Welcome to use EchoLife BM635 WiMAX CPE!

EchoLife BM635 WiMAX CPE
V100R001

User Guide

Issue	01
Date	2008-06-15
Doc Number	00405273

Huawei Technologies Co., Ltd.

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

Website: http://www.huawei.com

Email: terminal@huawei.com

Trademarks and Permissions

and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute the warranty of any kind, express or implied.

Conventions

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 that, 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 that, if not avoided, could cause equipment damage, data loss, and 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

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`	Terminal display is in `Courier New`.

Command Conventions

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 | ... }	Alternative items are grouped in braces and separated by vertical bars. One is selected.
[x | y | ...]	Optional alternative items are grouped in square brackets and separated by vertical bars. One or none is selected.
{ x | y | ... } *	Alternative items are grouped in braces and separated by vertical bars. A minimum of one or a maximum of all can be selected.

GUI Conventions

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

Keyboard Operation

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 Operation

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.

Safety Precautions

General Requirements:

- Before you install and use the device, read these safety precautions carefully and observe them during operation.
- During storage, transportation and operation of the device, keep the device dry.
- During storage, transportation and operation of the device, avoid collision and crash of the device.
- Never attempt to dismantle the device by yourself. In case of any fault, contact the appointed maintenance center for repair.
- Without prior written consent, no organization or individual is permitted to make any change to the structure or safety design of the device. Huawei Technologies Co., Ltd. is not liable to any consequences or legal issues due to such changes.
- While using the device, observe all applicable laws, directives and regulations, and respect the legal rights of other people.

Environmental Requirements:

- Place the device at a well-ventilated place. Do not dispose the device to direct sunlight.
- Keep the device clean and free of dusts.
- Place the device on a stable platform.
- Do not place any object on top of the device. Otherwise, the device may be too hot during operation. It can even be deformed or damaged by the heavy load.
- Keep at least 10 cm between the device and the closest object for heat dissipation.。
- Do not place the device on or near any object that can easily catch fire, such as something made of rubber.
- Keep the device far away from any heat source or bare fire, such as a candle or an electric heater.
- Keep the device far away from any household appliance with strong magnetic field or electromagnetic field, such as a microwave oven, a refrigerator or a satellite dish antennas.

Operating Requirements:

- Do no let a child operate the device without guidance.

- Do not let a child play with the device or any accessory. Swallowing the accessories may lead to peril.
- Use only the accessories provided or authorized by the manufacturer only.
- The power supply of the device must meet the requirements of the input voltage of the device.
- Before plugging or unplugging any cable, shut down the device and disconnect it from the power supply.
- While plugging or unplugging any cable, make sure that your hands are completely dry.
- Do not tread on, pull or over-bend any cable. This can damage the cable and lead to malfunction of the device.
- Do not use an old or a damaged cable.
- During lightning weather, stop using the device and disconnect it from the power supply.
- If the device is not going to be used for a long time, disconnect it from the power supply and unplug the power plug.
- In any of the following cases, stop using the device, disconnect it from the power supply and unplug the power plug immediately: there is smoke emitting from the device, there is an abnormal noise or a foul smell. Contact the appointed maintenance center for repair.
- Ensure that no objects (such as metal shavings) are entering the device from the heat dissipation intakes.
- Do not scratch or abrade the surface of the device. This may affect the functioning of the device. The painting material shed while scratching the surface of the device can lead to skin allergy.

Cleaning Requirements:

- Before cleaning the device, power off the device and disconnect it from the power supply.
- Use a soft cloth to clean the device.
- Keep the power plug clean and dry. Using a dirty or wet power plug may lead to electric shock or other accidents.

Contents

Figures

Tables

1 Description

About This Chapter

The following table lists the contents of this chapter.

Section	Describes
1.1 Functions	Basic functions and featured performance of the BM635.
1.2 BM635 Appearance	The upper panel, rear panel, and side panel of the BM635.
1.3 Installing the BM635	Preparation before the BM635 is installed.

1.1 Functions

The EchoLife BM635 WiMAX CPE (hereinafter referred to as the BM635) is a next generation gateway device used in the Worldwide Interoperability for Microwave Access (WiMAX) network. The BM635 provides a new service experience for users. With the BM635, users can enjoy wireless broadband services. With the BM635, family and enterprise users can easily set up a network and enjoy the services over a wireless network.

Wireless Broadband Services

- Supporting Internet wireless access
- Supporting seamless connection, which enables users to access the network at any time and any place
- Guaranteeing network security with reliability

VoIP Service

- Supporting the Voice over IP (VoIP) service based on session initiation protocol (SIP)
- Supporting the voice compression technology
- Providing high quality voice services

Enhanced Throughput

- Supporting up to 10 Mbit/s downlink bandwidth and up to 3 Mbit/s uplink bandwidth
- Supporting multiple-input multiple-output (MIMO)
- Supporting orthogonal frequency division multiple access (OFDMA), which increases spectrum utilization

Various Services

- Providing four RJ45 ports and two RJ11 ports
- Providing a friendly Web UI and abundant help information
- Supporting both local and remote upgrade of the BM635

1.2 BM635 Appearance

1.2.1 Upper Panel

Figure 1-1 shows the upper panel of the BM635.

Figure 1-1 Upper panel of the BM635

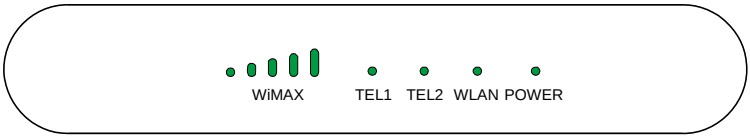


Table 1-1 lists the meanings of the indicators on the upper panel.

Table 1-1 Meanings of the indicators on the upper panel

Indicator	Status	Meaning
WiMAX	On	It indicates the signal strength of the WiMAX network. When the indicator illuminates in its full swing, it indicates that the highest signal strength is reached.
	Blinking	It indicates that the BM635 is being upgraded or the software is damaged.
	Off	It indicates that the BM635 cannot receive a signal from the WiMAX network.
TEL 1–2	On	It indicates that the TEL interface is being used.
	Blinking	It indicates that there is an incoming call from the TEL port.
	Off	It indicates that the phone connected to the TEL port hangs on or the TEL port is disabled.
WLAN	On	It indicates that the WLAN function is enabled.
	Blinking	It indicates that data is being transmitted.
	Off	It indicates that the WLAN function is disabled.
POWER	On	It indicates that the BM635 is powered on.

1.2.2 Rear Panel

Figure 1-2 shows the rear panel of the BM635.

Figure 1-2 Rear panel of the BM635

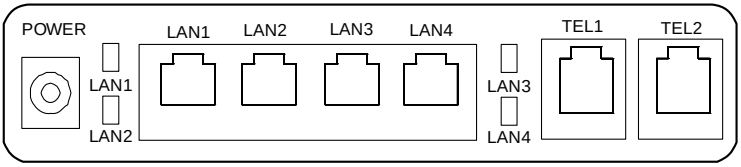


Table 1-2 lists the functions of the ports on the rear panel.

Table 1-2 Ports on the rear panel

Port/Button	Description
POWER	Power port
LAN1–4	It is the Ethernet port that is connected to a computer or switch. It indicates the operating status of the Ethernet port.
TEL1–2	It is connected to the phone line.
Note: LAN: local area network	

1.2.3 Side Panel

Figure 1-3 shows the side panel of the BM635.

Figure 1-3 Side panel of the BM635

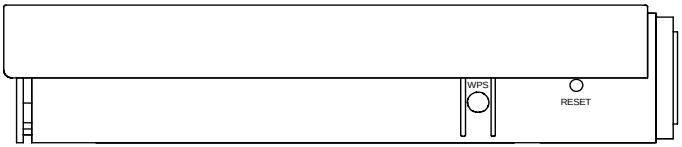


Table 1-3 lists the functions of the buttons on the side panel.

Table 1-3 Buttons on the side panel

Button	Description
WPS	Press this button to enable or disable the WLAN function.

Button	Description
RESET	Press and hold the button for one second to eight seconds to reboot the BM635. Press and hold this button for over eight seconds to restore the carrier settings of the BM635. **Once you restore the carrier settings, all the customized data will be lost. Use this function with caution.**
Note: WPS: Wi-Fi protected setup	

NOTE

The schematic diagram of the side panel is turned anticlockwise at 90 degrees.

1.3 Installing the BM635

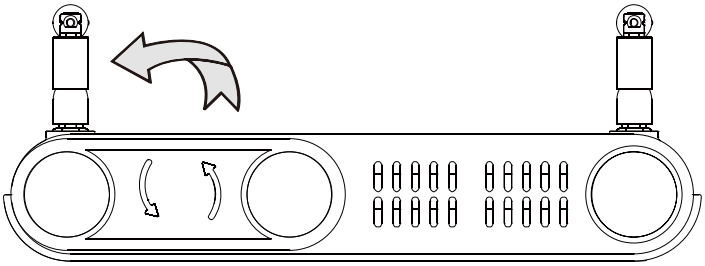
1.3.1 Selecting the Installation Environment

- The obstacles, such as a cement wall and a wooden wall affect signal transmission of the WiMAX network. An open place is recommended for installing the BM635.
- Place the BM635 far away from an electrical device that produces a strong magnetic field or strong electric field, such as a microwave oven, a fridge and a satellite dish antenna.

1.3.2 Rotating the Base

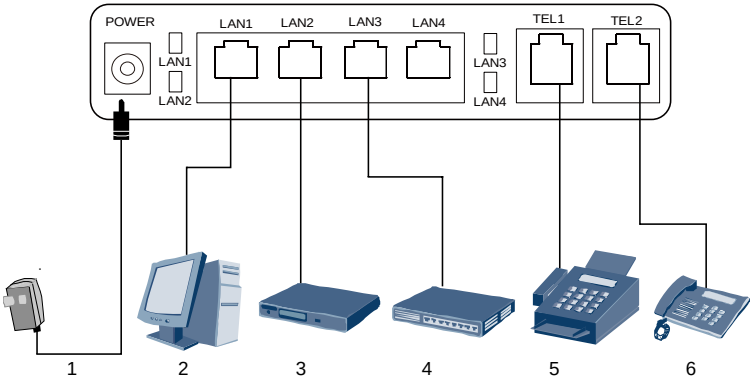
Rotate the supports on the base of the BM635 anticlockwise at 90 degrees so that the supports are vertical to the BM635, as shown in Figure 1-4.

Figure 1-4 Schematic diagram of rotating the base



1.3.3 Connecting Cables

Figure 1-5 Cable connection diagram of the BM635



1	Power adapter	2	Computer	3	Set top box
4	Switch	5	Fax	6	Phone

Use the cables and power adapters delivered with the BM635.

The schematic diagram of the cable connection is for reference only. You only need to connect a required device to the BM635.

When the cables are connected correctly, the BM635 will search the WiMAX network automatically, and can be used after the network is connected successfully.

2 Configuring the Network

About This Chapter

The following table lists the contents of this chapter.

Section	Describes
2.1 Logging in to the Web UI	How to set the parameters for logging in to the Web UI.
2.2 Configuring a WAN	How to set the parameters on the WAN side.
2.3 Configuring a LAN	How to set the parameters on the LAN side.

2.1 Logging in to the Web UI

Before configuring the network, log in to the Web UI. Take the Windows XP operating system and the Internet Explorer 6.0 as examples.

Perform the following steps to log in to the Web UI.

Step 1 Configure the IP address of the computer so that the IP address of the computer and the IP address of the BM635 are in the same network segment.

Note:

By default, the IP address of the BM635 is 192.168.1.1 and the subnet mask is 255.255.255.0. For example, you can set the IP address of the computer to 192.168.1.100 and the subnet mask to 255.255.255.0.

Step 2 Open the Internet Explorer, enter **http://192.168.1.1** in the address bar, and then press **Enter**.

Step 3 Enter the user name and the password in the login interface that is displayed, and then click **Login**.

Note:

The initial user name is **admin** and the corresponding password is also **admin**.

Step 4 After the authentication of the user name and the password succeeds, log in to the Web UI.

----End

2.2 Configuring a WAN

When you configure a WAN, the BM635 can act as a routing device or bridge device. With the BM635, a terminal at the LAN side is connected to the network.

- In routing mode, the BM635 acts as a routing device to connect to the network. Based on packet information, the BM635 searches for a route over which the packets are sent to the destination IP address.
- In bridge mode, the BM635 acts as a bridge device to connect to the network. The BM635 only transparent transmit packets.

Three modes of obtaining an IP address are available for the BM635:

- Dynamic Host Configuration Protocol (DHCP) mode: The IP address is obtained from the Internet service provider (ISP).
- Static IP address mode: The ISP configures a static IP address.
- Point-to-Point Protocol over Ethernet (PPPoE) mode: The IP address is obtained by PPPoE dialup.

2.2.1 Configuring the Routing Mode

Configuring the DHCP Routing Mode

Step 1 In the navigation tree, choose **Basic** > **WAN**, and then click the **WAN** tab.

Step 2 Select **Route** from **Mode**.

Step 3 Select **DHCP Auto get IP address from ISP**.

Step 4 Select whether to enable the network address transmission (NAT) function, if enable, the NAPT type is recommended.

Note:

When the NAT function is enabled to facilitate translation of IP addresses, the host IP address of LAN can be effectively hidden. Thus, the security of the intranet is ensured. Two NAT modes are available:

- network address port translation (NAPT)
- CONE NAT

Step 5 Click **Apply**.

----End

Configuring the Static IP Routing Mode

Step 1 In the navigation tree, choose **Basic** > **WAN**, and then click the **WAN** tab.

Step 2 Select **Route** from **Mode**.

Step 3 Select **Static Get static IP address from ISP**.

Step 4 Select whether to enable the network address transmission (NAT) function, if enable, the NAPT type is recommended.

Note:

When the NAT function is enabled to facilitate translation of IP addresses, the host IP address of LAN can be effectively hidden. Thus, the security of the intranet is ensured. Two NAT modes are available:

- network address port translation (NAPT)
- CONE NAT

Step 5 Enter the IP address in the **IP Address** text box.

Step 6 Enter the BM635 subnet mask in the **Subnet Mask** text box.

Step 7 Enter the BM635 default gateway in the **Default Gateway** text box.

Step 8 Enter the IP address of primary domain name server (DNS) in the **Primary DNS Server** text box.

Step 9 Enter the IP address of secondary DNS in the **Secondary DNS Server** text box.

Note:

IP Address, Subnet Mask, Default Gateway, Primary DNS Server, Secondary DNS Server is supplied by the carrier.

Step 10 Click **Apply**.

----End

Configuring the PPPoE Routing Mode

Step 1 In the navigation tree, choose **Basic** > **WAN**, and then click the **WAN** tab.

Step 2 Select **Route** from **Mode**.

Step 3 Select **PPPoE Get IP Address by using PPPoE**.

Step 4 Select whether to enable the network address transmission (NAT) function, if enable, the NAPT type is recommended.

Note:

When the NAT function is enabled to facilitate translation of IP addresses, the host IP address of LAN can be effectively hidden. Thus, the security of the intranet is ensured. Two NAT modes are available:

- network address port translation (NAPT)
- CONE NAT

Step 5 Enter the user name in the **UserName** text box.

Step 6 Enter the password in the **Password** text box.

Step 7 Select the dial method in the **Dial Method**.

Note:

Two dial types are available: Auto Dial and Manual Dial. If you select the Manual Dial type, please click the **Manual Dial** to dial.

Step 8 Click **Apply**.

----End

2.2.2 Configuring the Bridge Mode

The configuration of the bridge mode is similar to that of the routing mode. The difference between them lies in the necessity of selecting the bridge type for configuring the bridge mode.

- IP_Bridged: This option is recommended when the way of obtaining an IP address is DHCP mode or static IP mode.
- PPPoE_Bridged: This option is recommended when the way of obtaining an IP address is PPPoE mode.

Step 1 In the navigation tree, choose **Basic** > **WAN**, and then click the **WAN** tab.

Step 2 Select **Bridge** from **Mode**.

Step 3 For the details on how to set parameters, see section2.2.1 "Configuring the Routing Mode".

----End

2.3 Configuring a LAN

To configure an LAN, set DHCP parameters. After DHCP is enabled, the BM635 allocates an IP address pool to the network device at the LAN side.

Step 1 In the navigation tree, choose **Basic** > **LAN**, and then click the **DHCP** tab.

Step 2 Enter the BM635 IP address in the **IP Address** text box, for example, 192.168.1.1.

Step 3 Enter the BM635 subnet mask in the **Subnet Mask** text box, for example, 255.255.255.0.

Step 4 Click **Apply**.

Step 5 Select **Enable DHCP Server**.

Step 6 Enter the start IP address at the LAN side in the **Start IP Address** text box, for example, 192.168.1.2.

Step 7 Enter the end IP address at the LAN side in the **End IP Address** text box, for example, 192.168.1.254.

Step 8 Select the lease of the address from the **Lease (unit)**. The system automatically leases the address in advance according to the specified lease.

Step 9 Select the device type in the **Device Type**.

Step 10 Enter the start IP address of the selected device type in the **Start IP Address** text box.

Step 11 Enter the end IP address of the selected device type in the **End IP Address** text box.

Step 10 Select whether to enable the **DHCP relay** function.

Step 11 Click **Apply**.

----End

3 Configuring Basic Functions

About This Chapter

The following table lists the contents of this chapter.

Section	Describes
3.1 Configuring a WLAN	How to set WLAN parameters.
3.2 Configuring VoIP	How to set VoIP parameters.
3.3 Configuring RIP	How to set RIP parameters.
3.4 Configuring QoS	How to set QoS parameters.

3.1 Configuring a WLAN

A wireless local area network (WLAN) is set up based on wireless communication technologies without any cables. The setup of the WLAN is simple. With the WLAN function, the BM635 enables users to access the broadband network at any time and any place within the WLAN coverage area in addition to the provisioning of the legacy wired LAN services.

3.1.1 Configuring Basic WLAN Parameters

In the navigation tree, choose **Basic** > **LAN**, and then click the **WLAN** tab.

Select **Enable Wireless** to enable WLAN.

Parameter	Description
Mode	Three wireless network modes are available: • **802.11b** • **802.11g** • **802.11b/g** The default value is **802.11b/g**.
Regulatory Domain	Select the wireless standards of different countries, the default value is **US-UNITED STATES**.
Channel	It indicates the WLAN channel. The default value is **Auto**.
Rate	It indicates the rate of the specified channel. The default value is **Auto**.
Transmit Power	It indicates the transmit power. The more the transmit power, the larger the coverage area of the wireless network of the BM635. The value ranges from 1 dBm to 14 dBm. The default value is **14dm**.
Fragmentation Threshold	Set the size of the fragmentation field. The value ranges from 0B to 2345B. The default value is **2345B**.
Beacon Interval	Set the interval of the transmit frame. The value ranges from 1ms to 1000ms. The default value is **100ms**.
RTS/CTS Threshold	Set the duration of the subsequent frame and response frame. The value ranges from 0B to 1000B. The default value is **0B** (It means that this function is not enabled). **Note:** The wireless access device can be set as always use RTS/CTS, never use RTS/CTS, or use RTS/CTS when the frame length exceeds the threshold.
SSID Index	It indicates the SSID index.
SSID	It indicates the SSID name.

Maximum Associate Device Number	It indicates the maximum number of wireless devices to be connected. The value ranges from 1 to 32.
SSID Enable	It indicates whether to enable SSID device access.
Hide Broadcast	It indicates whether to enable SSID broadcast.
Note: SSID = service set identifier	

3.1.2 Configuring WLAN Security Parameters

In the **WLAN** tab, **Security Configure** provides four security modes: wired equivalent privacy (**WEP**), Wi-Fi protected access pre-shared key (**WPA-PSK**), Wi-Fi protected access 2 (**WPA2-PSK**), and **Mixed WPA2/WPA-PSK**.

You can select one of the following according to the network configuration:

- **WEP**: It indicates that the data transmitted wirelessly is encrypted according to the set encryption parameters.
- **WPA-PSK**: It indicates the simplified WPA authentication mode. The special authentication server is not required. To encrypt data, enter the secret key only.
- **WPA2-PSK**: It indicates the simplified WPA2 authentication mode. It supports the IEEE 802.11i Wi-Fi standard.
- **Mixed WPA2/WPA-PSK**: It indicates that support both WPA-PSK and WPA2-PSK authentication mode.

NOTE

No matter which security mode you select, ensure that the setting of the security mode parameter of the wireless access device is consistent with that of the security mode parameter of the BM635.

Configuring the WEP Security Mode

Parameter	Description
WEP Encryption	It indicates whether to enable the WEP encryption. • **Enable**: It indicates that the shared authentication mode based on WEP encryption is enabled. All the data transmitted over the wireless LAN is encrypted according to the encryption parameters defined by users. • **Disable**: It indicates that the open authentication mode without encryption is enabled. All the data transmitted over the wireless LAN is not encrypted.
Encryption key Length	It indicates the length of the encryption key.

Current Encryption Index	It indicates the encryption key index used currently.
Encryption key1~4	It indicates the encryption key.

Configuring the WPA-PSK, WPA2-PSK, Mixed WPA2/WPA-PSK Security Mode

Parameter	Description
WPA PreShared key	It indicates the pre-shared WPA key for authentication.
WPA Encryption	It indicates the WPA encryption mode. Three options are available: • TKIP • AES • TKIP+AES
Note: TKIP = Temporal Key Integrity Protocol; AES = Advanced Encryption Standard	

3.1.3 Configuring a WLAN Filter

You can enable or disable the WLAN function of the wireless access device according to the configured filtering mode.

Step 1 In the navigation tree, choose **Basic** > **LAN**, and then click the **WLAN Filter** tab.

Step 2 Select the **Enable WLAN MAC Filter** to enable the MAC address filter function.

Step 3 Select the **Black** or **White** filter mode.

NOTE

- Black: It indicates that the black list member does not have the corresponding rights.
- White: It indicates that the white list member has the corresponding rights.

Step 4 Enter the source MAC address in the **Source MAC Address** text box.

Step 5 Click **Apply**.

NOTE

Select a MAC address in the **Wireless Filter** list, and click **Remove** to delete the selected MAC address.

----End

3.2 Configuring VoIP

As the voice service based on SIP, VoIP enables users to make Internet phone calls and fax data.

As an application layer protocol, SIP is used for setting up, modifying, or completing a multimedia session.

3.2.1 Configuring basic VoIP function

Step 1 In the navigation tree, choose **Basic** > **VoIP**, and then click the **SIP User** tab.

Step 2 Enter the new ID, which is the telephone number in the **SIP ID** text box, and then click the **Check** button to verify the validity of the ID.

Step 3 Enter the username provided by the carrier in the **Username** text box.

Step 4 Enter the password provided by the carrier in the **Password** text box.

Step 5 Enter the port number in the **SIP Local Port** text box, for example, 6050. The value ranges from 1 to 65534.

Step 6 Select the correct caller identification display type from the **Caller Number Display Type**, for example, Display.

Step 7 Select whether to enable message waiting in the S**elect Message Waiting Indication Service**. When you enable the function, you need to enter the Uniform Resource Identifier (URI) in the **Message Waiting Indication Service Subscribe URI** text box.

Step 8 Click **Apply** to save the settings.

Step 9 Click the **SIP Server** tab.

Step 10 Select the correct interface name from the **InterfaceName**.

Step 11 Select the server type from the **Server**. Two options are available: **Primary server** and **Secondary server**.

Step 12 Enter the proxy server address in the **SIP Proxy Server Address** text box, for example 192.168.1.10.

Step 13 Enter the proxy server port in the **SIP Proxy Server Port** text box, for example, 5060. The value ranges from 1 to 65535.

Step 14 Enter the register server address in the **SIP Register Server Address** text box, for example 192.168.1.11.

Step 15 Enter the register server port in the **SIP Register Server Port** text box, for example, 5060. The value ranges from 1 to 65535.

Step 16 Enter the domain name of the SIP server in the **SIP Service Domain** text box.

Step 17 Click **Apply** to save the settings.

Note:

- Select a SIP ID to be modified, modify it, and then click **Apply**.
- Select **Remove** to delete the selected SIP ID. After they are removed, if you want to use the SIP ID, you need to create a SIP ID first.

----End

3.2.2 Configuring advance VoIP functions

Configuring Port

In the navigation tree, choose **Basic** > **VoIP**, and then click the **Port** tab.

Select a port ID to check the port information. Click **Modify** to modify the port attributes.

Parameter	Description
Inter Number	It indicates the short number of an internal VoIP call.
Note Information	It indicates the prompt of the corresponding internal short number.
Route Setting	It indicates the routing mode.
Associated SIP ID	It indicates the SIP ID bundled with the phone port.

Configuring Speed Dial

In the navigation tree, choose **Basic** > **VoIP**, and then click the **Speed Dial** tab.

Parameter	Description
Dial Number	It indicates the speed dial number.
Note	It indicates the prompt of the speed dial.
Real Number	It indicates the real phone number of the speed dial.

Click **Modify** to modify the selected speed dial.

Select **Remove** to delete the selected speed dial. Click **Remove All** to remove all speed dials. After they are removed, if you want to use the speed dial function, you need to create a speed dial number first.

Configuring SIP Advanced

In the navigation tree, choose **Advanced > VoIP**, and then click the **SIP Advanced** tab.

Parameter	Description
Expiration Duration	It indicates the validity period of registration. The value ranges from 20s to 65535s.
Register Re-send Timer	It indicates the validity period of re-sending registration. The value ranges from 1s to 65535s.
Session Expires	It indicates the validity period of a server session. The value ranges from 30s to 3600s.

Parameter	Description
Min-Session Expires	It indicates the shortest validity period of a server session. The value ranges from 20s to 1800s.
MWI Expires	It indicates the time for updating the MWI. The value ranges from 20s to 65535s.
Call-Waiting	It indicates whether to enable call waiting.
Conference	It indicates whether to enable the three-party service.
100rel Support	It indicates whether to enable real-time acknowledgement of a replay.
Urgency Use Priority	It indicates whether to enable an urgency call.
Hold Method	It indicates a call hold mode.
Dialing Interval	After you enter a number and wait for a certain interval, the entered number will be dialed automatically. The interval can be 5s, 10s, or 15s.
Note: MWI = message waiting indication	

Configuring Phone

In the navigation tree, choose **Advanced** > **VoIP**, and then click the **Phone** tab.

Parameter	Description
Transmit Gain	It specifies the volume of the telephone transmitter. The greater the parameter value is, the higher the volume is. Select a proper value.
Receive Gain	It specifies the volume of the telephone receiver. The greater the parameter value is, the higher the volume is. Select a proper value.
Echo Cancellation Enable	It indicates whether to enable echo cancellation. If echo cancellation is enabled, voice quality can be improved.
Auto Gain	It indicates whether to enable automatic gain.
Transmit Silence Suppression	It indicates whether to enable the silence suppression function of the voice service.
Transmit Packetization Period	It indicates the period for packetization.

Configuring Voice Codec

In the navigation tree, choose **Advanced** > **VoIP**, and then click the **Voice Codec** tab.

Parameter	Description
Primary Compression Type	It indicates the primary voice codec type. The default value is **G.711-PCMA**.
Secondary Compression Type	It indicates the secondary voice codec type. The default value is **G.711-PCMU**.
Third Compression Type	It indicates the third voice codec type. The default value is **G.726-32**.
Fourth Compression Type	It indicates the fourth voice codec type. The default value is **G.726-24**.
Fifth Compression Type	It indicates the fifth voice codec type. The default value is recommended.

Configuring Voice

In the navigation tree, choose **Advanced** > **VoIP**, and then click the **Voice** tab.

Parameter	Description
DTMF Method	It indicates the mode of DTMF transmission.
Region Settings	It indicates the country or region code.
Fax Option	It indicates the fax mode.
RTP Start Port	It indicates the RTP port number. The value is an even number ranging from 50000 to 65514.
Comfort Noise Generation	It indicates whether to enable comfort noise generation.
Jitter Buffer	It indicates whether to enable jitter buffer.
Jitter Buffer Length	It indicates the jitter buffer size. The value ranges from 20 to 1000.
Pack Lost Compensate	It indicates whether to enable packet loss compensation.
Jitter Buffer Type	It indicates the jitter buffer type.

Note:

DTMF = dual tone multi-frequency; RTP = Real-Time Transfer Protocol

3.3 Configuring RIP

Route is used to configure routes and forward packets. Routing Information Protocol (RIP) is used to automatically set parameters of a route. RIP is applied to set up a network with a complicated topology structure. The maintenance of a RIP network is simple.

Step 1 In the navigation tree, choose **Advanced > RIP**, and then click the **RIP** tab.

Step 2 Select an interface from **Interface**.

Step 3 Select an operation status from **Operation**.

Step 4 Select a version from **Version**.

Step 5 Click **Apply**.

----End

3.4 Configuring QoS

The quality of service (QoS) varies with the requirements of network applications.

Step 1 In the navigation tree, choose **Advanced > QoS**, and then click the **QoS** tab.

Step 2 The **Interface Name** list all interface names, enter the Differentiated Services Code Point (DSCP) in the **DSCP** text box.

Step 3 Select the priority of interface from the **Priority**.

Note:

- The priority is from one to five, one level is the highest priority.
- The priority of **local** cannot be modified.

Step 4 Click **Apply**.

----End

4 Configuring Advanced Functions

About This Chapter

The following table lists the contents of this chapter.

Section	Describes
4.1 Configuring the WiMAX Network	How to set WiMAX network parameters.
4.2 Configuring the NAT	How to set NAT parameters.
4.3 Configuring the ACL	How to set ACL parameters.
4.4 Configuring the SNTP	How to set SNTP parameters.
4.5 Configuring the Security	How to set Security parameters.

4.1 Configuring the WiMAX Network

In a WiMAX network, a subscriber station (SS) or mobile station (MS) can communicate with the base station (BS) after the WiMAX network parameters are properly set. After network parameters are properly set, an available connection can be set up between the BM635 and the WiMAX BS.

4.1.1 Configuring WiMAX Frequencies

Before you configure the network frequency point, you need to configure the network bandwidth. There are two types of bandwidth such as 5 M and 10 M. You are recommended to use the default bandwidth.

Step 1 In the navigation tree, choose **WiMAX** > **Scanset**, and then click the **Scanset** tab.

Step 2 Select the bandwidth from the **Working Bandwidth**.

Step 3 Click **Save**.

----End

After the bandwidth set correctly, then set the WiMAX frequency. The following frequency scanning modes are available:

- Smart scan mode: According to the specified start frequency, end frequency, and frequency step, the BM635 determines the range of frequency that can be searched for and searches for a frequency.
- Expert scan mode: The BM635 searches for the specified frequency only.

Smart Scan Mode

Parameter	Description
Frequency Step	It indicates the step of frequency scanning in smart scan mode.
Start frequency	It indicates the start frequency to be scanned in smart scan mode.
End frequency	It indicates the end frequency to be scanned in smart scan mode.

Expert Scan Mode

Parameter	Description
DL Frequency 1~10	It indicates the frequency to be scanned in expert scan mode. You can enter up to 10 frequencies to be scanned.

4.1.2 Configuring WiMAX Security Parameters

By configuring the security authentication mode and importing a certificate, you can finish the settings of the WiMAX security parameters.

Configuring the Security Authentication Mode

In the navigation tree, choose **WiMAX** > **Security**, and then click the **Security** tab.

The parameter description is as follows.

Parameter	Description
PKM	It indicates whether authentication is required during network access. There are two authentication modes: • NO PKM • PKMv2_EAP
Authentication	It indicates the authentication type. There are two authentication types: • TLS: It indicates device authentication. • TTLS: It indicates user authentication.
NAI	It indicates the NAI. The default value is **1E:CA:FE:00:00:00@huawei.com**.
User ID	It indicates the user ID provided by the ISP.
User Password	It indicates the user password provided by the ISP.
Note: EAP = Extensible Authentication Protocol; NAI = network access identifier PKM = Privacy key management; TLS = Transport layer security protocol TTLS = Tunneled transport layer security protocol	

Importing a Certificate

The certificate includes a personal certificate, a personal private key, and a certification authority (CA) root certificate. Each certificate can be uploaded to the server.

CAUTION

- Modify a certificate with caution, because improper modification may cause the BM635 to improperly operate.
- Do not modify the suffix of a certificate at will.

Functions of each certificate are as follows:

- Personal certificate: It indicates the certificate uploaded to the Authorization, Authentication and Accounting (AAA) server when the BM635 is authenticated.
- Personal private key: It indicates the personal private key allocated by the server to a BM635. This key is used together with a personal certificate.
- CA root certificate: It indicates the root certificate that is used to verify the AAA server at the front end.

Click **Browse** to select the correct corresponding certificate, and upload to the BM635.

4.2 Configuring the NAT

NAT is used to convert an IP address and a port so that the device on the LAN side uses an IP address of the same public network to access the network at the WAN side.

4.2.1 Configuring the ALG

Application layer gateway (ALG) is used to convert the specified data carried in IP packets, thus supporting LAN applications in the process of transmitting the packets on the LAN side and the packets at the WAN side.

In the navigation tree, choose **Advanced** > **NAT**, and then click the **ALG** tab.

Parameter	Description
Enable L2TP ALG	It indicates whether to enable L2TP ALG.
Enable IPSec ALG	It indicates whether to enable IPSec ALG.
Enable H.323 ALG	It indicates whether to enable H.323 ALG.
Enable RTSP ALG	It indicates whether to enable RTSP ALG.
Enable SIP ALG	It indicates whether to enable SIP ALG. After SIP ALG is enabled, enter the SIP port number.

Note:

L2TP = Layer 2 Tunneling Protocol; IPSec = IP Security Protocol; RTSP = Real-Time Streaming Protocol

4.2.2 Configuring the DMZ

Demilitarized zone (DMZ) is used to forward the packets from the WAN without port mapping to the host defined in the DMZ.

In the navigation tree, choose **Advanced** > **NAT**, and then click the **DMZ** tab.

Parameter	Description
Host Address	It indicates the host IP address.

Parameter	Description
Enable DMZ	It indicates whether to enable the DMZ.

4.2.3 Configuring Port Mapping

Port mapping supports the mapping between the interfaces at the WAN side and the interfaces at the LAN side. Up to 32 port mapping rules can be defined.

Adding Port Mapping

In the navigation tree, choose **Advanced** > **NAT**, and then click the **Port Mapping** tab.

Two port mapping modes are available:

- **Custom**: It indicates the self-defined mode.
- **Application**: It indicates the mode provided by the system.

When selecting **Custom**, you must set the following parameters.

Parameter	Description
Interface	It indicates the interface type.
Protocol	It indicates the interface protocol.
External Port	It indicates the external port number.
Internal Port	It indicates the internal port number.
Internal Host	It indicates the IP address of the internal host.
Source IP Address	It indicates the source host IP address.
Mapping Name	It indicates the mapping name.

When you select **Application**, the system displays values of all parameters. You can keep the default values or modify them.

Deleting Port Mapping

Select the mapping name to be deleted, and then click **Remove**.

4.2.4 Configuring a Port Trigger

During remote access, the specified port of the firewall on the router must be enabled for certain applications. Port trigger is used to set up a new connection between the remote applications at the WAN side and the applications at the LAN side that require the use of certain ports. Up to 32 port trigger rules can be defined.

Adding a Port Trigger

In the navigation tree, choose **Advanced** > **NAT**, and then click the **Port Trigger** tab.

Two port mapping modes are available:

- **Custom**: It indicates the self-defined mode.
- **Application**: It indicates the mode provided by the system.

When selecting **Custom**, you must set the following parameters.

Parameter	Description
Trigger Protocol	It indicates the protocol type.
Interface	It indicates the interface type.
Trigger Start Port	It indicates the start port number.
Trigger End Port	It indicates the end port number.
Open Start Port	It indicates the open start port number.
Open End Port	It indicates the open end port number.
Trigger Description	It indicates the new rule name.

When you select **Application**, the system displays values of all parameters. You can keep the default values or modify them.

Deleting a Port Trigger

Select the trigger name to be deleted, and then click **Remove**.

4.3 Configuring the ACL

Access control list (ACL) guarantees QoSs of File Transfer Protocol (FTP), Hypertext Transfer Protocol (HTTP), Telnet, and Secure Shell (SSH) services. By controlling and managing packets, ACL increases utilization of network links, limits network traffic, and enhances network performance.

Step 1 In the navigation tree, choose **Advanced** > **ACL**, and then click the **ACL** tab.

Step 2 The ACL of a service can be enabled or disabled.

Step 3 Click **Apply**.

----End

4.4 Configuring the SNTP

Simple Network Time Protocol (SNTP) is used to synchronize network time.

Step 1 In the navigation tree, choose **Advanced** > **SNTP**, and then click the **SNTP** tab.

Step 2 Select the **Auto Synchronization Network Time Server** check box.

Step 3 Select an option respectively from **Primary SNTP Server**, **Secondary SNTP Server**, and **Time Zone**.

Note:

If **Primary SNTP Server** and **Secondary SNTP Server** drop-down list boxes do not contain the required options, enter the server names in the text boxes.

Step 4 Click **Apply**.

----End

4.5 Configuring the Security

The security function is used to control the rights of sending and receiving packets and the period for accessing the network.

Two options are available:

- **Black**: It indicates that the black list member does not have the corresponding rights.
- **White**: It indicates that the white list member has the corresponding rights.

4.5.1 Configuring the URL Filter

The universal resource locator (URL) filter is used to prevent a network device at the LAN side to access certain web sites at the WAN side.

Adding a URL Filter Rule

Step 1 In the navigation tree, choose **Advanced** > **Security**, and then click the **URL Filter** tab.

Step 2 Select **Enable URL Filter** to enable the URL filter.

Step 3 Select **Black** or **White**.

Step 4 Click **New**.

Step 5 Enter an address in **URL**.

Step 6 Click **Apply**.

----End

Modifying a URL Filter Rule

Select a URL filter rule to be modified, modify it, and then click **Apply**.

Deleting a URL Filter Rule

Select the URL filter rule to be deleted, and then click **Remove**.

4.5.2 Configuring a MAC Filter

The MAC filter can filter data frames according to the defined filter rule. The filter takes effect only when all conditions of the filter rule are met.

Adding a MAC Filter Rule

Step 1 In the navigation tree, choose **Advanced** > **Security**, and then click the **MAC Filter** tab.

Step 2 Select **Enable MAC Filter** to enable the MAC filter.

Step 3 Select **Black** or **White**.

Step 4 Click **New**.

Step 5 Set the following parameters of the MAC filter rule.

Parameter	Description
Filter Name	It indicates the MAC filter rule name.
Source MAC Address	It indicates the source host MAC address.
Destination MAC Address	It indicates the destination host MAC address.
Start Time	It indicates the effective time of a rule, in the format of hh: mm.
End Time	It indicates the expiration time of a rule, in the format of hh: mm.
Day	It indicates the effective date of a rule.
Enable	It indicates whether to use this rule.

Step 6 Click **Apply**.

----End

Modifying a MAC Filter Rule

Select a MAC filter rule to be modified, modify it, and then click **Apply**.

Deleting a MAC Filter Rule

Select the MAC filter rule to be deleted, and then click **Remove**.

4.5.3 Configuring an IP Incoming Filter

When the firewall is enabled, the IP incoming filter can be used to receive certain specified IP packets at the WAN side.

Adding an IP Incoming Filter Rule

Step 1 In the navigation tree, choose **Advanced** > **Security**, and then click the **IP Incoming** tab.

Step 2 Select **Enable IP Incoming Filter** to enable the IP incoming filter.

Step 3 Click **New**.

Step 4 Set the following parameters of the IP incoming filter rule.

Parameter	Description
Filter Name	It indicates the name of an IP incoming filter rule.
Protocol	It indicates a protocol type.
Enable	It indicates whether to use this rule.
Source Start Address	It indicates the start IP address of the source host.
Source End Address	It indicates the end IP address of the source host.
Source Start Port	It indicates the start port number of the source host.
Source End Port	It indicates the end port number of the source host.
Destination Start Address	It indicates the start IP address of the destination host.
Destination End Address	It indicates the end IP address of the destination host.
Destination Start Port	It indicates the start port number of the destination host.
Destination End Port	It indicates the end port number of the destination host.
Interface	It indicates the interface type.

Step 5 Click **Apply**.

----End

Modifying an IP Incoming Filter Rule

Select an IP incoming filter rule to be modified, modify it, and then click **Apply**.

Deleting an IP Incoming Filter Rule

Select the IP incoming filter rule to be deleted, and then click **Remove**.

4.5.4 Configuring an IP Outgoing Filter

The IP outgoing filter is used to prevent the LAN side from sending certain IP packets.

The configuration of an IP outgoing filter rule is the same as that of an IP incoming filter rule. For detailed parameter settings, see section 4.5.3 "Configuring an IP Incoming Filter"

4.5.5 Configuring the Firewall

The firewall is used to prevent the protected network from the unauthorized or unverified access from the Internet. Users of an intranet are allowed to access the Internet.

In the navigation tree, choose **Advanced** > **Security**, and then click the **Firewall** tab.

Select a firewall level from **Security Level**.

The meanings of options are as follows:

- **Off**: It indicates that the firewall is disabled.
- **Low**: It indicates that the firewall acts as a state firewall. The firewall prevents port scan and IP address spoofing, but allows both ping operation and Internet Control Message Protocol (ICMP) redirection packet at the WAN side.
- **Middle**: Besides preventing port scan and IP address spoofing, the firewall prevents ICMP redirection packets.
- **High**: Besides preventing port scanning, IP address spoofing, and ICMP redirection packets, the firewall prevents the synchronous idle character (SYN) flood attack and the ping operation at the WAN side.

5 Managing the BM635

About This Chapter

The following table lists the contents of this chapter.

Section	Describes
5.1 Managing User Passwords	How to modify a user password.
5.2 Managing Logs of the BM635	How to manage logs of the BM635.
5.3 Managing Configuration Files	How to upload and download the configuration file of the BM635.
5.4 Rebooting the BM635	How to reboot the BM635.
5.5 Upgrading the Software	How to upgrade the software of the BM635.
5.6 Restoring Carrier Settings	How to restore carrier settings of the BM635.

5.1 Managing User Passwords

A user password is used to allow a user to set network parameters. The password is classified into two levels: admin and user. After the admin user log in to the BM635, you can modify the two level passwords and must keep the new password in mind.

If you forget the password, you can restore factory settings of the BM635 to validate the initial password or contact the local carrier.

Perform the following steps to modify a user password:

Step 1 In the navigation tree, choose **Maintain** > **Account**, and then click the **Account** tab.

Step 2 Select a user name from **Username**.

Step 3 Enter the user information follow the prompts.

Note:

- To change an admin password, you need to enter the original password and you cannot change the user name.
- To change a user password, you are not required to enter the original password and you can change the user name.

Step 4 Click **Apply**.

-----End

5.2 Managing Logs of the BM635

After you enable log management of the BM635, the BM635 starts to record the events of the specified log type. You can check various levels of system logs in real time.

Starting Log Management

Step 1 In the navigation tree, choose **Maintain** > **LOG**, and then click the **LOG** tab.

Step 2 Select **Enable** to enable log management.

Step 3 Select a log level from the **Log Level**.

NOTE

After you select a log level, the system displays the information on the logs at and below this level. For example, after you select **Error** from **Log Level**, the system records the information on the logs at **Error**, **Critical**, **Alert**, and **Fatal** levels.

Step 4 Click **Apply**.

----End

Checking Logs

Step 1 In the navigation tree, choose **Maintain** > **LOG**, and then click the **LOG Display** tab.

Step 2 Select a log level from **Display Level**.

The text box below displays the information on the logs at the specified level.

----End

5.3 Managing Configuration Files

CAUTION

Modifying a configuration file may cause the BM635 to improperly operate. Modify a configuration file with caution.

The configuration file saves the parameter settings of the BM635. You can back up, modify, and update a configuration file. The configuration file is classified into three types.

- User configuration file: This file saves current parameter settings of the BM635 of the user.
- Carrier configuration file: This file saves parameter settings of the BM635 of the carrier.
- Default configuration file: This file saves the default parameter settings of the BM635.

The management mode varies with the configuration file type. The following takes the management of a user configuration file as an example.

5.3.1 Backing up a Configuration File

Step 1 In the navigation tree, choose **Maintain** > **Device**, and then click the **Configure File** tab.

Step 2 Click **Download Configuration File**.

Step 3 Select the path for saving the configuration file, and then click **Confirm**.

----End

NOTE

To back up the carrier configuration file and the default configuration file, click the **Advanced** tab.

5.3.2 Importing a Configuration File

The configuration file prepared in advance can be imported to the BM635. If the BM635 cannot operate properly with the imported configuration file, import the configuration file without being modified or see section 5.6 "Restoring Carrier Settings" to restore carrier settings of the BM635.

Step 1 In the navigation tree, choose **Maintain** > **Device**, and then click the **Configure File** tab.

Step 2 Click **Browse**.

Step 3 Select the configuration file to be imported.

Step 4 Click **Upload Configuration File**.

----End

NOTE

To import the carrier configuration file and the default configuration file, click the **Advanced** tab.

5.4 Rebooting the BM635

After importing a configuration file, restart the BM635.

Step 1 In the navigation tree, choose **Maintain** > **Device**, and then click the **Reset** tab.

Step 2 Click **Reboot** to restart the BM635.

NOTE

You can also press the Reset button on the side panel to restart the BM635.

----End

5.5 Upgrading the Software

CAUTION

Do not power off the BM635 when the BM635 is being upgraded to avoid any damage.

The software of the BM635 can be upgraded locally or remotely. It takes about 8 minutes to upgrade the software of the BM635. After the software is upgraded, the BM635 restarts automatically.

Upgrading the BM635 Locally

To upgrade the software of the BM635, upload the local files for upgrade to the BM635. Perform the following steps to upgrade the BM635 locally:

Step 1 In the navigation tree, choose **Maintain** > **Device**, and then click **Firmware**.

Step 2 Click **Browse**.

Step 3 Select a file for upgrade.

Step 4 Click **Update Software**.

----End

NOTE

The carrier sends the files for upgrade or you obtain these files by negotiation.

Upgrading the BM635 Remotely

You can upgrade the BM635 through a remote server. The remote upgrade of the BM635 requires the corresponding user rights and the support from carrier. Perform the following steps to upgrade the BM635 remotely:

Step 1 In the navigation tree, choose **Maintain** > **Device**, and then click the **Firmware** tab.

Step 2 Enter the network address or IP address of the remote server in **Remote URL**.

Step 3 Fill in **User Name** and **Password** text boxes.

Step 4 Click **Remote Update Firmware**.

----End

5.6 Restoring Carrier Settings

CAUTION

After carrier settings are restored, the configuration file is restored to the carrier configuration file. Restore the carrier settings with caution.

To restore carrier settings of the BM635, perform the following steps:

Step 1 In the navigation tree, choose **Maintain** > **Device**, and then click the **Reset** tab.

Step 2 Click **Restore Carrier Configuration** to restore settings made by the carrier. Please login the Web UI after restore.

----End

6 Maintaining the BM635

About This Chapter

The following table lists the contents of this chapter.

Section	Describes
6.1 Checking the Information on the BM635	How to check the parameter settings of the BM635.
6.2 Detecting the BM635	How to detect the BM635.

6.1 Checking the Information on the BM635

By querying the status information, you can know about the operating status and the parameter settings of the BM635.

6.1.1 Checking the Device Information

The device information includes the product class, device ID, hardware version, software version, WAN MAC address, LAN MAC address, and WLAN MAC address.

In the navigation tree, choose **Status** > **Device**, and then click the **Device Info** tab to check device information.

6.1.2 Checking the Information on the WAN Side

The information on the WAN side contains the connection status and the DNS.

- The connection status information includes the MAC address, IP address, and subnet mask.
- The DNS information includes the connection name, default IP address of the gateway, IP address of the primary DNS server, and IP address of the secondary DNS server.

In the navigation tree, choose **Status** > **WAN**, and then click the **Internet Status** tab to check the information on the WAN side.

6.1.3 Checking the Information on the LAN Side

The information on the LAN side includes the information on the Ethernet and WLAN.

The Ethernet information includes the following:

- **LAN Host**: It specifies the IP address and MAC address of the LAN host.
- **LAN Status**: It specifies the connection status of each interface on the LAN side. The working mode of the device at the LAN side is auto-negotiation.
- **Device**: It specifies the IP address, MAC address, and connection status of each connected device at the LAN side.
- **Ethernet Packet**: It specifies the information on the packets sent or received over the Ethernet.

The WLAN information includes the device connection status, working mode, the information on the sent and received packets, and SSID.

In the navigation tree, choose **Status** > **LAN**, and then click the **Ethernet** or **WLAN** tab to check information on the LAN side.

6.1.4 Checking the Information on VoIP

The VoIP information includes SIP ID, status of the SIP registration server, and port number.

In the navigation tree, choose **Status** > **VoIP**, and then click the **VoIP Info** tab to check VoIP information.

6.1.5 Checking the Information on WiMAX

The WiMAX information includes the network access status of the WiMAX network, uplink and downlink rates, uplink and downlink signal strength, uplink and downlink quality, and the information on receiving and sending packets.

In the navigation tree, choose **Status** > **WiMAX**, and then click the **WiMAX Stat.** tab to check WiMAX information.

6.2 Detecting the BM635

The local network connection and network connection of the internet service provider can be tested.

To detect the BM635, perform the following steps:

Step 1 In the navigation tree, choose **Maintain** > **Diagnose**, and then click the **Diagnose** tab.

Step 2 In **IP Address**, enter the IP address to be detected.

Step 3 Click **Start**.

After the detection is complete, the BM635 reports the detection results to the server.

----End

7 Technical Specifications

Technical specifications may vary with the upgrade of the BM635.

Item	Sub-item	Specifications
Standard	Wireless interface	IEEE 802.16e
	Network band	3.4 to 3.62 GHz
WLAN parameters	Working band	2.4 to 2.4835 GHz
	Working mode	Hybrid mode: IEEE 802.11b, IEEE 802.11g, IEEE 802.11b, and IEEE802.11g
	Maximum number of users	32
Port	LAN	Four RJ45 ports
	TEL	Two RJ11 ports
Other parameters	Voltage	110 to 240 V AC
	Power consumption	< 18 W
	Power supply of the integrated system	12 V DC, 2 A
	Temperature	0℃ to +40℃ (32℉ to 104℉)
	Humidity	5% to 95% (non-condensing)
	Dimensions (Width × Depth × Height)	188 mm × 56 mm × 158 mm
	Weight	＜ 400g

8 FAQs

The power indicator is off.
• Please check the power supply, ensure that the power supply is properly connected. • Please check whether the power adapter meets the specification.
The WiMAX indicator is off.
• Please check the power supply, ensure that the power supply is properly connected. • Check whether you have activated the WiMAX online service. • Place the device in an open space without any obstacle around it, such as a cement wall and a wooden wall, which affects the WiMAX network signal. • Place the device far away from an electrical device that produces a strong magnetic field or strong electric field, such as a microwave oven, a fridge, and a satellite dish antenna.
You cannot make a VoIP call.
• Ensure that the phone line is properly connected. • Please check whether the VoIP parameters are properly set, see section 3.2 "Configuring VoIP".
The WiMAX network cannot be found.
• Ensure that the antenna is properly connected. • Please check the power supply, ensure that the power supply is properly connected. • Place the device in an open space without any obstacle around it, such as a cement wall and a wooden wall, which affects the WiMAX network signal. • Place the device far away from an electrical device that produces a strong magnetic field or strong electric field, such as a microwave oven, a fridge, and a satellite dish antenna.

You cannot log in to the Web UI.

- Please check the power supply, ensure that the power supply is properly connected.
- Please check whether the network cable between the device and the computer is properly connected. Ensure that the device is properly connected to the computer.
- Please check whether the Web UI parameters are properly set. see section 2.1 "Logging in to the Web UI".
- Please check the Internet Explorer parameters, ensure the proxy server is disable. Take the Internet Explorer 6.0 as an example. perform the following steps:
    1. Open the Internet Explorer 6.0.
    2. Choose **Tools** > **Internet Options...** , select the **Connections** tab.
    3. Click **LAN Settings...**.
    4. Deselect **Use a proxy server for your LAN**. If select, click the check box to deselect it. Then click **OK**.
    5. Login the Web UI.

The device or the power adapter overheats.

- The device overheats after operating for a long time. Therefore, power off the device when you do not use the device.
- Place the device in a well-ventilated place and avoid direct sunshine.

9 Abbreviations

A	
AAA	Authorization, Authentication and Accounting
ACL	Access Control List
ALG	Application Layer Gateway
C	
CA	Certification Authority
D	
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone
DNS	Domain Name Server
DSCP	Differentiated Services Code Point
DTMF	Dual Tone Multi-Frequency
E	
EAP	Extensible Authentication Protocol
F	
FTP	File Transfer Protocol
H	
HTTP	Hypertext Transfer Protocol
I	
ICMP	Internet Control Message Protocol
IGMP	Internet Group Management Protocol
IPSec	IP Security Protocol

ISP	Internet Service Provider
L	
L2TP	Layer 2 Tunneling Protocol
LAN	Local Area Network
M	
MAC	Medium Access Control
MIMO	Multiple-Input Multiple-Output
MS	Mobile Station
MWI	Message Waiting Indication
N	
NAI	Network Access Identifier
NAPT	Network Address Port Translation
NAT	Network Address Transmission
O	
OFDMA	Orthogonal Frequency Division Multiple Access
P	
PKM	Privacy Key Management
PPPoE	Point-to-Point Protocol over Ethernet
Q	
QoS	Quality of Service
R	
RIP	Routing Information Protocol
RTP	Real-time Transfer Protocol
RTSP	Real-Time Streaming Protocol
S	
SIP	Session Initiation Protocol

SNTP	Simple Network Time Protocol
SS	Subscriber Station
SSID	Service Set Identifier
SSH	Secure Shell
SYN	Synchronous
T	
TOS	Type of Service
TLS	transport layer security protocol
TTLS	tunneled transport layer security protocol
U	
URI	Uniform Resource Identifier
URL	Universal Resource Locator
V	
VoIP	Voice over IP
W	
WAN	Wide Area Network
WEP	Wired Equivalent Privacy
WiMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Network
WPA-PSK	Wi-Fi Protected Access Pre-Shared Key

Index