



# **Wireless – N Broadband Router**

## **User's Manual**

**Model # AWR-RT-11N**

## **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

2008 All Rights Reserved.

No part of this document can be copied or reproduced in any form without written consent from the company.

### **Trademarks:**

**All trade names and trademarks are the properties of their respective companies.**

## Revision History

Revision

V1

History

<sup>1st</sup> Release

## Table of Contents

<b>1. Introduction .....</b>	<b>6</b>
1.1 Features 6	
1.2 Package Contents .....	7
1.3 System Requirements .....	7
1.4 LEDs Indication & Connectors of Wireless Router.....	7
1.5 Installation Instruction.....	8
<b>2. PC Configuration.....</b>	<b>9</b>
2.1 TCP/IP Networking Setup .....	9
<b>3. Configure Wireless Router via Web Based Utility .....</b>	<b>18</b>
3.1 Access Web Based Configuration Utility .....	18
3.2 Operation Mode .....	19
3.3 Quick Start.....	28
3.4 Internet Settings.....	28
3.4.1 WAN 28	
3.4.2 LAN 29	
3.4.3 DHCP Clients.....	31
3.4.4 VPN Passthrough .....	32
3.4.5 DNS 32	
3.4.6 Advanced Routing .....	33
3.4.7 QoS 35	
3.5 Wireless Settings .....	36
3.5.1 Basic 36	
3.5.2 Advanced .....	39
3.5.3 Security .....	41
3.5.4 WPS 43	
3.5.5 Station list .....	45
3.5.6 Site Survey.....	45
3.6 Firewall 46	
3.6.1 MAC/IP/Port Filtering Settings.....	46
3.6.2 Port Forwarding.....	49
3.6.3 DMZ 50	
3.6.4 System Security Settings.....	51
3.6.5 Content Filtering.....	51
3.6.6 Port Trigger .....	54
3.7 Administration.....	55

<b>3.7.1 Administration .....</b>	<b>55</b>
<b>3.7.2 Upgrade Firmware .....</b>	<b>56</b>
<b>3.7.3 Setting Management.....</b>	<b>57</b>
<b>3.7.4 Status</b>	<b>58</b>
<b>3.7.5 Statistics.....</b>	<b>59</b>
<b>3.7.6 System Command .....</b>	<b>60</b>
<b>3.7.7 System Log .....</b>	<b>61</b>

## 1. Introduction

This Wireless Broadband Router is a draft 802.11n compliant device that provide faster and farther range than 802.11g while backward compatible with 802.11g and 802.11b devices. This Router uses advanced broadband router chipset and wireless LAN chipset solution 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. It creates a secure Wired and Wireless network for you to share photos, files, video, music, printer and network storage. This device also supports the latest wireless security features such as WEP, WPA, WPA2 and WPS to prevent from unauthorized access.



### 1.1 Features

- Compliant with IEEE 802.11n draft 2.0 standard
- Backward compatible with IEEE 802.11b/g
- Supports NAT, NAPT, DHCP Server/Client
- Supports VPN pass through - IPSec, PPTP, L2TP
- Supports Virtual Server / Port Trigger / Port Forward
- 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 Quality of Service (QoS) – WMM
- Supports MAC Filter, Client Filter, URL/IP Filter
- Supports Hacker Pattern Detection
- Supports Auto-crossover (MDI/MID-X) function
- Supports software upgrade through Web
- Friendly web-based GUI Configuration and Management

## 1.2 Package Contents

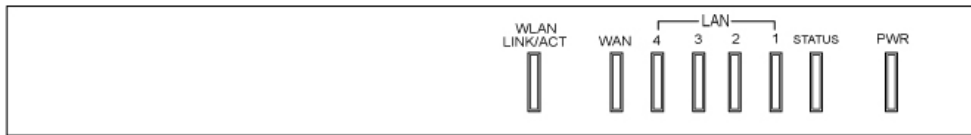
- One Wireless AP Router with 2 antennas
- One External Power Adapter
- One CD-ROM (user's manual)
- One RJ-45 Ethernet Cable

## 1.3 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.

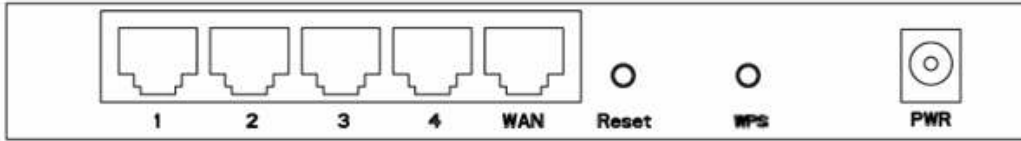
## 1.4 LEDs Indication & Connectors of Wireless Router

### Front Panel LEDs Indication



LED	Light Status	Description
PWR	On	Wireless Router is powered on.
	Off	Wireless Router is powered off.
Status	On	Wireless Router is hung.
	Blinking	Wireless Router is up and ready.
LAN (1, 2, 3, 4)	On	LAN port is successfully connected.
	Blinking	Data is being sent or received.
WAN	On	WAN port is successfully connected
	Blinking	Data is being sent or received.
WLAN LINK/ACT	Slow Blinking	WLAN 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 11n AP router to hang. Press the button and hold for 10 seconds.
WPS	Click WPS button about 2-3 seconds while you are connecting a PC with 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.
PWR	Power connector, connect to the power adapter packaged with the AP router.

### 1.5 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.

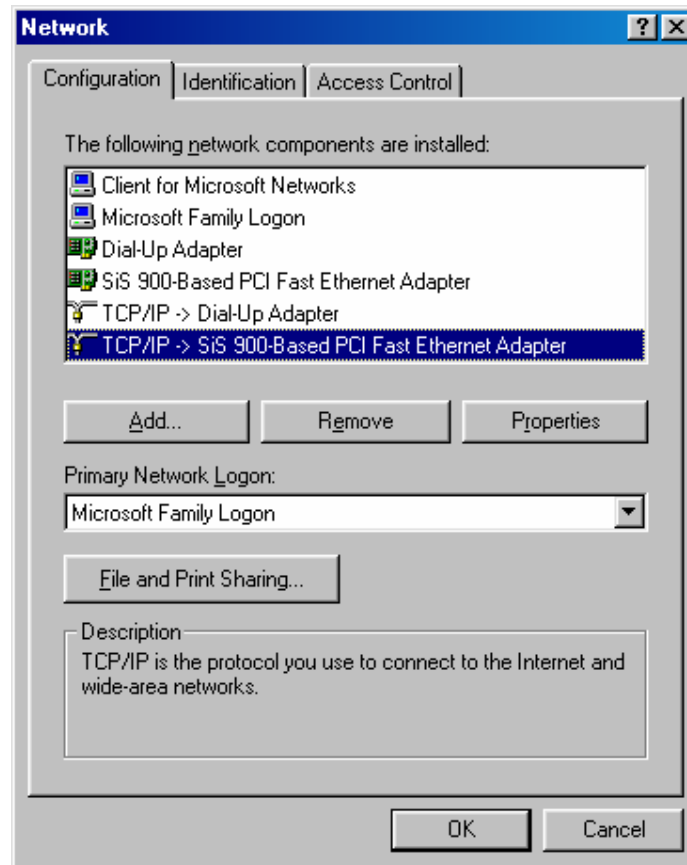
The 802.11n AP router assumes an IP address of 192.168.1.1 without network connectivity. This IP address is used for communicating with the 802.11n AP router via the web UI or Telnet, with the PC connected to the LAN port.

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.

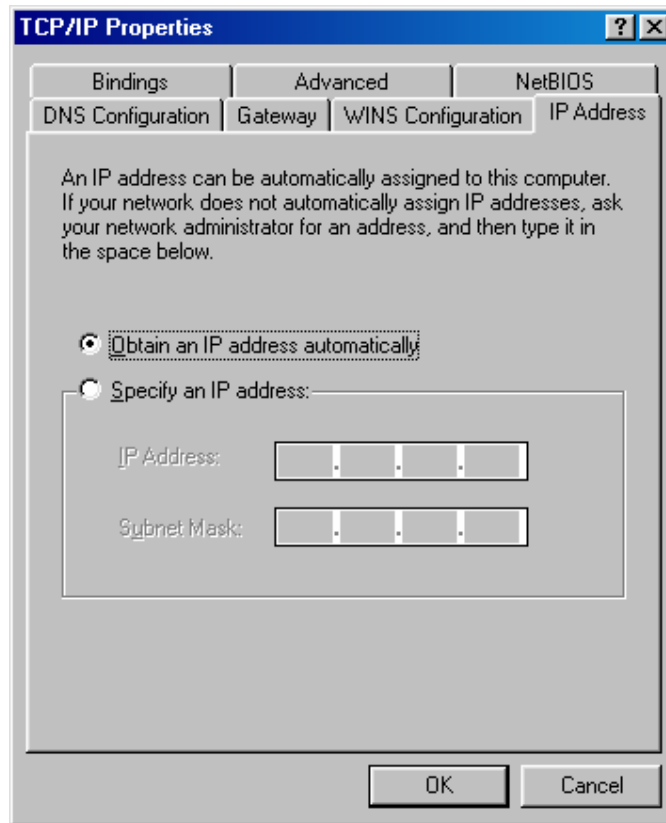
### 2.1 TCP/IP Networking Setup

#### *Checking TCP/IP Settings for Windows 9x/Me*

- a) Select “**Start → Control Panel → Network**”, the window below will appear,

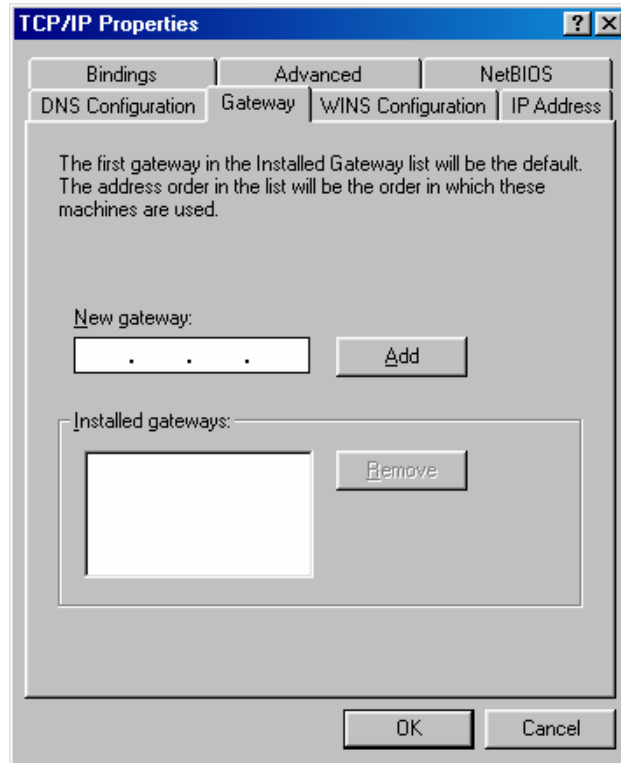


b) Click **“Properties”**, the window below will appear and then click **“IP Address”** tab,

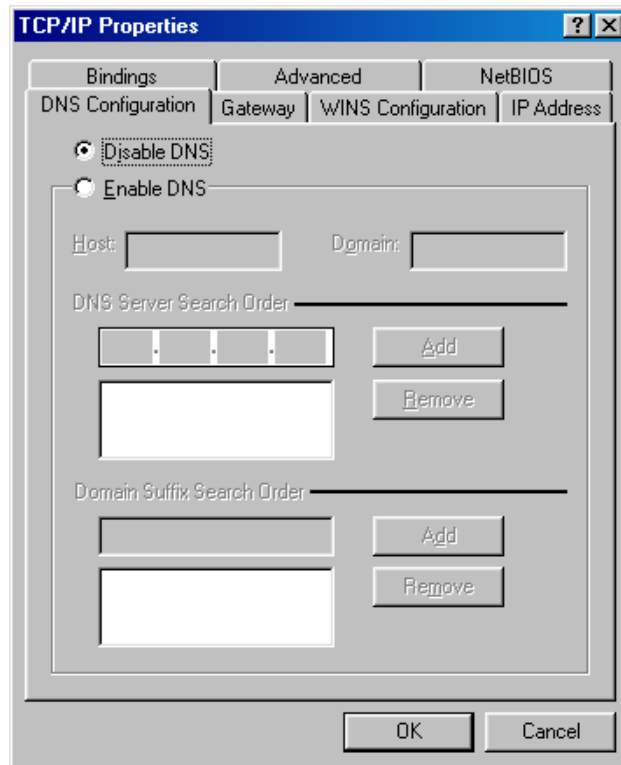


- If you decide to use DHCP, select **“Obtain an IP address automatically”**, then click **“OK”** to confirm your settings. Once you restart your system, Wireless Router will obtain an IP address for this system.
- If you decide to use fixed IP address for your system, select **“Specify an IP address”**, 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”**,

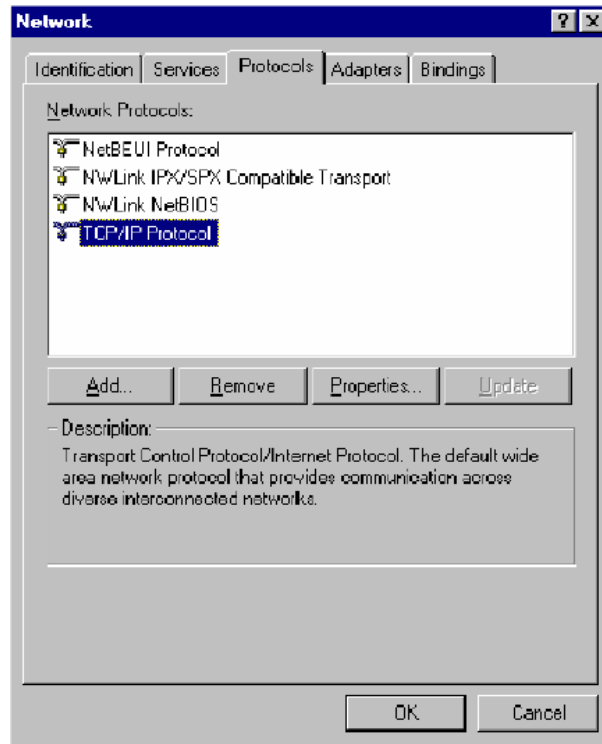


- d) Select “DNS Configuration” tab and make sure select “Enable DNS”, enter the DNS address provides from your ISP in the “DNS Server Search Order” field, then click “Add”,



*Checking TCIP Setting for Windows NT4.0*

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

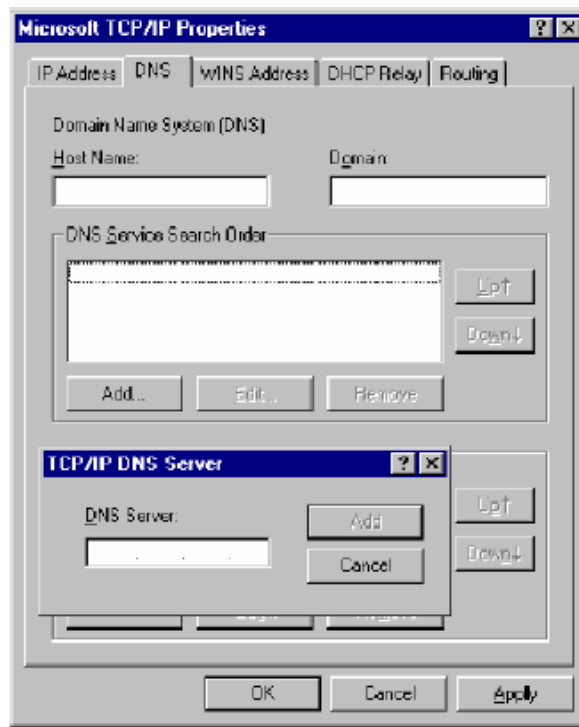


- b) Click “Properties”, window below will appear.



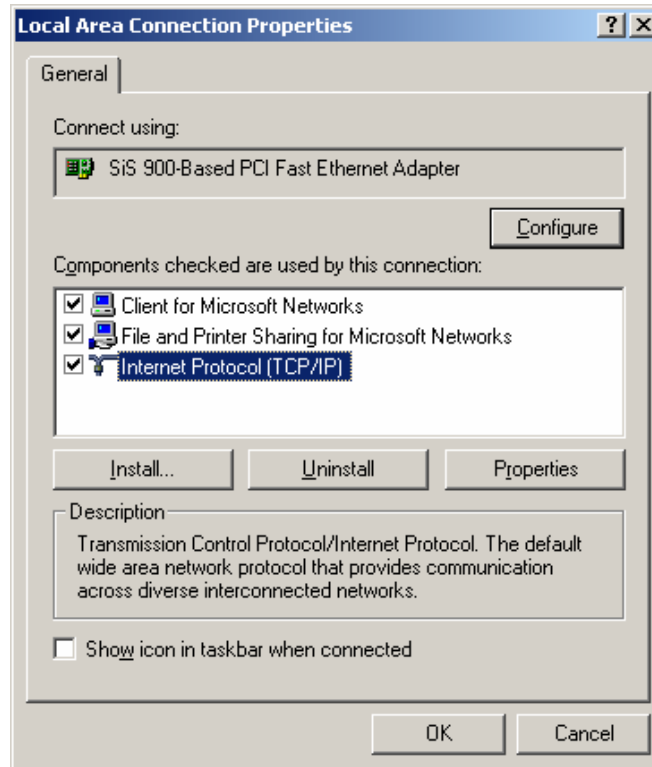
- Select the network card on your system from “**Adapter**” field.
- If you decide to use IP address from Wireless Router, select “**Obtain an IP address from a DHCP server**”.
- If you decide to use the IP address you are desired, select “**Specify an IP address**”. Make sure enter correct addresses 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**”.

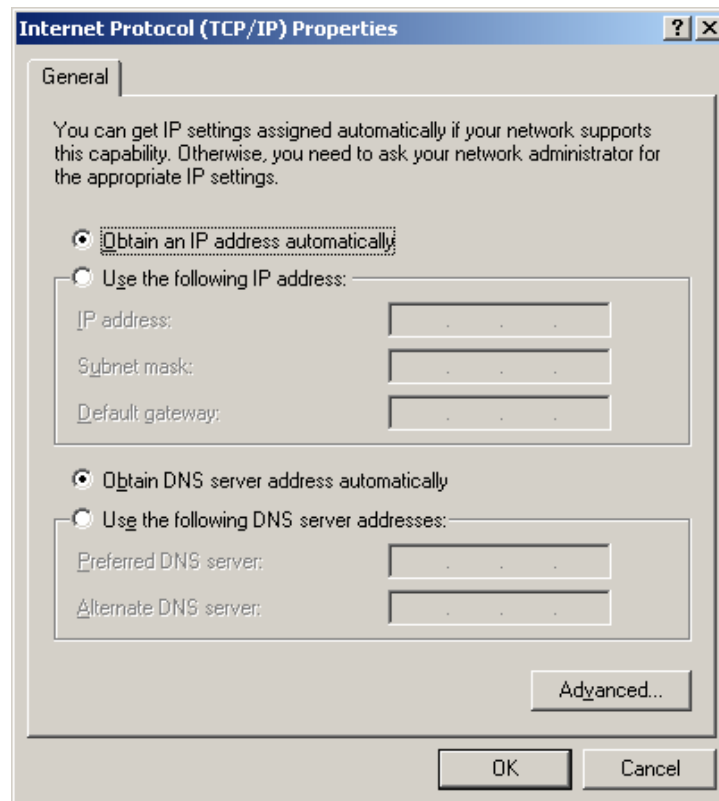


**Checking TCP/IP Settings for Windows 2000**

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



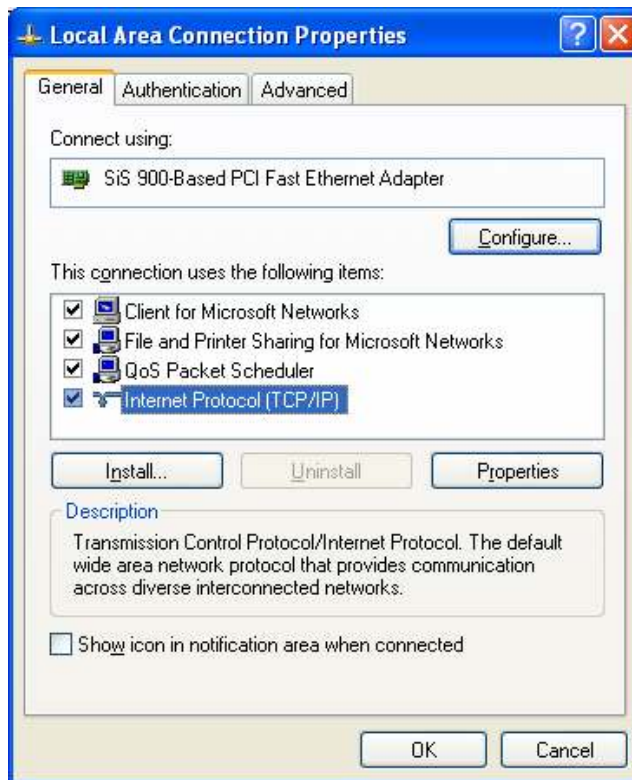
- b) Select the “Internet Protocol (TCP/IP)” for the network card on your system, then click “Properties”, window below will appear.



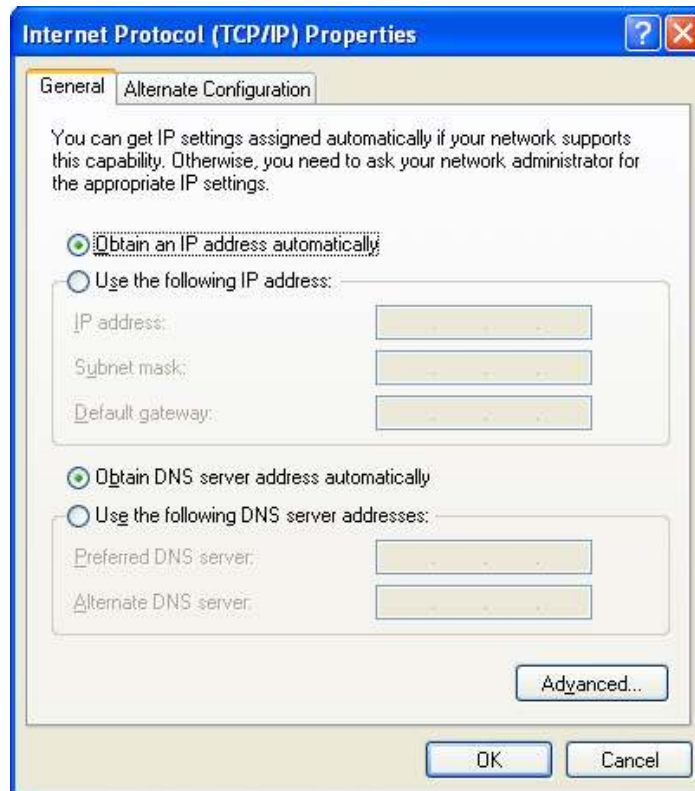
- If you decide to use IP address from Wireless Router, select “**Obtain an IP address automatically**”.
- If you decide to use the IP address you are desired, select “**Use the following IP address**”. Make sure enter correct addresses in “**IP Address**” and “**Subnet Mask**” fields.
- You must set 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.



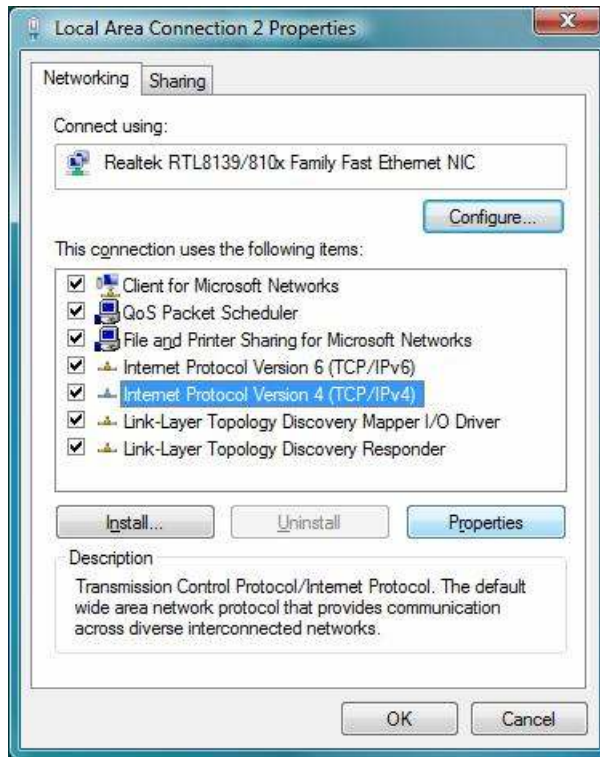
- b) Select “**Internet Protocol (TCP/IP)**” then click “**Properties**”, window below will appear.



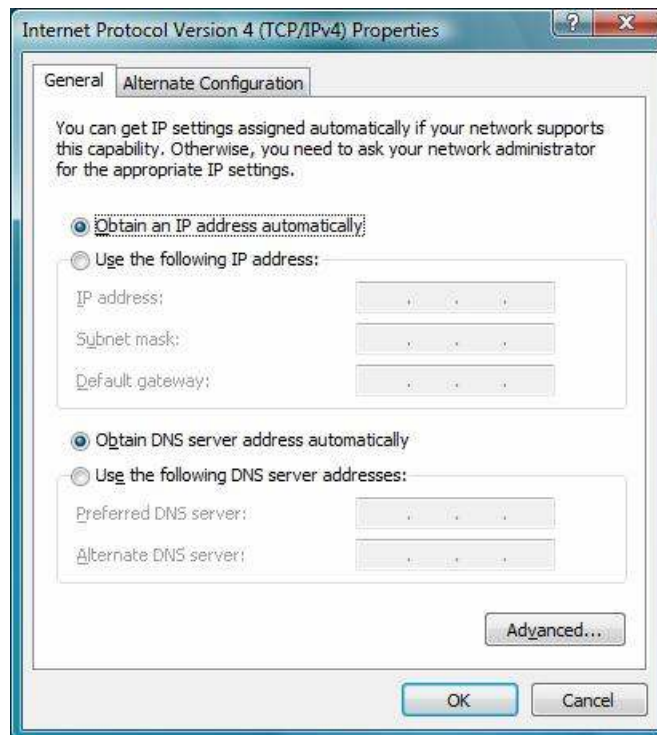
- If you decide to use IP address from Wireless Router, select “**Obtain an IP address automatically**”.
- If you decide to use the IP address you are desired, select “**Use the following IP address**”. Make sure enter correct addresses in “**IP Address**” and “**Subnet Mask**” fields.
- You must set 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**”.

### 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 5.0 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 “**Login**” to access Configuration Utility.



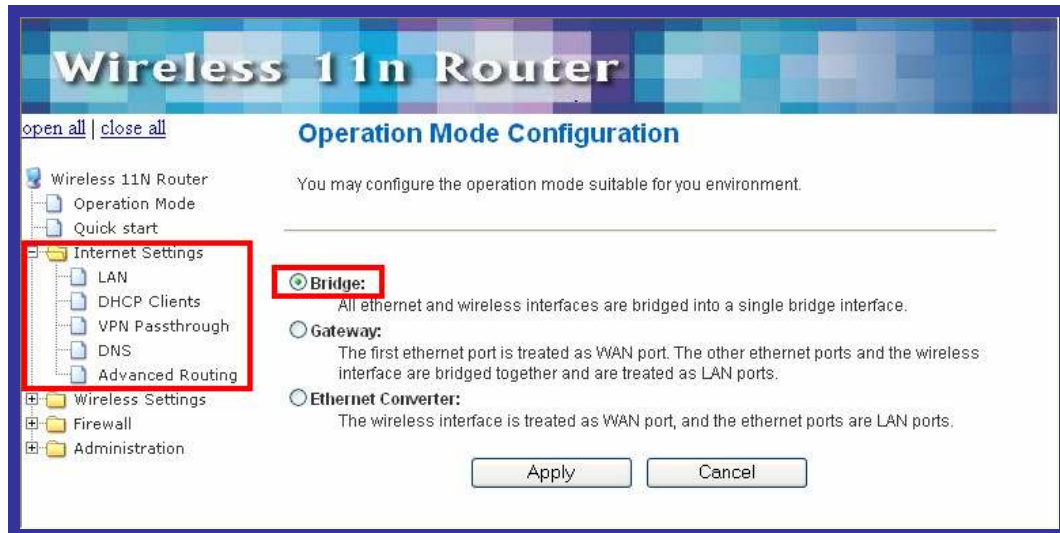
**Step3:** After log in, you can see the Main menu as below.



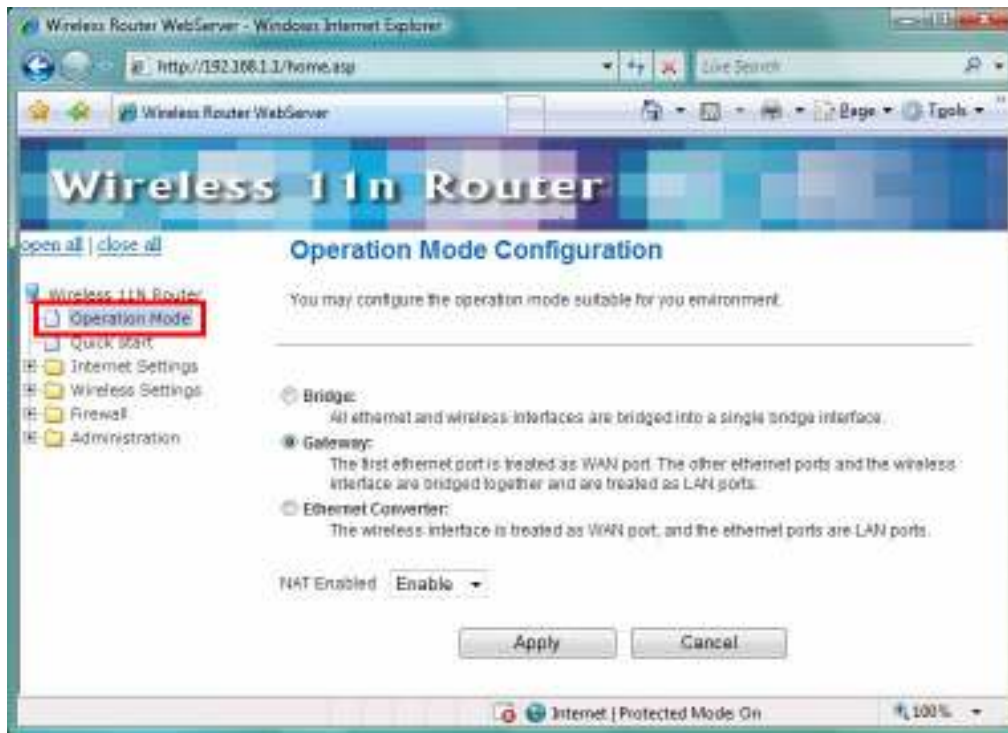
### 3.2 Operation Mode

In this option, you can configure the operation mode which suitable for your environment. The default setting is **Gateway**. There have three modes is provided:

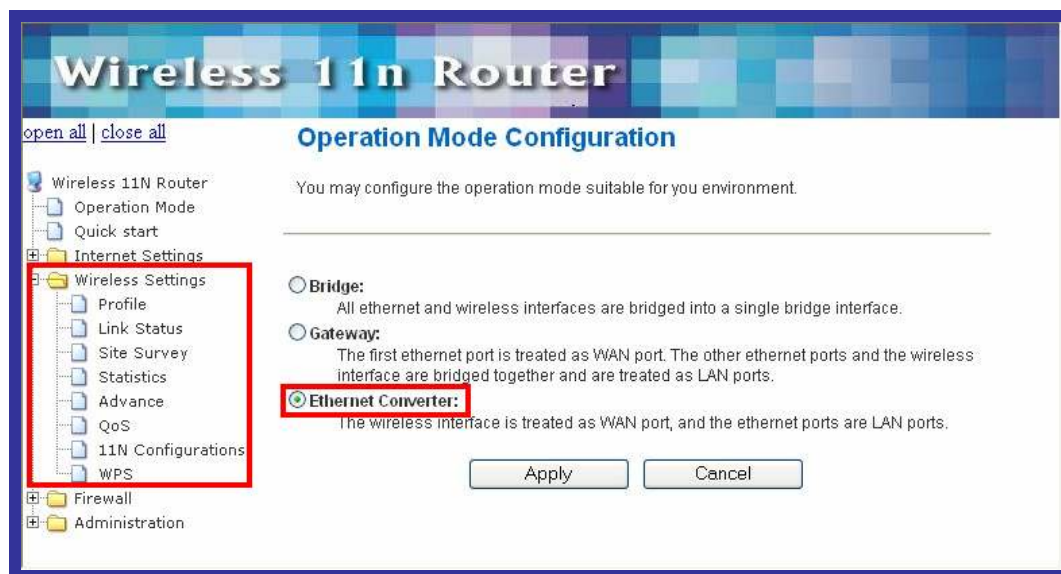
-- **Bridge:** All Ethernet and wireless interfaces are bridged into a single bridge interface. When Bridge mode is applied, there have some functions change in Internet Settings section. As you can see in below, Internet Settings section only has "LAN", "DHCP Client", "VPN Passthrough", "DNS", and "Advanced Routing" for Bridge Mode's configuration.



-- **Gateway:** The first Ethernet port is treated as WAN port. The other Ethernet ports and the wireless interface are bridge together and are treated as LAN ports.



-- **Ethernet Converter:** The wireless interface is treated as WAN port and the Ethernet ports are LAN ports. After Ethernet Converter mode is applied, the WAN will change from Ethernet type to wireless type. There will be five LAN ports and one wireless WAN port. User must configure wireless encryption connection and set the necessary protocols.



**[Profile]** The Station Profile page shows the settings and current operation status of the station.

**Station Profile**

The Status page shows the settings and current operation status of the Station.

Profile List						
Profile	SSID	Channel	Authentication	Encryption	Network Type	
PROF001	RT2561_1	Auto	OPEN	NONE	Infrastructure	

Buttons: Add, Delete, Edit, Activate

**[Link Status]** The Station Link Status page shows the settings and current operation status of the Station.

**Station Link Status**

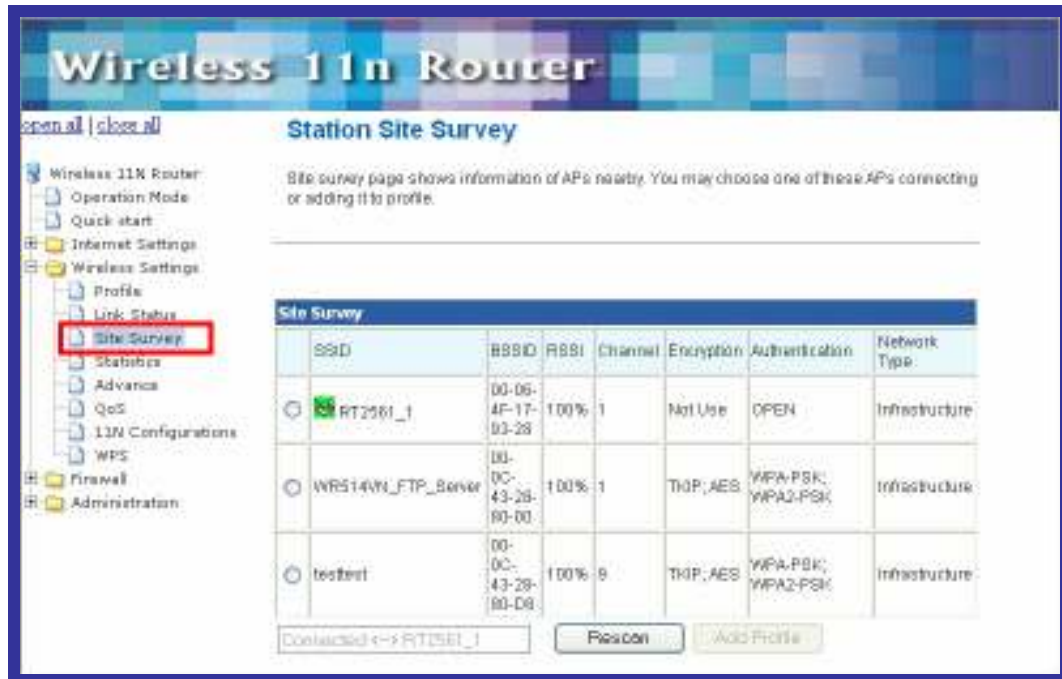
The Status page shows the settings and current operation status of the Station.

Link Status	
Status	RT2561_1 <-> 00-06-4F-17-93-28
Extra Info	Link is Up
Channel	1 <-> 2412000 KHz; Central Channel 1
Link Speed	Tx(Mbps) 54.0      Rx(Mbps) 54.0
Throughput	Tx(Mbps) 0.0      Rx(Mbps) 54.0
Link Quality	Good 100%
Signal Strength 1	Good 80%
Signal Strength 2	Good 90%
Signal Strength 3	Good 95%
Noise Level	Strength 98%

dBm format

MIMO	
BW	20
GI	long
STBC	none
MCS	7
SNR0	26
SNR1	4978192

[Site Survey] Station Site Survey page can show information of APs nearby, you can choose one of these APs connecting or adding it to profile.



For adding a profile, choose one AP and click "Add Profile". And you will see the below screen for AP profile configuration. Enter the necessary information and apply the settings.



**[Statistics]** The Station Statistics page shows the settings and current operation status of the Station.

The Status page shows the settings and current operation status of the Station.

Transmit Statistics	
Frames Transmitted Successfully	122
Frames Transmitted Successfully Without Retry	88
Frames Transmitted Successfully After Retry(s)	34
Frames Fail To Receive ACK After All Retries	0
RTS Frames Successfully Receive CTS	0
RTS Frames Fail To Receive CTS	0

Receive Statistics	
Frames Received Successfully	0
Frames Received With CRC Error	21440
Frames Dropped Due To Out-Of-Resource	0
Duplicate Frames Received	7

Reset Counters

**[Advance]** The Station Advanced Configuration page shows the settings and current operation status of the station.

The Status page shows the settings and current operation status of the Station.

Advance-Configuration	
Wireless Mode(Initial)	802.11 B/G/N mixed mode
Country/Region Code	11 B/G CH1-11
BSS Protection	Auto
TxRate	Auto
<input checked="" type="checkbox"/> Tx Burst	

HT Physical Mode	
HT	<input checked="" type="radio"/> 16M <input type="radio"/> OF
BW	<input type="radio"/> 20 <input checked="" type="radio"/> Auto
GI	<input type="radio"/> Long <input checked="" type="radio"/> Auto
MCS	Auto

RADIO OFF Apply

**Wireless Mode:** Select wireless mode. 802.11B/G mix, 802.11B only, 802.11G only, 802.11N only, 802.11 GN mix mode ,and 802.11B/G/N mix modes are supported.

**Country Region Code:** The available channel differs from different countries. For example: USA (FCC) is channel 1-11, Europe (ETSI) is channel 1-13. The operating frequency channel will be restricted to the country user located before importing. If you are in different country, you have to adjust the channel setting to comply the regulation of the country. Supporting region code for this section has CH1-11, CH10-11, CH10-13, CH14, CH1-14, CH3-9, and CH5-13. Please refer to below Channel Classification and range, Country Channel list to select your Country Region Code:

Country Name	Classification	Range	Country Name	Classification	Range
Argentina	0	CH1-11	Lebanon	1	CH1-13
Australia	1	CH1-13	Liechtenstein	1	CH1-13
Austria	1	CH1-13	Lithuania	1	CH1-13
Bahrain	1	CH1-13	Luxembourg	1	CH1-13
Belarus	1	CH1-13	Macedonia	1	CH1-13
Belgium	1	CH1-13	Malaysia	1	CH1-13
Bolivia	1	CH1-13	Mexico	0	CH1-11
Brazil	0	CH1-11	Morocco	1	CH1-13
Bulgaria	1	CH1-13	Netherlands	1	CH1-13
Canada	0	CH1-11	New Zealand	1	CH1-13
Chile	1	CH1-13	Nigeria	1	CH1-13
China	1	CH1-13	Norway	1	CH1-13
Colombia	0	CH1-11	Panama	1	CH1-13
Costa Rica	1	CH1-13	Paraguay	1	CH1-13
Croatia	1	CH1-13	Peru	1	CH1-13
Cyprus	1	CH1-13	Philippines	1	CH1-13
Czech Republic	1	CH1-13	Poland	1	CH1-13
Denmark	1	CH1-13	Portugal	1	CH1-13
Ecuador	1	CH1-13	Puerto Rico	1	CH1-13
Egypt	1	CH1-13	Romania	1	CH1-13
Estonia	1	CH1-13	Russia	1	CH1-13
Finland	1	CH1-13	Saudi Arabia	1	CH1-13
France	3	CH10-13	Singapore	1	CH1-13
France2	1	CH1-13	Slovakia	1	CH1-13
Germany	1	CH1-13	Slovenia	1	CH1-13
Greece	1	CH1-13	South Africa	1	CH1-13
Hong Kong	1	CH1-13	South Korea	1	CH1-13
Hungary	1	CH1-13	Spain	2	CH10-11
Iceland	1	CH1-13	Sweden	1	CH1-13
India	1	CH1-13	Switzerland	1	CH1-13
Indonesia	1	CH1-13	Taiwan	0	CH1-11
Ireland	1	CH1-13	Thailand	1	CH1-13
Israel	6	CH3-9	Turkey	1	CH1-13
Italy	1	CH1-13	United Arab Emirates	1	CH1-13
Japan	5	CH1-14	United Kingdom	1	CH1-13
Japan2	4	CH14-14	United States of America	0	CH1-11
Japan3	1	CH1-13	Uruguay	1	CH1-13
Jordan	3	CH10-13	Venezuela	1	CH1-13
Kuwait	1	CH1-13	Yugoslavia	0	CH1-11
Latvia	1	CH1-13			

Figure 1: Country Channel list

**B/G Protection:** User can choose from Auto, On, and Off

→ **Auto:** STA will dynamically change as AP announcement

→ **ON:** Always send frame with protection.

→ **Off:** Always send frame without protection.

**TX Rate:** Manually force the Transmit using selected rate. Default is auto.

**Tx Burst:** Frame burst mode.

**HT Physical Mode:** Configure HT Status in use, containing HT(MM or GF), BW(20 or Auto), GI(Long or Auto), and MCS(0~15, 32, or Auto) settings.

[QoS] The QoS configuration page can allow you to configure WMM and Direct Link settings



### (1) QoS Configuration

**WMM:** Enable Wi-Fi Multi-Media.

**WMM Power Saving:** Enable WMM Power Save.

**PS Mode:** Select which ACs you want to enable.

**Direct Link Setup:** Enable DLS (direct Link Setup).

### (2) Direct Link Setup

**MAC Address:** Fill in the blanks of Direct Link with MAC address of STA. Connect with the same AP that supports DLS features

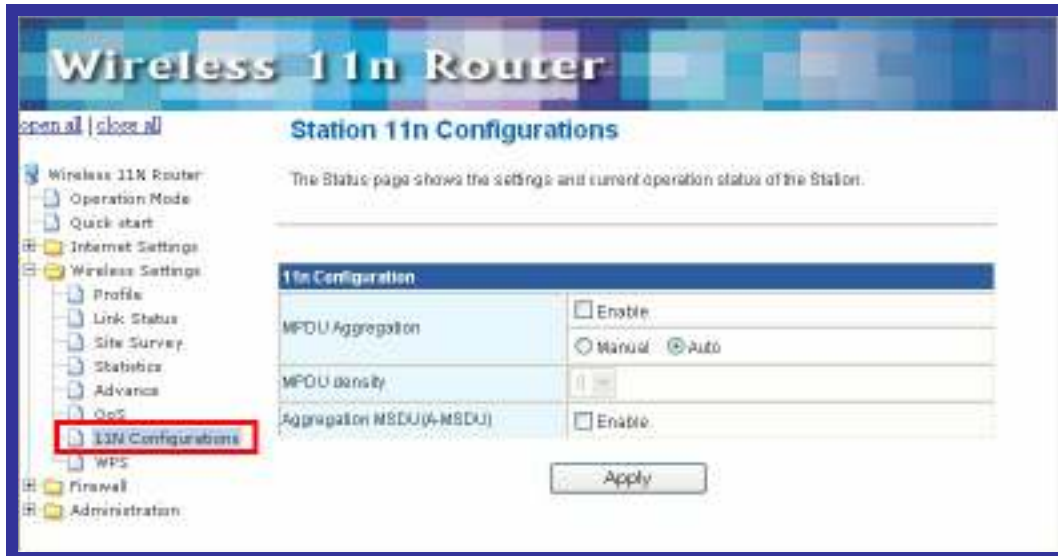
**Timeout Value:** Timeout Value represent that it disconnect automatically after some seconds. The value is integer. The integer must be between 0~65535. It represents that it always

connects if the value is zero.

### (3) DLS Status

After configuring DLS successfully, show MAC address of the opposite side and Timeout Value of setting in “DLS Status”. In “DLS Status” of the opposite side, it shows MAC address of itself and Timeout Value of setting.

**[11n Configurations]** The Station 11n Configurations page shows the settings and current operation status of the station.



**MPDU Aggregation:** MPDU stands for MAC Protocol Data Unit. MPDUs are the fragmented units of MSDU, also called MAC frames, encapsulate the higher layer protocol data or contain MAC management messages.

**MPDU Density:** Select 0~7 to configure the MPDU density.

**Aggregation MSDU (A-MSDU):** A-MSDU stands for Aggregate MAC service data unit. This option allows aggregation of multiple MSDU in one MPDU. The MSDU is that unit of data that is received from the LLC sub-layer which lies above the MAC sub-layer in a protocol stack. The LLC and MAC sub-layers are collectively referred to as the DLL.

[WPS] You can setup security easily by choosing PIN or PBC method to do Wi-Fi Protected setup.



**WPS AP Site Survey:** Display the information of surrounding APs with WPS IE from last scan result. List information includes SSID, BSSID, RSSI, Channel, ID (Device Password ID), Auth., Encrypt, Ver., and Status.

**Refresh:** Issue a rescan command to wireless NIC to update information on surrounding wireless network.

**Mode:** Our station role-playing as an Enrollee or an external Registrar.

**PIN :** 8-digit numbers. It is required to enter PIN Code into Registrar using PIN method. Each NIC Wireless has only one PIN Code of Enrollee.

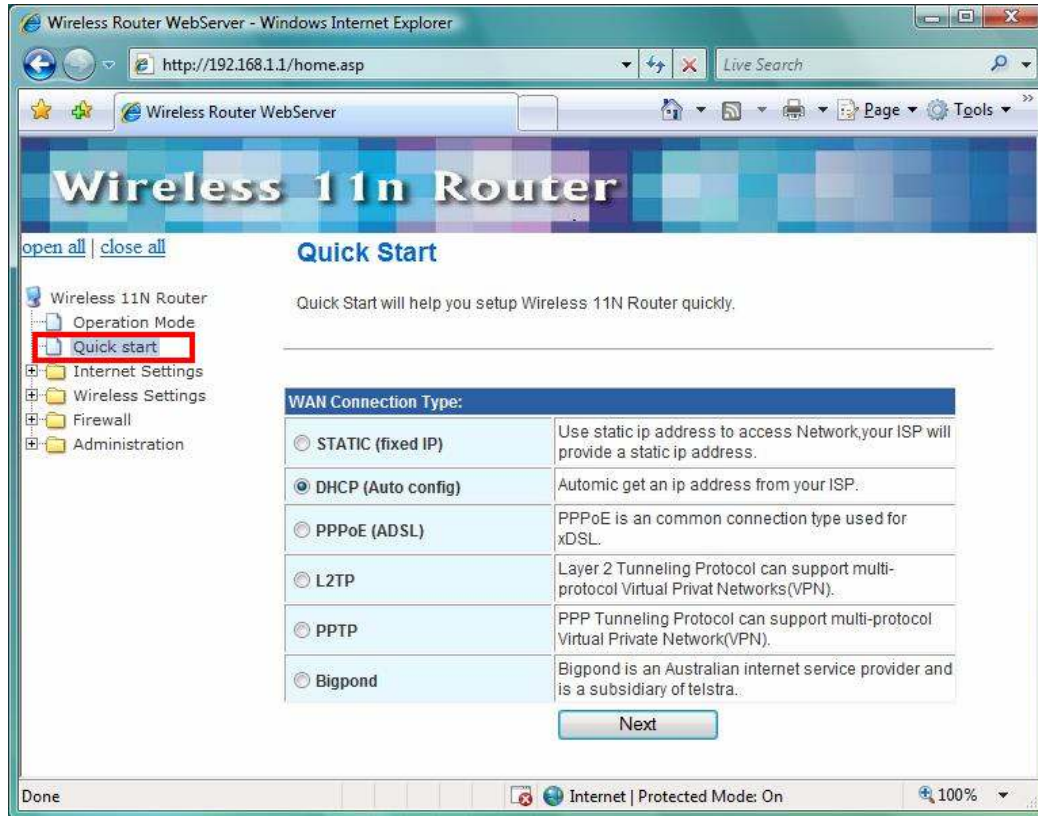
**PIN Start:** Start to add to Registrar using PIN configuration method. IF STA Registrar, remember that enter PIN Code read from you Enrollee before starting PIN.

**PBC Start:** Start to add to AP using PBC configuration method.

**WPS Status:** Display the current status of the WPS function.

### 3.3 Quick Start

Quick Start will help you setup Wireless 11n Router quickly. There have five types of WAN Connections: Static (Fixed IP), DHCP (Auto Config), PPPoE (ADSL), PPTP, L2TP, and BigPond.



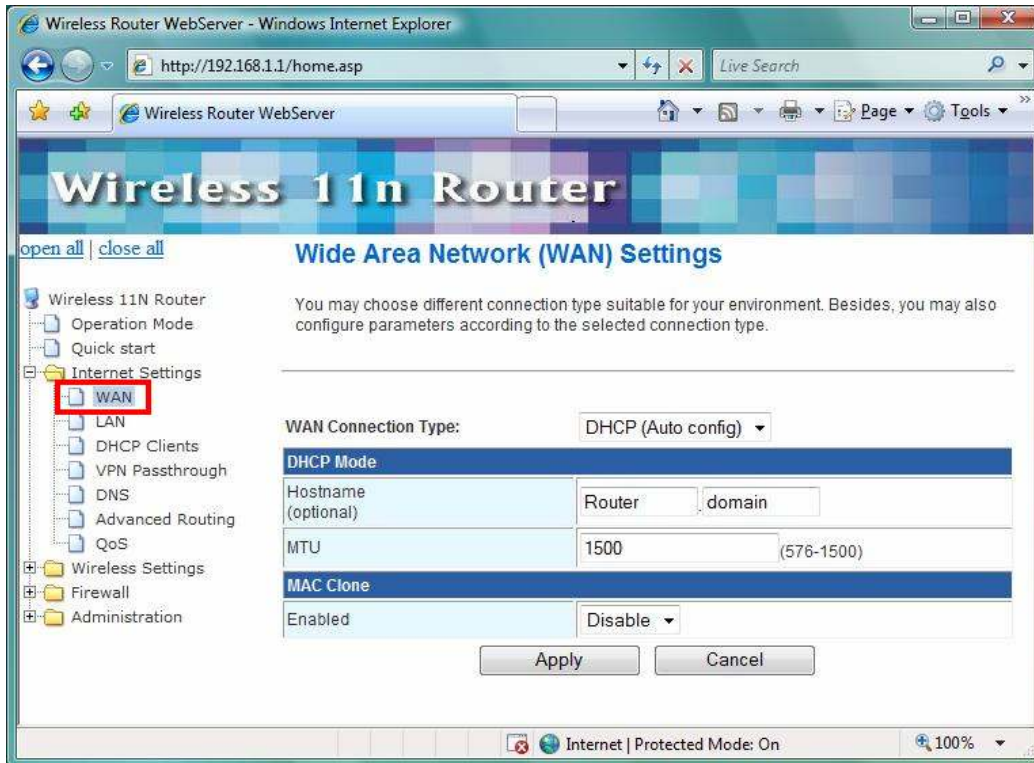
### 3.4 Internet Settings

The Internet Settings contains the following sections:

- WAN
- LAN
- DHCP Clients
- VPN Passthrough
- DNS
- Advanced Routing
- QoS

#### 3.4.1 WAN

The WAN port is the connection of the 802.11n AP Router module to existing broadband device such as Cable modem or ADSL CPE. Click **WAN** on Internet Setting, below screen will prompt for WAN setting.



This AP Router supports 5 methods of obtaining the WAN IP Address:

- **Static IP (fixed IP):** Use static IP address to access Network. Your ISP will provide a static IP address.
- **DHCP (Auto Config):** Automatic gets IP address from your ISP.
- **PPPoE (ADSL):** PPPoE is a common connection type used for xDSL.
- **PPTP:** PPP Tunneling Protocol can support multi-protocol Virtual Private Network (VPN).
- **L2TP:** Layer 2 Tunneling Protocol can support multi-protocol Virtual Private Networks (VPN)
- **BigBond:** Bigbond is an Australian internet service provider and is a subsidiary of Telstra.

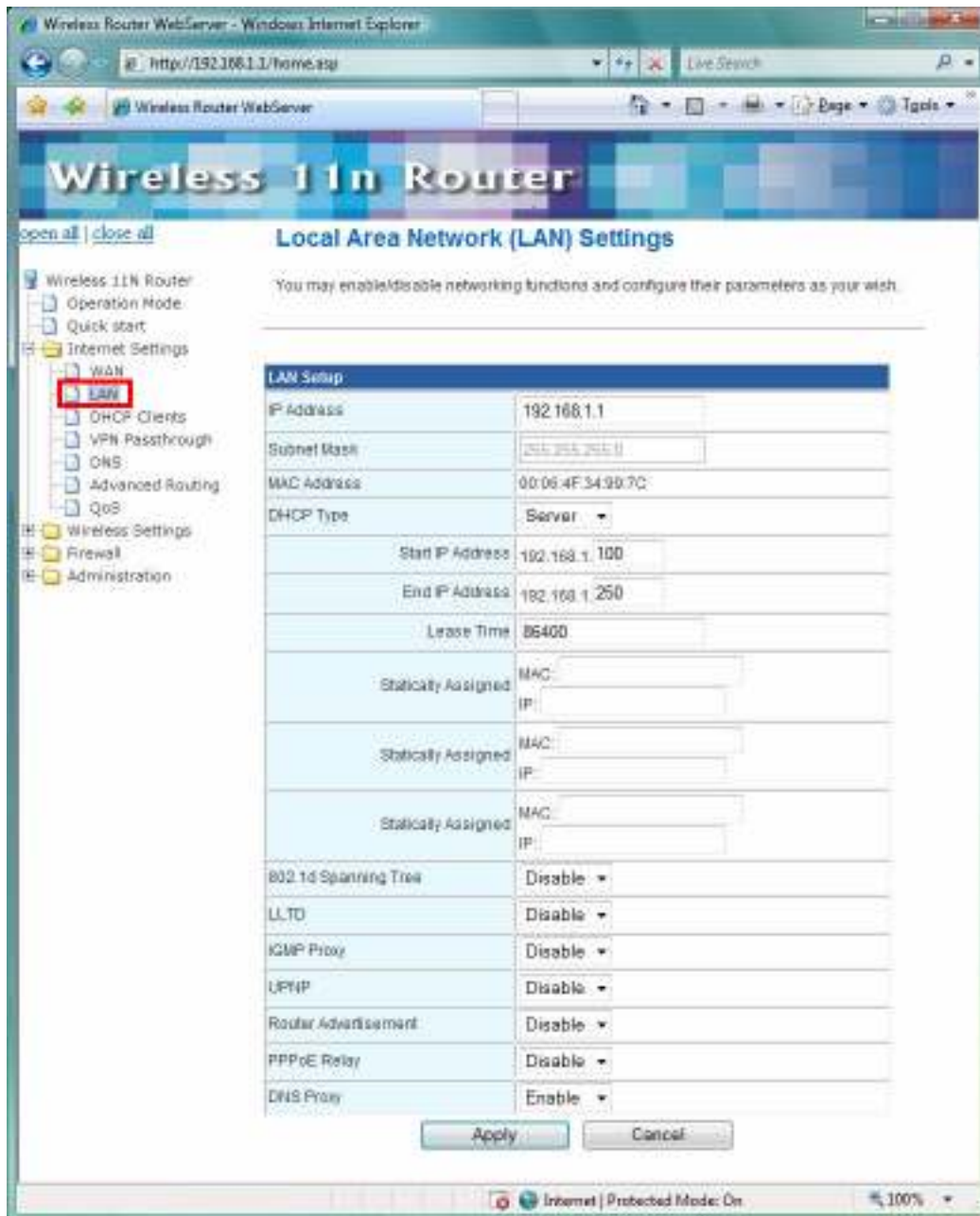
### 3.4.2 LAN

When the module operates in the Gateway mode, it supports the NAT (NAPT) feature. It means the WAN and LAN interfaces are located in different network segments and therefore the data traffic needs to be routed between the two interfaces.

To communicate with 802.11n router properly, must assign an IP address to the LAN port of the user's PC. There are two ways to assign a proper IP address to the user PC's LAN port:

- **Manual configuration of the user PC:** This required if the user configures the 802.11n router WAN port with a static IP address.
- **Dynamic IP assignment with DHCP:** 802.11n router can act as a DHCP server which dynamically assigns an IP address to user's PC located in the LAN-side network.

Click **LAN** on Internet Settings, below screen will prompt for LAN setting.



**LAN IP Address:** The LAN IP address. Default: **192.168.1.1**

**Subnet Mask:** The LAN net-mask. Default: **255.255.255.0**

**DHCP Type:** Select Disable to disable this Router to distribute IP address. Select Server to enable this Router to distribute IP addresses (DHCP server). And the following field will be activated for you to enter this starting IP address.

**Start IP address:** Specify the starting IP address of the IP address pool. Default Start IP: **192.168.1.100**.

**End IP address:** Specify the ending IP address of the IP address pool. Default End IP: **192.168.1.250**.

**Lease Time:** Specify the time duration for which the settings will be in effect. Default: **86400** seconds.

**802.1d Spanning Tree:** Default: **Disable**.

**LLTD:** Default: **Disable**.

**IGMP Proxy:** Default: **Disable**.

**UPnP:** UPnP is architecture for pervasive peer-to-peer network connectivity of PCs and intelligent devices or appliances, particularly within the home. UPnP builds on Internet standards and technologies, such as TCP/IP, HTTP, and XML, to enable these devices automatically connect with one another and work together to make networking – particularly home networking – possible for more people. Default: **Disable**.

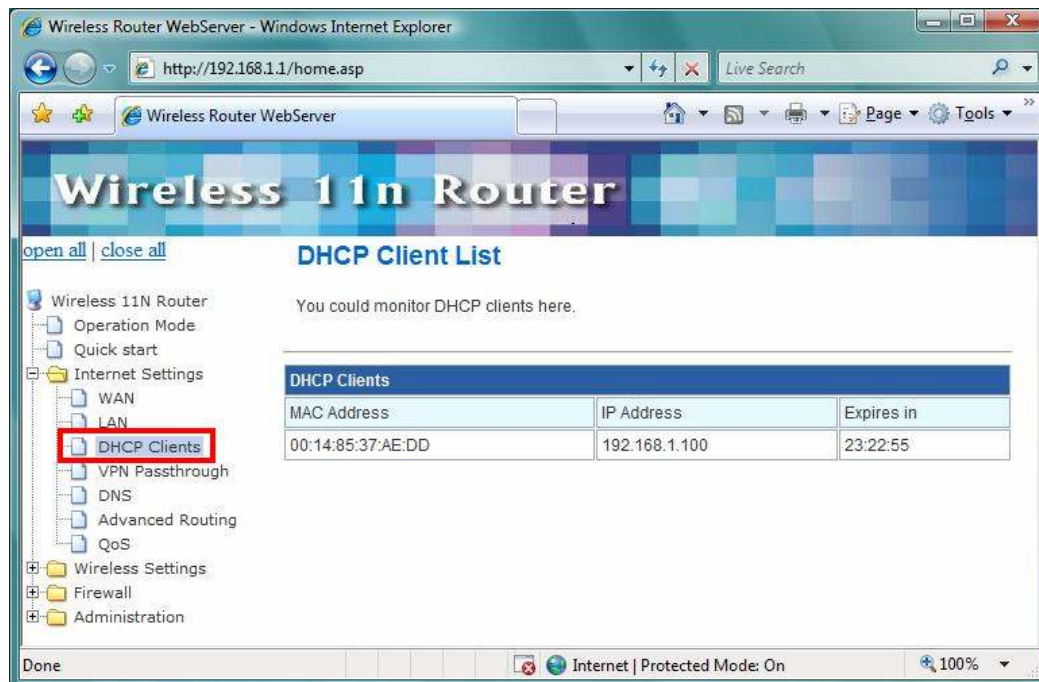
**Router Advertisement:** Default: **Disable**.

**PPPoE Relay:** Default: **Disable**.

**DNS Proxy:** Enable the DNS Proxy that will relay users'/clients' DNS requests to a real DNS server IP address. Users no need to specify real DNS server IP address. Default: **Enabled**.

### 3.4.3 DHCP Clients

DHCP client computers connected to the device will have their information displayed in the DHCP Client List table. The table will show the MAC Address, IP Address and Expires in of the DHCP lease for each client computer.



The screenshot shows a web browser window titled "Wireless Router WebServer - Windows Internet Explorer" with the address bar showing "http://192.168.1.1/home.asp". The page header reads "Wireless 11n Router". On the left, a navigation tree shows "Internet Settings" expanded, with "DHCP Clients" highlighted in red. The main content area is titled "DHCP Client List" and contains a table with the following data:

DHCP Clients		
MAC Address	IP Address	Expires in
00:14:85:37:AE:DD	192.168.1.100	23:22:55

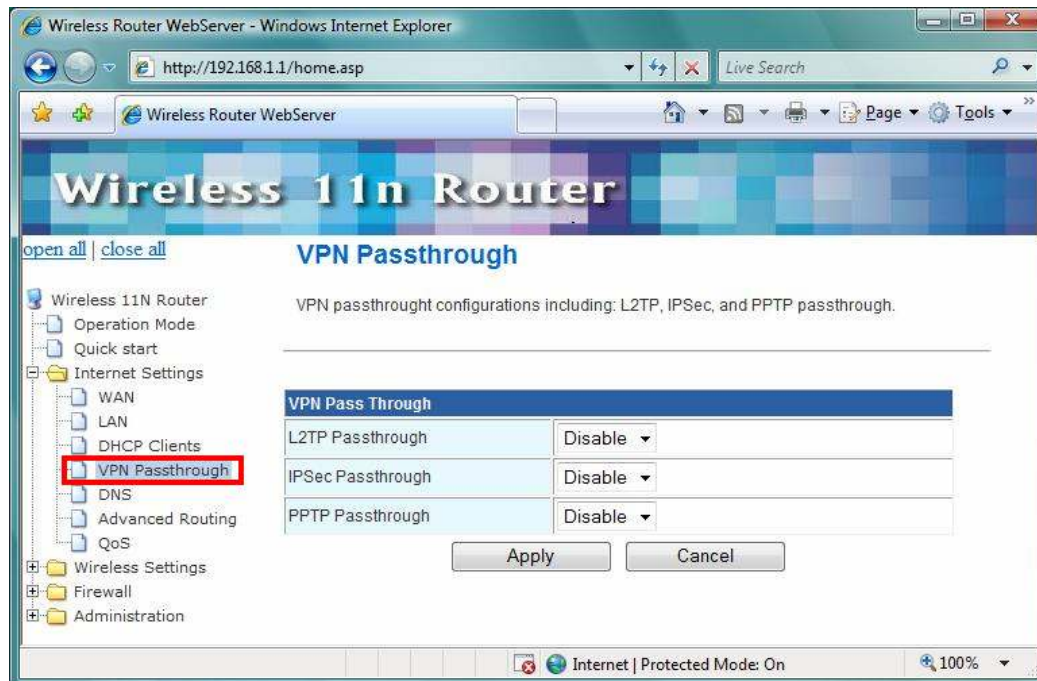
**MAC Address:** Shows the client MAC address information.

**IP address:** Shows the client IP address information.

**Expires in:** Shows the expired time of the client.

### 3.4.4 VPN Passthrough

VPN passthrough configurations including: L2TP, IPSec, and PPTP passthrough.



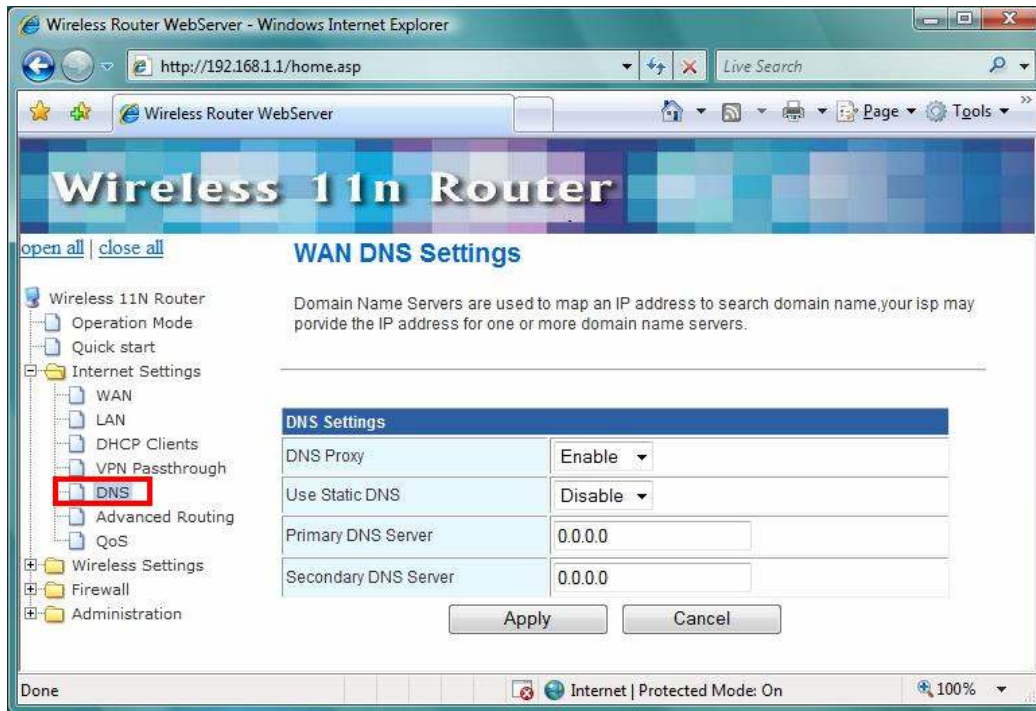
**L2TP Passthrough:** L2TP is an extension to the Point-to-Point Protocol, which is an important component for VPNs. VPNs allow users and telecommuters to connect to their corporate intranets or extranets.

**IPSec Passthrough:** IPSec is a framework for a set of protocols for security at the network or packet processing layer of network verification.

**PPTP Passthrough:** PPTP is a protocol that allows corporations to extend their own corporate network through private "tunnels" over the public Internet. Enable/Disable this protocol verification.

### 3.4.5 DNS

Domain Name Servers are used to map an IP address to search domain name, your ISP may provide the IP address for one or more domain name servers



**DNS Proxy:** Enable/Disable this Wireless Router DNS.

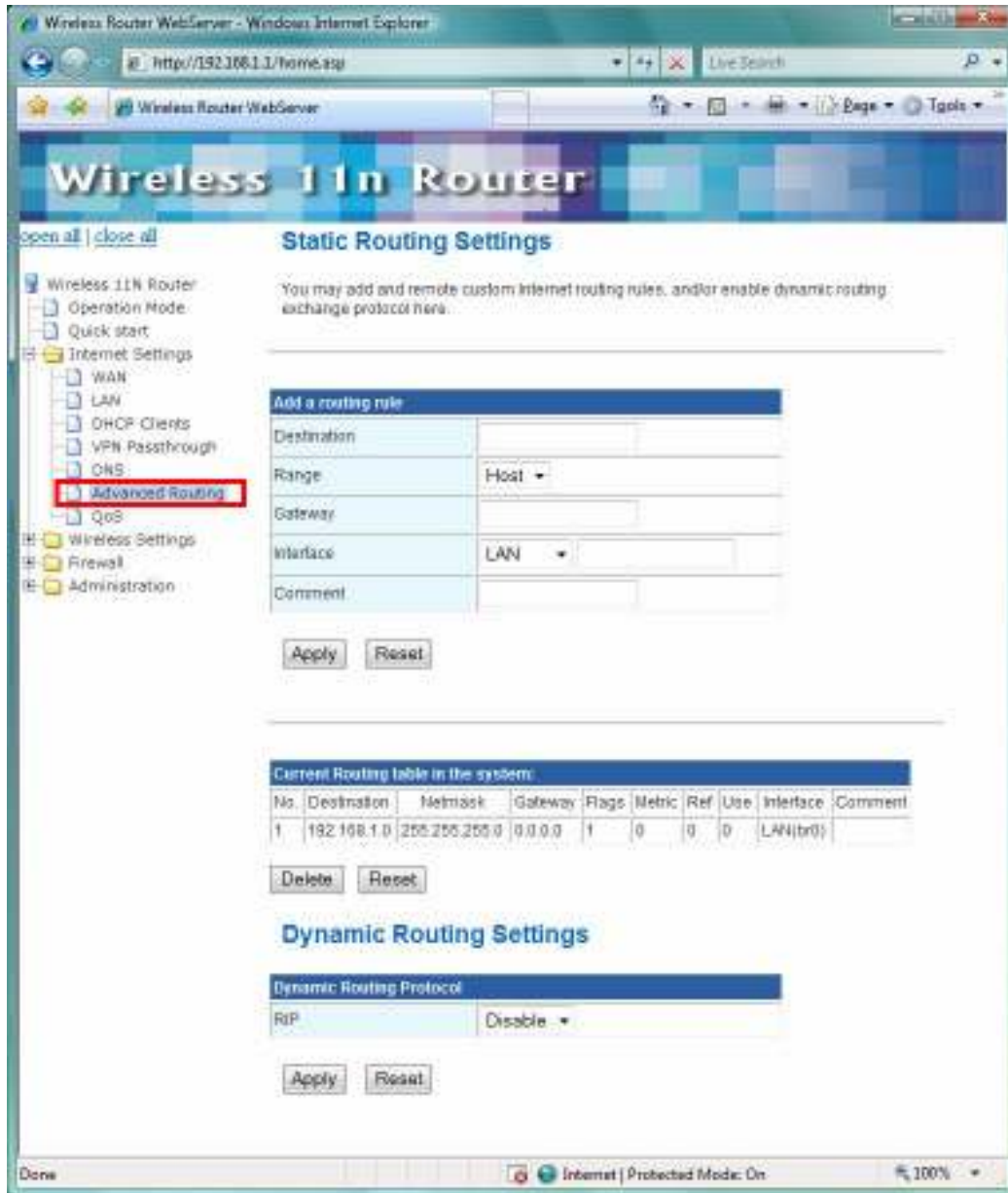
**Use Static DNS:** Specify the DNS server. Default is **Disable**.

**Primary DNS Server:** Enter the IP address of the Primary DNS Server provided by your ISP.

**Secondary DNS Server:** Enter the IP address of the Secondary DNS Server provided by your ISP.

### 3.4.6 Advanced Routing

Static routes are special routes that the network administrator manually enters into the router configuration. The route table allows the user to configure and define all the static routes supported by the router. You may add and remote custom Internet routing rules, and/or enable dynamic routing exchange protocol here.



**<Add a routing rule>**

**Destination:** Defines the base IP address (Network Number) that will be compared with the destination IP address (after an AND with NetMask) to see if this is the target route.

**Range:** select the range from drop down list

**Gateway:** Enter IP address of the next hop router that will be used to route traffic for this route. If this route is local (defines the locally connected hosts and Type = Host) then this IP address MUST be the IP Address of the router.

**Interface:** Select the interface mode from drop down list.

**Comment:** Enter the comment for this static route.

### <Current Routing table in the system>

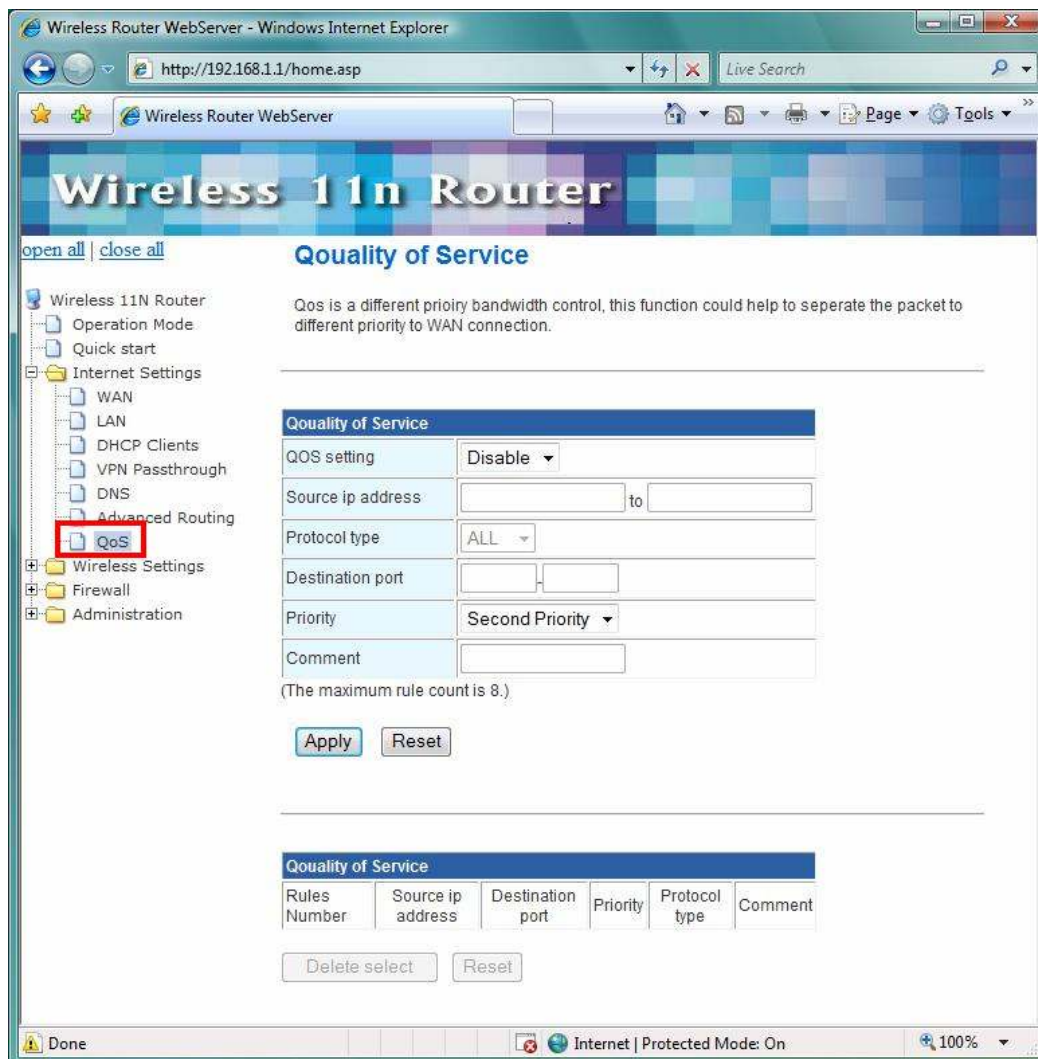
To see the detail settings of current routing table in the system.

### <Dynamic Routing Setting>

**RIP:** RIP can be used to cache routes learned by routing protocols, thus allowing the automation of static routing maintenance. The router, using the RIP (Routing Information Protocol) protocol, determines the network packet's route based on the fewest number of hops between the source and the destination. In this case, you could automatically adjust to physical changes in the network layout. Default is **Disable**.

## 3.4.7 QoS

QoS (Quality of Service) is a different priority bandwidth control; this function could help to separate the packet to different priority to WAN connection. This option will provide better service of selected network traffic over various technologies. Deploying QoS management to guarantee that all application receive the service levels required and sufficient bandwidth to meet performance expectations is indeed one important aspect of modern enterprise network.



**Source IP address:** Enter a single or range of IP Address for LAN source.

**Protocol type:** There have three type of this protocol, ALL, TCP, and UDP

**Destination port:** Specify a single port or range of port

**Priority:** Base on the QoS setting and priority level, packet will make the WAN connection by different priority.

### **3.5 Wireless Settings**

The wireless settings can be quickly configured as a wireless access point for roaming client by setting the access identifier and channel number. It also supports data encryption and client filtering. The Wireless Settings contains the following sections:

- Basic
- Advanced
- Security
- WPS
- Station List
- Site Survey

#### **3.5.1 Basic**

This function allows you to define SSID, and Channel for the wireless connection. These parameters are used for the wireless stations to connect to the Access Point. Click **Basic Setting** on Wireless Settings, below screen will prompt for Basic Setting.



### [Wireless Network]

**Radio On/Off:** Enable/Disable the Wireless radio feature. Default setting is **Radio OFF**.

**Network Mode:** Choose a mode from the pull-down menu. Make sure that you have the equipment you need. As you're looking for products in stores or on the Internet, you might notice that you can choose equipment that supports five different wireless networking technologies: **802.11b/g/n Mixed**, **802.11b/g Mixed**, **802.11b**, **802.11g**, and **802.11n**

**Network Name (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 20 characters long and contain letters and numbers. Default name is **Default\_11N**.

**Multiple SSID1~7:** A multiple SSID is referred to a network name because essentially it is a name that identifies a wireless network.

**Broadcast Network Name (SSID): Enable-** This wireless AP will broadcast its SSID to

station. **Disable**- This wireless AP will not broadcast its SSID to stations. If stations want to connect to this wireless AP, this AP's SSID should be known in advance to make a connection.

**BSSID**: MAC address of this wireless router.

**Frequency**: Select 1~13 or AutoSelect from the pull-down menu.



#### [Wireless Distribution System (WDS)]

**WDS Mode**: Select the mode from the pull-down menu, Disable, Lazy Mode, Bridge Mode, or Repeater Mode.

#### [HT Physical Mode]

**Operation Mode: Mixed mode operation** – In this mode, both the MIMO-OFDM system and the legacy systems shall co-exist. The MIMO system should have the capability to generate legacy packets for the legacy system and high throughput packets for MIMO-OFDM systems. So, the burst structure should be decodable to legacy systems and should provide better performance to MIMO-systems. **Green Field mode operation** – This mode is similar to mixed mode where the transmission happens only between the MIMO-OFDM systems in the presence of legacy receivers. However, the MIMO-OFDM packets transmitted in this mode will

have only MIMO specific preambles and no legacy format preambles are present.

**Channel Bandwidth:** Specify the channel bandwidth. Select 20 or 20/40, default setting is **20/40**.

**Guard Interval:** Guard-Interval is used to reduce interference of multi-path channel.

**MCS:** Select the MCS from the pull-down menu 0~15, 32 or Auto. Default: **Auto**.

**Reverse Direction Grant (RDG):** Enable/Disable RDG function.

**Extension Channel:** Choose extension channel from the drop down list.

**Aggregation MSDUA (A-MSDU):** This option allows aggregation of multiple MSDUs in one MPDU

**Auto Block ACK:** Enable/Disable Auto Block ACL function.

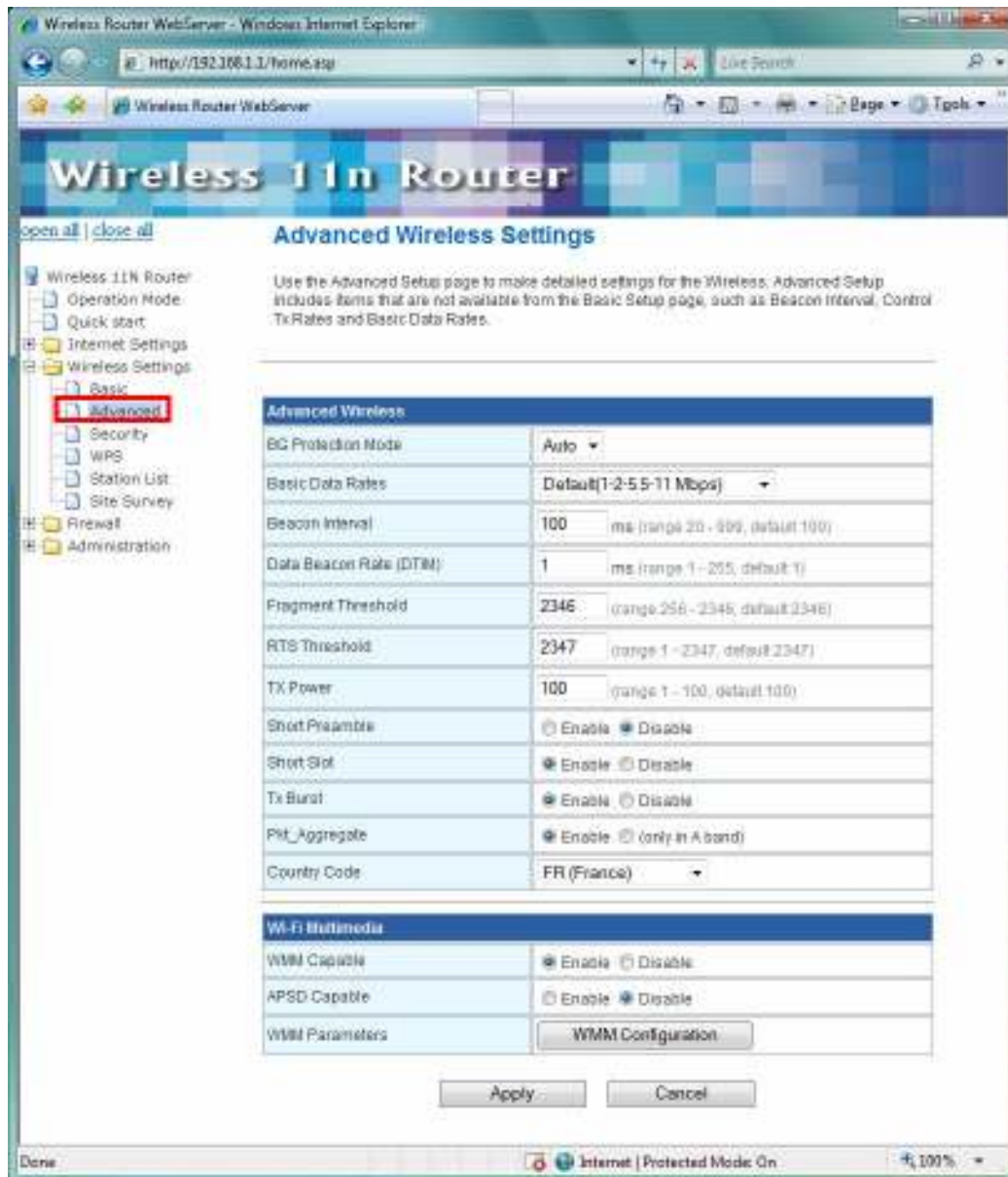
**Decline BA Request:** Enable/Disable BA request function.

**HT TxStream:** Select 1 or 2 from the pull-down menu.

**HT RxStream:** Select 1 or 2 from the pull-down menu.

### **3.5.2 Advanced**

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 AP router. Click **Advanced** on Wireless Settings, below screen will prompt for Advanced Setting.



**BG Protection Mode:** A protection mechanism prevents collisions among 802.11b/g modes. Select **Auto**, **On**, or **Off** from the pull-down menu.

**Basic Data Rates:** By default, the unit adaptively selects the highest possible rate from transmission. Select the basic rates to be used among the following options: **1-2Mbps**, **Default** (1-2-5.5-11Mbps), or **All** (1-2-5.5-6-11-12-24Mbps)

**Beacon Interval:** Beacon Interval is the amount of time between beacon transmissions. Before a station enters power save mode, the station needs the beacon interval to know when to wake up to receive the beacon. Range 20-999, default is **100**.

**Data Beacon Rate (DTIM):** The DTIM period indicates how many beacon frames can transmit before another DTIM is transmitted. Range from 1-255, default setting is **1**.

**Fragment Threshold:** Fragmentation mechanism is used for improving the efficiency when

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 than 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**.

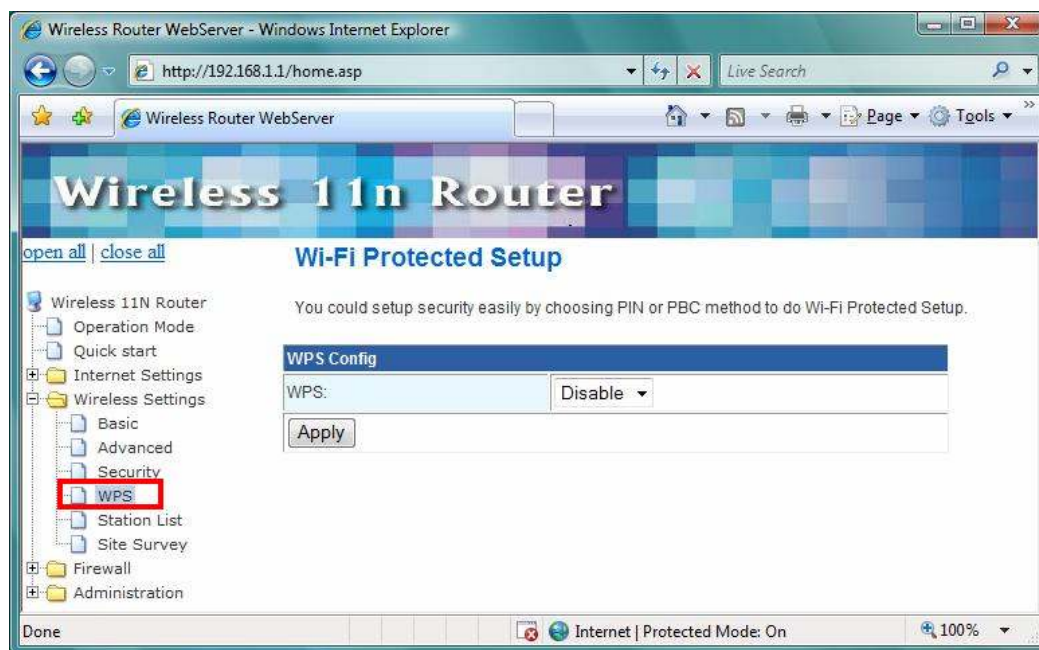
**Shared Secret:** Enter the password that the router shares with the RADIUS Server.

**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 reset 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, you 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 an 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.

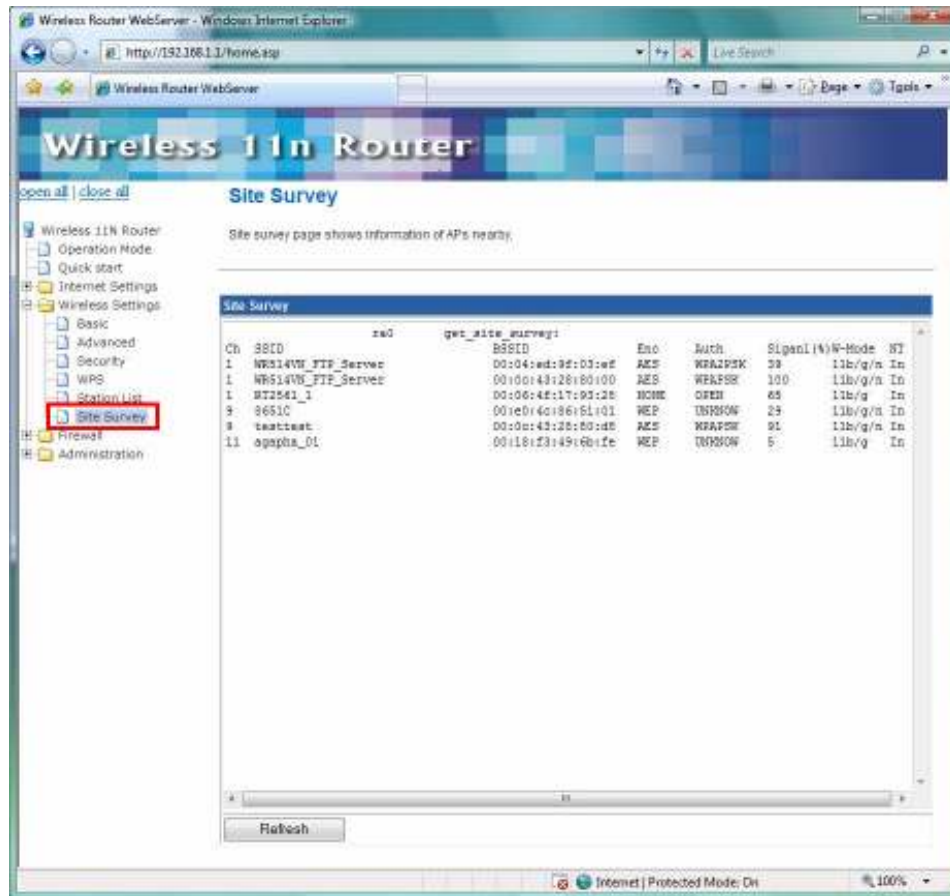
### 3.5.5 Station list

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.



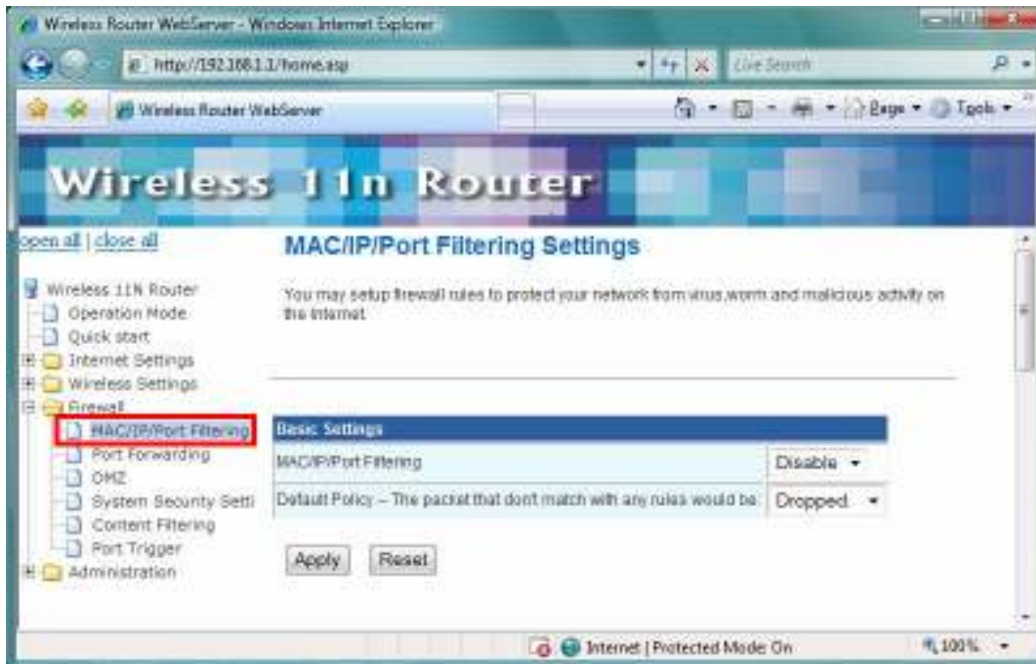
### 3.6 Firewall

The Firewall contains the following sections:

- MAC/IP/Port Filtering
- Port Forwarding
- DMZ
- System Security Setting
- Content Filtering
- Port Trigger

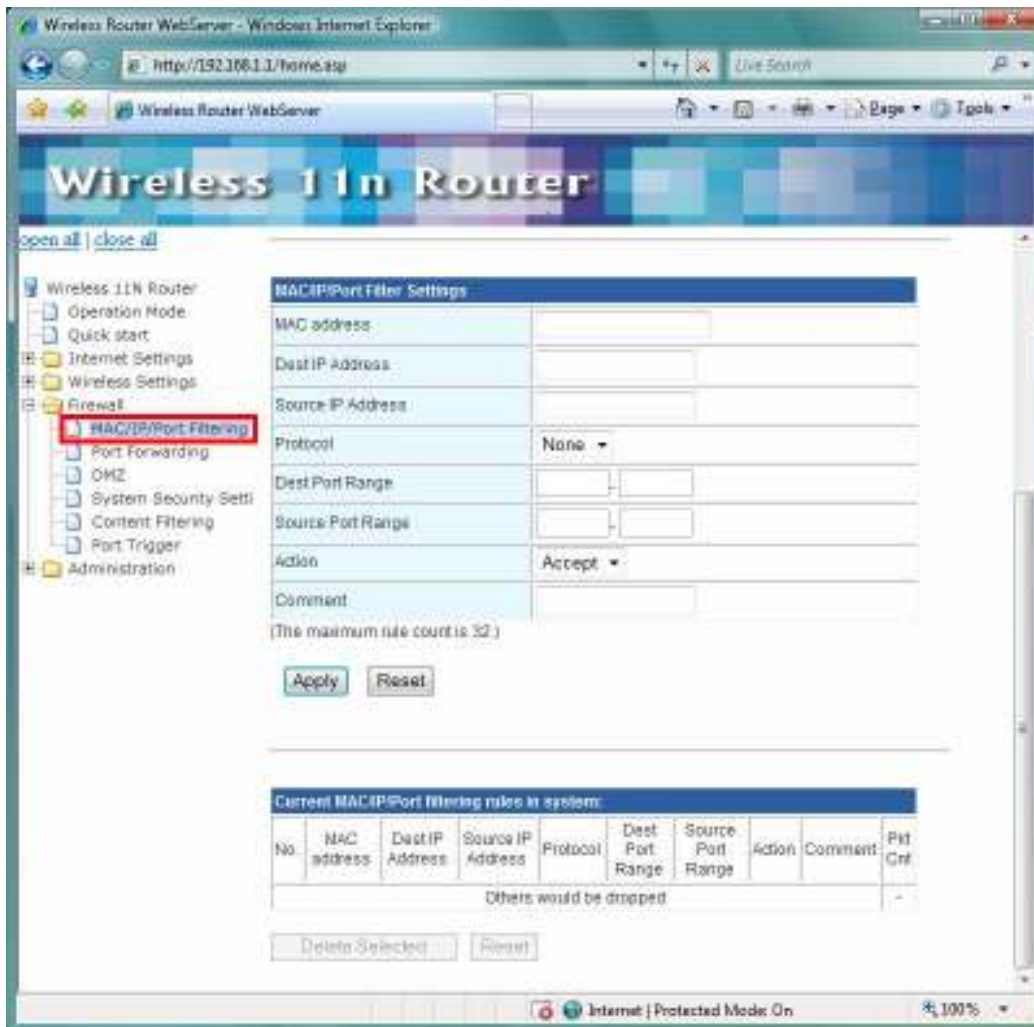
#### 3.6.1 MAC/IP/Port Filtering Settings

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.

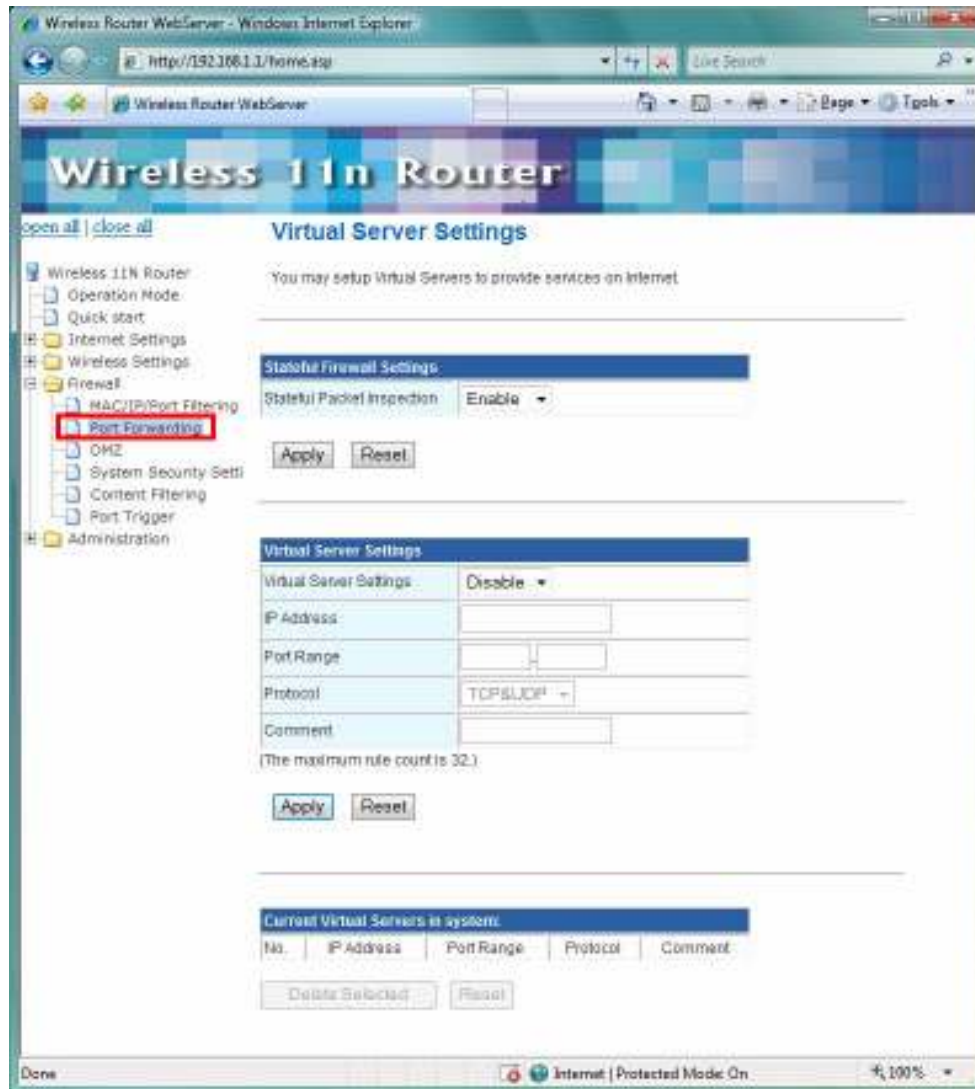
**Protocol:** This is the protocol type that will be used with the Port that will be blocked.

**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.

**ICMP Smurf Attack:** Do not response to the broadcasting ICMP request.

**Ping of Death:** To avoid the main system to receive overloading ICMP packet.

**Allow ICMP Maximum Packet Size:** You can set the maximum allowing ICMP packet size when Ping of Death function is enabled. (The total length is ICMP header + ICMP data + IP header).

**TCP/UDP Port Scan:** To detect any suspected port scan behavior within the packet flow.

**TCP Null Scan:** When checking the flags of TCP header without any setting, the router determines this situation as TCP Null Scan and drops this packet.

**TCP X'mas Tree Scan:** When checking the flags settings of TCP header do not comply with the rule of RFC793, the router will determines this situation as TCP X'mas Tree scan and drops this packet.

**TCP Full X'mas Tree Scan:** When checking the flags settings of TCP header have been configured, the router determines this situation as TCP Full X'mas Tree Scan and drops this packet.

**SYN Flood:** To block the suspected SYN Flood attacked.

**SYN Limit Rate:** When enable SYN Flood function, you can enter the limit rate for TCP SYN packets which allow to pass per second.

**FIN Flood:** To block the suspected FIN Flood attacked.

**FIN Limit Rate:** When enable FIN Flood function, you can enter the limit rate for TCP FIN packets which allow to pass per second.

**UDP Flood:** To block the suspected UDP Flood attacked.

**UDP Limit Rate:** When enable UDP Flood function, you can enter the limit rate for TCP UDP packets which allow to pass per second.

**ICMP Flood:** To block the suspected ICMP Flood attacked.

**ICMP Limit Rate:** When enable ICMP Flood function, you can enter the limit rate for TCP ICMP packets which allow to pass per second.

### 3.6.5 Content Filtering

You can setup content filter to restrict the improper content access.



**Content Filter Setting:** There have three options for this filter – Proxy, Java, and ActiveX. When those options are checked, the content filter will deny computer from access to the internet by contented those options.

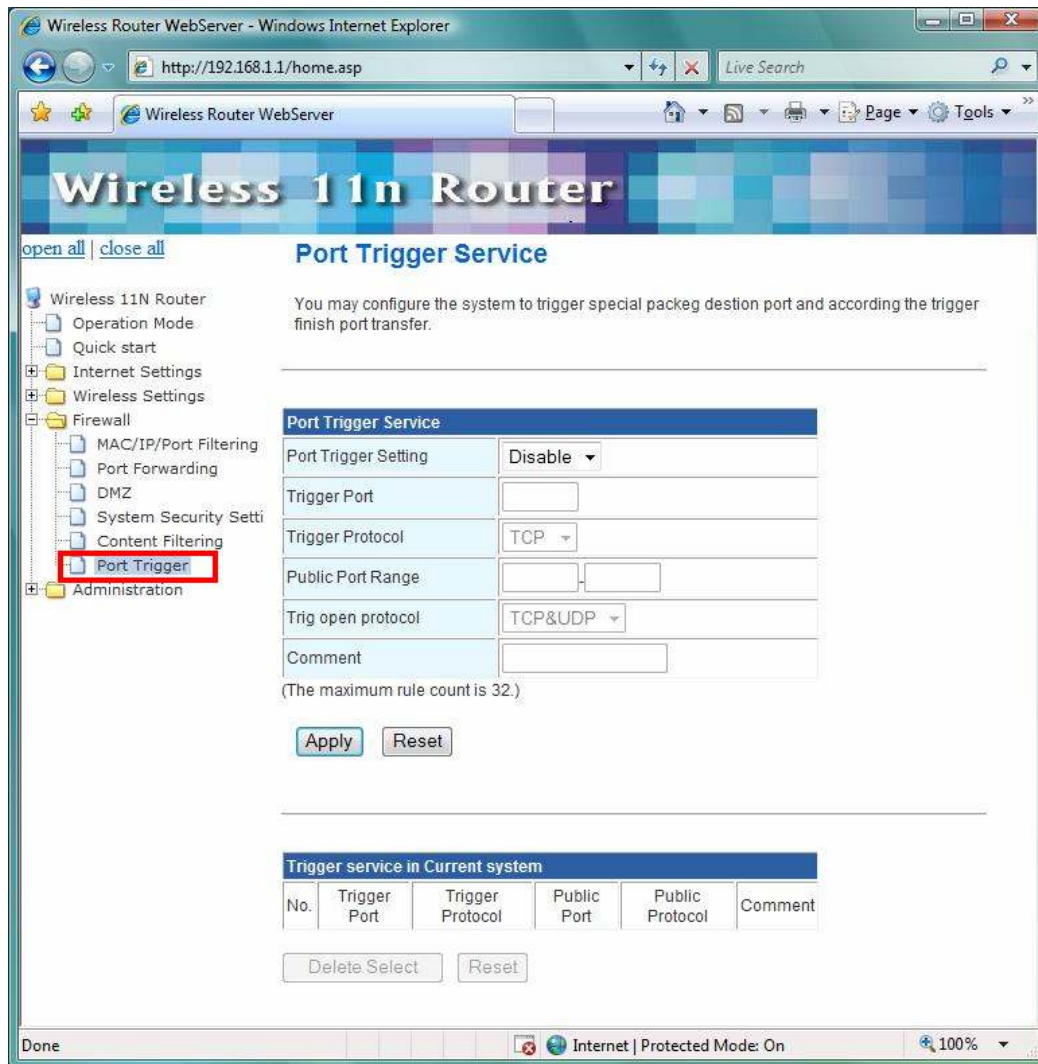
**Web URL Filter Setting:** With security reason, the URL Filter provides the enterprise to manage and restrict employee access to non-business or undesirable content on the Internet. URL Filter is a web solution that blocks web-sites access according the URL Filter String no matter the URL string is found full or partial matched with a keyword.

**Web Host Filter Settings:** Web Host Filter is a web solution that blocks web-sites access

according the Web Host name or partial matched with a keyword.

### 3.6.6 Port Trigger

Some applications require multiple connections, such as Internet gaming, video conferencing, Internet telephony and others. If you need to run applications that require multiple connections, specify the port normally associated with an application in the “Trigger Port” field, select the protocol type as TCP or UDP, then enter the public ports associated with the trigger port to open them for inbound traffic.



**Port Trigger Setting:** Enable/Disable the port trigger.

**Trigger Port:** This is the port used to trigger the application. It can be either a single port or a range of ports.

**Trigger Protocol:** This is the protocol used to trigger the special application.

**Public Port Range:** 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.

**Trig open protocol:** This is the protocol used for the special application.

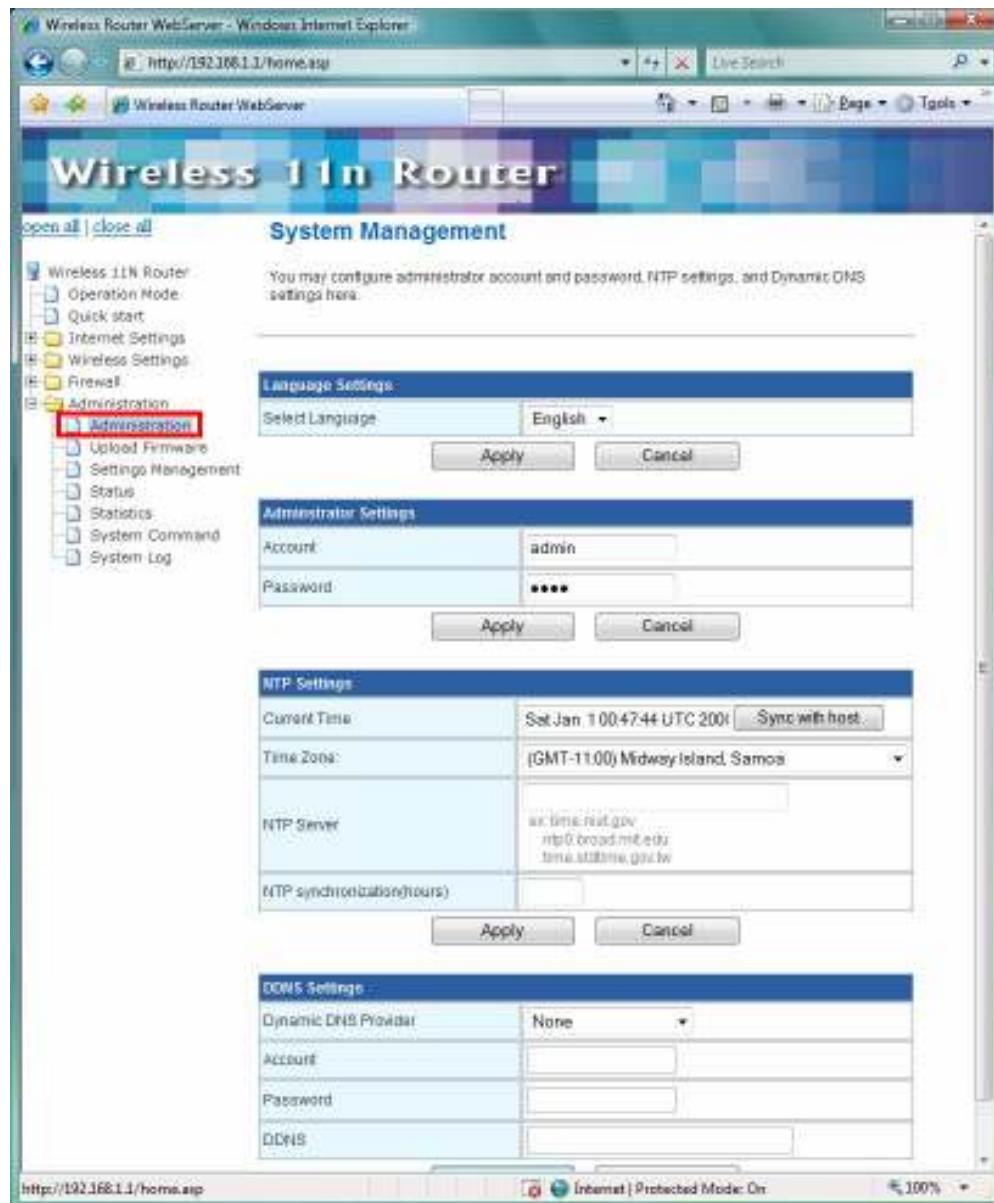
### 3.7 Administration

The Administration contains the following sections:

- Administration      Upload Firmware      Setting Management      Status
- Statistics              System Command      System Log

#### 3.7.1 Administration

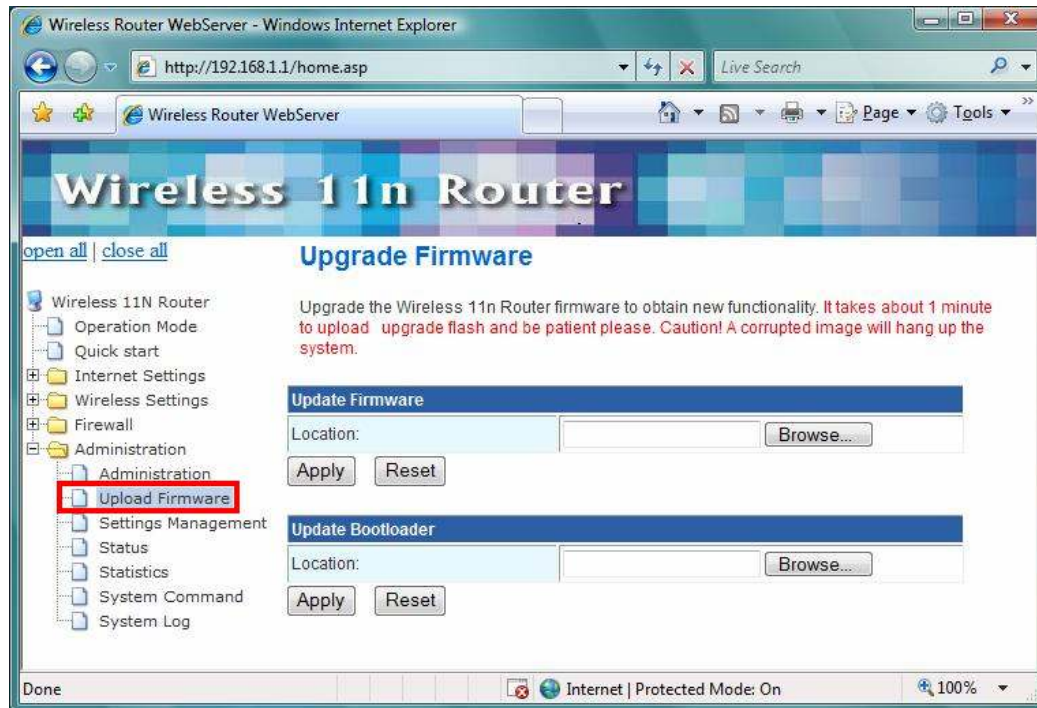
You may configure administrator account and password, NTP settings, and Dynamic DNS settings here.



### 3.7.2 Upgrade Firmware

Firmware is the main software image, which the AP Router needs to perform all tasks in real time. Firmware upgrades are required for adding new features or to resolves bugs. It takes about 1 minute to upload/upgrade flash and be patient please.

**Caution:** A corrupted image will hang up the system.



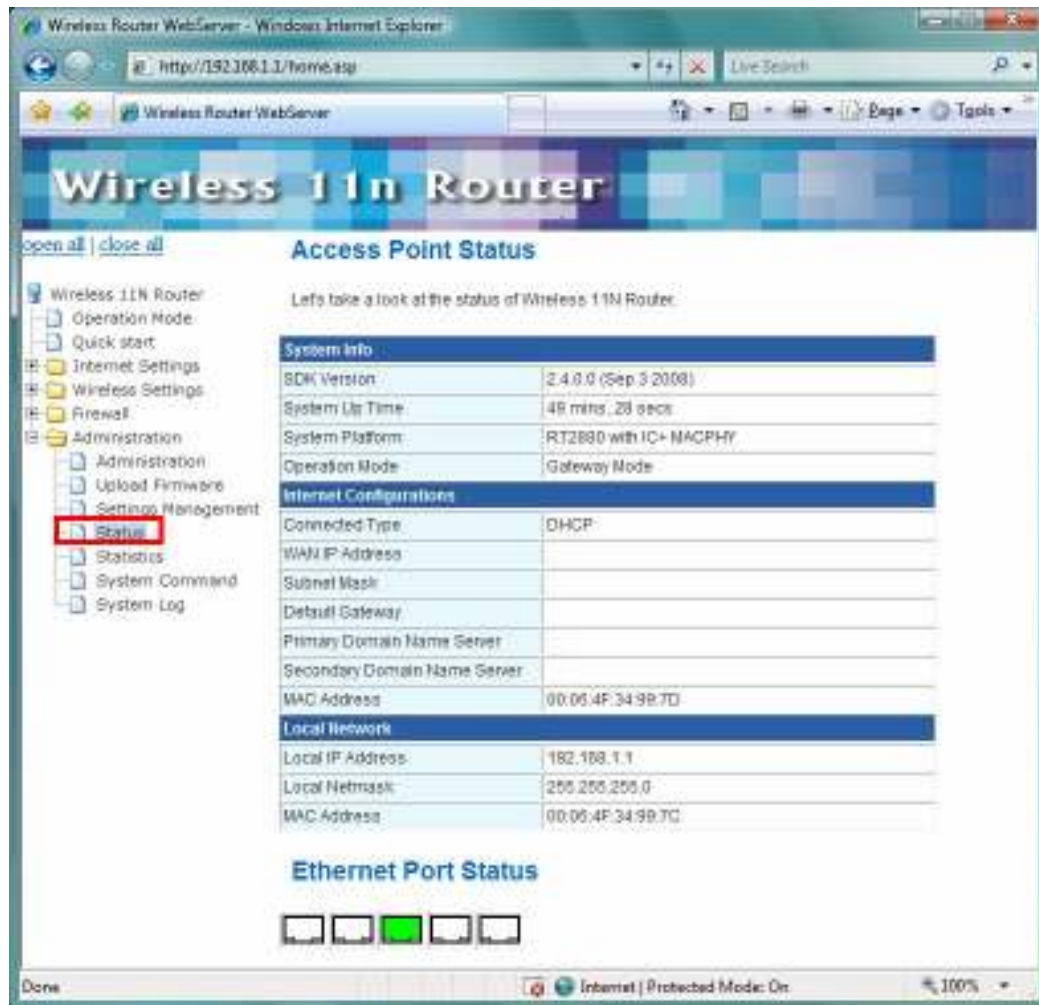
### 3.7.3 Setting Management

You might save system settings by exporting them to configuration file, restore them by import the file, or reset them to factory default.



### 3.7.4 Status

In this section, you can look at the status of this wireless 11n Router, such as System Info, Internet Configurations, and Local Network...etc.



The screenshot displays the 'Wireless 11n Router' web interface in a Windows Internet Explorer browser. The address bar shows 'http://192.168.1.1/home.asp'. The page title is 'Wireless 11n Router'. On the left, a navigation tree is visible with 'Status' highlighted in red. The main content area is titled 'Access Point Status' and includes a sub-header 'System Info' with the following details:

System Info	
BDK Version	2.4.0.0 (Sep 3 2008)
System Up Time	48 mins, 28 secs
System Platform	RT2880 with IC+ MACPHY
Operation Mode	Gateway Mode

Below this is the 'Internet Configurations' section:

Internet Configurations	
Connected Type	DHCP
WAN IP Address	
Subnet Mask	
Default Gateway	
Primary Domain Name Server	
Secondary Domain Name Server	
MAC Address	00:05:4F:34:9B:7D

The 'Local Network' section is also present:

Local Network	
Local IP Address	192.168.1.1
Local Netmask	255.255.255.0
MAC Address	00:05:4F:34:9B:7C

At the bottom, there is an 'Ethernet Port Status' section with five status indicators, the third of which is green.

### 3.7.5 Statistics

In this section, you can look at the statistics of this wireless 11n Router, such as Memory statistics, WAN/LAN's Rx & Tx packets, and all interface statistics...etc

The screenshot shows the 'Statistic' page of a Wireless 11n Router. The left sidebar contains a navigation menu with 'Statistics' highlighted. The main content area displays the following data:

Take a look at the router statistics.

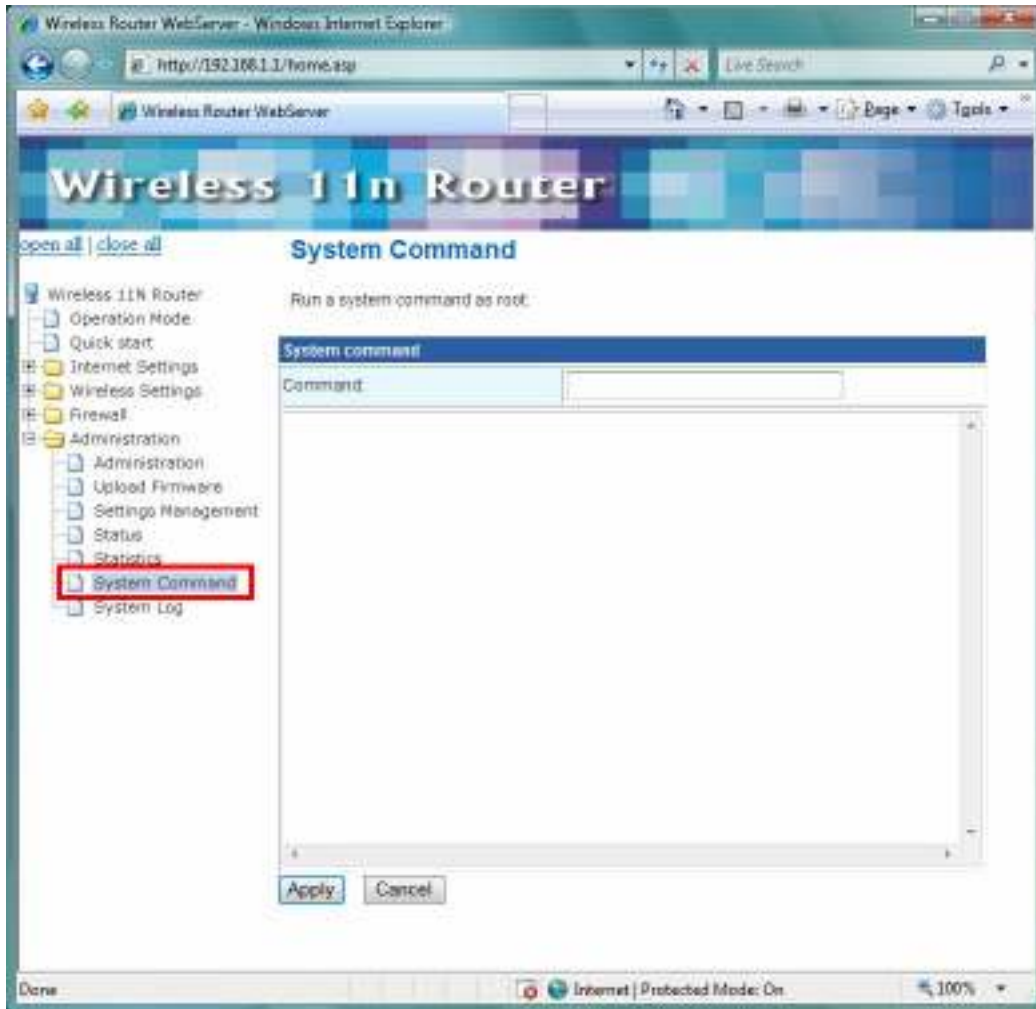
Memory	
Memory total:	28568 KB
Memory left:	14584 KB

WAN/LAN	
WAN Rx packets:	0
WAN Rx bytes:	0
WAN Tx packets:	139
WAN Tx bytes:	77842
LAN Rx packets:	2216
LAN Rx bytes:	170840
LAN Tx packets:	2211
LAN Tx bytes:	778646

All interfaces:	
Name	lo
Rx Packet	14
Rx Byte	2249
Tx Packet	14
Tx Byte	2249
Name	eth0
Rx Packet	0
Rx Byte	0
Tx Packet	0
Tx Byte	0
Name	eth1
Rx Packet	0
Rx Byte	0
Tx Packet	0
Tx Byte	0

### 3.7.6 System Command

In this section, you can run a system command as root.



### 3.7.7 System Log

This 802.11n Router supports sending system log (sending UDP packets and keeping log messages in Log Server. Click **Refresh** on **Administration**, below screen will prompt for System Log information

