Contents

Figures

Tables

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

- The antenna(s) used for this transmitter must be installed to provide a separation distance of at least 20 cm 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 HUAWEI HG256s home gateway (hereinafter referred to as the HG256s) provides a user-friendly GUI, complemented by a fresh and unique appearance. On the network side, it provides a high-speed Gigabit Ethernet (GE) interface for wide area network (WAN) access. On the user side, it supports the wireless local area network (WLAN) function and provides four GE 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.

2.2 Hardware

2.2.1 Interfaces and Buttons

Table 2-1 describes the interfaces and buttons of the HG256s.

Table 2-1 Interfaces and buttons of the HG256s

Interface or Button	Description
POWER	Interface used to connect the power adapter to the HG256s.
RESET	To restore the factory settings of the HG256s, power on the HG256s, 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, to the HG256s.
PHONE1, PHONE2	It is used to connect the phone to the HG256s.
WAN	Ethernet interface used to connect Ethernet devices that provide Internet access interfaces.
WPS	Button used to enable the WPS function.
WLAN	It is used to enable or disable the WLAN function.
ON/OFF	It is used to power on or off the HG256s.

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 HG256s.

Table 2-2 Indicators of the HG256s

Indicator	Color	Status	Indicates
POWER	Green	On	The HG256s is powered on.
	-	Off	The HG256s is powered off.
INTERNET	Green	On	A connection is set up between the Internet and the WAN interface of the HG256s, but no data is being transmitted on the WAN interface.
	Red	On	A physical connection is set up, but the HG256s is not connected to the Internet.
	-	Off	No network cable is connected to the WAN interface, or the HG256s is powered off.
WLAN	Green	Blinking	The WLAN function is enabled and data is being transmitted on the WLAN.
	Green	On	The WLAN function is enabled, but no data is being transmitted on the WLAN.
	-	Off	The WLAN function is disabled.
VOIP1, VOIP2	Green	On	The HG256s is successfully registered with the SIP server.
	Green	Blinking	The corresponding phone is picked up.
	-	Off	The HG256s is powered off or fails to be registered with the SIP server.

Indicator	Color	Status	Indicates
LAN1, LAN2, LAN3, LAN4	Green	Blinking	A connection is set up between the corresponding LAN interface of the HG256s and an Ethernet device (such as a PC) through a network cable and data is being transmitted.
	Green	On	A connection is set up between the corresponding LAN interface of the HG256s 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 HG256s and an Ethernet device (such as a PC).
USB	Green	Blinking	The USB connection is successfully established and data is being transmitted.
	Green	On	The USB connection is successfully established but no data is being transmitted.
	-	Off	The HG256s is powered off or the USB connection is not yet established.

3 Hardware Installation and Quick Start

3.1 Selecting a Position for the HG256s

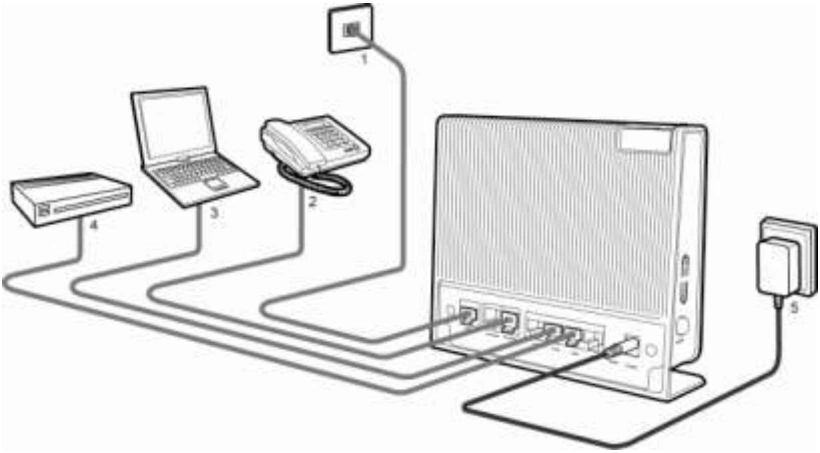
Place the HG256s in a stable and well-ventilated place and do not expose it to direct sunlight, as described in chapter 1 "Warnings and Precaution." If you want to use the WLAN function of the HG256s, you also need to pay attention to the following precautions for a better performance of the WLAN:

- Place the HG256s in an open space and ensure that no obstacle, such as a cement or wooden wall, exists between your PC and the HG256s. Otherwise, the transmission of radio signals on the WLAN is affected.
- Ensure that the HG256s 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.

Figure 3-1 Cable connections



1	Network jack on the wall	2	Phone	3	PC
4	Set-top box	5	Power adapter		

3.3 Powering On the HG256s

To power on the HG256s, finish the cable connections and press the **ON/OFF** button on the side panel of the HG256s. After you power on the HG256s, if the HG256s works properly, the indicators on the front panel turn on. HG256s works properly according to the descriptions in Table 2-2.

3.4 Logging In to the Web-Based Configuration Utility

The HG256s provides an easy-to-use Web-based configuration utility. You can view and set the parameters of the HG256s 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 HG256s is enabled. In this case, the HG256s 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 **http://192.168.1.1**, and then press **Enter**.

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

----End

4 Configuration of WLAN Parameters

4.1 Setting the WLAN Parameters of the Router

The HG256s provides the WLAN function. If a wireless network adapter is installed on your PC, you can connect your PC to the HG256s in the wireless manner.

The WLAN parameters of the HG256s are preset before delivery. Therefore, you can use the settings directly. If you want to change the WLAN settings, see section 6.2 "Improving the Security of a WLAN".

4.2 Setting Up a Wireless Connection Manually

You can set up a wireless connection between your PC and the HG256s 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 Zero Configuration that is provided by Windows XP to set up a wireless connection between your PC and the HG256s.

Takes Windows XP as an example, to set up a wireless connection between your PC and the HG256s manually, do as follows:

Step 1 Record the WLAN name.

TIP

The WLAN name (**SSID**) of the HG256s is preset before delivery. You can find it from the label on the rear panel of the HG256s.

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.

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 HG256s.

7. Close the **Wireless Network Connection** dialog box.
8. In the **Wireless Network Connection Properties** dialog box, click **OK**.

----End

4.3 Setting Up a Wireless Connection by the WPS Button

The HG256s 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 HG256s quickly. To set up a wireless connection, do as follows:

Step 1 Set the WLAN parameters of HG256s, and then set the **Security Mode** to **WPA-PSK**, **WPA2-PSK** or **WPA-PSK/WPA2-PSK** as prompted. For details, see section 6.2.3 "Using Secure Encryption".

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 HG256s to enable the HG256s to enter the WPS negotiation state.

The WLAN indicator of the HG256s blinks. If the WLAN 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).

The WLAN indicator of the HG256s becomes on from the blinking state, indicating that the HG256s is connected to your PC through the WLAN.

----End

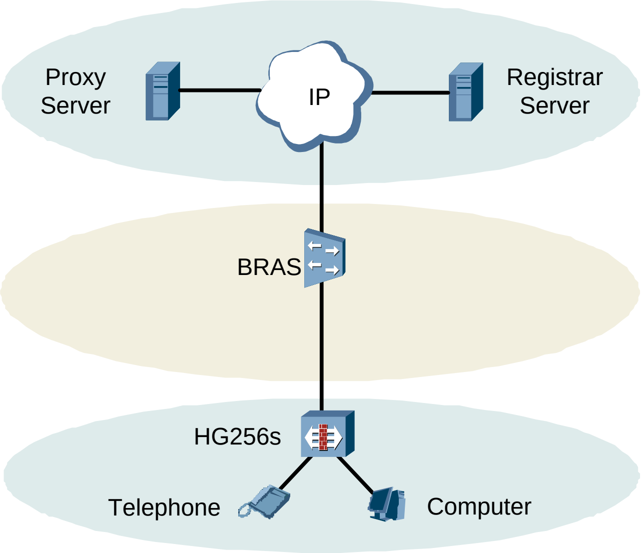
5 Configuration of VoIP

The HG256s supports voice services based on the Session Initiation Protocol (SIP).

The SIP is an application layer protocol used to create, modify, or end multimedia sessions.

5.1 Networking

Figure 5-1 Network model of voice services



Equipment	Description
Proxy Server	A server that forwards requests or responses in place of the client
Registrar Server	A server that receives registration requests
BRAS	Broadband Remote Access Server

5.2 Configuration Introduction

The VoIP parameter has been configured with the delivered HG256s. In general, this parameter does not need to be configured and please keep the default settings.

6 Configuring Frequently Used Functions

6.1 Enabling or Disabling the WLAN Function

Function Overview

The HG256s supports enabling or disabling the WLAN function. Thus, you can enable or disable the WLAN function as required.

Configuration Example

The WLAN function is enabled by default. 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**.

----End

TIP

- To enable the WLAN function, select **Enable WLAN**, and then click **Submit**.
- You can also use the WLAN button on the side panel of the HG256s to enable or disable the WLAN function.

6.2 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 HG256s provides multiple security-related settings for the WLAN function. You can change these settings as required to protect your WLAN from unauthorized access.

6.2.1 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 HG256s provides the function of hiding the SSID. After this function is enabled, the wireless signals transmitted from the HG256s 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 HG256s 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 Ensure select **Enable WLAN**.

Step 4 Select **SSID1** for **SSID Index**.

Step 5 Set **Enable SSID** to **Enable**.

Step 6 Set **Hide Broadcast** to **Enable**, and then click **Submit**.

Step 7 Select **SSID2** for **SSID Index**.

Step 8 Clear **Enable** for **Enable SSID**. Then click **Submit**.

Step 9 Repeat Step 7 and Step 8 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**.

6.2.2 Changing the Name of a WLAN

Function Overview

If the HG256s 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 HG256s is delivered, the SSID is preset. You can find this preset SSID on the label on the real panel of the HG256s. In addition, the HG256s 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

6.2.3 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 HG256s 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** or **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 HG256s 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@2010**.

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@2010**.

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.

6.2.4 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 HG256s, 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 HG256s 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 HG256s 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 HG256s 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

6.3 Using the Home Storage Function

Function Overview

The terminal supports the home storage function. Portable storage devices, such as USB flash drives and portable hard disks, can be connected to the USB interface on the terminal. If your portable storage device is a card reader, insert the storage card（for example CF, SD, and MMC card）in the card reader, and then connect the card reader to the USB interface of the terminal. The home storage function does not support the NTFS format.

Configuration Example

To access a portable storage device, do as follows:

Step 1 Configure parameters for the FTP server.

NOTE

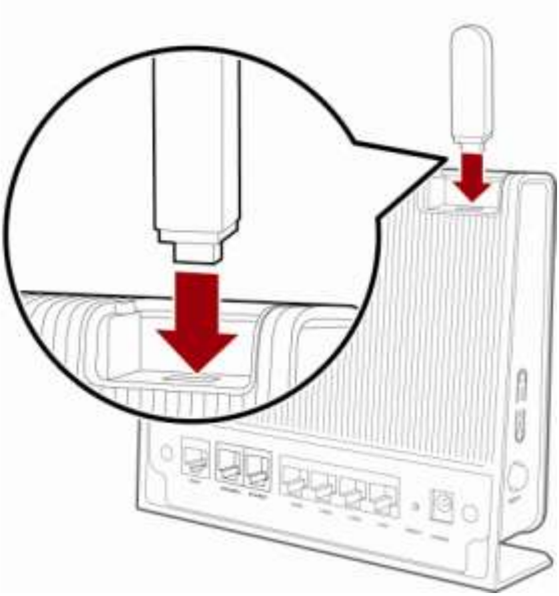
By default, the FTP server is enabled, the name and password of the FTP is **ftp**, and the port number for FTP server is **21**. You can just keep all the default settings and skip this step.

To change the default settings and configure new parameters for the FTP server, do as follows:

1. Log in to the Web-based configuration utility.
2. Choose **Advanced** > **USB port** in the navigation tree.
3. Ensure select **Ftp Enabled**.
4. Enter the new name and password of the FTP server in the **User name** and **Password** text boxes. Enter the password again in the **Confirm Password** text box.
5. Enter the new port number for FTP server.
6. Click **Submit** to save the settings.

Step 2 Connect a portable storage device to the USB interface on the terminal. For the connection method, see the following figure.

Figure 6-1 Home storage connection



Step 3 Accessing the Storage Device by the FTP Server.

To access the portable storage device by the FTP server, do as follows.

1. Launch the Internet Explorer and enter **FTP://192.168.1.1**.
2. In the Login dialog box, enter the user name and the password for logging in to the FTP server (the default user name and password are **ftp**) and then click **Login**.
3. After the password is verified, you can read and write the contents on the portable storage device connected to the terminal.

----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 certain computers are not allowed to access the Internet.

Through the MAC address filtering function of the HG256s, 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 HG256s to access the Internet. The wireless MAC filtering function controls the option of allowing a PC to be connected to the HG256s 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 HG256s 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**.

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 HG256s, the preceding functions can be implemented 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 ➖.

7 Maintenance Guide

7.1 Changing the Password of the Web-based Configuration Utility

Function Overview

You can configure all the parameters of the HG256s through the Web-based configuration utility. To prevent unauthorized personnel from changing these parameters, you need to use the user 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 password.

TIP

If you cannot remember the password that has been changed, you can restore the default settings of the HG256s 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 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 In **New username**, enter the user name **admin**.

Step 4 In the **Current password** text box, enter the currently used password **admin**.

Step 5 In the **New password** text box, 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 the IP address **192.168.1.1**. The IP address is used by the HG256s 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 HG256s are in the same network segment to enable the computer to access the Web-based configuration utility. In this case, 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 **192.168.1.1** 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 Restoring Default Settings

Function Overview

The HG256s provides powerful functions and rich parameters. Many parameters are set by default when the HG256s is manufactured. Those parameters enable the HG256s to work in most of network environments. In the following cases, you can restore the default settings of the HG256s: 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 HG256s.

When the HG256s is powered on, press and hold the RESET button for more than 3s, and then release it. Then the HG256s 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

8 FAQs

Q 1: Can I use the HG256s as a DHCP server?

Yes, you can. The HG256s incorporates the DHCP server software.

Q 2: How can I quickly restore the default settings of the HG256s?

When the HG256s is powered on, press and hold the RESET button for more than 3s, and then release it. Then the HG256s automatically restarts and the default settings are restored.

Q 3: What can I do if I cannot access the HG256s 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 HG256s.

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 HG256s configuration page.

If the problem persists, restore the default settings of the HG256s.

----End

Q 4: Does the WPS function have any special requirement on the wireless encryption settings of the HG256s?

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 HG256s through the WPS function at a particular moment.

Step 2 On the HG256s, ensure that the wireless network function and the WPS function implemented through the PBC method are enabled.

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 HG256s is forcibly disabled if the WEP encryption is used for accessing a WLAN.

Step 4 Check the positions of the wireless router and the PC. 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 HG256s 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 network cables of the HG256s are properly connected.

Step 2 Check whether the WLAN indicator of the HG256s is on.

If the WLAN indicator is off, you can infer that the wireless local area network (WLAN) function of the HG256s is disabled. In this case, enable the WLAN function.

For details about how to enable the WLAN function, see the manual of the HG256s.

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/g/n protocols.

If the wireless network adapter does not support the 802.11b/g/n 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 HG256s and ensure that no obstacles such as cement or wooden walls are present between the wireless client and the HG256s.

Step 6 Check whether the computer accesses the WLAN of the HG256s successfully.

Check the list of wireless network connections and ensure that the HG256s is connected to the WLAN.

Step 7 Try to access multiple Web sites to check whether the HG256s can access other Web sites.

If the HG256s cannot access other Web sites, restore the default settings of the HG256s. If the problem persists, contact your network service provider.

----End

Q 7: What can I do if the HG256s 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 HG256s 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

Q 9: Where should I install/position the HG256s in my home?

It is recommended that you place the HG256s 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 HG256s, you also need to pay attention to the following precautions so as to achieve the best performance of the WLAN:

- Place the HG256s in an open space and ensure that no obstacle, such as a cement or wooden wall, exists between your Desktops/Laptops/PCs and HG256s. Otherwise, the transmission of radio signals on the WLAN surely could be affected.
- Ensure that HG256s and your Desktops/Laptops/PCs are far from the electric appliances/devices (such as a microwave oven) that generate strong magnetic or electric fields. Magnetic or electric fields would interfere with WLAN wireless signal and result in bad reception performance.

Q 10: What are the factors that affect the wireless performance & range-coverage of the HG256s?

The wireless performance & range-coverage is impacted by the combined effects of various factors as below:

- Transmission attenuation – consider the health, wireless devices transmit power must be limited within a certain range. Meanwhile, household items and room walls will absorb the radio signal to generate signal attenuation. The more walls or objects between the computer and HG256s, the weaker of wireless signal and the lower of the rate.
- Distance attenuation - the wireless signal propagation in space is impacted by distance. Beyond a certain range, the wireless network connection speed will be reduced or even cannot receive the WLAN signal.
- Interference - wireless interference is the most universal WLAN problems. For radio interference, except the mutual interference between the WLANs, there are many electrical household equipment (such as microwave ovens, electric stove, refrigerator, air conditioning, telephone, etc.) produce radio radiation, which will affect the WLAN signal.
- Antenna - wireless equipments have transmitted antennas, subject to the direction of the antennas. Generally, the signal is not launched in all directions. HG256s in use. Additionally, movement of the device may induce the poor wireless coverage in some regions. If this always occurs, you should to rotate the antenna of the HG256s to find the appropriate direction. It is recommended to place the HG256s upright.
- Network Share - wireless network sharing is widely used; multiple users share the network will definitely decline the rate of wireless network for individual user. Please check the number of the wireless access connection. At the same time, please ensure that do not modify the default wireless configuration of the HG256s.

Q 11: What can I do to minimize wireless interference from other devices that can affect the HG256s?

It is advised to adjust the location of the HG256s, such as place it in the middle of the house. If you need more details, kindly refer to the answer of Q 9:.

Q 12: What can I do to improve the wireless coverage of the HG256s?

It is recommended to place the HG256s upright and place the HG256s in a stable and well-ventilated place and ensure that the HG256s and your PC are far from the electric appliances.

If you want to expend the wireless coverage obviously, please use the Wi-Fi repeater device to connect to the HG256s.

Q 13: What is the recommended encryption method to secure the wireless function of the HG256s?

For the WLAN encryption method, it is recommended to set the security mode to WPA2-PSK and encryption to AES. In advance, please ensure that the wireless adapter of your computer can support WPA2-PSK security and AES encryption.

Q 14: How can I connect a 3rd party wireless router behind the HG256s?

The HG256s can support various wireless routers. However, different vendors have different settings and configurations and will comply with various standards. So it might occur incompatible problem between the HG256s and other wireless routers. We highly recommend the end-uers to read and refer to the user guide of wireless router devices before connecting the wireless router to the HG256s.