HUAWEI HG231f Wireless-N Router Wireless-N Router

User Guide

HUAWEI TECHNOLOGIES CO., LTD.

HUAWEI HG231f Wireless-N Router
V100R001

User Guide

Issue	01
Date	2010-04-01
Part Number	202201

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.

Contents

Figures

Tables

About This Document

Purpose

This document describes the functions, features, and configuration methods of the HUAWEI HG231f Wireless-N Router (hereinafter referred to as the router).

By reading this document, you can understand the functions and features of the router and the procedures for installing and configuring the router.

Related Versions

The following table lists the product versions related to this document.

Product Name	Version
HG231f	V100R001

Intended Audience

This document is intended for small office or home office (SOHO) users.

Conventions

Symbol Conventions

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

Symbol	Description
⚠ CAUTION	Indicates a potentially hazardous situation, which if not avoided, could result in equipment damage, data loss, performance degradation, or unexpected results.
☞ TIP	Indicates a tip that may help you solve a problem or save time.
📖 NOTE	Provides additional information to emphasize or supplement important points of the main text.

General Conventions

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

Convention	Description
Times New Roman	Normal paragraphs are in Times New Roman.
Boldface	Names of files, directories, folders, and users are in **boldface**. For example, log in as user **root**.
Italic	Book titles are in *italics*.
Courier New	Examples of information displayed on the screen are in Courier New.

GUI Conventions

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

Convention	Description
Boldface	Buttons, menus, parameters, tabs, windows, and dialog titles are in **boldface**. For example, click **OK**.
>	Multi-level menus are in **boldface** and separated by the ">" signs. For example, choose **File** > **Create** > **Folder**.

Keyboard Operations

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

Format	Description
Key	Press the key. For example, press **Enter** and press **Tab**.
Key 1+**Key 2**	Press the keys concurrently. For example, pressing **Ctrl**+**Alt**+**A** means the three keys should be pressed concurrently.
Key 1, **Key 2**	Press the keys in turn. For example, pressing **Alt**, **A** means the two keys should be pressed in turn.

Mouse Operations

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

Action	Description
Click	Select and release the primary mouse button without moving the pointer.
Double-click	Press the primary mouse button twice continuously and quickly without moving the pointer.

1 Warnings and Precautions

To use the device properly and safely, read these warnings and precautions carefully and strictly observe them during operation. Unless otherwise specified, the term "device" refers to the device and its accessories.

Basic Requirements

- During storage, transportation, and operation of the device, keep it dry and prevent it from colliding with other objects.
- Do not dismantle the device. In case of any fault, contact an authorized service center for assistance or repair.
- Without authorization, no organization or individual can change the mechanical, safety, or performance design of the device.
- When using the device, observe all applicable laws and regulations and respect the legal rights of other people.

Environmental Requirements for Using the Device

- Before connecting and disconnecting cables, stop using the device, and then disconnect it from the power supply. Ensure that your hands are dry during operation.
- Keep the device far from sources of heat and fire, such as a heater or a candle.
- Keep the device far from electronic appliances that generate strong magnetic or electric fields, such as a microwave oven or a refrigerator.
- Place the device on a stable surface.
- Place the device in a cool and well-ventilated indoor area. Do not expose the device to direct sunlight. Use the device in an area with a temperature ranging from 0°C to 40°C.
- Do not block the openings on the device with any object. Reserve a minimum space of 10 cm around the device for heat dissipation.
- Do not place any object (such as a candle or a water container) on the device. If any foreign object or liquid enters the device, stop using the device immediately, power it off, remove all the cables connected to it, and then contact an authorized service center.
- During thunderstorms, power off the device, and then remove all the cables connected to it to prevent it from getting damaged due to lightning strikes.

Precautions for Using Wireless Devices

- When using the device, ensure that the antenna of the device is at least 20 cm away from all persons.
- Do not use the device where using wireless devices is prohibited or may cause interference or danger.
- The radio waves generated by the device may interfere with the operation of electronic medical devices. If you are using any electrical medical device, contact its manufacturer for the restrictions on the use of the device.
- Do not take the device into operating rooms, intensive care units (ICUs), or coronary care units (CCUs).

Areas with Inflammables and Explosives

- Do not use the device where inflammables or explosives are stored, for example, in a gas station, oil depot, or chemical plant. Otherwise, explosions or fires may occur. In addition, follow the instructions indicated in text or symbols.
- Do not store or transport the device in the same box as inflammable liquids, gases, or explosives.

Accessory Requirements

- Use only the accessories supplied or authorized by the device manufacturer. Otherwise, the performance of the device may get affected, the warranty for the device or the laws and regulations related to telecommunications terminals may become null and void, or an injury may occur.
- Do not use the power adapter if its cable is damaged. Otherwise, electric shocks or fires may occur.
- Ensure that the power adapter meets the specifications indicated on the device nameplate.
- Ensure that the power adapter meets the requirements of Clause 2.5 in IEC60950-1/EN60950-1 and it is tested and approved according to national or local standards.

Safety of Children

Keep the device and its accessories out of the reach of children. Otherwise, they may damage the device and its accessories by mistake, or they may swallow the small components of the device, causing suffocation or other dangerous situations.

Maintenance

- If the device is not used for a long time, power it off, and then remove all the cables connected to it.
- If any exception occurs, for example, if the device emits any smoke or unusual sound or smell, stop using the device immediately, power it off, remove all the cables connected to it, and then contact an authorized service center.

- Do not trample, pull, or overbend any cable. Otherwise, the cable may get damaged, causing malfunction of the device.
- Before cleaning the device, stop using it, power it off, and then remove all the cables connected to it.
- Use a clean, soft, and dry cloth to clean the device shell. Do not use any cleaning agent or spray to clean the device shell.

2 Product Overview

2.1 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 150 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
    - 64-bit and 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
- WLAN standards (IEEE 802.11b, 802.11g, and 802.11n) and Ethernet standard (IEEE 802.3u)
- 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
- Routing Information Protocol (RIP) version 1, RIP version 2, and Static Routing Protocol
- IP quality of service (QoS)

- Traffic control through which you can manage the downloading rate of peer-to-peer (P2P) software
- Local and remote configuration through a Web-based configuration utility

2.2 Hardware

2.2.1 Interfaces and Buttons

Table 2-1 describes the interfaces and buttons of the router.

Table 2-1 Interfaces and buttons of the router

Interface or Button	Description
POWER	Interface used to connect the power adapter to the router. **NOTE** To power on the router, connect the power adapter to the POWER interface of the router and then to a power socket. Then supply the power socket with electricity.
RESET	To restore the factory settings of the router, power on the router, press and hold the RESET button for at least 3s, and then release the button. **NOTE** When the factory settings are restored, your custom data is lost. Therefore, use the RESET button with caution.
LAN1–LAN4	Ethernet interfaces used to connect Ethernet devices, such as PCs and switches, to the router.
WAN	Ethernet interface used to connect Ethernet devices that provide Internet access interfaces, such as modems and switches.
WPS	Button used to enable the WPS function.

📖 **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.

2.2.2 Indicators

Table 2-2 describes the indicators of the router.

Table 2-2 Indicators of the router

Indicator	Color	Status	Indicates
POWER	White	On	The router is powered on.
	-	Off	The router is powered off.
INTERNET	White	Blinking	A connection is set up between the Internet and the WAN interface of the router and data is being transmitted on the WAN interface.
	White	On	A connection is set up between the Internet and the WAN interface of the router, but no data is being transmitted on the WAN interface.
	Orange	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 the router is not connected to the Internet.
	-	Off	No network cable is connected to the WAN interface of the router, or the router is powered off.
WLAN	White	Blinking	The WLAN function is enabled and data is being transmitted on the WLAN.
	White	On	The WLAN function is enabled, but no data is being transmitted on the WLAN.
	-	Off	The WLAN function is disabled.
WPS	White	Blinking	The router is attempting to set up a wireless connection with a wireless client (such as a PC on which a wireless network adapter is installed) through the WPS function. **NOTE** This state lasts no more than two minutes.
	White	On	A wireless connection is set up between the router and a wireless client through the WPS function. **NOTE** This state lasts 300s.
	-	Off	The WPS function is disabled.

Indicator	Color	Status	Indicates
LAN1–LAN4	White	Blinking	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 and data is being transmitted.
	White	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, but no 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 PC).
NOTE ADSL = asymmetrical digital subscriber line			

3 Hardware Installation

3.1 Selecting a Position for the Router

Place the router in a stable and well-ventilated place and do not expose it to direct sunlight, as described in chapter 1 "Warnings and Precaution." 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.

3.2 Knowing Cable Connections

Figure 3-1 shows the cable connections between the router and other devices.

Figure 3-1 Cable connections between the router and other devices
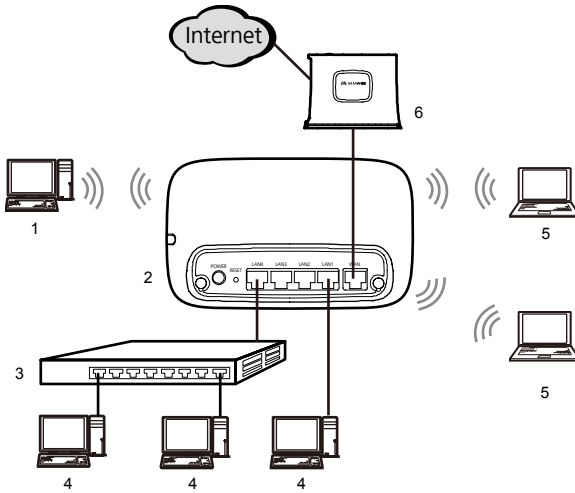
1. Desktop computer installed with a wireless network adapter   2. Router
3. Switch   4. PC
5. Laptop installed with a wireless network adapter   6. ADSL modem

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.

3.3 Powering On the Router

To power on the router, connect the power adapter to the POWER interface of the router and then to a power socket. Then supply the power socket with electricity. If the router works properly, the indicators on the front panel turn on. Table 3-1 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 3-1. For details about the indicators of the router, see Table 2-2.

Table 3-1 Indicators that turn on after the router is powered on

Indicator	Color	Status	Indicates
POWER	White	On	The router is powered on.

Indicator	Color	Status	Indicates
INTERNET	White	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.
	Orange	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. **NOTE** In this case, you need to configure the router as described in chapter 4 "Configuration of Internet Access Parameters."
WLAN	White	On	The WLAN function is enabled.
LAN1–LAN4	White	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.

3.4 Installing the Router on an ADSL Broadband Network

Figure 3-2 shows the cable connections of an ADSL broadband network before the router is installed on the network. On this 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 3-2 Cable connections of an ADSL broadband network before the router is installed on the network
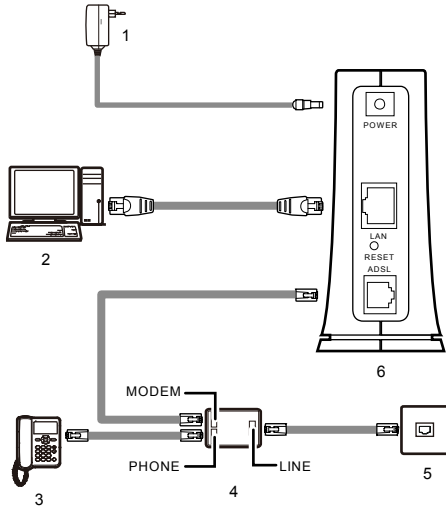
1. Power adapter of the ADSL modem   2. PC
3. Telephone   4. Splitter
5. Telephone line interface on the wall   6. ADSL modem

NOTE

Figure 3-2 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 3-2.

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

Figure 3-3 Cable connections of an ADSL broadband network after the router is installed on the network
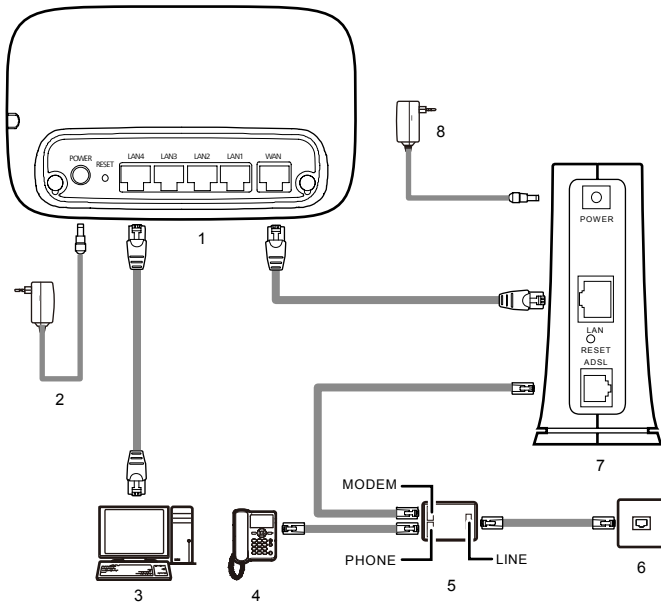
1. Router
3. PC
5. Splitter
7. ADSL modem

2. Power adapter of the router
4. Telephone
6. Telephone line interface on the wall
8. Power adapter of the ADSL modem

To install the router on an ADSL broadband network, do as follows:

Step 1   Connect the ADSL modem as described in its user guide.

Step 2   Use a network cable to connect the WAN interface of the router to the Ethernet interface of the ADSL modem.

Step 3   Use a network cable to connect any of the four LAN interfaces of the router to the Ethernet interface of a PC.

Step 4   Use the power adapter of the router to connect the POWER interface of the router to a power socket.

   ----End

3.5 Installing the Router on a CATV Broadband Network

Figure 3-4 shows the cable connections of a cable television (CATV) broadband network before the router is installed on the network. On this 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 3-4 Cable connections of a CATV broadband network before the router is installed on the network
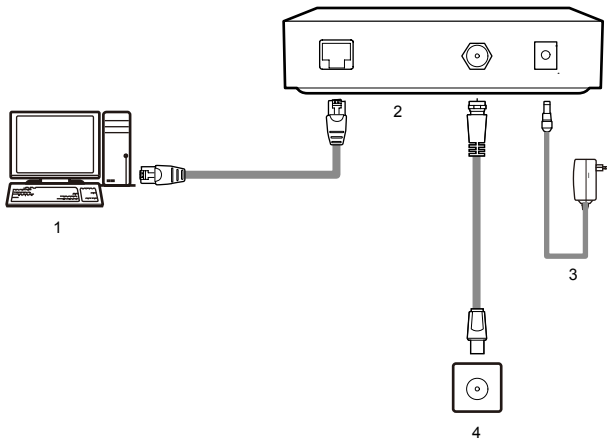
1. PC
2. Cable modem
3. Power adapter of the cable modem
4. CATV network interface on the wall

📖 NOTE

Cable modems provided by different manufacturers might vary in appearance and interface layout. The cable modem in Figure 3-4 is for your reference only.

Figure 3-5 shows the cable connections of a CATV broadband network after the router is installed on the network.

Figure 3-5 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
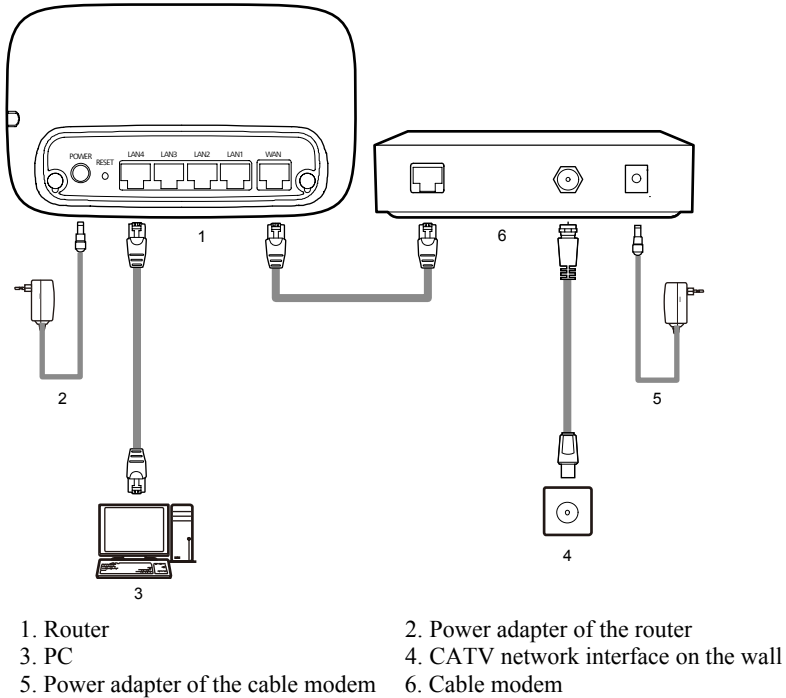
3.6 Installing the Router on a Community Broadband Network

In some communities, network service providers use Ethernet interfaces as Internet interfaces. In such a community, you can access the Internet through your PC if a network adapter is installed on the PC. Figure 3-6 shows the cable connection of a community broadband network before the router is installed on the network. On this network, your PC is directly connected to the Internet through the Ethernet interface provided by the network service provider.

Figure 3-6 Cable connection of a community broadband network before the router is installed on the network
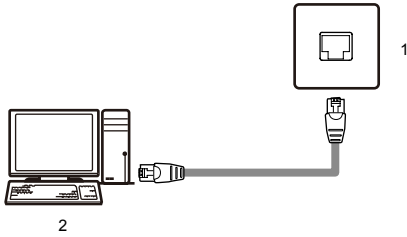
1. Community broadband network interface on the wall (Ethernet interface)
2. PC

Figure 3-7 shows the cable connections of a community broadband network after the router is installed on the network.

Figure 3-7 Cable connections of a community broadband network after the router is installed on the network
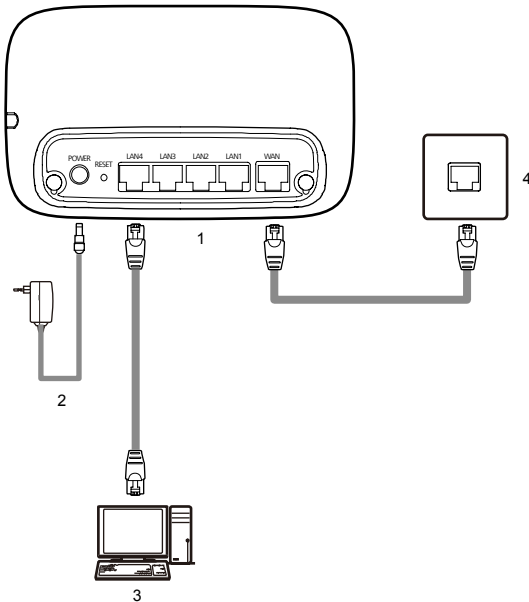
1. Router	2. Power adapter of the router
3. PC	4. Community broadband network interface on the wall (Ethernet interface)

4 Configuration of Internet Access Parameters

4.1 Logging In to the Web-Based Configuration Utility

The router provides an easy-to-use Web-based configuration utility. You can view and set the parameters of the router through this utility.

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

Step 1 Set the network connection of your PC and ensure that your PC obtains an IP address automatically.

○⊸ **TIP**

By default, the DHCP function of the router is enabled. In this case, the router assigns an IP address to your PC automatically and you do not need to configure the IP address of your PC.

Step 2 Start the Internet Explorer on your PC and ensure that the Internet Explorer does not use any proxy server.

Take the Internet Explorer 6.0 as an example. To ensure that the Internet Explorer does not use any proxy server, do as follows:

1. Start the Internet Explorer. Choose **Tools** > **Internet Options**.
2. On the **Connect** tab of the **Internet Options** dialog box, click **LAN Settings**.
3. In the **Proxy Server** area, ensure that **Use the proxy server for LAN** is cleared. If **Use the proxy server for LAN** is selected, clear **Use the proxy server for LAN**, and then click **OK**.

Step 3 In the address bar of the Internet Explorer, enter **hg231f.com**, and then press **Enter**.

Step 4 In the **Login** dialog box, enter the administrator account (**admin** by default) and the password (**admin** by default), and then click **OK**.

    ----End

📖 **NOTE**

You can use **hg231f.com** to access the Web-based configuration utility only when the IP address of your PC is dynamically assigned by the router. If you cannot access the utility by using **hg213f.com**, you can enter the IP address of the LAN interface of the router (**192.168.1.100** by default) to access the utility.

4.2 Using the Setup Wizard

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

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

☞ **TIP**

If you have configured the router before, you will not see the setup wizard page after logging in to the Web-based configuration utility. In this case, you can click **Installation** in the upper right corner to display the setup wizard page.

Step 1 Check the connections between your PC and the router and between the router and the network access device (such as an ADSL modem) as prompted, ensure that these connections are proper, and then click **Next**.

📖 **NOTE**

If a message is displayed, indicating that the connection between your PC and the router or between the router and the network access device (such as an ADSL modem) is improper, you need to check the cable connections as described in chapter 3 "Hardware Installation" and ensure that the hardware are properly installed and that all the connected devices are powered on.

Step 2 Set **Connection Type** based on your network type, set the other parameters corresponding to this type, and then click **Next**.

Step 3 Set WLAN parameters, and then click **Next**.

Step 4 Click **Submit**.

----End

5 Configuration of WLAN Parameters

5.1 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 PC and the router quickly. To set up a wireless connection, do as follows:

Step 1 Set the WLAN parameters of router, and then set the **Security Mode** to **WPA-PSK**, **WPA2-PSK** or **WPA-PSK/WPA2-PSK** as prompted. For details, see chapter 4 "Configuration of Internet Access Parameters."

> 📖 **NOTE**
>
> The WPS function can be used only when the security mode of the WLAN is set to WPA-PSK, WPA2-PSK, or WPA-PSK/WPA2-PSK.

Step 2 Press the WPS button of the router to enable the router to enter the WPS negotiation state.

The WPS indicator of the router blinks. If the WPS indicator does not blink, it indicates that the WPS function cannot be enabled. For the solutions to other WPS problems, see chapter 8 "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.

5.2 Setting Up a Wireless Connection Through the AP PIN Mode

The router supports the AP PIN mode of the WPS function. If your network adapter also supports the AP PIN mode of the WPS function; you can use the AP PIN mode to set up

a wireless connection between your PC and the router quickly. To set up a wireless connection, do as follows:

Step 1 Set the WLAN parameters of router, and set the **WPS mode** to **AP PIN**.

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

To log in to the Web-based configuration utility, see section 4.1 "Logging In to the Web-Based Configuration Utility".

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

3. Set the following parameters as planned.

   − SSID: MyNewSSID

   − Security Mode: WPA-PSK/WPA2-PSK

   − WPA Pre-Shared Key: MyPassword@2009

   − WPA Encryption: AES

   − WPS Mode: AP PIN

4. Click **Reset PIN**.

5. Click **Submit**.

Step 2 Record the WPS PIN in the **AP PIN** text box.

Step 3 Detect a WLAN through the configuration software of the wireless network adapter.

Step 4 In the Wireless Network Adapter's software configuration utility, select **MyNewSSID** from the WLAN list.

Step 5 Enter the WPS PIN in the Wireless Network Adapter's software configuration utility.

Step 6 Click the corresponding connection as prompted.

---End

©⚷ **TIP**

● After finishing the configuration, if the other PCs need to set a wireless connection through the AP PIN mode, please repeat Step 3 to Step 6.

● Click **Reset PIN**, the WPS PIN are restored to the default settings. You can check the label on the back panel of the router for the default WPS PIN.

● Click **Generate PIN**, the router will generate a new WPS PIN randomly.

5.3 Setting Up a Wireless Connection Manually

If your network adapter does not support the WPS function, you can set up a wireless connection between your PC and the router manually. 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.

If your PC runs on Windows XP, you can use the wireless configuration software that is provided by Windows XP to set up a wireless connection between your PC and the router.

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

To set up a wireless connection between your PC and the router manually, do as follows:

Step 1 Set the WLAN parameters of router, and set the Security Mode to WPA-PSK, WPA2-PSK or WPA-PSK/WPA2-PSK. You can set the WLAN parameters through the Web-based configuration utility. For details, see chapter 4 "Configuration of Internet Access Parameters."

Step 2 Enable the wireless configuration service provided by Windows XP.

1. Right-click **My Computer**, and then choose **Manage** from the shortcut menu.

2. In the **Computer Management** window, choose **Computer Management (Local)** > **Services and Applications** >**Services**.

3. From the services listed in the right pane of the **Computer Management** window, right-click **Wireless Zero Configuration**, and then choose **Properties** from the shortcut menu.

4. In the **Wireless Zero Configuration Properties (Local Computer)** dialog box, check whether **Service status** is **Started**. If not, click **Start**.

5. Click **OK** to close the dialog box, and then close the **Computer Management** window.

Step 3 Configure the wireless network connection on your computer.

1. Choose **Start** > **All Programs** > **Accessories** > **Communications** > **Network Connections**.

2. In the **Network Connections** window, right-click **Wireless Network Connection**, and then choose **Properties** from the shortcut menu.

3. In the **Wireless Network Connection Properties** dialog box, select **Wireless Networks**.

4. Select **Use Windows to configure my wireless network settings**.

5. Click **View Wireless Networks**.

6. In the **Wireless Network Connection** dialog box, select the WLAN with the same name as the WLAN name that you have recorded from the WLAN list, and then click **Connect** in the lower right corner of the dialog box.

7. In the displayed dialog box, enter the WLAN access password that you have recorded, and then click **Connect**.

After the password is authenticated, Connected is displayed in the upper right corner of the WLAN icon in the WLAN list, indicating that a wireless connection is set up between you PC and the router.

8. Close the **Wireless Network Connection** dialog box.

9. In the **Wireless Network Connection Properties** dialog box, click **OK**.

----End

⊙—⌐ **TIP**

After finishing the configuration, if the other PCs need to setting up a wireless connection manually, please repeat Step 3.

6 Configuring Frequently Used Functions

6.1 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 3 "Hardware Installation."

Step 2   Connect the laptop to the router wirelessly by configuring the laptop.

For details, see chapter 5 "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 4 "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 6.8 "Removing the Restriction Caused by the Binding of the Internet Access Account to the MAC Address."

6.2 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 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 Clear **Enable WLAN**, and then click **Submit**.

----End

◎━ TIP

To enable the WLAN function, select **Enable WLAN**, and then click **Submit**.

6.3 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.

6.3.1 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**.**

You can disable the SSIDs that are not required. After an SSID is disabled, a wireless client cannot connect to the WLAN that is indicated by this SSID. Note that all the external connection channels of a WLAN are closed if all the SSIDs of the WLAN are disabled. To use the WLAN, you need to enable the WLAN function and at least one SSID. In addition, to use the WPS function, you should enable **SSID1**.

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 **Enable SSID** to **Enable**.

Step 5 Set **Hide Broadcast** to **Enable**, and then click **Submit**.

Step 6 Select **SSID2** for **SSID Index**.

Step 7 Clear **Enable** for **Enable SSID**. Then click **Submit**.

Step 8 Repeat Step 6 and Step 7 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.

6.3.2 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**.

    ----End

6.3.3 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 6-1 lists the rules for setting the password used for accessing a WLAN in different security modes.

Table 6-1 Rules for setting the password used for accessing a WLAN

Security Mode	Password Setting Rule
WEP encryption	• 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. • 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.
WPA-PSK or WPA2-PSK	The password consists of 8–63 visible ASCII characters entered through a keyboard or 64 hexadecimal characters.

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@2009**.

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@2009**.

Step 5 Select **AES** for **WPA Encryption**.

Step 6 Click **Submit**.

----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.

6.3.4 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 6.4 "Controlling the Internet Access Rights of PCs" controls the option of allowing a PC connected to the router to access the Internet.

TIP

You can set the maximum number of the devices that are allowed to be connected to a WLAN, thus increasing the security of the WLAN. This maximum number ranges from 1 to 32. For example, you have only one laptop that needs to be connected to the WLAN. You can set this maximum number to **1**. After your laptop is connected to the WLAN, other PCs cannot be connected to the WLAN.

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 ⊞.

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

6.4 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:

- Blacklist: The PCs whose MAC addresses are listed in the filtering list are prohibited from accessing the Internet.
- Whitelist: The PCs whose MAC addresses are listed in the filtering list are allowed to access the Internet.

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

📖 **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 blacklist mode of 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 **Internet access is prohibited before 19:00 in the evening**.
- 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 **Internet access is prohibited after 20:00 in the evening**.

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**.

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

The parent control page is displayed.

Step 8 Click **MAC Filter**.

Step 9 Select **Blacklist**.

Step 10 Click ⊞.

Step 11 Set **Time control** to **Enable**.

Step 12 Set the following parameters based on rule 1.

- Rule name: Internet access is prohibited before 19:00 in the evening
- Source MAC address: 00:11:09:11:04:DD
- Start time: 00:00
- End time: 18:59
- Effective day: Select from Monday to Sunday.

Step 13 Click **Submit**.

Step 14 Click ⊞.

Step 15 Set **Time control** to **Enable**.

Step 16 Set the following parameters based on rule 2.

- Rule name: Internet access is prohibited after 20:00 in the evening
- Source MAC address: 00:11:09:11:04:DD
- Start time: 19:59
- End time: 23:59

● Effective day: Select from Monday to Sunday.

Step 17 Click **Submit**.

----End

◎━⊸ **TIP**

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

6.5 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.

The URL filtering function can be implemented in the following modes:

● Blacklist: Users cannot access the Web sites in the filtering rule list.
● Whitelist: Users can access only the Web sites in the filtering rule list.

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

Configuration Example

For example, the contents of the Web site whose address is **www.yyy.com** are not suitable for browsing. To prevent your family from browsing this Web site, you can use the URL filtering function and create a blacklist 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** > **Parent Control**.

The parent control page is displayed.

Step 3 Click **URL Filter**.

Step 4 Select **Blacklist**.

Step 5 Click [+].

Step 6 In **URL**, enter **www.yyy.com**.

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 ▭ .

6.6 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

You can configure a maximum of eight bandwidth control rules for eight PCs. The eight PCs can be connected to the router through a wired Ethernet network or a WLAN.

📖 NOTE

Each PC can be configured with only one bandwidth control rule.

A bandwidth control rule distinguishes different PCs based on the IP addresses of the PCs. It is recommended that you configure your PC to obtain an IP address from the router automatically. After the IP address of your PC is obtained, you can configure the bandwidth control rule based on this IP address. The router can record the mapping between the MAC address and IP address of a PC and thus ensure that the same IP address can be assigned to the same PC every time.

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**. To ensure a fast data transmission rate and smooth video quality, you can use the traffic control function of the router and configure a bandwidth control rule for the PC named **myPC**. The parameters of the rule are as follows:

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

The configuration procedure is as follows:

Step 1 Connect the PC named **myPC** to the router through a wired network or a WLAN.

Ensure that the PC can access the Internet.

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

Step 3 In the navigation tree, choose **Advanced** > **IP QoS**.

Step 4 Click **Enable P2P Traffic Management** check box.

The configuration page for the traffic control function is displayed.

Step 5 Under **LAN Host**, click the PC icon indicated by **myPC**.

Step 6 In the displayed dialog box, set the following parameters:
- Mode: Assure Minimum Bandwidth
- Download: 500 kbit/s
- Upload: 500 kbit/s

Step 7 Click **Apply**.

----End

⊙━ TIP

- To restrict the available bandwidth of a PC, select **Restrict Maximum Bandwidth** for **Mode**.
- To configure more than four rules, you can perform adding, deleting, and editing operations in the **Bandwidth** list in the lower area of the page.

6.7 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.

The firewall of the router provides multiple preset protective levels. Thus, you can configure the firewall quickly as required. Table 6-2 lists the preset protective levels and their protective effects.

Table 6-2 Protective effects of the preset protective levels of the firewall

Operation	Protective Effects Corresponding to the Preset Protective Levels of the Firewall					
	Block-All	High	Medium	Standard	Low	Disable
The user of a PC on a LAN configures the router by using the Web-based configuration utility.	√	√	√	√	√	√

Operation	Protective Effects Corresponding to the Preset Protective Levels of the Firewall					
	Block-All	High	Medium	Standard	Low	Disable
The user of a PC on a LAN browses Web pages.	×	√	√	√	√	√
The user of a PC on a LAN downloads files from an FTP server.	×	√	√	√	√	√
The user of a PC on a LAN accesses the shared folder of another PC in a different network segment through the router.	×	×	√	√	√	√
The user of a PC on a LAN performs other accessing operations on the Internet.	×	×	×	√	√	√
An Internet user runs the ping command to test the connectivity between the PC and your router.	×	×	×	×	√	√

Operation	Protective Effects Corresponding to the Preset Protective Levels of the Firewall					
	Block-All	**High**	**Medium**	**Standard**	**Low**	**Disable**
An Internet user performs other accessing operations on your router.	×	×	×	×	×	√
NOTE ● A tick (√) indicates that the firewall at this level allows the operation. ● A cross (×) indicates that the firewall at this level prohibits the operation. ● FTP = File Transfer Protocol						

When the router is delivered, the level of the firewall is set to **Standard**. Normally, it is recommended that you set the level of the firewall to **Standard**. Thus, the network security can be ensured and most requirements for using the network can be met.

If you have special requirements for using the network, you can set the protective level as required or define more firewall rules.

Configuration Example

For example, you have stringent requirements on network security. To allow the PCs on a LAN to only browse Web pages and prohibit Internet users from accessing the router, you can set the firewall level of the router to **High** 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 Select **High** for **Firewall level**.

Step 4 Click **Submit**.

----End

◎⌐ TIP

You cannot modify a predefined firewall level. To define a firewall level, select **Custom** for **Firewall level**. Then set the level name and protective rules.

6.8 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.

Figure 6-1 shows the network connection of the devices.

Figure 6-1 MAC address cloning

3. PC 1   4. PC 2   5. PC n
6. Laptop
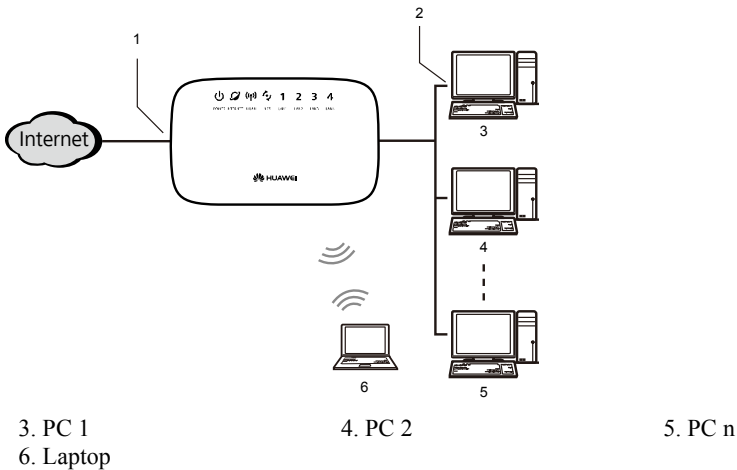
⊙━ **TIP**

- 1. Through the MAC address cloning function, the router has the same MAC address as that of PC 1 and this MAC address can be used for accessing the Internet.

- 2. The MAC address of PC 1 can be used for accessing the Internet.

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

6.9 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 **192.168.1.100**.
- The IP address of the Web server is **192.168.1.166**.

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. Suppose you apply for the DDNS to China Telecom. China Telecom provides you with the DDNS user name, namely **yourDDNSUserName** and the DDNS password, namely **yourDDNSPassword**.

- Apply for a domain name for the Web site to the institution for managing the domain names of Web sites. Suppose you have applied for the domain name, namely **bbs.myweb.com**.

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 (**192.168.1.166:80**) 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 ⊞.

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 port: 80
- External end port: 80
- Internal host: 192.168.1.166
- Internal port: 80

Step 7 Click **Submit**.

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

The DDNS configuration page is displayed.

Step 9 Select **China Telecom** 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 10 Set the following parameters as planned.

- Host: bbs
- Domain: myweb.com
- User name: yourDDNSUserName

- Password: yourDDNSPassword
- Server port: 80

Step 11 Click **Submit**.

----End

NOTE

Host and **Domain** constitute a complete Web site address.

6.10 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 6-3 lists three WDS working modes, functions in each working mode, and relevant setting requirements.

Table 6-3 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 **192.168.1.100** (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@2009**.
- 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 **192.168.1.101**.
- 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@2009**.
- 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.

1. Log in to the Web-based configuration utility of a router.
2. In the navigation tree, choose **Status** > **Device Information** > **WLAN**.
   The WLAN status page is displayed.
3. Record the value of **Wireless MAC**.
   The value of Wireless MAC is a character string that is similar to **00-11-09-11-04-DD**. This value is the wireless MAC address of the router. 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. Set the following parameters.
   - Country Code: 1
   - SSID Index: SSID1
   - SSID: mySSID
   - Enable SSID: Enable
   - Security Mode: WPA-PSK/WPA2-PSK
   - WPA Encryption: AES
   - WPA Pre-Shared Key: MyPassword@2009
4. Click **Submit**.

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 ![+].

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. Set the following parameters.

   - Country Code: 1

   - SSID Index: SSID1

   - SSID: mySSID

   - Enable SSID: Enable

   - Security Mode: WPA-PSK/WPA2-PSK

   - WPA Encryption: AES

   - WPA Pre-Shared Key: MyPassword@2009

4. Click **Submit**.

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 ![+].

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. Under **LAN Host Settings**, enter **192.168.1.101** in **IP address**.

3. 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. Under **DHCP Server**, clear **Enable**.
3. Under **DHCP Server**, click **Submit**.

Step 8   Enable the DHCP relay function of router B.

1. In the navigation tree, choose **Advanced** > **Link Interface**.
   The link interface configuration page is displayed.
2. Click **Port Relay**.
3. Click [+].
4. Select **LAN1** for **LAN port**.
5. Set **DHCP relay** to **Enable**.
6. Click **Submit**.
7. Repeat 3 to 6 to enable the DHCP relay function for each port in the **LAN port** drop-down list box.

----End

7 Maintenance Guide

7.1 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 3s. 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**.

----End

7.2 Changing the Login IP Address of the Web-based Configuration Utility

Function Overview

You can access the Web-based configuration utility by using either of the following methods:

1. By accessing **hg231f.com**. This method can be used only when your IP address is assigned dynamically by the router.
2. By accessing the IP address of the LAN interface of the router **192.168.1.100** (the subnet mask is **255.255.255.0**).

The IP address is used by the router to communicate with your PC on the current network.

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 **192.168.1.100** and the subnet mask is **255.255.255.0**. To change the IP address to **192.168.1.88** (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 In **IP address** under the **LAN Host Settings** group box, enter the new IP address **192.168.1.88** in **IP address**.

Step 4 Under **LAN Host Settings**, click **Submit**.

----End

7.3 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**.

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 On the **Configuration File** tab, click **Browse**.

Step 4 In the displayed dialog box, select the backup configuration file. Then click **OK**.

Step 5 Click **Upload Configuration File**.

  ----End

7.4 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 3s, 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 On the **Reset** tab, click **Restore Default Settings**.

  ----End

7.5 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://www.huaweidevice.com.

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 On the **Firmware Upgrade** tab, click **Browse**.

Step 4 In the displayed dialog box, select the upgrade file. Then click **OK**.

Step 5 Click **Software Upgrade**.

  ----End

8 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 the IP address of your computer and ensure that this IP address is in the same network segment as the LAN IP address of the router.

Step 2 Ensure that your Web browser does not use a proxy server.

Step 3 Ensure that you have entered the correct user name and user password that are used for accessing the router configuration page.

If the problem persists, restore the default settings of the router.

----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 Ensure that the power cables and telephone lines of the router are properly connected.

Step 2 Check whether the WLAN indicator of the router is on.

If the WLAN indicator is off, you can infer that the wireless local area network (WLAN) function of the router is disabled. In this case, enable the WLAN function.

For details about how to enable the WLAN function, see the manual of the router.

Step 3 See the description of the wireless network adapter that is installed on the computer and check whether the wireless network adapter supports the 802.11b and 802.11g protocols.

If the wireless network adapter does not support the 802.11b and 802.11g protocols, replace it with the network adapter that supports the protocols.

Step 4 Check whether the driver for the wireless network adapter is properly installed on the computer.

If the driver is improperly installed, install it properly.

Step 5 Check whether the computer can receive the signals of a WLAN.

Take a computer that runs Windows XP as an example. To check whether the computer can receive the signals of a WLAN, 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 **View Available Wireless Network**.

If the computer cannot detect a WLAN, place the computer close to the router and ensure that no obstacles such as cement or wooden walls are present between the wireless client and the router.

Step 6 Check whether the computer accesses the WLAN of the router successfully.

Check the list of wireless network connections and ensure that the router is connected to the WLAN.

Step 7 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.

----End

A Technical Specifications

Item	Specification	
Dimensions (L × W × H)	144 mm × 31 mm × 88 mm	
Weight (including the router support)	About 145 g	
Entire-device power consumption	< 5 W	
Entire-device power supply	12 V DC, 0.5 A	
Ambient temperature for operation	0℃ to 40℃ (32℉ to 104℉)	
Relative humidity for operation	5% to 95%, non-condensing	
WLAN standards	802.11b, 802.11g, and 802.11n (2.4 GHz)	
Wireless transmission rates	802.11b	1 Mbit/s, 2 Mbit/s, 5.5 Mbit/s, and 11 Mbit/s
	802.11g	6 Mbit/s, 9 Mbit/s, 12 Mbit/s, 18 Mbit/s, 24 Mbit/s, 36 Mbit/s, 48 Mbit/s, and 54 Mbit/s
	802.11n (a 1T × 1R antenna used)	6 Mbit/s, 6.5 Mbit/s, 13.0 Mbit/s, 13.5 Mbit/s, 19.5 Mbit/s, 26.0 Mbit/s, 27.0 Mbit/s, 39.0 Mbit/s, 40.5 Mbit/s, 52.0 Mbit/s, 54.0 Mbit/s, 58.5 Mbit/s, 65.0 Mbit/s, 81.0 Mbit/s, 104.0 Mbit/s, 108.0 Mbit/s, 121.5 Mbit/s, 135.0 Mbit/s, and 150.0 Mbit/s

B Default Settings

Parameter	Default Value
IP address of the LAN interface	192.168.1.100
Subnet mask of the LAN interface	255.255.255.0
Administrator name	admin
Administrator password	admin
DHCP server	Enabled
WLAN	Enabled

C Acronyms or Abbreviations

A

ADSL   Asymmetrical Digital Subscriber Line

ASCII   American Standard Code for Information Interchange

D

DHCP   Dynamic Host Configuration Protocol

DDNS   Dynamic Domain Name Service

DNS   Domain Name Server

DSL   Digital Subscriber Line

F

FTP   File Transfer Protocol

H

HTTP   Hyper Text Transport Protocol

I

IEEE   Institute for Electrical and Electronics Engineers

IP   Internet Protocol

L

LAN   Local Area Network

M

MAC   Media Access Control

N

NAT   Network Address Translation

P

PPPoE   Point to Point Protocol over Ethernet

Q

QoS   Quality of Service

R

RIP   Routing Information Protocol

S

SSID   Service Set Identifier

W

WAN   Wide Area Network

WDS   Wireless Distribution System

WLAN   Wireless Local Area Network

WEP   Wired Equivalent Privacy

WPA   Wi-Fi Protected Access

WPS   Wi-Fi Protected Setup