Tenda

Wireless Hotspot Router

User Guide

Copyright Statement

Tenda is a registered trademark legally held by Shenzhen Tenda Technology Co., Ltd. Other brand and product names mentioned herein are trademarks or registered trademarks of their respective holders. Copyright of the whole product as integration, including its accessories and software, belongs to Shenzhen Tenda Technology Co., Ltd. No part of this publication can be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means without the prior written permission of Shenzhen Tenda Technology Co., Ltd.

Disclaimer

Pictures, images and product specifications herein are for references only. To improve internal design, operational function, and/or reliability, Tenda reserves the right to make changes to the products without obligation to notify any person or organization of such revisions or changes. Tenda does not assume any liability that may occur due to the use or application of the product described herein. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information and recommendations in this document do not constitute a warranty of any kind, express or implied.

Preface

Thank you for choosing Tenda! Please read this user guide carefully before you start.

Conventions

This user guide is applicable to the following routers. W15E is used for illustrations here unless otherwise specified. The contained images and UI screenshots are subject to the actual products.

Product model	Description
W15E	AC1200 Wireless Hotspot Router
W18E	AC1200 Gigabit Wireless Hotspot Router

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

Item	Presentation	Example
Cascading menus	>	**System** > **Live Users**
Parameter and value	Bold	Set **User Name** to **Tom**.
Variable	Italic	Format: *XX*:*XX*:*XX*:*XX*:*XX*:*XX*
UI control	Bold	On the **Policy** page, click the **OK** button.
Message	“ ”	The “Success” message appears.

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

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

Acronym and Abbreviation

Acronym and Abbreviation	Full Spelling
AES	Advanced Encryption Standard
AH	Authentication Header
AP	Access Point
ARP	Address Resolution Protocol
ASCII	American Standard Code for Information Interchange
APSD	Automatic Power Save Delivery

Acronym and Abbreviation	Full Spelling
CPU	Central Processing Unit
DDNS	Dynamic Domain Name Server
DDoS	Distributed Denial of Service
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DPD	Digital Pre-Distortion
DMZ	Demilitarized Zone
DNS	Domain Name System
ESP	Encapsulating Security Payload
GBK	Chinese Internal Code Specification
GMT	Greenwich Mean Time
ICMP	Internet Control Message Protocol
IKE	Internet Key Exchange
IP	Internet Protocol
ISP	Internet Service Provider
IPSec	IP Security
L2TP	Layer 2 Tunneling Protocol
LAN	Local Area Network
MAC	Medium Access Control
MD5	Message Digest 5
MGMT	Management
MTU	Maximum Transmission Unit
NAT	Network Address Translation
PFS	Perfect Forward Secrecy
PoE	Power Over Ethernet
PPPoE	Point-to-Point Protocol Over Ethernet

Acronym and Abbreviation	Full Spelling
PPTP	Point to Point Tunneling Protocol
RSSI	Received Signal Strength Indicator
SA	Security Association
SSID	Service Set Identifier
SHA	Secure Hash Algorithm
Short GI	Short Guard Interval
SMS	Short Message Service
SPI	Security Parameter Index
SYN	Synchronize
SYS	System
TCP	Transmission Control Protocol
TKIP	Temporal Key Integrity Protocol
UDP	User Datagram Protocol
UI	User Interface
UPnP	Universal Plug and Play
URL	Uniform Resource Locator
UTF-8	8-bit Unicode Transformation Format
VPN	Virtual Private Network
WAN	Wide Area Network
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Networks
WMM	Wi-Fi multi-media

Technical Support

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

Hotline	Global: (86) 755-27657180 (China Time Zone)	**Email**	support@tenda.com.cn
	United States: 1-800-570-5892 (Toll Free: Daily-9am to 6pm PST)		
	Canada: 1-888-998-8966 (Toll Free: Mon - Fri 9 am - 6 pm PST)		
	Hong Kong: 00852-81931998		
Website	http://www.tendacn.com		

Contents

1 At a glance

1.1 Overview

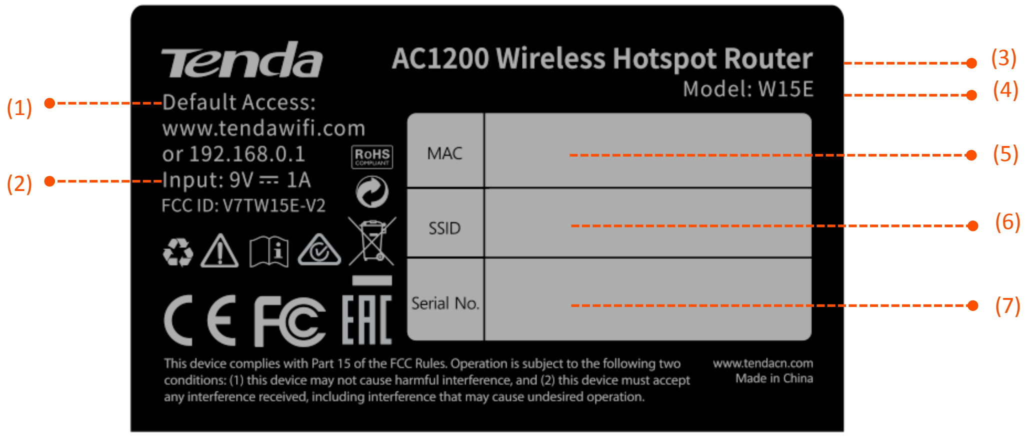
Tenda enterprise-level dual-band router offers a data rate as high as of 1167 Mbps. The enterprise router stands out both on hardware and software. With sleek appearance, four high-gain antennas, various interfaces, as well as an intuitive web UI that allows you to manage your network to achieve your very specific deployment purpose, such as authentication using captive portal or WiFi via WeChat, and VPN connections. You are assured to enjoy stable network and convenient management.

1.2 Main features

- Four high-gain antennas
- Up to 3 WAN ports
- At most three 2.4 GHz wireless networks and three 5 GHz wireless networks
- Offers a dual-band data rate up to 1167 Mbps
- Supports wireless network isolation
- Supports captive portal and WiFi via WeChat authentication
- Supports remote web management
- Supports smart and user-defined bandwidth control
- Supports IP/MAC/URL-based filter
- Supports PPTP/L2TP VPN server, PPTP/L2TP VPN client, and IPSec VPN connections
- High density user access

1.3 Label

You can refer to the label on the bottom of the device for checking the default information. W15E is used for illustration here.


Tenda
AC1200 Wireless Hotspot Router
Model: W15E
Default Access:
www.tendawifi.com
or 192.168.0.1
Input: 9V ⎓ 1A
FCC ID: V7TW15E-V2
RoHS
MAC
SSID
Serial No.
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.
www.tendacn.com
Made in China
(1)
(2)
(3)
(4)
(5)
(6)
(7)

(1) **Default Access**: Default domain name or IP address for logging in to the web UI of the router.

(2) **Input**: Power specification of the router. Check if the power sourcing equipment complies before powering it on.

(3) Product name of the router.

(4) **Model**: Product model of the router. You can use this model as a key word for searching related supporting materials across various channels, such as our official website, or e-commerce websites.

(5) **MAC**: MAC address of the router. A MAC address refers to the unique physical address built-in the device.

(6) **SSID**: Default wireless network name of the router.

(7) **Serial No.**: The unique serial number of the router.

2 Quick Setup

This chapter introduces how to set up to the internet access for the first time.

Step 1 Connecting your router

1. Connect the included power adapter to the **Power** jack of the router to power it on.
2. Use an Ethernet cable to connect an Ethernet jack or a LAN port of your modem to the WAN port of the router.
3. Either connect your computer to a LAN port of the router, or connect your WiFi-enabled device, such as a smart phone, to the wireless network of the router.

TIP

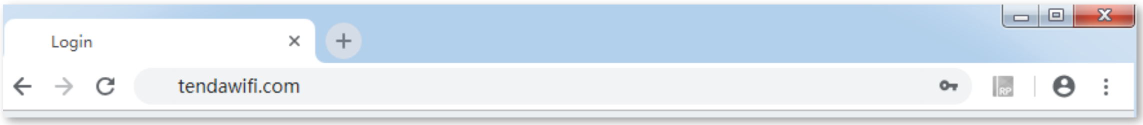
The default SSID is on the bottom Label of the router. By default, it has no WiFi password.

Step 2 Configuring your router

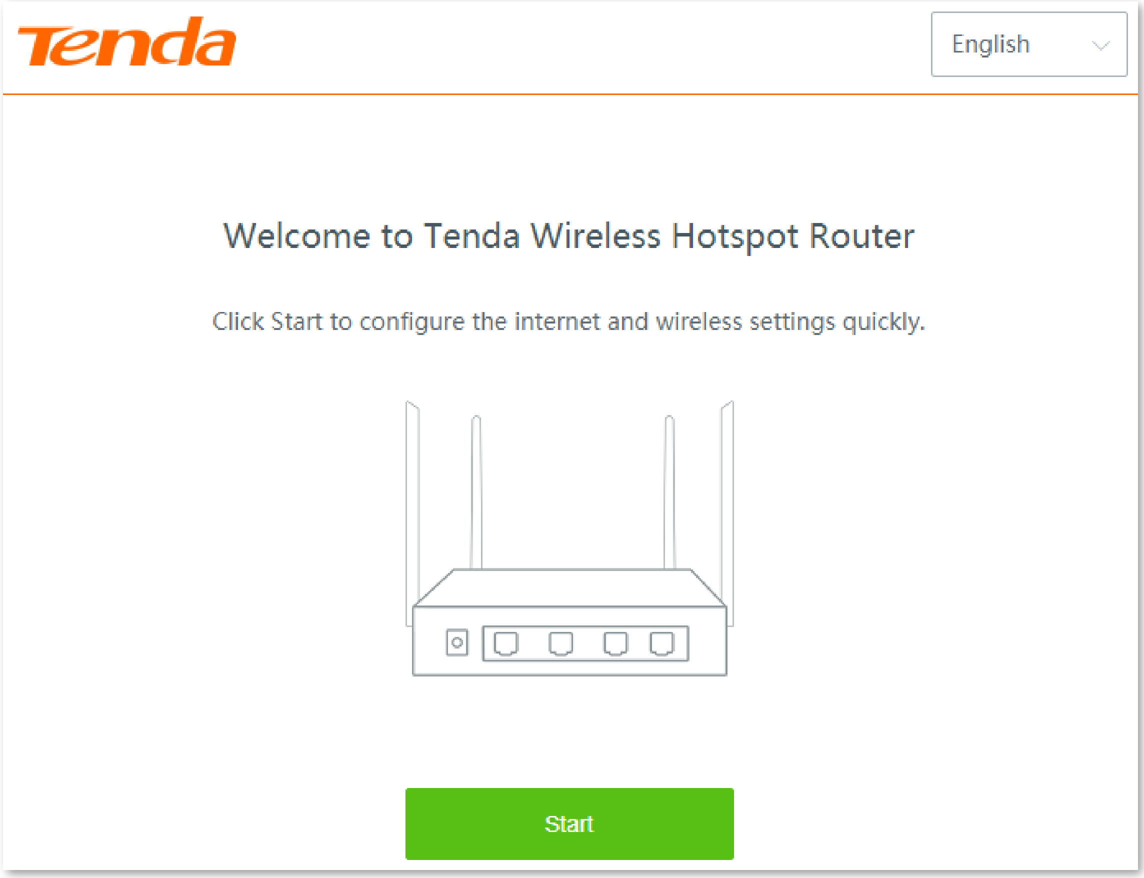
TIP

- You can perform quick setup either using a tethered computer or a smart phone. The configuration process is the same. The following takes a computer for example.
- If a smart phone is used, disable its mobile or cellular network function.

1. Start a web browser either on the computer tethered to the router to the wireless network of the router, and access **tendawifi.com**.



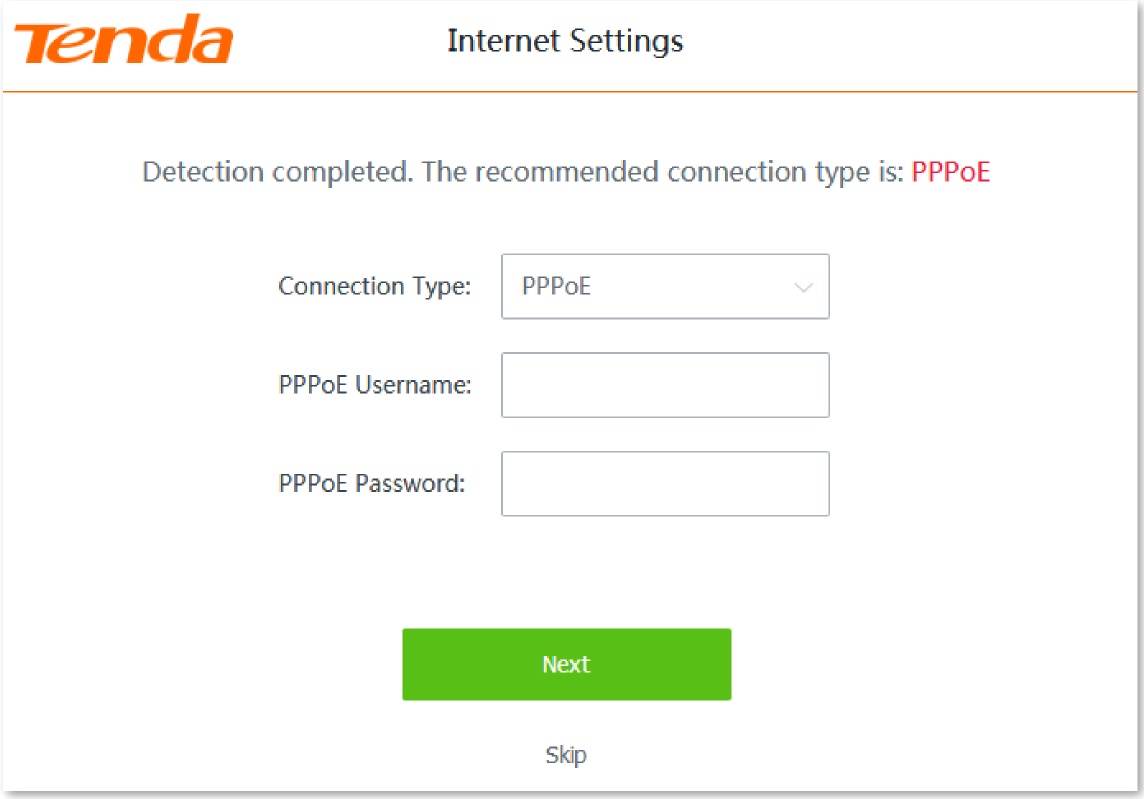
2. Click **Start**. The system automatically starts detecting your internet connection type.



Welcome to Tenda Wireless Hotspot Router

Click Start to configure the internet and wireless settings quickly.

3. After detection completed, just follow the on-screen instructions to set up your router. PPPoE is used for illustrating here. Enter the **PPPoE Username** and **PPPoE Password** provided by you ISP, and click **Next**.



Internet Settings

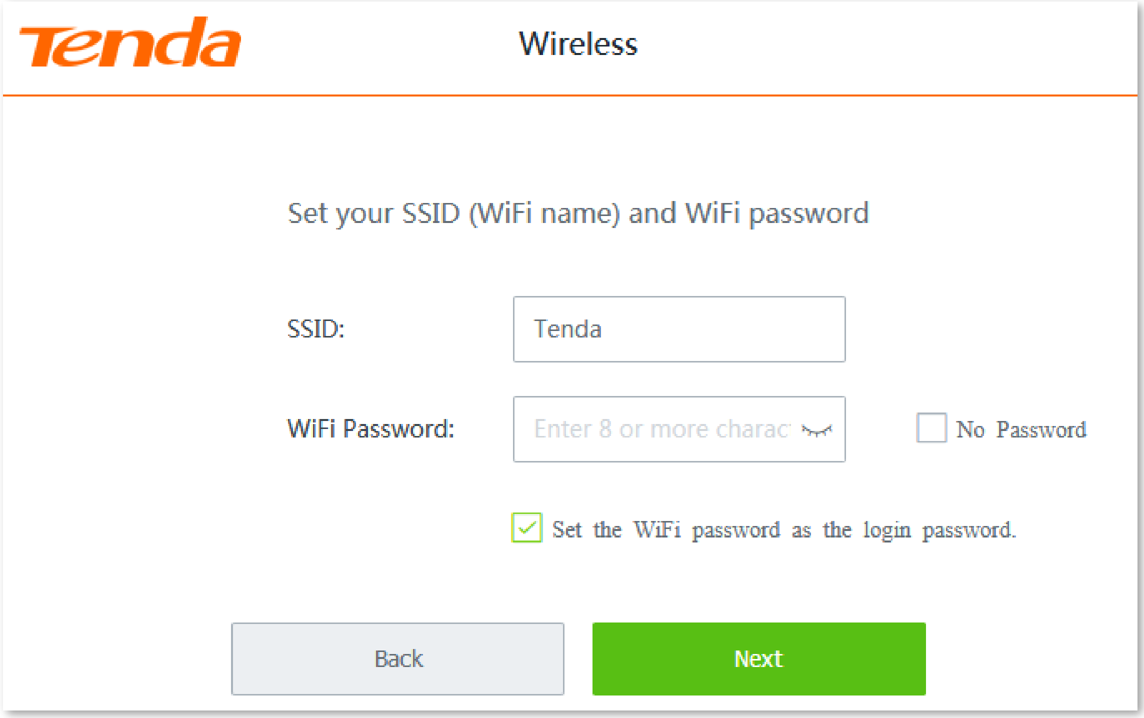
Detection completed. The recommended connection type is: PPPoE

Connection Type: PPPoE

PPPoE Username:

PPPoE Password:

4. Customize the **SSID** (wireless network name) and **WiFi password** as needed.



Wireless

Set your SSID (WiFi name) and WiFi password

SSID: Tenda

WiFi Password: Enter 8 or more charac □ No Password

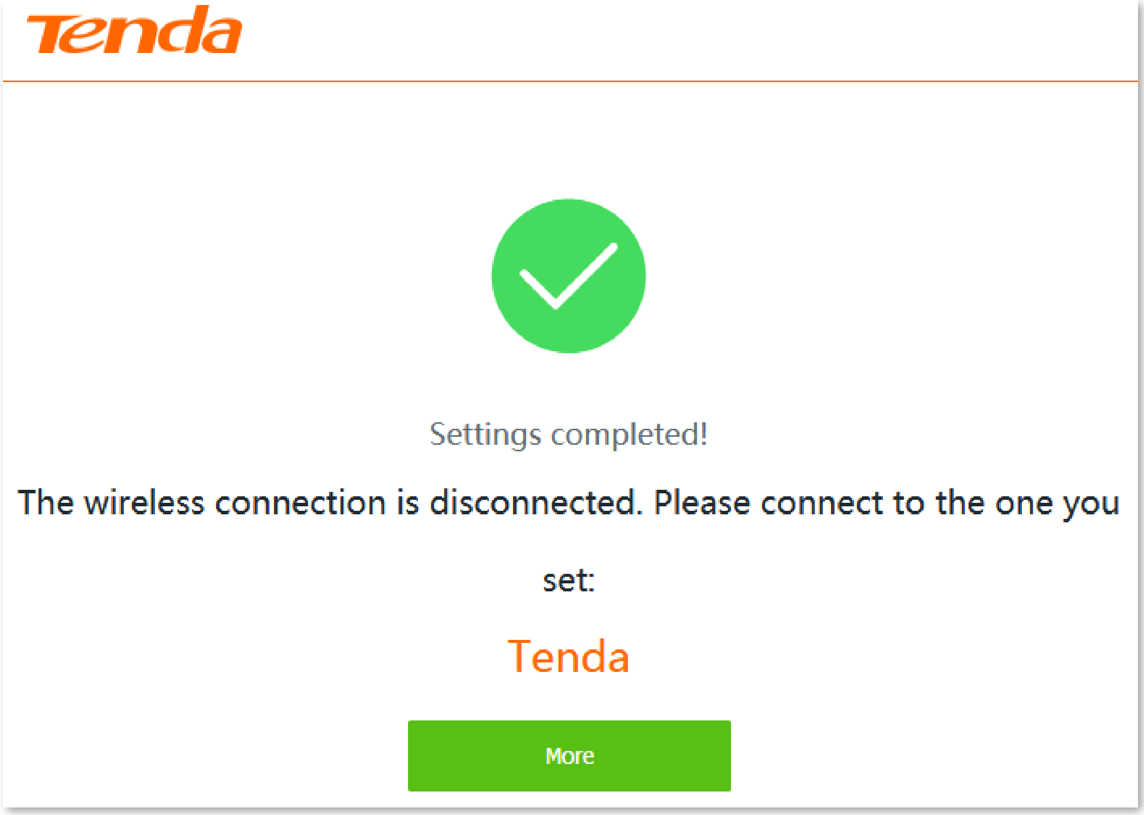
☑ Set the WiFi password as the login password.

TIP

- By default, the **WiFi password** is set as the **Login Password**, you can deselect the checkbox and customize them separately.
- **WiFi Password** is used for connecting to your wireless network, while **Login Password** is used for logging into the web UI of the router for management.

5. Click **Next**.

---- End



Settings completed!

The wireless connection is disconnected. Please connect to the one you set:

Tenda

To access the internet with:

- **Wireless clients**: Connect your wirelss clients to the SSID with the WiFi password you set.
- **Wired clients**: Connect the wired clients to LAN ports of the router.

3 Login

3.1 Login

TIP

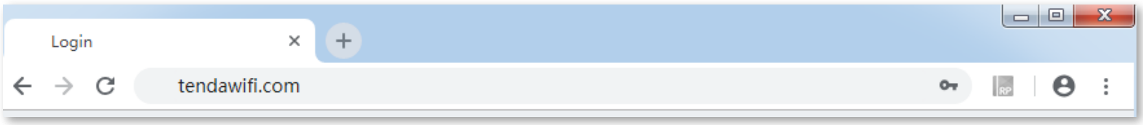
This section introduces how to log in to the web UI of the router for management. For initial use of the router, refer to Quick Setup.

3.1.1 Overview

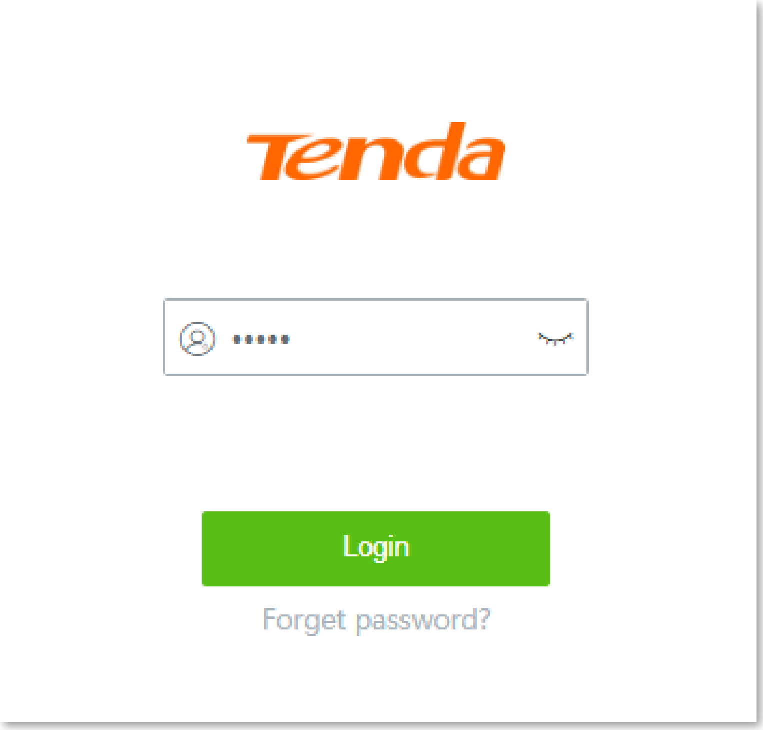
The router supports two account types: **Administrator** and **Authentication**. The **Administrator** account enjoys all access permission of the router, while the **Authentication** account only has permission for accessing **System Status** and **Authentication** modules. For detailed explanation, see Password manager.

3.1.2 Logging in to the web UI of the router

Step 1 Start a web browser on your device connected to the router, and access **tendawifi.com**.

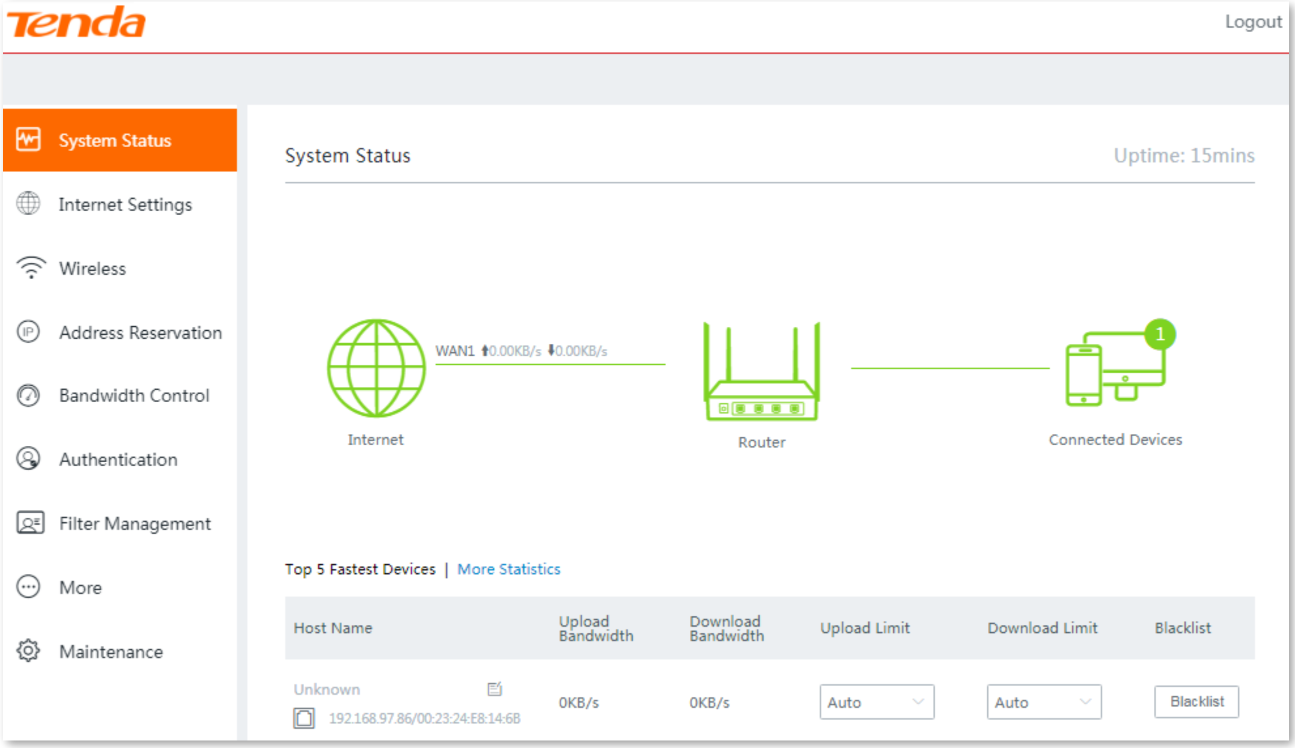


Step 2 Enter the login password of the router you set, and click **Login**.



---- End

Log in to the web UI of the router using the **Administrator** account successfully. See the following figure:



System Status

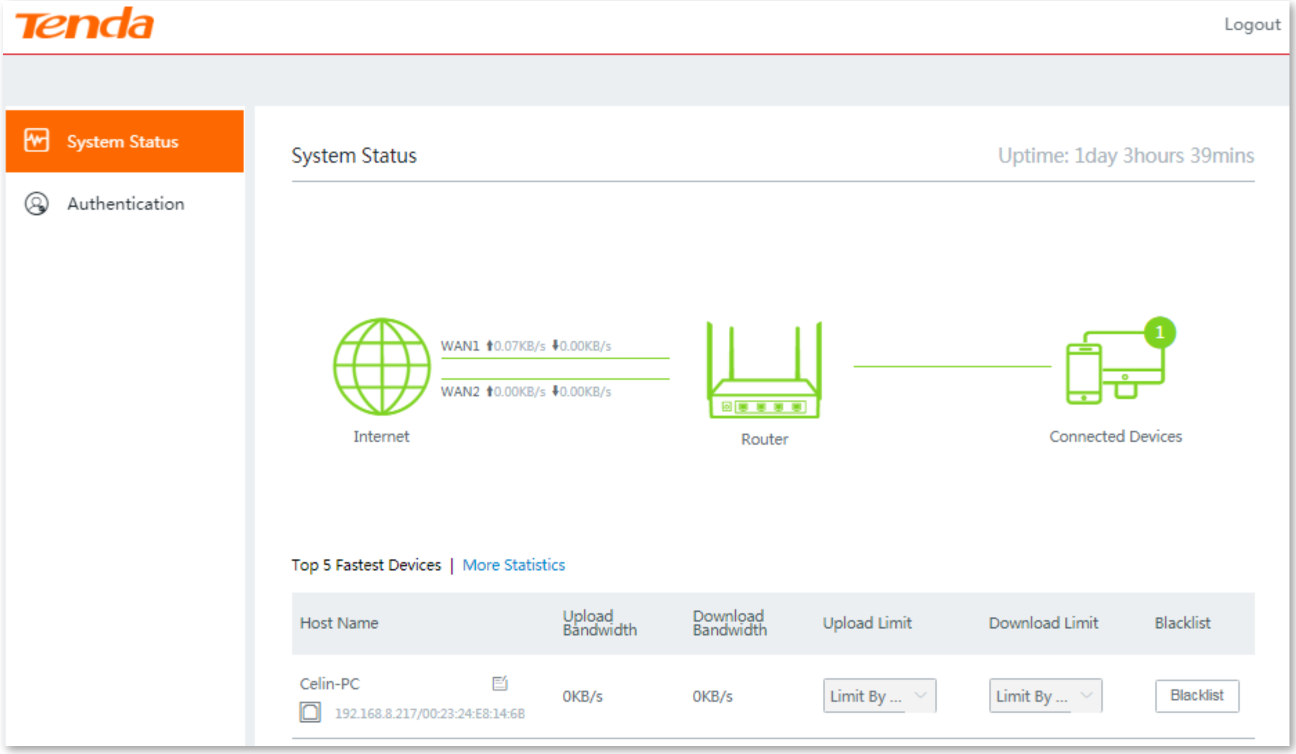
Uptime: 15mins

WAN1 ⬆0.00KB/s ⬇0.00KB/s

Top 5 Fastest Devices | More Statistics

Host Name	Upload Bandwidth	Download Bandwidth	Upload Limit	Download Limit	Blacklist
Unknown □ 192.168.97.86/00:23:24:E8:14:6B	0KB/s	0KB/s	Auto	Auto	Blacklist

Log in to the web UI of the router using the **Authentication** account successfully. See the following figure:



System Status

Uptime: 1day 3hours 39mins

WAN1 ⬆0.07KB/s ⬇0.00KB/s

WAN2 ⬆0.00KB/s ⬇0.00KB/s

Top 5 Fastest Devices | More Statistics

Host Name	Upload Bandwidth	Download Bandwidth	Upload Limit	Download Limit	Blacklist
Celin-PC □ 192.168.8.217/00:23:24:E8:14:6B	0KB/s	0KB/s	Limit By ...	Limit By ...	Blacklist

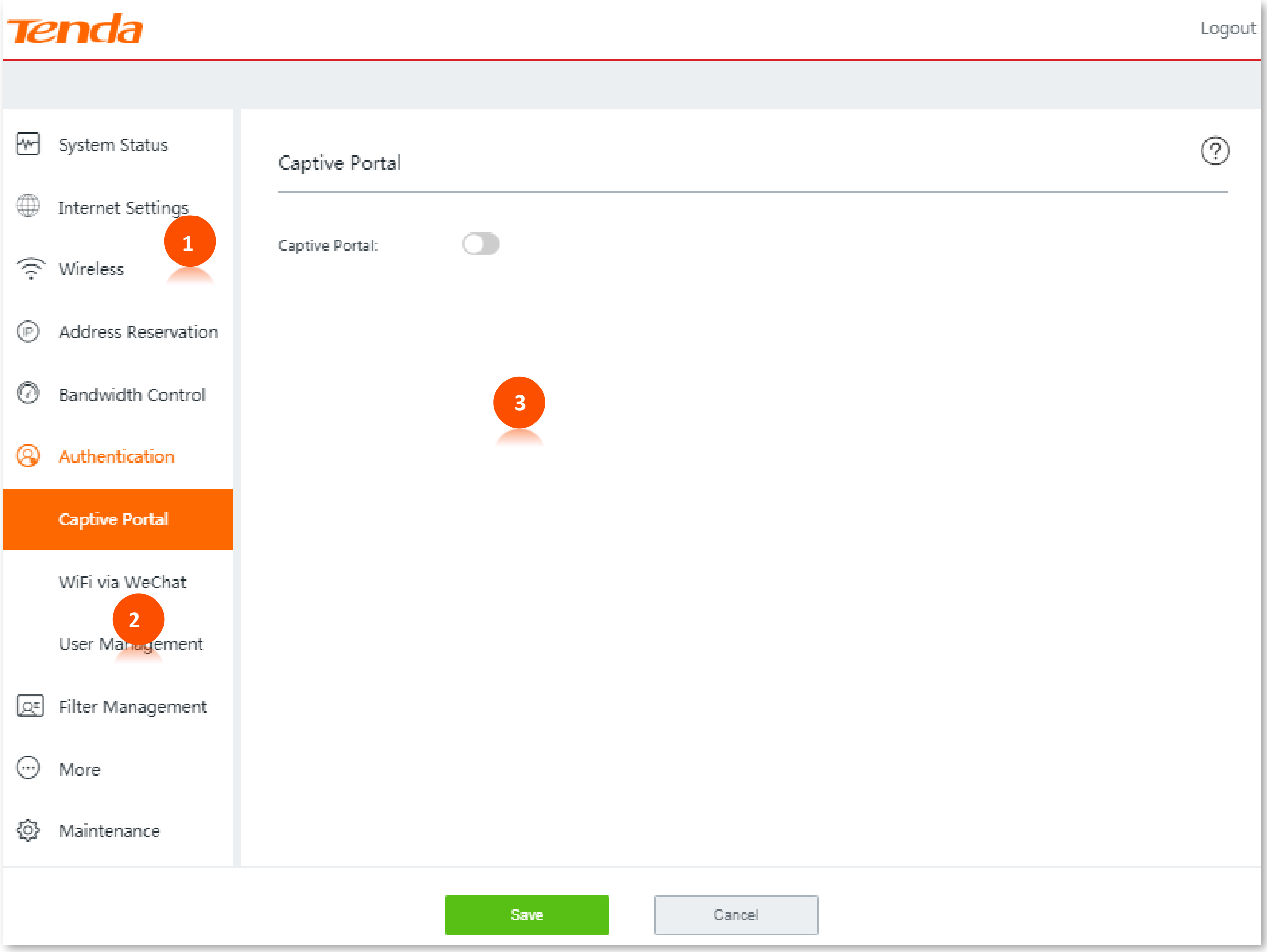
3.2 Log out

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

You can log out by clicking **Logout** on the upper right corner of the web UI as well.

3.3 Web UI layout

The web UI of the router consists of three sections, including the level-1, and level-2 navigation bar, and the configuration area as well. See the following figure:



SN	Name	Description
1	Level-1 navigation bar	Used to display the function menu of the router. Users can select functions in the navigation bars and the configuration appears in the configuration area.
2	Level-2 navigation bar	
3	Configuration area	Used to modify or view your configuration.

3.4 Frequently-used buttons

The following table describes the frequently-used buttons available on the web UI of the router.

Button	Description
Save	Used to save the configuration on the current page and enable the configuration to take effect.
Cancel	Used to change the current configuration on the current page back to the original configuration.
?	Used to get the online help.

4 System status

This chapter introduces:

- Checking physical connections and system status.
- Monitoring traffic.
- Managing online devices, such as control their speed, add them to or remove them from the blacklist.

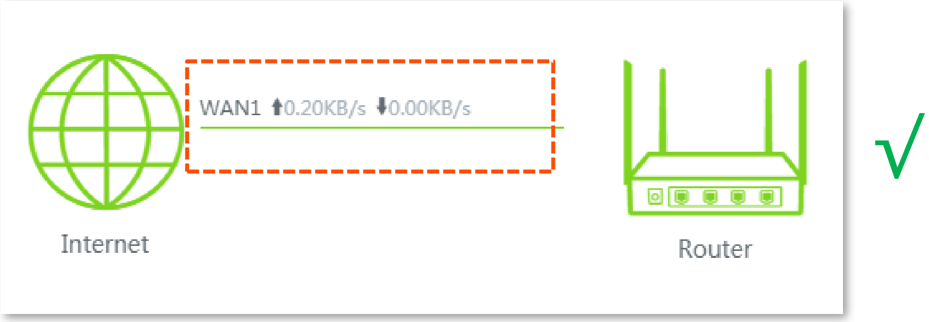
4.1 Checking physical connections and system status

To enter the configuration page, choose **System Status**.

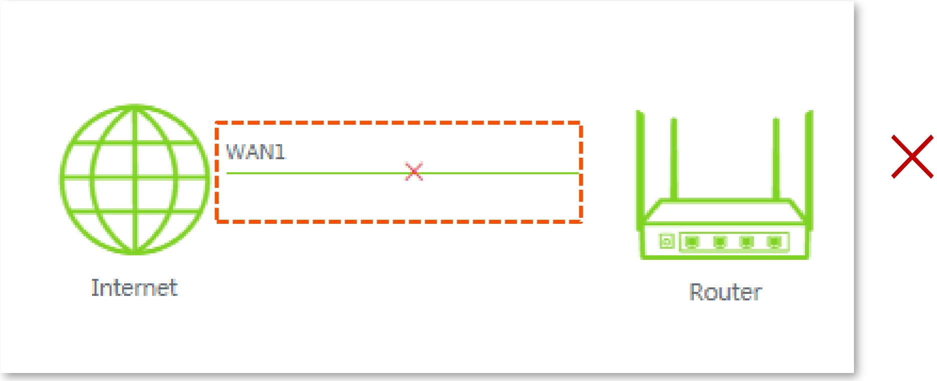
You can check if the physical connections are proper, or the router's system status here.

4.1.1 Checking physical connections

The following figure indicates that the router is connected to the internet properly through the WAN1 port.



The following figure indicates that connection between the router and the internet is abnormal. Please check if the router is properly connected to the WAN1 port, or the internet connection parameters you set are correct.

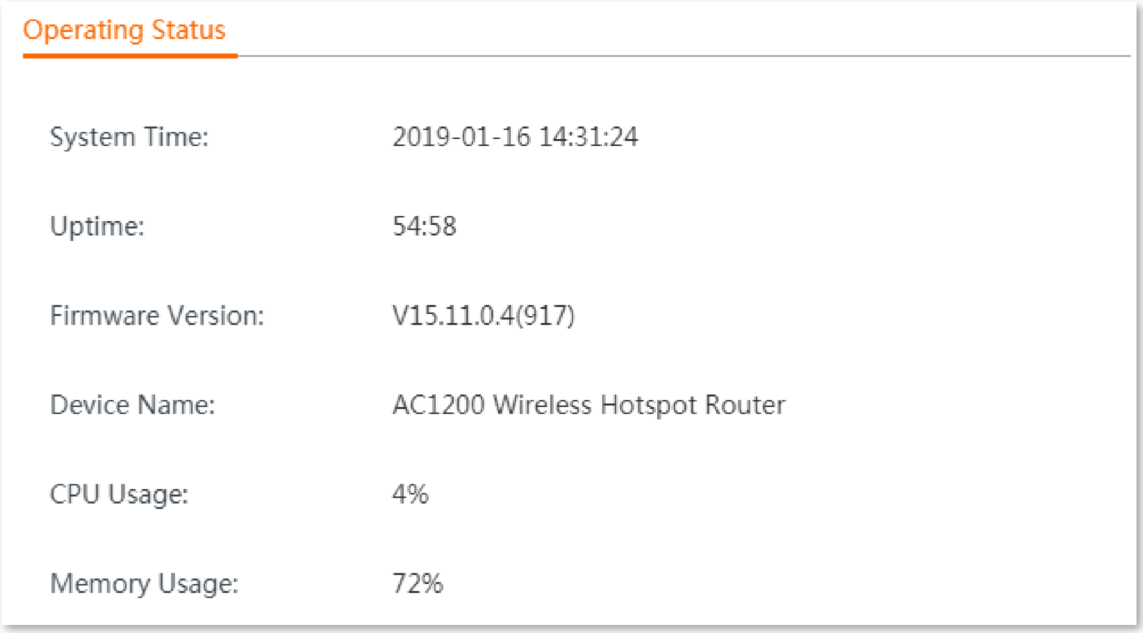


4.1.2 Viewing system status

On **System Status** page, click the **Router** icon , the **Device Info** window pops up.

The **Device Info** window consists of three parts: Operating Status, LAN Port Status, and WAN Info.

- **Operating Status**



Operating Status

System Time: 2019-01-16 14:31:24

Uptime: 54:58

Firmware Version: V15.11.0.4(917)

Device Name: AC1200 Wireless Hotspot Router

CPU Usage: 4%

Memory Usage: 72%

Parameter description

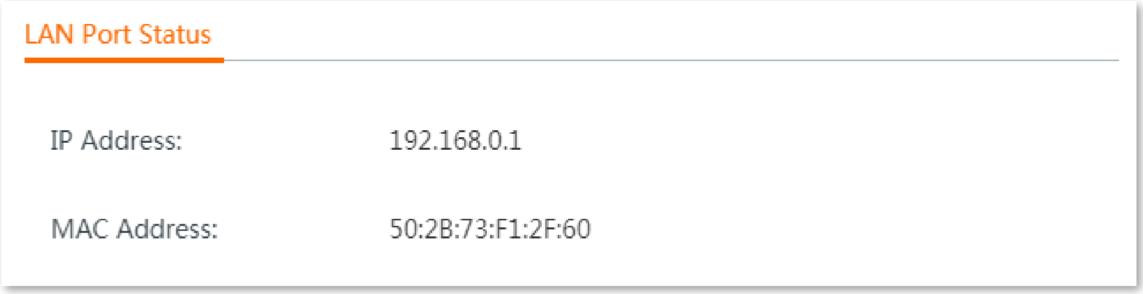
Parameter	Description
System Time	It specifies the current system time of the router. You can set system time by navigating to **Maintenance** > **System time**.
Uptime	It specifies the time that has elapsed since the router was started last time.
Firmware Version	It specifies the firmware version number of the router.
Device Name	It specifies the name of your router.
CPU Usage	It specifies the current CPU usage of the router.
Memory Usage	It specifies the current memory usage of the router.

LAN port status

This module shows the LAN IP address and the MAC address of the router.

TIP

You can modify LAN settings by navigating to **More** > LAN settings.



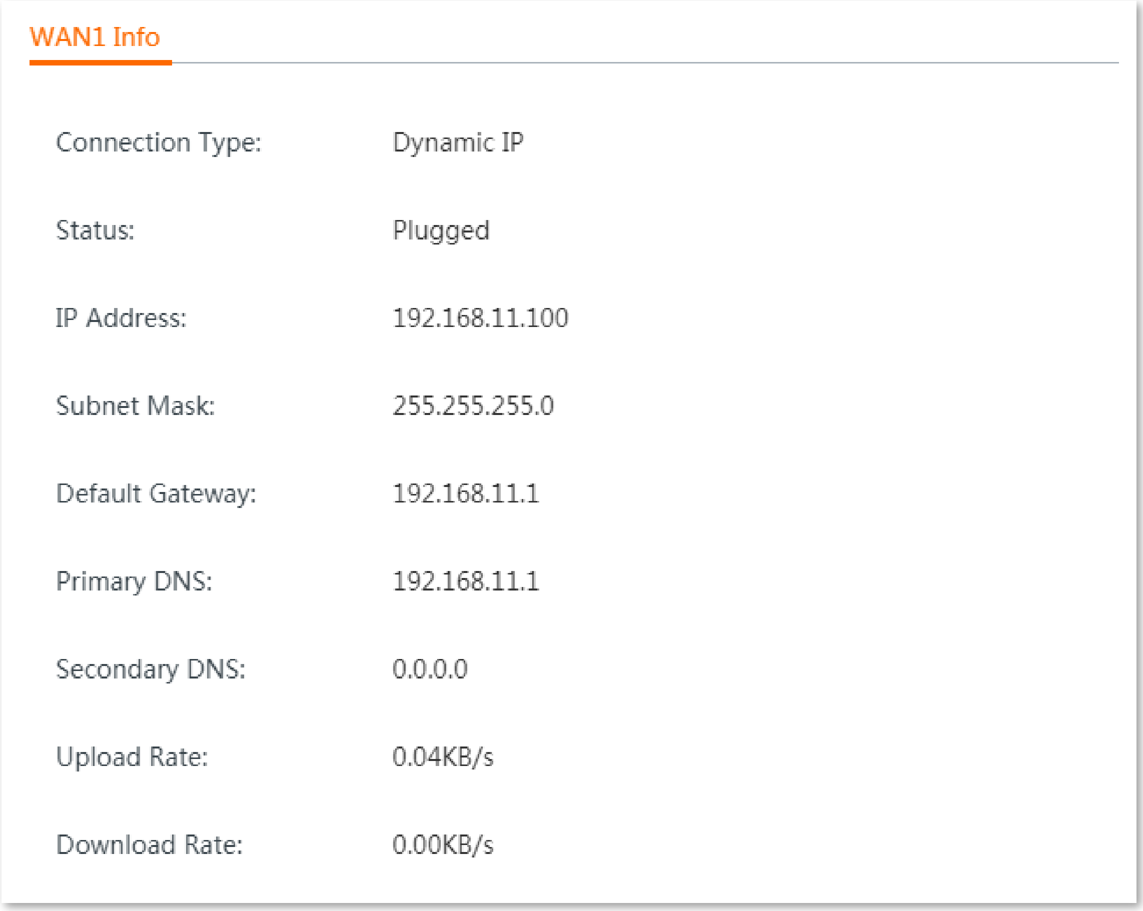
LAN Port Status

IP Address: 192.168.0.1

MAC Address: 50:2B:73:F1:2F:60

WAN Info

This module displays information about all enabled WAN ports, including **Connection Type**, **Status**, **and IP Address** and so on.



WAN1 Info

Connection Type: Dynamic IP

Status: Plugged

IP Address: 192.168.11.100

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.11.1

Primary DNS: 192.168.11.1

Secondary DNS: 0.0.0.0

Upload Rate: 0.04KB/s

Download Rate: 0.00KB/s

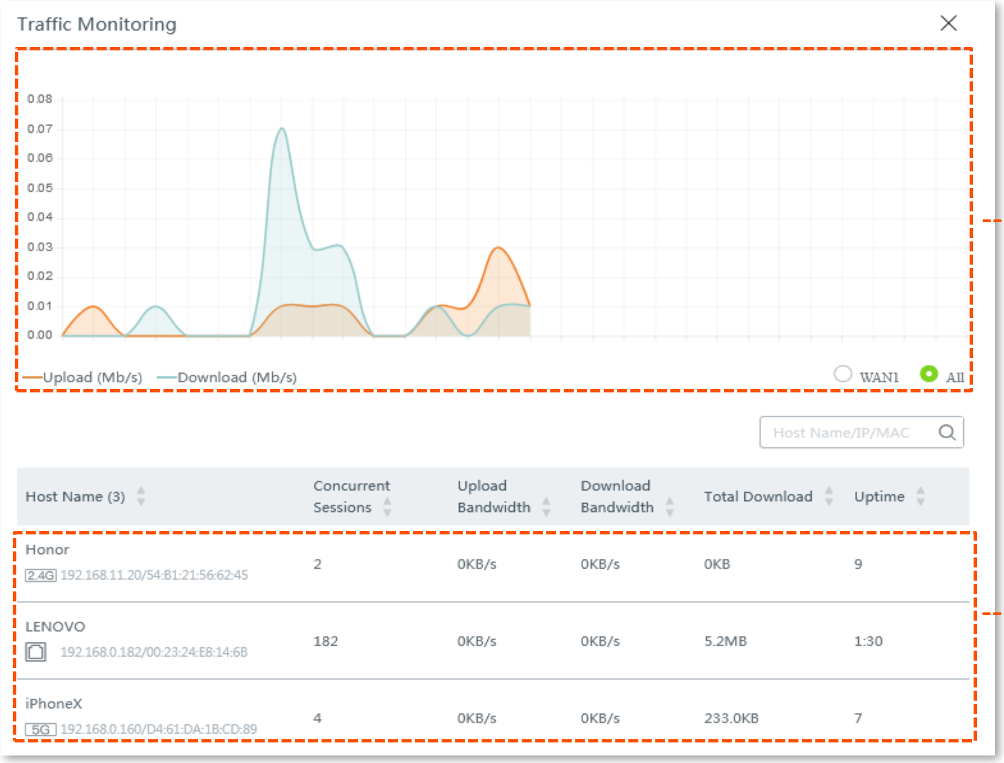
Parameter description

Parameter	**Description**
Connection Type	It specifies the internet connection type of the corresponding WAN port.
Status	It specifies whether or not the WAN port is plugged. If **Unplugged** appears, please check its physical connection.

Parameter	Description
IP Address	It indicates the IP address of the corresponding WAN port.
Subnet Mask	It indicates the subnet mask of the corresponding WAN port.
Default Gateway	It indicates the gateway IP address of the corresponding WAN port. Only forwarding packets through this gateway can clients access the internet.
Primary DNS	The primary/secondary DNS server address of the corresponding WAN port. The **Secondary DNS** is optional. If you do not set this parameter, it shows **0.0.0.0**.
Secondary DNS	
Upload Rate	The upload and download rate of the corresponding WAN port.
Download Rate	

4.2 Monitoring traffic

The router presents the traffic usage in an intuitive way. Click **More Statistics** on **System Status** page, the **Traffic Monitoring** window appears. See the following figure:



Host Name (3)	Concurrent Sessions	Upload Bandwidth	Download Bandwidth	Total Download	Uptime
Honor 2.4G 192.168.11.20/54:B1:21:56:62:45	2	0KB/s	0KB/s	0KB	9
LENOVO 192.168.0.182/00:23:24:E8:14:6B	182	0KB/s	0KB/s	5.2MB	1:30
iPhoneX 5G 192.168.0.160/D4:61:DA:1B:CD:89	4	0KB/s	0KB/s	233.0KB	7

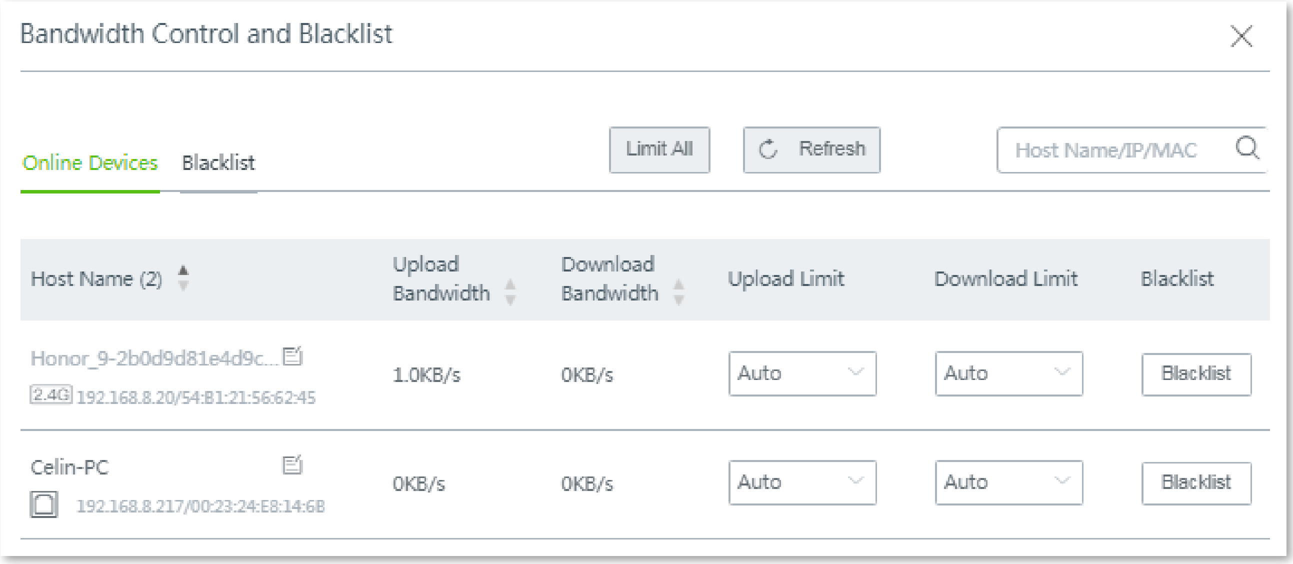
Monitoring traffic of selected WAN port(s).

Monitoring traffic of online client(s).

4.3 Managing online devices

To access the configuration page, click the **Connected Devices** icon on the **System Status** page. The **Bandwidth Control and Blacklist** window appears.

You can edit the name of connected clients, control the connected clients' upload and/or download bandwidth separately or in batch, and block a device from accessing your network.



Bandwidth Control and Blacklist

Host Name (2)	Upload Bandwidth	Download Bandwidth	Upload Limit	Download Limit	Blacklist
Honor_9-2b0d9d81e4d9c... ✎ 2.4G 192.168.8.20/54:B1:21:56:62:45	1.0KB/s	0KB/s	Auto	Auto	Blacklist
Celin-PC ✎ □ 192.168.8.217/00:23:24:E8:14:6B	0KB/s	0KB/s	Auto	Auto	Blacklist

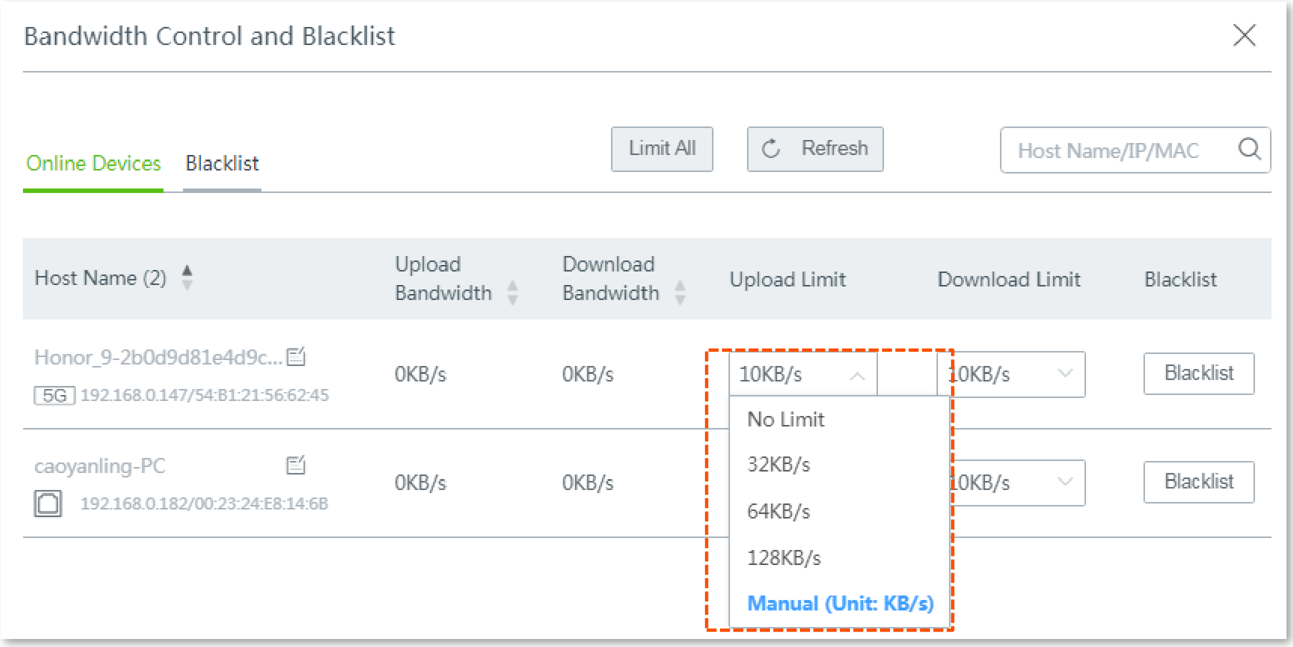
Parameter description

Parameter	Description
Host Name	It specifies the name of clients connected to the router, connection type, their IP addresses, and MAC addresses. You can click ✎ to personalize the host name for convenient management. NOTE For host name-based rules, such as Configuring authentication-free host using host name, you need to use the host name here. □ : The client connects to the router in a wired manner. 2.4G : The client connects to the router's 2.4 GHz wireless network. 5G : The client connects to the router's 5 GHz wireless network.
Concurrent Sessions	Concurrent sessions established of the corresponding client.
Upload Bandwidth	It indicates the real-time upload/download bandwidth of each client. You can control their maximum upload/download bandwidth manually, refer to Managing online devices.
Download Bandwidth	
Total Download	It specifies the total download traffic utilized by each client.
Uptime	It specifies the connection time of each client. The unit is minute.

4.3.1 Controling bandwidth of online devices

Control bandwidth of online devices separately

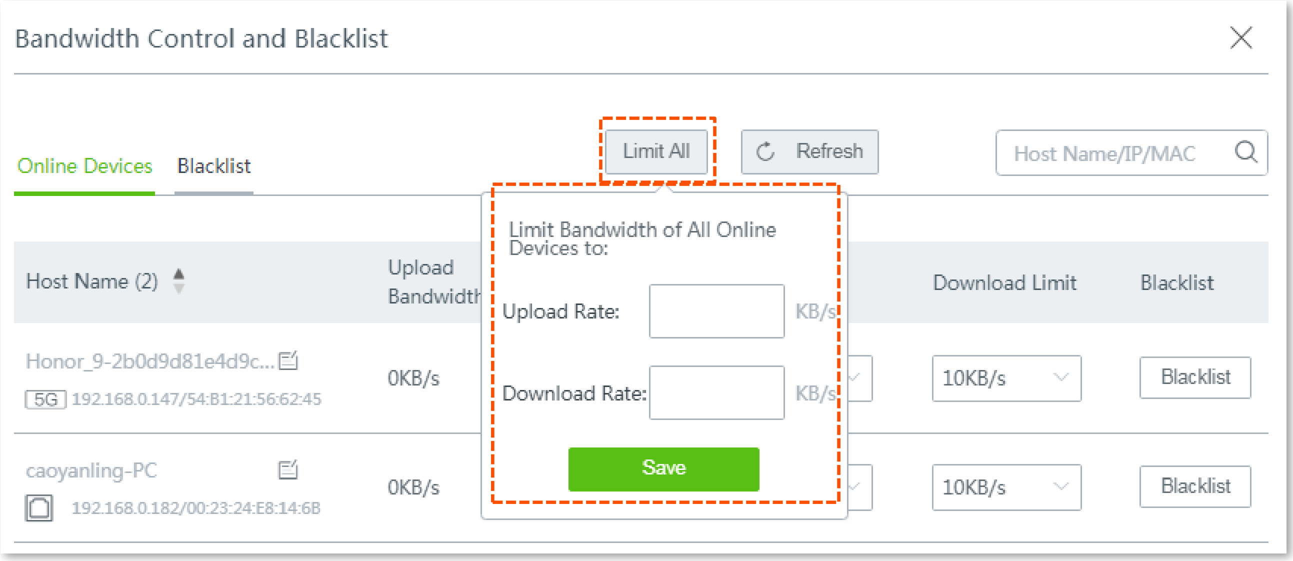
To limit the upload and/or download bandwidth of one or several devices, select a pre-defined value from the drop-down list menu of **Upload Limit** and/or **Download Limit**, or select **Manual** to specify a value manually.



Host Name (2)	Upload Bandwidth	Download Bandwidth	Upload Limit	Download Limit	Blacklist
Honor_9-2b0d9d81e4d9c... 5G 192.168.0.147/54:B1:21:56:62:45	0KB/s	0KB/s	10KB/s	10KB/s	Blacklist
caoyanling-PC 192.168.0.182/00:23:24:E8:14:6B	0KB/s	0KB/s		10KB/s	Blacklist

Control bandwidth of online devices in batch

Click **Limit All**, specify the values according to your actual situation, and click **Save** to apply your settings.



Limit Bandwidth of All Online Devices to:

Upload Rate: KB/s

Download Rate: KB/s

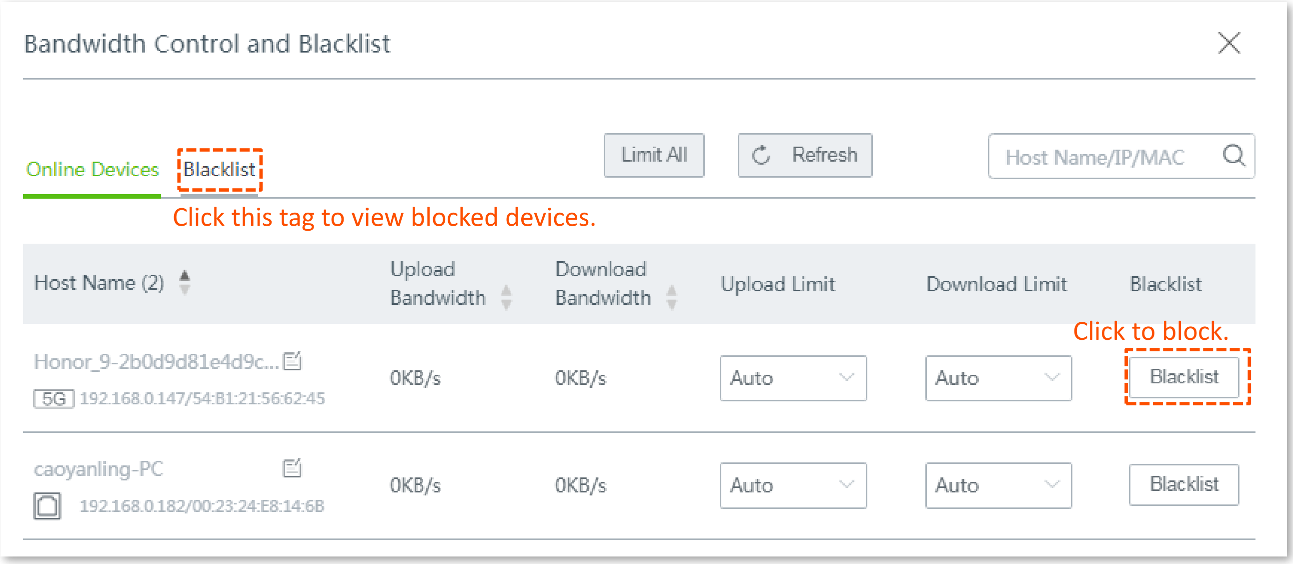
Host Name (2)	Upload Bandwidth	Download Limit	Blacklist
Honor_9-2b0d9d81e4d9c... 5G 192.168.0.147/54:B1:21:56:62:45	0KB/s	10KB/s	Blacklist
caoyanling-PC 192.168.0.182/00:23:24:E8:14:6B	0KB/s	10KB/s	Blacklist

NOTE

Upload/download limits of devices that controlled by **Limit by Group** policy cannot be modified here. Refer to Limit By Group for details.

4.3.2 Adding to blacklist

To protect your network from being accessed by unknown devices, click the **Blacklist** button to block them. The blocked devices will be moved to the **Blacklist** section, and cannot connect to your router.


Bandwidth Control and Blacklist
Online Devices
Blacklist
Limit All
Refresh
Host Name/IP/MAC
Click this tag to view blocked devices.
Click to block.

Host Name (2)	Upload Bandwidth	Download Bandwidth	Upload Limit	Download Limit	Blacklist
Honor_9-2b0d9d81e4d9c... 5G 192.168.0.147/54:B1:21:56:62:45	0KB/s	0KB/s	Auto	Auto	Blacklist
caoyanling-PC 192.168.0.182/00:23:24:E8:14:6B	0KB/s	0KB/s	Auto	Auto	Blacklist

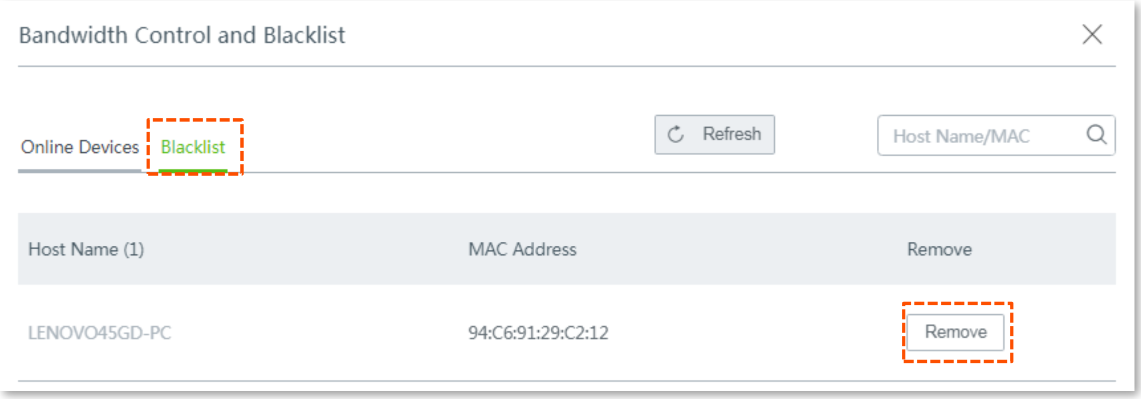
4.3.3 Removing from blacklist

Follow steps below to unblock devices from the blacklist.

Step 1 Click the **Connected Devices** icon on the **System Status** page. The **Bandwidth Control and Blacklist** window appears.

Step 2 Click the **Blacklist** tag.

Step 3 Click **Remove** that relates with the device you want to unblock.



Host Name (1)	MAC Address	Remove
LENOVO45GD-PC	94:C6:91:29:C2:12	Remove

---- End

The unblocked devices can connect to your router.

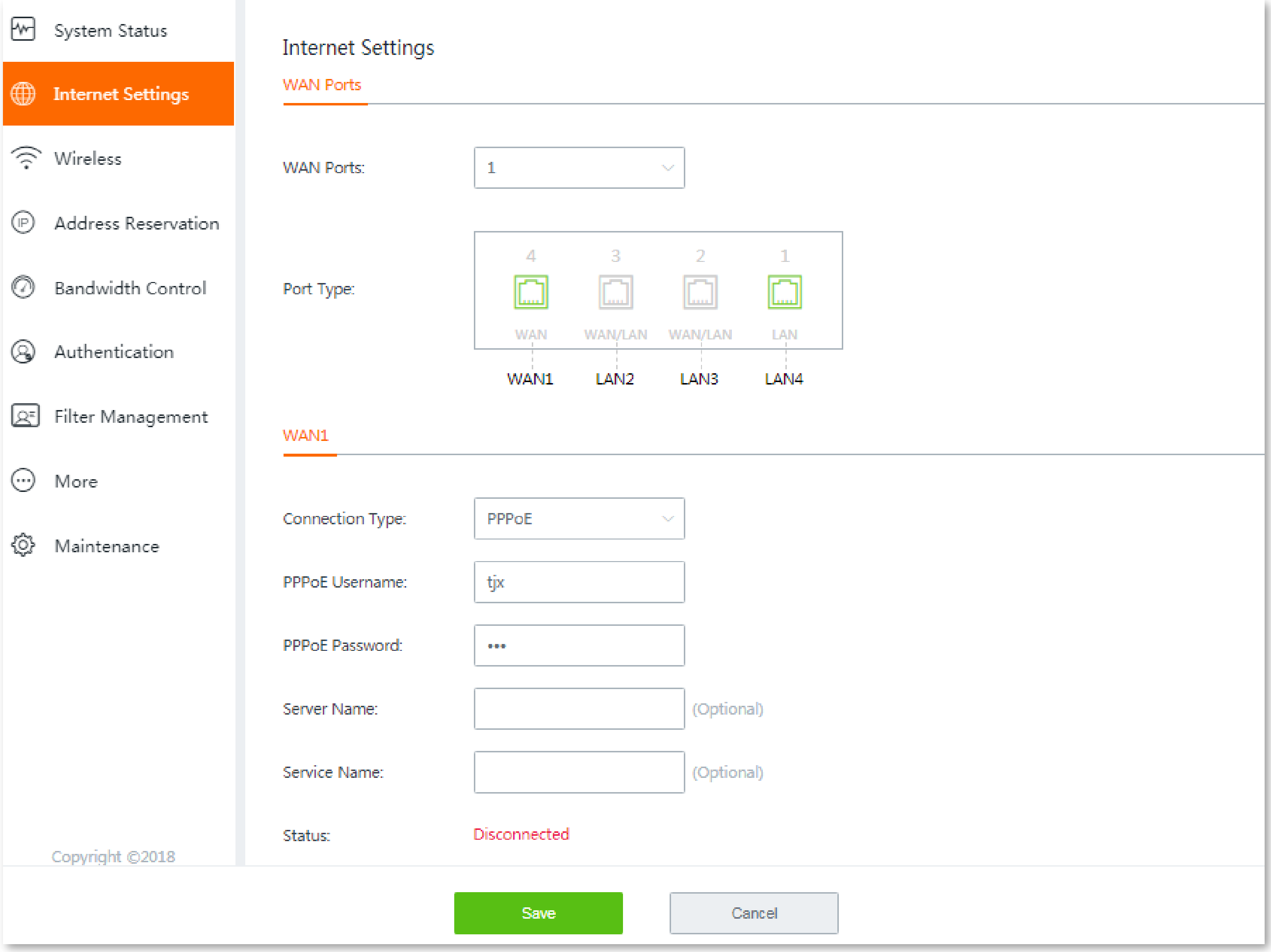
5 Internet Settings

This chapter introduces how to:

- Configuring multiple WAN ports.
- Setting up to access the internet with **PPPoE**, **Static IP**, or **Dynamic IP**.

5.1 Overview

To enter the configuration page, choose **Internet Settings**.



WAN Ports: 1

Port Type:

Connection Type: PPPoE

PPPoE Username: tjx

PPPoE Password: •••

Server Name: (Optional)

Service Name: (Optional)

Status: Disconnected

Parameter description

Parameter	Description
WAN Ports	It specifies how many WAN ports you can set on the router. By default, the router has only one WAN port (the WAN1 port), and you can set **3** WAN ports at most.

Parameter	Description
Port Type	It indicates that if the port functions as a WAN port or a LAN port, as well as if a port is connected or not. 🟩 : The port is connected properly. ⬜ : The port is disconnected or improperly connected.
Connection Type	It specifies in which way the router is connected to the internet. The router supports **PPPoE**, **Static IP**, and **Dynamic IP**. Refer to the table [Choose your connection type]() for details. TIP The router supports **PPPoE Russia**, **PPTP/PPTP Russia**, and **L2TP/L2TP Russia** as well. These three connection types are only applicable to Russia and its vicinity.
PPPoE Username	These two parameters are required only when your internet connection type is PPPoE. TIP - You can find them on the receipt provided by your ISP when you subscribed broadband service. - If you cannot find them, consult your ISP.
PPPoE Password	
Server Name	(Optional) Enter these two parameters provided by your ISP. If not, leave them blank.
Service Name	
IP Address	These parameters are required only when your internet connection type is **Static IP**. The **Secondary DNS** parameter is optional. TIP - You can find them on the receipt provided by your ISP when you subscribed broadband service. - If you cannot find them, consult your ISP.
Subnet Mask	
Default Gateway	
Primary DNS	
Secondary DNS	
Status	It indicates the connection status of the corresponding WAN port. - **Authenticated Successfully/Connected**: The corresponding WAN port has been connected properly, and obtained an IP address. - **Connecting…**: The router is connecting to the internet or server. - **Disconnected**: The port is disconnected, or fails to connect to the internet or server. Please check if the physical connections are proper, or the parameters you entered are correct.

5.2 Configuring multiple WAN ports

The router supports **3** WAN ports at most. The multi-WAN port feature lets you aggregate bandwidth, enjoy uninterrupted broadband service even in case of one connection malfunctions, and make ISP route selection, thus getting a better utilization of your bandwidth.

Assume that:

WAN1 internet connection type is **Static IP,** and the static IP information is as follows:

IP Address	192.168.97.86
Subnet Mask	255.255.255.0
Default Gateway	192.168.97.1
Primary DNS	192.168.108.107
Secondary DNS	192.168.108.108

WAN2 internet connection type is **Dynamic IP.**

Configuration procedure:

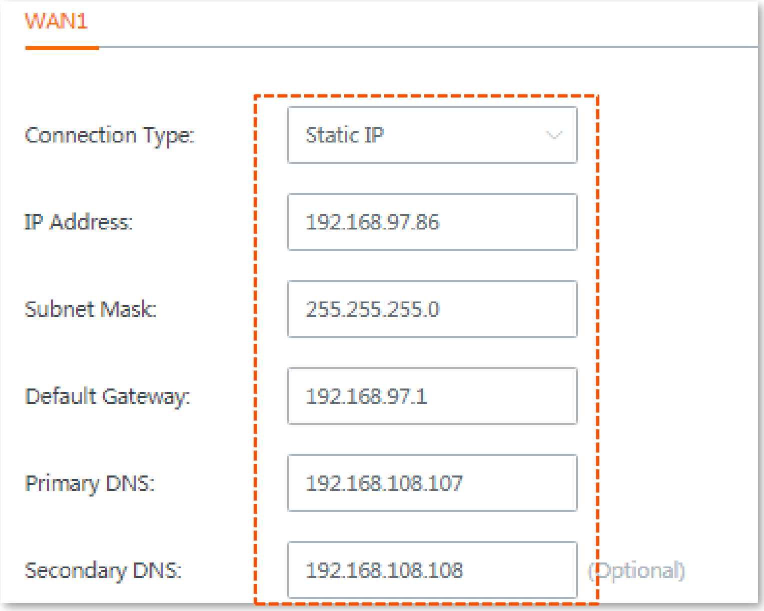
TIP

- Parameters for internet access are provided by your ISP. Refer to Choose your connection type table for detailed description. Values used here are only for examples.
- Modifying number of WAN port makes the router reboot.
- The following procedure describes how to configure 2 WAN ports. You can refer to the following steps to increase or decrease WAN ports as needed.

Step 1 Select the number of WAN ports from the **WAN Ports** drop-down list menu, which is **2** in this example.

The port marked with **LAN2** changes into **WAN2**, and the WAN2 configuration area appears.

Step 2 On **WAN1** configuration area, enter the static IP information provided by your ISP. The following figure is only for example.


WAN1

Connection Type: Static IP

IP Address: 192.168.97.86

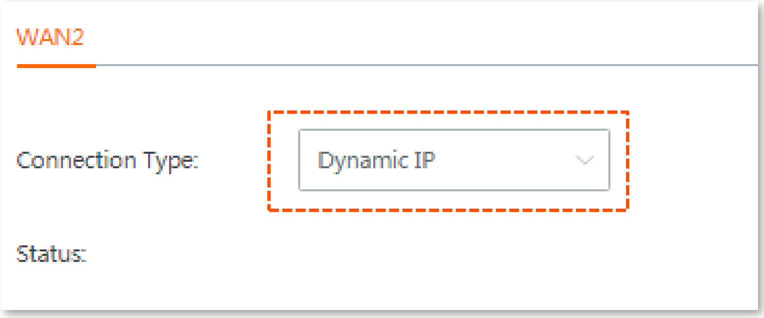
Subnet Mask: 255.255.255.0

Default Gateway: 192.168.97.1

Primary DNS: 192.168.108.107

Secondary DNS: 192.168.108.108 (Optional)

Step 3 On **WAN2** configuration area, select **Dynamic IP** from the drop-down list menu of **Connection Type.**


WAN2

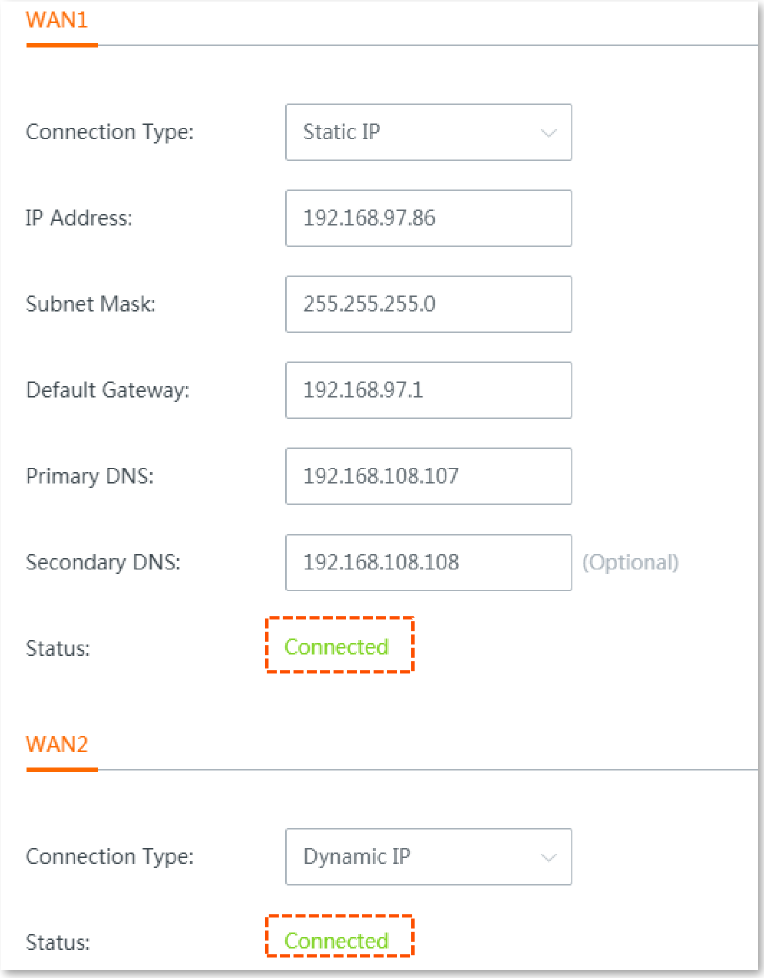
Connection Type: Dynamic IP

Status:

Step 4 Click **Save** at the bottom of the page.

---- End

Wait a moment. The router performs rebooting to apply your settings. When the status shows **Connected**, your configuration is successful. See the following figure:



WAN1

Connection Type: Static IP

IP Address: 192.168.97.86

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.97.1

Primary DNS: 192.168.108.107

Secondary DNS: 192.168.108.108 (Optional)

Status: Connected

WAN2

Connection Type: Dynamic IP

Status: Connected

5.3 Setting up to access the internet

This section describes how to set up to access the internet using different connection types.

Choose the proper connection type according to your actual environment. Use the table below to help you select your internet connection type if you are uncertain about how to select one.

Choose your connection type:

Connection Type	Parameters available
PPPoE	Your ISP provided you the PPPoE username and password.
Dynamic IP	Your ISP automatically assigns you a dynamic IP address.
Static IP	Your ISP provided you IP address, subnet mask, default gateway, DNS and so on.

5.3.1 Setting up to internet access with PPPoE

TIP

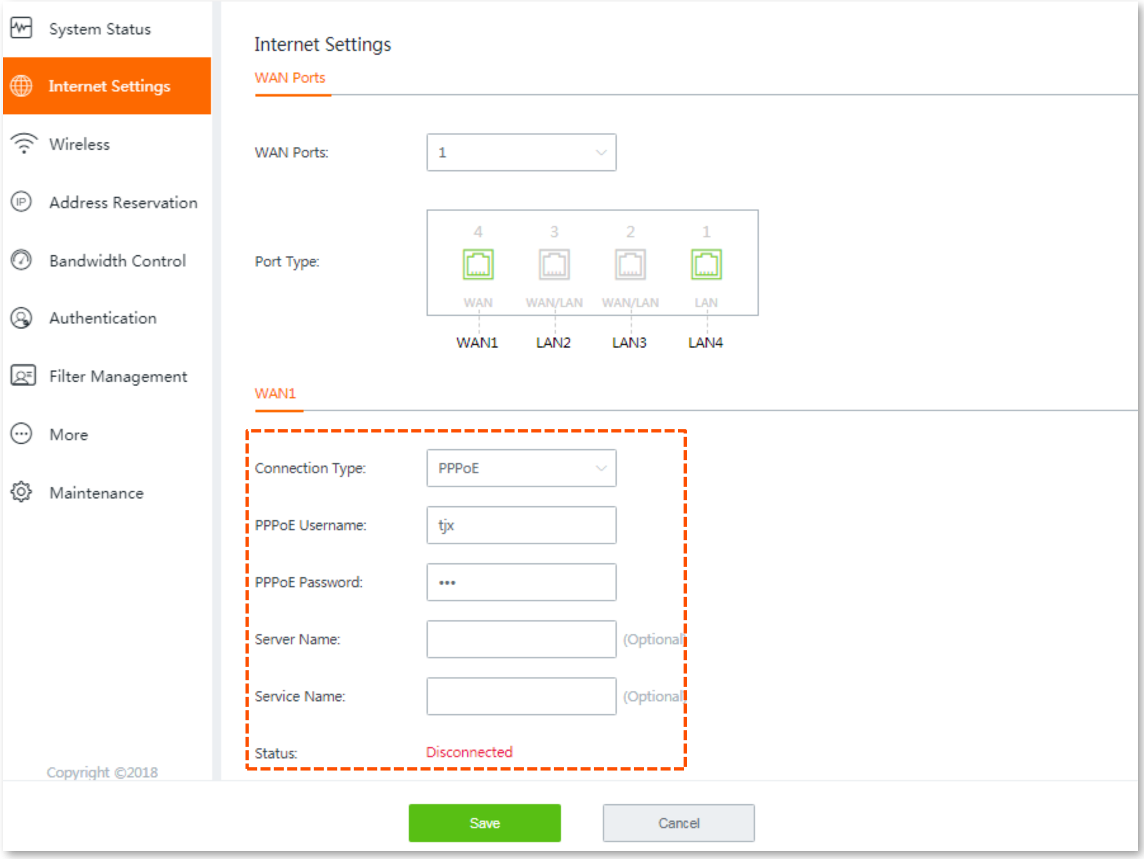
The following takes WAN1 for example.

Step 1 Choose **Internet Settings,** the configuration page appears.

Step 2 Select **PPPoE** from the drop-down list menu of **Connection Type**.

Step 3 Enter the **PPPoE Username** and **PPPoE Password** provided by your ISP.

Step 4 Click **Save** at the bottom of the page to apply your settings.



Internet Settings

WAN Ports

WAN Ports: 1

Port Type:

WAN1

Connection Type: PPPoE

PPPoE Username: tjx

PPPoE Password: •••

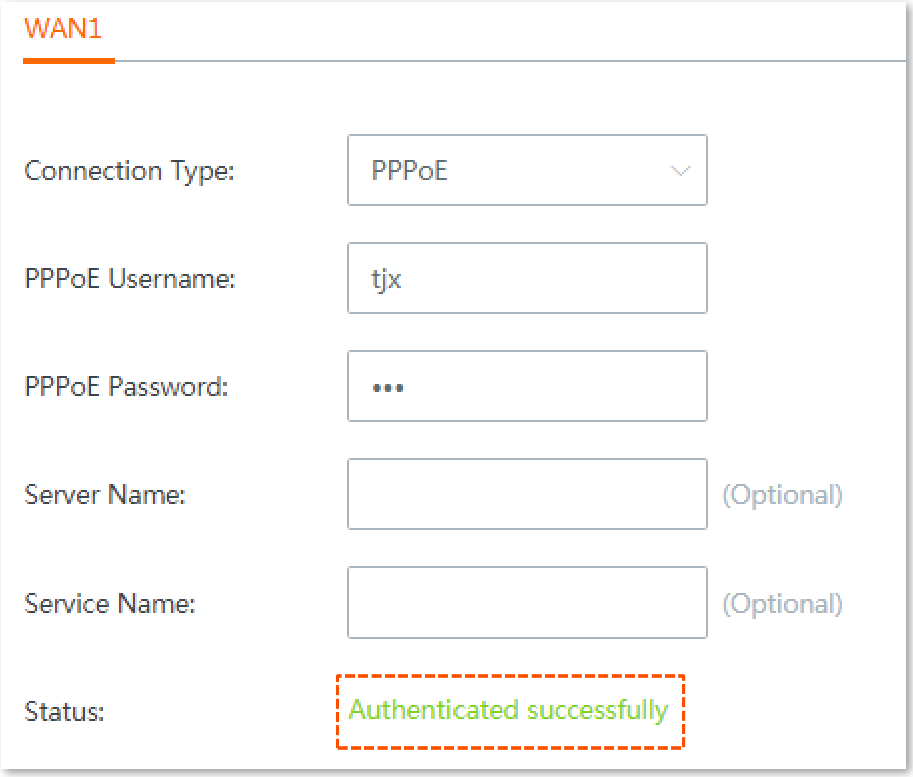
Server Name: (Optional)

Service Name: (Optional)

Status: Disconnected

---- End

Wait for the router to complete rebooting. The router connects to the internet successfully when the **Status** shows **Authenticated successfully**. Otherwise, check if the parameters you entered are correct.



WAN1

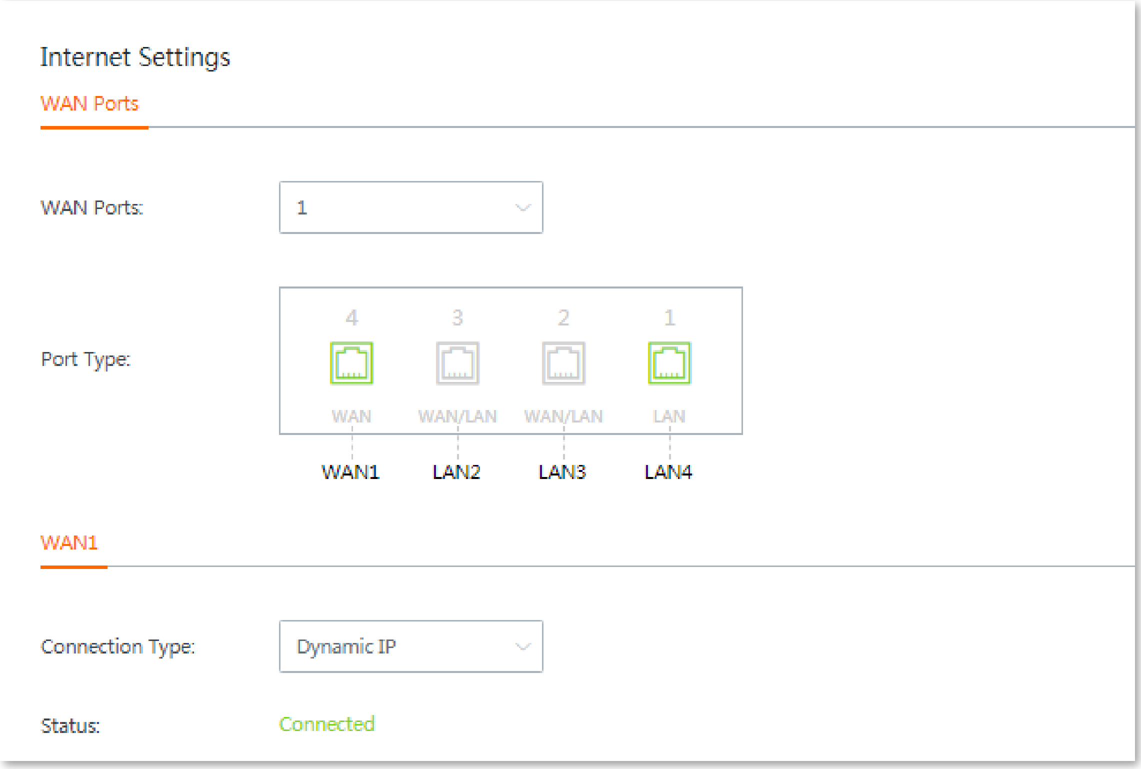
Connection Type:	PPPoE	
PPPoE Username:	tjx	
PPPoE Password:	•••	
Server Name:		(Optional)
Service Name:		(Optional)
Status:	Authenticated successfully	

5.3.2 Setting up to internet access with dynamic IP

Step 1 Click **Internet Settings**, the configuration page appears.

Step 2 Select **Dynamic IP** from the **Connection Type** drop-down list menu.

Step 3 Click **Save** at the bottom of the page to apply your settings.



Internet Settings

WAN Ports

WAN Ports: 1

Port Type:

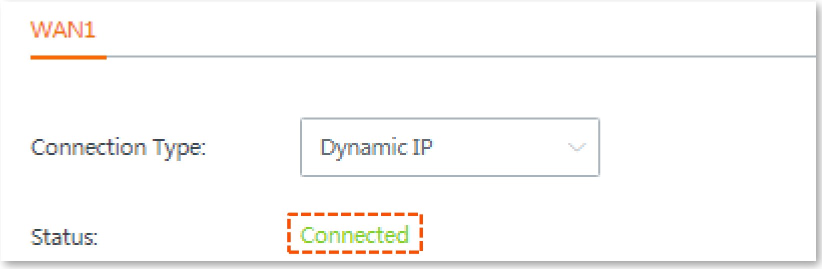
WAN1

Connection Type: Dynamic IP

Status: Connected

---- **End**

Wait for the router to complete rebooting. The router connects to the internet successfully when the **Status** shows **Connected**. You can enjoy internet now.



WAN1

Connection Type: Dynamic IP

Status: Connected

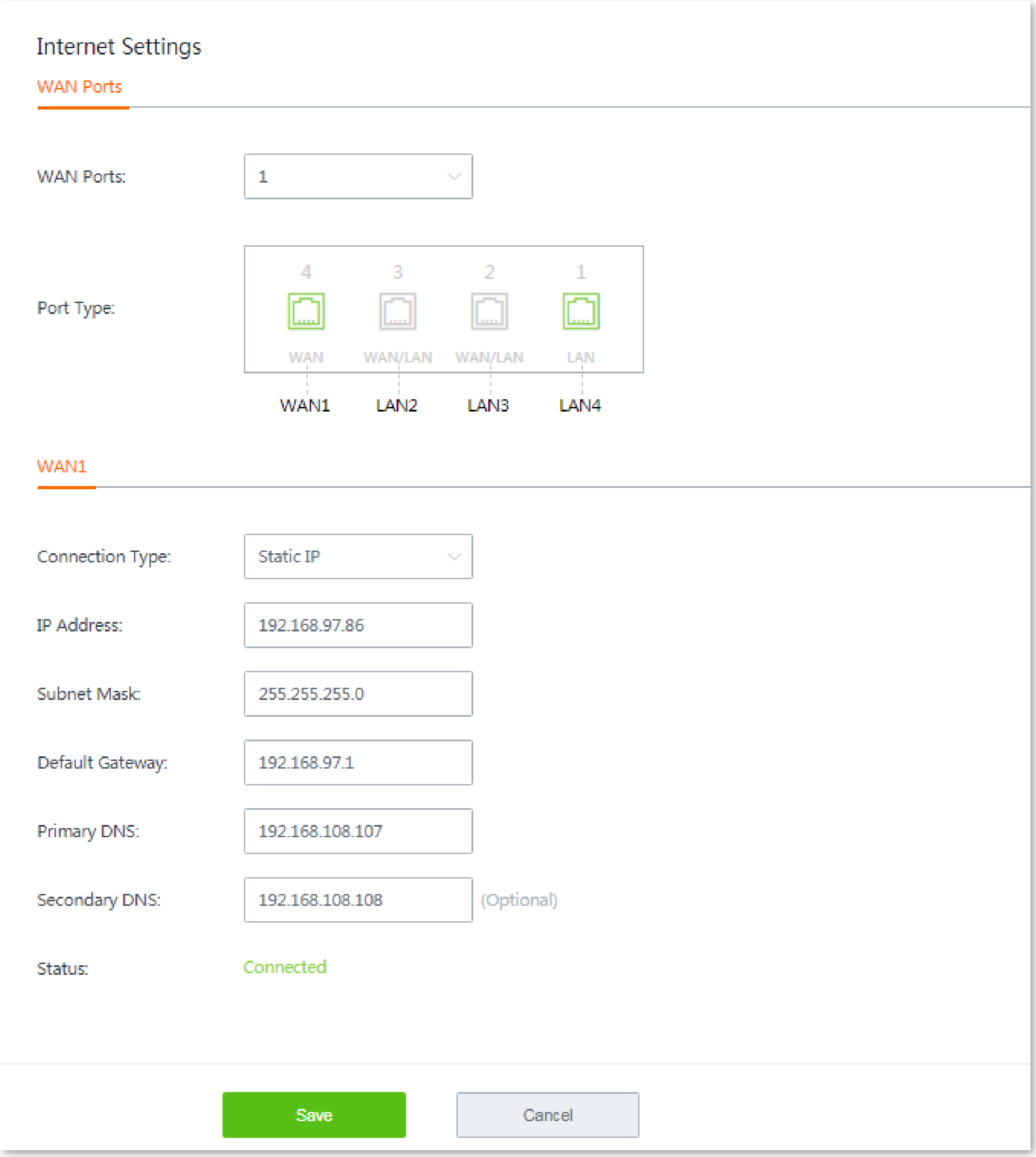
5.3.3 Setting up to internet access with static IP

Step 1 Click **Internet Settings**, the configuration page appears.

Step 2 Select **Static IP** from the drop-down list menu of **Connection Type**.

Step 3 Enter the **IP Address**, **Subnet Mask**, **Default Gateway and Primary/Secondary DNS parameters** provided by your ISP. Configurations on the following figure are only used for examples.

Step 4 Click **Save** at the bottom of the page to apply your settings.



Internet Settings

WAN Ports

WAN Ports: 1

Port Type:

WAN1

Connection Type: Static IP

IP Address: 192.168.97.86

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.97.1

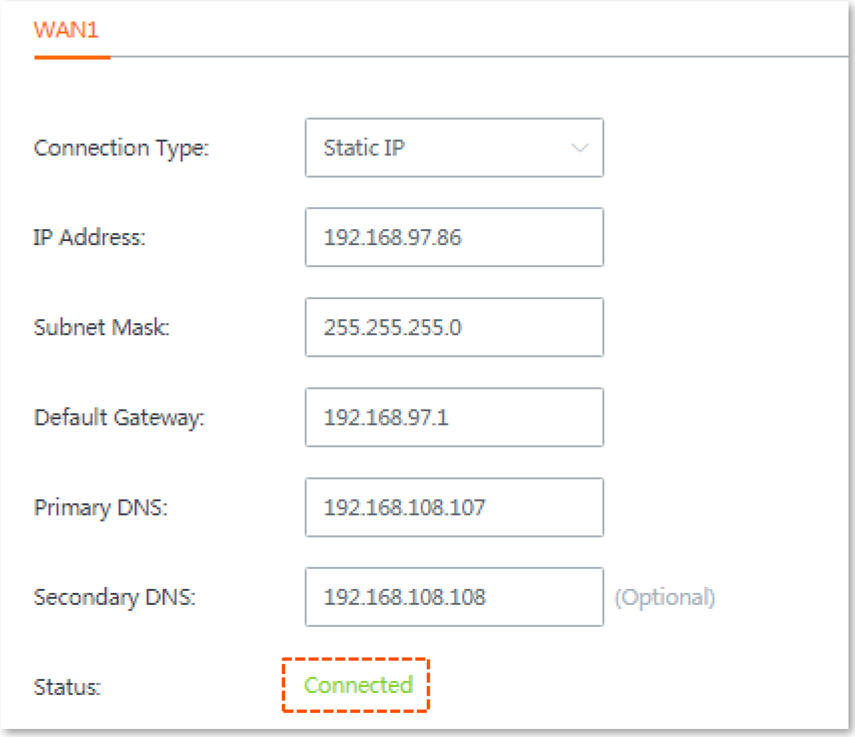
Primary DNS: 192.168.108.107

Secondary DNS: 192.168.108.108 (Optional)

Status: Connected

---- End

Wait for the router to complete rebooting. The router connects to the internet successfully when the **Status** shows **Connected**. You can enjoy internet now.


WAN1

Connection Type: Static IP

IP Address: 192.168.97.86

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.97.1

Primary DNS: 192.168.108.107

Secondary DNS: 192.168.108.108 (Optional)

Status: Connected

6 Wireless

6.1 Overview

This chapter describes:

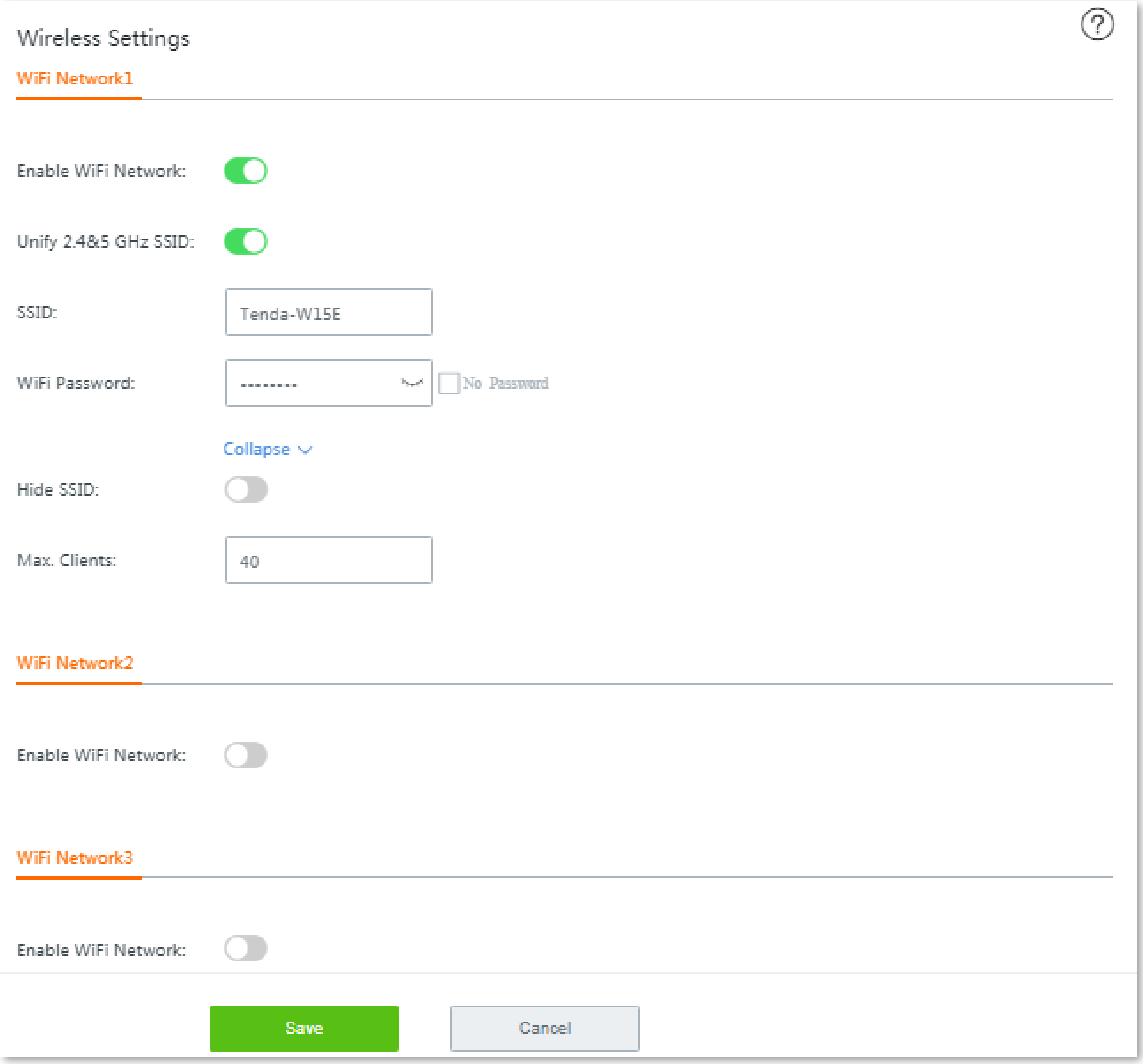
- Wireless settings
- Network isolation
- MAC filters
- Advanced settings
- Configuting guest network

6.2 Wireless settings

This dual-band router supports at most three 2.4 GHz wireless networks, and three 5 GHz wireless networks. By default, the 2.4 GHz and 5 GHz SSIDs for a wireless network are unified, and only **WiFi Network1** is enabled.

In this module, you are allowed to set up WiFi network-related configurations, such as view and edit wireless network names (SSID), WiFi passwords, configure 2.4 GHz and 5 GHz WiFi networks separately, hide your WiFi network so that nearby wireless clients cannot detect it, and specify how many wireless clients can connect to a wireless network.

To enter the configuration page, choose **Wireless** > **Wireless Settings**. See the following figure:



Wireless Settings

WiFi Network1

Enable WiFi Network: ●

Unify 2.4&5 GHz SSID: ●

SSID: Tenda-W15E

WiFi Password: •••••••• □ No Password

Hide SSID: ○

Max. Clients: 40

WiFi Network2

Enable WiFi Network: ○

WiFi Network3

Enable WiFi Network: ○

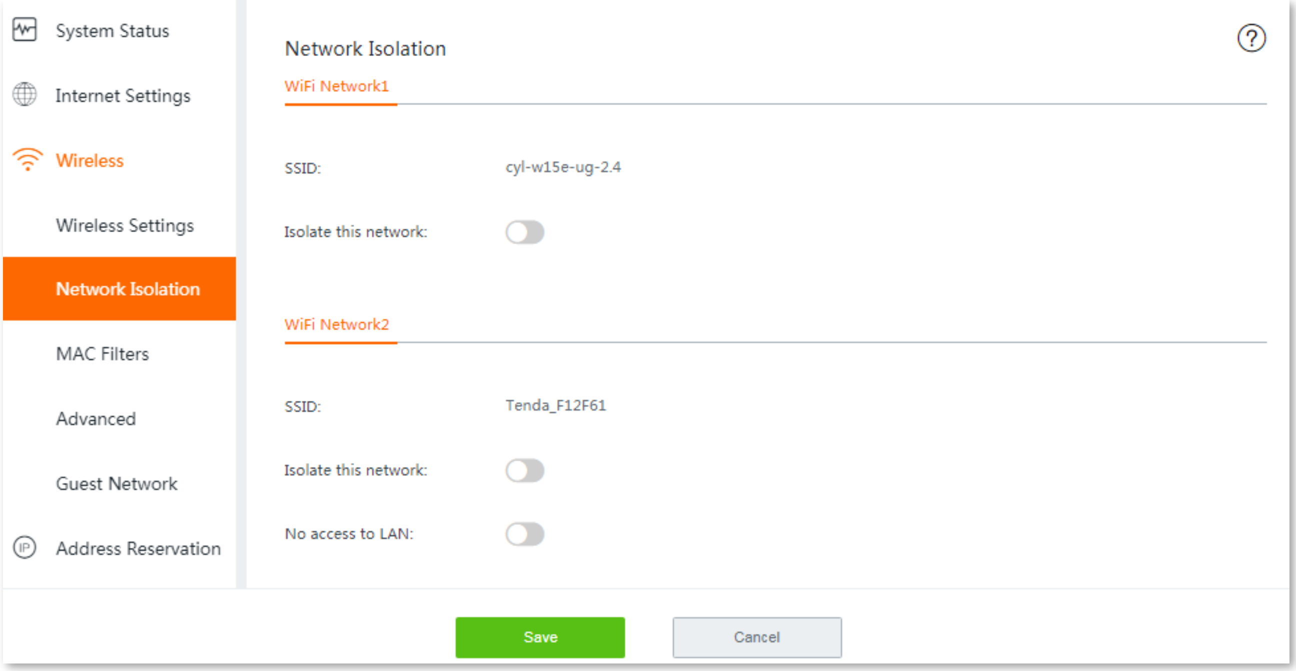
Parameter description

Parameter	Description
Enable WiFi Network	Used to enable/disable the wireless network of the router.
Unify 2.4&5 GHz SSID	Whether to unify SSIDs for 2.4 GHz and 5 GHz wireless networks.
SSID	Wireless network name of the corresponding WiFi network.
WiFi Password	Password used for wireless internet connection. You are recommended to use the combination of digits, letters and special characters for higher security. Selecting **No Password** indicates that wireless clients can connect to the wireless network without a password. Select this option only when necessary since it leads to weak network security.
Hide SSID	With this function enabled, nearby wireless clients cannot detect the SSID, and you need to manually enter the SSID on the wireless client to access the wireless network. Disable indicates that nearby wireless clients can detect the SSID. By

Parameter	Description
	default, this function is disabled.
Max. Clients	Maximum number of wireless clients that can be connected to the wireless network with the SSID. After the value is reached, this wireless network denies new connection requests. Clients connected to all the enabled wireless networks (including guest networks) of the router cannot exceed 128 on 2.4 GHz and 5 GHz bands respectively. If you enable multiple SSIDs, plan your maximum number of clients to each SSID first.

6.3 Network isolation

Isolating a network makes clients connected to it **cannot** communicate with clients connected to another network. To access the configuration page, choose **Wireless** > **Network Isolation**. See the following figure:



Network Isolation

WiFi Network1

SSID: cyl-w15e-ug-2.4

Isolate this network: ○

WiFi Network2

SSID: Tenda_F12F61

Isolate this network: ○

No access to LAN: ○

Parameter description

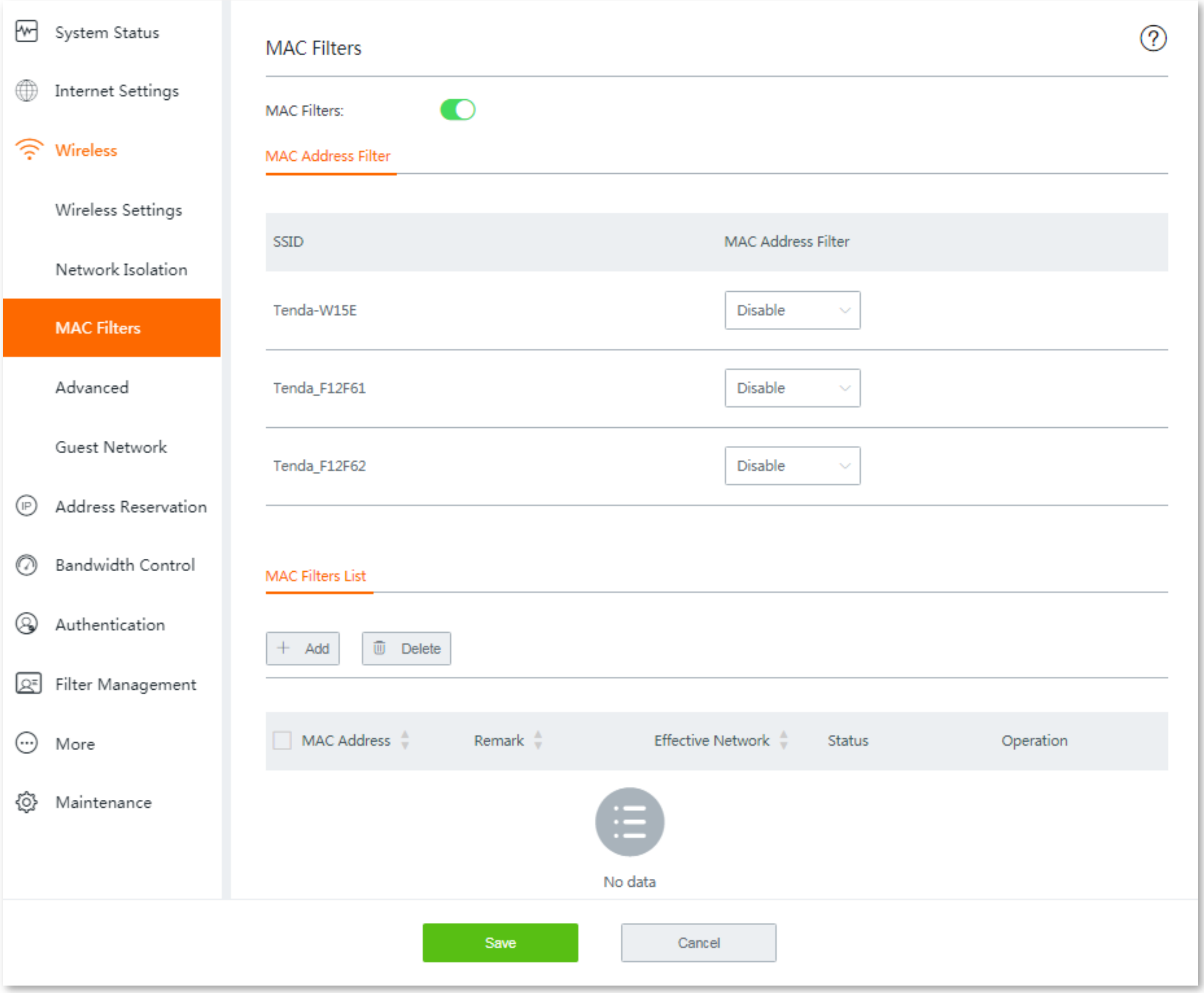
Parameter	Description
SSID	Wireless network name of the corresponding WiFi network.
Isolate this network	With this function enabled, clients connected to different wireless networks of this device cannot communicate with each other, leading to higher wireless network security. By default, this function is disabled.
No access to LAN	This function is only applicable to **WiFi Network2/3**. With this function enabled, clients connected to this wireless network cannot access the web UI and private network (LAN) of this router, protecting your LAN network security. By default, this function is disabled.

6.4 MAC filters

6.4.1 Overview

This module allows you to configure MAC address-based wireless access control rules. To enter the configuration page, choose **Wireless** > **MAC Filters**. By default, this function is disabled.

To enable this function, set the **MAC Filters** from ○ to ●, and click **Save** at the bottom of the page. The following configuration area appears:



MAC Filters: ●

SSID	MAC Address Filter
Tenda-W15E	Disable
Tenda_F12F61	Disable
Tenda_F12F62	Disable

□ MAC Address	Remark	Effective Network	Status	Operation

Parameter description

Parameter		Description
MAC Address Filter	SSID	It lists all the **main** wireless networks that the router supports. TIP If you unify the SSIDs for 2.4 GHz and 5 GHz bands, the corresponding wireless network only displays one SSID here.
	MAC Address Filter	It specifies the modes you can perform on the corresponding wireless network. There are three modes for selection: - **Disable**: This function is disabled, and all wireless clients can connect to

Parameter		Description
		this wireless network. - **Only Allow**: Only wireless clients with the specified MAC address **can** connect to this wireless network. - **Only Forbid**: Only wireless clients with the specified MAC address **cannot** connect to this wireless network.
MAC Filters List	MAC Filters List	It specifies the wireless access control list you configured.
	MAC Address	It specifies the MAC address of the client to which the rule applies.
	Remark	(Optional) It specifies the brief description you set for the corresponding MAC address.
	Effective Network	It specifies the wireless network(s) to which the wireless client with this MAC address applies.
	Status	It specifies whether or not the rule is enabled.

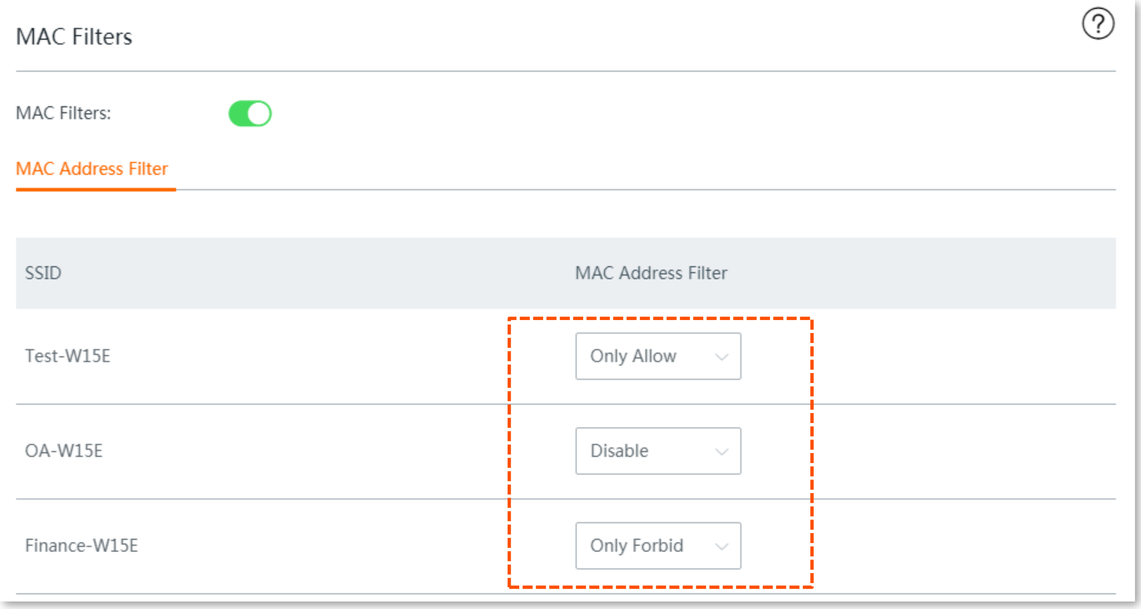
6.4.2 Configuring a MAC filter rule

NOTE

- A maximum of **64** rules is allowed for each SSID, and **100** rules for each frequency band.
- The MAC filter rule will be invalidated if the SSID it maps has been changed. You are required to manually choose an enabled wireless network to apply the MAC filter rule.

Step 1 Enable **MAC Filters**, and click **Save** at the bottom on the page.

Step 2 Configure MAC address filter mode for each SSID by selecting from the **MAC Address Filter** drop-down list menu.



MAC Filters

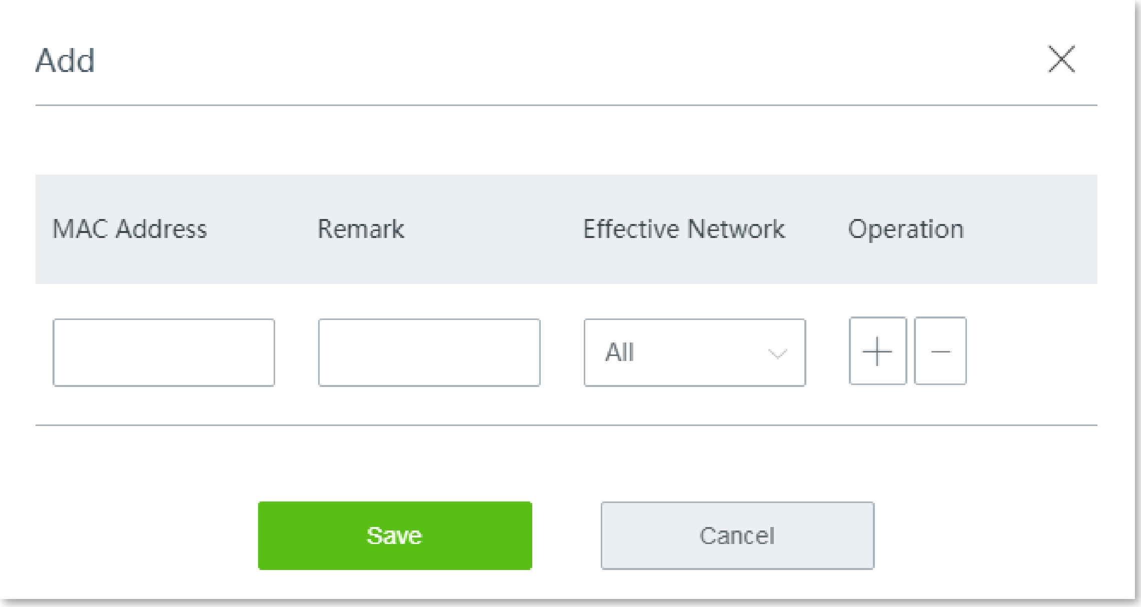
MAC Filters: ●

MAC Address Filter

SSID	MAC Address Filter
Test-W15E	Only Allow
OA-W15E	Disable
Finance-W15E	Only Forbid

Step 3 Add rule(s).

1. Click **Add**. The **Add** configuration window appears.



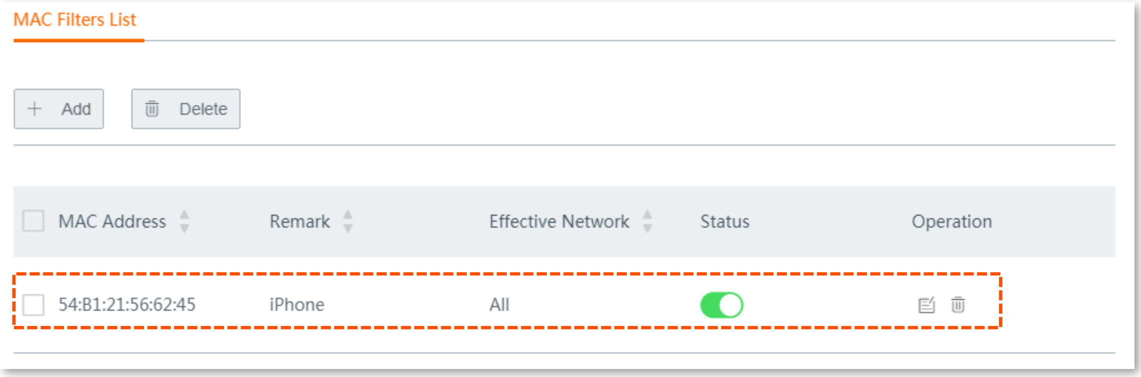
Add

MAC Address	Remark	Effective Network	Operation
		All	+ −

2. Enter the description of the client in **Remark**, and select the wireless network from the drop-down list menu of the **Effective Network**.
3. Click **Save**. The rule appears on the **MAC Filter List**.

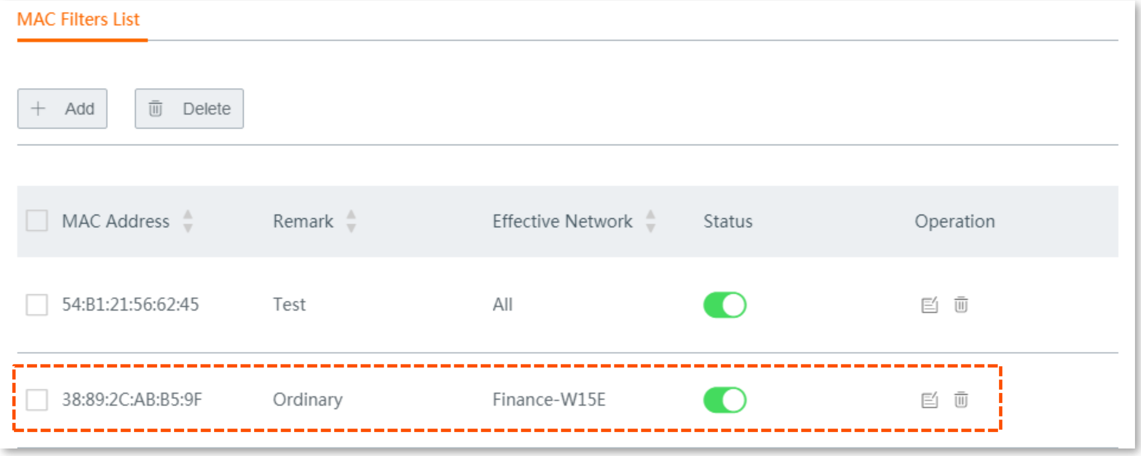
TIP

Parameters on the following figure are only used for examples. Please specify them based on your actual conditions.



□	MAC Address	Remark	Effective Network	Status	Operation
□	54:B1:21:56:62:45	iPhone	All	●	

4. Repeat Step 2 Add rule(s to add other clients one by one.

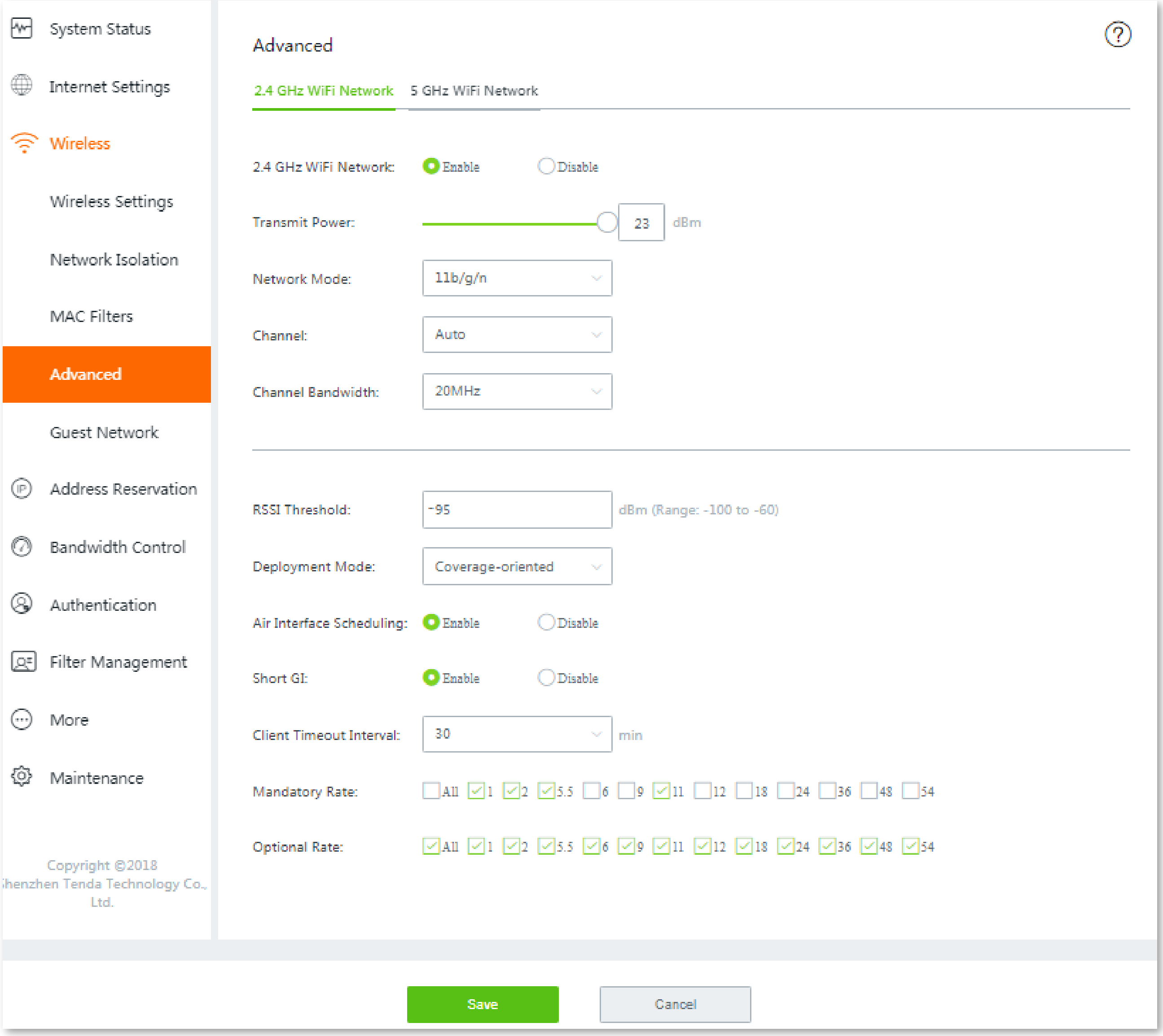


□	MAC Address	Remark	Effective Network	Status	Operation
□	54:B1:21:56:62:45	Test	All	●	
□	38:89:2C:AB:B5:9F	Ordinary	Finance-W15E	●	

---- End

6.5 Advanced settings

This section introduces wireless-related advanced settings. To enter the configuration page, choose **Wireless** > **Advanced**. See the following figure:



Advanced

2.4 GHz WiFi Network | 5 GHz WiFi Network

2.4 GHz WiFi Network: ● Enable ○ Disable

Transmit Power: 23 dBm

Network Mode: 11b/g/n

Channel: Auto

Channel Bandwidth: 20MHz

RSSI Threshold: -95 dBm (Range: -100 to -60)

Deployment Mode: Coverage-oriented

Air Interface Scheduling: ● Enable ○ Disable

Short GI: ● Enable ○ Disable

Client Timeout Interval: 30 min

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

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

Parameter description

Parameter	Description
2.4 GHz WiFi Network	Used to enable or disable the 2.4 GHz wireless network of the router.
5 GHz WiFi Network	Used to enable or disable the 5 GHz wireless network of the router.
Transmit Power	Transmit power of this device. A higher value leads to wider WiFi coverage. However, decreasing the value properly increases performance and security of the wireless network.
Network Mode	It specifies the wireless network mode (also called 802.11 mode, radio mode, or wireless mode) of the router. A proper network mode enables the clients to get the maximum transfer rate and compatibility.

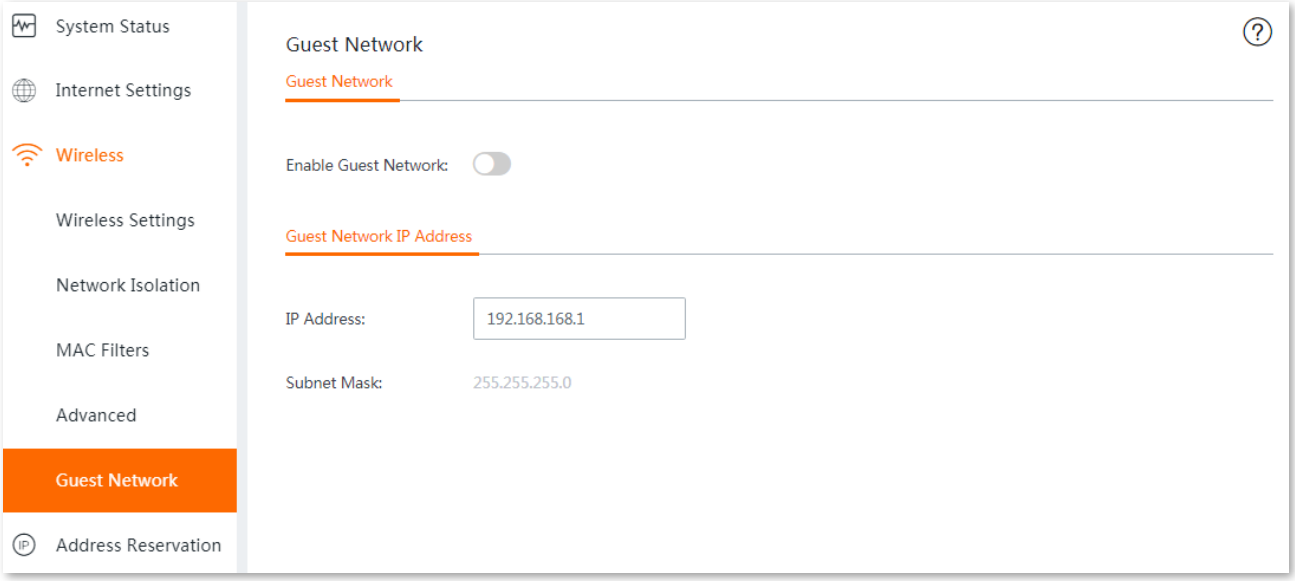
Parameter	Description
	Available options for **2.4 GHz** band: **11b**, **11g**, **11b/g**, and **11b/g/n** (default). Available options for **5 GHz** band: **11a**, **11ac** (default), and **11a/n mixed**. You are recommended to keep the default settings.
Channel	Specify the channel in which this device operates. Select one idle channel in the ambient environment to prevent interference. **Auto** indicates that this device automatically changes to a channel rarely used in the ambient environment to prevent interference.
Channel Bandwidth	Select the channel bandwidth to accommodate higher transmission speed. Available options for **2.4 GHz** band: **20MHz** (default), **40MHz**, and **20/40MHz**. Available options for **5 GHz** band: **20MHz**, **40MHz**, and **80MHz** (default).
RSSI Threshold	It specifies the minimum wireless client signal strength acceptable to the router. A mobile client with signal strength lower than this threshold cannot connect to the router. You can set this parameter to ensure that mobile clients connect to router with strong signal strength.
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: - **Coverage-oriented**: Apply to scenarios with large area, multiple walls, decentralized users and less than 10 SSIDs in ambient environment. - **Capacity-oriented**: Apply to scenarios with intensive users, open and large areas, and more than 25 SSIDs in ambient environment.
Prioritize 5 GHz	It specifies that a wireless client uses the 5 GHz SSID first to connect to the device if the wireless client supports both 5 GHz and 2.4 GHz networks and the networks use the same SSID and password. NOTE - To make this function take effect, the SSID cannot contain any Chinese characters. - The default RSSI threshold to enable this function is **-80** dBm. You can adjust the threshold by customizing the **Prioritize Threshold 5 GHz** parameter.
Prioritize Threshold 5 GHz	It specifies the RSSI threshold value to trigger the **Prioritize 5 GHz** function. The default value is **-80** dBm. You are recommended to keep the default settings.
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.
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

Parameter	Description
	helps reduce power consumption. By default, this mode is disabled.
Client Timeout Interval	It specifies the maximum period before a WiFi client is disconnected from the router if the client exchanges no data with the router. When data is exchanged within the period, countdown stops.
Short GI	Short guard interval for preventing data block interference. Propagation delays may occur on the receiver side due to factors such as multipath wireless signal transmission. If a data block is transmitted at an overly high speed, it may interfere with the previous data block. The short GI helps prevent such interference. Enabling the short GI can yield a 10% improvement in wireless data throughput.
Mandatory Rate	It specifies the basic rate sets that wireless clients must meet to connect to the router. Wireless clients are denied by the router if they fail to match the basic rate sets ticked here. NOTE You are recommended to keep the default settings. If you need to modify them, please do under professional guidance.
Optional Rate	It specifies that any connected wireless clients that support the data rate options ticked here may communicate with the router using that rate. NOTE You are recommended to keep the default settings. If you need to modify them, please do under professional guidance.

6.6 Configuting guest network

This section introduces guest network. You can configure a guest network for visitors to protect the security of the main network. In addition, the router allows you to set a guest network segment different from the main network.

To access the configuration page, choose **Wireless** > **Guest Network**. See the following figure. By default, this function is disabled.



Guest Network

Guest Network

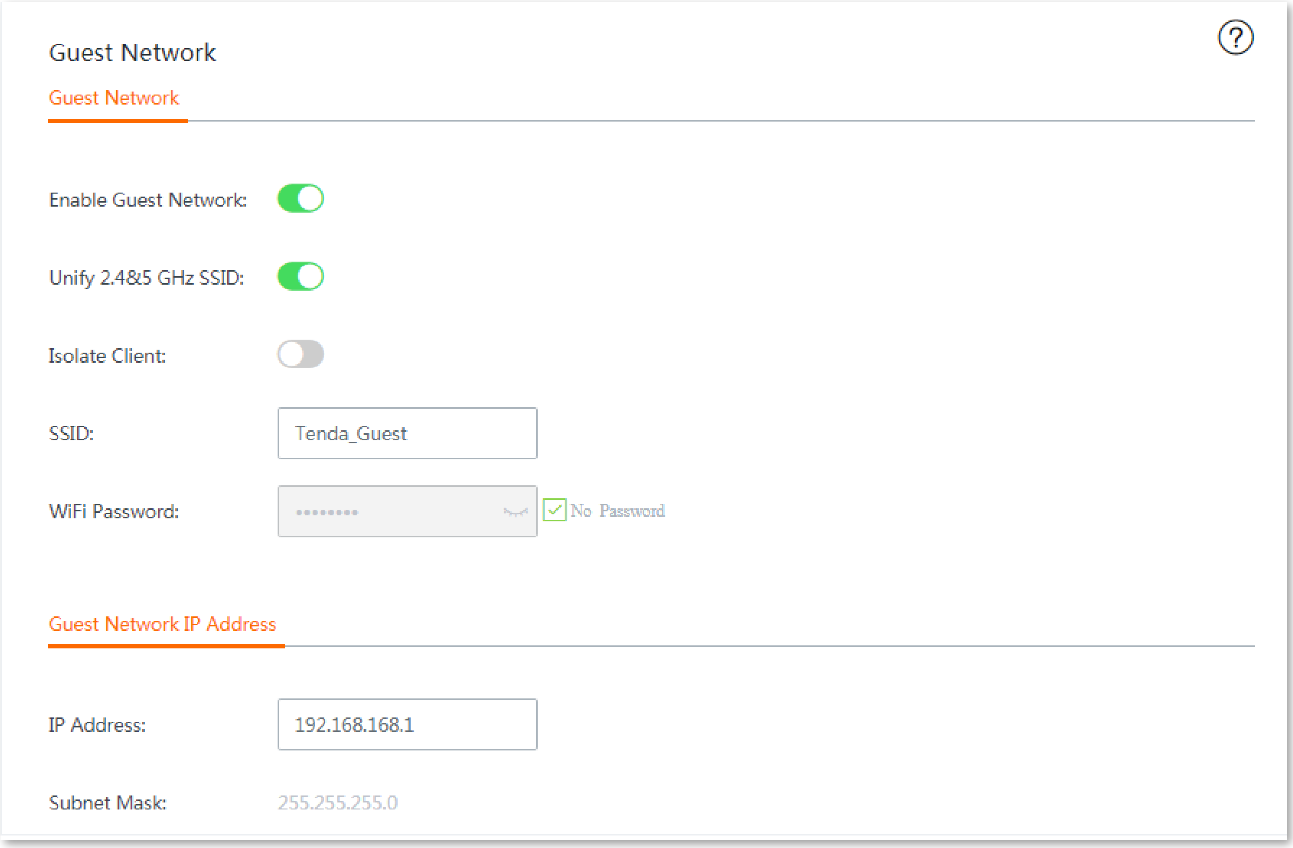
Enable Guest Network: ○

Guest Network IP Address

IP Address: 192.168.168.1

Subnet Mask: 255.255.255.0

Enable this function, the following page appears:



Guest Network

Guest Network

Enable Guest Network: ●

Unify 2.4&5 GHz SSID: ●

Isolate Client: ○

SSID: Tenda_Guest

WiFi Password: •••••••• ☑ No Password

Guest Network IP Address

IP Address: 192.168.168.1

Subnet Mask: 255.255.255.0

Parameter description

Parameter		Description
Guest Network	Enable Guest Network	Used to enable or disable this function.
	Unify 2.4&5 GHz SSID	Used to unify SSIDs for 2.4 GHz and 5 GHz guest wireless networks.
	Isolate Client	With this function enabled, clients connected to the guest network cannot communicate with each other, leading to higher wireless network security.
	SSID	Wireless network name of the guest network. TIP To differentiate the main network and the guest network, you are recommended to set the SSIDs differently.
	WiFi Password	Password used for wireless internet connection. You are recommended to use the combination of digits, letters and special characters for higher security.
	No Password	Wireless clients can connect to the wireless guest network without a password. Select this option only when necessary since it leads to weak network security.
Guest Network IP Address	IP Address	It specifies the IP address (default: **192.168.168.1)** of the guest network. The router assigns 192.168.168.*X* to wireless clients connected to it. You are recommended to keep the default settings.
	Subnet Mask	Subnet mask of the guest network.

7 Address reservation

The address reservation function always allows a host, such as a computer, on LAN to receive the same IP address each time when they connect to the DHCP server. If there are some hosts on LAN that require static IP addresses, you can configure the address reservation for this purpose.

This chapter introduces:

- Configuring on-line client-based quick address reservation.
- Configuring address reservation manually.
- Exporting/importing your address reservation configuration.

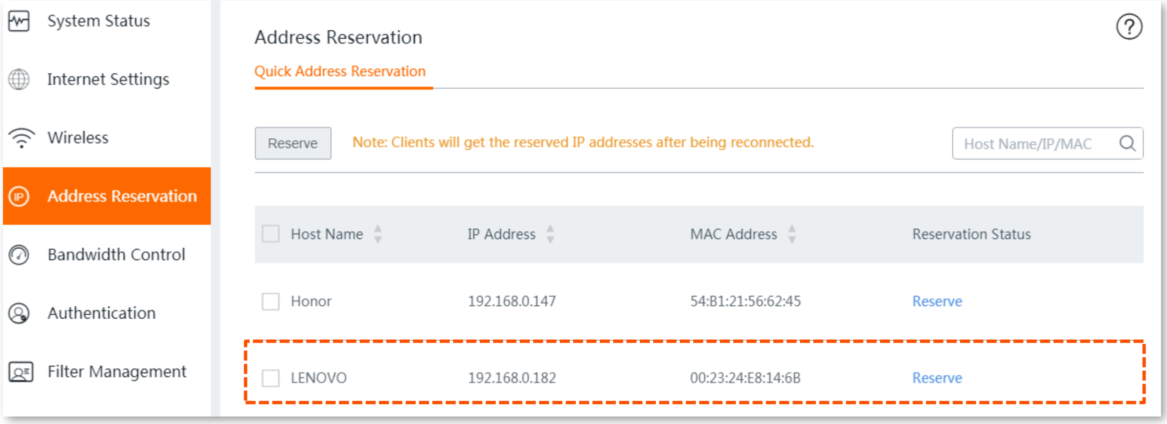
7.1 Configuring on-line client-based quick address reservation

The router allows you to conveniently reserve static IP addresses for on-line hosts one by one or in batch. Choose your scenario and perform steps below.

7.1.1 Configuring on-line client-based quick address reservation one by one

Step 1 Choose **Address Reservation** to enter the configuration page.

Step 2 Locate the host you want to reserve a static IP address, which is **LENOVO** in this example, and click **Reserve** next to it.



Address Reservation

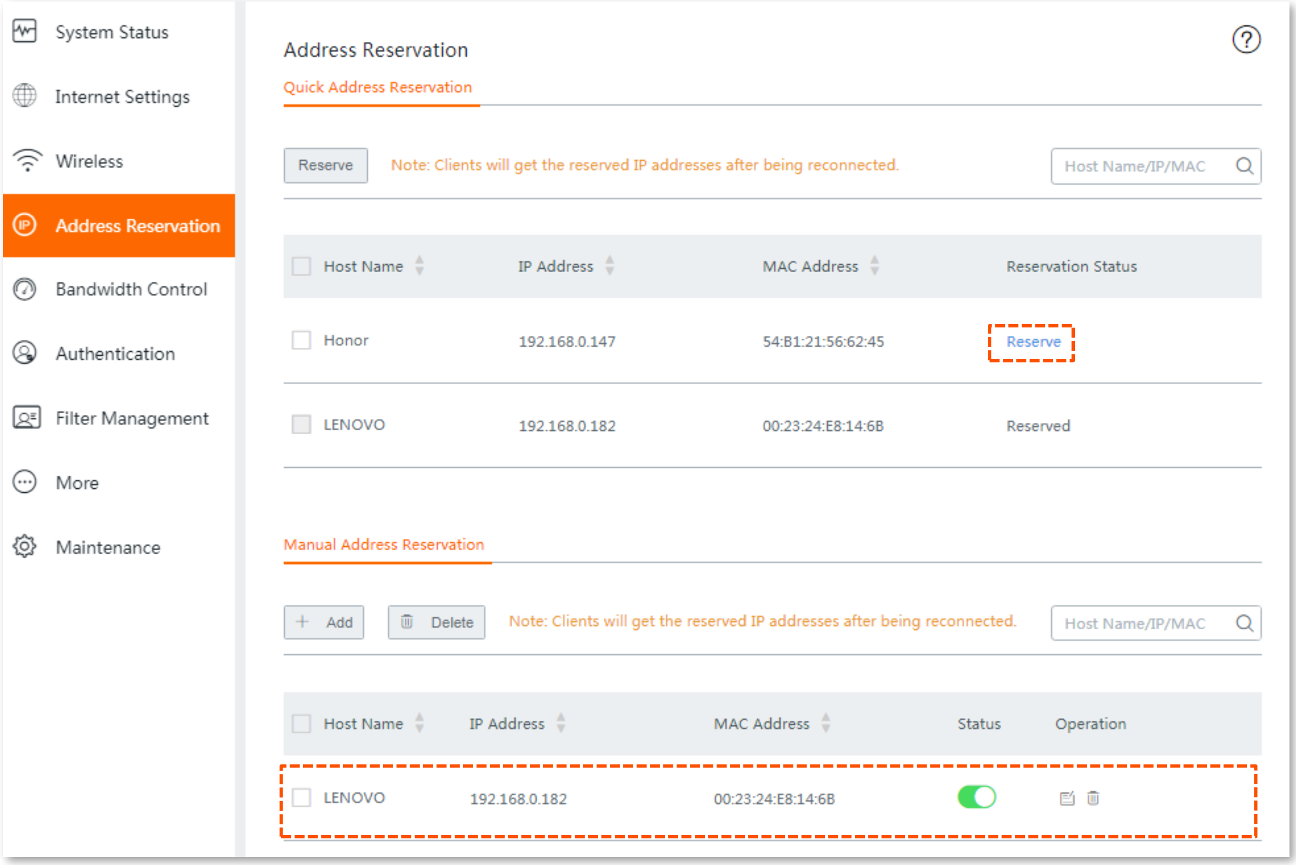
Quick Address Reservation

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

□ Host Name	IP Address	MAC Address	Reservation Status
□ Honor	192.168.0.147	54:B1:21:56:62:45	Reserve
□ LENOVO	192.168.0.182	00:23:24:E8:14:6B	Reserve

---- End

The **Reservation Status** of host named **LENOVO** is changed into **Reserved**, and displayed on the lower part of the page. See the following figure. Clients will get the reserved IP addresses after being reconnected.



Address Reservation

Quick Address Reservation

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

Host Name	IP Address	MAC Address	Reservation Status
□ Honor	192.168.0.147	54:B1:21:56:62:45	Reserve
□ LENOVO	192.168.0.182	00:23:24:E8:14:6B	Reserved

Manual Address Reservation

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

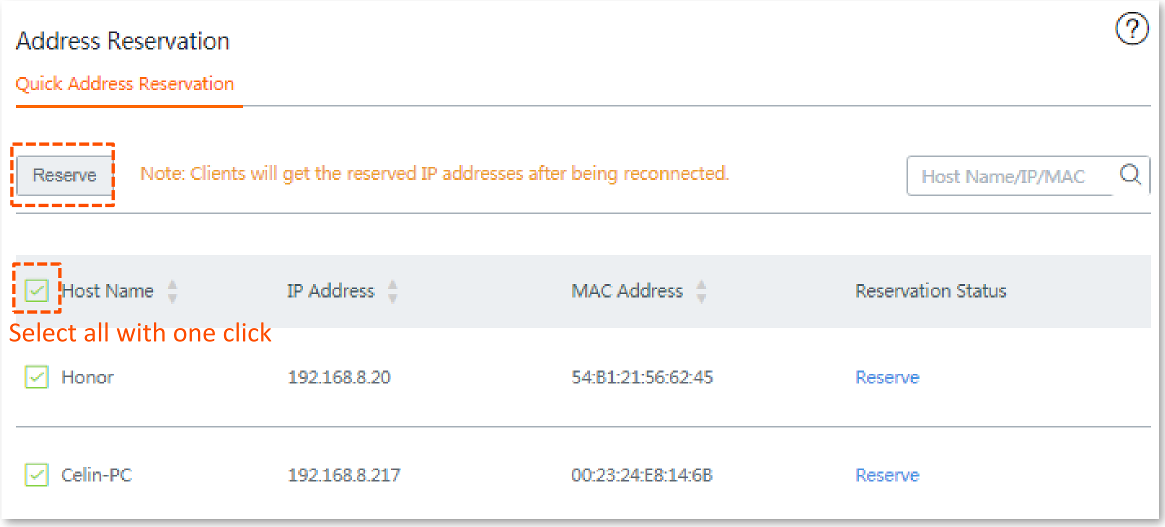
Host Name	IP Address	MAC Address	Status	Operation
□ LENOVO	192.168.0.182	00:23:24:E8:14:6B	●	

7.1.2 Configuring on-line client-based quick address reservation in batch

Step 1 Choose **Address Reservation** to enter the configuration page.

Step 2 Select hosts you want to reserve a static IP address, and click the **Reserve** button.

Or if you want to select all hosts on the list, check the checkbox next to **Host Name**.



Address Reservation

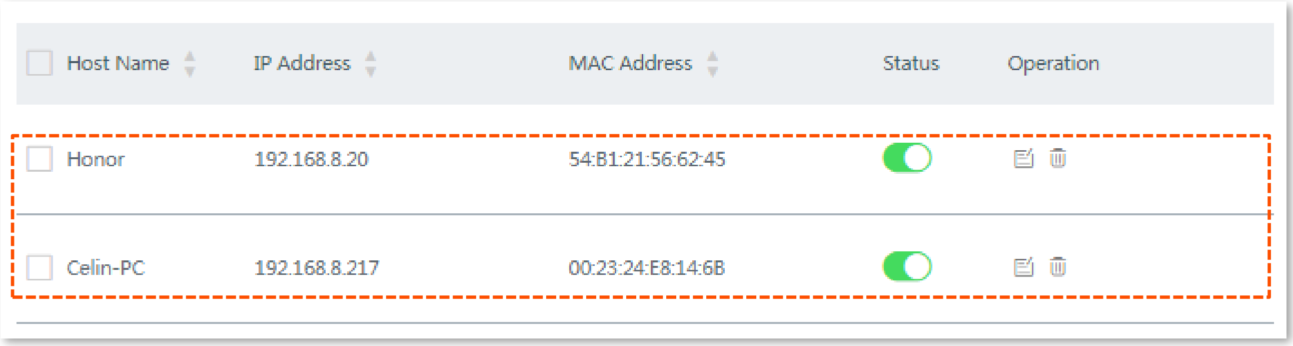
Quick Address Reservation

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

☑ Host Name	IP Address	MAC Address	Reservation Status
☑ Honor	192.168.8.20	54:B1:21:56:62:45	Reserve
☑ Celin-PC	192.168.8.217	00:23:24:E8:14:6B	Reserve

---- End

The **Reservation Status** of hosts are changed into **Reserved**, and displayed on the lower part of the page. See the following figure:



□	Host Name	IP Address	MAC Address	Status	Operation
□	Honor	192.168.8.20	54:B1:21:56:62:45	●	✎ 🗑
□	Celin-PC	192.168.8.217	00:23:24:E8:14:6B	●	✎ 🗑

7.2 Configuring address reservation manually

To reserve static IP addresses for hosts disconnected to the router, you can add the rule manually.

NOTE

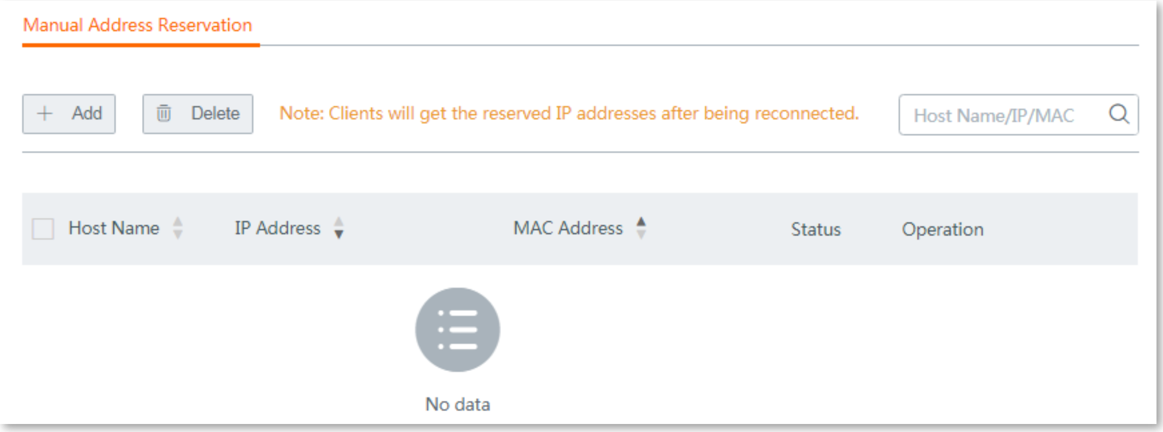
If the network segment of LAN IP of the router is modified in LAN settings, the IP address of the manually-reserved host will not change synchronously, but the rule remains effective.

Before you start

Obtain the IP addresses and MAC addresses of hosts you are going to add.

Configuration Procedure

Step 1 Choose **Address Reservation**, and move to the **Manual Address Reservation** configuration area. See the following figure.



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

Step 2 Click **+Add**. The **Add** configuration window appears.

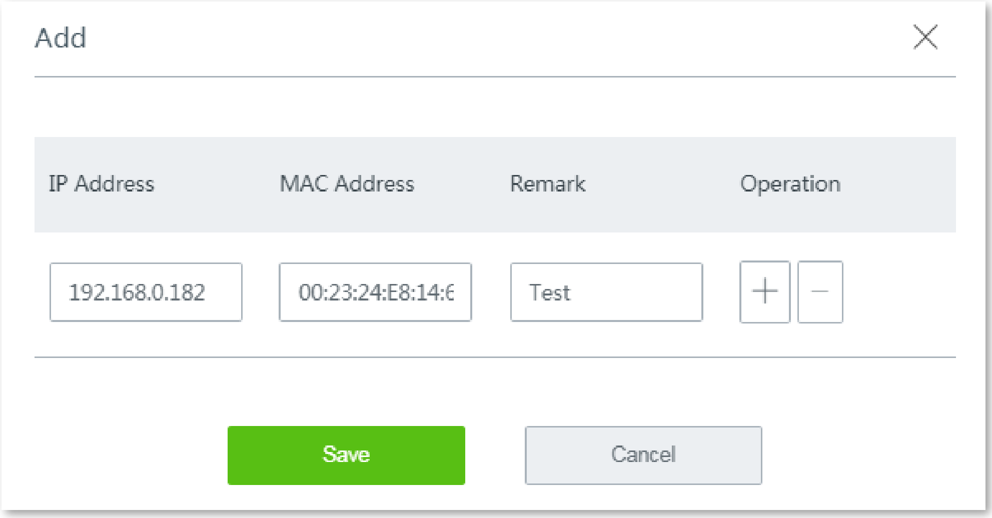
Step 3 Enter the **IP Address** and **MAC Address**, which is **192.168.0.182/00:23:24:E8:14:6B** in this example.

Step 4 (Optional) Add a brief description in the **Remark** filed, which is **Test** in this example.

TIP

For convenient management later, you are recommended to enter a brief description to distinguish different hosts.

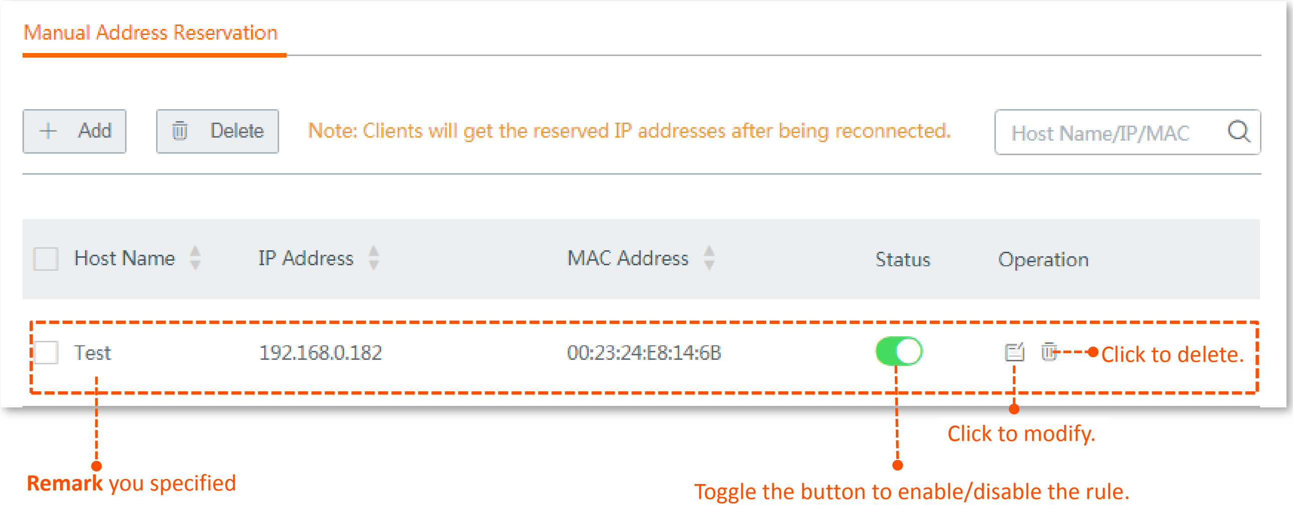
Step 5 Click **Save**.



IP Address	MAC Address	Remark	Operation
192.168.0.182	00:23:24:E8:14:6	Test	+ −

---- End

The **Reservation Status** of hosts are changed into **Reserved**, and displayed on the lower part of the page. See the following figure:



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

□ Host Name	IP Address	MAC Address	Status	Operation
□ Test	192.168.0.182	00:23:24:E8:14:6B	●	

Click to delete.

Click to modify.

Remark you specified

Toggle the button to enable/disable the rule.

7.3 Exporting/importing your address reservation configuration

The router supports to export the current configuration you set to your local PC for backup, and import the configuration file you backed up to the router, relieving your from repeated laborious efforts for configuration.

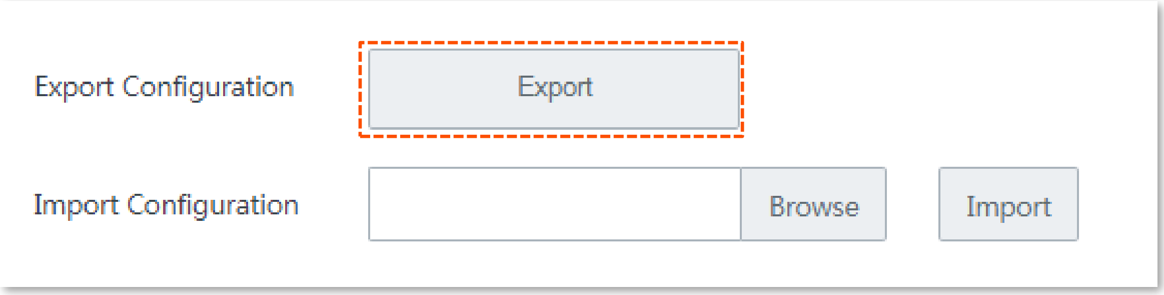
This section introduces:

- Exporting configuration file to your local PC.
- Importing configuration file to your router.

7.3.1 Exporting configuration file to your local PC

Step 1 Choose **Address Reservation**, and move to the bottom of the page.

Step 2 Click the **Export** button.



Export Configuration Export

Import Configuration Browse Import

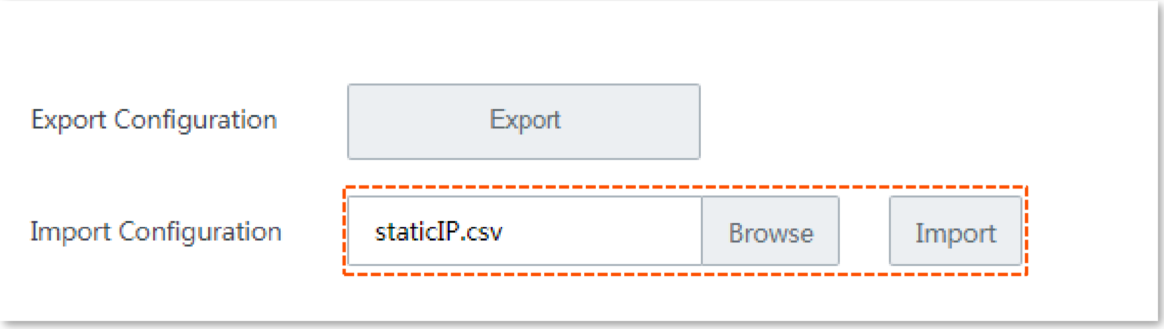
---- End

A file named **staicIP.csv** is exported to your local PC.

7.3.2 Importing configuration file to your router

Step 1 On the **Address Reservation** page, click **Browse**, and upload the address reservation configuration file you have backed up to your local PC.

Step 2 Click the **Import** button.



Export Configuration Export

Import Configuration staticIP.csv Browse Import

---- End

Your address reservation configurations have been imported to your router. You can check the imported configuration on this page.

8 Bandwidth control

8.1 Overview

Internet bandwidth is limited. Well-controlled traffic of users ensures that the bandwidth is properly used to effectively access resources over the internet.

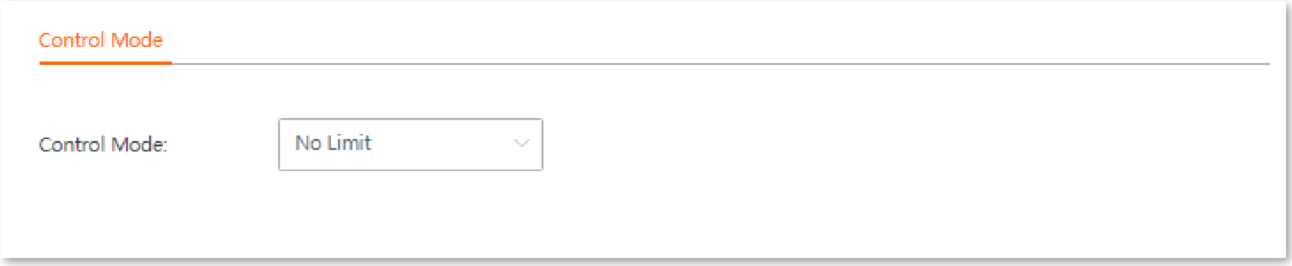
This chapter describes:

- Control mode description.
- Example of configuring group-based control rules.

8.2 Control mode description

The router allows you to control upload and download bandwidth for both online and offline clients with four control modes, including **No Limit**, **Auto**, **Manual**, and **Limit By Group** to meet your various requirements by unleashing the potential of your WAN broadband services.

8.2.1 No limit (default)

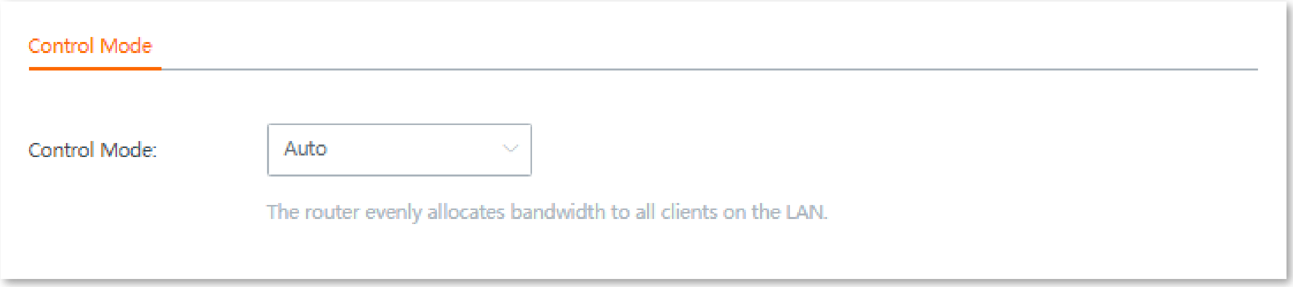


Control Mode

Control Mode: No Limit

It indicates that clients connected to the router compete for bandwidth resources without restriction.

8.2.2 Auto



Control Mode

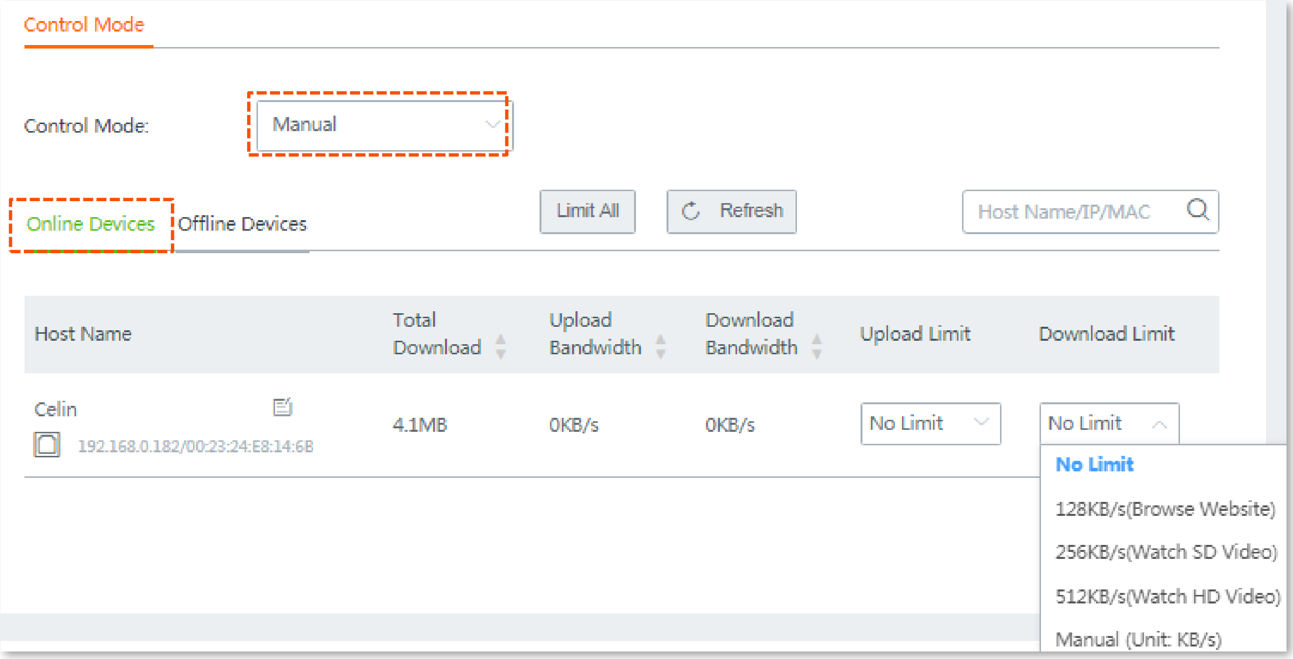
Control Mode: Auto

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

In this mode, the router evenly allocates bandwidth to all clients connected to it.

8.2.3 Manual

Select **Manual** from the **Control Mode** drop-down list menu, the configuration area appears. See the following figure:

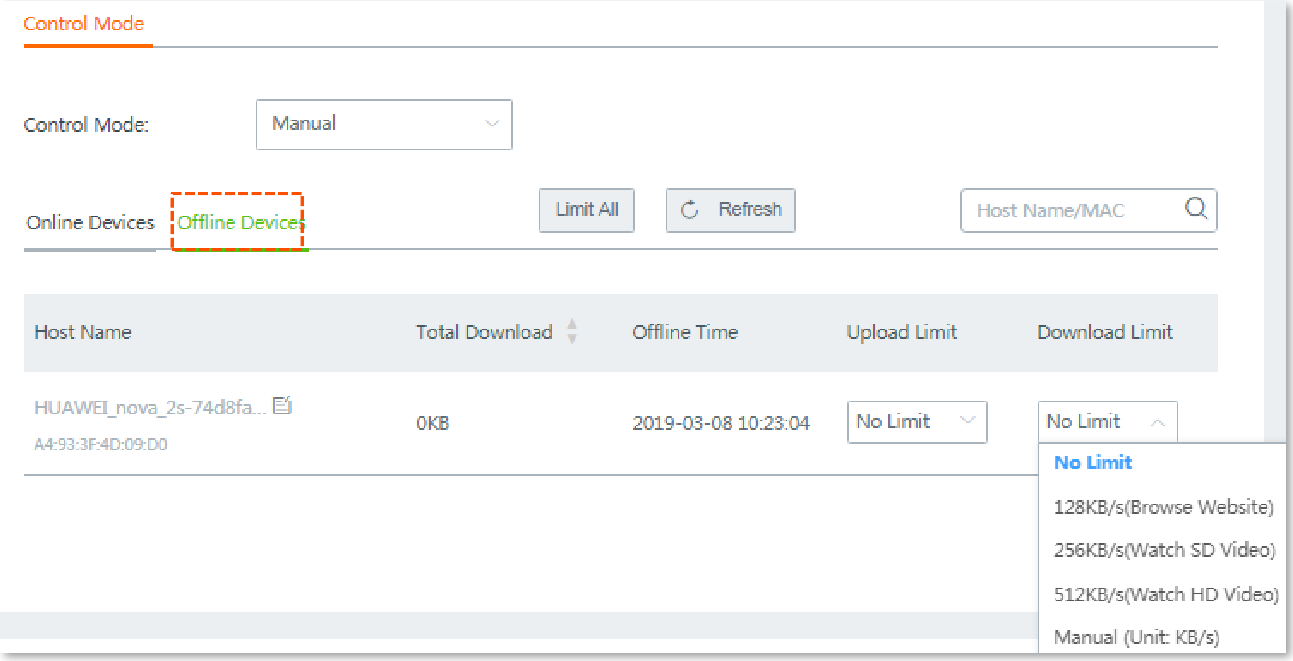


Control Mode

Control Mode: Manual

Host Name	Total Download	Upload Bandwidth	Download Bandwidth	Upload Limit	Download Limit
Celin 192.168.0.182/00:23:24:E8:14:6B	4.1MB	0KB/s	0KB/s	No Limit	No Limit

Click **Offline Devices** tag, the following configuration area appears:



Control Mode

Control Mode: Manual

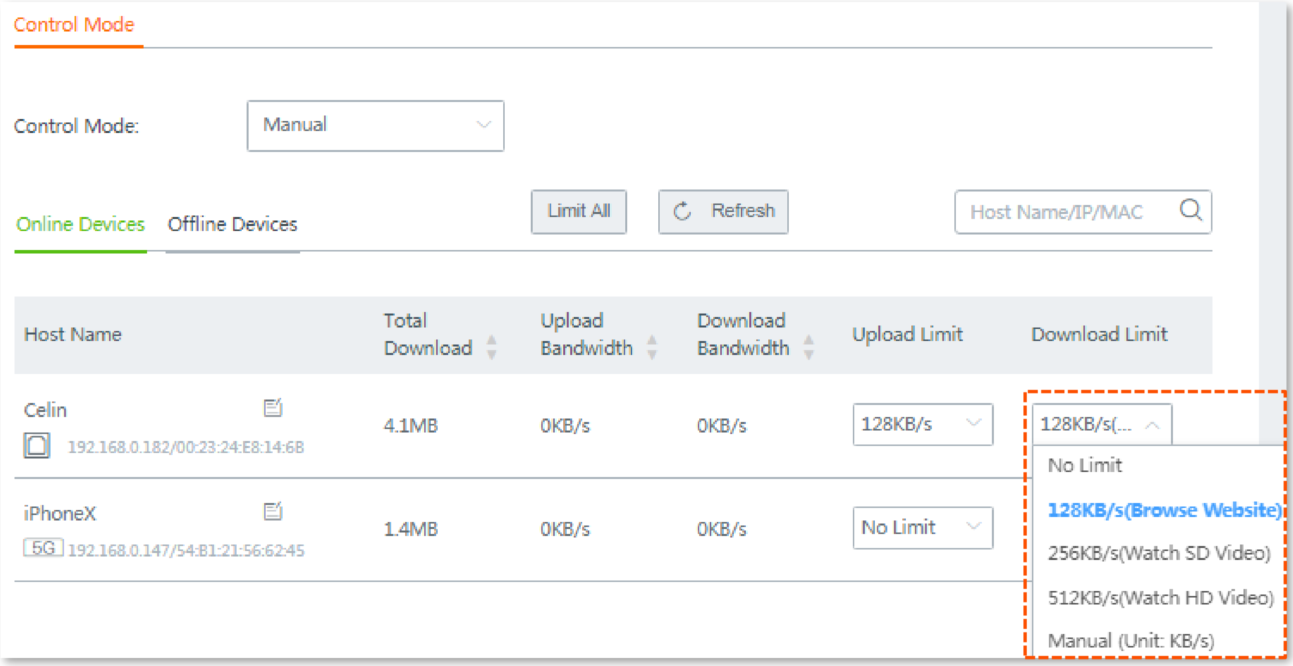
Host Name	Total Download	Offline Time	Upload Limit	Download Limit
HUAWEI_nova_2s-74d8fa... A4:93:3F:4D:09:D0	0KB	2019-03-08 10:23:04	No Limit	No Limit

Parameter description

Parameter	Description
Host Name	It specifies the name of clients connected to the router. You can click 📝 to personalize the host name for convenient management. NOTE - Modification of host name here will be applied to the whole system. - For host name-based rules, such as Configuring authentication-free host using host name, you need to use the host name here.
Total Download	It specifies the total download traffic utilized by each client.
Offline Time	Only available for offline devices. It indicates the time when the client is disconnected.
Upload Bandwidth	It indicates the real-time upload/download bandwidth of each client. TIP 1 Mbps=128 KB/s=1024 kb/s.
Download Bandwidth	
Upload Limit	The maximum upload/download rate you specified for each client. TIP 1 Mbps=128 KB/s=1024 kb/s.
Download Limit	

Control bandwidth of online/offline devices separately

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

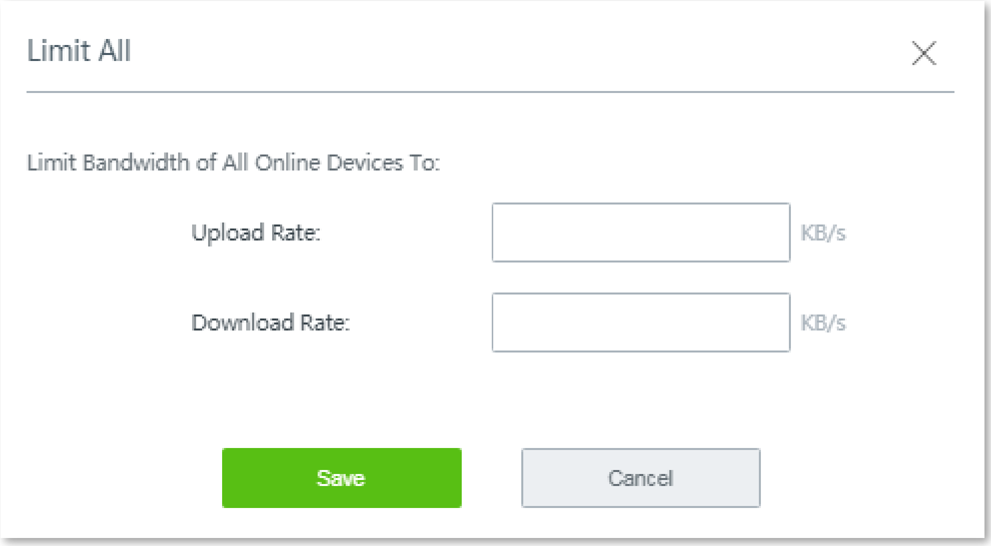


Control Mode: Manual

Host Name	Total Download	Upload Bandwidth	Download Bandwidth	Upload Limit	Download Limit
Celin 192.168.0.182/00:23:24:E8:14:6B	4.1MB	0KB/s	0KB/s	128KB/s	128KB/s(...
iPhoneX 5G 192.168.0.147/54:B1:21:56:62:45	1.4MB	0KB/s	0KB/s	No Limit	

Control bandwidth of online/offline devices in batch

Click **Limit All**, specify the values according to your actual situation on the configuration window, and click **Save** to apply your settings.



Limit All

Limit Bandwidth of All Online Devices To:

Upload Rate: KB/s

Download Rate: KB/s

8.2.4 Limit By Group

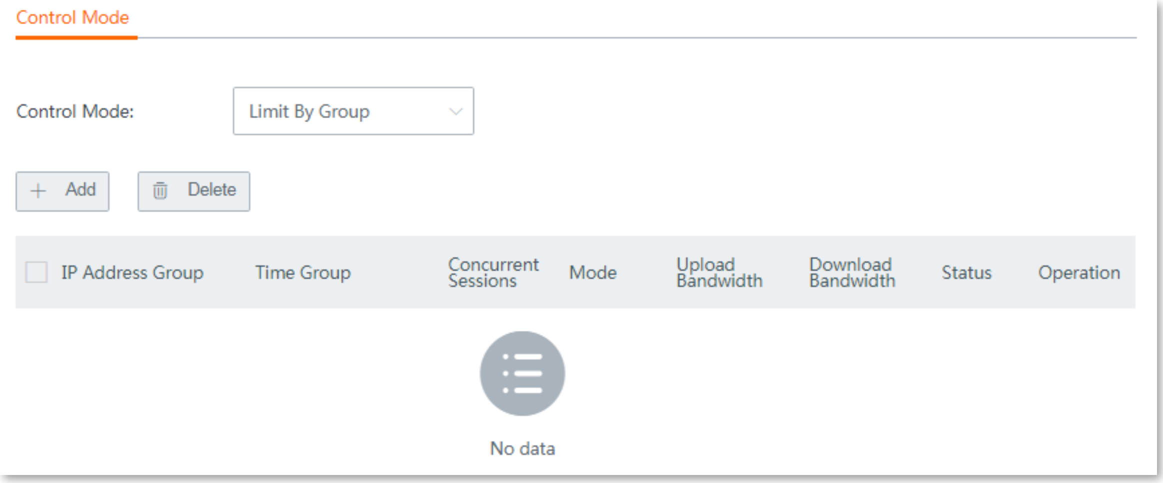
This mode allows you to customize control rules based on IP groups and time groups. The following describes the configuration procedure.

TIP

To control bandwidth based on groups, you need to configure IP group and time group first by navigating to **Filter Management** > **IP Group/Time Group**. Refer to Configuring IP group and time group for detailed description.

Step 1 Choose **Bandwidth Control**, and move to the **Control Mode** configuration area.

Step 2 Set **Control Mode** to **Limit By Group**, the following configuration area appears.



Control Mode

Control Mode: Limit By Group

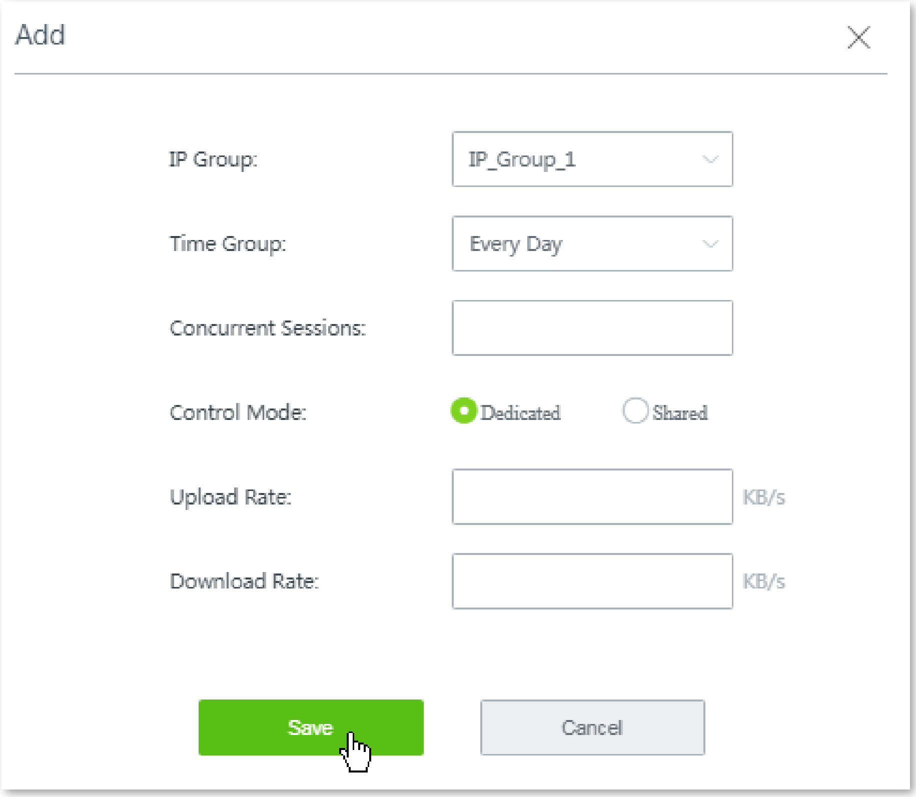
□	IP Address Group	Time Group	Concurrent Sessions	Mode	Upload Bandwidth	Download Bandwidth	Status	Operation

No data

Step 3 Click **Save** at the bottom of the page.

Step 4 Click **+Add** to add a bandwidth control policy.

Step 5 Set required parameters.



IP Group: IP_Group_1

Time Group: Every Day

Concurrent Sessions:

Control Mode: ● Dedicated ○ Shared

Upload Rate: KB/s

Download Rate: KB/s

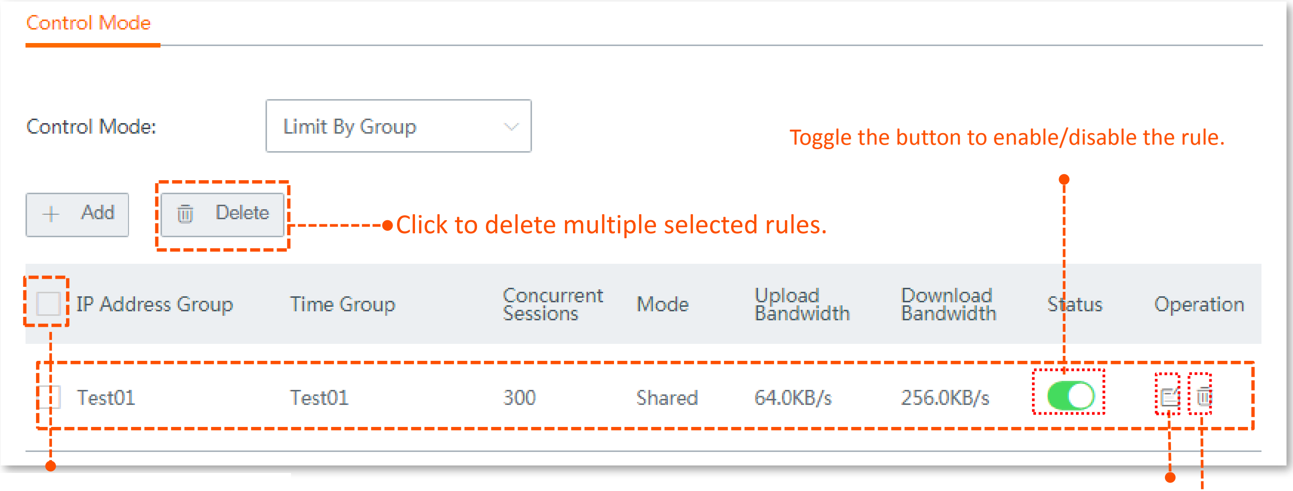
Parameter description

Parameter	Description
IP Group	Create or select the IP group to which the rule applies. To create an IP Group, choose **Filter Management** > **IP Group/Time Group**.
Time Group	Create or select the time group to which the rule applies. To create a time Group, choose **Filter Management** > **IP Group/Time Group**.
Concurrent Sessions	Maximum number of sessions of each device. Recommended value: 300.
Control Mode	This device supports the following two control modes: - **Shared**: All clients in the controlled IP groups share the upload/download rate you configured here. In this mode, bandwidth allocated to each client may vary. - **Dedicated**: Each client in the controlled IP groups exclusively enjoys the upload/download rate you configured here. In this mode, bandwidth allocated to each client is identical.
Upload Rate	Maximum upload rate a controlled client can reach.
Download Rate	Maximum download rate a controlled client can reach.

Step 6 Click **Save**.

---- End

Added successfully. See the following figure:



Control Mode

Control Mode: Limit By Group

□	IP Address Group	Time Group	Concurrent Sessions	Mode	Upload Bandwidth	Download Bandwidth	Status	Operation
□	Test01	Test01	300	Shared	64.0KB/s	256.0KB/s	🟩	

Toggle the button to enable/disable the rule.

Click to delete multiple selected rules.

Click to select all rules.

Click to modify the rule.

Click to delete the rule.

8.3 Example of configuring group-based control rules

Networking requirement

An enterprise uses W15E to set up a LAN to address the following requirement:

During business hours (08:30 to 18:00 on 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. See the following table:

Group name	IP range	Effective time	Upload bandwidth	Download bandwidth
IP group1	192.168.0.2~100	08:30~18:00 on weekday	1 Mbps	1 Mbps
IP group2	192.168.0.101~254	08:30~18:00 on weekday	No limit	No limit

Solutions

You can use the **Limit By Group** bandwidth control function of the router to meet this requirement.

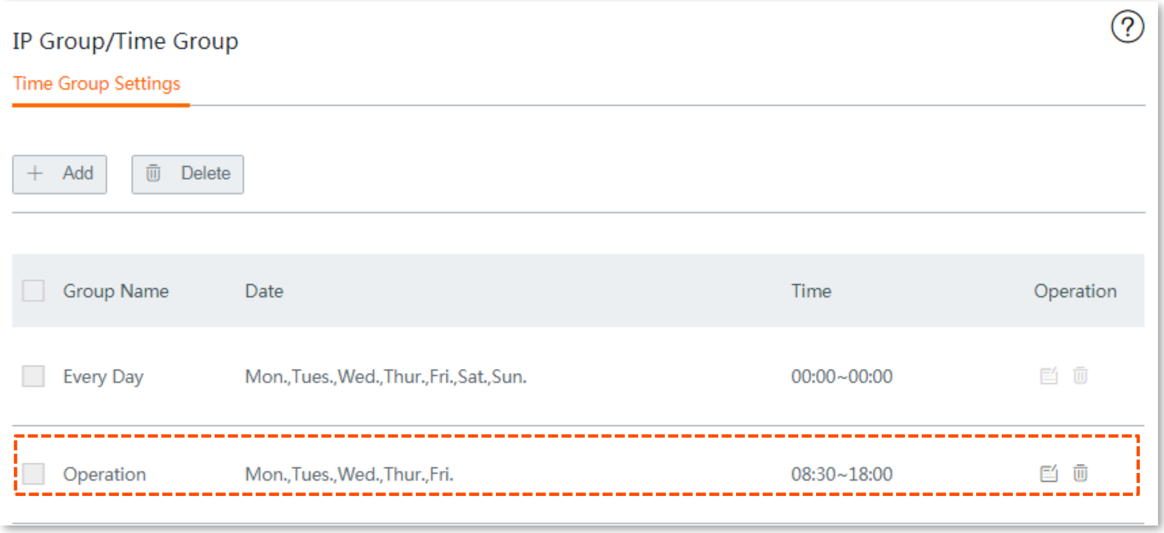
Configuration description

Step	Task	Description
1	Set a time group.	Set the time group on the **Filter Management** > **IP Group/Time Group** page.
2	Set an IP address group.	Set the IP address group on the **Filter Management** > **IP Group/Time Group** page.
3	Set bandwidth control rule(s).	Set a rule on the **Bandwidth Control** page.

Configuration procedure

Step 1 Set a time group.

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



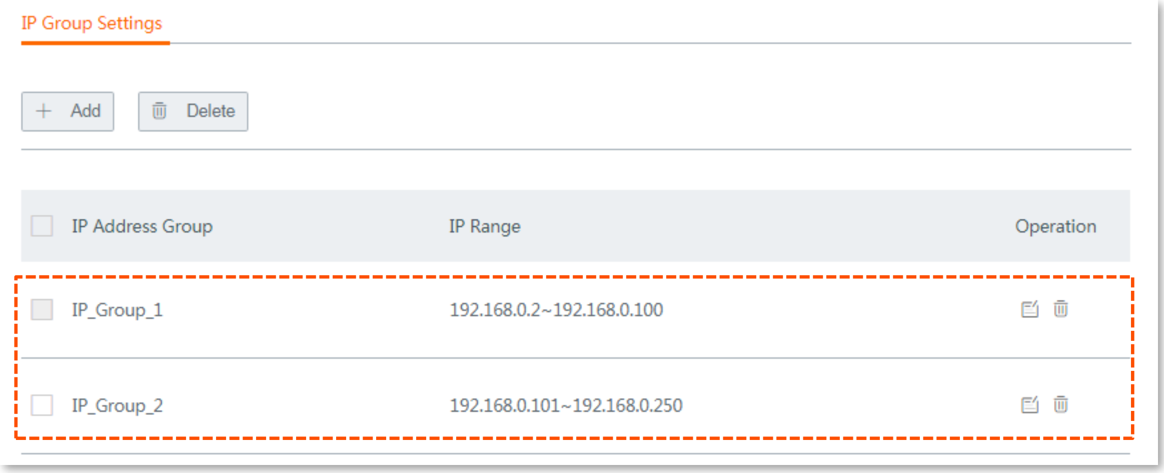
IP Group/Time Group

Time Group Settings

□	Group Name	Date	Time	Operation
□	Every Day	Mon.,Tues.,Wed.,Thur.,Fri.,Sat.,Sun.	00:00~00:00	
□	Operation	Mon.,Tues.,Wed.,Thur.,Fri.	08:30~18:00	

Step 2 Set an IP address group.

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

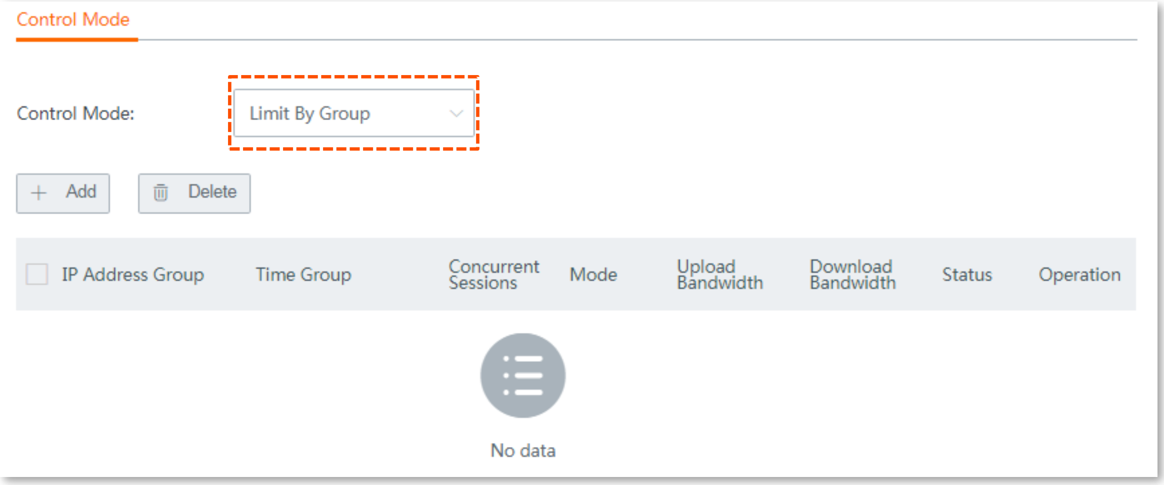


IP Group Settings

□	IP Address Group	IP Range	Operation
□	IP_Group_1	192.168.0.2~192.168.0.100	
□	IP_Group_2	192.168.0.101~192.168.0.250	

Step 3 Set bandwidth control rule(s).

1. On the **Bandwidth Control** page, set **Control Mode** to **Limit By Group**.
2. Click **Save** at the bottom of the page.



Control Mode

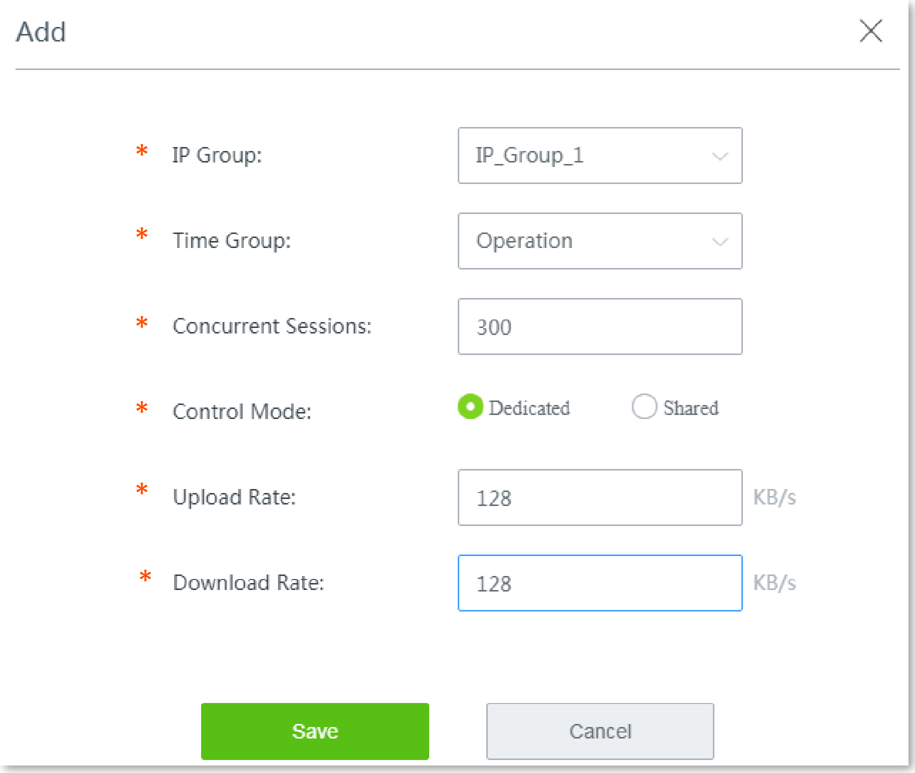
Control Mode: Limit By Group

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

No data

3. Click **+Add**. The **Add** configuration window appears.

4. Create a rule shown in the following figure, and click **Save**.



Add

* IP Group: IP_Group_1

* Time Group: Operation

* Concurrent Sessions: 300

* Control Mode: ● Dedicated ○ Shared

* Upload Rate: 128 KB/s

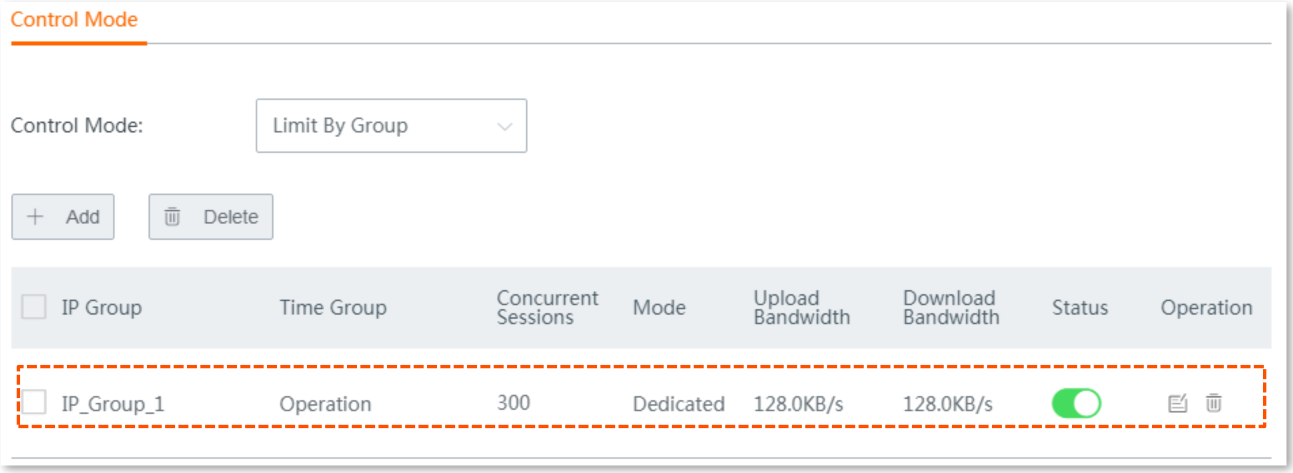
* Download Rate: 128 KB/s

TIP

- Parameters indicated with * are mandatory.
- 1 Mbps = 128 KB/s = 1024 kb/s.

---- End

Added successfully. See the following figure:



Control Mode

Control Mode: Limit By Group

IP Group	Time Group	Concurrent Sessions	Mode	Upload Bandwidth	Download Bandwidth	Status	Operation
IP_Group_1	Operation	300	Dedicated	128.0KB/s	128.0KB/s	●	

Verification

During business hours from 08:30 to 18:00 on weekday, each computer with an IP address ranging from 192.168.0.1 to 192.168.0.100 is allocated 1 Mbps (128 KB/s) 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.

9 Authentication

9.1 Overview

The router supports captive portal and WiFi via WeChat, and only one of them can be enabled on the router. Either captive portal or WiFi via WeChat can facilitate you to improve your brand visibility and attract more fans.

This chapter describes:

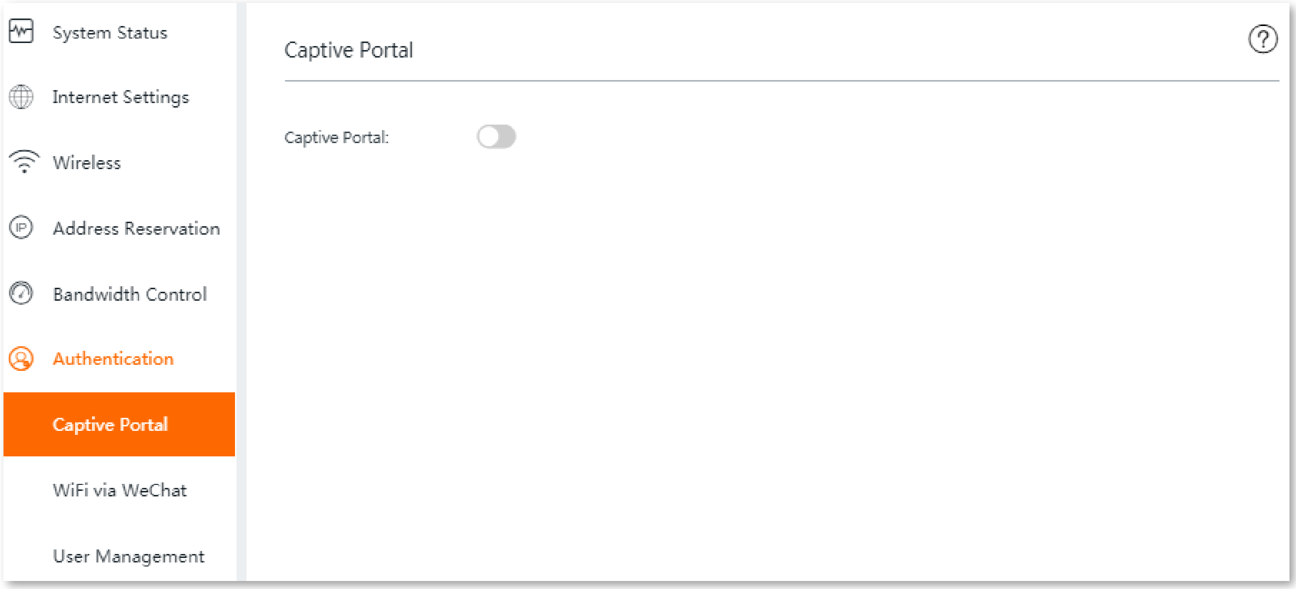
- Configuring captive portal.
- Configuring WiFi via WeChat.
- Configuring authentication-free host.
- Configuring user accounts used for captive portal.

9.2 Configuring captive portal

This section introduces how to configure captive portal.

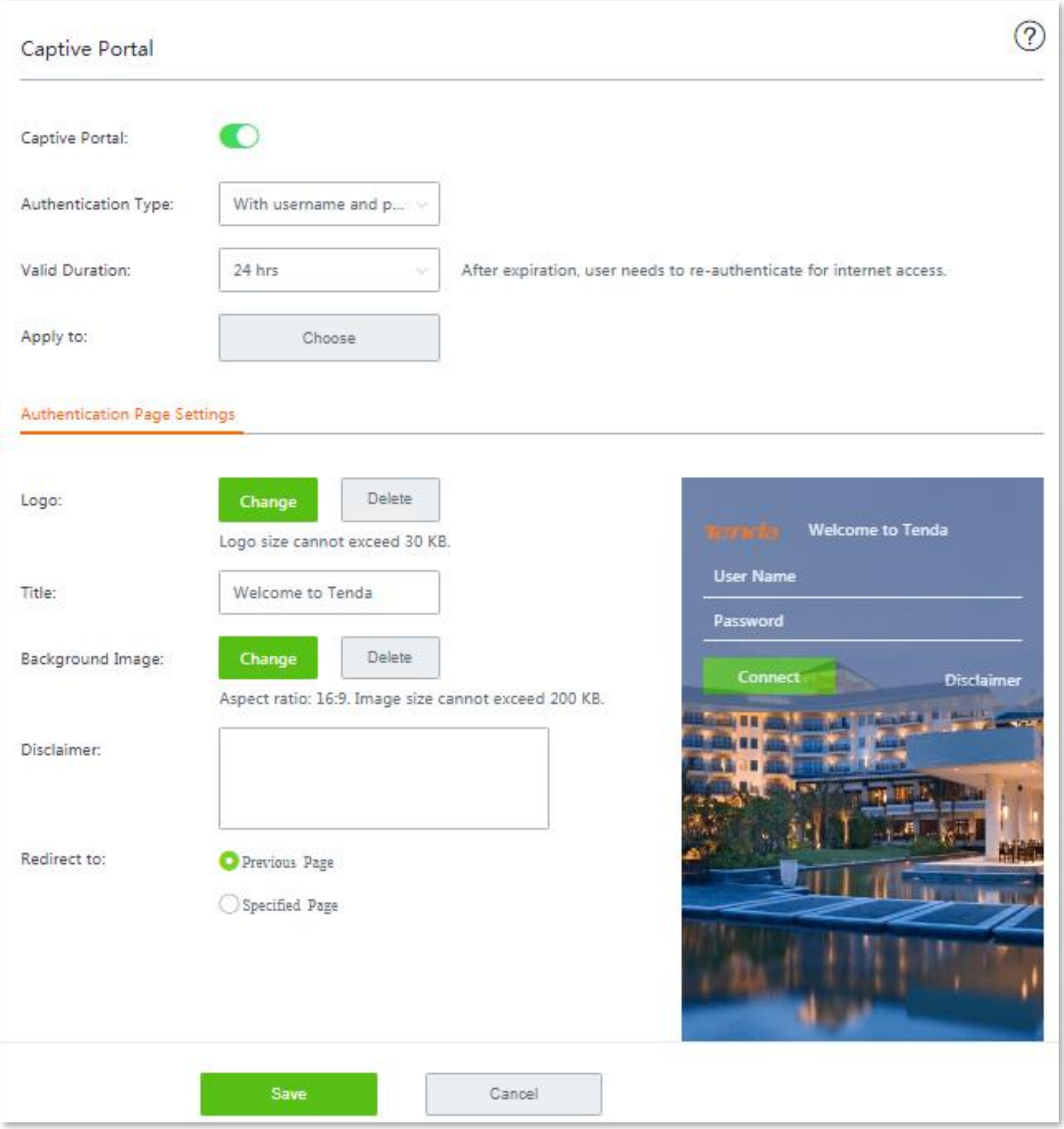
9.2.1 Overview

To access the configuration page, choose **Authentication** > **Captive Portal**. By default, this function is disabled. See the following figure:



Captive Portal:

Once captive portal is enabled, the following configuration page appears. On the page, you can select the authentication type, set the authentication validity period, choose the wired and/or wireless networks to be applied, and configure the authentication web page.


Captive Portal

Captive Portal: ●

Authentication Type: With username and p...

Valid Duration: 24 hrs After expiration, user needs to re-authenticate for internet access.

Apply to: Choose

Authentication Page Settings

Logo: Change Delete

Logo size cannot exceed 30 KB.

Title: Welcome to Tenda

Background Image: Change Delete

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

Disclaimer:

Redirect to: ● Previous Page ○ Specified Page

Parameter description

Parameter	Description
Captive Portal	It specifies whether or not to enable the captive portal function of the router. If this function is enabled, the WiFi via WeChat function becomes unavailable.
Authentication Type	It specifies the type of the captive portal. - **With username and password**: It allows a user to access the internet with a username and password on the authentication web page. The username and password should be added on **Authentication > User Management** page. - **One-key authentication**: It allows a user to access the internet by clicking **Connect** when receiving an authentication web page. - **WiFi via SMS:** It allows a user to access the internet with a verification code sent by SMS when receiving an authentication web page. To enable this authentication

Parameter	Description
	type, you need to configure **SMS Provider Settings** first. The router supports **Jixintong** and **NEXMO**, and allows you to **customize HTTP interconnection** yourself as well.
Valid Duration	It specifies the authentication validity period. A user must be re-authenticated for accessing the internet after the period expires.
Logo	It allows you to modify the logo displayed on the authentication web page.
Title	It allows you to modify the title displayed on the authentication web page. It is **Welcome to Tenda** by default.
Background Image	It allows you to modify the background image displayed on the authentication web page.
Change Image	Click it to change the image.
Delete	Click it to delete the image.
Disclaimer	It allows you to configure the disclaimer information. A maximum of **256** characters is allowed.
Redirected To	It specifies the website that the client automatically redirects to after passing authentication: - **Previous Page**: When the captive portal is passed, the page would redirect to the previous page the user visited. For example, if a user is visiting Google search page before authentication, the user will stay on Google search page after passing the authentication. - **Specified Page**: It specifies the website redirected to after passing the captive portal.

9.2.2 Configuring WiFi via SMS

Configuration description

Step	Task	Description
1	Configure basic settings.	Set authentication type, valid duration, and choose networks to be applied, as well as SMS provider settings.
2	Configure authentication page settings.	Configure the authentication page received by users.

Before you start

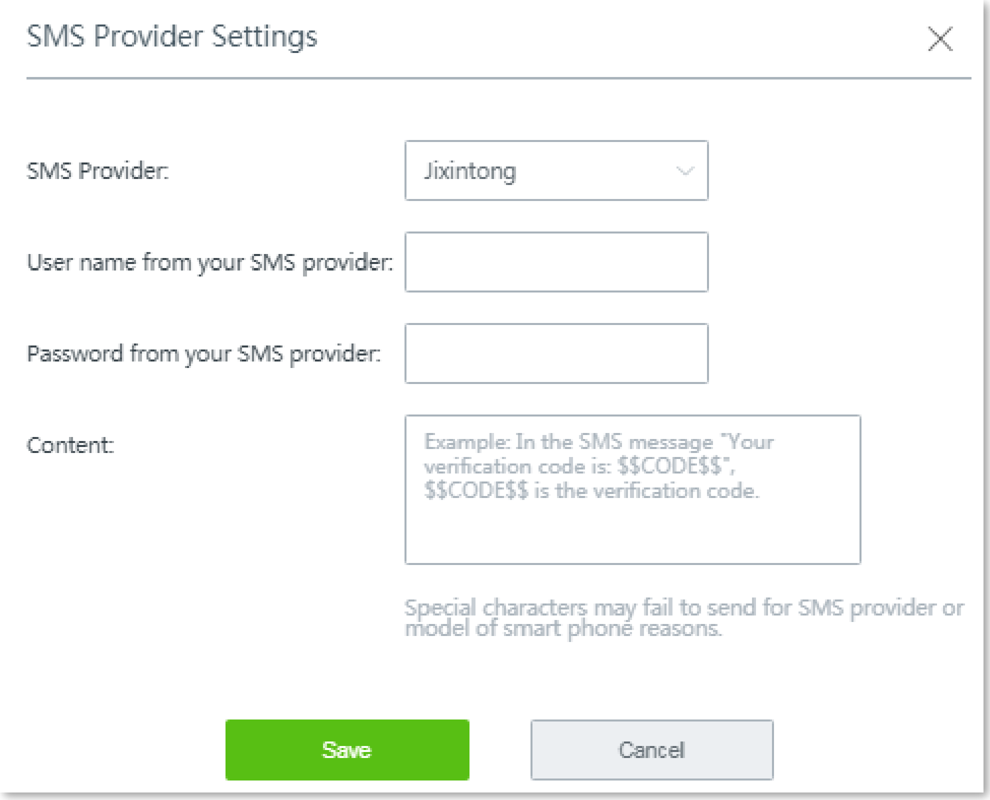
Obtain required information from your SMS provider first.

- Jixintong: **User Name** and **Password** you applied on Jixintong platform.
- NEXMO: **api_key** and **api_secret** you applied on NEXMO platform.
- Custom HTTP Interconnection: SMS gateway URL interface format defined by your SMS provider, and SMS error code from your SMS provider.

Configuration procedure

Step 1 **Configure basic settings.**

1. Choose **Authentication** > **Captive Portal**, and enable this function.
2. Select **WiFi via SMS** from the **Authentication Type** drop-down list menu.
3. Click **SMS Provider Settings**, the configuration window appears.



SMS Provider Settings

SMS Provider: Jixintong

User name from your SMS provider:

Password from your SMS provider:

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

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

Parameter description

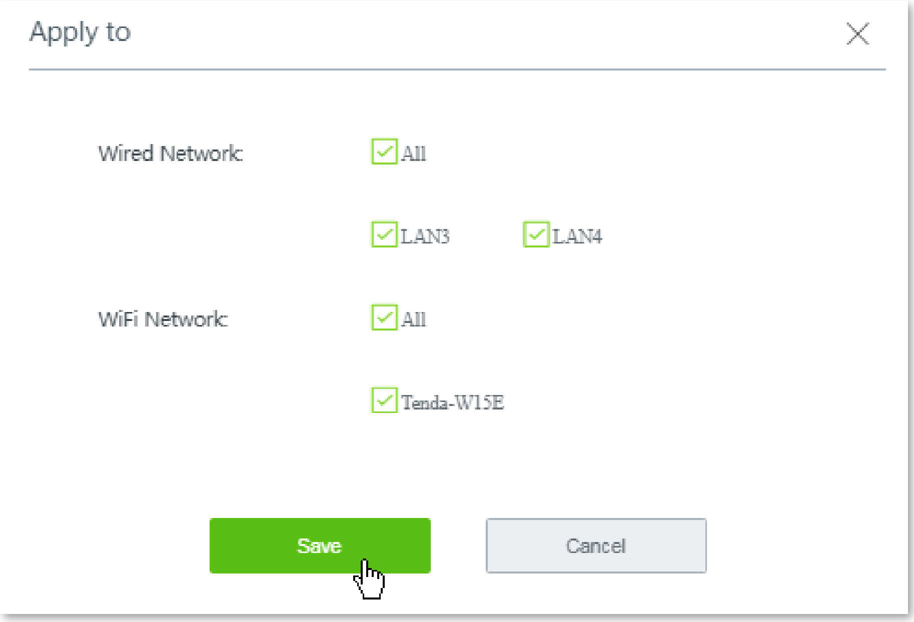
Parameter		Description
Jixintong	User name from your SMS provider	Enter the user name and password you've applied on the Jixintong platform.
	Password from your SMS provider	
	Content	Customize the short message sent to users. TIP The verification code format is **$$CODE$$**, which cannot be modified.
NEXMO	api_key	Enter the **api_key** you've applied on the NEXMO platform.
	api_secret	Enter the **api_secret** you've applied on the NEXMO platform.
	Content	Customize the short message sent to users. TIP The verification code format is **$$CODE$$**, which cannot be modified.

Parameter		Description
Customize HTTP Interconnection	Encoding	It specifies the character encoding format. Select the encoding format that your SMS provider supports. Available options include: - **GBK/GB2312:** GBK (GB abbreviates Guojia Biaozhun, which means national standard in Chinese, while K stands for Extension) is an extension of the GB2312 character set for simplified Chinese characters. - **UTF-8:** 8-bit Unicode Transformation Format.
	Content	Customize the short message sent to users. TIP The verification code format is **$$CODE$$**, which cannot be modified.
	SMS Gateway URL Interface	Enter the SMS gateway URL interface in the format defined by your SMS provider.
	SMS Error Code	It indicates the error code that tells the router a short message is unsent, and you can use this error code to consult your SMS provider for troubleshooting. You can consult your SMS provider to learn the specific content.

4. Set the required parameters, and click **Save.**

5. Set **Valid Duration**.

6. Click **Choose**, choose the network(s) to be applied, and click **Save**.



Apply to

Wired Network: ☑ All

☑ LAN3 ☑ LAN4

WiFi Network: ☑ All

☑ Tenda-W15E

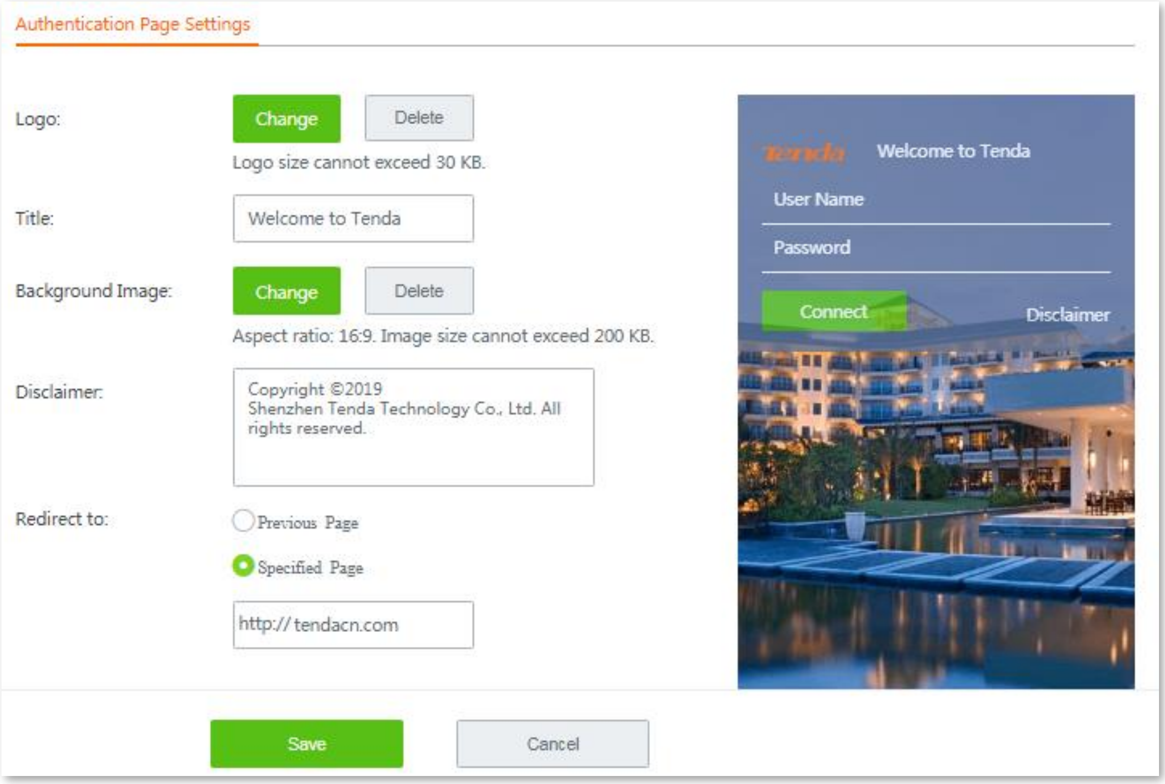
TIP

If the WiFi network name you selected is modified, it will be automatically deselected here. To make the WiFi network effective, you have to re-select the WiFi network with the new SSID here manually.

Step 2 Configure authentication page settings.

1. Set required parameters for the authentication page by following the on-screen

instructions. Configurations on the following figure are only used for examples.



Authentication Page Settings

Logo: Change Delete

Logo size cannot exceed 30 KB.

Title: Welcome to Tenda

Background Image: Change Delete

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

Disclaimer: Copyright ©2019 Shenzhen Tenda Technology Co., Ltd. All rights reserved.

Redirect to: ○ Previous Page ● Specified Page

http:// tendacn.com

Save Cancel

2. Click **Save** at the bottom on the page.

---- End

9.2.3 Configuring authentication with user name and password

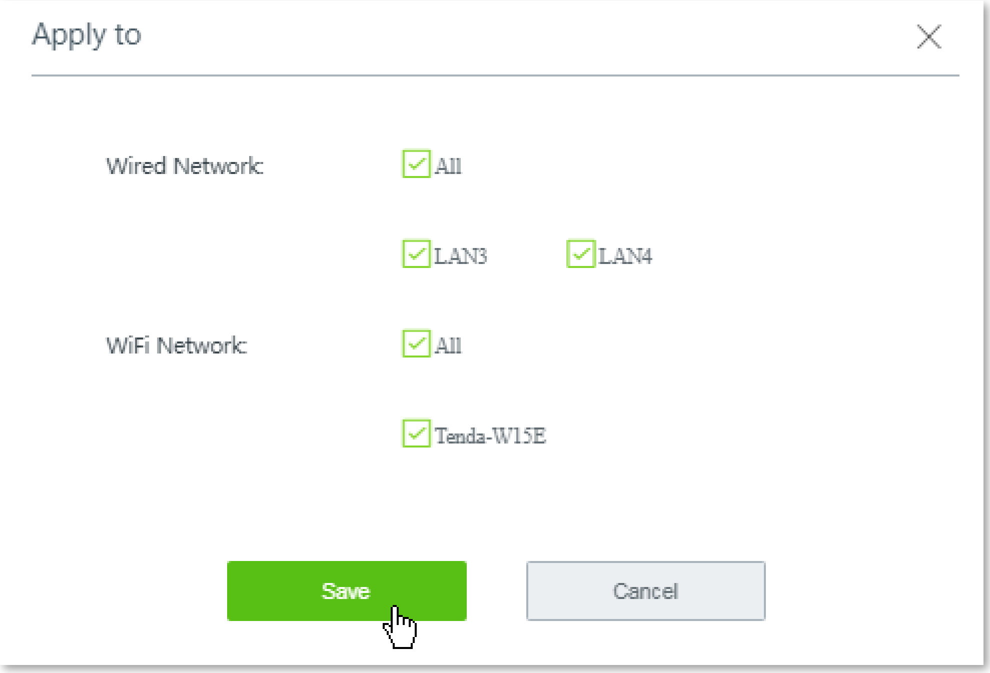
Configuration description

Step	Task	Description
1	Configure basic settings for captive portal.	Set authentication type, valid duration, and choose networks to be applied, as well as the required authentication page.
2	Add a user account for captive portal.	Configure user name, password, valid duration and other parameters.
3	Add user devices that can access the internet without being authenticated.	Add host(s) with host name, IP address, or MAC address as needed.

Configuration procedure

Step 1 Configure basic settings for captive portal.

1. Choose **Authentication** > **Captive Portal**, and enable this function.
2. Set **Authentication Type** to **With username and password**.
3. Set **Valid Duration** to **No Limit**.
4. Click **Choose**, choose the network(s) to be applied, and click **Save**.



Apply to

Wired Network: ☑ All

☑ LAN3 ☑ LAN4

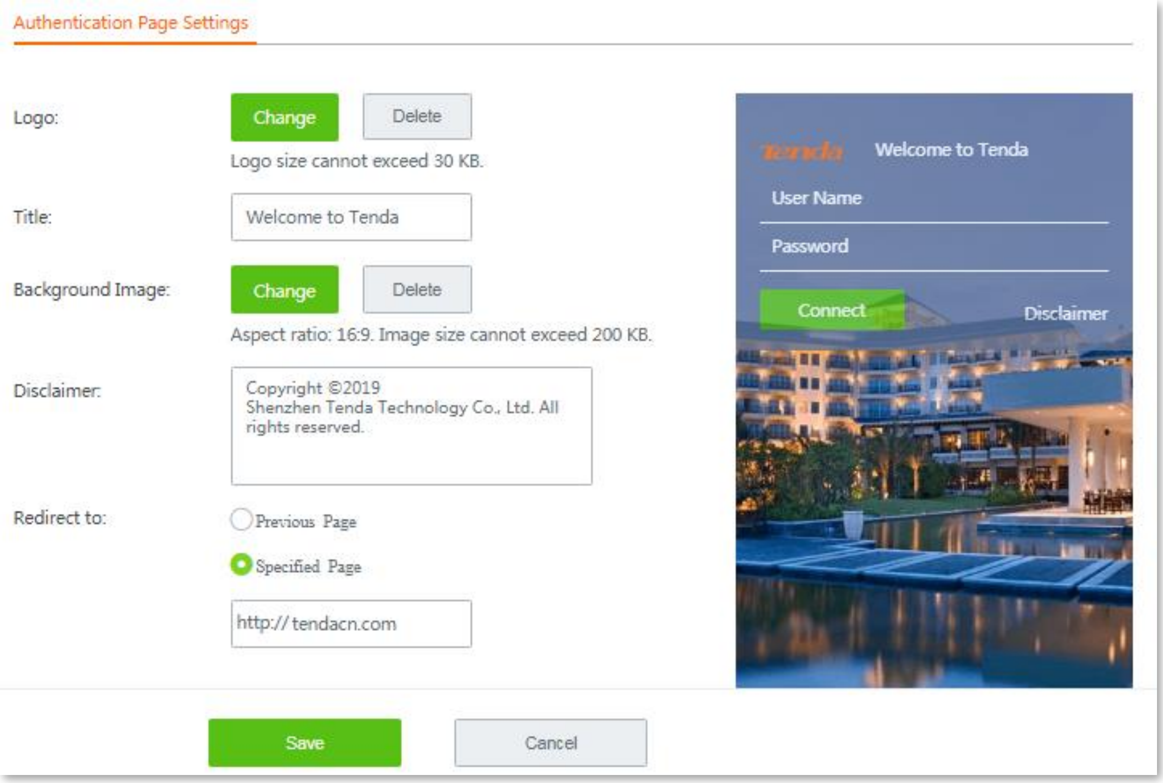
WiFi Network: ☑ All

☑ Tenda-W15E

TIP

If the WiFi network name you selected is modified, it will be automatically deselected here. To make the WiFi network effective, you have to re-select the WiFi network with the new SSID here manually.

5. Set required parameters for the authentication page by following the on-screen instructions. Configurations on the following figure are only used for examples.



Authentication Page Settings

Logo: Change Delete

Logo size cannot exceed 30 KB.

Title: Welcome to Tenda

Background Image: Change Delete

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

Disclaimer: Copyright ©2019 Shenzhen Tenda Technology Co., Ltd. All rights reserved.

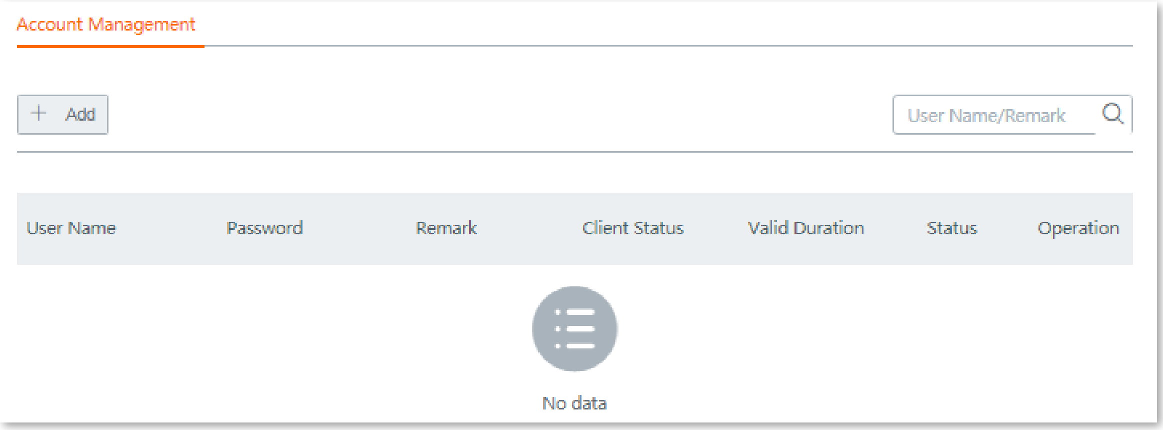
Redirect to: ○ Previous Page ● Specified Page

http:// tendacn.com

6. Click **Save** at the bottom on the page.

Step 2 **Add a user account for captive portal.**

1. Choose **Authentication** > **User Management**, and move the **Account Management** configuration area.



Account Management

+ Add

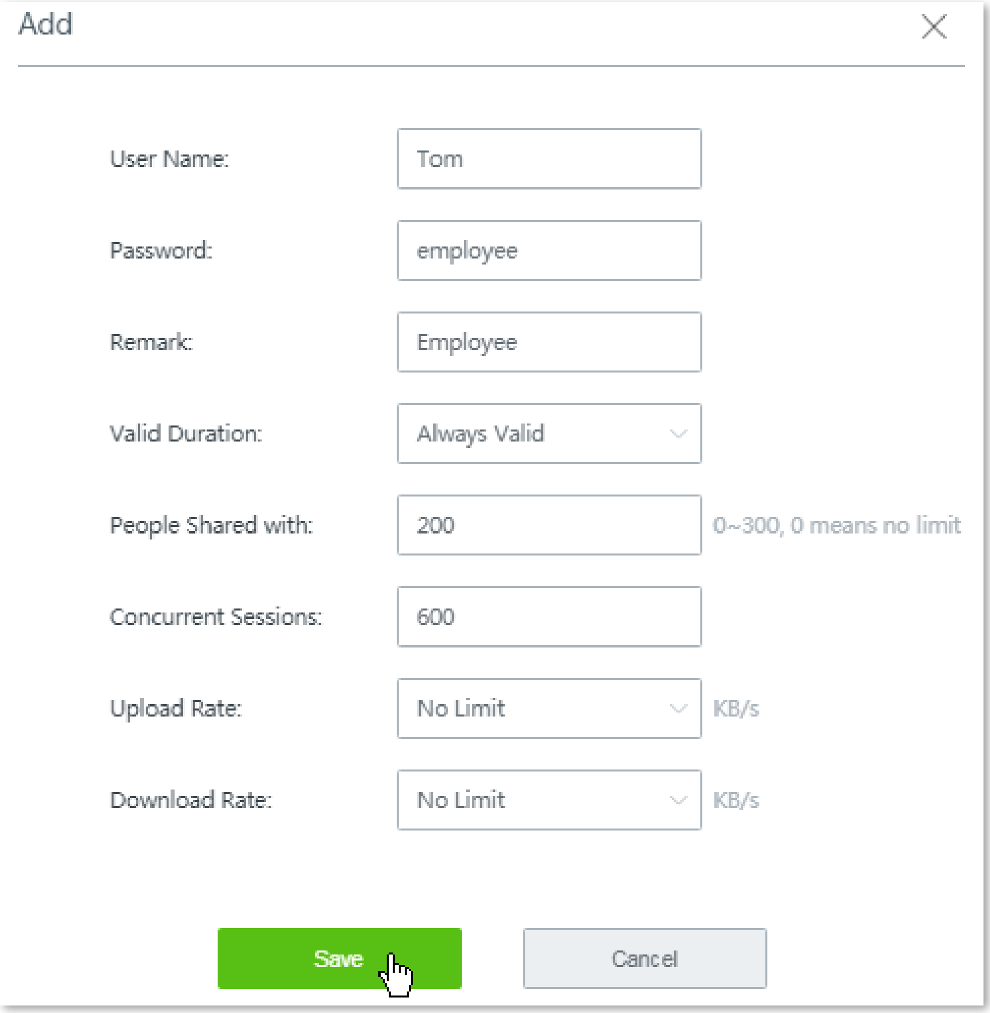
User Name/Remark

User Name	Password	Remark	Client Status	Valid Duration	Status	Operation

No data

2. Click **+ Add**. The **Add** configuration window appears.

3. Set required parameters. Configurations on the following figure are only used for examples.



Add

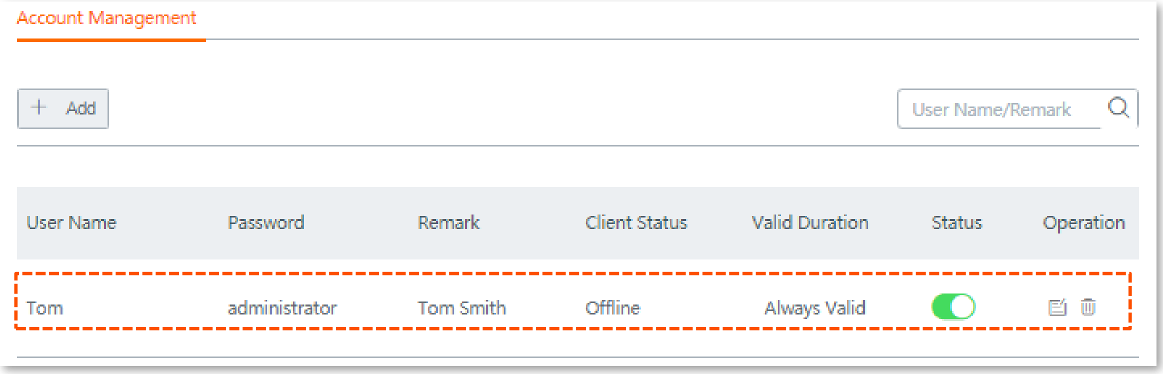
User Name:	Tom	
Password:	employee	
Remark:	Employee	
Valid Duration:	Always Valid	
People Shared with:	200	0~300, 0 means no limit
Concurrent Sessions:	600	
Upload Rate:	No Limit	KB/s
Download Rate:	No Limit	KB/s

TIP

To add more user accounts, repeat this step.

4. Click **Save**.

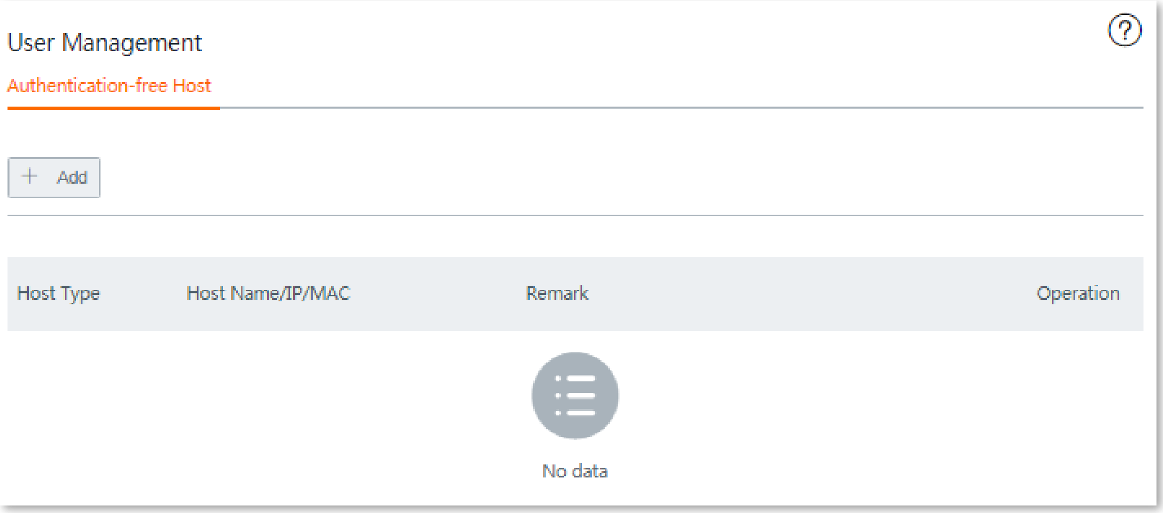
Added successfully, see the following figure.



User Name	Password	Remark	Client Status	Valid Duration	Status	Operation
Tom	administrator	Tom Smith	Offline	Always Valid	●	

Step 3 Add user devices that can access the internet without being authenticated.

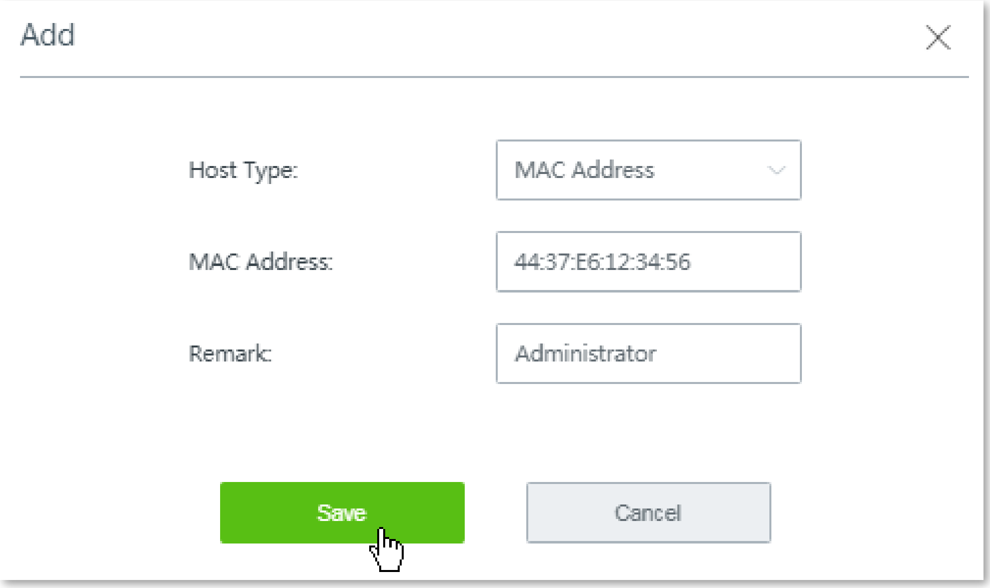
1. Choose **Authentication** > **User Management**, and move the **Authentication-free Host** configuration area.



Host Type	Host Name/IP/MAC	Remark	Operation

2. Click **+ Add** in the **Authentication-free Host** area. The **Add** configuration window appears.

3. Set required parameters. Configurations on the following figure are only used for examples.



Host Type: MAC Address

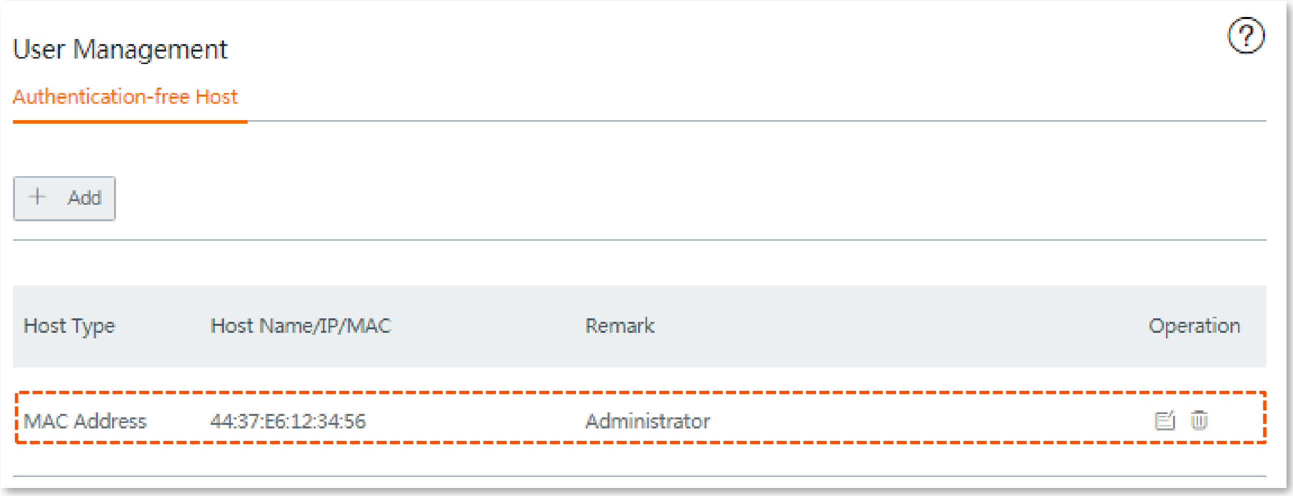
MAC Address: 44:37:E6:12:34:56

Remark: Administrator

4. Click **Save**.

---- End

Added successfully, see the following figure:



User Management

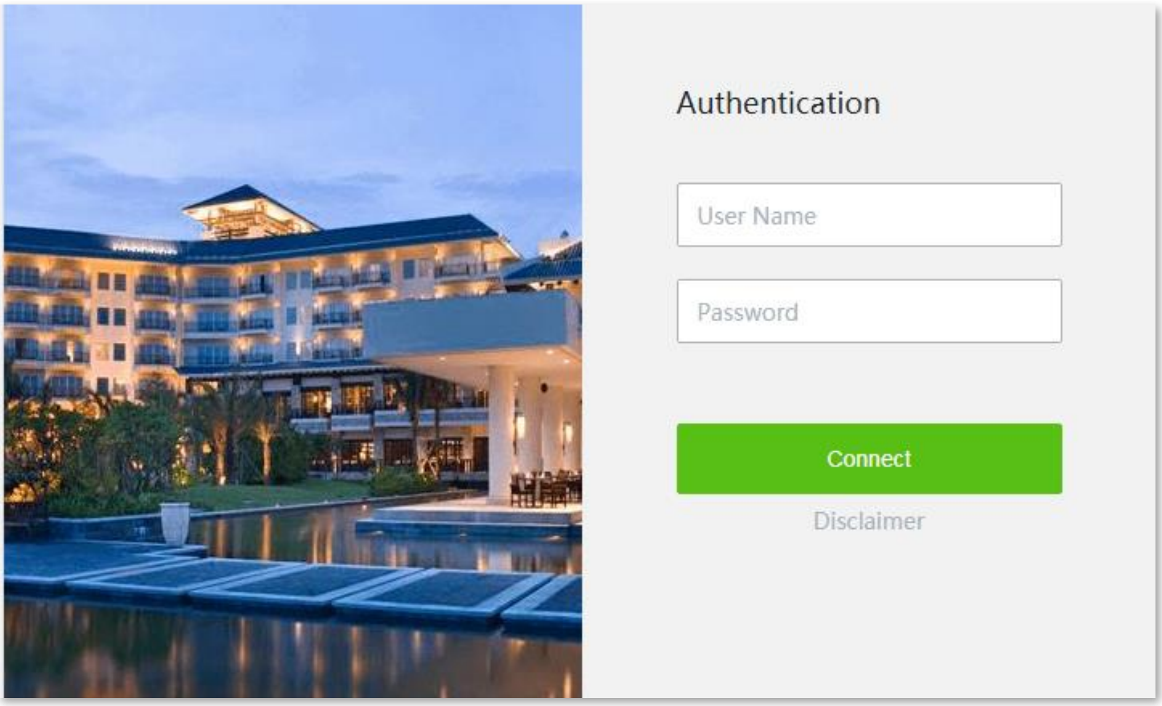
Authentication-free Host

Host Type	Host Name/IP/MAC	Remark	Operation
MAC Address	44:37:E6:12:34:56	Administrator	

Verification

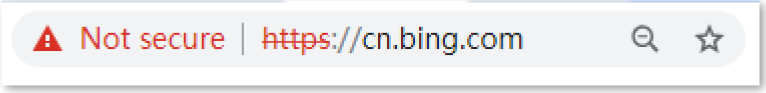
The network administrator can access the internet without being authenticated, while the other employees need to perform the following procedure to get authenticated before accessing the internet:

Step 1 Start an employee’s web browser and access a website. The captive portal page appears. See the following figure.



TIP

If the website you visited is encrypted with **https** protocol, a warning page shows **Your connection is not private** appears. In this case, try another website that is encrypted with ***http*** protocol.



Step 2 Enter a correct user name and password, which is **Tom/employee** in this example, on the

Authentication page, and click **Connect**.

---- End

When the employee is authenticated, the employee is redirected to the website www.tendacn.com.

9.2.4 Configuring one-key authentication

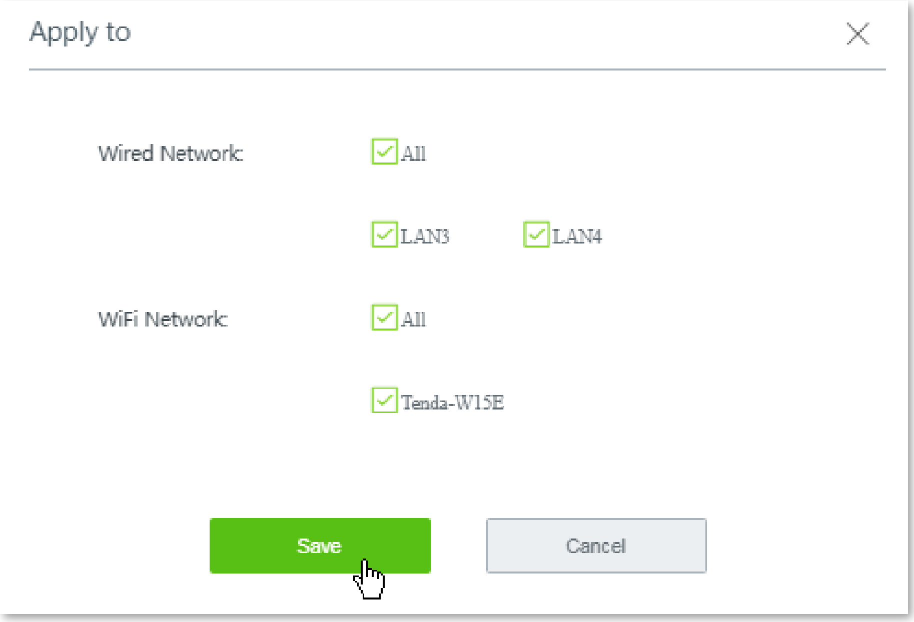
Configuration description

Step	Task	Description
1	Configure basic settings.	Set authentication type, valid duration, and choose networks to be applied.
2	Configure authentication page settings	Configure the page received by users.

Configuration procedure

Step 1 **Configure basic settings**.

1. Choose **Authentication** > **Captive Portal**, and enable this function.
2. Select **One-key authentication** from the **Authentication Type** drop-down list menu.
3. Set **Valid Duration**.
4. Click **Choose**, choose the network(s) to be applied, and click **Save**.



Apply to

Wired Network: ☑ All

☑ LAN3 ☑ LAN4

WiFi Network: ☑ All

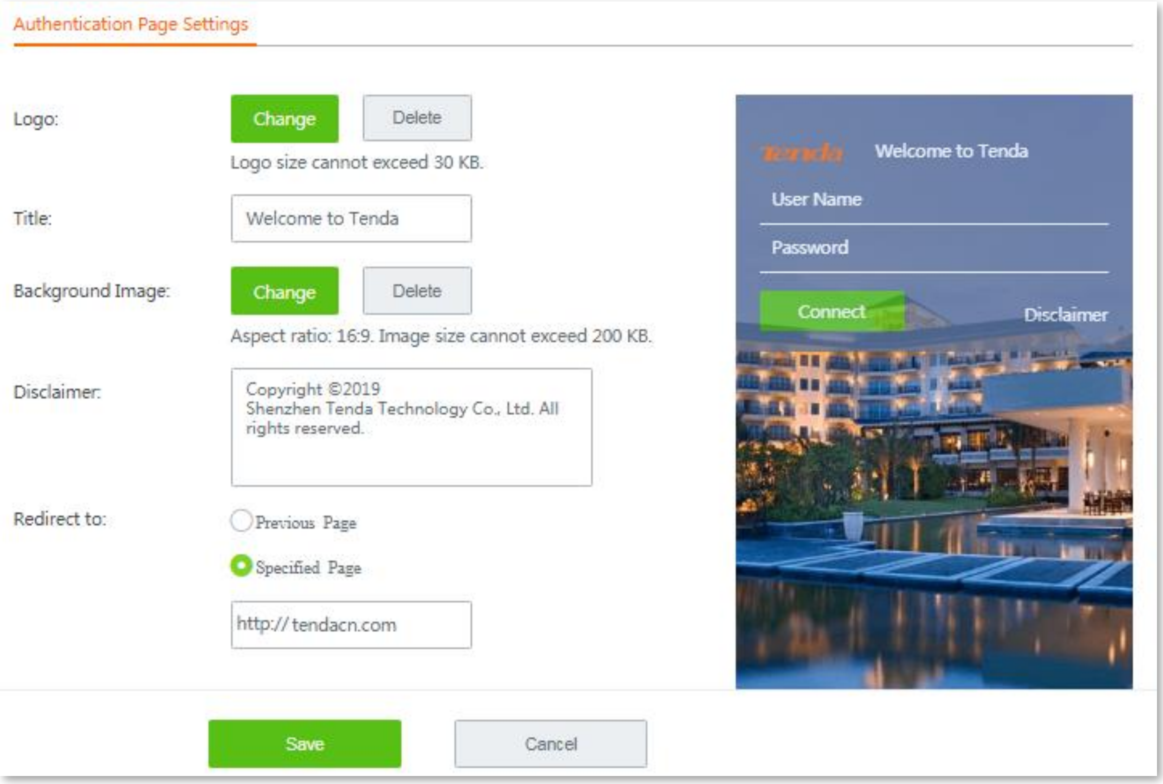
☑ Tenda-W15E

TIP

If the WiFi network name you selected is modified, it will be automatically deselected here. To make the WiFi network effective, you have to re-select the WiFi network with the new SSID here manually.

Step 2 Configure authentication page settings.

1. Set required parameters for the authentication page by following the on-screen instructions. Configurations on the following figure are only used for examples.



Authentication Page Settings

Logo: Change Delete

Logo size cannot exceed 30 KB.

Title: Welcome to Tenda

Background Image: Change Delete

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

Disclaimer: Copyright ©2019 Shenzhen Tenda Technology Co., Ltd. All rights reserved.

Redirect to: ○ Previous Page ● Specified Page

http:// tendacn.com

2. Click **Save** at the bottom on the page.

---- End

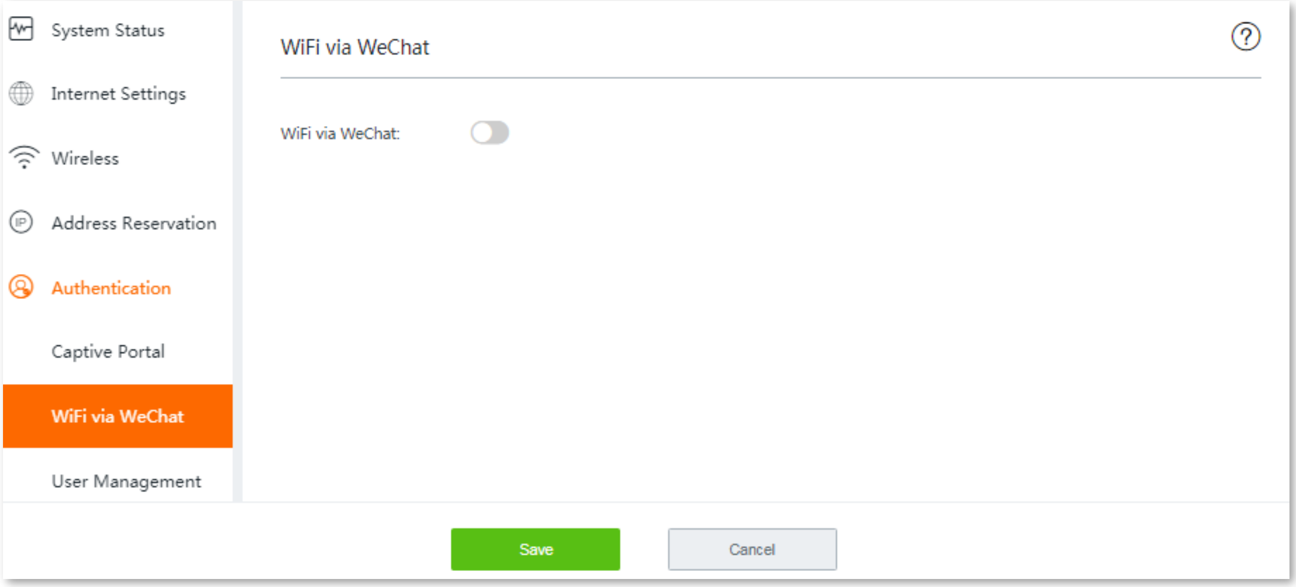
9.3 Configuring WiFi via WeChat

This section describes:

- Overview
- Example of configuring WiFi via WeChat

9.3.1 Overview

To access the configuration page, choose **Authentication** > **WiFi via WeChat**. The function is disabled by default.

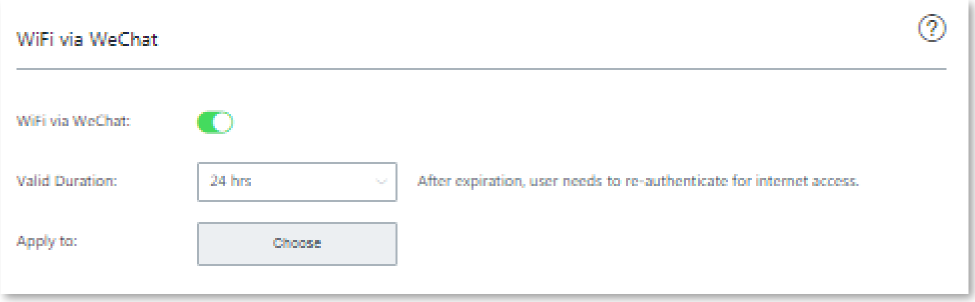


WiFi via WeChat

WiFi via WeChat: ○

Once this function is enabled, the configuration page appears. This page consists of three areas: Basic settings for WiFi via WeChat, WeChat Open Platform Settings, and WeChat Authentication Page Settings.

- **Basic settings for WiFi via WeChat**



WiFi via WeChat

WiFi via WeChat: ●

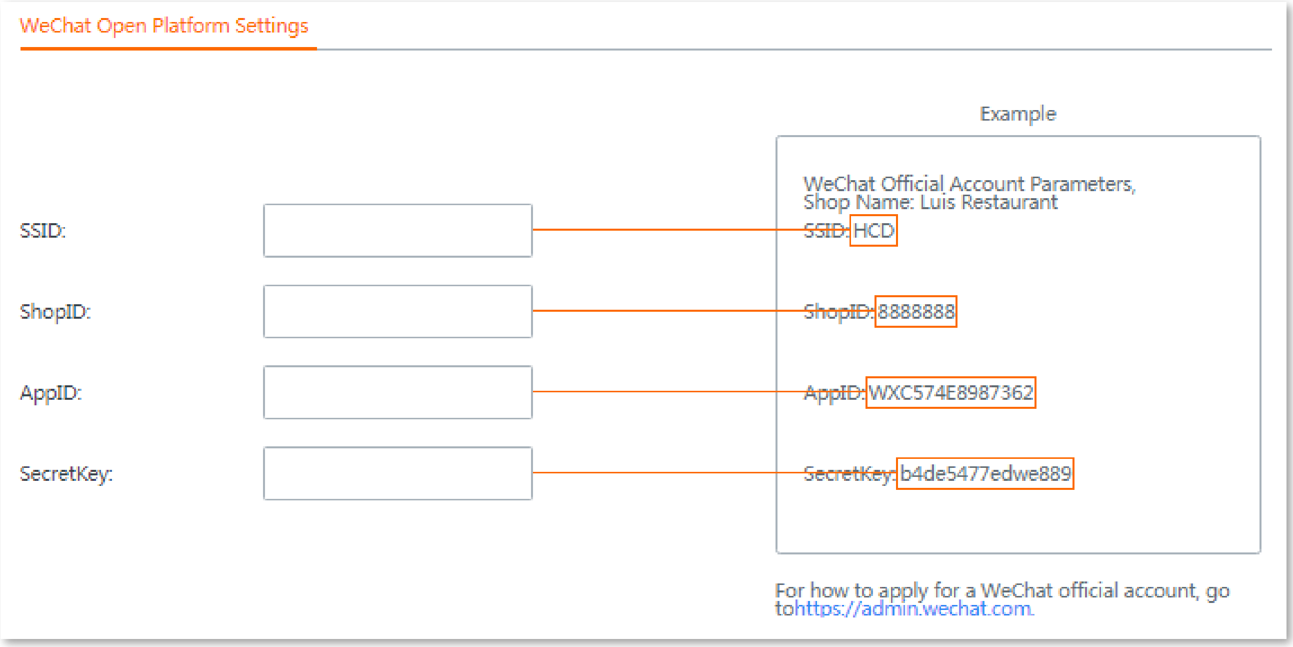
Valid Duration: 24 hrs   After expiration, user needs to re-authenticate for internet access.

Apply to: Choose

Parameter description

Parameter	Description
WiFi via WeChat	It specifies whether or not to enable the WiFi via WeChat function.
Valid Duration	It specifies the authentication validity period. A user must be re-authenticated for accessing the internet after the period expires.
Apply to	**Wired network**: It specifies the connected LAN ports. **Wireless network**: It specifies the enabled wireless network, including guest network. TIP - To make this function work properly, the wireless network to be applied should **not** be encrypted. Navigate to **Wireless** > **Wireless Settings**, select the **No Password** checkbox beside the applied wireless network and click **Save**. - If the WiFi network name you selected is modified, it will be automatically deselected here. To make the WiFi network effective, you have to re-select the WiFi network name with the new SSID here manually.

WeChat Open Platform Settings



WeChat Open Platform Settings

SSID:

ShopID:

AppID:

SecretKey:

Example

WeChat Official Account Parameters,
Shop Name: Luis Restaurant
SSID: HCD
ShopID: 8888888
AppID: WXC574E8987362
SecretKey: b4de5477edwe889

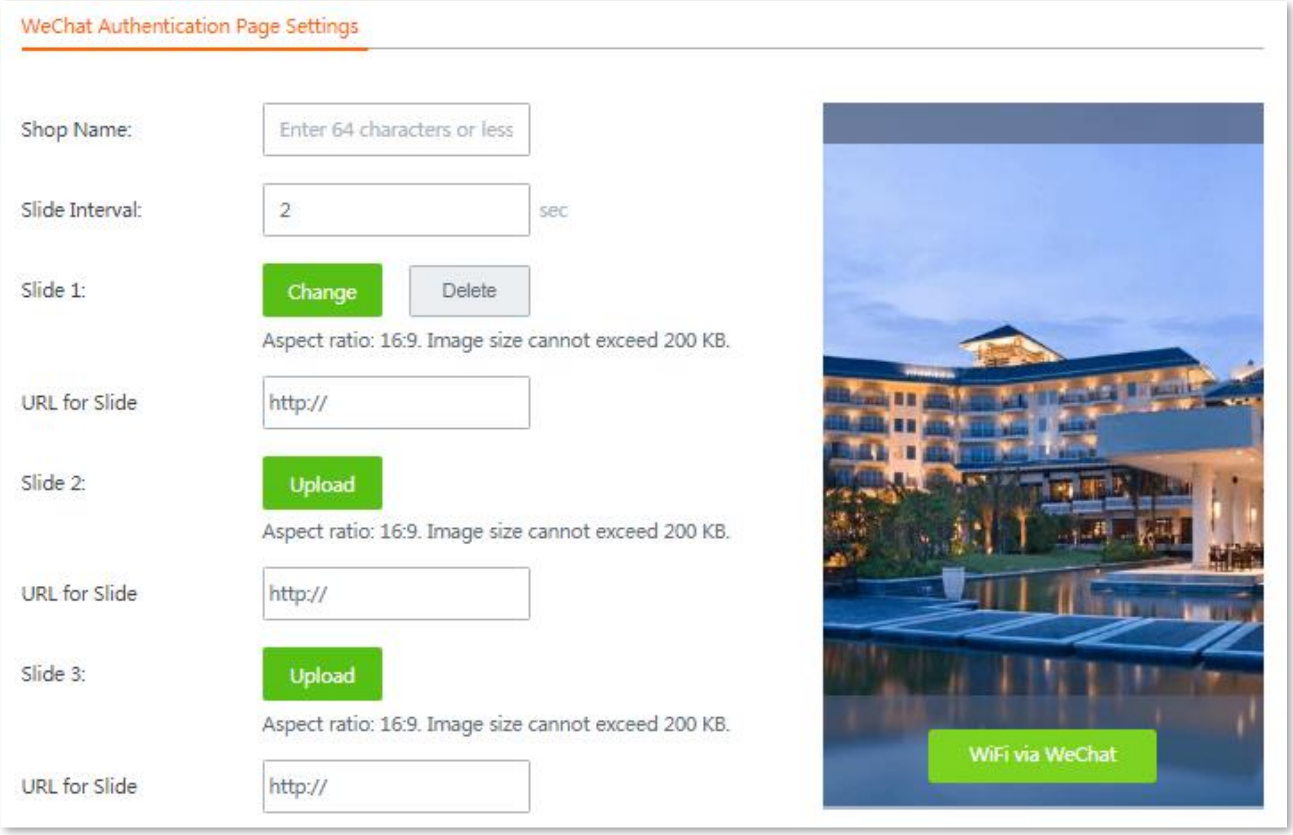
For how to apply for a WeChat official account, go tohttps://admin.wechat.com.

Parameter description

Parameter	Description
SSID	It specifies the wireless network name. You can enter the SSID you set on the WeChat open platform here. NOTE Once the SSID is modified, the SSID of **WiFi Network1** will be synchronized.
ShopID	It specifies the ID of the WeChat open platform shop, needs to be logged in to the WeChat public platform to check.

Parameter	Description
AppID	It specifies the unique identifier of the WeChat official account ID. You need to log in to the WeChat open platform to view it.
SecretKey	It specifies the key used for the encryption in the WeChat official account payment request, which can verify the unique identity of the merchant and must be logged in to the WeChat open platform to check.

WeChat Authentication Page Settings



WeChat Authentication Page Settings

Shop Name: Enter 64 characters or less

Slide Interval: 2 sec

Slide 1: Change Delete

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

URL for Slide http://

Slide 2: Upload

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

URL for Slide http://

Slide 3: Upload

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

URL for Slide http://

Parameter description

Parameter	Description
Shop Name	It allows you to set a shop name.
Slide Interval	It allows you to set the picture swapping period.
Slide 1/2/3	It specifies the pictures of the authentication page, supports adding up to 3 pictures.
URL for Slide 1/2/3	It specifies the website to link the picture, which can be an IP address or a domain name.
Change	It allows you to change a picture.
Delete	It allows you to delete an uploaded picture.
Upload	It allows you to upload a picture.

9.3.2 Example of configuring WiFi via WeChat

Networking requirement

A restaurant uses W15E to deploy its network. The enterprise has established a sound WeChat service platform, and plans to take the advantage of the mobile application with massive users to improve its visibility among customers, and improve customer's loyalty through agile services. It requires that:

- Restaurant manager and staffs can access to the wireless network without authentication.
- Guests need to get authenticated via WeChat when connecting to the wired and wireless network.

Solution

The WiFi via WeChat function can address this requirement.

Before you start

Get the following information first:

- WeChat open platform related parameters: including **ShopID**, **AppID**, and **SecretKey**
- **MAC address** or **IP address** of the clients used by restaurant managers and staffs

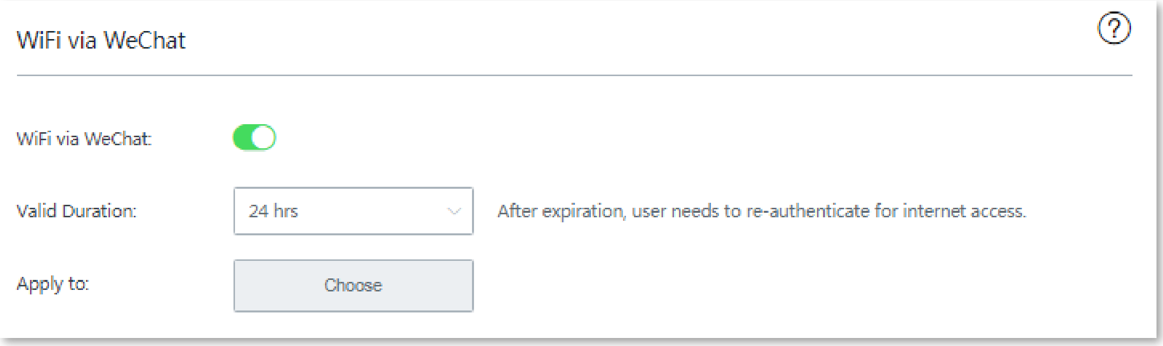
Procedure description

Step	Task	Description
1	Configuring basic network settings	Set up valid duration and networks to be applied to.
2	Registering and noting down WeChat open platform related parameters	Log in to the WeChat open platform, prepare and record the information of **SSID**, **ShopID**, **AppID**, and **SecretKey** to configure the router.
3	Configuring WeChat authentication page settings	Choose **WiFi via WeChat**, enable **WiFi via WeChat**, and set required parameters.
4	Adding hosts that do not need to get WeChat authentication.	Add authentication-free clients on **Authentication** > **User Management** page.

Configuration Procedure

Step 1 Configuring basic network settings.

1. Choose **Authentication** > **WiFi via WeChat**, and enable this function.



WiFi via WeChat

WiFi via WeChat: ●

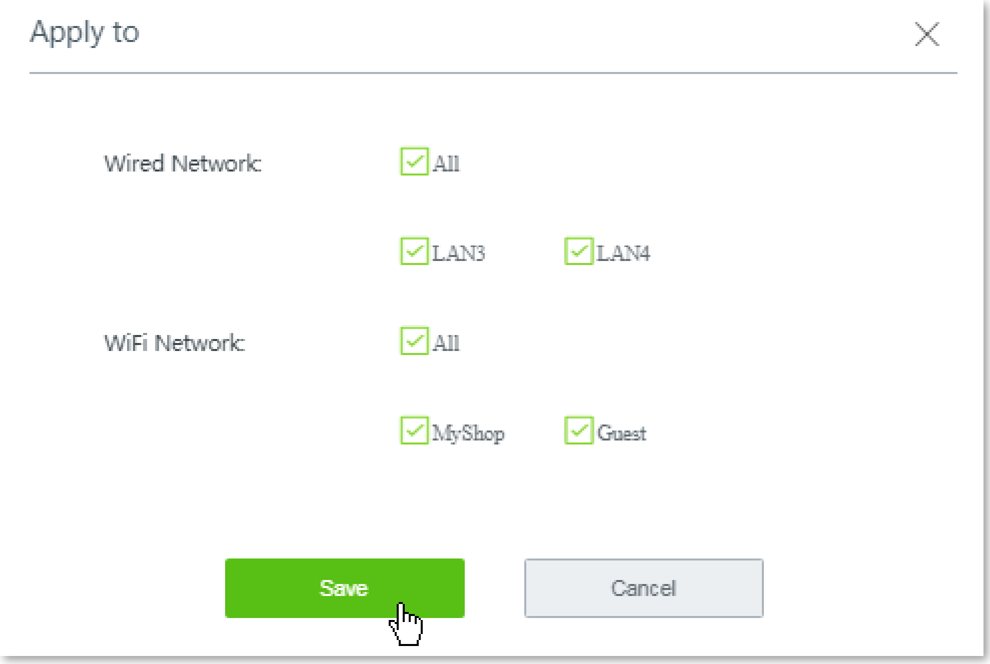
Valid Duration: 24 hrs

After expiration, user needs to re-authenticate for internet access.

Apply to:

2. Set up **Valid Duration** to **No Limit**.

3. Click **Choose** to choose networks to be applied, which is **All** for both wired and wireless networks, and click **Save**.



Apply to

Wired Network: ☑ All

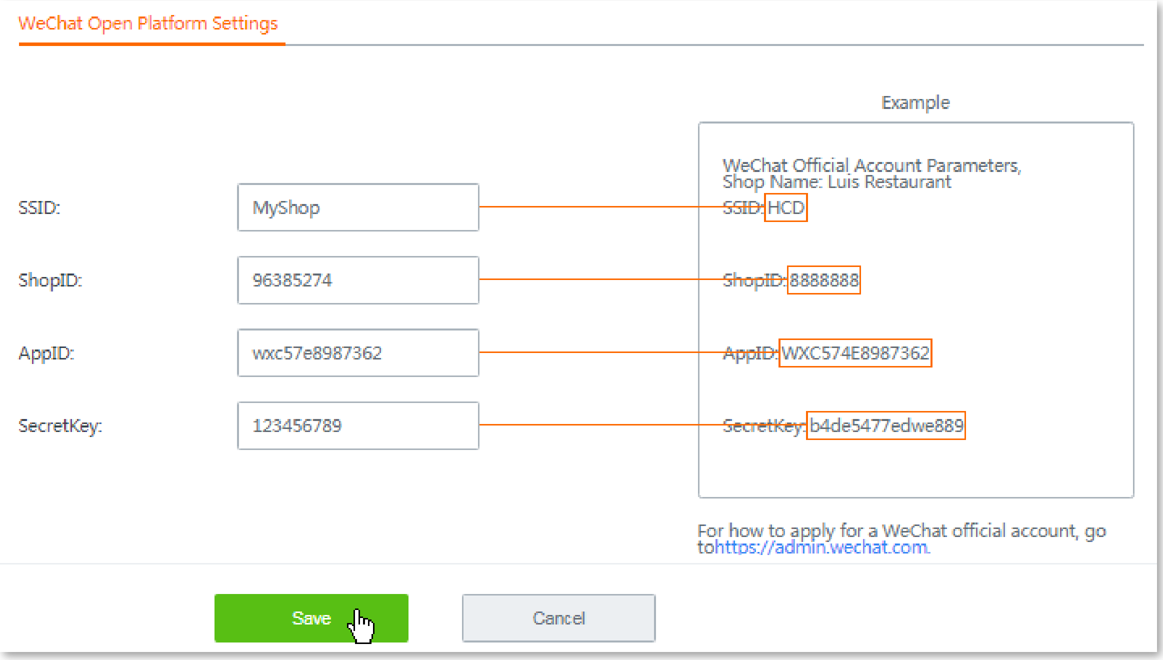
☑ LAN3 ☑ LAN4

WiFi Network: ☑ All

☑ MyShop ☑ Guest

Step 2 Register and note down WeChat open platform related parameters.

Assume that you have registered the following information:



WeChat Open Platform Settings

SSID: MyShop

ShopID: 96385274

AppID: wxc57e8987362

SecretKey: 123456789

Example

WeChat Official Account Parameters,
Shop Name: Luis Restaurant
SSID: HCD
ShopID: 8888888
AppID: WXC574E8987362
SecretKey: b4de5477edwe889

For how to apply for a WeChat official account, go tohttps://admin.wechat.com.

NOTE

Once the SSID is modified, the SSID of WiFi Network1 will be synchronized.

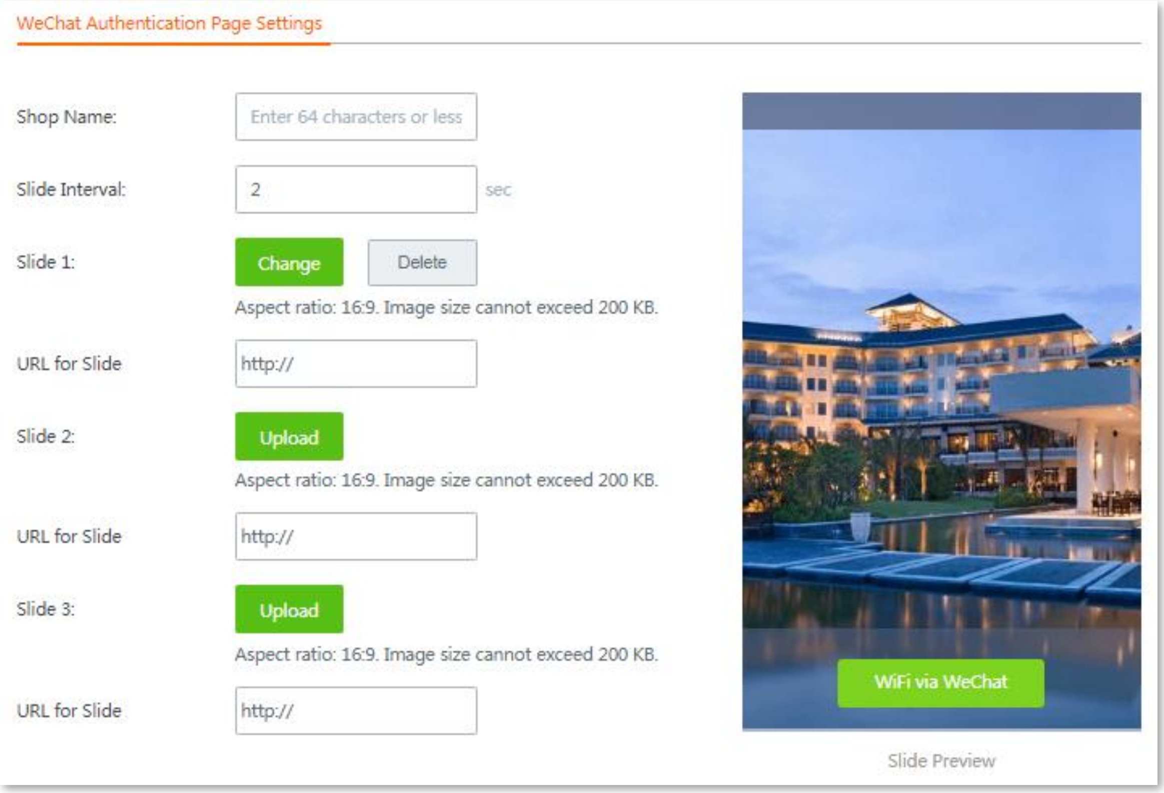
Step 3 **Set WeChat authentication page settings.**

1. Set **Shop Name**, which is **Tasty Restaurant** in this example.
2. Set **Slide Interval**, which is **2** seconds in this example.
3. Click **Change** or **Upload** to customize the images showing on the authentication page.

TIP

To replace an image, click **Delete** to delete it first, and upload a new one.

4. (Optional). Set the URL for slide 1/2/3, so that guests can be redirected to the website(s) you specified here when clicking the corresponding images.
5. Click **Save** at the bottom of the page.



WeChat Authentication Page Settings

Shop Name: Enter 64 characters or less

Slide Interval: 2 sec

Slide 1: Change Delete

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

URL for Slide http://

Slide 2: Upload

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

URL for Slide http://

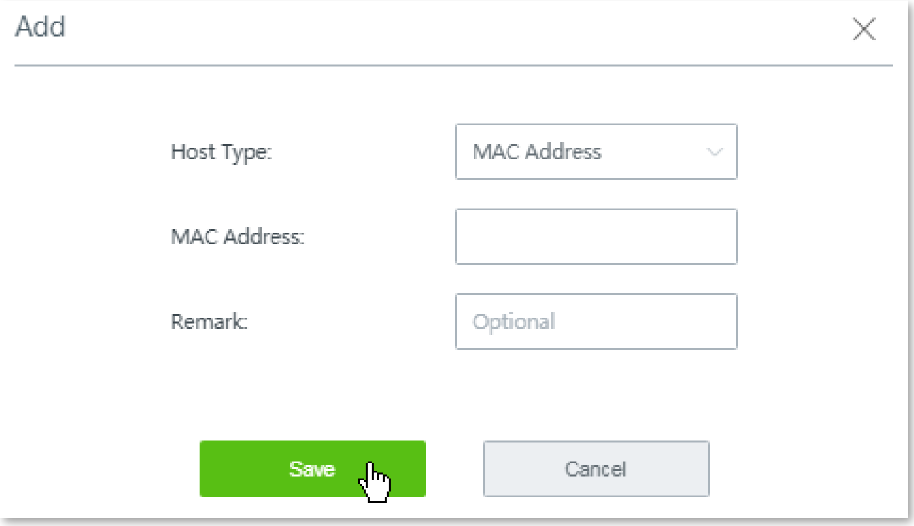
Slide 3: Upload

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

URL for Slide http://

Step 4 Add hosts that do not need to get WeChat authentication.

1. Choose **Authentication** > **User Management**, and locate the **Authentication-free Host** configuration area.
2. Click **+Add**. The **Add** configuration window appears.
3. Select **MAC Address** from the **Host Type** drop-down list menu, enter the MAC addresses of the client used by one staff, optionally enter a brief description in the **Remark** field for easy ID recognition, and click **Save**.



Add

Host Type: MAC Address

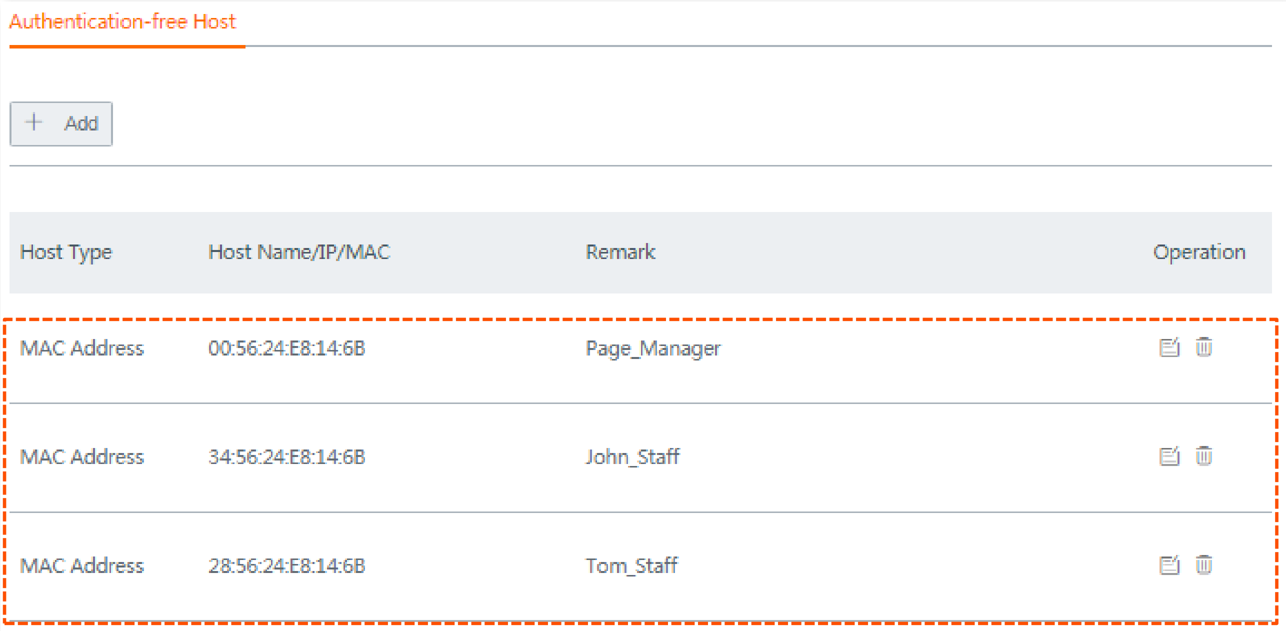
MAC Address:

Remark: Optional

4. Repeat the above step to add the rest authentication-free hosts one by one.

---- End

Added successfully. See the following figure:



Host Type	Host Name/IP/MAC	Remark	Operation
MAC Address	00:56:24:E8:14:6B	Page_Manager	
MAC Address	34:56:24:E8:14:6B	John_Staff	
MAC Address	28:56:24:E8:14:6B	Tom_Staff	

Verification

When guests connect to the wired and/or wireless networks with WiFi via WeChat enabled, they need to get authenticated through WeChat to access the internet.

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

Step 1 Connect to the wireless network with **WiFi via WeChat** enabled.

Step 2 Open a web browser on your mobile devices and access any website, it redirects to the user-defined WiFi via WeChat authentication page.

TIP

- For some mobile devices, the WiFi via WeChat authentication page will automatically pops up when they connect to the networks.
- If the website you visited is encrypted with **https** protocol, a warning page shows **Your connection is not private** appears. In this case, try another website that is encrypted with ***http*** protocol.

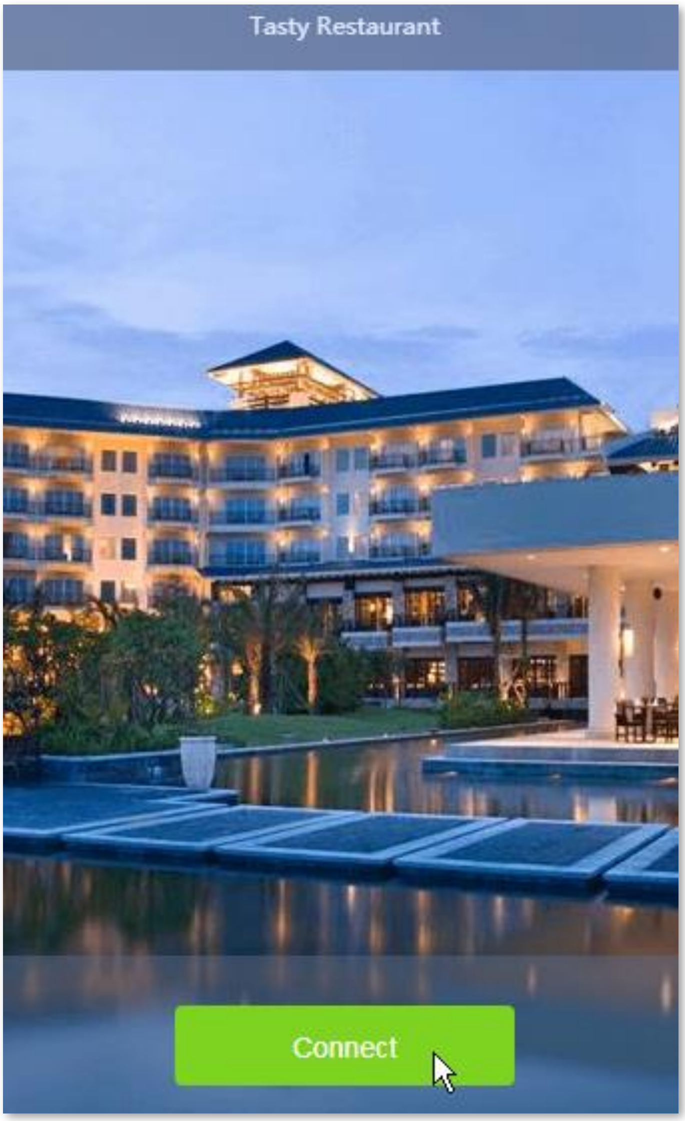
Step 3 Click **WiFi via WeChat**, and follow the on-screen instructions to access to the internet.

---- End

- Procedures for **computers** connected to the enabled wired or wireless network to connect using WiFi via WeChat are as follows:

Step 1 Connect to the wired or wireless network with **WiFi via WeChat** enabled.

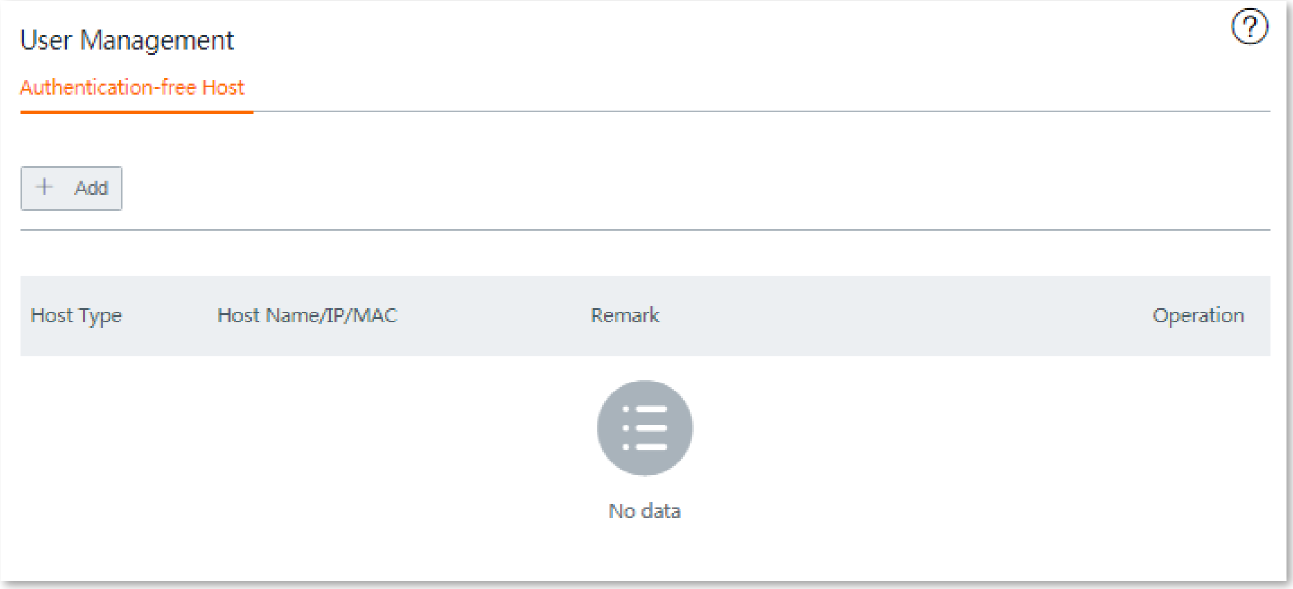
Step 2 On the authentication page, click **Connect** to access the internet.



---- End

9.4 Configuring authentication-free host

To add authentication-free host(s), choose **Authentication** > **User Management**. See the following figure.

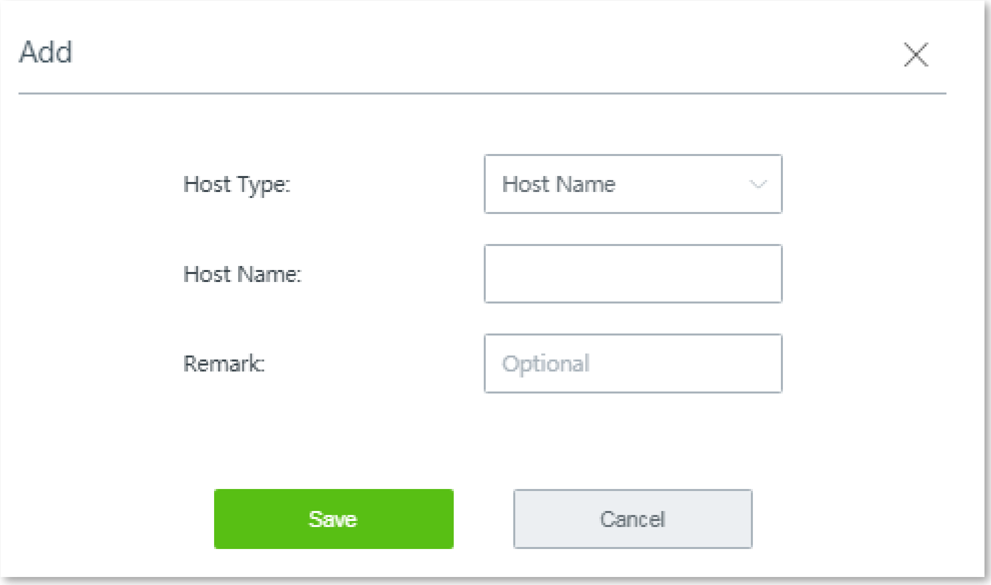


Host Type	Host Name/IP/MAC	Remark	Operation

Configuration procedure

Step 1 Click **+Add**.

Step 2 Set the required parameters.



Host Type: Host Name

Host Name:

Remark: Optional

Parameter description

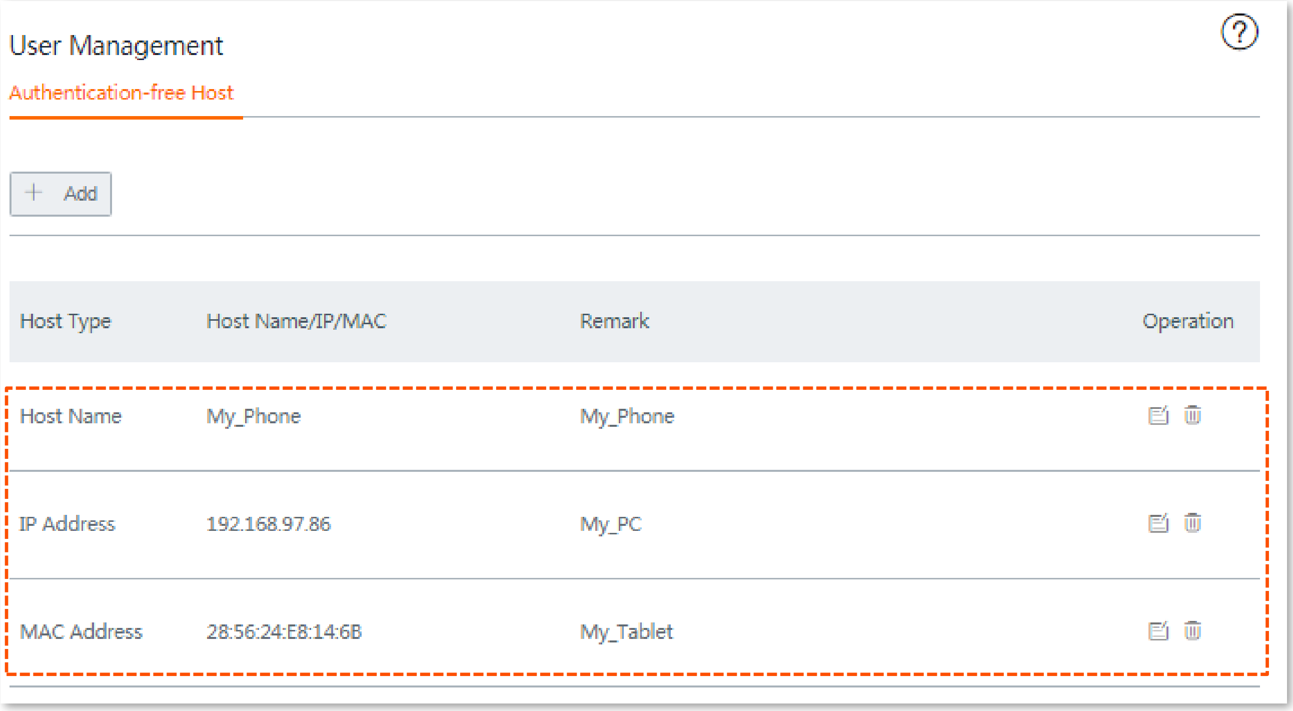
Parameter	Description
Host Type	It allows you to set a device without authentication based on host name, IP address or MAC address.
Host Name	When the **Host Type** is set as **Host Name**, input the host name of the authentication-free device. To get the host name of the device, navigate to **System Status** > **Online Devices**.

Parameter	Description
	TIP Once the host name is modified, the authentication-free rule will be disabled. To make such a rule effective, manually edit the **Host Name** here simultaneously.
IP Address	When **Host Type** is set as **IP Address**, input the IP address of the authentication-free device.
MAC Address	When **Host Type** is set as **MAC Address**, input the MAC address of the authentication-free device.
Remark	(Optional) It specifies a brief description of an authentication-free host.

Step 3 Click **Save**.

---- End

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



User Management

Host Type	Host Name/IP/MAC	Remark	Operation
Host Name	My_Phone	My_Phone	
IP Address	192.168.97.86	My_PC	
MAC Address	28:56:24:E8:14:6B	My_Tablet	

9.5 Configuring user accounts used for captive portal

On this area, you can:

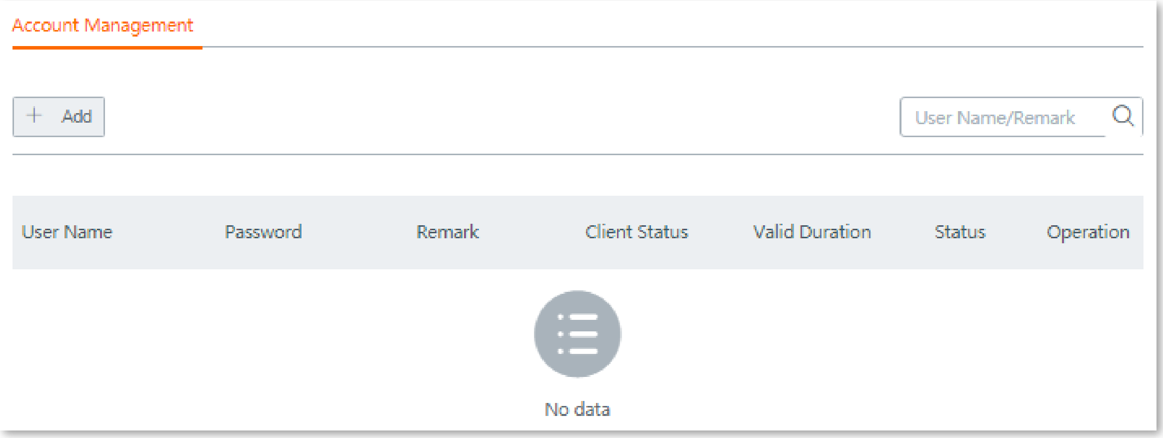
- Set up user accounts used for captive portal. If captive portal function is enabled, users can access the internet only after being authenticated with the accounts you created here.
- Export accounts data.
- Import accounts data.

9.5.1 Setting up users accounts used for captive portal

NOTE

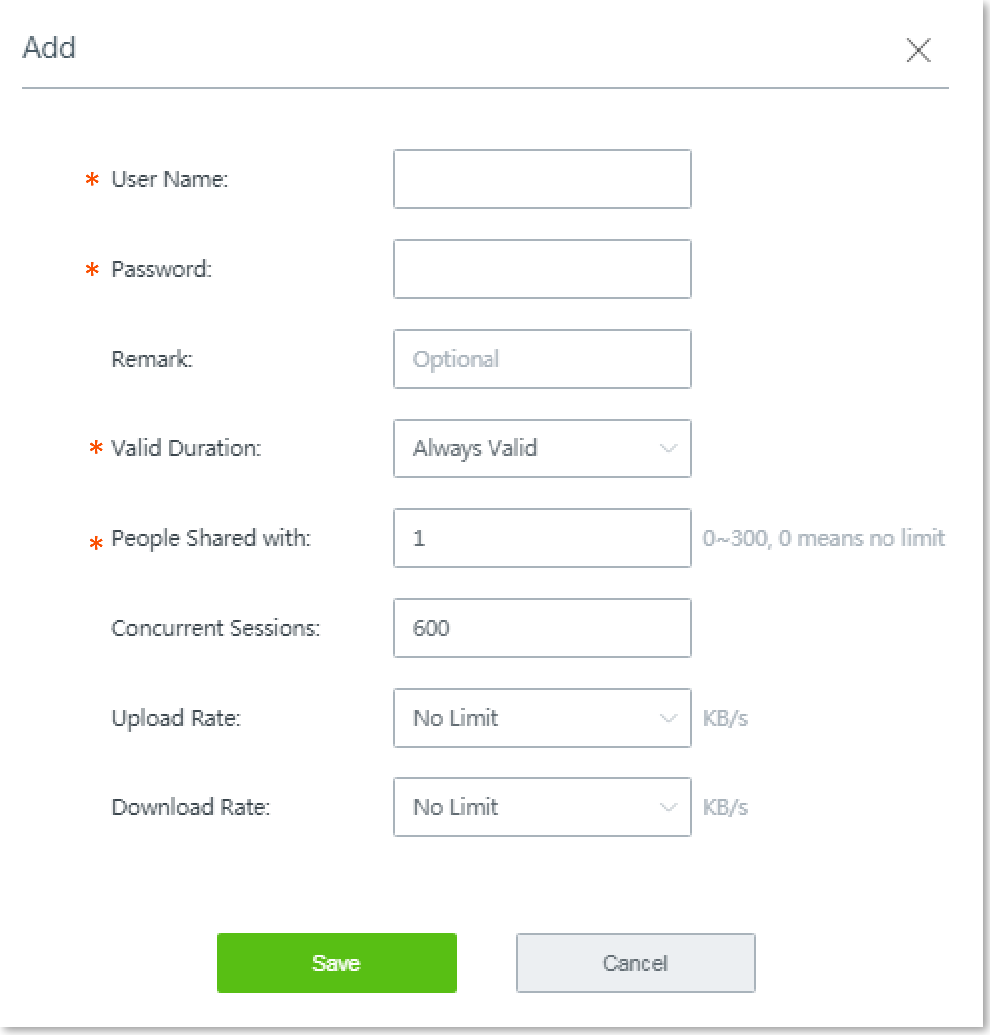
You are allowed to create a maximum of **300** accounts.

Step 1 Choose **Authentication** > **User Management**, and locate the **Account Management** configuration area.



Step 2 Click **+Add**.

Step 3 Set required parameters.



Add

* User Name:

* Password:

Remark: Optional

* Valid Duration: Always Valid

* People Shared with: 1 0~300, 0 means no limit

Concurrent Sessions: 600

Upload Rate: No Limit KB/s

Download Rate: No Limit KB/s

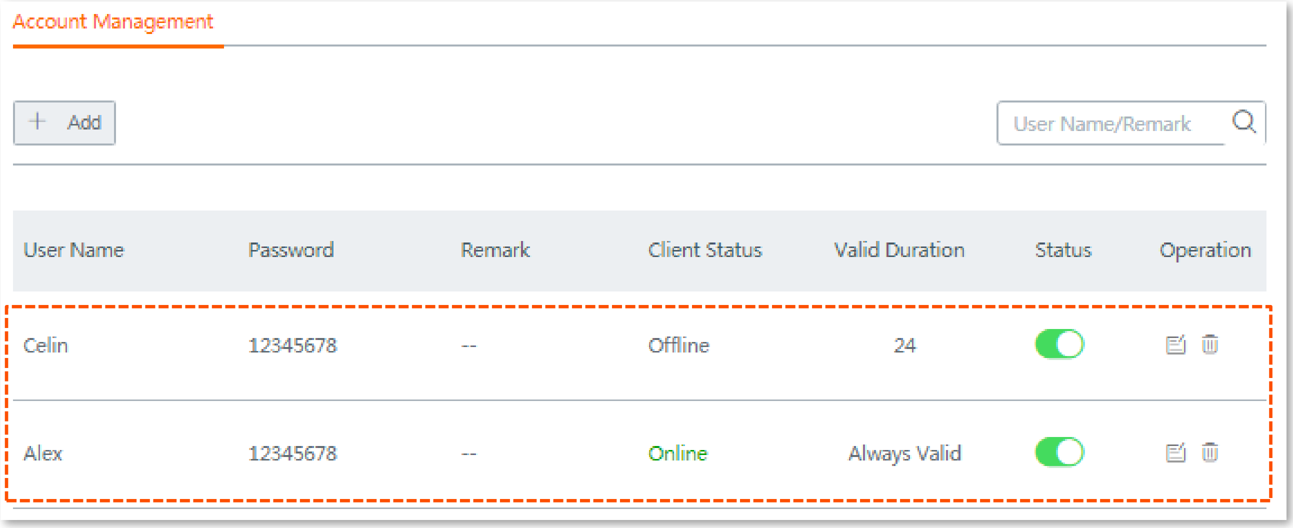
Parameter description

Parameter	Description
User Name	**User Name** specifies a user name for captive portal. **Password** specifies a password for captive portal. If captive portal is enabled, a user must be authenticated with a correct user name and password before accessing the internet.
Password	
Remark	(Optional). It specifies the description of a user account.
Valid Duration	It specifies the validity of a user account. **Valid Time**: Specify the validity time by hours. **Valid Date**: Specify the date before the account expires.
People Shared with	It specifies the number of users that the account is allowed for being authenticated.
Concurrent Sessions	It specifies the maximum number of connections that can be set up on each computer covered by the corresponding rule.
Upload Rate	It specifies the device’s maximum upload/download rate covered by the corresponding rule. TIP 1 Mbps=128 KB/s=1024 kb/s
Download Rate	

Step 4 Click **Save**.

---- End

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



User Name	Password	Remark	Client Status	Valid Duration	Status	Operation
Celin	12345678	--	Offline	24	●	✎ 🗑
Alex	12345678	--	Online	Always Valid	●	✎ 🗑

TIP

Client Status includes:

- **Offline**: The account is not in use.
- **Online**: The account is in use.

9.5.2 Exporting accounts data

Step 1 Choose **Authentication** > **User Management**, and move to the bottom of the page.

Step 2 Click **Export**.

----End

A file named ***auth_user.csv*** will be downloaded to your local computer.

9.5.3 Importing accounts data

NOTE

A maximum of **300** account data is allowed for importing at one time.

Step 1 Choose **Authentication** > **User Management**, and move to the bottom of the page.

Step 2 Click **Browse**, select and upload a file that you've backed up.

TIP

A proper file name may be indicated by **auth_user.csv**.

Step 3 Click **Import**.

----End

You can view the imported accounts information on the **Account Management** configuration area.

10 Filter management

10.1 Overview

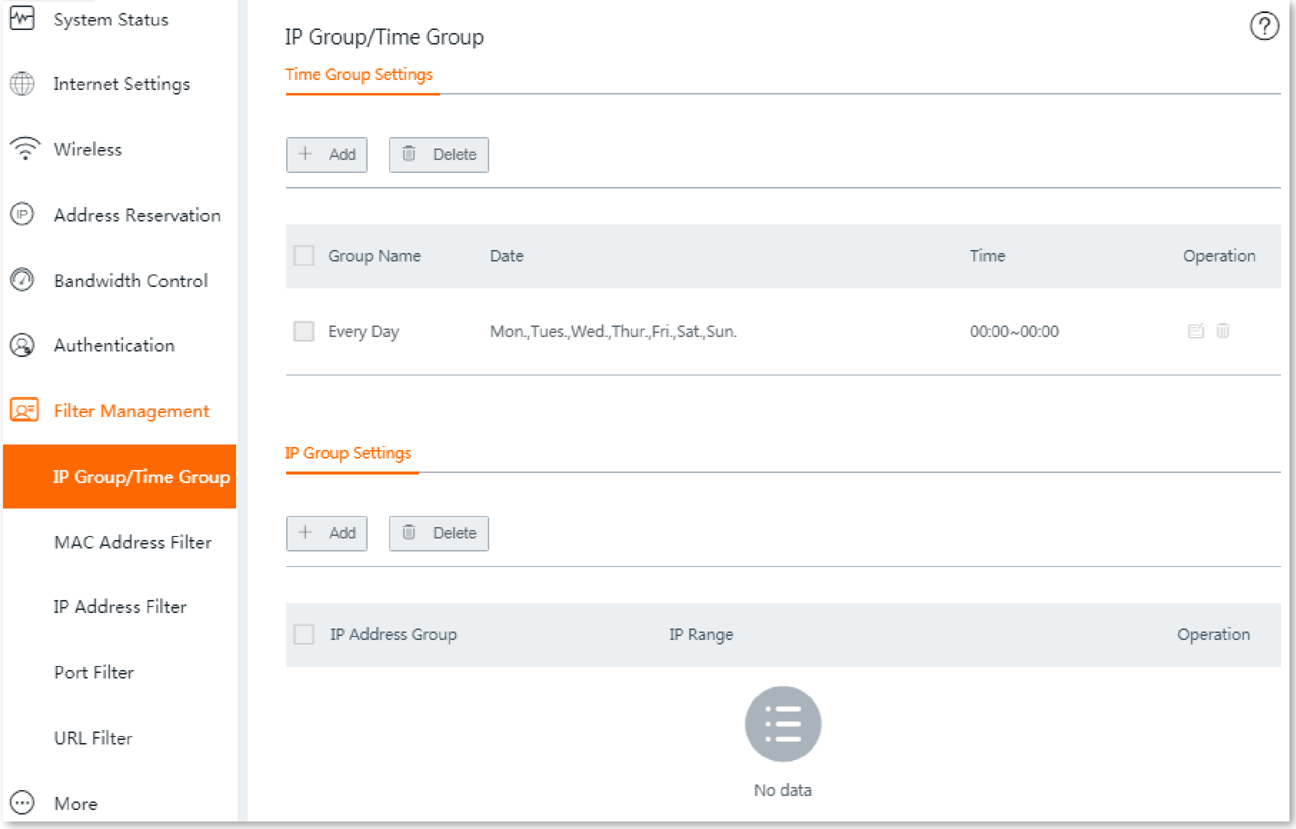
The router allows you to configure MAC address-based, port-based, and URL-based filter rules to control what clients can or cannot access what websites.

This chapter introduces how to configure:

- Configuring IP group and time group.
- MAC address filter
- IP address filter
- IP address filter
- URL filter

10.2 Configuring IP group and time group

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 Settings

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

IP Group Settings

□	IP Address Group	IP Range	Operation

No data

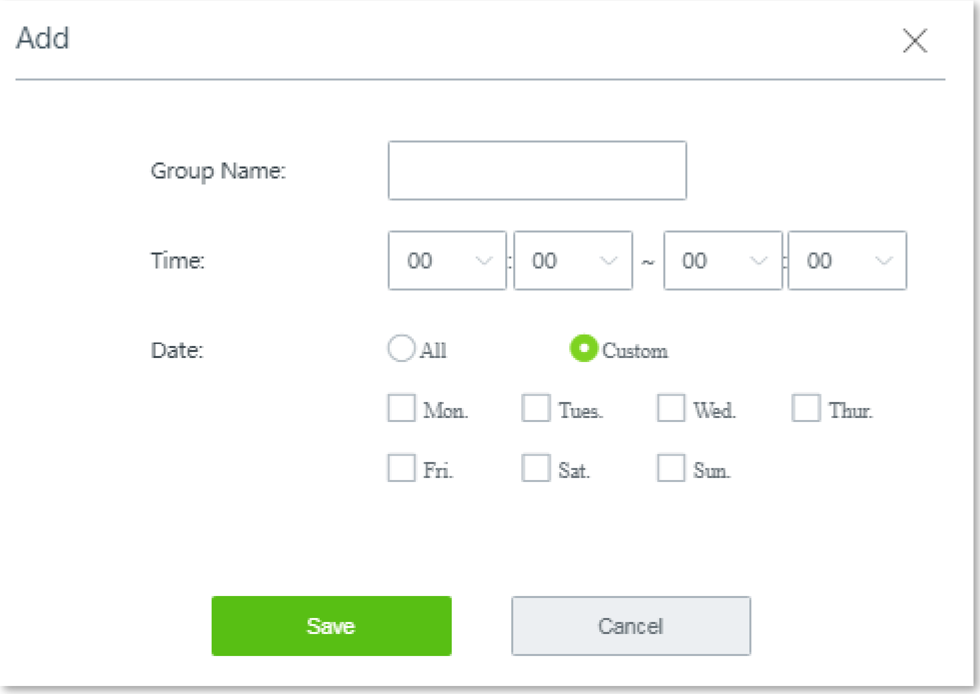
10.2.1 Configuring time groups

TIP

- By default, there is a time rule named **Every Day** which cannot be edited or deleted.
- A time group that has been referenced cannot be deleted.

Step 1 Choose **Filter Management** > **IP Group/Time Group** page, and locate the **Time Group Settings** configuration area.

Step 2 Click **+Add**. The **Add** configuration window appears.



Add

Group Name:

Time: 00 : 00 ~ 00 : 00

Date: ○ All ● Custom

□ Mon. □ Tues. □ Wed. □ Thur.

□ Fri. □ Sat. □ Sun.

Step 3 Set the required parameters.

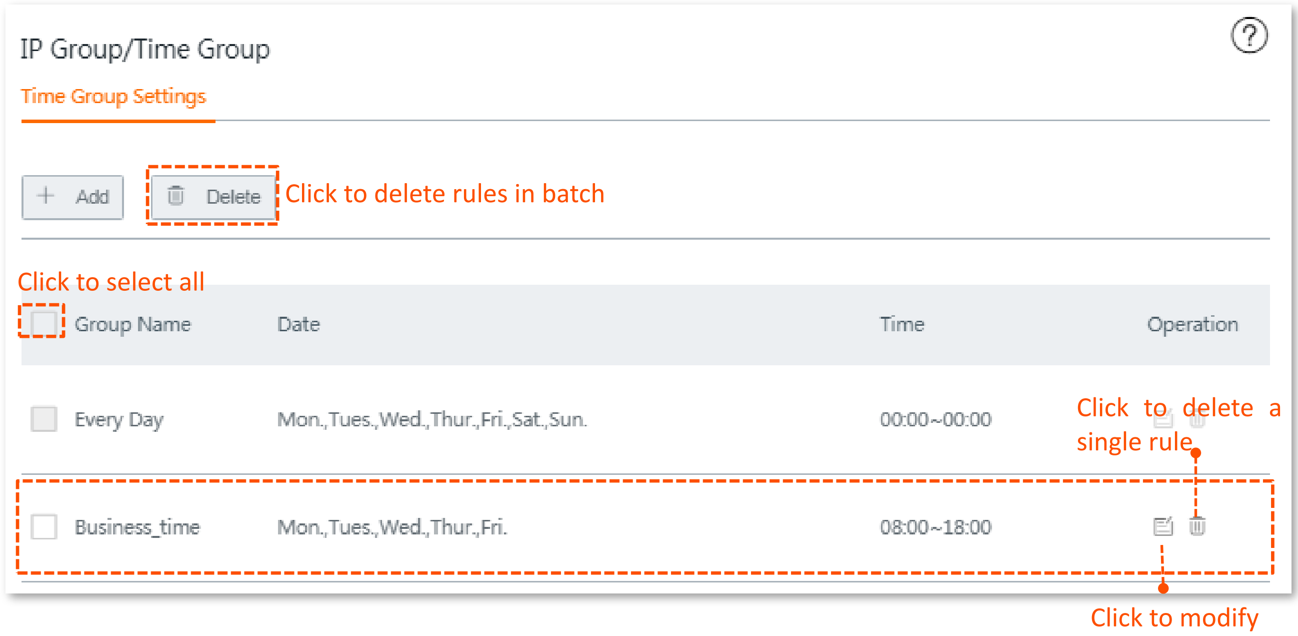
TIP

- Duplicate group names are **not** allowed.
- **00:00~00:00** indicates a whole day.

Step 4 Click **Save**.

---- End

Added successfully. See the following figure.



IP Group/Time Group

Time Group Settings

□ Group Name	Date	Time	Operation
□ Every Day	Mon.,Tues.,Wed.,Thur.,Fri.,Sat.,Sun.	00:00~00:00	
□ Business_time	Mon.,Tues.,Wed.,Thur.,Fri.	08:00~18:00	

Click to delete rules in batch

Click to select all

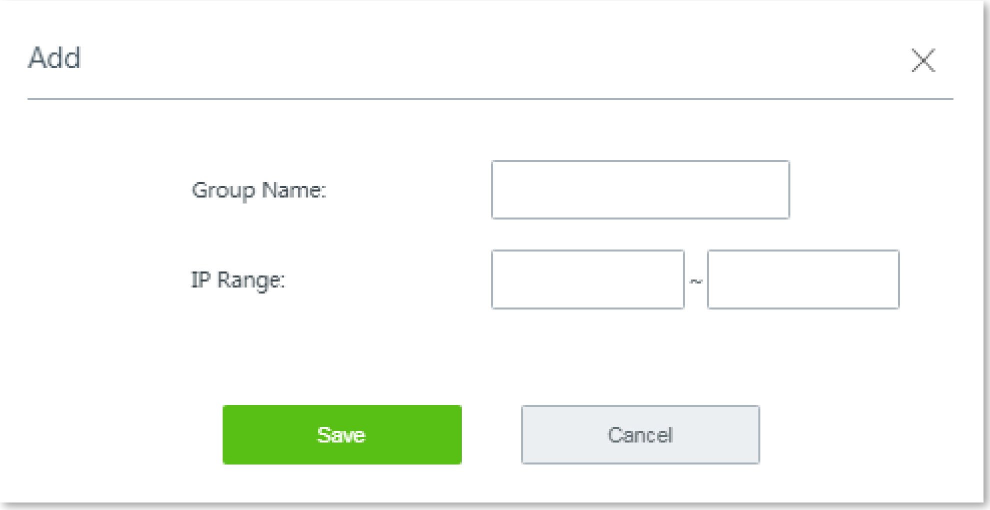
Click to delete a single rule

Click to modify

10.2.2 Configuring IP groups

Step 1 Choose **Filter Management** > **IP Group/Time Group**, and locate the **IP Group Settings** configuration area.

Step 2 Click **+Add**. The **Add** configuration window appears.



Add

Group Name:

IP Range: ~

Step 3 Set the required parameters.

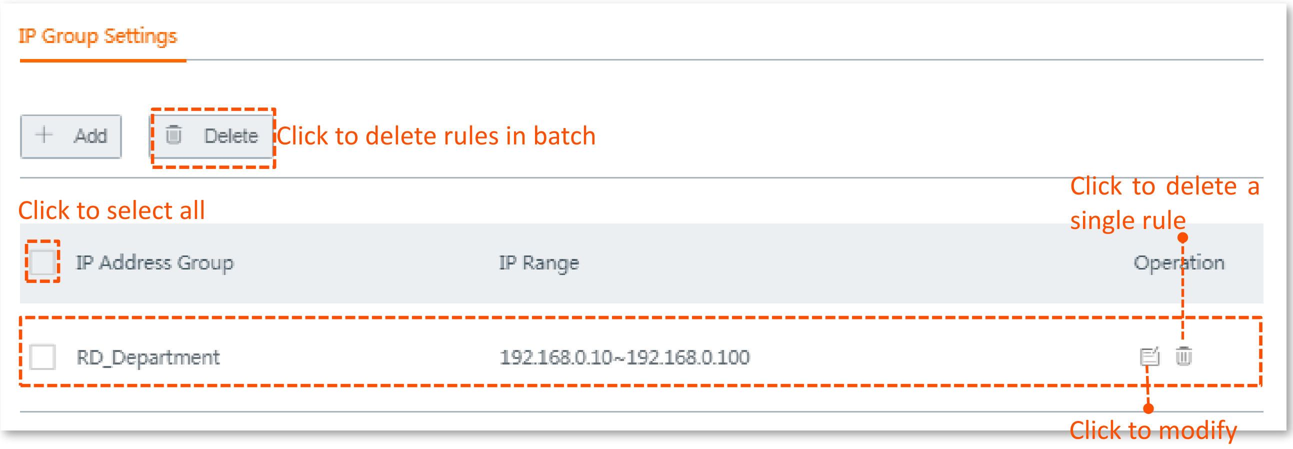
TIP

Duplicate group names are **not** allowed.

Step 4 Click **Save**.

---- End

Added successfully. See the following figure.



Click to delete rules in batch

Click to select all

Click to delete a single rule

Click to modify

□	IP Address Group	IP Range	Operation
□	RD_Department	192.168.0.10~192.168.0.100	

TIP

An IP address group that is in use cannot be deleted.

10.3 MAC address filter

This is a time group-related function. You can create MAC address-based rules to decide whether or not clients can access the internet through the router on what time.

10.3.1 Configuring the MAC address filter

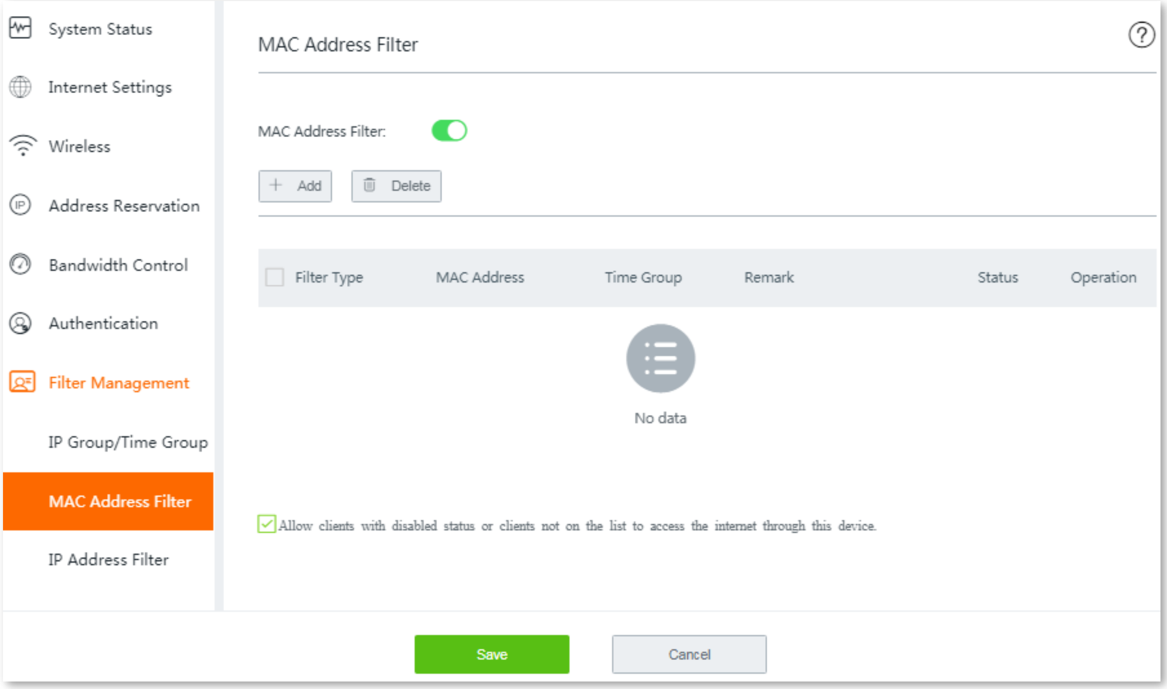
Before you start

Set up at least one time group rule. The default time group name is **Every Day**.

Configuration procedure

Step 1 Choose **Filter Management** > **MAC Address Filter**.

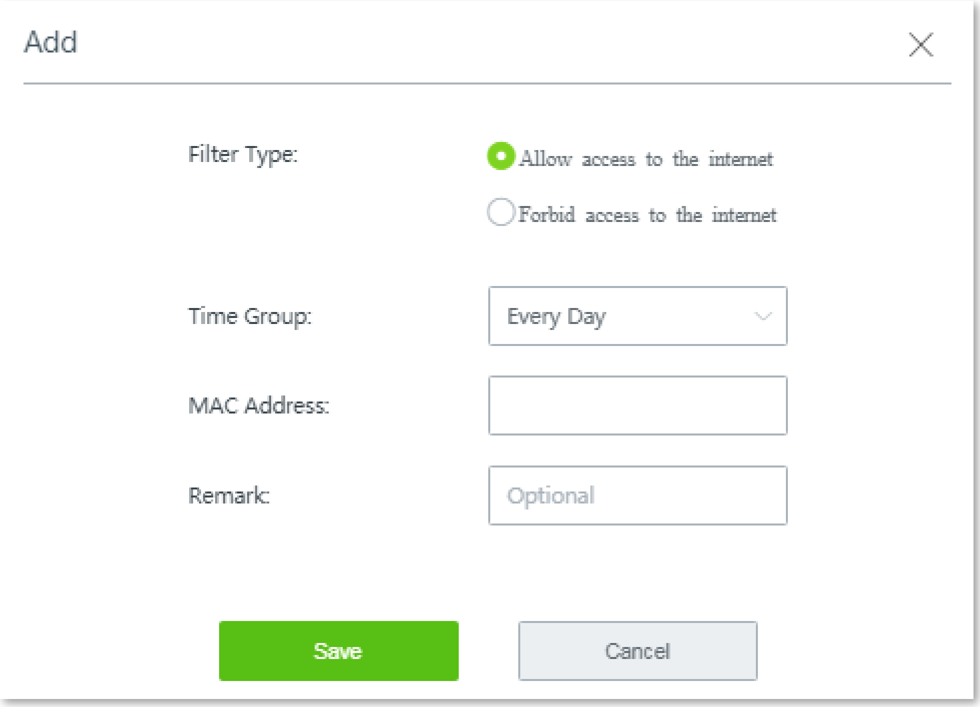
Step 2 Enable this function, and click **Save**.



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

Step 3 Configuring MAC address filter rule(s).

1. Click **+Add**. The **Add** configuration window appears.



Add

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

Time Group: Every Day

MAC Address:

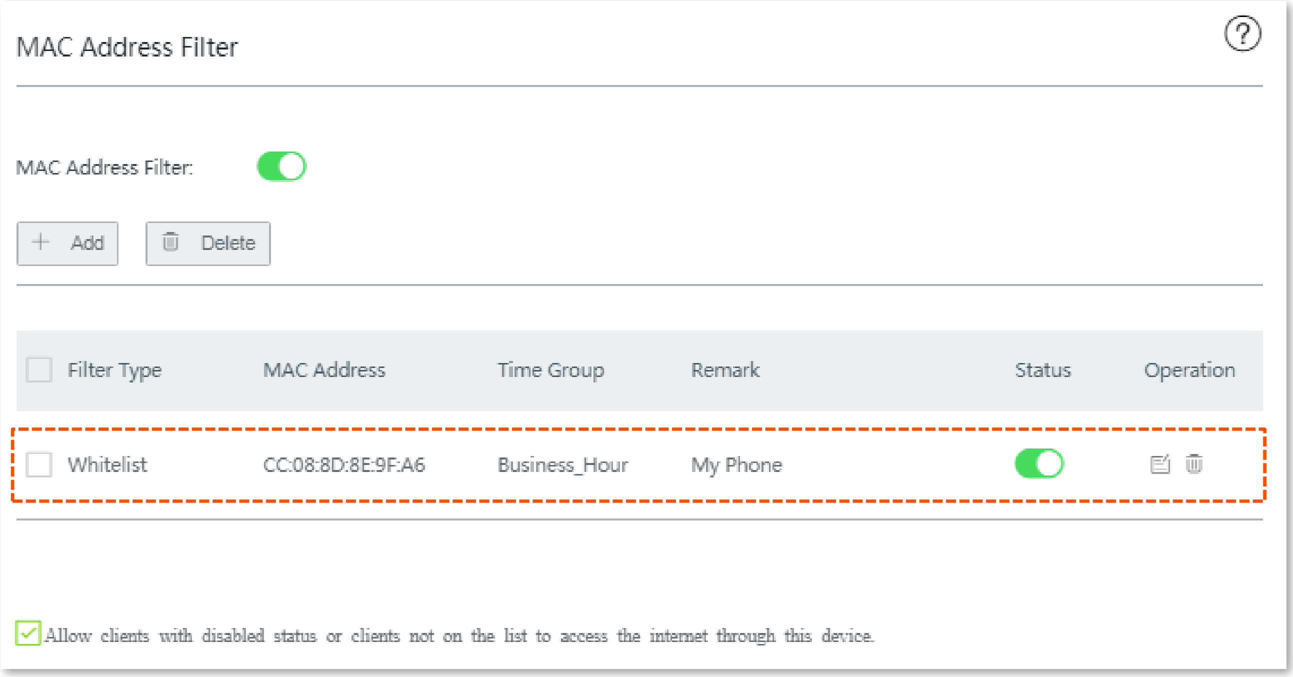
Remark: Optional

2. Set the required parameters.

3. Click **Save**.

---- **End**

Added successfully. See the following figure:



MAC Address Filter

MAC Address Filter: ●

□ Filter Type	MAC Address	Time Group	Remark	Status	Operation
□ Whitelist	CC:08:8D:8E:9F:A6	Business_Hour	My Phone	●	

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

10.3.2 Example of configuring MAC address filter rule(s)

Networking requirement

An enterprise uses W15E to set up a LAN to address the following requirement:

During business hours (08:00 to 18:00 on weekday), only the purchaser is allowed to access the internet. Assume that the MAC address of the purchaser's computer is CC:3A:61:71:1B:6E.

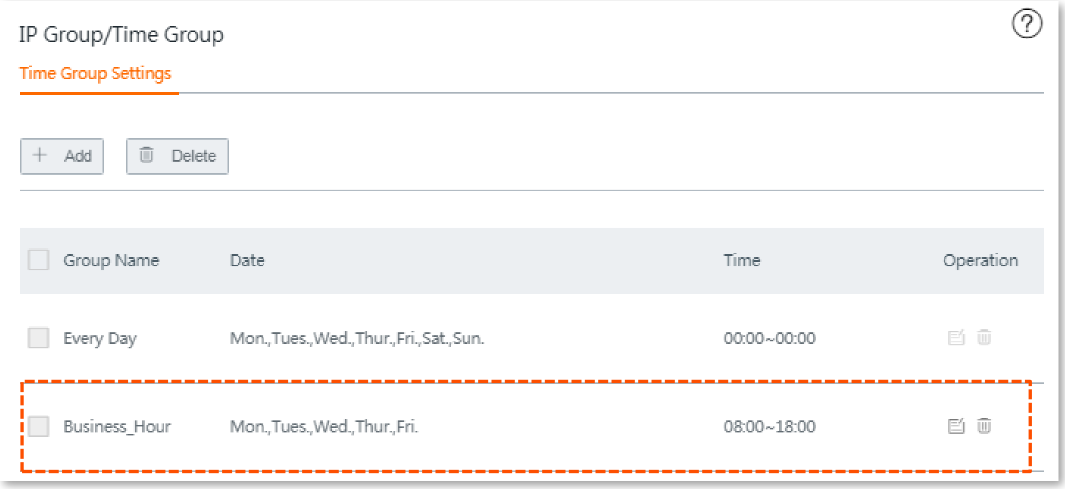
Solutions

The MAC address filter can meet this requirement.

Configuration procedure

Step 1 Set up a time group.

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



IP Group/Time Group

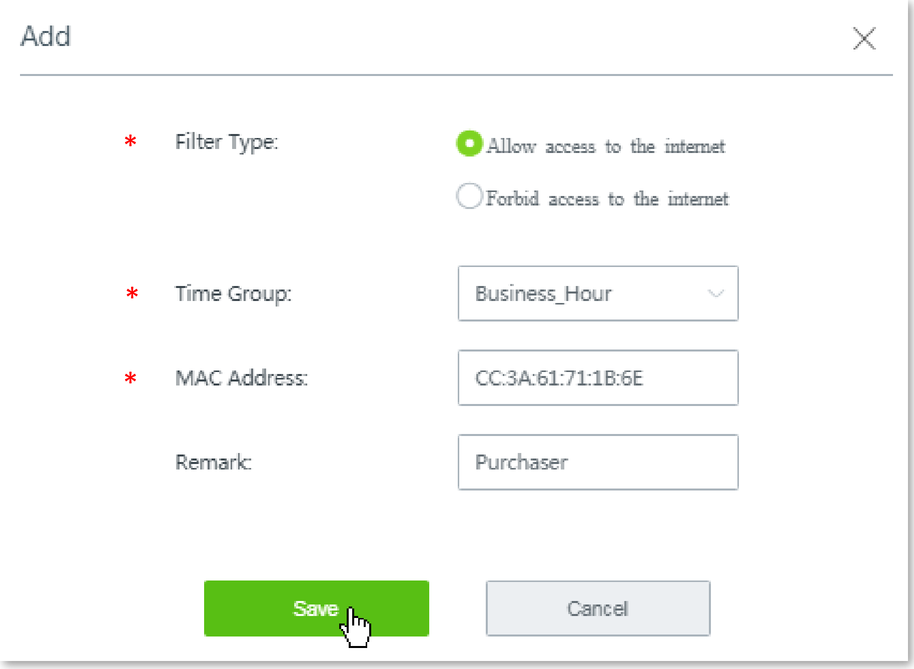
Time Group Settings

+ Add | Delete

□	Group Name	Date	Time	Operation
□	Every Day	Mon.,Tues.,Wed.,Thur.,Fri.,Sat.,Sun.	00:00~00:00	
□	Business_Hour	Mon.,Tues.,Wed.,Thur.,Fri.	08:00~18:00	

Step 2 Set an MAC address filter rule.

1. Choose **Filter Management** > **MAC Address Filter**, enable this function, and click **Save**.
2. Click **+Add**. The **Add** window appears.
3. Set the required parameter, and click **Save**. See the following figure.



Add

* Filter Type: ● Allow access to the internet ○ Forbid access to the internet

* Time Group: Business_Hour

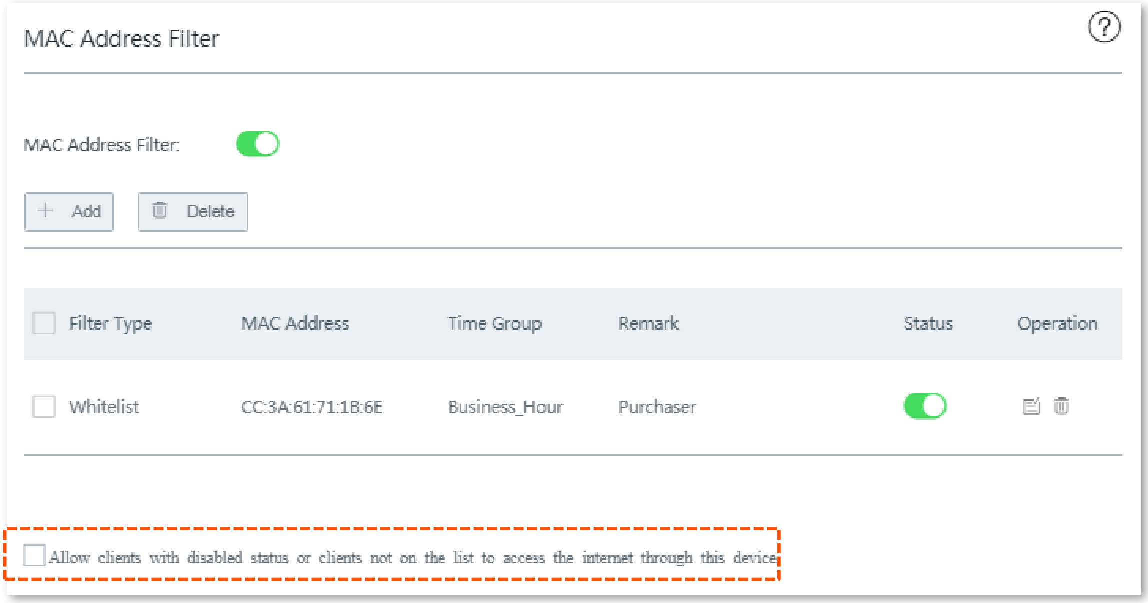
* MAC Address: CC:3A:61:71:1B:6E

Remark: Purchaser

TIP

- Parameters indicated with * are mandatory.
- You are recommended to enter a brief description on the rule in **Remark** field for later management.

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



MAC Address Filter

MAC Address Filter: ●

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

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

5. Click **Save** at the bottom of the page to apply your settings.

---- End

Verification

During 08:00 to 18:00 on weekdays, only the purchaser’s computer can access the internet.

10.4 IP address filter

This is a time group-related function. You can create IP address-based rules to decide whether or not clients can access the internet through the router on what time.

10.4.1 Configuring the IP address filter

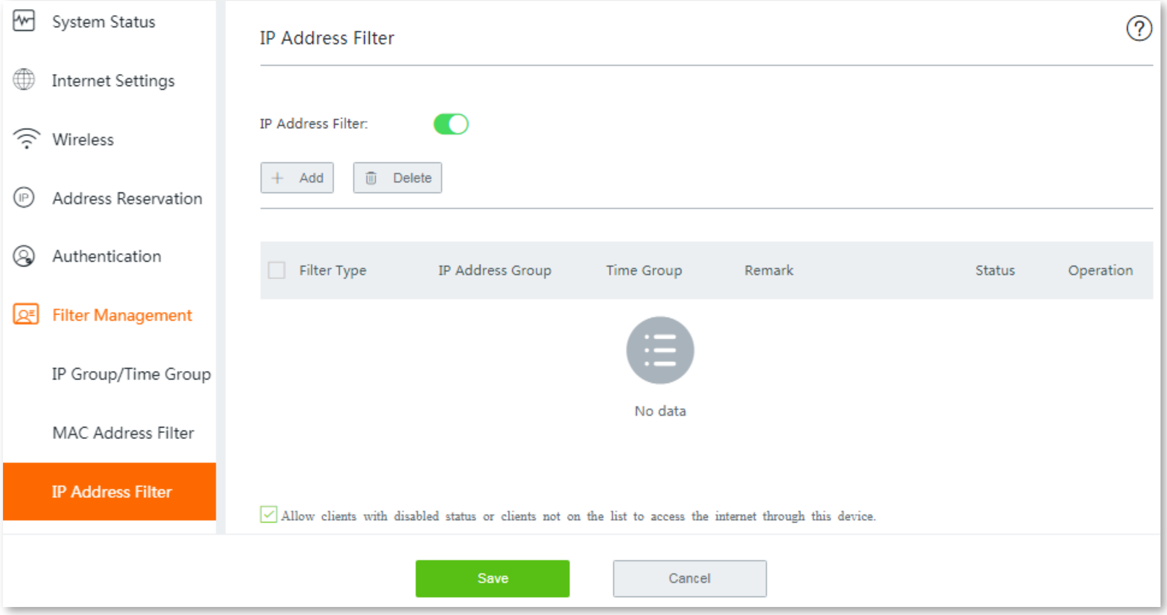
Before you start

- Set up at least one time group rule.
- Set up at least one IP group rule.
- To make IP address-based filter rules always take effect, specify a static IP address for the clients.

Configuration procedure

Step 1 Choose **Filter Management** > **IP Address Filter**.

Step 2 Enable this function, and click **Save**.



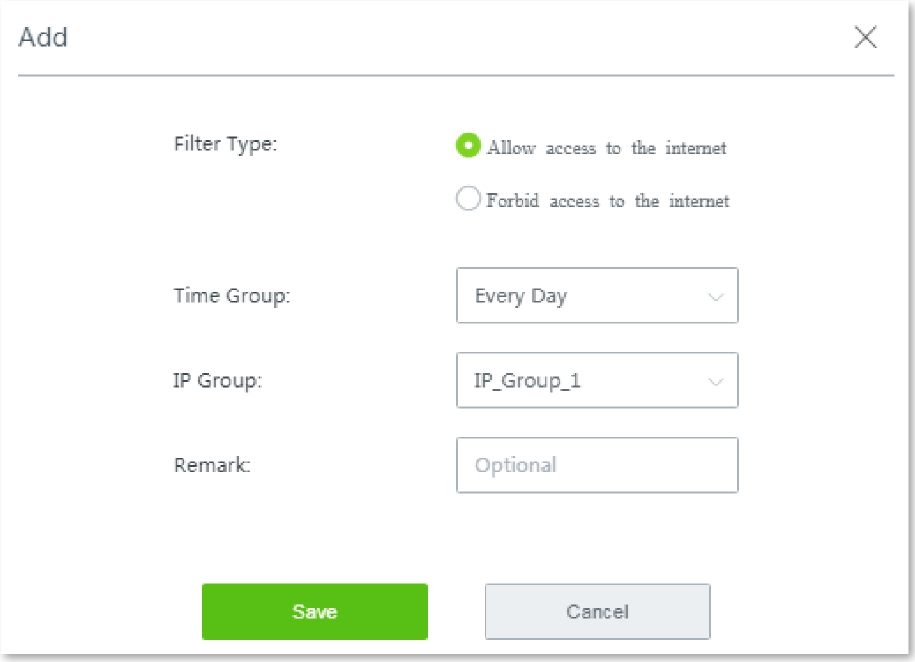
IP Address Filter: ●

□ Filter Type	IP Address Group	Time Group	Remark	Status	Operation

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

Step 3 Configure IP address filter rule(s).

1. Click **+Add**. The **Add** configuration window appears.



Add

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

Time Group: Every Day

IP Group: IP_Group_1

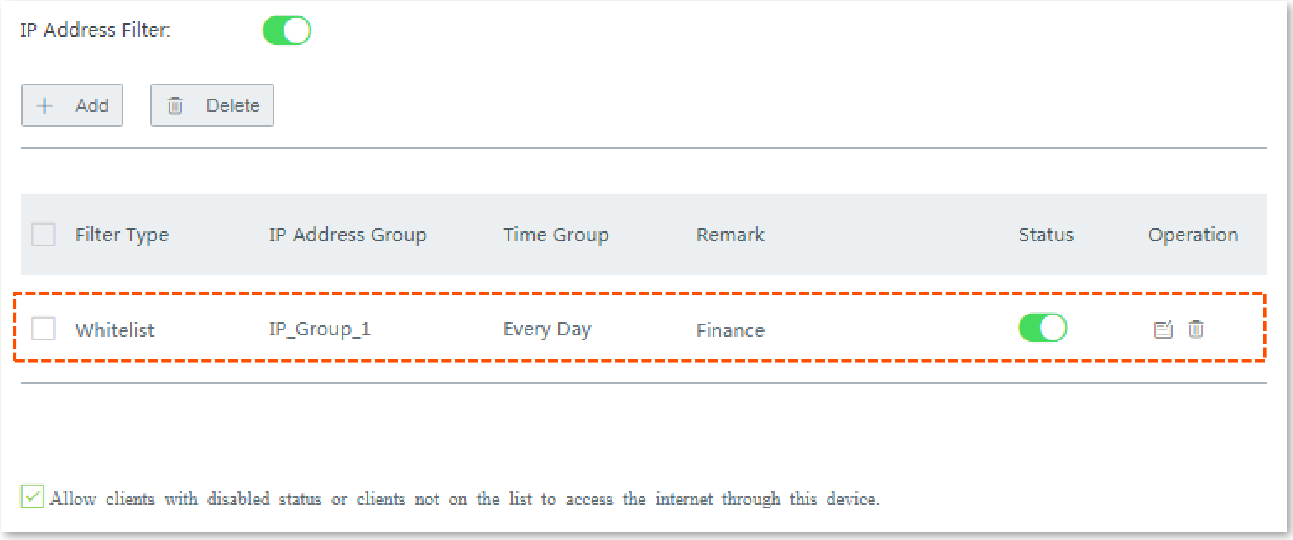
Remark: Optional

2. Set the required parameters.

3. Click **Save**.

---- End

Added successfully. See the following figure:



IP Address Filter:

□ Filter Type	IP Address Group	Time Group	Remark	Status	Operation
□ Whitelist	IP_Group_1	Every Day	Finance		

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

10.4.2 Example of configuring IP address filter rule(s)

Networking requirement

An enterprise uses W15E to set up a LAN to address the following requirement:

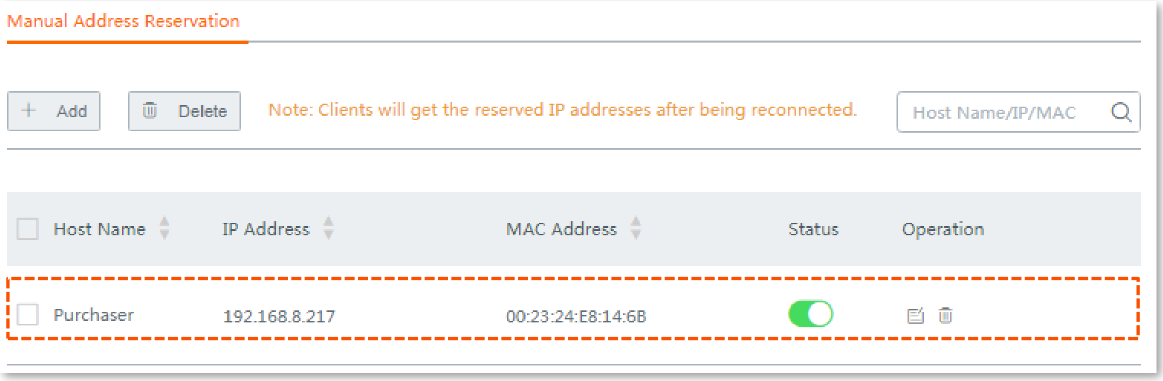
During business hours (08:00 to 18:00 on weekday), only the purchaser is allowed to access the internet. Assume that the IP address of the purchaser's computer is 192.168.8.217.

Solution

The IP address filter can meet this requirement.

Configuration procedure

Step 1 Specify a static IP address for the purchaser's computer, which is **192.168.8.217** in this example.


Manual Address Reservation
+ Add
Delete
Note: Clients will get the reserved IP addresses after being reconnected.
Host Name/IP/MAC

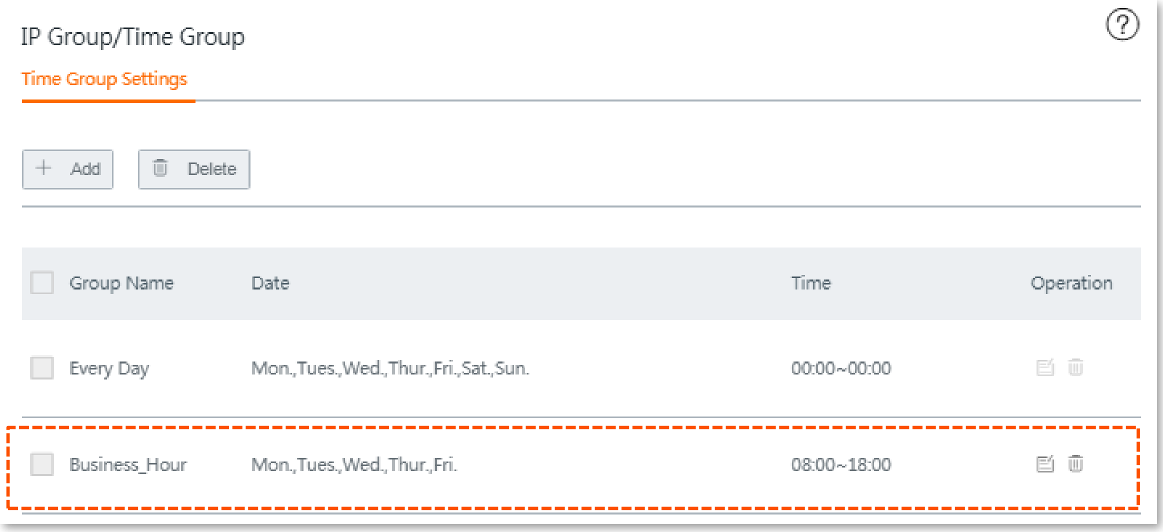
□	Host Name	IP Address	MAC Address	Status	Operation
□	Purchaser	192.168.8.217	00:23:24:E8:14:6B	●	

TIP

Refer to Address reservation for detailed description of configuration procedure.

Step 2 **Set up a time group.**

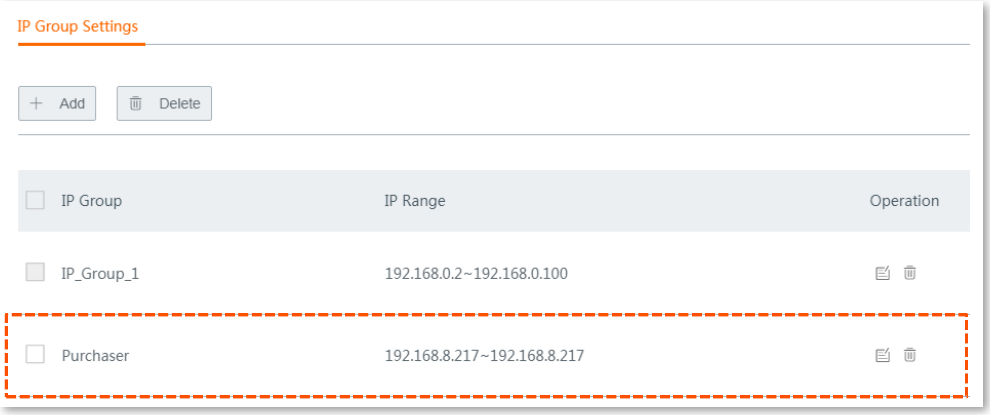
1. Choose **Filter Management** > **IP Group/Time Group**.
2. Set a time group shown in the following figure.



□	Group Name	Date	Time	Operation
□	Every Day	Mon.,Tues.,Wed.,Thur.,Fri.,Sat.,Sun.	00:00~00:00	
□	Business_Hour	Mon.,Tues.,Wed.,Thur.,Fri.	08:00~18:00	

Step 3 **Set up an IP group.**

1. Choose **Filter Management** > **IP Group/Time Group**, and locate the **IP Address Settings**.
2. Set an IP group shown in the following figure.



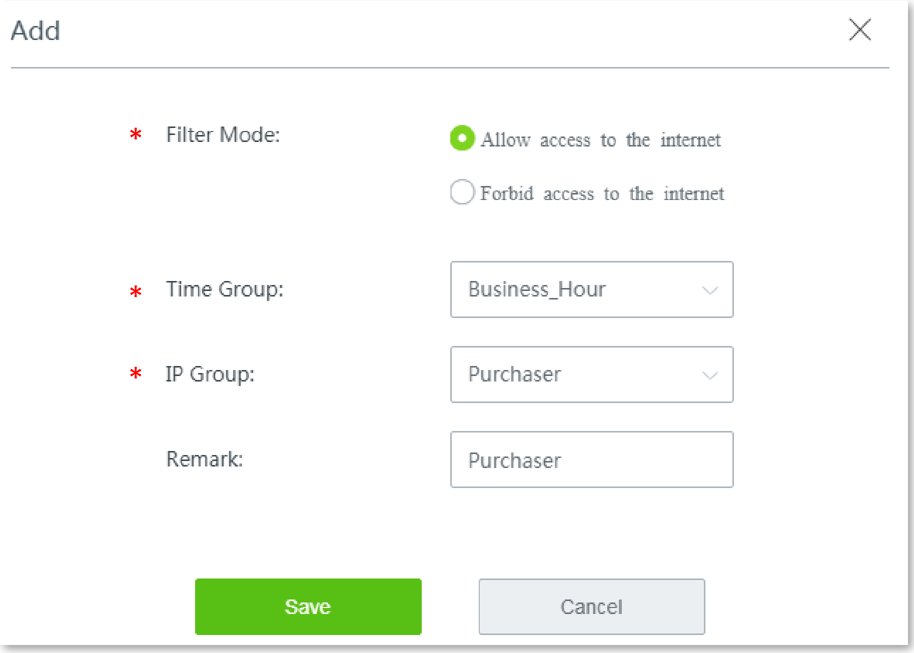
IP Group Settings

+ Add | Delete

□ IP Group	IP Range	Operation
□ IP_Group_1	192.168.0.2~192.168.0.100	
□ Purchaser	192.168.8.217~192.168.8.217	

Step 4 **Set IP address filter rule(s).**

1. Choose **Filter Management** > **IP Address Filter**.
2. Enable this function, and click **Save**.
3. Click **+Add**. The **Add** window appears.
4. Set required parameter, and click **Save**.



Add

* Filter Mode: ● Allow access to the internet ○ Forbid access to the internet

* Time Group: Business_Hour

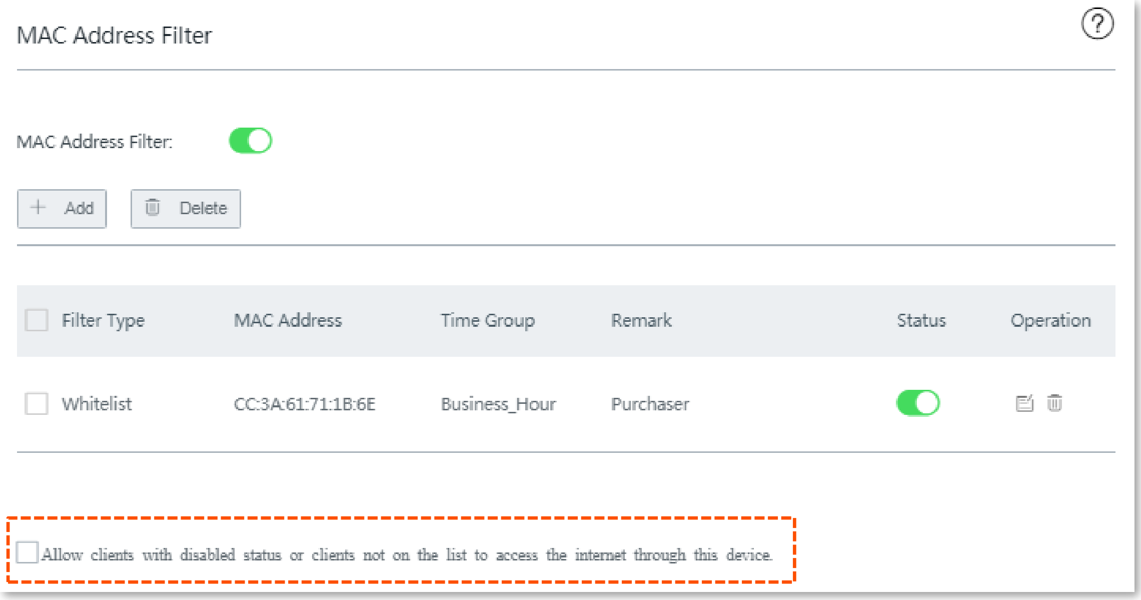
* IP Group: Purchaser

Remark: Purchaser

TIP

Parameters indicated with * are mandatory.

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



MAC Address Filter

MAC Address Filter: ●

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

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

6. Click **Save** at the bottom of the page to apply your settings.

---- End

Verification

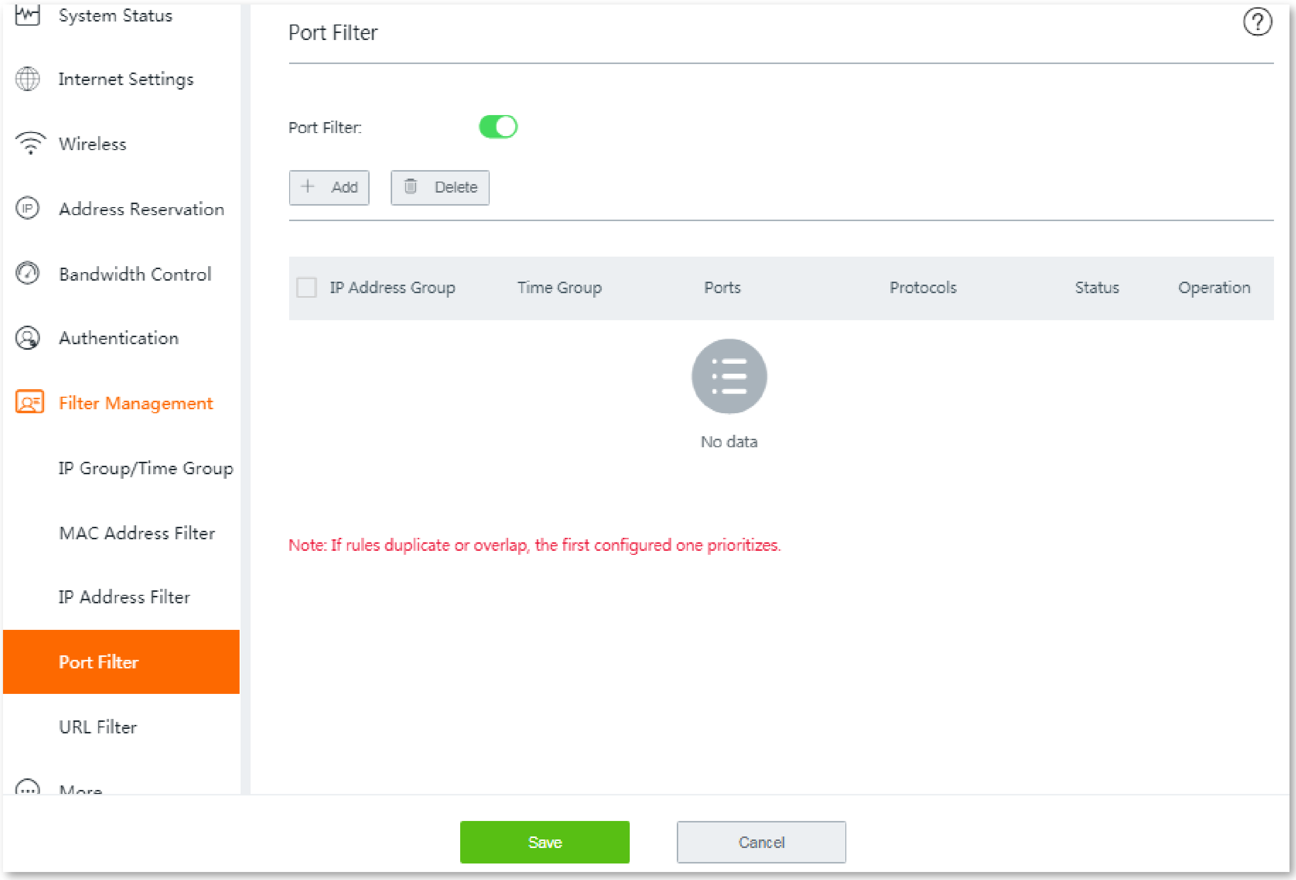
During 08:00 to 18:00 on weekdays, only the purchaser’s computer can access the internet.

10.5 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.

To access the page for setting the port filter, choose **Filter Management** > **Port Filter**. By default, this function is disabled. Once it is enabled, the following page appears.



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

10.5.1 Configuring port filtering rules

Before you start

- Set up at least one time group rule.
- Set up at least one IP group rule.

Configuration procedure

Step 1 Choose **Filter Management** > **Port Filter**.

Step 2 Enable this function, and click **Save**.

Step 3 Click **+Add**. The **Add** window appears.

Step 4 Set the required parameters.

- **To add a single port number:**

  Repeat the port number in the second box.

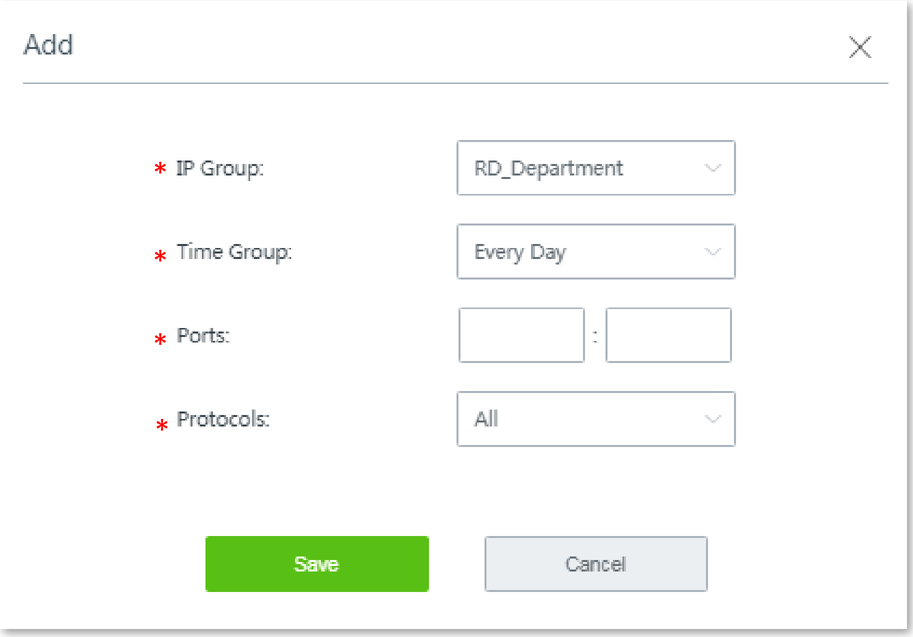
For example, to add the port number 80, enter 80 in the first box. Then repeat it in the second box.

- **To add consecutive port numbers**:

  Enter the start port number in the first box, and the end port number in the second box. The start port number cannot be greater than the end port number.

- **To add inconsecutive port numbers**:

  The router does not support to add inconsecutive port numbers with one rule. Therefore, to add inconsecutive port numbers, add multiple port number rules that meet your requirement.



Add

* IP Group: RD_Department

* Time Group: Every Day

* Ports: ____ : ____

* Protocols: All

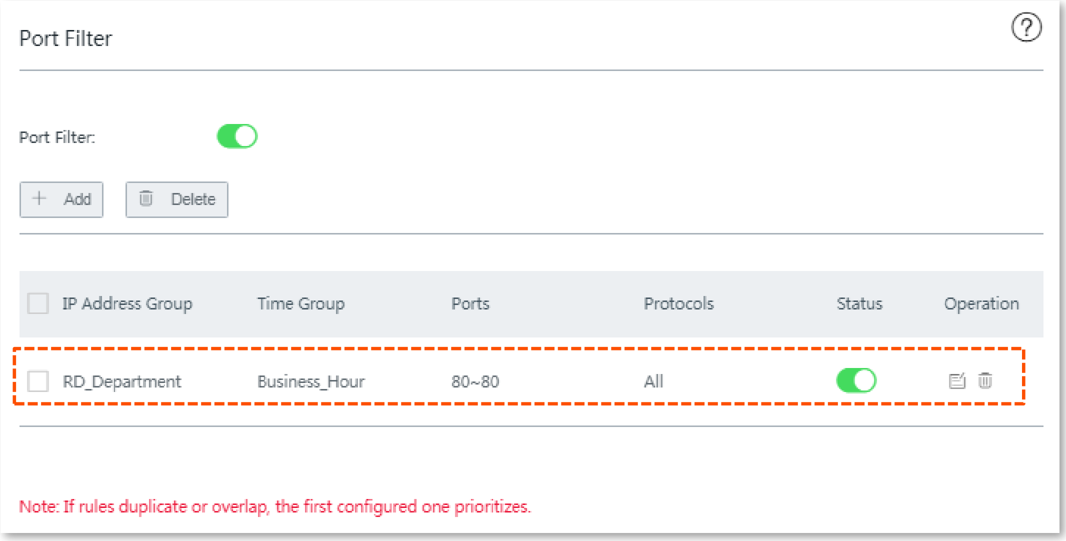
TIP

Parameters indicated with * are mandatory.

Step 5 Click **Save**.

---- End

Added successfully. See the following figure:



Port Filter

Port Filter: ●

□	IP Address Group	Time Group	Ports	Protocols	Status	Operation
□	RD_Department	Business_Hour	80~80	All	●	

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

10.5.2 Example of configuring port filter rules

Networking requirement

An enterprise uses W15E to set up a LAN to address the following requirement:

During business hours (08:00 to 18:00 on 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.

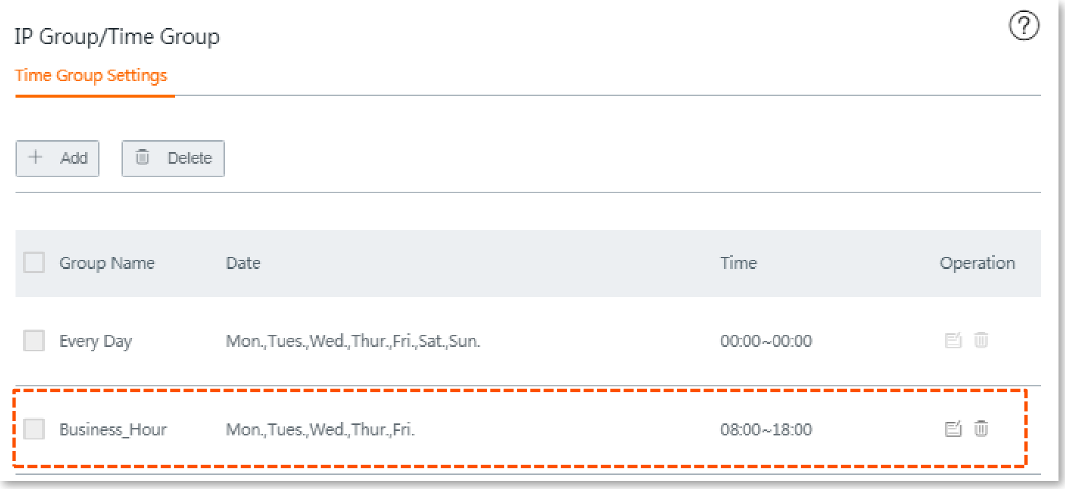
Solutions

The port filter function of the router can meet this requirement.

Configuration procedure

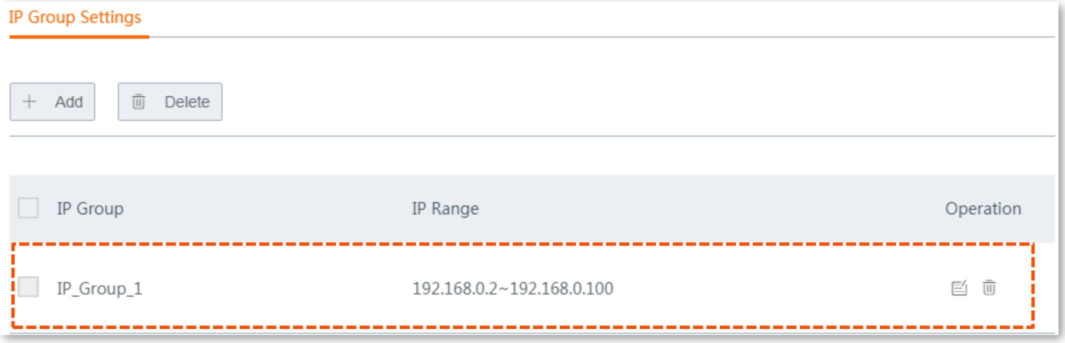
Step 1 Set up a time group.

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



□	Group Name	Date	Time	Operation
□	Every Day	Mon.,Tues.,Wed.,Thur.,Fri.,Sat.,Sun.	00:00~00:00	
□	Business_Hour	Mon.,Tues.,Wed.,Thur.,Fri.	08:00~18:00	

Step 2 Create an IP group for clients that are disallowed to use web service, which is **192.168.0.2** to **192.168.0.100** in this example.

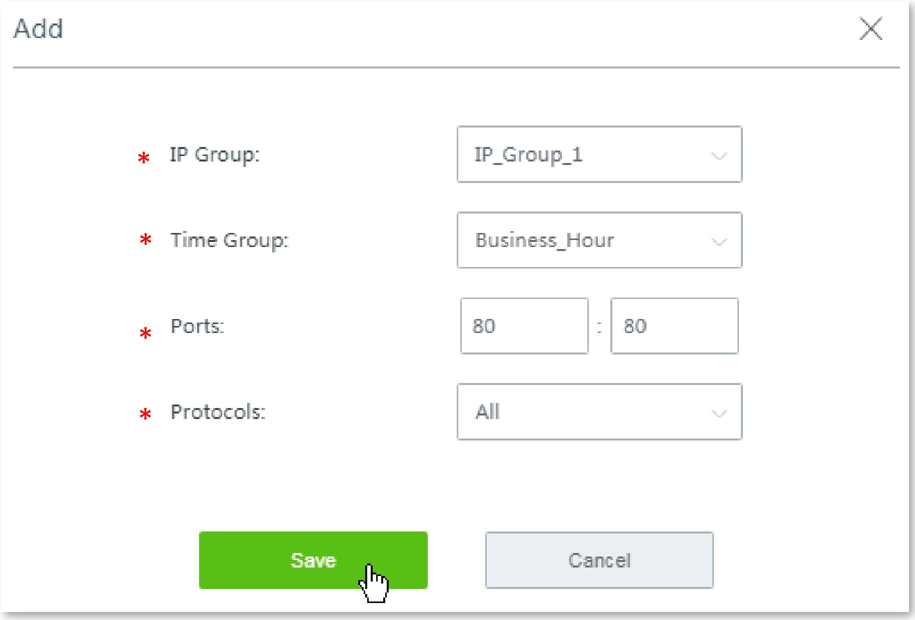


□	IP Group	IP Range	Operation
□	IP_Group_1	192.168.0.2~192.168.0.100	

Step 3 Set port filter rules.

1. Choose **Filter Management** > **Port Filter**.
2. Enable this function, and click **Save** at the bottom of the page.
3. Click **+Add**. The **Add** window appears.

4. Set the required parameters. Configurations on the following figure are only used for examples:



* IP Group: IP_Group_1

* Time Group: Business_Hour

* Ports: 80 : 80

* Protocols: All

TIP

- Parameters indicated with * are mandatory.
- To add consecutive port numbers, enter the start port number in the first box, and the end port number in the second box. The start port number cannot be greater than the end port number.
- The router does not support to add inconsecutive port numbers with one rule. Therefore, to add inconsecutive port numbers, add multiple port number rules that include your requirement.

5. Click **Save**.

---- End

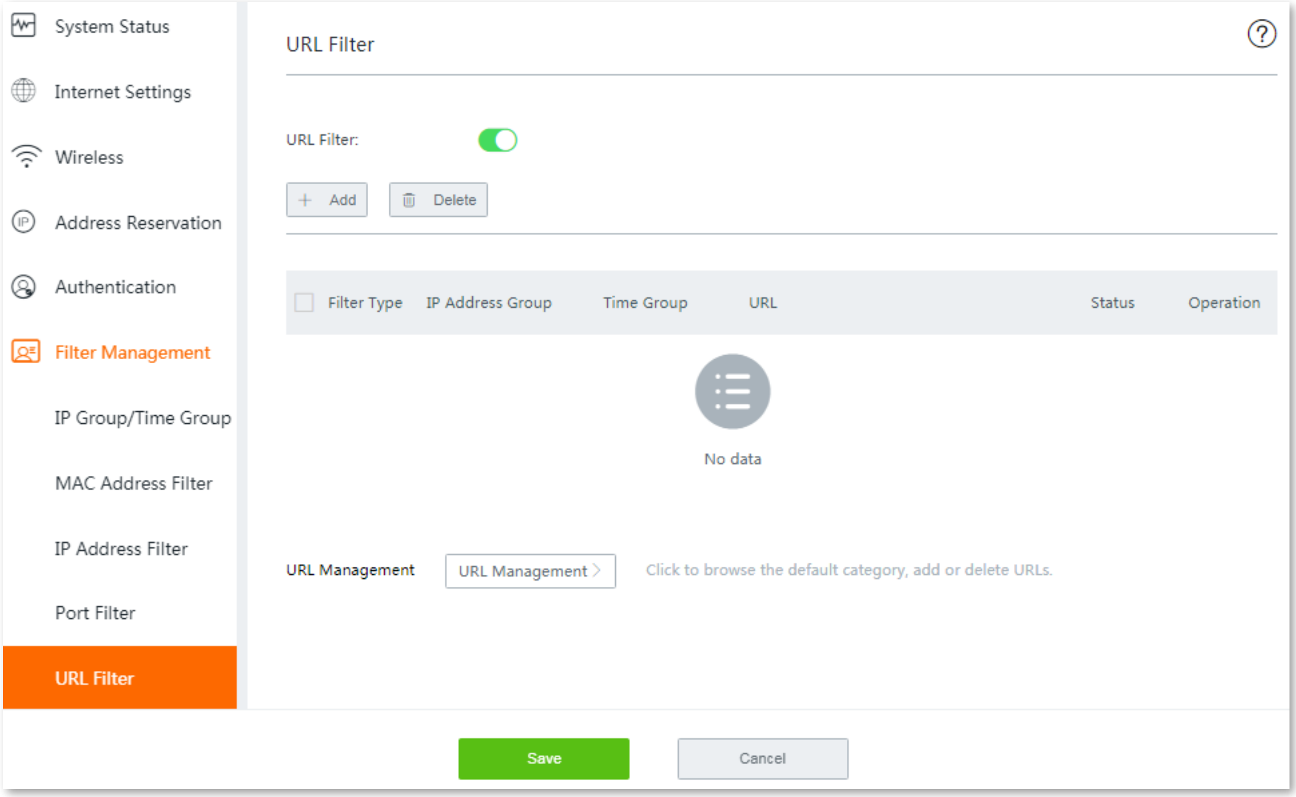
Verification

During 08:00 to 18:00 on weekdays, verify that the computers with IP addresses ranging from 192.168.0.2 to 192.168.0.100 cannot browse web pages.

10.6 URL filter

An URL 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.

To access the following page, choose **Filter Management** > **URL Filter**. By default, this function is disabled. Once it is enabled, the following page appears.



URL Filter

URL Filter: ●

□	Filter Type	IP Address Group	Time Group	URL	Status	Operation

No data

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

10.6.1 Configuring URL filter

Before you start

- Set up at least one time group rule.
- Set up at least one IP group rule.

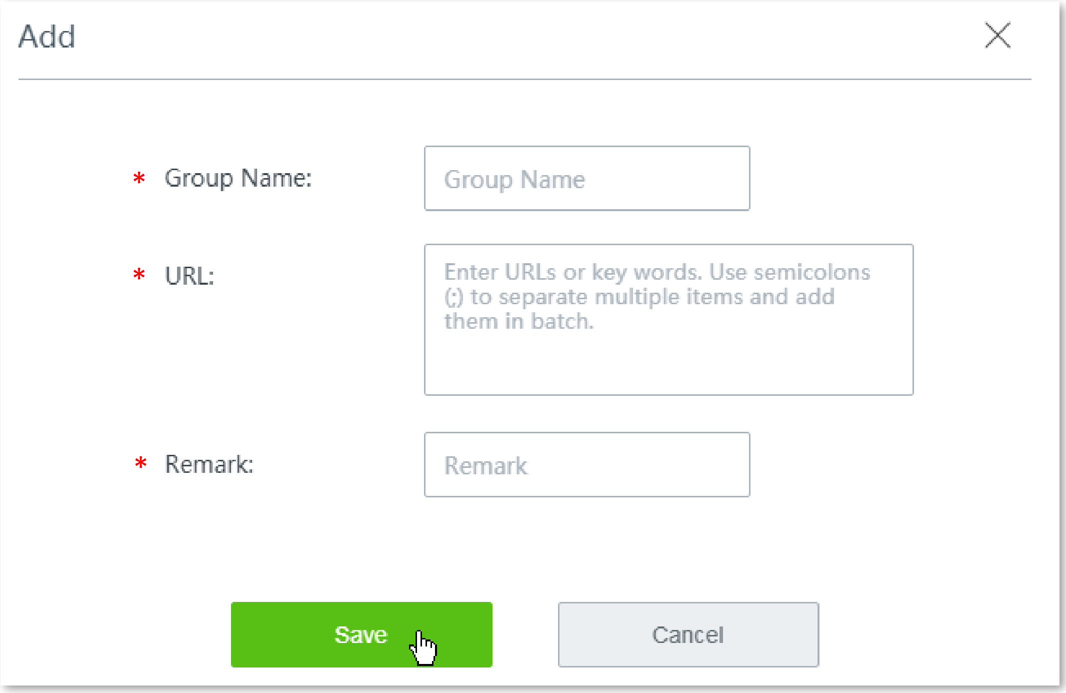
Configuration procedure

Step 1 Enable **URL Filter**.

1. Choose **Filter Management** > **URL Filter**.
2. Enable this function, and click **Save**.

Step 2 Customize URL library.

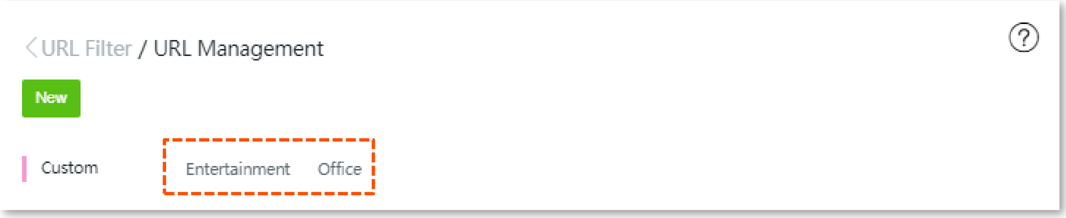
1. Click the **URL Management** button. The **URL Management** configuration page appears.
2. Click **New**. The **Add** window appears.


Add
* Group Name:
Group Name
* URL:
Enter URLs or key words. Use semicolons (;) to separate multiple items and add them in batch.
* Remark:
Remark
Save
Cancel

TIP

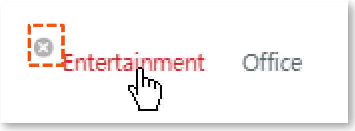
Parameters indicated with * are mandatory.

3. Set the required parameters by following the on-screen instructions, and click **Save**. The added URL groups are shown as follows:



TIP

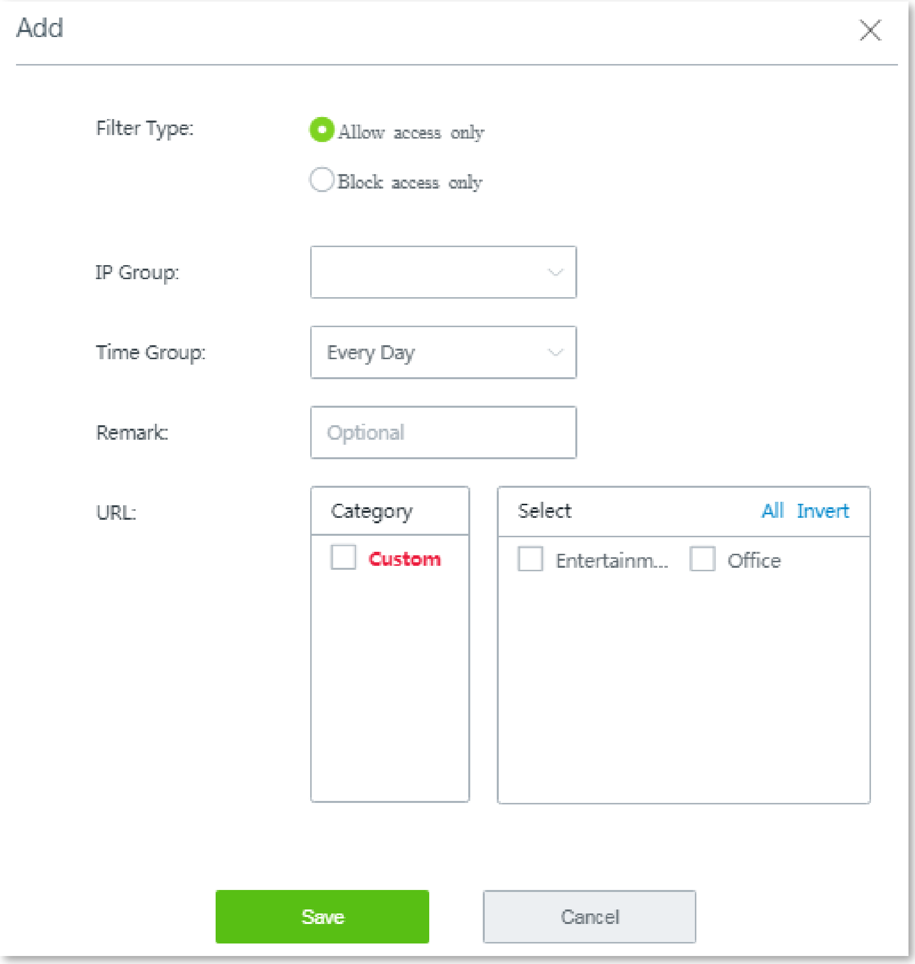
- To delete an URL group, move the mouse pointer to it, and click the ⊗ on the upper left corner.



- A rule in use cannot be deleted.

Step 3 Configure an URL filter rule.

1. Click **+Add**. The **Add** window appears.


Add

Filter Type: ● Allow access only ○ Block access only

IP Group:

Time Group: Every Day

Remark: Optional

URL:

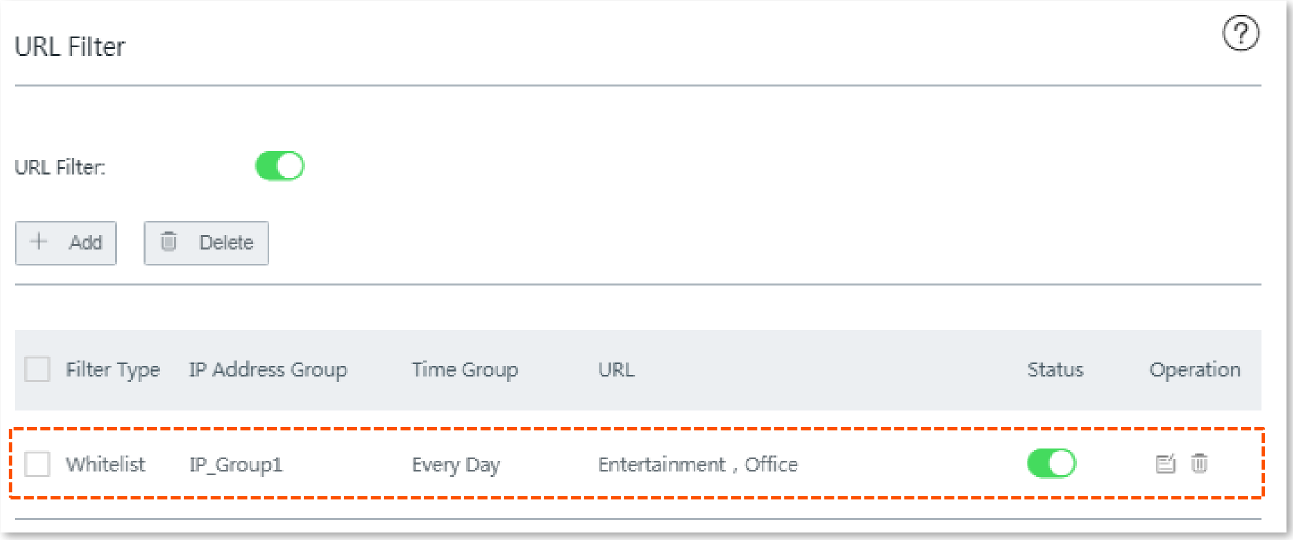
Category: □ Custom

Select: □ Entertainm... □ Office

2. Set the required parameters, and click **Save**.

---- End

Added successfully. See the following figure:


URL Filter

URL Filter: ●

□	Filter Type	IP Address Group	Time Group	URL	Status	Operation
□	Whitelist	IP_Group1	Every Day	Entertainment , Office	●	

10.6.2 Example of configuring URL filter

Networking requirement

An enterprise uses W15E to set up a LAN to address the following requirement:

During business hours (08:00 to 18:00 on weekday), staffs are not allowed to access social medias including Facebook, YouTube, and Tumblr.

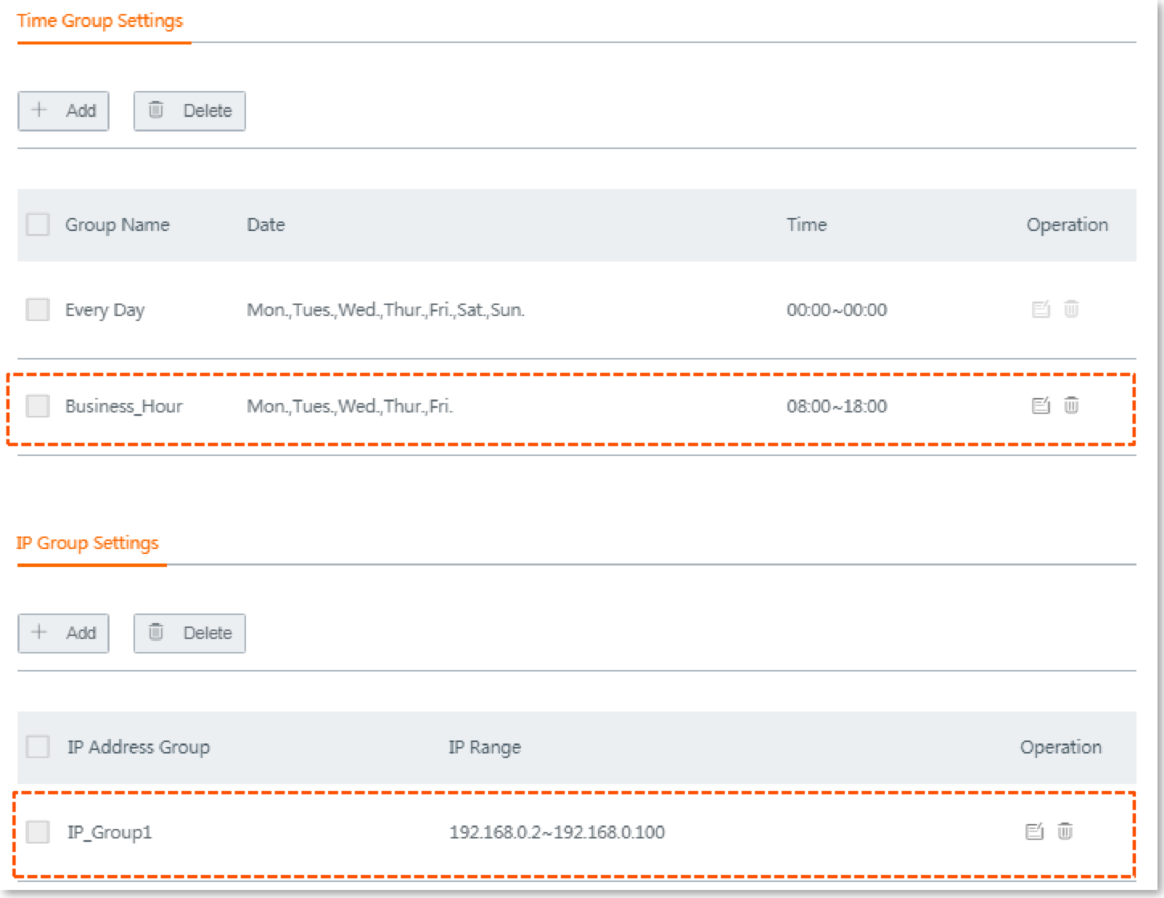
Solutions

The URL filter can meet this requirement.

Configuration procedure

Step 1 Set up time groups and IP groups.

1. Choose **Filter Management** > **IP Group/Time Group**.
2. Set up a time group from **08:00** to **18:00** on weekday, and an IP groups ranging from **192.168.0.2** to **192.168.0.100**. See the following figure:



□	Group Name	Date	Time	Operation
□	Every Day	Mon.,Tues.,Wed.,Thur.,Fri.,Sat.,Sun.	00:00~00:00	
□	Business_Hour	Mon.,Tues.,Wed.,Thur.,Fri.	08:00~18:00	

□	IP Address Group	IP Range	Operation
□	IP_Group1	192.168.0.2~192.168.0.100	

TIP

For detailed configuration steps, refer to Configuring IP group and time group.

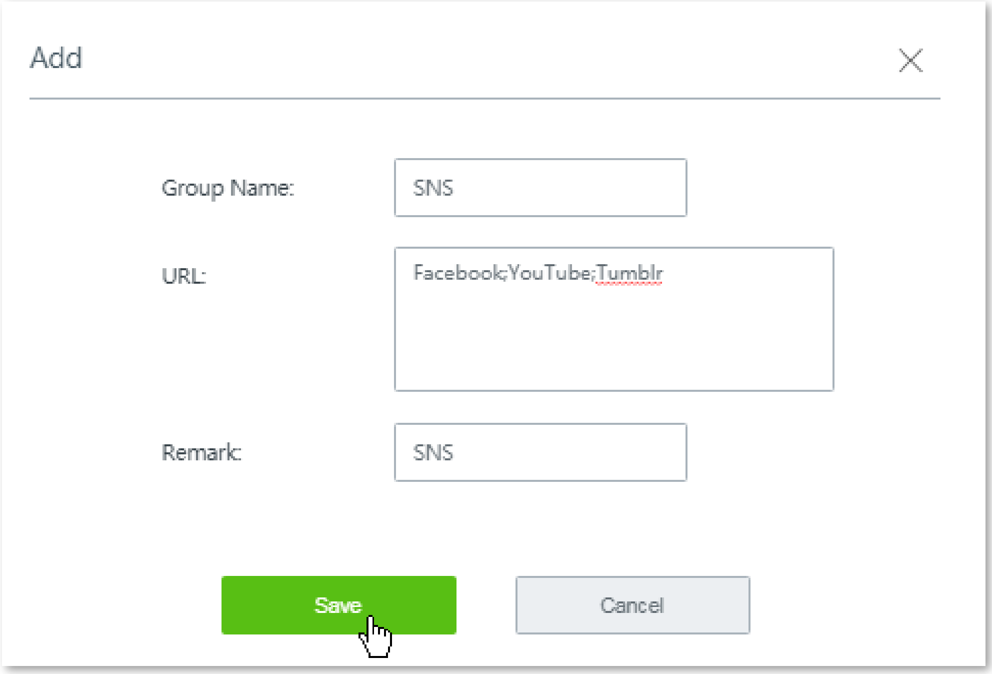
Step 2 Enable **URL Filter**.

1. Choose **Filter Management** > **URL Filter**.
2. Enable this function, and click **Save**.

Step 3 Customize URL library.

1. Click the **URL Management** button. The **URL Management** configuration page appears.
2. Click **New**. The **Add** window appears.

3. Set the required parameters. See the following figure.



Add

Group Name: SNS

URL: Facebook;YouTube;Tumblr

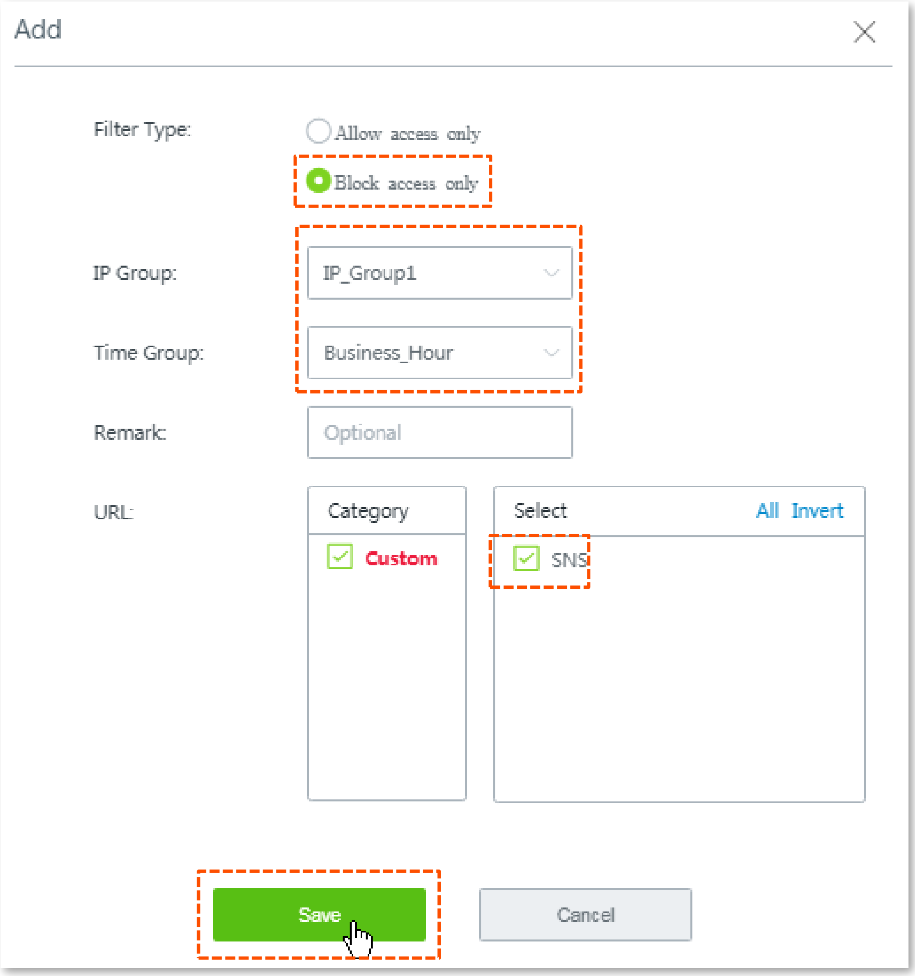
Remark: SNS

4. Click **Save**.

Step 4 Configure the URL filter rule.

1. Back to the URL filter configuration page, click **+Add**. The **Add** window appears.

2. Set the required parameters, and click **Save**.


Add

Filter Type: ○ Allow access only ● Block access only

IP Group: IP_Group1

Time Group: Business_Hour

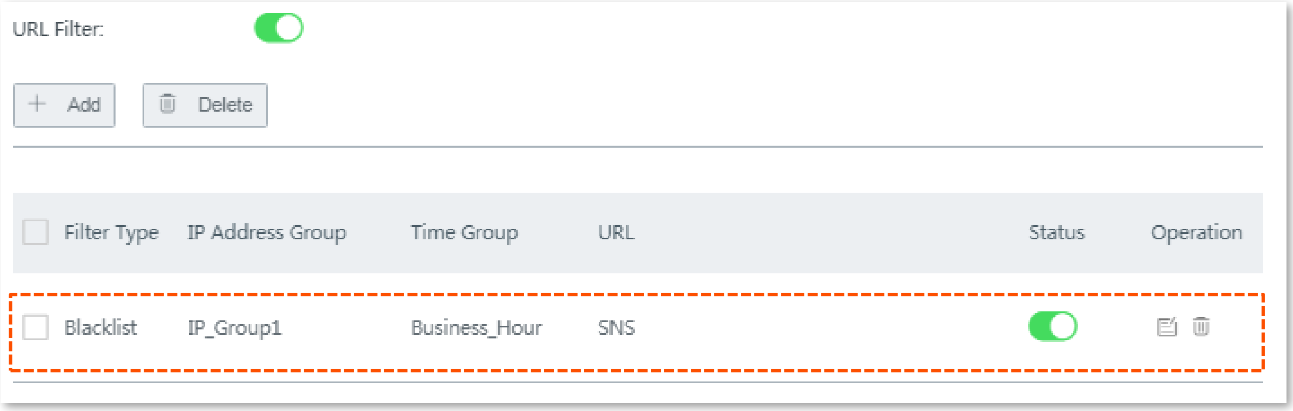
Remark: Optional

URL:

Category	Select All Invert
☑ Custom	☑ SNS

---- End

Added successfully. See the following figure:


URL Filter: ●

□	Filter Type	IP Address Group	Time Group	URL	Status	Operation
□	Blacklist	IP_Group1	Business_Hour	SNS	●	

Verification

During 08:00 to 18:00 on weekdays, clients with the IP address ranging from 192.168.0.2 to 192.168.0.100 cannot access Facebook, YouTube, and Tumblr.

11 More settings

This chapter describes how to modify LAN settings and WAN parameters, how to configure static router, port mirroring, DDNS, port forwarding, UPnP, DMZ host, and how to establish VPN connections.

11.1 LAN settings

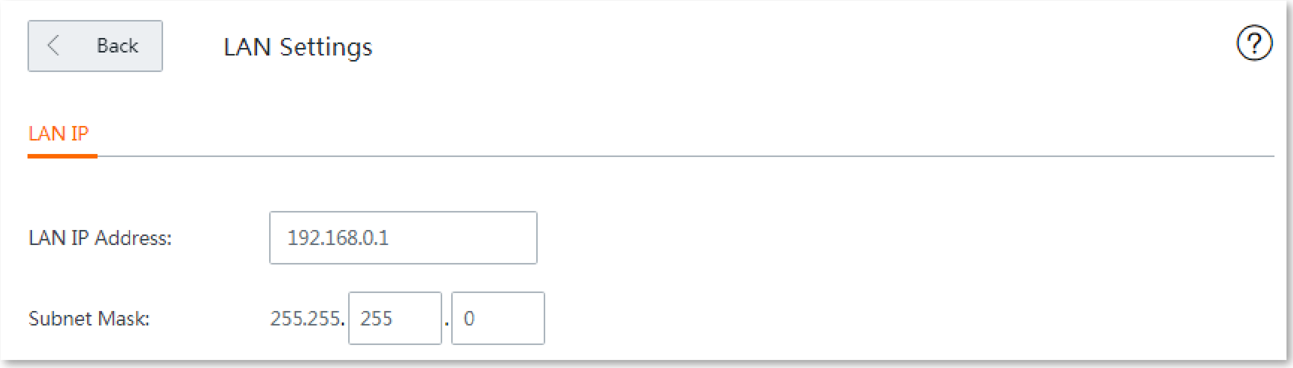
You can view and modify the LAN IP address of the router, and configure DHCP server here.

To enter the configuration page, choose **More** > **LAN Settings**.

11.1.1 Modifying LAN IP address of the router

The LAN IP address is also the login IP address of the router. The default LAN IP address is **192.168.0.1**.

Generally, you do not need to modify the LAN IP address of the router, unless an IP conflict happens on the router. An IP conflict happens when the WAN IP address and LAN IP address of the router are in the same network segment, or IP address of another device in the LAN is **192.168.0.1** too.



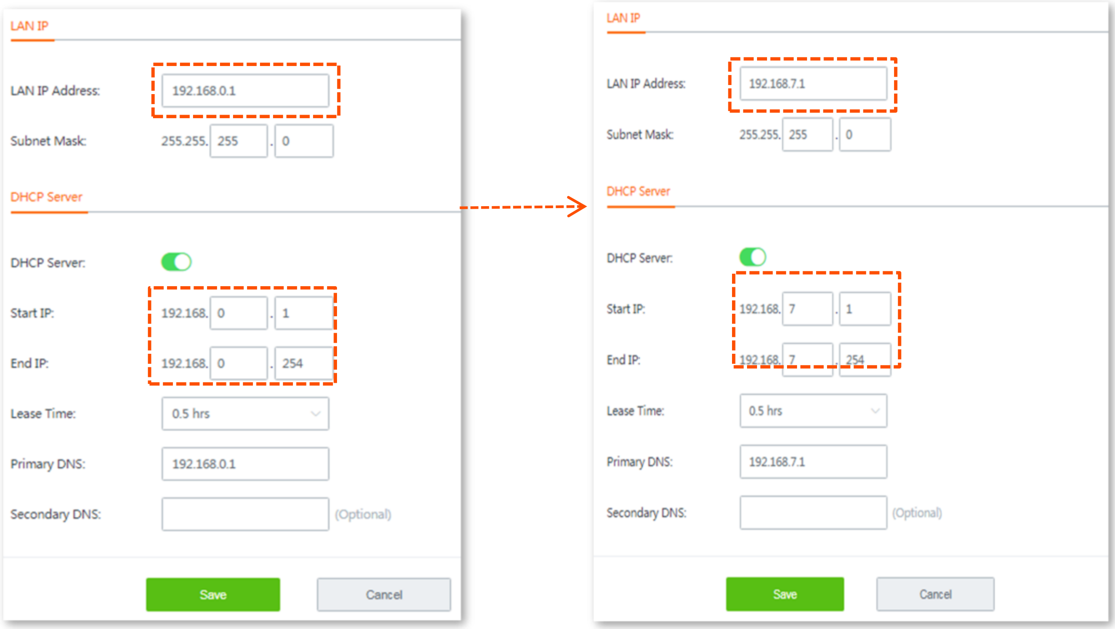
LAN IP Address: 192.168.0.1

Subnet Mask: 255.255. 255 . 0

Configuration procedure:

Step 1 Modify the LAN IP address, which is **192.168.7.1** in this example.

Since the network segment of the new LAN IP address is different from the original one, the router modifies the network segment of the DHCP server automatically. See the following figure:


LAN IP

LAN IP Address: 192.168.0.1

Subnet Mask: 255.255. 255 . 0

DHCP Server

DHCP Server:

Start IP: 192.168. 0 . 1

End IP: 192.168. 0 . 254

Lease Time: 0.5 hrs

Primary DNS: 192.168.0.1

Secondary DNS: (Optional)

LAN IP

LAN IP Address: 192.168.7.1

Subnet Mask: 255.255. 255 . 0

DHCP Server

DHCP Server:

Start IP: 192.168. 7 . 1

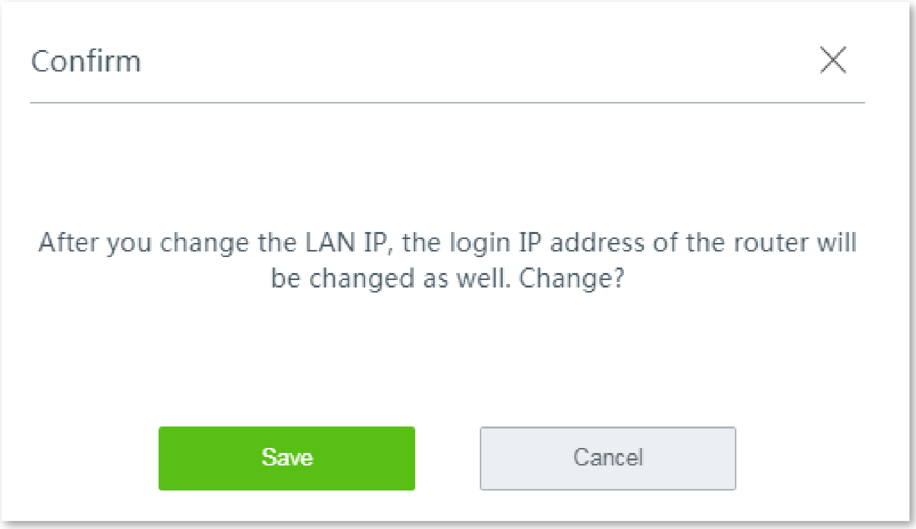
End IP: 192.168. 7 . 254

Lease Time: 0.5 hrs

Primary DNS: 192.168.7.1

Secondary DNS: (Optional)

Step 2 Click **Save**, the following message appears.


Confirm

After you change the LAN IP, the login IP address of the router will be changed as well. Change?

Step 3 Click **Save**.

---- End

Wait until the progress bar completes. You will be redirected to the login page.

Use the new LAN IP address to log in to the web UI of router later.

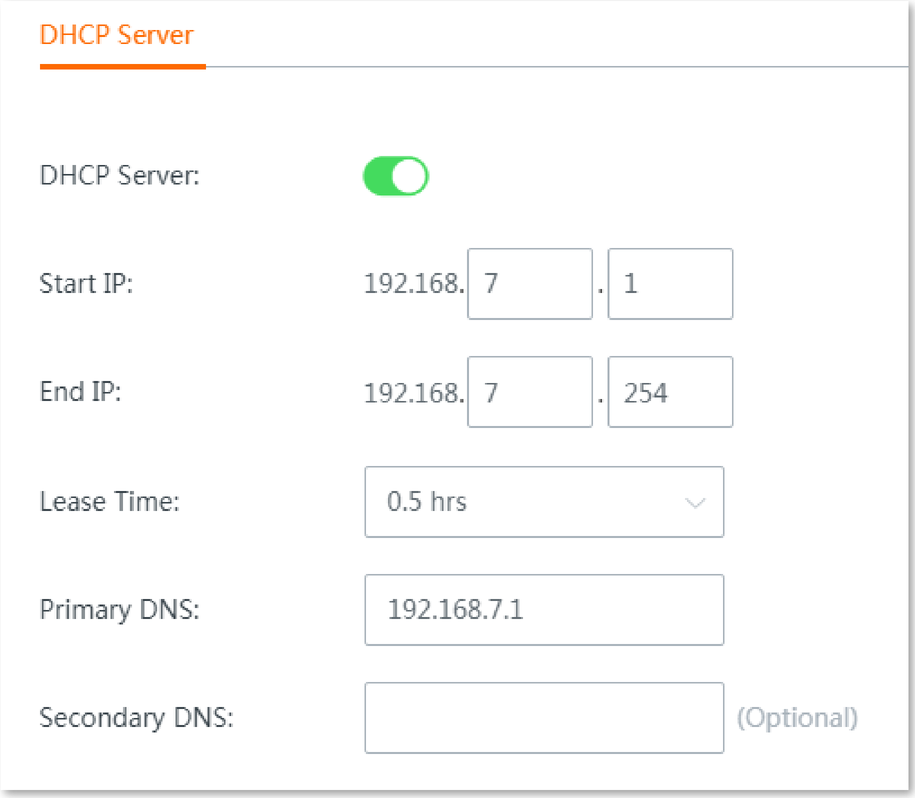
11.1.2 Modifyting DHCP server

DHCP server can automatically assign IP addresses, subnet mask, gateway and other internet parameters to devices connected to the router. If this function is disabled, you have to manually set IP address settings for your connected devices for internet access. Therefore, you are recommended to keep the DHCP server enabled.

To modify DHCP server information, modify the parameters as required and click **Save** to apply your settings.

TIP

With this function enabled, IP address-based functions, such as port forwarding and IP address filter may be affected.



DHCP Server

DHCP Server: ●

Start IP: 192.168. 7 . 1

End IP: 192.168. 7 . 254

Lease Time: 0.5 hrs

Primary DNS: 192.168.7.1

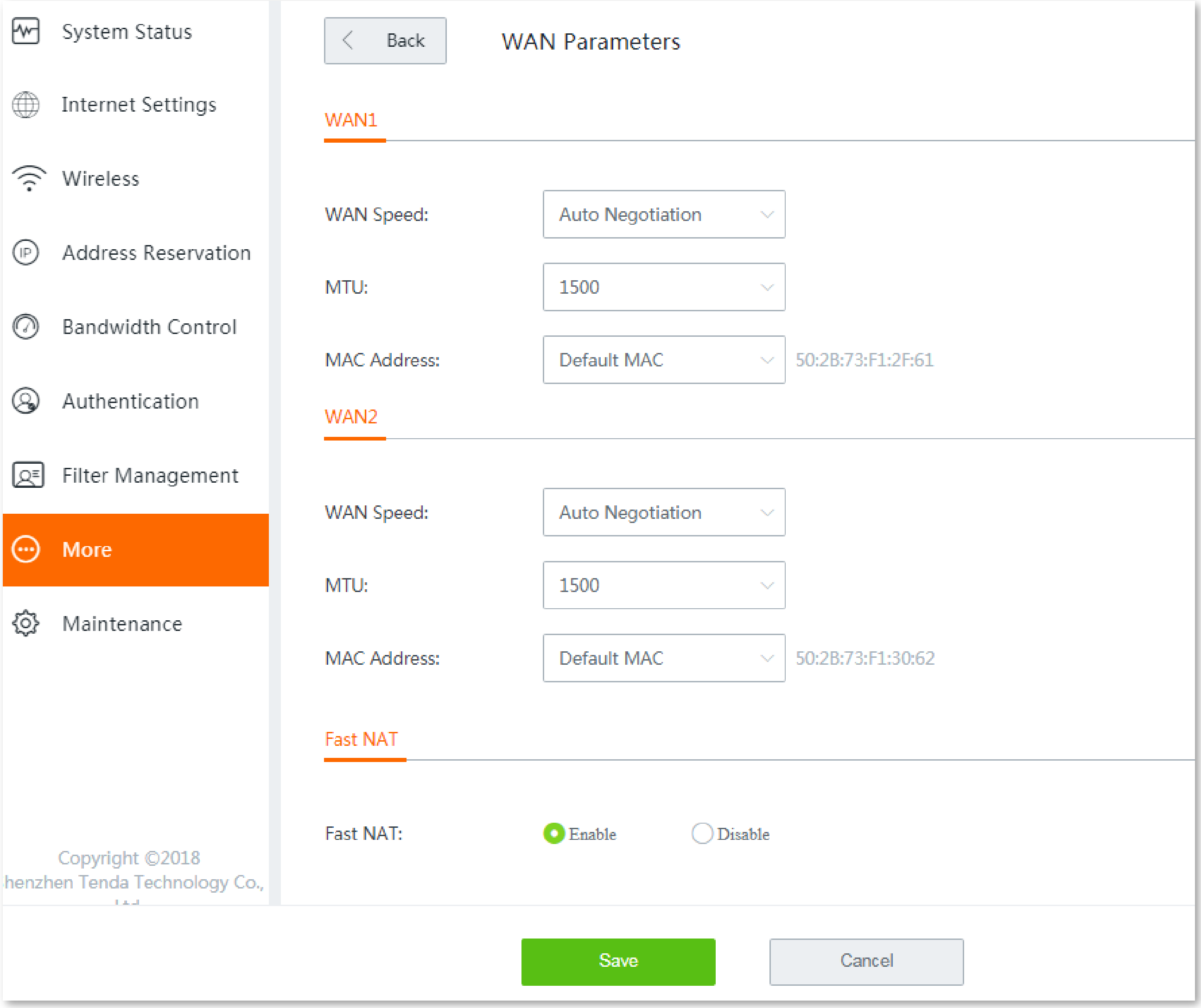
Secondary DNS: (Optional)

11.2 WAN parameters

11.2.1 Overview

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

To access the configuration page, choose **More** > **WAN Parameters**.



WAN Parameters

WAN1

WAN Speed: Auto Negotiation

MTU: 1500

MAC Address: Default MAC 50:2B:73:F1:2F:61

WAN2

WAN Speed: Auto Negotiation

MTU: 1500

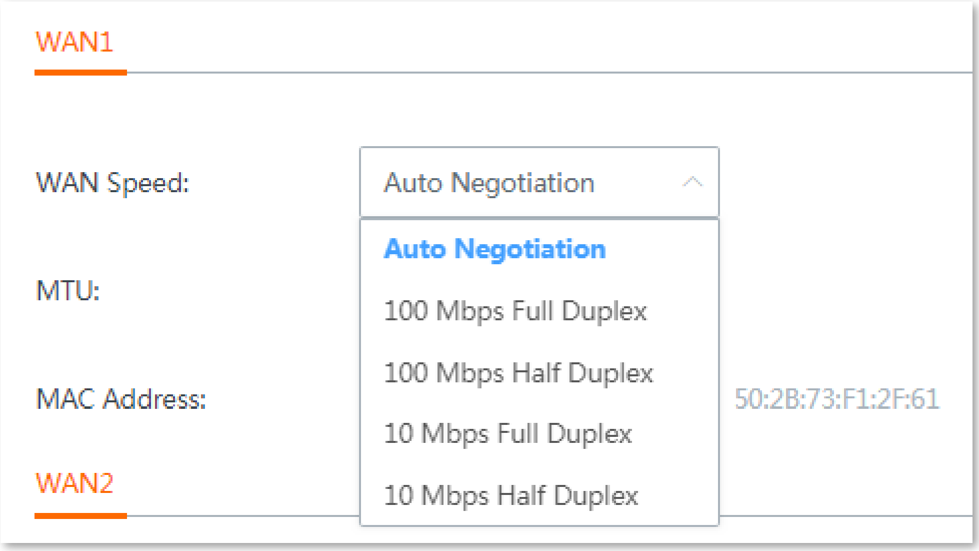
MAC Address: Default MAC 50:2B:73:F1:30:62

Fast NAT

Fast NAT: ● Enable ○ Disable

11.2.2 WAN speed

The speed of an Ethernet physical port is determined through negotiation with its peer device. The negotiated speed can be any speed within the interface capability. You can try to modify the speed and duplex mode when network connection issues occur.


WAN1

WAN Speed: Auto Negotiation

MTU:

MAC Address: 50:2B:73:F1:2F:61

WAN2

Duplex modes supported by the router and their scenarios:

Speed and Duplex	Applicable scenario
Auto Negotiation (default)	The duplex mode of the port is determined through auto negotiation between the router and its peer device. You are recommended to keep the default settings since auto negotiation is the default option for most of Ethernet network devices. If the router uses auto negotiation, while its peer uses non-auto negotiation, the negotiated duplex mode is half duplex.
10/100 Mbps Full Duplex	The interface can receive and send packets simultaneously, leading to low latency and high efficiency. **10/100Mbps** indicates the maximum link speed that both ends can negotiate. W18E also supports **1000 Mbps Full Duplex**. NOTE You are recommended to use the same speed link and duplex modes for both ends. Otherwise, network connection issues may occur.
10/100 Mbps Half Duplex	The interface can either receive or send packets at a time. **10/100Mbps** indicates the maximum link speed that both ends can negotiate. W18E also **supports 1000 Mbps Half Duplex**. NOTE You are recommended to use the same speed link and duplex modes for both ends. Otherwise, network connection issues may occur.

11.2.3 MTU

MTU is abbreviated for Maximum Transmission Unit. It specifies the maximum size of a packet that can be transmitted by a network device. Either larger or smaller MTU value affects the network performance. Do not modify the default settings unless the following situations happen:

- Some websites are inaccessible, or secure websites cannot be displayed properly, such as online banking websites, or PayPal.
- Email service suspends, or servers, such as FTP/POP servers, are inaccessible.

Commonly-used MTU value in different scenarios:

MTU (Bytes)	Scenario
1500	It is the most common value for non-PPPoE connections and non-VPN connections.
1492	It is used for PPPoE connections.
1480	It is the maximum value for the pinging function. (If a greater value is used, packets are split.)
1450	It is used for DHCP, which assigns dynamic IP addresses to connected devices.
1400	It is used for VPNs or PPTP.

11.2.1 Cloning MAC address

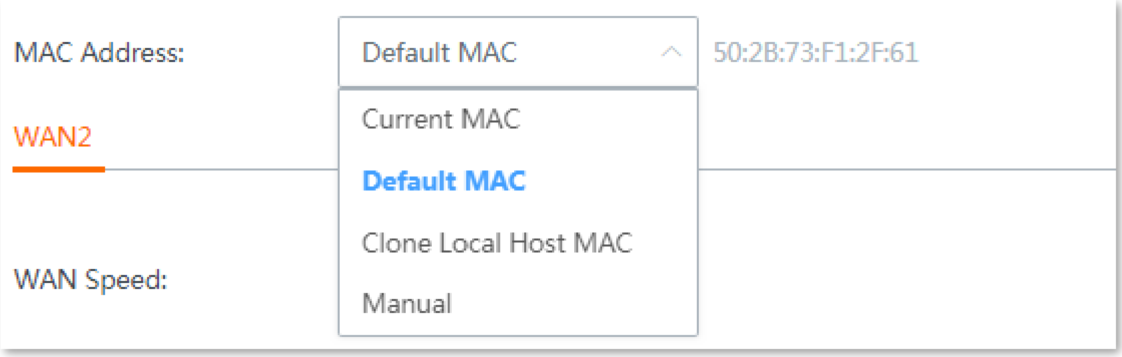
Overview

Some ISPs allow only a single or a certain number of computers to use the broadband service you subscribed, and register the MAC address of your computer when you first use their cable modem for internet access. Therefore, you may find yourself in the following situations after setting up the router:

- Only one computer can access the internet normally.
- No internet connection at all.

The reason why such a problem happens is that your ISP does not accept MAC addresses other than the registered one. To resolve this, you need to clone the MAC address of the registered computer to the router to pretend that the router has the same MAC address as the registered one.

The cloning MAC address function is designed for this purpose. Click **More > WAN Parameters** to enter the configuration page.



MAC Address: Default MAC 50:2B:73:F1:2F:61

Parameter description

Parameter	Description
Current MAC	It specifies the MAC address the router currently used.
Default MAC	It specifies the MAC address of the router itself. TIP - You can view the MAC address of the router on LAN port status page, or the Label on

Parameter	Description
	the bottom of your router. - If you clone the local host MAC, the MAC address of the router is changed to the MAC address you cloned.
Clone Local Host MAC	It specifies the MAC address of the computer that can access the internet normally. TIP To use this option, you need to keep the computer with internet connectivity connected to the router and disconnect all the other computers. Otherwise, find the correct MAC address, and enter it manually. You can consult your ISP as well.
Manual	It allows you to manually specify a MAC address.

Cloning MAC address

Step 1 Click **More** > **WAN Parameters**, and locate the corresponding WAN port.

Step 2 Select one option, or manually specify the MAC address according to your actual situation.

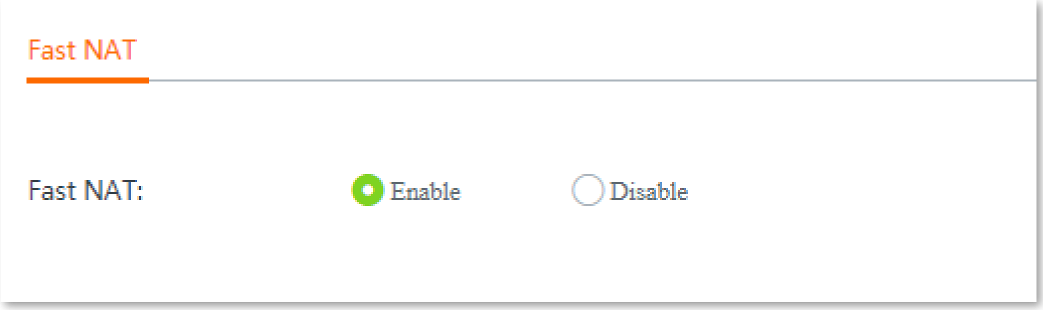
Step 3 Click **Save** to apply your settings.

---- End

11.2.2 Fast NAT

NAT (Network Address Translation) translates private addresses in intranet to global (public) addresses to achieve communication between the intranet and the internet. While fast NAT enables the router forward the traffic from the specific LAN to the chosen WAN directly. This function reduces the CPU loading and speed up the performance of the NAT sessions.

You are recommended to keep fast NAT enabled.



Fast NAT

Fast NAT: ● Enable ○ Disable

11.3 Configuring static route

11.3.1 Overview

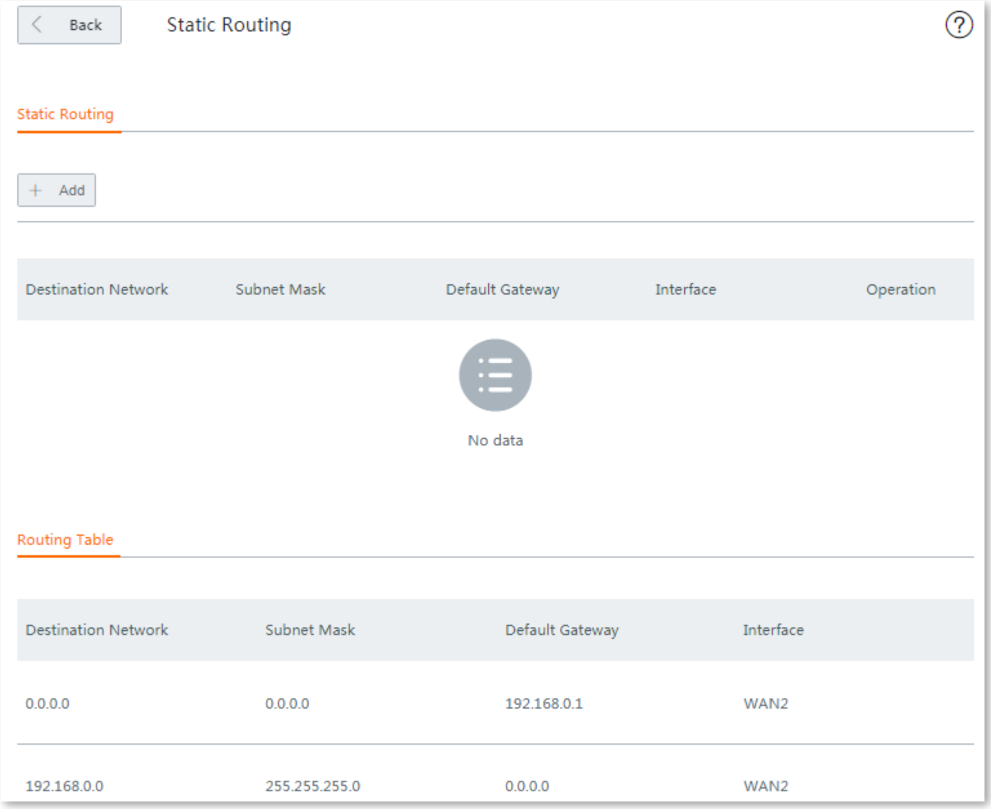
Routing is an operation to select the optimal route for delivering data from a source to a destination. A static route is a special route configured manually, which is simple, efficient, and reliable. Proper static routes help reduce route selection issues and prevent overload caused by route selection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

TIP

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.

To enter the configuration page, choose **More** > **Static Routing**.



Destination Network	Subnet Mask	Default Gateway	Interface	Operation

No data

Routing Table

Destination Network	Subnet Mask	Default Gateway	Interface
0.0.0.0	0.0.0.0	192.168.0.1	WAN2
192.168.0.0	255.255.255.0	0.0.0.0	WAN2

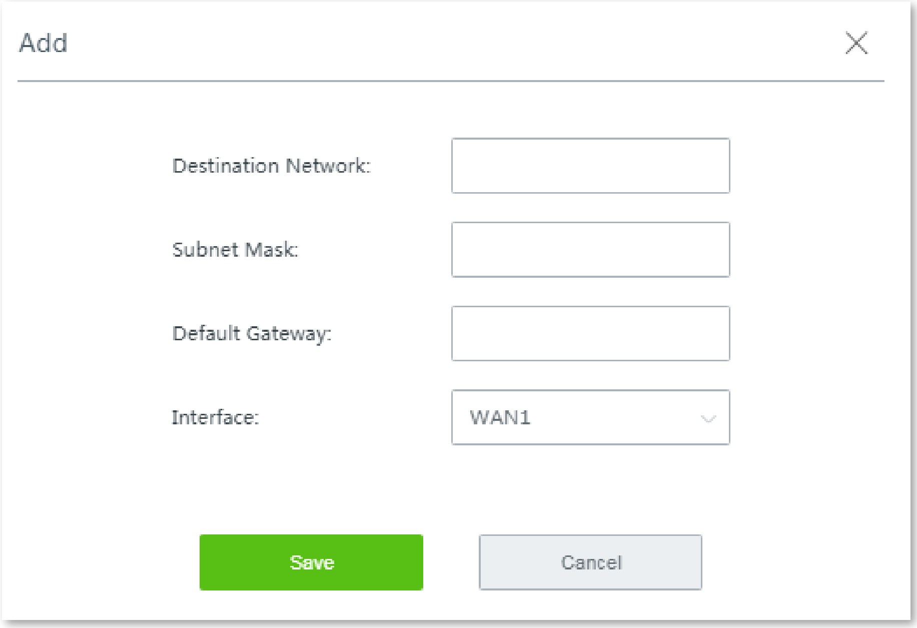
Parameter description

Parameter	Description
Destination Network	Destination network of packets.
Subnet Mask	Subnet mask of the destination network.
Default Gateway	IP address of the next hop to the final destination of packets.

Parameter	Description
Interface	Port through which packets are forwarded.

11.3.2 Configuring a static routing rule

Step 1 Choose **More** > **Static Routing** and click **+Add**. The **Add** configuration window appears.



Add

Destination Network:

Subnet Mask:

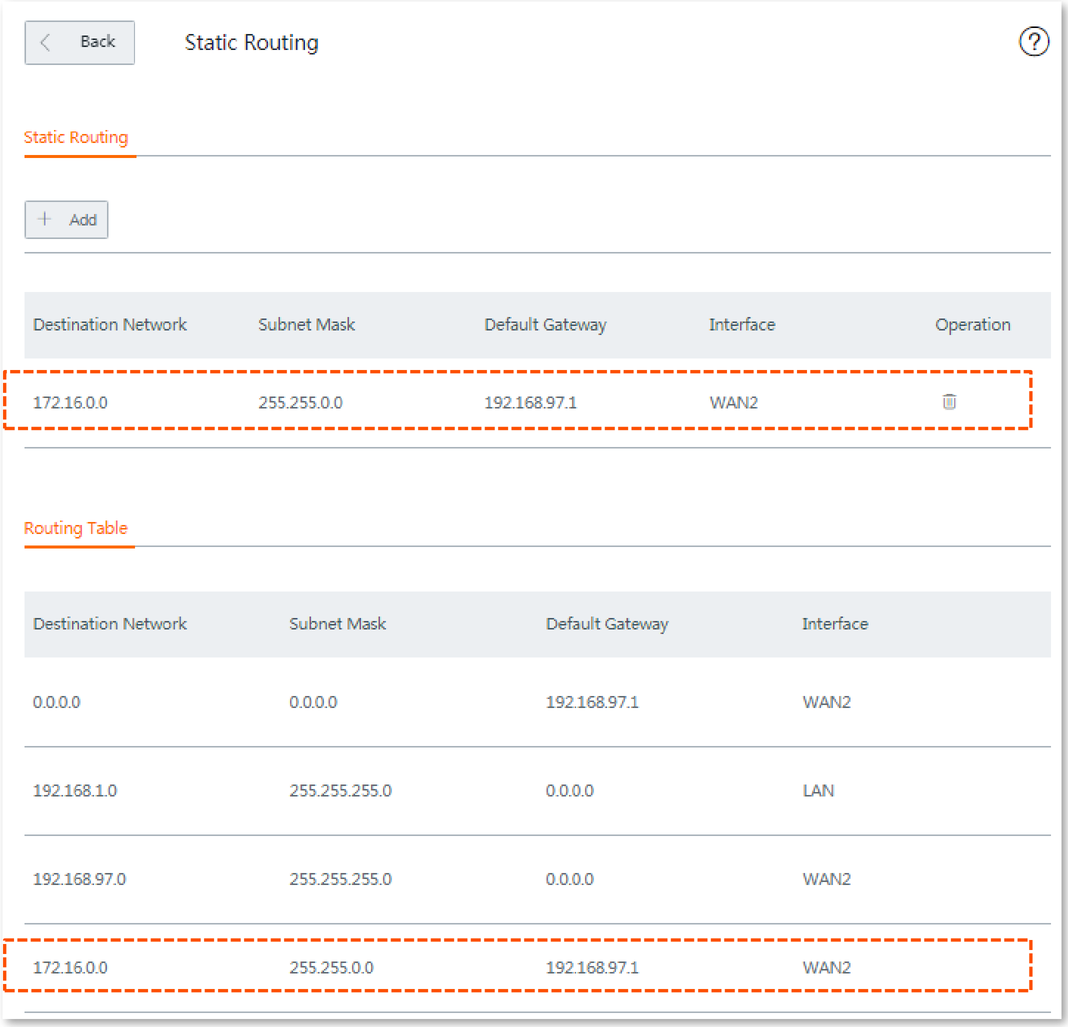
Default Gateway:

Interface: WAN1

Step 2 Set the parameters and click **Save**.

Step 3 Choose **More** > **Static Routing** and view the added static route.

The available static routes are displayed on the static routing page. See the following figure.



Destination Network	Subnet Mask	Default Gateway	Interface	Operation
172.16.0.0	255.255.0.0	192.168.97.1	WAN2	🗑

Destination Network	Subnet Mask	Default Gateway	Interface
0.0.0.0	0.0.0.0	192.168.97.1	WAN2
192.168.1.0	255.255.255.0	0.0.0.0	LAN
192.168.97.0	255.255.255.0	0.0.0.0	WAN2
172.16.0.0	255.255.0.0	192.168.97.1	WAN2

---- End

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.

TIP

If a static route conflicts with a user-defined multi-WAN policy, the static route prioritizes

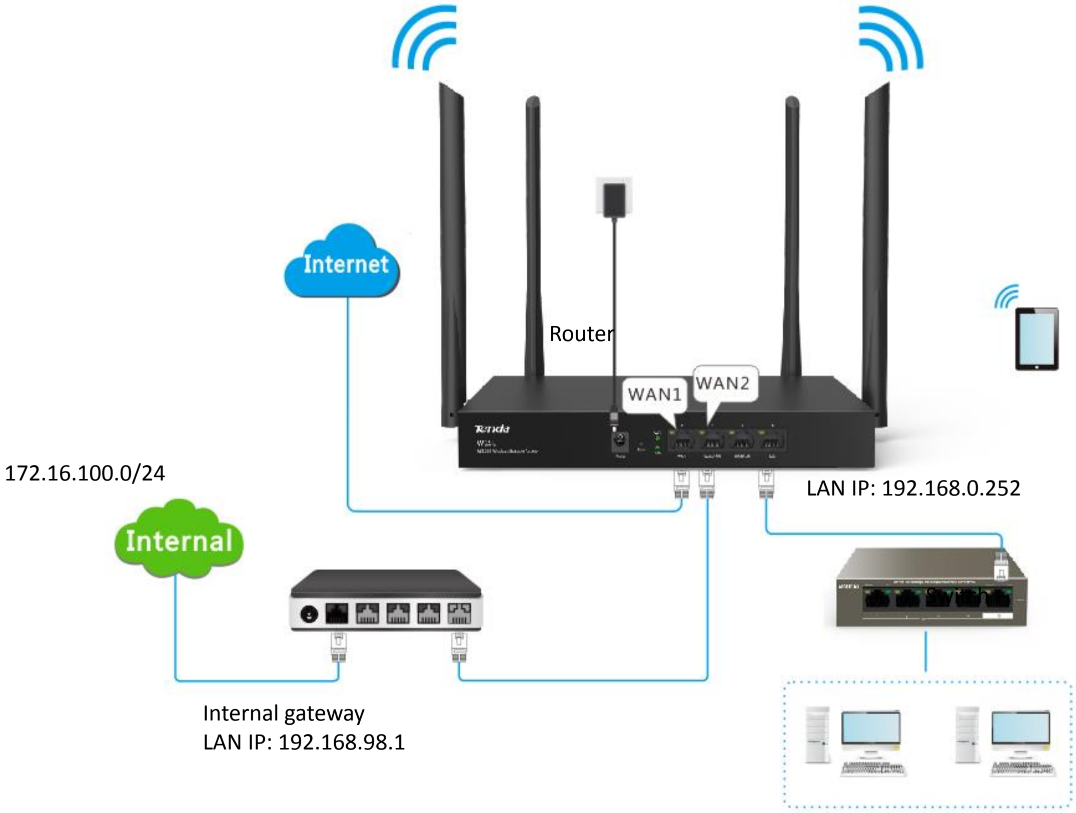
11.3.3 Example of configuring static route

Network requirement

An enterprise uses W15E for network construction. The internet is inaccessible to the enterprise LAN. The WAN1 port of W15E accesses the internet using a PPPoE connection and the WAN2 port of W15E accesses the enterprise LAN using a dynamic IP address. Users on the W15E LAN are allowed to access both the internet and enterprise LAN. Assume that the PPPoE user name and password are **tenda/tenda**.

Solutions

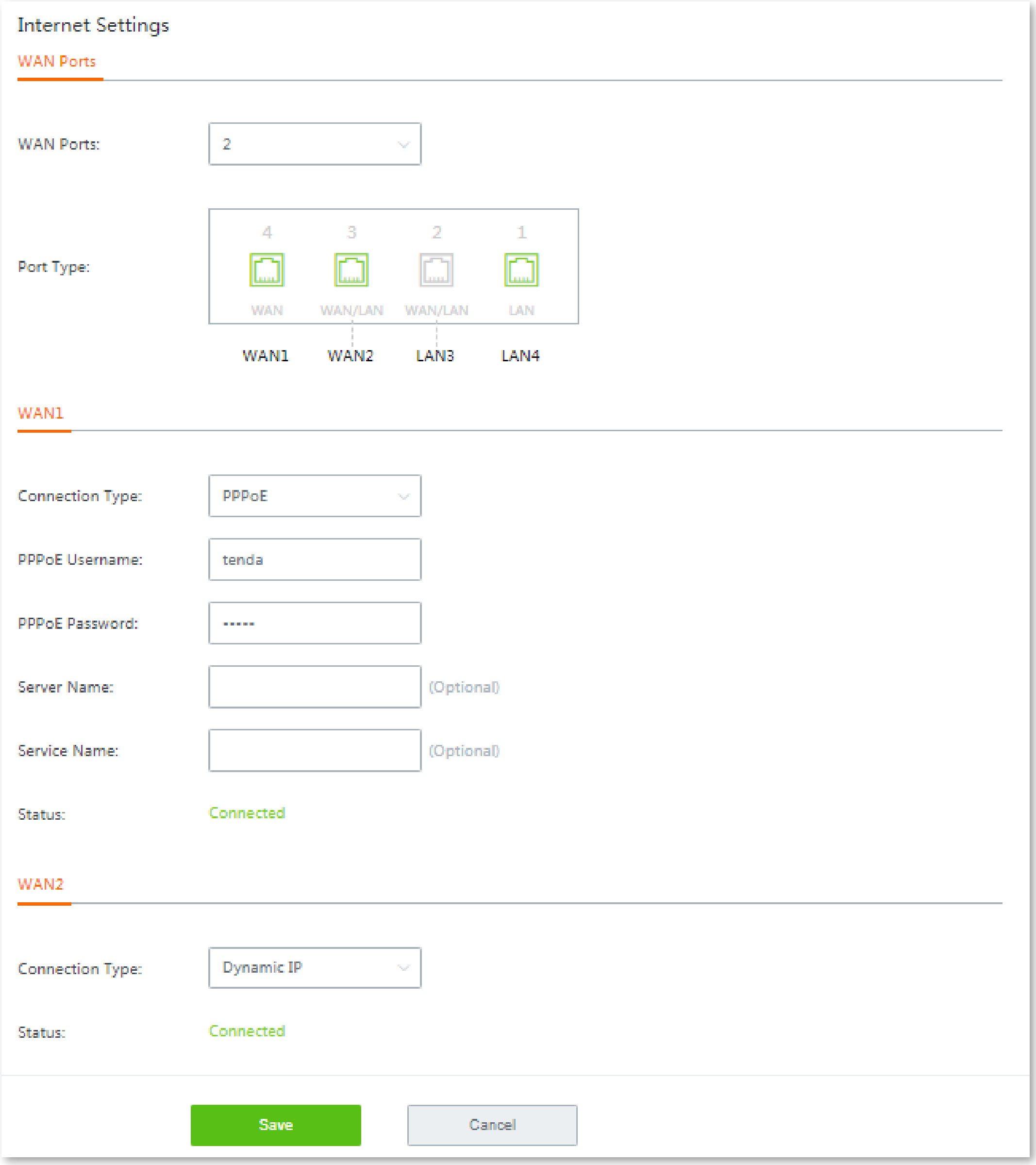
The static routing function can address this requirement.



Configuration procedure

Step 1 Configuring multiple WAN ports.

Refer to Configuring multiple WAN ports to configure the **WAN1** port to **PPPoE** and **WAN2** port to **Dynamic IP**. See the following figure:


Internet Settings

WAN Ports

WAN Ports: 2

Port Type:

WAN1

Connection Type: PPPoE

PPPoE Username: tenda

PPPoE Password: -----

Server Name: (Optional)

Service Name: (Optional)

Status: Connected

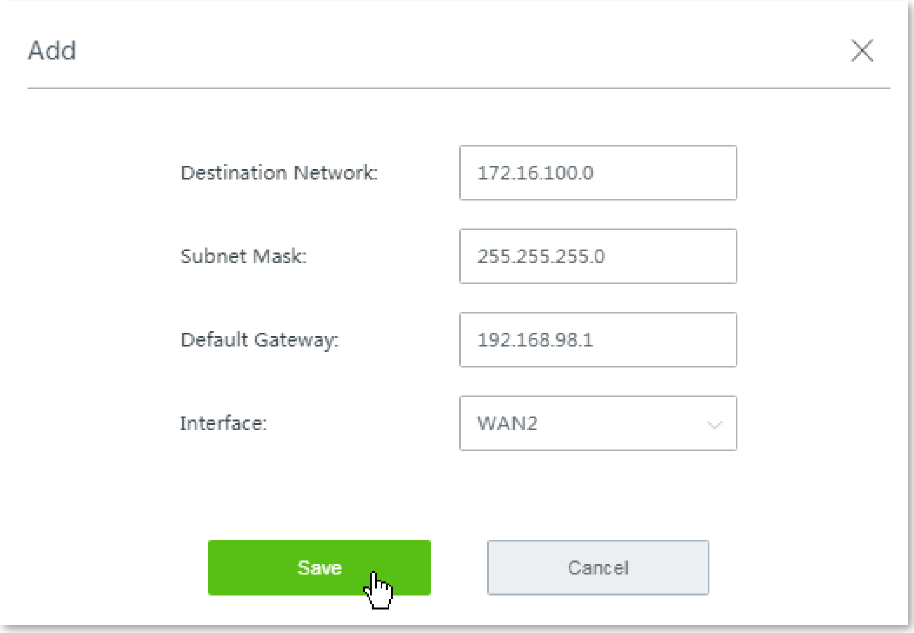
WAN2

Connection Type: Dynamic IP

Status: Connected

Step 2 Configuring static routing rules.

1. Navigate to **System Status** to view the default gateway of WAN2 port, which is **192.168.98.1** in this example.
2. Click **More** > **Static Routing**, and click **+Add**. The **Add** configuration window appears.
3. Set the parameters and click **Save**.

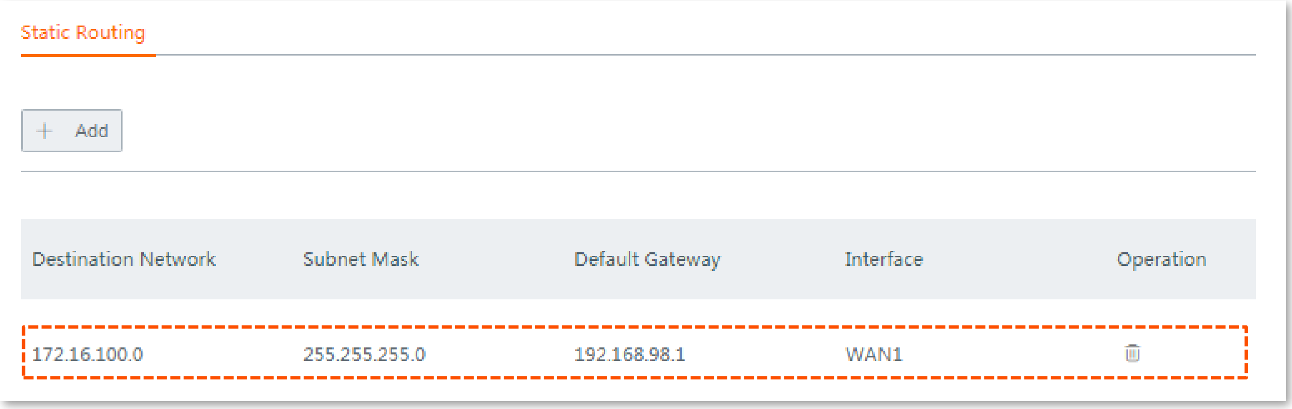


Add

Destination Network:	172.16.100.0
Subnet Mask:	255.255.255.0
Default Gateway:	192.168.98.1
Interface:	WAN2

---- End

Added successfully. See the following figure:



Destination Network	Subnet Mask	Default Gateway	Interface	Operation
172.16.100.0	255.255.255.0	192.168.98.1	WAN1	🗑

Verification

Computers in the LAN can access the internet and the intranet simultaneously.

TIP

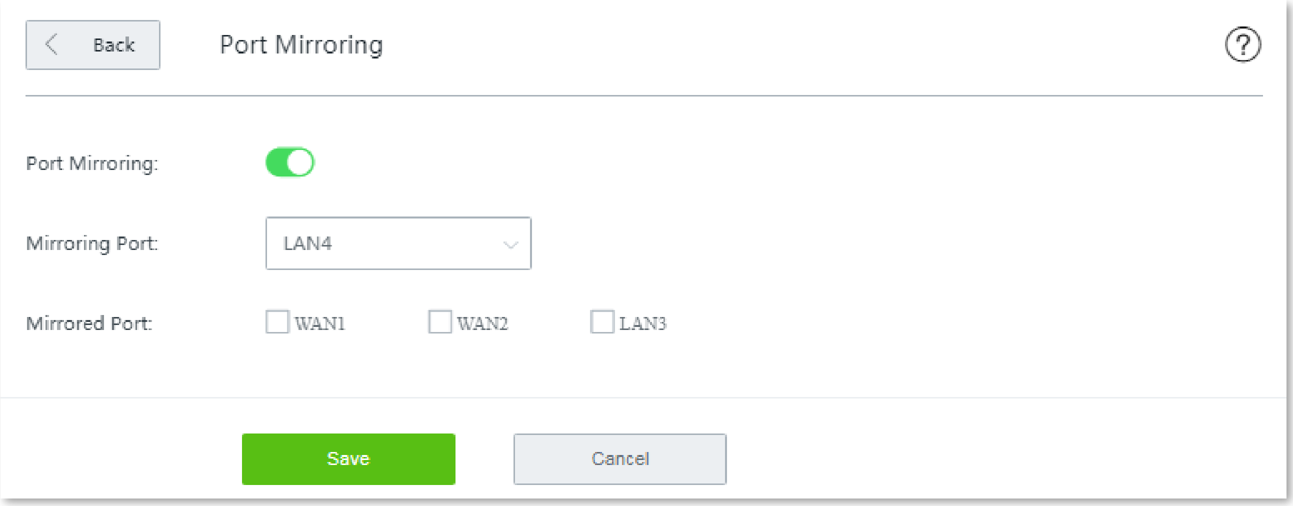
- If the enterprise LAN is connected to the internet, the router may point its default route to the other router, resulting in incorrect routing. In this case, navigate to **Bandwidth Control** and set **Upload/Download Rate** of the **WAN2** port to a value far smaller than the value of the **WAN1** port.
- If the preceding case occurs, it is recommended that you disable the smart load balancing function of the router and use a user-defined multi-WAN policy to ensure that all LAN users access the internet through the WAN1 port of the router.

11.4 Port mirroring

11.4.1 Overview

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

By default, this function is disabled. Choose **More** > **Port Mirroring**, and enable this function, the following configuration page appears:



Port Mirroring: ●

Mirroring Port: LAN4

Mirrored Port: □ WAN1 □ WAN2 □ LAN3

Parameter description

Parameter	Description
Port Mirroring	It is used to enable or disable the port mirroring function. The default option is **Disable**.
Mirroring Port	It indicates the monitoring port. A piece of monitoring software must be installed on the computer with this port to perform monitoring. The default mirroring port is **LAN4**.
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.

11.4.2 Configuring port mirroring

Step 1 Choose **More** > **Port Mirroring** to access the configuration page.

Step 2 Set **Port Mirroring** to **Enable**.

Step 3 Choose **Mirroring Port** and **Mirrored Port** as required.

Step 4 Click **Save** to apply your settings.

---- End

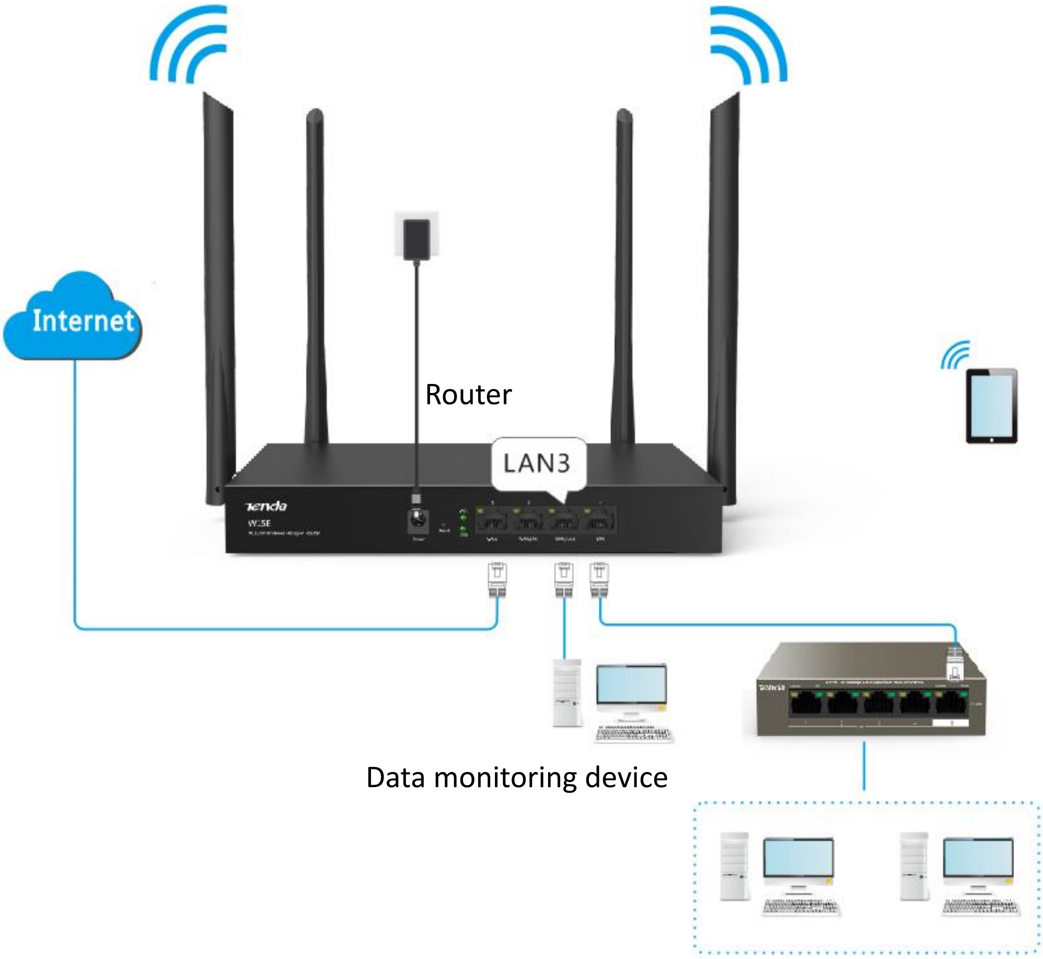
11.4.3 Example of configuring port mirroring

Networking requirement

An enterprise has used W15E 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.

Solutions

The port mirroring function of the router can meet this requirement.



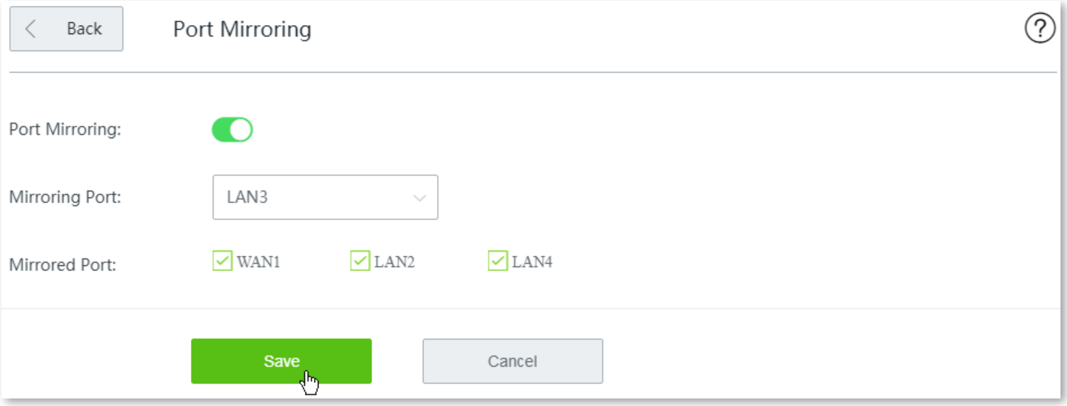
Configuration procedure

Step 1 Choose **More** > **Port Mirroring** to access the configuration page.

Step 2 Set **Port Mirroring** to **Enable**.

Step 3 Choose **Mirroring Port** and **Mirrored Port** as required.

Step 4 Click **Save** to apply your settings.



Port Mirroring: ●

Mirroring Port: LAN3

Mirrored Port: ☑ WAN1 ☑ LAN2 ☑ LAN4

---- End

Verification

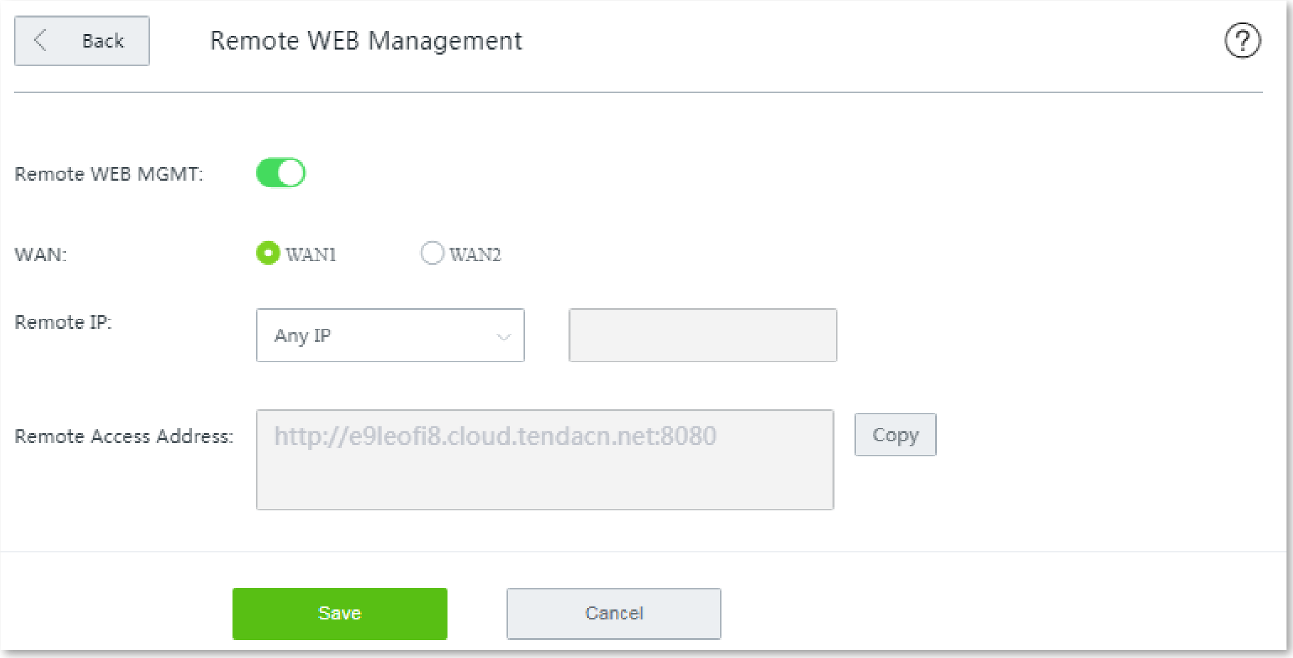
Run monitoring software such as Wireshark on the monitoring computer to verify the software can capture data packets from the mirrored ports.

11.5 Managing your router remotely using web UI

11.5.1 Overview

Generally, the web UI of the router can only be accessed on devices that are connecting to the router in wired or wireless manner. This costs in case of seeking technician to fix network problems. The remote web management function is designed to address such requirement. When you encounter network faulty, you can ask technician far away to diagnose and fix your problems, improving efficiency and reducing costs and efforts.

Choose **More** > **Remote WEB Management**, and enable this function, the configuration page appears. See the following figure:



Remote WEB Management

Remote WEB MGMT: enabled

WAN: ● WAN1 ○ WAN2

Remote IP: Any IP

Remote Access Address: http://e9leofi8.cloud.tendacn.net:8080

Parameter description

Parameter	Description
Remote IP	IP address of the computer that can access the router remotely. - **Any IP**: Any computers can access the router over the internet. Choose this option only when necessary since it lowers network security. - **Specified IP**: Only a computer with the specified IP address can access the router over the internet. If the computer is on a LAN, enter the WAN port IP address of the gateway of the computer.
Remote Access Address	With this function enabled, the router automatically generates one unique domain name that can be used to manage the router remotely.

11.5.2 Conifguring remote web management

Step 1 Click **More** > **Remote WEB Management**, and enable this function.

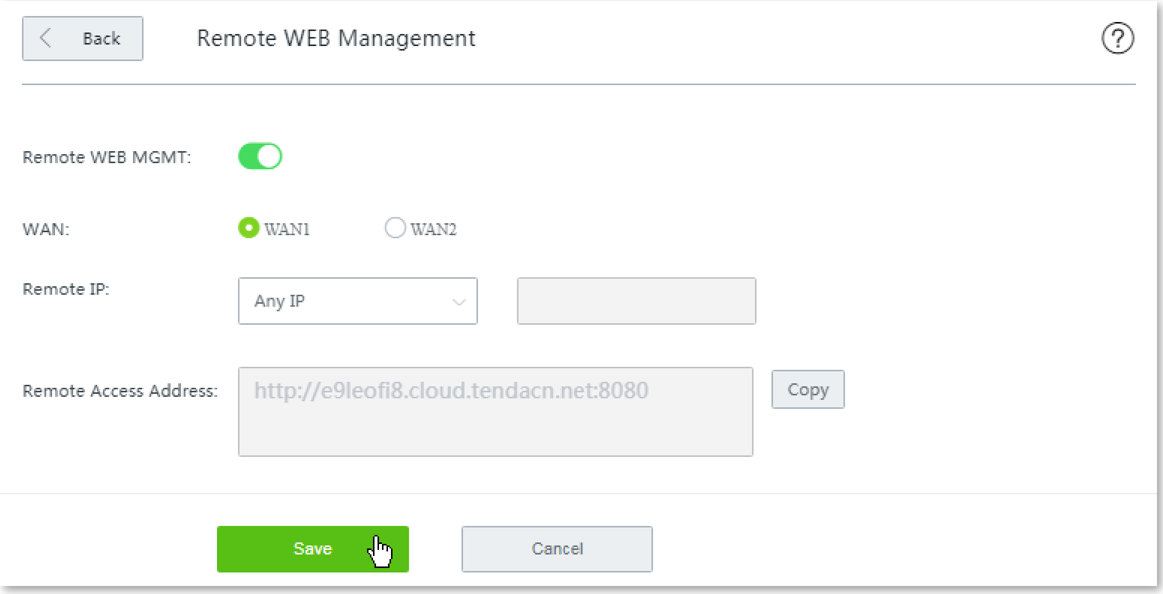
Step 2 Select the **WAN** port for remote access.

Step 3 Set the **Remote IP** to either of **Any IP** or **Specified IP**.

TIP

- **Any IP**: It indicates that all internet users can access the web UI of the router with the **Remote Access Address** here. For security of your network, select this option only when necessary.
- **Specified IP**: It indicates that only the host with the specified public IP address is allowed to access the web UI of router remotely.
- If the computer for remote access is in an intranet, enter the public IP address of the computer's gateway here.

Step 4 Click **Save** to apply your settings.



Remote WEB MGMT: ●

WAN: ● WAN1 ○ WAN2

Remote IP: Any IP

Remote Access Address: http://e9leofi8.cloud.tendacn.net:8080

---- End

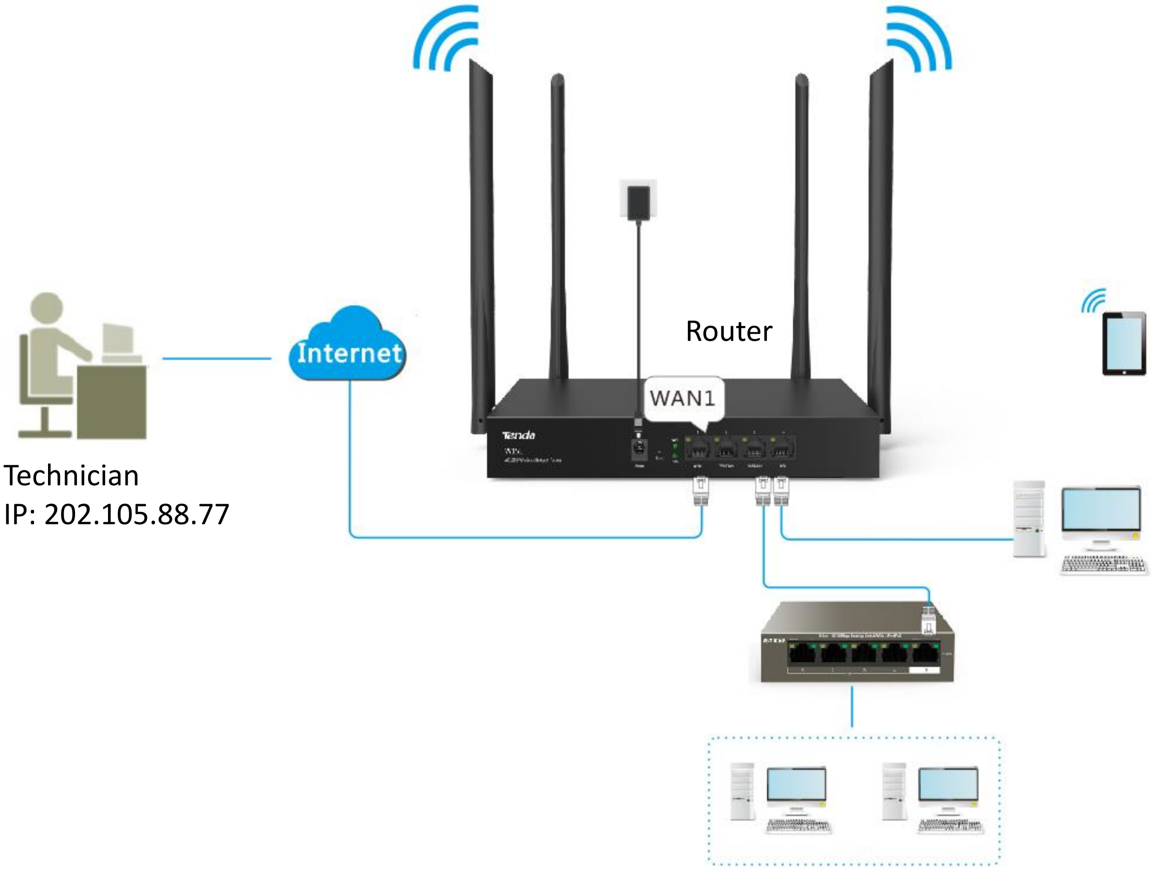
11.5.3 Example of conifguring remote web management

Networking requirement

An enterprise uses W15E to deploy its network. And its network administrator needs to seek a Tenda technician to solve a problem remotely.

Solutions

Remote web management function can meet this requirement.



Configuration procedure

Step 1 Click **More** > **Remote WEB Management**, and enable this function.

Step 2 Select the **WAN** port for remote access, which is **WAN2** in this example.

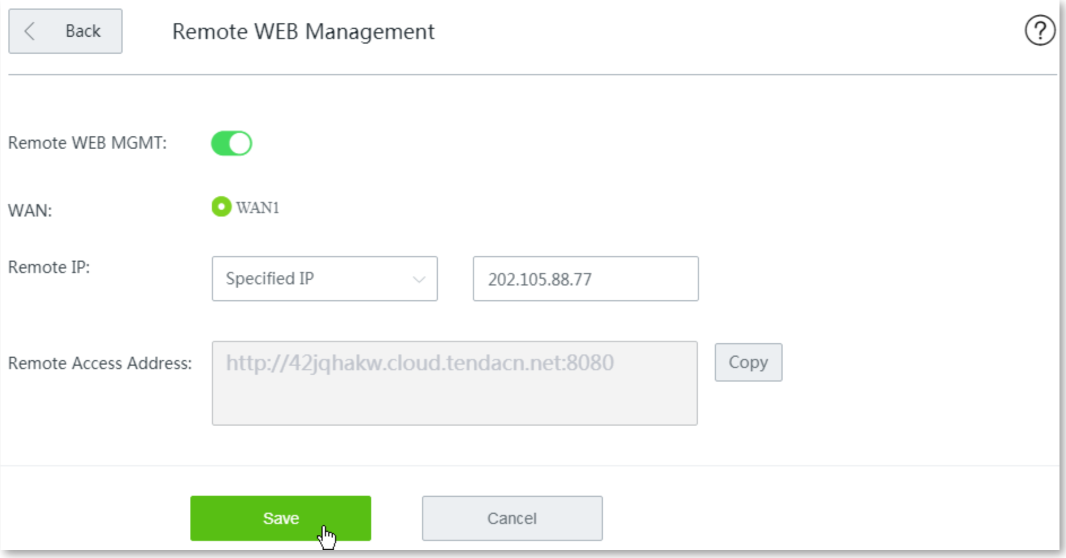
Step 3 Enter the IP address of the technician’s computer, which is **202.105.88.77** in this example.

TIP

If the technician’ computer is in a remote LAN network, set the WAN IP address of his router as the **Specified IP**.

Step 4 Click **Save** to apply your settings.

Step 5 Click **Copy** and send the **Remote Access Address** to the Tenda technician.



Remote WEB MGMT: ●

WAN: ● WAN1

Remote IP: Specified IP 202.105.88.77

Remote Access Address: http://42jqhakw.cloud.tendacn.net:8080

---- End

Verification

Tenda technician with a computer IP address 202.105.88.77 can use http://e9leofi8.cloud.tendacn.net:8080 to access the web UI of the router remotely.

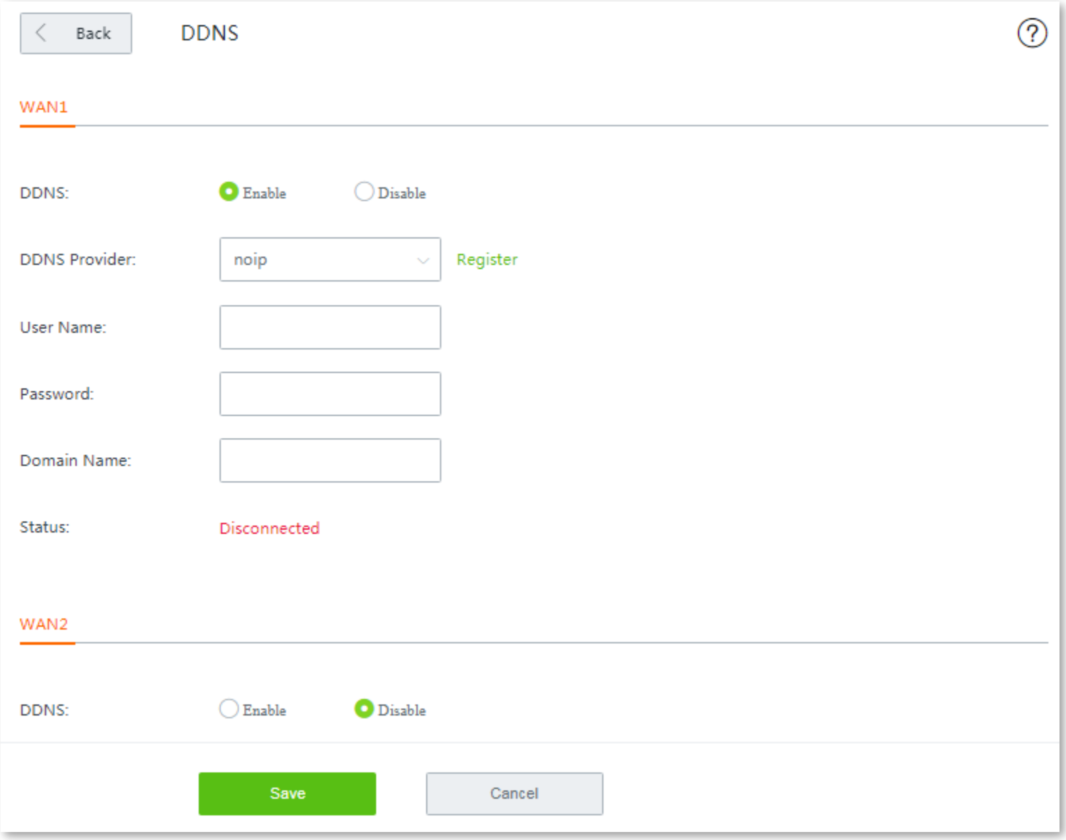
11.6 DDNS

11.6.1 Overview

DDNS is short for Dynamic Domain Name Server. It detects when your IP address changes and maps your dynamic IP address to a static domain name. When the service is running, the DDNS client on the router sends its current WAN port IP address to the DDNS server. Then the server updates the mapping between the domain name and the IP address in the database to implement dynamic domain name resolution. If you enable this function, the router sends its WAN IP address to the specified DDNS server when the WAN IP address is changed and the DDNS server maps the changed WAN IP address to a specified static domain name. This enables internet users to access services on your LAN through the static domain name instead of the changeable WAN IP address.

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

Choose **More** > **DDNS**, and enable this function, the configuration page appears. See the following figure:



Back DDNS

WAN1

DDNS: ● Enable ○ Disable

DDNS Provider: noip Register

User Name:

Password:

Domain Name:

Status: Disconnected

WAN2

DDNS: ○ Enable ● Disable

Save Cancel

Parameter description

Parameter	Description
DDNS	Used to enable or disable the function.
DDNS Provider	The router supports four DDNS providers: **noip**, **dyndns**, **oray**, and **gnway**.
User Name	It specifies the user name used to log in to a DDNS provider. It is registered on the website of the provider.

Parameter	Description
Password	It specifies the password used to log in to a DDNS provider.
Domain Name	It specifies the domain name obtained from a DDNS provider.
Status	It specifies the DDNS service status.

11.6.2 Configuring DDNS

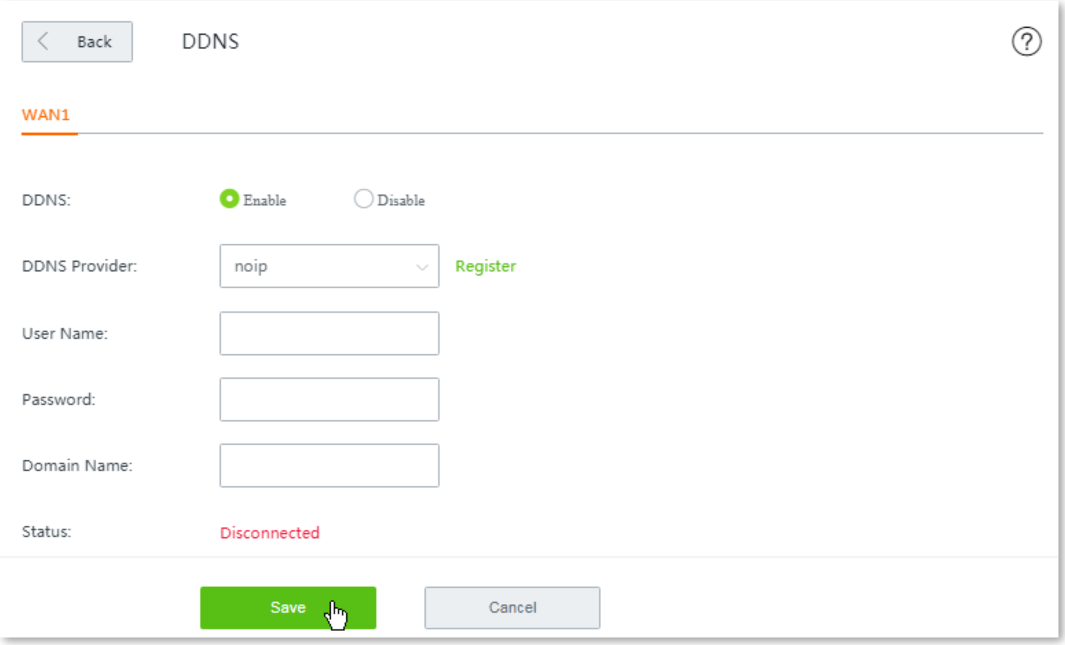
NOTE

- A dynamic IP address will disable the port forwarding rule. To use this function and make the rule always effective, set a static IP address for the specified local host.
- Some programs, such as firewall, antivirus software, and security guard, may hinder internet users to access the local service. Disable them when necessary.

Step 1 Choose **More** > **DDNS**, locate the WAN port and enable the function.

Step 2 Set required parameters.

Step 3 Click **Save** to apply your settings.



DDNS: ● Enable ○ Disable

DDNS Provider: noip

User Name:

Password:

Domain Name:

Status: Disconnected

---- End

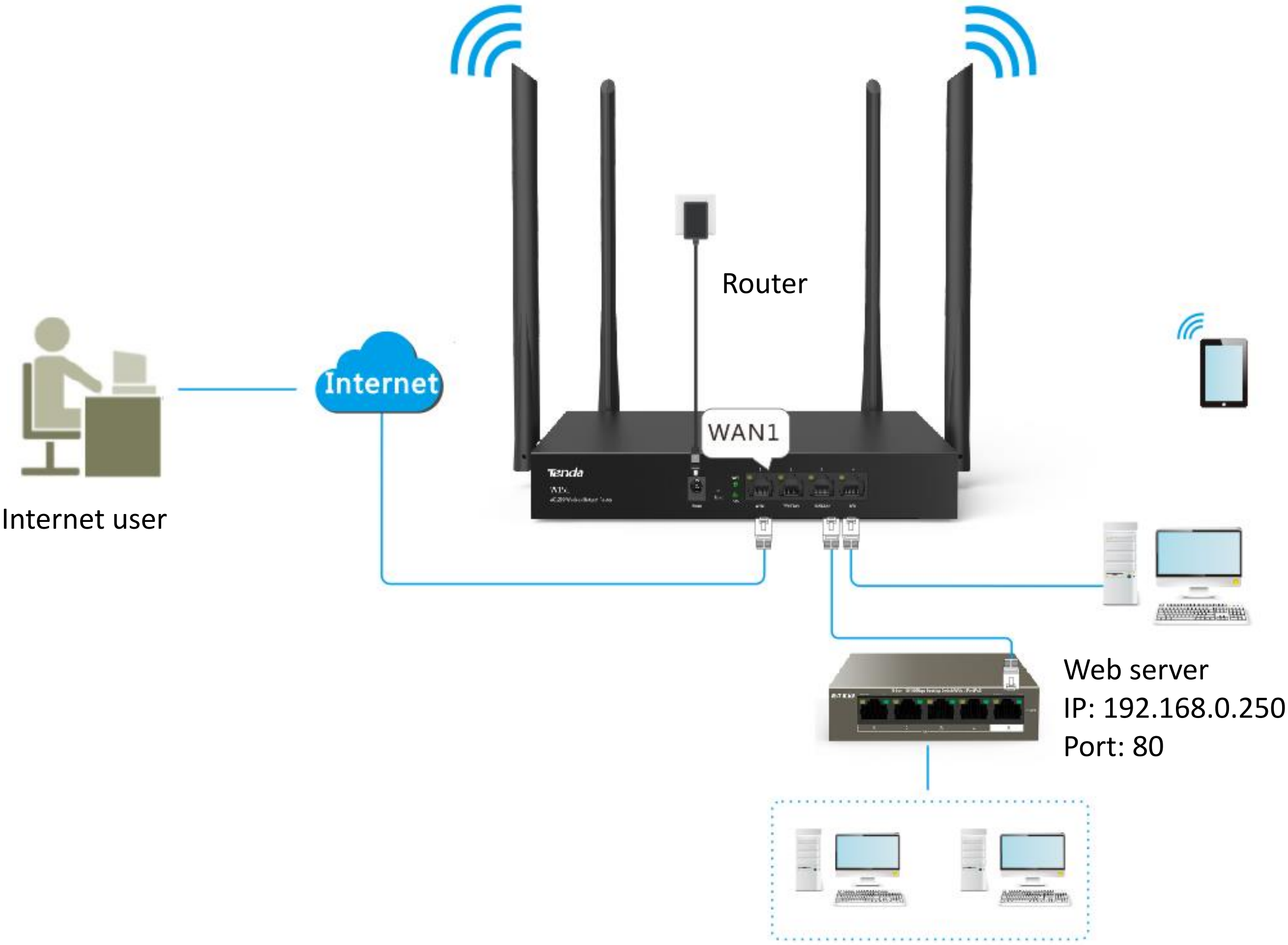
11.6.3 Example of configuring DDNS

Networking requirement

An enterprise uses W15E 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. Assume that the external port is 80.

Solutions

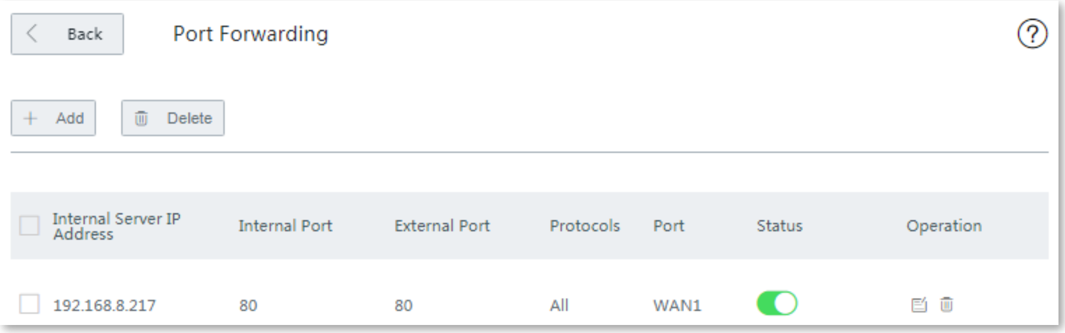
You can use Port Forwarding and DDNS function to meet this requirement.



Configuration procedure

Step 1 **Configuring port forwarding.**

Navigate to **More** > **Port Forwarding**, and add a rule. See Port forwarding for detailed configuration procedure.



□	Internal Server IP Address	Internal Port	External Port	Protocols	Port	Status	Operation
□	192.168.8.217	80	80	All	WAN1	●	

Step 2 **Configuring DDNS.**

1. Register a domain name.

   Select the DDNS provider from the drop-down list menu, which is **noip** in this example, and click **Register** next to the menu to register a domain name.

2. Set DDNS parameters.

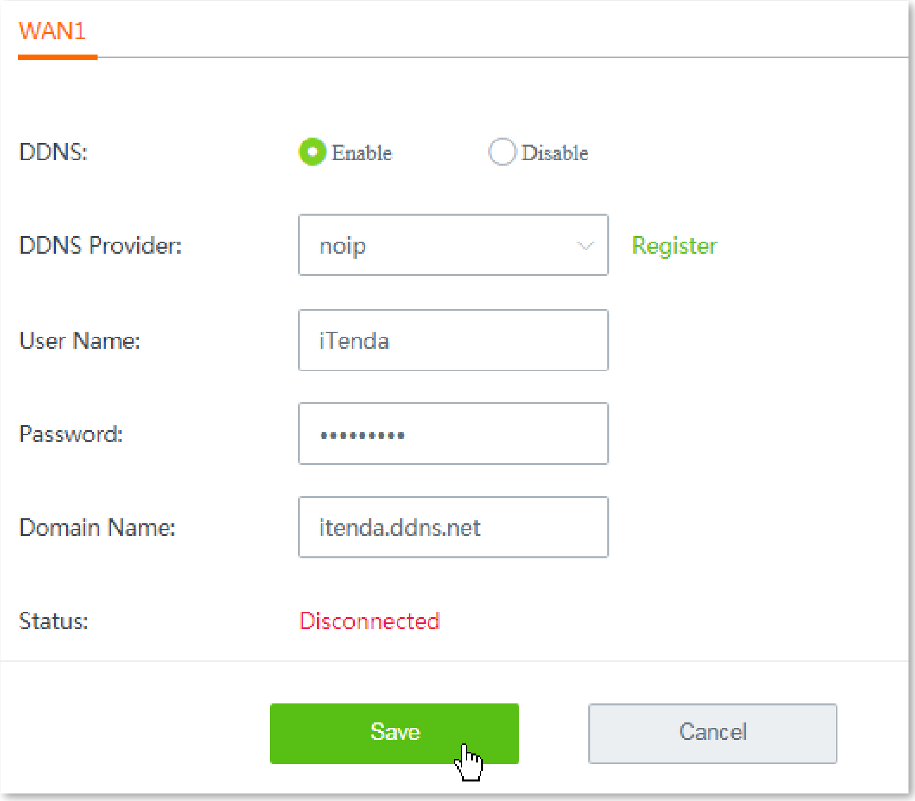
   (1) Log in to the web UI of the router, navigate to **More** > **DDNS**, and enable **WAN1** port's DDNS function.

   (2) Enter the DDNS-related parameters you registered on your DDNS provider's website.

Assume that you DDNS-related information are:

- User Name for DDNS: **iTenda**
- Password for DDNS: **itenda123**
- Domain Name for DDNS: **itenda.ddns.net**.

(3) Click **Save** to apply your settings.



WAN1

DDNS: ● Enable ○ Disable

DDNS Provider: noip

User Name: iTenda

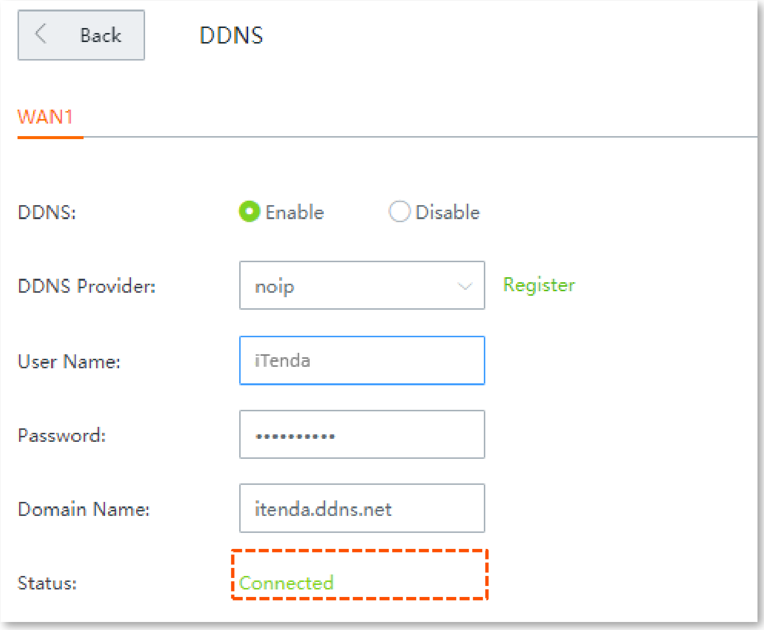
Password: ••••••••••

Domain Name: itenda.ddns.net

Status: Disconnected

---- End

Wait a moment, and refresh the page. When the **Status** shows **Connected**, the configuration completes successfully.



DDNS

WAN1

DDNS: ● Enable ○ Disable

DDNS Provider: noip

User Name: iTenda

Password: ••••••••••

Domain Name: itenda.ddns.net

Status: Connected

Verification

Internet users can use http://itenda.ddns.net:80 to access the web server. Among which:

- **http** indicates intranet service protocol name.
- **itenda.ddny.net** is the domain name you registered on your DDNS provider's website.
- **80** is the external port number.

TIP

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

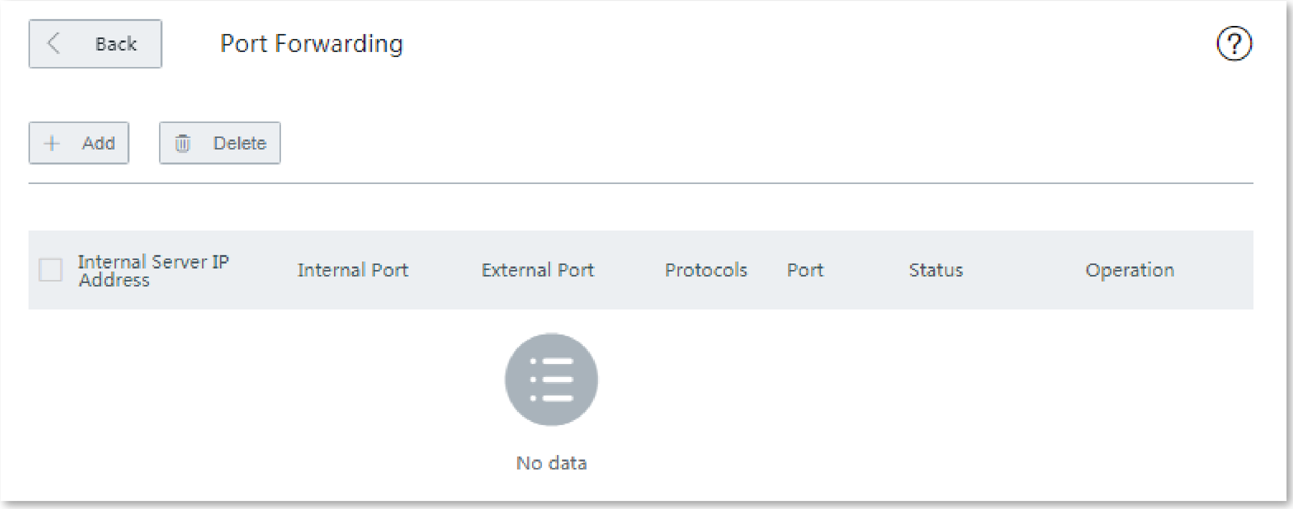
- Make sure that the WAN IP address of the router is a public IP address.
- Make sure that the intranet port number is the service port number on the local host.

11.7 Port forwarding

11.7.1 Overview

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

To access the configuration page, choose **More** > **Port forwarding**. See the following figure:



Parameter description

Parameter	Description
Internal Server IP Address	It specifies the IP address of a local computer that runs a specified service.
Internal Port	It specifies the service port of a server on a local computer.
External Port	It specifies the port for internet users to access a specified service.
Protocols	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**.
Port	It specifies the physical WAN port that internet users use to access the specified service.
Status	It specifies whether the rule is enabled or not.

11.7.2 Configuring a port forwarding rule

NOTE

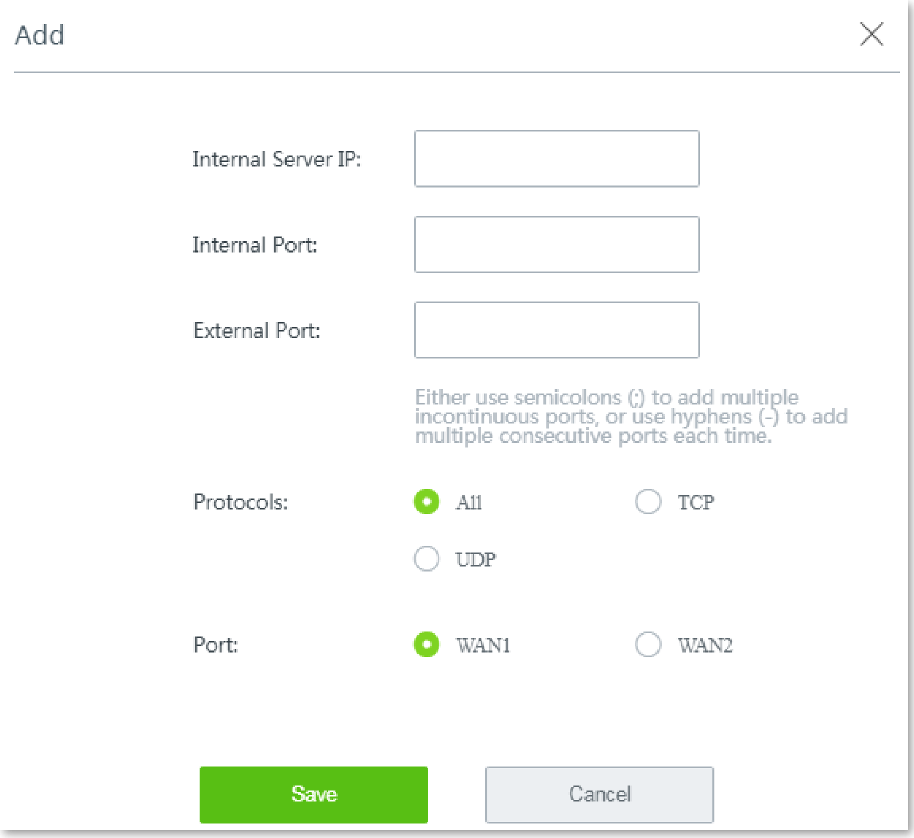
- A dynamic IP address will disable the port forwarding rule. To use this function and make the rule always effective, set a static IP address for the specified local host.
- Some programs, such as firewall, antivirus software, and security guard, may hinder internet users to access the local service. Disable them when necessary.

Step 1 Choose **More** > **Port Forwarding** to enter the configuration page.

Step 2 Click **+Add**. The **Add** configuration window appears.

Step 3 Set required parameters.

Step 4 Click **Save** to apply your settings.



Internal Server IP:

Internal Port:

External Port:

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

Protocols: ● All ○ TCP ○ UDP

Port: ● WAN1 ○ WAN2

---- End

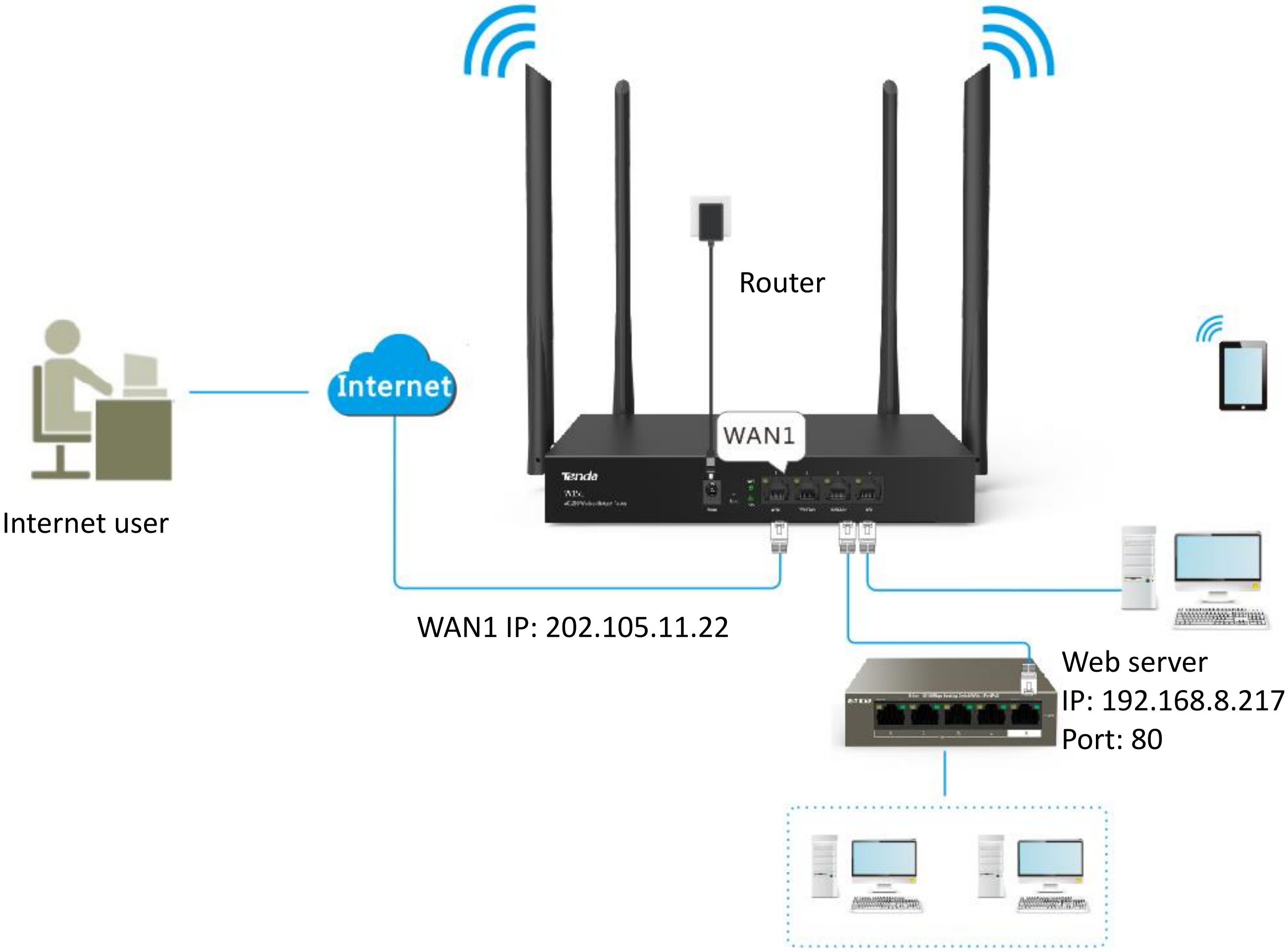
11.7.3 Example of configuring a port forwarding rule

Networking requirement

An enterprise uses W15E 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.

Solutions

You can use the port forwarding function to meet this requirement.



Configuration procedure

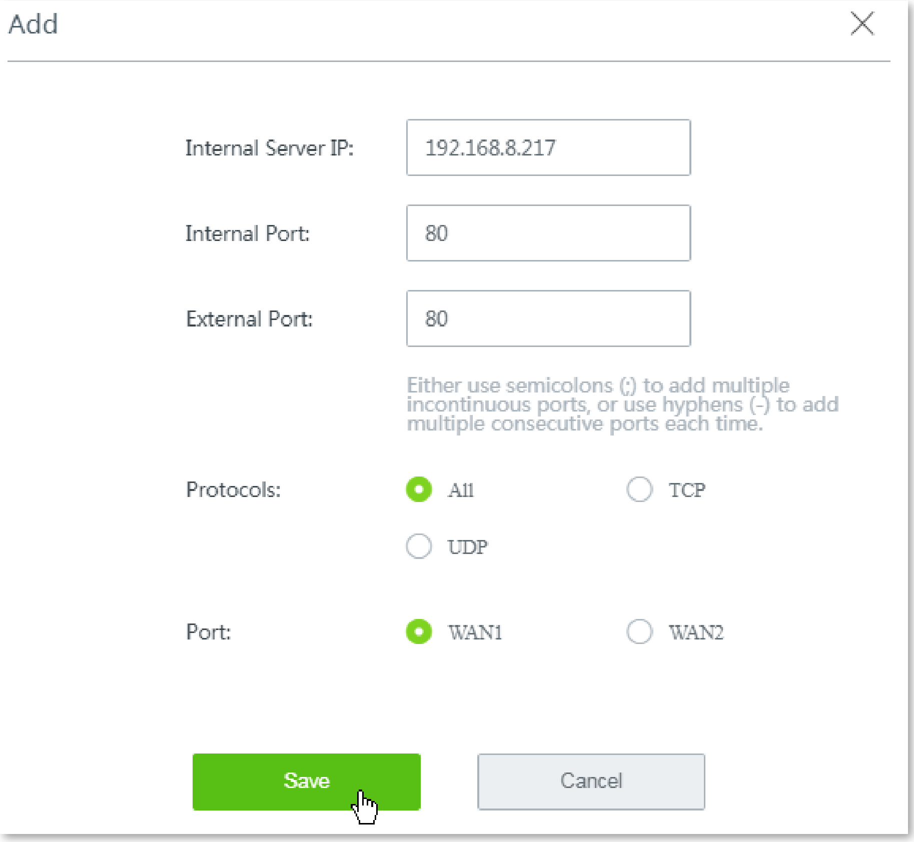
Step 1 Choose **More** > **Port Forwarding** to enter the configuration page.

Step 2 Click **+Add**. The **Add** configuration window appears.

Step 3 Set required parameters. In this example, the parameters are as follows:

- Internal Server IP: **192.168.8.217**
- Internal Port: **80**
- External Port: **80**
- Protocols: **All**
- Port: **WAN1**

Step 4 Click **Save** to apply your settings.



Add

Internal Server IP: 192.168.8.217

Internal Port: 80

External Port: 80

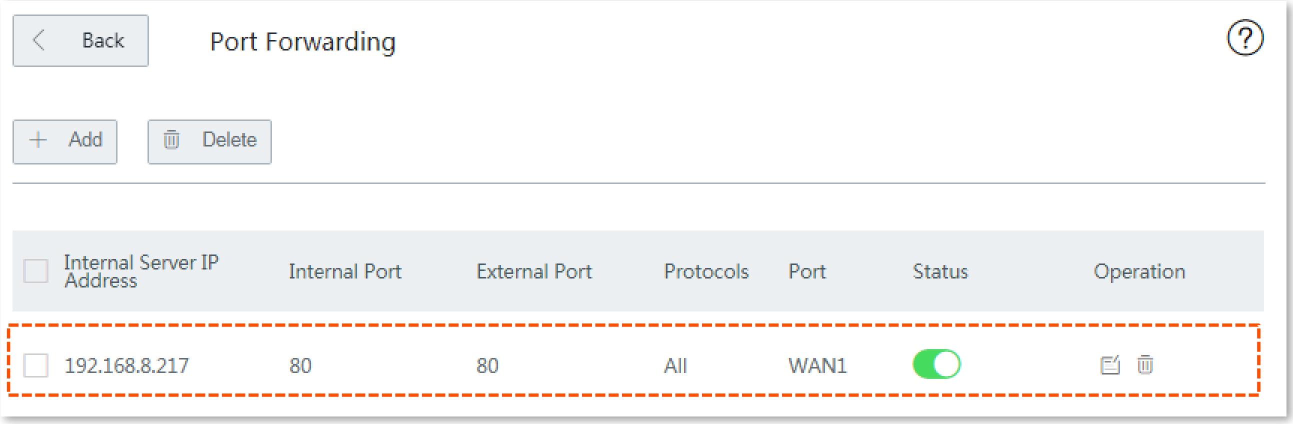
Either use semicolons (;) to add multiple incontinuous ports, or use hyphens (-) to add multiple consecutive ports each time.

Protocols: ● All ○ TCP ○ UDP

Port: ● WAN1 ○ WAN2

---- End

Added successfully. See the following figure:



Port Forwarding

□	Internal Server IP Address	Internal Port	External Port	Protocols	Port	Status	Operation
□	192.168.8.217	80	80	All	WAN1	●	

Verification

Internet users can use http://202.105.11.22:80 to access the web server. Among which:

- **http** indicates intranet service protocol name.
- **202.105.11.22** is the WAN1 IP address.
- **80** is the external port number.

In addition, If the corresponding WAN port is configured with DDNS, you can use **intranet service protocol name://domain name:external port** to access the web server.

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.

11.8 DMZ host

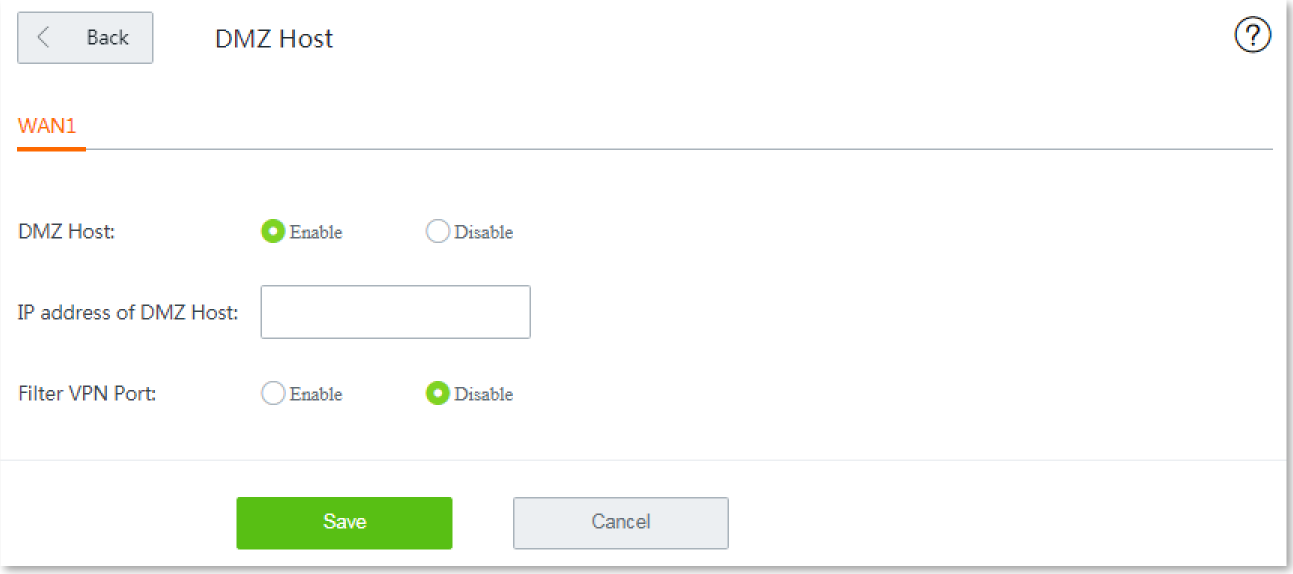
11.8.1 Overview

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.

Choose **More** > **DMZ Host**, and enable this function, the following configuration page appears.



DMZ Host: ● Enable ○ Disable

IP address of DMZ Host:

Filter VPN Port: ○ Enable ● Disable

Parameter description

Parameter	Description
DMZ Host	Used to enable or disable the function.
IP Address of DMZ Host	It specifies the IP address of the would-be DMZ host.
Filter VPN Port	It used to specify whether to filter the VPN port if DMZ is enabled for a host. By default, it is disabled. - **Enable**: The router filters the VPN port and responds to VPN requests from internet. - **Disable**: The router does not filter the VPN port and the VPN function of the router is disabled. VPN requests from internet users are responded by the DMZ host.

11.8.2 Configuring DMZ host

NOTE

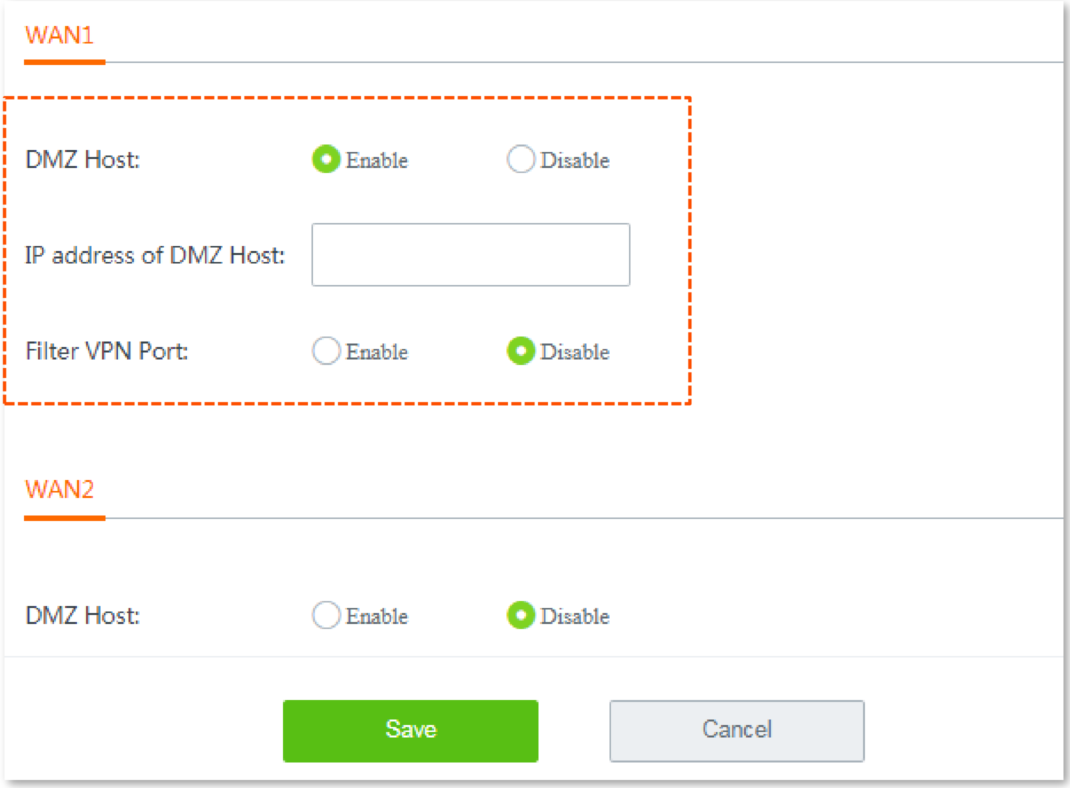
- A dynamic IP address will disable the port forwarding rule. To use this function and make the rule always effective, set a static IP address for the specified local host.
- Some programs, such as firewall, antivirus software, and security guard, may hinder internet users to access the local service. Disable them when necessary.

Step 1 Choose **More** > **DMZ Host**, and enable this function of the corresponding WAN port.

Step 2 Enter the **IP address of the DMZ Host**.

Step 3 Enable **Filter VPN Port** as required.

Step 4 Click **Save** to apply your settings.



WAN1

DMZ Host: ● Enable ○ Disable

IP address of DMZ Host:

Filter VPN Port: ○ Enable ● Disable

WAN2

DMZ Host: ○ Enable ● Disable

---- End

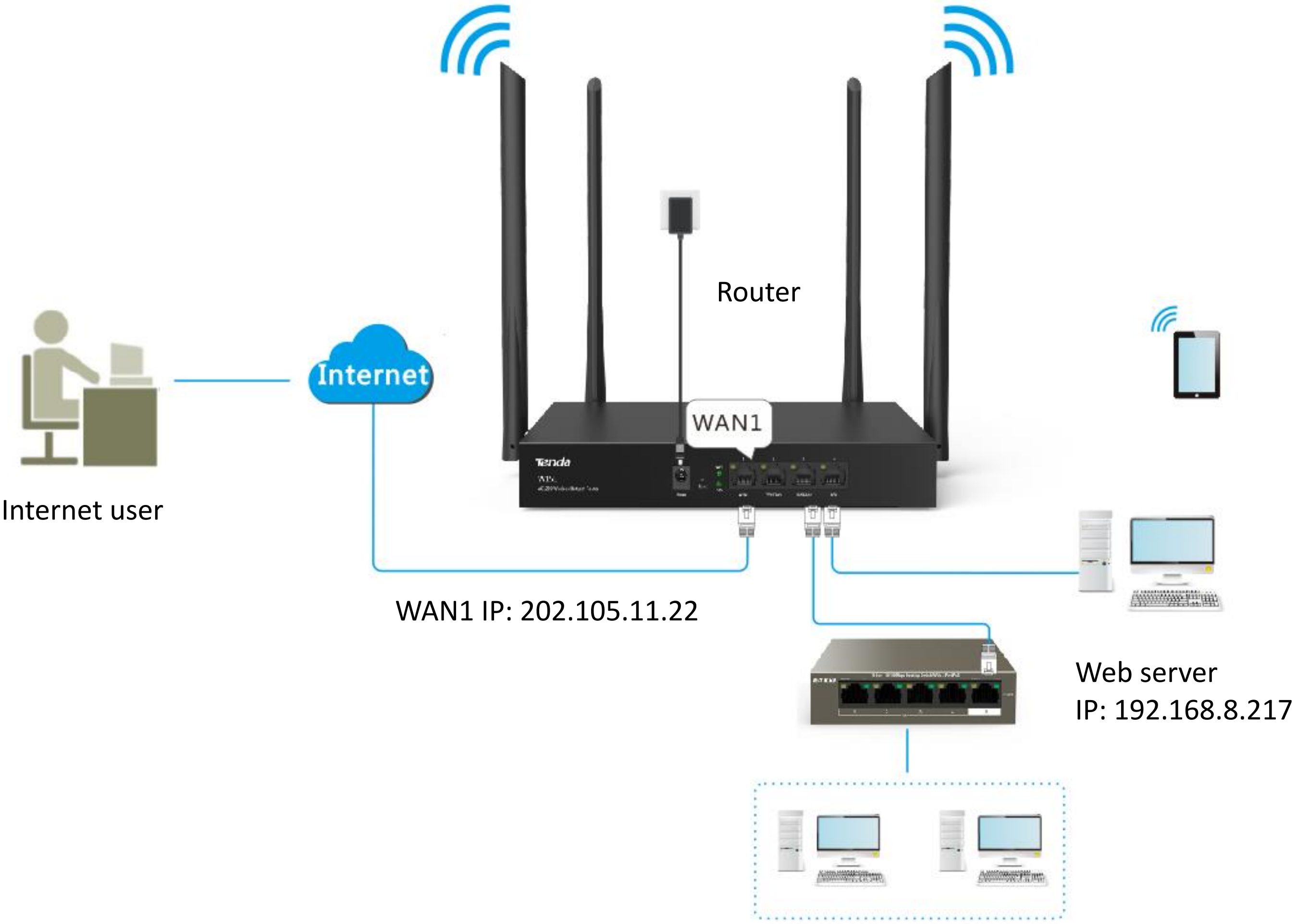
11.8.3 Example of configuring DMZ host

Networking requirement

An enterprise uses W15E 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.

Solutions

You can use the DMZ function to meet this requirement.



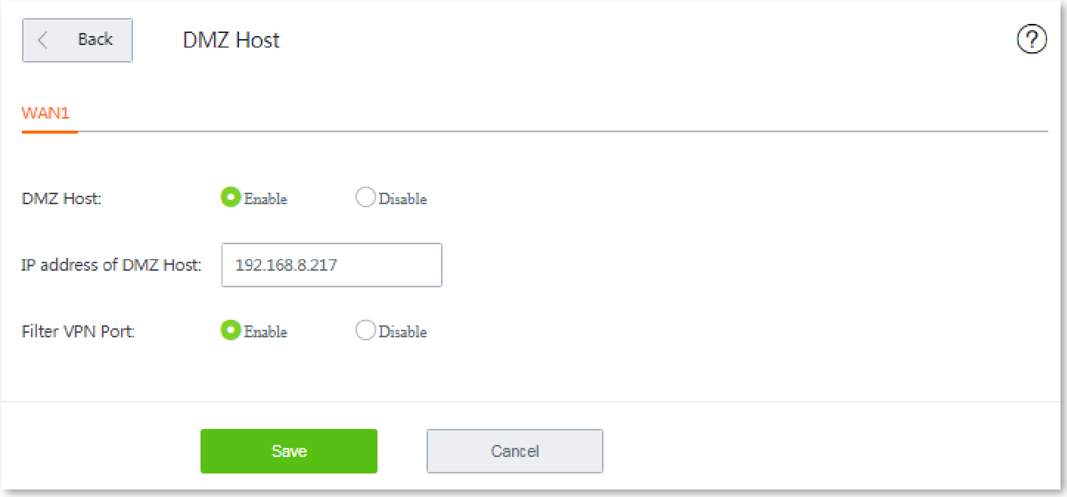
Configuration procedure

Step 1 Choose **More** > **DMZ Host**, and enable this function of the corresponding WAN port.

Step 2 Enter the **IP address of the DMZ Host**.

Step 3 Enable **Filter VPN Port** as required.

Step 4 Click **Save** to apply your settings.



DMZ Host: ● Enable ○ Disable

IP address of DMZ Host: 192.168.8.217

Filter VPN Port: ● Enable ○ Disable

---- End

Verification

Internet users can use http://202.105.11.22:80 to access the web server. Among which:

- **http** indicates intranet service protocol name.
- **202.105.11.22** is the WAN1 IP address.
- **80** is the external port number.

In addition, If the corresponding WAN port is configured with DDNS, you can use intranet service protocol name://domain name:external port to access the web server.

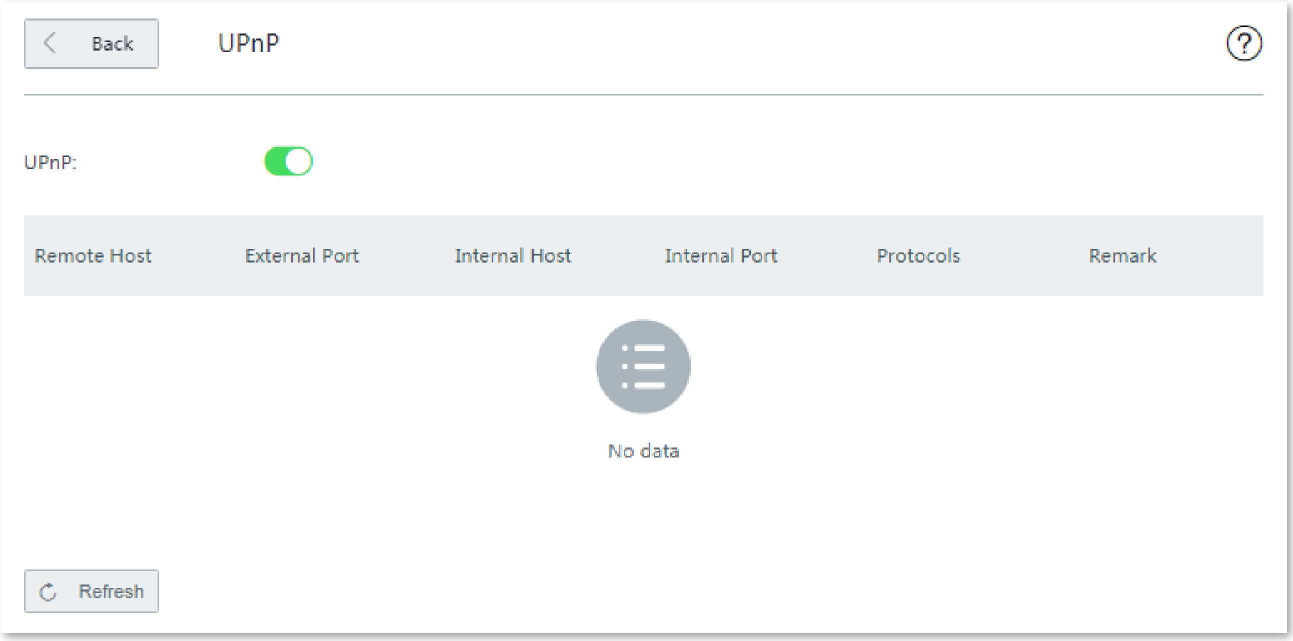
TIP

- 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.

11.9 UPnP

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

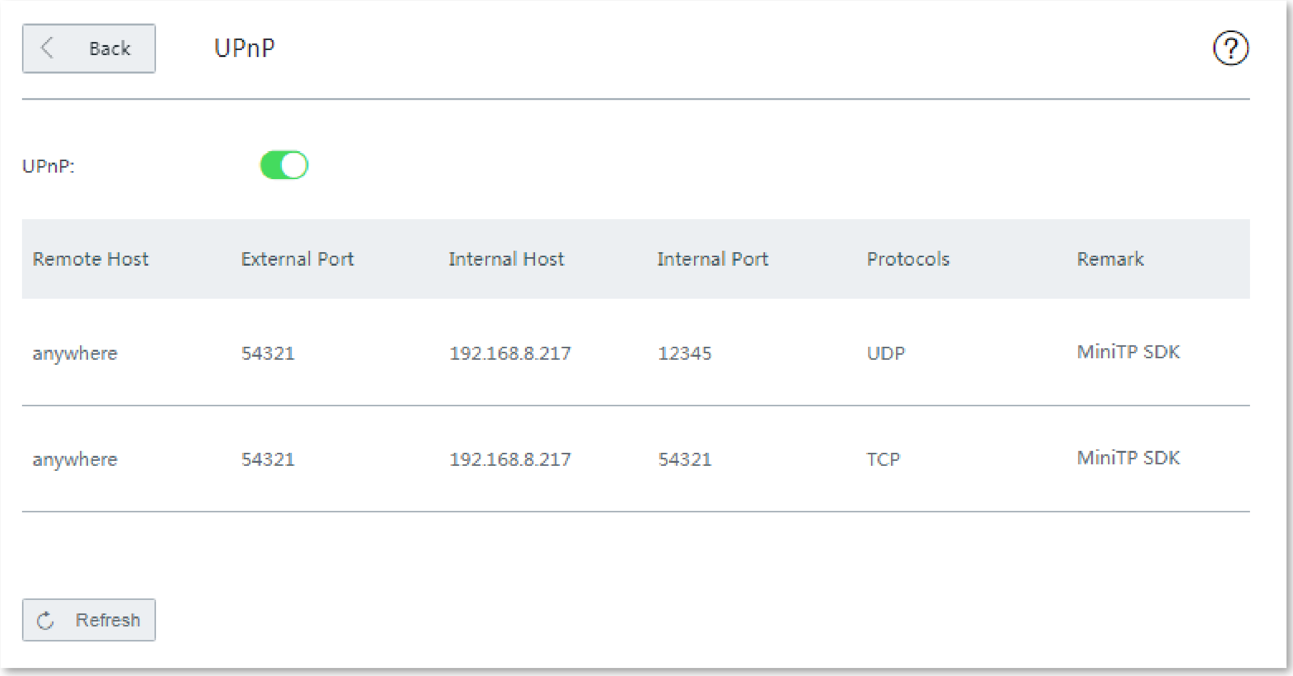
By default, this function is disabled. Choose **More** > **UPnP**, and enable this function, the following figure appears.



Remote Host	External Port	Internal Host	Internal Port	Protocols	Remark

No data

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



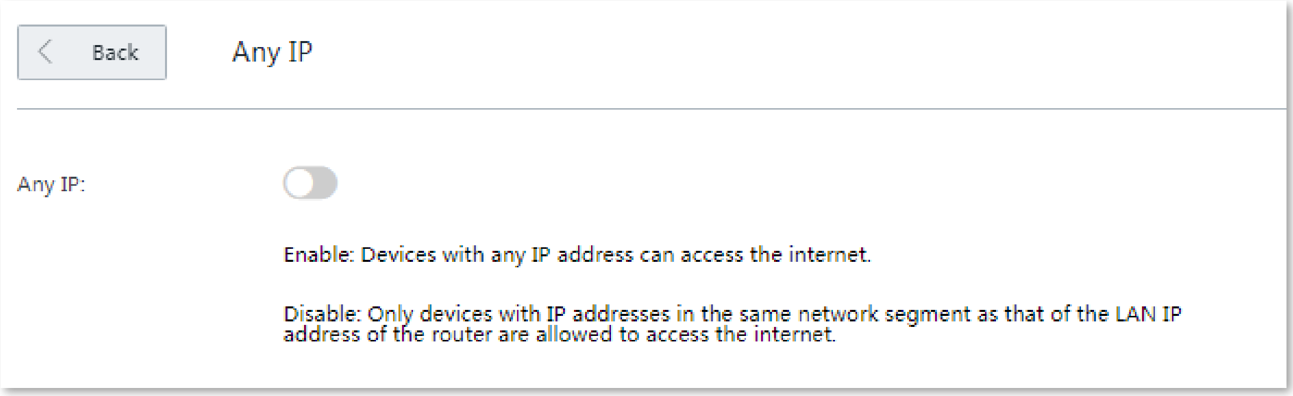
Remote Host	External Port	Internal Host	Internal Port	Protocols	Remark
anywhere	54321	192.168.8.217	12345	UDP	MiniTP SDK
anywhere	54321	192.168.8.217	54321	TCP	MiniTP SDK

11.10 Any IP

This function is typically used in public spaces, such as at a hotel. With this function enabled, devices with any IP address can access the internet through the router.

NOTE

This function cannot be enabled if **Captive Portal** or **WiFi via WeChat** is configured.



Any IP: ○

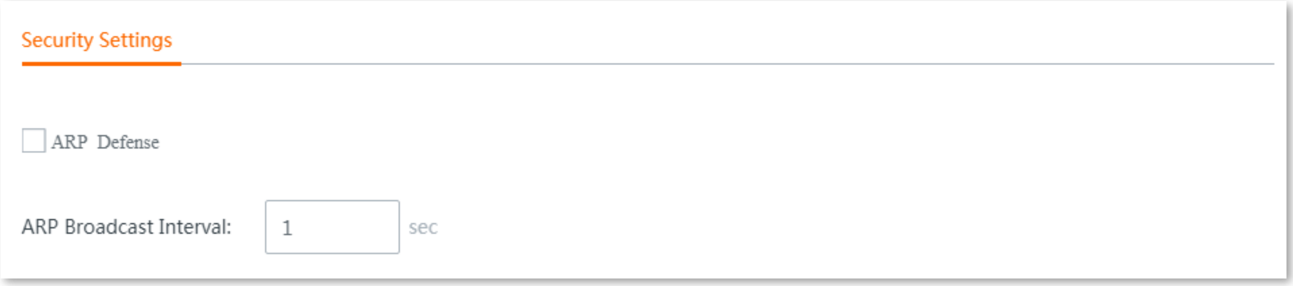
Enable: Devices with any IP address can access the internet.

Disable: Only devices with IP addresses in the same network segment as that of the LAN IP address of the router are allowed to access the internet.

11.11 Security settings

The router supports ARP defense, DDoS defense, IP attack defense, and Block WAN ping.

ARP defense



Security Settings

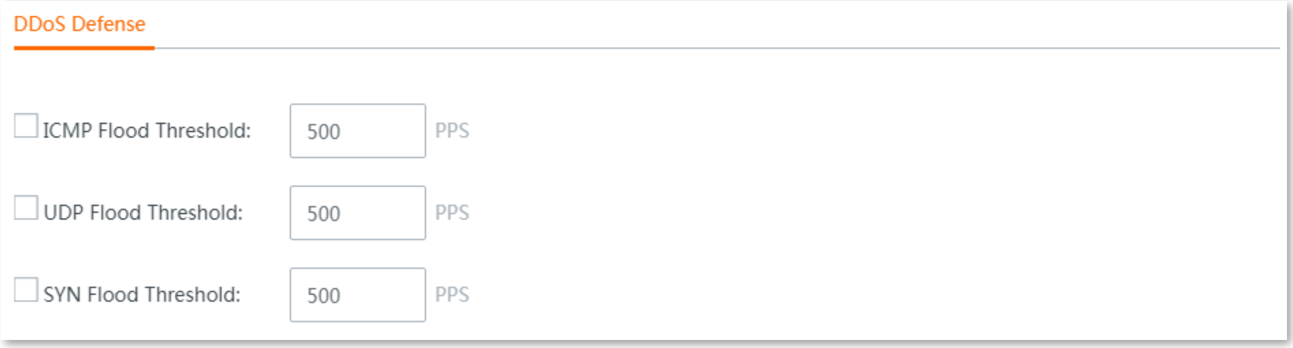
□ ARP Defense

ARP Broadcast Interval: 1 sec

Parameter description

Parameter	Description
ARP Defense	It is used to efficiently prevent the ARP attack from the local network.
ARP Broadcast Interval	It specifies the interval for sending ARP inquiry messages. Default: **1** second.

DDoS defense



DDoS Defense

□ ICMP Flood Threshold: 500 PPS

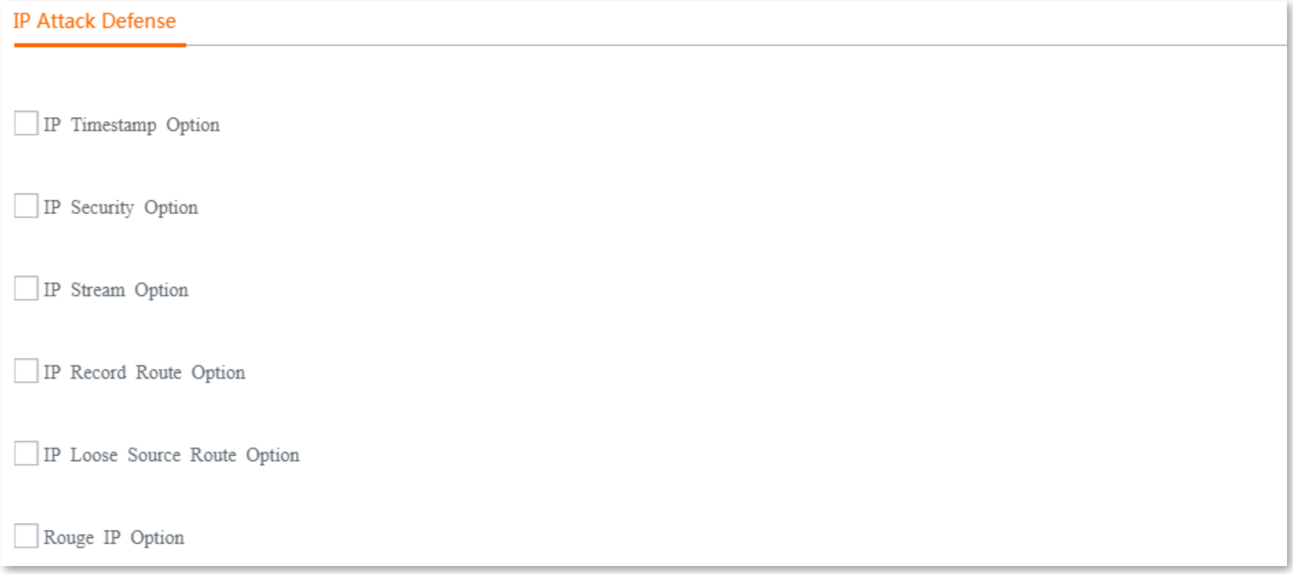
□ UDP Flood Threshold: 500 PPS

□ SYN Flood Threshold: 500 PPS

Parameter description

Parameter	Description
ICMP Flood Threshold	If ICMP request packets exceed the threshold within 1 second, the router suffers ICMP flood attack.
UDP Flood Threshold	If UDP request packets exceed the threshold within 1 second, the router suffers UDP flood attack.
SYN Flood Threshold	If SYN request packets exceed the threshold within 1 second, the router suffers SYN flood attack.

IP attack defense



IP Attack Defense

□ IP Timestamp Option

□ IP Security Option

□ IP Stream Option

□ IP Record Route Option

□ IP Loose Source Route Option

□ Rouge IP Option

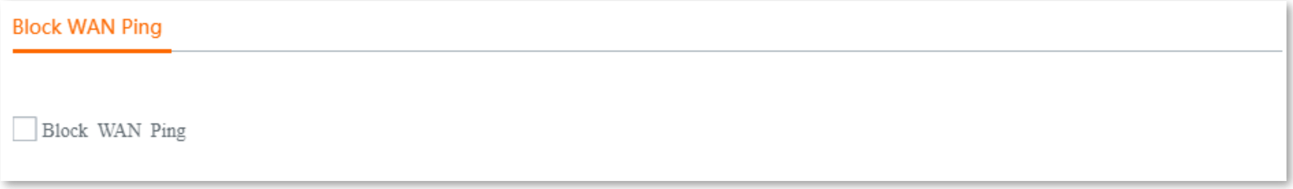
Parameter description

Parameter	Description
IP Timestamp Option	It is used to block IP packets that contain the Internet Timestamp option.
IP Secuirty Option	It is used to block IP packets that contain the Security option.
IP Stream Option	It is used to block IP packets that contain the Stream ID option.
IP Record Route Option	It is used to block IP packets that contain the Record Route option.
IP Loose Source Route Option	It is used to block IP packets that contain the Loose Source Route option.
Rouge IP Option	It is used to block IP packets that fail to pass integrity and correctness check.

NOTE

Packets meeting the above features may not be used for malicious attack. Therefore, enable attack defense as required.

Block WAN ping



Block WAN Ping

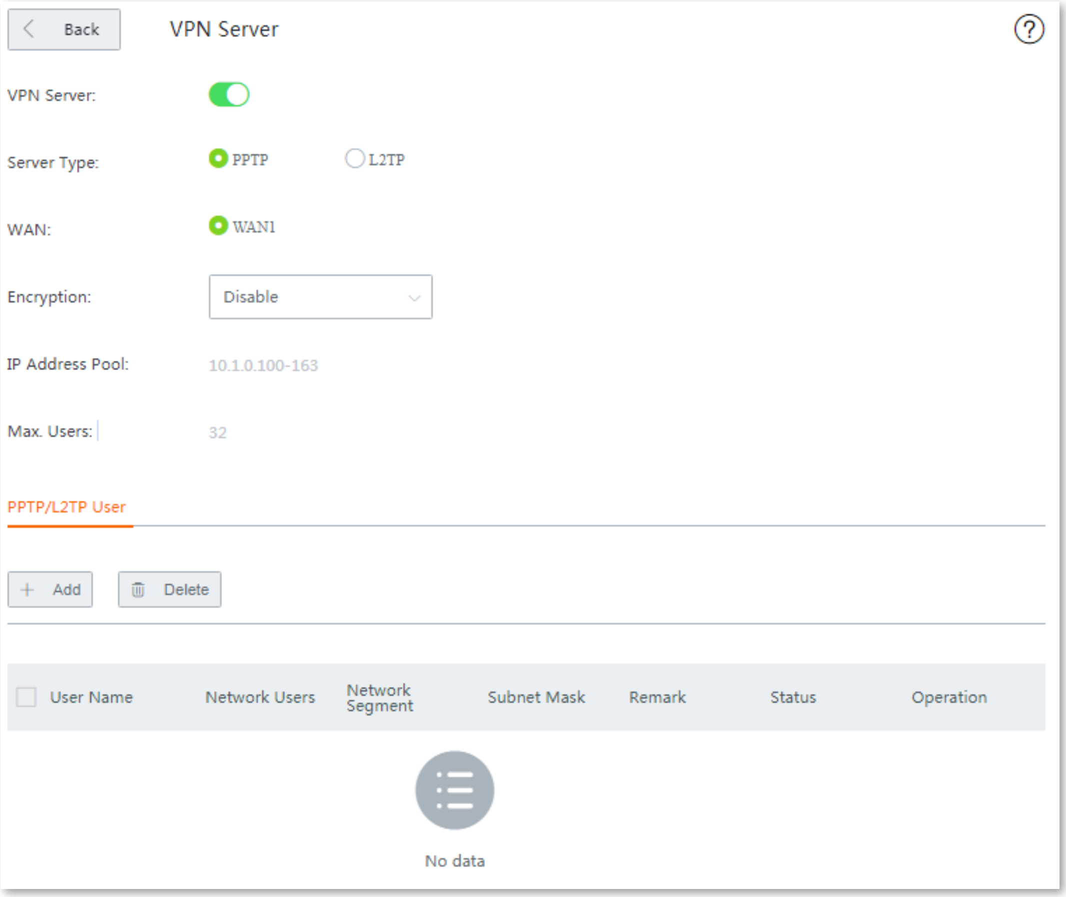
□ Block WAN Ping

With this function enabled, users cannot ping the WAN IP address of the router over the internet.

11.12 VPN server

11.12.1 Overview

The router supports PPTP server and L2TP server. To enter the configuration page, choose **More** > **VPN Server**. See the following figure.



VPN Server: ●

Server Type: ● PPTP ○ L2TP

WAN: ● WAN1

Encryption: Disable

IP Address Pool: 10.1.0.100-163

Max. Users: 32

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

No data

Parameter description

Parameter	Description
VPN Server	It is used to enable or disable the PPTP/L2TP VPN server function.
Server Type	It specifies the VPN server type that the router supports, including: - **PPTP:** The Point to Point Tunneling Protocol. If PPTP is selected, the peer VPN client should be set to PPTP client. - **L2TP:** Layer 2 Tunneling Protocol. If L2TP is selected, the peer VPN client should be set to L2TP client.
WAN	It specifies the WAN port of the router for setting up a VPN connection.
Encryption	It specifies whether to enable 128-bit data encryption. This parameter only appears when PPTP is selected. The value of this parameter must be consistent with that of the client. Otherwise, the client is unable to communicate with the server.
IP Address Pool	It specifies IP address range that the PPTP/L2TP clients can obtain from the VPN server to be connected.

Parameter	Description
Max. Users	It specifies the maximum number of VPN clients allowed to be connected to the PPTP/L2TP server. The value is fixed to **32**.
User Name	It specifies the user name and password used to dial in a PPTP/L2TP VPN connection.
Password	
Network Users	It specifies the password for the user name used to dial in PPTP/L2TP VPN connection.
Network Segment	It specifies whether a VPN client is a network. - **Yes**: The network segment and subnet mask of the VPN client are required. - **No**: The VPN client is a computer.
Subnet Mask	It specifies subnet mask of the LAN of a VPN client in case that the client is a network.
Remark	It specifies a short description about the corresponding account. You are recommended to add a remark to your VPN account for later management.
Status	It specifies whether or the corresponding rule is enabled.

11.12.2 Configuring the router as a PPTP/L2TP VPN server

TIP

To establish a VPN connection, the VPN server and VPN client should be configured consistently on **Client Type**, **WAN** and **Encryption**.

Step 1 Enable the PPTP/L2TP server function.

1. Choose **More** > **VPN Server**, enable **VPN Server**, and click **Save**.

2. Set the VPN server to **PPTP** or **L2TP** as required.

TIP

The peer VPN client should use the same type.

3. Select the egress WAN port of the tunnel between a PPTP/L2TP server and PPTP/L2TP clients.

TIP

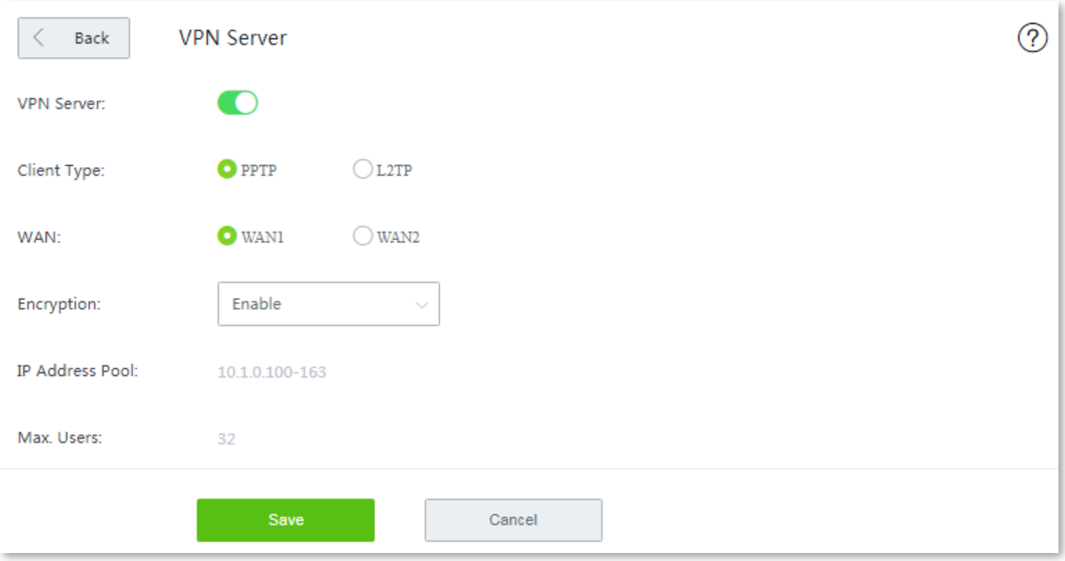
- If the egress WAN port you selected is set to a DMZ host, enable the port's **Filter VPN Port** first by navigating to **More** > **DMZ Host**.
- The IP address of the egress WAN port must be a public IP address. The following lists private IP address range of IPv4. IP addresses that are not in the range are public IP addresses.

  Category A: 10.0.0.0-10.255.255.255

  Category B: 172.16.0.0—172.31.255.255

  Category C: 192.168.0.0-192.168.255.255

4. Click **Save** to apply your settings.



Back VPN Server

VPN Server: ●

Client Type: ● PPTP ○ L2TP

WAN: ● WAN1 ○ WAN2

Encryption: Enable

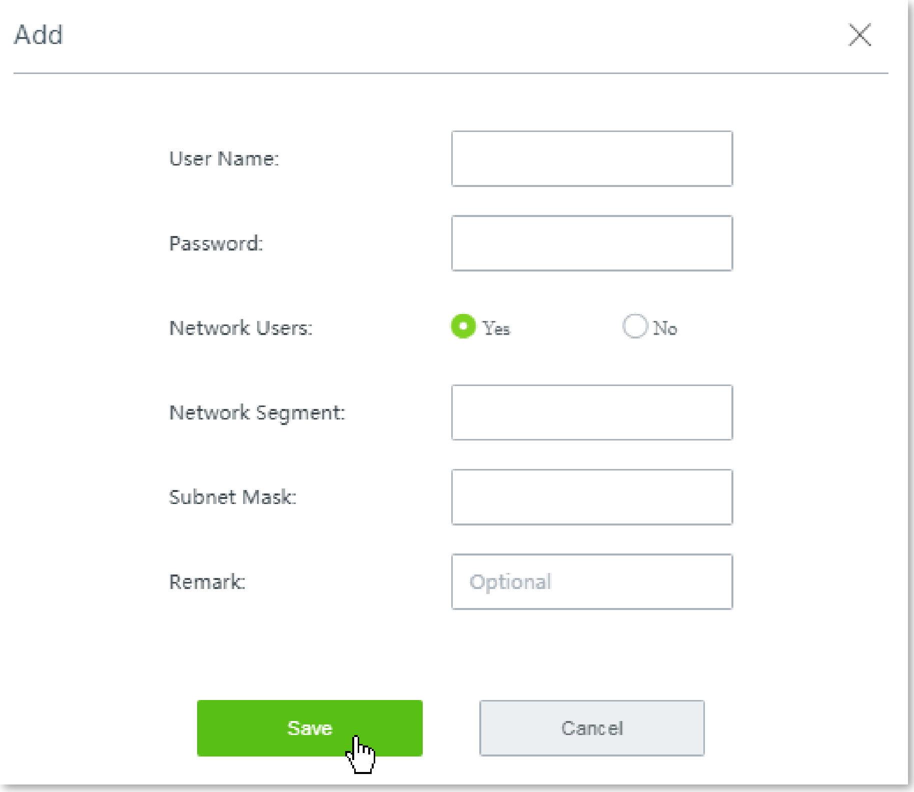
IP Address Pool: 10.1.0.100-163

Max. Users: 32

Save Cancel

Step 2 Add a PPTP/L2TP user.

1. Choose **More** > **VPN Server**, and go to the **PPTP/L2TP User** module.
2. Click **+Add**. The **Add** page appears.
3. Set required parameters, and click **Save**.



Add

User Name:

Password:

Network Users: ● Yes ○ No

Network Segment:

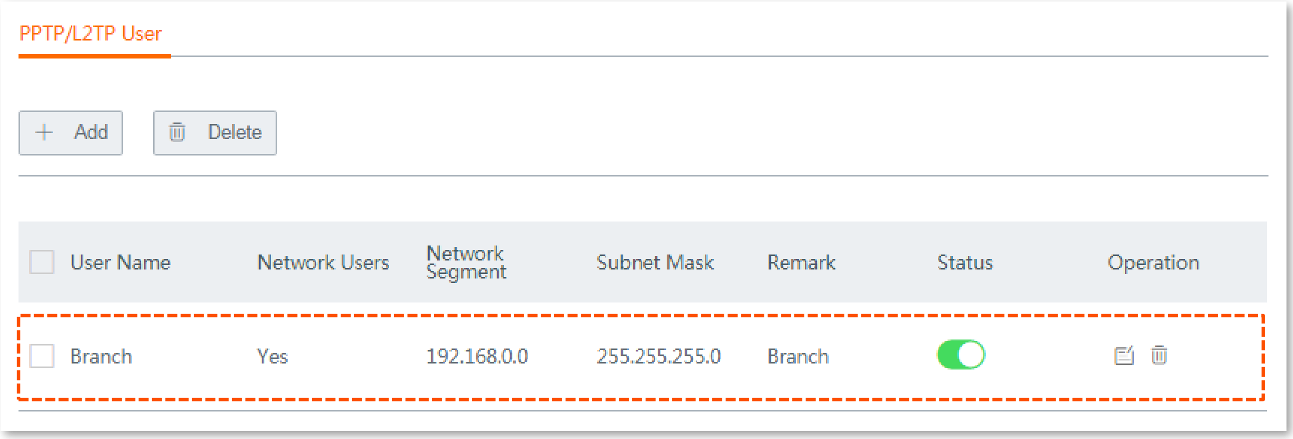
Subnet Mask:

Remark: Optional

Save Cancel

---- End

Added successfully. See the following figure:



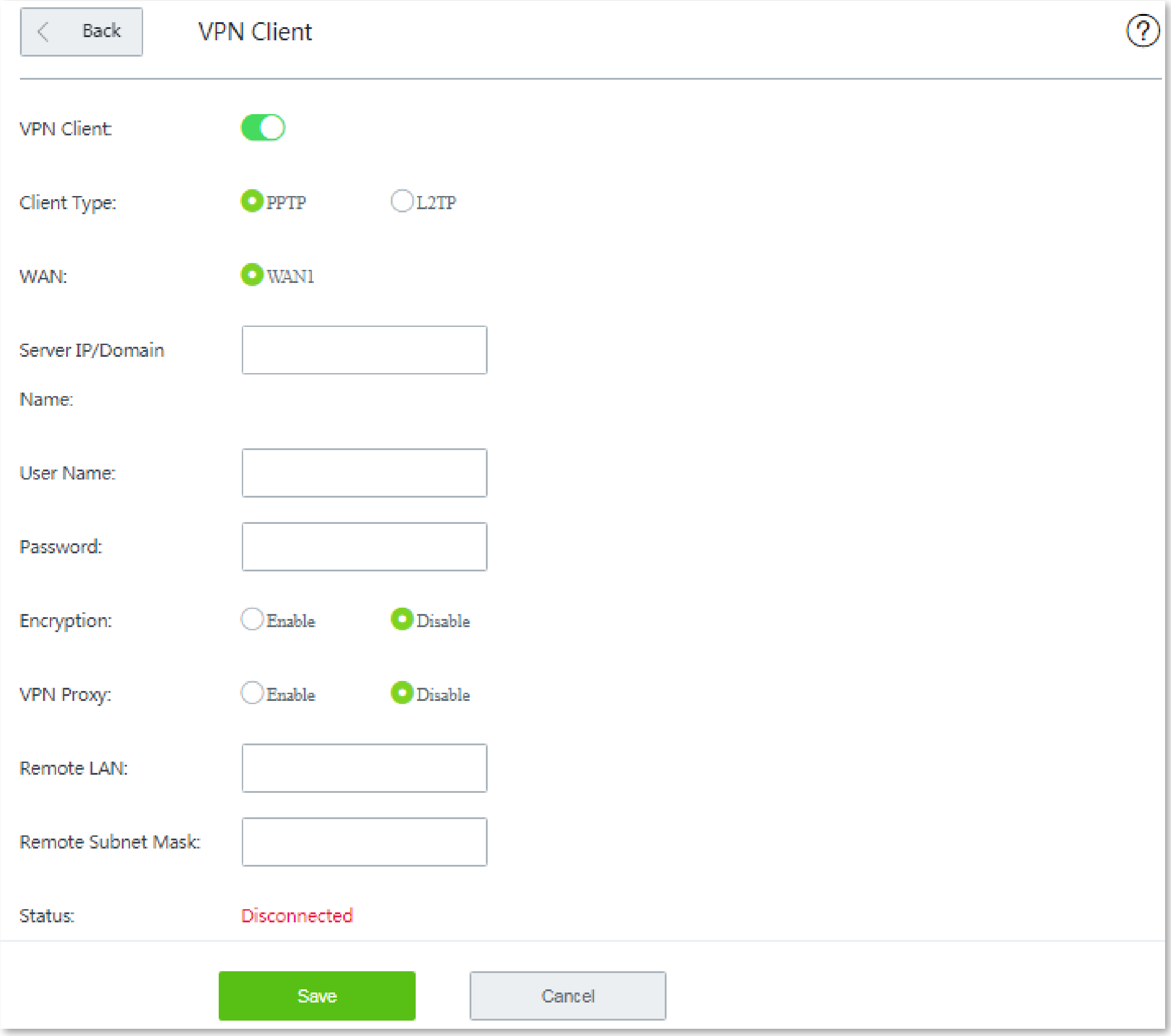
PPTP/L2TP User

□	User Name	Network Users	Network Segment	Subnet Mask	Remark	Status	Operation
□	Branch	Yes	192.168.0.0	255.255.255.0	Branch	●	

11.13 VPN client

11.13.1 Overview

To enter the configuration page, choose **More** > **VPN Client**. By default, this function is disabled. After you enable the function, the following page appears.



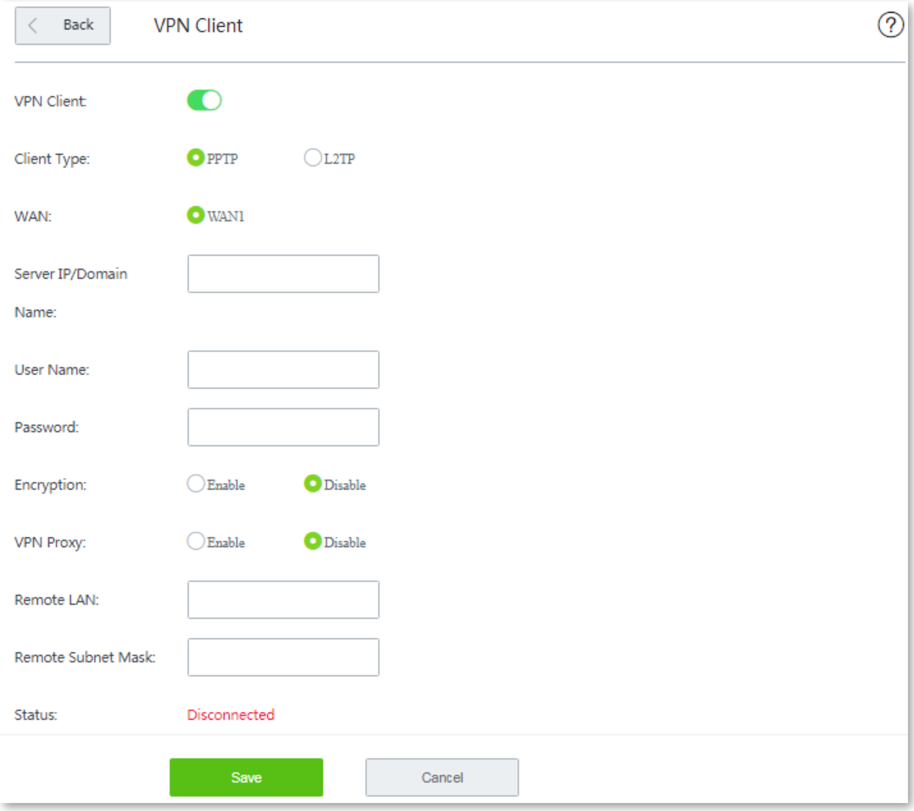
VPN Client:	●
Client Type:	● PPTP ○ L2TP
WAN:	● WAN1
Server IP/Domain Name:	
User Name:	
Password:	
Encryption:	○ Enable ● Disable
VPN Proxy:	○ Enable ● Disable
Remote LAN:	
Remote Subnet Mask:	
Status:	Disconnected

Parameter description

Parameter	Description
VPN Client	It is used to enable or disable the PPTP/L2TP VPN client function.
Client Type	It specifies the VPN client type that the router supports, including: - **PPTP:** The Point to Point Tunneling Protocol. If PPTP is selected, the peer VPN server should be set to PPTP client. - **L2TP:** Layer 2 Tunneling Protocol. If L2TP is selected, the peer VPN server should be set to L2TP client.
WAN	It specifies the WAN port of the router for setting up a VPN connection.
Server IP/Domain Name	It specifies the IP address or domain name of the peer VPN server.
User Name	It specifies the user name and password used to dial in a PPTP/L2TP VPN connection.
Password	
Encryption	It specifies whether to enable 128-bit data encryption. This parameter only appears when PPTP is selected. The value of this parameter must be consistent with that of the client. Otherwise, the client is unable to communicate with the server.
VPN Proxy	With this function enabled, clients access the internet through the peer router that has established a VPN 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 whether or the corresponding rule is enabled.

11.13.2 Configuring the router as a PPTP/L2TP VPN client

Step 1 Choose **More** > **VPN Client**, and enable the function. The following configuration page appears:



VPN Client: ●

Client Type: ● PPTP ○ L2TP

WAN: ● WAN1

Server IP/Domain Name:

User Name:

Password:

Encryption: ○ Enable ● Disable

VPN Proxy: ○ Enable ● Disable

Remote LAN:

Remote Subnet Mask:

Status: Disconnected

Step 2 Set required parameters.

TIP

- **Client Type**, **WAN**, and **Encryption** should be identical with its peer VPN server.
- Click ⓘ on the upper-right corner on the page to get the detailed explanation to the parameters here.

Step 3 Click **Save** to apply your settings.

---- End

11.14 IPSec

11.14.1 Overview

IPSec, abbreviated for Internet Protocol Security, is a protocol suite for transmitting data over the internet in a secure and encrypted manner. The following terms will be used in this document to describe IPSec configurations.

Encapsulation Mode

The router uses either Tunnel mode or Transport mode to encapsulate IP packets.

- Tunnel Mode: It is most commonly used between security gateways.
- Transport Mode: It is mainly used for end-to-end communications.

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).

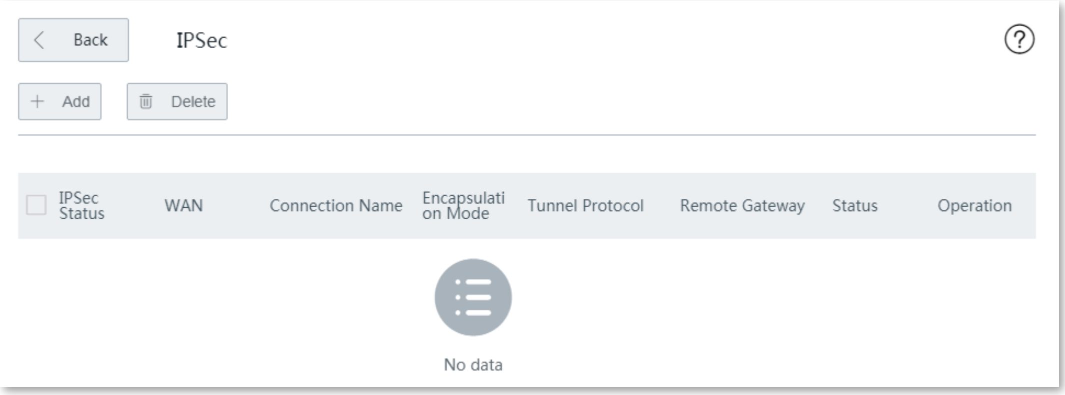
11.14.2 Creating IPSec connection

This section walks you through:

- Configuring Tunnel mode.
- Configuring transport mode.

Configuring Tunnel mode

Step 1 Choose **More** > **IPSec**. The following page appears.



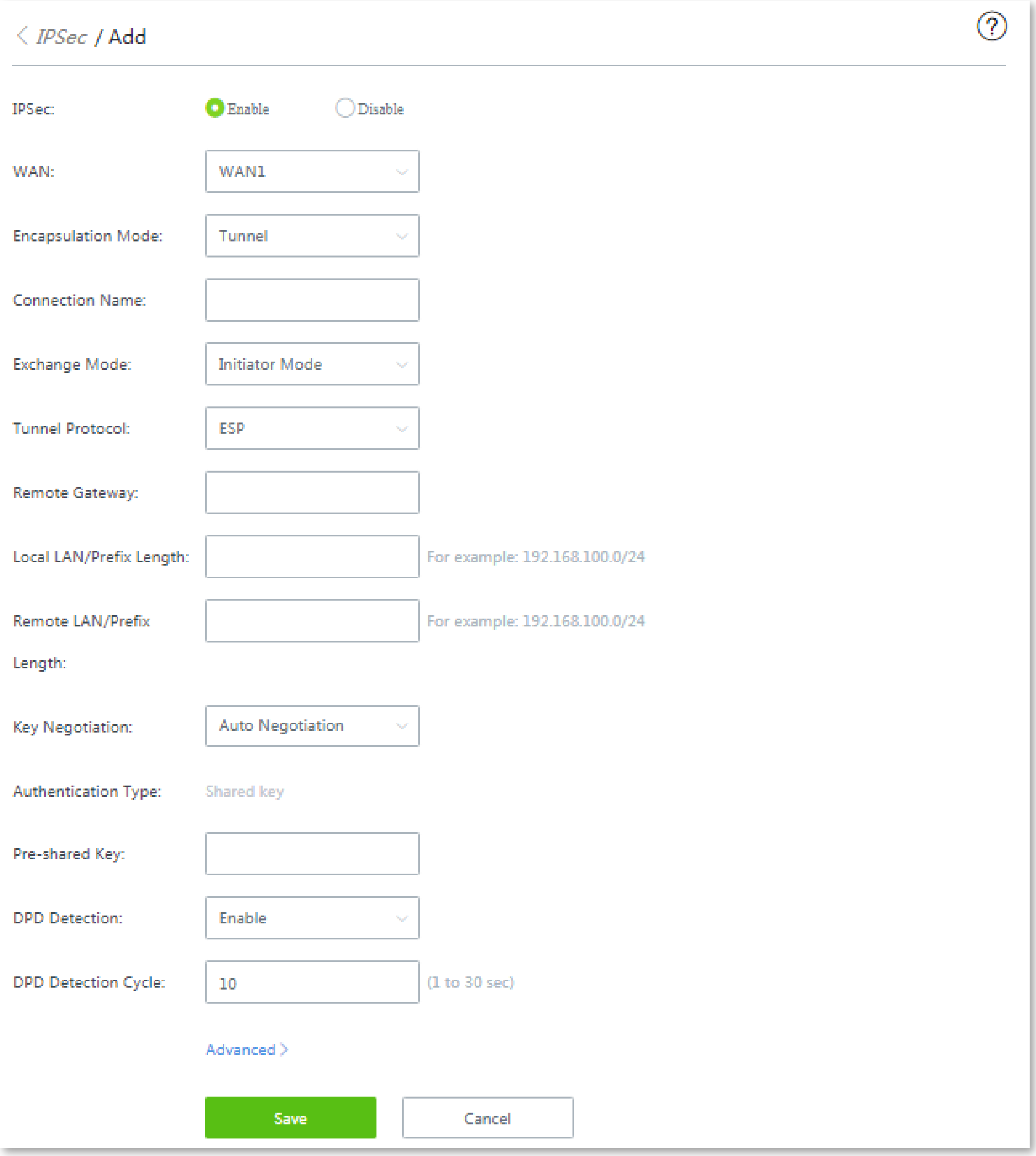
Back IPSec

+ Add   Delete

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

No data

Step 2 Click **+ Add**. The configuration page appears.



IPSec / Add

IPSec: ● Enable ○ Disable

WAN: WAN1

Encapsulation Mode: Tunnel

Connection Name:

Exchange Mode: Initiator Mode

Tunnel Protocol: ESP

Remote Gateway:

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

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

Key Negotiation: Auto Negotiation

Authentication Type: Shared key

Pre-shared Key:

DPD Detection: Enable

DPD Detection Cycle: 10 (1 to 30 sec)

Advanced >

Save   Cancel

Step 3 Tick **Enable** beside the **IPSec** option.

Step 4 Select the WAN port.

Step 5 Select **Tunnel** from the **Encapsulation Mode** drop-down list menu.

Step 6 Set required parameters, and click **Save** to apply your settings.

---- End

Parameter description

Parameter	Description
IPSec	It is used to enable or disable the IPSec function.
WAN	It specifies the WAN port of the IPSec connection on this end. The remote gateway of the IPSec peer should be the IP address of the WAN port you specified here.
Encapsulation Mode	The router uses either of the following to encapsulate IP packets. - **Tunnel Mode**: It is most commonly used between security gateways. - **Transport Mode**: It is mainly used for end-to-end communications.
Connection Name	It specifies the name of the IPSec tunnel.
Exchange Mode	It specifies whether the device is an imitator that starts the VPN request, or a responder that answers the request. - **Initiator mode**: It indicates the device that starts the VPN attempt. - **Responder mode**: It indicates the device that answers the Initiator’s request. NOTE IPSec peers cannot be set to **Responder** mode at the time. Otherwise, IPSec connection fails.
Tunnel Protocol	The router supports ESP and AH protocols, as well as the mix of the two. - **ESP**: It indicates the Encapsulating Security Payload 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. This compatible protocol is widely used in gateway products. - **AH**: It indicates the Authentication Header protocol used for verifying data integrity. If a packet is tampered during transmission, the receiver discards it during data integrity verification. - **AH+ESP**: It indicates that the router uses both AH and ESP protocols.
Remote Gateway	IP address or domain name of the specified WAN port of the IPSec peer.
Local LAN/Prefix Length	It specifies the network segment and subnet mask of LAN network of this device. For example: Assume that the LAN IP address and subnet mask of this device are 192.168.0.252 and 255.255.255.0 respectively, you can enter 192.168.0.0/24.
Remote LAN/Prefix Length	It specifies the LAN network segment and subnet mask of the IPSec peer. If the remote gateway is a single host, enter its IP address and subnet mask, such as 192.168.100.1/32.
Key Negotiation	The key negotiation method to establish an IPSec tunnel. - **Auto** (default): It indicates that an SA is set up, maintained, and deleted automatically using IKE (Internet Key Exchange). This reduces configuration complexity and simplifies IPSec usage and management. Such an SA (Security Association) has a life cycle and is updated regularly, leading to higher security. - **Manual**: It indicates that an SA is set up by manually specifying encryption and authentication algorithms and keys. Such an SA does not have a life cycle, and therefore it remains valid unless being manually deleted, leading to a security risks. Generally, this mode is used only for commissioning.

Key negotiation: Auto Negotiation

To protect information confidentiality when using auto negotiation, IKE is in place to negotiate keys for secure communication between IPSec peers. The IKE protocol is a hybrid of three other protocols:

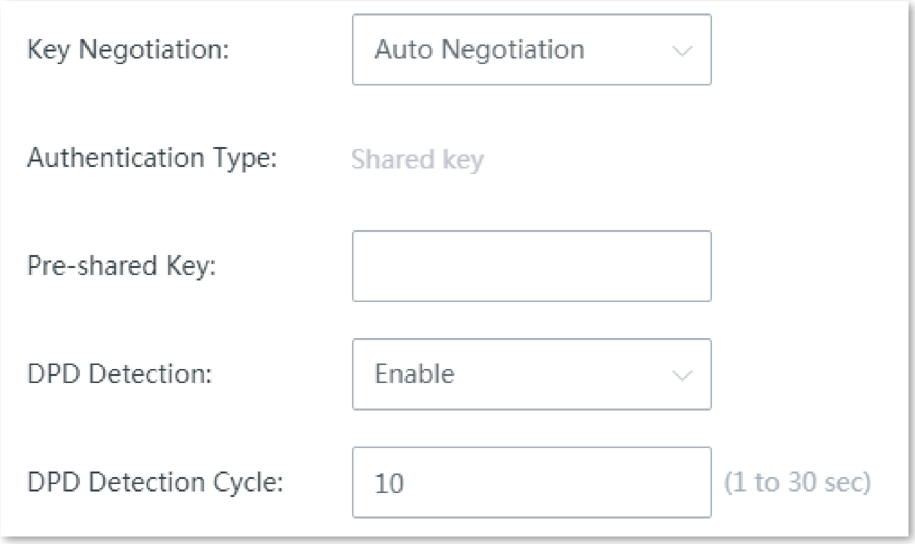
- **ISAKMP**: Internet Security Association and Key Management Protocol. It defines the procedures for authenticating a communicating peer, creation and management of Security Associations, key generation techniques, and threat mitigation.
- **Oakley**: Oakley Key Determination Protocol. It defines the specific key negotiation mechanism.
- **SKEME**: A secure and versatile key exchange protocol for key management over internet is presented.

IKE negotiation can be broke down into two periods.

Period 1: Period 1 is used to negotiate the parameters and key required to establish IKE Security Association (SA) between two IPSec peers.

Period 2: Period 2 then uses the Security Associations (SAs) negotiated in Period 1 to protect future IKE communication.

When **Auto Negotiation** is selected, the following page appears.



Key Negotiation: Auto Negotiation

Authentication Type: Shared key

Pre-shared Key:

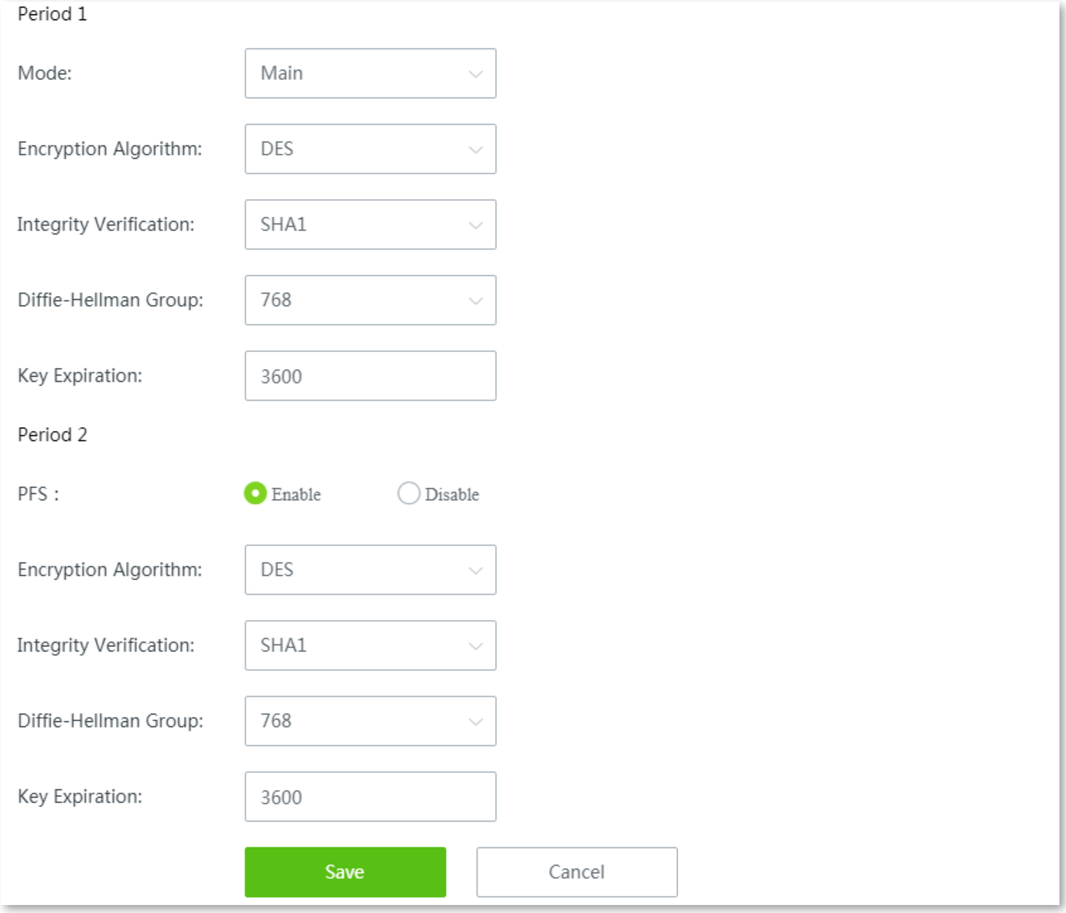
DPD Detection: Enable

DPD Detection Cycle: 10 (1 to 30 sec)

Parameter description

Parameter	Description
Authentication Type	The router supports IPSec authentication with **Shared Key**. Only authorized users can access the private network.
Pre-shared Key	It is used to encrypt Phase1 authentication information. A pre-shared key contains a maximum of 128 characters. This must be the same at both ends.
DPD Detection	Dead Peer Detection. It is used to detect the liveliness of its IIKE peer.
DPD Detection Cycle	It is used to configure the router to detect the liveliness of its IKE peer at regular intervals.

Clicking **Advanced** loads the following configuration area:



Period 1

Mode: Main

Encryption Algorithm: DES

Integrity Verification: SHA1

Diffie-Hellman Group: 768

Key Expiration: 3600

Period 2

PFS : ● Enable ○ Disable

Encryption Algorithm: DES

Integrity Verification: SHA1

Diffie-Hellman Group: 768

Key Expiration: 3600

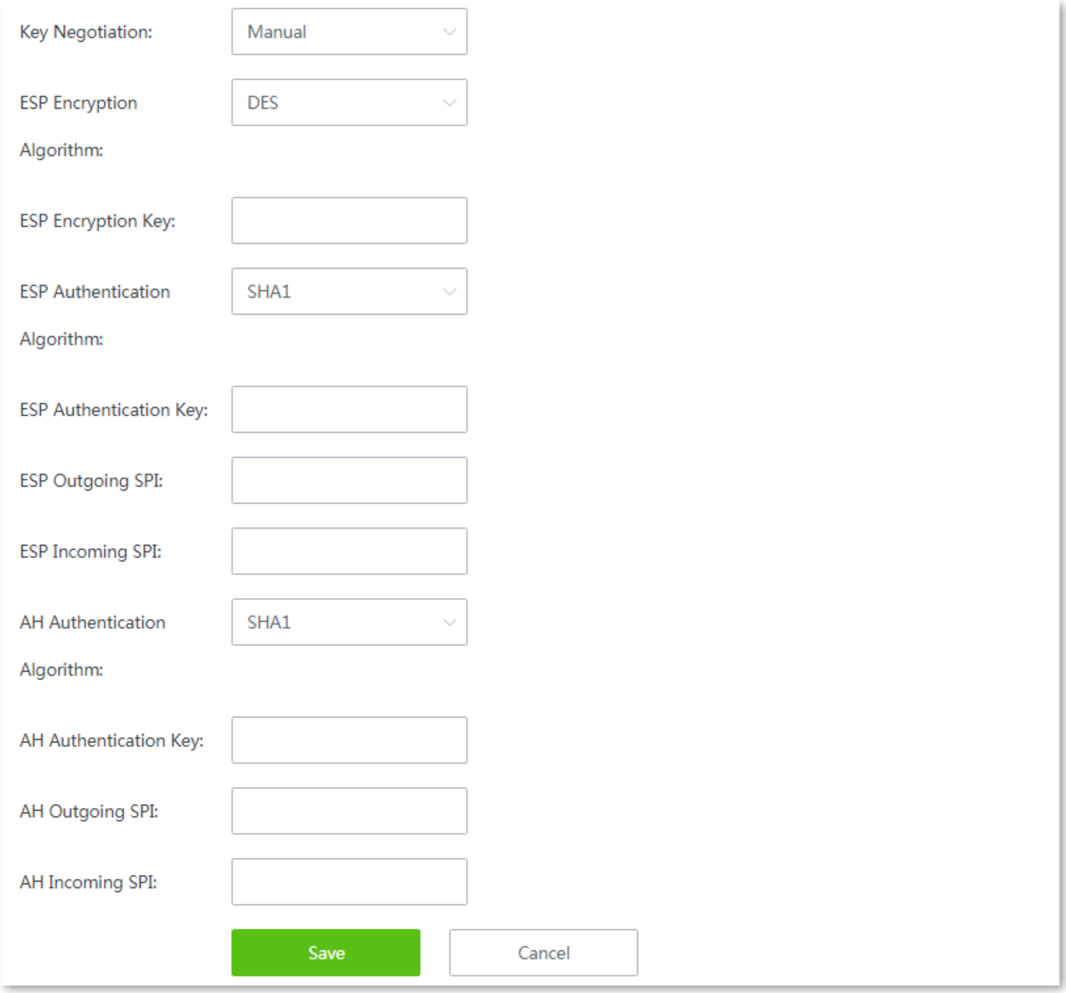
Parameter description

Parameter	Description
Period 1/2	It specifies the two periods that the IKE SA (IKE Security Association that is broken down. NOTE The router does not support IKEV2.0.
Mode	It specifies the mode that IPSec ends use to exchange information in Period 1. - **Main**: This mode requires double messages to be exchanged in Period 1, which provides higher security but lower efficiency. - **Aggressive**: This mode requires half of messages to be exchanged in Period 1, which provide lower security but higher efficiency.
Encryption Algorithm	The router supports the following algorithms: - **DES** (Data Encryption Standard): A 56-bit key is used to encrypt 64-bit data. The last 8 bits of the 64-bit data are used for parity check. - **3DES**: Three 56-bit keys are used for encryption. - **AES** (Advanced Encryption Standard): AES 128/192/256 indicates that 128/192/256-bit keys are used for encryption respectively.
Integrity Verification	The router supports the following algorithms to check key integrity: - **MD5** (Message Digest Algorithm): A 128-bit message digest is generated to prevent message tampering. - **SHA1** (Secure Hash Algorithm): A 160-bit message digest is generated to prevent

Parameter	Description
	message tampering, leading to higher security than MD5.
Diffle-Hellman Group	Group information for the Diffie-Hellman algorithm for generating a session key used to encrypt an IKE tunnel. The information should be the same as that of the remote gateway.
Key Expiration	It specifies the life cycle of IKE SA. The default time is 3600 seconds. The minimum time is 600 seconds. When 540 seconds are left, IKE SA will be negotiated again.
PFS	It indicates Perfect Forward Secrecy that improves security by forcing a new Diffie-Hellman exchange whenever key expires.

■ Key negotiation: Manual

The following configuration area appears in case that the **Tunnel Protocol** is set to **AH+ESP**.



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

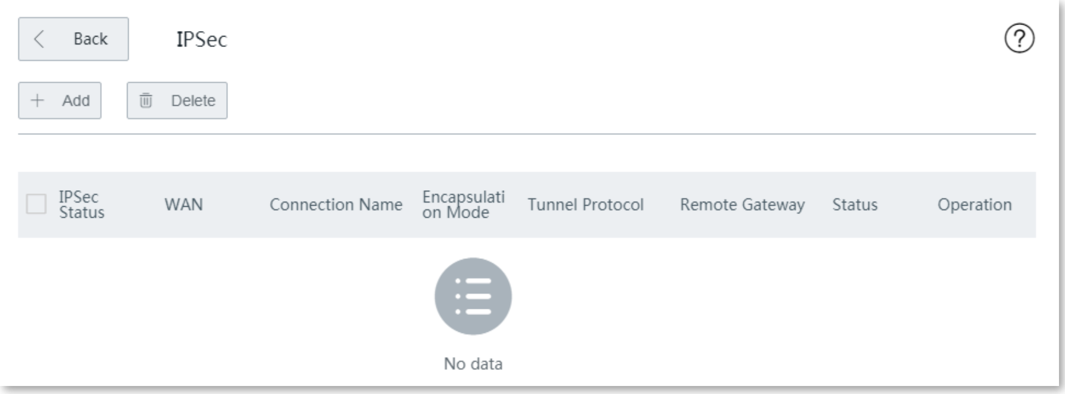
Parameter description

Parameter	Description
ESP Encryption Algorithm	The router supports the following ESP encryption algorithms: - **3DES** (default): Three 56-bit keys are used for encryption. A key of 24 ASCII characters or 48 hexadecimal characters is required. - **DES**: A 56-bit key is used to encrypt 64-bit data. The last 8 bits of the 64-bit data are used for parity check. A key of 8 ASCII characters or 16 hexadecimal characters is required. - **AES-128:** A 128-bit key is used for encryption. A key of 16 ASCII characters or 32 hexadecimal characters is required.

Parameter	Description
	- **AES-192**: A 192-bit key is used for encryption. A key of 24 ASCII characters or 48 hexadecimal characters is required. - **AES-256**: A 256-bit key is used for encryption. A key of 32 ASCII characters or 64 hexadecimal characters is required.
ESP Encryption Key	This parameter should be the same for IPSec peers.
ESP Authentication Algorithm	Optional service to ensure the integrity of data packets. - **MD5**: A 128-bit message digest is generated to prevent message tampering. The authentication key must be 16 ASCII characters or 32 hexadecimal characters. - **SHA1**: A 160-bit message digest is generated to prevent message tampering. The authentication key must be 20 ASCII characters or 40 hexadecimal characters.
ESP Authentication Key	This parameter should be the same for IPSec peers.
ESP Outgoing SPI	SPI is used to identify an IPSec SA with the IP address and security protocol of the remote gateway. This parameter should be the same for IPSec peers.
ESP Incoming SPI	This parameter should be the same for IPSec peers.
AH Authentication Algorithm	Optional service to ensure the integrity of data packets. - **MD5**: A 128-bit message digest is generated to prevent message tampering. The authentication key must be 16 ASCII characters or 32 hexadecimal characters. - **SHA1**: A 160-bit message digest is generated to prevent message tampering. The authentication key must be 20 ASCII characters or 40 hexadecimal characters.
AH Authentication Key	This parameter should be the same for IPSec peers.
AH Outgoing SPI	This parameter should be the same for IPSec peers.
AH Incoming SPI	This parameter should be the same for IPSec peers.

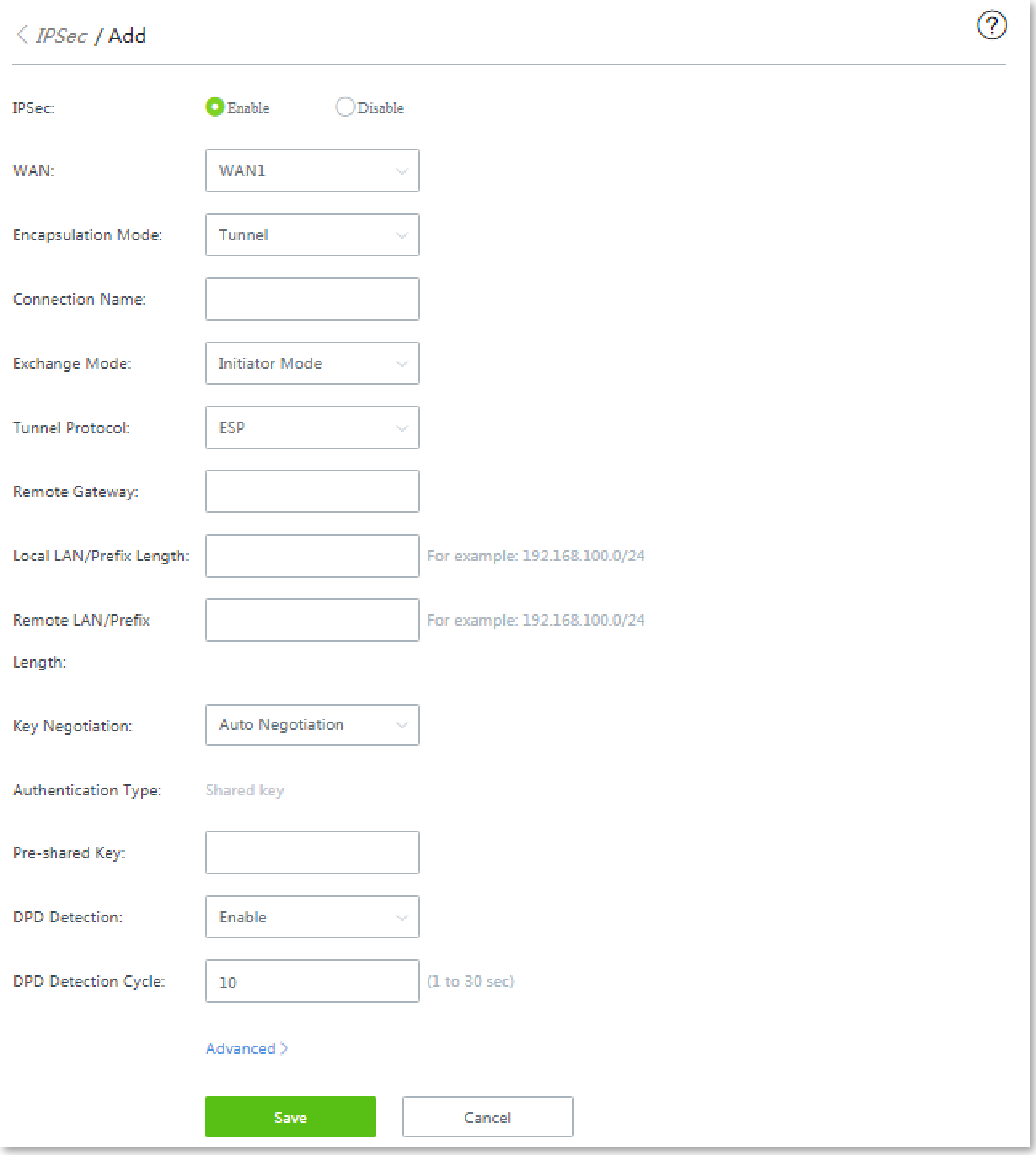
Configuring transport mode

Step 1 Choose **More** > **IPSec**. The following page appears.



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

Step 2 Click **+ Add**. The configuration page appears.



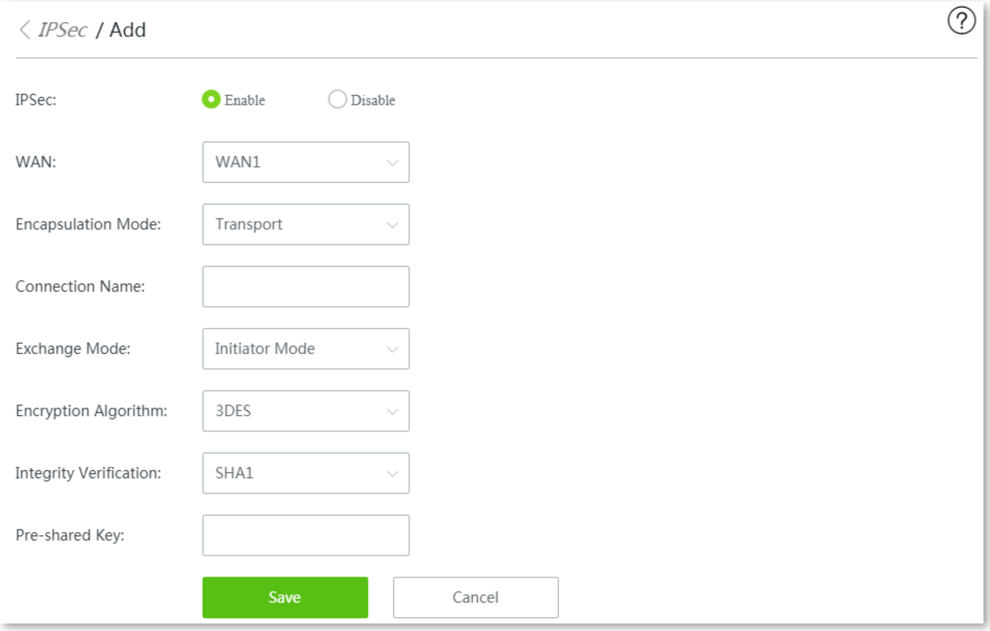
< IPSec / Add

IPSec:	● Enable ○ Disable	
WAN:	WAN1	
Encapsulation Mode:	Tunnel	
Connection Name:		
Exchange Mode:	Initiator Mode	
Tunnel Protocol:	ESP	
Remote Gateway:		
Local LAN/Prefix Length:		For example: 192.168.100.0/24
Remote LAN/Prefix Length:		For example: 192.168.100.0/24
Key Negotiation:	Auto Negotiation	
Authentication Type:	Shared key	
Pre-shared Key:		
DPD Detection:	Enable	
DPD Detection Cycle:	10	(1 to 30 sec)

Step 3 Tick **Enable** beside the IPSec option.

Step 4 Select the WAN port.

Step 5 Select **Transport** from the **Encapsulation Mode** drop-down list menu. The following page appears.



IPSec / Add

IPSec:	● Enable ○ Disable
WAN:	WAN1
Encapsulation Mode:	Transport
Connection Name:	
Exchange Mode:	Initiator Mode
Encryption Algorithm:	3DES
Integrity Verification:	SHA1
Pre-shared Key:	

Step 6 Set required parameters, and click **Save** to apply your settings.

---- End

Parameter description

Parameter	Description
IPSec	It is used to enable or disable 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.
Encapsulation Mode	The router supports two modes: - **Tunnel Mode**: It is most commonly used between gateways. - **Transport Mode**: It is mainly used for end-to-end communications.
Connection Name	It specifies the name of the IPSec tunnel.
Exchange Mode	It specifies whether the device is an imitator that starts the VPN request, or a responder that answers the request. - **Initiator mode**: It specifies the device that starts the VPN attempt. - **Responder mode**: It specifies the device that answers the Initiator’s request.
Encryption Algorithm	It specifies the IKE session encryption algorithm. - **DES** (Data Encryption Standard): A 56-bit key is used to encrypt 64-bit data. The last 8 bits of the 64-bit data are used for parity check. - **3DES**: Three 56-bit keys are used for encryption. - **AES** (Advanced Encryption Standard): AES 128/192/256 indicates that 128/192/256-bit keys are used for encryption respectively.
Integrity Verification	The router supports the following algorithms to check key integrity: - **MD5** (Message Digest Algorithm): A 128-bit message digest is generated to prevent message tampering. - **SHA1** (Secure Hash Algorithm): A 160-bit message digest is generated to prevent

Parameter	Description
	message tampering, leading to higher security than MD5.
Pre-shared Key	This must be the same at both ends.

11.15 Example of configuring VPN conenctions

11.15.1 Example of configuring a PPTP/L2TP VPN

Networking requirement

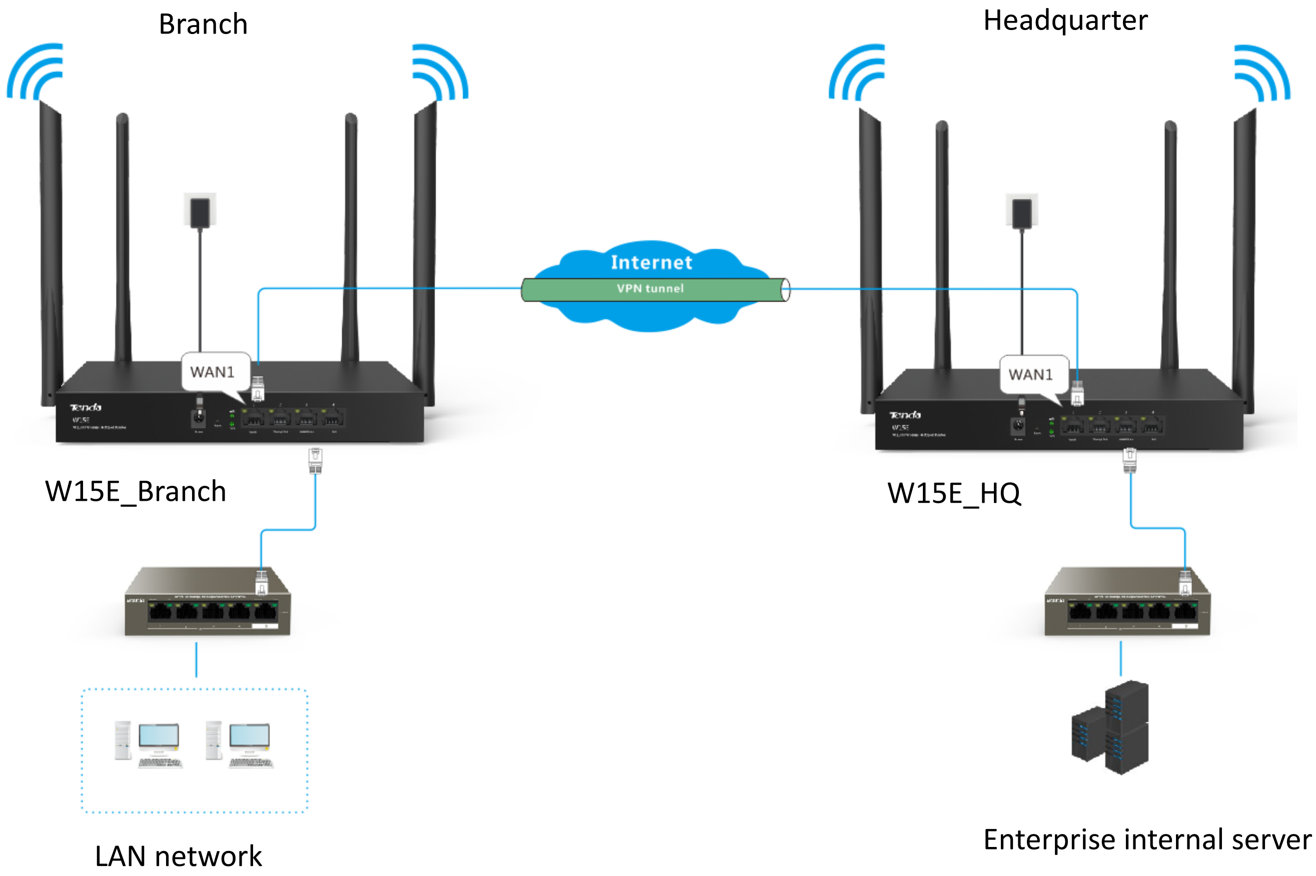
An enterprise has used W15E to set up a LAN and access the internet. Branch employees need to access the HQ's internal resources through the internet, such as internal data, OA, ERP, CRM, project management systems.

Solutions

PPTP/L2TP VPNs of W15E can address this requirement.

The following uses PPTP to illustrate the setup procedure. Set up the L2TP VPN in the same way.

Network topology



Configuration description

Step	Task	Description
1	Configure **W15E_HQ** as a VPN server	Enable VPN server on the router, configure **Client Type**, specify the egress **WAN** port, and enable the **Encryption**.
2	Configure a PPTP/L2TP user on **W15E_HQ**	Set a user name and password for connecting to VPN. Clarify whether or not the client is a network user. If yes, enter a proper network segment and subnet mask.
3	Configuring **W15E_Branch** as a VPN client	Enable VPN client on the router, set related parameters by following the on-screen instructions.

4	Verify the connectivity between the VPN server and VPN client	Check if VPN connection is established and access HQ LAN resources using VPN.

Configuration procedure

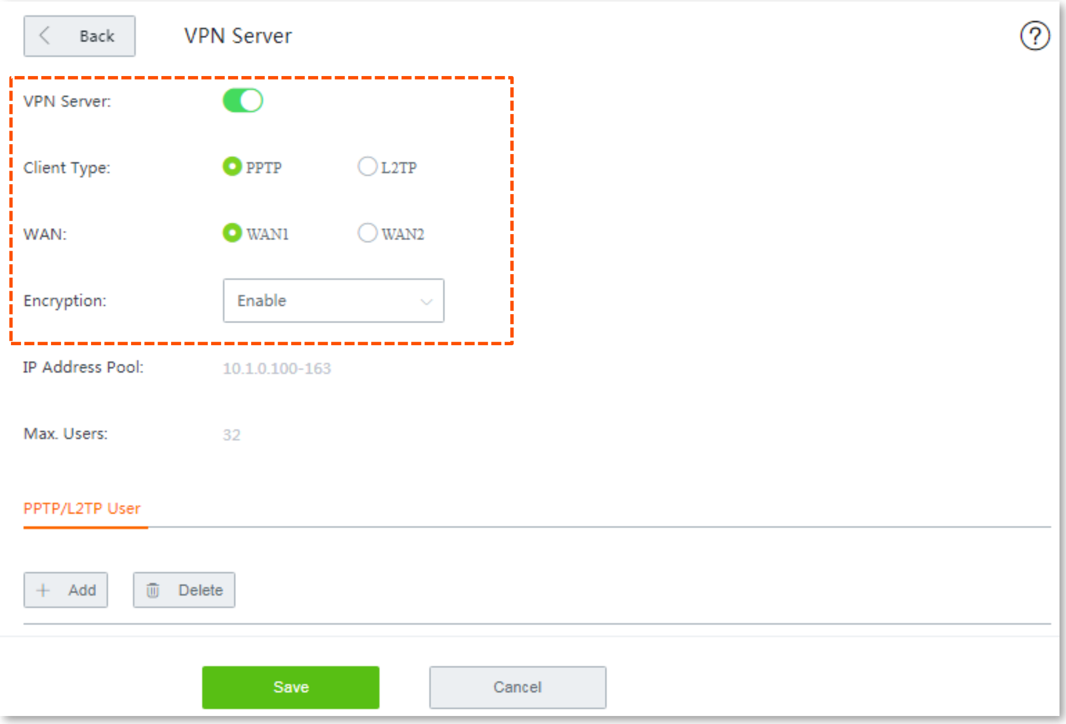
Step 1 Configure **W15E_HQ** as a VPN server.

1. On W15E_HQ, choose **More** > **VPN Server**, enable this function, and click **Save**.
2. Set **Client Type** to **PPTP**.
3. Set the egress port of the VPN server for setting up a tunnel with the VPN client, which is **WAN1** in this example.
4. Set **Encryption** to **Enable**.

TIP

The peer VPN client should use the same configuration.

5. Click **Save**.



VPN Server: ●

Client Type: ● PPTP ○ L2TP

WAN: ● WAN1 ○ WAN2

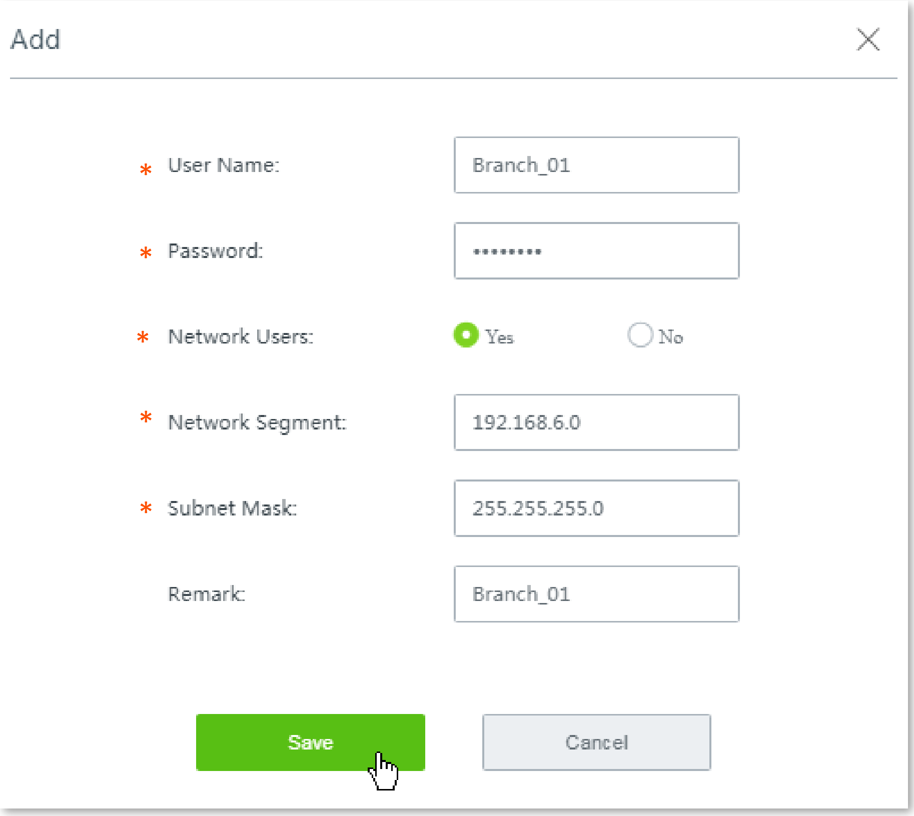
Encryption: Enable

IP Address Pool: 10.1.0.100-163

Max. Users: 32

Step 2 Configure a PPTP/L2TP user on W15E_HQ.

1. On W15E_HQ, choose **More** > **VPN Server**, and move to the **PPTP/L2TP User** module.
2. Click +Add. The **Add** configuration window appears.
3. Set the required parameters. The following shows the examples:


Add

* User Name: Branch_01

* Password: ••••••••

* Network Users: ● Yes ○ No

* Network Segment: 192.168.6.0

* Subnet Mask: 255.255.255.0

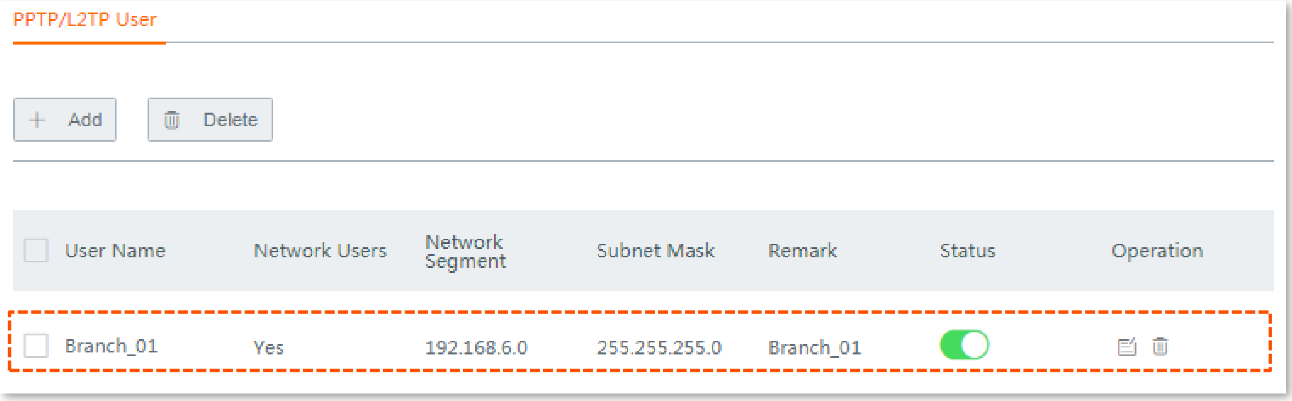
Remark: Branch_01

TIP

- Parameters indicated with * are mandatory.
- **Remark** is optional. However, you are recommended to add a brief description of the rule for convenient management later, which is **Branch_01** in this example.

4. Click **Save**.

Added successfully. See the following figure:



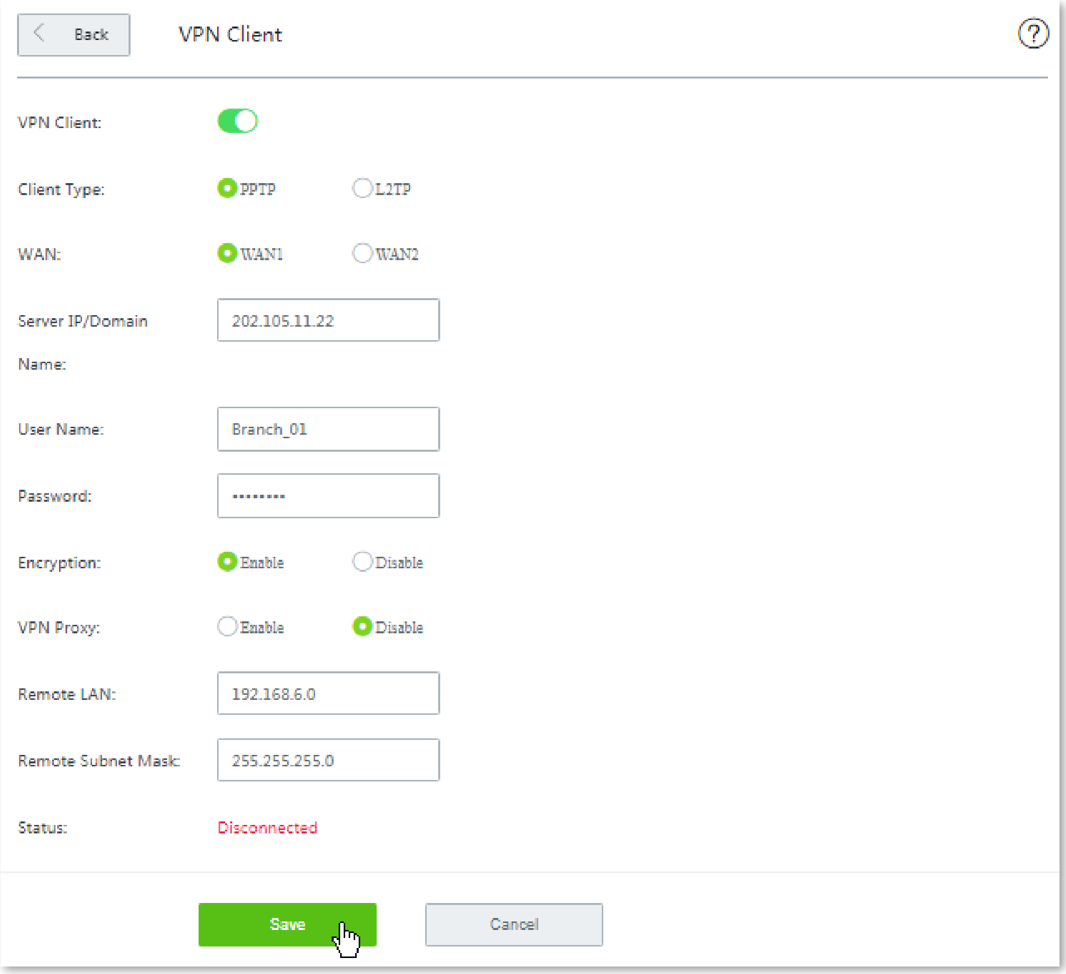
□ User Name	Network Users	Network Segment	Subnet Mask	Remark	Status	Operation
□ Branch_01	Yes	192.168.6.0	255.255.255.0	Branch_01	●	

Step 3 Configure **W15E_Branch** as a VPN client.

1. On W15E_Branch, choose **More** > **VPN Client,** and enable this function.
2. Set required parameters. The parameters should keep consistent with the VPN server.
   - Client Type: **PPTP Client**
   - WAN: **WAN1**
   - Server IP Address/Domain Name: **202.105.11.22**

- User name/Password: **Branch_HQ/12345678**
- Remote LAN: **192.168.6.0**
- Remote Subnet Mask: **255.255.255.0**

3. Disable **VPN Proxy**.
4. Click **Save** to apply your settings.



VPN Client: ●

Client Type: ● PPTP ○ L2TP

WAN: ● WAN1 ○ WAN2

Server IP/Domain Name: 202.105.11.22

User Name: Branch_01

Password: ••••••••

Encryption: ● Enable ○ Disable

VPN Proxy: ○ Enable ● Disable

Remote LAN: 192.168.6.0

Remote Subnet Mask: 255.255.255.0

Status: Disconnected

---- End

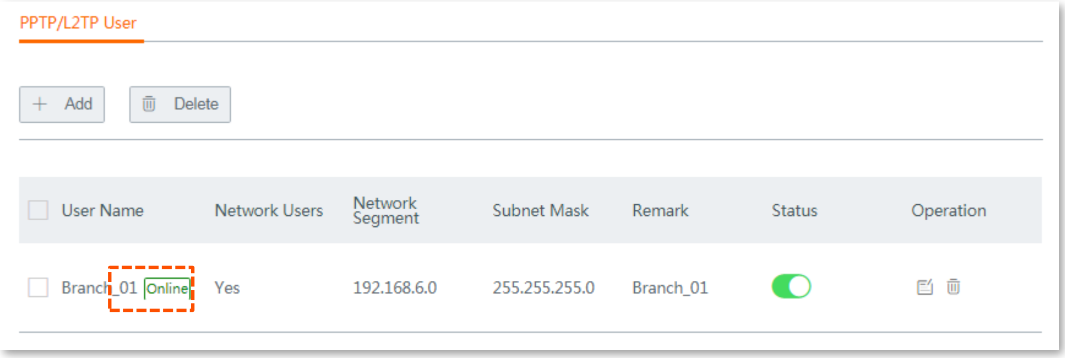
Verification

Step 1 Check if the VPN connection is established.

There are two methods for checking whether or not the VPN connection is established.

- **Method 1:**

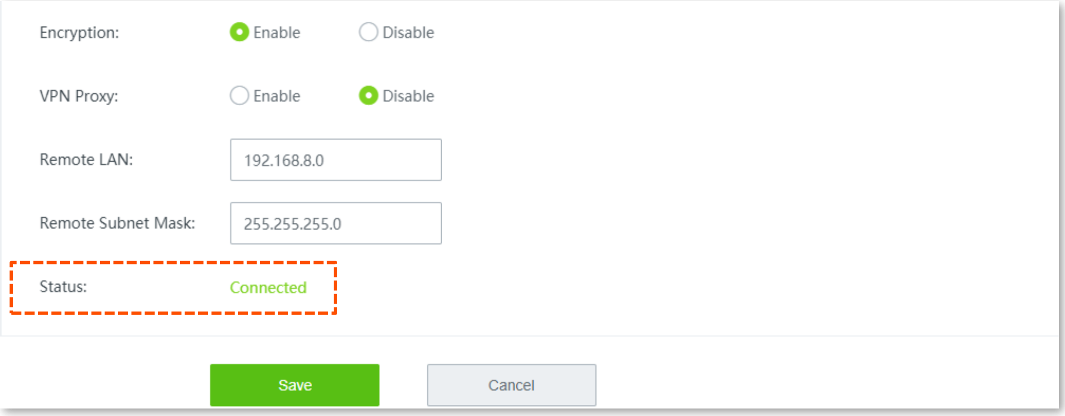
Log in to the web UI of **W15E_HQ**, choose **More** > **VPN Sever**, and move to the **PPTP/L2TP User** module, there is a squared tip **Online** next to the user name, indicating the VPN connection is established.



□	User Name	Network Users	Network Segment	Subnet Mask	Remark	Status	Operation
□	Branch_01 Online	Yes	192.168.6.0	255.255.255.0	Branch_01	●	

- **Method 2:**

Log in to the web UI of **W15E_Bracnh**, choose **More** > **VPN Client**, the **Status** changes into **Connected**, indicating the VPN connection is established.



Encryption: ● Enable ○ Disable

VPN Proxy: ○ Enable ● Disable

Remote LAN: 192.168.8.0

Remote Subnet Mask: 255.255.255.0

Status: Connected

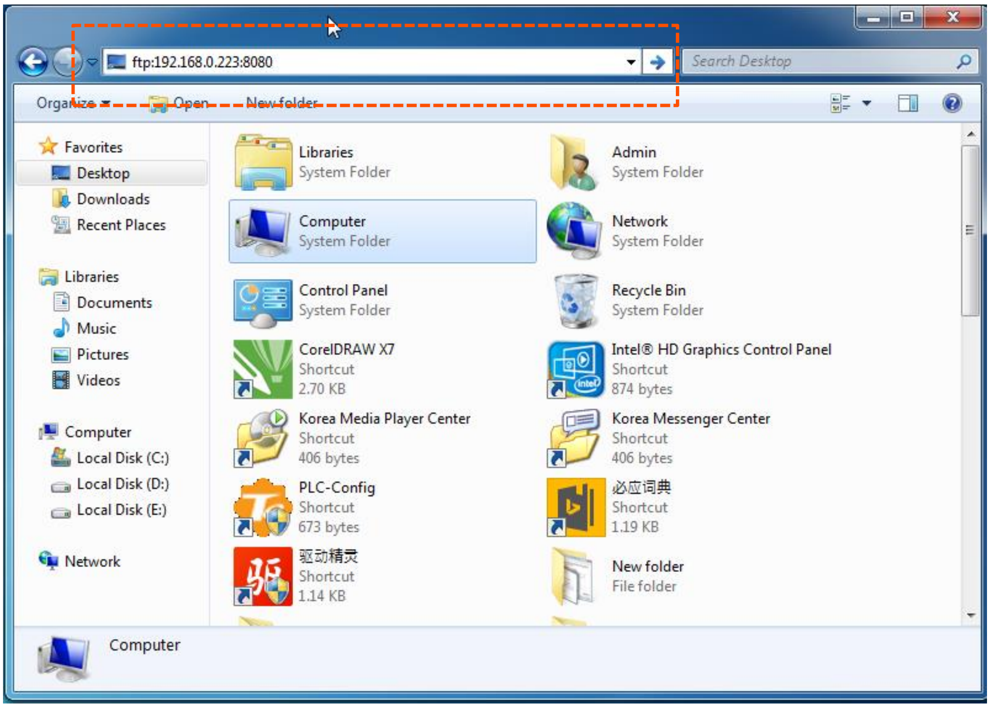
Step 2 Access HQ LAN resources remotely.

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

- IP address of the FTP server: **192.168.0.223**
- Server port: **8080**
- Login username and password: **admin/admin**

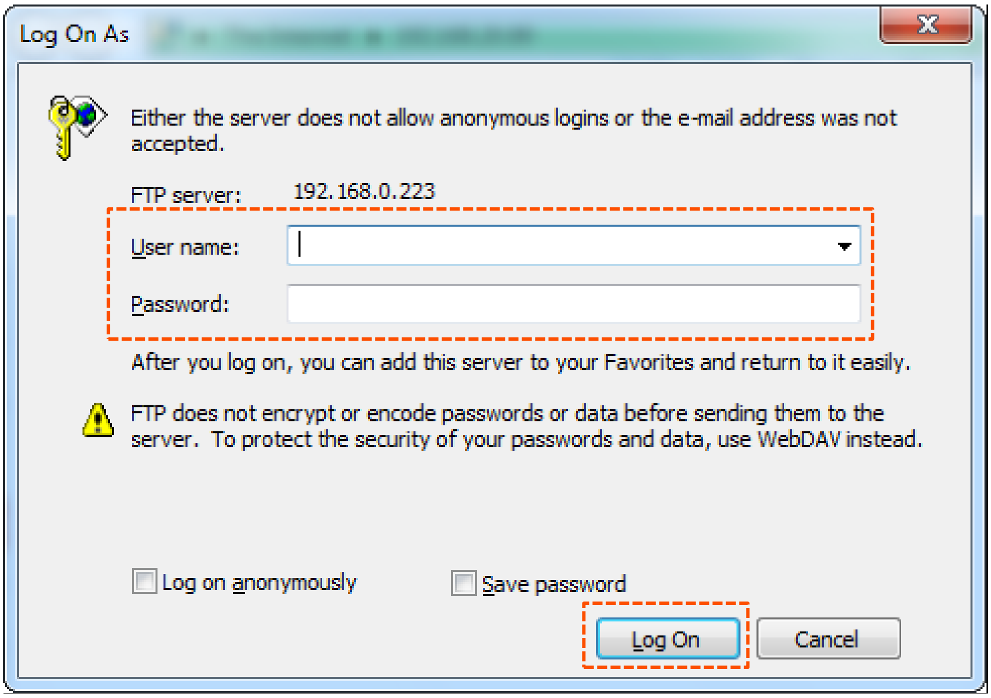
The procedures for employees at the branch access the HQ project data are as follow:

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



ftp:192.168.0.223:8080

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



Log On As

Either the server does not allow anonymous logins or the e-mail address was not accepted.

FTP server: 192.168.0.223

User name:

Password:

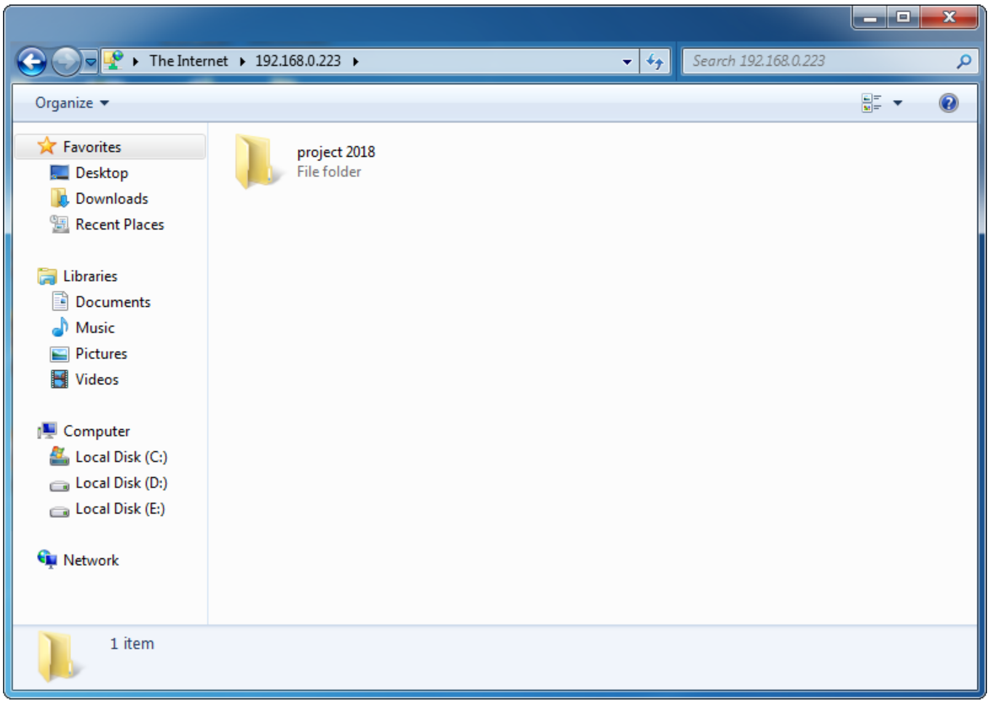
After you log on, you can add this server to your Favorites and return to it easily.

FTP does not encrypt or encode passwords or data before sending them to the server. To protect the security of your passwords and data, use WebDAV instead.

□ Log on anonymously □ Save password

---- End

Access the HQ LAN resources successfully.


The Internet
192.168.0.223
Search 192.168.0.223
Organize
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Computer
Local Disk (C:)
Local Disk (D:)
Local Disk (E:)
Network
project 2018
File folder
1 item

11.15.2 Example of configuring an IPSec VPN

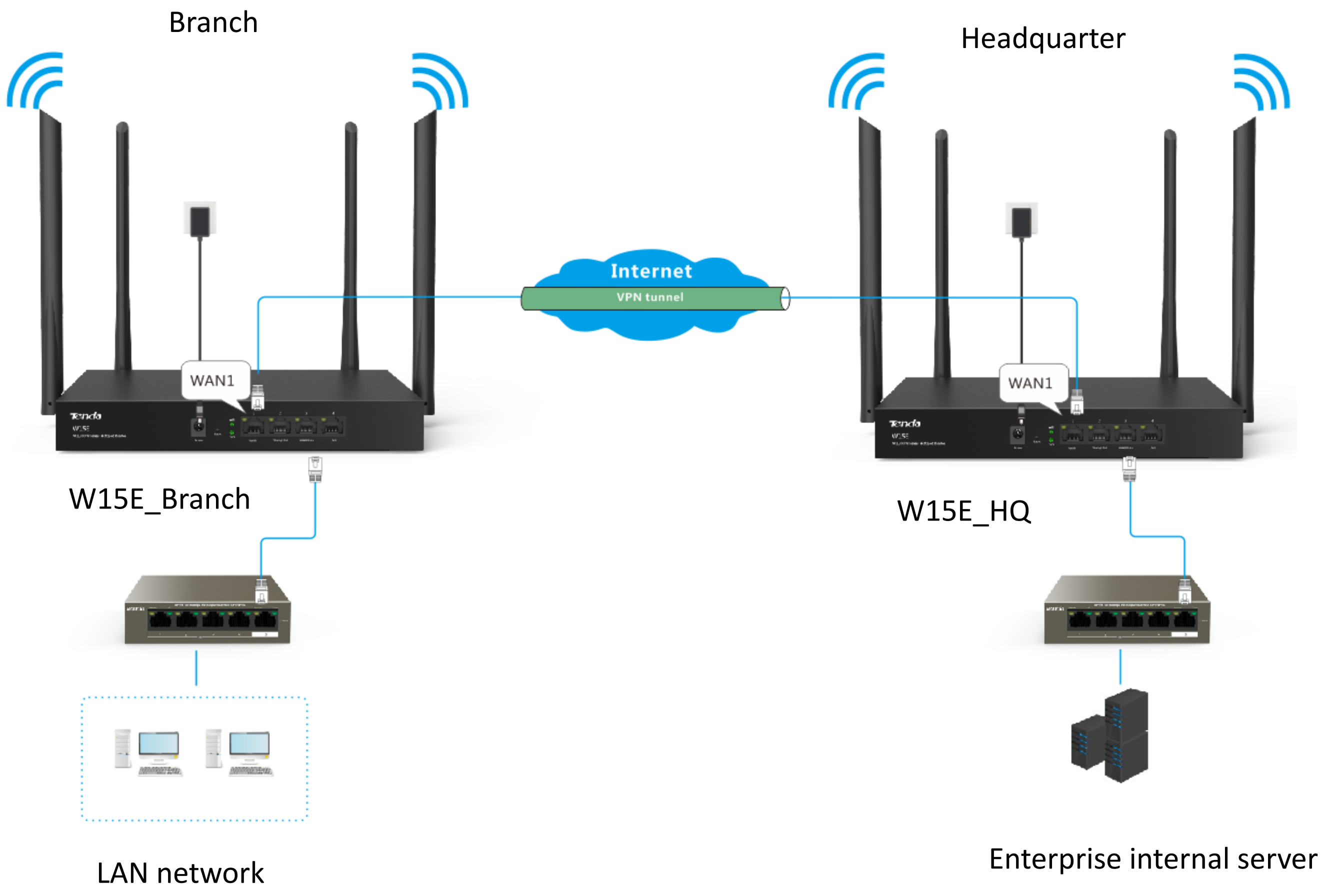
Networking requirement

An enterprise has used W15E to set up a LAN and access the internet. Branch employees need to access the HQ's internal resources through the internet, such as internal data, OA, ERP, CRM, project management systems.

Solutions

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

Network topology



Assume that:

WAN port enabled with IPSec: WAN1

WAN1 IP: 202.105.88.77

LAN network segment/subnet mask:

192.168.1.0/24

Assume that:

WAN port enabled with IPSec: WAN1

WAN1 IP: 202.105.11.22

LAN network segment/subnet mask:

192.168.0.0/24

Configuration procedure

TIP

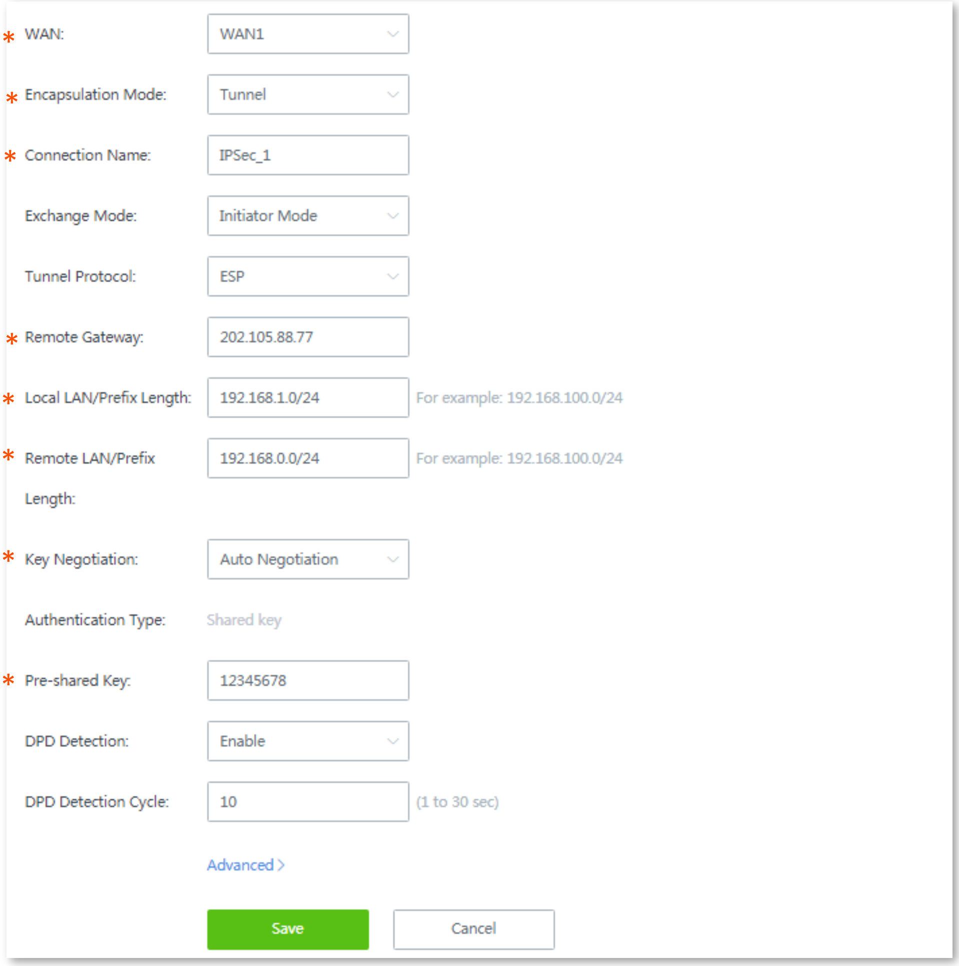
Security software, such as firewall, may fail the configuration. Therefore, you are recommended disable them.

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

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

Step 1 Configure **W15E_HQ** the IPSec connection.

1. Choose **More** > **IPsec**, and click **+Add**, the configuration page appears.
2. Set required parameters.
   (1) Select the WAN port enabled with IPSec, which is **WAN1** in this example.
   (2) Select **Tunnel** from the **Encapsulation Mode** drop-down list menu.
   (3) Customize a **Connection Name**, which is **IPSec_1** in this example.
   (4) **Remote Gateway**: Enter the WAN IP address of its peer W15E_Branch, which is **202.105.88.77** in this example.
   (5) **Local LAN/Prefix Length**: Enter the LAN network segment/subnet mask of W15E_HQ in the defined format, which is **192.168.1.0/24** in this example.
   (6) **Remote LAN/Prefix Length**: Enter the LAN network segment/subnet mask of its peer W15E_Branch in the defined format, which is **192.168.0.0/24** in this example.
   (7) Select **Auto negotiation** from the **Key Negotiation** drop-down list menu, and customize the **Pre-shared Key**, which is **12345678** in this example.
3. Click **Save**.



* WAN: WAN1

* Encapsulation Mode: Tunnel

* Connection Name: IPSec_1

Exchange Mode: Initiator Mode

Tunnel Protocol: ESP

* Remote Gateway: 202.105.88.77

* Local LAN/Prefix Length: 192.168.1.0/24 For example: 192.168.100.0/24

* Remote LAN/Prefix Length: 192.168.0.0/24 For example: 192.168.100.0/24

* Key Negotiation: Auto Negotiation

Authentication Type: Shared key

* Pre-shared Key: 12345678

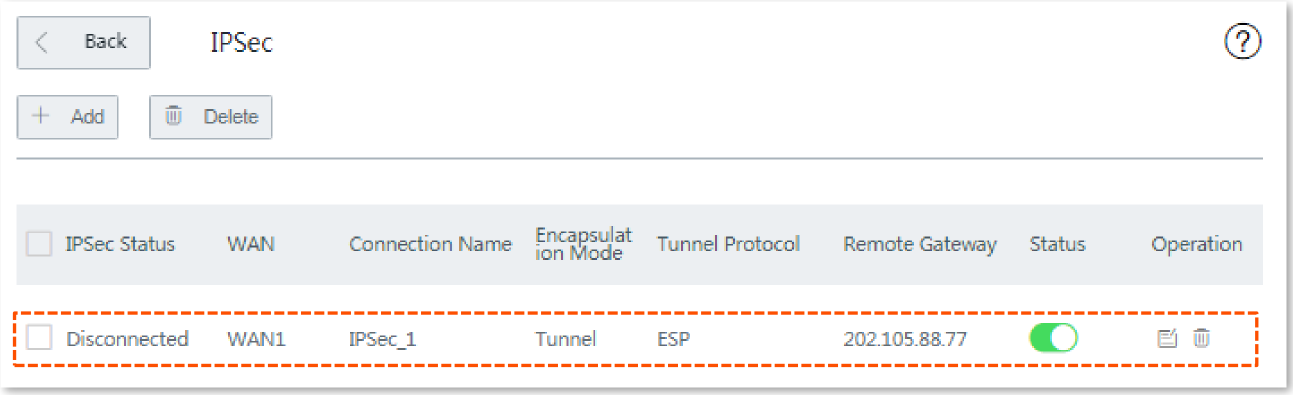
DPD Detection: Enable

DPD Detection Cycle: 10 (1 to 30 sec)

TIP

- Parameters indicated with * are mandatory.
- To configure advanced settings, click **Advanced**. And use the same configurations to set the peer device.

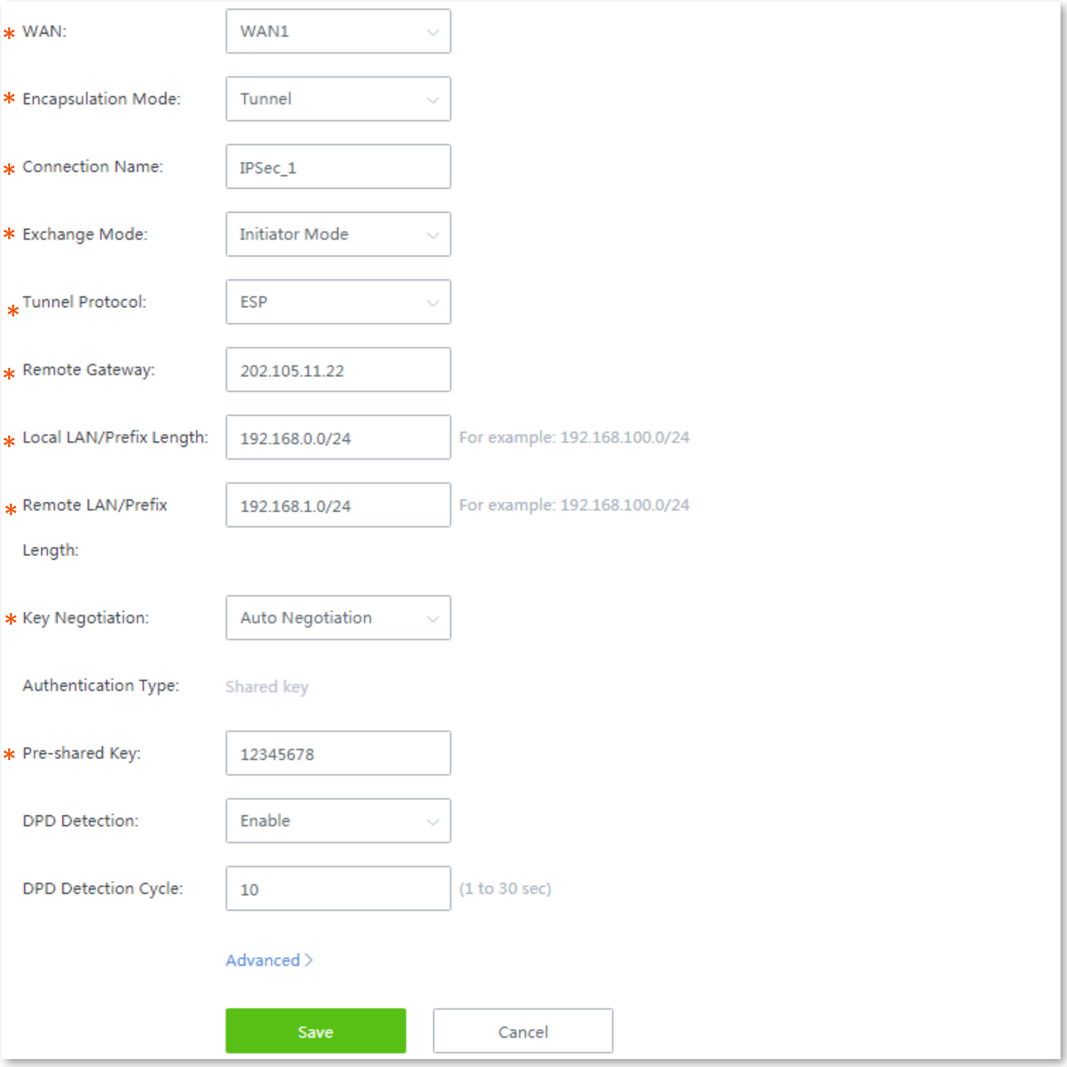
Added successfully. See the following figure:



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

Step 2 **Configure W15E_Branch.**

1. Log in to the web UI of the router W15E_Branch.
2. Choose **More** > **IPsec**, and click **+Add.** The **Add** configuration page appears.
3. Set required parameters.
   (1) Select the WAN port enabled with IPSec, which is **WAN1** in this example.
   (2) Keep **Encapsulation Mode**, **Connection Name**, **Tunnel Protocol**, **Key Negotiation**, and **Pre-shared Key** identical with its peer W15E_HQ.
   (3) **Remote Gateway**: Enter the WAN IP address of its peer W15E_HQ, which is **202.105.11.22** in this example.
   (4) **Local LAN/Prefix Length**: Enter the LAN network segment/subnet mask of W15EE_Branch in the defined format, which is **192.168.0.0/24** in this example.
   (5) **Remote LAN/Prefix Length**: Enter the LAN network segment/subnet mask of W15EE_HQ in the defined format, which is **192.168.1.0/24** in this example.
4. Click **Save**.



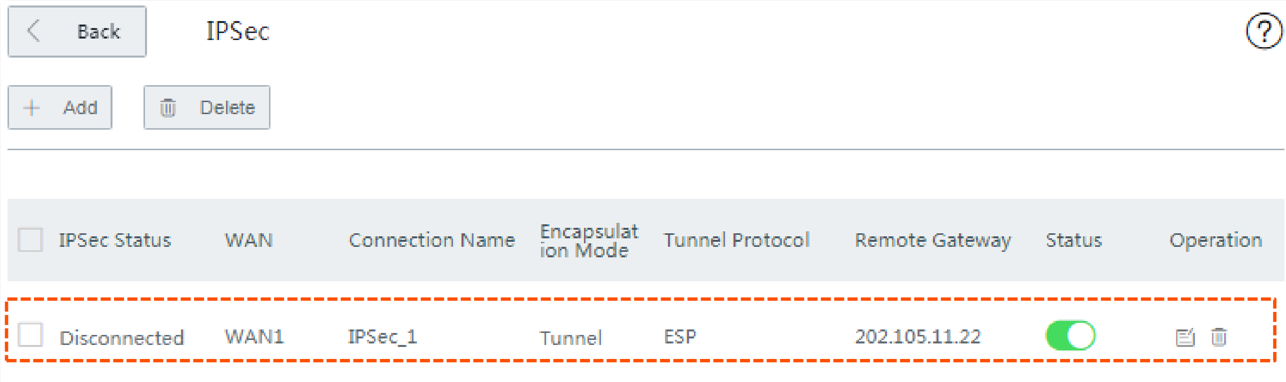
* WAN:	WAN1	
* Encapsulation Mode:	Tunnel	
* Connection Name:	IPSec_1	
* Exchange Mode:	Initiator Mode	
* Tunnel Protocol:	ESP	
* Remote Gateway:	202.105.11.22	
* Local LAN/Prefix Length:	192.168.0.0/24	For example: 192.168.100.0/24
* Remote LAN/Prefix Length:	192.168.1.0/24	For example: 192.168.100.0/24
* Key Negotiation:	Auto Negotiation	
Authentication Type:	Shared key	
* Pre-shared Key:	12345678	
DPD Detection:	Enable	
DPD Detection Cycle:	10	(1 to 30 sec)

TIP

Parameters indicated with * are mandatory.

---- End

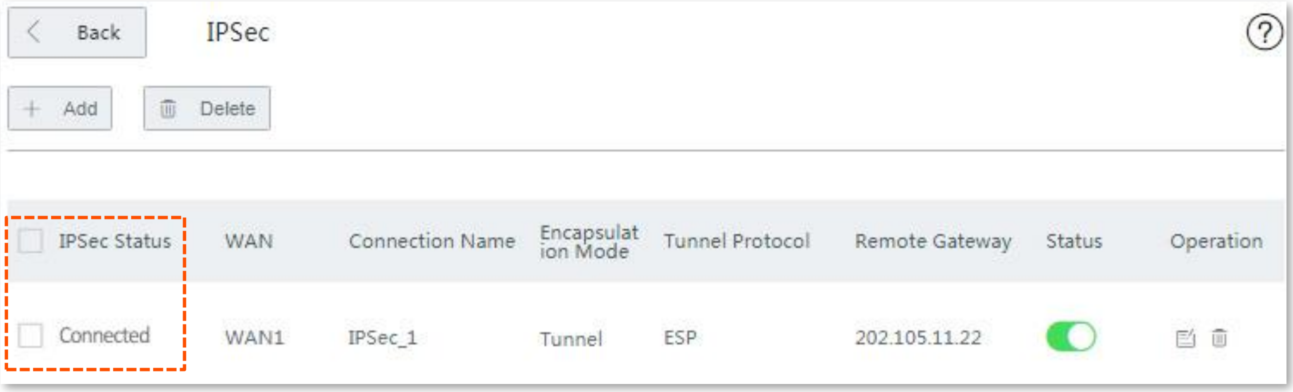
Added successfully. See the following figure.



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

Verification

When the **IPSec Status** of both ends shows **Connected**, the IPSec VPN is established successfully.



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

Then, employees at the branch and HQ can remotely access LAN resources on the other side through the internet in a secure manner.

11.15.3 Example of configuring a L2TP over IPSec VPN

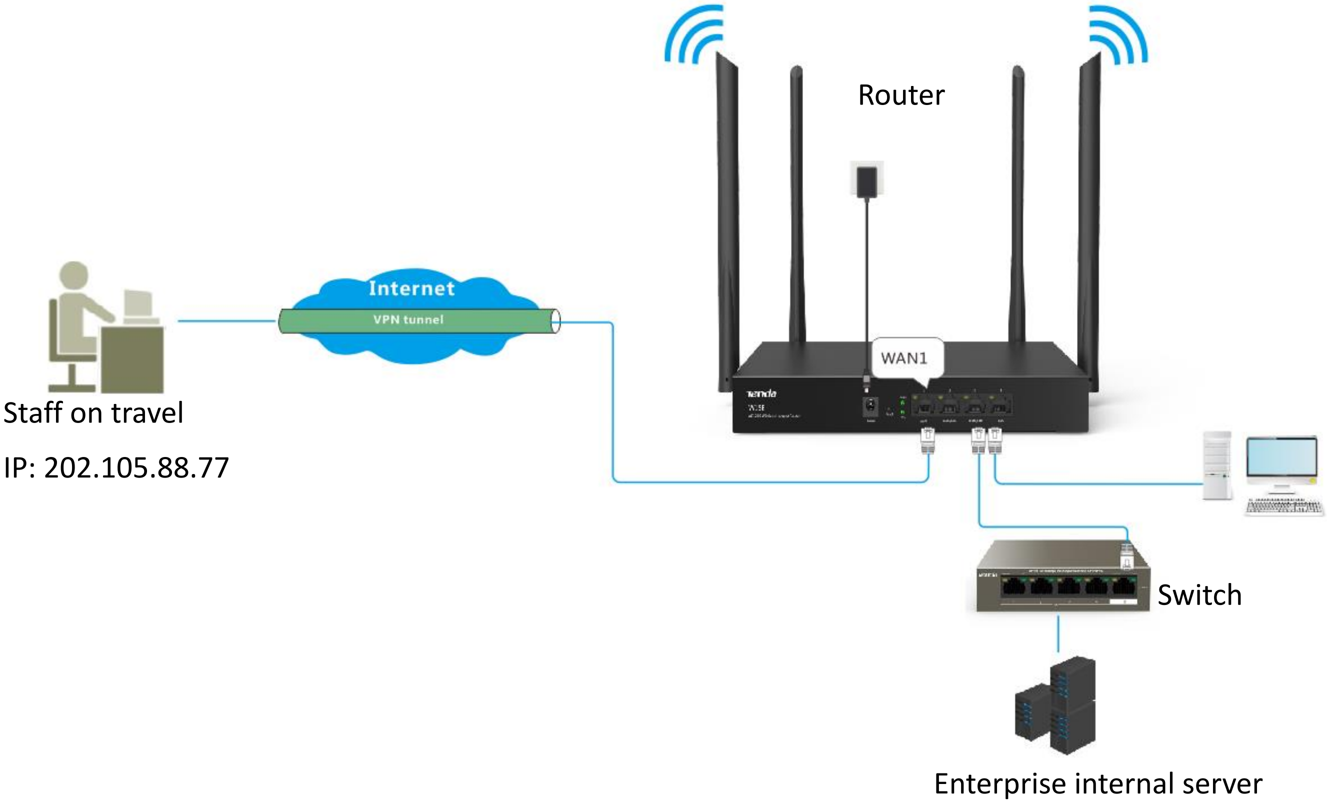
Networking requirement

An enterprise has used W15E 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 resources as well as the OA, ERP, CRM, and project management systems.

Solutions

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

Network topology



Configuration description

Step	Task	Description
1	Configure IPSec connection.	Configure basic IPSec parameters.
2	Configure L2TP server.	Set the router as a L2TP VPN server.
3	Add L2TP users	Create an account for connecting.

Configuration procedure

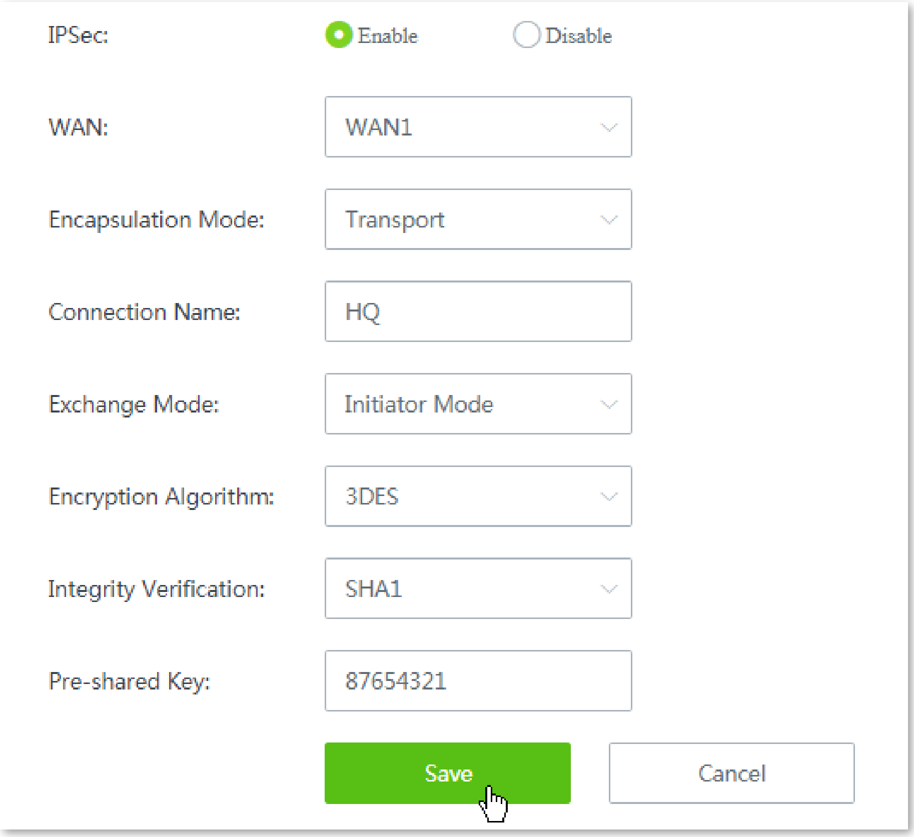
Assume that the two routers share the following basic IPSec information:

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

Step 1 Configure IPSec connection.

1. Choose **More** > **IPsec**, and click **+Add**. The **Add** configuration page appears.
2. Set required parameters.

   Configurations on the following figure are only used for examples.



IPSec: ● Enable ○ Disable

WAN: WAN1

Encapsulation Mode: Transport

Connection Name: HQ

Exchange Mode: Initiator Mode

Encryption Algorithm: 3DES

Integrity Verification: SHA1

Pre-shared Key: 87654321

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

(2) Set **Encapsulation Mode** to **Transport**.

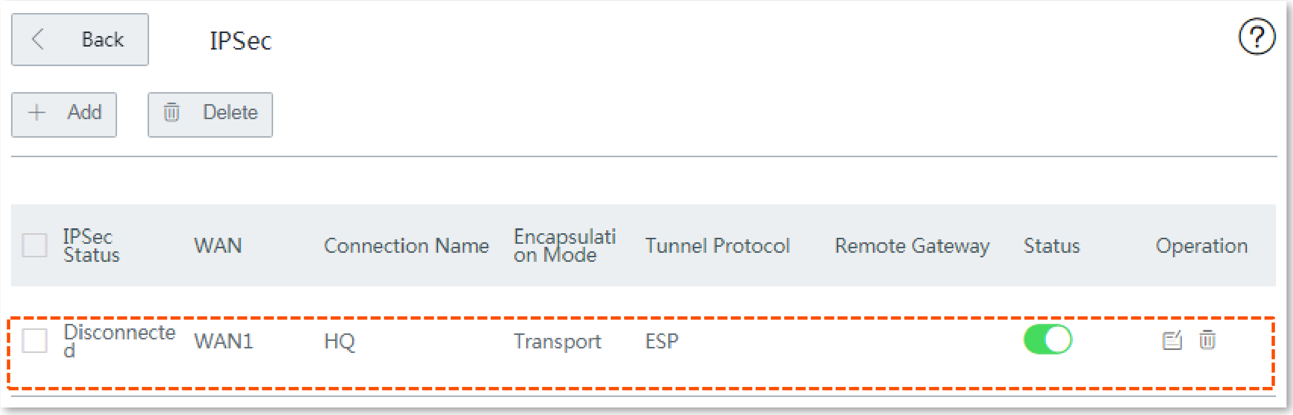
(3) Set **WAN** to the WAN port bound to the IPSec tunnel, which is **WAN1** in this example.

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

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

(6) Click **OK**.

Added successfully. See the following figure:



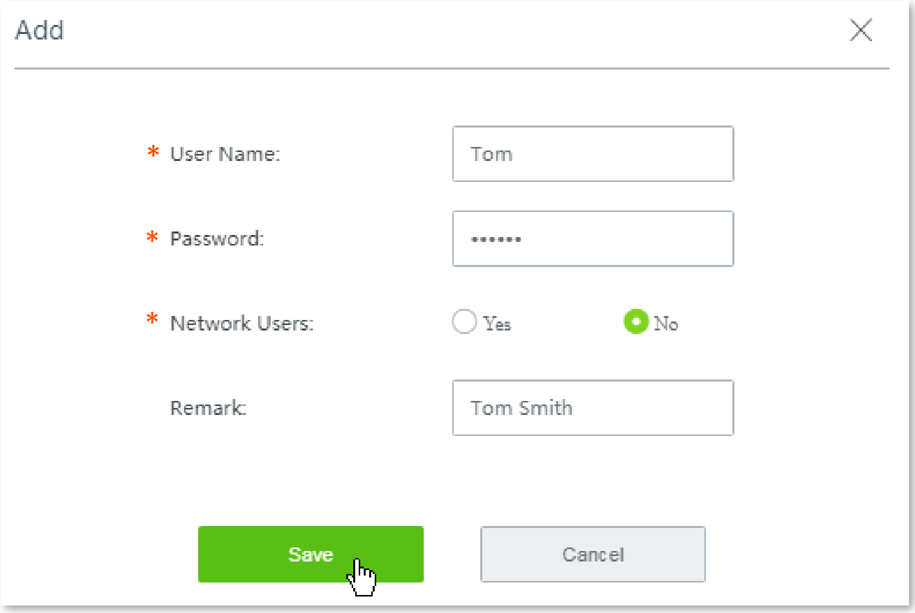
□	IPSec Status	WAN	Connection Name	Encapsulation Mode	Tunnel Protocol	Remote Gateway	Status	Operation
□	Disconnected	WAN1	HQ	Transport	ESP		●	

Step 2 **Configure L2TP server.**

1. Choose **VPN** > **VPN Server**.
2. Set required parameters.
   (1) Set **VPN Server** to **Enable**.
   (2) Set **Client Type** to **L2TP**.
   (3) Set **WAN** to the WAN port bound to the IPSec tunnel, which is **WAN1** in this example.
   (4) Set **IPSec Encryption** to **HQ**.
3. Click **Save.**

Step 3 **Add L2TP users.**

1. Choose **VPN** > **PPTP/L2TP Server**, locate **PPTP/L2TP User** module.
2. Click **+Add**. The **Add** configuration window appears.
3. Set required parameters. Configurations on the following figure are only used for examples.



* User Name: Tom

* Password: ••••••

* Network Users: ○ Yes ● No

Remark: Tom Smith

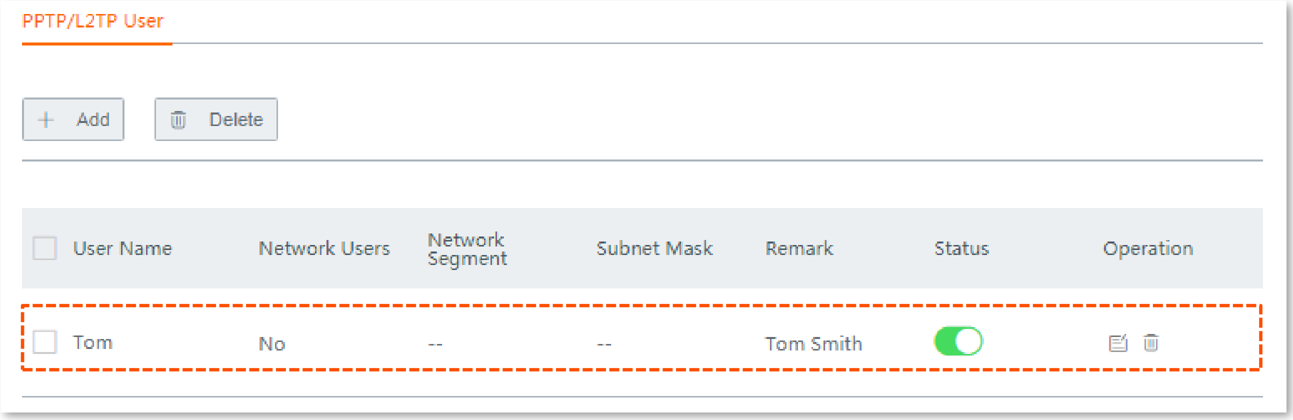
TIP

Parameters indicated with * are mandatory.

4. Click **Save**.

---- End

Added successfully. See the following figure.



PPTP/L2TP User

＋ Add　🗑 Delete

□	User Name	Network Users	Network Segment	Subnet Mask	Remark	Status	Operation
□	Tom	No	--	--	Tom Smith	●	

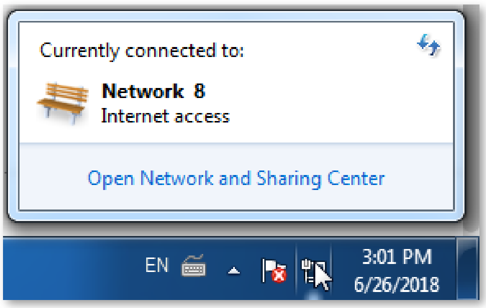
Verification

To access the HQ LAN resources, you have to configure your client. The document introduces how to create VPN dialing on Windows 7 and iOS. Choose the scenario according to your actual situations.

- **Create VPN connection on Windows 7**.

Step 1 Create VPN connections.

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

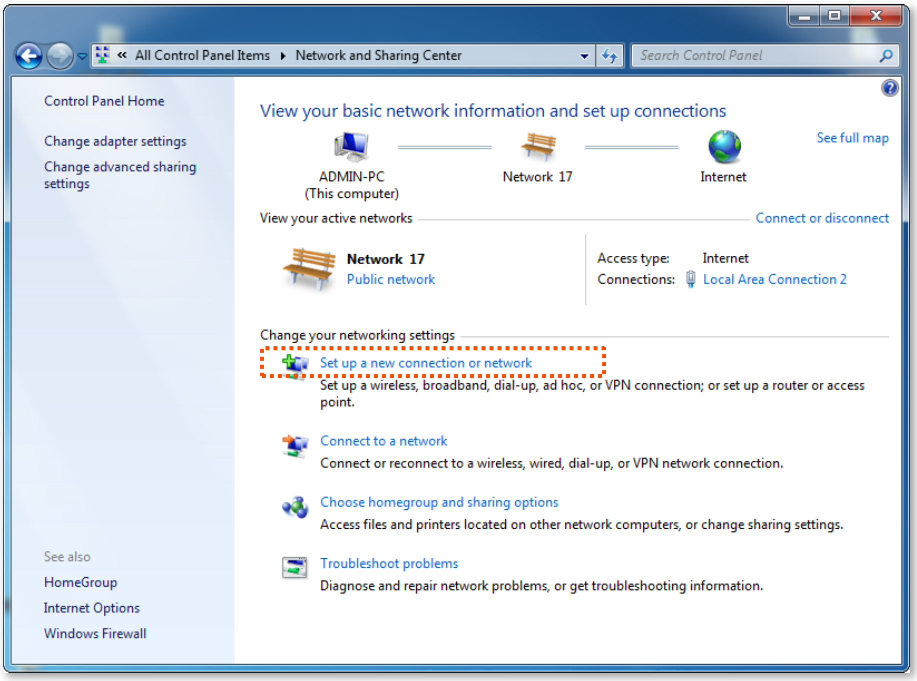


Currently connected to:

Network 8
Internet access

Open Network and Sharing Center

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



View your basic network information and set up connections

View your active networks

Network 17
Public network

Access type: Internet
Connections: Local Area Connection 2

Change your networking settings

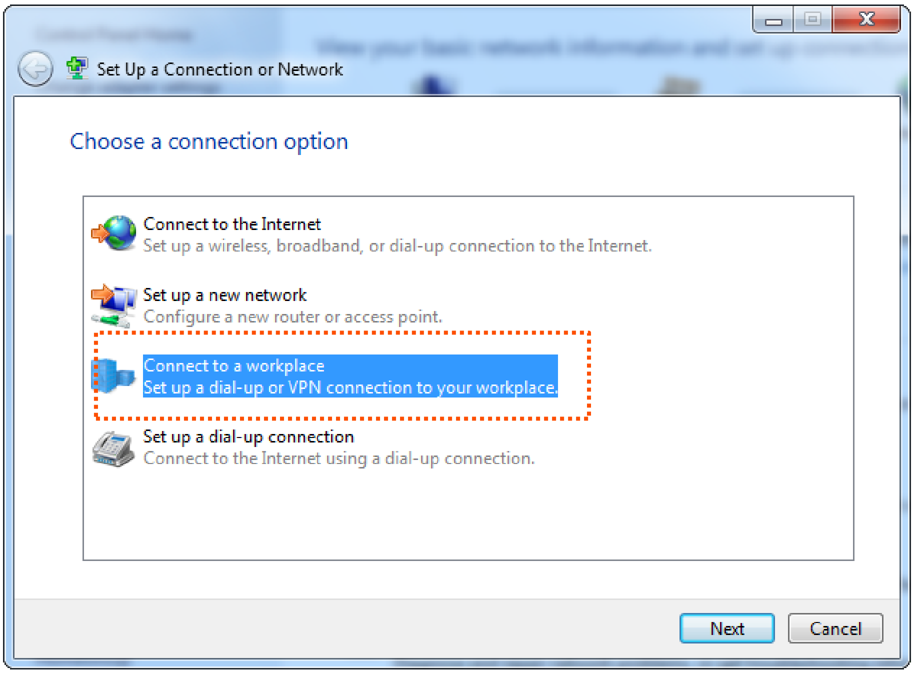
Set up a new connection or network
Set up a wireless, broadband, dial-up, ad hoc, or VPN connection; or set up a router or access point.

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 a workplace**, then click **Next**.



Choose a connection option

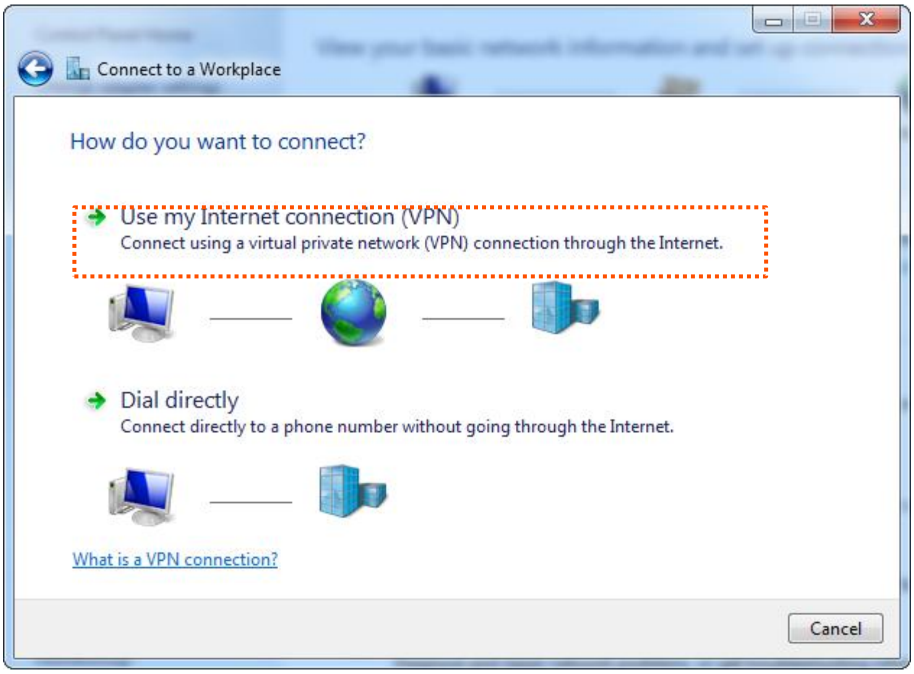
Connect to the Internet
Set up a wireless, broadband, or dial-up connection to the Internet.

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

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 **Use my internet connection (VPN)**. If any other window popup, follow the on-screen instructions.



Connect to a Workplace

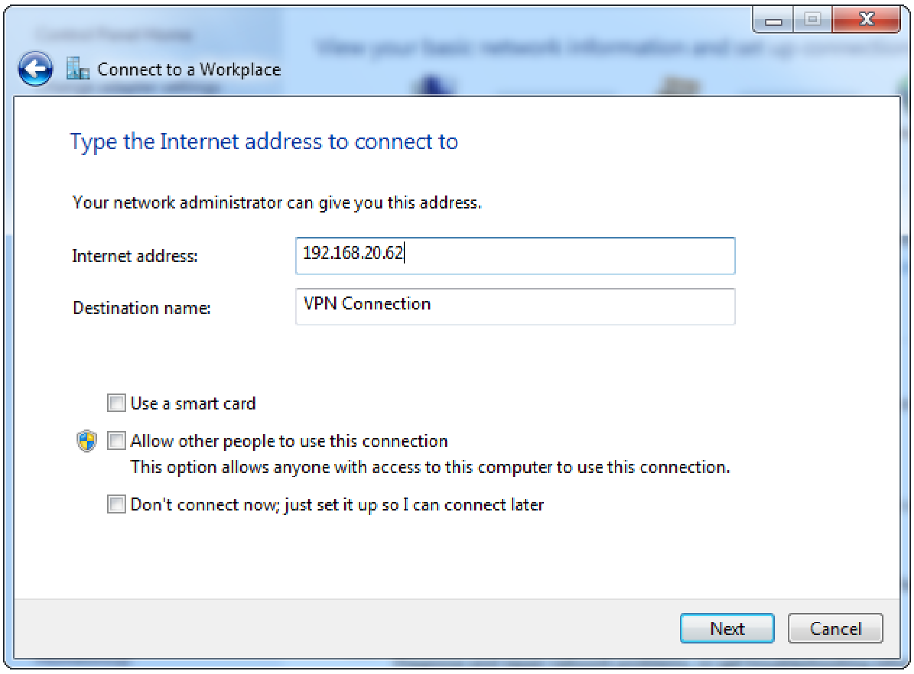
How do you want to connect?

➔ Use my Internet connection (VPN)
Connect using a virtual private network (VPN) connection through the Internet.

➔ Dial directly
Connect directly to a phone number without going through the Internet.

What is a VPN connection?

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



Connect to a Workplace

Type the Internet address to connect to

Your network administrator can give you this address.

Internet address: 192.168.20.62

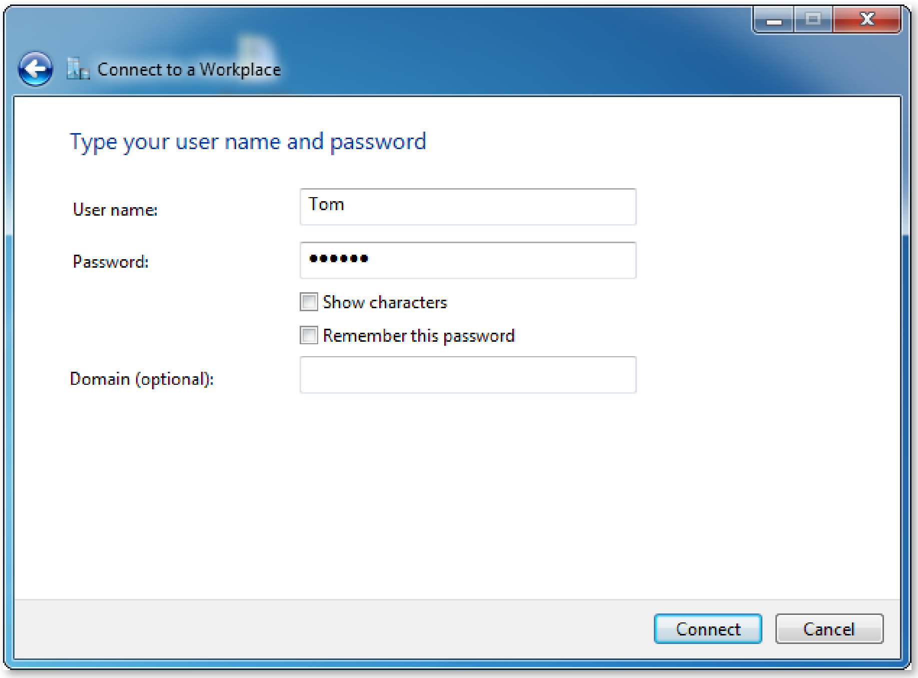
Destination name: VPN Connection

□ Use a smart card

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

□ Don't connect now; just set it up so I can connect later

6. Set the **User name** to **Tom**, and **password** to **Tom123**. Then click **Connect.**



Connect to a Workplace

Type your user name and password

User name: Tom

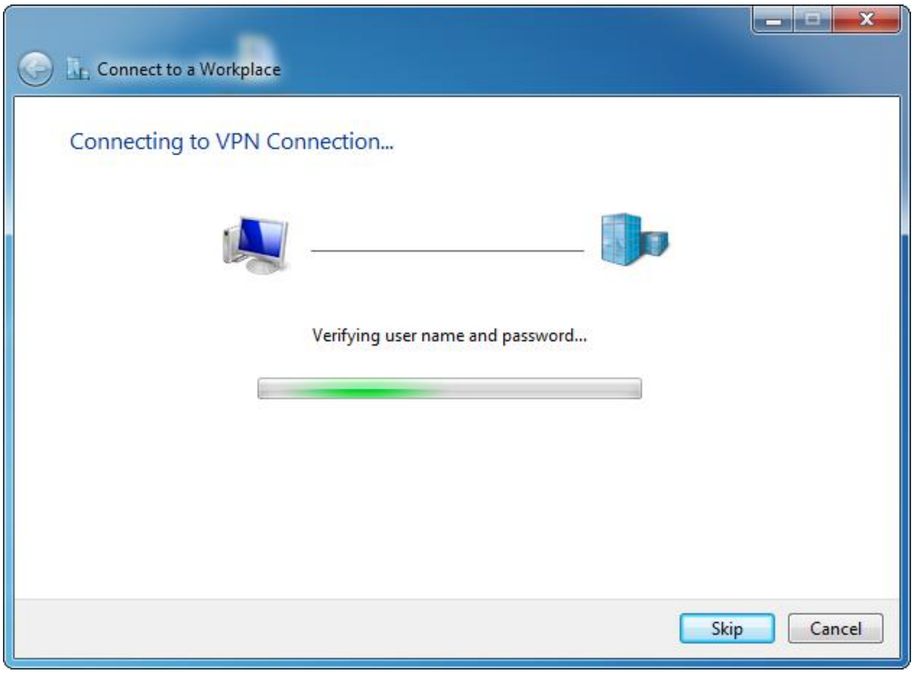
Password: ●●●●●●

☐ Show characters

☐ Remember this password

Domain (optional):

7. Wait for a moment to establish a connection.



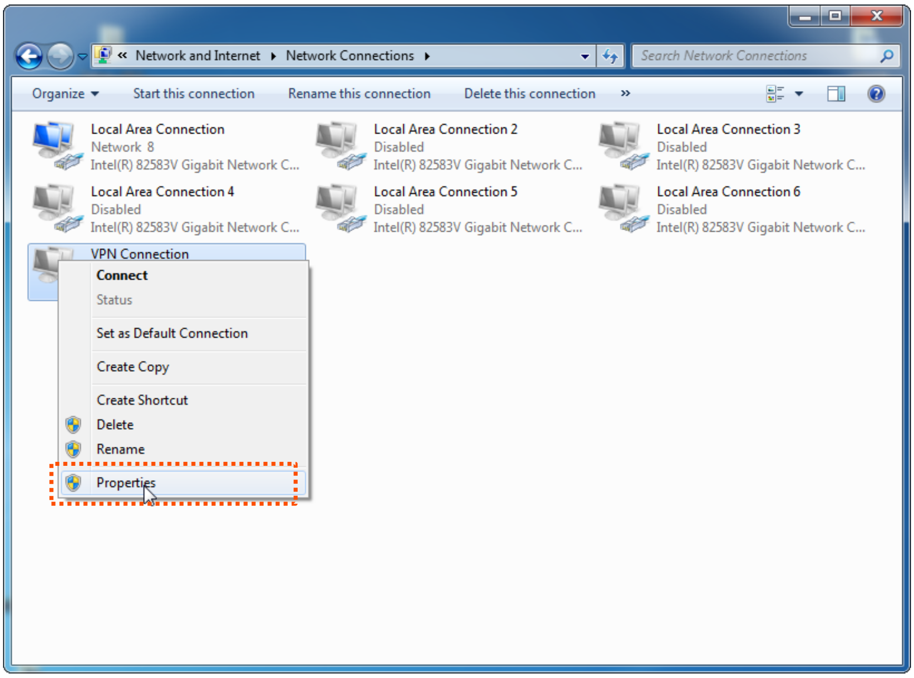
Connect to a Workplace

Connecting to VPN Connection...

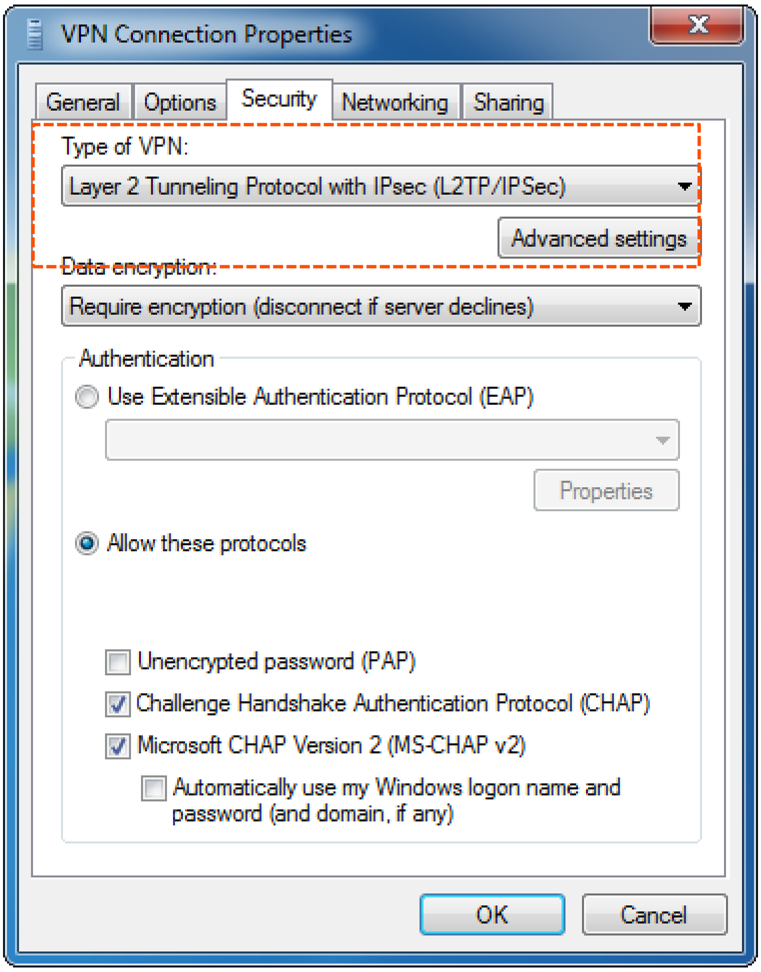
Verifying user name and password...

Step 2 Set VPN connection parameters.

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



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



VPN Connection Properties

General | Options | Security | Networking | Sharing

Type of VPN:

Layer 2 Tunneling Protocol with IPsec (L2TP/IPSec)

Advanced settings

Data encryption:

Require encryption (disconnect if server declines)

Authentication

○ Use Extensible Authentication Protocol (EAP)

Properties

● Allow these protocols

□ Unencrypted password (PAP)

☑ Challenge Handshake Authentication Protocol (CHAP)

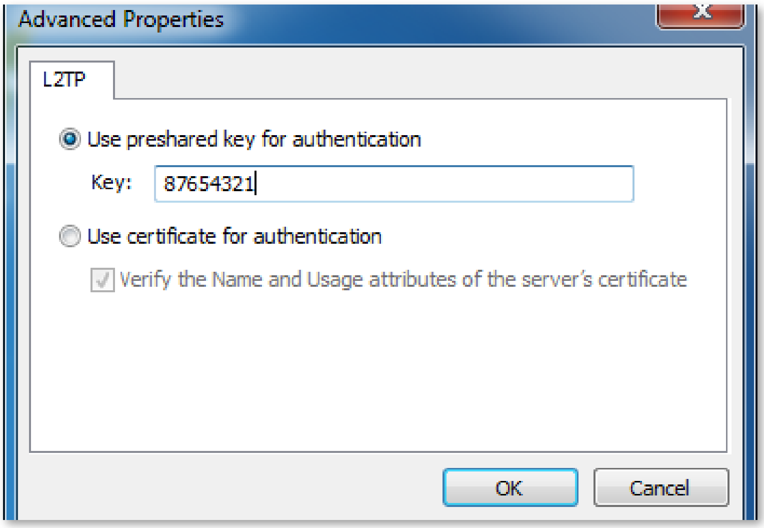
☑ Microsoft CHAP Version 2 (MS-CHAP v2)

□ Automatically use my Windows logon name and password (and domain, if any)

OK | Cancel

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

4. Click **OK**.



Advanced Properties

L2TP

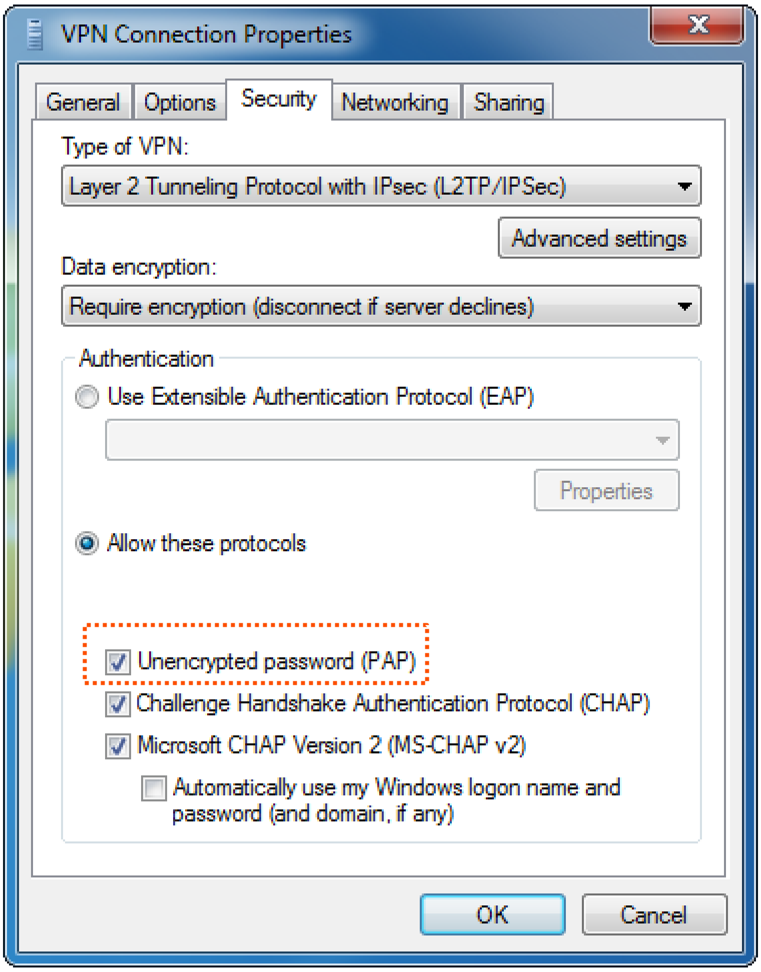
● Use preshared key for authentication

Key: 87654321

○ Use certificate for authentication

☑ Verify the Name and Usage attributes of the server's certificate

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



VPN Connection Properties

Type of VPN:

Layer 2 Tunneling Protocol with IPsec (L2TP/IPSec)

Data encryption:

Require encryption (disconnect if server declines)

Authentication

○ Use Extensible Authentication Protocol (EAP)

● Allow these protocols

☑ Unencrypted password (PAP)

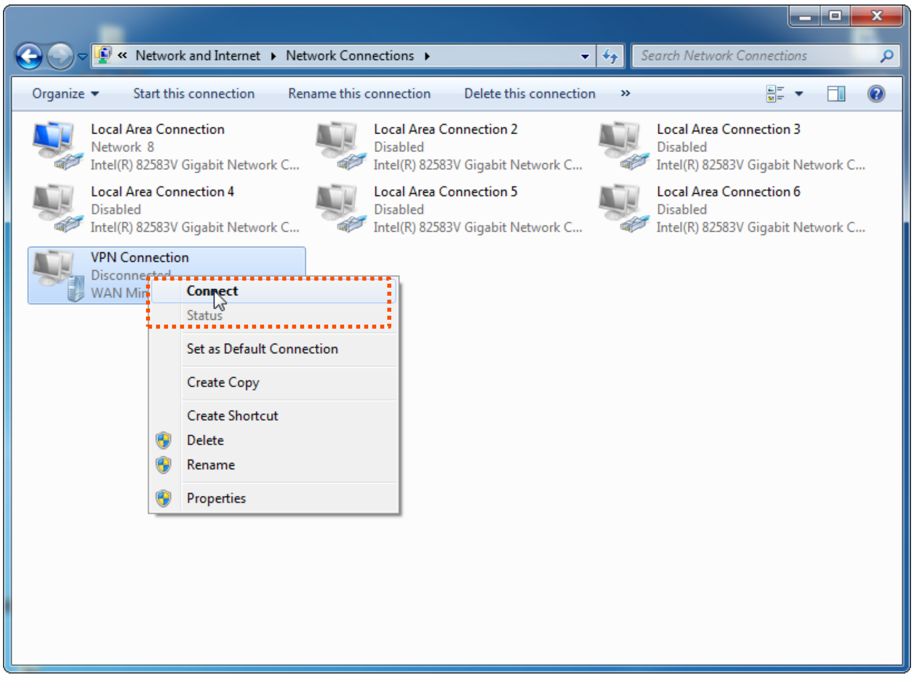
☑ Challenge Handshake Authentication Protocol (CHAP)

☑ Microsoft CHAP Version 2 (MS-CHAP v2)

□ Automatically use my Windows logon name and password (and domain, if any)

Step 3 Create VPN dialing.

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



« Network and Internet ▸ Network Connections ▸

Search Network Connections

Organize ▾ Start this connection Rename this connection Delete this connection »

Local Area Connection
Network 8
Intel(R) 82583V Gigabit Network C...

Local Area Connection 2
Disabled
Intel(R) 82583V Gigabit Network C...

Local Area Connection 3
Disabled
Intel(R) 82583V Gigabit Network C...

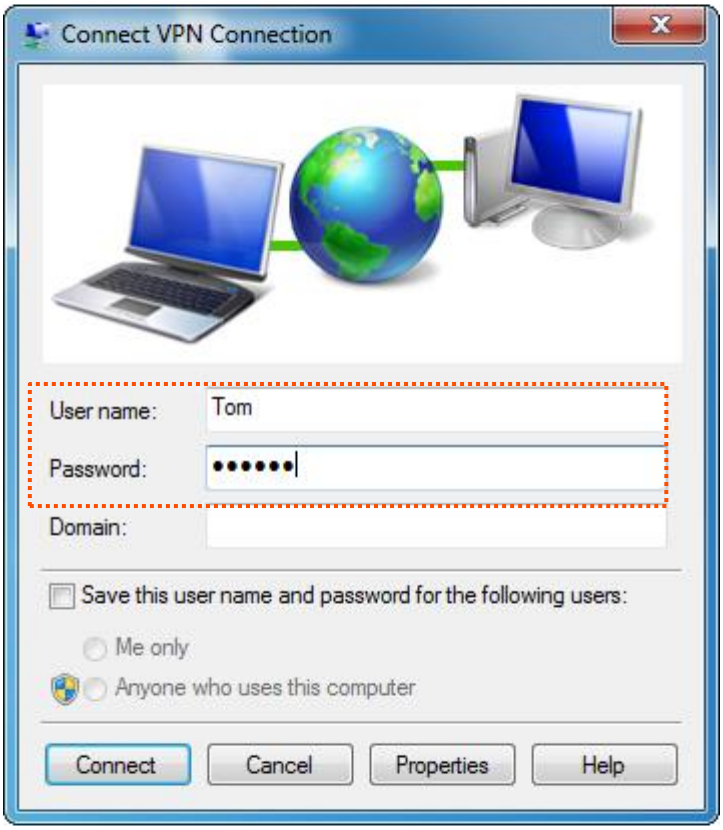
Local Area Connection 4
Disabled
Intel(R) 82583V Gigabit Network C...

Local Area Connection 5
Disabled
Intel(R) 82583V Gigabit Network C...

Local Area Connection 6
Disabled
Intel(R) 82583V Gigabit Network C...

VPN Connection
Disconnected
WAN Min

2. Enter User name to Tom, password to Tom123, and click Connect.



Connect VPN Connection

User name: Tom

Password: ••••••|

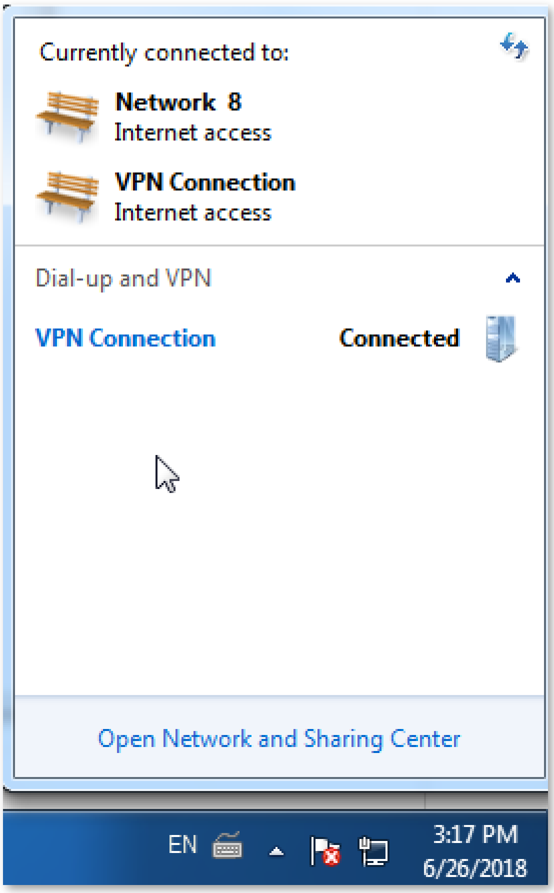
Domain:

□ Save this user name and password for the following users:

○ Me only

○ Anyone who uses this computer

Wait for a moment to establish a connection.



Currently connected to:

Network 8
Internet access

VPN Connection
Internet access

Dial-up and VPN

VPN Connection Connected

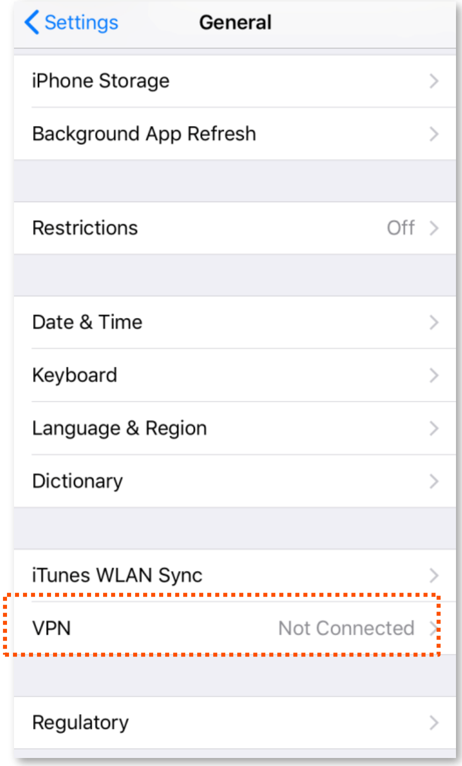
Open Network and Sharing Center

EN

3:17 PM
6/26/2018

- Create VPN connection on a mobile device (Example: iOS).

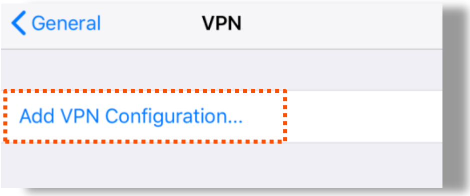
1. Tap ⚙ on the **Settings** page.
2. Tap **VPN.**



Settings General

iPhone Storage	
Background App Refresh	
Restrictions	Off
Date & Time	
Keyboard	
Language & Region	
Dictionary	
iTunes WLAN Sync	
VPN	Not Connected
Regulatory	

3. Tap **Add VPN Configuration**.



4. Set required parameters.

   (1) Set **Type** to **L2TP.**

   (2) Set **Description** to the name of the VPN connection, which is **HQ** in this example.

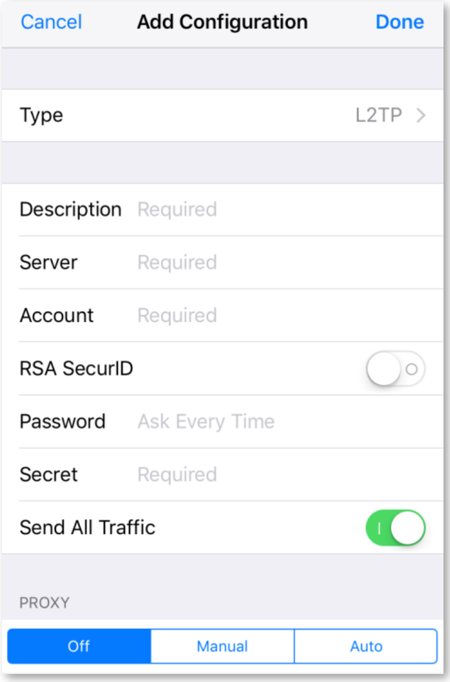
   (3) Set **Server** to the IP address of L2TP server, which is **192.168.20.62** in this example.

   (4) Set **Account** to the user name used to connect the VPN client to the VPN server, which is **Tom** in this example.

   (5) Set **Password** to the password for the user name, which is **Tom123** in this example.

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

   (7) Tap **Done.**



Type L2TP

Description Required

Server Required

Account Required

RSA SecurID ○

Password Ask Every Time

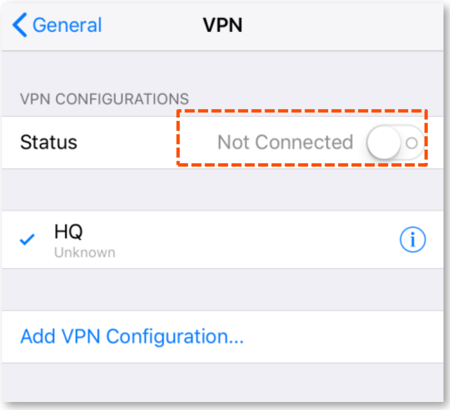
Secret Required

Send All Traffic ●

PROXY

Off | Manual | Auto

5. Tap ○.

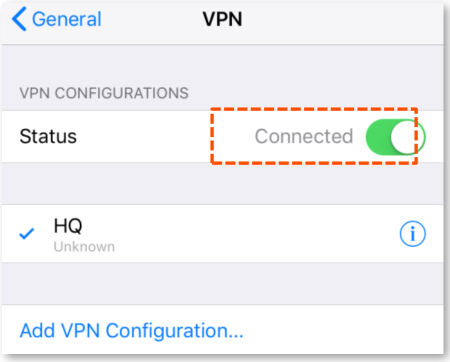


Status Not Connected ○

✓ HQ
Unknown

Add VPN Configuration...

Wait for a moment. When the **Status** turns to **Connected** , the IPSec connection is created successfully.



VPN CONFIGURATIONS

Status Connected

HQ
Unknown

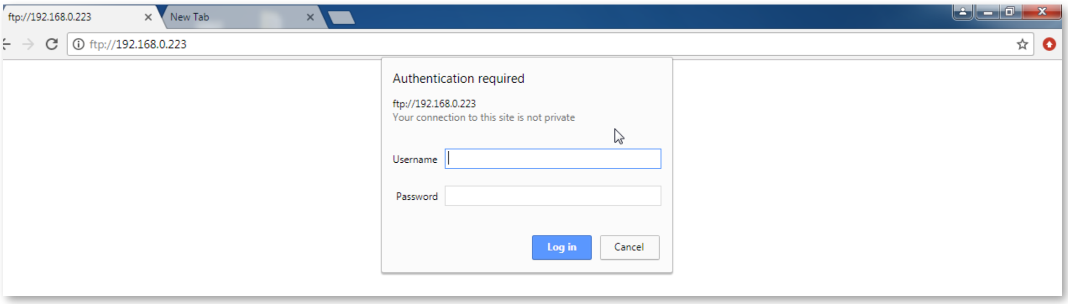
Add VPN Configuration...

Step 4 Accessing HQ data for employees on business trip

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

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

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



Authentication required

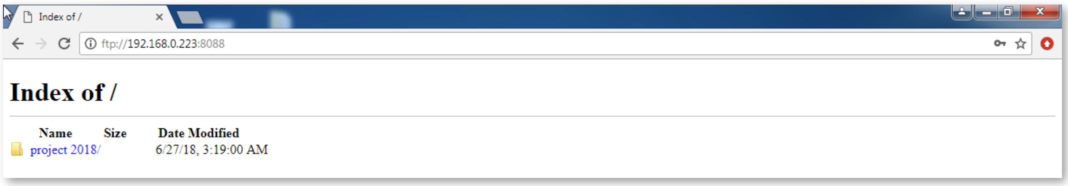
ftp://192.168.0.223
Your connection to this site is not private

Username

Password

2. Enter the **Username** and **Password** you set, which is Tom/Tom123 in this example.

Accessed successfully. See the following figure:



Index of /

Name	Size	Date Modified
project 2018/		6/27/18, 3:19:00 AM

TIP

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

11.16 Multi-WAN

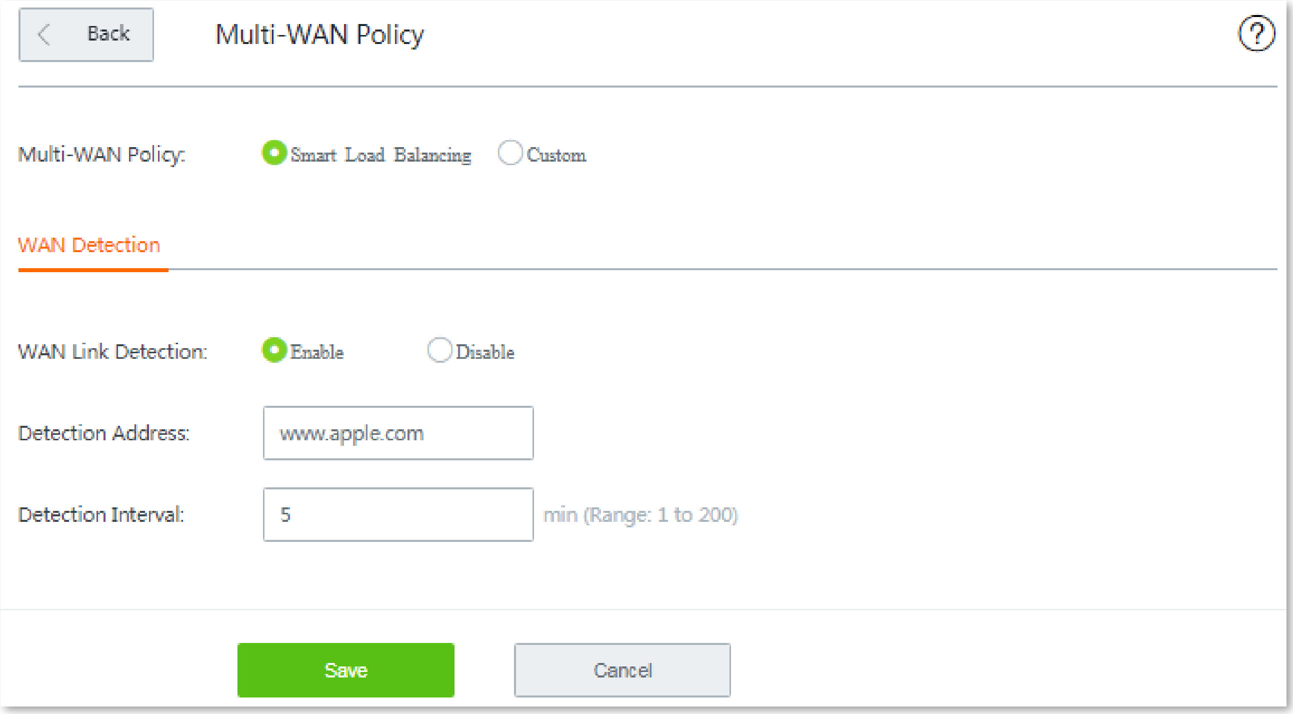
11.16.1 Overview

The router has 1 WAN port by default but allows a maximum of 3 WAN ports. When multiple WAN ports are operating at the same time, an appropriate multi-WAN policy can greatly improve the bandwidth usage of the router. The router supports the following types of multi-WAN policy:

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

11.16.2 Setting multi-WAN policies

To access the configuration page, choose **More** > **Multi-WAN Policy**. By default, the **WAN Detection** is disabled. The following page appears when the **WAN Detection** is enabled.



Multi-WAN Policy: ● Smart Load Balancing ○ Custom

WAN Link Detection: ● Enable ○ Disable

Detection Address: www.apple.com

Detection Interval: 5 min (Range: 1 to 200)

Parameter description

Parameter	Description
Mutil-WAN Policy	It specifies the policy through the WAN ports. - **Smart Load Balancing**: The system automatically distributes traffic through the WAN ports with the smallest amount of traffic. - **Custom**: It enables you to assign WAN ports to source IP addresses as required.
WAN Detection	The router regularly detects the connection status between the WAN ports and detection address.

Parameter	Description
	- **Detection Address:** The IP address or domain name to detect. - **Detection Interval:** The interval of detection, it is 5 minutes by default.

11.16.3 Customizing a multi-WAN policy

Before you start

Configure the following parameters first:

- **IP group(s):** Choose **Filter Management** > **Time group/IP group** for settings.
- **Bandwidth upload/download rate**: Choose **Bandwidth Control**, and locate the corresponding WAN port for settings.

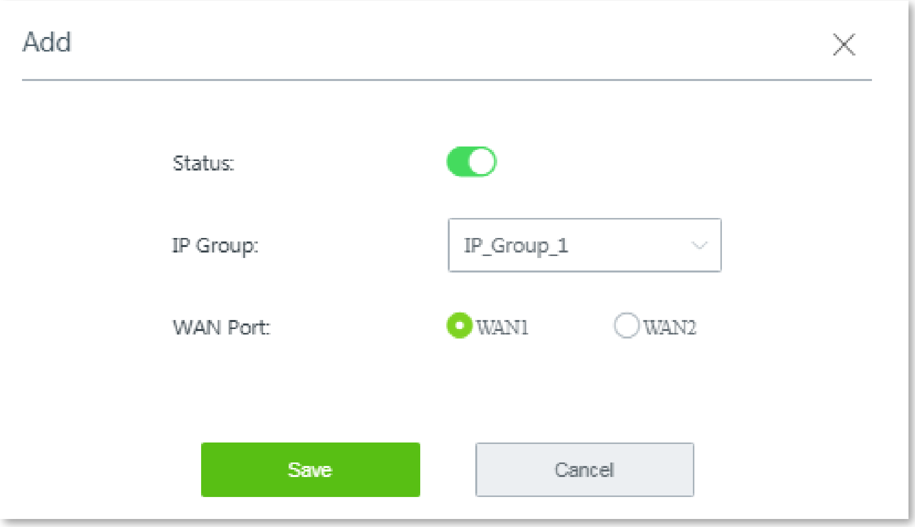
Configuration procedure

Step 1 Choose **More** > **Multi-WAN Policy**, and click **+Add**.

Step 2 Select the **IP Group** you set on **Filter Management** > **Time group/IP group** page.

Step 3 Select the WAN port to which the policy applies.

Step 4 Click **Save**.



Add

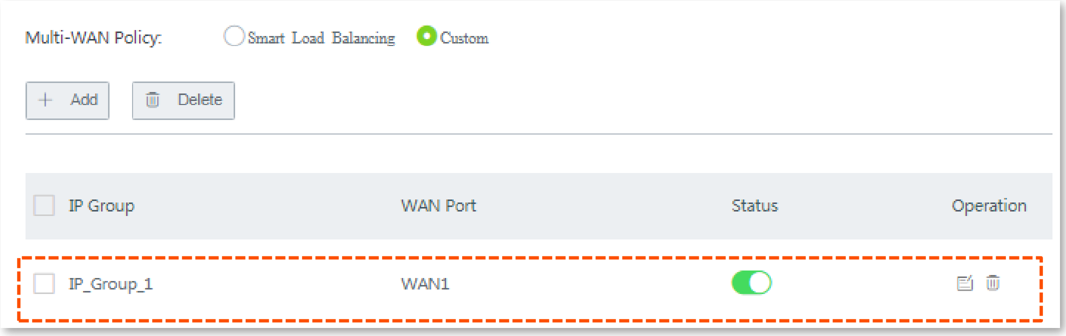
Status: ●

IP Group: IP_Group_1

WAN Port: ● WAN1 ○ WAN2

---- End

The policy is added successfully. See the following figure:



Multi-WAN Policy: ○ Smart Load Balancing ● Custom

□ IP Group	WAN Port	Status	Operation
□ IP_Group_1	WAN1	●	

11.16.4 Example of customizing a multi-WAN policy

Networking requirement

An enterprise has used W15E 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.

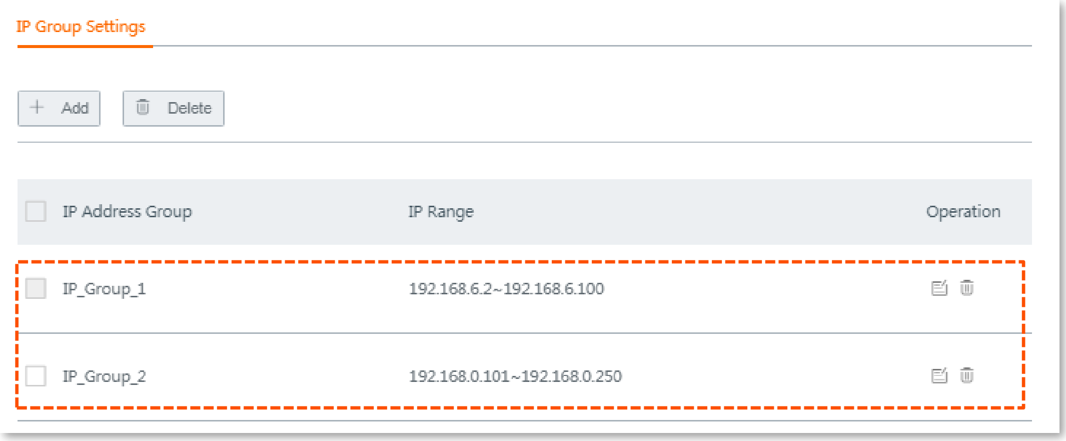
Solutions

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

Configuration procedure

Step 1 Set IP address groups.

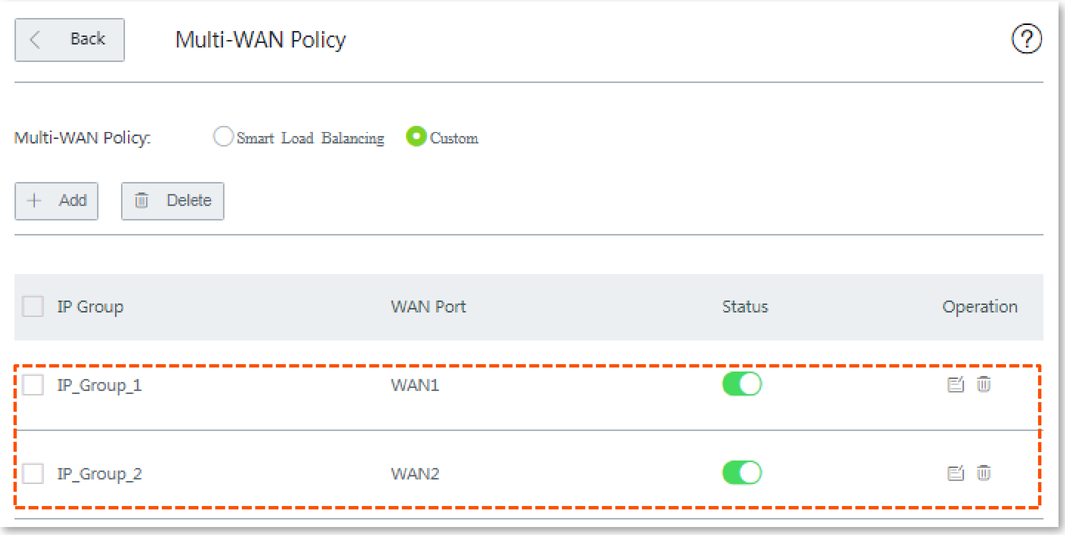
1. Choose **Filter Management** > **IP Group/Time Group**, and move to the **IP Group** configuration area.
2. Set the IP address group shown in the following figure.



□ IP Address Group	IP Range	Operation
□ IP_Group_1	192.168.6.2~192.168.6.100	
□ IP_Group_2	192.168.0.101~192.168.0.250	

Step 2 Customize multi-WAN policies.

1. Choose **More** > **Multi-WAN Policy**.
2. Select **Custom**, and click **Save**.
3. Click **+Add**, and set the rules shown in the following figure.



Multi-WAN Policy: ○ Smart Load Balancing ● Custom

□ IP Group	WAN Port	Status	Operation
□ IP_Group_1	WAN1	●	
□ IP_Group_2	WAN2	●	

---- End

Verification

The computers with IP addresses ranging from 192.168.0.2 to 192.168.0.100 can 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 can access the Internal through the mobile broadband connection with ISP B.

12 Maintenance

This chapter describes how to reboot, reset, and upgrade the router, how to modify the login password, how to backup your current configuration and restore the router to previous configuration, how to view the system logs and functions that are enabled or disabled, how to set up system time, and how to use the Ping and Traceroute commands.

12.1 Rebooting the router

12.1.1 Overview

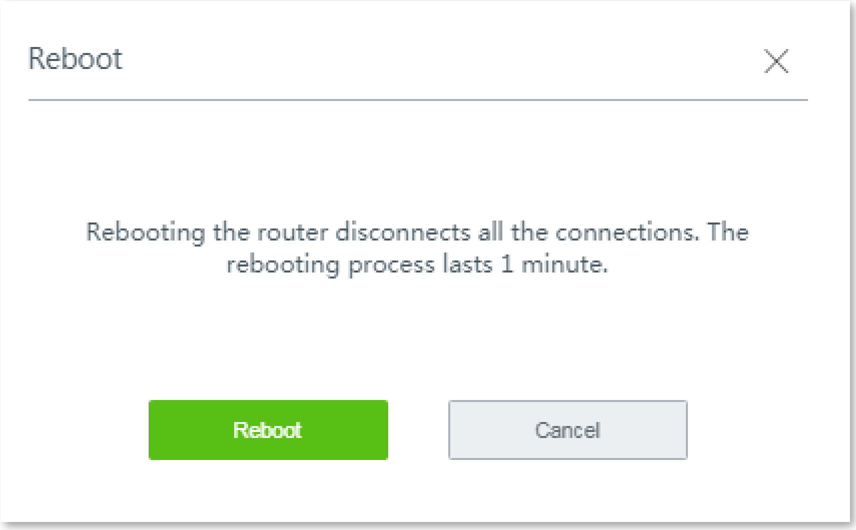
If a parameter does not take effect or the router does not work properly, you can try rebooting the router to resolve the problem.

The router supports two rebooting methods:

- Rebooting the router manually.
- Rebooting the router on schedule.

12.1.2 Rebooting the router manually

Choose **Maintenance > Reboot**, and follow the on-screen instruction to reboot the device.



Rebooting the router disconnects all the connections. The rebooting process lasts 1 minute.

12.1.3 Rebooting the router on schedule

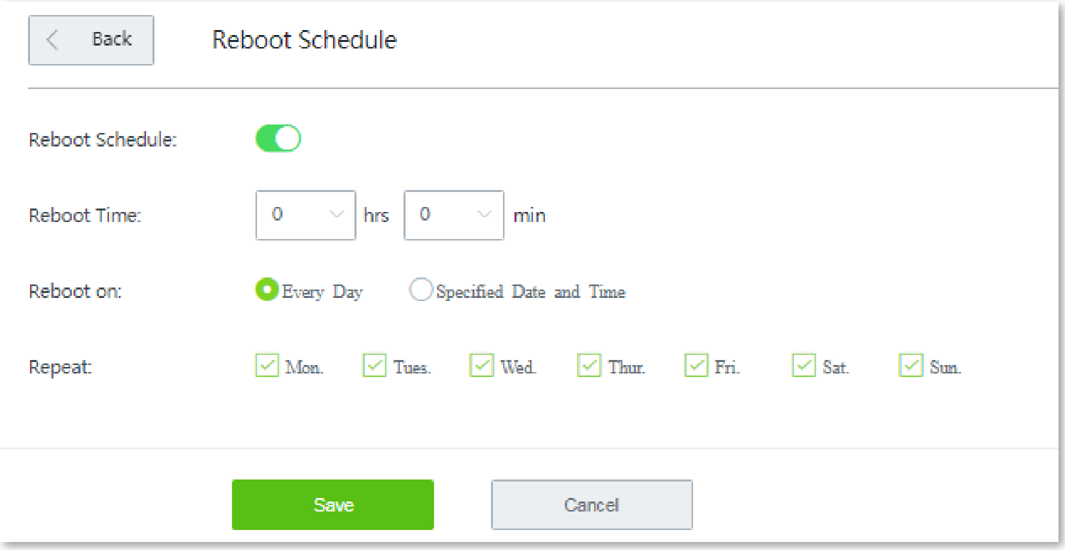
TIP

To enable reboot schedule function to work properly, ensure that the **Model** of your router is correct.

Step 1 Choose **Maintenance** > **Reboot Schedule** to enter the configuration page, and enable this function.

Step 2 Set the time and date when the router performs rebooting.

Step 3 Click **Save** to apply your settings.



Reboot Schedule: ●

Reboot Time: 0 hrs 0 min

Reboot on: ● Every Day ○ Specified Date and Time

Repeat: ☑ Mon. ☑ Tues. ☑ Wed. ☑ Thur. ☑ Fri. ☑ Sat. ☑ Sun.

---- End

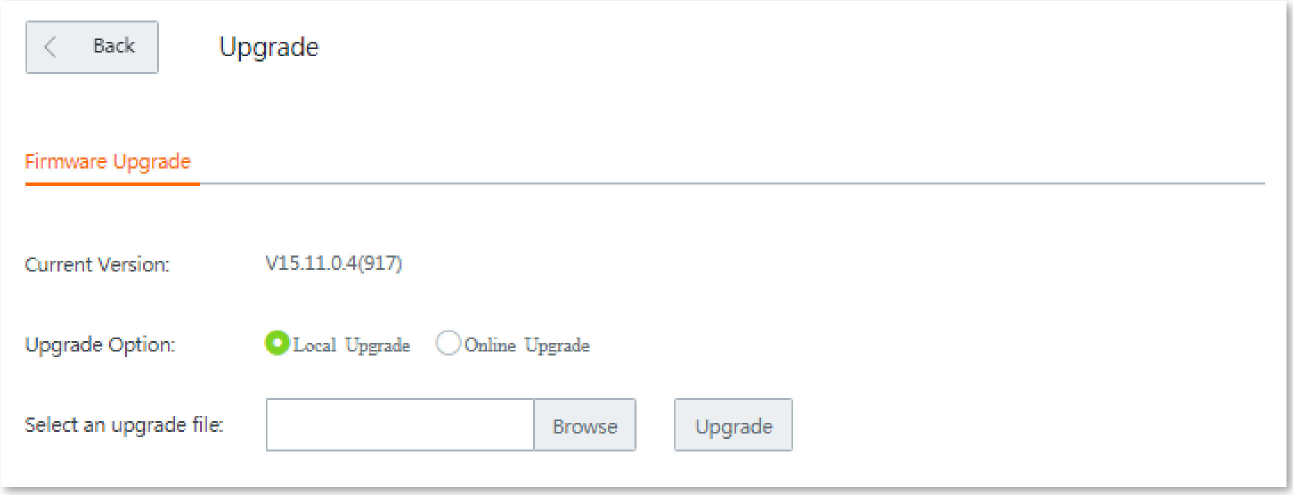
The router performs rebooting regularly on the time and date you set here.

12.2 Upgrade

12.2.1 Overview

The router supports **local** and **online** upgrades.

Choose **Maintenance** > **Upgrade** to enter the configuration page. See the following figure:



Current Version: V15.11.0.4(917)

Upgrade Option: ● Local Upgrade ○ Online Upgrade

Select an upgrade file:

12.2.2 Upgrading the rotuer manually

TIP

- To enable your router to work properly after an upgrade, ensure that the firmware used to upgrade complies with your Model.
- When upgrading, do not power off the router.

Step 1 Download the upgrade file to your local computer.

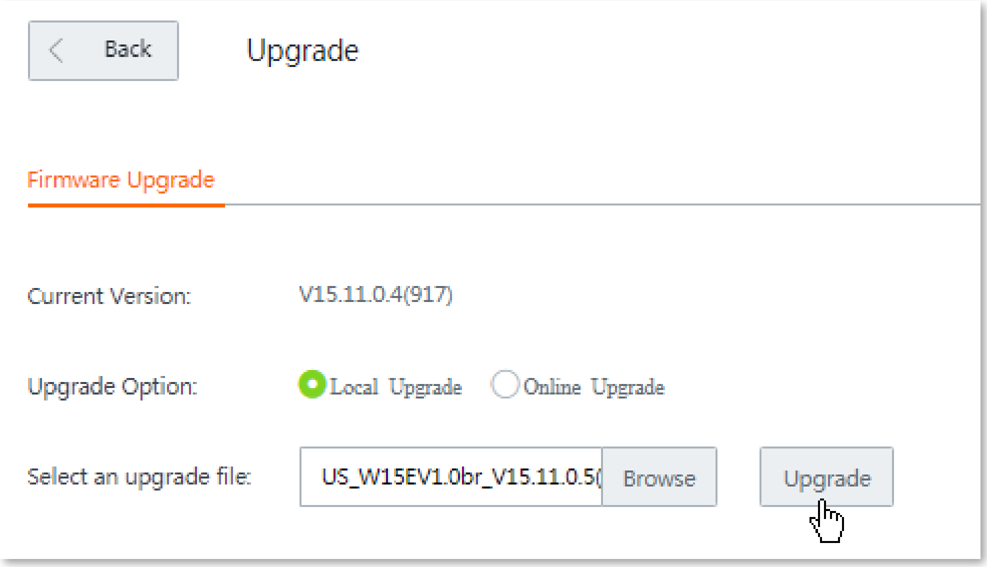
1. Visit http://www.tendacn.com, searching the **Model** in the searching bar to enter the product details page.
2. Locate the latest firmware, download it to your computer, and unzip it.

Step 2 Log in to the web UI of your router, click **Maintenance** > **Upgrade** to enter the configuration page.

Step 3 Set **Upgrade Option** to **Local Upgrade**.

Step 4 Click **Browse**, select and upload the firmware that has been downloaded to your computer.

Step 5 Click **Upgrade**. Wait until the progress bar completes.



Current Version: V15.11.0.4(917)

Upgrade Option: ● Local Upgrade ○ Online Upgrade

Select an upgrade file: US_W15EV1.0br_V15.11.0.5(Browse

NOTE

If upgrade does not apply, reset the router. Back up your configurations properly before reset.

12.2.3 Upgrading the rotuer automatically

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 latest version. If you want to upgrade the firmware, click **Upgrade**. Then the system will download the firmware and the router upgrades the firmware automatically.

12.3 Reset

12.3.1 Overview

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

The router supports two resetting methods:

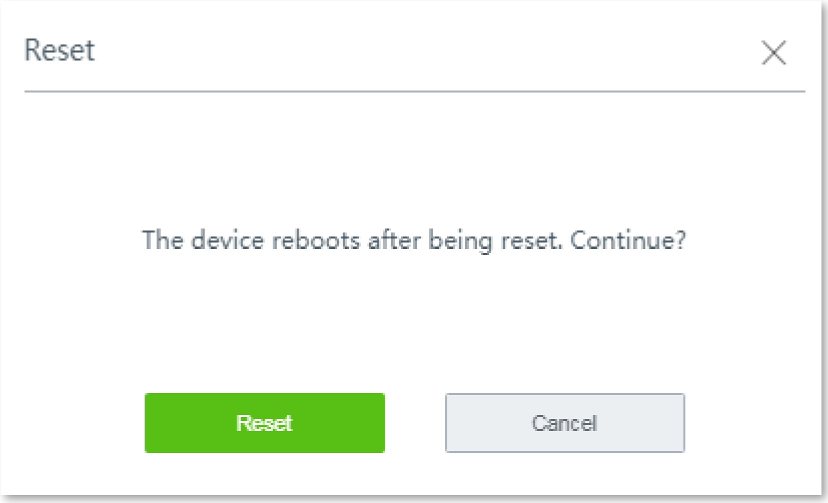
- Resetting the router using web UI.
- Resetting the router using the Reset button.

12.3.2 Resetting the router using web UI

TIP

- Resetting the router deletes all your current configurations and you need to reconfigure the router to access the internet.
- If it is necessary to reset the router, Backing up your current configuration first.
- When resetting, do not power off the router.

Choose **Maintenance > Reset**, and follow the on-screen instruction to reset the device.



Reset

The device reboots after being reset. Continue?

12.3.3 Resetting the router using the Reset button

With the SYS LED indicator blinking, hold down the **Reset** button using a paper clip for about 8 seconds, and then release it. When all LED indicators light up, the router is reset to the factory settings successfully.

12.4 Password manager

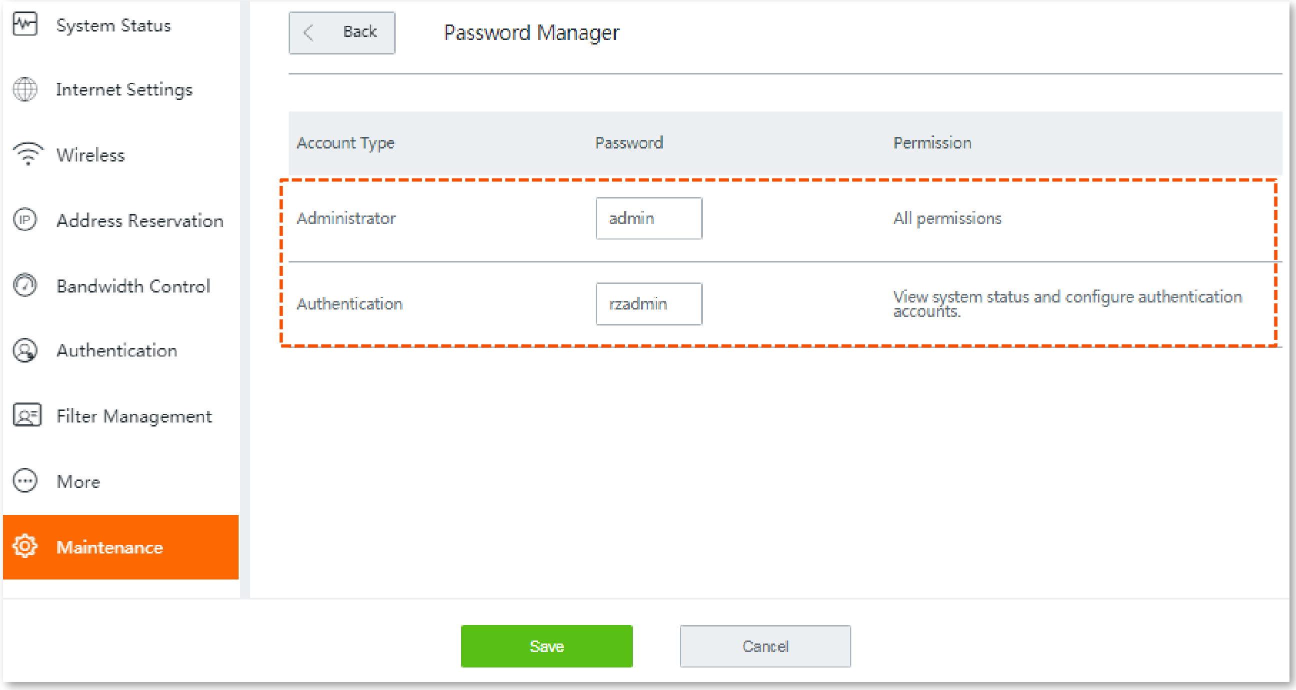
12.4.1 Overview

The router supports two account types: **Administrator** and **Authentication**. The difference between them is their access permission.

The **Administrator** account enjoys all access permission. Password for **Administrator** account is the login password you set during initial setup. You can view and modify it here.

The **Authentication** account only has permission for accessing **System Status** and **Authentication** modules. The default password for this account is **rzadmin**. You can view and modify it here.

To enter the configuration page, choose **Maintenance > Password Manager**.



Account Type	Password	Permission
Administrator	admin	All permissions
Authentication	rzadmin	View system status and configure authentication accounts.

12.4.2 Modifying login password

Step 1 Click **Maintenance > Password Manager** to enter the configuration page.

Step 2 Locate the account type and modify the password.

Step 3 Click **Save** on the bottom of the page to apply your settings.

---- End

Then you will be redirected to the login page. Enter the password corresponding to the administrator account you set just now, and click **Login** to log in to the router.

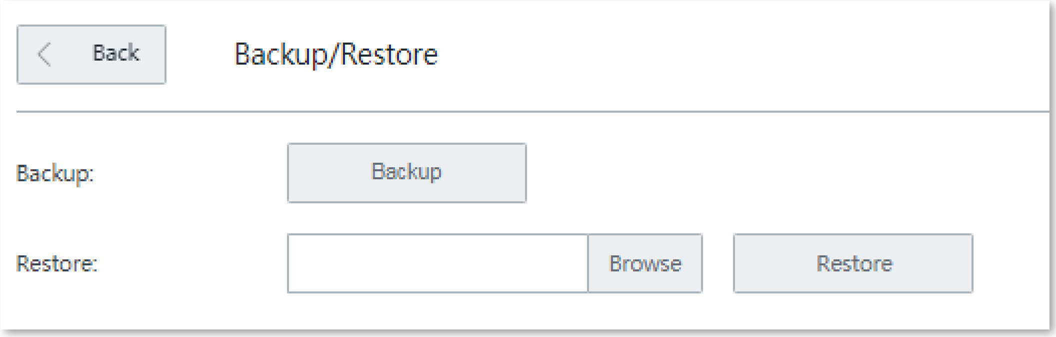
12.5 Backup/Restore

12.5.1 Overview

The **backup** function is used to export the current configuration of the router to your computer. The **restore** function is used to import a configuration file to the router.

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

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



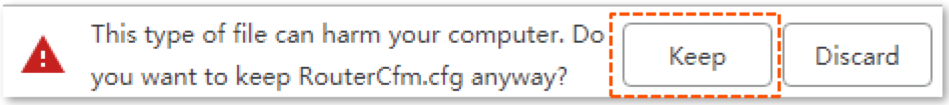
12.5.2 Backing up your current configuration

Step 1 Click **Maintenance** > **Backup/Restore** to enter the configuration page.

Step 2 Click **Backup**. The system exports the configuration file to your local computer.

TIP

If the following warning message appears, click **Keep**.


This type of file can harm your computer. Do you want to keep RouterCfm.cfg anyway?

---- End

12.5.3 Restoring your previous configuraiton

Step 1 Click **Maintenance** > **Backup/Restore** to enter the configuration page.

Step 2 Click **Browse**, and upload the configuration file ending with **.cfg**.

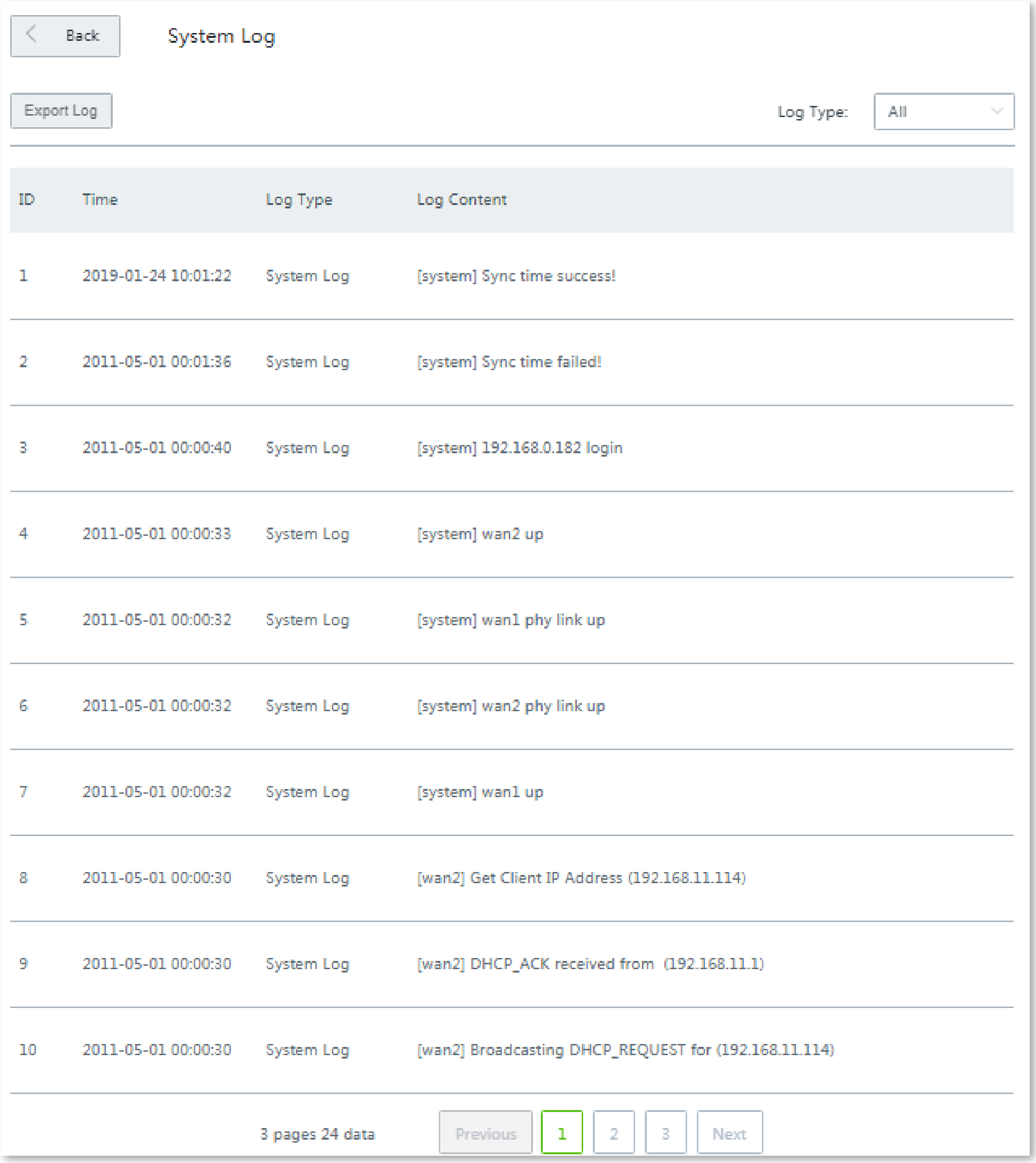
Step 3 Click **Restore** and follow the on-screen instruction to restore the configuration.

---- End

12.6 System log

System logs record information about system running status and the operation you performed on it. When system malfunctions occur, you can use system log for troubleshooting.

To enter the configuration page, click **Maintenance** > **System Log**.



Log Type: All

ID	Time	Log Type	Log Content
1	2019-01-24 10:01:22	System Log	[system] Sync time success!
2	2011-05-01 00:01:36	System Log	[system] Sync time failed!
3	2011-05-01 00:00:40	System Log	[system] 192.168.0.182 login
4	2011-05-01 00:00:33	System Log	[system] wan2 up
5	2011-05-01 00:00:32	System Log	[system] wan1 phy link up
6	2011-05-01 00:00:32	System Log	[system] wan2 phy link up
7	2011-05-01 00:00:32	System Log	[system] wan1 up
8	2011-05-01 00:00:30	System Log	[wan2] Get Client IP Address (192.168.11.114)
9	2011-05-01 00:00:30	System Log	[wan2] DHCP_ACK received from (192.168.11.1)
10	2011-05-01 00:00:30	System Log	[wan2] Broadcasting DHCP_REQUEST for (192.168.11.114)

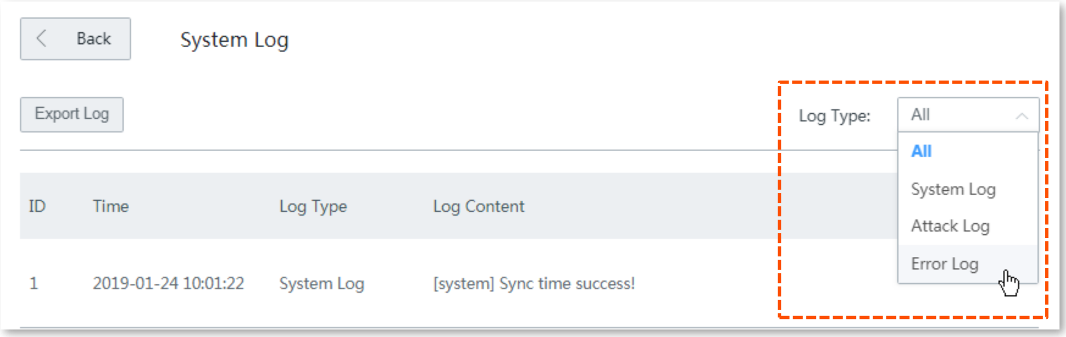
3 pages 24 data

12.6.1 Viewing system log

TIP

- System logs will be cleared each time the router reboots or resets.
- A maximum of **300** logs will be recorded.
- The system only keeps 300 logs that are generated the most recently.

The router records three log types: **System Log**, **Attack Log**, and **Error Log**. You can view all logs or filter the logs to view as needed.

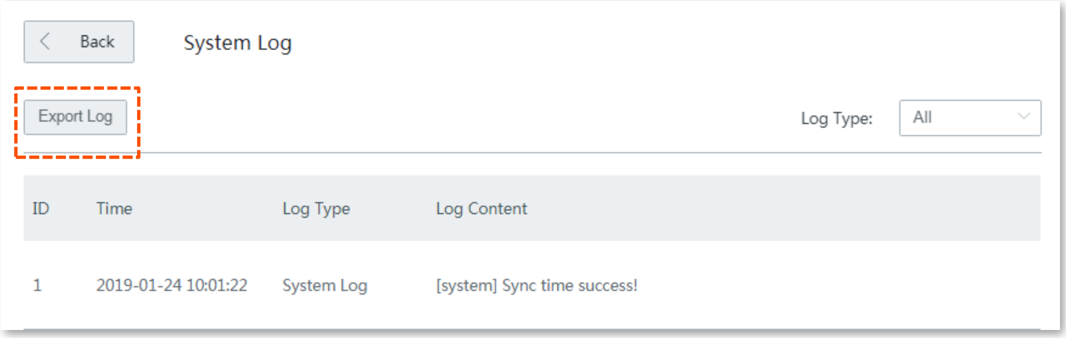


Log Type: All

ID	Time	Log Type	Log Content
1	2019-01-24 10:01:22	System Log	[system] Sync time success!

12.6.2 Exporting system log

Click **Export Log**, the log file will be downloaded to your local computer.



Log Type: All

ID	Time	Log Type	Log Content
1	2019-01-24 10:01:22	System Log	[system] Sync time success!

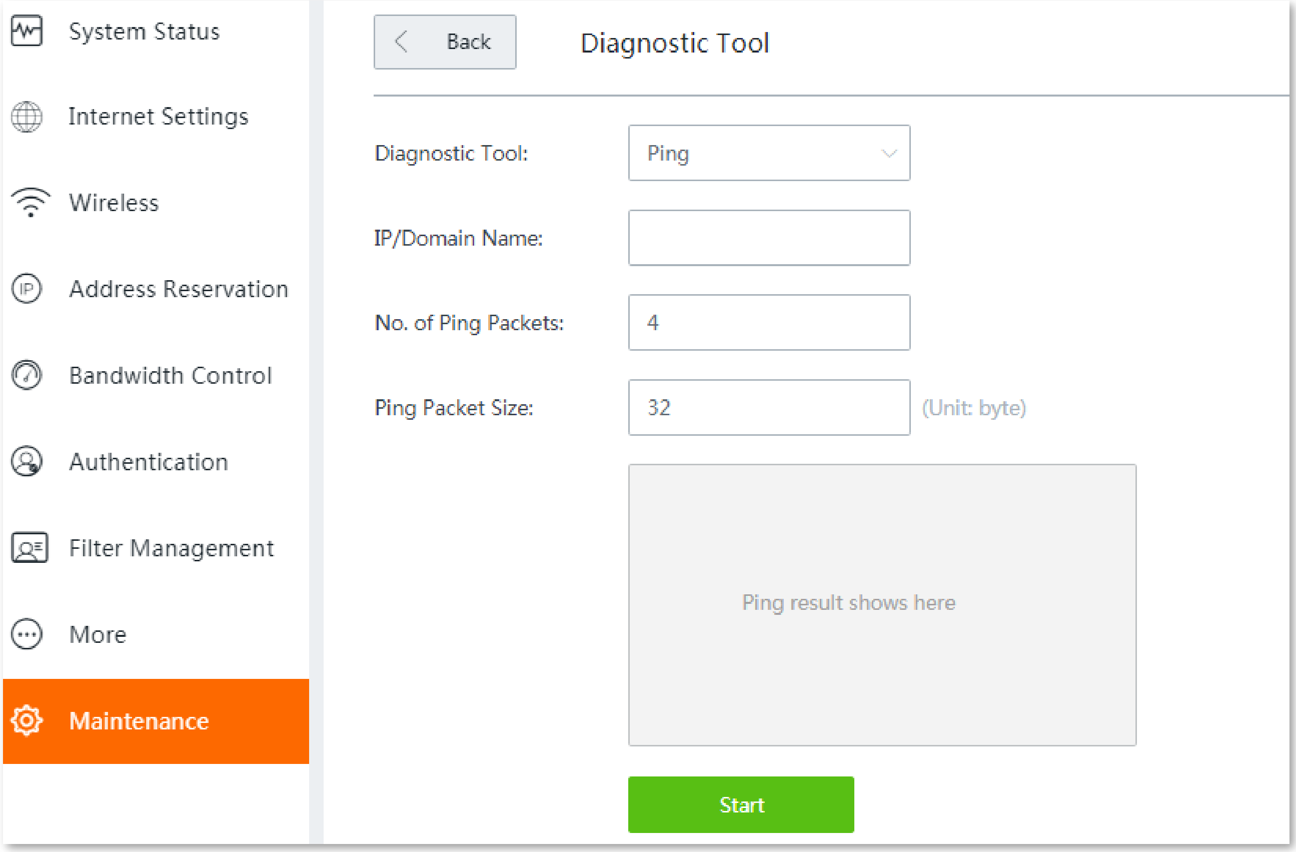
12.7 Diagnostic tool

12.7.1 Overview

You can execute Ping/Traceroute command on this page.

- **Ping**: Used to check whether the connection is correct and the connection quality.
- **Traceroute**: Used to detect the route from the bridge to the destination IP address or domain name.

To access the configuration page, click **Maintenance** > **Diagnosis Tool**.



Diagnostic Tool: Ping

IP/Domain Name:

No. of Ping Packets: 4

Ping Packet Size: 32 (Unit: byte)

Ping result shows here

12.7.2 Executing Ping command to detect connection quality

Assume that:

You need to detect the connectivity between the router and the **Bing** website.

Step 1 Click **Maintenance** > **Diagnosis Tool** to enter the configuration page.

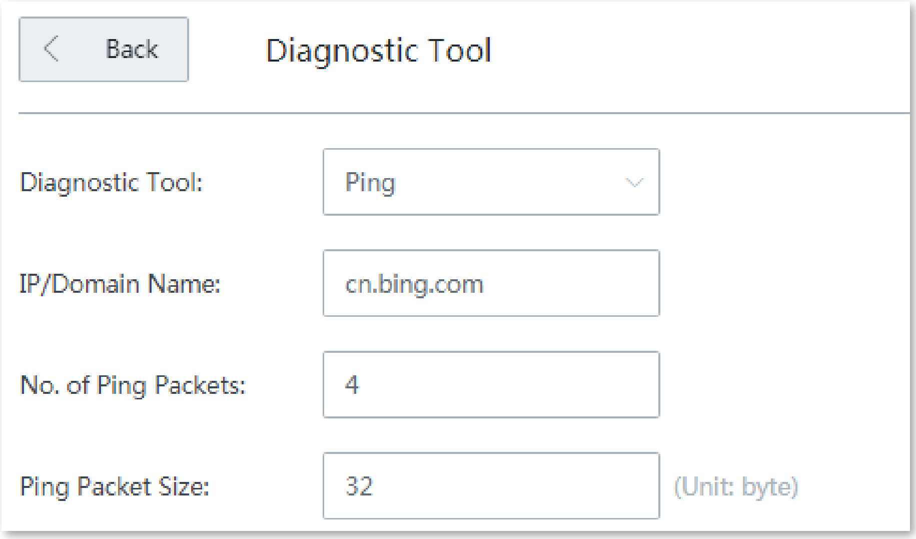
Step 2 Select **Ping** from the drop-down list menu of the **Tools**.

Step 3 Enter the IP address or domain name of the ping target, which is **cn.bing.com** in this example.

Step 4 Set **Number of Ping Packets** as required.

Step 5 Set **Ping Packet Size** as required.

Step 6 Click **Start**.



Diagnostic Tool: Ping

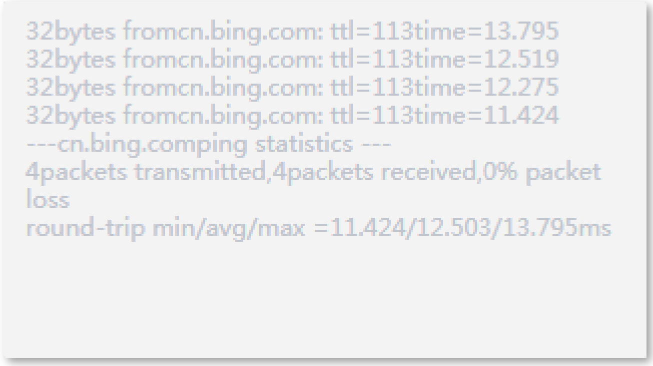
IP/Domain Name: cn.bing.com

No. of Ping Packets: 4

Ping Packet Size: 32 (Unit: byte)

---- End

Wait a moment. The ping result will be displayed in the result box. See the following figure:



```
32bytes fromcn.bing.com: ttl=113time=13.795
32bytes fromcn.bing.com: ttl=113time=12.519
32bytes fromcn.bing.com: ttl=113time=12.275
32bytes fromcn.bing.com: ttl=113time=11.424
---cn.bing.comping statistics ---
4packets transmitted,4packets received,0% packet
loss
round-trip min/avg/max =11.424/12.503/13.795ms
```

12.7.3 Executing Traceroute command to detect the route selection

Assume that:

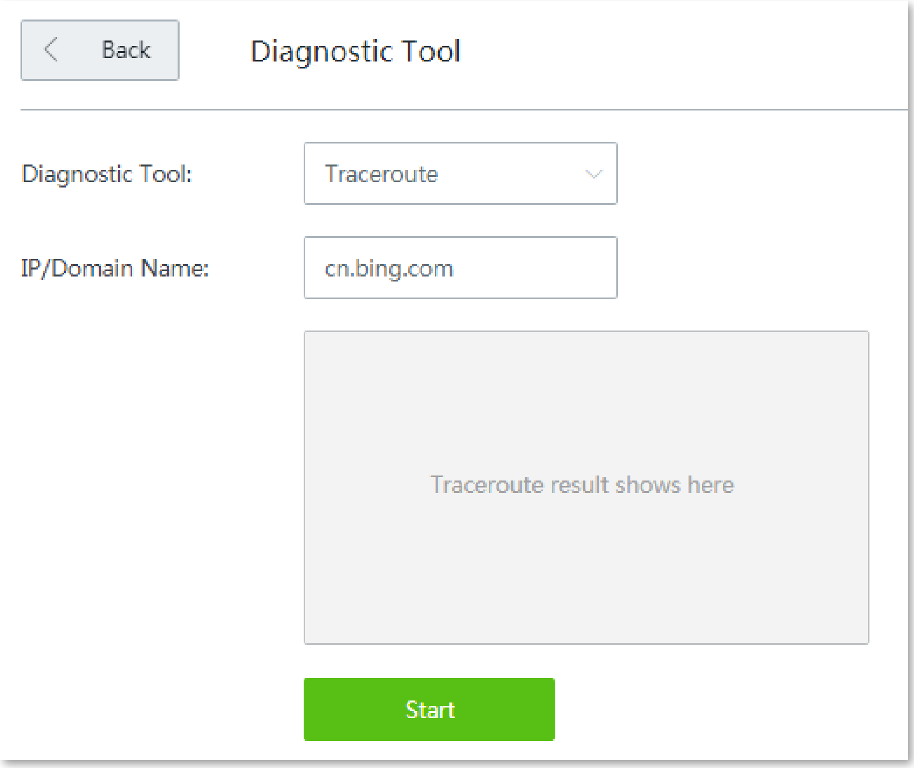
You need to detect the path from the router to **Bing** website.

Step 1 Click **Maintenance** > **Diagnosis Tool** to enter the configuration page.

Step 2 Select **Traceroute** from the drop-down list menu of the **Tools** menu.

Step 3 Enter the IP address or domain name of the traceroute target, which is **cn.bing.com** in this example.

Step 4 Click **Start**.

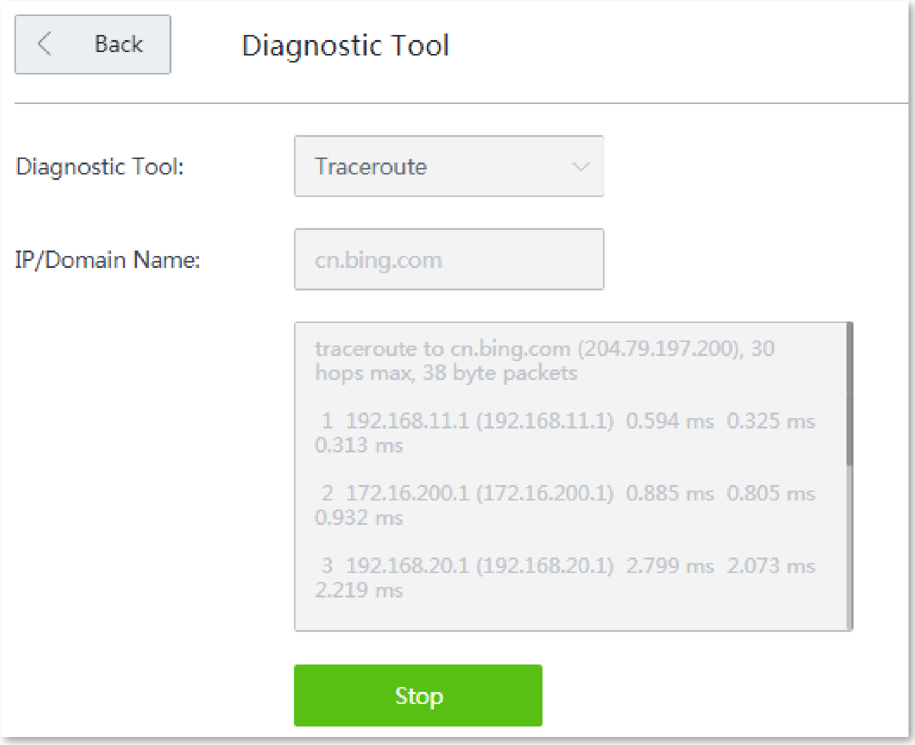


Diagnostic Tool: Traceroute

IP/Domain Name: cn.bing.com

---- End

Wait a moment. The traceroute result will be displayed in the result box. See the following figure:



Diagnostic Tool: Traceroute

IP/Domain Name: cn.bing.com

```
traceroute to cn.bing.com (204.79.197.200), 30 hops max, 38 byte packets

 1  192.168.11.1 (192.168.11.1)  0.594 ms  0.325 ms  0.313 ms

 2  172.16.200.1 (172.16.200.1)  0.885 ms  0.805 ms  0.932 ms

 3  192.168.20.1 (192.168.20.1)  2.799 ms  2.073 ms  2.219 ms
```

Click **Stop** to end the process as needed.

12.8 System time

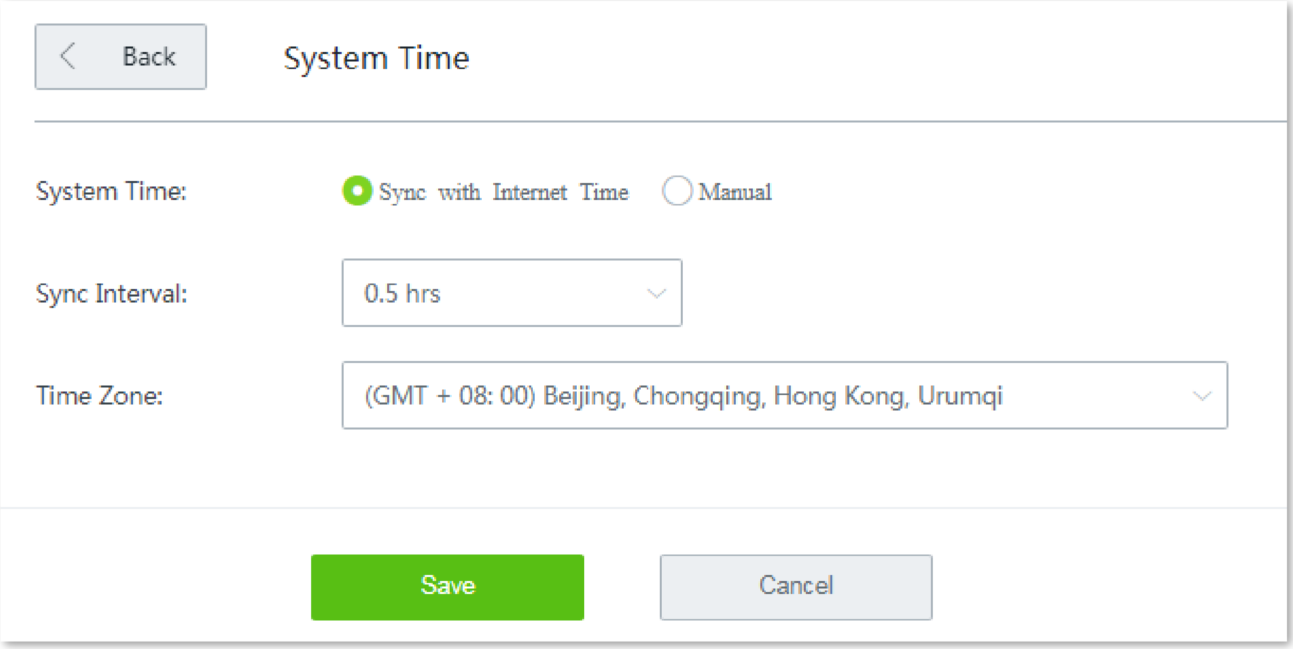
12.8.1 Overview

This function is used to set the system time of your router. To make the time-related functions effective, ensure that the system time of the router is set correctly.

The router supports:

- Synchronizing with internet time (default)
- Setting system time manually

To access the configuration page, click **Maintenance** > **System Time**. See the following figure:



System Time

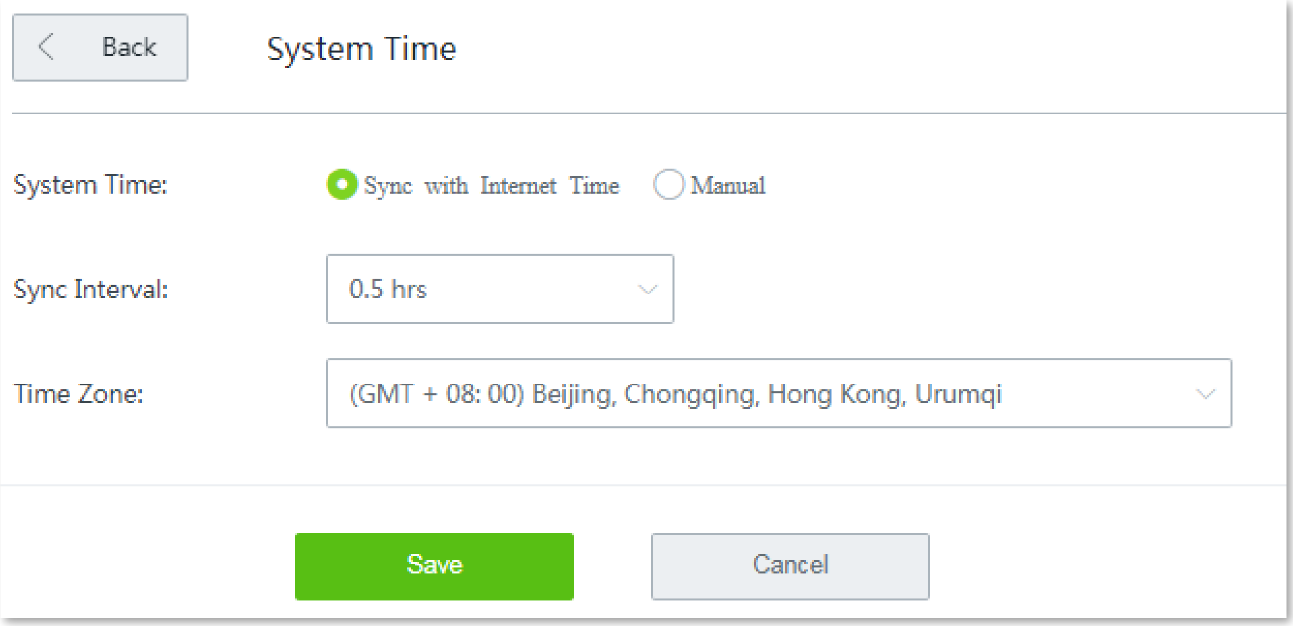
System Time: ● Sync with Internet Time ○ Manual

Sync Interval: 0.5 hrs

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

12.8.2 Synchronizing with internet time

With this method, the router automatically synchronizes its system time with the network time server (NTS). As long as the router is connecting to the internet, the system time is correct.



System Time

System Time: ● Sync with Internet Time ○ Manual

Sync Interval: 0.5 hrs

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

Parameter description

Parameter	Description
Sync Interval	It specifies an interval at which the router synchronizes its system time with the time server on the internet. By default, the router performs synchronization every **0.5** hours.
Time Zone	It specifies the time zone where the router is deployed.

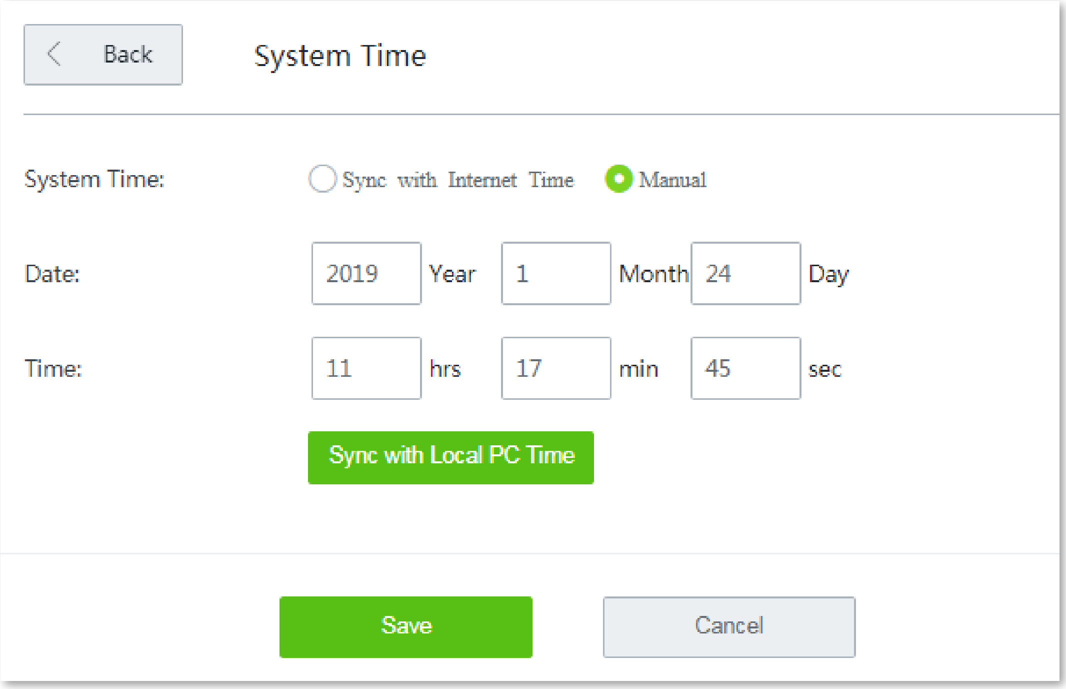
After configuration, navigate to the System status page to check whether it is synchronized.

12.8.3 Setting system time manually

With this method, you can manually specify a system time for the router. When **Manual** option is selected**,** the related parameters are shown as follows.

TIP

With this method, you need to manually reconfigure the system time each time the router reboots.



System Time: ○ Sync with Internet Time ● Manual

Date: 2019 Year 1 Month 24 Day

Time: 11 hrs 17 min 45 sec

Parameter description

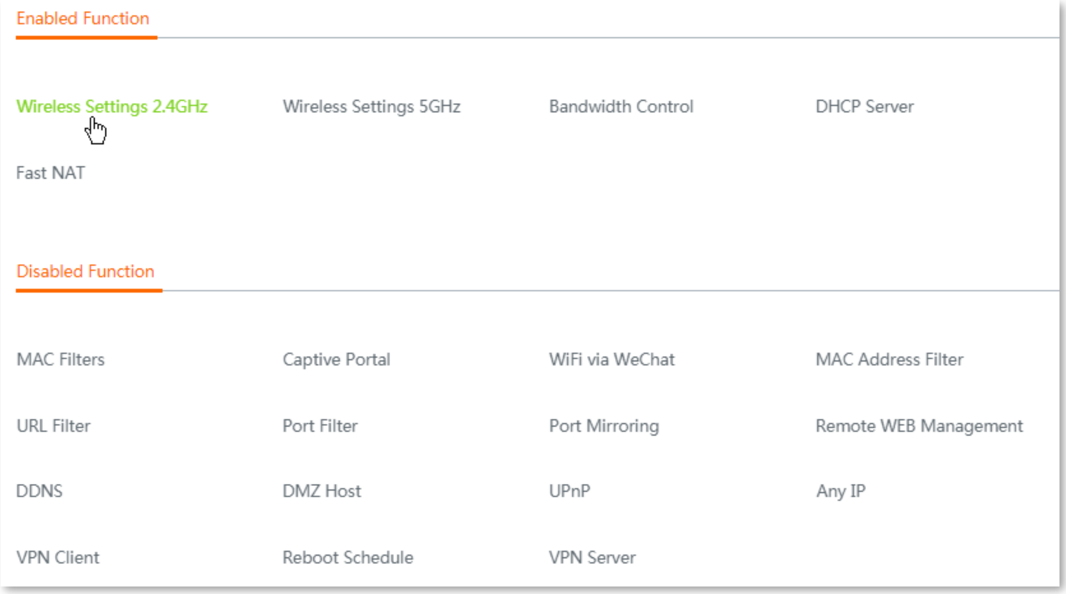
Parameter	Description
Date	Manually enter the date and time as needed.
Time	
Sync with Local PC Time	It allows you to synchronize the system time of the router with the system time of the management computer. Click this button, the router auto-fills the system time of your management computer.

After configuration, navigate to the System status page to check whether it is synchronized.

12.9 Function center

The function center groups all functions of the router into **Enabled Function** and **Disabled Function**, giving you a clearly insight into the functions that are enabled or disabled.

In addition, move the mouse pointer to a specific function and click it, you will be taken to the corresponding configuration page.



Appendixes

A.1 FAQ

Q1: I cannot log in to the web UI of the router with tendawifi.com. What should I do?

A1: Try the following solutions:

- Start a web browser, and enter **tendawifi.com** or **192.168.0.1** in the **address bar** (not searching bar).

  For configuration using a **smart phone**, ensure that:

  (1) Your smart phone has connected to the wireless network of the router.

  (2) Its **Mobile Data** function is disabled.

  For configuration using a **tethered computer**, ensure that:

  Your computer has securely connected to the LAN port of the router, and the corresponding activity LED indicator lights up.

- Reset the router.

Q2: My computer or smart phone cannot access the internet after configuration. What should I do?

A2: Try the following solutions:

- Log in to the web UI of the router, and check if the router is connected to the internet properly. If not, navigate to the **Internet Settings** page, and follow the on-screen instructions to solve it.
- If the wireless network is inaccessible:

  (1) Check if your wireless clients have been connected to the correct SSID.

  (2) If they have been connected to the correct SSID, but still cannot access the internet, forget this WiFi network, then try reconnecting to it.

- If the computer tethered to the router cannot access the internet, ensure that the computer is set to **Obtain an IP address automatically** and **Obtain DNS server address automatically**.
- Log in to the web UI of the router, and check if your clients are added into the blacklist. If yes, unblock them.
- If the problem persists, consult your ISP.

Q3: Why cannot my wireless clients scan the wireless signals of the router?

A3: Check if the **WiFi** LED indicator of the router lights up. If not, connect your computer to a LAN port of the router using an Ethernet cable, log in to its web UI, choose **Wireless > Wireless Settings**, and try the following solutions:

- Check if the wireless network of the router is enabled. If not, enable it and click **Save**. Then rescan using your smart phone.

- If the wireless network is already enabled, click **Expand**, and check if the **Hide SSID** is enabled. If yes, disable it, and click **Save**. Then rescan using your smart phone.
- By default, the 2.4 GHz and 5 GHz SSIDs of the router are unified. To customize the 5 GHz wireless network of the router separately, disable the **Unify 2.4&5 GHz SSID,** and the 5 GHz configuration part appears.
- Only 5 GHz-compliant wireless clients can scan the 5 GHz SSID.

A.2 Specification

Product Model	W15E	W18E
Max. clients	30	50
CPU	650 MHz	775 MHz
Internal storage	128 MB	128 MB
FLASH	8 MB	8 MB
Interface	4*10/100Mbps auto-negotiation RJ45 port	4*10/100/1000 Mbps auto-negotiation RJ45 port
LED indicator	1*SYS, 1*WiFi, 5*RJ45 activity	1*SYS, 1*WiFi, 5*RJ45 activity
Button	1*Reset	1*Reset
Operating environment	Operating temperature: 0℃ ~ 40℃ Operating humidity: (10 ~ 90) %RH, non-condensing	Operating temperature: 0℃ ~ 40℃ Operating humidity: (10 ~ 90) %RH, non-condensing
Storage environment	Storage temperature: -40℃ ~ 70℃ Storage humidity:（5 ~ 90）%RH, non-condensing	Storage temperature: -40℃ ~ 70℃ Storage humidity:（5 ~ 90）%RH, non-condensing
Power	9V⎓1A	12V⎓1A
Dimension (L x W x H)	220 mm×135 mm×30 mm	220 mm×135 mm×30 mm