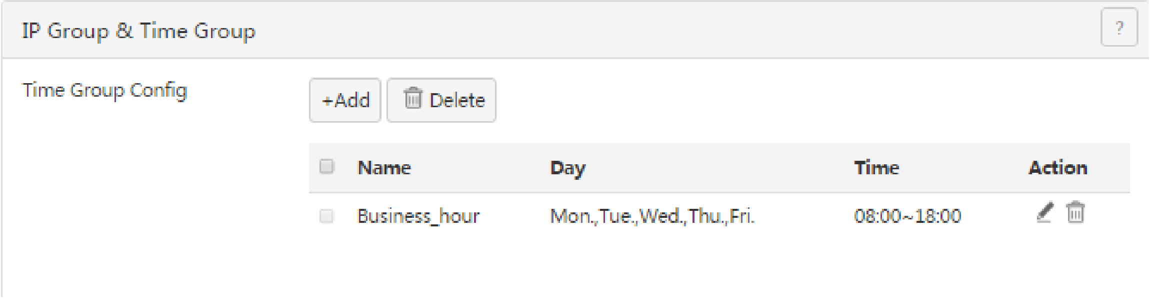
You can use the port filter of the router to meet this requirement.

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.



IP Group & Time Group

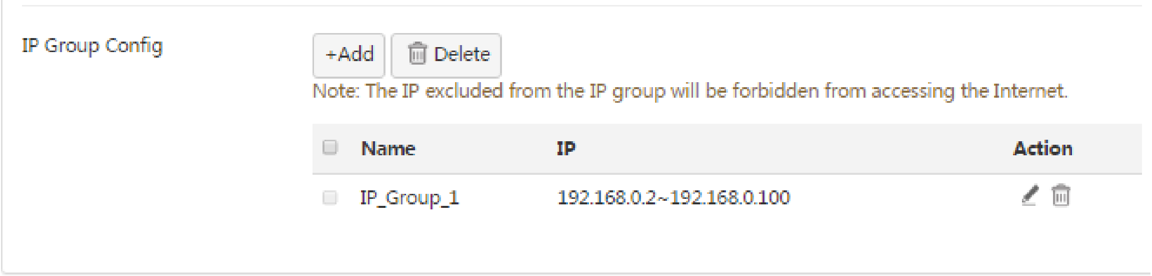
Time Group Config

□	Name	Day	Time	Action
□	Business_hour	Mon.,Tue.,Wed.,Thu.,Fri.	08:00~18:00	✎ 🗑

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.

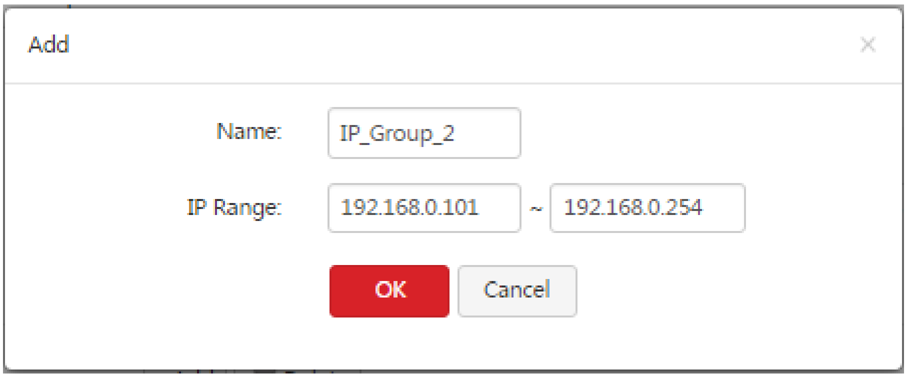


IP Group Config

Note: The IP excluded from the IP group will be forbidden from accessing the Internet.

□	Name	IP	Action
□	IP_Group_1	192.168.0.2~192.168.0.100	✎ 🗑

To allow the other computers with IP addresses ranging from 192.168.0.101 to 192.168.0.254 to access the internet, add another IP address group to include these IP addresses. See the following figure.



Add

Name: IP_Group_2

IP Range: 192.168.0.101 ~ 192.168.0.254

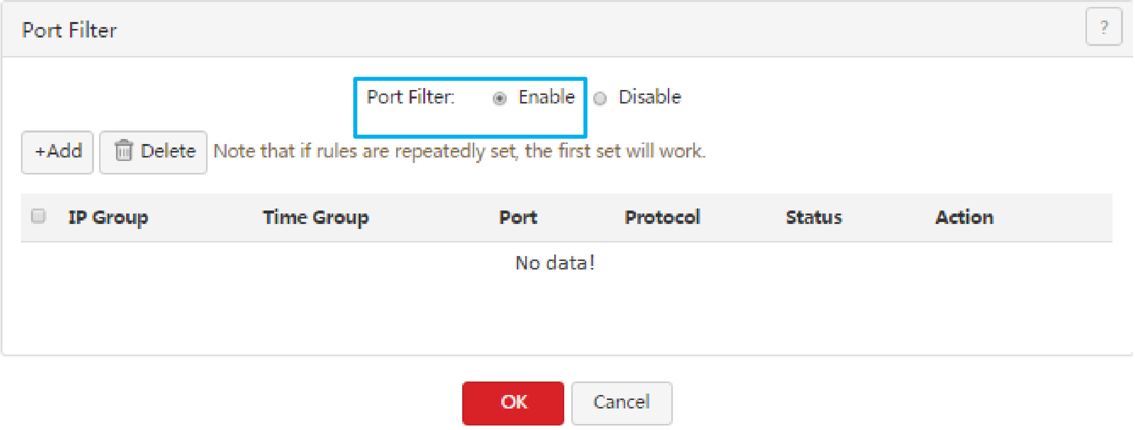
III. Set the port filter.

1. Enable the port filter as follows:

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

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

(3) Click **OK**.


Port Filter
?
Port Filter: ● Enable ○ Disable
+Add
Delete
Note that if rules are repeatedly set, the first set will work.
IP Group
Time Group
Port
Protocol
Status
Action
No data!
OK
Cancel

2. Set a port filtering rule.

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

(2) Click +Add.

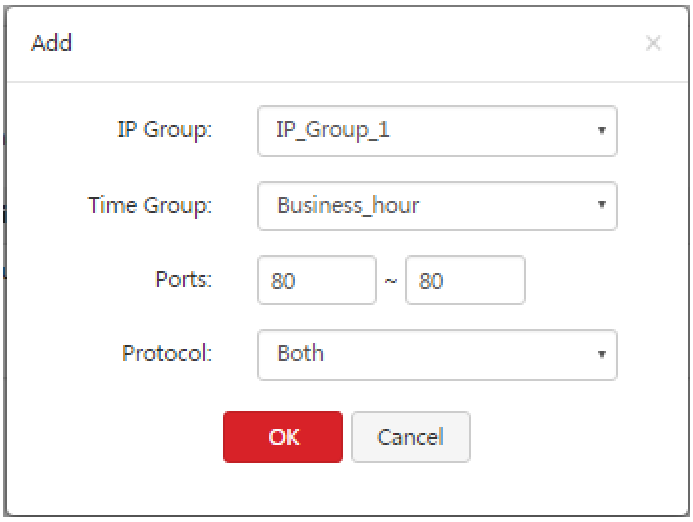
(3) Set **IP Group** to the IP address group that includes the computers disallowed to browse web pages.

(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 **Both** of **Protocol**.

(7) Click **OK**.



IP Group: IP_Group_1

Time Group: Business_hour

Ports: 80 ~ 80

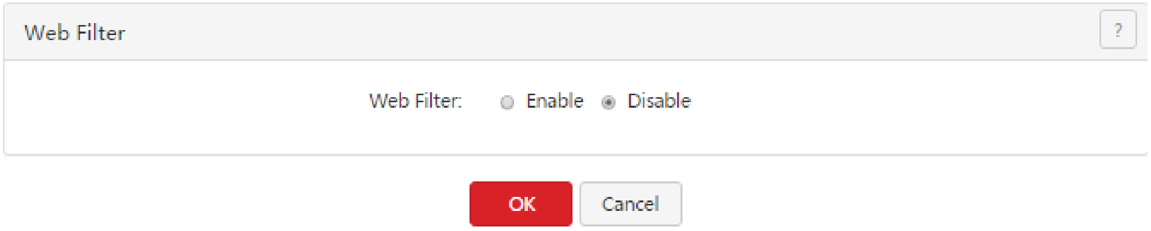
Protocol: Both

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.

5.5 Setting the web filter

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



Web Filter

Web Filter: ○ Enable ● Disable

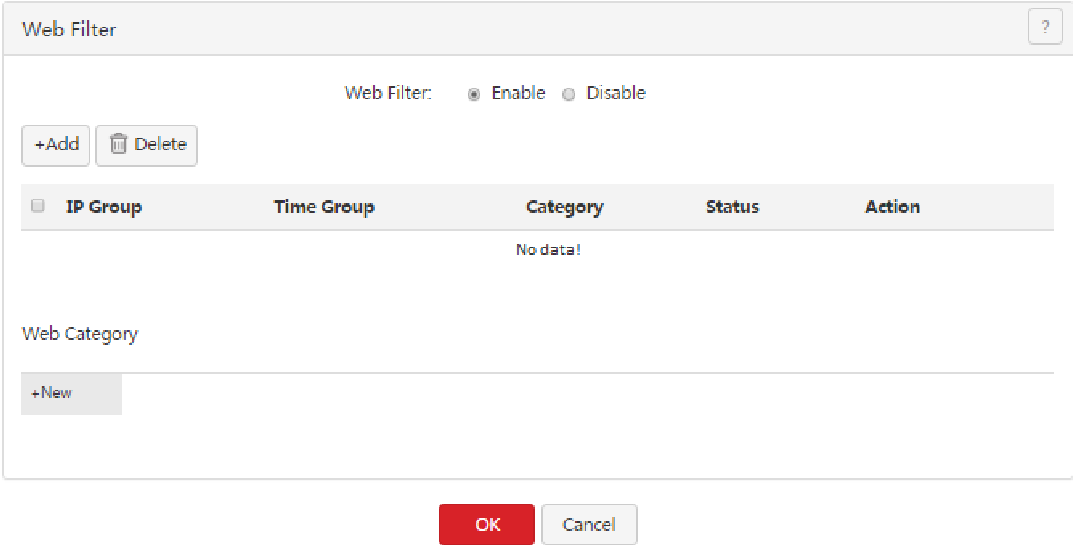
5.5.1 Setting the web filter

Enabling the web filter

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

2. Set **Web Filter** to **Enable**.

3. Click **OK**.



Web Filter

Web Filter: ● Enable ○ Disable

□	IP Group	Time Group	Category	Status	Action

No data!

Web Category

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

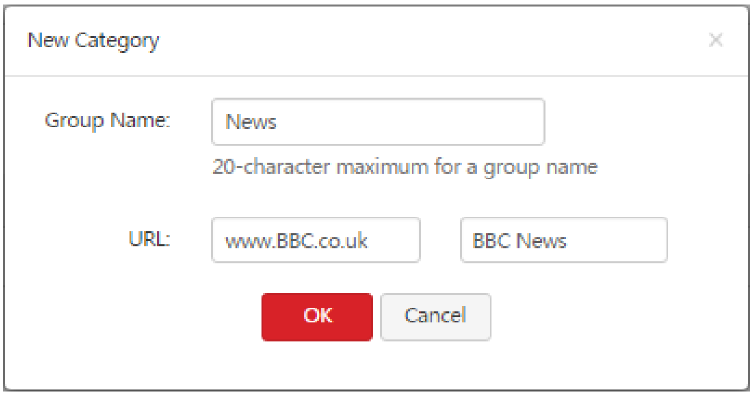
Adding a web categories

1. Choose **Filter Management** > **Web Filter**, click **+New** in the **Web Category** area.

2. Set **Group Name** to the name of a web category.

3. Set **URL** to the URL of a website to be used by web filters and the description of the website.

4. Click **OK**.



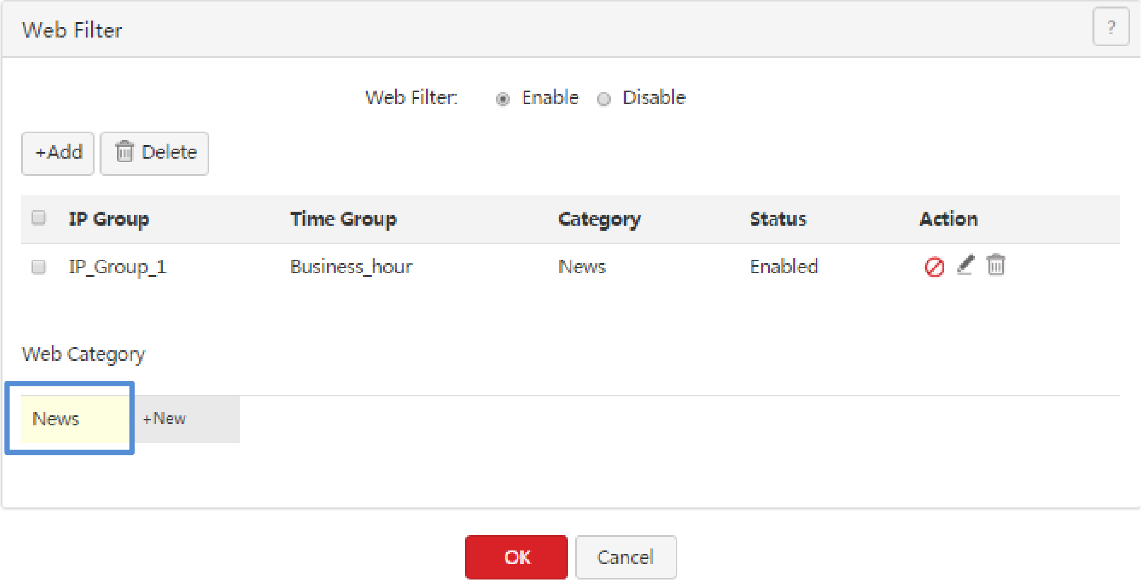
New Category

Group Name: News

20-character maximum for a group name

URL: www.BBC.co.uk BBC News

The Web Filter page appears, showing the added web category. See the following figure.



Web Filter

Web Filter: ● Enable ○ Disable

	IP Group	Time Group	Category	Status	Action
□	IP_Group_1	Business_hour	News	Enabled	

Web Category

News

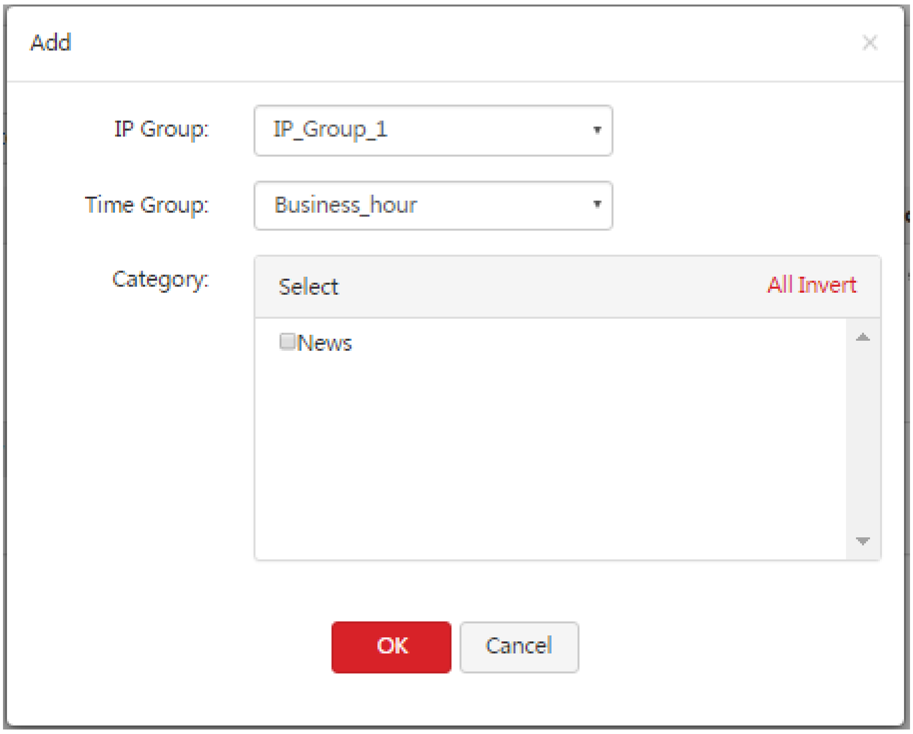
Setting web filtering rules

- Adding a rule

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

2. Click +Add.

The **Add** dialog box appears.



Add

IP Group: IP_Group_1

Time Group: Business_hour

Category:

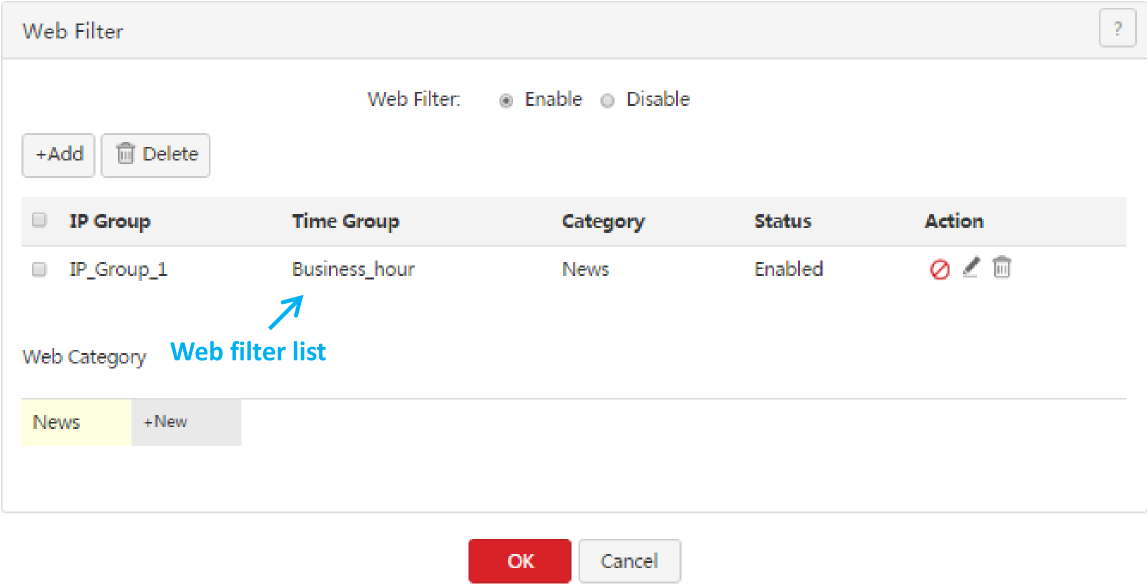
□News

The following table describes the parameters.

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.
Category	It specifies categories of websites inaccessible to specified users.

3. Set the parameters and click **OK**.

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



Web Filter

Web Filter: ● Enable ○ Disable

□	IP Group	Time Group	Category	Status	Action
□	IP_Group_1	Business_hour	News	Enabled	⊘ ✎ 🗑

Web Category

- Modifying a rule

1. Choose **Filter Management** > **Web Filter**.
2. Click ✎ corresponding to a web filtering rule.
3. Modify the rule.
4. To disable a rule, click ⊘ corresponding to the rule.
5. To 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.

   The rule is deleted.

3. To delete multiple web filtering rules at the same time, select them and click 🗑 Delete.

5.5.2 Example of setting the web filter

Networking requirement

An enterprise uses M50 to set up a LAN to address the following requirement:

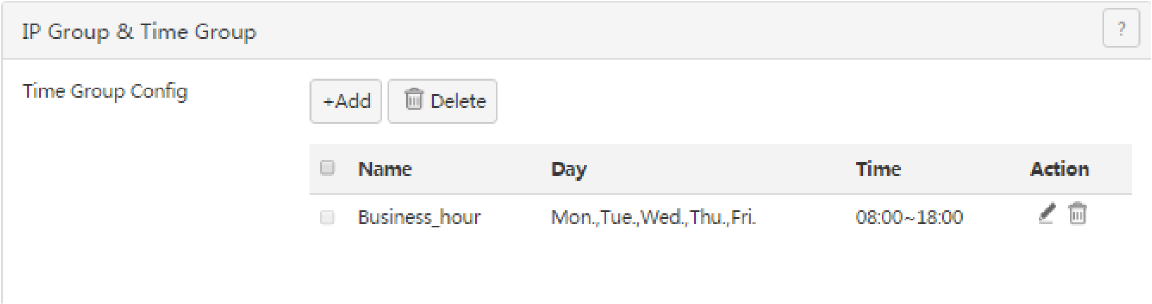
During business hours (08:00 to 18:00 every weekday), computers with IP addresses ranging from 192.168.0.2 to 192.168.0.100 are not allowed to browse news websites.

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.

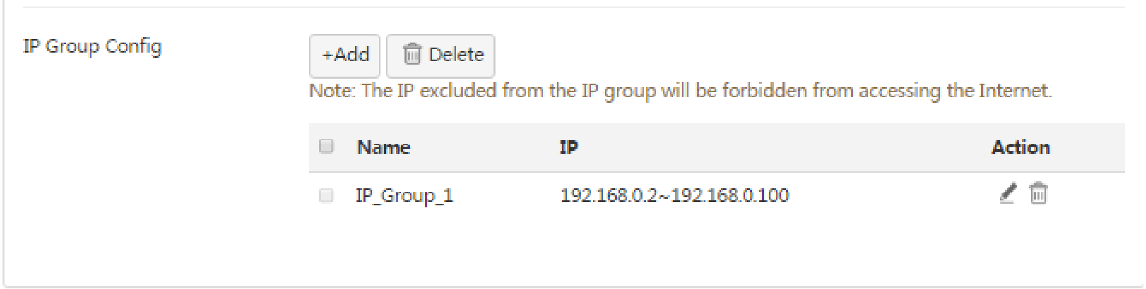


□	Name	Day	Time	Action
□	Business_hour	Mon.,Tue.,Wed.,Thu.,Fri.	08:00~18:00	✎ 🗑

II. Set an IP address group.

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

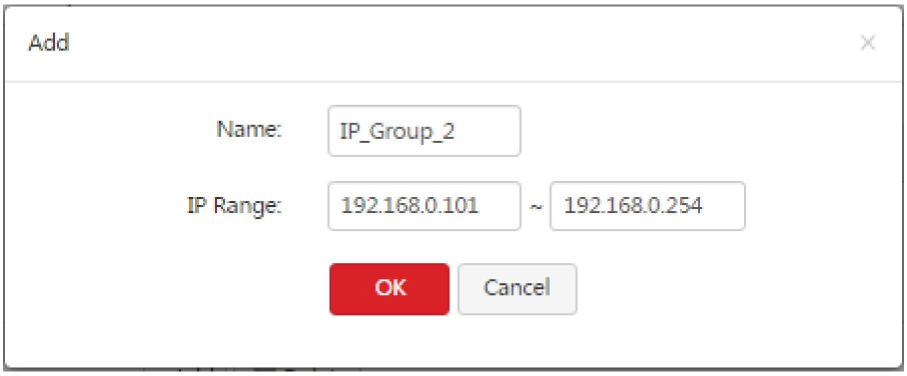
2. Set the IP address group shown in the following figure.



Note: The IP excluded from the IP group will be forbidden from accessing the Internet.

□	Name	IP	Action
□	IP_Group_1	192.168.0.2~192.168.0.100	✎ 🗑

To allow the other computers with IP addresses ranging from 192.168.0.101 to 192.168.0.254 to access the internet, add another IP address group to include these IP addresses. See the following figure.



Name: IP_Group_2

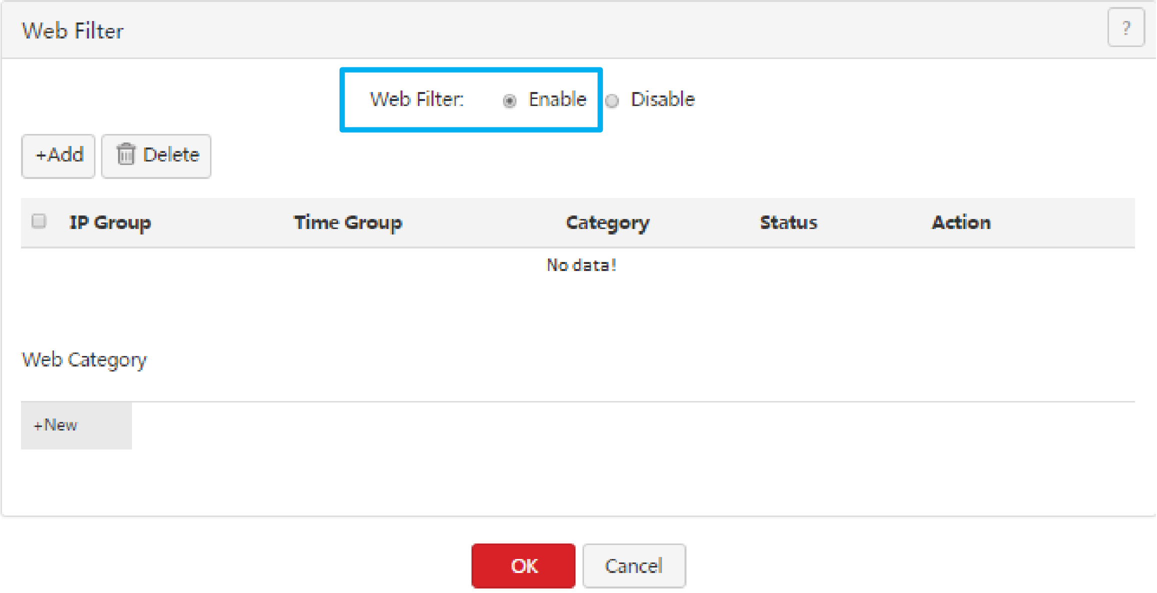
IP Range: 192.168.0.101 ~ 192.168.0.254

III. Enable the web filter.

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

2. Set **Web Filter** to **Enable**,

3. Click **OK**.



Web Filter: ● Enable ○ Disable

□ IP Group	Time Group	Category	Status	Action
		No data!		

IV. Add a web category.

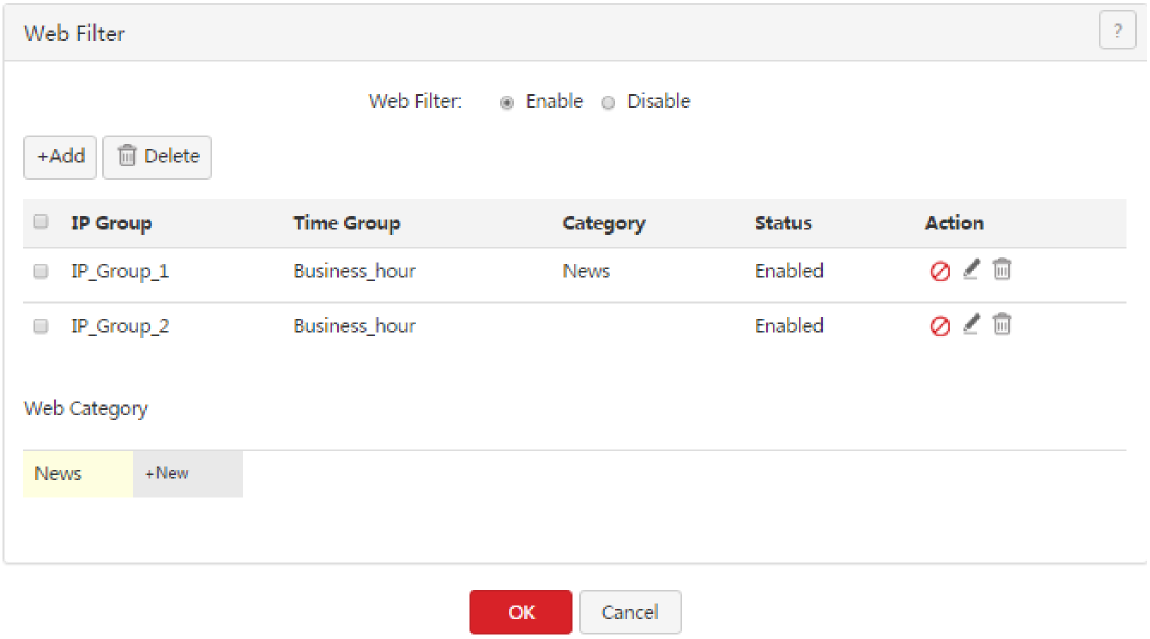
1. Choose **Filter Management** > **Web Filter**.

2. Click **+New**.

3. Set **Group Name** to **News**.

4. Set **URL** to the URL of a news website not accessible to the computers and the description of the website.

5. Click **OK**.



Web Filter ?

Web Filter: ● Enable ○ Disable

+Add | Delete

□	IP Group	Time Group	Category	Status	Action
□	IP_Group_1	Business_hour	News	Enabled	⊘ ✎ 🗑
□	IP_Group_2	Business_hour		Enabled	⊘ ✎ 🗑

Web Category

News | +New

OK | Cancel

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**.

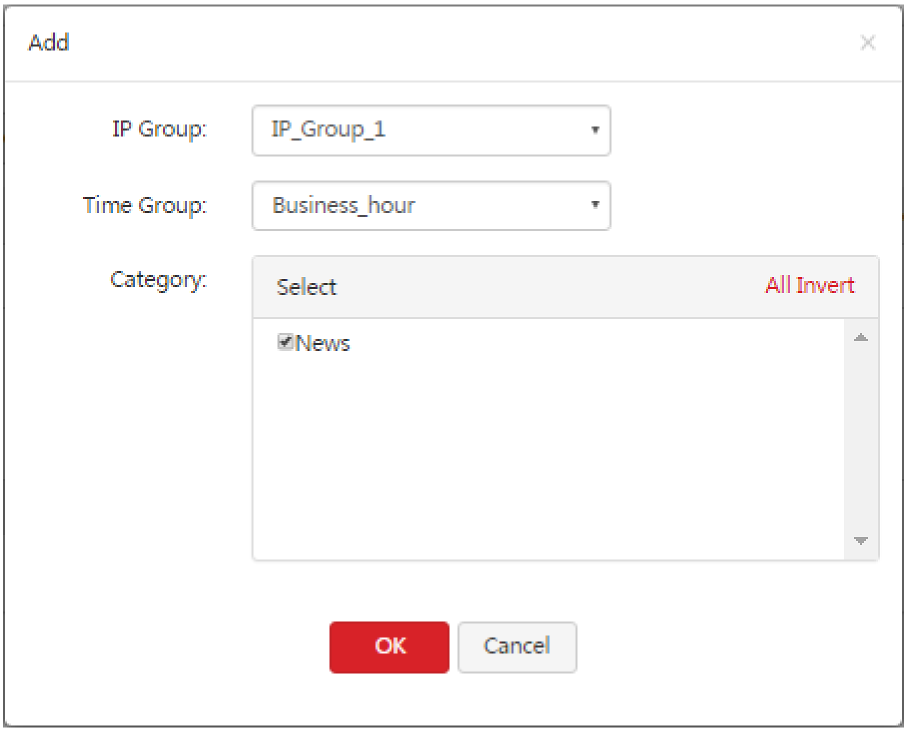
2. Click +Add.

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**.


Add

IP Group: IP_Group_1

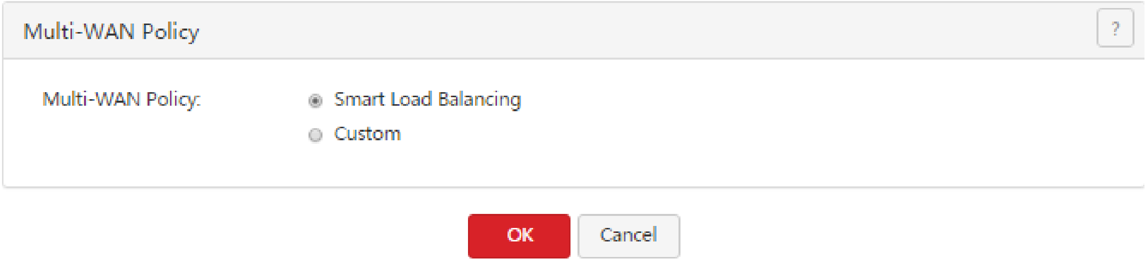
Time Group: Business_hour

Category:

☑News

5.6 Setting multi-WAN policies

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


Multi-WAN Policy

Multi-WAN Policy: ● Smart Load Balancing ○ Custom

The following table describes the parameters.

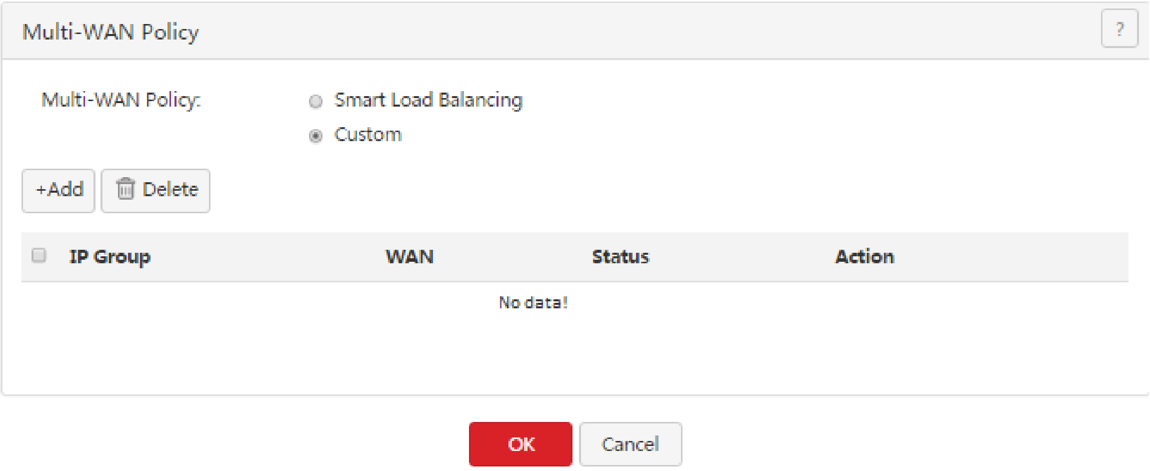
Parameter	Description
Smart Load Balancing	It specifies that the system automatically distributes traffic based on the following rules through the WAN ports to achieve load balancing: ● If the usage of the bandwidths specified by **Link Speed** preset on the **Network** > **Internet Setup** page is lower 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.

Parameter	Description
Custom	It enables you to assign WAN ports to source IP addresses as required.

5.6.1 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**.



Multi-WAN Policy

Multi-WAN Policy: ○ Smart Load Balancing ● Custom

□	IP Group	WAN	Status	Action

No data!

Then, you can customize multi-WAN policies.

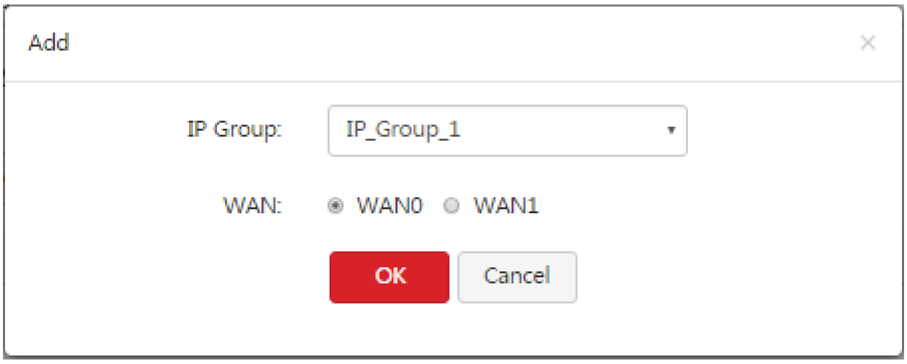
Setting multi-WAN rules

- Adding a rule

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

(2) Click +Add.

The **Add** dialog box appears.



Add

IP Group: IP_Group_1

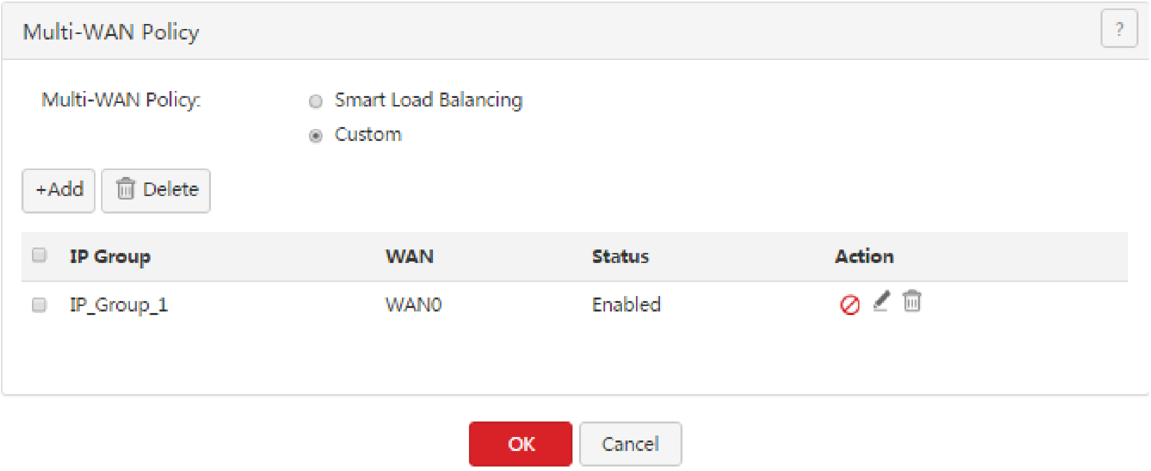
WAN: ● WAN0 ○ WAN1

The following table describes the parameters.

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.

(3) Set the parameters and click **OK**.

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



Multi-WAN Policy ?

Multi-WAN Policy: ○ Smart Load Balancing ● Custom

+Add 🗑 Delete

□	IP Group	WAN	Status	Action
□	IP_Group_1	WAN0	Enabled	⊘ ✎ 🗑

OK Cancel

- Modifying a rule

1. Choose **Filter Management** > **Multi-WAN Policy**.
2. Click ✎ corresponding to a rule.
3. Modify the rule.
4. To disable a rule, click ⊘ corresponding to the rule.
5. To 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.

   The rule is deleted.

3. To delete multiple web filtering rules at the same time, select them and click 🗑 Delete.

5.6.2 Example of customizing a multi-WAN policy

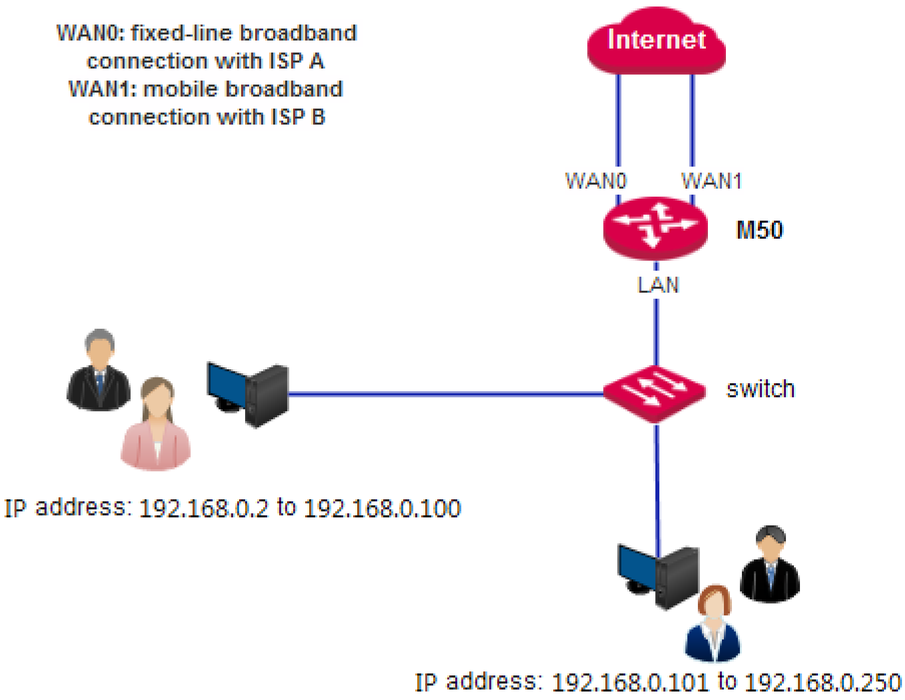
Networking requirement

An enterprise has used M50 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.

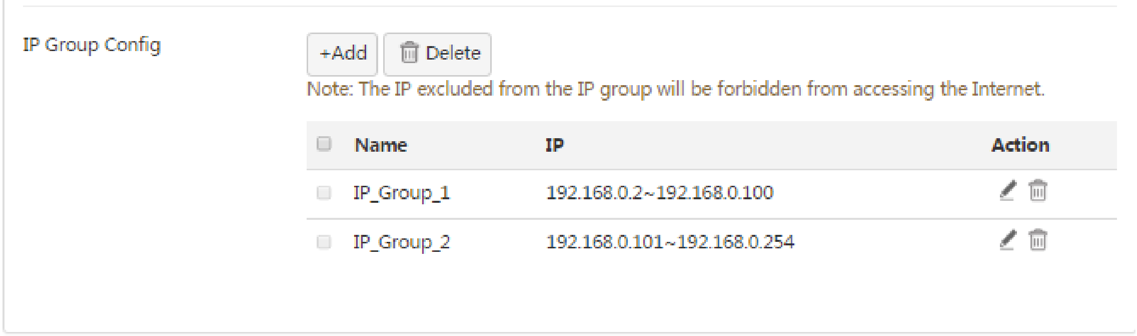
Network topology


WAN0: fixed-line broadband connection with ISP A
WAN1: mobile broadband connection with ISP B
Internet
WAN0
WAN1
M50
LAN
switch
IP address: 192.168.0.2 to 192.168.0.100
IP address: 192.168.0.101 to 192.168.0.250

Configuration procedure

I. Set an IP address group.

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



IP Group Config

+Add | Delete

Note: The IP excluded from the IP group will be forbidden from accessing the Internet.

□	Name	IP	Action
□	IP_Group_1	192.168.0.2~192.168.0.100	
□	IP_Group_2	192.168.0.101~192.168.0.254	

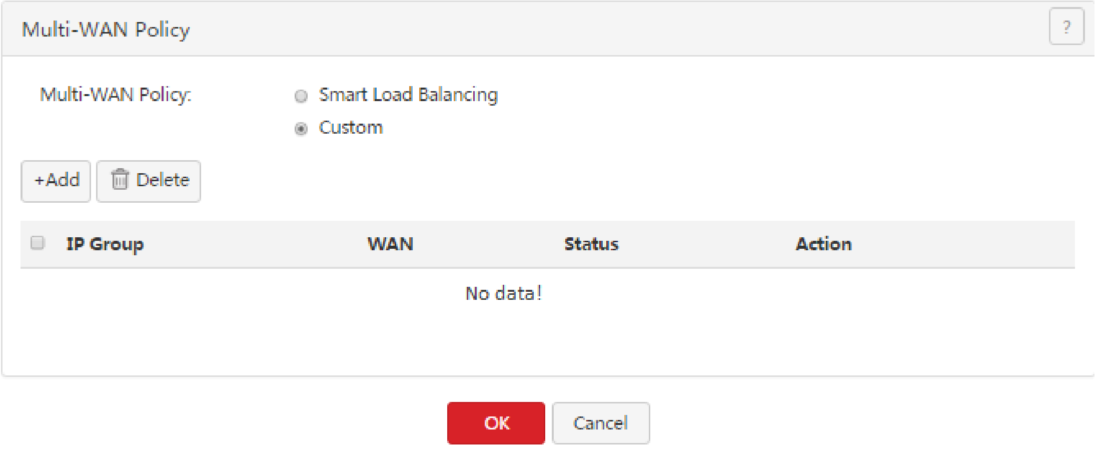
II. Customize a multi-WAN policy.

1. Enable multi-WAN policy customization.

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

(2) Select **Custom**.

(3) Click **OK**.



Multi-WAN Policy ?

Multi-WAN Policy: ○ Smart Load Balancing ● Custom

+Add 🗑 Delete

□	IP Group	WAN	Status	Action
		No data!		

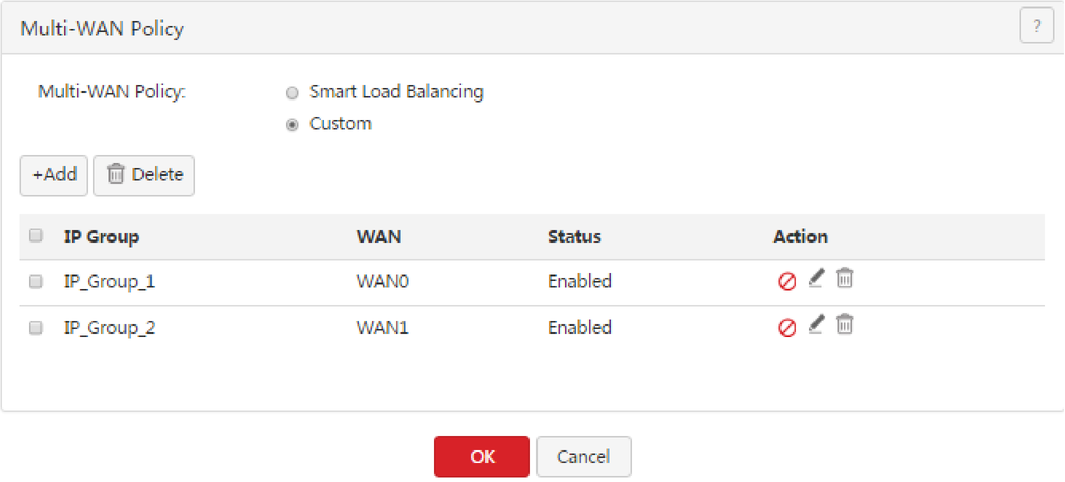
OK Cancel

2. Set multi-WAN rules.

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

(2) Click +Add.

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



Multi-WAN Policy ?

Multi-WAN Policy: ○ Smart Load Balancing ● Custom

+Add 🗑 Delete

□	IP Group	WAN	Status	Action
□	IP_Group_1	WAN0	Enabled	⊘ ✎ 🗑
□	IP_Group_2	WAN1	Enabled	⊘ ✎ 🗑

OK Cancel

Chapter 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 user-defined bandwidth control

6.1.1 Function introduction

M50 supports the following bandwidth control modes:

- Smart bandwidth control

In this mode, the router automatically allocate bandwidth to LAN users based on the Link Speed value that you set on the **Network** > **Internet Setup** page.

Before using smart bandwidth control, set **Link Speed** to the bandwidth of your broadband connection. Otherwise, smart bandwidth control may not be accurate.

- User-define bandwidth control

In this mode, manually set bandwidth control rules based on the actual environment. User-defined 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, user-define bandwidth control is more flexible than smart bandwidth control, while the latter is easier to use.

6.1.2 Configuration instruction

- Smart bandwidth control

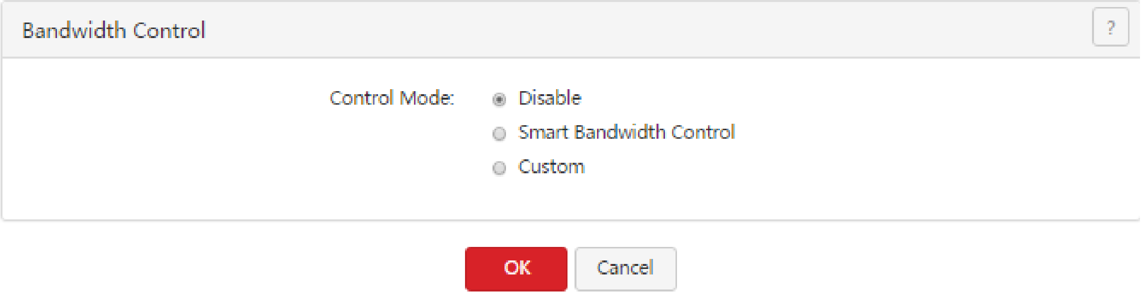
Step	Task	Description
1	Set the bandwidth of your broadband connection.	Set it on the **Network** > **Internet Setup** page. For details, see Setting up an internet connection.
2	Enable smart bandwidth control.	On the **Bandwidth Control** page, set **Control Mode** to **Smart Bandwidth Control** and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

- User-defined 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 user-defined 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 describes how to set user-defined bandwidth control.

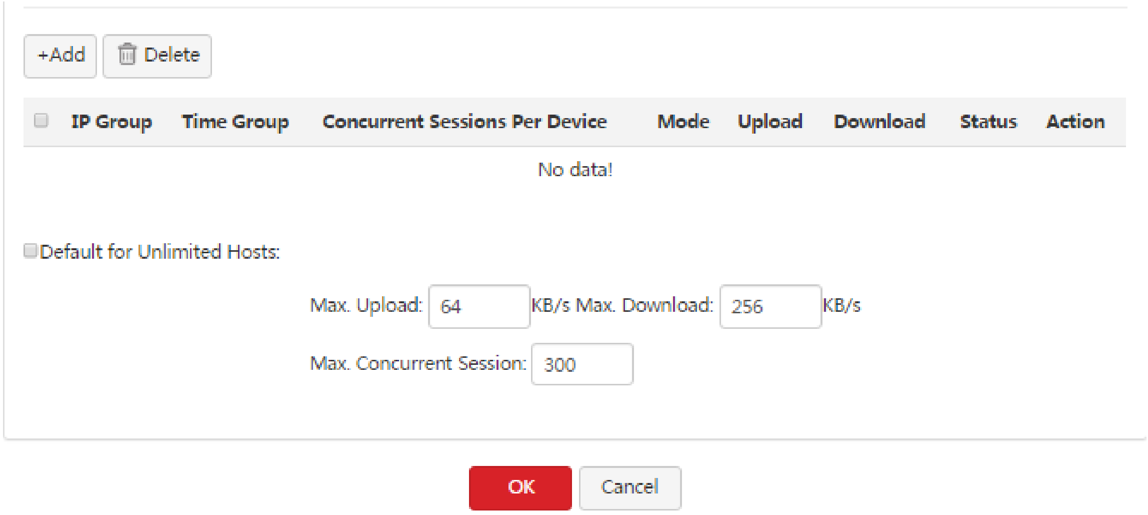


Bandwidth Control

Control Mode: ● Disable ○ Smart Bandwidth Control ○ Custom

6.2.1 Enabling user-defined bandwidth control

1. Choose **Bandwidth Control**.
2. Set **Control Mode** to **Custom**.
3. Click **OK**.
   Then, you can set user-defined bandwidth control rules.



+Add   Delete

☐	IP Group	Time Group	Concurrent Sessions Per Device	Mode	Upload	Download	Status	Action
No data!								

☐Default for Unlimited Hosts:

Max. Upload: 64 KB/s Max. Download: 256 KB/s

Max. Concurrent Session: 300

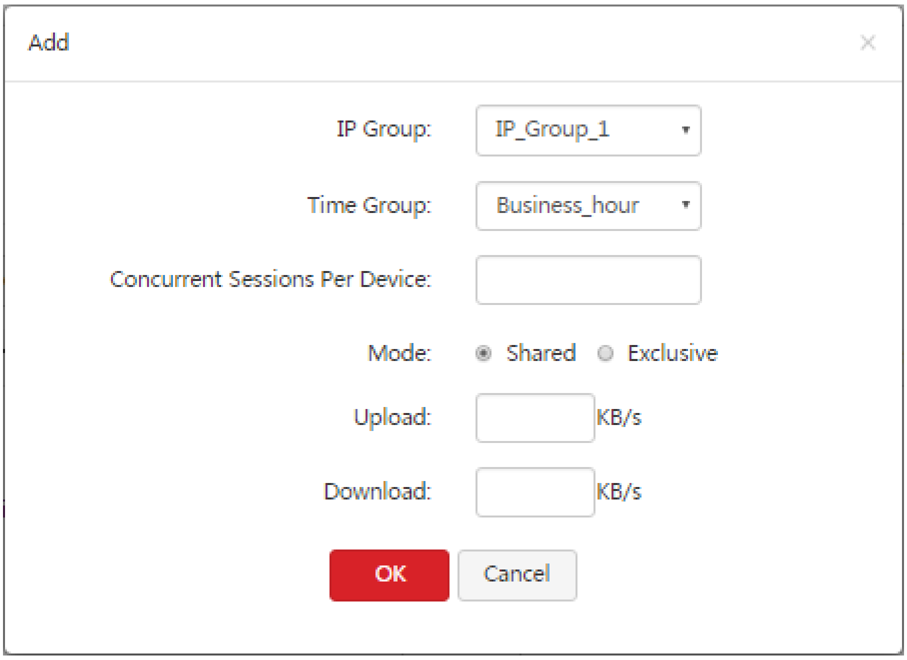
OK   Cancel

6.2.2 Setting user-defined bandwidth control rules

- Adding a rule

1. Choose **Bandwidth Control**.
2. Click +Add.

The **Add** dialog box appears.



Add

IP Group: IP_Group_1

Time Group: Business_hour

Concurrent Sessions Per Device:

Mode: ● Shared ○ Exclusive

Upload: KB/s

Download: KB/s

OK   Cancel

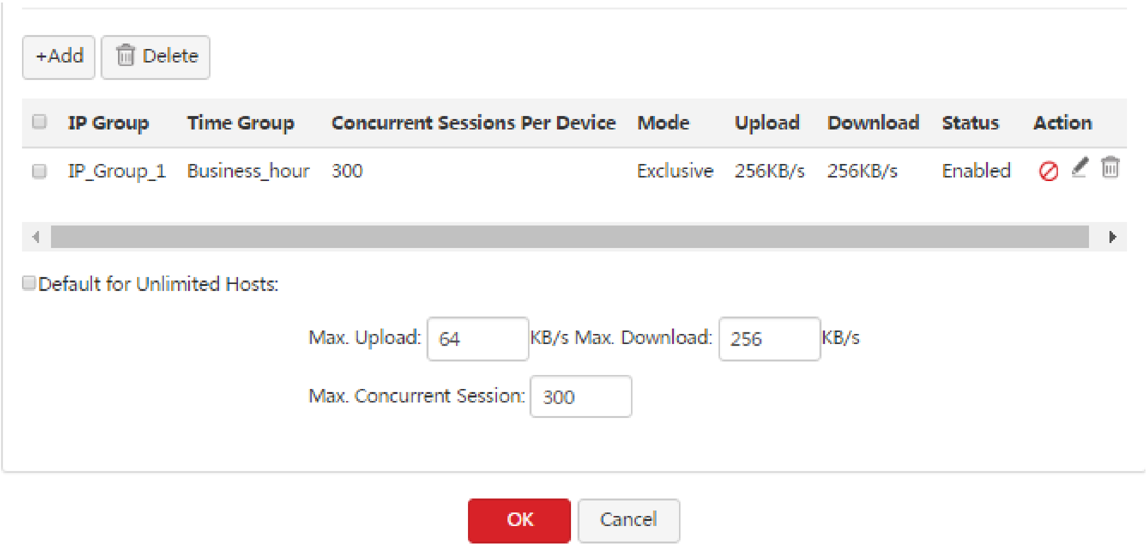
The following table describes the parameters.

Parameter	Description
IP Group	It specifies a referenced IP group that indicates the users to which a rule is applicable.

Parameter	Description
	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	

3. Set the parameters and click **OK**.

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



□	IP Group	Time Group	Concurrent Sessions Per Device	Mode	Upload	Download	Status	Action
□	IP_Group_1	Business_hour	300	Exclusive	256KB/s	256KB/s	Enabled	⊘ ✎ 🗑

□Default for Unlimited Hosts:

Max. Upload: 64 KB/s Max. Download: 256 KB/s

Max. Concurrent Session: 300

- Modifying a rule

1. Choose **Bandwidth Control**.
2. Click ✎ corresponding to a bandwidth control rule.
3. Modify the rule.
4. To disable a rule, click ⊘ corresponding to the rule.

5. To enable a rule, click ✓ corresponding to the rule.

- Deleting a rule

1. Choose **Bandwidth Control**.
2. Click 🗑 corresponding to a rule to be deleted.

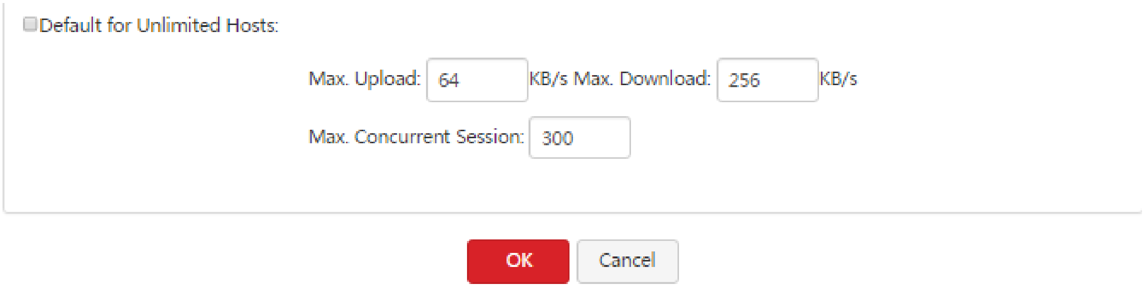
   The rule is deleted.

3. 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 user-defined 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 **Defaults for unlimited host**, the bandwidth and maximum number of concurrent sessions are not limited.



□Default for Unlimited Hosts:

Max. Upload: 64 KB/s Max. Download: 256 KB/s

Max. Concurrent Session: 300

Set the parameters and click **OK**.

6.3 Example of setting user-defined bandwidth control

Networking requirement

An enterprise uses M50 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, while the bandwidth allocated to the computers with an IP address ranging from 192.168.0.101 to 192.168.0.254 is not limited.

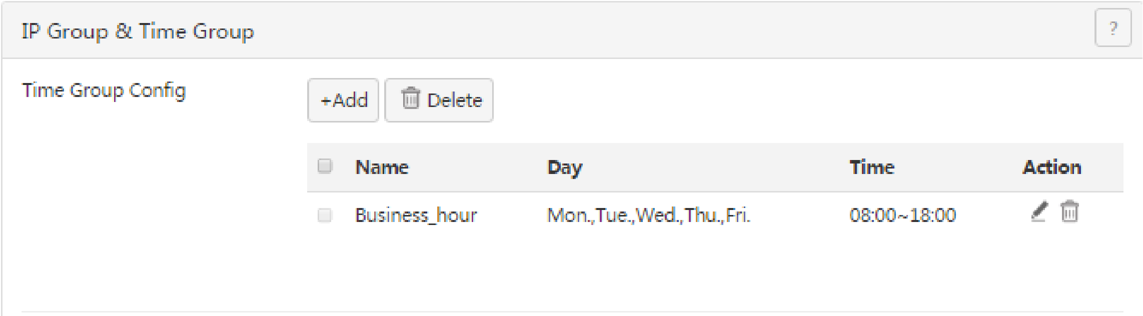
You can use the user-defined bandwidth control function of the router to meet this requirement. Assume that the maximum number of sessions for user device is 300.

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.



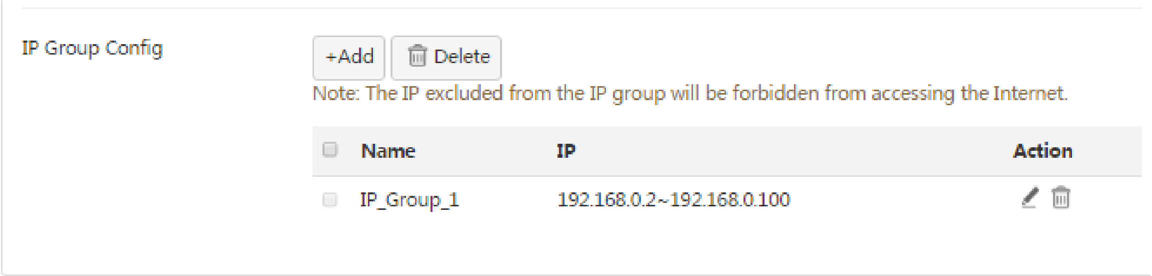
Time Group Config

□	Name	Day	Time	Action
□	Business_hour	Mon.,Tue.,Wed.,Thu.,Fri.	08:00~18:00	✎ 🗑

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.

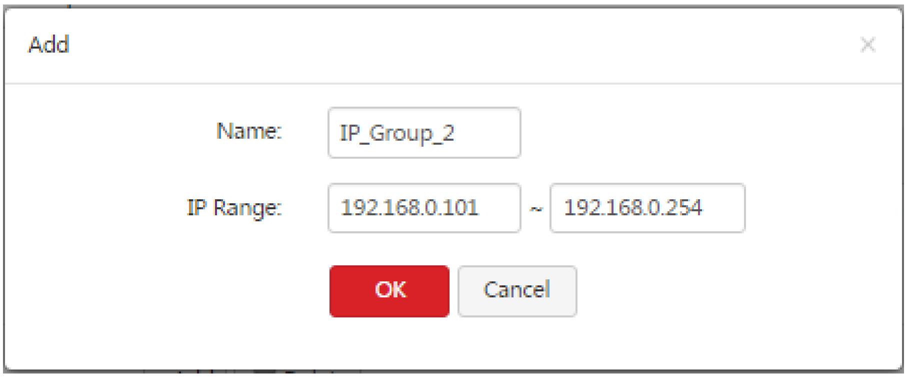


IP Group Config

Note: The IP excluded from the IP group will be forbidden from accessing the Internet.

□	Name	IP	Action
□	IP_Group_1	192.168.0.2~192.168.0.100	✎ 🗑

To allow the other computers with IP addresses ranging from 192.168.0.101 to 192.168.0.254 to access the internet, add another IP address group to include these IP addresses. See the following figure.



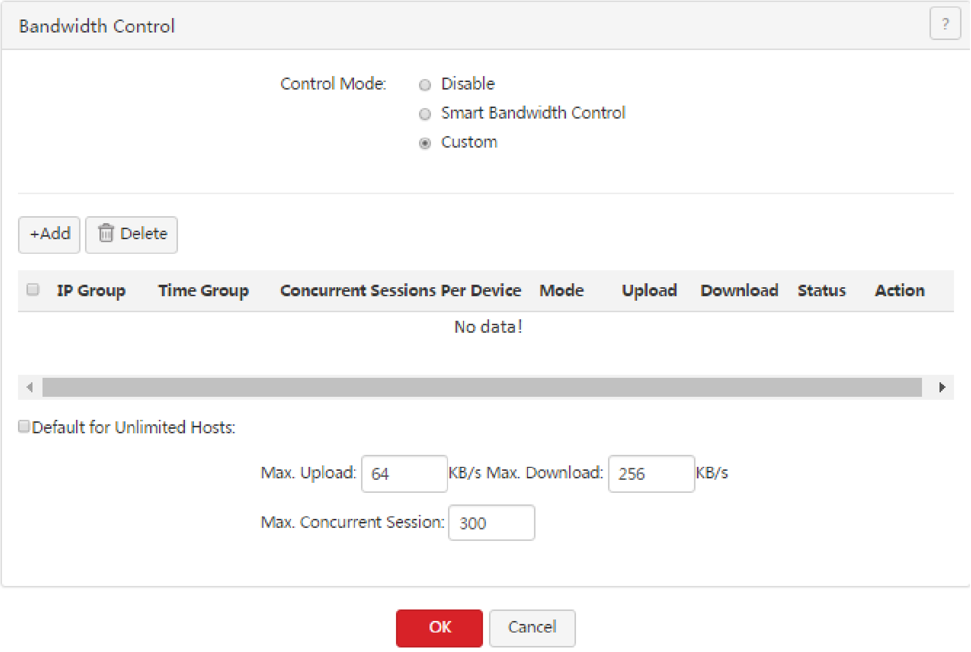
Name: IP_Group_2

IP Range: 192.168.0.101 ~ 192.168.0.254

III. Enabling user-defined bandwidth control.

1. On the **Bandwidth Control** page, select **Custom**.

2. Click **OK**.



Bandwidth Control

Control Mode: ○ Disable ○ Smart Bandwidth Control ● Custom

+Add | Delete

□	IP Group	Time Group	Concurrent Sessions Per Device	Mode	Upload	Download	Status	Action

No data!

□ Default for Unlimited Hosts:

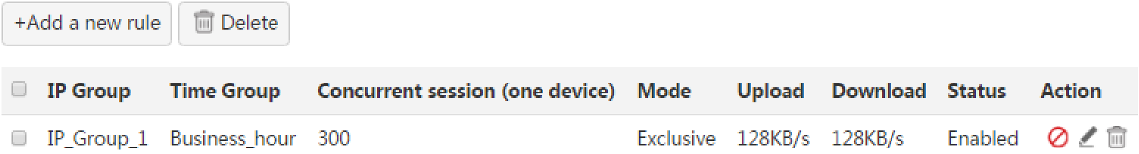
Max. Upload: 64 KB/s Max. Download: 256 KB/s

Max. Concurrent Session: 300

IV. Set a user-defined bandwidth control rule.

1. On the **Bandwidth Control** page, click +Add.

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



+Add a new rule | Delete

□	IP Group	Time Group	Concurrent session (one device)	Mode	Upload	Download	Status	Action
□	IP_Group_1	Business_hour	300	Exclusive	128KB/s	128KB/s	Enabled	⊘ ✎ 🗑

Chapter 7 VPN

7.1 Overview

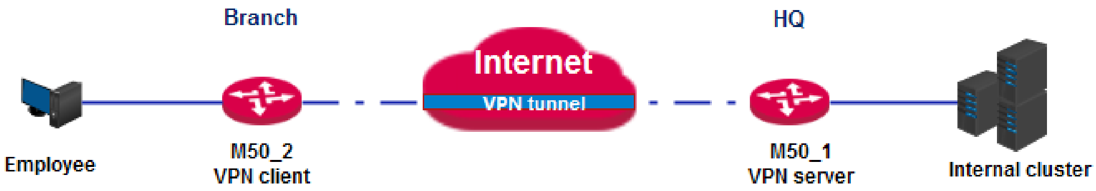
A Virtual Private Network (VPN) is a dedicated network set up on a public network (usually the internet). A VPN is a logically network without physical connections. Using the VPN technology, you can enable your branch employees to remotely share resources and access your HQ LAN, and meanwhile ensure 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 Network topology

The following figure shows the typical VPN network topology.



7.1.2 VPN types

M50 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.

M50 can functions 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.

7.1.3 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:

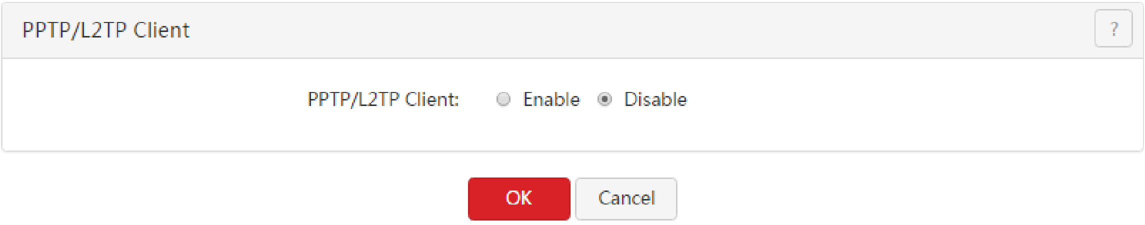
- A triplet {SPI, Destination IP address, Security protocol identifier} is used as a unique ID.
- An SA specifies the protocol, algorithm, and key for processing packets.
- Each IPsec SA is unidirectional with a life cycle.
- An SA can be created manually or generated automatically using internet Key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

7.2 Configuring a VPN

7.2.1 Configuring M50 as a PPTP/L2TP client

M50 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.

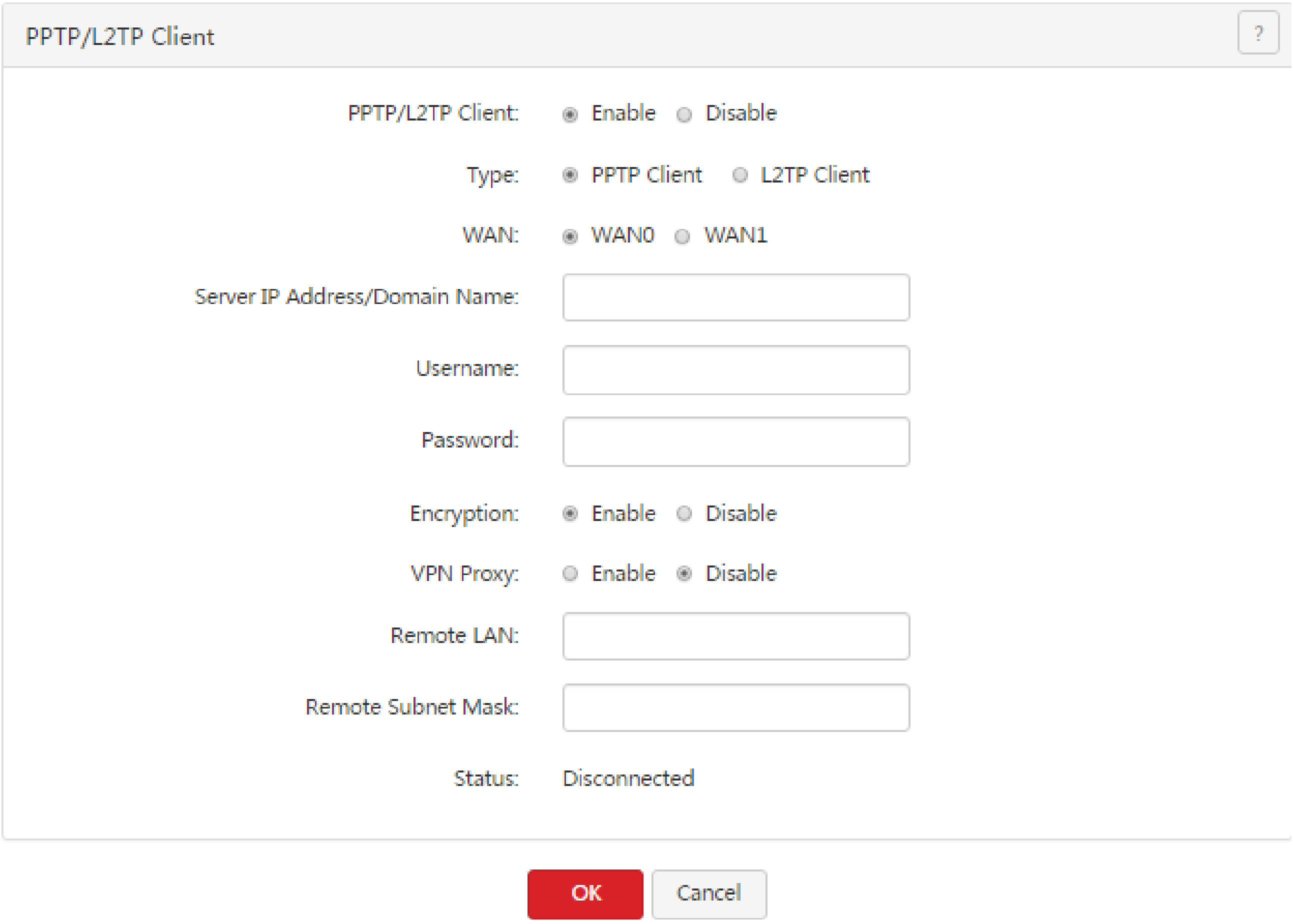
To access the page for configuring M50 as a PPTP/L2TP client, choose **VPN** > **PPTP/L2TP Client**. See the following figure.



PPTP/L2TP Client

PPTP/L2TP Client: ○ Enable ● Disable

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



PPTP/L2TP Client

PPTP/L2TP Client: ● Enable ○ Disable

Type: ● PPTP Client ○ L2TP Client

WAN: ● WAN0 ○ WAN1

Server IP Address/Domain Name:

Username:

Password:

Encryption: ● Enable ○ Disable

VPN Proxy: ○ Enable ● Disable

Remote LAN:

Remote Subnet Mask:

Status: Disconnected

The following table describes the parameters.

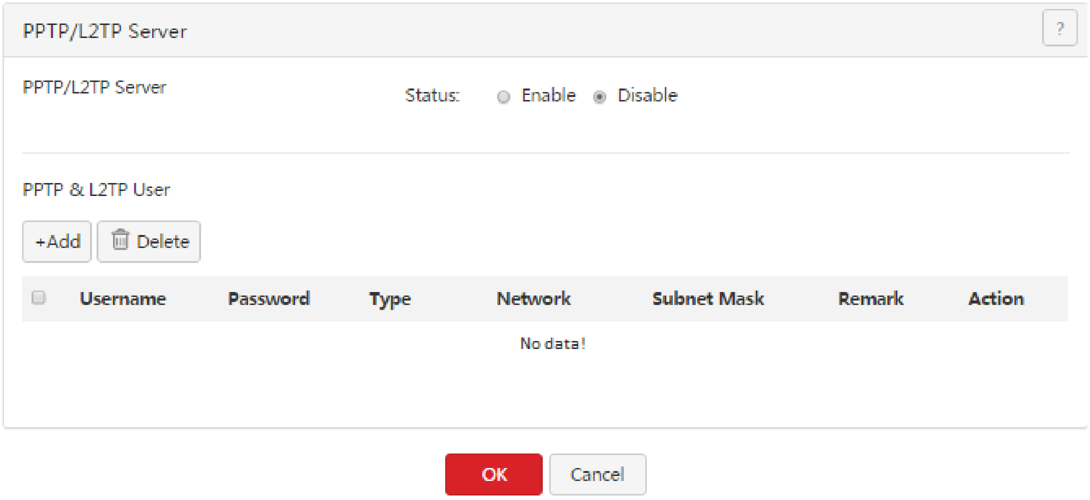
Parameter	Description
PPTP/L2TP Client	It specifies whether the PPTP/L2TP client function is enabled. If this parameter is set to **Enabled**, M50 functions as a PPTP/L2TP VPN client.
Type	It specifies the client type of the router. The router supports the following types: ● **PPTP Client**: Select this option if the VPN server to be connected is a PPTP server. ● **L2TP Client**: 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 M50 as a PPTP/L2TP server

M50 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 M50 as a PPTP/L2TP server, choose **VPN** > **PPTP/L2TP Server**. See the following figure.



PPTP/L2TP Server

PPTP/L2TP Server Status: ○ Enable ● Disable

PPTP & L2TP User

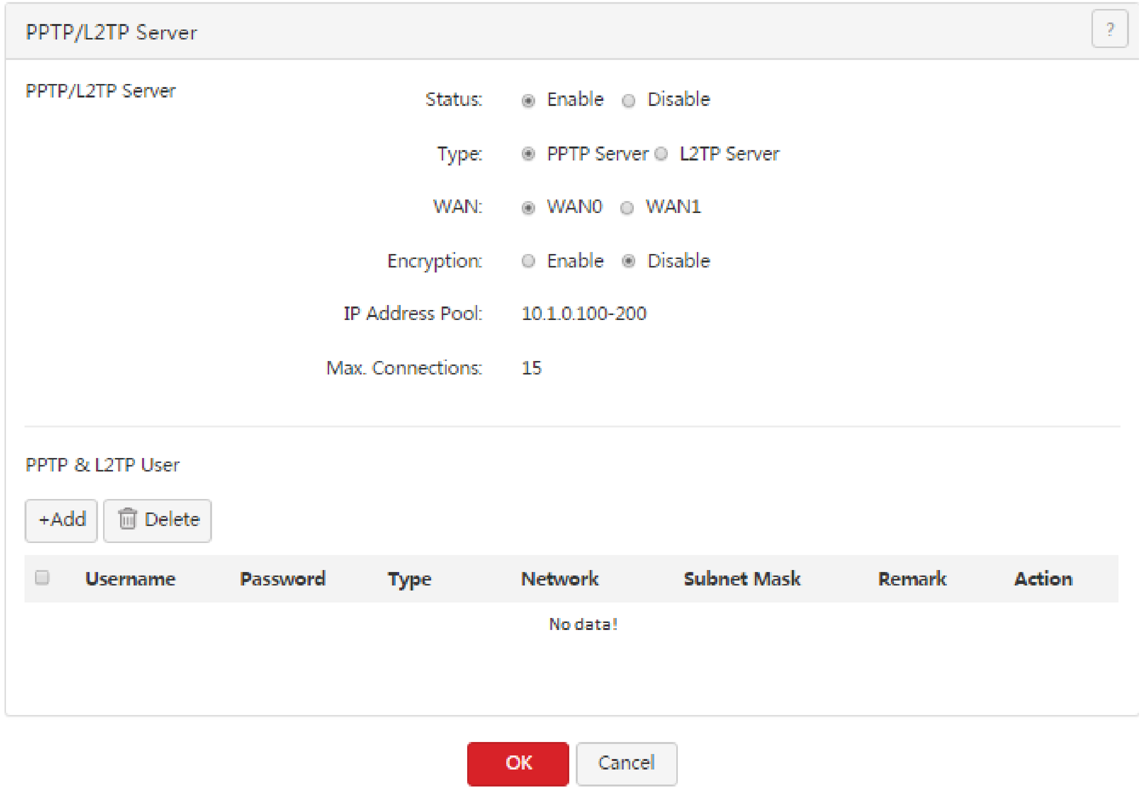
□	Username	Password	Type	Network	Subnet Mask	Remark	Action

No data!

To configure M50 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 and click **OK**.



PPTP/L2TP Server

PPTP/L2TP Server

Status: ● Enable ○ Disable

Type: ● PPTP Server ○ L2TP Server

WAN: ● WAN0 ○ WAN1

Encryption: ○ Enable ● Disable

IP Address Pool: 10.1.0.100-200

Max. Connections: 15

PPTP & L2TP User

□	Username	Password	Type	Network	Subnet Mask	Remark	Action

No data!

The following table describes the parameters.

Parameter	Description
Status	It specifies whether to enable the PPTP/L2TP server function. If this parameter is set to **Enabled**, M50 functions as a PPTP/L2TP server.
Type	It specifies the server type of the router. The router supports the following types: ● **PPTP Server**: If this option is selected, the server is accessible only to PPTP clients. ● **L2TP Server**: 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. 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 15.

Configuring a PPTP/L2TP account

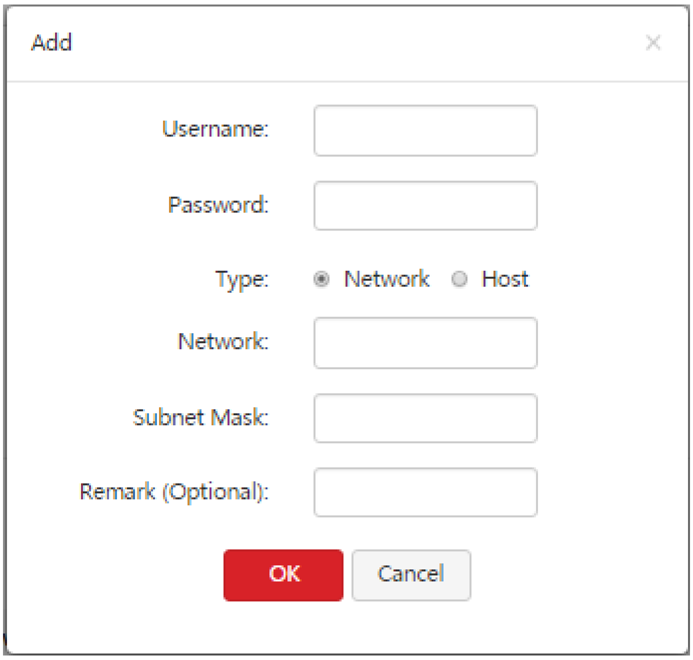
A PPTP/L2TP account is required when a VPN user accesses M50 that functions as a PPTP/L2TP server.

- Adding a user

1. Choose **VPN** > **PPTP/L2TP Server**.

2. Click +Add.

   The **Add** dialog box appears.



Add

Username:

Password:

Type: ● Network ○ Host

Network:

Subnet Mask:

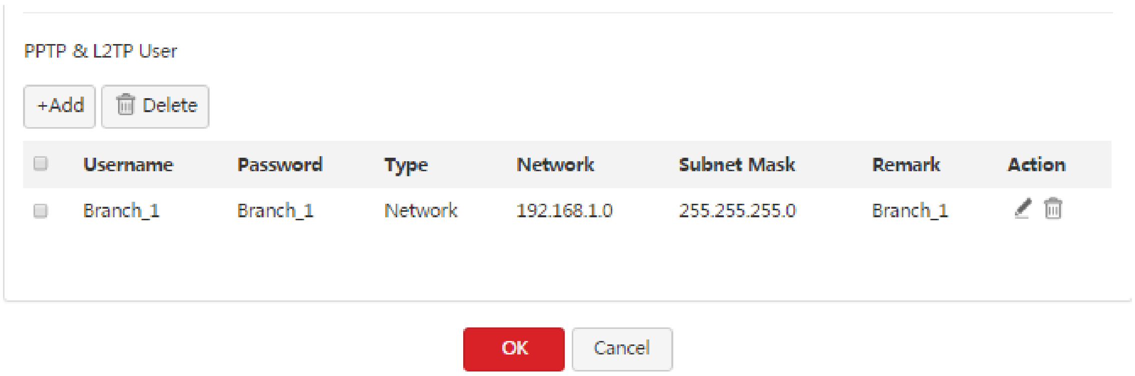
Remark (Optional):

The following table describes the parameters.

Parameter	Description
Username	**Username** specifies the user name used to set up a PPTP/L2TP VPN connection. **Password** specifies the password for the user name.
Password	
Type	● **Network**: It indicates that a VPN client is a network. If this option is selected, set the **Network** and **Subnet Mask** parameters as well. ● **Host**: It indicates that a VPN client is a computer.
Network	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 (Optional)	It specifies the description of a user. This parameter is optional.

3. Set the parameters and click **OK**.

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



PPTP & L2TP User

□	Username	Password	Type	Network	Subnet Mask	Remark	Action
□	Branch_1	Branch_1	Network	192.168.1.0	255.255.255.0	Branch_1	✎ 🗑

- Modifying a user

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

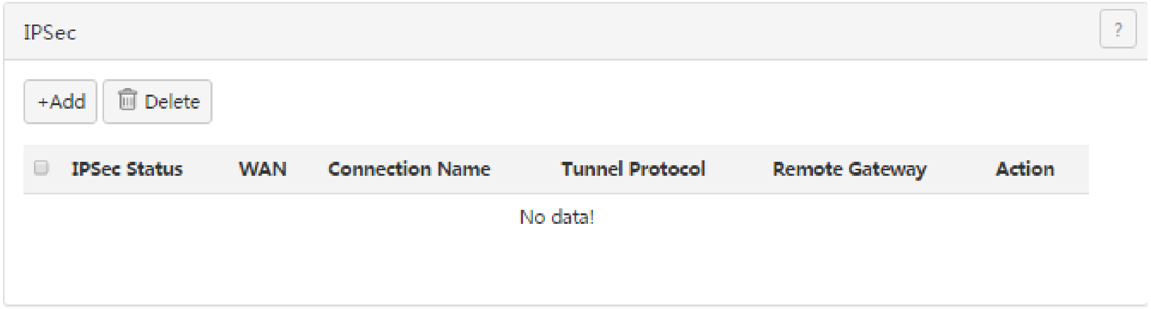
- Deleting a user

1. Choose **VPN** > **PPTP/L2TP Server**.
2. Click 🗑 corresponding to a user to be deleted.

   The user is deleted.
3. 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.



IPSec

□	IPSec Status	WAN	Connection Name	Tunnel Protocol	Remote Gateway	Action

No data!

The following table describes the parameters.

Parameter	Description
IPSec	It specifies whether to enable the IPSec function.
WAN	It specifies the local WAN port assigned to the IPSec function. The IP address of the WAN port must be set as the value of **Remote Gateway** of the IPSec peer.
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. M50 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	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	It specifies the key negotiation mode for an IPSec tunnel. The options include: ● **Auto**: 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. ● **Custom**: 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

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:

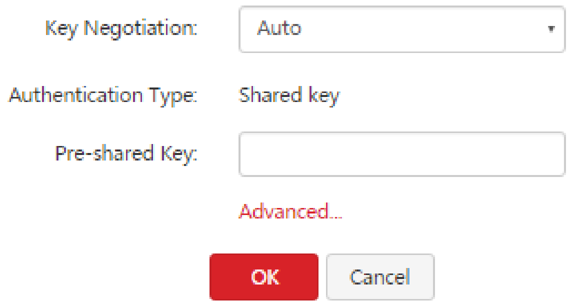
- ISAKMP: Short for internet Security Association and Key Management Protocol, ISAKMP provides a framework for key exchange and SA negotiation.
- Oakley: It describes a key exchange mechanism.
- SKEME: It describes a key exchange mechanism other than that described by the Oakley protocol.

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**.



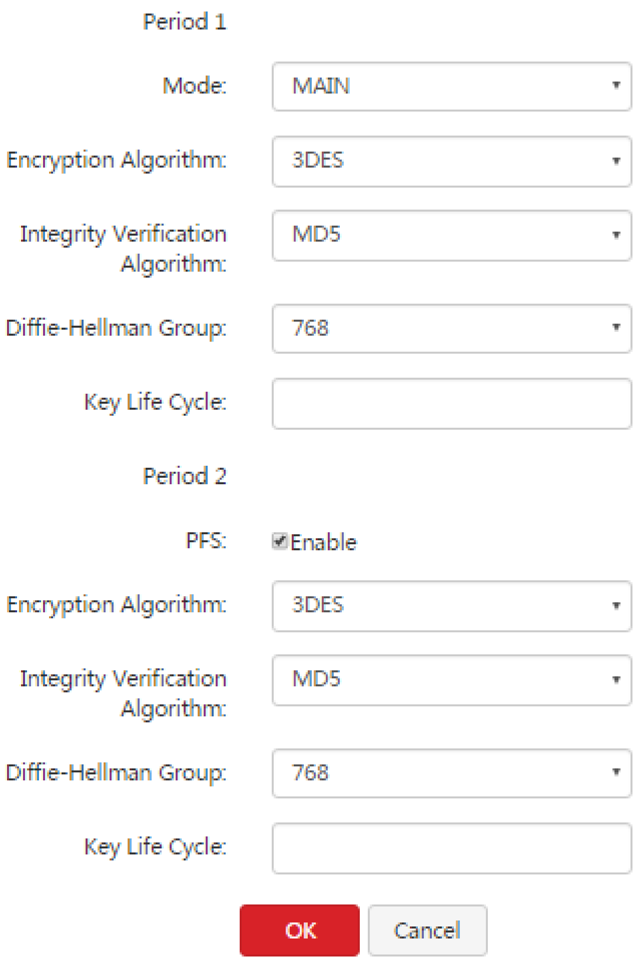
Key Negotiation: Auto

Authentication Type: Shared key

Pre-shared Key:

The following table describes the parameters.

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.



Period 1

Mode: MAIN

Encryption Algorithm: 3DES

Integrity Verification Algorithm: MD5

Diffie-Hellman Group: 768

Key Life Cycle:

Period 2

PFS: ☑Enable

Encryption Algorithm: 3DES

Integrity Verification Algorithm: MD5

Diffie-Hellman Group: 768

Key Life Cycle:

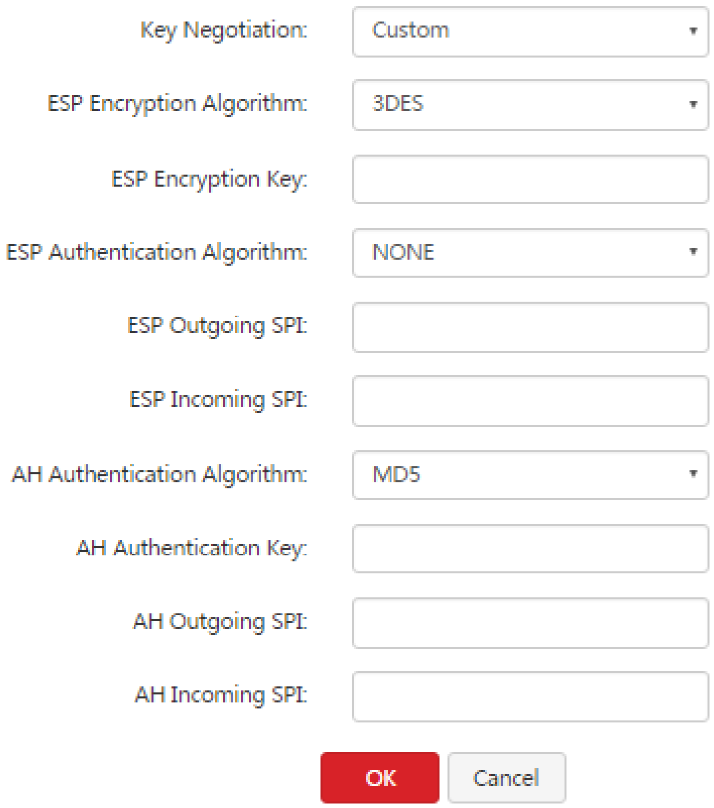
The following table describes the parameters.

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. M50 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	It specifies an IKE session verification algorithm. M50 supports the following

Parameter	Description
Algorithm	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 Life Cycle	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 – Custom

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



Key Negotiation:	Custom
ESP Encryption Algorithm:	3DES
ESP Encryption Key:	
ESP Authentication Algorithm:	NONE
ESP Outgoing SPI:	
ESP Incoming SPI:	
AH Authentication Algorithm:	MD5
AH Authentication Key:	
AH Outgoing SPI:	
AH Incoming SPI:	

The following table describes the parameters.

Parameter	Description
ESP Encryption Algorithm	It specifies the ESP encryption algorithm required in case that **Tunnel Protocol** is set to **ESP**. M50 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**. M50 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.
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.

7.3 Example of configuring a VPN

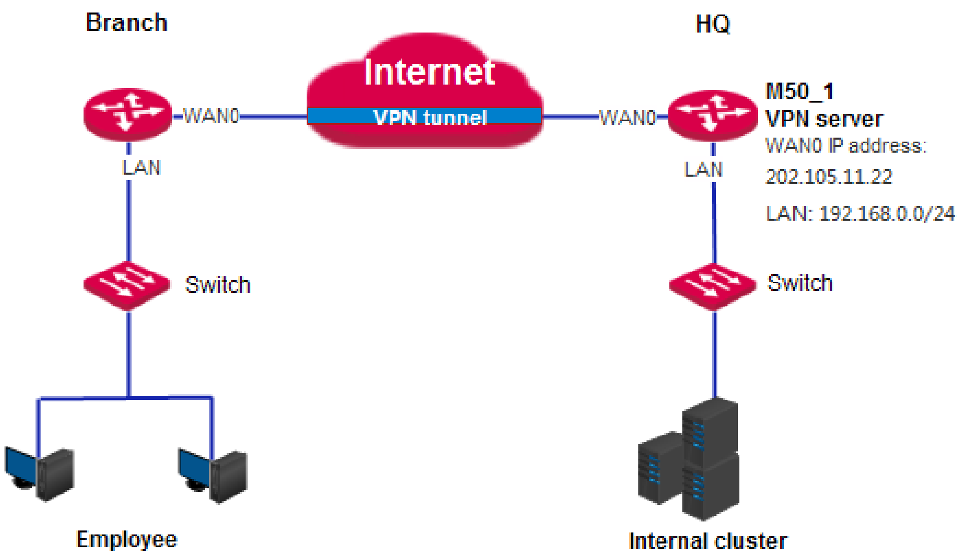
7.3.1 Example of configuring a PPTP/L2TP VPN

Networking requirement

An enterprise has used M50 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 a PPTP/L2TP VPN using the router to meet this requirement. This example describes the method to set up a PPTP VPN. You can set up an L2TP VPN using the same method.

Network topology



Configuration procedure

Configure M50_1 as a VPN server and M50_2 as a VPN client as follows:

I. Configure M50_1.

1. Enable the PPTP server function.

(1) On M50_1, choose **VPN** > **PPTP/L2TP Server**.

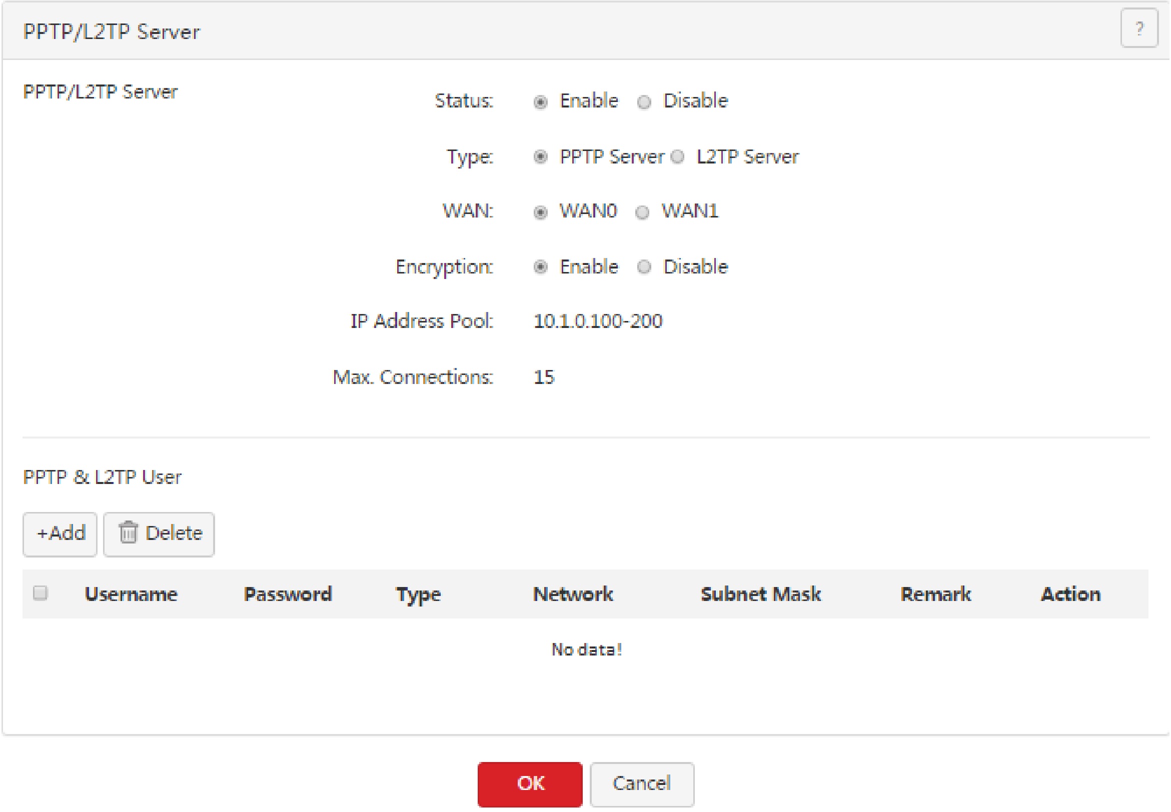
(2) Set **Status** to **Enable**.

(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**.



PPTP/L2TP Server

PPTP/L2TP Server

Status: ● Enable ○ Disable

Type: ● PPTP Server ○ L2TP Server

WAN: ● WAN0 ○ WAN1

Encryption: ● Enable ○ Disable

IP Address Pool: 10.1.0.100-200

Max. Connections: 15

PPTP & L2TP User

□	Username	Password	Type	Network	Subnet Mask	Remark	Action
				No data!			

2. Configure a PPTP/L2TP user.

(1) On M50_1, choose **VPN** > **PPTP/L2TP Server**.

(2) 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.

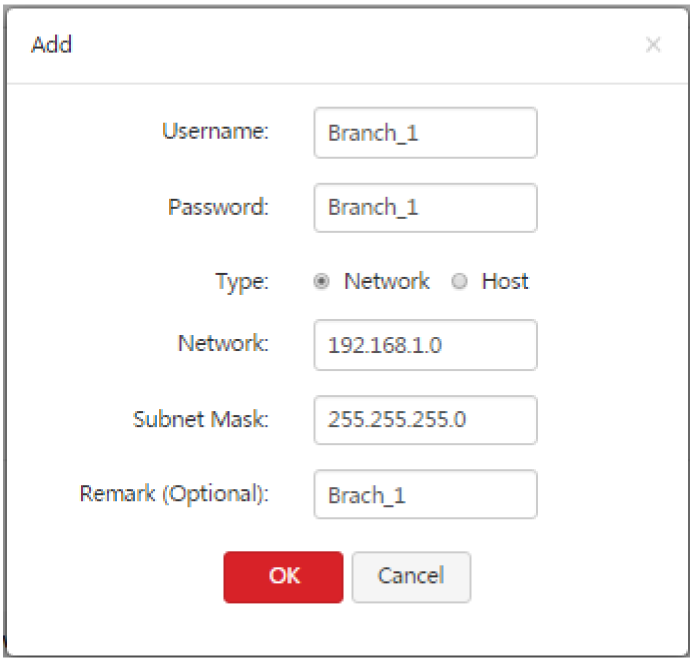
(4) Set **Password** to the password for the user name, which is **Branch_1** in this example.

(5) Set **Type** to **Network**.

(6) Set **Network** 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 (Optional)** to the description of the user, which is **Branch_1** in this example.


Add

Username: Branch_1

Password: Branch_1

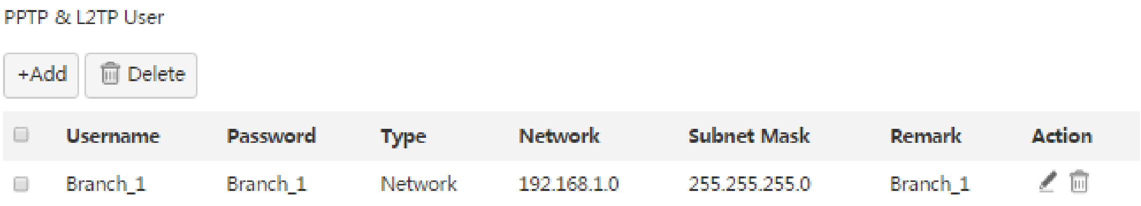
Type: ● Network ○ Host

Network: 192.168.1.0

Subnet Mask: 255.255.255.0

Remark (Optional): Brach_1

(9) Click **OK**.


PPTP & L2TP User

□	Username	Password	Type	Network	Subnet Mask	Remark	Action
□	Branch_1	Branch_1	Network	192.168.1.0	255.255.255.0	Branch_1	✎ 🗑

II. Configure M50_2.

(1) On M50_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.

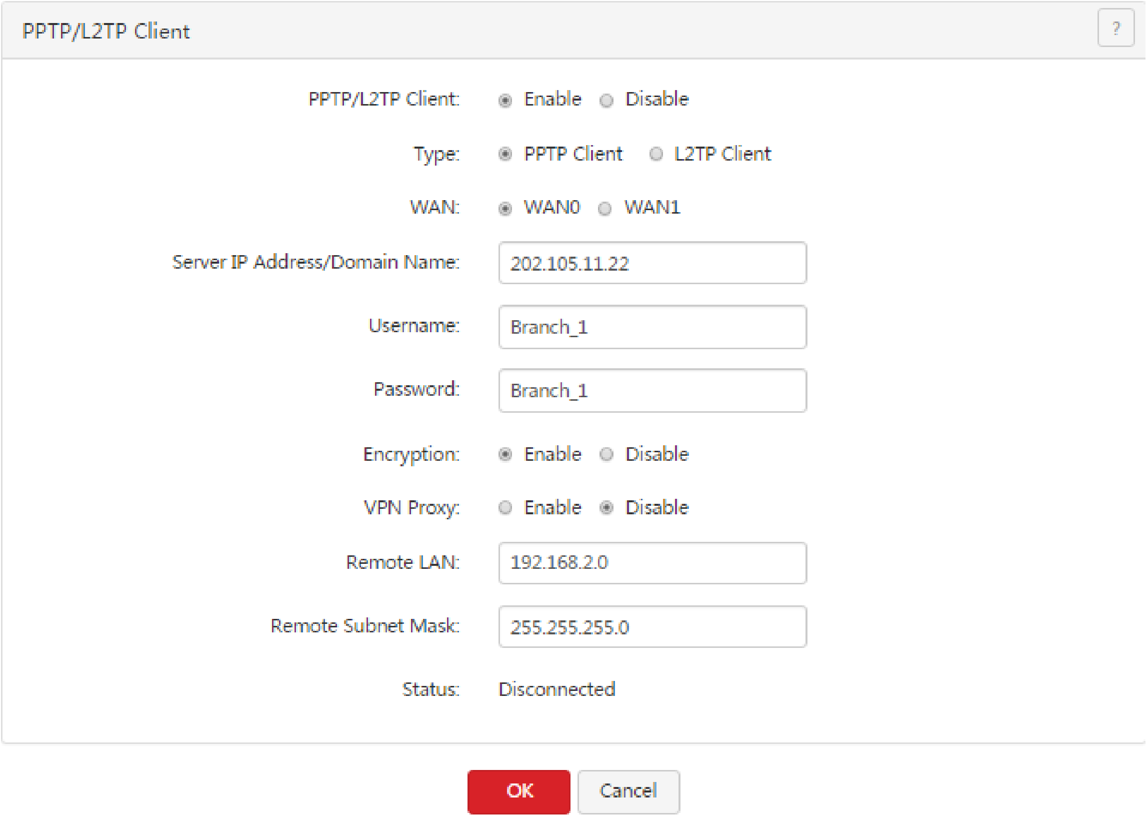
(7) Set **Encryption** to **Enable**. This setting must be the same as that on the VPN server.

(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**.



PPTP/L2TP Client

PPTP/L2TP Client: ● Enable ○ Disable

Type: ● PPTP Client ○ L2TP Client

WAN: ● WAN0 ○ WAN1

Server IP Address/Domain Name: 202.105.11.22

Username: Branch_1

Password: Branch_1

Encryption: ● Enable ○ Disable

VPN Proxy: ○ Enable ● Disable

Remote LAN: 192.168.2.0

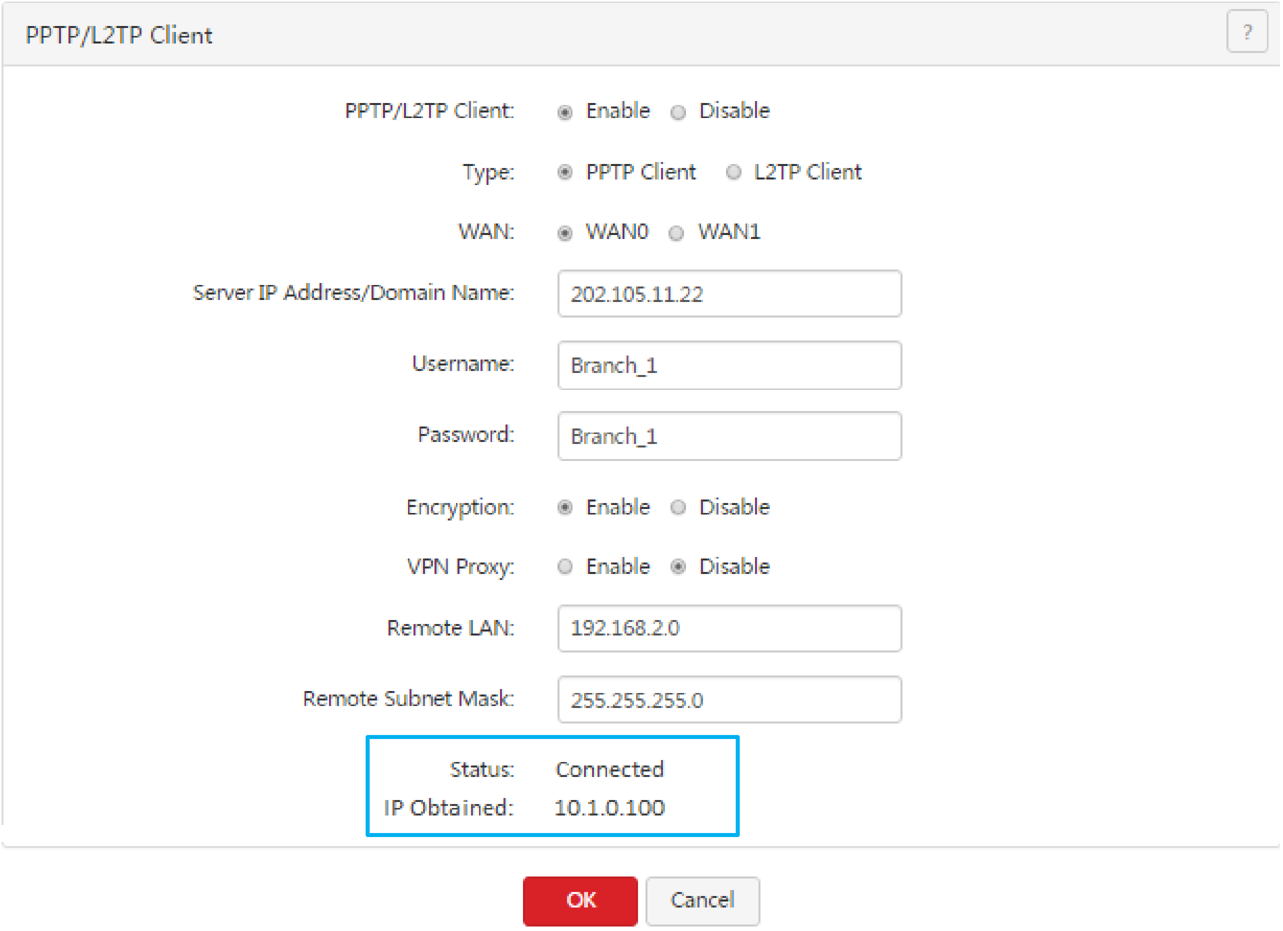
Remote Subnet Mask: 255.255.255.0

Status: Disconnected

Verification

1. On M50_2, choose **VPN** > **PPTP/L2TP Client**.

2. Verify that **Status** is **Connected** and an IP address has been obtained.
   See the following figure.



PPTP/L2TP Client

PPTP/L2TP Client: ● Enable ○ Disable

Type: ● PPTP Client ○ L2TP Client

WAN: ● WAN0 ○ WAN1

Server IP Address/Domain Name: 202.105.11.22

Username: Branch_1

Password: Branch_1

Encryption: ● Enable ○ Disable

VPN Proxy: ○ Enable ● Disable

Remote LAN: 192.168.2.0

Remote Subnet Mask: 255.255.255.0

Status: Connected

IP Obtained: 10.1.0.100

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.

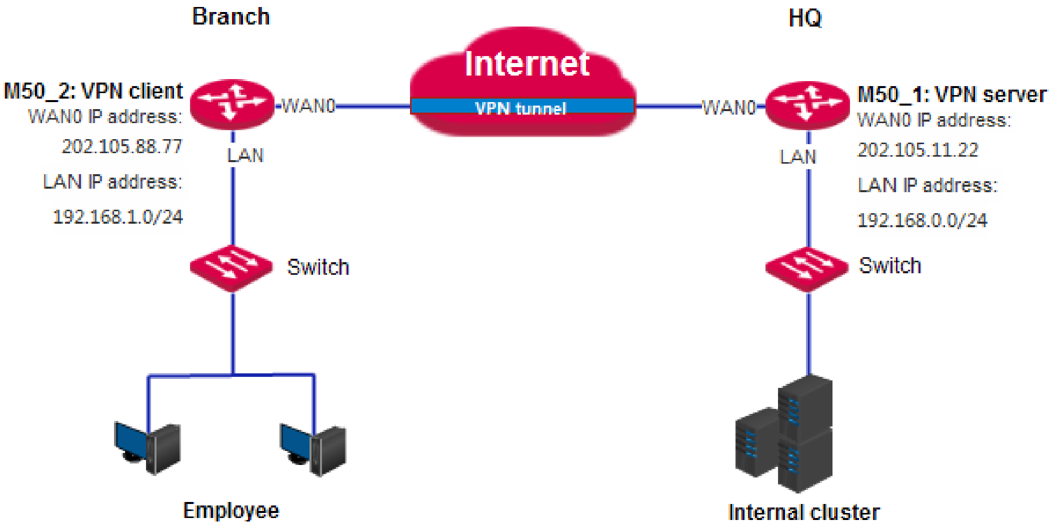
7.3.2 Example of configuring an IPSec VPN

Networking requirement

An enterprise has used M50 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 IPSec VPN using the router to meet this requirement.

Network topology



Configuration procedure

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

- Key negotiation mode: auto
- Pre-shared key: 12345678

I. Configure M50_1.

(1) On M50_1, choose **VPN** > **IPsec**.

(2) Click +Add a tunnel.

(3) Set **IPSec** to **Enable**.

(4) Set **WAN** to the WAN port bound to the IPSec tunnel, which is **WAN0** in this example.

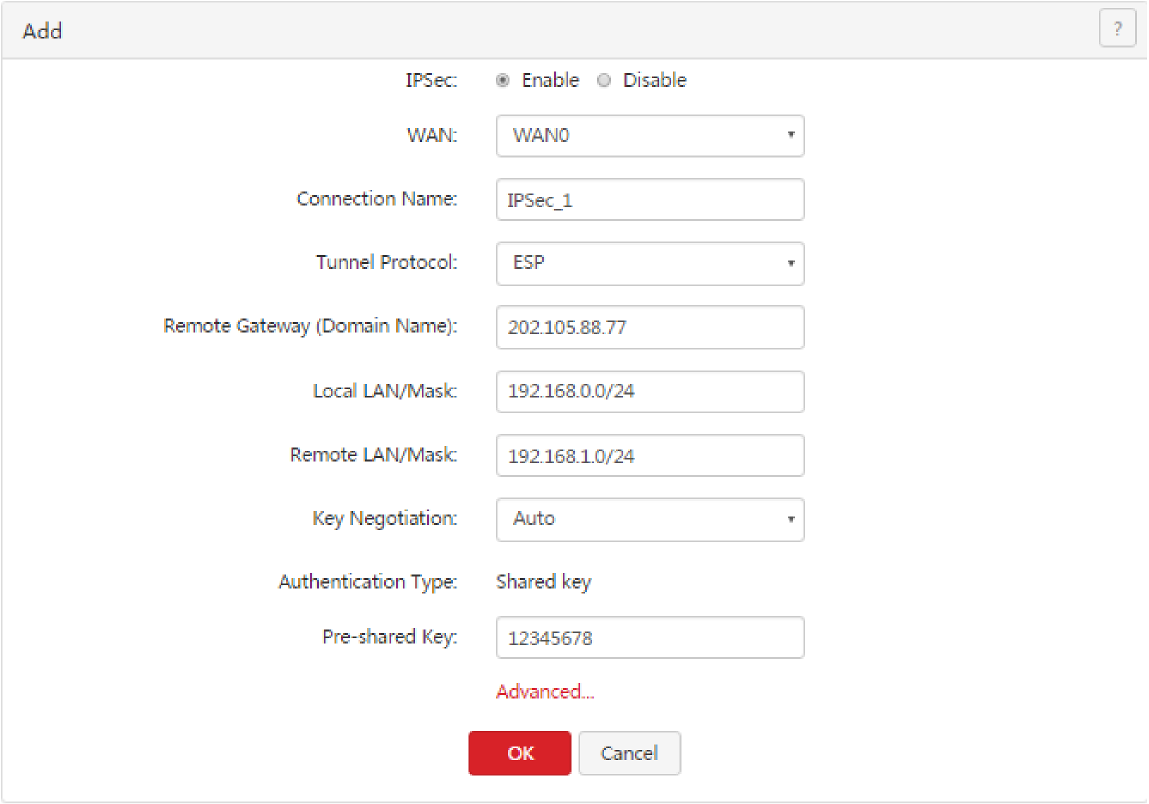
(5) Set **Connection Name** to the name of the IPSec tunnel, which is **IPSec_1** in this example.

(6) Set **Remote Gateway (Domain Name)** to the IP address of the M50_2 WAN port bound to the IPSec tunnel, which is **202.105.88.77** in this example.

(7) Set **Local LAN/Mask** to the LAN network segment and subnet mask of M50_1, which is **192.168.0.0/24** in this example.

(8) Set **Remote LAN/Mask** to the LAN network segment and subnet mask of M50_2, which is **192.168.1.0/24** in this example.

(9) Set **Pre-shared Key** to **12345678**.



Add

IPSec: ● Enable ○ Disable

WAN: WAN0

Connection Name: IPSec_1

Tunnel Protocol: ESP

Remote Gateway (Domain Name): 202.105.88.77

Local LAN/Mask: 192.168.0.0/24

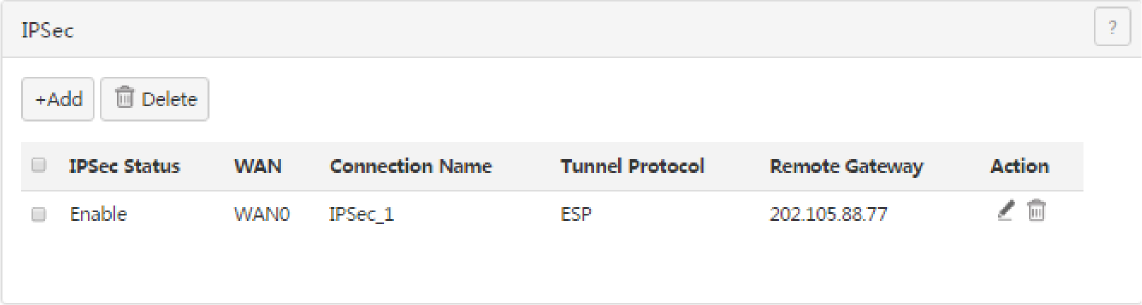
Remote LAN/Mask: 192.168.1.0/24

Key Negotiation: Auto

Authentication Type: Shared key

Pre-shared Key: 12345678

(10) Click **OK**.



IPSec

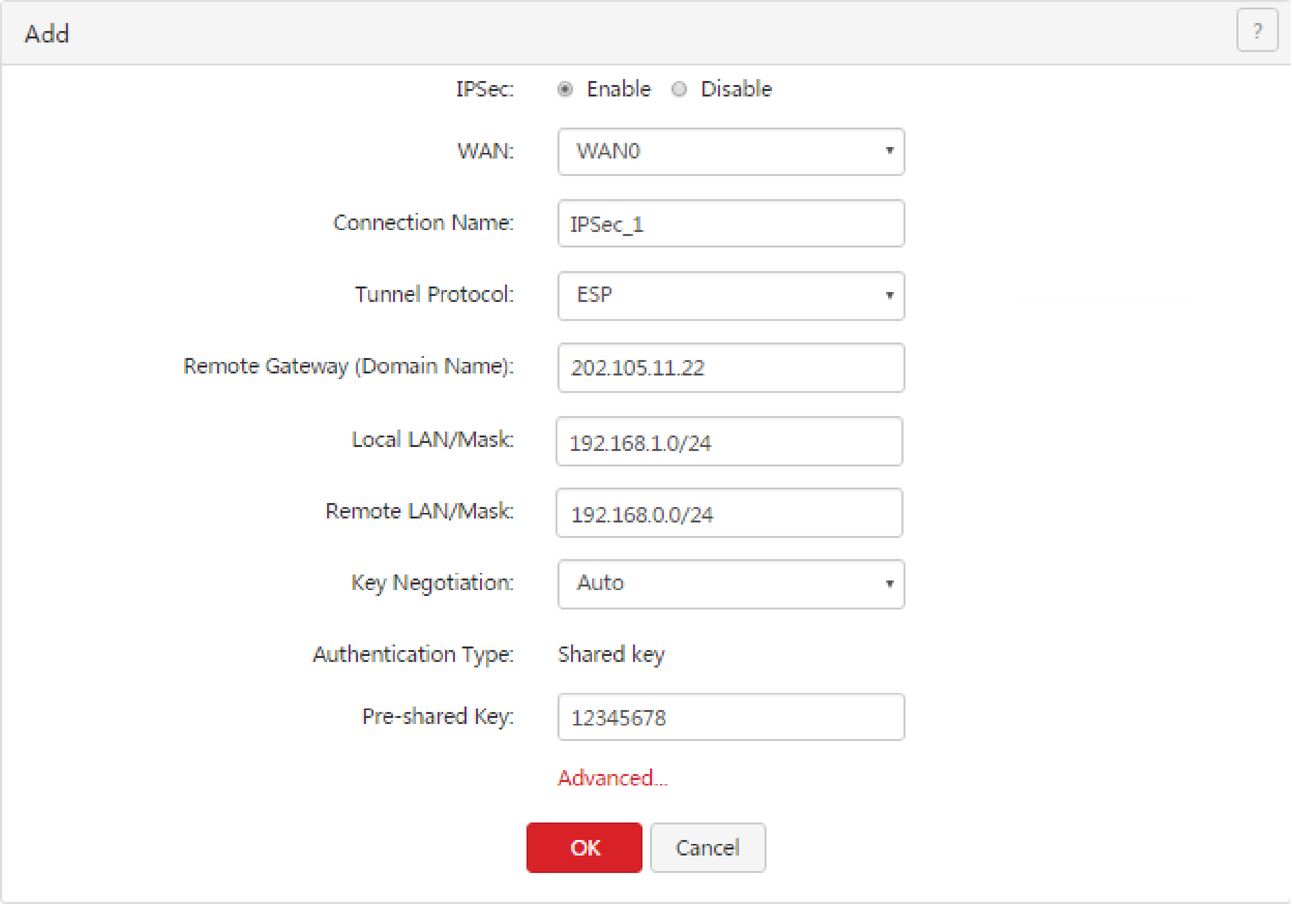
	IPSec Status	WAN	Connection Name	Tunnel Protocol	Remote Gateway	Action
□	Enable	WAN0	IPSec_1	ESP	202.105.88.77	

II. Configure M50_2.

(1) On M50_2, choose **VPN** > **IPsec**.

(2) Click +Add.

The **Add** page appears. See the following figure.



Add

IPSec: ● Enable ○ Disable

WAN: WAN0

Connection Name: IPSec_1

Tunnel Protocol: ESP

Remote Gateway (Domain Name): 202.105.11.22

Local LAN/Mask: 192.168.1.0/24

Remote LAN/Mask: 192.168.0.0/24

Key Negotiation: Auto

Authentication Type: Shared key

Pre-shared Key: 12345678

(3) Follow the M50_1 configuration procedure to set the parameters.

Verification

1. Log in to the routers, choose **System** > **Live Users**.
2. Verify that **IPSec** 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.

Note

- If advanced settings of the IPSec tunnel are required, apply the same settings to both routers.
- If Key Negotiation is set to Custom, the same encryption algorithm encryption key, and authentication algorithm must be applied to the IPSec peers. The outgoing SPI of M50_1 must be the same as the incoming SPI of M50_2, and the incoming SPI of M50_1 must be the same as the outgoing SPI of M50_2.

Chapter 8 Security

This chapter describes:

- Binding an IP address with a MAC address
- Protecting against attacks

8.1 Overview

The Security module of M50 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 Binging List can access the internet. This can effectively prevents unauthorized usage of LAN IP addresses, improving the network security.

M50 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.

Attack protection

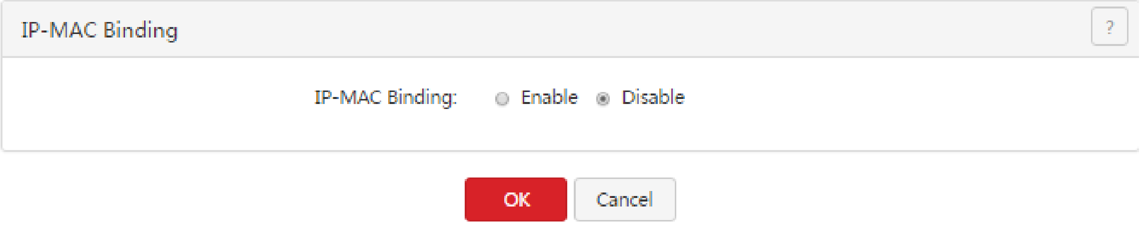
M50 can implement ARP attack defense, DDoS attack defense, IP attack defense, and WAN ping attack defense, which are described as follows:

- 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.
- WAN ping attack defense: 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.

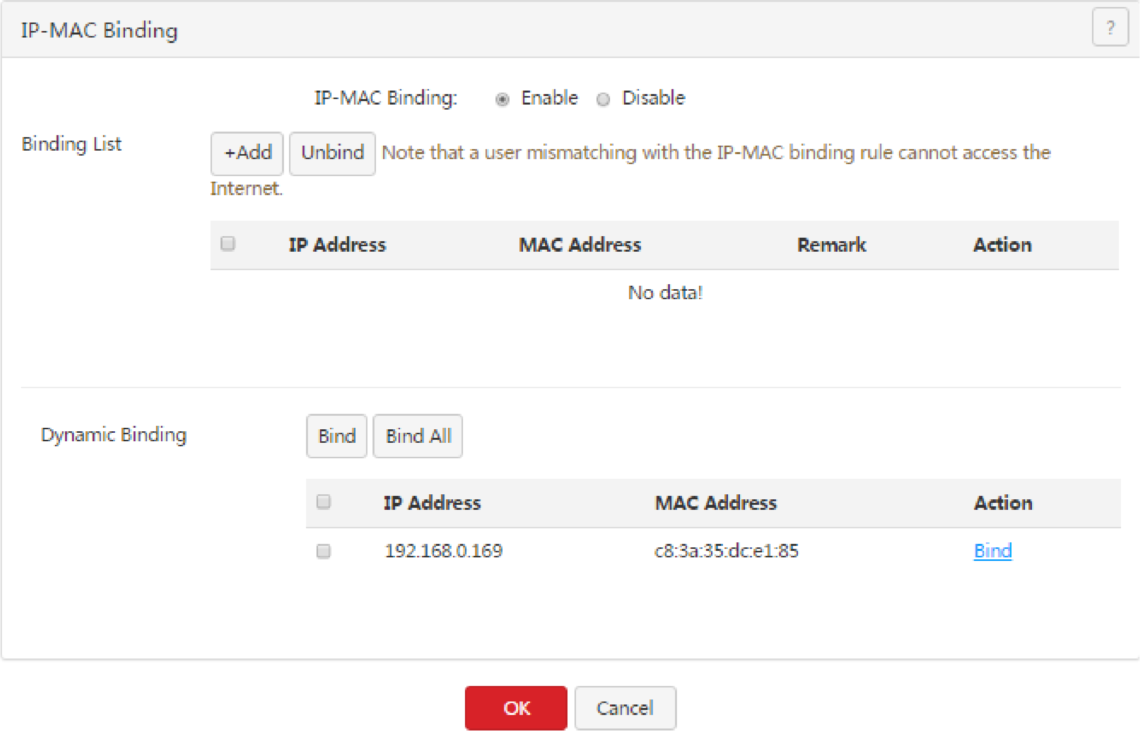


IP-MAC Binding

IP-MAC Binding: ○ Enable ● Disable

8.2.1 Enabling the IP-MAC binding function

To enable the IP-MAC binding function, set **IP-MAC Binding** to **Enable** and click **OK**. Then, you can bind IP addresses with MAC addresses.



IP-MAC Binding

IP-MAC Binding: ● Enable ○ Disable

Binding List

+Add Unbind Note that a user mismatching with the IP-MAC binding rule cannot access the Internet.

□	IP Address	MAC Address	Remark	Action
		No data!		

Dynamic Binding

Bind Bind All

□	IP Address	MAC Address	Action
□	192.168.0.169	c8:3a:35:dc:e1:85	Bind

The following table describes the parameters.

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.
	Unbind	It is used to unbind IP addresses from MAC addresses.

Parameter		Description
	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.
	Action	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	
	Action	It specifies a link that can be used on add the mapping between an IP address and a MAC address corresponding to the link to the binding list.

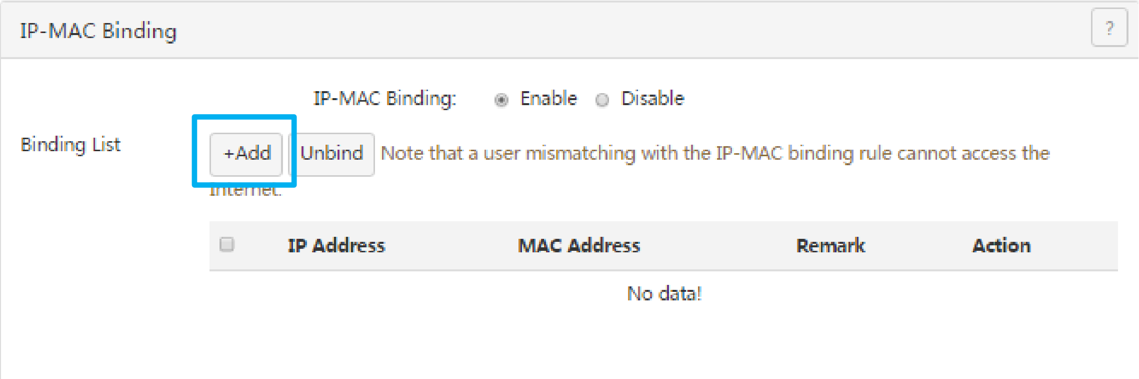
8.2.2 Configuring an IP-MAC binding entry

Manually adding an entry

1. Choose **Security** > **IP-MAC Binding**.

2. Click +Add.

3. Set the parameters.



IP-MAC Binding

IP-MAC Binding: ● Enable ○ Disable

Binding List

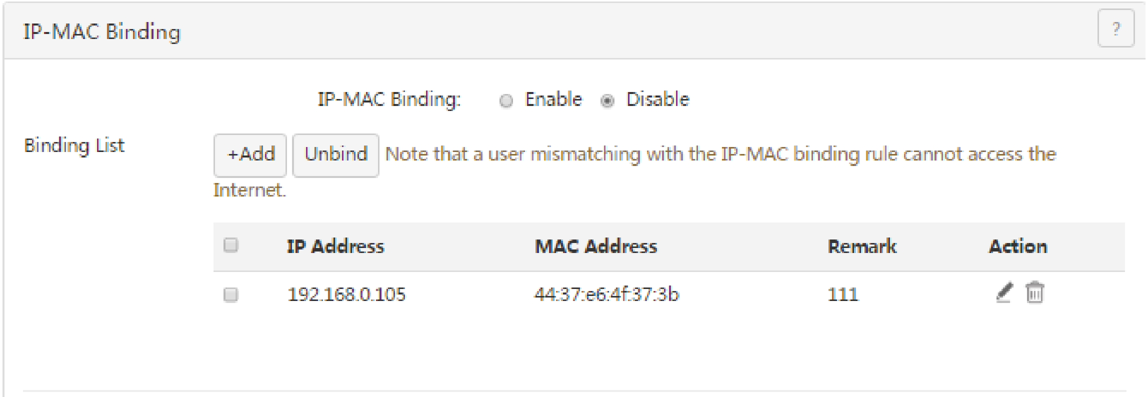
Note that a user mismatching with the IP-MAC binding rule cannot access the internet.

□	IP Address	MAC Address	Remark	Action

No data!

4. Click **OK**.

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



IP-MAC Binding

IP-MAC Binding: ○ Enable ● Disable

Binding List

+Add Unbind Note that a user mismatching with the IP-MAC binding rule cannot access the Internet.

□	IP Address	MAC Address	Remark	Action
□	192.168.0.105	44:37:e6:4f:37:3b	111	✎ 🗑

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.

   The entry is deleted.

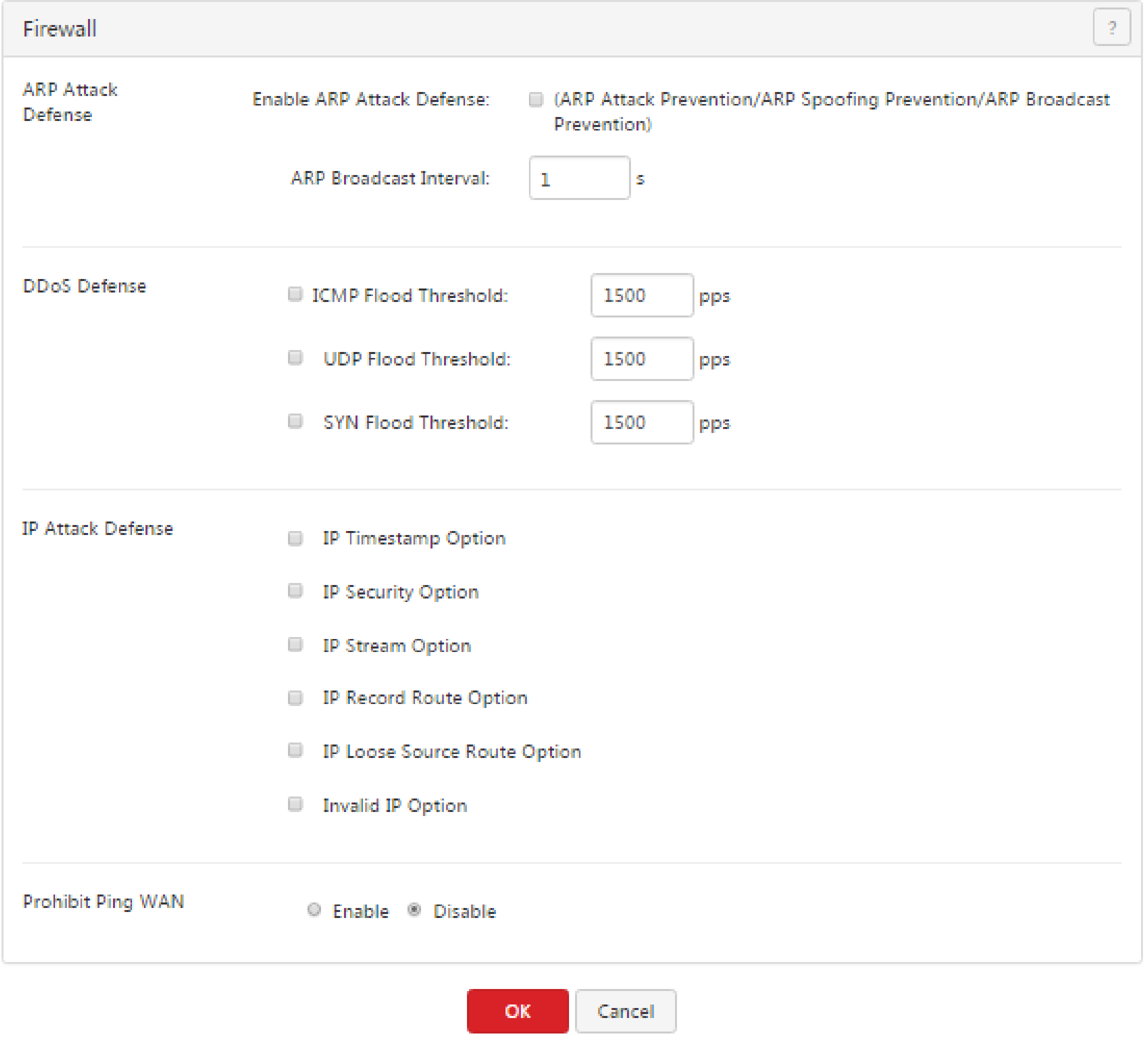
3. To delete multiple entries at the same time, select the entries and click Unbind.

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.



ARP Attack Defense

Enable ARP Attack Defense: □ (ARP Attack Prevention/ARP Spoofing Prevention/ARP Broadcast Prevention)

ARP Broadcast Interval: 1 s

DDoS Defense

□ ICMP Flood Threshold: 1500 pps

□ UDP Flood Threshold: 1500 pps

□ SYN Flood Threshold: 1500 pps

IP Attack Defense

□ IP Timestamp Option

□ IP Security Option

□ IP Stream Option

□ IP Record Route Option

□ IP Loose Source Route Option

□ Invalid IP Option

Prohibit Ping WAN ○ Enable ● Disable

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.

The following table describes the parameters.

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

Parameter		Description
		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.
Prohibit Ping WAN		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.

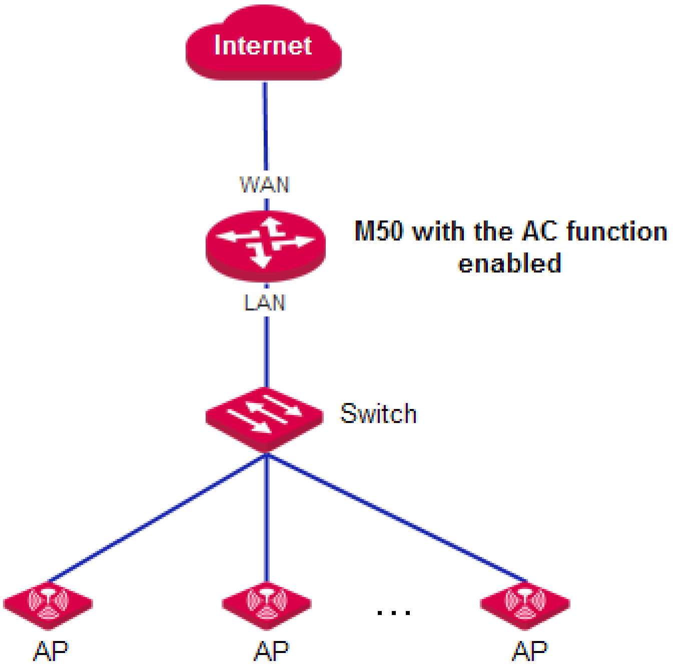
Chapter 9 AC management

This chapter describes:

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

9.1 Overview

M50 can work as an AC to manage a maximum of 16 IP-COM APs. The following figure shows the network topology where M50 functions as an AC to manage APs.



The AC management function of M50 allows you to configure wireless settings, Configuring advanced settings, Managing APs, Viewing user status.

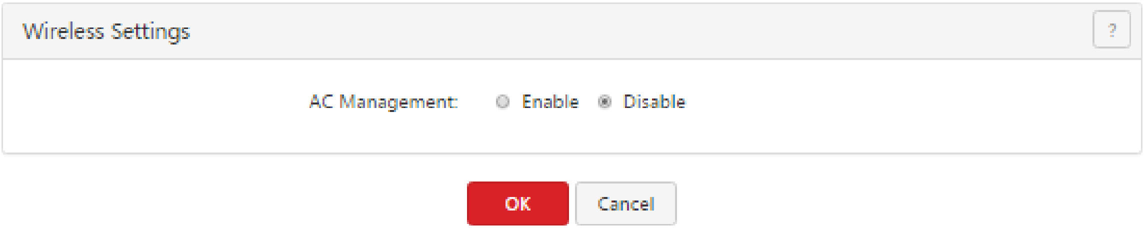
- Wireless Settings: This module allows you to enable or disable the AC management function of the router and configure SSID-related parameters for the APs on your LAN in a centralized manner. The parameters allow you to specify SSIDs, SSID status, frequencies, maximum number of users, VLAN IDs, authentication 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.



Wireless Settings

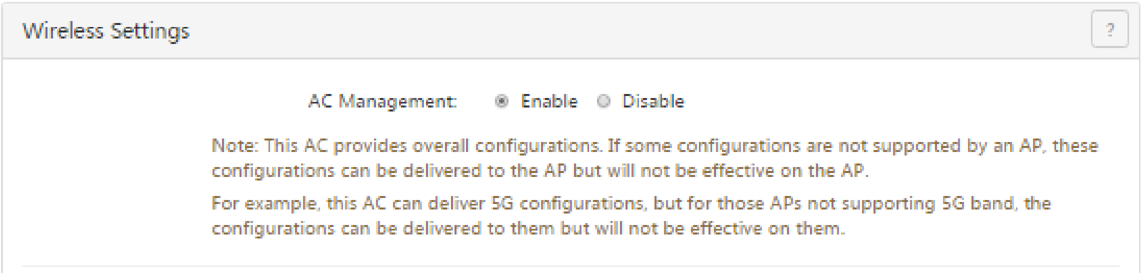
AC Management: ○ Enable ● Disable

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**.



Wireless Settings

AC Management: ● Enable ○ Disable

Note: This AC provides overall configurations. If some configurations are not supported by an AP, these configurations can be delivered to the AP but will not be effective on the AP.

For example, this AC can deliver 5G configurations, but for those APs not supporting 5G band, the configurations can be delivered to them but will not be effective on them.

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

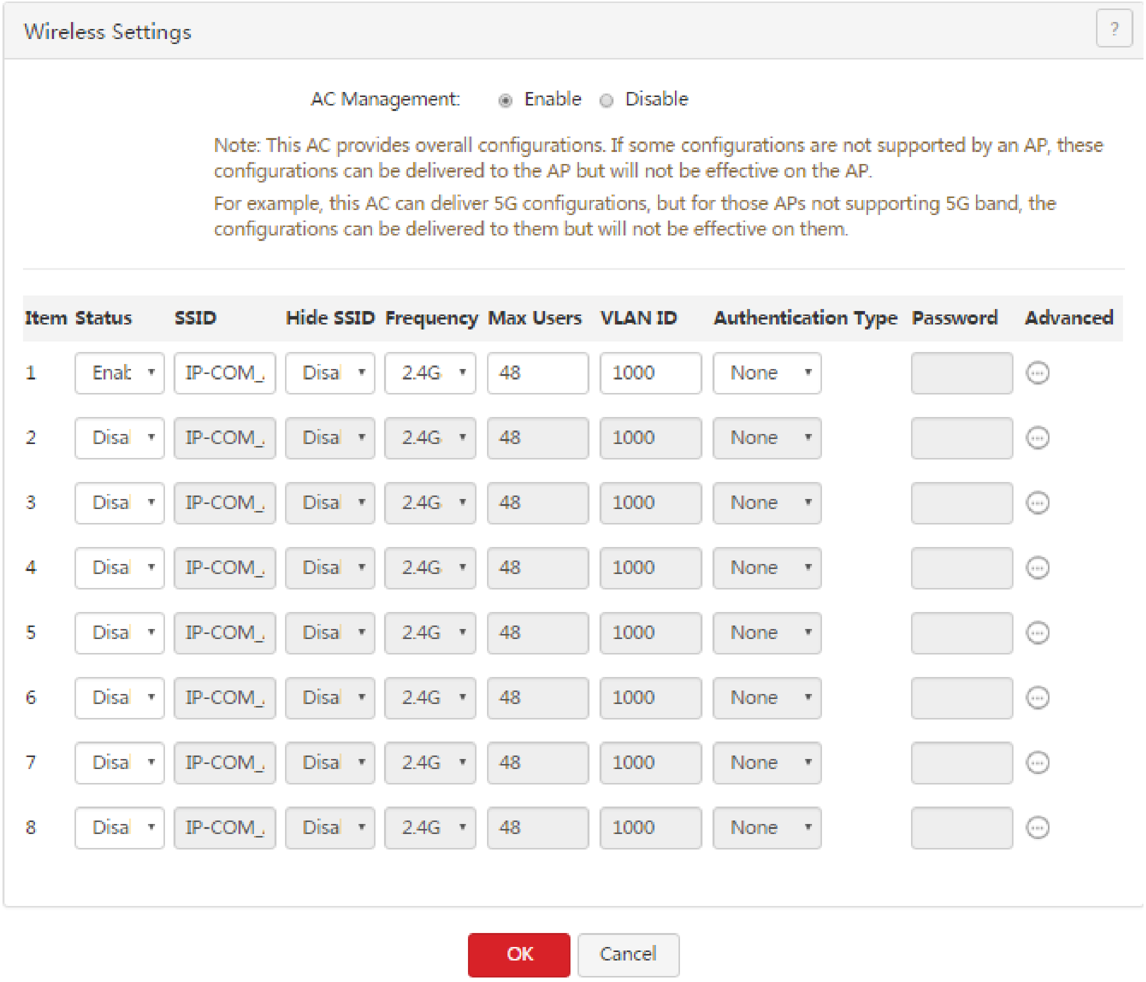
1. Choose **AC Management** > **Wireless Settings**.

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.



Wireless Settings ?

AC Management: ● Enable ○ Disable

Note: This AC provides overall configurations. If some configurations are not supported by an AP, these configurations can be delivered to the AP but will not be effective on the AP.

For example, this AC can deliver 5G configurations, but for those APs not supporting 5G band, the configurations can be delivered to them but will not be effective on them.

Item	Status	SSID	Hide SSID	Frequency	Max Users	VLAN ID	Authentication Type	Password	Advanced
1	Enab	IP-COM_	Disa	2.4G	48	1000	None		⋯
2	Disa	IP-COM_	Disa	2.4G	48	1000	None		⋯
3	Disa	IP-COM_	Disa	2.4G	48	1000	None		⋯
4	Disa	IP-COM_	Disa	2.4G	48	1000	None		⋯
5	Disa	IP-COM_	Disa	2.4G	48	1000	None		⋯
6	Disa	IP-COM_	Disa	2.4G	48	1000	None		⋯
7	Disa	IP-COM_	Disa	2.4G	48	1000	None		⋯
8	Disa	IP-COM_	Disa	2.4G	48	1000	None		⋯

OK Cancel

The following table describes the parameters.

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**

Parameter	Description
	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 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 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 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 QVLAN 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 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.

Parameter	Description
Advanced	It allows you to specify whether to enable the client isolation function. The options include: ● **Enable**: It indictes that wireless clients connected using the same SSID cannot communicate with each other. ● **Disable**: It indictes that wireless clients connected using the same SSID can communicate with each other.

9.3 Configuring advanced settings

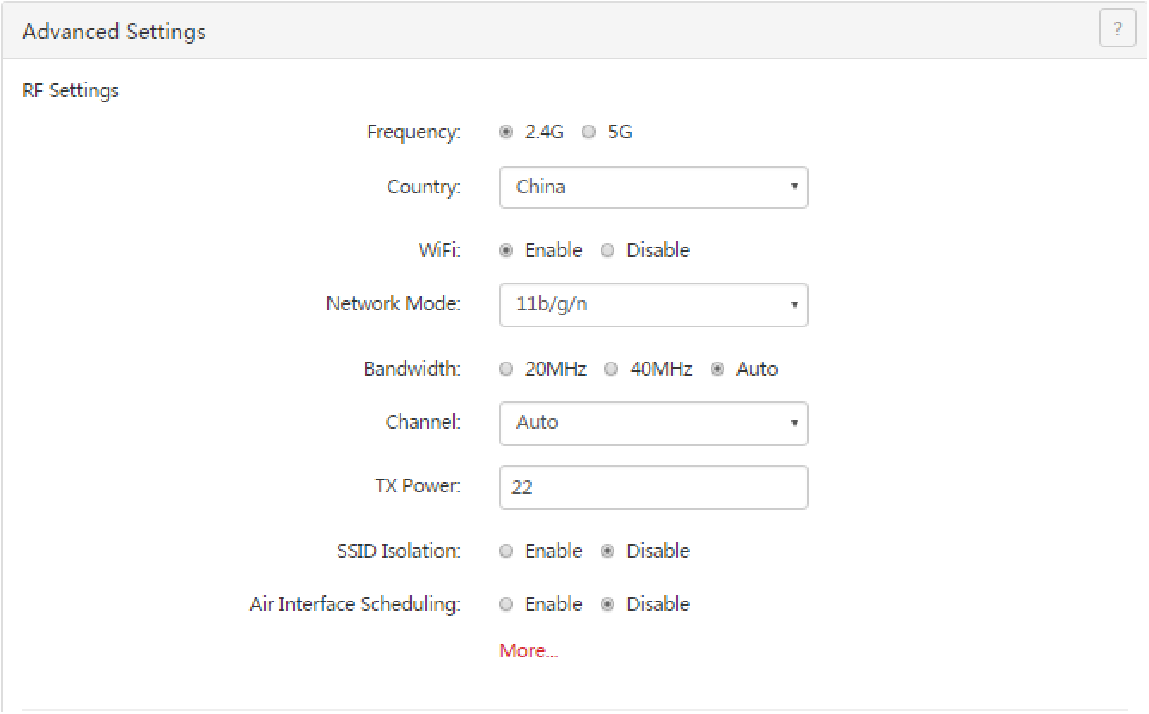
To access the page for configuring advanced settings, choose **AC Management** > **Advanced Settings**. The page includes RF settings and global settings for APs.

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, wireless network switch, and channel parameters, in the **RF Settings** area.



Advanced Settings

RF Settings

Frequency: ● 2.4G ○ 5G

Country: China

WiFi: ● Enable ○ Disable

Network Mode: 11b/g/n

Bandwidth: ○ 20MHz ○ 40MHz ● Auto

Channel: Auto

TX Power: 22

SSID Isolation: ○ Enable ● Disable

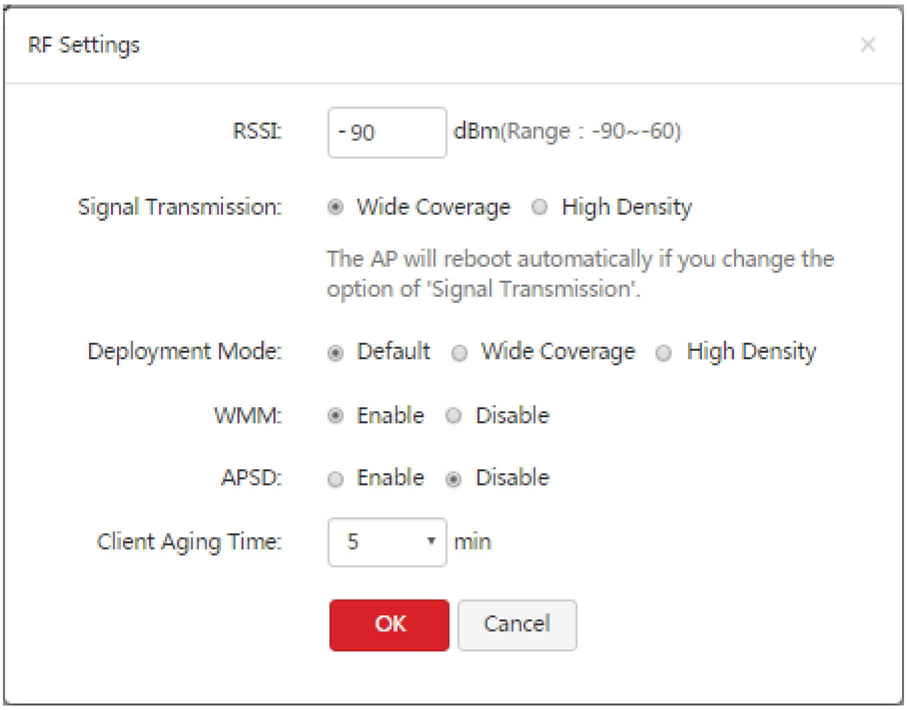
Air Interface Scheduling: ○ Enable ● Disable

The following table describes the parameters.

Parameter	Description
Frequency	It specifies the intended AP operating frequency of the parameters on the page. ⚠ **Note** The settings are delivered to all APs.
Country	It specifies the country 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: ● **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**.
TX 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.

Parameter	Description
SSID Isolation	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.



RF Settings ×

RSSI: -90 dBm(Range : -90~-60)

Signal Transmission: ● Wide Coverage ○ High Density

The AP will reboot automatically if you change the option of 'Signal Transmission'.

Deployment Mode: ● Default ○ Wide Coverage ○ High Density

WMM: ● Enable ○ Disable

APSD: ○ Enable ● Disable

Client Aging Time: 5 min

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

The following table describes the parameters.

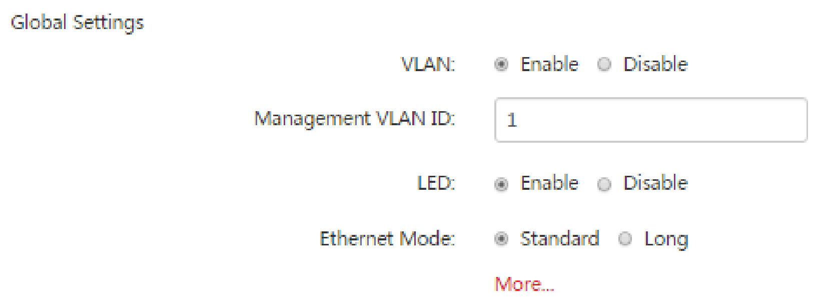
Parameter	Description
RSSI	It specifies the minimum wireless client signal strength acceptable to an AP. A mobile client with signal strength lower than this threshold cannot connect to the AP. You can set this parameter to ensure that mobile clients connect to APs with strong signal strength.
Signal 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

Parameter	Description
	application scenario of the router. The options include: ● Wide Coverage: This option is used in places with low AP density, such as offices, warehouses, and hospitals, to increase AP coverage. ● High Density: 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.
Deployment Mode	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: ● High Density: This option is used in scenarios with high AP density to ensure that clients connect to APs with strong signals. ● Wide Coverage: 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 Aging Time	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 Ethernet mode parameters, in the **Global Settings** area.



Global Settings

VLAN: ● Enable ○ Disable

Management VLAN ID: 1

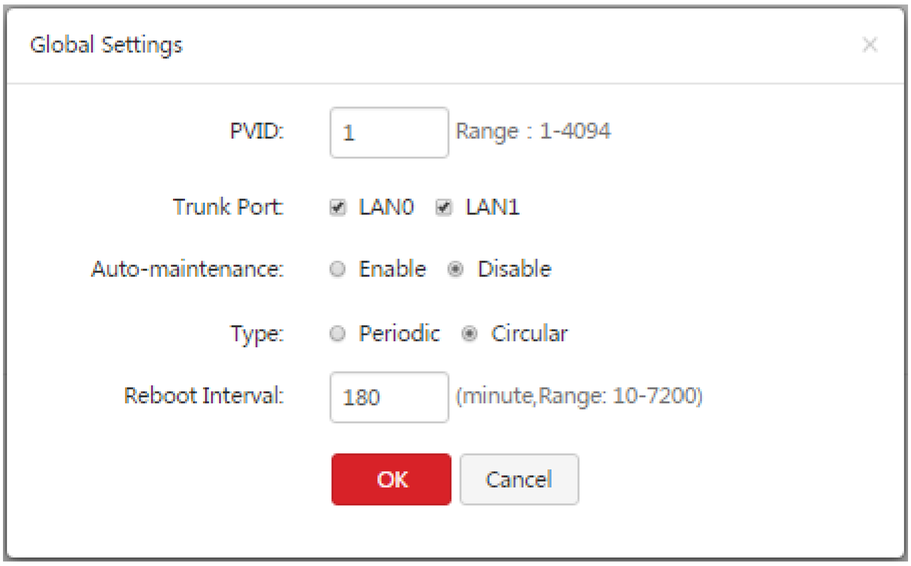
LED: ● Enable ○ Disable

Ethernet Mode: ● Standard ○ Long

The following table describes the parameters.

Parameter	Description
VLAN	It specifies whether to enable the QVLAN 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.
Ethernet Mode	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. ● **Long**: This option is recommended for a scenario that involves a long transmission distance and it results in a low transmission speed. Generally, 10 Mbps is adopted through negotiation. Use the **Long** 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.



Global Settings

PVID: 1 Range : 1-4094

Trunk Port: ☑ LAN0 ☑ LAN1

Auto-maintenance: ○ Enable ● Disable

Type: ○ Periodic ● Circular

Reboot Interval: 180 (minute,Range: 10-7200)

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

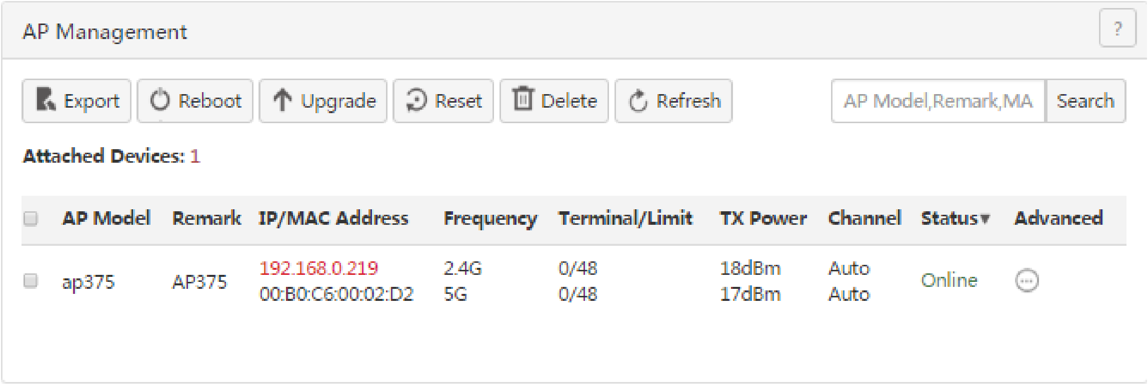
The following table describes the parameters.

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, set **Type** and then **Maintenance Time** (in case that **Type** is set to **Periodic**) or **Reboot Interval** (in case that **Type** is set to **Circular**). By default, this function is disabled. ⚠ **Note** This function help prevent WLAN performance decreases 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.

Parameter	Description
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.



Attached Devices: 1

□	AP Model	Remark	IP/MAC Address	Frequency	Terminal/Limit	TX Power	Channel	Status▾	Advanced
□	ap375	AP375	192.168.0.219 00:B0:C6:00:02:D2	2.4G 5G	0/48 0/48	18dBm 17dBm	Auto Auto	Online	⋯

9.4.1 Exporting information about APs managed by the router

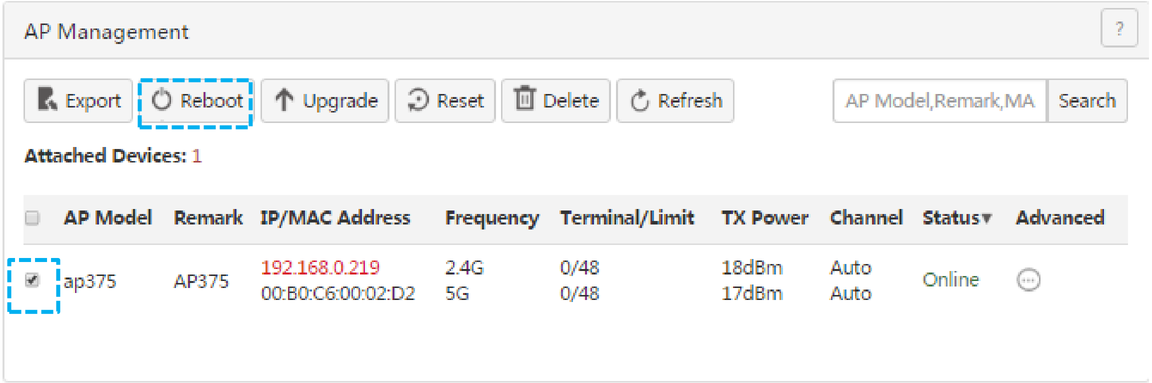
This function enables you to export information about APs managed by the router to an Excel file on your local computer.

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.



Attached Devices: 1

□	AP Model	Remark	IP/MAC Address	Frequency	Terminal/Limit	TX Power	Channel	Status▾	Advanced
☑	ap375	AP375	192.168.0.219 00:B0:C6:00:02:D2	2.4G 5G	0/48 0/48	18dBm 17dBm	Auto Auto	Online	⋯

When the APs are rebooting, they enter the Offline status. When rebooting is complete, the APs enter the Online status again. It takes about 1 to 2 minutes to complete this process. You can click **Refresh** to check the status change.

9.4.3 Upgrading APs

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

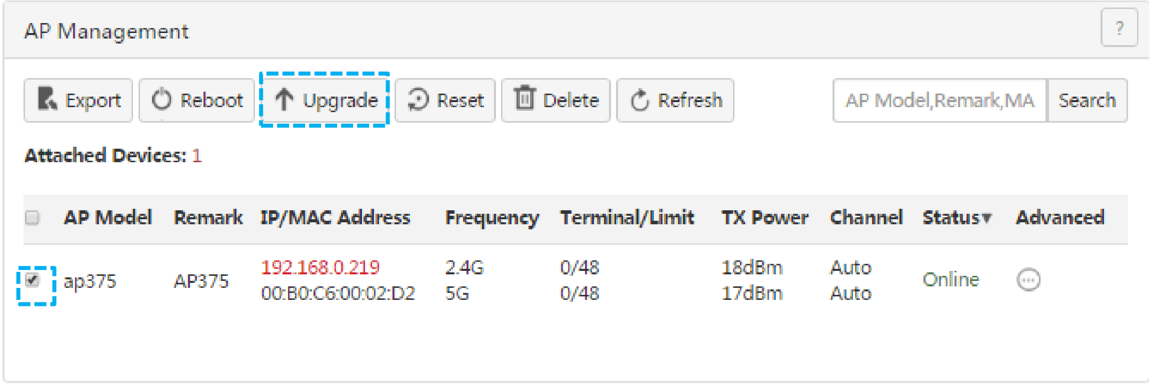
Note

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

1. Download corresponding fat 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.



Attached Devices: 1

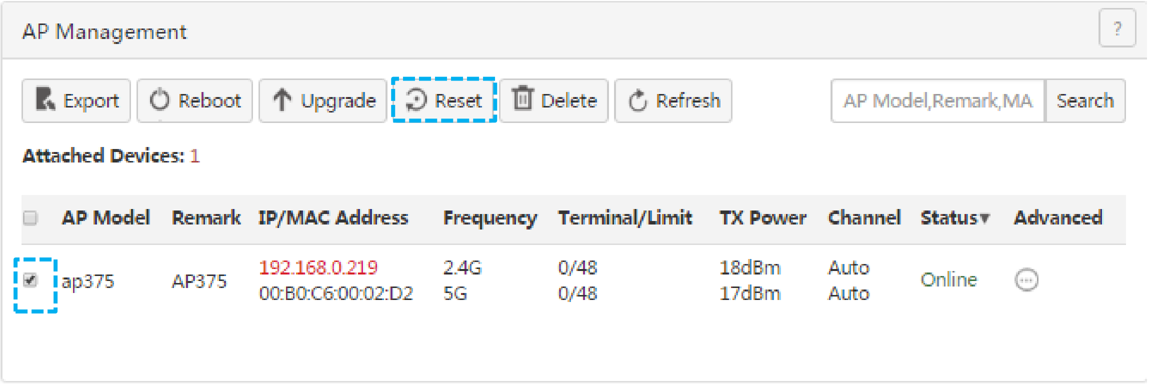
□	AP Model	Remark	IP/MAC Address	Frequency	Terminal/Limit	TX Power	Channel	Status▾	Advanced
☑	ap375	AP375	192.168.0.219 00:B0:C6:00:02:D2	2.4G 5G	0/48 0/48	18dBm 17dBm	Auto Auto	Online	⋯

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.



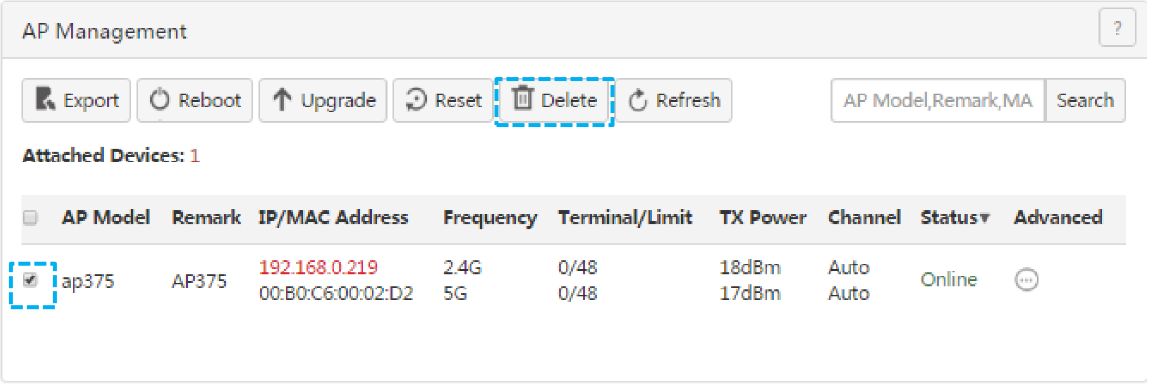
Attached Devices: 1

□	AP Model	Remark	IP/MAC Address	Frequency	Terminal/Limit	TX Power	Channel	Status▾	Advanced
☑	ap375	AP375	192.168.0.219 00:B0:C6:00:02:D2	2.4G 5G	0/48 0/48	18dBm 17dBm	Auto Auto	Online	⋯

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.



Attached Devices: 1

□	AP Model	Remark	IP/MAC Address	Frequency	Terminal/Limit	TX Power	Channel	Status▾	Advanced
☑	ap375	AP375	192.168.0.219 00:B0:C6:00:02:D2	2.4G 5G	0/48 0/48	18dBm 17dBm	Auto Auto	Online	⋯

Note

Online APs cannot be deleted.

9.4.6 Updating AP information

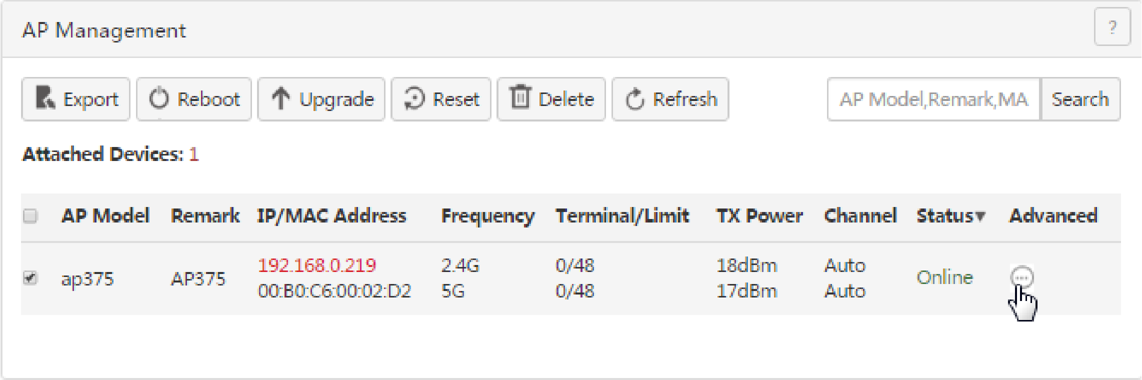
This function enables you to update information about APs.

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.

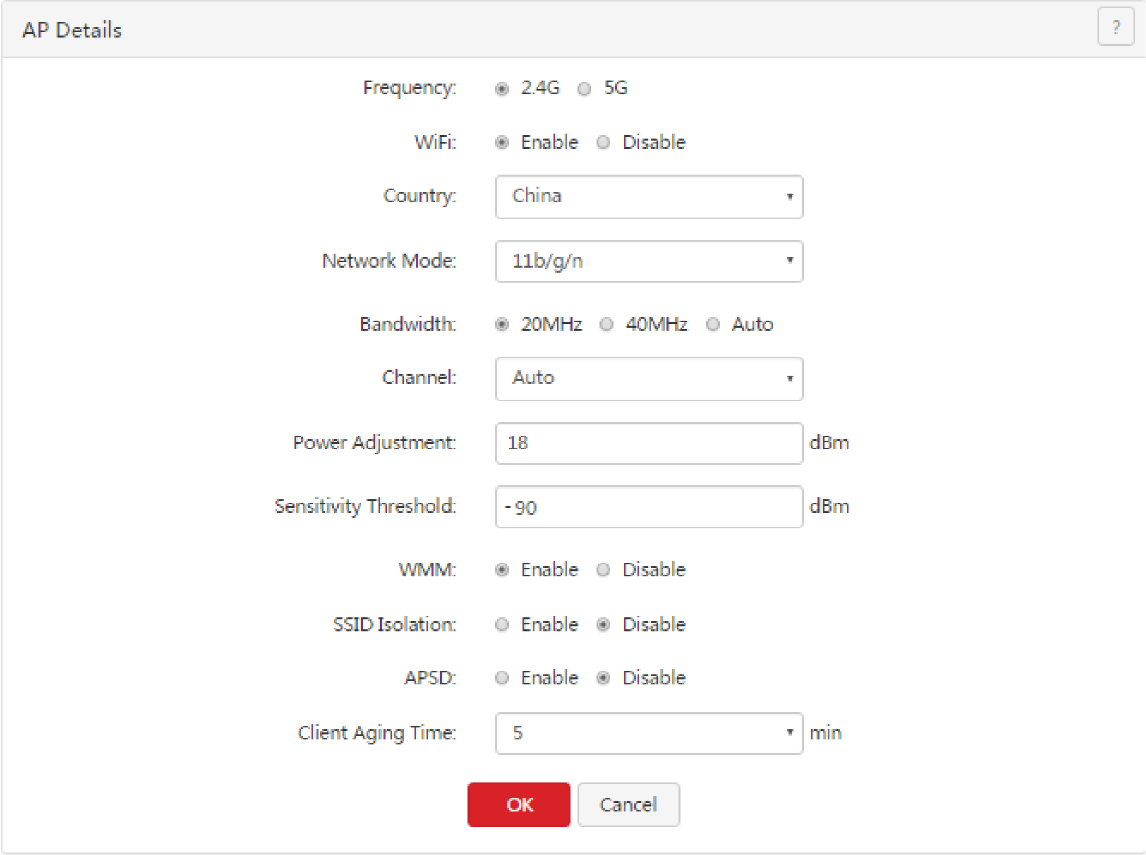


AP Management

Attached Devices: 1

□	AP Model	Remark	IP/MAC Address	Frequency	Terminal/Limit	TX Power	Channel	Status▾	Advanced
☑	ap375	AP375	192.168.0.219 00:B0:C6:00:02:D2	2.4G 5G	0/48 0/48	18dBm 17dBm	Auto Auto	Online	⋯

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

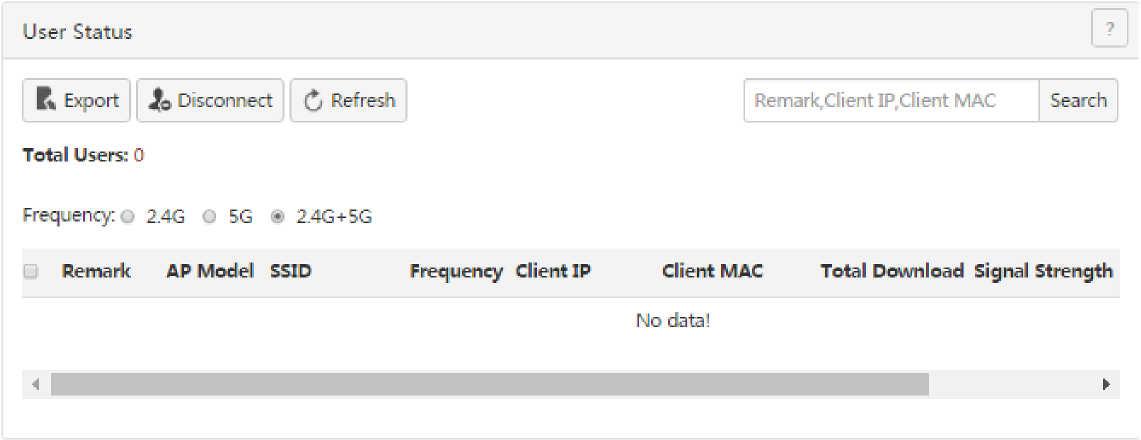


AP Details

Frequency:	● 2.4G ○ 5G
WiFi:	● Enable ○ Disable
Country:	China
Network Mode:	11b/g/n
Bandwidth:	● 20MHz ○ 40MHz ○ Auto
Channel:	Auto
Power Adjustment:	18 dBm
Sensitivity Threshold:	-90 dBm
WMM:	● Enable ○ Disable
SSID Isolation:	○ Enable ● Disable
APSD:	○ Enable ● Disable
Client Aging Time:	5 min

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.



User Status

Total Users: 0

Frequency: ○ 2.4G ○ 5G ● 2.4G+5G

□	Remark	AP Model	SSID	Frequency	Client IP	Client MAC	Total Download	Signal Strength

No data!

The following table describes the parameters.

Parameter	Description
Frequency (above the list)	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**.

If the user wants to access the network, he/she must reconnect to an AP.

9.6 Updating user information

1. Choose **AC Management** > **AP Management**.

2. Click **Refresh**.

Chapter 10 Captive portal

This chapter describes:

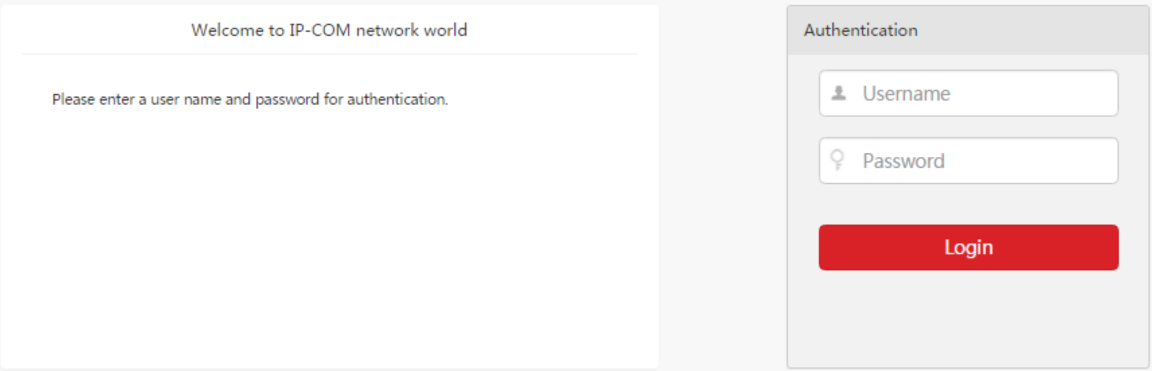
- Configuring web authentication
- Example of configuring web authentication

10.1 Overview

M50 supports web authentication and PPPoE authentication and only either of them can be enabled on the router. If the computers connected to your LAN with or without cables must be authenticated for accessing the internet, select either authentication mode.

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 web authentication 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.



Welcome to IP-COM network world

Please enter a user name and password for authentication.

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

10.1.2 Configuring web authentication

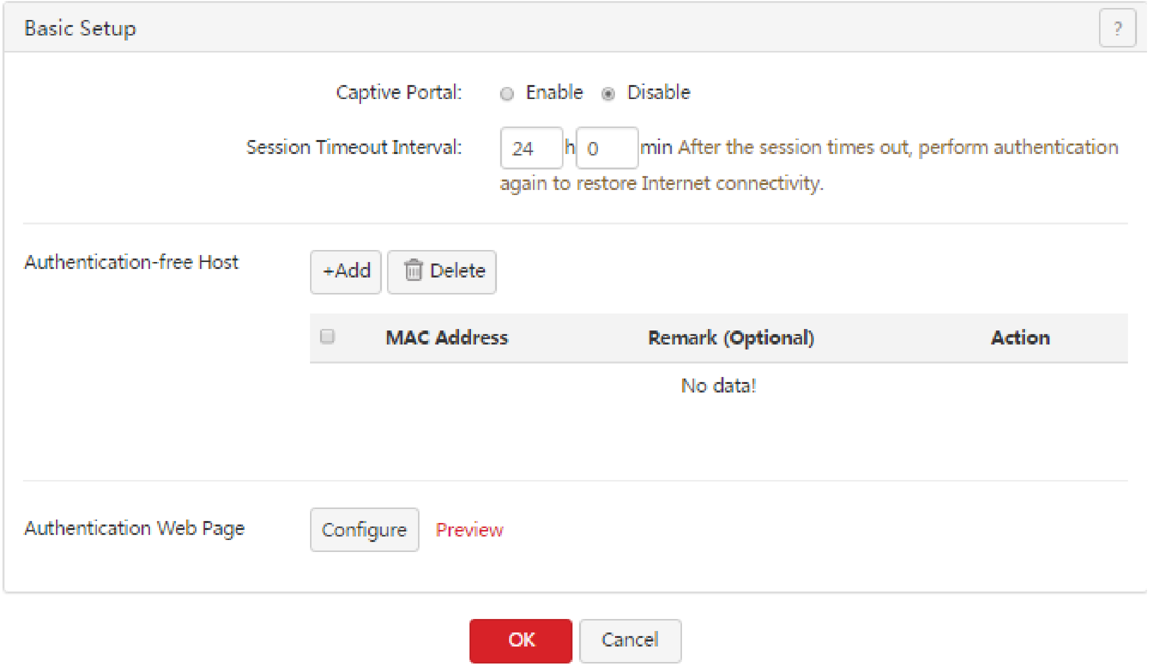
The following table describes the steps for configuring web authentication.

Step	Task	Description
1	Configuring basic settings	Choose **Captive Portal** > **Basic Setup** 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 web authentication

10.2.1 Configuring basic settings

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



Basic Setup

Captive Portal: ○ Enable ● Disable

Session Timeout Interval: 24 h 0 min After the session times out, perform authentication again to restore Internet connectivity.

Authentication-free Host

□	MAC Address	Remark (Optional)	Action
No data!			

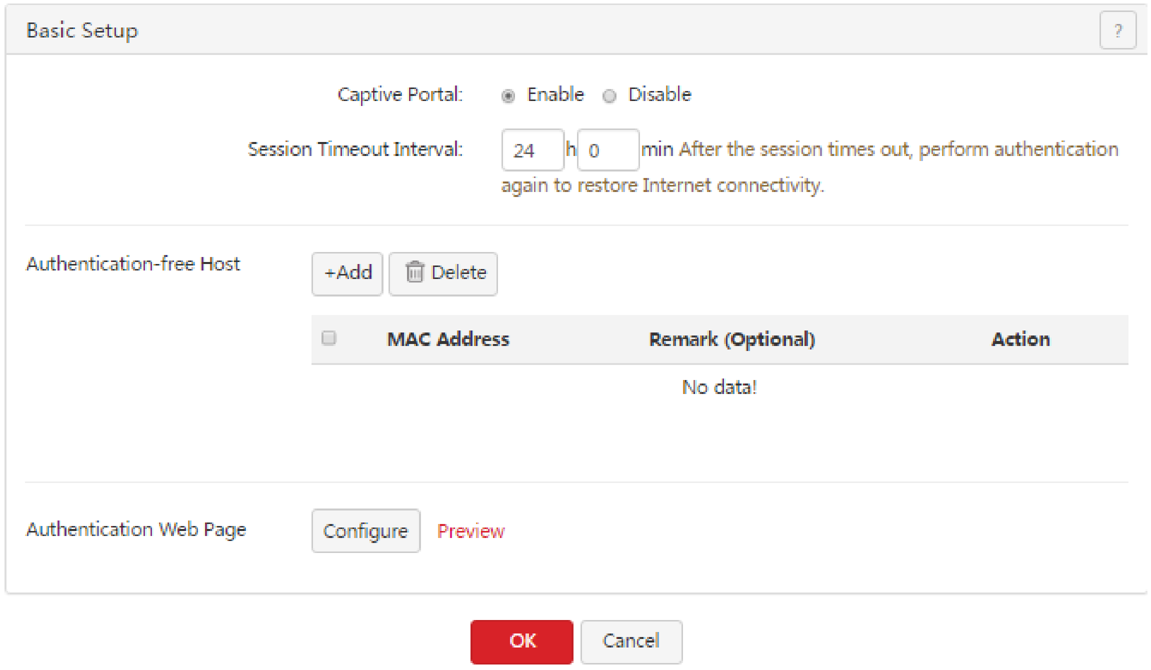
Authentication Web Page

The following table describes the parameters.

Parameter	Description
Captive Portal	It specifies whether to enable the web authentication function of the router. If the function is enabled, the PPPoE authentication function of the router is disabled.
Session Timeout Interval	It specifies the authentication validity period. A user must be re-authenticated for accessing the internet after the period expires.
Authentication-free Host	It specifies the user devices that can access the internet without being authenticated by the router after web authentication is enabled.
Authentication Web Page	It allows you to configure the authentication web page.

Enabling web authentication

1. Choose **Captive Portal** > **Basic Setup**.
2. Set **Captive Portal** to **Enable**.
3. Set **Session Timeout Interval** to a required authentication validity period.
4. Click **OK**.



Basic Setup ?

Captive Portal: ● Enable ○ Disable

Session Timeout Interval: 24 h 0 min After the session times out, perform authentication again to restore Internet connectivity.

Authentication-free Host +Add Delete

□	MAC Address	Remark (Optional)	Action
		No data!	

Authentication Web Page Configure Preview

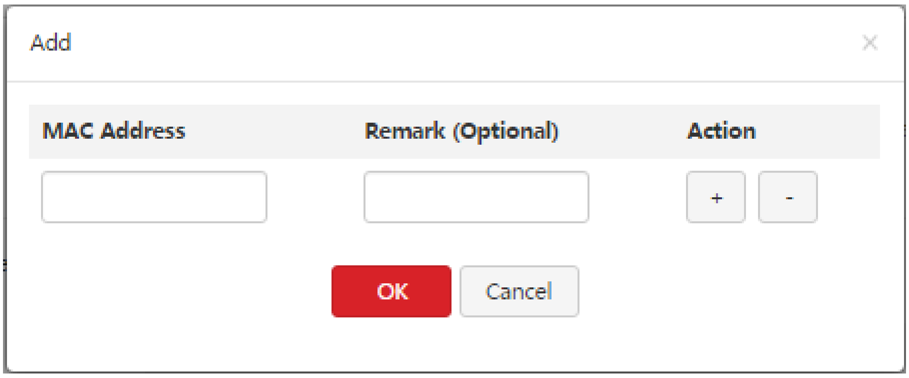
OK Cancel

Specifying the user devices that do not need to be authenticated

1. Choose **Captive Portal** > **Basic Setup**.

2. Click +Add in the **Authentication-free Host** area.

   The **Add** dialog box appears.



Add ×

MAC Address	Remark (Optional)	Action
		+ -

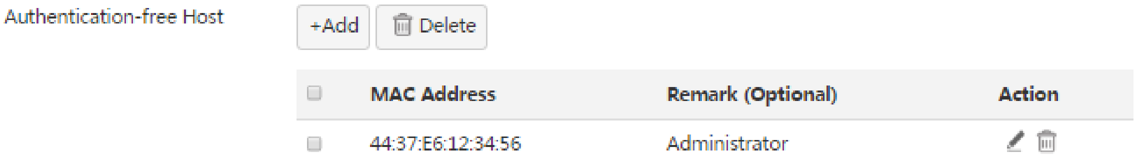
OK Cancel

The following table describes the parameters.

Parameter	Description
MAC Address	It specifies the MAC address of a user device that can access the internet without being authenticated by the router.
Remark (Optional)	It specifies the description of a user device that can access the internet without being authenticated by the router.
Action	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.

3. Set the parameters and click **OK**.

The **Basic Setup** page appears, showing the user devices that can access the internet without being authenticated by the router. See the following figure.



Authentication-free Host

+Add 🗑 Delete

□	MAC Address	Remark (Optional)	Action
□	44:37:E6:12:34:56	Administrator	✎ 🗑

4. To modify the information about a user device on the list, click ✎ corresponding to the user device.

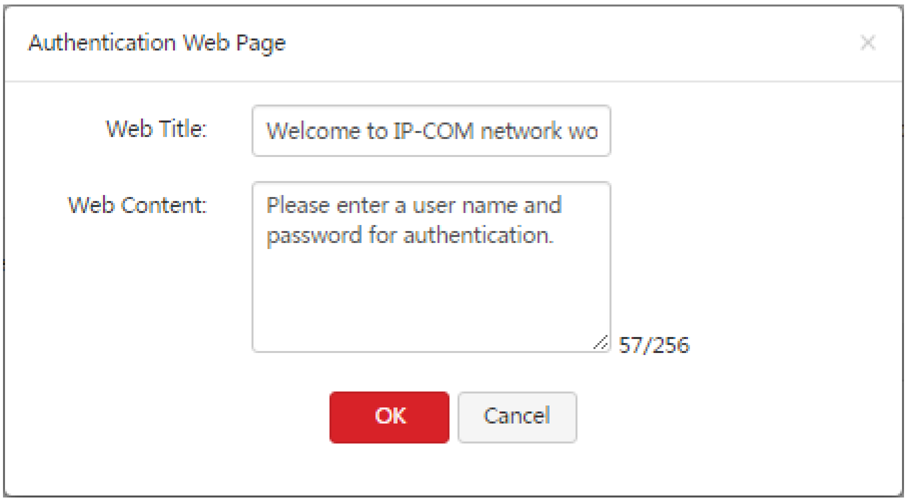
5. To delete the information about a user device from the list, click 🗑 corresponding to the user device.

6. To delete the information about multiple user devices from the list at the same time, select the user devices and click 🗑 Delete.

Configuring the web authentication page

1. Choose **Captive Portal** > **Basic Setup**。

2. Click Config in the **Authentication Web Page** area.
   The **Authentication Web Page** dialog box appears.



Authentication Web Page ×

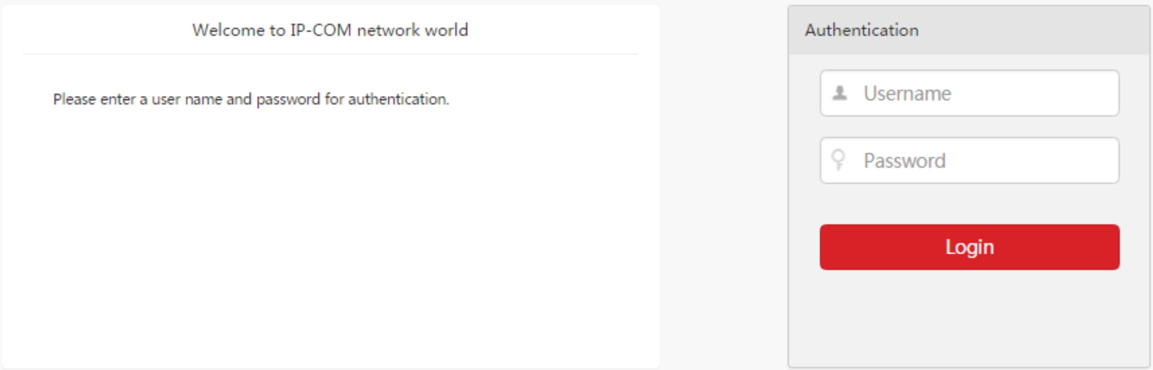
Web Title: Welcome to IP-COM network wo

Web Content: Please enter a user name and password for authentication.

57/256

3. Set the parameters and click **OK**.

The **Basic Setup** page appears. You can click Preview to preview the authentication web page. See the following figure.

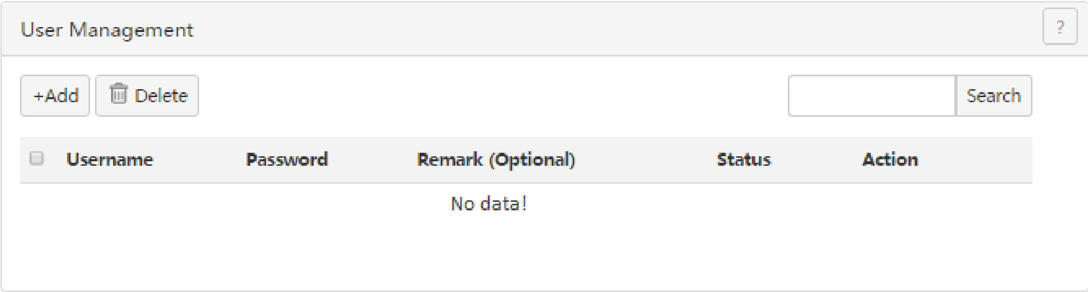


Welcome to IP-COM network world

Please enter a user name and password for authentication.

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 user accounts for web authentication. If web authentication is enabled, users can access the internet only after being authenticated with the accounts.



□	Username	Password	Remark (Optional)	Status	Action

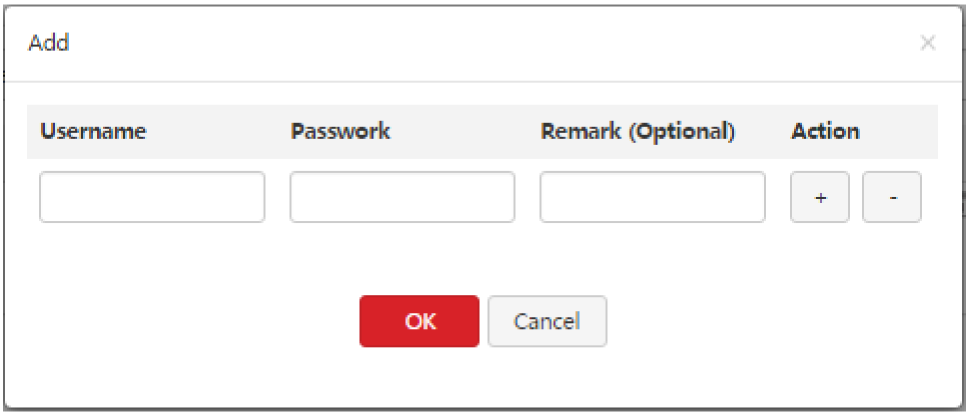
No data!

Adding a user account

1. Choose **Captive Portal** > **User Management**.

2. Click +Add.

   The **Add** dialog box appears.



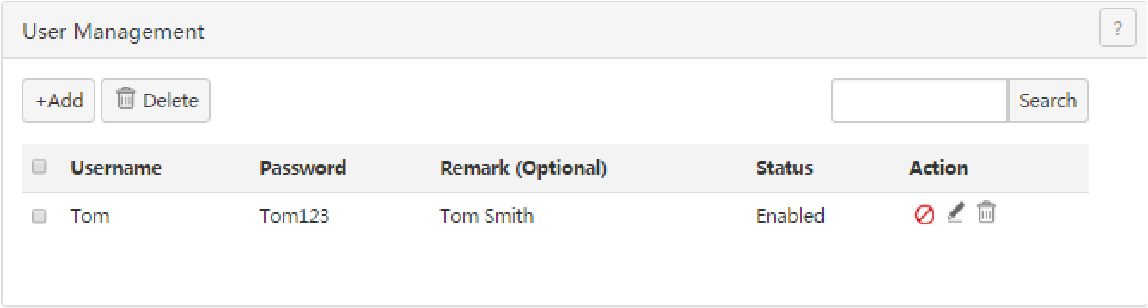
Username	Passwork	Remark (Optional)	Action

The following table describes the parameters.

Parameter	Description
Username Password	**Username** specifies a user name for web authentication. **Password** specifies a password for web authentication. If web authentication is enabled, a user must be authenticated with a correct user name and password before accessing the internet.
Remark (Optional)	It specifies the description of a user account.
Action	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.

3. Set the parameters and click **OK**.

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



User Management

+Add | 🗑 Delete | Search

□	Username	Password	Remark (Optional)	Status	Action
□	Tom	Tom123	Tom Smith	Enabled	⊘ ✎ 🗑

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.

   The account is deleted.

3. To delete multiple user accounts at the same time, select them and click 🗑 Delete.

10.3 Example of configuring web authentication

Networking Requirement

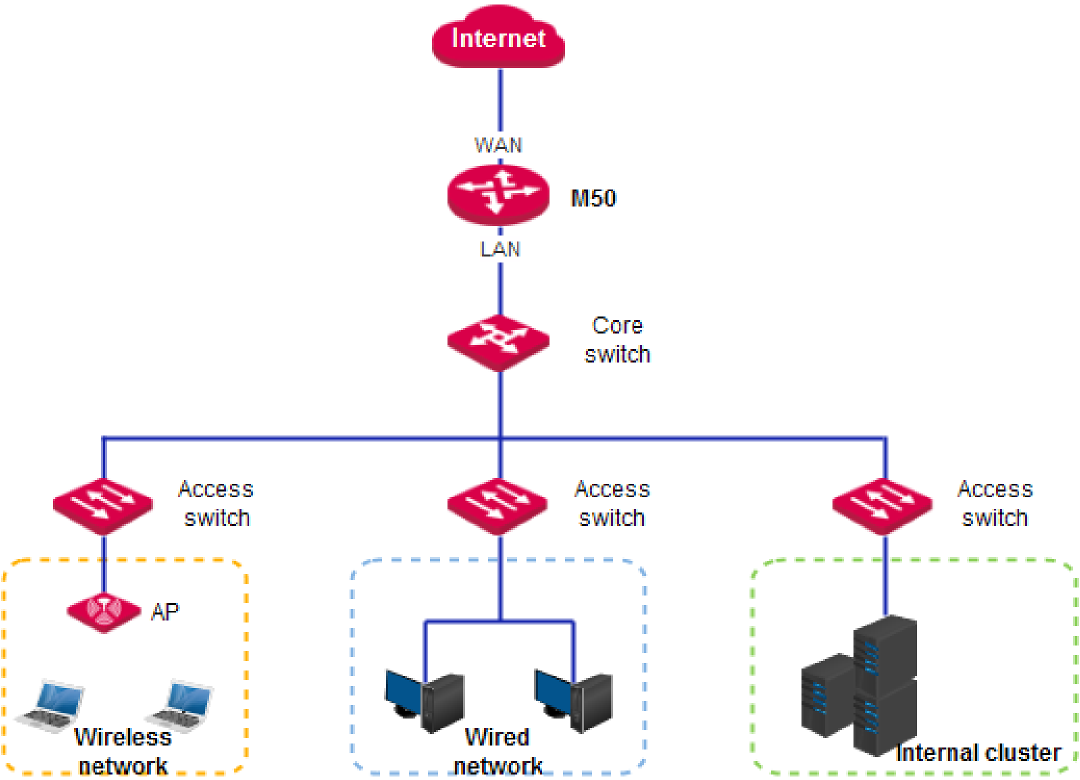
An enterprise uses M50 to set up a LAN to address the following requirement:

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 web authentication 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.

Network Topology

The following figure shows the network topology of the enterprise.



Configuration Procedure

I. Configure basic settings for web authentication.

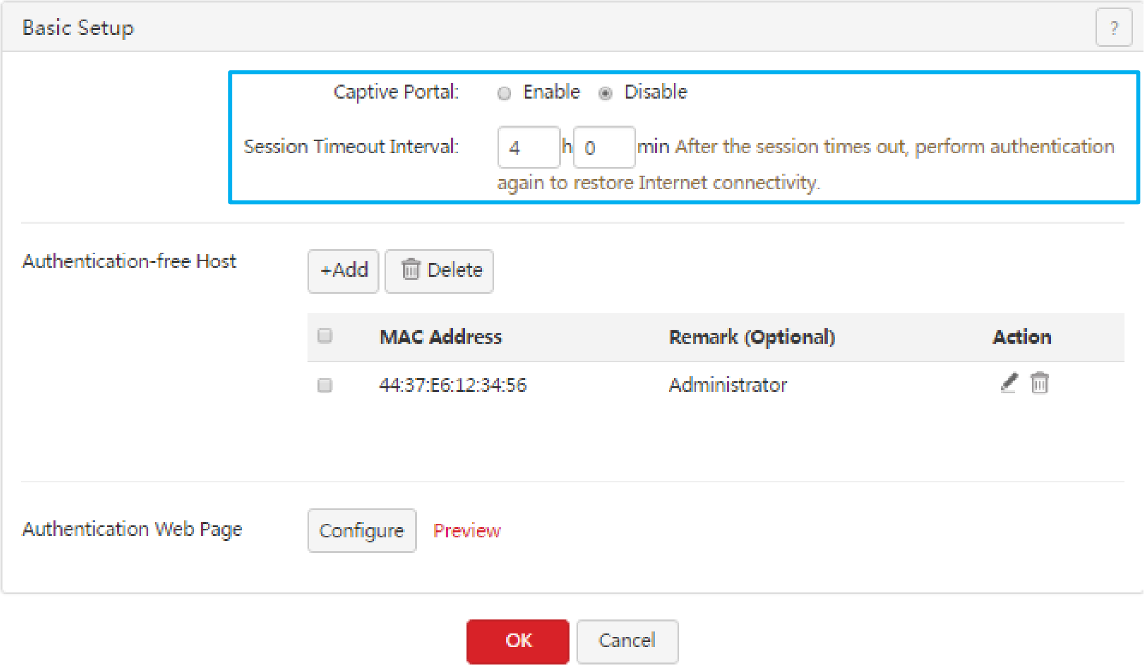
1. Enable web authentication.

(1) Choose **Captive Portal** > **Basic Setup**.

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

(3) Set **Session Timeout Interval** to **4 h**.

(4) Click **OK**.


Basic Setup

Captive Portal: ○ Enable ● Disable

Session Timeout Interval: 4 h 0 min After the session times out, perform authentication again to restore Internet connectivity.

Authentication-free Host

□	MAC Address	Remark (Optional)	Action
□	44:37:E6:12:34:56	Administrator	

Authentication Web Page

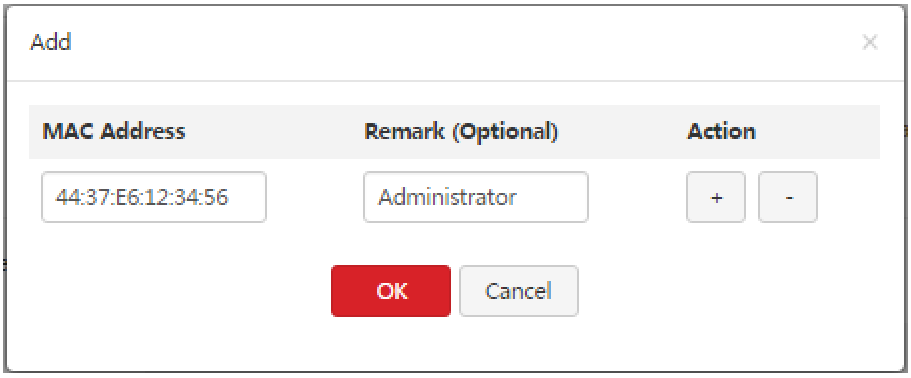
2. Add user devices that can access the internet without being authenticated.

(1) Choose **Captive Portal** > **Basic Setup** and click +Add in the **Authentication-free Host** area. The **Add** dialog box appears.

(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**.



MAC Address	Remark (Optional)	Action
44:37:E6:12:34:56	Administrator	+ -

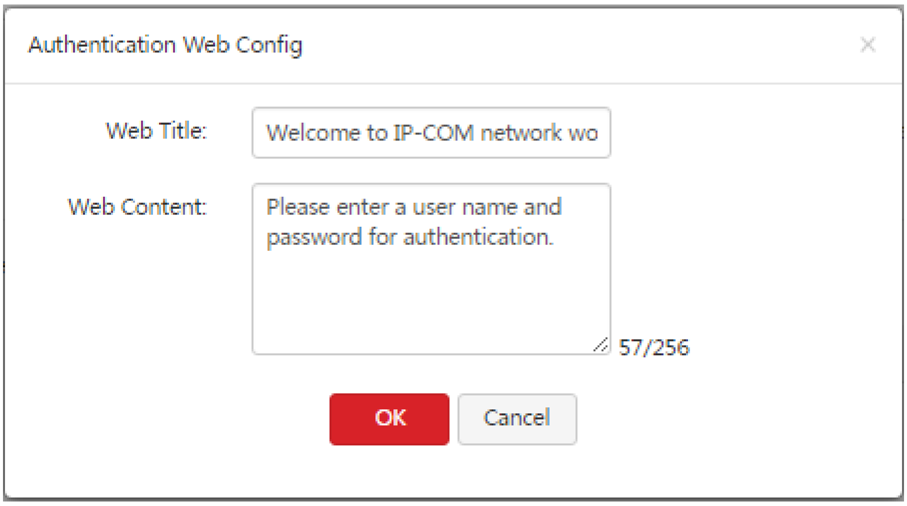
3. Configure the authentication web page.

(1) Choose **Captive Portal** > **Basic Setup** and click Configure in the **Authentication Web Page** area. The **Authentication Web Page** dialog box appears.

(2) Set **Web Title** to the title of the message to be displayed on the authentication web page, which is **Welcome to IP-COM network world** in this example.

(3) Set **Web Content** to the content of the message, which is **Please enter a user name and password for authentication** in this example.

(4) Click **OK**.



Web Title: Welcome to IP-COM network wo

Web Content: Please enter a user name and password for authentication.

57/256

II. Add a user account for web authentication.

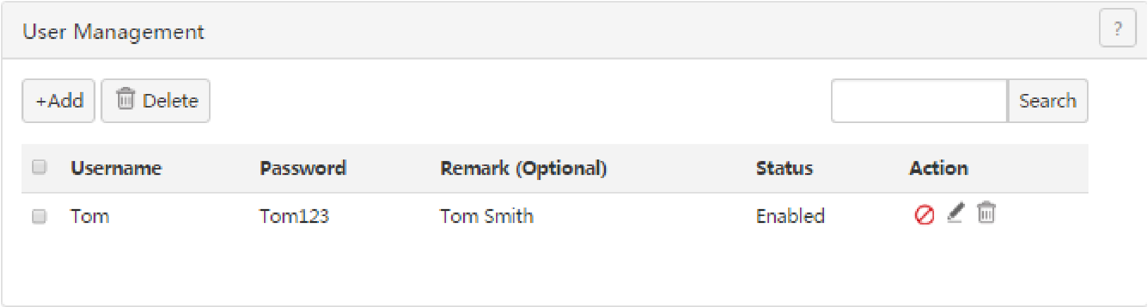
(1) Choose **Captive Portal** > **User Management** page and click +Add. The **Add** dialog box appears.

(2) Set **Username** to a user name for web authentication, which is **Tom** in this example.

(3) Set Password to the password of the user Tom, which is **Tom123** in this example.

(4) 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 another user account, click + and repeat the preceding steps.)

(5) Click **OK**.

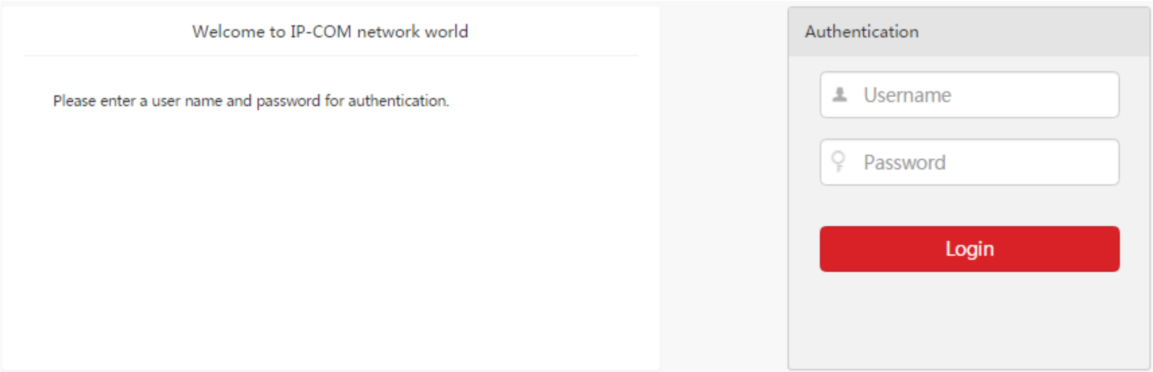


□	Username	Password	Remark (Optional)	Status	Action
□	Tom	Tom123	Tom Smith	Enabled	⊘ ✎ 🗑

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 web authentication page appears. See the following figure.



Welcome to IP-COM network world

Please enter a user name and password for authentication.

2. Enter a correct user name and password in the **Authentication** pane and click Login.

When the employee is authenticated, the employee is directed to the website specified before authentication.

Chapter 11 PPPoE authentication

11.1 Overview

M50 supports web authentication and PPPoE authentication and only either of them can be enabled on the router. If the computers connected to your LAN with or without cables must be authenticated for accessing the internet, select either authentication mode.

This chapter describes:

- Configuring PPPoE authentication
- Example of configuring PPPoE authentication

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.

M50 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, M50 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 Setup**, enable PPPoE authentication, and set the parameters.
2	Managing accounts	Choose **PPPoE Authentication** > **Account Management**, create accounts for users to set up PPPoE dial-up connections for accessing the internet.

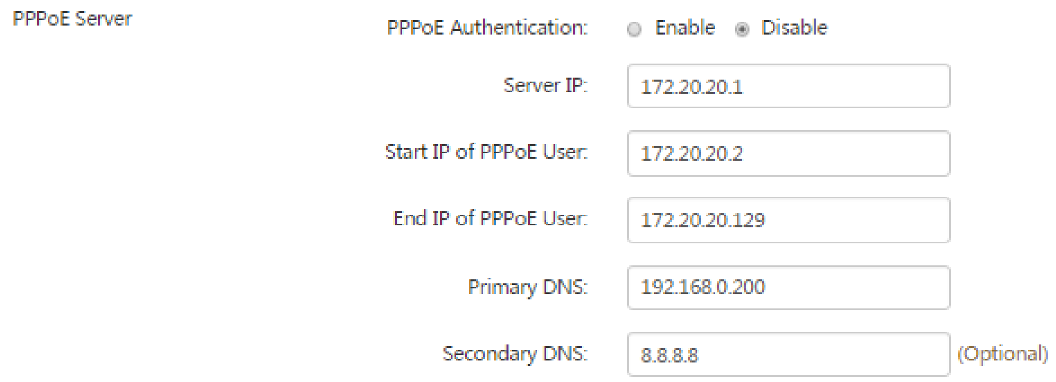
11.2 Configuring PPPoE authentication

11.2.1 Configuring basic settings

To access the page for configuring basic settings, choose **PPPoE Authentication** > **Basic Setup**. 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.



PPPoE Server

PPPoE Authentication: ○ Enable ● Disable

Server IP: 172.20.20.1

Start IP of PPPoE User: 172.20.20.2

End IP of PPPoE User: 172.20.20.129

Primary DNS: 192.168.0.200

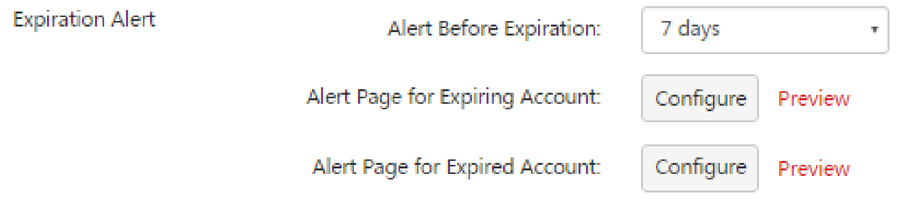
Secondary DNS: 8.8.8.8 (Optional)

The following table describes the parameters.

Parameter	Description
PPPoE Authentication	It specifies whether to enable PPPoE authentication. If the function is enabled, the web authentication 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 ● Class C IP addresses: 192.168.0.1–192.168.255.254
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 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.



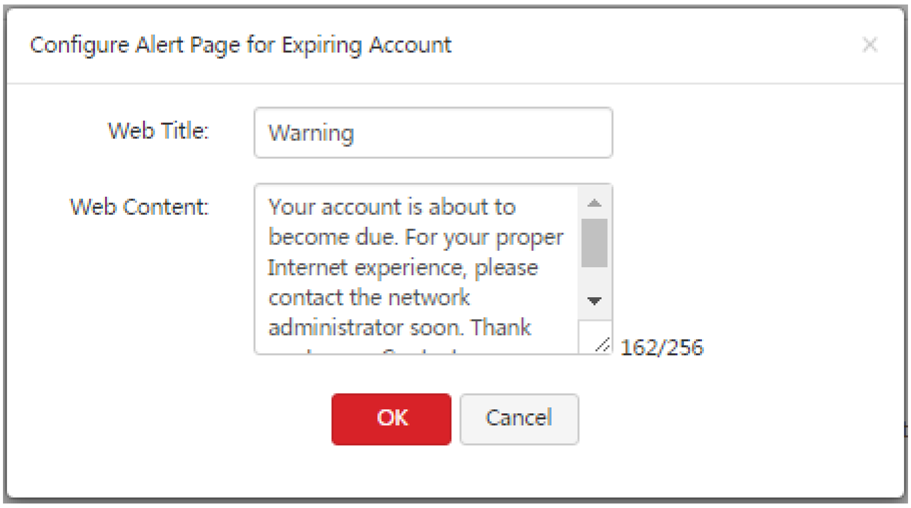
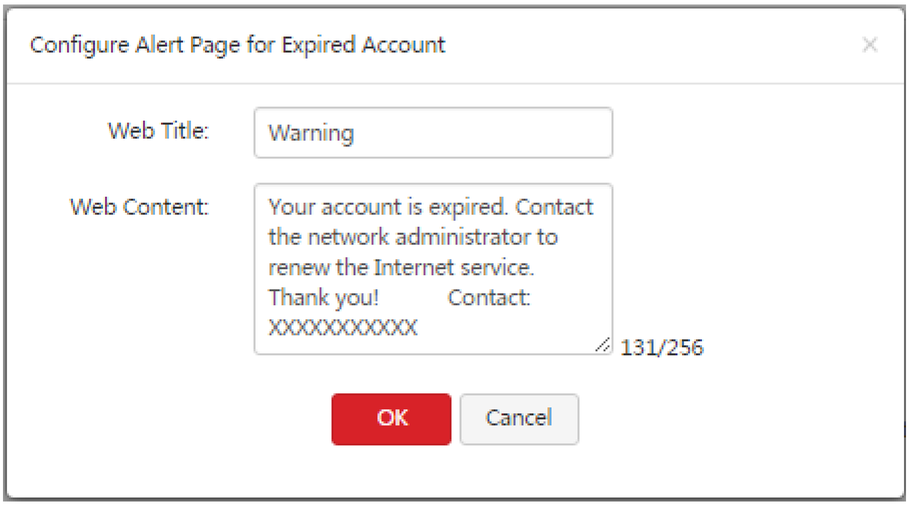
Expiration Alert

Alert Before Expiration: 7 days

Alert Page for Expiring Account:

Alert Page for Expired Account:

The following table describes the parameters.

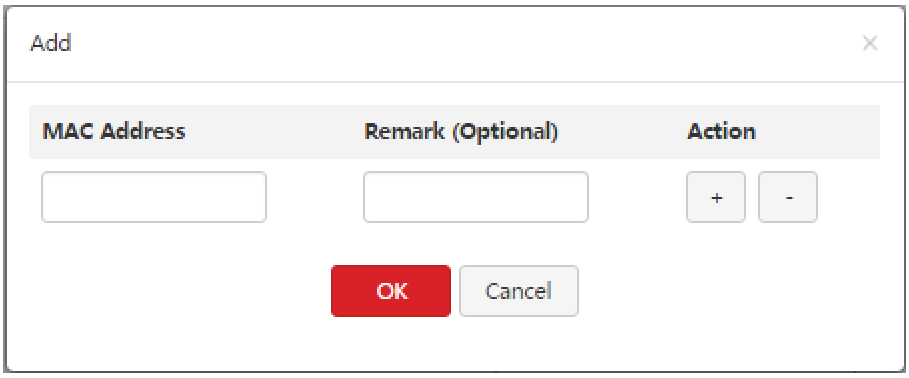
Parameter	Description
Alert Before Expiration	It specifies the number of days before account expiration to alert a user. By default, the router alerts a user 7 days before account expiration.
Alert Page for Expiring Account	It specifies the message on the alert page for expiring accounts. You can click Configure and modify the message. See the following figure.  Configure Alert Page for Expiring Account Web Title: Warning Web Content: Your account is about to become due. For your proper Internet experience, please contact the network administrator soon. Thank 162/256 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.  Configure Alert Page for Expired Account Web Title: Warning Web Content: Your account is expired. Contact the network administrator to renew the Internet service. Thank you! Contact: XXXXXXXXXXX 131/256 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 Setup**.

2. Click +Add in the **Authentication-free** area.

The **Add** dialog box appears.

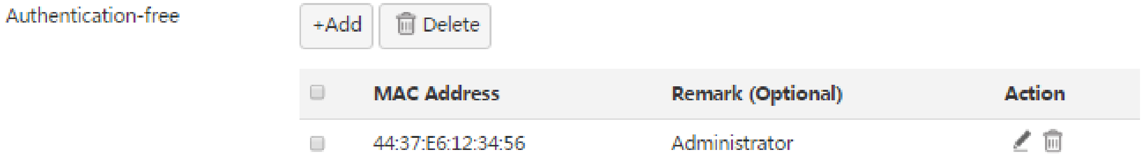


The following table describes the parameters.

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 (Optional)	It specifies the description of a host that can access the internet without being authenticated.
Action	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.

3. Set the parameters and click **OK**.

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



□	MAC Address	Remark (Optional)	Action
□	44:37:E6:12:34:56	Administrator	✎ 🗑

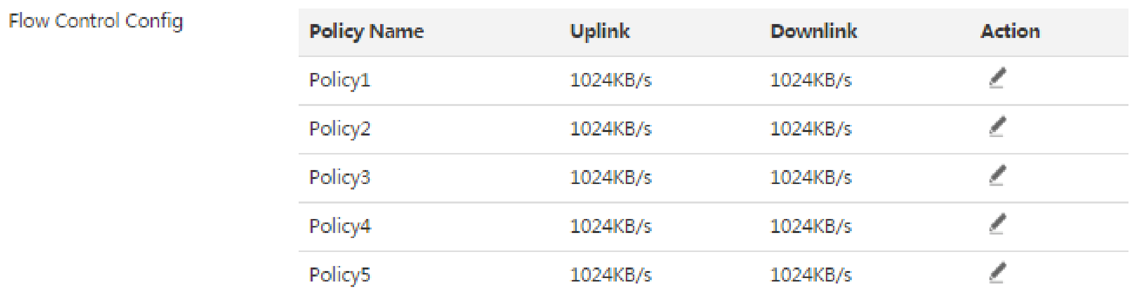
4. To modify the information about a host, click ✎ corresponding to the host and modify the information.

5. To delete a host, click 🗑 corresponding to the host.

6. To delete multiple hosts at the same time, select them and click 🗑 Delete .

Configuring flow control polices

The router can implement flow control policies to 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.



Flow Control Config

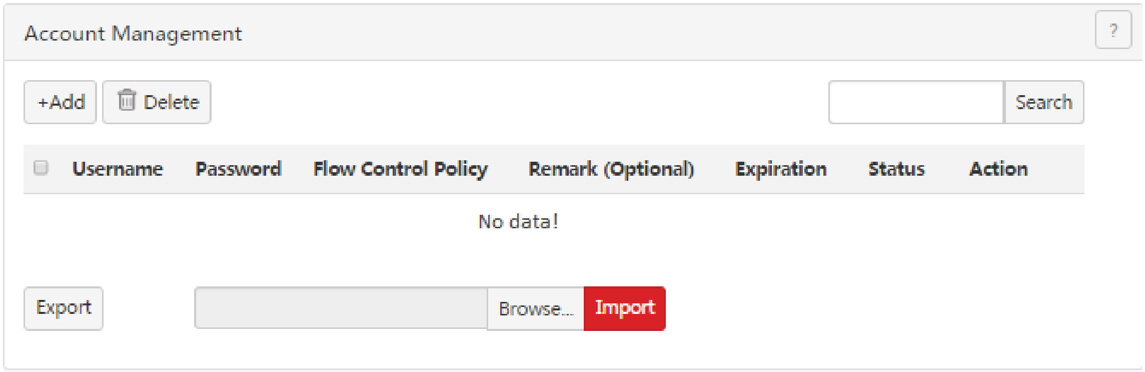
Policy Name	Uplink	Downlink	Action
Policy1	1024KB/s	1024KB/s	✎
Policy2	1024KB/s	1024KB/s	✎
Policy3	1024KB/s	1024KB/s	✎
Policy4	1024KB/s	1024KB/s	✎
Policy5	1024KB/s	1024KB/s	✎

The following table describes the parameters.

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.
Uplink and Downlink	**Uplink** specifies the maximum uplink throughputs for policies. **Downlink** 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.
Action	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.

11.2.2 Managing accounts

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.



Account Management

□	Username	Password	Flow Control Policy	Remark (Optional)	Expiration	Status	Action

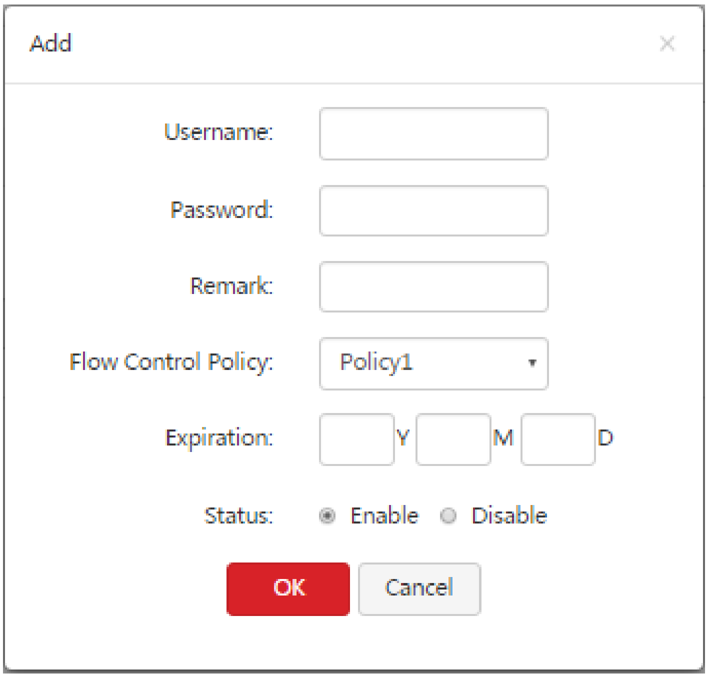
No data!

Adding an account

1. Choose **PPPoE Authentication** > **Account Management**.

2. Click +Add.

   The **Add** dialog box appears.



Add ×

Username:

Password:

Remark:

Flow Control Policy: Policy1

Expiration: Y M D

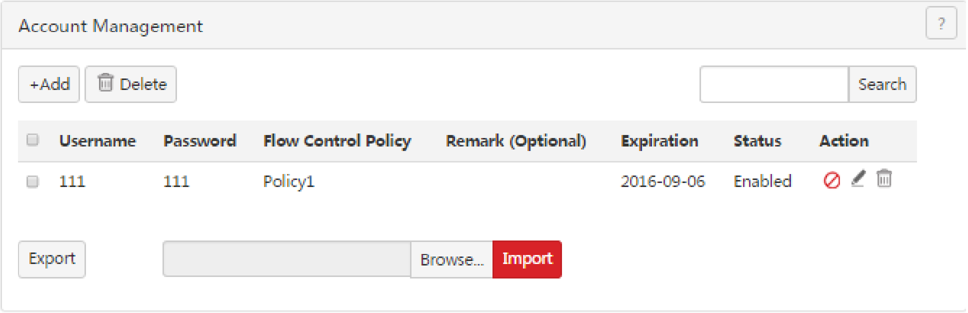
Status: ● Enable ○ Disable

The following table describes the parameters.

Parameter	Description
Username Password	**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.
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 Config** area on the **PPPoE Authentication** > **Basic Setup** 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.

3. Set the parameters and click **OK**.

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



Account Management

□	Username	Password	Flow Control Policy	Remark (Optional)	Expiration	Status	Action
□	111	111	Policy1		2016-09-06	Enabled	⊘ ✎ 🗑

Modifying an account

1. Choose **PPPoE Authentication** > **Account Management**.
2. Click ✎ corresponding to an account to be modified.
3. Modify the account.
4. To disable an account, click ⊘ corresponding to the account.
5. To enable an account, click ✓ corresponding to the account.

Deleting an account

1. Choose **PPPoE Authentication** > **Account Management**.
2. Click 🗑 corresponding to an account to be deleted.

   The account is deleted.
3. 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** > **Account 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** > **Account Management**.
2. Click Browse..., select the **pppoe_user.cfg** file, and click Import.

11.3 Example of configuring PPPoE authentication

Network Requirement

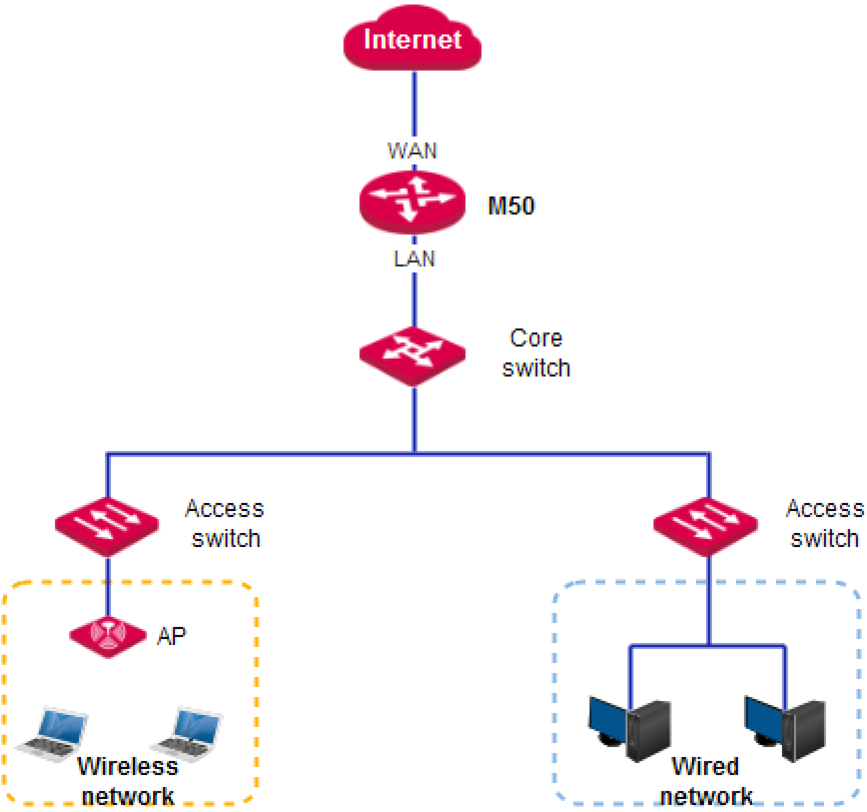
The ISP of a residential estate uses M50 to offer internet accessibility to a building to address the following requirement:

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.

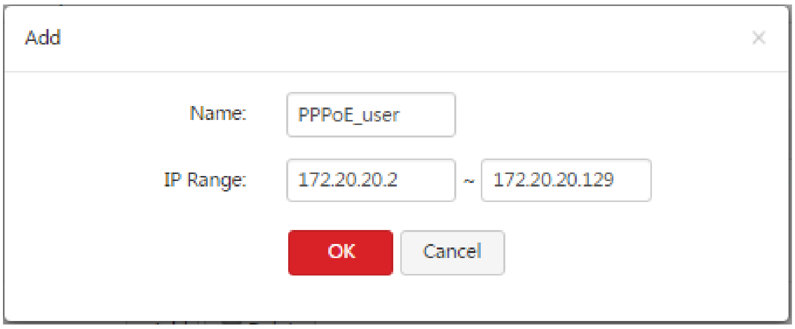


Configuration Procedure

Note

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

If an IP address group has been added for the router, add all the IP addresses in the IP address pool of the PPPoE server to the group (see the following figure). Otherwise, the internet may not be accessible after PPPoE dial-up connections are set up.



Name: PPPoE_user

IP Range: 172.20.20.2 ~ 172.20.20.129

I. Configure basic settings for PPPoE authentication.

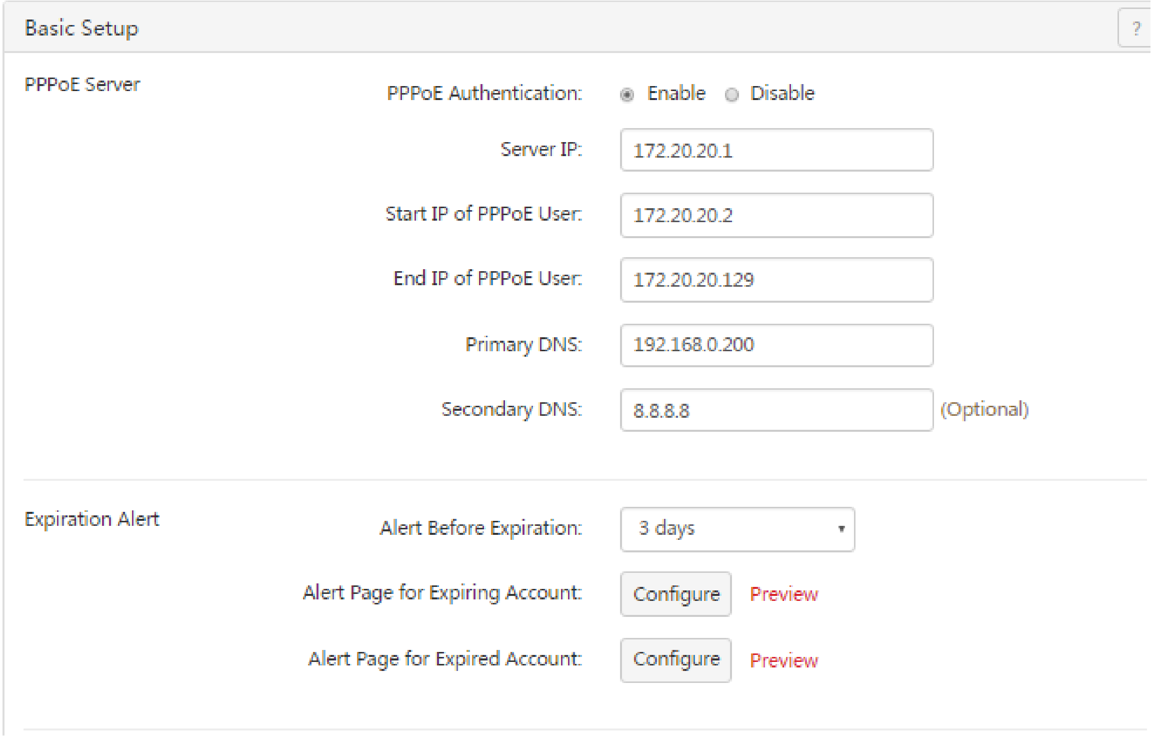
Choose **PPPoE Authentication** > **Basic Setup** and perform the following steps:

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

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

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

(3) Click **OK**.



Basic Setup

PPPoE Server

PPPoE Authentication: ● Enable ○ Disable

Server IP: 172.20.20.1

Start IP of PPPoE User: 172.20.20.2

End IP of PPPoE User: 172.20.20.129

Primary DNS: 192.168.0.200

Secondary DNS: 8.8.8.8 (Optional)

Expiration Alert

Alert Before Expiration: 3 days

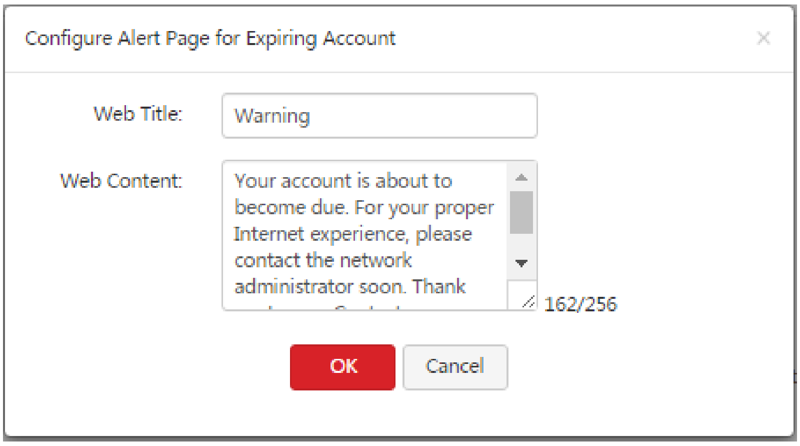
Alert Page for Expiring Account: Configure Preview

Alert Page for Expired Account: Configure Preview

2. Configure the account expiration alert pages.

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

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



Configure Alert Page for Expiring Account

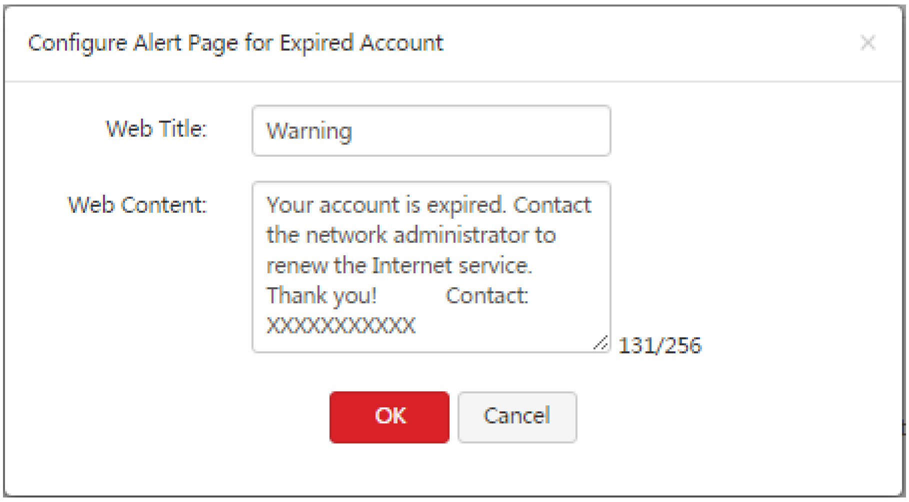
Web Title: Warning

Web Content: Your account is about to become due. For your proper Internet experience, please contact the network administrator soon. Thank

162/256

OK Cancel

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



Configure Alert Page for Expired Account ×

Web Title: Warning

Web Content: Your account is expired. Contact the network administrator to renew the Internet service. Thank you! Contact: XXXXXXXXXXX

131/256

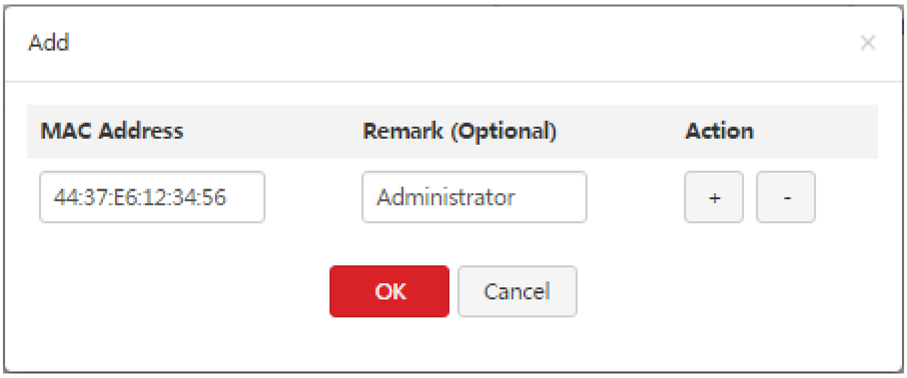
3. Add authentication-free hosts.

In the **Authentication-free** area, click +Add. The **Add** dialog box appears. Perform the following steps:

(1) 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.

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

(3) Click **OK**.

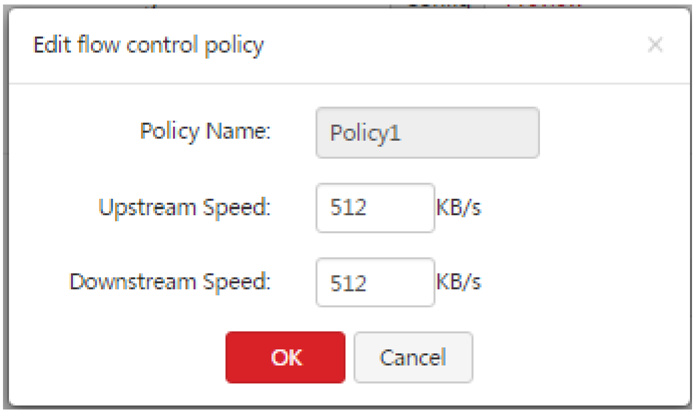


Add ×

MAC Address	Remark (Optional)	Action
44:37:E6:12:34:56	Administrator	+ -

4. Configure flow control policies.

In the **Flow Control Config** 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.



Edit flow control policy ×

Policy Name: Policy1

Upstream Speed: 512 KB/s

Downstream Speed: 512 KB/s

II. Add PPPoE accounts.

Choose **PPPoE Authentication** > **Account Management** and click +Add. The **Add** dialog box appears. Perform the following steps:

(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.

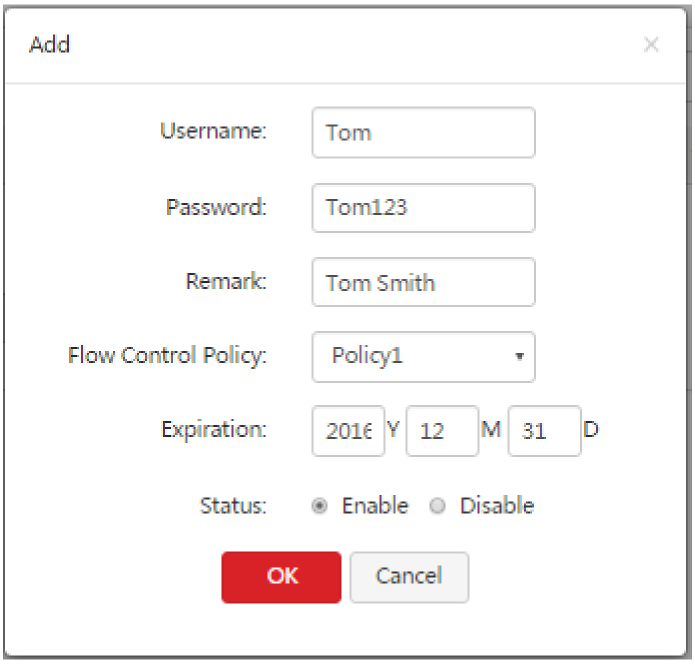
(3) Set **Remark** to the description of the user Tom, which is **Tom Smith** in this example. You can leave this parameter blank.

(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**.



Add

Username: Tom

Password: Tom123

Remark: Tom Smith

Flow Control Policy: Policy1

Expiration: 2016 Y 12 M 31 D

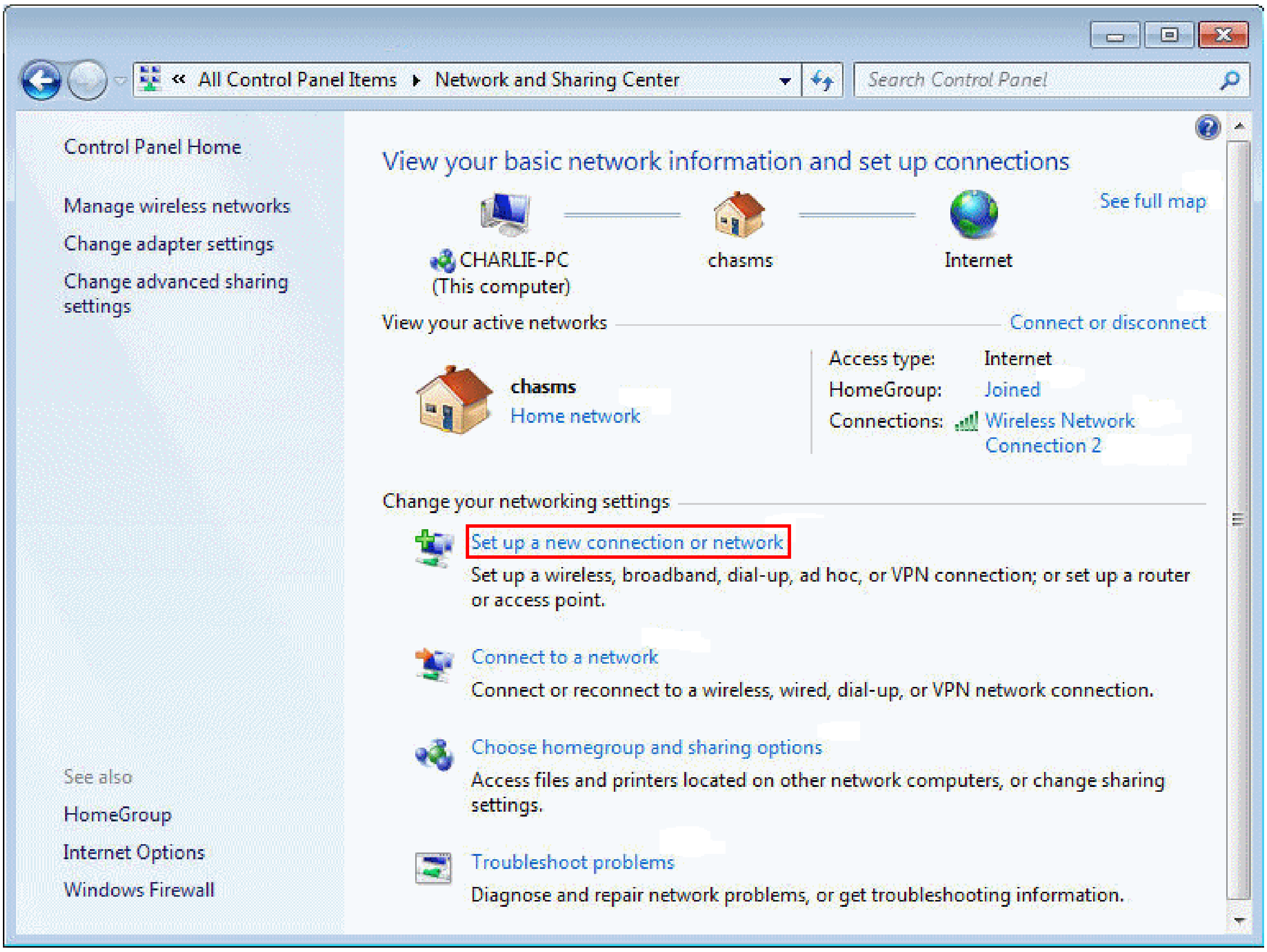
Status: ● Enable ○ Disable

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.
2. Click **Control Panel**. Click **Network and internet**. Click **Network and Sharing Center**. Click **Set up a new connection or network**.



Control Panel Home

Manage wireless networks

Change adapter settings

Change advanced sharing settings

See also

HomeGroup

Internet Options

Windows Firewall

View your basic network information and set up connections

CHARLIE-PC (This computer) — chasms — Internet

See full map

View your active networks

Connect or disconnect

chasms
Home network

Access type: Internet

HomeGroup: Joined

Connections: Wireless Network Connection 2

Change your networking settings

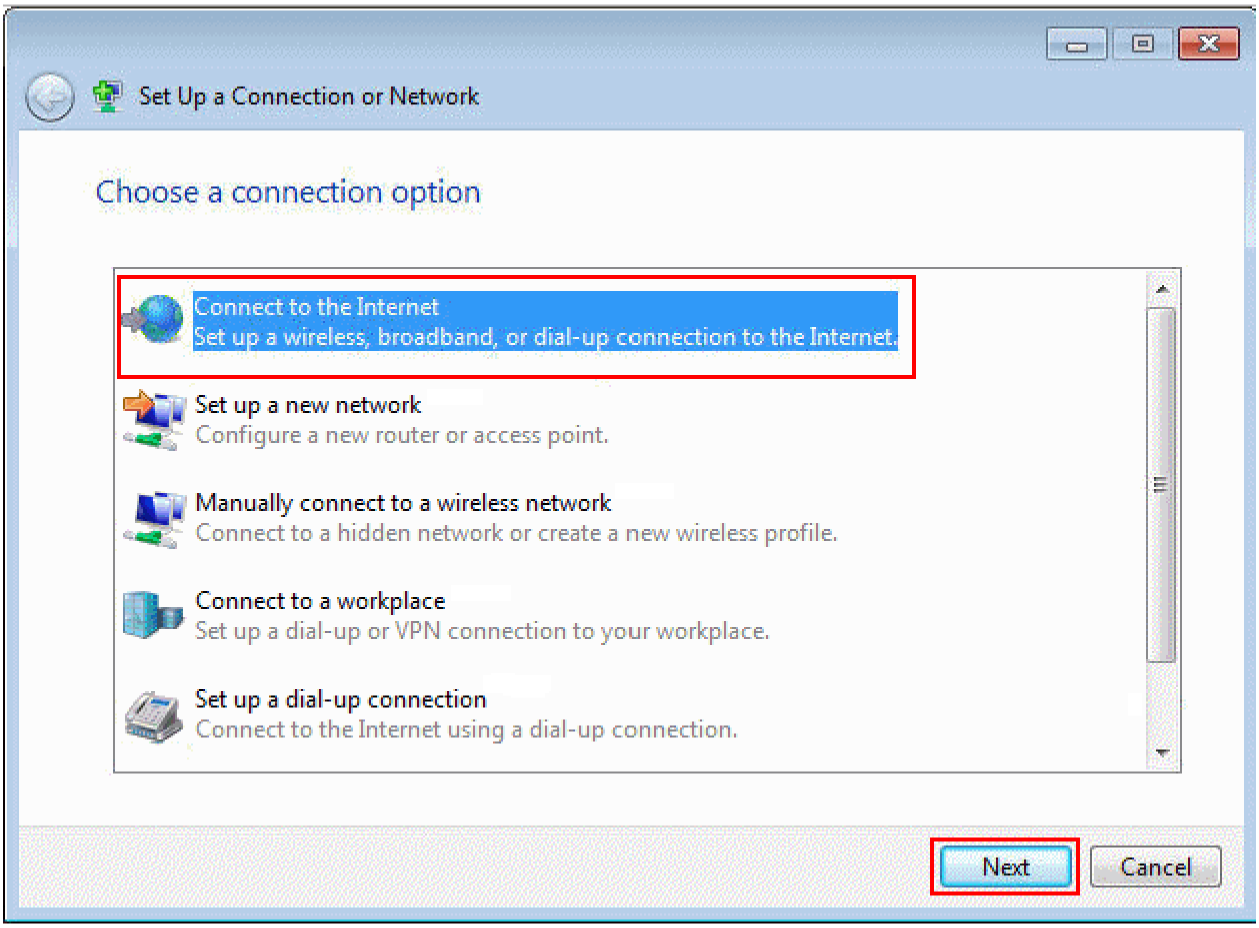
Set up a new connection or network
Set up a wireless, broadband, dial-up, ad hoc, or VPN connection; or set up a router or access point.

Connect to a network
Connect or reconnect to a wireless, wired, dial-up, or VPN network connection.

Choose homegroup and sharing options
Access files and printers located on other network computers, or change sharing settings.

Troubleshoot problems
Diagnose and repair network problems, or get troubleshooting information.

3. Click **Connect to the Internet** and click **Next**.



Set Up a Connection or Network

Choose a connection option

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

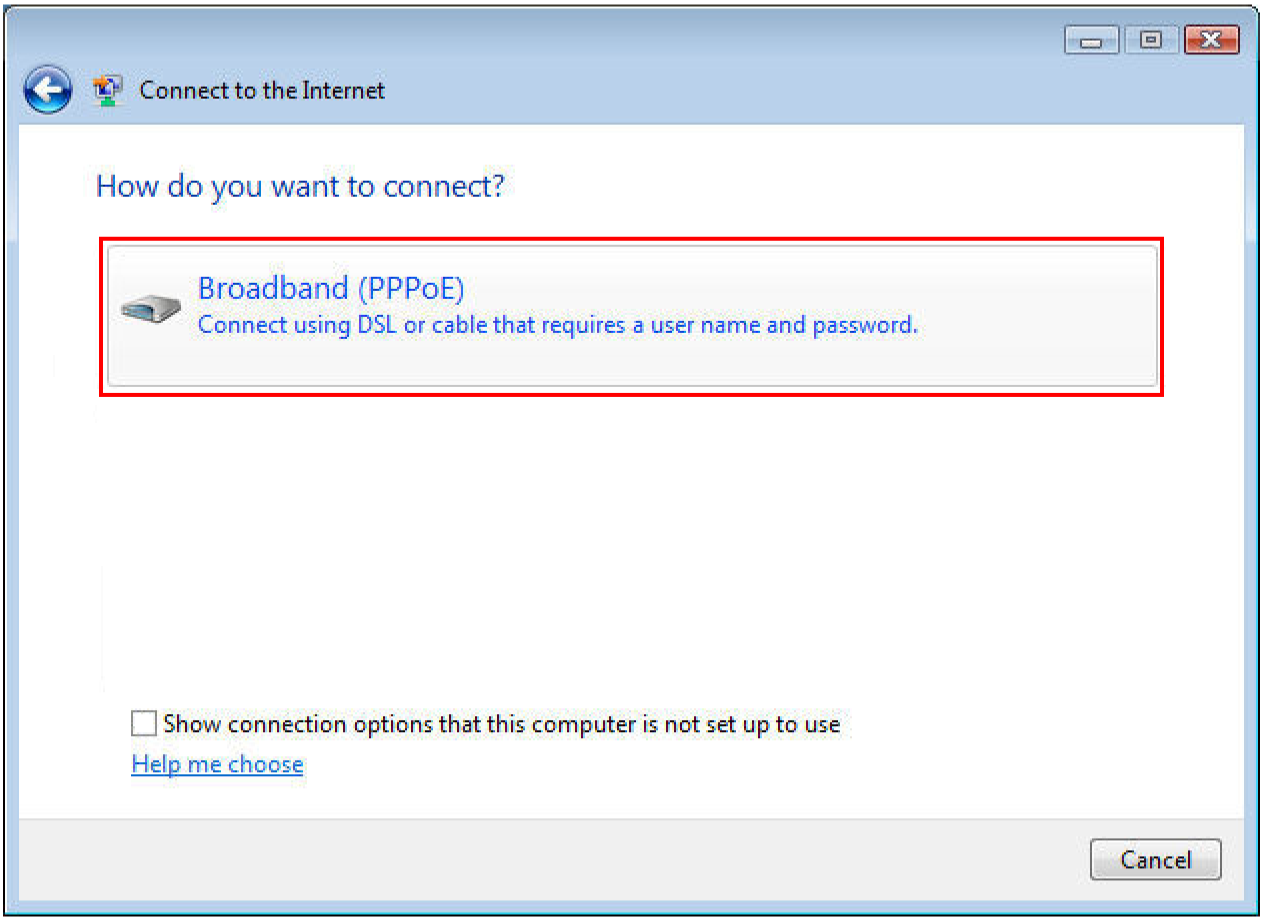
Set up a new network
Configure a new router or access point.

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

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

Set up a dial-up connection
Connect to the Internet using a dial-up connection.

4. Click **Broadband (PPPoE)**.



Connect to the Internet

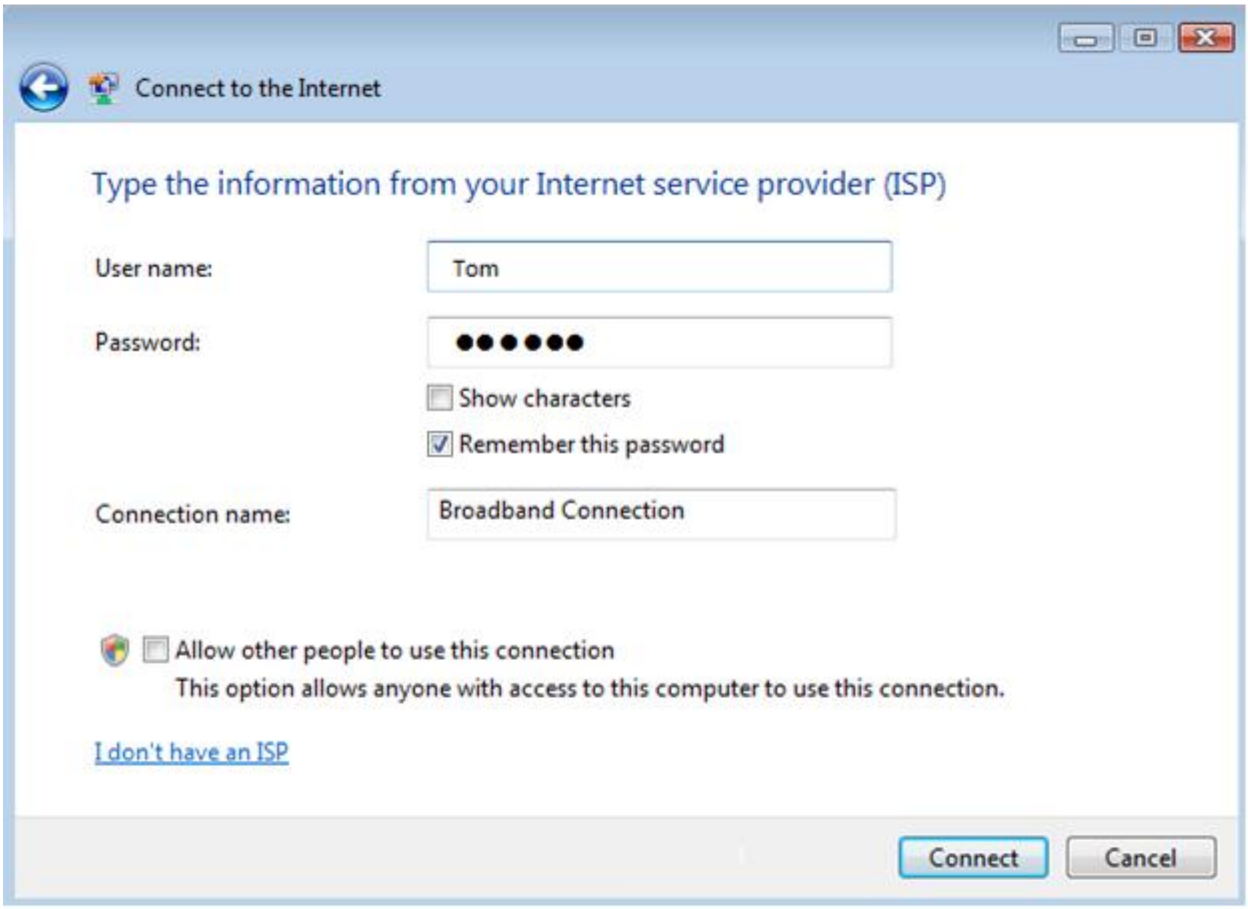
How do you want to connect?

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

□ Show connection options that this computer is not set up to use

Help me choose

5. 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** and click **Connect**.



Connect to the Internet

Type the information from your Internet service provider (ISP)

User name: Tom

Password: ●●●●●●

□ Show characters

☑ Remember this password

Connection name: Broadband Connection

□ Allow other people to use this connection
This option allows anyone with access to this computer to use this connection.

I don't have an ISP

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.

Chapter 12 Virtual server

12.1 Overview

This chapter describes:

- Port forwarding
- UPnP
- DMZ host
- DDNS

12.1.1 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.

12.1.2 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 AynChart, and helps to increase the download speed.

12.1.3 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.

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.

12.1.4 DDNS

DDNS is short for Dynamic Domain Name Server. 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.

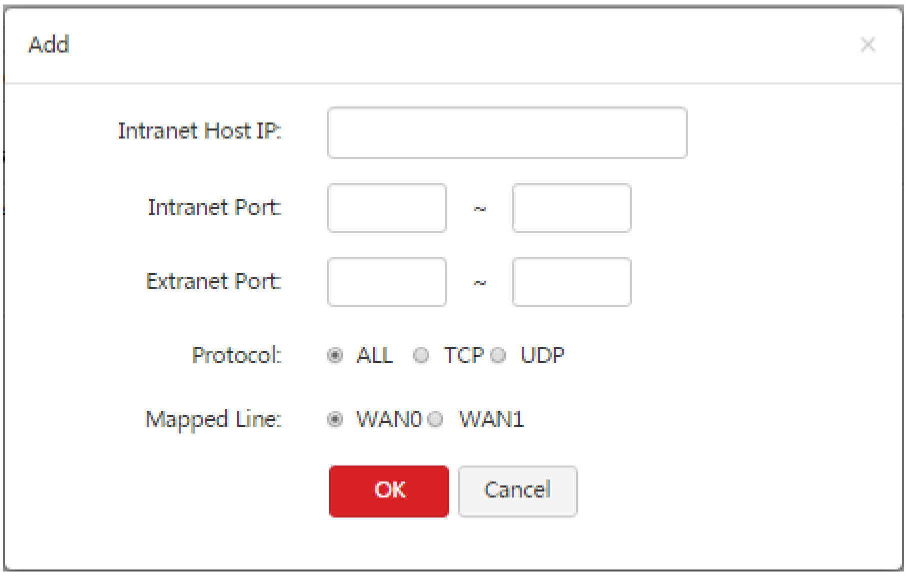
This function always interworks with other functions, such as Port Forwarding, DMZ Host and Remote Web Management.

12.2 Port forwarding

12.2.1 Configuring port forwarding

Adding a rule

1. Choose **Virtual Server** > **Port Forwarding**.
2. Click **Add**.
   The **Add** window appears.
3. Set the parameters and click **OK**.



Add ×

Intranet Host IP:

Intranet Port: ~

Extranet Port: ~

Protocol: ● ALL ○ TCP ○ UDP

Mapped Line: ● WAN0 ○ WAN1

The **Port Forwarding** appears, showing the added rule.

The following table describes the parameters.

Parameter	Description
Intranet Host IP	It specifies the IP address of a local computer that runs a specified service.
Intranet Port	It specifies the service port of a server on a local computer.
Extranet 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**.
Mapped Line	It specifies the physical WAN port that internet users use to access the specified service. For example, if you select **WAN0**, the service address is *protocol*://*WAN0 IP address*:*port*.

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.

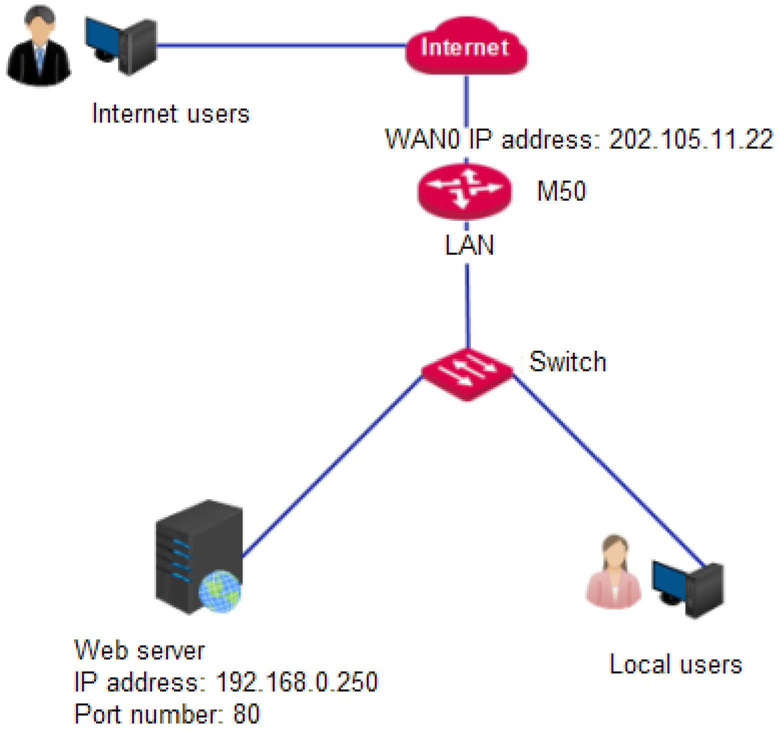
12.2.2 Example of port forwarding

Networking requirement

An enterprise uses M50 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.

Network topology



Configuration Procedure

1. Choose **Virtual Server** > **Port Forwarding**.

2. Click **Add**.

3. Set **Intranet Host IP** to **192.168.0.250**.

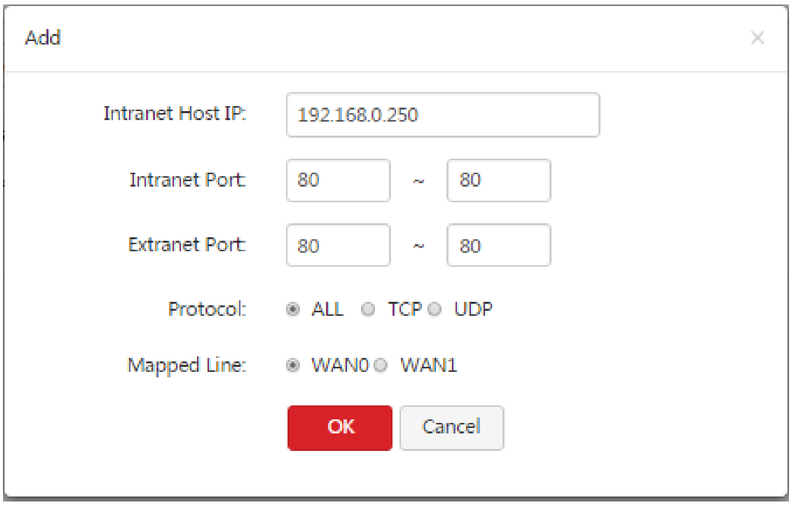
4. Set **Intranet Port** to **80**.

5. Set **Extranet Port** to **80**.

6. Set **Protocol** to **TCP** or **ALL**.

7. Set **Mapped Line** to **WAN0**.

8. Click **OK**.



Add

Intranet Host IP: 192.168.0.250

Intranet Port: 80 ~ 80

Extranet Port: 80 ~ 80

Protocol: ● ALL ○ TCP ○ UDP

Mapped Line: ● WAN0 ○ WAN1

Verification

Internet users can access the local web server at http://202.105.11.22.

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 http://ip-com.ddns.net.

Tip

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

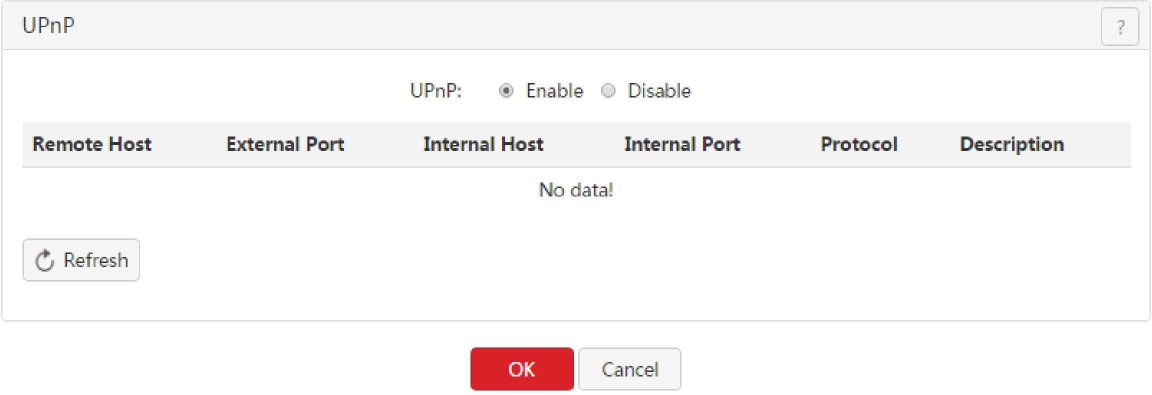
- Make sure that the WAN IP address of the router is a public IP address.
- Make sure that the intranet port number is the service port number on the local host. In this example, it is 80.
- Disable some programs, such as the firewall, anti-virus software, and security guard, which may forbid internet 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.

12.3 UPnP

To enable the function:

1. Choose **Virtual Server** > **UPnP**.

2. Select **Enable** and click **OK**.



UPnP

UPnP: ● Enable ○ Disable

Remote Host	External Port	Internal Host	Internal Port	Protocol	Description
No data!					

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

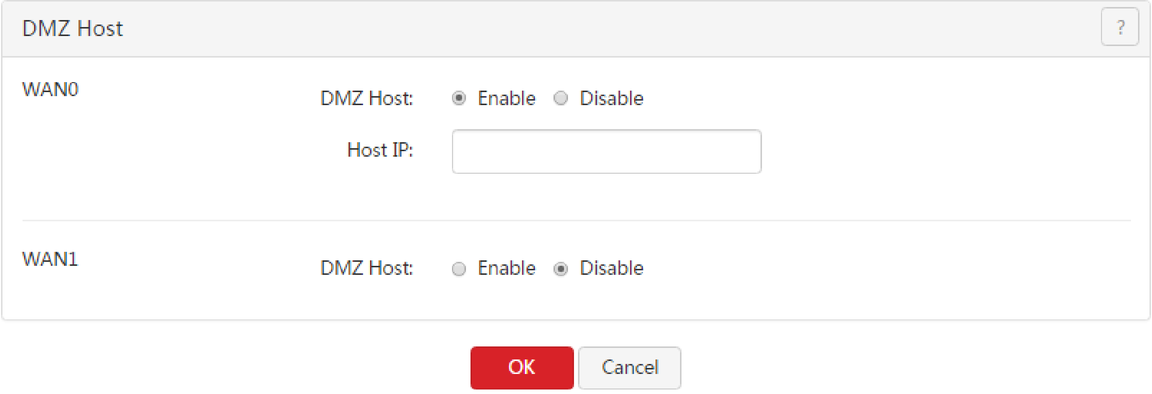
12.4 DMZ host

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.

12.4.1 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**.



DMZ Host

WAN0

DMZ Host: ● Enable ○ Disable

Host IP:

WAN1

DMZ Host: ○ Enable ● Disable

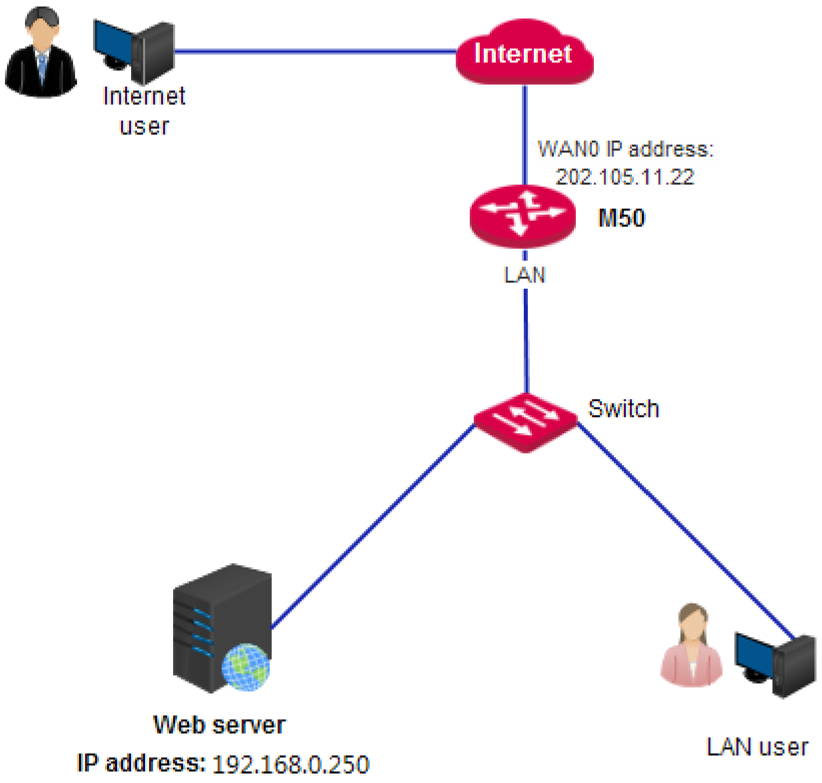
12.4.2 Example of configuring the DMZ host function

Networking requirement

An enterprise uses M50 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.

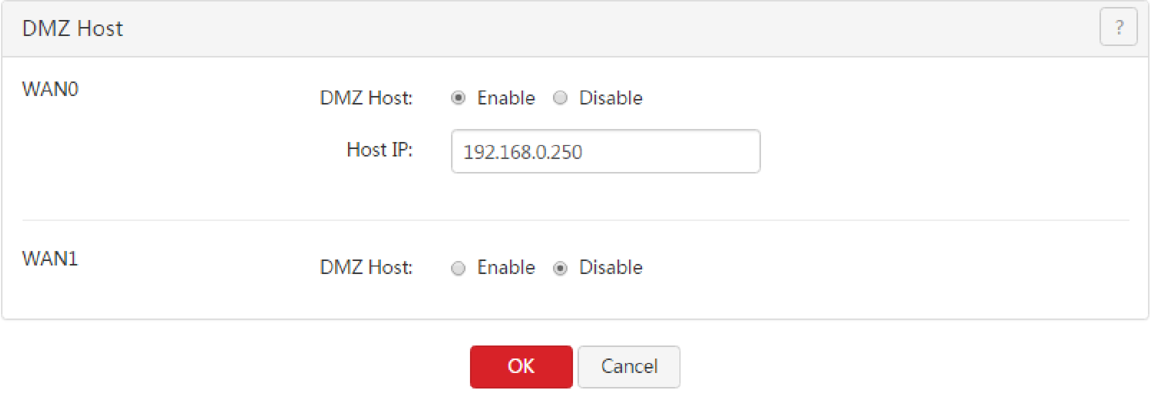
You can use the DMZ function to meet this requirement.

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**.



DMZ Host

WAN0

DMZ Host: ● Enable ○ Disable

Host IP: 192.168.0.250

WAN1

DMZ Host: ○ Enable ● Disable

Verification

Internet users can access the local web server at http://202.105.11.22.

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 http://ip-com.ddns.net.

Tip

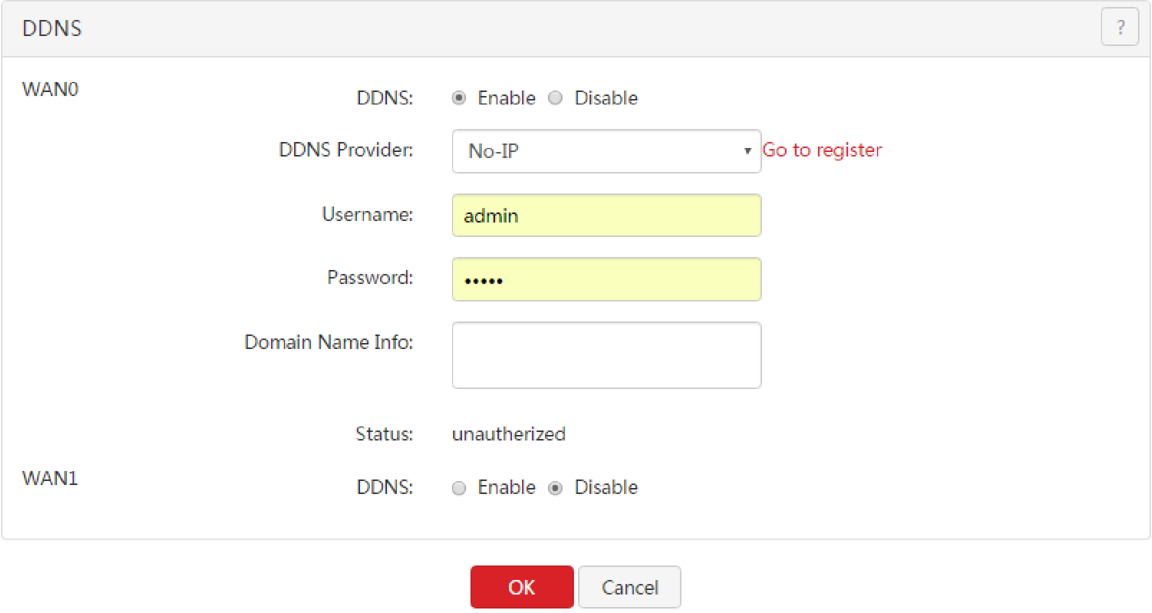
If you cannot access the web server, try the following methods to resolve the problem:

- 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.

12.5 DDNS

12.5.1 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**.



DDNS

WAN0

DDNS: ● Enable ○ Disable

DDNS Provider: No-IP

Username: admin

Password: •••••

Domain Name Info:

Status: unautherized

WAN1

DDNS: ○ Enable ● Disable

The following table describes the parameters.

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 3322.org, 88ip.cn, oray.com, gnway.com, DynDNS and No-IP DDNS providers.
Provider link	**Provider link** specifies the link to the website of a DDNS provider.

Parameter	Description
Service Type	**Service Type** specifies the type of the service provided by a DDNS provider. These two parameters are effective only for oray.com. You can click the link to learn more about the DDNS provider.
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	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.
Status	It indicates whether the router is connected to a DDNS provider.

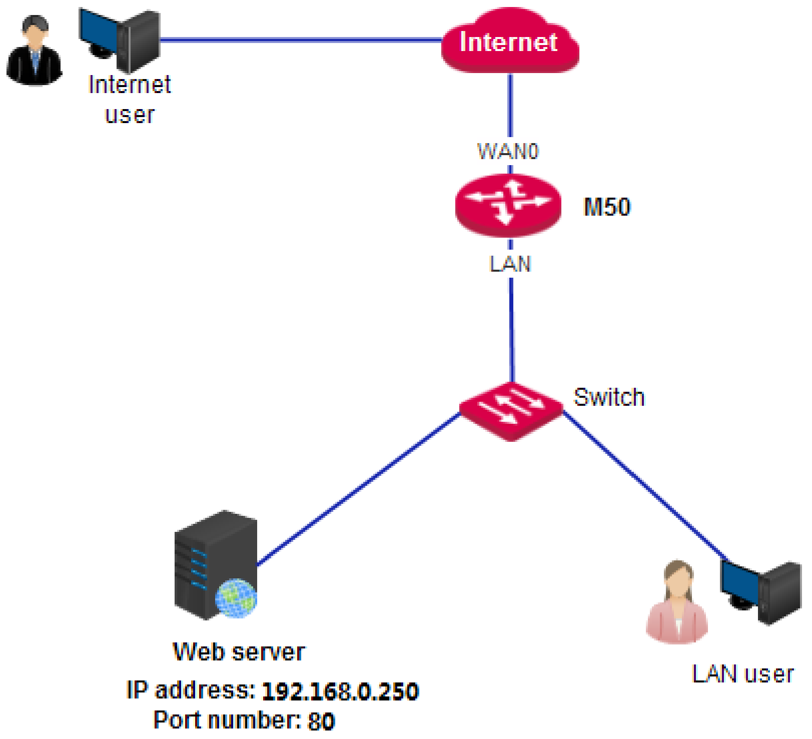
12.5.2 Example of configuring the DDNS function

Networking requirement

An enterprise uses M50 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. 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.

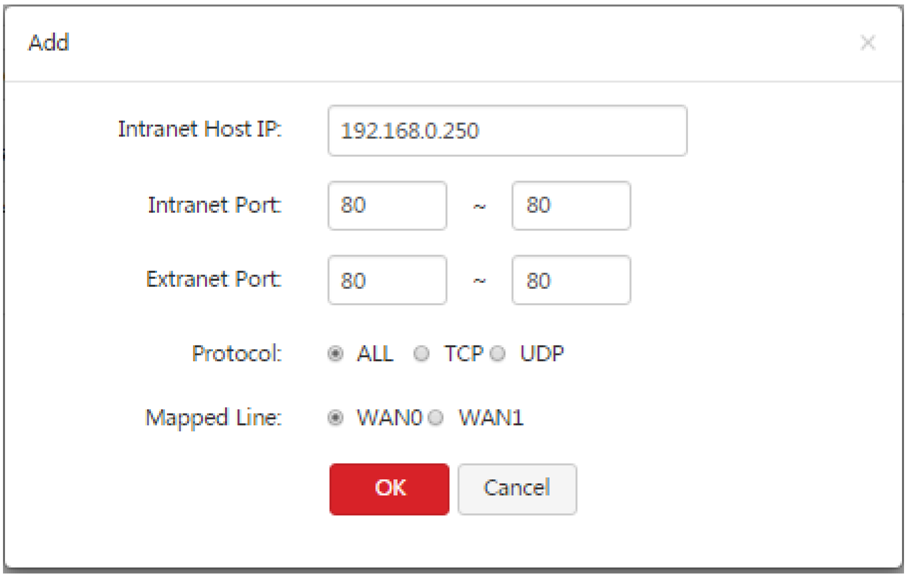
Network topology



Configuration Procedure

I. Configure the port forwarding function.

1. Choose **Virtual Server** > **Port Forwarding**.
2. Click **Add**.
3. Set **Intranet Host IP** to **192.168.0.250**.
4. Set **Intranet Port** to **80**.
5. Set **Extranet Port** to **80**.
6. Set **Protocol** to **TCP** or **ALL**.
7. Set **Mapped Line** to **WAN0**.
8. Click **OK**.



Add

Intranet Host IP: 192.168.0.250

Intranet Port: 80 ~ 80

Extranet Port: 80 ~ 80

Protocol: ● ALL ○ TCP ○ UDP

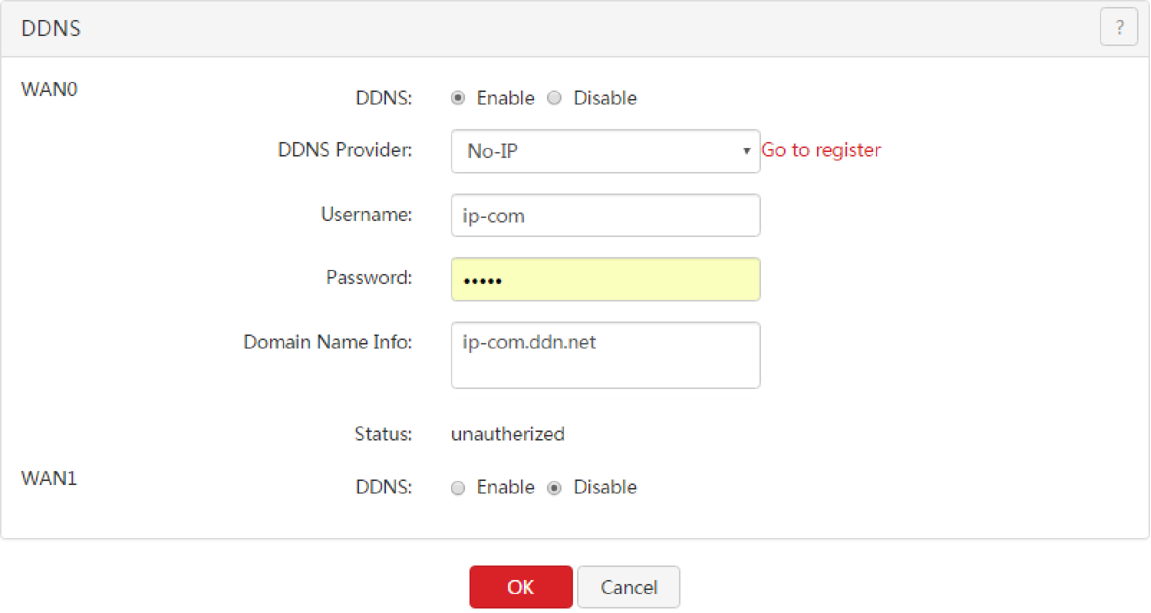
Mapped Line: ● WAN0 ○ WAN1

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. Choose **Virtual Server** > **DDNS**.
5. Set **Username** to **ip-com**.
6. Set **Password** to **123456**.
7. Set **Domain Name Info** to **ip-com.ddns.net**.
8. Click **OK**.



DDNS

WAN0

DDNS: ● Enable ○ Disable

DDNS Provider: No-IP

Username: ip-com

Password: •••••

Domain Name Info: ip-com.ddn.net

Status: unautherized

WAN1

DDNS: ○ Enable ● Disable

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

Verification

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

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.

Chapter 13 Maintenance

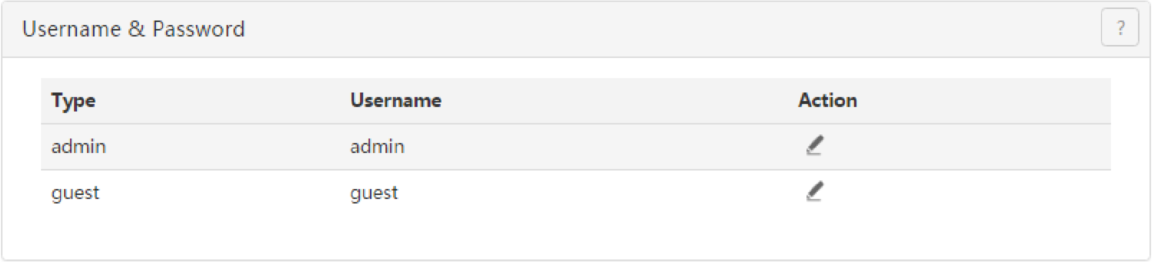
This chapter describes:

- Setting user names and passwords
- Rebooting the router
- Backing up and restoring configuration
- Upgrading the firmware
- Restoring the factory settings
- Setting the system date and time
- Remotly managing the router using the web UI

13.1 Setting user names and passwords

To access the page for changing the login user name or password of the router, choose **Maintenance** > **Username & Password**.

The router supports two login accounts: admin and guest. Both the default login user name and password of the **admin** account are **admin**. Both the default login user name and password of the **guest** account are **guest**.



Username & Password

Type	Username	Action
admin	admin	✎
guest	guest	✎

The following table describes the parameters.

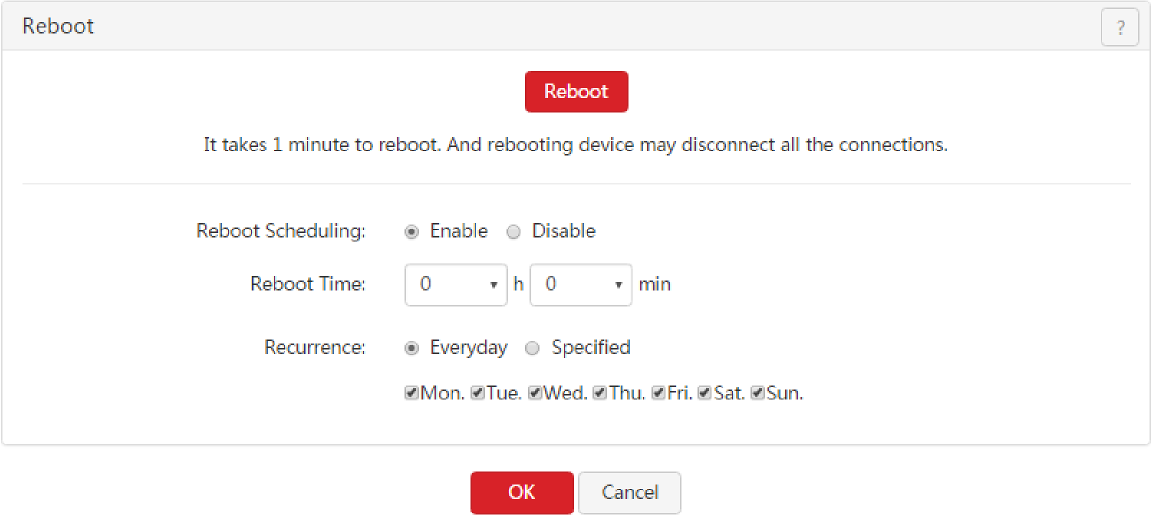
Parameter	Description
Type	It specifies the type of a router account. The options include: ● **admin**: It indicates the account used to view and modify the configuration of the router. ● **guest**: It indicates the account used only to view the configuration of the router.
Username	It specifies a login user name.
Action	It allows you to change a login user name or password. To change a login user name or password, click ✎ .

13.2 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 scheduling function to ensure the performance and stability of the router.



It takes 1 minute to reboot. And rebooting device may disconnect all the connections.

Reboot Scheduling: ● Enable ○ Disable

Reboot Time: 0 h 0 min

Recurrence: ● Everyday ○ Specified

☑Mon. ☑Tue. ☑Wed. ☑Thu. ☑Fri. ☑Sat. ☑Sun.

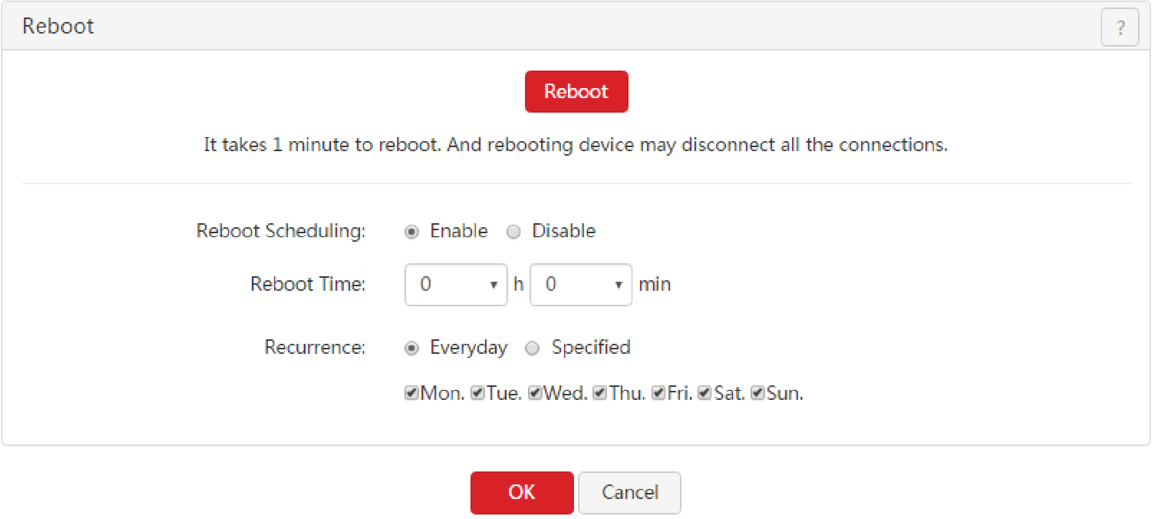
13.2.1 Rebooting the router manually

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

13.2.2 Rebooting the router regularly

1. Choose **Maintenance** > **Reboot**.
2. Set **Reboot Scheduling** to **Enable**.
3. Set **Reboot Time** to a time when the router is rebooted.
4. Set **Recurrence** to some or all weekdays.
5. Click **OK**.

After the configuration is completed, the router reboots as scheduled.



Reboot

It takes 1 minute to reboot. And rebooting device may disconnect all the connections.

Reboot Scheduling: ● Enable ○ Disable

Reboot Time: 0 h 0 min

Recurrence: ● Everyday ○ Specified

☑Mon. ☑Tue. ☑Wed. ☑Thu. ☑Fri. ☑Sat. ☑Sun.

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 date and time.

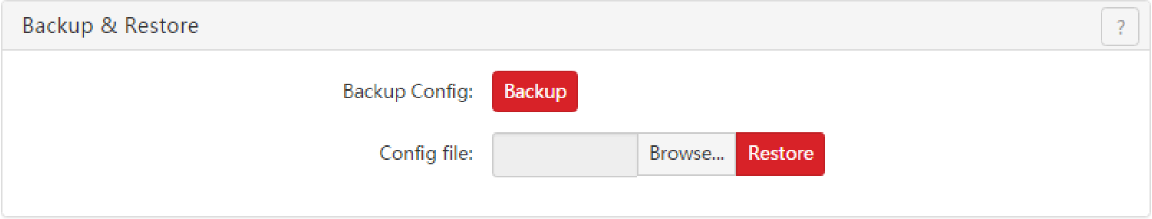
13.3 Backing up and restoring configuration

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.



Backup & Restore

Backup Config:

Config file:

13.3.1 Backing up a configuration

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

13.3.2 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.

13.4 Upgrading the firmware

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

- Local: In this method, you need to download a firmware version of your router and upgrade the firmware 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.

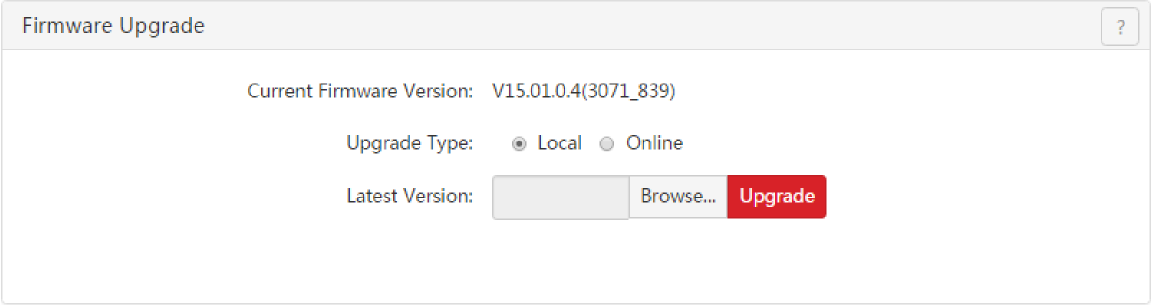
Because an online upgrade is simple, the following section describes only the local upgrade steps.

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 verion of the router to your computer.
2. Choose **Maintenance** > **Firmware Upgrade** on the router web UI.
3. Set **Upgrade Type** to **Local**.
4. Click **Browse** and upload the firmware version of the router.
5. Click **Upgrade** and follow the onscreen instruction to upgrade the firmware.



Firmware Upgrade

Current Firmware Version: V15.01.0.4(3071_839)

Upgrade Type: ● Local ○ Online

Latest Version:

When the upgrading progress is complete, you can log in to the router, go to page **Maintenance** > **Firmware Upgrade** and check the current firmware version.

Tip

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

13.5 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:

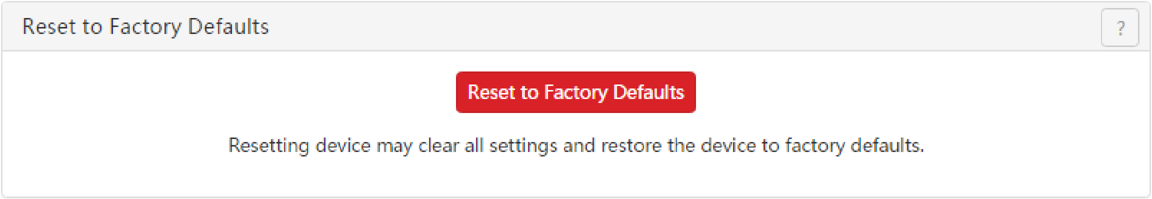
- IP address: 192.168.0.252
- Username: admin
- Password: admin

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.

13.5.1 Resetting the router through web UI

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



Reset to Factory Defaults

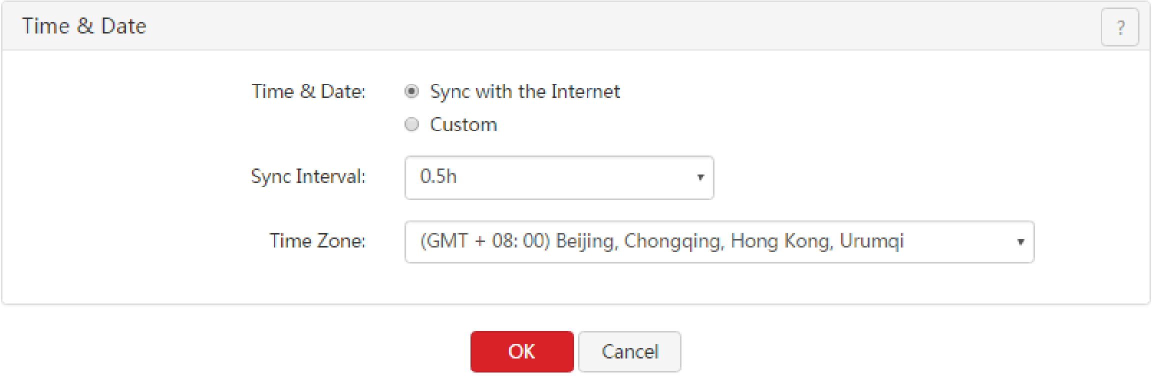
Resetting device may clear all settings and restore the device to factory defaults.

13.5.2 Resetting the router using the RESET button

After the router is powered on, use a needle to hold down the RESET button for 8 seconds. Wait about 45 seconds for the router to restore the factory settings.

13.6 Setting the system date and 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.



Time & Date

Time & Date: ● Sync with the Internet ○ Custom

Sync Interval: 0.5h

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

13.6.1 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 route is connected to the internet, the system time is correct, even after the router reboots.

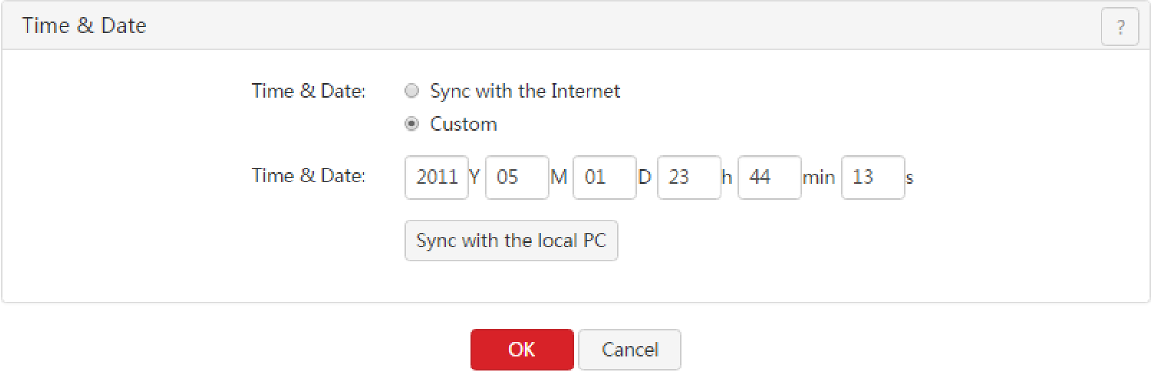
The following table describes the parameters.

Parameter	Description
Sync 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** > **System Info** > **System Info** and check whether the system time is correct.

13.6.2 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.



Time & Date

Time & Date: ○ Sync with the Internet ● Custom

Time & Date: 2011 Y 05 M 01 D 23 h 44 min 13 s

The following table describes the parameters.

Parameter	Description
Time & Date	It specifies the system time of the router.
Sync with the local PC	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.

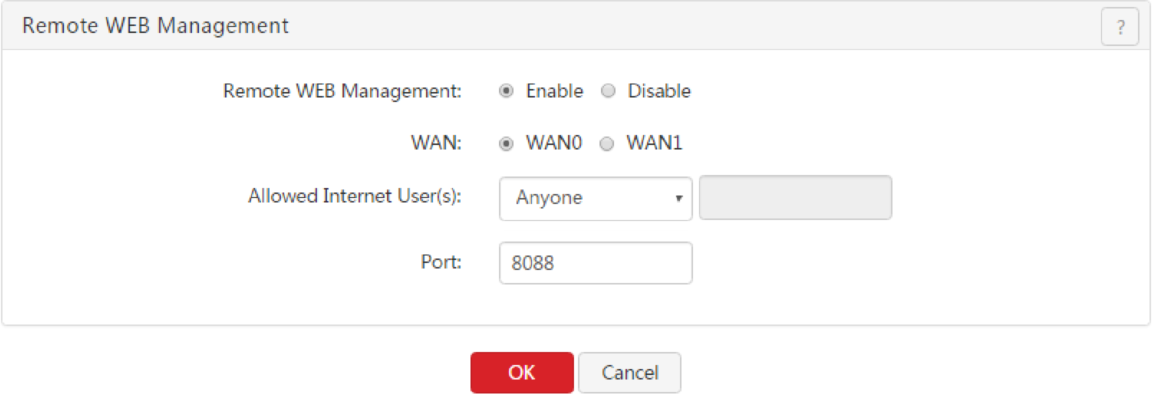
After you finish the configuration, you can choose **System** > **System Info** > **System Info and check** whether the system time is correct.

13.7 Remotly managing the router using the web UI

By default, only local computers that are connected to the router 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.

13.7.1 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 specify an IP address.
5. Set **Port** to a port for accessing the web UI.
6. Click **OK**.



Remote WEB Management

Remote WEB Management: ● Enable ○ Disable

WAN: ● WAN0 ○ WAN1

Allowed Internet User(s): Anyone

Port: 8088

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*.

The following table describes the parameters.

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.

Parameter	Description
	Tip Ports 1 to 1024 are reserved for common services. To avoid port conflicts, it is recommended that you enter a port number from 1025 to 65535.

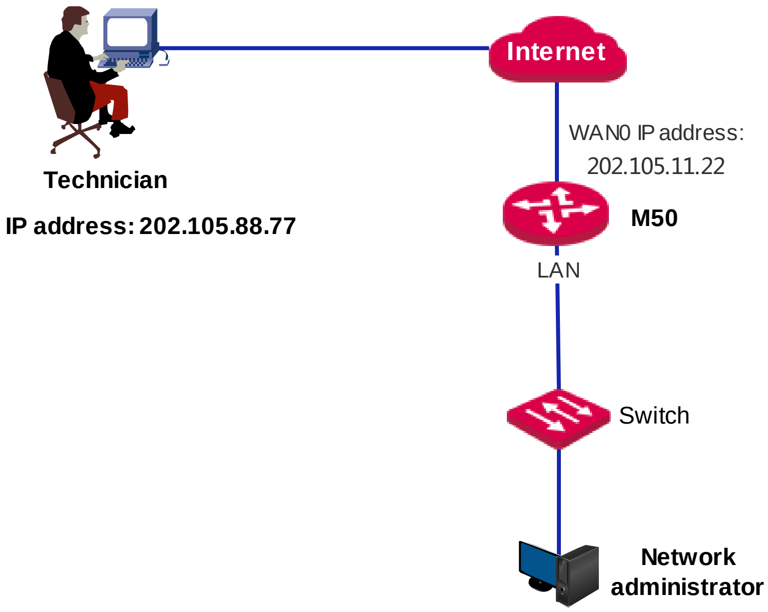
13.7.2 Example of configuring remote web management

Networking requirement

An enterprise uses M50 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**.

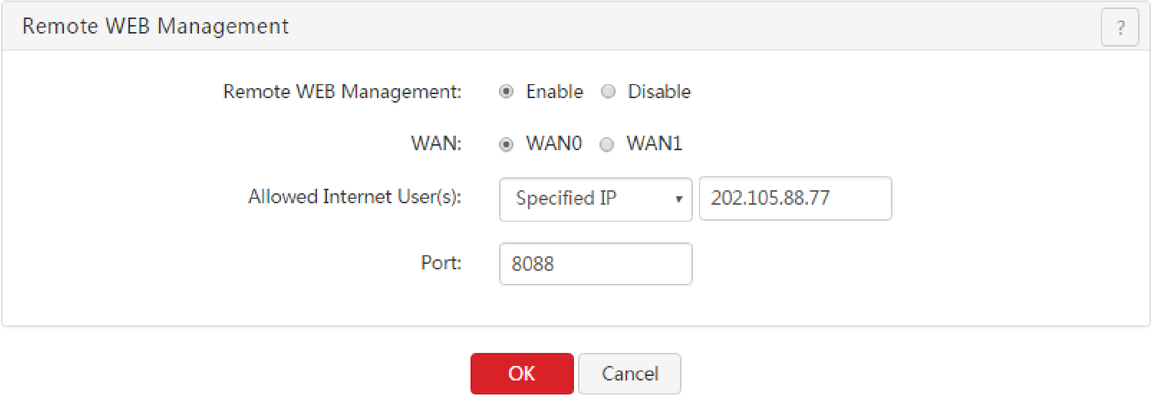
2. Set **Remote WEB Management** to **Enable**.

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**.



Remote WEB Management

Remote WEB Management: ● Enable ○ Disable

WAN: ● WAN0 ○ WAN1

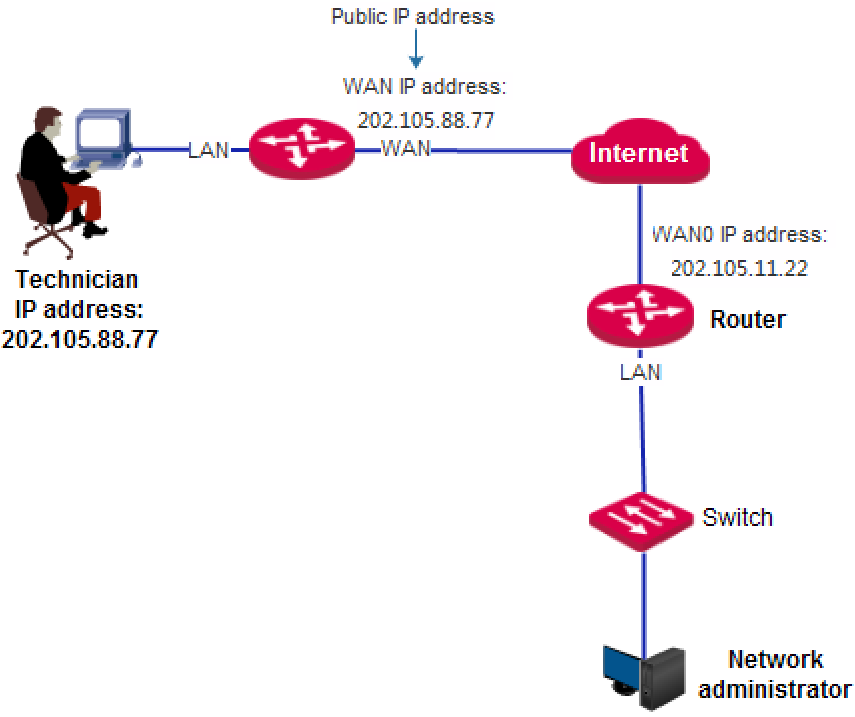
Allowed Internet User(s): Specified IP 202.105.88.77

Port: 8088

Verification

The IP-COM personnel 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 technical personnel to connect to the router. A private IP address is not applicable.



Chapter 14 System

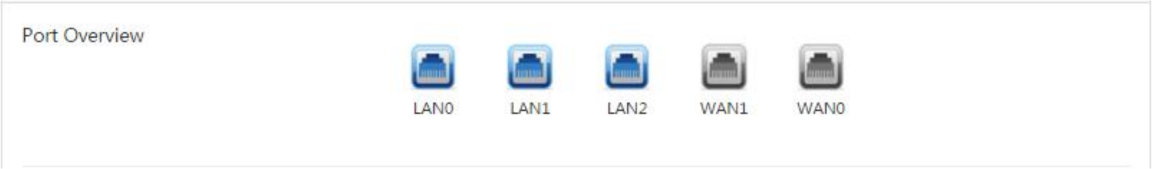
This chapter describes:

- Viewing router information
- Viewing online users
- Viewing traffic statistics
- Viewing defense logs
- Viewing system logs

14.1 Viewing router information

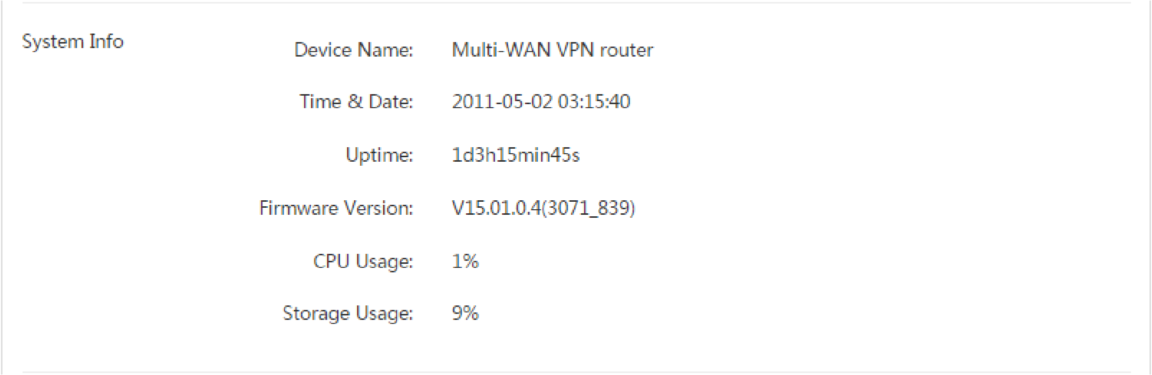
14.1.1 Port overview

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.



14.1.2 System information

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.

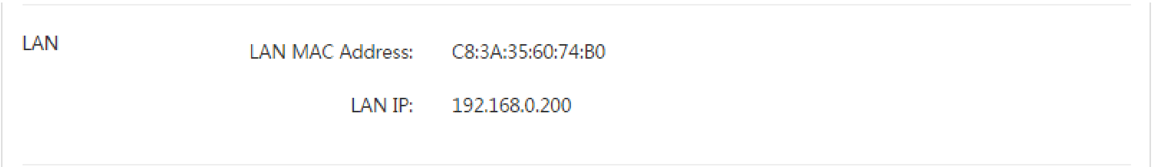


System Info

Device Name:	Multi-WAN VPN router
Time & Date:	2011-05-02 03:15:40
Uptime:	1d3h15min45s
Firmware Version:	V15.01.0.4(3071_839)
CPU Usage:	1%
Storage Usage:	9%

14.1.3 LAN information

In this area, you can check the LAN MAC address and LAN IP address of the router.



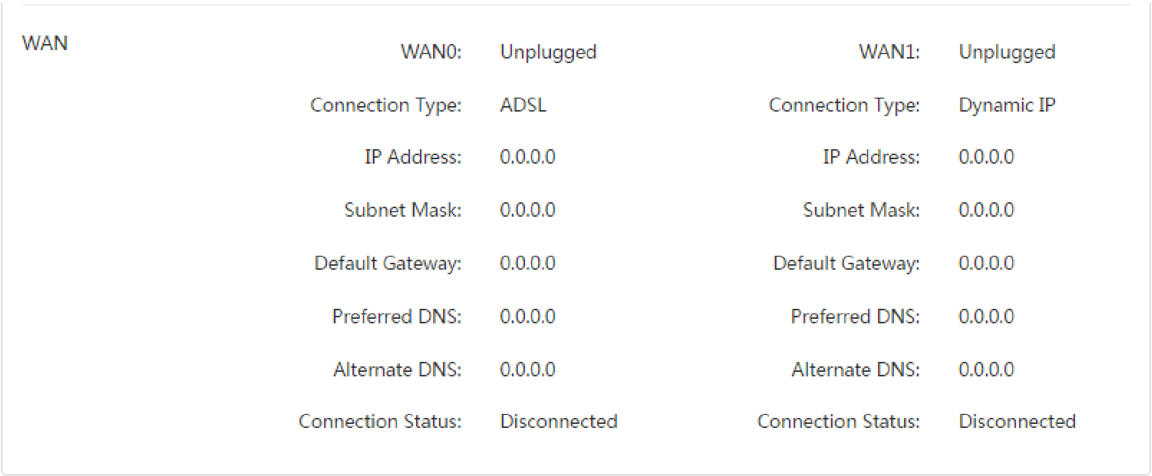
LAN

LAN MAC Address: C8:3A:35:60:74:B0

LAN IP: 192.168.0.200

14.1.4 WAN information

In this area, you can see information about all the WAN ports, including physical connection status, connection types, IP addresses, and so on.



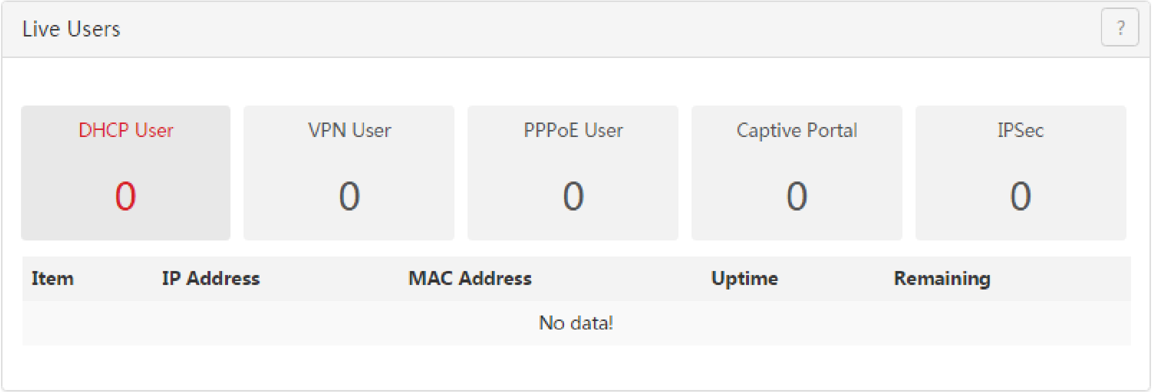
WAN

WAN0:	Unplugged	WAN1:	Unplugged
Connection Type:	ADSL	Connection Type:	Dynamic IP
IP Address:	0.0.0.0	IP Address:	0.0.0.0
Subnet Mask:	0.0.0.0	Subnet Mask:	0.0.0.0
Default Gateway:	0.0.0.0	Default Gateway:	0.0.0.0
Preferred DNS:	0.0.0.0	Preferred DNS:	0.0.0.0
Alternate DNS:	0.0.0.0	Alternate DNS:	0.0.0.0
Connection Status:	Disconnected	Connection Status:	Disconnected

14.2 Viewing online users

14.2.1 DHCP users

To access the page for viewing the information about DHCP clients of the router, choose **System** > **Live Users** > **DHCP User**.



Item	IP Address	MAC Address	Uptime	Remaining
No data!				

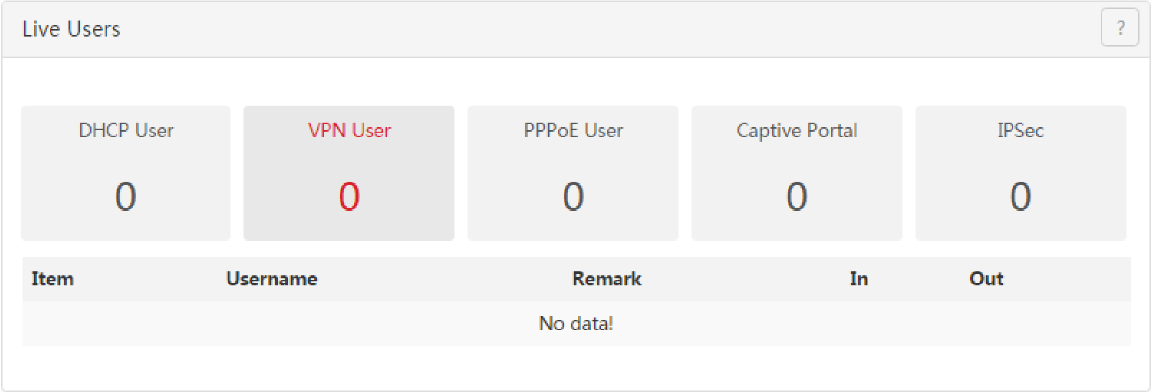
The following table describes the parameters.

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.

Parameter	Description
Uptime	It specifies the connection duration of a DHCP client.
Remaining	It specifies the remaining lease time of an IP address.

14.2.2 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** > **Live Users** > **VPN User**.


Live Users

DHCP User	VPN User	PPPoE User	Captive Portal	IPSec
0	0	0	0	0

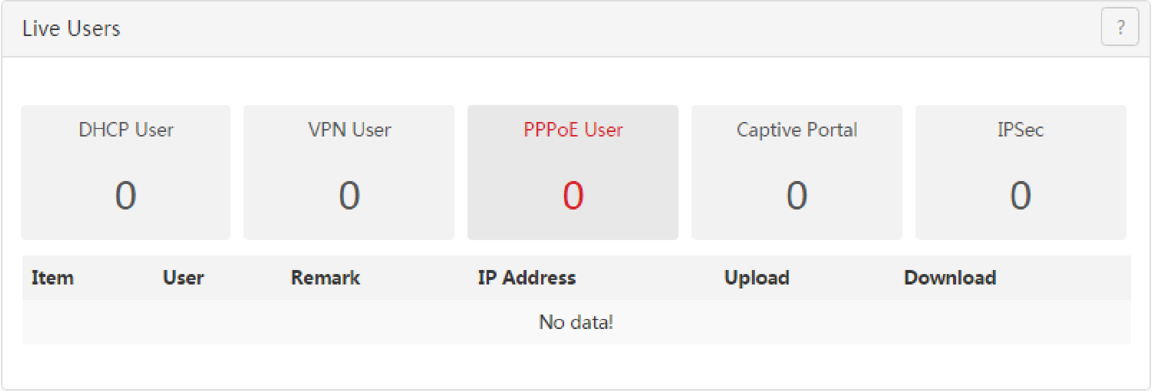
Item	Username	Remark	In	Out
No data!				

The following table describes the parameters.

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.
In	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.
Out	It specifies the IP address of a VPN client that is assigned by the VPN serer of the router.

14.2.3 PPPoE users

To access the page for viewing the information about PPPoE clients after you enable PPPoE authentication, choose **System** > **Live Users** > **PPPoE User**.


Live Users

DHCP User	VPN User	PPPoE User	Captive Portal	IPSec
0	0	0	0	0

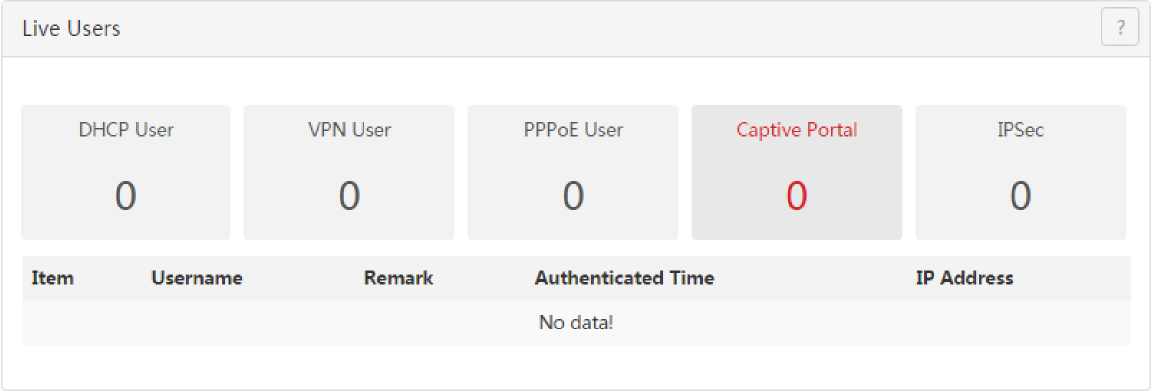
Item	User	Remark	IP Address	Upload	Download
No data!					

The following table describes the parameters.

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.

14.2.4 Captive portal

To access the page for viewing the information about connected clients after you enable the captive portal, choose **System** > **Live Users** > **Captive Portal**.



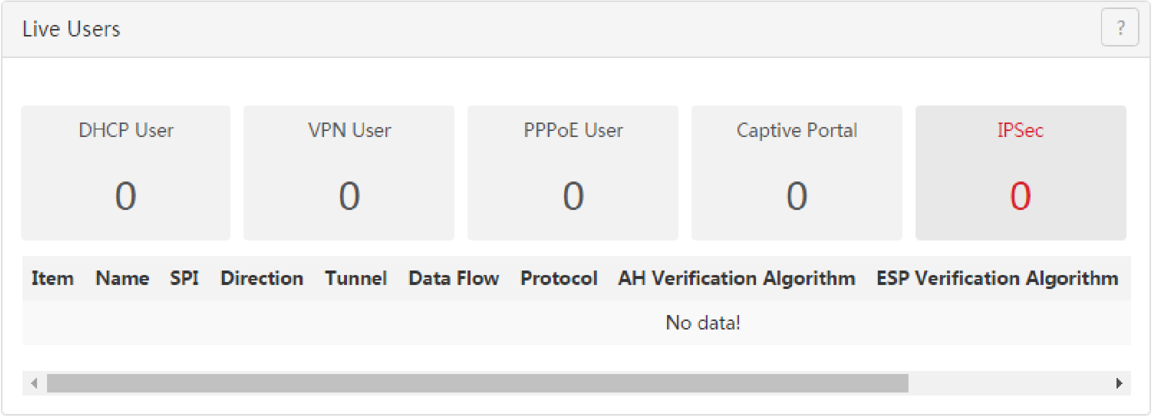
Item	Username	Remark	Authenticated Time	IP Address
			No data!	

The following table describes the parameters.

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.

14.2.5 IPSec

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** > **Live Users** > **IPSec**.



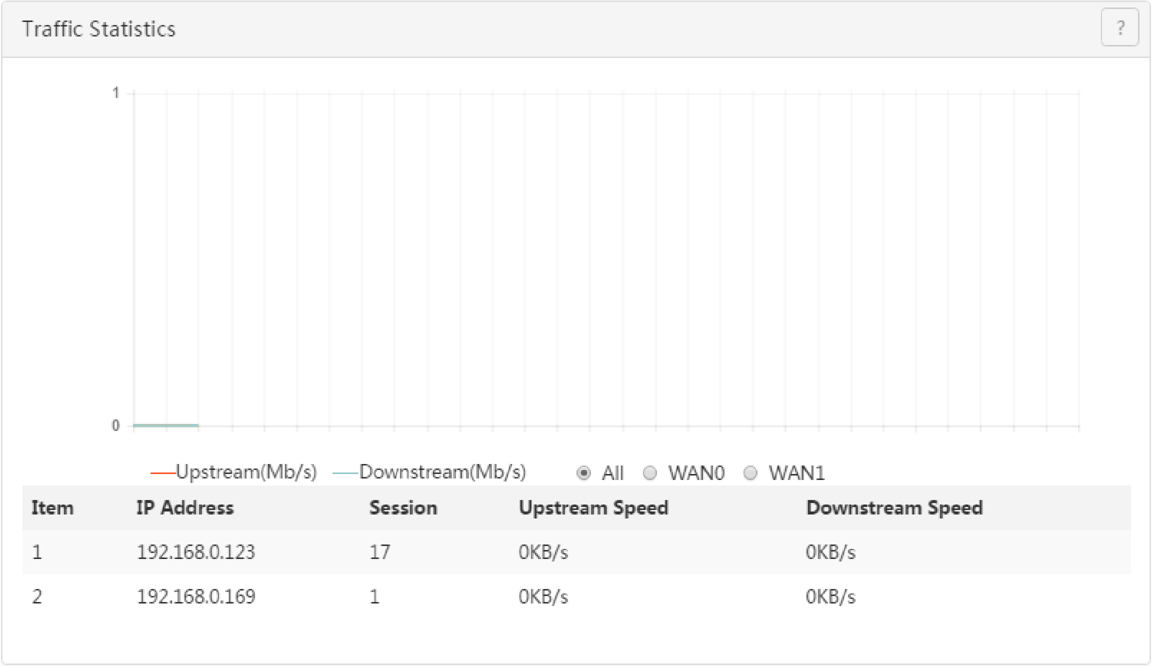
Item	Name	SPI	Direction	Tunnel	Data Flow	Protocol	AH Verification Algorithm	ESP Verification Algorithm
No data!								

The following table describes the parameters.

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 oprions 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.
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.

14.3 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** > **Traffic Statistics**.

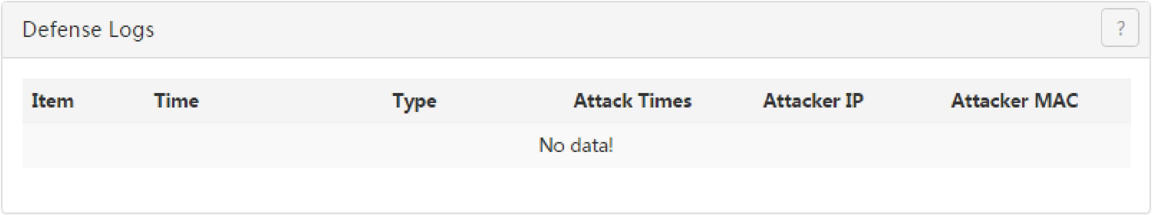


Item	IP Address	Session	Upstream Speed	Downstream Speed
1	192.168.0.123	17	0KB/s	0KB/s
2	192.168.0.169	1	0KB/s	0KB/s

14.4 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** > **Defense Logs**.

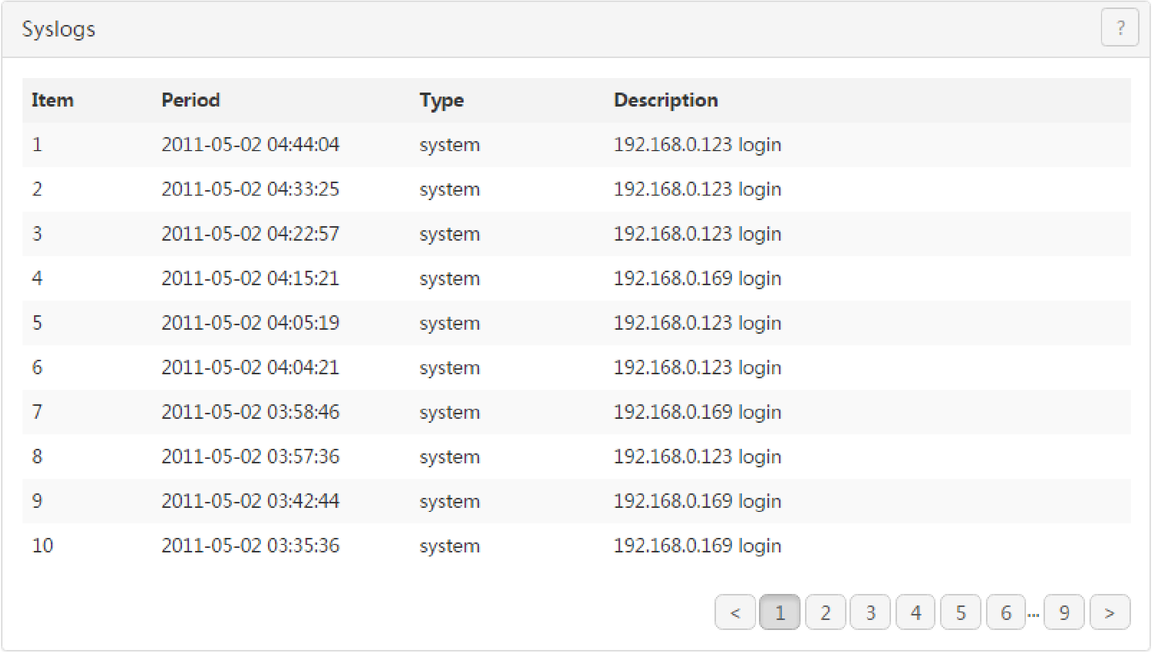


Item	Time	Type	Attack Times	Attacker IP	Attacker MAC
No data!					

14.5 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** > **Syslogs**.



Syslogs

Item	Period	Type	Description
1	2011-05-02 04:44:04	system	192.168.0.123 login
2	2011-05-02 04:33:25	system	192.168.0.123 login
3	2011-05-02 04:22:57	system	192.168.0.123 login
4	2011-05-02 04:15:21	system	192.168.0.169 login
5	2011-05-02 04:05:19	system	192.168.0.123 login
6	2011-05-02 04:04:21	system	192.168.0.123 login
7	2011-05-02 03:58:46	system	192.168.0.169 login
8	2011-05-02 03:57:36	system	192.168.0.123 login
9	2011-05-02 03:42:44	system	192.168.0.169 login
10	2011-05-02 03:35:36	system	192.168.0.169 login

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** > **Time & Date** 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 and make sure that the browser does not automatically set up a dial-up connection.
- 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: First, try logging in using the default IP addres **192.168.0.252** and the default user name and password **admin**. If login fails, restore the device to the factory settings and use the default login information to re-log in. 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 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.

For more technical support, contact us by:

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

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.