

G2wifilll

User's Guide

Version: 1.0

Date: September 18, 2013

3JTech Co., Ltd.
2F, No. 342, Fu-Shing N. Rd.
Taipei, Taiwan
Tel: +886-2-2500 6916
e-mail: info@3jtech.com.tw

Revision History

Version	Date	Changes
1.0	09/18/2013	First Release of G2wifilll User's Manual

Table of Contents

Revision History	2
TABLE OF CONTENTS.....	3
CHAPTER 1. PRODUCT OVERVIEW.....	6
1.1 INTRODUCTION	6
1.2 FEATURES	7
1.3 PACKAGE CONTENTS	8
CHAPTER 2. PHYSICAL DESCRIPTION	9
2.1 PANELS	9
2.1.1 Front Panel.....	9
2.1.2 Rear Panel	10
2.2 ILLUSTRATION	11
2.2.1 Front Panel Information.....	12
Power Supply Connector	12
WAN Port	12
LAN Network Connectors	12
RESET Button	12
2.2.2 Rear Panel Information.....	12
LEDs	12
2.2.3 LED Description on the Rear Panel	13
CHAPTER 3. WEB-BASED MANAGEMENT.....	14
3.1. INTERNET SETTINGS	16
3.1.1 WAN	16
3.1.1.1 Static(Fixed IP) WAN Mode	17
3.1.1.2 DHCP(Auto Config) WAN Mode.....	17
3.1.1.3 PPPoE (ADSL) WAN Mode	18
3.1.2 LAN.....	19
3.1.3 DHCP Client	21
3.1.4 Advanced Routing Settings.....	22
3.2 WIRELESS SETTINGS	23
3.2.1 Basic Wireless Settings.....	23
3.2.2 Wireless Security/Encryption Settings	28
3.2.2.1 Disable Mode	28
3.2.2.2 WEPAUTO(WEP) Mode.....	29
3.2.2.3 WPA-PSK / WPA2-PSK Mode	31

3.2.3 Station List	33
3.2.4 Wireless Statistics	34
3.3 FIREWALL SETTINGS	35
3.3.1 MAC/IP/Port Filtering Settings	35
3.3.2 Port Forwarding Settings	37
3.3.2.1 Create a Port Forwarding	37
3.3.3 DMZ Settings.....	40
3.3.4 System Security Settings	41
3.4 MANAGEMENT	43
3.4.1 System Management.....	43
3.4.2 TR-069.....	45
3.4.3 Firmware Upgrade	46
3.4.4 Configuration Management.....	47
3.4.5 Status.....	48
3.4.6 Statistic.....	49

FCC STATEMENT

1. 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.
 - (2) This device must accept any interference received, including interference that may cause undesired operation.
2. Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

NOTE: 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.

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

1. Product Overview

1.1 Introduction

G2wifiIII, a WiFi Router with a WAN port, is the perfect option to connect a small group of PCs to a high-speed broadband Internet connection or to an Ethernet backbone. Configurable as a DHCP server, G2wifiIII acts as the only externally recognized Internet device on your local area network (LAN). The G2wifiIII also serves as an Internet firewall to protect your network from being accessed by outside users.



1.2 Features

- Router Mode
 - 3 WAN Modes (It includes Static(Fixed IP), DHCP(Auto Config) and PPPoE (ADSL))
 - DHCP Sever
 - NAPT (Network Address and Port Translation)
 - NAT (Network Address Translation)
- Internet Access
 - TCP/IP,UDP, ICMP, ARP, PPP, NAT, DHCP (Server), Static IP assignment
- Security Features
 - Password protected configuration access
 - User authentication (PAP/CHAP) for PPP connection
- Wireless Features
 - Support 802.11b/g, 802.11n draft 3.0 Wireless Access Point
 - Support 128-Bit and 64-Bit WEP encryption, WPA-PSK, WPA2-PSK
- Security
 - Support packet inspection and filtering
 - Intrusion detection and protection
 - Password protected system management
- Ethernet Interface
 - Compliant with IEEE 802.3 and 802.3u 10/100 Mbps
- HTTP Web-Based Management
 - Firmware upgrade by UI
 - WAN and LAN side connection statistics
 - Password protected access
 - Wireless LAN
- Support TR-069 management function

1.3 Package Contents

- 1 x G2wifiIII
- 1 x RJ45 Ethernet Cable
- 1 x Power Adapter
- 1 x CD with this User's Manual
- Quick Setup Guide

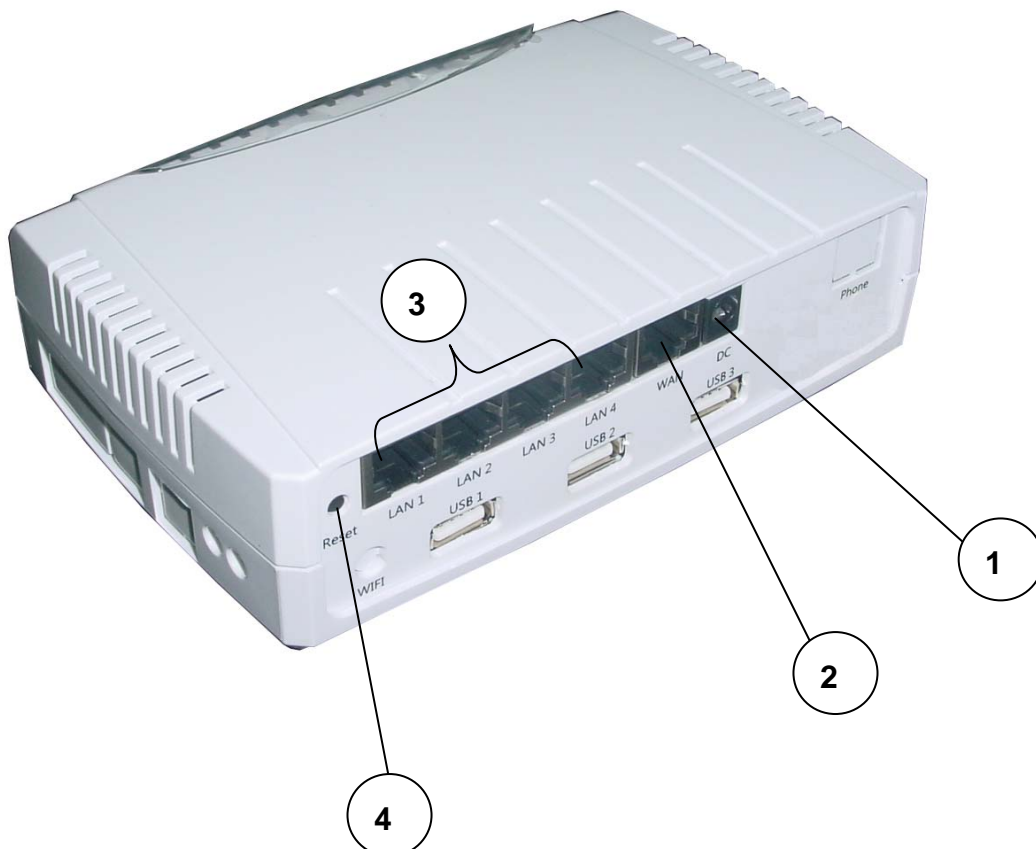
2. Physical Description

The following information contains the physical description of the G2wifiIII. This includes the functions and the locations of each connector and indicator. This information provides useful reference when installing the product. Please familiarize yourself with the G2wifiIII.

2.1 Panels

2.1.1 Front Panel

For more related description, please refer to the Section 2.2 and Section 2.2.1.



2.1.2 Rear Panel

For more detailed description, please refer to the Section 2.2 and Section 2.2.2.



2.2 Illustration

No. in Figures	Name on G2wifilll	Description	Remark
1	Power Supply Connector	To connect with the G2wifilll and the power adapter	Refer to Section 2.2.1 for front panel information
2	WAN Port	For the access of Internet	Refer to Section 2.2.1 for front panel information
3	LAN Network Connectors	To connect to the device and Ethernet port via RJ45 cable	Refer to Section 2.2.1 for front panel information
4	Reset Button	To reset the G2wifilll to its factory defaults	Refer to Section 2.2.1 for front panel information
5	LEDs	To display the status of G2wifilll	Refer to Section 2.2.2 for rear panel information and Section 2.2.3 for LED description on the rear panel

2.2.1 Front Panel Information

Power Supply Connector

Plug the power adapter. The specifications of G2wifiIII's power adapter are as follows:

- Input: 100 ~ 240V AC, 50/60Hz
- Output: 12V DC / 1.5A

WAN Port

Offer the access of Internet.

LAN Network Connectors

G2wifiIII is designed for 10/100Mbps Ethernet networks. G2wifiIII connects to the network via category 5 cable.

RESET Button

Support the hardware reset function. Press this button 2 seconds around, and the settings of the device will return to the factory defaults.

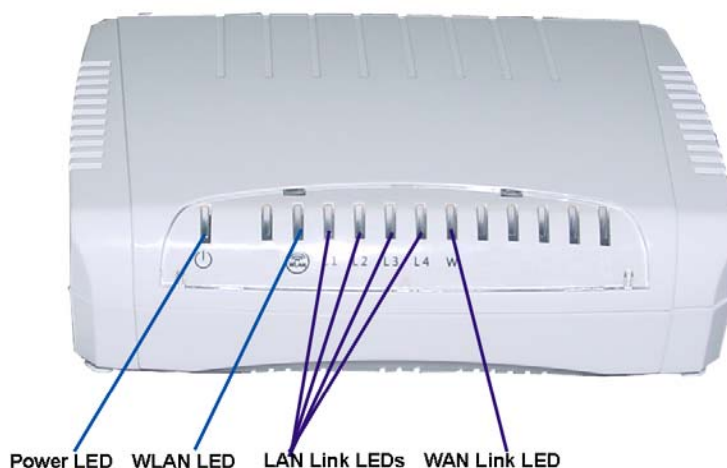
Note: Please do not power off the router while resetting it to the factory default.





2.2.2 Rear Panel Information

LEDs

Include the LEDs of POWER, WLAN (Wireless LAN), LAN Link, and WAN Link.

2.2.3 LED Description on the Rear Panel

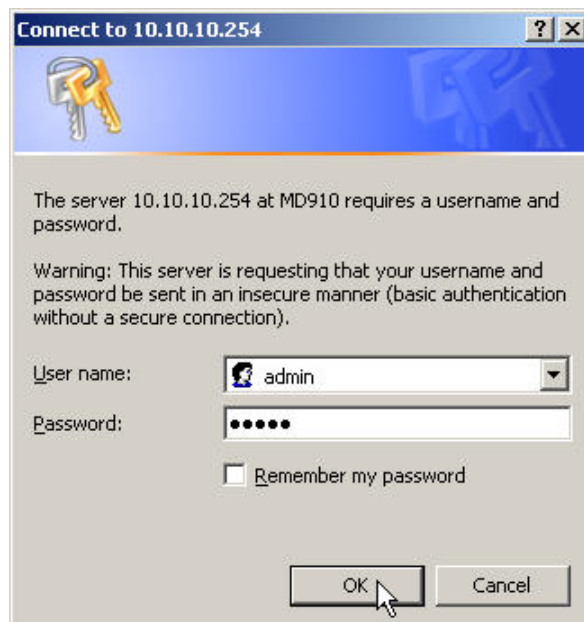


LED	Color	Status
POWER ()	Yellow	Lit when +12V DC power is on and working.
WLAN (Wireless LAN )	Yellow	Lit when the WiFi function is enabled. Flash when the data is transmitting. Off when the WiFi function is disabled.
LAN Link ()	Yellow	Lit when the cable connection with device exists. Flash when the data is transmitting. Off when no cable connection exists.
WAN Link ()	Yellow	Lit when the cable connection with device exists. Flash when the data is transmitting. Off when no cable connection exists.

3. Web-Based Management

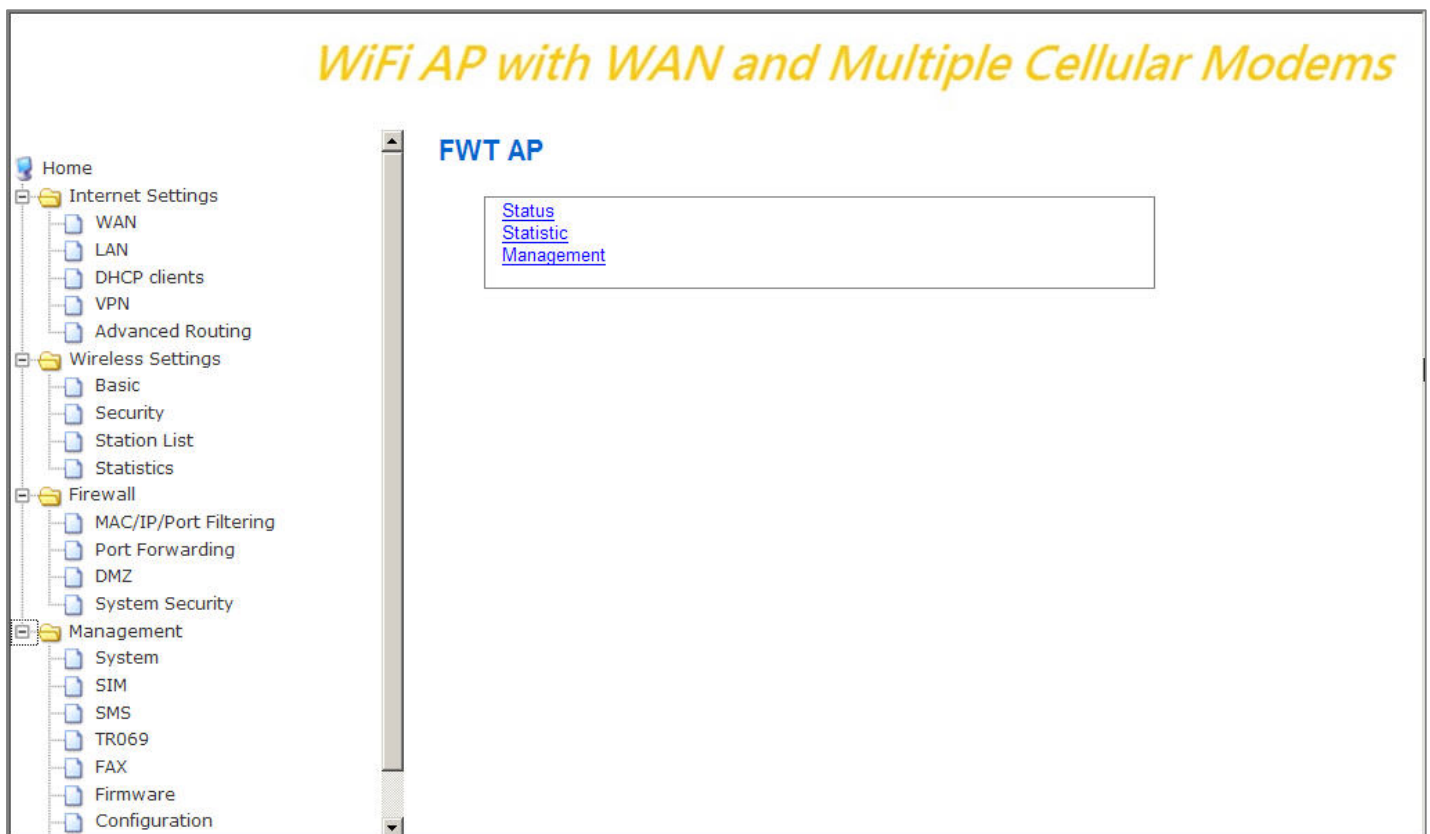
This chapter instructs you how to configure and manage the G2wifilll through the web user interface it supports. With this facility, you can easily access and monitor through the LAN port of the G2wifilll.

After the G2wifilll has been connected to your PC via RJ45 network cable, type <http://10.10.10.254> in IE browser, it will show the following screen and ask you to input the user name and password in order to login and access authentication. The default user name and the password are both “**admin**”. For the first time to use, please enter this default user name and the password, then click the **OK** button. The root setup page for G2wifilll will be displayed once the login process is successful. The user will be able to fully access and configure the system.



In the G2wifiIII, it supports a simple user management function to configure the system. As the figure below shows, for example, left section is the whole function tree with web user interface while each of main functions, including INTERNET SETTINGS, WIRELESS SETTINGS, FIREWALL, and MANAGEMENT is selected.

By means of the hyperlink of Status, Statistic or Management in this root setup page, you can directly jump to the related pages if you would like to realize the basic information of the system.



3.1. Internet Settings

3.1.1 WAN

The WAN (Wide Area Network) section is where you configure your Internet connection type. There are three WAN connection modes to choose from: Static (Fixed IP), DHCP(Auto Config) and PPPoE(ADSL). If you are unsure of your connection method, please contact your Internet Service Provider before configuring the required parameters. Note: If using the PPPoE option, you will need to ensure that any PPPoE client software on your computers is removed or disabled.

Wide Area Network (WAN) Settings

WAN Connection Type:

DHCP (Auto config)

STATIC (fixed IP)

DHCP (Auto config)

PPPoE (ADSL)

DHCP Mode

Hostname (optional)

3G Mode

APN

Internet

Dial Number

*99#

Username

user

Pasword

password

Auth Mode

Auto

Connection Type

3G + 2G(3G Preferred)

3G Mode:1

APN

Internet

Dial Number

*99#

3G Mode:2

APN

Internet

Dial Number

*99#

3G Mode:3

APN

Internet

Dail Number

*99#

Username

user

Password

password

Auth Mode

Auto

Connection Type

3G+2G(3G Preferred)

WAN Weight

WAN1 (Ether Cable)

1

WAN2 (3G Internal)

1

WAN3 (3G USB1)

1

WAN4 (3G USB2)

1

WAN5 (3G USB3)

1

Apply

Cancel

3.1.1.1 Static(Fixed IP) WAN Mode

Used when your ISP provides you a set IP address that does not change. The IP information is manually entered in your IP configuration settings. You must enter the **IP address**, **Subnet Mask**, **Default Gateway**, **Primary DNS Server**, and **Secondary DNS Server**. Your ISP provides you with all of this information.

WAN Connection Type:		STATIC (fixed IP) ▼
Static Mode		
IP Address	<input type="text"/>	
Subnet Mask	<input type="text"/>	
Default Gateway	<input type="text"/>	
Primary DNS Server	<input type="text"/>	
Secondary DNS Server	<input type="text"/>	

3.1.1.2 DHCP(Auto Config) WAN Mode

A method of connection where the ISP assigns your IP address when your router requests one from the ISP's server. Some ISP's require you to make some settings on your side before your router can connect to the Internet.

WAN Connection Type:		DHCP (Auto config) ▼
DHCP Mode		
Hostname (optional)	<input type="text"/>	

Hostname: Some ISP's may check your computer's hostname. The hostname identifies your system to the ISP's server. This way they know your computer is eligible to receive an IP address. In other words, they know that you are paying for their service.

3.1.1.3 PPPoE (ADSL) WAN Mode

Select this option if your ISP requires you to use a PPPoE (Point to Point Protocol over Ethernet) connection. DSL providers typically use this option. This method of connection requires you to enter a **User Name** and **Password** (provided by your Internet Service Provider) to gain access to the Internet.

WAN Connection Type:		PPPoE (ADSL) ▼
PPPoE Mode		
User Name	<input type="text"/>	
Password	<input type="password"/>	
Verify Password	<input type="password"/>	
Operation Mode	Keep Alive ▼	
	Keep Alive Mode: Redial Period <input type="text" value="60"/> seconds	

Operation Mode: Typically, connections are not always on. The router allows you to set the reconnection mode. The setting is:

- **Keep Alive:** A connection to the Internet is always maintained. When this option is selected, please enter a value in the field of **Redial Period** which is the time interval the machine will be redialed before the PPPoE connection is disconnected.

3.1.2 LAN

These are the settings of the LAN (Local Area Network) interface for the AP. The AP's local network (LAN) settings are configured based on the IP Address and Subnet Mask assigned in this section. The IP address is also used to access this web-based management interface. It is recommended that you use the default settings if you do not have an existing network.

Local Area Network (LAN) Settings	
You may enable/disable networking functions and configure their parameters as your wish.	
LAN Setup	
IP Address	10.10.10.254
Subnet Mask	255.255.255.0
MAC Address	00:0A:EB:38:B8:85
DHCP Type	Server
Start IP Address	10.10.10.100
End IP Address	10.10.10.200
Subnet Mask	255.255.255.0
Primary DNS Server	168.95.1.1
Secondary DNS Server	8.8.8.8
Lease Time	86400
Statically Assigned	MAC: <input type="text"/> IP: <input type="text"/>
Statically Assigned	MAC: <input type="text"/> IP: <input type="text"/>
Statically Assigned	MAC: <input type="text"/> IP: <input type="text"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

IP Address: The IP address of your router's LAN port. Default: 10.10.10.254.

Subnet Mask: Subnet Mask of your LAN (default: 255.255.255.0). All devices on the network must have the same subnet mask to communicate on the network.

DHCP Type: DHCP stands for Dynamic Host Configuration Protocol. The DHCP section is where you configure the built-in DHCP Server to assign IP addresses to the computers and other devices on your local area network (LAN). When you select **Server** item from this pull-down list to enable this function, the following parameters will be displayed. You must enter the IP address, Subnet Mask, Primary DNS Server and/or Secondary DNS Server.

Start IP Address: Specify the DHCP Client IP address that will start.

End IP Address: Specify the DHCP Client IP address that will end.

Note: The number of the “End IP” must be greater than “Start IP”, and cannot be the same as the router’s IP address.

DHCP Lease Time: Designate the amount of the time for the device to recycle and give out the IP addresses to the devices in your network (default: 86400).

Statically Assigned: You can statically assign the client MAC and IP address. Up to three IPs and MACs can be assigned.

3.1.3 DHCP Client

In this section, you can see clearly which devices are currently leasing IP addresses that you had defined for the DHCP Server's allocation of addresses to computers and devices on your Local Area Network.

DHCP Client List			
DHCP Clients			
Hostname	MAC Address	IP Address	Expires in
iris	00:0C:6E:AB:9B:E6	10.10.10.100	17:21:11

Host Name: A name for each computer or device that is given an IP address by the DHCP Server. This may help you keep track of which computers are assigned this way.

MAC Address: A MAC address is usually located on a sticker at the bottom of a network device. The MAC address is comprised of twelve digits. Each pair of hexadecimal digits are usually separated by dashes or colons such as 00-0D-88-11-22-33 or 00:0D:88:11:22:33.

IP Address: The address which is obtained from the DHCP Server.

Expires in: The remaining time of the IP address's lease. A specific LAN device no longer needs the leased IP address when the time ends up, and this device will also free the IP address it had leased.

3.1.4 Advanced Routing Settings

In Static Routing Settings, the user can set up a route rule (table) here. Refer to the description of the following parameters to set up the necessary route rule, and click the **Apply** button when you complete.

Add a routing rule

Destination

Range

Host

Gateway

Interface

LAN

Comment

Apply

Reset

Current Routing table in the system:

No.	Destination	Netmask	Gateway	Flags	Metric	Ref	Use	Interface	Comment
1	255.255.255.255	255.255.255.255	0.0.0.0	5	0	0	0	LAN (br0)	
2	10.10.10.0	255.255.255.0	0.0.0.0	1	0	0	0	LAN (br0)	

Delete

Reset

Destination: The IP address of packets that will take this route.

Range: Includes **Host** and **Net** options. When selecting “Net”, there is another “Netmask” column that needs to be filled out.

Netmask: The bits in the mask specify which bits of the IP address must match.

Gateway: The gateway for the routing.

Interface: Specifies the interface -- **LAN** or **WAN** -- that the IP packet must use to transit out of the router when this route is used. Or you can choose the user-defined way by selecting the **Custom** option.

Comment: Memo for the routing rule.

Routing Table: Lists the current route rules you have added before. Click on the **Delete** button to delete the selected route rule.

3.2 Wireless Settings

The wireless section is used to configure the wireless settings for your router. Please note that changes made on this section may also need to be duplicated on your wireless client.

To protect your privacy, use the wireless security mode to configure the wireless security features. This device supports three wireless security modes including: WEP(WEPAUTO), WPA-PSK, and WPA2-PSK. WEP is the original wireless encryption standard. WPA provides a higher level of security. In WPA encryption, it supports TKIP or AES of WPA-PSK/WPA2-PSK.

3.2.1 Basic Wireless Settings

Through the basic wireless setting page, the user can control the ON/OFF status of WiFi function, and set up the 802.11 mode, Network Name (SSID) as well as Channel. Besides, you can do the further settings related to the HT Physical Mode.

Basic Wireless Settings	
You could configure the minimum number of Wireless settings for communication, such as Network Name (SSID) and Channel. The Access Point can be set simply with only the minimum setting items.	
Wireless Network	
WiFi On/Off	WiFi OFF
Network Mode	11b/g/n mixed mode
Network Name(SSID)	default Hidden <input type="checkbox"/>
Multiple SSID1	<input type="text"/> Hidden <input type="checkbox"/>
Multiple SSID2	<input type="text"/> Hidden <input type="checkbox"/>
Multiple SSID3	<input type="text"/> Hidden <input type="checkbox"/>
Broadcast Network Name (SSID)	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
AP Isolation	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
MBSSID AP Isolation	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Frequency (Channel)	2437MHz (Channel 6)

HT Physical Mode	
Operating Mode	<input checked="" type="radio"/> Mixed Mode <input type="radio"/> Green Field
Channel BandWidth	<input type="radio"/> 20 <input checked="" type="radio"/> 20/40
Guard Interval	<input type="radio"/> Long <input checked="" type="radio"/> Auto
MCS	Auto
Reverse Direction Grant(RDG)	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Extension Channel	2457MHz (Channel 10)
Aggregation MSDU(A-MSDU)	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
Auto Block ACK	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Decline BA Request	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
<div>Apply Cancel</div>	

Wireless Network Settings:

WiFi On/Off: This option turns on and off the wireless connection feature of the router. Simply click on the **WiFi ON / WiFi OFF** button. The system will automatically detect the current status of the router and switch the button accordingly.

Network Mode: There are 5 modes including, 802.11b/g mixed mode, 802.11b only, 802.11g only, 802.11/b/g/n mixed mode, and 802.11n only(2.4G) can be chosen.

Network Name(SSID): When you are browsing for available wireless networks, this is the name that will appear in the list (unless you set it to Hidden, see below). This name is also referred to as the SSID. For security purposes, it is highly recommended to change from the pre-configured network name. Default is "default".

Hidden: The option allows you to hide your wireless network. When this option is unchecked, your wireless network name is broadcast to anyone within the range of your signal. If you're not using encryption then they could connect to your network. When you click on this checkbox to enable this function, you must enter the Wireless Network Name (SSID) on the client manually to connect to the network.

Multiple SSID 1 ~ 3: Up to three SSIDs you can additionally set up for this wireless network.

Broadcast Network Name (SSID): Enable/Disable the SSID broadcast function. This function is used to control the broadcast status of all SSIDs. If this function is disabled, all SSIDs you had set up for the router will be hidden. To cancel the hidden status for the specific SSID, you can uncheck the “Hidden” option in the back of your desired SSID.

AP Isolation: Enable/Disable this function. Create a separate virtual network for your wireless network. When this feature is enabled, each of your wireless clients will be in its own virtual network and will not be able to communicate with each other. You may want to utilize this feature if you have many guests that frequent your wireless network.

MBSSID AP Isolation: Enable/Disable the MBSSID AP Isolation function. The router supports multiple SSIDs. You can decide whether the clients associated to different SSIDs on the device can see each other or not. Enable the option to block it. Default is “Disable”.

Frequency (Channel): A wireless network uses specific channels in the 2.4GHz wireless spectrum to handle communication between clients. Some channels in your area may have interference from other electronic devices. Choose the clearest channel to help optimize the performance and coverage of your wireless network. If you select **AutoSelect**, the router automatically finds the channel with least interference and uses that channel for wireless networking.

Rate: Exist only when selecting 802.11b/g mixed mode, 802.11b only, 802.11g only as the Network Mode for the router. You can set up the desired transmitting rate for these network modes. Default is Auto.

HT Physical Mode Settings: This mode settings exist only when 802.11b/g/n mixed mode or 802.11n only(2.4G) is chosen as your router's Network Mode.

Operating Mode: Select the option to enable the Mixed Mode or the Green Field Mode for physical layer transceivers. Default: Mixed Mode.

Mixed mode: In this mode the device transmits the packets with preamble compatible legacy (802.11g), so they can be decoded by legacy devices. The device receives and decodes both Mixed Mode packets and legacy packets.

Green Field mode: The device transmits HT packets without legacy compatible part. But the device receives and decodes both Green Field and legacy packets.

Channel BandWidth: This option only works when selecting Network mode in 11b/g/n mixed mode and 11n mode. Select the option to choose 20 MHz or 20/40MHz. This option affects the Phy data rate of radio. Please refer to the table below, which shows the relationship among Phy data rate, Bandwidth and Guard Interval.

Guard Interval: The 11n device inserts the Guard Interval into the signal. You can choose the interval between "Long" and "Auto". This option affects the Phy data rate of radio. For more details, please refer to the table below.

MCS: It means "Modulation Coding Scheme". The available options are "Auto, 0, 1, ...15, and 32". It changes the modulation of this device and effect the maximum Phy data rate. We recommend "Auto" setting. For more details, please refer to the table below.

The table below shows the relationship among Phy data rate, Bandwidth and Guard Interval.

Data Rate Mbps MCS	Bandwidth = 20MHz		Bandwidth = 40MHz	
	Short Guard Interval	Long Guard Interval	Short Guard Interval	Long Guard Interval
0 (1S)	7.2	6.5	15	13.5
1	14.4	13	30	27
2	21.7	19.5	45	40.5
3	28.9	26	60	54
4	43.3	39	90	81
5	57.8	52	120	108
6	65	58.5	135	121.5
7	72.2	65	150	135
8 (2S)	14.4	13	30	27
9	28.9	26	60	54
10	43.3	39	90	81
11	57.8	52	120	108
12	86.7	78	180	162
13	115.6	104	240	216
14	130	117	270	243
15	144.4	130	300	270
32	Not Supported	Not Supported	6.7	6

MCS: Modulation Coding Scheme
MCS=0~7 (1S, One Tx Stream)
MCS=8~15 (2S, Two Tx Stream)
MCS 32: BPSK

Reverse Direction Grant(RDG): This is the 11n performance parameter. Enable it if needed.

Extension Channel: Exist only when selecting “20/40” as the Channel BandWidth for the router. For example, if channel 6 is selected, it means you can select channel 2 or channel 10 as the extension channel. Choose the unused channel as the extension channel.

Aggregation MSDU(A-MSDU): The multiple HT packets can be transmitted with single ACK reply packet. Enable it to apply this function and reduce the network congestion.

Auto Block ACK: It is another aggregation technique which prevents sending ACK in the communication to increase the throughput. If this option is enabled, the device will activate this function when transmitting massive data.

Decline BA Request: Enable this option to decline the Block ACK request addressed by the other devices.

3.2.2 Wireless Security/Encryption Settings

In this section, you can configure the wireless security and encryption to prevent from unauthorized access and monitoring. Please choose a SSID you had created for this router in the *Wireless Settings* → *Basic* setting page from the **SSID Choice** pull-down list.

There are 4 encryption modes, including **Disable**, **WEPAUTO(WEP)**, **WPA-PSK** and **WPA2-PSK** offered for your selection. Please also pull down the **Security Mode** list and select the desired mode for your router's wireless security. For more details about the setup in these different modes, please refer to the following sections.

3.2.2.1 Disable Mode

In this mode, wireless clients can directly connect to the router without inputting any key.

Wireless Security/Encryption Settings

Setup the wireless security and encryption to prevent from unauthorized access and monitoring.

Select SSID

SSID choice FWT AP ▼

"FWT AP"

Security Mode Disable ▼

Apply Cancel

3.2.2.2 WEPAUTO(WEP) Mode

WEP is a method of encrypting data for wireless communication intended to provide the same level of privacy as a wired network. WEP is not as secure as WPA encryption. To gain access to a WEP network, you must know the key. The key is a string of characters that you create. When using WEP, you must determine the level of encryption. The type of encryption determines the key length. 128-bit encryption requires a longer key than 64-bit encryption. Keys are defined by entering in a string in HEX (hexadecimal - using characters 0-9, A-F(a-f)) or ASCII (American Standard Code for Information Interchange - alphanumeric characters) format. ASCII format is provided so you can enter a string that is easier to remember. The ASCII string is converted to HEX for use over the network.

Example,

64-bit hexadecimal keys are exactly 10 characters in length. (12345678FA is a valid string of 10 characters for 64-bit encryption.)

128-bit hexadecimal keys are exactly 26 characters in length.
(456FBCDF12340012225271730 is a valid string of 26 characters for 128-bit encryption.)

64-bit ASCII keys are up to 5 characters in length (DMODE is a valid string of 5 characters for 64-bit encryption.)

128-bit ASCII keys are up to 13 characters in length (2002HALOSWIN1 is a valid string of 13 characters for 128-bit encryption.)

Wireless Security/Encryption Settings

Setup the wireless security and encryption to prevent from unauthorized access and monitoring.

Select SSID

SSID choice: FWT AP

"FWT AP"

Security Mode: WEPAUTO

Wire Equivalence Protection (WEP)

WEP Keys: [Empty text box]

Key Format: Hex (selected), ASCII, Hex

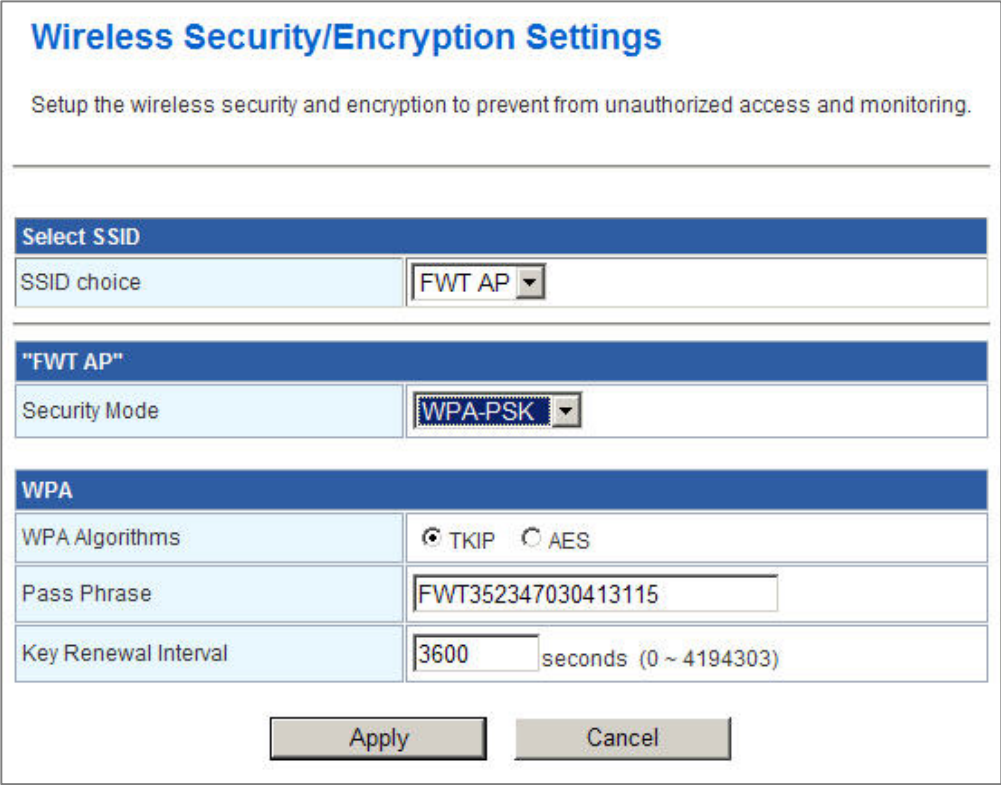
Apply Cancel

WEP Keys: Select “ASCII” or “Hex” from the pull-down list to set up the key value. ASCII (American Standard Code for Information Interchange) is a code for representing char as numbers from 0-127. Hexadecimal digits consist of the numbers 0-9 and the letters A-F (a-f).

3.2.2.3 WPA-PSK / WPA2-PSK Mode

WPA (Wi-Fi Protected Access) is the older standard; select this option if the clients that will be used with the router only support the older standard. WPA2 is the newer implementation of the stronger IEEE 802.11i security standard.

PSK(Pre-Shared Key) is the key which is entered as a pass-phrase of up to 63 alphanumeric characters in ASCII (American Standard Code for Information Interchange) format or 64 digits in HEX format at both ends of the wireless connection. When inputting ASCII strings, it cannot be shorter than eight characters, although for proper security it needs to be of ample length and should not be a commonly known phrase. This phrase is used to generate session keys that are unique for each wireless client.



The image shows a web-based configuration interface titled "Wireless Security/Encryption Settings". Below the title is a subtitle: "Setup the wireless security and encryption to prevent from unauthorized access and monitoring." The form is divided into three main sections: "Select SSID", "'FWT AP'", and "WPA".

- Select SSID:** Contains a label "SSID choice" and a dropdown menu currently showing "FWT AP".
- "FWT AP":** Contains a label "Security Mode" and a dropdown menu currently showing "WPA-PSK".
- WPA:** Contains three fields:
 - WPA Algorithms:** Two radio buttons, "TKIP" (which is selected) and "AES".
 - Pass Phrase:** A text input field containing the value "FWT352347030413115".
 - Key Renewal Interval:** A text input field containing "3600" followed by the text "seconds (0 ~ 4194303)".

At the bottom of the form are two buttons: "Apply" and "Cancel".

WPA Algorithms: Mark the option to enable modes of TKIP or AES.

Pass Phrase: This mode requires only an access point and client station that supports WPA-PSK. The WPA-PSK settings include Key Format, Length and Value. They must be as same as each wireless client in your wireless network. When Key format is Passphrase, the key value should have 8-63 ASCII characters or 64 digits in HEX format.

Key Renewal Interval: Enter a value to set up the WPA key renewal interval. The device regenerates the key in every interval seconds that you have setup without disconnection. The WPA Algorithm will regroup the key for a period. The default value is 3600 seconds, and you can adjust the time interval (Valid Range: 0 ~ 4194303).

3.2.3 Station List

From the list of Station, you can see which devices are currently connecting to your G2wifiIII in the wireless way through the MAC address. You also can have a clear realization of status, including Aid, PSM, MimoPS, MCS, BW(Bandwidth), SGI and STBC for each Wifi connection.

Station List							
You could monitor stations which associated to this AP here.							
Wireless Network							
MAC Address	Aid	PSM	MimoPS	MCS	BW	SGI	STBC
74:2F:68:90:35:F4	1	0	0	7	20M	0	0

3.2.4 Wireless Statistics

The G2wifiIII offers the counter function to collect all wireless traffic counting information about the transmitting/ receiving packets of this router. The system will automatically update these wireless data per 3 seconds. To restart the counting, please click on the **Reset Counters** button.

AP Wireless Statistics	
Wireless TX and RX statistics	
Transmit Statistics	
Tx Success	54
Tx Retry Count	0, PER=0.0%
Tx Fail after retry	0, PLR=0.0e+00
RTS Successfully Receive CTS	0
RTS Fail To Receive CTS	0
Receive Statistics	
Frames Received Successfully	313760
Frames Received With CRC Error	243, PER=0.1%
SNR	
SNR	n/a, n/a, n/a
Reset Counters	

Tx Success: Display the transmitted number of the successful packets.

Tx Retry Count: Display the transmitted number of the retry packets.

Tx Fail after retry: Display the transmitted number of the unsuccessful packets after retry.

RTS Successfully Receive CTS: Display the transmitted number of RTS(Request To Send) packets which receive CTS(Clear To Send) packets successfully.

RTS Fail To Receive CTS: Display the transmitted number of RTS(Request To Send) packets which receive CTS(Clear To Send) packets unsuccessfully.

Frames Received Successfully: Display the received number of the successful frames.

Frames Received With CRC Error: Display the received number of frames with CRC error packets.

SNR: Signal-to-Noise ratio (SNR). It stands that how fast wireless data of the router can travel and how far a wireless signal of the router can reach.

3.3 FireWall Settings

3.3.1 MAC/IP/Port Filtering Settings

The router could filter the outgoing packets for security or management consideration. You can set up the filter against the IP addresses to block specific internal users from accessing the Internet. The firewall could not only obstruct outside intruders from intruding your system, but also restricting the LAN users. Port filter restricts certain type of data packets from your LAN to Internet through the router.

MAC/IP/Port Filtering Settings
You may setup firewall rules to protect your network from virus, worm and malicious activity on the Internet.

Basic Settings

MAC/IP/Port Filtering

Default Policy -- The packet that doesn't match with any rules must be:

MAC/IP/Port Filter Settings

Source MAC address

Dest IP Address

Source IP Address

Protocol

Dest Port Range

-

Source Port Range

-

Action

Comment

(The maximum rule count is 32.)

Current MAC/IP/Port filtering rules in system:

No.	Source MAC address	Dest IP Address	Source IP Address	Protocol	Dest Port Range	Source Port Range	Action	Comment	Pkt Cnt
Packets dropped that don't match with any rules above									-

Basic Settings:

MAC/IP/Port Filtering: Enable/Disable the function of MAC/IP/Port Filtering.

Default Policy - The packet that doesn't match with any rules must be: Dropped/Accepted.
For example, if you select "Dropped", all packets that do not match the rule you set up in the following **MAC/IP/Port FilteringSettings** would be dropped.

MAC/IP/Port Filtering Settings:

Source MAC address: Fill out the MAC address that you wish to filter.

Dest IP Address: Fill in the destination IP address that you wish to filter.

Source IP Address: Fill in the source IP address that you wish to filter.

Protocol: Select the protocol type of TCP, UDP or ICMP.

Dest Port Range: Fill in the destination port range that you wish to filter.

Source Port Range: Fill in the source port range that you wish to filter.

Action: You can either choose "Accept" or "Drop" to permit or prevent the action.

Comment: Input any text to describe this mapping, up to 16 alphanumerical characters.

IP/Port Filter Rule List: Lists the IP / Port Filter Settings you have added before. Click on the **Delete Selected** button to delete the selected list.

3.3.2 Port Forwarding Settings

This function offers the way of Port Forwarding / Virtual Server in order to help redirect requests from computers on the LAN to a server set up on the LAN. You can set up an Internet service on the computer on local network, without exposing it on Internet directly. You can also build many sets of port redirection, to provide many different Internet services on different local computers via a single Internet IP address.

3.3.2.1 Create a Port Forwarding

In this section, you can add a new port forwarding to the port forwarding table below or delete an existing entry from this table.

Port Forwarding				
Port Forwarding	Enable ▾			
IP Address	<input type="text"/>			
Port Range	<input type="text"/> - <input type="text"/>			
Protocol	TCP&UDP ▾			
Comment	<input type="text"/>			
(The maximum rule count is 32.)				
<input type="button" value="Apply"/> <input type="button" value="Reset"/>				
Current Port Forwarding in system:				
No.	IP Address	Port Range	Protocol	Comment
1 <input type="checkbox"/>	10.10.10.10	100 - 111	TCP + UDP	
<input type="button" value="Delete Selected"/> <input type="button" value="Reset"/>				

Port Forwarding: Enable/Disable the function of Port Forwarding.

IP Address: Fill in the IP address of your LAN Server.

Port Range: Fill in the port range that you wish to filter.

Protocol: Select the protocol type, including TCP, UDP or TCP&UDP used by the service.

Comment: Input any text to describe this mapping. Up to 16 alphanumeric characters can be filled in.

Port Forwarding Mapping List: After completing the above settings, please click on the **Apply** button. The entry of Port Forwarding you had added will be listed on this table if it is created successfully. Clicking on the **Delete Selected** button will remove the existing entry you select from this table.

3.3.2.2 Create a Virtual Server

In this section, you can add a new virtual server to the virtual server table below or delete an existing entry from this table.

The Virtual Server option gives Internet users access to services on your LAN. This feature is useful for hosting online services such as FTP, Web, or game servers. For each Virtual Server, you define a public port on your router for redirection to an internal LAN IP Address and LAN port. For Example,

You are hosting a Web Server on a PC that has LAN IP Address of 10.10.10.50 and your ISP is blocking Port 80.

1. Enter the IP Address of the machine on your LAN (for example: **10.10.10.50**)
2. Enter the Public Port as [8888]
3. Enter the Private Port as [80]
4. Select the Protocol - TCP
5. Click the **Apply** button to add the settings to the Virtual Server Table
6. Repeat these steps for each Virtual Server Rule you wish to add. With this Virtual Server entry, all Internet traffic on Port 8888 will be redirected to your internal web server on port 80 at IP Address 10.10.10.50.

Virtual Server					
Virtual Server	Enable <input type="button" value="v"/>				
IP Address	<input type="text"/>				
Public Port	<input type="text"/>				
Private Port	<input type="text"/>				
Protocol	TCP&UDP <input type="button" value="v"/>				
Comment	<input type="text"/>				
(The maximum rule count is 32.)					
<input type="button" value="Apply"/> <input type="button" value="Reset"/>					
Current Virtual Servers in system:					
No.	IP Address	Public Port	Private Port	Protocol	Comment
1 <input type="checkbox"/>	10.10.10.50	8888	80	TCP	Web
<input type="button" value="Delete Selected"/> <input type="button" value="Reset"/>					

Virtual Server: Enable/Disable the function of Virtual Server.

IP Address: The IP address of the system on your internal network that will provide the virtual service, for example, **10.10.10.50**.

Public Port: The port that will be accessed from the Internet.

Private Port: The port that will be used on your internal network.

Protocol: Select the protocol type, including TCP, UDP or TCP&UDP used by the service.

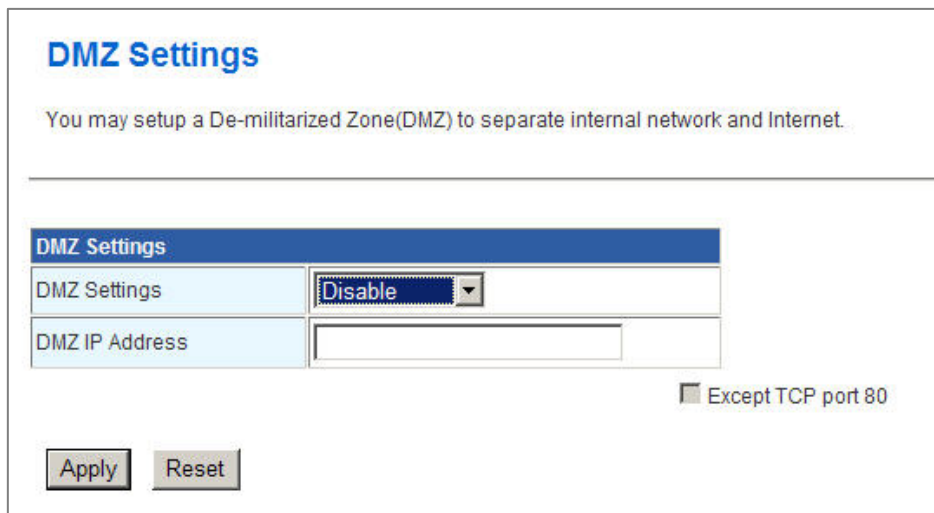
Comment: Input any text to describe this mapping. Up to 16 alphanumerical characters can be filled in.

Virtual Server Mapping List: After completing the above settings, please click on the **Apply** button. The entry of Virtual Server you had added will be listed on this table if it is created successfully. Clicking on the **Delete Selected** button will remove the existing entry you select from this table.

3.3.3 DMZ Settings

The DMZ (Demilitarized Zone) is used to enable protocols, which needs to open ports on the router. The router will forward all unspecified incoming traffic to the host specified in this setting page. To configure it, mark to enable virtual DMZ and then enter the Host IP (private IP address) and click the **Apply** button to enact the setting.

Note: Putting a computer in the DMZ may expose that computer to a variety of security risks. Use of this option is only recommended as a last resort.



DMZ Settings: Enable/Disable the function of DMZ.

DMZ IP Address: Specify the IP address of the computer on the LAN that you want to have unrestricted Internet communication. If this computer obtains its address automatically using DHCP, then you may want to make a static reservation in the field of **Statically Assigned** on the *Internet Settings* → *LAN* setting page so that the IP address of the DMZ machine does not change.

Except TCP port 80: If you click on the checkbox in front of **Except TCP port 80** function, it means that TCP port 80 cannot be used for DMZ; otherwise, you can use this port for DMZ.

3.3.4 System Security Settings

To improve the safety of the internal network environment, G2wifiIII offers a variety of basic firewall management functions, including Remote management (via WAN), Ping from WAN Filter, Block port scan, Block SYN Flood and SPI Firewall. By the configuration the following system security settings, you can protect the router itself from being attacked, scanned or intruded.

System Security Settings	
You may configure the system firewall to protect AP/Router from unauthorized access.	
Remote management	
Remote management (via WAN)	Deny
Ping from WAN Filter	
Ping from WAN Filter	Disable
Block Port Scan	
Block port scan	Disable
Block SYN Flood	
Block SYN Flood	Disable
Stateful Packet Inspection (SPI)	
SPI Firewall	Disable
<input type="button" value="Apply"/> <input type="button" value="Reset"/>	

Remote management (via WAN): Allow or Not Allow the user to log in the system with the WAN IP.

Ping from WAN Filter: Enable/Disable the function of Ping from WAN Filter. If the function is enabled, the system will reject to response the ICMP(ping) packets coming from the WAN.

Block port scan: Enable/Disable the function of Block port scan. The port scan actions will be dropped if you enable this function.

Block SYN Flood: Block TCP SYN Flood or not. If this function is enabled, it can prevent the system from being attacked by a large amount of SYN packets.

SPI Firewall: SPI ("stateful packet inspection" also known as "dynamic packet filtering") helps to prevent cyberattacks by tracking more state per session. It validates that the traffic passing through that session conforms to the protocol.

3.4 Management

3.4.1 System Management

You may configure language, administrator's account and password, and NTP settings here.

Language Settings	
Select Language	English
<div>Apply Cancel</div>	

Administrator Settings	
Account	admin
Password	•••••
<div>Apply Cancel</div>	

NTP Settings	
Current Time	Sat Jan 1 01:28:47 UTC 2000
Time Zone:	(GMT-11:00) Midway Island, Samoa
NTP Server	<div>ex: time.nist.gov ntp0.broad.mit.edu gps.ntp.br</div>
NTP synchronization	<div>hours</div>
<div>Apply Cancel</div>	

Language Settings: Select the language which you would like. Currently, only English is included.

Administrator Settings: Modify the account and password to set up and manage the G2wifiIII. The default settings for administrator are as follows:

Username: admin

Password: admin

NTP Settings: Set up the system time by syncing from the NTP server.

Current Time: Show the system time of the router. Its format: day of week, month, day, hours : minutes : seconds, year. For instance, Wed, Aug. 29, 12:10:10, 2012.

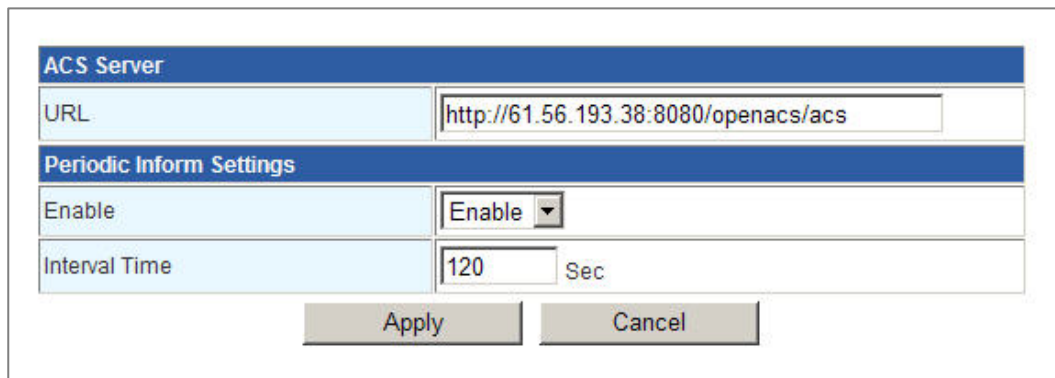
Time Zone: It is an offset time off GMT. You have to select the time zone first and then perform time sync via NTP because the router will combine this time zone offset and updated NTP time to come out the local time, otherwise, you will not able to get the correct time. The router supports configurable time zone from -11 to +12 step 1 hour. Default Time zone: -11 Hrs.

NTP Sever: NTP is Network Time Protocol and is used to sync the network time based Greenwich Mean Time (GMT). If you manually specify an IP address of user-defined NTP server as well as Time Zone, the router will sync the time immediately after pressing the **Apply** button.

NTP Synchronization: Though it synchronizes the time automatically, NTP does not update the time periodically without user's processing. You can set up the time interval (Valid range: 1 ~ 300 hours) to have the assigned NTP server do the synchronization of time for your router.

3.4.2 TR-069

Due to the built-in TR-069 function, G2wifilll will allow the administrator to remotely do the firmware upgrade, system configuration, management, troubleshooting via the Auto-Configuration Server (ACS) in the method of HTTP Internet network connection. ACS is a TR-069_based automatic configuration server, implementing CPE WAN Management Protocol (CWMP). For more details on the ACS, please refer to our ACS Administrator's User Manual.



ACS Server	
URL	<input type="text" value="http://61.56.193.38:8080/openacs/acs"/>
Periodic Inform Settings	
Enable	<input type="button" value="Enable"/>
Interval Time	<input type="text" value="120"/> Sec
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

URL of ACS Server: For G2wifilll's access of TR-069 service from ACS through the web browser, please fill in the path in which the ACS is built. For example, <http://61.56.193.38:8080/openacs/acs>)

Enable: Activate/Deactivate G2wifilll's TR-069 functionality.

Interval Time of Periodic Inform Settings: Enter a value to set up or change the Periodic Inform Interval of the G2wifilll. Upon this time interval you had set up, G2wifilll will communicate with ACS periodically and automatically. Please note that the value of **Periodic Inform Interval Time** must be more than 30 seconds, and the maximum of this Interval Time can be 4294967295 in seconds.

3.4.3 Firmware Upgrade

Software upgrade tool is used to help upgrade the software function in order to fix or improve the function. User can upgrade the firmware in this page. Please note that power cannot be off in the process of the software upgrade. You must do it carefully.

Specify the filename and directory where the file is located via the **Browse...** button, and click on the **Apply** button when it is completed. When the upload is finished, the router will start upgrading software. A reboot message will be prompted after completing upgrading software. At this time, you must reboot the router to have the new software worked.

If your upload is unsuccessful, an error message will be shown in the webpage, and it will not upgrade the software as well.

For G2wifiIII's NVRAM value update, you should press the **Reset** button (more than 2 seconds) when the device is on and have it restart. And then power off the router and power on for its normal working.

Upgrade Firmware

Upgrade the FWT AP firmware to obtain new functionality. The update process takes approximately 1 minute. Wait for the program to complete the update.

Upload Firmware

Location:

Location: File path and filename stored the image file you would like to upgrade.

3.4.4 Configuration Management

With this function, user can back up or reload the config files by exporting/ importing settings.

Besides through the press of the **RESET** button in the front panel to execute the hardware reset function as we had mentioned in Section 2.2.1 for the router. The software reset function provided here takes the same effect as the **RESET** button on the front panel of the router. It will take about 30~60 seconds to complete the system boot.

The screenshot shows a web interface titled "Settings Management". Below the title is a descriptive text: "You might save system settings by exporting them to a configuration file, restore them by importing the file, or reset them to factory default." The interface is divided into three main sections: "Export", "Import", and "Factory Defaults". The "Export" section has a link "Click here to export current configuration" and an "Export" button. The "Import" section has a text input field "Locate import file", a "Browse..." button, and "Import" and "Cancel" buttons. The "Factory Defaults" section has a link "Click here to load factory defaults" and a "Load Default" button.

Export: To export the current settings stored in the flash to a config file, just press the **Export** button.

Import: Import the config file into your router. Specify the filename and directory where the file is located via the **Browse...** button, and press the **Import** button when completed.

Factory Defaults: Restoring the unit to the factory default settings will erase all settings, including any rules that you had created. To have the router's settings be returned to the factory default, just press the **Load Default** button. Please note that the router cannot be powered off while resetting to the factory default.

3.4.5 Status

In the Status page, it tells you the basic information of the system. You can check the device status, including the firmware version, system up time, WAN/Local IP address, MAC address and so on. They will be refreshed per 3 seconds. With these information, it is helpful while malfunctioning.

Device Status	
System Info	
Firmware Version	10.0.2.5
System Up Time	3 mins, 22 secs
Operation Mode	Gateway Mode
Internet Configurations	
WAN IP Address	192.168.100.58
Subnet Mask	255.255.255.0
Default Gateway	192.168.100.1
Primary Domain Name Server	168.95.1.1
Secondary Domain Name Server	168.95.1.1

3.4.6 Statistic

G2wifiIII offers the counter function to collect all counting information about the memory status and all interfaces' receiving/transmitting packets of this router.

Statistic	
Memory	
Memory total:	28572 kB
Memory left:	10780 kB
All interfaces	
Name	ra0
Rx Packet	7143
Rx Byte	1083841
Tx Packet	66
Tx Byte	0
Name	eth2.2
Rx Packet	0
Rx Byte	0
Tx Packet	22
Tx Byte	2146
Name	br0
Rx Packet	324
Rx Byte	22871
Tx Packet	144
Tx Byte	86510