EchoLife HG556a Home Gateway

Service Manual

HUAWEI TECHNOLOGIES CO., LTD.

EchoLife HG556a
V100R001

Service Manual

Issue	0G
Date	20F€ €G €3
Part Number	202219

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

Huawei Technologies Co., Ltd.

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

Website: http://www.huawei.com

Contents

Figures

Tables

About This Document

Purpose

This document describes the functions, features, and configuration methods of the EchoLife HG556a Home Gateway (hereinafter referred to as the terminal).

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

Related Versions

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

Product Name	Version
HG556a	V100R001

Intended Audience

This document is intended for:

- Installation and commissioning engineers
- Technical support engineers

Organization

This document is organized as follows.

Chapter	Describes
1 Safety Precautions	The safety precautions to be followed during the use of the terminal.
2 Product Overview	The functions and features of the terminal, the functional differences between different models of the terminal, and the indicator definitions and interface functions of the terminal.

Chapter	Describes
3 Quick Start	The methods for connecting the terminal, powering on the terminal, and logging in to the Web-based configuration utility of the terminal.
4 Configuration of Internet Access Parameters	The methods for configuring the Internet access parameters of the terminal.
5 Configuration of WLAN	The methods for setting up a wireless connection.
6 Configuration Frequently Used Functions	The methods for using some frequent functions of the terminal.
7 Maintenance Guide	Some maintenance operations related to the terminal, such as login account management, software upgrade, and network status diagnosis.
8 FAQs	Some common questions about the use of the terminal and the related solutions.
A Technical Specifications	The technical specifications of the terminal.
B Default Settings	The default settings of the terminal.
C Acronyms and Abbreviations	The acronyms and abbreviations involved in this document.

Conventions

Symbol Conventions

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

Symbol	Description
⚠ DANGER	Indicates a hazard with a high level of risk, which if not avoided, will result in death or serious injury.
⚠ WARNING	Indicates a hazard with a medium or low level of risk, which if not avoided, could result in minor or moderate injury.
⚠ 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`.

Command Conventions

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

Convention	Description
Boldface	The keywords of a command line are in **boldface**.
Italic	Command arguments are in *italics*.
[ ]	Items (keywords or arguments) in square brackets [ ] are optional.
{ x	y	... }	Optional items are grouped in braces and separated by vertical bars. One item is selected.
[x	y	...]	Optional items are grouped in brackets and separated by vertical bars. One item is selected or no item is selected.
{ x	y	... } *	Optional items are grouped in braces and separated by vertical bars. A minimum of one item or a maximum of all items can be selected.
[x	y	...] *	Optional items are grouped in brackets and separated by vertical bars. Several items or no item can be selected.

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**.

Convention	Description
>	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.
Drag	Press and hold the primary mouse button and move the pointer to a certain position.

1 Safety Precautions

To use the device properly and safely, read these warnings and precautions carefully and strictly observe them during operation.

NOTE

Unless otherwise specified, the device includes 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.

Disposal and Recycling Information

This symbol on the device (and any included batteries) indicates that the device (and any included batteries) should not be disposed of as normal household garbage. Do not dispose of your device or batteries as unsorted municipal waste. The device (and any batteries) should be handed over to a certified collection point for recycling or proper disposal at the end of its life.

For more detailed information about the recycling of the device or batteries, contact your local city office, the household waste disposal service, or the retail store where you purchased this device.

The disposal of this device is subject to the Waste from Electrical and Electronic Equipment (WEEE) Directive of the European Union. The purpose for separating WEEE and batteries from other waste is to minimize any environmental impact and health hazard due to the presence of hazardous substances.

Reduction of Hazardous Substances

This device is compliant with the EU Registration, Evaluation, Authorisation and Restriction of Chemicals (REACH) Regulation (Regulation No 1907/2006/EC of the European Parliament and of the Council) and the EU Restriction of Hazardous Substances (RoHS) Directive (Directive 2002/95/EC of the European Parliament and of the Council). For more information about the REACH compliance of the device, visit the Web site www.huaweidevice.com/certification. You are recommended to visit the Web site regularly for up-to-date information.

EU Regulatory Conformance

The antenna(s) used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons.

Български: С настоящето Huawei Technologies Co., Ltd. декларира, че този уред съответства на основните изисквания и другите разпоредби на Директива 1999/5/EC.

Česky: Huawei Technologies Co., Ltd., tímto prohlašuje, že toto zařízení je ve shodě se základními požadavky a dalšími souvisejícími opatřeními směrnice 1999/5/EC.

Dansk: Huawei Technologies Co., Ltd. erklærer hermed at denne enhed er i overensstemmelse med de obligatoriske krav og andre relevante bestemmelser i direktiv 1999/5/EF.

Nederlands: Hierbij verklaart Huawei Technologies Co., Ltd. dat dit apparaat in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EC.

English: Hereby, Huawei Technologies Co., Ltd. declares that this device is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.

Eesti: Käesolevaga kinnitab Huawei Technologies Co., Ltd., et see seade vastab Direktiivi 1999/5/EÜ põhinõudmistele ja teistele asjakohastele määrustele.

Suomi: Huawei Technologies Co., Ltd. vakuuttaa täten, että tämä laite on yhdenmukainen direktiivin 1999/5/EY olennaisten vaatimusten ja direktiivin muiden asiaankuuluvien lausumien kanssa.

Français (Européen) : Le fabricant déclare que ce produit est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE.

Deutsch: Huawei Technologies Co., Ltd. erklärt hiermit, dass dieses Produkt die erforderlichen Bestimmungen und andere relevante Verordnungen der Richtlinie 1999/5/EG einhält.

Ελληνικά: Δια της παρούσης η Huawei Technologies Co., Ltd. δηλώνει ότι αυτή η συσκευή συμμορφώνεται με τις βασικές απαιτήσεις και άλλες σχετικές διατάξεις της οδηγίας 1999/5/E.K.

Magyar: Jelen nyilatkozaton keresztül a Huawei Technologies Co., Ltd. kijelenti, hogy a készülék megfelel az EC/5/1999 Irányelv összes lényeges követelményének és vonatkozó előírásának.

Gaeilge: Fograíonn Huawei Technologies Co., Ltd leis seo go bhfuil an fheiste seo i gcomhlíonadh leis na fíor-riachtanais agus na forálacha eile maidir le Treoir 1999/5/AE.

Italiano: Col presente documento, Huawei Technologies Co., Ltd. dichiara che questo dispositivo è conforme ai requisiti essenziali e alle altre disposizioni applicabili della Direttiva 1999/5/CE.

Latviski: Ar šo Huawei Technologies Co., Ltd. paziņo, ka šī ierīce atbilst Direktīvas 1999/5/EC pamatprasībām un piemērojamajiem nosacījumiem.

Lietuviškai: Šiuo Huawei Technologies Co., Ltd. praneša, kad šis įtaisas atitinka Direktyvos 1999/5/EC pagrindinius reikalavimus ir taikomas sąlygas.

Malti: Hawnhekk, Huawei Technologies Co., Ltd. tiddikjara li dan it-tagħmir hu konformi mal-ħtiġijiet essenzjali u provvedimenti rilevanti oħrajn ta' Direttiva 1999/5/KE.

Polski: Wymieniona w tym dokumencie firma Huawei Technologies Co., Ltd. deklaruje, że niniejsze urządzenie spełnia zasadnicze wymagania w zakresie zgodności oraz inne odnośne postanowienia Dyrektywy 1999/5/EC.

Português (Europeu) : Deste modo, a Huawei Technologies Co., Ltd. declara que este dispositivo está em conformidade com os requisitos essenciais e outras provisões relevantes da Directiva 1999/5/CE.

Română: Prin prezenta Huawei Technologies Co., Ltd. declară că acest dispozitiv este conform cu cerinţele esenţiale şi alte prevederi relevante ale directivei 1999/5/CE.

Slovenčina: Huawei Technologies Co., Ltd. týmto vyhlasuje, že zariadenie je v súlade so základnými požiadavkami a inými relevantnými predpismi Smernice 1999/5/ES.

Slovenščina: Huawei Technologies Co., Ltd. izjavlja, da je ta naprava v skladu z bistvenimi zahtevami in drugimi ustreznimi določbami Direktive 1999/5/ES.

Español (Europeo) : Con el presente documento, Huawei Technologies Co., Ltd. declara que este dispositivo cumple con los requisitos esenciales y con las demás disposiciones correspondientes de la Directiva 1999/5/CE.

Svenska: Huawei Technologies Co., Ltd. förklarar härmed att denna produkt överensstämmer med de grundläggande kraven och andra relevanta föreskrifter i direktiv 1999/5/EG.

For the declaration of conformity, visit the Web site www.huaweidevice.com/certification.

CE0678①

Notice: This device can be operated in all European countries.

France: Outdoor use limited to 10 mW e.i.r.p. within the band 2454-2483.5 MHz.

Italy: For private use, a general authorisation is required if WAS/RLAN's are used outside own premises. For public use, a general authorisation is required.

Luxembourg: General authorisation required for network and service supply.

Norway: This subsection does not apply for the geographical area within a radius of 20 km from the centre of Ny-Ålesund.

2 Product Overview

2.1 Product Features

The EchoLife HG556a Home Gateway (hereinafter referred to as the terminal) is a home gateway using the Asymmetric Digital Subscriber Line (ADSL) technology. It also supports high-speed wireless uplink through HSPA stick.

The Home Gateway is the core component of the digital home. In addition to the high-speed WAN interface, the terminal also provides abundant LAN interfaces to facilitate flexible LAN networking of business terminals and interworking between household terminals. The terminal can function as a print server when connected to a printer through the USB 2.0 host interface. It also supports multiple USB devices, such as the USB stick, USB hard disk, and USB card reader.

2.2 Hardware

2.2.1 Indicators

Table 2-1 describes the indicators of the terminal.

Table 2-1 Indicators of the terminal

Indicator	Color	Status	Meaning
Message	-	Off	There is no message.
	Red	On	There is an incoming message.
HSPA	-	Off	The HSPA module is not connected or used.
	Red	Blinking slowly	The HSPA connection is normal and data connection is being established.
	Red	Blinking quickly	The HSPA connection is normal and voice connection is being established.
	Red	On	The connected HSPA module works normally.

Indicator	Color	Status	Meaning
Wi-Fi ((ɪ))	-	Off	The Wi-Fi network is not activated.
	Red	Blinking slowly	The Wi-Fi Protected Setup (WPS) process is in progress.
	Red	On	The Wi-Fi connection is in good condition.
	Red	Blinking quickly	The Wi-Fi connection is normal and data is being transmitted on the link.
DSL	-	Off	The ADSL connection is not activated.
	Red	Blinking slowly	The ADSL connection is in process.
	Red	On	The ADSL connection is in good condition.
	Red	Blinking quickly	DSL synchronization is in progress.
POWER	-	Off	The terminal is powered off.
	Red	On	The terminal is powered on.
LAN LAN	-	Off	The diagnostic button is not pressed.
	Green	On	The Ethernet connection is in good condition.
	Red	On	The LAN connection is not connected.

NOTE

The four LAN indicators are off by default.

When the diagnostic button is pressed, the four LAN indicators turn red or green.

2.2.2 Interfaces and Buttons

Table 2-2 describes the interfaces and buttons of the terminal.

Table 2-2 Interfaces and buttons of the terminal

Interface or Button	Meaning
◯ ?	Diagnostic button, press this button to check the status of the four LAN indicators.
ADSL	Connects the telephone jack on the wall.
PHONE1, PHONE2	Connects a phone to the PHONE1 or PHONE2 respectively. The actual function have to consult the Internet Service Provider.
LAN1,LAN2, LAN3, LAN4	Connects PCs, switches, or other equipment.

2 Product Overview

Interface or Button	Meaning
Wi-Fi	Enable or disable the Wi-Fi function and the WPS function.
USB	Connects a USB storage device, such as a USB disk, a printer etc.
RESET	Restores the factory settings if this button is pressed and hold more than 5 seconds. **NOTE** After you restore the factory settings, the customized data will be lost. Therefore, press the **RESET** button with caution.
POWER	Connects a power adapter.
RESTART	Restarts the terminal if this button is pressed and hold more than 0.5 seconds.

NOTE

- The initial configuration for the Wi-Fi function of the terminal is enabled.

- Press and hold the Wi-Fi button for less than four seconds to disable the Wi-Fi function.

- Press and hold the Wi-Fi button for more than four seconds to enable the WPS function.

3 Quick Start

3.1 Connecting Cables

Figure 3-1 shows the cable connections of the terminal.

Figure 3-1 Cable connections of the terminal
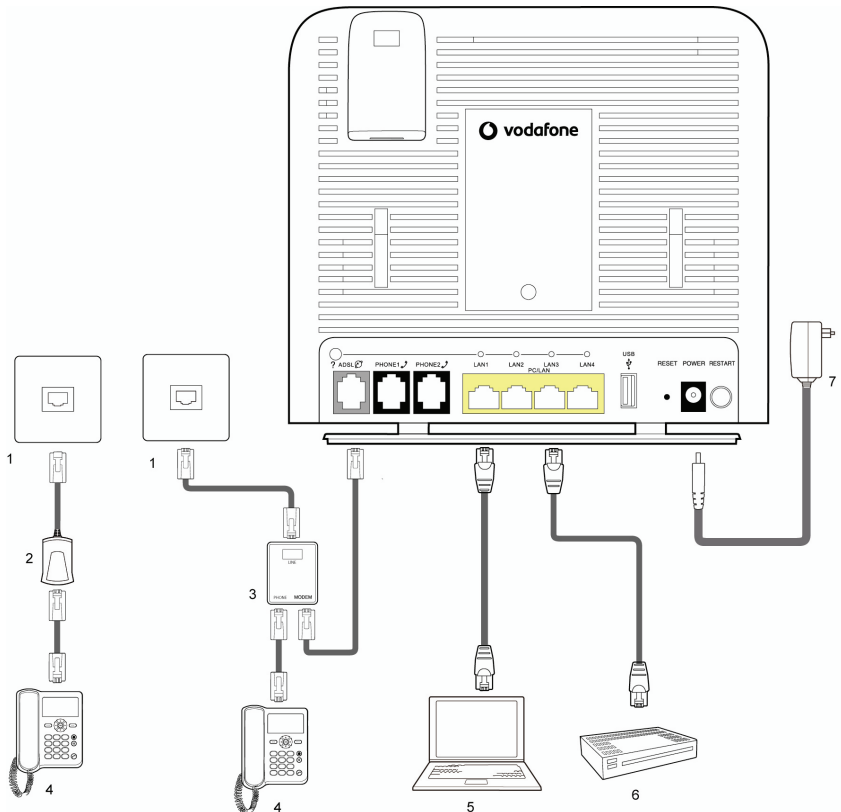
1. Telephone jack on the wall   2. Micro-filter   3. Splitter
4. Telephone   5. PC   6. Set-top box
7. Power adapter

If you have another phone, do as follows refer to the left of the Figure 3-1:

1. Unplug your telephone cable from the wall socket.
2. Connect the micro-filter to the wall socket.
3. Connect the phone to the micro-filter with the DSL cable.

3.2 Inserting the USB Stick

1. Remove the SIM card holder from the USB stick.
2. Insert the SIM card into the card holder.
3. Reinsert the SIM card holder into the USB stick.
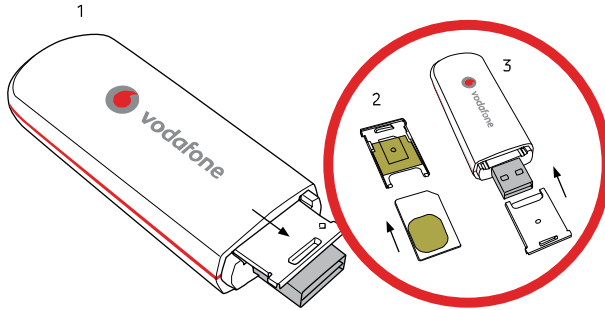
4. Remove the lid on the back of the terminal and insert the USB stick into the slot.
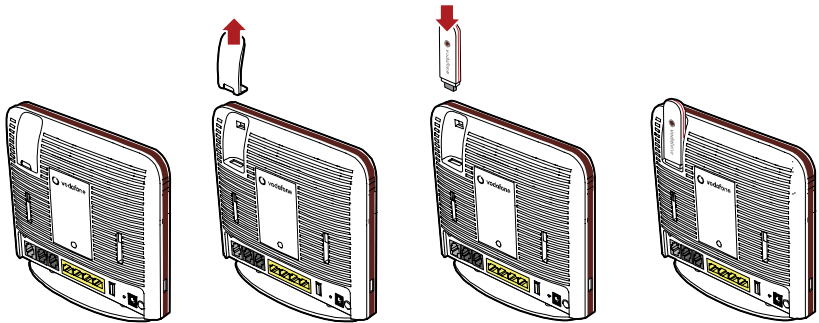
☐ NOTE

The previous USB stick is just the sample for your reference, you can choose other kind of USB stick that assigned by the Internet Service Provider (ISP) and use the same way to install.

Huawei Proprietary and Confidential
Copyright © Huawei Technologies Co., Ltd.

3.3 Logging In to the Web-Based Configuration Utility

The terminal provides simple and easy Web-based configuration utility, through which you can view or configure the working parameters of the terminal.

Table 3-1 lists the PC settings required to log in to the Web-based configuration utility of the terminal.

Table 3-1 PC settings required to log in to the Web-based configuration utility

Item	Requirement
Network protocol	Enable TCP/IP.
PC IP address	Set the IP address of the PC to the same network segment as the IP address of the LAN interface of the terminal.
	By default, the IP address of the LAN interface of the terminal is 192.168.1.1.
	By default, the DHCP function is enabled on the terminal. Therefore, you can configure the PC to obtain an IP address automatically.
Internet Explorer	Do not use the proxy server.

To log in to the Web-based configuration utility, perform the following steps:

Step 1 Start the Internet Explorer on the PC and ensure that the Internet Explorer does not use any proxy server.

Take Internet Explorer 6.0 as an example. To check that the Internet Explorer does not use any proxy server, perform the following steps:

1. Start the Internet Explorer. Choose **Tools** > **Internet Options** on the menu bar.
2. Click the **Connect** tab in the **Internet Options** dialog box, and then 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 2 Enter **http://192.168.1.1** in the address bar of the Internet Explorer, and then press **Enter**.

Step 3 Enter the administrator account (User name is admin and password is **VF-IRhg556** by default) in the **Login** dialog box, and then click **OK**.

----End

📖 NOTE

By default, the IP address of the LAN interface of the terminal is 192.168.1.1. You can change this IP address. After changing this IP address, ensure that the IP address of the PC is in the same network segment as the IP address of the LAN interface of the terminal.

4 Configuring the WAN Interface

The terminal supports ADSL uplink and HSPA uplink, and you can choose any of the two modes to access the Internet.

☞ **TIP**

Just keep the default settings, you can access the Internet and do not need to do any configuration.

4.1 Selecting ADSL uplink mode

When you select the ADSL uplink mode, the WAN interface of the terminal supports multiple work modes, as listed in Table 4-1.

Table 4-1 Work mode of the WAN interface

Work Mode	Description
PPP over ATM (PPPoA)	• The terminal serves as a router. • Data packets use the PPPoA encapsulation mode
PPP over Ethernet (PPPoE)	• The terminal serves as a router. • Dialing is performed through the embedded PPP dialer software of the terminal. • Data packets are encapsulated in PPPoEoA mode.
MAC Encapsulation Routing (MER)	• The terminal serves as a router. • Data packets use the IPoEoA encapsulation mode. • WAN IP address of the terminal can be a static IP address or allocated by the upper-layer DHCP server automatically.
IP over ATM (IPoA)	• The terminal serves as a router. • Data packets use the IPoA encapsulation mode.
Bridge	• The terminal serves as a network bridge. • Dialing is performed through the PPP dialer software installed on the PC. • The IP address of the computer is a static IP address or is assigned by an upper-layer device.

Table 4-2 lists the information to be collected before configuring the ADSL uplink mode.

Table 4-2 Parameter for the **ATM PVC Configuration** page

Parameter	Description
VPI/VCI	It specifies the VPI and VCI of the PVC. The value is set as 8/35 by default. The VPI and VCI of the PVC of the terminal should be consistent with those of the PVC of the devices on operator networks so that the connection between the terminal and the devices can be set up through the PVC.
Service Category	It specifies the traffic management type used by the PVC. • **UBR Without PCR**: It refers to an unspecified bit rate without a peak cell rate. Since the transmission rate is not specified, the ATM network tries its best to transmit UBR user information, which is called the best effort. In this case, however, the transmission quality cannot be ensured. For example, the cell loss and the delay and jitter of cell transmission may occur. This type is applicable when an end-to-end fault tolerance mechanism or protocol exists at an upper layer and when no stringent requirement is imposed on the network transmission capability. • **UBR With PCR**: It refers to an unspecified bit rate with a peak cell rate. • **CBR**: It refers to a constant bit rate. Fixed requirements are imposed on the bandwidth (rate). This type is applicable to real-time transmission of audio and video signals. • **Non Realtime VBR**: It refers to a non-real-time variable bit rate. No stringent requirement is imposed on the cell delay. For example, when a user retrieves the MPEG-2 video from the video server through the ATM network, seconds of network delay does not affect the video quality. You should set transmission rates, such as the PCR and the SCR, on the network, thus reducing the cell loss rate. • **Realtime VBR**: It refers to a real-time variable bit rate. The cell delay is restricted stringently. This type is mainly used for real-time services, such as the video output by a variable rate encoder, video monitoring, and compressed voice communication.
Connection type	It specifies the protocol used by the PVC. You should select the protocol that meets the requirements of the DSLAM. The optional protocols vary with the working mode of the PVC.
Encapsulation Mode	It specifies the packet encapsulation mode. It is assigned by the Internet Service Provider.
Enable 802.1q	It specifies whether to enable the VLAN function.

4.1.1 Configuring the PPPoA Mode

To configure the PPPoA mode for the WAN interface, do as follows

Step 1 Logging in to the Web-based configuration utility. For details, see section 3.3 "Logging In to the Web-Based Configuration Utility."

Step 2 Choose **Advanced Setup** > **WAN** in the navigation tree.

Step 3 Select **ADSL Uplink**.

Step 4 Click **Next** to show the **Wide Area Network (WAN) Setup** page.

Figure 4-1 Wide Area Network (WAN) Setup page

Step 5 Click **Add** to show the **ATM PVC Configuration** page, set the parameters refer to Table 4-2.

Figure 4-2 ATM PVC Configuration page

Step 6 Enter the value in the **VPI** and **VCI** text boxes that provided by the Internet Service Provider.

Step 7 Click **Next** to show the **Connection Type** page.

Figure 4-3 Connection Type page
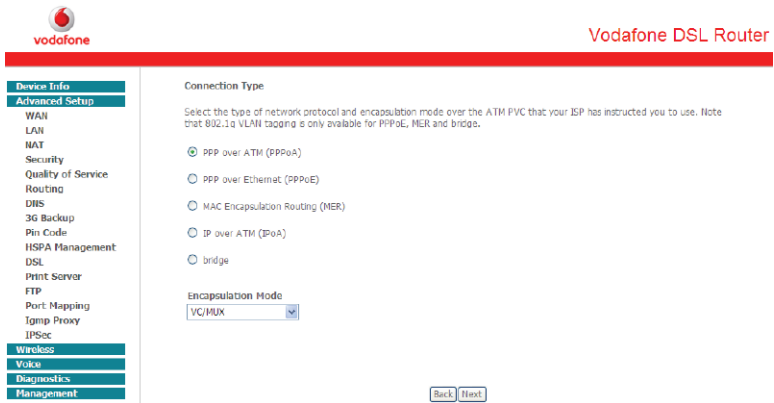
Step 8 Select **PPP over ATM (PPPoA)**. Choose **LLC/ENCAPSULATION** in the **Encapsulation Mode** drop-down list box.

Step 9 Click **Next** to show the **PPP Username and Password** page for PPPoA, set the parameters refer to Table 4-3.

Figure 4-4 PPP Username and Password page for PPPoA

Huawei Proprietary and Confidential

Copyright © Huawei Technologies Co., Ltd.
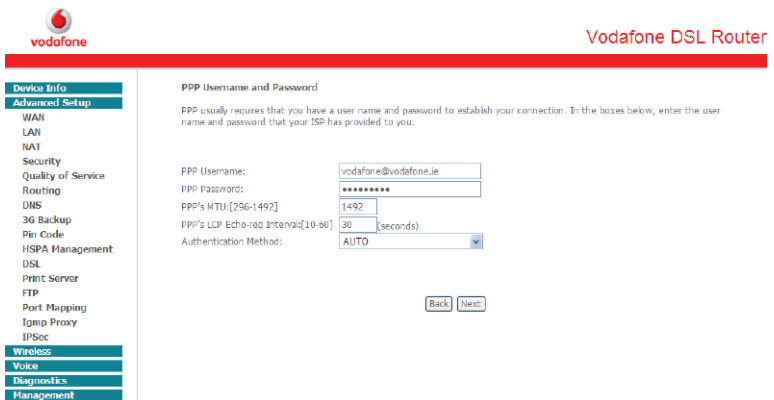
Table 4-3 Parameters for the **PPP Username and Password** page

Parameter	Description
PPP Username	The user name of the PPP, which is provided by the Internet Service Provider.
PPP Password	The user name of the PPP, which is provided by the Internet Service Provider.
PPP's MTU:[296-1492]	The maximum length of the transported IP package with the selected PPPoA protocol.
PPP's LCP Echo-req Interval:[10-60]	It specifies the time interval of the two echo-requests.
Authentication Method	The authentication method of the PPP protocol.

Step 10 Click **Next** to show the **Enable WAN Service** page, just keep the default settings. Make sure choose **Data** in the **Service Name** drop-down list box.

Step 11 Click **Next** to show the **WAN Setup-Summary** page, click **Save** to save the settings.

📖 **NOTE**

Click **Back** to make any modifications. Reboot the terminal so that the settings take effect.

----End

4.1.2 Configuring the PPPoE Mode

To configure the PPPoE mode for the WAN interface, do as follows:

Step 1 Repeat from the step1 to the step 7 of 4.1.1 "Configuring the PPPoA Mode."

Step 2 On the **Connection Type** page, select **PPP over Ethernet (PPPoE)**. Keep other settings by the Internet Service Provider.

Step 3 Click **Next** to show the **PPP Username and Password** page for PPPoE, you can keep the default settings or set the parameters refer to Table 4-4.

Figure 4-5 PPP Username and Password page for PPPoE
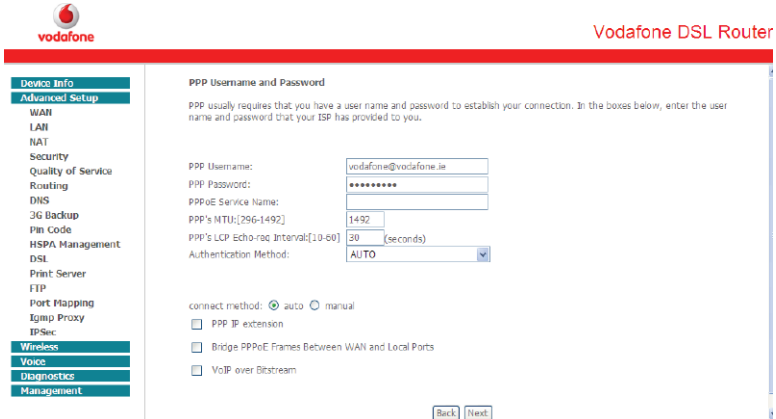
Table 4-4 Parameters for the **PPP Username and Password** page

Parameter	Description
PPP Username	The user name of the PPP, which is provided by the Internet Service Provider.
PPP Password	The user name of the PPP, which is provided by the Internet Service Provider.
PPPoE Service Name	The name of the PPPoE, which is provided by the Internet Service Provider.
PPP's MTU:[296-1492]	The maximum length of the transported IP package with the selected PPPoA protocol.
PPP's LCP Echo-req Interval:[10-60]	It specifies the time interval of the two echo-requests.
Authentication Method	The authentication method of the PPP protocol.
Connect method	It is assigned by the Internet Service Provider.

Step 4 Click **Next** to show the **Enable WAN Service** page, just keep the default settings. Make sure choose **Data** in the **Service Name** drop-down list box.

Step 5 Click **Next** to show the **WAN Setup-Summary** page, click **Save** to save the settings.

📖 **NOTE**

Click **Back** to make any modifications. Reboot the terminal so that the settings take effect.

----End

4.1.3 Configuring the MER Mode

To configure the MER mode for the WAN interface, do as follows:

Step 1 Repeat from the step1 to the step 7 of 4.1.1 "Configuring the PPPoA Mode."

Step 2 On the **Connection Type** page, select **MAC Encapsulation Routing (MER)**. Keep other settings by the Internet Service Provider.

Step 3 Click **Next** to show the **WAN IP Settings** page, you can keep the default settings or set the parameters refer to Table 4-5.

Table 4-5 Parameters for the **WAN IP Settings** page

Parameter	Description
DHCP Class Identifier	It specifies the client.
WAN IP Address	It specifies the WAN IP address of the PVC. When the method for obtaining an IP address is set to using a static IP address, the terminal provides this parameter.
WAN Subnet Mask	It specifies the WAN subnet mask of the PVC. When the method for obtaining an IP address is set to using a static IP address, the terminal provides this parameter.
Primary DNS server	It specifies the IP address of the primary DNS server used by the PVC. When the method for obtaining an IP address is set to using a static IP address, the terminal provides this parameter.
Secondary DNS server	It specifies the IP address of the secondary DNS server used by the PVC. When the method for obtaining an IP address is set to using a static IP address, the terminal provides this parameter.
IpoE's MTU:[296-1500]	The maximum length of the transported IP package with the selected IPoE protocol.

Step 4 Click **Next** to show the **Network Address Translation Settings** page, just keep the default settings. Make sure choose **Data** in the **Service Name** drop-down list box.

Step 5 Click **Next** to show the **WAN Setup-Summary** page, click **Save** to save the settings.

⬜ NOTE

Click **Back** to make any modifications. Reboot the terminal so that the settings take effect.

----End

4.1.4 Configuring the IPoA Mode

To configure the IPoA mode for the WAN interface, do as follows:

Step 1 Repeat from the step1 to the step 7 of 4.1.1 "Configuring the PPPoA Mode."

Step 2 On the **Connection Type** page, select **IP over ATM (IPoA)**.

Step 3 Click **Next** to show the **WAN IP Settings** page for IPoA, you can keep the default settings or set the parameters refer to Table 4-6.

Figure 4-6 WAN IP Settings page for IPoA
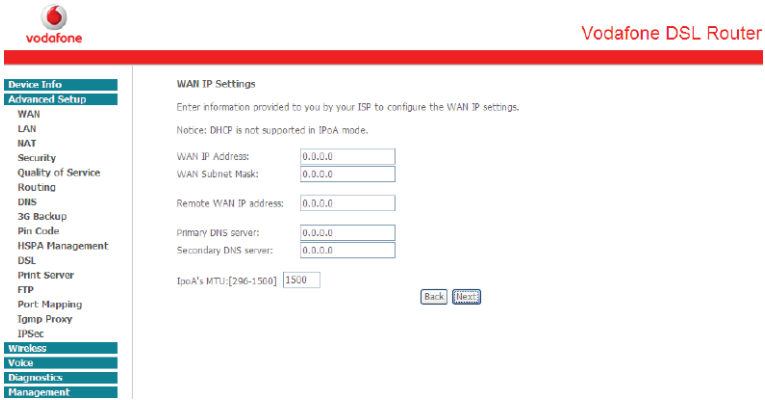
Table 4-6 Parameters for the **WAN IP Settings** page for IPoA

Parameter	Description
WAN IP Address	It specifies the WAN IP address of the PVC. This parameter is provided by the Internet Service Provider.
WAN Subnet Mask	It specifies the WAN subnet mask of the PVC. This parameter is provided by the Internet Service Provider.
Remote WAN IP address	It specifies the remote WAN IP address of the PVC. This parameter is provided by the Internet Service Provider.
Primary DNS server	It specifies the IP address of the primary DNS server used by the PVC. This parameter is provided by the Internet Service Provider.
Secondary DNS server	It specifies the IP address of the secondary DNS server used by the PVC. This parameter is provided by the Internet Service Provider.
IpoA's MTU:[296-1500]	The maximum length of the transported IP package with the selected IPoA protocol.

Step 4 Click **Next** to show the **Network Address Translation Settings** page, just keep the default settings. Make sure choose **Data** in the **Service Name** drop-down list box.

Step 5 Click **Next** to show the **WAN Setup-Summary** page, click **Save** to save the settings.

📖 NOTE

Click **Back** to make any modifications. Reboot the terminal so that the settings take effect.

----End

4.1.5 Configuring the Bridge Mode

To configure the Bridge mode for the WAN interface, do as follows:

Step 1 Repeat from the step1 to the step 7 of 4.1.1 "Configuring the PPPoA Mode."

Step 2 On the **Connection Type** page, select **bridge**. Keep other settings by the Internet Service Provider.

Step 3 Click **Next** to show the **Unselect the check box below to disable this WAN service** page, keep the default settings. Make sure choose **Data** in the **Service Name** drop-down list box.

Step 4 Click **Next** to show the **WAN Setup-Summary** page, click **Save** to save the settings.

📖 NOTE

Click **Back** to make any modifications. Reboot the terminal so that the settings take effect.

----End

4.2 Selecting HSPA uplink mode

To configure the WAN parameters by HSPA uplink mode, do as follows:

Step 1   Logging in to the Web-based configuration utility. For details, see section 3.3 "Logging In to the Web-Based Configuration Utility."

Step 2   Choose **Advanced Setup** > **WAN** in the navigation tree.

Step 3   Select **USB Uplink**. If you choose the USB uplink, insert the USB stick firstly. More details, see section 3.2 "Inserting the USB Stick."

Step 4   Click **Next** to show the **Hsdpa Profile Settings** page, just keep the default settings on the page.

Step 5   Click **Next** three times again.

Step 6   Click **Save** to save the settings, click **Save/Reboot** to save the settings and reboot the terminal to make the new configuration effective.

   ----End

If the SIM card of your USB stick set the PIN code, you have to verify the pin code:

Step 1   Choose **Advanced Setup** > **Pin Code** in the navigation tree.

Step 2   Enter the pin code of the USB stick in the **Pin Code** text box.

Step 3   Click **Check**. After verifying the pin code, you can access the Internet.

   ----End

5 Configuration of WLAN

5.1 Setting Up a Wireless Connection by the Wi-Fi Button

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

Step 1 Press the Wi-Fi button on the side panel and hold it for more than four seconds to enter the WPS negotiation state. The Wi-Fi indicator starts to blink slowly in a few seconds.

📖 NOTE

● By default, the Wi-Fi function of the terminal is enabled. Press the Wi-Fi button on the side panel and hold it for less than four seconds to disable the Wi-Fi function, and hold it for more than four seconds to enable the WPS function.

● If the Wi-Fi indicator does not blink, it indicates that the WPS function cannot be enabled. Note that the WPS function can be used only when the security mode of the WLAN is set to WPA-PSK or WPA2-PSK.

Step 2 Access the WLAN through the wireless network adapter on your PC.

After you install a wireless network adapter on your PC and enable the WPS negotiation function, the wireless network adapter automatically searches for an available wireless network and connect to the wireless network automatically.

Step 3 Wait for a few seconds, and then you can see the wireless icon on the corner to the right of the task bar of the PC.

----End

5.2 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 terminal 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 terminal.

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

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

Step 1 Record the WLAN name and the WLAN access password.

◎⚊ TIP

The WLAN name (**SSID**) and WLAN access password of the terminal are preset before delivery. You can find them from the label on the rear panel of the terminal.

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 terminal.

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

6 Configuring Frequently Used Functions

6.1 Configuring Multiple PCs to Access the Internet

Function Overview

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

Configuration Example

For example, you have two desktop computers 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 terminal are completed before delivery. You only need to connect the desktop computers and the laptop to the terminal and set certain Internet access parameters of the terminal as follows:

Step 1 Connect the two desktop computers to the terminal by using network cables.

For details, see section 3.1 "Connecting Cables."

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

For details, see chapter 5 "Configuration of WLAN."

Step 3 Set the Internet access parameters of the terminal to connect the terminal to the Internet.

For details, see chapter 4 "Configuring the WAN Interface."

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 Internet 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, consult the Internet Service Provider.

6.2 Enabling or Disabling the WLAN Function

Function Overview

The terminal 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 Choose **Wireless** > **Basic** in the navigation tree.

The WLAN configuration page is displayed.

Step 3 Clear **Enable Wireless**, and then click **Submit**.

----End

⊙━ᴬ **TIP**

You can also use the Wi-Fi button on the side panel of the terminal to enable or disable the WLAN function. More details, see 5.1 "Setting Up a Wireless Connection by the Wi-Fi Button."

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 port 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 hard disks of the NTFS format support read only, cannot write.

Configuration Example

To access a portable storage device, do as follows:

Step 1 Enable the FTP server. To configure parameters of the FTP server, do as follows:

1. Log in to the Web-based configuration utility.
2. Choose **Advanced Setup** > **FTP** in the navigation tree.
3. Select **Enabled**.
4. Enter the name and password of the FTP in the **UserName** and **Password** text boxes. Enter the password again in the **Confirm Password** text box.
5. Click **Save/Apply** to save the settings.

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

Figure 6-1 Home storage connection
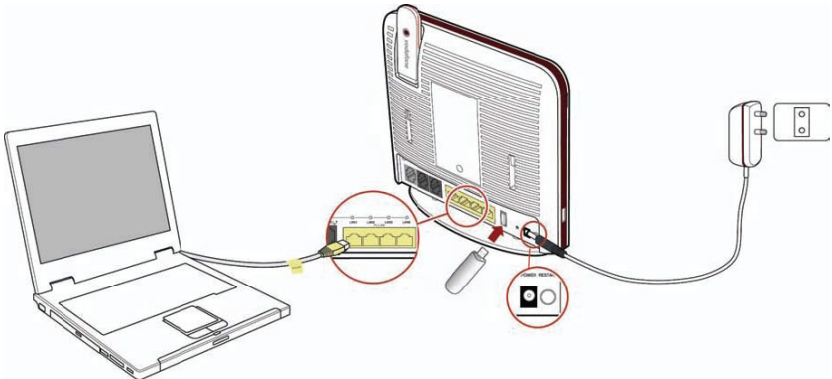
After connecting the cables, you can access the portable storage device through the three methods as follows.

----End

6.3.1 Accessing the Storage Device by the FTP Client

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

Step 1 Launch the Internet Explorer and enter **FTP://192.168.1.1**.

Step 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 **vodafone**) and then click **Login**.

Step 3 After the password is verified, you can read and write the contents on the portable storage device connected to the terminal.

----End

6.3.2 Accessing the Storage Device by the Samba Function

To access the portable storage device by the Samba Function, do as follows.

Step 1 Launch the Internet Explorer and enter **\\192.168.1.1** in the address bar, then press **Enter** to display the **Share** folder.

Figure 6-2 Share folder
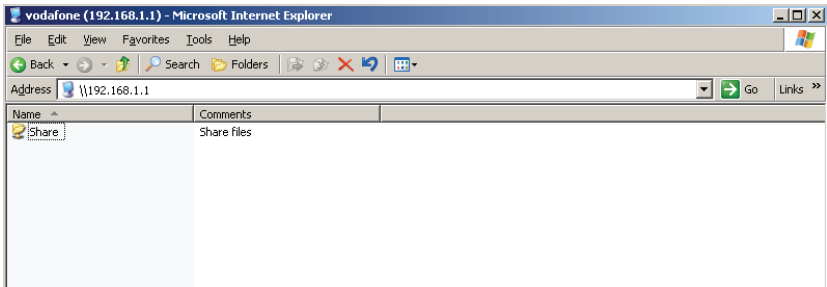
Step 2 Double-click the Share folder. Then you can share the contents on the portable storage device.

Figure 6-3 USBDisk_1 folder

Huawei Proprietary and Confidential
Copyright © Huawei Technologies Co., Ltd.
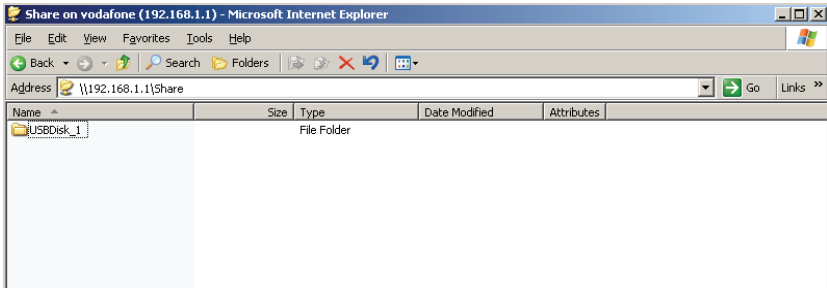
Step 3   Double click the **USBDisk_1** folder, and then you can see the folder structure of your portable storage device.

    ----End

6.3.3 Accessing the Storage Device by Mapping Network Drive

The terminal allows you to accessing the portable storage device by mapping as a network drive, do as follows:

Step 1   Right click the **My Computer** icon on the desktop of your PC.

Step 2   Choose **Map Network Drive** to display the **Map Network Drive** page, see Figure 6-4.

Step 3   Specify the drive name (take **Z** as an example) in the **Drive** drop-list box.

Step 4   Enter the path of the shared folder: \\192.168.1.1\share.

Step 5   Click **finish**.

Step 6   Double click the My Computer icon to see a mapped network drive named Z.

Step 7   Double click the **Z** disk to see the content in your portable storage device.

Figure 6-4 Map Network Drive page
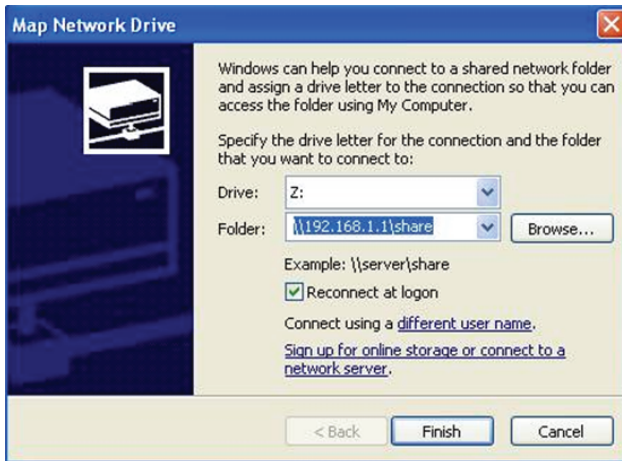
    ----End

6.4 Using the USB Printer Function

To enable the USB printer function, do as follows.

Step 1 Connect the cables refer to Figure 6-5.

Figure 6-5 USB printer connection
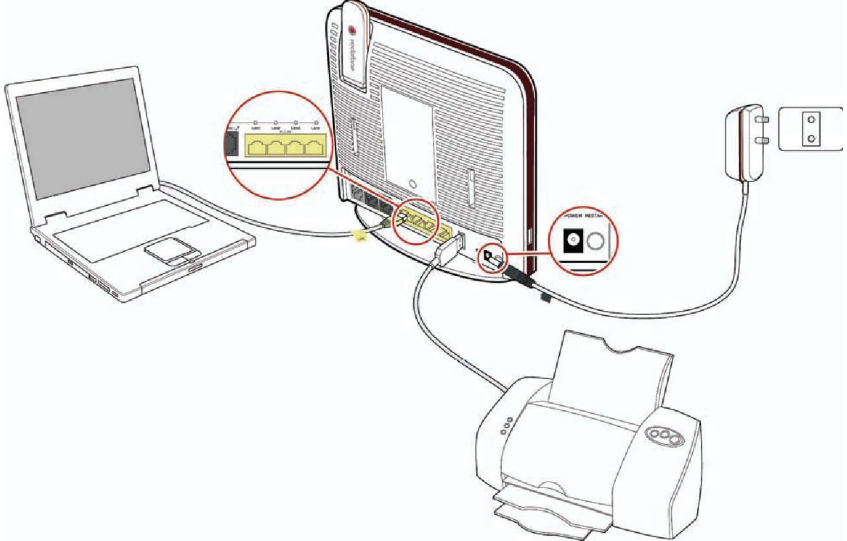
Step 2 Configure the web page as follows:

1. Launch the Internet Explorer on your computer and enter **http://192.168.1.1** in the address bar.
2. Enter the user name and the password in the displayed window, and then click **OK**.
3. Choose **Advanced Setup** > **Printer Server** in the navigation tree.
4. Enable the **Enable on-board print server** option text box.
5. Enter the printer name and the model of your printer in the **Printer name** and **Make and model** text boxes.
6. Click **Save/Apply** to save the settings.

Step 3 Set the printer parameters on the PC.

1. Choose **Start** > **Printers and Faxes**. Then click the Add Printer icon on the left side of the displayed page.
2. Click **Next** in the **Welcome to the Add Printer Wizard** page.

Figure 6-6 Welcome to the Add Printer Wizard page
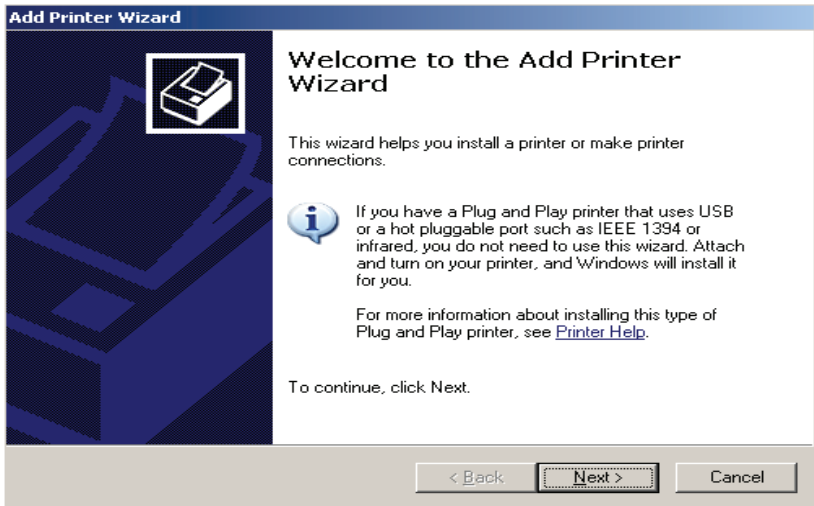
3. Select **A network printer, or a printer attached to another computer** and then click **Next**.

Figure 6-7 Add Printer Wizard page
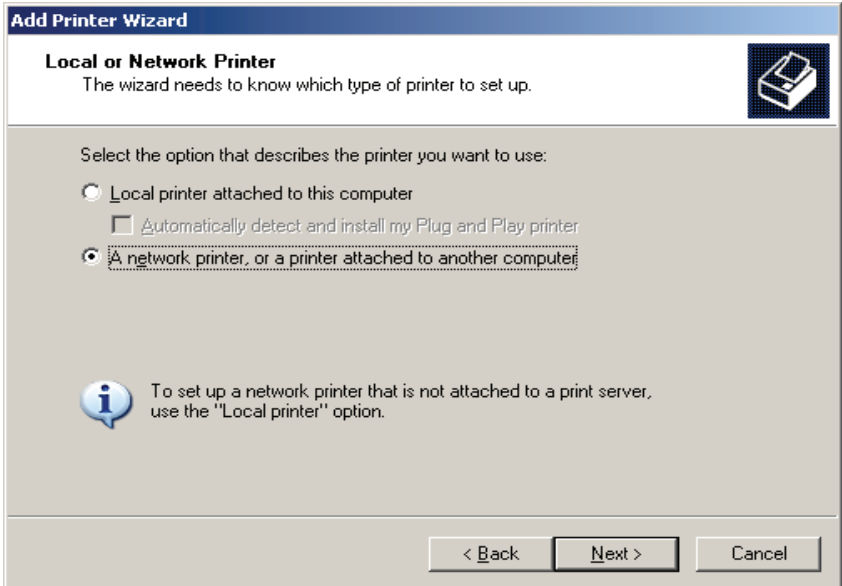
4. Select Connect to a printer on the Internet or on a home or office network.

5. Enter **http://192.168.1.1:631/printers/myprinter** in the URL text box, click **Next**.

⊙━ TIP

The address **192.168.1.1:631** is preset and cannot be changed, **myprinter** is the printer name that you specified.

6. Choose the printer model that you want.

If there is no printer model for you to choose, please install the printer driver on your PC first.

7. Click **OK** to set the current printer as the default printer.

8. Click **Finish** to complete the settings.

Open the files you want to print on your PC. Then you can choose the printer just installed to print your files.

----End

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

6.5.1 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 terminal 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 terminal provides the function of hiding the SSID. After this function is enabled, the wireless signals transmitted from the terminal 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 terminal also provides the multi-SSID function. You can configure 4 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   Choose **Wireless** > **Basic** in the navigation tree.

The WLAN configuration page is displayed.

Step 3   Enter **SSID1** in the **SSID** text box.

Step 4   Enable the **Enable Wireless** option text box.

Step 5   Clear the **Hide Access Point** option text box, and then click **Save/Apply**.

Step 6   In the **Wireless - Guest/Virtual Access Points** area, enter **SSID2** in the **SSID** text box.

Step 7   Clear the **Enabled** option text box. Then click **Save/Apply**.

Step 8   Repeat Step 6 and Step 7 to disable other SSIDs.

      ----End

      ◎━ **TIP**

        If you consider the use of a WLAN is 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 **Save/Apply**.

6.5.2 Changing the Name of a WLAN

Function Overview

If the terminal 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 terminal is delivered, the SSID is preset. You can find this preset SSID on the label on the real panel of the terminal. In addition, the terminal 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   Choose **Wireless** > **Basic** in the navigation tree.

      The WLAN configuration page is displayed.

Step 3   Clear **SSID1** in **SSID** text box, and enter **MyNewSSID**.

Step 4   Click **Save/Apply**.

      ----End

6.5.3 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 terminal 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 terminal 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**.

To set the preceding parameters, do as follows:

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

Step 2   Choose **Wireless** > **Security** in the navigation tree.

The WLAN configuration page is displayed.

Step 3 Select **Mixed WPA2/WPA-PSK** in **Network Authentication** drop-down list box.

Step 4 In **WPA Pre-Shared Key** text box, enter **MyPassword**.

Step 5 Select **AES** in **WPA Encryption** drop-down list box.

Step 6 Click **Save/Apply**.

----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.

6.5.4 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 terminal, 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 terminal through a WLAN. The MAC address filtering function described in section **6.6**
> "Controlling the Internet Access Rights of PCs" controls the option of allowing a PC
> connected to the terminal 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 terminal 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 Choose **Wireless** > **MAC Filter** in the navigation tree.

The WLAN configuration page is displayed.

Step 4 Select **MyNewSSID** in the **Select SSID** drop-down list box.

Step 5 Select **Allow**.

Step 6 Click **Add**.

Step 7 In **MAC address** text box, enter the MAC address of the laptop.

For example, the MAC address is **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 8 Click **Save/Apply**.

----End

6.6 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 terminal, 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 terminal to access the Internet. The wireless MAC filtering function controls the option of allowing a PC to be connected to the terminal 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 terminal 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 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 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 Setup > Security** > **Parental Control**.

Step 3 Click **Add**.

Step 4 Set the following parameters based on rule 1.

- User Name: Internet access before 19:00 in the evening
- Other MAC Address: 00:11:09:11:04:DD

- Click to select: Select from Monday to Sunday
- Start Blocking Time (hh:mm): 00:00
- End Blocking Time (hh:mm): 18:59

Step 5 Click **Save/Apply**.

Step 6 Click **Add**.

Step 7 Set the following parameters based on rule 2.

- User name: Internet access after 20:00 in the evening
- Other MAC address: 00:11:09:11:04:DD
- Click to select: Select from Monday to Sunday
- Start Blocking Time (hh:mm): 19:59
- End Blocking Time (hh:mm): 23:59

Step 8 Click **Save/Apply**.

----End

◎—᷃ **TIP**

- Make sure enable auto synchronization with network time. If not, contact the Internet Service Provider.
- To delete a rule, select the rule from the rule list. In the **Remove** column, select the rule. Then click **Remove**.

7 Maintenance Guide

7.1 Changing the Administrator Password

Function Overview

You can configure all the parameters of the terminal 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 terminal 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 **VF-IRhg556**. When the default settings are restored, your customized data is lost. Therefore, use the RESET button with caution.

Configuration Example

The administrator password is **VF-IRhg556**. For example, to change the password to **MyWebPassword**, do as follows:

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

Step 2 Choose **Management** > **Access Control > User Management** in the navigation tree.

Step 3 Select **admin** from the **Username** drop-down list box.

Step 4 Enter the currently used password **VF-IRhg556** in **Old Password** text box.

Step 5 Enter the new password **MyWebPassword** in **New Password** text box. Enter the new password **MyWebPassword** again in **Confirm Password** text box.

Step 6 Click **Save/Apply**.

    ----End

7.2 Configuring the LAN Interface

To configure the LAN parameters, do as follows:

Step 1   Choose **Advanced Setup** > **LAN** in the navigation tree.

Step 2   Change the parameters refer to Table 7-1. Generally keep the default settings is OK.

Table 7-1 Parameters for the **Local Area Network (LAN) Setup** page

Parameter	Description
IP Address	It specifies the IP address of the LAN interface of the terminal. You can access the Web-based configuration utility of the terminal by using this IP address. If the DHCP function of the terminal is enabled, the terminal assigns an IP address that is in the same network segment as that of this interface to a computer. If the IP address of the LAN interface is changed, ensure that the IP address of the computer and the IP address of the LAN interface of the terminal are in the same network segment. In this case, you need to enter the new IP address in the address bar of an explorer.
Subnet Mask	It specifies the subnet mask of the LAN interface.
LAN Domain	It specifies the domain to enter the web Web-based configuration utility. The default LAN domain is **Vodafone.DSLRouter**. In this case, to access the Web-based configuration utility, you need to enter **Vodafone.DSLRouter** in the address bar of Internet Explorer.
LAN MTU:[296-1500]	The maximum length of the transported IP package of the LAN interface.
Enable IGMP Snooping	It specifies whether to enable the IGMP Snooping function of the terminal.
Enable/Disable DHCP Server	An IP address pool contains multiple consecutive IP addresses that can be assigned to the computers on the LAN. This parameter specifies the start IP address of the IP address pool.
Start/End IP Address	It specifies the end IP address of the IP address pool.
Leased Time (hour)	It specifies the period during which a computer on the LAN can use an assigned IP address.

Step 3   Click **Save** to save the LAN configuration. Click **Save/Reboot** to save the LAN configuration and reboot the terminal to make the new configuration effective.

----End

7.3 Backing Up or Updating a Configuration File

Function Overview

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

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 mis-operations, you can back up the configuration file of the terminal. Once the modification of the parameters fails, you can quickly restore the terminal 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   Choose **Management** > **Settings > Backup** in the navigation tree.

Step 3   Click **Backup Settings**.

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

    ----End

To update the configuration file, do as follows:

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

Step 2   Choose **Management** > **Settings > Update** in the navigation tree.

Step 3   Click **Browse**.

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

Step 5   Click **Update Settings**.

    ----End

7.4 Restoring Default Settings

Function Overview

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

When the terminal is powered on, press and hold the RESET button for more than 3s, and then release it. Then the terminal 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   Choose **Management** > **Settings > Restore Default** in the navigation tree.

Step 3   Click **Restore Default Settings**.

----End

7.5 Restarting the Terminal

Function Overview

The terminal provides restart function.

You can restart the terminal by using either of the following methods:

- Pressing the RESTART 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 wish to make it effective, you can press the RESTART button to quickly use the new password.

To restart the terminal through the web-based configuration utility, do as follows:

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

Step 2   Choose **Management** > **Save > Reboot** in the navigation tree.

Step 3   Click **Save/Reboot**.

----End

7.6 Updating Software

Function Overview

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

⚠ **CAUTION**

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

Configuration Example

You can download the latest software from your Internet Service Provider.

To update the software of the terminal, do as follows:

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

Step 2   Choose **Management** > **Update Software** in the navigation tree.

Step 3   Click **Browse**.

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

Step 5   Click **Update Software.**

   ----End

8 FAQs

Question 1: Can I use the terminal as a DHCP server?

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

Question 2: How can I quickly restore the default settings of the terminal?

To restore the default settings of the terminal, power on the terminal, press and hold the RESET button for a minimum of five seconds, and then release the RESET button.

Question 3: What can I do if I cannot access the terminal 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 terminal.

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 terminal configuration page.

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

----End

Question 4: What can I do if Web pages often cannot be displayed during Web page browsing and can be displayed after the terminal is restarted?

Step 1 Ensure that the terminal and other devices such as telephones or fax machines are connected to the telephone cable through a splitter.

For details about how to install a splitter, see the related description in the manual.

Step 2 Ensure that telephone cables are properly connected.

If the telephone cables are improperly connected, the stability of the network connection is affected.

Step 3 Check the positions of your terminal and computer. Ensure that they are far from the electric appliances such as microwave ovens, refrigerators, or cordless telephones that generate strong magnetic or electric fields.

If the problem persists, contact your service provider.

----End

Question 5: What can I do if noises exist during telephone calls?

Step 1 Ensure that a splitter is installed.

A splitter helps to protect the call quality of the asymmetric digital subscriber line (ADSL) from being affected due to the interference of other type of signals.

Step 2 Ensure that telephone cables are properly connected. Especially ensure that the telephone cable connecting to the splitter is properly connected.

Step 3 Replace telephone cables and ensure that the telephone cables are not faulty.

Step 4 Check the positions of your terminal and computer. Ensure that they are far from the electric appliances such as microwave ovens, refrigerators, or cordless telephones that generate strong magnetic or electric fields.

----End

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

Step 1 Ensure that the power cables and telephone cables of the terminal are properly connected.

Step 2 Check whether the Wi-Fi indicator of the terminal is on.

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

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

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, 802.11g and 802.11n protocols.

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

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

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

Step 7 Ensure that the PPP dialing software is properly installed and that the parameters of the software are correctly configured.

Step 8 Check whether you can use the PPP dialing software to dial successfully.

Step 9 Try to access multiple Web sites to check whether the terminal can access other Web sites.

If the terminal cannot access other Web sites either, restore the default settings of the terminal. If the problem persists, contact your Internet Service Provider.

----End

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

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

Step 2 Place your terminal in an open position.

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 terminal.

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

Step 4 Place your terminal and computer in another direction.

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

----End

Question 8: What can I do if the WLAN of the terminal 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

Huawei Proprietary and Confidential
Copyright © Huawei Technologies Co., Ltd.

Free Manuals Download Website

http://myh66.com

http://usermanuals.us

http://www.somanuals.com

http://www.4manuals.cc

http://www.manual-lib.com

http://www.404manual.com

http://www.luxmanual.com

http://aubethermostatmanual.com

Golf course search by state

http://golfingnear.com

Email search by domain

http://emailbydomain.com

Auto manuals search

http://auto.somanuals.com

TV manuals search

http://tv.somanuals.com