

802.11g Wireless High-power Broadband Router

with passive PoE

User's Manual

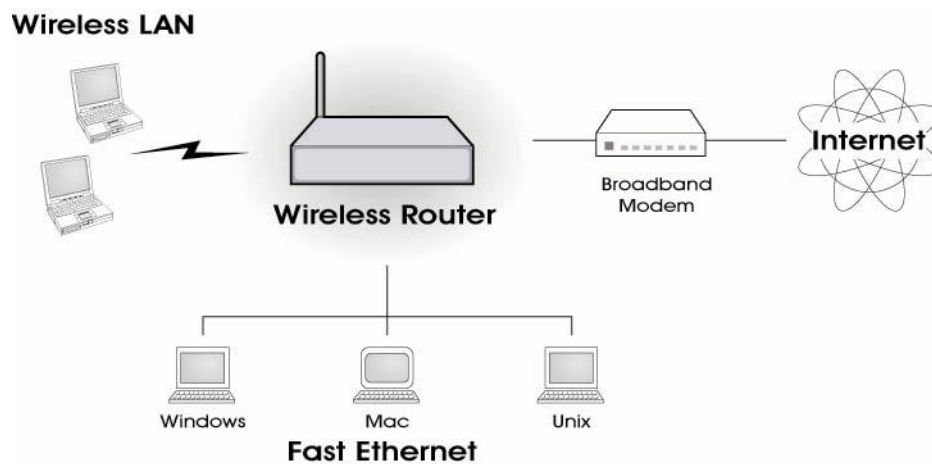
Table of Contents

CHAPTER 1: INTRODUCTION	2
WIRELESS ROUTER FEATURES	2
PACKAGE CONTENTS	4
PHYSICAL DETAILS	5
ABOUT THE OPERATION MODES	7
CHAPTER 2: INSTALLATION	9
REQUIREMENTS	9
PROCEDURE	9
CHAPTER 3: CONFIGURATION	11
OVERVIEW	11
CONFIGURATION PROGRAM	11
SETUP WIZARD	13
CONFIGURATION VIA WEB	16
CHAPTER 4: PC CONFIGURATION	42
OVERVIEW	42
WINDOWS CLIENTS	42
MACINTOSH CLIENTS	47
LINUX CLIENTS	47
OTHER UNIX SYSTEMS	47
WIRELESS STATION CONFIGURATION	48
APPENDIX A: TROUBLESHOOTING	49
OVERVIEW	49
GENERAL PROBLEMS	49
INTERNET ACCESS	50
WIRELESS ACCESS	51
APPENDIX B: ABOUT WIRELESS LANS	52
MODES	52
BSS	52
CHANNELS	52
SECURITY	53
WIRELESS LAN CONFIGURATION	54
APPENDIX C: SPECIFICATIONS	55
MULTI-FUNCTION WIRELESS ROUTER	55
WIRELESS INTERFACE	55
REGULATORY APPROVALS	56

Chapter I: Introduction

Congratulations on the purchase of your new Wireless Router. The Wireless Router is a multi-function device providing the following services:

- **Shared Broadband Internet Access** for all LAN users.
- **4-Port Switching Hub** for 10BaseT or 100BaseT connections.
- **Wireless Access Point** for 802.11b and 802.11g Wireless Stations.



Wireless Router Features

The Wireless Router incorporates many advanced features, carefully designed to provide sophisticated functions while being easy to use.

Internet Access Features

- **Shared Internet Access.** All users on the LAN or WLAN can access the Internet through the Wireless Router, using only a single external IP Address. The local (invalid) IP Addresses are hidden from external sources. This process is called NAT (Network Address Translation).
- **DSL & Cable Modem Support.** The Wireless Router has a 10/100BaseT Ethernet port for connecting a DSL or Cable Modem. All popular DSL and Cable Modems are supported. SingTel RAS and Big Pond (Australia) login support is also included.
- **PPPoE and PPTP.** The Internet (WAN port) connection supports PPPoE (PPP over Ethernet), PPTP (Peer-to-Peer Tunneling Protocol), as well as "Direct Connection" type services. Unnumbered IP with PPPoE is also supported.
- **Fixed or Dynamic IP Address.** On the Internet (WAN port) connection, the Wireless Router supports both Dynamic IP Address (IP Address is allocated on connection) and Fixed IP Address.

Advanced Internet Functions

- **Communication Applications.** Support for Internet communication applications, such as interactive games, telephony, and conferencing applications, which are often difficult to use when behind a Firewall, is included.
- **Special Internet Applications.** Applications which use non-standard connections or port numbers are normally blocked by the Firewall. The ability to define and allow such applications is provided, to enable such applications to be used normally.
- **Virtual Servers.** This feature allows Internet users to access Internet servers on your LAN. The required setup is quick and easy.
- **DDNS Support.** DDNS (Dynamic DNS) allows Internet users to connect to Virtual Servers on your LAN using a domain name, even if your IP address is not fixed.
- **DMZ.** For each WAN (Internet) IP address allocated to you, only one (1) PC on your local LAN can be configured to allow unrestricted 2-way communication with servers or individual users on the Internet. This provides the ability to run programs which are incompatible with Firewalls.
- **URL Filter.** Use the URL Filter to block access to undesirable Web sites by LAN users.
- **Internet Access Log.** See which Internet connections have been made.
- **Access Control.** Using the Access Control feature, you can assign LAN users to different groups, and determine which Internet services are available to each group.
- **VPN Pass through Support.** PCs with VPN (Virtual Private Networking) software using PPTP, L2TP and IPSec are transparently supported - no configuration is required.

Wireless Features

- **Standards Compliant.** The Wireless Router complies with the IEEE802.11g (DSSS) specifications for Wireless LANs.
- **Supports both 802.11b and 802.11g Wireless Stations.** The 802.11g standard provides for backward compatibility with the 802.11b standard, so both 802.11b and 802.11g wireless stations can be used simultaneously.
- **Speeds up to 54Mbps.** All speeds up to the 802.11g maximum of 54Mbps are supported.
- **WEP support.** Support for WEP (Wired Equivalent Privacy) is included. Key sizes of 64 Bit and 128 Bit are supported.
- **Wireless MAC Access Control.** The Wireless Access Control feature can check the MAC address (hardware address) of wireless stations to ensure that only trusted wireless stations can access your LAN.
- **Simple Configuration.** If the default settings are unsuitable, they can be changed quickly and easily.

LAN Features

- **4-Port Switching Hub.** The Wireless Router incorporates a 4-port 10/100BaseT switching hub, making it easy to create or extend your LAN.
- **DHCP Server Support.** Dynamic Host Configuration Protocol provides a dynamic IP address to PCs and other devices upon request. The Wireless Router can act as a **DHCP Server** for devices on your local LAN and WLAN.

Configuration and Management

- **Easy Setup.** Use your WEB browser from anywhere on the LAN or WLAN for configuration.
- **Configuration File Upload and Download.** Save (download) the configuration data from the Wireless Router to your PC and restore (upload) a previously-saved configuration file to the Wireless Router.
- **Remote Management.** The Wireless Router can be managed from any PC on your LAN. And, if the Internet connection exists, it can also (optionally) be configured via the Internet.
- **Network Diagnostics.** You can use the Wireless Router to perform a *Ping* or *DNS lookup*.
- **UPnP Support.** UPnP (Universal Plug and Play) allows automatic discovery and configuration of the Wireless Router. UPnP is by supported by Windows 2000, XP, or later.

Security Features

- **Password - Protected Configuration.** Optional password protection is provided to prevent unauthorized users from modifying the configuration data and settings.
- **Wireless LAN Security.** WEP (Wired Equivalent Privacy) is supported, as well as wireless access control to prevent unknown wireless stations from accessing your LAN.
- **NAT Protection.** An intrinsic side effect of NAT (Network Address Translation) technology is that by allowing all LAN users to share a single IP address, the location and even the existence of each PC is hidden. From the external viewpoint, there is no network, only a single device - the Wireless Router.
- **Protection against DoS attacks.** DoS (Denial of Service) attacks can flood your Internet connection with invalid packets and connection requests, using so much bandwidth and so many resources that Internet access becomes unavailable. The Wireless Router incorporates protection against DoS attacks.

Package Contents

The following items should be included:

- The Wireless Router Unit
- Power Adapter
- Quick Installation Guide
- CD-ROM containing the on-line manual.

If any of the above items are damaged or missing, please contact your dealer immediately.

Physical Details

Front-mounted LEDs

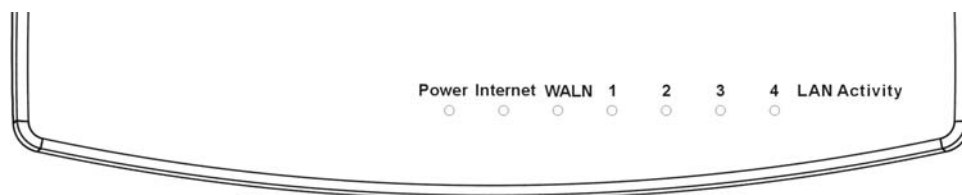


Figure 1: Front Panel

Power LED	<p>On - Power on.</p> <p>Off - No power.</p>
Internet LED	<p>On - Connection to the Broadband Modem attached to the WAN (Internet) port is established.</p> <p>Off - No connection to the Broadband Modem.</p> <p>Flashing - Data is being transmitted or received via the WAN port.</p>
WLAN LED	<p>On - Wireless connection available; Wireless Access Point is ready for using.</p> <p>Off - No Wireless connection available.</p> <p>Flashing - Data is being transmitted or received via the Wireless access point. Data includes "network traffic" as well as user data.</p>
LAN LED 1~4	<ul style="list-style-type: none">• LAN Activity<ul style="list-style-type: none">• On - Corresponding LAN (hub) port is active.• Off - No active connection on the corresponding LAN (hub) port.• Flashing - Data is being transmitted or received via the corresponding LAN (hub) port.

Rear Panel

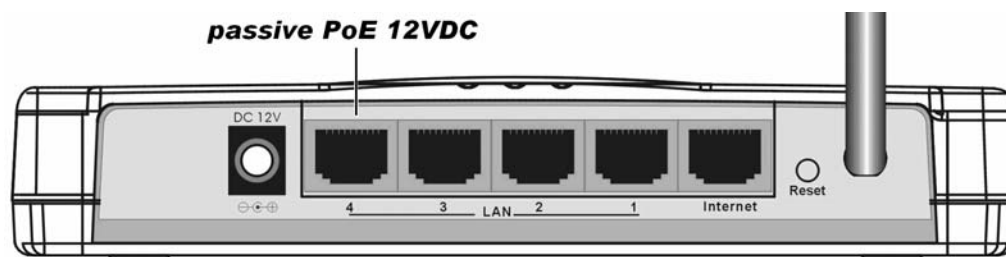


Figure 2: Rear Panel

Power port	Connect the supplied power adapter here.
10/100BaseT LAN port	<p>Use standard LAN cables (RJ45 connectors) to connect your PCs to these ports.</p> <p>If required, any port can be connected to another hub. Any LAN port will automatically function as an "Uplink" port when necessary.</p>
Internet port (10/100BaseT)	Connect the DSL or Cable Modem here. If your modem came with a cable, use the supplied cable. Otherwise, use a standard LAN cable.
Reset Button	<p>This button has two (2) functions:</p> <ul style="list-style-type: none"> • Reboot. When pressed within 3~5 seconds, the power LED lights amber then released, the Wireless Router will reboot (restart). • Clear All Data. This button can also be used to clear ALL data and restore ALL settings to the factory default values. <p>To Clear All Data and restore the factory default values:</p> <ol style="list-style-type: none"> 1. After Power On. 2. Press the Reset Button. 3. Keep pressing the Reset Button more than 5 seconds, until the Orange LED has flashed. 4. Release the Reset Button. The Wireless Router is now using the factory default values.

About the Operation Modes

Access Point Mode

When acting as an access point, 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.

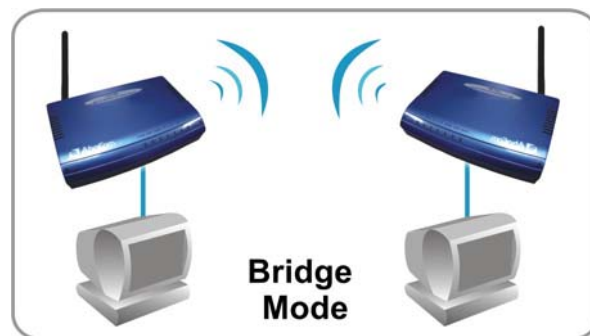


Bridge Mode

The WDS (Wireless Distributed System) function lets this access point act as a wireless LAN access point and repeater at the same time. Users can use this feature to build up a large wireless network in a large space like airports, hotels and schools and so on. This feature is also useful when users want to bridge networks between buildings where it is impossible to deploy network cable connections between these buildings.

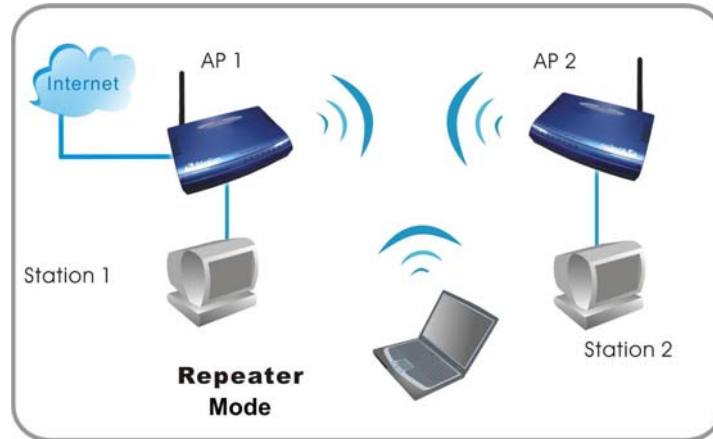
In this mode, all Ethernet ports and wireless interface are bridge together and NAT function is disabled. All the WAN related function and firewall are not supported.

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



Repeater Mode

Refer to the illustration below. While acting as Bridges, AP1 (with Station 1 being associated) and AP2 (with Station 2 being associated) can communicate with each other through wireless interface (with WDS). Thus, Station 1 can communicate with Station 2 and both Station 1 and Station 2 are able to access the Internet if only AP1 or AP2 has the Internet connection. After setting up WDS, the client or AP can be set up to communicate with the stations.

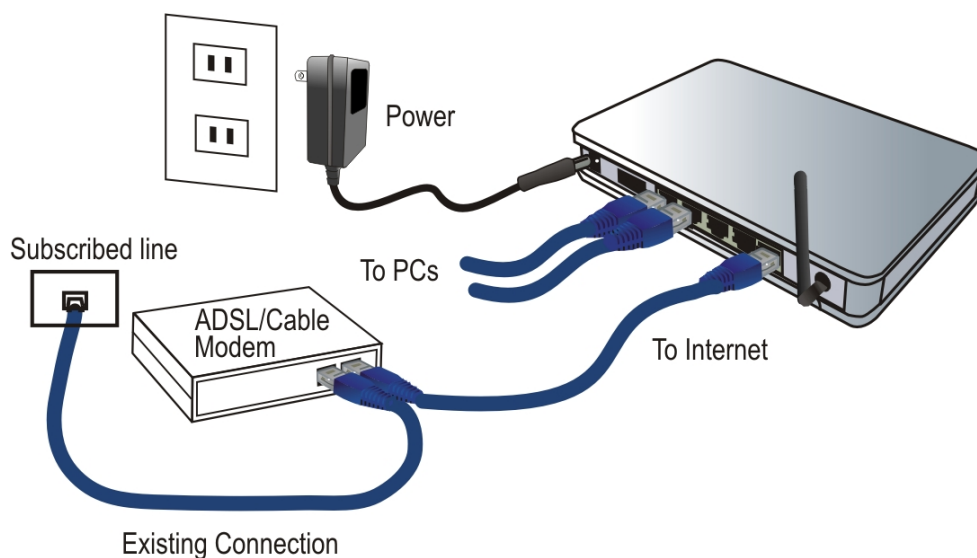


Chapter 2: Installation

Requirements

- Network cables. Use standard 10/100BaseT network (UTP) cables with RJ45 connectors.
- TCP/IP protocol must be installed on all PCs.
- For Internet Access, an Internet Access account with an ISP, and either of a DSL or Cable modem (for WAN port usage.)
- To use the Wireless Access Point, all wireless devices must be compliant with the IEEE802.11b or IEEE802.11g specifications.

Procedure



1. Choose an Installation Site

Select a suitable place on the network to install the Wireless Router.
Ensure the Wireless Router and the DSL/Cable modem are powered OFF.

2. Connect LAN Cables

Use standard LAN cables to connect PCs to the switching hub ports on the Wireless Router. Both 10BaseT and 100BaseT connections can be used simultaneously.

If required, connect any port to a normal port on another hub, using a standard LAN cable. Any LAN port on the Wireless Router will automatically function as an "Uplink" port when required.

3. Connect WAN Cable

Connect the DSL or Cable modem to the WAN port on the Wireless Router. Use the cable supplied with your DSL/Cable modem. If no cable was supplied, use a standard cable.

4. Power Up

- Power on the Cable or DSL modem.
- Connect the supplied power adapter to the Wireless Router and power up.
Use only the power adapter provided. Using a different one may cause hardware damaged.

5. Check the LEDs

- The *Power* LED should be ON.
- The *Status* LED should flash and then turn off. If it stays on, there is a hardware error.
- For each LAN (PC) connection, the LAN *Link/Act* LED should be ON (provided the PC is also ON.)
- The *WAN* LED should be ON.
- The *WLAN* LED should be ON.

For more information, refer to *Front-mounted LEDs* in Chapter 1.

Chapter 3: Configuration

Overview

This chapter describes the setup procedure for:

- Internet Access
- LAN configuration
- Wireless setup
- Assigning a password to protect the configuration data

PCs on your local LAN may also require configuration. For details, see [Chapter 4 - PC Configuration](#).

Other configuration may also be required, depending on which features and functions of the Wireless Router you wish to use. Use the table below to locate detailed instructions for the required functions.

Configuration Program

The Wireless Router contains a HTTP server. This enables you to connect to it, and configure it, using your Web Browser. **Your Browser must support JavaScript.**

The configuration program has been tested on the following browsers:

- Netscape V4.08 or later
- Internet Explorer V4 or later

Preparations

Before attempting to configure the Wireless Router, please ensure that:

- Your PC can establish a physical connection to the Wireless Router. The PC and the Wireless Router must be directly connected (using the Hub ports on the Wireless Router) or on the same LAN segment.
- The Wireless Router must be installed and powered ON.
- If the Wireless Router's default IP Address (192.168.1.254) is already used by another device, the other device must be turned OFF until the Wireless Router is allocated a new IP Address during configuration.

Using UPnP

If your Windows system supports UPnP, an icon for the Wireless Router will appear in the system tray, notifying you that a new network device has been found, and offering to create a new desktop shortcut to the newly-discovered device.

- Unless you intend to change the IP Address of the Wireless Router, you can accept the desktop shortcut.
- Whether you accept the desktop shortcut or not, you can always find UPnP devices in *My Network Places* (previously called *Network Neighborhood*).
- Double - click the icon for the Wireless Router (either on the Desktop, or in *My Network Places*) to start the configuration. Refer to the following section *Setup Wizard* for details of the initial configuration process.

Using your Web Browser

To establish a connection from your PC to the Wireless Router:

1. After installing the Wireless Router in your LAN, start your PC. If your PC is already running, please restart it.
2. Start your Web Browser.
3. In the *Address* box, enter "HTTP://" and the IP Address of the Wireless Router, as in this example, which uses the Wireless Router's default IP Address:

[HTTP://192.168.1.254](http://192.168.1.254)

No password is required by default, simply enter the username "admin", which is fixed and cannot be changed. However, you can assign a set of password for future security. See the [Password Setup](#) section later in this chapter for details.

If you can't connect...

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

- The Wireless Router is properly installed, LAN connection is OK, and it is powered ON. You can test the connection by using the "Ping" command:
 - Open the MS-DOS window or command prompt window.
 - Enter the command:
`ping 192.168.1.254`
If no response is received, either the connection is not working, or your PC's IP address is not compatible with the Wireless Router's IP Address. (See next item.)
- If your PC is using a fixed IP Address, its IP Address must be within the range 192.168.1.1 to 192.168.1.253 to be compatible with the Wireless 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 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.

Setup Wizard

The Setup Wizard provides brief and basic configuration of this device, you may enter each screen to change the default settings. For more detailed settings, you may refer to the “[Configuration via Web](#)” section.

1. View the listed configuration items and click **Next** to continue.

The screenshot shows the 'Setup Wizard' main screen. On the left is a sidebar menu with options: Setup Wizard, LAN, Password, Status, Wireless, Advanced, and Administration. The 'Log Out' button is at the bottom of the sidebar. The main content area is titled 'Setup Wizard' and contains the text: 'The setup wizard will guide you to configure the router for the first time. Please follow the setup wizard step by step.' Below this text is a numbered list of steps: 1. Choose your Time Zone, 2. Setup LAN Interface, 3. Setup WAN Interface, 4. Wireless LAN Setting, and 5. Wireless Security Setting. At the bottom right of the main area are two buttons: 'Cancel' and 'Next >>'.

2. Configure Time Zone and NTP server by enabling NTP client update. Click **Next** to continue.

The screenshot shows the 'Setup Wizard - Time Zone Setting' screen. The sidebar menu is the same as in the previous screen. The main content area is titled 'Setup Wizard - Time Zone Setting' and contains the text: 'You can maintain the system time by synchronizing with a public time server over the Internet.' Below this text is a checkbox labeled 'Enable NTP client update' which is checked. Underneath is a 'Time Zone Select:' dropdown menu showing '(GMT+08:00)Taipei'. Below that is an 'NTP server:' dropdown menu showing '192.5.41.41 - North America'. At the bottom right are three buttons: 'Cancel', '<< Back', and 'Next >>'.

3. Configure the parameters for area network (If you want to change the default parameters) by entering New IP Address and Subnet Mask.

The screenshot shows the 'Setup Wizard - LAN Interface Setup' screen. The sidebar menu is the same as in the previous screens. The main content area is titled 'Setup Wizard - LAN Interface Setup' and contains the text: '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.' Below this text are two input fields: 'IP Address:' with the value '192.168.1.254' and 'Subnet Mask:' with the value '255.255.255.0'. At the bottom right are three buttons: 'Cancel', '<< Back', and 'Next >>'.

4. Change the access method (Static IP, DHCP Client, PPPoE, PPTP or L2TP) by selecting for the pull-down menu. Then click **Next** to continue.

Setup Wizard - WAN Interface Setup

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

WAN Access Type: DHCP Client

Cancel << Back Next >>

5. To configure the parameters for wireless LAN clients. You can check **Disable Access Point** box to disable the settings of the wireless function in this page. Or just click **Next** to continue.

Setup Wizard - Wireless Basic Settings

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

☐ Disable Access Point

Band: 2.4 GHz (B+G)

Mode: AP

SSID: Testing

Channel Number: 11

Cancel << Back Next >>

6. To manage your wireless network security by selecting the encryption type (None, WEP, WPA, WPA2 (AES) and WPA2 Mixed) from the pull-down menu. Click **Finished** to exit **Setup Wizard** screen.

Setup Wizard - Wireless Security Setup

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.

Encryption: None

Cancel << Back Finished

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).

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.

Configuration via Web

LAN Interface Setup

Setup Wizard

LAN

Password

Status

▼ Wireless

▼ Advanced

▼ Administration

Log Out

LAN Interface Setup

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, DHCP, etc..

IP Address:

192.168.1.254

Subnet Mask:

255.255.255.0

DHCP:

Server

DHCP Client Range:

192.168.1.1

-

192.168.1.100

Show DHCP Client

Save

Reset

Add DHCP Static Lease Client

MAC Address:

Lease IP Address:

Save

Reset

Current Static Lease Clients:

MAC Address

Leased IP

Select

Delete Selected

Delete All

Reset

IP Address	Default: 192.168.1.254 (this is the local address of this Router.)
Subnet Mask	Default: 255.255.255.0
DHCP	Disabled: Select to disable this Router to distribute IP addresses. Server: Select to enable this Router to distribute IP Addresses (DHCP Server). And the following field will be activated for you to enter the IP Address range.
DHCP Client Range	The starting address of this local IP network address pool. The pool is a piece of continuous IP address segment. Keep the default value 192.168.1.1 should work for most cases. <ul style="list-style-type: none">Maximum: 253. Default value 253 should work for most cases. <i>Note: If “Continuous IP address pool starts” is set at 192.168.1.1 and the “Number of IP address in pool” is 253, the device will distribute IP addresses from 192.168.1.1 to 192.168.1.253 to all the computers in the network that request IP addresses from DHCP server (Router.)</i>
Show DHCP Client	Click to show Active DHCP Client Table.
Save	After completing the settings on this page, click Save button to save the settings.
Reset	Click Reset button to restore to default values.

Add DHCP Static Lease Client	<p>MAC Address: 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 they connected.</p> <p>Lease IP Address: Enter the fixed IP address that DHCP Server assigned to a certain connected station.</p> <p>Current Static Lease Clients: Here shows the static IP address that have been assigned according to the MAC address.</p>
-------------------------------------	---

Password Setup

Password Setup

This page is used to set the account to access the web server of this router. Empty user name and password will disable the protection.

New Password:

Confirmed Password:

Save Reset

New Password	Maximum input is 36 alphanumeric characters (case sensitive.)
Confirmed Password	Key in the password again to confirm.
Save	After completing the settings on this page, click Save to save the settings.
Reset	Click Reset to clear settings.

Status

Status

Internet

Connection Method:

Fixed IP

Internet IP Address:

10.0.2.225

Connection Details

LAN

IP Address:

192.168.1.254

Network Mask:

255.255.255.0

DHCP Server:

ON

System

Firmware Version:

v11.2.3.0.1e

System Data

Refresh Screen

Internet	Shows the Internet connection method and Internet IP address status.
Connection Details	Click to show more details of the Internet connection.
LAN	Shows the Local Area Network information.
System	Shows the device firmware information.
System Data	Click to show the detailed information of the system.
Refresh Screen	Click to renew all data.

Wireless

Wireless Basic Settings

Wireless Basic Settings

This page is used to configure the parameters for wireless LAN clients which may connect to your Access Point. Here you may change wireless encryption settings as well as wireless network parameters.

☐ Disable Access Point

Band:

2.4 GHz (B+G)

Mode:

AP

SSID:

Testing

Channel Number:

11

Associated Clients:

Show Active Clients

Save

Reset

Disable Access Point	<p>Check to disable the Access Point function.</p> <p>The wireless (WLAN) LED on front panel will remain OFF if the Wireless interface is disabled.</p>
Band	<p>You can choose one mode of the following you need.</p> <p><input type="radio"/> 2.4GHz (B): 802.11b supported rate only.</p> <p><input type="radio"/> 2.4GHz (G): 802.11g supported rate only.</p> <p><input type="radio"/> 2.4GHz (B+G): 802.11b supported rate and 802.11g supported rate.</p> <p>The default is 2.4GHz (B+G) mode.</p>
Mode	You can select AP, Bridge or Repeater mode as you need.
SSID	A SSID is referred to a network name because essentially it is a name that identifies a wireless network.
Channel Number	Select which channel to be located (from 1 to 11 or Auto.)
Associated Clients	Click to show all the listed active clients.
Save	After completing the settings on this page, click Save to save the settings.
Reset	Click Reset to restore to default values.

Wireless Advanced Settings

Wireless Advanced Settings

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

Authentication Type:
☐ Open System
 ☐ Shared Key
 ☒ Auto

Preamble Type:
☒ Long Preamble
 ☐ Short Preamble

Broadcast SSID:
☒ Enabled
 ☐ Disabled

Authentication Type	<p>Open System: If your access point/ wireless router is using "Open" authentication, then the wireless adapter will need to be set to the same authentication type.</p> <p>Shared Key: Shared Key is when both the sender and the recipient share a secret key.</p> <p>Auto: Select Auto switch for the adapter to automatically select the appropriate recipient or sender.</p>
----------------------------	--

Preamble Type	<p>A preamble is a signal used in wireless environment to synchronize the transmitting timing including Synchronization and Start frame delimiter.</p> <p>(Note: If you want to change the Preamble type into Long or Short, please check the setting of AP.)</p>
Broadcast SSID	<p>Enabled: This wireless AP will broadcast its SSID to stations.</p> <p>Disabled: 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.</p>
Save	After completing the settings on this page, click Save to apply the settings.
Reset	Click Reset to restore to default values.

Security

Here you can configure the security of your wireless network. Selecting different method will enable you to have different level of security. Please note that by using any encryption, by which data packet is encrypted before transmission to prevent data packets from being eaves-dropped by unrelated people, there may be a significant degradation of the data throughput on the wireless link.

Note: This security function only enabled under **AP mode** and **Repeater mode**.

Wireless Security Setup

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

Encryption: None Set WEP Key

Note: When encryption WEP is selected, you must set WEP key value.

☐ Use 802.1x Authentication

☒ WEP 64bits ☐ WEP 128bits

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

WPA Cipher Suite: ☒ TKIP ☐ AES

WPA(Pre-Shared Key) Format: Passphrase

WPA Pre-Shared Key:

Group Key Life Time: 86400 sec

☐ Enable Pre-Authentication

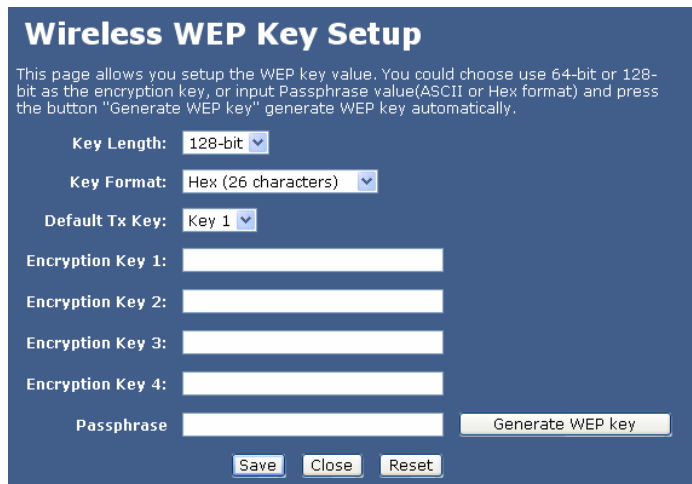
Authentication RADIUS Server: Port 1812 IP address Password

Save Reset

Encryption	<p>None (Encryption is set to None by default).</p> <p>If Use 802.1x Authentication is selected, the RADIUS Server will proceed to check the 802.1x Authentication.</p>
-------------------	--

WEP

If **WEP** is selected, users will have to **Set WEP keys** either manually or select to **Use 802.1x Authentication** to make the RADIUS server to issue the WEP key dynamically.



The image shows a screenshot of a web-based configuration page titled "Wireless WEP Key Setup". The page has a dark blue header with the title in white. Below the header, there is a paragraph of text explaining the purpose of the page: "This page allows you setup the WEP key value. You could choose use 64-bit or 128-bit as the encryption key, or input Passphrase value(ASCII or Hex format) and press the button 'Generate WEP key' generate WEP key automatically." The form contains several fields and buttons: "Key Length:" with a dropdown menu set to "128-bit"; "Key Format:" with a dropdown menu set to "Hex (26 characters)"; "Default Tx Key:" with a dropdown menu set to "Key 1"; four "Encryption Key" fields (1, 2, 3, 4) which are empty text boxes; a "Passphrase" field which is an empty text box; a "Generate WEP key" button; and three buttons at the bottom: "Save", "Close", and "Reset".

Wireless WEP Key Setup:

Key Length: Select the key length from the pull-down menu, either 64-bit or 128-bit.

Key Format: Select Hex if you are using hexadecimal numbers (0-9, or A-F). Select ASCII if you are using ASCII characters (case-sensitive).

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

Default Tx Key: You can specify up to 4 different keys to decrypt wireless data. Select the Default key index from the pull-down menu. Select the key 1~4 index from the pull-down menu.

Encryption Key 1~4: To configure your WEP settings. **WEP (Wired Equivalent Privacy)** encryption can be used to ensure the security of your wireless network. Select one **Key** and **Key Length** then fill in the appropriate value or phrase in **Encryption** field.

Note: *You must use the same **Key** and **Encryption** settings for the both sides of the wireless network connection.*

Passphrase: Enter the passphrase and click **Generate WEP Key** button to generate the WEP encryption key automatically.

Save: Press to apply the new settings on the screen.

Close: Click to leave the screen.

Reset: Click to restore the screen.

WPA

WPA (TKIP/AES): If **WPA** is selected, users will have to select the **WPA Authentication Modes** between **Enterprise**

	<p>(RADIUS) and Personal (Pre-shared Key), and select WPA Cipher Suite for TKIP or AES. Then enter the WPA Pre-shared Key in the column to setup the wireless network security if you select Personal (Pre-shared Key) authentication mode or enter the Port, IP address and Password if you select the Enterprise (RADIUS) authentication mode.</p> <p>WPA2 (AES)/WPA2 Mixed</p> <p>If WPA2 (AES)/WPA2 Mixed is selected from encryption pull-down menu, users will have to select the WPA Authentication Modes between Enterprise (RADIUS) –set the Port, IP address and Password, and Personal (Pre-shared Key) –select Passphrase or Hex (64 characters) then enter the WPA Pre-shared Key in the column to setup the wireless network security.</p>
WPA (Pre-shared Key) Format	<p>The WPA (Pre-shared Key) Format will be enabled when WPA, WPA2 (AES) and WPA2 Mixed encryption be selected.</p> <p>There are two formats for choice to set the Pre-shared key, Passphrase and Hex (64 characters). If Hex is selected, users will have to enter a 64 characters string. For easier configuration, the Passphrase (at least 8 characters) format is recommended.</p>
WPA Pre-Shared Key	<p>Pre-Shared Key serves as a password. Users may key in 8 to 63 characters string if you select Passphrase Pre-shared key format to set the passwords or leave it blank, in which the 802.1x Authentication will be activated. Make sure the same password is used on client's end.</p>
Group Key Life Time	<p>Enter the number of seconds that will elapse before the group key change automatically. The default is 86400 seconds.</p>
Enable Pre-Authentication	<p>The two most important features beyond WPA to become standardized through 802.11i/WPA2 are pre-authentication, which enables secure fast roaming without noticeable signal latency.</p> <p>Pre-authentication provides a way to establish a PMK security association before a client associates. The advantage is that the client reduces the time that it's disconnected to the network.</p>
Authentication RADIUS Server	<p>Port: Enter the RADIUS Server's port number provided by your ISP. The default is 1812.</p> <p>IP Address: Enter the RADIUS Server's IP Address provided by your ISP.</p> <p>Password: Enter the password that the AP shares with the RADIUS Server.</p>
Save	<p>Press to apply the new settings on the screen.</p>
Reset	<p>Press to discard the current settings.</p>

WDS Settings

WDS Settings

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

☐ Enable WDS

Add WDS AP: MAC Address Comment

Current WDS AP List:

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

Enable WDS	Check the box to enable the WDS function.
Add WDS AP	<p>MAC Address: Enter the Wireless BSSID (MAC) of the wireless AP that you want to connect with. To check your wireless router's MAC address, please go to Status and then click the System Data button to find your MAC address.</p> <p>Comment: Enter a description for the device.</p>
Set Security	<p>Enable the WDS function and then click Set Security button to set up the WDS security.</p> <div><h3>WDS Security Setup</h3><p>This page allows you setup the wireless security for WDS. When enabled, you must make sure each WDS device has adopted the same encryption algorithm and Key.</p><p>Encryption: <input type="text" value="None"/></p><p>WEP Key Format: <input type="text" value="ASCII"/></p><p>WEP Key: <input type="text"/></p><p>Pre-Shared Key Format: <input type="text" value="Passphrase"/></p><p>Pre-Shared Key: <input type="text"/></p><p><input type="button" value="Save"/> <input type="button" value="Close"/> <input type="button" value="Reset"/></p></div> <p>WDS Security Setup</p> <p>Encryption: Select the encryption type None, WEP 64 bits, WEP 128 bits, WPA (TKIP) and WPA2 (AES) from the pull-down menu.</p> <p>WEP Key Format: For WEP 64 bits and WEP 128 bits encryption type, the selection of WEP Key Format are Hex and ASCII.</p> <p>WEP Key: If select Hex if you are using hexadecimal numbers (0-9, or A-F). Select ASCII if you are using ASCII characters (case-sensitive).</p>

	<ul style="list-style-type: none">● 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). <p>Pre-Shared Key Format: The Pre-shared Key Format will be enabled when WPA (TKIP) and WPA2 (AES) encryption be selected. There are two formats for choice to set the Pre-shared key, Passphrase and Hex (64 characters). If Hex is selected, users will have to enter a 64 characters string. For easier configuration, the Passphrase (at least 8 characters) format is recommended.</p> <p>Pre-Shared Key: Pre-Shared-Key serves as a password. Users may key in 8 to 63 characters string to set the passwords or leave it blank, in which the 802.1x Authentication will be activated. Make sure the same password is used on client's end.</p> <p>Save: Press to save the new settings on the screen.</p> <p>Close: Click to leave the screen.</p> <p>Reset: Click to restore the screen.</p>					
Show Statistics	<p>Click to show the current WDS AP table. This table shows the MAC address, transmission packets and errors, reception packets and Tx Rate (Mbps) counters for each configured WDS AP.</p> <div><div><h3>WDS AP Table</h3><p>This table shows the MAC address, transmission, reception packet counters for each configured WDS AP.</p><table><tr><td>MAC Address</td><td>Tx Packets</td><td>Tx Errors</td><td>Rx Packets</td><td>Tx Rate(Mbps)</td></tr></table><div><div>Refresh</div><div>Close</div></div></div></div> <p>Refresh: Click to renew the counters information.</p> <p>Close: Click to leave the screen.</p>	MAC Address	Tx Packets	Tx Errors	Rx Packets	Tx Rate(Mbps)
MAC Address	Tx Packets	Tx Errors	Rx Packets	Tx Rate(Mbps)		
Save	Click Save to save the current settings.					
Reset	Click Reset to clear and reset.					
Current WDS AP List	Here shows the current WDS AP information.					
Delete Selected	Click Delete Selected to delete the selected AP information.					
Delete All	Click Delete All to delete all the items.					
Reset	Click Reset to restore the settings.					

Trusted Stations

The Trusted Stations screen allows you to configure this device to give exclusive access to up to 20 devices. Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02. You need to know the MAC address of the devices to configure this screen.

If you choose 'Allow Listed', only those clients whose wireless MAC addresses are in the access control list will be able to connect to your Access Point.

Wireless Trusted Stations

If you choose 'Allow Listed', only those clients whose wireless MAC addresses are in the access control list will be able to connect to your Access Point.

Wireless Access Control Mode: Disable

MAC Address:

Comment:

Save Reset

Current Access Control List:

MAC Address	Comment	Select
Delete Selected Delete All Reset		

Wireless Access Control Mode	Select the Access Control Mode from the pull-down menu. Disable: Select to disable Wireless Access Control Mode. Allow Listed: Only the stations shown in the table can associate with the AP.
MAC Address	Enter the MAC addresses of the wireless station that are allowed or denied access to this wireless router in these address fields. Enter the MAC addresses in a valid MAC address format, that is, six hexadecimal character pairs, for example, 12:34:56:78:9a:bc.
Comment	Enter in a descriptive name so you know which device the MAC address is associated with.
Save	After completing the settings on this page, click Save to save the settings.
Reset	Click Reset to restore to default values.
Current Access Control List	Shows the current access control list.
Delete Selected	Select the MAC Address (es) you want to delete and then click the Delete Selected button to delete the selected items.
Delete All	Click to delete all the MAC Address (es) listed.
Reset	Click Reset to restore to default values.

Advanced

WAN Port

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

WAN Port Configuration

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

WAN Access Type: DHCP Client

☒ Attain DNS Automatically

☐ Set DNS Manually

DNS 1:

DNS 2:

DNS 3:

Clone MAC Address:

☐ Respond to WAN Ping

☒ Enable UPnP

☒ Enable IPsec pass through on VPN connection

☒ Enable PPTP pass through on VPN connection

☒ Enable L2TP pass through on VPN connection

Save Reset

WAN Access Type	Select the WAN Access Type (Static IP , DHCP Client , PPPoE , PPTP and L2TP) from the pull-down menu. Default setting is DHCP Client enabled.
Attain DNS Automatically Set DNS Manually	Select to Attain DNS Automatically or select Set DNS Manually to set the DNS server IP address at the following DNS 1~3 columns. Default setting is Attain DNS Automatically .
DNS 1 DNS 2 DNS 3	Enter the DNS server IP address(es) provided by your ISP, or you can specify your own preferred DNS server IP address(es). DNS 2 and DNS 3 servers are optional. You can enter another DNS server's IP address as a backup. DNS 2 and DNS 3 servers will be used when the DNS 1 server fails.
Clone MAC Address	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 this Clone MAC address in this section to replace the WAN MAC address with the MAC address of that PC.
<input type="checkbox"/> Enable uPNP <input type="checkbox"/> Enable Ipsec pass through on VPN connection <input type="checkbox"/> Enable L2TP pass through on VPN connection	Check to enable the listed functions.
Save	After completing the settings on this page, click Save to save the settings.
Reset	Click Reset to restore to default values.

Access Control

This screen allows you to block access to specified Internet services based on port number used. This can be used restrict Internet access to only certain applications or to block applications you feel may be harmful.

Access Control

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Router. Here you can restrict local LAN clients to access Internet application/services which use certain port to work. Use of such filters can be helpful in securing or restricting your local network.

☐ Enable Access Control

Select Services to Block

Port Range: -

Protocol:

Description:

Current Blocked Table:

Port Range	Protocol	Description	Select
<input type="button" value="Delete Selected"/> <input type="button" value="Delete All"/> <input type="button" value="Reset"/>			

Enable Access Control	Select to enable access control function.
Select Services to Block	This lists all defined Services. Select the Services you wish to block from the pull-down menu.
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 at both the start and finish fields.
Protocol	Select the protocol (TCP, UDP or Both) used to the remote system or service from the pull-down menu.
Description	You may key in a description for port range.

Save	After completing the settings on this page, click Save to save the settings.
Reset	Click Reset to restore to default values.
Current Blocked Table	Shows the current blocked information.
Delete Selected	Click Delete Selected to delete items which are selected.
Delete All	Click Delete All to delete all the items.
Reset	Click Reset to rest

Dynamic DNS

Dynamic DNS allows you to update your current dynamic IP address with one or many dynamic DNS services so that anyone can contact you (in NetMeeting, CU-SeeMe, etc.). You can also access your FTP server or Web site on your own computer using a domain name (for instance myhost.dhs.org, where myhost is a name of your choice) that will never change instead of using an IP address that changes each time you reconnect. Your friends or relatives will always be able to call you even if they don't know your IP address.

First of all, you need to have registered a dynamic DNS account with either www.dyndns.org or www.tzo.com. This is for people with a dynamic IP from their ISP or DHCP server that would still like to have a domain name. The Dynamic DNS service provider will give you a password or key.

Dynamic DNS Setting

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

☐ Enable DDNS

Service Provider: DynDNS

Domain Name:

User Name/Email:

Password/Key:

Result:

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

Enable DDNS	<p>Check to enable DDNS function.</p> <p>This free service is very useful when combined with the Virtual Server feature. It allows Internet users to connect to your Virtual Servers using a URL, rather than an IP Address. This also solves the problem of having a dynamic IP address. With a dynamic IP address, your IP address may change whenever you connect, which makes it difficult to connect to you.</p>
--------------------	---

Service Provider	<ul style="list-style-type: none"> • Select the desired DDNS Service Provider DynDNS or TZO from the pull-down menu. • Details of your DDNS account (Name, password, Domain name) must then be entered and saved on this screen. • This device will then automatically ensure that your current IP Address is recorded by the DDNS Service Provider. • From the Internet, users will now be able to connect to your Virtual Servers (or DMZ PC) using your Domain name.
Domain Name	Apply for a Domain Name, and ensure it is allocated to you.
User Name/Email	Enter your username or email for the DDNS Service.
Password/key	Enter your current password or key for the DDNS Service.
Result	Tells you the current result from trying to register your IP address with the DDNS provider.
Update	Click Update to renew the DDNS information.
Reset	Click Reset to restore to default values.

DMZ

A Demilitarized Zone is used to provide Internet services without sacrificing unauthorized access to its local private network. Typically, the DMZ host contains devices accessible to Internet traffic, such as Web (HTTP) servers, FTP servers, SMTP (e-mail) servers and DNS servers.

DMZ

A Demilitarized Zone is used to provide Internet services without sacrificing unauthorized access to its local private network. Typically, the DMZ host contains devices accessible to Internet traffic, such as Web (HTTP) servers, FTP servers, SMTP (e-mail) servers and DNS servers.

☐ Enable DMZ

DMZ Host IP Address:

Enable DMZ	Check the box to enable DMZ function. 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.
DMZ Host IP Address	<p>Enter the IP address of a particular host in your LAN which will receive all the packets originally going to the WAN port/Public IP address above.</p> <p>Note: You need to give your LAN PC clients a fixed/static IP address for DMZ to work properly.</p>

Save	After completing the settings on this page, click Save to save the settings.
Reset	Click Reset to restore to default values.

DoS Setting

DoS (Denial of Service) attacks can flood your Internet connection with invalid packets and connection requests, using so much bandwidth and so many resources that Internet access becomes unavailable. The Wireless Router incorporates protection against DoS attacks. This screen allows you to configure DoS protection.

Denial of Service

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

☐ Enable DoS Prevention

☐ Whole System Flood: SYN

50 Packets/Second

☐ Whole System Flood: FIN

50 Packets/Second

☐ Whole System Flood: UDP

50 Packets/Second

☐ Whole System Flood: ICMP

50 Packets/Second

☐ Per-Source IP Flood: SYN

50 Packets/Second

☐ Per-Source IP Flood: FIN

50 Packets/Second

☐ Per-Source IP Flood: UDP

50 Packets/Second

☐ Per-Source IP Flood: ICMP

50 Packets/Second

☐ TCP/UDP PortScan

Low Sensitivity

☐ ICMP Smurf

☐ IP Land

☐ IP Spoof

☐ IP TearDrop

☐ PingOfDeath

☐ TCP Scan

☐ TCP SynWithData

☐ UDP Bomb

☐ UDP EchoChargen

☐ Enable Source IP Blocking 30 Block time (sec)

Select All

Clear All

Apply Changes

Enable DoS Prevention	Check to enable the DoS prevention function. Select the item listed to enable.
------------------------------	--

Enable Source IP Blocking	Set the threshold for the frequency of packets that are allowed to pass through. The default value is 30 packets per seconds. You can adjust the value according to your need. It is recommended that you set a practical number so that your network performance won't be hampered.
Block time (sec)	
Select All	Click to select all listed items.
Clear All	Click to clear all listed items.
Apply Changes	Click to save the current settings.

Virtual Servers

The Virtual Server function is a list of inside (behind NAT on the LAN) servers, for example, web or FTP, that you can make visible to the outside world even though NAT makes your whole inside network appear as a single computer to the outside world. You may enter a single port number or a range of port numbers to be forwarded, and the local IP address of the desired server. The port number identifies a service; for example, web service is on port 80 and FTP on port 21. In some cases, such as for unknown services or where one server can support more than one service (for example both FTP and web service), it might be better to specify a range of port numbers. You can allocate a server IP address that corresponds to a port or a range of ports. Many residential broadband ISP accounts do not allow you to run any server processes (such as a Web or FTP server) from your location. Your ISP may periodically check for servers and may suspend your account if it discovers any active services at your location. If you are unsure, refer to your ISP.

Virtual Servers

Entries in this table allow you to automatically redirect common network services to a specific machine behind the NAT firewall. These settings are only necessary if you wish to host some sort of server like a web server or mail server on the private local network behind your Gateway's NAT firewall.

☐ Enable Virtual Servers

Servers:

Local IP Address:

Protocol: Both

Port Range: -

Description:

Current Virtual Servers Table:

Local IP Address	Protocol	Port Range	Description	Select
<input type="button" value="Delete Selected"/> <input type="button" value="Delete All"/> <input type="button" value="Reset"/>				

Enable Virtual Servers	Check to enable virtual servers function.
Servers	You can set up a local server with specific port number that stands for the service Web, FTP, E-Mail(POP3), E-Mail (SMTP), DNS and Telnet listed in the pull-down. (e.g. web

	(80), FTP (21), Telnet (23)). When this device receives an incoming access request for this specific port, it will be forwarded to the corresponding internal server. You can add virtual servers by either port numbers or by names. Maximum 24 Server entries are allowed and each port number can only be assigned to one IP address.
Local IP Address	Enter the Local Server's IP address.
Protocol	Select the protocol (TCP, UDP or Both) used to the remote system or service.
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.
Description	You may key in a description for the local IP address.
Save	After completing the settings on this page, click Save to save the settings.
Reset	Click Reset to restore to default values.
Current Virtual Servers Table	Shows the current virtual servers information.
Delete Selected	Click Delete Selected to delete items which are selected.
Delete All	Click Delete All to delete all the items.
Reset	Click Reset to restore to default values.

Special Applications

If you use Internet applications that use non-standard connections or port numbers, you may find that they do not function correctly because they are blocked by the Wireless Router's firewall. In this case, you can define those applications as "**Special Applications**" so that they can function properly.

You can define your Special Applications. You will need detailed information about the application such as number of port required; this is normally available from the supplier of the application.

Also, please note that "**Incoming Type**" on this screen refer to traffic from the client (PC) viewpoint.

You have to firstly check **Enable** box, at the right side of the screen, before you add or edit an application.

Special Applications

Some applications require multiple connections, such as Internet gaming, video conferencing, Internet telephony and others. These applications cannot work when Network Address Translation (NAT) is enabled. If you need to run applications that require multiple connections, specify the port normally associated with an application in the "Trigger Port" field, select the protocol type as TCP or UDP, then enter the public ports associated with the trigger port to open them for inbound traffic.

Name	Incoming Type	Incoming Start Port	Incoming Finish Port	Trigger Type	Trigger Start Port	Trigger Finish Port	Enable
Quick Time 4	BOTH	6970	6999	BOTH	554	554	<input type="checkbox"/>
Dialpad	BOTH	51200	51201	BOTH	7175	7175	<input type="checkbox"/>
PalTalk	BOTH	2090	2091	BOTH	8200	8700	<input type="checkbox"/>
Battle.net	UDP	6112	6119	TCP	6112	6112	<input type="checkbox"/>
	TCP	0	0	TCP	0	0	<input type="checkbox"/>
	TCP	0	0	TCP	0	0	<input type="checkbox"/>
	TCP	0	0	TCP	0	0	<input type="checkbox"/>
	TCP	0	0	TCP	0	0	<input type="checkbox"/>

Save Reset

Name	Enter the application name.
Incoming Type	Click pull-down menu to select the incoming application type (TCP, UDP or BOTH.)
Incoming Start Port	Type a port number or the starting port number in a range of port numbers.
Incoming Finish Port	Type a port number or the ending port number in a range of port numbers.
Trigger Type	Click pull-down menu to select the trigger type (TCP or UDP)
Trigger Start Port	Enter a port number as the starting outbound port for the special application defined in the preceding field.
Trigger Finish Port	Enter a port number as the ending outbound port for the special application defined in the preceding field.
Enable	Check the box to add or edit the special applications function.
Save	Press to save the new settings on the screen.
Reset	Press to discard the data you have entered since last time you press Reset .

Ping

This screen allows you to perform a "**Ping**". The **response** messages that will appear below can be useful in diagnosing network problems.

Ping Toolkit

This page can be used to run ping command.

IP Address / Host Name

Response <Empty>

IP Address/ Host name	Enter the IP address or domain name that you want to ping.
Run	Click to start pinging.
Reset	Click to clear the current IP address /Host name.
Response	Here shows the ping executed results.

Diagnostics

This screen allows you to perform a DNS lookup on any host name you enter. This can be used to help diagnose network problems.

Network Diagnostics - DNS Lookup

Domain name/URL:

Domain Name/URL	Enter the domain name you want to lookup.
Start Lookup	Click this button to activate the DNS lookup.

Administration

Remote management

Remote management allows you to remotely configure your router over your Internet connection. Since this is a potential security risk, thus, this feature is turned off by default.

The Wireless Router can be managed from any PC on your LAN. And, if the Internet connection exists, it can also (optionally) be configured via the Internet.

Remote Management

If enabled, this device can be administrated via the internet, using your Web Browser with desired port number.

☐ Enable Web Server Access via WAN

Port Number:

Enable Web Server Access via WAN	Check to enable the function.
Port number	Enter the port number in the column.
Save	Click to save the current settings.
Reset	Click to clear the current settings.

Config File

This feature allows you to download the current settings from the Wireless Router, and save them to a file on your PC.

You can restore a previously downloaded configuration file to the Wireless Router, by uploading it to the Wireless Router.

This screen also allows you to set the Wireless Router back to its factory default configuration. Any existing settings will be deleted.

An example *Config File* screen is shown below.

Config File

In this section you may save your routers current settings for future use.
Select **DOWNLOAD** to save the current settings to a file on your computer.
You may also load previously saved settings by accessing the **RESTORE** feature.
The **Restore Defaults** selection resets your router to its original default settings

Backup Config:

Restore Config:

Default Config:

Backup Config	Use this to download a copy of the current configurations, and store the file on your PC. Click Download button to start saving current settings. Also you can click back to Upgrade Firmware button to go to the Upgrade Firmware screen to update firmware.
Restore Config	<p>This allows you to restore a previously saved configuration file back to the Wireless Router.</p> <p>Click Browse button to select the configuration file, then click Restore to upload the configuration file.</p> <p>WARNING! <i>Uploading a configuration file will destroy (overwrite) ALL of the existing settings.</i></p>
Default Config	<p>Clicking the Restore Defaults button will reset the Wireless Router to its factory default settings.</p> <p>WARNING! <i>This action will delete ALL of the existing settings.</i></p>

Logs

The Logs record various types of activity on the Wireless Router. This data is useful for troubleshooting, but enabling all logs will generate a large amount of data and adversely affect performance.

System Log

☐ Enable Log

☐ System all
☐ Wireless only
☐ DoS only

Apply Changes

Refresh

Clear

Enable Log	Check to enable logging function.
System All	Activates all logging functions.
Wireless Only	Only logs related to the wireless LAN will be recorded.
DoS Only	Only logs related to the DoS protection will be recorded.
Apply Changes	After completing the settings on this page, click Save to save the settings.
Refresh	Click to renew the logs.
Clear	Click to delete the logs.

IP Filtering

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Router. Here you can restrict local LAN clients to access Internet application/services by IP Address. Use of such filters can be helpful in securing or restricting your local network.

IP Filtering

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Router. Here you can restrict local LAN clients to access Internet application/services by IP Address. Use of such filters can be helpful in securing or restricting your local network.

☐ Enable IP Filtering

Local IP Address:

Protocol:

Description:

Current Filter Table:

Local IP Address	Protocol	Description	Select
<input type="button" value="Delete Selected"/> <input type="button" value="Delete All"/> <input type="button" value="Reset"/>			

Enable IP Filtering	Check to enable the IP filtering function.
Local IP Address	Enter the client IP address.
Protocol	Select the protocol (TCP, UDP or Both) used to the remote system or service.
Description	You may key in a description for the local IP address
Save	After completing the settings on this page, click Save to save the settings.

Reset	Click Reset to restore to default values.
Current Filter Table	Shows the current filter information.
Delete Selected	Click Delete Selected to delete items which are selected.
Delete All	Click Delete All to delete all the items.
Reset	Press to discard the data you have entered since last time you press Reset .

MAC Filtering

This screen is used to restrict devices on your local network from being able to access the Internet. You do this by entering the MAC address of any device you want to restrict.

MAC Filtering

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Router. Here you can restrict local LAN clients to access Internet application/services by MAC Address. Use of such filters can be helpful in securing or restricting your local network.

☐ Enable MAC Filtering

MAC Address:

Description:

Current Filter Table:

MAC Address	Description	Select
<input type="button" value="Delete Selected"/> <input type="button" value="Delete All"/> <input type="button" value="Reset"/>		

Enable MAC Filtering	Check to enable MAC filtering function.
MAC Address	Enter the client MAC address.
Description	You may key in a description for the MAC address.
Save	After completing the settings on this page, click Save to save the settings.
Reset	Click Reset to restore to default values.
Current Filter Table	Shows the current filter information.
Delete Selected	Click Delete Selected to delete items which are selected.
Delete All	Click Delete All to delete all the items.
Reset	Click Reset to restore to default values.

URL Filtering

URL filter is used to deny LAN users from accessing the internet. Block those URLs which contain keywords listed below.

URL Filtering

URL filter is used to deny LAN users from accessing the internet. Block those URLs which contain keywords listed below.

☐ Enable URL Filtering

URL Address:

Apply Changes Reset

Current Filter Table:

URL Address	Select
-------------	--------

Delete Selected Delete All Reset

Enable URL Filtering	Check to enable URL filtering function.
URL Address	Enter the local URL address.
Apply Changes	After completing the settings on this page, click Save to save the settings.
Reset	Click Reset to restore to default values.
Current Filter Table	Shows the current filter information.
Delete Selected	Click Delete Selected to delete items which are slected.
Delete All	Click Delete All to delete all the items.
Reset	Click Reset button to restore to default values.

Statistics

Statistics

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

Wireless LAN	Sent Packets	85
	Received Packets	8269
Ethernet LAN	Sent Packets	212
	Received Packets	4604
Ethernet WAN	Sent Packets	125
	Received Packets	0

Refresh

Refresh	Click Refresh button to update the statistics table.
---------	---

Time Zone Setting

Time Zone Setting

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

Current Time: Year Month Day Hr Min Sec

☐ Enable NTP client update

Time Zone Select:

NTP server: ☒
☐ (Manual IP Setting)

SaveResetRefresh

Current Time	Enter the current time of this wireless router.
Enable NTP client update	Check to enable NTP (Network Time Protocol Server) client update function.
Time Zone Select	Select the time zone from the pull-down menu.
NTP server	You may choose to select NTP server from the pull-down menu or enter an IP address of a specific server manually.
Save	After completing the settings on this page, click Save to save the settings.
Reset	Click Reset to restore to default values.
Refresh	Click Refresh button to renew current time.

Upgrade Firmware

Upgrade Firmware

This page allows you to upgrade this router's firmware to new version.
If you want to keep the current configuration, remember to backup the config file before upgrading firmware, and restore the config file after upgrading firmware.
Please note, **DO NOT** power off the router during this process because it may crash the system.

Select File:

Browse	Click the Browse button to find and open the firmware file (the browser will display to correct file path.)
Start Upgrade	Click the Start Upgrade button to perform.
Reset	Click Reset to restore to default values.

Chapter 4: PC Configuration

Overview

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

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

Windows Clients

This section describes how to configure Windows clients for Internet access via the Wireless Router.

The first step is to check the PC's TCP/IP settings.

The Wireless Router uses the TCP/IP network protocol for all functions, so it is essential that the TCP/IP protocol be installed and configured on each PC.

TCP/IP Settings - Overview

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

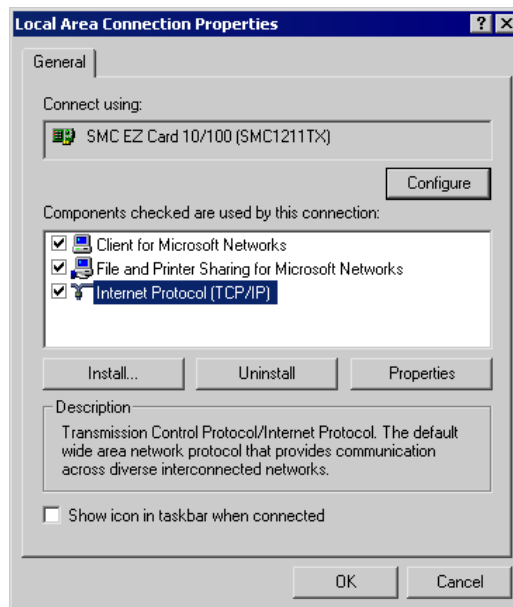
- By default, the Wireless Router will act as a DHCP Server, automatically providing a suitable IP Address (and related information) to each PC when the PC boots.
- For all non-Server versions of Windows, the default TCP/IP setting is to act as a DHCP client.

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

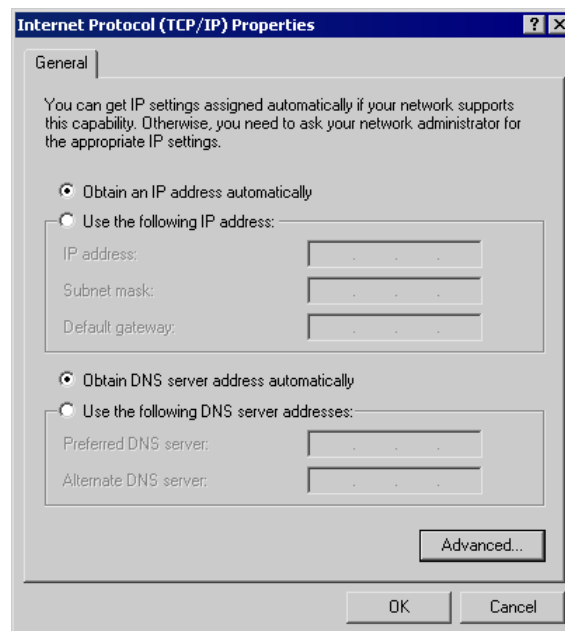
- The *Gateway* must be set to the IP address of the Wireless Router.
- The *DNS* should be set to the address provided by your ISP.

Checking TCP/IP Settings - Windows 2000:

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



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 *Obtain an IP Address automatically*. This is Windows default setting. **Using this setting is recommended.** By default, the Wireless Router will act as a DHCP Server.

Restart your PC to ensure it obtains an IP Address from the Wireless Router.

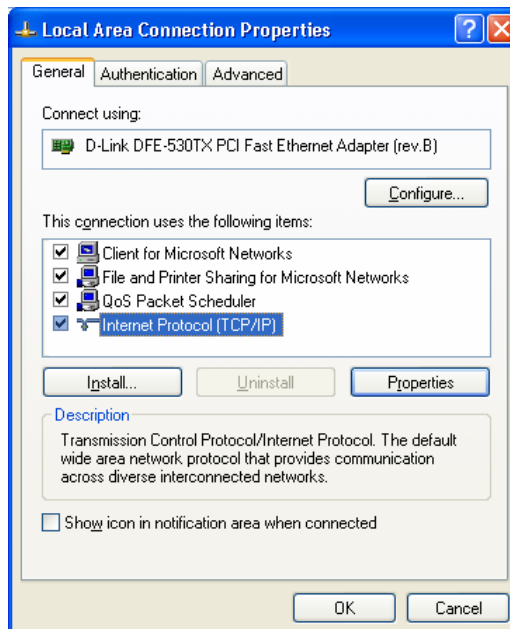
Using a fixed IP Address ("Use the following IP Address")

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

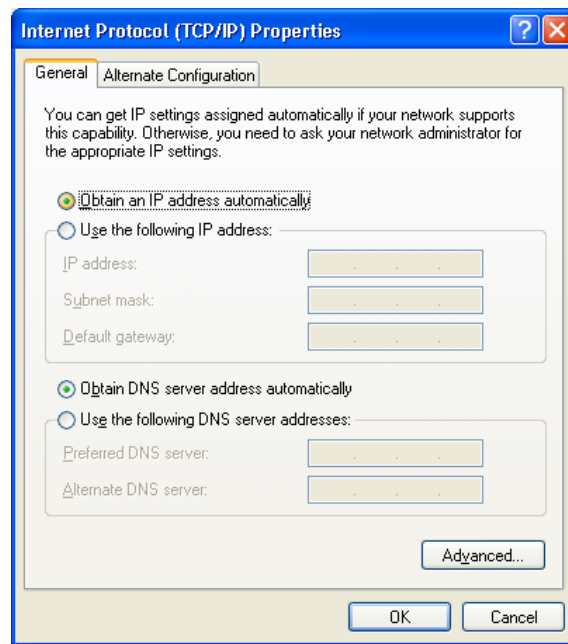
- Enter the Wireless Router's IP address in the *Default gateway* field and click *OK*. (Your LAN administrator can advise you of the IP Address they assigned to the Wireless Router.)
- If the *DNS Server* fields are empty, select *Use the following DNS server addresses*, and enter the DNS address or 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 setting is recommended.** By default, the Wireless Router will act as a DHCP Server.

Restart your PC to ensure it obtains an IP Address from the Wireless Router.

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

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

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

Internet Access

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

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

For Windows 2000

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

For Windows XP

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

Accessing AOL

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

- 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.
- Click the *Setup* button.
- Select *Create Location*, and change the location name from "New Locality" to "Wireless Router".
- Click *Edit Location*. Select *TCP/IP* for the *Network* field. (Leave the *Phone Number* blank.)
- Click *Save*, then *OK*.
Configuration is now complete.
- Before clicking "Sign On", always ensure that you are using the "Wireless Router" location.

Macintosh Clients

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

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

Note:

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

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

Linux Clients

To access the Internet via the Wireless Router, it is only necessary to set the Wireless Router as the "Gateway".

Ensure you are logged in as "root" before attempting any changes.

Fixed IP Address

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

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

To act as a DHCP Client (recommended)

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

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

Other Unix Systems

To access the Internet via the Wireless Router:

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

Wireless Station Configuration

This section applies to all Wireless stations wishing to use the Wireless Router's Access Point, regardless of the operating system which is used on the client.

To use the Wireless Access Point in the Wireless Router, each Wireless Station must have compatible settings, as follows:

Mode	The mode must be set to <i>Infrastructure</i> .
SSID (ESSID)	This must match the value used on the Wireless Router. The default value is Untitled Note! The SSID is case sensitive.
WEP	By default, WEP on the Wireless Router is disabled . <ul style="list-style-type: none">• If WEP remains disabled on the Wireless Router, all stations must have WEP disabled.• If WEP is enabled on the Wireless Router, each station must use the same settings as the Wireless Router.
WPA WPA2 (AES) WPA2 Mixed	WPA (TKIP/AES)/ WPA2 (AES)/ WPA2 Mixed: If one of these securities is enabled on the Wireless Router, each station must use the same settings as the Wireless Router. If there is no security is enabled on the Wireless Router, the security of each station should be disabled as well.

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

Appendix A:

Troubleshooting



Overview

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

General Problems

Problem 1:	Can't connect to the Wireless Router to configure it.
Solution 1:	<p>Check the following:</p> <ul style="list-style-type: none">• The Wireless Router is properly installed, LAN connections are OK, and it is powered ON.• Ensure that your PC and the Wireless Router are on the same network segment. (If you don't have a router, this must be the case.)• If your PC is set to "Obtain an IP Address automatically" (DHCP client), 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 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 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 Router. Ensure that it is connected and ON. Connect to it and check its settings. (If you can't connect to it, check the LAN and power connections.) • If the Wireless Router is configured correctly, check your Internet connection (DSL/Cable modem etc) to see that it is working correctly.
Problem 2:	Some applications do not run properly when using the Wireless Router.
Solution 2:	<p>The Wireless Router processes the data passing through it, so it is not transparent.</p> <p>Use the <i>Special Applications</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 Access Point.
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 Access Point are the same. Remember that the SSID is case-sensitive. So, for example "Workgroup" does NOT match "workgroup". • Both your PC and the Wireless Router must have the same setting for security. The default setting for the Wireless Router is disabled, so your wireless station should also have security disabled. • If security of the Wireless Router is on, your PC must have the same security enabled. • If the Wireless Router's <i>Wireless</i> screen is set to <i>Allow LAN access to selected Wireless Stations only</i>, then each of your Wireless stations must have been selected, or access will be blocked. • To see if radio interference is causing a problem, see if connection is possible when close to the Wireless Router. Remember that the connection range can be as little as 100 feet in poor environments.
Problem 2:	Wireless connection speed is very slow.
Solution 2:	<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"> • Wireless Router location. Try adjusting the location and orientation of the Wireless Router. • Wireless Channel If interference is the problem, changing to another channel may show a marked improvement. • Radio Interference Other devices may be causing interference. You can experiment by switching other devices Off, and see if this helps. Any "noisy" devices should be shielded or relocated. • RF Shielding Your environment may tend to block transmission between the wireless stations. This will mean high access speed is only possible when close to the Wireless Router.

Appendix B:

About Wireless LANs



Modes

Wireless LANs can work in either of two (2) modes:

- Ad-hoc
- Infrastructure

Ad-hoc Mode

Ad-hoc mode does not require an Access Point or a wired (Ethernet) LAN. Wireless Stations (e.g. notebook PCs with wireless cards) communicate directly with each other.

Infrastructure Mode

In Infrastructure Mode, one or more Access Points are used to connect Wireless Stations (e.g. Notebook PCs with wireless cards) to a wired (Ethernet) LAN. The Wireless Stations can then access all LAN resources.

	Access Points can only function in "Infrastructure" mode, and can communicate only with Wireless Stations which are set to "Infrastructure" mode.
--	--

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.)

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 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 four encryption options: **TKIP**, **AES**, **TKIP-AES** and additional setup for **RADIUS** is required in this method.

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.

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.

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	On client Wireless Stations, the mode must be set to "Infrastructure". (The Access Point is always in "Infrastructure" mode.)
SSID (ESSID)	Wireless Stations should use the same SSID (ESSID) as the Access Point they wish to connect to, but the SSID can not set to be null (blank).
WEP	<p>The Wireless Stations and the Access Point must use the same settings for WEP (64 Bit, 128 Bit).</p> <p>WEP Key: If WEP is enabled, the Key must be the same on the Wireless Stations and the Access Point.</p> <p>WEP Authentication: If WEP is enabled, all Wireless Stations must use the same setting as the Access Point (either "Open System" or "Shared Key").</p>
WPA WPA2 (AES) WPA2 Mixed	WPA (TKIP/AES)/ WPA2 (AES)/ WPA2 Mixed: If one of these securities is enabled on the Wireless Router, each station must use the same settings as the Wireless Router. If there is no security is enabled on the Wireless Router, the security of each station should be disabled as well.

Appendix C:

Specifications



Multi-Function Wireless Router

Model	Wireless Router
Dimensions	141mm(W) * 100mm(D) * 27mm(H)
Operating Temperature	0° C to 40° C
Storage Temperature	-10° C to 70° C
Network Protocol:	TCP/IP
Network Interface:	5 Ethernet: 4 * 10/100BaseT (RJ45) LAN connection 1 * 10/100BaseT (RJ45) for WAN
LEDs	12
Power Adapter	12 V DC External

Wireless Interface

Standards	IEEE802.11g WLAN, JEIDA 4.2, roaming support
Frequency	2.4 to 2.4835GHz (Industrial Scientific Medical Band)
Channels	Maximum 14 Channels, depending on regulatory authorities
Modulation	DSSS BPSK/QPSK/CCK, OFDM/CCK
Data Rate	Up to 54 Mbps
Coverage Area	Indoors : 15m @54Mbps, 120m @6Mbps or lower Outdoors : 40m @54Mbps, 300m @6Mbps or lower
Security	WEP 64 Bits, 128 Bits, WPA, WPA2, 802.1x
Output Power	13dBm (typical)
Receiver Sensitivity	-80dBm Min.

Regulatory Approvals

CE Standards

This product complies with the 99/5/EEC directives, including the following safety and EMC standards:

- EN300328-2
- EN301489-1/-17
- EN60950

CE Marking Warning

This is a Class B product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.