

Wireless 802.11b/g/n Portable 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.....	1
Features.....	1
Physical Details.....	1
CHAPTER 2: ABOUT OPERATION MODES.....	3
Operation Modes.....	3
Access Point Mode.....	3
Gateway Mode.....	4
Client Mode.....	5
CHAPTER 3: CONFIGURATION.....	6
Hardware Connection.....	6
Login.....	6
Wizard (GW).....	10
Internet Settings.....	15
Wireless Settings.....	23
Firewall (GW).....	47
Administrator.....	54
CHAPTER 4: PC CONFIGURATION.....	59
Overview.....	59
Windows Clients.....	59
Macintosh Clients.....	63
Linux Clients.....	63
Other Unix Systems.....	64
Wireless Station Configuration.....	64
APPENDIX A: TROUBLESHOOTING.....	65
Overview.....	65
General Problems.....	65
Internet Access.....	65
Wireless Access.....	66
APPENDIX B: ABOUT WIRELESS LANS.....	68
BSS.....	68
Channels.....	68
Security.....	68
Wireless LAN Configuration.....	69

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

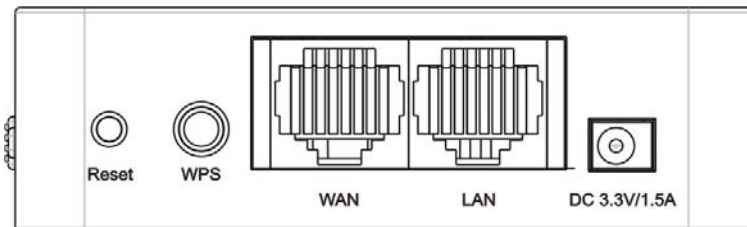
Front LEDs



LED Behavior				
LED	Printed	Color	Behavior	Indication
Power		Green	ON	Power on
			OFF	Power off
WPS		Green	ON	WPS function on
			OFF	WPS function off
			Blinking	WPS is enabled to make a connection

Wireless LAN		Green	OFF	WLAN off
			ON	WLAN link / active
			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 (Go to Wireless Settings> WPS), then press the physical WPS button on the Wireless Portable Router once, then the GREEN LED will start to flash. Please 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 (RJ45 connectors).
LAN	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.
DC 3.3V/1.5A	Connect the supplied power adapter here.

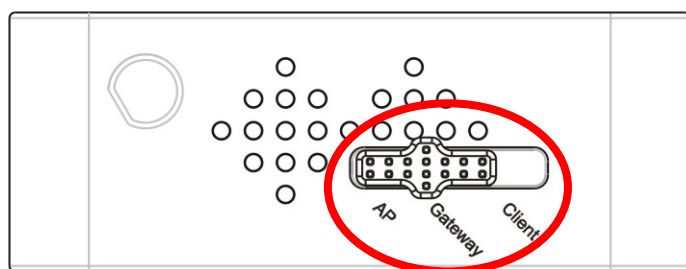
Chapter 2: About Operation Modes

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

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.

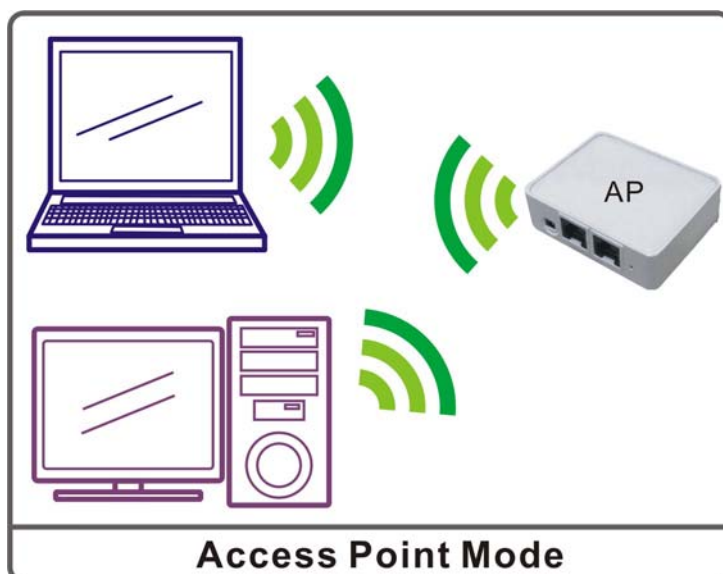
Operation Modes

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

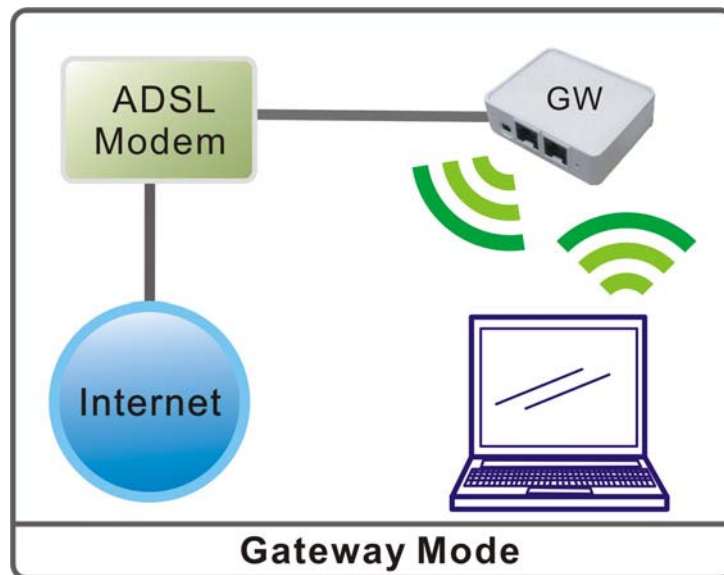
Let's take a look at the status of system.

System Info

Item	Status
Firmware Version	21.4.0.0.0.2e (Aug 19 2009)
System Up Time	0day:0h:26m:12s
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

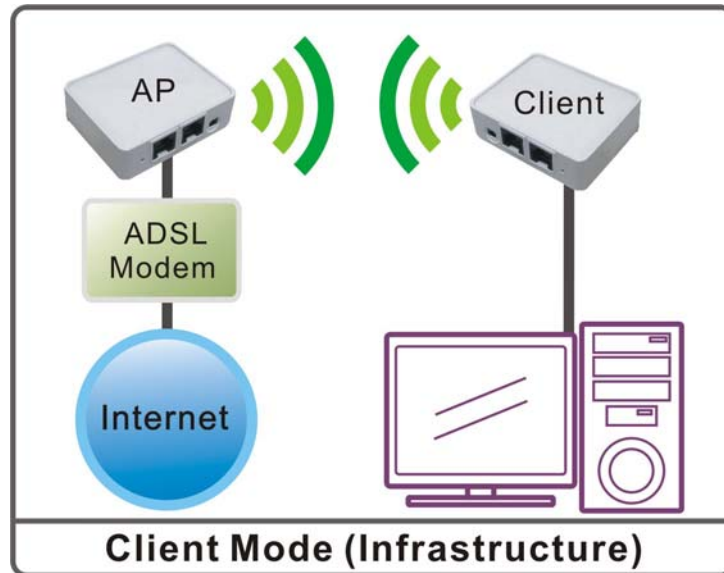
Let's take a look at the status of system.

System Info

Item	Status
Firmware Version	21.4.0.0.0.2e (Aug 19 2009)
System Up Time	0day:0h:28m:5s
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.

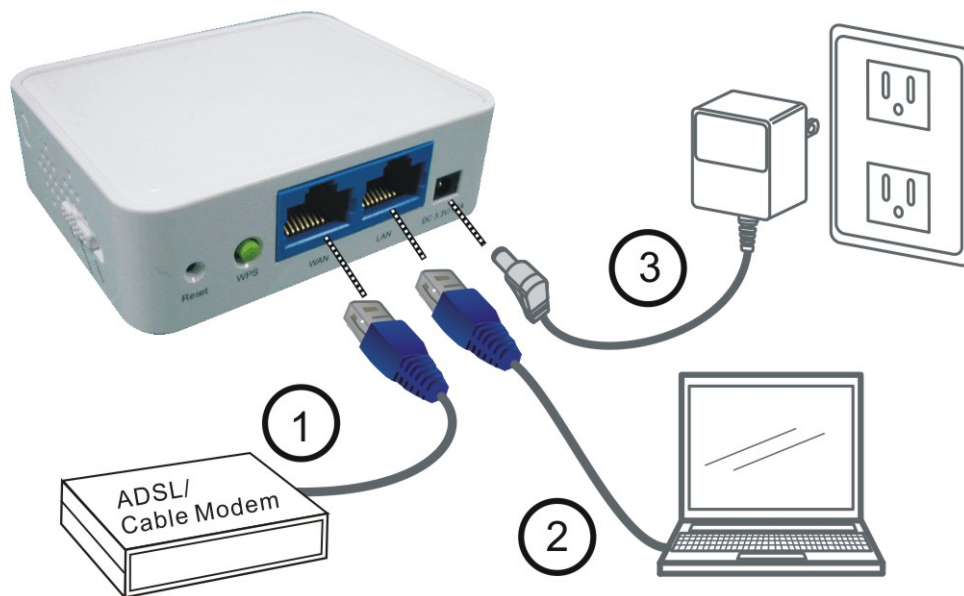
System Info

Item	Status
Firmware Version	21.4.0.0.0.2e (Aug 19 2009)
System Up Time	0day:0h:0m:31s
Operation Mode	Client Mode

Chapter 3: Configuration

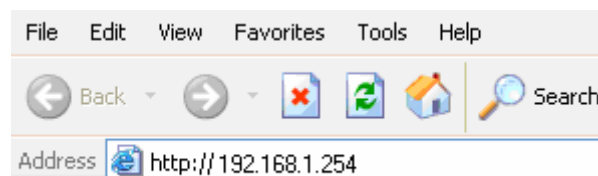
Hardware Connection

1. Connect one end of the Ethernet cable to the WAN port of the Wireless Portable Router, another end to the ADSL or cable modem.
2. Then, connect another Ethernet cable one end to the LAN port of the Wireless Portable Router, the other end to your PC or notebook.
3. Finally, 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://192.168.1.254>



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

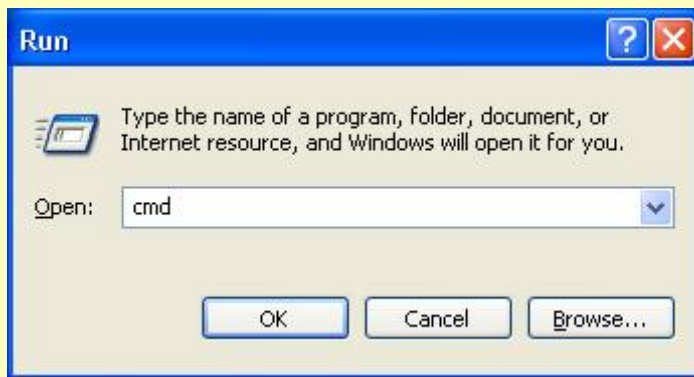


The image shows a login dialog box. At the top left, there is a blue header with a yellow key icon. Below the header, the main area is light beige. It contains a 'User name:' label followed by a dropdown menu showing 'admin'. Below that is a 'Password:' label followed by a text box containing six black dots. Underneath the password field is a checkbox labeled 'Remember my password'. At the bottom right, there are two buttons: 'OK' and 'Cancel'.

If you cannot connect...

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

- The Wireless Portable 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.



- Enter the command: **ping 192.168.1.254**

```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\al1787>ping 192.168.1.254

Pinging 192.168.1.254 with 32 bytes of data:

Reply from 192.168.1.254: bytes=32 time=1ms TTL=64
Reply from 192.168.1.254: bytes=32 time<1ms TTL=64
Reply from 192.168.1.254: bytes=32 time<1ms TTL=64
Reply from 192.168.1.254: bytes=32 time=1ms TTL=64

Ping statistics for 192.168.1.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

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 192.168.1.1. to 192.168.1.253 to be compatible with the Wireless Portable Router's default IP Address of 192.168.1.254. 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).	<ul style="list-style-type: none"> ● PPTP Server IP Address. ● User name and password. ● IP Address allocated to you, if Static (Fixed).
L2TP	Mainly used in Europe. You connect to the ISP only when required. The IP address is usually allocated automatically, but may be Static (Fixed).	<ul style="list-style-type: none"> ● L2TP 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.

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:

WAN Access Type	DHCP Client
	WAN Access Type: <input type="text" value="DHCP Client"/>
	<input type="button" value="Cancel"/> <input type="button" value=" << Back"/> <input type="button" value=" Next >>"/>
	If the DHCP Client WAN connection be selected, the PC will obtain the IP address automatically.
	Static IP
	WAN Access Type: <input type="text" value="Static IP"/>
	IP Address: <input type="text" value="172.10.1.1"/>
	Subnet Mask: <input type="text" value="255.255.255.0"/>
	Default Gateway: <input type="text" value="172.10.1.254"/>
	<input type="button" value="Next >>"/>
	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: <input type="text" value="PPPoE"/>
	User Name: <input type="text" value="pppoe_user"/>
	Password: <input type="password" value="....."/>
	<input type="button" value="Cancel"/> <input type="button" value=" << Back"/> <input type="button" value=" Next >>"/>

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

Next >>

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

Next >>

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).

	<p>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.</p> <p>IP Address: Enter the WAN IP address provided by your ISP here.</p> <p>Subnet Mask: Enter the subnet mask here.</p> <p>Default Gateway: Enter the default gateway IP address provided by your ISP here.</p>
--	---

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.

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	<input type="text" value="192.168.1.254"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>
DHCP Type	Server <input type="button" value="v"/>
DHCP Start IP	<input type="text" value="192.168.1.100"/>
DHCP End IP	<input type="text" value="192.168.1.200"/>
DHCP Primary DNS	<input type="text" value="192.168.1.254"/>
DHCP Secondary DNS	<input type="text" value="0.0.0.0"/>
DHCP Lease Time	<input type="text" value="86400"/>

IP Address	Shows the IP address of the Wireless Portable Router (Default IP address is 192.168.1.254.)
Subnet Mask	The subnet mask of the Wireless Portable Router (Default subnet mask is 255.255.255.0.)
DHCP Type	<p>Disable: Select to disable this Wireless Portable Router to distribute IP addresses to connected clients.</p> <p>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.</p>
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 192.168.1.100 should work for most cases.
DHCP End IP	The end IP address, the maximum is 253. Default value 253 should work for most cases (192.168.1.253.) If “ Start IP Address ” is set at 192.168.1.100 and the “ End IP address ” is 192.168.1.253, the device will distribute IP addresses from 192.168.1.100 to 192.168.1.253 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). 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 which may connect to your Access Point.

Network Mode	11b/g/n mixed mode ▾
Network Name(SSID)	GENERIC
Frequency (Channel)	2462MHz (Channel 11) ▾

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 1~11 or Auto Select from the pull-down menu.

Step 4- Security

Here can set up the wireless security of the Wireless Portable 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
---------------	---------

Cancel << Back Finished

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

Security Mode	OPEN
Default Key	Key 1
WEP Key 1 :	<input type="text"/> Hex
WEP Key 2 :	<input type="text"/> Hex
WEP Key 3 :	<input type="text"/> Hex
WEP Key 4 :	<input type="text"/> Hex

Cancel << Back Finished

Security Mode

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

Security Mode	WPA2-PSK
WPA Algorithms	<input type="radio"/> TKIP <input checked="" type="radio"/> AES <input type="radio"/> TKIP/AES
Pass Phrase	12345678

Cancel << Back Finished

WPA Algorithms: Select the type of algorithm, TKIP or AES for WPA-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.

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 ▼

Apply Cancel

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 ▼

Apply

Cancel

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 Mode	
User Name	<input type="text" value="pppoe_user"/>
Password	<input type="password" value="....."/>
Verify Password	<input type="password" value="....."/>

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 Mode	
Server IP	<input type="text" value="0.0.0.0"/>
User Name	<input type="text" value="l2tp_user"/>
Password	<input type="password" value="....."/>
Address Mode	<input type="text" value="Static"/>
IP Address	<input type="text" value="172.10.1.1"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>
Internet Default Gateway	<input type="text" value="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

	<p style="text-align: right;">WAN Connection Type: PPTP <input type="button" value="v"/></p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr style="background-color: #0056b3; color: white;"> <th colspan="2">PPTP Mode</th> </tr> </thead> <tbody> <tr> <td>Server IP</td> <td><input type="text" value="0.0.0.0"/></td> </tr> <tr> <td>User Name</td> <td><input type="text" value="pptp_user"/></td> </tr> <tr> <td>Password</td> <td><input type="password" value="••••••••"/></td> </tr> <tr> <td>Address Mode</td> <td>Static <input type="button" value="v"/></td> </tr> <tr> <td>IP Address</td> <td><input type="text" value="172.10.1.254"/></td> </tr> <tr> <td>Subnet Mask</td> <td><input type="text" value="255.255.255.0"/></td> </tr> <tr> <td>Internet Default Gateway</td> <td><input type="text" value="172.10.1.254"/></td> </tr> </tbody> </table> <p>Server IP: Enter the L2TP Server IP Address in this column.</p> <p>User Name: Maximum input is 32 alphanumeric characters (case sensitive).</p> <p>Password: Maximum input is 32 alphanumeric characters (case sensitive).</p> <p>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.</p> <p>IP Address: Enter the WAN IP address provided by your ISP in this column.</p> <p>Subnet Mask: Enter the subnet mask in this column.</p> <p>Internet Default Gateway: Enter the default gateway IP address provided by your ISP in this column.</p>	PPTP Mode		Server IP	<input type="text" value="0.0.0.0"/>	User Name	<input type="text" value="pptp_user"/>	Password	<input type="password" value="••••••••"/>	Address Mode	Static <input type="button" value="v"/>	IP Address	<input type="text" value="172.10.1.254"/>	Subnet Mask	<input type="text" value="255.255.255.0"/>	Internet Default Gateway	<input type="text" value="172.10.1.254"/>
PPTP Mode																	
Server IP	<input type="text" value="0.0.0.0"/>																
User Name	<input type="text" value="pptp_user"/>																
Password	<input type="password" value="••••••••"/>																
Address Mode	Static <input type="button" value="v"/>																
IP Address	<input type="text" value="172.10.1.254"/>																
Subnet Mask	<input type="text" value="255.255.255.0"/>																
Internet Default Gateway	<input type="text" value="172.10.1.254"/>																
<p>MAC Clone</p>	<p>Your ISP may require a particular MAC address in order for you to connect to the Internet. This MAC address is the PC's MAC address that your ISP had originally connected your Internet connection to. Type in or click Fill my MAC to replace the WAN MAC address with the MAC address of that PC.</p> <p>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.</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr style="background-color: #0056b3; color: white;"> <th colspan="2">MAC Clone</th> </tr> </thead> <tbody> <tr> <td>Enabled</td> <td>Enable <input type="button" value="v"/></td> </tr> <tr> <td>MAC Address</td> <td><input type="text" value="00:0C:6E:B3:AE:21"/> <input type="button" value="Fill my MAC"/></td> </tr> <tr> <td colspan="2" style="text-align: center;"> <input type="button" value="Apply"/> <input type="button" value="Cancel"/> </td> </tr> </tbody> </table>	MAC Clone		Enabled	Enable <input type="button" value="v"/>	MAC Address	<input type="text" value="00:0C:6E:B3:AE:21"/> <input type="button" value="Fill my MAC"/>	<input type="button" value="Apply"/> <input type="button" value="Cancel"/>									
MAC Clone																	
Enabled	Enable <input type="button" value="v"/>																
MAC Address	<input type="text" value="00:0C:6E:B3:AE:21"/> <input type="button" value="Fill my MAC"/>																
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>																	
<p>Apply</p>	<p>After completing the settings on this page, click Apply button to save the settings.</p>																
<p>Cancel</p>	<p>Click Cancel to restore to default values.</p>																

LAN

Local Area Network (LAN) Settings

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

LAN Setup	
IP Address	<input type="text" value="192.168.1.254"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>
Internet Default Gateway	<input type="text"/>
Internet Primary DNS	<input type="text"/>
Internet Secondary DNS	<input type="text"/>
MAC Address	00:12:0E:AF:13:EA
DHCP Type	Server <input type="button" value="v"/>
DHCP Start IP Address	<input type="text" value="192.168.1.100"/>
DHCP End IP Address	<input type="text" value="192.168.1.200"/>
DHCP Primary DNS	<input type="text" value="192.168.1.254"/>
DHCP Secondary DNS	<input type="text" value="0.0.0.0"/>
DHCP Lease Time	<input type="text" value="86400"/>
Statically Assigned	MAC: <input type="text" value="00:00:00:00:00:00"/> IP: <input type="text" value="0.0.0.0"/>
Statically Assigned	MAC: <input type="text" value="00:00:00:00:00:00"/> IP: <input type="text" value="0.0.0.0"/>
Statically Assigned	MAC: <input type="text" value="00:00:00:00:00:00"/> IP: <input type="text" value="0.0.0.0"/>
802.1d Spanning Tree	Disable <input type="button" value="v"/>
LLTD	Disable <input type="button" value="v"/>
IGMP Proxy	Disable <input type="button" value="v"/>
UPNP	Disable <input type="button" value="v"/>
PPPoE Relay	Disable <input type="button" value="v"/>
DNS Proxy	Disable <input type="button" value="v"/>

This part is only available in AP and Client mode.

IP Address	Shows the IP address of the Wireless Portable Router (Default IP address is 192.168.1.254.)
Subnet Mask	The subnet mask of the Wireless Portable Router (Default subnet mask is 255.255.255.0.)
Internet Default Gateway	<u>This section is only available in AP and Client Mode.</u> 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> 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> The Secondary DNS is used for resolve the URL address to physical IP address.
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.
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 192.168.1.100 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 (192.168.1.253.) If “ Start IP Address ” is set at 192.168.1.100 and the “ End IP address ” is 192.168.1.253, the device will distribute IP addresses from 192.168.1.100 to 192.168.1.253 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. 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.

VPN Passthrough (GW)

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

VPN Passthrough

VPN passthrough 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. 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.

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	<input type="text"/>
Range	Host <input type="button" value="v"/>
Gateway	<input type="text"/>
Interface	LAN <input type="button" value="v"/>
Comment	<input type="text"/>

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 <input type="button" value="v"/>
-----	--

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-down 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	<input type="button" value="RADIO OFF"/>
Network Mode	11b/g/n mixed mode ▾
Network Name(SSID)	GENERIC
Multiple SSID1	
Multiple SSID2	
Multiple SSID3	
Broadcast Network Name (SSID)	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
AP Isolation	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
MBSSID AP Isolation	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
BSSID	00:12:0E:AF:13:E8
Frequency (Channel)	2462MHz (Channel 11) ▾
HT Physical Mode	
Operating Mode	<input checked="" type="radio"/> Mixed Mode <input type="radio"/> Green Field
Channel BandWidth	<input type="radio"/> 20 <input checked="" type="radio"/> 20/40
Guard Interval	<input type="radio"/> Long <input checked="" type="radio"/> Auto
MCS	Auto
Reverse Direction Grant(RDG)	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Extension Channel	2442MHz (Channel 7) ▾
Aggregation MSDU(A-MSDU)	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
Auto Block ACK	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Decline BA Request	<input checked="" type="radio"/> Disable <input type="radio"/> 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. 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. 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. 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 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	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 <input type="button" value="v"/>
Beacon Interval	<input type="text" value="100"/> ms (range 20 - 999, default 100)
Data Beacon Rate (DTIM)	<input type="text" value="1"/> ms (range 1 - 255, default 1)
Fragment Threshold	<input type="text" value="2346"/> (range 256 - 2346, default 2346)
RTS Threshold	<input type="text" value="2347"/> (range 1 - 2347, default 2347)
TX Power	<input type="text" value="100"/> (range 1 - 100, default 100)
Short Preamble	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Short Slot	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Tx Burst	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Pkt_Aggregate	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Wi-Fi Multimedia	
WMM Capable	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
APSD Capable	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
DLS Capable	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
WMM Parameters	<input type="button" value="WMM Configuration"/>
Multicast-to-Unicast Converter	
Multicast-to-Unicast	<input type="radio"/> Enable <input checked="" type="radio"/> 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 Portable 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	<p>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.)</p> <p>Warning: Enabling RTS Threshold will cause redundant network overhead that could negatively affect the throughput performance instead of providing a remedy.</p> <p>This value should remain at its default setting of 2347. Should you encounter inconsistent data flow, only minor modifications of this value are recommended.</p>
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 Portable 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.)
Wi-Fi Multimedia	
WMM Capable	<p>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.</p> <p>Select Disable or Enable to use or stop Wi-Fi Multimedia function. (Default setting is Enable.)</p>
APSD Capable	<p>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.</p> <p>Select Disable or Enable this function. (Default setting is Disable.)</p>

DLS Capable	<p>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.</p> <p>Select Disable or Enable this function. (Default setting is Disable.)</p>																																																																	
WMM Parameters	<p>Click the WMM Configuration button to go further settings.</p> <div style="border: 1px solid #ccc; padding: 5px;"> <p style="text-align: center; margin: 0;">WMM Parameters of Access Point</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 10%;"></th> <th style="width: 15%;">Aifsn</th> <th style="width: 15%;">CWMin</th> <th style="width: 15%;">CWMax</th> <th style="width: 15%;">Txop</th> <th style="width: 10%;">ACM</th> <th style="width: 10%;">AckPolicy</th> </tr> </thead> <tbody> <tr> <td>AC_BE</td> <td><input type="text" value="3"/></td> <td><input type="text" value="15"/></td> <td><input type="text" value="63"/></td> <td><input type="text" value="0"/></td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td>AC_BK</td> <td><input type="text" value="7"/></td> <td><input type="text" value="15"/></td> <td><input type="text" value="1023"/></td> <td><input type="text" value="0"/></td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td>AC_VI</td> <td><input type="text" value="1"/></td> <td><input type="text" value="7"/></td> <td><input type="text" value="15"/></td> <td><input type="text" value="94"/></td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td>AC_VO</td> <td><input type="text" value="1"/></td> <td><input type="text" value="3"/></td> <td><input type="text" value="7"/></td> <td><input type="text" value="47"/></td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> </tbody> </table> <p style="text-align: center; margin: 0;">WMM Parameters of Station</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 10%;"></th> <th style="width: 15%;">Aifsn</th> <th style="width: 15%;">CWMin</th> <th style="width: 15%;">CWMax</th> <th style="width: 15%;">Txop</th> <th style="width: 10%;">ACM</th> </tr> </thead> <tbody> <tr> <td>AC_BE</td> <td><input type="text" value="3"/></td> <td><input type="text" value="15"/></td> <td><input type="text" value="1023"/></td> <td><input type="text" value="0"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td>AC_BK</td> <td><input type="text" value="7"/></td> <td><input type="text" value="15"/></td> <td><input type="text" value="1023"/></td> <td><input type="text" value="0"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td>AC_VI</td> <td><input type="text" value="2"/></td> <td><input type="text" value="7"/></td> <td><input type="text" value="15"/></td> <td><input type="text" value="94"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td>AC_VO</td> <td><input type="text" value="2"/></td> <td><input type="text" value="3"/></td> <td><input type="text" value="7"/></td> <td><input type="text" value="47"/></td> <td><input type="checkbox"/></td> </tr> </tbody> </table> <p style="text-align: center; margin: 5px 0;"> <input type="button" value="Apply"/> <input type="button" value="Cancel"/> <input type="button" value="Close"/> </p> </div>		Aifsn	CWMin	CWMax	Txop	ACM	AckPolicy	AC_BE	<input type="text" value="3"/>	<input type="text" value="15"/>	<input type="text" value="63"/>	<input type="text" value="0"/>	<input type="checkbox"/>	<input type="checkbox"/>	AC_BK	<input type="text" value="7"/>	<input type="text" value="15"/>	<input type="text" value="1023"/>	<input type="text" value="0"/>	<input type="checkbox"/>	<input type="checkbox"/>	AC_VI	<input type="text" value="1"/>	<input type="text" value="7"/>	<input type="text" value="15"/>	<input type="text" value="94"/>	<input type="checkbox"/>	<input type="checkbox"/>	AC_VO	<input type="text" value="1"/>	<input type="text" value="3"/>	<input type="text" value="7"/>	<input type="text" value="47"/>	<input type="checkbox"/>	<input type="checkbox"/>		Aifsn	CWMin	CWMax	Txop	ACM	AC_BE	<input type="text" value="3"/>	<input type="text" value="15"/>	<input type="text" value="1023"/>	<input type="text" value="0"/>	<input type="checkbox"/>	AC_BK	<input type="text" value="7"/>	<input type="text" value="15"/>	<input type="text" value="1023"/>	<input type="text" value="0"/>	<input type="checkbox"/>	AC_VI	<input type="text" value="2"/>	<input type="text" value="7"/>	<input type="text" value="15"/>	<input type="text" value="94"/>	<input type="checkbox"/>	AC_VO	<input type="text" value="2"/>	<input type="text" value="3"/>	<input type="text" value="7"/>	<input type="text" value="47"/>	<input type="checkbox"/>
	Aifsn	CWMin	CWMax	Txop	ACM	AckPolicy																																																												
AC_BE	<input type="text" value="3"/>	<input type="text" value="15"/>	<input type="text" value="63"/>	<input type="text" value="0"/>	<input type="checkbox"/>	<input type="checkbox"/>																																																												
AC_BK	<input type="text" value="7"/>	<input type="text" value="15"/>	<input type="text" value="1023"/>	<input type="text" value="0"/>	<input type="checkbox"/>	<input type="checkbox"/>																																																												
AC_VI	<input type="text" value="1"/>	<input type="text" value="7"/>	<input type="text" value="15"/>	<input type="text" value="94"/>	<input type="checkbox"/>	<input type="checkbox"/>																																																												
AC_VO	<input type="text" value="1"/>	<input type="text" value="3"/>	<input type="text" value="7"/>	<input type="text" value="47"/>	<input type="checkbox"/>	<input type="checkbox"/>																																																												
	Aifsn	CWMin	CWMax	Txop	ACM																																																													
AC_BE	<input type="text" value="3"/>	<input type="text" value="15"/>	<input type="text" value="1023"/>	<input type="text" value="0"/>	<input type="checkbox"/>																																																													
AC_BK	<input type="text" value="7"/>	<input type="text" value="15"/>	<input type="text" value="1023"/>	<input type="text" value="0"/>	<input type="checkbox"/>																																																													
AC_VI	<input type="text" value="2"/>	<input type="text" value="7"/>	<input type="text" value="15"/>	<input type="text" value="94"/>	<input type="checkbox"/>																																																													
AC_VO	<input type="text" value="2"/>	<input type="text" value="3"/>	<input type="text" value="7"/>	<input type="text" value="47"/>	<input type="checkbox"/>																																																													
Multicast-to-Unicast Converter																																																																		
Multicast-to-Unicast	<p>Select Disable or Enable this function. (Default setting is Disable.)</p>																																																																	

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:	<input type="text"/>

(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	<p>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.</p> <p>The client or station must use the same encryption and enter the same password when make a connection with the Wireless Portable Router.</p> <p>Note:</p> <ul style="list-style-type: none">➤ 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 Portable Router can accept clients connect by using OPEN-WEP or SHARED-WEP. <p>OPEN/ WEP AUTO</p> <p>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.</p>

Security Mode	OPEN	
Wire Equivalence Protection (WEP)		
Default Key	Key 1	
WEP Key 1 :	<input type="text"/>	Hex
WEP Key 2 :	<input type="text"/>	Hex
WEP Key 3 :	<input type="text"/>	Hex
WEP Key 4 :	<input type="text"/>	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 :	<input type="text"/>	Hex
WEP Key 2 :	<input type="text"/>	Hex
WEP Key 3 :	<input type="text"/>	Hex
WEP Key 4 :	<input type="text"/>	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/ WPA1-WPA2

"GENERIC"	
Security Mode	WPA2

WPA	
WPA Algorithms	<input type="radio"/> TKIP <input type="radio"/> AES <input type="radio"/> TKIPAES
Key Renewal Interval	3600 seconds
PMK Cache Period	10 minute
Pre-Authentication	<input checked="" type="radio"/> Disable <input type="radio"/> 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, WPA1-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 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.

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

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

WPA	
WPA Algorithms	<input type="radio"/> TKIP <input type="radio"/> AES <input type="radio"/> 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	<input type="radio"/> Disable <input type="radio"/> Enable
Radius Server	
IP Address	<input type="text"/>
Port	1812
Shared Secret	<input type="text"/>
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 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.

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 (WDS)

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(BSSID)** of each other to make the WDS connection.

Step 1: Setup the same **SSID** and **Channel** on wireless APs.

WDS Mode

Wireless Network	
Radio On/Off	RADIO OFF
Network Mode	11b/g/n mixed mode
Network Name(SSID)	GENERIC
Multiple SSID1	
Multiple SSID2	
Multiple SSID3	
Multiple SSID4	
Multiple SSID5	
Multiple SSID6	
Multiple SSID7	
Broadcast Network Name (SSID)	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
AP Isolation	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
MBSSID AP Isolation	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
BSSID	00:12:0E:AF:13:E8
Frequency (Channel)	2462MHz (Channel 11)

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)	GENERIC
Multiple SSID1	
Multiple SSID2	
Multiple SSID3	
Multiple SSID4	
Multiple SSID5	
Multiple SSID6	
Multiple SSID7	
Broadcast Network Name (SSID)	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
AP Isolation	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
MBSSID AP Isolation	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
BSSID	00:12:0E:AF:13:E8
Frequency (Channel)	2462MHz (Channel 11)

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 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.

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	

Apply Cancel

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.

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	<input type="text"/>
AP2 EncrypType	NONE
Encryp Key	<input type="text"/>
AP3 EncrypType	NONE
Encryp Key	<input type="text"/>
AP4 EncrypType	NONE
Encryp Key	<input type="text"/>
AP1 MAC Address	<input type="text"/>
AP2 MAC Address	<input type="text"/>
AP3 MAC Address	<input type="text"/>
AP4 MAC Address	<input type="text"/>

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.

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:

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

WPS Progress

WPS mode PIN PBC

PIN

WPS Status

WPS: Idle

WPS Config

WPS

To use WPS (Wi-Fi Protected Setup) function, push physical WPS button on Wireless Portable Router to make a WPS connection. Default setting is **Enable**.

WPS Summary

WPS Current Status

After enabling the WPS function, if there is connection the status will show Configured, otherwise, the status will show Idle.

WPS Configured	<p>Trigger WPS AP to do simple config with WPS Client. If WPS configured, here shows Yes, otherwise, NO.</p> <table border="1" data-bbox="496 264 1305 676"> <thead> <tr> <th colspan="2">WPS Summary</th> </tr> </thead> <tbody> <tr> <td>WPS Current Status:</td> <td>Configured</td> </tr> <tr> <td>WPS Configured:</td> <td>Yes</td> </tr> <tr> <td>WPS SSID:</td> <td>GENERIC</td> </tr> <tr> <td>WPS Auth Mode:</td> <td>WPA-PSKWPA2-PSK</td> </tr> <tr> <td>WPS Encryp Type:</td> <td>TKIPAES</td> </tr> <tr> <td>WPS Default Key Index:</td> <td>2</td> </tr> <tr> <td>WPS Key(ASCII)</td> <td>3cd338d1a1350a49cd48f5c1d1638d58 cb4ac082938cfcf900ce79f4c8978bbb</td> </tr> <tr> <td>AP PIN:</td> <td>31663441</td> </tr> </tbody> </table> <p><input type="button" value="Reset OOB"/></p>	WPS Summary		WPS Current Status:	Configured	WPS Configured:	Yes	WPS SSID:	GENERIC	WPS Auth Mode:	WPA-PSKWPA2-PSK	WPS Encryp Type:	TKIPAES	WPS Default Key Index:	2	WPS Key(ASCII)	3cd338d1a1350a49cd48f5c1d1638d58 cb4ac082938cfcf900ce79f4c8978bbb	AP PIN:	31663441
WPS Summary																			
WPS Current Status:	Configured																		
WPS Configured:	Yes																		
WPS SSID:	GENERIC																		
WPS Auth Mode:	WPA-PSKWPA2-PSK																		
WPS Encryp Type:	TKIPAES																		
WPS Default Key Index:	2																		
WPS Key(ASCII)	3cd338d1a1350a49cd48f5c1d1638d58 cb4ac082938cfcf900ce79f4c8978bbb																		
AP PIN:	31663441																		
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 stop the (OOB, out-of-box) configuration.																		
WPS Process																			
WPS mode	<p>PIN: Personal Identification Number. Select PIN then click Apply to make a WPS connection.</p> <p>PBC: Push Button Communication. Select PBC then click Apply to make a WPS connection.</p>																		
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.																		

Client Mode

Profile

Station Profile

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

Profile List

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

Add Delete Edit
Activate

Add

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

System Configuration	
Profile Name	PROF001
SSID	
Network Type	Infrastructure
Power Saving Mode	<input checked="" type="radio"/> CAM (Constantly Awake Mode) <input type="radio"/> Power Saving Mode
RTS Threshold	<input type="checkbox"/> Used 2347
Fragment Threshold	<input type="checkbox"/> 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 Keys	WEP Key 1:	
	WEP Key 2:	
	WEP Key 3:	
	WEP Key 4:	
Default Key	Key 1	

Apply Cancel

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 Keys	WEP Key 1 :	<input type="text"/>
	WEP Key 2 :	<input type="text"/>
	WEP Key 3 :	<input type="text"/>
	WEP Key 4 :	<input type="text"/>
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	<input checked="" type="radio"/> TKIP <input type="radio"/> AES
Pass Phrase	<input type="text"/>

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%	<input type="checkbox"/> 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
<input checked="" type="radio"/>	Cherry Wireless	00-E0-98-94-30-62	20%	6	Not Use	OPEN	Infrastructure
<input type="radio"/>	Untitled	00-E0-98-AC-85-E6	50%	10	Not Use	OPEN	Infrastructure
<input type="radio"/>	GENERIC	00-0C-43-30-52-88	70%	11	Not Use	OPEN	Infrastructure
<input type="radio"/>	Cherry TEST	00-E0-98-94-02-11	100%	11	Not Use	OPEN	Infrastructure
<input type="radio"/>	3089AP	00-90-CC-BE-6C-83	20%	11	Not Use	OPEN	Infrastructure
<input type="radio"/>	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 Successfully 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

Reset Counters

Refresh

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 CH1-11
B/G Protection	Auto ▾
<input checked="" type="checkbox"/> Tx Burst	

HT Physical Mode	
HT	<input checked="" type="radio"/> MM <input type="radio"/> GF
BW	<input type="radio"/> 20 <input checked="" type="radio"/> Auto
GI	<input type="radio"/> Long <input checked="" type="radio"/> 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 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
<input checked="" type="radio"/>	Cherry@3312	000C43418844	86%	6	WPA-PSK; WPA2-PSK	TKIP; AES	1.0	Conf.
<input type="radio"/>	3059_Z	00E098222200	39%	1	OPEN	Not Use	1.0	Conf.
<input type="radio"/>	3090_ZyXEL	000C43585858	29%	1	WPA2-PSK	AES	1.0	Conf.
<input type="radio"/>	NBG-419N	0019CB165300	50%	6	WPA2-PSK	AES	1.0	Conf.
<input type="radio"/>	PROLiNK_PWH2004	000C433052B0	0%	6	OPEN	Not Use	1.0	Unconf.
<input type="radio"/>	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

Refresh Mode: Enrollee PIN: 14738968

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. 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 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 ▾

Apply

MAC filter

Mac address

(The maximum count of MAC filter rule is 16)

Add

Reset

Current MAC filter rules in system

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

Delete Selected

Delete All

Reset

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 ▾

Apply

Add a URL filter:

URL

(The maximum count of URL filter rule is 16)

Add

Reset

Current Webs URL Filters

URL	Number
-----	--------

Delete Selected

Delete All

Reset

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	<input type="text"/>
Port Range	<input type="text"/> - <input type="text"/>
Protocol	TCP&UDP ▾
Comment	<input type="text"/>

(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	<input type="text"/>

Apply

Reset

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 ▾

Remote port

8080

Ping form WAN Filter

Ping form WAN Filter

Enable ▾

Stateful Packet Inspection (SPI)

SPI Firewall

Disable ▾

Apply

Reset

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.

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.

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

Apply

Reset

Webs Host Filter Settings

Current Website Host Filters:

Host(Keyword)

No

Delete

Reset

Add a Host(keyword) Filter:

Keyword

(The maximum rule count is 16)

Add

Reset

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.

Administrator Settings

Account	<input type="text" value="admin"/>
Password	<input type="password" value="•••••"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

NTP Settings

Current Time	<input type="text" value="Sat Jan 1 00:54:58 UTC 2000"/> <input type="button" value="Sync with host"/>
Time Zone:	<input type="text" value="(GMT-11:00) Midway Island, Samoa"/> <input type="button" value="v"/>
NTP Server	<input type="text" value="time.nist.gov"/> ex. time.nist.gov ntp0.broad.mit.edu time.stdtime.gov.tw
NTP synchronization(hours)	<input type="text" value="1"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

Green AP

Duration	Action
<input type="text" value="00"/> : <input type="text" value="00"/> : <input type="text" value="00"/> ~ <input type="text" value="00"/> : <input type="text" value="00"/>	<input type="text" value="Disable"/> <input type="button" value="v"/>
<input type="text" value="00"/> : <input type="text" value="00"/> : <input type="text" value="00"/> ~ <input type="text" value="00"/> : <input type="text" value="00"/>	<input type="text" value="Disable"/> <input type="button" value="v"/>
<input type="text" value="00"/> : <input type="text" value="00"/> : <input type="text" value="00"/> ~ <input type="text" value="00"/> : <input type="text" value="00"/>	<input type="text" value="Disable"/> <input type="button" value="v"/>
<input type="text" value="00"/> : <input type="text" value="00"/> : <input type="text" value="00"/> ~ <input type="text" value="00"/> : <input type="text" value="00"/>	<input type="text" value="Disable"/> <input type="button" value="v"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

DDNS Settings

Dynamic DNS Provider	<input type="text" value="None"/> <input type="button" value="v"/>
Account	<input type="text"/>
Password	<input type="text"/>
DDNS	<input type="text"/>
Result:	
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

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. 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

Upgrade Firmware

Upgrade the Ralink SoC firmware to obtain new functionality.

Update Firmware	
Location:	<input type="text"/> <input type="button" value="Browse..."/>
<input type="button" value="Apply"/>	

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 Portable 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

Export

Import Settings

Settings file location

Browse...

Import

Cancel

Load Factory Defaults

Load Default Button

Load Default

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 Portable 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.

System Log

Syslog:

Refresh

Clear

System Log

```
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 Portable Router.

System Reboot

The page will reboot system by user.

Reboot

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.

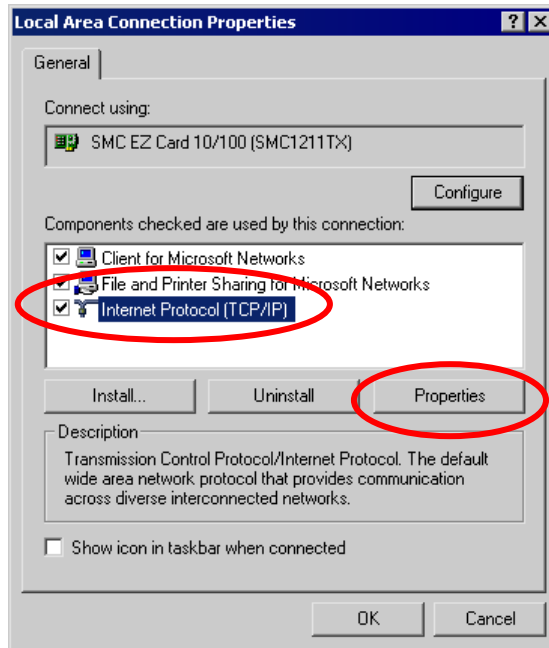
- By default, the Wireless Portable Router will act as a DHCP Server, automatically providing a suitable IP address (and related information) to each PC when the PC boots.
- For all non-Server versions of Windows, the default TCP/IP setting is to act as a DHCP client.

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

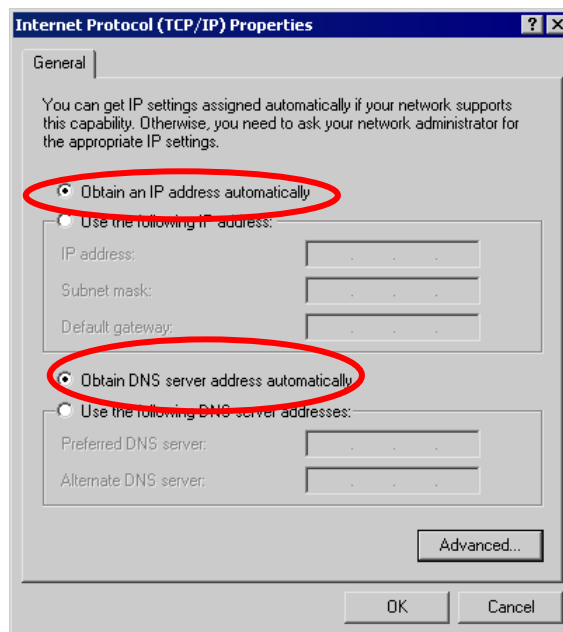
- The *Gateway* must be set to the IP address of the Wireless Portable Router.
- The *DNS* should be set to the address provided by your ISP.

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")

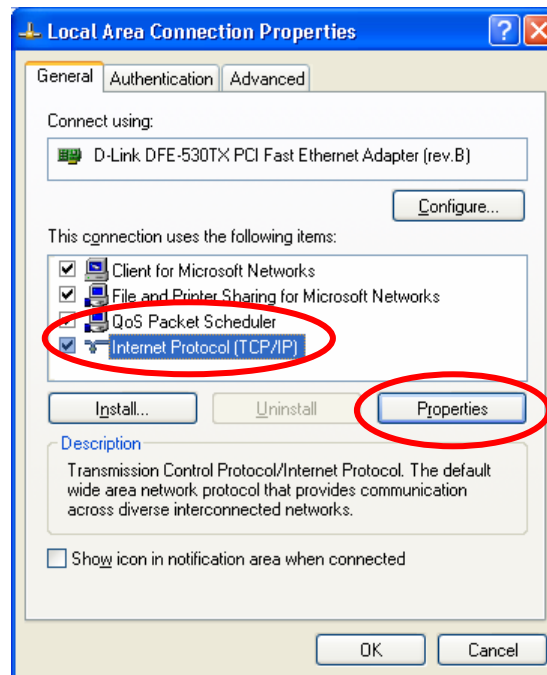
If your PC is already configured, check with your network administrator before making the following changes.

- 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.)

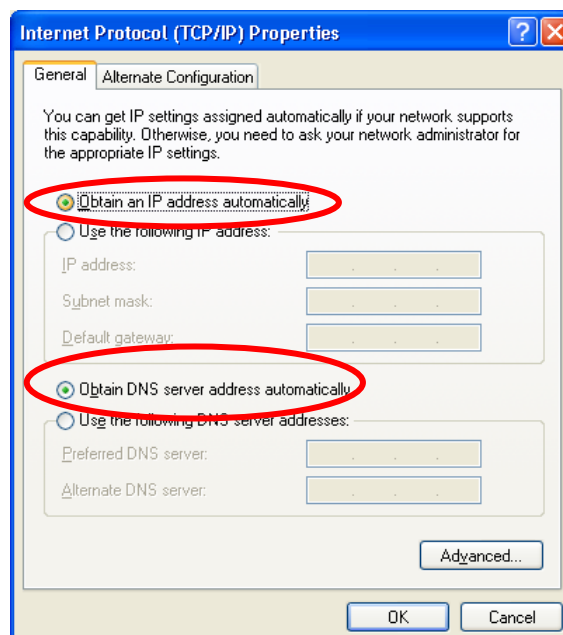
- If the *DNS Server* fields are empty, select *Use the following DNS server addresses*, and enter the DNS address or addresses provided by your ISP, then click *OK*.

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 enter 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 <i>Infrastructure</i> .
SSID (ESSID)	The network name must match the value used on the Wireless Portable Router. <i>Note! The SSID is case- sensitive.</i>
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. <ul style="list-style-type: none"> • 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:	<p>Check the following:</p> <ul style="list-style-type: none">• 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 192.168.1.1 to 192.168.1.253 and thus compatible with the Wireless Portable Router's default IP Address of 192.168.1.254. Also, the Network Mask should be set to 255.255.255.0 to match the Wireless Portable Router. <p>In Windows, you can check these settings by using <i>Control Panel-Network</i> to check the <i>Properties</i> for the TCP/IP protocol.</p>

Internet Access

Problem 1:	When I enter a URL or IP address I get a time out error.
Solution 1:	<p>A number of things could be causing this. Try the following troubleshooting steps.</p> <ul style="list-style-type: none">• 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

	<p>settings. (If you can't connect to it, check the LAN and power connections.)</p> <ul style="list-style-type: none"> ● 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:	<p>The Wireless Portable Router processes the data passing through it, so it is not transparent.</p> <p>Use the <i>Content Filter Settings</i> feature to allow the use of Internet applications, which do not function correctly.</p> <p>If this does solve the problem you can use the <i>DMZ</i> function. This should work with almost every application, but:</p> <ul style="list-style-type: none"> ● 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:	<p>Check the following:</p> <ul style="list-style-type: none"> ● Your PC is set to <i>Infrastructure Mode</i>. (Access Points are always in <i>Infrastructure Mode</i>) ● The SSID on your PC and the Wireless Portable Router are the same. Remember that the SSID is case-sensitive. So, for example "<u>W</u>orkgroup" does NOT match "<u>w</u>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:	<p>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:</p> <ul style="list-style-type: none"> ● <u>Wireless Portable Router location</u> Try adjusting the location and orientation of the Wireless Portable Router. ● <u>Wireless Channel</u> If interference is the problem, changing to another channel may show a marked improvement. ● <u>Radio Interference</u> Other devices may be causing interference. You can experiment by switching

	<p>other devices off, and see if this helps. Any "noisy" devices should be shielded or relocated.</p> <ul style="list-style-type: none"><li data-bbox="427 286 1345 427">● <u>RF Shielding</u> 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



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 channels 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 <i>Infrastructure</i> .
SSID (ESSID)	The network name must match the value used on the Wireless Portable Router. <i>Note! The SSID is case- sensitive.</i>
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. <ul style="list-style-type: none">• 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.

<p>WPA-PSK WPA2-PSK WPA-PSK/WPA2-PSK</p>	<p>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.</p>
<p>WPA WPA2 WPA WPA2 802.1x</p>	<p>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.</p>