

Welltech

Wi-Fi VoIP Gateway

(WellGate 3512)

Technical Manual



Revision information		
Version	Date	Description
EN-V1.00	Jul-19-2007	1 st English version

TABLE OF CONTENT

CHAPTER 1 OVERVIEW OF THE WG3512	5
Front View	8
Back View	9
Specification of connector	9
Call Features	10
Direct IP Call	10
Proxy Call	10
Call Waiting	10
Three-way Conference	10
Call Transfer (Blind Transfer)	10
CHAPTER 2 CONFIGURING THE WG3512 THROUGH VOICE PROMPT AND PHONE SET	12
CHAPTER 3 CONFIGURING THE WG3512 THROUGH WEB PAGES	14
Step 1. Power on the WG3512	14
Step 2. Check the LEDs	14
Step 3. Connect PC with one of LAN port	14
Step 4. Browse the Default IP Address of WG3512 and enter the web interface main screen	14
Step 5. Start to configure	15
Setup Wizard	16
Operation Mode:	16
Time Zone Setting	17
LAN Interface Setup	18
WAN Interface Setup	18
Wireless Basic Settings	20
Wireless Security Setup	21

Operation Mode	24
Wireless	25
Basic Settings	25
Advanced Setting	26
Security	28
Access Control	30
WDS Settings	30
Site Survey	31
TCP/IP Settings	31
LAN Interface	31
WAN Interface	32
Firewall	36
Port Filtering	36
IP Filtering	36
MAC Filtering	37
URL Filtering	38
Port Forwarding	38
DMZ	39
VoIP Settings	39
Port1	39
Port 2	39
Tone	45
Ring	46
PSTN	47
Other	47
Config	48
Management	49
Status	49
Statistics	50
DDNS	50
Time Zone Setting	51
Denial-of-Service	52
Log	52
Upgrade Firmware	53
Save/Reload Settings	54

Password	54
System Reboot	55
CHAPTER 4 WIRELESS OPERATION MODES	56
Access Point	56
Access point with NAT	56
Access point With Bridge mode (Without NAT)	57
Client (Infrastructure)	58
Client (Ad-hoc)	59
P2P Bridge	60
WDS Repeater	61
Universal Repeater	63
WISP	64
WISP + Universal Repeater	65

Chapter 1 Overview of the WG3512

WellGate 3512 is a two-port FXS + one PSTN wireless gateway, which supports RFC3261 SIP protocol. Telephone will switch to PSTN port automatically under power failure. User can also select to dial out through PSTN line manually. WG-3512 complies with wireless protocol 802.11 b/g, and can operate as Access Point or Client. Built-in four LAN ports and NAT function allows other devices to access network more easily.

Benefits

- **Easy access to IP from phone set or PBX**
- **Cost Saving - Telephone call from VPN or public Internet**
- **Follows the existing telephone call dial plan**
- **Easy interface to ADSL/Cable Modem or Leased line equipment**
- **Easy to integrate with all kinds of IP-PBXs**

Physical interface

- **RJ-45**
 - WAN X 1 for connecting to HUB or ATU-R directly
 - LAN X 4 for PC or other devices
- **RJ-11**
 - Phone X 2 for regular phone connection
 - PSTN X 1 for Dialing and Receiving PSTN call.
- **Power: Input AC 100V~240V Output DC12V**
- **LED Indicator: Power, WLAN, WAN, LAN, FXS, PSTN**

Voice Feature

- **Codec: G.711u/A-Law, G.729A , G.726, GSM-FR**
- **VAD/CNG**
- **Adaptive Jitter Buffer**
- **Line Echo Canceller**
- **FAX/Modem tone detection and pass through**
- **DTMF: Inband, RFC-2833, SIP Info**

Network

- **Auto MDI/MDI-X**
- **802.11 b/g Access Point, WiFi compliant**
 - 802.1x, WEP, WPA TKIP and WPA2 AES/Mixed
 - mode for PSK and TLS (Radius)
 - 802.11f (IAPP)
 - Wireless Auto-channel selection
 - Wireless access control by MAC address (deny or accept)

- 802.11b/g client mode
- WISP Mode
- WDS and Universal Repeater Mode
- 802.1d with spanning tree protocol
- NAT/NAPT
- Firewall
- Virtual DMZ
- ALG for:FTP, SIP, VPN pass-through with multiple sessions (IPSEC, L2TP)
- DHCP client and server
- Up to 98MB throughput at Bridge Mode
- Qos: 802.1Q (VLAN)
- Bandwidth Control
- PPPoE
- UPnP IGD
- STUN
- DDNS and NTP client
- QOS - DSCP class0-7 and EF
- URL Filtering and DoS (Deny of Service)
- DNS relay

Telephony Features

- Caller ID: TypeI/II DTMF, FSK
- Flash Hook Timer Configuration
- Gain Adjustments
- PSTN Bypass: Power Failure, Manually
- Call Waiting
- Call Hold
- Blind Transfer
- Call Forward
- 3-way Conference
- 10 Speed Dials
- T.38 FAX

Dimension

- 17.5 x 12.5 x 3.2 cm

Protocol

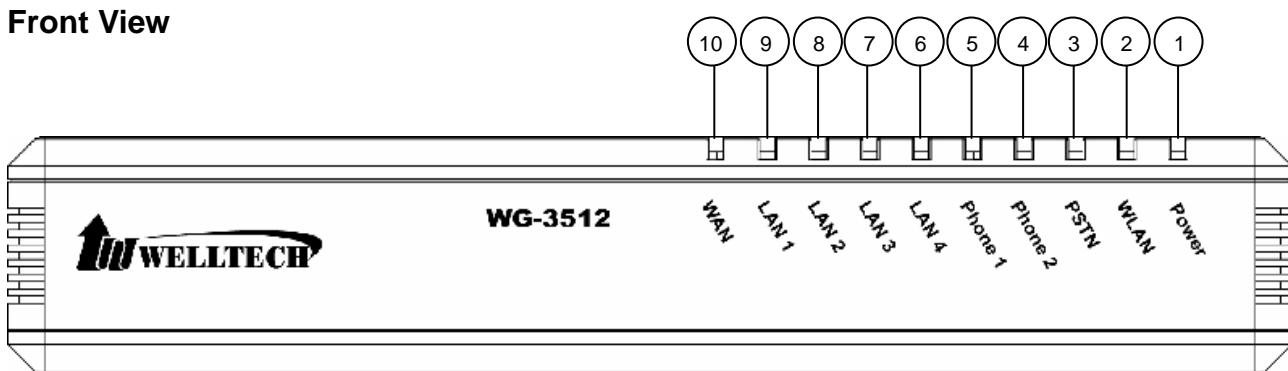
- SIP RFC3261
- TCP/UDP/IP/ICMP/ARP

Management

- **System log**
- **Display real-time information for system setting, statistics, and associated wireless client status.**
- **User name/password authentication for web server login and logout**
- **Web-based configuration and management interface**
- **Firmware update through web**
- **Configuration backup/restore to/from a file. Reset configuration to factory default**
- **IVR-Configuration by phone keys with Interactive Voice Prompts**

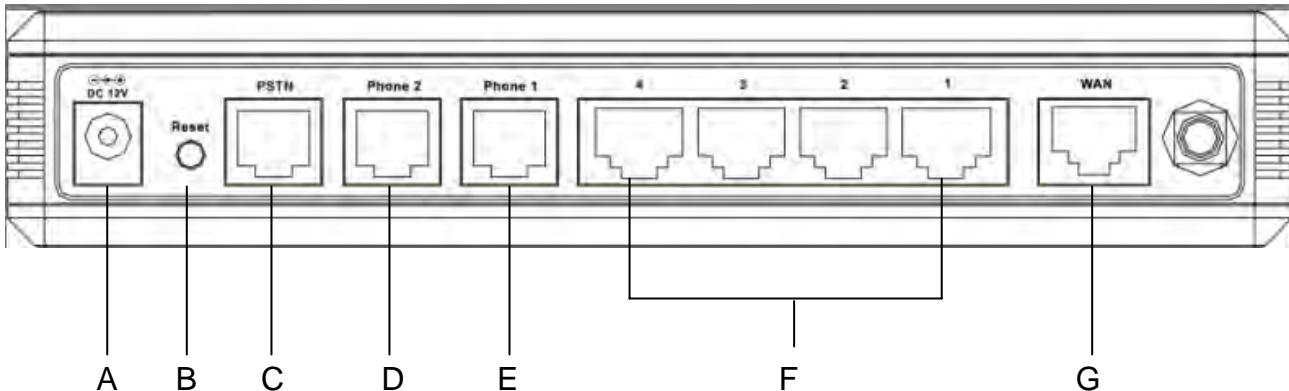
Certification

- **CE, FCC**

Front View


	LED Indicator	Status		
		Light On	Light Off	Light Flashing
1	Power	power on	power off	N/A
2	WLAN	N/A	N/A	WLAN is transmitting or receiving data.
3	PSTN	Gateway fails to register on Proxy	Gateway succeeds to register on Proxy	PSTN has incoming call or PSTN line is in use.
4	Phone 2	Phone 2 succeeds to register on Proxy	Phone 2 fails to register on Proxy	Phone 2 has incoming call or Phone 2 is in use.
5	Phone 1	Phone 1 succeeds to register on Proxy	Phone 1 fails to register on Proxy	Phone 1 has incoming call or Phone 1 is in use.
6	LAN 4	Network is connected	Network is not connected	Network is transmitting or receiving data.
7	LAN 3	Network is connected	Network is not connected	Network is transmitting or receiving data.
8	LAN 2	Network is connected	Network is not connected	Network is transmitting or receiving data.
9	LAN 1	Network is connected	Network is not connected	Network is transmitting or receiving data.
10	WAN	Network is connected	Network is not connected	Network is transmitting or receiving data.

Back View

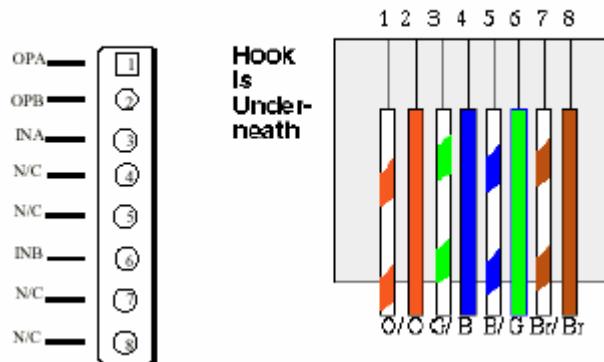


	Port/ Button	Functions
A	12V DC	Input AC 100V~120V. Output DC12V.
B	Reset	Press Reset key over 5 seconds, WG3512 will reboot and all configurations will restore to default values. If user press Reset key for 3-5 seconds, WG3512 will only reboot, but not return to default values.
C	PSTN	RJ-11 interface for connecting the extension line of PABX or PSTN Line.
D	Phone 2	RJ-11 interface for connecting the analog phone sets or trunk line of PABX.
E	Phone 1	RJ-11 interface for connecting the analog phone sets or trunk line of PABX.
F	LAN 4 3 2 1	10/100 Base-T; RJ-45 socket, complied with ETHERNET 10/100base-T.
G	WAN	10/100 Base-T; RJ-45 socket, complied with ETHERNET 10/100base-T.

Specification of connector

■ Ethernet Port

Ethernet port is for connecting WG3512 to network, transmit rate supports 10/100 Base-T.



Call Features

■ Direct IP Call

User can dial out call with IP address directly.

- Dial IP: ex. To dial out IP 192.168.1.1 via phone set need to press **192*168*1*1#**. "#" means to dial out immediately, if user doesn't follow by "#" sign, WG3512 will dial out after "auto dial time".
- Dial IP and port: To dial out IP 192.168.1.1 and port 5061 via phone set need to press **192*168*1*1**5061#**. "#" means to dial out immediately, if user doesn't follow by "#" sign, WG3512 will dial out after "auto dial time".

■ Proxy Call

User can dial out phone number if WG3512 registered to Proxy successfully. Ex. To dial out phone number 100 via phone set need to press 100#. "#" means to dial out immediately, if user doesn't follow by "#" sign, WG3512 will dial out after "auto dial time".

Note:

If WG3512 registered on Proxy successfully, the LED of Phone will light up, and on web page—VoIP Settings—Phone—SIP Proxy—Register Status will display registered.

■ Call Waiting

When Phone is in communication, WG3512 can receive another incoming call.

➤ Call Scenario:

- 1) Phone 1 is in communication with A. B calls in Phone 1. From Phone 1 will hear call waiting tone.
- 2) Phone 1 press flash hook, A will be put on hold, and Phone 1 will enter communication with B.
- 3) Phone 1 press flash hook again can return to communicate with A, and B will be put on hold.

■ Three-way Conference

WG3512 supports three-way conference.

➤ Call Scenario:

- 1) Phone 1 is in communication with A.
- 2) Phone 1 press flash hook will hear dial tone.
- 3) Dial out to B, after talk with B, press flash hook again will get into conference call with A and B.

■ Call Transfer (Blind Transfer)

WG3512 supports Blind Transfer only.

➤ Call Scenario:

- 1) Phone 1 is in communication with A.
- 2) Phone 1 press ***1**
- 3) B will be put on hold, and Phone 1 will hear Dial tone.

- 4) Phone 1 dial to B, both Phone 1 and A will hear ring back tone.
- 5) B picks up, B and C in communication, A hear busy tone and disconnect.

Chapter 2 Configuring the WG3512 through Voice Prompt and Phone set

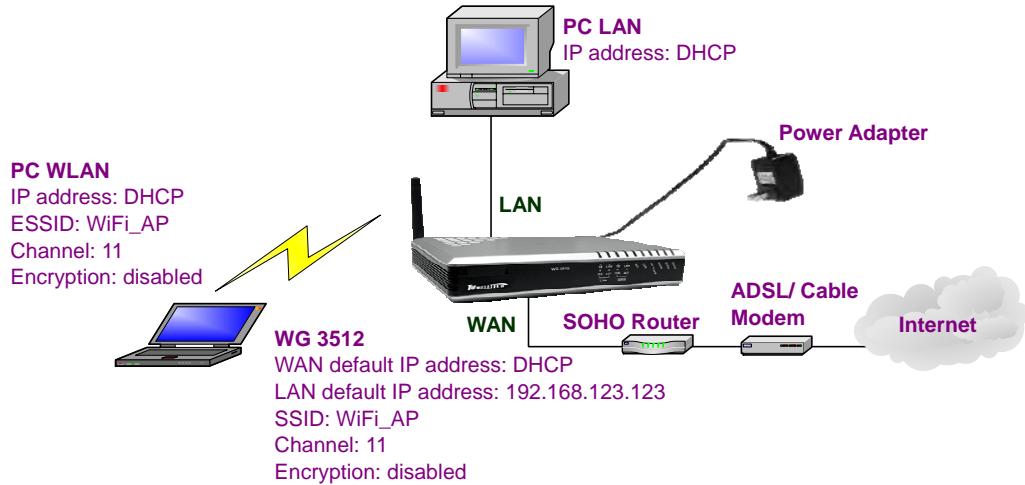
Please connect one analog phone set with Phone 1 port of WG3512, and then input specific keys as below to get some information or make brief configurations.

Category	Function	Input Key	Example
Set Network Settings	DHCP client for WAN	#111	#111#
	Set Fixed IP for WAN	#112	#112192*168*0*100# set IP as 192.168.0.100
	Set Netmask for WAN	#113	#113255*255*255*0# set netmask as 255.255.255.0
	Set Gateway for WAN	#114	#114192*168*1*254# set gateway as 192.168.1.254
	Set DNS	#115	#115168*95*1*1# set DNS ad 168.95.1.1
	Set Fixed IP for LAN	#116	#116192*168*1*254# set IP as 192.168.1.254
Voice Network Settings	Voice LAN IP address	#120	#120#
	Voice IP type	#121	#121#
	Voice SIP register ID	#122	#122#
	Voice netmask	#123	#123#
	Voice gateway	#124	#124#
	Voice DNS	#125	#125#
	Voice WAN IP address	#126	#126#
	Voice firmware version	#128	#128#

VoIP Settings	Set first priority codec	#130 + first priority codec	#13001# Set 711 u-law to be first priority codec. Codec Number: 01: G.711 u-law 02: G.711 a-law 03: G.729 04: G.723 6.3k 05: G.723 5.3k 06: G.726-16 07: G.726-24 08: G.726-32 09: G.726-40
	Handset gain	#131	#13109# Set handset gain as 9 (Range of gain: 1~10)
	Handset volume	#132	#13209# Set handset volume as 9 (Range of gain: 1~10)
	Enable call waiting	#138	#138#
	Disable call waiting	#139	#139#
	Forward setting	#140 + Forward type +Forwarded Phone Number	#1401101#Immediate forward to 101 Forward Type: 1: Immediate forward2. Busy forward3. No answer forward
	Disable forward setting	#141	#141#
Others	Apply Setting	#195	#195#
	Reset to default	#198	#198#

Chapter 3 Configuring the WG3512 through Web Pages

The HTTP web management interface provides user an easy way to configure WG3512.



Step 1. Power on the WG3512

Step 2. Check the LEDs

After power on, the [Power] and [PSTN] LEDs should be on; [WLAN] LED should be blinking.

Step 3. Connect PC with one of LAN port

Please connect PC with one of the LAN port on WG3512 and set PC as DHCP mode. PC will get one dynamic IP from WG3512, such as 192.168.123.1.

Step 4. Browse the Default IP Address of WG3512 and enter the web interface main screen

Please enter IP address of WG3512 in web browser. The default IP address of WG3512 is **192.168.123.123**. There is no user name and password of default values, and the user can see web interface main screen as below.





The screenshot shows the 'VoIP WiFi Gateway' setup wizard. On the left, a sidebar lists 'Site contents' with options: Setup Wizard, Operation Mode, Wireless, TCP/IP Settings, Firewall, VoIP Settings, Management, and System Reboot. The main content area is titled 'Setup Wizard' and contains the following text:
Welcome to Setup Wizard.
The Wizard will guide you through following steps. Begin by clicking on Next.
A numbered list of steps is provided:

1. Setup Operation Mode
2. Choose your Time Zone
3. Setup LAN Interface
4. Setup WAN Interface
5. Wireless LAN Setting
6. Wireless Security Setting

A 'Next>>' button is located at the bottom right of the content area.

Step 5. Start to configure

After enter web management interface, user can see 8 main items.

- 1. Setup Wizard:** User can follow steps in wizard to make first-time initial configuration.
- 2. Operation Mode:** User can setup different modes to LAN and WLAN interface for NAT and bridging function.
- 3. Wireless:** User can set all wireless related parameters here.
- 4. TCP/IP:** User can set LAN and WAN related configurations here.
- 5. Firewall:** User can set firewall function of WG3512 here.
- 6. VoIP Setting:** User can set VoIP related parameters here.
- 7. Management:** User can check information or manage WG3512 here.
- 8. System Reboot:** User can remote reboot WG3512 here.

Button Definition:

- 1. Apply Changes:** After change or input any parameter, press this button will save data into WG3512.
- 2. Reset:** Press this button will clean data input by user and restore to original data.

Setup Wizard

The setup wizard will guide you to configure access point for first time. Please follow the setup wizard step by step.

Press **Cancel** will return to the first page of Setup Wizard.

Press **Next>>** to next step.

Press **<<Back** will return to last step of Setup Wizard.

Press **Finished** will save all configurations and WG3512 will reboot.



■ Operation Mode:

You can setup different modes to LAN and WLAN interface for NAT and bridging function. WG3512 provide all 3 primary modes and 4 extended modes. Here you can find 3 primary modes, including:

1) Gateway mode, 2) Bridge mode, 3) Wireless ISP. Another 4 extended modes are changes from these 3 mainly modes and plus some application, including: 1) Client mode, 2) WDS Repeater Mode, 3) Universal Repeater mode, 4) WISP + Universal Repeater mode.

- **Gateway:** In this mode, the device is supposed to connect to internet via ADSL/Cable Modem. The NAT is enabled and PCs in four LAN ports share the same IP to ISP through WAN port. The connection type can be setup in WAN page by using PPPOE, DHCP client or static IP.
- **Bridge:** In this mode, all ethernet ports and wireless interface are bridged together and NAT function is disabled. All the WAN related function and firewall are not supported
- **Wireless ISP:** In this mode, all ethernet ports are bridged together and the wireless client will connect to ISP access point. The NAT is enabled and PCs in ethernet ports share the same IP to ISP through wireless LAN. You must set the wireless to client mode first and connect to the ISP AP in Site-Survey page. The connection type can be setup in WAN page by using PPPOE,

DHCP client or static IP.

VoIP WiFi Gateway

1. Operation Mode

You can setup different modes to LAN and WLAN interface for NAT and bridging function.

Gateway: In this mode, the device is supposed to connect to internet via ADSL/Cable Modem. The NAT is enabled and PCs in four LAN ports share the same IP to ISP through WAN port. The connection type can be setup in WAN page by using PPPOE, DHCP client or static IP.

Bridge: In this mode, all ethernet ports and wireless interface are bridged together and NAT function is disabled. All the WAN related function and firewall are not supported.

Wireless ISP: In this mode, all ethernet ports are bridged together and the wireless client will connect to ISP access point. The NAT is enabled and PCs in ethernet ports share the same IP to ISP through wireless LAN. You must set the wireless to client mode first and connect to the ISP AP in Site-Survey page. The connection type can be setup in WAN page by using PPPOE, DHCP client or static IP.

[Cancel](#) [<<Back](#) [Next>>](#)

■ Time Zone Setting

You can maintain the system time by synchronizing with a public time server over the Internet.

- **Enable NTP client update:** User can update time of WG3512 from NTP server if this function is enabled.
- **Time Zone Select:** Select the time zone according to location.
- **NTP server:** User may select one NTP server for WG3512 to update current time.

VoIP WiFi Gateway

2. Time Zone Setting

You can maintain the system time by synchronizing with a public time server over the Internet.

Enable NTP client update

Time Zone Select : (GMT+08:00)Taipei

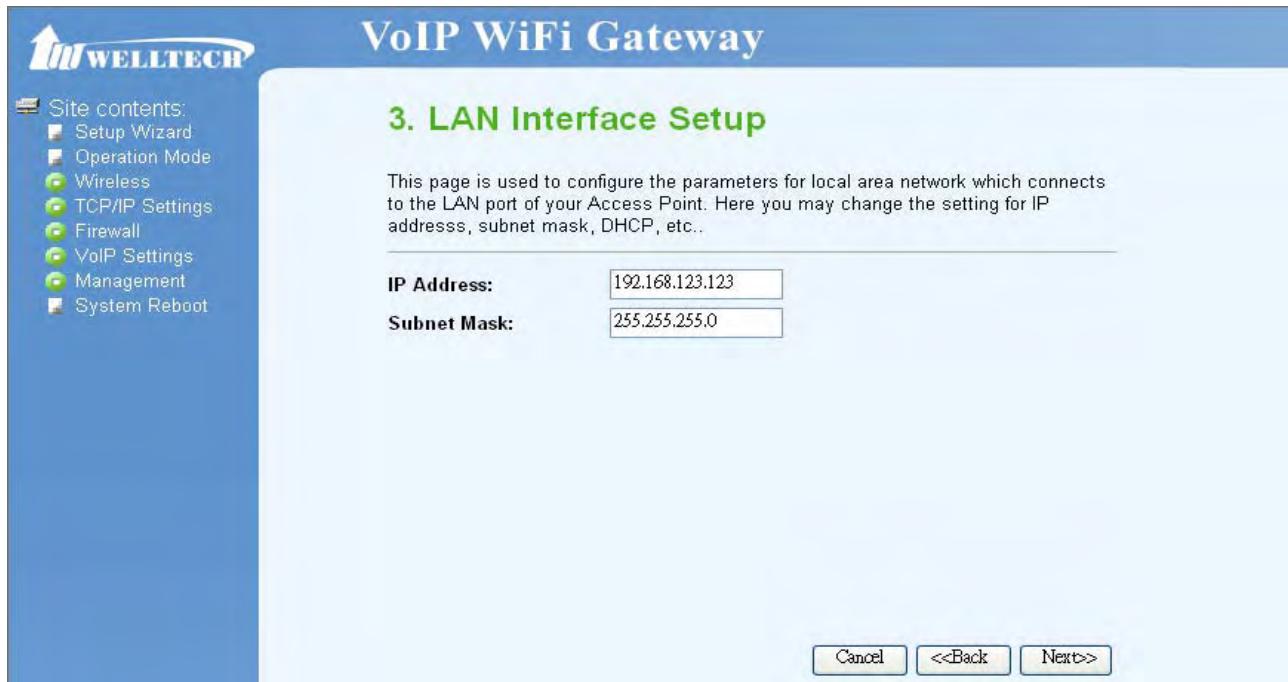
NTP server : 192.5.41.41 - North America

[Cancel](#) [<<Back](#) [Next>>](#)

■ LAN Interface Setup

This page is used to configure the parameters for local area network which connects to the LAN port of your Access Point. Here you may change the setting for IP address, subnet mask, DHCP, etc...

- IP Address: Set IP address of LAN interface.
- Subnet Mask: Set subnet mask of LAN interface.



VoIP WiFi Gateway

3. LAN Interface Setup

This page is used to configure the parameters for local area network which connects to the LAN port of your Access Point. Here you may change the setting for IP addresss, subnet mask, DHCP, etc..

IP Address:

Subnet Mask:

Site contents:

- Setup Wizard
- Operation Mode
- Wireless
- TCP/IP Settings
- Firewall
- VoIP Settings
- Management
- System Reboot

Cancel <<Back Next>>

■ WAN Interface Setup

This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE or PPTP by click the item value of WAN Access type.

- Static IP: Set WAN interface as Static IP mode.
 - 1) IP Address: set IP address of WAN interface.
 - 2) Subnet Mask: set subnet mask of WAN interface.
 - 3) Default Gateway: set default gateway of WAN interface.
 - 4) DNS: set Domain Name Server for WAN interface.

VoIP WiFi Gateway

4. WAN Interface Setup

This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP or PPPoE by click the item value of WAN Access type.

WAN Access Type:

IP Address: 192.168.1.1

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.1.254

DNS : 168.95.1.1

- DHCP Client: Set WAN interface as DHCP mode.

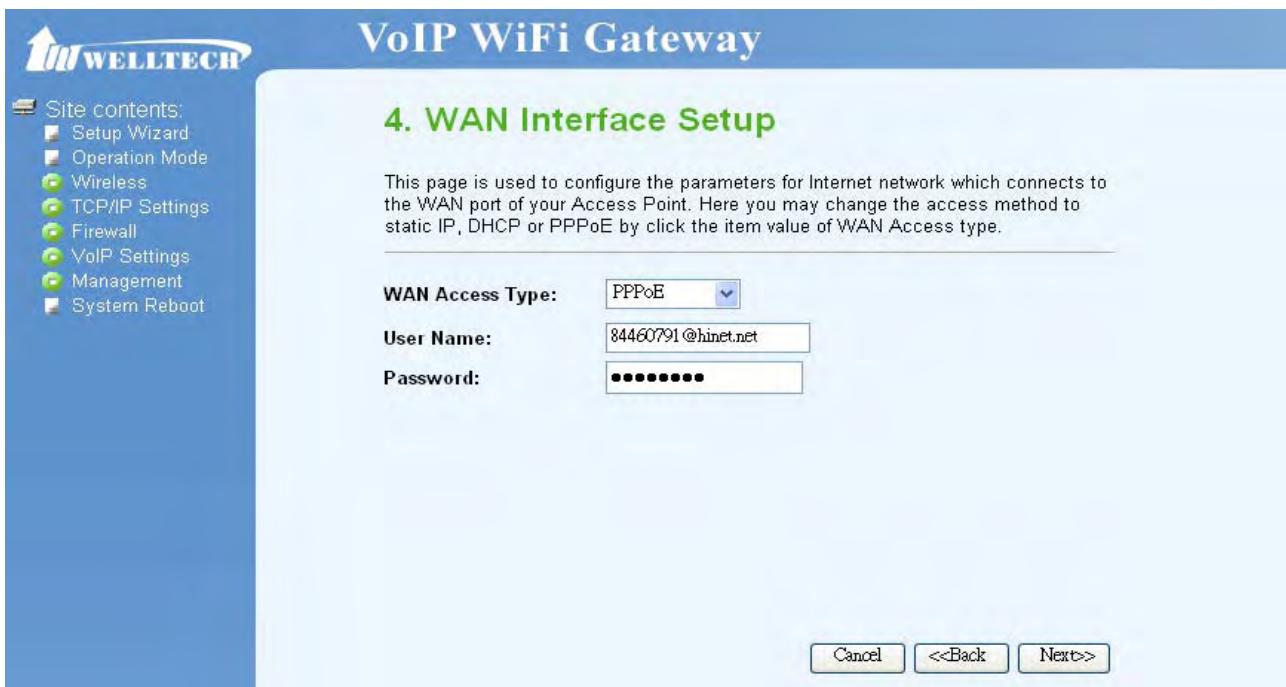
VoIP WiFi Gateway

4. WAN Interface Setup

This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP or PPPoE by click the item value of WAN Access type.

WAN Access Type:

- PPPoE: Set WAN interface as PPPoE mode.
 - 1) User Name: Set user name of PPPoE connection.
 - 2) Password: Set password of PPPoE connection.

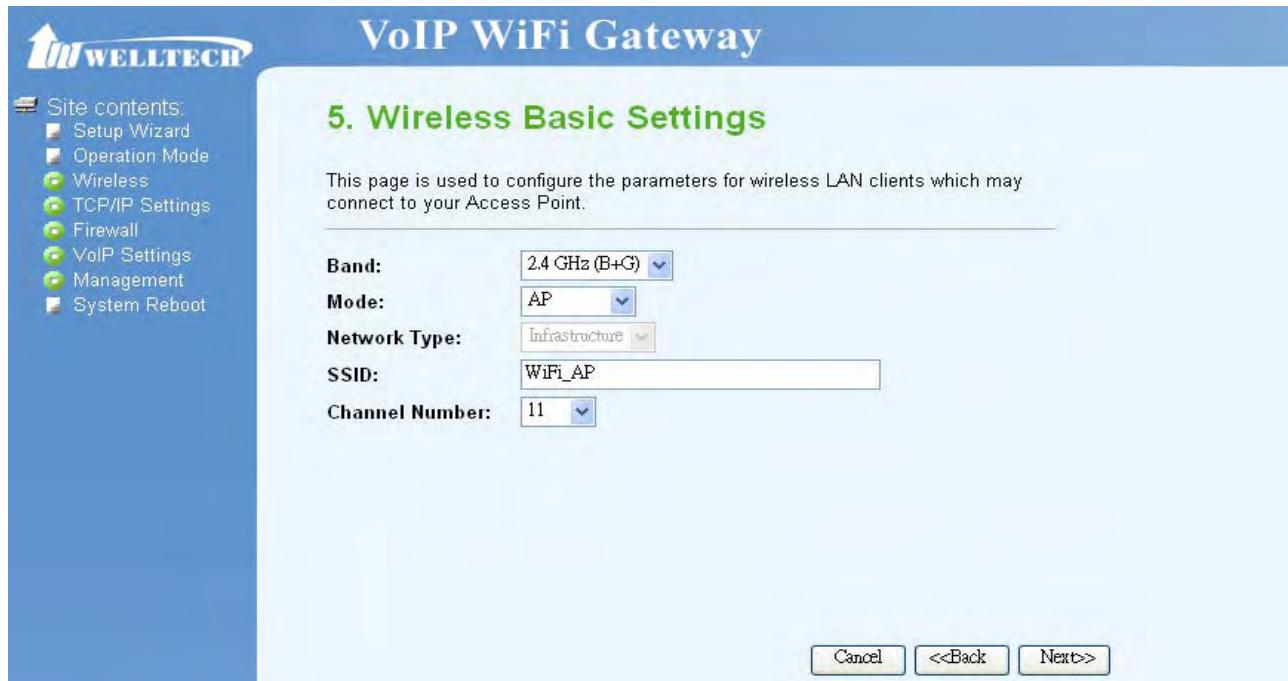


■ Wireless Basic Settings

This page is used to configure the parameters for wireless LAN clients, which may connect to your Access Point.

- Band: Select wireless band as 802.11b, 802.11g, or 802.11b+g.
- Mode: Select wireless mode. User could find 4 different modes here, including AP, Client, WDS, AP+WDS. AP mode enables WG3512 as wireless access point and allows other devices to connect wirelessly to a wired Ethernet network. Client mode enables WG3512 to perform as a wireless client card and other devices can connect with Ethernet cable to WG3512. WDS mode is to extend the wireless coverage of another wireless AP. AP+WDS enables WG3512 to perform as an AP and a WDS repeater. Here we will guide you how to setup it with AP mode.
- Network Type: Only when wireless mode set as client, user can select network type as infrastructure or Ad hoc. Infrastructure represents a wireless network centered about an access point. Ad hoc represents a wireless network composed only of stations within mutual communication range of each other.
- SSID: specify to the WG3512 an SSID (Service Set Identifier), which is a unique identifier attached to packets over WLAN. The SSID is up to 32 ASCII characters that differentiate the WG3512 from other WiFi AP, and it is also referred to as the ESSID (Extended Service Set Identifier). You may use the default SSID unless there more than one WG3512 in the same area. In this case, you should specify different SSID for each WG3512.
- Channel Number: Set channel for wireless connection. You can set channel for radio

communication manually. If you set it as Auto, the WG3512 will select a clear channel during boot up.



5. Wireless Basic Settings

This page is used to configure the parameters for wireless LAN clients which may connect to your Access Point.

Band: 2.4 GHz (B+G)

Mode: AP

Network Type: Infrastructure

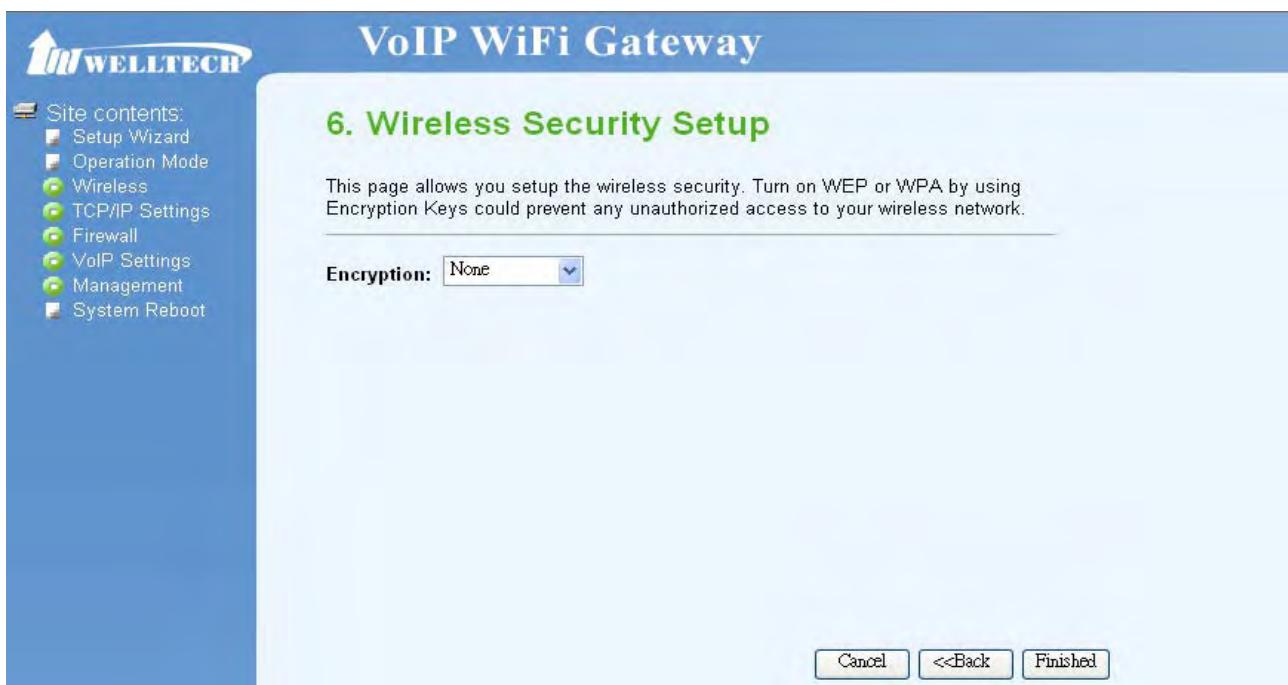
SSID: WiFi_AP

Channel Number: 11

■ Wireless Security Setup

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

- **Encryption:** Set encryption as none, WEP, WPA, WPA2 or WPA2 Mixed.



6. Wireless Security Setup

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

Encryption:

- 1) WEP: When encryption WEP is selected, you must set WEP key value. Only user with the same WEP key can connect to the WG3512.
 - Key Length: set WEP key length as 64 or 128 bits and select user to transmit data using 64 or 128 bits WEP key encryption. 64 bits represents a lower level encryption for security, and uses ASCII (5 characters) or Hex (10 characters) encryption scheme as a secret key. 128 bits represents a higher level encryption for security, and uses ASCII (13 characters) or Hex (26 characters) encryption scheme as a secret key.
 - Key Format: set key format as ASCII (5 characters) or Hex (10 characters) for 64 bits encryption; ASCII (13 characters) or Hex (26 characters) for 128 bits encryption.
 - Default Tx Key: set default key as key 1, 2, 3, or 4. User can specify which of the four keys to use for transmitting data over WLAN.
 - Encryption Key 1/2/3/4: user can set 4 sets of encryption keys. Keys 1-4 allow you to easily change wireless encryption settings to maintain a secure network. WEP key is either 5/10 or 13/26 ASCII/hexadecimal characters based on user select 64 or 128 bits key length.



The screenshot shows the '6. Wireless Security Setup' page of the VoIP WiFi Gateway. The left sidebar contains a 'Site contents' menu with options: Setup Wizard, Operation Mode, Wireless, TCP/IP Settings, Firewall, VoIP Settings, Management, and System Reboot. The main content area has a blue header 'VoIP WiFi Gateway'. Below it, the section title '6. Wireless Security Setup' is displayed in green. A descriptive text states: 'This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.' Below this, there are several configuration fields:

- Encryption:** A dropdown menu set to 'WEP'.
- Key Length:** A dropdown menu set to '64-bit'.
- Key Format:** A dropdown menu set to 'Hex (10 characters)'.
- Default Tx Key:** A dropdown menu set to 'Key 1'.
- Encryption Key 1:** An input field containing '*****'.
- Encryption Key 2:** An input field containing '*****'.
- Encryption Key 3:** An input field containing '*****'.
- Encryption Key 4:** An input field containing '*****'.

At the bottom right of the page are three buttons: 'Cancel', '<<Back', and 'Finished'.

- 2) WPA(TKIP): only user with the same WPA pre-shared key can connect to WG3512 and transmit data using TKIP encryption.
 - Pre-Shared Key Format: Select Pre-Shared Key Format as Passphrase or Hex (64 characters).

- Pre-Shared Key: set pre-shared key manually.



The screenshot shows the '6. Wireless Security Setup' page. The left sidebar lists 'Site contents' with 'Wireless' selected. The main area has 'Encryption' set to 'WPA (TKIP)', 'Pre-Shared Key Format' set to 'Passphrase', and a 'Pre-Shared Key' input field. Buttons at the bottom include 'Cancel', '<<Back', and 'Finished'.

3) WPA2(AES): AES (Advance Encryption Standard) is the U.S. government's next generation cryptography algorithm.

- Pre-Shared Key Format: Select Pre-Shared Key Format as Passphrase or Hex (64 characters).
- Pre-Shared Key: set pre-shared key manually.



The screenshot shows the '6. Wireless Security Setup' page. The left sidebar lists 'Site contents' with 'Wireless' selected. The main area has 'Encryption' set to 'WPA2(AES)', 'Pre-Shared Key Format' set to 'Passphrase', and a 'Pre-Shared Key' input field. Buttons at the bottom include 'Cancel', '<<Back', and 'Finished'.

4) WPA2 Mixed

- Pre-Shared Key Format: Select Pre-Shared Key Format as Passphrase or Hex (64 characters).
- Pre-Shared Key: set pre-shared key manually.



6. Wireless Security Setup

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

Encryption: WPA2 Mixed

Pre-Shared Key Format: Passphrase

Pre-Shared Key:

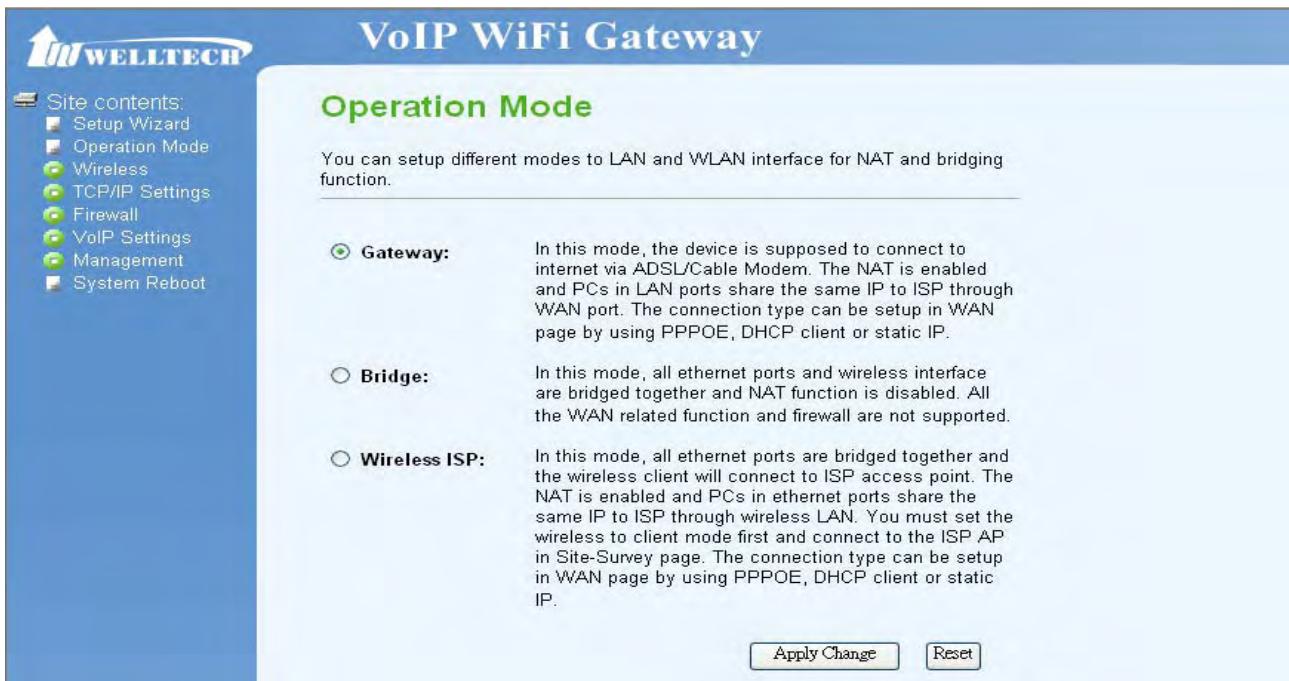
Cancel <<Back Finished

Operation Mode

You can setup different modes to LAN and WLAN interface for NAT and bridging function. WG3512 provide all 3 primary modes and 4 extended modes. Here you can find 3 primary modes, including: 1) Gateway mode, 2) Bridge mode, 3) Wireless ISP. Another 4 extended modes are changes from these 3 mainly modes and plus some application, including: 1) Client mode, 2) WDS Repeater Mode, 3) Universal Repeater mode, 4) WISP + Universal Repeater mode.

- **Gateway:** In this mode, the device is supposed to connect to internet via ADSL/Cable Modem. The NAT is enabled and PCs in four LAN ports share the same IP to ISP through WAN port. The connection type can be setup in WAN page by using PPPOE, DHCP client or static IP.
- **Bridge:** In this mode, all ethernet ports and wireless interface are bridged together and NAT function is disabled. All the WAN related function and firewall are not supported
- **Wireless ISP:** In this mode, all ethernet ports are bridged together and the wireless client will connect to ISP access point. The NAT is enabled and PCs in ethernet ports share the same IP to ISP through wireless LAN. You must set the wireless to client mode first and connect to the ISP AP in Site-Survey page. The connection type can be setup in WAN page by using PPPOE, DHCP client or static IP.

For more information regarding Operation Modes, please refer to **CH 4 Wireless Operation Modes**.



Operation Mode

You can setup different modes to LAN and WLAN interface for NAT and bridging function.

Gateway: In this mode, the device is supposed to connect to internet via ADSL/Cable Modem. The NAT is enabled and PCs in LAN ports share the same IP to ISP through WAN port. The connection type can be setup in WAN page by using PPPOE, DHCP client or static IP.

Bridge: In this mode, all ethernet ports and wireless interface are bridged together and NAT function is disabled. All the WAN related function and firewall are not supported.

Wireless ISP: In this mode, all ethernet ports are bridged together and the wireless client will connect to ISP access point. The NAT is enabled and PCs in ethernet ports share the same IP to ISP through wireless LAN. You must set the wireless to client mode first and connect to the ISP AP in Site-Survey page. The connection type can be setup in WAN page by using PPPOE, DHCP client or static IP.

Wireless

■ Basic Settings

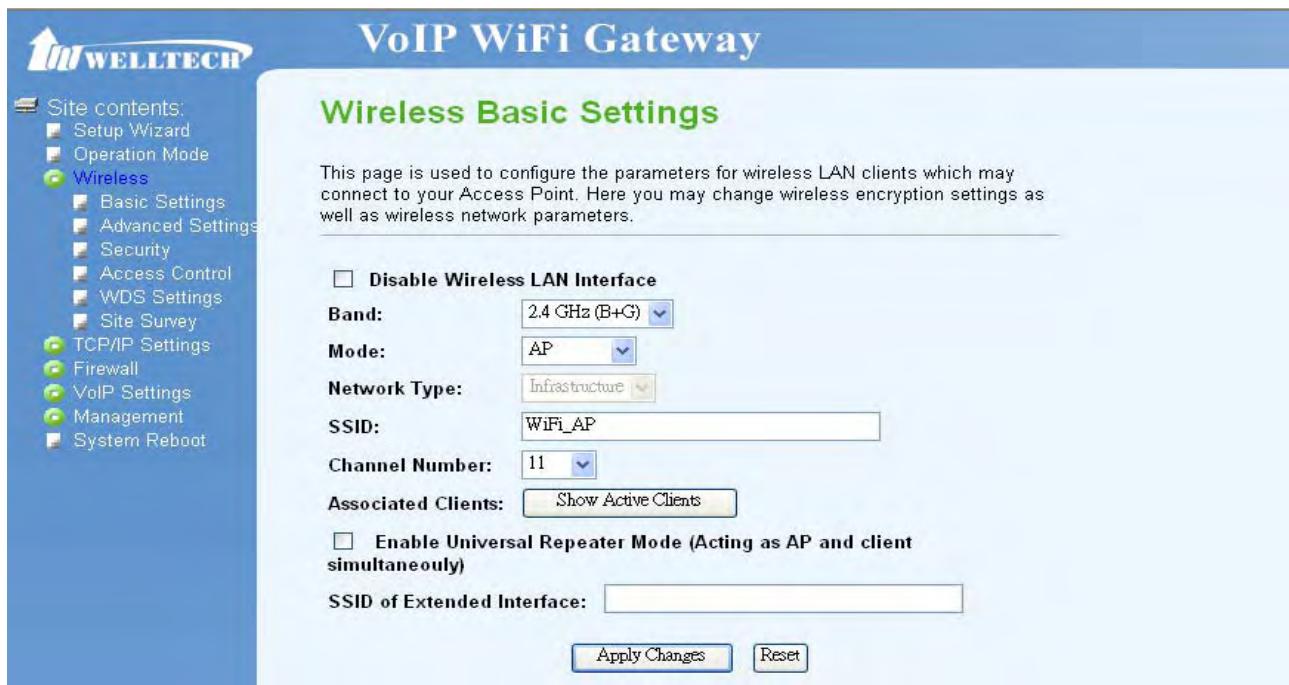
This page is used to configure the parameters for wireless LAN clients which may connect to your Access Point.

- **Disable Wireless LAN Interface:** If user checks this function, wireless LAN will be disabled. In other words, this device will not be visible by any wireless station.
- **Band:** Select wireless band as 802.11b, 802.11g, or 802.11b+g.
- **Mode:** Select wireless mode as AP, Client, WDS and AP+WDS. AP mode enables WG3512 to work as wireless an access point and allow other devices to connect wirelessly to a wired Ethernet network. Client mode enables WG3512 to perform as a wireless client card and other devices can connect with Ethernet cable to WG3512. WDS and AP+WDS are used for Repeater. If AP+WDS is enabled, WG3512 could be working as AP and WDS Repeater together.
- **Network Type:** Only when wireless mode set as client, user can select network type as infrastructure or Ad hoc. Infrastructure represents a wireless network centered about an access point. Ad hoc represents a wireless network composed only of stations within mutual communication range of each other. (No Access Point).
- **SSID:** specify to the WG3512 an SSID (Service Set Identifier), which is a unique identifier attached to packets over WLAN. The SSID is up to 32 ASCII characters that differentiate the WG3512 from other WiFi AP, and it is also referred to as the ESSID (Extended Service Set

Identifier). You may use the default SSID unless there are more than one WG3512 in the same area. In this case, you should specify different SSID for each WG3512.

- Channel Number: Set channel for wireless connection. You can set channel for radio communication manually. If you set it as Auto, the WG3512 will select a clear channel during boot up.
- Associated Clients: Press **Show Active Clients** to see which client registers on this WG3512.
- Enable Universal Repeater Mode (Acting as AP and client simultaneously): Enable this feature will perform WG3512 to work as Universal Repeater.
- SSID of Extended Interface: User could input SSID of Extended Interface here if Universal Repeater is enabled.

For more information regarding WDS, AP+WDS and Universal Repeater mode, please refer to CH 4 Wireless Operation Modes.



Wireless Basic Settings

This page is used to configure the parameters for wireless LAN clients which may connect to your Access Point. Here you may change wireless encryption settings as well as wireless network parameters.

Disable Wireless LAN Interface

Band: 2.4 GHz (B+G)

Mode: AP

Network Type: Infrastructure

SSID: WiFi_AP

Channel Number: 11

Associated Clients:

Enable Universal Repeater Mode (Acting as AP and client simultaneously)

SSID of Extended Interface:

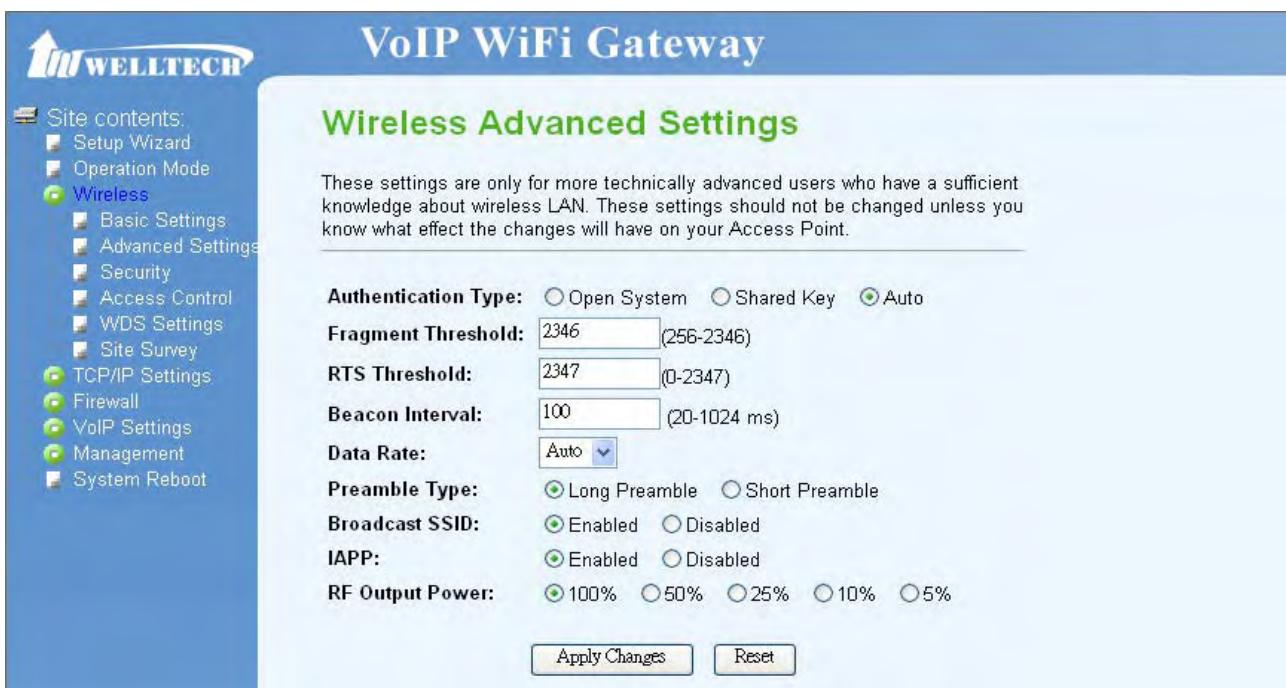
■ Advanced Setting

These settings are only for more technically advanced users who have a sufficient knowledge about wireless LAN. These settings should not be changed unless you know what effect the changes will have on your Access Point.

- Authentication Type: Select authentication type as Open System, Shared Key, or Auto. With Open System authentication, a wireless PC can join any network and receive any messages that are not encrypted. With Shared Key authentication, only those PCs that possess the correct authentication key can join the network.
- Fragment Threshold (256-2346): set fragment threshold size. Fragments are small pieces

divided from 802.11 frames. If there are excessive collisions over WLAN, user can try different fragment size to increase reliability.

- RTS Threshold (0-2347): RTS Threshold is a mechanism implemented to prevent the problem of “Hidden Node”. “Hidden Node” is a situation in which two stations are within range of the same Access Point, but are not within range of each other. Therefore, they are hidden nodes for each other. When station starts data transmission with the Access Point, it might not notice that the other station is already using the wireless medium. When these two stations send data at the same time, they might collide when arriving simultaneously at the Access Point. The collision will most certainly result in a loss of messages for both stations. Thus, the RTS Threshold mechanism provides a solution to prevent data collisions. If the “Hidden Node” problem is an issue, please specify the packet size. The RTS mechanism will be activated if the data size exceeds the value you set. Default value is 2347.
- Beacon Interval: set beacon interval time in milliseconds. System broadcast packet or a beacon to synchronize the wireless network.
- Data Rate: specify the transmission rate. Leave on “Auto” to maximize performance versus distance.
- Preamble Type: A preamble is a signal used in wireless environment to synchronize the transmitting timing including Synchronization and Start frame delimiter. In a “noisy” network environment, the Preamble Type should be set to Long Preamble. The Short Preamble is intended for applications where minimum overhead and maximum performance is desired.
- Broadcast SSID: enable or disable SSID broadcast function. If user enables this function, other wireless clients can broadcast and find this wireless AP to connect.
- IAPP: IAPP is a portable implementation of the 802.11F specification for Inter Access Point Protocol (IAPP) to enable end-station mobility across Access Points.
- RF Output Power: set radio output power level as 100%, 50%, 25%, 10% or 5%.



Wireless Advanced Settings

These settings are only for more technically advanced users who have a sufficient knowledge about wireless LAN. These settings should not be changed unless you know what effect the changes will have on your Access Point.

Authentication Type: Open System Shared Key Auto

Fragment Threshold: 2346 (256-2346)

RTS Threshold: 2347 (0-2347)

Beacon Interval: 100 (20-1024 ms)

Data Rate: Auto

Preamble Type: Long Preamble Short Preamble

Broadcast SSID: Enabled Disabled

IAPP: Enabled Disabled

RF Output Power: 100% 50% 25% 10% 5%

Buttons: Apply Changes, Reset

■ Security

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

- **Encryption:** Set encryption as none, WEP, WPA, WPA2 or WPA2 Mixed.
- **Set WEP Key:** When encryption WEP is selected, you must set WEP key value.
 - 1) **Key Length:** Set WEP key length as 64 or 128 bits.
 - 2) **Key Format:** Set key format as **ASCII** (5 characters) if you are using **ASCII** characters. Select **HEX** if you are using hexadecimal numbers.
 - 3) **Default Tx Key:** Set default transmit key as key 1, 2, 3, or 4.
 - 4) **Encryption Key 1/2/3/4:** user can set 4 sets of encryption keys. Keys 1-4 allow you to easily change wireless encryption settings to maintain a secure network. WEP key is either 5/10 or 13/26 ASCII/decimal characters based on user select 64 or 128 bits key length.

10 hexadecimal digits or 5 ASCII characters are needed if 64 bit WEP is used; 26 hexadecimal digits or 13 ASCII characters are needed if 64 bit WEP is used

- **Use 802.1x Authentication:** Check to use Radius 802.1x authentication and select authentication level as WEP 64 bits or 128bits. In this case, please set Authentication RADIUS Server information.
- **WPA Authentication Mode:** Select WPA authentication mode as Enterprise (RADIUS) or Personal (Pre-Shared Key). If user select Enterprise mode, please fill in Authentication RADIUS Server information. If user select Personal mode, please select Pre-Shared key

format and fill in Pre-Shared Key.

- WPA Cipher Suite: Select WPA Cipher Suite to be TKIP or AES, this field is used as a password to begin the encryption process.

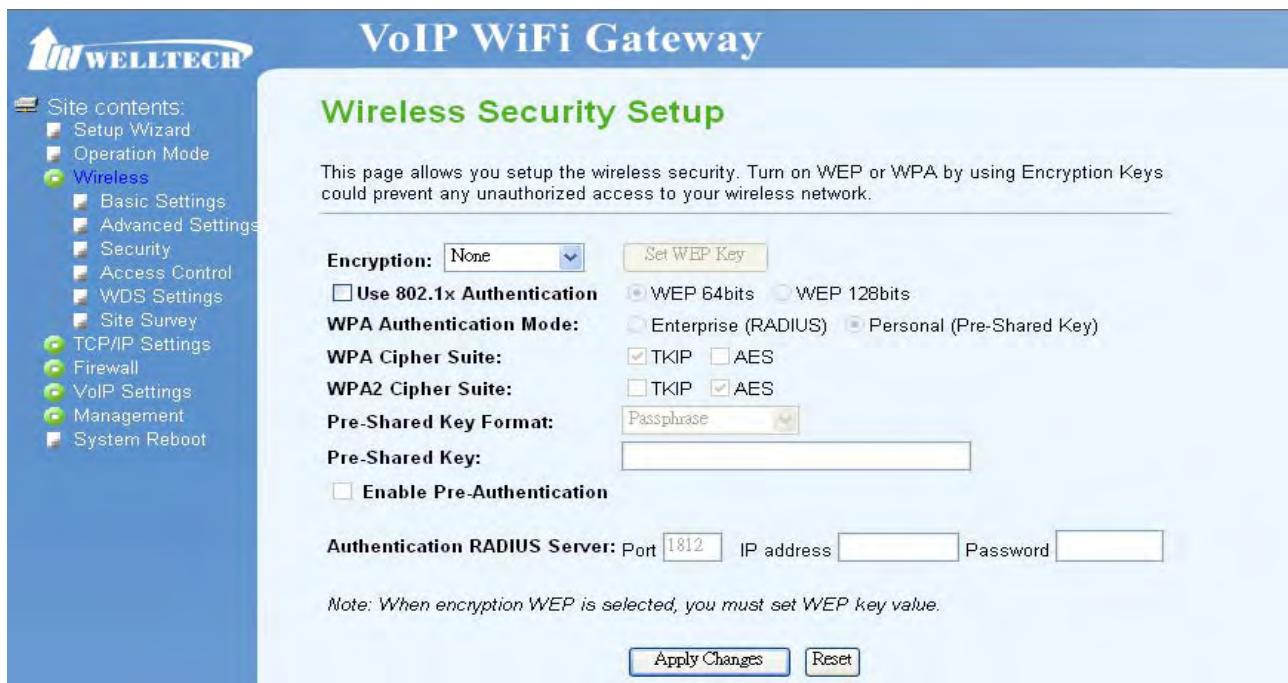
- WPA2 Cipher Suite: Select WPA Cipher Suite to be TKIP or AES.

WPA is an encryption standard proposed by WiFi for advance protection. It is more secure than WEP encryption.

- Pre-Shared Key Format: There are two formats for choice to set the Pre-Shared key, i.e. **Passphrase** and **Hex**. Select Pre-Shared Key Format as Passphrase (at least 8 characters) or Hex (64 characters). For easier configuration, The **Passphrase** is recommended.
- Pre-Shared Key: Set pre-shared key manually.

When WPA is enabled and the WPA Authentication Mode is set to Personal. You should also input Pre-shared Key for encryption.

- Enable Pre-Authentication: Pre-Authentication, which enables secure fast roaming without noticeable signal latency, provides a way to establish a PMK security association before a client associates. The advantage is that the client reduces the time that it's disconnected to the network.
- Authentication RADIUS Server: set port, IP address, and password of Radius Server for WG3512 to initial a Radius connection and get dynamic WEP key.



VoIP WiFi Gateway

Wireless Security Setup

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

Encryption:

Use 802.1x Authentication

WEP 64bits **WEP 128bits**

Enterprise (RADIUS) **Personal (Pre-Shared Key)**

WPA Authentication Mode:

TKIP **AES**

TKIP **AES**

Pre-Shared Key Format:

Pre-Shared Key:

Enable Pre-Authentication

Authentication RADIUS Server: Port IP address Password

Note: When encryption WEP is selected, you must set WEP key value.

■ Access Control

If you choose **Allowed Listed**, only those clients whose wireless MAC addresses are in the access control list will be able to connect to your Access Point. When **Deny Listed** is selected, these wireless clients on the list will not be able to connect the Access Point.

- Wireless Access Control Mode: Set disable control, allow list or deny list.

If user set control mode as Allow Listed, please add MAC address below to increase Allow List. If user set control mode as Deny Listed, please add MAC address below to increase Deny List.

- MAC Address: Input MAC address for allow or deny list.
- Comment: Give description for each data.
- Current Access Control List: Show current control list.
- User can press **Delete Selected** to delete specified data or press **Delete All** to delete all lists.



■ WDS Settings

Wireless Distribution System uses wireless media to communicate with other APs, like the Ethernet does. To do this, you must set these APs in the same channel and set MAC address of other APs which you want to communicate with in the table and then enable the WDS.

- Enable WDS: Enable WDS to start transmitting and receiving WDS packets. You can only use this feature when wireless mode set to WDS or AP+WDS.
- MAC address: Enter 12 digits in hex numbers in this field and press Apply Changes to associate with other's Wireless access point. Before you want to use WDS Repeater mode, you have to enter the other's AP/Router MAC address that the device want to connect.
- Reset: Reset the settings of WDS.

- Set Security: This setting is use between both wireless AP/ Router device.
- Show Statistics: Show the current statistics of WDS.
- Current WDS AP List: Show the current WDS AP list.



■ Site Survey

This page provides tool to scan the wireless network. If any Access Point or IBSS is found, you could choose to connect it manually when client mode is enabled.

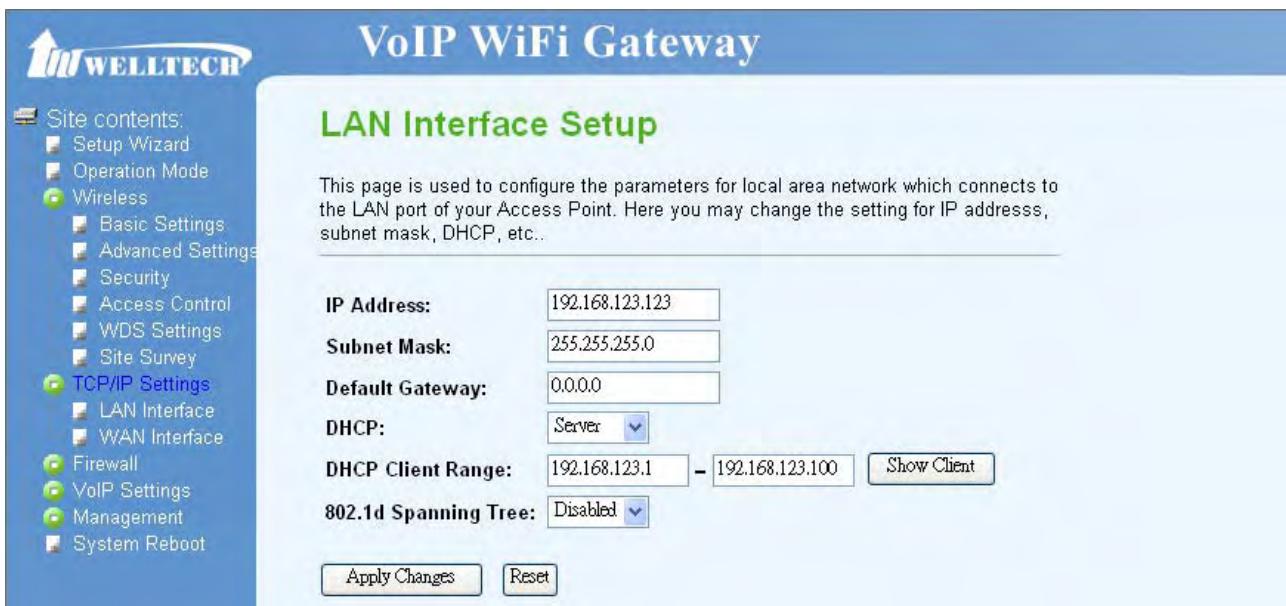


TCP/IP Settings

■ LAN Interface

- IP Address: Set IP address of LAN interface.
- Subnet Mask: Set subnet mask of LAN interface.

- Default Gateway: Set default gateway of LAN interface. It is normally used when Bridge mode is enabled.
- DHCP: Set DHCP mode to be disabled, Client, or Server. When user set DHCP mode as server mode, please set **DHCP Client Range** for LAN interface to assign DHCP IP.
- **Show Client**: Press this key can check current DHCP clients that captured IP from WG3512. Press **Refresh** can renew screen display, and press **Close** can close window.
- DHCP Client Range: Set DHCP IP range for WG3512 to assign IP address for other device in LAN.
- 802.1d Spanning: Enable or disable 802.1d Spanning Tree function.

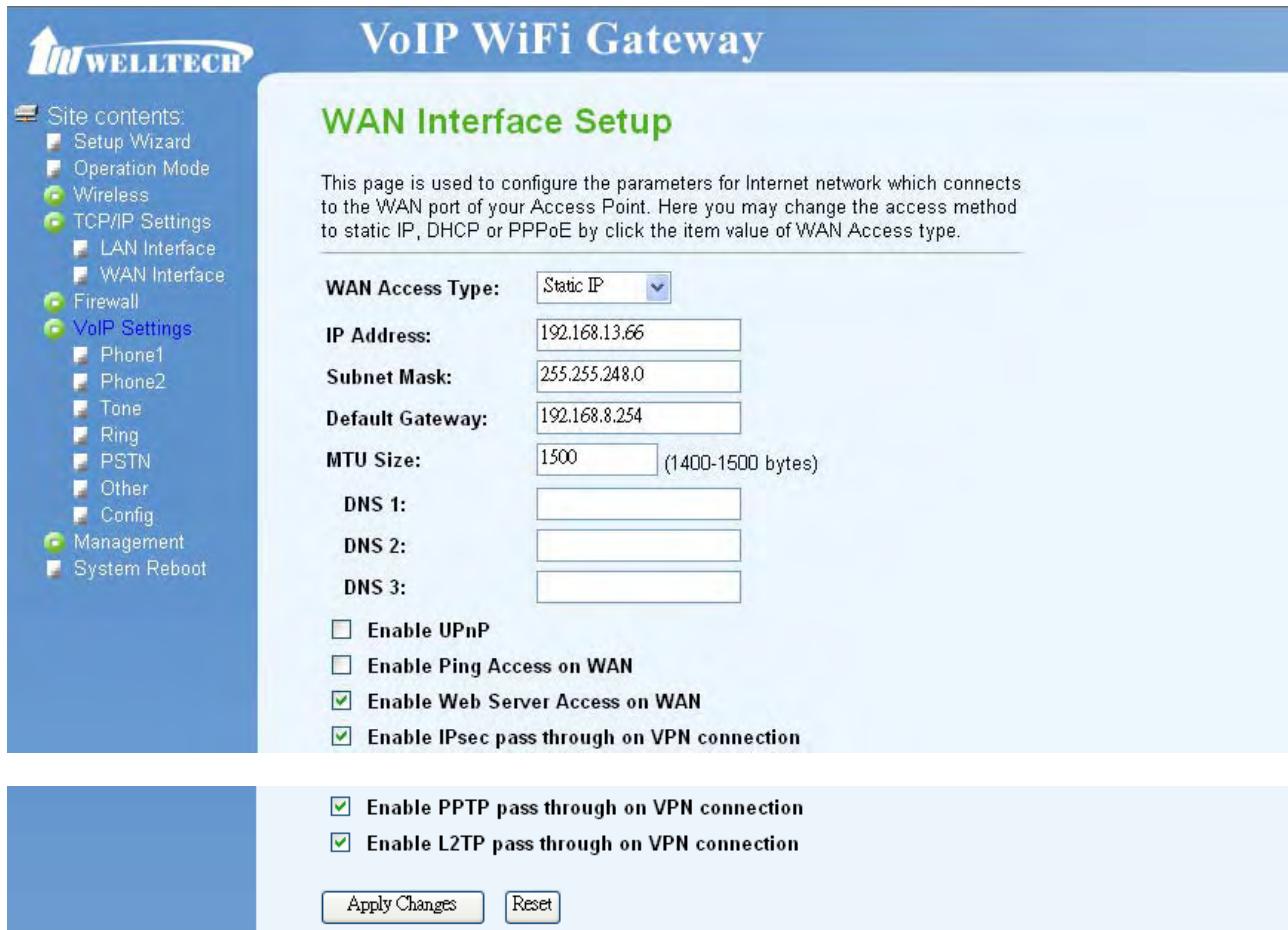


■ WAN Interface

This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP or PPPoE by click the item value of WAN Access type.

- WAN Access Type: Select WAN mode as Static IP/ DHCP Client/ PPPoE.
 - 1) Static IP: Set WAN interface as Static IP mode.
 - 2) IP Address: Set IP address of WAN interface.
 - 3) Subnet Mask: Set subnet mask of WAN interface.
 - 4) Default Gateway: Set default gateway of WAN interface.
 - 5) MTU Size: Set MTU (maximum transmission unit) size.
 - 6) DNS 1/DNS 2/ DNS 3: Set three alternative Domain Name Server for WAN interface.
 - 7) Enable UPnP: check to enable UPnP function.
 - 8) Enable Ping Access on WAN: If this function is checked to enable, user can reach WG3512 via Ping WAN IP address.

- 9) Enable Web Server Access on WAN: If this function is checked to enable, user can enter Web Server management of WG3512 through WAN IP address.
- 10) Enable IPsec pass through on VPN connection: check to enable IPsec function.
- 11) Enable PPTP pass through on VPN connection: check to enable PPTP pass through function.
- 12) Enable L2TP pass through on VPN connection: check to enable L2TP pass through function.



➤ DHCP Client: Set WAN interface as DHCP mode.

- 1) MTU Size: Set MTU (maximum transmission unit) size.
- 2) Attain DNS Automatically/Set DNS Manually: select to attain DNS automatically from server or user wants to set DNS manually.

After setting to DHCP, the IP information will be displayed in the page of Management→Status.

- 3) DNS 1/DNS 2/ DNS 3: Set three alternative Domain Name Server manually for WAN interface.
- 4) Enable UPnP: check to enable UPnP function.

- 5) Enable Ping Access on WAN: If this function is checked to enable, user can reach WG3512 via Ping WAN IP address.
- 6) Enable Web Server Access on WAN: If this function is checked to enable, user can enter Web Server management of WG3512 through WAN IP address.
- 7) Enable IPsec pass through on VPN connection: check to enable IPsec function.
- 8) Enable PPTP pass through on VPN connection: check to enable PPTP pass through function.
- 9) Enable L2TP pass through on VPN connection: check to enable L2TP pass through function.



VoIP WiFi Gateway

WAN Interface Setup

This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP or PPPoE by click the item value of WAN Access type.

WAN Access Type:

Host Name:

MTU Size: (1400-1492 bytes)

Attain DNS Automatically
 Set DNS Manually

DNS 1:

DNS 2:

DNS 3:

Enable UPnP
 Enable Ping Access on WAN
 Enable Web Server Access on WAN
 Enable IPsec pass through on VPN connection

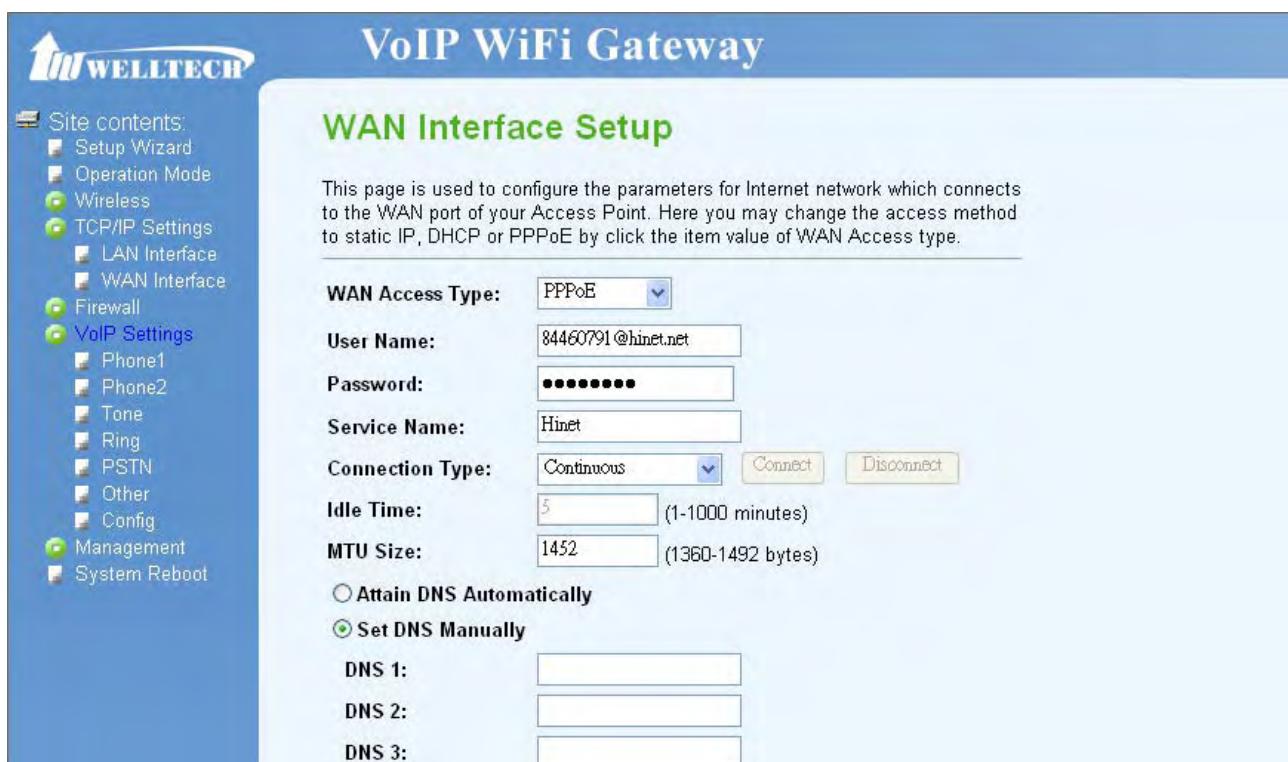
Enable PPTP pass through on VPN connection
 Enable L2TP pass through on VPN connection

➤ PPPoE: Set WAN interface as PPPoE mode.

- 1) User Name: Set user name of PPPoE connection.
- 2) Password: Set password of PPPoE connection.
- 3) Service Name: Set Service Name of PPPoE for description.
- 4) Connection Type: Set PPPoE connection type to be Continuous/ Connect on Demand/ Manual. If user set type as Continuous, WG3512 will keep trying to connect to server

when PPPoE disconnect. If user set type as Connect on Demand, please set following idle time, WG3512 will check connection after this time. If user set type as Manual, WG3512 will only connect or disconnect by press **Connect** or **Disconnect** manually.

- 5) Idle Time: Set PPPoE connection idle time for Connect on Demand.
- 6) MTU Size: Set MTU (maximum transmission unit) size.
- 7) Attain DNS Automatically/Set DNS Manually: Select to attain DNS automatically from server or user wants to set DNS manually.
- 8) DNS 1/DNS 2/ DNS 3: Set three alternative Domain Name Server manually for WAN interface.
- 9) Enable UPnP: Check to enable UPnP function.
- 10) Enable Ping Access on WAN: If this function is checked to enable, user can reach WG3512 via Ping WAN IP address.
- 11) Enable Web Server Access on WAN: If this function is checked to enable, user can enter Web Server management of WG3512 through WAN IP address.
- 12) Enable IPsec pass through on VPN connection: check to enable IPsec function.
- 13) Enable PPTP pass through on VPN connection: check to enable PPTP pass through function.
- 14) Enable L2TP pass through on VPN connection: check to enable L2TP pass through function.





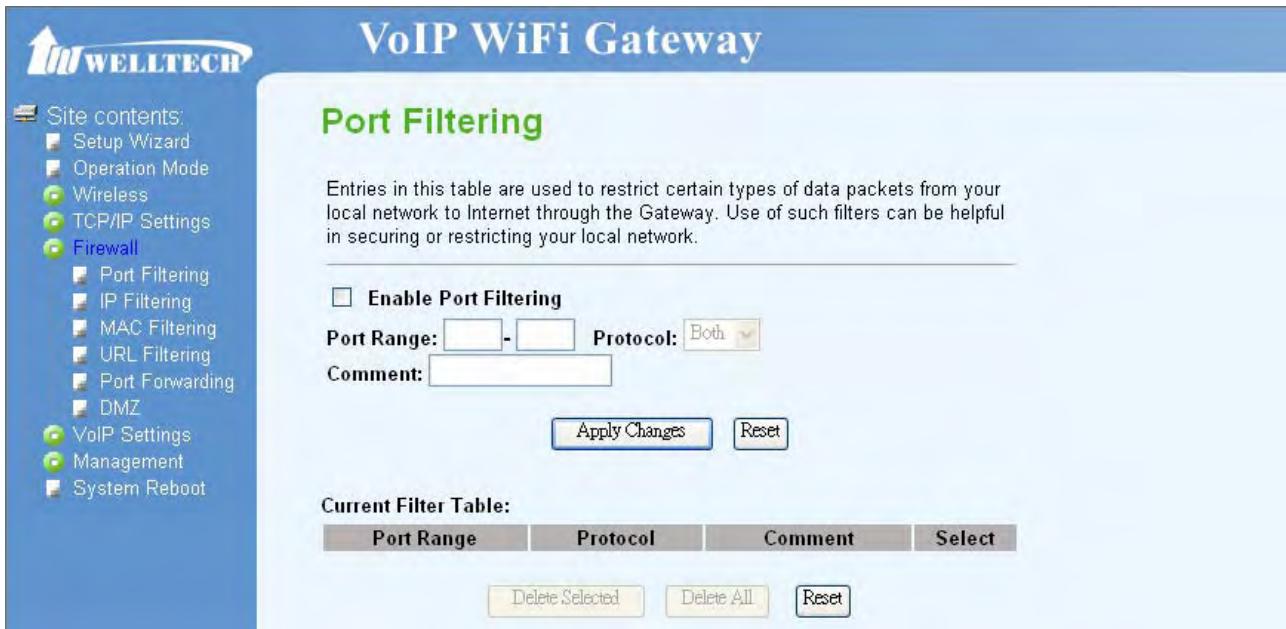
Enable UPnP
 Enable Ping Access on WAN
 Enable Web Server Access on WAN
 Enable IPsec pass through on VPN connection
 Enable PPTP pass through on VPN connection
 Enable L2TP pass through on VPN connection

Firewall

■ Port Filtering

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

- Enable Port Filtering: check to enable Port Filtering function.
- Port Range: set start port and end port for port filtering range.
- Protocol: set protocol as TCP or UDP or both protocol.
- Comment: Make description for this port filtering rule.



Enable Port Filtering
 Port Range: - Protocol:

Comment:

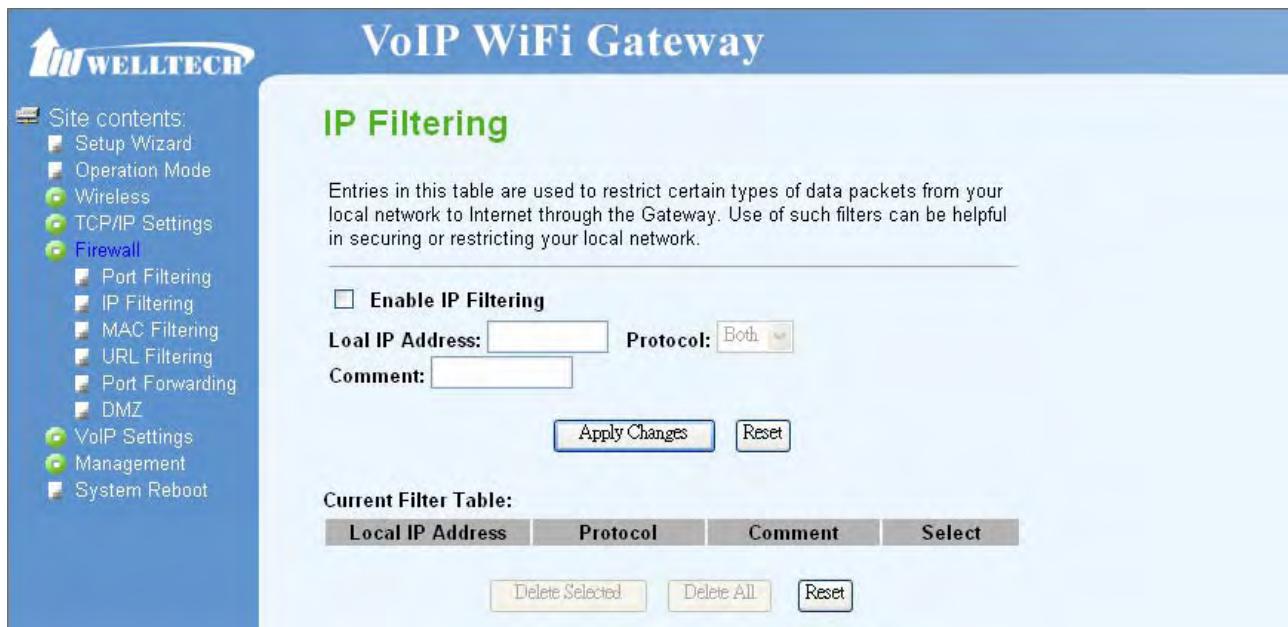
Port Range	Protocol	Comment	Select
<input type="button" value="Delete Selected"/>	<input type="button" value="Delete All"/>	<input type="button" value="Reset"/>	

■ IP Filtering

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

- Enable IP Filtering: check to enable IP Filtering function.
- Local IP Address: set IP Address for IP filtering.
- Protocol: set protocol as TCP or UDP or both protocol.

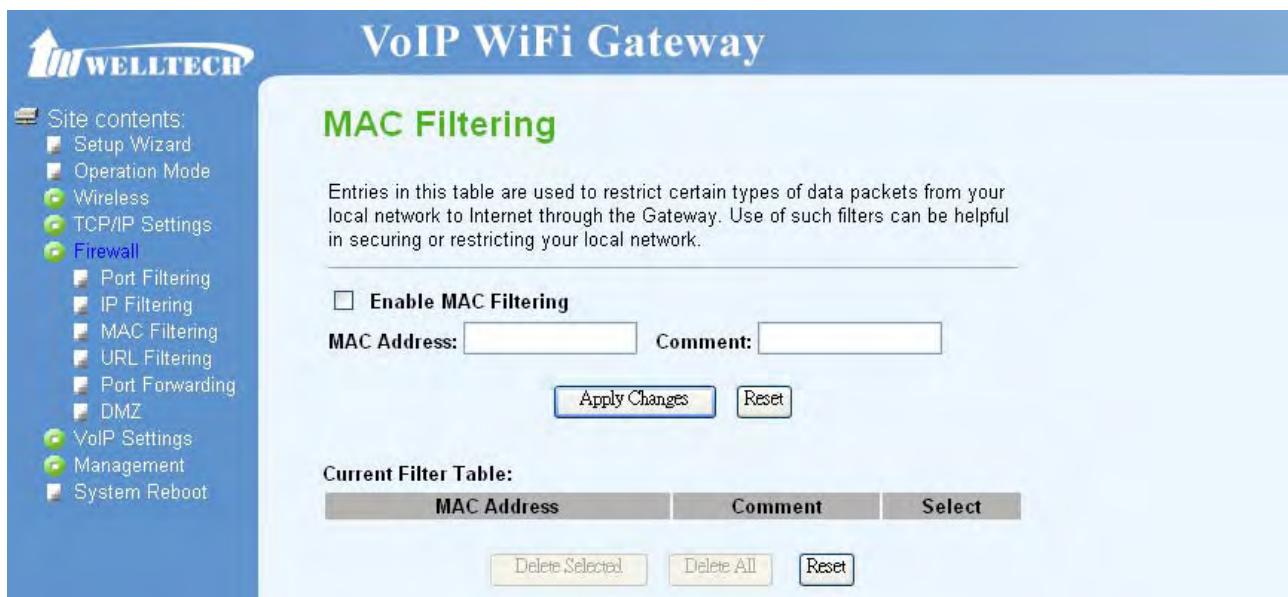
- Comment: Make description for this IP filtering rule.



■ MAC Filtering

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

- Enable MAC Filtering: check to enable MAC Filtering function.
- MAC Address: set MAC Address for MAC filtering.
- Comment: Make description for this MAC filtering rule.



■ URL Filtering

URL filter is used to deny LAN users from accessing the internet. Block those URLs which contain keywords listed below.

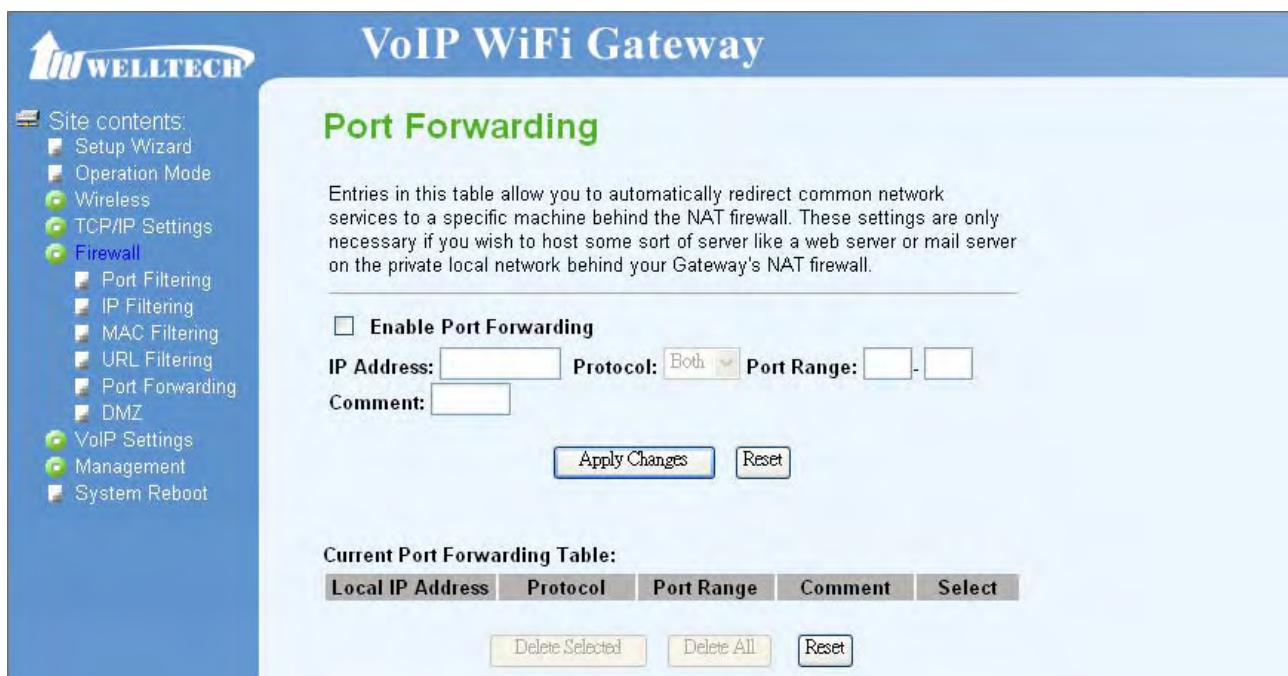
- Enable URL Filtering: check to enable URL Filtering function.
- URL Address: set URL address for URL filtering function.



■ Port Forwarding

Entries in this table allow you to automatically redirect common network services to a specific machine behind the NAT firewall. These settings are only necessary if you wish to host some sort of server like a web server or mail server on the private local network behind your Gateway's NAT firewall.

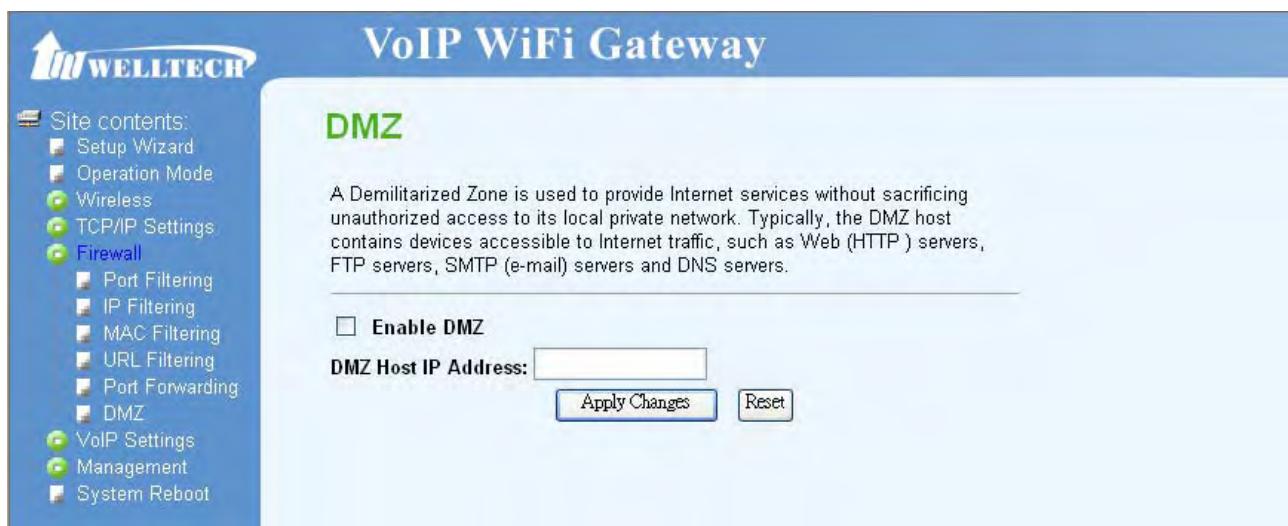
- Enable Port Forwarding: check to enable Port Forwarding function.
- IP Address: set IP address for port forwarding.
- Protocol: Set Protocol type for port forwarding.
- Port Range: set start port and end port for port forwarding range.
- Comment: Make description for this port forwarding rule.



■ DMZ

A Demilitarized Zone is used to provide Internet services without sacrificing unauthorized access to its local private network. Typically, the DMZ host contains devices accessible to Internet traffic, such as Web (HTTP) servers, FTP servers, SMTP (e-mail) servers and DNS servers.

- Enable DMZ: check to enable DMZ function.
- DMZ Host Address: set IP address for DMZ function.



VoIP Settings

■ Port1 ■ Port 2

Here is to set VoIP Phone 1 and Phone 2 related configurations.

- SIP Account

- 1) Display Name: Set WiFi Phone display name for caller ID information.
- 2) Number: Set registering Phone number.
- 3) Login ID: If Proxy server needs registration authentication please input Login ID here.
- 4) Password: If Proxy server needs registration authentication please input password here.
- SIP Proxy
 - 1) Proxy: Check to enable Proxy mode.
 - 2) Proxy Addr: If user enable Proxy mode, please input Proxy address.
 - 3) Proxy Port: If user enable Proxy mode, please input Proxy port.
 - 4) SIP Domain: Set SIP domain name for SIP signaling.
 - 5) Register Status: Here will display SIP account register status.
 - 6) Outbound Proxy: Check to enable Outbound Proxy mode.
 - 7) Outbound Proxy Addr: If user enables Outbound Proxy, please input Outbound Proxy address.
 - 8) Outbound Proxy Port: If user enables Outbound Proxy, please input Outbound Proxy port.
 - 9) STUN: check to enable STUN function.
 - 10) Stun Server Addr: If user enables STUN function, please input STUN Server address.
 - 11) Stun Server Port: If user enables STUN function, please input STUN Server port.
- SIP Advanced
 - 1) Reg Expire (sec): Set expire time of registration. WG3512 will keep re-registering to proxy server before expire timed out
 - 2) SIP Port: Set local SIP listening port.
 - 3) Media Port: Set RTP port for sending voice data.
 - 4) DTMF Relay: Select DTMF Relay to be In band, RFC 2833, or SIP INFO.
 - 5) RFC2833 Payload Type: If user select DTMF as RFC 2833 type, here can modify RFC 2833 payload type.
 - 6) SIP INFO Duration (ms): If user select DTMF as SIP INFO type, here can modify SIP INFO duration. Gateway will send out DTMF as this duration.
 - 7) Call Waiting: Check to enable Call Waiting function.
 - 8) Call Waiting Caller ID: Check to enable call waiting caller ID function. If this function is enabled, caller ID will display when having waiting call. Please note that your phone set should also support such function.
- Forward Mode
 - 1) Immediate Forward to: This is unconditional forward setting. All incoming call will be forwarded to specified number. Check to enable immediate forward function.
 - 2) Immediate Number: Enter the assigned number for Immediate forward.
 - 3) Busy Forward to: Check to enable Busy Forward function. When phone is busy, incoming call will be forwarded to assigned number.

- 4) Busy Number: Enter the assigned number for busy forward.
- 5) No Answer Forward to: Check to enable no answer forward function. When phone is not answered for a period of time, incoming call will be forwarded to assigned number.
- 6) No Answer Number: Enter assigned number for no answer forward.
- 7) No Answer Time (sec): Set no answer time. Once phone is not picked up after this time, incoming call will be forwarded to assigned number.

➤ Speed Dial

- 1) Position: Speed Dial access code. Press this speed dial number and followed by # can dial out assigned phone number.
- 2) Name: Name of this speed dial.
- 3) Phone Number: Set phone number for Gateway to make speed dial.
- 4) Select: User can delete selected speed dial data.

➤ Dial Plan

- 1) Replace prefix code: Select to enable (On) or disable (Off) prefix replace function.
- 2) Replace rule: Set prefix replace rule. Once user dial number matched prefix, Gateway will replace the number with assigned number. Available parameters are “0~9”, “#”, “*”, “+”, “x”. Symbol “+” means “or”, “x” could be numbers 0~9. For example, if user set Replace rule as **002+009->005**, which means if user dial 002 87654321 or 009 87654321, these number will be dial out as 005 87654321.
- 3) Dial Plan: User can set how many digits or which number for Gateway to dial out immediately. Available parameters are “0~9”, “#”, “*”, “+”, “x”. Symbol “+” means “or”, “x” could be numbers “0~9”. For example, user can set Dial Plan as “911+xxxxxxxx+*xx”, which means if user dial **911, 87654321**, or ***11**, these number will be dial out immediately without waiting for dial time or pressing # sign.
- 4) Auto Prefix: If user set Auto Prefix number, all number dialed out will be added with this prefix number. Available parameters are “0~9”, “#”, “*”. For example, user set Auto Prefix as 02, number 87654321 will be dial out as 02 87654321.
- 5) Prefix Unset Plan: User can set special access code to disable Auto Prefix function in single call. Available parameters are “0~9”, “#”, “*”, “+”, “x”. Symbol “+” means “or”, “x” could be numbers “0~9”. For example, if user set Prefix Unset Plan as ***1+xxxxxxxxxx**. When dialed number as ***1 87654321** or 10 digits of number, for this call will not be added with Auto Prefix number.

➤ Codec

- 1) Precedence: Set codec priority sequence.
- 2) Rate: Set G.723.1 codec with 5.3 or 6.3k mode.

➤ T.38(FAX)

- 1) T.38: Check to enable T.38 function.

- 2) T.38 Port: Set T.38 port for FAX.
- Hot Line
 - 1) Use Hot Line: Check to enable Hot Line function.
 - 2) Hot Line Number: Set the destination number for Hot Line function..
- DND (Don't Disturb)
 - 1) DND Mode: You can select 3 mode of DND. The call will be always rejected if Always is selected. The call will be rejected by below Time setting (From and To) if Enable is selected. The call will be accepted if Disable is selected.
 - 2) From: Set the start time for DND with Enable mode.
 - 3) To: Set the end time for DND with Enable mode.
- You can check the current time by the page of Time Zone Setting.**
- DSP
 - 1) FXS Volume
 - i. Handset Gain: Set Handset receiver volume from 1 to 10.
 - ii. Handset Volume: Set Handset transmit volume from 1 to 10.
 - 2) VAD: Check to enable VAD (Voice Activity Function) function.
 - 3) Caller ID Mode: Select caller ID mode as FSK(Bellcore), FSK(ETSI), FSK(BT), FSK(NTT), or DTMF from FXS to send out.
 - 4) FSK Date & Time Sync: Check to send FSK Date and Time to caller ID display device.
 - 5) Reverse Polarity before Caller ID: Check to send reverse polarity before caller ID.
 - 6) Short Ring before Caller ID: Check to send short ring before caller ID.
 - 7) Dual Tone before Caller ID: Check to send dual tone before caller ID.
 - 8) Caller ID Prior First Ring: Check to send caller ID before first ring.
 - 9) Caller ID DTMF Start Digit: Set caller ID DTMF start digit.
 - 10) Caller ID DTMF End Digit: Set caller ID DTMF end digit.
 - 11) Flash Time Setting (ms) [Space:10 , Max:2000]: Set Minimum and Maximum Flash time.
 - 12) Speaker Voice Gain (dB) [-32~31],Mute:-32: Set Speaker voice volume.
 - 13) Mic Voice Gain (dB) [-32~31],Mute:-32: Set microphone voice gain volume.



Site contents:

- Setup Wizard
- Operation Mode
- Wireless
- TCP/IP Settings
- Firewall
- VoIP Settings
 - Phone1
 - Phone2
 - Tone
 - Ring
 - PSTN
 - Other
 - Config
- Management
- System Reboot

VoIP WiFi Gateway

SIP Account

Display Name	1002
*Number	1002
*Login ID	1002
*Password	*****

SIP Proxy

Proxy	<input checked="" type="checkbox"/> Enable
Proxy Addr	10.1.1.2
Proxy Port	5060
SIP Domain	
Register Status	Not Registered
Outbound Proxy	<input type="checkbox"/> Enable
Outbound Proxy Addr	
Outbound Proxy Port	5060
Stun	<input type="checkbox"/> Enable
Stun Server Addr	
Stun Server Port	3478

SIP Advanced

Reg Expire (sec)	60
SIP Port	5061
Media Port	9004
DMTF Relay	RPC2833
RFC2833 Payload Type	101
SIP INFO Duration (ms)	250
Call Waiting	<input checked="" type="checkbox"/> Enable
Call Waiting Caller ID	<input type="checkbox"/> Enable

Forward Mode

Unconditional Forward to	<input checked="" type="radio"/> Off <input type="radio"/> On
Unconditional Forward Number	
Busy Forward to	<input checked="" type="radio"/> Off <input type="radio"/> On
Busy Number	
No Answer Forward to	<input checked="" type="radio"/> Off <input type="radio"/> On
No Answer Number	
No Answer Time (sec)	0

- Site contents:
 - Setup Wizard
 - Operation Mode
 - Wireless
 - TCP/IP Settings
 - Firewall
 - VoIP Settings
 - Phone1
 - Phone2
 - Tone
 - Ring
 - PSTN
 - Other
 - Config
 - Management
 - System Reboot

Speed Dial

Position	Name	Phone Number	Select
0	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
1	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
2	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
3	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
4	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
5	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
6	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
7	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
8	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
9	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>

Dial plan

Replace prefix code On Off

Replace rule ->

Dial Plan

Auto Prefix

Prefix Unset Plan

Codec

Type	Precedence									Rate
	1	2	3	4	5	6	7	8	9	
G711-ulaw	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	6.3k
G711-alaw	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
G729	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
G723	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
G726-16k	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
G726-24k	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>					
G726-32k	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>						
G726-40k	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>							
GSM-FR	<input type="checkbox"/>	<input checked="" type="checkbox"/>								

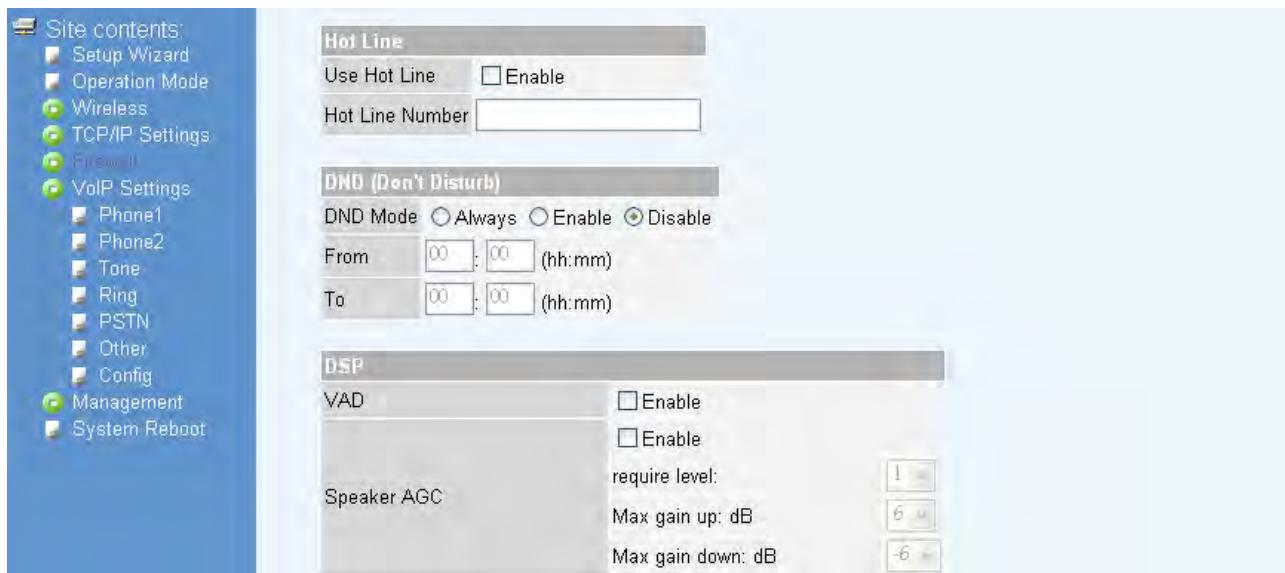
T.38(FAX)

T.38 Enable

T.38 Port

Copyright © 2007 Welltech Computer Co., Ltd. All right reserved.

44



The screenshot shows the 'Site contents' menu on the left with 'VoIP Settings' selected. The main panel displays three configuration sections: 'Hot Line', 'DND (Don't Disturb)', and 'DSP'.

Hot Line: 'Use Hot Line' checkbox is checked. 'Hot Line Number' field is empty.

DND (Don't Disturb): 'DND Mode' radio buttons are set to 'Disable'. 'From' and 'To' time ranges are set to 00:00 to 00:00.

DSP: 'VAD' checkboxes are checked. 'Speaker AGC' settings include 'require level' (1), 'Max gain up: dB' (6), and 'Max gain down: dB' (-6).



The screenshot shows the 'Site contents' menu on the left with 'VoIP Settings' selected. The main panel displays two configuration sections: 'MIC AGC' and 'Caller ID Mode'.

MIC AGC: 'Enable' checkbox is checked. 'require level' is set to 1, 'Max gain up: dB' is set to 6, and 'Max gain down: dB' is set to -6.

Caller ID Mode: 'DTMF' is selected in the dropdown. Other options include 'FSK Date & Time Sync', 'Reverse Polarity before Caller ID', 'Short Ring before Caller ID', 'Dual Tone before Caller ID', 'Caller ID Prior First Ring' (checked), 'Caller ID DTMF Start Digit' (DTMF_A), 'Caller ID DTMF End Digit' (DTMF_C), 'Caller ID Soft FSK Gen' (checked), 'Flash Time Setting (ms)' (0 to 300), 'Speaker Voice Gain (dB)' (0), and 'Mic Voice Gain (dB)' (0). 'Apply' and 'Reset' buttons are at the bottom.

■ Tone

➤ Select Country

User can select country to specify tone parameters (Dial Tone, Ring Tone, Busy Tone, and Waiting Tone). If user wants to set tone manually, please select CUSTOMER. After selecting CUSTOMER, user can assign Custom 1 to 8 for each tone.

➤ Select Custom Tone: Select Custom tone number to set Tone Parameters.

➤ Tone Parameters:

1) CanOn: set cadence time for tone to play in ms. For example, if set CanOn as 100, the

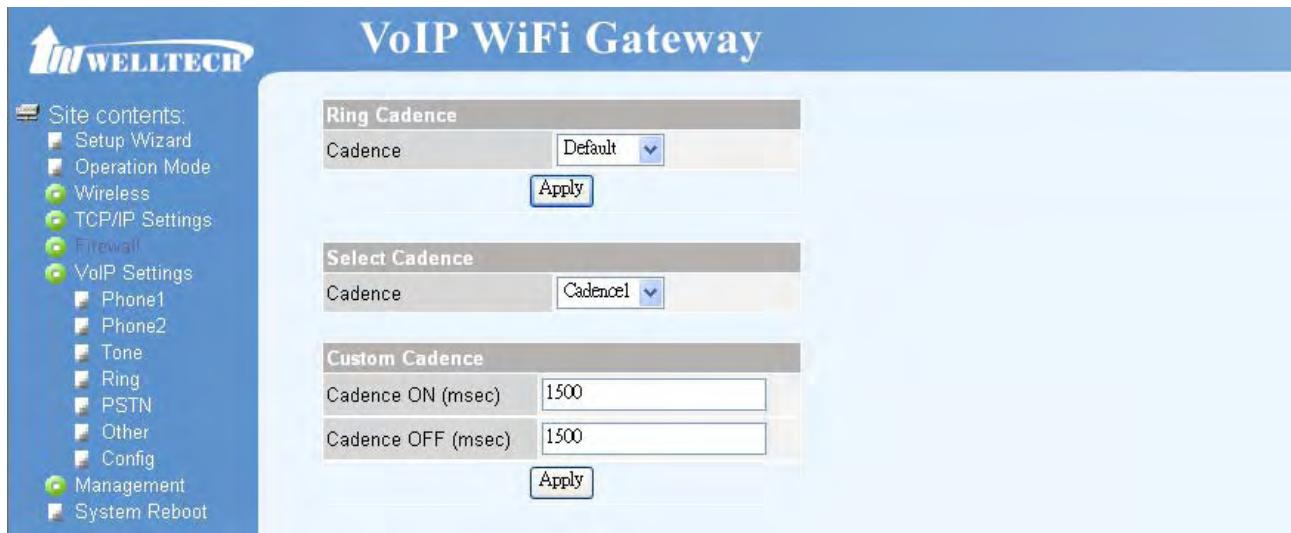
tone will be played for 100ms.

- 2) CanOff: set cadence time for tone not to play in ms. For example, if set CanOff as 100, the tone will stop playing for 100ms.
- 3) Freq1: set first set of tone frequency in Hz.
- 4) Freq2: set second set of tone frequency in Hz. This frequency is optional.
- 5) Gain1: set volume level of Freq1 in dB (-7~-10). Please set this parameter under zero and suggested to set between -7 to -10.
- 6) Gain2: set volume level of Freq2 in dB (-7~-10). Please set this parameter under zero and suggested to set between -7 to -10.



■ Ring

- Ring Cadence-Cadence: Set Ring cadence for PSTN port. User can set 8 sets of cadence value and select one set to be system Ring cadence.
- Select Cadence: Select which cadence to set value.
- Custom Cadence: Set ring cadence ON/OFF time in mini-second.



The screenshot shows the 'Ring Cadence' configuration page. It includes three sections: 'Ring Cadence' (with a dropdown menu set to 'Default' and an 'Apply' button), 'Select Cadence' (with a dropdown menu set to 'Cadence1' and an 'Apply' button), and 'Custom Cadence' (with input fields for 'Cadence ON (msec)' set to 1500 and 'Cadence OFF (msec)' set to 1500, and an 'Apply' button). The left sidebar lists various configuration options under 'Site contents'.

■ PSTN

Set hotkey to switch to PSTN line. Please notice that the key must be *+0~9. When user wants to dial out from PSTN line, press this special key first, phone will pass to PSTN line.



The screenshot shows the 'PSTN Setting' configuration page. It features a red warning message: 'Function Key: Must be * + 0~9'. Below it is a dropdown menu for 'Switch to PSTN' set to '*0' (default: *0), with an 'Apply' and 'Reset' button. The left sidebar lists various configuration options under 'Site contents'.

■ Other

- Call Transfer: Set call transfer function key.
- Auto Dial Time: Set Auto dial time. When user finish input number after this time, Gateway will dial out immediately.

If the call is ended by "#", the call will be sent immediately and you do not need to wait for the Auto Dial Time.

- Off-Hook Alarm: Set off-hook alarm time. If phone set has been off-hook, after this time, from phone set will hear alarm.
- OoS: You can define the DSCP code here for SIP and RTP. Higher DSCP, higher priority.

When DSCP is defined, a DSCP will be added in SIP and RTP packets, and the priority of voice should be higher than data.

➤ VLAN

- 1) VLAN Packets: Check to enable VLAN function.
- 2) VLAN ID: Set VLAN ID.
- 3) User Priority: Set user priority.
- 4) CFI: Set CFI (canonical format indicator).



The screenshot shows the 'VoIP WiFi Gateway' configuration interface. On the left is a navigation menu with the following items:

- Site contents:
 - Setup Wizard
 - Operation Mode
 - Wireless
 - TCP/IP Settings
 - Firewall
 - VoIP Settings
 - Phone1
 - Phone2
 - Tone
 - Ring
 - PSTN
 - Other
 - Config
 - Management
 - System Reboot

The main configuration area is titled 'VLAN Tags for Voice and Data' and contains the following settings:

Use VLAN Tags	<input checked="" type="checkbox"/> Enable
Voice: VLAN ID	5 (1~4093)
Voice: User Priority	5 (0~7)
Voice: CFI	0 (0~1)
Data: VLAN ID	5 (1~4093)
Data: User Priority	0 (0~7)
Data: CFI	0 (0~1)

At the bottom are 'Apply' and 'Reset' buttons.

■ **Config**

- Save Settings to File: Save current VoIP settings to a file.
- Load Settings from File: Browse and load setting from file.
- Reset Settings to Default: Press **Reset** to reset settings of VoIP to default values.



The screenshot shows the 'Save/Reload Setting' page of the VoIP WiFi Gateway. On the left, a sidebar lists 'Site contents' with options like Setup Wizard, Operation Mode, Wireless, TCP/IP Settings, Firewall, VoIP Settings (selected), Management, and System Reboot. The main area has three buttons: 'Save Settings to File' with a 'Save...' button, 'Load Settings from File' with a '瀏覽...' button and 'Upload' button, and 'Reset Settings to Default' with a 'Reset' button.

Management

■ Status

In this page can show the current status and some basic settings of the WG3512.

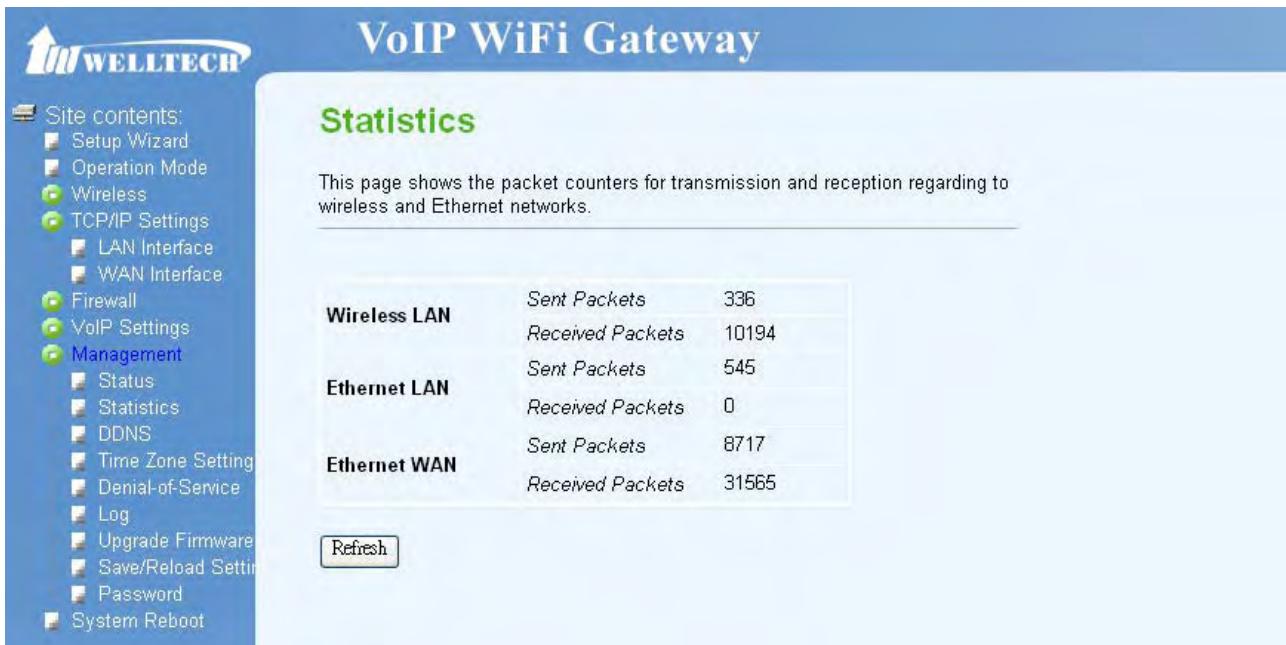


The screenshot shows the 'Access Point Status' page. The sidebar is identical to the previous screenshot. The main area displays the current status and basic settings of the device. A message at the top states: 'This page shows the current status and some basic settings of the device.' Below this, there are three tables: 'System', 'Wireless Configuration', and 'TCP/IP Configuration'. The 'System' table includes Uptime (0day:3h:1m:9s), Firmware Version (2FxSPW.100.bin), and Build Time (Mon Jul 16 13:17:28 CST 2007). The 'Wireless Configuration' table includes Mode (AP), Band (2.4 GHz (B+G)), SSID (WiFi_AP), Channel Number (11), Encryption (Disabled), and BSSID (00:01:a8:04:bd:f6). The 'TCP/IP Configuration' table includes Attain IP Protocol (Fixed IP), IP Address (192.168.123.123), Subnet Mask (255.255.255.0), Default Gateway (192.168.123.123), and DHCP Server (Enabled). At the bottom, there are two more tables: 'MAC Address' (00:01:a8:04:bc:9c) and 'WAN Configuration', which includes Attain IP Protocol (DHCP), IP Address (192.168.15.48), and Subnet Mask (255.255.248.0).

Default Gateway	192.168.8.254
MAC Address	00:01:a8:04:bc:9d
VoIP	
SIP Version	0.7
DSP Version	0.7

■ Statistics

This page shows the packet counters for transmission and reception regarding to wireless and Ethernet networks.



The screenshot shows the 'Statistics' page of the VoIP WiFi Gateway. The left sidebar contains a navigation menu with items like Site contents, Setup Wizard, Operation Mode, Wireless, TCP/IP Settings, LAN Interface, WAN Interface, Firewall, VoIP Settings, Management, Status, Statistics, DDNS, Time Zone Setting, Denial-of-Service, Log, Upgrade Firmware, Save/Reload Settings, Password, and System Reboot. The main content area is titled 'Statistics' and contains a table with packet counts for Wireless LAN, Ethernet LAN, and Ethernet WAN. A 'Refresh' button is at the bottom of the table.

	Sent Packets	Received Packets
Wireless LAN	336	10194
Ethernet LAN	545	0
Ethernet WAN	8717	31565

■ DDNS

Dynamic DNS is a service, which provides you with a valid, unchanging, internet domain name (an URL) to go with that (possibly ever-changing) IP-address. Before setting this page, you should click below link to DynDNS or TZO to apply an account for DDNS.

- **Enable DDNS:** Check to enable DDNS function. User may register to DDNS server for DDNS function.
- **Server Provider:** Select which server provider to implement DDNS function. For now we provide two servers: DynDNS and TZO.
- **Domain Name:** Input the applied domain name for WG3512.
- **User Name/Email:** Input user name for DDNS server login.
- **Password/Key:** Input password for DDNS server login.



Dynamic DNS Setting

Dynamic DNS is a service, that provides you with a valid, unchanging, internet domain name (an URL) to go with that (possibly everchanging) IP-address.

Enable DDNS

Service Provider :

Domain Name :

User Name/Email:

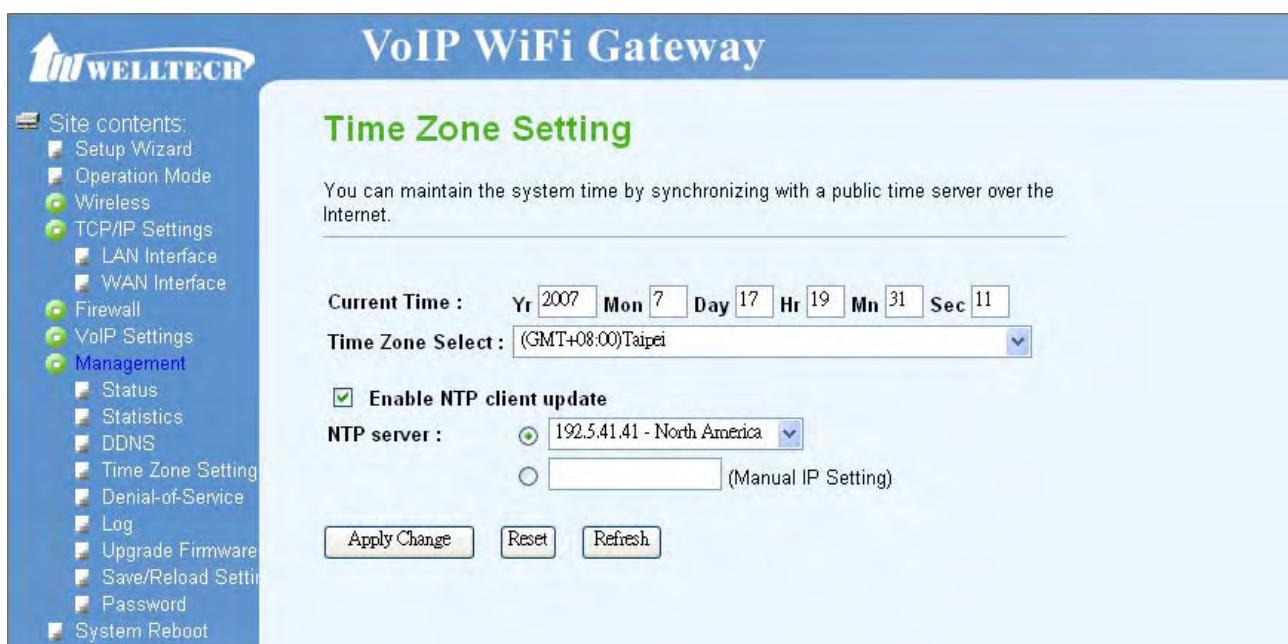
Password/Key:

Note:
For TZO, you can have a 30 days free trial [here](#) or manage your TZO account in [control panel](#)
For DynDNS, you can create your DynDNS account [here](#)

■ Time Zone Setting

You can maintain the system time by synchronizing with a public time server over the Internet.

- Current Time: input current time manually.
- Time Zone Select: select local time zone according to location.
- Enable NTP client update: check to enable NTP update. Once this function is enabled, WG3512 will automatically update current time from NTP server.
- NTP Server: User may select prefer NTP sever or input address of NTP server manually.



Time Zone Setting

You can maintain the system time by synchronizing with a public time server over the Internet.

Current Time : Yr Mon Day Hr Mn Sec

Time Zone Select :

Enable NTP client update

NTP server : 192.5.41.41 - North America (Manual IP Setting)

■ Denial-of-Service

A "denial-of-service" (DoS) attack is characterized by an explicit attempt by hackers to prevent legitimate users of a service from using that service.

- Enable DoS Prevention: Check to enable DoS function.
- User may set other related configurations about DoS below.



Denial of Service

A "denial-of-service" (DoS) attack is characterized by an explicit attempt by hackers to prevent legitimate users of a service from using that service.

Enable DoS Prevention

Whole System Flood: SYN Packets/Second

Whole System Flood: FIN Packets/Second

Whole System Flood: UDP Packets/Second

Whole System Flood: ICMP Packets/Second

Per-Source IP Flood: SYN Packets/Second

Per-Source IP Flood: FIN Packets/Second

Per-Source IP Flood: UDP Packets/Second

Per-Source IP Flood: ICMP Packets/Second

TCP/UDP PortScan Sensitivity

ICMP Smurf

IP Land

IP Spoof

IP TearDrop

PingOfDeath

TCP Scan

TCP SynWithData

UDP Bomb

UDP EchoChadden

Enable Source IP Blocking Block time (sec)

■ Log

This page can be used to set remote log server and show the system log.

- Enable Log: check to enable log function.
- System all/wireless/Dos: select which log you want to check. Related information will be shown at below.
- Enable Remote Log: Once user input Log Server IP Address, all selected log will be restored

in this remote server. This is compatible with Linux Syslog server.



The screenshot shows the 'System Log' configuration page of the VoIP WiFi Gateway. On the left, a sidebar lists various management options. The main area is titled 'System Log' and contains the following configuration:

- Enable Log**
 - system all
 - wireless
 - DoS
- Enable Remote Log**
- Log Server IP Address:**

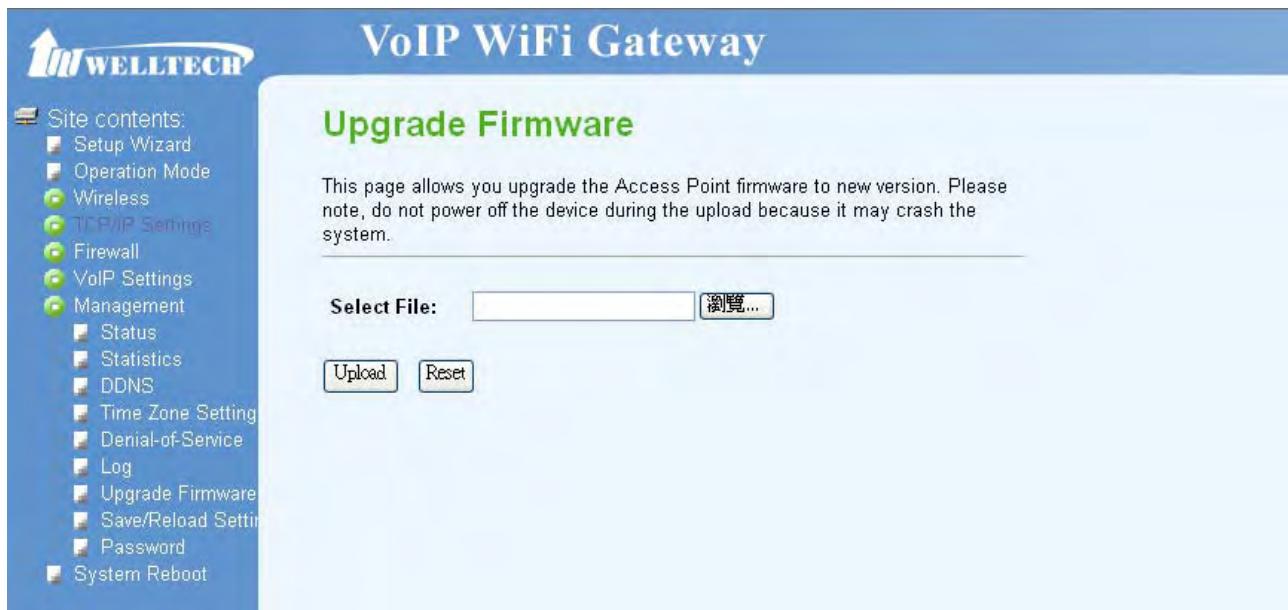
At the bottom of the page are 'Apply Changes' and 'Refresh' buttons.

■ Upgrade Firmware

This page allows you upgrade the Access Point firmware to new version. Please note, do not power off the device during the upload because it may crash the system.

- Select File: browse and select file you want to upgrade and press **Upload** to perform upgrade.

Please wait till on screen shows related information after upgrade finished.



Upgrade Firmware

This page allows you upgrade the Access Point firmware to new version. Please note, do not power off the device during the upload because it may crash the system.

Select File:

■ Save/Reload Settings

This page allows you save current settings to a file or reload the settings from the file which was saved previously. Besides, you could reset the current configuration to factory default.

- Save Settings to File: save current settings to a file.
- Load Settings from File: browse a file and upload to reload settings.
- Reset Settings to Default: press will clean all current configurations and return to default values.



Save/Reload Settings

This page allows you save current settings to a file or reload the settings from the file which was saved previously. Besides, you could reset the current configuration to factory default.

Save Settings to File:

Load Settings from File:

Reset Settings to Default:

■ Password

This page is used to set the account to access the web server of Access Point. Empty user name and password will disable the protection.

- User Name: Enter user name.
- New Password: input password for this user.
- Confirmed Password: confirm password again.



VoIP WiFi Gateway

Password Setup

This page is used to set the account to access the web server of Access Point. Empty user name and password will disable the protection.

User Name:

New Password:

Confirmed Password:

Site contents:

- Setup Wizard
- Operation Mode
- Wireless
- TCP/IP Settings
- Firewall
- VoIP Settings
- Management**
 - Status
 - Statistics
 - DDNS
 - Time Zone Setting
 - Denial-of-Service
 - Log
 - Upgrade Firmware
 - Save/Reload Setting
 - Password
- System Reboot

System Reboot

Press Reboot to reboot system. Please wait for a few minutes and reload web page again.



VoIP WiFi Gateway

System Reboot

Press Reboot to reboot system. Please wait for a few time and reload web page again.

Site contents:

- Setup Wizard
- Operation Mode
- Wireless
- TCP/IP Settings
- Firewall
- VoIP Settings
- Management**
- System Reboot

Chapter 4 Wireless Operation Modes

The WG3512 provides 8 modes for wireless operation, including:

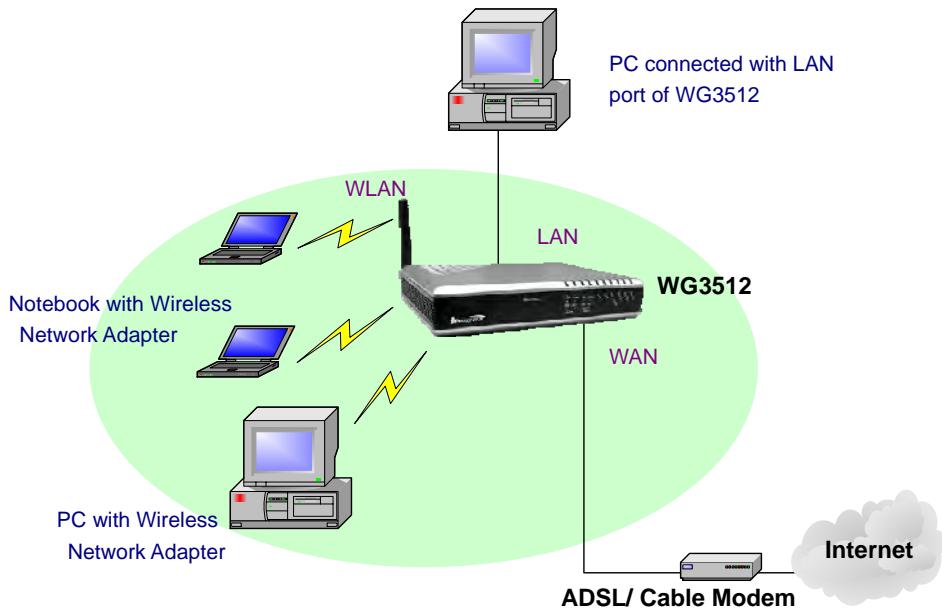
- Access Point: With NAT and Without NAT.
- Client (Infrastructure)
- Client (Ad-hoc)
- P2P Bridge
- WDS Repeater
- Universal Repeater
- WISP
- WISP + Universal Repeater

Here we will guide the purpose and configuration steps for these modes.

Access Point

When acting as Access Point, the WG3512 connects all the stations (PC or Notebook with wireless network adapter) to a wired network. All stations can have the Internet access if only the WG3512 has the Internet connection. In this mode, you can also enable or disable NAT function. Below is example to show you Access Point mode with NAT and Access Point mode with out NAT.

■ Access point with NAT

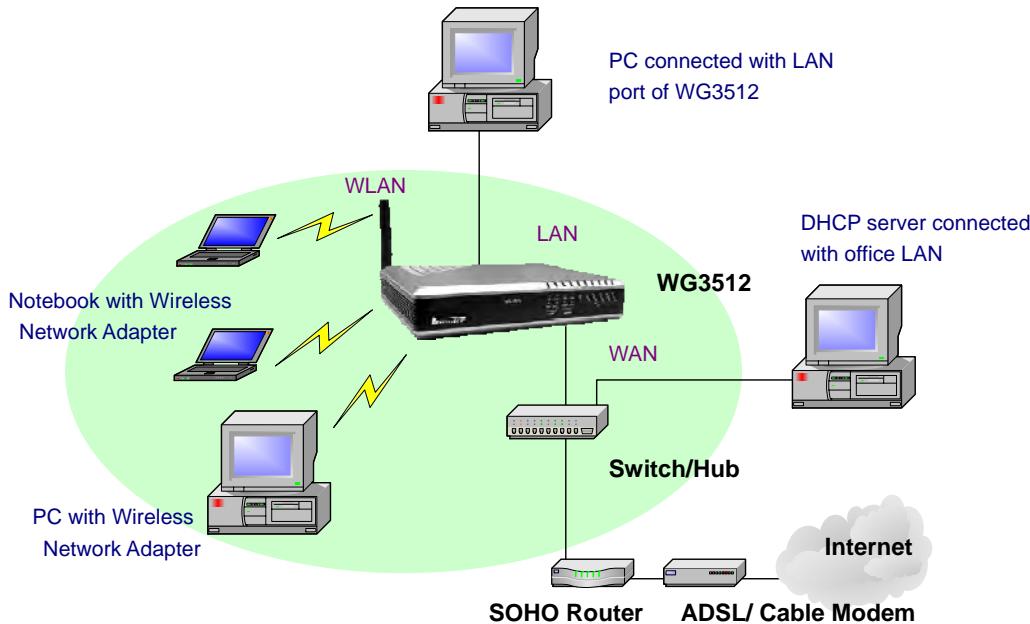


- Step1: Power on WG3512 and set one pc to connect with WG3512. Set PC to DHCP then PC should got an IP as 192.168.123.x by default.
- Step2: Enter 192.168.123.123 for the WEB interface of WG3512 with no login ID and password.
- Step3: Go to the page of Operation, set WG3512 to Gateway mode. In this mode, NAT is

enabled and PCs in LAN ports and WLAN share the same IP to ISP through WAN port.

- Step4: Go to the page of TCP/IP→ WAN set the necessary IP information for WAN.
- Step5: If necessary, go to the page of TCP/IP→ LAN to set the advanced settings for LAN. Such as DHCP server...etc.
- Step6: Go to the page of Wireless→ Basic Settings, set the mode to AP. Please also change the SSID to another name if necessary.
- Step7: We strongly suggest user also go to the page of Wireless→ Security, set the Encryption type and other necessary settings for authentication.
- Step8: At this time, a station could be able to search the WG3512 by WiFi, and that station should be able to access Internet via WG3512.

■ Access point With Bridge mode (Without NAT)



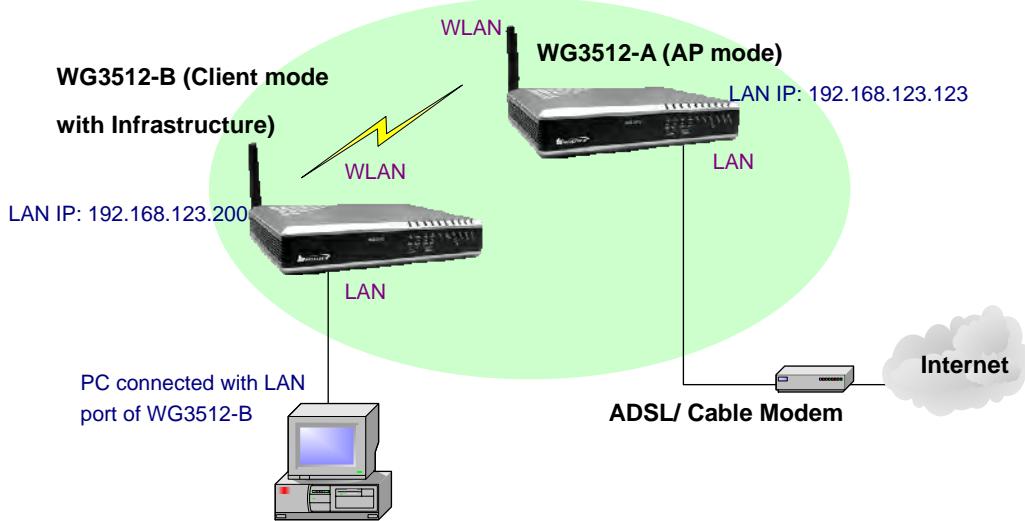
- Step1: Power on WG3512 and set one pc to connect with WG3512. Set PC to DHCP then PC should got an IP as 192.168.123.x by default.
- Step2: Enter 192.168.123.123 for the WEB interface of WG3512 with no login ID and password.
- Step3: Go to the page of Operation, set WG3512 to Bridge mode. In this mode, all Ethernet ports and wireless interface are bridged together and NAT function is disabled. **All the WAN related function and firewall are not supported.**
- Step4: When Bridge mode is enabled, the WAN configuration is disabled, so please go to the page of TCP/IP→ LAN to set the network settings to connect with your Office LAN. And you may also need to disable DHCP server function of WG3512, otherwise there may 2 DHCP

servers exist in your Office LAN and your PCs may get IP from a wrong DHCP server.

- Step5: Please renew the IP settings of the PC which connect with the LAN port of 3512. Then the PC should get new IP from the DHCP server which connected with your Office LAN.
- Step6: Go to the page of Wireless→ Basic Settings, set the mode to AP. Please also change the SSID to another name if necessary.
- Step7: We strongly suggest user also go to the page of Wireless→ Security, set the Encryption type and other necessary settings.
- Step8: At this time, a station could be able to search the WG3512 by WiFi, and that station should be able to access Internet via WG3512.

Client (Infrastructure)

If Client (Infrastructure) is enabled, the WG3512 can work like a wireless station when it's connected to a computer so that the computer can send packets from wired to wireless interface. Below is an example to show you how to implement Client (infrastructure) mode.



In WG3512-A, it is working as Access point with NAT.

In WG3512-B, it is working as Client mode with Infrastructure. The configure steps is as below.

- Step1: Power on WG3512-B and set one pc to connect with WG3512-B. Set PC to a Fixed IP, such as 192.168.123.100.
- Step2: Enter 192.168.123.123 for the WEB interface of WG3512-B with no login ID and password.
- Step3: Go to the page of Operation, set WG3512 to Bridge mode. In this mode, all Ethernet ports and wireless interface are bridged together and NAT function is disabled. **All the WAN related function and firewall are not supported.**
- Step4: When Bridge mode is enabled, the WAN configuration is disabled, so please go to the

page of TCP/IP→ LAN to set the network settings to connect with WG3512-A. Maybe you could set the IP to 192.168.123.200 and set Default Gateway to 192.168.123.123.

- Step5: Go to the page of Wireless→ Basic Settings, set the mode to Client and set the Network Type to Infrastructure.
- Step6: Go to the page of Wireless→ Security, to set the necessary authentication method for WG3512-A if WG3512-A has enable authentication.
- Step7: Go to the page of Wireless→ Site Survey to search and connect to WG3512-A. When connection is OK, there should be a successful message appeared.
- Step8: At this time, the PC connected to the LAN of WG3512-B could be able to reach the WG3512-A, and access Internet via it.

Client (Ad-hoc)

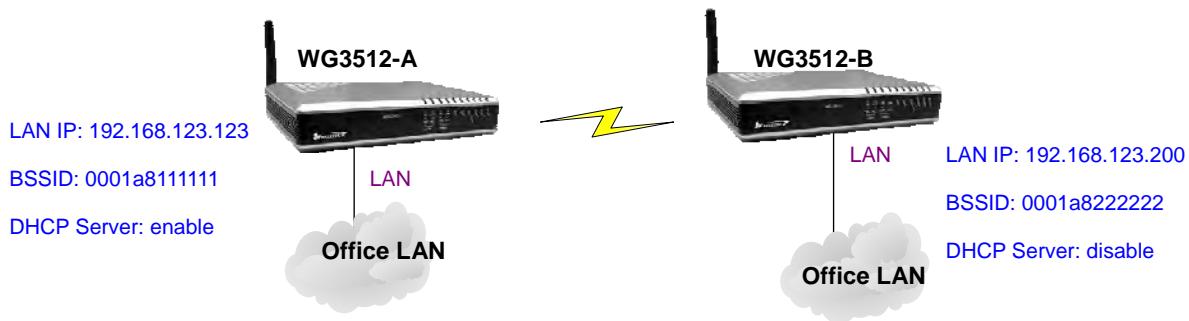
If Client (Ad-hoc) is enabled, the WG3512 can work like a wireless station when it's connected to a computer so that the computer can send packets from wired to wireless interface. You can share files and printers between wireless stations. Below is an example to show you how to implement Client (Ad-hoc) mode.



- Step1: Power on WG3512 and set one pc to connect with WG3512. Set PC to a Fixed IP, such as 192.168.123.100.
- Step2: Enter 192.168.123.123 for the WEB interface of WG3512 with no login ID and password.
- Step3: Go to the page of Wireless→ Basic Settings, set the mode to Client and set the Network Type to Ad-hoc.
- Step4: Go to the page of Wireless→ Security, to set the necessary authentication method.
- Step5: At this time, the PC or Notebook with wireless network adapter should be able to search the WG3512 and use WiFi to send packets to PC connected to the LAN of WG3512.

P2P Bridge

In this mode, 2 access points in two remote locations connect to each other to provide a wireless bridge between 2 remote LANs. It is mostly used by enterprise to connect 2 remote office's network together. This feature is also useful when users want to bridge networks between buildings where it is impossible to deploy network cable connections between these buildings. The P2P Bridge should be connected by using WDS Repeater. Below is an example to show you how to implement WG3512 with P2P Bridge.



In WG3512-A:

- Step1: Power on WG3512-A and set one pc to connect with WG3512-A's LAN. Set PC to DHCP then PC should got an IP as 192.168.123.x by default.
- Step2: Enter 192.168.123.123 for the WEB interface of WG3512-A with no login ID and password.
- Step3: Go to the page of Operation, set WG3512-A to Bridge mode. In this mode, all Ethernet ports and wireless interface are bridged together and NAT function is disabled. **All the WAN related function and firewall are not supported.**
- Step4: When Bridge mode is enabled, the WAN configuration is disabled, so please go to the page of TCP/IP→ LAN to set the network settings to connect with your Office LAN.
- Step5: Go to the page of Wireless→ Basic Settings, set the mode to WDS. Set the Channel to a fixed one, such as 11.
- Step6: Go to the page of Wireless→ WDS Settings, enable WDS and input the WG3512-B's MAC address (BSSID) into the WDS table.

In WG3512-B:

- Step1: Power on WG3512-B and set one pc to connect with WG3512-B. Set PC to a Fixed IP, such as 192.168.123.100.
- Step2: Enter 192.168.123.123 for the WEB interface of WG3512-B with no login ID and password.
- Step3: Go to the page of Operation, set WG3512 to Bridge mode. In this mode, all Ethernet ports and wireless interface are bridged together and NAT function is disabled. **All the WAN related function and firewall are not supported.**

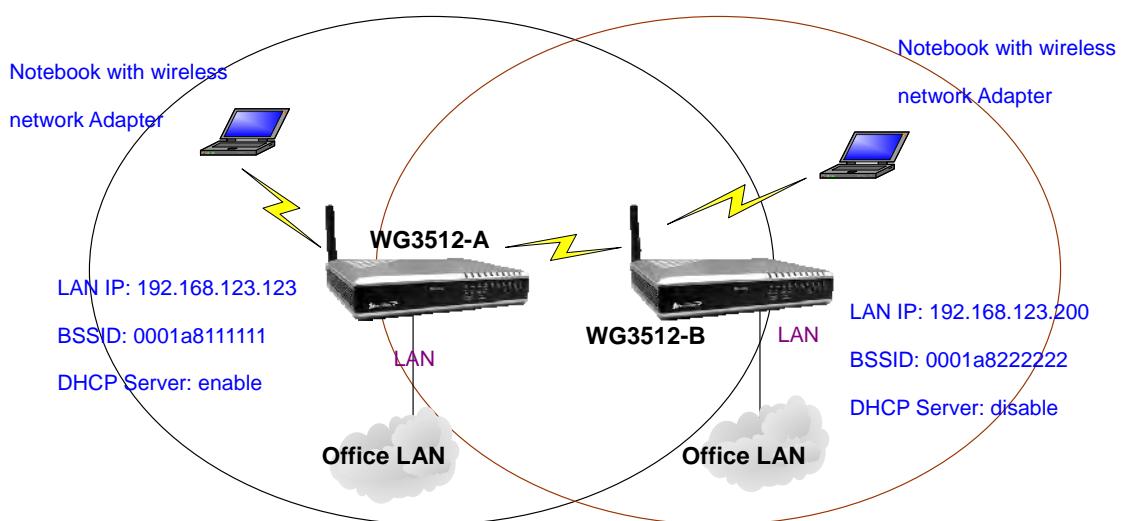
- Step4: When Bridge mode is enabled, the WAN configuration is disabled, so please go to the page of TCP/IP→ LAN to set the network settings to connect with your Office LAN. In this example, we set the LAN IP to 192.168.123.200 and DHCP is disabled.
- Step5: Login 192.168.123.200. Go to the page of Wireless→ Basic Settings, set the mode to WDS. Set the Channel to a fixed one, such as 11.
- Step6: Go to the page of Wireless→ WDS Settings, enable WDS and input the WG3512-A's MAC address (BSSID) into the WDS table.
- Step7: If configuration ok, both office LAN should have the same subnet (192.168.123.x), and the PCs of both office LAN could send packets to each other via WDS Repeater connection.

Note:

- **When both WG3512-A and WG3512-B has been setup successfully, you could go to the page of Wireless→ WDS Settings→ Show Statics, to confirm the WDS Statics.**
- **P2P Bridge should use WDS for WiFi connection. When WDS is enable, both WG3512 need to have the same channel. And you should set the WDS table for each other.**
- **When you set the mode to WDS, the AP function will be disable. If you hope the AP still be workable, please choose the mode to AP+WDS and the SSID of both WG3512 could be the same or different.**

WDS Repeater

A repeater's function is to extend the wireless coverage of another wireless AP or router. For WDS repeater to work, the remote wireless AP/Router should also support WDS. Below is an example to show you how to implement WDS plus AP with Bridge mode.



In WG3512-A:

- Step1: Power on WG3512-A and set one pc to connect with WG3512-A's LAN. Set PC to DHCP then PC should got an IP as 192.168.123.x by default.

- Step2: Enter 192.168.123.123 for the WEB interface of WG3512-A with no login ID and password.
- Step3: Go to the page of Operation, set WG3512-A to Bridge mode. In this mode, all Ethernet ports and wireless interface are bridged together and NAT function is disabled. **All the WAN related function and firewall are not supported.**
- Step4: When Bridge mode is enabled, the WAN configuration is disabled, so please go to the page of TCP/IP→ LAN to set the network settings to connect with your Office LAN.
- Step5: Go to the page of Wireless→ Basic Settings, set the mode to AP+WDS. Set the Channel to a fixed one, such as 11.
- Step6: Go to the page of Wireless→ Security to set the authentication method if necessary.
- Step7: Go to the page of Wireless→ WDS Settings, enable WDS and input the WG3512-B's MAC address (BSSID) into the WDS table.

In WG3512-B:

- Step1: Power on WG3512-B and set one pc to connect with WG3512-B. Set PC to a Fixed IP, such as 192.168.123.100.
- Step2: Enter 192.168.123.123 for the WEB interface of WG3512-B with no login ID and password.
- Step3: Go to the page of Operation, set WG3512 to Bridge mode. In this mode, all Ethernet ports and wireless interface are bridged together and NAT function is disabled. **All the WAN related function and firewall are not supported.**
- Step4: When Bridge mode is enabled, the WAN configuration is disabled, so please go to the page of TCP/IP→ LAN to set the network settings to connect with your Office LAN. In this example, we set the LAN IP to 192.168.123.200 and DHCP is disabled.
- Step5: Go to the page of Wireless→ Basic Settings, set the mode to AP+WDS. Set the Channel to a fixed one, such as 11.
- Step6: Go to the page of Wireless→ Security to set the authentication method if necessary.
- Step7: Go to the page of Wireless→ WDS Settings, enable WDS and input the WG3512-A's MAC address (BSSID) into the WDS table.
- Step8: If configuration ok, both office LAN should have the same subnet (192.168.123.x), and the PCs of both office LAN could send packets to each other via WDS connection. The notebook with wireless network adapter could also roam between 2 APs and access both the Office LAN.

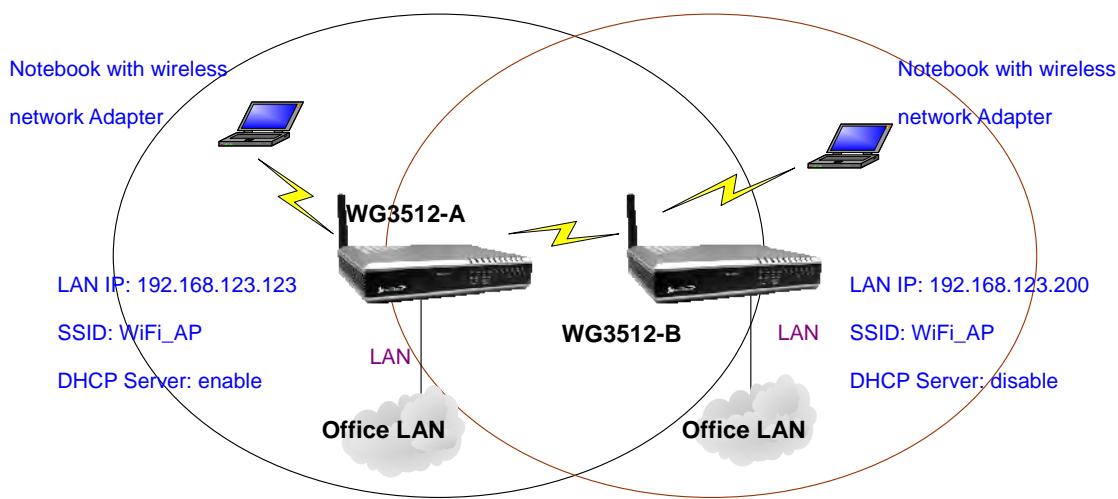
Note:

- **When both WG3512-A and WG3512-B has been setup successfully, you could go to the page of Wireless→ WDS Settings→ Show Statics, to confirm the WDS Statics.**
- **When WDS is enabled, both WG3512 need to have the same channel, the SSID of both**

WG3512 could be the same or different. And you should set the WDS table for each other.

Universal Repeater

A Universal repeater can also extend the wireless coverage of another wireless AP or router. But the Universal Repeater does not require the remote side to have WDS function. Below is an example to show you how to implement Universal Repeater with Bridge mode.



In WG3512-A:

- Step1: Power on WG3512-A and set one pc to connect with WG3512-A's LAN. Set PC to DHCP then PC should got an IP as 192.168.123.x by default.
- Step2: Enter 192.168.123.123 for the WEB interface of WG3512-A with no login ID and password.
- Step3: Go to the page of Operation, set WG3512-A to Bridge mode. In this mode, all Ethernet ports and wireless interface are bridged together and NAT function is disabled. **All the WAN related function and firewall are not supported.**
- Step4: When Bridge mode is enabled, the WAN configuration is disabled, so please go to the page of TCP/IP→ LAN to set the network settings to connect with your Office LAN.
- Step5: Go to the page of Wireless→ Basic Settings, set the mode to AP. Set the Channel to a fixed one, such as 11. Disable the “Enable Universal Repeater Mode (Acting as AP and client simultaneously)”.
- Step6: Go to the page of Wireless→ Security to set the authentication method if necessary.

In WG3512-B:

- Step1: Power on WG3512-B and set one pc to connect with WG3512-B. Set PC to a Fixed IP, such as 192.168.123.100.
- Step2: Enter 192.168.123.123 for the WEB interface of WG3512-B with no login ID and

password.

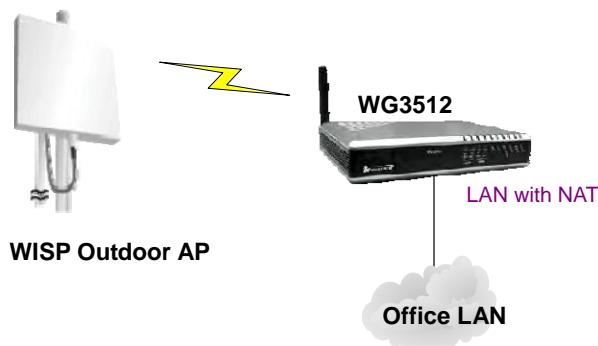
- Step3: Go to the page of Operation, set WG3512 to Bridge mode. In this mode, all Ethernet ports and wireless interface are bridged together and NAT function is disabled. **All the WAN related function and firewall are not supported.**
- Step4: When Bridge mode is enabled, the WAN configuration is disabled, so please go to the page of TCP/IP→ LAN to set the network settings to connect with your Office LAN. In this example, we set the LAN IP to 192.168.123.200 and DHCP is disabled.
- Step5: Go to the page of Wireless→ Basic Settings, set the mode to AP. Set the Channel to a fixed one, such as 11. Enable the “Enable Universal Repeater Mode (Acting as AP and client simultaneously)” and input the WG3512-A’s SSID (WiFi-AP).
- Step6: Go to the page of Wireless→ Security to set the authentication method if necessary.
- Step7: If configuration ok, both office LAN should have the same subnet (192.168.123.x), and the PCs of both office LAN could send packets to each other via Universal Repeater connection. The notebook with wireless network adapter could also roam between 2 APs and access both the Office LAN.

Note:

- **When Universal Repeater is enabled, both WG3512 need to have the same channel and the SSID could be same or different.**
- **Please notify that you can only choose one to enable the “Enable Universal Repeater Mode (Acting as AP and client simultaneously)”, otherwise there will be some error occurred.**

WISP

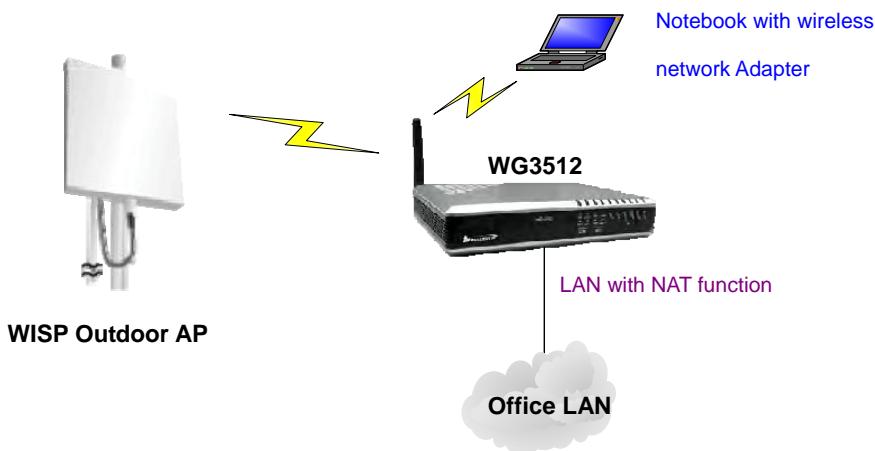
In WISP mode, the AP will behave just the same as the Client (Infrastructure) mode for wireless function. However, route functions are added between the wireless WAN side and Ethernet LAN side. The NAT is enabled and PCs in ethernet ports share the same IP to ISP through wireless LAN. You must set the wireless to client mode first and connect to the ISP AP in Site-Survey page. The connection type can be setup in WAN page by using PPPOE, DHCP client or static IP. Below is an example to show you how to implement WISP mode.



- Step1: Power on WG3512-A and set one pc to connect with WG3512-A's LAN. Set PC to DHCP then PC should got an IP as 192.168.123.x by default.
- Step2: Enter 192.168.123.123 for the WEB interface of WG3512-A with no login ID and password.
- Step3: Go to the page of Operation, set WG3512-A to Wireless ISP mode.
- Step4: Go to the page of Wireless→ Basic Settings, set the mode to Client and set the Network Type to Infrastructure.
- Step5: Go to the page of Wireless→ Security, to set the necessary authentication method for WISP Outdoor AP, if WISP Outdoor AP has enable authentication.
- Step6: Go to the page of Wireless→ Site Survey to search and connect to WISP Outdoor AP. When connection is OK, there should be a successful message appeared.
- Step7: Go to the page of TCP/IP→ WAN to configure the IP settings.
- Step8: If configuration ok, PCs of office LAN could send packets via WISP Outdoor AP.

WISP + Universal Repeater

In this mode, the AP will behave same as the WISP mode for wireless function except one thing: the WG3512 can also work as a AP. However, route functions are added between the wireless WAN side and Ethernet LAN side. The NAT is enabled and PCs in ethernet ports share the same IP to ISP through wireless LAN. You must set the wireless to client mode first and connect to the ISP AP in Site-Survey page. The connection type can be setup in WAN page by using PPPOE, DHCP client or static IP. Below is an example to show you how to implement WISP mode.



- Step1: Power on WG3512-A and set one pc to connect with WG3512-A's LAN. Set PC to DHCP then PC should got an IP as 192.168.123.x by default.
- Step2: Enter 192.168.123.123 for the WEB interface of WG3512-A with no login ID and password.
- Step3: Go to the page of Operation, set WG3512-A to Gateway mode.

- Step4: Go to the page of Wireless→ Basic Settings, set the mode to Client and set the Network Type to Infrastructure.
- Step5: Go to the page of Wireless→ Security, to set the necessary authentication method for WISP Outdoor AP, if WISP Outdoor AP has enable authentication.
- Step6: Go to the page of Wireless→ Site Survey to search and connect to WISP Outdoor AP. When connection is OK, there should be a successful message appeared.
- Step7: Go to the page of TCP/IP→ WAN to configure the IP settings.
- Step8: Go to the page of Wireless→ Basic Settings, enable the “Enable Universal Repeater Mode (Acting as AP and client simultaneouly)” and input the WISP Outdoor AP's SSID.
- Step9: If configuration ok, PCs of office LAN could send packets via WISP Outdoor AP. And the Notebook of the WG3512's WLAN should be also use WiFi to access internet via WISP Outdoor AP.



FCC COMPLIANCE

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: WellGate 3512 Technical Manual EN-V1.00

- (1) This device may not cause harmful interference, and**
- (2) This device must accept any interference received, including interference that may cause undesired operation.**

This equipment must be installed and operated in accordance with provided instructions and the antenna(s) used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter. End-users and installers must be provide with antenna installation instructions and transmitter operating conditions for satisfying RF exposure compliance.

NOTE: THE MANUFACTURER IS NOT RESPONSIBLE FOR ANY RADIO OR TV INTERFERENCE CAUSED BY UNAUTHORIZED MODIFICATIONS TO THIS EQUIPMENT. SUCH MODIFICATIONS COULD VOID THE USER'S AUTHORITY TO OPERATE THE EQUIPMENT.