11n Wireless Broadband Router

User's Manual

APRIL 2011

FCC Warning

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

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

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment. This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

IMPORTANT NOTE:

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of about eight inches (20cm) between the radiator and your body. This transmitter must not be co-located or operated in conjunction with any other antenna or transmitter. IEEE802.11b or 802.11g operation of this product in the USA is firmware-limited to channels 1 through 11.

Notice

Changes or modifications to the equipment, which are not approved by the party responsible for compliance could affect the user's authority to operate the equipment. Company has an on-going policy of upgrading its products and it may be possible that information in this

document is not up-to-date. Please check with your local distributors for the latest information.

Copyright

Revision History

Revision	History
V1	1st Release

Table of Contents

1. Introduction

This Wireless Broadband Router complies with IEEE 802.11n, and provides faster and farther range than 802.11g while being backward compatible with 802.11g and 802.11b mode. This router uses advanced broadband router chipset and wireless LAN chipset solution to let you enjoy high-speed Wired and Wireless connection. Simply connect this device to a Cable or DSL modem and then you can share your high-speed Internet access with multiple PCs at your home with or without wires. It creates a secure Wired and Wireless network for you to share photos, files, video, music, printer and network storage. WR750R provides maximum transfer rate up to 150Mbps and supports WEP, WPA, WPA2, WPS, 802.1x high-level WLAN security features that guarantee the best security for users.

This product is made in ISO9001 approved factory and complies with FCC part 15 regulations and CE approval.

1.1 Features

- Up to 150 Mbps data transfer rates at 802.11n (Wireless)
- Backward compatible with IEEE 802.11b/g
- Built-in 4 port 10/100 Ethernet switch with auto speed sensing
- Supports NAT, NAPT, DHCP Server/Client
- Supports VPN pass through - IPSec, PPTP, L2TP
- Supports Virtual Server / Port Trigger
- Supports Virtual DMZ Host, DNS Proxy, DDNS, UPnP
- Supports 64/128-bit WEP Data Encryption
- Supports WPA / WPA2 / WPS / 802.1x Authentication
- Supports WDS (Wireless Distribution System) mode
- Supports MAC Filter, Client Filter, URL/IP Filter
- Supports Auto-crossover (MDI/MID-X) function
- Supports software upgrade through Web
- Friendly web-based GUI Configuration and Management
-

1.2 Specifications

Data Transfer Rates	300 Mbps (802.11n mode) 54Mbps (802.11g mode) 11Mbps (802.11b mode)

Standard	IEEE 802.11b / 802.11g / 802.11n (Wireless) IEEE 802.3, IEEE 802.3u, IEEE 802.3x Full Duplex Flow Control (Wired)
Operating Radius	100M Indoor, 400M Outdoor
Internet Access	Connect to Broadband (Cable or xDSL) modem or Ethernet backbone for Internet Surfing
WAN Connection	Dynamic IP, Static IP, PPPoE, PPTP, L2TP
IP Management	NAT (Network Address Translation) NAPT (Network Address and Port Translation) DHCP (Dynamic Host Configuration Protocol) Server/Client Support VPN pass through – IPSec, PPTP, L2TP Support Virtual server / Port Trigger Support Virtual DMZ host Support DNS Proxy Support Dynamic DNS Support UPnP (Internet Gate Device)
Security	Support 64/128-bit WEP Data Encryption Support WPA, WPA2 (802.11i) security Support MAC ACL (MAC Access Control List) Support WDS (Wireless Distribution System) Support WPS (Wi-Fi Protected Setup). Support PAP / CHAP / MS-CHAP / MS-CHAPv2 authentication Support 802.1x RADIUS Server
Firewall	Support MAC filter Support IP filter Support URL blocking Support NAT Protection Support Hacker pattern filter (Port Scan , Land attack, DOS...etc)
Management	Web-based GUI Configuration / Management Telnet remote management / Web Remote Login from WAN. Software Upgrade through Web Support NTP update. Support System Log

	Support Configuration setting Backup/Restore/Reset Default
Interface	LAN x 4, WAN x 1, USB2.0
LED Indicators	POWER, STATUS, LAN x 4, WAN x 1, WLAN x 1
Antenna	1 Antennas
Wireless Frequency	2.4000~2.4835GHz
Output Power	15 dBm
Receiver Sensitivity	IEEE 802.11b : -88 dBm (Typical), IEEE 802.11g : -70dBm (Typical) IEEE 802.11n: 20Mhz -68dBm ; 40Mhz -65dBm (Typical)
Transmit Output Power	11b : 18±1 dBm, 11g : 15±1 dBm , 11n : 15±1 dBm
Power	DC 5V, 2A
Operating Temperature	0°C ~ 40°C
Humidity	5 % ~ 95 % (non-condensing)
Storage Temperature	0°C ~ 70°C
Supported OS	Windows 98SE, ME, 2000, XP, Vista, Win7, Mac and Linux
Regulations	FCC, CE
RoHS Compliant	RoHS Compliant

1.3 Package Contents

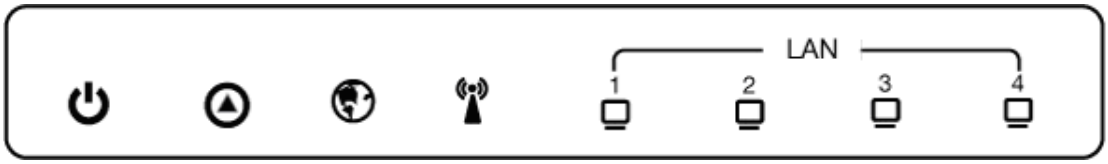
- One Wireless AP Router with 2 antennas
- One External Power Adapter
- One CD-ROM (user's manual)
- One RJ-45 Ethernet Cable

1.4 System Requirements

- Computers with an installed Ethernet adapter.
- Valid Internet Access account and Ethernet based DSL or Cable modem.
- 10/100Base-T Ethernet cable with RJ-45 connector.
- TCP/IP protocol must be installed on all PCs.
- System with MS Internet Explorer ver. 5.0 or later, or Netscape Navigator ver. 4.7 or later.

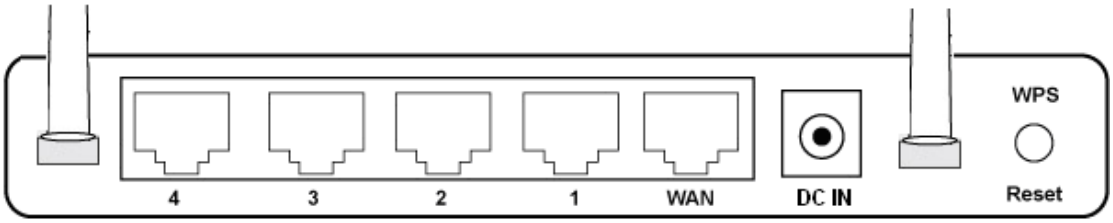
1.5 LEDs Indication & Connectors of Wireless Router

Front Panel LEDs Indication



LED	Light Status	Description
PWR	On	Wireless Router is powered on.
	Off	Wireless Router is powered off.
Status	On (Steady Green)	Reset: When the router is resenting the configuration, the light will steady on
	Slow Blinking	Status: System is up and ready.
	Flashing	WPS: When the router is connecting a pc of wireless adapter with WPS function.
WAN	On	WAN port is successfully connected
	Blinking	Data is being sent or received.
WLAN	Slow Blinking	WLAN is successfully connected.
	Blinking	Data is being sent or received.
LAN (1, 2, 3, 4)	On	LAN port is successfully connected.
	Blinking	Data is being sent or received.

Back Panel Connectors



Button/Port	Description
Reset	Reset configurations to default. You would use the reset button only when a program error has caused your Wireless AP router to hang. Press the button and hold after 6 seconds.
WPS	Click WPS button 1 to 3 seconds while you are connecting a PC of wireless adapter with WPS function (you must enable WPS' PBC function).
LAN (1x, 2x, 3x, 4x)	Ethernet RJ-45 connector, connect to PC with a RJ-45 Ethernet cable.
WAN	Ethernet RJ-45 connector, connect to WAN access device, such as the

	Cable modem or ADSL modem.
DC-IN	Power connector, connect to the power adapter (DC-5V, 2A) packaged with the AP router.
USB 	Connect the 3G/3.5G USB device to USB Port. The 3G/3.5G USB port locates at right-side of the wireless router.

1.6 Installation Instruction

1) Power off 802.11n AP Router and DSL/Cable modem.
2) Connect computer to the LAN port on the Wireless Router with Ethernet cable.
3) Connect the DSL or Cable modem to the WAN port on the Wireless Router with Ethernet cable.
4) Power on DSL or Cable modem first, then connect power adapter to the power jack on the rear panel of Wireless Router and plug the power cable into an outlet.
5) Check LEDs.
   a) Once power on Wireless Router, Power LED should be on.
   b) LAN LED should be on for each active LAN connection.
   c) The WAN LED should be on when the DSL or cable modem is connected.

Warning: Only use the power adapter is provided from this package, use other power adapter may cause hardware damage

2. PC Configuration

To communicate and configure 802.11n AP router, the PC on your LAN must install TCP/IP protocol. Make sure the TCP/IP protocol of the PC is configured for Obtain IP address from DHCP and is connected to LAN (Ethernet) port of the AP router. In doing so, the PC obtains an IP address of 192.168.1.1 from 802.11n AP router.

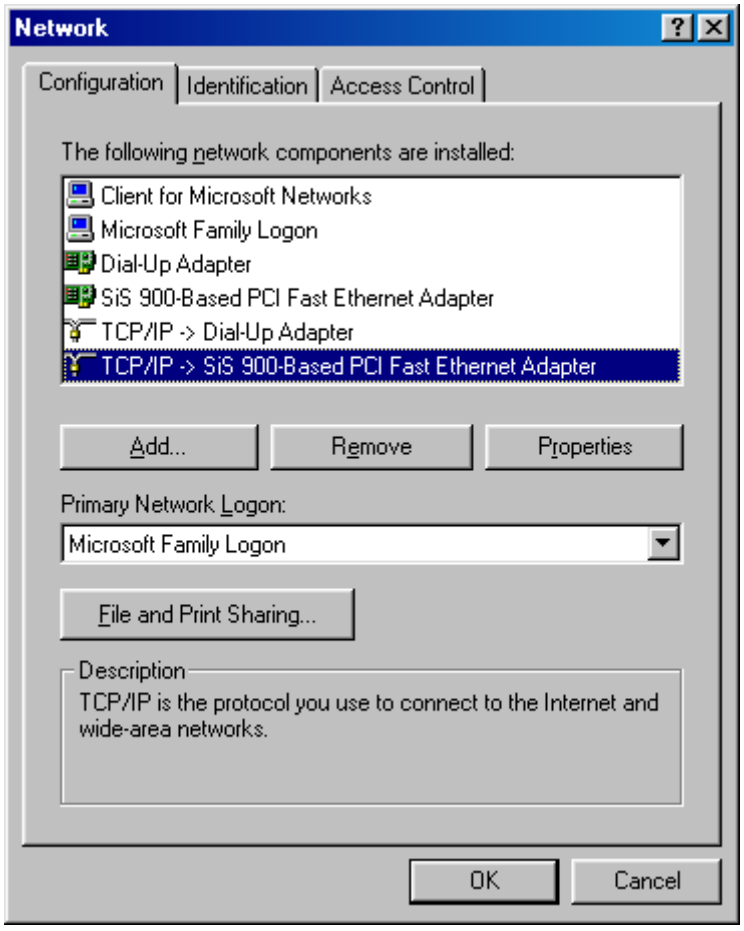
The 802.11n AP router assumes an IP address of 192.168.1.1 without network connectivity. This IP address is used for communicating with the 802.11n AP router via the web UI or Telnet, with the PC connected to the LAN port.

The 802.11n AP router assumes a DHCP IP address on the WAN side if connected to the network. In this case user can communicate with the same IP address 192.168.1.1 with PC connected to the LAN port. PC in the network can communicate with the DHCP IP address allocated to 802.11n router.

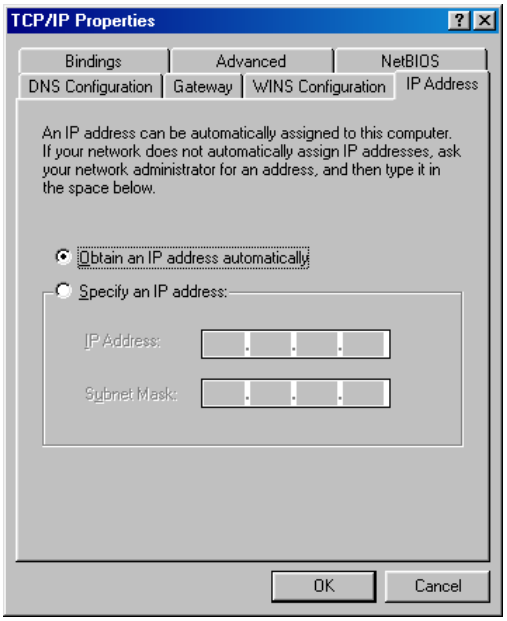
2.1 TCP/IP Networking Setup

Checking TCP/IP Settings for Windows 9x/Me

a) Select **"Start → Control Panel → Network"**, the window below will appear,

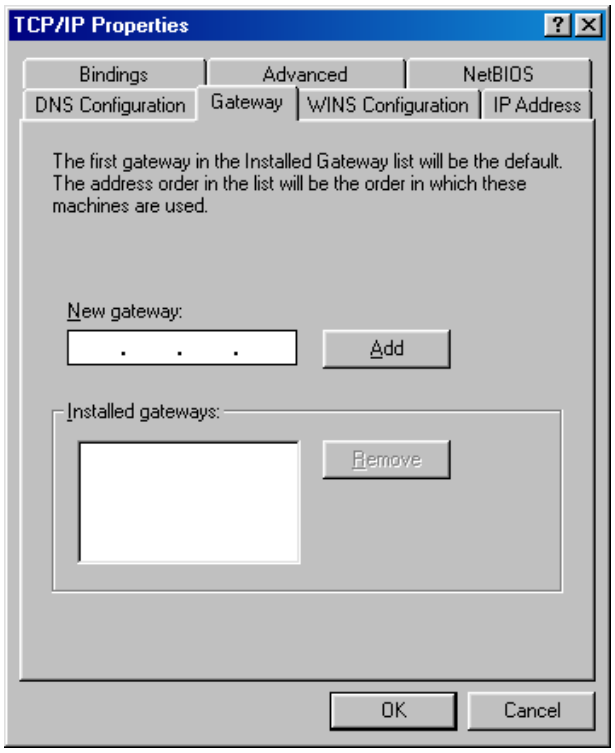


b) Click **"Properties"**, the window below will appear and then click **"IP Address"** tab,

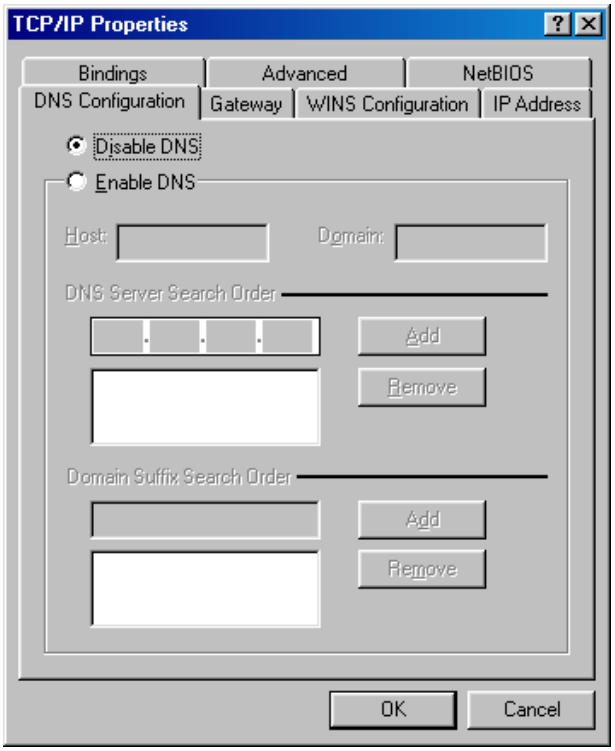


- If you decide to use DHCP, select **"Obtain an IP address automatically"**, then click **"OK"** to confirm your settings. Once you restart your system, Wireless Router will obtain an IP address for this system.
- If you decide to use fixed IP address for your system, select **"Specify an IP address"**, and make sure that **IP Address** and **Subnet Mask** are correct.

c) Select **"Gateway"** tab and enter correct gateway address in **"New gateway"** field, then click **"Add"**,

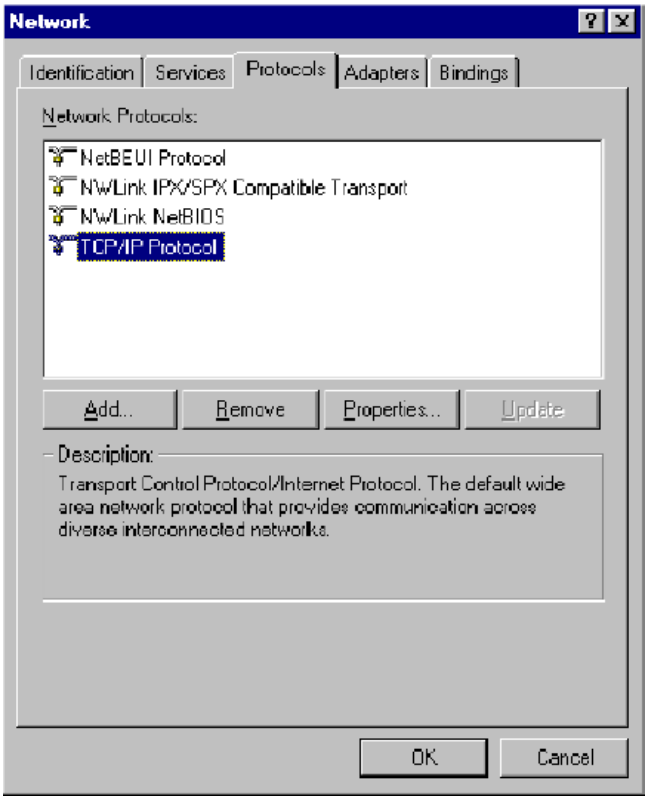


d) Select **"DNS Configuration"** tab and make sure select **"Enable DNS"**, enter the DNS address provides from your ISP in the **"DNS Server Search Order"** field, then click **"Add"**,

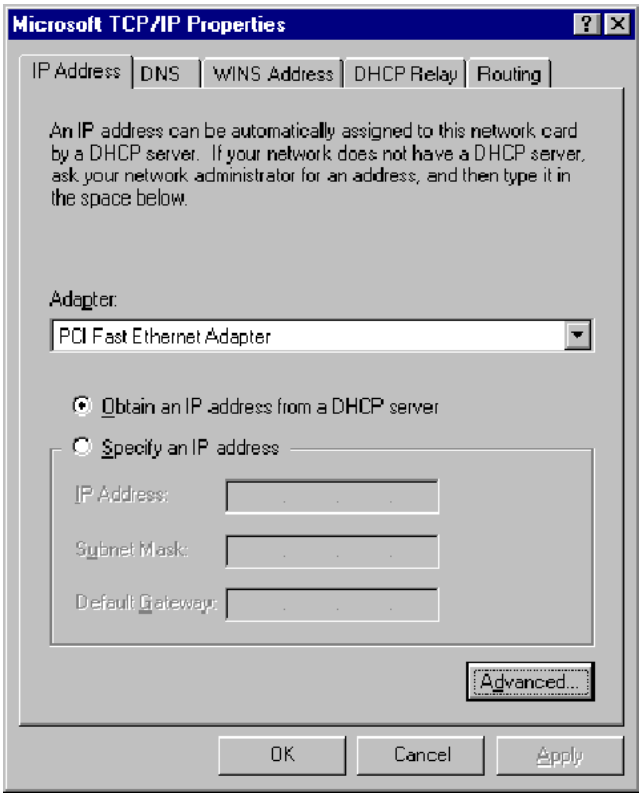


Checking TCI/IP Setting for Windows NT4.0

a) Select "Control Panel → Network", window below will appear, click "Protocols" tab then select "TCP/IP protocol",



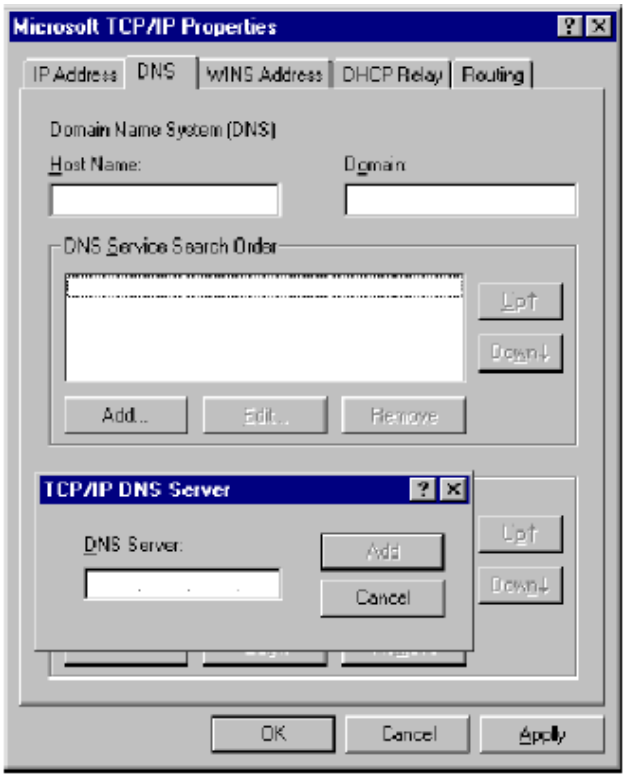
b) Click “Properties”, window below will appear.



- Select the network card on your system from “Adapter” field.
- If you decide to use IP address from Wireless Router, select “Obtain an IP address from a DHCP server”.

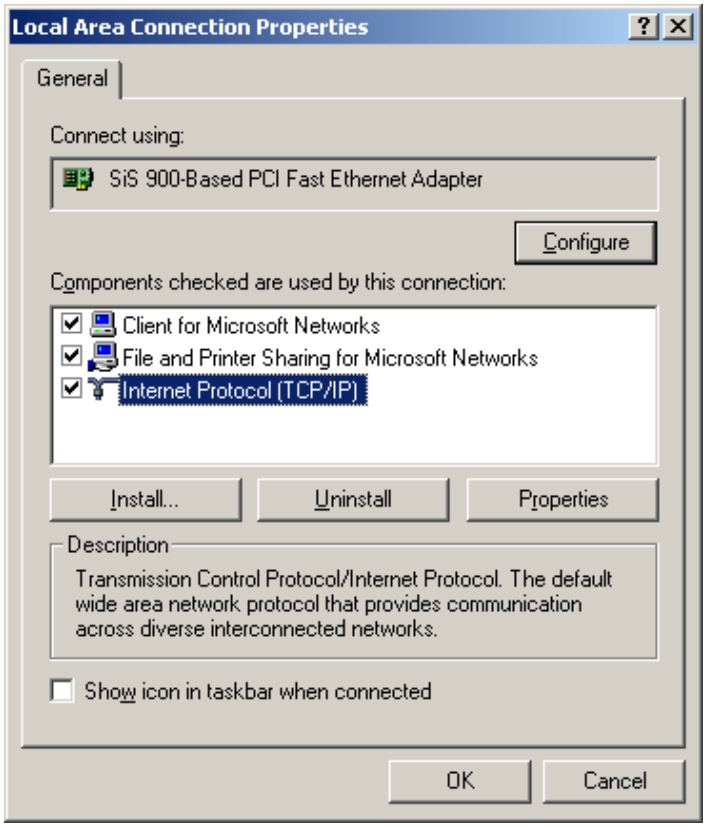
- If you decide to use the IP address you are desired, select “Specify an IP address”. Make sure enter correct addresses in “IP Address” and “Subnet Mask” fields.
- You must set Wireless Router’s IP address as “Default Gateway”.

c) To enter DNS address is provided from your ISP. Select “DNS” tab, click “Add” under “DNS Service Search Order” list, then enter DNS Server IP address in “TCP/IP DNS Server” window and click “Add”.

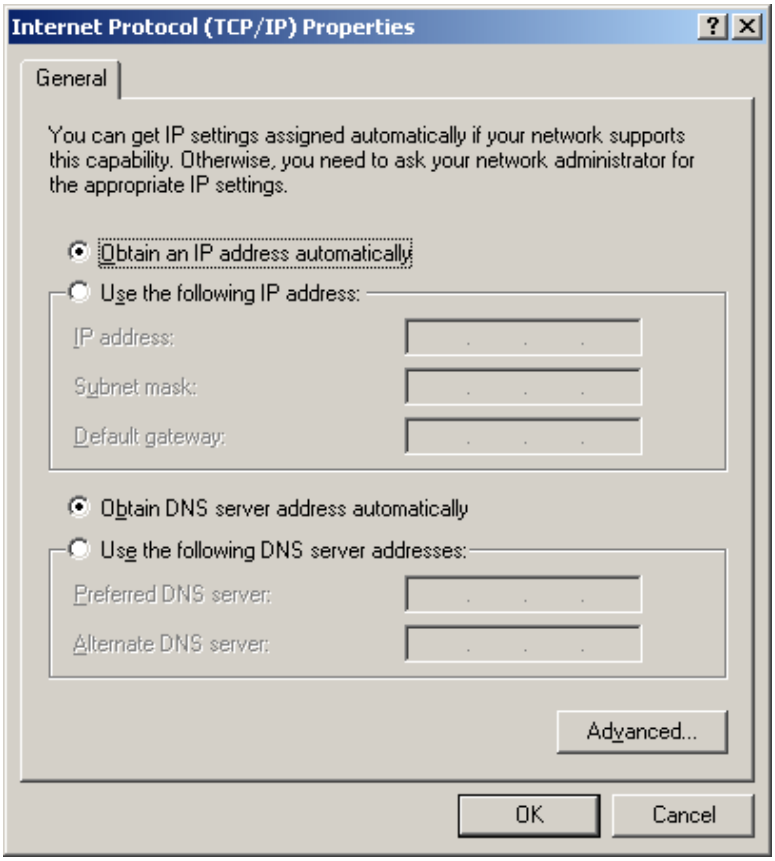


Checking TCP/IP Settings for Windows 2000

a) Select “Start → Control Panel → Network and Dial-up Connection” and right click “Local Area Connection” then click “Properties”,



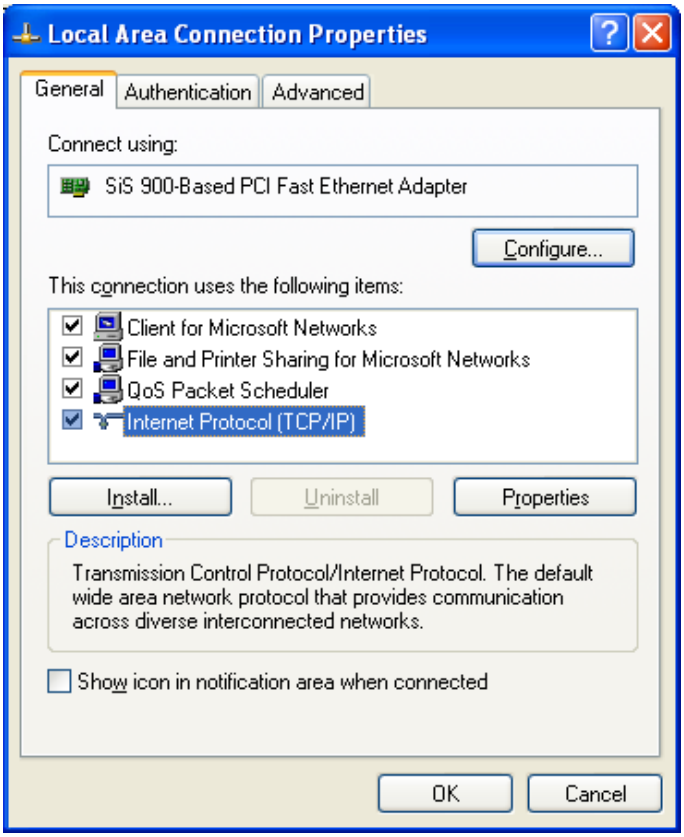
b) Select the "Internet Protocol (TCP/IP)" for the network card on your system, then click "Properties", window below will appear.



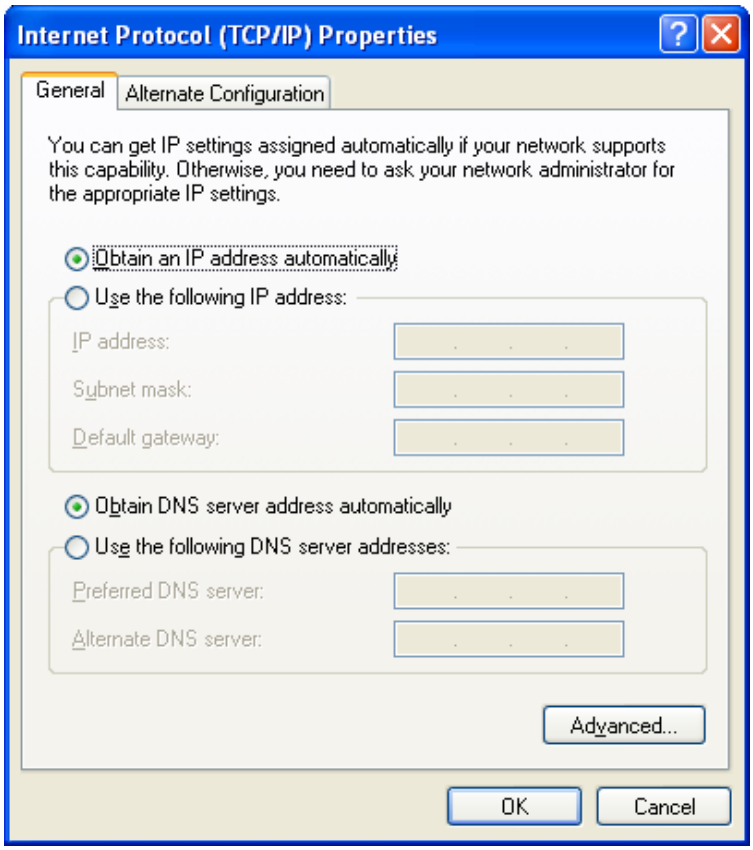
- If you decide to use IP address from Wireless Router, select “Obtain an IP address automatically”.
- If you decide to use the IP address you are desired, select “Use the following IP address”. Make sure enter correct addresses in “IP Address” and “Subnet Mask” fields.
- You must set Wireless Router’s IP address as “Default Gateway”.
- If the DNS Server fields are empty, select “Use the following DNS server addresses” and enter the DNS address is provided by your ISP, then click “OK”.

Checking TCP/IP Settings for Windows XP

a) Click “Start”, select “Control Panel → Network Connection” and right click “Local Area Connection” then select “Properties”, window below will appear.



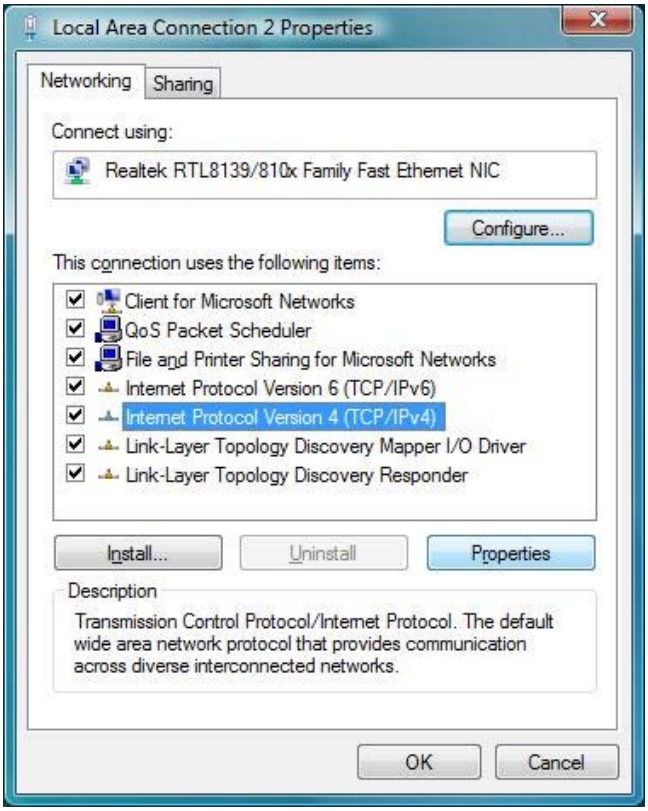
b) Select “Internet Protocol (TCP/IP)” then click “Properties”, window below will appear.



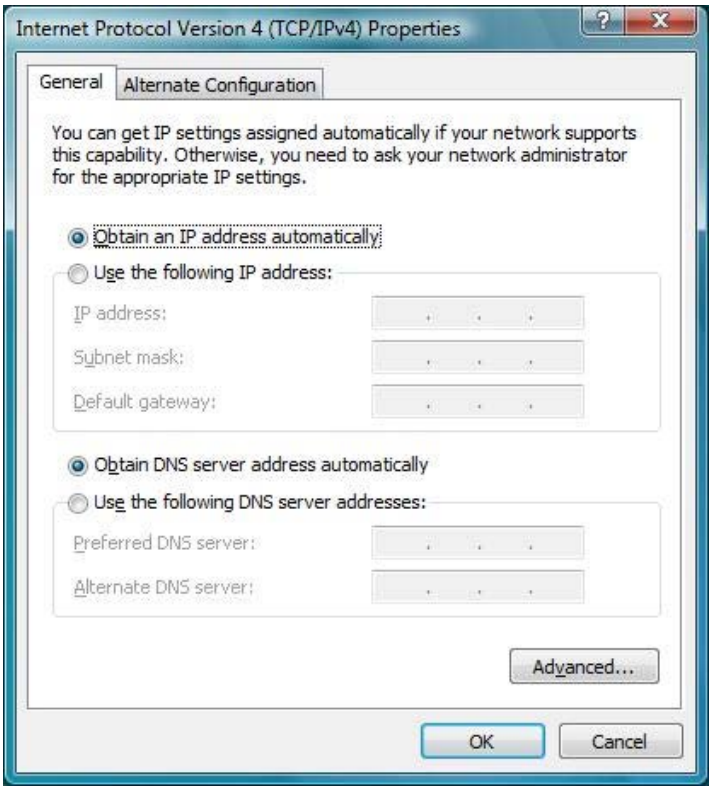
- If you decide to use IP address from Wireless Router, select "Obtain an IP address automatically".
- If you decide to use the IP address you are desired, select "Use the following IP address". Make sure enter correct addresses in "IP Address" and "Subnet Mask" fields.
- You must set Wireless Router's IP address as "Default Gateway".
- If the DNS Server fields are empty, select "Use the following DNS server addresses" and enter the DNS address is provided by your ISP, then click "OK".

Checking TCP/IP Settings for Windows Vista

a) Click "Start" → "Control Panel → "Manage Network Connections" and right click "Local Area Connection" then select "Properties", window below will appear.



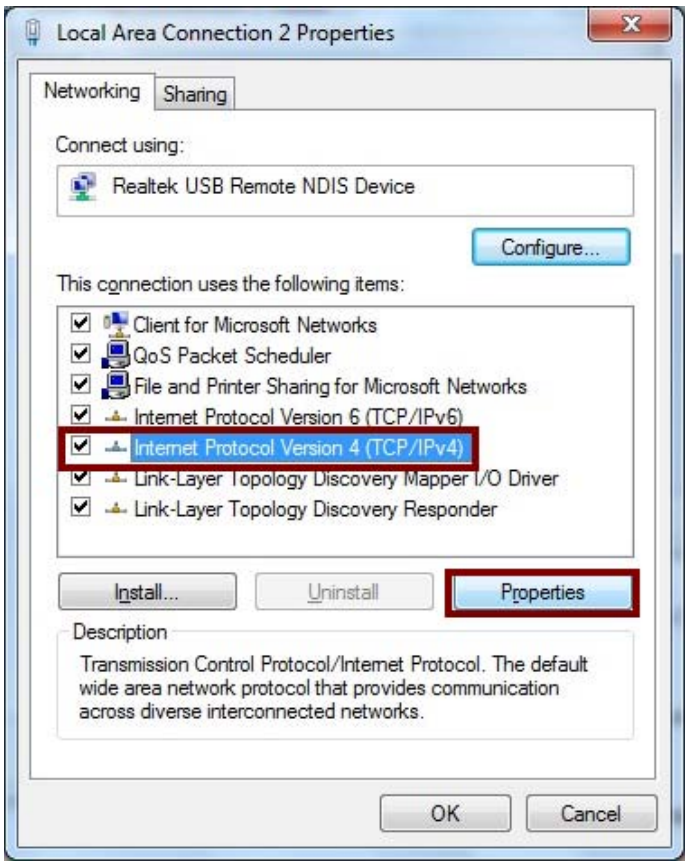
b) Select "Internet Protocol (TCP/IP)" then click "Properties", window below will appear.



- If you decide to use IP address from Wireless Router, select "Obtain an IP address automatically".
- If you decide to use the IP address you are desired, select "Use the following IP address". Make sure enter correct addresses in "IP Address" and "Subnet Mask" fields.
- You must set Wireless Router's IP address as "Default Gateway".
- If the DNS Server fields are empty, select "Use the following DNS server addresses" and enter the DNS address is provided by your ISP, then click "OK".

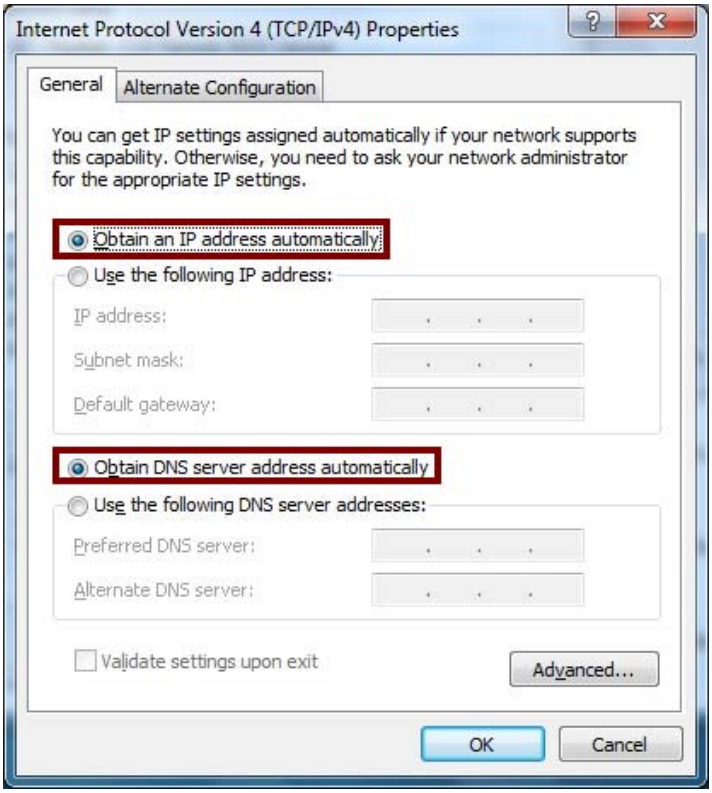
Checking TCP/IP Settings for Windows 7

a) Click "Start" → "Control Panel" → Double-click Network and Sharing Center icon → Select "Local Area Connection #". (Local network your ADSL hooked up with) → Select "Properties" → Select "Internet Protocol Version 4 (TCP/IPv4)" then click "Properties"



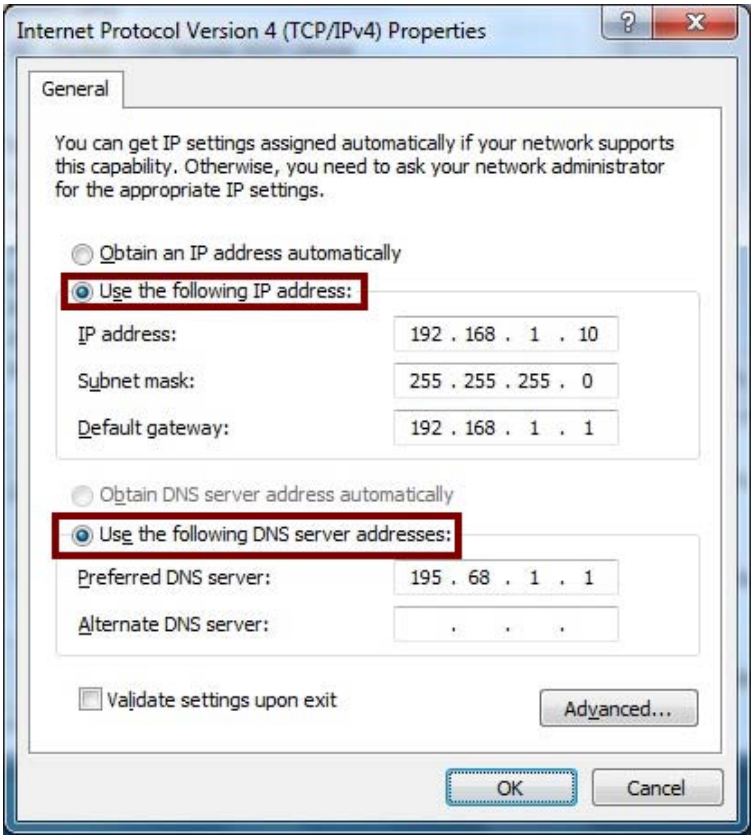
Configure IP address Automatically:

b) Select "Obtain an IP address automatically" and "Obtain DNS server address automatically" Click "OK" to finish the configuration.



Configure IP Address Manually:

c) Select "Use the following IP address" and "Use the following DNS server addresses".

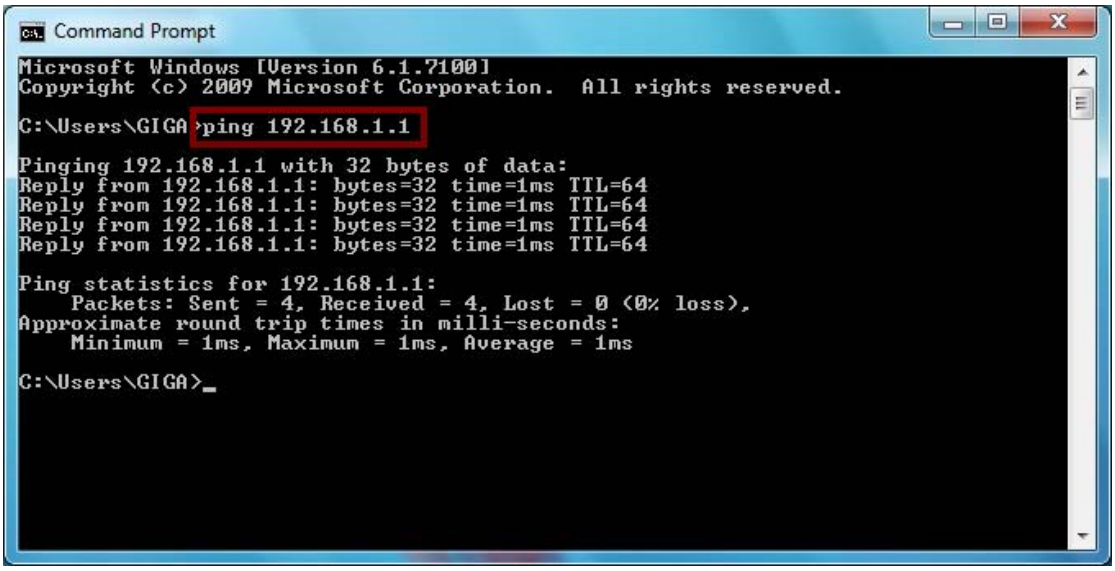


IP address: Fill in IP address 192.168.1.x (x is a number between 2 to 254).
Subnet mask: Default value is 255.255.255.0.
Default gateway: Default value is 192.168.1.1.
Preferred DNS server: Fill in preferred DNS server IP address.
Alternate DNS server: Fill in alternate DNS server IP address.

- If you decide to use IP address from Wireless Router, select "Obtain an IP address automatically".
- If you decide to use the IP address you are desired, select "Use the following IP address". Make sure enter correct addresses in "IP Address" and "Subnet Mask" fields.
- You must set Wireless Router's IP address as "Default Gateway".
- If the DNS Server fields are empty, select "Use the following DNS server addresses" and enter the DNS address is provided by your ISP, then click "OK".

You can use ping command under DOS prompt to check if you have setup TCP/IP protocol correctly and if your computer has successfully connected to this router.

1) Type ping 192.168.1.1 under DOS prompt and the following messages will appear:



If the communication link between your computer and router is not setup correctly, after you type ping 192.168.1.1 under DOS prompt following messages will appear:

Pinging 192.168.1.1 with 32 bytes of data:
Request timed out.

Request timed out.

Request timed out.

This failure might be caused by cable issue or something wrong in configuration procedure.

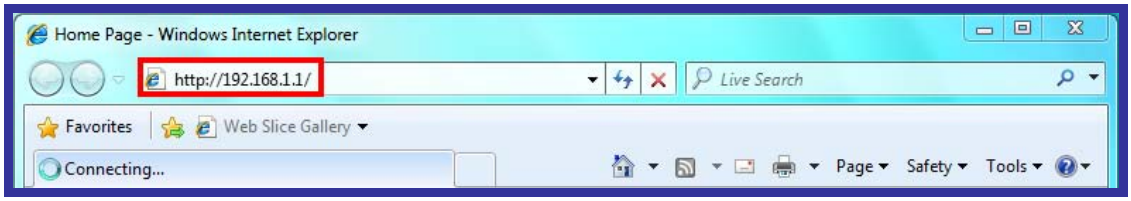
3. Configure Wireless Router via Web Based Utility

The Wireless Router implements a Web server allowing user configure this device via the web based Utility. This Utility provides comprehensive system management scheme, including system configuration, performance monitoring, system maintenance and administration.

3.1 Access Web Based Configuration Utility

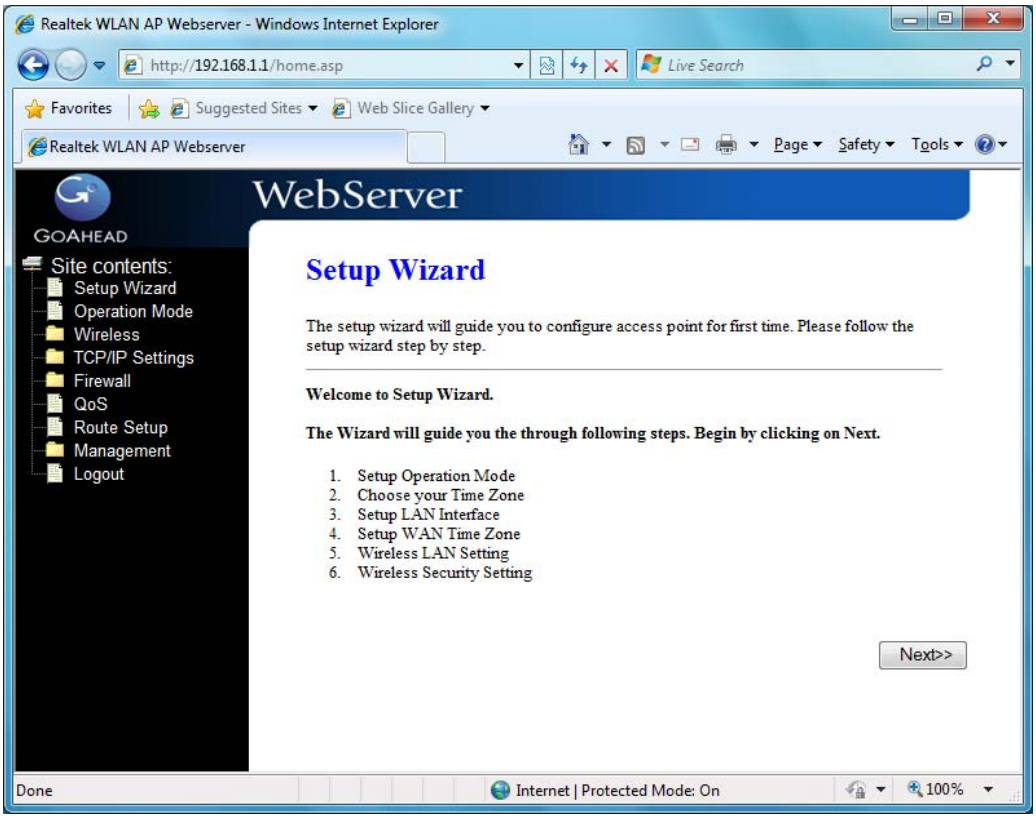
To access the Web-Based Configuration Utility, you have to launch your Internet Browser. (MS IE 6.0 or later, Netscape Navigator 4.7 or later).

Step1: Enter Wireless Router's default IP address as **http://192.168.1.1** in the Address field then press Enter.



Step2: Login dialog box will appear, enter **admin** as Administrator Name and **1234** as default Administrator Password, and then click **"OK"** to access Configuration Utility.

Step3: After log in, you can see the Main menu as below.

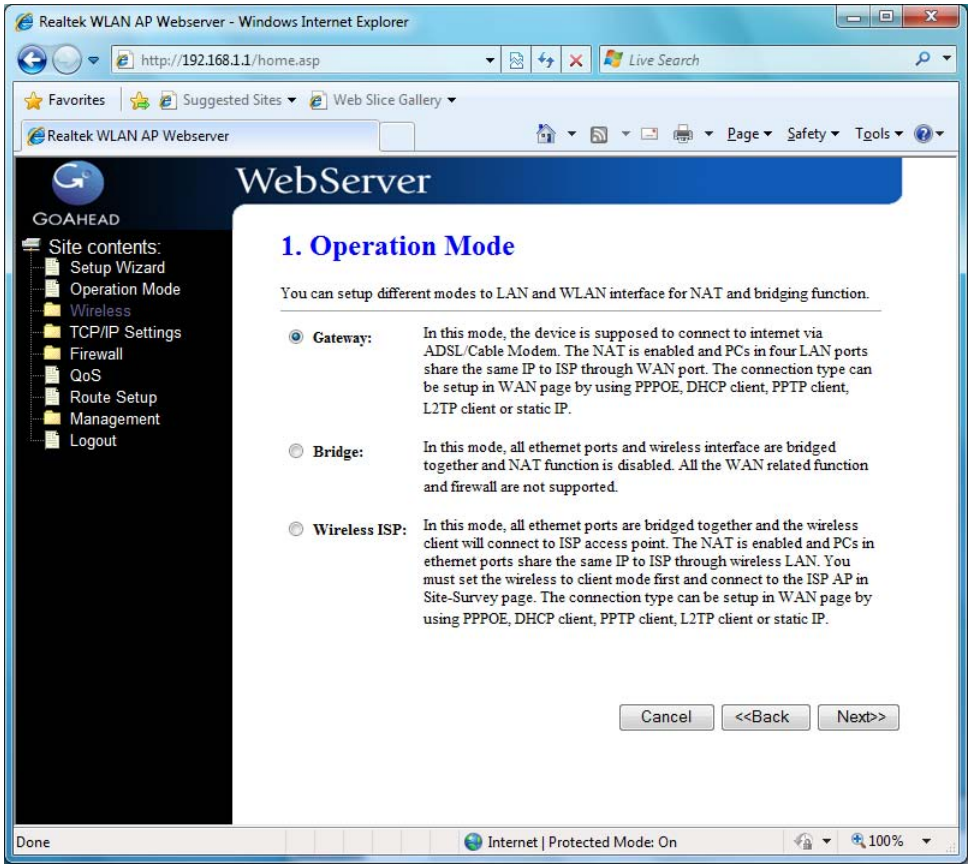


3.2 Setup Wizard

This page guides you to configure wireless broadband router for first time.

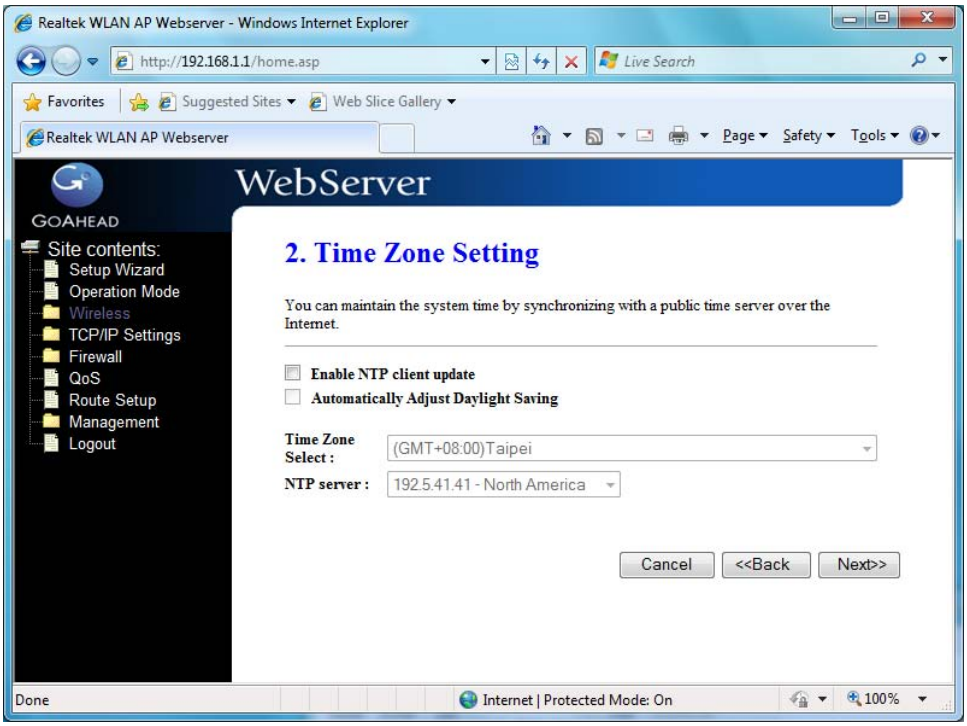
3.2.1 Operation Mode

This page followed by Setup Wizard page to define the operation mode.



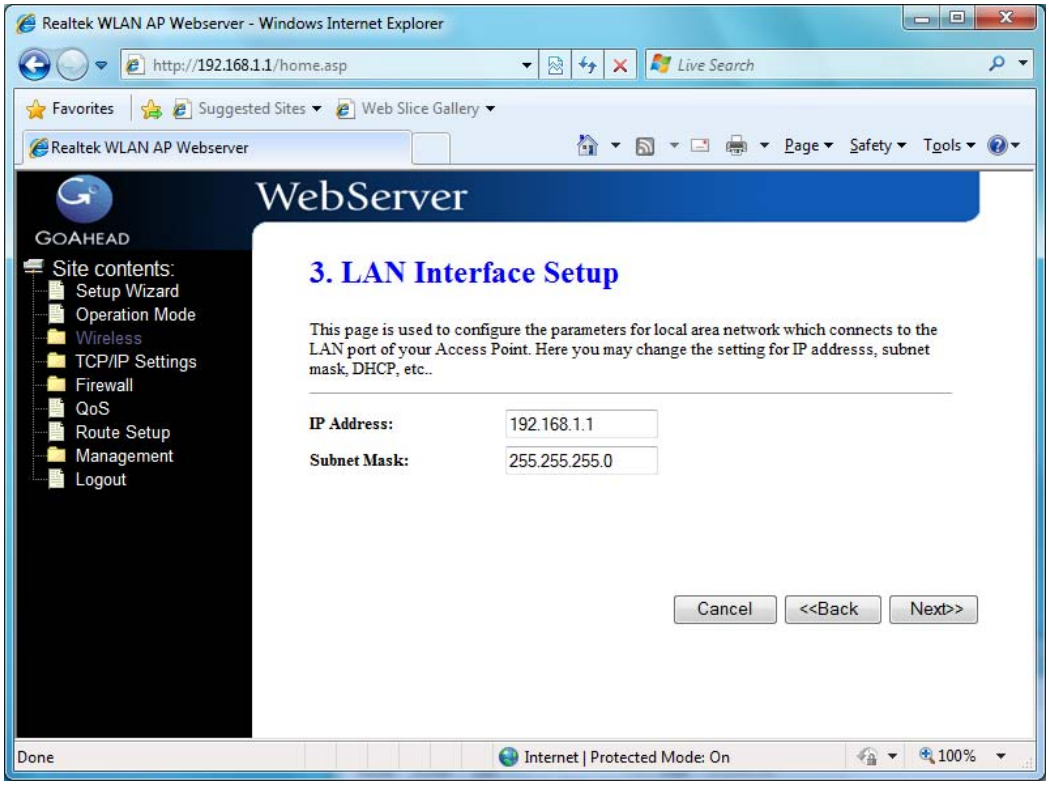
3.2.2 Time Zone Setting

This page is used to enable and configure NTP client.



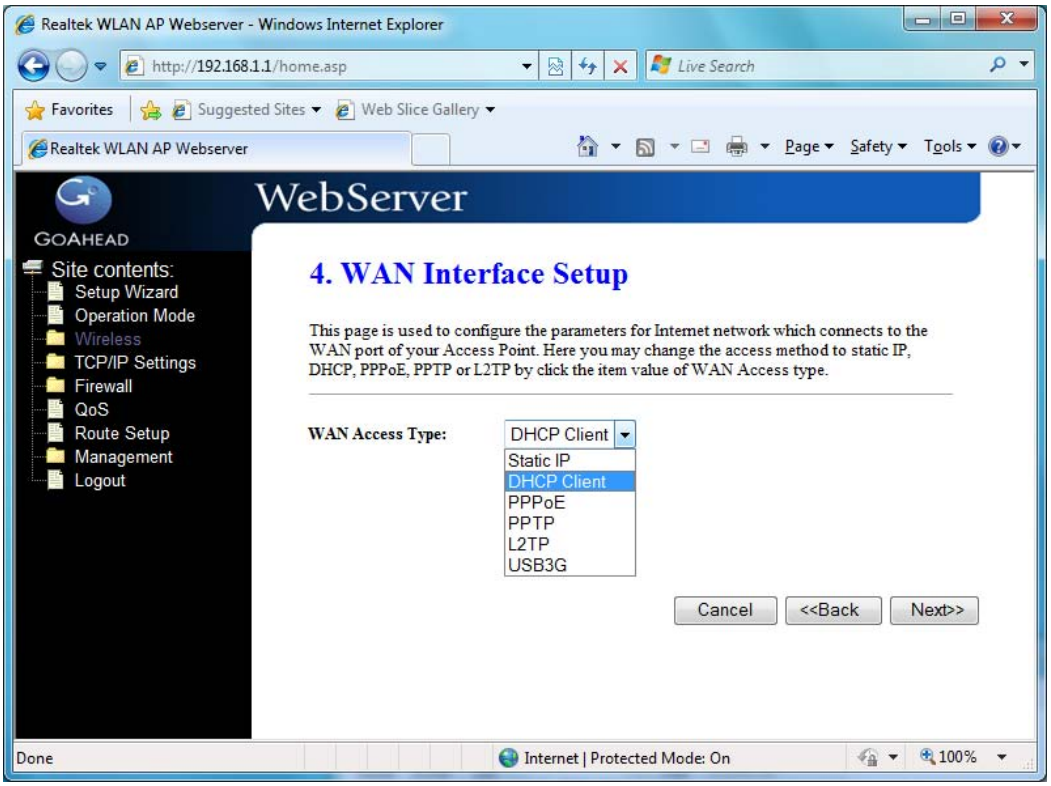
3.2.3 LAN Interface Setup

This page is used to configure local area network IP address and subnet mask.



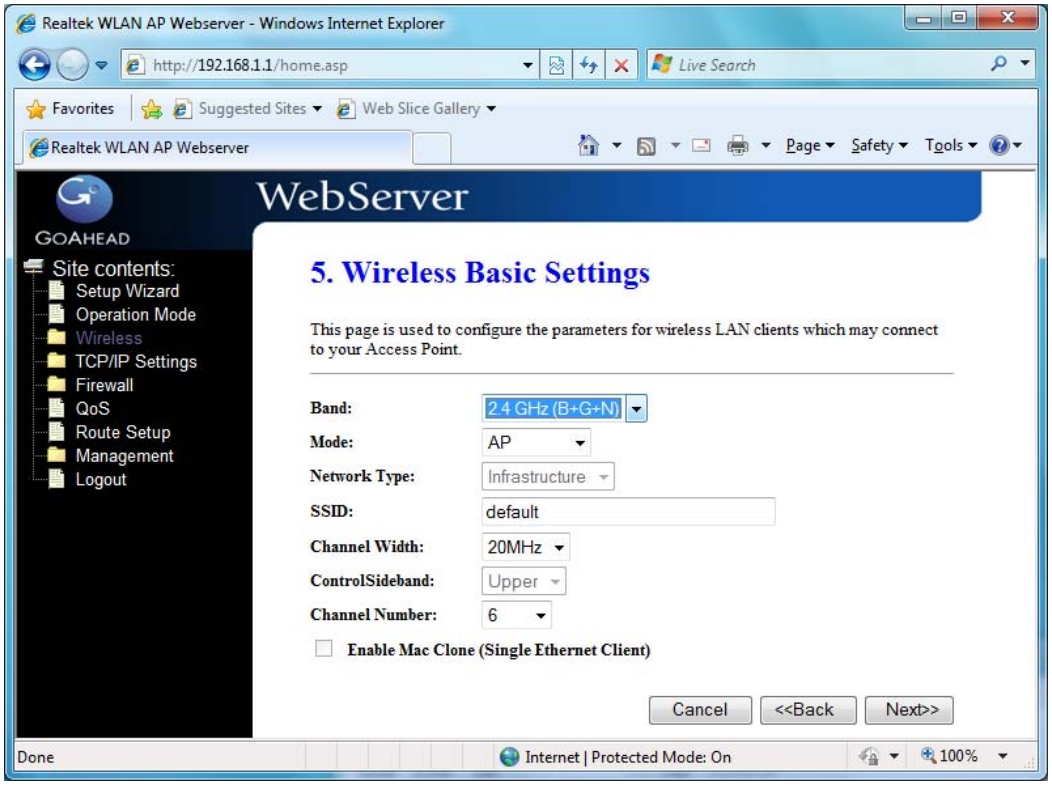
3.2.4 WAN Interface Setup

This page is used to configure WAN access type



3.2.5 Wireless Basic Settings

This page is used to configure basic wireless parameters like Band, Mode, Network Type SSID, Channel Number, Enable Mac Clone(Single Ethernet Client).

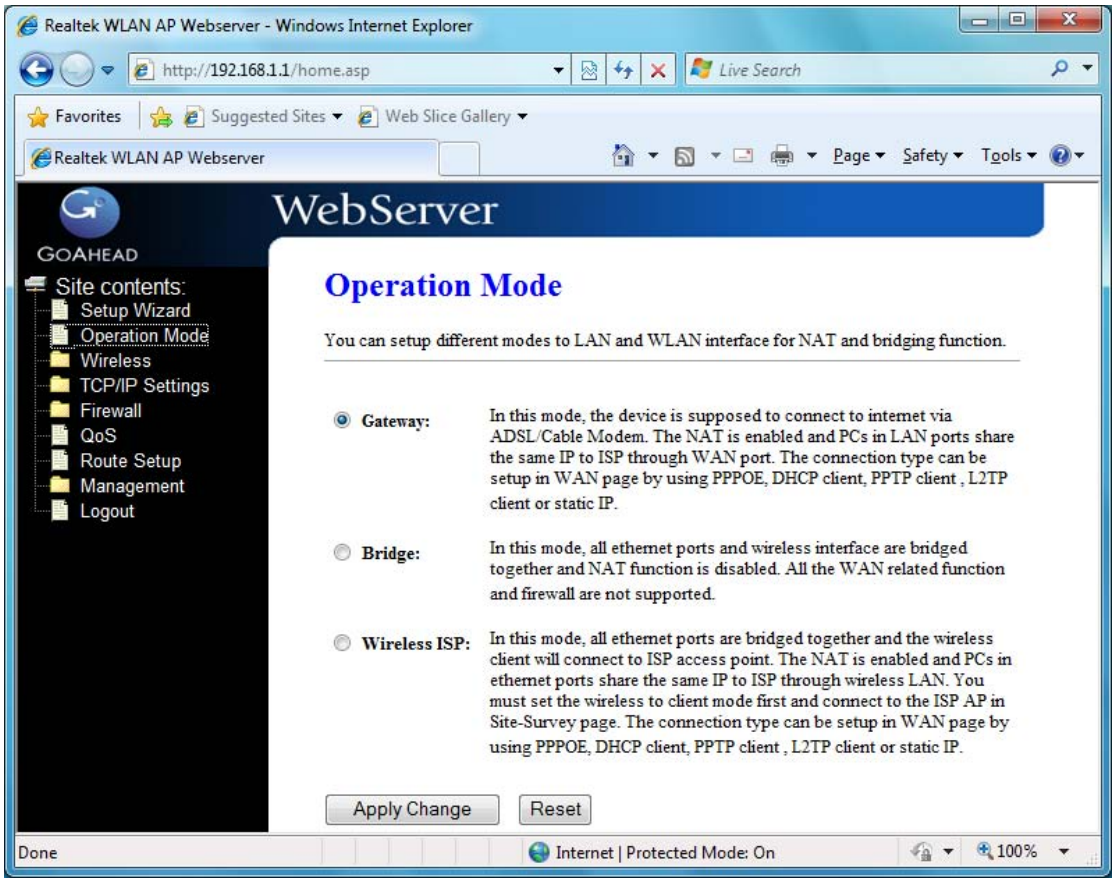


3.2.6 Wireless Security Setup

This page is used to configure wireless security.

3.3 Operation Mode

This page is used to configure which mode wireless broadband router acts.



Gateway: Traditional gateway configuration. It always connects internet via ADSL/Cable Modem. LAN interface, WAN interface, Wireless interface, NAT and Firewall modules are applied to this mode.

Bridge: Each interface (LAN, WAN and Wireless) regards as bridge. NAT, Firewall and all routers' functions are not supported.

Wireless ISP: Switch Wireless interface to WAN port and all Ethernet ports in bridge mode. Wireless interface can do all routers' functions.

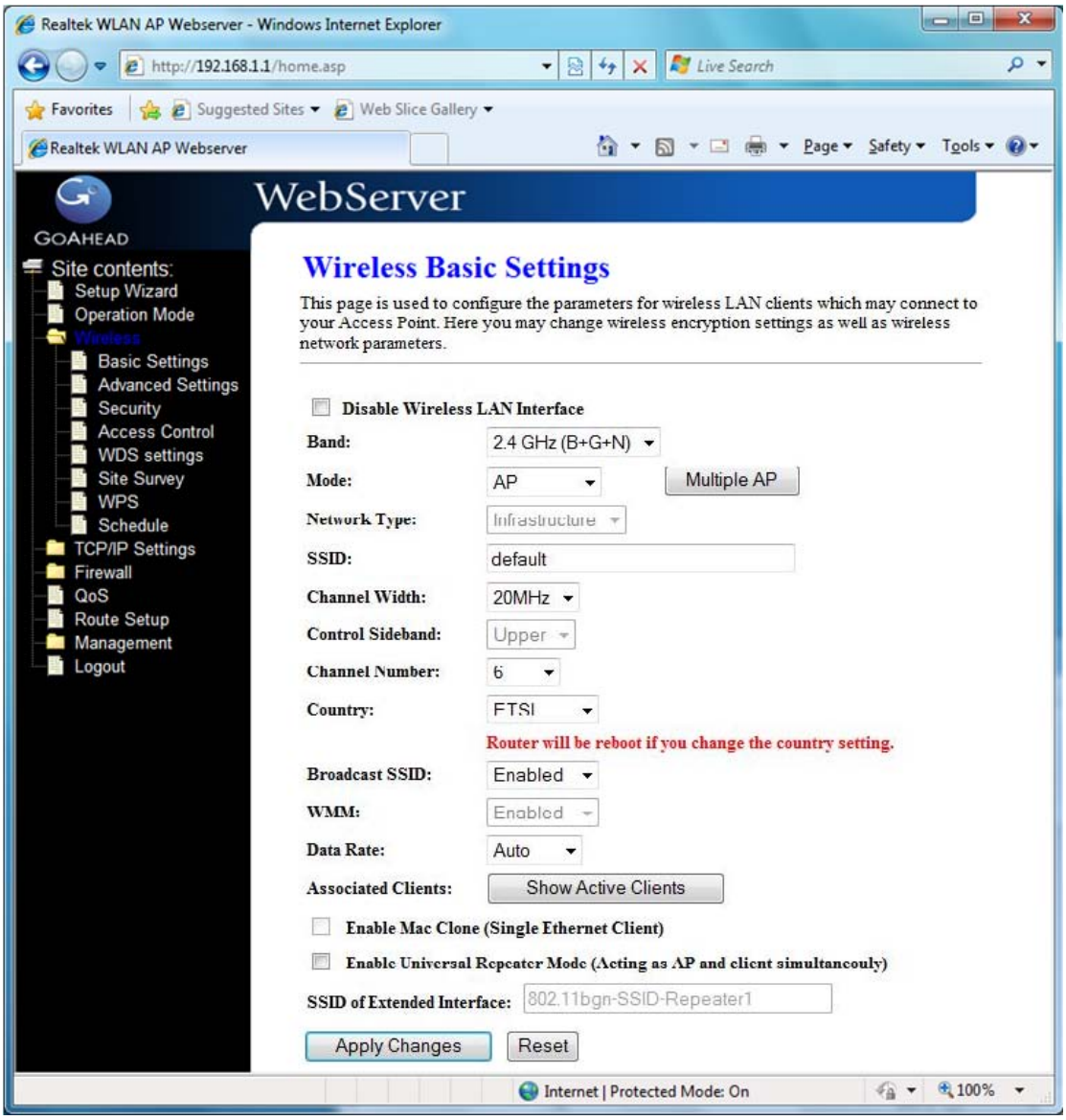
Apply Changes: Click the Apply Changes button to complete the new configuration setting.

Reset: Click the Reset button to abort change and recover the previous configuration setting.

3.4 Wireless

3.4.1 Basic Settings

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



Disable Wireless LAN Interface: Click on to disable the wireless LAN data transmission.

Band: This is the range of frequencies the gateway will use to communicate with your wireless devices. As you're looking for products in stores or on the Internet, you might notice that you can choose equipment that supports six different wireless networking technologies: 2.4 GHz(B), 2.4 GHz(G), 2.4 GHz(B+G), 2.4 GHz(N), 2.4 GHz(G+N), and 2.4 GHz(B+G+N).

Mode: Click to select the WLAN AP / Client / WDS / AP+WDS wireless mode. Default set to AP mode.

Network Type: While Mode is selected to be Client. Click to select the network type infrastructure or Ad hoc.

SSID: Specify the network name. Each Wireless LAN network uses a unique Network Name to identify the network. This name is called the Service Set

Identifier (SSID). When you set up your wireless adapter, you specify the SSID. If you want to connect to an existing network, you must use the make up your own name and use it on each computer. The name can be up to 32 characters long and contain letters and numbers.

Channel Width: There have 2 options – 20MHZ and 40 MHZ [N band only].

Control Sideband: Specify if the extension channel should be in the Upper or Lower sideband [N band only].

Channel Number: Sets the channel on which the gateway operates.

Broadcast SSID: Click to enable or disable the SSID broadcast function.

WMM: Click Enabled/Disabled to init WMM feature.

Data Rate: Select the transmission data rate from pull-down menu. Data rate can be auto-select, 1M to 54Mbps or MCS.

Associated Clients: This table shows MAC address, transmission, reception packet counters and encrypted status for each associated wireless clients.

Enable Mac Clone (Single Ethernet Client): Take Laptop NIC MAC address as wireless client

MAC address. [Client Mode only]

Enable Universal Repeater Mode (Acting as AP and Client simultaneously): Click to enable Universal Repeater Mode.

SSID of Extended Interface: Assign SSID when enables Universal Repeater Mode.

3.4.2 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 WLAN Broadband Router.

Fragment Threshold: Fragmentation Threshold sets the frame size of incoming messages (ranging from 256 to 2346 bytes) used as fragmentation boundary. If the frame size is too big, the heavy interference affects transmission reliability. If the frame size is too small, it decreases transmission efficiency. Default setting is 2346.

RTS Threshold: Lower the signal RTS (Request To Send) to promote the transmission efficiency in condition of noisy environment or too many clients. Default setting is 2347.

Beacon Interval: Beacon Interval means the period of time between one beacon and the next one. The default value is 100 (the unit is millisecond, or 1/1000 second). Lower the Beacon Interval to improve transmission performance in unstable environment or for roaming clients, but it will be power consuming.

Preamble type: Preamble is the first sub field of PPDU, which is the appropriate frame format for transmission to PHY (Physical layer). There are two options, Short Preamble and Long Preamble.

IAPP: Click to enable or disable the IAPP function.

Protection: Protect 802.11n user priority.

Aggregation: Click to enable or disable the Aggregation function.

Short GI: Using a short (400ns) guard interval can increase throughput. However, it can also increase error rate in some installations, due to increased sensitivity to radio-frequency reflections

WLAN Partition: Click to enable or disable the WLAN Partition function.

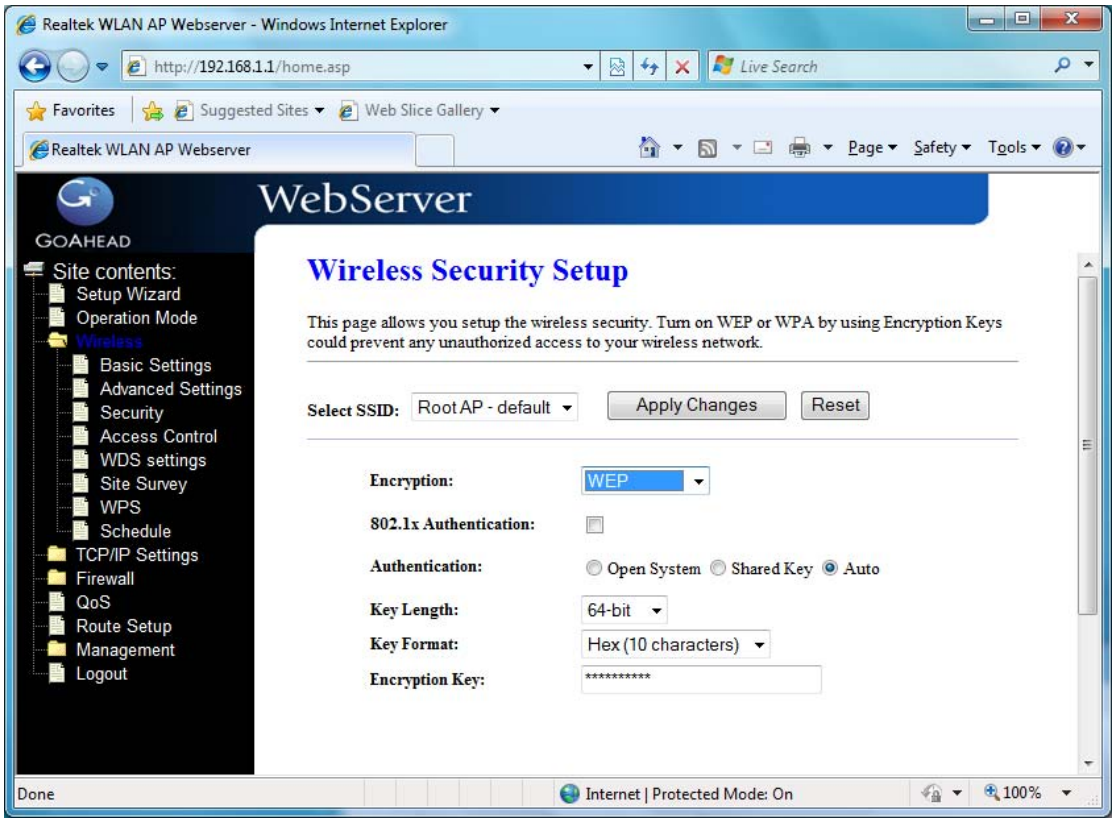
STBC: Click to enable or disable the STBC function.

20/40MHz Coexist: Click to enable or disable the Coexist function.

RF Output Power: To adjust transmission power level.

3.4.3 Security

This page allows you setup the wireless security. Turn on WEP, WPA, WPA2 by using encryption keys could prevent any unauthorized access to your wireless network.



Select SSID: Select the SSID from multiple APs.

Encryption: Select the encryption supported over wireless access. The encryption method can be None, WEP, WPA, WPA2 or WPA-Mixed.

Use 802.1x Authentication: While Encryption is selected to be WEP. Click the check box to enable IEEE 802.1x authentication function.

Authentication Type: Click to select the authentication type in Open System,

Shared Key or Auto selection.

Key Length: Select the WEP shared secret key length from pull-down menu. The length can be chose between 64-bit and 128-bit (known as “WEP2”) keys. The WEP key is composed of initialization vector (24 bits) and secret key (40-bit or 104-bit).

Key Format: Select the WEP shared secret key format from pull-down menu. The format can be chose between plant text (ASCII) and hexadecimal (HEX) code.

Encryption Key: Secret key of WEP security encryption function.

WPA Authentication Mode: While Encryption is selected to be WPA. Click to select the WPA Authentication Mode with Enterprise (RADIUS) or Personal (Pre-Shared Key).

WPA Cipher Suite: Select the Cipher Suite for WPA encryption.

WPA2 Cipher Suite: Select the Cipher Suite for WPA2 encryption.

Pre-Shared Key Format: While Encryption is selected to be WPA. Select the Pre-shared key format from the pull-down menu. The format can be Passphrase or Hex (64 characters). [WPA, Personal(Pre-Shared Key) only]

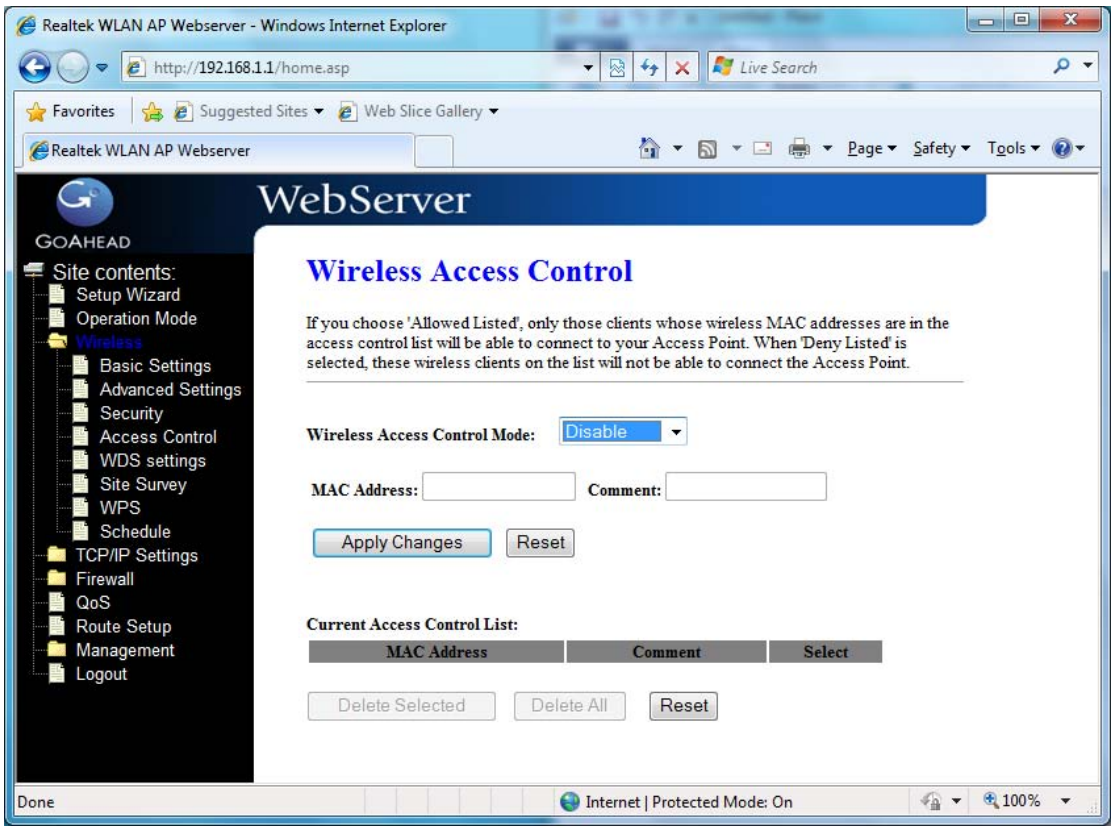
Pre-Shared Key: Fill in the key value. [WPA, Personal(Pre-Shared Key) only]

Enable Pre-Authentication: Click to enable Pre-Authentication. [WPA2/WPA2 Mixed only, Enterprise only]

Authentication RADIUS Server: Set the IP address, port and login password information of authentication RADIUS sever.

3.4.4 Access Control

If you enable wireless access control, only those clients whose wireless MAC addresses are in the access control list will be able to connect to your Access Point. When this option is enabled, no wireless clients will be able to connect if the list contains no entries.



Wireless Access Control Mode: Click the Disabled, ***Allow Listed*** or ***Deny Listed*** of drop down menu choose wireless access control mode. This is a security control function; only those clients registered in the access control list can link to this WLAN Broadband Router.

MAC Address: Fill in the MAC address of client to register this WLAN Broadband Router access capability.

Comment: Fill in the comment tag for the registered client.

Current Access Control List: It shows the registered clients that are allowed to link to this WLAN Broadband Router.

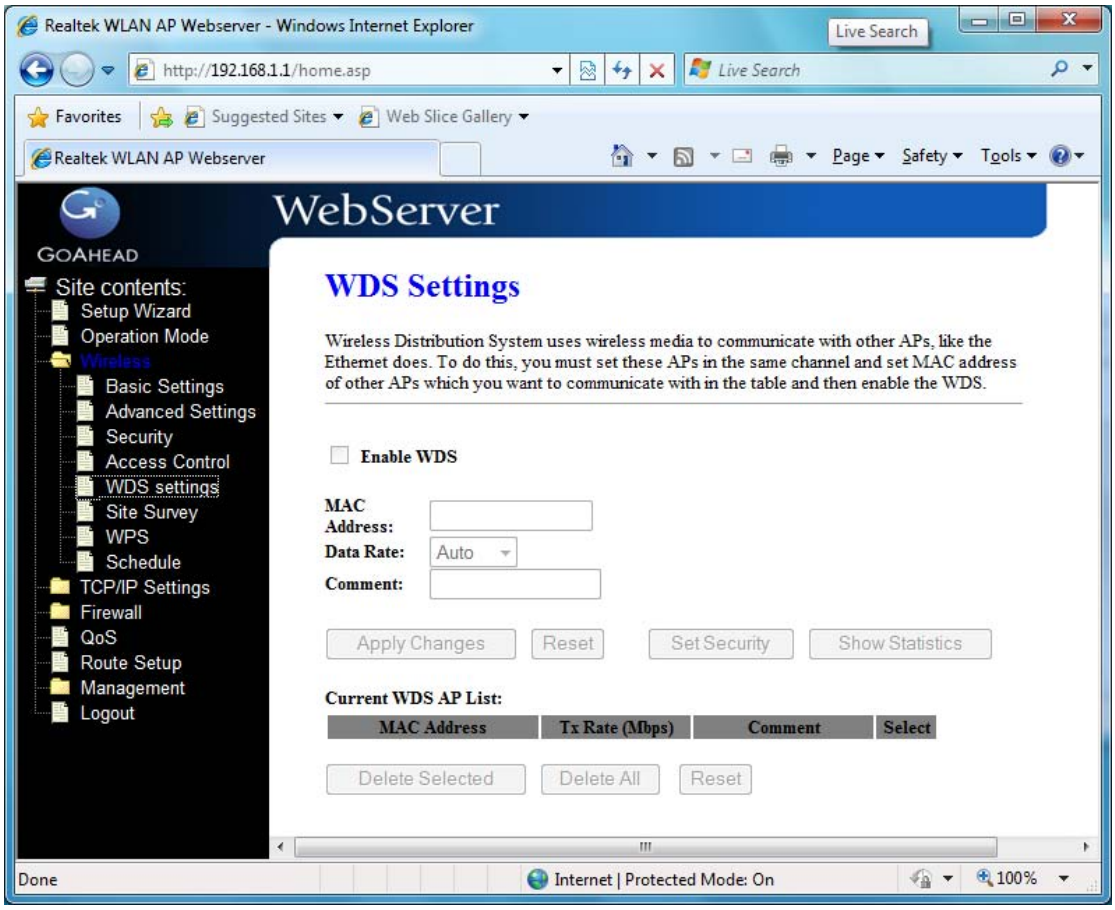
Delete Selected: Click to delete the selected clients that will be access right removed from this WLAN Broadband Router.

Delete All: Click to delete all the registered clients from the access allowed list.

Reset: Click the Reset button to abort change and recover the previous configuration setting.

3.4.5 WDS Setting

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 AP that you want to communicate with in the table and then enable the WDS.



Enable WDS: Click the check box to enable wireless distribution system.

MAC Address: Fill in the MAC address of AP to register the wireless distribution system access capability.

Data Rate: Select the transmission data rate from pull-down menu.

Data rate: can be auto-select, 1M to 54Mbps or MCS.

Comment: Fill in the comment tag for the registered AP.

Apply Changes: Click the Apply Changes button to complete the new configuration setting.

Reset: Click the Reset button to abort change and recover the previous configuration setting.

Set Security: Click button to configure wireless security like WEP(64bits), WEP(128bits), WPA(TKIP), WPA2(AES) or None

Show Statistics: It shows the TX, RX packets, rate statistics.

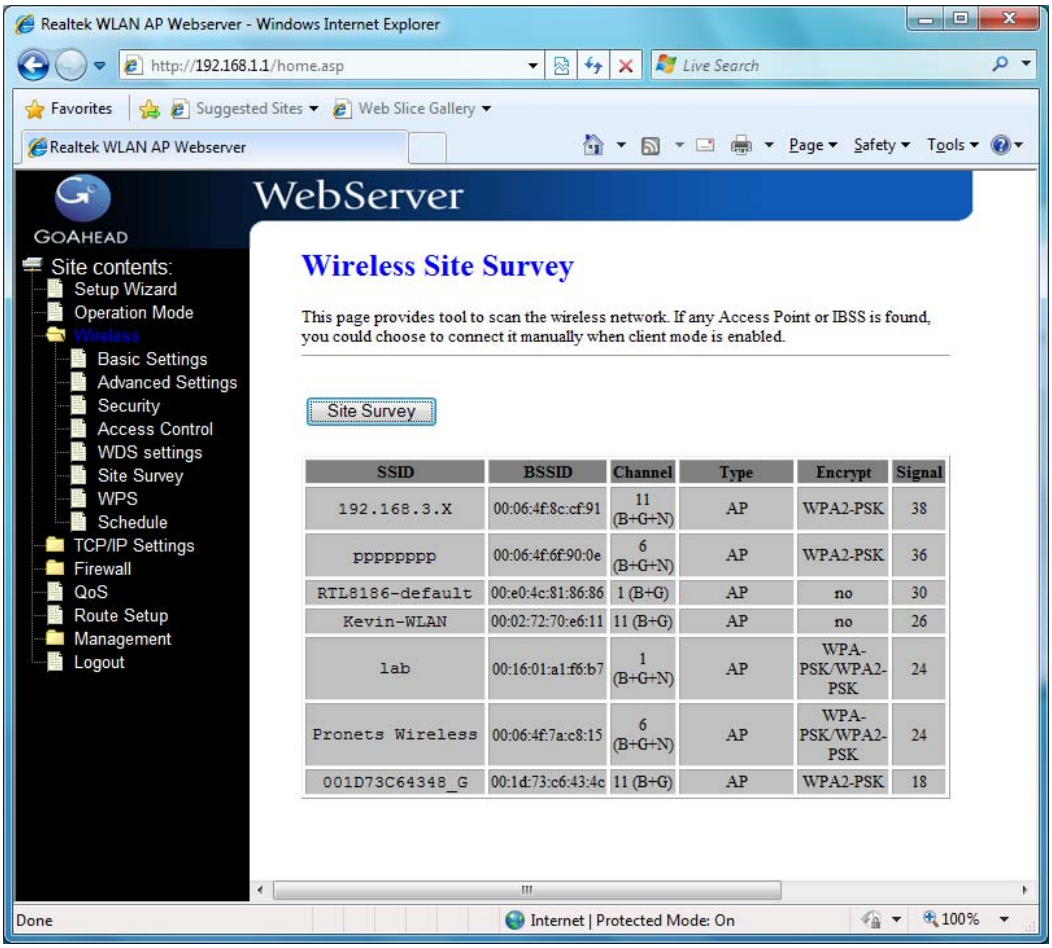
Delete Selected: Click to delete the selected clients that will be access right removed from this WLAN Broadband Router.

Delete All: Click to delete all the registered clients from the access allowed list.

Reset: Click the Reset button to abort change and recover the previous configuration setting.

3.4.6 Site Survey

This page is used to view or configure other APs near yours.



SSID: It shows the SSID of AP.

BSSID: It shows BSSID of AP.

Channel: It show the current channel of AP occupied.

Type: It show which type AP acts.

Encrypt: It shows the encryption status.

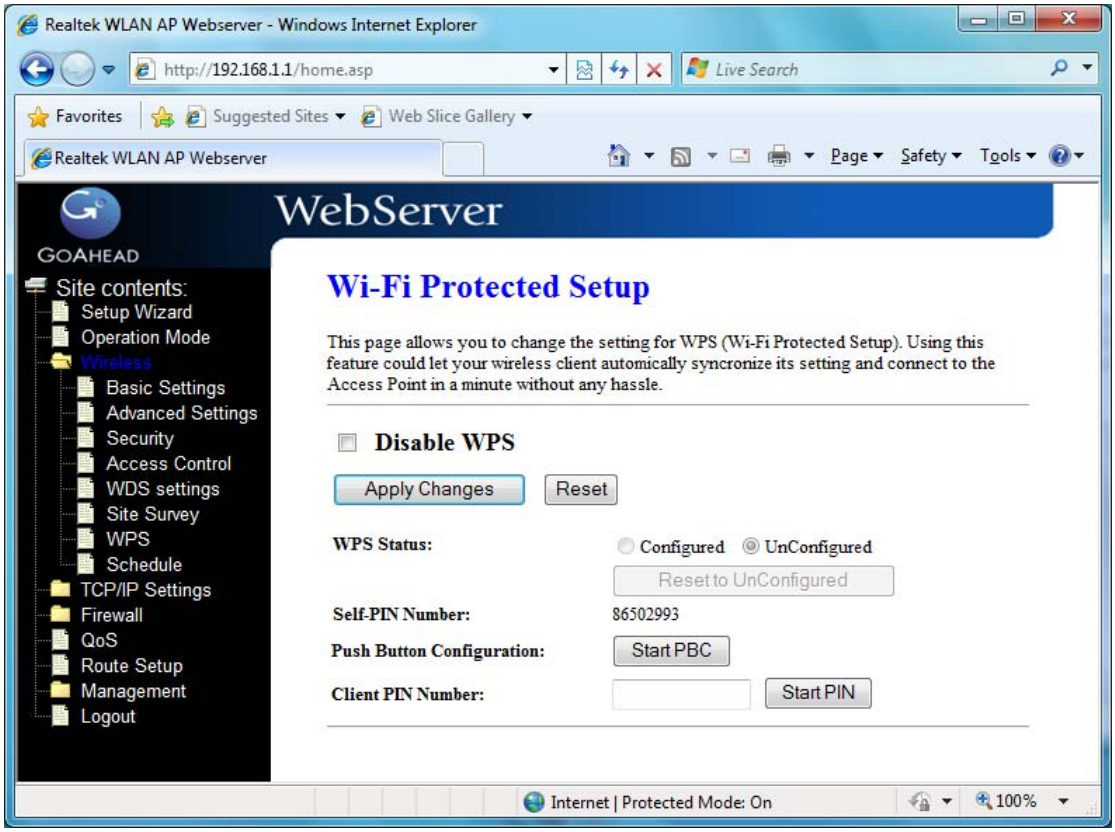
Signal: It shows the power level of current AP.

Refresh: Click the Refresh button to re-scan site survey on the screen.

Connect: Click the Connect button to establish connection

3.4.7 WPS

This page allows you to change the setting for WPS (Wi-Fi Protected Setup). Using this feature could let your wireless client atomically synchronize its setting and connect to the Access Point in a minute without any hassle.



Disable WPS: Click on to disable the Wi-Fi Protected Setup function.

WPS Status: Show WPS status is Configured or UnConfigured.

Self-PIN Number: Fill in the PIN Number of AP to register the wireless distribution system access capability.

Push Button Configuration: The Start PBC button provides tool to scan the wireless network. If any Access Point or IBSS is found, you could connect it automatically when client join PBC mode.

Apply Changes: Click the Apply Changes button to complete the new configuration setting.

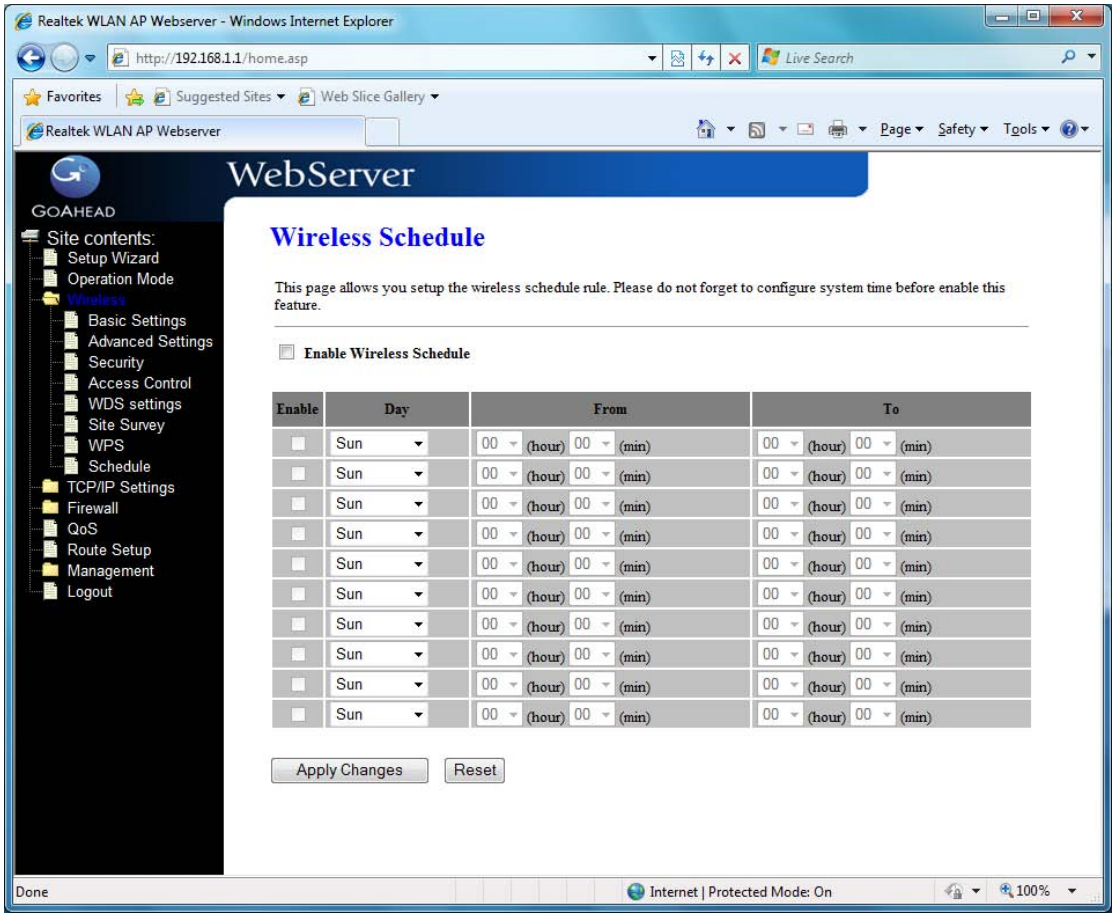
Reset: Click the Reset button to abort change and recover the previous configuration setting.

Current Key Info: Authentication-It shows the Authentication is opened or closed. Encryption-It shows the Encryption mode. Key-It shows the Encryption key.

Client PIN Number: Fill in the Client PIN Number from your Client sites.

3.4.8 Schedule

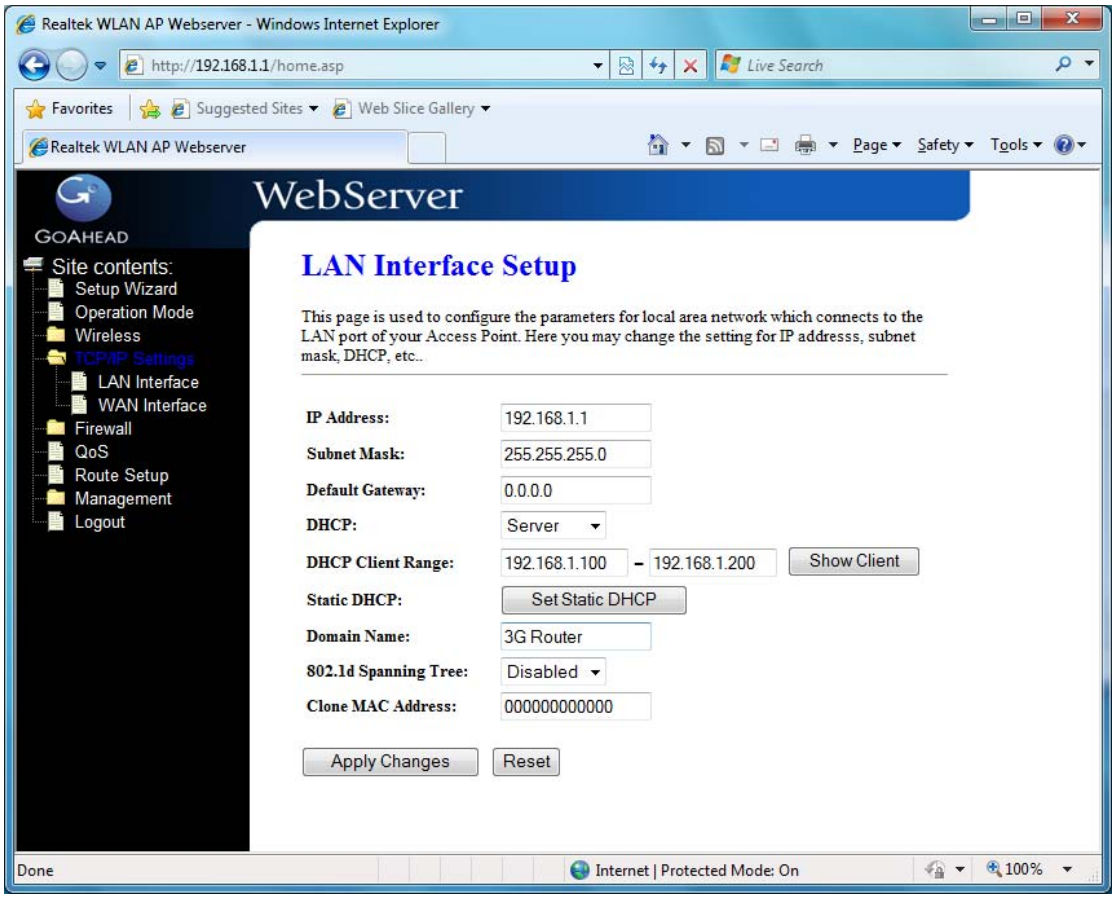
This page allows you setup the wireless schedule rule. Please do not forget to configure system time before enable this feature.



3.5 TCP/IP Settings

3.5.1 LAN Interface

This page is used to configure the parameters for local area network that connects to the LAN ports of your WLAN Broadband Router. Here you may change the setting for IP address, subnet mask, DHCP, etc.



IP Address: Fill in the IP address of LAN interfaces of this WLAN Access Point.

Subnet Mask: Fill in the subnet mask of LAN interfaces of this WLAN Access Point.

Default Gateway: Fill in the default gateway for LAN interfaces out going data packets.

DHCP: Click to select Disabled, Client or Server in different operation mode of wireless Access Point.

DHCP Client Range: Fill in the start IP address and end IP address to allocate a range of IP addresses; client with DHCP function set will be assigned an IP address from the range.

Show Client: Click to open the Active DHCP Client Table window that shows the active clients with their assigned IP address, MAC address and time expired information. [Server mode only]

Static DHCP: Select enable or disable the Static DHCP function from pull-down menu. [Server mode only]

Set Static DHCP: Manual setup Static DHCP IP address for specific MAC address. [Server mode only]

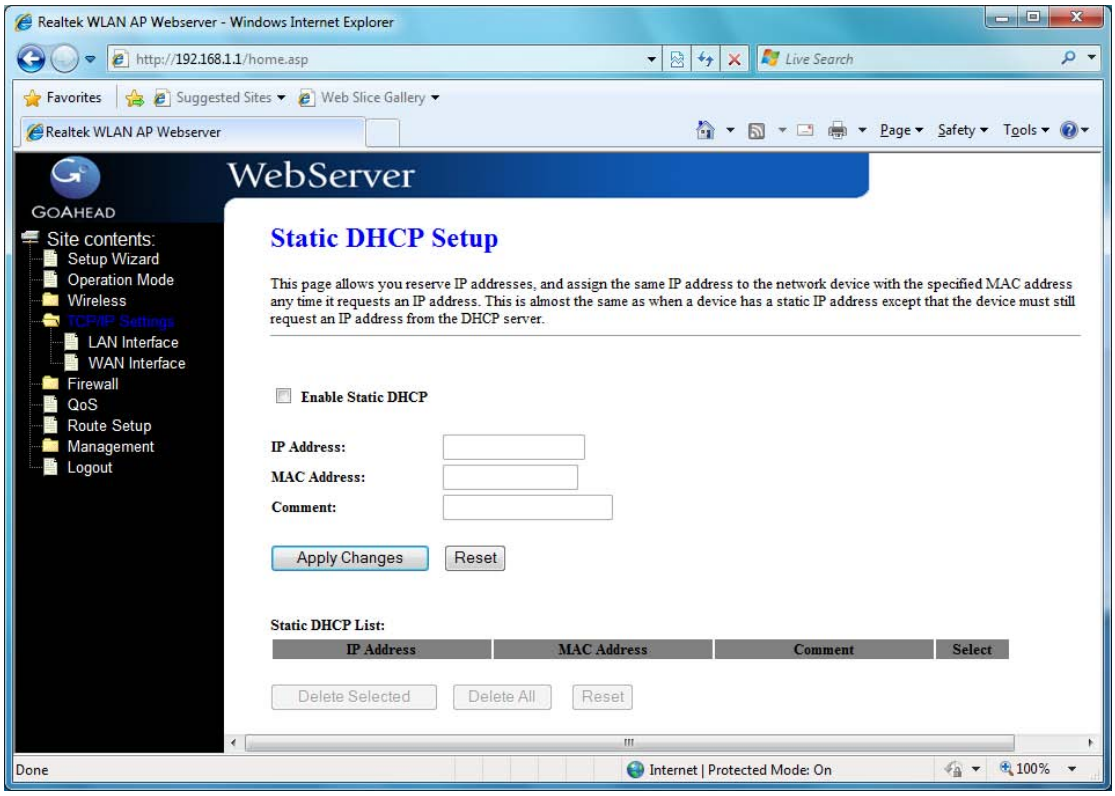
Domain Name: Assign Domain Name and dispatch to DHCP clients. It is optional field.

802.1d Spanning Tree: Select enable or disable the IEEE 802.1d Spanning Tree function from pull-down menu.

Clone MAC Address: Fill in the MAC address that is the MAC address to be cloned.

3.5.1.1 Static DHCP Setup

This page allows you reserve IP address and assign the same IP address to the network device with the specified MAC address any time it requests an IP address. This is almost the same as when a device has a static IP address except that the device must still request an IP address from the DHCP server.



IP Address: If you select the Set Static DHCP on LAN interface, fill in the IP address for it.

MAC Address: If you select the Set Static DHCP on LAN interface, fill in the MAC address for it.

Comment: Fill in the comment tag for the registered Static DHCP.

Static DHCP List: It shows IP Address MAC Address from the Static DHCP.

Delete Selected: Click to delete the selected clients that will be removed from the Static DHCP list.

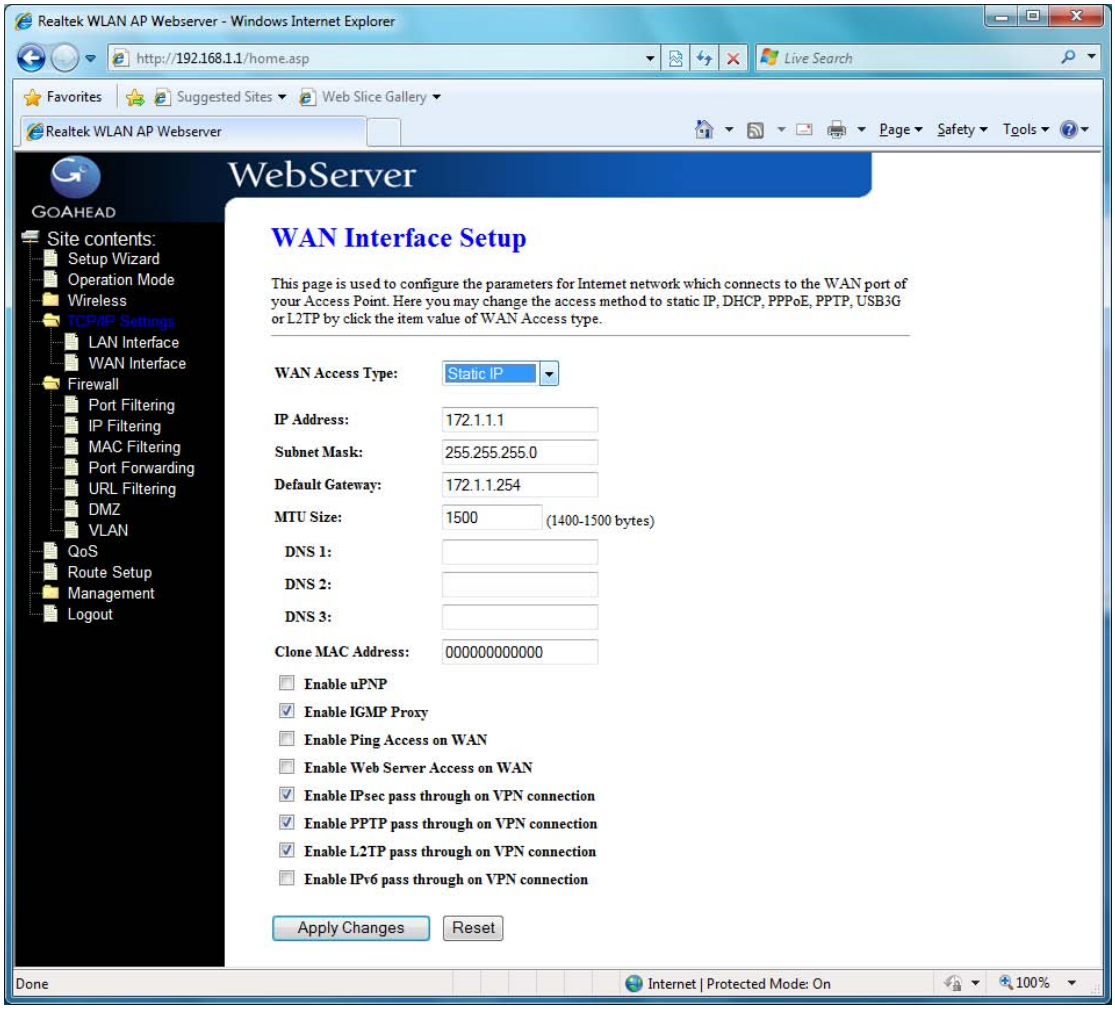
Delete All: Click to delete all the registered clients from the Static DHCP list.

Reset: Click the Reset button to abort change and recover the previous configuration setting.

3.5.2 WAN Interface

This page is used to configure the parameters for wide area network that connects to the WAN port of your WLAN Broadband Router. 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]



Static IP: Click to select Static IP support on WAN interface. There are IP address, subnet mask and default gateway settings need to be done.

IP Address: If you select the Static IP support on WAN interface, fill in the IP address for it.

Subnet Mask: If you select the Static IP support on WAN interface, fill in the subnet mask for it.

Default Gateway: If you select the Static IP support on WAN interface, fill in the default gateway for WAN interface out going data packets.

MTU Size: Fill in the mtu size of MTU Size. The default value is 1400.

DNS 1: Fill in the IP address of Domain Name Server 1.

DNS 2: Fill in the IP address of Domain Name Server 2.

DNS 3: Fill in the IP address of Domain Name Server 3.

Clone MAC Address: Fill in the MAC address that is the MAC address to be cloned.

Enable uPNP: Click the checkbox to enable uPNP function.

Enable IGMP Proxy: Click the checkbox to enable IGMP Proxy.

Enable Ping Access on WAN: Click the checkbox to enable WAN ICMP response.

Enable Web Server Access on WAN: Click the checkbox to enable web configuration from WAN side.

Enable IPsec pass through on VPN connection: Click the checkbox to enable IPSec packet pass through.

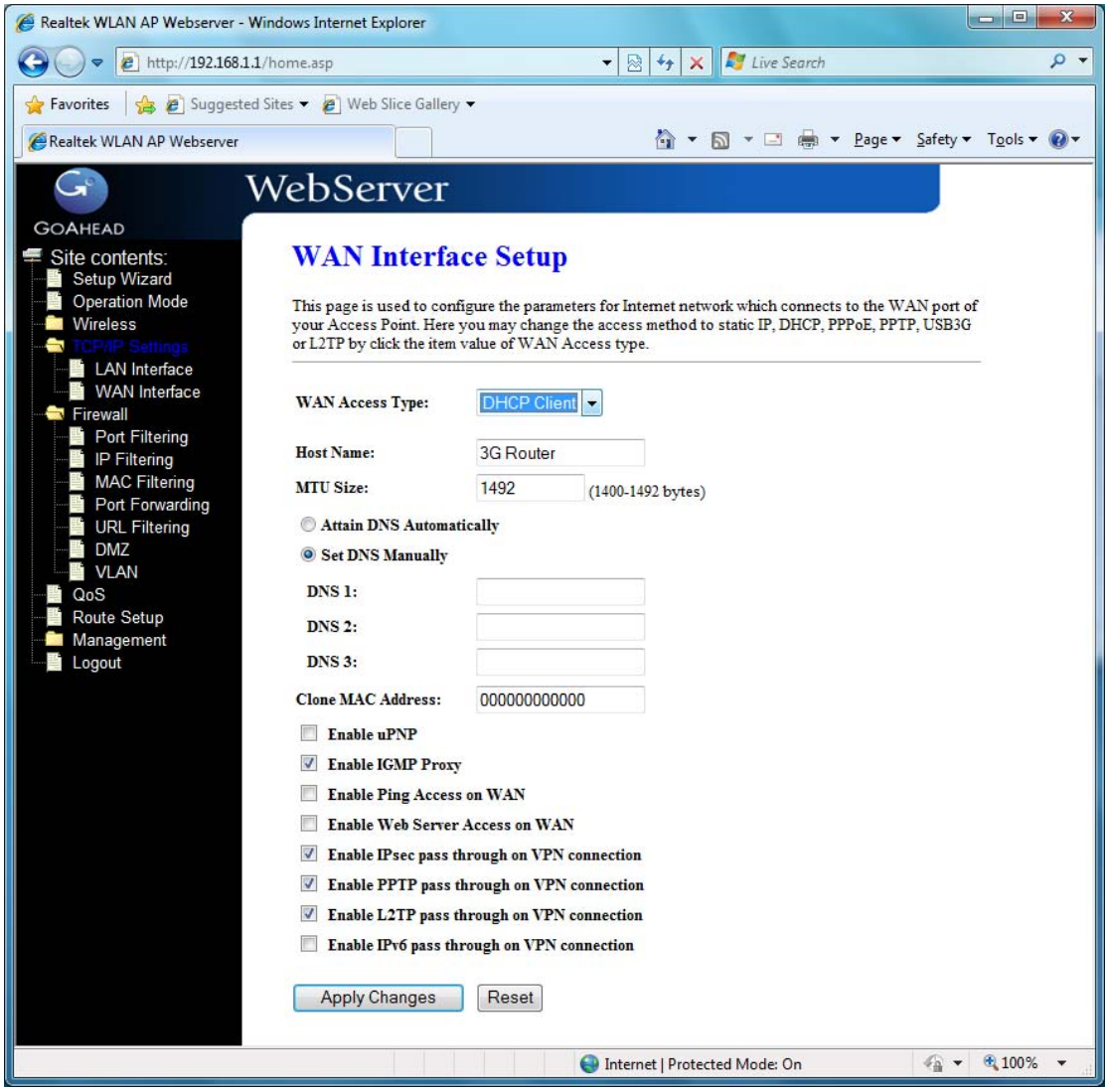
Enable PPTP pass through on VPN connection: Click the checkbox to enable PPTP packet pass through.

Enable L2TP pass through on VPN connection: Click the checkbox to enable L2TP packet pass through.

Apply Changes: Click the ***Apply Changes*** button to complete the new configuration setting.

Reset: Click the ***Reset*** button to abort change and recover the previous configuration setting.

[DHCP Client]



DHCP Client: Click to select DHCP support on WAN interface for IP address assigned automatically from a DHCP server.

Host Name: Fill in the host name of Host Name. The default value is empty.

MTU Size: Fill in the mtu size of MTU Size. The default value is 1400.

Attain DNS Automatically: Click to select getting DNS address for ***DHCP*** support. Please select ***Set DNS Manually*** if the ***DHCP*** support is selected.

Set DNS Manually: Click to select getting DNS address for ***DHCP*** support.

DNS 1: Fill in the IP address of Domain Name Server 1.

DNS 2: Fill in the IP address of Domain Name Server 2.

DNS 3: Fill in the IP address of Domain Name Server 3.

Clone MAC Address: Fill in the MAC address that is the MAC address to be cloned.

Enable uPNP: Click the checkbox to enable uPNP function.

Enable IGMP Proxy: Click the checkbox to enable IGMP Proxy.

Enable Ping Access on WAN: Click the checkbox to enable WAN ICMP

response.

Enable Web Server Access on WAN: Click the checkbox to enable web configuration from WAN side.

Enable IPsec pass through on VPN connection: Click the checkbox to enable IPSec packet pass through.

Enable PPTP pass through on VPN connection: Click the checkbox to enable PPTP packet pass through.

Enable L2TP pass through on VPN connection: Click the checkbox to enable L2TP packet pass through.

Apply Changes: Click the ***Apply Changes*** button to complete the new configuration setting.

Reset: Click the ***Reset*** button to abort change and recover the previous configuration setting.

[PPPoE]

PPPoE: Click to select PPPoE support on WAN interface. There are user name, password, connection type and idle time settings need to be done.

User Name: If you select the PPPoE support on WAN interface, fill in the user name and password to login the PPPoE server.

Password: If you select the PPPoE support on WAN interface, fill in the user name and password to login the PPPoE server.

Service Name: Fill in the service name of Service Name. The default value is empty.

Connection Type: Select the connection type from pull-down menu. There are ***Continuous***, ***Connect on Demand*** and ***Manual*** three types to select.

- ***Continuous*** connection type means to setup the connection through PPPoE protocol whenever this WLAN AP Router is powered on.
- ***Connect on Demand*** connection type means to setup the connection through PPPoE protocol whenever you send the data packets out through the WAN interface; there are a watchdog implemented to close the PPPoE connection while there are no data sent out longer than the idle time set.
- ***Manual*** connection type means to setup the connection through the PPPoE protocol by clicking the ***Connect*** button manually, and clicking the ***Disconnect*** button manually.

Idle Time: If you select the ***PPPoE*** and ***Connect on Demand*** connection type, fill in the idle time for auto-disconnect function. Value can be between 1 and 1000 minutes.

MTU Size: Fill in the MTU size of MTU Size. The default value is 1400.

Attain DNS Automatically: Click to select getting DNS address for ***DHCP*** support. Please select ***Set DNS Manually*** if the ***DHCP*** support is selected.

Set DNS Manually: Click to select getting DNS address for ***DHCP*** support.

DNS 1: Fill in the IP address of Domain Name Server 1.

DNS 2: Fill in the IP address of Domain Name Server 2.

DNS 3: Fill in the IP address of Domain Name Server 3.

Clone MAC Address: Fill in the MAC address that is the MAC address to be cloned.

Enable uPNP: Click the checkbox to enable uPNP function.

Enable IGMP Proxy: Click the checkbox to enable IGMP Proxy.

Enable Ping Access on WAN: Click the checkbox to enable WAN ICMP response.

Enable Web Server Access on WAN: Click the checkbox to enable web configuration from WAN side.

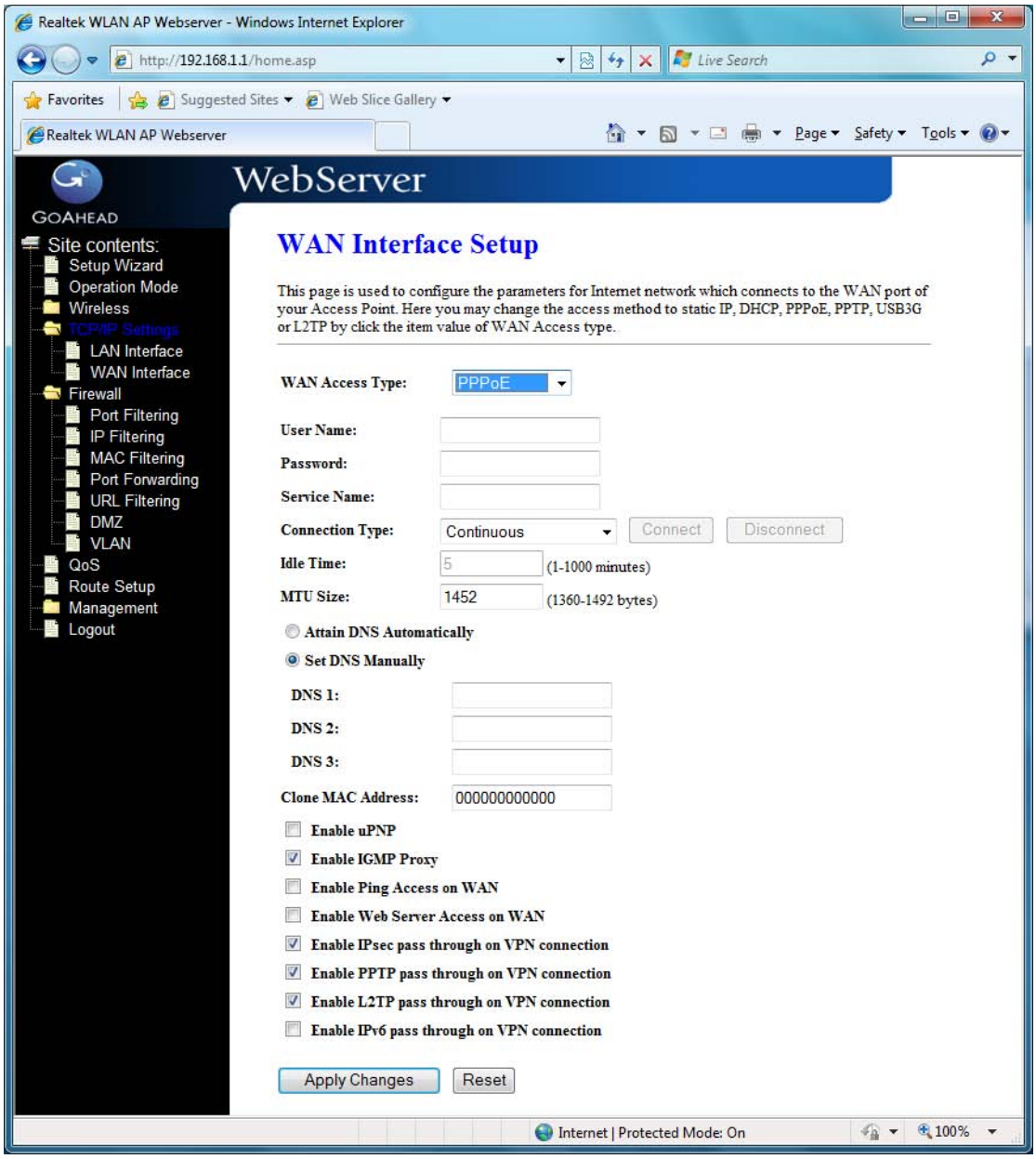
Enable IPsec pass through on VPN connection: Click the checkbox to enable IPSec packet pass through.

Enable PPTP pass through on VPN connection: Click the checkbox to enable PPTP packet pass through.

Enable L2TP pass through on VPN connection: Click the checkbox to enable L2TP packet pass through.

Apply Changes: Click the ***Apply Changes*** button to complete the new configuration setting.

Reset: Click the ***Reset*** button to abort change and recover the previous configuration setting.



[PPTP]

PPTP: Allow user to make a tunnel with remote site directly to secure the data transmission among the connection. User can use embedded PPTP client supported by this router to make a VPN connection.

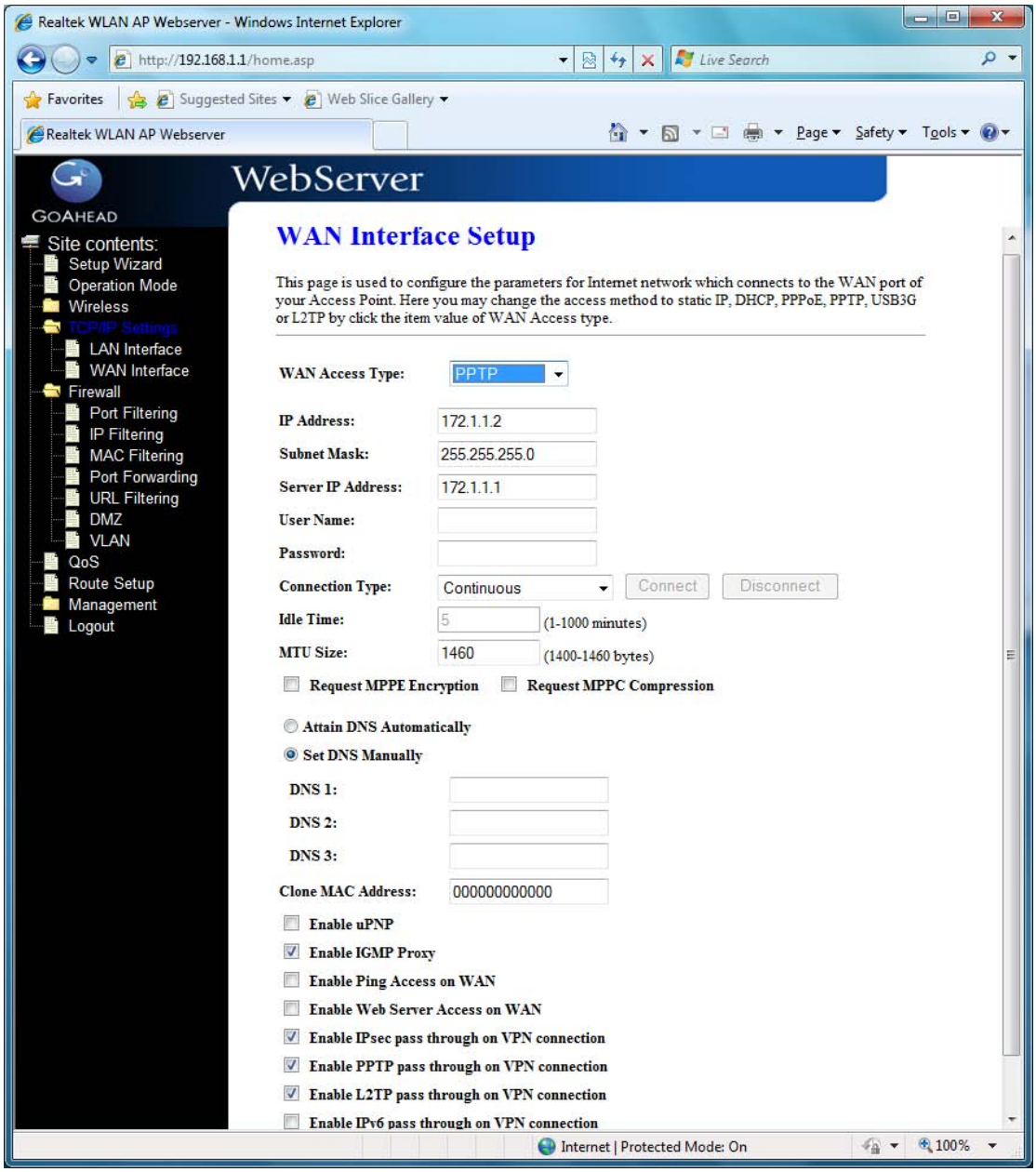
Get the WAN IP Automatically: Click to select PPTP Dynamic support on WAN interface for IP address assigned automatically from a PPTP server.

IP Address: If you select the PPTP support on WAN interface, fill in the IP address for it.

Subnet Mask: If you select the PPTP support on WAN interface, fill in the subnet mask for it.

Gateway: If you select the Static PPTP support on WAN interface, fill in the

gateway for WAN interface out going data packets.



Server IP Address : Enter the IP address of the PPTP Server.

Server Domain Name: Assign Domain Name and dispatch to PPTP servers. It is optional field.

User Name: If you select the PPTP support on WAN interface, fill in the user name and password to login the PPTP server.

Password: you select the PPTP support on WAN interface, fill in the user name and password to login the PPTP server.

MTU Size: Fill in the mtu size of MTU Size. The default value is 1400.

Request MPPE Encryption: Click the checkbox to enable request MPPE encryption.

Attain DNS Automatically: Click to select getting DNS address for ***PPTP*** support. Please select ***Set DNS Manually*** if the ***PPTP*** support is selected.

Set DNS Manually: Click to select getting DNS address for ***PPTP*** support.

DNS 1: Fill in the IP address of Domain Name Server 1.

DNS 2: Fill in the IP address of Domain Name Server 2.

DNS 3: Fill in the IP address of Domain Name Server 3.

Clone MAC Address: Fill in the MAC address that is the MAC address to be cloned.

Enable uPNP: Click the checkbox to enable uPNP function.

Enable IGMP Proxy: Click the checkbox to enable IGMP Proxy.

Enable Ping Access on WAN: Click the checkbox to enable WAN ICMP response.

Enable Web Server Access on WAN: Click the checkbox to enable web configuration from WAN side.

Enable IPsec pass through on VPN connection: Click the checkbox to enable IPSec packet pass through.

Enable PPTP pass through on VPN connection: Click the checkbox to enable PPTP packet pass through.

Enable L2TP pass through on VPN connection: Click the checkbox to enable L2TP packet pass through.

Apply Changes: Click the ***Apply Changes*** button to complete the new configuration setting.

Reset: Click the ***Reset*** button to abort change and recover the previous configuration setting.

Note: PPTP Gateway Your ISP will provide you with the Gateway IP Address. If your LAN has a PPTP gateway, then enter that PPTP gateway IP address here. If you do not have PPTP gateway then enter the ISP's Gateway IP address above.

[L2TP]

L2TP: Allow user to make a tunnel with remote site directly to secure the data transmission among the connection. User can use embedded L2TP client supported by this router to make a VPN connection.

Get the WAN IP Automatically: Click to select L2TP Dynamic support on WAN interface for IP address assigned automatically from a PPTP server.

IP Address: If you select the L2TP support on WAN interface, fill in the IP address for it.

Subnet Mask: If you select the L2TP support on WAN interface, fill in the subnet

mask for it.

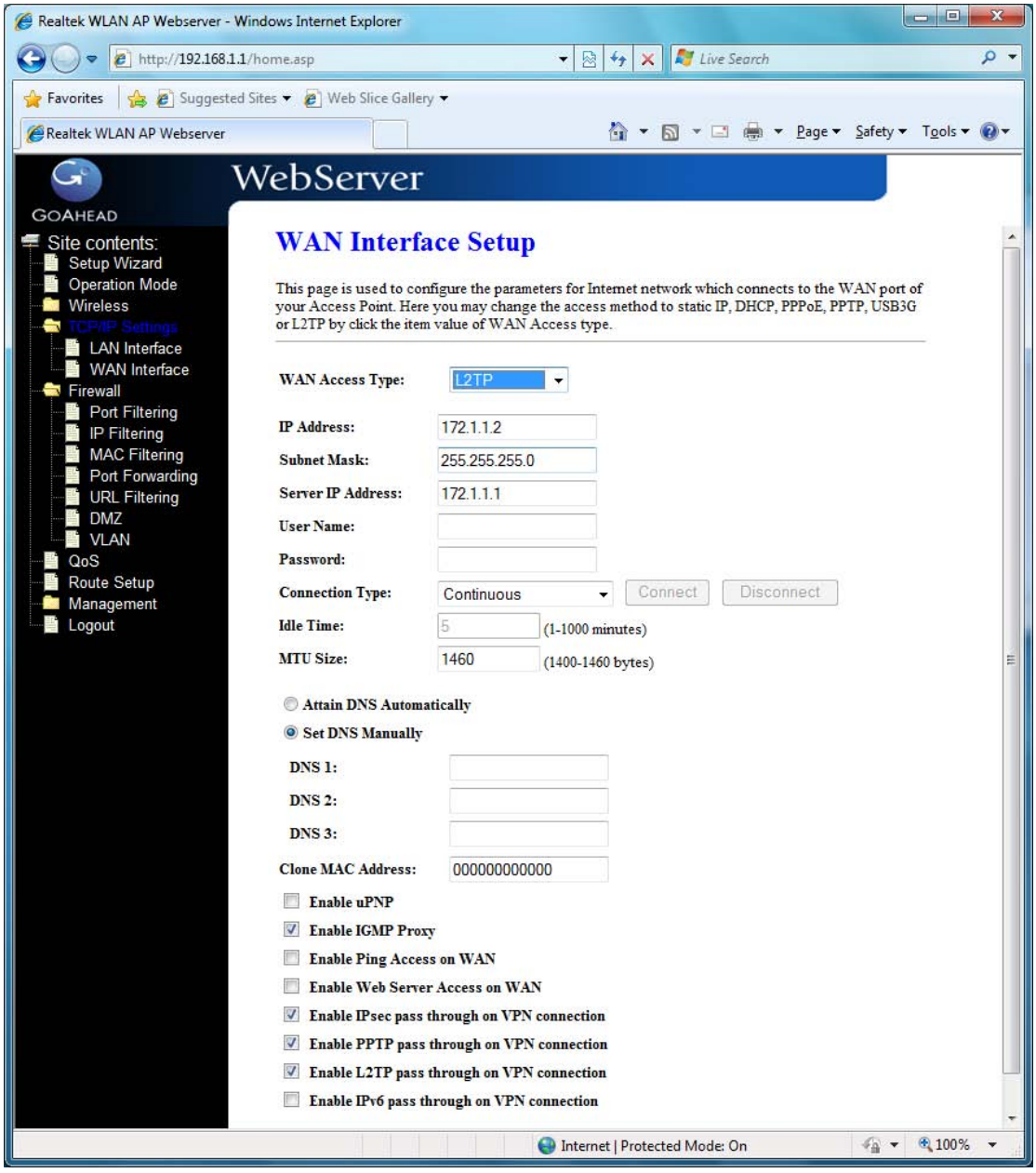
Gateway: If you select the Static L2TP support on WAN interface, fill in the gateway for WAN interface out going data packets.

Server IP Address: Enter the IP address of the L2TP Server.

Server Domain Name: Assign Domain Name and dispatch to L2TP servers. It is optional field.

User Name: If you select the L2TP support on WAN interface, fill in the user name and password to login the PPTP server.

Password: you select the L2TP support on WAN interface; fill in the user name and password to login the PPTP server.



MTU Size: Fill in the MTU size of MTU Size. The default value is 1400.

Request MPPE Encryption: Click the checkbox to enable request MPPE encryption.

Attain DNS Automatically: Click to select getting DNS address for **L2*TP*** support. Please select ***Set DNS Manually*** if the ***L2TP*** support is selected.

Set DNS Manually: Click to select getting DNS address for ***L2TP*** support.

DNS 1: Fill in the IP address of Domain Name Server 1.

DNS 2: Fill in the IP address of Domain Name Server 2.

DNS 3: Fill in the IP address of Domain Name Server 3.

Clone MAC Address: Fill in the MAC address that is the MAC address to be cloned.

Enable uPNP: Click the checkbox to enable uPNP function.

Enable IGMP Proxy: Click the checkbox to enable IGMP Proxy.

Enable Ping Access on WAN: Click the checkbox to enable WAN ICMP response.

Enable Web Server Access on WAN: Click the checkbox to enable web configuration from WAN side.

Enable IPsec pass through on VPN connection: Click the checkbox to enable IPSec packet pass through.

Enable PPTP pass through on VPN connection: Click the checkbox to enable PPTP packet pass through.

Enable L2TP pass through on VPN connection: Click the checkbox to enable L2TP packet pass through.

Apply Changes: Click the ***Apply Changes*** button to complete the new configuration setting.

Reset: Click the ***Reset*** button to abort change and recover the previous configuration setting.

[USB3G]

USB3G : This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point.

User Name: If you select the USB3G support on WAN interface, fill in the user name and password to login the USB3G server.

Password: If you select the USB3G support on WAN interface, fill in the user name and password to login the USB3G server.

Connection Type: Select the connection type from pull-down menu. There are ***Continuous***, ***Connect on Demand*** and ***Manual*** three types to select.

- ***Continuous*** connection type means to setup the connection through USB3G protocol whenever this WLAN

AP Router is powered on.

- ***Connect on Demand*** connection type means to setup the connection through USB3G protocol whenever you send the data packets out through the WAN interface; there are a watchdog implemented to close the USB3G connection while there are no data sent out longer than the idle time set.
- ***Manual*** connection type means to setup the connection through the USB3G protocol by clicking the ***Connect*** button manually, and clicking the ***Disconnect*** button manually.

Idle Time: If you select the USB3G and ***Connect on Demand*** connection type, fill in the idle time for auto-disconnect function. Value can be between 1 and 1000 minutes.

MTU Size: Fill in the MTU size of MTU Size. The default value is 1490.

Attain DNS Automatically: Click to select getting DNS address for ***DHCP*** support. Please select ***Set DNS Manually*** if the ***DHCP*** support is selected.

Set DNS Manually: Click to select getting DNS address for ***DHCP*** support.

DNS 1: Fill in the IP address of Domain Name Server 1.

DNS 2: Fill in the IP address of Domain Name Server 2.

DNS 3: Fill in the IP address of Domain Name Server 3.

Clone MAC Address: Fill in the MAC address that is the MAC address to be cloned.

Enable uPNP: Click the checkbox to enable uPNP function.

Enable IGMP Proxy: Click the checkbox to enable IGMP Proxy.

Enable Ping Access on WAN: Click the checkbox to enable WAN ICMP response.

Enable Web Server Access on WAN: Click the checkbox to enable web configuration from WAN side.

Enable IPsec pass through on VPN connection: Click the checkbox to enable IPSec packet pass through.

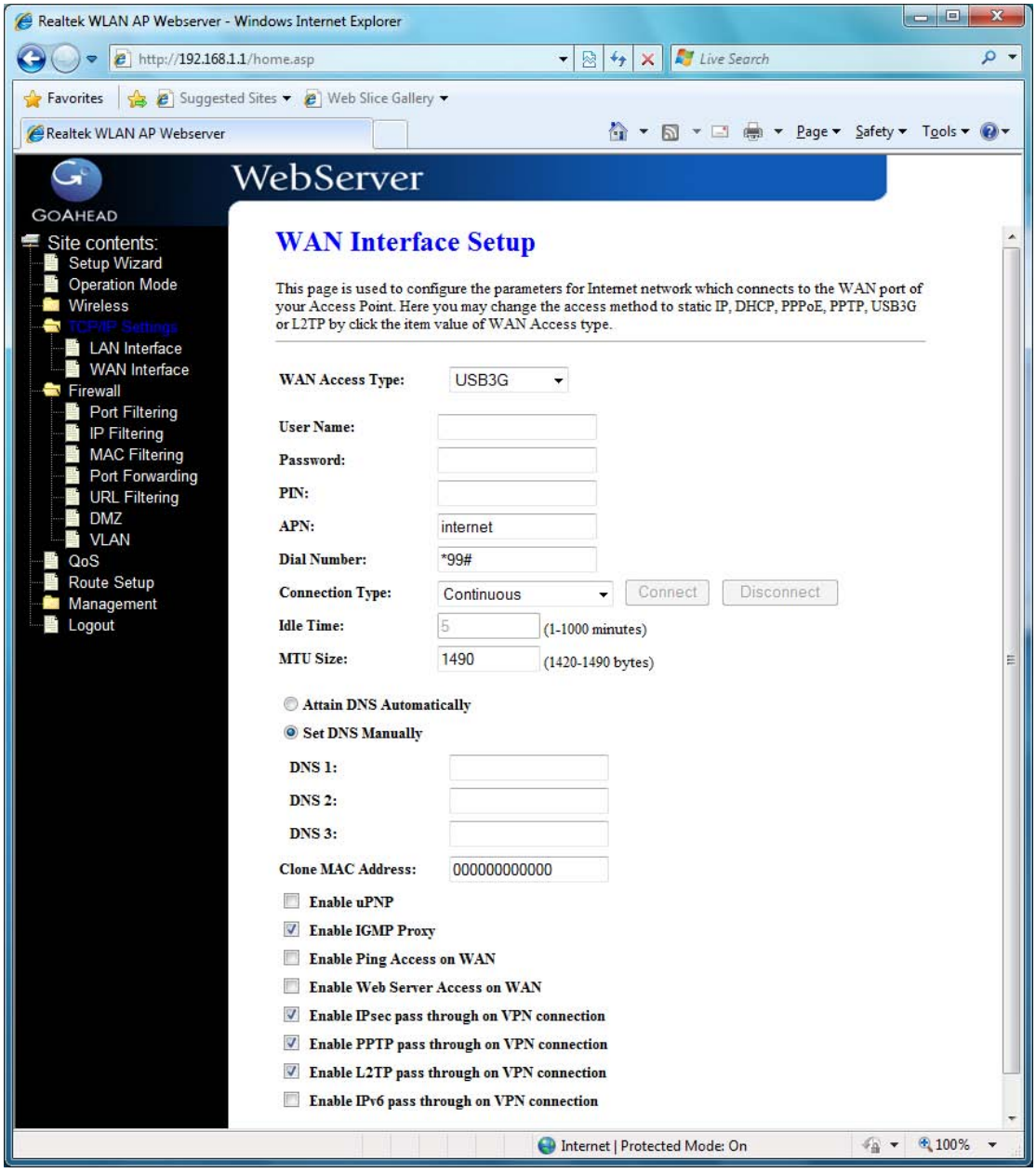
Enable PPTP pass through on VPN connection: Click the checkbox to enable PPTP packet pass through.

Enable L2TP pass through on VPN connection: Click the checkbox to enable L2TP packet pass through.

Apply Changes: Click the ***Apply Changes*** button to complete the new configuration setting.

Reset: Click the ***Reset*** button to abort change and recover the previous

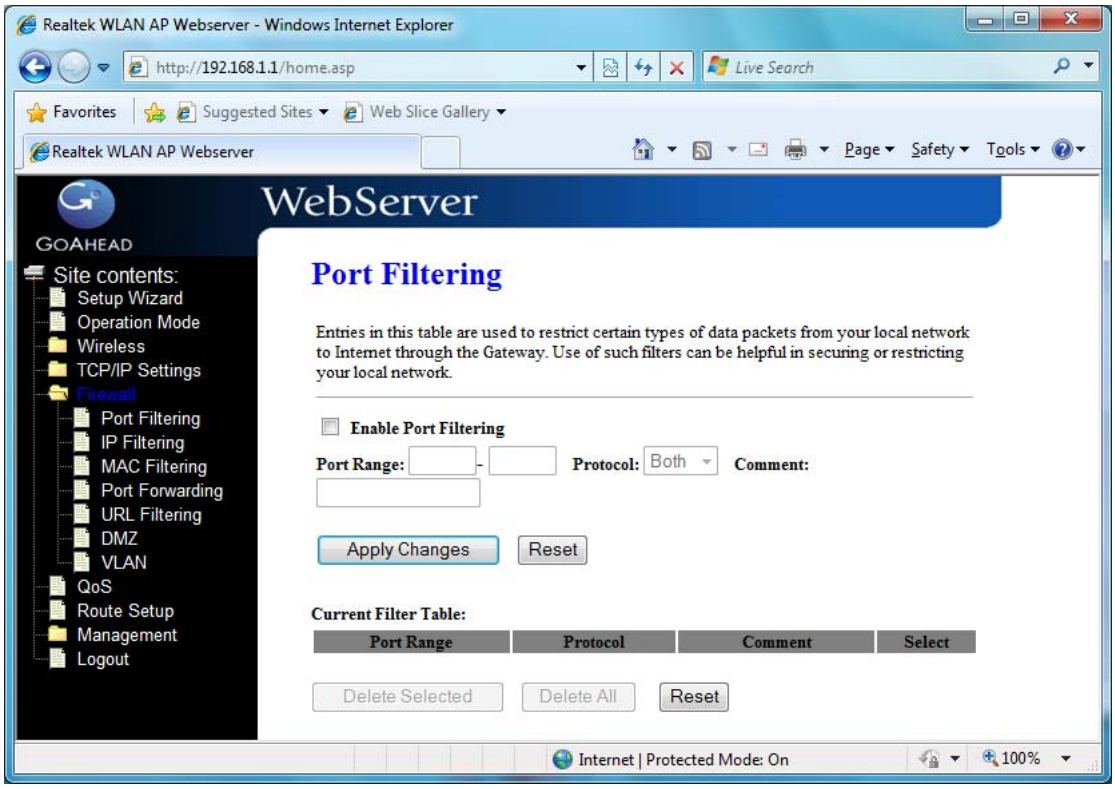
configuration setting.



3.6 Firewall

3.6.1 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: Click to enable the port filtering security function.

Port Range/Protocol/Comments: To restrict data transmission from the local network on certain ports, fill in the range of start-port and end-port, and the protocol, also put your comments on it. The ***Protocol*** can be TCP, UDP or Both. ***Comments*** let you know about whys to restrict data from the ports.

3.6.2 IP Filtering

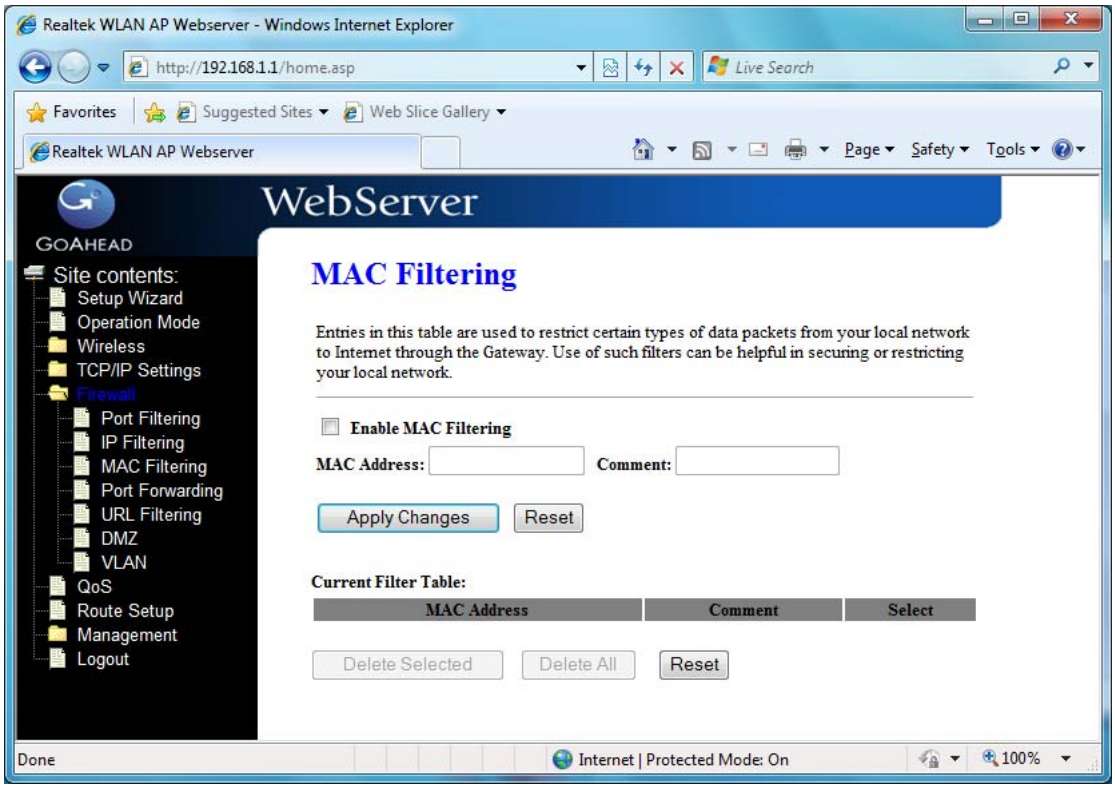
Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

Enable IP Filtering: Click to enable the IP filtering security function.

Local IP Address/Protocol/Comments: To restrict data transmission from local network on certain IP addresses, fill in the IP address and the protocol; also put your comments on it. The ***Protocol*** can be TCP, UDP or Both. ***Comments*** let you know about whys to restrict data from the IP address.

3.6.3 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.

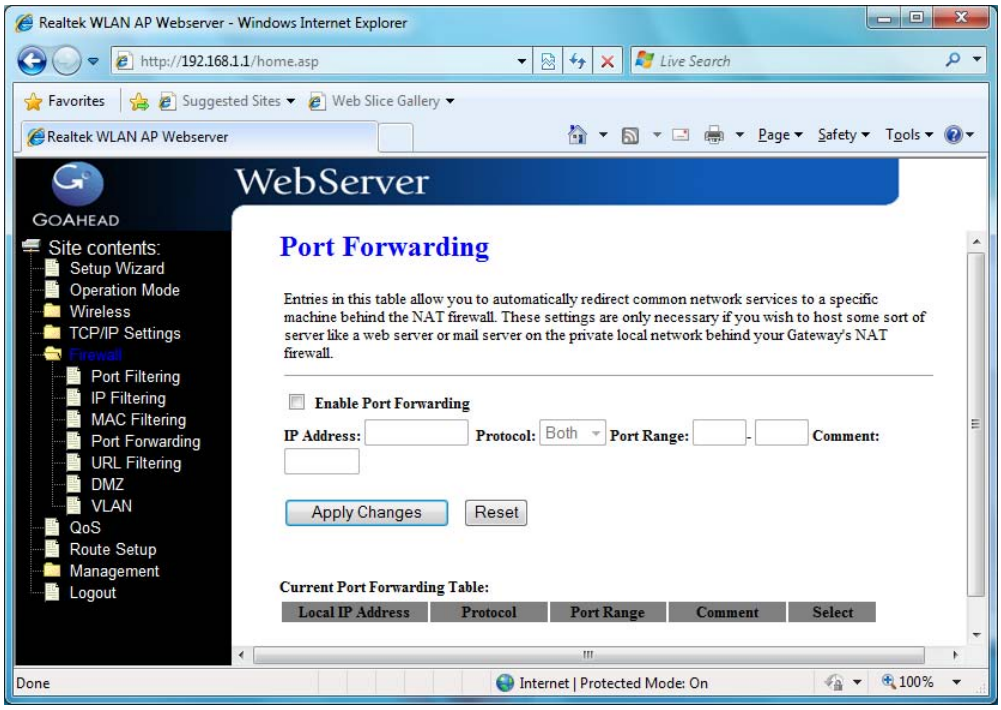


Enable MAC Filtering: Click to enable the MAC filtering security function.

MAC Address/Comments: To restrict data transmission from local network on certain MAC addresses, fill in the MAC address and your comments on it. ***Comments*** let you know about whys to restrict data from the MAC address.

3.6.4 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.

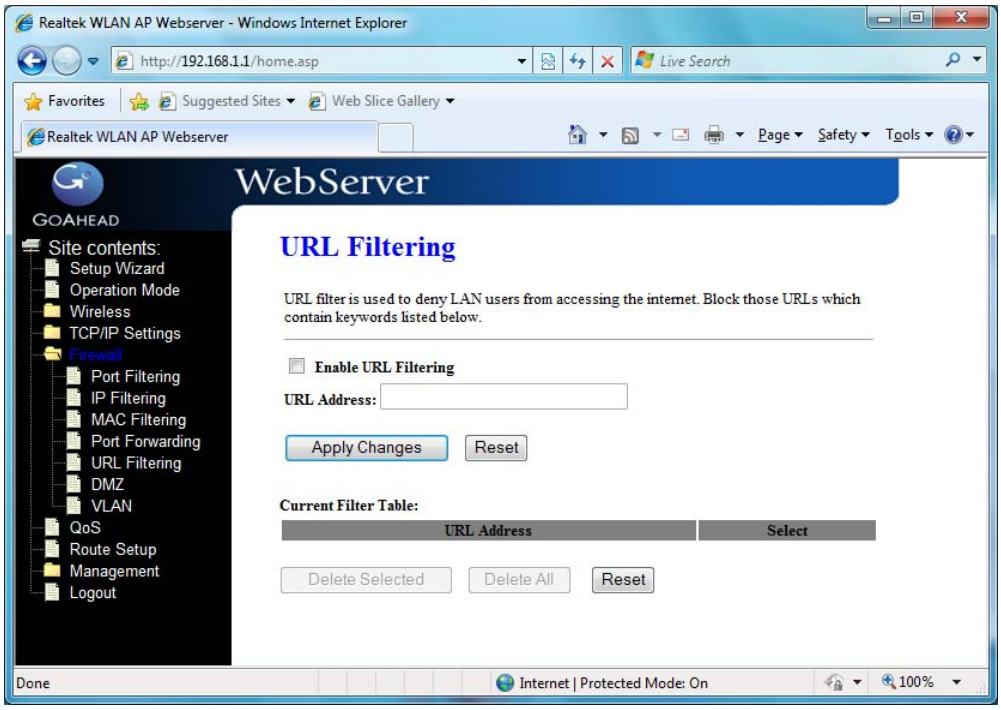


Enable Port Forwarding: Click to enable the Port Forwarding security function.

Local IP Address/Protocol/Port Range/Comment: To forward data packets coming from WAN to a specific IP address that hosted in local network behind the NAT firewall, fill in the IP address, protocol, port range and your comments. The ***Protocol*** can be TCP, UDP or Both. The ***Port Range*** is for data transmission. ***Comments*** let you know about whys to allow data packets forward to the IP address and port number.

3.6.5 URL Filter

URL Filtering is used to restrict users to access specific websites in internet.



Enable URL Filtering: Click to enable the URL Filtering function.

URL Address: Add one URL address.

3.6.6 DMZ

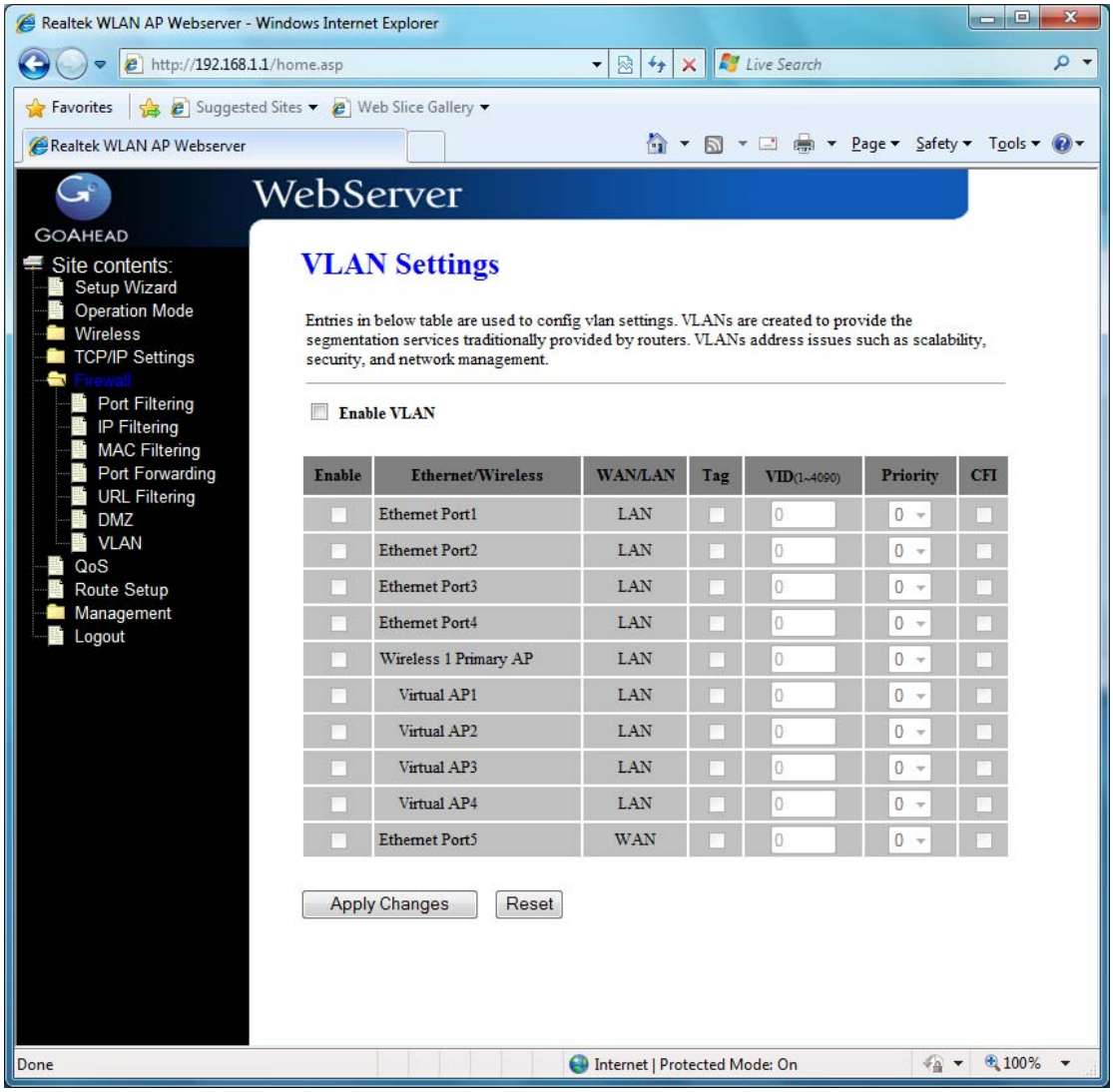
A Demilitarized Zone is used to provide Internet services without sacrificing unauthorized access to its local private network. Typically, the DMZ host contains devices accessible to Internet traffic, such as Web (HTTP) servers, FTP servers, SMTP (e-mail) servers and DNS servers.

Enable DMZ: Click to enable the DMZ function.

DMZ Host IP Address: To support DMZ in your firewall design, fill in the IP address of DMZ host that can be access from the WAN interface.

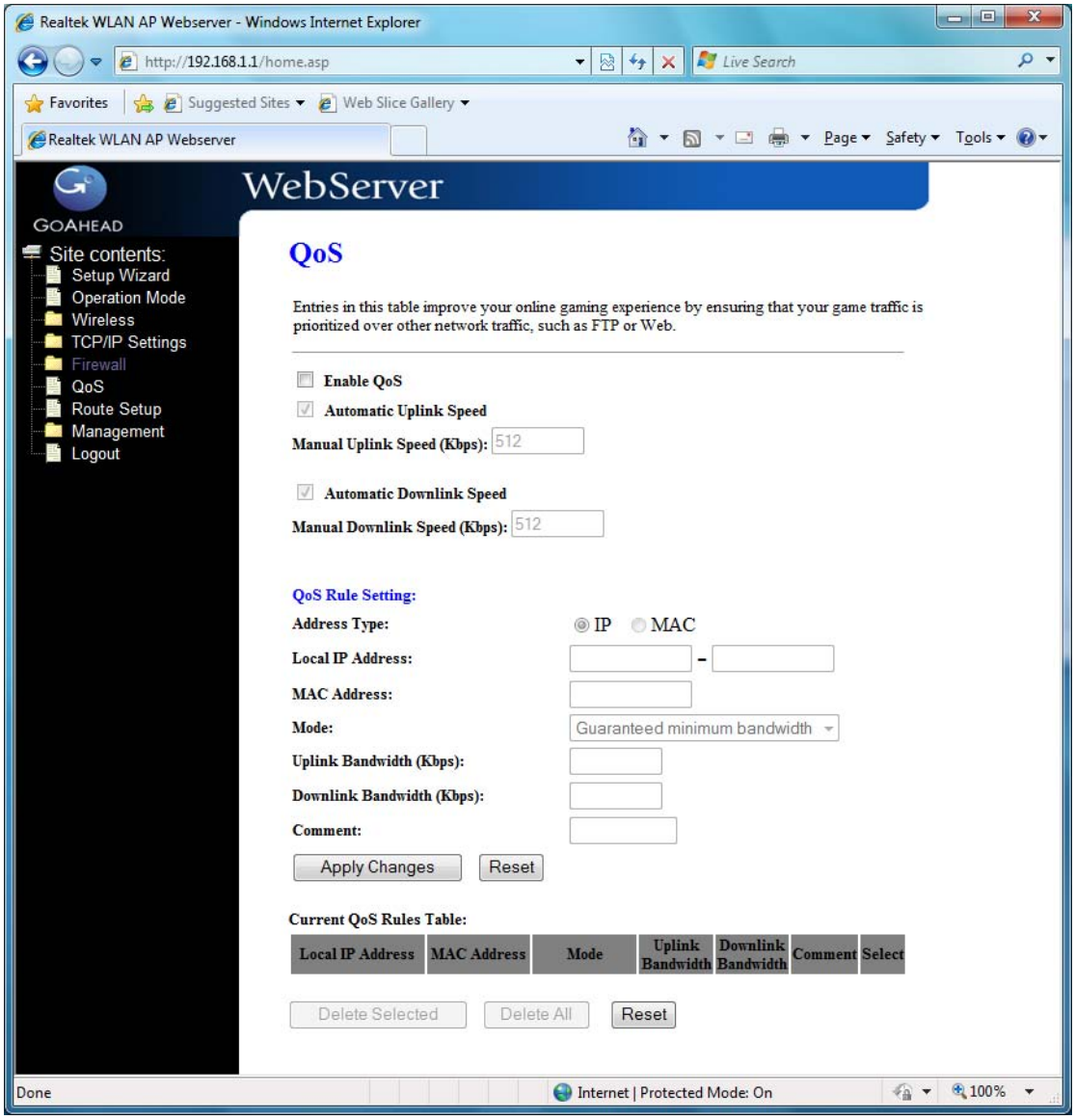
3.6.7 VLAN

Enter in below table are used to configure VLAN settings. VLANs are created to provide the segmentation services traditionally provided by routers. VLANs address issue such as scalability, security, and network management.



3.7 QoS

Entries in this table improve your online gaming experience by ensuring that your game traffic is prioritized over other network traffic, such as FTP or Web.

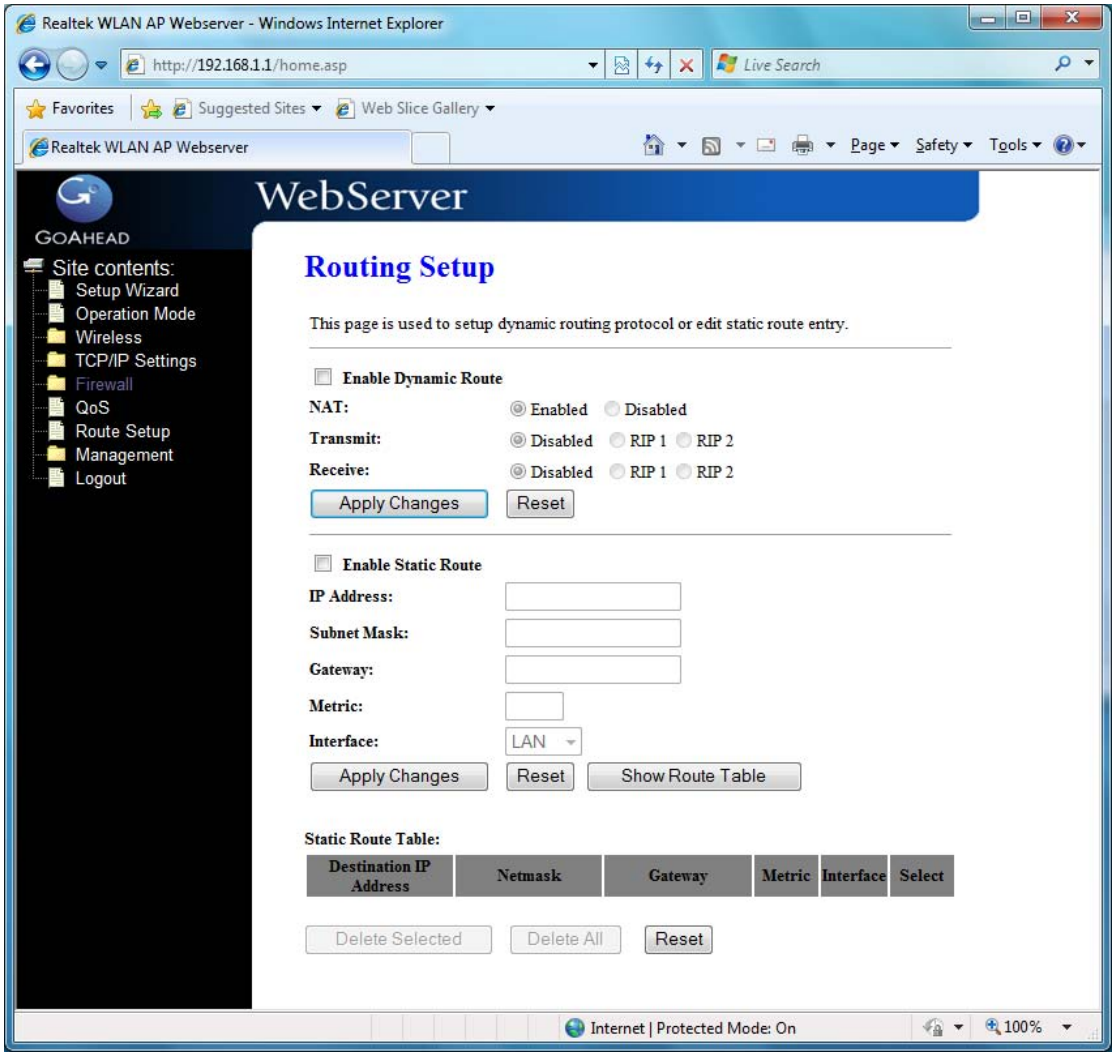


How to setup your QoS:

1. In **QoS** Setup Section, **Enable QoS** feature.
2. Choose Uplink & Downlink Speed: "**Automatic**" or "**Manual**"
3. Select Address Type: "**IP**" or "**Address**"
4. Configure QoS Rules – Mode("**Guaranteed Minimum bandwidth**" & "**Restricted Maximum bandwidt**h"), Uplink/Downlink Bandwidth, Comment.
5. Click "**Apply Changes**" to save QoS configurations.

3.8 Route Setup

This page is used to setup dynamic routing protocol or edit static route entry.



[Dynamic Route]

Dynamic routing is a technique developed to automatically adjust routing tables in the event of network failures. The most common dynamic routing protocols is RIP (Routing Information Protocol), which is very common on small networks.

[Static Route]

It menu allows you to define your own static routes for network traffic. Follow the instructions below to define a static router:

1. Enter the target IP address in the textbox near '**IP Address**'.
2. Enter the subnet mask in the textbox near '**Subnet Mask**'.
3. Enter the gateway IP address in the textbox near '**Gateway**'.
4. Enter the number of 'hops' in the textbox near '**Metric**' (normally you can set the value to '0').

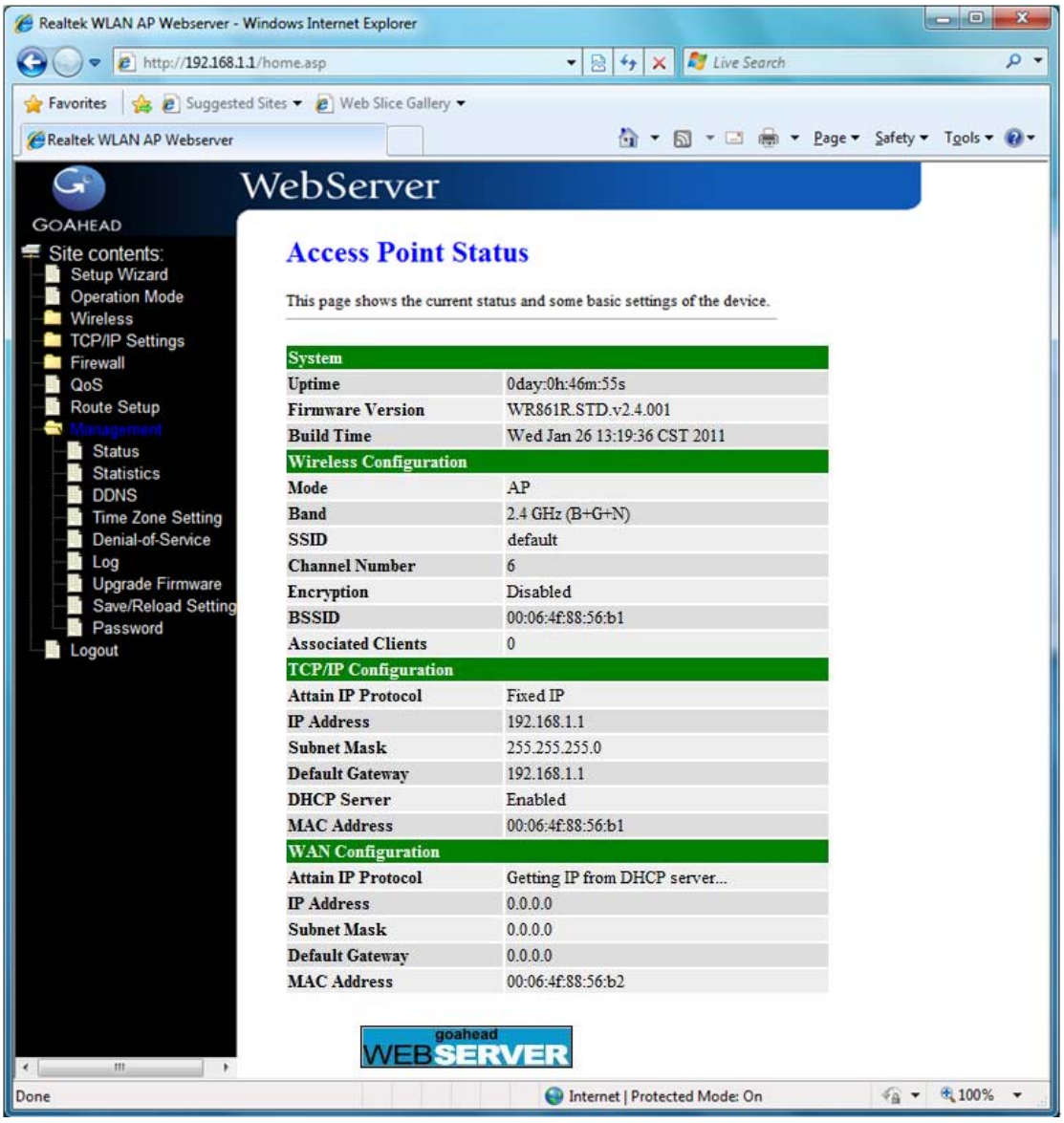
5. Select the correct port type in the dropdown box near '**Interface**'.

6. Click the '**Apply Changes**' button to add the route.

3.9 Management

3.9.1 Status

This page shows the current status and some basic settings of the device, includes system, wireless, Ethernet LAN and WAN configuration information.



[System]

Uptime: It shows the duration since WLAN AP Router is powered on.

Firmware version: It shows the firmware version of WLAN AP Router.

[Wireless configuration]

Mode: It shows wireless operation mode

Band: It shows the current wireless operating frequency.

SSID: It shows the SSID of this WLAN AP Router. The SSID is the unique name of

WLAN AP Router and shared among its service area, so all device sat tempts to join the same wireless network can identify it.

Channel Number: It shows the wireless channel connected currently.

Encryption: It shows the status of encryption function.

Associated Clients: It shows the number of connected clients (or stations, PCs).

BSSID: It shows the BSSID address of the WLAN AP Router BSSID is a six-byte address.

[LAN configuration]

IP Address: It shows the IP address of LAN interfaces of WLAN AP Router.

Subnet Mask: It shows the IP subnet mask of LAN interfaces of WLAN AP Router.

Default Gateway: It shows the default gateway setting for LAN interfaces outgoing data packets.

DHCP Server: It shows the DHCP server is enabled or not.

MAC Address: It shows the MAC address of LAN interfaces of WLAN AP Router.

[WAN configuration]

Attain IP Protocol: It shows how the WLAN AP Router gets the IP address. The IP address can be set manually to a fixed one or set dynamically by DHCP server or attain IP by PPPoE / PPTP connection.

IP Address: It shows the IP address of WAN interface of WLAN AP Router.

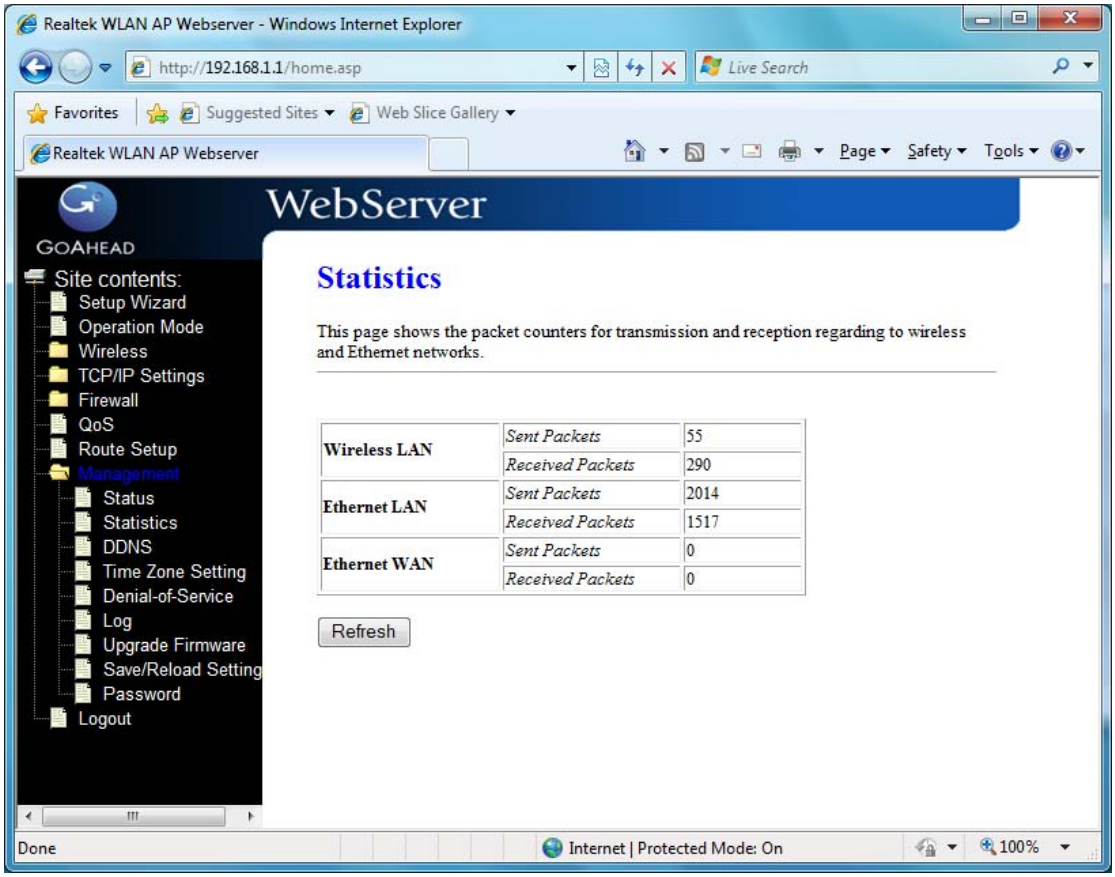
Subnet Mask: It shows the IP subnet mask of WAN interface of WLAN AP Router.

Default Gateway: It shows the default gateway setting for WAN interface outgoing data packets.

MAC Address: It shows the MAC address of WAN interface of WLAN AP Router.

3.9.2 Statistics

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



[Wireless LAN]

Sent Packets: It shows the statistic count of sent packets on the wireless LAN interface.

Received Packets: It shows the statistic count of received packets on the wireless LAN interface.

[Ethernet LAN]

Sent Packets: It shows the statistic count of sent packets on the Ethernet LAN interface.

Received Packets: It shows the statistic count of received packets on the Ethernet LAN interface.

[Ethernet WAN]

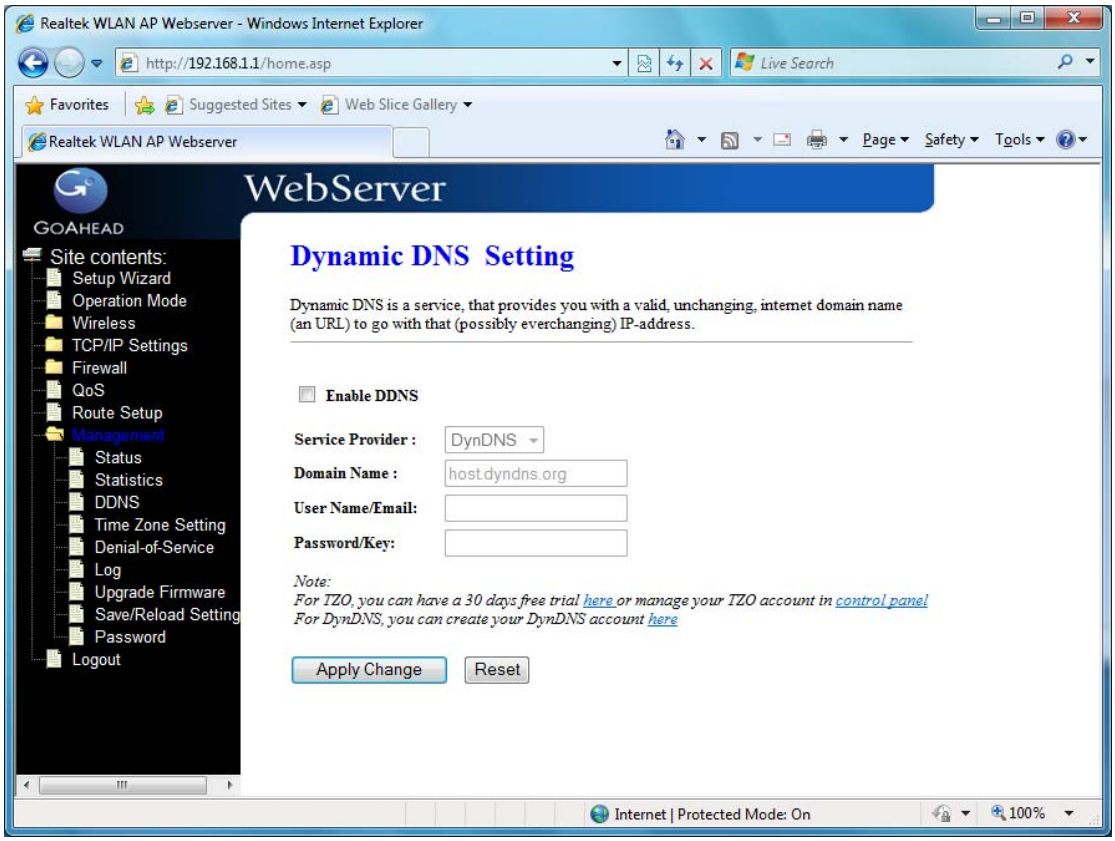
Sent Packets: It shows the statistic count of sent packets on the Ethernet WAN interface.

Received Packets: It shows the statistic count of received packets on the Ethernet WAN interface.

Refresh: Click the refresh the statistic counters on the screen.

3.9.3 DDNS

This page is used to configure Dynamic DNS service to have DNS with dynamic IP address.



Enable DDNS: Click the checkbox to enable ***DDNS*** service.

Service Provider: Click the drop down menu to pickup the right provider.

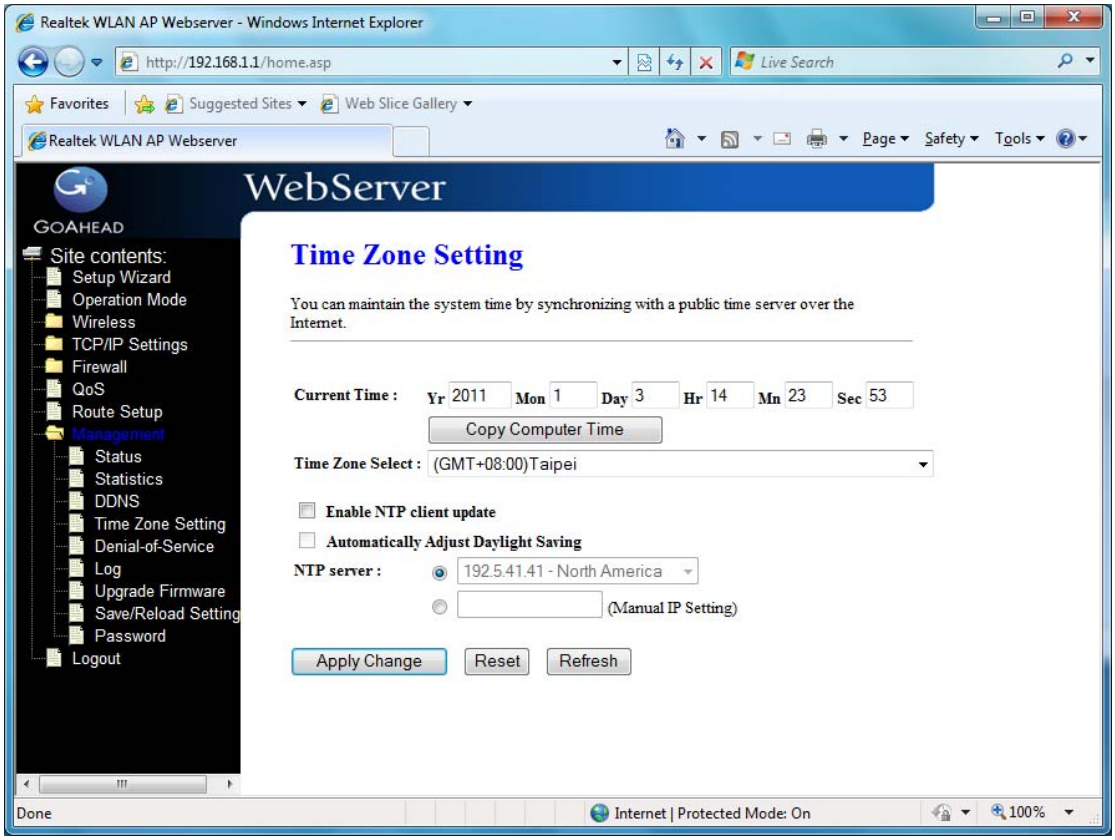
Domain Name: To configure the Domain Name.

User Name/Email: Configure User Name, Email.

Password/Key: Configure Password, Key.

3.9.4 Time Zone Setting

Click the Reset button to abort change and recover the previous configuration setting.



Current Time: It shows the current time.

Time Zone Select: Click the time zone in your country.

Enable NTP client update: Click the checkbox to enable NTP client update.

NTP Server: Click select default or input NTP server IP address.

Apply Change: Click the ***Apply Changes*** button to save and enable NTP client service.

Reset: Click the ***Reset*** button to abort change and recover the previous configuration setting.

Refresh: Click the refresh the current time shown on the screen.

3.9.5 Denial-of-Service

This page is used to enable and setup protection to prevent attack by hacker's program. It provides more security for users.

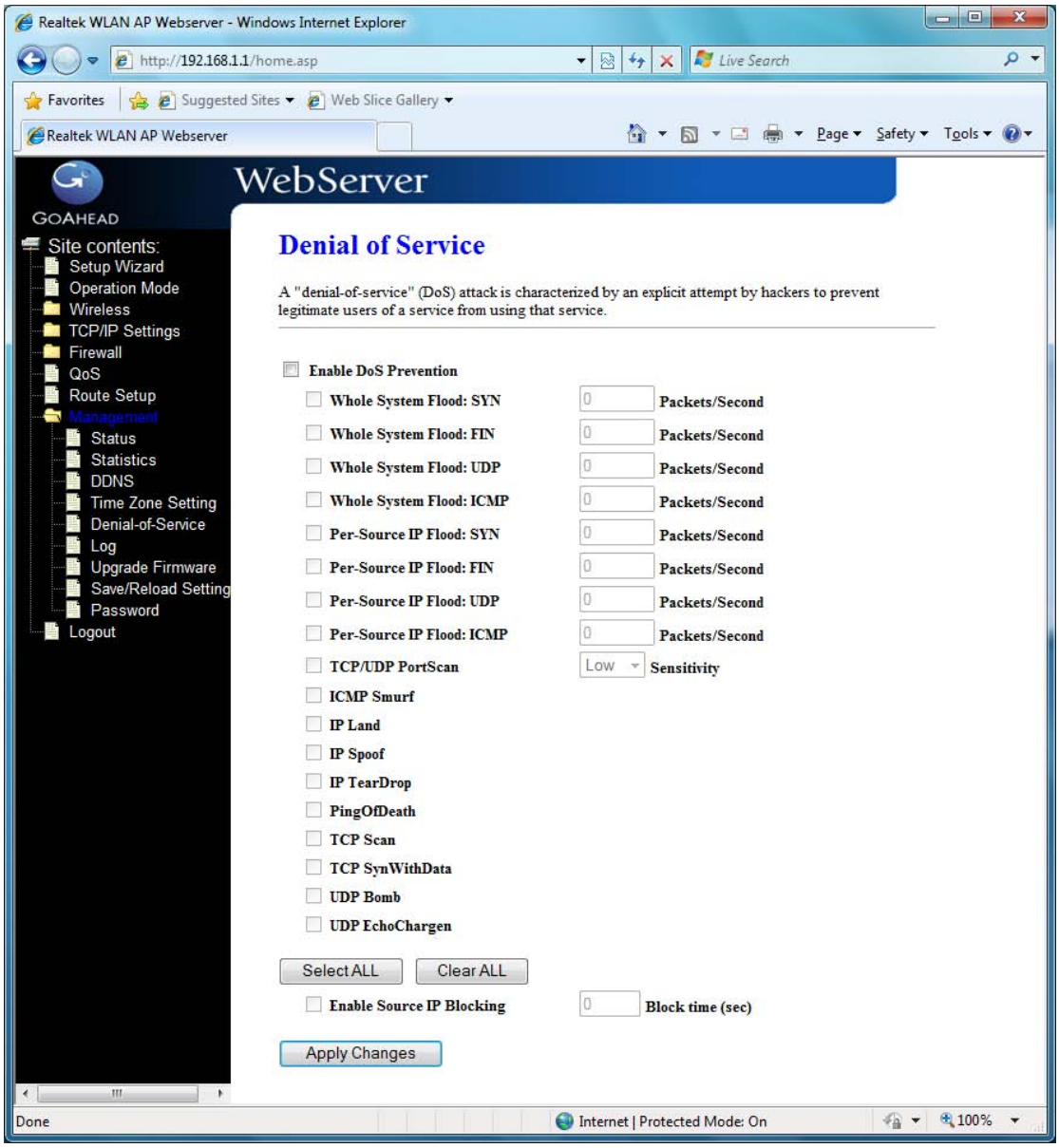
Enable DoS Prevention: Click the checkbox to enable DoS prevention.

Whole System Flood / Per-Source IP Flood...: Enable and setup prevention in details.

Select ALL: Click the checkbox to enable all prevention items.

Clear ALL: Click the checkbox to disable all prevention items.

Apply Changes: Click the ***Apply Changes*** button to save above settings.

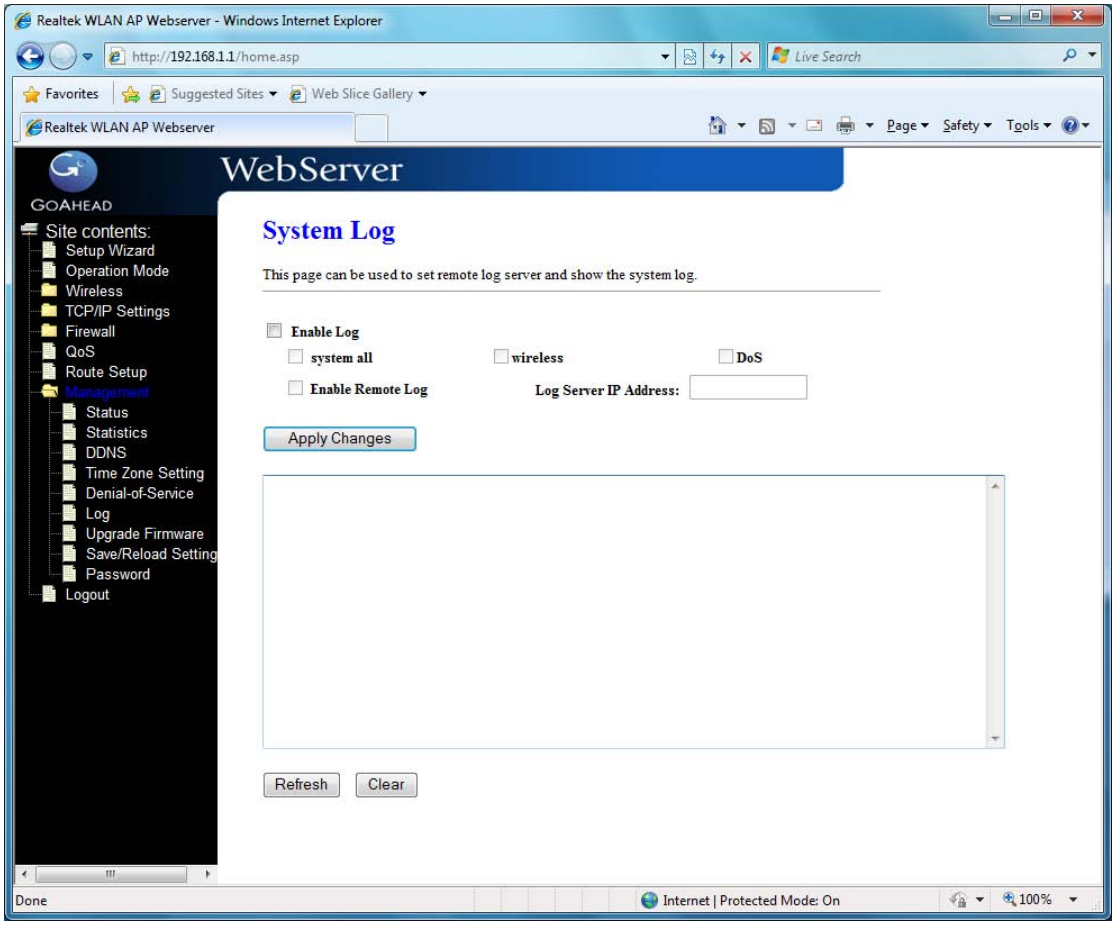


3.9.6 Log

This page is used to configure the remote log server and shown the current log.

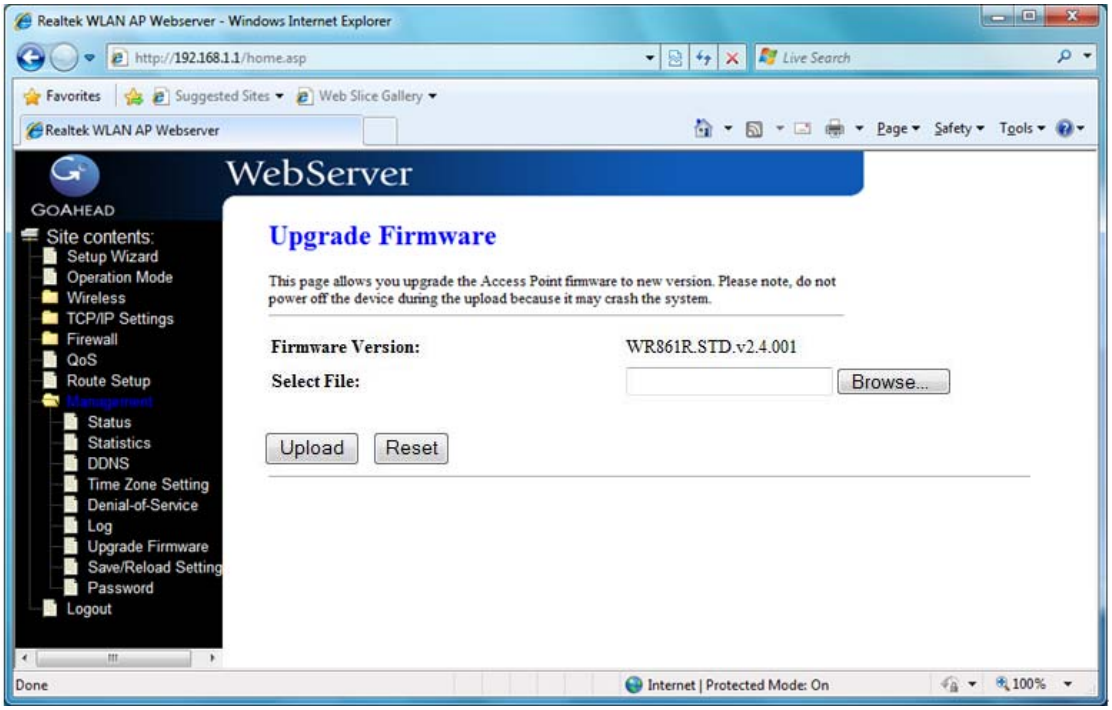
Enable Log: Click the checkbox to enable log.
System all: Show all log of wireless broadband router.
Wireless: Only show wireless log
DoS: Only show Denial-of-Service log
Enable Remote Log: Click the checkbox to enable remote log service.
Log Server IP Address: Input the remote log IP address.
Apply Changes: Click the ***Apply Changes*** button to save above settings.
Refresh: Click the refresh the log shown on the screen.

Clear: Clear log display screen.



3.9.7 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.



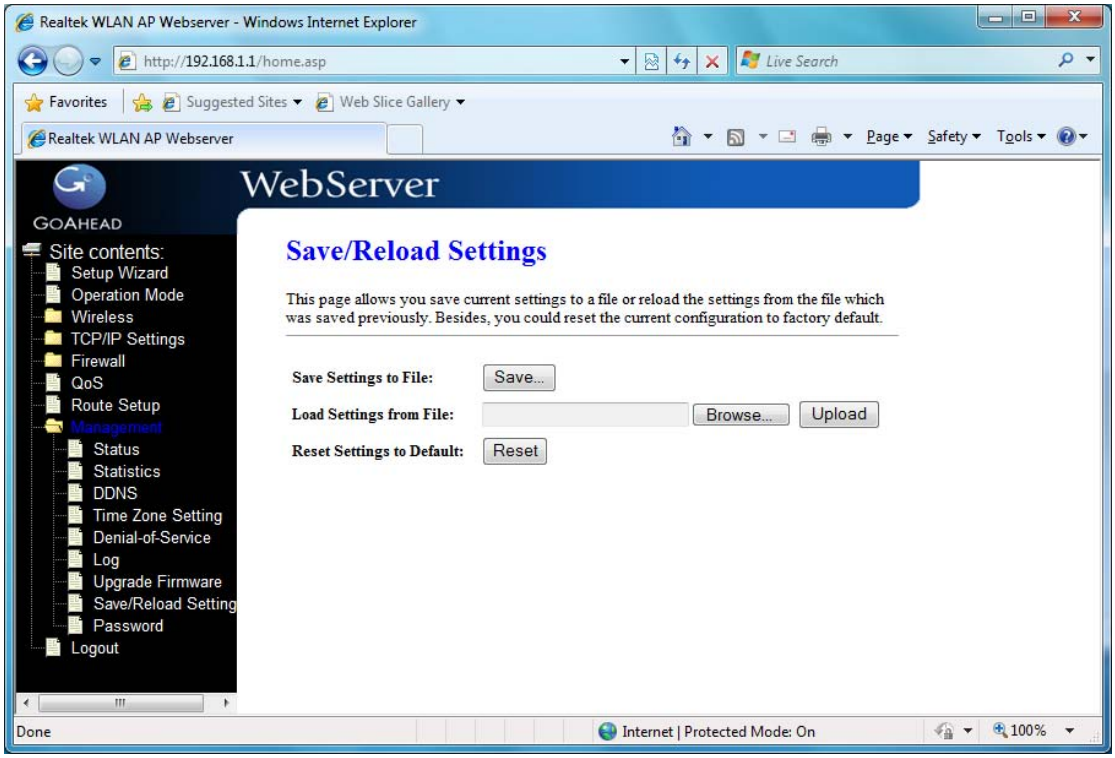
Select File: Click the ***Browse*** button to select the new version of web firmware image file.

Upload: Click the ***Upload*** button to update the selected web firmware image to the WLAN Broadband Router.

Reset: Click the ***Reset*** button to abort change and recover the previous configuration setting.

3.9.8 Save/Reload Setting

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



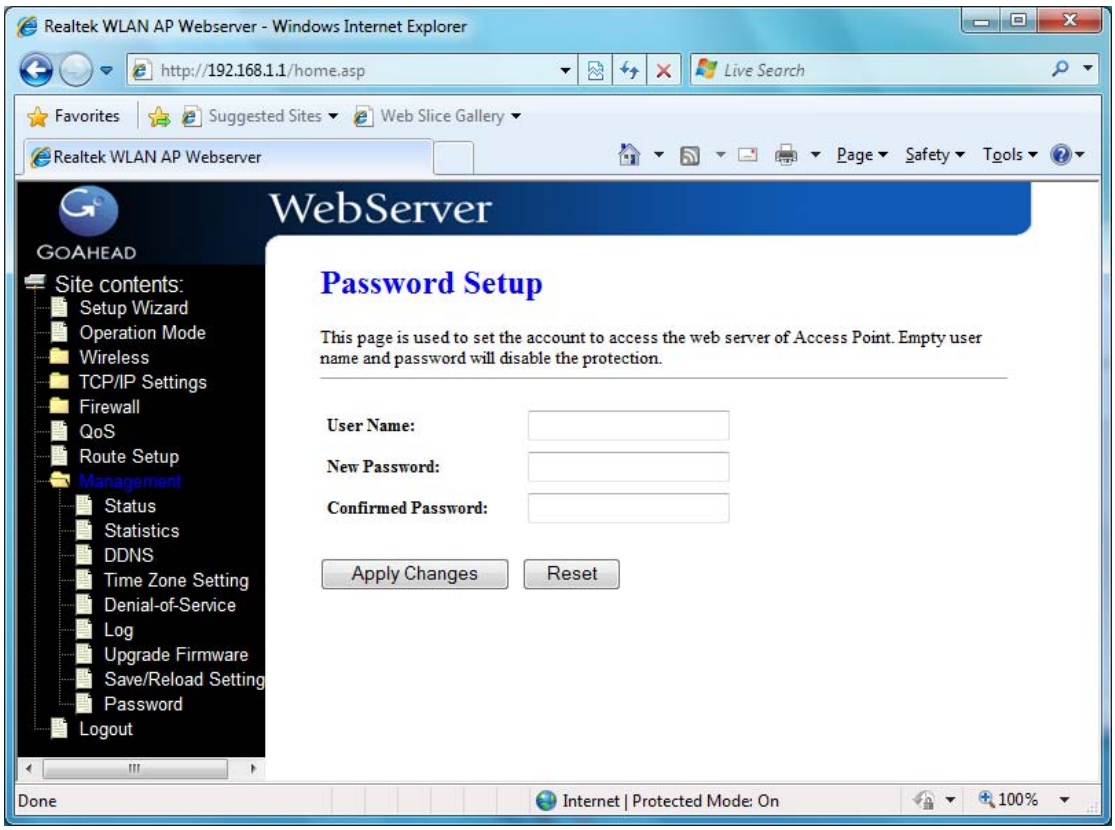
Save Settings to File: Click the Save button to download the configuration parameters to your personal computer.

Load Settings from File: Click the Browse button to select the configuration files then click the Upload button to update the selected configuration to the WLAN Broadband Router.

Reset Settings to Default: Click the Reset button to reset the configuration parameter to factory defaults.

3.9.9 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: Fill in the user name for web management login control.

New Password: Fill in the password for web management login control.

Confirmed Password: Because of the password input is invisible, fill in the password again for confirming purpose.

Apply Changes: Clear the User Name and Password fields to empty, means to apply no web management login control. Click the Apply Changes button to complete the new configuration setting.

Reset: Click the Reset button to abort change and recover the previous configuration setting.