

**802.11n/b/g  
Wireless Broadband  
Router**

**USER'S GUIDE**

## **REGULATORY STATEMENTS**

### **FCC Certification**

The United States Federal Communication Commission (FCC) and the Canadian Department of Communications have established certain rules governing the use of electronic equipment.

Part15, Class B

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.

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

### **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 of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

### **CAUTION:**

Any changes or modifications not expressly approved by the grantee of this device could void the user's authority to operate the equipment.

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

### **FCC Radiation Exposure Statement:**

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

### **CE Statement:**

Hereby, AboCom, declares that this device is in compliance with the essential requirement and other relevant provisions of the R&TTE Directive 1999/5/EC.

# TABLE OF CONTENTS

<b>CHAPTER 1: INTRODUCTION .....</b>	<b>1</b>
Features .....	1
<b>CHAPTER 2: ABOUT THE OPERATING MODES.....</b>	<b>2</b>
Access Point Mode.....	2
Gateway Mode .....	3
<b>CHAPTER 3: ROUTER CONFIGURATION .....</b>	<b>4</b>
Login.....	4
Setup Wizard .....	7
Configuration via Web.....	7
Internet Settings .....	8
Wireless Settings.....	18
Firewall.....	29
Administration.....	37
<b>CHAPTER 4: PC CONFIGURATION.....</b>	<b>44</b>
Overview .....	44
Windows Clients.....	44
Macintosh Clients .....	49
Linux Clients.....	50
Other Unix Systems.....	50
Wireless Station Configuration .....	50
<b>APPENDIX A: TROUBLESHOOTING .....</b>	<b>52</b>
Overview .....	52
General Problems .....	52
Internet Access.....	52
Wireless Access .....	53
<b>APPENDIX B: ABOUT WIRELESS LANS.....</b>	<b>54</b>
BSS.....	54
Channels.....	54
Security.....	54
Wireless LAN Configuration.....	56
Regulatory Approvals .....	56

# CHAPTER 1:

## INTRODUCTION

The **802.11n/b/g Wireless Broadband Router** with the advanced MIMO technology, it can support the data transmission rate 6 times more (up to 300Mbps) and the coverage 3 times more than IEEE 802.11b/g devices. Router enables your whole network sharing a high-speed cable or DSL Internet connection. The incredible speed of **802.11n/b/g Wireless Broadband Router** makes it ideal for media-centric applications like streaming video, gaming, and Voice over IP technology, ensure optimum performance and maximum coverage with three external antennas.

With **802.11n/b/g Wireless Broadband Router**, you can share a high-speed Internet connection, files, printers, and multi-player games at incredible speeds, without the hassle of stringing wires. **802.11n/b/g Wireless Broadband Router** offers easy configuration for your wireless network in the home and presents wireless network to you home of high functionality, security, and flexibility.

## FEATURES

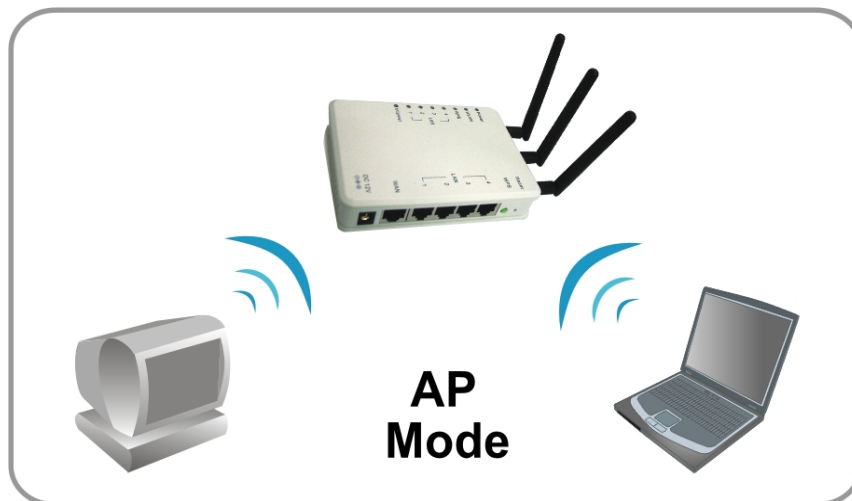
1. Support the IEEE 802.11n/b/g standard, high speed data rate up to 300Mbps.
2. Support WPS (Wi-Fi Protected Setup) with physical reset button.
3. High security with build-in Security: WEP 64/128, WPA, WPA2, WPA-PSK, WPA2-PSK 802.1x and 802.11i.
4. Support Gateway and AP mode.
5. Advanced Quality of Service (QoS) - 802.11e, WMM.
6. Easy configuration for home user setup.
7. MAC and Port filtering.

# CHAPTER 2: ABOUT THE OPERATING MODES

This device provides operational applications with **AP** and **Gateway** modes, which are mutually exclusive. If you want to change the settings in order to perform more advanced configuration or even change the mode of operation, you can use the web-based utility provided by the manufacturer as described in the following sections.

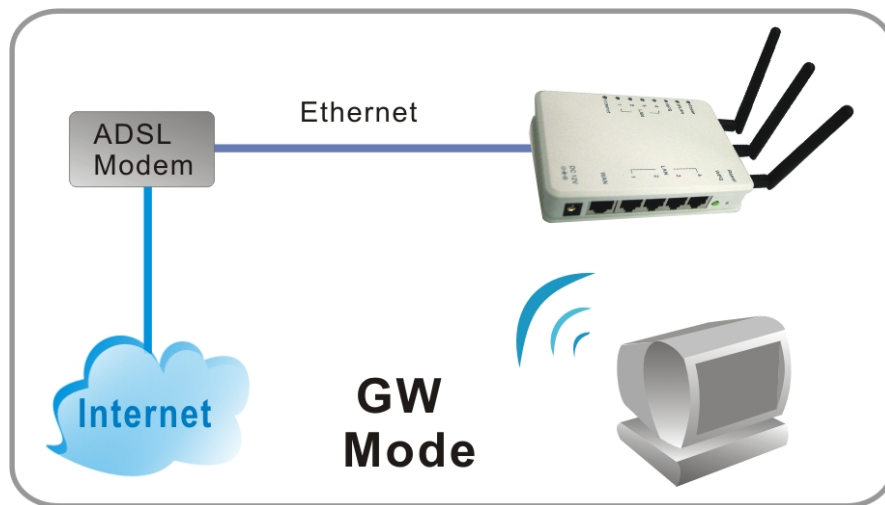
## ACCESS POINT MODE

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



# GATEWAY MODE

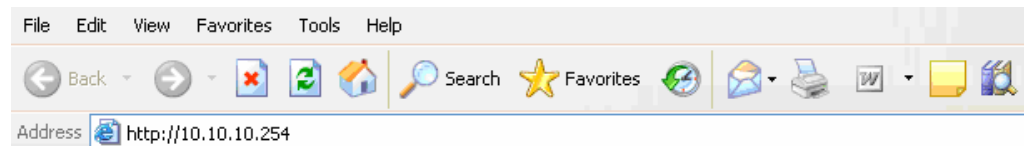
When GW mode is selected, the Router will enter the gateway mode. And the wireless connection will be set up from a point-to-point local LAN into a point-to-multipoint WAN.



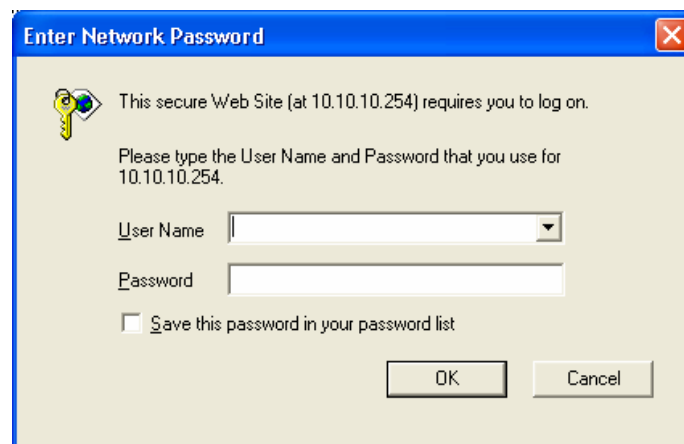
# CHAPTER 3: ROUTER CONFIGURATION

## LOGIN

1. Start your computer. Connect an Ethernet cable between your computer and the Wireless Router.
2. Make sure your wired station is set to the same subnet as the Wireless Router, i.e. 10.10.10.254
3. Start your WEB browser. In the *Address* box, enter the following: <http://10.10.10.254>



4. Please enter the username “admin” and password “admin” for login.



The configuration menu is divided into four folders: Internet Settings, Wireless Settings, Firewall, and Administration. Click on the desired setup item to expand the folder in the main navigation page. The setup pages covered in this utility are described below.

[open all](#) | [close all](#)

- Status
- Setup Wizard
- Operation Mode
- Internet Settings
- Wireless Settings
- Firewall
- Administration

## Status

System Info	
Firmware Version	3.0.1.0.2_B1_en_US (May 5 2008)
System Up Time	0day:0h:0m:49s
Operation Mode	Gateway Mode
Internet Configurations	
Connected Type	DHCP
Connection State	There is no cable plug in WAN port .
Physical Address	00:0C:43:28:60:E1
WAN IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Default Gateway	0.0.0.0
Domain Name Server	0.0.0.0
Local Network	
Physical Address	00:0C:43:28:60:E0
Local IP Address	10.10.10.254
Local Netmask	255.255.255.0



# 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"> <li>• PPTP Server IP Address.</li> <li>• User name and password.</li> <li>• IP Address allocated to you, if Static (Fixed).</li> </ul>

## 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.

# 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.

## SETUP WIZARD

The setup wizard will guide you to configure the router for the first time. Please follow the setup wizard step by step.

1. Setup LAN Interface
2. Setup WAN Interface
3. Wireless LAN Setting
4. Wireless Security Setting

Cancel

Next >>

# CONFIGURATION VIA WEB

## Operation Mode

Select an operation mode then click **Apply** to enable the mode you preferred or click **Reset** button to discard current settings. Default operation mode is Gateway mode.

### Operation Mode Configuration

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

**Access Point**

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

**Gateway**

In this mode, the device is supposed to connect to internet via ADSL/Cable Modem. The NAT is enabled and PCs in LAN ports connected to ISP through WAN port. The connection type can be setup in WAN page by using PPPoE, DHCP client, PPTP client or Static IP.

Apply

Reset

Operation Mode	
<b>Access Point</b>	When acting as an access point, this device connects all the stations (PC/notebook with wireless network adapter) to a wired network. All stations can have the Internet access if only the Access Point has the Internet connection.
<b>Gateway</b>	In this mode, the device is supposed to connect to internet via ADSL/Cable Modem. The NAT is enabled and PCs in LAN ports share the same IP to ISP through WAN port. The connection type can be setup in WAN page by using PPPOE, DHCP client, PPTP client or static IP.

## INTERNET SETTINGS

### WAN (Wide Area Network) Settings

**WAN Connection Type**, select the WAN access type (Static Mode (fixed IP), DHCP (Auto Config), PPPoE (ADSL), L2TP and PPTP) from the pull-down menu. (Default setting is DHCP (Auto Config) Type.)

#### 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 Address Cloning**

Clone PC's MAC

Clone MAC Address

Clone IP Address

Apply Cancel

Static Mode	
<p><b>WAN Connection Type:</b> <span style="float: right;">Static Mode (fixed IP) ▼</span></p>	
<b>Static Mode</b>	
IP Address	<input type="text" value="192.168.1.1"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>
Default Gateway	<input type="text" value="192.168.1.254"/>
Primary DNS Server	<input type="text" value="0.0.0.0"/>
Secondary DNS Server	<input type="text" value="0.0.0.0"/>
<b>MAC Address Cloning</b>	
<input type="checkbox"/> Clone PC's MAC	
Clone MAC Address	<input type="text"/>
Clone IP Address	<input type="text" value="▼"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	
<b>IP Address</b>	Enter the WAN IP address provided by your ISP in this column.
<b>Subnet Mask</b>	Enter the Subnet Mask in this column.
<b>Default Gateway</b>	Enter the default gateway IP provided by your ISP in this column.
<b>Primary and Secondary DNS Server</b>	The <i>DNS</i> should be set to the address provided by your ISP.
<b>Clone PC's MAC Address</b>	Check to enable this function.
<b>Clone MAC Address</b>	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.
<b>Clone IP Address</b>	Shows the IP address of the device from the pull-down menu.
<b>Apply</b>	Click to save and apply the current settings.
<b>Cancel</b>	Click to discard the current settings.

DHCP Mode	
WAN Connection Type: DHCP (Auto Config) ▼	
<b>DHCP Mode</b>	
Primary DNS Server	0.0.0.0
Secondary DNS Server	0.0.0.0
<b>MAC Address Cloning</b>	
<input checked="" type="checkbox"/> Clone PC's MAC	
Clone MAC Address	
Clone IP Address	▼
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	
<b>Primary and Secondary DNS Server</b>	The DNS should be set to the address provided by your ISP.
<b>Clone PC's MAC Address</b>	Check to enable this function.
<b>Clone MAC Address</b>	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.
<b>Clone IP Address</b>	Shows the IP address of the device from the pull-down menu.
<b>Apply</b>	Click to save and apply the current settings.
<b>Cancel</b>	Click to discard the current settings.

PPPoE Mode	
WAN Connection Type: <span style="float: right;">PPPOE (ADSL) ▼</span>	
<b>PPPoE Mode</b>	
User Name	<input type="text" value="pppoe_user"/>
Password	<input type="password" value="••••••••••"/>
MTU	<input type="text" value="1492"/>
Authentication Type	PAP ▼
MPPE Encryption Level	NONE ▼
PPPOE IP Address Mode	Dynamic ▼
Physical IP Address Mode	Dynamic ▼
DNS Mode	Dynamic ▼
<b>MAC Address Cloning</b>	
<input checked="" type="checkbox"/> Clone PC's MAC	
Clone MAC Address	<input type="text"/>
Clone IP Address	<input type="text" value="▼"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

<b>User Name</b>	Maximum input is 20 alphanumeric characters (case sensitive).
<b>Password</b>	Maximum input is 20 alphanumeric characters (case sensitive).
<b>MTU (Maximum Transmission Unit)</b>	Click the pull-down menu to select the most appropriate MTU (Maximum Transmission Unit, namely the maximum packet size, the default value is 1492) for your application. Reducing the packet size can help connecting to certain web sites or speeding up packet transfer rate. If the incorrect selection is entered, you may not be able to open certain web sites.
<b>Authentication Type</b>	Select PAP, CHAP, MSCHAP-v1, MSCHAP-v2 or Auto form the pull-down menu.
<b>MPPE Encryption Level</b>	When the authentication type has been set to be MSCHAP-v1, MSCHAP-v2 or Auto, here can select None, 40 bits, 56bits, 128bits or Auto form the pull-down menu.
<b>PPPoE IP Address Mode</b>	Select Dynamic or Static for the pull-down menu.
<b>Physical IP Address</b>	Select Dynamic or Static for the pull-down menu.

<b>Mode</b>	
<b>DNS mode</b>	Select from the pull-down menu for Static or Dynamic DNS mode.
<b>Clone PC's MAC Address</b>	Check to enable this function.
<b>Clone MAC Address</b>	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.
<b>Clone IP Address</b>	Shows the IP address of the device from the pull-down menu.
<b>Apply</b>	Click to save and apply the current settings.
<b>Cancel</b>	Click to discard the current settings.

### L2TP Mode

WAN Connection Type: L2TP

L2TP Mode	
Server Information	IP address <span style="float: right;">▼</span>
L2TP Server IP Address	<input type="text" value="172.1.1.1"/>
L2TP Server URL Address	<input type="text" value="l2tp_server"/>
User Name	<input type="text" value="l2tp_user"/>
Password	<input type="password" value="••••••••"/>
MTU	<input type="text" value="1400"/>
Authentication Type:	PAP <span style="float: right;">▼</span>
MPPE Encryption Level:	None <span style="float: right;">▼</span>
L2TP IP Address Mode	Dynamic <span style="float: right;">▼</span>
Physical IP Address Mode	Dynamic <span style="float: right;">▼</span>
DNS Mode	Dynamic <span style="float: right;">▼</span>
MAC Address Cloning	
<input checked="" type="checkbox"/> Clone PC's MAC	
Clone MAC Address	<input type="text"/>
Clone IP Address	<input style="float: right; text-align: right; width: 50px;" type="text"/> <span style="float: right;">▼</span>

<b>Server Information</b>	Select IP address or URL address form the pull-down menu.
<b>L2TP Server IP Address</b>	Enter the L2TP Server IP Address in this column.
<b>L2TP Server URL Address</b>	Enter the L2TP Server URL Address in this column.
<b>User Name</b>	Maximum input is 20 alphanumeric characters (case sensitive).
<b>Password</b>	Maximum input is 20 alphanumeric characters (case sensitive).
<b>MTU (Maximum Transmission Unit)</b>	Click the pull-down menu to select the most appropriate MTU (Maximum Transmission Unit, namely the maximum packet size, the default value is 1400) for your application. Reducing the packet size can help connecting to certain web sites or speeding up packet transfer rate. If the incorrect selection is entered, you may not be able to open certain web sites.
<b>Authentication Type</b>	Select PAP, CHAP, MSCHAP-v1, MSCHAP-v2 or Auto form the pull-down menu.
<b>MPPE Encryption Level</b>	When the authentication type has been set to be MSCHAP-v1, MSCHAP-v2 or Auto, here can select None, 40 bits, 56bits, 128bits or Auto form the pull-down menu.
<b>L2TP IP Address Mode</b>	Select Dynamic or Static for the pull-down menu.
<b>Physical IP Address Mode</b>	Select Dynamic or Static for the pull-down menu.
<b>DNS mode</b>	Select from the pull-down menu for Static or Dynamic DNS mode.
<b>Clone PC's MAC Address</b>	Check to enable this function.
<b>Clone MAC Address</b>	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.
<b>Clone IP Address</b>	Shows the IP address of the device from the pull-down menu.
<b>Apply</b>	Click to save and apply the current settings.



<b>Cancel</b>	Click to discard the current settings.																														
<b>PPTP Mode</b>																															
<p><b>WAN Connection Type:</b> PPTP <input type="button" value="v"/></p> <p><b>PPTP Mode</b></p> <table border="1"> <tr> <td>Server Information</td> <td>IP address <input type="button" value="v"/></td> </tr> <tr> <td>PPTP Server IP Address</td> <td>172.1.1.1</td> </tr> <tr> <td>PPTP Server URL Address</td> <td>pptp_server</td> </tr> <tr> <td>User Name</td> <td>pptp_user</td> </tr> <tr> <td>Password</td> <td>●●●●●●●●</td> </tr> <tr> <td>MTU</td> <td>1400</td> </tr> <tr> <td>Authentication Type:</td> <td>PAP <input type="button" value="v"/></td> </tr> <tr> <td>MPPE Encryption Level:</td> <td>None <input type="button" value="v"/></td> </tr> <tr> <td>PPTP IP Address Mode</td> <td>Dynamic <input type="button" value="v"/></td> </tr> <tr> <td>Physical IP Address Mode</td> <td>Dynamic <input type="button" value="v"/></td> </tr> <tr> <td>DNS Mode</td> <td>Dynamic <input type="button" value="v"/></td> </tr> <tr> <td colspan="2"><b>MAC Address Cloning</b></td> </tr> <tr> <td><input type="checkbox"/> Clone PC's MAC</td> <td></td> </tr> <tr> <td>Clone MAC Address</td> <td><input type="text"/></td> </tr> <tr> <td>Clone IP Address</td> <td><input type="button" value="v"/></td> </tr> </table> <p style="text-align: center;"> <input type="button" value="Apply"/> <input type="button" value="Cancel"/> </p>		Server Information	IP address <input type="button" value="v"/>	PPTP Server IP Address	172.1.1.1	PPTP Server URL Address	pptp_server	User Name	pptp_user	Password	●●●●●●●●	MTU	1400	Authentication Type:	PAP <input type="button" value="v"/>	MPPE Encryption Level:	None <input type="button" value="v"/>	PPTP IP Address Mode	Dynamic <input type="button" value="v"/>	Physical IP Address Mode	Dynamic <input type="button" value="v"/>	DNS Mode	Dynamic <input type="button" value="v"/>	<b>MAC Address Cloning</b>		<input type="checkbox"/> Clone PC's MAC		Clone MAC Address	<input type="text"/>	Clone IP Address	<input type="button" value="v"/>
Server Information	IP address <input type="button" value="v"/>																														
PPTP Server IP Address	172.1.1.1																														
PPTP Server URL Address	pptp_server																														
User Name	pptp_user																														
Password	●●●●●●●●																														
MTU	1400																														
Authentication Type:	PAP <input type="button" value="v"/>																														
MPPE Encryption Level:	None <input type="button" value="v"/>																														
PPTP IP Address Mode	Dynamic <input type="button" value="v"/>																														
Physical IP Address Mode	Dynamic <input type="button" value="v"/>																														
DNS Mode	Dynamic <input type="button" value="v"/>																														
<b>MAC Address Cloning</b>																															
<input type="checkbox"/> Clone PC's MAC																															
Clone MAC Address	<input type="text"/>																														
Clone IP Address	<input type="button" value="v"/>																														
<b>Server Information</b>	Select IP address or URL address form the pull-down menu.																														
<b>PPTP Server IP Address</b>	Enter the PPTP Server IP Address in this column.																														
<b>PPTP Server URL Address</b>	Enter the PPTP Server URL Address in this column.																														
<b>User Name</b>	Maximum input is 20 alphanumeric characters (case sensitive).																														
<b>Password</b>	Maximum input is 20 alphanumeric characters (case sensitive).																														
<b>MTU (Maximum Transmission Unit)</b>	Click the pull-down menu to select the most appropriate MTU (Maximum Transmission Unit, namely the maximum packet size, the default value is 1400) for your application. Reducing the packet size can help connecting to certain web sites or speeding up packet transfer rate. If the incorrect selection is entered, you may not be able to open certain web sites.																														

<b>Authentication Type</b>	Select PAP, CHAP, MSCHAP-v1, MSCHAP-v2 or Auto form the pull-down menu.
<b>MPPE Encryption Level</b>	When the authentication type has been set to be MSCHAP-v1, MSCHAP-v2 or Auto, here can select None, 40 bits, 56bits, 128bits or Auto form the pull-down menu.
<b>PPTP IP Address Mode</b>	Select Dynamic or Static for the pull-down menu.
<b>Physical IP Address Mode</b>	Select Dynamic or Static for the pull-down menu.
<b>DNS mode</b>	Select from the pull-down menu for Static or Dynamic DNS mode.
<b>Clone PC's MAC Address</b>	Check to enable this function.
<b>Clone MAC Address</b>	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.
<b>Clone IP Address</b>	Shows the IP address of the device from the pull-down menu.
<b>Apply</b>	Click to save and apply the current settings.
<b>Cancel</b>	Click to discard the current settings.

# LAN (Local Area Network) Settings

## Local Area Network (LAN) Settings

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

LAN Interface Setup	
IP Address	<input type="text" value="10.10.10.254"/>
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="10.10.10.100"/>
DHCP End IP	<input type="text" value="10.10.10.200"/>
DHCP Subnet Mask	<input type="text" value="255.255.255.0"/>
DHCP Lease Time	<input type="text" value="86400"/>
IGMP proxy	Disable <input type="button" value="v"/>

LAN Interface Setup	
<b>IP Address</b>	Shows the IP address of the router.
<b>Subnet Mask</b>	The subnet mask of the router.
<b>DHCP Type</b>	<p><b>Disable:</b> Select to disable this Router to distribute IP addresses.</p> <p><b>Server:</b> Select to enable this Router to distribute IP Addresses (DHCP Server). And the following field will be activated for you to enter the starting IP Address.</p>
<b>DHCP Start IP</b>	The starting address of this local IP network address pool.
<b>DHCP End IP</b>	The ending address of this local IP network address pool.
<b>DHCP Subnet Mask</b>	Shows the DHCP subnet mask.
<b>DHCP Lease Time</b>	Default settings are 86400 seconds.
<b>IGMP Proxy</b>	Select Disable or Enable from the pull-down menu.
<b>Apply</b>	Click to save and apply the current settings.
<b>Refresh</b>	Click to get the latest information.

# DHCP Clients

## DHCP Client List

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

DHCP Clients		
MAC Address	IP Address	Expires in
00:0C:43:28:60:E1	10.10.10.100	00:00:00

DHCP Clients	
<b>MAC Address</b>	Shows the client MAC address information.
<b>IP Address</b>	Shows the client IP address information.
<b>Expires in</b>	Shows the expired time of the client.


# WIRELESS SETTINGS

## Basic

### Basic Wireless Settings

This page is used to 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)	Untitled
Multiple SSID1	<input type="text"/>
Multiple SSID2	<input type="text"/>
Multiple SSID3	<input type="text"/>
Multiple SSID4	<input type="text"/>
Multiple SSID5	<input type="text"/>
Multiple SSID6	<input type="text"/>
Broadcast Network Name (SSID)	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
BSSID	000C432860E0
Frequency (Channel)	2437MHz (Channel 6) ▾
Wireless Distribution System(WDS)	
WDS Mode	Disable ▾
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	2457MHz (Channel 10) ▾
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
Other	
HT TxStream	2 ▾
HT RxStream	2 ▾

Wireless Network	
<b>Radio On/Off</b>	Click <b>Radio OFF</b> button to turn off the radio function.
<b>Network Mode</b>	Select 11 b/g mixed mode, 11b only, 11g only or 11 b/g/n mixed mode from the pull-down menu. (Default is 11 b/g/n mixed mode.)
<b>Network Name (SSID)</b>	A SSID is referred to a network name because essentially it is a name that identifies a wireless network. (Default SSID is Untitled.)
<b>Multiple SSID 1~6</b>	A multiple SSID is referred to a network name because essentially it is a name that identifies a wireless network.
<b>Broadcast Network Name(SSID)</b>	<b>Enable:</b> This wireless AP will broadcast its SSID to stations. <b>Disable:</b> 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.
<b>BSSID</b>	Shows the MAC address of the router.
<b>Frequency (Channel)</b>	Select 1~11 or Auto Select from the pull-down menu.
Wireless Distribution System (WDS)	
<b>WDS Mode</b>	<p>Select the mode from the pull-down menu, <b>Disable, Lazy Mode, Bridge Mode or Repeater Mode.</b> (Default WDS mode is Disable.)</p> <p>If the users would like to set up the WDS function, the APs should use the same <b>SSID</b> and <b>Channel</b> then enter <b>Wireless MAC</b> of each other to make the WDS connection.</p> <p><b>Step 1:</b> Setup the same SSID and Channel on both wireless APs.</p>  <p><b>Step 2:</b> Enter <b>Wireless MAC</b> address to each other.</p>

### Lazy Mode

If Lazy mode be selected, only set up Wireless MAC address on the other wireless AP then WDS function will be active.

Wireless Distribution System(WDS)	
WDS Mode	Lazy Mode
EncrypType	NONE

### Bridge Mode

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

Wireless Distribution System(WDS)	
WDS Mode	Bridge Mode
EncrypType	NONE
AP MAC Address	00:e0:98:30:02:83
AP MAC Address	
AP MAC Address	
AP MAC Address	

### Repeater Mode

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

Wireless Distribution System(WDS)	
WDS Mode	Repeater Mode
EncrypType	NONE
AP MAC Address	00:e0:98:30:02:83
AP MAC Address	
AP MAC Address	
AP MAC Address	

**Encryption Type:** There are only **Lazy, Bridge, Repeater** modes support encryption. Select **NONE, WEP, TKIP** and **AES** from pull-down menu. (Default encryption type is NONE.)

**WEP:** Users should go to the main web page of the wireless router **Status > Wireless settings > Security** page to set up WEP encryption under OPEN, SHARED, WEP AUTO security.

If select Hex users should use hexadecimal numbers (0-9, or A-F). Select ASCII if use ASCII characters (case-sensitive).

- **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><b>TKIP/AES:</b></p> <p>If users select TKIP or AES encryption, please enter the password in the Encryption Key column that must be filled with characters longer than 1 and less than 64 lengths to set up the security.</p> <table border="1"> <tr> <td>EncrypType</td> <td>TKIP ▼</td> </tr> <tr> <td>Encryp Key</td> <td>0</td> </tr> <tr> <td>EncrypType</td> <td>AES ▼</td> </tr> <tr> <td>Encryp Key</td> <td>0</td> </tr> </table>	EncrypType	TKIP ▼	Encryp Key	0	EncrypType	AES ▼	Encryp Key	0
EncrypType	TKIP ▼								
Encryp Key	0								
EncrypType	AES ▼								
Encryp Key	0								
<b>HT Physical Mode</b>									
<b>Operating Mode</b>	Select Mixed Mode or Green Field. (Default operating mode is Mixed Mode.)								
<b>Channel Band Width</b>	Select 20 or 20/40. (Default setting is 20/40.)								
<b>Guard Interval</b>	Select Long or Auto. (Default setting is Auto.)								
<b>MCS</b>	Select form the pull-down menu 0~15, 32 or Auto. (Default setting is Auto.)								
<b>Reverse Direction Grant(RDG)</b>	Select Disable or Enable this function. (Default setting is Enable.)								
<b>Extension Channel</b>	You can select 2457MHz (Channel 10) or 2417MHz (Channel 2) form the pull-down menu.								
<b>Aggregation MSDU (A-MSDU)</b>	Select Disable or Enable. (Default setting is Disable.)								
<b>Auto Block ACK</b>	Select Disable or Enable. (Default setting is Enable.)								
<b>Decline BA Request</b>	Select Disable or Enable. (Default setting is Disable.)								
<b>Other</b>									
<b>HT Tx Stream</b>	Select 1 or 2 form the pull-down menu.								
<b>HT Rx Stream</b>	Select 1 or 2 form the pull-down menu.								
<b>Apply</b>	Click to save and apply the current settings.								
<b>Cancel</b>	Click to discard the current settings.								



# Advanced

## Advanced Wireless Settings

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

Advanced Wireless	
BG Protection Mode	Auto ▾
Basic Data Rates	Default(1-2-5.5-11 Mbps) ▾
Beacon Interval	100 ms (range 20 - 999, default 100)
Data Beacon Rate (DTIM)	1 ms (range 1 - 255, default 1)
Fragment Threshold	2346 (range 256 - 2346, default 2346)
RTS Threshold	2347 (range 1 - 2347, default 2347)
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
IGMP Snooping	<input type="radio"/> Enable <input checked="" 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
WMM Parameters	WMM Configuration

Advanced Wireless	
<b>BG Protection Mode</b>	Select <b>Auto</b> , <b>On</b> or <b>Off</b> from the pull-down menu.
<b>Basic Data Rates</b>	By default, the unit adaptively selects the highest possible rate for transmission. Select the basic rates to be used among the following options: 1-2Mbps, Default (1-2-5.5-11Mbps), or All(1-2-5,5-6-11-12-24Mbps.)
<b>Beacon Interval</b>	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.)
<b>Data Beacon Rate (DTIM)</b>	Range from 1 to 255. (Default data beacon rate is 1.)

<b>Fragment Threshold</b>	Fragmentation mechanism is used for improving the efficiency when high traffic flows along in the wireless network. If the 802.11g MIMO Wireless Router often transmit large files in wireless network, you can enter new Fragment Threshold value to split the packet. The value can be set from 256 to 2346. (The default value is <b>2346</b> .)
<b>RTS Threshold</b>	<p>RTS Threshold is a mechanism implemented to prevent the “<b>Hidden Node</b>” problem. If the “Hidden Node” problem is an issue, please specify the packet size. <i>The RTS mechanism will be activated if the data size exceeds the value you set.</i> (The default value is <b>2347</b>.)</p> <p><b>Warning:</b> 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 <b>2347</b>. Should you encounter inconsistent data flow, only minor modifications of this value are recommended.</p>
<b>Short Preamble</b>	Select Disable or Enable this function. (Default setting is <b>Disable</b> .) A preamble is a signal used in wireless environment to synchronize the transmitting timing including Synchronization and Start frame delimiter.
<b>Short Slot</b>	Select Disable or Enable this function. (Default short slot setting is Enable.)
<b>Tx Burst</b>	Select Disable or Enable this function. (Default Tx Burst setting is Enable.)
<b>Pkt_Aggregate</b>	Select Disable or Enable this function. (Default setting is Enable.)
<b>IGMP Snooping</b>	Select Disable or Enable this function. (Default setting is Disable.)
<b>Wi-Fi Multimedia</b>	
<b>WMM Capable</b>	Select Disable or Enable this function. (Default setting is Enable.)
<b>APSD Capable</b>	Select Disable or Enable this function. (Default setting is Disable.)
<b>WMM Parameters</b>	Click the <b>WMM Configuration</b> button to go further settings.
<b>Apply</b>	Click to save and apply the current settings.
<b>Cancel</b>	Click to discard the current settings.

# Security

## Wireless Security Settings

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.

Select SSID	
SSID choice	Untitled ▾
Security Mode -- "Untitled"	
Security Mode	Disable ▾

Select SSID	
<b>SSID choice</b>	Select the SSID form the pull-down menu for security settings.
<b>Security Mode</b>	<p>There are eleven type of authentication modes including <b>Disable, Open, Shared, WEP Auto, WPA, WPA-PSK, WPA2, WPA2-PSK, WPA-PSK/WPA2-PSK, WPA/WPA2 and 802.1X.</b></p> <ul style="list-style-type: none"> <li>• <b>Open:</b> If your wireless router is using "Open" authentication, then the wireless adapter will need to be set to the same authentication type.</li> <li>• <b>Shared:</b> Shared key is when both the sender and the recipient share a secret key.</li> <li>• <b>WPA, WPA-PSK, WPA2, WPA2-PSK, WPA-PSK/WPA2-PSK, and WPA1/WPA2:</b> WPA-PSK offers two encryption methods, TKIP and AES. Select the type of algorithm, TKIP or AES and then enter a WPA Shared Key of 8~64 characters in the WPA Pre-shared Key field.</li> </ul> <p><b>Encryption Type:</b> For <b>Open</b> and <b>Shared</b> authentication mode, the selection of encryption type are <b>None</b> and <b>WEP</b>. For <b>WPA, WPA2, WPA-PSK</b> and <b>WPA2-PSK</b> authentication mode, the encryption type supports both <b>TKIP</b> and <b>AES</b>.</p> <p><b>WPA Pre-shared Key:</b> This is the shared secret between AP and STA. For WPA-PSK and WPA2-PSK authentication mode, this field must be filled with character longer than 8 and less than 64 lengths.</p> <p><b>WEP Key:</b> Only valid when using WEP encryption algorithm. The key must match with the AP's key. There are several formats to enter the keys.</p> <ul style="list-style-type: none"> <li>• <b>Hexadecimal (WEP 64 bits):</b> 10 Hex characters (0~9,</li> </ul>

	<p>a~f).</p> <ul style="list-style-type: none"> <li>● <b>Hexadecimal (WEP 128 bits):</b> 26 Hex characters (0~9, a~f).</li> <li>● <b>ASCII (WEP 64 bits):</b> 5 ASCII characters (case-sensitive).</li> <li>● <b>ASCII (WEP 128 bits):</b> 13 ASCII characters (case-sensitive).</li> </ul>
<b>WPA Algorithms</b>	Select TKIP, AES or TKIP/AES for the WPA Algorithms.
<b>Enable Pre-Authentication</b>	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.
<b>RADIUS Server</b>	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.
<b>IP Address</b>	Enter the RADIUS Server's IP Address provided by your ISP.
<b>Port</b>	Enter the RADIUS Server's port number provided by your ISP. (The default is <b>1812</b> .)
<b>Shared Secret</b>	Enter the password that the router shares with the RADIUS Server.
<b>Apply</b>	Click to save and apply the current settings.
<b>Cancel</b>	Click to discard the current settings.

# WPS

## Wi-Fi Protected Setup

This page is used to setup security easily by choosing PIN or PBC method to do Wi-Fi Protected Setup.

WPS Config	
WPS:	Enable ▾
<input type="button" value="Apply"/>	

WPS Summary	
WPS Current Status:	Idle
WPS Configured:	No
WPS SSID:	Untitled
WPS Auth Mode:	Open
WPS Encrypt Type:	None
WPS Default Key Index:	1
WPS Key(ASCII)	
AP PIN:	26462400
<input type="button" value="Reset OOB"/>	

WPS Progress	
WPS mode	<input checked="" type="radio"/> PIN <input type="radio"/> PBC
PIN	<input type="text"/>
<input type="button" value="Apply"/>	

WPS Status	
WSC: Idle	

WPS Configuration	
<b>WPS</b>	Select Enable or Disable from the pull-down menu.
<b>Apply</b>	Click to save and apply the current settings.
<b>WPS Summary</b>	Here shows the WPS function status.
<b>Reset OOB</b>	Click the button to reset the settings.
WPS Process	
<b>WPS mode</b>	Select PCB or PIN WPS mode.
<b>PIN</b>	Enter the PIN code form the registrar or enrollee.
<b>Apply</b>	Click to save and apply the current settings.
<b>WPS Status</b>	Here shows the current status of the WPS function.

# Trusted Stations

## Trusted Stations Settings

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

---

Select SSID	
SSID choice	Untitled ▾

---

Trusted Stations Policy -- "Untitled"	
Trusted Stations Policy	Disable ▾
Station MAC Address	<input type="text"/>

---

Current Trusted Stations rules		
No.	Station Address	Status

Select SSID	
<b>SSID choice</b>	Select the SSID from the pull-down menu.
Trusted Stations Policy	
<b>Trusted Stations Policy</b>	Select Disable, Enable –Rules for DROP, or Enable –Rules for ACCEPT form the pull-down menu.
<b>Station MAC Address</b>	Enter the MAC address of the station.
<b>Apply</b>	Click to save and apply the current settings.
<b>Reset</b>	Press to discard the current settings.
<b>Current Trusted Stations rules</b>	Here shows the information of the trusted stations clients.
<b>Delete Selected</b>	Select the unwanted trusted station MAC addresses and then click the Delete Selected button to eliminate them.
<b>Delete All</b>	Click to delete all the trusted station MAC addresses in the table.
<b>Reset</b>	Click to clear the current settings.

# Station List

Here shows the information of stations that connected with the AP.

## Wireless Stations List

This page is used to monitor stations which associated to this AP here.

Active Clients						
MAC Address	Tx Rate(Mbps)	MCS	BW	PhyMode	WMM	PSM
00:12:0E:28:70:45	54M	15	40M	HTMIX	Yes	No

# FIREWALL

## MAC Filtering

### MAC Filtering Settings

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.

MAC Filter Settings	
MAC Filtering	Disable <input type="button" value="v"/>
MAC Address	<input type="text"/>
Comment	<input type="text"/>

Current MAC filtering rules:			
No.	MAC Address	Status	Comment

MAC Filtering Settings	
<b>MAC Filtering</b>	Select Disable, enable –Rules for DROP, or enable –Rules for ACCEPT form the pull-down menu.
<b>MAC Address</b>	Enter the client MAC address.
<b>Comment</b>	You may key in a description for the MAC address.
<b>Apply</b>	Click to save and apply the current settings.
<b>Reset</b>	Press to discard the current settings.
<b>Current MAC filtering rules</b>	Here shows the information of the MAC filtering clients.
<b>Delete Selected</b>	Select the unwanted MAC addresses and then click the Delete Selected button to eliminate them.
<b>Delete All</b>	Click to delete all the MAC addresses in the table.
<b>Reset</b>	Click to clear the current settings.



# Access Control

## Access Control Settings

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. Default policy defines the packet that don't match with any rules would use default policy to drop or accept the rest of packets

Basic Settings	
Access Control	Disable ▾
Default Policy -- The packet that don't match with any rules would be:	Accepted ▾
<input type="button" value="Apply"/> <input type="button" value="Reset"/>	

Access Control Settings			
Source IP Address	<input type="text"/>	Port Range	<input type="text"/> - <input type="text"/>
Dest IP Address	<input type="text"/>	Port Range	<input type="text"/> - <input type="text"/>
Protocol	TCP&UDP ▾		
Action	Drop ▾		
Comment	<input type="text"/>		
<input type="button" value="Apply"/> <input type="button" value="Reset"/>			

Current Access Control rules:							
No.	Source IP Address	Source Port Range	Dest IP Address	Dest Port Range	Protocol	Action	Comment
<input type="button" value="Delete Selected"/> <input type="button" value="Delete All"/> <input type="button" value="Reset"/>							

Basic Settings	
<b>Access Control</b>	Select Disable or Enable from the pull-down menu.
<b>Default Policy -- The packet that don't match with any rules would be:</b>	Select Accepted or Dropped from the pull-down menu.
<b>Apply</b>	Click to save and apply the current settings.
<b>Reset</b>	Press to discard the current settings.
Access Control Settings	
<b>Source IP Address</b>	Enter the client IP address.
<b>Dest IP Address</b>	Enter the destined IP address.

<b>Port Range</b>	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.
<b>Protocol</b>	Select the protocol (TCP, UDP or TCP&UDP) used to the remote system or service.
<b>Action</b>	Select Drop or Accept from the pull-down menu.
<b>Comment</b>	You may key in a description for the local IP address
<b>Apply</b>	Click to save and apply the current settings.
<b>Reset</b>	Press to discard the current settings.
<b>Current Access Control rules</b>	Here shows the information of the Access Control clients.
<b>Delete Selected</b>	Select the unwanted IP addresses and then click the Delete Selected button to eliminate them.
<b>Delete All</b>	Click to delete all the IP addresses in the table.
<b>Reset</b>	Click to clear the current settings.

## URL Filtering

### URL Filtering Settings

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

URL Filter Settings	
URL Filtering	Disable <input type="button" value="v"/>
URL String	<input type="text"/>
Comment	<input type="text"/>

Current URL filtering rules:		
No.	URL String	Comment

URL Filter Settings	
<b>URL Filtering</b>	Select Disable or Enable from the pull-down menu.
<b>URL String</b>	You can block websites with specific URL addresses.
<b>Comment</b>	You may key in a description for the URL address.
<b>Apply</b>	Click to save and apply the current settings.
<b>Reset</b>	Press to discard the current settings.
<b>Current URL filtering rules</b>	Shows the current URL address status.
<b>Delete Selected</b>	Select the unwanted URL addresses and then click the Delete Selected button to eliminate them.
<b>Delete All</b>	Click to delete all the URL addresses in the table.
<b>Reset</b>	Click to clear the current settings.

## Port Trigger

### Port Trigger Settings

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 Range" 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.

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

Current Port Trigger list:					
No.	Incoming Protocol	Incoming Port Range	Trigger Protocol	Trigger Port Range	Comment
<input type="button" value="Delete Selected"/> <input type="button" value="Delete All"/> <input type="button" value="Reset"/>					

<b>Port Trigger Settings</b>	
<b>Port Trigger Settings</b>	Select Disable or Enable from the pull-down menu.
<b>Incoming Protocol</b>	Select the protocol (TCP, UDP or TCP&UDP) used to the remote system or service.
<b>Incoming Port Range</b>	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.
<b>Trigger Protocol</b>	Select the protocol (TCP, UDP or TCP&UDP) used to the remote system or service.
<b>Trigger Port Range</b>	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.
<b>Comment</b>	You may key in a description for the port trigger.
<b>Current Port Trigger list</b>	Shows the current Port Trigger status.
<b>Delete Selected</b>	Select the unwanted URL addresses and then click the Delete Selected button to eliminate them.
<b>Delete All</b>	Click to delete all the URL addresses in the table.
<b>Reset</b>	Click to clear the current settings.

# Virtual Server

## Virtual Server Settings

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.

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"/>

Current Virtual Servers list:				
No.	IP Address	Port Range	Protocol	Comment
<input type="button" value="Delete Selected"/> <input type="button" value="Delete All"/> <input type="button" value="Reset"/>				

Virtual Server Settings	
<b>Virtual Server Settings</b>	Select Enable or Disable from the pull-down menu.
<b>IP Address</b>	Enter the local server's IP address.
<b>Port Range</b>	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.
<b>Protocol</b>	Select the protocol (TCP, UDP or TCP&UDP) used to the remote system or service.
<b>Comment</b>	You may key in a description for the IP address.
<b>Apply</b>	Click to save and apply the current settings.
<b>Reset</b>	Press to discard the current settings.
<b>Delete Selected</b>	Select the unwanted IP addresses and then click the Delete Selected button to eliminate them.
<b>Delete All</b>	Click to delete all the IP addresses in the table.
<b>Reset</b>	Click to clear the current settings.

# DMZ

## DMZ Settings

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 Settings	
DMZ Settings	Disable ▾
DMZ IP Address	<input type="text"/>

DMZ Settings	
<b>DMZ Settings</b>	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.
<b>DMZ IP Address</b>	Enter the IP address of a particular host in your LAN that will receive all the packets originally going to the WAN port/ Public IP address above. <b>Note: You need to give your LAN PC clients a fixed/ static IP address for DMZ to work properly.</b>
<b>Apply</b>	Click to save and apply the current settings.
<b>Reset</b>	Press to discard current settings.

# Denial of Service

## Denial of Service Settings

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

<input type="checkbox"/> Whole System Flood: SYN	<input type="text" value="50"/>	Packets/Second
<input type="checkbox"/> Whole System Flood: FIN	<input type="text" value="50"/>	Packets/Second
<input type="checkbox"/> Whole System Flood: UDP	<input type="text" value="50"/>	Packets/Second
<input type="checkbox"/> Whole System Flood: ICMP	<input type="text" value="50"/>	Packets/Second
<input type="checkbox"/> Per-Source IP Flood: SYN	<input type="text" value="50"/>	Packets/Second
<input type="checkbox"/> Per-Source IP Flood: FIN	<input type="text" value="50"/>	Packets/Second
<input type="checkbox"/> Per-Source IP Flood: UDP	<input type="text" value="50"/>	Packets/Second
<input type="checkbox"/> Per-Source IP Flood: ICMP	<input type="text" value="50"/>	Packets/Second
<input type="checkbox"/> TCP/UDP PortScan		
<input type="checkbox"/> ICMP Smurf		
<input type="checkbox"/> IP Land		
<input type="checkbox"/> IP Spoof		
<input type="checkbox"/> IP TearDrop		
<input type="checkbox"/> PingOfDeath		
<input type="checkbox"/> TCP Scan		
<input type="checkbox"/> TCP SynWithData		
<input type="checkbox"/> UDP Bomb		
<input type="checkbox"/> UDP EchoChargen		

Denial of Service Settings	
<b>Enable DoS Prevention</b>	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. Check the box to enable the DoS settings.
<b>Select All</b>	After you enabled the DoS prevention, you can click to select all DoS preventions.
<b>Clear All</b>	After you enabled the DoS prevention, you can click to uncheck all DoS preventions.
<b>Apply</b>	Click to enable selected DoS preventions.

# ADMINISTRATION

## User/ Password

### System Account Management

You may configure administrator account and password here.

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

Administrator Settings	
<b>Account</b>	Enter the user name for managing this device. Maximum Input is 16 alphanumeric characters.
<b>Password</b>	Enter the passwords for managing this device.
<b>Apply</b>	Click to save and apply the current settings.
<b>Cancel</b>	Click to discard the current settings.



# Time Zone Setting

## Time Zone Management

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

Current Time: Saturday, January 01 2000 | AM 3:43:55

Enable NTP Client

Time Zone Select (GMT+08:00) Taipei

NTP Servers

Auto Selection  NTP Server at UK

Manual IP  140.130.175.9

Daylight Saving

Start Month JAN Day 1

End Month FEB Day 1

Save Refresh Smart Update

Time Zone Management	
<b>Current Time</b>	Here shows the current time information.
<b>Enable NTP Client</b>	Check the box to enable below time zone settings.
<b>Time Zone Select</b>	Select the preferred time zone from the pull-down menu.
<b>NTP Servers</b>	<b>Auto Selection:</b> Select Auto Selection to choose the server automatically. <b>Manual IP:</b> Enter an IP address of a specific server.
<b>Daylight Saving</b>	Check the box to enable this function, select start and end date from the pull-down menu.
<b>Save</b>	Click to save the current settings.
<b>Refresh</b>	Click to renew the current settings.
<b>Smart Update</b>	Click to update the current time information.

# System Log

## System Log Management

You may Set or Show various system log messages here.

---

Enable Log  
 System all  802.1X only

System Log Management	
<b>Enable Log</b>	Check the box to enable this function.
<b>System all</b>	Check to show all system related log files.
<b>802.1X only</b>	Check to show 802.1X log file only.
<b>Apply Changes</b>	Click this button to save the settings.
<b>Refresh</b>	Click to renew the current log message.
<b>Clear</b>	Click to remove current log message.

# DDNS

## DDNS Management

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.

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

DDNS Settings	
<b>Dynamic DNS Provider</b>	<ul style="list-style-type: none"> <li>Select the desired DDNS Service Provider <b>None, Dyndns.org, www.zoneedit.com, or www.no-ip.com</b> from the pull-down list.</li> <li>Details of your DDNS account (Name, password, Domain name) must then be entered and saved on this screen.</li> <li>This device will then automatically ensure that your current IP Address is recorded by the DDNS Service Provider.</li> <li>From the Internet, users will now be able to connect to your Virtual Servers (or DMZ PC) using your Domain name.</li> </ul>
<b>Account</b>	Enter the user name for managing this device.
<b>Password</b>	Enter the password for managing this device.
<b>DDNS</b>	Apply for a Domain Name, and ensure it is allocated to you.
<b>Result</b>	The result of the update DNS result will show here.
<b>Apply</b>	Click to save and apply the current settings.
<b>Cancel</b>	Click to discard the current settings.
<b>Refresh</b>	Click to refresh the settings.

# Upload Firmware

## Upgrade Firmware

This page allows you to upgrade this device'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 device during this process because it may crash the system.

---

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

Update Firmware	
<b>Location</b>	Click the <b>Browse</b> button, find and open the firmware file (the browser will display to correct file path).
<b>Apply</b>	Click the Apply button to perform.
<b>Reset</b>	Click Reset to restore to default values.

# Settings Management

## Settings Management

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

Export Settings	
Export Button	<input type="button" value="Export"/>

Import Settings	
Settings file location	<input type="text"/> <input type="button" value="Browse..."/>
<input type="button" value="Import"/>	<input type="button" value="Cancel"/>

Load Factory Defaults	
Load Default Button	<input type="button" value="Load Default"/>

Export Settings	
<b>Export Button</b>	Click the <b>Export</b> button to export the current device settings.
Import Settings	
<b>Settings file location</b>	Click the <b>Browse</b> button, find and open the file that has been saved before. (The browser will display to correct file path).
<b>Import</b>	Click the <b>Import</b> button to import the device settings.
<b>Cancel</b>	Click to discard the current settings.
Load Factory Defaults	
<b>Load Default Button</b>	Click to <b>Load Default</b> button to set the device back to factory default settings.

# Statistics

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

## Statistic

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

Memory	
Memory total:	28196 kB
Memory left:	18640 kB
WAN	
WAN Rx packets:	0
WAN Rx bytes:	0
WAN Tx packets:	282
WAN Tx bytes:	167508
LAN	
LAN Rx packets:	15476
LAN Rx bytes:	2174210
LAN Tx packets:	3852
LAN Tx bytes:	1735742
WLAN	
WLAN Rx packets:	18585
WLAN Rx bytes:	2651936
WLAN Tx packets:	0
WLAN Tx bytes:	7085096

# CHAPTER 4:

# PC CONFIGURATION

## OVERVIEW

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

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

## WINDOWS CLIENTS

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

## TCP/IP Settings - Overview

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

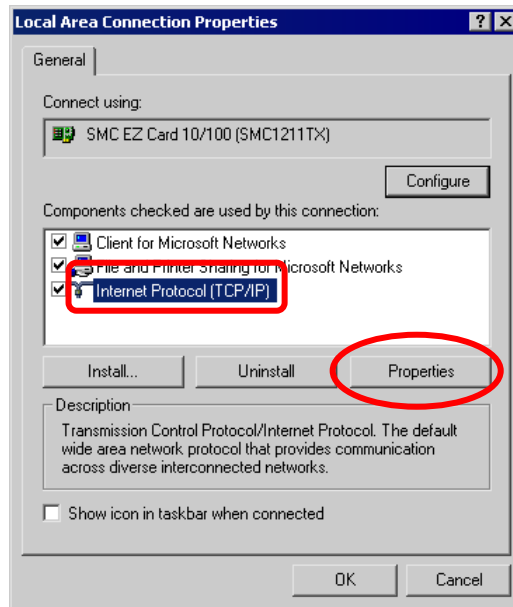
- By default, the Wireless Router will act as a DHCP Server, automatically providing a suitable IP Address (and related information) to each PC when the PC boots.
- For all non-Server versions of Windows, the default TCP/IP setting is to act as a DHCP client.

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

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

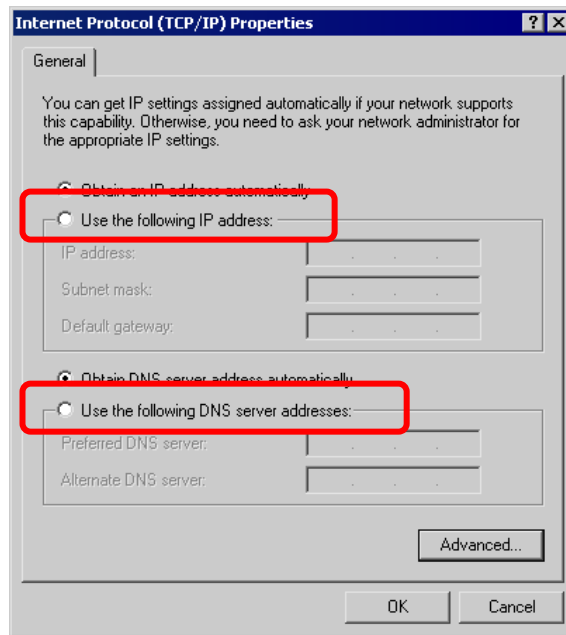
## Checking TCP/IP Settings - Windows 2000

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



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

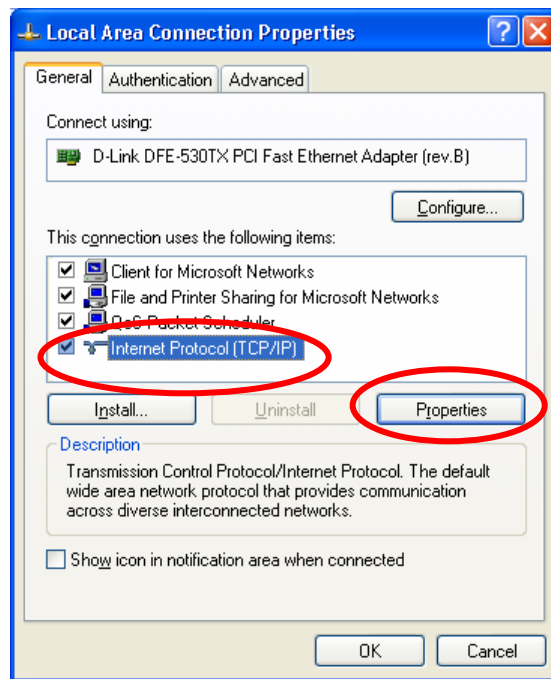
### Using a fixed IP Address ("Use the following IP Address")

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

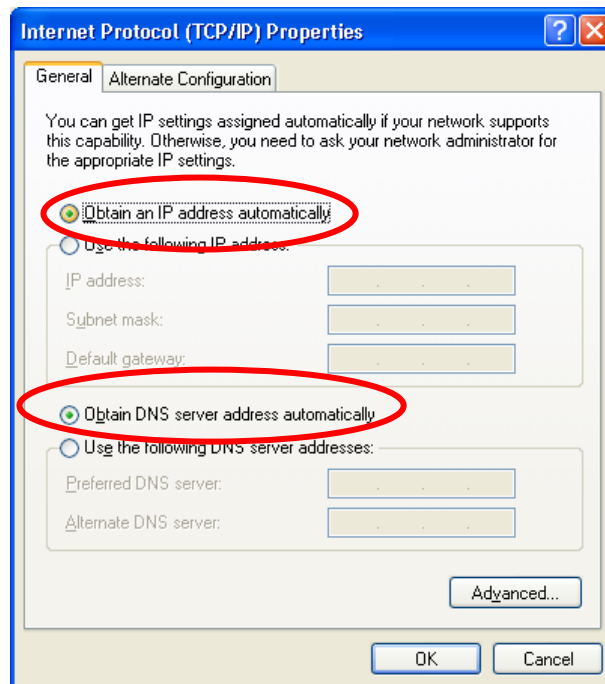
- Enter the Wireless Router's IP address in the *Default gateway* field and click *OK*. (Your LAN administrator can advise you of the IP Address they assigned to the Wireless Router.)
- If the *DNS Server* fields are empty, select *Use the following DNS server addresses*, and enter the DNS address or 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 *Obtain an IP Address automatically*. This is the default Windows setting. **Using this is recommended.** By default, the Wireless Router will act as a DHCP Server.
- Restart your PC to ensure it obtains an IP Address from the Wireless Router.

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

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

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

1. Start the *AOL for Windows* communication software. Ensure that it is Version 2.5, 3.0 or later. This procedure will not work with earlier versions.
2. Click the *Setup* button.
3. Select *Create Location*, and change the location name from "New Locality" to "Wireless Router."
4. Click *Edit Location*. Select *TCP/IP* for the *Network* field. (Leave the *Phone Number* blank.)
5. Click *Save*, then *OK*. Configuration is now complete.
6. 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 that is used on the client.
- To use the Wireless Station with Wireless Router, each Wireless Station must have compatible settings, as follows:

<b>Mode</b>	The mode must be set to <i>Infrastructure</i> .
<b>SSID (ESSID)</b>	This must match the value used on the Wireless Router. The default value is <b>Untitled</b> . <b>Note! The SSID is case sensitive.</b>
<b>WEP</b>	By default, the security setting on the Wireless Router is <b>Disabled</b> . <ul style="list-style-type: none"> <li>• If security setting remains disabled on the Wireless Router, all stations must have it disabled.</li> <li>• If security setting is enabled on the Wireless Router, each station must use the same settings as the Wireless Router.</li> </ul>
<b>WPA</b> <b>WPA2 (AES)</b> <b>WPA2 Mixed</b>	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

<b>Problem 1:</b>	<b>Can't connect to the Wireless Router to configure it.</b>
<b>Solution 1:</b>	<p>Check the following:</p> <ul style="list-style-type: none"><li>• The Wireless Router is properly installed, LAN connections are OK, and it is powered ON.</li><li>• 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.)</li><li>• If your PC is set to "Obtain an IP Address automatically" (DHCP client), restart it.</li><li>• If your PC uses a Fixed (Static) IP address, ensure that it is using an IP Address within the range 10.10.10.1 to 10.10.10.253 and thus compatible with the Wireless Router's default IP Address of 10.10.10.254.</li></ul> <p>Also, the Network Mask should be set to 255.255.255.0 to match the Wireless Router.</p> <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

<b>Problem 1:</b>	<b>When I enter a URL or IP address I get a time out error.</b>
<b>Solution 1:</b>	<p>A number of things could be causing this. Try the following troubleshooting steps.</p> <ul style="list-style-type: none"><li>• 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.</li><li>• 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.)</li><li>• If the Wireless Router is configured correctly, check your Internet connection (DSL/Cable modem etc) to see that it is working correctly.</li></ul>

<b>Problem 2:</b>	<b>Some applications do not run properly when using the Wireless Router.</b>
<b>Solution 2:</b>	<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. 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"> <li>• It is a security risk, since the firewall is disabled.</li> <li>• Only one (1) PC can use this feature.</li> </ul>

## WIRELESS ACCESS

<b>Problem 1:</b>	<b>My PC can't locate the Wireless Router.</b>
<b>Solution 1:</b>	<p>Check the following:</p> <ul style="list-style-type: none"> <li>• Your PC is set to <i>Infrastructure Mode</i>. (Access Points are always in <i>Infrastructure Mode</i>.)</li> <li>• The SSID on your PC and the Wireless Router are the same. Remember that the SSID is case-sensitive. So, for example "Workgroup" does NOT match "workgroup".</li> <li>• 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 setting disabled.</li> <li>• If security setting is enabled on the Wireless Router, your PC must have it enabled, and the password or key must match.</li> <li>• 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.</li> <li>• 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.</li> </ul>
<b>Problem 2:</b>	<b>Wireless connection speed is very slow.</b>
<b>Solution 2:</b>	<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"> <li>• <b>Wireless Router location.</b> Try adjusting the location and orientation of the Wireless Router.</li> <li>• <b>Wireless Channel.</b> If interference is the problem, changing to another channel may show a marked improvement.</li> <li>• <b>Radio Interference.</b> 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.</li> <li>• <b>RF Shielding.</b> 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.</li> </ul>



# 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.)

## SECURITY

Authentication methods include **Disable, Open, Shared, WEP Auto, WPA, WPA-PSK, WPA2, WPA2-PSK, WPA-PSK/WPA2-PSK, WPA1/WPA2 and 802.1X**. Once you choose your authentication, you then need to select the **Data Encryption** methods which may include **WEP Key, Pass Phrase** and **Radius Server** settings.

### Encryption

Enabling **WEP** can protect your data from eavesdroppers. There are two levels of WEP Encryption: 64 bits and 128 bits. 64 bits WEP encryption requires entering 10 Hex characters as a "secret key", whereas 128 bits WEP requires users to enter 26 Hex characters as "secret key".

**PASS PHRASE** is applicable only when you select to use WPA-PSK authentication. You will need to enter an 8~63 character password to kick off the encryption process, which will generate four WEP keys automatically.

**RADIUS** setup is used to set up additional parameters for authorizing wireless clients through RADIUS server. The **RADIUS** setup is required when you select to use **Open System with 802.1x** or **WPA/WPA2** authentication.

## Open, Shared, WEP auto

With **Shared Key** or **Open System**, the Wireless Router can automatically change its authentication method to **Shared Key** or **Open System** depending on its client's setting.

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 that 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:**

<b>WEP</b>	Off, 64 Bit, 128 Bit.
<b>Key</b>	For 64 Bit encryption, the Key value must match. For 128 Bit encryption, the Key value must match.
<b>WEP Authentication</b>	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
<b>TKIP</b>	<b>NOT REQUIRED</b>	<b>8-63 characters</b>
<b>AES</b>		

## 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:

<b>Mode</b>	On client Wireless Stations, the mode must be set to "Infrastructure." (The Access Point is always in "Infrastructure" mode.)
<b>SSID (ESSID)</b>	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).
<b>WEP</b>	The Wireless Stations and the Access Point must use the same settings for WEP (Off, 64 Bit, 128 Bit). <b>WEP Key:</b> If WEP is enabled, the Key must be the same on the Wireless Stations and the Access Point. <b>WEP Authentication:</b> If WEP is enabled, all Wireless Stations must use the same setting as the Access Point (either "Open System" or "Shared Key").
<b>WPA</b> <b>WPA2 (AES)</b> <b>WPA2 Mixed</b>	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.

# 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.