

# **802.11 b/g/n Giga Router**

User's Manual

# Federal Communication Commission

## Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications.

However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

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

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

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

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



### CAUTION:

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

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

# Table of Content

<b>CHAPTER 1: INTRODUCTION.....</b>	<b>1</b>
Features.....	1
Physical Details.....	1
<b>CHAPTER 2: ABOUT OPERATION MODES.....</b>	<b>4</b>
Operation Modes.....	4
Router Mode.....	4
Access Point Mode.....	5
Converter Mode.....	6
<b>CHAPTER 3: CONFIGURATION.....</b>	<b>7</b>
Hardware Connection.....	7
Login.....	7
Status.....	11
Network.....	12
Wireless.....	22
Firewall.....	34
Administration.....	41
<b>CHAPTER 4: PC CONFIGURATION.....</b>	<b>48</b>
Overview.....	48
Windows Clients.....	48
Macintosh Clients.....	56
Linux Clients.....	56
Other Unix Systems.....	57
Wireless Station Configuration.....	57
<b>APPENDIX A: TROUBLESHOOTING.....</b>	<b>59</b>
Overview.....	59
General Problems.....	59
Internet Access.....	59
Wireless Access.....	60
<b>APPENDIX B: ABOUT WIRELESS LANS.....</b>	<b>62</b>
BSS (Basic Service Set).....	62
Channels.....	62
Security.....	62
Wireless LAN Configuration.....	63

# Chapter 1: Introduction

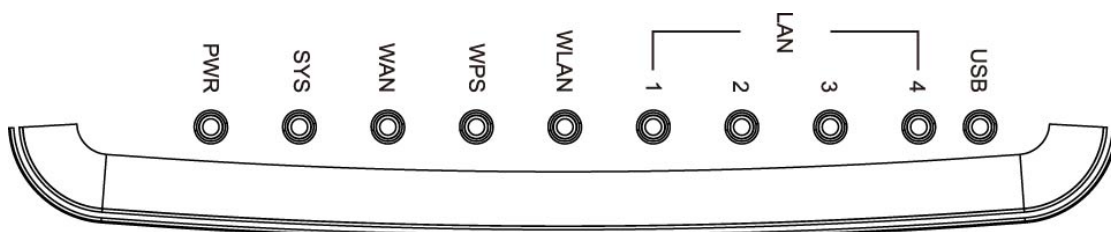
The 802.11b/g/n Wireless Giga Router supports 4 ports 10/100/1000M Ethernet for LAN and 1 port 10/100/1000M Ethernet interface for WAN. With the advanced MIMO technology, it can support the data transmission rate 6 times more (up to 300 Mbps) and the coverage 3 times more than IEEE 802.11b/g devices. The Wireless Router enables your whole network sharing a high-speed cable or DSL Internet connection. With it, you can share a high-speed Internet connection, files, printers, and multi-player games at incredible speeds, without the hassle of stringing wires. It also offers easy configuration for your wireless network at home and presents wireless network of high functionality, security, and flexibility.

## Features

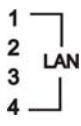
1. Support 4 ports 10/100/1000M Ethernet for LAN and 1 port 10/100/1000M Ethernet interface for WAN.
2. Clock rate up to 600MHz.
3. Support the IEEE 802.11n/b/g standard, high speed data rate up to 300Mbps, two transmit and two receive path(2T2R)
4. High security with build-in Security: WEP 64/128, WPA, WPA2, 802.1x and 802.11i.
5. Supports 1 additional USB port.
6. Supports WPS (Wi-Fi Protected Setup) with physical push button.
7. High security with build-in Security: WEP 64/128, WPA, WPA2, 802.1x and 802.11i.
8. Support Client, AP, WDS, AP+WDS mode.
9. Advanced Quality of Service (QoS), WMM.
10. Easy web browser configuration for home user setup.
11. Support USB Network attached storage (NAS) and media share function.

## Physical Details

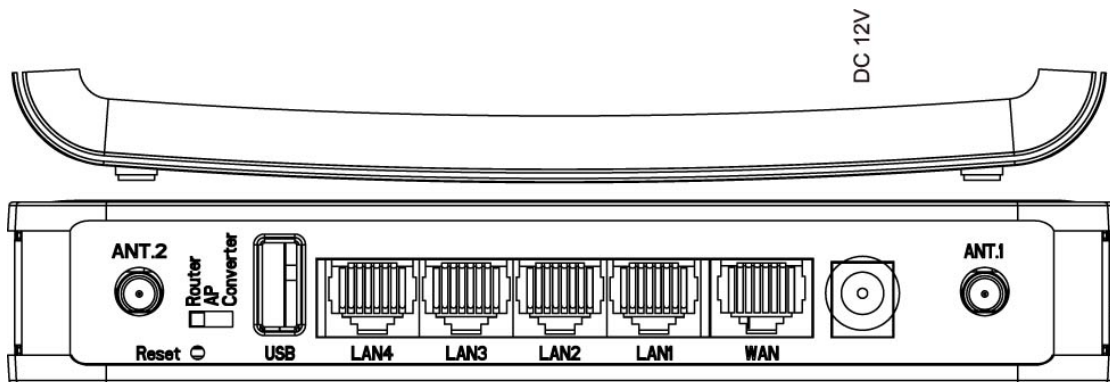
### Top LEDs



LED Behavior				
LED	Printed	Color	Behavior	Indication
Power	PWR	Green	ON	Power on
			OFF	Power off

Internet	WAN	Green	ON	Internet link / active
			OFF	Internet function off
			Blinking	Internet traffic transmitting
WPS	WPS	Green	ON	WPS setup successfully
			OFF	WPS is disabled
			Blinking	WPS is enabled to make a connection
Wireless LAN	WLAN	Green	OFF	WLAN off
			ON	WLAN link / active
			Blinking	WLAN traffic transmitting
LAN		Green	OFF	LAN function off
			ON	LAN link / active
			Blinking	LAN traffic transmitting
USB	WPS	Green	ON	USB is connected
			OFF	USB is disconnected

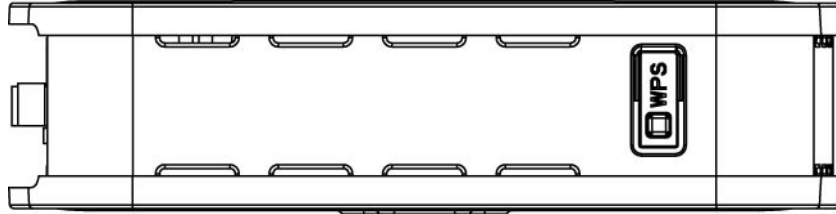
## Ports and Buttons



### Ports and buttons

Ant. 1 Ant. 2	Install the appending antennas here.
Reset	Keep on pressing the Reset button more than 3 seconds, the Wireless Router will set all setting back to factory default.
USB	Insert the USB 3.5G card that provided by your ISP (Internet Service Provider) or USB network attached storage here.
LAN 1-4	Use standard LAN cables (RJ45 connectors) to connect your PCs to this port. If required, any port can be connected to another hub. Any LAN port will automatically function as an "Uplink" port when necessary.

<b>WAN</b>	Connect the ADSL or Cable Modem here with RJ45 cable. If your modem came with a cable, use the supplied cable, otherwise, use a standard LAN cable (RJ45 connectors).
<b>DC 12V</b>	Connect the supplied power adapter here.



<b>WPS</b>	
<b>WPS</b>	To enable the WPS function press the physical WPS button on the Wireless Router once, then the LED will start to flash. Please make a connection with other WPS supported device within 2 minutes.

# Chapter 2: About Operation Modes

This device provides operational applications with Router, AP and Converter modes, which are mutually exclusive.

This device is shipped with configuration that is functional right out of the box. If you want to change the settings in order to perform more advanced configuration or even change the mode of operation, you can MANUALLY switch to the mode you desired by the manufacturer as described in the following sections.

## Operation Modes

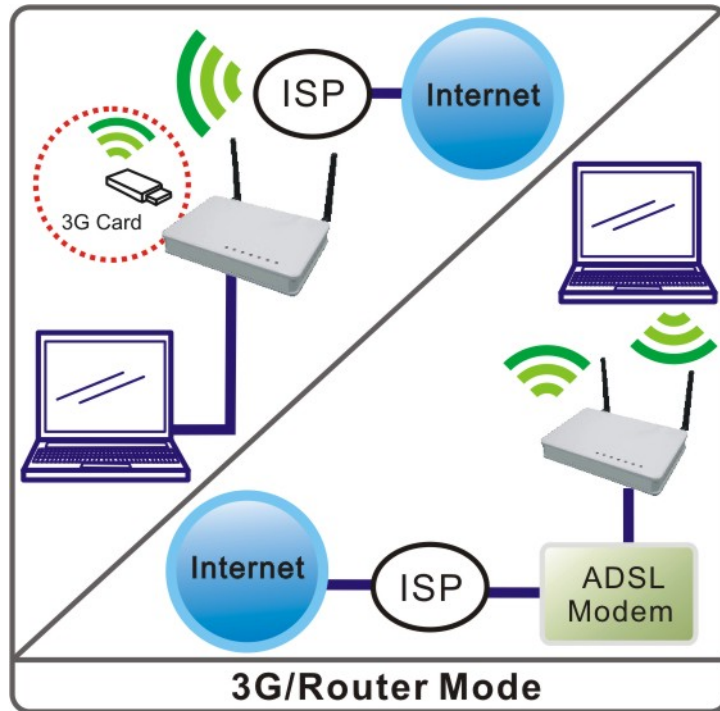
You have to MANUALLY switch the bar into the mode you preferred, Router, AP or Converter modes, then the device will reboot automatically into the mode you have selected.



## Router Mode

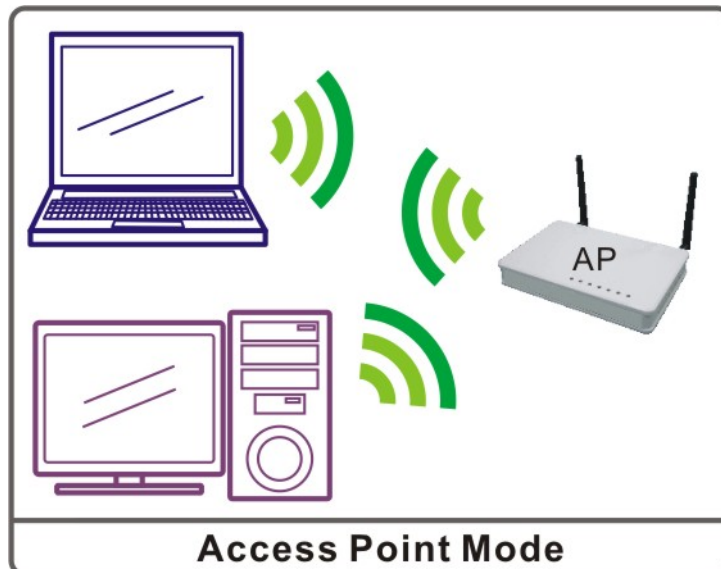
In this mode, the device is supposed to connect to internet via ADSL/Cable Modem. The NAT is enabled and PCs in LAN ports share the same IP address to ISP(Internet Service Provider) through WAN port. The connection type can be setup in PPPoE, DHCP client, PPTP client, L2TP client or static IP.

The wireless connection will be set up from a point-to-point LAN into a point-to-multipoint WAN. This device connects all the stations (PC or notebook with wireless function) to a wireless network. All stations can have the Internet access if only the device has the Internet connection.



## Access Point Mode

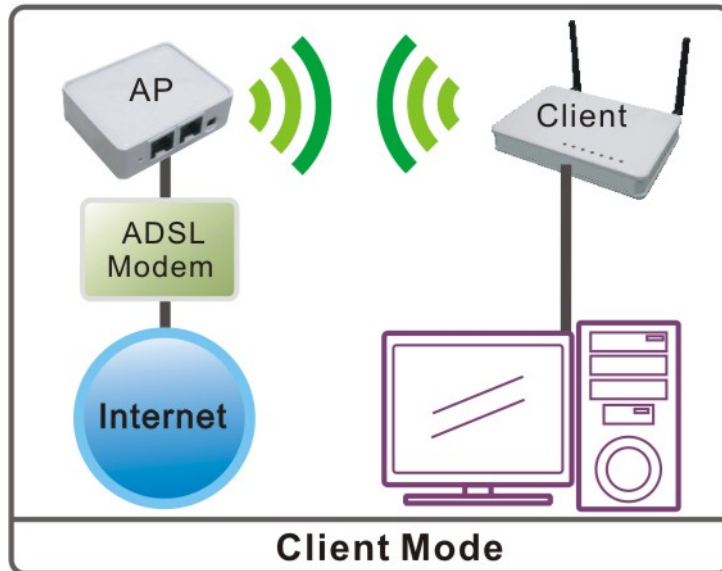
When acting as an Access Point (AP), this device connects all the stations (PC/notebook with wireless network adapter) to a wireless network. All stations can have the Internet access if only the Access Point has the Internet connection.





# Converter Mode

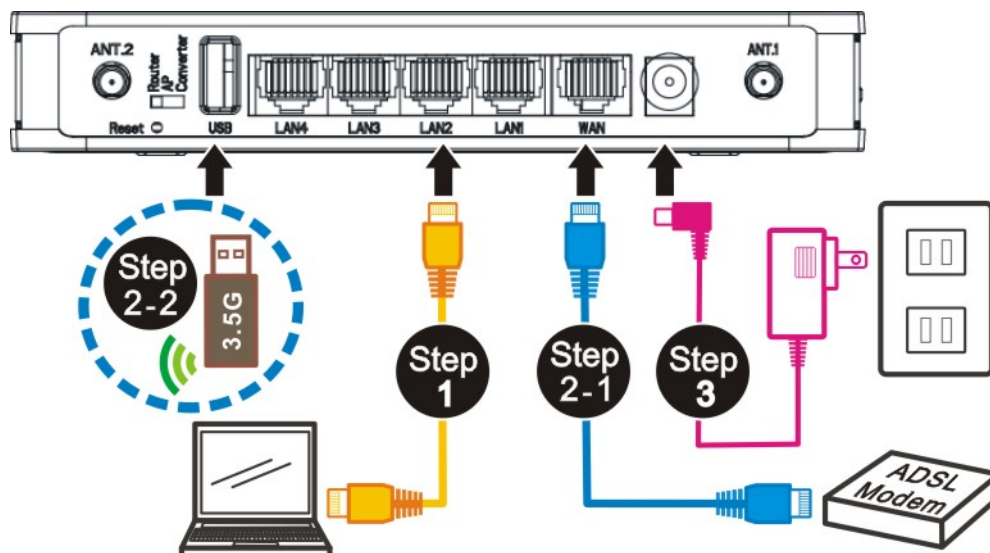
If set to Converter mode, a device connects to each other through an access point or a base station (gateway or router.) This device can work like a wireless station when it's connected to a computer directly, so that the computer can send packets from wired end to wireless interface.



# Chapter 3: Configuration

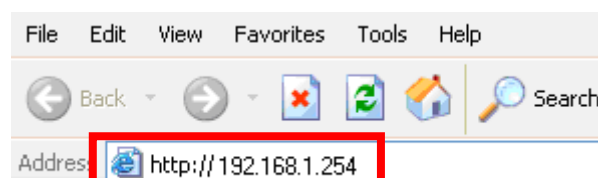
## Hardware Connection

- Step 1.** Connect one end of the Ethernet cable to the LAN port (1~4) of the Wireless Router, another end to your PC or notebook.
- Step 2.** There are two connection methods to connect to Internet (**Only one can be used**):
  - 2-1. Connect Ethernet cable one end to the WAN (Internet) port of the Wireless Router, the other end to the ADSL or cable modem.
  - 2-2. Or you can insert 3.5G USB card (that provide by your ISP) into USB port.
- Step 3.** Finally, connect the Wireless Router with a power to an outlet.



## Login

1. Start your computer and make sure the connection by an Ethernet cable between your computer and the Wireless Router.
2. Start your Web Browser.
3. In the *Address* box, enter the IP address of the Wireless Router, as in this example, which uses the Wireless Router's default IP address: <http://192.168.1.254>



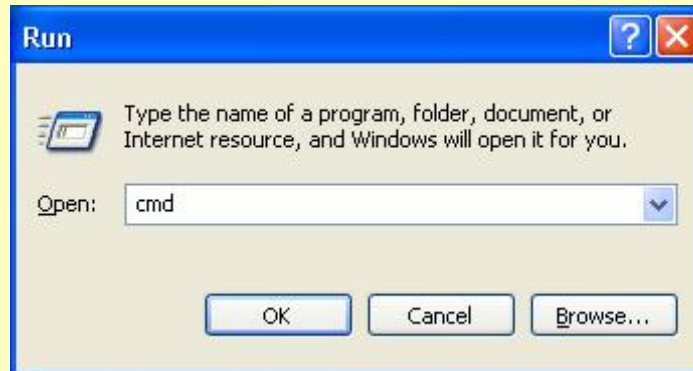
4. After connected successfully, the following screen will show up. Simply enter the username "**admin**" and password "**password**" to login.



## **If you cannot 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:
- Please go to **Start>Run...>** Enter "cmd" command in the column to open the MS-DOS window.



- Enter the command:  
ping 192.168.1.254

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

Pinging 192.168.1.254 with 32 bytes of data:

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

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

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

- If your PC is using a fixed IP Address, its IP Address must be within the range 192.168.1.2 to 192.168.1.253 to be compatible with the Wireless Router's default IP Address of 192.168.1.253. Also, the Network *Mask* must be set to 255.255.255.0. See [Chapter 4 - PC Configuration](#) for details on checking your PC's TCP/IP settings.
- Ensure that your PC and the Wireless Router are on the same network segment. (If you don't have a router, this must be the case.)
- Ensure you are using the wired LAN interface. The Wireless interface can only be used if its configuration matches your PC's wireless settings.

## Common Connection Types

The Internet connection type according to the ISP (Internet Service Provider) that you selected.

### 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.

### Other Modems (e.g. 3.5G Wireless card)

Type	Details	ISP Data required
Dynamic IP address	Your IP address is allocated automatically, when you connect to you ISP.	The ISP's may require you to use a particular Hostname, Domain name, or MAC (physical) address.

# Status

## Status

This page shows the current status and some basic settings of the device.

### System

<b>Uptime</b>	0day:0h:40m:57s
<b>Firmware Version</b>	v2.2.2
<b>Build Time</b>	Thu Sep 2 10:02:25 CST 2010

### Wireless Configuration

<b>Mode</b>	AP
<b>Band</b>	2.4 GHz (B+G+N)
<b>SSID</b>	Wireless Giga Router
<b>Channel Number</b>	11
<b>Encryption</b>	Disabled
<b>BSSID</b>	00:e0:4c:81:96:c1
<b>Associated Clients</b>	1

### TCP/IP Configuration

<b>Attain IP Protocol</b>	Fixed IP
<b>IP Address</b>	192.168.1.254
<b>Subnet Mask</b>	255.255.255.0
<b>Default Gateway</b>	192.168.1.254
<b>DHCP Server</b>	Enabled
<b>MAC Address</b>	00:e0:4c:81:96:c1

### WAN Configuration

<b>Attain IP Protocol</b>	Getting IP from DHCP server...
<b>IP Address</b>	0.0.0.0
<b>Subnet Mask</b>	0.0.0.0
<b>Default Gateway</b>	0.0.0.0
<b>MAC Address</b>	00:e0:4c:81:96:c9

# Network

## LAN Interface Setup

### LAN Interface Setup

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

### LAN Interface Setup

IP Address	<input type="text" value="192.168.1.254"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>
Default Gateway	<input type="text" value="192.168.1.254"/>
DHCP Mode	Server ▾
DHCP Client Range	<input type="text" value="192.168.1.100"/> - <input type="text" value="192.168.1.200"/>
	<input type="button" value="Show Client"/>
Static DHCP	<input type="button" value="Set Static DHCP"/>
Clone MAC Address	<input type="text" value="000000000000"/>
<input type="button" value="Apply Changes"/> <input type="button" value="Reset"/>	

<b>IP Address</b>	Shows the IP address of the Wireless Router (Default IP address is 192.168.1.254)
<b>Subnet Mask</b>	The subnet mask of the Wireless Router (Default subnet mask is 255.255.255.0.)
<b>Default Gateway</b>	Shows the default gateway of this Wireless Router.
<b>DHCP Mode</b>	<p><b>Disable:</b> Select to disable this Wireless Router to distribute IP addresses to connected clients.</p> <p><b>Server:</b> Select to enable this Wireless Router to distribute IP addresses (DHCP Server) to connected clients. And the following field will be activated for you to enter the starting IP address.</p> <p><b>Client:</b> Select the client mode to use the</p>
<b>DHCP Client Range</b>	<p>The starting address of this local IP network address pool. The pool is a piece of continuous IP address segment, the device will distribute IP addresses from 192.168.1.100 to 192.168.1.200 to all the computers in the network that request IP addresses from DHCP server (Router). The end IP address maximum is 253.</p> <p><b>Note:</b> If “Continuous IP address pool starts” is set at 192.168.1.1 and the “Number of IP address in pool end” is 253, the device will distribute IP addresses from 192.168.1.100 to 192.168.1.253 to all the computers in the network that request IP addresses from DHCP server (Router).</p> <p>Click <b>Show Client</b> button to show <b>Active DHCP Client Table</b>. The table shows</p>

assigned IP address, MAC address and time expired for each client.

Active DHCP Client Table

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

---

DHCP Client List

IP Address	MAC Address	Time Expired(s)
192.168.1.100	00:17:c4:a9:07:f4	863062

**Refresh:** Click this button to refresh the table.  
**Close:** Click this button to close the window.

**Static DHCP**

Check the box to enable the Static DHCP function, default setting is disabled. When set to enabled, user can click **Set Static DHCP** button to set the **Static DHCP** function.

Static DHCP Setup

This page allows you reserve IP addresses, and assign the same IP address to the network device with the specified MAC address any time it requests an IP address. This is almost the same as when a device has a static IP address except that the device must still request an IP address from the DHCP server.

---

Static DHCP Setup

**Enable Static DHCP**

**IP Address**

**MAC Address**

**Comment**

---

Static DHCP List

IP Address	MAC Address	Comment	Select

**IP Address:** Enter the fixed IP address that DHCP Server assigned to a certain connected station.  
**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.  
**Comment:** You can enter a comment to description above IP address or MAC address.  
**Apply Changes:** After completing the settings on this page, click Apply changes button to save the settings.  
**Reset:** Click Reset to restore to default values.  
**Static DHCP List:** Here shows the static IP address that have been assigned according to the MAC address.  
**Delete Selected:** Click Delete Selected to delete items which are selected.  
**Delete All:** Click **Delete All** button to delete all the items.  
**Reset:** Click **Reset** button to rest.



**Clone MAC Address**

This table displays you the station MAC information.

## Internet Service Setup

### Internet Service 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 click the item value of WAN Access type.

#### WAN Interface Settings

<b>WAN Access Type</b>	DHCP Client ▾
<b>Host Name</b>	Cherry
<b>MTU Size</b>	1492 (1400-1492 bytes)
<input checked="" type="radio"/> <b>Attain DNS Automatically</b>	
<input type="radio"/> <b>Set DNS Manually</b>	
<b>DNS 1</b>	10.0.0.6
<b>DNS 2</b>	
<b>DNS 3</b>	

#### WAN Interface Advance Settings

- Enable UPnP**
- Enable IGMP Proxy**
- Enable Ping Access on WAN**
- Enable Web Server Access on WAN**
- Enable IPsec pass through on VPN connection**
- Enable PPTP pass through on VPN connection**
- Enable L2TP pass through on VPN connection**
- Enable IPV6 pass through on WAN connection**


**WAN Access Type**

Select the WAN Access Type **Static IP**, **DHCP Client**, **PPPoE**, or **Mobile Networks** from the pull-down list. Default setting is **DHCP (Auto Config)** enabled.

**DHCP Client**

<b>WAN Access Type</b>	DHCP Client
<b>Host Name</b>	Cherry
<b>MTU Size</b>	1492 (1400-1492 bytes)
<input checked="" type="radio"/> <b>Attain DNS Automatically</b>	
<input type="radio"/> <b>Set DNS Manually</b>	
<b>DNS 1</b>	
<b>DNS 2</b>	
<b>DNS 3</b>	

If the DHCP Client be selected, the computer will obtain the IP address automatically.

**Hostname:** Enter the hostname that assigned IP address to your computer in this field. Maximum input is 32 alphanumeric characters (case sensitive).

**MTU Size:** 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 packet size is entered, you may not be able to open certain web sites.

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:** Enter the DNS server IP address(es) provided by your ISP, or you can specify your own preferred DNS server IP address(es).

**DNS 2~3:** This servers are optional. You can enter another DNS server's IP address as a backup. DNS 2 and 3 servers will be used when the DNS 1 server fails.

**Static (Fixed IP)**

<b>WAN Access Type</b>	Static IP
<b>IP Address</b>	
<b>Subnet Mask</b>	
<b>Default Gateway</b>	
<b>MTU Size</b>	1500 (1400-1500 bytes)
<b>DNS 1</b>	
<b>DNS 2</b>	
<b>DNS 3</b>	

If the Static IP be selected, user have to set up the IP address, subnet mask and default gateway according to the ISP (Internet Service

Provider) that provide the related information.

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

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

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

**MTU Size:** 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 packet size is entered, you may not be able to open certain web sites.

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:** Enter the DNS server IP address(es) provided by your ISP, or you can specify your own preferred DNS server IP address(es).

**DNS 2~3:** These servers are optional. You can enter another DNS server's IP address as a backup. DNS 2 and 3 servers will be used when the DNS 1 server fails.

### PPPoE

WAN Access Type	PPPoE
User Name	Normal PPPoE
Multi-PPPoE Provider	Flets West
Public Range	<input type="text"/> - <input type="text"/>
User Name	<input type="text"/>
Password	<input type="text"/>
Service Name	<input type="text"/>
Connection Type	Continuous <input type="button" value="Connect"/> <input type="button" value="Disconnect"/>
Idle Time	5 (1-1000 minutes)
MTU Size	1452 (1360-1492 bytes)
<input type="radio"/> Attain DNS Automatically	
<input checked="" type="radio"/> Set DNS Manually	
DNS 1	<input type="text"/>
DNS 2	<input type="text"/>
DNS 3	<input type="text"/>

If the PPPoE be selected, user have to set up the user name and password according to the ISP (Internet Service Provider) that provided the related information.

**PPPoE Type:** Select the PPPoE types, Normal PPPoE, Multiple PPPoE and Unnumbered PPPoE from the pull-down menu.

**Multi-PPPoE provider:** If user select Multiple PPPoE type, user have to setup the PPPoE provider here. Select Flets West, Next West, Flets East, and Flets Next from the pull-down menu.

**Public Range:** If user selected Unnumbered PPPoE type, have to setup the range here.

**User Name:** Enter the username that provide by your ISP (Internet Service Provider). Maximum input is 32 alphanumeric characters (case sensitive).

**Password:** Enter the password that provide by your ISP. Maximum input is 32 alphanumeric characters (case-sensitive).

**Service Name:** Enter the Internet service provider's name here.

**Connection Type:** Select the connection type **Continuous**, **Connect on Demand** or **Manual** from the pull-down menu. If selected **Manual** user can click **Connect** button to make a connection.

**Idle Time:** It represents that the device will idle after the minutes you set. The time must be set between 1~1000 minutes. Default value of idle time is 5 minutes. This function will be available when the **Connection Type** is selected to **Connect on Demand**.

**MTU Size:** MTU(Maximum Transmission Unit, namely the maximum packet size) 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.

**Connection Type:** Select the connection type **Continuous**, **Connect on Demand** or **Manual** from the pull-down menu. If selected **Manual** user can click **Connect** button to make a connection.

**Idle Time:** It represents that the device will idle after the minutes you set. The time must be set between 1~1000 minutes. Default value of idle time is 5 minutes. This function will be available when the **Connection Type** is selected to **Connect on Demand**.

### Mobile Networks

WAN Interface Settings

**WAN Access Type** Mobile Networks ▾

**Auto APN**

**Service Name**

**Dial Number**

**Authentication**

**User Name**

**Password**

**Pin Code**

**Pin code Number**

**Connection Type** Continuous ▾

**Idle Time**  (1-1000 minutes)

**MTU Size**  (1360-1492 bytes)

**User have to insert USB card that provide by Internet service provider into the USB port of the wireless router**

	<p><b><u>first, therefore, the Mobile networks function can be used.</u></b></p> <p><b>Auto APN:</b> APN(Access Point Name.) If this function be selected, the system will auto detect the mobile network setting via the USB that provide by the Internet service provider(ISP). To use the default settings is recommend.</p> <p><b>Service Name:</b> Keep the default setting or enter the service name that ISP provided.</p> <p><b>Dial Number:</b> Keep the default setting or enter the dial number that ISP provided.</p> <p><b>Authentication:</b> Check the box to enable to authentication function.</p> <ul style="list-style-type: none"> <li>● <b>User Name:</b> Enter the user name that provide by your ISP.</li> <li>● <b>Password:</b> Enter the password that provide by your ISP.</li> </ul> <p><b>Pin code:</b> Keep the default setting or enter the SIM card Pin code that ISP provided.</p> <p><b>Connection Type:</b> Select the connection type <b>Continuous</b>, <b>Connect on Demand</b> from the pull-down menu.</p> <p><b>Idle Time:</b> It represents that the device will idle after the minutes you set. The time must be set between 1~1000 minutes. Default value of idle time is 5 minutes. This function will be available when the <b>Connection Type</b> is selected to <b>Connect on Demand</b>.</p> <p><b>MTU Size:</b> MTU(Maximum Transmission Unit, namely the maximum packet size) 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.</p>
<b>Enable uPNP...</b>	Check to enable the listed functions.
<b>Apply</b>	After completing the settings on this page, click <b>Apply</b> button to save the settings.
<b>Cancel</b>	Click <b>Cancel</b> to restore to default values.

## Advanced Routing

If you connect several routers with this Wireless Router, you may need to set up a predefined routing rule to have more effective network topology/traffic, this is called static route between those routers and the Wireless Router.

### Advanced Routing

This page is used to setup dynamic routing protocol or edit static route entry.

#### Dynamic Route Setup

Enable Dynamic Route

NAT  Enabled  Disabled

Transmit  Disabled  RIP 1  RIP 2

Receive  Disabled  RIP 1  RIP 2

Apply Changes

Reset

#### Static Route Setup

Enable Static Route

IP Address

Subnet Mask

Gateway

Metric

Interface

Apply Changes

Reset

Show Route Table

#### Route Table

Destination IP Address	Netmask	Gateway	Metric	Interface	Select
------------------------	---------	---------	--------	-----------	--------

Delete Selected

Delete All

Reset

<b>Enable Dynamic Route</b>	<p>Check to enable the dynamic route function.</p> <p><b>NAT:</b> Select to enable the network address translation function.</p> <p><b>Transmit:</b> Select to use the Routing Information Protocol, the function will select the packet transmitting route that pass through least routers.</p> <p><b>Receive:</b> Select to use the Routing Information Protocol, the function will select the packet receiving route that pass through least routers.</p>
<b>Enable Static Route</b>	<p><b>IP address:</b> Enter the Gateway IP address in the field.</p> <p><b>Subnet Mask:</b> Enter the Gateway subnet mask here.</p> <p><b>Gateway:</b> Enter the gateway name or domain name here.</p>

	<p><b>Metric:</b> The route with the lowest metric is the preferred route.</p> <p><b>Interface:</b> Select to use <b>LAN</b> or <b>WAN</b> as the physical interface from where the packets will be sent.</p>
<b>Destination</b>	The network address of the destination LAN segment. When a packet with destination IP address that matches to this field, it will route to the device set in the Route Gateway field.
<b>Range</b>	Select <b>Host</b> or <b>Net</b> from the pull-down menu. If select Net, please enter the <b>Netmask</b> in the following column.
<b>IP address</b>	Enter the Gateway IP address in the field.
<b>Interface</b>	You can
<b>Comment</b>	Enter note or remark here.
<b>Apply</b>	After completing the settings on this page, click <b>Apply</b> button to save the settings.
<b>Reset</b>	Click to discard current setting.

## PPTP Server

### PPTP Server

A PPTP (Point-To-Point Tunneling Protocol) Server allows you to connect securely from a remote location (such as your home) to an LAN (Local Area Network) located in another location, such as your workplace, business office, etc.

#### PPTP Server Settings

**Enable PPTP Server**

**User Name**

**Password**

**PPTP Server IP Address**

(xxx.xxx.xxx.xxx)

**PPTP Client's IP start**

(xxx.xxx.xxx.xxx)

**Max Connect Users**




<b>Enable PPTP Server</b>	Check to enable the PPTP server function, this function allows you to connect securely from a remote location (such as your home) to an LAN (Local Area Network) located in another location, such as your workplace, business office and so on.
<b>User Name</b>	Enter username in the column, when the PPTP client try to connect to the PPTP sever should login with the username.
<b>Password</b>	Setup the password in the column, when the PPTP client try to connect to the PPTP sever should login with the password.
<b>PPTP Server IP address</b>	Setup the PPTP server IP address here.
<b>PPTP Client's IP Start</b>	Setup the Client's start IP address here.
<b>Max Connect Users</b>	Setup the PPTP client allowed maximum here.



# Wireless

## Basic

### 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.

### Wireless Basic Settings

**Disable Wireless LAN Interface**

**Band**

**Mode**

**Network Type**

**SSID**

**Channel Width**

**Channel Number**

**Broadcast SSID**

**WMM**

**Data Rate**

**Associated Clients**

**Enable Mac Clone (Single Ethernet Client)**

<b>Disable Wireless LAN Interface</b>	Check to disable the wireless function. If the wireless LAN interface be disabled, the WLAN LED on the front LED will be off.
<b>Band</b>	<p>You can choose one mode of the following you need.</p> <ul style="list-style-type: none"> <li>● 2.4GHz (B): 802.11b supported rate only.</li> <li>● 2.4GHz (G): 802.11g supported rate only.</li> <li>● 2.4GHz (N): 802.11n supported rate only.</li> <li>● 2.4GHz (B+G): 802.11b supported rate and 802.11g supported rate.</li> <li>● 2.4GHz (G+N): 802.11g supported rate and 802.11n supported rate.</li> <li>● 2.4GHz (B+G+N): 802.11b, 802.11g and 802.11n supported rate.</li> </ul> <p>The default is 2.4GHz (B+G+N) mode.</p>
<b>Mode</b>	Under Router operation mode, user can select AP, WDS, and AP+WDS from the pull-down list. For AP mode, user can select AP, Client, WDS and AP+WDS mode. Under client mode, there is only Client mode can be selected.

	<p><b>Multiple APs</b></p> <p>This page shows and updates the wireless setting for multiple APs.</p> <div style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;"> <p style="text-align: center; background-color: #007bff; color: white; margin: 0;">Multiple APs</p> <p style="text-align: center; font-size: small; margin: 5px 0;">This page shows and updates the wireless setting for multiple APs.</p> </div> <table border="1" style="width: 100%; border-collapse: collapse; margin: 10px 0;"> <thead> <tr style="background-color: #007bff; color: white;"> <th colspan="9">Multiple APs Table</th> </tr> <tr> <th>No.</th> <th>Enable</th> <th>Band</th> <th>SSID</th> <th>Data Rate</th> <th>Broadcast SSID</th> <th>WMM</th> <th>Access</th> <th>Active Client List</th> </tr> </thead> <tbody> <tr> <td>AP1</td> <td><input type="checkbox"/></td> <td>2.4 GHz (B+G+N)</td> <td>RTK 11n AP VAP1</td> <td>Auto</td> <td>Enabled</td> <td>Enabled</td> <td>LAN+WAN</td> <td>Show</td> </tr> <tr> <td>AP2</td> <td><input type="checkbox"/></td> <td>2.4 GHz (B+G+N)</td> <td>RTK 11n AP VAP2</td> <td>Auto</td> <td>Enabled</td> <td>Enabled</td> <td>LAN+WAN</td> <td>Show</td> </tr> <tr> <td>AP3</td> <td><input type="checkbox"/></td> <td>2.4 GHz (B+G+N)</td> <td>RTK 11n AP VAP3</td> <td>Auto</td> <td>Enabled</td> <td>Enabled</td> <td>LAN+WAN</td> <td>Show</td> </tr> <tr> <td>AP4</td> <td><input type="checkbox"/></td> <td>2.4 GHz (B+G+N)</td> <td>RTK 11n AP VAP4</td> <td>Auto</td> <td>Enabled</td> <td>Enabled</td> <td>LAN+WAN</td> <td>Show</td> </tr> </tbody> </table> <p style="text-align: center; margin: 10px 0;"> <input type="button" value="Apply Changes"/> <input type="button" value="Reset"/> </p> <p>User can set up the multiple AP here.</p>	Multiple APs Table									No.	Enable	Band	SSID	Data Rate	Broadcast SSID	WMM	Access	Active Client List	AP1	<input type="checkbox"/>	2.4 GHz (B+G+N)	RTK 11n AP VAP1	Auto	Enabled	Enabled	LAN+WAN	Show	AP2	<input type="checkbox"/>	2.4 GHz (B+G+N)	RTK 11n AP VAP2	Auto	Enabled	Enabled	LAN+WAN	Show	AP3	<input type="checkbox"/>	2.4 GHz (B+G+N)	RTK 11n AP VAP3	Auto	Enabled	Enabled	LAN+WAN	Show	AP4	<input type="checkbox"/>	2.4 GHz (B+G+N)	RTK 11n AP VAP4	Auto	Enabled	Enabled	LAN+WAN	Show
Multiple APs Table																																																							
No.	Enable	Band	SSID	Data Rate	Broadcast SSID	WMM	Access	Active Client List																																															
AP1	<input type="checkbox"/>	2.4 GHz (B+G+N)	RTK 11n AP VAP1	Auto	Enabled	Enabled	LAN+WAN	Show																																															
AP2	<input type="checkbox"/>	2.4 GHz (B+G+N)	RTK 11n AP VAP2	Auto	Enabled	Enabled	LAN+WAN	Show																																															
AP3	<input type="checkbox"/>	2.4 GHz (B+G+N)	RTK 11n AP VAP3	Auto	Enabled	Enabled	LAN+WAN	Show																																															
AP4	<input type="checkbox"/>	2.4 GHz (B+G+N)	RTK 11n AP VAP4	Auto	Enabled	Enabled	LAN+WAN	Show																																															
<b>Network Type</b>	If the mode be set to AP or Client mode that the network type can be set to Infrastructure or Ad hoc.																																																						
<b>SSID</b>	A SSID(Service Set Identifier) is referred to a network name because essentially it is a name that identifies a wireless network (case-sensitive).																																																						
<b>Channel Width</b>	Select 20MHz/40MHz channel width, the channel number will be form 5~11 and auto; Select 20MHz channel width the channel number will be form 1~11 and auto. Default is 20MHz/40MHz.																																																						
<b>Channel Selection</b>	The channel number base on the channel width you select.																																																						
<b>Broadcast SSID</b>	<p><b>Enabled:</b> This wireless AP will broadcast its SSID to stations.</p> <p><b>Disabled:</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.</p>																																																						
<b>WMM</b>	The WiFi Multiple Media function is available under 2.4GHz (B), 2.4GHz (G) and 2.4GHz (B+G) band, and it is <b>disabled</b> under 2.4GHz (N), 2.4GHz (G+N) and 2.4GHz (B+G+N) band.																																																						
<b>Data Rate</b>	There are several data rate that you can select from the pull-down menu.																																																						
<b>Associated Clients</b>	<p>Click <b>Show Active Clients</b> button to show all the listed active clients.</p> <div style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;"> <p style="text-align: center; background-color: #007bff; color: white; margin: 0;">Active Wireless Client Table</p> <p style="text-align: center; font-size: small; margin: 5px 0;">This table shows the MAC address, transmission, reception packet counters and encrypted status for each associated wireless client.</p> </div> <table border="1" style="width: 100%; border-collapse: collapse; margin: 10px 0;"> <thead> <tr style="background-color: #007bff; color: white;"> <th colspan="7">Wireless Client Table</th> </tr> <tr> <th>MAC Address</th> <th>Mode</th> <th>Tx Packet</th> <th>Rx Packet</th> <th>Tx Rate (Mbps)</th> <th>Power Saving</th> <th>Expired Time (s)</th> </tr> </thead> <tbody> <tr> <td>None</td> <td>---</td> <td>---</td> <td>---</td> <td>---</td> <td>---</td> <td>---</td> </tr> </tbody> </table> <p style="text-align: center; margin: 10px 0;"> <input type="button" value="Refresh"/> <input type="button" value="Close"/> </p>	Wireless Client Table							MAC Address	Mode	Tx Packet	Rx Packet	Tx Rate (Mbps)	Power Saving	Expired Time (s)	None	---	---	---	---	---	---																																	
Wireless Client Table																																																							
MAC Address	Mode	Tx Packet	Rx Packet	Tx Rate (Mbps)	Power Saving	Expired Time (s)																																																	
None	---	---	---	---	---	---																																																	
<b>Enable Mac Clone (Single Ethernet Client)</b>	This function will be enabled under Client mode.																																																						

## Advanced

### 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.

#### Wireless Advanced Settings

<b>Fragment Threshold</b>	<input type="text" value="2346"/> (256-2346)
<b>RTS Threshold</b>	<input type="text" value="2347"/> (0-2347)
<b>Beacon Interval</b>	<input type="text" value="100"/> (20-1024 ms)
<b>Preamble Type</b>	<input checked="" type="radio"/> Long Preamble <input type="radio"/> Short Preamble
<b>IAPP</b>	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
<b>Protection</b>	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
<b>Aggregation</b>	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
<b>Short GI</b>	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
<b>WLAN Partition</b>	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
<b>STBC</b>	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
<b>20/40MHz Coexist</b>	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
<b>RF Output Power</b>	<input checked="" type="radio"/> 100% <input type="radio"/> 70% <input type="radio"/> 50% <input type="radio"/> 35% <input type="radio"/> 15%



<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 2346.
<b>RTS Threshold</b>	RTS Threshold is a mechanism implemented to prevent the “Hidden Node” problem. If the “Hidden Node” problem is an issue, please specify the packet size. The RTS mechanism will be activated if the data size exceeds the value you set. Warning: Enabling RTS Threshold will cause redundant network overhead that could negatively affect the throughput performance instead of providing a remedy. This value should remain at its default setting of 2347. Should you encounter inconsistent data flow, only minor modifications of this value are recommended.
<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 20-1024 ms, default is 100.
<b>Preamble Type</b>	A preamble is a signal used in wireless environment to synchronize the transmitting timing including Synchronization and Start frame delimiter.

	You can select Long or Short for the preamble type.
<b>IAPP</b>	Select Enabled or Disabled to execute this function.
<b>Protection</b>	Select Enabled or Disabled to execute the security function.
<b>Aggregation</b>	Select Enabled or Disabled to execute this function.
<b>Short GI</b>	Select Enabled or Disabled to execute this function.
<b>WLAN Partition</b>	Select Enabled or Disabled to execute this function.
<b>STBC</b>	Select Enabled or Disabled to execute this function.
<b>20/40MHz Coexist</b>	Select Enabled or Disabled to execute this function.
<b>RF Output Power</b>	Select the transmitting power rate 100%, 70%, 50%, 35%, 15%.

## Security

### Wireless Security Setup

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

#### Security Settings

Select SSID

Wireless Giga Router ▾

Apply Changes

Reset

Encryption

Disabled ▾

#### Security Settings

<b>Select SSID</b>	Select SSID(Service Set Identifier) to set up the security form the pull-down list.
<b>Encryption</b>	<p>There are several type of encryption modes including <b>Disabled</b>, <b>WEP(Open System)</b>, <b>WEP(Shared Key)</b>, <b>WEP( AUTO)</b>, <b>WPA(Personal)</b>, <b>WPA2(Personal)</b>, and <b>WPA-Mixed</b>. The security default setting is Disabled. It is strongly recommended to set up security mode to prevent any unauthorized accessing.</p> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>➤ AUTO(Open/Shared) means AP can accept client(station) to connect to it by using OPEN-WEP or SHARED-WEP.</li> </ul> <p><b>WEP</b></p>

<b>Encryption</b>	WEP ▾
<b>Authentication</b>	<input type="radio"/> Open System <input type="radio"/> Shared Key <input checked="" type="radio"/> Auto
<b>Key Length</b>	64-bit ▾
<b>Key Format</b>	Hex ▾
<b>Encryption Key</b>	*****

**Authentication:** Select Open System, Shared Key or Auto.  
**Key Length:** select key length 64-bit or 128-bit.  
**Key Format:**

- **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).

**Encryption Key:** Enter the key in the key setting field.

---

<b>WPA-PSK/ WPA2-PSK/ WPA-PSK WPA2-PSK</b>	
<b>Encryption</b>	WPA-Mixed ▾
<b>Authentication Mode</b>	<input checked="" type="radio"/> Personal (Pre-Shared Key)
<b>WPA Cipher Suite</b>	<input type="checkbox"/> TKIP <input checked="" type="checkbox"/> AES
<b>WPA2 Cipher Suite</b>	<input type="checkbox"/> TKIP <input checked="" type="checkbox"/> AES
<b>Pre-Shared Key Format</b>	Passphrase ▾
<b>Pre-Shared Key</b>	

**Authentication Mode:** Select Enterprise (RADIUS) or Personal (Pre-Shared Key) mode.  
**WPA Cipher Suite:** here supported AES only.  
**WPA2 Cipher Suite:** here supported AES only.  
**Pre-Shared Key Format:** 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.  
**Pre-Shared Key :** Pre-Shared Key serves as a password. Users may key in 8 to 63 characters string if you selected 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.

## ACL

### Wireless Access Control

If you choose 'Allowed Listed', only those clients whose wireless MAC addresses are in the access control list will be able to connect to your Access Point. When 'Deny Listed' is selected, these wireless clients on the list will not be able to connect the Access Point.

#### Wireless Access Control Settings

**Wireless Access Control Mode**

**MAC Address**

**Comment**  (Maximum characters is 20)

(The maximum rule count is 20)



#### Current Access Control List

MAC Address	Comment	Select
-------------	---------	--------




<b>Wireless Access Control Mode</b>	Select <b>Allow Listed</b> or <b>Deny Listed</b> form the pull-down menu to enable access control function. Default setting is <b>Disabled</b> .
<b>MAC Address</b>	Enter the MAC address (12 characters) of a station that is allowed to access this Access Point.
<b>Comment</b>	You may enter up to 20 characters as a remark to the previous MAC address.
<b>Current Access Control List</b>	This table displays you the station MAC information.
<b>Delete Selected</b>	Click <b>Delete Selected</b> to delete items which are selected.
<b>Delete All</b>	Click <b>Delete All</b> to delete all the items.
<b>Reset</b>	Click <b>Reset</b> to rest.

## WDS

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.

To use WDS function:

1. The APs must support WDS function.
2. To set the same SSID (Network name).
3. The channel must be set to the same on the APs.
4. To set the same Wireless MAC address (BSSID) on the APs.
5. To set same security (WEP or WPA) on the APs.

### Note !

**To setup WDS must use the same wireless products (the same model will be better); due to different wireless products might support different WDS settings. Thus, it is suggested that to use the same wireless products that support WDS function.**

## WDS

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.

### WDS Settings

Enable WDS

MAC Address

Data Rate

Comment

Apply Changes

Reset

Set Security

Show Statistics

### Current WDS AP List

MAC Address	Tx Rate (Mbps)	Comment	Select
-------------	----------------	---------	--------

Delete Selected

Delete All

Reset

- Step 1.** Users would like to set up the WDS function, please go to **Wireless > Basic** page to set up the mode into **WDS** or **AP+ WDS** (Repeater) mode, and set the APs into the same **Network Name(SSID)** and **Channel** (If set to WDS mode, the SSID do not need to change). After setting up, please click **Apply Changes** button to execute.

### Wireless Basic Settings

Disable Wireless LAN Interface

Band: 2.4 GHz (B+G+N)

**1** Mode: AP

Network Type: Infrastructure

**2** SSID: Wireless Giga Router

Channel Width: 40MHz

**3** Channel Number: 11

Broadcast SSID: Enabled

WMM: Enabled

Data Rate: Auto

Associated Clients:

Enable Mac Clone (Single Ethernet Client)

**Step 2.** Then go to **Wireless > WDS** page to (1) enable the WDS function and (2) enter APs **Wireless MAC address** (please go to **Status > Wireless Configuration** to make sure the **BSSID**) to each other to make the WDS connection. Please click **Apply** button to execute.

### WDS

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.

### WDS Settings

**1**  Enable WDS

**2** MAC Address:

Data Rate: Auto

Comment:

### Current WDS AP List

MAC Address	Tx Rate (Mbps)	Comment	Select
<input type="button" value="Delete Selected"/> <input type="button" value="Delete All"/> <input type="button" value="Reset"/>			

<b>Enable WDS</b>	Check the box to enable the WDS function.
-------------------	---



<p><b>MAC Address</b></p>	<p><b>MAC Address:</b> Enter the Wireless BSSID (MAC) 12 characters of the wireless AP that you want to connect with. To check your wireless router's MAC address, please go to <b>Status &gt; Wireless Configuration</b> to find your <b>BSSID</b> (Wireless MAC address.)</p> <div style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;"> <p style="background-color: #0070c0; color: white; padding: 2px;"><b>Wireless Configuration</b></p> <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="padding: 2px;"><b>Mode</b></td> <td style="padding: 2px;">AP+WDS</td> </tr> <tr> <td style="padding: 2px;"><b>Band</b></td> <td style="padding: 2px;">2.4 GHz (B+G+N)</td> </tr> <tr> <td style="padding: 2px;"><b>SSID</b></td> <td style="padding: 2px;">Wireless Giga Router</td> </tr> <tr> <td style="padding: 2px;"><b>Channel Number</b></td> <td style="padding: 2px;">11</td> </tr> <tr> <td style="padding: 2px;"><b>Encryption</b></td> <td style="padding: 2px;">Disabled(AP), Disabled(WDS)</td> </tr> <tr> <td style="padding: 2px;"><b>BSSID</b></td> <td style="padding: 2px;">00:e0:4c:81:96:c1</td> </tr> <tr> <td style="padding: 2px;"><b>Associated Clients</b></td> <td style="padding: 2px;">0</td> </tr> </table> </div>	<b>Mode</b>	AP+WDS	<b>Band</b>	2.4 GHz (B+G+N)	<b>SSID</b>	Wireless Giga Router	<b>Channel Number</b>	11	<b>Encryption</b>	Disabled(AP), Disabled(WDS)	<b>BSSID</b>	00:e0:4c:81:96:c1	<b>Associated Clients</b>	0
<b>Mode</b>	AP+WDS														
<b>Band</b>	2.4 GHz (B+G+N)														
<b>SSID</b>	Wireless Giga Router														
<b>Channel Number</b>	11														
<b>Encryption</b>	Disabled(AP), Disabled(WDS)														
<b>BSSID</b>	00:e0:4c:81:96:c1														
<b>Associated Clients</b>	0														
<p><b>Data Rate</b></p>	<p>Select the data rate form the pull-down list.</p>														
<p><b>Comment</b></p>	<p>Enter a description for the device.</p>														
<p><b>Apply Changes</b></p>	<p>After completing the settings on this page, click <b>Apply changes</b> button to save the settings.</p>														
<p><b>Reset</b></p>	<p>Click <b>Reset</b> to restore to default values.</p>														
<p><b>Set Security</b></p>	<p>Enable the WDS function and then click <b>Set Security</b> button to set up the WDS security.</p> <p style="font-size: small; color: #0070c0;">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> <hr style="border: 1px solid #0070c0;"/> <div style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;"> <p style="background-color: #0070c0; color: white; padding: 2px;"><b>WDS Security Setup</b></p> <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="padding: 2px;"><b>Encryption</b></td> <td style="padding: 2px;"><input type="text" value="None"/></td> </tr> <tr> <td style="padding: 2px;"><b>WEP Key Format</b></td> <td style="padding: 2px;"><input type="text" value="ASCII (5 characters)"/></td> </tr> <tr> <td style="padding: 2px;"><b>WEP Key</b></td> <td style="padding: 2px;"><input type="text"/></td> </tr> <tr> <td style="padding: 2px;"><b>Pre-Shared Key Format</b></td> <td style="padding: 2px;"><input type="text" value="Passphrase"/></td> </tr> <tr> <td style="padding: 2px;"><b>Pre-Shared Key</b></td> <td style="padding: 2px;"><input type="text"/></td> </tr> </table> <p style="text-align: center; margin-top: 5px;"> <input type="button" value="Apply Changes"/> <input type="button" value="Reset"/> </p> </div> <p><b>Encryption:</b> Select the encryption type <b>None</b>, <b>WEP 64 bits</b>, <b>WEP 128 bits</b>, and <b>WPA2(AES)</b> from the pull-down menu.</p> <p><b>WEP Key Format:</b> For <b>WEP 64 bits</b> and <b>WEP 128 bits</b> encryption type, the selection of <b>WEP Key Format</b> are <b>Hex</b> and <b>ASCII</b>.</p> <p><b>WEP Key:</b> 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"> <li>● <b>Hexadecimal (WEP 64 bits):</b> 10 Hex characters (0~9, a~f).</li> <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> <p><b>Pre-Shared Key Format:</b> The <b>Pre-shared Key Format</b> will be enabled when <b>WPA (TKIP)</b> and <b>WPA2 (AES)</b> encryption be selected. There are two formats for choice to set the Pre-shared key, <b>Passphrase</b> and <b>Hex (64 characters)</b>. If <b>Hex</b> is selected, users will have to enter a 64 characters string. For easier configuration, the <b>Passphrase</b> (at least 8 characters) format is recommended.</p> <p><b>Pre-Shared Key:</b> 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</p>	<b>Encryption</b>	<input type="text" value="None"/>	<b>WEP Key Format</b>	<input type="text" value="ASCII (5 characters)"/>	<b>WEP Key</b>	<input type="text"/>	<b>Pre-Shared Key Format</b>	<input type="text" value="Passphrase"/>	<b>Pre-Shared Key</b>	<input type="text"/>				
<b>Encryption</b>	<input type="text" value="None"/>														
<b>WEP Key Format</b>	<input type="text" value="ASCII (5 characters)"/>														
<b>WEP Key</b>	<input type="text"/>														
<b>Pre-Shared Key Format</b>	<input type="text" value="Passphrase"/>														
<b>Pre-Shared Key</b>	<input type="text"/>														

	used on client's end.															
<b>Show Statistics</b>	<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> <p>This table shows the MAC address, transmission, reception packet counters and state information for each configured WDS AP.</p> <hr/> <table border="1"> <thead> <tr> <th colspan="5">WDS AP Table</th> </tr> <tr> <th>MAC Address</th> <th>Tx Packets</th> <th>Tx Errors</th> <th>Rx Packets</th> <th>Tx Rate (Mbps)</th> </tr> </thead> <tbody> <tr> <td colspan="5" style="text-align: center;"> <input type="button" value="Refresh"/> <input type="button" value="Close"/> </td> </tr> </tbody> </table> <p><b>Refresh:</b> Click to renew the counters information.  <b>Close:</b> Click to leave the screen.</p>	WDS AP Table					MAC Address	Tx Packets	Tx Errors	Rx Packets	Tx Rate (Mbps)	<input type="button" value="Refresh"/> <input type="button" value="Close"/>				
WDS AP Table																
MAC Address	Tx Packets	Tx Errors	Rx Packets	Tx Rate (Mbps)												
<input type="button" value="Refresh"/> <input type="button" value="Close"/>																
<b>Current WDS AP List</b>	Here shows the current WDS AP information.															
<b>Delete Selected</b>	Click <b>Delete Selected</b> to delete the selected AP information.															
<b>Delete All</b>	Click <b>Delete All</b> to delete all the items.															
<b>Reset</b>	Click <b>Reset</b> to restore the settings.															

# WPS

## Wi-Fi Protected Setup

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

### Wi-Fi Protected Setup Settings

**Disable WPS**

**WPS Status**

Configured  UnConfigured

Reset to UnConfigured

**Self-PIN Number**

55291668

**Push Button Configuration**

Start PBC

Apply Changes

Reset

### Current Key Info

Encryption	Cipher Suite	Key
Open	None	N/A

### Client PIN Number

**Client PIN Number**

Start PIN

<b>Disable WPS</b>	Check the box to disable the WPS function, default setting is enabled.
<b>WPS Status</b>	Here shows the current status of the WPS function. Default setting is Configured, click <b>Reset to Unconfigured</b> to re-configured the WPS connection.
<b>Self-PIN Number</b>	Here shows the 8 characters PIN code of the router itself.
<b>Push Button Configuration</b>	Click <b>Start PBC</b> button to make a WPS connection with client.
<b>Client PIN Number</b>	Enter the client PIN code into the blank field then click the <b>Start PIN</b> button to make a WPS connection with client.

# Schedule

## Wireless Schedule

This page allows you setup the wireless schedule rule. Please do not forget to configure system time before enable this feature.

### Wireless Schedule Settings

**Enable Wireless Schedule**

**Days**

Everyday

Sun  Mon  Tue  Wed  Thu  Fri  Sat

**Time**

24 Hours

From  :  To  :

Apply Changes

Reset

#### Enable Wireless Schedule

Check the box to enable the schedule function. Set up the time to schedule the wireless access rule. Select the day and time you want to enable the wireless function.

# Firewall

## DMZ Settings

### 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

**Enable DMZ**

**DMZ Host IP Address**

**Apply Changes**

**Reset**

<b>Enable DMZ</b>	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.
<b>DMZ Host IP Address</b>	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. <b>Note:</b> You need to give your LAN PC clients a fixed/static IP address for DMZ to work properly.
<b>Apply Changes</b>	After completing the settings on this page, click <b>Apply Changes</b> button to save the settings.
<b>Reset</b>	Click <b>Reset</b> button to restore to default values.

# URL Filter Settings

## URL Filter Settings

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

### URL Filter Settings

**Enable URL Filtering**

**URL Address**  (Maximum characters is 30)

(The maximum rule count is 8)

**Apply Changes**

**Reset**

### Current URL Filter Table

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

**Delete Selected**

**Delete All**

**Reset**

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

# MAC Filtering

## MAC Filtering

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

### MAC Filtering Settings

**Enable MAC Filtering**

**MAC Address**

**Comment**

 (Maximum characters is 20)

(The maximum rule count is 20)



### Current MAC Filter Table

MAC Address	Comment	Select
-------------	---------	--------




<b>Enable MAC Filtering</b>	Check to enable MAC filtering function.
<b>MAC Address</b>	Enter the client MAC address in the field.
<b>Comment</b>	You may key in a description MAC address.
<b>Apply Changes</b>	After completing the settings on this page, click <b>Apply Changes</b> button to save the settings.
<b>Reset</b>	Click <b>Reset</b> button to restore to default values.
<b>Current Filter Table</b>	Shows the current MAC filter information.
<b>Delete Selected</b>	Click <b>Delete Selected</b> button to delete items which are selected.
<b>Delete All</b>	Click <b>Delete All</b> button to delete all the items.
<b>Reset</b>	Click <b>Reset</b> button to rest.

## Port Filtering Settings

### Port Filter Settings

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

#### Port Filter Settings

**Enable Port Filtering**

**Port Range**

 - 

**Protocol**

**Comment**

 (Maximum characters is 20)

(The maximum rule count is 20)



#### Current Port Filter Table

Port Range	Protocol	Comment	Select
------------	----------	---------	--------




<b>Enable Port Filtering</b>	Check to enable Port Filtering function.
<b>Port Range</b>	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 Both) used to the remote system or service.
<b>Comment</b>	You may key in a description MAC address.
<b>Apply Changes</b>	After completing the settings on this page, click <b>Apply Changes</b> button to save the settings.
<b>Reset</b>	Click <b>Reset</b> button to restore to default values.
<b>Current Port Forwarding Table</b>	Shows the current Port Forwarding information.
<b>Delete Selected</b>	Click <b>Delete Selected</b> button to delete items which are selected.
<b>Delete All</b>	Click <b>Delete All</b> button to delete all the items.
<b>Reset</b>	Click <b>Reset</b> button to rest.



# IP Filtering

## IP Filtering

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

### IP Filtering Settings

**Enable IP Filtering**

**Local IP Address**

**Protocol**

**Comment**

 (Maximum characters is 20)

(The maximum rule count is 20)



### Current IP Filter Table

Local IP Address	Protocol	Comment	Select
------------------	----------	---------	--------




<b>Enable IP Filtering</b>	Check to enable IP filtering function.
<b>Local IP Address</b>	Enter the local server's IP address.
<b>Protocol</b>	Select the protocol (TCP, UDP or Both) used to the remote system or service.
<b>Comment</b>	You may key in a description for the port range.
<b>Apply Changes</b>	After completing the settings on this page, click <b>Apply Changes</b> button to save the settings.
<b>Reset</b>	Click <b>Reset</b> button to restore to default values.
<b>Current Filter Table</b>	Shows the current IP filter information.
<b>Delete Selected</b>	Click <b>Delete Selected</b> button to delete items which are selected.
<b>Delete All</b>	Click <b>Delete All</b> button to delete all the items.
<b>Reset</b>	Click <b>Reset</b> button to rest.

## Virtual Server

### Virtual Server

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

**Enable Port Forwarding**

**IP Address**

**Protocol**

**Port Range**

 - 

**Comment**

 (Maximum characters is 20)

(The maximum rule count is 20)



#### Current Port Forwarding Table

IP Address	Protocol	Port Range	Comment	Select
------------	----------	------------	---------	--------




<b>Enable Port Forwarding</b>	Check to enable Port Forwarding function.
<b>IP Address</b>	Enter the IP address in the field.
<b>Protocol</b>	Select the protocol (TCP, UDP or Both) used to the remote system or service.
<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>Comment</b>	You may key in a description MAC address.
<b>Apply Changes</b>	After completing the settings on this page, click <b>Apply Changes</b> button to save the settings.
<b>Reset</b>	Click <b>Reset</b> button to restore to default values.
<b>Current Port Forwarding Table</b>	Shows the current Port Forwarding information.
<b>Delete Selected</b>	Click <b>Delete Selected</b> button to delete items which are selected.
<b>Delete All</b>	Click <b>Delete All</b> button to delete all the items.
<b>Reset</b>	Click <b>Reset</b> button to rest.

# VLAN

## VLAN

Entries in below table are used to config vlan settings. VLANs are created to provide the segmentation services traditionally provided by routers. VLANs address issues such as scalability, security, and network management.

### VLAN Settings

Enable VLAN

Enable	Ethernet/Wireless	WAN/LAN	Tag	VID(1~4090)	Priority	CFI
<input type="checkbox"/>	Ethernet Port1	LAN	<input type="checkbox"/>	<input type="text" value="3022"/>	<input type="text" value="7"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Ethernet Port2	LAN	<input type="checkbox"/>	<input type="text" value="3030"/>	<input type="text" value="0"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Ethernet Port3	LAN	<input type="checkbox"/>	<input type="text" value="500"/>	<input type="text" value="3"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Ethernet Port4	LAN	<input type="checkbox"/>	<input type="text" value="1"/>	<input type="text" value="0"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Wireless Primary AP	LAN	<input type="checkbox"/>	<input type="text" value="1"/>	<input type="text" value="0"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Virtual AP1	LAN	<input type="checkbox"/>	<input type="text" value="1"/>	<input type="text" value="0"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Virtual AP2	LAN	<input type="checkbox"/>	<input type="text" value="1"/>	<input type="text" value="0"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Virtual AP3	LAN	<input type="checkbox"/>	<input type="text" value="1"/>	<input type="text" value="0"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Virtual AP4	LAN	<input type="checkbox"/>	<input type="text" value="1"/>	<input type="text" value="0"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Ethernet Port5	WAN	<input type="checkbox"/>	<input type="text" value="1"/>	<input type="text" value="0"/>	<input checked="" type="checkbox"/>

Apply Changes

Reset

#### Enable VLAN

Entries in below table are used to config vlan settings. VLANs are created to provide the segmentation services traditionally provided by routers. VLANs address issues such as scalability, security, and network management.

# Administration

## Password

### Password

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

### Password Setup

User Name

New Password

Confirmed Password

(Maximum characters is 30)



<b>User Name</b>	To set up the login username to protect the Wireless Router configuration accessing via web browser. Empty user name and password will disable the protection. It's strongly recommended to assign a set of password for further security.
<b>New Password</b>	To set up the login password to protect the Wireless Router configuration accessing via web browser. Maximum input is 30 alphanumeric characters (case sensitive.)
<b>Confirmed Password</b>	Key in the password again to confirm.

# NAS

## NAS

Network-attached storage (NAS) allows user access data through network service. user can use FTP, Samba solutions to share USB storage device in the networks.

### FTP Server Settings

**FTP Service Enable**

FTP Port

Login Timeout  (0: Use default setting 120 seconds)

Stay Timeout  (0: Use default setting 300 seconds)

Login Users

Share Mode

**Use anonymous login**

User Name

Password

<b>FTP Service Enable</b>	Network attached storage (NAS) allows user access data through network service. User can use FTP, Samba solutions to share USB storage device in the networks.
<b>FTP Port</b>	Enter the FTP port here.
<b>Login Timeout</b>	Setup the login time limit seconds here.
<b>Stay Timeout</b>	Setup the login stay time limit seconds here.
<b>Login Users</b>	Setup the login user limit numbers here.
<b>Share Mode</b>	To control the data authentication for login user.
<b>Use anonymous login</b>	Do not need to login with a s username or password. If you do not want to use anonymous login, please enter the user name and password in the field.

## Media Share

### Media Service

The media server allows user sharing multi media files on local networks.

#### DLNA Media Server

**Enable Media Server**

**Share Folder Name**  (Multimedia share folder.)

<b>Enable Media Server</b>	The media server allows user sharing multi-media files on local networks.
<b>Share Folder Name</b>	Enter the file name that shared on the local area network here.

## NTP

### NTP

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

#### Time Zone Setting

**Current Time** Yr  Mon  Day  Hr  Mn  Sec

**Time Zone Select**

**Enable NTP client update**

**Automatically Adjust Daylight Saving**

**NTP server**

(Manual IP Setting)

<b>Current Time</b>	Enter the current time of this wireless router or click the <b>Copy Computer Time</b> button to synchronize the time with the connected computer automatically.
<b>Time Zone Select</b>	Select the local time zone from the pull-down menu.
<b>Enable NTP client update</b>	Check to enable <b>NTP</b> (Network Time Protocol Server) <b>client update</b> function.
<b>Automatically Adjust</b>	Check the box to enable this function.

<b>Daylight Saving</b>	
<b>NTP server Manual IP setting</b>	You may choose to select NTP server from the pull-down menu or enter an IP address of a specific server manually.
<b>Apply Changes</b>	After completing the settings on this page, click <b>Apply Changes</b> button to save current settings.
<b>Refresh</b>	Click <b>Refresh</b> button to renew current time.

## Dynamic DNS Setting

### 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.

### Dynamic DNS Setting

**Enable DDNS**

**Service Provider**

DynDNS ▾

**Domain Name**

host.dyndns.org

**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](#)

<b>Enable DDNS</b>	Check to enable the DDNS function.
<b>Service Provider</b>	Select the desired DDNS Service Provider DynDNS, TZO or Oray from the pull-down list.
<b>Domain Name</b>	Here shows the domain name of the service provider.
<b>User Name/Email</b>	Enter your email that you registered in service provider website. (You can refer to below Note information to apply a account form the service provider website.)
<b>Password/Key</b>	Enter your passwords that you registered in service provider website. Maximum input is 30 alphanumeric characters (case sensitive).
<b>Apply Changes</b>	After completing the settings on this page, click Apply Changes button to save the settings.
<b>Reset</b>	Click Reset button to restore to default values.

## Upgrade Firmware

### Upgrade Firmware

This page allows you upgrade the Access Point firmware to new version. Please note, do not power off the device during the upload because it may crash the system.

### Upgrade Firmware

<b>Firmware Version</b>	v2.2.2
<b>Select File</b>	<input type="text"/> <input type="button" value="Browse..."/>
	<input type="button" value="Upload"/> <input type="button" value="Reset"/>

<b>Firmware Version</b>	Here display the latest firmware version.
<b>Select File</b>	Click the <b>Browse</b> button to find and open the firmware file (the browser will display to correct file path.)
<b>Upload</b>	Click the <b>Upload</b> button to perform.
<b>Reset</b>	Click <b>Reset</b> button 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

<b>Save Settings to File</b>	<input type="button" value="Save..."/>
------------------------------	--

### Import Settings

<b>Load Settings from File</b>	<input type="text"/> <input type="button" value="Browse..."/> <input type="button" value="Upload"/>
--------------------------------	---

### Load Factory Default

<b>Reset Settings to Default</b>	<input type="button" value="Reset"/>
----------------------------------	--------------------------------------

<b>Save Settings to File</b>	Click the <b>Save</b> button to save the current settings file in the PC.
<b>Load Settings form File</b>	Click the <b>Browse</b> button to find and open the previous saved file (the browser will display to correct file path.) Then, click <b>Upload</b> button to upload the previous file.
<b>Reset Settings to Default</b>	Click <b>Reset</b> button to set the device back to default settings.



## Statistics

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

### Statistics

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

#### Wireless LAN

Sent Packets	3642
Received Packets	130019

#### Ethernet LAN

Sent Packets	980
Received Packets	1192

#### Ethernet WAN

Sent Packets	2115
Received Packets	0

Refresh

## System Log

### System Log

This page can be used to set remote log server and show the system log.

#### System Log

Enable Log

system all

Enable Remote Log

Wireless  DoS

Log Server IP Address

Apply change

Refresh

Clear

<b>Enable Log</b>	Check to enable logging function.
<b>System all</b>	Activates all logging functions.
<b>Wireless</b>	Only logs related to the wireless LAN will be recorded.
<b>DoS</b>	Only logs related to the DoS protection will be recorded.
<b>Enable Remote Log</b>	Only logs related to the Remote control will be recorded.
<b>Log Server IP address</b>	Only logs related to the server will be recorded.
<b>Apply Changes</b>	After completing the settings on this page, click <b>Apply Changes</b> button to save current settings.
<b>Refresh</b>	Click <b>Refresh</b> button to renew the logs.
<b>Clear</b>	Click <b>Clear</b> button to delete the logs.

## Reboot

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

**Reboot**

This page is used to restart.

**System Restart**

**Restart**

# 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.

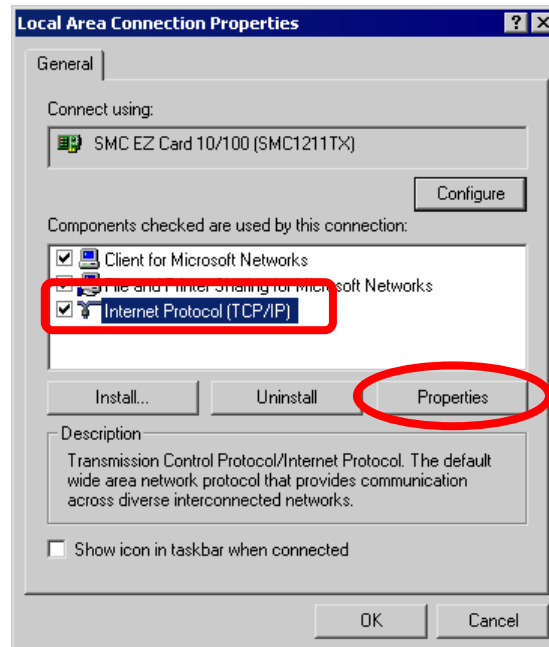
- By default, the Wireless Router will act as a DHCP Server, automatically providing a suitable IP address (and related information) to each PC when the PC boots.
- For all non-server versions of Windows, the default TCP/IP setting is to act as a DHCP client.

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

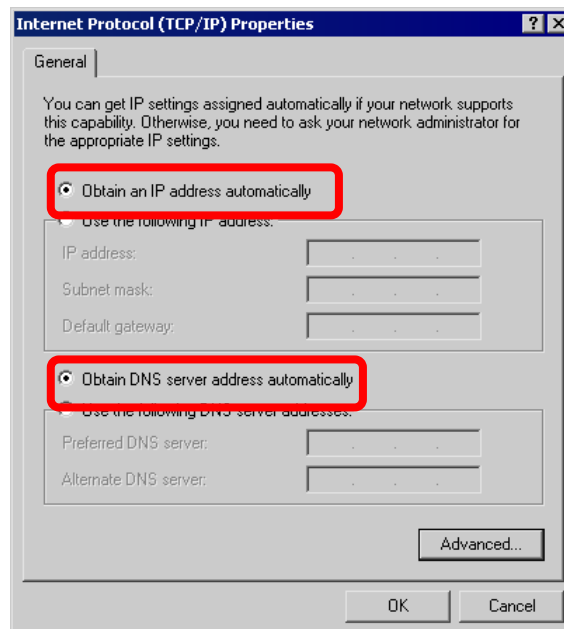
- The *Gateway* must be set to the IP address of the Wireless Router.
- The *DNS* should be set to the address provided by your ISP (Internet Service Provider.)

## Checking TCP/IP Settings - Windows 2000

1. Go to *Start > 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 *Internet Protocol (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** and **Obtain DNS server 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 automatically.

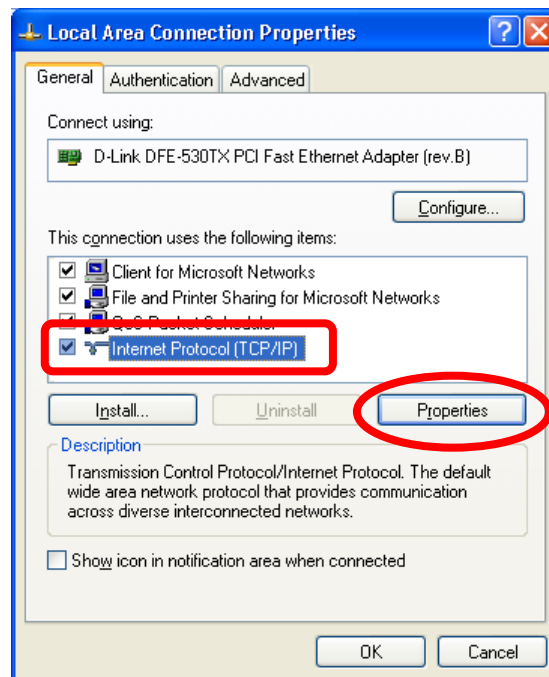
## Using a fixed IP Address ("Use the following IP Address")

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

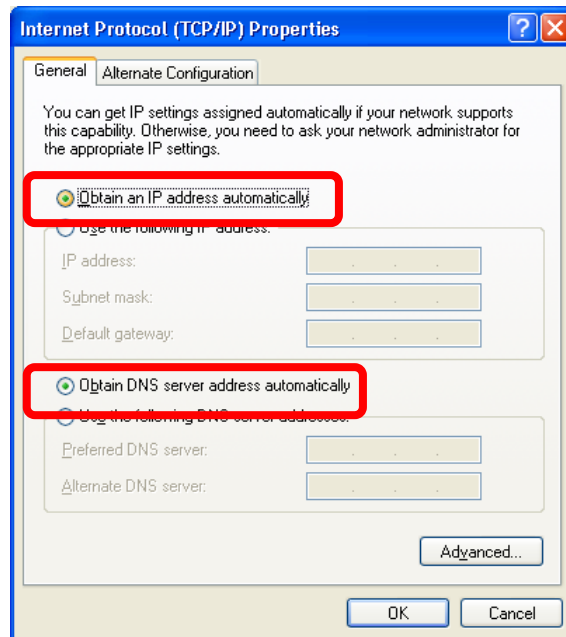
- Enter the Wireless Router 's IP address in the **Default gateway** field. (Your LAN administrator can advise you of the IP address they assigned to the Wireless Router.)
- If the **DNS Server** fields are empty, select **Use the following DNS server addresses**, and enters the DNS address or addresses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

# Checking TCP/IP Settings - Windows XP

1. Go to **Start > Control Panel > Network Connection**.
2. Right click the **Local Area Connection** icon and choose **Properties**. You should see a screen like the following:



3. Select the **Internet Protocol (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** and **Obtain DNS server 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.

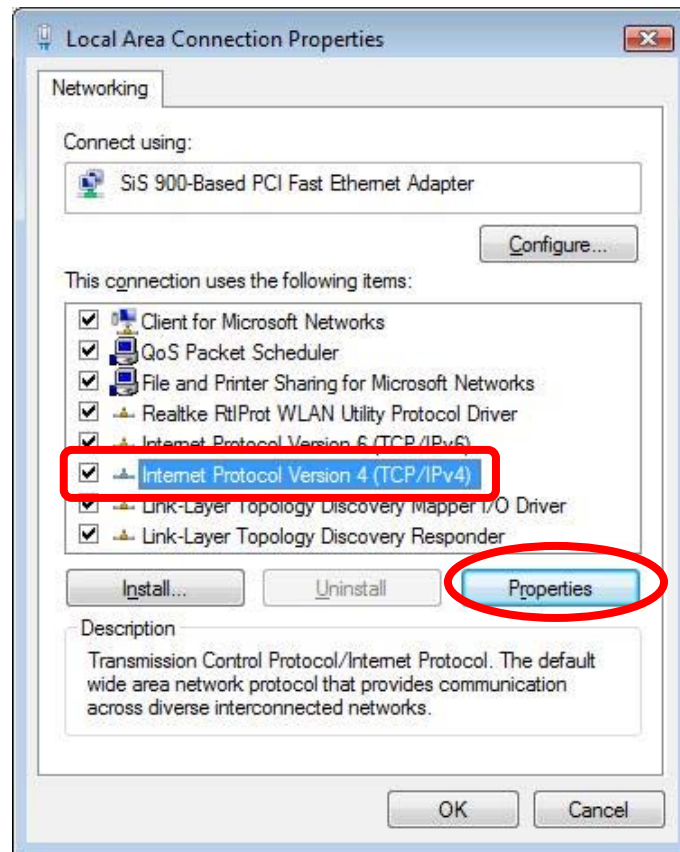
### Using a fixed IP Address ("Use the following IP Address")

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

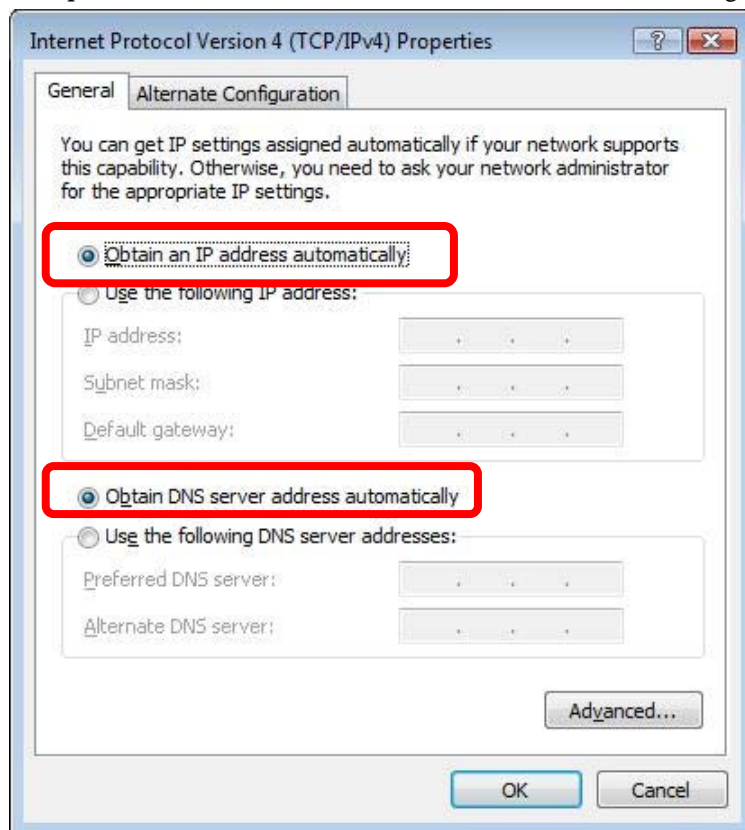
- In the **Default gateway** field, enter the Wireless Router 's IP address. Your LAN administrator can advise you of the IP address they assigned to the Wireless Router.
- If the **DNS Server** fields are empty, select **Use the following DNS server addresses**, and enters the DNS address or addresses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

## Checking TCP/IP Settings - Windows Vista

1. Go to **Start > Control Panel > Network and Internet > Network and Sharing Center > Manage Network Connections > Local Area Connection**.
2. Right click the **Local Area Connection** icon and choose **Properties**. You should see a screen like the following:



3. Select the **Internet Protocol Version 4(TCP/IPv4)** or **6 (TCP/IPv6)** 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** and **Obtain DNS server 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.

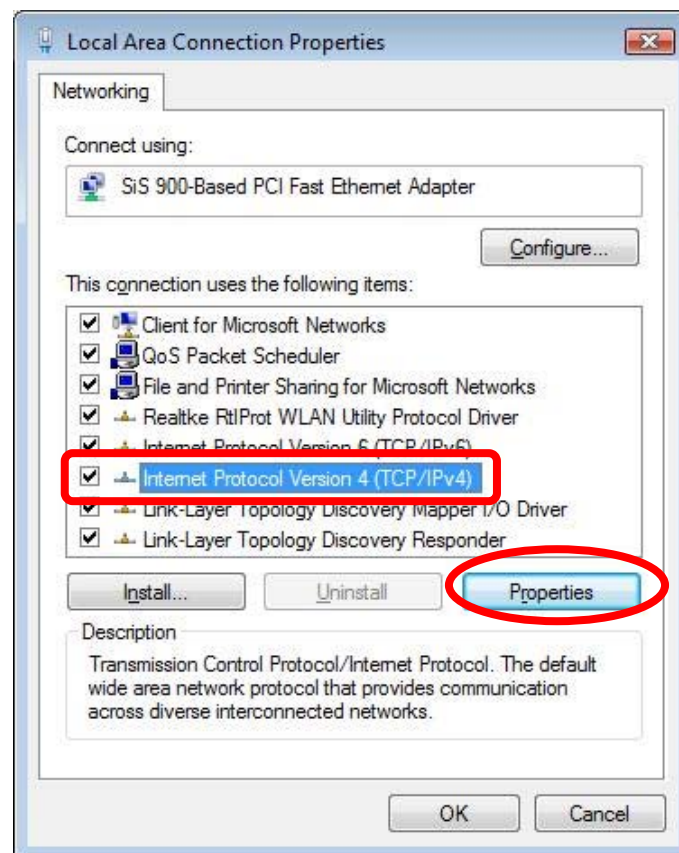
## Using a fixed IP Address ("Use the following IP Address")

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

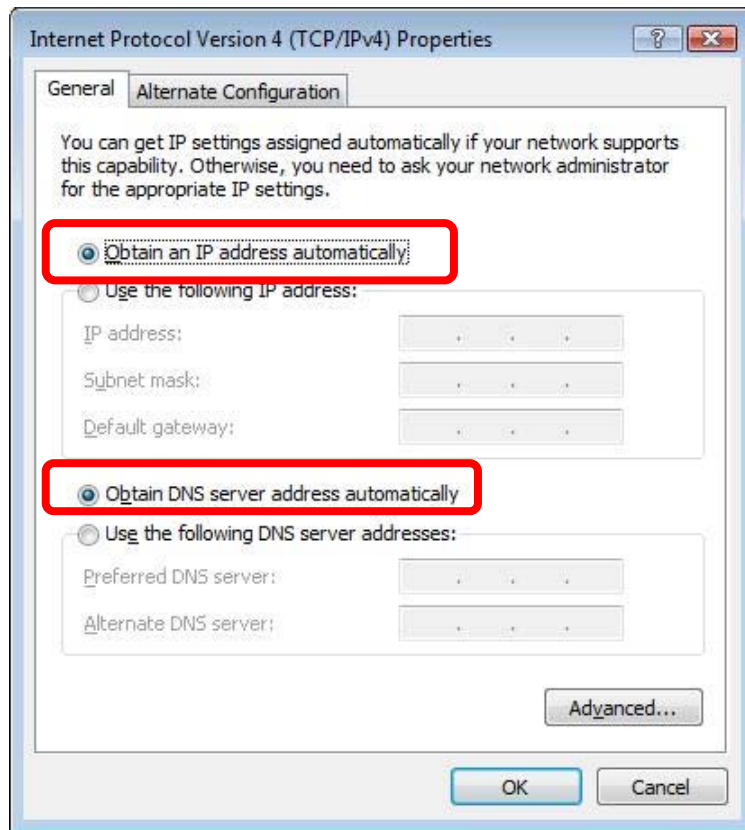
# Checking TCP/IP Settings - Windows 7

1. Go to **Start > Control Panel > Network and Sharing Center > Manage Network Connections > Local Area Connection**.
2. Right click the **Local Area Connection** icon and choose **Properties**. You should see a screen like the following:



3. Select the **Internet Protocol Version 4(TCP/IPv4) or 6 (TCP/IPv6)** 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** and **Obtain DNS server 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. Your LAN administrator can advise you of the IP address they assigned to the Wireless Router.
- If the **DNS Server** fields are empty, select **Use the following DNS server addresses**, and enters the DNS address or addresses provided by your ISP, then click **OK**.

## Internet Access

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

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

## **For Windows 2000**

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

## **For Windows XP**

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

## **For Windows Vista**

1. Select *Start* menu > *Control Panel* > *Network and Internet* > *Network and Sharing Center*.
2. Select *Set up a connection or network*.
3. Select *Connect to the Internet* and click *Next* to continue.
4. Select *Broadband (PPPoE)*.
5. Enter *User name* and *Password* that provided by the ISP, then click *Connect* to make a connection.

## **For Windows 7**

1. Select *Start* menu > *Control Panel* > *Network Sharing Center*.
2. Select *Set up a new connection or network*.
3. Select *Connect to the Internet* and click *Next* to continue.
4. Select *Broadband (PPPoE)*.
5. Enter *User name* and *Password* that provided by the ISP, then click *Connect* to make a connection.

## Accessing AOL

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

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

## Macintosh Clients

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

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

### **Note:**

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

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

## Linux Clients

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

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

### **Fixed IP Address**

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

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

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

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

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

- Use the "Deactivate" and "Activate" buttons, if available.
- OR, restart your system.

## Other Unix Systems

To access the Internet via the Wireless Router:

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

## Wireless Station Configuration

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

<b>Mode</b>	The mode must be set to <i>Infrastructure</i> .
<b>SSID (ESSID)</b> (Extended Service Set Identifier)	The network name must match the value used on the Wireless Router. <i>Note! The SSID(service set identifier) is case- sensitive.</i>
<b>Disable</b>	If there is no security is enabled on the Wireless Router, the security of each station should be disabled as well. And, you can connect the Wireless Router without security, but it is NOT recommended.
<b>WEP</b> <b>Open System/ Shared Key/ Auto</b>	By default, WEP on the Wireless Router is disabled. Shared Key only supports WEP as encryption method. AUTO(Open/Shared) means AP can accept STA connect to it using OPEN-WEP or SHARED-WEP. <ul style="list-style-type: none"> <li>• If WEP remains disabled on the Wireless Router, all stations must have WEP disabled.</li> <li>• If WEP is enabled on the Wireless Router, each station must use the same settings as the Wireless Router.</li> </ul>
<b>Personal (Pre-Shared Key)</b> <b>WPA</b> <b>WPA2</b> <b>WPA2-Mixed</b>	WPA-PSK(TKIP/AES)/ WPA2-PSK(TKIP/AES): If one of these securities is enabled on the Wireless Router. To make a connection, each station must use the same algorithms and pass phrase as the Wireless Router. <b>Pre-Shared Key Format:</b> There are two formats for choice to set the Pre-shared key, <b>Passphrase</b> and <b>Hex (64 characters)</b> . If <b>Hex</b> is selected, users will have to enter 64 characters string at a time. For easier configuration, the <b>Passphrase</b> (at least 8 characters) format is recommended. <b>Pre-Shared Key :</b> Pre-Shared Key serves as a password. Users may key in 8 to 63 characters string if you selected 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.
<b>Enterprise (RADIUS)</b>  <b>WPA</b> <b>WPA2</b> <b>WPA2-Mixed</b> <b>802.1x</b>	<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 RADIUS is a server that has access to a user database with authentication information. Each station must set up the RADIUS Server's IP address, port and passwords that provided by your ISP.

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

# 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>	Can't connect to the Wireless Router to configure it.
<b>Solution 1:</b>	<p>Check the following:</p> <ul style="list-style-type: none"> <li>• Check 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.</li> <li>• If your PC is set to "Obtain an IP address automatically" (DHCP client), please restart it.</li> <li>• 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.</li> </ul> <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. You can check Chapter 4: PC Configuration- TCP/IP settings for reference.</p>

## Internet Access

<b>Problem 1:</b>	When I enter a URL or IP address I get a time out error.
<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</li> </ul>

	<p>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.)</p> <ul style="list-style-type: none"> <li>• If the Wireless Router is configured correctly, check your Internet connection (ADSL/Cable modem) to see that it is working correctly.</li> </ul>
<b>Problem 2:</b>	Some applications do not run properly when using the Wireless Router.
<b>Solution 2:</b>	<p>The Wireless Router processes the data passing through it, so it is not transparent. Use the <i>Filter Settings</i> feature to allow the use of Internet applications, which do not function correctly.</p> <p>If this does solve the problem you can use the <i>DMZ</i> function. This should work with almost every application, but:</p> <ul style="list-style-type: none"> <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>	My PC can't locate the Wireless Router.
<b>Solution 1:</b>	<p>Check the following:</p> <ul style="list-style-type: none"> <li>• <b>Mode:</b> Your PC is set to <i>Infrastructure Mode</i>. (Access Points are always in <i>Infrastructure Mode</i>)</li> <li>• <b>SSID:</b> The SSID(service set identifier) on your PC and the Wireless Router are the same. Remember that the SSID (service set identifier) is case-sensitive. So, for example "<u>W</u>orkgroup" does NOT match "<u>w</u>orkgroup."</li> <li>• <b>Security:</b> Both your PC and the Wireless Router must have the same setting for security. <ul style="list-style-type: none"> <li>✧ <b>Disabled:</b> The default setting for the Wireless Router security is disabled, so your wireless station should also has security disabled.</li> <li>✧ <b>Enabled:</b> If security is enabled on the Wireless Router, your PC must have security enabled, and the key must be matched.</li> <li>✧ It's strongly suggest to set up security that could prevent any unauthorized accessing to your wireless network. Setting WPA2 security is recommended that offers stronger security than WEP. Both your computer and the Wireless Router must have the same settings for security.</li> </ul> </li> <li>• <b>Channel:</b> The wireless local area network is activated and configured by default. If necessary, please check and match channel for the terminal, for example, your notebook. Both your computer (client) and the Wireless Router must set to the same channel for connection.</li> </ul>
<b>Problem 2:</b>	Wireless connection speed is very slow.
<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</li> </ul>

	<p>Wireless Router. 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.</p> <ul style="list-style-type: none"><li>● <b>Wireless Channels:</b> If interference is the problem, changing to another channel may show a well improvement.</li><li>● <b>Radio Interference:</b> Other devices may be causing interference. You can try to turn off other wireless devices, 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 (Basic Service Set)

BSS (Basic Service Set)

A group of wireless stations and a single access point, all using the same SSID(service set identifier), form a Basic Service Set (BSS).

Using the same SSID (service set identifier) 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(Extended Service Set)).
- ESS: In Infrastructure mode, one or more BSS(Basic Service Set) can set up a ESS (Extended Service Set). User can access and roaming BSS data and the access point should be set to the same ESSID(Extended Service Set Identifier) to allow roaming.

### Note to US model owner:

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

## Security

### WEP

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

**If WEP is used, the wireless stations and the access point must have the same security settings for each of the following:**

<b>WEP</b>	64 Bits, 128 Bits.
<b>Key</b>	For 64 Bits encryption, the Key value must match. For 128 Bits encryption, the Key value must match.
<b>WEP Authentication</b>	Open System or Shared Key.

## WPA/ WPA2/ WPA-Mixed

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

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

## 802.1x

With **802.1x** authentication, a wireless PC can join any network and receive any messages that are not encrypted, however, additional setup for **RADIUS** to issue the WEP key dynamically will be required. RADIUS is an authentication, authorization, and accounting client-server protocol. The client is a network access server that desires to authenticate its links. The server has access to a user database with authentication information.

# Wireless LAN Configuration

To allow wireless stations(STA) to access the access point(AP), the wireless stations and the access point must use the same settings, as follows:

<b>Mode</b>	The mode must be set to <i>Infrastructure</i> .
<b>SSID (ESSID)</b> (Extended Service Set Identifier)	The network name must match the value used on the Wireless Router. <i>Note! The SSID(service set identifier) is case- sensitive.</i>
<b>Disable</b>	If there is no security is enabled on the Wireless Router, the security of each station should be disabled as well. And, you can connect the Wireless Router without security, but it is NOT recommended.
<b>WEP</b> <b>Open System/</b> <b>Shared Key/</b> <b>Auto</b>	By default, WEP on the Wireless Router is disabled. Shared Key only supports WEP as encryption method. AUTO(Open/Shared) means AP can accept STA connect to it using OPEN-WEP or SHARED-WEP. <ul style="list-style-type: none"> <li>• If WEP remains disabled on the Wireless Router, all stations must have WEP disabled.</li> <li>• If WEP is enabled on the Wireless Router, each station must use the same settings as the Wireless Router.</li> </ul>
<b>Personal (Pre-Shared Key)</b> <b>WPA</b> <b>WPA2</b> <b>WPA2-Mixed</b>	WPA-PSK(TKIP/AES)/ WPA2-PSK(TKIP/AES): If one of these securities is enabled on the Wireless Router. To make a connection, each station must use the same algorithms and pass phrase as the Wireless Router.

	<p><b>Pre-Shared Key Format:</b> There are two formats for choice to set the Pre-shared key, <b>Passphrase</b> and <b>Hex (64 characters)</b>. If <b>Hex</b> is selected, users will have to enter 64 characters string at a time. For easier configuration, the <b>Passphrase</b> (at least 8 characters) format is recommended.</p> <p><b>Pre-Shared Key:</b> Pre-Shared Key serves as a password. Users may key in 8 to 63 characters string if you selected 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>
<p><b>Enterprise (RADIUS)</b> <b>WPA</b> <b>WPA2</b> <b>WPA2-Mixed</b> <b>802.1x</b></p>	<p><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 RADIUS is a server that has access to a user database with authentication information. Each station must set up the RADIUS server's IP address, port and passwords that provided by your ISP.</p>