

# Wireless IEEE802.11b/g/n 300Mbps Tiny Router

## R4020A

# User Manual

Version 1.0

Date: Aug. 22, 2011

## FCC Certifications



### Federal Communication Commission Interference Statement

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.

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 communications. 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 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 the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

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 transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

### 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 minimum distance 20cm between the radiator & your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

## CE Mark Warning



This equipment complies with the requirements relating to electromagnetic compatibility, EN 55022 class B for ITE, the essential protection requirement of Council Directive 2004/108/EC on the approximation of the laws of the Member States relating to electromagnetic compatibility.

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. 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.

Copyright © 2009, All Rights Reserved.

Note: The country code selection is for non-US model only and is not available to all US model. Per FCC regulation, all WiFi product marketed in US must fixed to US operation channels only.

### 以下警語適用台灣地區

經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。前項合法通信，指依電信法規定作業之無線電通信。低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

# Contents

Unpacking Information .....	6
Chapter 1 Introduction to Wireless Router .....	7
1.1 General Description .....	7
1.2 Key Features .....	7
Chapter 2 Installing and Using Wireless Router .....	8
2.1 Connecting this Router to your network .....	8
2.2 Configuring the IP address of your computer .....	8
Chapter 3 Management .....	12
3.1 Starting the WEB-Based Management Interface .....	12
3.2 The Graphic User Interface .....	12
3.3 Setup Wizard .....	14
3.4 Operation Mode .....	19
3.5 Wireless .....	20
3.5.1 Basic Settings .....	20
3.5.2 Advanced Settings .....	23
3.5.3 Security .....	25
3.5.4 Access Control .....	29
3.5.5 WDS Settings .....	30
3.5.6 Site Survey .....	31
3.5.7 WPS Settings .....	31
3.5.8 Schedule .....	32
3.6 TCP/IP Settings .....	34
3.6.1 LAN Interface Setup .....	34
3.6.2 WAN Interface Setup .....	36
3.7 Firewall Settings .....	44
3.7.1 Port Filter .....	44
3.7.2 IP Filter .....	45
3.7.3 MAC Filter .....	47
3.7.4 Port Forwarding .....	48
3.7.5 URL Filter .....	49
3.7.6 DMZ .....	50
3.8 QoS .....	50
3.9 Management .....	51
3.9.1 Status .....	51
3.9.2 Statistics .....	52
3.9.3 DDNS Settings .....	53

3.9.4	Time Zone Setting .....	54
3.9.5	Denial-of-Service .....	55
3.9.6	Log.....	57
3.9.7	Upgrade Firmware.....	58
3.9.8	Save/Reload Setting.....	58
3.9.9	Password.....	59

## Unpacking Information

Thank you for purchasing the product. Before you start, please check all the contents of this package.

The product package should include the following:

1. One Wireless Router
2. One Power Adapter
3. One resource CD, including:
  - ✧ User's Manual
  - ✧ QIG

**Note:**

Make sure that the package contains the above items. If any of the listed items are damaged or missing, please contact with your distributor.

## Conventions

The Router mentioned in this guide stands for IEEE 802.11n Wireless Router without any explanation.

## Chapter 1 Introduction to Wireless Router

### 1.1 General Description

#### **Draft 802.11n Wireless Connectivity**

The IEEE802.11n Wireless Router provides a better wireless signal for network than existing wireless 802.11g technology. It complies with IEEE 802.11n draft 2.0 and IEEE802.11b/g wireless standards.

#### **Greater Range and Coverage**

The router allows multiple users to share one broadband connection, as well as secures your private network. With its built-in switch port and wireless AP, LAN users can share files, printers, or playing network games all at a blazing speed. This technology maximizes the speed and range of your wireless signal to significantly outperform 802.11g devices.

#### **Advanced Network Security**

As for security, it also supports the latest wireless security features to help prevent unauthorized access, be it from over a wireless network or from the Internet. Moreover, supporting for WPA and WPA2 standards ensure that you will be able to use the best possible encryption, regardless of your client devices. In addition, this Wireless 11n Router utilizes dual active firewalls (SPI and NAT) to prevent potential attacks from across the Internet.

### 1.2 Key Features

- Supports 2.4 GHz frequency band
- Supports wireless data encryption with WPA, WPA2, Open/ shared key, and pair-wise key authentication services
- Supports QoS: WMM, WMM-SA Client mode, Ingress and Egress bandwidth control
- Supports authentication for wireless connectivity based on ESSID
- Provides MAC access control and hidden SSID function
- Support MDI/MDIX auto crossover function
- Supports NAT IP Sharing and DHCP server
- Supports WAN connection type: Static IP, PPPoE, PPTP, DHCP L2TP client
- Supports ACL, DOS, Virtual DMZ, DNS relay, UPnP, VPN-Pass through
- Supports DDNS (DynDNS, TZO)
- Supports firmware upgrade function via Web

## Chapter 2 Installing and Using Wireless Router

This chapter provides a step-by-step guide to the installation and configuration of the Wireless Router. We suggest you go over the whole chapter and then do more advanced operation.

### 2.1 Connecting this Router to your network

Steps to build up the network:

- Connect the phone line from the wall socket to the line-in port on the ADSL modem, or the coaxial cable to the line-in port on the Cable modem.
- Connect the ADSL or Cable modem to the Ethernet WAN port on the back of the Wireless Router by using the UTP cable.
- Plug-in the power adapter to the modem and turn on the power. Install the Ethernet card into the computer by referring to the User Guide that came with the card.
- Connect the computer to the Wireless Router by using standard twisted-pair Ethernet cable from the computer's Ethernet card to a 10/100Mbps Ethernet port on the back of the Wireless Router.
- Plug-in the power adapter to the Router and the other side to the wall outlet.

### 2.2 Configuring the IP address of your computer

In order to communicate with this Wireless Router, you have to configure the IP addresses of your computer to make it compatible with the device.

**Note:** The router supports DHCP server and it is enabled as default. Users that configure your IP address as “**Obtain an IP address automatically**” may skip the following IP configuration instruction.

1. The default network setting of the device:

**IP address:** 192.168.2.1

**Subnet Mask:** 255.255.255.0

**DHCP Server:** enable

2. In the following TCP/IP configuration guide, the IP address “192.168.2.2” is assumed to be your IP address if you want to specify IP addresses manually. Please **DO NOT** choose “192.168.2.1” as the IP address. For the IP address “192.168.2.1” has been set as the

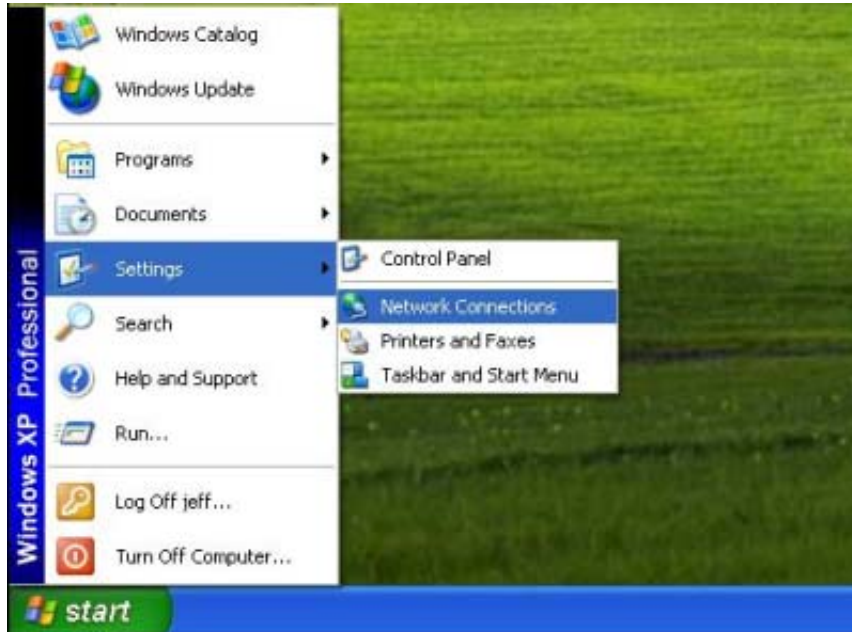


default IP for this device.

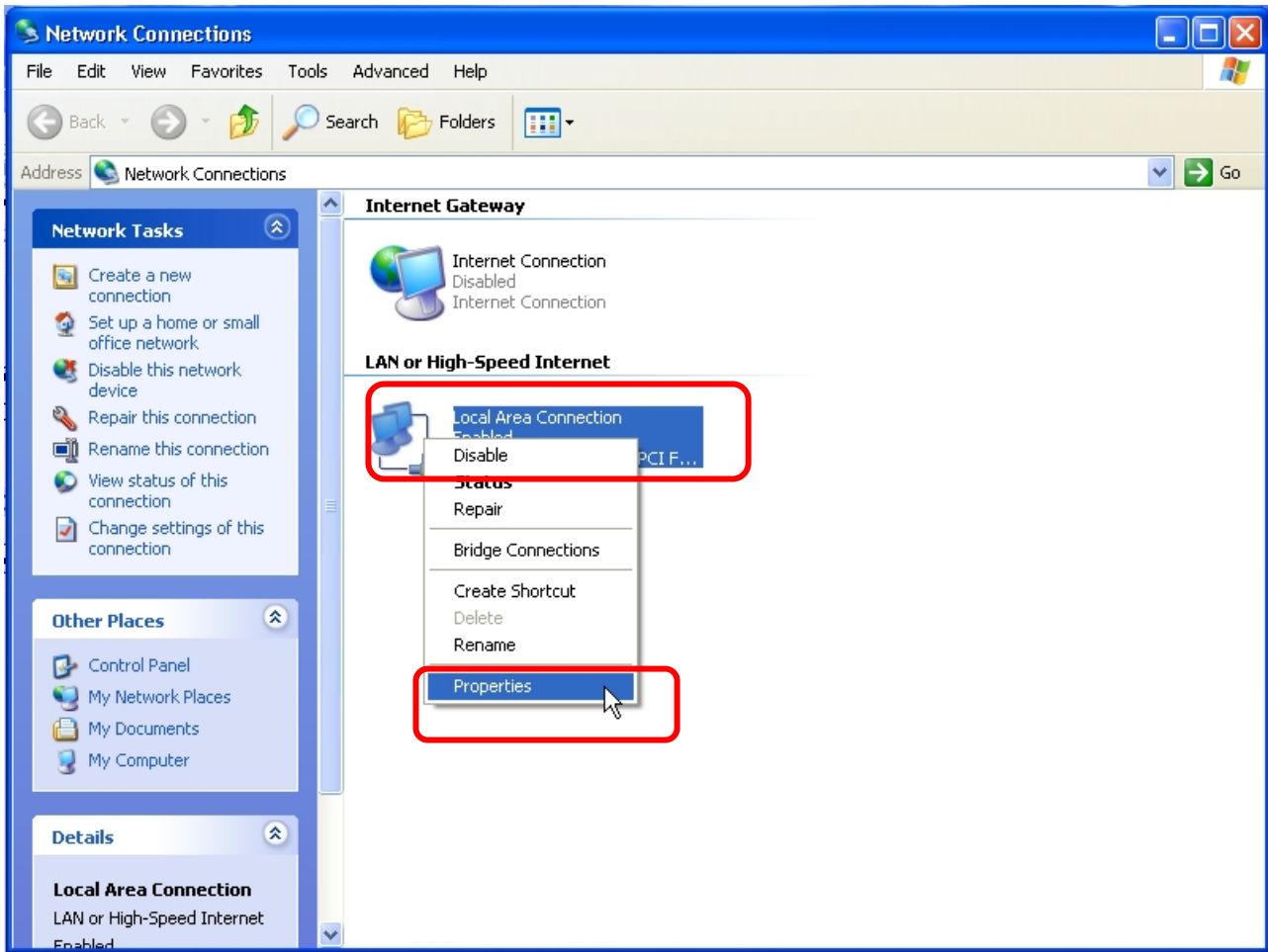
3. The following TCP/IP configuration guide uses windows XP as the presumed operation system.

#### Procedures to configure IP addresses for your computer

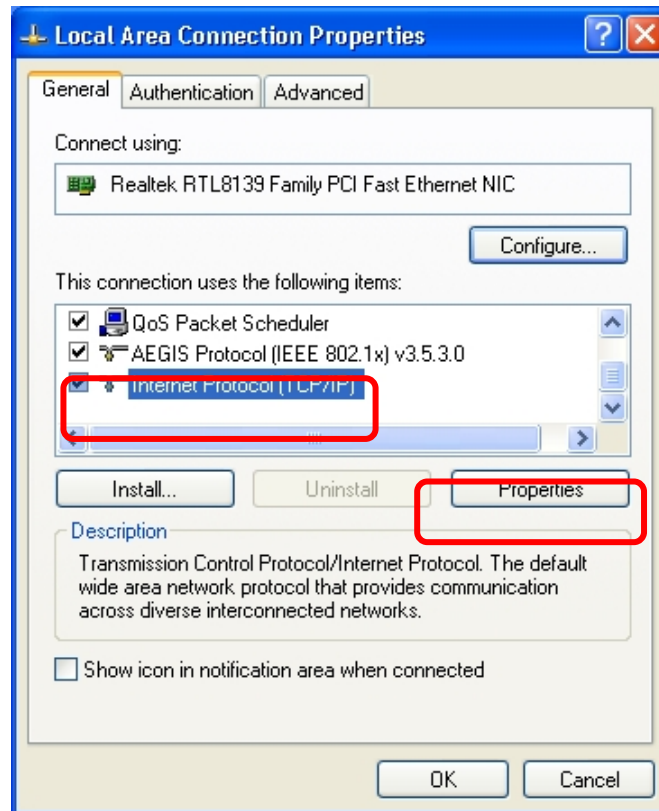
1. If you are in Classic Start menu view, click **Start > Settings > Network Connections**.  
If you are in Start menu view, click **Start > Control Panel > Network Connections**.



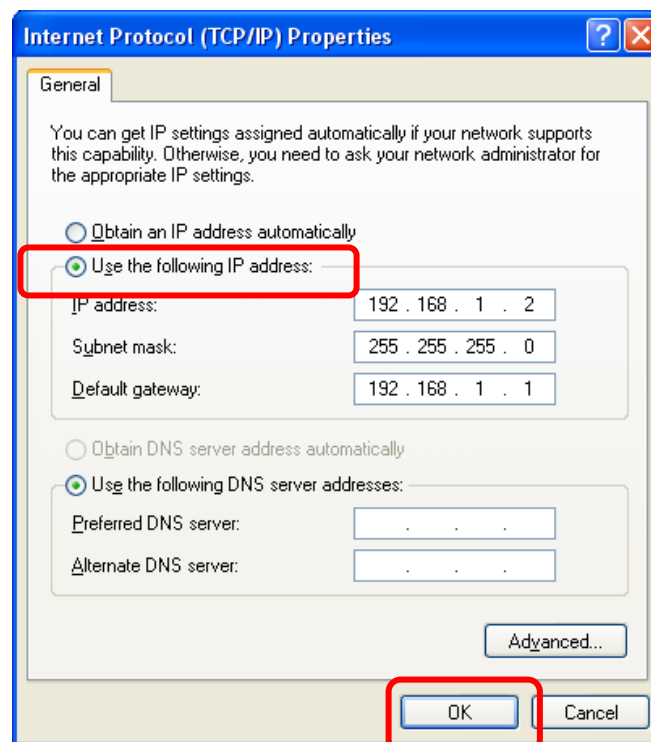
2. Right-click on **Local Area Connection** item and click on **Properties**.



3. Choose **Internet Protocol (TCP/IP)** and click **Properties**.



4. You may choose “Obtain an IP address automatically” (recommend) to get IP address automatically or choose “Use the following IP address” to specify IP addresses manually. Please click the OK button after your configuration.



## Chapter 3 Management

### 3.1 Starting the WEB-Based Management Interface

The device uses WEB as the management interface. You can use a browser to access the management interface easily. Please follow the steps listed below.

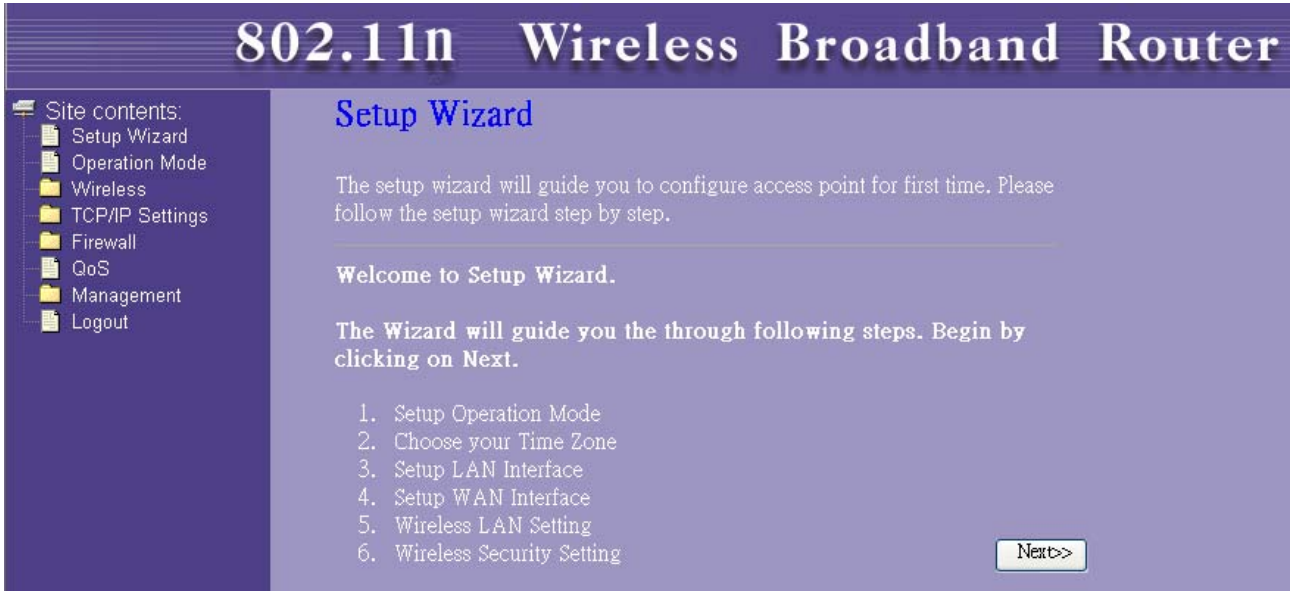
1. Open the Internet WEB browser.
2. Type **192.168.2.1** into the URL WEB address location and press Enter.
3. The Login window appears.
  - Enter **admin** in the User Name location (default value).
  - Enter **admin** in the Password location (default value).
  - Click **OK** button.



### 3.2 The Graphic User Interface

After the password authorization, the information page shows up as the home page of the Graphic User interface. You may click on each folder on left column of each page to get access to each configuration page. Please note that you should click the Save Settings button to apply your configuration to this device. You can also restore the default settings by clicking the Reset Settings button.

If you purchase **Wireless 11n 2T2R Router / Travel Router**, the Graphic User Interface as follows:



If you purchase **Wireless 11n 1T1R Router / Travel Router**, the Graphic User Interface as follows:



### 3.3 Setup Wizard

If you are using the router for the first time, please follow the procedures of the setup wizard to do a step-by-step configuration.

**Note:** The following instruction does an overall introduction to the Setup Wizard. For detail information to each item, please refer to instruction of each page.

1. To start the Setup Wizard, click the “Next” button to proceed.



2. Select your demanding operation mode and click “Next”.

## 1. Operation Mode

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

- Gateway:** In this mode, the device is supposed to connect to internet via ADSL/Cable Modem. The NAT is enabled and PCs in four LAN ports share the same IP to ISP through WAN port. The connection type can be setup in WAN page by using PPPOE, DHCP client, PPTP client, L2TP client or static IP.
- Bridge:** In this mode, all ethernet ports and wireless interface are bridged together and NAT function is disabled. All the WAN related function and firewall are not supported.
- Wireless ISP:** In this mode, all ethernet ports are bridged together and the wireless client will connect to ISP access point. The NAT is enabled and PCs in ethernet ports share the same IP to ISP through wireless LAN. You must set the wireless to client mode first and connect to the ISP AP in Site-Survey page. The connection type can be setup in WAN page by using PPPOE, DHCP client, PPTP client, L2TP client or static IP.

3. Mark the check box to enable synchronizing time by NTP server. Select the religion you live and a NTP server by clicking the drop list then click "Next".

## 2. Time Zone Setting

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

- Enable NTP client update**
- Automatically Adjust Daylight Saving**

Time Zone

Select :

(GMT+08:00)Taipei

NTP server :

192.5.41.41 - North America

4. Specify an IP address and subnet mask for connecting to the router in LAN.

### 3. LAN Interface Setup

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

IP Address:

Subnet Mask:

5. Select a WAN access type for the router to connect to Internet. Fill in the parameters that required in each blank, and then click the "Next" button. You may get those parameters from your ISP. WAN Access Type : Static IP, DHCP Client, PPPoE, PPTP, L2TP

### 4. WAN Interface Setup

This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE, PPTP or L2TP by click the item value of WAN Access type.

WAN Access Type:

- Static IP
- DHCP Client**
- PPPoE
- PPTP
- L2TP

6. Select the wireless parameters that are used for associating with this router and click "Next".



## 5. Wireless Basic Settings

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

Band:

Mode:

Network Type:

SSID:

Country:

Channel Width:

ControlSideband:

Channel Number:

Enable Mac Clone (Single Ethernet Client)

Items	Information
<b>Band</b>	2.4GHz(B),2.4GHz(G),2.4GHz(N),2.4GHz(B+G),2.4GHz(G+N), 2.4GHz(B+G+N)
<b>Mode</b>	AP, Client, WDS, AP+WDS
<b>Network Type</b>	Infrastructure, Ad-hoc
<b>Channel Width</b>	40MHz, 20MHz
<b>ControlSideband</b>	Upper, Lower
<b>Channel Number</b>	Auto,1,2,3,4,5,6,7,8,9
<b>Country</b>	This contains USA(FCC), Canada(IC), Europe(ETSI), Spain, France, Japan(MKK)

- 1.Note to US model owner: To comply with US FCC regulation, the country selection function has been completely removed from all US models. The above function is for non-US models only.
- 2.The availability of some specific channels and/or operational frequency bands are country dependent and are firmware programmed at the factory to match the intended destination. The firmware setting is not accessible by the end user.

- Click the drop list to select the encryption type for your wireless network. Fill in the parameters for the encryption type you select and click finish to complete configuration. Encryption type : None, WEP, WPA(TKIP), WPA2(AES), WPA2 Mixed

## 6. Wireless Security Setup

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

Encryption:

- None
- WEP
- WPA (TKIP)
- WPA2(AES)
- WPA2 Mixed

### 3.4 Operation Mode

To select an operation mode for this router, click on the mode that you want to perform and click the  button to execute.

## Operation Mode

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

- Gateway:** In this mode, the device is supposed to connect to internet via ADSL/Cable Modem. The NAT is enabled and PCs in LAN ports share the same IP to ISP through WAN port. The connection type can be setup in WAN page by using PPPOE, DHCP client, PPTP client , L2TP client or static IP.
- Bridge:** In this mode, all ethernet ports and wireless interface are bridged together and NAT function is disabled. All the WAN related function and firewall are not supported.
- Wireless ISP:** In this mode, all ethernet ports are bridged together and the wireless client will connect to ISP access point. The NAT is enabled and PCs in ethernet ports share the same IP to ISP through wireless LAN. You must set the wireless to client mode first and connect to the ISP AP in Site-Survey page. The connection type can be setup in WAN page by using PPPOE, DHCP client, PPTP client , L2TP client or static IP.

## 3.5 Wireless

### 3.5.1 Basic Settings

You can set up the configuration of your Wireless basic settings and monitor the Wireless Clients associate with your router.

**Disable Wireless LAN Interface**

Band: 2.4 GHz (B+G+N) ▼

Mode: AP ▼ Multiple AP

Network Type: Infrastructure ▼

SSID: Wireless-11n-Router

Channel Width: 40MHz ▼

Control Sideband: Lower ▼

Channel Number: 1 ▼

Country: USA(FCC) ▼

Broadcast SSID: Enabled ▼

WMM: Enabled ▼

Data Rate: Auto ▼

Associated Clients: Show Active Clients

**Enable Mac Clone (Single Ethernet Client)**  
 **Enable Universal Repeater Mode (Acting as AP and client simultaneously)**

SSID of Extended Interface:

Apply Changes
Reset

Items	Information
<b>Disable Wireless LAN Interface</b>	Mark the checkbox to disable interface of Wireless LAN
<b>Band</b>	To select a band for this device to match 802.11b, 802.11g, 802.11n, 802.11b/g, 802.11g/n or 802.11b/g/n. optional parameters: 2.4GHz(B),2.4GHz(G),2.4GHz(N),2.4GHz(B+G),2.4GHz(G+N), 2.4GHz(B+G+N)


<b>Mode</b>	Configure this device as AP, Client, WDS or AP+WDS. If you set this device as AP or AP+WDS mode, the <input type="button" value="Multiple AP"/> button is available for you to set up four SSID for this wireless network. Click on this button to do more configurations.
<b>Network Type</b>	<p>When you configure this device in Client mode, this drop-down list allows users to change the network type into infrastructure mode or ad-hoc mode.</p> <p><b>Ad-Hoc mode:</b> connects two computers directly without the use of a router or AP. It is also know as a peer-to-peer network.</p> <p><b>Infrastructure Mode:</b> the wireless network contains at least one wireless client and one wireless AP or router. This client connects to Internet or intranet by communicating with this wireless AP.</p>
<b>SSID</b>	Service set identifier (SSID) for the name of the wireless network.
<b>Channel Width</b>	Select to use 20MHz or 40MHz as the wireless channel frequency.
<b>Control Sideband</b>	If you have selected the channel width of 40MHz for this router, you can control this router to use the frequency for a deflection of "Upper" or "Lower."
<b>Channel Number</b>	Select a channel for the wireless network of this device.
<b>Country</b>	This contains USA(FCC), Canada(IC), Europe(ETSI), Spain, France, Japan(MKK)
<b>Broadcast SSID</b>	If you enable "Broadcast SSID", every wireless station located within the coverage of this wireless router can discover this wireless router easily. If you are building a public wireless network, enabling this feature is recommended. Disabling "Broadcast SSID" can provide better security.
<b>WMM</b>	This will enhance the data transfer performance of multimedia contents when they're being transferred over wireless network. WMM is not available in 11n mode.
<b>Data Rate</b>	The transmit limitation of data packets of this wireless router. The wireless router will use the highest possible selected transmission rate to transmit the data packets.
<b>Associated Client</b>	Click "Show Active Clients" button, then an "Active Wireless Client Table" pops up. You can see the status of all active wireless stations that are connecting to the access point.
<b>Enable MAC clone</b>	Mark the checkbox to clone the MAC address of the device. This function is only available when you set this router as Client mode. You can also manually set the MAC address in WAN setting.
<b>Enable Universal Repeater Mode</b>	Mark this checkbox to enable Universal Repeater Mode which acts this device as an AP and client simultaneously.

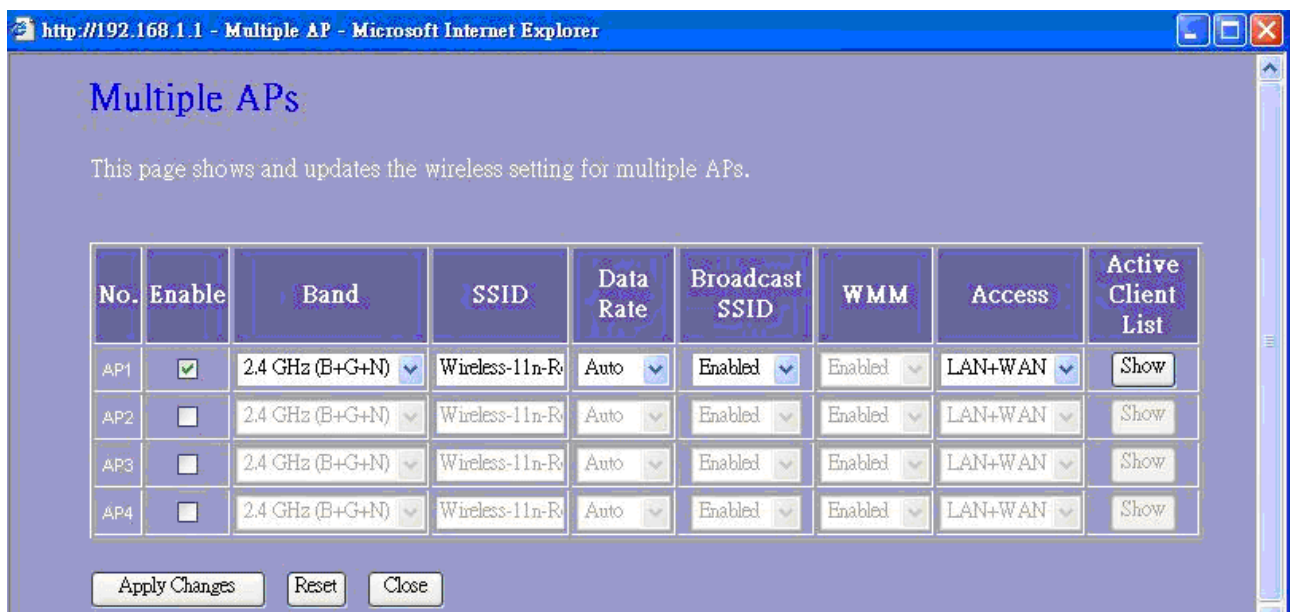
<b>SSID of Extended Interface</b>	While you enable the Universal Repeater Mode, you have to specify an SSID for the extended interface.
-----------------------------------	-------------------------------------------------------------------------------------------------------

\* Please click on the **Apply Changes** button or the **Reset** button at the bottom to save/reset the configurations.

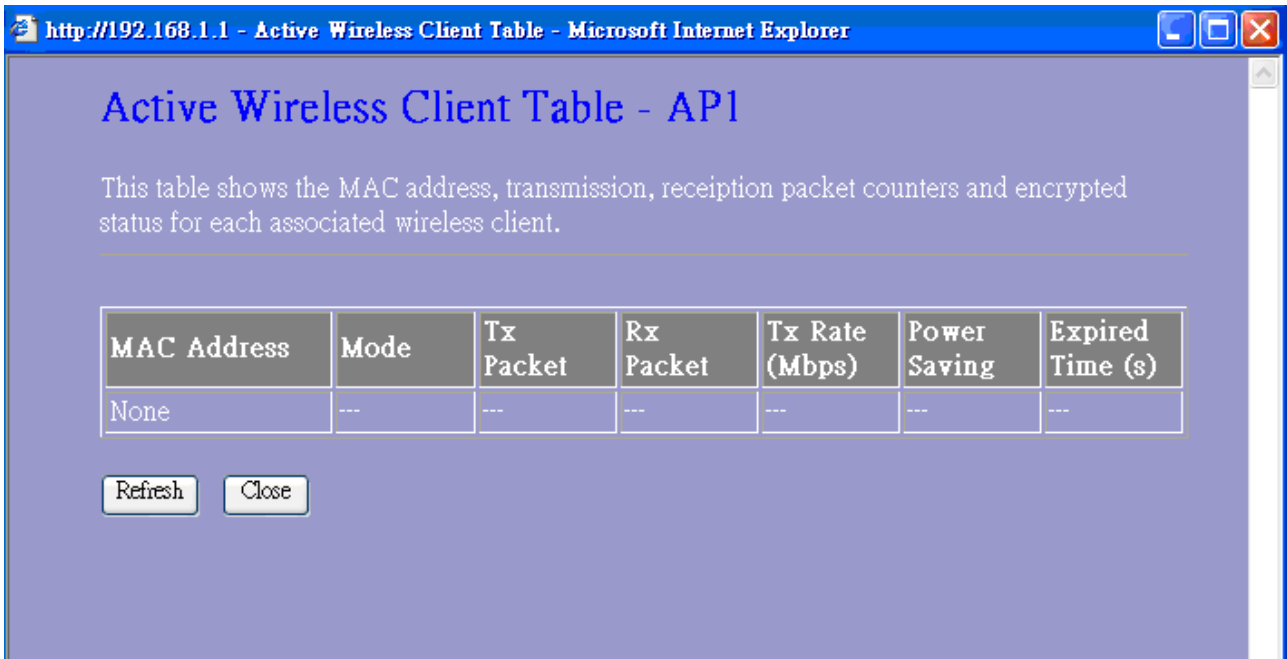
1. Note to US model owner: To comply with US FCC regulation, the country selection function has been completely removed from all US models. The above function is for non-US models only.
2. The availability of some specific channels and/or operational frequency bands are country dependent and are firmware programmed at the factory to match the intended destination. The firmware setting is not accessible by the end user.

## 1. Multiple APs

This is the window that pops up after clicking the  button.

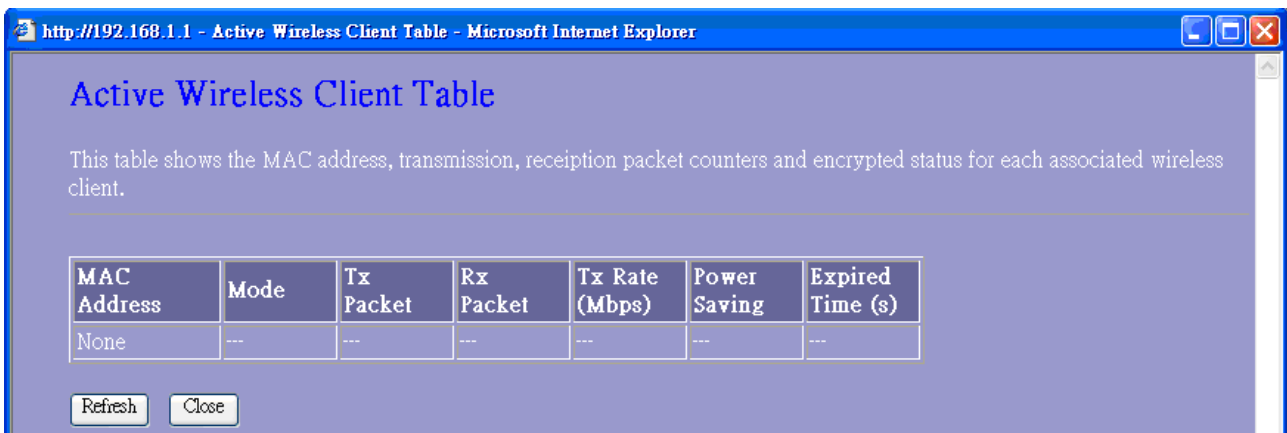


Select one of the AP, and then click the button “Show”, “Active Wireless Client Table – AP1” windows pops up.



## 2. Active Wireless Client Table

This is the window that pops up after clicking the  button.



### 3.5.2 Advanced Settings

You can set advanced wireless LAN parameters of this router. We recommend not changing these parameters unless you know what changes will be on this router.

## Wireless Advanced Settings

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

**Fragment Threshold:**  (256-2346)  
**RTS Threshold:**  (0-2347)  
**Beacon Interval:**  (20-1024 ms)  
**Preamble Type:**  Long Preamble  Short Preamble  
**IAPP:**  Enabled  Disabled  
**Protection:**  Enabled  Disabled  
**Aggregation:**  Enabled  Disabled  
**Short GI:**  Enabled  Disabled  
**WLAN Partition:**  Enabled  Disabled  
**RF Output Power:**  100%  70%  50%  35%  15%

Items	Information
<b>Fragment Threshold</b>	This value should remain at its default setting of 2346. If you experience a high packet error rate, you may slightly increase your fragmentation threshold within the value range of 0 to 2346. Setting the fragmentation threshold too low may result in poor performance.
<b>RTS Threshold</b>	Request To Send threshold. This value should remain at its default setting of 2347. If you encounter inconsistent data flow, only minor modifications to the value range between 1 and 2347 are recommended.
<b>Beacon Interval</b>	Beacons are packets sent by an access point to synchronize a wireless network. Specify a beacon interval value. Default (100ms) is recommended.
<b>Preamble Type</b>	The length of CRC blocks in the frames during the wireless communication.
<b>IAPP</b>	To enables multiple AP to communicate and pass information regarding the location of associated Stations.
<b>Protection</b>	Some 802.11g wireless adapters support 802.11g protections, which allows the adapter search for 802.11b/g singles only. Select



	“Enabled” to support protection or select “Disabled” to disable this function.
<b>Aggregation</b>	To aggregate lots of packets into a big one before transmitting packets. This can reduce control packet overhead.
<b>Short GI</b>	Indicates that the 802.11g network is using a short slot time because there are no legacy (802.11b) stations present
<b>RF Output Power</b>	Select the signal strength for the wireless network.

\* Please click on the **Apply Changes** button or the **Reset** button at the bottom to save/reset the configurations.

### 3.5.3 Security

The Security function protects your wireless network from invasion. We provide WEP and WPA encryption to secure your wireless network. Please select Disable, WEP, WPA, WPA2, and WPA-Mixed in the drop list. If you select none, any data will be transmitted without encryption and any station can access the router.

Items	Information
<b>Select SSID</b>	Please choose a SSID you have set for this router in the <a href="#">Wireless &gt; Basic Settings</a> from the drop-down list. The SSID will be shown on the wireless network for recognizing.
<b>Encryption</b>	There are 5 modes for you to select: Disable, WEP, WPA, WPA2, and WPA-Mixed. Please refer to the following description.
<b>802.1x Authentication</b>	Users that do not use this function or connecting to an open-wireless network please skip this part. Please configure the settings in accordance with the Certificated Server.

## Wireless Security Setup

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

Select SSID:

Encryption:

802.1x Authentication:

### 1. Security Mode -- WEP

## Wireless Security Setup

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

Select SSID:

Encryption:

802.1x Authentication:

Authentication:  Open System  Shared Key  Auto

Key Length:

Key Format:

Encryption Key:

Items	Information
<b>Encryption</b>	Select a security encryption mode for this router.
<b>Authentication</b>	There provide three options for selecting: Open System,

	Shared Key, Auto
<b>Key Length</b>	Select 64-bit or 128-bit as the key encryption length.
<b>Key Format</b>	Select ASCII <sup>1</sup> or Hex <sup>2</sup> to setup the key value.
<b>Encryption Key</b>	Enter the key according to the key format you select.

\* Please click on the **Apply Changes** button or the **Reset** button to save/reset the configurations.

## 2. Security Mode – WPA / WPA 2

### Wireless Security Setup

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

---

Select SSID: Root AP - Wireless-11n-Router Apply Changes Reset

---

Encryption: WPA

Authentication Mode:  Enterprise (RADIUS)  Personal (Pre-Shared Key)

WPA Cipher Suite:  TKIP  AES

Pre-Shared Key Format: Passphrase

Pre-Shared Key:

Items	Information
<b>Authentication Mode</b>	There are two items, “Enterprise (RADIUS)” and “Personal (Pre-Shared Key)”. You can select the mode by clicking the item.
<b>WPA Cipher Suite</b>	Select the WPA Cipher Suite to be TKIP or AES.
<b>Pre-Shared Key Format</b>	To decide the format, select Pass phrase or Hex in the drop list.
<b>Pre-Shared Key</b>	Enter the Pre-shared Key according to the pre-shared key format you select. This is the shared secret between AP and STA. This field must be filled with character longer than 8 and less than 64 lengths.

<sup>1</sup> ASCII (American Standard Code for Information Interchange) is a code for representing English letters as numbers from 0-127.

<sup>2</sup> Hexadecimal digits consist of the numbers 0-9 and the letters A-F.

### 3. Security Mode – WPA-Mixed

## Wireless Security Setup

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

---

Select SSID: Root AP - Wireless-11n-Router ▾ Apply Changes Reset

---

Encryption: WPA-Mixed ▾

Authentication Mode:  Enterprise (RADIUS)  Personal (Pre-Shared Key)

WPA Cipher Suite:  TKIP  AES

WPA2 Cipher Suite:  TKIP  AES

Pre-Shared Key Format: Passphrase ▾

Pre-Shared Key:

Items	Information
<b>Authentication Mode</b>	There are two items, “Enterprise (WPA-Radius)” and “Personal (Pre-Shared Key)”. You can select the mode by clicking the item.
<b>WPA / WPA2 Cipher Suite</b>	Select the WPA/WPA2 Cipher Suite to be TKIP or AES.
<b>Pre-Shared Key Format</b>	To decide the format, select Passphrase or Hex in the drop list.
<b>Pre-Shared Key</b>	Enter the Pre-shared Key according to the pre-shared key format you select. This field must be filled with character longer than 8 and less than 64 lengths.

\* Please click on the **Apply Changes** button or the **Reset** button to save/reset the configurations.

### 3.5.4 Access Control

To restrict the clients of Access authentication of Stations, set up the control list in this page.

## Wireless Access Control

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

---

Wireless Access Control Mode: Disable ▼

MAC Address:  Comment:

Apply Changes Reset

Current Access Control List:

MAC Address	Comment	Select

Delete Selected Delete All Reset

Items	Information
<b>Wireless Access Control Mode</b>	Click on the drop list to choose the access control mode. You may select "Allow listed" to allow those allowed MAC addresses or select "Deny Listed" to ban those MAC addresses from accessing to this device or select "Disable".
<b>MAC Address &amp; Comment</b>	Fill in the MAC address that you wish to control, and give a definition to it.
<b>Current Access Control list</b>	Lists the MAC Access Control Settings you have added before. Click on the list to change configuration. To Delete the station on the list, mark the check box in the select item and click the "Delete Selected". If you want to delete all stations on the list, click "Delete All" to remove all of them.

\* Please click on the **Apply Changes** button or the **Reset** button to save/reset the configurations.

### 3.5.5 WDS Settings

When you use this device as WDS or AP+WDS mode, “WDS Setting” function can be operated. Wireless Distribution System allows the router to communicate with other APs wirelessly. To make it work, you must ensure that these APs and the Router are in the same channel. Please add these APs MAC address and comment values into the WDS list. Don’t Forget to Enable the WDS by click the check box of “Enable WDS” and press “Apply Changes” button to save. To Delete the AP on the list, Click the check box in the select item and click the “Delete Selected”. If you want to delete all APs on the list, click “Delete All” to remove all of them.

### WDS Settings

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

**Enable WDS**

MAC Address:

Data Rate: Auto ▼

Comment:

Apply Changes
Reset
Set Security
Show Statistics

**Current WDS AP List:**

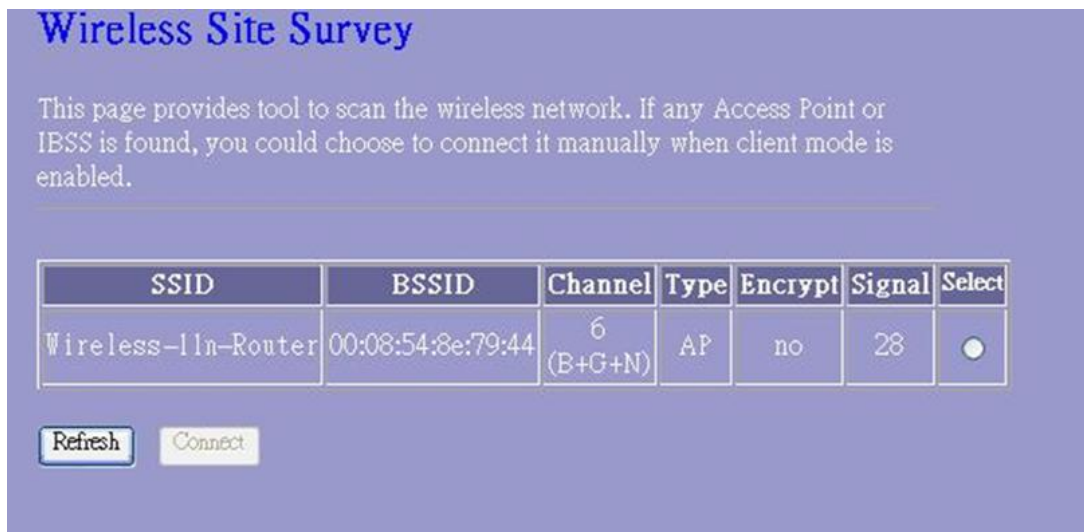
MAC Address	Tx Rate (Mbps)	Comment	Select
<div style="display: flex; justify-content: space-between; margin: 0;"> <span style="border: 1px solid #ccc; padding: 2px 10px;">Delete Selected</span> <span style="border: 1px solid #ccc; padding: 2px 10px;">Delete All</span> <span style="border: 1px solid #ccc; padding: 2px 10px;">Reset</span> </div>			

Items	Information
<b>MAC Address &amp; Comment</b>	Fill in the MAC address that you wish to control, and give a definition to it.
<b>Data Rate</b>	The transmit limitation of data packets of this wireless router. The wireless router will use the highest possible selected transmission rate to transmit the data packets.
<b>Current WDS AP List</b>	Lists the WDS Settings you have added before. Click on the list to change configuration. To Delete the station on the list, mark the check box in the select item and click the “Delete Selected”. If you want to delete all stations on the list, click

“Delete All” to remove all of them.

### 3.5.6 Site Survey

This page shows available wireless network information. When you use this device as a client station (STA), you may connect to other AP or Router. Select one of the lists in the site survey table and click on  to connect to other wireless network nearby. The  button can be used to scan nearby Router and AP again.



**Wireless Site Survey**

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

SSID	BSSID	Channel	Type	Encrypt	Signal	Select
Wireless-11n-Router	00:08:54:8e:79:44	6 (B+G+N)	AP	no	28	<input type="radio"/>

### 3.5.7 WPS Settings

The primary goal of Wi-Fi Protected Setup (Wi-Fi Simple Configuration) is to simplify the security setup and management of Wi-Fi networks. This Router supports the configuration setup using PIN configuration method or PBC configuration method through an internal or external Registrar.

## Wi-Fi Protected Setup

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

---

**Disable WPS**

WPS Status:  Configured  UnConfigured

Self-PIN Number: 08904089

Push Button Configuration:

---

Client PIN Number:

Items	Information
<b>WPS Status</b>	You cannot manually select the items here. The WPS Status will change from “UnConfigured” to “Configured” after you enable WPS function and setup a wireless security key for this device.
<b>Self-PIN Number</b>	If you use this device as a client, you can use this code when trying to connect this device to other AP by using the PIN method.
<b>Push Button Configuration</b>	Push Button Communication (PBC) method use a simple action of pushing a button on both the AP and the new STA to reach the function of easy setup WPS connection. You can simply click the <input type="button" value="Start PBC"/> button in this GUI page. After click on the button, please run the client’s WPS and push the PBC button within 2 minutes.
<b>Client PIN Number</b>	Personal Identification Number (PIN) method. Users have to fill in the PIN code of enrollee device and click on the <input type="button" value="Start PIN"/> button to make communication with other AP. After click on the button, please run the client’s WPS and push the PIN button within 2 minutes.

Please click on the **Apply Changes** button or the **Reset** button at the bottom to save/reset the configurations.

### 3.5.8 Schedule

You can configure the schedule via this page. Click “Enable Wireless Schedule”, then config days or time which you want. Wireless will start or stop at your scheduled time. Please do not forget to configure system time before enabling this feature.



## Wireless Schedule

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

Enable Wireless Schedule

Days :

Everyday  Sun  Mon  Tue  Wed  Thu  Fri  Sat

Time :

24 Hours  From  :  To  :

Apply Changes

Reset

## 3.6 TCP/IP Settings

### 3.6.1 LAN Interface Setup

To set up the configuration of LAN interface, private IP of your router LAN port and subnet mask for your LAN segment.

### 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:	<input type="text" value="192.168.1.1"/>
Subnet Mask:	<input type="text" value="255.255.255.0"/>
Default Gateway:	<input type="text" value="0.0.0.0"/>
DHCP:	<input type="button" value="Server"/> <input type="button" value="v"/>
DHCP Client Range:	<input type="text" value="192.168.1.100"/> - <input type="text" value="192.168.1.200"/> <input type="button" value="Show Client"/>
Static DHCP:	<input type="button" value="Disabled"/> <input type="button" value="v"/> <input type="button" value="Set Static DHCP"/>
Domain Name:	<input type="text"/>
802.1d Spanning Tree:	<input type="button" value="Disabled"/> <input type="button" value="v"/>
Clone MAC Address:	<input type="text" value="000000000000"/>

Items	Information
<b>IP Address</b>	The IP of your Router LAN port (default 192.168.2.1).
<b>Subnet Mask</b>	Subnet Mask of you LAN (default 255.255.255.0). All devices on the network must have the same subnet mask to communicate on the network.
<b>Default Gateway</b>	Enter the IP Address of the router in your network.
<b>DHCP</b>	DHCP stands for Dynamic Host Configuration Protocol. It is a protocol for assigning dynamic IP addresses "automatically." You can select to use this router as a DHCP client or DHCP server. To give your LAN client an IP, you have to enable "DHCP Server". If not, manual setting up your client IP is necessary when you want to use

	the router as your client's default gateway.
<b>DHCP Client Range</b>	Specify the DHCP Client IP address range (default start from 150 and end to 200). You can also click the "Show Client" button to list those connected DHCP clients.
<b>Static DHCP</b>	This function is only available when you use this router as a DHCP server. This router may automatically assign the static DHCP address to the specific clients.
<b>Domain Name</b>	(Optional) The name of your local domain.
<b>802.1d Spanning Tree</b>	To prevent from network loops and preserve the quality of bridged network
<b>Clone MAC Address</b>	<p>Your ISP may require a particular MAC address in order for you to connect to the Internet. This MAC address is the PC's MAC address that your ISP had originally connected your Internet connection to.</p> <p>MAC cloning feature allows the MAC address reported by WAN side network interface card to be set to the MAC address already registered with the ISP eliminating the need to register the new MAC address with the ISP. This feature does not change the actual MAC address on the NIC, but instead changes the MAC address reported by Wireless Router to client requests. To Change the MAC address, enter it in the text box.</p>

\* Please click on the **Apply Changes** button or the **Reset** button at the bottom to save/reset the configurations.

## 1. Active DHCP Client List

This is the window that pops up after clicking the  button. It shows the information of IP/MAC address and expire time of the DHCP clients that have connected with this device.



http://192.168.1.1 - Active DHCP Client Table - Microsoft Internet Explorer


### Active DHCP Client Table

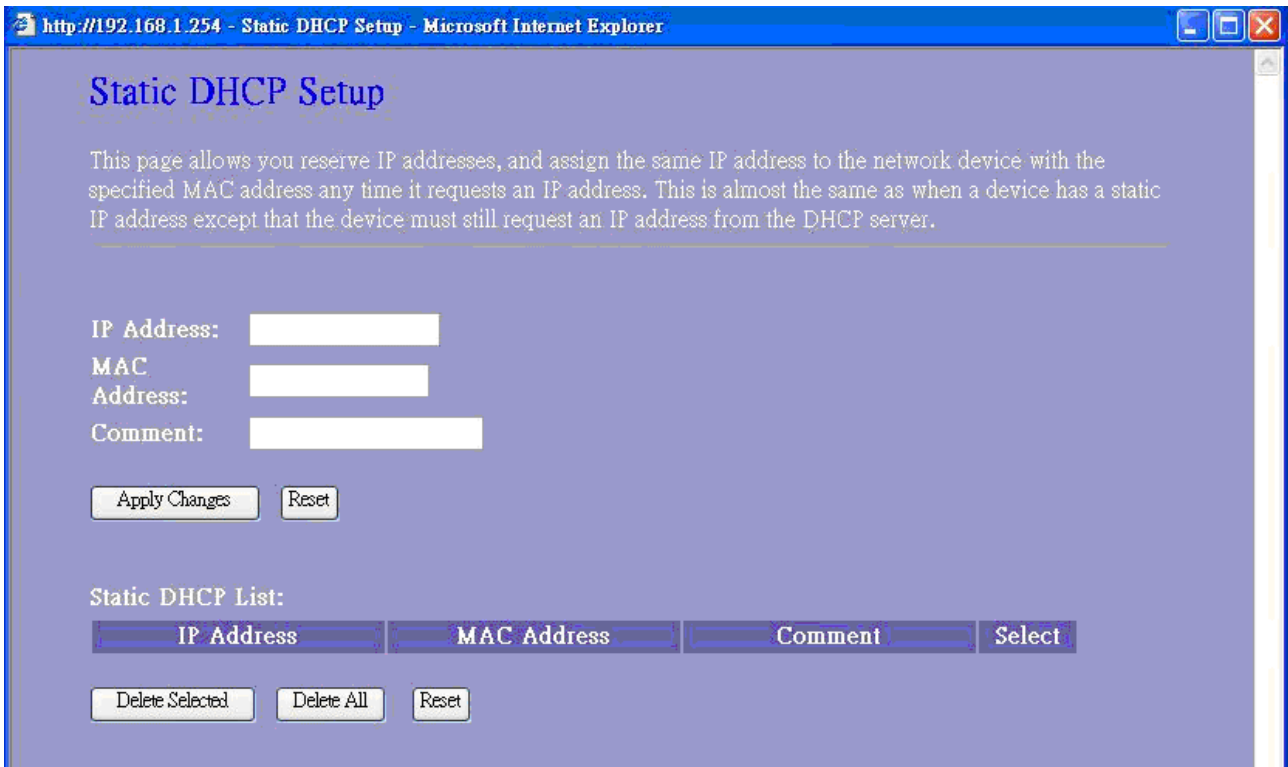
This table shows the assigned IP address, MAC address and time expired for each DHCP leased client.

IP Address	MAC Address	Time Expired(s)
None	----	----

Refresh Close

## 2. Static DHCP Setup

This is the window that pops up after clicking the  button. Click on the list to change configuration. To delete the station on the list, mark the check box in the select item and click the “Delete Selected”. If you want to delete all stations on the list, click “Delete All” to remove all of them.



http://192.168.1.254 - Static DHCP Setup - Microsoft Internet Explorer

### 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.

IP Address:

MAC Address:

Comment:

Static DHCP List:

IP Address	MAC Address	Comment	Select
------------	-------------	---------	--------

### 3.6.2 WAN Interface Setup

This page allows users to configure those parameters for connecting to Internet. You may select the Internet connection type from the “My Connection type” drop list and configure parameters for each mode. Five modes for selection: Static, DHCP, PPPoE, L2TP, and PPTP mode.

### 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:

Host Name:

MTU Size:  (1400-1492 bytes)

Attain DNS Automatically  
 Set DNS Manually

DNS 1:

DNS 2:

DNS 3:

Clone MAC Address:

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

#### 1. Static Mode (fixed IP)

Devices that are assigned the same IP address may not be visible on the network. Enter the IP address of the DNS server. The DNS server translates domain names into IP addresses.

WAN Access Type:

IP Address:

Subnet Mask:

Default Gateway:

MTU Size:  (1400-1500 bytes)

DNS 1:

DNS 2:

DNS 3:

Items	Information
<b>IP Address, Subnet Mask and Default Gateway</b>	Fill in the IP address, Subnet Mask and Default Gateway that provided by your Internet Service Provider (ISP).
<b>MTU Size</b>	<p>To Enable the Maximum Transmission Unit of Router setup. Any packet over this number will be chopped up into suitable size before sending. Larger number will enhance the transmission performance.</p> <p>Enter the MTU number in the blank to set the limitation (default 1500 bytes).</p>
<b>DNS 1~3</b>	To specify the Domain Name System (DNS). The DNS server translates domain names into IP addresses. Enter the DNS provided by your ISP in 1 <sup>st</sup> , 2 <sup>nd</sup> and 3 <sup>rd</sup> server.

\* Please click on the **Apply Changes** button or the **Reset** button at the bottom to save/reset the configurations.

## 2. DHCP (Auto Config)

WAN Access Type:

Host Name:

MTU Size:  (1400-1492 bytes)

Attain DNS Automatically

Set DNS Manually

DNS 1:

DNS 2:

DNS 3:

Items	Information
<b>Host Name</b>	The name of this device.
<b>MTU Size</b>	To Enable the Maximum Transmission Unit of Router setup. Any packet over this number will be chopped up into suitable size before sending. Larger number will enhance the transmission performance.  Enter your MTU number in the text-box to set the limitation (default 1492 bytes).
<b>Attain DNS Automatically</b>	If your DNS provide by ISP is dynamic, choose "Attain DNS automatically"

<b>Set DNS Manually</b>	To specify the Domain Name System (DNS). The DNS server translates domain names into IP addresses. Enter the DNS provided by your ISP in 1 <sup>st</sup> , 2 <sup>nd</sup> and 3 <sup>rd</sup> server.
-------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

\* Please click on the **Apply Changes** button or the **Reset** button at the bottom to save/reset the configurations.

### 3. PPPoE (ADSL)

WAN Access Type:

User Name:

Password:

Service Name:

Connection Type:

Idle Time:  (1-1000 minutes)

MTU Size:  (1360-1492 bytes)

Attain DNS Automatically  
 Set DNS Manually

DNS 1:

DNS 2:

DNS 3:

Items	Information
-------	-------------

<b>Username, Password and Service Name</b>	Fill in the User Name, password and service name that provided by your ISP.
<b>Connection Type</b>	<p>There are three connection types:</p> <p><b>“Continuous”</b>: always keep connection.</p> <p><b>“Connect on demand”</b>: bill by connection time. You can set up the idle time for the value. Specifies the number of time that elapses before the system automatically disconnects the PPPoE session.</p> <p><b>“Manual”</b>: To connect to ISP, click “Connect” manually from the WEB user interface. The WAN connection will not lose its connection even the idle time is out. If the WAN line breaks down and latter links again, the router will not auto-connect to the ISP.</p>
<b>Idle Time</b>	The value specifies the number of idle time that elapses before the system automatically disconnects the PPPoE session.
<b>MTU Size</b>	<p>To Enable the Maximum Transmission Unit of Router setup. Any packet over this number will be chopped up into suitable size before sending. Larger number will enhance the transmission performance.</p> <p>Enter your MTU number in the text-box to set the limitation (default 1452 bytes).</p>
<b>Attain DNS Automatically</b>	If your DNS provide by ISP is dynamic, choose “Attain DNS automatically
<b>Set DNS Manually</b>	To specify the Domain Name System (DNS). The DNS server translates domain names into IP addresses. Enter the DNS provided by your ISP in 1 <sup>st</sup> , 2 <sup>nd</sup> and 3 <sup>rd</sup> server.

\* Please click on the **Apply Changes** button or the **Reset** button at the bottom to save/reset the configurations.

#### 4. PPTP

Point-to-Point Tunneling Protocol (PPTP) is a method for implementing virtual private networks (VPNs).



WAN Access Type: PPTP   
 IP Address:   
 Subnet Mask:   
 Server IP Address:   
 User Name:   
 Password:   
 Connection Type: Continuous     
 Idle Time:  (1-1000 minutes)  
 MTU Size:  (1400-1460 bytes)  
 Request MPPE Encryption     Request MPPE Compression  
 Attain DNS Automatically  
 Set DNS Manually  
 DNS 1:   
 DNS 2:   
 DNS 3:

Items	Information
<b>IP address &amp; Subnet Mask</b>	Fill in IP address & Subnet Mask that match the same subnet provided by your Internet Service Provider (ISP).
<b>Username and Password</b>	Fill in Username and Password that provided by your Internet Service Provider (ISP).
<b>Idle Time</b>	The value specifies the number of idle time that elapses before the system automatically disconnects the PPTP session.
<b>MTU Size</b>	<p>To Enable the Maximum Transmission Unit of Router setup. Any packet over this number will be chopped up into suitable size before sending. Larger number will enhance the transmission performance.</p> <p>Enter the MTU number in the blank to set the limitation (default 1460 bytes).</p>
<b>Request MPPE Encryption</b>	Mark to enable the Microsoft Point-to-Point Encryption function. MPPE compresses data across PPP or VPN

	links.
<b>Request MPPC Compression</b>	Mark to enable the Microsoft Point-to-Point Compression function. MPPC can only be used in products that implement the Point to Point Protocol AND for the sole purpose of interoperating with other MPPC and Point to Point Protocol implementations.
<b>Attain DNS Automatically</b>	If your DNS provide by ISP is dynamic, choose "Attain DNS automatically"
<b>DNS 1~3</b>	To specify the Domain Name System (DNS). The DNS server translates domain names into IP addresses. Enter the DNS provided by your ISP in 1 <sup>st</sup> , 2 <sup>nd</sup> and 3 <sup>rd</sup> server.

\* Please click on the **Apply Changes** button or the **Reset** button at the bottom to save/reset the configurations.

## 5. L2TP

The Layer Two Tunneling Protocol (L2TP) provides a standard method for transporting the link layer of the Point-to-Point Protocol (PPP) between a dial-up server and a Network Access Server, using a network connection in lieu of a physical point-to-point connection.

WAN Access Type:

IP Address:

Subnet Mask:

Server IP Address:

User Name:

Password:

Connection Type:

Idle Time:  (1-1000 minutes)

MTU Size:  (1400-1460 bytes)

Attain DNS Automatically  
 Set DNS Manually

DNS 1:

DNS 2:

DNS 3:

Items	Information
<b>IP address &amp; Subnet Mask</b>	Fill in IP address & Subnet Mask that match the same subnet provided by your Internet Service Provider (ISP).
<b>Username and Password</b>	Fill in the Username and Password that provided by your Internet Service Provider (ISP).
<b>MTU Size</b>	<p>To Enable the Maximum Transmission Unit of Router setup. Any packet over this number will be chopped up into suitable size before sending. Larger number will enhance the transmission performance.</p> <p>Enter the MTU number in the blank to set the limitation (default 1460bytes).</p>
<b>Attain DNS Automatically</b>	If your DNS provide by ISP is dynamic, choose "Attain DNS automatically"
<b>DNS 1~3</b>	To specify the Domain Name System (DNS). The DNS server translates domain names into IP addresses. Enter the DNS provided by your ISP in 1 <sup>st</sup> , 2 <sup>nd</sup> and 3 <sup>rd</sup> server.

## 6. Common configurations for WAN interface

Clone MAC Address:

- 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

There are some settings are able to be configured on each WAN access types:

Items	Information
-------	-------------

<p><b>Clone MAC Address</b></p>	<p>When ISP use MAC address authentication (with DHCP), then the MAC address of the Ethernet card attached to your Cable modem must be registered with the ISP before connecting to the WAN (Internet). If the Ethernet card is changed, the new MAC address must be registered with the ISP.</p> <p>MAC cloning feature allows the MAC address reported by WAN side network interface card to be set to the MAC address already registered with the ISP eliminating the need to register the new MAC address with the ISP. This feature does not change the actual MAC address on the NIC, but instead changes the MAC address reported by Wireless Router to client requests. To Change the MAC address, enter it in the text box.</p>
<p><b>Enable Web Server Access on WAN from port</b></p>	<p>To Enable the user to access this Router with WAN port IP address from Internet</p>
<p><b>Enable IPsec pass through on VPN connection</b></p>	<p>Mark the check box to enable IPsec pass through on VPN connection and clear the checkbox to disable.</p>
<p><b>Enable PPTP pass through on VPN connection</b></p>	<p>Mark the check box to enable PPTP pass through on VPN connection and clear the checkbox to disable.</p>
<p><b>Enable L2TP pass through on VPN connection</b></p>	<p>Mark the check box to enable L2TP pass through on VPN connection and clear the checkbox to disable.</p>

\* Please click on the **Apply Changes** button or the **Reset** button at the bottom to save/reset the configurations.

## 3.7 Firewall Settings

### 3.7.1 Port Filter

The firewall could not only obstruct outside intruders from intruding your system, but also restricting the LAN users. Port filter restricts certain type of data packets from your LAN to Internet through the router.

## 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:  Comment:

Current Filter Table:

Port Range	Protocol	Comment	Select
------------	----------	---------	--------

Items	Information
<b>Enable Port Filtering</b>	Mark to enable the configuration, and clear to disable.
<b>Port Range</b>	Fill in the port range that you wish to filter. The valid numbers are 1~65535.
<b>Protocol</b>	Select the protocol type of TCP, UDP or Both.
<b>Comment</b>	Input any text to describe this mapping
<b>Current Filter Table</b>	Lists the Port Filter Settings you have added before. To delete the settings on the list, click the check box in the select item and click the "Delete Selected". If you want to delete all entries on the list, click "Delete All" to remove all of them.

\* Please click on the **Apply Changes** button or the **Reset** button at the bottom to save/reset the configurations.

### 3.7.2 IP Filter

The Wireless Router could filter the outgoing packets for security or management consideration.

## 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**

Local IP Address:  Protocol:  Comment:






Current Filter Table:

Local IP Address	Protocol	Comment	Select
------------------	----------	---------	--------

Items	Information
<b>Enable IP Filtering</b>	Mark to enable the configuration, and clear to disable.
<b>Local IP Address</b>	Fill in the IP address that you wish to filter.
<b>Protocol</b>	Select the protocol type of "TCP", "UDP" or both.
<b>Comment</b>	Input any text to describe this mapping,
<b>Current Filter Table</b>	Lists the IP Filter Settings you have added before. To delete the settings on the list, click the check box in the select item and click the "Delete Selected". If you want to delete all entries on the list, click "Delete All" to remove all of them.

\* Please click on the **Apply Changes** button or the **Reset** button at the bottom to save/reset the configurations.

### 3.7.3 MAC Filter

The Wireless Router could filter the outgoing packets for security or management consideration.

## 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:

**Current Filter Table:**

MAC Address	Comment	Select

Items	Information
<b>Enable MAC Filtering</b>	Mark to enable the configuration, and clear to disable.
<b>MAC Address</b>	Fill in the MAC address that you wish to filter.
<b>Comment</b>	Input any text to describe this mapping.
<b>Current Filter Table</b>	Lists the MAC Filter Settings you have added before. To delete the settings on the list, click the check box in the select item and click the "Delete Selected". If you want to delete all entries on the list, click "Delete All" to remove all of them.

Please click on the **Apply Changes** button or the **Reset** button at the bottom to save/reset the configurations.

### 3.7.4 Port Forwarding

The Port Forwarding allows you to re-direct a particular range of service port numbers (from the Internet/WAN Ports) to a particular LAN IP address.

## 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:

Both  
Both  
 TCP  
 UDP

**Current Port Forwarding Table:**

Local IP Address	Protocol	Port Range	Comment	Select

Items	Information
<b>Enable Port Forwarding</b>	Mark to enable the configuration, and clear to disable.
<b>IP Address</b>	Fill in the IP address that you wish to forward.
<b>Protocol</b>	Select the protocol type of TCP, UDP or Both.
<b>Port Range</b>	Fill in the port range that you wish to forward. The valid numbers are 1~65535.
<b>Comment</b>	Input any text to describe this mapping.
<b>Current Port Forwarding Table</b>	Lists the Port Forward Settings you have added before. To delete the settings on the list, click the check box in the select item and click the "Delete Selected". If you want to delete all entries on the list, click "Delete All" to remove all of them.

Please click on the **Apply Changes** button or the **Reset** button at the bottom to save/reset the configurations.



### 3.7.5 URL Filter

The URL Filter allows users to prevent certain URL from accessing by users in LAN. This filter will block those URLs that contain certain keywords.

## 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:

**Current Filter Table:**

URL Address	Select


Items	Information
<b>Enable URL Filtering</b>	Mark to enable the configuration, and clear to disable.
<b>URL Address</b>	Fill in the URL address that you wish to filter.
<b>Current Filter Table</b>	Lists the URL Filter Settings you have added before. To delete the settings on the list, click the check box in the select item and click the "Delete Selected". If you want to delete all entries on the list, click "Delete All" to remove all of them.

\* Please click on the **Apply Changes** button or the **Reset** button at the bottom to save/reset the configurations.

### 3.7.6 DMZ

To configure it, mark to enable virtual DMZ and then enter the Host IP (private IP address) and

click  to enact the setting.



**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:

### 3.8 QoS

The QoS (Quality of Service) Settings page provides different priority to different users.

**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):

**QoS Rule Setting:**  
 Address Type:  IP  MAC  
 Local IP Address:  -   
 MAC Address:   
 Mode:   
 Bandwidth (Kbps):   
 Comment:

Current QoS Rules Table:

Local IP Address	MAC Address	Mode	Bandwidth	Comment	Select
<input type="button" value="Delete Selected"/> <input type="button" value="Delete All"/> <input type="button" value="Reset"/>					

### 3.9 Management

#### 3.9.1 Status

This information page shows the current settings of this device. You could check if the parameters match your configuration.

System	
Uptime	0day:0h:27m:7s
Firmware Version	v1.3
Build Time	Thu Apr 30 16:45:15 CST 2009
Wireless Configuration	
Mode	Infrastructure Client
Band	2.4 GHz (B+G+N)
SSID	Wireless-11n-Router
Channel Number	8
Encryption	Disabled
BSSID	00:00:00:00:00:00
State	Scanning
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:b1
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:b9

### 3.9.2 Statistics

This page allows users to get information of data transferring condition, and monitor the status and performance of this router including receiving and sending packets. To see the latest report,

click  button.

## Statistics

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

Ethernet LAN	<i>Sent Packets</i>	267
	<i>Received Packets</i>	209
Ethernet WAN	<i>Sent Packets</i>	57
	<i>Received Packets</i>	0

Refresh

### 3.9.3 DDNS Settings

DDNS (Dynamic Domain Name Server) service allows users to connect to this device via a fixed and easy-to-remember hostname. This router supports DDNS service of following service providers:

DynDNS (<http://www.dyndns.org>), TZO (<http://www.tzo.com>)

Please go to one of DDNS service provider's web page listed above, and get a free DDNS account by the instructions given on their web page.

## Dynamic DNS Setting

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

Enable DDNS

Service Provider :  

Domain Name :

User Name/Email:

Password/Key:

*Note:*

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

Items	Information
<b>Service Provider</b>	The website that provides DDNS service. Please select from the drop-down list.
<b>Domain Name</b>	The hostname that you have applied for the device.
<b>User Name/Email</b>	DDNS login account. For DynDNS users, please fill in your user name; for TZO users, please fill in your email address.
<b>Password/Key</b>	The password of your DDNS service account.

\* Please click on the **Apply Changes** button or the **Reset** button at the bottom to save/reset the configurations.

### 3.9.4 Time Zone Setting

This page allows users to configure the time of the router. To specify manually, fill in the blanks in "Current Time" and click the "Apply Change" button. To synchronize time from a timeserver, please mark the "Enable NTP client update" checkbox, select a NTP server from the drop list or manually enter a NTP server. Click the "Apply Change" button after your configuration.

## Time Zone Setting

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

Current Time : Yr  Mon  Day  Hr  Mn  Sec

Time Zone  
Select :

Enable NTP client update

Automatically Adjust Daylight Saving

NTP server :

(Manual IP Setting)

### 3.9.5 Denial-of-Service

A DoS (Denial of Service) attack attempt to disrupt the network and information system by sending abnormal packets to overload your Internet connection. DoS protect function helps to detect and block those malevolent DoS attack. It is strongly recommended that this setting be left enabled. Please mark to enable the DoS protection function. Manually adjust the value of packet threshold

and click  to enact the setting.

## Denial of Service

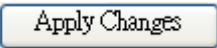
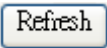

A "denial-of-service" (DoS) attack is characterized by an explicit attempt by hackers to prevent legitimate users of a service from using that service.


- Enable DoS Prevention**
    - Whole System Flood: SYN  Packets/Second
    - Whole System Flood: FIN  Packets/Second
    - Whole System Flood: UDP  Packets/Second
    - Whole System Flood: ICMP  Packets/Second
    - Per-Source IP Flood: SYN  Packets/Second
    - Per-Source IP Flood: FIN  Packets/Second
    - Per-Source IP Flood: UDP  Packets/Second
    - Per-Source IP Flood: ICMP  Packets/Second
    - TCP/UDP PortScan  Sensitivity
    - ICMP Smurf
    - IP Land
    - IP Spoof
    - IP TearDrop
    - PingOfDeath
    - TCP Scan
    - TCP SynWithData
    - UDP Bomb
    - UDP EchoChargen
- 
- Enable Source IP Blocking  Block time (sec)



### 3.9.6 Log

This System Log page shows the information of the current activities on the router. To enable system log function:

1. Mark the “Enable Log” checkbox.
2. To see all information of the system, select the “system all” checkbox.  
To see wireless information only, select the “wireless” checkbox.  
To send the log information to a certain note, select the “Enable Remote Log” checkbox and fill in the IP address in the “Log Server IP Address” box.
3. Click the  button to activate. You could also click the  button to refresh the log information or click the  button to clean the log table.



**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:



### 3.9.7 Upgrade Firmware

Sometimes a new firmware may be issued to upgrade the system of this device. You could upgrade the firmware you got in this page. To upgrade the firmware, please click on the

button, locate the firmware in your computer and then click the  button to execute.



The screenshot shows a web page titled "Upgrade Firmware" with a purple background. The text reads: "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." Below the text, there is a "Select File:" label, a text input field, and a "Browse..." button. At the bottom, there are two buttons: "Upload" and "Reset".

### 3.9.8 Save/Reload Setting

The Save/Reload Setting page allows users to backup and download the configuration status of the device or restore the factory default configuration.

## Save/Reload Settings

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

Save Settings to File:

Load Settings from File:

Reset Settings to Default:

Items	Information
<b>Save Settings to File</b>	Click on the <input type="button" value="Save..."/> button to save the currently configure settings.
<b>Load Settings from File</b>	Click <input type="button" value="Browse..."/> to select the file that you save, and then click <input type="button" value="Upload"/> to start the process. Please wait for it to complete.
<b>Reset Settings to Default</b>	Click <input type="button" value="Reset"/> to start the process and it will be completed till the status LED starts blinking.

### 3.9.9 Password

To set up the Administrator Account information, enter the Username, New password, and reenter the password on the text box. Don't forget to click the  to save the configuration.

## 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:

Apply Changes

Reset