WiFi Mobile Broadband Gateway

User Manual

無線路由器

CDM530AM

Copyright

Trademarks

FCC 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 radio interference in a commercial environment. This equipment can generate, use and radiate radio frequency energy and, if not installed and used in accordance with the instructions in this manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause interference, in which case the user, at his own expense, will be required to take whatever measures are necessary to correct the interference.

CE Declaration of Conformity

This equipment complies with the requirements relating to electromagnetic compatibility, EN 55022/A1 Class B.

The specification is subject to change without notice.

Table of Contents

1. Introduction

The WiFi Mobile Broadband Gateway is a high-performance tool that supports wireless networking at home, work, or in a public place. The WiFi Mobile Broadband Gateway supports uses a USB 3G modem card, either WCDMA or EVDO and even HSDPA as well, and supports wireless data transfers up to 80M bps, and wired data transfers up to 100 Mbps.
The WiFi Mobile Broadband Gateway is compatible with industry security features.

1.1. Package Contents

Importance: Check your product package contents FIRST.

The WiFi Mobile Broadband Gateway package should contain the items listed below. If any of the items are missing, please contact your reseller.

items	Description	Quantity
1	**WiFi Mobile Broadband Gateway**	**1**
2	**RJ-45 Cable**	**1**
3	**Power adapter 5V 2.5A**	**1**
4	**CD**	**1**
5	**Leather case**	**1**
6	**QIG**	**1**
7	**Li-ion Battery**	**1**

Caution: Using a power supply with a different voltage rating than the one included with the WiFi Mobile Broadband Gateway will cause damage and void the warranty for this product.

1.2. System Requirements for Configuration

• A compatible USB 3G modem card *with service*

Note: Subject to services and service terms available from your carrier.

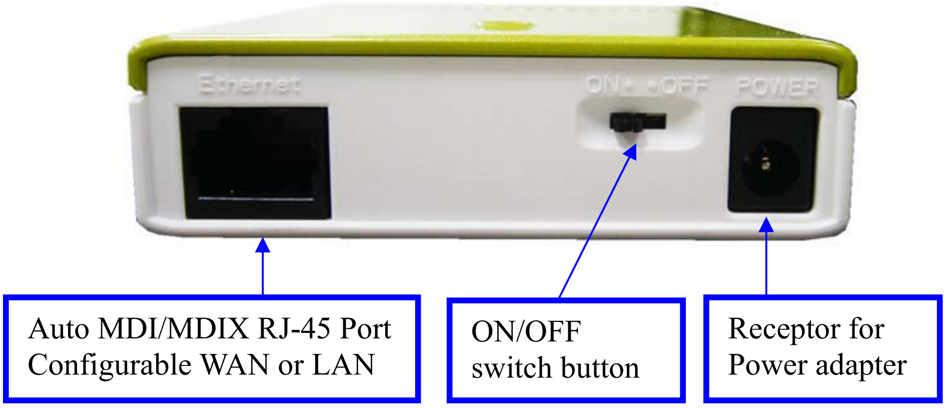
• Computers with Windows, Macintosh, or Linux-based operating systems with an installed Ethernet adapter.

• Internet Explorer version 6.0 or Netscape Navigator version 7.0 and above.

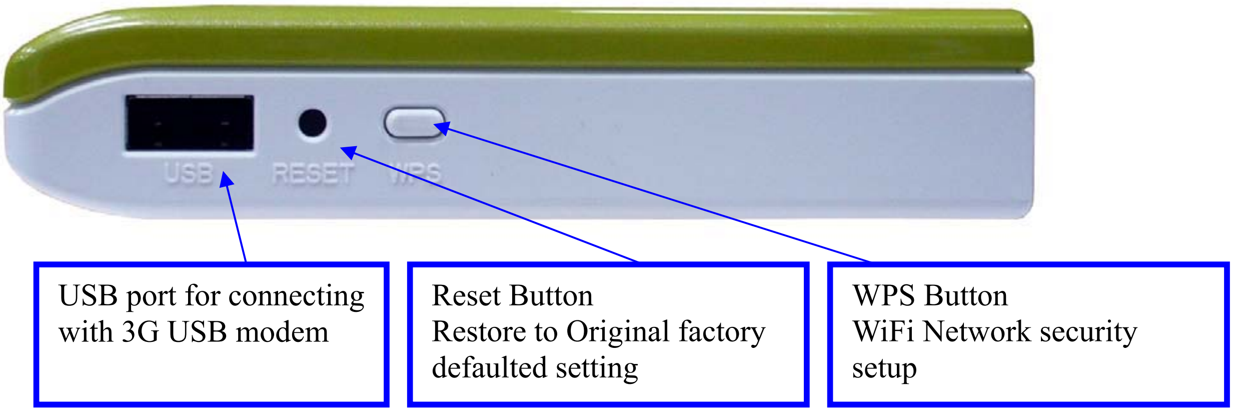
• Wi-Fi System Requirements: An 802.11b, 802.11g, or 802.11n Adapter.

1.3. Interfaces

The Rear View



The Side View



USB port for connecting with 3G USB modem

Reset Button
Restore to Original factory defaulted setting

WPS Button
WiFi Network security setup

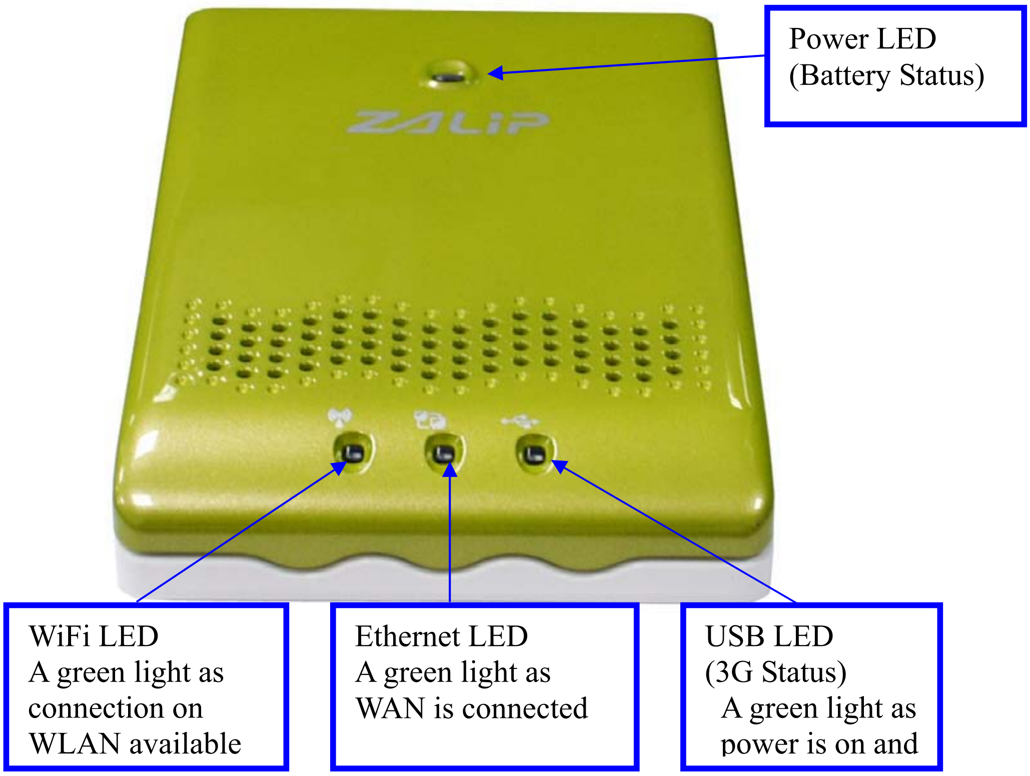
NOTE:

Press the reset button 3 seconds: the LEDs (WiFi and USB) will flash 2 times, and Ethernet port be resented to LAN.

Press the reset button 8 seconds: the LEDs (WiFi and USB) will flash 3 times, and restore the setting back to original factory defaulted setting as if your convenience of forgetting your applicable setting

Press the WPS button enables user to establish a wireless home network easily under secure environment between router and clients in air connection.

1.4. LEDs– The Top View



Power LED: (and Battery Status)

- **when device is on and with battery inside**
  - Green: power adapter is plugged, and battery is fully charged
  - Green in flash: power is provided by battery
  - Amber: power adapter is plugged, and charging the battery
  - Red: battery low
- **when device is on and without battery inside**
  - Amber: power adapter or CLA is plugged
- **when device is off and with battery inside**
  - Amber: power adapter is plugged, and charging the battery
  - NA: power adapter is plugged, and battery charging finished
  - NA: no power adapter is plugged
- **when device is off and without battery inside**
  - NA: no matter power adapter or CLA is plugged or not.

Ethernet LED:

- Green: Ethernet connection is established

- Green in flash: data packet transferred via Ethernet

USB LED: (WAN)

- Green: 3G/3.5G connection is established
- Green in flash: data packet transferred via 3G/3.5G connection

WiFi LED:

- Green: WLAN is active and available
- Green in flash: data packet transferred via WLAN

1.5. Features

- IEEE 802.11b/g/n compliant
  - Backward compatible to IEEE 802.11b standards
  - Max physical rate up to 54Mbps in 802.11g mode
  - Security Supports: WEP (64/128 bits), WPA, WPA2, WPA-PSK, WPA2-PSK, and 802.1x
- Provide 1 * 10/100 RJ-45 port
  - LAN or WAN (Configurable)
- WAN connection through external USB 3G/3.5G modem card
- WAN connection through 3G tethered-data-enabled cell phone
- WAN connection through Ethernet
  - Dynamic IP (DHCP Client)
  - Static IP
  - PPPoE
  - PPTP
  - L2TP
- PPTP over 3G WAN connection
- Built-in NAT function: one IP sharing with PCs
- Built-in firewall to protect your Intranet
- VPN pass through supported
  - PPTP
  - L2TP
  - IPSec
- Easy to upgrade firmware
  - Web UI
  - Windows utility
- Easy to manage:
  - Web UI
  - SNMP
  - UPnP
- L3/L4 QoS
- Network Protocols
  - UDP/TCP/IP/ARP/RARP/ICMP
  - DHCP/PPPoE
  - DNS/TFTP/HTTP
- Antenna
  - 1 x Internal Wi-Fi antenna
- Continue working 100 minutes with built-in Li-Ion battery (1700mAh)

Note: The WiFi Mobile Broadband Gateway is designed to work with either EVDO or WCDMA (UMTS) even up to 3.5G HSPA PC interface.
Please refer to your service provider for detailed feature information.

2. Configuring Wireless WAN Mobile broadband Router

2.1. Installation Considerations

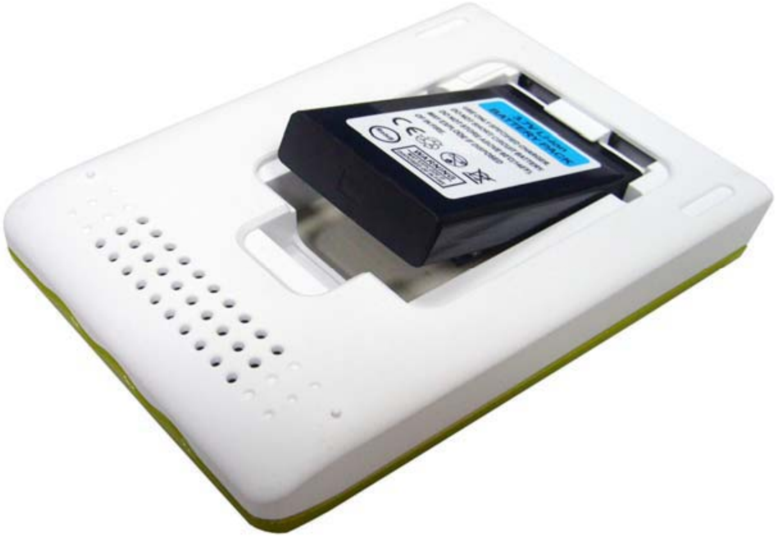
The WiFi Mobile Broadband Gateway allows you access your network using a wireless connection, from virtually anywhere within its operating range. Keep in mind however, that the number, thickness, and location of walls, ceilings, or other objects that the wireless signals must pass through, may limit this range.
Typical ranges vary depending on the types of materials used, and background RF (radio frequency) noise in your home or business.

To maximize your wireless range, please follow these guidelines:

1. Keep the number of walls and ceilings between the WiFi Mobile Broadband Gateway and other network devices to a minimum. Each wall or ceiling can reduce the Wireless WAN Mobile Broadband Router's range from 3-90 feet (1-30 meters).
   Note: The same considerations apply to your broadband EVDO connection.
2. Keep your product aware from electrical devices (such as microwaves, air conditioners, and televisions) that emit large quantities of RFI (Radio Frequency Interference).

2.1.1. Installation Instructions- Get Start Networking

Connect the WiFi Mobile Broadband Gateway to Your Network
Note: DO NOT switch on WiFi Mobile Broadband Gateway before performing the installation steps below.
1. Turn off the power switch.
2. Attach the Li-ion battery. ---picture 2.1



Picture 2.1

a. Insert the battery into battery holder

3. Connect a USB modem *with service* to the WiFi Mobile Broadband Gateway in one of the following ways:
→ You can plug your USB modem into the USB interface. **---see Picture 2.2**

Picture 2.2

Note: The WiFi Mobile Broadband Gateway is designed to work with either UMTS or EV-DO and even HSDPA 3G card that can be used as a modem (support tethered data). Please refer to your service provider for detailed feature information.

3. Insert the Ethernet patch cable into Ethernet Port on the back panel of the WiFi Mobile Broadband Gateway, and an available Ethernet port on the network adapter in the computer you will use to configure the unit.-**see Picture 2.3**

Picture 2.3

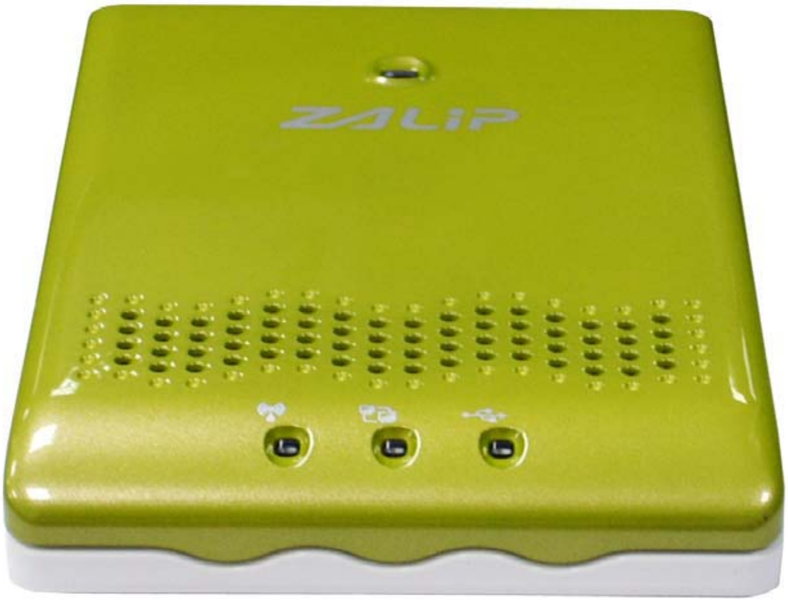
Note: The WiFi Mobile Broadband Gateway Ethernet Port is "Auto-MDI/MDIX." This provides patch Ethernet cable Ethernet Port access.

4. Connect the power adapter to the receptor on the back panel of your WiFi Mobile Broadband Gateway. Then plug the other end of the power adapter into a wall outlet or power strip. ---Picture 2.4

Picture 2.4

5. Turn on the power switch.

6. The LEDs (See Picture 2.5)
   a. The Power LED will turn ON to indicate power has been applied.
   b. Reference the Section 1.4, LEDs– the Top View.



Picture 2.5

2.1.2. Establish WiFi Connection

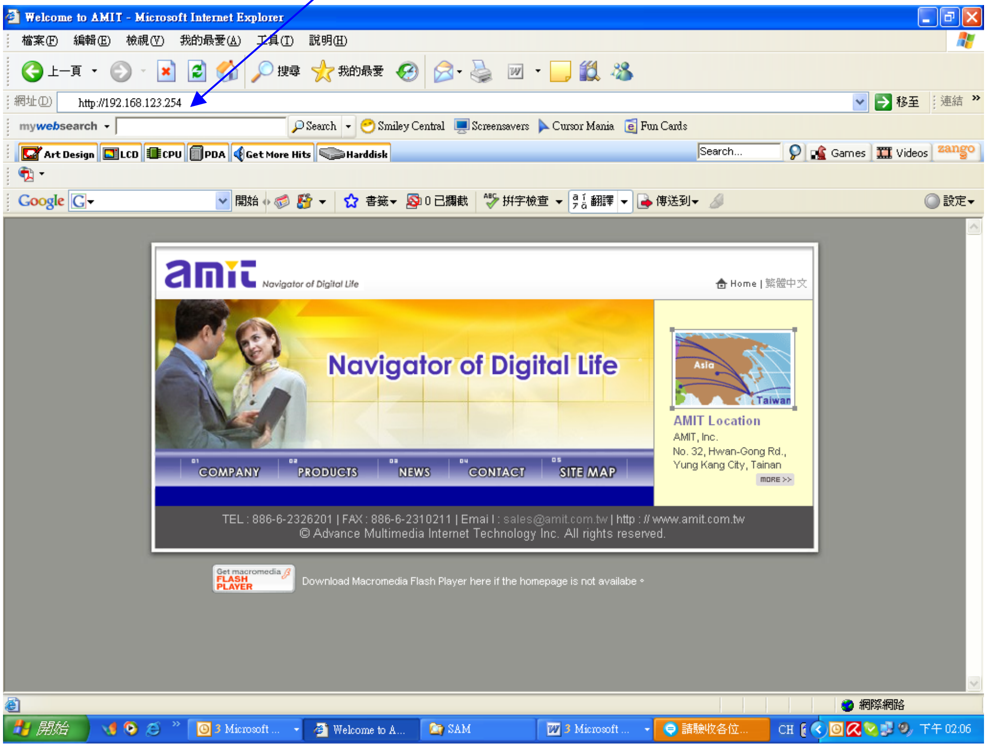
If you selected either **WEP** or **WPA-PSK** encryption, ensure these settings match your WiFi adapter settings.

WiFi and encryption settings must match for access to the HSPA Wireless WAN Mobile Broadband Router Configuration Menu, and the Internet. Please refer to your WiFi adapter documentation for additional information.

3. Using the Configuration Menu

Once properly configured, the WiFi Mobile Broadband Gateway will obtain and assign IP address information automatically. Configuration settings can be established through the WiFi Mobile Broadband Gateway Configuration Menu. You can access this interface by performing the steps listed below:

1. Open a web-browser.
2. Type in the **IP Address** (http://192.168.123.254) of the WiFi Mobile Broadband Gateway.



Welcome to AMIT - Microsoft Internet Explorer
檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)
上一頁 搜尋 我的最愛
網址(D)
移至 連結
mywebsearch Search Smiley Central Screensavers Cursor Mania Fun Cards
Art Design LCD CPU PDA Get More Hits Harddisk
Games Videos zango
Google 開始 書籤 0 已攔截 拼字檢查 翻譯 傳送到 設定
amit Navigator of Digital Life
Home | 繁體中文
Navigator of Digital Life
Asia Taiwan
01 COMPANY 02 PRODUCTS 03 NEWS 04 CONTACT 05 SITE MAP
MORE >>
Get macromedia FLASH PLAYER
網際網路
開始 3 Microsoft ... Welcome to A... SAM 3 Microsoft ... 請點收各位... CH 下午 02:06

http://192.168.123.254

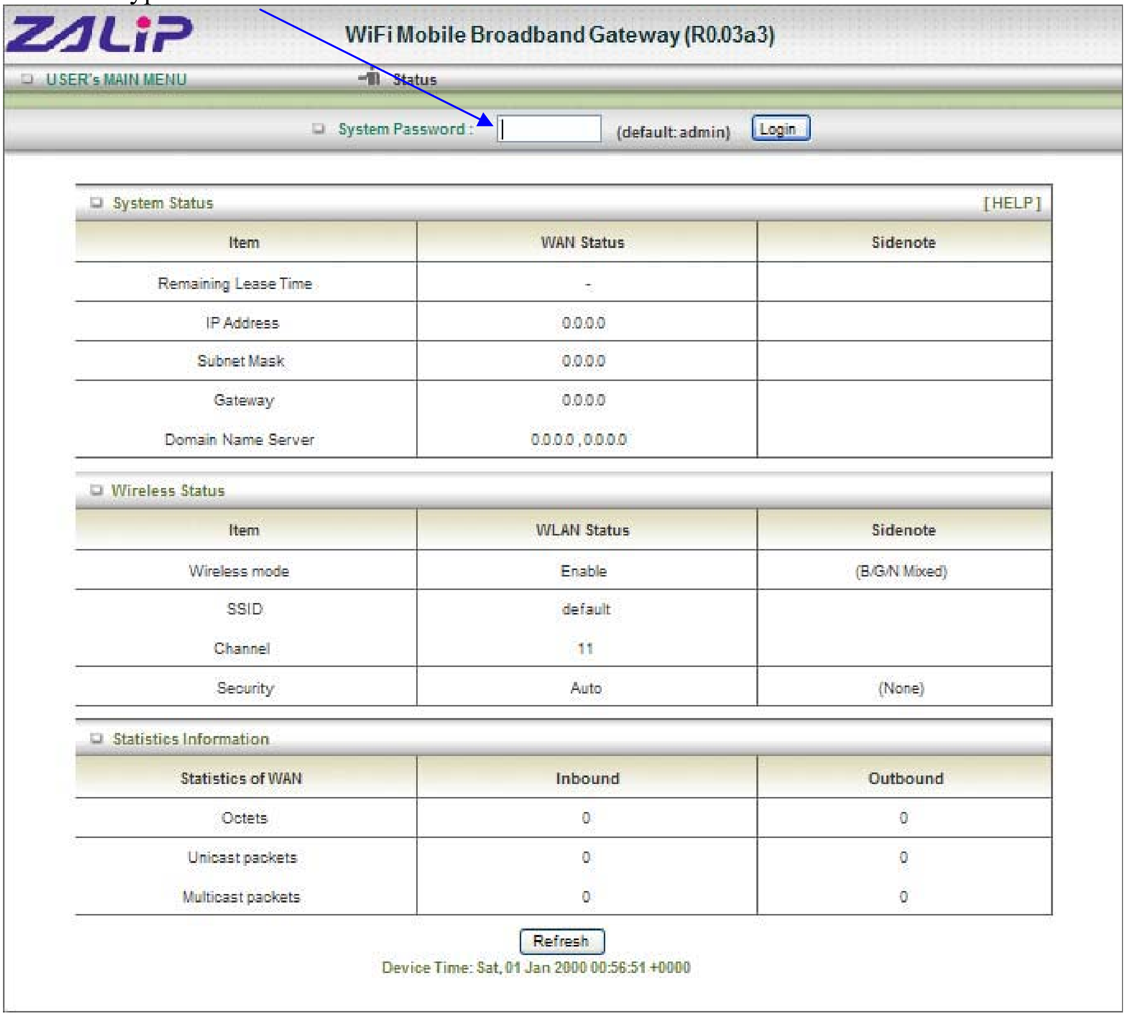
AMIT Location
AMIT, Inc.
No. 32, Hwan-Gong Rd.,
Yung Kang City, Tainan

TEL : 886-6-2326201 | FAX : 886-6-2310211 | Email : sales@amit.com.tw | http : // www.amit.com.tw
© Advance Multimedia Internet Technology Inc. All rights reserved.

Download Macromedia Flash Player here if the homepage is not availabe

Note: If you have changed the **default** IP Address assigned to the WiFi Mobile Broadband Gateway, ensure you enter the correct IP Address now.

3. Type “**admin”** in the **Password** field.



WiFi Mobile Broadband Gateway (R0.03a3)

System Password : (default: admin)

System Status [HELP]

Item	WAN Status	Sidenote
Remaining Lease Time	-	
IP Address	0.0.0.0	
Subnet Mask	0.0.0.0	
Gateway	0.0.0.0	
Domain Name Server	0.0.0.0 , 0.0.0.0	

Wireless Status

Item	WLAN Status	Sidenote
Wireless mode	Enable	(B/G/N Mixed)
SSID	default	
Channel	11	
Security	Auto	(None)

Statistics Information

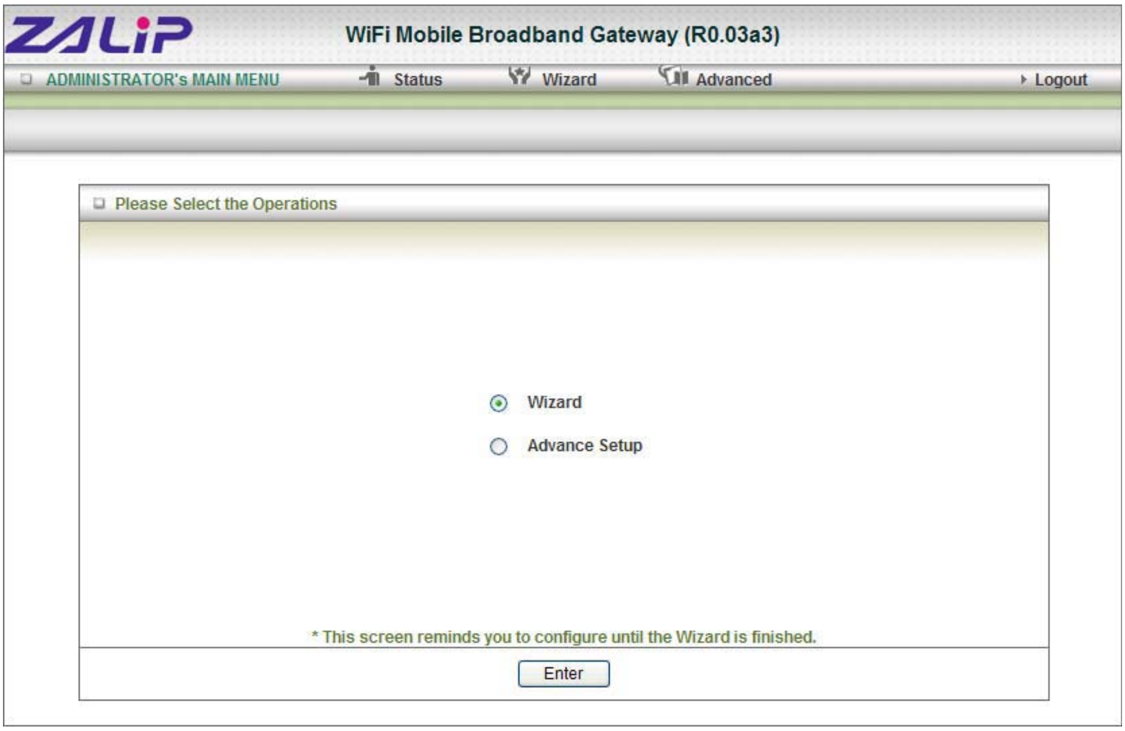
Statistics of WAN	Inbound	Outbound
Octets	0	0
Unicast packets	0	0
Multicast packets	0	0

Device Time: Sat, 01 Jan 2000 00:56:51 +0000

4. Click “login” button.

3.1. Wizard setting

- Press “**Wizard**” button → for basic settings with simpler way. (Please check section 3.1)
- Or you may click on “**Advanced Setup**” → for advanced settings. (Please check the section Administrator’s Main Menu. Each item from section 3.2)


ZALiP
WiFi Mobile Broadband Gateway (R0.03a3)
ADMINISTRATOR's MAIN MENU
Status
Wizard
Advanced
Logout
Please Select the Operations

● Wizard

○ Advance Setup

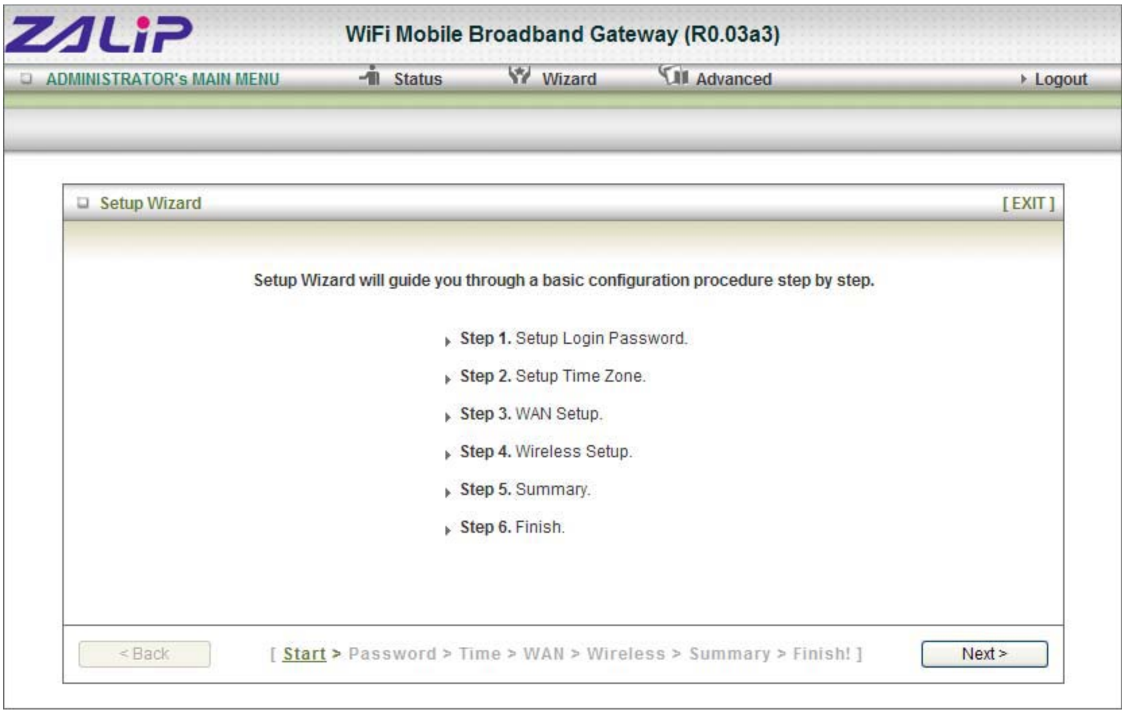
* This screen reminds you to configure until the Wizard is finished.

- **Click on “Enter” button to get start.**

With wizard setting steps, you could configure the router in a very simple way. This configuration wizard includes settings of

a. **Login Password**,
b. **Time Zone,**
c. **WAN Setup**
d. **Wireless Setup**,

Press **“Next”** button to start configuration.



ZALiP WiFi Mobile Broadband Gateway (R0.03a3)

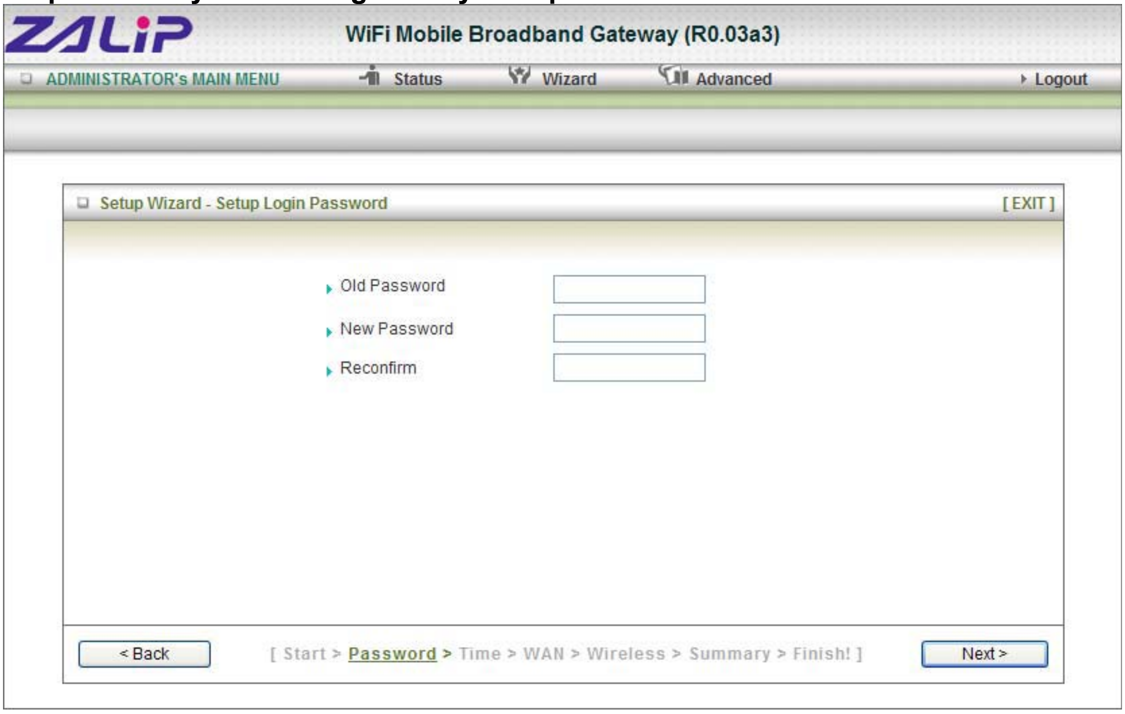
ADMINISTRATOR's MAIN MENU
Status
Wizard
Advanced
Logout
Setup Wizard
[EXIT]

Setup Wizard will guide you through a basic configuration procedure step by step.

- **Step 1.** Setup Login Password.
- **Step 2.** Setup Time Zone.
- **Step 3.** WAN Setup.
- **Step 4.** Wireless Setup.
- **Step 5.** Summary.
- **Step 6.** Finish.

< Back
[Start > Password > Time > WAN > Wireless > Summary > Finish!]
Next >

Step 1: Allow you to change the system password.



ZALiP WiFi Mobile Broadband Gateway (R0.03a3)

ADMINISTRATOR's MAIN MENU
Status
Wizard
Advanced
Logout
Setup Wizard - Setup Login Password
[EXIT]

- Old Password
- New Password
- Reconfirm

< Back
[Start > Password > Time > WAN > Wireless > Summary > Finish!]
Next >

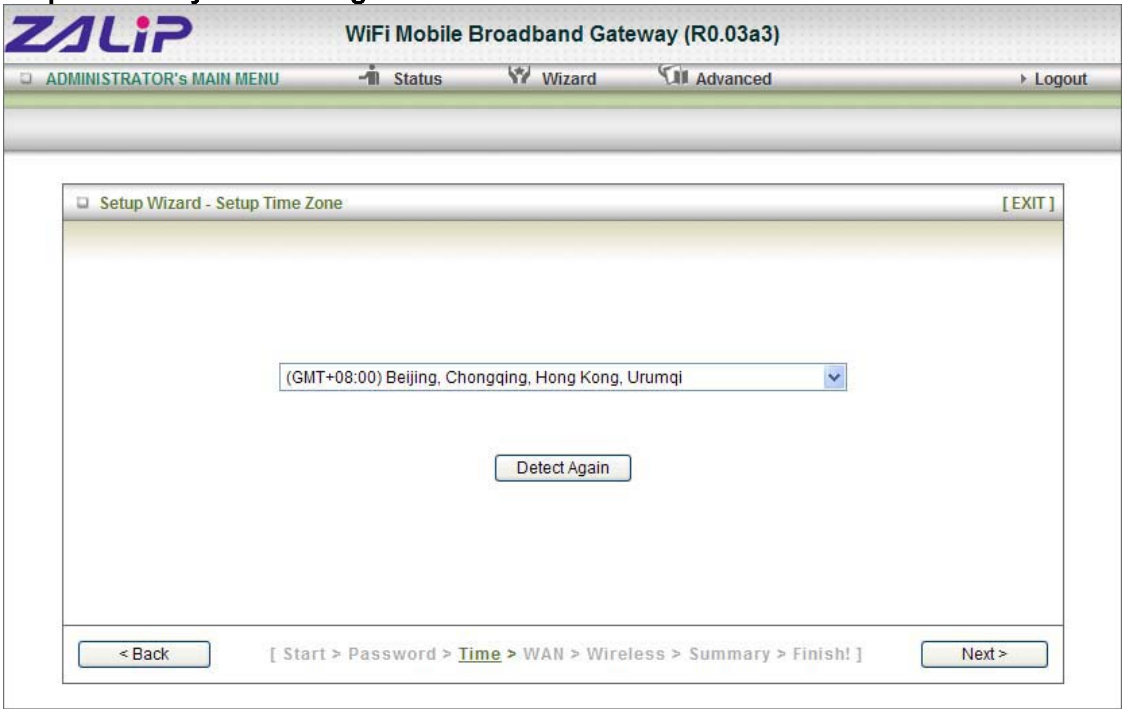
You can change Password here.
It is recommended that you change the system password into the one you prefer to on the basis of security.

1. Key in your Old Password (if it is the first initiation, the “admin” will be the defaulted one.
2: Enter your New Password

3: Enter your Password again for confirmation; it must be the same as the New Password.

4. Then click on “Next” to get into next installation.

Step 2: Allow you to change the Time Zone.

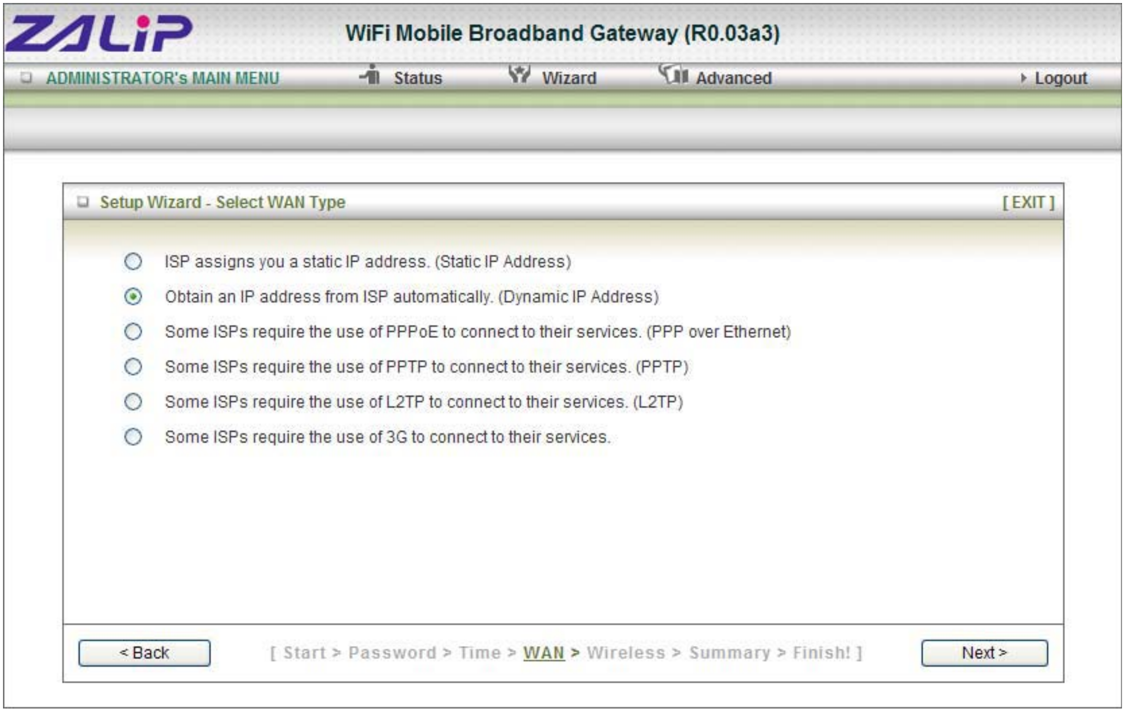


ZALiP
WiFi Mobile Broadband Gateway (R0.03a3)
ADMINISTRATOR's MAIN MENU
Status
Wizard
Advanced
Logout
Setup Wizard - Setup Time Zone
[EXIT]
Detect Again
< Back
[Start > Password > Time > WAN > Wireless > Summary > Finish!]
Next >

(GMT+08:00) Beijing, Chongqing, Hong Kong, Urumqi

You can change Time Zone here.
Or you can click the button “Detect Again”, the Time Zone will be changed to same with your PC.

Step 3: Select WAN Types will be used for Internet connection


ZALiP
WiFi Mobile Broadband Gateway (R0.03a3)
ADMINISTRATOR's MAIN MENU
Status
Wizard
Advanced
Logout

Setup Wizard - Select WAN Type [EXIT]

○ ISP assigns you a static IP address. (Static IP Address)

● Obtain an IP address from ISP automatically. (Dynamic IP Address)

○ Some ISPs require the use of PPPoE to connect to their services. (PPP over Ethernet)

○ Some ISPs require the use of PPTP to connect to their services. (PPTP)

○ Some ISPs require the use of L2TP to connect to their services. (L2TP)

○ Some ISPs require the use of 3G to connect to their services.

< Back
[Start > Password > Time > WAN > Wireless > Summary > Finish!]
Next >

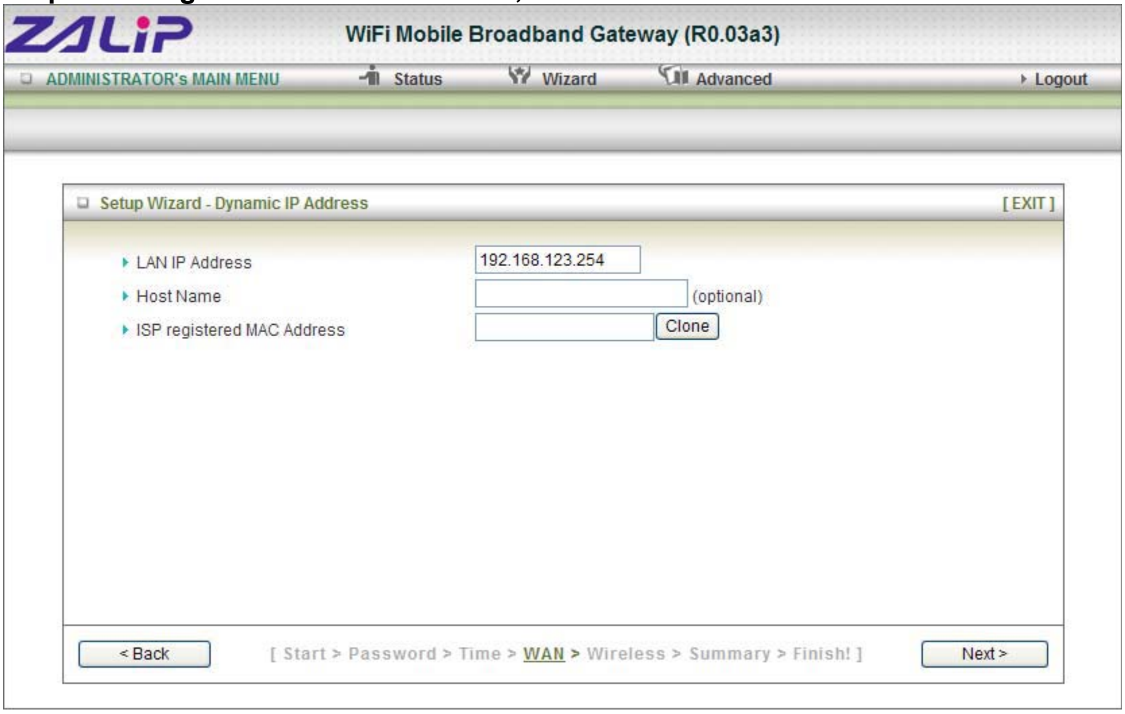
The Ethernet Port will be set as *WAN* port, if you select the Dynamic, Static, PPPOE, PPTP or L2TP WAN Types.

The Ethernet Port will be set as *LAN* port, if you select the 3G WAN Type.

Pick up one of types you preferred to.

Click on “**Next”** button

Step 4: Configure the LAN IP Address, Host Name and WAN MAC Address.


ZALiP
WiFi Mobile Broadband Gateway (R0.03a3)
ADMINISTRATOR's MAIN MENU
Status
Wizard
Advanced
Logout
Setup Wizard - Dynamic IP Address
[EXIT]

- LAN IP Address: 192.168.123.254
- Host Name: (optional)
- ISP registered MAC Address: Clone

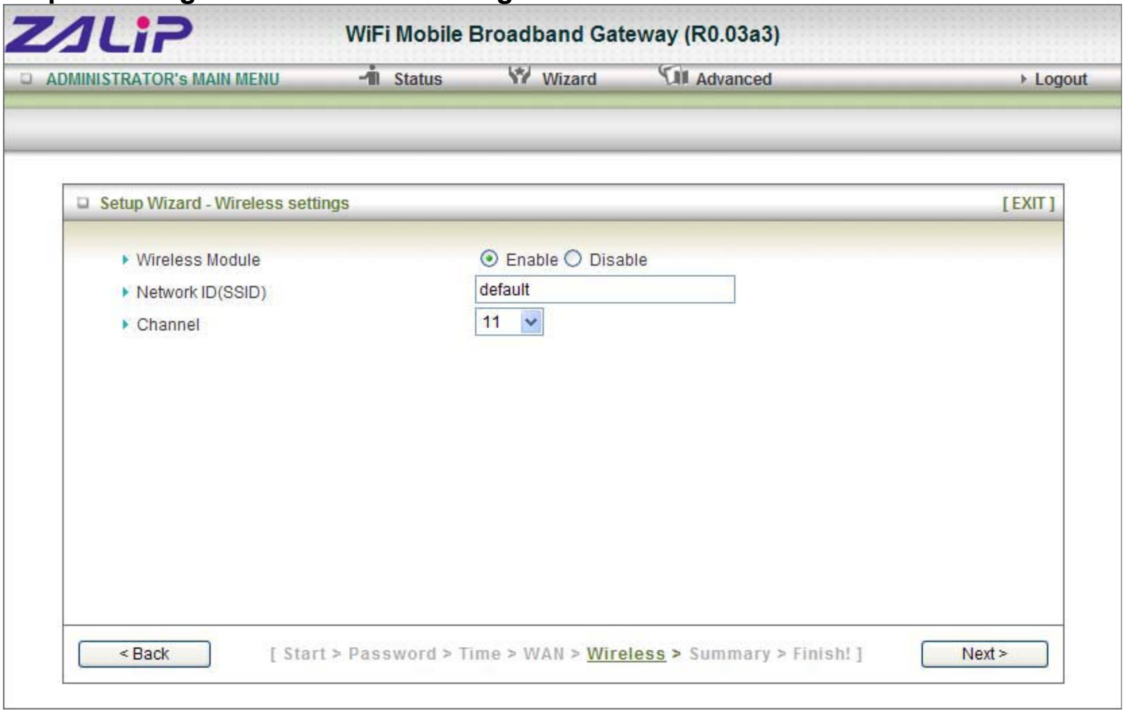
< Back
[Start > Password > Time > WAN > Wireless > Summary > Finish!]
Next >

LAN is short for Local Area Network, and is considered your internal network. These are the IP settings of the LAN interface for the WiFi Mobile Broadband Gateway, and they may be referred to as Private settings. You may change the LAN IP address if needed. The LAN IP address is private to your internal network and cannot be seen on the Internet.

Note: There are 254 addresses available on the WiFi Mobile Broadband Gateway when using a 255.255.255.0 (Class C) subnet. Example: The router's IP address is 192.168.123.1. The available client IP range is 192.168.123.2 through 192.168.123.254.

1. **LAN IP Address-** The IP address of the LAN interface. The **default** IP address is: **192.168.123.254**
2. Host Name is optional
3. WAN's MAC Address
   If you click the Clone MAC button, you will find the MAC address of your NIC shown in WAN's MAC Address
4. Click on "**Next**" to continue.

Step 5: Configure the wireless settings.



ZALiP
WiFi Mobile Broadband Gateway (R0.03a3)
ADMINISTRATOR's MAIN MENU
Status
Wizard
Advanced
Logout
Setup Wizard - Wireless settings
[EXIT]
< Back
[Start > Password > Time > WAN > Wireless > Summary > Finish!]
Next >

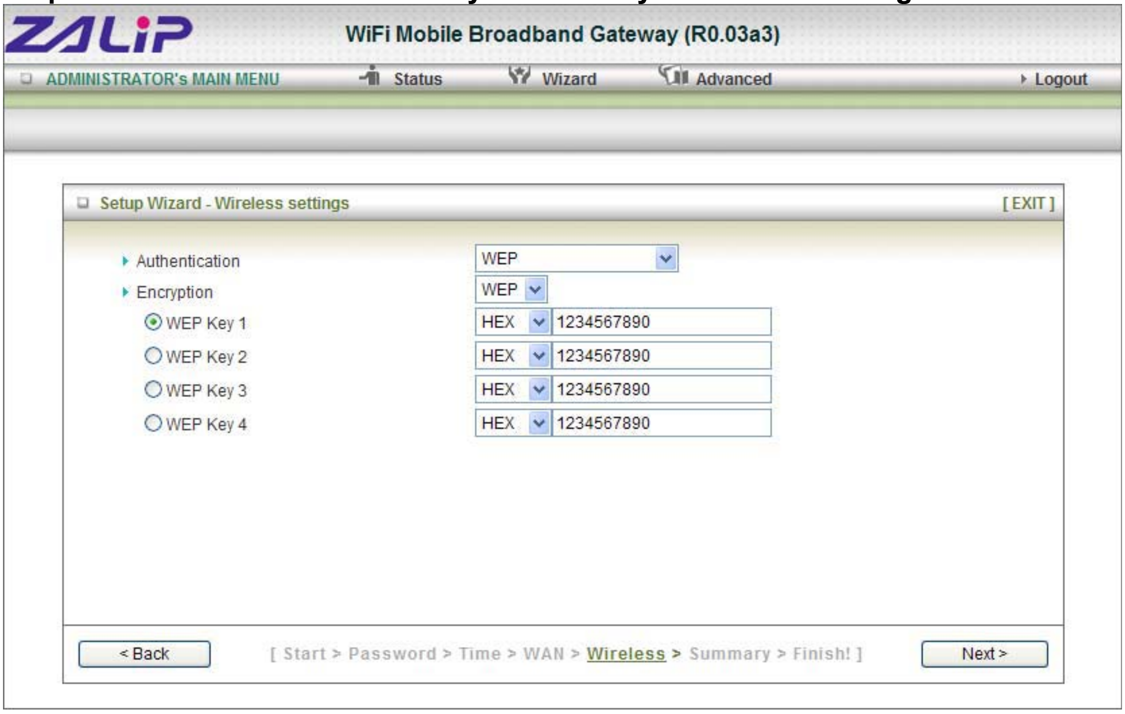
Wireless Module ● Enable ○ Disable

Network ID(SSID) default

Channel 11

1. Select “**Enable**” or “**Disable**”. The default setting is “**Enable**”.
2. Network ID(SSID) will be defaulted.
3. **Channel→** Select Wireless Channel matching to your local area for Wireless connection.
4. Click on “**Next**” to continue.

Step 6: Select the Wireless security method of your wireless configuration.



ZALiP
WiFi Mobile Broadband Gateway (R0.03a3)
ADMINISTRATOR's MAIN MENU
Status
Wizard
Advanced
Logout
Setup Wizard - Wireless settings
[EXIT]
< Back
[Start > Password > Time > WAN > Wireless > Summary > Finish!]
Next >

Authentication: WEP

Encryption: WEP

● WEP Key 1: HEX 1234567890

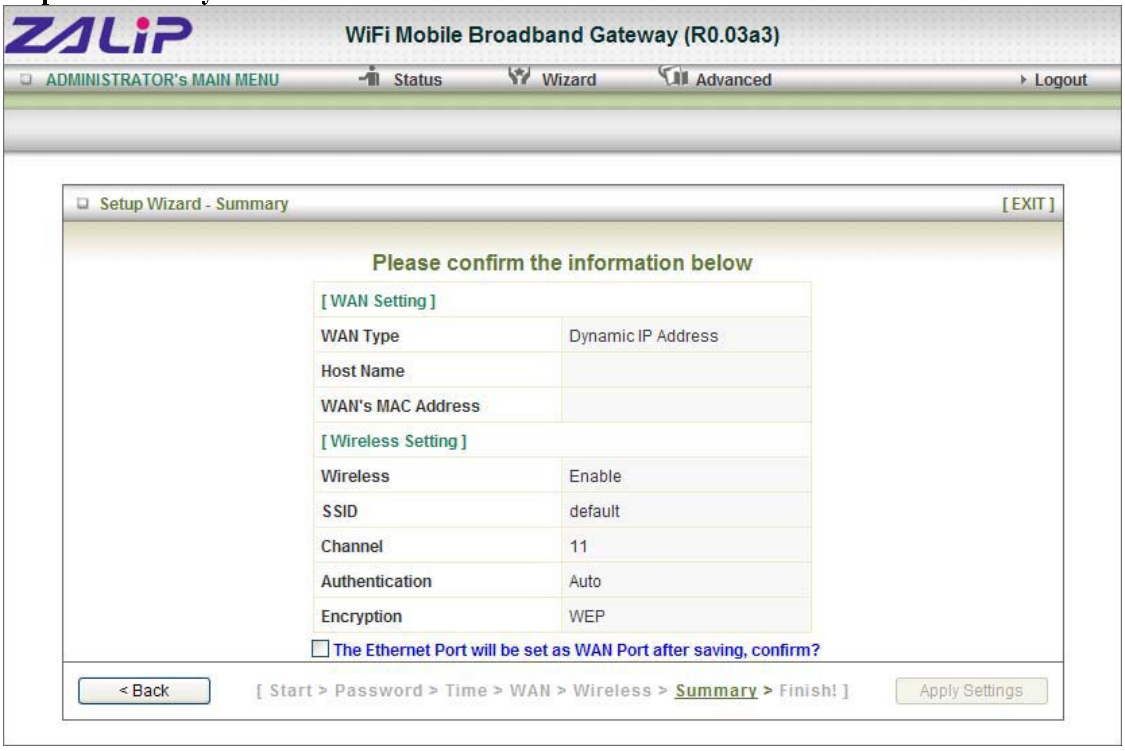
○ WEP Key 2: HEX 1234567890

○ WEP Key 3: HEX 1234567890

○ WEP Key 4: HEX 1234567890

Click on “**Next**” to continue.

Step 7: Summary



ZALiP
WiFi Mobile Broadband Gateway (R0.03a3)
ADMINISTRATOR's MAIN MENU
Status
Wizard
Advanced
Logout
Setup Wizard - Summary
[EXIT]

Please confirm the information below

[WAN Setting]	
WAN Type	Dynamic IP Address
Host Name	
WAN's MAC Address	
[Wireless Setting]	
Wireless	Enable
SSID	default
Channel	11
Authentication	Auto
Encryption	WEP

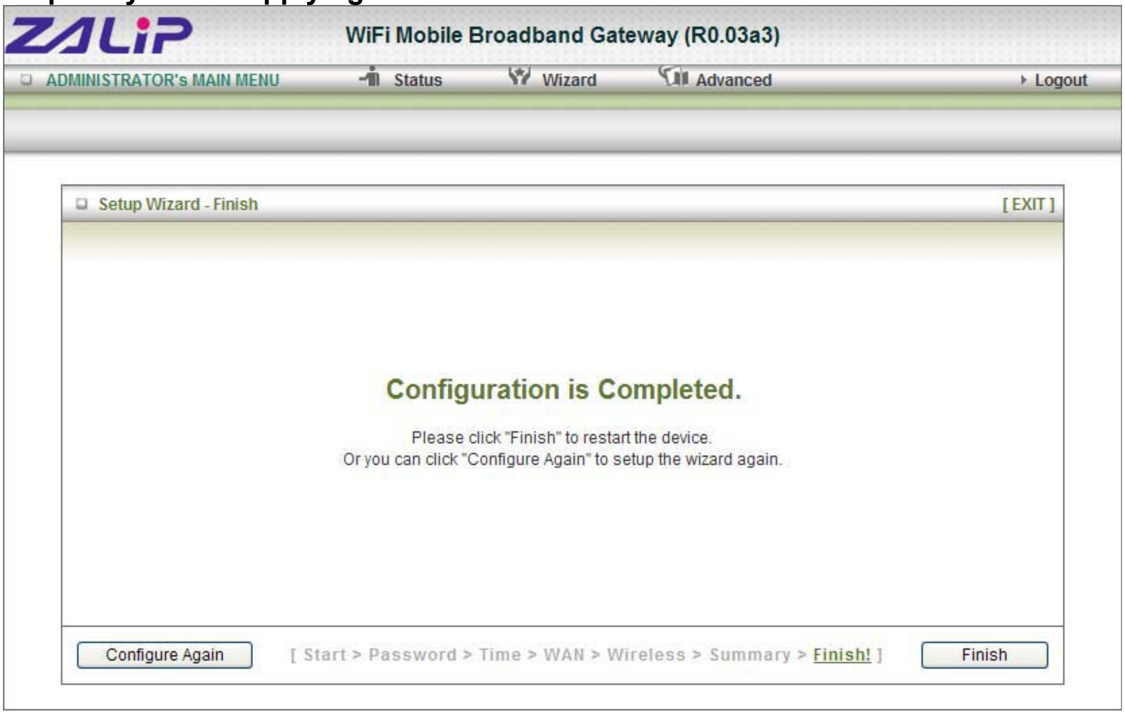
□ The Ethernet Port will be set as WAN Port after saving, confirm?

< Back
[Start > Password > Time > WAN > Wireless > Summary > Finish!]
Apply Settings

1. Select the option box **"The Ethernet Port will be set as WAN Port after saving, confirm?" or "The Ethernet Port will be set as LAN Port after saving, confirm?"** for continues.

2. Click on the "**Apply Settings**" button.

Step 8: System is applying.



ZALiP
WiFi Mobile Broadband Gateway (R0.03a3)
ADMINISTRATOR's MAIN MENU
Status
Wizard
Advanced
Logout
Setup Wizard - Finish
[EXIT]

Configuration is Completed.

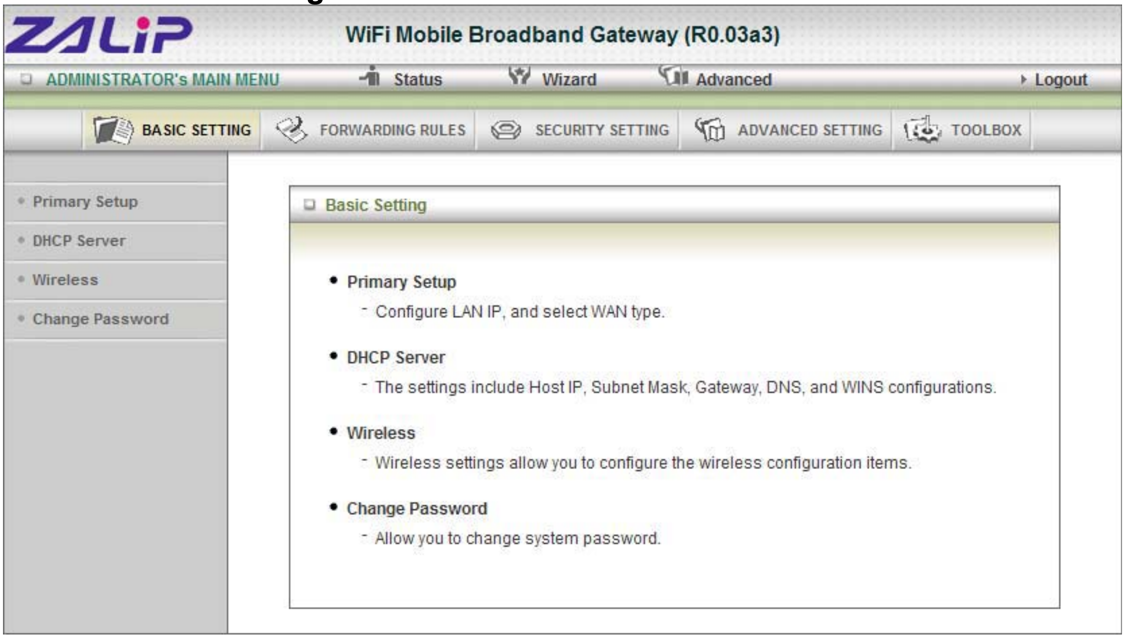
Please click "Finish" to restart the device.
Or you can click "Configure Again" to setup the wizard again.

Configure Again
[Start > Password > Time > WAN > Wireless > Summary > Finish!]
Finish

Click "**Finish**" button to back the Status Page.

3.2. Administrator's Main Menu

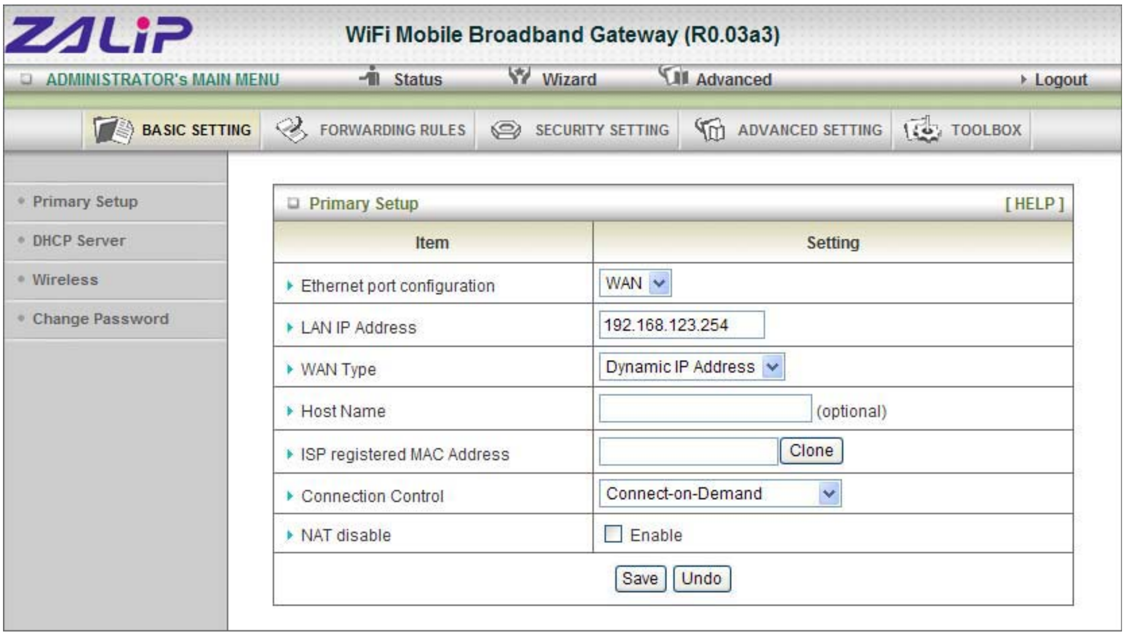
3.2.1 Basic Setting



Basic Setting

- Primary Setup
  - Configure LAN IP, and select WAN type.
- DHCP Server
  - The settings include Host IP, Subnet Mask, Gateway, DNS, and WINS configurations.
- Wireless
  - Wireless settings allow you to configure the wireless configuration items.
- Change Password
  - Allow you to change system password.

3.2.1.1 Primary Setup

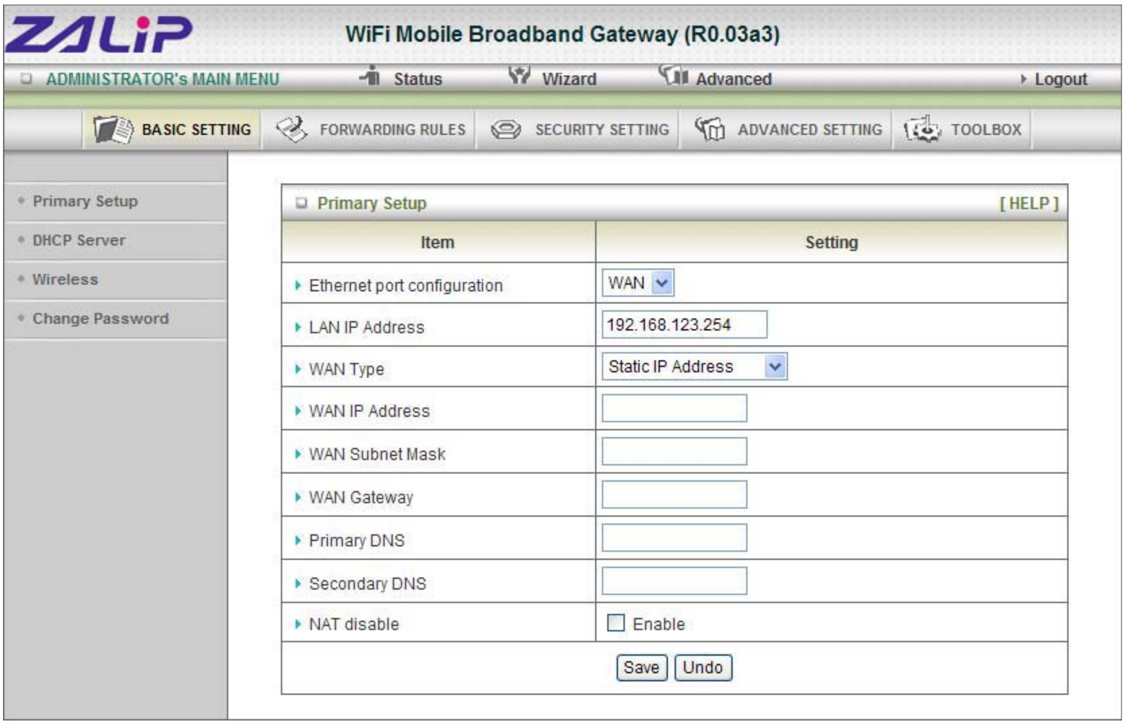


Primary Setup

Item	Setting
Ethernet port configuration	WAN
LAN IP Address	192.168.123.254
WAN Type	Dynamic IP Address
Host Name	(optional)
ISP registered MAC Address	Clone
Connection Control	Connect-on-Demand
NAT disable	□ Enable

1. **Ethernet port Configuration:**
   Off: Disable the Ethernet port.
   LAN: The Ethernet port is as LAN port.
   WAN: The Ethernet port is as LAN port.
   Auto: It will be WAN Port if detect a DHCP server on the Ethernet port. Otherwise will be LAN port.
2. **LAP IP Address:** the local IP address of this device. The computers on your network must use the LAN IP address of your product as their Default Gateway. You can change it if necessary.
3. **Auto-Backup:** The WAN type will be change to 3G automatically, if the Wired-WAN is defunct.
4. **WAN Type**: WAN connection type of your ISP. You can click WAN Type Combo button to choose a correct one from the following options:

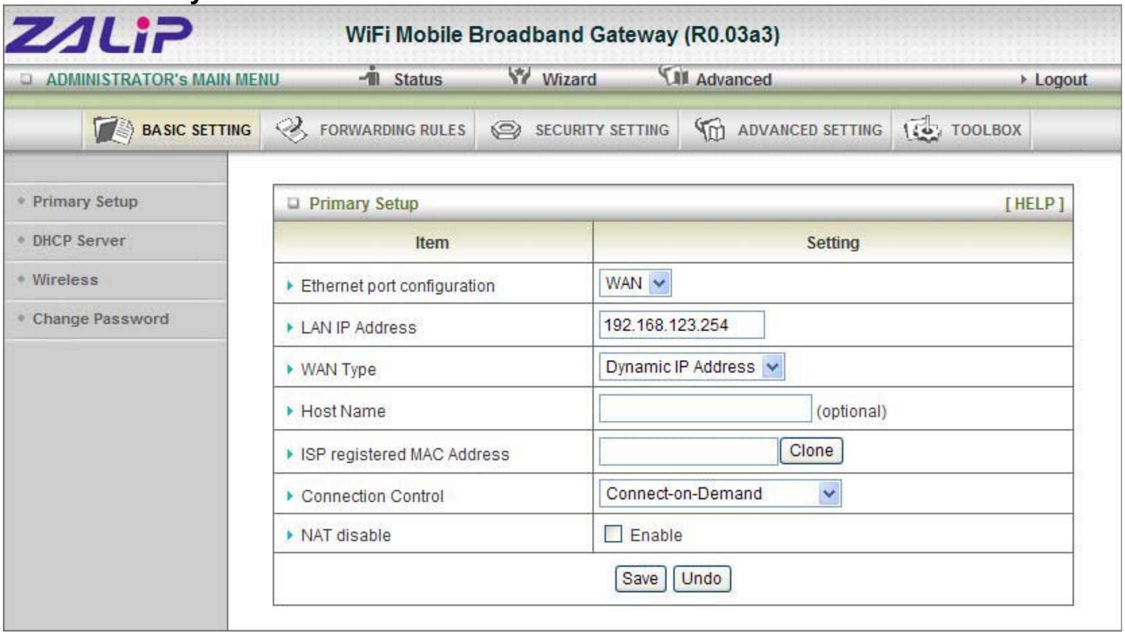
   4.1 **Static IP Address:**
   WAN IP Address, Subnet Mask, Gateway, Primary and Secondary DNS: enter the proper setting provided by your ISP.



Primary Setup [HELP]

Item	Setting
Ethernet port configuration	WAN
LAN IP Address	192.168.123.254
WAN Type	Static IP Address
WAN IP Address	
WAN Subnet Mask	
WAN Gateway	
Primary DNS	
Secondary DNS	
NAT disable	☐ Enable

4.2 Dynamic IP Address:



Primary Setup [HELP]

Item	Setting
Ethernet port configuration	WAN
LAN IP Address	192.168.123.254
WAN Type	Dynamic IP Address
Host Name	(optional)
ISP registered MAC Address	Clone
Connection Control	Connect-on-Demand
NAT disable	☐ Enable

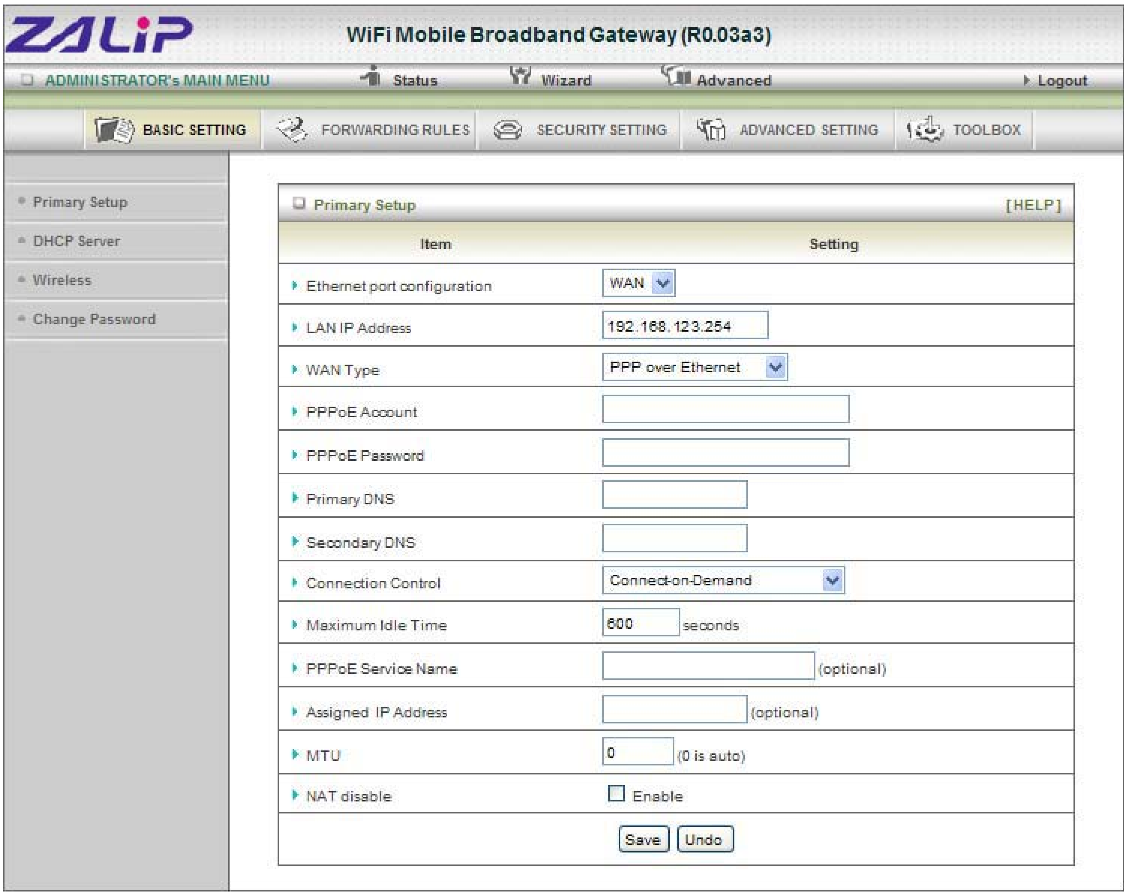
1. Host Name: optional, required by some ISPs, for example, @Home.
2. Connection Control: There are 3 modes to select:
   Connect-on-demand: The device will link up with ISP when the clients send

outgoing packets.

Auto Reconnect (Always-on): The device will link with ISP until the connection is established.

Manually: The device will not make the link until someone clicks the connect-button in the Status-page.

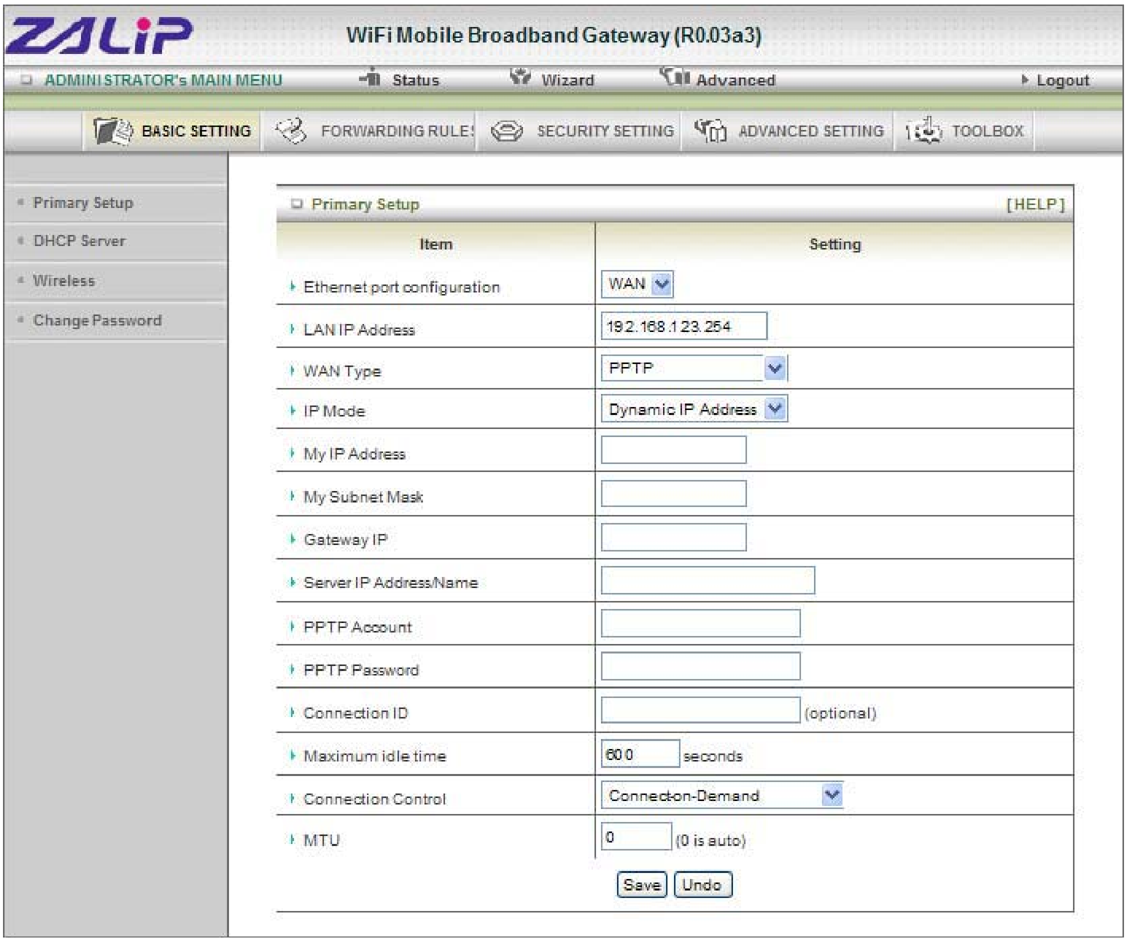
4.3 PPP over Ethernet



Item	Setting
Ethernet port configuration	WAN
LAN IP Address	192.168.123.254
WAN Type	PPP over Ethernet
PPPoE Account	
PPPoE Password	
Primary DNS	
Secondary DNS	
Connection Control	Connect-on-Demand
Maximum Idle Time	600 seconds
PPPoE Service Name	(optional)
Assigned IP Address	(optional)
MTU	0 (0 is auto)
NAT disable	□ Enable

1. PPPoE Account and Password: the account and password your ISP assigned to you. For security, this field appears blank. If you don't want to change the password, leave it empty.
2. Connection Control: There are 3 modes to select:
   Connect-on-demand: The device will link up with ISP when the clients send outgoing packets.
   Auto Reconnect (Always-on): The device will link with ISP until the connection is established.
   Manually: The device will not make the link until someone clicks the connect-button in the Status-page.
3. Maximum Idle Time: the amount of time of inactivity before disconnecting your PPPoE session. Set it to zero or enable Auto-reconnect to disable this feature.
4. PPPoE Service Name: optional. Input the service name if your ISP requires it. Otherwise, leave it blank.
5. Maximum Transmission Unit (MTU): Most ISP offers MTU value to users. The default MTU value is 0(auto).

4.4 PPTP



Primary Setup [HELP]

Item	Setting
Ethernet port configuration	WAN
LAN IP Address	192.168.123.254
WAN Type	PPTP
IP Mode	Dynamic IP Address
My IP Address	
My Subnet Mask	
Gateway IP	
Server IP Address/Name	
PPTP Account	
PPTP Password	
Connection ID	(optional)
Maximum idle time	600 seconds
Connection Control	Connect-on-Demand
MTU	0 (0 is auto)

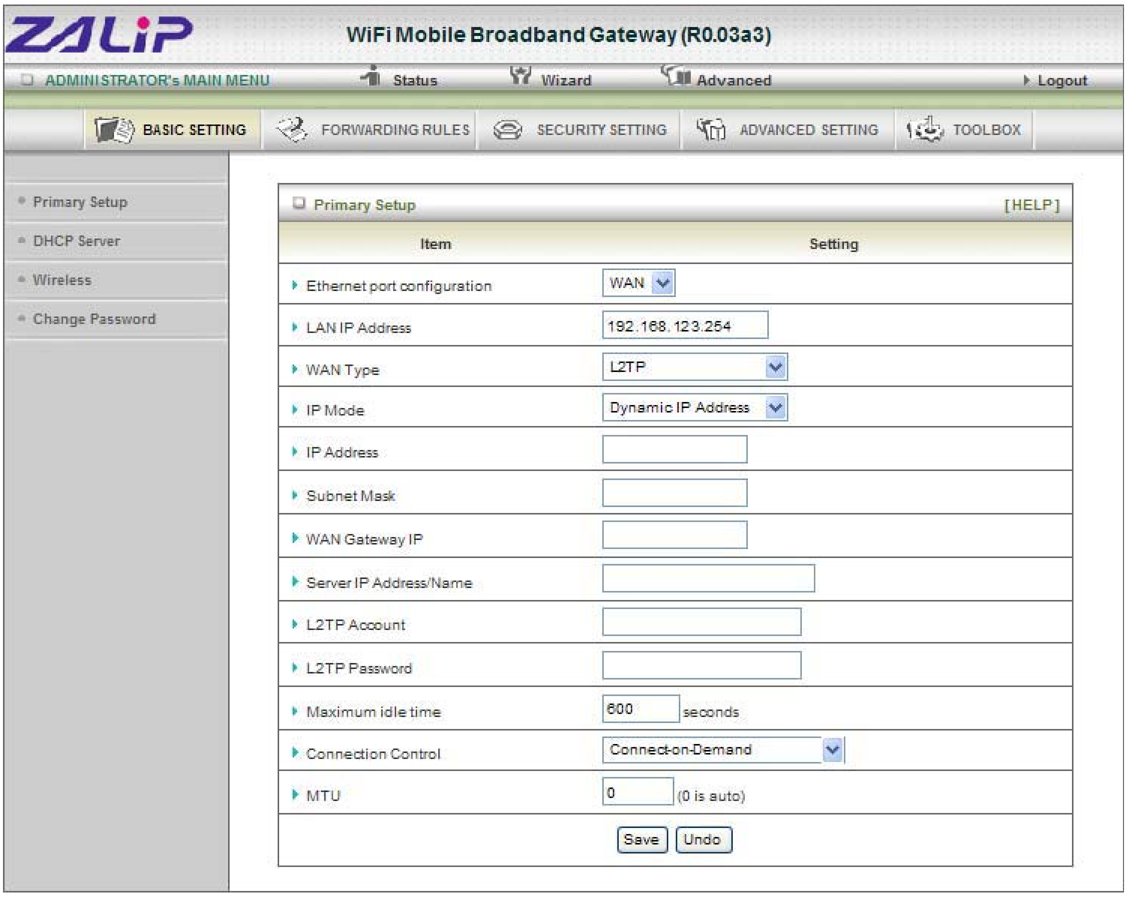
Save Undo

First, please check your ISP assigned and Select Static IP Address or Dynamic IP Address. For example: Use Static, the private IP address, subnet mask and Gateway are your ISP assigned to you.

1. My IP Address and My Subnet Mask: the private IP address and subnet mask your ISP assigned to you.
2. Server IP Address: the IP address of the PPTP server.
3. PPTP Account and Password: the account and password your ISP assigned to you. If you don't want to change the password, keep it empty.
4. Connection ID: optional. Input the connection ID if your ISP requires it.
5. Maximum Idle Time: the time of no activity to disconnect your PPTP session. Set it to zero or enable Auto-reconnect to disable this feature. If Auto-reconnect is enabled, this product will connect to ISP automatically, after system is restarted or connection is dropped.
6. Connection Control: There are 3 modes to select:
   Connect-on-demand: The device will link up with ISP when the clients send outgoing packets.
   Auto Reconnect (Always-on): The device will link with ISP until the connection is established.
   Manually: The device will not make the link until someone clicks the connect-button in the Status-page.
7. Maximum Transmission Unit (MTU): Most ISP offers MTU value to users. The

default MTU value is 0(auto).

4.5 L2TP

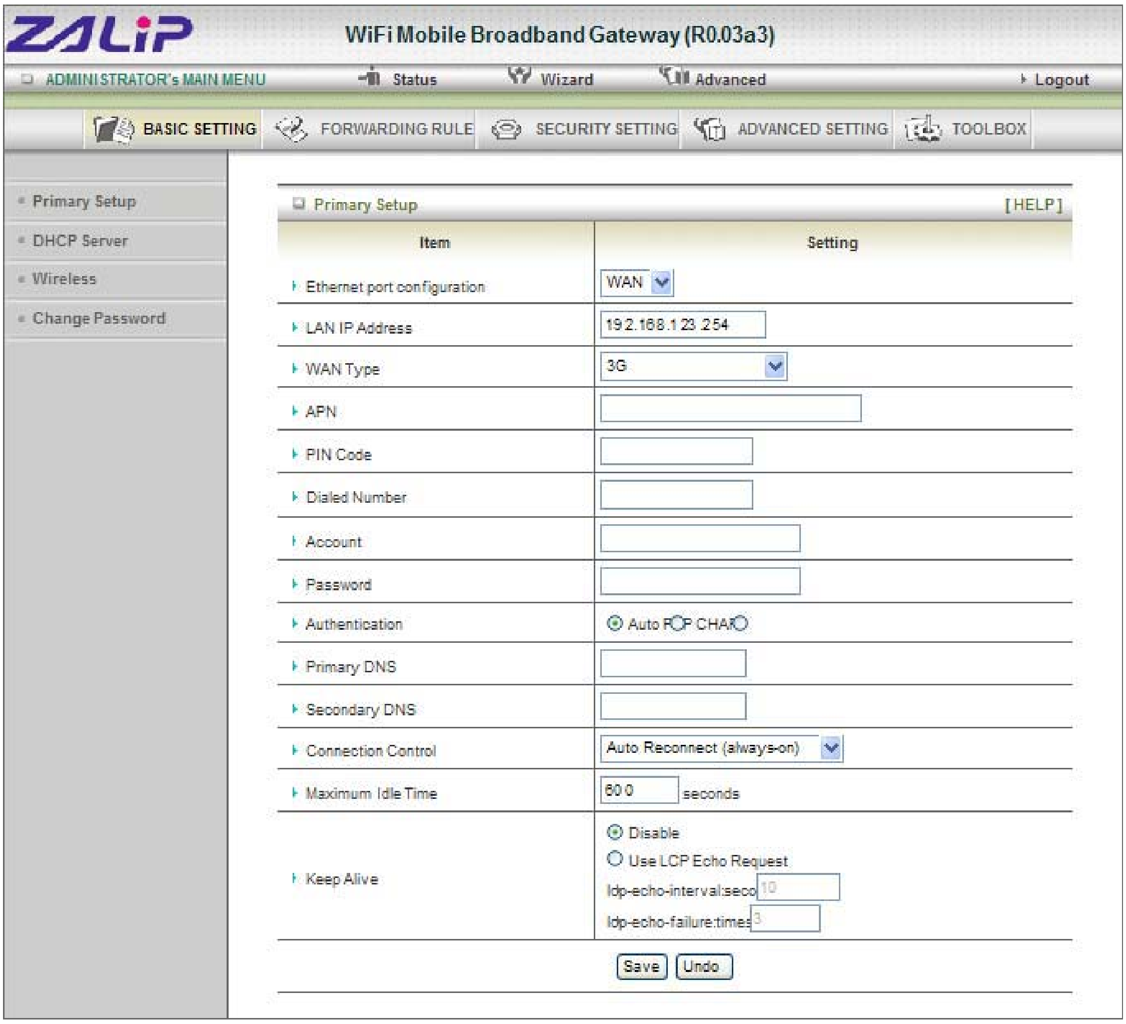


Item	Setting
Ethernet port configuration	WAN
LAN IP Address	192.168.123.254
WAN Type	L2TP
IP Mode	Dynamic IP Address
IP Address	
Subnet Mask	
WAN Gateway IP	
Server IP Address/Name	
L2TP Account	
L2TP Password	
Maximum idle time	600 seconds
Connection Control	Connect-on-Demand
MTU	0 (0 is auto)

First, please check your ISP assigned and Select Static IP Address or Dynamic IP Address. For example: Use Static, the private IP address, subnet mask and Gateway are your ISP assigned to you.

1. My IP Address and My Subnet Mask: the private IP address and subnet mask your ISP assigned to you.
2. Server IP Address: the IP address of the PPTP server.
3. PPTP Account and Password: the account and password your ISP assigned to you. If you don't want to change the password, keep it empty.
4. Connection ID: optional. Input the connection ID if your ISP requires it.
5. Maximum Idle Time: the time of no activity to disconnect your L2TP session. Set it to zero or enable Auto-reconnect to disable this feature. If Auto-reconnect is enabled, this product will connect to ISP automatically, after system is restarted or connection is dropped.
6. Connection Control: There are 3 modes to select:
   Connect-on-demand: The device will link up with ISP when the clients send outgoing packets.
   Auto Reconnect (Always-on): The device will link with ISP until the connection is established.
   Manually: The device will not make the link until someone clicks the connect-button in the Status-page.
7. Maximum Transmission Unit (MTU): Most ISP offers MTU value to users. The default MTU value is 0(auto).

4.6 3G



Primary Setup

Item	Setting
Ethernet port configuration	WAN
LAN IP Address	192.168.123.254
WAN Type	3G
APN	
PIN Code	
Dialed Number	
Account	
Password	
Authentication	● Auto ○ PAP ○ CHAP
Primary DNS	
Secondary DNS	
Connection Control	Auto Reconnect (always-on)
Maximum Idle Time	600 seconds
Keep Alive	● Disable ○ Use LCP Echo Request lcp-echo-interval:seco 10 lcp-echo-failure:times 3

For 3G WAN Networking. The WAN fields may not be necessary for your connection. The information on this page will only be used when your service provider requires you to enter a User Name and Password to connect to the 3G network.

Please refer to your documentation or service provider for additional information.

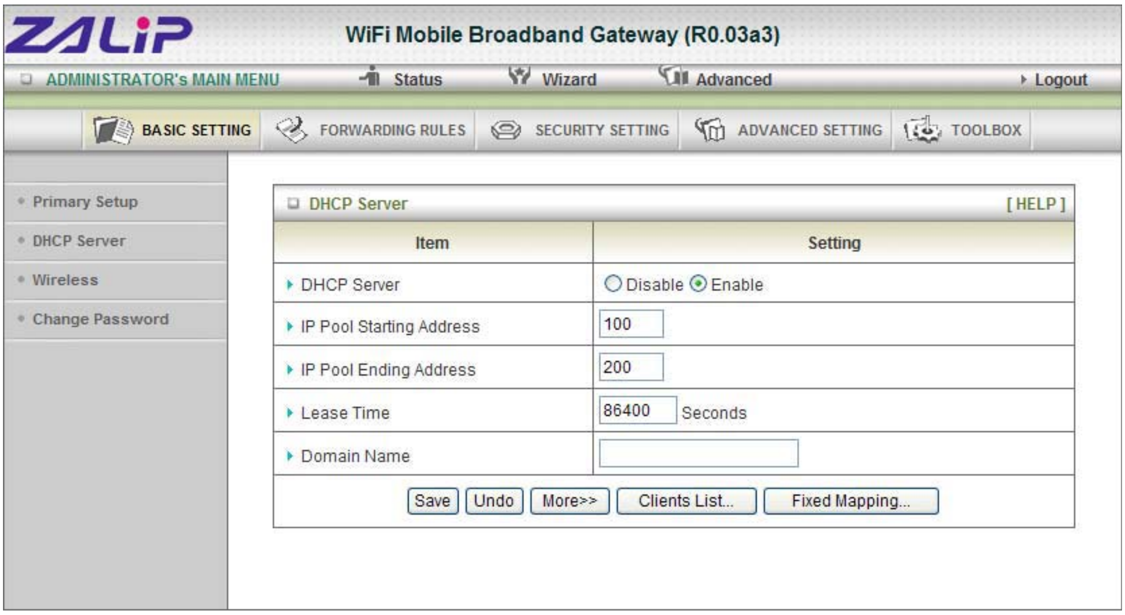
1. APN: Enter the APN for your PC card here.
2. Pin Code: Enter the Pin Code for your SIM card
3. Dial-Number: This field should not be altered except when required by your service provider.
4. User Name: Enter the new *User Name* for your PC card here.
5. Password: Enter the new *Password* for your PC card here.
6. Primary DNS: This feature allows you to assign a Primary DNS Server（Optional）
7. Secondary DNS: This feature allows you to assign a Secondary DNS Server（Optional）
8. Connection Control: There are 3 modes to select:

   Connect-on-demand: The device will link up with ISP when the clients send outgoing packets.

   Auto Reconnect (Always-on): The device will link with ISP until the connection is established.

9. Manually: The device will not make the link until someone clicks the connect-button in the Status-page.
10. Maximum Idle Time: The Connection will be broken when the idle time arrives.
11. Maximum Transmission Unit (MTU): Most ISP offers MTU value to users. The default MTU value is 0(auto).

3.2.1.2 DHCP Server



DHCP Server

Item	Setting
DHCP Server	○ Disable ● Enable
IP Pool Starting Address	100
IP Pool Ending Address	200
Lease Time	86400 Seconds
Domain Name	

Press **“More>>”,**

1. **DHCP Server:** Choose either **Disable** or **Enable**
2. **Lease Time:** DHCP lease time to the DHCP client
3. **IP Pool Starting/Ending Address:** Whenever there is a request, the DHCP server will automatically allocate an unused IP address from the IP address pool to the requesting computer. You must specify the starting / ending address of the IP address pool
4. **Domain Name:** Optional, this information will be passed to the client
5. **Primary DNS/Secondary DNS:** Optional, This feature allows you to assign a DNS Servers
6. **Primary WINS/Secondary WINS:** Optional, this feature allows you to assign a WINS Servers
7. **Gateway:** Optional, Gateway Address would be the IP address of an alternate Gateway.

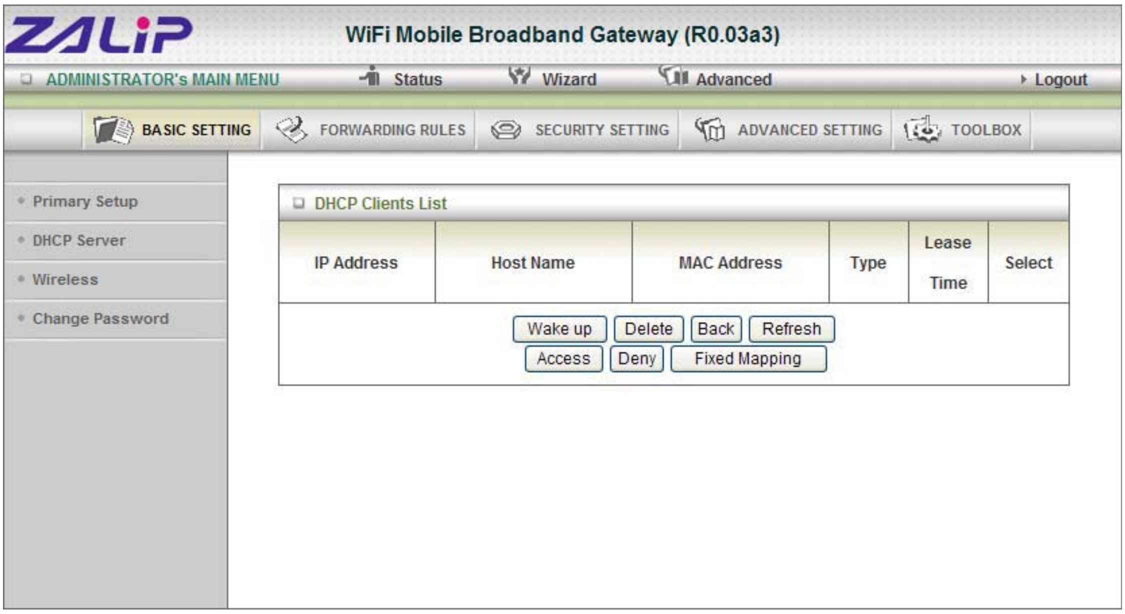
   This function enables you to assign another gateway to your PC, when DHCP server offers an IP to your PC.

After you finish your selection then

Either Click on **“Save”** to store what you just pick or click “**Undo”** to give up

DHCP Clients List

The list of DHCP clients shows here.

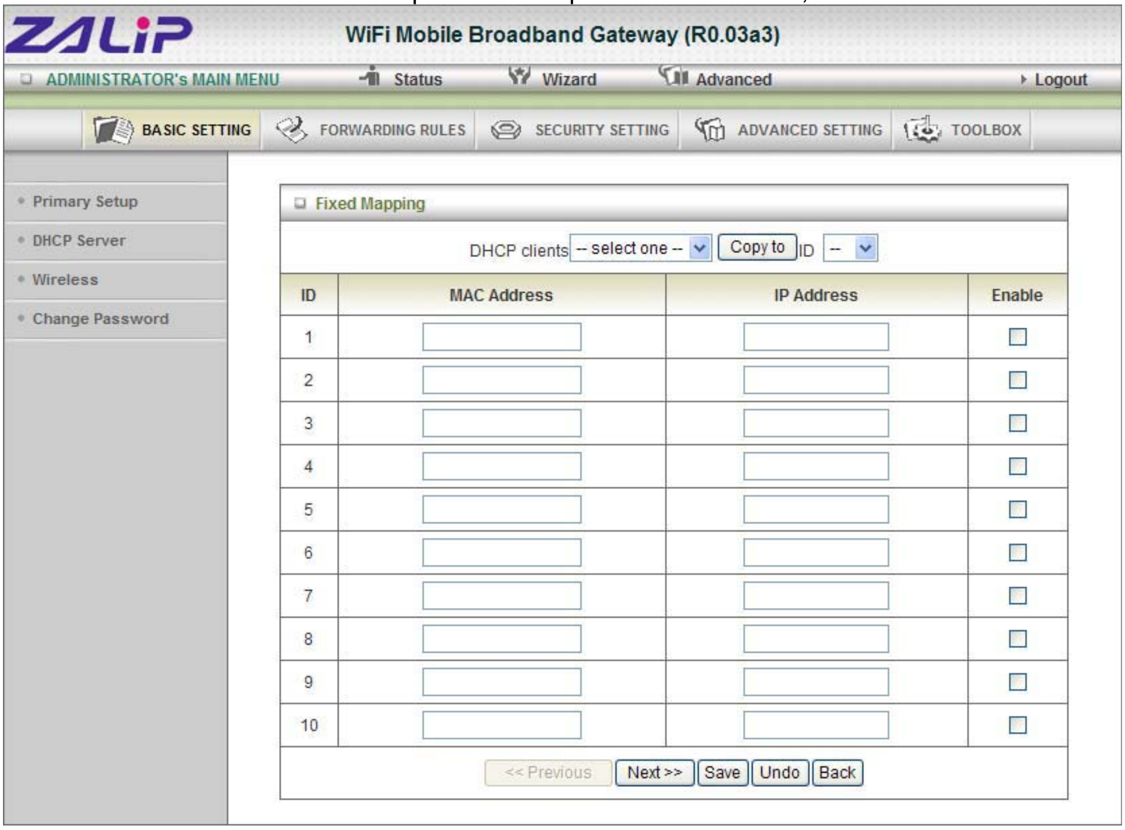


DHCP Clients List

IP Address	Host Name	MAC Address	Type	Lease Time	Select

DHCP Fixed Mapping

The DHCP Server will reserve the special IP for special MAC address, shows below.

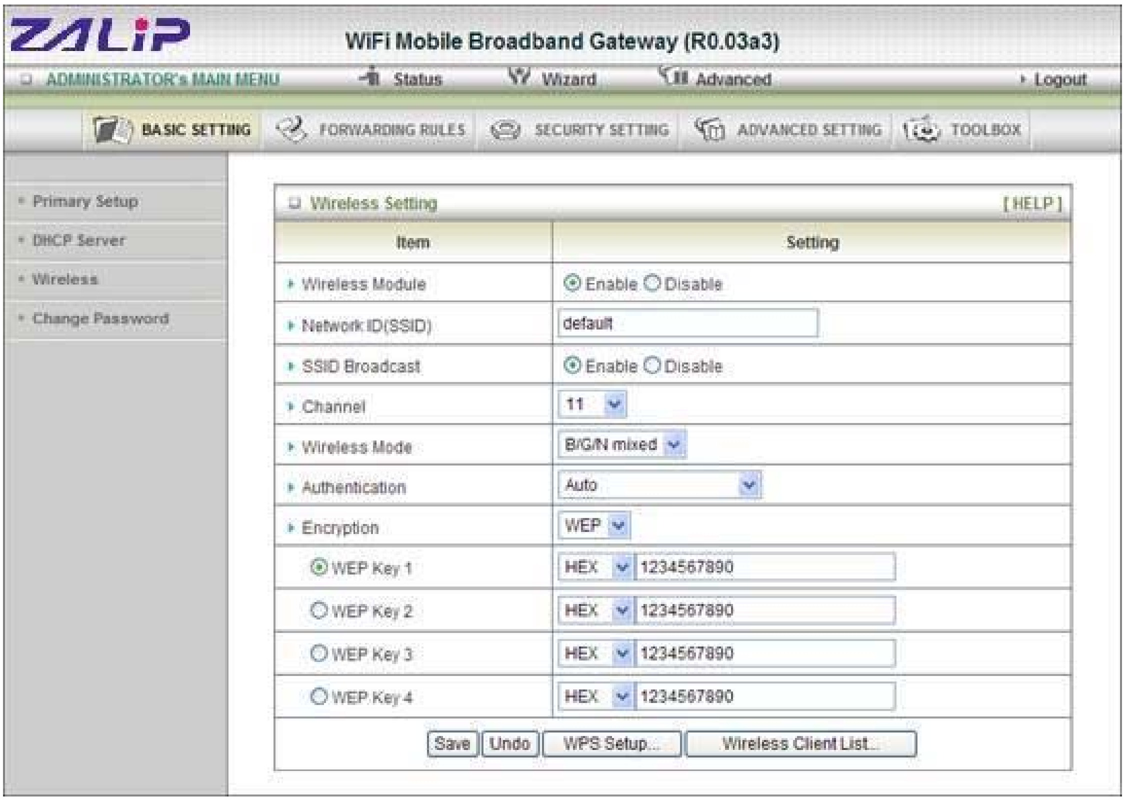


Fixed Mapping

DHCP clients -- select one -- ID --

ID	MAC Address	IP Address	Enable
1			□
2			□
3			□
4			□
5			□
6			□
7			□
8			□
9			□
10			□

3.2.1.3 Wireless Settings



Item	Setting
Wireless Module	● Enable ○ Disable
Network ID(SSID)	default
SSID Broadcast	● Enable ○ Disable
Channel	11
Wireless Mode	B/G/N mixed
Authentication	Auto
Encryption	WEP
● WEP Key 1	HEX 1234567890
○ WEP Key 2	HEX 1234567890
○ WEP Key 3	HEX 1234567890
○ WEP Key 4	HEX 1234567890

Wireless settings allow you to set the wireless configuration items.

1. **Wireless:** *Enabled* is the default**.** Selecting this option will allow you to set your Wireless Access Point (WAP) settings.
2. **Wireless Operation Mode:** Choose AP mode or Client mode. The factory default setting is AP mode.
3. **Network ID(SSID):** Service Set Identifier (SSID) is the name designated for a specific wireless local area network (WLAN). The SSID's factory default setting is *default*. The SSID can be easily changed to establish a new wireless network. (Note: SSID names may contain up to 32 ASCII characters).
4. **SSID Broadcast**: The router will broadcast beacons that have some information, including ssid so that wireless clients can know how many AP devices by scanning function in the network. Therefore, this function is disabled; the wireless clients can not find the device from beacons.
5. **Channel:** *Auto* is the default. Devices on the network must share the same channel. (Note: Wireless adapters automatically scan and match the wireless settings. You may also select the channel you wish to use).
6. **Wireless Mode:** Choose *B/G Mixed, B only, G only, N only, G/N Mixed or B/G/N mixed*. The factory default setting is *B/G/N mixed*.
7. **Authentication mode:** You may select from nine kinds of authentication to secure your wireless network: Open, Shared, Auto, WPA-PSK, WPA, WPA2-PSK, WPA2, WPA-PSK/WPA2-PSK, WPA/WPA2.

Open

Open system authentication simply consists of two communications. The first is an authentication request by the client that contains the station ID (typically the MAC address). This is followed by an authentication response from the AP/router containing a success or failure message. An example of when a failure may occur is if the client's MAC address is explicitly excluded in the AP/router configuration.

Shared

Shared key authentication relies on the fact that both stations taking part in the authentication process have the same "shared" key or passphrase. The shared key is manually set on both the client station and the AP/router. Three types of shared key authentication are available today for home or small office WLAN environments.

Auto

The AP will Select the Open or Shared by the client’s request automatically.

WPA-PSK

Select Encryption and Pre-share Key Mode

If you select HEX, you have to fill in 64 hexadecimal (0, 1, 2…8, 9, A, B…F) digits.

If you select ASCII, the length of pre-share key is from 8 to 63.

Fill in the key, Ex 12345678

WPA

Check Box was used to switch the function of the WPA. When the WPA function is enabled, the Wireless user must **authenticate** to this router first to use the Network service. RADIUS Server IP address or the 802.1X server’s domain-name.

Select Encryption and RADIUS Shared Key

If you select HEX, you have to fill in 64 hexadecimal (0, 1, 2…8, 9, A, B…F) digits

If you select ASCII, the length of pre-share key is from 8 to 63.

Key value shared by the RADIUS server and this router. This key value is consistent with the key value in the RADIUS server.

WPA-PSK2

WPA-PSK2 user AES and TKIP for Same the encryption, the others are same the WPA-PSK.

WPA2

WPA2 add uses AES and TKIP for encryption, the others are same the WPA.

WPA-PSK/WPA-PSK2

Another encryption options for WPA-PSK-TKIP and WPA-PSK2-AES, the others are same the WPA-PSK.

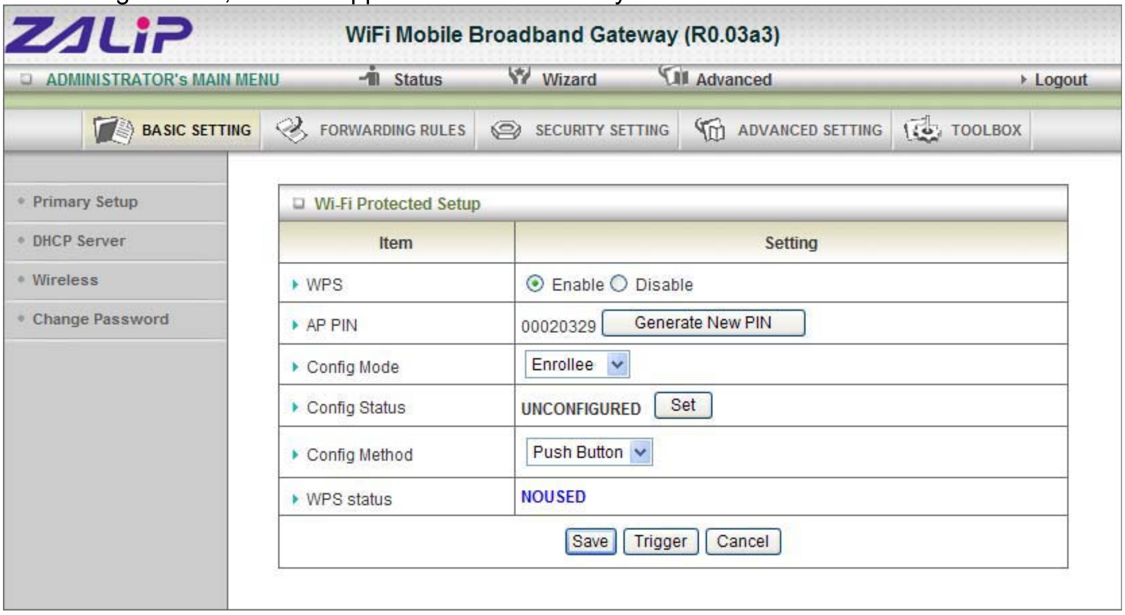
WPA/WPA2

Another encryption options for WPA-TKIP and WPA2-AES, the others are same the WPA.

WPS (Wi-Fi Protection Setup)

WPS is Wi-Fi Protection Setup which is similar to WCN-NET and offers safe and easy way in Wireless Connection.

The Config Method, we are support the PIN Code only.

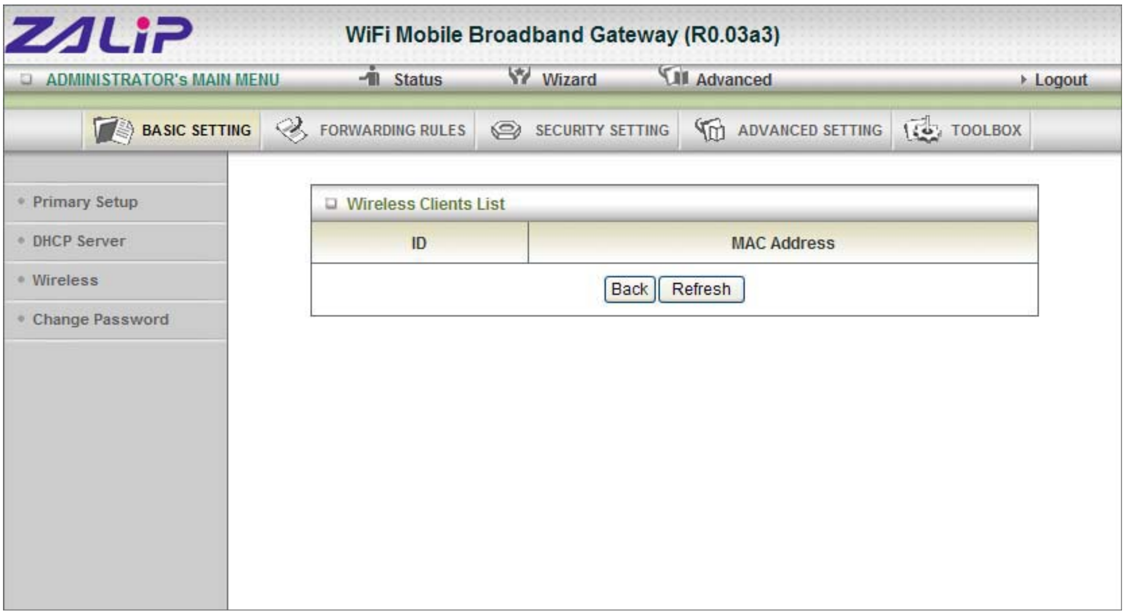


Wi-Fi Protected Setup

Item	Setting
WPS	● Enable ○ Disable
AP PIN	00020329 Generate New PIN
Config Mode	Enrollee
Config Status	UNCONFIGURED Set
Config Method	Push Button
WPS status	NOUSED

Wireless Client List

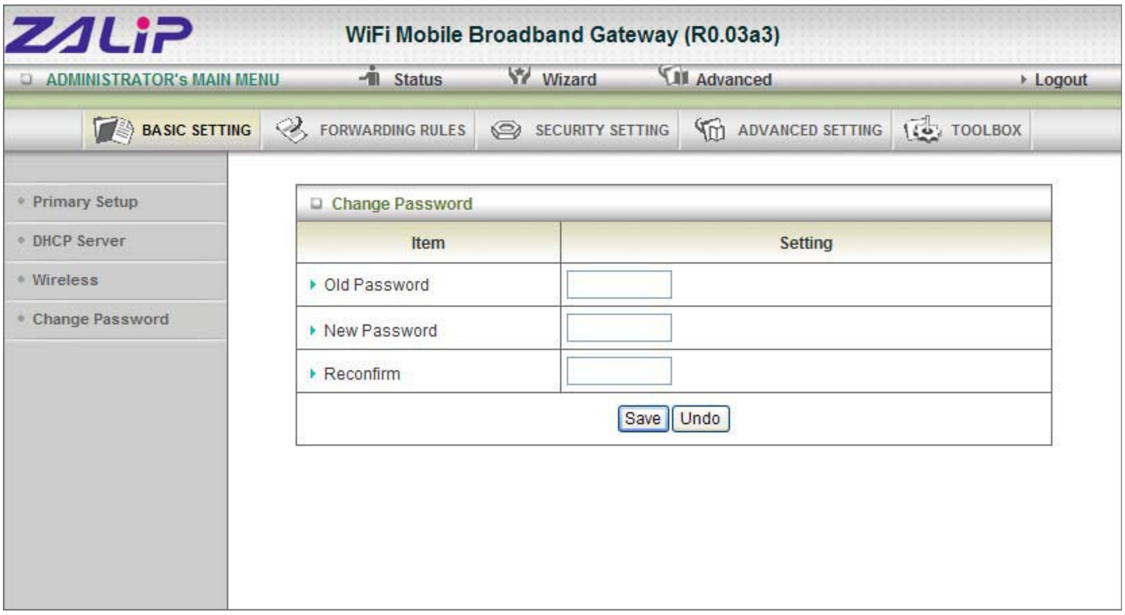
The list of wireless client is shows here.



Wireless Clients List

ID	MAC Address

3.2.1.4 Change Password



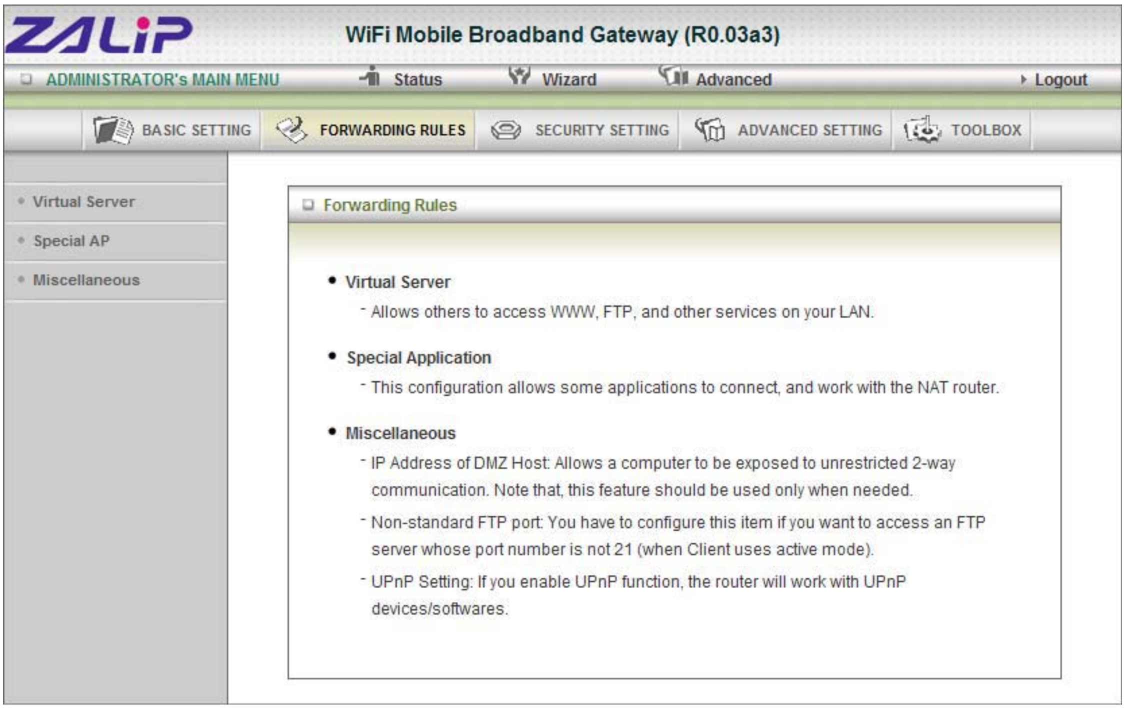
Change Password

Item	Setting
Old Password	
New Password	
Reconfirm	

You can change Password here. We **strongly** recommend you to change the system password for security reason.

Click on “Save” to store what you just select or “Undo” to give up

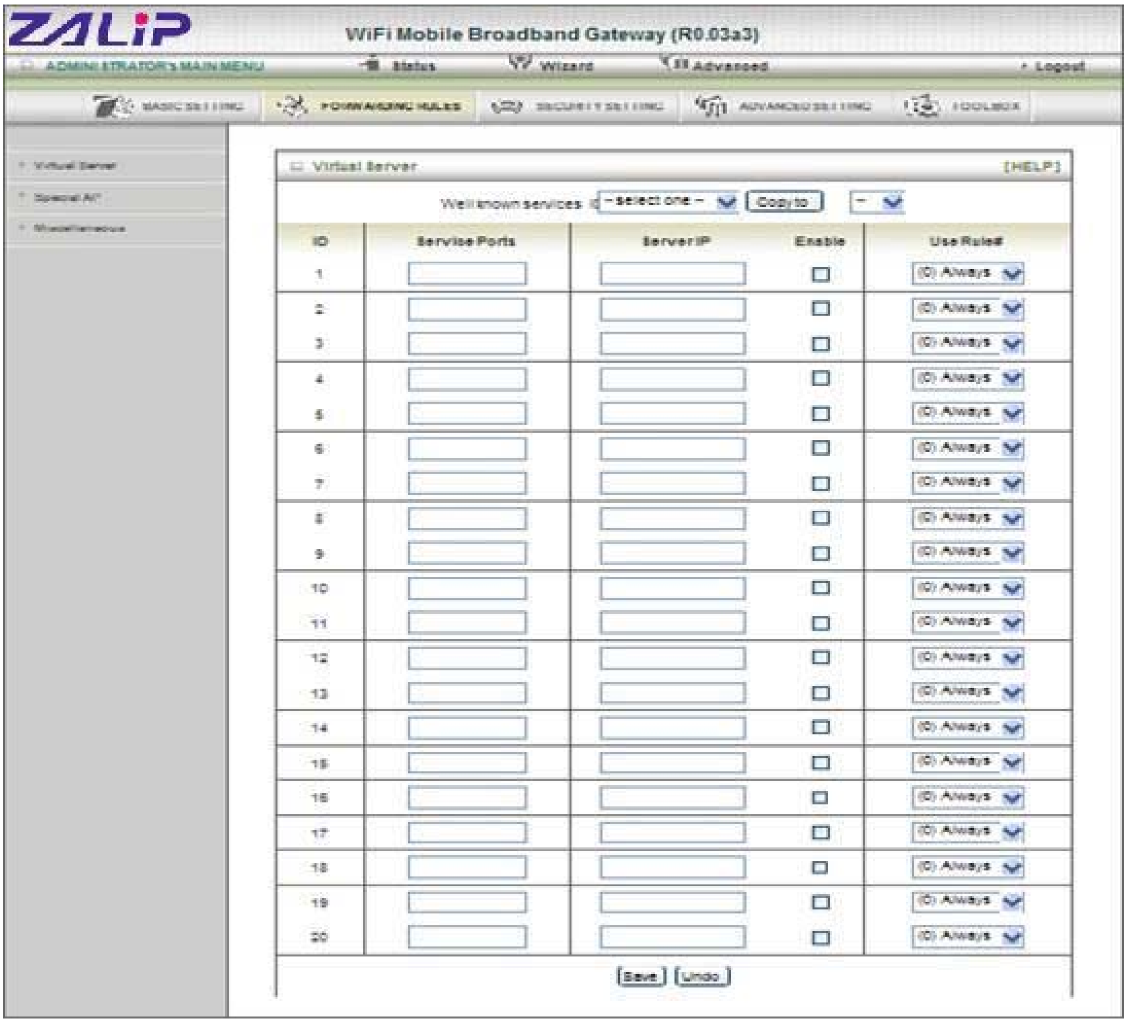
3.2.2 Forwarding Rules



Forwarding Rules

- Virtual Server
  - Allows others to access WWW, FTP, and other services on your LAN.
- Special Application
  - This configuration allows some applications to connect, and work with the NAT router.
- Miscellaneous
  - IP Address of DMZ Host: Allows a computer to be exposed to unrestricted 2-way communication. Note that, this feature should be used only when needed.
  - Non-standard FTP port: You have to configure this item if you want to access an FTP server whose port number is not 21 (when Client uses active mode).
  - UPnP Setting: If you enable UPnP function, the router will work with UPnP devices/softwares.

3.2.2.1 Virtual Server



ID	Service Ports	Server IP	Enable	Use Rule#
1			□	(0) Always
2			□	(0) Always
3			□	(0) Always
4			□	(0) Always
5			□	(0) Always
6			□	(0) Always
7			□	(0) Always
8			□	(0) Always
9			□	(0) Always
10			□	(0) Always
11			□	(0) Always
12			□	(0) Always
13			□	(0) Always
14			□	(0) Always
15			□	(0) Always
16			□	(0) Always
17			□	(0) Always
18			□	(0) Always
19			□	(0) Always
20			□	(0) Always

This product's NAT firewall filters out unrecognized packets to protect your Intranet, so all hosts behind this product are invisible to the outside world. If you wish, you can make some of them accessible by enabling the Virtual Server Mapping.

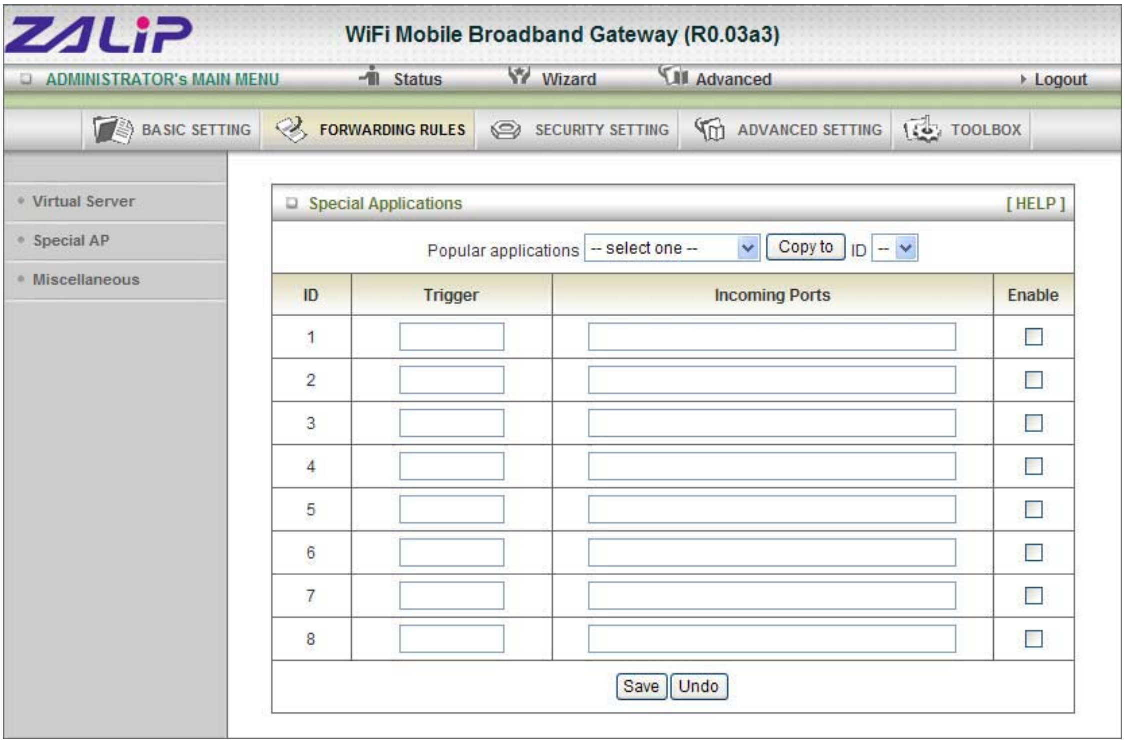
A virtual server is defined as a Service Port, and all requests to this port will be redirected to the computer specified by the Server IP. Virtual Server can work with Scheduling Rules, and give user more flexibility on Access control. For Detail, please refer to Scheduling Rule.

For example, if you have an FTP server (port 21) at 192.168.123.1, a Web server (port 80) at 192.168.123.2, and a VPN server at 192.168.123.6, then you need to specify the following virtual server mapping table:

Service Port	Server IP	Enable
21	192.168.123.1	V
80	192.168.123.2	V
1723	192.168.123.6	V

Click on "Save" to store what you just select or "Undo" to give up

3.2.2.2 Special AP



ID	Trigger	Incoming Ports	Enable
1			□
2			□
3			□
4			□
5			□
6			□
7			□
8			□

Some applications require multiple connections, like Internet games, Video conferencing, Internet telephony, etc. Because of the firewall function, these applications cannot work with a pure NAT router. The Special Applications feature allows some of these applications to work with this product. If the mechanism of Special Applications fails to make an application work, try setting your computer as the DMZ host instead.

1. **Trigger:** the outbound port number issued by the application.
2. **Incoming Ports**: when the trigger packet is detected, the inbound packets sent to the specified port numbers are allowed to pass through the firewall.

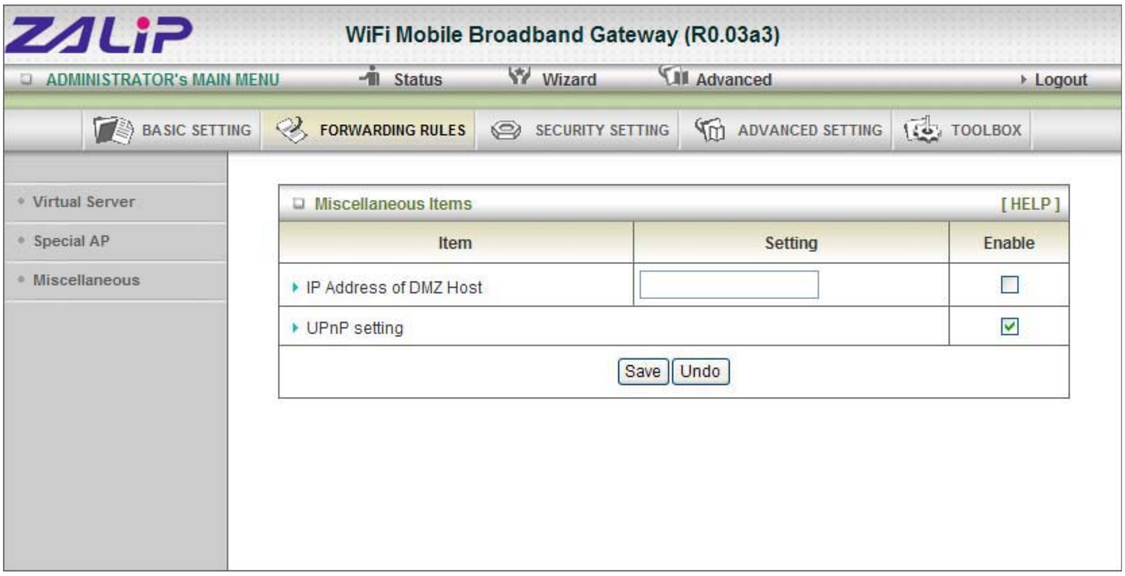
   This product provides some predefined settings.

   1. Select your application and
   2. Click “**Copy to”** to add the predefined setting to your list.

   Note! At any given time, only one PC can use each Special Application tunnel.

Click on “Save” to store what you just select or” Undo” to give up

3.2.2.3 Miscellaneous



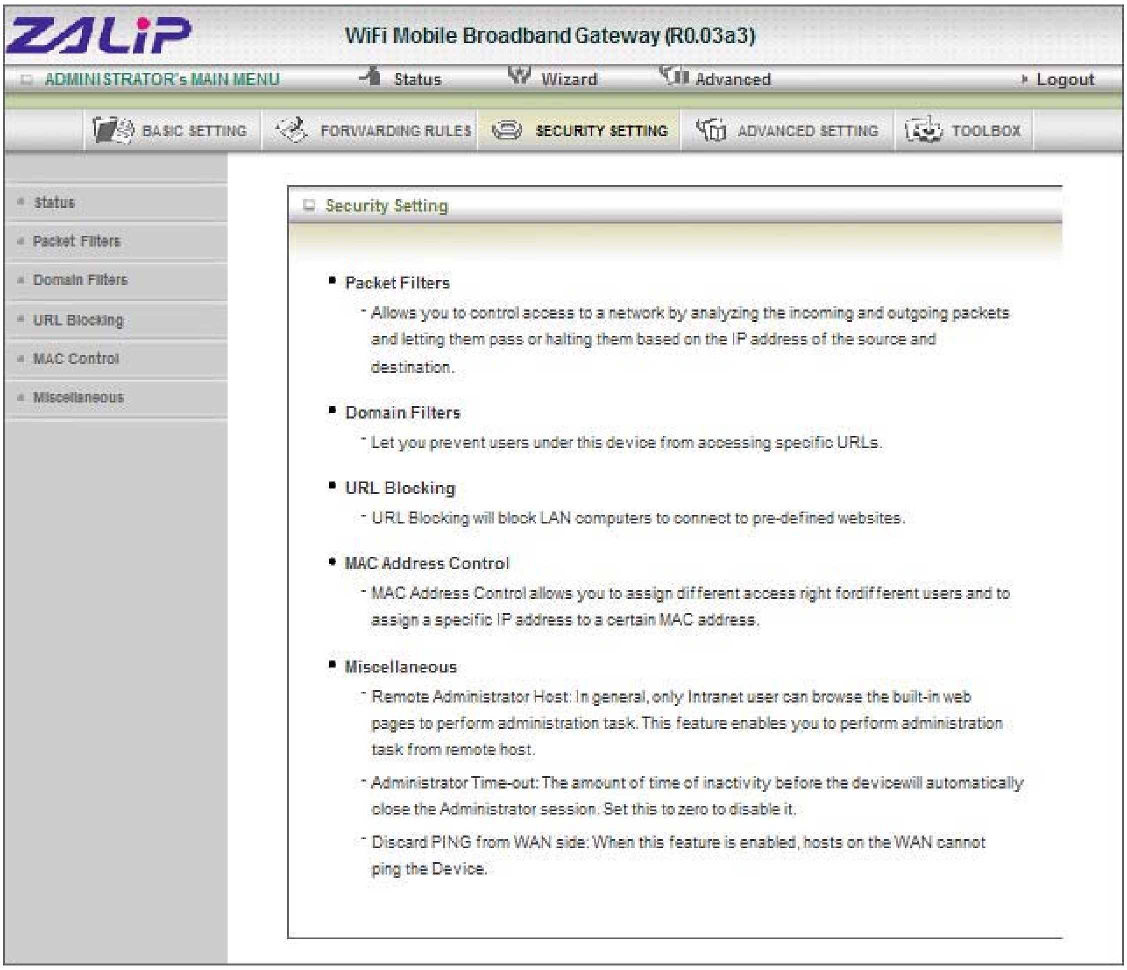
Miscellaneous Items

Item	Setting	Enable
IP Address of DMZ Host		□
UPnP setting		☑

1. **IP Address of DMZ Host**
   DMZ (Demilitarized Zone) Host is a host without the protection of firewall. It allows a computer to be exposed to unrestricted 2-way communication for Internet games, Video conferencing, Internet telephony and other special applications.
2. **UPnP Setting**
   The device also supports this function. If the OS supports this function enable it, like Windows XP. When the user gets IP from Device and will see icon as below:
3. **IGMP setting**
   Select the “Enable” item to enable the IGMP Multicast.

Click on “Save” to store what you just select or “Undo” to give up

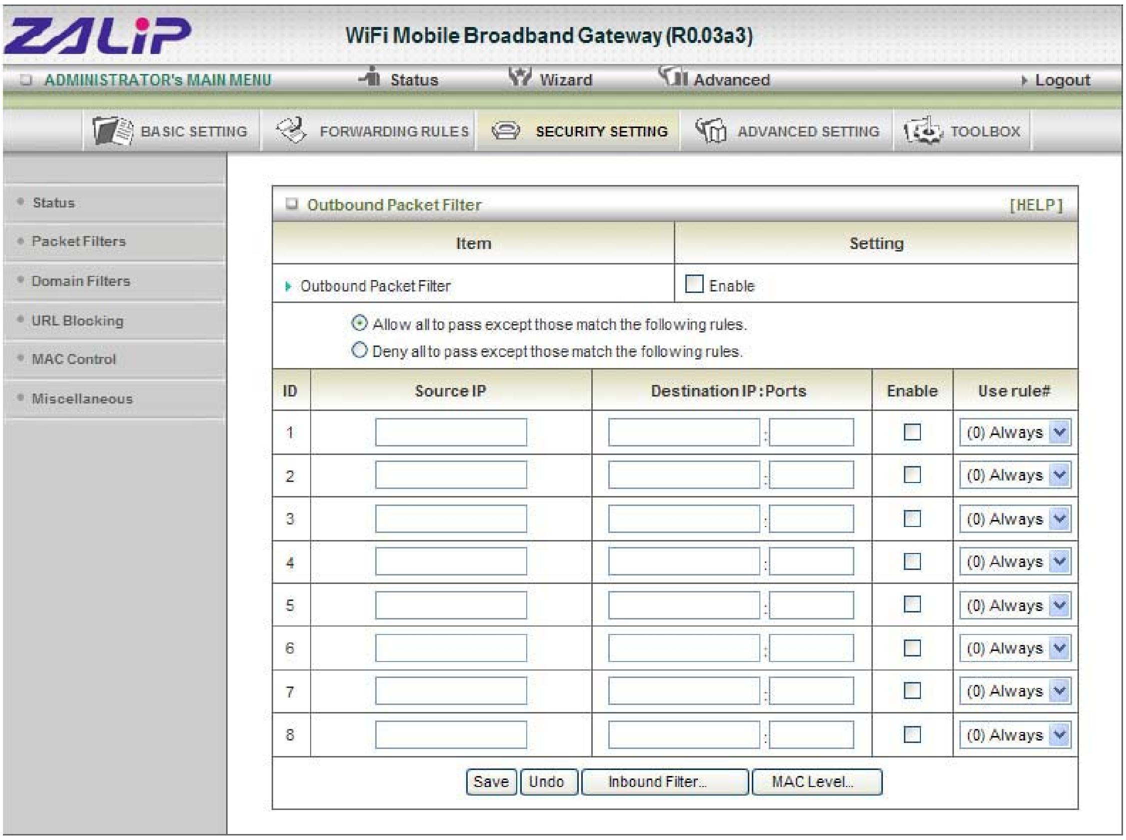
3.2.3 Security Setting



Security Setting

- Packet Filters
  - Allows you to control access to a network by analyzing the incoming and outgoing packets and letting them pass or halting them based on the IP address of the source and destination.
- Domain Filters
  - Let you prevent users under this device from accessing specific URLs.
- URL Blocking
  - URL Blocking will block LAN computers to connect to pre-defined websites.
- MAC Address Control
  - MAC Address Control allows you to assign different access right fordifferent users and to assign a specific IP address to a certain MAC address.
- Miscellaneous
  - Remote Administrator Host: In general, only Intranet user can browse the built-in web pages to perform administration task. This feature enables you to perform administration task from remote host.
  - Administrator Time-out: The amount of time of inactivity before the devicewill automatically close the Administrator session. Set this to zero to disable it.
  - Discard PING from WAN side: When this feature is enabled, hosts on the WAN cannot ping the Device.

3.2.3.1 Packet Filters



Outbound Packet Filter [HELP]

Item	Setting
Outbound Packet Filter	□ Enable

● Allow all to pass except those match the following rules.
○ Deny all to pass except those match the following rules.

ID	Source IP	Destination IP : Ports	Enable	Use rule#
1		:	□	(0) Always
2		:	□	(0) Always
3		:	□	(0) Always
4		:	□	(0) Always
5		:	□	(0) Always
6		:	□	(0) Always
7		:	□	(0) Always
8		:	□	(0) Always

Packet Filter includes both outbound filter and inbound filter. And they have same way to setting. Packet Filter enables you to control what packets are allowed to pass the router. Outbound filter applies on all outbound packets. However, inbound filter applies on packets that destined to Virtual Servers or DMZ host only. You can select one of the two filtering policies:

1. Allow all to pass except those match the specified rules
2. Deny all to pass except those match the specified rules

You can specify 8 rules for each direction: inbound or outbound. For each rule, you can define the following:

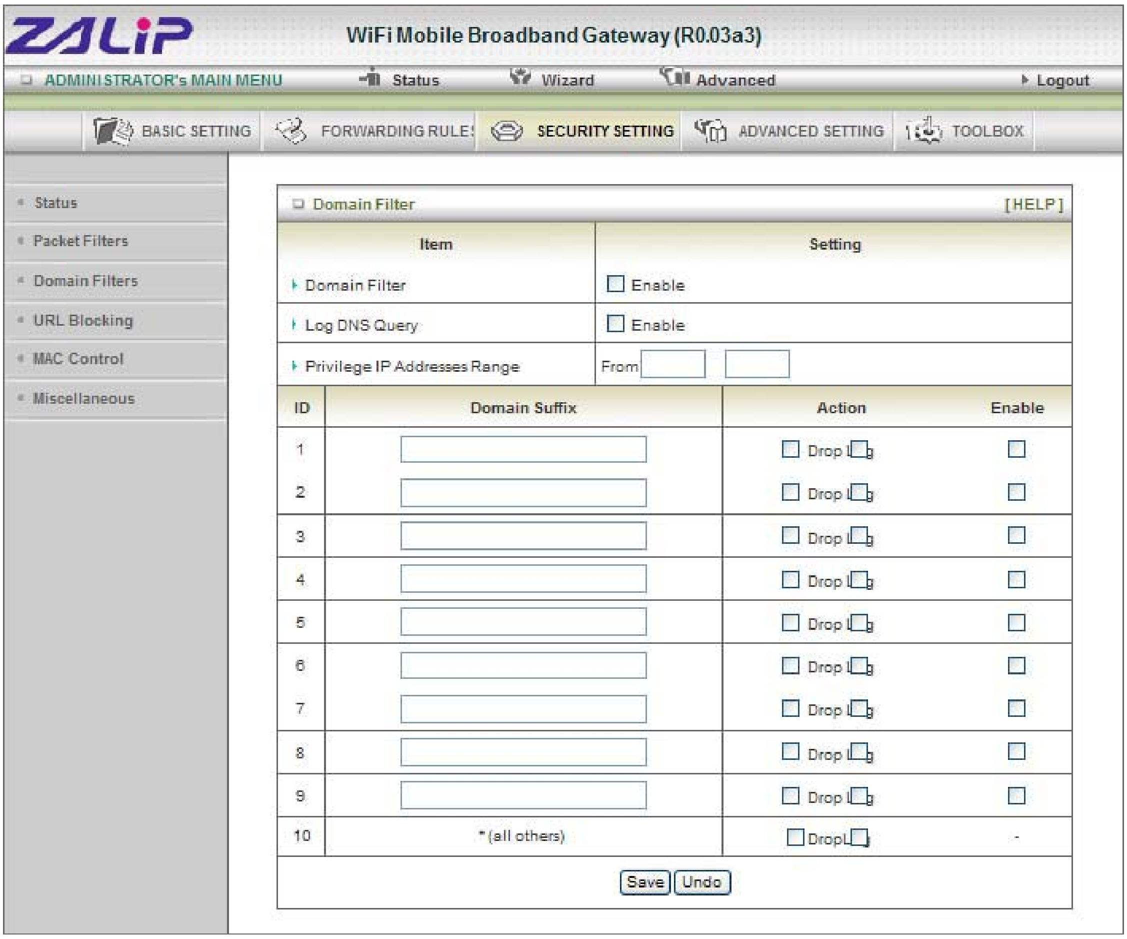
- Source IP address
- Source port
- Destination IP address
- Destination port
- Protocol: TCP or UDP or both.
- Use Rule#

For source or destination IP address, you can define a single IP address (4.3.2.1) or a range of IP addresses (4.3.2.1-4.3.2.254). An empty implies all IP addresses.
For source or destination port, you can define a single port (80) or a range of ports (1000-1999). Add prefix "T" or "U" to specify TCP or UDP protocol. For example, T80, U53, U2000-2999, No prefix indicates both TCP and UDP are defined. An empty implies all port addresses. Packet Filter can work with Scheduling Rules, and give user more flexibility on Access control. For Detail, please refer to Scheduling Rule.

Each rule can be enabled or disabled individually.

Click on “Save” to store what you just select or “Undo” to give up

3.2.3.2 Domain Filters



Domain Filter [HELP]

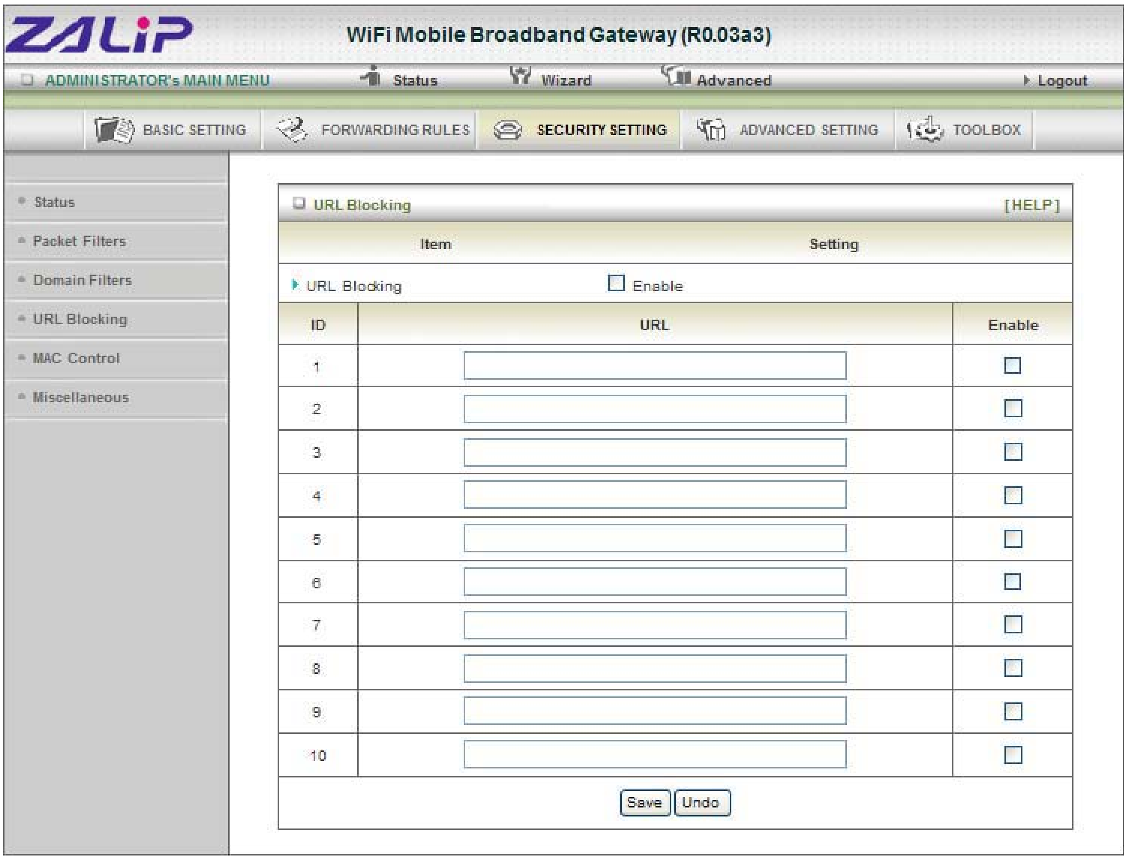
Item	Setting
Domain Filter	☐ Enable
Log DNS Query	☐ Enable
Privilege IP Addresses Range	From ▭ ▭

ID	Domain Suffix	Action	Enable
1	▭	☐ Drop ☐ Log	☐
2	▭	☐ Drop ☐ Log	☐
3	▭	☐ Drop ☐ Log	☐
4	▭	☐ Drop ☐ Log	☐
5	▭	☐ Drop ☐ Log	☐
6	▭	☐ Drop ☐ Log	☐
7	▭	☐ Drop ☐ Log	☐
8	▭	☐ Drop ☐ Log	☐
9	▭	☐ Drop ☐ Log	☐
10	* (all others)	☐ Drop ☐ Log	-

1. **Domain Filter**
   Let you prevent users under this device from accessing specific URLs.
2. **Domain Filter Enable**
   Check if you want to enable Domain Filter.
3. **Log DNS Query**
   Check if you want to log the action when someone accesses the specific URLs.
4. **Privilege IP Address Range**
   Setting a group of hosts and privilege these hosts to access network without restriction.
5. **Domain Suffix**
   A suffix of URL can be restricted, for example, ".com", "xxx.com".
6. **Action**
   When someone is accessing the URL met the domain-suffix, what kind of action you want. Check drop to block the access. Check “log” to log these access.
7. **Enable**
   Check to enable each rule.

Click on “Save” to store what you just select or “Undo” to give up

URL Blocking



URL Blocking

Item	Setting
URL Blocking	□ Enable

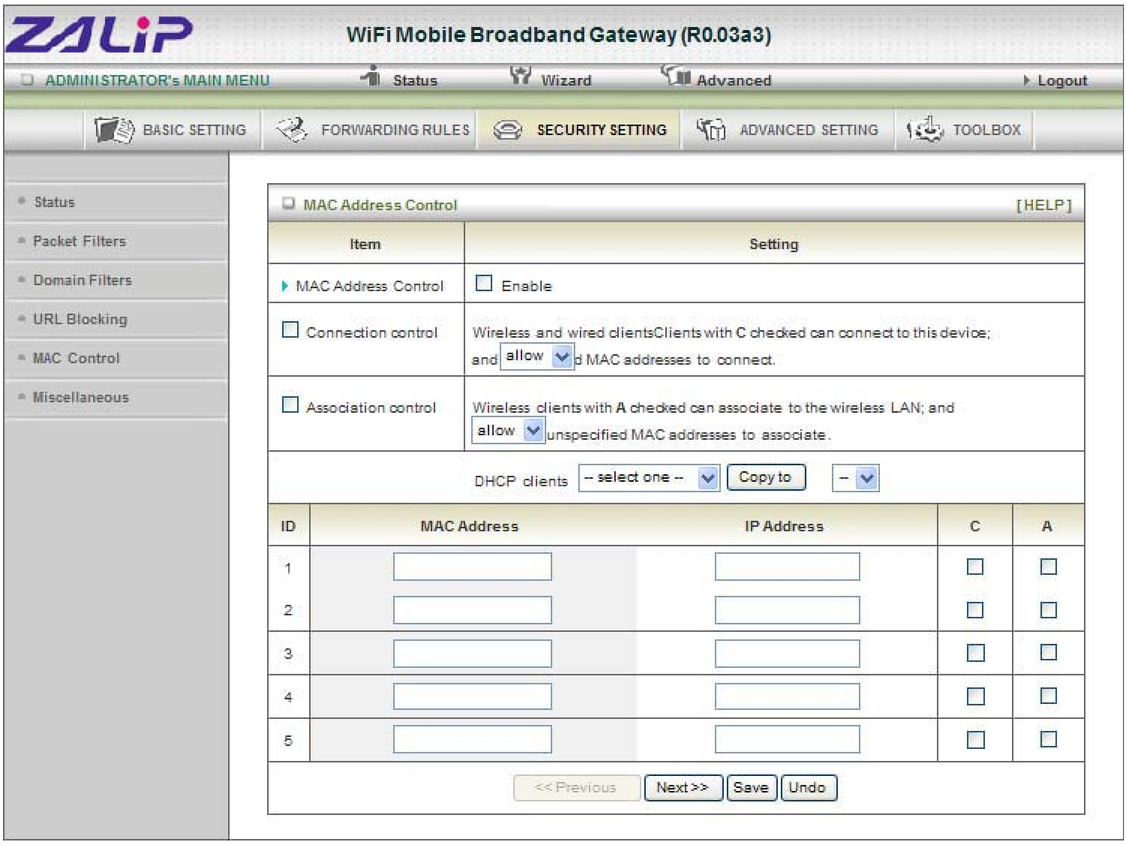
ID	URL	Enable
1		□
2		□
3		□
4		□
5		□
6		□
7		□
8		□
9		□
10		□

URL Blocking will block LAN computers to connect to pre-define Websites. The major difference between “Domain filter” and “URL Blocking” is Domain filter require user to input suffix (like .com or .org, etc), while URL Blocking require user to input a keyword only. In other words, Domain filter can block specific website, while URL Blocking can block hundreds of websites by simply a keyword.

1. **URL Blocking Enable**
   Check if you want to enable URL Blocking.
2. **URL**
   If any part of the Website's URL matches the pre-defined word, the connection will be blocked.
   For example, you can use pre-defined word "sex" to block all websites if their URLs contain pre-defined word "sex".
3. **Enable**
   Check to enable each rule.

Click on “Save” to store what you just select or “Undo” to give up

3.2.3.3 MAC Control



Item	Setting
MAC Address Control	□ Enable
□ Connection control	Wireless and wired clientsClients with C checked can connect to this device; and allow d MAC addresses to connect.
□ Association control	Wireless clients with A checked can associate to the wireless LAN; and allow unspecified MAC addresses to associate.

DHCP clients -- select one -- Copy to --

ID	MAC Address	IP Address	C	A
1			□	□
2			□	□
3			□	□
4			□	□
5			□	□

MAC Address Control allows you to assign different access right for different users and to assign a specific IP address to a certain MAC address.

1. **MAC Address Control**

   Check “Enable” to enable the “MAC Address Control”. All of the settings in this page will take effect only when “Enable” is checked.

2. **Connection control**

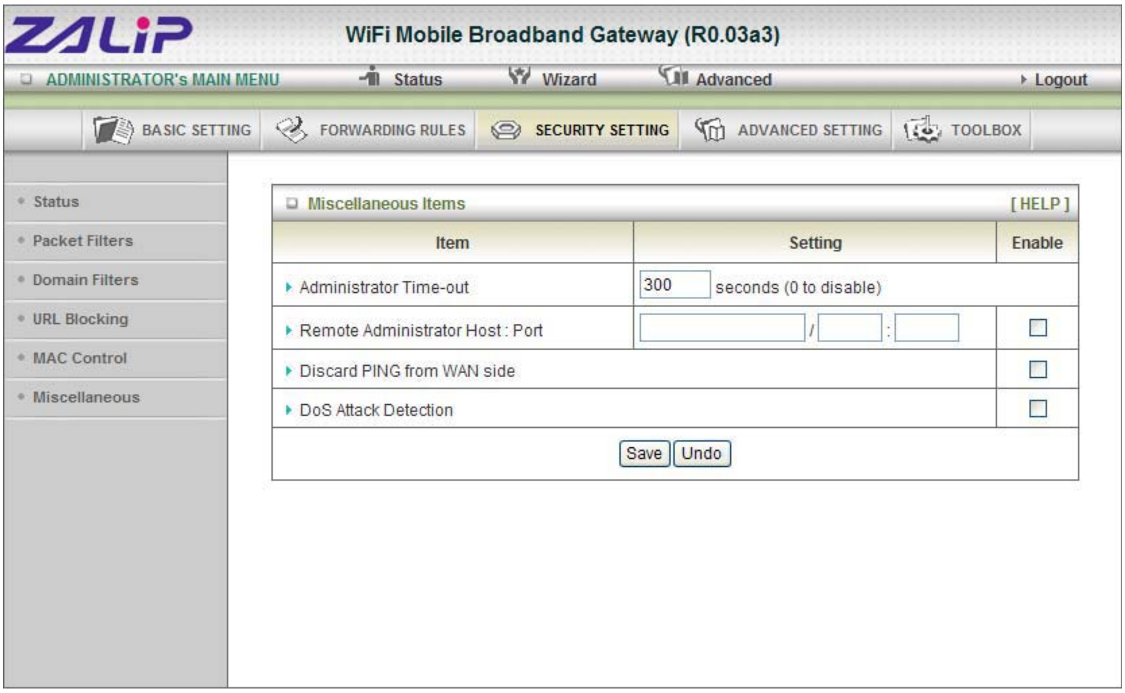
   Check "Connection control" to enable the controlling of which wired and wireless clients can connect to this device. If a client is denied to connect to this device, it means the client can't access to the Internet either. Choose "allow" or "deny" to allow or deny the clients, whose MAC addresses are not in the "Control table" (please see below), to connect to this device.

3. **Association control**

   Check "Association control" to enable the controlling of which wireless client can associate to the wireless LAN. If a client is denied to associate to the wireless LAN, it means the client can't send or receive any data via this device. Choose "allow" or "deny" to allow or deny the clients, whose MAC addresses are not in the "Control table", to associate to the wireless LAN

Click on “Save” to store what you just select or “Undo” to give up
Click on “Next Page” to go down or “Previous page” back to last page

3.2.3.4 Miscellaneous



Miscellaneous Items

Item	Setting	Enable
Administrator Time-out	300 seconds (0 to disable)	
Remote Administrator Host : Port	/ :	□
Discard PING from WAN side		□
DoS Attack Detection		□

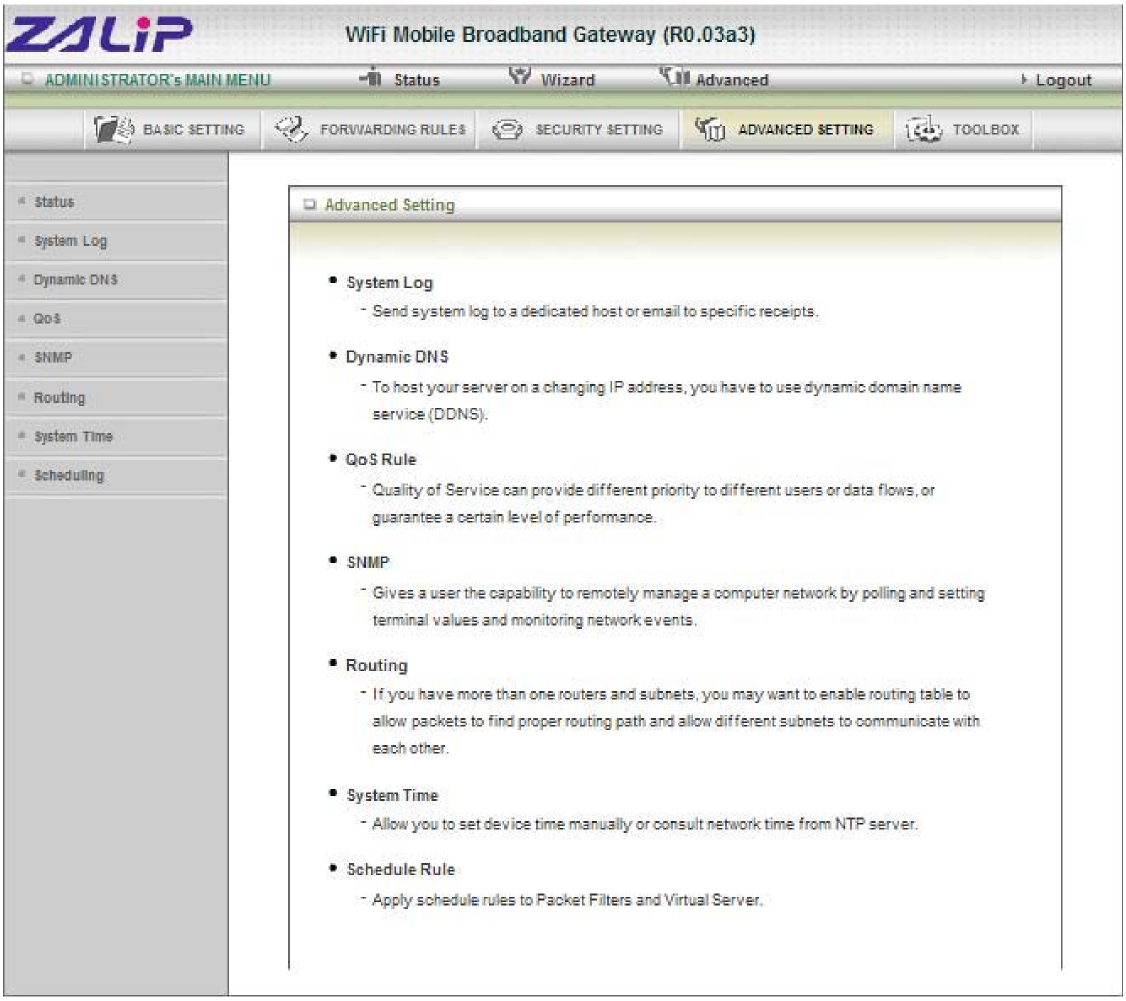
1. **Administrator Time-out**
   The time of no activity to logout automatically, you may set it to zero to disable this feature.
2. **Remote Administrator Host/Port**
   In general, only Intranet user can browse the built-in web pages to perform administration task. This feature enables you to perform administration task from remote host. If this feature is enabled, only the specified IP address can perform remote administration. If the specified IP address is 0.0.0.0, any host can connect to this product to perform administration task. You can use subnet mask bits "/nn" notation to specified a group of trusted IP addresses for example, "10.1.2.0/24".
   NOTE: When Remote Administration is enabled, the web server port will be shifted to 80. You can change web server port to other port, too.
3. **Discard PING from WAN side**

   When this feature is enabled, any host on the WAN cannot ping this product.
4. **DoS Attack Detection**

   When this feature is enabled, the router will detect and log the DoS attack comes from the Internet. Currently, the router can detect the following DoS attack: SYN Attack, WinNuke, Port Scan, Ping of Death, Land Attack etc.

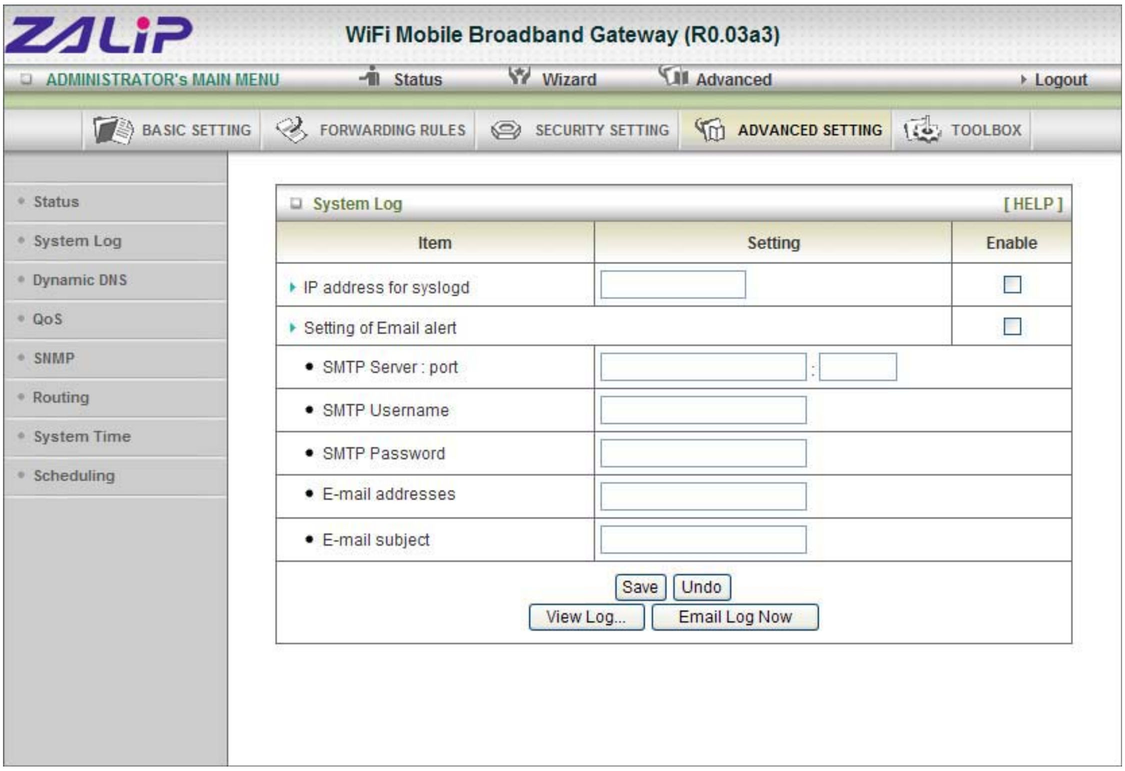
Click on “Save” to store what you just select or” Undo” to give up

3.2.3.5 Advanced Setting



- System Log
  - Send system log to a dedicated host or email to specific receipts.
- Dynamic DNS
  - To host your server on a changing IP address, you have to use dynamic domain name service (DDNS).
- QoS Rule
  - Quality of Service can provide different priority to different users or data flows, or guarantee a certain level of performance.
- SNMP
  - Gives a user the capability to remotely manage a computer network by polling and setting terminal values and monitoring network events.
- Routing
  - If you have more than one routers and subnets, you may want to enable routing table to allow packets to find proper routing path and allow different subnets to communicate with each other.
- System Time
  - Allow you to set device time manually or consult network time from NTP server.
- Schedule Rule
  - Apply schedule rules to Packet Filters and Virtual Server.

3.2.3.6 System Log



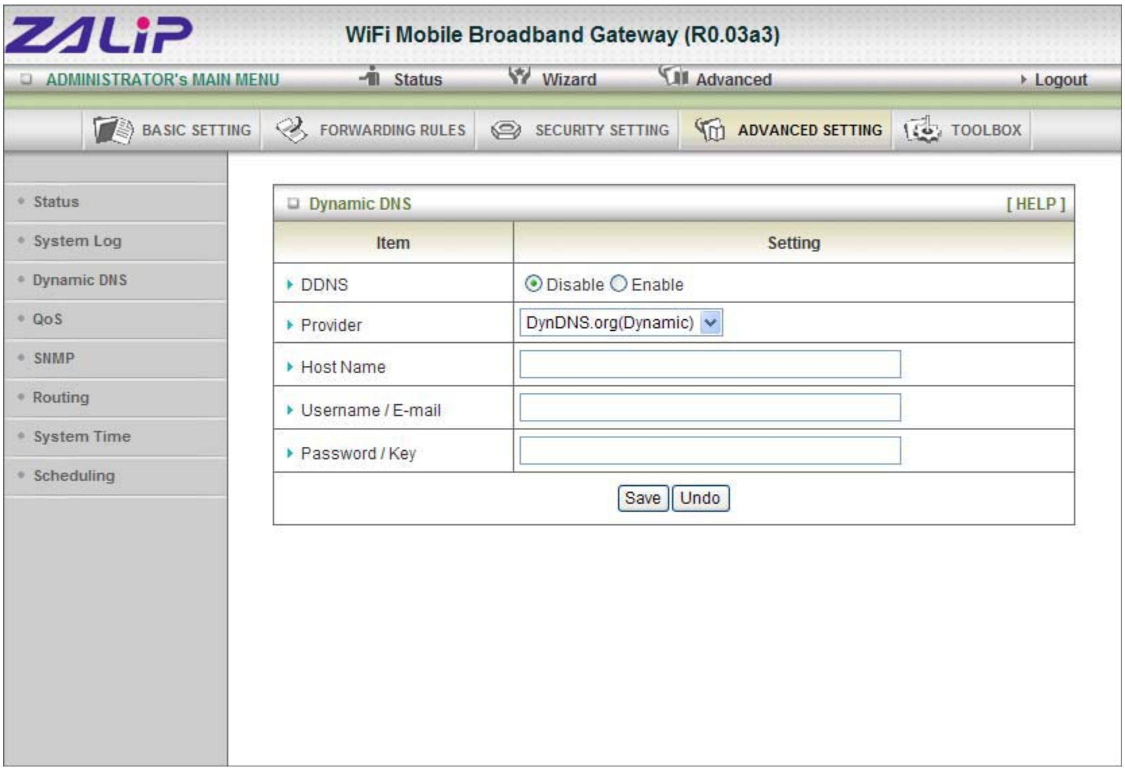
Item	Setting	Enable
IP address for syslogd		□
Setting of Email alert		□
• SMTP Server : port	:	
• SMTP Username		
• SMTP Password		
• E-mail addresses		
• E-mail subject		

This page support two methods to export system logs to specific destination by means of syslog (UDP) and SMTP(TCP). The items you have to setup including:

1. **IP Address for Sys log**
   Host IP of destination where sys log will be sent to.
   Check **Enable** to enable this function.
2. **E-mail Alert Enable**
   Check if you want to enable Email alert (send syslog via email).
3. **SMTP Server IP and Port**
   Input the SMTP server IP and port, which are connected with ':'. If you do not specify port number, the default value is 25.
   For example, "mail.your_url.com" or "192.168.1.100:26".
4. **Send E-mail alert to**
   The recipients who will receive these logs, you can assign more than 1 recipient, using ';' or ',' to separate these email addresses.
5. **E-mail Subject**
   The subject of email alert, this setting is optional.

Click on “Save” to store what you just select or “Undo” to give up

3.2.3.7 Dynamic DNS



Dynamic DNS

Item	Setting
DDNS	● Disable ○ Enable
Provider	DynDNS.org(Dynamic)
Host Name	
Username / E-mail	
Password / Key	

To host your server on a changing IP address, you have to use dynamic domain name service (DDNS).
So that anyone wishing to reach your host only needs to know the name of it. Dynamic DNS will map the name of your host to your current IP address, which changes each time you connect your Internet service provider.

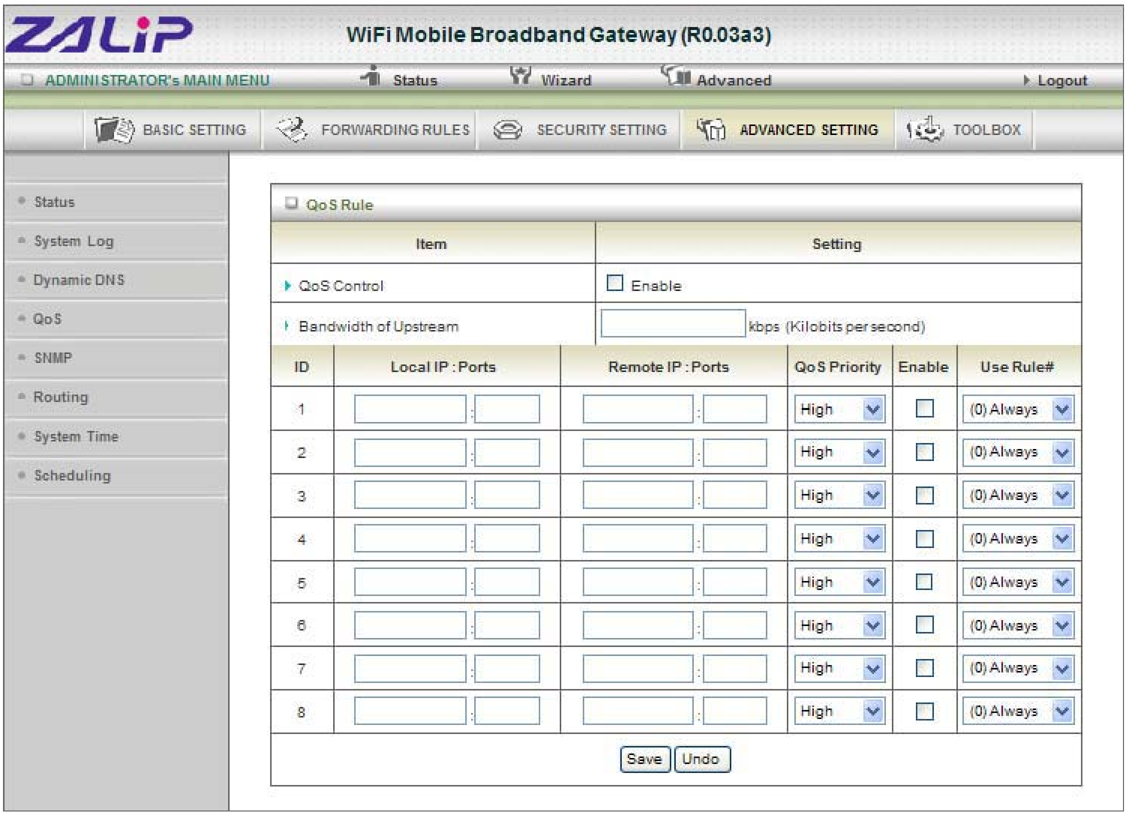
Before you enable Dynamic DNS, you need to register an account on one of these Dynamic DNS servers that we list in provider field.
To enable Dynamic DNS click the check box next to Enable in the DDNS field.
Next you can enter the appropriate information about your Dynamic DNS Server.

You have to define:
Provider
Host Name
Username/E-mail
Password/Key

You will get this information when you register an account on a Dynamic DNS server.

Click on "Save" to store what you just select or "Undo" to give up

3.2.3.8 QOS



QoS Rule

Item	Setting
QoS Control	□ Enable
Bandwidth of Upstream	kbps (Kilobits per second)

ID	Local IP : Ports	Remote IP : Ports	QoS Priority	Enable	Use Rule#
1	:	:	High	□	(0) Always
2	:	:	High	□	(0) Always
3	:	:	High	□	(0) Always
4	:	:	High	□	(0) Always
5	:	:	High	□	(0) Always
6	:	:	High	□	(0) Always
7	:	:	High	□	(0) Always
8	:	:	High	□	(0) Always

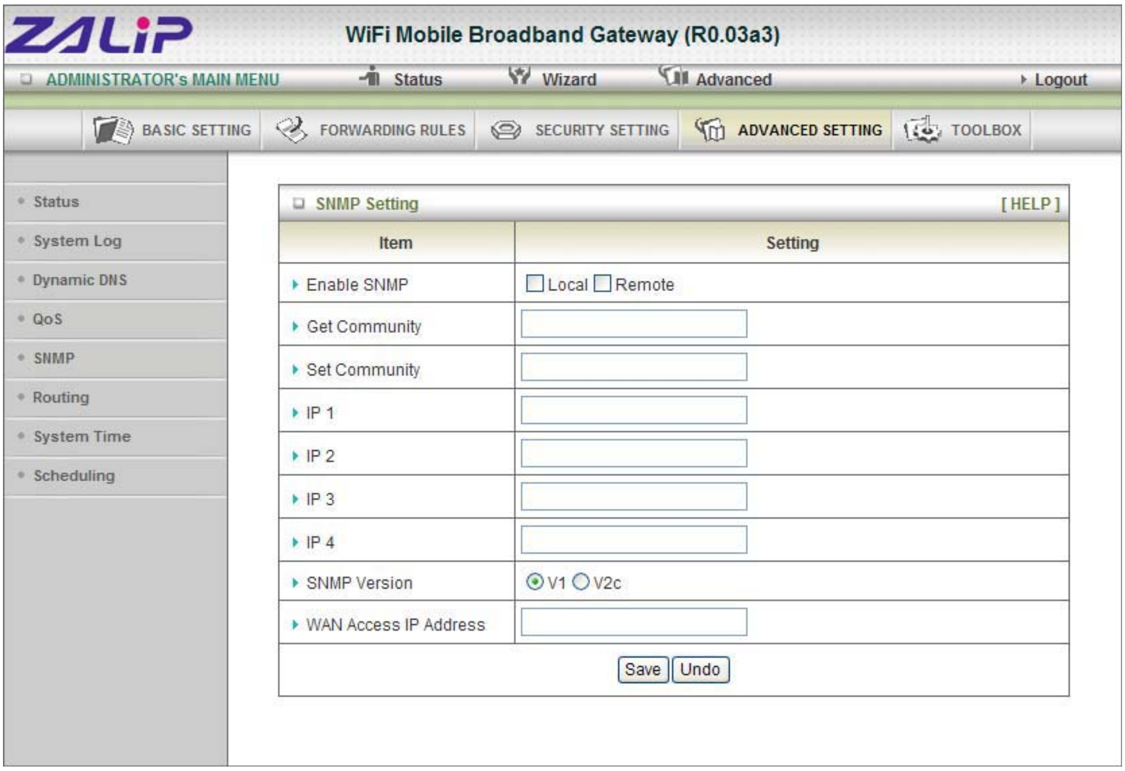
Provide different priority to different users or data flows, or guarantee a certain level of performance.

1. **Enable**
   This Item enables QoS function or not.
2. **Bandwidth of Upstream**
   Set the limitation of upstream speed.
3. **Local: IP**
   Define the Local IP address of packets here.
4. **Local: Ports**
   Define the Local port of the packets in this field.
5. **Remote: IP**
   Define the Remote IP address of packets here.
6. **Remote: Ports**
   Define the Remote port of the packets in this field.
7. **QoS Priority**
   This defines the priority level of the current Policy Configuration. Packets associated with this policy will be serviced based upon the priority level set. For critical applications High or Normal levels are recommended. For non-critical applications select a Low level.
8. **User Rule#**
   The QoS item can work with Scheduling Rule number#. Please reference the section

4.7.7 schedule.

Click on “Save” to store what you just select or “Undo” to give up

3.2.3.9 SNMP



Item	Setting
Enable SNMP	□ Local □ Remote
Get Community	
Set Community	
IP 1	
IP 2	
IP 3	
IP 4	
SNMP Version	● V1 ○ V2c
WAN Access IP Address	

In brief, SNMP, the Simple Network Management Protocol, is a protocol designed to give a user the capability to remotely manage a computer network by polling and setting terminal values and monitoring network events.

1. **Enable SNMP**

   You must check Local, Remote or both to enable SNMP function. If Local is checked, this device will response request from LAN. If Remote is checked, this device will response request from WAN.

2. **Get Community**

   Setting the community of GetRequest your device will response.

3. **Set Community**

   Setting the community of SetRequest your device will accept.

   IP 1, IP 2, IP 3, IP 4

   Input your SNMP Management PC's IP here. User has to configure to where this device should send SNMP Trap message.

4. **SNMP Version**

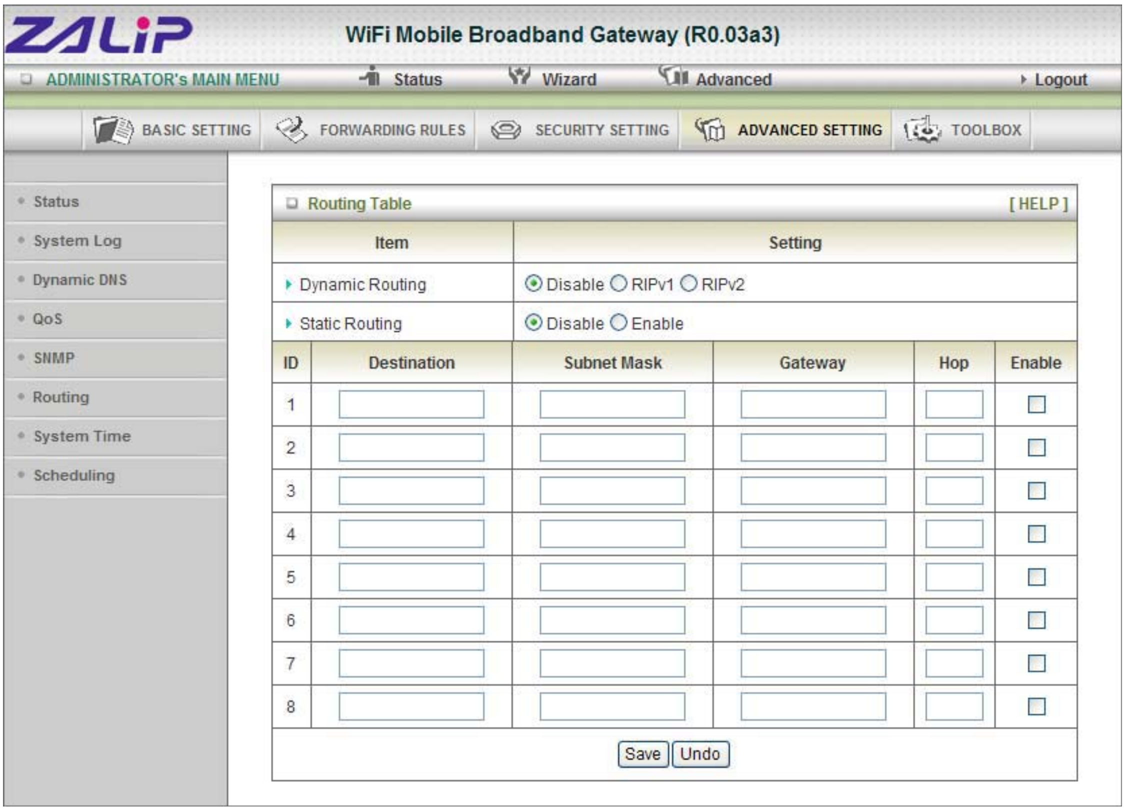
   Please select proper SNMP Version that your SNMP Management software supports.

5. **WAN Access IP Address**

   If the user wants to limit to specific the IP address to access, please input in the item. The default 0.0.0.0 and means every IP of Internet can get some information of device with SNMP protocol.

Click on "Save" to store what you just select or "Undo" to give up.

3.2.3.10 Routing



Routing Table [HELP]

Item	Setting
Dynamic Routing	● Disable ○ RIPv1 ○ RIPv2
Static Routing	● Disable ○ Enable

ID	Destination	Subnet Mask	Gateway	Hop	Enable
1					□
2					□
3					□
4					□
5					□
6					□
7					□
8					□

1. **Routing Tables**

   Allow you to determine which physical interface address to use for outgoing IP data grams. If you have more than one routers and subnets, you will need to enable routing table to allow packets to find proper routing path and allow different subnets to communicate with each other.

   Routing Table settings are settings used to setup the functions of static and dynamic routing.

2. **Dynamic Routing**

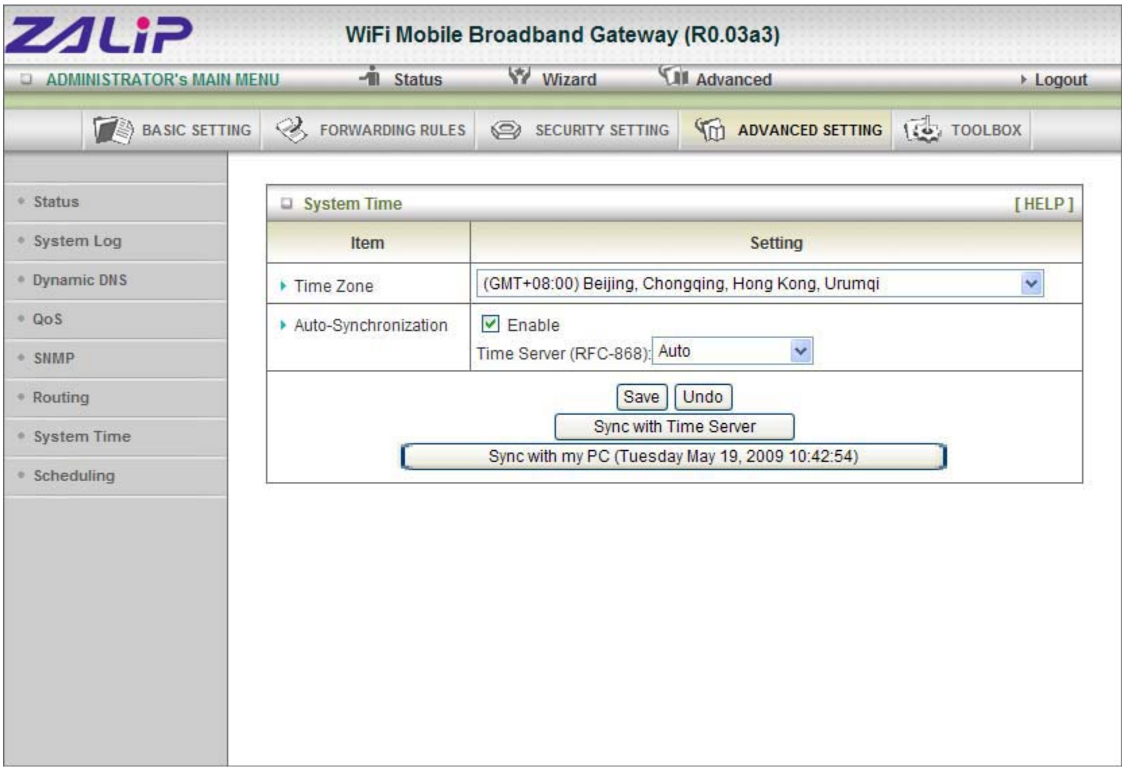
   Routing Information Protocol (RIP) will exchange information about destinations for computing routes throughout the network. Please select RIPv2 only if you have different subnet in your network. Otherwise, please select RIPv1 if you need this protocol.

3. **Static Routing**

   For static routing, you can specify up to 8 routing rules. You can enter the destination IP address, subnet mask, gateway, hop for each routing rule, and then enable or disable the rule by checking or un-checking the Enable checkbox.

Click on “Save” to store what you just select or “Undo” to give up.

3.2.3.11 System Time



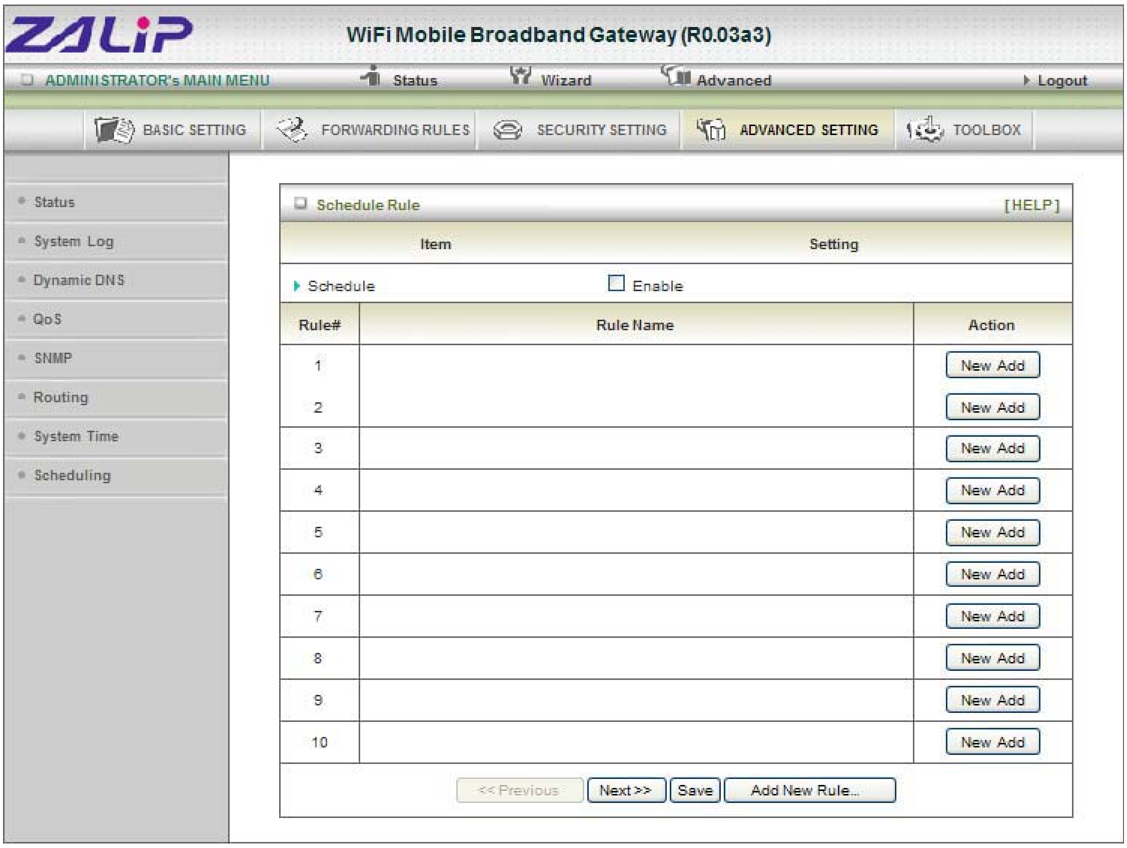
System Time

Item	Setting
Time Zone	(GMT+08:00) Beijing, Chongqing, Hong Kong, Urumqi
Auto-Synchronization	☑ Enable Time Server (RFC-868): Auto

1. **Time Zone**
   Select a time zone where this device locates.
2. **Auto-Synchronization**
   Select the “Enable” item to enable this function.
3. **Time Server**
   Select a NTP time server to consult UTC time
4. **Sync with Time Server**
   Select if you want to set Date and Time by NTP Protocol.
5. **Sync with my PC**
   Select if you want to set Date and Time using PC’s Date and Time

Click on “Save” to store what you just select or “Undo” to give up.

3.2.3.12 Scheduling

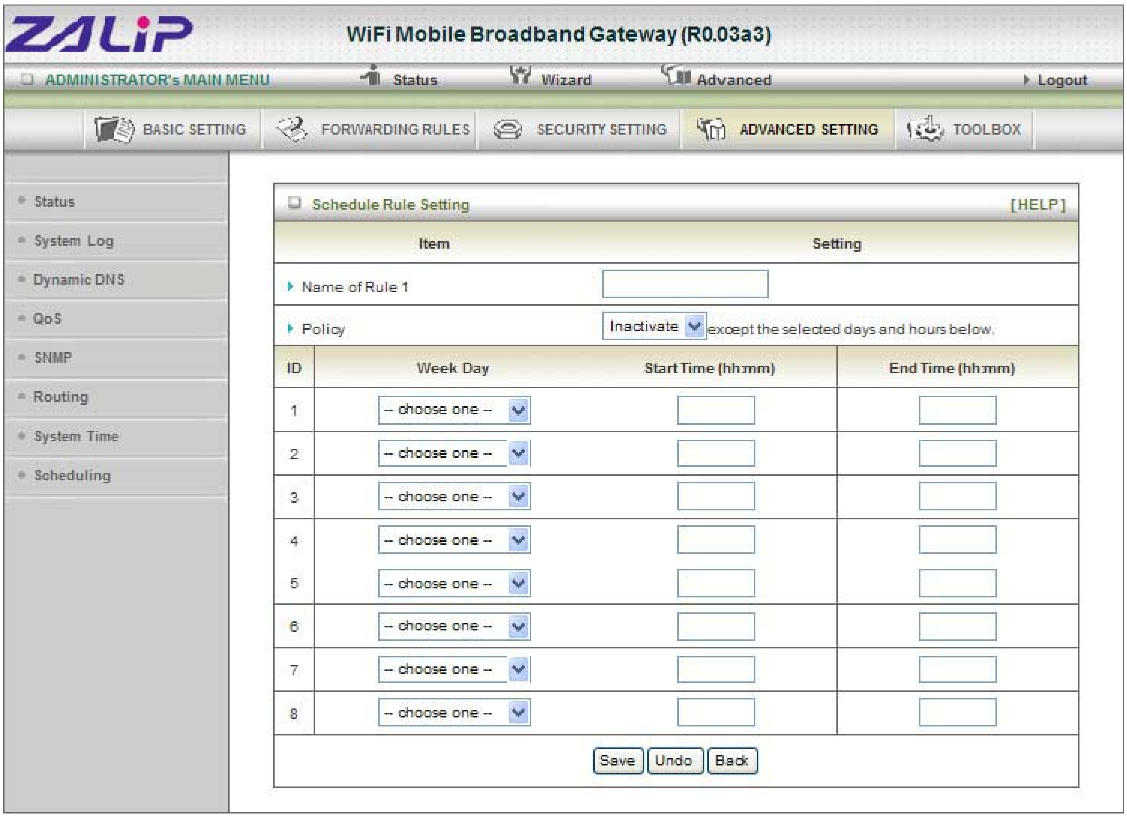


Schedule Rule [HELP]

Item	Setting
Schedule	□ Enable

Rule#	Rule Name	Action
1		New Add
2		New Add
3		New Add
4		New Add
5		New Add
6		New Add
7		New Add
8		New Add
9		New Add
10		New Add

You can set the schedule time to decide which service will be turned on or off.
Select the “Enable” item. Press “Add New Rule” You can write a rule name and set which day and what time to schedule from “Start Time” to “End Time”. The following example configure “ftp time” as everyday 14:10 to 16:20



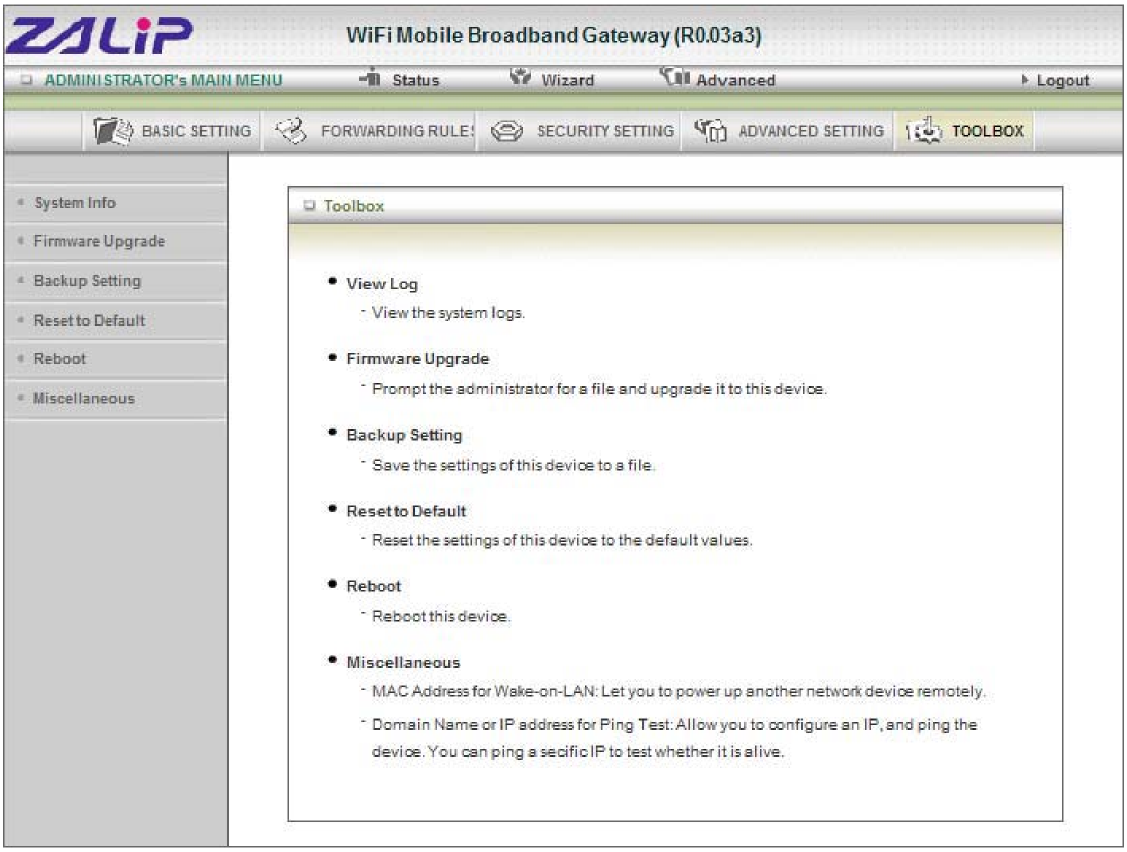
Schedule Rule Setting [HELP]

Item	Setting
Name of Rule 1	
Policy	Inactivate except the selected days and hours below.

ID	Week Day	Start Time (hh:mm)	End Time (hh:mm)
1	-- choose one --		
2	-- choose one --		
3	-- choose one --		
4	-- choose one --		
5	-- choose one --		
6	-- choose one --		
7	-- choose one --		
8	-- choose one --		

Click on “Save” to store what you just select.

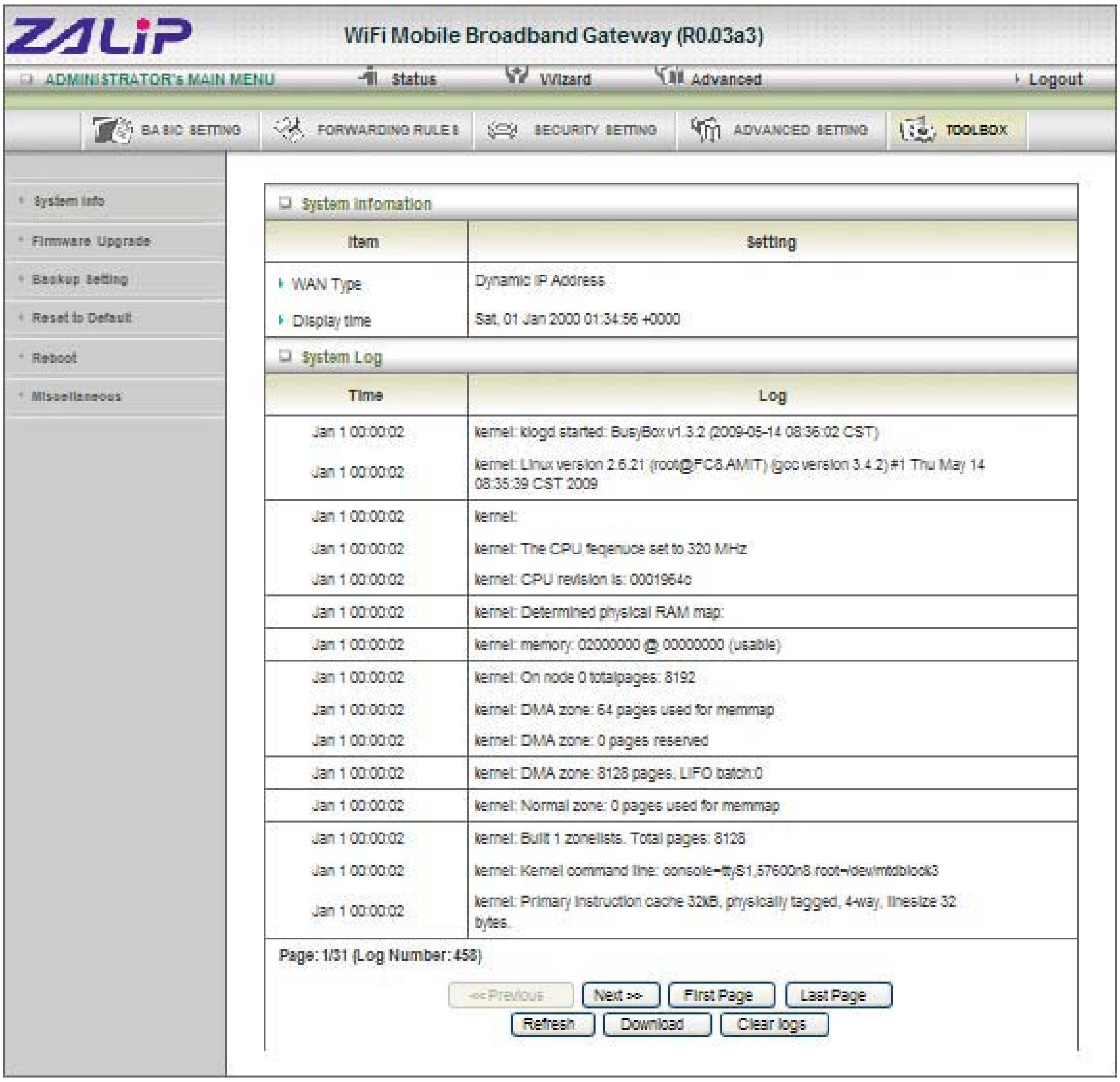
3.2.4 Tool Box



Toolbox

- View Log
  - View the system logs.
- Firmware Upgrade
  - Prompt the administrator for a file and upgrade it to this device.
- Backup Setting
  - Save the settings of this device to a file.
- Reset to Default
  - Reset the settings of this device to the default values.
- Reboot
  - Reboot this device.
- Miscellaneous
  - MAC Address for Wake-on-LAN: Let you to power up another network device remotely.
  - Domain Name or IP address for Ping Test: Allow you to configure an IP, and ping the device. You can ping a secific IP to test whether it is alive.

3.2.4.1 System Info



System Information

Item	Setting
WAN Type	Dynamic IP Address
Display time	Sat, 01 Jan 2000 01:34:56 +0000

System Log

Time	Log
Jan 1 00:00:02	kernel: klogd started: BusyBox v1.3.2 (2009-05-14 08:36:02 CST)
Jan 1 00:00:02	kernel: Linux version 2.6.21 (root@FC8.AMIT) (gcc version 3.4.2) #1 Thu May 14 08:35:39 CST 2009
Jan 1 00:00:02	kernel:
Jan 1 00:00:02	kernel: The CPU feqenuce set to 320 MHz
Jan 1 00:00:02	kernel: CPU revision is: 0001964c
Jan 1 00:00:02	kernel: Determined physical RAM map:
Jan 1 00:00:02	kernel: memory: 02000000 @ 00000000 (usable)
Jan 1 00:00:02	kernel: On node 0 totalpages: 8192
Jan 1 00:00:02	kernel: DMA zone: 64 pages used for memmap
Jan 1 00:00:02	kernel: DMA zone: 0 pages reserved
Jan 1 00:00:02	kernel: DMA zone: 8128 pages, LIFO batch:0
Jan 1 00:00:02	kernel: Normal zone: 0 pages used for memmap
Jan 1 00:00:02	kernel: Built 1 zonelists. Total pages: 8128
Jan 1 00:00:02	kernel: Kernel command line: console=ttyS1,57600n8 root=/dev/mtdblock3
Jan 1 00:00:02	kernel: Primary instruction cache 32kB, physically tagged, 4-way, linesize 32 bytes.

Page: 1/31 (Log Number: 458)

You can view the System Information and System log.
And download/clear the System log, in this page.

3.2.4.2 Firmware Upgrade

You can upgrade firmware by clicking “Upgrade” button.

3.2.4.3 Backup Setting

You can backup your settings by clicking the “**Backup Setting”** button and save it as a bin file. Once you want to restore these settings, please reference the Section 3.2.5.2 **Firmware Upgrade**.

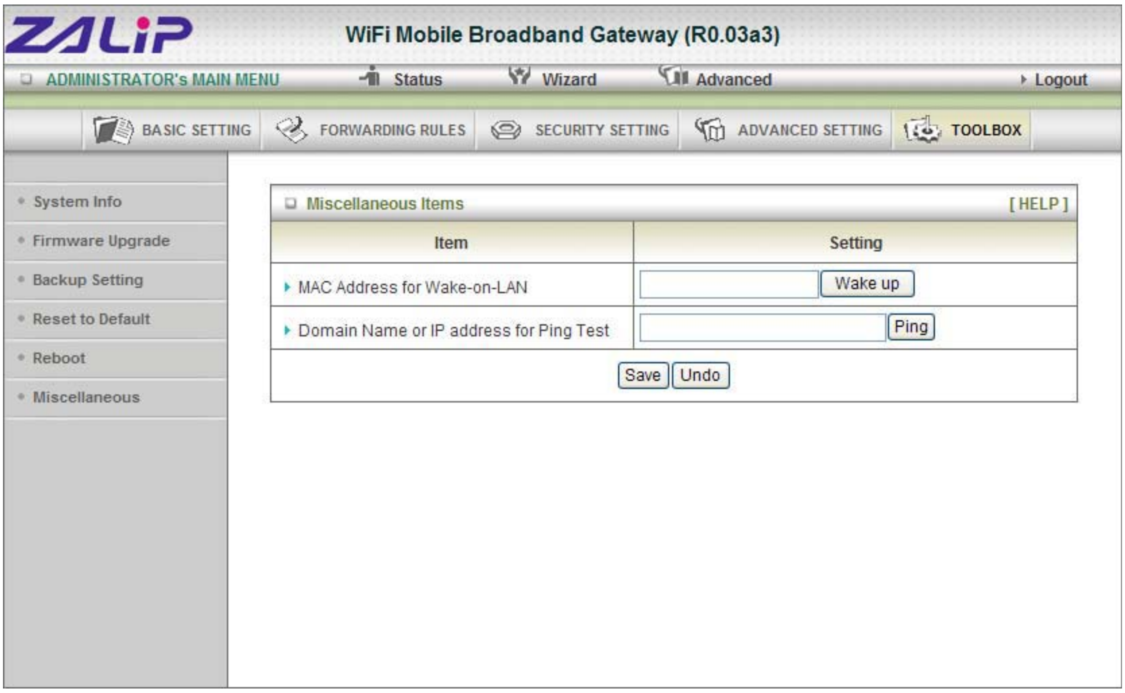
3.2.4.4 Reset to Default

You can also reset this product to factory default by clicking the **Reset to default** button.

3.2.4.5 Reboot

You can also reboot this product by clicking the **Reboot** button.

3.2.4.6 Miscellaneous



Item	Setting
MAC Address for Wake-on-LAN	Wake up
Domain Name or IP address for Ping Test	Ping

1. **MAC Address for Wake-on-LAN**

   Wake-on-LAN is a technology that enables you to power up a networked device remotely. In order to enjoy this feature, the target device must be Wake-on-LAN enabled and you have to know the MAC address of this device, say 00-11-22-33-44-55. Clicking "Wake up" button will make the router to send the wake-up frame to the target device immediately.

2. **Domain Name or IP address for Ping Test**

   You can key in URL or IP address, and then click the “Ping” button for test.

4. Troubleshooting

This section provides an overview of common issues, and possible solutions for the installation and operation of the WiFi Mobile Broadband Gateway.

1. Unable to access the Configuration Menu when I use my computer to configure the router. Why?
Note: It is recommended that you use an Ethernet connection to configure the

Ensure that the **Ethernet LED** on the WiFi Mobile Broadband Gateway is **ON**.
If the **LED** is **NOT ON**, check to see if the cable for the Ethernet connection is securely inserted.

> **Note:** Ensure that the **IP Address** is in the same range and subnet as the WiFi Mobile Broadband Gateway. The IP Address of the WiFi Mobile Broadband Gateway is 192.168.123.254. All the computers on the network must have a unique IP Address within the same range (e.g., 192.168.123.x). Any computers that have identical IP Addresses will not be visible on the network. All computers must also have the same subnet mask (e.g., 255.255.255.0).

Do a **Ping test** to make sure that the WiFi Mobile Broadband Gateway is responding.

Go to **Start > Run**.

1: Type **cmd**.
2: Press **Enter.**
3: Type "**ping 192.168.123.254".** A successful ping shows four replies.
Note: If you have changed the **default** IP Address, ensure you ping the correct IP Address assigned to the WiFi Mobile Broadband Gateway.

Ensure that your Ethernet Adapter is working properly, and that all network drivers are installed properly.

Note: Network adapter names will vary depending on your specific adapter. The installation steps listed below are applicable for all network adapters.

1. Go to **Start > My Computer > Properties**.
2. **Select** the **Hardware Tab**.
3. Click **Device Manager**.
4. Double-click on "**Network Adapters"**.
5. Right-click on **Wireless Cardbus Adapter**, or **your specific network adapter**.
6. Select **Properties** to ensure that all drivers are installed properly.
7. Look under **Device Status** to see if the device is working properly.
8. Click "**OK"**.

2**: Why my wireless client can NOT access the Internet?**
Note: Establish WiFi Connection. As long as you select either **WEP** or **WPA-PSK** encryption, ensure encryption settings match your WiFi settings. Please refer to your WiFi adapter documentation for additional information.

Ensure that the wireless client is associated and joined with the correct Access Point. To check this connection, follow the steps below:

1. **Right-click** on the **Local Area Connection icon** in the taskbar.
2. Select **View Available Wireless Networks in Wireless Configure**. The **Connect to**

Wireless Network screen appears. Ensure you have selected the correct available network.

Ensure the IP Address assigned to the wireless adapter is within the same subnet as the Access Point and gateway. The WiFi Mobile Broadband Gateway has an IP Address of **192.168.123.254.** Wireless adapters must have an IP Address in the same range (e.g., 192.168.123.x). Although the subnet mask must be the same for all the computers on

the network, no two devices may have the same IP Address. Therefore, each device must have a unique IP Address.

To check the **IP Address** assigned to the wireless adapter, follow the steps below:

1.Enter ipconfig /all in command mode

2.Enter ping 192.168.123.254.to check if you can access the WiFi Mobile Broadband Gateway

3. Why does my wireless connection keep dropping?

You may try following steps to solve.

- Antenna Orientation.
  1: Try different antenna orientations for the WiFi Mobile Broadband Gateway.
  2: Try to keep the antenna at least 6 inches away from the wall or other objects.
- Try changing the channel on the WiFi Mobile Broadband Gateway, and your Access Point and Wireless adapter to a different channel to avoid interference.
- Keep your product away (at least 3-6 feet) from electrical devices that generate RF noise, like microwaves, monitors, electric motors, etc.

4. Why I am unable to achieve a wireless connection?

Note: An Ethernet connection is required to troubleshoot the WiFi Mobile Broadband Gateway.

If you have enabled Encryption on the WiFi Mobile Broadband Gateway, you must also enable encryption on all wireless clients in order to establish a wireless connection.

- For 802.11g, the encryption settings are: 64 or 128 bit. Ensure that the encryption bit level is the same for both the WiFi Mobile Broadband Gateway, and your Wireless Client.
- Ensure that the SSID (Service Set Identifier) on the WiFi Mobile Broadband Gateway and the Wireless Client are exactly the same.
  If they are not, your wireless connection will not be established.
- Move the WiFi Mobile Broadband Gateway and the wireless client into the same room, and then test the wireless connection.
- Disable all security settings such as **WEP**, and **MAC Address Control**.
- Turn off the WiFi Mobile Broadband Gateway and the client.
  Turn the WiFi Mobile Broadband Gateway back on again, and then turn on the client.
- Ensure that all devices are set to **Infrastructure** mode.
- Ensure that the LED indicators are indicating normal activity. If not, ensure that the AC power and Ethernet cables are firmly connected.
- Ensure that the IP Address, subnet mask, gateway and DNS settings are correctly entered for the network.
- If you are using 2.4GHz cordless phones, X-10 equipment, or other home security systems, ceiling fans, or lights, your wireless connection may degrade dramatically,

or drop altogether.

To avoid interference, change the Channel on the WiFi Mobile Broadband Gateway, and all devices in your network.

- Keep your product at least 3-6 feet away from electrical devices that generate RF noise. Examples include: microwaves, monitors, electric motors, and so forth.

5. I just do not remember my encryption key. What should I do?

- If you forgot your encryption key, the WiFi card will be unable to establish a proper connection.

If an encryption key setting has been set for the WiFi Mobile Broadband Gateway, it must also be set for the WiFi card that will connect to the WiFi Mobile Broadband Gateway.

To reset the encryption key(s), login to the WiFi Mobile Broadband Gateway using a wired connection. (Please refer to “Basic > Wireless (Security–No Encryption)” on page 10, for additional information).

7. How do I reset my WiFi Mobile Broadband Gateway to its factory default settings?

If other troubleshooting methods have failed, you may choose to **Reset** the WiFi Mobile Broadband Gateway to its factory default settings.

To hard-reset the WiFi Mobile Broadband Gateway its factory **default** settings, follow the steps listed below:

1. Ensure the WiFi Mobile Broadband Gateway is powered on
2. Locate the **Reset** button on the back of the WiFi Mobile Broadband Gateway.
3. Use a paper clip to press the **Reset** button.
4. Hold for 8 seconds and then release.
5. After the WiFi Mobile Broadband Gateway reboots, it is reset to the factory **default** settings.

Note: Please note that this process will take a few minutes.

8. What is VPN?

- VPN stands for “Virtual Private Networking.” VPNs create a "tunnel" through an existing Internet connection using PPTP (Point-to-Point Tunneling Protocol) or IPSec (IP Security) protocols with various encryption schemes including Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) .
- This feature allows you to use your existing Internet connection to connect to a remote site with added security. If your VPN connection is not functional, verify that your VPN dial-up configuration is correct.

Note: This information should be provided to you from your VPN provider.
Pressing the Reset Button restores to its original factory **default** settings.

9. What can I do if my Ethernet cable does not work properly?

- First, ensure that there is a solid cable connection between the Ethernet port on the Router, and your NIC (Network Interface Card).
- Second, ensure that the settings on your NIC adapter are “Enabled,” and set to accept an IP address from the DHCP.
- If settings appear to be correct, ensure that you are *not* using a crossover Ethernet cable. Although the WiFi Mobile Broadband Gateway is MDI/MDIX compatible, not all NICs are. Therefore, it is recommended that you use a patch cable when possible.

產品規格書 Product Specifications

產品類別 **Product Type**	IEEE 802.11 B\G\N wireless router (1T1R)
產品名稱 **Product Name**	WiFi Mobile Broadband Gateway
型號 **Model Name**	CDM530AM
RF 輸出功率 **Transmit Power**	IEEE 802.11b Mode : 19.28dBm IEEE 802.11g Mode : 19.86dBm IEEE 802.11n HT20 Mode : 16.56dBm IEEE 802.11n HT40 Mode : 16.61dBm
使用頻率 **Frequency Range**	2412MHz~2462MHz for N. America (FCC) & for Canada (DOC) 2412MHz~2472MHz for Europe (Except Spain and France) (ETSI)
使用頻道數 **Channel Number**	Channel 1- Channel 11 for N. America (FCC) & for Canada (DOC) Channel 1- Channel 13 for Europe (Except Spain and France) (ETSI) Channel 1- Channel 14 for Japan (TELEC)
調變技術 **Type of Modulation**	DSSS (CCK, DQPSK, DBPSK) for 802.11b OFDM (64QAM, 16QAM, QPSK, BPSK) for 802.11g, 802.11n HT20/40
資料傳輸速率 **Transmit Data Rate**	IEEE 802.11b : 11, 5.5, 2, 1 Mbps IEEE 802.11g : 54, 48 ,36, 24, 18, 12, 9, 6 Mbps IEEE 802.11n HT20 : 65, 58.5, 52, 39, 26, 19.5, 13, 6.5 Mbps IEEE 802.11n HT40 : 135, 121.5, 108, 81, 54, 40.5, 27, 13.5 Mbps
供應電源 **Power Source**	5Vdc, 2.0A or 5Vdc, 2.5A
天線型式 **Antenna Type**	**One antenna** PIFA Antenna (× 1) Manufacture: WHA YU INDUSTRIAL CO., LTD. Model: C381-510152-A(SSR-91246) Gain: 2.9 dBi
模組 **RF Module**	RT3050

第十二條

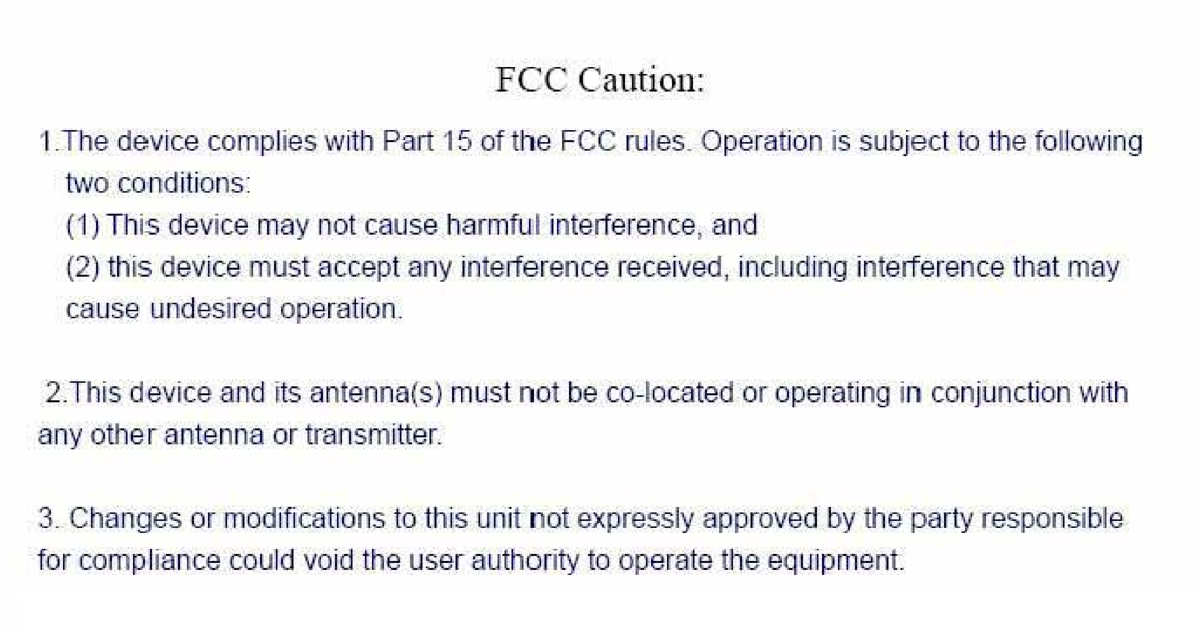
型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

第十四條

低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。

前項合法通信，指依電信法規定作業之無線電通信。

低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。



FCC Caution:

1.The device complies with Part 15 of the FCC rules. Operation is subject to the following two conditions:

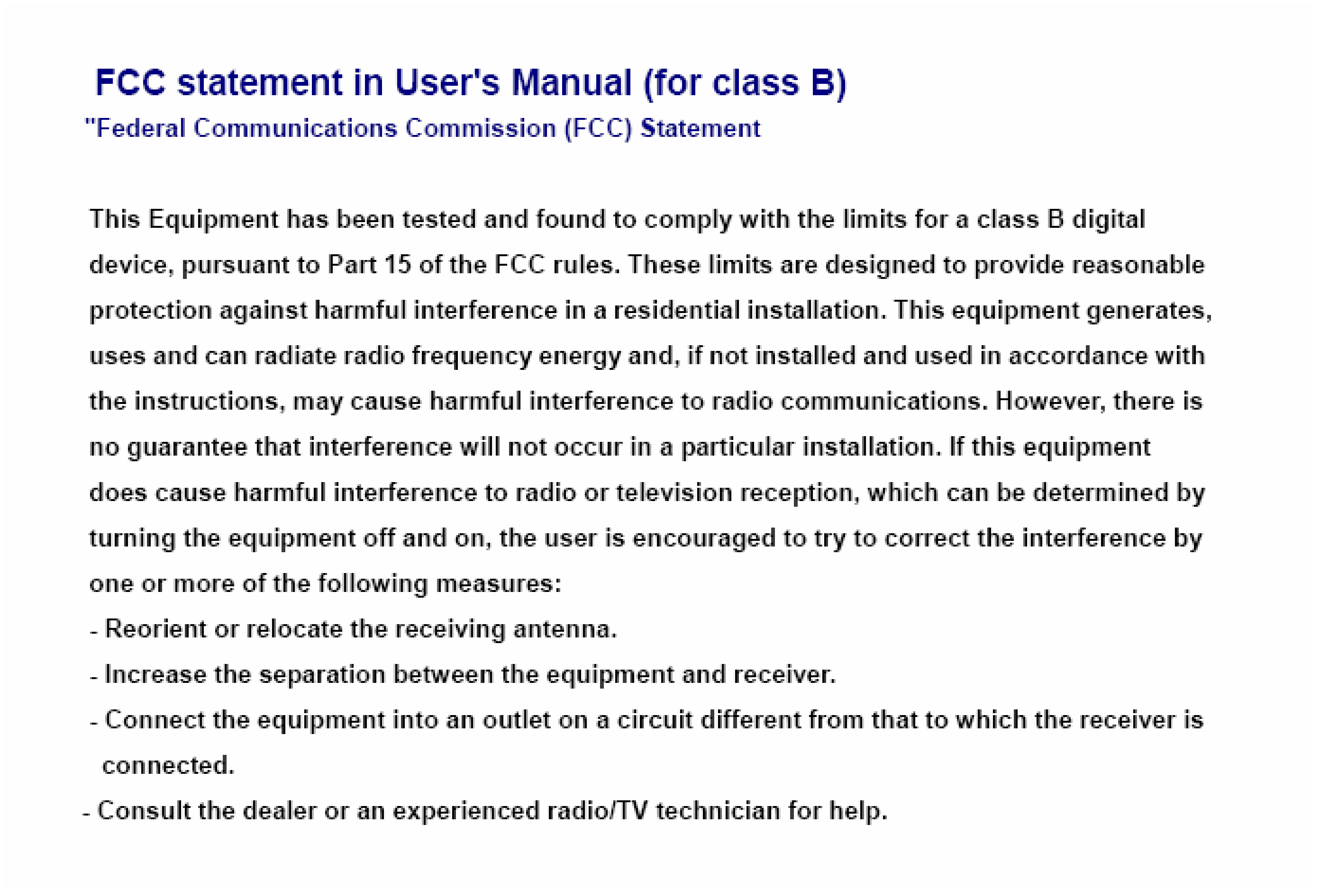
(1) This device may not cause harmful interference, and

(2) this device must accept any interference received, including interference that may cause undesired operation.

2.This device and its antenna(s) must not be co-located or operating in conjunction with any other antenna or transmitter.

3. Changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user authority to operate the equipment.

IMPORTANT NOTE:
FCC 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.



FCC statement in User's Manual (for class B)

"Federal Communications Commission (FCC) 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 or more 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.