# 802.11n/b/g High Power Router with Passive PoE

User's Manual

# Federal Communication Commission

## Interference Statement

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 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 the receiver is needed.

□ Consult the dealer or an experienced radio/TV technician for help.

Warning: Changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user authority to operate the 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.

The user’s manual or instruction manual for an intentional or unintentional radiator shall caution the user that changes or modifications not expressly approved by the party responsible for compliance could void the user’s authority to operate the equipment.

For product available in the USA/Canada market, only channel 1~11 can be operated. Selection of other channels is not possible.

**CAUTION:**

1. To comply with FCC RF exposure compliance requirements, a separation distance of at least 20 cm must be maintained between the antenna of this device and all persons.
2. This Transmitter must not be co-located or operating in conjunction with any other antenna or transmitter

# Table of Content

# Chapter 1: Introduction

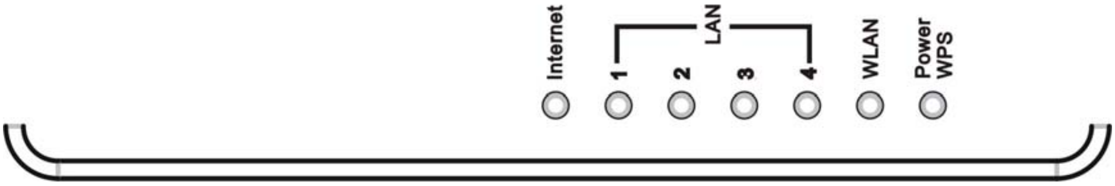
The Router is a draft 802.11n/b/g compliant Wireless Broadband Router with 4-port Fast Ethernet Switch. With the advanced MIMO technology, it can support the data transmission rate 6 times more (up to 300Mbps) and the coverage 3 times more than IEEE 802.11b/g devices. The Router enables your whole network sharing a high-speed cable or DSL Internet connection. The incredible speed of the Router makes it ideal for media-centric applications like streaming video, gaming, and Voice over IP technology, ensure optimum performance and maximum coverage with the external antennas. With the Router, you can share a high-speed Internet connection, files, printers, and multi-player games at incredible speeds, without the hassle of stringing wires. The Router offers easy configuration for your wireless network in the home and presents wireless network to you home of high functionality, security, and flexibility.

## Features

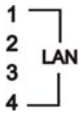
- Support the IEEE 802.11n/b/g standard, high speed date rate up to 300Mbps.
- Support WPS (Wi-Fi Protected Setup) button.
- High security with build-in Security: WEP 64/128, WPA, WPA2, 802.1x and 802.11i
- Support Gateway, AP, WDS (Bridge + Repeater) and Client modes.
- Advanced Quality of Service (QoS) - 802.11e, WMM
- Easy configuration for home user setup.

## Physical Details

### Front LEDs

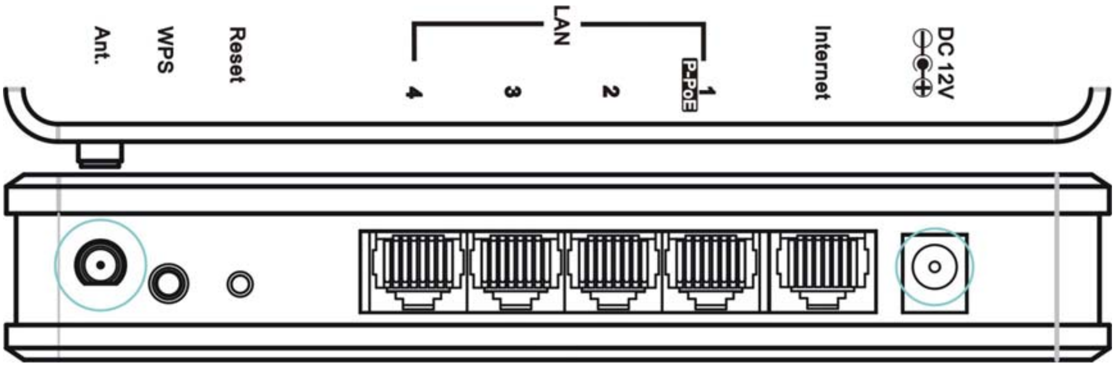


**LED Behavior**

| LED | Printed | Color | Behavior | Indication |
|---|---|---|---|---|
| **Internet** | **Internet** | Green | ON | Internet link / active |
| | | | OFF | Internet function off |
| | | | Blinking | Internet traffic transmitting |
| **LAN** |  | Green | OFF | LAN function off |
| | | | ON | LAN link / active |
| | | | Blinking | LAN traffic transmitting |

| | | | | |
|---|---|---|---|---|
| **Wireless LAN** | **WLAN** | Green | OFF | WLAN off |
| | | | ON | WLAN link / active |
| | | | Blinking | WLAN traffic transmitting |
| **Power WPS** | **Power WPS** | Green | ON | Power on |
| | | | OFF | Power off |
| | | | Blinking | WPS is enabled to make a connection |

# Rear Panel



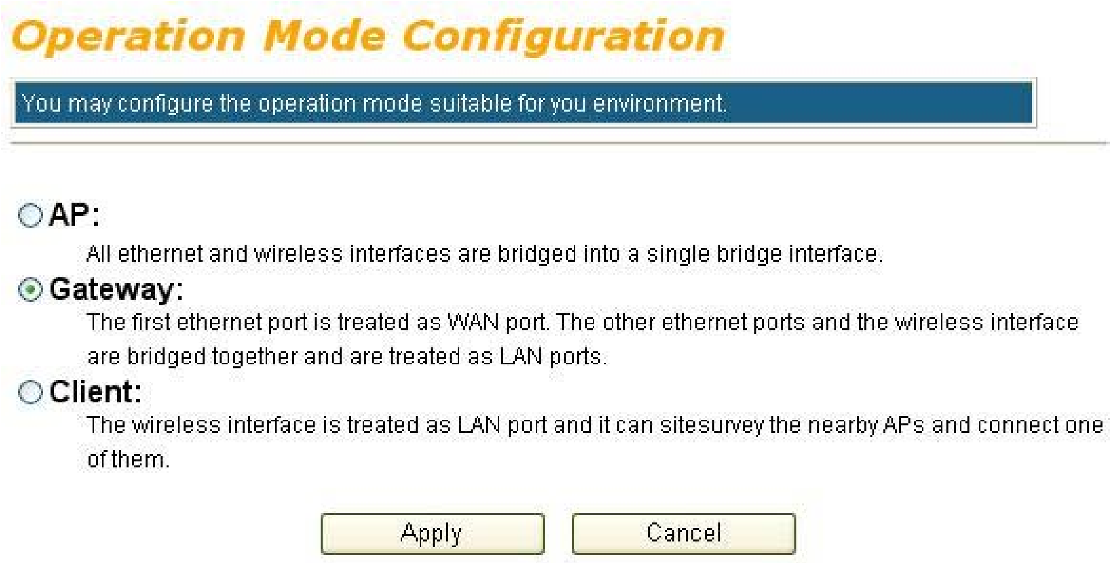
| **Ports and buttons** | |
|---|---|
| **Ant.** | Install the appending antenna here. |
| **WPS** | To enable the WPS function via web configuration (Go to **Wireless Settings> WPS**), then press the physical WPS button on the Wireless Router once, then the LED will start to flash. Please make a connection with other WPS supported device within 2 minutes. |
| **Reset** | Keep on pressing the Reset button more than 3 seconds, the Wireless Router will set all setting back to factory default values. |
| **LAN  1-4** | Use standard LAN cables (RJ45 connectors) to connect your PCs to this port. If required, any port can be connected to another hub. Any LAN port will automatically function as an "Uplink" port when necessary. |
| **Internet** | Connect the ADSL or Cable Modem here with RJ45 cable. If your modem came with a cable, use the supplied cable, otherwise, use a standard LAN cable (RJ45 connectors). |
| **DC 12V** | Connect the supplied power adapter here. |

# Chapter 2: About Operation Modes

This device provides operational applications with AP, Gateway and Client (Infrastructure) modes, which are mutually exclusive.

If you want to change the settings in order to perform more advanced configuration or even change the mode of operation, you can select the mode you desired by the manufacturer as described in the following sections.

The default setting mode is Gateway mode.



Operation Mode Configuration

You may configure the operation mode suitable for you environment.

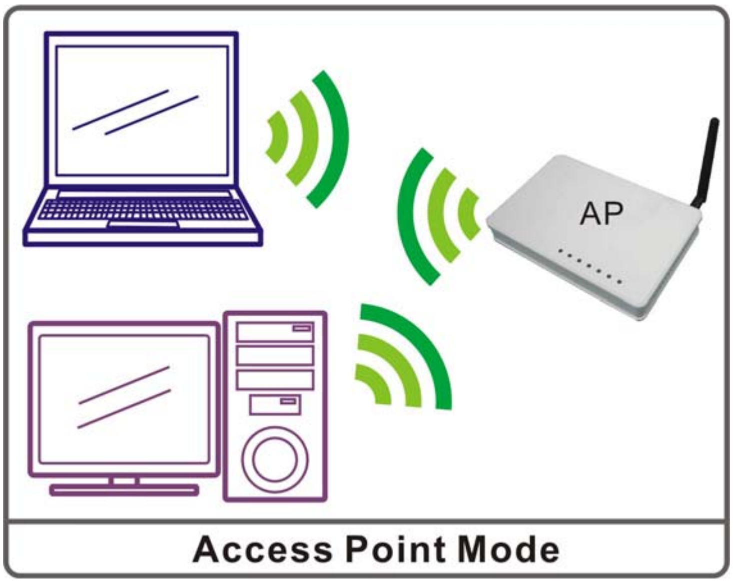
○ AP:
All ethernet and wireless interfaces are bridged into a single bridge interface.

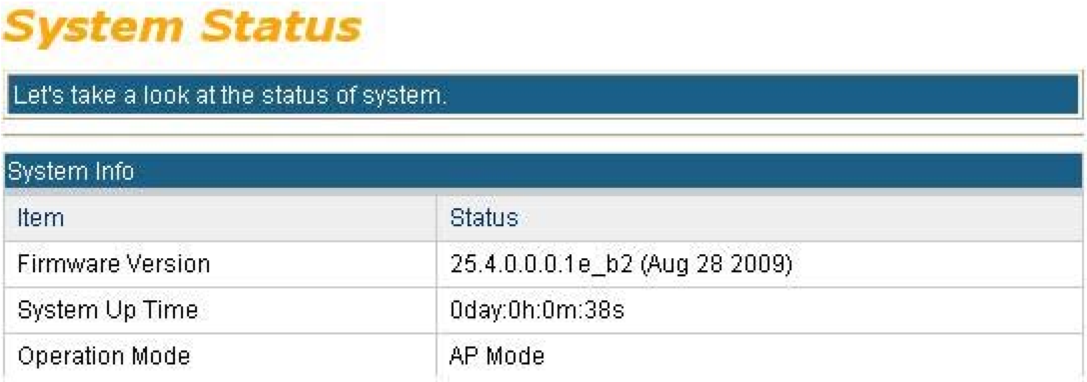
● Gateway:
The first ethernet port is treated as WAN port. The other ethernet ports and the wireless interface are bridged together and are treated as LAN ports.

○ Client:
The wireless interface is treated as LAN port and it can sitesurvey the nearby APs and connect one of them.

## Access Point Mode

When acting as an Access Point (AP), this device connects all the stations (PC/notebook with wireless network adapter) to a wireless network. All stations can have the Internet access if only the Access Point has the Internet connection.





System Status

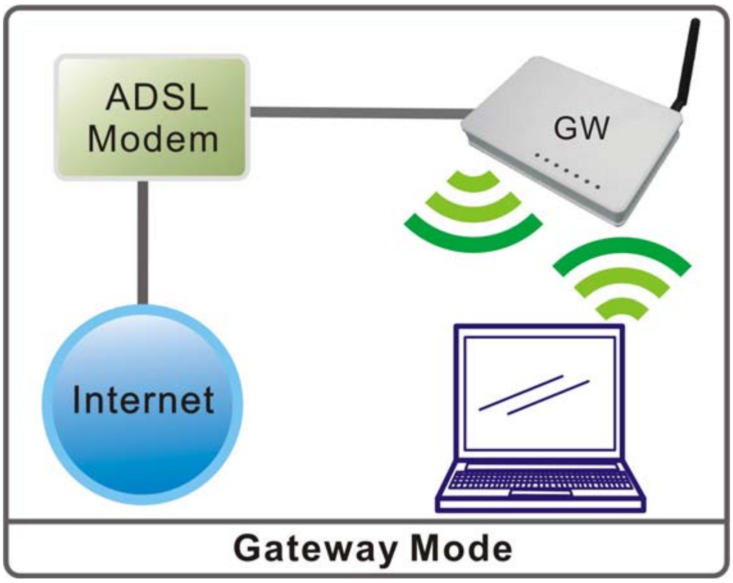
Let's take a look at the status of system.

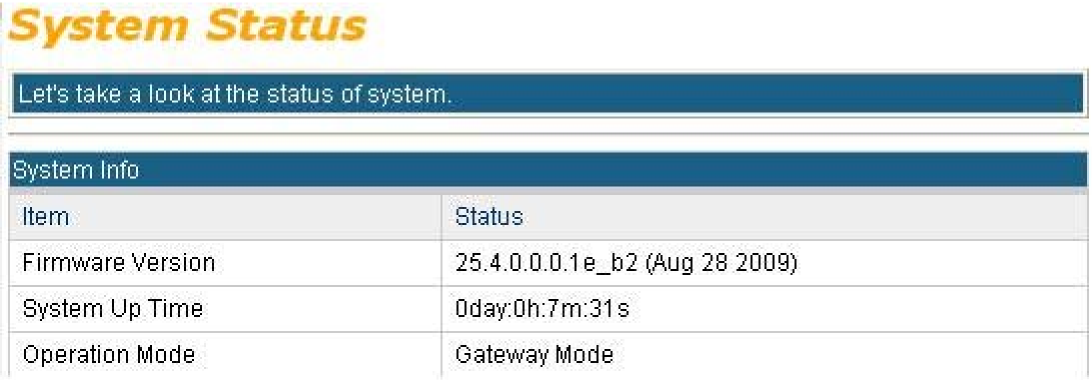
System Info

| Item | Status |
|---|---|
| Firmware Version | 25.4.0.0.0.1e_b2 (Aug 28 2009) |
| System Up Time | 0day:0h:0m:38s |
| Operation Mode | AP Mode |

# Gateway Mode

When Gateway (GW) mode is selected, the device will enter gateway mode. And the wireless connection will be set up from a point-to-point local LAN into a point-to-multipoint WAN.





System Status

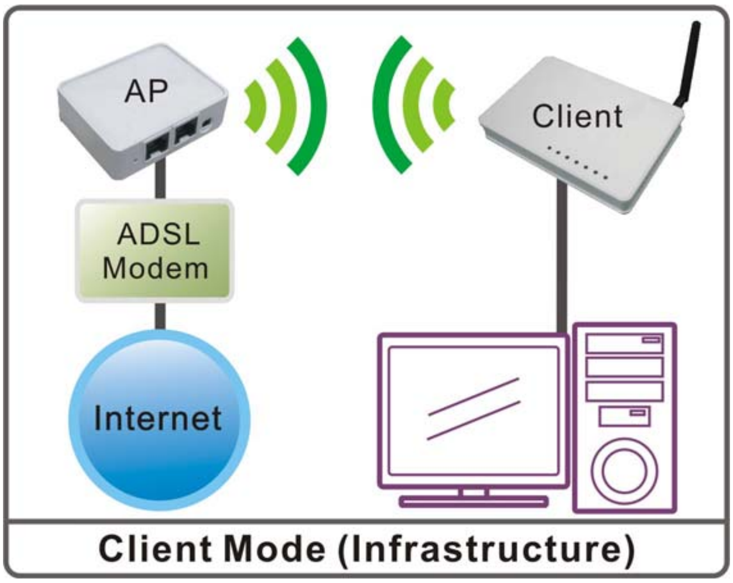
Let's take a look at the status of system.

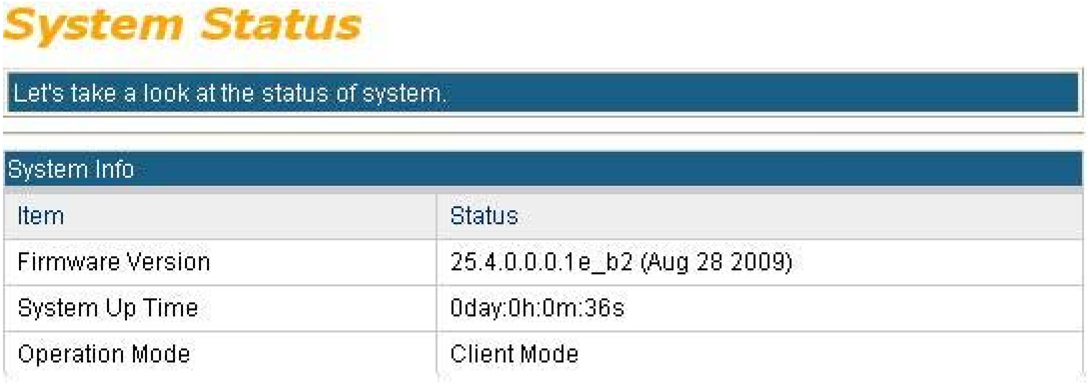
System Info

| Item | Status |
|---|---|
| Firmware Version | 25.4.0.0.0.1e_b2 (Aug 28 2009) |
| System Up Time | 0day:0h:7m:31s |
| Operation Mode | Gateway Mode |

# Client Mode

If set to Client (Infrastructure) mode, a device connects to each other through an access point or a base station (gateway or router.) This device can work like a wireless station when it’s connected to a computer directly, so that the computer can send packets from wired end to wireless interface.





## System Status

Let's take a look at the status of system.

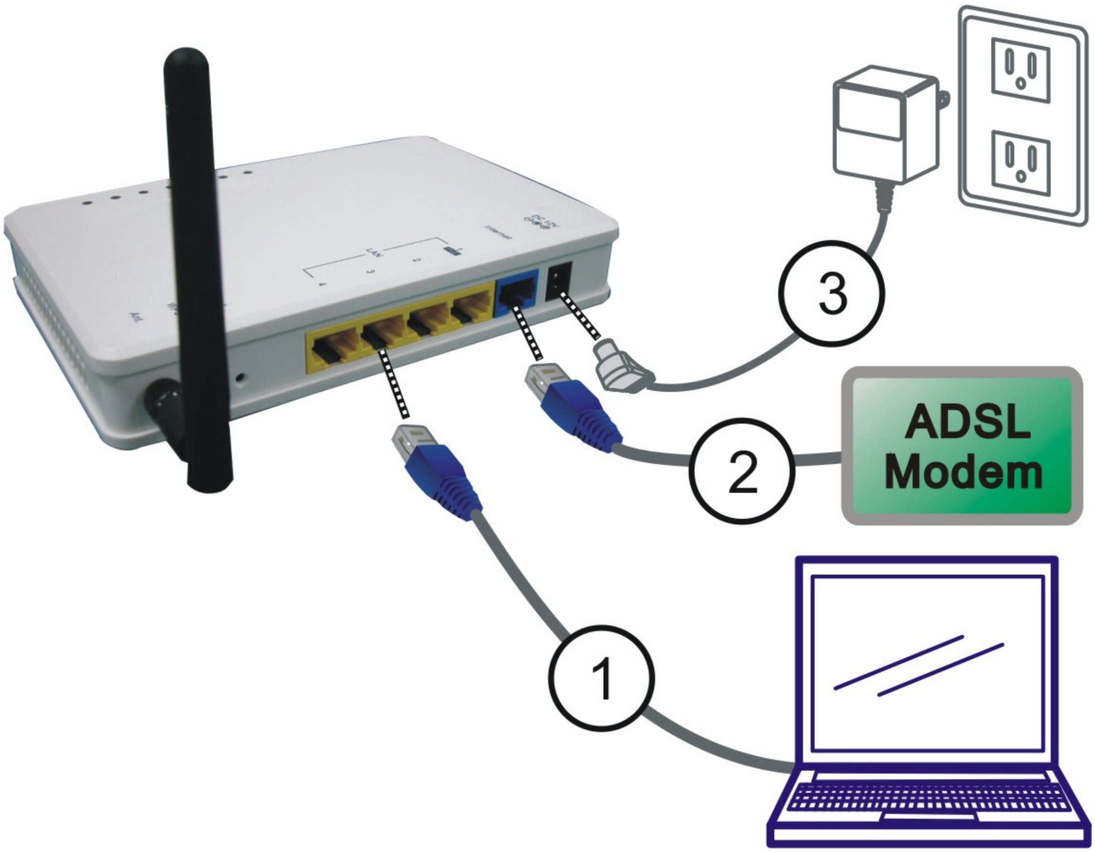
System Info

| Item | Status |
|---|---|
| Firmware Version | 25.4.0.0.0.1e_b2 (Aug 28 2009) |
| System Up Time | 0day:0h:0m:36s |
| Operation Mode | Client Mode |

# Chapter 3: Configuration

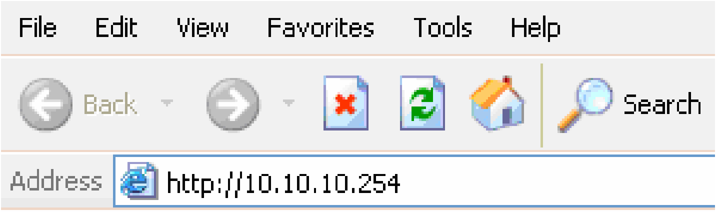
## Hardware Connection

1. Connect one end of the Ethernet cable to the LAN port of the Wireless Router,  another end to your PC or notebook.
2. Then, connect another Ethernet cable one end to the  Internet port of the Wireless Router, the other end to the ADSL or cable modem.
3. Finally, connect the Wireless Router with a power to an outlet.



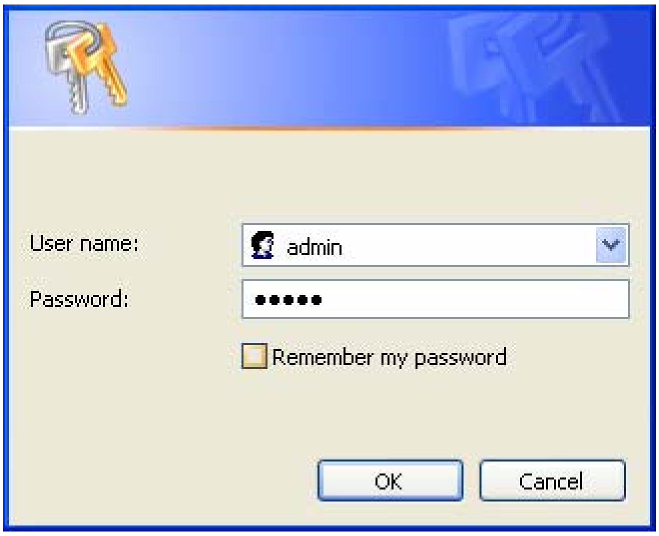
# Login

1. Start your computer and make sure the connection by an Ethernet cable between your computer and the Wireless Router.
2. Start your Web Browser.
3. In the *Address* box, enter the IP address of the Wireless Router, as in this example, which uses the Wireless Router's default IP address: http://10.10.10.254



Address http://10.10.10.254

4. After connected successfully, the following screen will show up. Simply enter the username "**admin**" and password “**admin**” to login.



User name: admin

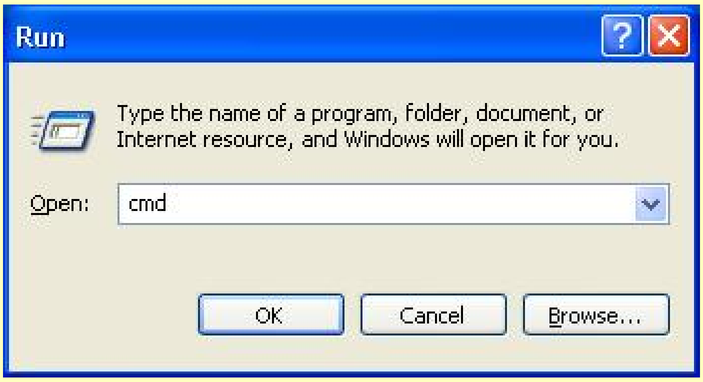
Password: ●●●●●

□ Remember my password

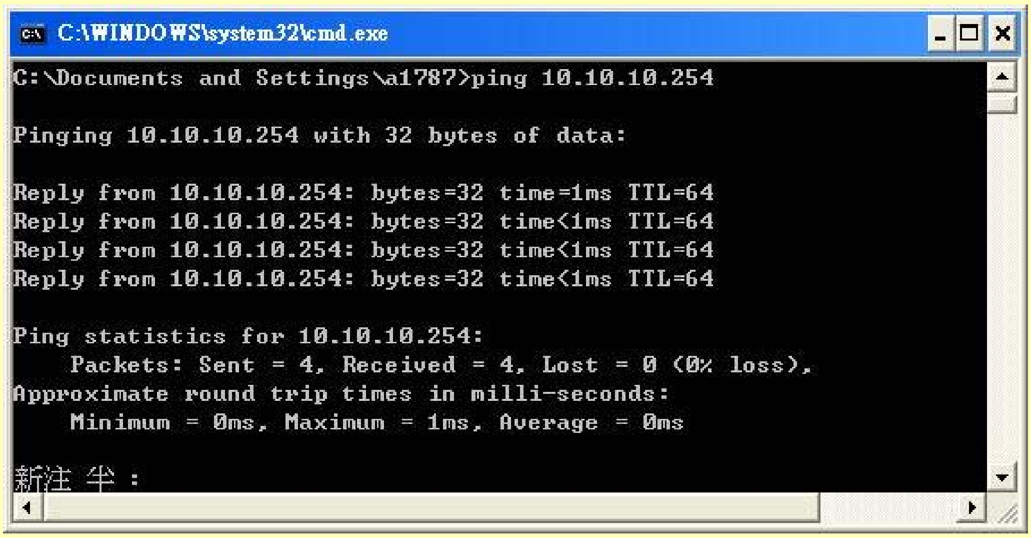
## If you cannot connect...

If the Wireless Router does not respond, please check following:

- The Wireless Router is properly installed, LAN connection is OK, and it is already powered ON. You can test the connection by using the "**Ping**" command:
  - Please go to **Start**>**Run…**> Enter "**cmd**" command in the column to open the MS-DOS window.


Run
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
Open: cmd
OK
Cancel
Browse...

  - Enter the command: **ping 10.10.10.254**



```
C:\Documents and Settings\a1787>ping 10.10.10.254

Pinging 10.10.10.254 with 32 bytes of data:

Reply from 10.10.10.254: bytes=32 time=1ms TTL=64
Reply from 10.10.10.254: bytes=32 time<1ms TTL=64
Reply from 10.10.10.254: bytes=32 time<1ms TTL=64
Reply from 10.10.10.254: bytes=32 time<1ms TTL=64

Ping statistics for 10.10.10.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

新注 半 :
```

  If no response is received, either the connection is not working, or your PC's IP address is not compatible with the Wireless Router's IP Address. (See next item.)

- If your PC is using a fixed IP address, its IP address must be within the range 10.10.10.1. to 10.10.10.253 to be compatible with the Wireless Router's default IP Address of 10.10.10.254. Also, the Network *Mask* must be set to 255.255.255.0. See *Chapter 4 - PC Configuration* for details on checking your PC's TCP/IP settings.
- Ensure that your PC and the Wireless Router are on the same network segment. (If you don't have a router, this must be the case.)
- Ensure you are using the wired LAN interface. The Wireless interface can only be used if its configuration matches your PC's wireless settings.

# Common Connection Types

## Cable Modems

| Type | Details | ISP Data required |
|---|---|---|
| Dynamic IP Address | Your IP Address is allocated automatically, when you connect to you ISP. | Usually, none.<br>However, some ISP's may require you to use a particular Hostname, Domain name, or MAC (physical) address. |
| Static (Fixed) IP Address | Your ISP allocates a permanent IP Address to you. | IP Address allocated to you.<br>Some ISP's may also require you to use a particular Hostname, Domain name, or MAC (physical) address. |

## DSL Modems

| Type | Details | ISP Data required |
|---|---|---|
| Dynamic<br>IP Address | Your IP Address is allocated automatically, when you connect to you ISP. | None. |
| Static (Fixed)<br>IP Address | Your ISP allocates a permanent IP Address to you. | IP Address allocated to you. |
| PPPoE | You connect to the ISP only when required. The IP address is usually allocated automatically. | User name and password. |
| PPTP | Mainly used in Europe.<br>You connect to the ISP only when required. The IP address is usually allocated automatically, but may be Static (Fixed). | ● PPTP Server IP Address.<br>● User name and password.<br>● IP Address allocated to you, if Static (Fixed). |
| L2TP | Mainly used in Europe.<br>You connect to the ISP only when required. The IP address is usually allocated automatically, but may be Static (Fixed). | ● L2TP Server IP Address.<br>● User name and password.<br>● IP Address allocated to you, if Static (Fixed). |

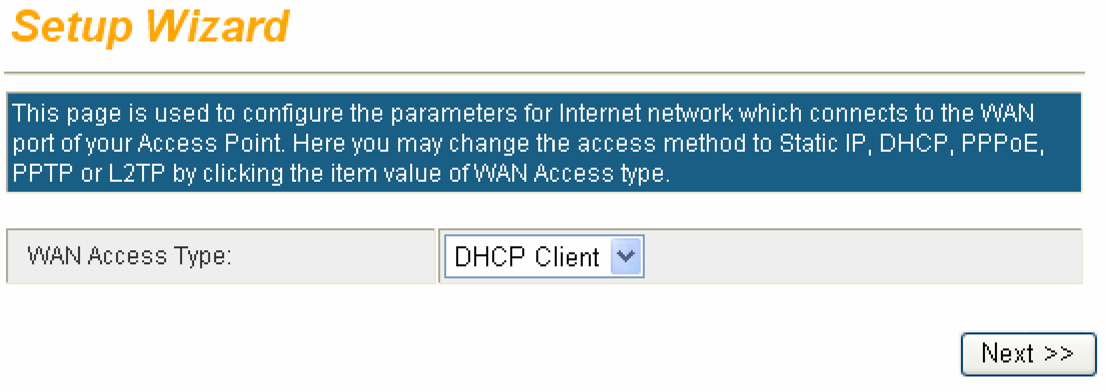
## Other Modems (e.g. Broadband Wireless)

| Type | Details | ISP Data required |
|---|---|---|
| Dynamic<br>IP Address | Your IP Address is allocated automatically, when you connect to you ISP. | None. |
| Static (Fixed)<br>IP Address | Your ISP allocates a permanent IP Address to you. | IP Address allocated to you. |

# Wizard (GW)

## Step 1- WAN Access Type

Here user can set up the WAN connection type easily. Select the WAN Connection Type **Static IP, DHCP Client, PPPoE** or **L2TP, PPTP** and click **Next** to continue.



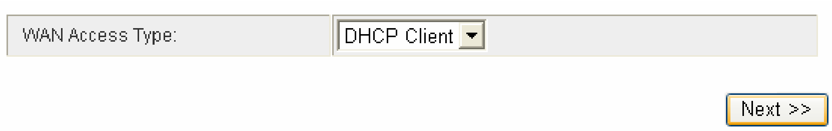
Setup Wizard

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 clicking the item value of WAN Access type.

| | |
|---|---|
| WAN Access Type: | DHCP Client |

**WAN Access Type**

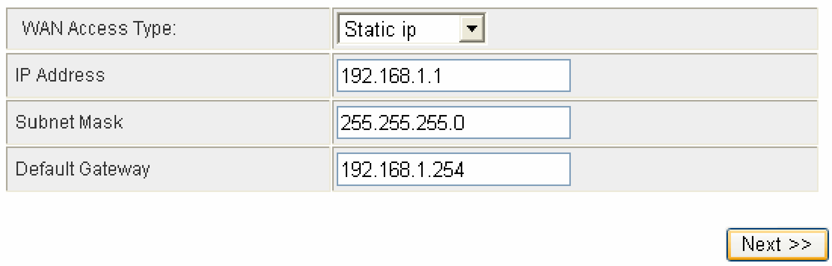
**DHCP Client**



| | |
|---|---|
| WAN Access Type: | DHCP Client |

If the DHCP Client WAN connection be selected, the PC will obtain the IP address automatically.

**Static IP**



| | |
|---|---|
| WAN Access Type: | Static ip |
| IP Address | 192.168.1.1 |
| Subnet Mask | 255.255.255.0 |
| Default Gateway | 192.168.1.254 |

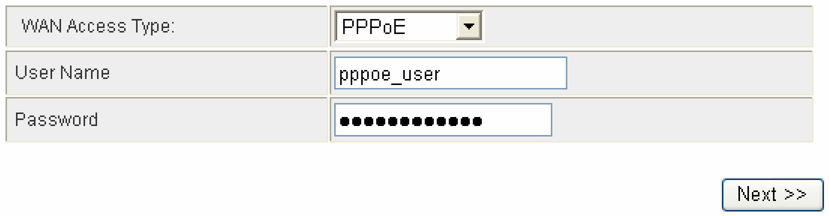
If the Static IP be selected, user have to set up the IP address, subnet mask and default gateway according to the ISP (Internet Service Provider) that provided the related information.

**IP Address:** Enter the WAN IP address provided by your ISP here.

**Subnet Mask:** Enter the subnet mask here.

**Default Gateway:** Enter the default gateway IP address provided by your ISP here.

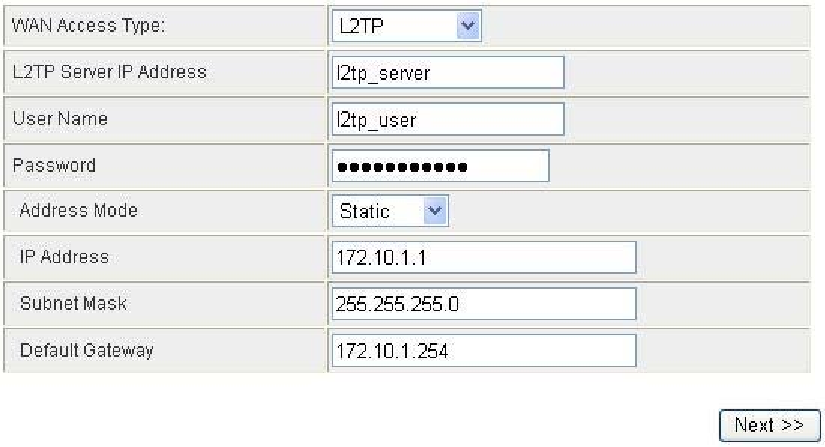
**PPPoE**



| | |
|---|---|
| WAN Access Type: | PPPoE |
| User Name | pppoe_user |
| Password | ●●●●●●●●●●●● |

If the PPPoE be selected, user have to set up the user name and password according to the ISP that provided the related information.
**User Name:** Enter the username that provide by your ISP provider. Maximum input is 32 alphanumeric characters (case sensitive).
**Password:** Enter the password that provide by your ISP provider. Maximum input is 32 alphanumeric characters (case sensitive).

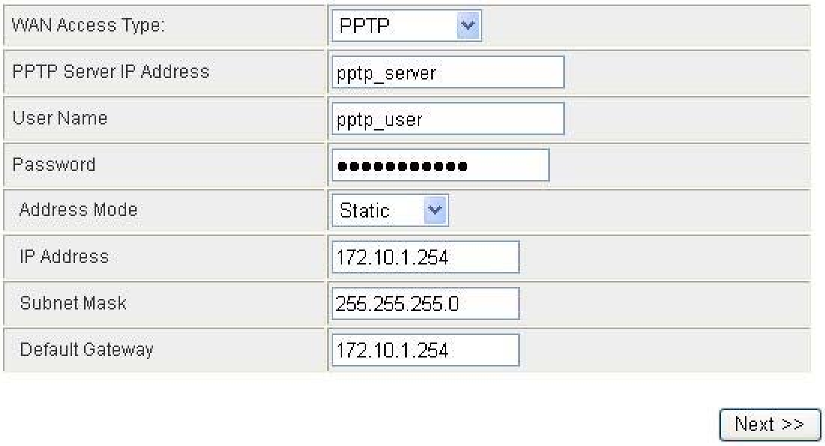
### L2TP



| | |
|---|---|
| WAN Access Type: | L2TP |
| L2TP Server IP Address | l2tp_server |
| User Name | l2tp_user |
| Password | ●●●●●●●●●●●● |
| Address Mode | Static |
| IP Address | 172.10.1.1 |
| Subnet Mask | 255.255.255.0 |
| Default Gateway | 172.10.1.254 |

If the L2TP be selected, user have to set up the server IP address, user name and password according to the ISP that provided the related information.
**L2TP Server IP Address:** Enter the L2TP Server IP Address in this column.
**User Name:** Maximum input is 20 alphanumeric characters (case sensitive).
**Password:** Maximum input is 32 alphanumeric characters (case sensitive).
**Address Mode**: Select **Static** to set up the IP address that provide by your ISP manually, or select **Dynamic** to obtain the IP address automatically.
**IP Address:** Enter the WAN IP address provided by your ISP here.
**Subnet Mask:** Enter the subnet mask here.
**Default Gateway:** Enter the default gateway IP address provided by your ISP here.

### PPTP



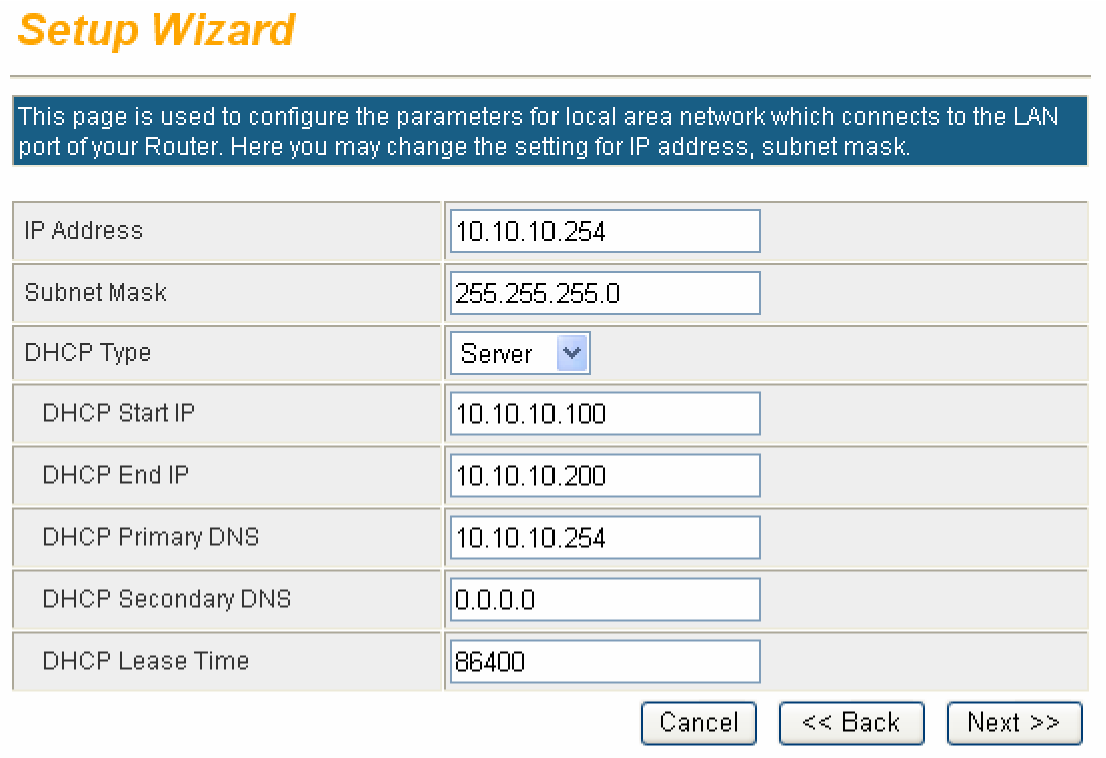
| | |
|---|---|
| WAN Access Type: | PPTP |
| PPTP Server IP Address | pptp_server |
| User Name | pptp_user |
| Password | ●●●●●●●●●●●● |
| Address Mode | Static |
| IP Address | 172.10.1.254 |
| Subnet Mask | 255.255.255.0 |
| Default Gateway | 172.10.1.254 |

If the PPTP be selected, user have to set up the server IP address, user name and password according to the ISP that provided the related information.
**PPTP Server IP Address:** Enter the PPTP Server IP Address in this column.
**User Name:** Maximum input is 20 alphanumeric characters (case sensitive).
**Password:** Maximum input is 32 alphanumeric characters (case sensitive).

| | |
|---|---|
| | **Address Mode**: Select **Static** to set up the IP address that provide by your ISP manually, or select **Dynamic** to obtain the IP address automatically.<br>**IP Address:** Enter the WAN IP address provided by your ISP here.<br>**Subnet Mask:** Enter the subnet mask here.<br>**Default Gateway:** Enter the default gateway IP address provided by your ISP here. |

# Step 2- LAN

This step can set up Wireless Router's IP address, subnet mask, DHCP type, DHCP IP addresses range, DHCP subnet mask and DHCP lease time.



Setup Wizard

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

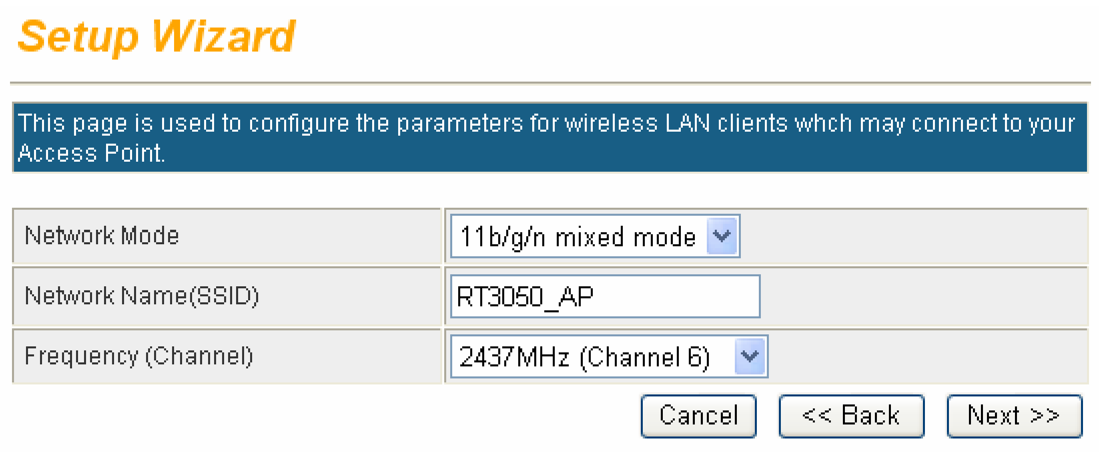
| | |
|---|---|
| IP Address | 10.10.10.254 |
| Subnet Mask | 255.255.255.0 |
| DHCP Type | Server |
| DHCP Start IP | 10.10.10.100 |
| DHCP End IP | 10.10.10.200 |
| DHCP Primary DNS | 10.10.10.254 |
| DHCP Secondary DNS | 0.0.0.0 |
| DHCP Lease Time | 86400 |

| | |
|---|---|
| **IP Address** | Shows the IP address of the Wireless Router (Default IP address is 10.10.10.254.) |
| **Subnet Mask** | The subnet mask of the Wireless Router (Default subnet mask is 255.255.255.0.) |
| **DHCP Type** | **Disable**: Select to disable this Wireless Router to distribute IP addresses to connected clients.<br>**Server**: Select to enable this Wireless Router to distribute IP Addresses (DHCP Server) to connected clients. And the following field will be activated for you to enter the starting IP Address. |
| **DHCP Start IP** | The starting address of this local IP network address pool. The pool is a piece of continuous IP address segment. Keep the default value 10.10.10.100 should work for most cases. |
| **DHCP End IP** | The end IP address, the maximum is 253. Default value 253 should work for most cases (10.10.10.253.) If "**Start IP Address**" is set at 10.10.10.100 and the "**End IP address**" is 10.10.10.253, the device will distribute IP addresses from 10.10.10.100 to 10.10.10.253 to all the computers in the network that request IP addresses from DHCP server (Router). |

| | |
|---|---|
| **DHCP Primary DNS** | You can specify your own preferred DNS server IP address(es). |
| **DHCP Secondary DNS** | You can specify your own preferred DNS server IP address(es).<br>You can enter another DNS server's IP address as a backup. |
| **DHCP Lease Time** | The lease time of the distribute IP Addresses. Default settings are 86400 seconds. |

## Step 3- Network Mode

This step can set up wireless network mode, network name and channel.



Setup Wizard

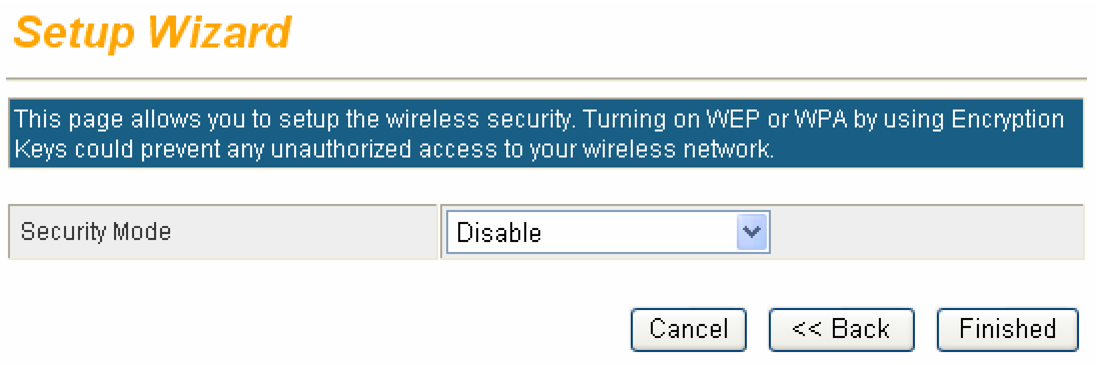
This page is used to configure the parameters for wireless LAN clients whch may connect to your Access Point.

| | |
|---|---|
| Network Mode | 11b/g/n mixed mode |
| Network Name(SSID) | RT3050_AP |
| Frequency (Channel) | 2437MHz (Channel 6) |

| | |
|---|---|
| **Network Mode** | Select 11b/g mixed, 11b only, 11g only, or 11b/g/n mixed mode from the pull-down menu. (Default is 11b/g/n mixed mode.) |
| **Network Name (SSID)** | A SSID is referred to a network name because essentially it is a name that identifies a wireless network. |
| **Frequency (Channel)** | Select **1~13** or **Auto Select** from the pull-down menu. |

## Step 4- Security

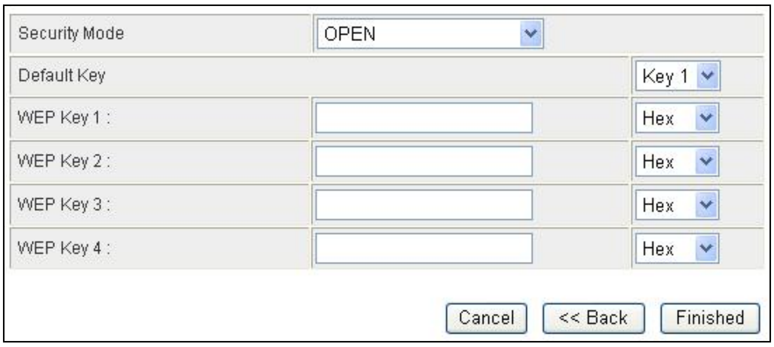
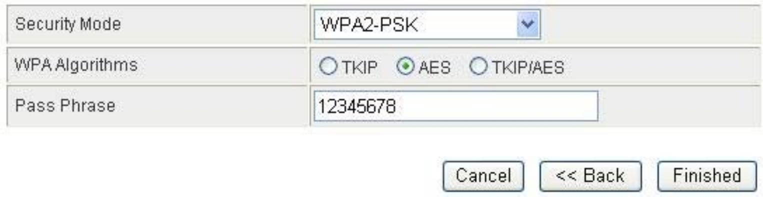
Here can set up the wireless security of the Wireless Router.



Setup Wizard

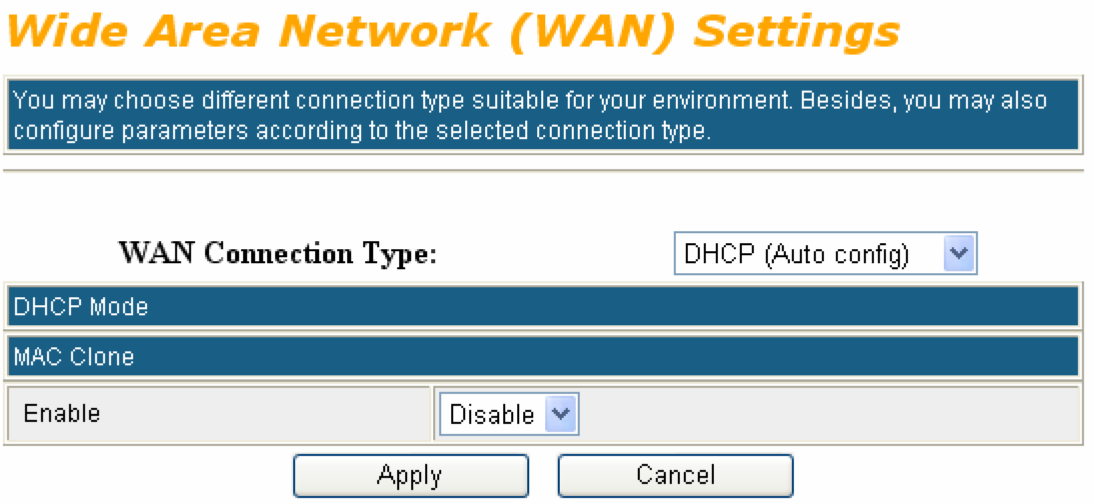
This page allows you to setup the wireless security. Turning on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

| | |
|---|---|
| Security Mode | Disable |

| | |
|---|---|
| **Security Mode** | Select desired security type from the pull-down menu **Disable, OPEN, SHARED, WEP AUTO, WPA-PSK, WPA2-PSK**, and **WPA-PSK/WPA2-PSK**. The default setting is **Disable**. It is strongly recommended to set up security mode (OPEN, SHARED, WEP AUTO, WPA-PSK, WPA2-PSK, WPA-PSK/WPA2-PSK) to prevent any unauthorized accessing.<br>**OPEN/SHARED/WEP AUTO**<br><br>Security Mode: OPEN<br>Default Key: Key 1<br>WEP Key 1 : Hex<br>WEP Key 2 : Hex<br>WEP Key 3 : Hex<br>WEP Key 4 : Hex<br> <br>**Default Key**: Select the default key Key1~4.<br>**WEP Key 1~4:** Enter the key in the selected key field. Only valid when using WEP encryption algorithm. The key must match with the AP's key. There are several formats to enter the keys.<br>● **Hexadecimal (WEP 64 bits):** 10 Hex characters (0~9, a~f).<br>● **Hexadecimal (WEP 128 bits):** 26 Hex characters (0~9, a~f).<br>● **ASCII (WEP 64 bits):** 5 ASCII characters (case-sensitive).<br>● **ASCII (WEP 128 bits):** 13 ASCII characters (case-sensitive).<br>**WPA-PSK/ WPA2-PSK/ WPA-PSK/WPA2-PSK**<br><br>Security Mode: WPA2-PSK<br>WPA Algorithms: ○ TKIP ● AES ○ TKIP/AES<br>Pass Phrase: 12345678<br> <br>**WPA Algorithms**: Select the type of algorithm, TKIP or AES for WP-PSK, and TKIP, AES or TKIP/AES for WPA2-PSK, WPA-PSK/WPA2-PSK.<br>**Pass Phrase**: Enter the pass phrase 8~63 ASCII characters in the column. |

# Internet Settings

## WAN (GW)



Wide Area Network (WAN) Settings

You may choose different connection type suitable for your environment. Besides, you may also configure parameters according to the selected connection type.

WAN Connection Type: DHCP (Auto config)

DHCP Mode

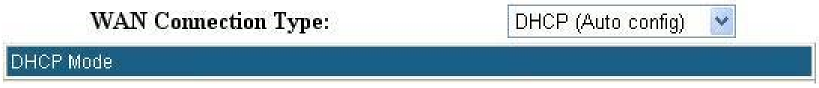
MAC Clone

| | |
|---|---|
| Enable | Disable |

**WAN Connection Type**

Select the WAN Connection Type **Static (fixed IP), DHCP (Auto Config), PPPoE (ADSL), L2TP,** and **PPTP**. Default setting is **DHCP** enabled.

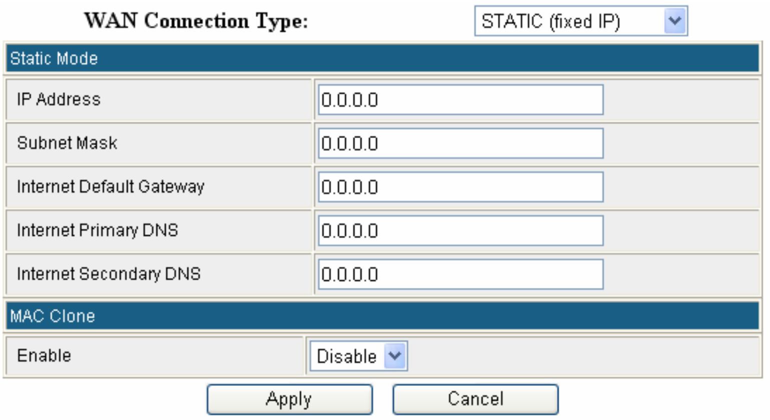
**DHCP (Auto Config)**



WAN Connection Type: DHCP (Auto config)

DHCP Mode

**Static (fixed IP)**



WAN Connection Type: STATIC (fixed IP)

Static Mode

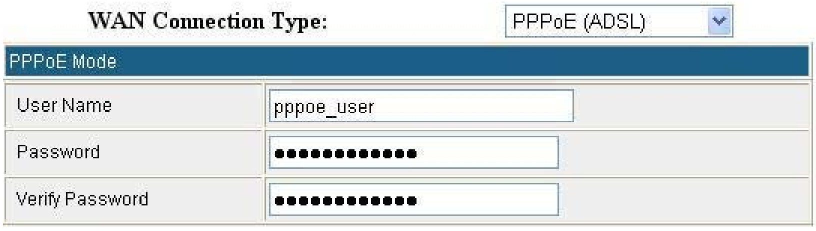
| | |
|---|---|
| IP Address | 0.0.0.0 |
| Subnet Mask | 0.0.0.0 |
| Internet Default Gateway | 0.0.0.0 |
| Internet Primary DNS | 0.0.0.0 |
| Internet Secondary DNS | 0.0.0.0 |

MAC Clone

| | |
|---|---|
| Enable | Disable |

**IP Address:** Enter the WAN IP address provided by your ISP in this column.
**Subnet Mask:** Enter the Subnet Mask in this column.
**Internet Default Gateway:** Enter the default gateway IP address provided by your ISP in this column.
**Internet Primary DNS:** The *DNS* should be set to the address provided by your ISP.
**Internet Secondary DNS:** The *DNS* should be set to the address provided by your ISP.

## PPPoE (ADSL)



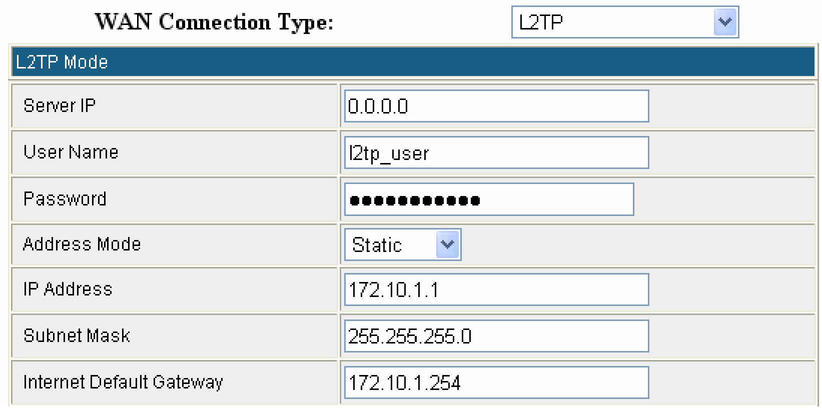
WAN Connection Type: PPPoE (ADSL)

PPPoE Mode

| | |
|---|---|
| User Name | pppoe_user |
| Password | ●●●●●●●●●●●● |
| Verify Password | ●●●●●●●●●●●● |

**User Name:** Enter the username that provide by your ISP. Maximum input is 32 alphanumeric characters (case sensitive).
**Password:** Enter the password that provide by your ISP. Maximum input is 32 alphanumeric characters (case sensitive).
**Verify Password:** To confirm the password, please enter the same password in the filed again.

## L2TP



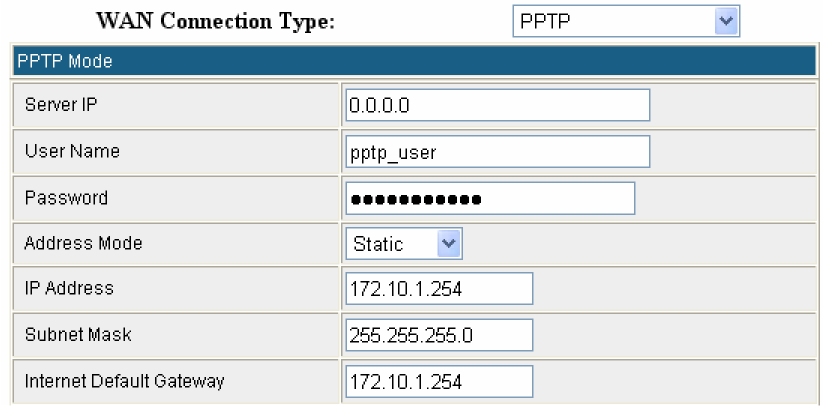
WAN Connection Type: L2TP

L2TP Mode

| | |
|---|---|
| Server IP | 0.0.0.0 |
| User Name | l2tp_user |
| Password | ●●●●●●●●●●● |
| Address Mode | Static |
| IP Address | 172.10.1.1 |
| Subnet Mask | 255.255.255.0 |
| Internet Default Gateway | 172.10.1.254 |

**Server IP:** Enter the L2TP Server IP Address in this column.
**User Name:** Maximum input is 32 alphanumeric characters (case sensitive).
**Password:** Maximum input is 32 alphanumeric characters (case sensitive).
**Address Mode**: Select **Static** to set up the IP address that provide by your ISP manually, or select **Dynamic** to obtain the IP address automatically.
**IP Address:** Enter the WAN IP address provided by your ISP in this column.
**Subnet Mask:** Enter the subnet mask in this column.
**Internet Default Gateway:** Enter the default gateway IP address provided by your ISP in this column.

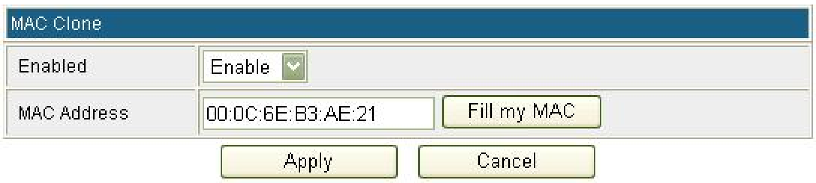
## PPTP



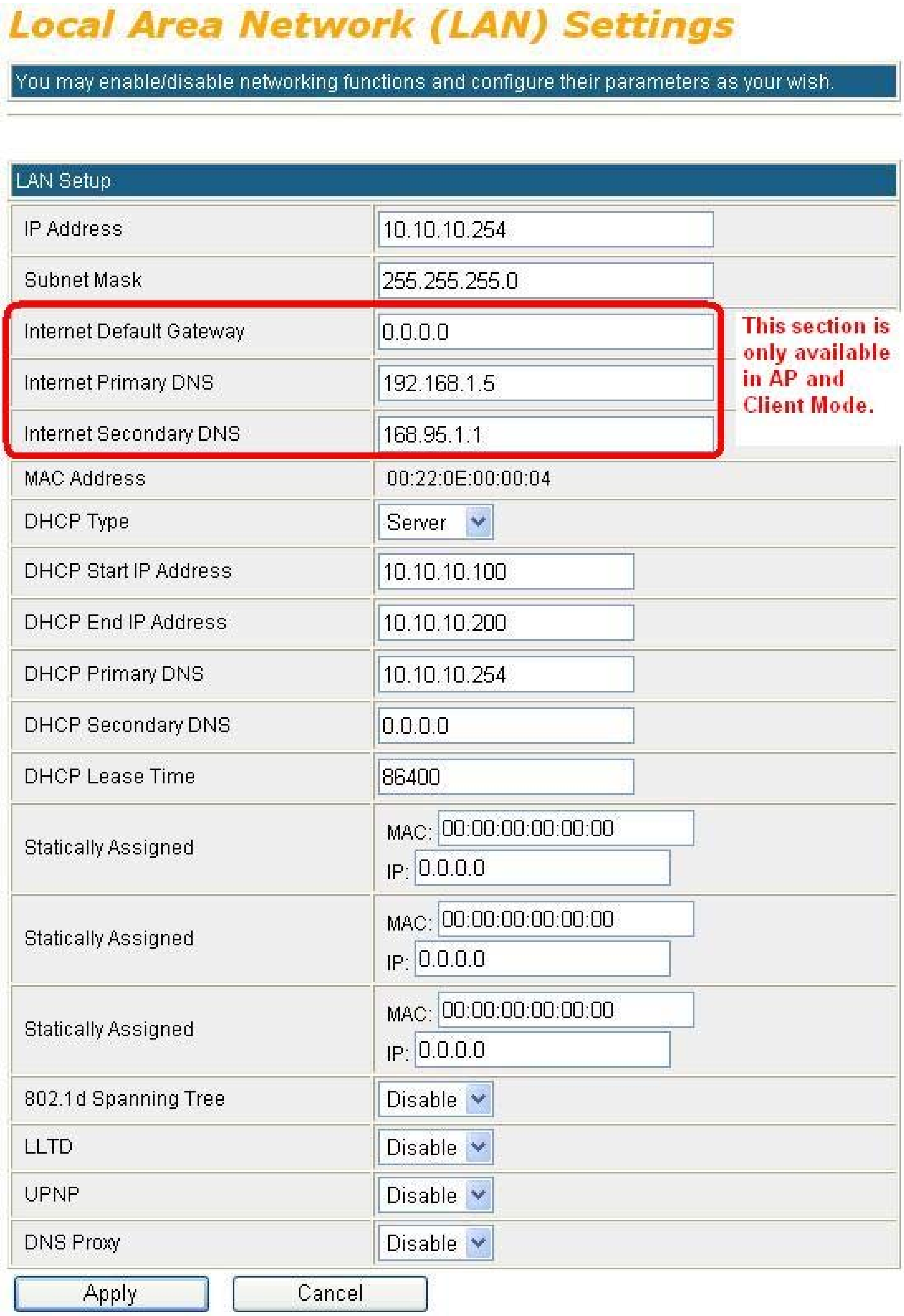
WAN Connection Type: PPTP

PPTP Mode

| | |
|---|---|
| Server IP | 0.0.0.0 |
| User Name | pptp_user |
| Password | ●●●●●●●●●●● |
| Address Mode | Static |
| IP Address | 172.10.1.254 |
| Subnet Mask | 255.255.255.0 |
| Internet Default Gateway | 172.10.1.254 |

| | |
|---|---|
| | **Server IP:** Enter the L2TP Server IP Address in this column.<br>**User Name:** Maximum input is 32 alphanumeric characters (case sensitive).<br>**Password:** Maximum input is 32 alphanumeric characters (case sensitive).<br>**Address Mode**: Select **Static** to set up the IP address that provide by your ISP manually, or select **Dynamic** to obtain the IP address automatically.<br>**IP Address:** Enter the WAN IP address provided by your ISP in this column.<br>**Subnet Mask:** Enter the subnet mask in this column.<br>**Internet Default Gateway:** Enter the default gateway IP address provided by your ISP in this column. |
| **MAC Clone** | 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. Type in or click **Fill my MAC** to replace the WAN MAC address with the MAC address of that PC.<br>Default setting is Disable. User can select **Enable** form the pull-down list, and click **Fill my MAC** button to fill in your PC's MAC address in the blank field.<br><br>MAC Clone<br>Enabled: Enable<br>MAC Address: 00:0C:6E:B3:AE:21<br> |
| **Apply** | After completing the settings on this page, click **Apply** button to save the settings. |
| **Cancel** | Click **Cancel** to restore to default values. |

# LAN



## Local Area Network (LAN) Settings

You may enable/disable networking functions and configure their parameters as your wish.

| LAN Setup | |
|---|---|
| IP Address | 10.10.10.254 |
| Subnet Mask | 255.255.255.0 |
| Internet Default Gateway | 0.0.0.0 |
| Internet Primary DNS | 192.168.1.5 |
| Internet Secondary DNS | 168.95.1.1 |
| MAC Address | 00:22:0E:00:00:04 |
| DHCP Type | Server |
| DHCP Start IP Address | 10.10.10.100 |
| DHCP End IP Address | 10.10.10.200 |
| DHCP Primary DNS | 10.10.10.254 |
| DHCP Secondary DNS | 0.0.0.0 |
| DHCP Lease Time | 86400 |
| Statically Assigned | MAC: 00:00:00:00:00:00<br>IP: 0.0.0.0 |
| Statically Assigned | MAC: 00:00:00:00:00:00<br>IP: 0.0.0.0 |
| Statically Assigned | MAC: 00:00:00:00:00:00<br>IP: 0.0.0.0 |
| 802.1d Spanning Tree | Disable |
| LLTD | Disable |
| UPNP | Disable |
| DNS Proxy | Disable |

This section is only available in AP and Client Mode.

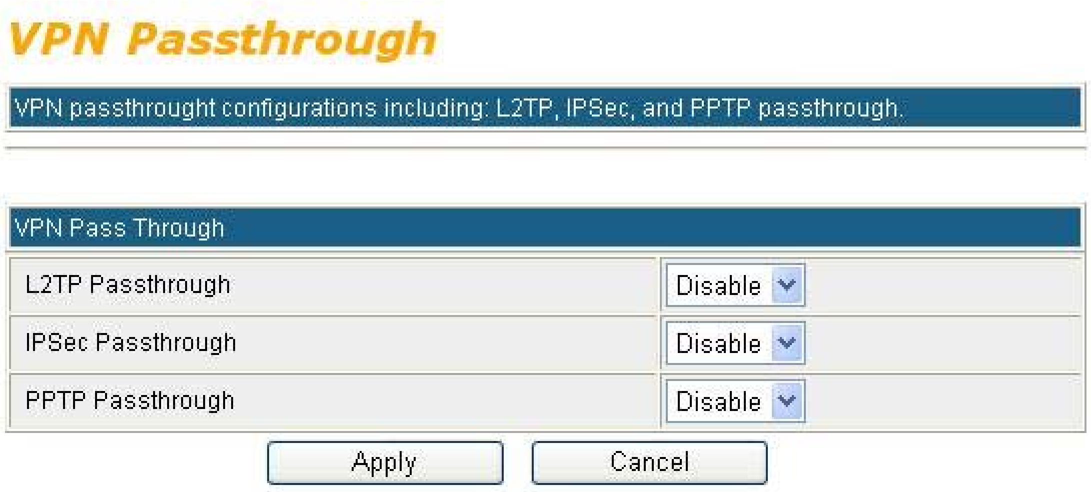
| | |
|---|---|
| **IP Address** | Shows the IP address of the Wireless Router (Default IP address is 10.10.10.254.) |
| **Subnet Mask** | The subnet mask of the Wireless Router (Default subnet mask is 255.255.255.0.) |

| | |
|---|---|
| **Internet Default Gateway** | **<u>This section is only available in AP and Client Mode.</u>**<br>Enter the Internet default gateway LAN IP address in this column. And, the default gateway should has a connection with the Internet. |
| **Internet Primary DNS** | **<u>This section is only available in AP and Client Mode.</u>**<br>The Primary DNS is used for resolve the URL address to physical IP address. |
| **Internet Secondary DNS** | **<u>This section is only available in AP and Client Mode.</u>**<br>The Secondary DNS is used for resolve the URL address to physical IP address. |
| **MAC Address** | Shows the MAC address of this Wireless Router. |
| **DHCP Type** | **Disable**: Select to disable this Wireless Router to distribute IP addresses to connected clients.<br>**Server**: Select to enable this Wireless Router to distribute IP Addresses (DHCP Server) to connected clients. And the following field will be activated for you to enter the starting IP address. |
| **DHCP Start IP Address** | The starting address of this local IP network address pool. The pool is a piece of continuous IP address segment. Keep the default value 10.10.10.100 should work for most cases. |
| **DHCP End IP Address** | The end IP address, the maximum is 253. Default value 253 should work for most cases (10.10.10.253.) If “**Start IP Address**” is set at 10.10.10.100 and the “**End IP address**” is 10.10.10.253, the device will distribute IP addresses from 10.10.10.100 to 10.10.10.253 to all the computers in the network that request IP addresses from DHCP server (Router). |
| **DHCP Primary DNS** | You can specify your own preferred DNS server IP address(es). |
| **DHCP Secondary DNS** | Secondary DNS Server is optional. You can enter another DNS server’s IP address as a backup. |
| **DHCP Lease Time** | The lease time of the distribute IP Addresses. Default settings are 86400 seconds. |
| **Statically Assigned** | **MAC**: Enter the MAC address of a certain station, and then the DHCP Server will to distribute a fixed IP address to the station automatically once be connected.<br>**IP**: Enter the fixed IP address that DHCP Server assigned to a certain connected station.<br>User can set up 3 set of fixed IP addresses that distribute form the Wireless Router when the DHCP Type function be selected to Server. |
| **802.1d Spanning Tree** | Select Enabled or Disabled from the pull-down menu. |
| **LLTD** | Link Layer Topology Discovery (LLTD) is a proprietary Link Layer protocol for network topology discovery and quality of service diagnostics. The LLTD protocol operates over both wired (IEEE 802.3 Ethernet) as well as wireless (IEEE 802.11) networks.<br>LLTD is included in Windows Vista and is used by its Network Map feature to display a graphical representation of the LAN or WLAN, to which the computer is connected. Windows XP does not contain the LLTD protocol as a standard component and as a result, Windows XP computers do not appear on the Network Map unless the LLTD responder is installed on Windows XP computers.<br>Select Enabled or Disabled from the pull-down menu. |
| **IGMP Proxy** | **<u>This section is only available in Gateway Mode.</u>**<br>The Internet Group Management Protocol (IGMP) is a communications protocol used to manage the membership of Internet Protocol multicast groups. IGMP is used by IP hosts and adjacent multicast routers to establish multicast group memberships. |

| | |
|---|---|
| | Select Disable or Enable from the pull-down menu. |
| **UPNP** | Universal Plug and Play (UPnP) is a set of computer protocols promulgated by the UPnP Forum. The goals of UPnP are to allow devices to connect seamlessly and to simplify the implementation of networks in the home (data sharing, communications, and entertainment) and in corporate environments for simplified installation of computer components. UPnP achieves this by defining and publishing UPnP device control protocols built upon open, Internet-based communication standards. The term UPnP is derived from plug-and-play, a technology for dynamically attaching devices directly to a computer.<br>Select Disable or Enable from the pull-down menu. |
| **PPPoE Relay** | **This section is only available in Gateway Mode.**<br>Select Disable or Enable from the pull-down menu. |
| **DNS Proxy** | Select Disable or Enable from the pull-down menu. |
| **Apply** | After completing the settings on this page, click **Apply** button to save the settings. |
| **Cancel** | Click **Cancel** to restore to default values. |

# VPN Passthrough (GW)

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



VPN Passthrough

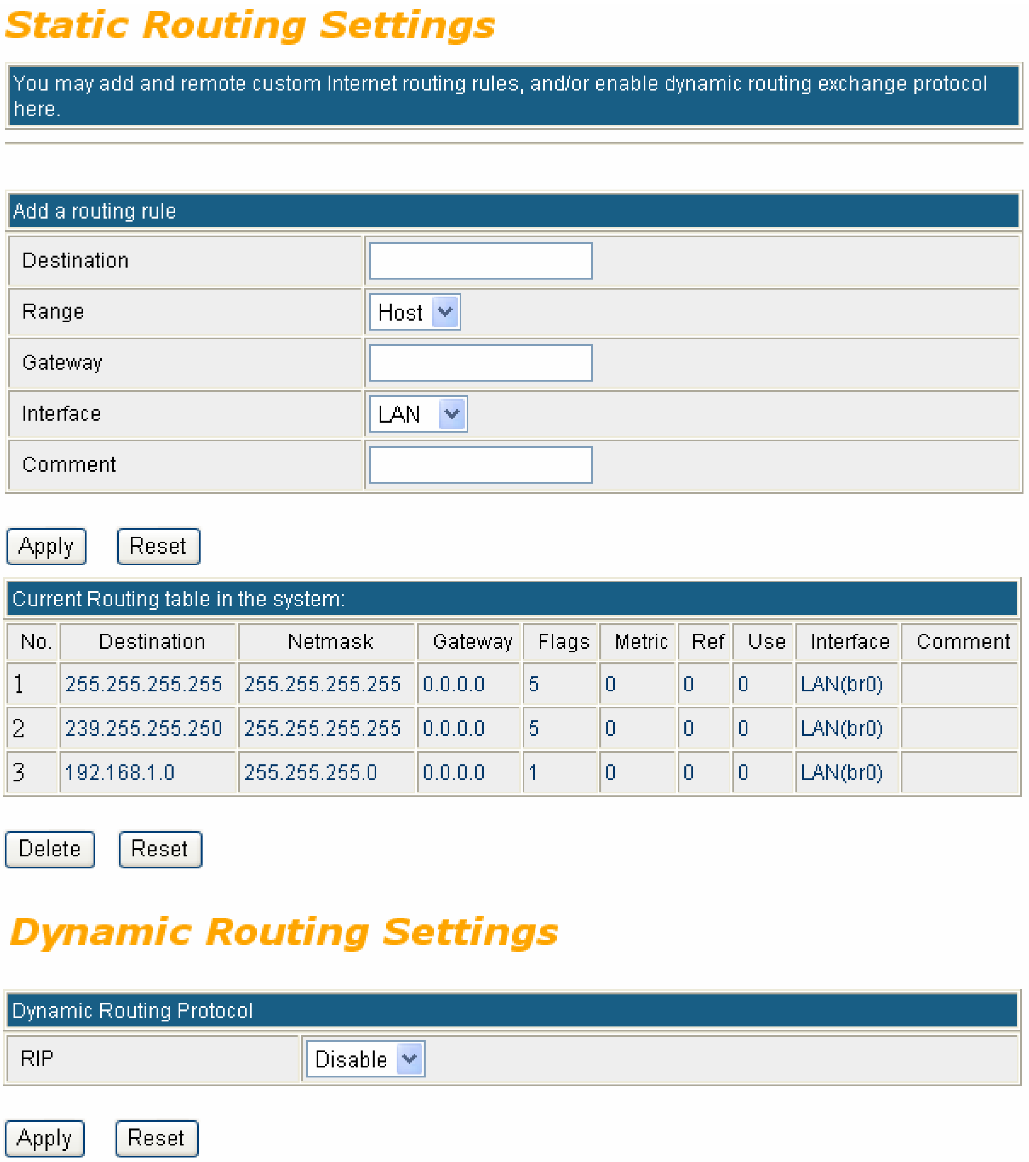
VPN passthrought configurations including: L2TP, IPSec, and PPTP passthrough.

| VPN Pass Through | |
|---|---|
| L2TP Passthrough | Disable |
| IPSec Passthrough | Disable |
| PPTP Passthrough | Disable |

| | |
|---|---|
| **L2TP Passthrough** | L2TP, Layer Two Tunneling Protocol (L2TP). Use the L2TP with VPN that user can access the personal network via Internet.<br>Select Enabled or Disabled from the pull-down menu. |
| **IPSec Passthrough** | IPSec, Internet Protocol Security. Select Enabled or Disabled from the pull-down menu. |
| **PPTP Passthrough** | PPTP, Point-to-Point Tunneling Protocol. Select Enabled or Disabled from the pull-down menu. |

# Advanced Routing (GW)

If you connect several routers with this Wireless Router, you may need to set up a predefined routing rule to have more effective network topology/traffic, this is called static route between those routers and the Wireless Router.
To set static routers, enter the settings including route IP address, route mask route gateway the route Interface from LAN or WAN.



Static Routing Settings

You may add and remote custom Internet routing rules, and/or enable dynamic routing exchange protocol here.

| Add a routing rule | |
|---|---|
| Destination | |
| Range | Host |
| Gateway | |
| Interface | LAN |
| Comment | |

Current Routing table in the system:

| No. | Destination | Netmask | Gateway | Flags | Metric | Ref | Use | Interface | Comment |
|---|---|---|---|---|---|---|---|---|---|
| 1 | 255.255.255.255 | 255.255.255.255 | 0.0.0.0 | 5 | 0 | 0 | 0 | LAN(br0) | |
| 2 | 239.255.255.250 | 255.255.255.255 | 0.0.0.0 | 5 | 0 | 0 | 0 | LAN(br0) | |
| 3 | 192.168.1.0 | 255.255.255.0 | 0.0.0.0 | 1 | 0 | 0 | 0 | LAN(br0) | |

Dynamic Routing Settings

| Dynamic Routing Protocol | |
|---|---|
| RIP | Disable |

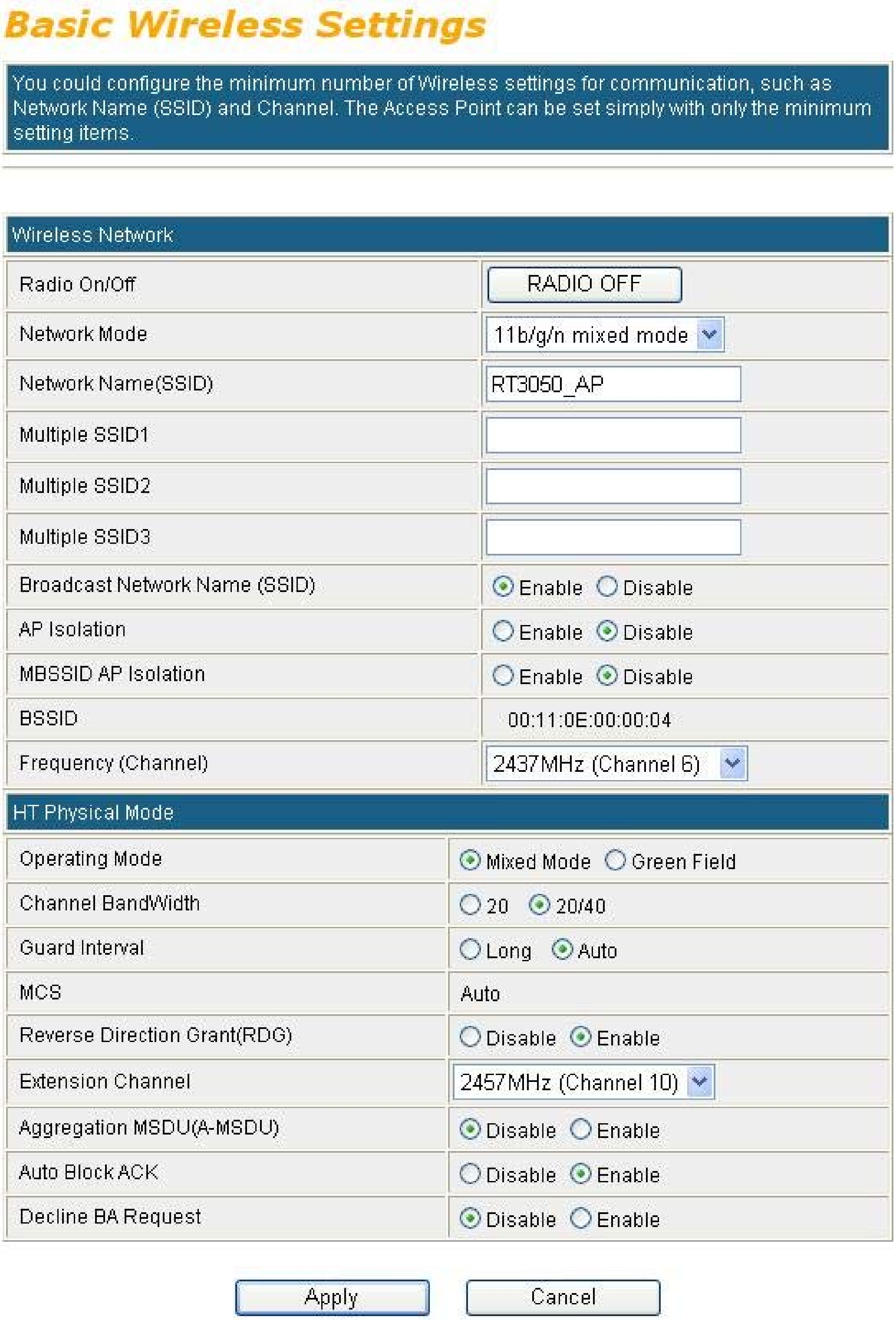
| | |
|---|---|
| **Destination** | The network address of the destination LAN segment. When a packet with destination IP address that matches to this field, it will route to the device set in the Route Gateway field. |
| **Range** | Select Host or Net from the pull-down menu. |
| **Gateway** | Enter the Gateway IP address in the field. |
| **Interface** | You can select to use LAN, WAN or Custom as the physical interface from where the packets will be sent. |
| **Comment** | Enter note or remark here. |
| **Dynamic Routing Settings** | Select Disable or Enable form pull-dowm list to use the RIP function. |

| | |
|---|---|
| **Apply** | After completing the settings on this page, click **Apply** button to save the settings. |
| **Reset** | Click to discard current setting. |

# Wireless Settings

## Gateway / Access Point Modes

### Basic



Basic Wireless Settings

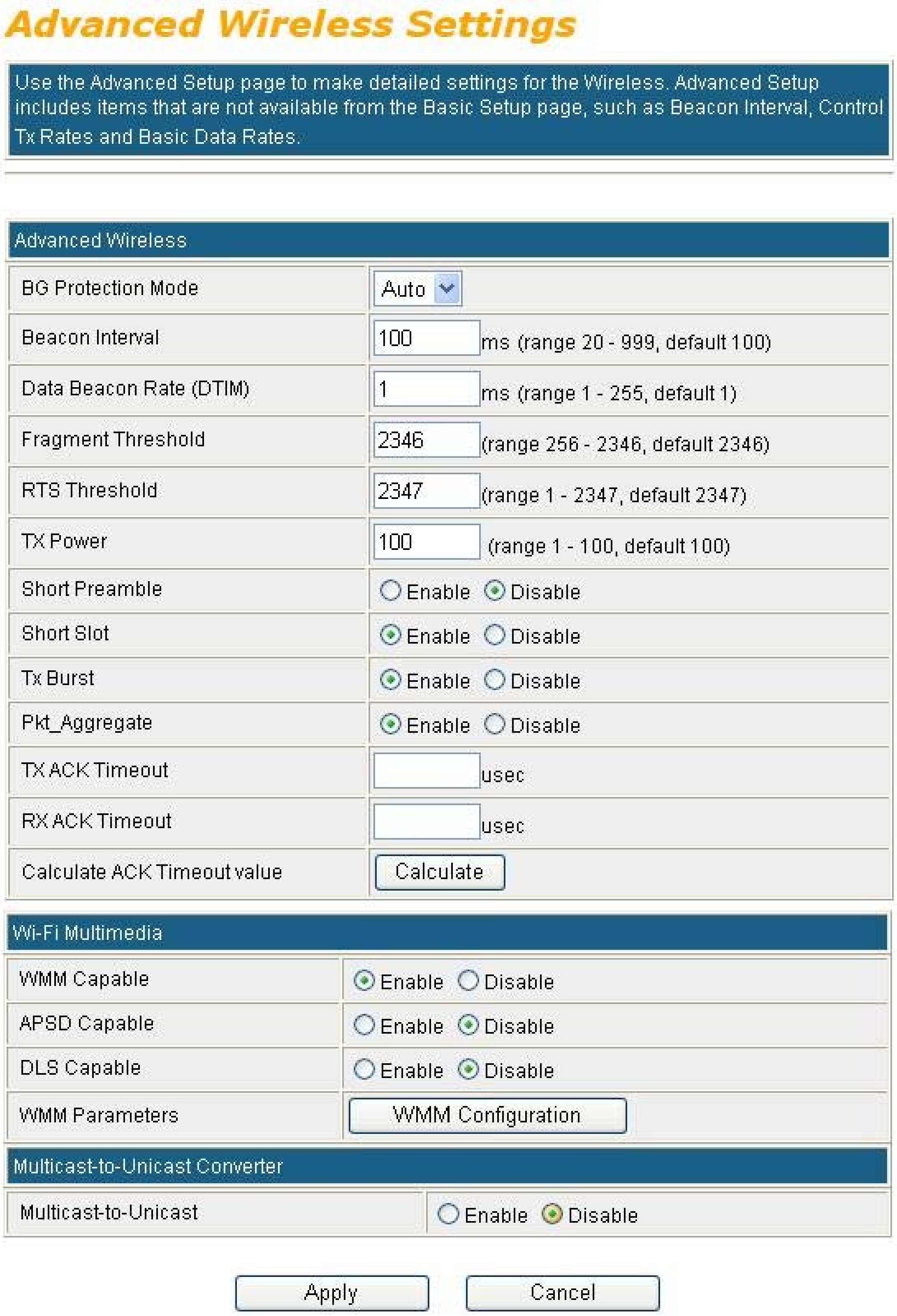
You could configure the minimum number of Wireless settings for communication, such as Network Name (SSID) and Channel. The Access Point can be set simply with only the minimum setting items.

| Wireless Network | |
|---|---|
| Radio On/Off | RADIO OFF |
| Network Mode | 11b/g/n mixed mode |
| Network Name(SSID) | RT3050_AP |
| Multiple SSID1 | |
| Multiple SSID2 | |
| Multiple SSID3 | |
| Broadcast Network Name (SSID) | ● Enable ○ Disable |
| AP Isolation | ○ Enable ● Disable |
| MBSSID AP Isolation | ○ Enable ● Disable |
| BSSID | 00:11:0E:00:00:04 |
| Frequency (Channel) | 2437MHz (Channel 6) |

| HT Physical Mode | |
|---|---|
| Operating Mode | ● Mixed Mode ○ Green Field |
| Channel BandWidth | ○ 20 ● 20/40 |
| Guard Interval | ○ Long ● Auto |
| MCS | Auto |
| Reverse Direction Grant(RDG) | ○ Disable ● Enable |
| Extension Channel | 2457MHz (Channel 10) |
| Aggregation MSDU(A-MSDU) | ● Disable ○ Enable |
| Auto Block ACK | ○ Disable ● Enable |
| Decline BA Request | ● Disable ○ Enable |

| Wireless Network | |
|---|---|
| **Radio On/Off** | Click **Radio ON/OFF** button to turn on/off the radio function. |
| **Network Mode** | Select 11b/g mixed, 11b only, 11g only, or 11b/g/n mixed mode from the pull-down menu. (Default is 11b/g/n mixed mode.) |
| **Network Name (SSID)** | A SSID is referred to a network name because essentially it is a name that identifies a wireless network. |
| **Multiple SSID 1~3** | 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 stations.<br>**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. |
| **AP Isolation** | Select Enable or Disable to enable this function.<br>Access Point Isolation, this function is used to separate wireless clients to access each other while connected to the same access point. |
| **MBSSID AP Isolation** | Select Enable or Disable to enable this function.<br>When this function be enabled, clients connected to different network name(SSID) access points cannot access to each other, but can access to the clients that under connecting to the same SSID AP. |
| **BSSID** | Shows the **Wireless MAC address** of the Wireless Router. |
| **Frequency (Channel)** | Select 1~13 or Auto Select from the pull-down menu. |
| **HT Physical Mode** | |
| **Operating Mode** | Green Field (11n mode), Mixed Mode(11b/g/n mode). Select Mixed Mode or Green Field. (Default operating mode is Mixed Mode.) |
| **Channel Band Width** | Select 20 or 20/40. (Default setting is 20/40.) |
| **Guard Interval** | Select Long or Auto. (Default setting is Auto.) |
| **MCS** | Default setting is Auto. |
| **Reverse Direction Grant(RDG)** | Select Disable or Enable this function. (Default setting is Enable.) |
| **Extension Channel** | According the Frequency (Channel) that you selected, here will show the Extension Channel(s). |
| **Aggregation MSDU (A-MSDU)** | Select Disable or Enable. (Default setting is Disable.) |
| **Auto Block ACK** | Select Disable or Enable. (Default setting is Enable.) |
| **Decline BA Request** | Select Disable or Enable. (Default setting is Disable.) |

## Advanced



Advanced Wireless Settings

Use the Advanced Setup page to make detailed settings for the Wireless. Advanced Setup includes items that are not available from the Basic Setup page, such as Beacon Interval, Control Tx Rates and Basic Data Rates.

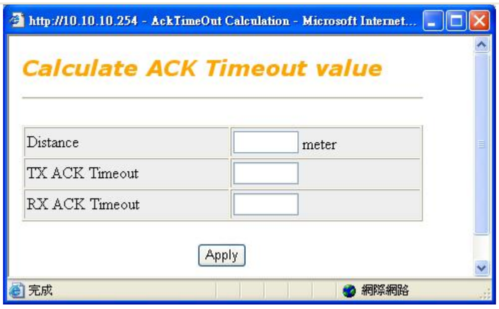
| Advanced Wireless | |
|---|---|
| BG Protection Mode | Auto |
| Beacon Interval | 100 ms (range 20 - 999, default 100) |
| Data Beacon Rate (DTIM) | 1 ms (range 1 - 255, default 1) |
| Fragment Threshold | 2346 (range 256 - 2346, default 2346) |
| RTS Threshold | 2347 (range 1 - 2347, default 2347) |
| TX Power | 100 (range 1 - 100, default 100) |
| Short Preamble | ○ Enable ● Disable |
| Short Slot | ● Enable ○ Disable |
| Tx Burst | ● Enable ○ Disable |
| Pkt_Aggregate | ● Enable ○ Disable |
| TX ACK Timeout | usec |
| RX ACK Timeout | usec |
| Calculate ACK Timeout value | Calculate |

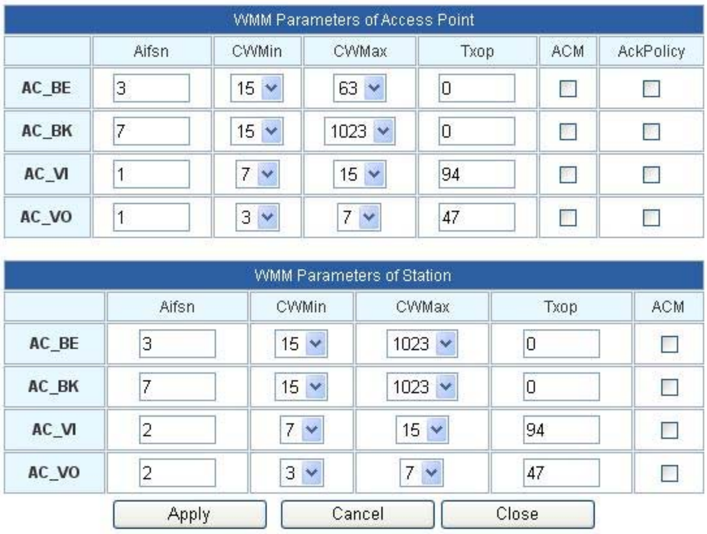
| Wi-Fi Multimedia | |
|---|---|
| WMM Capable | ● Enable ○ Disable |
| APSD Capable | ○ Enable ● Disable |
| DLS Capable | ○ Enable ● Disable |
| WMM Parameters | WMM Configuration |

| Multicast-to-Unicast Converter | |
|---|---|
| Multicast-to-Unicast | ○ Enable ● Disable |

| Advanced Wireless | |
|---|---|
| **BG Protection Mode** | Select the protection mode form the pull-down list, Auto, On and Off. |
| **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 Beacon Interval is 100.) |
| **Data Beacon Rate (DTIM)** | Range from 1 to 255. (Default data beacon rate is 1.) |
| **Fragment Threshold** | Fragmentation mechanism is used for improving the efficiency when high traffic flows along in the wireless network. If the 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 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 value is 2347.)<br>**Warning:** Enabling RTS Threshold will cause redundant network overhead that could negatively affect the throughput performance instead of providing a remedy.<br>This value should remain at its default setting of 2347. Should you encounter inconsistent data flow, only minor modifications of this value are recommended. |
| **TX Power** | Transmit power, the amount of power used by a radio transceiver to send the signal out. |
| **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** | Select Disable or Enable this function. (Default short slot setting is Enable.) |
| **Tx Burst** | Check to enable this function (Default Tx Burst setting is Enable.) This function enables the Wireless Router to deliver better throughput during a period of time, it only takes effect when connecting with the device that supports this function. |
| **Pkt_Aggregate** | Select Disable or Enable this function. (Default setting is Enable.) |
| **TX ACK Timeout** | ACK time out means "Acknowledgement Time Out", meaning that the system (the computer on sprint's end) didn't acknowledge your SMS in the time allotted. This is probably because of a communication error, and they'll have it fixed soon. |
| **RX ACK Timeout** | ACK time out means "Acknowledgement Time Out", meaning that the system (the computer on sprint's end) didn't acknowledge your SMS in the time allotted. This is probably because of a communication error, and they'll have it fixed soon. |

| | |
|---|---|
| **Calculate ACK Timeout value** | <br>http://10.10.10.254 - AckTimeOut Calculation - Microsoft Internet...<br>Calculate ACK Timeout value<br>Distance □ meter<br>TX ACK Timeout □<br>RX ACK Timeout □<br>Apply<br>完成 網際網路 |
| **Wi-Fi Multimedia** | |
| **WMM Capable** | WMM Power Save is a set of features for Wi-Fi networks that help conserve battery power in small devices such as phones, PDAs, and audio players. The certification for both access points and client devices uses mechanisms from the recently ratified IEEE 802.11e standard, and is an enhancement of legacy 802.11 power save. WMM Power Save helps pave the way for rapid proliferation of Wi-Fi technology into devices dependent on battery power.<br>Select Disable or Enable to use or stop Wi-Fi Multimedia function. (Default setting is Enable.) |
| **APSD Capable** | Automatic Power Save Delivery is a more efficient power management method than legacy 802.11 Power Save Polling. Most newer 802.11 station already support a power management mechanism similar to APSD. APSD is very useful for a VoIP phone, as data rates are roughly the same in both directions. Whenever Voice data are sent to the Access Point, the Access Point is triggered to send the buffered Voice data in the other direction. After that the Voice over IP phone enters doze state until next Voice data have to be sent to the Access Point.<br>Select Disable or Enable this function. (Default setting is Disable.) |
| **DLS Capable** | Direct Link Setup, this function will be enabled under the connection with AP which must support the DLS function. Direct Link Setup allows direct STA-to-STA frame transfer within a BSS (Basic Service Set). This is designed for consumer use, where STA-to-STA transfer is more commonly used.<br>Select Disable or Enable this function. (Default setting is Disable.) |
| **WMM Parameters** | Click the WMM Configuration button to go further settings. |

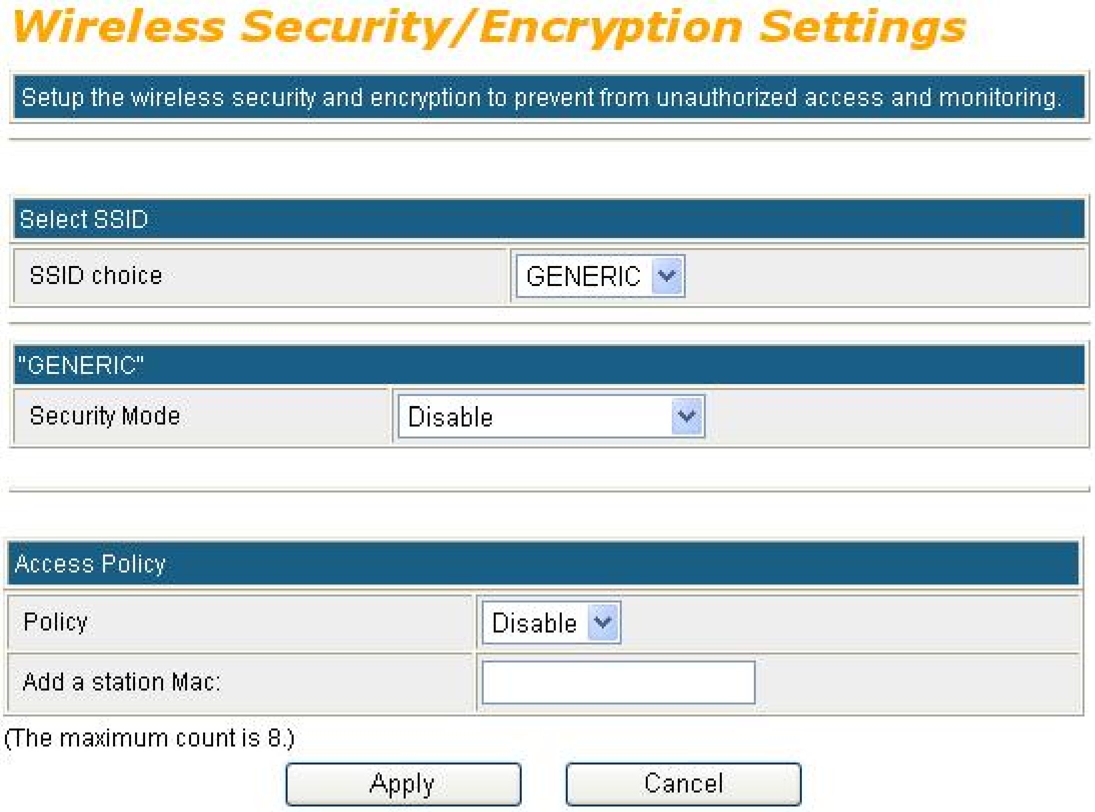
| | |
|---|---|
| |  |

| WMM Parameters of Access Point | | | | | | |
|---|---|---|---|---|---|---|
| | Aifsn | CWMin | CWMax | Txop | ACM | AckPolicy |
| AC_BE | 3 | 15 | 63 | 0 | □ | □ |
| AC_BK | 7 | 15 | 1023 | 0 | □ | □ |
| AC_VI | 1 | 7 | 15 | 94 | □ | □ |
| AC_VO | 1 | 3 | 7 | 47 | □ | □ |

| WMM Parameters of Station | | | | | |
|---|---|---|---|---|---|
| | Aifsn | CWMin | CWMax | Txop | ACM |
| AC_BE | 3 | 15 | 1023 | 0 | □ |
| AC_BK | 7 | 15 | 1023 | 0 | □ |
| AC_VI | 2 | 7 | 15 | 94 | □ |
| AC_VO | 2 | 3 | 7 | 47 | □ |

| **Multicast-to-Unicast Converter** | |
|---|---|
| **Multicast-to-Unicast** | Select Disable or Enable this function. (Default setting is Disable.) |

## Security



### Wireless Security/Encryption Settings

Setup the wireless security and encryption to prevent from unauthorized access and monitoring.

| Select SSID | |
|---|---|
| SSID choice | GENERIC |

| "GENERIC" | |
|---|---|
| Security Mode | Disable |

| Access Policy | |
|---|---|
| Policy | Disable |
| Add a station Mac: | |

(The maximum count is 8.)

| **Wireless Security/Encryption Settings** | |
|---|---|
| **Select choice** | Select SSID to set up the security form the pull-down list. |

**Security Mode**

There are eleven type of authentication modes including **Disable**, **OPEN, SHARED, WEP AUTO, WPA, WPA-PSK, WPA2, WPA2-PSK**, **WPA-PSK/ WPA2-PSK, WPA/WPA2** and **802.1X**. The security default setting is Disable.

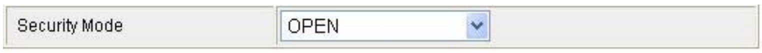
The client or station must use the same encryption and enter the same password when make a connection with the Wireless Router.

**Note:**

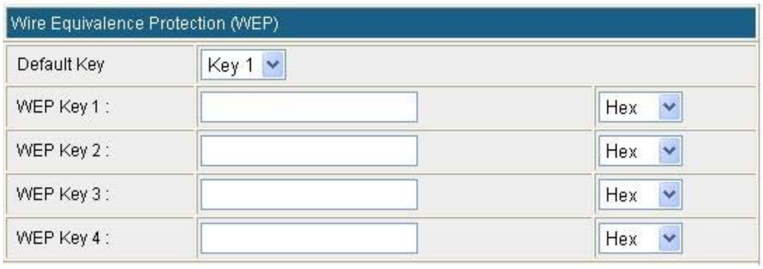
- Disable means none security.
- WPA and WPA-PSK only support TKIP and AES as encryption method.
- SHARED only supports WEP as encryption method.
- WEP AUTO means Wireless Router can accept clients connect by using OPEN-WEP or SHARED-WEP.

**OPEN/ WEP AUTO**

If your wireless router is using **OPEN** or **WEP AUTO** authentication, then the wireless adapter will need to be set to the same authentication type.



| | |
|---|---|
| Security Mode | OPEN |



Wire Equivalence Protection (WEP)

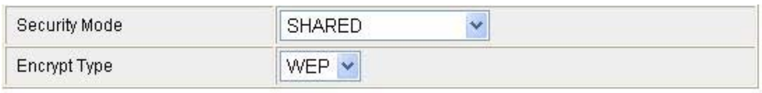
| | | |
|---|---|---|
| Default Key | Key 1 | |
| WEP Key 1 : | | Hex |
| WEP Key 2 : | | Hex |
| WEP Key 3 : | | Hex |
| WEP Key 4 : | | Hex |

**Default Key**: Select the default key.
**WEP Key 1~4:** Enter the key in the selected key field. Only valid when using WEP encryption algorithm. The key must match with the AP's key. There are several formats to enter the keys.

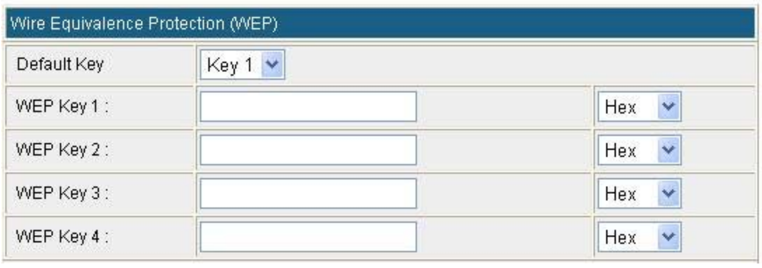
- **Hexadecimal (WEP 64 bits):** 10 Hex characters (0~9, a~f).
- **Hexadecimal (WEP 128 bits):** 26 Hex characters (0~9, a~f).
- **ASCII (WEP 64 bits):** 5 ASCII characters (case-sensitive).
- **ASCII (WEP 128 bits):** 13 ASCII characters (case-sensitive).

**Shared**

Shared key is when both the sender and the recipient share a secret key.



| | |
|---|---|
| Security Mode | SHARED |
| Encrypt Type | WEP |



Wire Equivalence Protection (WEP)

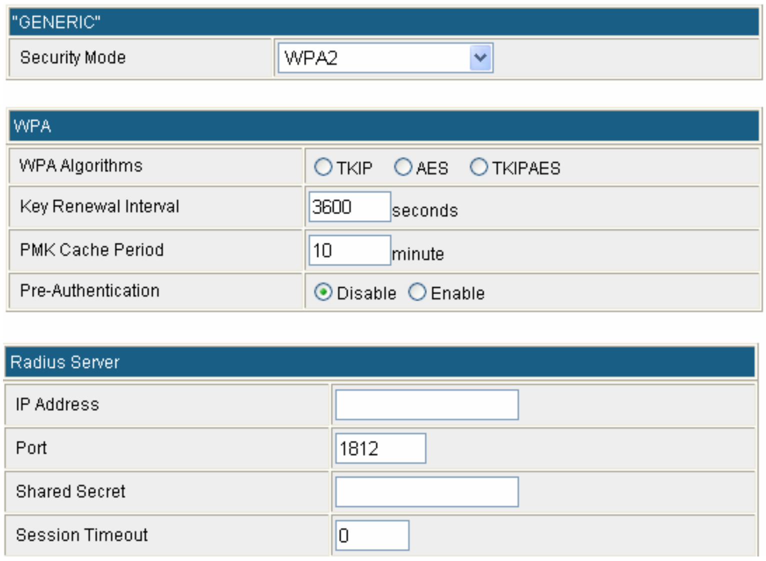
| | | |
|---|---|---|
| Default Key | Key 1 | |
| WEP Key 1 : | | Hex |
| WEP Key 2 : | | Hex |
| WEP Key 3 : | | Hex |
| WEP Key 4 : | | Hex |

**Encryption Type**: The encryption type is WEP.
**Default Key**: Select the default key 1~4.

**WEP Key 1~4:** Enter the key in the selected key field. 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 (WEP 64 bits):** 10 Hex characters (0~9, a~f).
- **Hexadecimal (WEP 128 bits):** 26 Hex characters (0~9, a~f).
- **ASCII (WEP 64 bits):** 5 ASCII characters (case-sensitive).
- **ASCII (WEP 128 bits):** 13 ASCII characters (case-sensitive).

**WPA/ WAP2/ WPA-WPA2**



"GENERIC"

| | |
|---|---|
| Security Mode | WPA2 |

WPA

| | |
|---|---|
| WPA Algorithms | ○ TKIP ○ AES ○ TKIPAES |
| Key Renewal Interval | 3600 seconds |
| PMK Cache Period | 10 minute |
| Pre-Authentication | ● Disable ○ Enable |

Radius Server

| | |
|---|---|
| IP Address | |
| Port | 1812 |
| Shared Secret | |
| Session Timeout | 0 |

**WPA Algorithms**: Select the type of algorithm, TKIP or AES for WPA; TKIP, AES or TKIP AES for WPA2, WPA-WPA2.
**Key Renewal Interval**: Enter the renewal security time (seconds) in the column. Default is 3600 seconds. Set 0 to disable re-key.
**PMK Cache Period: Only valid in WPA2 security.** Set WPA2 PMKID cache timeout period, after time out, the cached key will be deleted. PMK Cache Period unit is minute.

**Pre-Authentication**: **Only valid in WPA2 security.** The 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.

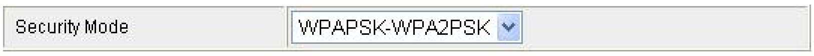
**IP Address:** Enter the RADIUS Server's IP Address provided by your ISP.

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

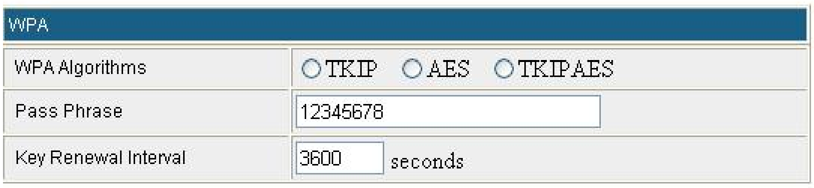
**Shared Secret:** Enter the password that the Wireless Router shares with the RADIUS Server.

**Session Timeout**: Session timeout interval is for 802.1x re-authentication setting. Set to zero to disable 802.1x re-authentication service for each session. Session timeout interval unit is second and must be larger than 60.

**WPA-PSK/ WAP2-PSK/ WPA PSK-WPA2 PSK**



| | |
|---|---|
| Security Mode | WPAPSK-WPA2PSK |

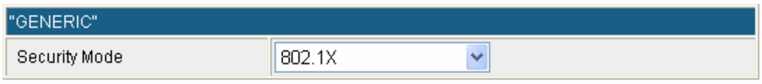


| WPA | |
|---|---|
| WPA Algorithms | ○ TKIP ○ AES ○ TKIPAES |
| Pass Phrase | 12345678 |
| Key Renewal Interval | 3600 seconds |

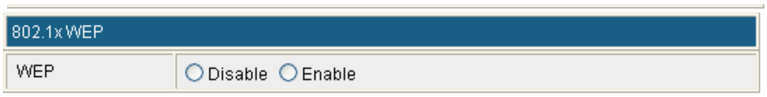
**WPA Algorithms**: Select the type of algorithm, TKIP or AES for WP-PSK, and TKIP, AES or TKIP AES for WPA2-PSK, WPA PSK WPA2 PSK.
**Pass Phrase**: Enter the pass phrase 8~63 ASCII characters in the column.

**Key Renewal Interval**: Enter the renewal security time (seconds) in the column. Default is 3600 seconds. Set 0 to disable re-key.

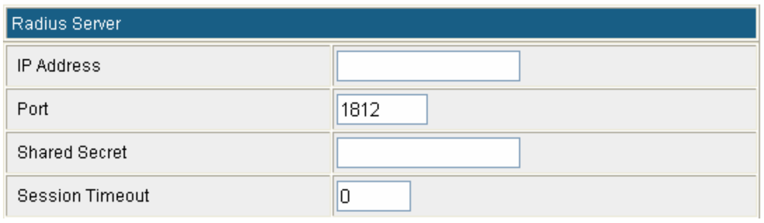
**802.1x**



| "GENERIC" | |
|---|---|
| Security Mode | 802.1X |



| 802.1x WEP | |
|---|---|
| WEP | ○ Disable ○ Enable |



| Radius Server | |
|---|---|
| IP Address | |
| Port | 1812 |
| Shared Secret | |
| Session Timeout | 0 |

**WEP**: Select Disable or Enable to this function.

**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 Wireless Router shares with the RADIUS Server.

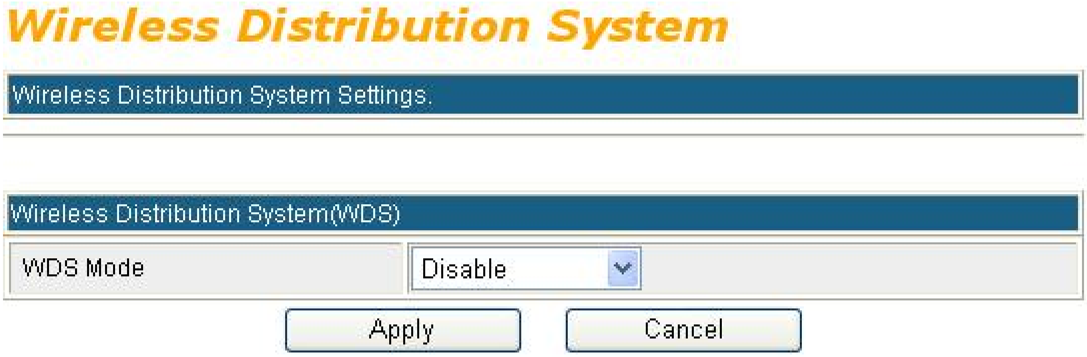
**Session Timeout**: Session timeout interval is for 802.1x re-authentication setting. Set to zero to disable 802.1x re-authentication service for each session. Session timeout interval unit is second and must be larger than 60.

| **Access Policy** | |
|---|---|
| **Policy** | Set access control policy of the stations. Select Disable, Allow or Reject form the pull-down menu. The policy supports 8 sets MAC for each SSID. |
| **Add a station Mac** | Enter a station MAC in the blank field. |

## WDS

To use WDS function:

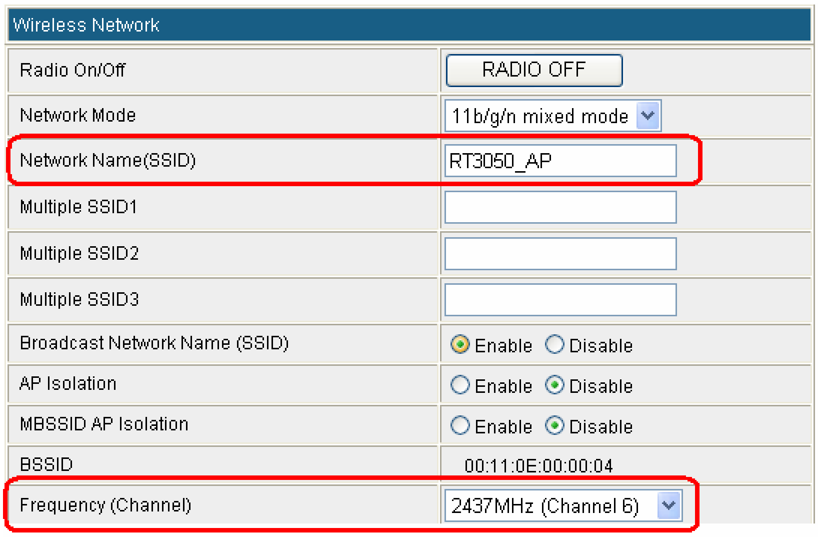
1. The APs must support WDS function.
   (To set WDS must use the same **wireless products** (the same **model** will be better); due to different wireless products might support different WDS settings. Thus, it is suggested that to use the same wireless products that support WDS function.)
2. To set the same **SSID** on the APs.
3. To set the same **channel** on the APs.
4. To set the same **Wireless MAC address(BSSID)** on the APs.
5. To set same **security** (WEP or WPA) on the APs.

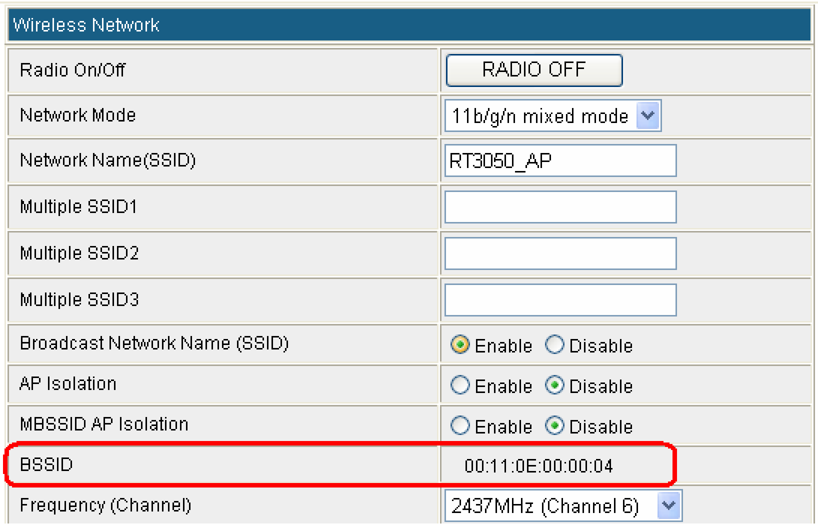


Wireless Distribution System

Wireless Distribution System Settings.

| Wireless Distribution System(WDS) | |
|---|---|
| WDS Mode | Disable |

| Wireless Distribution System (WDS) | |
|---|---|
| **WDS Mode** | Select the mode from the pull-down menu, **Disable, Lazy Mode, Bridge Mode** or **Repeater Mode**. (Default WDS mode is Disable.)<br>If the users would like to set up the WDS function, please go to **Wireless Settings> Basic** to set up APs that should use the same **SSID** and **Channel** , then go back to **Wireless settings> WDS** to enter **Wireless MAC(BSSID)** of each other to make the WDS connection.<br>**Step 1**: Setup the same **SSID** and **Channel** on wireless APs.<br><br>Wireless Network<br>Radio On/Off: RADIO OFF<br>Network Mode: 11b/g/n mixed mode<br>Network Name(SSID): RT3050_AP<br>Multiple SSID1:<br>Multiple SSID2:<br>Multiple SSID3:<br>Broadcast Network Name (SSID): ● Enable ○ Disable<br>AP Isolation: ○ Enable ● Disable<br>MBSSID AP Isolation: ○ Enable ● Disable<br>BSSID: 00:11:0E:00:00:04<br>Frequency (Channel): 2437MHz (Channel 6)<br>**Step 2**: Enter **Wireless MAC (BSSID) address** to each other. (According to the WDS mode that user selected, for example, Lazy mode is unnecessary to enter another AP's MAC address.) |

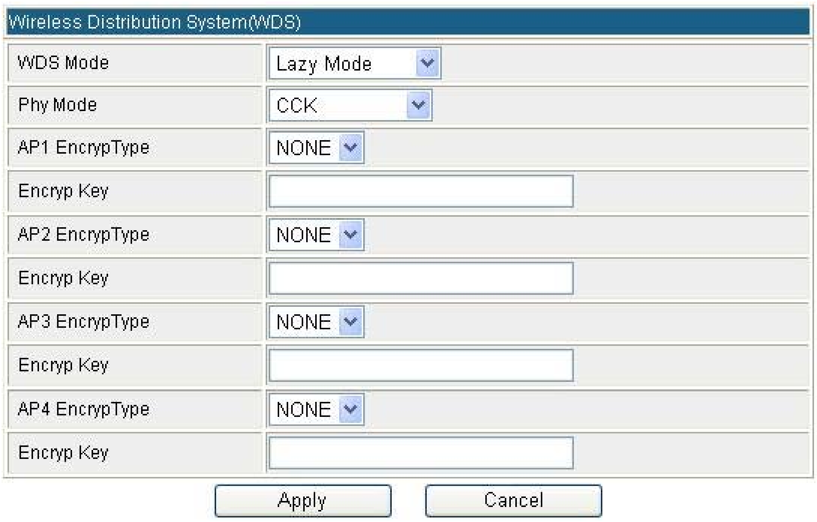


Wireless Network

| | |
|---|---|
| Radio On/Off | RADIO OFF |
| Network Mode | 11b/g/n mixed mode |
| Network Name(SSID) | RT3050_AP |
| Multiple SSID1 | |
| Multiple SSID2 | |
| Multiple SSID3 | |
| Broadcast Network Name (SSID) | ● Enable ○ Disable |
| AP Isolation | ○ Enable ● Disable |
| MBSSID AP Isolation | ○ Enable ● Disable |
| BSSID | 00:11:0E:00:00:04 |
| Frequency (Channel) | 2437MHz (Channel 6) |

## Lazy Mode

If Lazy mode be selected, it is unnecessary to set up Wireless MAC address here, just go to set up Wireless MAC address on the other wireless AP then WDS function will be active.



Wireless Distribution System(WDS)

| | |
|---|---|
| WDS Mode | Lazy Mode |
| Phy Mode | CCK |
| AP1 EncrypType | NONE |
| Encryp Key | |
| AP2 EncrypType | NONE |
| Encryp Key | |
| AP3 EncrypType | NONE |
| Encryp Key | |
| AP4 EncrypType | NONE |
| Encryp Key | |

**Phy Mode:** Select CCK(11b mode), OFDM(11g mode), HTMIX(11b/g/n mixed mode) or GREENFIELD(11n mode) from the pull-down menu. Each APs should be setup to the same Phy mode.

**AP1~AP4 Encrypt Type:** Users should go to the main web page of the Wireless Router **Wireless settings > Security** page to set up security mode under **Open, Shared, WEP Auto, WPA, WPA-PSK, WPA2, WPA2-PSK, WPA-PSK/ WPA2-PSK, WPA/WPA2**.
Select **NONE, WEP, TKIP** and **AES** encryption type from pull-down menu. (Default encryption type is NONE.)

**Encrypt Key:** Enter the corresponding encryption keys in the field.

Select the type of **Open, Shared, WEP Auto** authentication, for **WEP** encryption.

- **Hexadecimal (WEP 64 bits):** 10 Hex characters (0~9, a~f).
- **Hexadecimal (WEP 128 bits):** 26 Hex characters (0~9, a~f).

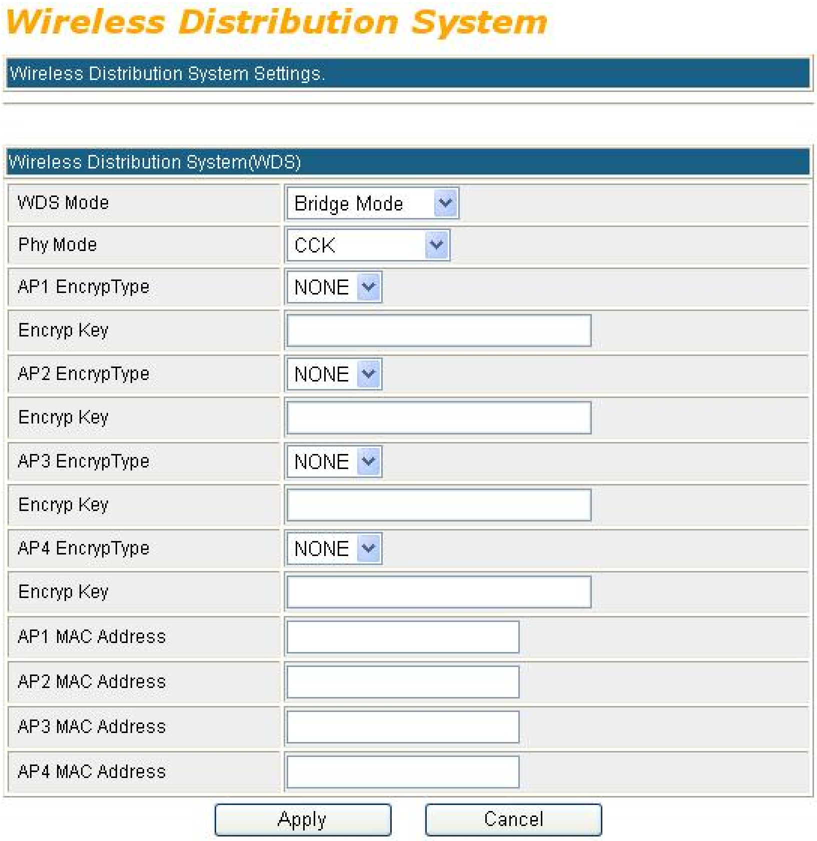
- **ASCII (WEP 64 bits):** 5 ASCII characters (case-sensitive).
- **ASCII (WEP 128 bits):** 13 ASCII characters (case-sensitive).

Select the type **WPA, WPA-PSK, WPA2, WPA2-PSK**, **WPA-PSK/ WPA2-PSK, WPA/WPA2** authentication, for **TKIP** or **AES** encryption.

If users select TKIP or AES encryption, please enter the password in the Encryption Key column that must be filled with characters longer than 8 and less than 64 lengths to set up the security.

## Bridge Mode

If the Bridge mode be selected, set up Wireless MAC address to each other to enable WDS function.



Wireless Distribution System

Wireless Distribution System Settings.

Wireless Distribution System(WDS)

| | |
|---|---|
| WDS Mode | Bridge Mode |
| Phy Mode | CCK |
| AP1 EncrypType | NONE |
| Encryp Key | |
| AP2 EncrypType | NONE |
| Encryp Key | |
| AP3 EncrypType | NONE |
| Encryp Key | |
| AP4 EncrypType | NONE |
| Encryp Key | |
| AP1 MAC Address | |
| AP2 MAC Address | |
| AP3 MAC Address | |
| AP4 MAC Address | |

**Phy Mode:** Select CCK(11b mode), OFDM(11g mode), HTMIX(11b/g/n mixed mode) or GREENFIELD(11n mode) from the pull-down menu. Each AP should be setup to the same Phy mode.

**AP1~AP4 Encrypt Type:** Users should go to the main web page of the Wireless Router **Wireless settings > Security** page to set up security mode under **Open, Shared, WEP Auto, WPA, WPA-PSK, WPA2, WPA2-PSK**, **WPA-PSK/ WPA2-PSK, WPA/WPA2**.
Select **NONE, WEP, TKIP** and **AES** encryption type from pull-down menu. (Default encryption type is NONE.)

**Encrypt Key:** Enter the corresponding encryption keys in the field.
Select the type of **Open, Shared, WEP Auto** authentication, for **WEP** encryption.

- **Hexadecimal (WEP 64 bits):** 10 Hex characters (0~9, a~f).

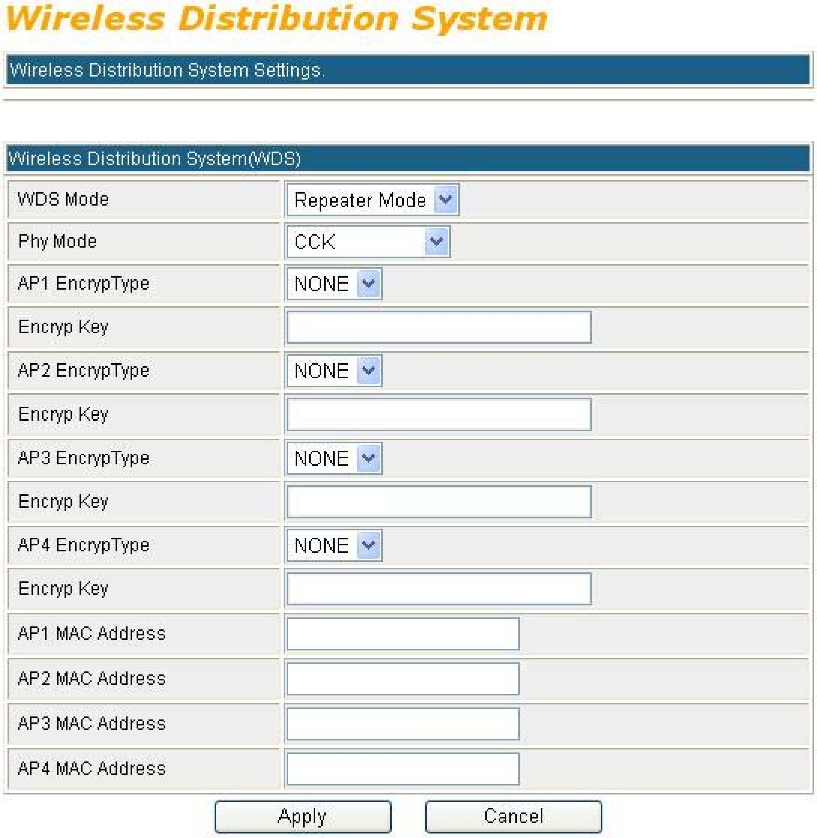
- **Hexadecimal (WEP 128 bits):** 26 Hex characters (0~9, a~f).
- **ASCII (WEP 64 bits):** 5 ASCII characters (case-sensitive).
- **ASCII (WEP 128 bits):** 13 ASCII characters (case-sensitive).

Select the type **WPA, WPA-PSK, WPA2, WPA2-PSK**, **WPA-PSK/ WPA2-PSK, WPA/WPA2** authentication, for **TKIP** or **AES** encryption. If users select TKIP or AES encryption, please enter the password in the Encryption Key column that must be filled with characters longer than 8 and less than 64 lengths to set up the security.

**AP1~AP4 MAC Address:** Enter **Wireless MAC** of each other to make the WDS connection.

### Repeater Mode

If the Repeater mode be selected, set up Wireless MAC address to each other to enable WDS function.



Wireless Distribution System

Wireless Distribution System Settings.

| Wireless Distribution System(WDS) | |
|---|---|
| WDS Mode | Repeater Mode |
| Phy Mode | CCK |
| AP1 EncrypType | NONE |
| Encryp Key | |
| AP2 EncrypType | NONE |
| Encryp Key | |
| AP3 EncrypType | NONE |
| Encryp Key | |
| AP4 EncrypType | NONE |
| Encryp Key | |
| AP1 MAC Address | |
| AP2 MAC Address | |
| AP3 MAC Address | |
| AP4 MAC Address | |

**Phy Mode:** Select CCK(11b mode), OFDM(11g mode), HTMIX(11b/g/n mixed mode) or GREENFIELD(11n mode) from the pull-down menu. Each AP should be setup to the same Phy mode.

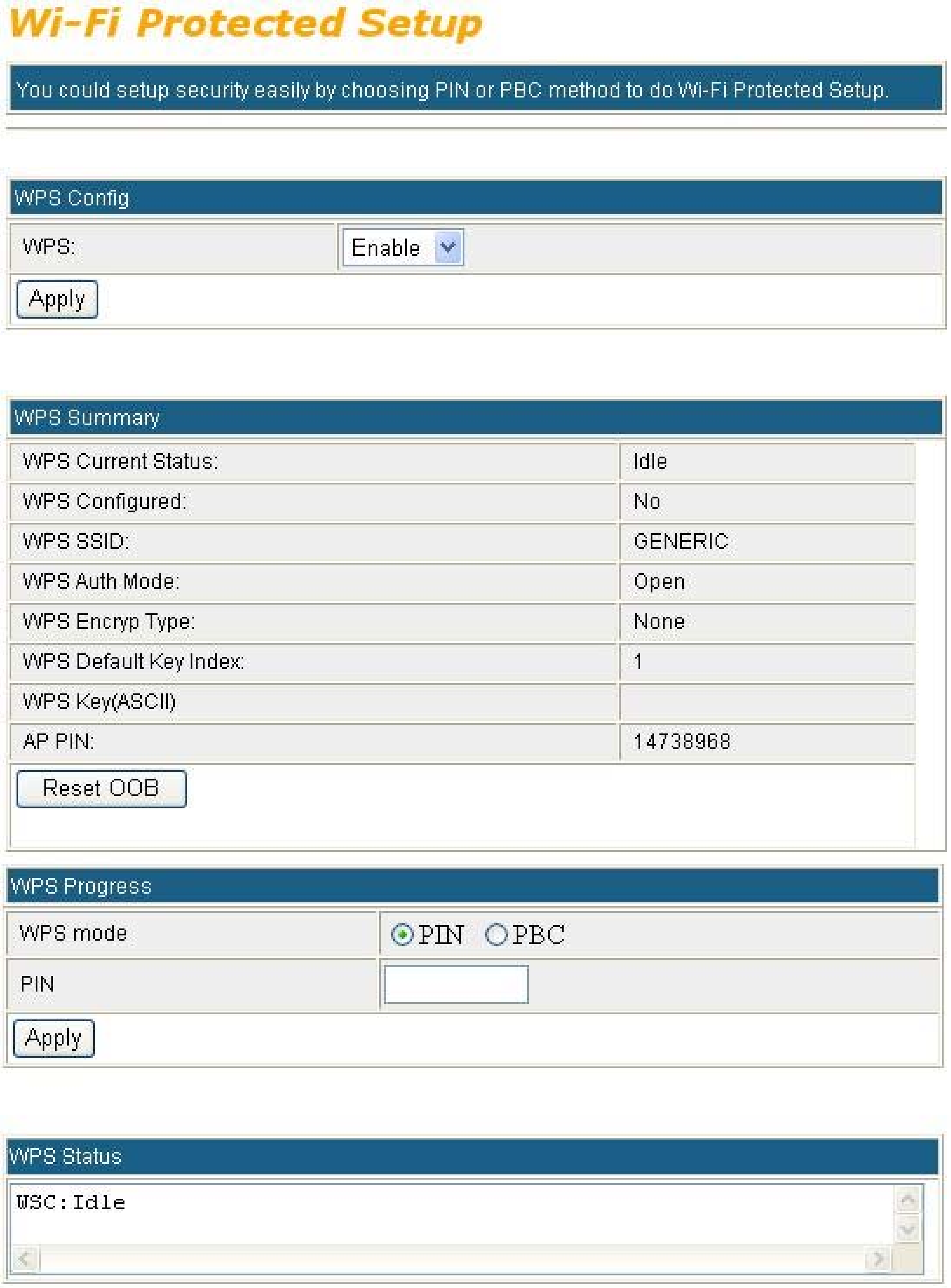
**AP1~AP4 Encrypt Type:** Users should go to the main web page of the Wireless Router **Wireless settings > Security** page to set up security mode under **Open, Shared, WEP Auto, WPA, WPA-PSK, WPA2, WPA2-PSK**, **WPA-PSK/ WPA2-PSK, WPA/WPA2**.
Select **NONE, WEP, TKIP** and **AES** encryption type from pull-down menu. (Default encryption type is NONE.)

**Encrypt Key:** Enter the corresponding encryption keys in the field.
Select the type of **Open, Shared, WEP Auto** authentication, for **WEP** encryption.

- **Hexadecimal (WEP 64 bits):** 10 Hex characters (0~9, a~f).

| | |
|---|---|
| | ● **Hexadecimal (WEP 128 bits):** 26 Hex characters (0~9, a~f).<br>● **ASCII (WEP 64 bits):** 5 ASCII characters (case-sensitive).<br>● **ASCII (WEP 128 bits):** 13 ASCII characters (case-sensitive).<br>Select the type **WPA, WPA-PSK, WPA2, WPA2-PSK**, **WPA-PSK/ WPA2-PSK, WPA/WPA2** authentication, for **TKIP** or **AES** encryption. If users select TKIP or AES encryption, please enter the password in the Encryption Key column that must be filled with characters longer than 8 and less than 64 lengths to set up the security.<br>**AP1~AP4 MAC Address:** Enter **Wireless MAC** of each other to make the WDS connection. |

## WPS



Wi-Fi Protected Setup

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

| WPS Config | |
|---|---|
| WPS: | Enable |

Apply

| WPS Summary | |
|---|---|
| WPS Current Status: | Idle |
| WPS Configured: | No |
| WPS SSID: | GENERIC |
| WPS Auth Mode: | Open |
| WPS Encryp Type: | None |
| WPS Default Key Index: | 1 |
| WPS Key(ASCII) | |
| AP PIN: | 14738968 |

Reset OOB

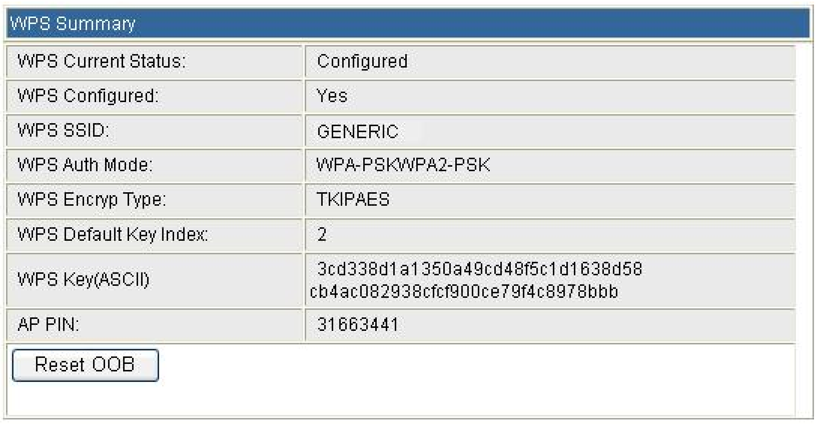
| WPS Progress | |
|---|---|
| WPS mode | ● PIN ○ PBC |
| PIN | |

Apply

WPS Status

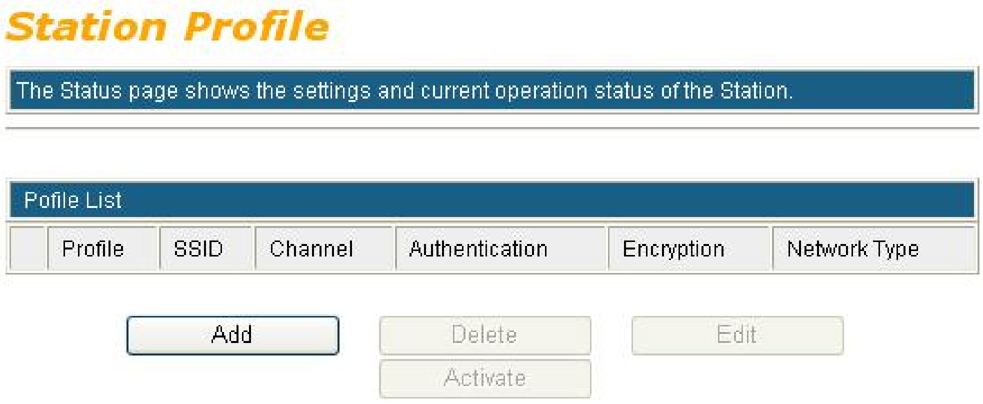
```
WSC:Idle
```

| WPS Config | |
|---|---|
| **WPS** | To use WPS (Wi-Fi Protected Setup) function, push physical WPS button on Wireless Router to make a WPS connection. Default setting is **Enable**. |
| **WPS Summary** | |
| **WPS Current Status** | After enabling the WPS function, if there is a connection the status will show Configured, otherwise, will show Idle. |

| | |
|---|---|
| **WPS Configured** | Trigger WPS AP to do simple config with WPS Client. If WPS configured, here shows Yes, otherwise, NO.<br><br>WPS Summary<br>WPS Current Status: Configured<br>WPS Configured: Yes<br>WPS SSID: GENERIC<br>WPS Auth Mode: WPA-PSKWPA2-PSK<br>WPS Encryp Type: TKIPAES<br>WPS Default Key Index: 2<br>WPS Key(ASCII): 3cd338d1a1350a49cd48f5c1d1638d58 cb4ac082938cfcf900ce79f4c8978bbb<br>AP PIN: 31663441<br> |
| **WPS SSID** | Shows the Wireless Router network name. |
| **WPS Auth Mode** | The WPS authentication type supports **Open, Shared, WEP Auto, WPA-PSK, WPA2, WPA2-PSK**, **WPA-PSK/ WPA2-PSK**. Please go to the configuration page **Wireless Settings > Security** to set up the WPS security. |
| **WPS Encryp Type** | For **Open** authentication mode, the selection of encryption type are **NONE** and **WEP**. For **WPA-PSK, WPA2-PSK** and **WPA-PSK/ WPA2-PSK** authentication mode, the encryption type supports **TKIP, AES** and **TKIP/AES**. |
| **WPS Default Key Index** | Shows the WEP default key (1~4). |
| **WPS Key(ASCII)** | Shows the WPS security keys (ASCII). The key can be used to ensure the security of the wireless network. |
| **AP PIN** | Here shows the AP's PIN code (Personal Identification Number) that the enrollee should enter the registrar's PIN code to make a connection. |
| **Reset OOB** | Reset WPS AP to stop the (OOB, out-of-box) configuration. |
| **WPS Process** | |
| **WPS mode** | **PIN**: **Personal Identification Number**. Select PIN then click **Apply** to make a WPS connection.<br>**PBC**: **Push Button Communication**. Select PBC then click **Apply** to make a WPS connection. |
| **PIN** | Personal Identification Number. Input Enrollee's Pin Code to AP-Registrar. |
| **WPS Status** | Here shows the current status of the WPS. If there is connection the status shows WSC Success, otherwise, shows Idle. |

# Client Mode

## Profile



Station Profile

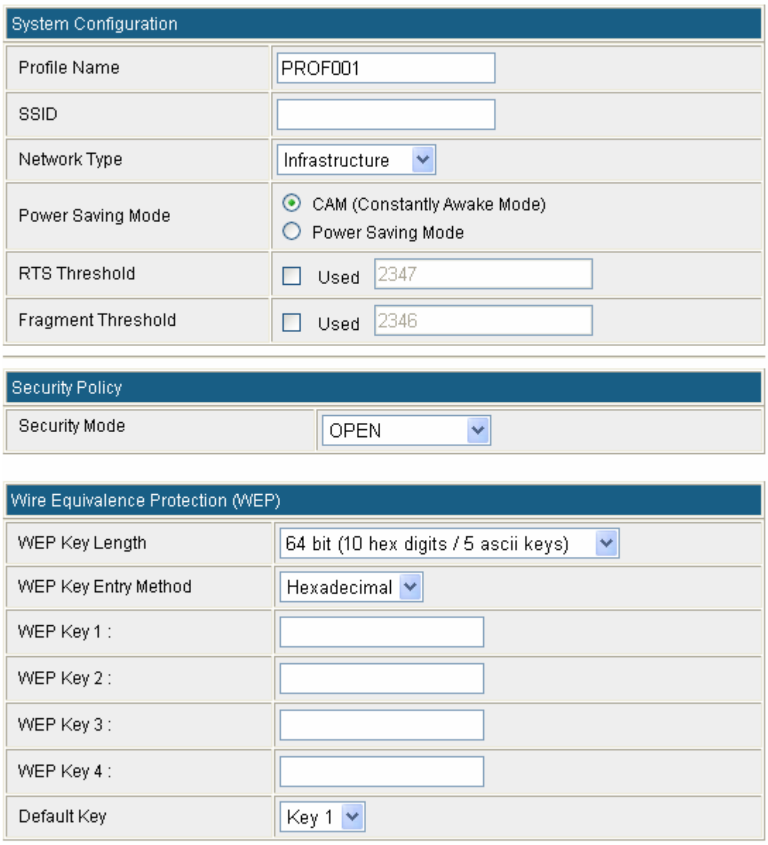
The Status page shows the settings and current operation status of the Station.

Pofile List

| | Profile | SSID | Channel | Authentication | Encryption | Network Type |
|---|---|---|---|---|---|---|

**Add**

Click **Add** button to set the station profile.



System Configuration

| | |
|---|---|
| Profile Name | PROF001 |
| SSID | |
| Network Type | Infrastructure |
| Power Saving Mode | ● CAM (Constantly Awake Mode)<br>○ Power Saving Mode |
| RTS Threshold | □ Used 2347 |
| Fragment Threshold | □ Used 2346 |

Security Policy

| | |
|---|---|
| Security Mode | OPEN |

Wire Equivalence Protection (WEP)

| | |
|---|---|
| WEP Key Length | 64 bit (10 hex digits / 5 ascii keys) |
| WEP Key Entry Method | Hexadecimal |
| WEP Key 1 : | |
| WEP Key 2 : | |
| WEP Key 3 : | |
| WEP Key 4 : | |
| Default Key | Key 1 |

**Profile Name**: Default profile name is PROF001, or enter desired profile name here.

**SSID**: Enter the network name (case-sensitive) of the access point or station.

**Network Type**: Select **Infrastructure** or **802.11 Ad Hoc** from the pull-down list. Infrastructure type to make a connection via a access point; 802.11 Ad Hoc to make a connection directly between stations.

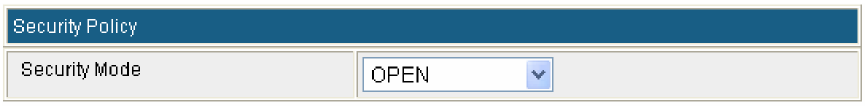
**Power Saving Mode**: CAM (Constantly Awake Mode) or Power Saving Mode.

**RTS Threshold**: Check the box to use the function. The maximum is 2347.

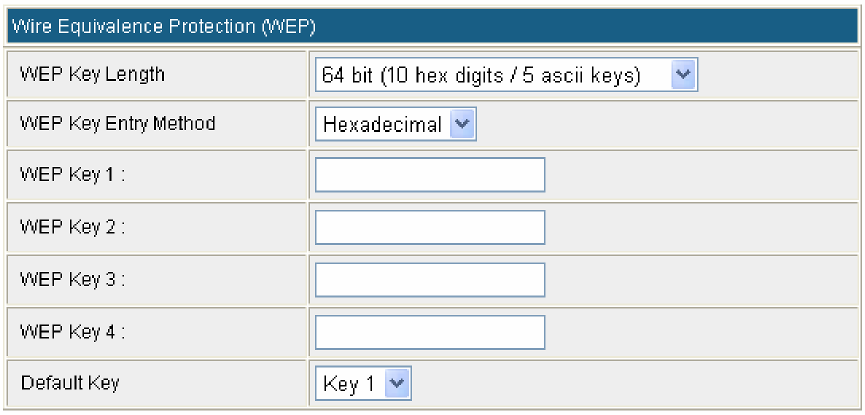
**Fragment Threshold**: Check the box to use the function. The maximum is 2346.

**Security Mode**: Select the security **OPEN, SHARED, WPA-Personal** or **WPA2-Personal** form the pull-down menu.

**OPEN/SHARED**



| Security Policy | |
|---|---|
| Security Mode | OPEN |



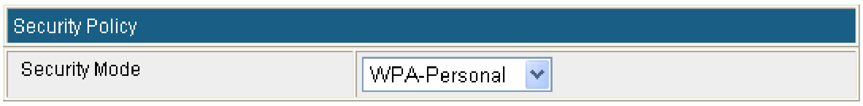
| Wire Equivalence Protection (WEP) | |
|---|---|
| WEP Key Length | 64 bit (10 hex digits / 5 ascii keys) |
| WEP Key Entry Method | Hexadecimal |
| WEP Key 1 : | |
| WEP Key 2 : | |
| WEP Key 3 : | |
| WEP Key 4 : | |
| Default Key | Key 1 |

**WEP Key Length/ WEP Key Entry Method**: Only valid when using **WEP** encryption algorithm. There are several formats to enter the keys.

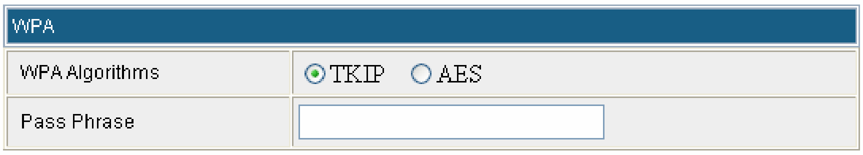
- **Hexadecimal (64 bits)**: 10 Hex characters.
- **Hexadecimal (128 bits)**: 26 Hex characters.
- **ASCII (64 bits)**: 5 ASCII characters.
- **ASCII (128 bits)**: 13 ASCII characters.

**WEP Key 1~4**: Enter the password in the encryption key field that the encryption key number must match the selected Tx key.
**Default Key**: There are four keys 1~4 that you can select at will. All computers, access points, and wireless adapters must use the same key when making a connection.

**WPA-Personal / WPA2-Personal**



| Security Policy | |
|---|---|
| Security Mode | WPA-Personal |



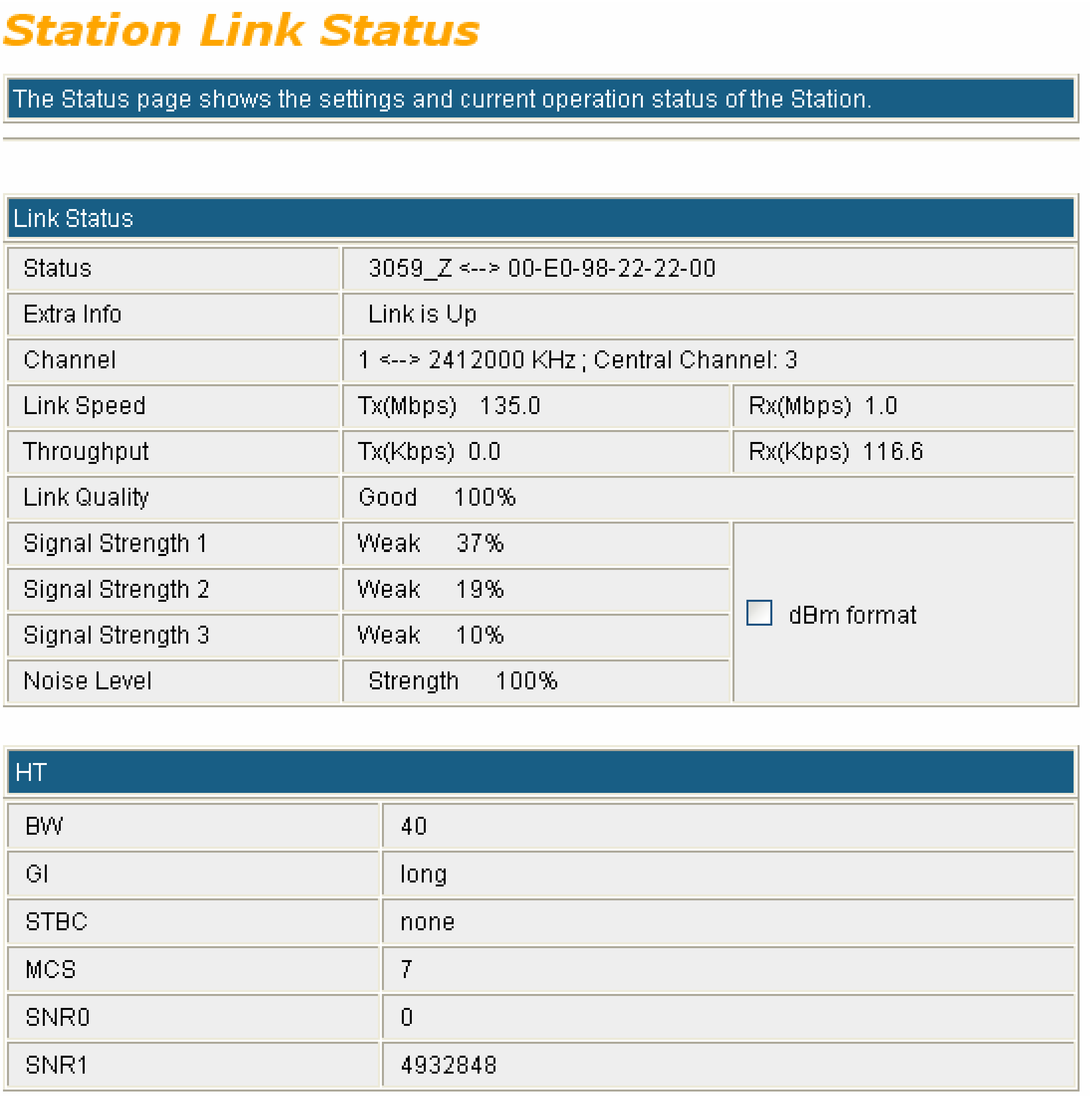
| WPA | |
|---|---|
| WPA Algorithms | ● TKIP ○ AES |
| Pass Phrase | |

**WPA Algorithms:** Select TKIP or AES encryption algorithm.

**Pass Phrase:** Enter the pass phrase 8~63 ASCII or 64 HEX characters in the column.

## Link Status

After making a connection with an AP, this page will show the related link status, check the **dBm format** box to show the Signal Strength and Noise Level information in dBm format.



Station Link Status

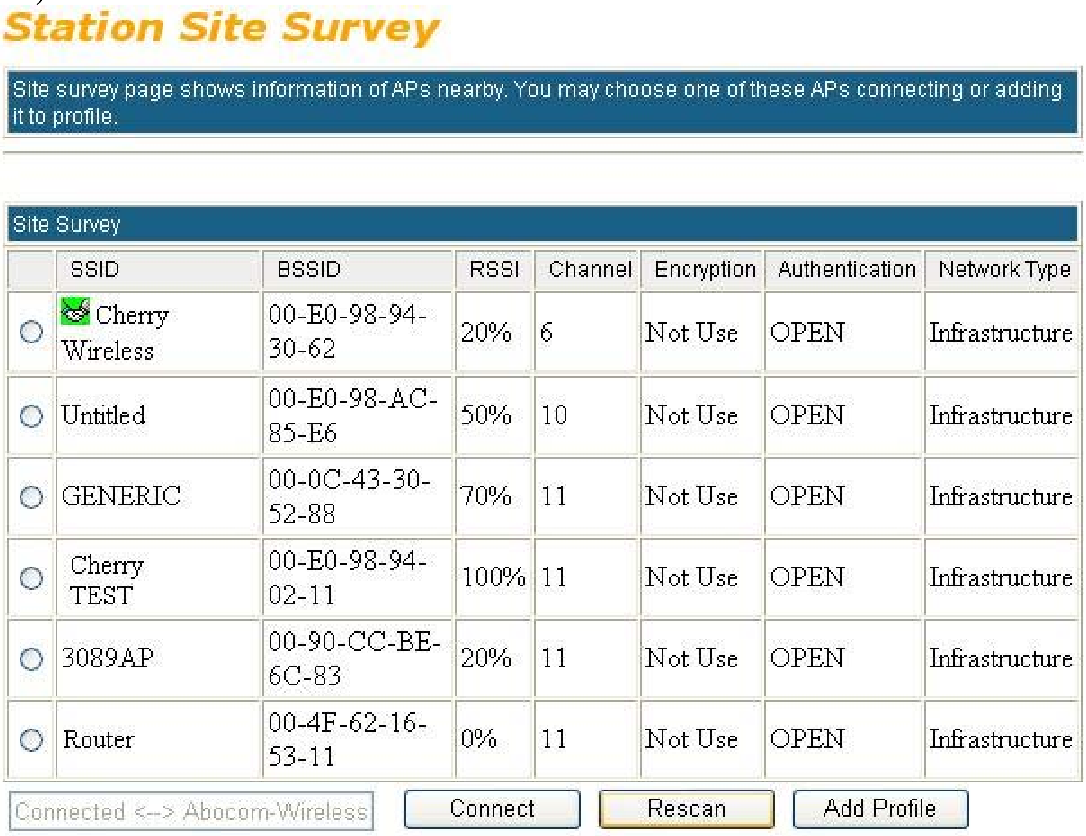
The Status page shows the settings and current operation status of the Station.

| Link Status | | |
|---|---|---|
| Status | 3059_Z <--> 00-E0-98-22-22-00 | |
| Extra Info | Link is Up | |
| Channel | 1 <--> 2412000 KHz ; Central Channel: 3 | |
| Link Speed | Tx(Mbps) 135.0 | Rx(Mbps) 1.0 |
| Throughput | Tx(Kbps) 0.0 | Rx(Kbps) 116.6 |
| Link Quality | Good 100% | |
| Signal Strength 1 | Weak 37% | □ dBm format |
| Signal Strength 2 | Weak 19% | |
| Signal Strength 3 | Weak 10% | |
| Noise Level | Strength 100% | |

| HT | |
|---|---|
| BW | 40 |
| GI | long |
| STBC | none |
| MCS | 7 |
| SNR0 | 0 |
| SNR1 | 4932848 |

## Site Survey

Here shows the AP nearby, select desired AP to make a connection. Click **Rescan** button to survey the APs. Select preferred AP, then click **Connect** button to make a connection. And you can also set the preferred AP in to profile, click **Add Profile** to add (Please refer to Profile section for station profile add.)



Station Site Survey

Site survey page shows information of APs nearby. You may choose one of these APs connecting or adding it to profile.

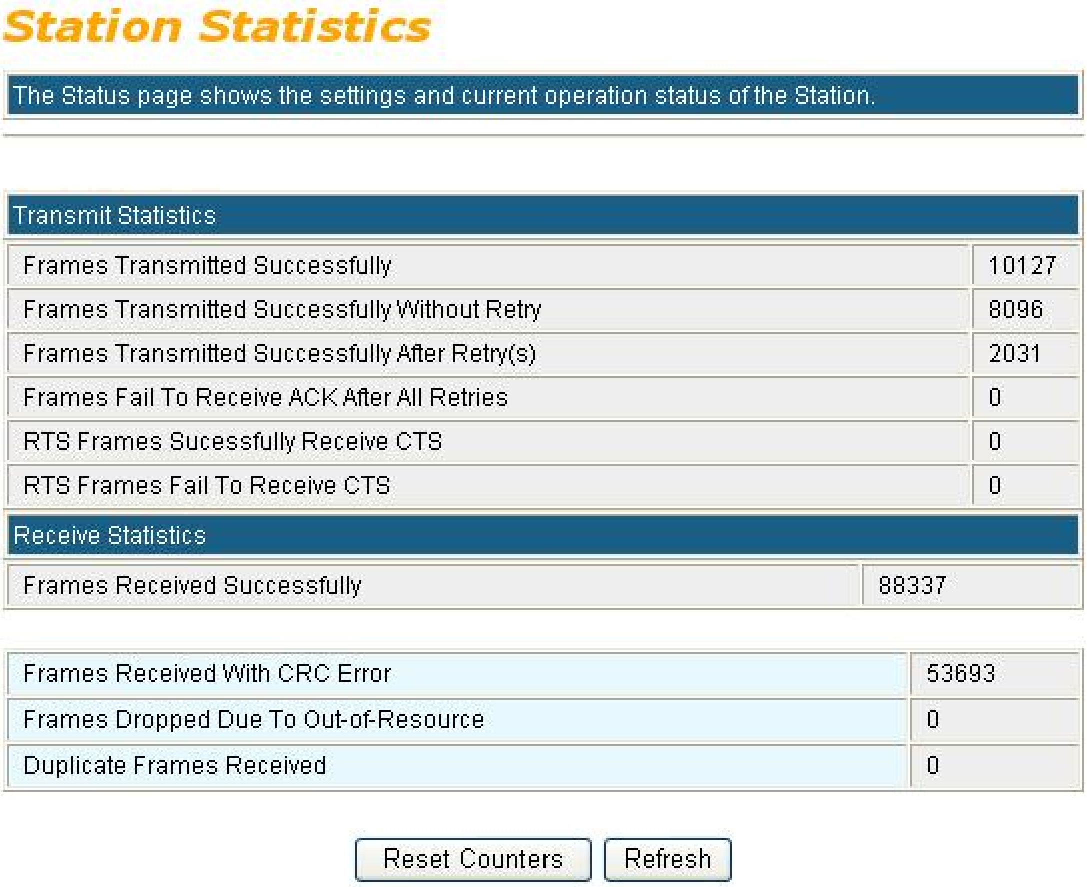
Site Survey

| | SSID | BSSID | RSSI | Channel | Encryption | Authentication | Network Type |
|---|---|---|---|---|---|---|---|
| ○ | Cherry Wireless | 00-E0-98-94-30-62 | 20% | 6 | Not Use | OPEN | Infrastructure |
| ○ | Untitled | 00-E0-98-AC-85-E6 | 50% | 10 | Not Use | OPEN | Infrastructure |
| ○ | GENERIC | 00-0C-43-30-52-88 | 70% | 11 | Not Use | OPEN | Infrastructure |
| ○ | Cherry TEST | 00-E0-98-94-02-11 | 100% | 11 | Not Use | OPEN | Infrastructure |
| ○ | 3089AP | 00-90-CC-BE-6C-83 | 20% | 11 | Not Use | OPEN | Infrastructure |
| ○ | Router | 00-4F-62-16-53-11 | 0% | 11 | Not Use | OPEN | Infrastructure |

Connected <--> Abocom-Wireless

## Statistics

This screen displays the transmission and reception statistics on your current networks.



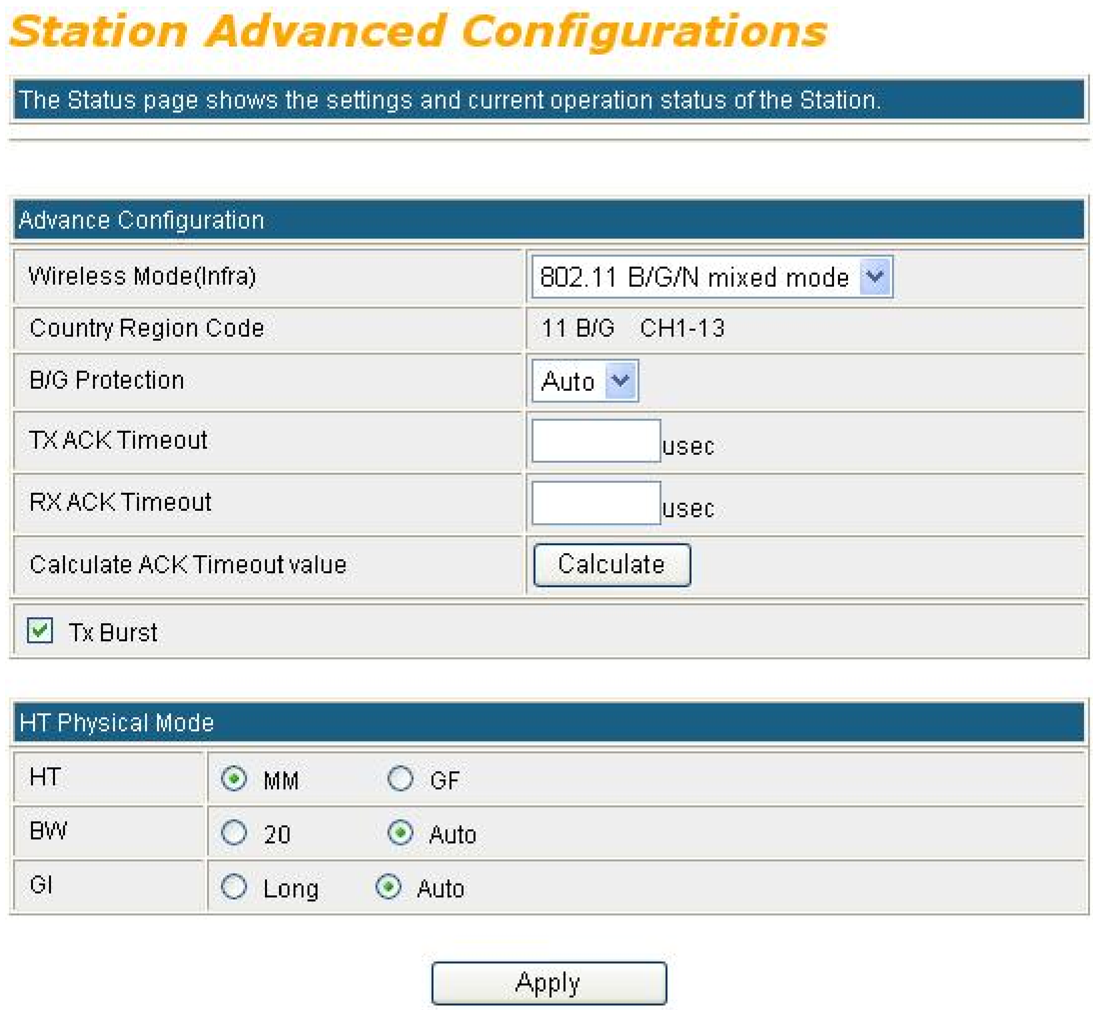
Station Statistics

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

| Transmit Statistics | |
|---|---|
| Frames Transmitted Successfully | 10127 |
| Frames Transmitted Successfully Without Retry | 8096 |
| Frames Transmitted Successfully After Retry(s) | 2031 |
| Frames Fail To Receive ACK After All Retries | 0 |
| RTS Frames Sucessfully Receive CTS | 0 |
| RTS Frames Fail To Receive CTS | 0 |

| Receive Statistics | |
|---|---|
| Frames Received Successfully | 88337 |
| Frames Received With CRC Error | 53693 |
| Frames Dropped Due To Out-of-Resource | 0 |
| Duplicate Frames Received | 0 |

## Advance



### Station Advanced Configurations

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

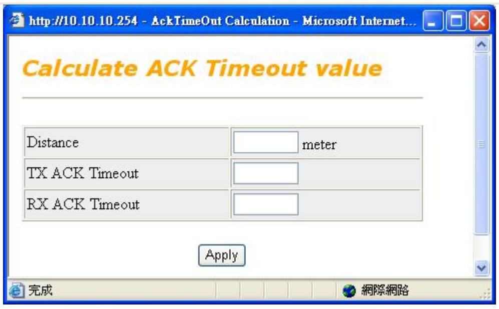
| Advance Configuration | |
|---|---|
| Wireless Mode(Infra) | 802.11 B/G/N mixed mode |
| Country Region Code | 11 B/G CH1-13 |
| B/G Protection | Auto |
| TX ACK Timeout | usec |
| RX ACK Timeout | usec |
| Calculate ACK Timeout value | Calculate |

☑ Tx Burst

| HT Physical Mode | | |
|---|---|---|
| HT | ● MM | ○ GF |
| BW | ○ 20 | ● Auto |
| GI | ○ Long | ● Auto |

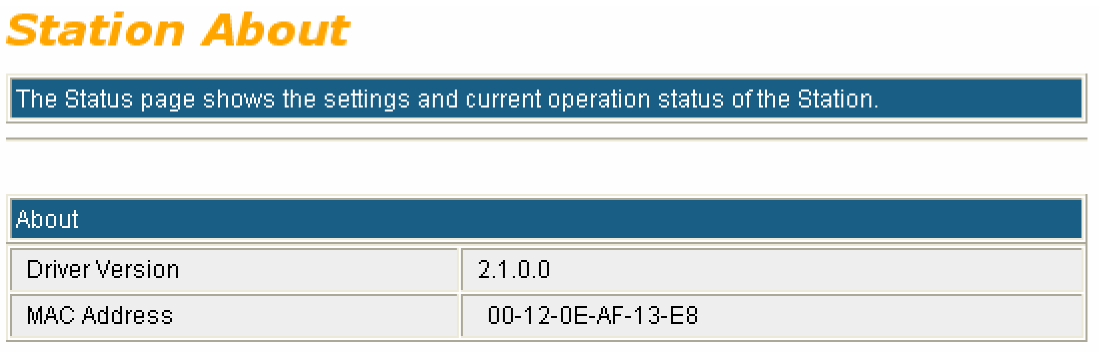
Apply

| Advance Configuration | |
|---|---|
| **Wireless Mode (Infra)** | Select 802.11 B/G/N mixed mode, 802.11B only, 802.11G only, 802.11N only, 802.11 G/N mixed mode, or 802.11 B/G mixed mode from the pull-down menu. (Default is 802.11 B/G/N mixed mode.) |
| **Country Region Code** | Here shows the channels range. |
| **B/G Protection** | Select **Auto**, **On** or **Off** from the pull-down menu. |
| **TX ACK Timeout** | ACK time out means "Acknowledgement Time Out", meaning that the system (the computer on sprint's end) didn't acknowledge your SMS in the time allotted. This is probably because of a communication error, and they'll have it fixed soon. |
| **RX ACK Timeout** | ACK time out means "Acknowledgement Time Out", meaning that the system (the computer on sprint's end) didn't acknowledge your SMS in the time allotted. This is probably because of a communication error, and they'll have it fixed soon. |

| | |
|---|---|
| **Calculate ACK Timeout value** | <br>http://10.10.10.254 - AckTimeOut Calculation - Microsoft Internet...<br>Calculate ACK Timeout value<br>Distance ___ meter<br>TX ACK Timeout ___<br>RX ACK Timeout ___<br>Apply<br>完成 網際網路 |
| **Tx Burst** | Check the box to enable the Tx Burst function. (Default Tx Burst setting is Enable.) |
| **HT Physical Mode** | |
| **HT** | Select MM or GF. Default setting is MM. |
| **BW** | **Channel Band Width**. Select 20 or Auto. (Default setting is Auto.) |
| **GI** | **Guard Interval**. Select Long or Auto. (Default setting is Auto.) |

# About

Here shows the information of the station.



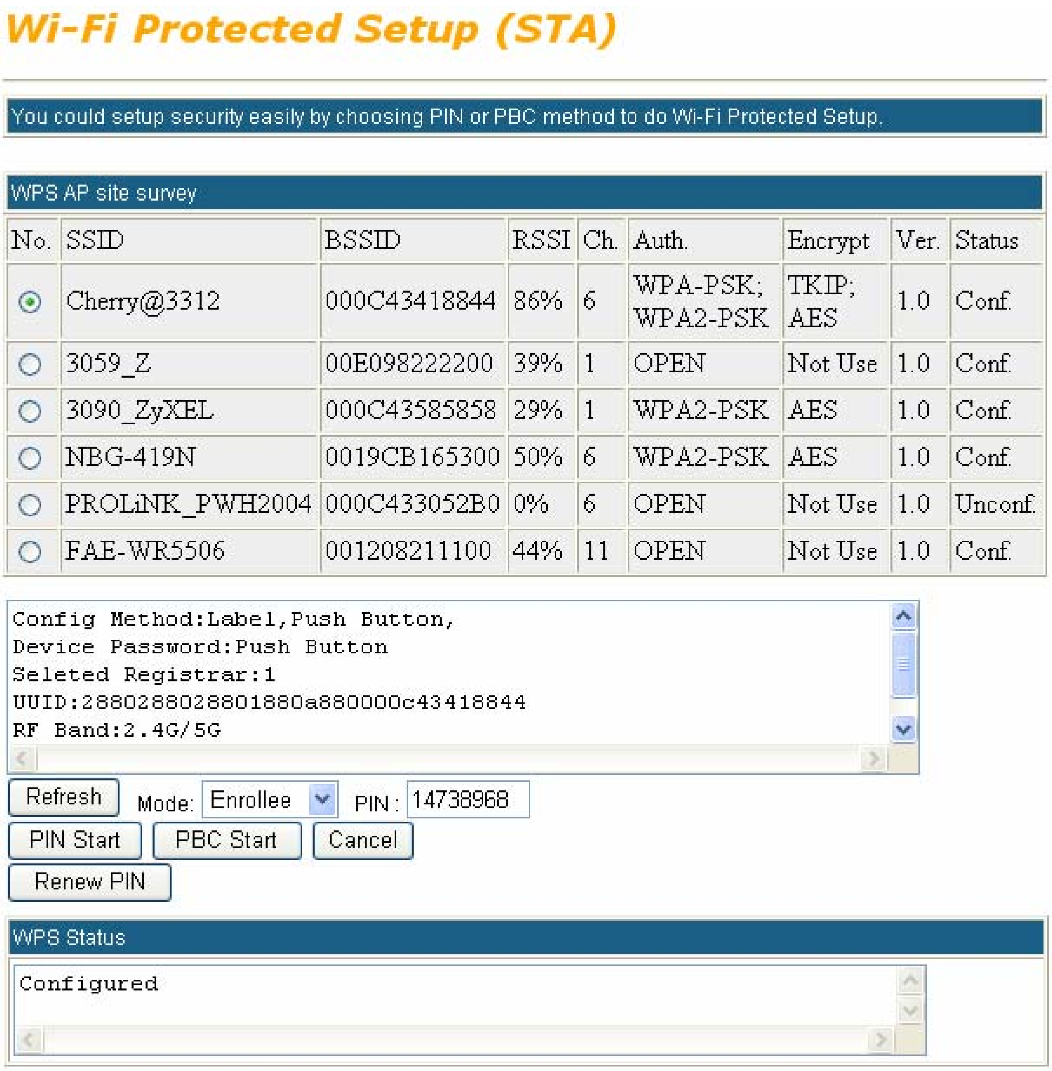
Station About

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

| About | |
|---|---|
| Driver Version | 2.1.0.0 |
| MAC Address | 00-12-0E-AF-13-E8 |

# WPS

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



Wi-Fi Protected Setup (STA)

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

WPS AP site survey

| No. | SSID | BSSID | RSSI | Ch. | Auth. | Encrypt | Ver. | Status |
|---|---|---|---|---|---|---|---|---|
| ● | Cherry@3312 | 000C43418844 | 86% | 6 | WPA-PSK;<br>WPA2-PSK | TKIP;<br>AES | 1.0 | Conf. |
| ○ | 3059_Z | 00E098222200 | 39% | 1 | OPEN | Not Use | 1.0 | Conf. |
| ○ | 3090_ZyXEL | 000C43585858 | 29% | 1 | WPA2-PSK | AES | 1.0 | Conf. |
| ○ | NBG-419N | 0019CB165300 | 50% | 6 | WPA2-PSK | AES | 1.0 | Conf. |
| ○ | PROLiNK_PWH2004 | 000C433052B0 | 0% | 6 | OPEN | Not Use | 1.0 | Unconf. |
| ○ | FAE-WR5506 | 001208211100 | 44% | 11 | OPEN | Not Use | 1.0 | Conf. |

```
Config Method:Label,Push Button,
Device Password:Push Button
Seleted Registrar:1
UUID:2880288028801880a880000c43418844
RF Band:2.4G/5G
```

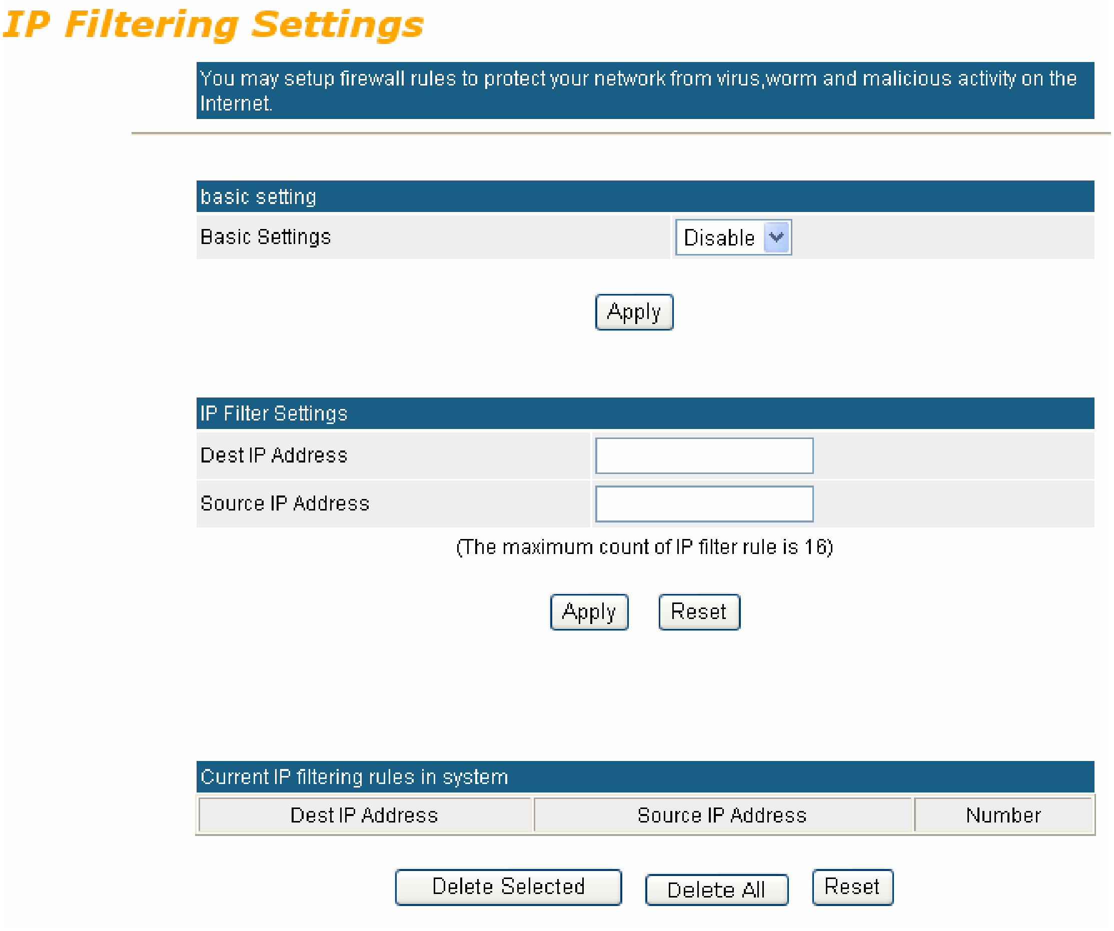
WPS Status

```
Configured
```

| | |
|---|---|
| **WPS AP Site Survey** | Display the information of surrounding APs with WPS function from last scan result. List information included SSID, BSSID(Wireless MAC address), RSSI, Channel, Authentication, Encryption, Version, and Status. |
| **Refresh** | Issue a rescan command to wireless NIC to update information on surrounding wireless network. |
| **Mode** | Select from the pull-down menu to decide the station role-playing as an Enrollee or an external Registrar.<br>**Registrar**: Add the AP's PIN code into the PIN code column, and press the device PIN button. It will connect with the AP in 2 minutes and get IP address.<br>**Enrollee**: Input the device's PIN code into the PIN code column of AP. Start AP WPS process and click device PIN button. Then, the device will connect to AP in two minutes and get IP address. |
| **PIN Start** | It is required to enter PIN (Personal Identification Number) Code (8-digit numbers) into Registrar when using PIN method. When STA is Enrollee, users can use "**Renew PIN**" button to re-generate new PIN Code. |
| **PBC Start** | **Push Button Communication**. Click **Start PBC** button to make a WPS connection within 2 minutes. |
| **Cancel** | Click **Cancel** button to discard the WPS connection. |
| **WPS Status** | Here shows the current WPS connection status. If the WPS connected successfully, here shows Configured; otherwise, Not used. |

# Firewall (GW)

## IP Filter



### IP Filtering Settings

You may setup firewall rules to protect your network from virus,worm and malicious activity on the Internet.

basic setting

| | |
|---|---|
| Basic Settings | Disable |

IP Filter Settings

| | |
|---|---|
| Dest IP Address | |
| Source IP Address | |

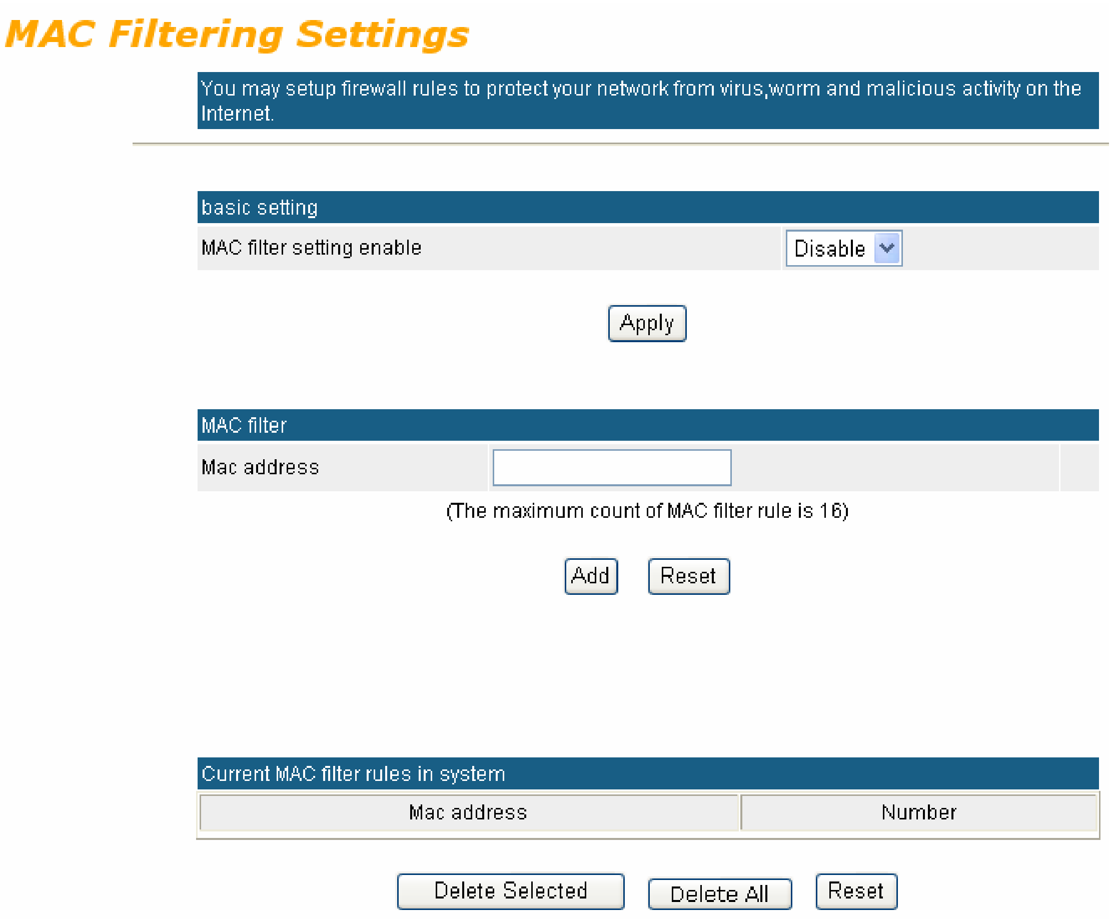
(The maximum count of IP filter rule is 16)

Current IP filtering rules in system

| Dest IP Address | Source IP Address | Number |
|---|---|---|

| | |
|---|---|
| **Basic Settings** | |
| **Basic Settings** | Select Enable or Disable from the pull-down list. |
| **IP Filter Settings** | |
| **Dest IP Address** | Enter the IP address that user would like to disconnect(drop). |
| **Source IP Address** | Enter the IP address that at the same segment with the current IP address. |
| **Apply** | Click to save and apply the current settings. |
| **Reset** | Press to discard the current settings. |
| **Current IP filtering rules in system** | |
| **Dest IP Address** | Here shows the Dest IP address that added in the filter list. |
| **Source IP Address** | Here shows the Source IP address that added in the filter list. |
| **Number** | Here shows the number that IP address listed. The maximum rule count is 16. |

# MAC Filter



MAC Filtering Settings

You may setup firewall rules to protect your network from virus,worm and malicious activity on the Internet.

basic setting

MAC filter setting enable: Disable

MAC filter

Mac address:

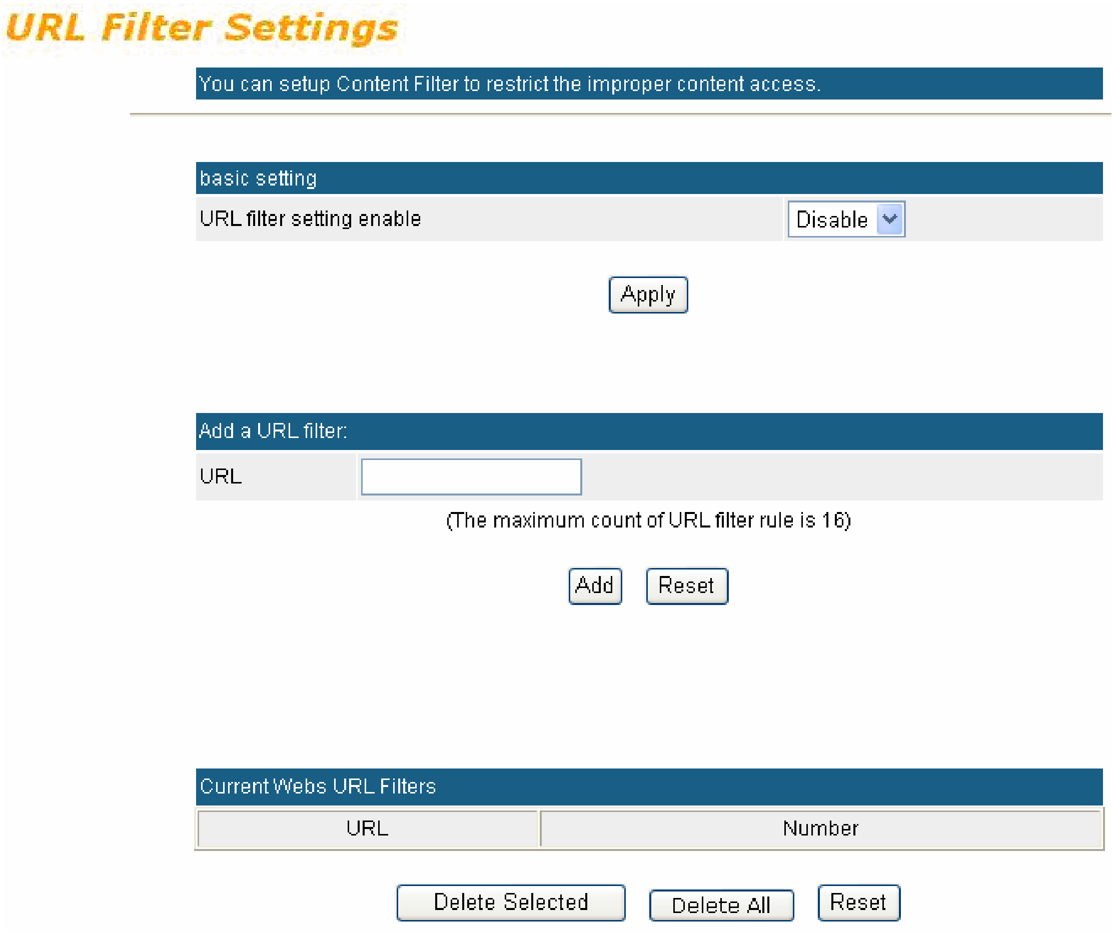
(The maximum count of MAC filter rule is 16)

Current MAC filter rules in system

| Mac address | Number |
|---|---|

| | |
|---|---|
| **Basic Settings** | |
| **MAC Filter setting enable** | Select Enable or Disable from the pull-down list. |
| **MAC Filter Settings** | |
| **MAC Address** | Enter the client MAC address that user would like to disconnect(drop). |
| **Add** | Click to save and apply the current settings. |
| **Reset** | Press to discard the current settings. |
| **Current MAC rules in system** | |
| **MAC Address** | Here shows the MAC address that added in the filter list. |
| **Number** | Here shows the number that MAC address listed. The maximum rule count is 16. |

# URL Filter



URL Filter Settings

You can setup Content Filter to restrict the improper content access.

basic setting

URL filter setting enable: Disable

Add a URL filter:

URL

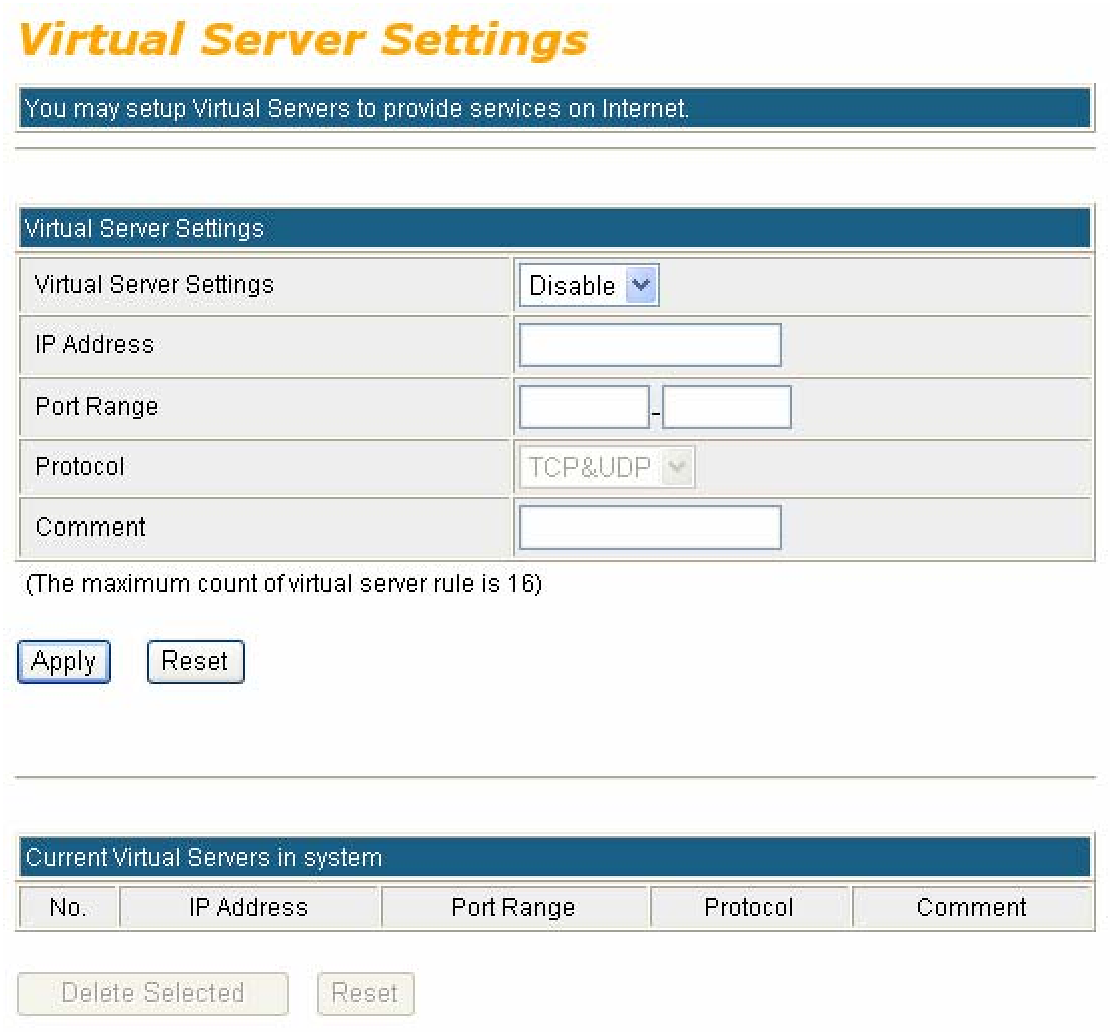
(The maximum count of URL filter rule is 16)

Current Webs URL Filters

| URL | Number |
|---|---|

| | |
|---|---|
| **Basic Settings** | |
| **URL Filter setting enable** | Select Disable or Enable from the pull-down menu. Default setting is Disable. |
| **Add a URL filter** | |
| **URL** | Enter the URL to restrict the improper content access. For example, www.xxx.com.tw. |
| **Add** | Click to save and apply the current settings. |
| **Reset** | Press to discard the current settings. |
| **Current Webs URL Filters** | |
| **URL** | Here shows the URL information that added in the URL filter list. |
| **Number** | Here shows the number that URL listed. The maximum rule count is 16. |

# Port Forwarding



## Virtual Server Settings

You may setup Virtual Servers to provide services on Internet.

| Virtual Server Settings | |
|---|---|
| Virtual Server Settings | Disable |
| IP Address | |
| Port Range | - |
| Protocol | TCP&UDP |
| Comment | |

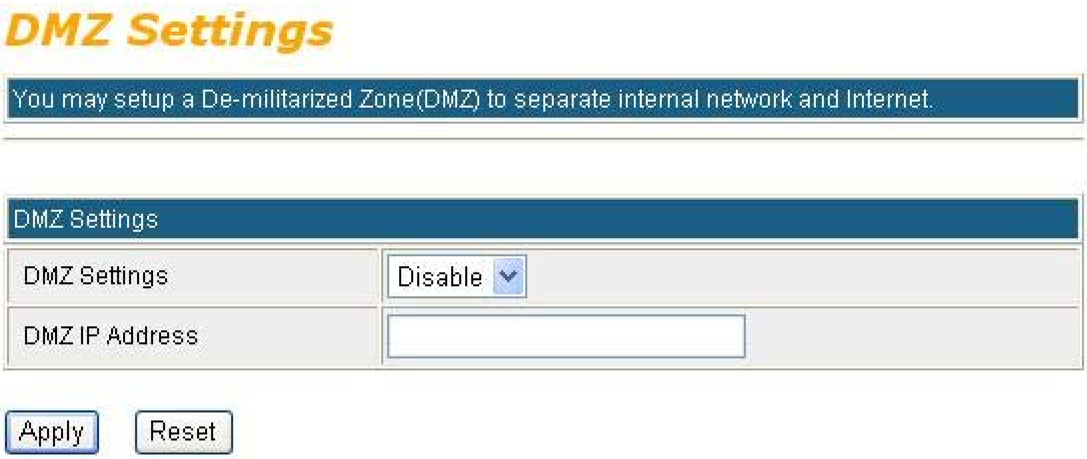
(The maximum count of virtual server rule is 16)

Current Virtual Servers in system

| No. | IP Address | Port Range | Protocol | Comment |
|---|---|---|---|---|

| Virtual Server Settings | |
|---|---|
| **Virtual Server Settings** | Select Enable or Disable from the pull-down menu. |
| **IP Address** | Enter the local server's IP address. |
| **Port Range** | For 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 server's IP address. |

# DMZ



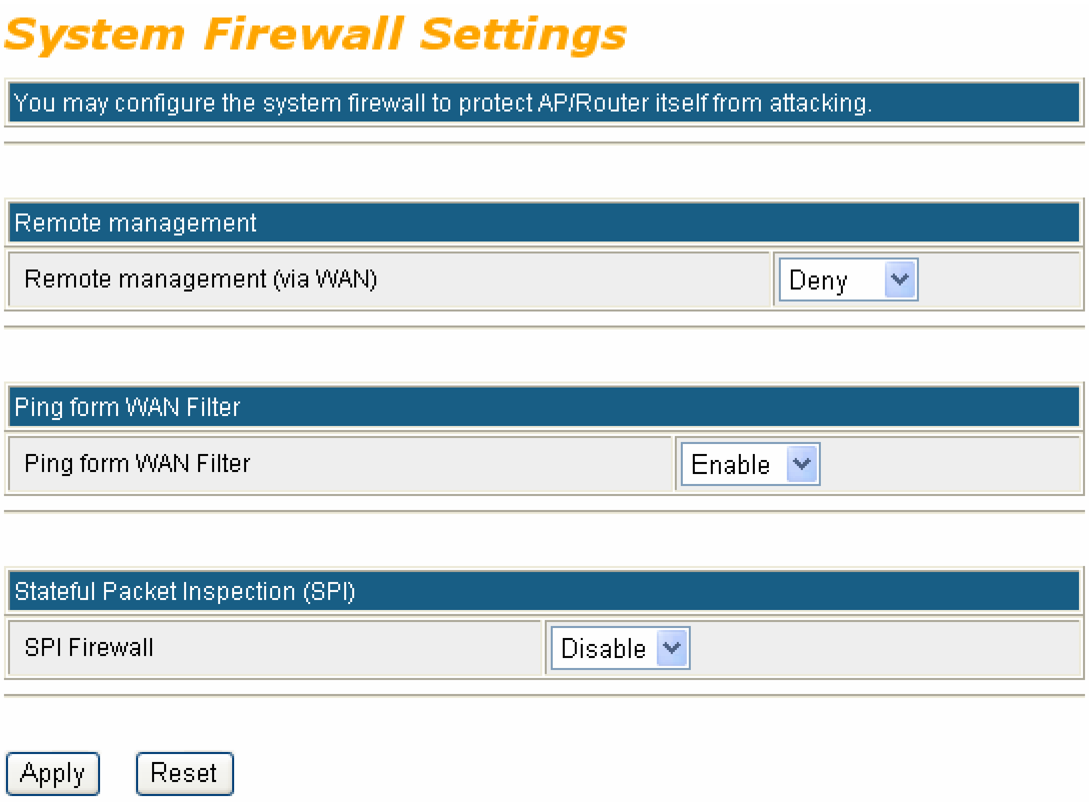
## DMZ Settings

You may setup a De-militarized Zone(DMZ) to separate internal network and Internet.

| DMZ Settings | |
|---|---|
| DMZ Settings | Disable |
| DMZ IP Address | |

| | |
|---|---|
| **DMZ Settings** | 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 access the local host from WAN side. |
| **Apply** | Click to save and apply the current settings. |
| **Reset** | Press to discard current settings. |

# System Security



System Firewall Settings

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

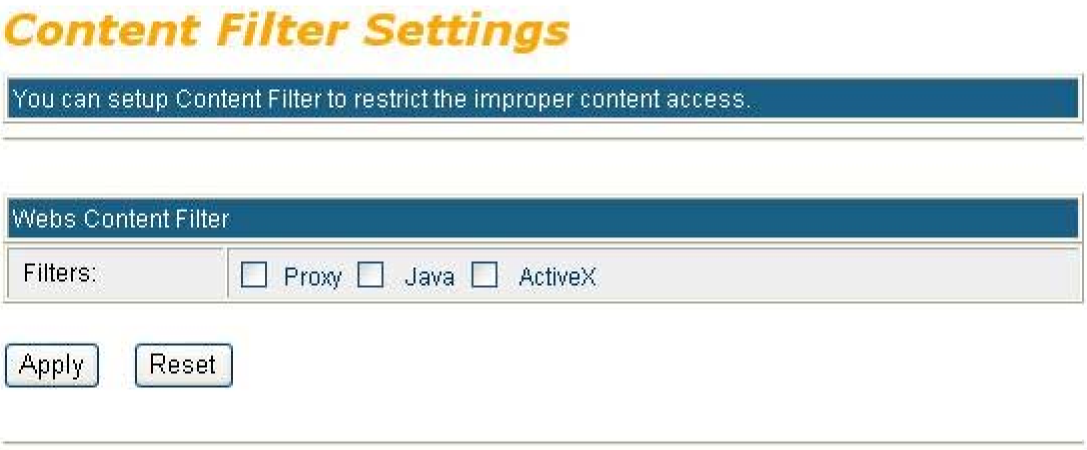
| Remote management | |
|---|---|
| Remote management (via WAN) | Deny |

| Ping form WAN Filter | |
|---|---|
| Ping form WAN Filter | Enable |

| Stateful Packet Inspection (SPI) | |
|---|---|
| SPI Firewall | Disable |

| Remote management | |
|---|---|
| **Remote management (via WAN)** | Select **Deny** or **Allow** form the pull-down list to enable or disable the remote client to control the Wireless Router via WAN. Default setting is Deny. |
| **Remote Port** | After Allow the Remote management, user can enter the port number here. |
| **Ping form WAN Filter** | |
| **Ping form WAN Filter** | To execute the Ping action from the WAN side. Select Disable or Enable from the pull-down list. Default setting is Enable. |
| **Stateful Packet Inspection (SPI)** | |
| **SPI Firewall** | Stateful packet inspection (SPI) is a firewall that keeps track of the state of network connections (such as TCP streams, UDP communication) traveling across it. The firewall is programmed to distinguish legitimate packets for different types of connections. Only packets matching a known connection state will be allowed by the firewall; others will be rejected.<br>Select Disable or Enable the SPI firewall function from the pull-down list. Default setting is Disable. |

# Content Filtering

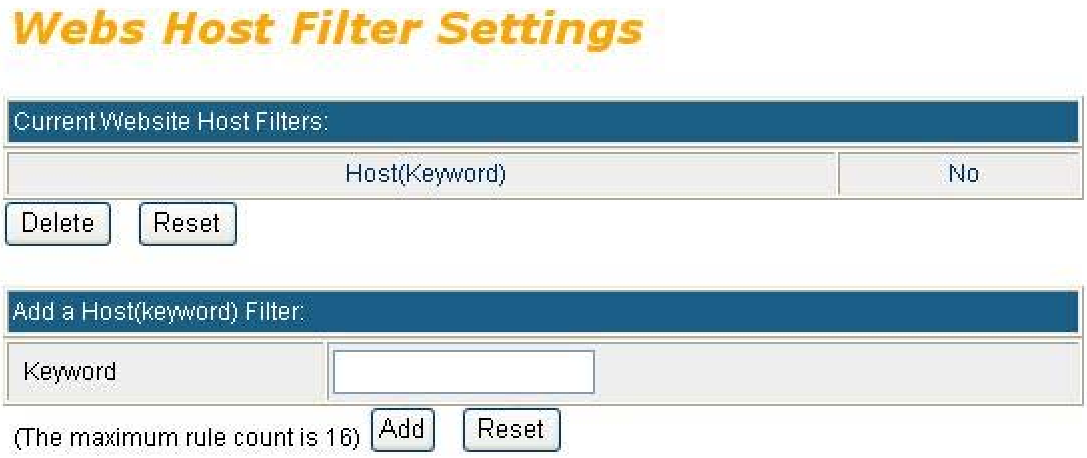


Content Filter Settings

You can setup Content Filter to restrict the improper content access.

Webs Content Filter

Filters: □ Proxy □ Java □ ActiveX



Webs Host Filter Settings

Current Website Host Filters:

| Host(Keyword) | No |
|---|---|

Add a Host(keyword) Filter:

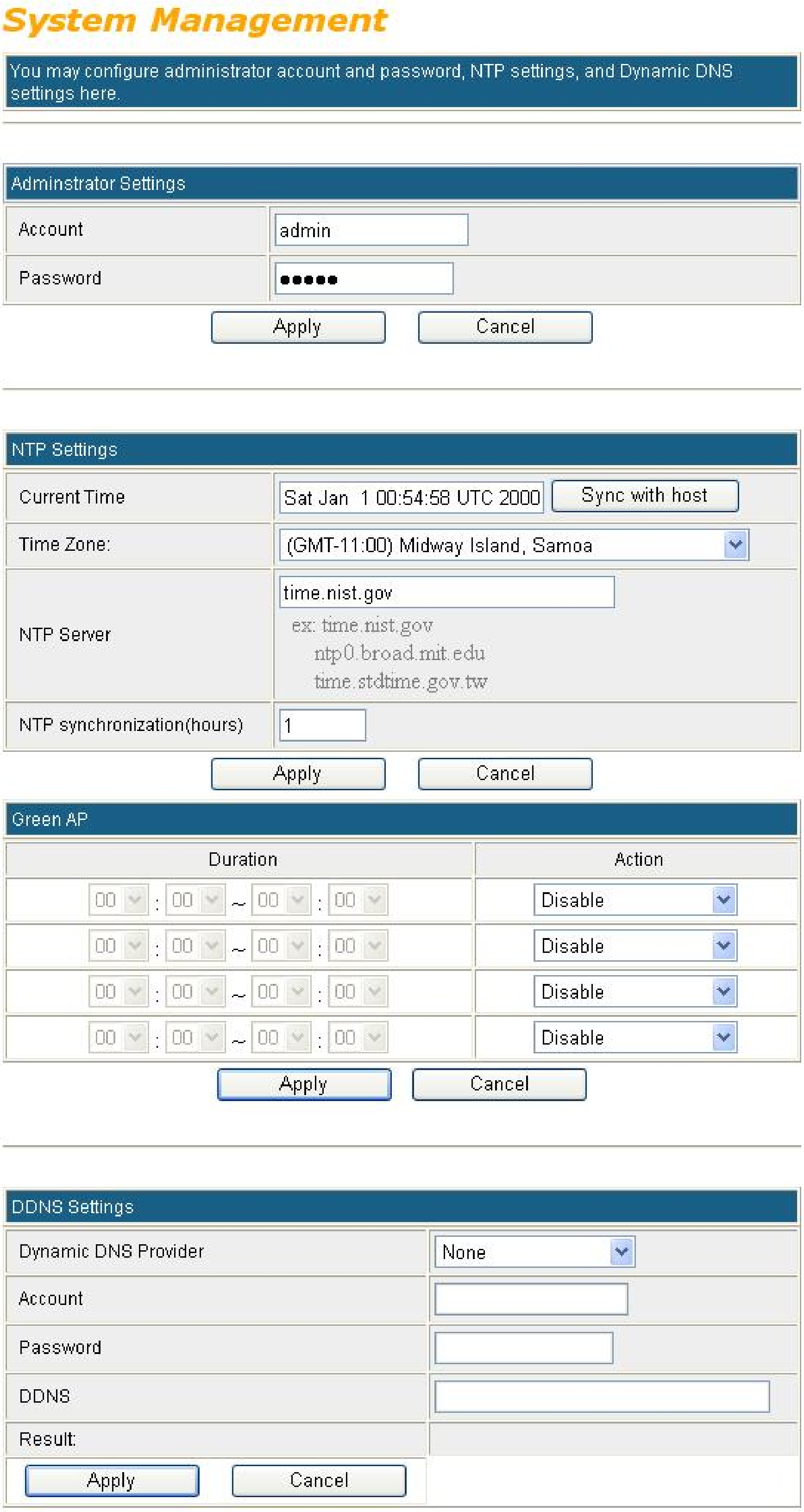
Keyword

(The maximum rule count is 16)

| | |
|---|---|
| **Content Filter Settings** | Select Webs Content Filters, Proxy, Java or ActiveX. |
| **Webs Host Filter Settings** | Enter the keyword in the field for a host filtering. |

# Administrator

## Management



### System Management

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

**Adminstrator Settings**

| | |
|---|---|
| Account | admin |
| Password | ●●●●● |

**NTP Settings**

| | |
|---|---|
| Current Time | Sat Jan 1 00:54:58 UTC 2000 |
| Time Zone: | (GMT-11:00) Midway Island, Samoa |
| NTP Server | time.nist.gov<br>ex: time.nist.gov<br>ntp0.broad.mit.edu<br>time.stdtime.gov.tw |
| NTP synchronization(hours) | 1 |

**Green AP**

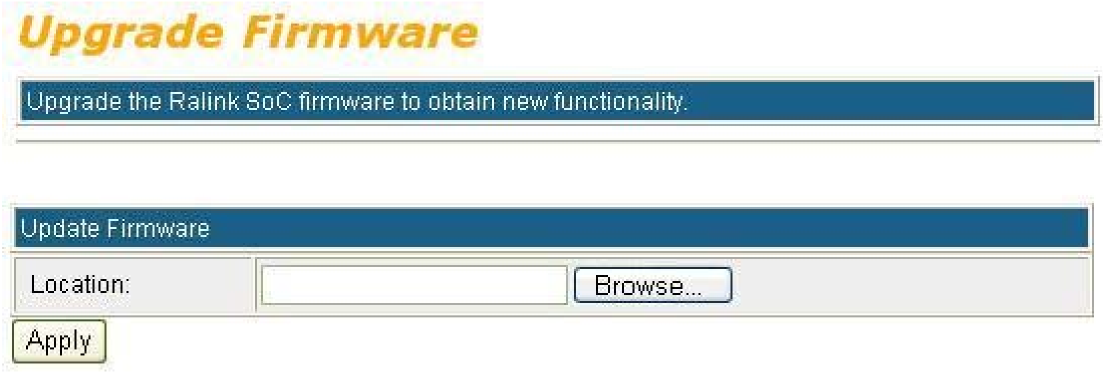
| Duration | Action |
|---|---|
| 00 : 00 ~ 00 : 00 | Disable |
| 00 : 00 ~ 00 : 00 | Disable |
| 00 : 00 ~ 00 : 00 | Disable |
| 00 : 00 ~ 00 : 00 | Disable |

**DDNS Settings**

| | |
|---|---|
| Dynamic DNS Provider | None |
| Account | |
| Password | |
| DDNS | |
| Result: | |

| | |
|---|---|
| **Administrator Settings** | |
| **Account** | User can key in a new login user name here. |
| **Password** | Maximum input is 36 alphanumeric characters (case sensitive.) |
| **NTP Settings** | |
| **Current Time** | Click **Sync with host** button to synchronize the time with the host PC. |
| **Time Zone** | Select the time zone area that you located from the pull-down list. |
| **NTP Server** | Enter the Network Time Protocol Server here. Ex: time.nist.gov, ntp0.broad.mit.edu, or time.stdtime.gov.tw. |
| **NTP synchronization(hours)** | The device will synchronize time with the server according to the hour(s) that entered. |
| **Green AP** | |
| **Duration** | User has to set up the **NTP Server** and **NTP synchronization(hours)** first that the Green AP function can be set up.<br>Set up a period of time to enable or disable the wireless TX function. |
| **Action** | Select Disable, WiFi TX power OFF, WiFi TX power 25%, WiFi TX power 50%, or WiFi TX power 75% from the pull-down menu, to enable or disable the wireless TX function of the Wireless Router. |
| **DDNS Settings** | |
| **Dynamic DNS Provider** | Select the DNS provider form the pull-down list. DNS provider is a company that provides access to the internet. |
| **Account** | Enter your account that you registered in DNS provider website. |
| **Password** | Enter your passwords that you registered. |
| **DDNS** | Apply for a Domain Name, and ensure it is allocated to you. |
| **Result** | Here shows the DDNS status. |

# Upload Firmware



Upgrade Firmware

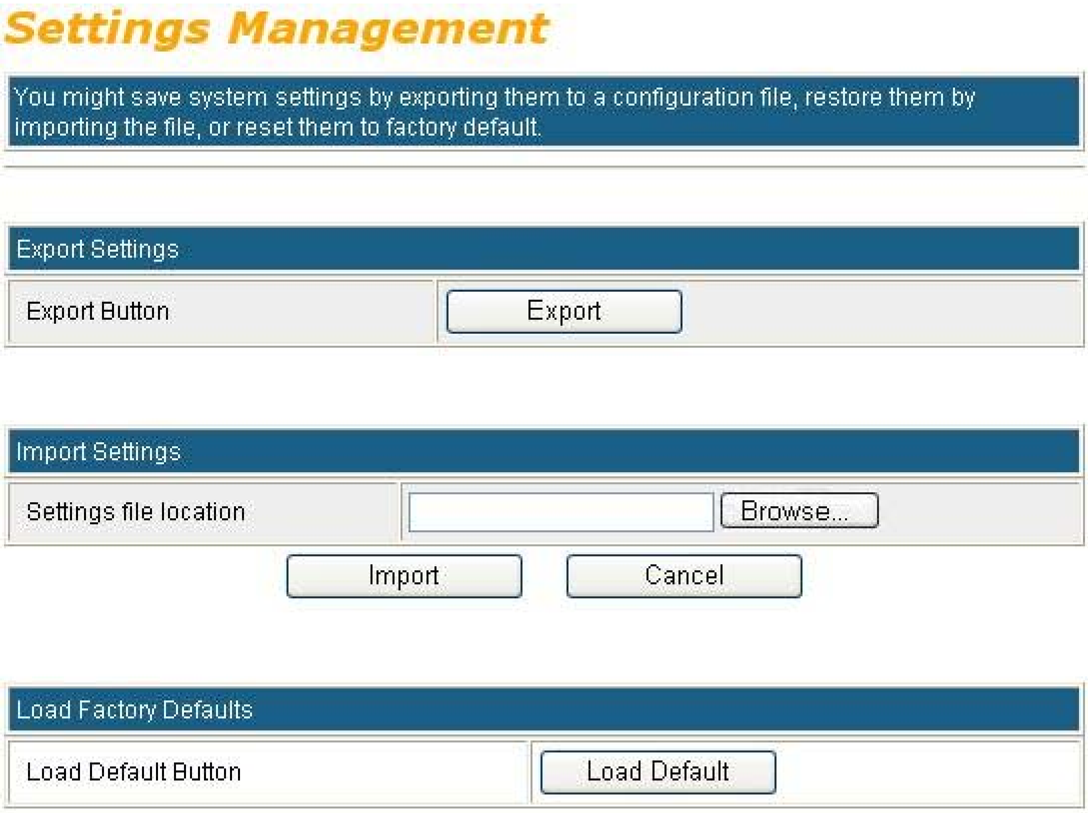
Upgrade the Ralink SoC firmware to obtain new functionality.

Update Firmware

Location:

| | |
|---|---|
| **Update Firmware** | |
| **Location** | Click the **Browse…** button, find and open the firmware file (the browser will display the correct file path) then click **Apply** to upgrade the Wireless Router’s firmware. |

# Settings Management



Settings Management

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

Export Settings

Export Button

Import Settings

Settings file location

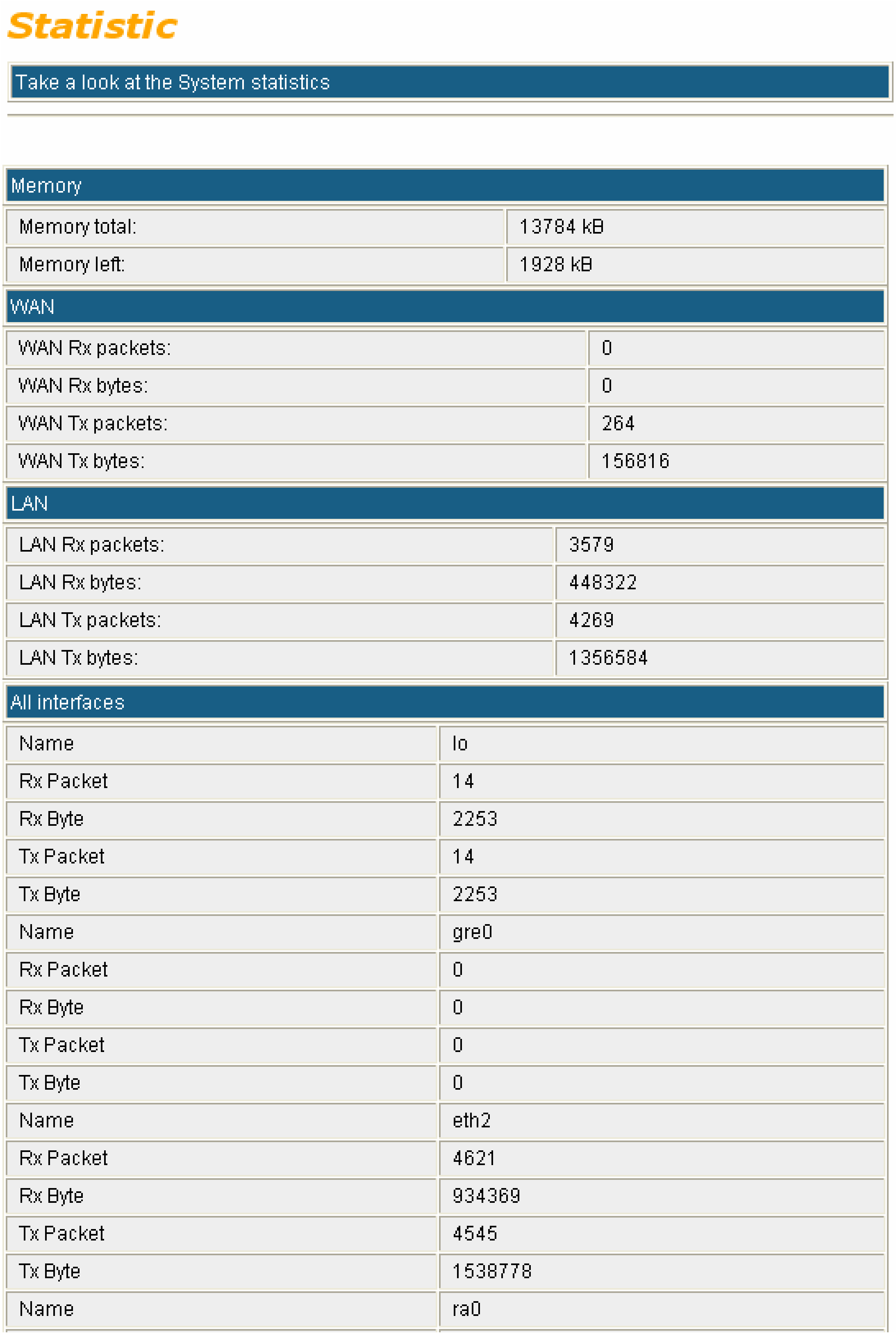
Load Factory Defaults

Load Default Button

| | |
|---|---|
| **Export Settings** | |
| **Export Button** | Click the **Export** button to save the current device settings to located computer. |
| **Import Settings** | |
| **Settings file location** | Click the **Browse…** button, find and open the settings file (the browser will display to correct file path), then click the **Import** button to use the device settings that previous saved. |
| **Cancel** | Click to discard the file that you selected form your located computer. |
| **Load Factory Defaults** | |
| **Load Default Button** | Click to **Load Default** button to set the Wireless Router back to factory default settings. |

# Statistics

This page shows all system memory, WAN/LAN, all interfaces statistics.



Statistic

Take a look at the System statistics

| Memory | |
|---|---|
| Memory total: | 13784 kB |
| Memory left: | 1928 kB |

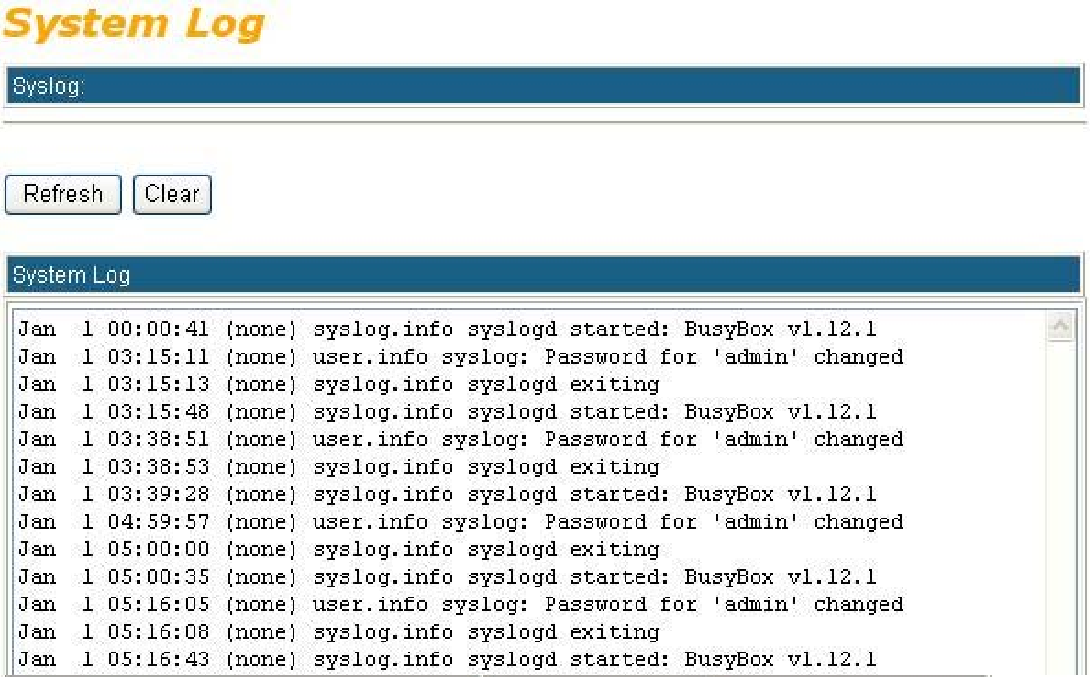
| WAN | |
|---|---|
| WAN Rx packets: | 0 |
| WAN Rx bytes: | 0 |
| WAN Tx packets: | 264 |
| WAN Tx bytes: | 156816 |

| LAN | |
|---|---|
| LAN Rx packets: | 3579 |
| LAN Rx bytes: | 448322 |
| LAN Tx packets: | 4269 |
| LAN Tx bytes: | 1356584 |

| All interfaces | |
|---|---|
| Name | lo |
| Rx Packet | 14 |
| Rx Byte | 2253 |
| Tx Packet | 14 |
| Tx Byte | 2253 |
| Name | gre0 |
| Rx Packet | 0 |
| Rx Byte | 0 |
| Tx Packet | 0 |
| Tx Byte | 0 |
| Name | eth2 |
| Rx Packet | 4621 |
| Rx Byte | 934369 |
| Tx Packet | 4545 |
| Tx Byte | 1538778 |
| Name | ra0 |

# System Log

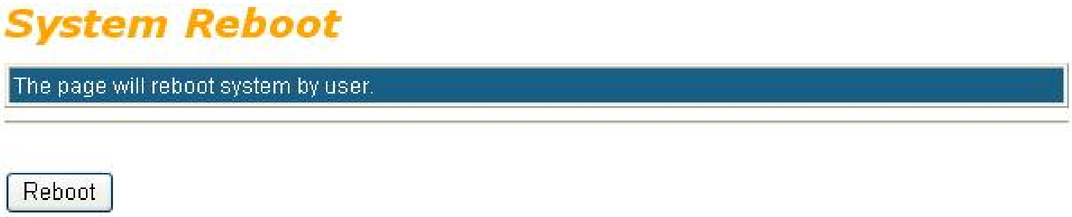
Here shows the system log file information. Click **Refresh** button to update system log file, or click **Clear** button to review the log file.



```
Jan  1 00:00:41 (none) syslog.info syslogd started: BusyBox v1.12.1
Jan  1 03:15:11 (none) user.info syslog: Password for 'admin' changed
Jan  1 03:15:13 (none) syslog.info syslogd exiting
Jan  1 03:15:48 (none) syslog.info syslogd started: BusyBox v1.12.1
Jan  1 03:38:51 (none) user.info syslog: Password for 'admin' changed
Jan  1 03:38:53 (none) syslog.info syslogd exiting
Jan  1 03:39:28 (none) syslog.info syslogd started: BusyBox v1.12.1
Jan  1 04:59:57 (none) user.info syslog: Password for 'admin' changed
Jan  1 05:00:00 (none) syslog.info syslogd exiting
Jan  1 05:00:35 (none) syslog.info syslogd started: BusyBox v1.12.1
Jan  1 05:16:05 (none) user.info syslog: Password for 'admin' changed
Jan  1 05:16:08 (none) syslog.info syslogd exiting
Jan  1 05:16:43 (none) syslog.info syslogd started: BusyBox v1.12.1
```

# Reboot

Click the **Reboot** button to restart the Wireless Router.



# Chapter 4: PC Configuration

## Overview

For each PC, the following may need to be configured:

- TCP/IP network settings
- Internet Access configuration
- Wireless configuration

## Windows Clients

- This section describes how to configure Windows clients for Internet access via the Wireless Router.
- The first step is to check the PC's TCP/IP settings.
- The Wireless Router uses the TCP/IP network protocol for all functions, so it is essential that the TCP/IP protocol be installed and configured on each PC.

### TCP/IP Settings - Overview

If using default Wireless Router settings, and default Windows TCP/IP settings, no changes need to be made.

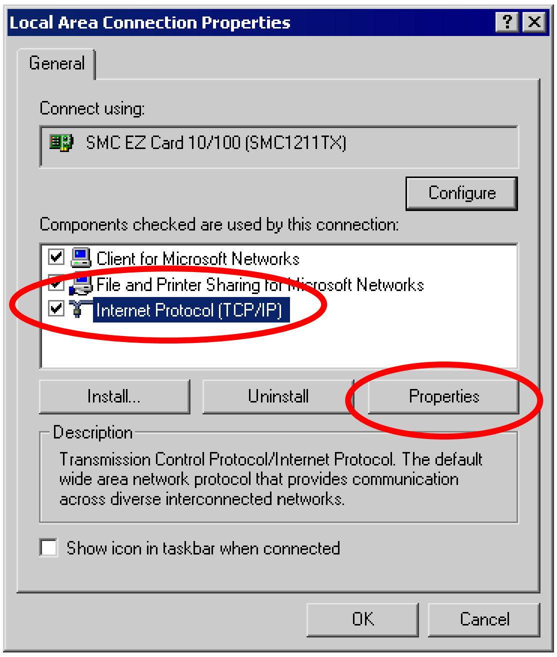
- By default, the Wireless Router will act as a DHCP Server, automatically providing a suitable IP address (and related information) to each PC when the PC boots.
- For all non-Server versions of Windows, the default TCP/IP setting is to act as a DHCP client.

If using a Fixed (specified) IP address, the following changes are required:

- The *Gateway* must be set to the IP address of the Wireless Router.
- The *DNS* should be set to the address provided by your ISP.

### Checking TCP/IP Settings - Windows 2000

1. Select Control Panel - Network and Dial-up Connection.
2. Right - click the *Local Area Connection* icon and select *Properties*. You should see a screen like the following:



Local Area Connection Properties

General

Connect using:

SMC EZ Card 10/100 (SMC1211TX)

Components checked are used by this connection:

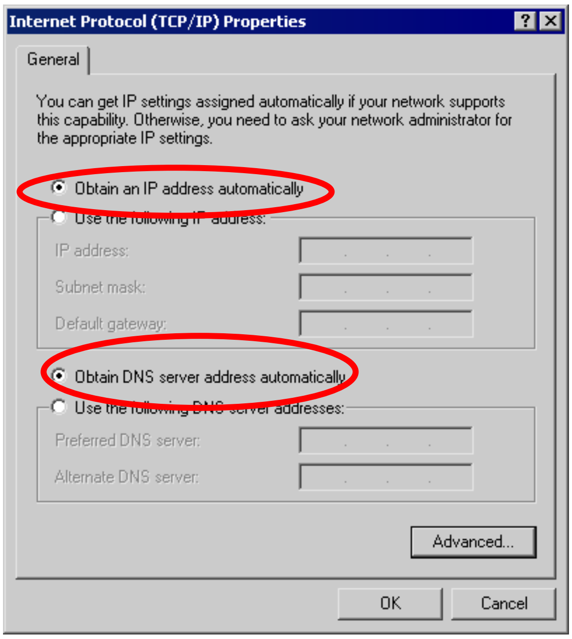
- ☑ Client for Microsoft Networks
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Internet Protocol (TCP/IP)

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

☐ Show icon in taskbar when connected

3. Select the *TCP/IP* protocol for your network card.
4. Click on the *Properties* button. You should then see a screen like the following.



Internet Protocol (TCP/IP) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

5. Ensure your TCP/IP settings are correct, as described below.

## Using DHCP

- To use DHCP, select the radio button *Obtain an IP Address automatically*. This is the default Windows setting. Using this is recommended. By default, the Wireless Router will act as a DHCP Server.
- Restart your PC to ensure it obtains an IP Address from the Wireless Router.

## Using a fixed IP Address ("Use the following IP Address")

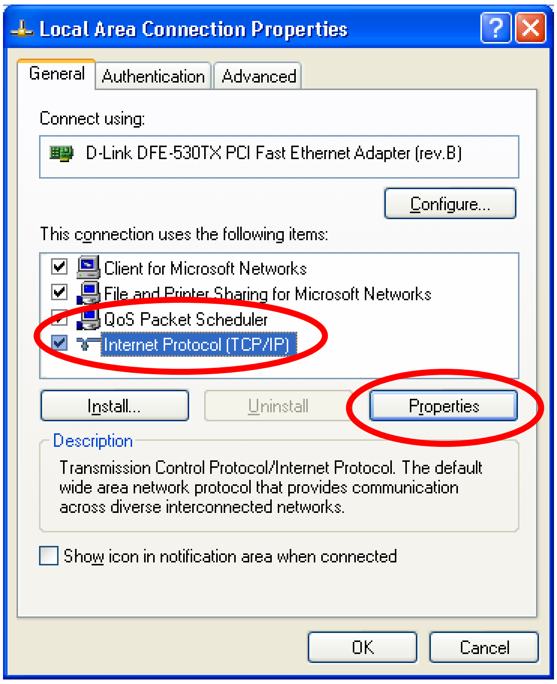
If your PC is already configured, check with your network administrator before making the following changes.

- Enter the Wireless Router 's IP address in the *Default gateway* field and click *OK*. (Your LAN administrator can advise you of the IP Address they assigned to the Wireless Router.)

- If the *DNS Server* fields are empty, select *Use the following DNS server addresses*, and enters the DNS address or addresses provided by your ISP, then click *OK*.

## Checking TCP/IP Settings - Windows XP

1. Select Control Panel - Network Connection.
2. Right click the *Local Area Connection* and choose *Properties*. You should see a screen like the following:



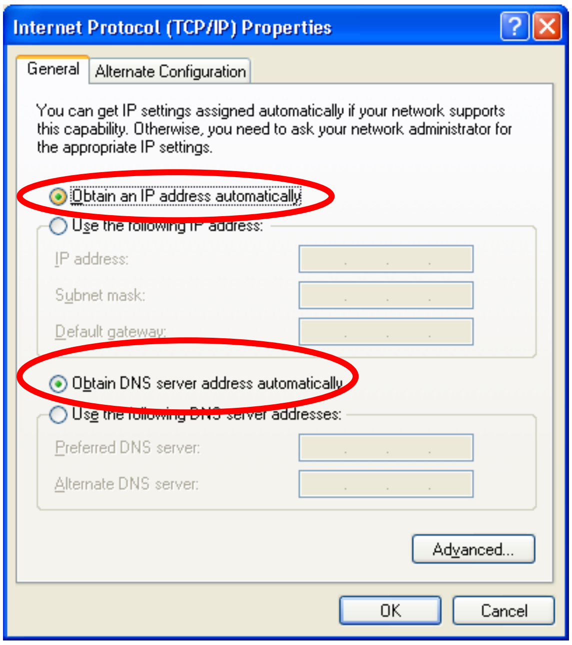
Connect using:
D-Link DFE-530TX PCI Fast Ethernet Adapter (rev.B)

This connection uses the following items:
☑ Client for Microsoft Networks
☑ File and Printer Sharing for Microsoft Networks
☐ QoS Packet Scheduler
☑ Internet Protocol (TCP/IP)

Description
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

☐ Show icon in notification area when connected

3. Select the *TCP/IP* protocol for your network card.
4. Click on the *Properties* button. You should then see a screen like the following.



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically
○ Use the following IP address:
IP address: . . .
Subnet mask: . . .
Default gateway: . . .

● Obtain DNS server address automatically
○ Use the following DNS server addresses:
Preferred DNS server: . . .
Alternate DNS server: . . .

5. Ensure your TCP/IP settings are correct.

### Using DHCP

- To use DHCP, select the radio button *Obtain an IP Address automatically*. This is the default Windows setting. Using this is recommended. By default, the Wireless Router will act as a DHCP Server.
- Restart your PC to ensure it obtains an IP address from the Wireless Router.

### Using a fixed IP Address ("Use the following IP Address")

If your PC is already configured, check with your network administrator before making the following changes.

- In the *Default gateway* field, enter the Wireless Router 's IP address and click *OK*. Your LAN administrator can advise you of the IP Address they assigned to the Wireless Router.
- If the *DNS Server* fields are empty, select *Use the following DNS server addresses*, and enters the DNS address or addresses provided by your ISP, then click *OK*.

# Internet Access

To configure your PCs to use the Wireless Router for Internet access:

- Ensure that the ADSL modem, DSL modem, Cable modem, or other permanent connection is functional.
- Use the following procedure to configure your Browser to access the Internet via the LAN, rather than by a Dial-up connection.

## For Windows 2000

1. Select Start menu - Settings - Control Panel - Internet Options.
2. Select the Connection tab, and click the *Setup* button.
3. Select "I want to set up my Internet connection manually, or I want to connect through a local area network (LAN)" and click *Next*.
4. Select "I connect through a local area network (LAN)" and click *Next*.
5. Ensure all of the boxes on the following Local area network Internet Configuration screen are unchecked.
6. Check the "No" option when prompted "Do you want to set up an Internet mail account now?"
7. Click *Finish* to close the Internet Connection Wizard. Setup is now completed.

## For Windows XP

1. Select ***Start*** menu >***Control Panel > Network and Internet Connections***.
2. Select ***Set up or change your Internet Connection***.
3. Select the ***Connection*** tab, and click the ***Setup*** button.
4. Cancel the pop-up "***Location Information***" screen.
5. Click ***Next*** on the "***New Connection Wizard***" screen.
6. Select "***Connect to the Internet***" and click ***Next***.
7. Select "***Set up my connection manually***" and click ***Next***.
8. Check "***Connect using a broadband connection that is always on***" and click ***Next***.
9. Click ***Finish*** to close the New Connection Wizard. Setup is now completed.

## Accessing AOL

To access AOL (America On Line) through the Wireless Router, the *AOL for Windows* software must be configured to use TCP/IP network access, rather than a dial-up connection. The configuration process is as follows:

1. Start the AOL for Windows communication software. Ensure that it is Version 2.5, 3.0 or later. This procedure will not work with earlier versions.
2. Click the Setup button.
3. Select Create Location, and change the location name from "New Locality" to " Wireless Router ".
4. Click Edit Location. Select TCP/IP for the Network field. (Leave the Phone Number blank.)
5. Click Save, then OK.
6. Configuration is now complete.
7. Before clicking "Sign On", always ensure that you are using the " Wireless Router " location.

# Macintosh Clients

From your Macintosh, you can access the Internet via the Wireless Router. The procedure is as follows.

1. Open the TCP/IP Control Panel.
2. Select *Ethernet* from the *Connect via* pop-up menu.
3. Select *Using DHCP Server* from the *Configure* pop-up menu. The DHCP Client ID field can be left blank.
4. Close the TCP/IP panel, saving your settings.

***Note:***

If using manually assigned IP addresses instead of DHCP, the required changes are:

- Set the *Router Address* field to the Wireless Router 's IP Address.
- Ensure your DNS settings are correct.

# Linux Clients

To access the Internet via the Wireless Router, it is only necessary to set the Wireless Router as the "Gateway".
Ensure you are logged in as "root" before attempting any changes.

### Fixed IP Address

By default, most Unix installations use a fixed IP Address. If you wish to continue using a fixed IP Address, make the following changes to your configuration.

- Set your "Default Gateway" to the IP Address of the Wireless Router.
- Ensure your DNS (Domain Name server) settings are correct.

### To act as a DHCP Client (Recommended)

The procedure below may vary according to your version of Linux and X -windows shell.

1. Start your X Windows client.
2. Select *Control Panel – Network.*
3. Select the "Interface" entry for your Network card. Normally, this will be called "eth0".
4. Click the *Edit* button, set the "protocol" to "DHCP", and save this data.
5. To apply your changes:
   - Use the "Deactivate" and "Activate" buttons, if available.
   - OR, restart your system.

# Other Unix Systems

To access the Internet via the Wireless Router:

- Ensure the "Gateway" field for your network card is set to the IP Address of the Wireless Router.
- Ensure your DNS (Name Server) settings are correct.

# Wireless Station Configuration

- This section applies to all wireless stations wishing to use the Wireless Router 's access point, regardless of the operating system that is used on the client.
- To use the Wireless Router, each wireless station must have compatible settings, as following:

| | |
|---|---|
| **Mode** | The mode must be set to *Infrastructure*. |
| **SSID (ESSID)** | The network name must match the value used on the Wireless Router.<br>***Note! The SSID is case- sensitive.*** |
| **Open**<br>**Shared Key** | If there is no security is enabled on the Wireless Router, the security of each station should be disabled as well. And, you can connect the Wireless Router without security, but it is NOT recommended. |
| **WEP auto** | By default, WEP on the Wireless Router is disabled.<br>● If WEP remains disabled on the Wireless Router, all stations must have WEP disabled.<br>● If WEP is enabled on the Wireless Router, each station must use the same settings as the Wireless Router. |
| **WPA-PSK**<br>**WPA2-PSK**<br>**WPA-PSK WPA2-PSK** | WPA-PSK (TKIP/AES)/ WPA2-PSK (TKIP/AES)/ WPA-RADIUS (TKIP/AES)/ WPA2 -RADIUS (TKIP/AES): If one of these securities is enabled on the Wireless Router. To make a connection, each station must use the same algorithms and pass phrase as the Wireless Router. |
| **WPA**<br>**WPA2**<br>**WPA WPA2**<br>**802.1x** | 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. Each station must set up the RADIUS Server’s IP address, port and passwords that provided by your ISP. |

***Note: By default, the Wireless Router will allow 802.11b, 802.11g and 802.11n connections.***

A

# Appendix A: Troubleshooting

## Overview

This chapter covers some common problems that may be encountered while using the Wireless Router and some possible solutions to them. If you follow the suggested steps and the Wireless Router still does not function properly, contact your dealer for further advice.

## General Problems

| | |
|---|---|
| ***Problem 1:*** | Can't connect to the Wireless Router to configure it. |
| **Solution 1:** | Check the following:<br>● Check the Wireless Router is properly installed, LAN connections are OK, and it is powered ON.<br>● Ensure that your PC and the Wireless Router are on the same network segment.<br>● If your PC is set to "Obtain an IP Address automatically" (DHCP client), please restart it.<br>● If your PC uses a Fixed (Static) IP address, ensure that it is using an IP Address within the range 10.10.10.1 to 10.10.10.253 and thus compatible with the Wireless Router's default IP Address of 10.10.10.254.<br>Also, the Network Mask should be set to 255.255.255.0 to match the Wireless Router.<br>In Windows, you can check these settings by using *Control Panel-Network* to check the *Properties* for the TCP/IP protocol. |

## Internet Access

| | |
|---|---|
| ***Problem 1:*** | When I enter a URL or IP address I get a time out error. |
| **Solution 1:** | A number of things could be causing this. Try the following troubleshooting steps.<br>● Check if other PCs work. If they do, ensure that your PCs IP settings are correct. If using a Fixed (Static) IP Address, check the Network Mask, Default gateway and DNS as well as the IP Address.<br>● If the PCs are configured correctly, but still not working, check the Wireless Router. Ensure that it is connected and ON. Connect to it and check its settings. (If you can't connect to it, check the LAN and power connections.) |

| | |
|---|---|
| | ● If the Wireless Router is configured correctly, check your Internet connection (DSL/Cable modem etc) to see that it is working correctly. |
| ***Problem 2:*** | Some applications do not run properly when using the Wireless Router. |
| **Solution 2:** | The Wireless Router processes the data passing through it, so it is not transparent.<br>Use the *Content Filter Settings* feature to allow the use of Internet applications, which do not function correctly.<br>If this does solve the problem you can use the *DMZ* function. This should work with almost every application, but:<br>● It is a security risk, since the firewall is disabled.<br>● Only one (1) PC can use this feature. |

# Wireless Access

| | |
|---|---|
| ***Problem 1:*** | My PC can't locate the Wireless Router. |
| **Solution 1:** | Check the following:<br>● Your PC is set to *Infrastructure Mode*. (Access Points are always in *Infrastructure Mode*)<br>● The SSID on your PC and the Wireless Router are the same. Remember that the SSID is case-sensitive. So, for example "**W**orkgroup" does NOT match "**w**orkgroup."<br>● Both your PC and the Wireless Router must have the same setting for security. The default setting for the Wireless Router security is disabled, so your wireless station should also have security disabled.<br>● If security is enabled on the Wireless Router, your PC must have security enabled, and the key must be matched.<br>● To see if radio interference is causing a problem, see if connection is possible when close to the Wireless Router. Remember that the connection range can be as little as 100 feet in poor environments. |
| ***Problem 2:*** | Wireless connection speed is very slow. |
| **Solution 2:** | The wireless system will connect at the highest possible speed, depending on the distance and the environment. To obtain the highest possible connection speed, you can experiment with the following:<br>● Wireless Router location<br>Try adjusting the location and orientation of the Wireless Router.<br>● Wireless Channel<br>If interference is the problem, changing to another channel may show a marked improvement.<br>● Radio Interference<br>Other devices may be causing interference. You can experiment by switching other devices off, and see if this helps. Any "noisy" devices should be shielded or relocated. |

| | |
|---|---|
| | ● RF Shielding<br>Your environment may tend to block transmission between the wireless stations. This will mean high access speed is only possible when close to the Wireless Router. |

# Appendix B: About Wireless LANs

B

## BSS

BSS

A group of Wireless Stations and a single Access Point, all using the same ID (SSID), form a Basic Service Set (BSS).

Using the same SSID is essential. Devices with different SSIDs are unable to communicate with each other.

## Channels

The Wireless Channel sets the radio frequency used for communication.

- Wireless Router uses a fixed Channel. You can select the Channel used. This allows you to choose a Channel which provides the least interference and best performance. Due to different country, the Wireless Router supported different country region channels. In the USA and Canada, there are 11 channels available. In European, there are 13 channels available. In Japan, there are 14 channels available. If using multiple Wireless Routers, it is better if adjacent Wireless Routers use different Channels to reduce interference.
- In "Infrastructure" mode, Wireless Stations normally scan all Channels, looking for an Access Point. If more than one Access Point can be used, the one with the strongest signal is used. (This can only happen within an ESS.)

## Security

### WEP

WEP (Wired Equivalent Privacy) is a standard for encrypting data before it is transmitted. This is desirable because it is impossible to prevent snoopers from receiving any data which is transmitted by your Wireless Stations. But if the data is encrypted, then it is meaningless unless the receiver can decrypt it.

**If WEP is used, the Wireless Stations and the Access Point must have the same security settings for each of the following:**

| | |
|---|---|
| **WEP** | 64 Bits, 128 Bits. |
| **Key** | For 64 Bits encryption, the Key value must match.<br>For 128 Bits encryption, the Key value must match. |
| **WEP Authentication** | Open System or Shared Key. |

## WPA/WPA2

WPA/WPA2 (Wi-Fi Protected Access) is more secure than WEP. It uses a “Shared Key” which allows the encryption keys to be regenerated at a specified interval. There are several encryption options: **TKIP, AES, TKIP-AES** and additional setup for **RADIUS** is required in this method. The most important features beyond WPA to become standardized through 802.11i/WPA2 are: pre-authentication, which enables secure fast roaming without noticeable signal latency.

**If WPA or WPA2 is used, the Wireless Stations and the Access Point must have the same security settings.**

## WPA-PSK/ WPA2-PSK

WPA/WPA2 (Wi-Fi Protected Access using Pre-Shared Key) is recommended for users who are not using a RADIUS server in a home environment and all their clients support WPA/WPA2. This method provides a better security.

**If WPA-PSK or WPA2-PSK is used, the wireless stations and the access point must have the same security settings.**

| Encryption | WEP Key 1~4 | Passphrase |
|---|---|---|
| **TKIP** | **NOT REQUIRED** | **8-63 characters** |
| **AES** | | |

## 802.1x

With **802.1x** authentication, a wireless PC can join any network and receive any messages that are not encrypted, however, additional setup for **RADIUS** to issue the WEP key dynamically will be required. 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.

# Wireless LAN Configuration

To allow Wireless Stations to use the Access Point, the Wireless Stations and the Access Point must use the same settings, as follows:

| | |
|---|---|
| **Mode** | The mode must be set to *Infrastructure*. |
| **SSID (ESSID)** | The network name must match the value used on the Wireless Router.<br>***Note! The SSID is case- sensitive.*** |
| **Open**<br>**Shared Key** | If there is no security is enabled on the Wireless Router, the security of each station should be disabled as well. And, you can connect the Wireless Router without security, but it is NOT recommended. |
| **WEP AUTO** | By default, WEP on the Wireless Router is disabled.<br>● If WEP remains disabled on the Wireless Router, all stations must have WEP disabled.<br>● If WEP is enabled on the Wireless Router, each station must use the same settings as the Wireless Router. |
| **WPA-PSK**<br>**WPA2-PSK** | WPA-PSK (TKIP/AES)/ WPA2-PSK (TKIP/AES): If one of these |

| | |
|---|---|
| **WPA-PSK/WPA2-PSK** | securities is enabled on the Wireless Router. To make a connection, each station must use the same algorithms and pass phrase as the Wireless Router. |
| **WPA**<br>**WPA2**<br>**WPA WPA2**<br>**802.1x** | 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. Each station must set up the RADIUS Server's IP address, port and passwords that provided by your ISP. |