

IDU R2561
V100R001C00SPC012
User Guide

Issue 01
Date 2020-07-06



Copyright © Huawei Technologies Co., Ltd. 2019. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Technologies Co., Ltd.

Trademarks and Permissions



HUAWEI 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 purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

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 a warranty of any kind, express or implied.

Huawei Technologies Co., Ltd.

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

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

Email: support@huawei.com

Contents

1 About this Guide.....	1
1.1 Prerequisite Skills and Knowledge	1
1.2 Conventions Used in this Document.....	1
2 Introduction.....	2
2.1 Product Overview	2
2.2 Product Package.....	2
2.3 Connectors	2
2.4 LED Indicators.....	4
2.5 Installation	4
2.5.1 Installing IDU R2561.....	4
2.5.2 Connecting the Cable.....	5
3 Web Interface	6
3.1 Login to Web-GUI.....	6
3.2 Function Button	8
3.3 Status and device information.....	8
3.3.1 Status > Device Status	8
3.3.2 Status > Telephony Status	10
3.3.3 Status > Network Status.....	11
3.3.4 Status > About.....	12
3.4 Menu Structure	13
4 Reference Manual	15
4.1 Management	15
4.1.1 Management > Setup Wizard.....	15
4.1.2 Management > WAN Setup	17
4.1.3 Management > LAN Setup.....	18
4.1.4 Management > Telephony.....	21
4.1.5 Management > Diagnostics	27
4.1.6 Management > System Log	28
4.2 Personalization.....	31
4.2.1 Personalization > Configuration	31
4.2.2 Personalization > Device Setup	32
4.2.3 Personalization > Software	34

4.3 Basic	34
4.3.1 Basic > Firewall	34
4.3.2 Basic > DMZ	36
4.3.3 Basic > UPnP	36
4.3.4 Basic > Dynamic DNS	37
4.3.5 Basic > VPN Passthrough	38
4.4 Advanced	39
4.4.1 Advanced > MAC Filtering	39
4.4.2 Advanced > IP Filtering	41
4.4.3 Advanced > Port Forwarding	42
4.4.4 Advanced > Port Triggering	43
4.4.5 Advanced > Layer 7 Filtering	44
4.4.6 Advanced > URL Filtering	45
4.4.7 Advanced > ACL Filtering	46
4.4.8 Advanced > Parental Control	48
4.4.9 Advanced > Static Routing	49
4.5 Wi-Fi	50
4.5.1 Wi-Fi > Basic	50
4.5.2 Wi-Fi > Advanced	53
4.5.3 Wi-Fi > WPS	55
4.5.4 Wi-Fi > Connected Client	56
4.6 Engineering	57
4.6.1 How to Login Engineering page	57
4.6.2 Engineering > DM Settings	58
5 Federal Communication Commission	15
5.1 Federal Communication Commission Interference Statement	15

1 About this Guide




1.1 Prerequisite Skills and Knowledge

To use this document effectively, you should have a working knowledge of Local Area Networking (LAN) concepts and wireless Internet access infrastructures. In addition, you should be familiar with the following:

- Hardware installers should have a working knowledge of basic electronics and mechanical assembly.
- Network administrators should have a solid understanding of software installation procedures for network operating system and troubleshooting knowledge. Please refer to the following pages for more detail.

1.2 Conventions Used in this Document

The following typographic conventions and symbols are used throughout this document:

	Very important information. Failure to observe this may result in damage.
	Important information that should be observed.
	Additional information that may be helpful but not required.
bold	Menu commands, buttons and input fields are displayed in bold

2 Introduction


2.1 Product Overview

IDU R2561 is an Indoor CPE.

- Support 2 LAN ports and 1 VoIP port
- Support HTTPs Web GUI

2.2 Product Package

Number	Item	Q'ty
1	Indoor Router	1
2	Power Adapter	1

	If any item of mentioned above is missing or damaged, please contact our customer support immediately.
---	--

2.3 Connectors

WAN : One RJ-45 connector for connecting to the ODU LAN port.

Figure 2-1 IDU Rear Panel

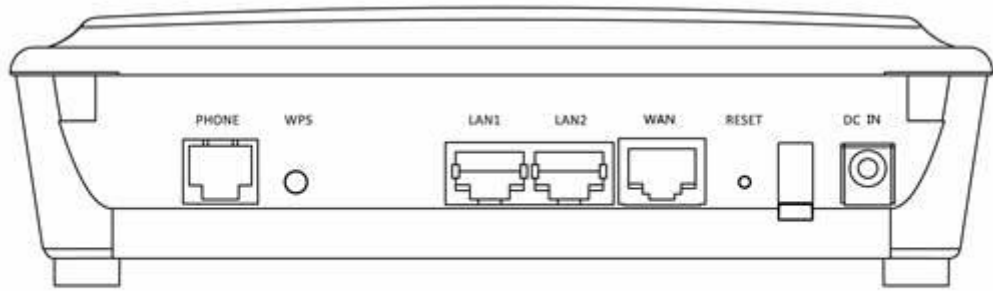
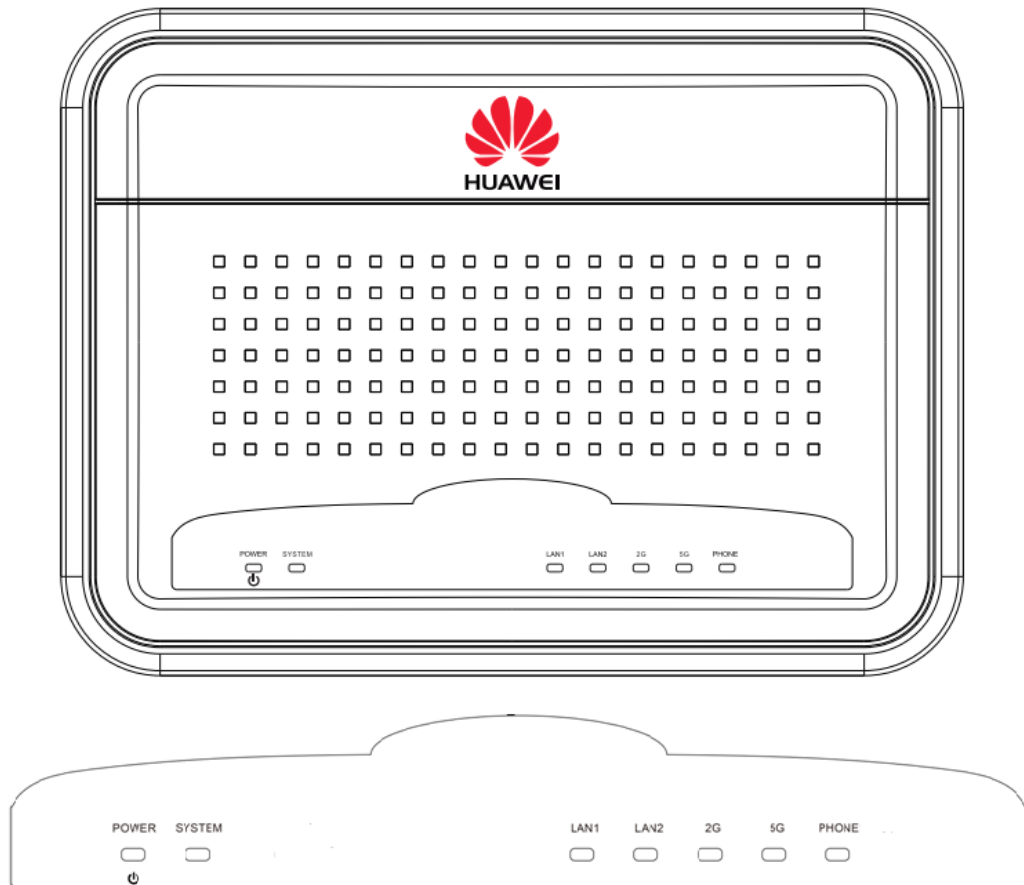


Figure 2-2 IDU Front Panel



2.4 LED Indicators

Table 2-1 IDU R2561 LED Indicators as following table

Number	LED name	Color	LED Behavior	Status Indication
1	Main Power	Green	On	Power On
			Off	Power Off
2	System	Green	On	System is connected
			Blinking	System is upgrading
			Off	System is disconnected
3	LAN 1 & 2	Green	Blinking	Ethernet connected
			Off	No Ethernet connected
4	2.4G	Green	On	Enable 2.4G Wi-Fi
			Blinking	Data transmission
			Off	Disable 2.4G Wi-Fi
5	5G	Green	On	Enable 5G Wi-Fi
			Blinking	Data transmission
			Off	Disable 5G Wi-Fi
6	Phone	Green	On	Registered
			Blinking	Busy
			Off	De-registered

2.5 Installation

Before installing the IDU R2561, verify that you have all the items listed in the package checklist. If any of the items is missing or damaged, contact your service provider.



Only experienced installation professionals who are familiar with local building and safety codes and, where applicable, are licensed by the appropriate government regulatory authorities should install outdoor units and antennas.

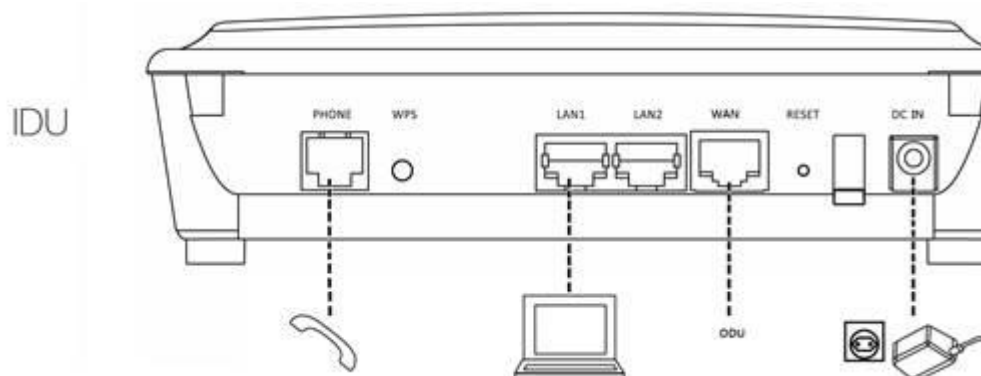
2.5.1 Installing IDU R2561

Any of the items are missing or damaged, contact your LTE service provider.

2.5.2 Connecting the Cable

Step 1 Physical connection as following

1. Connect the Ethernet cable to the RJ45 ports of IDU R2561 and ODU.
2. Connect the Ethernet cable from the computer to one of the IDU R2561's Ethernet Ports.
3. Connect the supplied power adapter to the IDU R2561. The PWR LED shines a steady green when device ready.
4. Mounting the Device.



Step 2 Connect to the Internet

Physical connection is as following (Refer to Installing Device Instruction).

1. Connect IDU R2561 (WAN) and ODU(RJ45) via Ethernet cable.
2. Use power adapter to connect IDU R2561 (Power)
3. Connect IDU R2561 (ETHERNET PORTS) and PC via Ethernet cable.
4. PC will get default IP 192.168.1.xxx (xxx: 2-254). Open a web browser and go to 192.168.1.1.



Use **ONLY** the indoor router which supplied with the IDU R2561. Otherwise, Device may be damaged.

----End

3 Web Interface

3.1 Login to Web-GUI

Step 1 Open the Web browser and enter the default IP address of the device, which is: **192.168.1.1**

Step 2 Enter the default Username (**admin**) and Password (**IDU@huawei**) to access advanced interface or enter the default Username (**user**) and Password (**LTE@Endusr**) to access web management interface.

- Default Log-in information:

Username: user

Password: LTE@Endusr

- Log-in protection:

If you key-in the log-in username or password error more than three times, the device would locked you to enter username or password five minutes.

----End



You need to change the default Login passwords while the first time log-in.
Please change the default password to protect your account.

Figure 3-1 Web UI - Normal

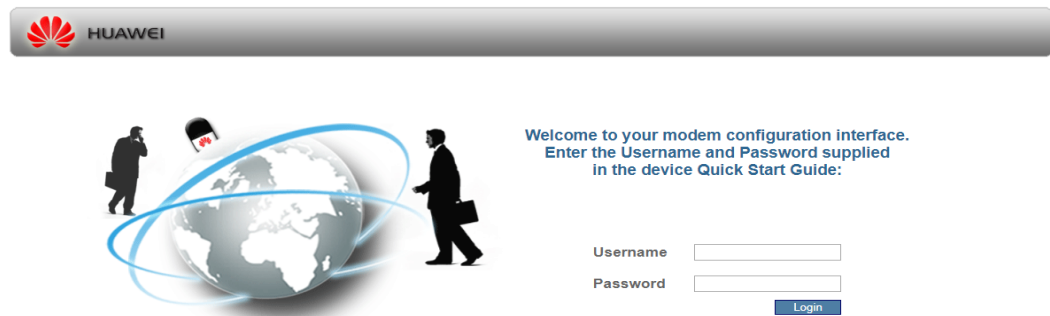


Figure 3-2 Web UI - V Incorrect Username or Password

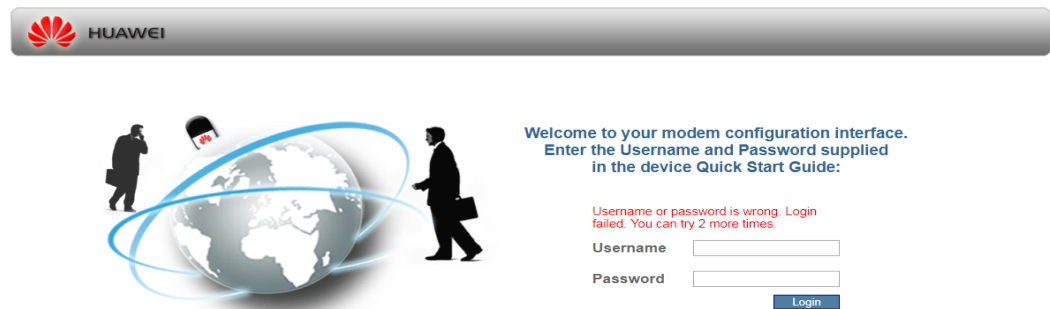
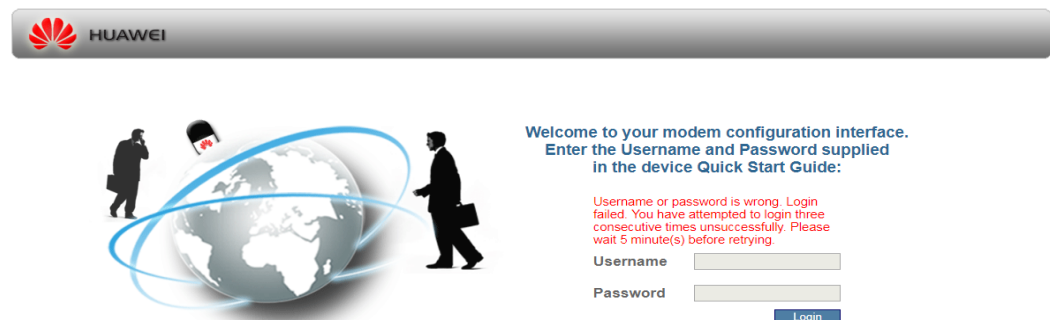

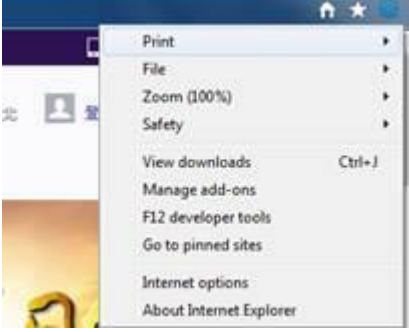



Figure 3-3 Web UI - V Enter incorrect Username or Password three times



 If you're successfully connected to the Internet but cannot view webpages in Internet Explorer 8, maybe the settings of your browser is changed by some reasons. Suggest you to RESET your browser or follow below steps.

1. **Open IE8 browser -> F12 developer tools**

2. **Browser Mode -> Internet Explorer 8**


3.2 Function Button

Function button is located at each Web UI page Top-Right corner.



REBOOT

Force device to initial a reboot.

LOGOUT

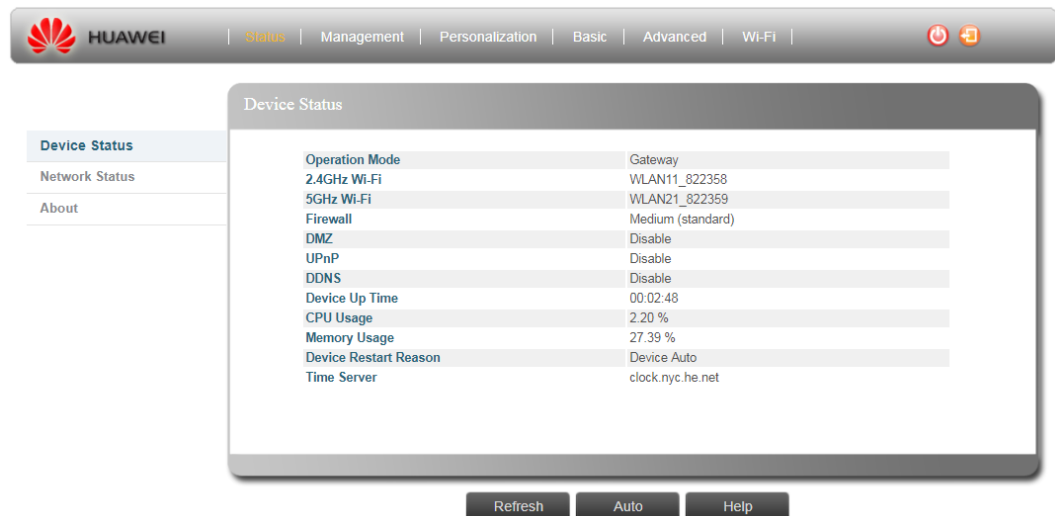
Quickly logout the device, device will back to log-in page.

3.3 Status and device information

3.3.1 Status > Device Status

This page is information only, here displays the current status of the device such as system uptime and WAN information. You can refer to below column for detail definitions.

Figure 3-4 Device Status



- **Operation Mode**

The mode to forward data packets between Internets.

- **2.4GHz Wi-Fi**

2.4GHz Wi-Fi SSID Service Set ID (SSID) that identifies the Wi-Fi network.

- **5GHz Wi-Fi**

5GHz Wi-Fi SSID

- **Firewall**

Here displayed your current firewall level; there are three default configurations for you to select: Low/Medium/High or you can select Custom to configure by your preference. For more detail please refer to **Basic> Firewall** section.

- **DMZ**

DMZ enabled or disabled.

- **UPnP**

UPnP enabled or disabled.

- **DDNS**

DDNS enabled or disabled.

- **Device Up Time**

The duration since the unit is powered on in format "x day(s) <hour>:<minute>:<second>".

- **CPU Usage**

System's CPU Usage.

- **Memory Usage**


System's memory usage.

- **Device Restart Reason**

The reason for last device reboot (e.g. Device auto, Software Upgrade, etc.).

- **Time Server**

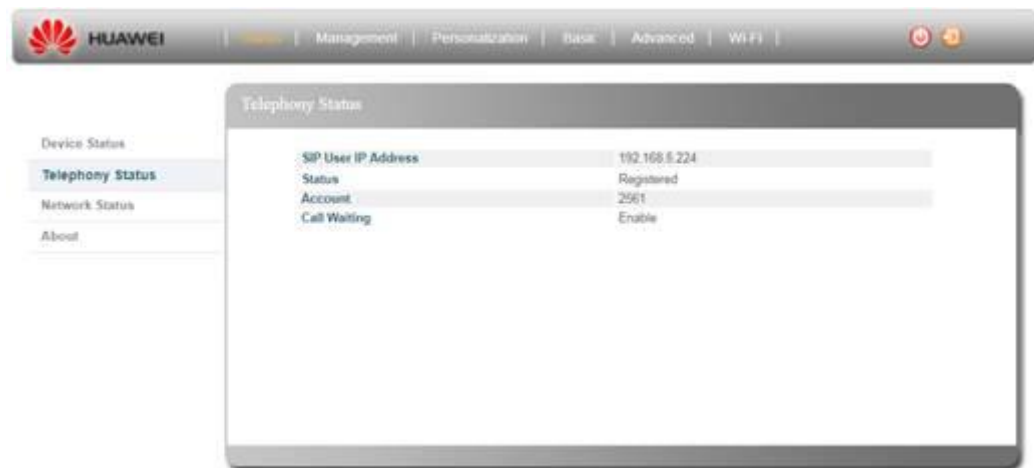
The NTP (Network Time Protocol) server address.

	<p>Click the "Refresh" button manual update the current status.</p> <p>Click the "Auto" button auto update the current status.</p>
---	--

3.3.2 Status > Telephony Status

The Telephony Status displays a summary of the VoIP registration .The information includes:

Figure 3- 5 Telephony Status



- **SIP User IP Address**

IP address of the Session Initiation Protocol (SIP), an application-layer control protocol that can establish, modify, and terminate multimedia sessions such as Internet telephony calls (VOIP).

- **Status**

Registered or De-registered in the SIP server. This information also can be observing on the front panel voice line LED.

- **Account**


The SIP Account. The account format depends on the SIP Server.

- **Call Waiting**

Allow the second caller to wait on-line while an existing phone call is on-going.

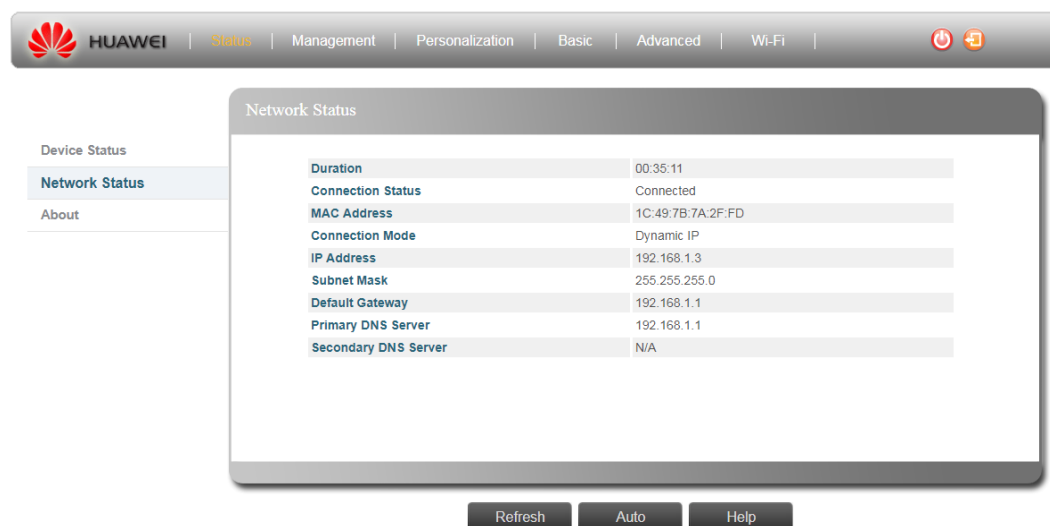
If you want switch the call please press "flash" key on your telephone.

You can go [Management>Telephony](#) to change the setting Disable/Enable.


	<p>Click the "Refresh" button manual update the current status.</p> <p>Click the "Auto" button auto update the current status.</p>
---	--

3.3.3 Status > Network Status

Figure 3- 6 Network Status



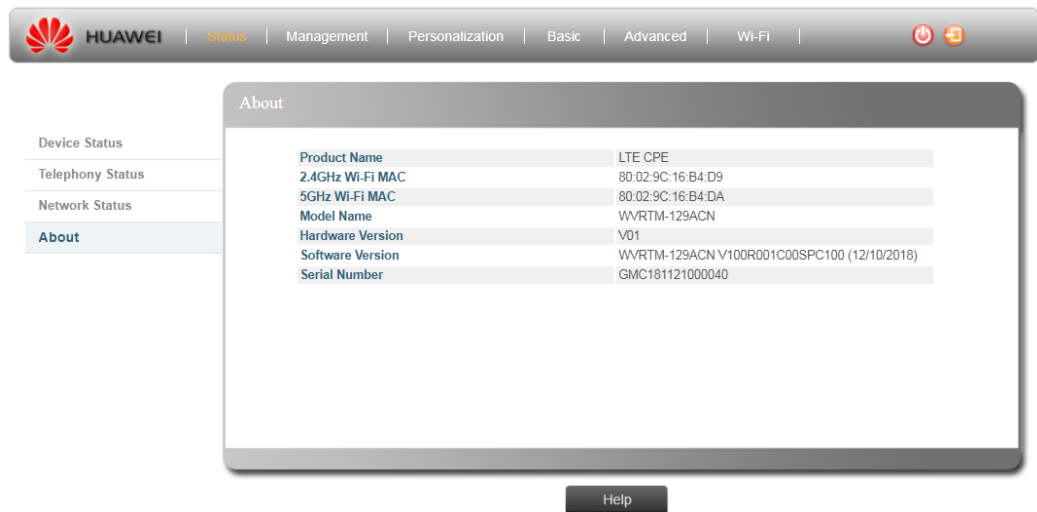
- **Duration**
The time period of active WAN connection.
- **Connection Status**
Connected means Ethernet link is up and IP is obtained, otherwise, Disconnected is shown.
- **MAC Address**
The MAC address used for device's WAN network interface.
- **Connection Mode**
Determine how Ethernet ports behave for network connection.
- **IP Address**
WAN IP address of device.
- **Subnet Mask**
WAN subnet mask of device.
- **Default Gateway**
WAN default gateway of device.
- **Primary DNS Server**
Primary DNS server for DNS query.
- **Secondary DNS Server**
Secondary DNS server for DNS query.

	<p>Click the "Refresh" button manual update the current status.</p> <p>Click the "Auto" button auto update the current status.</p>
---	--

3.3.4 Status > About

This page displays the device default necessary information. Those values are set by the manufacturer as the factory defaults.

Figure 3- 7 About



- **Product Name**
Product type.
- **2.4GHz Wi-Fi MAC**
2.4GHz Wi-Fi MAC address
- **5GHz Wi-Fi MAC**
5GHz Wi-Fi MAC address
- **Model Name**
Device model name.
- **Hardware Version**
Device HW version
- **Software Version**
Device's SW/FW version.
- **Serial Number**
Device's serial number.

3.4 Menu Structure

After entering "Detailed Configuration Page", the user can quickly jump to the specified Sub Menu. (By clicking "Quick Panel" at the bottom of the page.)

Users can refer to the menu structure given below:

Status	Device Status
	Telephony Status (If VoIP is enabled)
	Network Status
	About
Management	Setup Wizard
	WAN Setup
	LAN Setup
	Telephony Setup
	Diagnostics
	System Log
Personalization	Configuration
	Device Setup
	Software
Basic	Firewall
	DMZ
	UPnP
	Dynamic DNS
	VPN Passthrough
Advanced	MAC Filtering
	IP Filtering
	Port Forwarding
	Port Triggering
	Layer 7 Filtering
	URL Filtering
	ACL Filtering
	Parental Control
	Static Routing
Wi-Fi	Basic

	Advanced
	WPS
	Connected Client

4 Reference Manual

4.1 Management

4.1.1 Management > Setup Wizard

Figure 4- 1 Setup Wizard

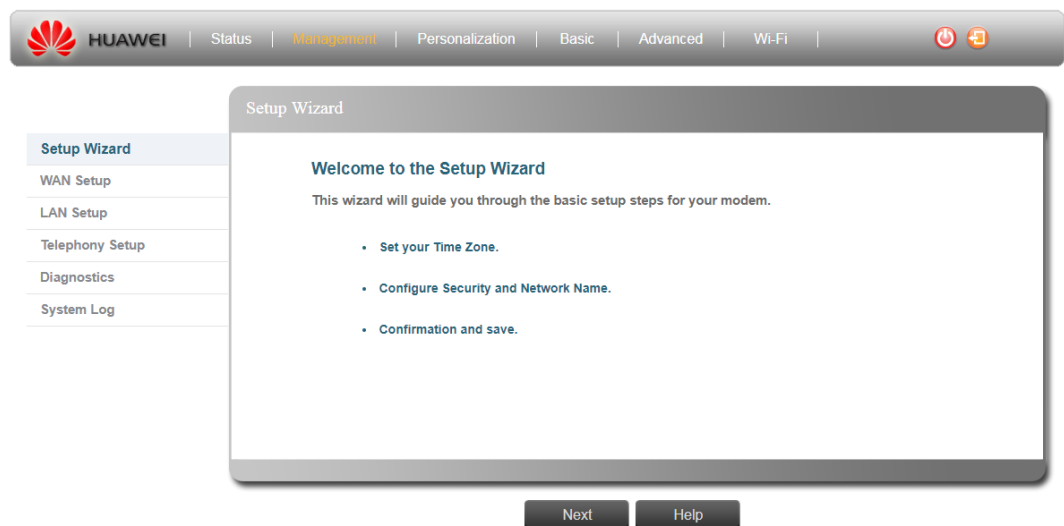


Figure 4- 2 Setup Wizard - Set your Time Zone

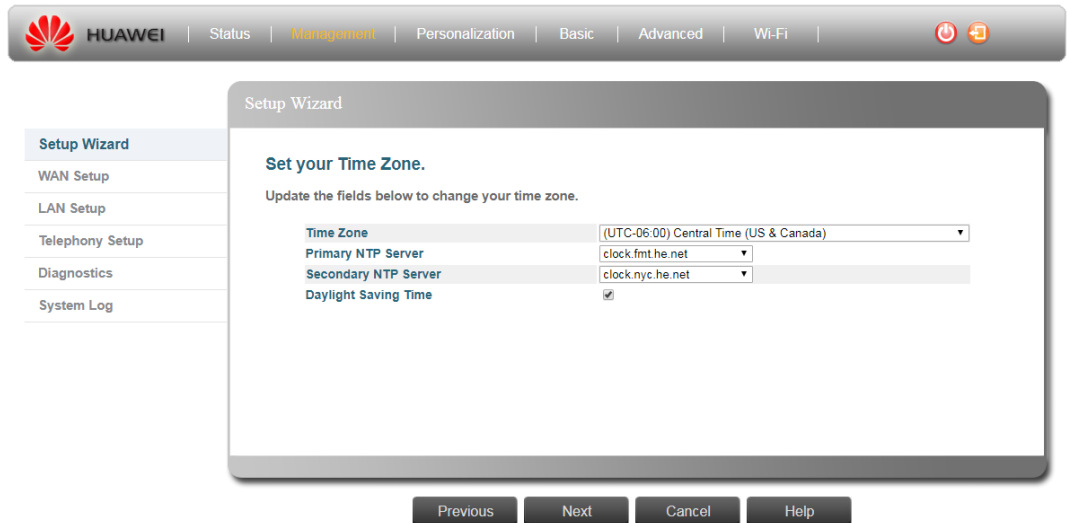


Figure 4- 3 Setup Wizard - Configure Security and Network Name

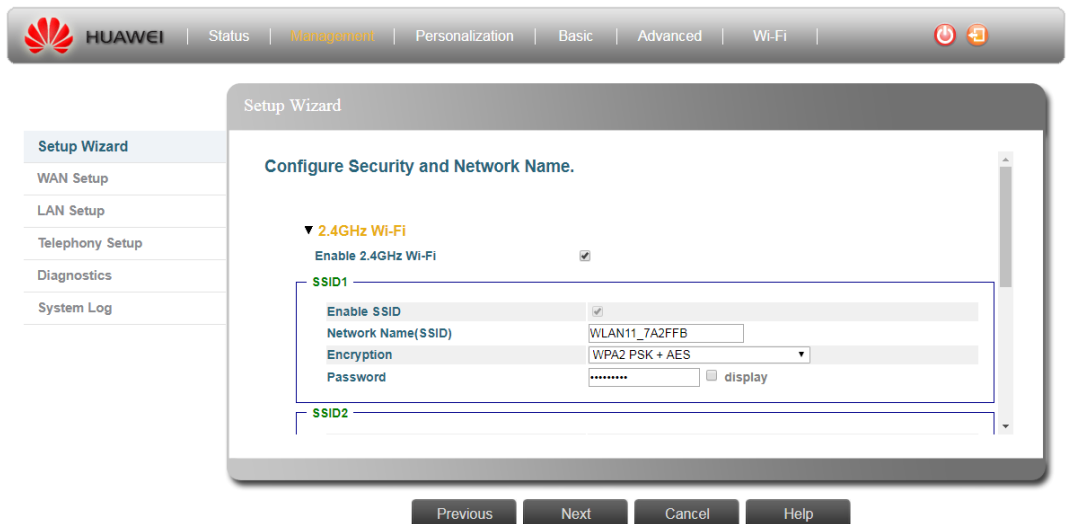
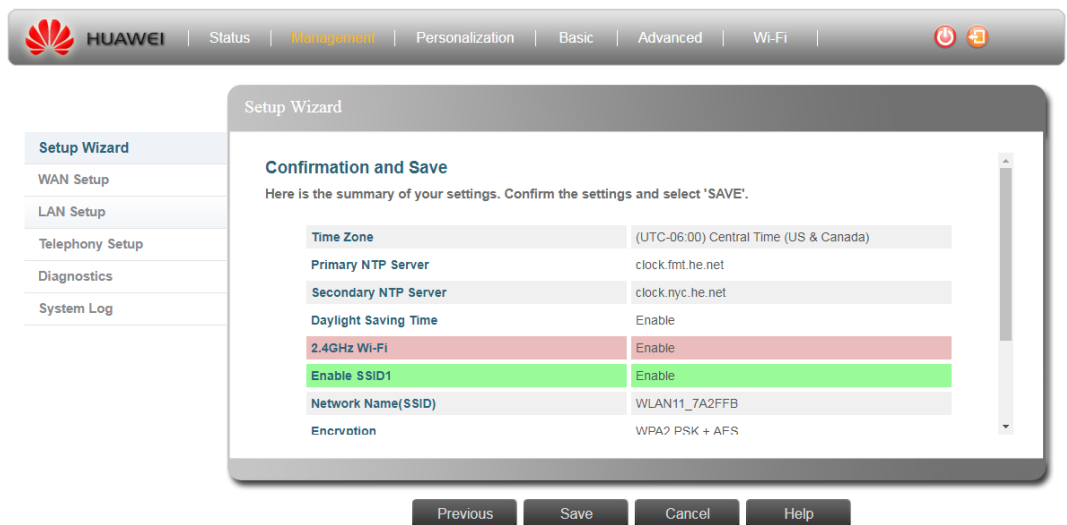


Figure 4- 4 Setup Wizard - Summary



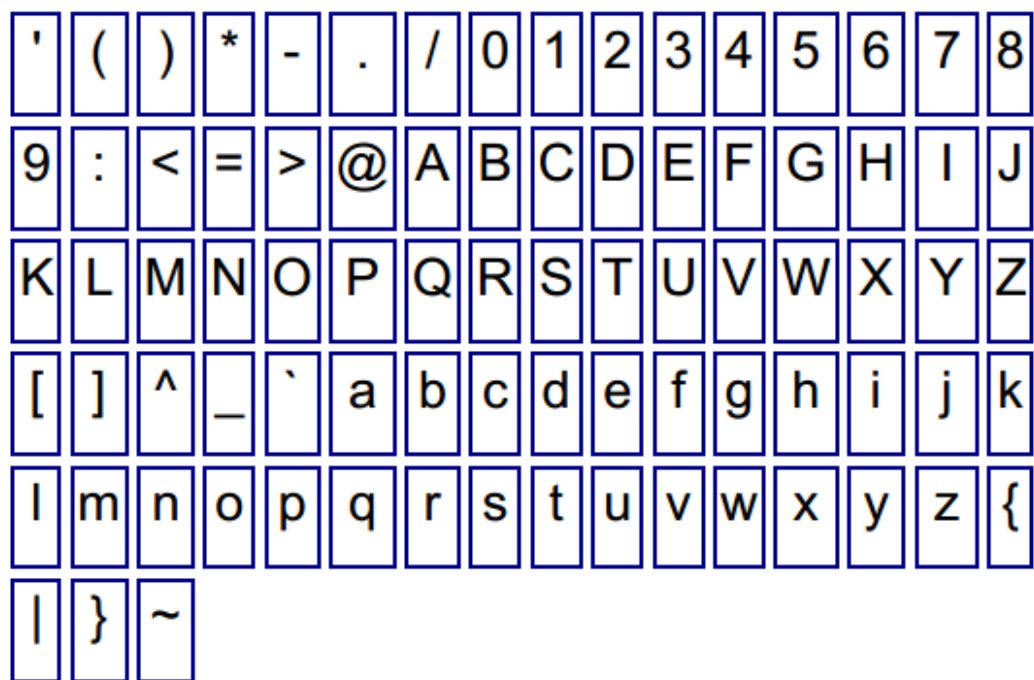
The Setup Wizard will guide you to do the important setting of the device.

- Step 1** By press the "Next" button to start Wizard, we will guide you to set up your Time zone.
- Step 2** 1. Selection your locate country, NTP server and location time zone, and check if your Location have daylight saving. 2. Review all your settings, if no problem, please press "Next".
- Step 3** Set up your 2.4GHz and 5GHz Wi-Fi network name/Encryption and Wi-Fi Password, then press "Next".

The Service Set ID (SSID) that identifies the Wi-Fi network. The SSID is case sensitive and can


consist of up to 32 alphanumeric characters.

Following characters is valid for Network Name (SSID).



- Step 4** Check your settings again and then press "Save" button to apply the change.

----End

	<p>Click the "Next" button to launch the Setup Wizard.</p> <p>Click the "Previous" button to go back to the previous page</p> <p>Click the "Cancel" button to return to the first page.</p> <p>Click the "Save" button to save any modified settings.</p>
---	---

4.1.2 Management > WAN Setup

This page is information only, here displays the current status of the device such as system uptime and WAN information. You can refer to below column for detail definitions.

Figure 4- 5 WAN Setup - Dynamic IP

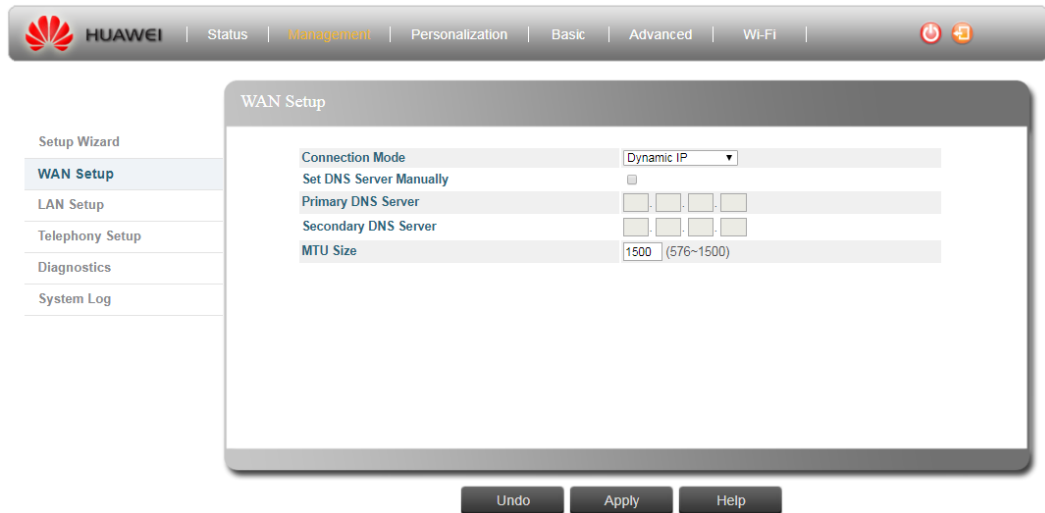
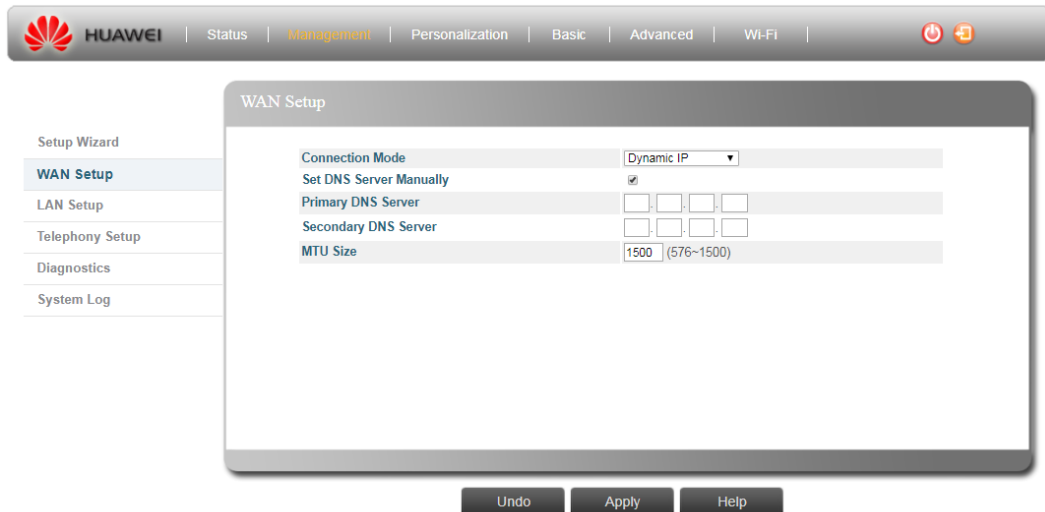


Figure 4- 6 Set DNS Server Manually (Enable)



Connection Mode

Determine how Ethernet ports behave for network connection.

Dynamic IP Mode

One dedicated Ethernet port behaves as WAN connection via DHCP and the rest for LAN connection.

- **Set DNS Server Manually** : Use manually configured DNS server(s) for DNS query.
- **Primary DNS Server** : Primary DNS server for DNS query.
- **Secondary DNS Server** : Secondary DNS server for DNS query.
- **MTU Size** : Maximum transmission packet size of device's WAN interface.

4.1.3 Management > LAN Setup

In this page, you can change the Web UI and device local IP address distribution range.

Figure 4- 7 LAN Setup - Disable



Figure 4- 8 LAN Setup - Server

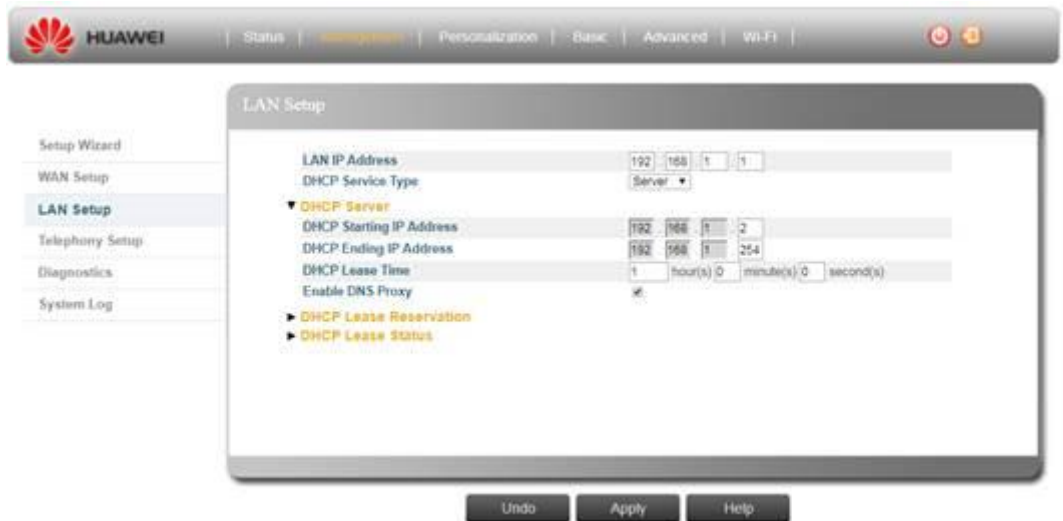


Figure 4- 9 LAN Setup - Relay



LAN IP Address:

Please input the LAN IP address here, the default value is 192.168.1.1

DHCP Service Type: Please select the DHCP service type, options are Disable, Server and Relay

- **Disable:** The device will not assign LAN IP address to PC; you have to manually set static IP address to the connected PC to access the UI.
- **Server:** The unit has a built-in DHCP server that can be used for managing the distribution of IP addresses for the devices connected to the local LAN port (Ethernet or Wi-Fi) and Web UI. In the DHCP Server page you set DHCP parameters for dynamic IP assignment.
- **Relay:** LAN PC will be assigned from DHCP Server that behind the BS.

DHCP Server

- **DHCP Starting IP Address:** Enter the first IP address assigned by the DHCP server.
- **DHCP Ending IP Address:** Enter the last IP address assigned by the DHCP server.
- **DHCP Lease Time:** Set the time, how long you want to renew the IP.
- **Enable DNS Proxy:** Enable or disable DNS proxy. Default is enabled (check).
 - **Check:** DNS proxy is device's IP.
 - **Uncheck:** DNS proxy is from WAN's DNS information.


- **DHCP Lease Reservation**

The Lease Reservation page displays information on reserved IP addresses for leasing. In this page you assign the specific IP addresses to the specific client device connected to the Ethernet ports and Wi-Fi access point. You can also add, delete, or modify the reservation settings.

- **Select:** Select an IP to delete.
- **Host Name:** Enter a name to the host.
- **MAC Address:** Add a device MAC address.
- **IP Address:** Specify a reservation IP address for a specified MAC address.
- **Enabled:** Select if to enable or disable a specified IP setting.
- **DHCP Lease Status:** The Lease Status page displays information regarding the leased IP address(es):
- **Client Host Name:** This is display the connected PC name which connected to the LTE device.
- **MAC Address:** This is display the connected PC MAC address which connected to the LTE device.
- **IP Address:** This is display the IP address that assigned to this LAN device(Host PC)
- **Remaining Lease Duration:** This display how many seconds remain for this assigned IP
- **Action:**
 - **Block:** To Block the specific PC; After press the "**Block**" button the LAN device cannot access this LTE device any more.
 - **Unblock:** Press "**Unblock**" button to allow the LAN device to back to connect again. This function is for you to easily manage the LAN devices to avoid the unexpected device access from your LAN
- **Status:** This shows the current IP assignment availability.

DHCP Relay Server IP Address:

The device will request IP address from the DHCP Relay server, please input the DHCP relay Server's IP address for obtain the IP address. If you input wrong DHCP Relay server IP address or Relay server is not working, please manually set static IP address to the connected PC to access the UI.

	Use the Add or Delete buttons to add or clear reserved IPs for leasing, please click Apply button to confirm the Add or Del. Click Undo to clear the changes that you have made to this window. Click the Auto button auto update the current status.
---	---

4.1.4 Management > Telephony

This chapter describes how to configure VoIP parameters.

Voice over Internet Protocol (VoIP) technology is a way of using the Internet to make phone calls. You can make VoIP calls by connecting a regular phone to the unit's Phone ports.

Before using the VoIP Phone ports on the unit, you must have an account with a SIP service provider. To change the settings below, please always double confirm your service provider.

Figure 4- 10 Telephony - Account



Figure 4- 11 Telephony - Server settings

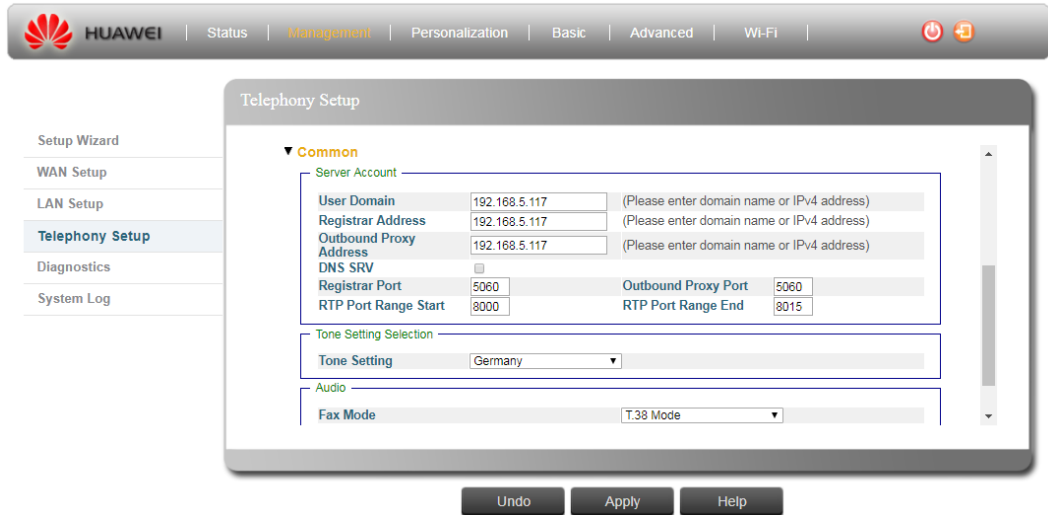


Figure 4- 12 Telephony - Tone Setting Selection

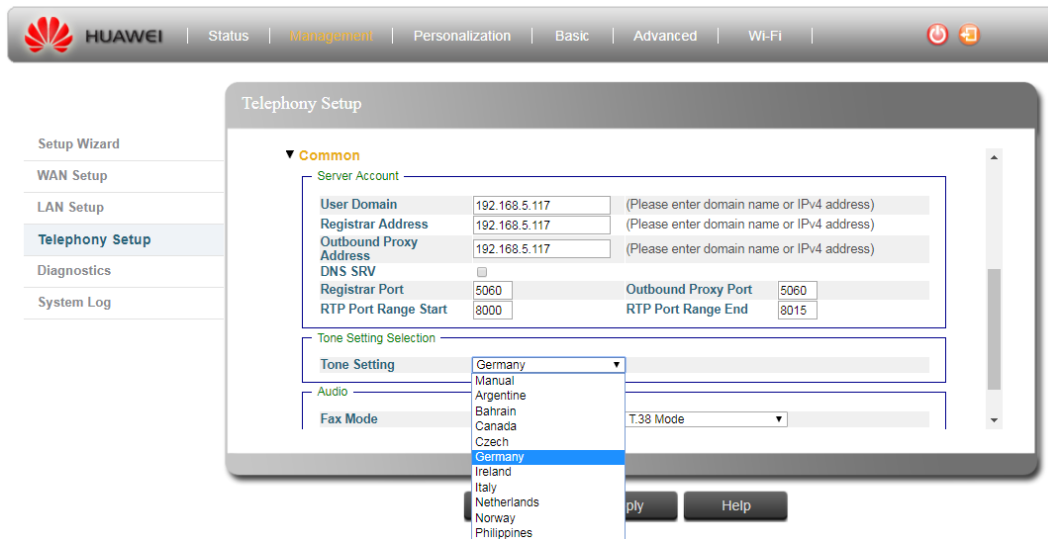


Figure 4- 13 Telephony - Call Feature Settings

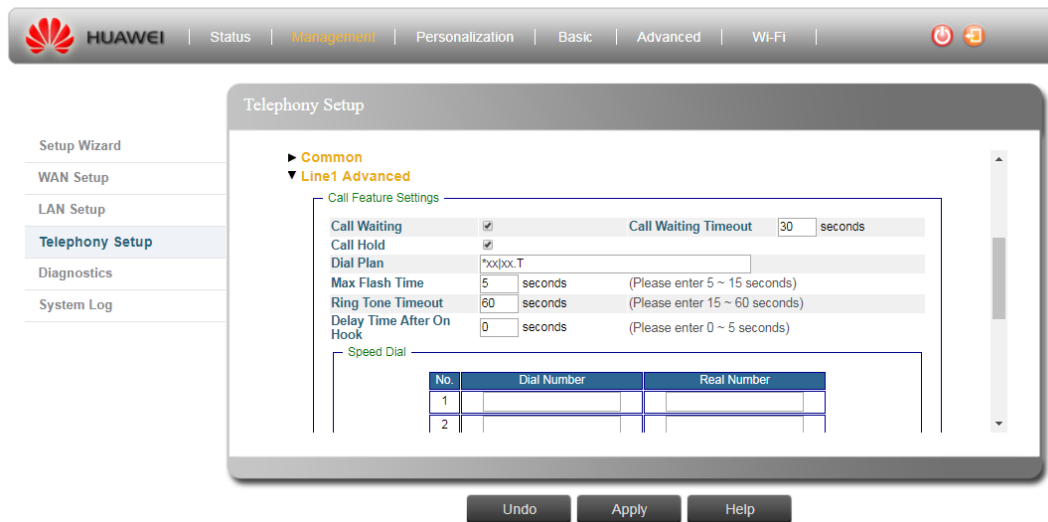


Figure 4- 14 Telephony - Speed Dial

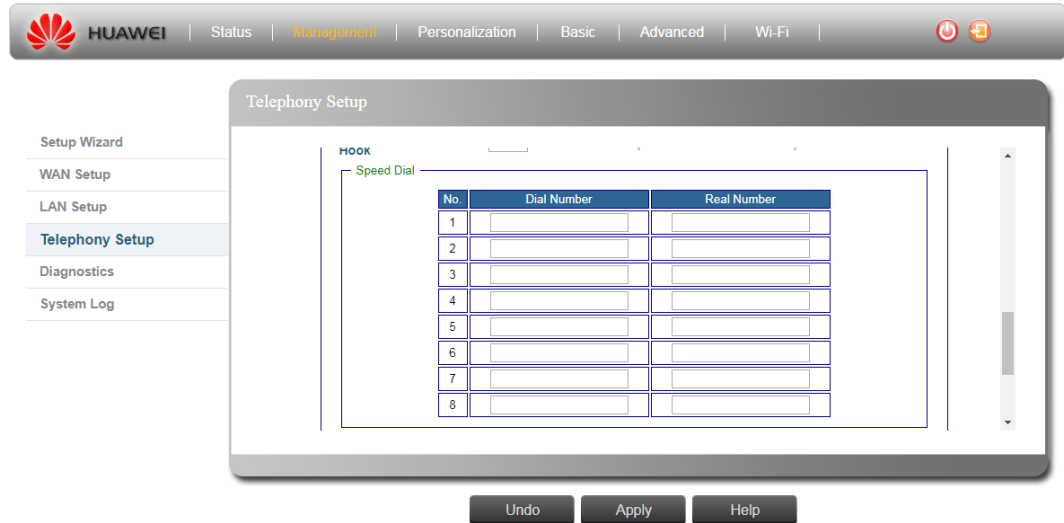
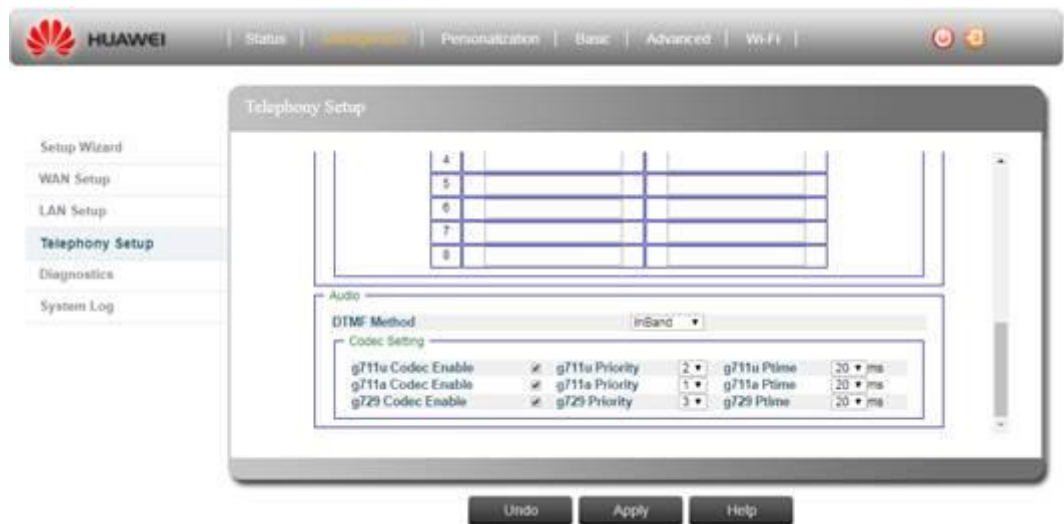


Figure 4- 15 Telephony - Audio



Enable VoIP

This is a check box, please checked to enable the VoIP function or un-check to disable VoIP.

Account

- **User account**

- **Username**

The SIP (Session Initiation Protocol) User name. Its format depends on the SIP Server.

- **User Account**

The SIP Account. Its format depends on the SIP Server.

- **Password**

The SIP user Password.

- **Password Confirm**

Enter the SIP user Password again.

- **Display Name**

Enter the name that will be displayed as your ID/number, for the outgoing call the receiver will see your Display name as Caller ID (if supported by the SIP server).

- **Server Account**

- **User Domain**

This LTE Device's domain name.

- **Registrar Address**

SIP server IPv4 address

- **Outbound Proxy Address**

A SIP Outbound Proxy acts, like any proxy server. Listening on an unblocked port number and forwarding requests between SIP client and your VoIP provider, it helps bypassing the restrictions imposed by your Internet provider.

If both an Outbound Proxy and a Registrar are configured, the Register message is sent to the Outbound Proxy, which forwards it to the Registrar.

- **DNS SRV**

We use DNS procedures to allow the client to resolve a SIP Uniform Resource Identifier (URI) into the IP address, port, and transport protocol of the next hop to contact. By default, we compiled with basic DNS functionality that includes A/AAAA queries to resolve IP addresses of hosts given as a domain name. The CPE enables a second mode of operation, an DNS SRV mode. When using the DNS SRV mode, the behavior of the ability to maintain a list of resolved addresses that the application will be able to try one after the other, in case of a send failure.

- **Registrar Port**

Port number of the SIP Server.

- **Outbound Proxy Port**

The number of the Port on which the outbound Proxy listens.

- **RTP Port Range Start**

Enter the listening start port number(s) for RTP traffic, if your VoIP service provider gave you this information. Otherwise, keep the default values.

- **RTP Port Range End**

Enter the listening end port number(s) for RTP traffic, if your VoIP service provider gave you this information. Otherwise, keep the default values.

IF you only have one port for listening RTP, please insert the same number in Start/End field.

- **Tone Setting Selection**

- **Tone Setting:**

You can select the tone settings according to your country. If your country is not listed in this list, or if you want to set a custom tone sound, you can select the manual option and determine the tone sound in the fields below.

- **Ring Back Tone**

You can determine the ring tone sound here

- **Frequency Quota:**

You can set the ring tone frequency here, the value should between 300~800 Hz. The device supports to set 1 or 2 frequency.

- **Ring Back Tone On:**

Set ring back tone continues for how long in a ring tone cycle, please enter 0~4 seconds

or asterisk (*) to set continue on

– **Ring Back Tone Off**

Set ring back tone off for how long-in a ring tone cycle, please enter 0~10 seconds.

• **Call Waiting Tone**

You can determine the call waiting tone sound here

• **Frequency Quota:**

You can set the call waiting tone frequency here, the value should between 300~800 Hz. The device supports to set 1 or 2 frequency.

– **Call Waiting Tone On:**

Set call waiting tone continues for how long in a ring tone cycle, please enter 0~4 seconds or asterisk (*) to set continue on

– **Call Waiting Tone Off:**

Set call waiting tone off for how long in a ring tone cycle, please enter 0~10 seconds.

1. **Dial Tone**

You can determine the dial tone sound here

– **Frequency Quota:**

You can set the dial tone frequency here, the value should between 300~800 Hz. The device supports to set 1 or 2 frequency.

– **Dial Tone On:**

Set dial tone continues for how long in a ring tone cycle, please enter 0~4 seconds or asterisk (*) to set continue on

– **Dial Tone Off**

Set dial tone off for how long in a ring tone cycle, please enter 0~10 seconds.

• **Busy Tone**

You can determine the busy tone sound here

– **Frequency Quota:**

You can set the busy tone frequency here, the value should between 300~800 Hz. The device supports to set 1 or 2 frequency.

– **Busy Tone On:**

Set busy tone continues for how long in a ring tone cycle, please enter 0~4 seconds or asterisk (*) to set continue on.

– **Busy Tone Off**

Set busy tone off for how long in a ring tone cycle, please enter 0~10 seconds.

• **Audio**

– **Fax mode:**

What codec if you do a fax action. (T.38 Mode / G.711a Passthrough Mode / G.711u Passthrough Mode).

Advanced

• **Call Feature Settings**

– **Call Waiting**

Enables or Disable the second caller can wait on line while you are on the call, you can press the flash key on the telephone to switch the call.

– **Call Waiting TimeOut**

Enter a number of seconds after which the call waiting is timed out

– **Call Hold**

Enables or Disable the Call Hold function

The Call Hold function is allow you to hold current call by press the flash key on the telephone

– **Dial Plan**

A dial plan is a set of rules used for determining whether a complete set of numbers has been entered for the IP address of SIP server.

The device support two dial plans:

***xx :**

"*" represent the asterisk key on the phone; "x" represent any number (0~9). This dial plan is for the two digits number start with "*"|" represent or, you can set several dial plans but separate them by |.

xx.T :

"x" represent any number(0~9) ; "." means arbitrary number of digits ; T is just a symbol means end number. You didn't need to key-in anything to end the dial, just wait dial time out (3sec), if you don't want to wait for 3sec, just set the dial plan as: xx.#. For example, you could dial 1111#, and the phone number 1111 would be dialed immediately.

– **Max Flash Time**

Set the max Flash key press time, if you press the Flash key over x seconds define in the column, the action will be ignored. (Please enter 5~15 seconds).

– **Ring Tone TimeOut**

Set how long you want the ring tone exist. (Please enter 15 ~ 60 seconds)

– **Delay Time After On Hook**

Set a really hang up delay time. When you hang up the call for x seconds the call will be really dropped. (Please enter 0 ~ 5 seconds).

– **Speed dial**

Please pre-set the mapping table for speed dial.

– Dial Number: Please define the speed dial number, this column is only allow to key-in: numbers 0~9

– Real Number: Please correctly fill-in the real dial number here, this column is only allow to key-in: numbers 0~9,#,*

• **Audio**

– **DTMF Method**

You can select different DTMF method here; there are three options InBand / RFC2833/ SIPInfo.

– **Codec Setting:** Codec Enable: There are three codecs supported: g711u/g711a/g729. Check the checkbox to enable or uncheck to disable.

Priority: You can also set the priority of the codec

Ptime: It defines the length of time in milliseconds represented by the media in a packet. The ptime value tells the length of the speech block in the RTP packets. For the g711 u/a codecs, there are four options: 5/10/20/30ms; for the g729, there are three options: 10/20/30ms.

4.1.5 Management > Diagnostics

This Diagnostics page will help you to perform a Ping or the Traceroute to troubleshoot the network connection.

Figure 4- 16 Diagnostics - Ping

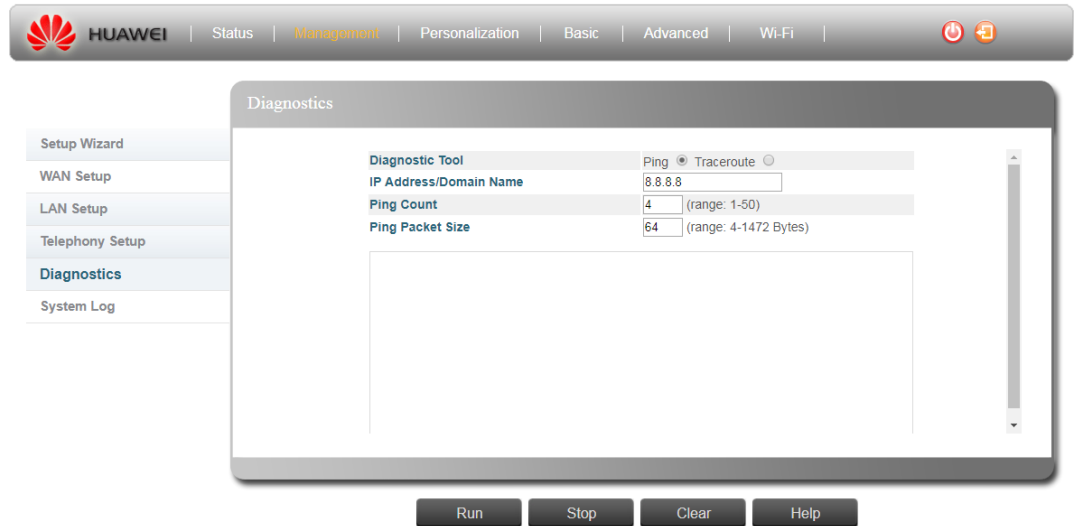
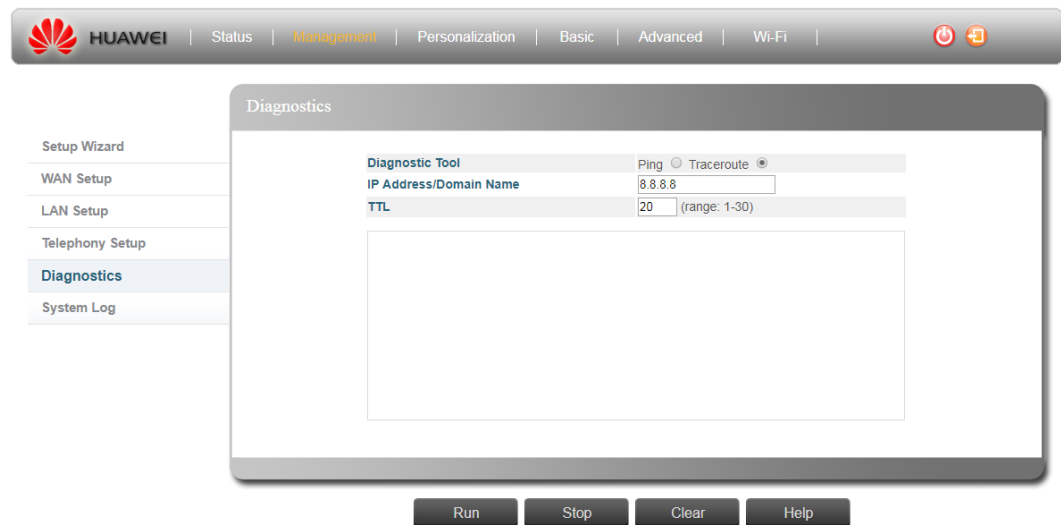


Figure 4- 17 Diagnostics - Traceroute



Diagnostics Tool

- **Ping**

- **IP address/Domain Name:**

To issue a Test, please enter the destination IP address and Domain name here.

- **Ping Count:**

Please fill how many times the test need to be performed (Range: 1-50).

- **Ping Packet Size:**

Please fill how many buffer you want to add in a range of 4-1472 Bytes.

Example

If the CPE fails to access the Internet, run the ping command to preliminarily identify the problem. To do so:

1. Choose **Management > Diagnostics**. On the Diagnosis Tools, set to **Ping**. The Ping page is displayed.
2. Enter the IP or domain name in the **IP address/Domain Name** field, for example, www.google.com.
3. Set **Ping Count** and **Ping Packet Size**.
4. Click **Run**
5. Wait until the ping command is executed.
6. The execution results are displayed in the box.

Diagnostic Tool

- **Traceroute**

- **IP address/Domain Name:**

- To issue a Test, please enter the destination IP address and Domain name here.

- **TTL**

- Time To Live value; in the Traceroute test, please fill in a test value for the packet path time and check what is the path time that a packet takes to the specified host (Range: 1-30).

Example

If the CPE fails to access the Internet, run the traceroute command to preliminarily identify the problem. To do so:

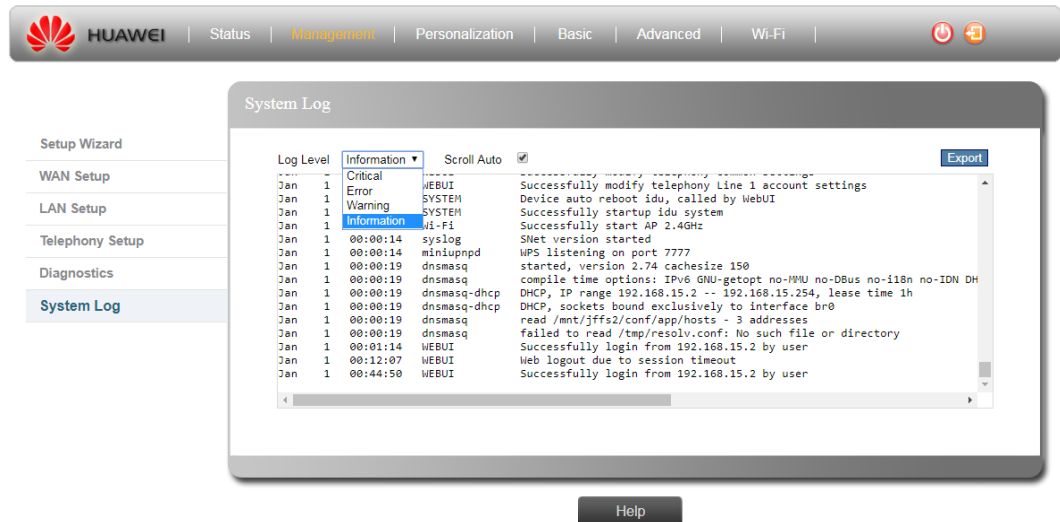
1. Choose **Management > Diagnostics**. On the Diagnosis Tools, set to **Traceroute**. The Traceroute page is displayed.
2. Enter the IP or domain name in the **IP address/Domain Name** field, for example, www.google.com.
3. Set **TTL**
4. Click **Run**
5. Wait until the traceroute command is executed.
6. The execution results are displayed in the box.

4.1.6 Management > System Log

The system log allows you can provide more detail information to your network provider.

System log will not be recorded any individual privacy.

Figure 4- 18 System Log



Log level

There are four levels pre-defined: Critical/Error/Warning/Information, Please see below table.

- **Scroll Auto:**

If you checked the Scroll Auto checkbox the syslog will always scroll to the bottom line to display the latest log

If you just want to view the previously log, please un-checked it.

- **Export:**

You can export your syslog out for the further analysis or issue tracking; the export format will be the .txt file with .tar compress.

- **System Log**


Information	<ul style="list-style-type: none"> • System <ul style="list-style-type: none"> - Start/Reboot/Reset • Connection Manager <ul style="list-style-type: none"> - WAN Connection - WAN IP obtained • VoIP <ul style="list-style-type: none"> - Started/Stopped - Register to SIP server - Call Out/In - Call session established • Wi-Fi <ul style="list-style-type: none"> - AP: started/stopped - Client: associated/disassociated • FOTA <ul style="list-style-type: none"> - Started/Stopped - Periodic Firmware check/upgrade result
--------------------	---

	<ul style="list-style-type: none"> - Starts download firmware - Start upgrade firmware • TR069
Warning	<ul style="list-style-type: none"> • Connection Manager <ul style="list-style-type: none"> - SIM card is not inserted - Verify PIN failed • VoIP <ul style="list-style-type: none"> - Failed to register to SIP - Failed to establish phone call - Failed to send register message to SIP server • Wi-Fi <ul style="list-style-type: none"> - Client: unauthorized • FOTA <ul style="list-style-type: none"> - Failed to connect to server - Failed to download Packages or firmware • TR069
Error	<ul style="list-style-type: none"> • FOTA <ul style="list-style-type: none"> - Failed to upgrade firmware - Failed to verify firmware • TR069
Critical	

- **Operation Log**

Information	<ul style="list-style-type: none"> • Web login/logout by user • Web logout due to session timeout • Web login password is changed • DHCP server IP is changed • Firewall level is changed • Block/Un-block DHCP client • FW upgrade from UI • Wi-Fi SSID is changed • Wi-Fi security is changed • Modify each page • Start/Stop WPS • Start/Stop Ping • Start/Stop Traceroute • Export/Import Configuration File
Warning	<ul style="list-style-type: none"> • Web login is failed • User cancels the upgrade notification

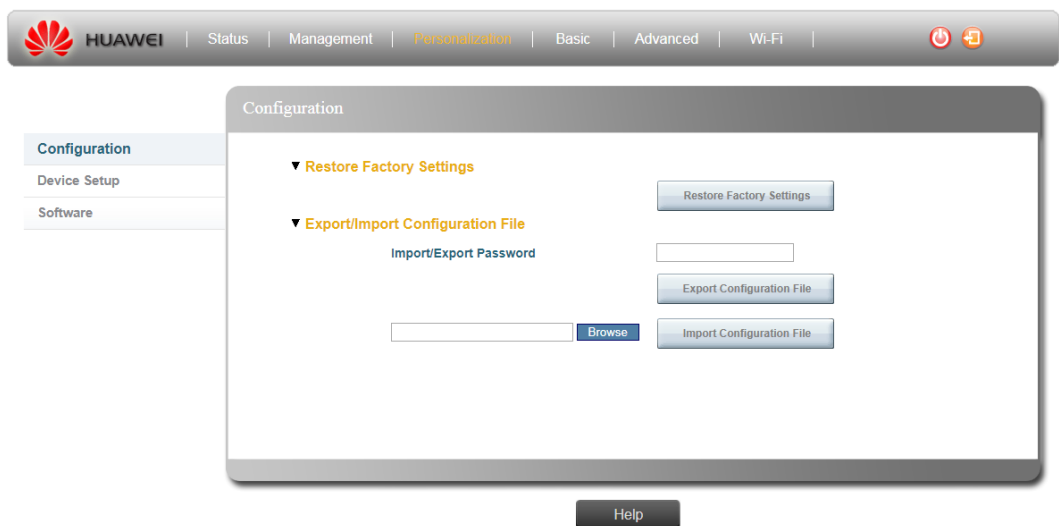
	<ul style="list-style-type: none"> Firmware upgrade fail
Error	
Critical	

	UNABLE to export System Log on IE8 browser
---	--

4.2 Personalization

4.2.1 Personalization > Configuration

Figure 4- 19 Configuration



Restore Factory Settings

You can use Reset Factory Settings function to set device to factory default settings. When returning to factory defaults, it will reset all the parameters/settings you had ever done. All the changes different from factory default settings will be lost; you will need to manually change the parameter again.

- Restore Factory Settings**


To restore settings to factory defaults, click the Restore Factory Settings button. After applying factory defaults, device will reboot.

Export/Import Configuration File

- Import/Export Password**

Before export the file or import a file you need to input the password here (Password must contain 2 cases of uppercase letter, lowercase letter, number, space, and special characters(^~!@#\$\$%^&*()-_+=|[{}];:","<.>/?)) Length is 8 - 128; Import/Export Password would be the same as login password.

- **Export Configuration File**
You could export all of user settings in this device to a file.
- **Import Configuration File**
You could browse a configuration file and import it back.

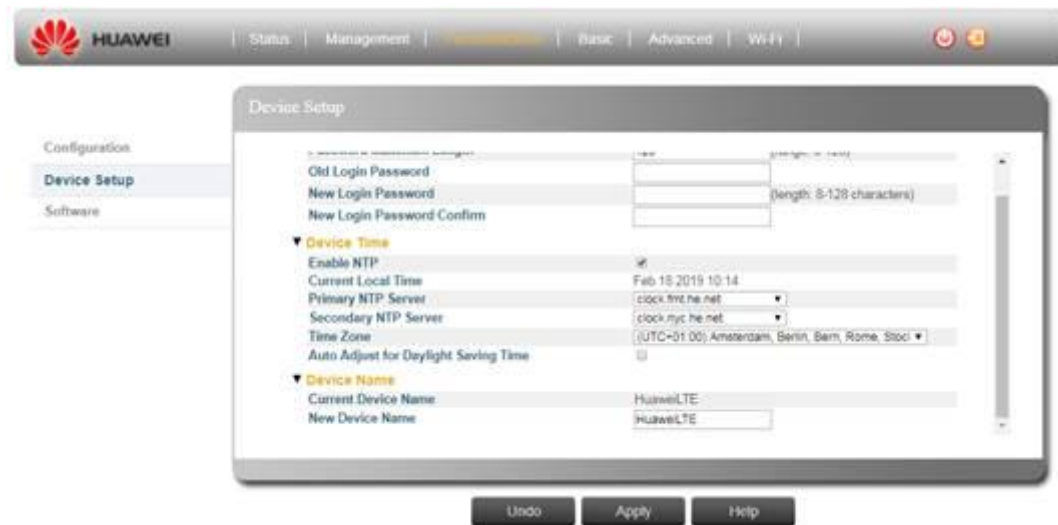
	<ol style="list-style-type: none">1. UNABLE to export Configuration file on IE8 browser.2. The imported config file name must be alphabet (A-Z or a-z), digit (0-9), minus sign (-) and underline(_).3. The imported config file name extension must be ".tar".
---	---

4.2.2 Personalization > Device Setup

Figure 4- 20 Device Setup - Password



Figure 4- 21 Device Setup - Device Time & Device Name



Password

You can change the default Graphical User Interface (GUI) access password here.

- **Password Maximum Length:**

Please define the password maximum length here in a range of 8~128.

- **Old Login Password:**

Input the original /current login password.

- **New Login Password:**

Enter a new log-in password you want to change, the new password total digits can't more than the value you set on the "**Password Maximum Length**" column.

- **New Login Password Confirm:**

Enter the new password again for verification.



You need to change the default Login passwords while the first time log-in. Please change the default password to protect your account.

Device Time

The modem uses the Simple Network Time Protocol (SNTP) to set its internal clock based on periodic updates from a time server. Maintaining an accurate time on the device will keep the system log to recording meaningful dates and times for event entries.

The Device Time area displays the following information:

- **Enable NTP**

Allows user to connect what type of time server, if any.

- **Current Local Time**

Displays the current time of the system clock.

- **Primary NTP Server**

You can change the Primary NTP server if the default NTP server is not work.

- **Secondary NTP Server**

You can set the secondary NTP server in case of the Primary NTP server didn't work in some time.

- **Time Zone**

SNTP uses Greenwich Mean Time, or GMT (also known as Universal Time Coordinated, or UTC) based on the time at the Earth's prime meridian, zero degrees longitude. To display a time corresponding to your local time, select your time zone from the pull-down list. The default is UTC-06.00, for Central Time (US and Canada.)

- **Auto Adjust for Daylight Saving Time**

Select this check-box to set the daylight saving time if the unit operates in a region that observes daylight saving time.



Click the **Undo** to clear the changes that you have made to this window.

Click the **Apply** to activate your changes.

4.2.3 Personalization > Software

Figure 4- 22 Software - Upgrade from file



- **Upgrade From file:**
 - a. Click Browse button to select the IPK file. The IPK is the file with .ipkg, in each release you will get the ipk file release
huawei-indoor-nomodem-unknown_V100R001C00SPCxxx_mips.ipk
 - b. Click Install Software button to install the selected IPK file.
- **Upgrade From FOTA: (Remote management server):**

Please manually press "**Check Version**" button and device will request the latest update from the remote access server.

After checked, server will return message: *Can't connect to Server/Latest Version, if your device SW is not up to date, you can do update or not.*

	<p>While FW is upgrading, please keep your device powering on. Don't turn off the device to prevent the possible damage.</p> <p>The upgrade FW name must be alphabet (A-Z or a-z), digits (0-9), dot(.), minus sign (-), and underline (_).</p> <p>The upgrade FW file name extension must be ".ipk".</p>
--	---

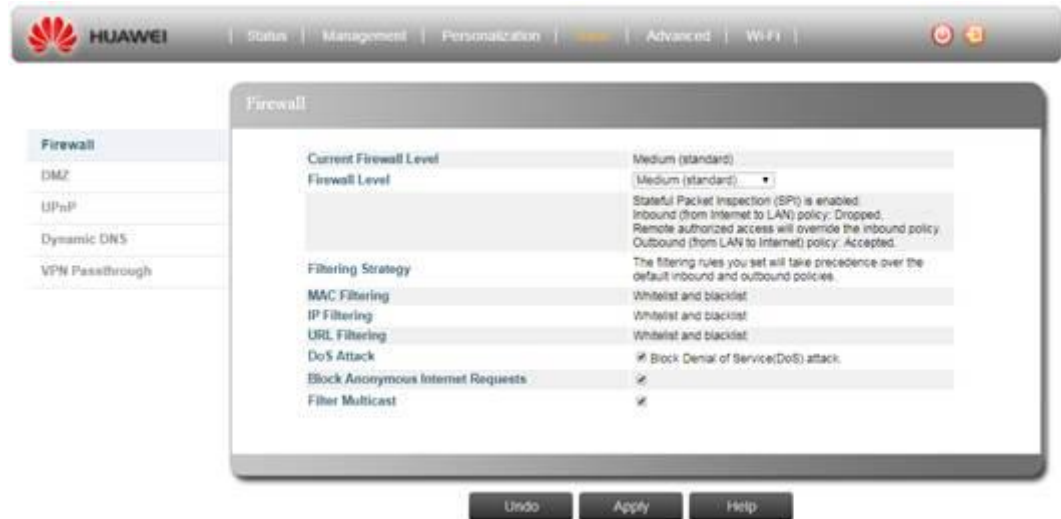
4.3 Basic

4.3.1 Basic > Firewall

The modem provides extensive firewall protection by restricting connection parameters to limit the risk of intrusion and defending against a wide array of common hacker attacks.

This page is to configure and change the firewall settings. The firewall feature can be used to block unauthorized access and allowing only authorized communications from the Internet network. It also allows the device to be managed over the Internet by authorized user.

Figure 4- 23 Firewall



Current Firewall Level

Shows the current device firewall level.

Firewall Level

Allows user to change the device firewall level here, there are four options pre-defined:

- Low (filtering disabled)
- Medium (standard)
- High
- Custom (If you chose Custom option, you can customize the MAC Filtering, IP Filtering and URL Filtering options)

Filtering Strategy

The filtering rules you set will take precedence over the default inbound and outbound policies.

MAC Filtering

Block or allow the client device's internet access via MAC address, you can go Advanced > MAC Filtering to edit whitelist and blacklist

IP Filtering

Block or allow the client device's internet access via IP address, you can go Advanced > IP Filtering to edit whitelist and blacklist

URL Filtering

Block or allow the client device's internet access via URL(web address), you can go Advanced > URL Filter to edit whitelist and blacklist

DoS Attack


Block Denial of Service (DoS) attack from the LAN and Internet, such as SYN floods and ping floods.

Block Anonymous Internet Requests

Select this check-box to reject anonymous Internet requests

Filter Multicast

Select this check-box to filter out multicast packets

	Click the Undo to clear the changes that you have made to this window. Click the Apply to activate your changes.
---	---


4.3.2 Basic > DMZ

For applications that require unrestricted access to the Internet, you can configure a specific client/server as a demilitarized zone (DMZ).

Figure 4- 24 DMZ

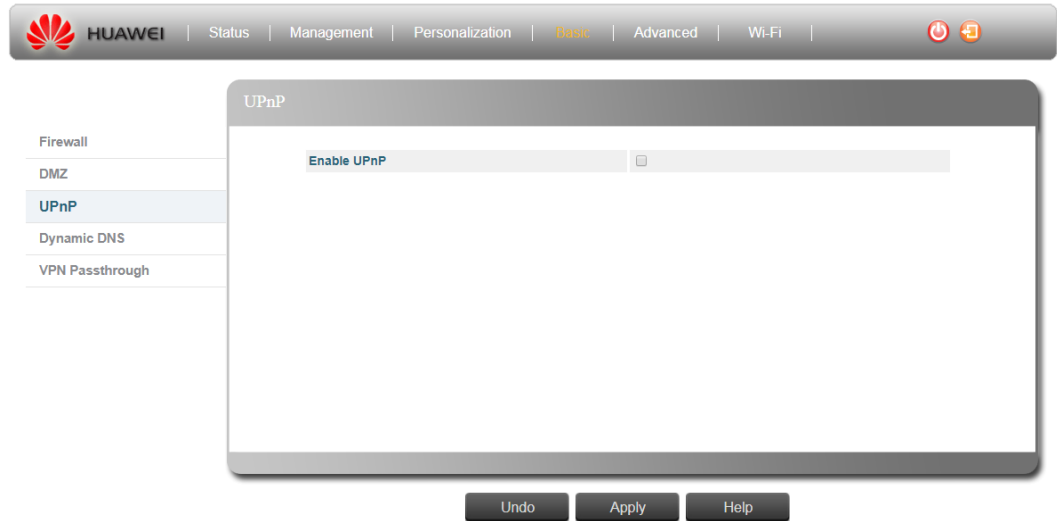


- **Enable DMZ** Select this check-box to enable or disable DMZ.
- **DMZ IP Address** Set client/server that acts as a "neutral zone" (DMZ stands for "Demilitarized Zone") and separates an internal network from a public one in order to prevent outside access to private data. The DMZ forwards the network traffic to specific hosts based on the protocol and port number.

	Click the Undo to clear the changes that you have made to this window. Click the Apply to activate your changes.
---	---

4.3.3 Basic > UPnP

Figure 4- 25 UPnP



UPnP

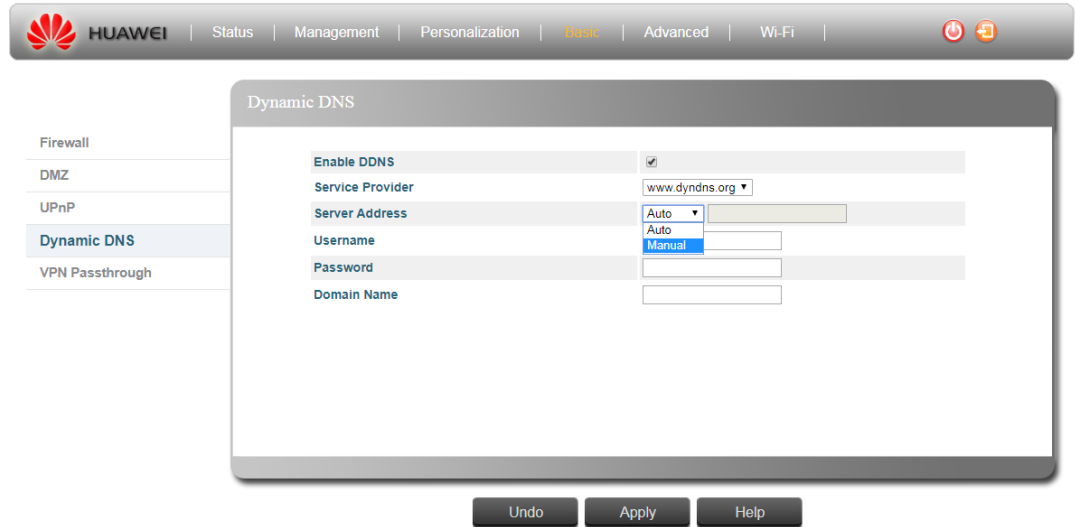
Enable UPnP IGD - Select this check-box to enable/disable Universal Plug and Play Internet Gateway Device - a protocol that simplifies device connection and network implementation. When this option is enabled, certain Windows applications would setup the port forwarding rule dynamically.

	Click the Undo to clear the changes that you have made to this window. Click the Apply to activate your changes.
--	---

4.3.4 Basic > Dynamic DNS

Dynamic Domain Name System (DNS) is a mechanism used for translating host names for network nodes into IP addresses in real-time. This page allows enabling the Dynamic DNS and selecting the service provider. The Dynamic DNS page includes the following parameters:

Figure 4- 26 Dynamic DNS




Enable DDNS

Select this check-box if the unit has a non-static IP address to keep the domain name associated with an ever-changing IP address. When DDNS is enabled, configure the following parameters:

- Server Address
- Username
- Password
- Domain Name

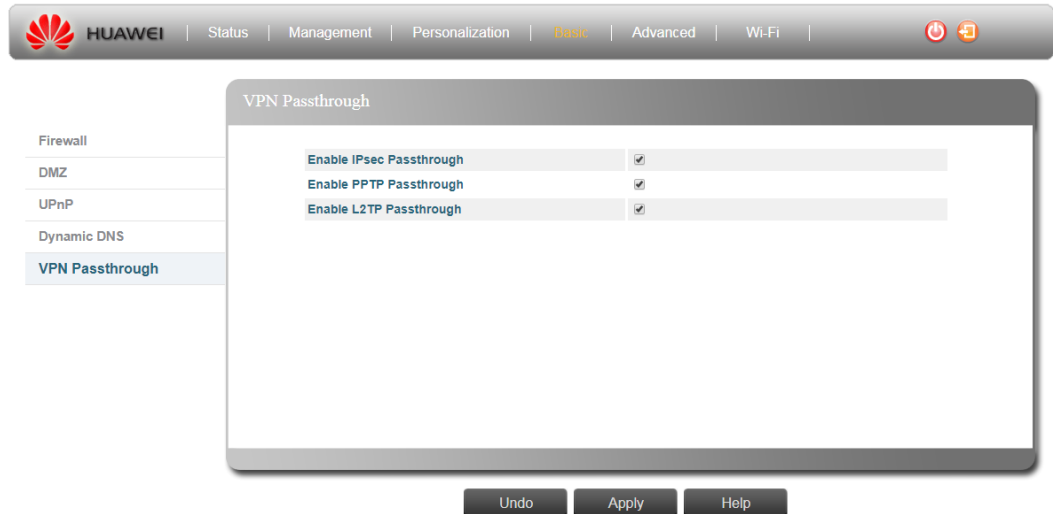
Service Provider

Select the DDNS service provider from the drop-down list.

	<p>Click the Undo to clear the changes that you have made to this window.</p> <p>Click the Apply to activate your changes.</p>
---	--

4.3.5 Basic > VPN Passthrough

Figure 4- 27 VPN Passthrough



Enable IPsecPassthrough


Internet Protocol Security; IPsec provides encrypted security services at the IP layer, and enables to use encrypted tunnels/traffic between two hosts.

Enable PPTP Passthrough

Point to Point Tunneling Protocol; This protocol enables the transfer of data packets of TCP/IP through a foreign network that is not based on these protocols (by marking the packet with an address suited to the foreign network).

Enable L2TP Passthrough

Layer 2 Tunneling Protocol; An open standard with multivendor interoperability and acceptance.

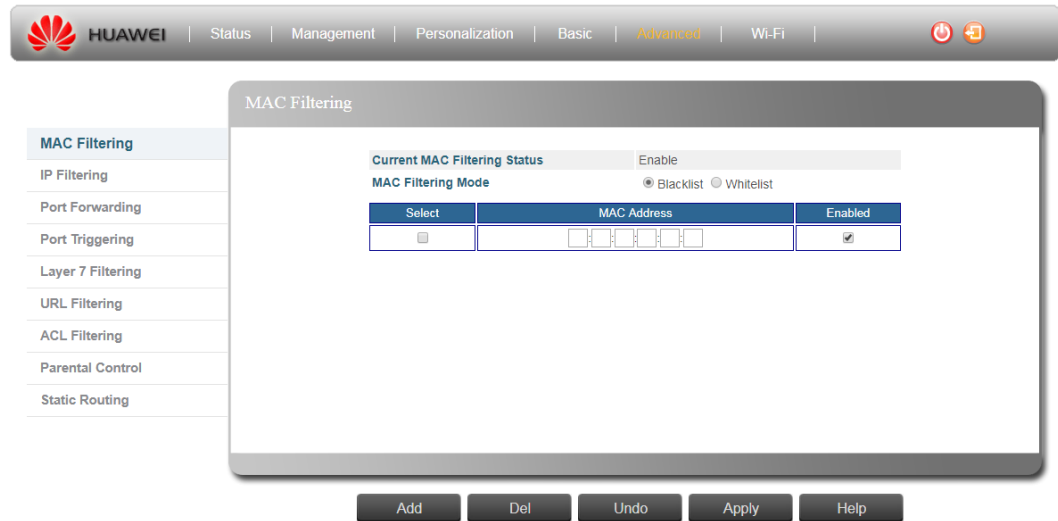
	<p>Click the Undo to clear the changes that you have made to this window.</p> <p>Click the Apply to activate your changes.</p>
---	--

4.4 Advanced

4.4.1 Advanced > MAC Filtering

You can block access to the Internet from clients on the local network by MAC addresses. In the MAC Filter page you set MAC addresses to be filtered out by the security system. You can add addresses to the filtered group or delete them, and also enable or disable filtering at different times. The following configuration parameters are available:

Figure 4- 28 MAC Filtering



Current MAC filtering Status

Shows the MAC filtering function is disable or enable.

To enable or disable, you need to go to the **Basic > Firewall level** to change the firewall setting.

- **Low:** Filtering disable
- **Medium:** Filtering enable, you can set filtering by blacklist or whitelist on **MAC filtering mode**.
- **High:** Filtering enable, you can set filtering by blacklist or whitelist on **MAC filtering mode**.
- **Custom:** You can customize if you want to Disable or set Blacklist/Whitelist

Disable Blacklist Whitelist

MAC filtering Mode

Select MAC filtering by Whitelist or Blacklist

- **Blacklist:** Block internet access which listed on the blacklist.
- **Whitelist:** Will ONLY allow the units listed on the list to access the network.

Select


Selecting this check-box and press Del button to delete this row.

MAC address:

Please key-in the client device which you want to do the MAC filtering MAC address.

Enabled

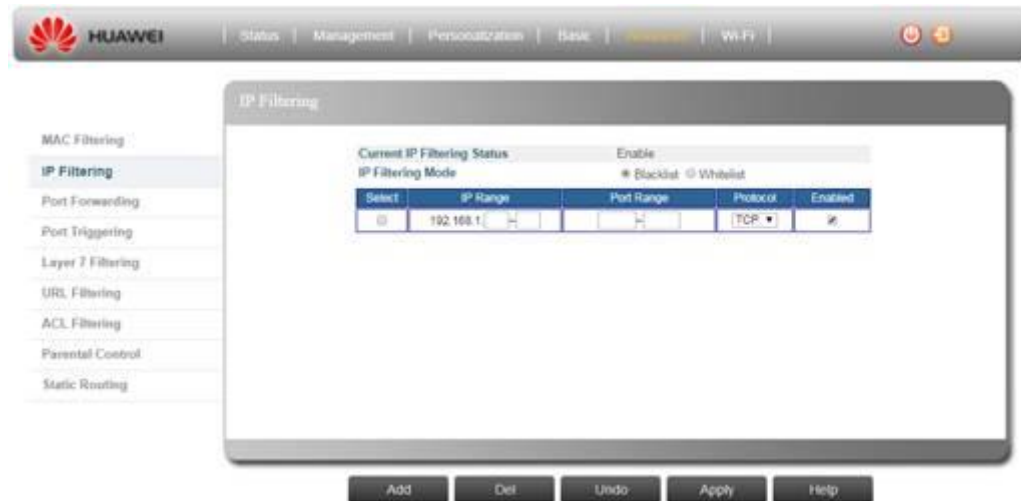
Select this check-box to enable/disable filter for the specific client device's MAC address

	<p>Use the Add or Del buttons to add the rule to the group or clear it from the group, please click Apply button to confirm the Add or Del.</p> <p>Click the Undo to clear the changes that you have made to this window.</p> <p>Click the Apply to activate your changes.</p>
---	---

4.4.2 Advanced > IP Filtering

You can block access to the Internet from clients on the local network by specifying IP addresses and TCP/UDP port numbers. You can configure up to five IP filters on the unit. In the IP Filter page you set IP addresses to be filtered out by the security system. You can add addresses to the filtered group or delete them. You can also enable or disable filtering at different times. The following configuration parameters are available:

Figure 4- 29 IP Filtering



Current IP filtering Status

Shows the IP filtering function is disable or enable.

To enable or disable, you need to go to the **Basic > Firewall level** to change the firewall setting.

- **Low:** Filtering disable
- **Medium:** Filtering enable, you can set filtering by blacklist or whitelist on **IP filtering mode**.
- **High:** Filtering enable, you can set filtering by blacklist or whitelist on **IP filtering mode**.
- **Custom:** You can customize if you want to Disable or set Blacklist/Whitelist

Disable Blacklist Whitelist

IP filtering Mode

Select IP filtering by Whitelist or Blacklist

- Blacklist: Block internet access which listed on the Blacklist.
- Whitelist: Will ONLY allow the units listed on the list to access the network.

Select

Selecting this check-box and press Del button to delete this row.

IP Range

Specify an IP address or range on the local network

Port Range


Enter the port range to be filtered.

Protocol

Set the protocol to be filtered: TCP or UDP.

Enabled

Select this check-box to enable or disable filtering for the specific table entry.

	<p>Use the Add or Del buttons to add the rule to the group or clear it from the group, please click Apply button to confirm the Add or Del.</p> <p>Click the Undo to clear the changes that you have made to this window.</p> <p>Click the Apply to activate your changes.</p>
---	--

4.4.3 Advanced > Port Forwarding

Port Forwarding instructs the router to which computer on the local area network to send data. According to the port forwarding rules or setup, the router sends the data from the external IP address: port number to an internal IP address: port number. Port Forwarding rules are created per port. The Port Forwarding page enables managing and setup of the rules for Port Forwarding. The following configuration parameters are available:

Figure 4- 30 Port Forwarding



Select

Select this check-box and press Del button to delete this row.

Protocol

Set the protocol for port forwarding: TCP, UDP or Both.

WAN Port

Enter the port number range for WAN side.

LAN Port


Enter the port number for LAN side.

LAN IP

Enter the IP address that identifies the IP subnet of the remote network.

Enabled

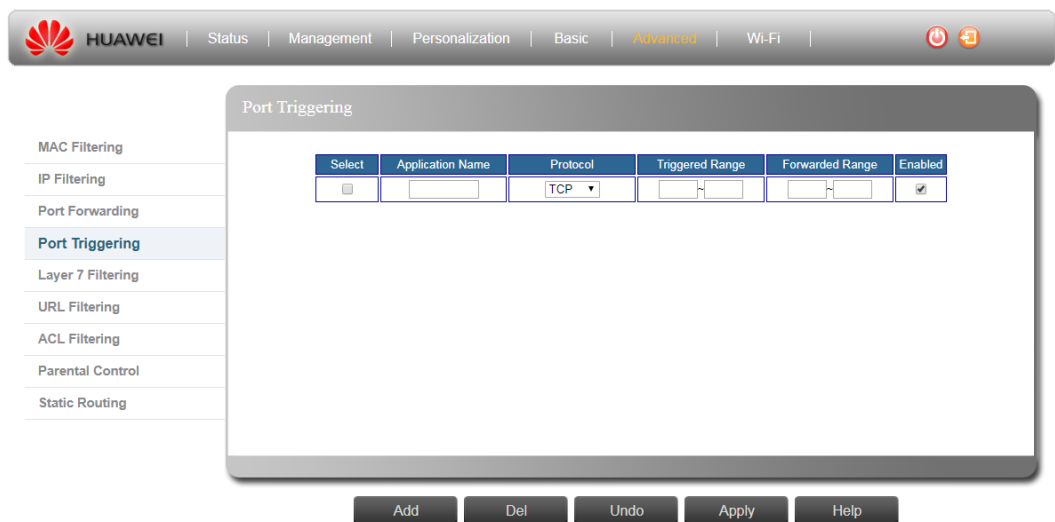
Select this check-box to enable/disable port forwarding for the specific IP.

	<p>Use the Add or Del buttons to add the rule to the group or clear it from the group, please click Apply button to confirm the Add or Del.</p> <p>Click the Undo to clear the changes that you have made to this window.</p> <p>Click the Apply to activate your changes.</p>
---	--

4.4.4 Advanced > Port Triggering

Port triggering is a way to automate port forwarding: outbound traffic on predefined ports ('triggering ports') causes inbound traffic to specific incoming ports to be dynamically forwarded to the initiating host, while the outbound ports are in use. This allows computers behind a NAT-enabled router on a local network to provide services that would normally require the computer to have a fixed address on the local network. Port triggering can open an incoming port when a client on the local network makes an outgoing connection on a predetermined port or range of ports. In the Port Triggering page you can specify up to 15 rules with parameters for Port Triggering. The following configuration parameters are available:

Figure 4- 31 Port Triggering



Select

Select this check-box and press Del button to delete this row.

Application Name

Enter a name for identifying this port trigger protocol.

Protocol

Set the protocol for port trigger: TCP, UDP or BOTH.

Triggered Range


Enter the trigger range (1~65535).

Forwarded Range

Enter the forwarded range (1~65535).

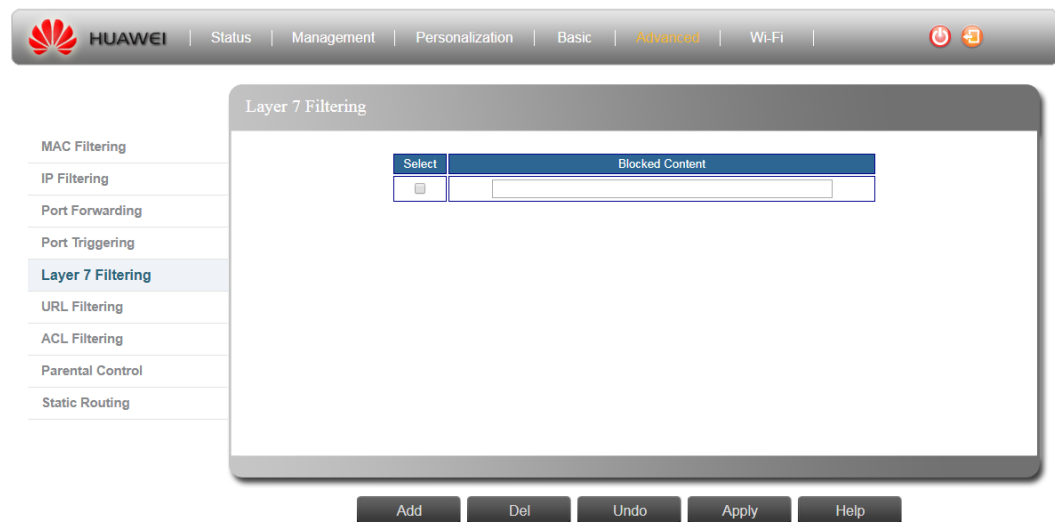
Enabled

Select this check-box to enable/disable port trigger for the specific application.

	<p>Use the Add or Del buttons to add the rule to the group or clear it from the group, please click Apply button to confirm the Add or Del.</p> <p>Click the Undo to clear the changes that you have made to this window.</p> <p>Click the Apply to activate your changes.</p>
---	--

4.4.5 Advanced > Layer 7 Filtering

Figure 4- 32 Layer 7 Filtering




Select

Select this check-box and press Del button to delete this row.

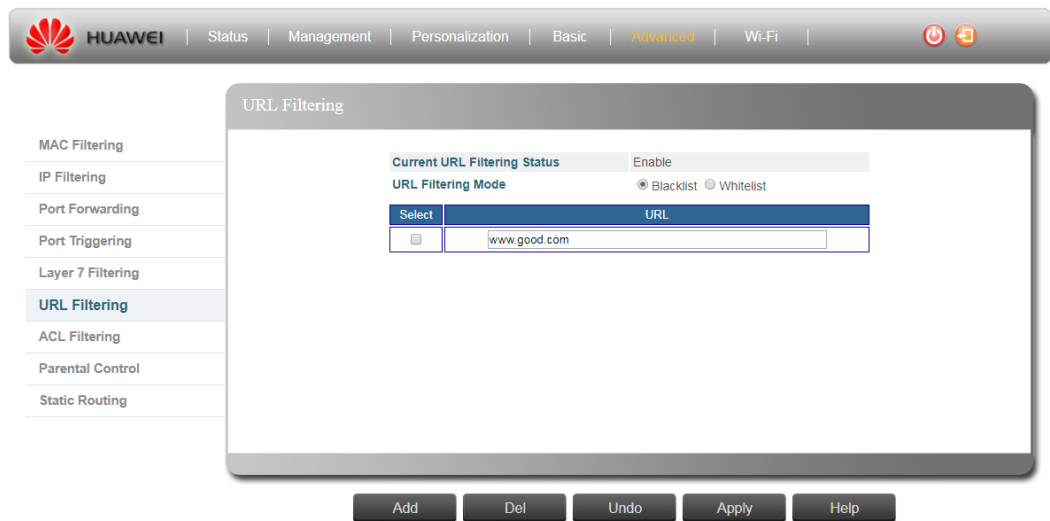
Blocked Content

Enter the keywords that need to be filtered on layer 7. (Please double check your Capital and Lower case letters, it matters to the filtering result)

	<p>Use the Add or Del buttons to add the rule to the group or clear it from the group, please click Apply button to confirm the Add or Del.</p> <p>Click the Undo to clear the changes that you have made to this window.</p> <p>Click the Apply to activate your changes.</p>
---	---

4.4.6 Advanced > URL Filtering

Figure 4- 33 URL Filtering



Current URL filtering status

Shows the URL filtering function is disable or enable.

To enable or disable, you need to go to the **Basic > Firewall level** to change the firewall setting.

- **Low:** Filtering disable
- **Medium:** Filtering enable, you can set filtering by blacklist or whitelist on **URL filtering mode**.
- **High:** Filtering enable, you can set filtering by blacklist or whitelist on **URL filtering mode**.
- **Custom:** You can customize if you want to Disable or set Blacklist/Whitelist

Disable Blacklist Whitelist

URL filtering mode

Select URL filtering by Whitelist or Blacklist

- **Blacklist:** Block internet access which listed on the Blacklist.
- **Whitelist:** Will ONLY allow the unit listed on the list to access the network.

Select

Select this check-box and press Del button to delete this row.

URL

Enter the URL or URL's keywords that needs to be filtered. (Please double check your

Capital and Lower case letters, it matters to filtering)

i	<p>Use the Add or Del buttons to add the rule to the group or clear it from the group, please click Apply button to confirm the Add or Del.</p> <p>Click the Undo to clear the changes that you have made to this window.</p> <p>Click the Apply to activate your changes.</p>
----------	--

4.4.7 Advanced > ACL Filtering

Figure 4- 34 ACL Filtering - 1

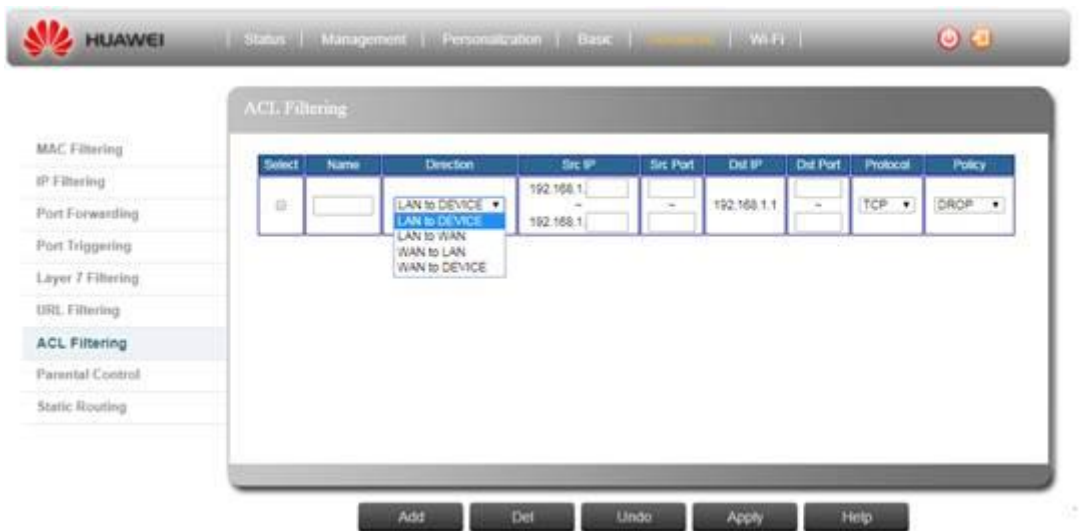


Figure 4- 35 ACL Filtering - 2

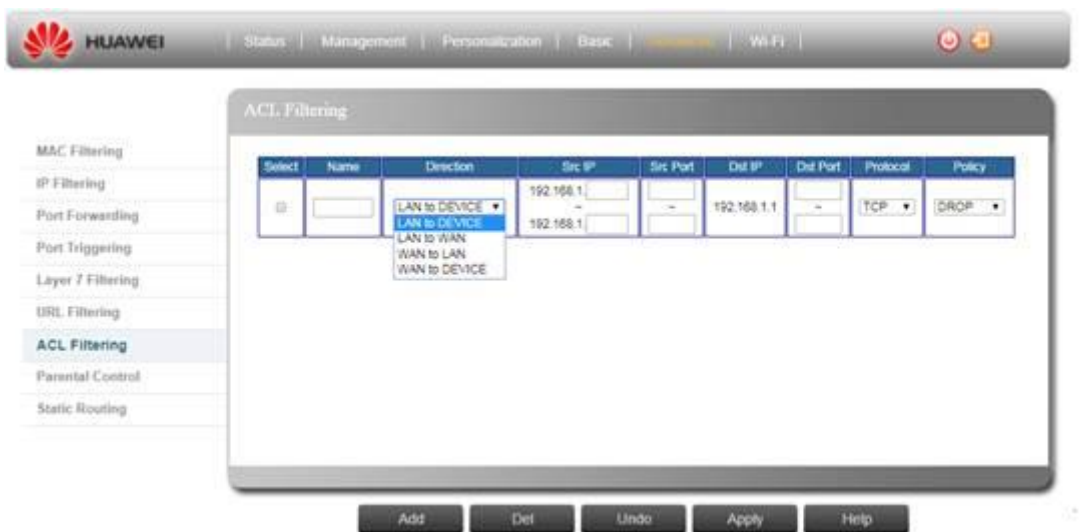


Figure 4- 36 ACL Filtering - 3



Select

Select this check-box and press Del button to delete this row.

Name

Enter a name for identifying this ACL filter rule; it is free defining with 10 units' characters.

Direction

Define which direction for the filter

- LAN to Device
- LAN to WAN
- WAN to LAN
- WAN to Device

Src IP

Please define the start and end source IP address that the filter rule applies.

Src Port

Please fill in the source port number range.

Dst IP

Please define the start and end destination IP address that the filter rule applies.

Dst Port

Please fill in the destination port number range.

Protocol

Please select which type of package for filtering.


- TCP
- UDP
- BOTH

Policy

Please define what action to do for the filtering.

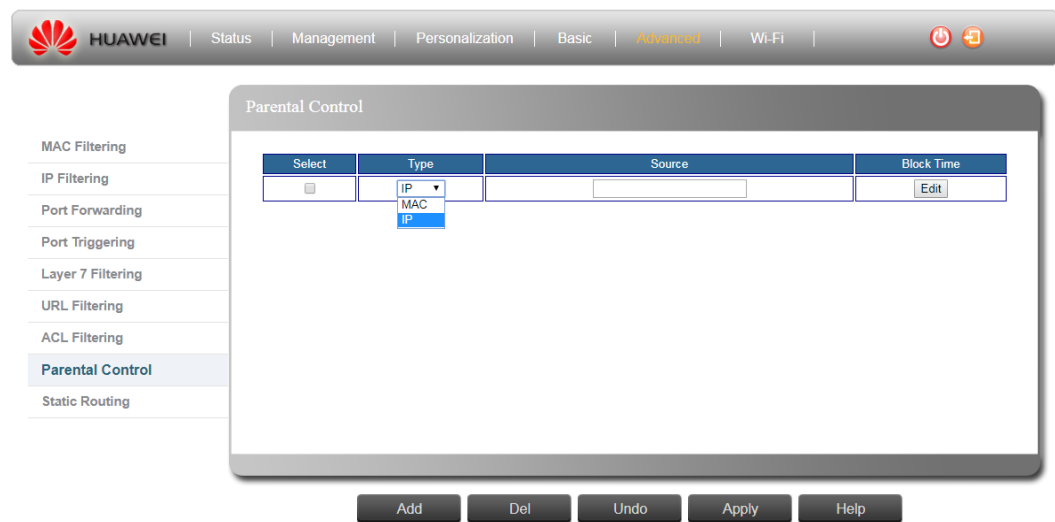
- DROP

- ACCEPT

	<p>Use the Add or Del buttons to add the rule to the group or clear it from the group, please click Apply button to confirm the Add or Del.</p> <p>Click the Undo to clear the changes that you have made to this window.</p> <p>Click the Apply to activate your changes.</p>
---	--

4.4.8 Advanced > Parental Control

Figure 4- 37 Parental Control



Select

Select this check-box and press Del button to delete this row.

Type


Which type you want to control

Source

Please fill-in the source IP/MAC address for the route.

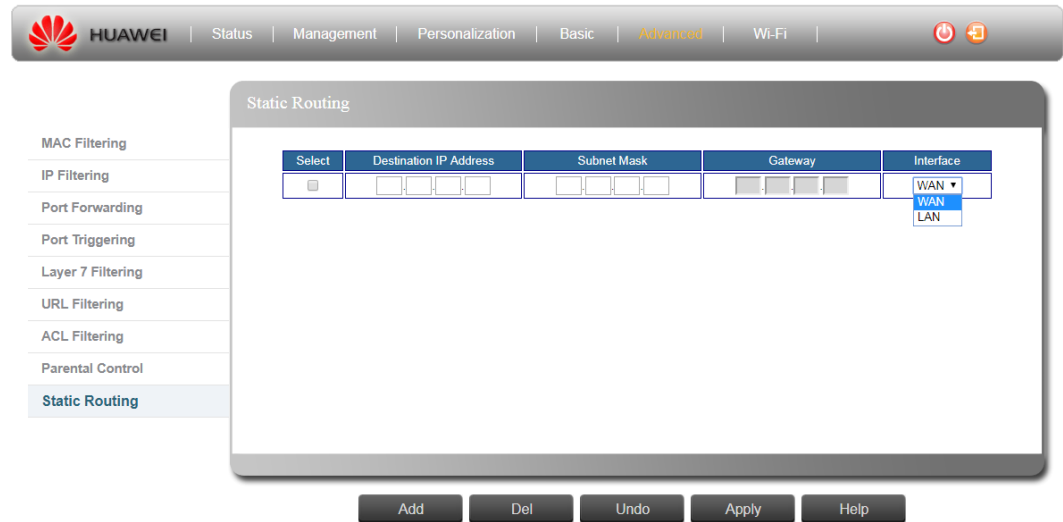
Block Time

Choose time to control the out-going traffic

	<p>Use the Add or Del buttons to add the rule to the group or clear it from the group, please click Apply button to confirm the Add or Del.</p> <p>Click the Undo to clear the changes that you have made to this window.</p> <p>Click the Apply to activate your changes.</p>
---	--

4.4.9 Advanced > Static Routing

Figure 4- 38 Static Routing - Gateway mode



Select

Select this check-box and press Del button to delete this row.

Destination IP Address

Please fill-in the destination IP address for the route.

Subnet Mask

Please fill-in the subnet mask of the destination IP network.

Gateway

Please fill-in Gateway IP of the destination IP network. (Only for LAN)

Interface

The gateway may be a router or switch on the same network segment as the device's LAN/WAN interface. Please indicate the interface for setting the route rule.



Use the **Add** or **Del** buttons to add the rule to the group or clear it from the group, please click Apply button to confirm the Add or Del.

Click the **Undo** to clear the changes that you have made to this window.

Click the **Apply** to activate your changes.

4.5 Wi-Fi

4.5.1 Wi-Fi > Basic

Figure 4- 39 Wi-Fi - Basic -1

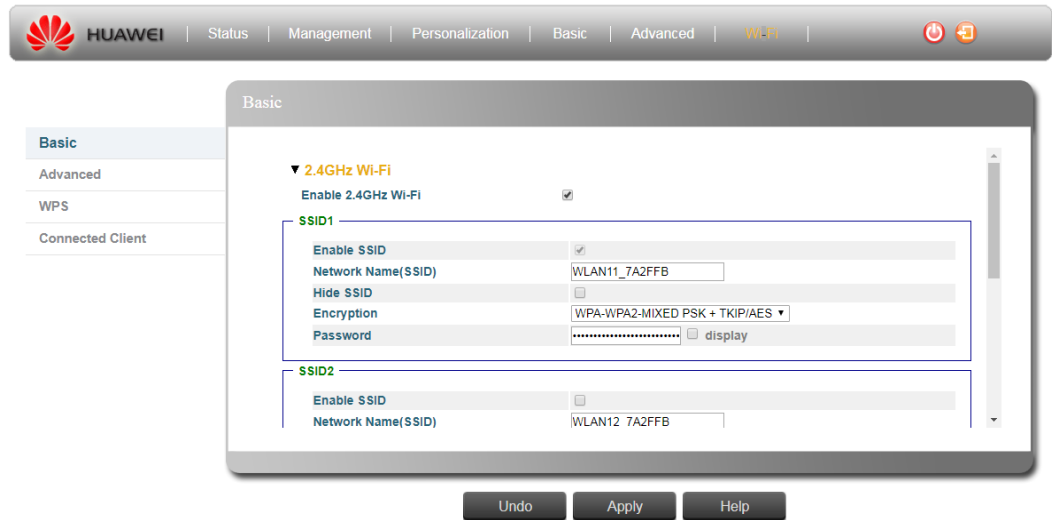
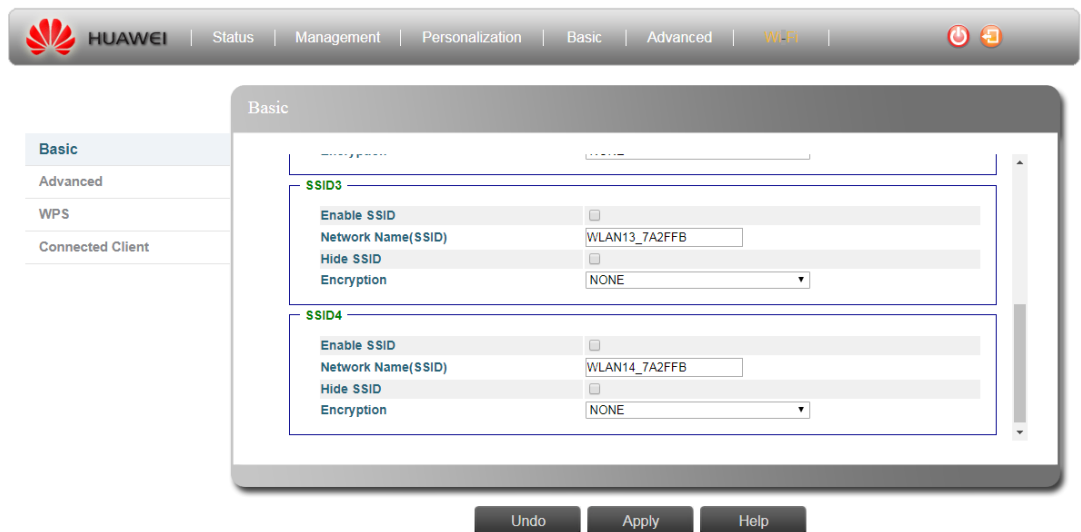


Figure 4- 40 Wi-Fi - Basic -2



Enable Wi-Fi

Enables / disables the Wi-Fi radio

2.4GHz Wi-Fi

- **Enable 2.4GHz Wi-Fi**

Enables / disables the 2.4GHz Wi-Fi radio.

- **Network Name(SSID1/SSID2/SSID3/SSID4)**

The Service Set ID (SSID) that identifies the Wi-Fi network. The SSID is case sensitive and can consist of up to 32 alphanumeric characters.

Following characters is valid for Network Name (SSID).

'	()	*	-	.	/	0	1	2	3	4	5	6	7	8
9	:	<	=	>	@	A	B	C	D	E	F	G	H	I	J
K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
[]	^	_	`	a	b	c	d	e	f	g	h	i	j	k
l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	{
	}	~													

- **Hide SSID**

This function is to allow you to hide the SSID to prevent the unexpected connection request, please checked the checkbox to hide the SSID and unchecked it to broadcast the SSID.

- **Encryption**

Data passing between the unit and clients must be protected from interception and eavesdropping.

For a more secure network, the modem can implement one of several security mechanisms. The security mechanism employed depends on the level of security required, the network and management resources available, and the software support provided on wireless clients.

There are security options available. When you select the security type from the list, the required settings are displayed. The option "None" together with encryption disabled is equivalent to no security; all clients will be able to immediately connect to the Wi-Fi network.

The following security options are available for the Wi-Fi network.

- **WPA2 PSK + AES**
- **WPA-WPA2-Mixed PSK +TKIP/AES**

- **Password**

Wi-Fi password

5GHz Wi-Fi

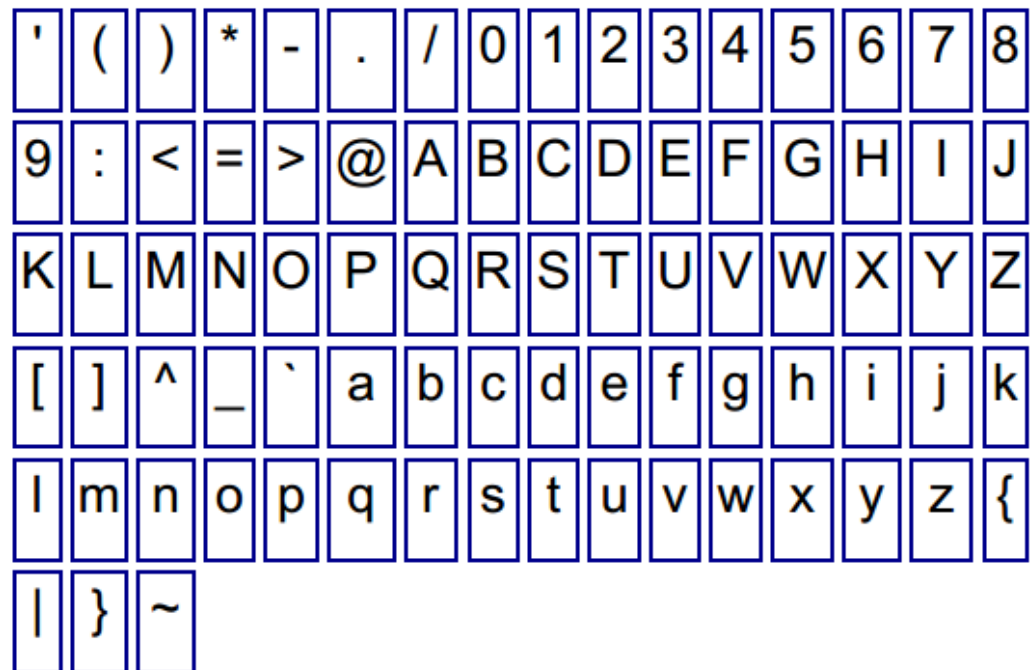
- **Enable 5GHz Wi-Fi**

Enables / disables the 5GHz Wi-Fi radio.

- **Network Name(SSID)**

The Service Set ID (SSID) that identifies the Wi-Fi network. The SSID is case sensitive and can consist of up to 32 alphanumeric characters.

Following characters is valid for Network Name (SSID).



- **Hide SSID**

This function is to allow you to hide the SSID to prevent the unexpected connection request, please checked the checkbox to hide the SSID and unchecked it to broadcast the SSID.

- **Encryption**

Data passing between the unit and clients must be protected from interception and eavesdropping.

For a more secure network, the modem can implement one of several security mechanisms. The security mechanism employed depends on the level of security required, the network and management resources available, and the software support provided on wireless clients.


There are security options available. When you select the security type from the list, the required settings are displayed. The option "None" together with encryption disabled is equivalent to no security; all clients will be able to immediately connect to the Wi-Fi network.

The following security options are available for the Wi-Fi network.

- **WPA2 PSK**
- **WPA-WPA2-Mixed PSK**

- **Password**

Wi-Fi password

	<p>Click the Undo to clear the changes that you have made to this window.</p> <p>Click the Apply to activate your changes.</p>
---	---

4.5.2 Wi-Fi > Advanced

Figure 4- 41 Wi-Fi - Advanced -1

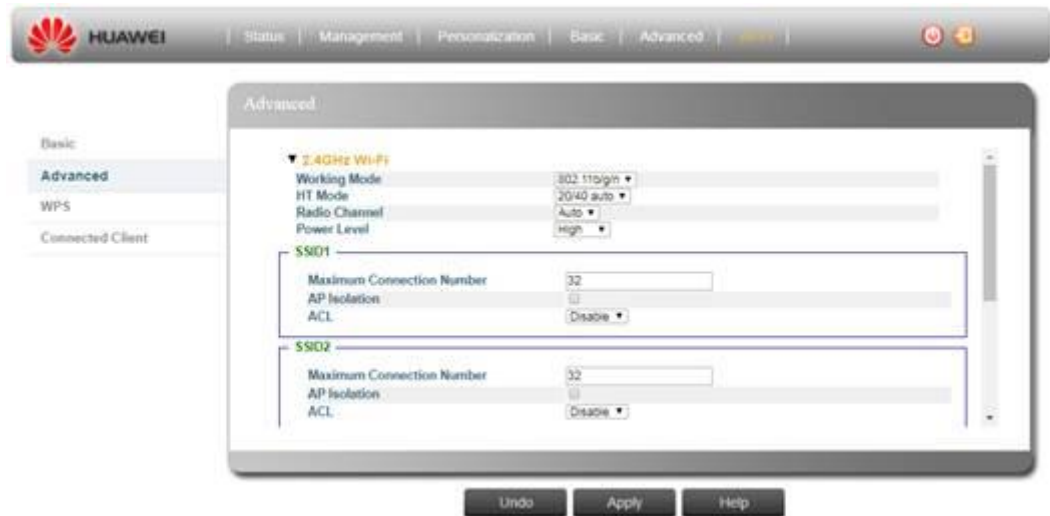
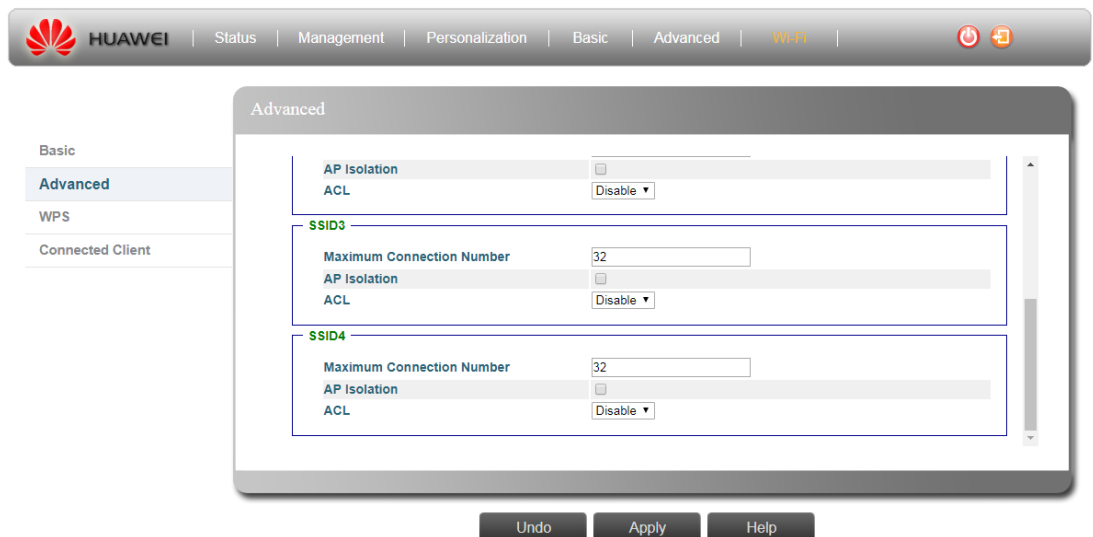


Figure 4- 42 Wi-Fi - Advanced -2



2.4GHz Wi-Fi

- **Working Mode**

It shows what Wi-Fi standard protocol is supported 802.11 b/g/n is supported.

- **HT Mode**

The HT mode is channel bandwidth. You can select 20MHz or 20/40MHz to affect the performance on your network.

- **Radio Channel**

The radio channel is used by the unit and its clients to communicate with each other. This channel must be the same on the unit and all of its wireless clients. The available channel settings are limited by local regulations.

- **Power Level**

The power level High/Middle/Low stands for Wi-Fi Tx power, you can adjust it base on

your environment condition.

- **Maximum connection number**

The maximum Wi-Fi clients can connect to device at the same time.

- **AP Isolation**

When the AP isolation is set to OFF: All the connected Wi-Fi clients can ping each other. When the AP isolation is set to ON: The Wi-Fi clients can't ping each other

- **ACL**

In this section you can add MAC addresses of clients which are allowed to access the system, or denied from accessing.

1. Select either of **Disable**, **Allow** or **Deny**.
2. For the Allow and Deny lists, click **Insert** to add a MAC address to the list, and specify the details.

5GHz Wi-Fi

- **Working Mode**

It shows what Wi-Fi standard protocol is supported 802.11 a/an/ac is supported.

- **HT Mode**

The HT mode is channel bandwidth. You can select 20MHz or 20/40MHz or 20/40/80MHz to affect the performance on your network.

- **Radio Channel**

The radio channel is used by the unit and its clients to communicate with each other. This channel must be the same on the unit and all of its wireless clients. The available channel settings are limited by local regulations.

- **Power Level**

The power level High/Middle/Low stands for Wi-Fi Tx power, you can adjust it base on your environment condition.

- **Maximum connection number**

The maximum Wi-Fi clients can connect to device at the same time.

- **AP Isolation**

When the AP isolation is set to OFF: All the connected Wi-Fi clients can ping each other. When the AP isolation is set to ON: The Wi-Fi clients can't ping each other

- **ACL**

In this section you can add MAC addresses of clients which are allowed to access the system, or denied from accessing.

Step 1: Select either of Disable, Allow or Deny.

Step 2: For the Allow and Deny lists, click Insert to add a MAC address to the list, and specify the details.

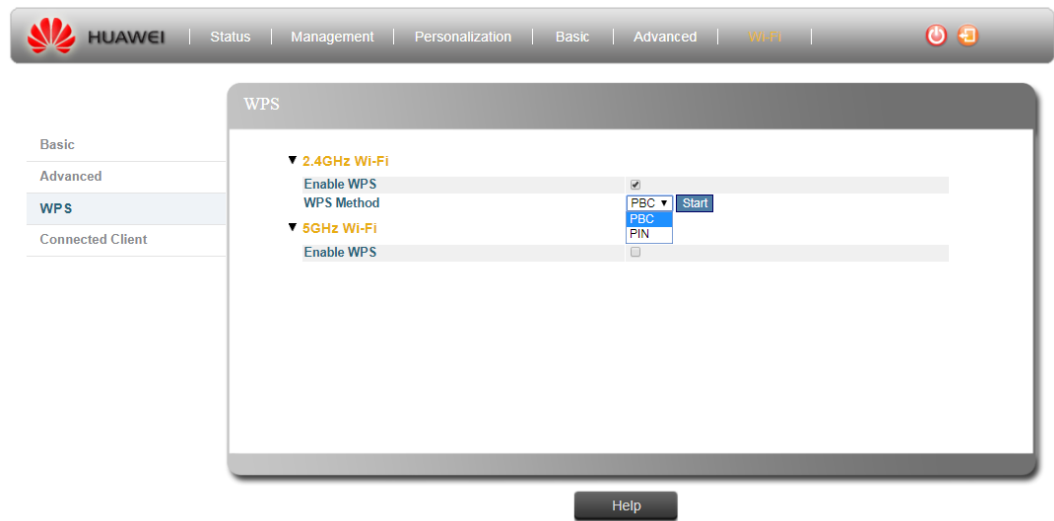


Click the **Undo** to clear the changes that you have made to this window.

Click the **Apply** to activate your changes.

4.5.3 Wi-Fi > WPS

Figure 4- 43 Wi-Fi - WPS



2.4GHz Wi-Fi

2.4G support NONE, WPA2 PSK + AES, WPA-WPA2-MIXED PSK + TKIP/AES.

- **PBC**

User may connect multiple devices to the network and enable data encryption by pushing a button. Users should be aware that during the two-minute setup period which follows the push of the button, unintended devices could join the network if they are in range.

- Start

Select PBC and press start button, the WPS will start and trying to connecting with the available clients.

- **PIN**

In Wi-Fi Protected Setup networks, a unique PIN (Personal Identification Number) will be required for each device to join the network.

- PIN code:

Another client would provide 4 or 8 PIN codes. Please insert the specific WPS client PIN code accordingly and the start icon would show up.

- Start

After input the PIN code then press the start, WPS will start and trying to connecting with the available clients.

5GHz Wi-Fi

5G support NONE, WPA2 PSK + AES, WPA-WPA2-MIXED PSK + TKIP/AES.

- **PBC**

User may connect multiple devices to the network and enable data encryption by pushing a button. Users should be aware that during the two-minute setup period which follows the push of the button, unintended devices could join the network if they are in range.

- Start

Select PBC and press start button, the WPS will start and trying to connecting with

the available clients.

- **PIN**

In Wi-Fi Protected Setup networks, a unique PIN (Personal Identification Number) will be required for each device to join the network.

- PIN code:

Another client would provide 4 or 8 PIN codes. Please insert the specific WPS client PIN code accordingly and the start icon would show up.

- Start

After input the PIN code then press the start, WPS will start and trying to connecting with the available clients.

4.5.4 Wi-Fi > Connected Client

Figure 4- 44 Connected Client



Device Name

Wi-Fi client's name.

IP Address

Wi-Fi client gotten IP address from device.

MAC Address

Wi-Fi client's MAC address.

Mode


Wi-Fi client's use working mode to connect to device.

RSSI(dBm)

Received Signal Strength Indication.

Speed(Mbps)

Support maximum speed.

	Click the " Refresh " button manual update the current status.
---	---

4.6 Engineering

4.6.1 How to Login Engineering page

Step 1 Open the Web browser and enter the default IP address of the device, which is: **192.168.1.1**

Figure 4- 45 Login page



Step 2 Enter the advanced user login credentials to access web management interface.

Default Log-in information:

Username: admin

Password: IDU@huawei

Step 3 Click the Engineering menu.

----End


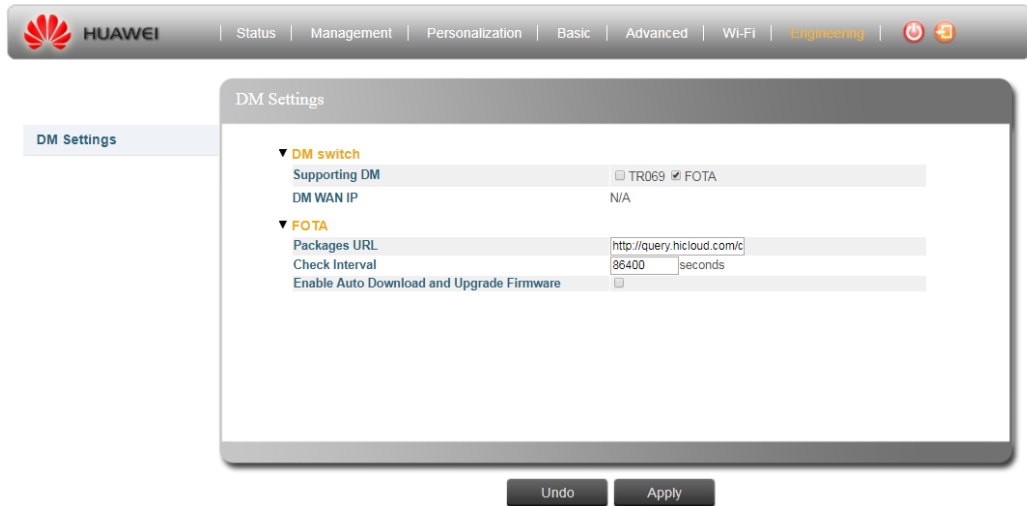
	You need to change the default Login password while the first time log-in. Please change the default password to protect your account.
---	--

Figure 4- 46 Engineering page



4.6.2 Engineering > DM Settings

Figure 4- 47 DM Settings - TR069

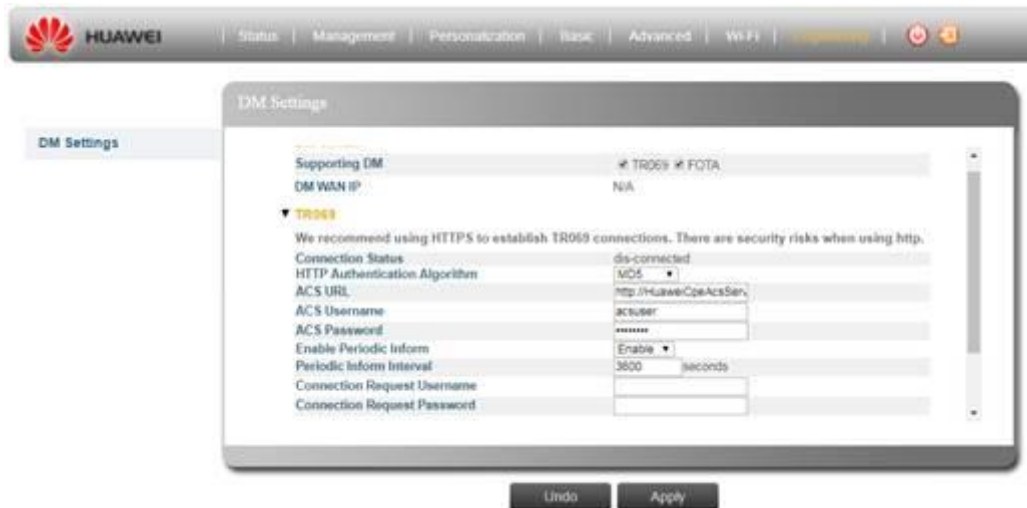
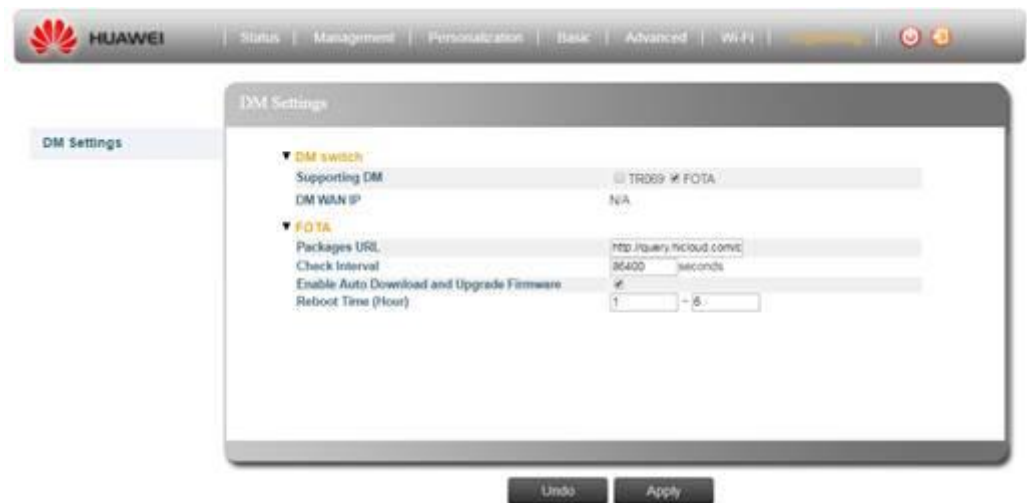


Figure 4- 48 DM Settings - FOTA



DM switch

- **Supporting DM**

You can multiple choose the DM for the device.

- **DM WAN IP**

Display the current WAN IP

TR069

- **Connection Status**

Display the current connection status: connected / dis-connected

- **HTTP Authentication Algorithm**

SHA256 or MD5

- **ACS URL**

Enter the URL of the TR-069 ACS to establish the TR-069 session with ACS.

- **ACS UserName**

Enter the user name for the authentication during connecting with ACS.

- **ACS UserPassword**

Enter the user password for the authentication during connecting with ACS.

- **Enable Periodic Inform**

Enable or Disable the device to connect to the ACS periodically

- **Periodic Inform Interval**

This field is enabled only when Periodic Inform Enabled is enabled. It defines the time in seconds between a successful connection with ACS and a new attempt to connect to ACS.

- **Connection Request User Name**

Enter the user name for authenticate incoming connection requests.

- **Connection Request Password**

Enter the password for authenticate incoming connection requests.

FOTA

- **Packages URL** Enter the FOTA server URL; device will connect this URL to access FW version check.

- **Check Interval** This Check Interval is to set the regular connecting cycle time to FOTA server. Default set as: 86400 seconds, 24hr it defines the time in seconds.

- **Enable Auto Download and Upgrade Firmware**

- Checked: Active Auto Download and Upgrade Firmware.
- Unchecked: Inactive Auto Download and Upgrade Firmware.

- **Reboot Time (Hour)**

Reboot device during a specific period time after upgrading FW from FOTA.

5 Federal Communication Commission

5.1 Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

IMPORTANT NOTE:

Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Country Code selection feature to be disabled for products marketed to the US/CANADA

Operation of this device is restricted to indoor use only.