802.11b/g/n Compact Wireless Router

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.

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

This is a compact/travel size IEEE802.11b/g/n router with 2 fast Ethernet ports, which provides a powerful high-speed wireless connection for compatible wireless-enabled devices into the network with the freedom to roam. With web-based UI, this Access Point is easy to be setup and maintained. All functions can be configured within the easy and friendly user interface via web browser. Via the fast wireless network speed up to 150 Mbps, you can be very comfortable to have experience of high speed web surfing, files downloading, online game playing, and video conference session and streaming high quality multimedia materials. The Wireless Portable Router provides WPA/WPA2, 64/128 bit WEP encryption and IEEE802.1x which ensures a high level of security to protect users' data and privacy when you are traveling.

Features

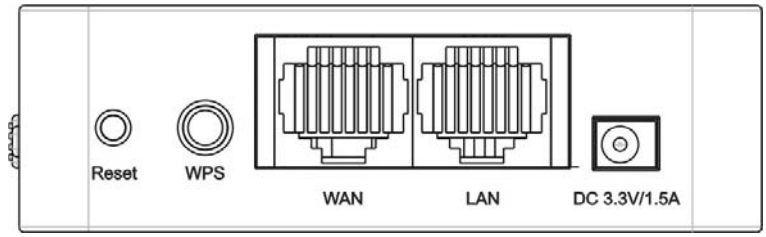
- Create temporary, personal, wireless access in your hotel room or a coffee shop hotspot
- Travel size design with selectable extra 2dBi high gain dipole antenna to enhance performance
- High security with build-in: WEP 64/128, WPA, WPA2 mixed, 802.1x and 802.11i
- Support AP,Gateway and Client Mode
- Wireless Quality of Service (QoS) - 802.11e,WMM
- Support WPS (Push button/ Pin code)
- Slide switch to change mode (Gateway/AP/Client) easily.

Physical Details

Front LEDs

LED Behavior				
LED	**Printed**	**Color**	**Behavior**	**Indication**
Power	⏻	Green	ON	Power on
		Green	OFF	Power off
WPS	🔑	Green	ON	WPS function on
		Green	OFF	WPS function off
Wireless LAN	(( ))	Green	OFF	WLAN off
		Green	ON	WLAN link / active
		Green	Blinking	WLAN traffic transmitting

Rear Panel



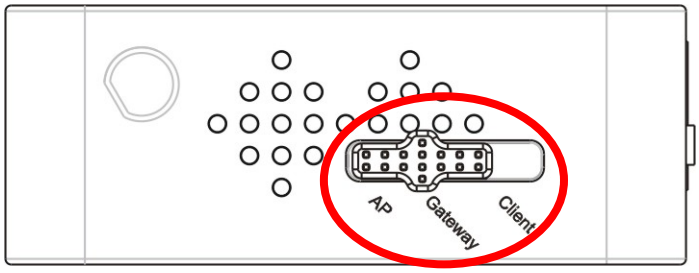
Reset	Keep on pressing the Reset button more than 3 seconds, the Wireless Portable Router will set all setting back to factory default values.
WPS	To enable the WPS function via web configuration (Wireless Settings> WPS), then press the WPS button once on the Wireless Portable Router, the GREEN LED will start to flash. To make a connection with other WPS supported device within 2 minutes.
WAN	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.
LAN	Use standard LAN cables (RJ45 connectors) to connect your PCs to the port. If required, any port can be connected to another hub. Any LAN port will automatically function as an "Uplink" port when necessary.
DC 3.3V/1.5A	Connect the power supply adapter here.

Chapter 2: About Operation Modes

This device provides operational applications with AP, Gateway and Client (Infrastructure) modes, which are mutually exclusive.
This device is shipped with configuration that is functional right out of the box. If you want to change the settings in order to perform more advanced configuration or even change the mode of operation, you can MANUALLY switch to the mode you desired by the manufacturer as described in the following sections.

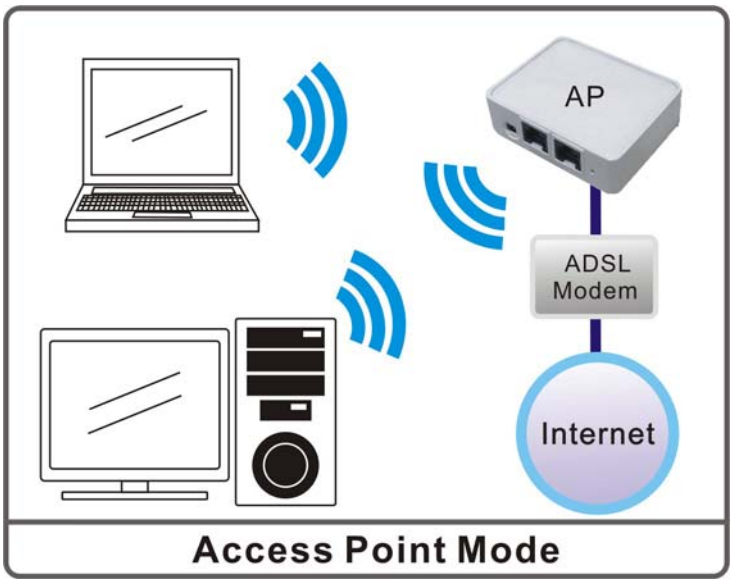
Operation Modes

You have to MANUALLY switch the bar into the mode you preferred, AP, Gateway, or Client mode, then the device will reboot automatically into the mode you have selected.



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.

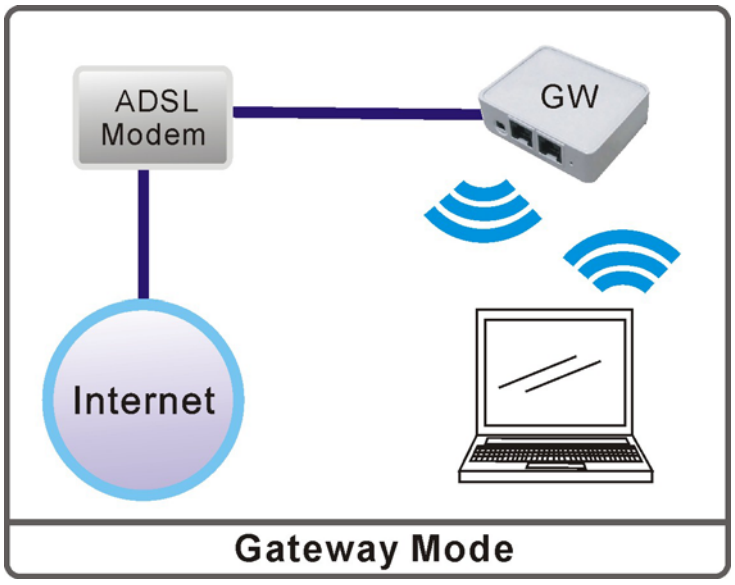


System Status

Let's take a look at the status of system.	
Internet	
Item	**Status**
Firmware Version	21.4.0.0.0.1e_b4 (Mar 24 2009)
System Up Time	54 secs
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.

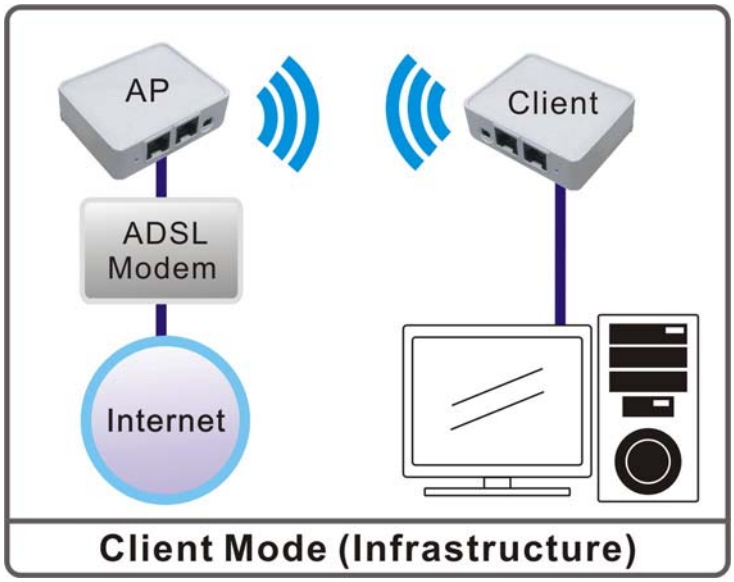


System Status

Let's take a look at the status of system.	
Internet	
Item	**Status**
Firmware Version	21.4.0.0.0.1e_b4 (Mar 24 2009)
System Up Time	27 secs
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.

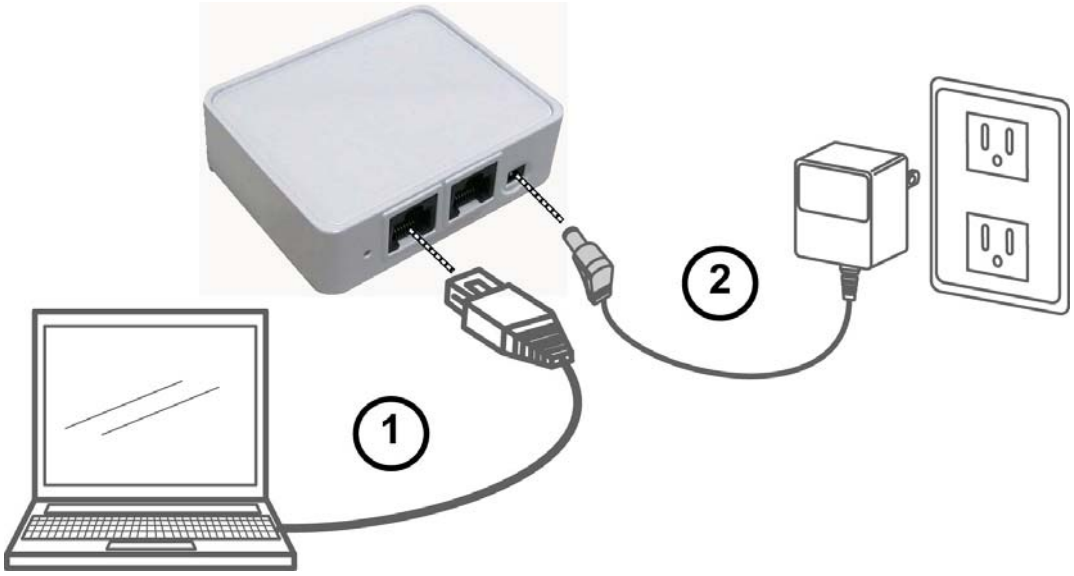
Internet

Item	Status
Firmware Version	21.4.0.0.0.1e_b4 (Mar 24 2009)
System Up Time	28 secs
Operation Mode	Client Mode

Chapter 3: Configuration

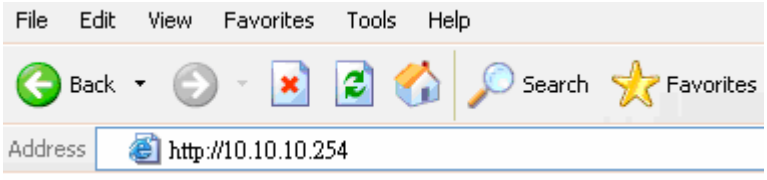
Hardware Connection

1. Connect one end of the Ethernet cable to the Wireless Portable Router, another end to your PC or notebook.
2. Then, connect the Wireless Portable 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 Portable Router.
2. Start your Web Browser.
3. In the *Address* box, enter the IP address of the Wireless Portable Router, as in this example, which uses the Wireless Portable Router's default IP 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.

If you cannot connect...

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

- The Wireless Portable Router is properly installed, LAN connection is OK, and it is powered ON. You can test the connection by using the "Ping" command:
  - Open the MS-DOS window or command prompt window.
  - Enter the command:
    ping 10.10.10.254
    If no response is received, either the connection is not working, or your PC's IP address is not compatible with the Wireless Portable 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 Portable 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 Portable 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. 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. 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 IP Address	Your IP Address is allocated automatically, when you connect to you ISP.	None.
Static (Fixed) 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. You connect to the ISP only when required. The IP address is usually allocated automatically, but may be Static (Fixed).	• PPTP Server IP Address. • User name and password. • IP Address allocated to you, if Static (Fixed).

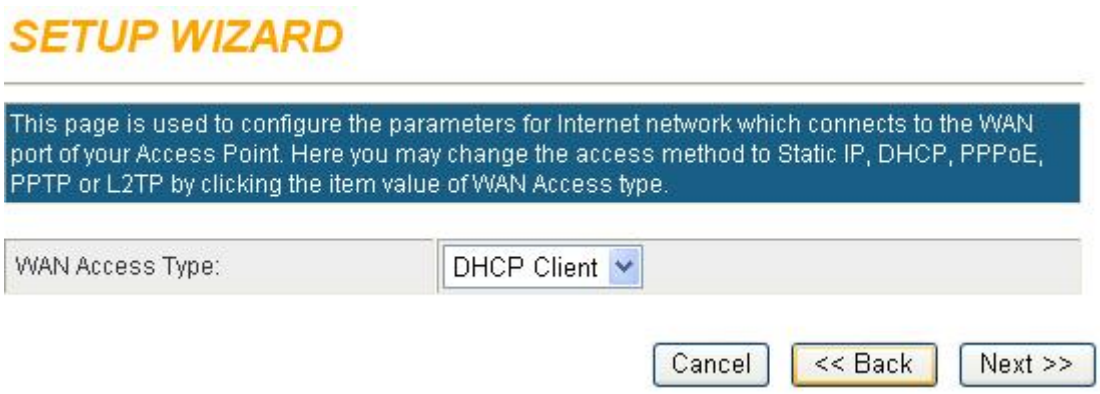
Other Modems (e.g. Broadband Wireless)

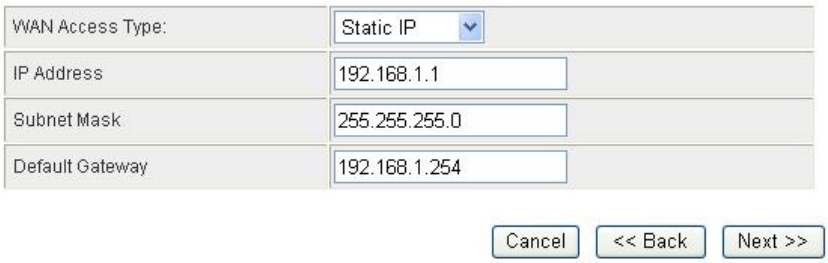
Type	Details	ISP Data required
Dynamic IP Address	Your IP Address is allocated automatically, when you connect to you ISP.	None.
Static (Fixed) IP Address	Your ISP allocates a permanent IP Address to you.	IP Address allocated to you.

Wizard (GW)

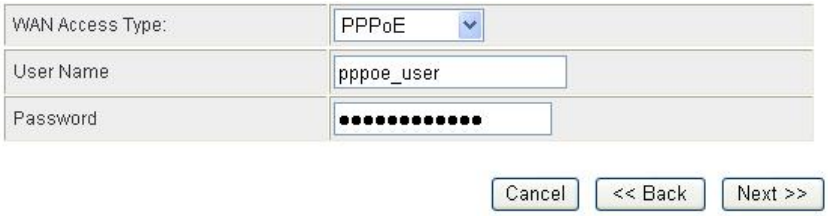
Step 1- WAN Access Type

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.



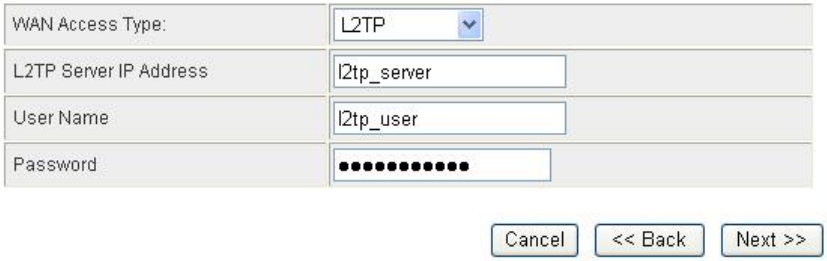
WAN Access Type	**DHCP Client**  If the DHCP Client WAN connection be selected, the PC will obtain the IP address automatically. **Static IP**  If the Static IP be selected, user have to set up the IP address, subnet mask and default gateway according to the ISP that provided the related information. **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



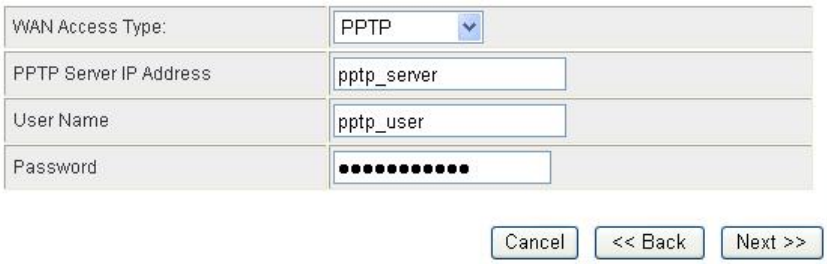
If the PPPoE be selected, user have to set up the user name and password according to the ISP that provided the related information.
User Name: Enter the username that provide by your ISP provider. Maximum input is 32 alphanumeric characters (case sensitive).
Password: Enter the password that provide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

L2TP



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).

PPTP



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).

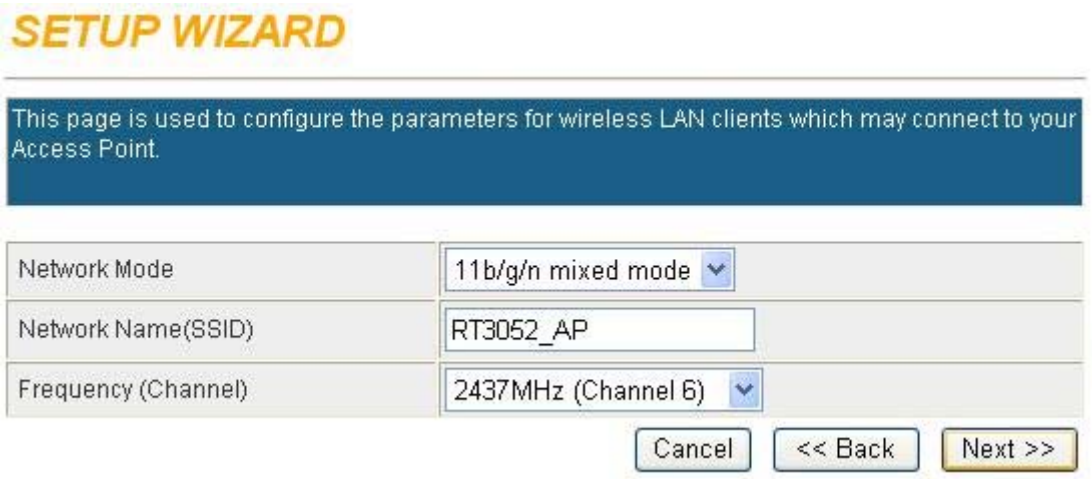
Step 2- LAN

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

IP Address	Shows the IP address of the Wireless Portable Router (Default IP address is 10.10.10.254.)
Subnet Mask	The subnet mask of the Wireless Portable Router (Default subnet mask is 255.255.255.0.)
DHCP Type	**Disable**: Select to disable this Wireless Portable Router to distribute IP addresses to connected clients. **Server**: Select to enable this Wireless Portable 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 Subnet Mask	The subnet mask of the distribute IP addresses clients, the subnet mask must be set at the same segment as the Wireless Portable Router.
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.



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 (SSID)	A SSID is referred to a network name because essentially it is a name that identifies a wireless network.
Frequency (Channel)	Select 1~11 or Auto Select from the pull-down menu.

Step 4- Security

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

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.

OPEN/SHARED/WEP AUTO

Default Key: Select the default key Key1~4.
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).

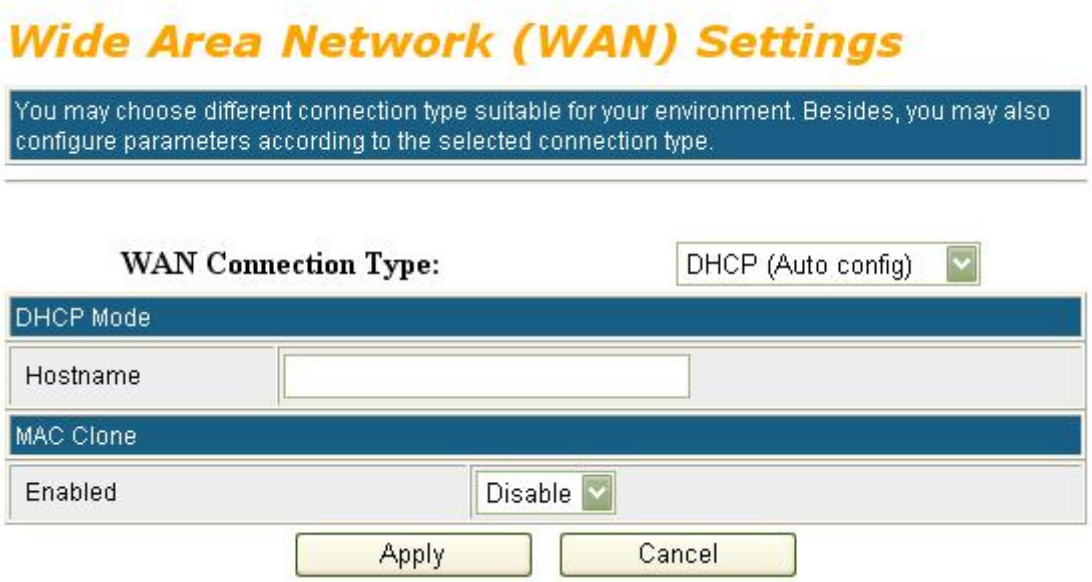
WPA-PSK/ WPA2-PSK/ WPA-PSK/WPA2-PSK

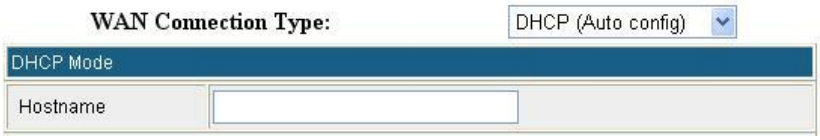
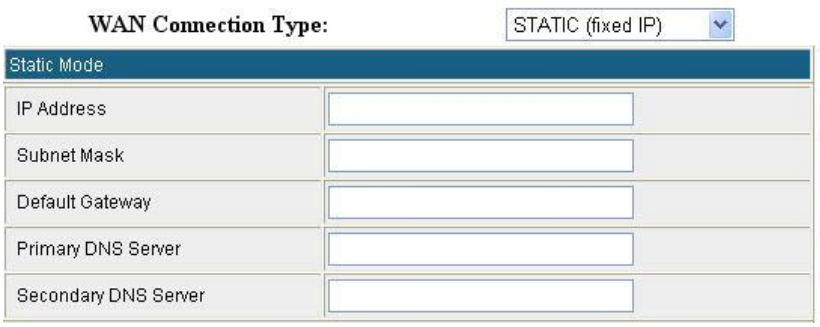
WPA Algorithms: Select the type of algorithm, TKIP or AES for WP-PSK, and TKIP, AES or TKIP/AES for WPA2-PSK, WPA-PSK/WPA2-PSK.

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

Internet Settings

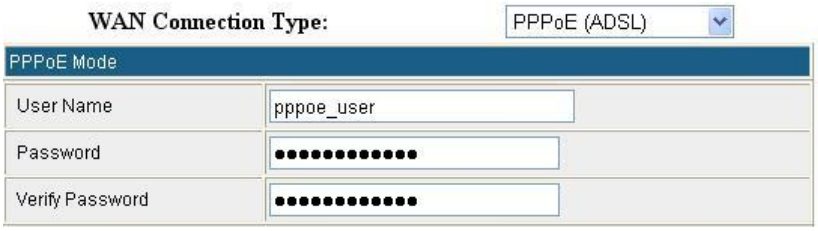
WAN (GW)



WAN Connection Type	Select the WAN Connection Type **Static (fixed IP), DHCP (Auto Config), PPPoE (ADSL)** and **L2TP, PPTP**. Default setting is **DHCP** enabled. **DHCP (Auto Config)**  **Hostname:** Enter the hostname that assigned IP address to user's computer in this field. Maximum input is 32 alphanumeric characters (case sensitive). **Static (fixed IP)**  **IP Address:** Enter the WAN IP address provided by your ISP in this column. **Subnet Mask:** Enter the Subnet Mask in this column.

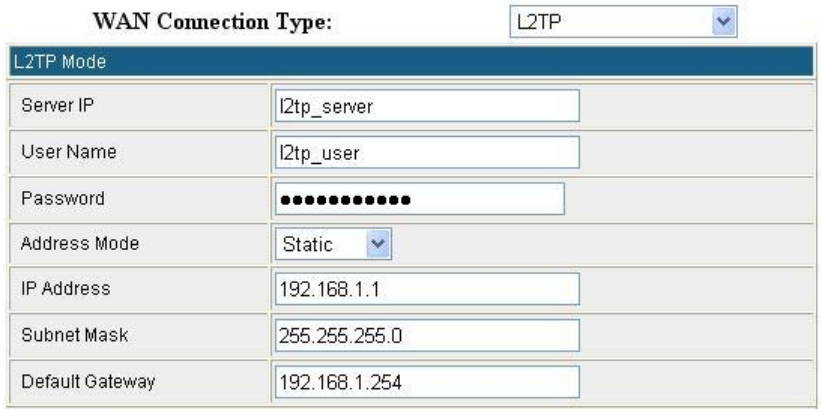
Default Gateway: Enter the default gateway IP address provided by your ISP in this column.
Primary DNS Server: The *DNS* should be set to the address provided by your ISP.
Secondary DNS Server: The *DNS* should be set to the address provided by your ISP.

PPPoE (ADSL)

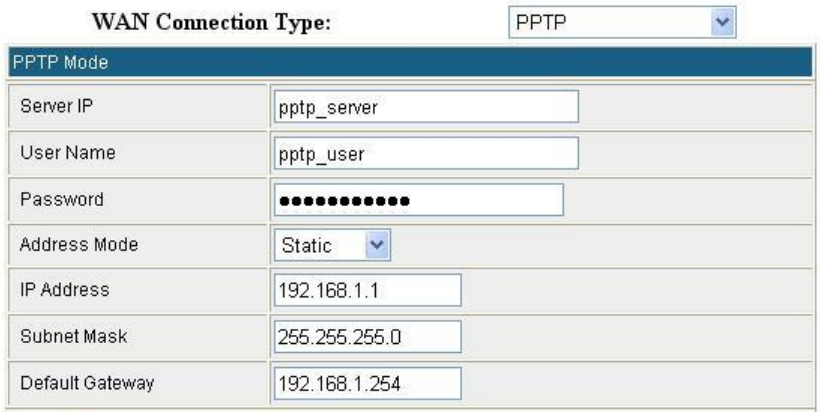
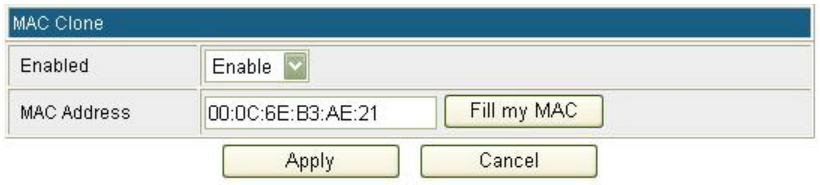


User Name: Enter the username that provide by your ISP provider. Maximum input is 32 alphanumeric characters (case sensitive).
Password: Enter the password that provide by your ISP provider. Maximum input is 32 alphanumeric characters (case sensitive).
Verify Password: To confirm the password, please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

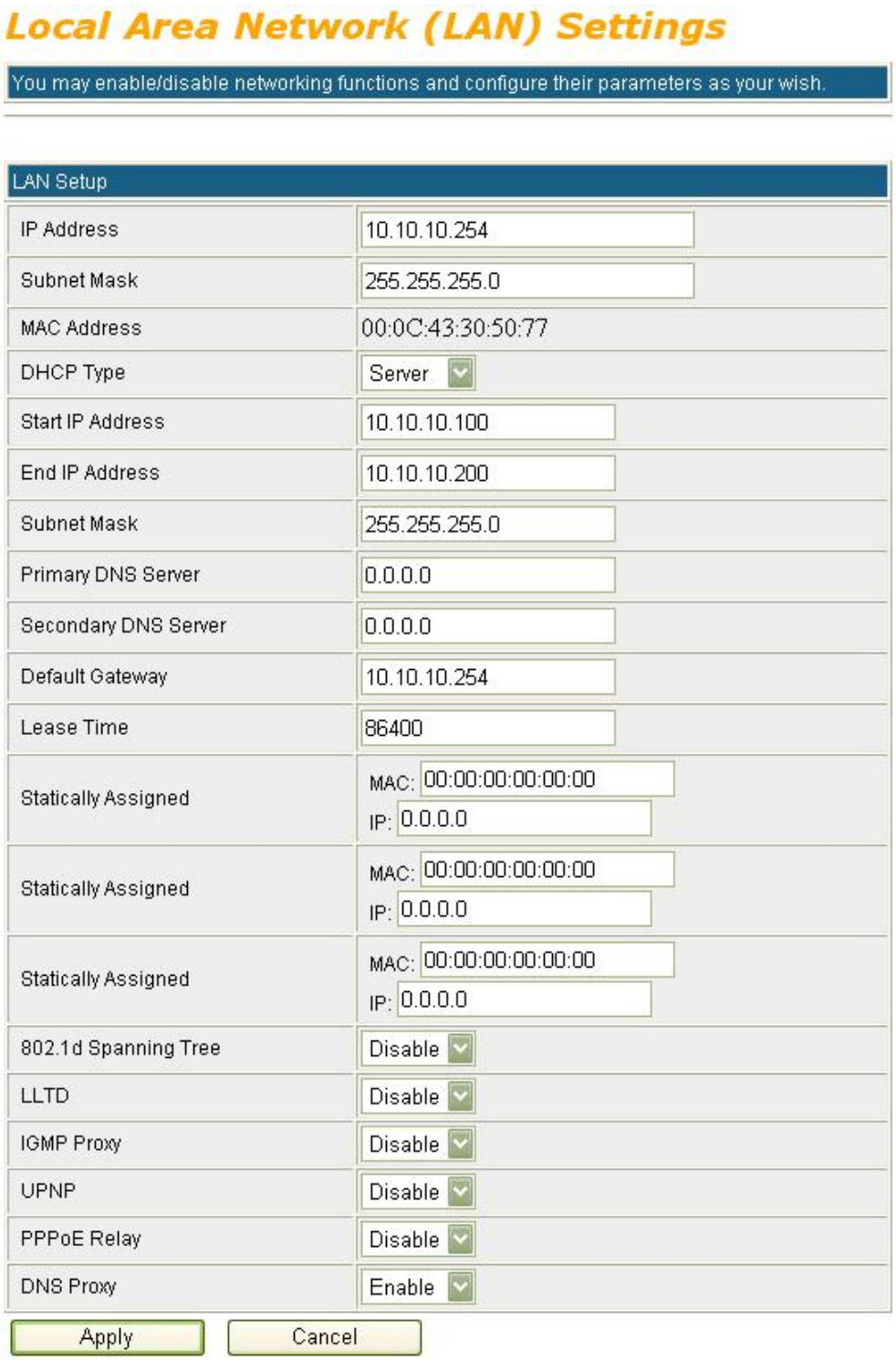
L2TP



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 Dynamic or Static IP address mode for the pull-down menu.
IP Address: Enter the WAN IP address provided by your ISP in this column.
Subnet Mask: Enter the subnet mask in this column.
Default Gateway: Enter the default gateway IP address provided by your ISP in this column.

	PPTP  **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 Dynamic or Static IP address mode for the pull-down menu. **IP Address:** Enter the WAN IP address provided by your ISP in this column. **Subnet Mask:** Enter the subnet mask in this column. **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. 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. 
Apply	After completing the settings on this page, click **Apply** button to save the settings.
Cancel	Click **Cancel** to restore to default values.

LAN



IP Address	Shows the IP address of the Wireless Portable Router (Default IP address is 10.10.10.254.)
Subnet Mask	The subnet mask of the Wireless Portable Router (Default subnet mask is 255.255.255.0.)
MAC Address	Shows the MAC address of this Wireless Portable Router.
DHCP Type	**Disable**: Select to disable this Wireless Portable Router to distribute IP

	addresses to connected clients. **Server**: Select to enable this Wireless Portable 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.
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.
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).
Subnet Mask	The subnet mask of the distribute IP addresses clients, the subnet mask must be set at the same segment as the Wireless Portable Router.
Primary DNS Server	Enter the DNS server IP address(es) that provided by your ISP, or you can specify your own preferred DNS server IP address(es).
Secondary DNS Server	Secondary DNS Server is optional. You can enter another DNS server's IP address as a backup.
Default Gateway	Shows the default gateway IP address.
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. **IP**: Enter the fixed IP address that DHCP Server assigned to a certain connected station. User can set up 3 set of fixed IP addresses that distribute form the Wireless Portable 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. 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. Select Enabled or Disabled from the pull-down menu.
IGMP Proxy	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

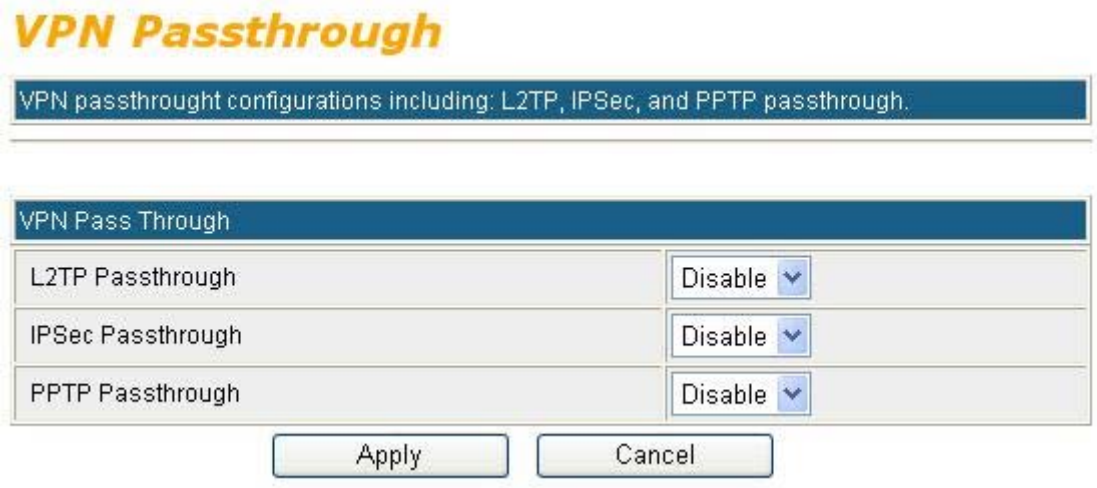
	built upon open, Internet-based communication standards. The term UPnP is derived from plug-and-play, a technology for dynamically attaching devices directly to a computer. Select Disable or Enable from the pull-down menu.
PPPoE Relay	Select Disable or Enable from the pull-down menu.
DNS Proxy	Select 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.

DHCP clients

Here shows the IP assigned clients that computer in the network requests IP addresses from DHCP server (Wireless Portable Router).

VPN Passthrough (GW)

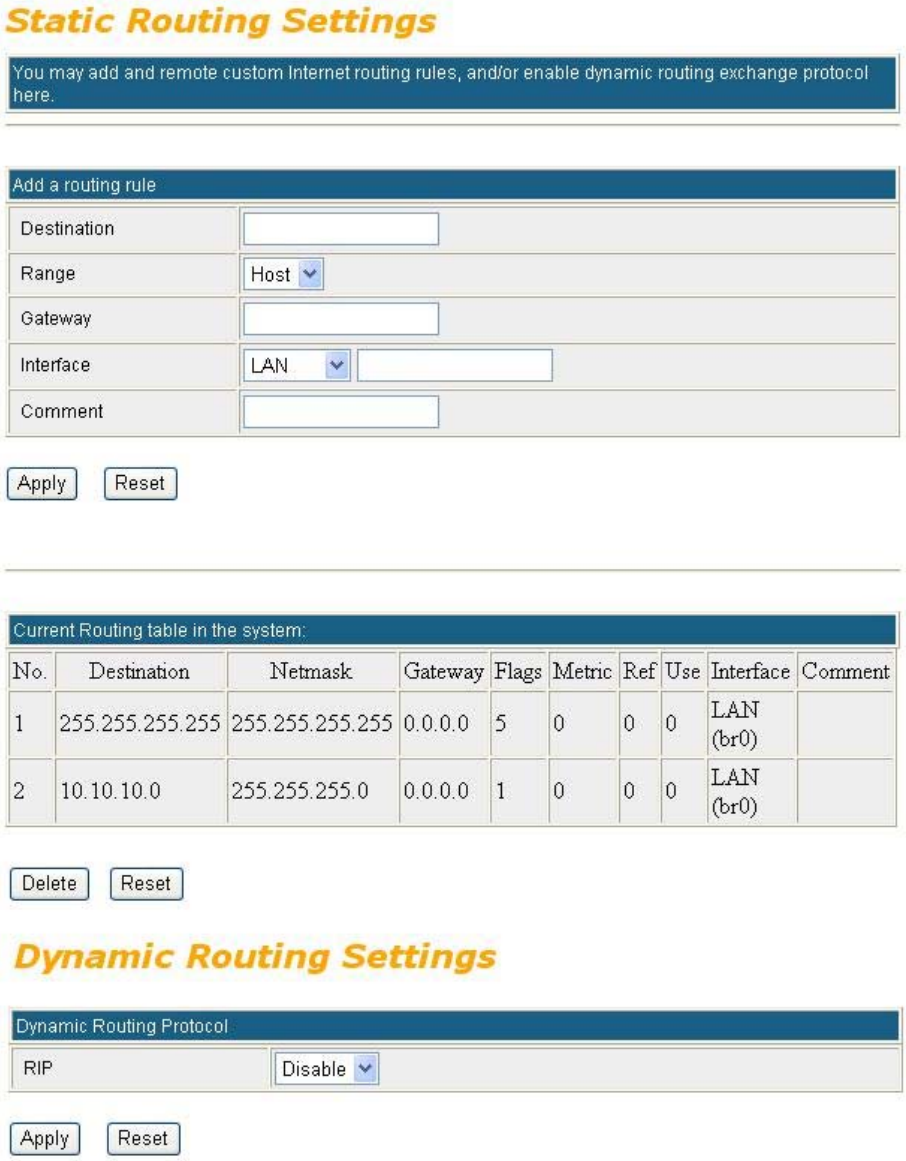
VPN passthrough configurations including: L2TP, IPSec, and PPTP passthrough.



L2TP Passthrough	L2TP, Layer Two Tunneling Protocol (L2TP). Use the L2TP with VPN that user can access the personal network via Internet. 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.

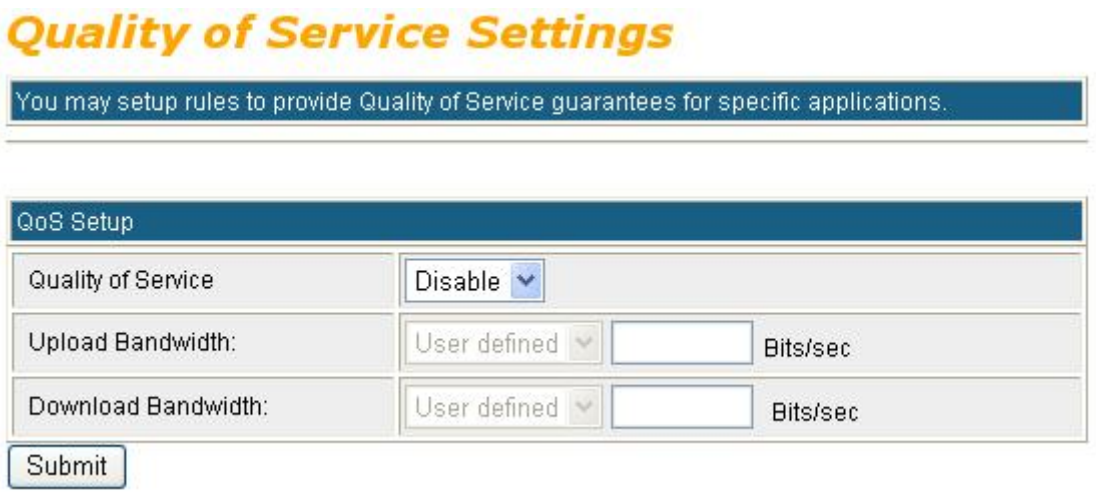
Advanced Routing (GW)

If you connect several routers with this Wireless Portable 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 Portable Router.
To set static routers, enter the settings including route IP address, route mask route gateway the route Interface from LAN or WAN.



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.

QoS



Quality of Service	Select Disable or Enable from the pull-down menu. (Default setting is Disable.)
Upload Bandwidth	Select User defined to enter the upload transmitting bandwidth bits/sec in the blank or select the upload bandwidth from pull-down list.
Download Bandwidth	Select User defined to enter the download transmitting bandwidth bits/sec in the blank or select the download bandwidth from pull-down list.

Wireless Settings

Gateway / Access Point Modes

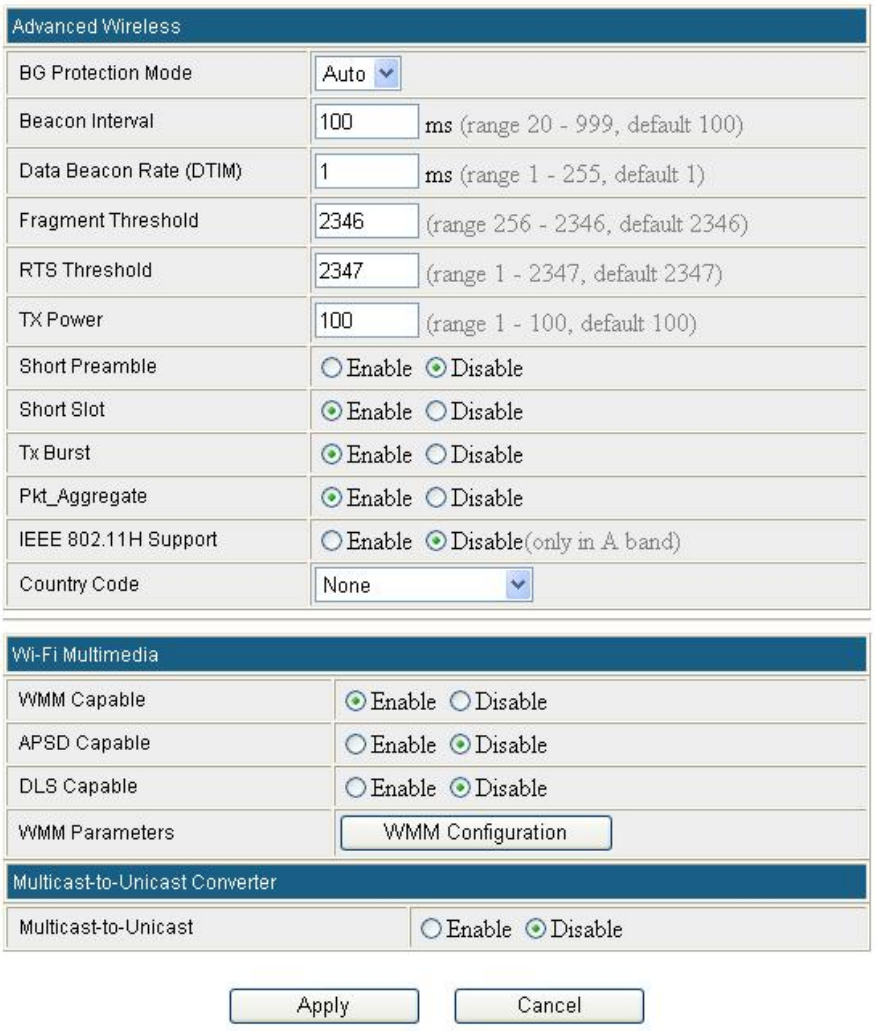
Basic

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 1~7	A multiple SSID is referred to a network name because essentially it is a name that identifies a wireless network.
Broadcast Network Name(SSID)	**Enable**: This wireless AP will broadcast its SSID to stations. **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.
MBSSID AP Isolation	Select Enable or Disable to enable this function.
BSSID	Shows the MAC address of the Wireless Portable Router.
Frequency (Channel)	Select 1~11 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	Select form the pull-down menu 0~15, 32 or Auto. (Default setting is Auto.)
Reverse Direction Grant(RDG)	Select Disable or Enable this function. (Default setting is Enable.)
Extension Channel	You can select 2457MHz (Channel 10) or 2417MHz (Channel 2) form the pull-down menu.
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.)
Other	
HT Tx Stream	Select 1 or 2 form the pull-down menu.
HT Rx Stream	Select 1 or 2 form the pull-down menu.
Apply	Click to save and apply the current settings.
Cancel	Click to discard the current settings.

Advanced

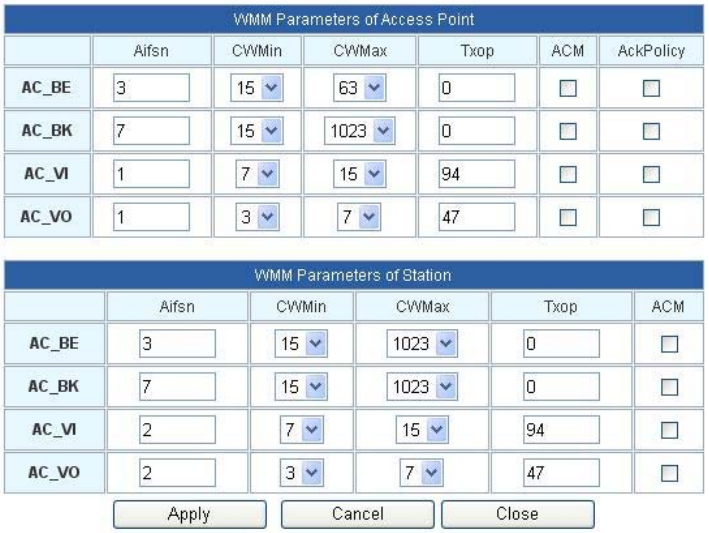
Advanced Wireless Settings

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.

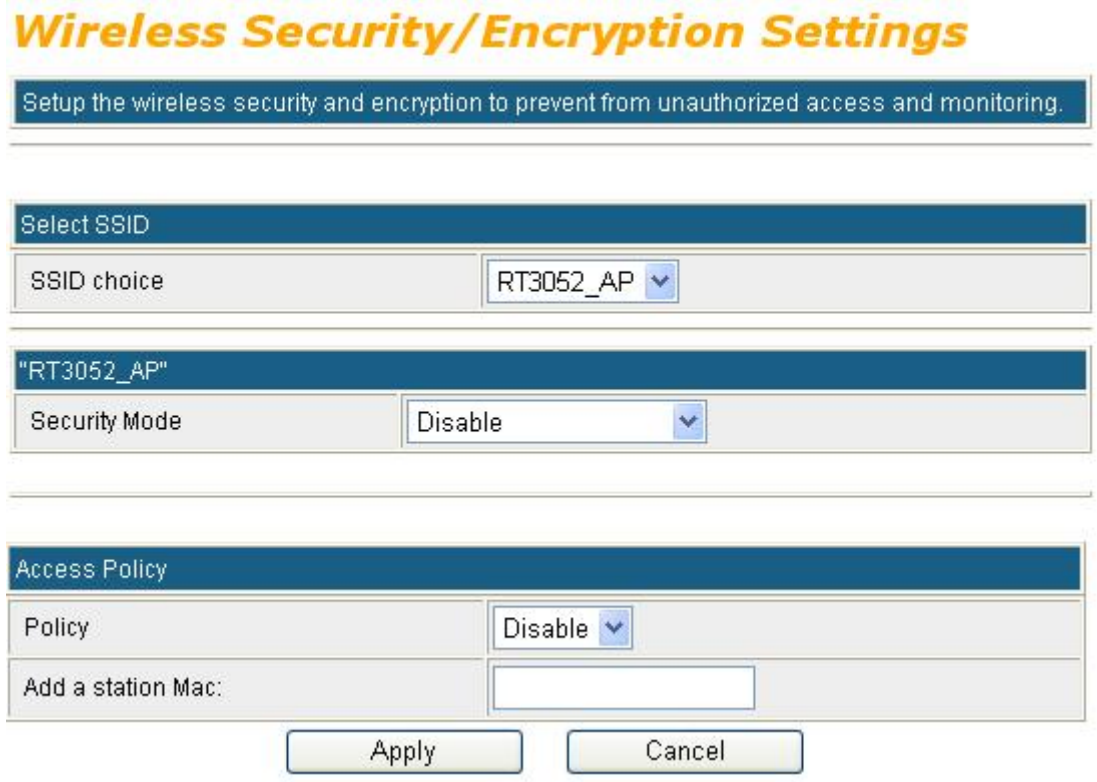


Advanced Wireless	
BG Protection Mode	Select the protection mode form the pull-down list, Auto, On and Off.
Beacon Interval	Beacon Interval is the amount of time between beacon transmissions. Before a station enters power save mode, the station needs the beacon interval to know when to wake up to receive 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	Fragmentation mechanism is used for improving the efficiency when high traffic flows along in the wireless network. If the Wireless Portable

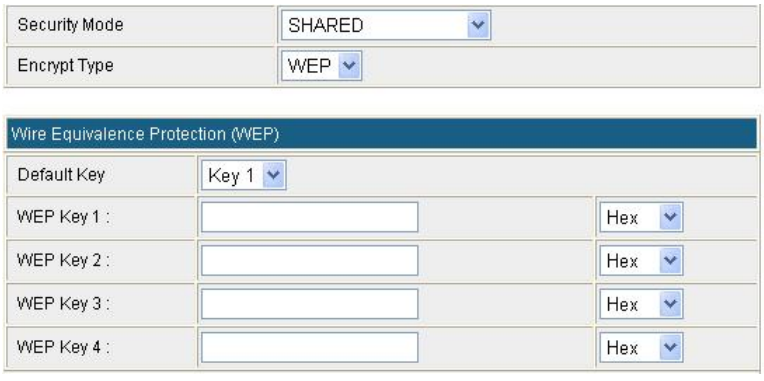
Threshold	Router often transmit large files in wireless network, you can enter new Fragment Threshold value to split the packet. The value can be set from 256 to 2346. (The default value is 2346.)
RTS Threshold	RTS Threshold is a mechanism implemented to prevent the "Hidden Node" problem. If the "Hidden 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.) **Warning:** Enabling RTS Threshold will cause redundant network overhead that could negatively affect the throughput performance instead of providing a remedy. This value should remain at its default setting of 2347. Should you encounter inconsistent data flow, only minor modifications of this value are recommended.
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 the box to enable the Tx Burst function. (Default Tx Burst setting is Enable.)
Pkt_Aggregate	Select Disable or Enable this function. (Default setting is Enable.)
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. 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. 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. Select Disable or Enable this function. (Default setting is Disable.)

WMM Parameters	Click the WMM Configuration button to go further settings. 
Multicast-to-Unicast Converter	
Multicast-to-Unicast	Select Disable or Enable this function. (Default setting is Disable.)

Security



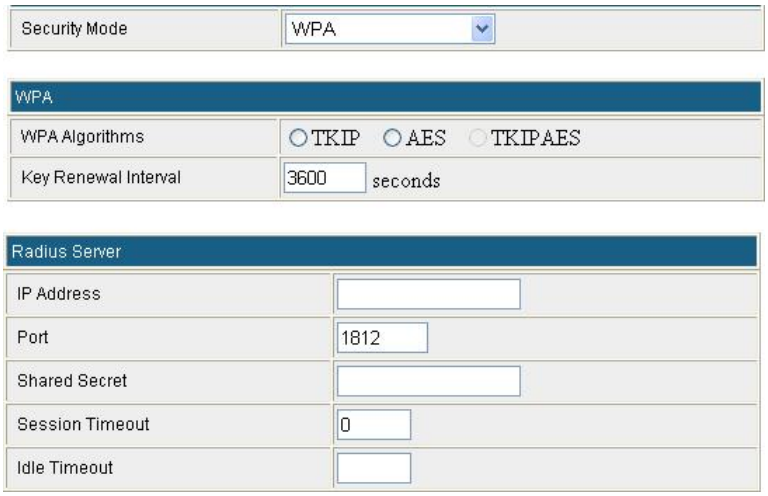
Wireless Security/Encryption Settings	
Select choice	Select SSID to set up the security form the pull-down list.

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. **Note:** ➢ WPA and WPA-PAK only support TKIP and AES as encryption method. ➢ SHARED only supports WEP as encryption method. ➢ WEP AUTO means AP can accept STA connect to it 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.  **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.  **Encryption Type**: The encryption type is WEP. **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).

WPA2, WPA2-PSK, WPA-PSK/WPA2-PSK, and WPA1 WPA2 offer three encryption methods, TKIP, AES and TKIP AES.

WPA/ WAP2/ WPA1 WPA2



WPA Algorithms: Select the type of algorithm, TKIP or AES for WPA, and TKIP, AES or TKIP AES for WPA2, WPA1/WPA2.
Key Renewal Interval: Enter the renewal security time (seconds) in the column. Default is 3600 seconds. Set 0 to disable re-key.

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**.)

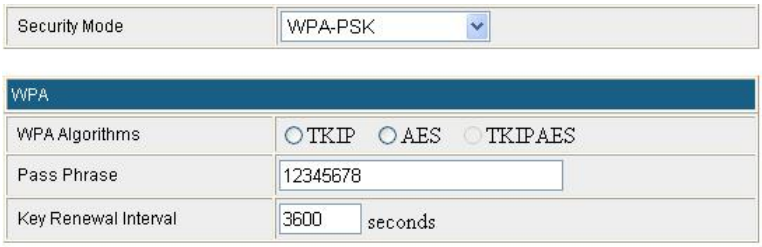
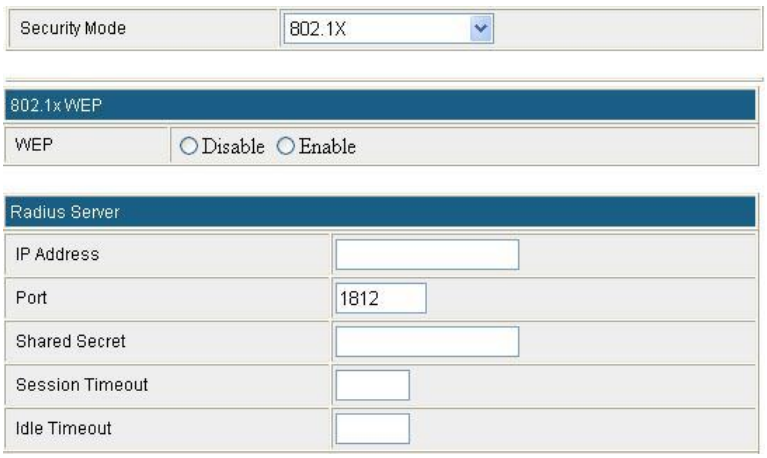
Shared Secret: Enter the password that the Wireless Portable Router shares with the RADIUS Server.

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.

Idle Timeout: Enter the idle timeout in the column.

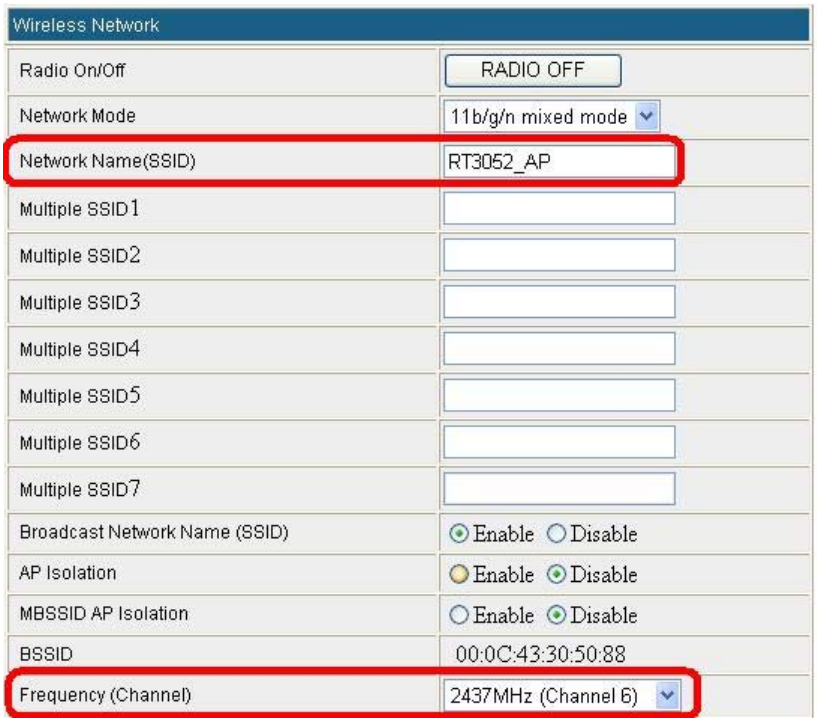
PMK Cache Period: Only valid in WPA2 security. Set WPA2 PMKID cache timeout period, after time out, the cached key will be deleted. PMK Cache Period unit is minute.

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.

	WPA-PSK/ WAP2-PSK/ WPA-PSK WPA2-PSK  **WPA Algorithms**: Select the type of algorithm, TKIP or AES for WP-PSK, and TKIP, AES or TKIP AES for WPA2-PSK, WPA1 PSK WPA2 PSK. **Pass Phrase**: Enter the pass phrase 8~63 ASCII or 64 HEX 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**  **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 Portable 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. **Idle Timeout**: Enter the idle timeout in the column.
Policy	Set access control policy of the stations. Select Disable, Allow or Reject form the pull-down menu.
Add a station Mac	Enter a station MAC in the blank field.

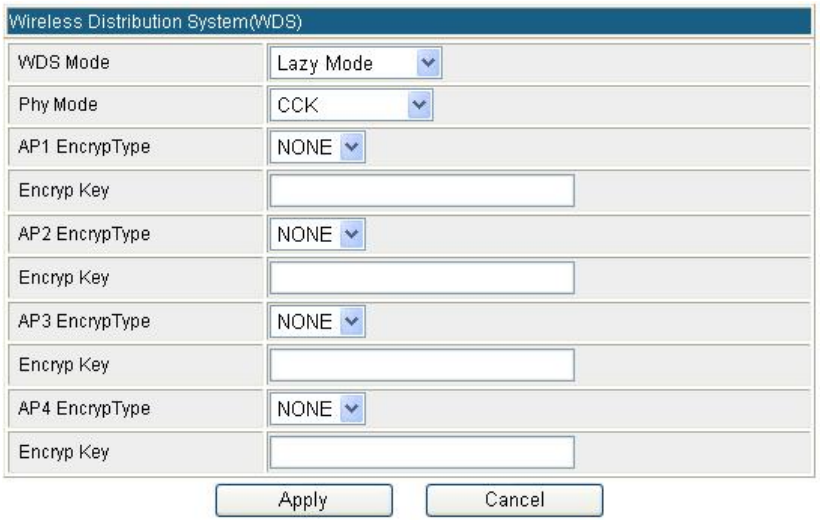
WDS

Wireless Distribution System

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.) 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** of each other to make the WDS connection. **Step 1**: Setup the same **SSID** and **Channel** on both wireless APs.  **Step 2**: Enter **Wireless MAC** address to each other(according to the WDS mode that user selected).

Lazy Mode

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



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 Portable 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.

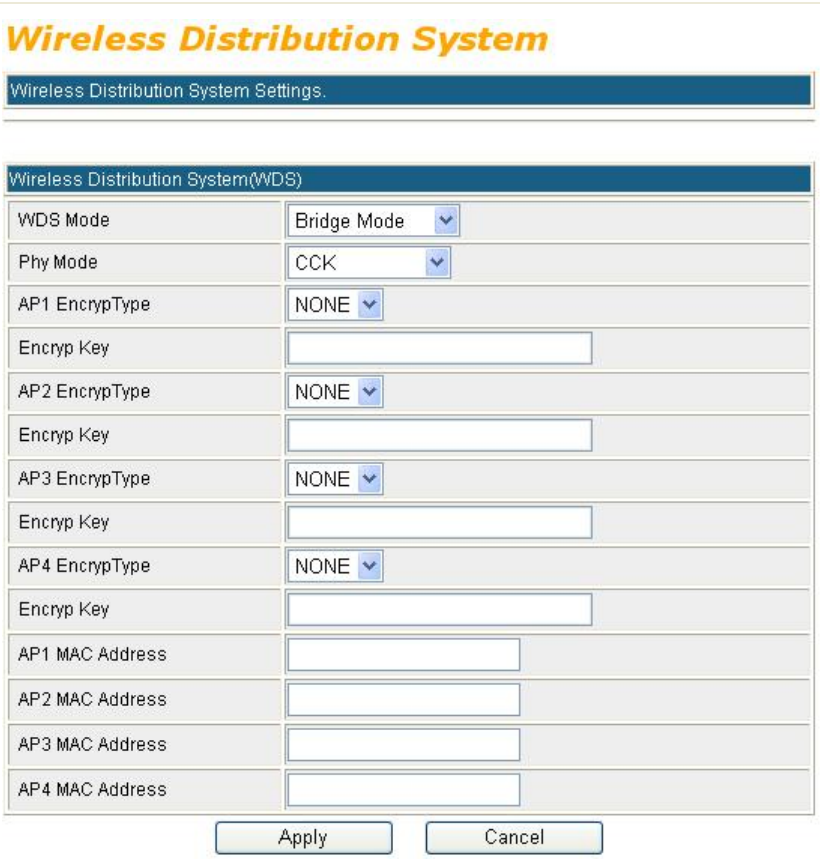
- **Hexadecimal (WEP 64 bits):** 10 Hex characters (0~9, a~f).
- **Hexadecimal (WEP 128 bits):** 26 Hex characters (0~9, a~f).
- **ASCII (WEP 64 bits):** 5 ASCII characters (case-sensitive).
- **ASCII (WEP 128 bits):** 13 ASCII characters (case-sensitive).

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.



Phy Mode: Select CCK, OFDM, HTMIX or GREENFIELD 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 Portable 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.

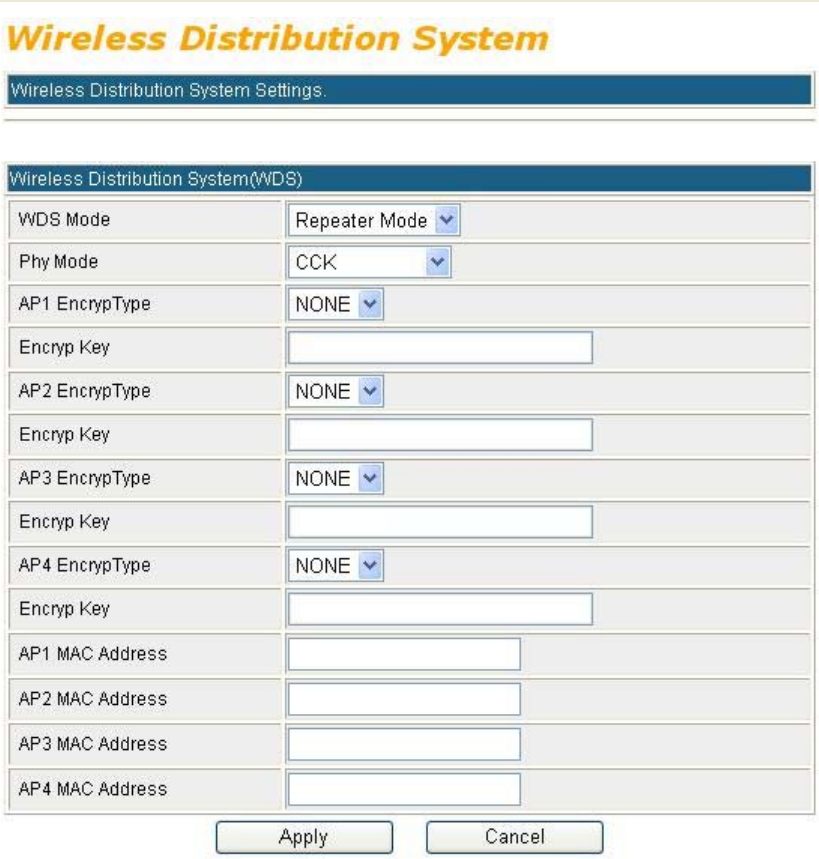
- **Hexadecimal (WEP 64 bits):** 10 Hex characters (0~9, a~f).
- **Hexadecimal (WEP 128 bits):** 26 Hex characters (0~9, a~f).
- **ASCII (WEP 64 bits):** 5 ASCII characters (case-sensitive).
- **ASCII (WEP 128 bits):** 13 ASCII characters (case-sensitive).

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.



Phy Mode: Select CCK, OFDM, HTMIX or GREENFIELD 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 Portable 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).

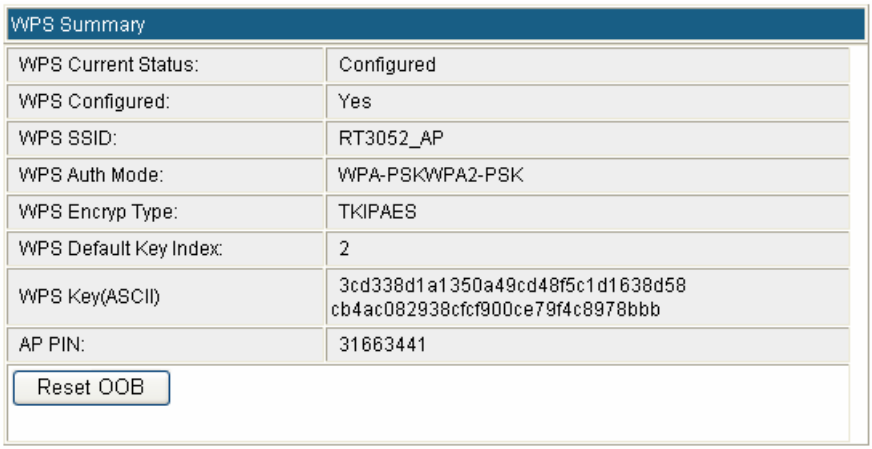
Select the type **WPA, WPA-PSK, WPA2, WPA2-PSK**, **WPA-PSK/ WPA2-PSK, WPA/WPA2** authentication, for **TKIP** or **AES** encryption.
If users select TKIP or AES encryption, please enter the password in the Encryption Key column that must be filled with characters longer than 8 and less than 64 lengths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

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

WPS

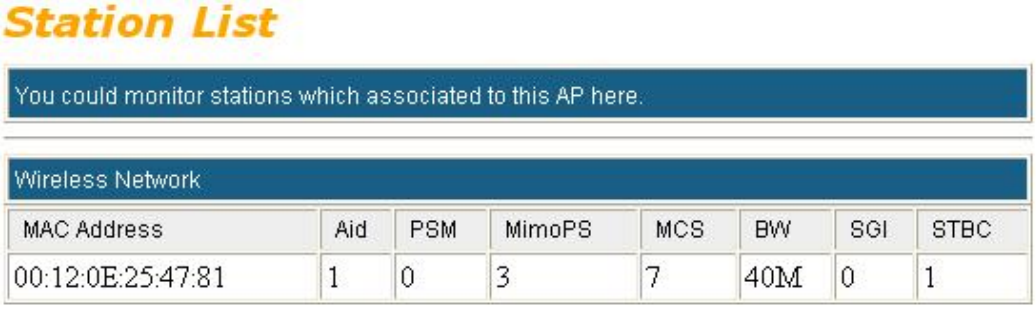
WPS Config	
WPS	Select **Enable** then click **Apply** to use WPS (Wi-Fi Protected Setup) function, then push physical WPS button on Wireless Portable Router to make a WPS connection. Default setting is **Disable**.
WPS Summary	
WPS Current	After enabling the WPS function, if there is connection the status will show

Status	Configured, otherwise, the status will show Idle.
WPS Configured	Trigger WPS AP to do simple config with WPS Client. If WPS configured, here shows Yes, otherwise, NO.
WPS SSID	Shows the Wireless Portable 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 the OOB (out-of-box) configuration.
WPS Process	
WPS mode	**PIN**: **Personal Identification Number**. Select PIN then click **Apply** to make a WPS connection. **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, the status shows Idle.



Station List

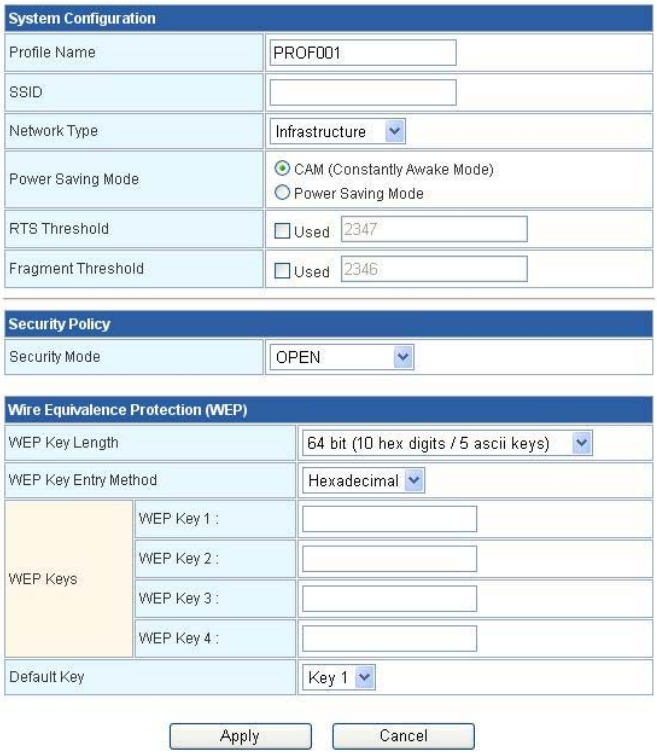
Here shows the station information that connected with the Wireless Portable Router.



Client Mode

Profile

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



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

SSID: Enter the station's network name here.

Network Type: Select Infrastructure or 802.11 Ad Hoc from the pull-down list.

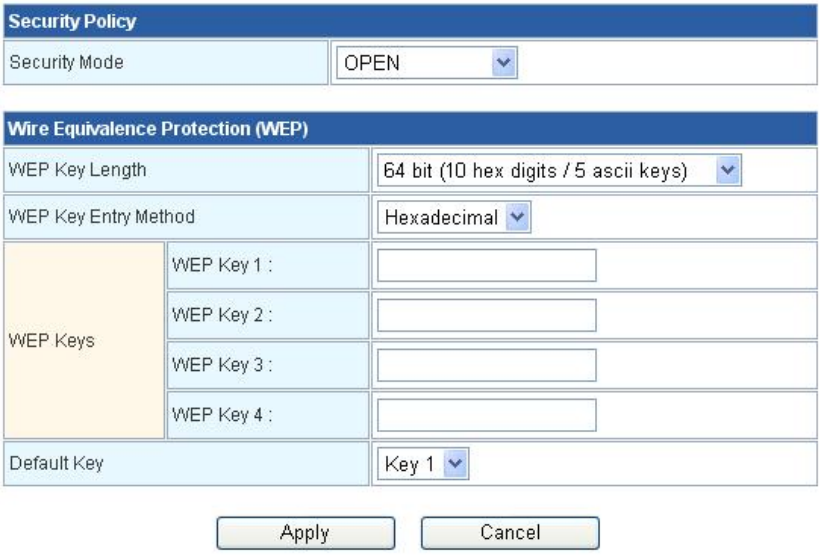
Power Saving Mode: CAM (Constantly Awake Mode) or Power Saving Mode.

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

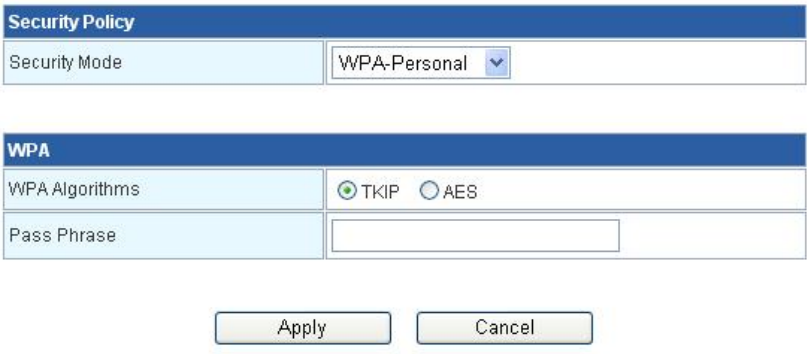


WEP Key Length/ WEP Key Entry Method: Only valid when using **WEP** encryption algorithm. There are several formats to enter the keys.

- **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



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

This page shows the linking information of the station.

Station Link Status

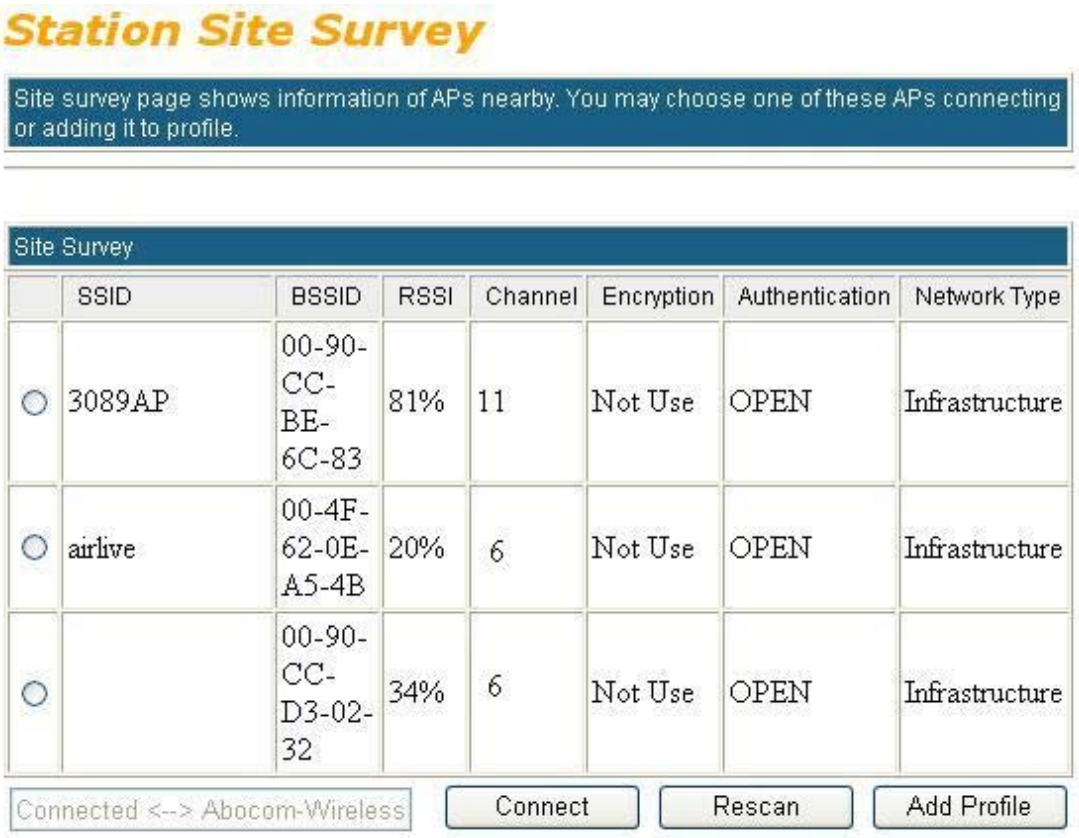
The Status page shows the settings and current operation status of the Station.

Link Status		
Status	3GSHARE <--> 00-0C-43-30-50-30	
Extra Info	Link is Up	
Channel	6 <--> 2437000 KHz ; Central Channel: 8	
Link Speed	Tx(Mbps) 135.0	Rx(Mbps) 58.5
Throughput	Tx(Kbps) 0.0	Rx(Kbps) 242.9
Link Quality	Good 73%	
Signal Strength 1	Weak 32%	☐ dBm format
Signal Strength 2	Weak 16%	
Signal Strength 3	Weak 8%	
Noise Level3	Strength 100%	

HT	
BW	40
GI	long
STBC	none
MCS	7
SNR0	7
SNR1	4898576

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.



Statistics

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

Station Statistics

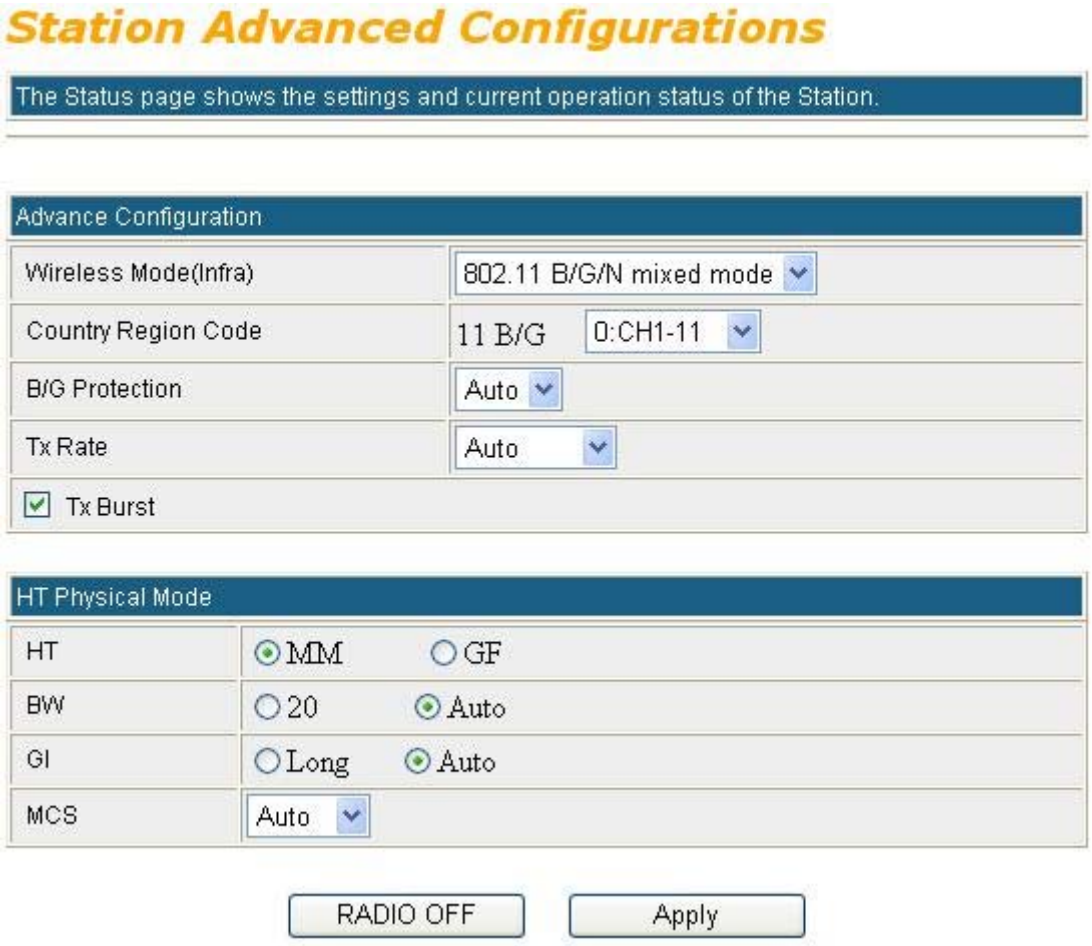
The Status page shows the settings and current operation status of the Station.

Transmit Statistics	
Frames Transmitted Successfully	1127
Frames Transmitted Successfully Without Retry	357
Frames Transmitted Successfully After Retry(s)	770
Frames Fail To Receive ACK After All Retries	1
RTS Frames Sucessfully Receive CTS	0
RTS Frames Fail To Receive CTS	0

Receive Statistics	
Frames Received Successfully	73702
Frames Received With CRC Error	62827
Frames Dropped Due To Out-of-Resource	0
Duplicate Frames Received	10

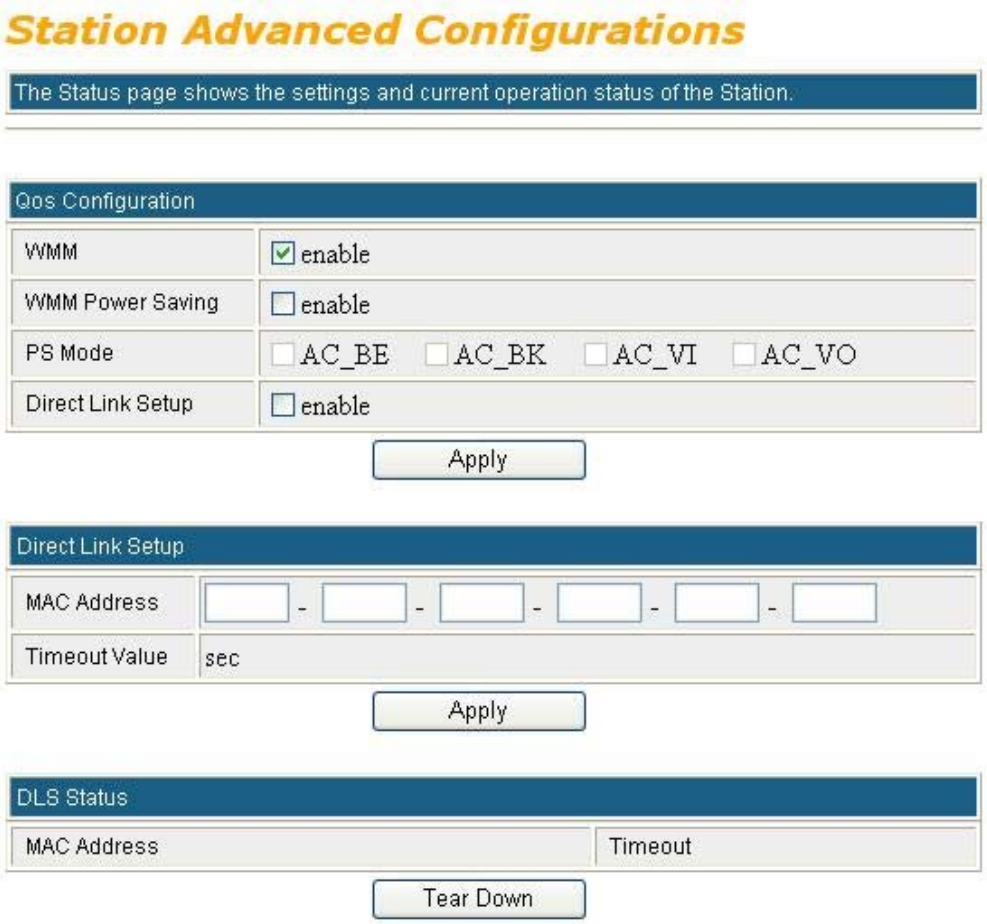
Reset Counters Refresh

Advanced



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.)
B/G Protection	Select **Auto**, **On** or **Off** from the pull-down menu.
Tx Rate	Select preferred Tx rate form the pull-down list.
Tx Burst	Check the box to enable the Tx Burst function. (Default Tx Burst setting is Enable.)
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.)
MCS	Select form the pull-down menu 0~15, 32 or Auto. (Default setting is Auto.)
RADIO OFF	Click this button to turn on or off the wireless function.

QoS



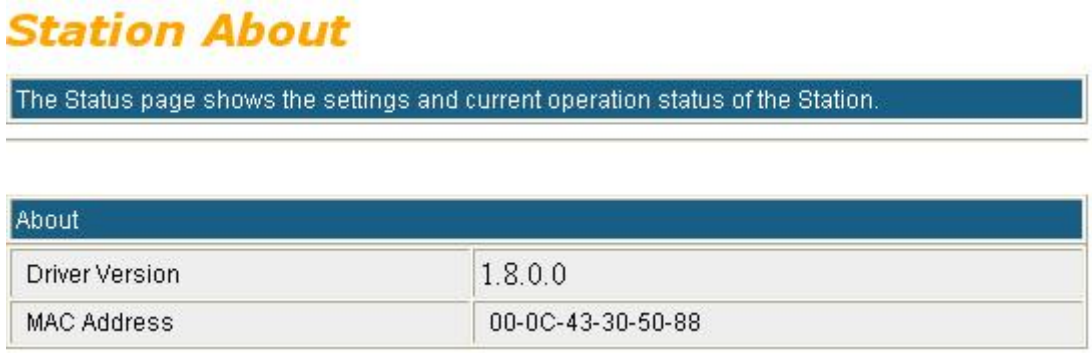
WMM	Check the box to enable or disable the WMM function. (Default setting is Enable.)
WMM Power Saving	Check the box to enable this function. (Default setting is disable.)
PS Mode	Select preferred power save mode, AC_BE, AC_BK, AC_VI, AC_VO.
Direct Link Setup	Check the box to enable Direct Link Setup (DLS) and enter the MAC address in below column. 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.
Tear Down	Click the Tear Down button to disable the DLS function.

11n Configurations

MPDU Aggregation	Check the box to enable this function. (Default setting is Disable.) Select **Manual** or **Auto** to set up the **MPDU desity** form 0~7. Default setting is Auto.
Aggregation MSDU (A-MSDU)	Check the box to enable this function. (Default setting is Disable.)

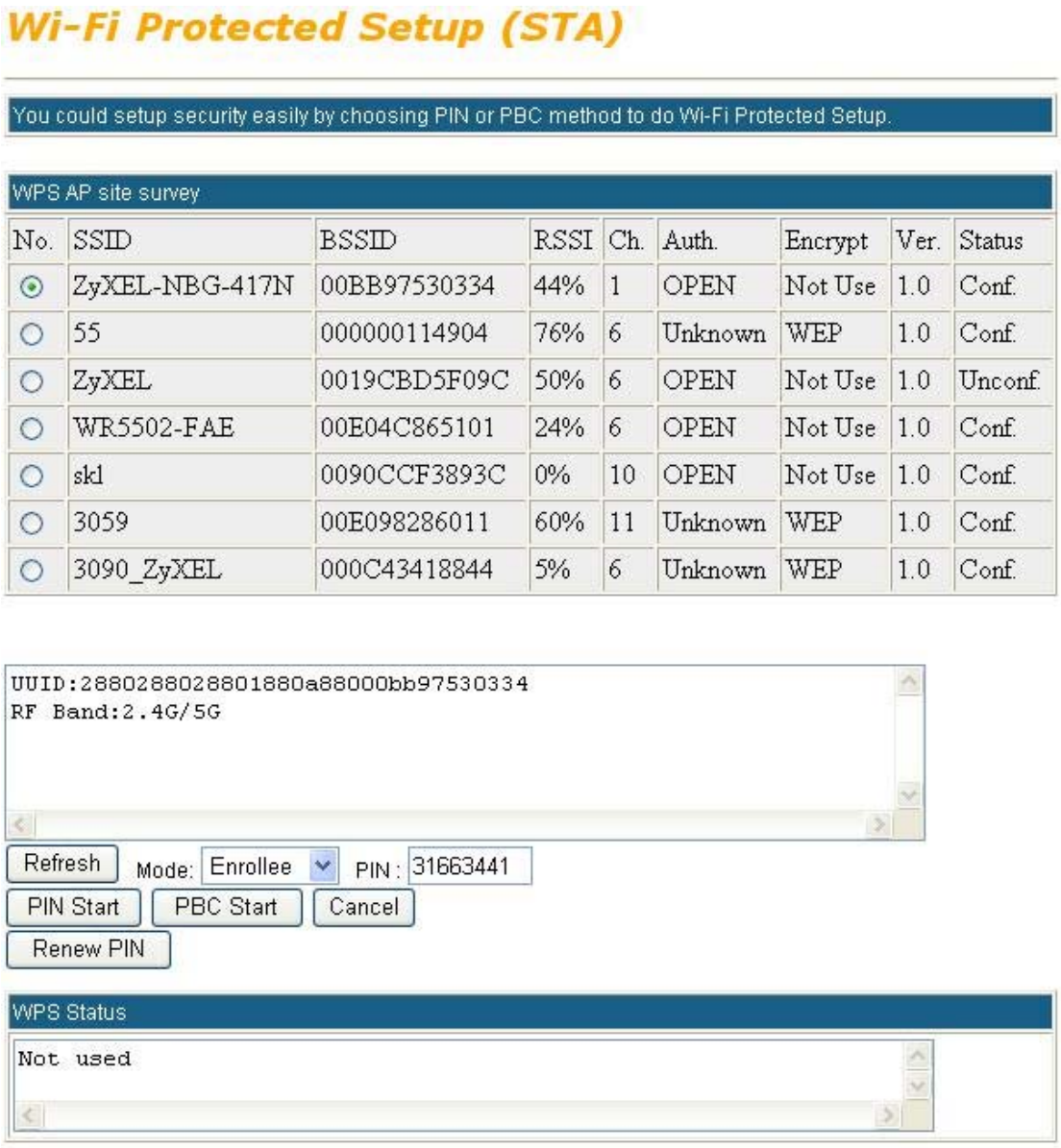
About

Here shows the information of the station.



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.



WPS AP Site Survey	Display the information of surrounding APs with WPS function from last scan result. List information included SSID, BSSID, 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. **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. **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 status of the WPS function.

Firewall (GW)

MAC/IP/Port Filtering

MAC/IP/Port Filtering Settings

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

Basic Settings	
MAC/IP/Port Filtering	Enable
Default Policy -- The packet that don't match with any rules would be:	Dropped.

Apply Reset

MAC/IP/Port Filter Settings	
MAC address	
Dest IP Address	
Source IP Address	
Protocol	None
Dest Port Range	-
Source Port Range	-
Action	Accept
Comment	

(The maximum rule count is 32.)

Apply Reset

Current MAC/IP/Port filtering rules in system:

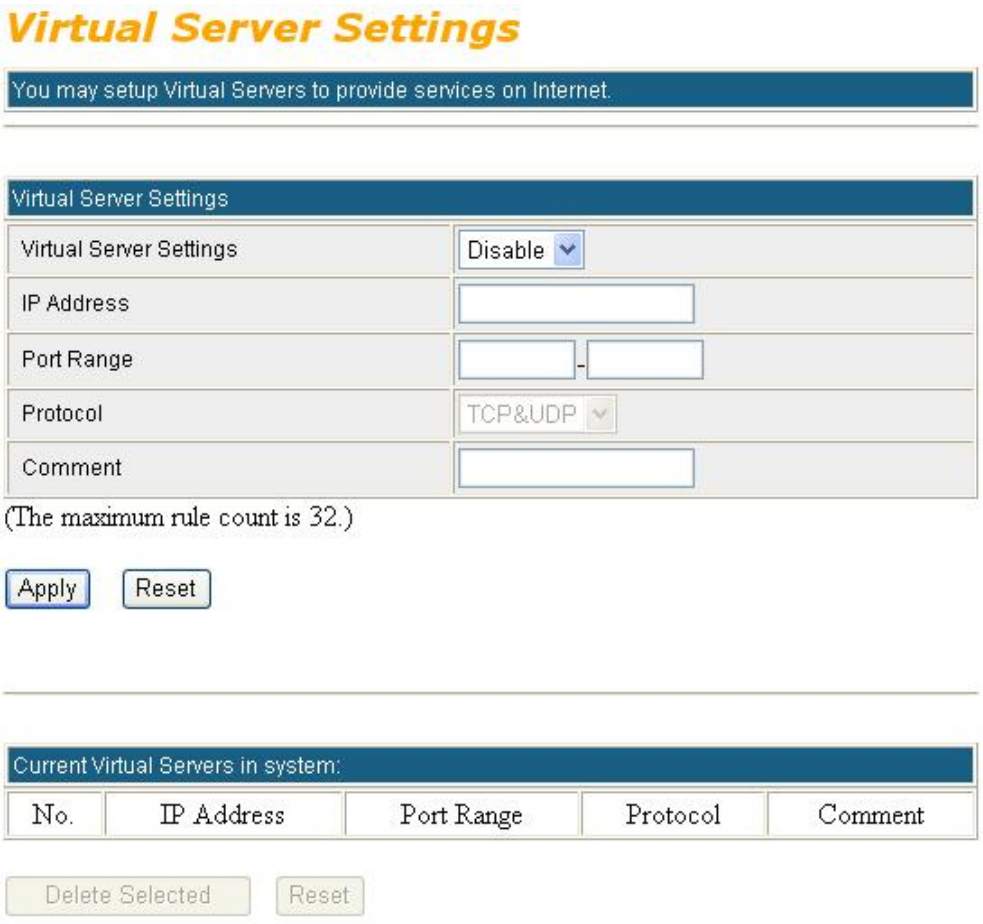
No.	MAC address	Dest IP Address	Source IP Address	Protocol	Dest Port Range	Source Port Range	Action	Comment	Pkt Cnt
1 ☐	00:12:0E:25:47:81	10.10.10.101	255.255.255.0	-	-	-	Accept		0
Others would be dropped									-

Delete Selected Reset

MAC/IP/Port Filtering	Select Enable or Disable from the pull-down list.
Default Policy -- The packet	Select Accepted or Dropped from the pull-down menu, to accept

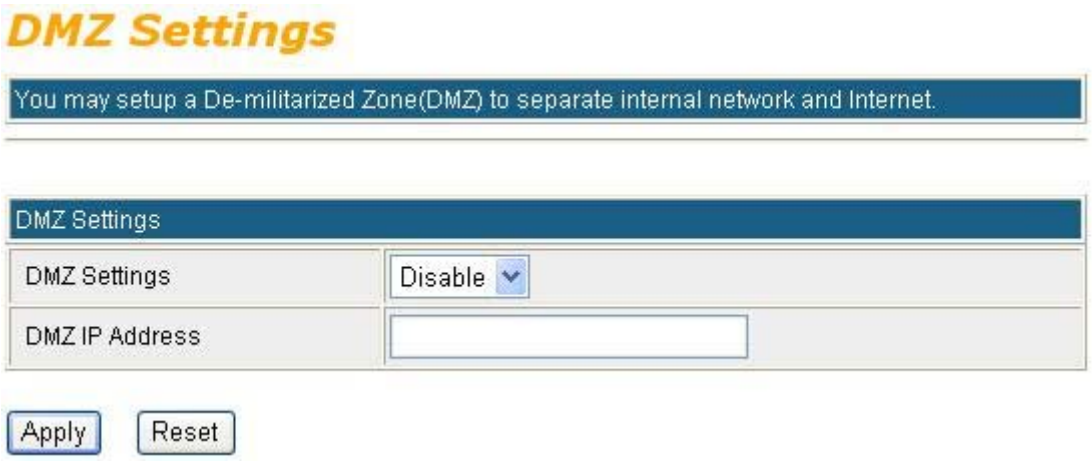
that don't match with any rules would be:	or deny connection for the MAC that user set in below settings.
Apply	Click to save and apply the current settings.
Reset	Press to discard the current settings.
MAC Address	Enter the client MAC address that user would like to connect(accept) or disconnect(drop).
Dest IP Address	Enter the local server's IP address.
Source IP Address	Enter the source IP address.
Protocol	Select the protocol (None, TCP, UDP or ICMP) used to the remote system or service.
Dest Port Range **Source 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.
Action	Select rules for DROP, or rules for ACCEPT form the pull-down menu. Select Drop to disconnect with the Wireless Portable Router that MAC address has be set, and ACCEPT to allow the device that connect with the Wireless Portable Router.
Comment	Key in a description for these settings.

Port Forwarding



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 IP address.

DMZ

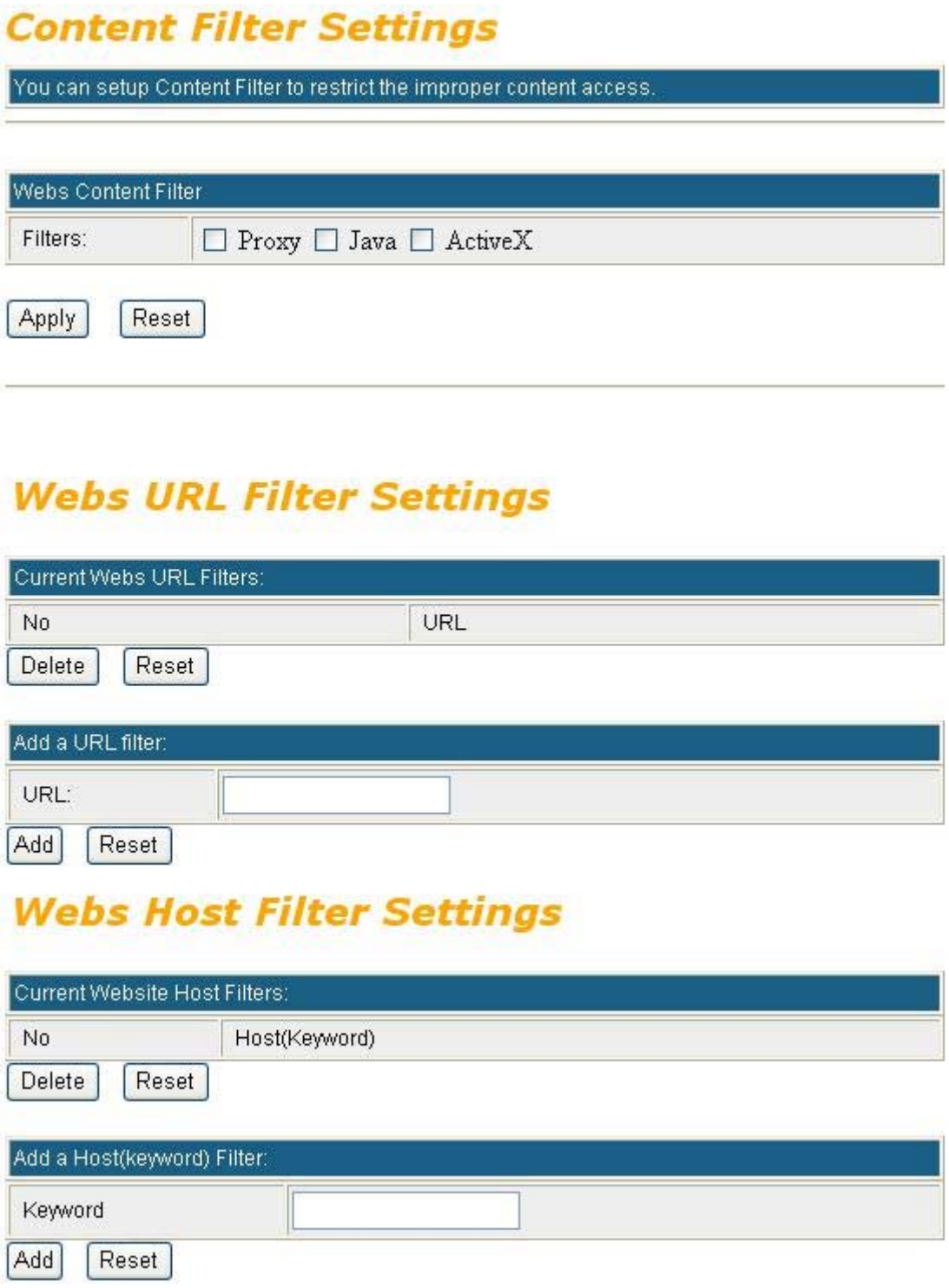


DMZ Settings	If the DMZ Host Function is enabled, it means that you set up DMZ host at a particular computer to be exposed to the Internet so that some applications/software, especially Internet / online game can have two-way connections. Select Enable or Disable from the pull-down menu.
DMZ IP Address	Enter the IP address of a particular host in your LAN that will receive all the packets originally going to the WAN port/ Public IP address above. **Note: You need to give your LAN PC clients a fixed/ static IP address for DMZ to work properly.**
Apply	Click to save and apply the current settings.
Reset	Press to discard current settings.

System Security

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 Portable Router via WAN. Default setting is Deny.
Ping form WAN Filter	
Ping form WAN Filter	Select Disable or Enable from the pull-down list. Default setting is Disable.
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. Select Disable or Enable the SPI firewall function from the pull-down list. Default setting is Disable.

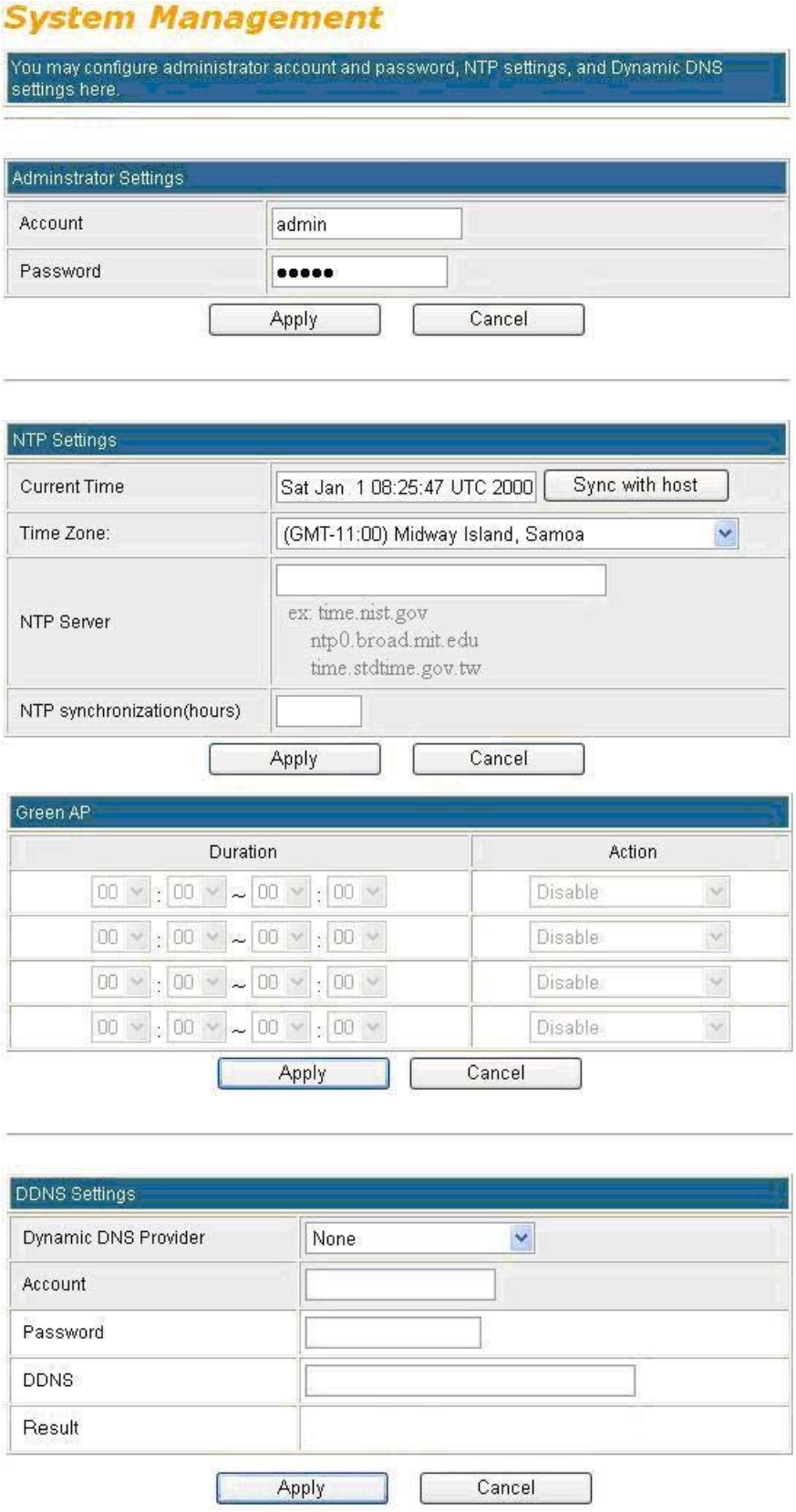
Content Filtering



Webs Content Filter Settings	Select Webs Content Filters, Proxy, Java or ActiveX.
Webs URL Filter Settings	Enter the IP address for URL filtering.
Webs Host Filter Settings	Enter the keyword in the field for a host filtering.

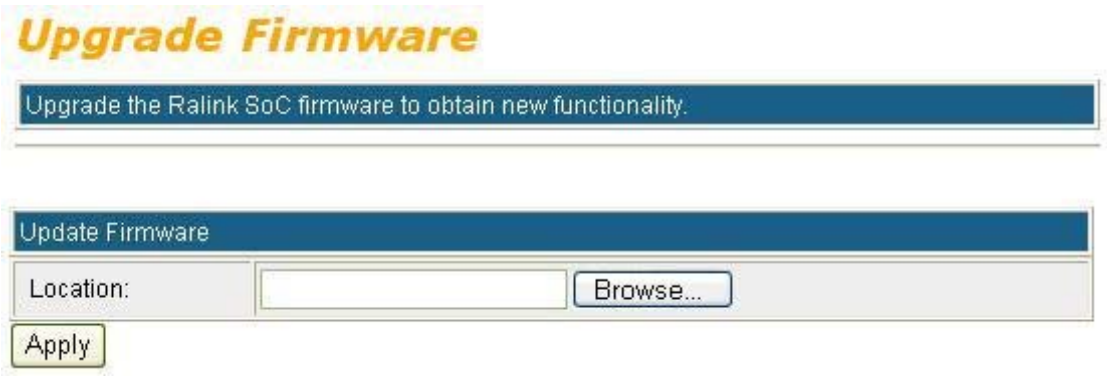
Administrator

Management



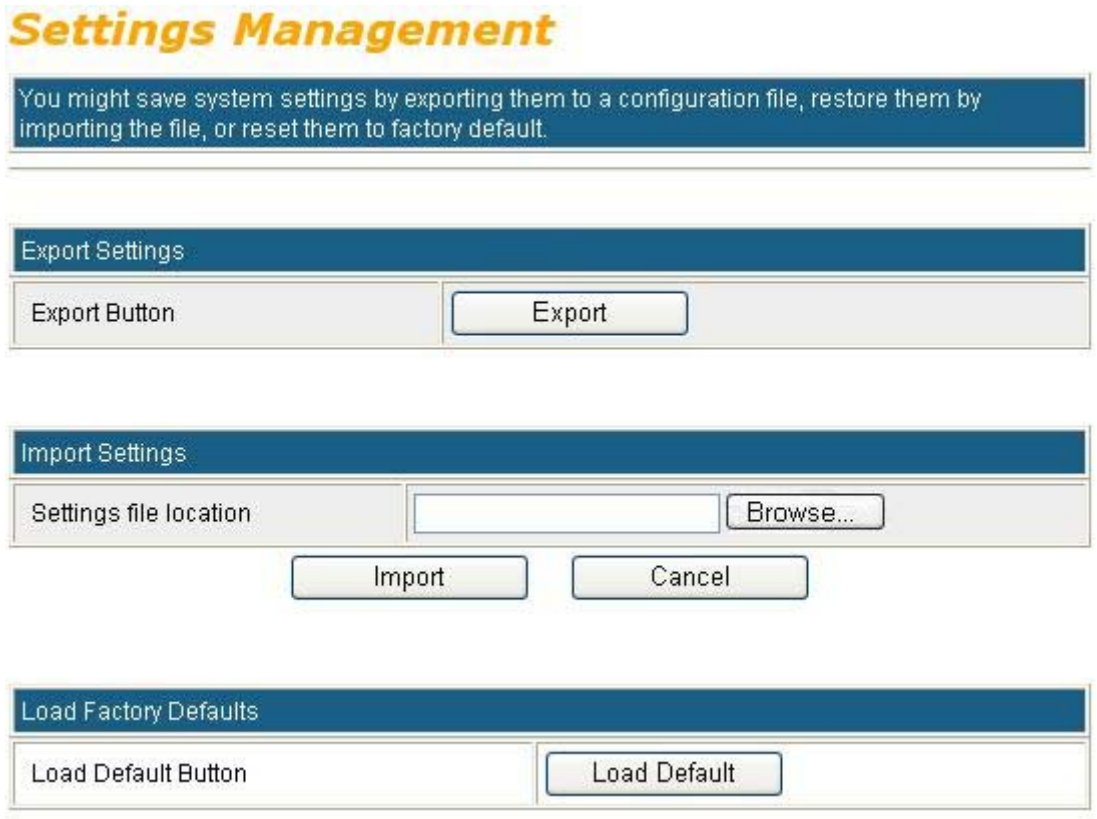
Administrator Settings	
Account	Key in a new login user name in the blank field.
Password	Maximum input is 36 alphanumeric characters (case sensitive.)
NTP Settings	
Current Time	Click **Sync with host** button to synchronize the time with the server.
Time Zone	Select the time zone area that you located 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)	Enter the hour(s) here to synchronize time of the Wireless Portable Router with the server selected.
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. 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 Portable 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



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

Settings Management



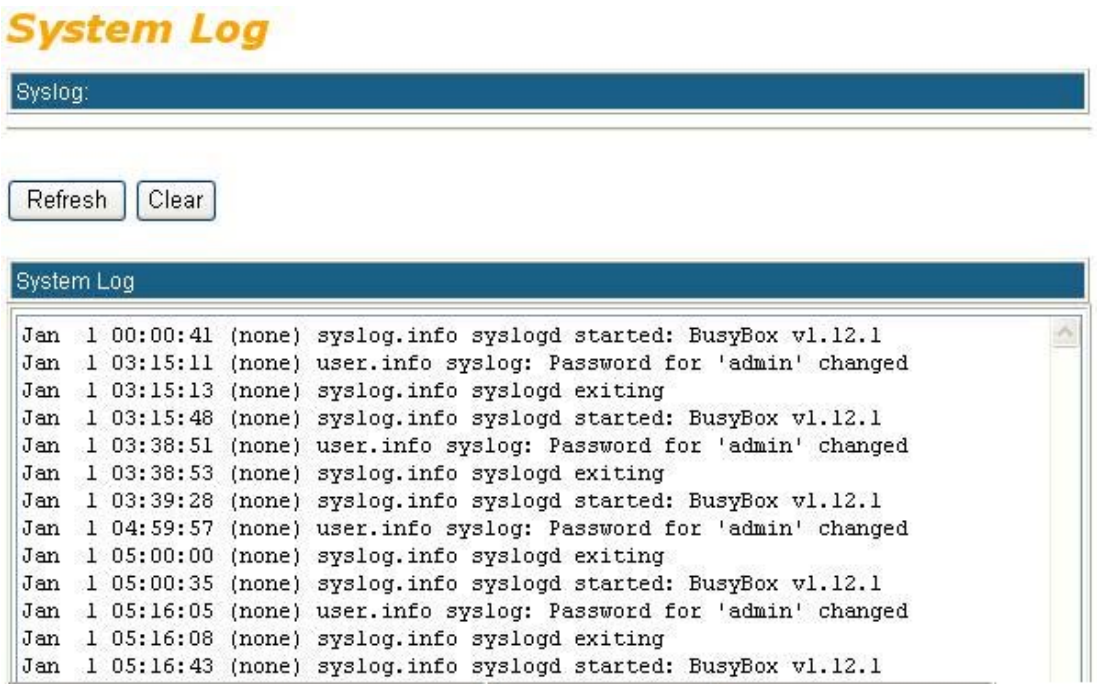
Export Settings	
Export Button	Click the **Export** button to save the current device settings to located computer.
Import Settings	
Import	Click the **Browse…** button, find and open the settings file (the browser will display to correct file path), then click the **Import** button to use the device 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 Portable Router back to factory default settings.

Statistics

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

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.



Reboot

Click the **Reboot** button to restart the Wireless Portable 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 Portable Router.
- The first step is to check the PC's TCP/IP settings.
- The Wireless Portable 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 Portable Router settings, and default Windows TCP/IP settings, no changes need to be made.

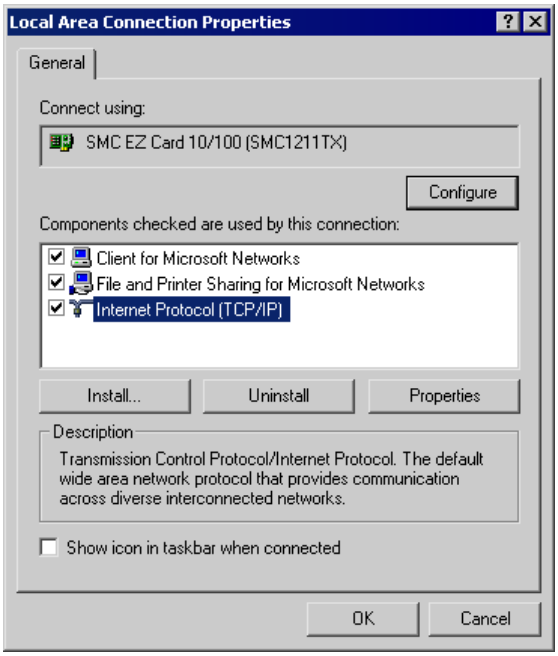
- By default, the Wireless Portable Router will act as a DHCP Server, automatically providing a suitable IP Address (and related information) to each PC when the PC boots.
- For all non-Server versions of Windows, the default TCP/IP setting is to act as a DHCP client.

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

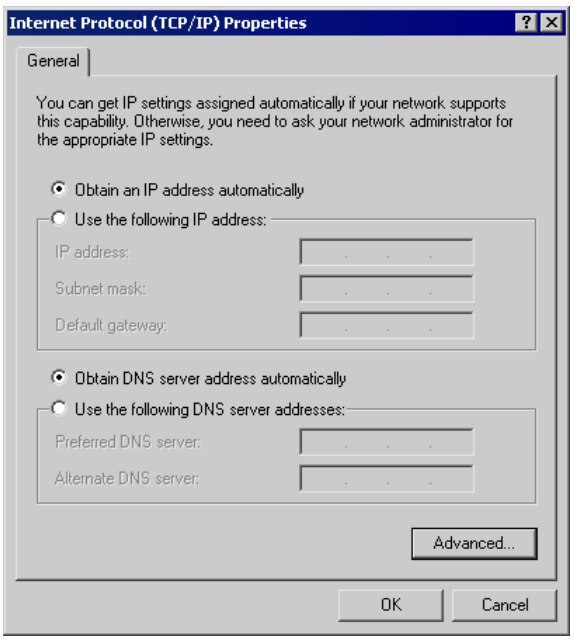
- The *Gateway* must be set to the IP address of the Wireless Portable Router.
- The *DNS* should be set to the address provided by your ISP.

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:



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.



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 Portable Router will act as a DHCP Server.
- Restart your PC to ensure it obtains an IP Address from the Wireless Portable Router.

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

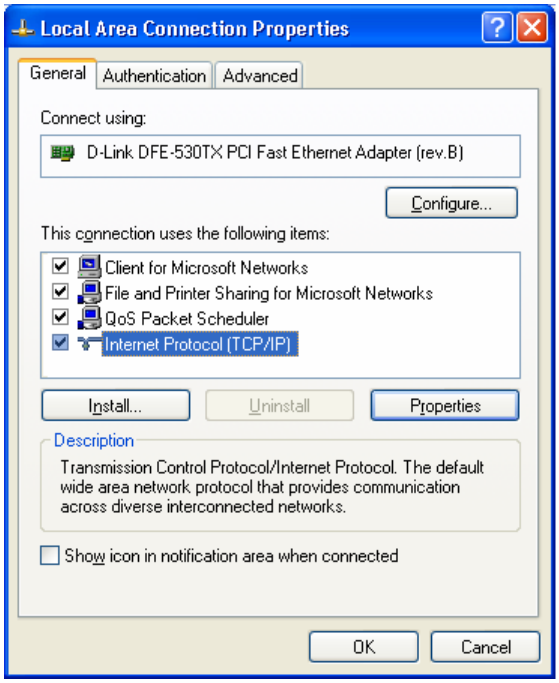
If your PC is already configured, check with your network administrator before making the following changes.

- Enter the Wireless Portable 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 Portable Router.)

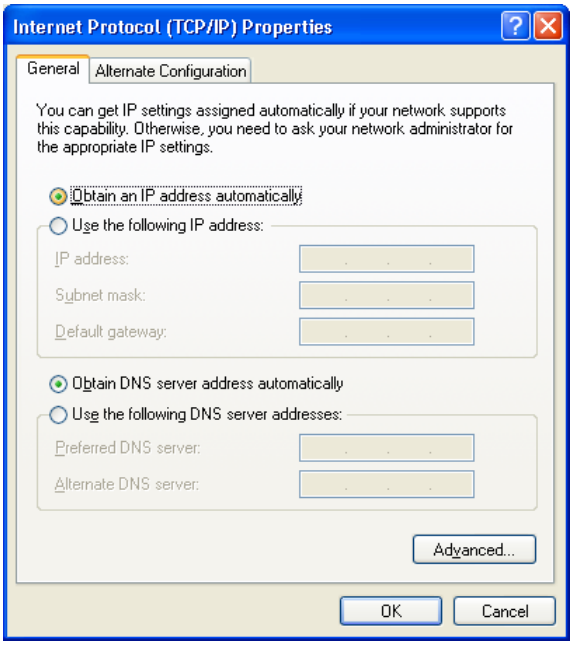
- If the *DNS Server* fields are empty, select *Use the following DNS server addresses*, and enters the DNS address or addresses provided by your ISP, then click *OK*.

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:



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.



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 Portable Router will act as a DHCP Server.
- Restart your PC to ensure it obtains an IP Address from the Wireless Portable 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 Portable Router 's IP address and click *OK*. Your LAN administrator can advise you of the IP Address they assigned to the Wireless Portable 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 Portable 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 Portable 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 Portable 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 Portable Router " location.

Macintosh Clients

From your Macintosh, you can access the Internet via the Wireless Portable 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 Portable Router 's IP Address.
- Ensure your DNS settings are correct.

Linux Clients

To access the Internet via the Wireless Portable Router, it is only necessary to set the Wireless Portable 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 Portable 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 Portable Router:

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

Wireless Station Configuration

- This section applies to all wireless stations wishing to use the Wireless Portable Router 's access point, regardless of the operating system that is used on the client.
- To use the Wireless Portable 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 Portable Router. ***Note! The SSID is case sensitive.***
Open **Shared Key**	If there is no security is enabled on the Wireless Portable Router, the security of each station should be disabled as well. And, you can connect the Wireless Portable Router without security, but it is NOT recommended.
WEP auto	By default, WEP on the Wireless Portable Router is disabled. • If WEP remains disabled on the Wireless Portable Router, all stations must have WEP disabled. • If WEP is enabled on the Wireless Portable Router, each station must use the same settings as the Wireless Portable Router.
WPA-PSK **WPA2-PSK** **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 Portable Router. To make a connection, each station must use the same algorithms and pass phrase as the Wireless Portable Router.
WPA **WPA2** **WPA WPA2** **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 Portable Router will allow 802.11b, 802.11g and 802.11n connections.

Appendix A: Troubleshooting

Overview

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

General Problems

Problem 1:	Can't connect to the Wireless Portable Router to configure it.
Solution 1:	Check the following: • Check the Wireless Portable Router is properly installed, LAN connections are OK, and it is powered ON. • Ensure that your PC and the Wireless Portable Router are on the same network segment. • If your PC is set to "Obtain an IP Address automatically" (DHCP client), please restart it. • 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 Portable Router's default IP Address of 10.10.10.254. Also, the Network Mask should be set to 255.255.255.0 to match the Wireless Portable Router. 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. • 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. • If the PCs are configured correctly, but still not working, check the Wireless Portable 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 Portable 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 Portable Router.
Solution 2:	The Wireless Portable Router processes the data passing through it, so it is not transparent. Use the *Content Filter Settings* feature to allow the use of Internet applications, which do not function correctly. If this does solve the problem you can use the *DMZ* function. This should work with almost every application, but: • It is a security risk, since the firewall is disabled. • Only one (1) PC can use this feature.

Wireless Access

Problem 1:	My PC can't locate the Wireless Portable Router.
Solution 1:	Check the following: • Your PC is set to *Infrastructure Mode*. (Access Points are always in *Infrastructure Mode*) • The SSID on your PC and the Wireless Portable Router are the same. Remember that the SSID is case-sensitive. So, for example "**W**orkgroup" does NOT match "**w**orkgroup." • Both your PC and the Wireless Portable Router must have the same setting for security. The default setting for the Wireless Portable Router security is disabled, so your wireless station should also have security disabled. • If security is enabled on the Wireless Portable Router, your PC must have security enabled, and the key must be matched. • To see if radio interference is causing a problem, see if connection is possible when close to the Wireless Portable 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: • Wireless Portable Router location Try adjusting the location and orientation of the Wireless Portable Router. • Wireless Channel If interference is the problem, changing to another channel may show a marked improvement. • Radio Interference 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 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 Portable 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.

- Access Points use a fixed Channel. You can select the Channel used. This allows you to choose a Channel which provides the least interference and best performance. In the USA and Canada, 11 channel are available. If using multiple Access Points, it is better if adjacent Access Points 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.)

Note to US model owner: To comply with US FCC regulation, the country selection function has been completely removed from all US models. The above function is for non-US models only.

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. 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 Portable Router. ***Note! The SSID is case sensitive.***
Open **Shared Key**	If there is no security is enabled on the Wireless Portable Router, the security of each station should be disabled as well. And, you can connect the Wireless Portable Router without security, but it is NOT recommended.
WEP AUTO	By default, WEP on the Wireless Portable Router is disabled. • If WEP remains disabled on the Wireless Portable Router, all stations must have WEP disabled. • If WEP is enabled on the Wireless Portable Router, each station must use the same settings as the Wireless Portable Router.

WPA-PSK **WPA2-PSK** **WPA-PSK WPA2-PSK**	WPA-PSK (TKIP/AES)/ WPA2-PSK (TKIP/AES: If one of these securities is enabled on the Wireless Portable Router. To make a connection, each station must use the same algorithms and pass phrase as the Wireless Portable Router.
WPA **WPA2** **WPA WPA2** **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.