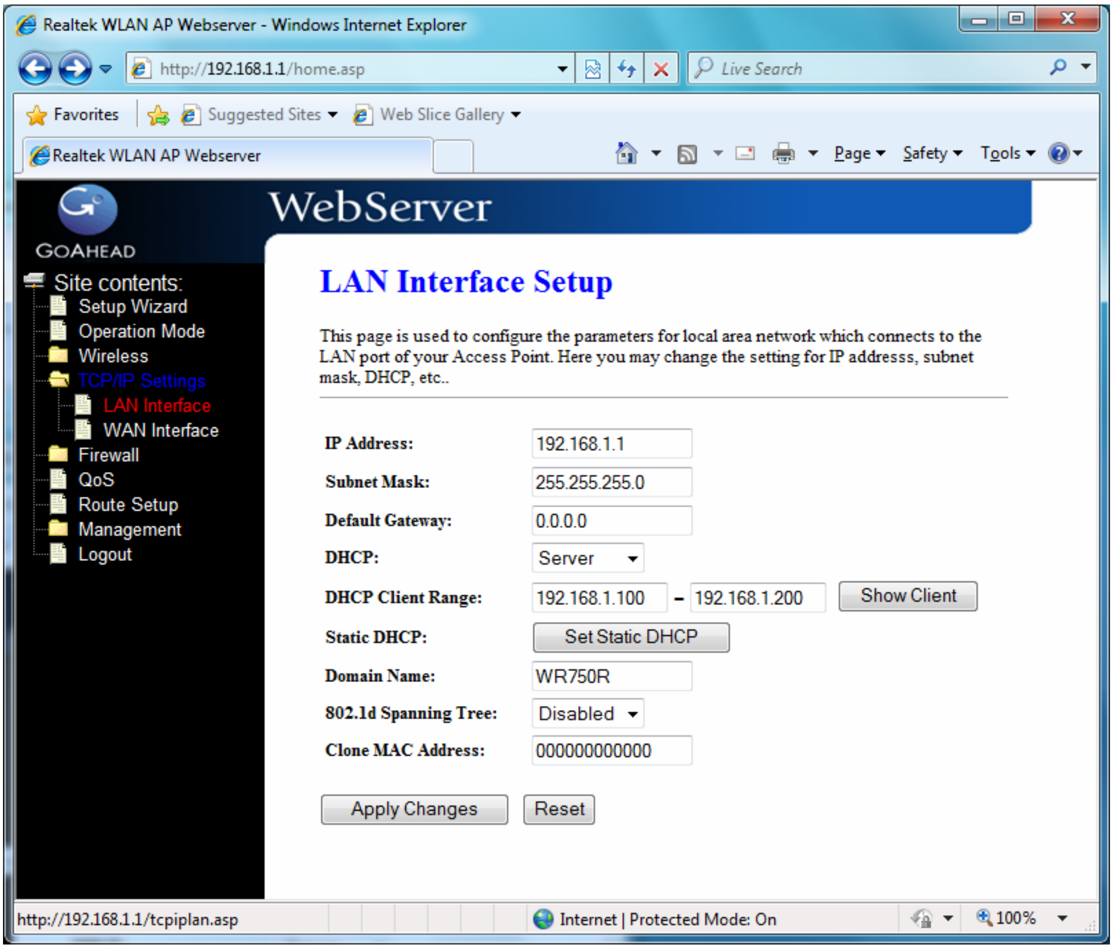


LAN Interface Setup

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:	192.168.1.1
Subnet Mask:	255.255.255.0
Default Gateway:	0.0.0.0
DHCP:	Server
DHCP Client Range:	192.168.1.100 – 192.168.1.200
Domain Name:	WR750R
802.1d Spanning Tree:	Disabled
Clone MAC Address:	000000000000

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]

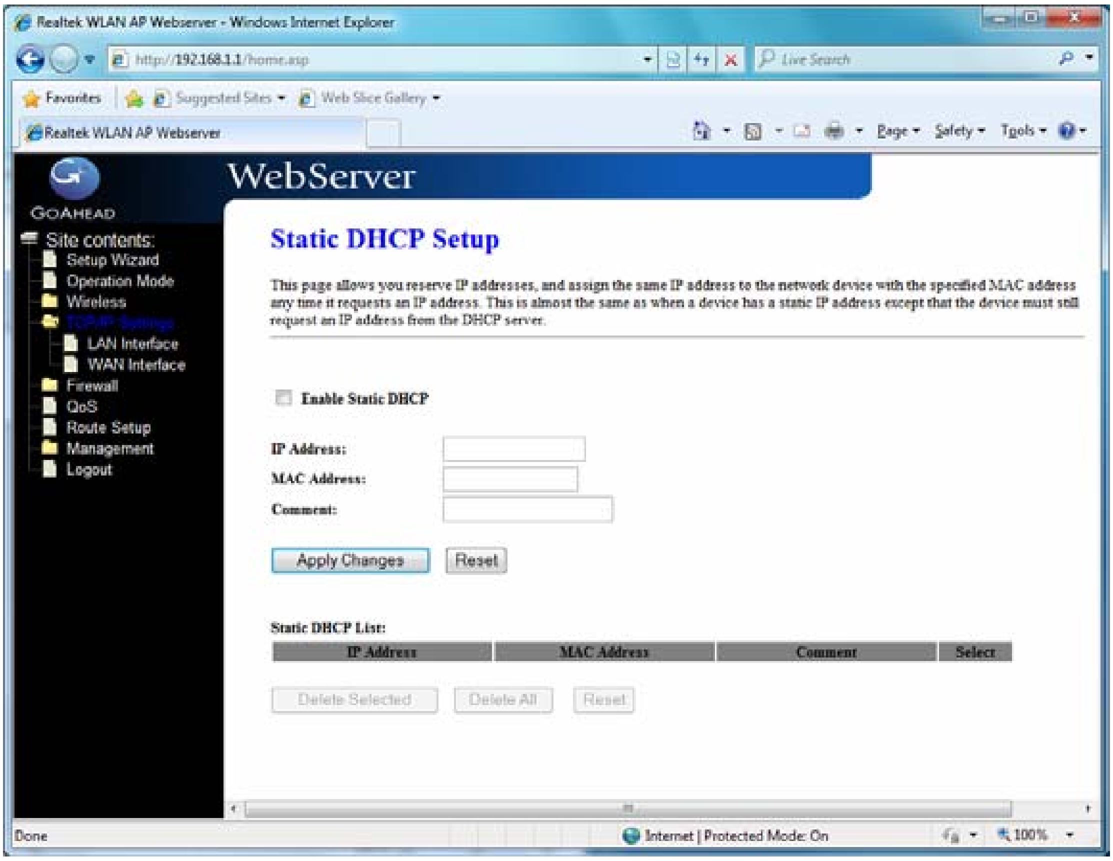
Domain Name: Assign Domain Name and dispatch to DHCP clients. It is optional field.

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.



Static DHCP Setup

This page allows you reserve IP addresses, 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.

□ Enable Static DHCP

IP Address:

MAC Address:

Comment:

Apply Changes | Reset

Static DHCP List:

IP Address	MAC Address	Comment	Select

Delete Selected | Delete All | Reset

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.

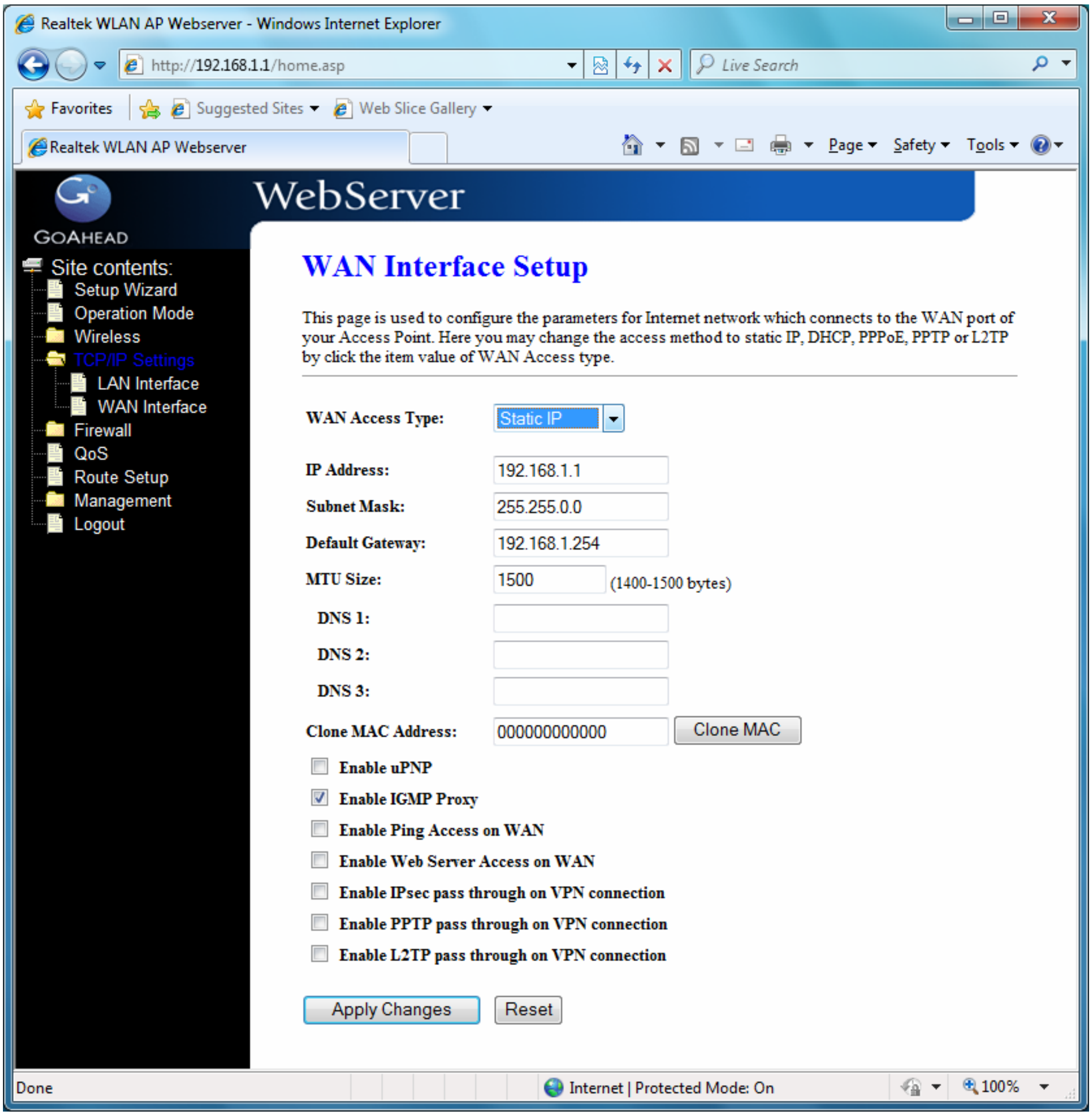
Delete All: Click to delete all the registered clients from the Static DHCP list.

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]



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, PPTP or L2TP by click the item value of WAN Access type.

WAN Access Type:	Static IP
IP Address:	192.168.1.1
Subnet Mask:	255.255.0.0
Default Gateway:	192.168.1.254
MTU Size:	1500 (1400-1500 bytes)
DNS 1:	
DNS 2:	
DNS 3:	
Clone MAC Address:	000000000000 Clone MAC

□ Enable uPNP
☑ Enable IGMP Proxy
□ 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

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.

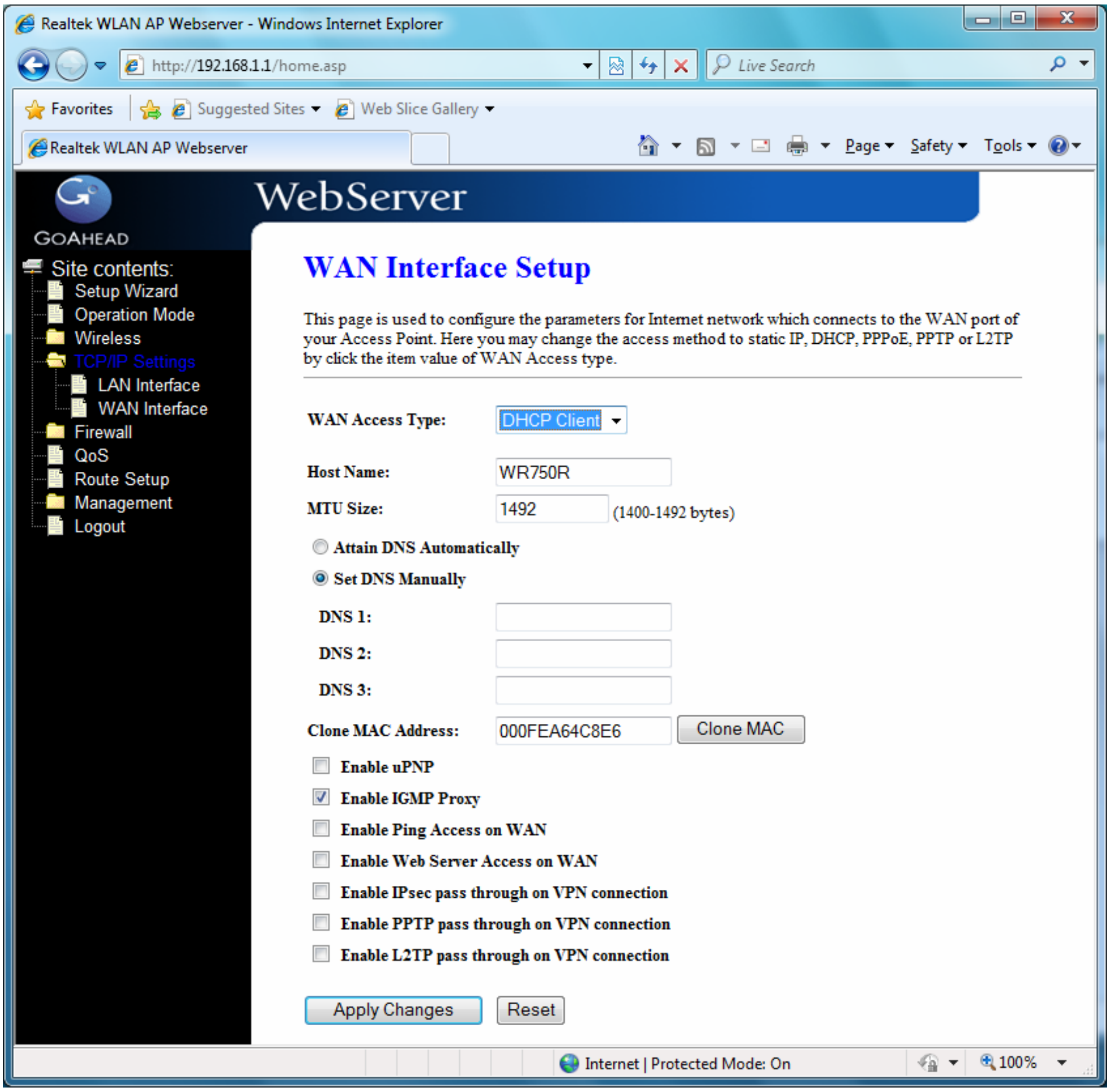
Enable PPTP pass through on VPN connection: Click the checkbox to enable PPTP packet pass through.

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]



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, PPTP or L2TP by click the item value of WAN Access type.

WAN Access Type:	DHCP Client
Host Name:	WR750R
MTU Size:	1492 (1400-1492 bytes)

○ Attain DNS Automatically

● Set DNS Manually

DNS 1:	
DNS 2:	
DNS 3:	
Clone MAC Address:	000FEA64C8E6 [Clone MAC]

□ Enable uPNP

☑ Enable IGMP Proxy

□ 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

[Apply Changes] [Reset]

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.

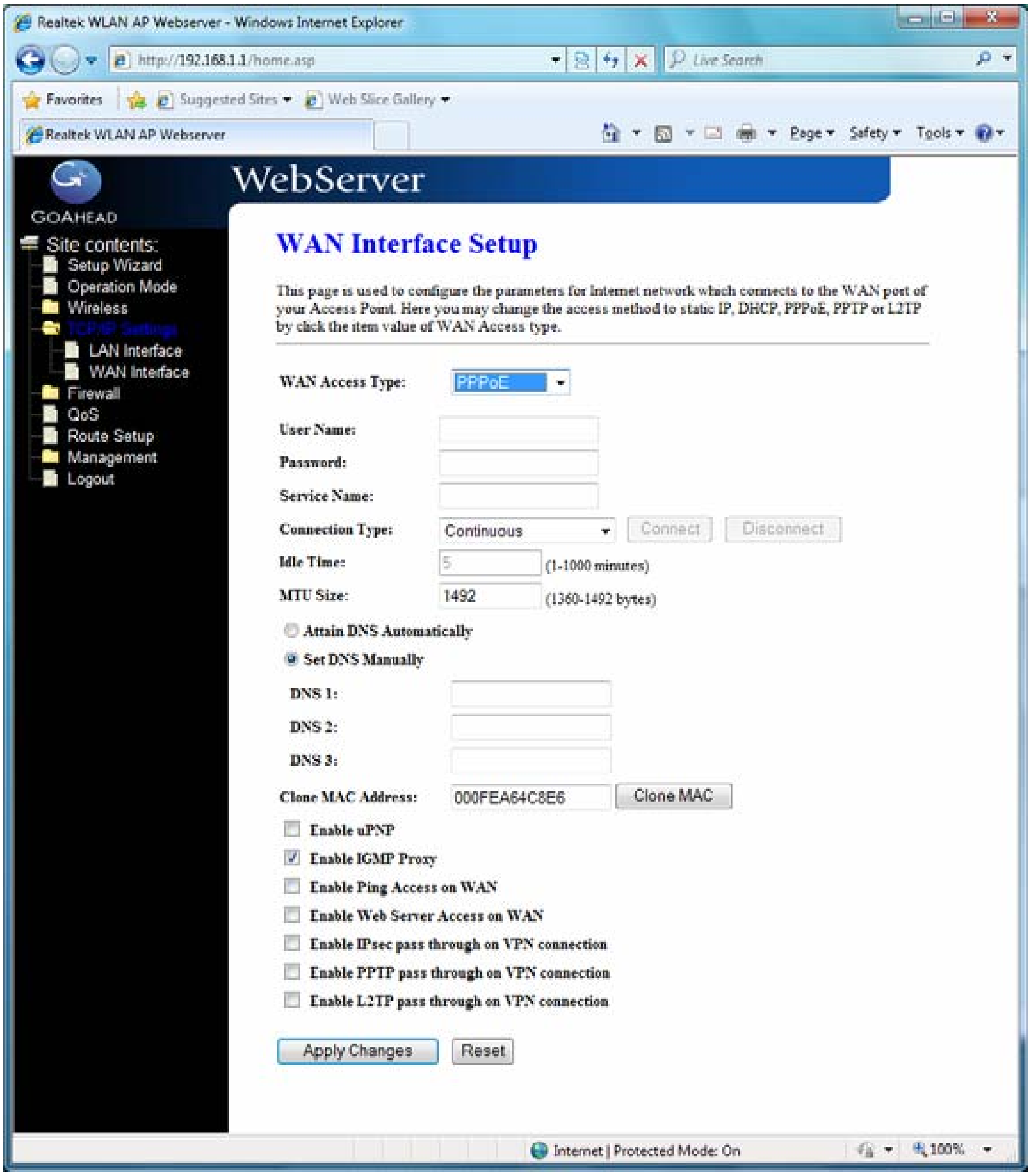
Enable IPsec pass through on VPN connection: Click the checkbox to enable IPSec packet pass through.

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.



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, PPTP or L2TP by click the item value of WAN Access type.

WAN Access Type: PPPoE

User Name:

Password:

Service Name:

Connection Type: Continuous

Idle Time: 5 (1-1000 minutes)

MTU Size: 1492 (1360-1492 bytes)

○ Attain DNS Automatically

● Set DNS Manually

DNS 1:

DNS 2:

DNS 3:

Clone MAC Address: 000FEA64C8E6

□ Enable uPNP

☑ Enable IGMP Proxy

□ 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

[PPTP]

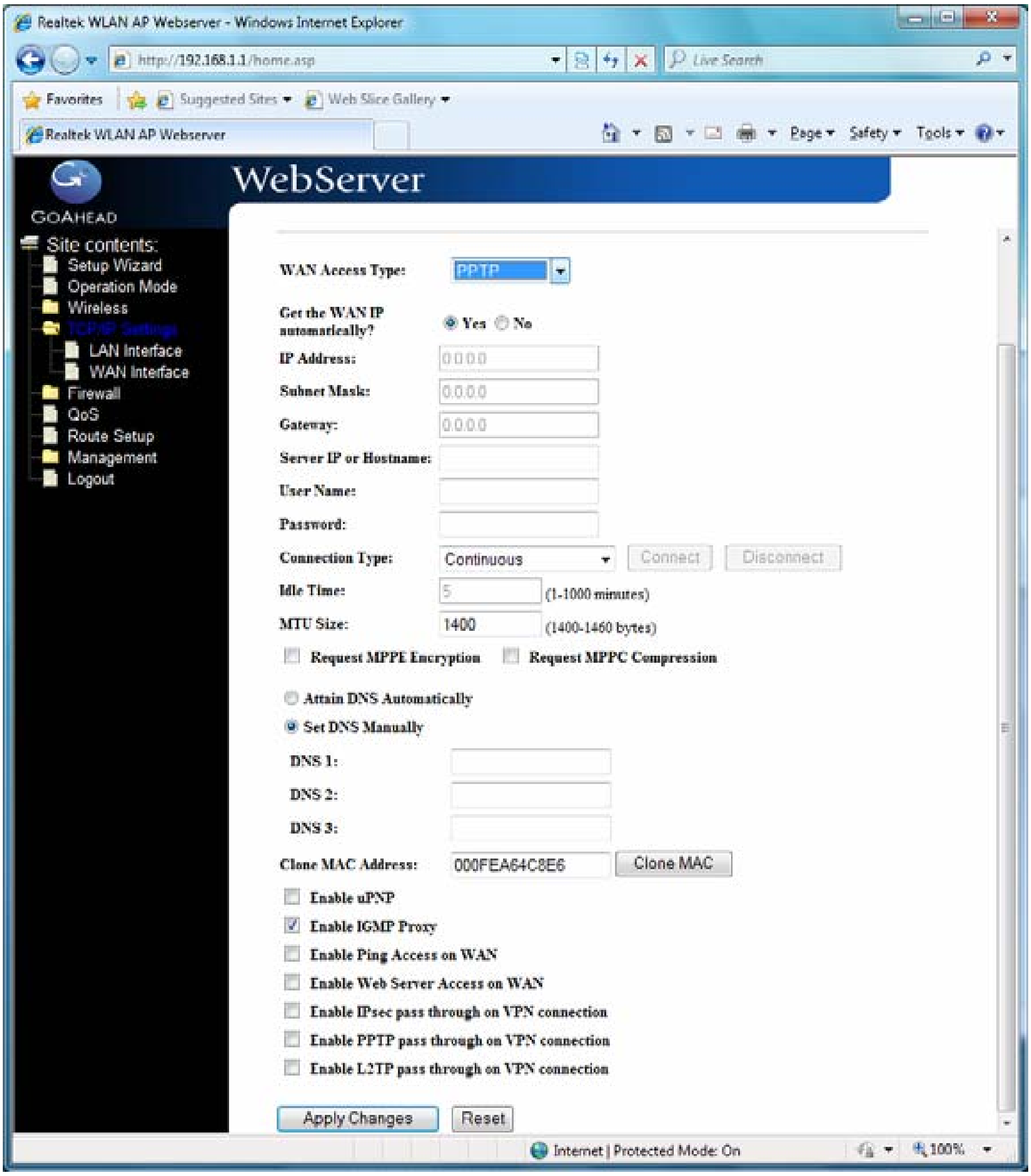
PPTP: Allow user to make a tunnel with remote site directly to secure the data transmission among the connection. User can use embedded PPTP client supported by this router to make a VPN connection.

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.



WAN Access Type:	PPTP
Get the WAN IP automatically?	● Yes ○ No
IP Address:	0.0.0.0
Subnet Mask:	0.0.0.0
Gateway:	0.0.0.0
Server IP or Hostname:	
User Name:	
Password:	
Connection Type:	Continuous [Connect] [Disconnect]
Idle Time:	5 (1-1000 minutes)
MTU Size:	1400 (1400-1460 bytes)

□ Request MPPE Encryption □ Request MPPC Compression

○ Attain DNS Automatically

● Set DNS Manually

DNS 1:	
DNS 2:	
DNS 3:	
Clone MAC Address:	000FEA64C8E6 [Clone MAC]

□ Enable uPNP

☑ Enable IGMP Proxy

□ 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

[Apply Changes] [Reset]

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.

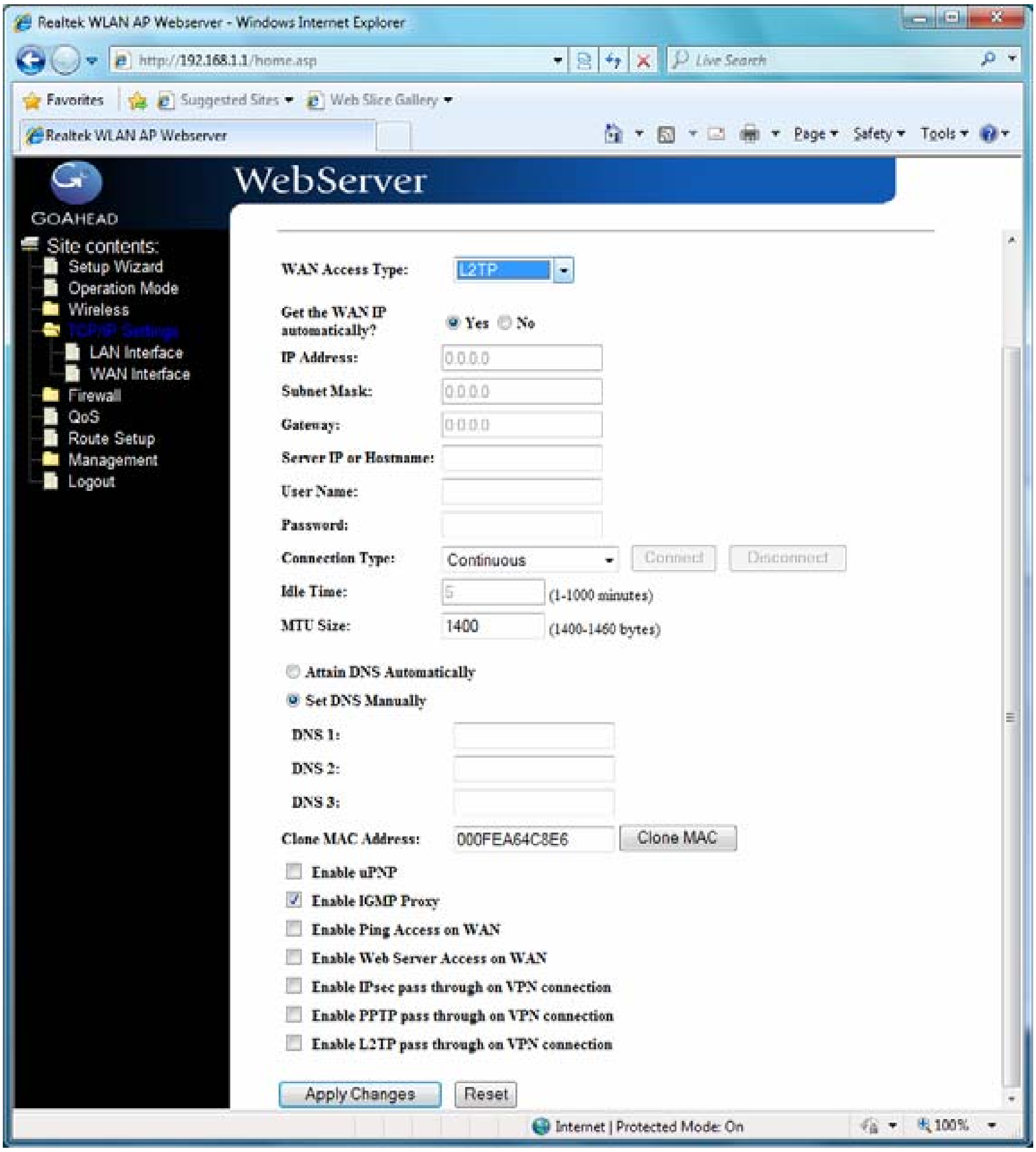
Gateway: If you select the Static L2TP support on WAN interface, fill in the gateway for WAN interface out going data packets.

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.



WAN Access Type: L2TP

Get the WAN IP automatically? ● Yes ○ No

IP Address: 0.0.0.0

Subnet Mask: 0.0.0.0

Gateway: 0.0.0.0

Server IP or Hostname:

User Name:

Password:

Connection Type: Continuous

Idle Time: 5 (1-1000 minutes)

MTU Size: 1400 (1400-1460 bytes)

○ Attain DNS Automatically

● Set DNS Manually

DNS 1:

DNS 2:

DNS 3:

Clone MAC Address: 000FEA64C8E6

□ Enable uPNP

☑ Enable IGMP Proxy

□ 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

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.

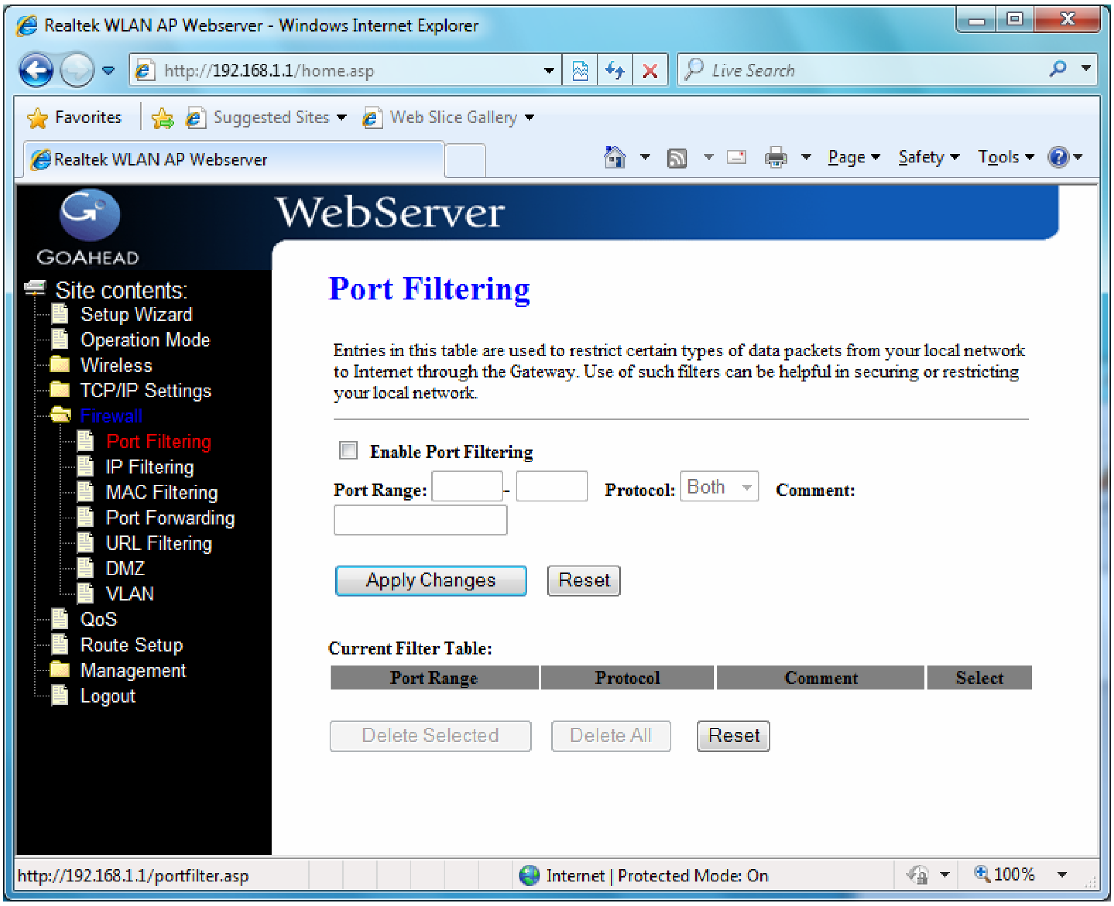
Apply Changes: Click the ***Apply Changes*** button to complete the new configuration setting.

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

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.



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**

Port Range: ____ - ____ **Protocol:** Both **Comment:** ____

Apply Changes | Reset

Current Filter Table:

Port Range	Protocol	Comment	Select

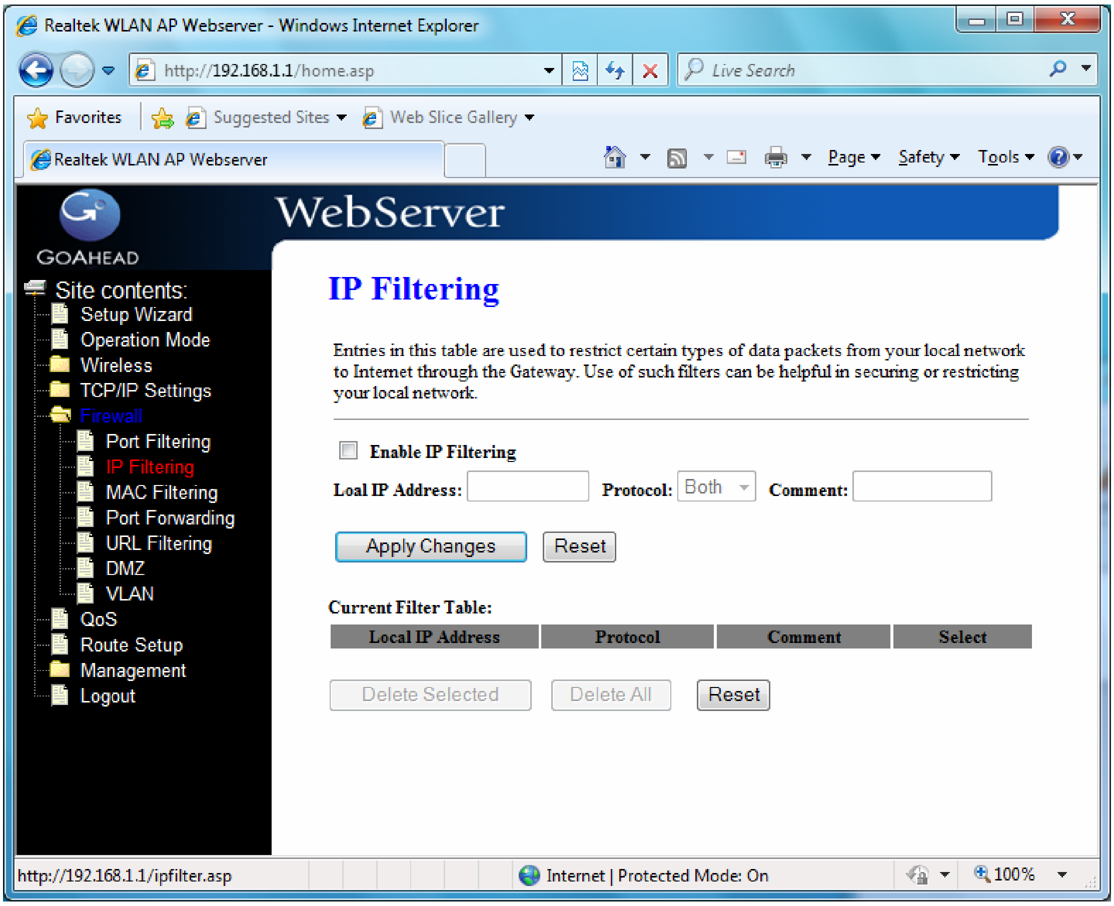
Delete Selected | Delete All | Reset

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.



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**

Loal IP Address: ______ **Protocol:** Both **Comment:** ______

Apply Changes | Reset

Current Filter Table:

Local IP Address	Protocol	Comment	Select

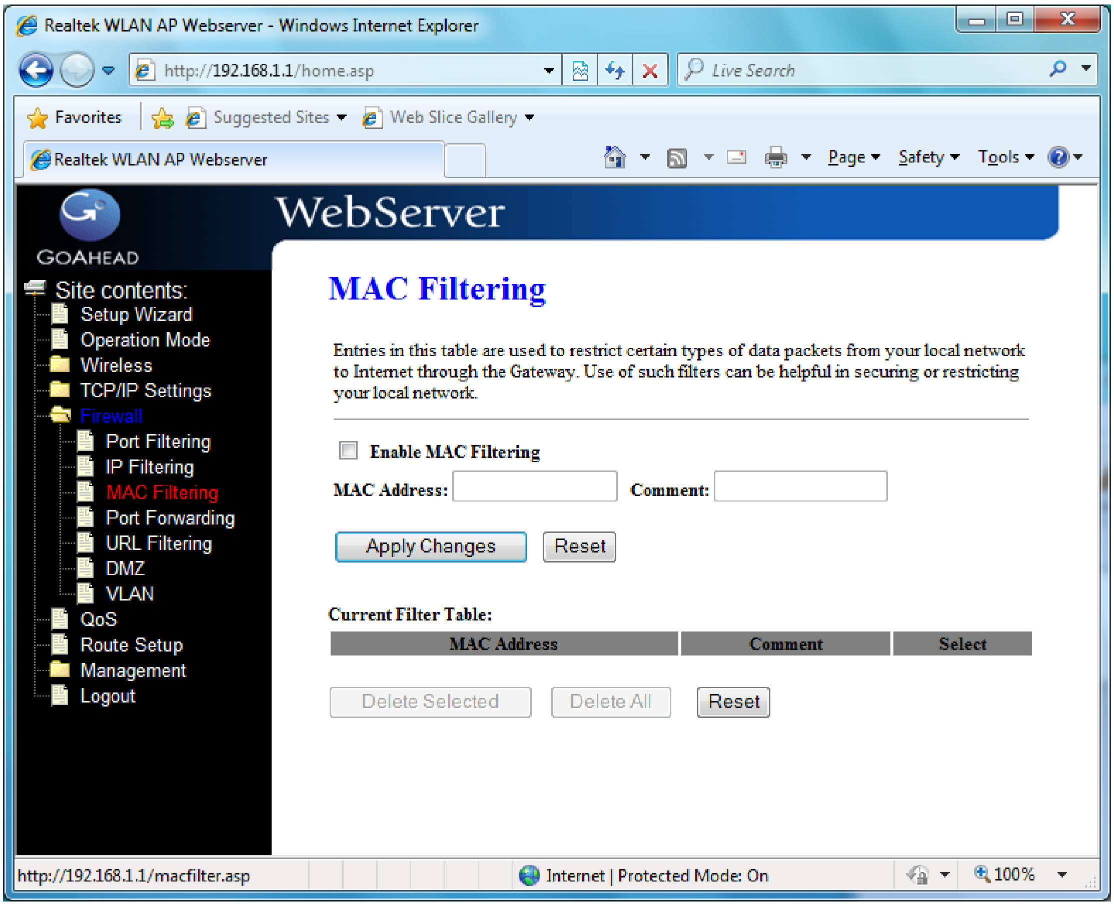
Delete Selected | Delete All | Reset

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.



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

MAC Address: ____ Comment: ____

Apply Changes | Reset

Current Filter Table:

MAC Address	Comment	Select

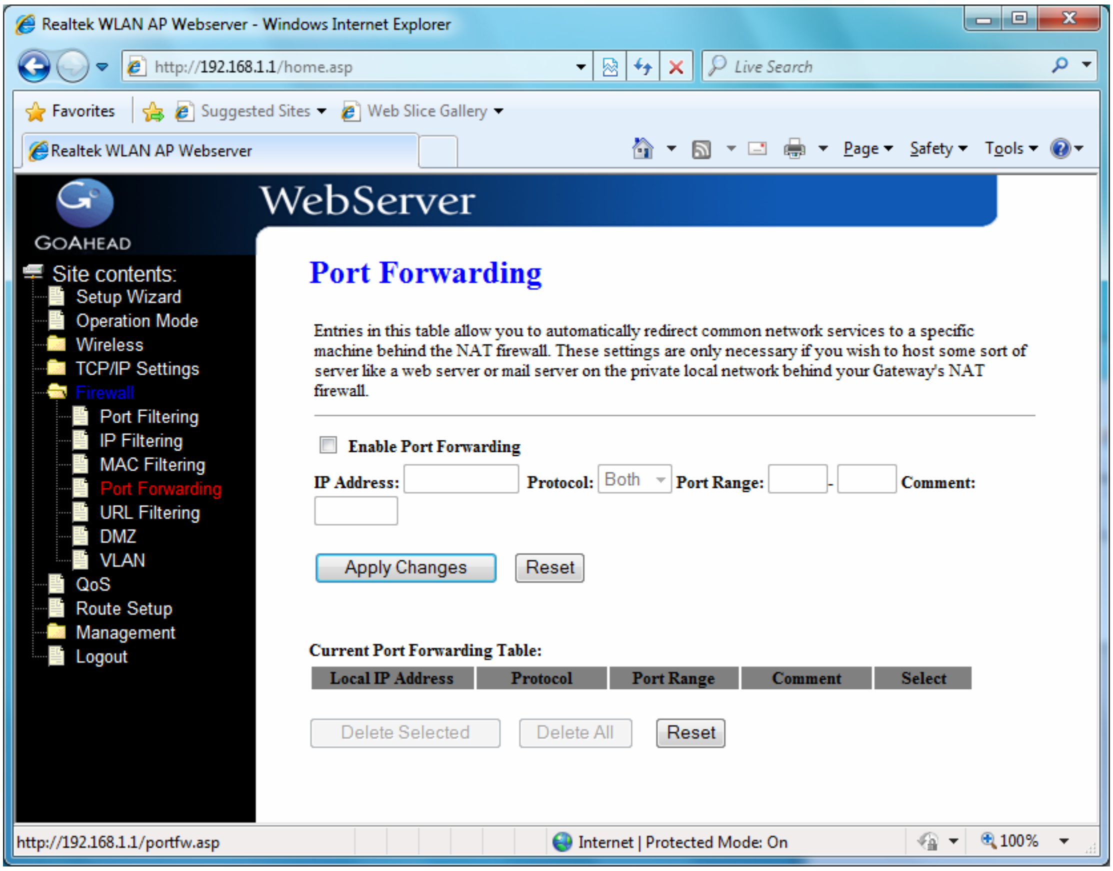
Delete Selected | Delete All | Reset

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.



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

IP Address: ______ Protocol: Both Port Range: ______ - ______ Comment: ______

Current Port Forwarding Table:

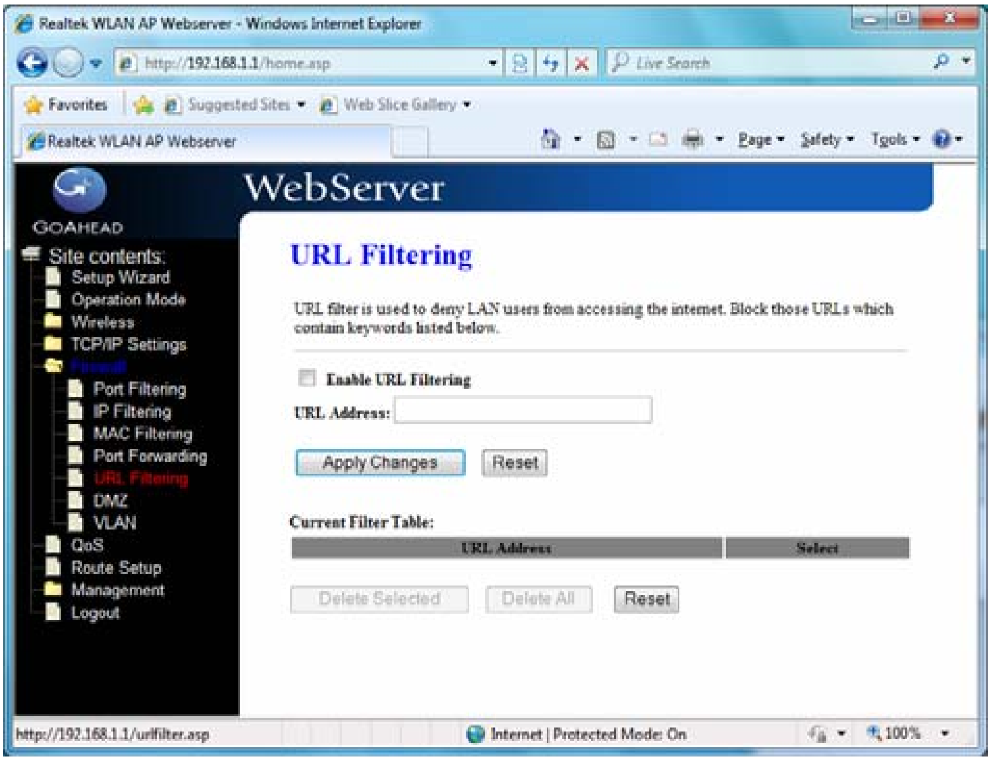
Local IP Address	Protocol	Port Range	Comment	Select

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.



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

URL Address:

Apply Changes | Reset

Current Filter Table:

URL Address	Select

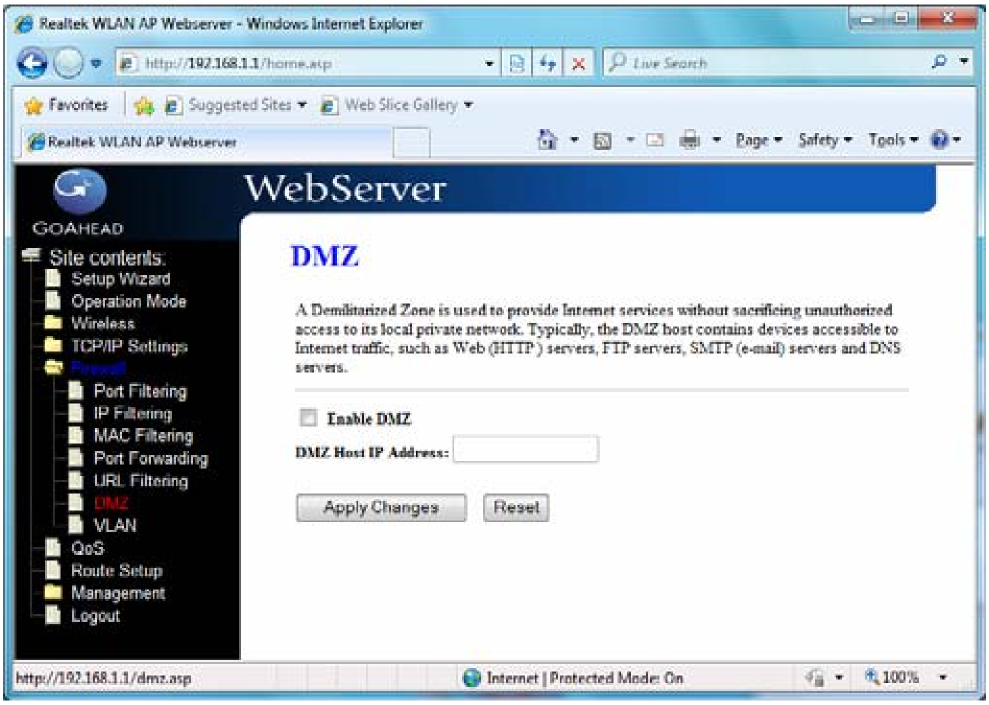
Delete Selected | Delete All | Reset

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.



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

DMZ Host IP Address:

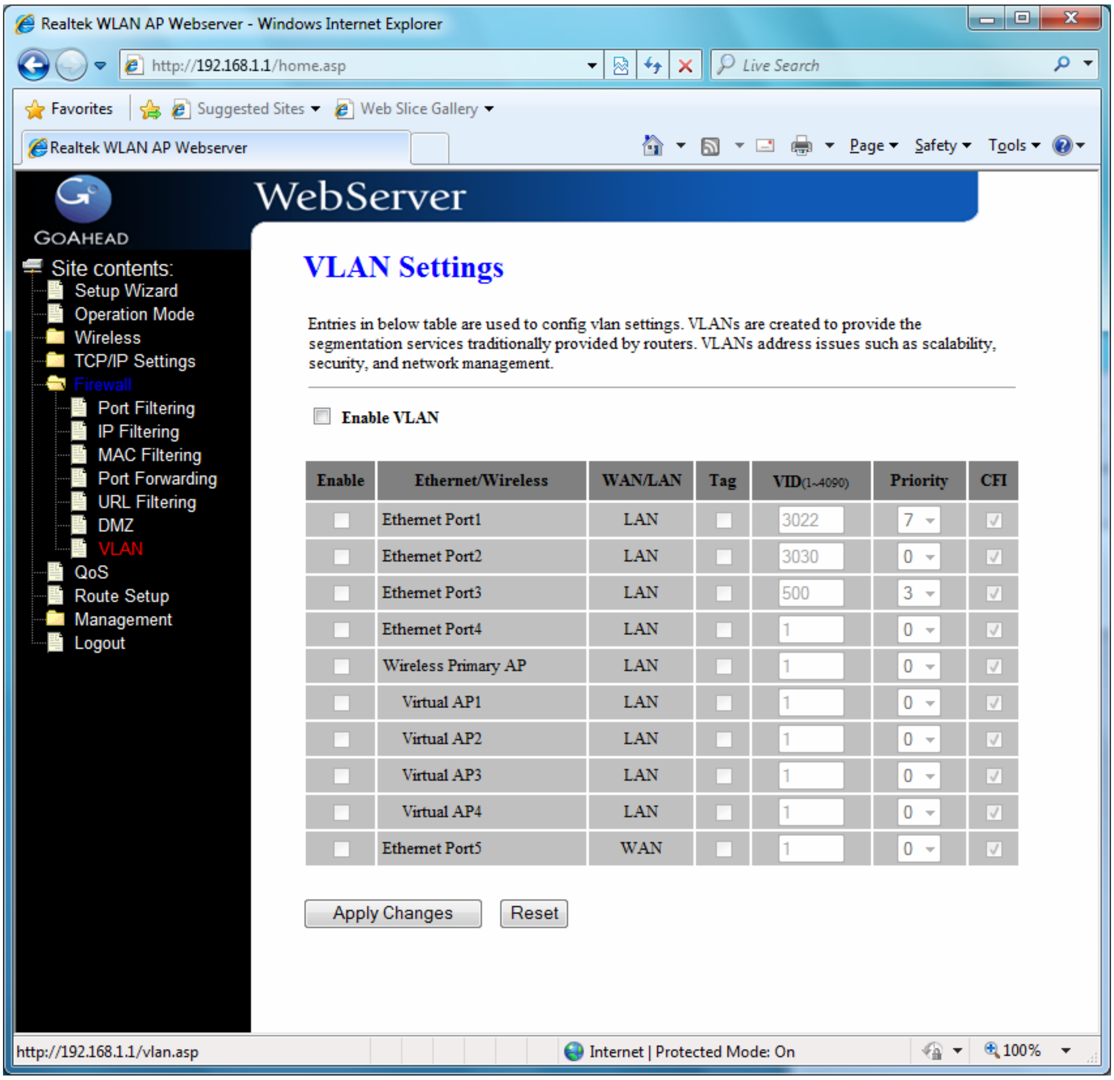
Apply Changes | Reset

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.



VLAN Settings

Entries in below table are used to config vlan settings. VLANs are created to provide the segmentation services traditionally provided by routers. VLANs address issues such as scalability, security, and network management.

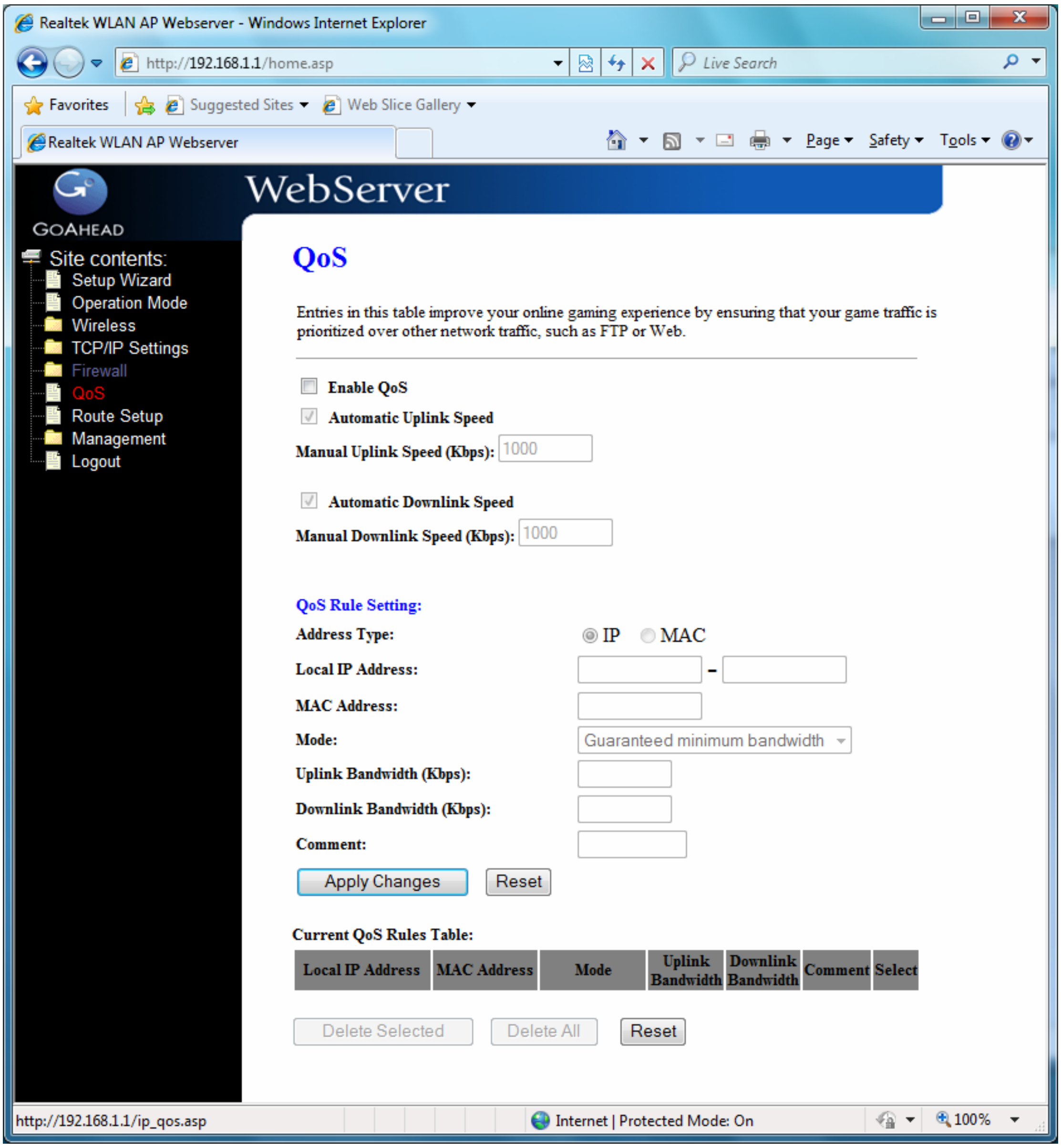
□ **Enable VLAN**

Enable	Ethernet/Wireless	WAN/LAN	Tag	VID(1~4090)	Priority	CFI
□	Ethernet Port1	LAN	□	3022	7	☑
□	Ethernet Port2	LAN	□	3030	0	☑
□	Ethernet Port3	LAN	□	500	3	☑
□	Ethernet Port4	LAN	□	1	0	☑
□	Wireless Primary AP	LAN	□	1	0	☑
□	Virtual AP1	LAN	□	1	0	☑
□	Virtual AP2	LAN	□	1	0	☑
□	Virtual AP3	LAN	□	1	0	☑
□	Virtual AP4	LAN	□	1	0	☑
□	Ethernet Port5	WAN	□	1	0	☑

Apply Changes | Reset

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.



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.

☐ Enable QoS

☑ Automatic Uplink Speed

Manual Uplink Speed (Kbps): 1000

☑ Automatic Downlink Speed

Manual Downlink Speed (Kbps): 1000

QoS Rule Setting:

Address Type: ● IP ○ MAC

Local IP Address: ____ - ____

MAC Address:

Mode: Guaranteed minimum bandwidth

Uplink Bandwidth (Kbps):

Downlink Bandwidth (Kbps):

Comment:

Current QoS Rules Table:

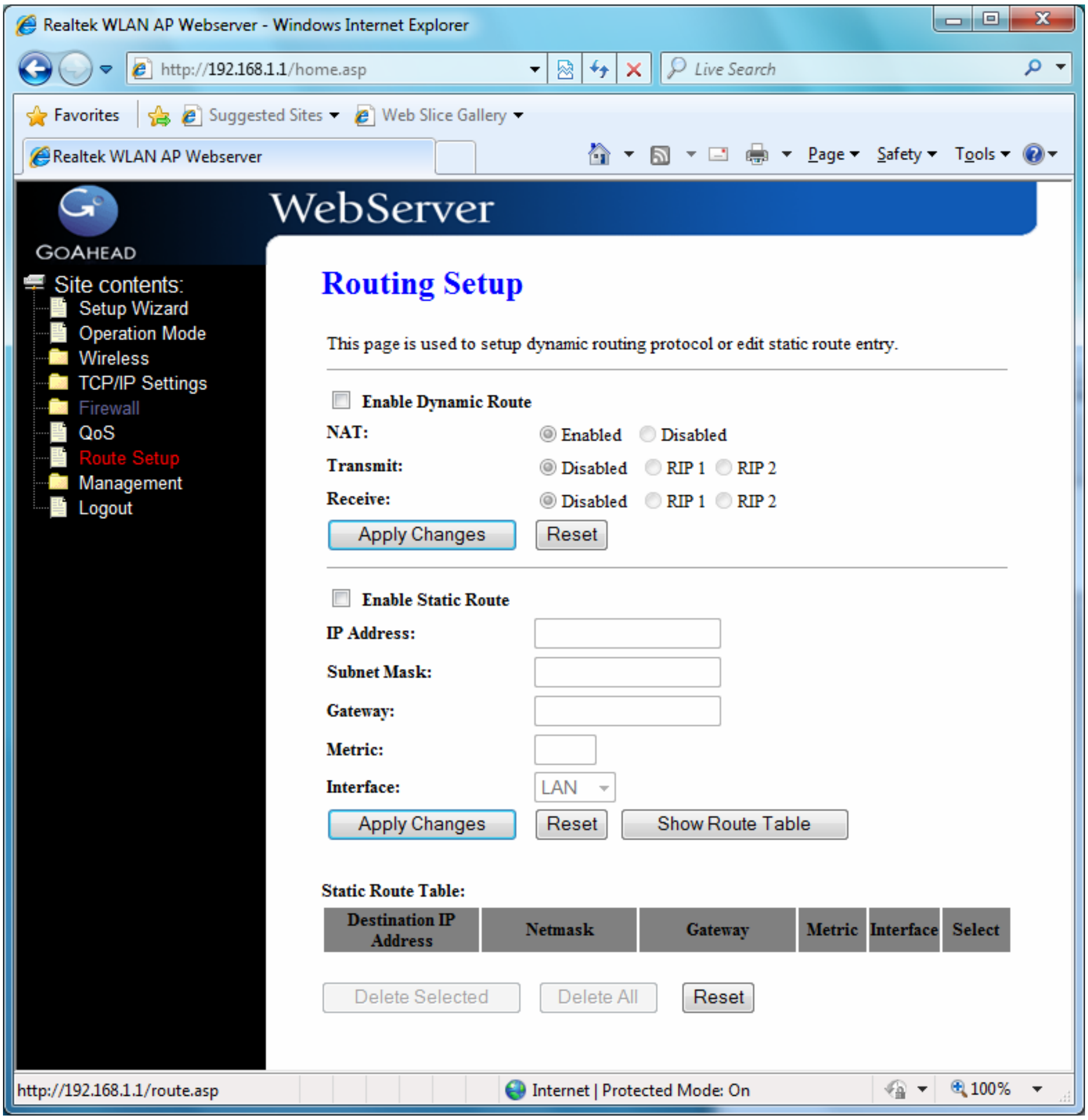
Local IP Address	MAC Address	Mode	Uplink Bandwidth	Downlink Bandwidth	Comment	Select

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.



Routing Setup

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

☐ Enable Dynamic Route

NAT: ● Enabled ○ Disabled

Transmit: ● Disabled ○ RIP 1 ○ RIP 2

Receive: ● Disabled ○ RIP 1 ○ RIP 2

Apply Changes | Reset

☐ Enable Static Route

IP Address:

Subnet Mask:

Gateway:

Metric:

Interface: LAN

Apply Changes | Reset | Show Route Table

Static Route Table:

Destination IP Address	Netmask	Gateway	Metric	Interface	Select

Delete Selected | Delete All | Reset

[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]

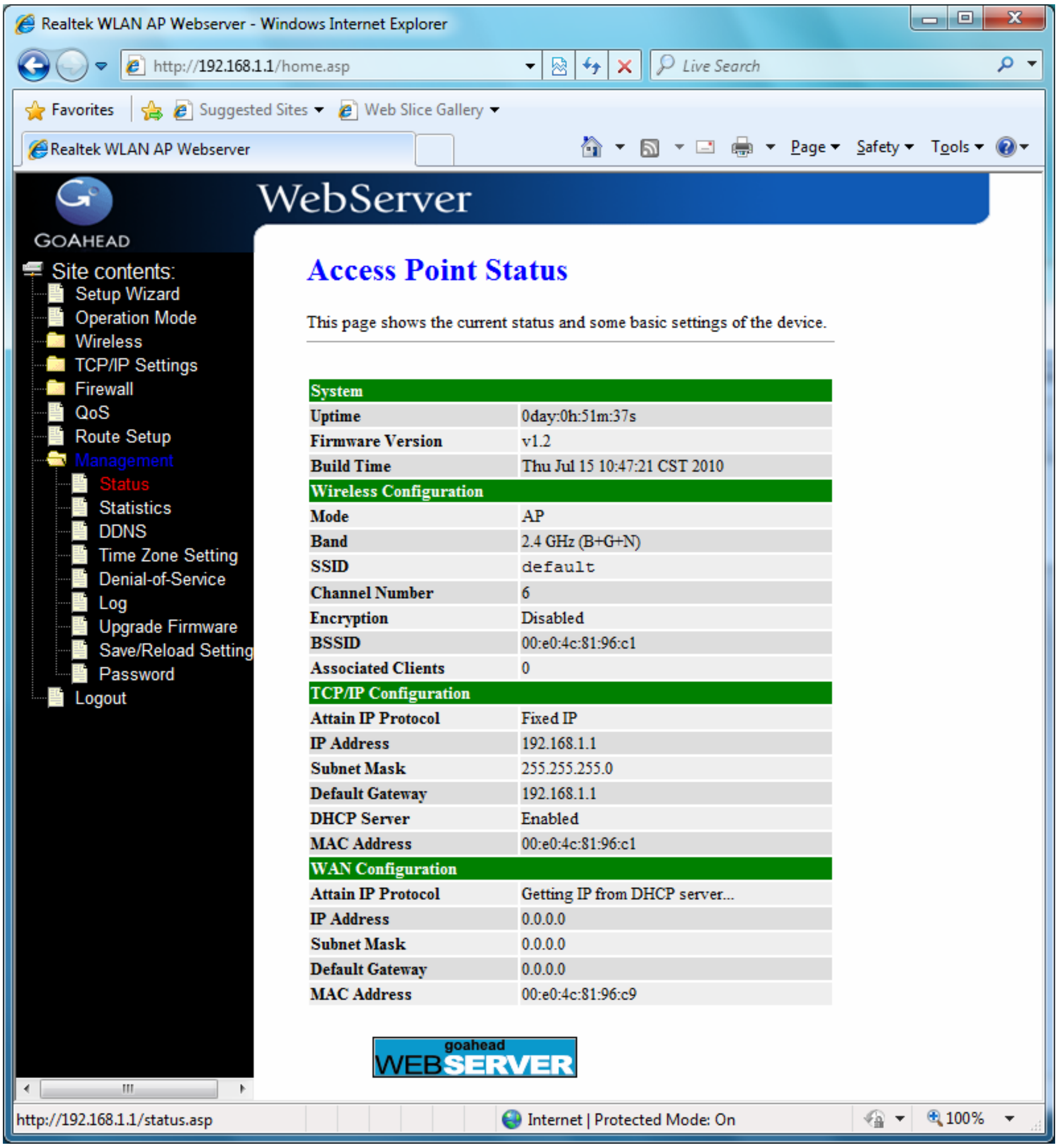
Attain IP Protocol: It shows how the WLAN AP Router gets the IP address. The IP address can be set manually to a fixed one or set dynamically by DHCP server or attain IP by PPPoE / PPTP connection.

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.



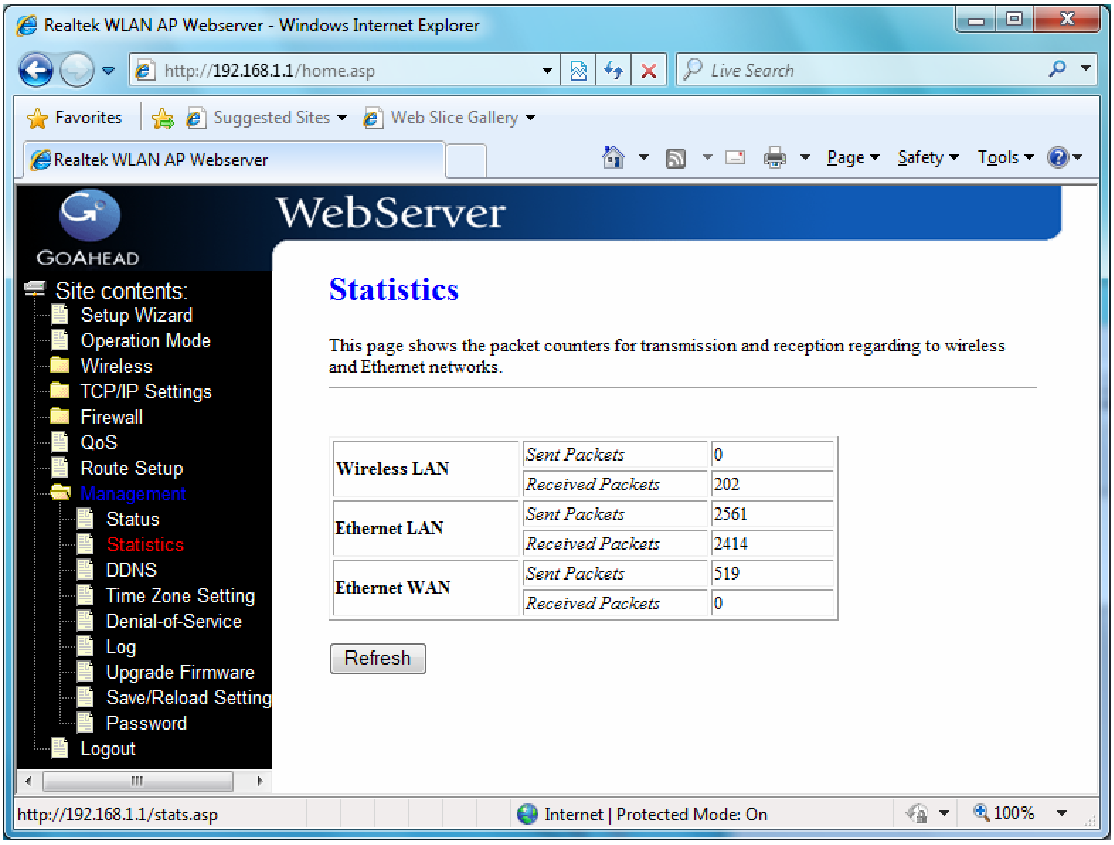
Access Point Status

This page shows the current status and some basic settings of the device.

System	
Uptime	0day:0h:51m:37s
Firmware Version	v1.2
Build Time	Thu Jul 15 10:47:21 CST 2010
Wireless Configuration	
Mode	AP
Band	2.4 GHz (B+G+N)
SSID	default
Channel Number	6
Encryption	Disabled
BSSID	00:e0:4c:81:96:c1
Associated Clients	0
TCP/IP Configuration	
Attain IP Protocol	Fixed IP
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.1
DHCP Server	Enabled
MAC Address	00:e0:4c:81:96:c1
WAN Configuration	
Attain IP Protocol	Getting IP from DHCP server...
IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Default Gateway	0.0.0.0
MAC Address	00:e0:4c:81:96:c9

3.9.2 Statistics

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



Statistics

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

Wireless LAN	*Sent Packets*	0
	Received Packets	202
Ethernet LAN	*Sent Packets*	2561
	Received Packets	2414
Ethernet WAN	*Sent Packets*	519
	Received Packets	0

[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]

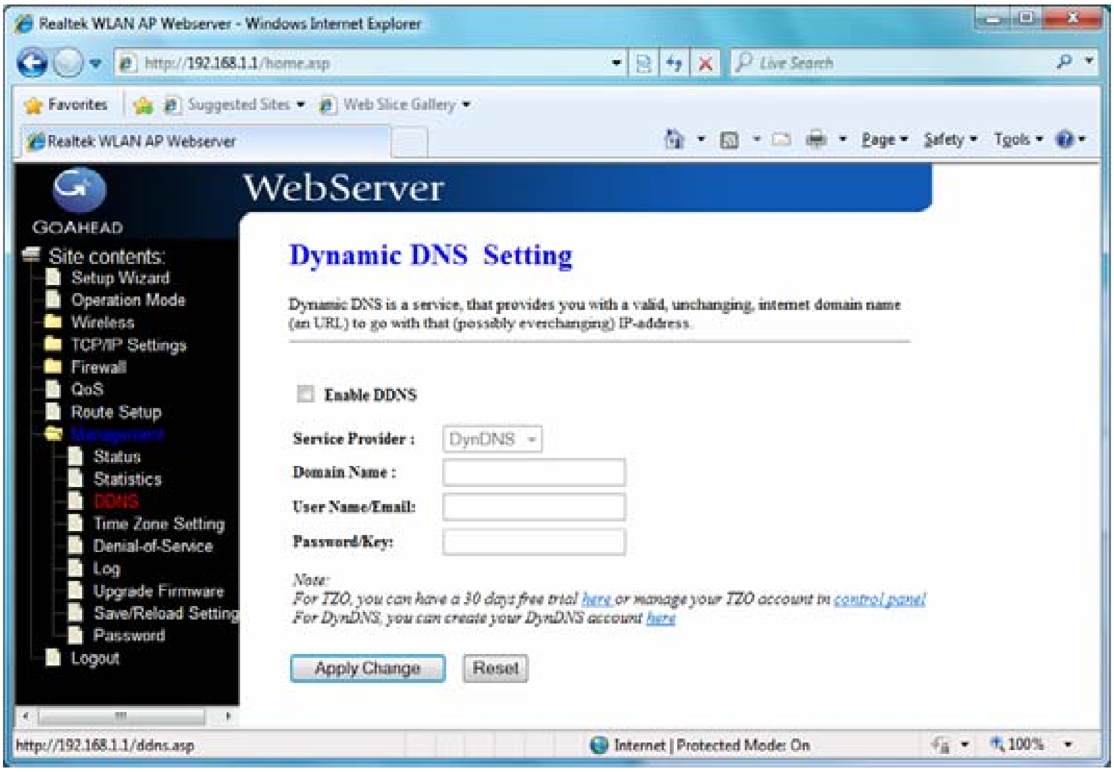
Sent Packets: It shows the statistic count of sent packets on the Ethernet WAN interface.

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.



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 : DynDNS

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

Apply Change | Reset

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.

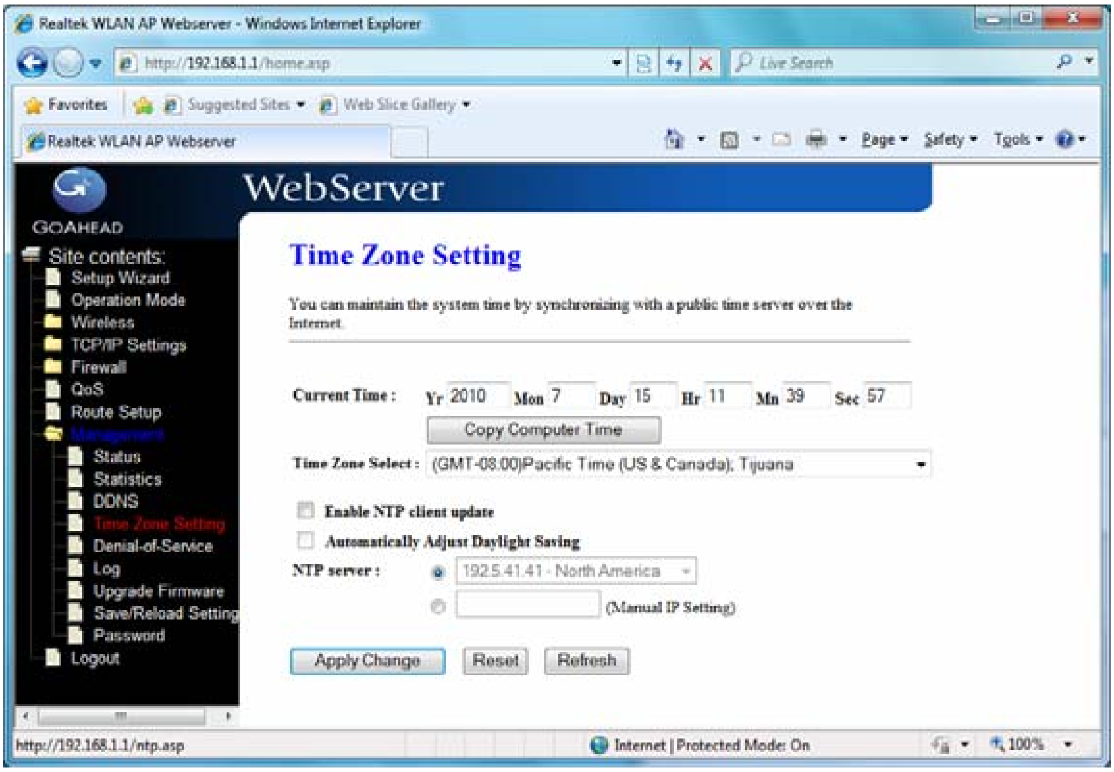
Enable NTP client update: Click the checkbox to enable NTP client update.

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.



Time Zone Setting

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

Current Time : Yr 2010 Mon 7 Day 15 Hr 11 Mn 39 Sec 57

Time Zone Select : (GMT-08:00)Pacific Time (US & Canada); Tijuana

□ Enable NTP client update

□ Automatically Adjust Daylight Saving

NTP server : ● 192.5.41.41 - North America

○ (Manual IP Setting)

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.

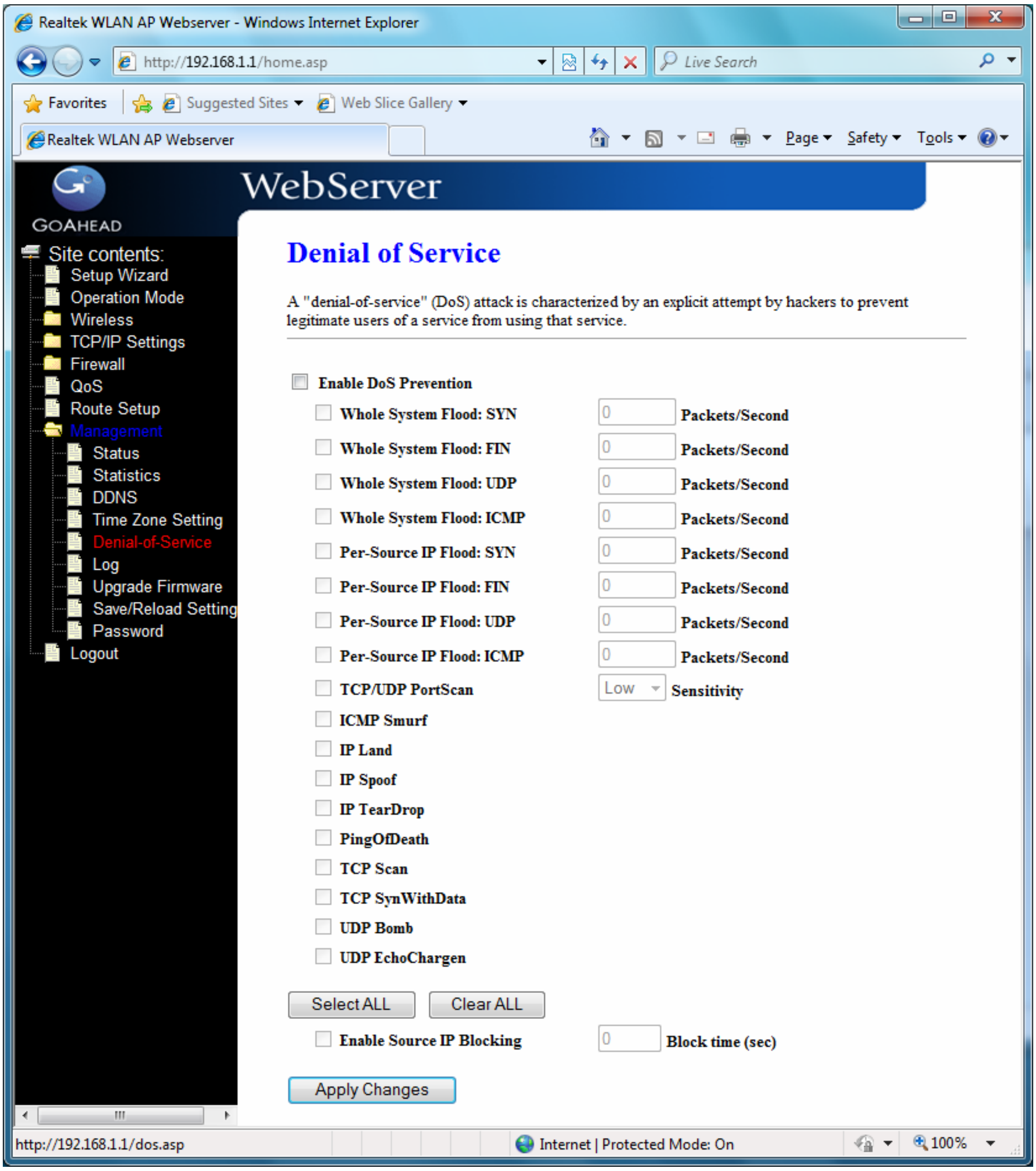
Enable DoS Prevention: Click the checkbox to enable DoS prevention.

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.



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	0	Packets/Second
□ Whole System Flood: FIN	0	Packets/Second
□ Whole System Flood: UDP	0	Packets/Second
□ Whole System Flood: ICMP	0	Packets/Second
□ Per-Source IP Flood: SYN	0	Packets/Second
□ Per-Source IP Flood: FIN	0	Packets/Second
□ Per-Source IP Flood: UDP	0	Packets/Second
□ Per-Source IP Flood: ICMP	0	Packets/Second
□ TCP/UDP PortScan	Low	Sensitivity
□ ICMP Smurf		
□ IP Land		
□ IP Spoof		
□ IP TearDrop		
□ PingOfDeath		
□ TCP Scan		
□ TCP SynWithData		
□ UDP Bomb		
□ UDP EchoChargen		

Select ALL | Clear ALL

□ Enable Source IP Blocking 0 Block time (sec)

Apply Changes

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

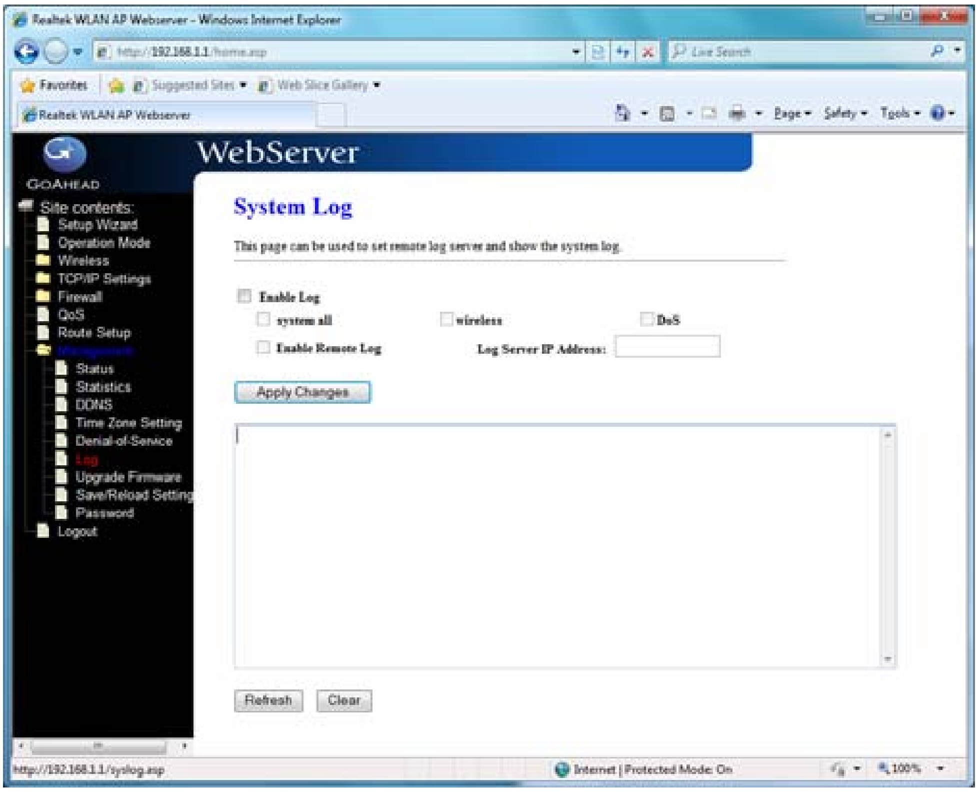
Enable Remote Log: Click the checkbox to enable remote log service.

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.



System Log

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

□ Enable Log

□ system all □ wireless □ DoS

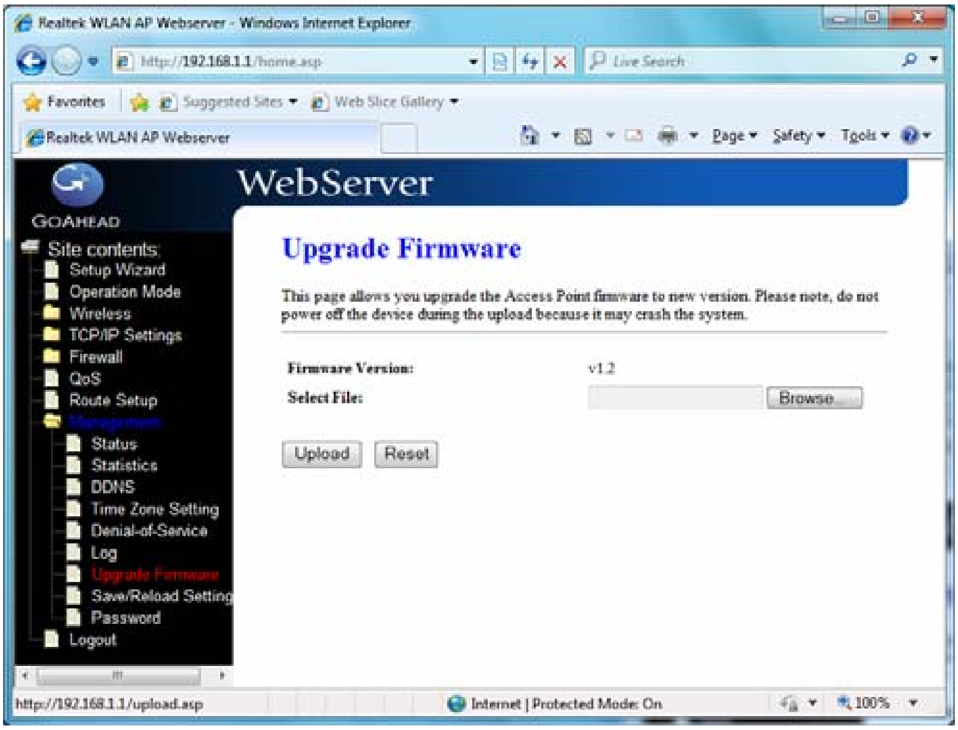
□ Enable Remote Log Log Server IP Address:

Apply Changes

Refresh Clear

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.



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.

Firmware Version: v1.2

Select File: Browse...

Upload Reset

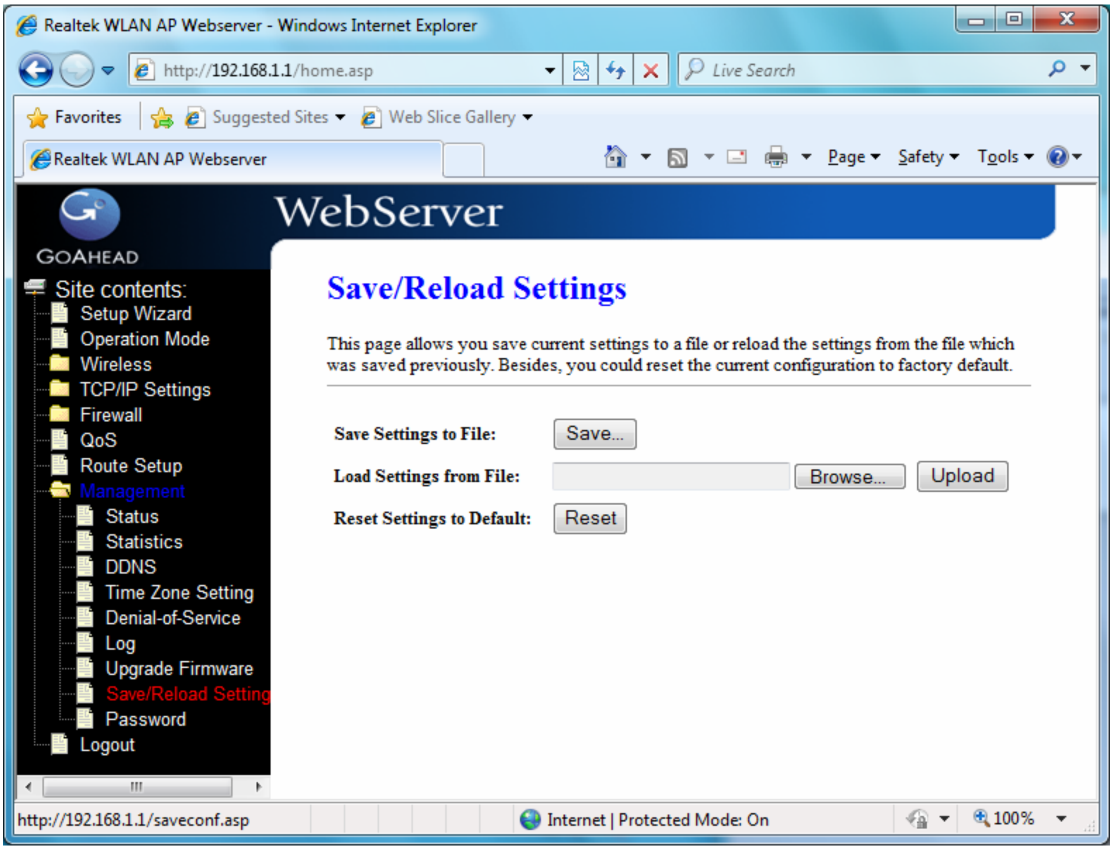
Select File: Click the ***Browse*** button to select the new version of web firmware image file.

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/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...

Load Settings from File: Browse... Upload

Reset Settings to Default: Reset

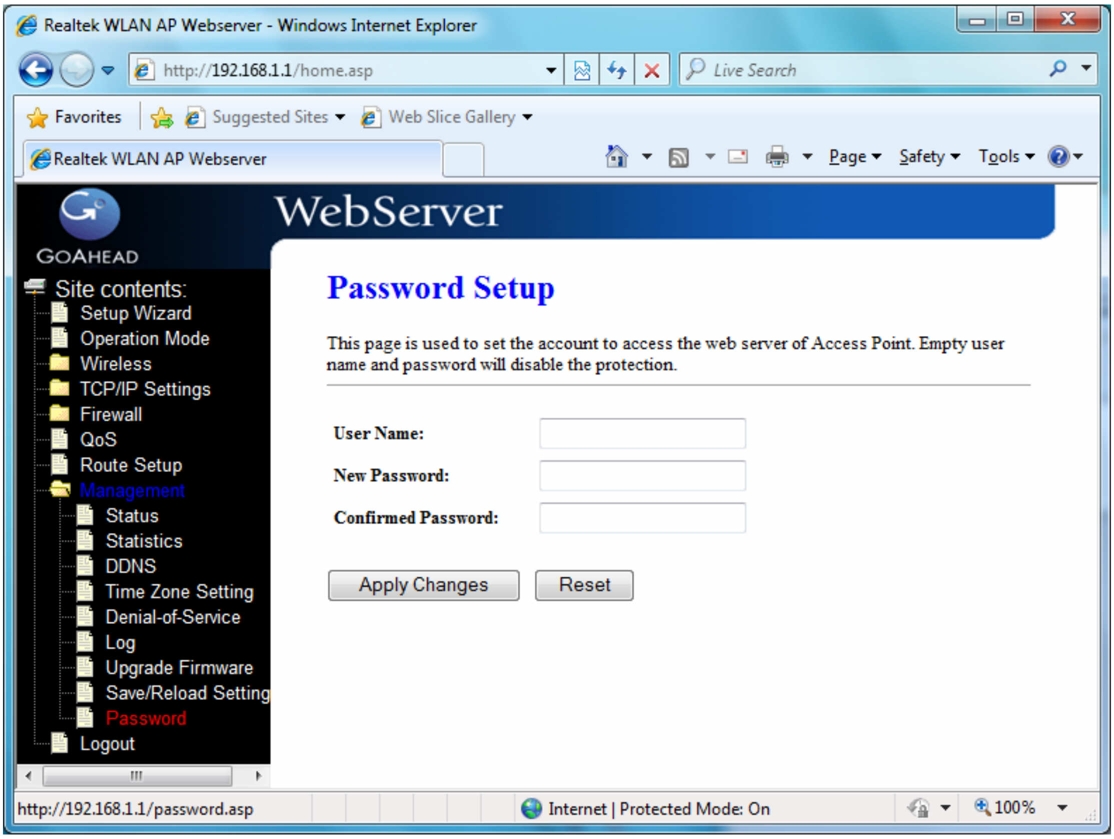
Save Settings to File: Click the Save button to download the configuration parameters to your personal computer.

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.



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:

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.