



300 Mbps Wireless Router

User Guide

Legal Information

©2022 Hangzhou Hikvision Digital Technology Co., Ltd. All rights reserved.

About this Manual

The Manual includes instructions for using and managing the Product. Pictures, charts, images and all other information hereinafter are for description and explanation only. The information contained in the Manual is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version of this Manual at the Hikvision website (<https://www.hikvision.com/>).

Please use this Manual with the guidance and assistance of professionals trained in supporting the Product.

Trademarks

HIKVISION and other Hikvision's trademarks and logos are the properties of Hikvision in various jurisdictions. Other trademarks and logos mentioned are the properties of their respective owners.

Disclaimer

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THIS MANUAL AND THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, ARE PROVIDED "AS IS" AND "WITH ALL FAULTS AND ERRORS". HIKVISION MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY QUALITY, OR FITNESS FOR A PARTICULAR PURPOSE. THE USE OF THE PRODUCT BY YOU IS AT YOUR OWN RISK. IN NO EVENT WILL HIKVISION BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, OR INDIRECT DAMAGES, INCLUDING, AMONG OTHERS, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF DATA, CORRUPTION OF SYSTEMS, OR LOSS OF DOCUMENTATION, WHETHER BASED ON BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY, OR OTHERWISE, IN CONNECTION WITH THE USE OF THE PRODUCT, EVEN IF HIKVISION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR LOSS.

YOU ACKNOWLEDGE THAT THE NATURE OF THE INTERNET PROVIDES FOR INHERENT SECURITY RISKS, AND HIKVISION SHALL NOT TAKE ANY RESPONSIBILITIES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER-ATTACK, HACKER ATTACK, VIRUS INFECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, HIKVISION WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.

YOU AGREE TO USE THIS PRODUCT IN COMPLIANCE WITH ALL APPLICABLE LAWS, AND YOU ARE SOLELY RESPONSIBLE FOR ENSURING THAT YOUR USE CONFORMS TO THE APPLICABLE LAW. ESPECIALLY, YOU ARE RESPONSIBLE, FOR USING THIS PRODUCT IN A MANNER THAT DOES NOT INFRINGE ON THE RIGHTS OF THIRD PARTIES, INCLUDING WITHOUT LIMITATION, RIGHTS OF PUBLICITY, INTELLECTUAL PROPERTY RIGHTS, OR DATA PROTECTION AND OTHER PRIVACY RIGHTS. YOU SHALL NOT USE THIS PRODUCT FOR ANY PROHIBITED END-USES, INCLUDING THE DEVELOPMENT OR PRODUCTION OF WEAPONS OF MASS DESTRUCTION, THE DEVELOPMENT OR PRODUCTION OF CHEMICAL OR BIOLOGICAL WEAPONS, ANY ACTIVITIES IN THE CONTEXT RELATED TO ANY NUCLEAR EXPLOSIVE OR UNSAFE NUCLEAR FUEL-CYCLE, OR IN SUPPORT OF HUMAN RIGHTS ABUSES.

IN THE EVENT OF ANY CONFLICTS BETWEEN THIS MANUAL AND THE APPLICABLE LAW, THE LATTER PREVAILS.

Regulatory Information

FCC Information

Please take attention that changes or modification not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

FCC Compliance


This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

FCC Conditions

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.
2. This device must accept any interference received, including interference that may cause undesired operation.


EU Conformity Statement

 This product and - if applicable - the supplied accessories too are marked with "CE" and comply therefore with the applicable harmonized European standards listed under the Directive 2014/30/EU, the Directive 2014/35/EU, the Directive 2011/65/EU.

Hereby, Hikvision declares that the radio equipment type Wireless Router is in compliance with Directive 2014/53/EU. The full text of the EU declaration of conformity is available at the following internet address: <https://www.hikvision.com/europe/support/download/declaration-of-conformity/>

Model	Received frequency	Transmitted frequency	Bandwidth	Transmit power
DS-3WR3N	2400-2483.5 MHz	2400-2483.5 MHz	2.4 GHz: 20 MHz and 40 MHz	2.4 GHz:18.5 dBm

 2012/19/EU (WEEE directive): Products marked with this symbol cannot be disposed of as unsorted municipal waste in the European Union. For proper recycling, return this product to your local supplier upon the purchase of equivalent new equipment, or dispose of it at designated collection points. For more information see: www.recyclethis.info

 2006/66/EC (battery directive): This product contains a battery that cannot be disposed of as unsorted municipal waste in the European Union. See the product documentation for specific battery information. The battery is marked with this symbol, which may include lettering to indicate cadmium (Cd), lead (Pb), or mercury (Hg). For proper recycling, return the

battery to your supplier or to a designated collection point. For more information see: www.recyclethis.info

Industry Canada ICES-003 Compliance

This device meets the CAN ICES-3 (A)/NMB-3(A) standards requirements.

This device complies with Industry Canada licence-exempt RSS standard(s). Operation is subject to the following two conditions:

- (1) this device may not cause interference, and
- (2) this device must accept any interference, including interference that may cause undesired operation of the device.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radioexempts de licence. L'exploitation est autorisée aux deux conditions suivantes :

- (1) l'appareil ne doit pas produire de brouillage, et
- (2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

Under Industry Canada regulations, this radio transmitter may only operate using an antenna of a type and maximum (or lesser) gain approved for the transmitter by Industry Canada. To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (e.i.r.p.) is not more than that necessary for successful communication.

Conformément à la réglementation d'Industrie Canada, le présent émetteur radio peut fonctionner avec une antenne d'un type et d'un gain maximal (ou inférieur) approuvé pour l'émetteur par Industrie Canada. Dans le but de réduire les risques de brouillage radioélectrique à l'intention des autres utilisateurs, il faut choisir le type d'antenne et son gain de sorte que la puissance isotrope rayonnée équivalente (p.i.r.e.) ne dépasse pas l'intensité nécessaire à l'établissement d'une communication satisfaisante.

This equipment should be installed and operated with a minimum distance 20cm between the radiator and your body.




Cet équipement doit être installé et utilisé à une distance minimale de 20 cm entre le radiateur et votre corps.

Applicable Models

This guide applies to the model: DS-3WR3N.

Symbol Conventions

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

Symbol	Description
 Note	Provides additional information to emphasize or supplement important points of the main text.
 Caution	Indicates a potentially hazardous situation, which if not avoided, could result in equipment damage, data loss, performance degradation, or unexpected results.
 Danger	Indicates a hazard with a high level of risk, which if not avoided, will result in death or serious injury.

Safety Instructions

Before operating, read the operation instructions and precautions to be taken, and follow them to prevent accidents. The warning and danger items in other documents do not cover all the safety precautions that must be followed. They are only supplementary information, and the installation and maintenance personnel need to understand the basic safety precautions to be taken.

- Do not use the device in a place where wireless devices are not allowed.
- Please use the included power adapter.
- Mains plug is used as the disconnect device and shall remain readily operable.
- The power socket shall be installed near the device and easily accessible.
- Operating environment: Temperature: 0°C - 40°C; Humidity: (10% - 90%) RH, non-condensing; Storage environment: Temperature: -40°C - 70°C; Humidity: (5% - 90%) RH, non-condensing.
- Keep the device away from water, fire, high electric field, high magnetic field, and inflammable and explosive items.
- Unplug this device and disconnect all cables during lightning storms or when the device is unused for long periods.
- Do not use the power adapter if its plug or cord is damaged.
- If such phenomena as smoke, abnormal sound, or smell appear when you use the device, immediately stop using it and disconnect its power supply, unplug all connected cables, and contact the after-sales service personnel.

- Disassembling or modifying the device or its accessories without authorization voids the warranty, and might cause safety hazards.

TABLE OF CONTENTS

Chapter 1 Get to know your device	1
1.1 Overview.....	1
1.2 Appearance.....	1
1.2.1 LED indicator.....	1
1.2.2 Jack, ports, and button.....	3
1.3 Label.....	4
Chapter 2 Web UI	5
2.1 Log in to the web UI.....	5
2.2 Log out of the web UI.....	7
2.3 Web UI layout.....	8
2.4 Common element.....	9
Chapter 3 Status	10
3.1 View internet connection status.....	10
3.2 View online device information.....	15
3.3 View system information.....	16
Chapter 4 Route settings	18
4.1 Internet settings.....	18
4.1.1 Overview.....	18
4.1.2 Serve as a router.....	19
4.1.3 Serve as a WiFi extender.....	26
4.1.4 Serve as an AP.....	34
4.2 Wireless settings.....	40
4.2.1 WiFi on/off.....	40
4.2.2 WiFi name and password.....	40
4.2.3 Multi SSID and password.....	45
4.2.4 WiFi schedule.....	47
4.2.5 WPS.....	48
4.2.6 WiFi parameters.....	55
Chapter 5 Client management	57
5.1 Access control.....	57
5.1.1 Overview.....	57
5.1.2 Set the upload and download speed limit.....	59
5.1.3 Add the device to the blacklist.....	60
5.1.4 Remove the device from the blacklist.....	61
5.2 Parental control.....	62
5.2.1 Overview.....	62
5.2.2 An example of configuring parental control.....	64
Chapter 6 Advanced	66
6.1 MAC address filter.....	66
6.1.1 Overview.....	66
6.1.2 Only allow specified device to access the internet.....	67
6.2 IP-MAC binding.....	69
6.2.1 Overview.....	69
6.2.2 Assign fixed IP addresses to LAN clients.....	69
6.3 Port mapping.....	71

6.3.1 Overview	71
6.3.2 Enable internet users to access LAN resources using an IP address.....	72
6.4 DDNS.....	77
6.4.1 Overview	77
6.4.2 Enable internet users to access LAN resources using a domain name	78
6.5 DMZ host.....	83
6.5.1 Overview	83
6.5.2 Enable internet users to access LAN resources using an IP address.....	84
6.6 PING WAN	87
6.7 UPnP	88
6.8 AP Isolation	89
Chapter 7 Administration	90
7.1 Login password	90
7.2 WAN parameters	91
7.2.1 Change the MTU value.....	91
7.2.2 Clone WAN MAC address.....	92
7.2.3 Change the WAN speed	94
7.3 LAN parameters	95
7.4 Remote web management	97
7.4.1 Overview	97
7.4.2 Internet users access the web UI	98
7.5 Date & time.....	100
7.6 Device management	101
7.6.1 Reboot the router	101
7.6.2 Reset the router	102
7.6.3 Backup/restore configuration	104
7.6.4 Export system log.....	106
7.6.5 Upgrade firmware.....	106
7.6.6 Automatic maintenance	109
Appendix A	110
A.1 Configuring the computer to obtain an IPv4 address automatically	110
A.1.1 Windows 10	110
A.1.2 Windows 8	113
A.1.3 Windows 7	115
A.2 Default parameters.....	117
A.3 Acronyms and abbreviations	118

Chapter 1 Get to know your device

1.1 Overview

Hikvision wireless N300 home router is an eco-friendly wireless router dedicated to small and medium apartments. With 4 external 5 dBi antennas and built-in Qualcomm WiFi chip, it works perfectly with popular mobile phones and blanks your home with a reliable and stable internet connection. The WISP mode allows you to extend your existing WiFi network with one single step. In addition, the WiFi schedule function helps save power consumption by setting your router to turn on and off the WiFi network regularly.

1.2 Appearance

1.2.1 LED indicator



Figure 1-1 LED indicator

Table 1-1 LED indicator description

LED indicator	Status	Description
SYS	Solid on	The system is working properly.
	Off	The system is faulty.
WLAN	Solid on	The WiFi network is enabled.
	Blinking	Data is being transmitted wirelessly.
	Off	The WiFi network is disabled.
1, 2, 3	Solid on	The corresponding LAN port is connected properly, but no data is being transmitted over the LAN port.
	Blinking	The corresponding LAN port is connected properly, and data is being transmitted over the corresponding LAN port.
	Off	The corresponding port is disconnected or improperly connected.
WAN	Solid on	The corresponding WAN port is connected properly, and data is being transmitted over the corresponding WAN port.
	Blinking	Data is being transmitted over the WAN port.
	Off	The WAN port is disconnected or improperly connected.

1.2.2 Jack, ports, and button

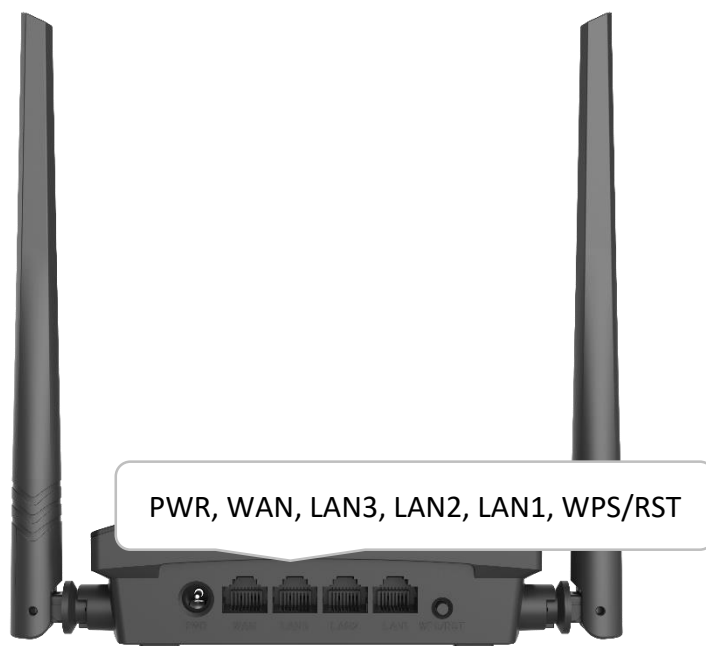


Figure 1-2 Jack, ports, and button

Table 1-2 Jack, ports and button description

Jack/port/button	Description
PWR	Power jack Used to power on the router (with the included power adapter).
WAN	10/100 Mbps auto-negotiation WAN port. Used to connect to the external network.
LAN3, LAN2, LAN1	10/100 Mbps auto-negotiation LAN port. Used to connect to computers, and switches.
WPS/RST	Used for WPS negotiation or reset. <ul style="list-style-type: none"> ● WPS: Press the WPS/RST button for 1 to 3 seconds, and enable the WPS function of another WPS-enabled device within 2 minutes to establish a WPS connection. ● RST: When the router completes startup, hold down the WPS/RST button for about 8 seconds, and then release it when all the LED indicators blink once. The router is reset successfully.

1.3 Label

The bottom label shows the login IP address, SSID, MAC address, and serial number (SN) of the router. See the following figure.

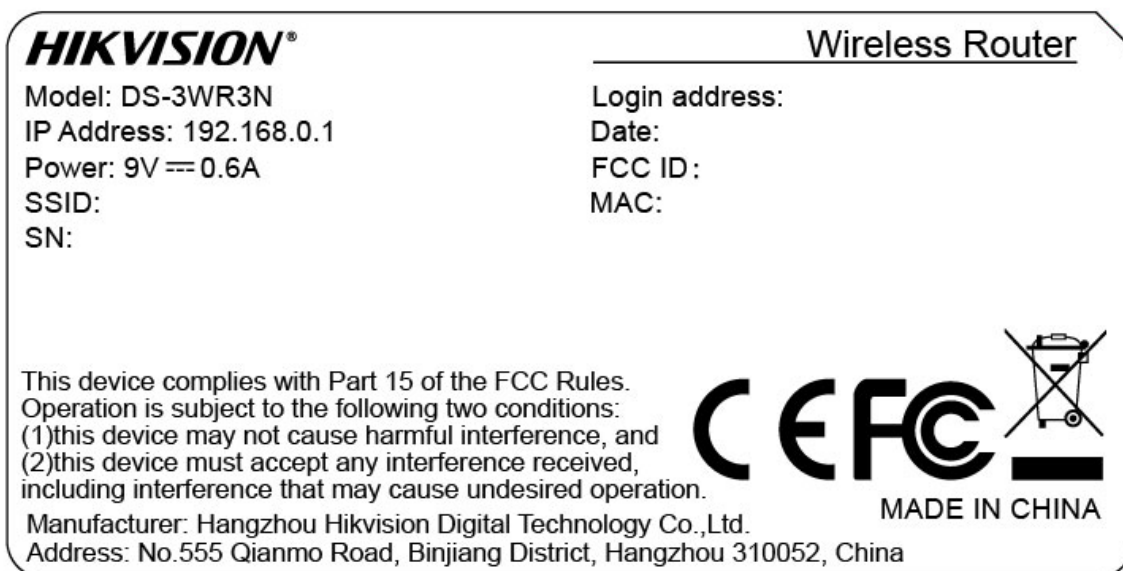


Figure 1-3 Label

Login address: It is the domain name used to log in to the web UI of the router.

IP Address: It is the default address used to log in to the web UI of the router.

SSID: It specifies the default WiFi name of the router.

SN: It is required if you need technical assistance.

MAC: It specifies the MAC address of the router.

Chapter 2 Web UI

2.1 Log in to the web UI

Step 1 Connect your smartphone to the WiFi network of the router, or connect your computer to a LAN port of the router.

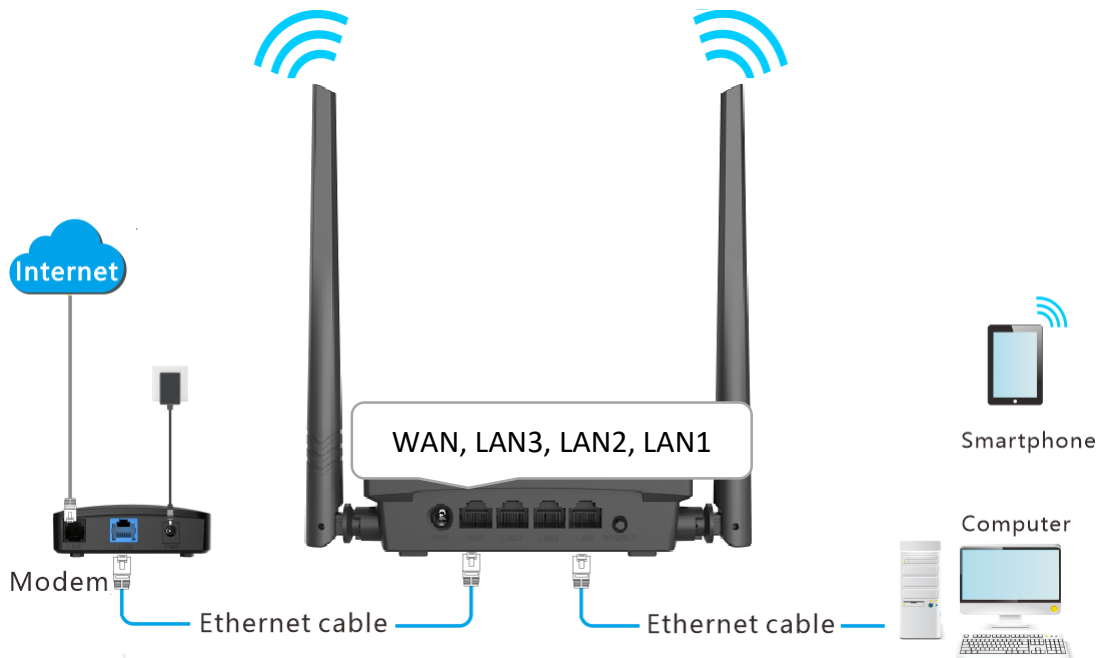


Figure 2-1 Connect your device to the router

Step 2 Launch a web browser on the device connected to the router, and visit **<http://hikvisionwifi.local>**.

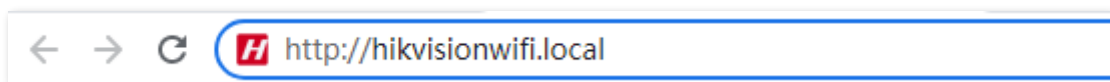


Figure 2-2 Visit the domain name of the router

The following page appears.

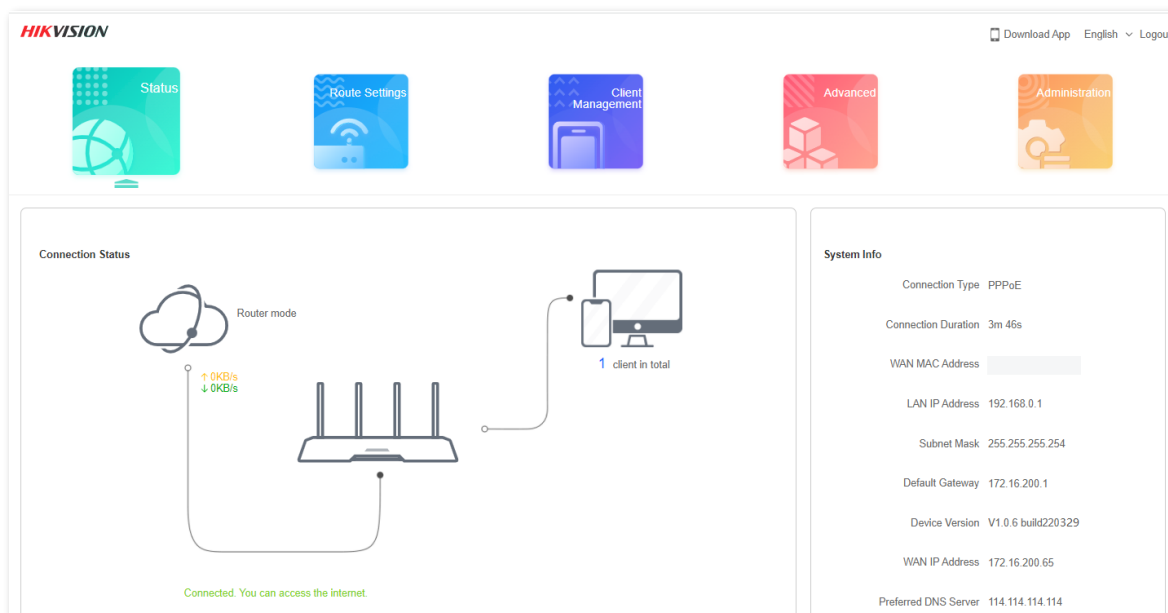


Figure 2-3 Web UI

Note

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

- Ensure that the router is powered on properly.
- If you are using a computer to access the page, check whether the computer obtains an IP address automatically. Refer to [A.1 Configuring the computer to obtain an IPv4 address automatically](#).
- If you are using a smartphone to access the page, ensure that your cellular network is disabled.
- [Reset the router](#) and log in to the web UI of the router.

2.2 Log out of the web UI

If you log in to the web UI of the router and perform no operation within 5 minutes, the router logs you out automatically. You can also log out by clicking **Logout** in the upper right corner of the web UI.

2.3 Web UI layout

The web UI of the router consists of two parts, including the navigation bar and the configuration area. See the following figure.

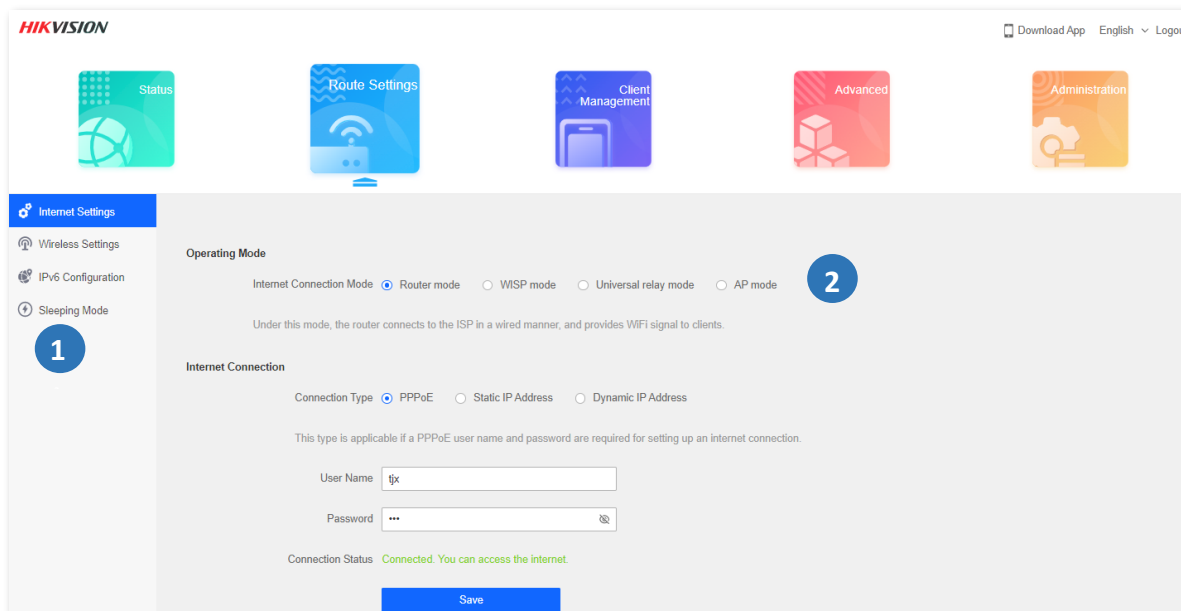


Figure 2-4 Web UI layout

Note

The functions and parameters shown in gray indicate that the functions are not supported or cannot be modified.


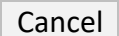
Table 2-1 Navigation bar and configuration area description

SN	Name	Description
1	Navigation bar	It is used to show the function menu of the router. Users can select functions in the navigation bar and the configuration appears in the configuration area.
2	Configuration area	It is used to modify or view your configurations.

2.4 Common element

The common elements used on the web UI are as follows.

Table 2-2 Common element description

Common element	Description
	It is used to save the current configurations and enable them to take effect.
	It is used to cancel the current configurations and restore the previous settings.

Chapter 3 Status

Log in to the web UI of the router and choose **Status** to enter the page. On this page, you can:

- [View internet connection status](#)
- [View online device information](#)
- [View system information](#)

3.1 View internet connection status

You can view the internet connection status on this page.

Procedures:

Step 1 Launch a web browser on a device connected to the router and visit **<http://hikvisionwifi.local>** to log in to the web UI of the router.

Step 2 Navigate to **Status > Connection Status**.

When the internet and the router are connected and **Connected. You can access the internet.** is shown as below, the router is connected to the internet successfully and you can access the internet via the router.

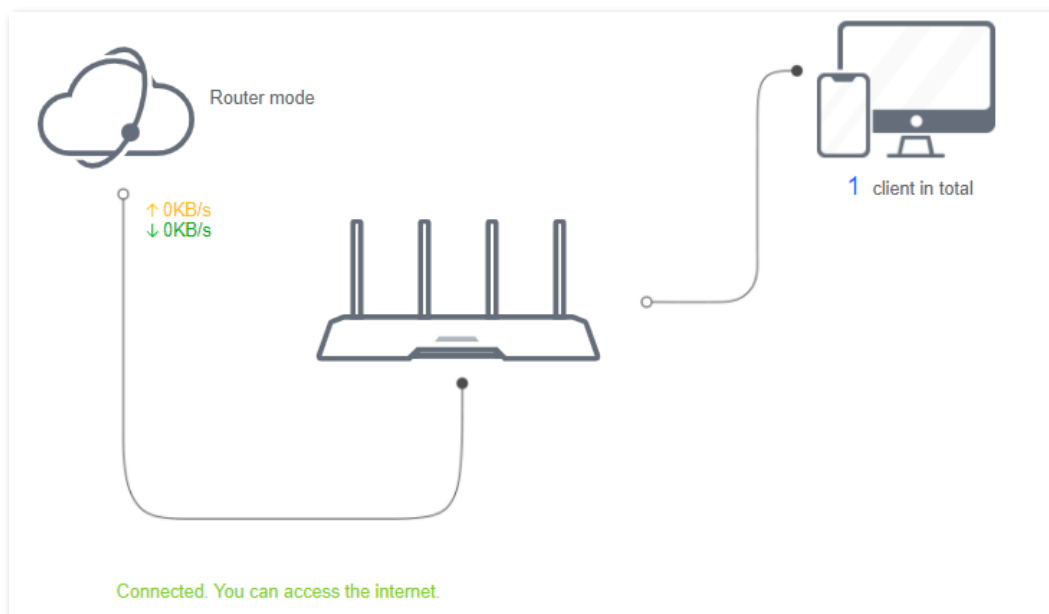


Figure 3-1 Internet connection status

When a red cross and "**Disconnected**" are shown between the internet and the router, and **WAN port disconnected. Please connect an Ethernet cable with Internet connectivity to the port.** is shown on the page, it indicates that the Ethernet cable is not connected properly. Please ensure that the Ethernet cable is connected properly.

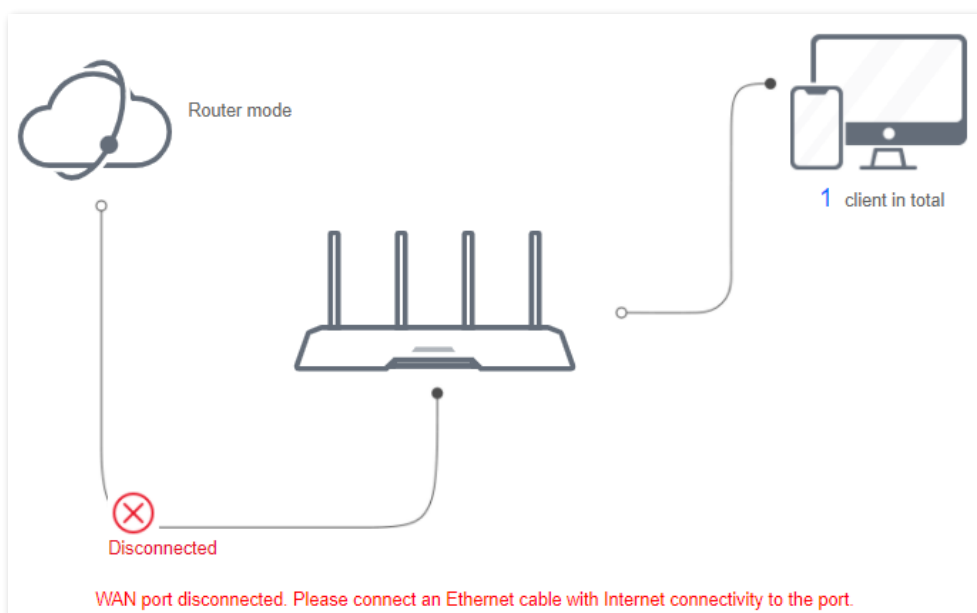


Figure 3-2 Internet connection status

When a red cross and "Disconnected" are shown between the internet and the router, and **Failed. Please confirm your user name and password and try again.** is shown on the page, it indicates that the user name and password you entered were incorrect. Please navigate to the **Internet Settings** page to try again.

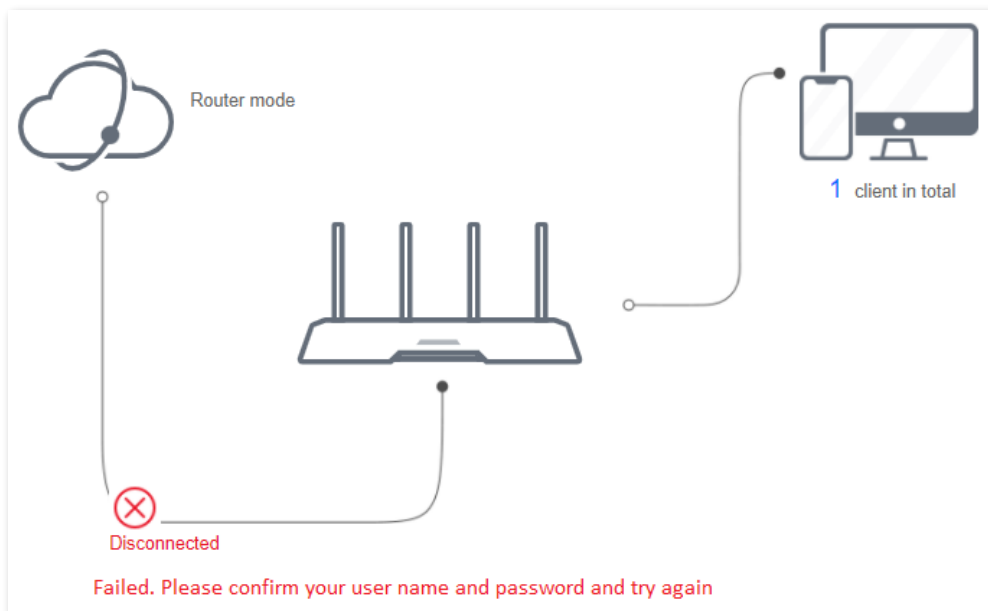


Figure 3-3 Internet connection status

 **Note**

Please consider the following tips when entering the username and password:

- Pay attention to case sensitivity, such as "Z" and "z".
- Pay attention to similar letters and numbers, such as "l" and "1".
- Ensure the completeness of account parameters, such as "0755000513@163.gd", rather than "0755000513"

If the problem persists, contact your ISP.

When a red cross and “**Disconnected**” are shown between the internet and the router, and **Error: No response from the remote server. Please contact your ISP.** is shown on the page, try the following solutions:

- Ensure that the Ethernet cable is connected properly.
- Ensure that you choose the proper connection type (Contact your ISP for any doubt about the connection type).
- Power off the router and wait for several minutes, then power it on and try again.

If the problem persists, consult your ISP.

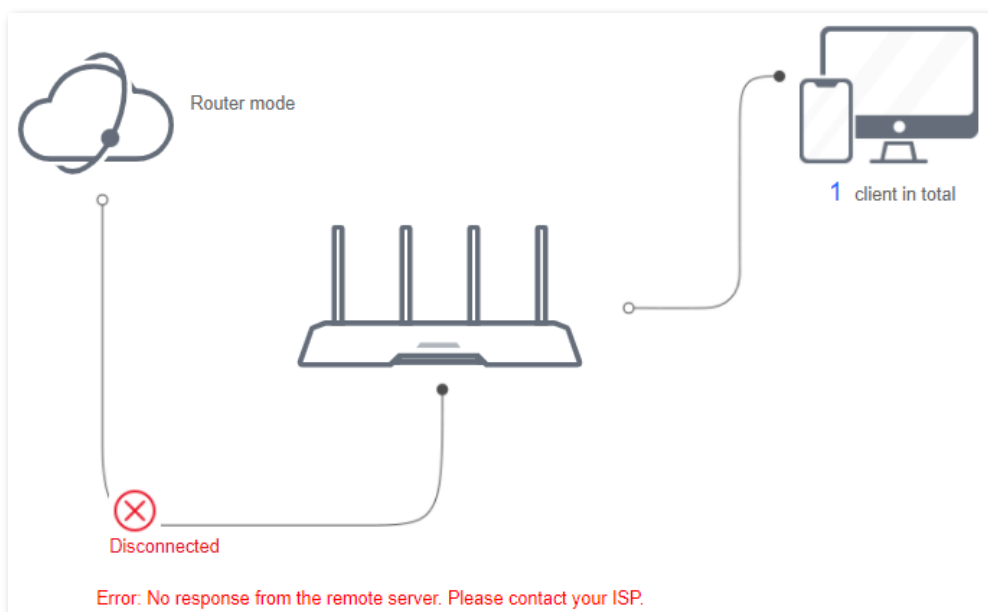


Figure 3-4 Internet connection status

When a red cross and “Disconnected” are shown between the internet and the router, and **Dial-up connection succeeded but the internet is inaccessible. Please contact your ISP.** is shown on the page, contact your ISP for the problem.

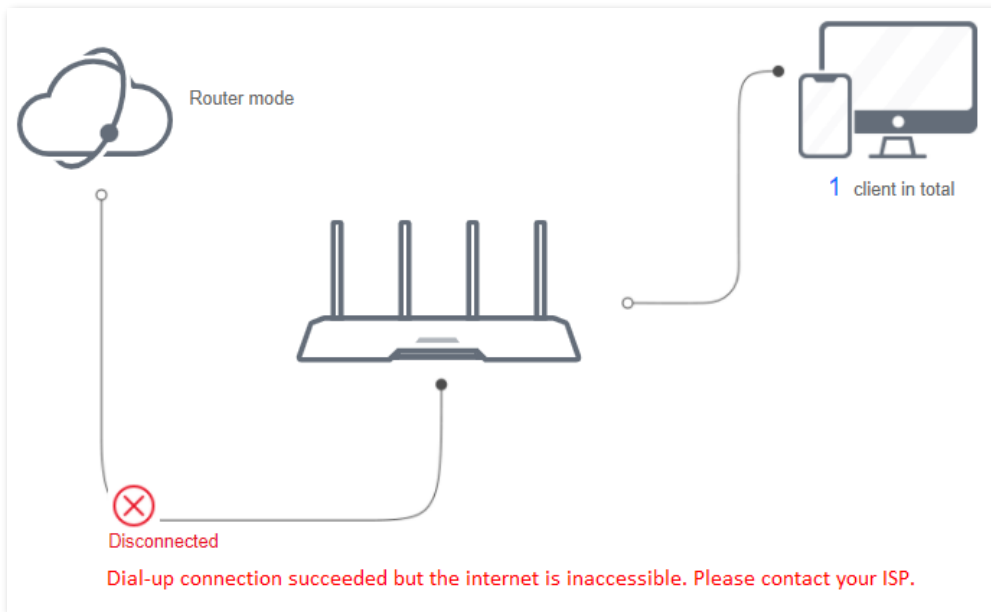


Figure 3-5 Internet connection status

When a red cross and "Disconnected" are shown between the internet and the router, and **The router has obtained a valid IP address but cannot access the Internet. Please try the solutions below one by one.** is shown as below, follow the instructions on the page to solve the problem.

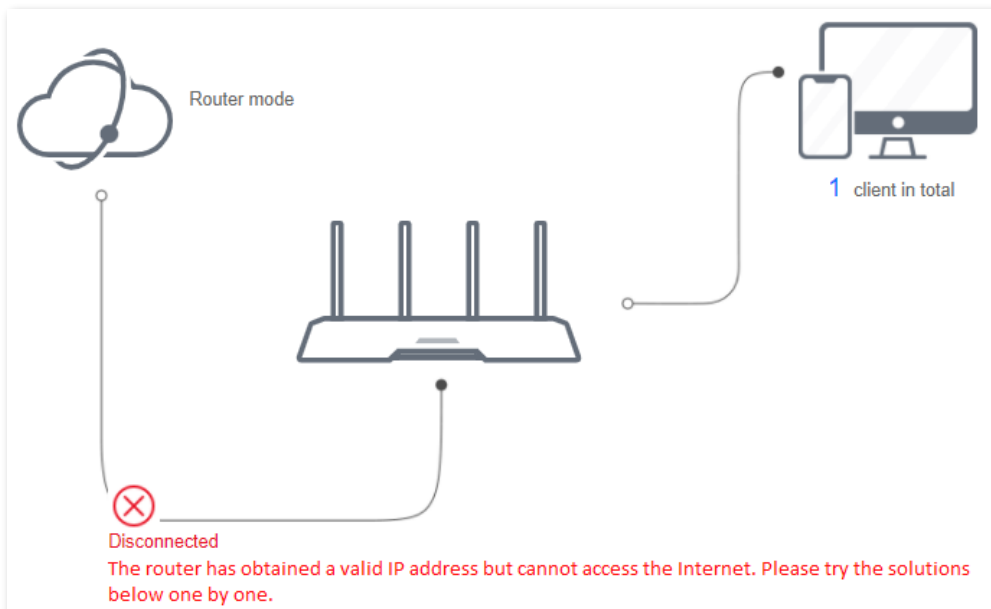



Figure 3-6 Internet connection status

3.2 View online device information

This part shows the information of online devices, such as the number and real-time upload/download speed.

To access the page, log in to the web UI of the router and navigate to **Status** >  (Online devices).

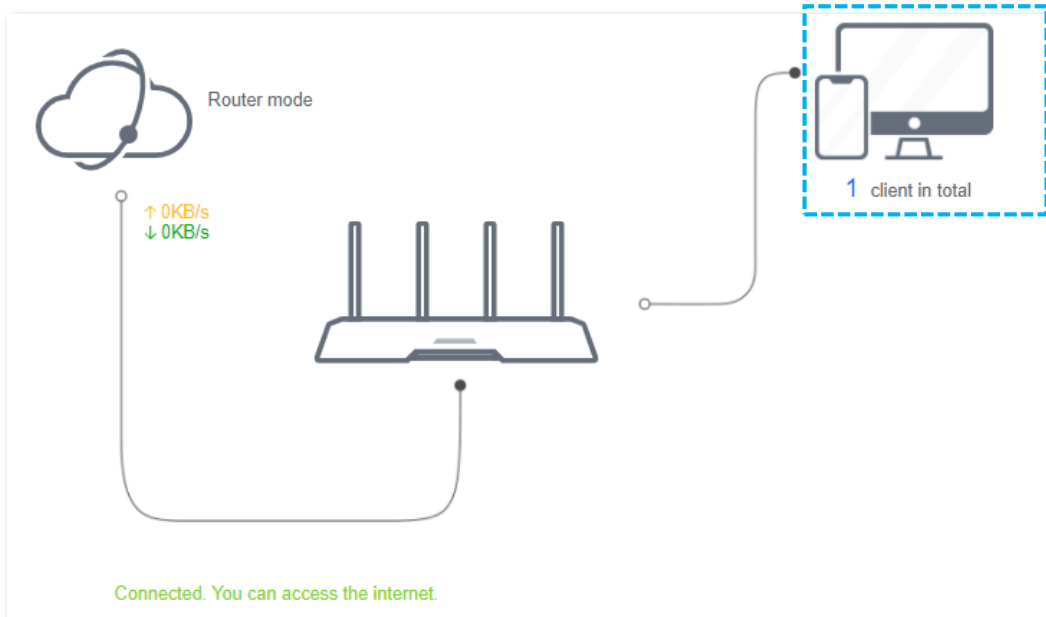


Figure 3-7 Online device information

To control the bandwidth of online devices, click the **Download Speed** and **Upload Speed** area to enter the [Access Control](#) page.


Online Device (1)					
Device Name	Download Speed	Upload Speed	Download Limit	Upload Limit	Internet Access
 MININT-GV610BB 192.168.0.200 6C:4B:90:41:E2:AD	↓ 0KB/s	↑ 0KB/s	No Limit	No Limit	Local
Blocked Device (Blacklist)					
Device Name	MAC Address	Unlimit			
No device					

Figure 3-8 Online device information

3.3 View system information

This section shows the basic information of the router, including connection type, connection duration, WAN IP address and so on.

To access the page, log in to the web UI of the router and navigate to **Status > System Info**.

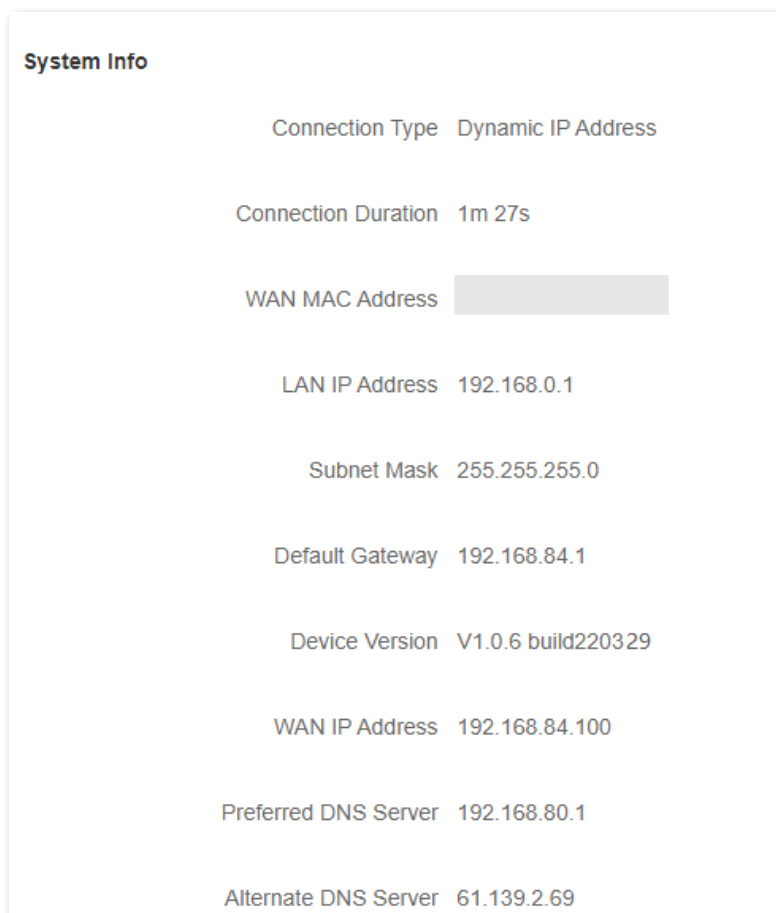


Figure 3-9 System information

Table 3-1 System information parameter description

Parameter	Description
Connection Type	It shows the current IPv4 connection type of the router.
Connection Duration	It specifies the time that has elapsed since the router connects to the IPv4 internet successfully.
WAN MAC Address	It specifies the MAC address of the WAN port of the router.
LAN IP Address	It specifies the IP address of the LAN port for the router. LAN users can access the web UI of the router by visiting this IP address. Default: 192.168.0.1.

Parameter	Description
Subnet Mask	It specifies the subnet mask of the WAN port.
Default Gateway	It specifies the IPv4 default gateway of the router.
Device Version	It specifies the current version number of the router's firmware.
WAN IP Address	It specifies the IPv4 address of the WAN port.
Preferred DNS Server	They show the preferred and alternative IPv4 DNS server address of the WAN port.
Alternate DNS Server	

Chapter 4 Route settings

4.1 Internet settings

4.1.1 Overview

On this page, you can complete the internet settings to achieve shared internet access for multiple users.

To access the page, log in to the web UI of the router and navigate to **Route Settings > Internet Settings**.

Figure 4-1 Internet settings

The router supports multiple working modes, including router mode, WISP mode, universal relay mode and AP mode. Choose the suitable mode according to your context of use.

Table 4-1 Working mode of the router

Context of use	Suitable mode
Connect your router to a modem or Ethernet jack using an Ethernet cable.	Router mode
Bridge the existing WiFi network and extend the wireless coverage.	WISP mode or Universal relay mode
Connect the router to a smart home gateway to provide wireless coverage.	AP mode

4.1.2 Serve as a router

If you use the router for the first time or the router is restored to factory settings, follow the quick installation guide to configure the internet access. If you want to modify internet parameters or other settings, you can follow the instruction in this chapter.

By default, the router works in router mode. Under this mode, connect the WAN port of the router to the internet, connect the LAN ports to user devices and complete the internet settings, then you can access the internet on these devices.

Note

Parameters are provided by your ISP. Contact your ISP for any doubts.

Set up a PPPoE connection

If the ISP provides you with a PPPoE user name and password, you can choose this connection type to access the internet. The application scenario is shown below.

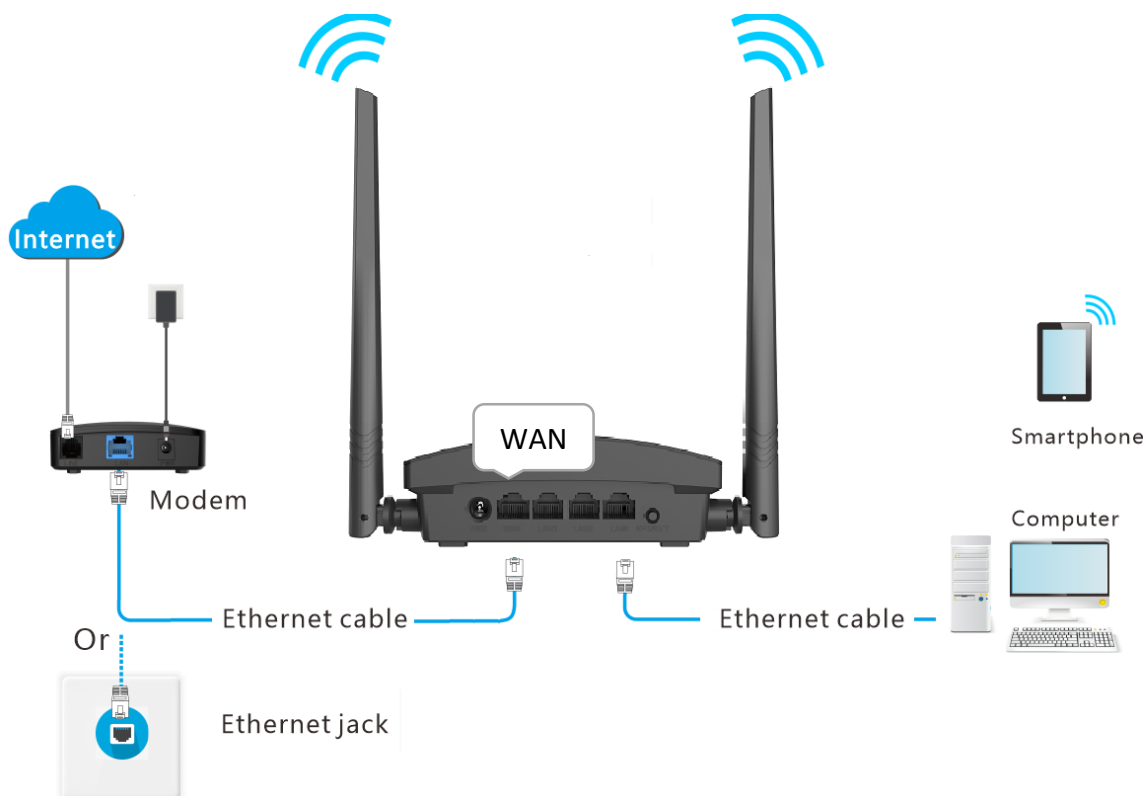


Figure 4-2 Application scenario

Procedures:

Step 1 Launch a web browser on a device connected to the router and visit **http://hikvisionwifi.local** to log in to the web UI of the router.

Step 2 Navigate to **Route Settings > Internet Settings**.

Step 3 Set **Operating Mode** to **Router Mode**.

Step 4 Set **Connection Type** to **PPPoE**.

Step 5 Enter the **User Name** and **Password** provided by your ISP.

Step 6 Click **Save** at the bottom of the page.

The screenshot displays the 'Internet Settings' configuration page. It is divided into two main sections: 'Operating Mode' and 'Internet Connection'.
In the 'Operating Mode' section, there are four radio button options: 'Router mode' (which is selected), 'WISP mode', 'Universal relay mode', and 'AP mode'. Below these options is a descriptive text: 'Under this mode, the router connects to the ISP in a wired manner, and provides WiFi signal to clients.'
The 'Internet Connection' section contains three radio button options: 'PPPoE' (selected), 'Static IP Address', and 'Dynamic IP Address'. Below these is another descriptive text: 'This type is applicable if a PPPoE user name and password are required for setting up an internet connection.'
At the bottom of this section, there are two input fields: 'User Name' and 'Password'. The 'Password' field includes a small icon for toggling password visibility. At the very bottom of the form is a blue 'Save' button.

Figure 4-3 Set up a PPPoE connection

Wait a moment. When “**Connected. You can access the internet.**” is shown on the page, the router is connected to the internet.

Internet Connection

Connection Type PPPoE Static IP Address Dynamic IP Address

This type is applicable if a PPPoE user name and password are required for setting up an internet connection.

User Name

Password

Connection Status **Connected. You can access the internet.**

Figure 4-4 Connection status

 **Note**

If you still cannot access the internet, try the following solutions:

- If “**Error: No response from the remote server. Please contact your ISP.**” is shown on the page, you are recommended to set the Connection Type to Dynamic IP Address.
- If the problem persists, refer to [3.1 View internet connection status](#) to find a solution.

Table 4-2 PPPoE parameter description

Parameter	Description
User Name	They specify the PPPoE user name and password provided by your ISP.
Password	
Connection Status	<p>It specifies the connection status of the WAN port.</p> <ul style="list-style-type: none"> ● When “Connected. You can access the internet now.” is shown here, the router is connected to the internet successfully. ● When other information is shown here, the router fails to connect to the internet. Please take corresponding measures according to the information shown here.

Set up a static IP connection

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

Procedures:

Step 1 Launch a web browser on a device connected to the router and visit **<http://hikvisionwifi.local>** to log in to the web UI of the router.

Step 2 Navigate to **Route Settings > Internet Settings**.

Step 3 Set **Connection Type** to **Static IP Address**.

Step 4 Set the required parameters provided by your ISP.

Step 5 Click **Save** at the bottom of the page.

Internet Connection

Connection Type PPPoE Static IP Address Dynamic IP Address

This type is applicable if a static IP address is required for setting up an internet connection.

IP Address . . .

Subnet Mask . . .

Default Gateway . . .

Preferred DNS Server . . .

Alternate DNS Server . . .

Save

Figure 4-5 Set up a static IP connection

Wait a moment. When "Connected. You can access the internet." is shown on the page, you can access the internet.

The screenshot shows the 'Internet Connection' configuration interface. At the top, there are three radio buttons for 'Connection Type': 'PPPoE', 'Static IP Address' (which is selected), and 'Dynamic IP Address'. Below this, a note states: 'This type is applicable if a static IP address is required for setting up an internet connection'. The configuration fields are as follows:


- IP Address:** 192 . 168 . 20 . 155
- Subnet Mask:** 255 . 255 . 255 . 0
- Default Gateway:** 192 . 168 . 20 . 100
- Preferred DNS Server:** 192 . 168 . 20 . 100
- Alternate DNS Server:** (All four input boxes are empty)

At the bottom, the 'Connection Status' is displayed as 'Connected. You can access the internet.' in green text.

Figure 4-6 Connection status

If you still cannot access the internet, refer to [3.1 View internet connection status](#) to find a solution.

Table 4-3 Static IP address parameter description

Parameter	Description
IP Address	When the static IP address is chosen as the connection type, enter the fixed IP address information provided by your ISP.
Subnet Mask	
Default Gateway	
Preferred DNS	 Note If your ISP only provides one DNS server address, you can leave the Alternate DNS blank.
Alternate DNS	
Connection Status	It specifies the connection status of the WAN port. <ul style="list-style-type: none"> • When "Connected. You can access the internet now." is shown here, the router is connected to the internet successfully. • When other information is shown here, the router fails to connect to the internet. Please take corresponding measures according to the information shown here.

Set up a dynamic IP connection

Generally, accessing the internet through a dynamic IP address is applicable in the following situations:

- Your ISP does not provide PPPoE user name and password, or any information including IP address, subnet mask, default gateway and DNS server.
- You have a router with internet access and want to add another router.

The application scenario is shown below.



Figure 4-7 Application scenario

Procedures:

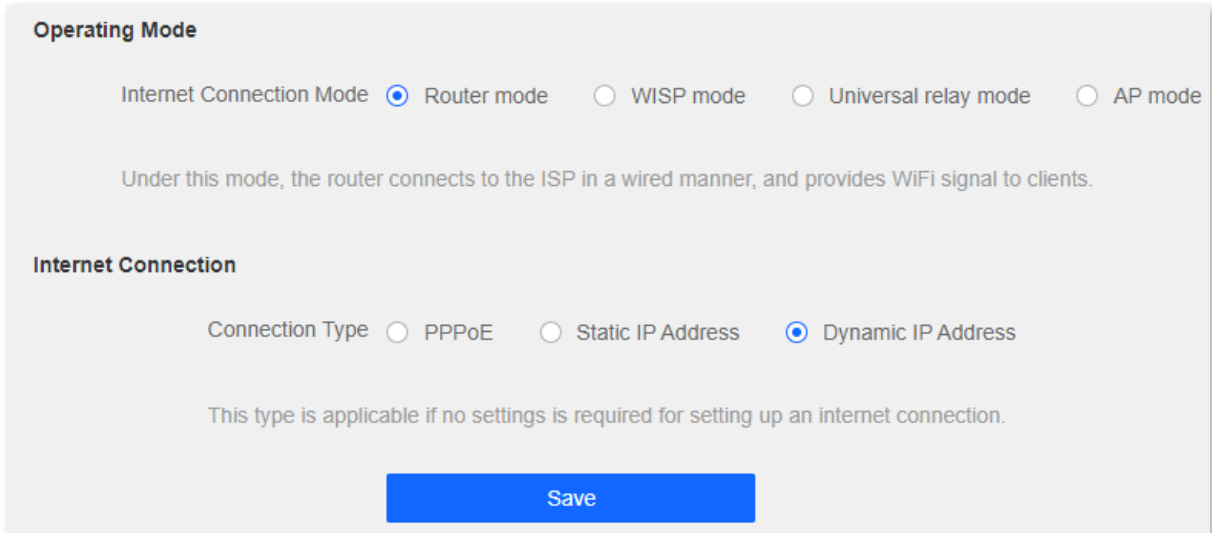
Step 1 Launch a web browser on a device connected to the router and visit <http://hikvisionwifi.local> to log in to the web UI of the router.

Step 2 Navigate to **Route Settings > Internet Settings**.

Step 3 Set **Operating Mode** to **Router Mode**.

Step 4 Set **Connection Type** to **Dynamic IP Address**.

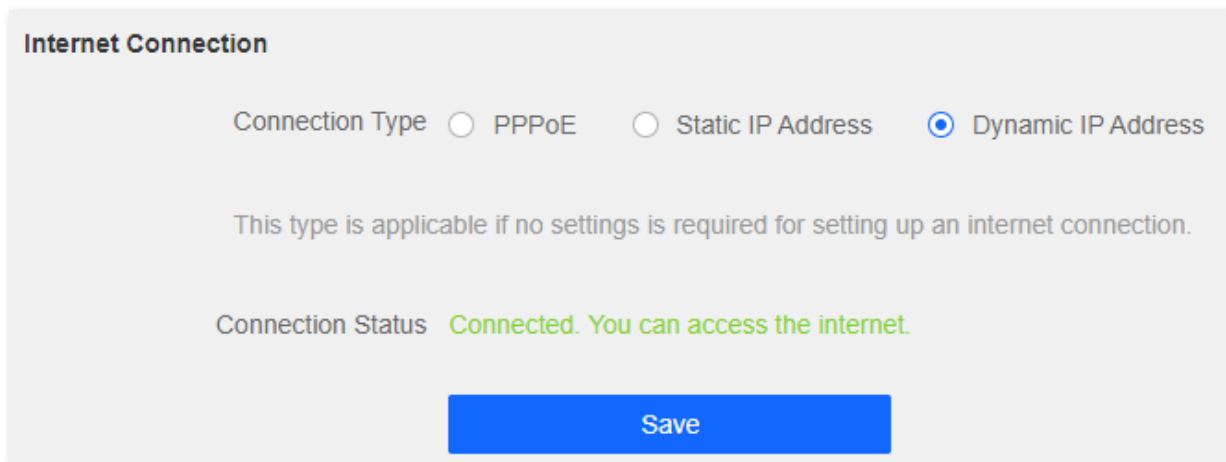
Step 5 Click **Save** at the bottom of the page.



The screenshot shows a configuration panel with two main sections. The first section, titled "Operating Mode", contains four radio buttons: "Router mode" (selected), "WISP mode", "Universal relay mode", and "AP mode". Below these is a descriptive sentence: "Under this mode, the router connects to the ISP in a wired manner, and provides WiFi signal to clients." The second section, titled "Internet Connection", contains three radio buttons: "PPPoE", "Static IP Address", and "Dynamic IP Address" (selected). Below these is another descriptive sentence: "This type is applicable if no settings is required for setting up an internet connection." At the bottom of the panel is a blue "Save" button.

Figure 4-8 Set up a dynamic IP connection

Wait a moment. When “**Connected. You can access the internet.**” is shown on the page, you can access the internet.



This screenshot shows the "Internet Connection" section of the configuration page. It features the same three radio buttons as Figure 4-8: "PPPoE", "Static IP Address", and "Dynamic IP Address" (selected). The descriptive sentence is present. Below it, a "Connection Status" label is followed by the text "Connected. You can access the internet." in green. A blue "Save" button is at the bottom.

Figure 4-9 Connection status

If you still cannot access the internet, refer to [3.1 View internet connection status](#) to find a solution.

4.1.3 Serve as a WiFi extender

If you have a router that is connected to the internet and wants to extend the WiFi coverage, you can refer to this chapter.

Assume that the information about your existing WiFi network is as follows:

- WiFi name: My_home_WiFi
- WiFi password: Hikvision123456

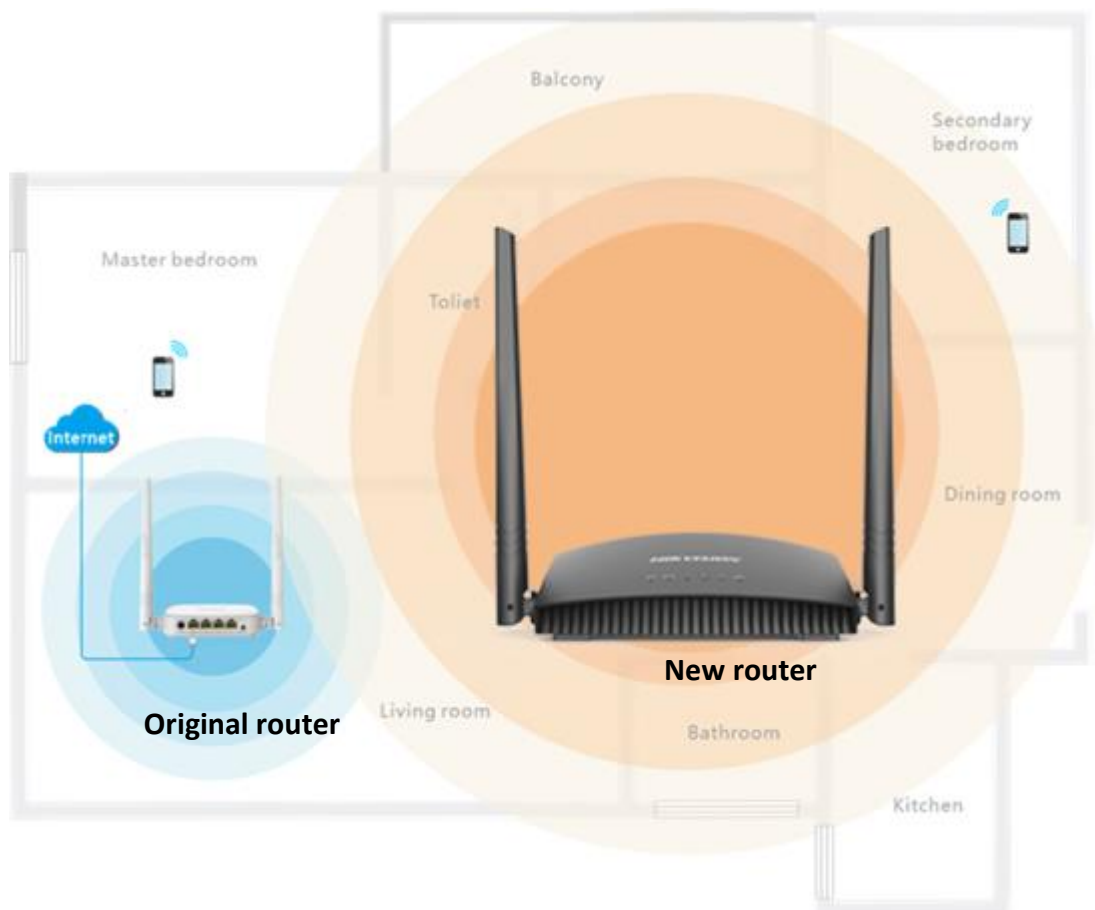


Figure 4-10 Application scenario

Method 1: Set the router to WISP mode

Procedures:

Step 1 Launch a web browser on a device connected to the router and visit <http://hikvisionwifi.local> to log in to the web UI of the router.

Note

If you use the router for the first time or have reset the router, proceed with the following steps. If you have already configured the router, skip **Step 2**.

Step 2 Set **Connection Type** to **Dynamic IP Address**, and click **Save**. You will be directed to the **Status** page.

Note

If you are using a wireless device for configuration and are not directed to the **Status** page automatically, ensure that your wireless device is still connected to the WiFi network of the router.

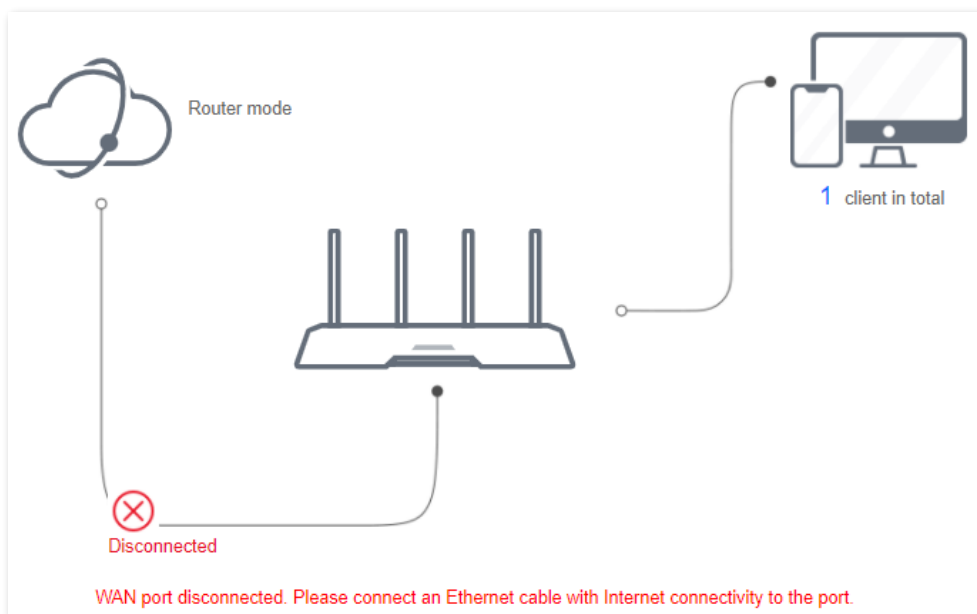


Figure 4-11 Internet connection status

Step 3 Navigate to **Route Settings > Internet Settings > Operating Mode**.

Step 4 Set **Operating Mode** to **WISP**.

Step 5 Select the ISP hotspot, which is **My_home_WiFi** in this example.

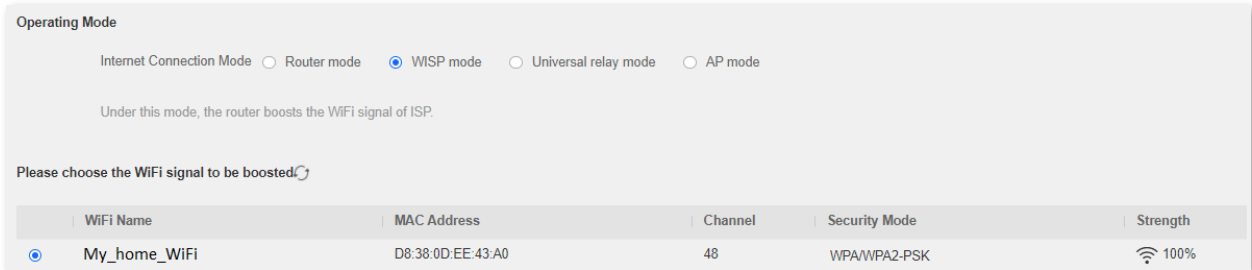


Figure 4-12 Select the WiFi signal to be boosted

Step 6 Enter the password of the WiFi network, which is **Hikvision123456** in this example.

Step 7 Click **OK**. The router will reboot to activate the settings.

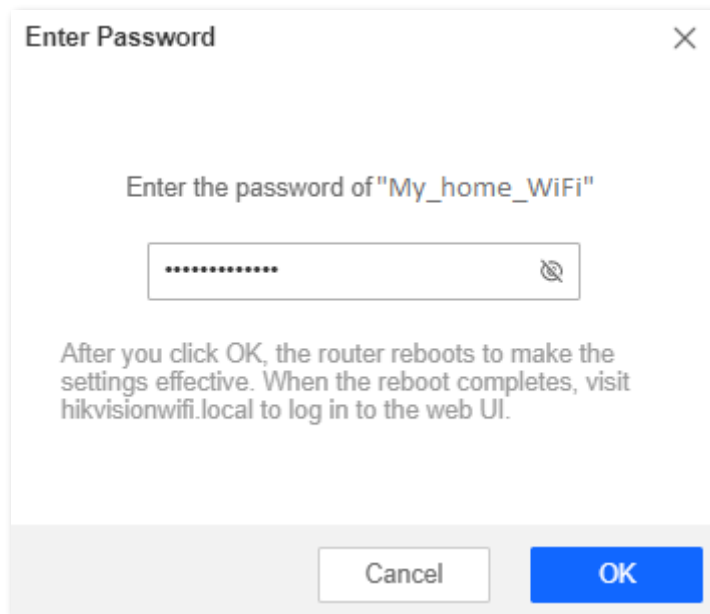


Figure 4-13 Enter password

Step 8 Log in to the web UI of the router again, and navigate to **Status > Connection Status** to ensure that **Connected. You can access the internet.** is shown on this page.

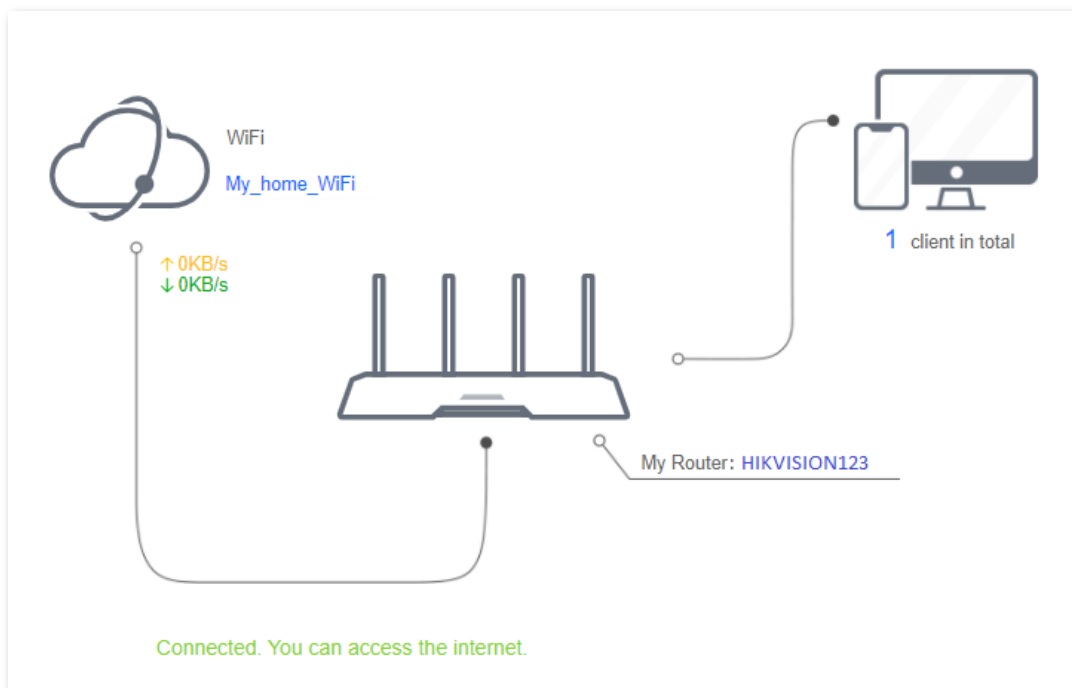


Figure 4-14 Connection status

Note

If the connection between **WiFi** and **My Router** failed, try the following solutions:

- Ensure that you have entered the correct WiFi password of the WiFi, and mind case sensitivity.
- Ensure that **My Router** is within the wireless coverage of the **WiFi**.

Step 9 Relocate the new router by referring to the following suggestions and power it on again:

- Between the original router and the uncovered area, but within the coverage of the original router.
- Away from the microwave oven, electromagnetic oven or refrigerator.
- Above the ground with few obstacles.

Caution

Do not connect any device to the WAN port of the new router after setting the router to WISP mode.

To access the internet, connect your computer to a LAN port of the new router, or connect your smartphone to the WiFi network of the new router.

Navigate to **Route Settings > Wireless Settings > WiFi Name and Password** to check the WiFi name and password. If the network is not encrypted, you can also set a WiFi password on this page for security.

WiFi Name and Password

Unify 2.4 GHz & 5 GHz Enable Disable

After this function is enabled, the 2.4 GHz and 5 GHz networks use the same WiFi name; in this way, the router can automatically choose the best WiFi network for clients.

WiFi Network Enable Disable

WiFi Name Hide WiFi network

Security Mode

WiFi Password

Figure 4-15 WiFi name and password

Note

If you cannot access the internet, try the following solutions:

- Ensure that the existing router is connected to the internet successfully.
- Ensure that your wireless devices are connected to the WiFi network of the new router.
- If the computer connected to the router for repeating cannot access the internet, ensure that the computer is configured to obtain an IP address and DNS server automatically.

Method 2: Set the router to universal relay mode

Procedures:

Step 1 Launch a web browser on a device connected to the router and visit <http://hikvisionwifi.local> to log in to the web UI of the router.

Note

If you use the router for the first time or have reset the router, proceed with the following steps. If you have already configured the router, skip **Step 2**.

Step 2 Set **Connection Type** to **Dynamic IP Address**, and click **Save**. You will be directed to the **Status** page.

Note

If you are using a wireless device for configuration and are not directed to the **Status** page automatically, ensure that your wireless device is still connected to the WiFi network of the router.

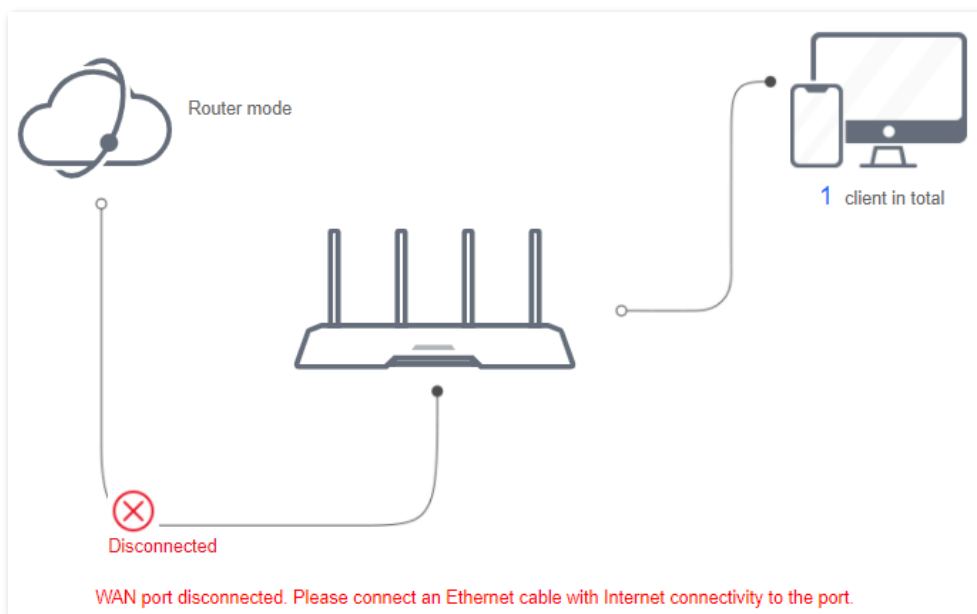


Figure 4-16 Internet connection status

Step 3 Navigate to **Route Settings > Internet Settings > Operating Mode**.

Step 4 Set **Operating Mode** to **Universal relay mode**.

Step 5 Select the ISP hotspot, which is **My_home_WiFi** in this example.

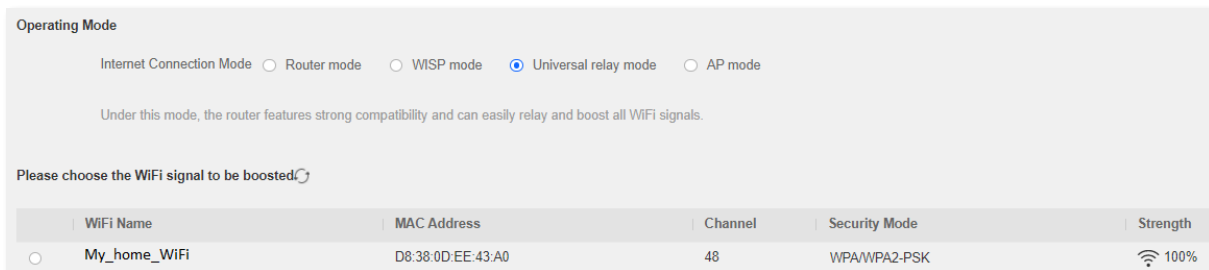


Figure 4-17 Select the ISP hotspot to be boosted

Step 6 Enter the password of the selected WiFi network, which is **Hikvision123456** in this example.

Step 7 Click **OK**. The router will reboot to activate the settings.

Step 8 Log in to the web UI of the router again, and navigate to **Status > Connection Status** to ensure that **Bridged in Universal Repeater mode** is shown on this page.

Note

The LAN IP address of the router will change. Please log in to the web UI of the router by visiting **<http://hikvisionwifi.local>**. If there is another network device with the same login domain name (hikvisionwifi.local) as the router, log in to the upstream router and find the IP address obtained by the new router in the client list. Then you can log in to the web UI of the router by visiting the IP address.

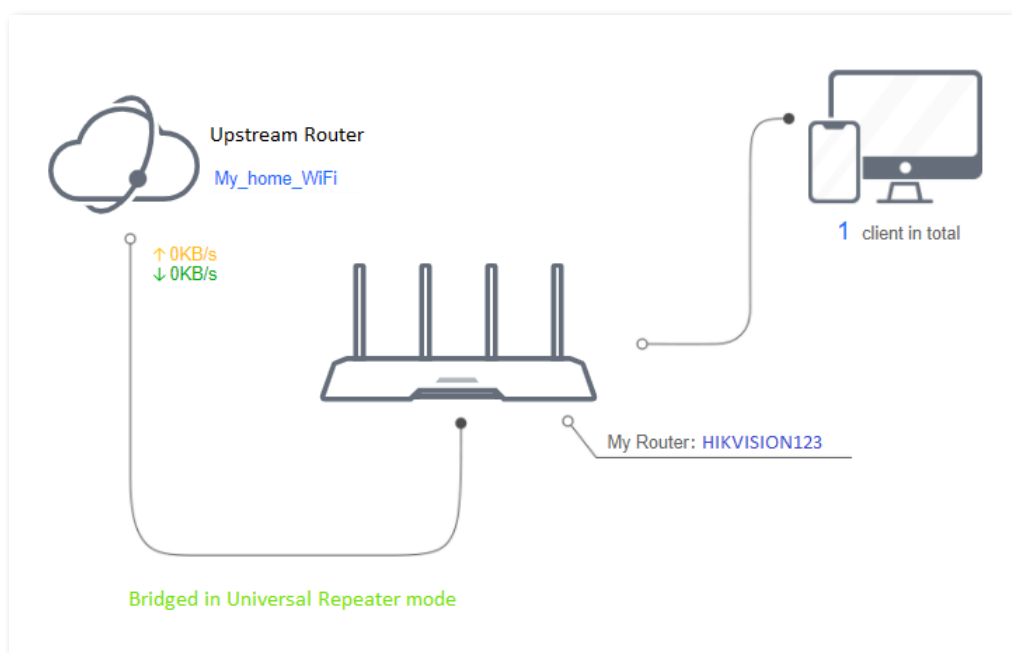


Figure 4-18 Connection status

 **Note**

If the connection between the **Upstream Router** and **My Router** failed, try the following solutions:

- Ensure that you have entered the correct WiFi password of the WiFi, and mind case sensitivity.
- Ensure that **My Router** is within the wireless coverage of the **Upstream Router**.

Step 9 Relocate the new router by referring to the following suggestions and power it on again:

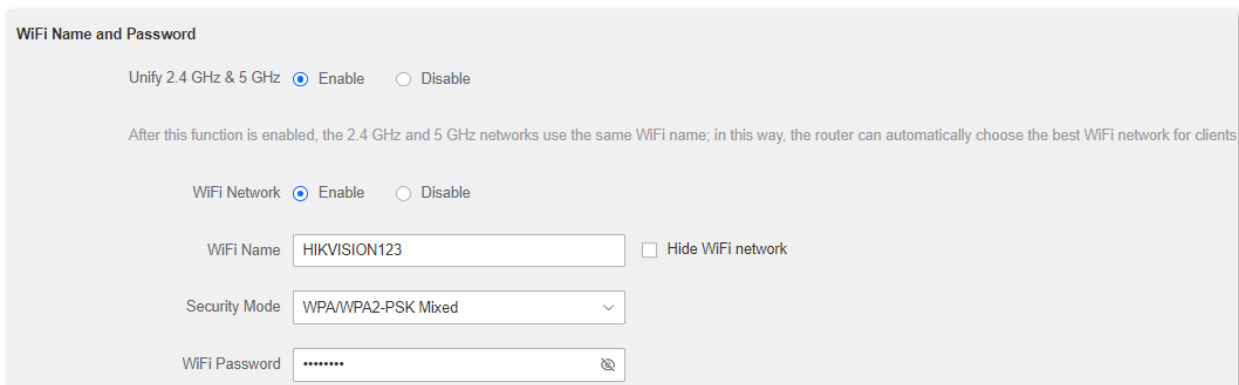
- Between the original router and the uncovered area, but within the coverage of the original router.
- Away from the microwave oven, electromagnetic oven, and refrigerator.
- Above the ground with few obstacles.

 **Caution**

After the new router is set to universal relay mode, Do NOT connect any device to the WAN port of the new router.

To access the internet, connect your computer to a LAN port of the new router, or connect your smartphone to the WiFi network of the new router.

Navigate to **Wireless Settings > WiFi Name and Password** to check the WiFi name and password. If the network is not encrypted, you can also set a WiFi password on this page for security.



WiFi Name and Password

Unify 2.4 GHz & 5 GHz Enable Disable

After this function is enabled, the 2.4 GHz and 5 GHz networks use the same WiFi name; in this way, the router can automatically choose the best WiFi network for clients

WiFi Network Enable Disable

WiFi Name Hide WiFi network

Security Mode

WiFi Password

Figure 4-19 WiFi name and password



Note

If you cannot access the internet, try the following solutions:

- Ensure that the existing router is connected to the internet successfully.
- Ensure that your wireless devices are connected to the WiFi network of the new router.
- If the computer connected to the router for repeating cannot access the internet, ensure that the computer is configured to obtain an IP address and DNS server automatically.

4.1.4 Serve as an AP

When you have a smart home gateway that only provides wired internet access, you can set the router to work in AP mode to provide wireless coverage.



Note

When the router is set to AP mode:

- Every physical port can be used as a LAN port.
- The LAN IP address of the router will be changed. Please log in to the web UI of the router by visiting **<http://hikvisionwifi.local>**.
- Functions, such as bandwidth control and port mapping will be unavailable. Refer to the web UI for available functions.

Procedures:

Step 1 Power on the router. Connect a computer to a LAN port of the router, or connect your smartphone to the WiFi network of the router.

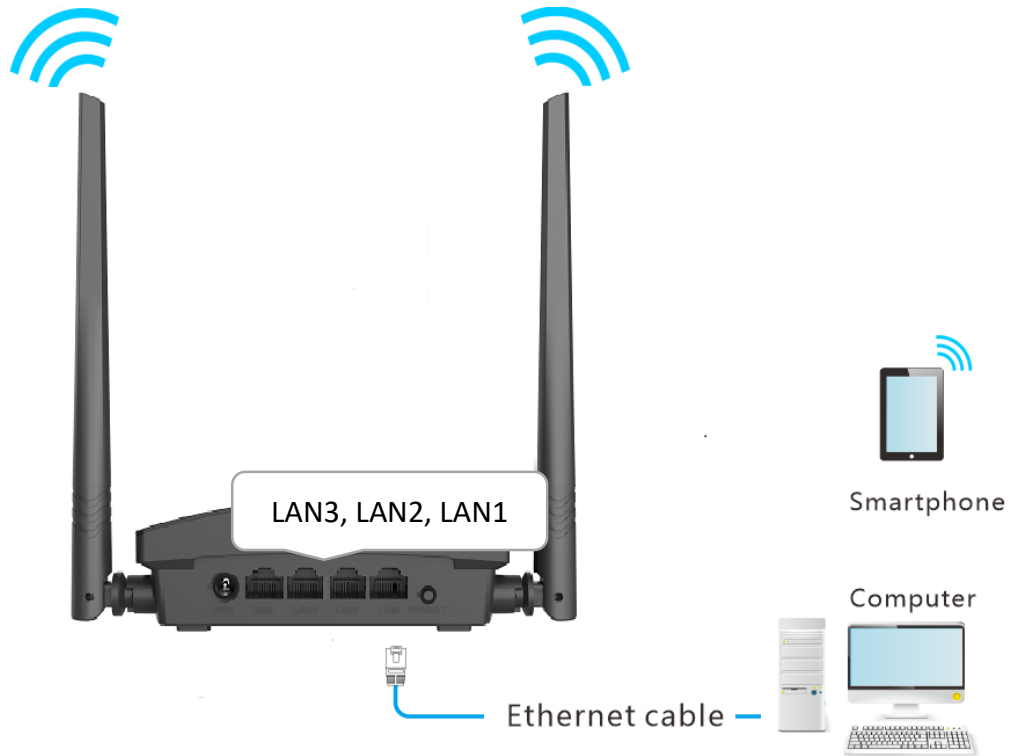


Figure 4-20 Application scenario

Note

If you have finished the quick setup wizard before, launch a web browser and visit <http://hikvisionwifi.local> and skip **Step 2**.

Step 2 Log in to the web UI of the router.

- 1) Launch a web browser on a device connected to the router and visit **<http://hikvisionwifi.local>** to log in to the web UI of the router. A computer is used for the illustration below.
- 2) Set **Connection Type** to **Dynamic IP Address**, and click **Save**. You will be directed to the **Status** page.

 **Note**

If you are using a wireless device for configuration and are not directed to the **Status** page automatically, ensure that your wireless device is still connected to the WiFi network of the router.

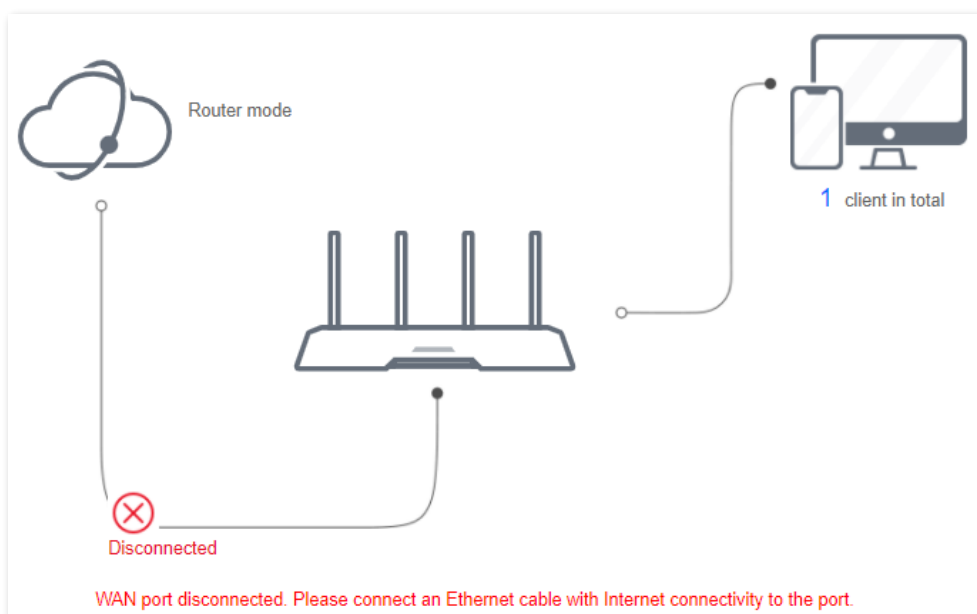


Figure 4-21 Connection status

Step 3 Set the router to **AP mode**.

- 1) Navigate to **Route Settings > Internet Settings > Operating Mode**.
- 2) Set **Operating Mode** to **AP**, and click **Save** at the bottom of the page.

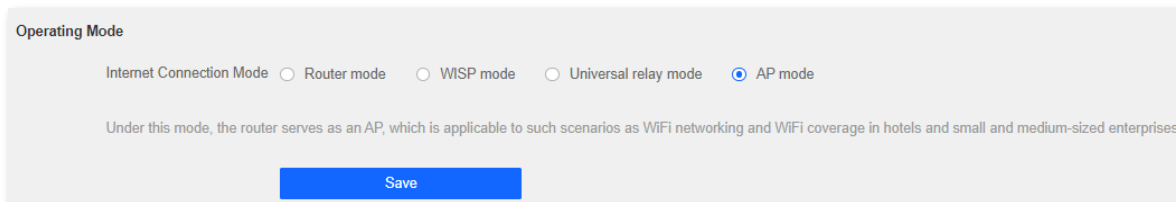


Figure 4-22 Set the router to **AP mode**

- 3) Click **OK** in the popup window. The router will reboot to activate the settings.

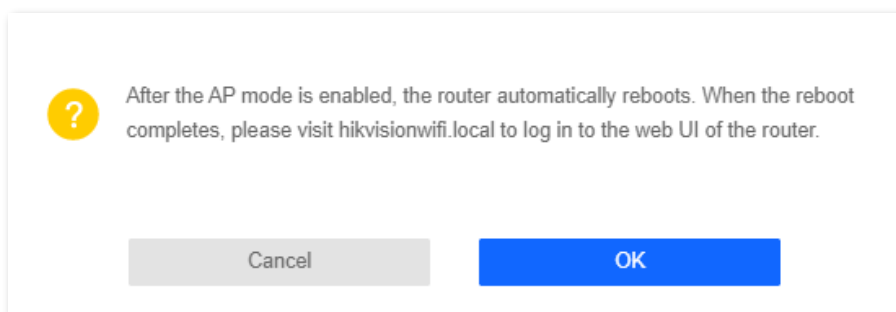


Figure 4-23 Click **OK**

Step 4 Connect the upstream device, such as a gateway, to any port of the router.



Figure 4-24 Application scenario

Log in to the web UI of the router again, and navigate to **Status > Connection Status** to check if the AP mode is configured successfully as follows.

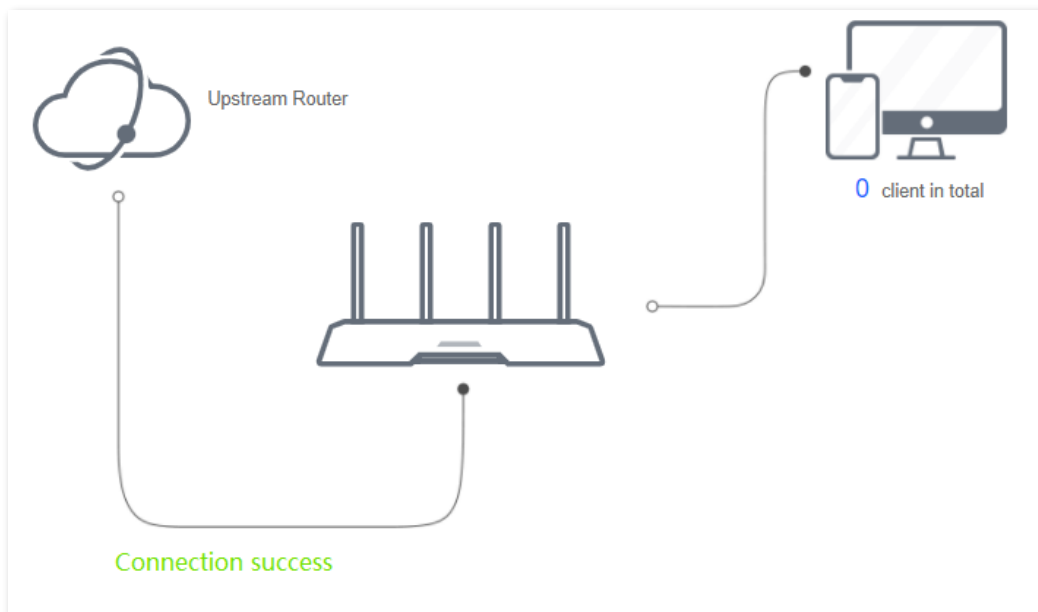


Figure 4-25 Internet connection status

Note

If there is another network device with the same login domain name (hikvisionwifi.local) as the router, log in to the upstream router and find the IP address obtained by the new router in the client list. Then you can log in to the web UI of the router by visiting the IP address.

To access the internet, connect your computer to a physical port, or connect your smartphone to the WiFi network.

Navigate to **Route Settings > Wireless Settings > WiFi Name and Password** to check the WiFi name and password. If the network is not encrypted, you can also set a WiFi password on this page for security.

The screenshot shows the 'WiFi Name and Password' configuration page. At the top, there are two radio buttons for 'Unify 2.4 GHz & 5 GHz', with 'Enable' selected. Below this is a note: 'After this function is enabled, the 2.4 GHz and 5 GHz networks use the same WiFi name; in this way, the router can automatically choose the best WiFi network for clients.' Below the note are two radio buttons for 'WiFi Network', with 'Enable' selected. There are three input fields: 'WiFi Name' containing 'HIKVISION123', 'Security Mode' set to 'WPA/WPA2-PSK Mixed', and 'WiFi Password' with masked characters. A 'Hide WiFi network' checkbox is also present.

Figure 4-26 WiFi name and password

 **Note**

If you cannot access the internet, try the following solutions:

- Ensure that the existing router is connected to the internet successfully.
- Ensure that your wireless devices are connected to the correct WiFi network of the new router.
- If the computer connected to the router cannot access the internet, ensure that the computer is configured to obtain an IP address and DNS server automatically.

4.2 Wireless settings

4.2.1 WiFi on/off

You can enable/disable the wireless network of the router.

To access the configuration page, log in to the web UI of the router, and navigate to **Route Settings > Wireless Settings > WiFi On/Off**.

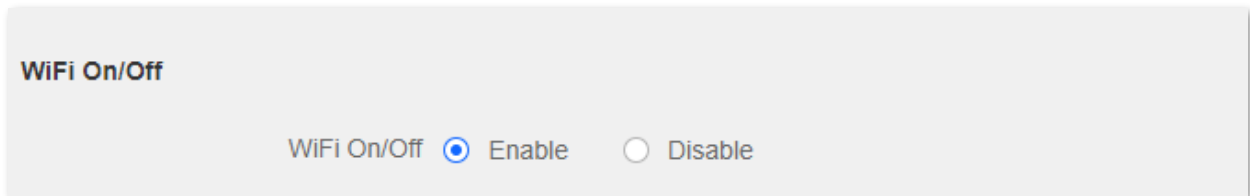


Figure 4-27 WiFi on/off

4.2.2 WiFi name and password

Overview


On this page, you can configure basic WiFi parameters, such as the WiFi name and password.

To access the configuration page, log in to the web UI of the router, and navigate to **Route Settings > Wireless Settings > WiFi Name and Password**.



Figure 4-28 WiFi name and password

Table 4-4 WiFi name and password parameter description

Parameter	Description
WiFi Name	It specifies the WiFi network name (SSID) of the WiFi network.
Security Mode	<p>It specifies the encryption modes supported by the router, including:</p> <ul style="list-style-type: none"> ● None: It indicates that a WiFi network is not encrypted and any clients can access the network without a password. This option is not recommended as it leads to low network security. ● WPA-PSK: It indicates that WPA-PSK is adopted to authenticate users. ● WPA2-PSK: It indicates that WPA2-PSK is adopted to authenticate users. ● WPA/WPA2-PSK Mixed: It indicates that WPA-PSK and WPA2-PSK are adopted to authenticate users.
WiFi Password	<p>It specifies the password for connecting to the WiFi network. You are strongly recommended to set a WiFi password for security.</p> <p> Note</p> <p>It is recommended to use the combination of numbers, uppercase letters, lowercase letters and special symbols in the password to enhance the security of the WiFi network.</p>
Hide network	<p>WiFi</p> <p>With this function enabled, wireless clients cannot find the SSID, and you need to enter the SSID on the wireless clients to access the WiFi network. By default, this function is disabled.</p>

Change the WiFi name and WiFi password

The router supports a 2.4 GHz WiFi network.

Assume that you want to change the WiFi name and password to **John_Doe_2.4GHz** and **Hikvision+Wireless24**. The network adopts **WPA/WPA2-PSK Mixed** as the encryption type.

Procedures:

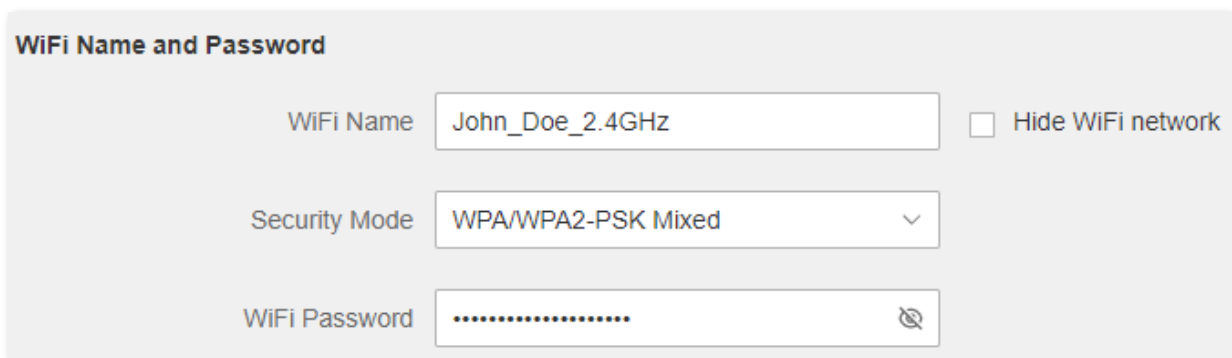
Step 1 Launch a web browser on a device connected to the router and visit **http://hikvisionwifi.local** to log in to the web UI of the router.

Step 2 Navigate to **Route Settings > Wireless Settings > WiFi Name and Password**.

Step 3 Change the parameters of the WiFi network.

- 1) Change the WiFi Name of the WiFi network, which is **John_Doe_2.4GHz** in this example.
- 2) Select an Encryption Mode, which is **WPA/WPA2-PSK Mixed** in this example.
- 3) Change the WiFi Password of the WiFi network, which is **Hikvision+Wireless24** in this example.

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



The screenshot shows the 'WiFi Name and Password' configuration page. It contains the following elements:

- WiFi Name:** A text input field containing 'John_Doe_2.4GHz'.
- Security Mode:** A dropdown menu currently set to 'WPA/WPA2-PSK Mixed'.
- WiFi Password:** A text input field with the password masked by dots.
- Hide WiFi network:** An unchecked checkbox.

Figure 4-29 Change WiFi name and password

When completing the configurations, you can connect your wireless devices to the WiFi networks of the router to access the internet.

Hide the WiFi network

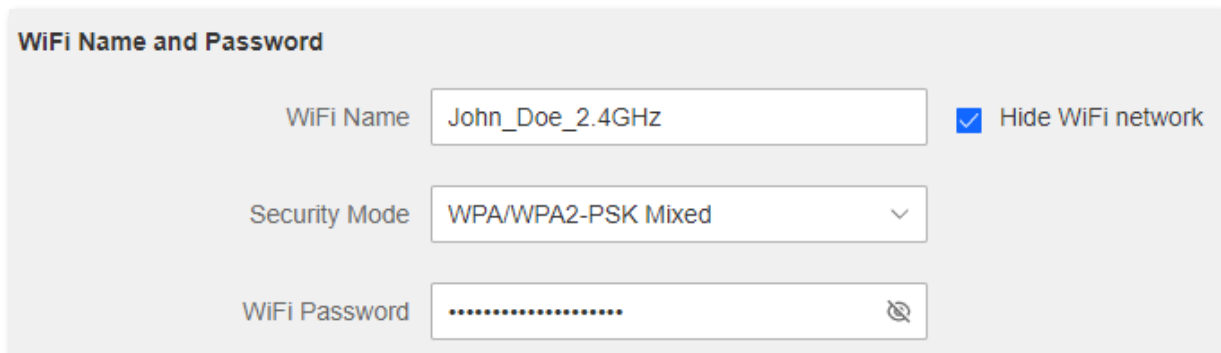
Procedures:

Step 1 Launch a web browser on a device connected to the router and visit **<http://hikvisionwifi.local>** to log in to the web UI of the router.

Step 2 Navigate to **Route Settings > Wireless Settings > WiFi Name and Password**.

Step 3 Tick **Hide WiFi network** of the target network.

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



WiFi Name and Password

WiFi Name: John_Doe_2.4GHz Hide WiFi network

Security Mode: WPA/WPA2-PSK Mixed

WiFi Password:

Figure 4-30 Hide WiFi network

When the configurations are completed, the corresponding WiFi network is invisible to wireless devices.

Connect to a hidden WiFi network

When a WiFi network is hidden, you need to enter the WiFi name manually to connect to it.

Assume that the WiFi parameters are:

- WiFi name: Jone_Doe
- Encryption type: WPA/WPA2-PSK Mixed
- WiFi password: Hikvision+Wireless245

Note

If you do not remember the wireless parameters of the WiFi network, log in to the web UI of the router and navigate to **Route Settings > Wireless Settings > WiFi Name and Password** to find them.

Procedures (Example: iPhone):

Step 1 Tap **Settings** on your phone, and find **WLAN**.

Step 2 Enable **WLAN**.

Step 3 Scroll the WiFi list to the bottom, and tap **Other...**

Step 4 Enter the WiFi name and password, which are **John_Doe** and **Hikvision+Wireless245** in this example.

Step 5 Set security to **WPA2/WPA3** (if WPA2/WPA3 is not available, choose WPA2).

Step 6 Tap **Join**.

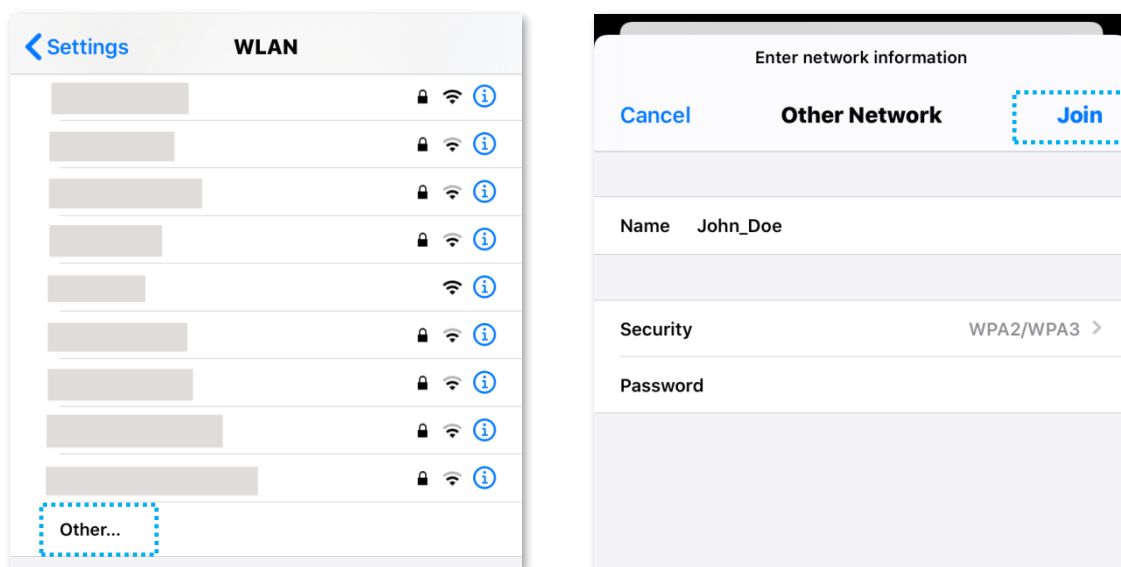


Figure 4-31 Connect to a hidden WiFi network

When the configurations are completed, you can connect to the hidden WiFi network to access the internet.

4.2.3 Multi SSID and password


Overview

In this module, you can enable/disable the Multi SSID and password function and change the WiFi name and password of the guest network.

To access the configuration page, log in to the web UI of the router and navigate to **Route Settings > Wireless Settings > Multi SSID and Password**. This function is disabled by default.

Figure 4-32 Multi SSID and Password

Table 4-5 Multi SSID and password parameter description

Parameter	Description
Multi SSID	It is used to enable the Multi SSID and password function.
WiFi Name	<p>It specifies the WiFi name of the router's guest network.</p> <p> Note</p> <p>You can change the SSIDs (WiFi name) if required. To distinguish the guest network from the main network, you are recommended to set the different WiFi network names.</p>
WiFi Password	It specifies the password for the router's guest network.

Set up the guest network

Scenario: A group of friends is going to visit your home.

Goal: Prevent the use of WiFi networks by guests from affecting the network speed of your computer for work purposes.

Solution: You can configure the guest network function and let your guests use the guest networks.

Assume that the parameters you are going to set for the guest WiFi network:

- WiFi name for WiFi network: John_Doe.
- WiFi password for WiFi network: Hikvision+245.

Procedures:

Step 1 Launch a web browser on a device connected to the router and visit <http://hikvisionwifi.local> to log in to the web UI of the router.

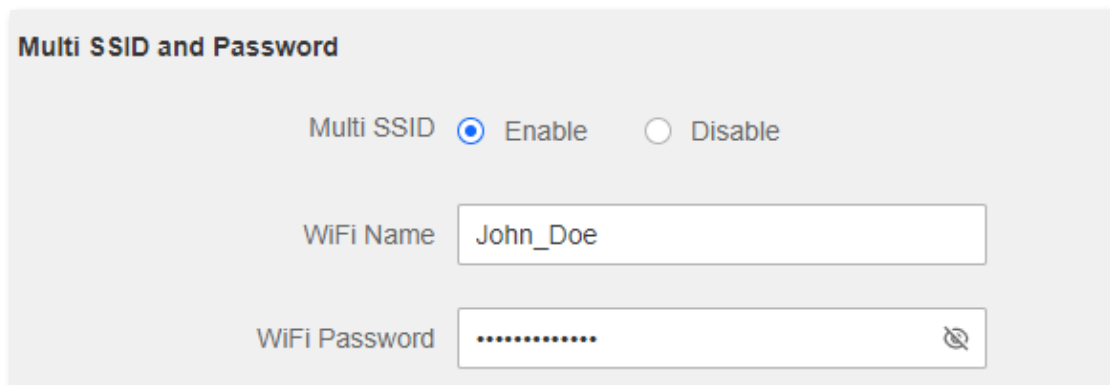
Step 2 Navigate to **Route Settings > Wireless Settings > Multi SSID and Password**.

Step 3 Set **Multi SSID and Password** to **Enable**.

Step 4 Change the WiFi Name, which is **John_Doe** in this example.

Step 5 Set **WiFi Password**, which is **Hikvision+245** in this example.

Step 6 Click **Save** at the bottom of the page.



The screenshot shows the 'Multi SSID and Password' configuration page. At the top, the title 'Multi SSID and Password' is displayed. Below the title, there are two radio buttons: 'Multi SSID' with 'Enable' selected (indicated by a blue dot) and 'Disable' (indicated by an empty circle). Underneath, there are two input fields. The first is labeled 'WiFi Name' and contains the text 'John_Doe'. The second is labeled 'WiFi Password' and contains a series of dots, with a small eye icon to its right for toggling visibility.

Figure 4-33 Set up the multi SSID and password

After the configuration, guests can connect their wireless devices, such as smartphones, to **John_Doe** to access the internet.

4.2.4 WiFi schedule

Overview

In this module, you can enable/disable the WiFi schedule function.

To access the configuration page, log in to the web UI of the router and navigate to **Route Settings > Wireless Settings > WiFi Schedule**. This function is disabled by default.

WiFi Schedule

WiFi Schedule Enable Disable

Turn WiFi Off At 00 : 00 ~ 07 : 00

Turn WiFi Off On Everyday Monday Tuesday Wednesday Thursday Friday Saturday Sunday

Figure 4-34 WiFi schedule

Table 4-6 WiFi schedule parameter description

Parameter	Description
WiFi Schedule	Used to enable/disable the WiFi schedule function of the router.
Turn WiFi Off At	It specifies the period to turn off WiFi. 00:00-00:00 indicates a whole day.
Turn WiFi Off On	It specifies the date to turn off WiFi.

Set up WiFi schedule

Procedures:

- Step 1 Launch a web browser on a device connected to the router and visit <http://hikvisionwifi.local> to log in to the web UI of the router.
- Step 2 Navigate to Route **Settings > Wireless Settings > WiFi Schedule**.
- Step 3 Set **WiFi Schedule** to **Enable**.
- Step 4 Specify a period to turn off the WiFi network, which is **03:00 ~ 08:00** in this example.
- Step 5 Choose the specified date to turn off the WiFi network, which is **Everyday** in this example.
- Step 6 Click **Save** at the bottom of the page.

WiFi Schedule

WiFi Schedule Enable Disable

Turn WiFi Off At 03 : 00 ~ 08 : 00

Turn WiFi Off On Everyday Monday Tuesday Wednesday Thursday Friday Saturday Sunday

Figure 4-35 Set up WiFi schedule

4.2.5 WPS

The WPS function enables wireless devices such as smartphones to connect to WiFi networks of the router quickly and easily.

To access the page, log in to the web UI of the router and navigate to **Route Settings > Wireless Settings > WPS**.



This function is only applicable to WPS-enabled wireless devices.


Connect to the WiFi network using the WPS button

Step 1 Press the WPS button on the router.



Figure 4-36 Press the WPS button

Step 2 Configure the WPS function on your wireless devices within 2 minutes. Configurations on various devices may differ (Example: HUAWEI P10).

- 1) Find **Settings** on the phone.
- 2) Select **WLAN**.
- 3) Tap , and select **WLAN settings**.

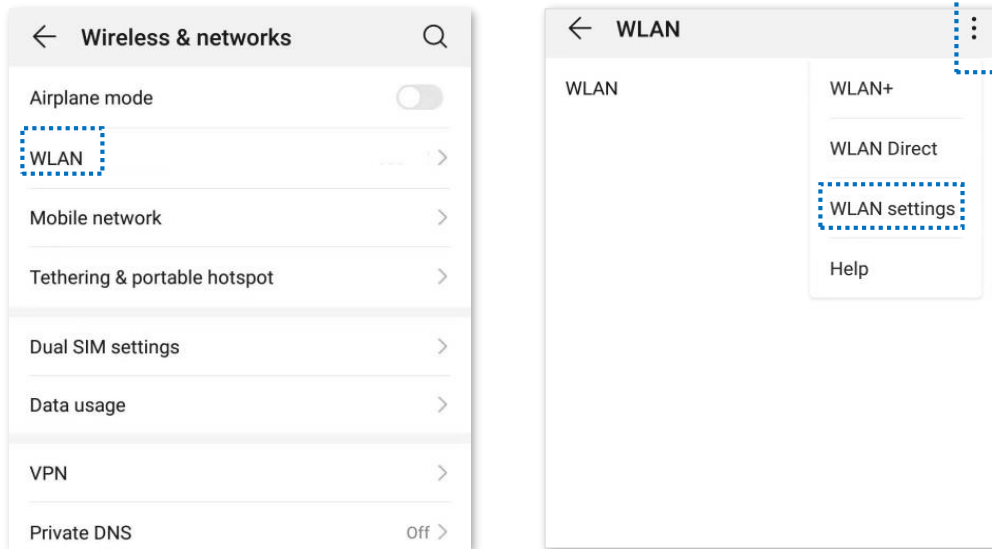


Figure 4-37 Configure the WPS function

- 4) Select **WPS connection**.

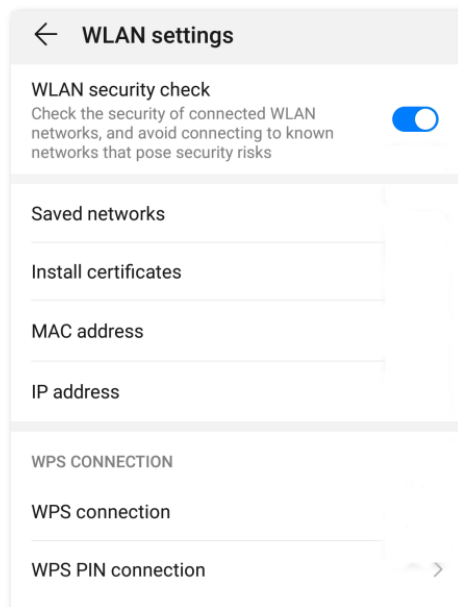


Figure 4-38 Select WPS connection

Wait a moment until the WPS negotiation is completed, and the phone is connected to the WiFi network.

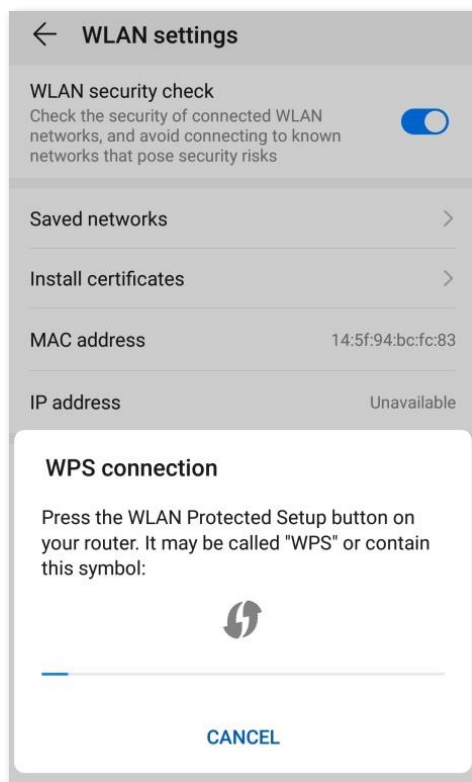


Figure 4-39 WPS negotiation completed

Connect to the WiFi network using the PBC button

Procedures:

Step 1 Launch a web browser on a device connected to the router and visit <http://hikvisionwifi.local> to log in to the web UI of the router.


Step 2 Navigate to **Route Settings > Wireless Settings > WPS**.

Step 3 Enable the WPS.

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

Step 5 Click **PBC**.

Step 6 Configure the WPS function on your wireless devices within 2 minutes. Configurations on various devices may differ (Example: HUAWEI P10).

- 1) Find **WLAN** settings on the phone.
- 2) Tap , and choose **WLAN settings**.

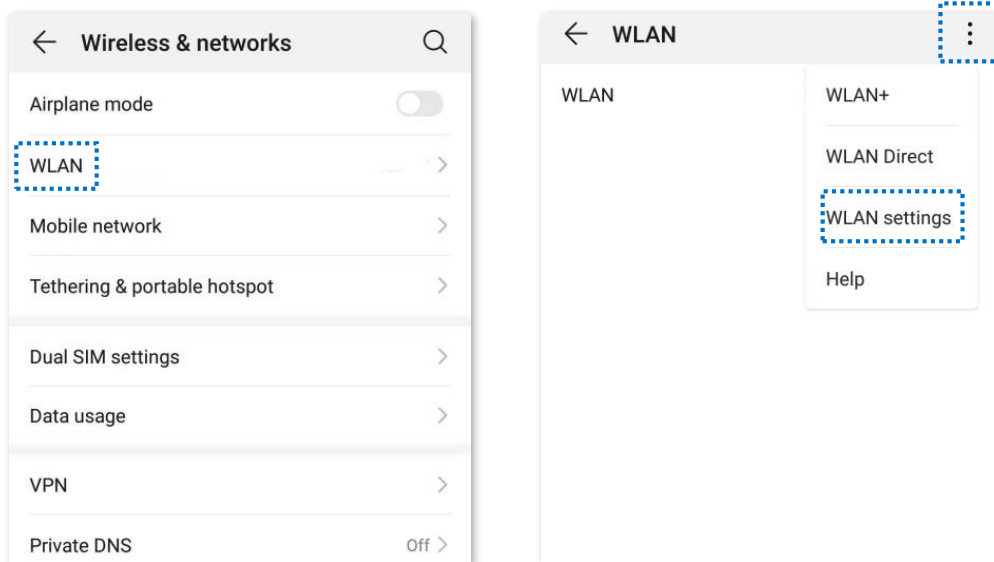


Figure 4-40 Configure the WPS function

- 3) Select **WPS connection**.

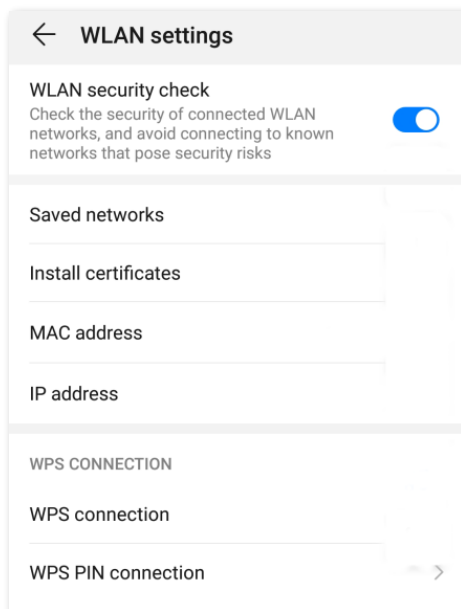


Figure 4-41 Select WPS connection

Wait a moment until the WPS negotiation is completed, and the phone is connected to the WiFi network.

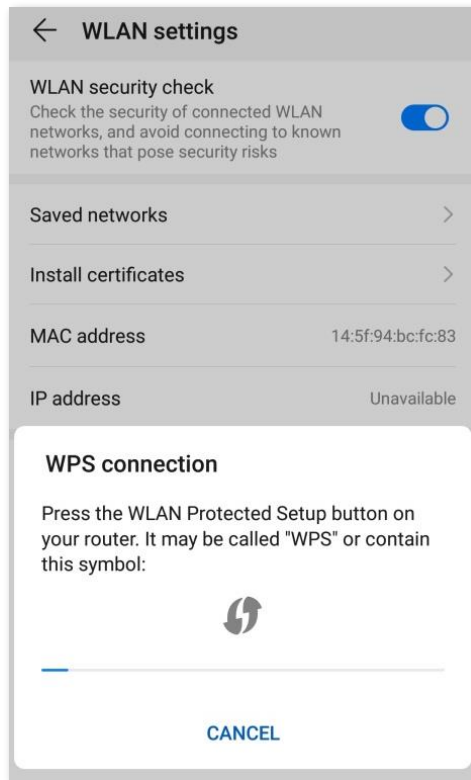


Figure 4-42 WPS negotiation completed

Wait until the smartphone or computer is connected to the WiFi network of the router successfully.

Connect to the WiFi network using the PIN code



Caution

WPS connection using pin code is generally applied on a computer with a wireless adapter. Please refer to the relevant adapter's user guide for detailed instructions.

Step 1 Find the PIN code.

Launch a web browser on the device connected to the router, and visit <http://hikvisionwifi.local>. Navigate to **Route Settings** > **Wireless Settings** > **WPS** to check the PIN code.

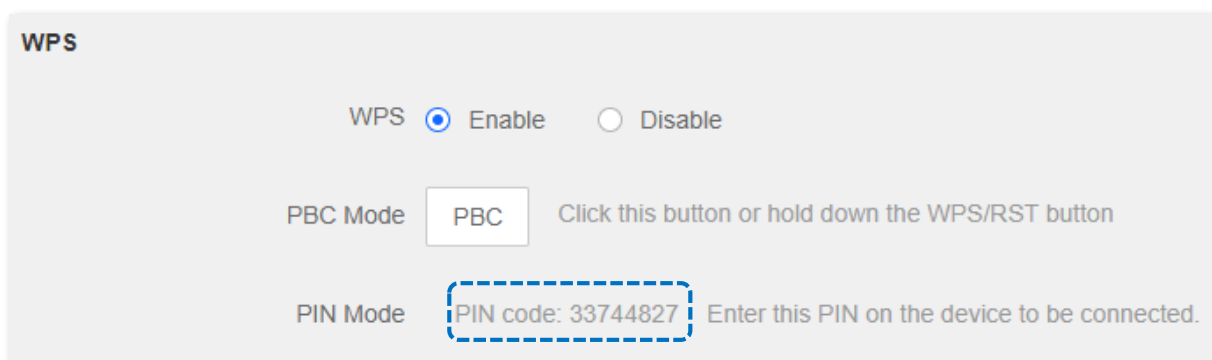


Figure 4-43 Check PIN code

Step 2 Enter the PIN code on the wireless device for connection.

Wait until the smartphone or computer is connected to the WiFi network of the router successfully.

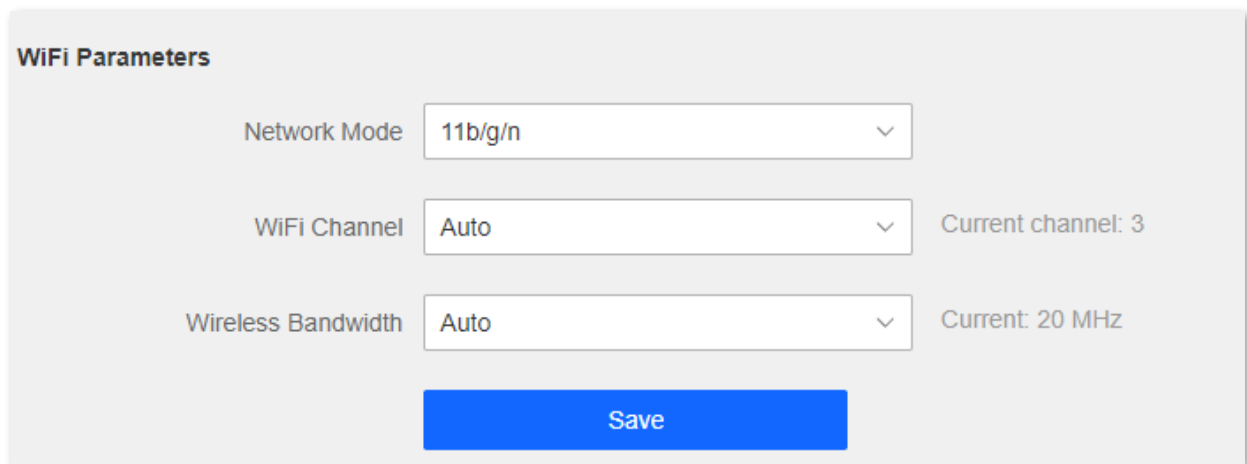
4.2.6 WiFi parameters

In this section, you can change network mode, wireless channel, and wireless bandwidth of 2.4 GHz WiFi network.

To access the configuration page, log in to the web UI of the router, and navigate to **Route Settings > Wireless Settings > WiFi Parameters**.

Note

In order not to influence the wireless performance, it is recommended to maintain the default settings on this page without professional instructions.



WiFi Parameters

Network Mode	11b/g/n	
WiFi Channel	Auto	Current channel: 3
Wireless Bandwidth	Auto	Current: 20 MHz

Save

Figure 4-44 WiFi parameters

Table 4-7 WiFi parameter description

Parameter	Description
Network Mode	<p>It specifies various protocols adopted for wireless transmission. 2.4 GHz WiFi network supports 11b, 11g, 11b/g mixed and 11b/g/n mixed modes.</p> <ul style="list-style-type: none"> ● 11b/g/n: It indicates that all devices compliant with IEEE 802.11b or IEEE 802.11g protocol, or work at 2.4 GHz with IEEE 802.11n protocol can connect to the 2.4 GHz WiFi network of the router, therefore enjoying a maximum transmission rate of 300 Mbps. ● 11b/g: It indicates that devices compliant with IEEE 802.11b or IEEE 802.11g protocol can connect to the 2.4 GHz WiFi network of the router, enjoying a maximum transmission rate of 54 Mbps. ● 11b: It indicates that devices compliant with IEEE 802.11b protocol can connect to the 2.4 GHz WiFi network of the router, enjoying a maximum transmission rate of 11 Mbps. ● 11g: It indicates that devices compliant with IEEE 802.11g protocol can connect to the 2.4 GHz WiFi network of the router, enjoying a maximum transmission rate of 54 Mbps.
WiFi Channel	<p>It specifies the operating channel of a WiFi network. By default, the wireless channel is Auto, which indicates that the router selects a channel for the WiFi network automatically. You are recommended to choose a channel with less interference for better wireless transmission efficiency. You can use a third-party tool to scan the WiFi signals nearby to understand the channel usage situations.</p>
Wireless Bandwidth	<p>It specifies the bandwidth of the wireless channel of a WiFi network. Change the default settings only when necessary. By default, the wireless bandwidth is Auto.</p> <ul style="list-style-type: none"> ● 40MHz: It indicates that the channel bandwidth of a router is 40 MHz. ● 20MHz: It indicates that the channel bandwidth of a router is to 20 MHz.

Chapter 5 Client management

5.1 Access control

5.1.1 Overview

By configuring this function, you can limit the upload and download speed of devices connected to the router and allocate the bandwidth reasonably. On this page you can:

- [Set the upload and download speed limit](#)
- [Add devices to the blacklist](#)
- [Remove devices from the blacklist](#)

To access the configuration page, log in to the web UI of the router and navigate to **Client Management > Access Control**.

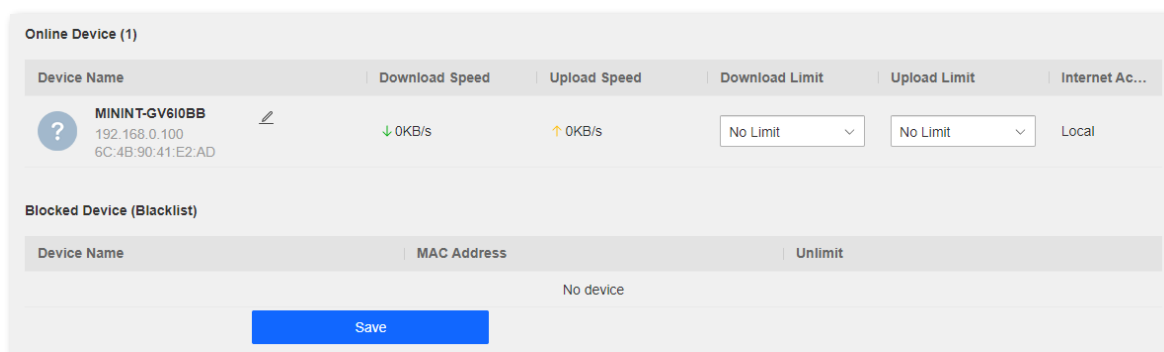





Figure 5-1 Access control

Table 5-1 Access control parameter description

Parameter		Description
Online Device	Device Name	It shows the information of the online device, including the device name and IP address. You can click  to customize the device name for easier management.
	Download Speed	It specifies the current upload and download speeds of the device.
	Upload Speed	
	Download Limit	It allows you to specify the maximum upload and download speeds for the device.
	Upload Limit	
Internet Access	It specifies whether the device can access the internet. <ul style="list-style-type: none"> ●  : It indicates that the device can access the internet. ●  : It indicates that the device is unable to access the internet. ● Local: It indicates that the device is managing the web UI of the router. 	
Blocked Device (Blacklist)	Device Name	It specifies the device name of a blocked device.
	MAC Address	It specifies the MAC address of a blocked device.
	Unlimit	It is used to remove a blocked device from the blacklist. After being removed from the blacklist, the device can reconnect to the router for internet access.

5.1.2 Set the upload and download speed limit

Scenario: You want to allocate bandwidth equally and enable all connected devices to enjoy smooth 720p videos.

Solution: Configure the bandwidth control function to meet the requirement.

Procedures:

Step 1 Launch a web browser on a device connected to the router and visit <http://hikvisionwifi.local> to log in to the web UI of the router.

Step 2 Navigate to **Client Management > Access Control**.

Step 3 Target the devices to be controlled, set the **Download Limit** to **512 KB/s (HD Videos)**, and set the **Upload Limit** to **32KB/s**.

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

Device Name	Download Speed	Upload Speed	Download Limit	Upload Limit	Internet Access
MININT-GV610BB 192.168.0.200 6C:4B:90:41:E2:AD	↓ 0KB/s	↑ 0KB/s	512 KB/s (HD Videos)	32KB/s	Local
User 192.168.0.199 32:D0:08:4B:64:48	↓ 0KB/s	↑ 0KB/s	128 KB/s (Web)	32KB/s	<input checked="" type="checkbox"/>

Figure 5-2 Set the upload and download speed limit

After the configuration, the highest speed for the device is 4 Mbps (or 512 KB/s) and satisfies the requirement of 720p videos.

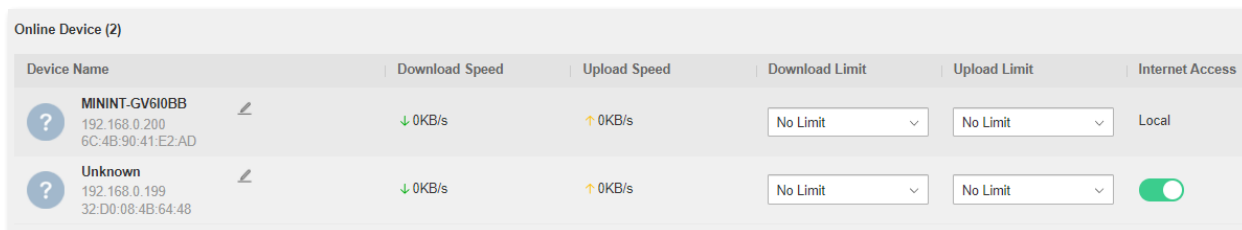
5.1.3 Add the device to the blacklist

Add devices to the blacklist to block internet access:

Step 1 Launch a web browser on a device connected to the router and visit **http://hikvisionwifi.local** to log in to the web UI of the router.

Step 2 Navigate to **Client Management > Access Control**.

Step 3 Click corresponded to the device to be blocked to change the status to .

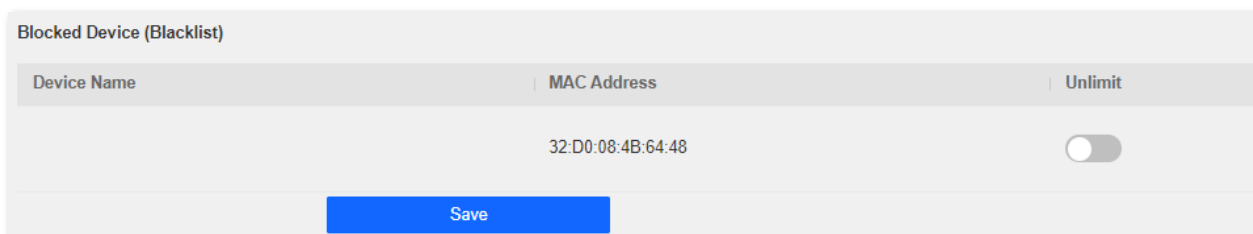


Device Name	Download Speed	Upload Speed	Download Limit	Upload Limit	Internet Access
MININT-GV6I0BB 192.168.0.200 6C:4B:90:41:E2:AD	↓ 0KB/s	↑ 0KB/s	No Limit	No Limit	Local
Unknown 192.168.0.199 32:D0:08:4B:64:48	↓ 0KB/s	↑ 0KB/s	No Limit	No Limit	<input checked="" type="checkbox"/>

Figure 5-3 Add device to the blacklist

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

The blocked device is shown on the blacklist.



Device Name	MAC Address	Unlimit
	32:D0:08:4B:64:48	<input type="checkbox"/>

Save

Figure 5-4 Blocked device

5.1.4 Remove the device from the blacklist

Procedures:

Step 1 Launch a web browser on a device connected to the router and visit **<http://hikvisionwifi.local>** to log in to the web UI of the router.

Step 2 Navigate to **Client Management > Access Control > Blocked Device (Blacklist)**.

Step 3 Target the device and click to .

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

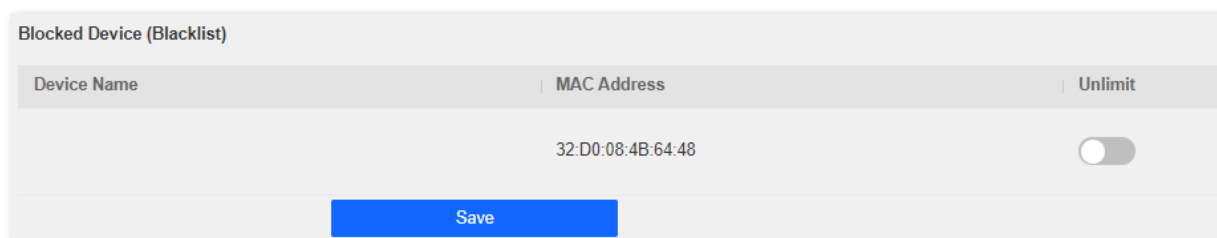


Figure 5-5 Blocked device

After the device is removed from the blacklist, it can access the internet through the router again.

5.2 Parental control

5.2.1 Overview

On the parental control page, you can view the information of online devices and configure their internet access options.

To access the configuration page, log in to the web UI of the router, and navigate to **Client Management > Parental Control Rules** page.

Online Device (1)

Device Name	Online Duration	Manage
MININT-GV6IOBB 192.168.0.200	2h 22m 37s	<input type="checkbox"/>

Parental Control Rules

The following rules take effect on all devices enabling parental control



Allow access during 19 : 00 ~ 21 : 00

Repeat on Everyday Monday Tuesday Wednesday Thursday Friday Saturday Sunday

Website Restrictions

Figure 5-6 Parental control

Table 5-2 Parental control parameter description

Parameter		Description
Online Device	Device Name	It specifies the name of the online device. You can click  to customize the device name for easier management.
	IP Address	It specifies the IP address of the online device.
	Online Duration	It specifies the time that has elapsed since the device connects to the router successfully.
	Manage	It specifies the status of a rule. You can enable/disable the rule by switching the button.
Parental Control Rules	Allow access during	It specifies the period when the internet connection is allowed.
	Repeat on	It specifies the dates when the internet connection is allowed.
	Website Restrictions	It specifies the modes of website restrictions. <ul style="list-style-type: none"> ● Disable: It specifies that all websites are accessible. ● Only Permit: It specifies that only the websites listed in Unblocked Websites are accessible. ● Only Forbid: It specifies that only the websites listed in Blocked Websites are inaccessible.
	Unblocked Websites	It specifies the websites that devices can or cannot access during the " Allow access during " period.
	Blocked Websites	 Note Key words are supported for access restriction. Full website addresses are recommended for precise limits.

5.2.2 An example of configuring parental control

Scenario: The final exam for your daughter is approaching and you want to configure her internet access through the router.



Goal: Your daughter cannot access websites, such as Facebook, Twitter, Youtube, and Instagram, from 8:00 to 22:00 on weekends using the computer in her room, and cannot access the internet from 22:00 to 8:00.

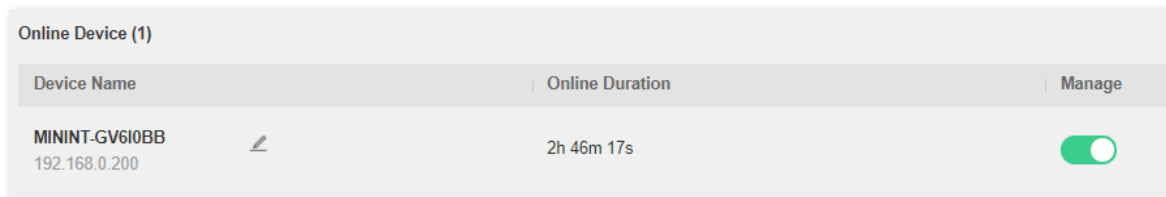
Solution: You can configure the parental controls function to reach the goal.

Procedures:

Step 1 Launch a web browser on a device connected to the router and visit **<http://hikvisionwifi.local>** to log in to the web UI of the router.

Step 2 Navigate to **Client Management > Parental Control Rules**.

Step 3 Set the button from  to .



Online Device (1)		
Device Name	Online Duration	Manage
MININT-GV6I0BB 192.168.0.200	2h 46m 17s	<input checked="" type="checkbox"/>

Figure 5-7 Configure parental control

Step 4 Specify the period when the target websites cannot be accessed, which is **8:00 ~ 22:00** in this example.

Step 5 Tick the days when the rule is applied, which are **Saturday** and **Sunday** in this example.

Step 6 Set **Website Restrictions** to **Only Forbid**.

Step 7 Set **Blocked Websites**, which are **facebook.com**, **twitter.com**, **youtube.com** and **instagram.com**.

Step 8 Click **Save** at the bottom of the page.

Parental Control Rules

The following rules take effect on all devices enabling parental control

Allow access during 08 : 00 ~ 22 : 00

Repeat on Everyday Monday Tuesday Wednesday Thursday Friday Saturday Sunday

Website Restrictions Only Forbid

Blocked Websites Please enter

- 1 facebook.com
- 2 twitter.com
- 3 youtube.com
- 4 instagram.com

Save

Figure 5-8 Set parental control rules

After the configuration is completed, your daughter can access any websites except for Facebook, Twitter, Youtube, and Instagram from 8:00 to 22:00 on weekends, and she cannot access the internet at all between 22:00 to 8:00.

Chapter 6 Advanced

6.1 MAC address filter



6.1.1 Overview

This function enables you to add devices to the whitelist or blacklist to enable or disable specified users to access the internet through the router.

To access the configuration page, log in to the web UI of the router, and navigate to **Advanced > MAC Address Filter**.

Figure 6-1 MAC address filter

Table 6-1 MAC address filter parameter description

Parameter	Description
Filter Mode	It specifies the MAC address filter mode. <ul style="list-style-type: none"> ● Blacklist: Wireless devices listed are unable to connect to the WiFi network of the router, and wired devices listed are unable to access the internet. ● Whitelist: Only wireless devices listed can connect to the WiFi network of the router, and wired devices listed can access the internet.
Blacklisted MAC Address	It specifies the MAC address of the device to which a rule applies.
Whitelisted MAC Address	
Remark (Optional)	It specifies the description of a rule.
Operation	<div style="display: flex; flex-direction: column; gap: 5px;">  : Click it to add a device to the blacklist/whitelist.  : Click it to delete a device from the blacklist/whitelist. </div>
Whitelist all online devices	It is only available when you set the whitelist for the first time. By clicking it, you can add all currently connected devices to the whitelist.

6.1.2 Only allow specified device to access the internet

Scenario: The WiFi network in your home is misused by unknown users sometimes.

Goal: Only allow certain devices of family members to access the internet.

Solution: You can configure the MAC address filter function to reach the goal.

Assume the MAC address and connection status of your domestic devices are as follows.

Table 6-2 MAC address connection status

Device	MAC address	Status
Your own phone	6C:4B:90:41:E2:AD	Connected
Wife's phone	94:C6:91:29:C2:12	Disconnected
Daughter's phone	98:9C:57:19:D0:1B	Disconnected

Procedures:

Step 1 Launch a web browser on a device connected to the router and visit <http://hikvisionwifi.local> to log in to the web UI of the router.

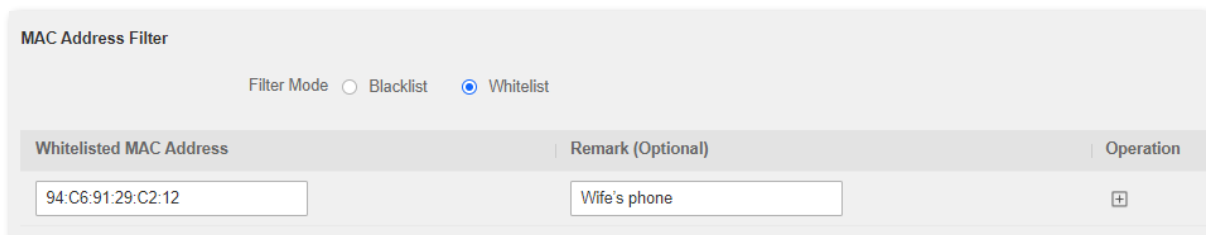
Step 2 Navigate to **Advanced > MAC Address Filter**.

Step 3 Set the **Filter Mode** to **Whitelist**.

Step 4 Enter the **Whitelisted MAC Address** of the device, which is **94:C6:91:29:C2:12** in this example.

Step 5 (Optional) Enter the remark for the device, which is **Wife's phone** in this example.

Step 6 Click  .



MAC Address Filter

Filter Mode Blacklist Whitelist


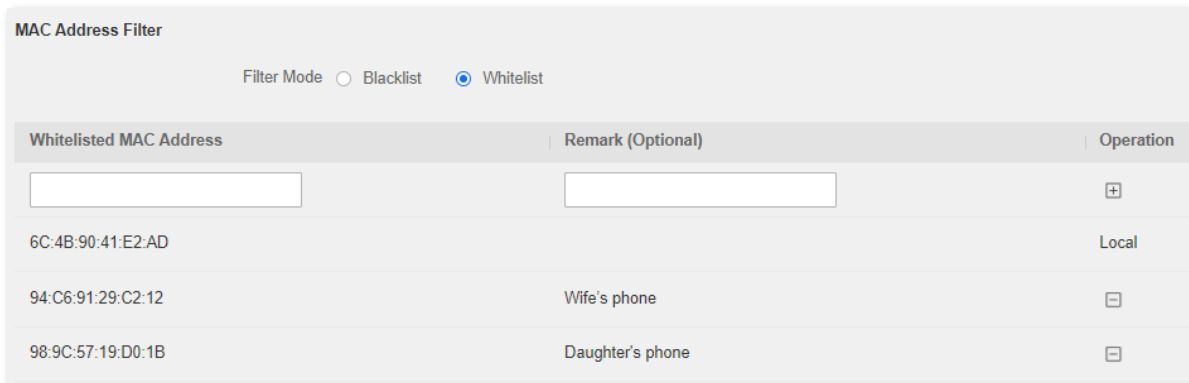
Whitelisted MAC Address	Remark (Optional)	Operation
94:C6:91:29:C2:12	Wife's phone	

Figure 6-2 Add white MAC address

Step 7 Repeat **Step 4** to **Step 6** to add the **Daughter's phone (98:9C:57:19:D0:1B)** to the whitelist.

Step 8 Click **Save** at the bottom of the page.



MAC Address Filter

Filter Mode Blacklist Whitelist

Whitelisted MAC Address	Remark (Optional)	Operation
<input type="text"/>	<input type="text"/>	<input type="button" value="⊕"/>
6C:4B:90:41:E2:AD		Local
94:C6:91:29:C2:12	Wife's phone	<input type="button" value="⊖"/>
98:9C:57:19:D0:1B	Daughter's phone	<input type="button" value="⊖"/>

Figure 6-3 Whitelisted MAC address

When the configuration is completed, only the three devices added can access the internet through the router.

6.2 IP-MAC binding



6.2.1 Overview

Through the IP-MAC binding function, specified clients can always obtain the same IP address when connecting to the router, ensuring that the router's "Port Mapping", "DDNS", "DMZ host" and other functions can function normally. This function takes effect only when the DHCP server function of the router is enabled.

To access the configuration page, log in to the web UI of the router, and navigate to **Advanced > IP-MAC Binding**.

Figure 6-4 IP-MAC binding

Table 6-3 IP-MAC binding parameter description

Parameter	Description
IP Address	It specifies the IP address to be reserved for the client with the specified MAC address. It should belong to the DHCP address pool.
MAC Address	It specifies the MAC address of the client that needs a fixed IP address.
Operation	<p> : It is used to add an IP-MAC binding rule.</p> <p> : It is used to delete an IP-MAC binding rule.</p>

6.2.2 Assign fixed IP addresses to LAN clients

Scenario: You have set up an FTP server within your LAN.

Goal: Assign a fixed IP address to the host of the FTP server and prevent the failure of access to the FTP server owing to the change of IP address.

Solution: You can configure the IP-MAC binding function to reach the goal.

Assume that the information of the FTP server includes:

- The fixed IP address for the server: 192.168.0.136
- MAC address of the FTP server host: 00 00 00 00 00 01

Procedures:

Step 1 Launch a web browser on a device connected to the router and visit **http://hikvisionwifi.local** to log in to the web UI of the router.

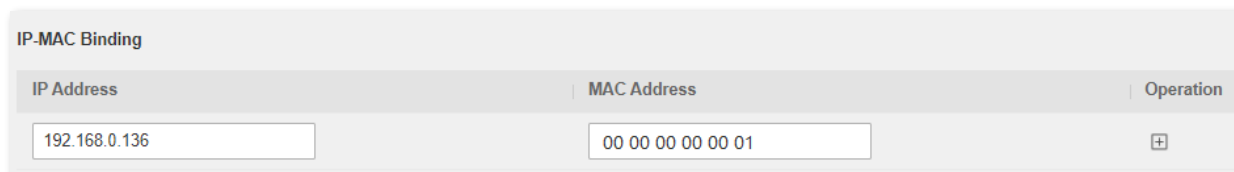
Step 2 Navigate to **Advanced > IP-MAC Binding**.

Step 3 Enter an IP address included in the DHCP address pool, which is **192.168.0.136** in this example.

Step 4 Enter the MAC address of the client which needs a fixed IP address, which is **00:00:00:00:00:01** in this example.

Step 5 Click **+** .

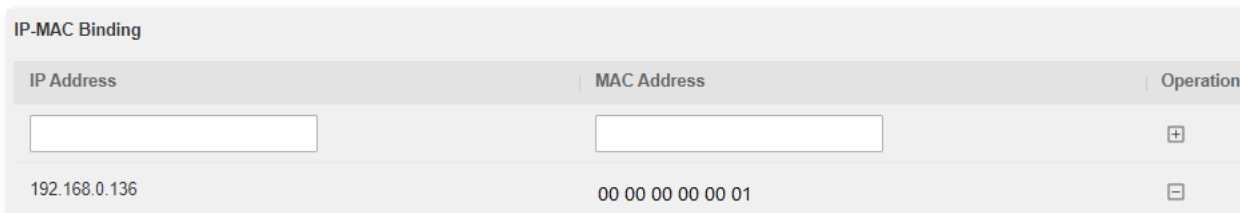
Step 6 Click **Save** at the bottom of the page.



IP Address	MAC Address	Operation
192.168.0.136	00 00 00 00 00 01	+

Figure 6-5 IP-MAC binding

When the configuration is completed, the page is shown as below and the FTP server host always gets the same IP address when connecting to the router, which is 192.168.0.136 in this example.



IP Address	MAC Address	Operation
		+
192.168.0.136	00 00 00 00 00 01	-

Figure 6-6 IP-MAC binding

6.3 Port mapping

6.3.1 Overview

By default, internet users cannot actively access the LAN of the router.

The port mapping function opens a port of the router, and binds the LAN server to the port using the server's IP address and intranet service port. All-access requests to the WAN port of the router will be directed to the server. Therefore, the server within the LAN can be accessed by internet users and the LAN can be free from attacks from the internet.

For example, the port mapping function enables internet users to access web servers or FTP servers within the LAN.

To access the configuration page, log in to the web UI of the router, and navigate to **Advanced > Port Mapping**.

Internal IP Address	Internal Port	External Port	Protocol	Operation
<input type="text"/>	21 (FTP) ▾	21	Both ▾	+

Figure 6-7 Port mapping

Table 6-4 Port mapping parameter description

Parameter	Description
Internal IP Address	It specifies the IP address of a server that resides on the LAN.
Internal Port	It specifies the service port number of the internal server. You can either choose a port from the drop-down list or specify a port manually.
External Port	It specifies the service port number for internet users to access a specified service. When the internal port is selected or specified, the external port will be occupied automatically. You can also change it as required.
Protocol	It specifies the protocol that specified service uses. Both indicate that both TCP and UDP are used. If you are uncertain about it, Both are recommended.
Operation	+ : It is used to add a port mapping rule. - : It is used to delete a port mapping rule.

6.3.2 Enable internet users to access LAN resources using an IP address

Scenario: You have set up an FTP server within your LAN.

Goal: Open the FTP server to internet users and enable family members who are not at home to access the resources of the FTP server from the internet.

Solution: You can configure the port mapping function to reach the goal.

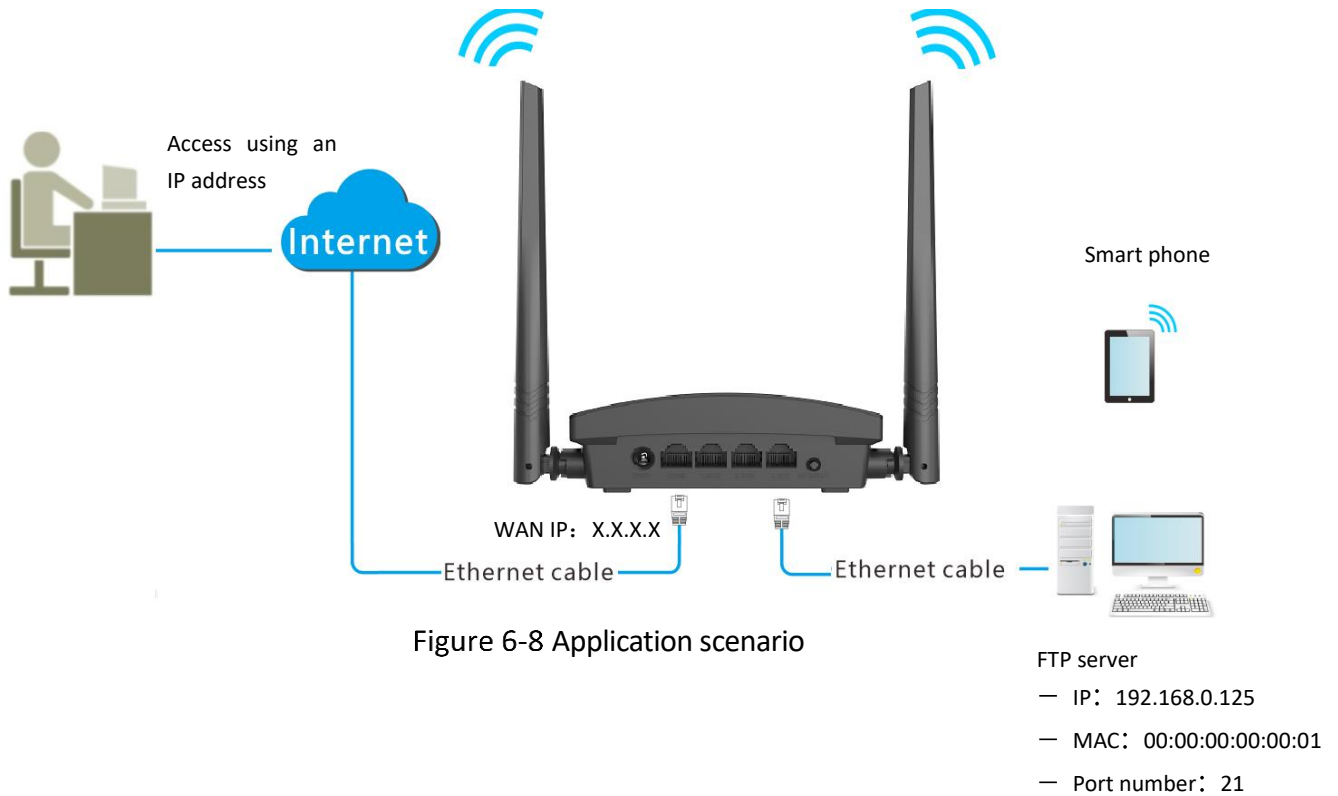
Assume that the information of the FTP server includes:

- IP address: 192.168.0.125
- MAC address: 00 00 00 00 00 01
- Service port: 21
- The WAN IP address of the router: X.X.X.X.



Note

- Please ensure that the router obtains an IP address from the public network. This function may not work on a host with an IP address of a private network or an intranet IP address assigned by ISPs that start with 100. Common IPv4 addresses are classified into class A, class B and class C. Private IP addresses of class A range from 10.0.0.0 to 10.255.255.255; Private IP addresses of class B range from 172.16.0.0 to 172.31.255.255; Private IP addresses of class C range from 192.168.0.0 to 192.168.255.255.
- ISPs may block unreported web services to be accessed with the default port number 80. Therefore, when the default LAN port number is 80, please change it to an uncommon port number (1024 to 65535) manually, such as 9999.
- The LAN port number and the WAN port number can be different.



Procedures:

Step 1 Launch a web browser on a device connected to the router and visit <http://hikvisionwifi.local> to log in to the web UI of the router.

Step 2 Add a port mapping.

- 1) Navigate to **Advanced > Port Mapping**.
- 2) Enter the **Internal IP Address**, which is **192.168.0.125** in this example.
- 3) Select an **Internal Port** in the drop-down box, which is **21** in this example.
- 4) Select a protocol, which is **Both** in this example.
- 5) Click **+** .
- 6) Click **Save** at the bottom of the page.

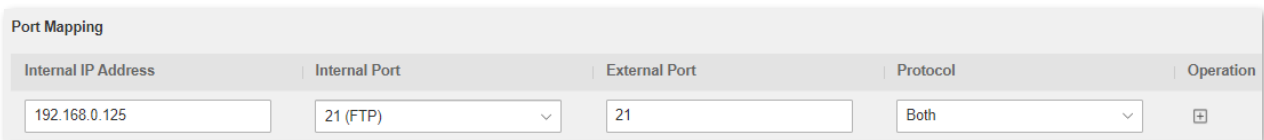


Figure 6-9 Add a port mapping

The port mapping rule is added when the page is shown as below.

Port Mapping				
Internal IP Address	Internal Port	External Port	Protocol	Operation
<input type="text"/>	21 (FTP)	21	Both	<input type="button" value="⊕"/>
192.168.0.125	21	21	Both	<input type="button" value="⊖"/>

Figure 6-10 Port mapping rule is added

Step 3 Assign a fixed IP address to the host where the server locates.

- 1) Navigate to **Advanced > IP-MAC Binding**.
- 2) Specifies an **IP Address** for the host of the server, which is **192.168.0.125** in this example.
- 3) Enter the **MAC Address** of the host of the server, which is **00:00:00:00:00:01** in this example.
- 4) Click .
- 5) Click **Save** at the bottom of the page.

IP-MAC Binding		
IP Address	MAC Address	Operation
<input type="text"/>	<input type="text"/>	<input type="button" value="⊕"/>
192.168.0.125	00 00 00 00 00 01	<input type="button" value="⊖"/>

Figure 6-11 IP-MAC binding

When completing the configurations, users from the internet can access the FTP server by visiting “Intranet service application layer protocol name://WAN IP address of the router”. If the external port number is not the same as the default intranet service port number, the visiting address should be: “Intranet service application layer protocol name://WAN IP address of the router:external port number”.

In this example, the address is "**ftp://X.X.X.X**". You can find the WAN IP address of the router in [View system information](#).

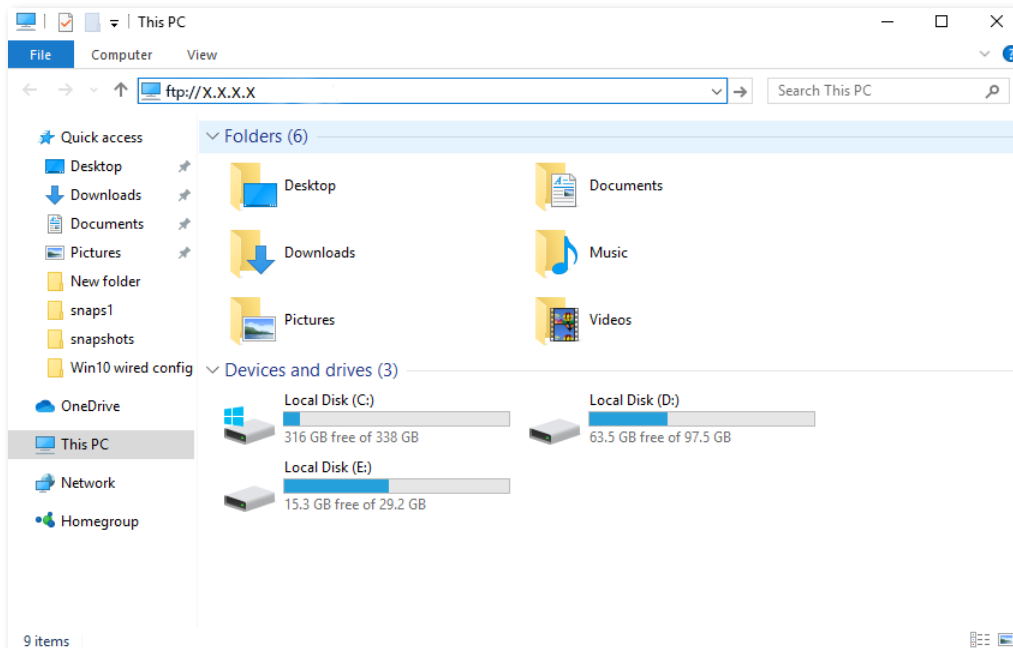


Figure 6-12 Enter the **ftp://X.X.X.X**

Enter the user name and password to access the resources on the FTP server.

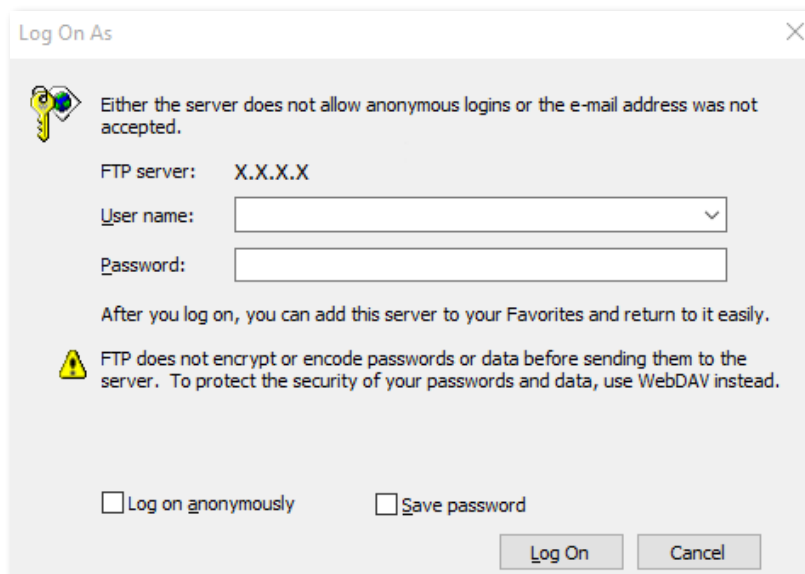


Figure 6-13 Enter the user name and password

If you want to access the server within a LAN using a domain name, refer to the solution [DDNS](#) + [Port mapping](#).

 **Note**

After the configurations, if internet users still cannot access the FTP server, try the following methods:

- Ensure that the internal port number configured in the port mapping function is the same as the service port number set on the server.
- Close the firewall, antivirus software and security guards on the host of the FTP server and try again.

6.4 DDNS

6.4.1 Overview

DDNS normally interworks with port mapping, DMZ host and remote management, so that the internet users can be free from the influence of dynamic WAN IP addresses and access the internal server or the router's web UI with a fixed domain name.

To access the configuration page, log in to the web UI of the router, and navigate to **Advanced > DDNS**.

This function is disabled by default. When it is enabled, the page is shown as below.

DDNS

DDNS Enable Disable

Service Provider [Register Now](#)

DDNS User Name

DDNS Password

Connection Status

Figure 6-14 DDNS

Table 6-5 DDNS parameter description

Parameter	Description
DDNS	It specifies whether to enable the DDNS function.
Service Provider	It specifies a DDNS service provider, including oray.com, 88ip.cn and dyn.com.
DDNS User Name	It specifies the user name and password registered on a DDNS service provider's website for logging in to the DDNS service.
DDNS Password	
DDNS Host Name	It specifies the domain name you applied on the website of your service provider. It is only required when dyn.com is chosen as the service provider.
Connection Status	It specifies the current connection status of the DDNS service.

6.4.2 Enable internet users to access LAN resources using a domain name

Scenario: You have set up an FTP server within your LAN.

Goal: Open the FTP server to internet users and enable family members who are not at home to access the resources of the FTP server from the internet with a domain name.

Solution: You can configure the DDNS and port mapping functions to reach the goal.

Assume that the information of the FTP server includes:

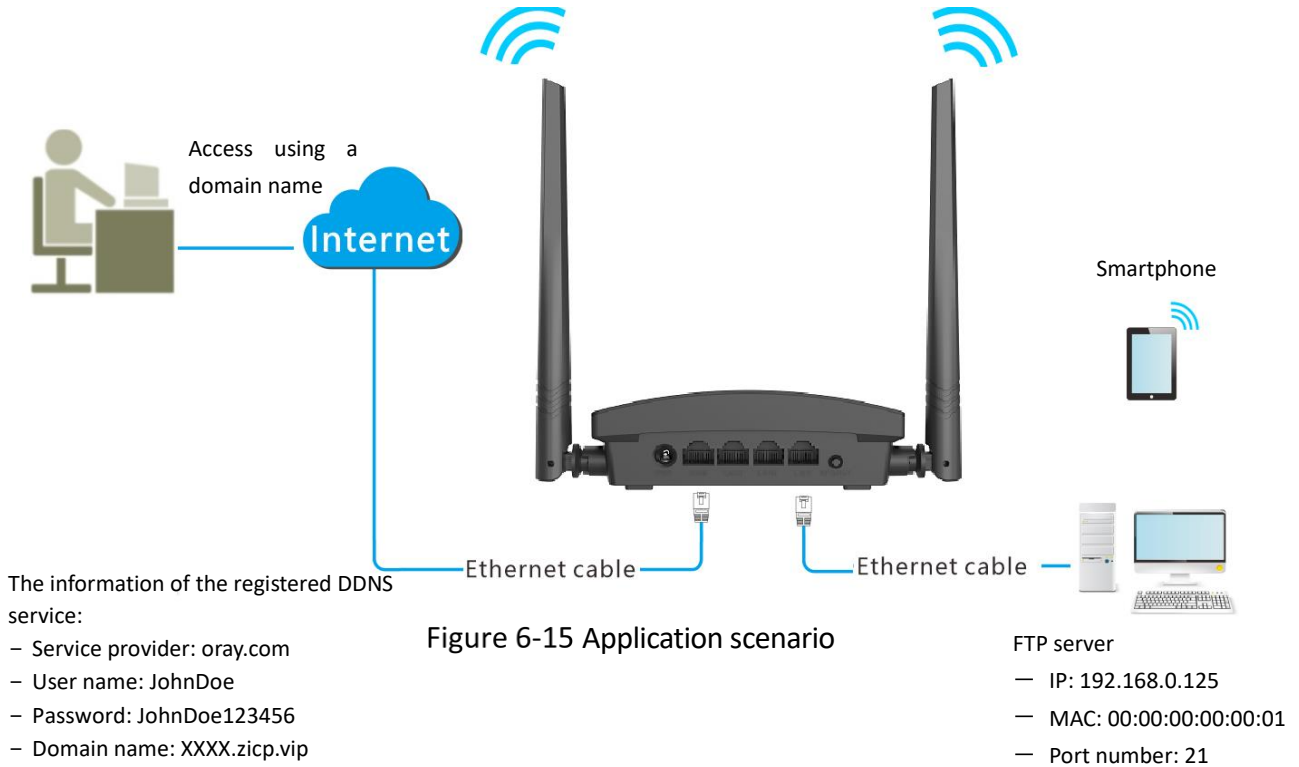
- IP address: 192.168.0.125
- MAC address of the host: 00:00:00:00:00:01
- Service port: 21

The information of the registered DDNS service:

- Service provider: oray.com
- User name: JohnDoe
- Password: JohnDoe123456
- Domain name: XXXX.zicp.vip

Note

Please ensure that the router obtains an IP address from the public network. This function may not work on a host with an IP address of a private network or an intranet IP address assigned by ISPs that start with 100. Common IPv4 addresses are classified into class A, class B and class C. Private IP addresses of class A range from 10.0.0.0 to 10.255.255.255; Private IP addresses of class B range from 172.16.0.0-172.31.255.255; Private IP addresses of class C range from 192.168.0.0-192.168.255.255.



Procedures:

Step 2 Launch a web browser on a device connected to the router and visit **http://hikvisionwifi.local** to log in to the web UI of the router.

Step 3 Configure the DDNS function.

- 1) Navigate to **Advanced > DDNS**.
- 2) Set **DDNS** to **Enable**.
- 3) Select a service provider, which is **oray.com** in this example.
- 4) Enter the user name and password, which are **JohnDoe** and **JohnDoe123456** in this example.
- 5) Click **Save** at the bottom of the page.

DDNS

DDNS Enable Disable

Service Provider oray.com Register Now

DDNS User Name JohnDoe

DDNS Password

Connection Status

Figure 6-16 Configure DDNS

Wait a moment, when the Connection Status turns **Connected**, the configurations succeed.

Step 4 Configure the port mapping function (refer to [Port mapping](#)).

When completing the configurations, users from the internet can access the FTP server by visiting “Intranet service application layer protocol name://the domain name”. If the external port number is not the same as the default intranet service port number, the visiting address should be: “Intranet service application layer protocol name://the domain name:external port number”.

In this example, the address is **ftp://XXXX.zicp.vip**.

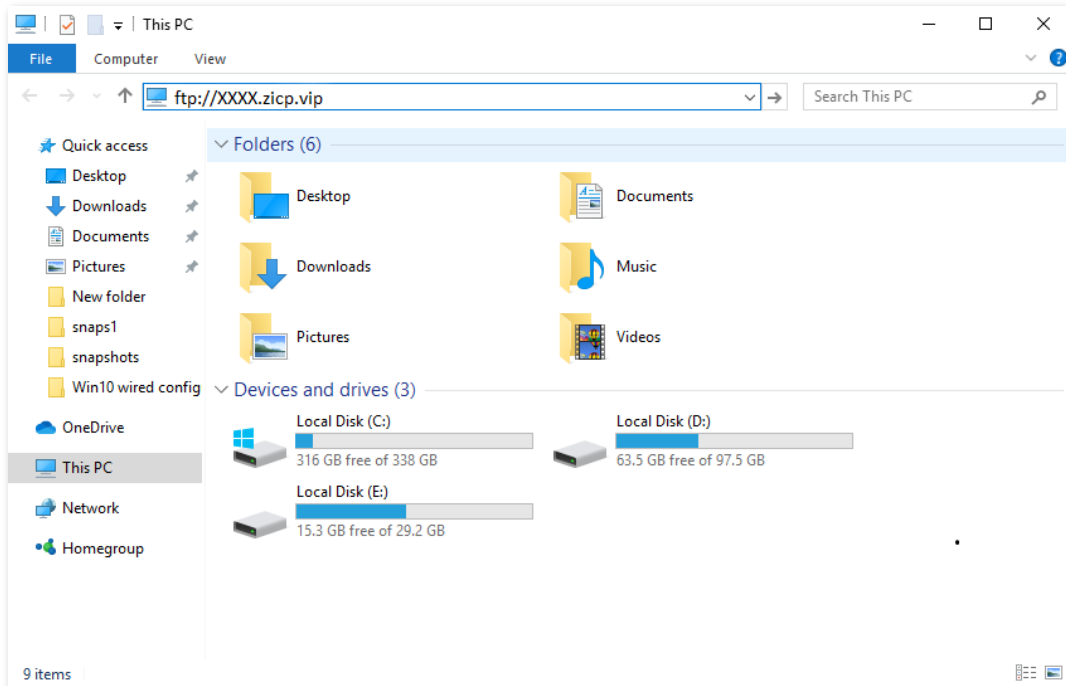


Figure 6-17 Enter the **ftp://XXXX.zicp.vip**

Enter the user name and password to access the resources on the FTP server.

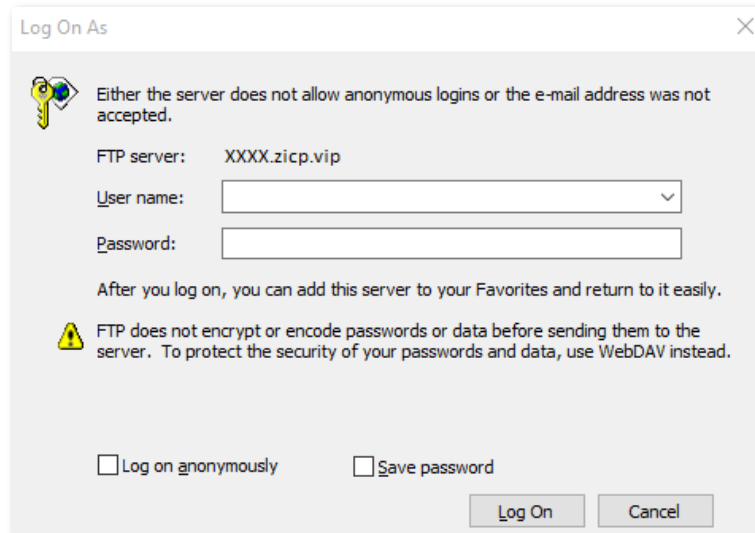


Figure 6-18 Enter the user name and password

 **Note**

After the configurations, if internet users still cannot access the FTP server, try the following methods:

- Ensure that the LAN port number configured in the port mapping function is the same as the service port number set on the server.
- Close the firewall, antivirus software and security guards on the host of the FTP server and try again.

6.5 DMZ host

6.5.1 Overview

A DMZ host on a LAN is free from restrictions when communicating with the internet. It is useful for getting a better and smoother experience in video conferences and online games. You can also set the host of a server within the LAN as a DMZ host when in need of accessing the server from the internet.

Caution

- A DMZ host is not protected by the firewall of the router. A hacker may leverage the DMZ host to attack your LAN. Therefore, enable the DMZ function only when necessary.
- Hackers may leverage the DMZ host to attack the local network. Do not use the DMZ host function randomly.
- Security software, antivirus software, and the built-in OS firewall of the computer may cause DMZ function failures. Disable them when using the DMZ function. If the DMZ function is not required, you are recommended to disable it and enable your firewall, security, and antivirus software.

To access the configuration page, log in to the web UI of the router, and navigate to **Advanced > DMZ Host**.

This function is disabled by default. When it is enabled, the page is shown as below.

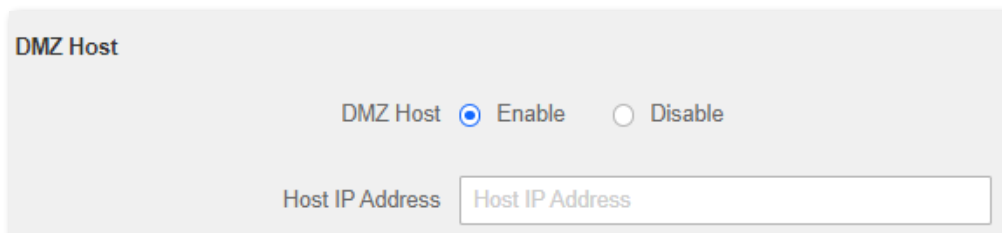


Figure 6-19 DMZ host

Table 6-6 DMZ parameter description

Parameter	Description
DMZ Host	It is used to enable or disable the DMZ function.
Host IP Address	It specifies the IP address to be set as the DMZ host.

6.5.2 Enable internet users to access LAN resources using an IP address

Scenario: You have set up an FTP server within your LAN.

Goal: Open the FTP server to internet users and enable family members who are not at home to access the resources of the FTP server from the internet.

Solution: You can configure the DMZ host function to reach the goal.

Assume that the information of the FTP server includes:

- IP address: 192.168.0.125
- MAC address: 00:00:00:00:00:01
- Service port: 21
- The WAN IP address of the router: X.X.X.X.

Note

Please ensure that the router obtains an IP address from the public network. This function may not work on a host with an IP address of a private network or an intranet IP address assigned by ISPs that start with 100. Common IPv4 addresses are classified into class A, class B and class C. Private IP addresses of class A range from 10.0.0.0 to 10.255.255.255; Private IP addresses of class B range from 172.16.0.0-172.31.255.255; Private IP addresses of class C range from 192.168.0.0-192.168.255.255.

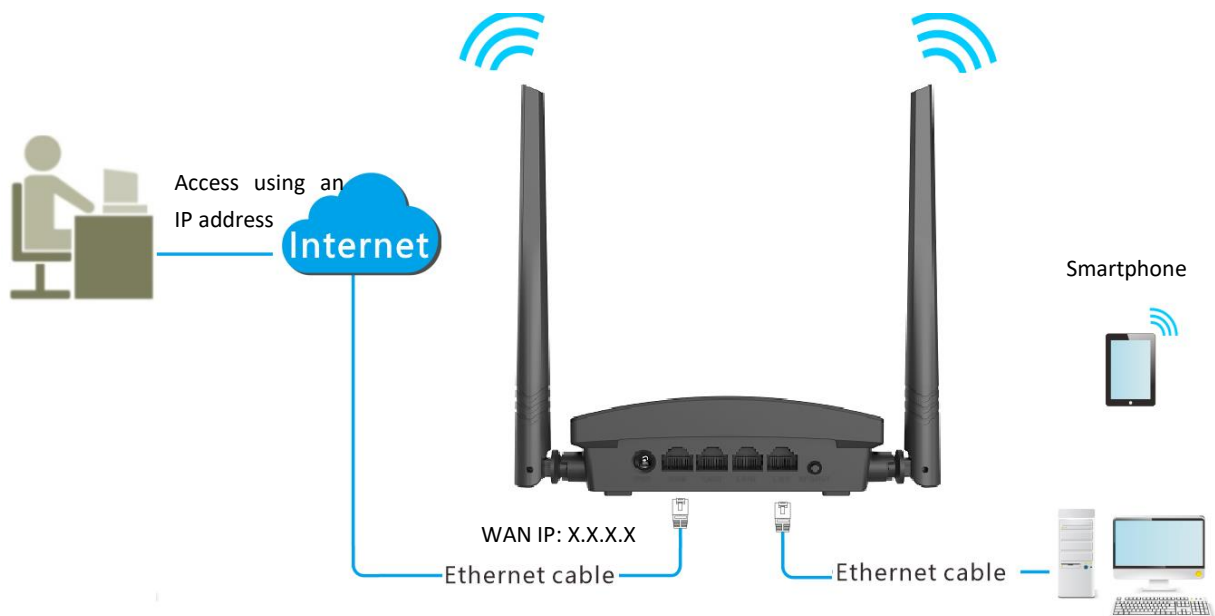


Figure 6-20 Application description

- FTP server
- IP: 192.168.0.125
 - MAC: 00:00:00:00:00:01
 - Port number: 21

Procedures:

Step 1 Launch a web browser on a device connected to the router and visit **http://hikvisionwifi.local** to log in to the web UI of the router.

Step 2 Set the server host as the DMZ host.

- 1) Navigate to **Advanced > DMZ Host**.
- 2) Set **DMZ Host** to **Enable**.
- 3) Enter the IP address of the host, which is **192.168.0.125** in this example.
- 4) Click **Save** at the bottom of the page.

DMZ Host

DMZ Host Enable Disable

Host IP Address

Figure 6-21 Enter the IP address of the host

Step 3 Assign a fixed IP address to the host where the server locates.

- 1) Navigate to **Advanced > IP-MAC Binding**.
- 2) Enter the **IP Address** for the FTP server host, which is **192.168.0.125** in this example.
- 3) Enter the **MAC Address** of the host of the FTP server, which is **00:00:00:00:00:01** in this example.
- 4) Click **+** .

IP Address	MAC Address	Operation
<input type="text" value="192.168.0.125"/>	<input type="text" value="00 00 00 00 00 01"/>	<input style="border: none; background: none;" type="button" value="+"/>

Figure 6-22 IP-MAC binding

- 5) Click **Save** at the bottom of the page.

When the configurations are completed, users from the internet can access the DMZ host by visiting “Intranet service application layer protocol name://WAN IP address of the router”. If the intranet service port number is not the default number, the visiting address should be: “Intranet service application layer protocol name://WAN IP address of the router:intranet service port number”.

In this example, the address is "ftp://X.X.X.X". You can find the WAN IP address of the router in [View system information](#).

 **Note**

When the default intranet service port number is 80, please change the service port number to an uncommon one (1024 to 65535), such as 9999.

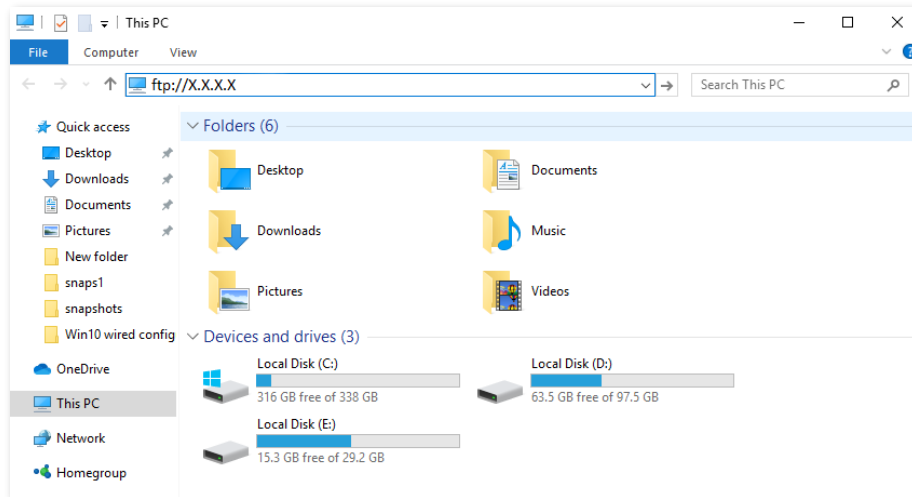


Figure 6-23 Enter the **ftp://X.X.X.X**

Enter the user name and password to access the resources on the FTP server.

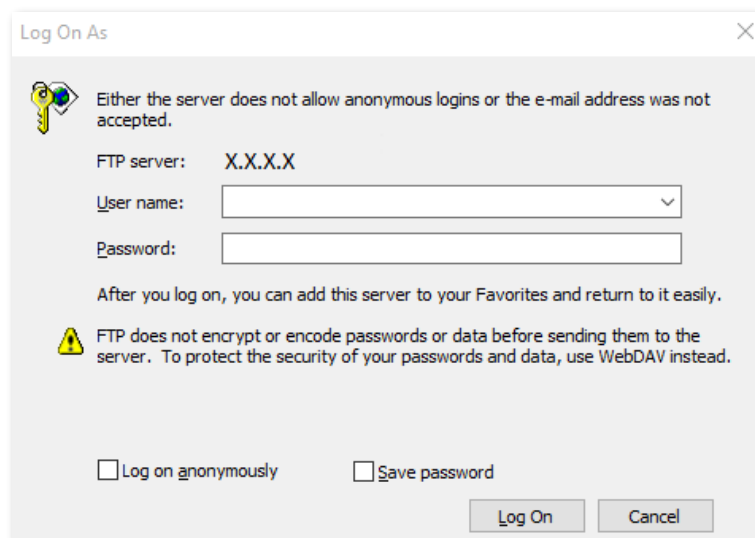


Figure 6-24 Enter the user name and password

If you want to access the server within a LAN using a domain name, refer to the solution [DMZ + DDNS](#).

 **Note**

After the configuration is completed, if internet users still cannot access the FTP server, close the firewall, antivirus software and security guards on the host of the FTP server and try again.

6.6 PING WAN

The PING WAN function enables you to ping the WAN port IP address over the internet to check the connectivity between the router and the internet. It is enabled by default.

Choose **Advance**, and move to the **PING WAN** module to enter the configuration page. This function is disabled by default. When it is enabled, the page is shown as below.

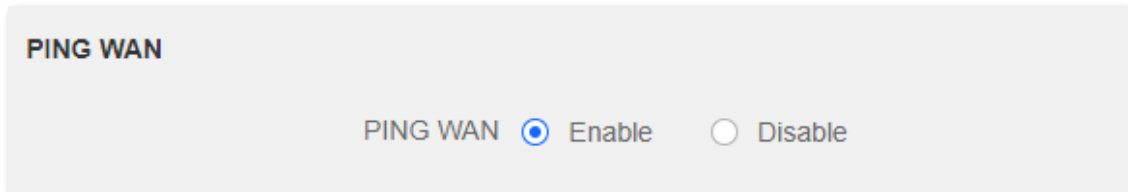


Figure 6-25 PING WAN

6.7 UPnP

UPnP is short for Universal Plug and Play. This function enables the router open port automatically for UPnP-based programs. It is generally used for P2P programs, such as BitComet and AnyChat, and helps increase the download speed.

To access the configuration page, log in to the web UI of the router, and navigate to **Advanced > UPnP**.

This function is enabled by default.

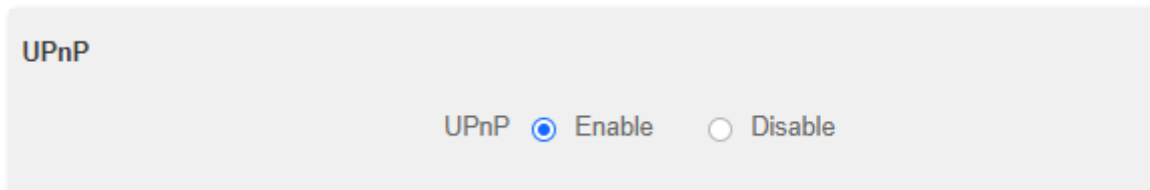
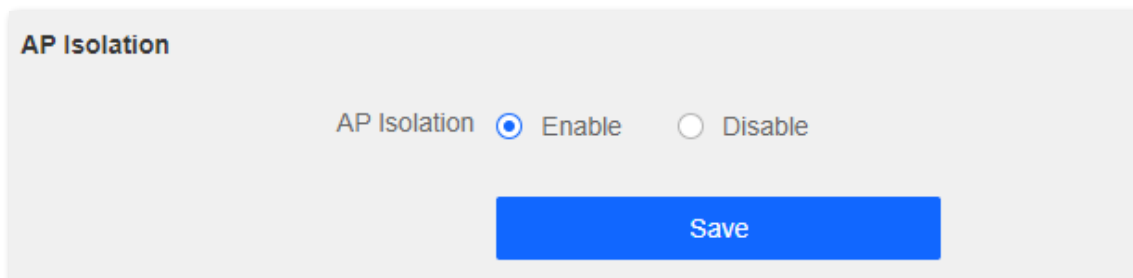


Figure 6-26 UPnP

6.8 AP Isolation

When this function is enabled, wireless clients connected to the same SSID will not be able to communicate with each other, which can enhance wireless network security. This function is disabled by default. When it is enabled, the page is shown as below.



AP Isolation

AP Isolation Enable Disable

Save

Figure 6-27 AP isolation

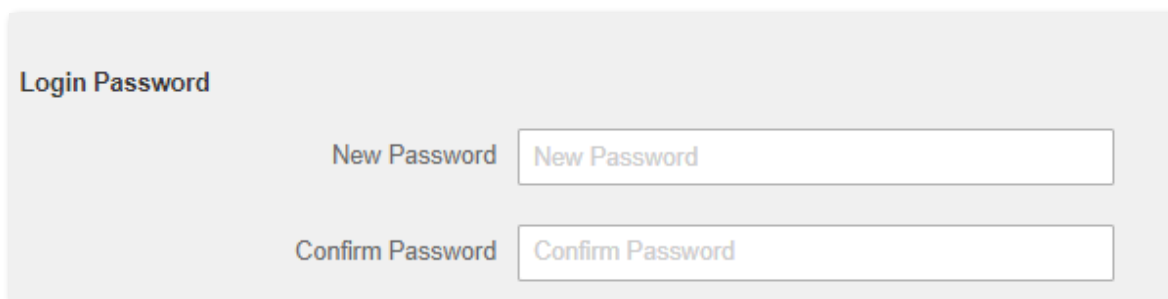
Chapter 7 Administration

7.1 Login password

To ensure network security, a login password is recommended. We recommend you set a complex login password with more types of characters, such as uppercase letters, lowercase letters, numbers and special characters.

To access the login password configuration page, log in to the web UI and navigate to **Administration > Login Password**.

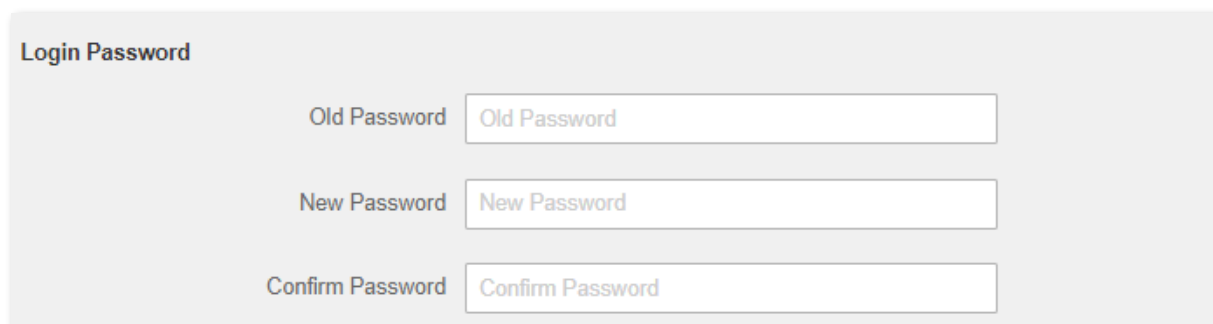
When you use the router for the first time, no password is required to log in to the web UI of the router and you can set a login password on this page.



The screenshot shows a web form titled "Login Password". It contains two input fields: "New Password" and "Confirm Password". Both fields have placeholder text "New Password" and "Confirm Password" respectively.

Figure 7-1 Login password

If you have already set a login password, you can change the password on this page, but the old password is required.



The screenshot shows a web form titled "Login Password". It contains three input fields: "Old Password", "New Password", and "Confirm Password". Each field has placeholder text: "Old Password", "New Password", and "Confirm Password" respectively.

Figure 7-2 Login password

Note

If you forget your login password and cannot log in to the web UI of the router, refer to [Reset the router](#) and log in to the web UI without a password.

7.2 WAN parameters

7.2.1 Change the MTU value

MTU (Maximum Transmission Unit) is the largest data packet transmitted by a network device. When the connection type is PPPoE, the default MTU value is 1480. When the connection type is the dynamic IP address or static IP address, the default MTU value is 1500. Do not change the value unless necessary. If you need to, please refer to the following instructions.

To access the configuration page, log in to the web UI of the router, and navigate to **Administration > WAN Parameters**.

The screenshot shows the 'WAN Parameters' configuration page. The 'MTU' field is highlighted with a blue dashed box. The value is '1500' with a dropdown arrow and the text 'Do not change if unnecessary.' to its right. Below it, the 'Clone MAC Address' is set to 'Restore Default MAC' and the 'WAN Port Speed' is set to 'Auto-negotiation'.

Figure 7-3 Change the MTU value

Generally, the default value is recommended. Try to change the MTU value when:

- You cannot access some specific websites or encrypted websites (such as E-banking or Paypal websites).
- You cannot receive or send Emails or access an FTP or POP server.

You can try reducing the value of MTU gradually from 1500 until the problem is resolved (The recommended range is 1400 to 1500).

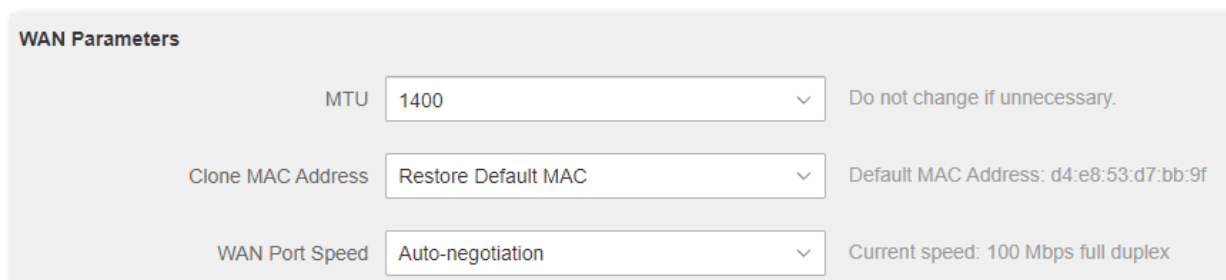
Table 7-1 MTU application description

MTU	Application
1500	It is commonly used for non-ADSL and non-VPN dial-up connections.
1492, 1480	It is used for ADSL dial-up connections.
1472	It is the maximum value for the ping command. A packet with a larger size is fragmented.
1468	It is used for DHCP connections.
1436	It is used for VPN or PPTP connections.

7.2.2 Clone WAN MAC address

If you still cannot access the internet after completing [Internet settings](#), it could be the result of the ISP's configuration to bind the internet account information with a fixed MAC address. In this case, you can clone and change the MAC address of the router to solve the problem.

To access the configuration page, log in to the web UI of the router, and navigate to **Administration > WAN Parameters**.



The screenshot shows the 'WAN Parameters' configuration page. It contains three rows of settings, each with a label, a dropdown menu, and a descriptive note:

Setting	Value	Note
MTU	1400	Do not change if unnecessary.
Clone MAC Address	Restore Default MAC	Default MAC Address: d4:e8:53:d7:bb:9f
WAN Port Speed	Auto-negotiation	Current speed: 100 Mbps full duplex

Figure 7-4 Clone WAN MAC address

- **Restore Default MAC:** Restore the factory setting of the MAC address.
- **Clone Local Host MAC:** Set the MAC address of the router to the same as that of the device which is configuring the router.
- **Manual:** Manually set a MAC address.

Note

Please ensure the cloned MAC address is that of the computer or the router which is already able to access the internet.

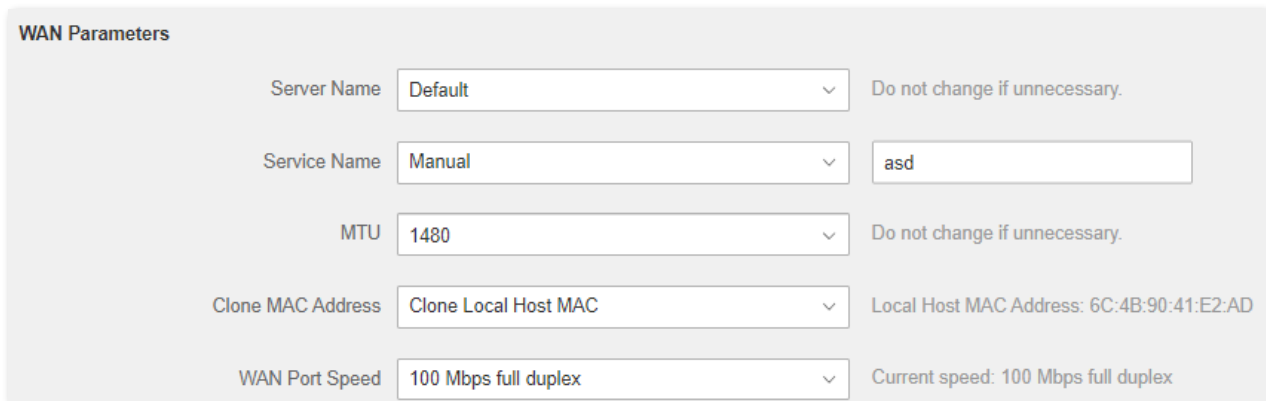
Procedures:

Step 1 Launch a web browser on a device connected to the router and visit **http://hikvisionwifi.local** to log in to the web UI of the router.

Step 2 Navigate to **Administration > WAN Parameters**.

Step 3 Click the drop-down box of **Clone MAC Address**, and choose **Clone Local Host MAC** to copy the MAC address of the management device, or **Manual** to enter the desired MAC address.

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



The screenshot shows the WAN Parameters configuration page. The 'Clone MAC Address' dropdown is set to 'Clone Local Host MAC', and the 'Local Host MAC Address' is displayed as '6C:4B:90:41:E2:AD'. Other parameters include 'Server Name' (Default), 'Service Name' (Manual), 'MTU' (1480), and 'WAN Port Speed' (100 Mbps full duplex).

Parameter	Value	Notes
Server Name	Default	Do not change if unnecessary.
Service Name	Manual	asd
MTU	1480	Do not change if unnecessary.
Clone MAC Address	Clone Local Host MAC	Local Host MAC Address: 6C:4B:90:41:E2:AD
WAN Port Speed	100 Mbps full duplex	Current speed: 100 Mbps full duplex

Figure 7-5 Clone WAN MAC address

7.2.3 Change the WAN speed

To access the configuration page, log in to the web UI of the router, and navigate to **Administration > WAN Parameters**.

When the Ethernet cable is not damaged and connected to the WAN port properly, but **Ethernet cable disconnected** is still shown on the **Internet Settings** page, you can try to change the **WAN Speed** to **10 Mbps full-duplex** or **10 Mbps half-duplex** to solve the problem. Otherwise, keep the default settings.

The screenshot shows the 'WAN Parameters' configuration page. It includes three dropdown menus: 'MTU' (set to 1400), 'Clone MAC Address' (set to Restore Default MAC), and 'WAN Port Speed' (set to Auto-negotiation). The 'WAN Port Speed' dropdown is highlighted with a blue dashed border. To the right of the 'WAN Port Speed' dropdown, it says 'Current speed: 100 Mbps full duplex'.

Figure 7-6 Change the WAN speed

Table 7-2 WAN speed parameter description

WAN Speed	Description
Auto-negotiation	It indicates that the speed and duplex mode are determined through the negotiation with the peer port.
100 Mbps full duplex	It indicates that the WAN port is working at the speed of 100 Mbps, and the port can receive and send data packets at the same time.
100 Mbps half duplex	It indicates that the WAN port is working at the speed of 100 Mbps, but the port can only receive or send data packets alternately.
10 Mbps full duplex	It indicates that the WAN port is working at the speed of 10 Mbps, and the port can receive and send data packets at the same time.
10 Mbps half duplex	It indicates that the WAN port is working at the speed of 10 Mbps, but the port can only receive or send data packets alternately.

7.3 LAN parameters

On this page, you can:

- **Change the LAN IP address and subnet mask of the router.**
- **Change the DHCP server parameters of the router.**

The DHCP server can automatically assign an IP address, subnet mask, gateway and other information to clients within the LAN. If you disable this function, you need to manually configure the IP address information on the client to access the Internet. Do not disable the DHCP server function unless necessary.

- **Configure the DNS information assigned to clients.**

To access the configuration page, log in to the web UI of the router, and navigate to **Administration > LAN Parameters**.

LAN Parameters

LAN IP Address

Subnet Mask

DHCP Server Enable Once disabled, the router no longer assigns IP addresses to hosts

Start IP 192.168.0.


End IP 192.168.0.

Preferred DNS Server

Alternate DNS Server

Figure 7-7 LAN parameters

Table 7-3 LAN parameter description

Parameter	Description
LAN IP Address	It specifies the LAN IP address of the router, which is also the management IP address for logging in to the web UI of the router.
Subnet Mask	It specifies the subnet mask of the LAN port, used to identify the IP address range of the local area network.
DHCP Server	When the DHCP server is enabled, the router automatically assigns an IP address to clients connected to the router
Start IP	It specifies the range of IP addresses that can be assigned to devices connected to the router. The default range is 192.168.0.100 to 192.168.0.200.
End IP	
Preferred DNS Server	<p>It specifies the primary DNS address of the router used to assign to the clients. You can change it if necessary.</p> <p> Note</p> <p>Make sure that the primary DNS server is the IP address of the correct DNS server or DNS proxy. Otherwise, you may fail to access the internet.</p>
Alternate DNS Server	It specifies the secondary DNS address of the router used to assign to the clients. It is an optional field and is left blank by default.

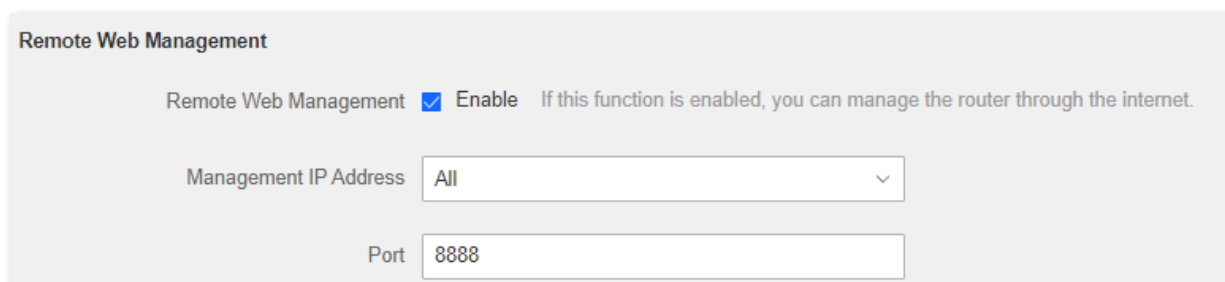
7.4 Remote web management

7.4.1 Overview

Generally, the web UI of the router can only be accessed on devices that are connected to the router by a LAN port or wireless connection. When you encounter a network fault, you can ask for remote technical assistance, which improves efficiency and reduces costs and efforts.

To access the configuration page, log in to the web UI of the router, and navigate to **Administration > Remote Web Management**.

By default, this function is disabled. When this function is enabled, the page is shown as below.



Remote Web Management


Remote Web Management Enable If this function is enabled, you can manage the router through the internet.

Management IP Address All

Port 8888

Figure 7-8 Remote web management

Table 7-4 Remote web management parameter description

Parameter	Description
Remote Web Management	It is used to enable or disable the remote management function of the router.
Management IP Address	It specifies the IP address of the host which can access the web UI of the router remotely. <ul style="list-style-type: none"> ● All: It indicates that hosts with any IP address from the internet can access the web UI of the router. It is not recommended for security. ● Specific: Only the host with the specified IP address can access the web UI of the router remotely. If the host is under a LAN, ensure that the IP address is the IP address of the gateway of the host (a public IP address).
Port	It specifies the port number of the router which is opened for remote management. Change it as required. <p> Note</p> <ul style="list-style-type: none"> ● The port number from 1 to 1024 has been occupied by familiar services. It is strongly recommended to enter a port number from 1025 to 65535 to prevent conflict. ● Remote management can be achieved by visiting "http://the WAN IP address of the router:port number". If the DDNS host function is enabled, the web UI can also be accessed through "http://the domain name of the router's WAN port:port number".

7.4.2 Internet users access the web UI

It specifies the port number of the router which is opened for remote management. Change it as required.

Scenario: You encounter a problem in configuring the router, and the router can access the internet.

Goal: Ask technical support to help you configure the router remotely.

Solution: You can configure the remote management function to reach the goal.

Assume that:

- The IP address of the device that remotely accesses the web UI: 210.76.200.101
- The WAN port IP address of the router: X.X.X.X

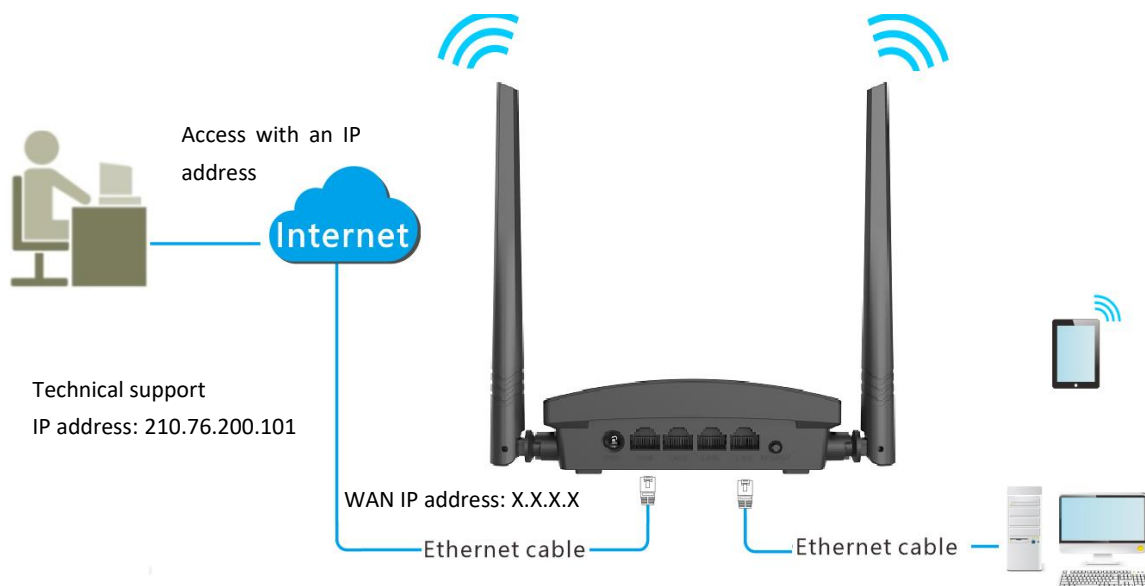


Figure 7-9 Application scenario

Procedures:

- Step 1 Launch a web browser on a device connected to the router and visit **<http://hikvisionwifi.local>** to log in to the web UI of the router.
- Step 2 Navigate to **Administration > Remote Web Management**.
- Step 3 Tick **Enable** of **Remote Web Management** function.
- Step 4 Set **Management IP Address** to **Specific**, and enter the IP address of the device that remotely accesses the web UI, which is **210.76.200.101** in this example.
- Step 5 Enter a port number used to access the router remotely.
- Step 6 Click **Save** at the bottom of the page.

Remote Web Management

Remote Web Management **Enable** If this function is enabled, you can manage the router through the internet.

Management IP Address Specific 210.76.200.101

Port 8888

Figure 7-10 Configure management IP address

When the configuration is completed, the technical support can access and manage the router by visiting "<http://X.X.X.X:8888>" on the computer.

7.5 Date & time

If the system time of the router is incorrect, time-based functions of the router cannot take effect correctly, including the WiFi schedule, parental controls and automatic maintenance functions.

The router supports the synchronization of time with the internet. when the router is connected to the internet, the router will calibrate the system time of the router. You can also set the time zone for your router.

To access the page, log in to the web Ui of the router and navigate to **Administration > Date & Time**.

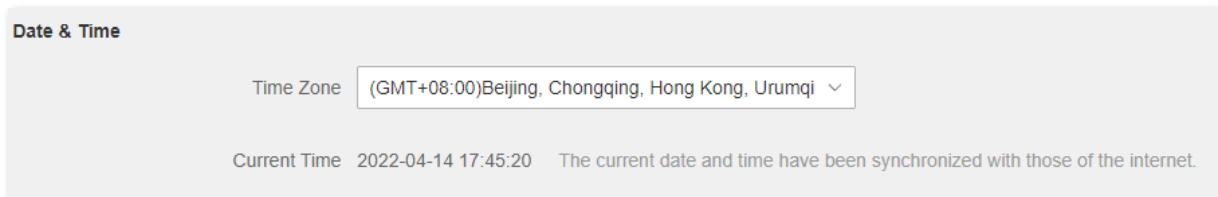


Figure 7-11 Date & time

7.6 Device management

7.6.1 Reboot the router

If any parameter fails to take effect or the router does not work properly, you can try rebooting the router.

Note

Rebooting the router will disconnect all connections to the router. Reboot the router during leisure time.

To reboot the router, log in to the web UI of the router and navigate to **Administration** > **Device Management**. Click **Reboot** to reboot the router.

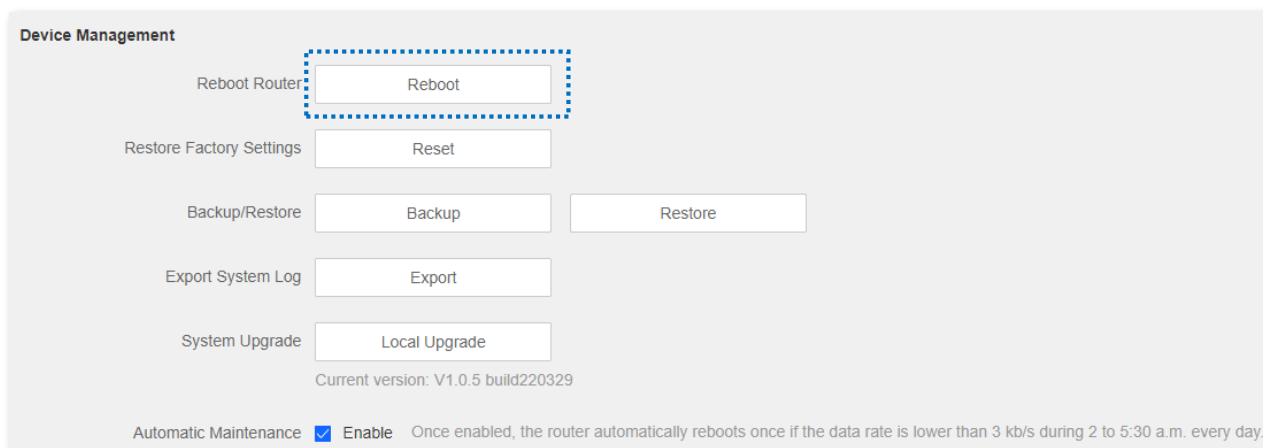


Figure 7-12 Reboot the router

Wait for a moment until the ongoing process finishes. The router reboots successfully.

7.6.2 Reset the router

If you are uncertain about why the internet is inaccessible through the router or you forget the login password of the router, you can reset the router.

Note

- Resetting the router is not recommended unless you cannot find a solution for the current problem anyway. You need to reconfigure the router after it is reset.
- Ensure that the power supply of the router is normal when the router is reset. Otherwise, the router could be damaged.
- The default login IP address is 192.168.0.1 after resetting, and no password is required.

Reset the router using the reset button

Hold down the reset button for about 8 seconds and release it when the LED indicator blinks fast. The router is reset.



Figure 7-13 Reset the router using the reset button

Reset the router on the web UI

Procedures:

Step 1 Launch a web browser on a device connected to the router and visit **<http://hikvisionwifi.local>** to log in to the web UI of the router.

Step 2 Navigate to **Administration > Device Management**.

Step 3 Click **Reset**.

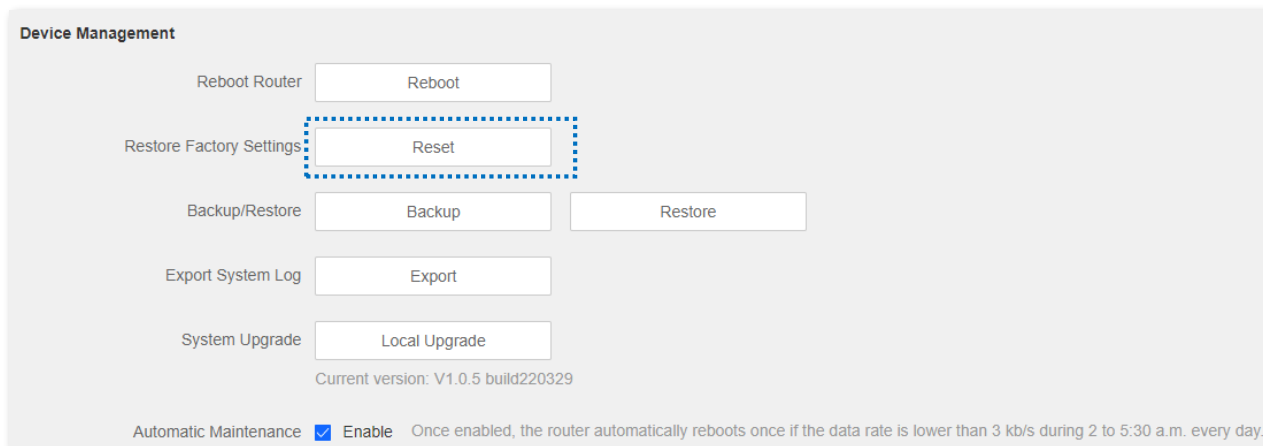


Figure 7-14 Reset the router on the web UI

Step 4 Click **OK** in the pop-up window.

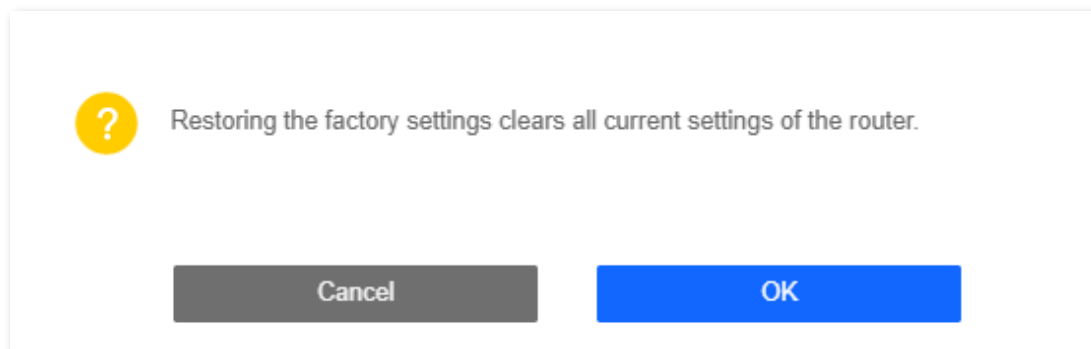


Figure 7-15 Click OK

Wait for a moment until the ongoing process finishes. The router is reset.

7.6.3 Backup/restore configuration

In this module, you can back up the current configurations of the router to your computer. You are recommended to back up the configuration after the settings of the router are significantly changed, or the router works in a good condition.

After you restore the router to factory settings or upgrade it, you can use this function to restore the configurations that have been backed up.

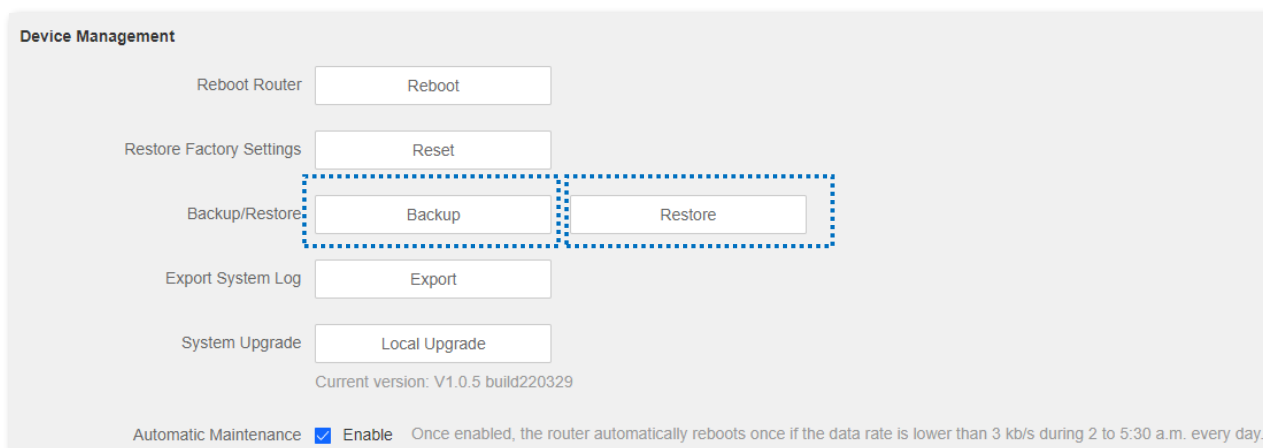


Figure 7-16 Backup/restore configuration

Back up the configurations of the router

Procedures:

Step 1 Launch a web browser on a device connected to the router and visit <http://hikvisionwifi.local> to log in to the web UI of the router.

Step 2 Navigate to **Administration > Device Management**.

Step 3 Click **Backup**.

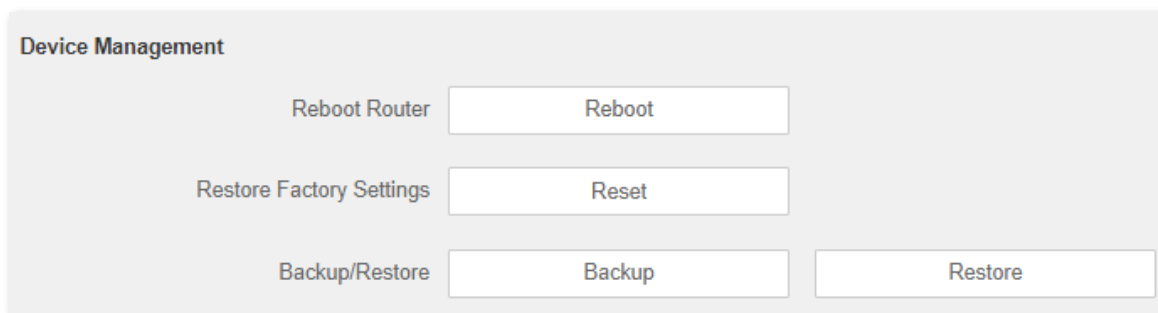


Figure 7-17 Back up the configurations

After the file is downloaded, you can name it **RouterCfm.cfg**.

Restore previous configurations of the router

Procedures:

Step 1 Launch a web browser on a device connected to the router and visit **http://hikvisionwifi.local** to log in to the web UI of the router.

Step 2 Navigate to **Administration > Device Management**.

Step 3 Click **Restore**.

Step 4 Select the configuration file to be restored (extension: **cfg**), and click **Open**.

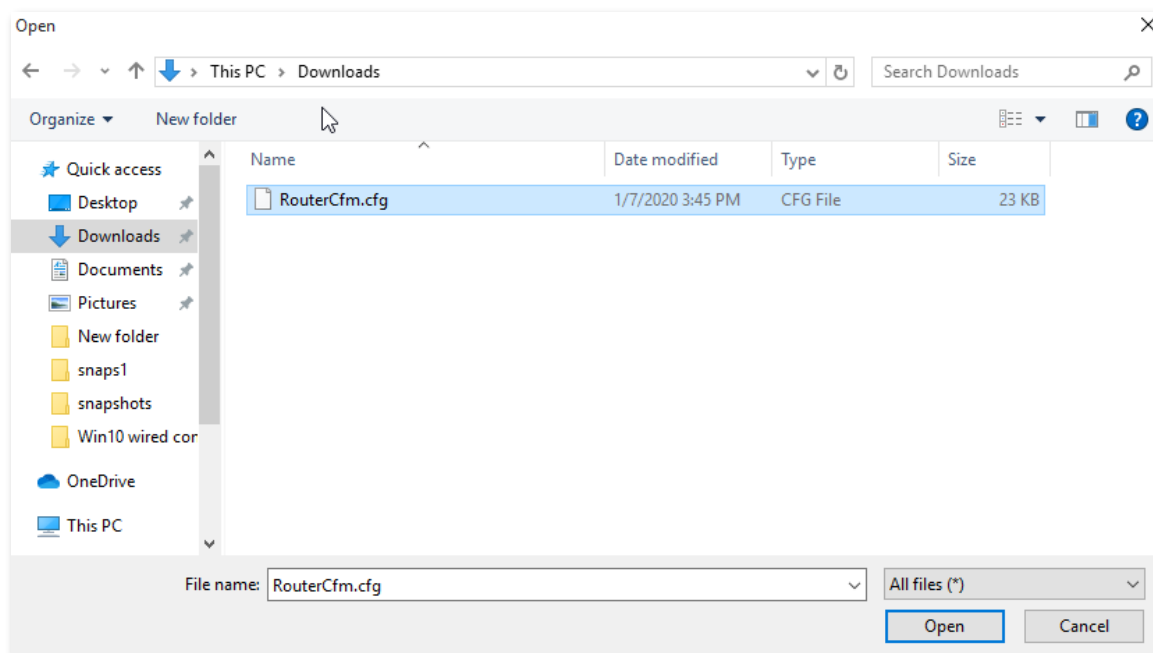


Figure 7-18 Restore previous configurations of the router

Step 5 Click **OK** in the pop-up window.

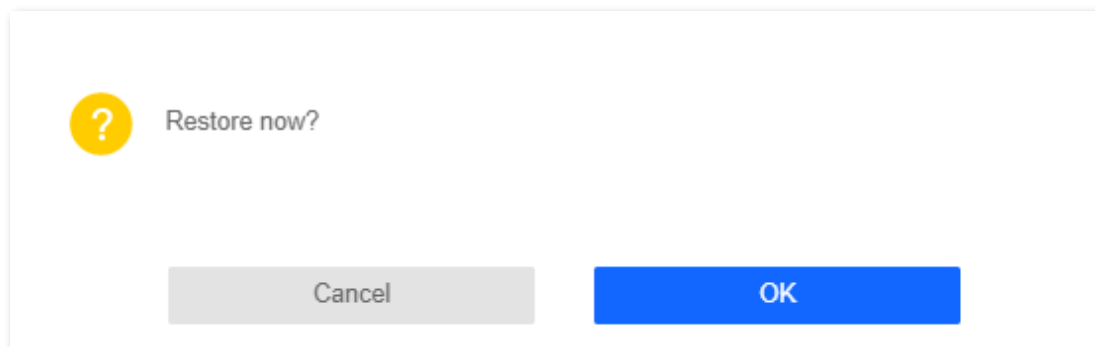


Figure 7-19 Click **OK**

Wait for a moment until the ongoing process finishes, and the router restores previous settings.

7.6.4 Export system log

This function logs all key events that occur after the router is started. If you encounter a network fault, you can turn to system logs for fault rectification.

To access the configuration page, log in to the web UI of the router, and navigate to **Administration > Device Management**. Click **Export** to save the system logs to your local host.

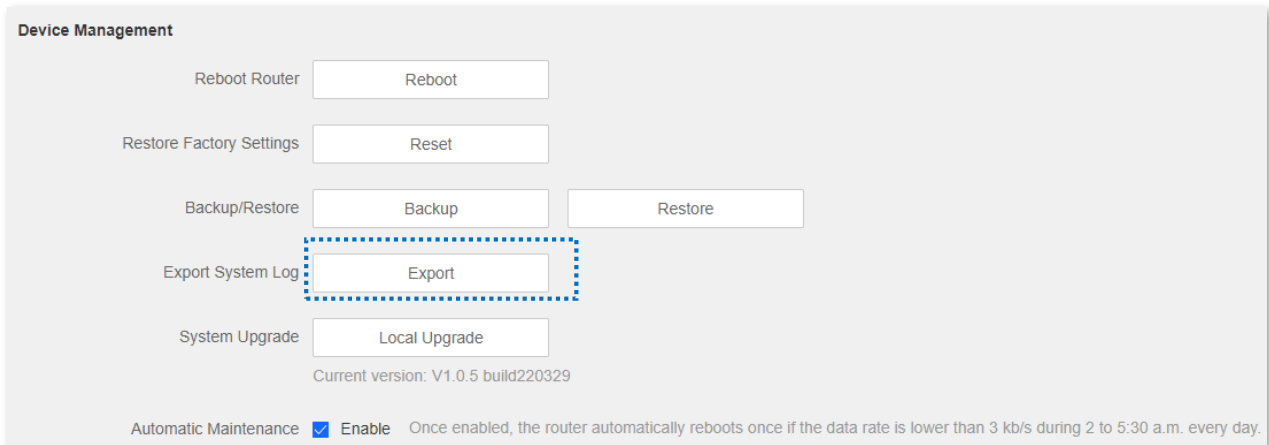


Figure 7-20 Export system log

7.6.5 Upgrade firmware

This function enables the router to obtain the latest functions and more stable performance. The router supports local firmware upgrade.

Local upgrade



To prevent the router from being damaged:

- Ensure that the firmware applies to the router.
 - It is recommended to upgrade the firmware by connecting a LAN port to a computer and performing the upgrade on the web UI.
 - When you are upgrading the firmware, do not power off the router.
-

Procedures:

Step 1 Go to www.hikvision.com/en. Download an applicable firmware of the router to your local computer and unzip it.

Step 2 Launch a web browser on a device connected to the router and visit **http://hikvisionwifi.local** to log in to the web UI of the router.

Step 3 Navigate to **Administration > Device Management**.

Step 4 Click **Local Upgrade**.

Step 5 Click the firmware file downloaded previously (extension: bin), and click **Open**.

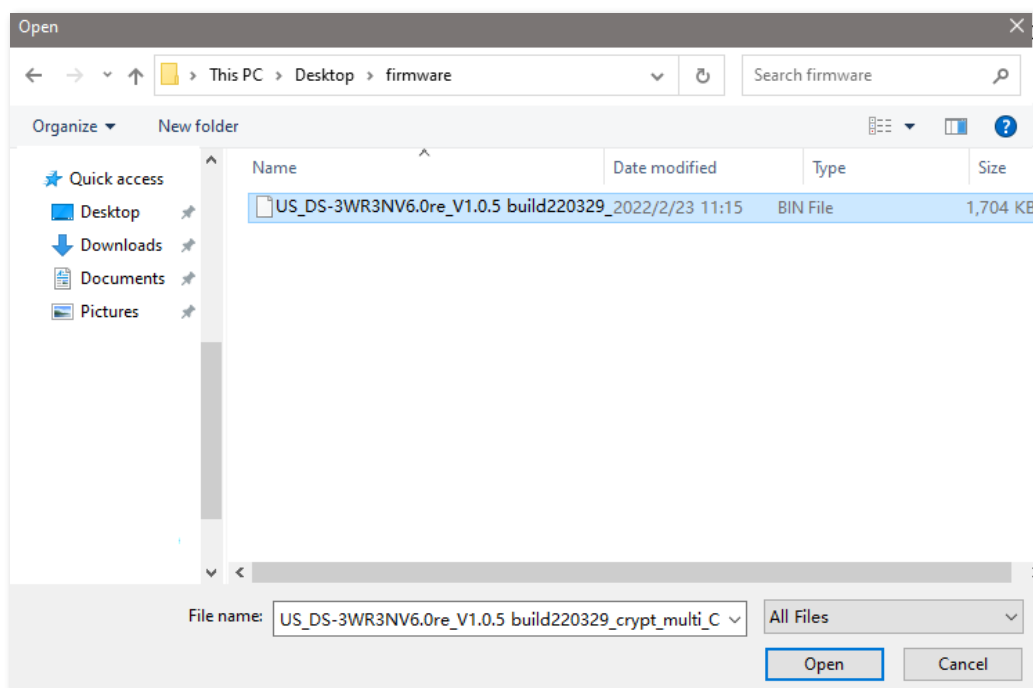


Figure 7-21 Local upgrade

Step 6 Click **OK**.

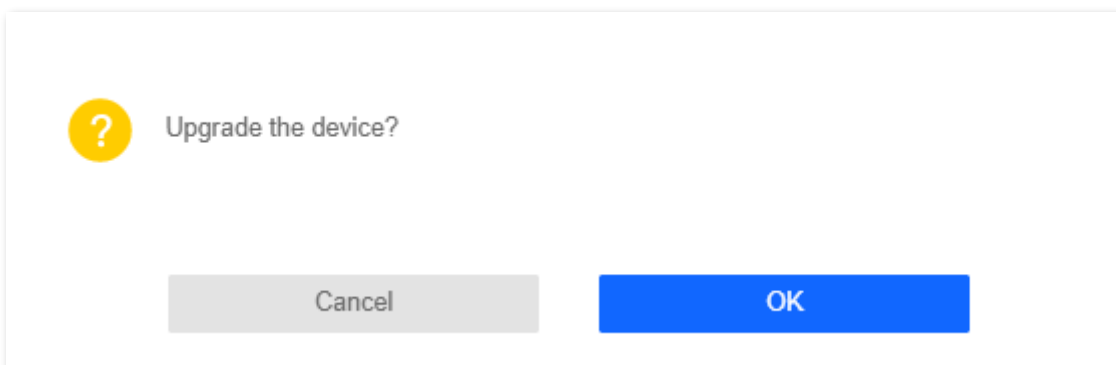


Figure 7-22 Click OK

Wait for a moment until the ongoing process finishes. Log in to the web UI of the router again. Navigate to **Administration > Device Management** and check whether the upgrade is successful based on the **Current Firmware Version**.

 **Note**

For better performance of the new firmware, you are recommended to reset the router to factory default settings and re-configure the router when the upgrading is completed.

7.6.6 Automatic maintenance

Automatic maintenance enables you to make the router restart regularly. It helps improve the stability and service life of the router.

To configure the automatic maintenance function, navigate to **Administration > Device Management**.

When this function is enabled, from 02:00 to 05:30 every day in the morning, if there is any user connected to the router and the traffic over the router's WAN port exceeds 3 KB/s within 30 minutes, the router will delay rebooting. If there is any user connected to the router and the traffic over the WAN port does not exceed 3 KB/s within 30 minutes, or there is no user connected to the router and the traffic over the router's WAN port is slower than 3 KB/s within 3 minutes, the router will reboot automatically.

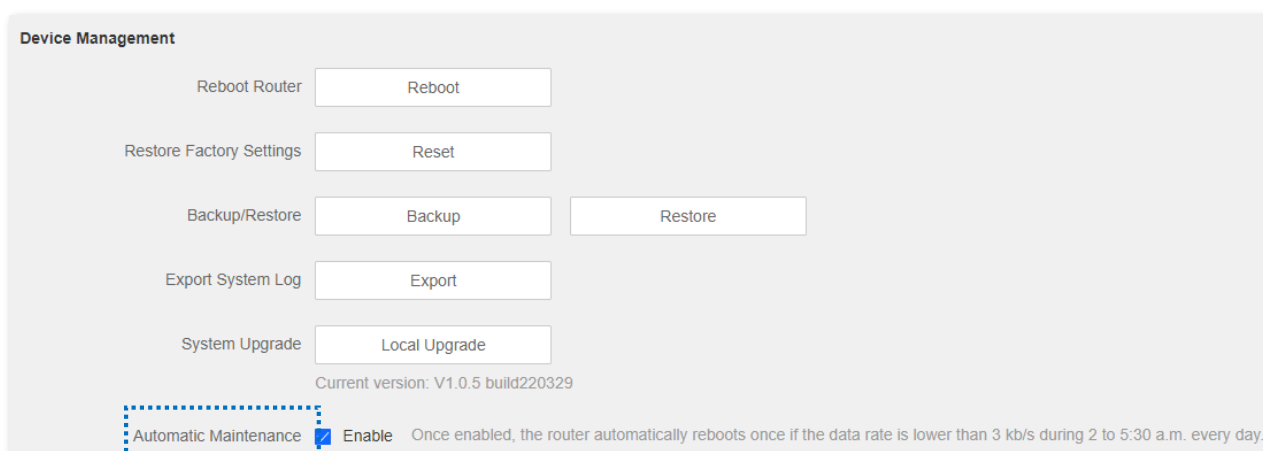


Figure 7-23 Automatic maintenance

Appendix A

A.1 Configuring the computer to obtain an IPv4 address automatically

Perform the Configuring procedures corresponding to [Windows 10](#), [Windows 8](#) and [Windows 7](#) as required. A computer installed with a wired network adapter is used as an example to describe the procedures. The procedures for configuring computers installed with a WiFi network adapter are similar.

A.1.1 Windows 10


Step 1 Click  in the bottom right corner of the desktop and choose **Network settings**.



Figure 7-24 Network settings

Step 2 Click **Change adapter options**.

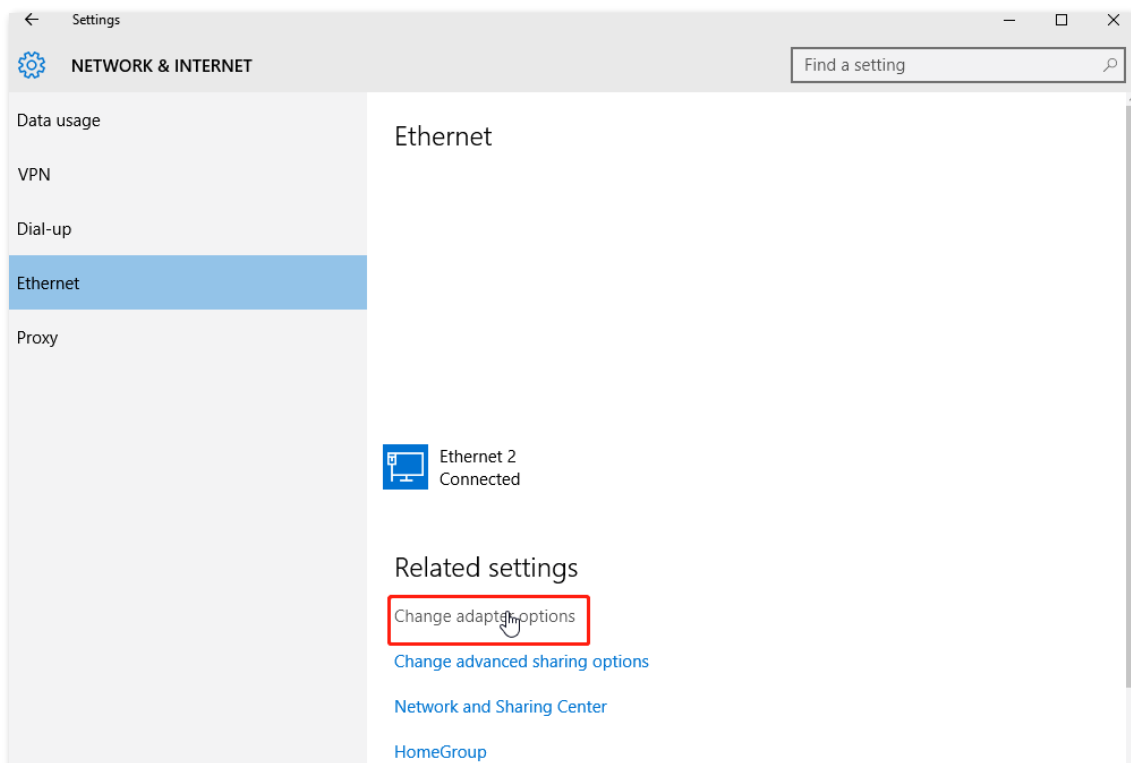


Figure 7-25 Click **Change adapter options**

Step 3 Right-click on the connection which is being connected, and then click **Properties**.

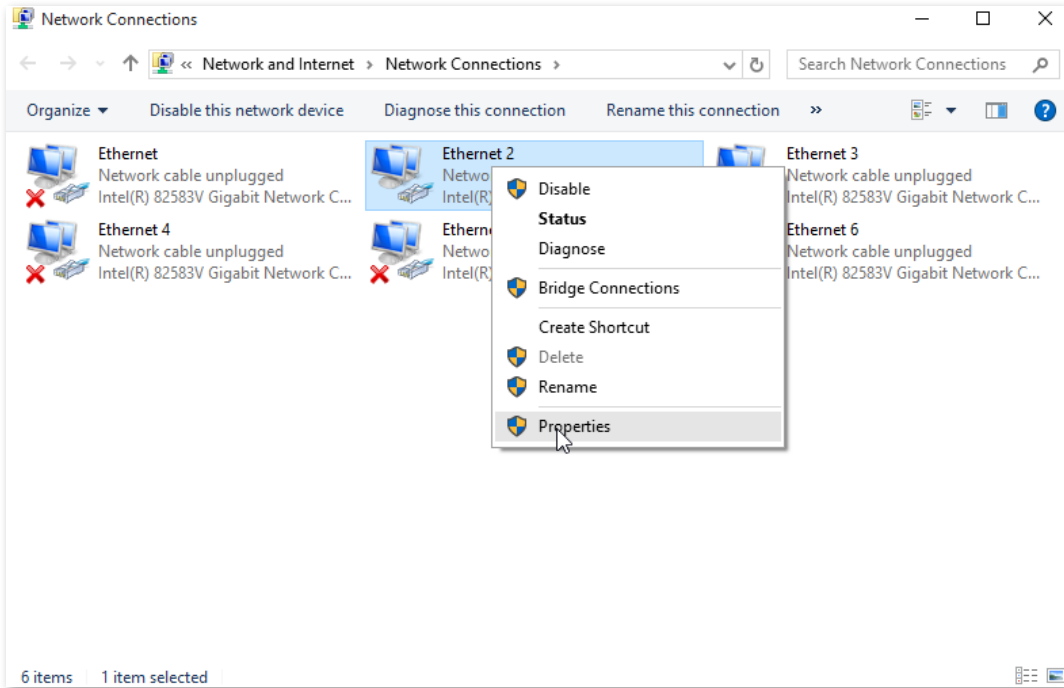


Figure 7-26 Click properties

Step 4 Double-click **Internet Protocol Version 4 (TCP/IPv4)**.

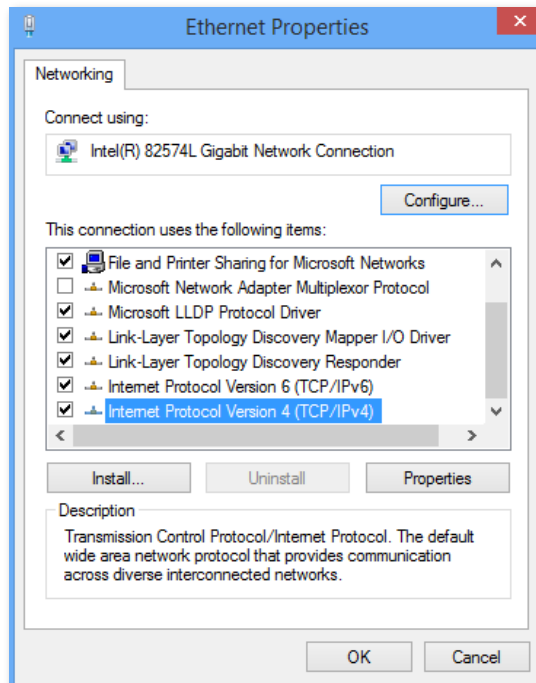


Figure 7-27 Click Internet Protocol Version 4(TCP/IPv4)

Step 5 Select **Obtain an IP address automatically** and **Obtain DNS server address automatically**, and click **OK**.

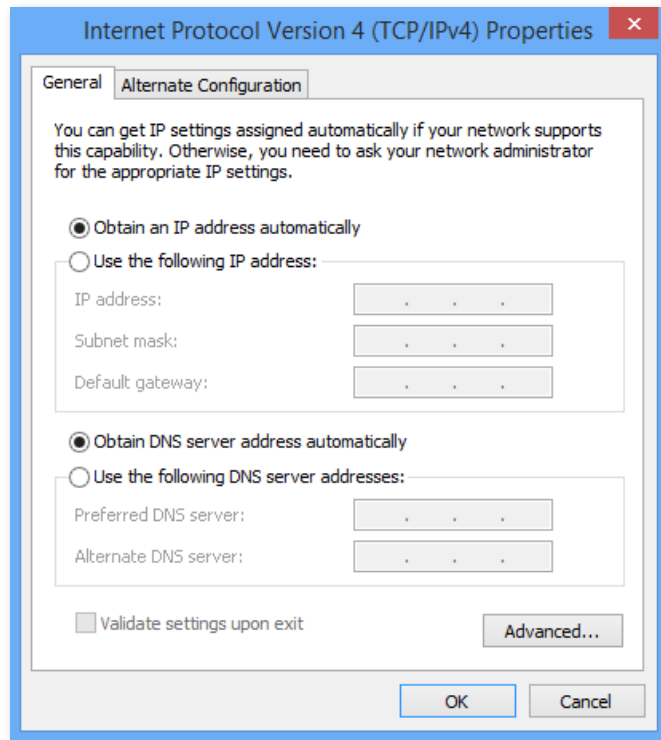



Figure 7-28 Click **OK**

Step 6 Click **Close** in the **Ethernet Properties** window.

A.1.2 Windows 8

Step 1 Right-click  in the bottom right corner of the desktop and choose **Open Network and Sharing Center**.

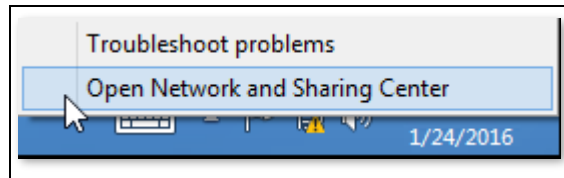


Figure 7-29 Choose **Open Network and Sharing Center**

Step 2 Click **Ethernet** and then **Properties**.

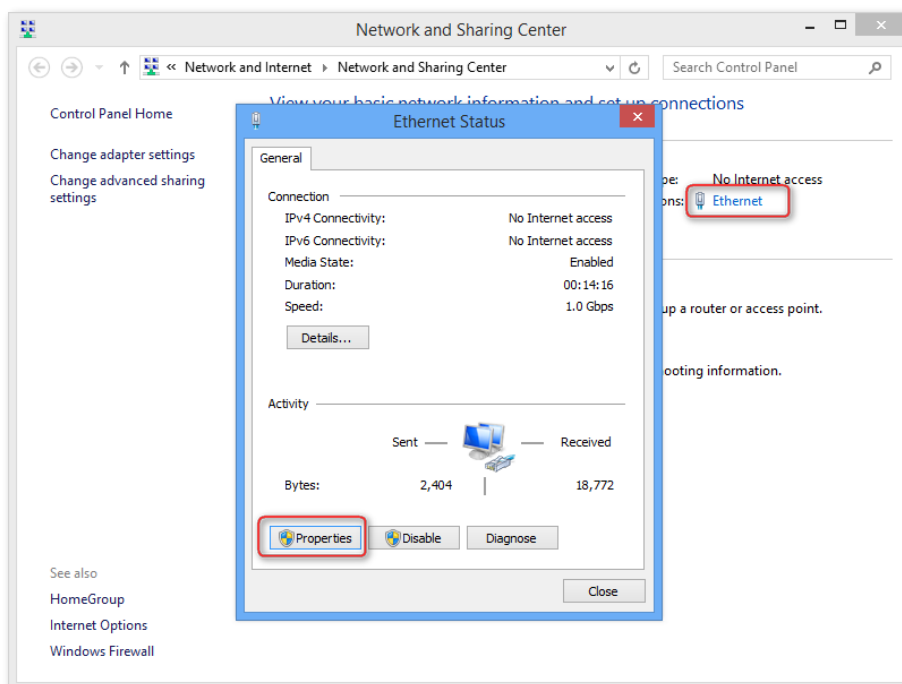


Figure 7-30 Click **Ethernet** and then **Properties**

Step 3 Double-click **Internet Protocol Version 4 (TCP/IPv4)**.

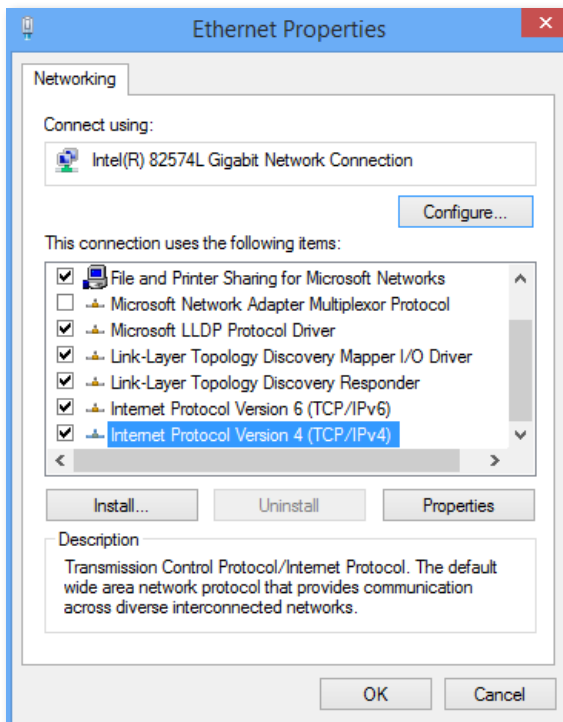


Figure 7-31 Double-click **Internet Protocol Version 4(TCP/IPv4)**

Step 4 Select **Obtain an IP address automatically** and **Obtain DNS server address automatically**, and click **OK**.

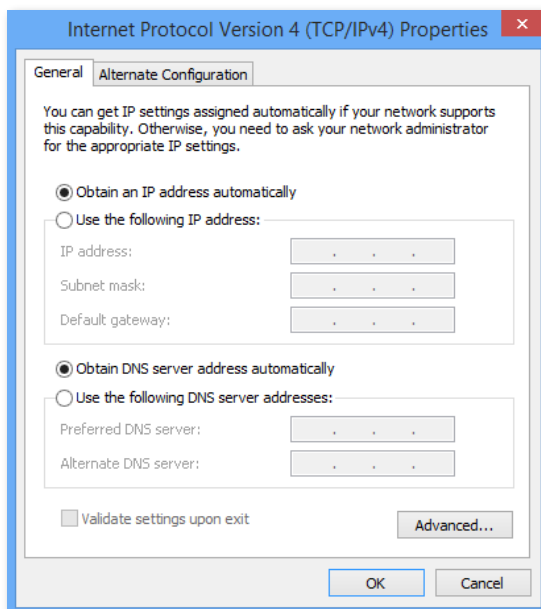



Figure 7-32 Click **OK**

Step 5 Click **OK** in the Ethernet Properties window.

A.1.3 Windows 7

Step 1 Click  in the bottom right corner of the desktop and choose **Open Network and Sharing Center**.

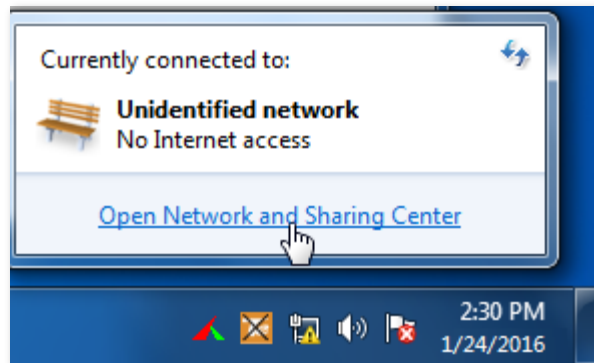


Figure 7-33 Choose **Open Network and Sharing Center**

Step 2 Click **Local Area Connection** and then **Properties**.

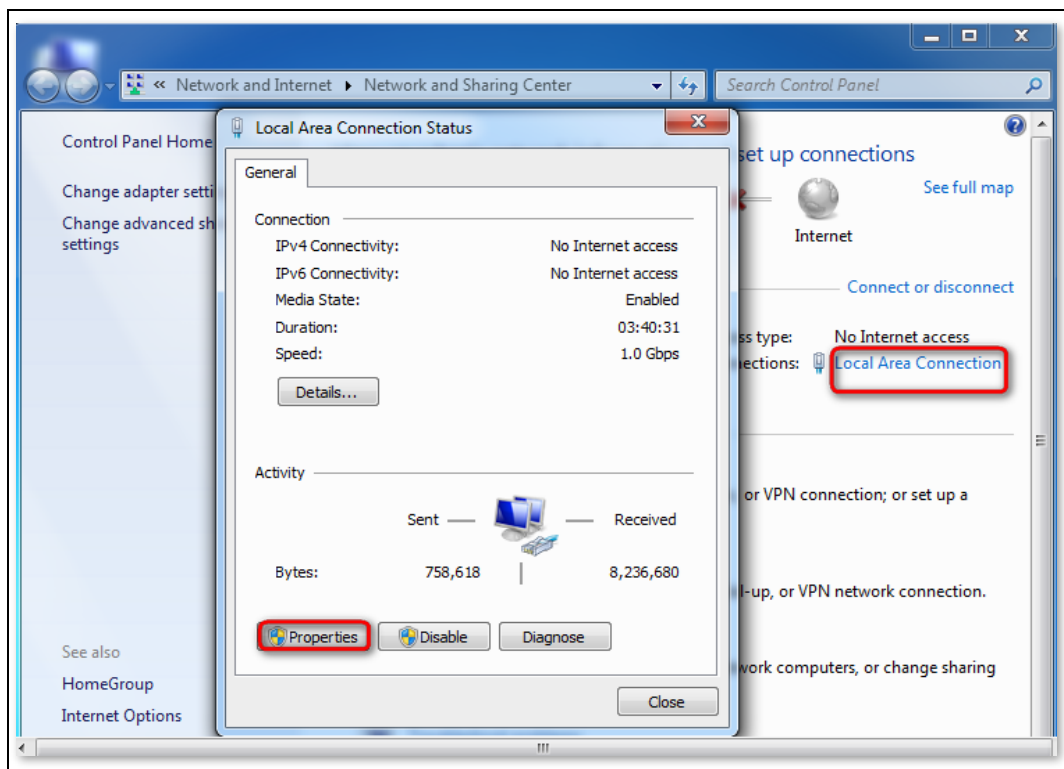


Figure 7-34 Click **Local Area Connection** and then **Properties**

Step 3 Double-click **Internet Protocol Version 4 (TCP/IPv4)**.

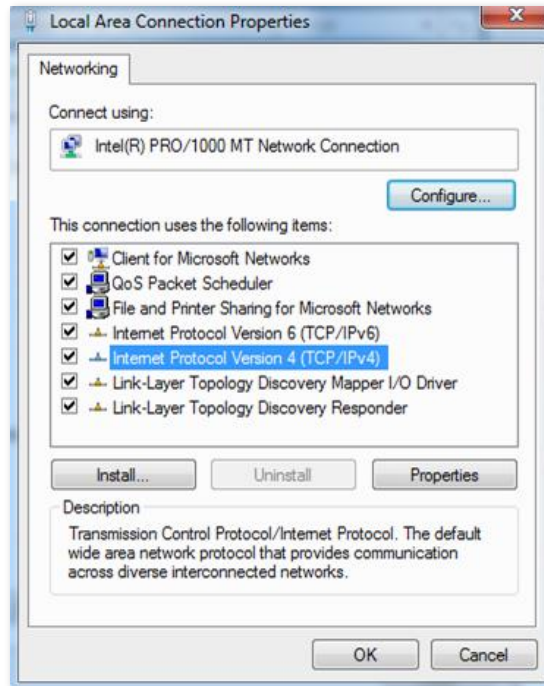


Figure 7-35 Double-click **Internet Protocol Version 4 (TCP/IPv4)**

Step 4 Select **Obtain an IP address automatically** and **Obtain DNS server address automatically**, and click **OK**.

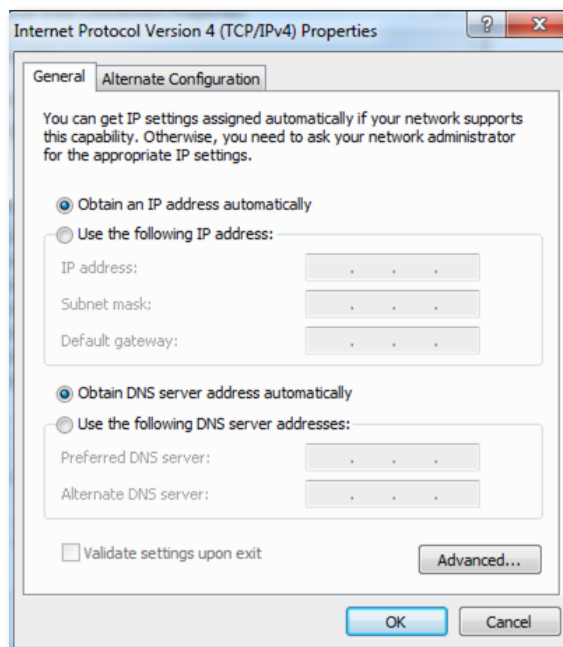


Figure 7-36 Click **OK**

Step 5 Click **OK** in the **Local Area Connection Properties** window.

A.2 Default parameters

Table 7-5 Parameter

Parameter		Default
Login	IP Address	192.168.0.1
	Password	None
LAN Parameter	IP Address	192.168.0.1
	Subnet Mask	255.255.255.0
DHCP Server	DHCP Server	Enabled
	Start IP Address	192.168.0.100
	End IP Address	192.168.0.200
	Preferred DNS Server	192.168.0.1
Operating Mode		Router mode
Wireless Settings	WiFi Name	See the label on the bottom of the router
	WiFi Password	None
	WiFi Schedule	Disabled

A.3 Acronyms and abbreviations

Table 7-6 Acronyms and abbreviations

Abbreviations	Full spelling
AES	Advanced Encryption Standard
AP	Access Point
DDNS	Dynamic Domain Name Server
DHCP	Dynamic Host Configuration Protocol
DHCPv6	Dynamic Host Configuration Protocol for IPv6
DMZ	Demilitarized Zone
DNS	Domain Name System
GMT	Greenwich Mean Time
IP	Internet Protocol
IPv4	Internet Protocol version 4
LAN	Local Area Network
MAC	Medium Access Control
MTU	Maximum Transmission Unit
NAT	Network Address Translation
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
UPnP	Universal Plug and Play
WAN	Wide Area Network
WISP	Wireless Internet Service Provider
WPA-PSK	WPA-Preshared Key



See Far, Go Further