high traffic flows along in the wireless network. If the 802.11g MIMO Wireless Router often transmit large files in wireless network, you can enter new Fragment Threshold value to split the packet. The value can be set from 256 to 2346. The default value is **2346**.

RTS Threshold: RTS stands for "**Request to Send**". This parameter controls what size data packet the low level RF protocol issues to an RTS packet. RTS Threshold is a mechanism implemented to prevent the "Hidden Node" problem. If the "Hidden Node" problem is an issue, please specify the packet size. The RTS mechanism will be activated if the data size exceeds the value you set. The default is **2347**.

Tx Power: TX Power measurement.

Short Preamble: Select Disable or Enable this function, default setting is Disable. A preamble is a signal used in wireless environment to synchronize the transmitting timing including Synchronization and Start frame delimiter.

Short Slot: When short slot is Enable, the wireless device uses the short slot time only when all clients associated to the 802.11g, 2.4-GHz radio supports short slot time. Short slot time is an 802.11g-only feature and does not apply to 802.11a radios.

Tx Burst: Enable the transmitted time slot can increase transmission throughput.

Pkt_Aggregate: The parameter can be used to increase the delivered bandwidth in community networks including fixed and mobile stations.

Country Code: Select your local Country code for pull-down menu. For Safety (FCC or CE rule) reason, please don't change this default setting.

WMM Capable: Enable/Disable the Wi-Fi Multimedia (WMM) support.

APSD Capable: Enable/Disable the APSD support.

WMM Parameters: Click "WMM Configuration" to setup the WMM function.

3.5.3 Security

This function allows you setup the wireless security. Setup the wireless security and encryption to prevent from unauthorized access and monitoring.

SSID Choice: Select the SSID which you want to configure.

Security Mode: This function allows you setup the wireless security. Enable security mode could prevent any unauthorized access to your wireless network. [***Open***: If your wireless router is using "Open" authentication, then the wireless adapter will need to set to the same authentication type. ***Shared***: Shared key is when both the sender and the recipient share a secret key. ***WPA, WPA-PSK, WPA2, WPA2-PSK, WPA-PSK/WPA2-PSK, and WPA1/WPA2***: WPA-PSK offers two encryption methods, TKIP and AES. Select the type of algorithm, TKIP or AES and then enter a WPA Shared Key of 8~64 characters in the WPA Pre-shared key field.]

Encryption Type: For **Open** & **Shared** authentication mode, the selection of encryption type are **None** and **WEP**. For **WPA, WPA2, WPA-PSK, and WPA2-PSK** authentication mode, the encryption type supports both **TKIP** and **AES**.

WPA Pre-shared Key: This is the shared secret between AP and STA, For **WPA-PSK and WPA2-PSK** authentication mode, this field must be filled with character longer than 8 and less then 64 lengths.

WEP Key: Only valid when using WEP encryption algorithm. The key must match with the AP's Key. There are several formats to enter the keys.

-- Hexadecimal (128bits): 26 Hex characters (0-9, a-f)

-- ASCII (128bits): 13 ASCII characters.

WPA Algorithms: Select **TKIP**, **AES**, **TKIP/AES** for the WPA Algorithms.

Enable Pre-Authentication: The two most important features beyond WPA to become

standardized through 802.11i/WPA2 are: pre-authentication, which enables secure fast roaming without noticeable signal latency.

RADIUS Server: RADIUS is an authentication, authorization and accounting client-server protocol. The client is a Network Access Server that desires to authenticate its links. The server is a server that has access to a user database with authentication information.

IP Address: Enter the RADIUS Server's IP address provided by your ISP.

Port: Enter the RADIUS Server's port number provided by your ISP. The default is **1812**.

Shared Secret: Enter the password that the router shares with the RADIUS Server.

Capable: Specify the SSID's capability.

New: For security reason, enter the MAC address in this section can prevent others to connect this wireless router.

3.5.4 WPS

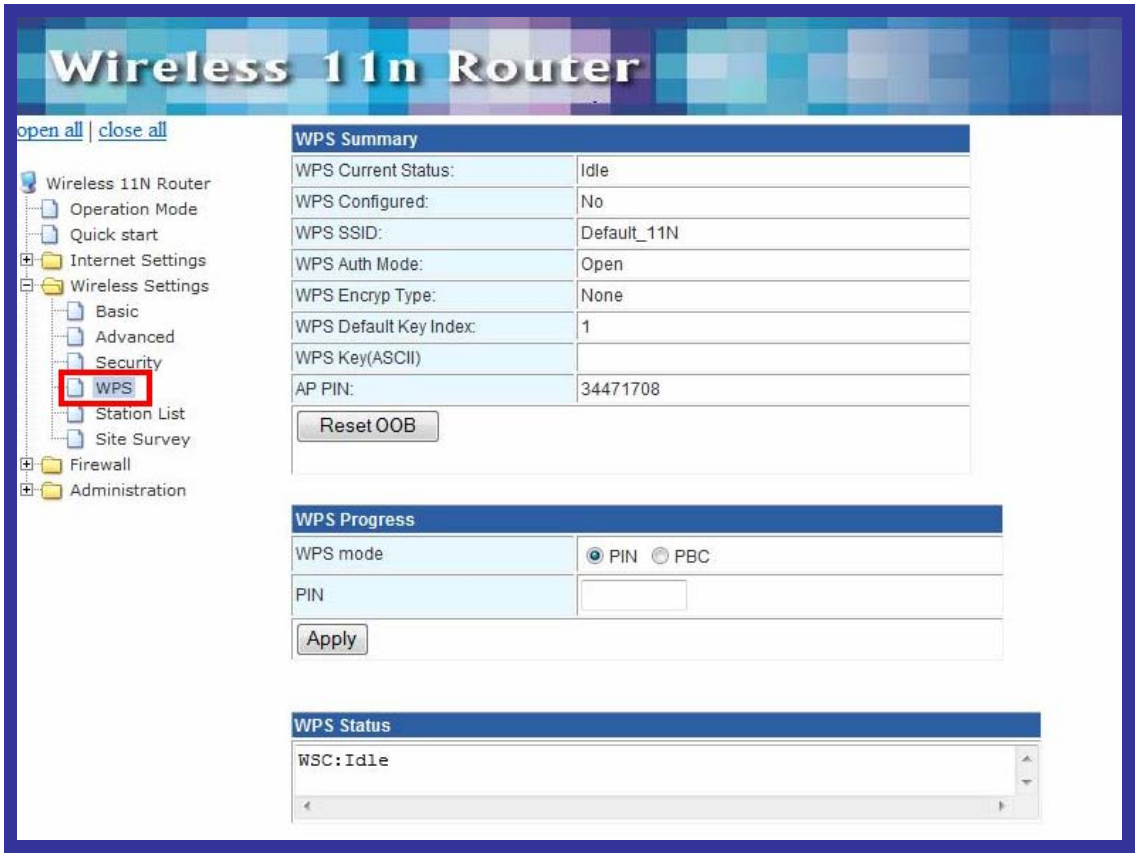
You could setup security easily by choosing PIN or PBC method to do Wi-Fi protected setup.

Wi-Fi Protected Setup was designed to ease setup of security enabled WiFi networks in the home and small office environment. It supports methods that are familiar to most consumers to configure a network and enable security, like pushing a button (PBC method) or entering a PIN code (PIN method). The new system, which will be incorporated in Windows Vista, will work with computers, gateways peripherals, and consumer electronics.

You would initiate a WPS mode on gateway and then enter a simple sequence of digits (like a PIN code) or press a button, use a similarly easy method to start a secure key exchange to retrieve the WPA/WPA2 key.

This function allows you to change the setting for WPS (Wi-Fi Protected Setup). WPS can help

your wireless client earlier automatically connect to the Access Point.



[WPS Summary]

From this section, you can view the current WPS status, Configured, SSID, Auth mode, Encrypt Type, Default Key Index, WPS Key, and AP PIN information.

Reset OOB: Click this button to rest the settings.

[WPS Progress]

WPS Mode: Specify the AP router acts as a **Registrar** or an **Enrollee**.

In PIN method (PIN-Personal Identification Number), When your 11n router acts as a Registrar, your must enter "**Add Enrollee PIN code**" on WPS config section, this Enrollee PIN code should be provided by the Enrollee. If your 11n router acts as a Enrollee, in WPS config section, the "**PIN code of this AP**" will automatically generate for you. The purpose of PIN code is to provide the security key to Registrar (AP/Server). Therefore, WPS (Wi-Fi Protected Setup) can be established completely.

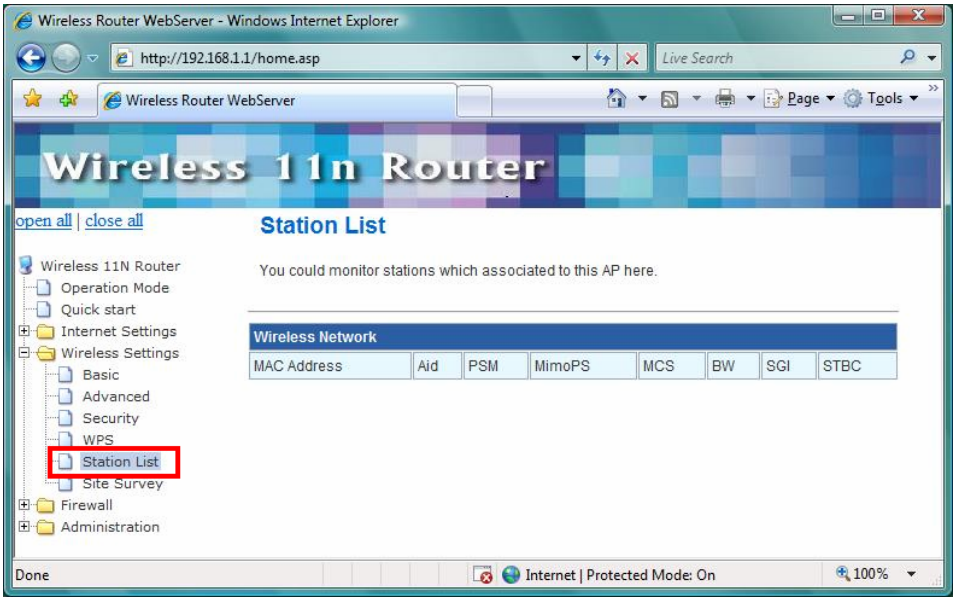
In PBC Method (PBC-Push Button Communication), while the AP router acts as Registrar or Enrollee, and click "**Start WPS Config**" button, the WPS (Wi-Fi Protected Setup) will establish the connection automatically.

PIN: Enter the PIN code from the registrar or enrollee.

WPS Status: Here shows the current status of the WPS function.

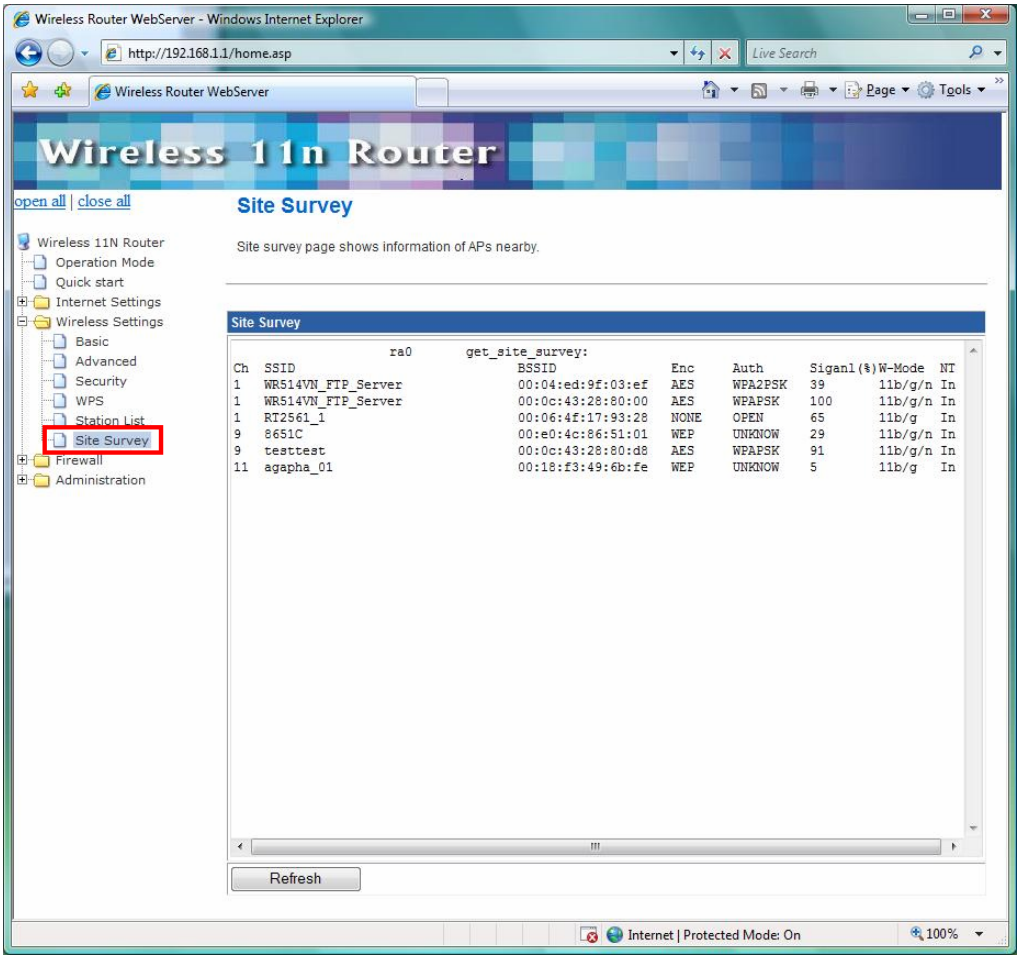
3.5.5 Station list

In this section, you can monitor stations which associated to this AP.



3.5.6 Site Survey

Site Survey page shows information of AP nearby.



3.6 Firewall

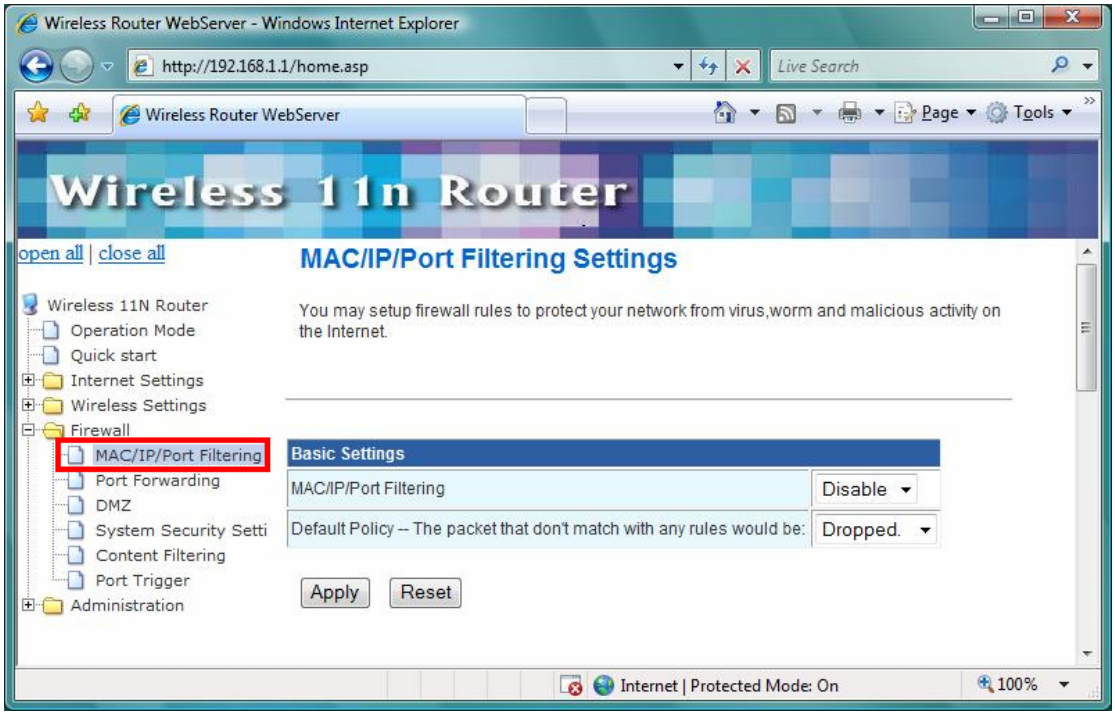
The Firewall contains the following sections:

◎MAC/IP/Port Filtering ◎Port Forwarding ◎DMZ

◎System Security Setting ◎Content Filtering ◎Port Trigger

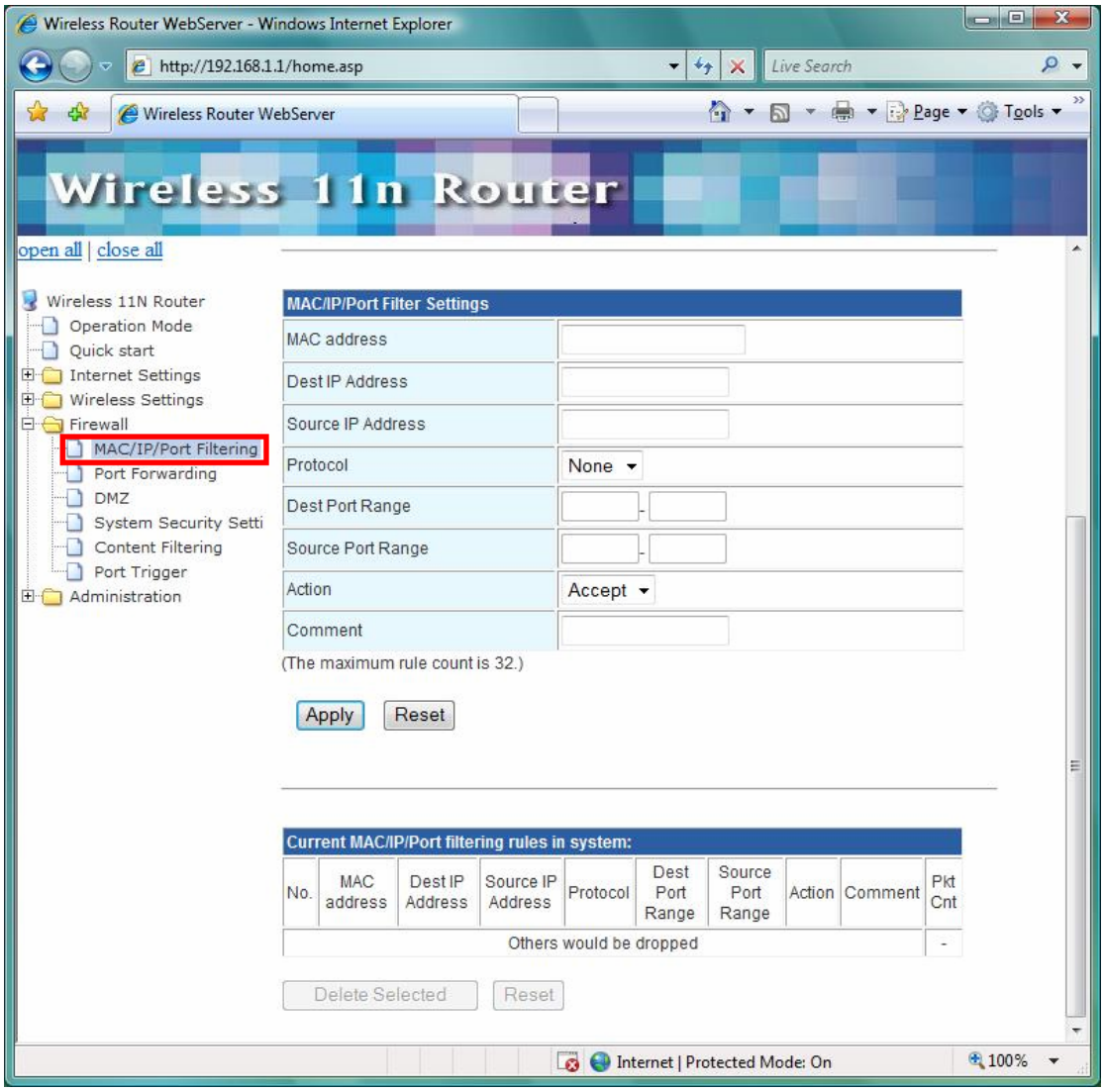
3.6.1 MAC/IP/Port Filtering Settings

You can setup firewall rules to protect your network from virus, worm and malicious activity on the internet. Filters are used to deny or allow LAN computers from access the Internet. Within the local area network, the unit can be setup to deny Internet access to computers using the assigned IP or MAC addresses. The unit can also block users from accessing restricted web site.



MAC/IP/Port Filtering: Enable this function, all list from the filtering will be deny the internet access.

Default Policy: There have 2 options, Dropped and Accepted.



MAC Address: The MAC address of the computer in the LAN (Local Area Network) to be used in the MAC filter table. Enter the MAC address of LAN port, e.g. 00:00:27:88:81:18

Dest IP Address: The IP address that will be denied to access.

Source IP Address: The IP address that will be denied access to the Internet.

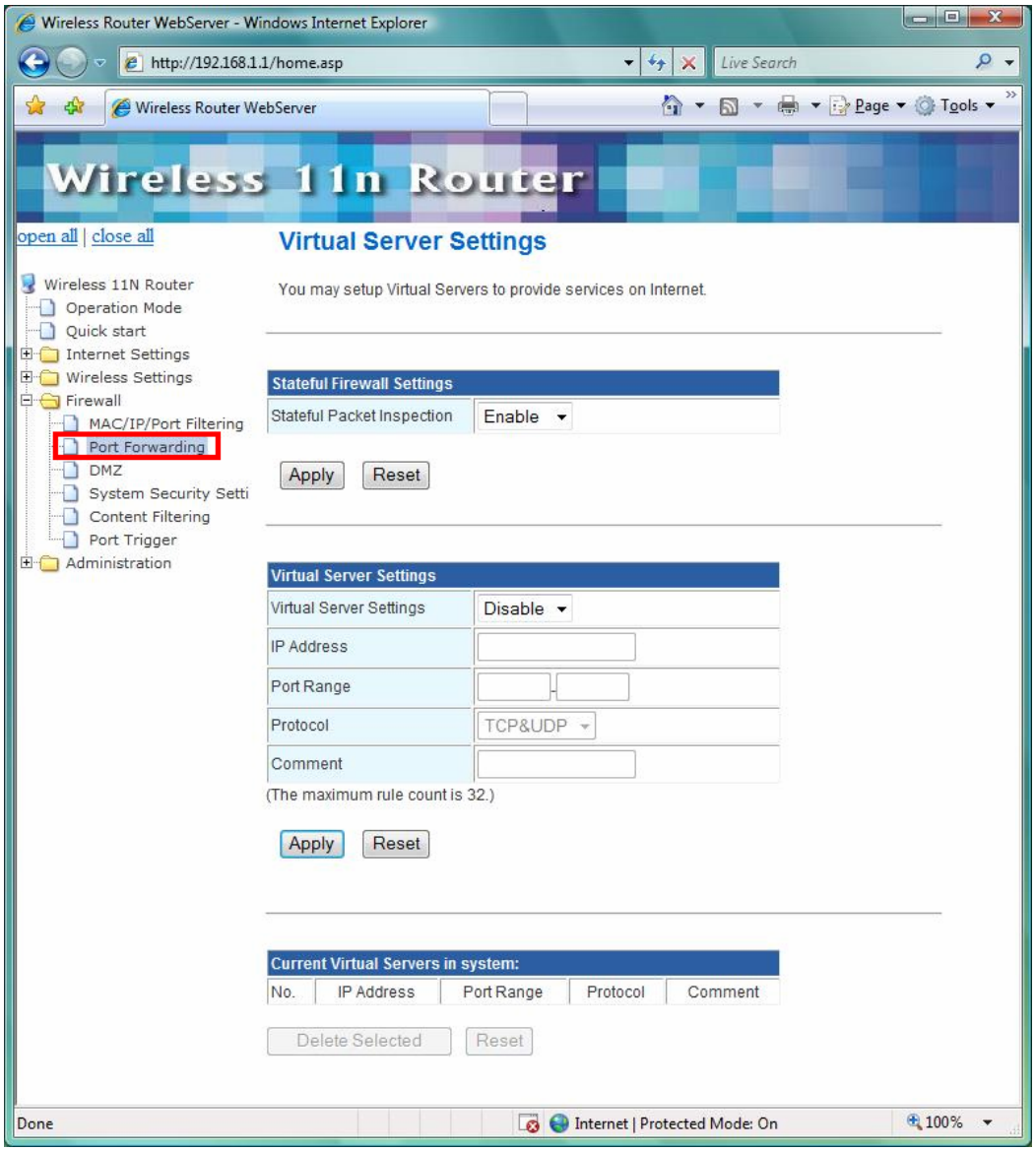
Protocol: This is the protocol type that will be used with the Port that will be blocked.

Destination Port Range: The single port or port range that will be denied to access. If no port is specified, all ports will be denied access.

Source Port Range: The single port or port range that will be denied access to the Internet. If no port is specified, all ports will be denied access.

3.6.2 Port Forwarding

You may setup virtual servers to provide service on internet.



Virtual Server Setting: Enable/Disable the port forward.

IP Address: This is the port number on the WAN side that will be used to access the application. You may define a single port or a range of ports. You can use a comma to add multiple ports or port ranges.

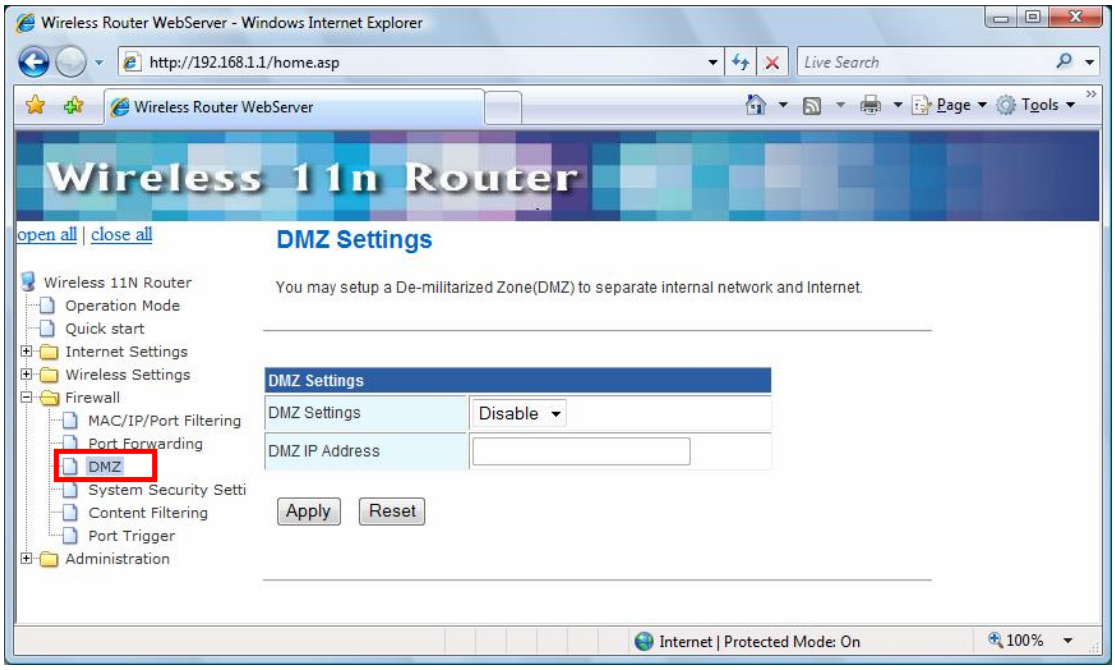
Port Range: This is the port used to forward the application. It can be either a single port or a range of ports. For the TCP and UDP services enter the beginning of the range of port numbers used by the service. If the service uses a single port number, enter it in both the start and finish fields.

Protocol: Select the protocol (TCP, UDP, or TCP & UDP) used to the remote system or service.

Comment: You may key in a description for the IP address.

3.6.3 DMZ

You may setup a De-Militarized Zone (DMZ) to separate internet network and internet.



DMZ Setting: If the DMZ Host Function is enabled, it means that you set up DMZ host at a particular computer to be exposed to the Internet so that some applications/software, especially Internet/Online game can have two-way connections. Select Enable or Disable from the pull-down menu.

DMZ IP Address: Enter the IP address of a particular host in your LAN that will receive all the packets originally going to the WAN port/Public IP address above. **Note:** You need to give your LAN PC clients a fixed/static IP address for DMZ to work properly.

3.6.4 System Security Settings

You may configure the system firewall to protect AP/Router itself from attacking.

Malformed Packet Detection: Filter the packet's header unreasonable or unusual, such as IP, TCP, UDP, and ICMP protocols' packet.

IP Land Attack: When packet's source IP and destination IP are same and the source port is also same as destination port, the packet is determined the IP Land attack and dropped by the router.

IP Spoof: The packet from WAN and the source IP network is same as LAN IP network, this packet is determined the IP Spoof attack and dropped by the router.