



# **WS325 300Mbps Wireless Router**

## **User Guide**



WS325 300Mbps Wireless Router  
V100R001

## User Guide

Issue                    02  
Part Number        202549

Huawei Technologies Co., Ltd. provides customers with comprehensive technical support and service. For any assistance, please contact our local office or company headquarters.

**Huawei Technologies Co., Ltd.**

Address:        Huawei Industrial Base  
                  Bantian, Longgang  
                  Shenzhen 518129  
                  People's Republic of China

Website:        <http://www.huawei.com>

Email:            [mobile@huawei.com](mailto:mobile@huawei.com)

## **Copyright © Huawei Technologies Co., Ltd. 2013. All rights reserved.**


No part of this manual may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Technologies Co., Ltd. and its affiliates ("Huawei").

The product described in this manual may include copyrighted software of Huawei and possible licensors. Customers shall not in any manner reproduce, distribute, modify, decompile, disassemble, decrypt, extract, reverse engineer, lease, assign, or sublicense the said software, unless such restrictions are prohibited by applicable laws or such actions are approved by respective copyright holders.

## **Trademarks and Permissions**



HUAWEI

**HUAWEI**, and  are trademarks or registered trademarks of Huawei Technologies Co., Ltd.

Other trademarks, product, service and company names mentioned may be the property of their respective owners.

## **Notice**

Some features of the product and its accessories described herein rely on the software installed, capacities and settings of local network, and therefore may not be activated or may be limited by local network operators or network service providers.

Thus, the descriptions herein may not exactly match the product or its accessories which you purchase.

Huawei reserves the right to change or modify any information or specifications contained in this manual without prior notice and without any liability.

## **DISCLAIMER**

ALL CONTENTS OF THIS MANUAL ARE PROVIDED "AS IS". EXCEPT AS REQUIRED BY APPLICABLE LAWS, NO WARRANTIES OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, ARE MADE IN RELATION TO THE ACCURACY, RELIABILITY OR CONTENTS OF THIS MANUAL.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL HUAWEI BE LIABLE FOR ANY SPECIAL, INCIDENTAL, INDIRECT, OR CONSEQUENTIAL DAMAGES, OR LOSS OF PROFITS, BUSINESS, REVENUE, DATA, GOODWILL SAVINGS OR ANTICIPATED SAVINGS REGARDLESS OF WHETHER SUCH LOSSES ARE FORSEEABLE OR NOT.

THE MAXIMUM LIABILITY (THIS LIMITATION SHALL NOT APPLY TO LIABILITY FOR PERSONAL INJURY TO THE EXTENT APPLICABLE LAW PROHIBITS SUCH A LIMITATION) OF HUAWEI ARISING FROM THE USE OF THE PRODUCT DESCRIBED IN THIS MANUAL SHALL BE LIMITED TO THE AMOUNT PAID BY CUSTOMERS FOR THE PURCHASE OF THIS PRODUCT.

## **Import and Export Regulations**

Customers shall comply with all applicable export or import laws and regulations and

be responsible to obtain all necessary governmental permits and licenses in order to export, re-export or import the product mentioned in this manual including the software and technical data therein.

## **Privacy Policy**

To better understand how we protect your personal information, please see the privacy policy at <http://consumer.huawei.com/en/privacy-policy/index.htm>.

---

# Contents

---

<b>1 Product Overview .....</b>	<b>1-1</b>
1.1 Product Features.....	1-1
1.2 Hardware.....	1-2
1.2.1 Interfaces and Buttons.....	1-2
1.2.2 Indicators.....	1-3
<b>2 Hardware Installation .....</b>	<b>2-1</b>
2.1 Selecting a Position for the Router.....	2-1
2.2 Connecting Cables.....	2-1
2.2.1 Knowing Cable Connections.....	2-1
2.2.2 Installing the Router on a Community Broadband Network .....	2-2
2.2.3 Installing the Router on an ADSL Broadband Network.....	2-2
2.2.4 Installing the Router on a CATV Broadband Network .....	2-3
2.3 Powering On the Router.....	2-4
<b>3 Configuration of Internet Access Parameters.....</b>	<b>3-1</b>
3.1 Logging In to the Web-Based Configuration Utility .....	3-1
3.2 Using the Setup Wizard.....	3-4
<b>4 Configuration of WLAN Parameters.....</b>	<b>4-1</b>
4.1 Setting Up a Wireless Connection Manually.....	4-1
4.2 Setting Up a Wireless Connection Through the WPS Button.....	4-3
<b>5 Configuring Frequently Used Functions.....</b>	<b>5-1</b>
5.1 Configuring Multiple PCs to Access the Internet Simultaneously .....	5-1
5.2 Enabling or Disabling the WLAN Function.....	5-2
5.3 Improving the Security of a WLAN .....	5-3
5.3.1 Hiding the Name of a WLAN .....	5-3
5.3.2 Changing the Name of a WLAN.....	5-5
5.3.3 Using Secure Encryption.....	5-6
5.3.4 Allowing Only Specified PCs to Be Connected to a WLAN .....	5-8
5.4 Controlling the Internet Access Rights of PCs.....	5-10
5.5 Prohibiting PCs from Accessing Specified Web Sites .....	5-13
5.6 Setting the Available Bandwidth of a PC.....	5-14

5.7 Preventing Attacks on the Internet .....	5-19
5.8 Removing the Restriction Caused by the Binding of the Internet Access Account to the MAC Address .....	5-20
5.9 Binding the IP address and MAC address .....	5-21
5.10 Allowing Internet Users to Access an Internal Resource Server .....	5-23
5.11 Expanding the Coverage of a WLAN.....	5-25
<b>6 Maintenance Guide .....</b>	<b>6-1</b>
6.1 Changing the Administrator Password of the Web-based Configuration Utility .....	6-1
6.2 Changing the Login IP Address of the Web-based Configuration Utility .....	6-2
6.3 Backing Up or Importing a Configuration File .....	6-3
6.4 Restoring Default Settings.....	6-4
6.5 Upgrading Software .....	6-5
<b>7 FAQs.....</b>	<b>7-1</b>
<b>8 Appendix.....</b>	<b>8-5</b>
8.1 Default Settings .....	8-5
8.2 Technical Specifications.....	8-5
<b>9 For More Help .....</b>	<b>9-6</b>

# 1 Product Overview

---

## 1.1 Product Features

The router is a network access device designed for home users and small or home office (SOHO) users. It supports the wireless local area network (WLAN) function on the user side and provides four Ethernet interfaces through which you can connect various home terminal devices, such as personal computers (PCs) and Internet Protocol (IP) set-top boxes (STBs), to the Internet. It supports the following functions:

- WLAN function
  - High-performance built-in antenna with extra strong penetration
  - Wireless data rate of 300 Mbit/s
  - Compatibility with Institute of Electrical and Electronics Engineers (IEEE) 802.11b, 802.11g, and 802.11n
  - Establishment of a secure wireless connection by pressing the Wi-Fi Protected Setup (WPS) button
  - Easy and secure configuration and management of a WLAN
  - Advanced Encryption Standard (AES), temporary key integrity protocol (TKIP), and 64/128-bit wired equivalent privacy (WEP) encryption
  - Security modes of Wi-Fi Protected Access (WPA and WPA2) and hybrid cryptosystem
  - Wireless Distribution System (WDS) through which a WLAN can be expanded
  - Low radiation
  - Certification by the Wi-Fi Alliance
- Integration of the functions of wireless access points (APs), routers, four-port switches, and firewalls
- One 10/100 Mbit/s adaptive uplink Ethernet interface connected to a wide area network (WAN) and four 10/100 Mbit/s adaptive downlink Ethernet interfaces connected to a local area network (LAN)
- Multiple networking applications, such as accessing a broadband network in Point-to-Point Protocol over Ethernet (PPPoE) dial-up mode, obtaining an IP address through the Dynamic Host Configuration Protocol (DHCP), and configuring a static IP address
- A flexible network configuration and quality of service (QoS) strategy is available. It supports bandwidth control and allocates bandwidth to different computers in your home based on IP addresses, MAC addresses, physical ports and applications in the

LAN. This lets your family access the Internet, play games, and watch videos without interfering with each other

- The router can bundle an IP address and MAC address bi-directionally, effectively protecting a LAN from Address Resolution Protocol (ARP) attacks
- Built-in firewall and Parents Control Feature
- Local and remote configuration through a Web-based configuration utility

## 1.2 Hardware

### 1.2.1 Interfaces and Buttons

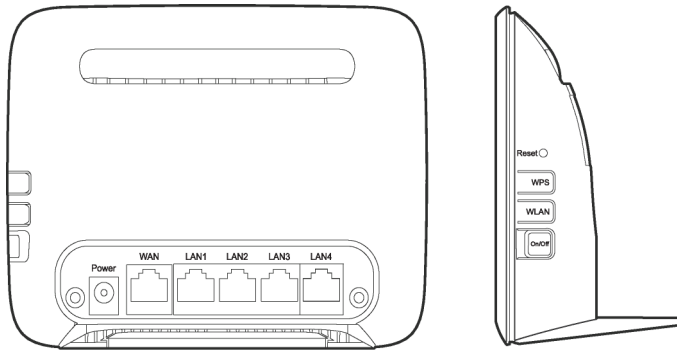


Table 1-1 describes the interfaces and buttons of the router.

**Table 1-1** Interfaces and buttons of the router

Interface or Button	Description
Reset	To restore the router to its default settings, power the router on, press and hold the <b>Reset</b> button for 6 or more seconds, and then release it.  <b>NOTE</b> When the default settings are restored, your custom data is lost. Therefore, exercise caution when using the <b>Reset</b> button.
WPS	Used to enable the WPS function.
WLAN	Used to enable or disable the wireless network function.
On/Off	Used to power the router on or off.
Power	Used to connect to the power adapter.
WAN	Used to connect to Ethernet devices that provide Internet access interfaces, such as network jacks on walls, modems, and switches.

Interface or Button	Description
LAN1 ~ LAN4	Used to connect Ethernet devices, such as computers and switches, to the router.

 **NOTE**

WPS is a standard for easy and secure establishment of a WLAN. Through the WPS function, you can access a WLAN on your wireless terminal devices securely without entering the name and password of the WLAN.

### 1.2.2 Indicators

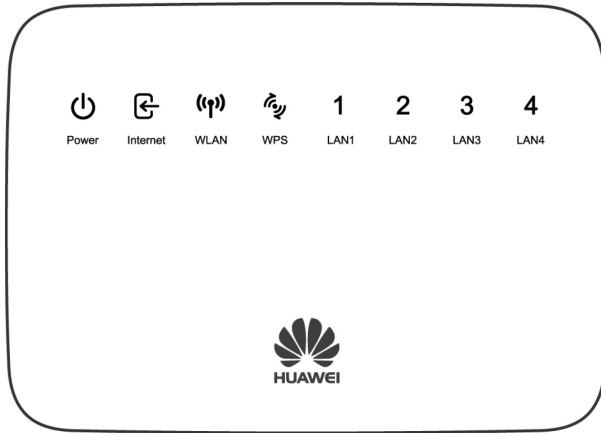


Table 1-2 describes the indicators of the router.

**Table 1-2** Indicators of the router

Indicator	Color	Status	Indicates
Power	Green	On	The router is powered on.
	-	Off	The router is powered off.

Indicator	Color	Status	Indicates
Internet	Green	On	<ul style="list-style-type: none"> <li>The router is working in routing mode.</li> <li>The WAN connection is set up and an IP address has been obtained.</li> <li>No data is being transmitted.</li> </ul>
	Green	Blinking	<ul style="list-style-type: none"> <li>The router is working in routing mode.</li> <li>The WAN connection is set up.</li> <li>Data is being transmitted.</li> </ul>
	Red	On	<ul style="list-style-type: none"> <li>The router is working in routing mode.</li> <li>The WAN connection is set up and no IP address is obtained.</li> <li>The router is working in routing mode, but no data is being transmitted.</li> </ul>
	Red	Blinking	<ul style="list-style-type: none"> <li>The router is working in bridge mode.</li> <li>The WAN connection is set up.</li> <li>Data is being transmitted.</li> </ul>
	-	Off	The router is powered off or no WAN connection is set up.
WLAN	Green	On	The WLAN function is enabled, but no data is being transmitted on the WLAN.
	Green	Blinking	The WLAN function is enabled and data is being transmitted on the WLAN.
	-	Off	The WLAN function is disabled.
WPS	Green	On	A wireless connection is set up between the router and a wireless client through the WPS function. This state lasts 300 seconds.
	Green	Blinking	The router is attempting to set up a wireless connection with a wireless client (such as a computer with a wireless network adapter installed) through the WPS function. This state lasts no more than 2 minutes.
	-	Off	The WPS function is disabled.

Indicator	Color	Status	Indicates
LAN1~LAN4	Green	On	A connection is set up between the corresponding LAN interface of the router and an Ethernet device (such as a computer) through a network cable, but no data is being transmitted.
	Green	Blinking	A connection is set up between the corresponding LAN interface of the router and an Ethernet device (such as a computer) through a network cable and data is being transmitted.
	-	Off	No connection is set up between the corresponding LAN interface of the router and an Ethernet device (such as a computer).

# 2 Hardware Installation

## 2.1 Selecting a Position for the Router

Place the router in a stable and well-ventilated place and do not expose it to direct sunlight. If you want to use the WLAN function of the router, you also need to pay attention to the following precautions for a better performance of the WLAN:

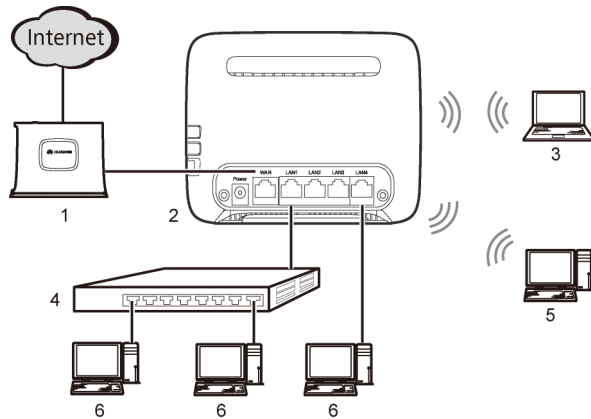
- Place the router in an open space and ensure that no obstacle, such as a cement or wooden wall, exists between your PC and the router. Otherwise, the transmission of radio signals on the WLAN is affected.
- Ensure that the router and your PC are far from the electric appliances (such as a microwave oven) that generate strong magnetic or electric fields.

## 2.2 Connecting Cables

### 2.2.1 Knowing Cable Connections

Figure 2-1 shows the cable connections between the router and other devices.

**Figure 2-1** Cable connections between the router and other devices



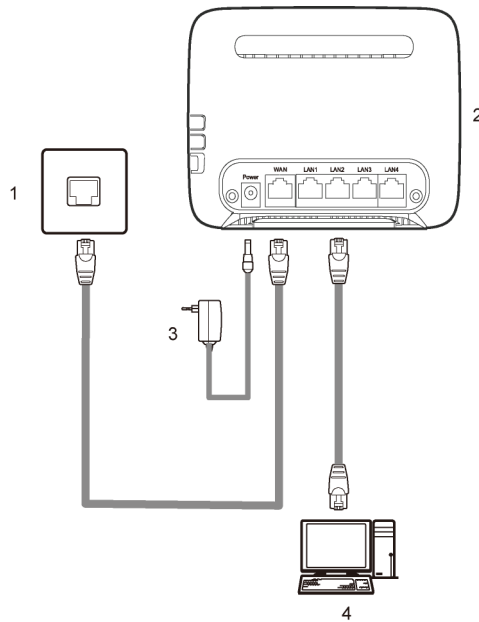
- |   |           |
|---|-----------|
| 1. ADSL modem   | 2. Router |
| 3. Laptop installed with a wireless network adapter           | 4. Switch |
| 5. Desktop computer installed with a wireless network adapter | 6. PC     |

As the interface that connects your home or SOHO network to the Internet, the WAN interface of the router is used to connect the router to a network access device, such as an ADSL modem. The PCs and switches on your home or SOHO network are connected through the WLAN that is set up through the router and the LAN interfaces of the router. For the cable connections of the router on other types of networks, see the descriptions in the other sections of this chapter.

## 2.2.2 Installing the Router on a Community Broadband Network

In some communities, network service providers use Ethernet interfaces as Internet interfaces. Figure 2-2 shows the cable connections of a community broadband network after the router is installed on the network.

**Figure 2-2** Cable connections of a community broadband network after the router is installed on the network



- |  |           |
|--|-----------|
| 1. Community broadband network interface on the wall<br>(Ethernet interface) | 2. Router |
| 3. Power adapter of the router   | 4. PC     |

## 2.2.3 Installing the Router on an ADSL Broadband Network

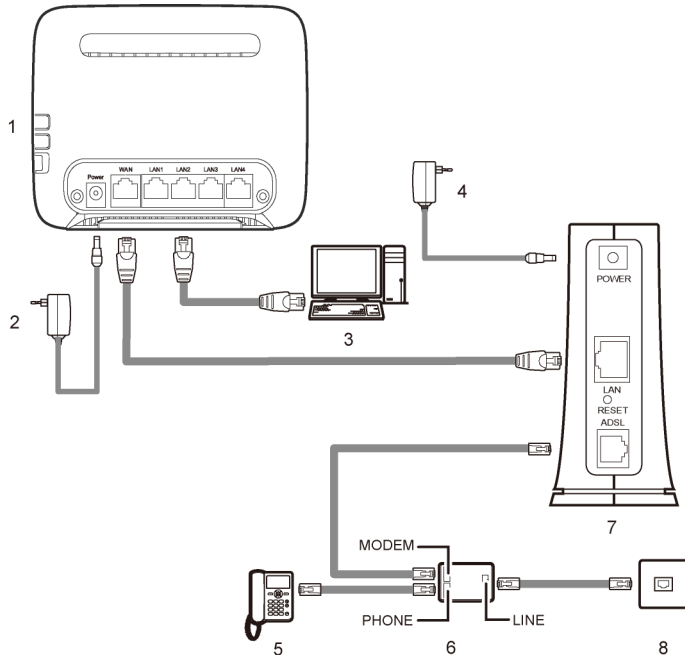
On an ADSL broadband network, the ADSL modem provides an Ethernet interface used to connect a PC to the Internet.

**NOTE**

ADSL is a technology that uses telephone lines to provide broadband access services. To access an ADSL network through your PC, you need to use an ADSL modem.

Figure 2-3 shows the cable connections of an ADSL broadband network after the router is installed on the network.

**Figure 2-3** Cable connections of an ADSL broadband network after the router is installed on the network



- 1. Router
- 2. Power adapter of the router
- 3. PC
- 4. Power adapter of the ADSL modem
- 5. Telephone
- 6. Splitter
- 7. ADSL modem
- 8. Telephone line interface on the wall

**NOTE**

Figure 2-3 takes the Huawei SmartAX MT880d ADSL customer-premises equipment (CPE) as an example of the ADSL modem on the ADSL broadband network. Other models of ADSL modems might vary in appearance. Their interface types and cable connections, however, are similar to those of the modem as shown in Figure 2-3.

## 2.2.4 Installing the Router on a CATV Broadband Network

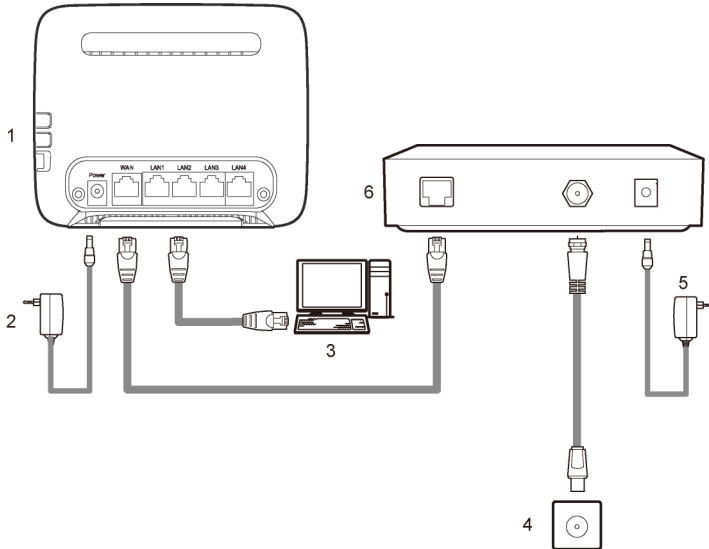
On a CATV Broadband Network, the cable modem provides an Ethernet interface used to connect a PC to the Internet.

 **NOTE**

A CATV broadband network is a network that uses the coaxial cables of CATV to provide broadband access services. To access such a network through your PC, you need to use a cable modem. Typically, CATV companies provide broadband access services through CATV broadband networks.

Figure 2-4 shows the cable connections of a CATV broadband network after the router is installed on the network.

**Figure 2-4** Cable connections of a CATV broadband network after the router is installed on the network



- |                                     |                                       |
|-------------------------------------|---------------------------------------|
| 1. Router                           | 2. Power adapter of the router        |
| 3. PC                               | 4. CATV network interface on the wall |
| 5. Power adapter of the cable modem | 6. Cable modem                        |

 **NOTE**

Cable modems provided by different manufacturers might vary in appearance and interface layout. The cable modem in Figure 2-4 is for your reference only.

## 2.3 Powering On the Router

Press the **On/Off** button on the side panel to power the router on. If the router works properly, the indicators on the front panel turn on. Table 2-1 describes the indicators that turn on after the router is powered on. You can check whether the router works properly according to the descriptions in Table 2-1. For details about the indicators of the router, see Table 1-2.

**Table 2-1** Indicators that turn on after the router is powered on

Indicator	Color	Status	Indicates
Power	Green	On	The router is powered on.
Internet	Green	On	A physical connection is set up between the WAN interface of the router and the Ethernet interface of an Ethernet device (such as an ADSL modem) through a network cable and you can access the Internet through the router.
	Red	On	A physical connection is set up between the WAN interface of the router and the Ethernet interface of an Ethernet device (such as an ADSL modem) through a network cable, but you cannot access the Internet through the router.  <b>NOTE</b> In this case, you need to configure the router as described in chapter 3 "Configuration of Internet Access Parameters."
WLAN	Green	On	The WLAN function is enabled.
LAN1~LAN4	Green	On	A connection is set up between the corresponding LAN interface of the router and an Ethernet device (such as a PC) through a network cable.

# 3 Configuration of Internet Access Parameters


## 3.1 Logging In to the Web-Based Configuration Utility

Most of the router parameters are pre-set before delivery to meet common home application scenarios. To check the router's working status or configure certain advanced network functions, use the web-based configuration utility.

To log in to the Web-based configuration utility, do as follows:

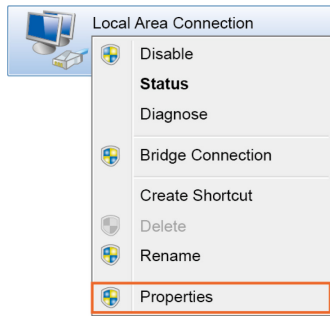
- Step 1** Set up network access for your computer. Set the network connection of your computer to obtain an IP address automatically.

### Procedure on Computers Running Windows 7

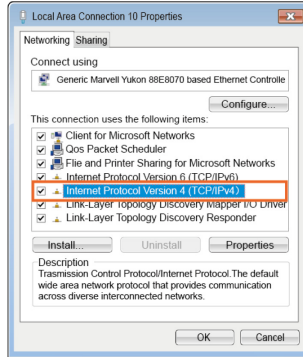
1. Click  in the lower right corner of your desktop, and choose **Open Network and Sharing Center**.



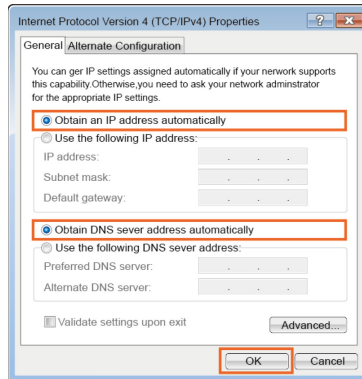
2. Choose **Change adapter settings**. Right-click **Local Area Connection** and choose **Properties**.




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



4. Select **Obtain an IP address automatically** and **Obtain DNS server address automatically**. Click **OK**.

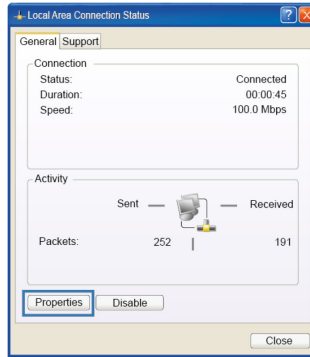


**Procedure on Computers Running Windows XP**

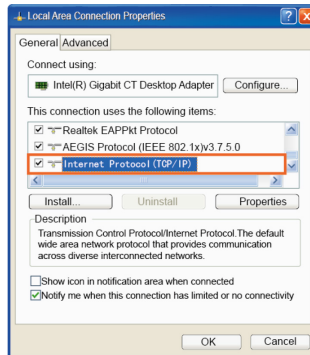
1. Click  in the lower right corner of your desktop.



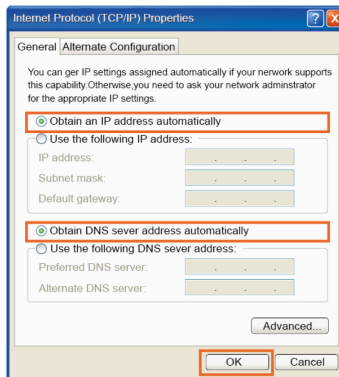
2. In the displayed dialog box, click **Properties**.



3. Double-click **Internet Protocol (TCP/IP)**.



4. Select **Obtain an IP address automatically** and **Obtain DNS server address automatically**. Click **OK**.



**Step 2** Launch a browser, enter **http://192.168.3.1**, and press **Enter**. In the **Login** window, enter **admin** for both the **user name** and **password**, and click **Login**.



----End

#### NOTE

- To protect your router from unauthorized access, change the user name and password after the first login. For details, see chapter 6.1 “Changing the Administrator Password of the Web-based Configuration Utility”.
- The first time you log in to the web-based configuration utility, a setup wizard is displayed. To skip the wizard and go immediately to the configuration page, click **Here** when the following message displays: **Click Here to enter the advanced configuration page**.

## 3.2 Using the Setup Wizard

After logging in to the web-based configuration utility, you can use the setup wizard provided by the utility to quickly configure the router.

When you configure the router for the first time, you can view the setup wizard page after logging in to the utility. To configure the router through the setup wizard:

**Step 1** Log in to the Web-based configuration utility.

**Step 1** Choose the network connection type and configure the network connection parameters. Choose the connection type based on the application scenario. The Table 3-1 describes the connection types.

**Table 3-1** Configuring the Internet access parameters

Application Scenario	Connection Type
The user name and password are provided by your service provider.	PPPoE (recommended)
The user name and password are provided by your service provider. Set up a dial-up connection on one computer only.	Bridge
Certain parameters, such as the static IP address and DNS server address, are provided by your service provider.	Static IP
No parameters are provided by your service provider. The IP address is automatically assigned by the service provider.	DHCP

If you choose **PPPoE** or **Static IP**, enter the parameters provided by your service provider, and click **Next**.

The screenshot shows the 'Quick Configure Internet' page with a blue header. Below the header, it says 'Please enter the Username and Password provided by Network operators.' There is a 'Connection type:' dropdown menu set to 'PPPoE'. Below it are two text input fields for 'Username:' and 'Password:'. A 'Next' button is located below the password field. At the bottom, there is a link: 'Click [Here](#) to enter the advanced configuration page.'

The screenshot shows the 'Quick Configure Internet' page with a blue header. Below the header, it says 'Please enter the Username and Password provided by Network operators.' There is a 'Connection type:' dropdown menu set to 'Static IP'. Below it are five text input fields for 'IP address:', 'Subnet mask:', 'Default gateway:', 'Primary DNS:', and 'Secondary DNS:'. A 'Next' button is located below the DNS fields. At the bottom, there is a link: 'Click [Here](#) to enter the advanced configuration page.'

If you choose **DHCP** or **Bridge**, click **Next** without changing any configurations.

Quick Configure Internet

Connection type: Bridge

Next

Click [Here](#) to enter the advanced configuration page.

Quick Configure Internet

Connection type: DHCP

Next

Click [Here](#) to enter the advanced configuration page.



**NOTE**

- If you choose **PPPoE**, **Static IP**, or **DHCP**, the computer automatically connects to the Internet as long as the router is working properly.
- If you choose **Bridge**, use the dial-up software on the computer to set up a dial-up connection each time you access the Internet.

**Step 2** Enter the service set identifier (SSID) and key, and click **Next**.

Quick Configure Wireless Network

Please enter SSID and Key, or enter advanced for more settings.

SSID: huawei

Key: ●●●●●●

Back Next

Click [Here](#) to enter the advanced configuration page.

---End



**NOTE**

The default SSID and key are printed on the router's rear label. To protect your wireless network from unauthorized access, change the SSID and key promptly. For details, see chapter 5.3.2 “Changing the Name of a WLAN” and 5.3.3 “Using Secure Encryption”.

# 4 Configuration of WLAN Parameters


## 4.1 Setting Up a Wireless Connection Manually

If a wireless network adapter is installed on your computer, you can connect your computer to the router over a wireless connection. To manually set up a wireless connection, use either of the following methods:

- Use the tool provided by your network adapter.  
For details, see the user guide of your network adapter.
- Use the wireless configuration software provided by the operating system of your PC.

This section takes Windows XP and Windows 7 as an example and describes how to set up a wireless connection between your PC and the router manually.

### Procedure on Computers Running Windows 7

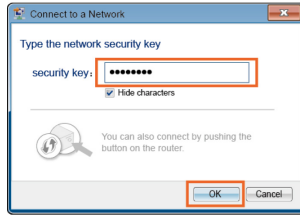
**Step 1** Click  in the lower right corner of your desktop.



**Step 2** From the wireless network list, select the WLAN provided by the router. Click **Connect**.



**Step 3** In the displayed dialog box, enter the WLAN password and click **OK**.




**Step 4** In the wireless network list, check the WLAN connection status. If the status is **Connected**, the computer is wirelessly connected to the router.



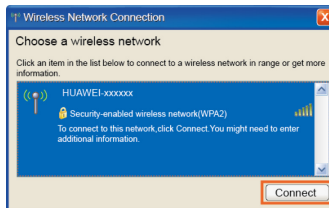
----End

### Procedure on Computers Running Windows XP

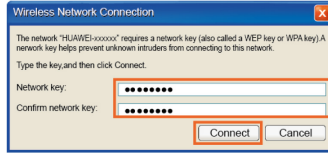
**Step 1** Click  in the lower right corner of your desktop.



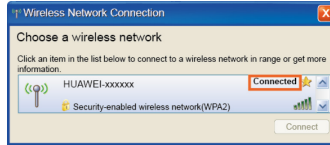
**Step 2** From the wireless network list, select the WLAN provided by the router. Click **Connect**.



**Step 3** In the displayed dialog box, enter the WLAN password and click **Connect**.



**Step 4** In the wireless network list, check the WLAN connection status. If the status is **Connected**, the computer is wirelessly connected to the router.



---End

## 4.2 Setting Up a Wireless Connection Through the WPS Button

The router supports the WPS function. If your network adapter also supports the WPS function, you can use the WPS function to set up a wireless connection between your computer and the router quickly. To set up such a wireless connection:

**Step 1** Check whether the WLAN indicator light of the router is on. If the WLAN indicator light is off, press the **WLAN** button on the side panel of the router to enable the WLAN function.

**Step 2** Press and hold the **WPS** button for 2 or more seconds on the side panel of the router.

The WPS indicator light of the router starts blinking. If the WPS indicator light does not start blinking, the WPS function cannot be enabled. For solutions to other WPS issues, see chapter 7 "FAQs."

**Step 3** Enable the WPS negotiation function of the wireless network adapter on your PC within two minutes, and then wait for a moment (typically 10s and at most 120s).

The WPS indicator of the router becomes on from the blinking state, indicating that the router is connected to your PC through the WLAN. This state lasts 300s. Then the WPS indicator turns off.

---End

### **NOTE**

After finishing the configuration, if the other PCs need to set a wireless connection through the WPS button, please repeat Step 2 to Step 3.

# 5 Configuring Frequently Used Functions

---

## 5.1 Configuring Multiple PCs to Access the Internet Simultaneously

### Function Overview

The router provides four Ethernet interfaces and the WLAN function. Thus, you can connect multiple PCs to the router wirelessly or through the Ethernet interfaces. Then the PCs can access the Internet simultaneously through the routing function of the router.

### Configuration Example

For example, you have a desktop computer that is used for accessing the Internet, a new desktop computer, and a new laptop with a wireless network adapter installed. You can configure the desktop computers and the laptop to access the Internet simultaneously. In this example, the laptop is configured to access the Internet wirelessly.

Most configurations of the router are completed before delivery. You only need to connect the desktop computers and the laptop to the router and set certain Internet access parameters of the router as follows:

- Step 1** Connect the two desktop computers to the router by using network cables.  
For details, see chapter 2 "Hardware Installation."
- Step 2** Connect the laptop to the router wirelessly by configuring the laptop.  
For details, see chapter 4 "Configuration of WLAN Parameters."
- Step 3** Set the Internet access parameters of the router to connect the router to the Internet.  
For details, see chapter 3 "Configuration of Internet Access Parameters."
- Step 4** Configure network connections on the desktop computers and the laptop so that these PCs can obtain IP addresses automatically.

---End

### NOTE

If the desktop computers and the laptop cannot access the Internet after the preceding configuration, the network service provider might have bound your Internet access account to the Media Access Control (MAC) address of the network adapter of your old desktop computer. To remove the restriction, see section 5.8 "Removing the Restriction Caused by the Binding of the Internet Access Account to the MAC Address."

## 5.2 Enabling or Disabling the WLAN Function

### Function Overview

The router supports enabling or disabling the WLAN function. Thus, you can enable or disable the WLAN function as required.

### Configuration Example

To enable or disable the WLAN function, do as follows:

- Step 1** Log in to the Web-based configuration utility.
- Step 2** In the navigation tree, choose **Basic** > **WLAN**.
- The WLAN configuration page is displayed.

- Step 3** Select **Enable WLAN**.
- Select **Enable WLAN** to enable the **WLAN** function, and then click **Submit**.

The screenshot shows the WLAN configuration interface. At the top, there are three tabs: 'WLAN', 'WLAN WDS', and 'WLAN Filtering'. The 'WLAN' tab is selected and highlighted with a red box. Below the tabs, there is a checkbox labeled 'Enable WLAN' which is checked and also highlighted with a red box. Underneath, there is a section titled 'Wireless Settings' with various configuration options: Mode (802.11 b/g/n), Country (CHINA), Channel (Auto), Transmit power (100%), Power Enhance (disabled), SSID index (SSID1), SSID (huawei), Hide broadcast (checked), AP isolation (disabled), Band width (20/40 MHz), Security (WPA2-PSK), WPA pre-shared key (masked with dots), and WPA encryption (AES). A 'Submit' button is located at the bottom right of the settings area and is highlighted with a red box.

- Clear **Enable WLAN** to disable the **WLAN** function.

This screenshot shows the same WLAN configuration page as above, but the 'Enable WLAN' checkbox is now unchecked and highlighted with a red box. The 'Submit' button is no longer visible in this view.

---End

## 5.3 Improving the Security of a WLAN

The signals of a WLAN are transmitted in the air. Therefore, unauthorized persons can receive the wireless signals easily. If the wireless signals are not encrypted, unauthorized persons may use your WLAN or obtain the data transmitted on the WLAN. To ensure the security of the data transmitted on the WLAN, the router provides multiple security-related settings for the WLAN function. You can change these settings as required to protect your WLAN from unauthorized access.

### 5.3.1 Hiding the Name of a WLAN

#### Function Overview

When accessing a WLAN, the user of a wireless client needs to enter the correct name of the WLAN, that is, the service set identifier (SSID) of the WLAN. Generally, the wireless signals transmitted from a wireless router carries the SSID. The wireless adapter of a PC can find and display the SSID for selection and confirmation. Thus, manual operations for selecting and configuring the WLAN can be simplified. The SSID, however, is not encrypted. Therefore, anyone can find the WLAN, and then view the SSID, and the security of the WLAN is reduced.

The router provides the function of hiding the SSID. After this function is enabled, the wireless signals transmitted from the router do not carry the SSID. Thus, it is not possible for unauthorized people to obtain the SSID from the wireless signals. In addition, the user of a PC needs to enter the correct SSID manually to add the PC to the WLAN. Thus, the security of the WLAN is increased.

The router also provides the multi-SSID function. You can configure multiple SSIDs, and then enable one or multiple of them.



#### NOTE

Through the multi-SSID function, multiple virtual access points of a WLAN can be established. For a wireless client, each virtual access point can be used as a physical access point. In addition, each virtual access point has its SSID.

#### Configuration Example

To use and hide **SSID1** and disable the other SSIDs (so that the WLAN cannot be found by others), do as follows:

- Step 1** Log in to the Web-based configuration utility.
- Step 2** In the navigation tree, choose **Basic > WLAN**.  
The WLAN configuration page is displayed.
- Step 3** Select **SSID1** for **SSID Index**.

**Step 4** Set **Hide broadcast** to **Enable**, and then click **Submit**.

The screenshot shows the WLAN configuration interface. The 'WLAN' tab is active. The 'Enable WLAN' checkbox is checked. Under the 'Wireless Settings' section, the following fields are visible: Mode (802.11b/g/n), Country (CHINA), Channel (Auto), Transmit power (100%), Power Enhance (unchecked), SSID index (SSID1), SSID (huawei), Hide broadcast (checked/Enable), AP isolation (unchecked), Band width (20/40 MHz), Security (WPA2-PSK), WPA pre-shared key (masked), and WPA encryption (AES). The 'Submit' button is located at the bottom right and is highlighted with a red box.

**Step 5** Select **SSID2** for **SSID Index**.

**Step 6** Clear **Enable** for **SSID**. Then click **Submit**.

The screenshot shows the WLAN configuration interface after the second step. The 'WLAN' tab is active. The 'Enable WLAN' checkbox is checked. Under the 'Wireless Settings' section, the following fields are visible: Mode (802.11b/g/n), Country (CHINA), Channel (Auto), Transmit power (100%), Power Enhance (unchecked), SSID index (SSID2), SSID (SSID2), SSID (unchecked), Hide broadcast (unchecked), AP isolation (unchecked), Band width (20/40 MHz), Security (WPA2-PSK), WPA pre-shared key (masked), and WPA encryption (AES). The 'Submit' button is located at the bottom right and is highlighted with a red box.

**Step 7** Repeat Step 5 and Step 6 to disable other SSIDs.

---End

 **TIP**

If you consider the use of a WLAN as inconvenient after the SSID of the WLAN is hidden, you can restore the function of broadcasting the SSID as follows: For Hide Broadcast, clear Enable. Then click Submit.

## 5.3.2 Changing the Name of a WLAN

### Function Overview

If the router has hidden the SSID of a WLAN, you need to enter the SSID of the WLAN manually when you use a PC to access the WLAN. If you enter a wrong SSID, the PC cannot connect to the WLAN. Therefore, the security of the WLAN can be improved if the SSID is difficult to be predicted.

An SSID consists of 1–32 American Standard Code for Information Interchange (ASCII) characters. When the router is delivered, the SSID is preset. You can find this preset SSID on the label on the real panel of the router. In addition, the router supports the change of the SSID. You can change the SSID as required.

### Configuration Example

If your current SSID index is **SSID1** and if you have used this SSID for a certain period, to change this SSID to **MyNewSSID**, do as follows:

**Step 1** Log in to the Web-based configuration utility.

**Step 2** In the navigation tree, choose **Basic > WLAN**.

The WLAN configuration page is displayed.

**Step 3** Select **SSID1** for **SSID Index**.

**Step 4** In **SSID**, enter **MyNewSSID**.

**Step 5** Click **Submit**.

The screenshot shows the configuration interface for the WLAN. At the top, there are three tabs: 'WLAN', 'WLAN WDS', and 'WLAN Filtering'. Below the tabs, there is a checkbox for 'Enable WLAN' which is checked. The 'Wireless Settings' section is highlighted with a blue header. It contains the following fields:

- Mode: 802.11b/g/n
- Country: CHINA
- Channel: Auto
- Transmit power: 100%
- Power Enhance:  Enable
- SSID index: SSID1
- SSID: MyNewSSID
- Hide broadcast:  Enable
- AP isolation:  Enable
- Band width: 20/40 MHz
- Security: WPA2-PSK
- WPA pre-shared key: [Masked]
- WPA encryption: AES
- WPS:  Enable
- WPS mode: PBC

The 'Submit' button is located in the bottom right corner of the configuration area.

---End

### 5.3.3 Using Secure Encryption

#### Function Overview

To ensure the security of a WLAN, an important solution is to select an optimum security mode for the WLAN. After this security mode is used, a wireless client should provide the corresponding password when connecting to the WLAN and data is being transmitted after secure encryption. Thus, only authorized persons can use the WLAN and the data transmitted on the WLAN is protected against unauthorized access.

The router supports WEP encryption and multiple security modes, such as WPA-PSK and WPA2-PSK, thus meeting security requirements in diversified network environments.

It is recommended that you set the security mode to **WPA-PSK/WPA2-PSK** and the encryption mode to **AES**. Thus, the WLAN works efficiently and the security of the WLAN is ensured. In addition, if a wireless adapter does not support a certain security mode, it cannot be connected to the WLAN in this security mode. If you use the recommended security and encryption modes, this problem can be avoided.



**NOTE**

- The WPS function can be used only when the security mode is set to **WPA-PSK**, **WPA2-PSK**, or **WPA-PSK/WPA2-PSK**.
- AES = Advanced Encryption Standard

Table 5-1 lists the rules for setting the password used for accessing a WLAN in different security modes.

**Table 5-1** Rules for setting the password used for accessing a WLAN

Security Mode	Password Setting Rule
WEP encryption	<ul style="list-style-type: none"><li>• It uses 64-bit encryption (also referred to as 40-bit encryption). The password consists of five visible ASCII characters entered through a keyboard or 10 hexadecimal characters.</li><li>• It uses 128-bit encryption (also referred to as 104-bit encryption). The password consists of 13 visible ASCII characters entered through a keyboard or 26 hexadecimal characters.</li></ul>
WPA-PSK	The password consists of 8–63 visible ASCII characters entered through a keyboard or 64 hexadecimal characters.
WPA2-PSK	
WPA-PSK/ WPA2-PSK	

### Configuration Example

If you use the router at home, to select an optimum security mode, plan the parameters as follows:

- Set the security mode to **WPA-PSK/WPA2-PSK**.
- Set the encryption mode to **AES**.
- Set the password used for accessing the WLAN to **MyPassword@2012**.

To set the preceding parameters, do as follows:

- Step 1** Log in to the Web-based configuration utility.
- Step 2** In the navigation tree, choose **Basic > WLAN**.  
The WLAN configuration page is displayed.
- Step 3** Select **WPA-PSK/WPA2-PSK** for **Security Mode**.
- Step 4** In **WPA Pre-Shared Key**, enter **MyPassword@2012**.
- Step 5** Select **AES** for **WPA Encryption**.

**Step 6 Click Submit.**

The screenshot shows the configuration interface for the WLAN function. At the top, there are three tabs: 'WLAN', 'WLAN WDS', and 'WLAN Filtering'. The 'WLAN' tab is active. Below the tabs, there is a checkbox labeled 'Enable WLAN' which is checked. A section titled 'Wireless Settings' contains various configuration options: Mode (802.11 b/g/n), Country (CHINA), Channel (Auto), Transmit power (100%), Power Enhance (unchecked), SSID index (SSID1), SSID (MyNewSSID), Hide broadcast (unchecked), AP isolation (checked), Band width (20/40 MHz), Security (WPA-PSK/WPA2-P), WPA pre-shared key (a series of 12 black dots), WPA encryption (AES), WPS (checked), and WPS mode (PBC). A red box highlights the 'WPA pre-shared key' field and the 'Submit' button at the bottom right.

---End

 **NOTE**

After the password used for accessing a WLAN is changed, you need to enter the new password when connecting a PC to the WLAN.

### 5.3.4 Allowing Only Specified PCs to Be Connected to a WLAN

#### Function Overview

After the SSID is hidden and an optimum security mode is used, your WLAN is in a secure state. You can prohibit certain PCs from being connected to the WLAN or allow only specified PCs to be connected to the WLAN, thus preventing unauthorized users from accessing the WLAN.

Through the wireless MAC filtering function of the router, the preceding functions can be used after you enter the MAC addresses of the PCs to be controlled.

The wireless MAC filtering function can be implemented in the following modes:

- Blacklist: The PCs whose MAC addresses are listed in the filtering list are prohibited from being connected to the WLAN.
- Whitelist: The PCs whose MAC addresses are listed in the filtering list are allowed to be connected to the WLAN.

You can select either of the preceding modes for the wireless MAC filtering function.



**NOTE**

The wireless MAC filtering function controls the option of allowing a PC to be connected to the router through a WLAN. The MAC address filtering function described in section 5.4 "Controlling the Internet Access Rights of PCs" controls the option of allowing a PC connected to the router to access the Internet.

## Configuration Example

For example, you have a desktop computer and a laptop at home. The SSID of your WLAN is **MyNewSSID**. The desktop computer is connected to the router through a network cable. A wireless network adapter is installed on the laptop. To allow only the laptop to be connected to the WLAN and prohibit other unauthorized users from accessing the WLAN, you can use the whitelist mode of the wireless MAC filtering function. To create a whitelist and allow only your laptop to be connected to the WLAN, do as follows:

**Step 1** View and record the MAC address of the laptop.

Take the Windows XP operating system as an example. To view the MAC address of a PC, do as follows:

1. Choose **Start > Run**.
2. In **Open**, enter **cmd**. Then press **Enter**.
3. In the displayed command line window, enter **ipconfig /all**. Then press **Enter**.

Multiple lines of information is displayed. You can find a line of information that is similar to **Physical Address. . . . . : 00-11-09-11-04-DD. 00-11-09-11-04-DD** is the MAC address of the PC.

**Step 2** Log in to the Web-based configuration utility.

**Step 3** In the navigation tree, choose **Basic > WLAN**.

The WLAN configuration page is displayed.

**Step 4** Click **WLAN Filtering**.

**Step 5** Select **Enable**.

**Step 6** Select **Whitelist**.

**Step 7** Click **New**.

**Step 8** Select **MyNewSSID** for **Select SSID**.

**Step 9** In **Source MAC address**, enter the MAC address of the laptop.

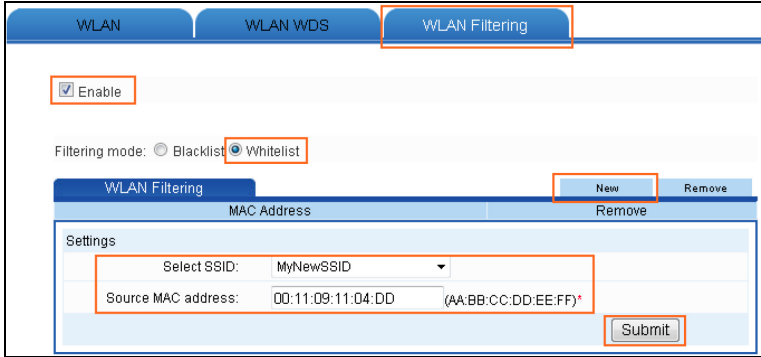
For example, the MAC address can be **00:11:09:11:04:DD**.



**NOTE**

The format of the MAC address entered in **Source MAC address** is different from that of the MAC address displayed in the command line window of a Windows XP operating system. The colons (:) replace the hyphens (-).

**Step 10 Click Submit.**



---End

## 5.4 Controlling the Internet Access Rights of PCs

### Function Overview

You can prohibit certain PCs from accessing the Internet or allow only certain PCs to access the Internet. In addition, you can set the period during which the PCs are not allowed to access the Internet.

Through the MAC address filtering function of the router, the preceding requirements can be met after you enter the MAC addresses of the PCs to be controlled.

The MAC address filtering function can be implemented in the following modes:

 **NOTE**

The MAC address filtering function controls the option of allowing a PC connected to the router to access the Internet. The wireless MAC filtering function controls the option of allowing a PC to be connected to the router through a wireless network.

### Configuration Example

For example, you have bought a PC for your child who is in a primary school. To restrict the Internet access period of the child to from 19:00 to 20:00 in each evening and to protect your PC from being restricted, you can use the MAC address filtering function.

Suppose the MAC address of the PC of your child is **00:11:09:11:04:DD**.

After the function of automatically synchronizing the time of the router with the network time is enabled, you need to create the following two filtering rules:

- Rule 1: From 00:00 to 18:59 each day, prohibit the PC whose MAC address is **00:11:09:11:04:DD** from accessing the Internet. The name of this rule is **Prohibited before 19:00**.

- Rule 2: From 19:59 to 23:59 each day, prohibit the PC whose MAC address is **00:11:09:11:04:DD** from accessing the Internet. The name of this rule is **Prohibited after 20:00**.

The configuration procedure is as follows:

**Step 1** Log in to the Web-based configuration utility.

**Step 2** In the navigation tree, choose **Advanced** > **SNTP**.

The network time configuration page is displayed.

**Step 3** Select **Enable auto synchronization with network time**.

**Step 4** Select a time service address for **Time server 1**.

For example, you can select **clock.fmt.he.net**.

**Step 5** Select your time zone for **Time zone**.

For example, if you are in China, you can select **(GMT+08:00) Beijing, Chongqing, Hong Kong, Urumqi**.

**Step 6** Click **Submit**.

Status	
Status	Disabled
Current Time	2011-12-31 16:45:15
<input checked="" type="checkbox"/> Enable auto synchronization with network time	

Settings	
Time server 1:	clock.fmt.he.net
Time server 2:	clock.nyc.he.net
Time server 3:	clock.sjc.he.net
Time server 4:	clock.via.net
Time server 5:	None
Time zone:	(GMT+08:00) Beijing, Chongqing, Hong Kong, Urumqi
<input type="checkbox"/> Enable daylight saving time	

**Step 7** In the navigation tree, choose **Advanced** > **Filter**.

The filter page is displayed.

**Step 8** Click **MAC Filter**.

**Step 9** Click **New**.

**Step 10** Set the following parameters based on rule 1.

- Rule name: Prohibited before 19:00
- Source MAC address: 00:11:09:11:04:DD
- Time control: Enable
- Start time: 00:00
- End time: 18:59

- Effective day: Select from Monday to Sunday.
- Status: Disable

**Step 11** Click **Submit**.

The screenshot shows the MAC Filtering configuration interface. At the top, there are tabs for 'MAC Filter', 'IP Filter', 'Application Filter', and 'URL Filter'. The 'MAC Filter' tab is active. Below it, there are 'New' and 'Remove' buttons. A table lists existing rules with columns: Rule Name, Source MAC Address, Destination MAC Address, Time Control, Sunday to Saturday, Time, Priority, Status, and Remove. Below the table is a 'Settings' section with the following fields:

- Rule name: Prohibited before 19:00
- Source MAC address: 00:11:09:04:DD (AA:BB:CC:DD:EE:FF)
- Bridge destination MAC address: (AA:BB:CC:DD:EE:FF)
- Time control:  Enable
- Start time: 00:00
- End time: 18:59
- Effective day:  Sunday,  Monday,  Tuesday,  Wednesday,  Thursday,  Friday,  Saturday
- Priority: 0
- Status: Disable

A 'Submit' button is located at the bottom right of the settings section.

**Step 12** Click **New**.

**Step 13** Set the following parameters based on rule 2.

- Rule name: Prohibited after 20:00
- Source MAC address: 00:11:09:11:04:DD
- Time control: Enable
- Start time: 19:59
- End time: 23:59
- Effective day: Select from Monday to Sunday.
- Status: Disable

**Step 14** Click **Submit**.

MAC Filtering				New		Remove		
Rule Name	Source MAC Address	Destination MAC Address	Time Control	Sunday to Saturday	Time	Priority	Status	Remove
Prohibited before 19:00	00:11:09:11:04:DD		Enable	YYYYYY	00:00-18:59	0	Disable	<input type="checkbox"/>

Settings

Rule name:

Source MAC address:  (AA:BB:CC:DD:EE:FF)

Bridge destination MAC address:  (AA:BB:CC:DD:EE:FF)

Time control:  Enable

Start time:

End time:

Effective day:  Sunday  Monday  Tuesday  
 Wednesday  Thursday  Friday  
 Saturday

Priority:

Status:

---End

**TIP**

To delete a rule, select the rule from the rule list. In the **Remove** column, select the rule. Then click **Remove**.

## 5.5 Prohibiting PCs from Accessing Specified Web Sites

### Function Overview

You can prohibit PCs from accessing specified Web sites or restrict PCs to accessing only specified Web sites.

Through the Uniform Resource Locator (URL) filtering function of the router, the preceding requirements can be met after you enter the addresses of the Web sites to be controlled.

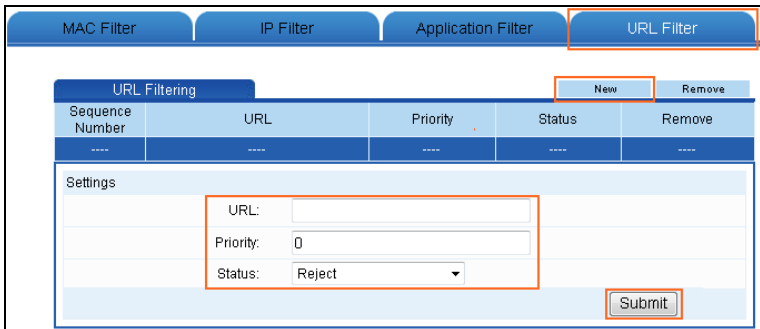
### Configuration Example

For example, the contents of the Web site whose address is **www\*.com** (\* indicates any domain name that you specify) are not suitable for browsing. To prevent your family

from browsing this Web site, you can use the URL filtering function and create a rule used for prohibiting this Web site from being accessed.

The configuration procedure is as follows:

- Step 1** Log in to the Web-based configuration utility.
- Step 2** In the navigation tree, choose **Advanced > Filter**.  
The filter page is displayed.
- Step 3** Click **URL Filter**.
- Step 4** Click **New**.
- Step 5** In **URL**, enter the Web site address you specify.
- Step 6** In **Status**, select **Reject**.
- Step 7** Click **Submit**.



----End

 **TIP**

To delete a rule, select the rule from the rule list. In the **Remove** column, select the rule. Then click **Remove**.

## 5.6 Setting the Available Bandwidth of a PC

### Function Overview

The router provides traffic management function to control the bandwidth used by a PC for accessing the Internet. Through different bandwidth control rules, the router can implement the following bandwidth control functions:

- Ensuring the bandwidth used by a specified PC for accessing the Internet is not less than a specified bandwidth so that the PC can access the Internet at a required rate
- Restricting the bandwidth used by a specified PC for accessing the Internet to a specified bandwidth so that this PC cannot use excessive bandwidth and the Internet access rates of other PCs are not affected

The router supports four types of traffic management. You can select one of them to let it take effect.

- IP Address: Manage traffic according to the IP address of the LAN side device.
- MAC Address: Manage traffic according to the MAC address of the LAN side device.
- LAN Interface: Manage traffic according to the LAN interface.
- Application: Manage traffic according to the application.

## Configuration Example

For example, you use a PC for video communications with your friend over the Internet and the name of your PC is **myPC**. The PC connects with the router through "LAN1" interface and its IP address is **192.168.3.2**, MAC address is **3C-D9-2B-5C-C0-23**. To ensure a fast data transmission rate and smooth video quality, you can use the following four ways to meet the demand for bandwidth control.

### Manage Traffic according to the IP Address

The configuration procedure is as follows:

**Step 1** Log in to the Web-based configuration utility.

**Step 2** In the navigation tree, choose **Advanced > IP QoS**.

**Step 3** Select **Enable Traffic Management**.

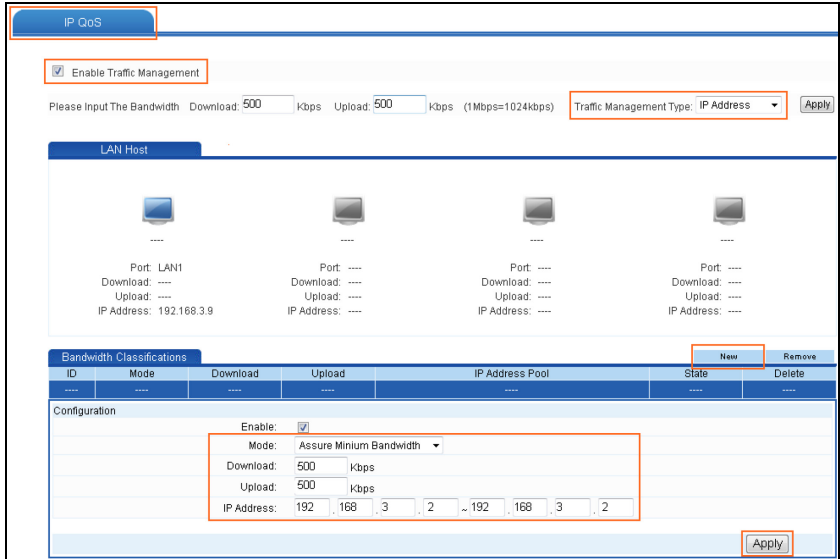
The configuration page for the traffic control function is displayed.

**Step 4** In **Traffic Management Type**, select **IP Address**.

**Step 5** Under **Bandwidth Classifications**, click **New** and set the following parameters:

- Mode: Assure Minimum Bandwidth
- Download: 500 kbit/s
- Upload: 500 kbit/s
- IP Address: 192.168.3.2~192.168.3.2

**Step 6 Click Apply.**



---End

**Manage Traffic according to the MAC Address**

The configuration procedure is as follows:

**Step 1** Log in to the Web-based configuration utility.

**Step 2** In the navigation tree, choose **Advanced > IP QoS**.

**Step 3** Select **Enable Traffic Management**.

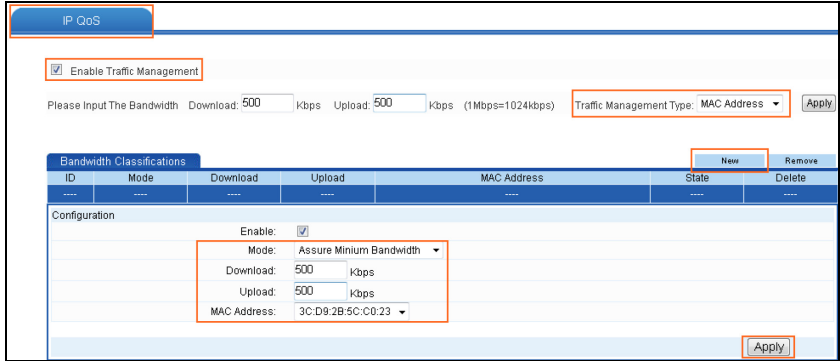
The configuration page for the traffic control function is displayed.

**Step 4** In **Traffic Management Type**, select **MAC Address**.

**Step 5** Under **Bandwidth Classifications**, click **New** and set the following parameters:

- Mode: Assure Minimum Bandwidth
- Download: 500 kbit/s
- Upload: 500 kbit/s
- MAC Address: 3C:D9:2B:5C:C0:23

**Step 6** Click **Apply**.



----End

## Manage Traffic according to the LAN Interface

The configuration procedure is as follows:

**Step 1** Log in to the Web-based configuration utility.

**Step 2** In the navigation tree, choose **Advanced > IP QoS**.

**Step 3** Select **Enable Traffic Management**.

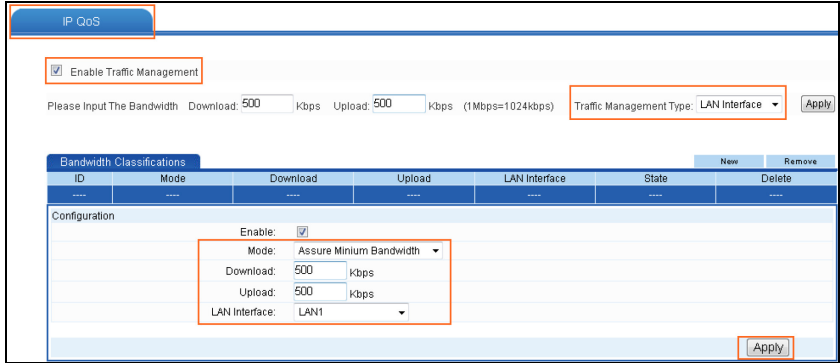
The configuration page for the traffic control function is displayed.

**Step 4** In **Traffic Management Type**, select **LAN Interface**.

**Step 5** Under **Bandwidth Classifications**, click **New** and set the following parameters:

- Mode: Assure Minimum Bandwidth
- Download: 500 kbit/s
- Upload: 500 kbit/s
- LAN Interface: LAN1

**Step 6** Click **Apply**.



---End

**Manage Traffic according to the Application**

The configuration procedure is as follows:

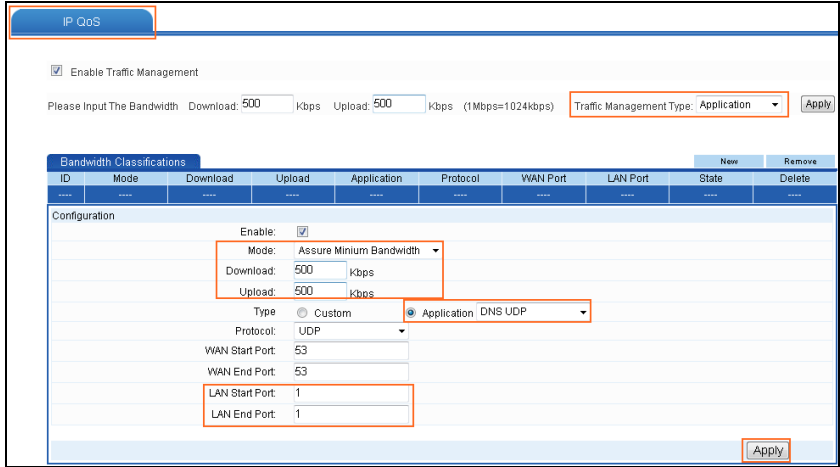
- Step 1** Log in to the Web-based configuration utility.
- Step 2** In the navigation tree, choose **Advanced > IP QoS**.
- Step 3** Select **Enable Traffic Management**.  
The configuration page for the traffic control function is displayed.
- Step 4** In **Traffic Management Type**, select **Application**.
- Step 5** Under **Bandwidth Classifications**, click **New**.
- Step 6** Select **Application**. Then select **DNS UDP** for **Application**.

**TIP**

The router provides parameter setting templates of multiple applications. After a template is selected, the router sets certain parameters automatically. You can change the parameter settings as required. You can also set all the parameters manually based on the requirements of other applications.

- Step 7** Set the following parameters:
  - Mode: Assure Minimum Bandwidth
  - Download: 500 kbit/s
  - Upload: 500 kbit/s
  - LAN Start Port: 1
  - LAN End Port: 1

**Step 8** Click **Apply**.



----End

## 5.7 Preventing Attacks on the Internet

### Function Overview

The Internet is an open network that is connected to PCs all over the world. Therefore, the PCs on the Internet may be attacked anytime. The router provides powerful firewall functions. By using the firewall, a protective shelter is established between your home network and the Internet, thus protecting your PC from attacks on the Internet.

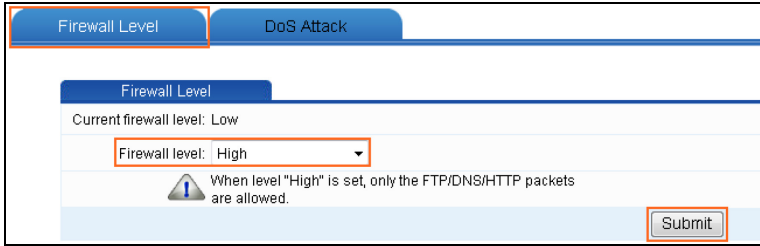
### Configuration Example

If you have stringent requirements on network security, you can set the firewall level of the router to **High** and set the router to prevent DoS attacks.

The configuration procedure is as follows:

- Step 1** Log in to the Web-based configuration utility.
- Step 2** In the navigation tree, choose **Advanced** > **Firewall**.  
The firewall page is displayed.
- Step 3** Click **Firewall Level**.
- Step 4** Select **High** for **Firewall level**.

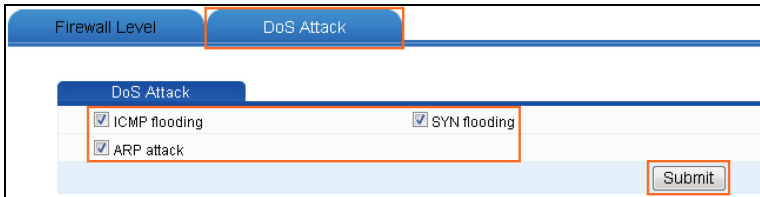
**Step 5** Click **Submit**.



**Step 6** Click **DoS Attack**.

**Step 7** Under **DoS Attack**, select the **ICMP flooding**, **SYN flooding** and **ARP attack**.

**Step 8** Click **Submit**.



----End

## 5.8 Removing the Restriction Caused by the Binding of the Internet Access Account to the MAC Address

### Function Overview

Certain network service providers bind your Internet access account to the MAC address of the network adapter of your PC. Thus, only the PC with that MAC address can be connected to the Internet. In this case, the MAC address of the router cannot be found in the network devices of a network service provider. Therefore, the router cannot be connected to the Internet and the PCs connected to the router cannot access the Internet also.

You can use the MAC address cloning function of the router to remove the restriction caused by the binding of the Internet access account and the MAC address. Through this function, the MAC address used during the communications between the router and the network devices of a network service provider is the MAC address that is bound to the Internet access account. Thus, the router can be connected to the Internet properly.

## Configuration Example

For example, you use PC 1 for accessing the Internet. Your network service provider binds your Internet access account to the MAC address of the network adapter of PC 1. Now, multiple PCs are added to your home and you need to use the router for accessing the Internet. You can use the MAC address cloning function of the router. Thus, the MAC address of the router is the same as that of the network adapter of PC 1.

The configuration procedure is as follows:

**Step 1** Log in to the Web-based configuration utility on PC 1.

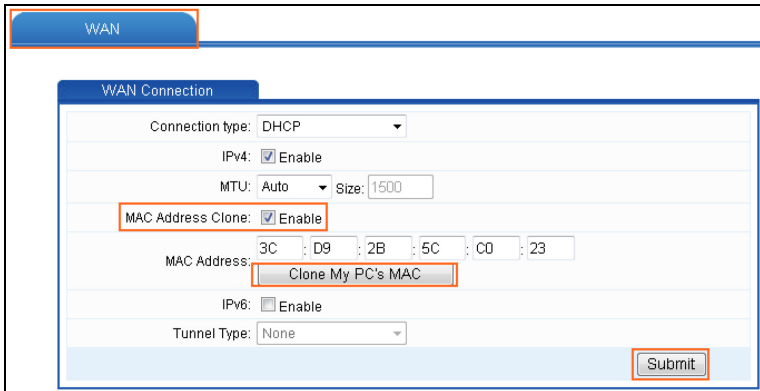
**Step 2** In the navigation tree, choose **Basic > WAN**.

The WAN interface configuration page is displayed.

**Step 3** Set **MAC Address Clone** to **Enable**.

**Step 4** Click **Clone My PC's MAC**.

**Step 5** Click **Submit**.



----End

## 5.9 Binding the IP address and MAC address

### Function Overview

Binding the IP address and MAC address of the computer can effectively prevent from ARP attacks. The router provides both the uplink binding and downlink binding. You can specify the IP address or MAC address binding constraints IP address or MAC address to prevent from the ARP attacks and safely access to the Internet.

### Configuration Example

Binding a computer with the IP address **192.168.3.2** and MAC address **44-37-E6-97-C8-3E**, refer to the following steps:

- Step 1** Log in to the Web-based configuration utility.
- Step 2** In the navigation tree, choose **Advanced > IP MAC Bind**.  
The IP MAC bind configuration page is displayed.
- Step 3** Select **Enable Bind**.
- Step 4** In **IP**, enter the IP address **192.168.3.2**.
- Step 5** In **MAC**, Enter the MAC address **44:37:E6:97:C8:3E**.
- Step 6** Click **Submit**.

The screenshot shows the 'IP MAC Bind' configuration page. At the top, there are two tabs: 'IP MAC Bind' and 'ARP'. The 'IP MAC Bind' tab is active. Below the tabs, there is a checkbox labeled 'Enable Bind' which is checked. Underneath, there is a table with the following structure:

ID	IP	MAC	Remove
----	----	----	----

Below the table, there is a 'Settings' section with two input fields: 'IP: 192.168.3.2' and 'MAC: 44:37:E6:97:C8:3E'. A 'Submit' button is located at the bottom right of the settings section. A 'New' button is also visible above the table.

Enable a binding rule in the ARP table, refer to the following steps:

- Step 1** Click **ARP**.
- Step 2** Select the desired binding rule, and click **Bind**.

The screenshot shows the 'ARP' configuration page. At the top, there are two tabs: 'IP MAC Bind' and 'ARP'. The 'ARP' tab is active. Below the tabs, there is a table titled 'ARP List' with the following structure:

ID	IP	MAC	Status	Bind
1	192.168.3.2	44:37:e6:97:c8:3e	BIND	Bind
2	192.168.3.9	3c:d9:2b:5c:c0:23	UNBIND	Bind

At the bottom right of the table, there is a 'Bind All' button. The 'Bind' button in the second row is highlighted.

----End



**NOTE**

To delete a binding rule, select the corresponding check box in the Remove column and click **Remove**.

## 5.10 Allowing Internet Users to Access an Internal Resource Server

### Function Overview

Without special settings, Internet users cannot access the Web or FTP servers on a LAN. By using the network address translation (NAT) function of the router, Internet users are allowed to access the Web and FTP servers on the LAN.

In addition, the IP addresses used by most users for accessing the Internet are dynamically assigned by network service providers. Thus, Internet users cannot use fixed IP addresses to access the resources provided on servers. Through the Dynamic Domain Name Service (DDNS) function of the router, Internet users can use fixed domain names to access the resources provided on servers.

After the DDNS function is enabled, the router automatically submits the new IP address obtained each time to the server of a DDNS provider. On the DDNS server, the IP address that corresponds to the domain name is updated to the latest IP address. When a PC on the Internet accesses the domain name, the DDNS server provides the latest IP address to the PC.

### Configuration Example

For example, you deploy a Web server on a LAN. You want Internet users to be able to access the Web site on the Web server through a fixed domain name. The IP addresses of the relevant devices are as follows:

- The IP address of the LAN interface of the router is **192.168.3.1**.
- The IP address of the Web server is **192.168.3.166**.

You can use the port relay function of the NAT and the DDNS function to implement the preceding requirement.

Before configuration, you need to complete the following preparations:

- Apply for the DDNS to a DDNS provider and obtain the relevant parameters.
- Apply for a domain name for the Web site to the institution for managing the domain names of Web sites.

After the preceding preparations, plan the parameters of the router as follows:

- Configure a port mapping rule, and then map the IP address of the Web server (**192.168.3.166:80**) to the **80** port of the WAN interface.
- Configure the DDNS. Ensure that the router can submit IP addresses to the DDNS server automatically.

The configuration procedure is as follows:

**Step 1** Log in to the Web-based configuration utility.

**Step 2** In the navigation tree, choose **Advanced > NAT**.

The NAT page is displayed.

**Step 3** Click **Port Mapping**.

**Step 4** Click **New**.

**Step 5** Select **Application**. Then select **Security Web server (HTTPS)** for **Application**.

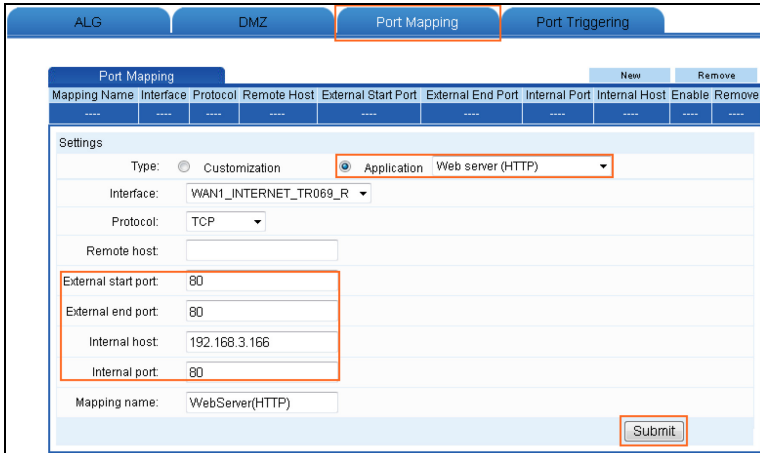
 **TIP**

The port mapping function of the router provides parameter setting templates of multiple applications. After a template is selected, the router sets certain parameters automatically. You can change the parameter settings as required. You can also set all the parameters manually based on the requirements of other applications.

**Step 6** Set the following parameters as planned.

- External start port: 80
- External end port: 80
- Internal host: 192.168.3.166
- Internal port: 80

**Step 7** Click **Submit**.



The screenshot shows the 'Port Mapping' configuration page. At the top, there are tabs for 'ALG', 'DMZ', 'Port Mapping', and 'Port Triggering'. The 'Port Mapping' tab is active. Below the tabs, there is a table with columns: 'Mapping Name', 'Interface', 'Protocol', 'Remote Host', 'External Start Port', 'External End Port', 'Internal Port', 'Internal Host', 'Enable', and 'Remove'. Below the table, there is a 'Settings' section. In the 'Settings' section, 'Type' is set to 'Application' with a dropdown menu showing 'Web server (HTTP)'. 'Interface' is set to 'WAN1\_INTERNET\_TR069\_R'. 'Protocol' is set to 'TCP'. 'Remote host' is empty. 'External start port' is set to '80'. 'External end port' is set to '80'. 'Internal host' is set to '192.168.3.166'. 'Internal port' is set to '80'. 'Mapping name' is set to 'WebServer(HTTP)'. A 'Submit' button is located at the bottom right of the settings section.

**Step 8** In the navigation tree, choose **Advanced** > **DDNS**.

The DDNS configuration page is displayed.

**Step 9** Click **New**.

**Step 10** Select **Others** for **Service provider**.

 **TIP**

The DDNS function of the router provides parameter setting templates of multiple DDNS providers. After a template is selected, the router sets certain parameters automatically. You can change the parameter settings as required. You can also set all the parameters again as required.

**Step 11** Set the parameters provided by your network service provider.

**Step 12 Click Submit.**

---End

## 5.11 Expanding the Coverage of a WLAN

### Function Overview

The router supports the WDS function. Through the WDS function, two routers can be connected wirelessly, thus expanding the coverage of a WLAN.

Table 5-1 lists three WDS working modes, functions in each working mode, and relevant setting requirements.

**Table 5-1** WDS working modes

Working Mode	Function	Setting Requirements
Bridge	Two WLANs can be connected wirelessly in this mode but other wireless clients cannot be connected to the router.	On each router, add the wireless MAC address of the peer router to the WDS MAC list.
Repeater	It is used to expand the coverage of a WLAN. The router can set up a connection with another wireless router or wireless client.	On each router, add the wireless MAC address of the peer router to the WDS MAC list.
Lazy	The function in this mode is the same as that in repeater mode. No WDS MAC list, however, is required to be configured on the router in lazy mode.	No WDS MAC list is required to be configured on the router in lazy mode. The MAC address of the router in lazy mode, however, needs to be added to the WDS MAC list of the peer router.

When configuring the WDS function, you should comply with the following principles:

- Both wireless routers should support the WDS function.
- The WDS function should be enabled on both wireless routers.
- On each router, add the wireless MAC address of the peer router to the WDS MAC list. No WDS MAC list is required to be configured on the router in lazy mode but a WDS MAC list should be configured on the peer router.
- The settings of the following parameters on both wireless routers should be the same:
  - Wireless channel
  - Encryption mode
  - Encryption password

**NOTE**

- The security modes set on the two wireless routers can be different but the encryption modes should be the same.
- The SSIDs of the two WLANs can be different but it is recommended that the two WLANs use the same SSID. Thus, wireless terminals can use one SSID to connect to the WLAN that is expanded.
- If the repeater mode is used for expanding the coverage of a WLAN, note that:
  - The IP addresses of the LAN interfaces of the two routers should be in the same network segment. In addition, the IP addresses should be different.
  - Enable the DHCP server function only on the wireless router that is used to connect to uplink devices. Disable the DHCP function and enable the DHCP relay function on other wireless routers.

## Configuration Example

For example, you have router A in your spacious house. The signals of router A cannot cover the area that is far from the router. In this case, you can add another router, that is, router B. By configuring the WDS function on the two routers, you can expand the coverage of a WLAN.

The parameters of the routers are planned as follows:

Router A:

- Set the IP address of the LAN interface to **192.168.3.1** (default value).
- Set the subnet mask of the LAN interface to **255.255.255.0** (default value).
- Enable the DHCP server function (default value).
- Select **SSID1** for **SSID** (default value).
- Set the name of **SSID1** to **mySSID**.
- Set the WLAN channel to **1**.
- The WLAN encryption settings are as follows:
  - Set the security mode to **WPA-PSK/WPA2-PSK**.
  - Set the encryption mode to **AES**.
  - Set the password used for accessing the WLAN to **MyPassword@2012**.

- Enable the WDS function and set the WDS mode to **Repeater**.
- Add the wireless MAC address of router B to the WDS MAC list.

Router B:

- Set the IP address of the LAN interface to **192.168.3.100**.
- Set the subnet mask of the LAN interface to **255.255.255.0**.
- Disable the DHCP server function.
- Enable the DHCP relay function.
- Select **SSID1** for **SSID** (default value).
- Set the name of **SSID1** to **my SSID** that is the same as the setting on router A.
- Set the WLAN channel to **1** that is the same as the setting on router A.
- The WLAN encryption settings are as follows (the same as the settings on router A):
  - Set the security mode to **WPA-PSK/WPA2-PSK**.
  - Set the encryption mode to **AES**.
  - Set the password used for accessing the WLAN to **MyPassword@2012**.
- Enable the WDS function and set the WDS mode to **Repeater**.
- Add the wireless MAC address of router A to the WDS MAC list.

The configuration procedure is as follows:

 **NOTE**

The following procedure describes how to change the parameter settings as required. You can retain the default settings of the parameters that do not need to be changed.

**Step 1** Find and record the wireless MAC addresses of router A and router B (You can obtain the wireless MAC address by the wireless card client).

Suppose the wireless MAC address of router A is **AA:AA:AA:AA:AA:AA** and that of router B is **BB:BB:BB:BB:BB:BB**.

**Step 2** Set the WLAN parameters of router A.

1. Log in to the Web-based configuration utility of router A.
2. In the navigation tree, choose **Basic > WLAN**.  
The WLAN configuration page is displayed.
3. Click **WLAN**.
4. Select **Enable WLAN**.
5. Set the following parameters.
  - Channel: 1
  - SSID Index: SSID1
  - SSID: mySSID
  - Security: WPA-PSK/WPA2-PSK
  - WPA pre-Shared key: MyPassword@2012
  - WPA encryption: AES
6. Click **Submit**.

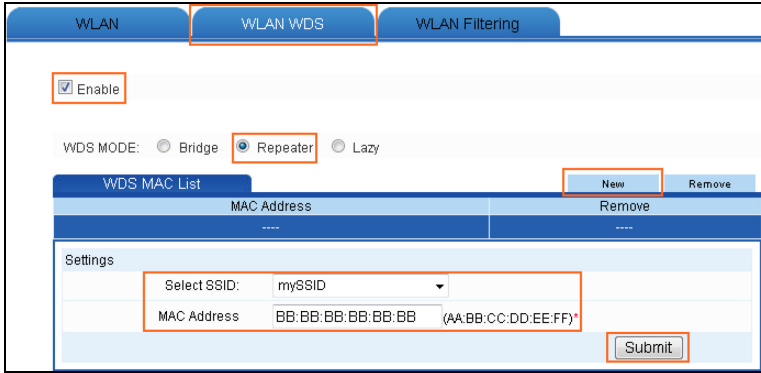
The screenshot shows the WLAN configuration interface. At the top, there are three tabs: 'WLAN', 'WLAN WDS', and 'WLAN Filtering'. The 'WLAN' tab is active. Below the tabs, there is a checkbox labeled 'Enable WLAN' which is checked. A section titled 'Wireless Settings' contains the following fields:

- Mode: 802.11b/g/n
- Country: CHINA
- Channel: 1
- Transmit power: 100%
- Power Enhance:  Enable
- SSID index: SSID1
- SSID: mySSID
- Hide broadcast:  Enable
- AP isolation:  Enable
- Band width: 20/40 MHz
- Security: WPA-PSK/WPA2-P
- WPA pre-shared key: 12345678901234567890123456789012
- WPA encryption: AES
- WPS:  Enable
- WPS mode: PBC

A 'Submit' button is located at the bottom right of the configuration area.

**Step 3** Configure the WDS function of router A.

1. In the navigation tree, choose **Basic > WLAN**.  
The WLAN configuration page is displayed.
2. Click **WLAN WDS**.
3. Select **Enable**.
4. Select **Repeater** for **WDS Mode**.
5. Click **New**.
6. Select **mySSID** for **Select SSID**.
7. In **MAC Address**, enter **BB:BB:BB:BB:BB:BB**.  
This MAC address is the wireless MAC address of router B and is recorded in Step 1.
8. Click **Submit**.



- Step 4** Set the WLAN parameters of router B.
1. Log in to the Web-based configuration utility of router B.
  2. In the navigation tree, choose **Basic > WLAN**.  
The WLAN configuration page is displayed.
  3. Click **WLAN**.
  4. Select **Enable WLAN**.
  5. Set the following parameters.
    - Channel: 1
    - SSID Index: SSID1
    - SSID: mySSID
    - Security: WPA-PSK/WPA2-PSK
    - WPA pre-Shared Key: MyPassword@2012
    - WPA encryption: AES

6. Click **Submit**.

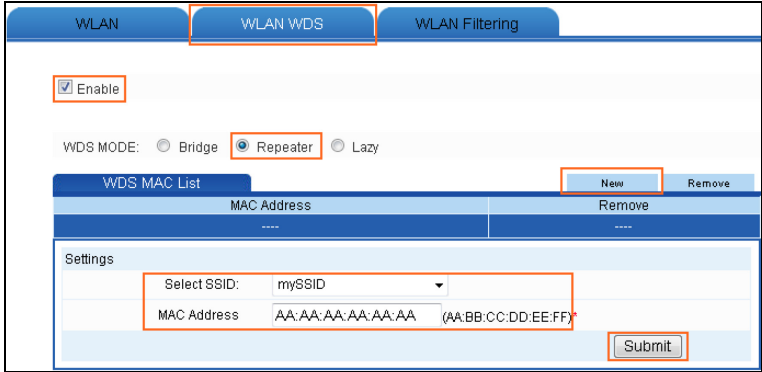
The screenshot shows the WLAN configuration interface. At the top, there are three tabs: 'WLAN', 'WLAN WDS', and 'WLAN Filtering'. The 'WLAN' tab is selected. Below the tabs, there is a checkbox labeled 'Enable WLAN' which is checked. Underneath, there is a section titled 'Wireless Settings'. The settings include: Mode: 802.11b/g/n; Country: CHINA; Channel: 1; Transmit power: 100%; Power Enhance: [ ] Enable; SSID index: SSID1; SSID: mySSID; Hide broadcast: [ ] Enable; AP isolation: [ ] Enable; Band width: 20/40 MHz; Security: WPA-PSK/WPA2-P; WPA pre-shared key: a series of 12 black dots; WPA encryption: AES; WPS: [ ] Enable; WPS mode: PBC. A 'Submit' button is located at the bottom right of the configuration area.

**Step 5** Configure the WDS function of router B.

1. In the navigation tree, choose **Basic > WLAN**.  
The WLAN configuration page is displayed.
2. Click **WLAN WDS**.
3. Select **Enable**.
4. Select **Repeater** for **WDS Mode**.
5. Click **New**.
6. Select **mySSID** for **Select SSID**.
7. In **MAC Address**, enter **AA:AA:AA:AA:AA:AA**.

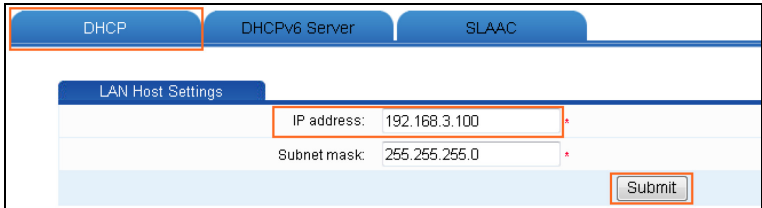
This MAC address is the wireless MAC address of router A and is recorded in Step 1.

8. Click **Submit**.



**Step 6** Change the IP address of the LAN interface of router B.

1. In the navigation tree, choose **Basic > LAN**.  
The LAN configuration page is displayed.
2. Click **DHCP**.
3. Under **LAN Host Settings**, enter **192.168.3.100** in **IP address**.
4. Under **LAN Host Settings**, click **Submit**.



**Step 7** Disable the DHCP server function of router B.

1. In the navigation tree, choose **Basic > LAN**.  
The LAN configuration page is displayed.
2. Click **DHCP**.
3. Under **DHCP Server**, clear **Enable**.

- Under **DHCP Server**, click **Submit**.

The screenshot shows the DHCP Server configuration interface. At the top, there are three tabs: 'DHCP', 'DHCPv6 Server', and 'SLAAC'. The 'DHCP' tab is selected. Below the tabs, there is a sub-tab 'DHCP Server'. The main configuration area includes:
 

- 'DHCP server':  Enable
- 'Start IP address': 192.168.3.101
- 'End IP address': 192.168.3.254
- 'Lease duration':  Infinite lease; 1 day(s), 0 hour(s), 0 minute(s); 0 second(s)
- 'Primary DNS server address': 192.168.3.100
- 'Secondary DNS server address': (empty)
- 'Submit' button at the bottom right.

**Step 8** Enable the DHCP relay function of router B.

- In the navigation tree, choose **Basic > LAN**.  
The LAN configuration page is displayed.
- Click **DHCP**.
- Under **DHCP Option Pool**, select a device type for **Device type**, such as **computer**.
- Under **DHCP Option Pool**, select **Enable** for **DHCP relay**.
- Under **DHCP Option Pool**, click **Submit**.

The screenshot shows the DHCP Option Pool configuration interface. At the top, there are three tabs: 'DHCP', 'DHCPv6 Server', and 'SLAAC'. The 'DHCP' tab is selected. Below the tabs, there is a sub-tab 'DHCP Option Pool'. The main configuration area includes:
 

- 'Device type': Computer (dropdown menu)
- 'DHCP Option pool':  Enable
- 'Start IP address': 0.0.0.0
- 'End IP address': 0.0.0.0
- 'DHCP relay':  Enable
- 'Operation':  Set,  Delete,  Update
- 'Submit' button at the bottom right.

---End

---

# 6 Maintenance Guide

---

## 6.1 Changing the Administrator Password of the Web-based Configuration Utility

### Function Overview

You can configure all the parameters of the router through the Web-based configuration utility. To prevent unauthorized personnel from changing these parameters, you need to use the administrator name and password to log in to the Web-based configuration utility.

After logging in to the Web-based configuration utility, you can change the administrator password.

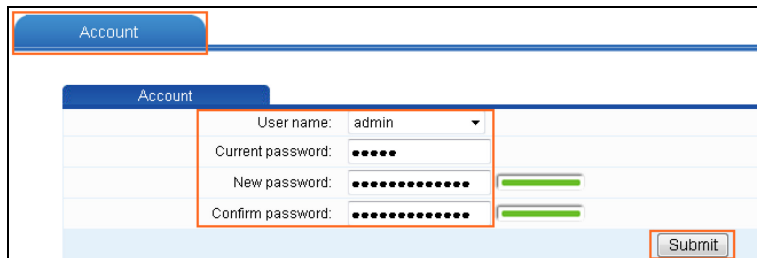
 **TIP**

If you cannot remember the password that has been changed, you can restore the default settings of the router by pressing and holding the RESET button for more than 6s. In this case, the login password of the Web-based configuration utility is restored to **admin**. When the default settings are restored, your customized data is lost. Therefore, use the RESET button with caution.

### Configuration Example

For example, the administrator password is **admin**. To change the password to **MyWebPassword**, do as follows:

- Step 1** Log in to the Web-based configuration utility.
- Step 2** In the navigation tree, choose **Maintenance** > **Account** to display the account management page.
- Step 3** Select **admin** from the **User Name** drop-down list box.
- Step 4** In **Current password**, enter the currently used password **admin**.
- Step 5** In **New password**, enter the new password **MyWebPassword**. In **Confirm password**, enter the new password **MyWebPassword** again.

**Step 6** Click **Submit**.

The screenshot shows a web-based login interface. At the top, there is a blue header bar with the word "Account" in white. Below this, there is a main content area with a blue sub-header "Account". The login form consists of four fields: "User name:" with a dropdown menu showing "admin", "Current password:" with a masked password field, "New password:" with a masked password field and a green progress indicator to its right, and "Confirm password:" with a masked password field and a green progress indicator to its right. At the bottom right of the form is a "Submit" button. Red boxes highlight the "Account" header, the login form fields, and the "Submit" button.

---End

## 6.2 Changing the Login IP Address of the Web-based Configuration Utility

### Function Overview

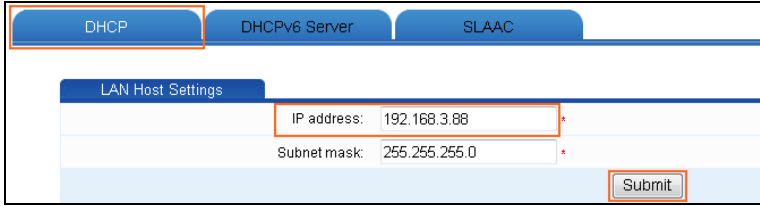
You can access the Web-based configuration utility by accessing the IP address of the LAN interface of the router **192.168.3.1** (the subnet mask is **255.255.255.0**). You can also change the IP address according to actual requirements. If you change the IP address of the LAN interface, ensure that the IP address of the computer and the IP address of the LAN interface of the router are in the same network segment to enable the computer to access the Web-based configuration utility. In this case, to access the Web-based configuration utility, you need to enter the new IP address in the address bar.

### Configuration Example

For example, the login IP address of the Web-based configuration utility is **192.168.3.1** and the subnet mask is **255.255.255.0**. To change the IP address to **192.168.3.88** (the subnet mask remains the same), do as follows:

- Step 1** Log in to the Web-based configuration utility.
- Step 2** In the navigation tree, choose **Basic** > **LAN** to display the LAN configuration page.
- Step 3** Click **DHCP**.
- Step 4** In **IP address** under the **LAN Host Settings** group box, enter the new IP address **192.168.3.88** in **IP address**.

**Step 5** Under **LAN Host Settings**, click **Submit**.



DHCP		DHCPv6 Server	SLAAC
LAN Host Settings			
IP address:	192.168.3.88	*	
Subnet mask:	255.255.255.0	*	
			Submit

---End

## 6.3 Backing Up or Importing a Configuration File

### Function Overview

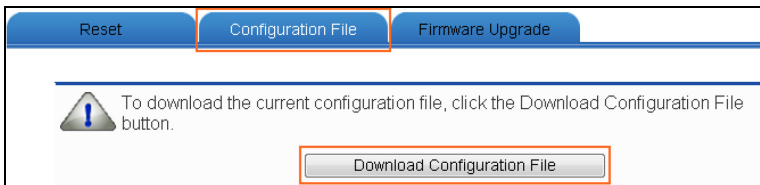
By using the parameter backup function, you can save a backup of the configuration file of the router to a PC. If the configuration file of the router is modified by mistake, you can import the backup file to the router.

### Configuration Example

For example, you have modified multiple advanced parameters according to actual requirements; and you need to modify the parameters again for some reasons. To prevent a network access failure due to misoperations, you can back up the configuration file of the router. Once the modification of the parameters fails, you can quickly restore the router to the normal state.

To back up the configuration file, do as follows:

- Step 1** Log in to the Web-based configuration utility.
- Step 2** In the navigation tree, choose **Maintenance > Device**.
- Step 3** On the **Configuration File** tab, click **Download Configuration File**.



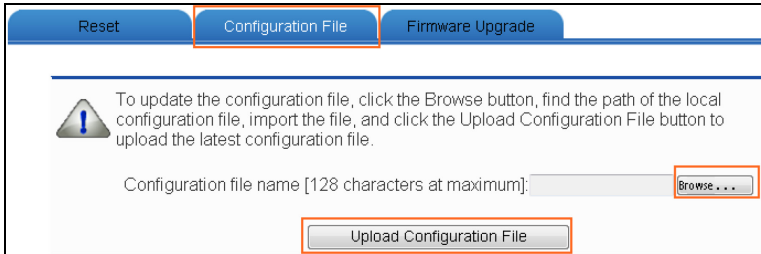
Reset	Configuration File	Firmware Upgrade
To download the current configuration file, click the Download Configuration File button.		
Download Configuration File		

**Step 4** In the displayed dialog box, set the name and storage location of the configuration file. Then click **OK**.

---End

To import the configuration file, do as follows:

- Step 1** Log in to the Web-based configuration utility.
- Step 2** In the navigation tree, choose **Maintenance > Device**.
- Step 3** Click **Configuration File**.
- Step 4** Click **Browse**.
- Step 5** In the displayed dialog box, select the backup configuration file. Then click **OK**.
- Step 6** Click **Upload Configuration File**.



---End

## 6.4 Restoring Default Settings

### Function Overview

The router provides powerful functions and rich parameters. Many parameters are set by default when the router is manufactured. Those parameters enable the router to work in most of network environments. In the following cases, you can restore the default settings of the router: You cannot access the network after you have changed the parameters or you have forgotten the login password of the Web-based configuration utility.

You can restore the default settings by using either of the following methods:

- Pressing the RESET button
- Using the Web-based configuration utility

### Configuration Example

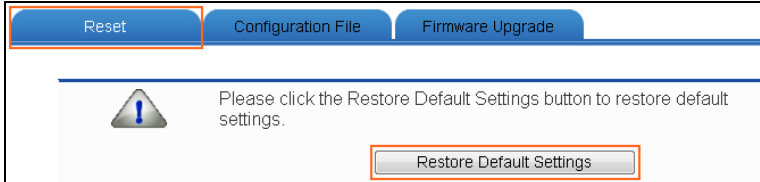
For example, you have changed the login password of the Web-based configuration utility and you have forgotten the login password. You can press the RESET button to quickly restore the default settings of the router.

When the router is powered on, press and hold the RESET button for more than 6s, and then release it. Then the router automatically restarts and the default settings are restored.

If your operations fail after multiple configurations and if you need to cancel all the preceding configurations, you can use the Web-based configuration utility to restore the

default settings. To restore the default settings through the web-based configuration utility, do as follows:

- Step 1** Log in to the Web-based configuration utility.
- Step 2** In the navigation tree, choose **Maintenance > Device**.
- Step 3** Click **Reset**.
- Step 4** Click **Restore Default Settings**.



- Step 5** In the displayed dialog box, click **OK**.  
---End

## 6.5 Upgrading Software

### Function Overview

By using the software upgrading function, you can upgrade the software of the router to the latest version.



### CAUTION

During the upgrade, do not power off the router; otherwise, the router may get damaged.

### Configuration Example


You can download the latest software from the technical support Web site: <http://consumer.huawei.com/en/>

To upgrade the software of the router, do as follows:

- Step 1** Log in to the Web-based configuration utility.
- Step 2** In the navigation tree, choose **Maintenance > Device**.
- Step 3** Click **Firmware Upgrade**.
- Step 4** Click **Browse**.
- Step 5** In the displayed dialog box, select the upgrade file. Then click **OK**.

**Step 6** Click **Software Upgrade**.

Reset Configuration File **Firmware Upgrade**

 To upgrade your home gateway, click the Browse button, find the path of the local image file, import the file, and click the Software Upgrade button to upload your image file.

Upgrade file name [128 characters at maximum]:  **Browse...**

**Software Upgrade**

**---End**

---

# 7 FAQs

---

## Q 1: Can I use the router as a DHCP server?

---

Yes, you can. The router incorporates the DHCP server software.

## Q 2: How can I quickly restore the default settings of the router?

---

When the router is powered on, press and hold the RESET button for more than 3s, and then release it. Then the router automatically restarts and the default settings are restored.

## Q 3: What can I do if I cannot access the router configuration page?

---

**Step 1** Check that the cables, such as the power cable and telephone cable, are securely connected, and that the LAN port's indicator is on.

**Step 2** Check that the user name and password to access the web management page are correct.

**Step 3** Check whether the computer's IP address is 192.168.3.\*. (\* is any integer from 2 to 254.) If not, see chapter 3.1 "Logging In to the Web-Based Configuration Utility" to set the IP address. If the computer cannot properly obtain an IP address, restart the computer.

**Step 4** Launch the Internet Explorer, choose **Tools > Internet Options > Connections > LAN settings**, and ensure that none of the check boxes are selected.

If the problem persists, restore the router to its factory settings.

---End

## Q 4: Does the WPS function have any special requirement on the wireless encryption settings of the router?

---

The WPS function can be used only when the security mode of the WLAN is set to **WPA-PSK** or **WPA2-PSK** and the SSID is set to **SSID1**. It is recommended that you set the security mode to **WPA-PSK/WPA2-PSK** for the WLAN.

## Q 5: If my PC fails to connect to a WLAN after I press and hold the WPS button, what should I do?

---

**Step 1** Ensure that only one computer is trying to connect to the router through the WPS function at a particular moment.

**Step 2** On the router, ensure that the wireless network function and the WPS function implemented through the PBC method are enabled. Note that on some wireless routers,

the WPS function is forcibly disabled if the WEP encryption is used for accessing a wireless network.

- Step 3** Ensure that the security mode of the WLAN is set to **WPA-PSK** or **WPA2-PSK** and the SSID is set to **SSID1**. Note that the WPS function of the router is forcibly disabled if the WEP encryption is used for accessing a WLAN.
- Step 4** Check the positions of the wireless router and the PCs. Ensure that they are far from electrical appliances, such as a microwave oven, a refrigerator, or a cordless telephone, that generate strong magnetic or electric fields.
- Step 5** It is recommended that you place the router and the PC in an open space. Although radio signals can pass through obstacles, passing through too many obstacles such as cement or wooden walls can affect the transmission of radio signals of a WLAN.

---End

## Q 6: What can I do if I cannot access the Internet through a wireless network adapter?

- Step 1** Check whether the router's WLAN indicator is on.  
If the WLAN indicator is off, the WLAN function of the router is disabled. Log in to the web management page, choose **Basic > WLAN**, and select **Enable WLAN**.
- Step 2** Check that the WLAN function is enabled on the computer. A computer running Windows 7 is used as an example: Right-click **My Computer**, and choose **Manage > Services and Applications > Services**, and check whether **WLAN AutoConfig** is **Started**. If not, right-click **WLAN AutoConfig**, and choose **Start**.



### NOTE

The following procedure describes how to change the parameter settings as required. You can retain the default settings of the parameters that do not need to be changed.

- Step 3** Check that the driver for the wireless network adapter is properly installed and the network adapter is enabled. A computer running Windows 7 is used as an example. Right-click **My Computer**, and choose **Properties > Device Manager > Network adapters** to check the network adapter status.
- If the wireless network adapter driver is installed and the network adapter is enabled, a green icon is displayed next to it.
  - If the wireless network adapter is disabled, a red X is displayed next to it. To enable the network adapter, right-click it and choose **Enable**.
  - If the network adapter driver is not properly installed, a question mark or exclamation mark is displayed. In this case, re-install the network adapter driver.
  - If no network adapter is found, right-click any icon, and choose **Scan for hardware changes**.
- Step 4** Place the router close to the computer, and make sure that there are no obstacles, such as concrete or wooden walls, between them.
- Step 5** Go to the wireless network connection list to check whether the computer is connected to the wireless network set up by the router.
- Step 6** Try to access multiple Web sites to check whether the router can access other Web sites.

If the router cannot access other Web sites, restore the default settings of the router. If the problem persists, contact your network service provider.

----End

---

**Q 7: What can I do if the router cannot access the Internet through a wireless network adapter sometimes or if the WLAN connection is unsteady?**

---

**Step 1** Check the positions of your router and computer. Ensure that they are far from electrical appliances such as microwave ovens, refrigerators, or cordless telephones that generate strong magnetic or electric fields.

**Step 2** Place your router in a vacant area.

Although radio signals can pass through obstacles, the transmission effects of WLAN radio signals are affected if radio signals pass through too many obstacles such as cement or wooden walls.

**Step 3** Place your computer close to your router.

If your computer is far from your router, the transmission effects of the WLAN are affected.

**Step 4** Place your router and computer in another direction.

**Step 5** Do not use your router to access a WLAN during thunderstorms.

----End

---

**Q 8: What can I do if the WLAN of the router is not encrypted and the computer cannot access the WLAN?**

---

**Step 1** Delete the settings of wireless network connections from your computer.

Take a computer that runs Windows XP as an example. To delete the settings of wireless network connections, do as follows:

1. In the **Control Panel** window, double-click **Network Connections** to display the **Network Connections** window.
2. In the **Network Connections** window, right-click **Wireless Network Connection** and choose **Properties**.
3. In the **Wireless Network Connection Properties** dialog box, click the **Wireless Networks** tab.
4. In the **Preferred Networks** group box, select the latest wireless network connection saved on your computer. Then click **Remove**.
5. Delete all the other wireless network connections from the **Preferred Networks** group box.
6. Click **OK**.

**Step 2** Create a wireless network connection that is not encrypted. If your current SSID index is **SSID1**, to create a wireless network connection that is not encrypted, do as follows:

1. Log in to the Web-based configuration utility.

2. In the navigation tree, choose **Basic > WLAN**.
3. Select **SSID1** for **SSID Index**.
4. Select **OPEN** for **Security**.
5. Click **Submit**.

---**End**

# 8 Appendix

## 8.1 Default Settings

Parameter	Default Value
LAN port IP address	192.168.3.1
LAN port subnet mask	255.255.255.0
User name to log in to the web configuration page	admin
Password to log in to the web configuration page	admin
WLAN standards	802.11b, 802.11g and 802.11n (2.4 GHz)
WLAN name	Labeled on the product cover
WLAN password	Labeled on the product cover
Dynamic Host Configuration Protocol (DHCP) server	Enabled
WLAN	Enabled

## 8.2 Technical Specifications

Item	Specifications	
Ambient temperature for operation	0°C to 40°C (32°F to 104°F)	
Dimensions (H × W × D)	About 103 mm × 136 mm × 60 mm	
Weight	< 200g	
Relative humidity for operation	5% to 95% RH (non-condensing)	
WLAN standards	802.11b, 802.11g and 802.11n (2.4 GHz)	
Wireless transmission rates	802.11b	Up to 11 Mbit/s
	802.11g	Up to 54 Mbit/s
	802.11n (with 2T2R antenna used)	Up to 300.0 Mbit/s

# 9 For More Help

---

Please visit [www.huaweidevice.com/worldwide/support/hotline](http://www.huaweidevice.com/worldwide/support/hotline) for recently updated hotline and email address in your country or region.