

# FIBRAIN FSR-R2

## WLAN AP ROUTER



## User's Manual

# Table of Contents

	FIBRAIN FSR-R2 .....	1
	WLAN AP ROUTER.....	1
	User's Manual.....	1
<b>1</b>	<b>Introduction.....</b>	<b>6</b>
	Features .....	6
	Device Requirements .....	6
	Using this Document .....	7
	Getting Support.....	7
<b>2</b>	<b>Getting to know the device .....</b>	<b>8</b>
	Computer / System requirements.....	8
	Package Contents .....	8
	LED meanings & activations.....	9
<b>3</b>	<b>Computer configurations under     different OS, to obtain IP address     automatically.....</b>	<b>13</b>
	For Windows 98SE / ME / 2000 / XP .....	13
	For Windows Vista-32/64.....	17
	For Windows 7-32/64 .....	22
<b>4</b>	<b>Connecting your device .....</b>	<b>26</b>
	Connecting the Hardware .....	26
	802.11n WLAN Router Configuration .....	28
	Wireless Connection.....	33
<b>5</b>	<b>What the Internet/WAN access of your     own Network now is .....</b>	<b>35</b>
	Internet/WAN access is the DHCP client.....	37
	Internet/WAN access is the Static IP.....	38
	Internet/WAN access is the PPPoE client .....	40
<b>6</b>	<b>Getting Started with the Web pages .....</b>	<b>41</b>
	Accessing the Web pages .....	41
	Testing your Setup.....	43
	Default device settings .....	43
<b>7</b>	<b>Wide Area Network (WAN) Settings .....</b>	<b>45</b>
	Static IP (Fixed IP address assignment).....	46
	DHCP.....	47
	PPPoE .....	48
<b>8</b>	<b>Local Area Network (LAN) Settings.....</b>	<b>49</b>

<b>9</b>	<b>Routing Settings</b> .....	<b>50</b>
	Add Routing Rule.....	50
	Example of Routing Rule .....	51
<b>10</b>	<b>DHCP Server Settings</b> .....	<b>52</b>
<b>11</b>	<b>DDNS Settings</b> .....	<b>53</b>
<b>12</b>	<b>MAC Address Clone Settings</b> .....	<b>54</b>
<b>13</b>	<b>VLAN Settings</b> .....	<b>55</b>
<b>14</b>	<b>Wireless - Basic Setting</b> .....	<b>57</b>
	WLAN 1 Settings .....	59
	SSID Settings.....	60
	WEP Settings.....	61
	WPA Pre-shared Key / WPA2 Pre-shared Key Settings .....	62
	WPA / WPA2 Radius Settings.....	63
<b>15</b>	<b>Wireless - Advanced Setting</b> .....	<b>64</b>
<b>16</b>	<b>Wireless - WDS Setting</b> .....	<b>66</b>
<b>17</b>	<b>Wireless - Universal Repeater Setting</b> .....	<b>67</b>
<b>18</b>	<b>Wireless - WPS Setting</b> .....	<b>68</b>
<b>19</b>	<b>Security - Firewall Setting</b> .....	<b>69</b>
<b>20</b>	<b>Security - ACCESS CONTROL LIST (ACL) SETUP Setting</b> .....	<b>71</b>
	Add Access Control List (ACL) Rule .....	72
	Example: Filter and block MSN usage.....	73
<b>21</b>	<b>Security - MAC Access Control Setting</b> .....	<b>74</b>
	Add MAC Access Control Rule.....	75
	Example: Bind IP to a MAC .....	76
<b>22</b>	<b>Security - Web Filtering Setting</b> .....	<b>77</b>
	Add Web Filtering Rule .....	78
	Example: Block a URL with Keyword.....	79
<b>23</b>	<b>Bandwidth - INTELLIGENT DYNAMIC BANDWIDTH MANAGEMENT</b> .....	<b>80</b>
	DBM - WAN 1 Settings.....	81
	Modify Bandwidth Management Group Rule .....	82
	Add Static Bandwidth Management (SBM) Rule .....	83
<b>24</b>	<b>Bandwidth - Throughput Optimizer</b> .....	<b>84</b>
<b>25</b>	<b>Bandwidth - TurboNAT</b> .....	<b>85</b>
<b>26</b>	<b>Applications - Port Range Forward</b> .....	<b>86</b>

	DMZ - WAN 1 Settings .....	88
	Port Range Forwarding Settings .....	88
	Add Port Range Forwarding Rule .....	89
<b>27</b>	Applications - Virtual Hosts .....	90
	Add Virtual Host Rule .....	91
<b>28</b>	Applications - Streaming / VPN .....	92
	Streaming Settings .....	92
	Streaming Settings .....	93
	VPN Pass-through Settings .....	93
<b>29</b>	Applications - UPnP / NAT-PMP .....	94
<b>30</b>	Admin - Management .....	95
	Administration Interface Settings .....	96
	Reboot Settings .....	96
	Configuration Settings .....	97
	Firmware Upgrade Settings .....	97
	APS Settings .....	98
<b>31</b>	Admin - System Utilities .....	99
	Ping Settings .....	100
	ARPing (Within the same broadcasting domain) Settings .....	100
	Trace Route Settings .....	101
<b>32</b>	Admin - TIME SETUP .....	102
<b>33</b>	Status - Router .....	103
	Router Information Settings .....	104
	WAN Settings .....	104
	LAN Settings .....	105
	Wireless Network 1 Settings .....	106
<b>34</b>	Status - User / DHCP .....	107
<b>35</b>	Status – User / Current .....	108
<b>36</b>	Status – Log .....	109
<b>A</b>	Configuring your Computers .....	110
	Configuring Ethernet PCs .....	110
<b>B</b>	IP Addresses, Network Masks, and Subnets .....	115
	IP Addresses .....	115
	Subnet masks .....	116
<b>C</b>	UPnP Control Point Software on Windows ME/XP .....	118
	UPnP Control Point Software on Windows ME .....	118

	UPnP Control Point Software on Windows XP with Firewall .....	119
<b>D</b>	Troubleshooting .....	122
	Troubleshooting Suggestions .....	122
	Diagnosing Problem using IP Utilities .....	124
<b>E</b>	Glossary .....	126

# 1 Introduction

Congratulations on becoming the owner of the Wireless Gateway. You will now be able to access the Internet using your high-speed xDSL/Cable modem connection.

This User Guide will show you how to connect your Wireless Gateway, and how to customize its configuration to get the most out of your new product.

## Features

---

The list below contains the main features of the device and may be useful to users with knowledge of networking protocols. If you are not an experienced user, the chapters throughout this guide will provide you with enough information to get the most out of your device.

Features include:

- 10/100Base-T Ethernet router to provide Internet connectivity to all computers on your LAN
- Network address translation (NAT) functions to provide security for your LAN
- Network configuration through DHCP Server and DHCP Client
- Services including IP route and DNS configuration, RIP, and IP
- IOP (Inter-Operability) with major soft-switch vendors
- SIP signaling supporting
- Supports remote software upgrades
- Plug & Play, Auto Configuration / Auto Provisioning
- User-friendly configuration program accessed via a web browser

The Wireless Gateway has the internal Ethernet switch allows for a direct connection to a 10/100BASE-T Ethernet network via an RJ-45 interface, with LAN connectivity for both the Wireless Gateway and a co-located PC or other Ethernet-based device.

## Device Requirements

---

In order to use the Wireless Gateway, you must have the following:

- One RJ-45 Broadband Internet connection via cable modem or xDSL modem
- Instructions from your ISP on what type of Internet access you will be using, and the addresses needed to set up access
- One or more computers each containing an Ethernet card (10Base-T/100Base-T network interface card (NIC))

- TCP/IP protocol for each PC
- For system configuration using the supplied
  - a. web-based program: a web browser such as Internet Explorer v7 or later. Note that version 7 of each browser is the minimum version requirement – for optimum display quality, use Internet Explorer v8



#### Note

*You do not need to use a hub or switch in order to connect more than one Ethernet PC to your device. Instead, you can connect up to four Ethernet PCs directly to your device using the ports labeled Ethernet on the rear panel.*

## Using this Document

---

### Notational conventions

- Acronyms are defined the first time they appear in the text and also in the glossary.
- For brevity, the Wireless Gateway is referred to as “the device”.
- The term *LAN* refers to a group of Ethernet-connected computers at one site.

### Typographical conventions

- *Italic* text is used for items you select from menus and drop-down lists and the names of displayed web pages.
- **Bold** text is used for text strings that you type when prompted by the program, and to emphasize important points.

### Special messages

This document uses the following icons to draw your attention to specific instructions or explanations.



#### Note

*Provides clarifying or non-essential information on the current topic.*



#### Definition

*Explains terms or acronyms that may be unfamiliar to many readers. These terms are also included in the Glossary.*



#### WARNING

*Provides messages of high importance, including messages relating to personal safety or system integrity.*

## Getting Support

---

Supplied by:  
Helpdesk Number:  
Website:

## 2 Getting to know the device

### **Computer / System requirements**

---

- 1. Pentium 200MHZ processor or above
- 2. Windows 98SE, Windows Me, Windows 2000, Windows XP, Windows Vista and Windows 7
- 3. 64MB of RAM or above
- 4. 25MB free disk space

### **Package Contents**

---

1. 802.11n WLAN Router
2. CD-ROM (Software & Manual)
3. Quick Installation Guide
4. Ethernet Cable (RJ-45)
5. Power Adapter



## LED meanings & activations

### Front Panel

The front panel contains lights called Light Emitting Diodes (LEDs) that indicate the status of the unit.



Figure 1: Front Panel and LEDs

Label	Color	Function
POWER	green	On: device is powered on Off: device is powered off
WAN	green	On: WAN link established and active Off: No LAN link Blink: Valid Ethernet packet being transferred
WLAN	green	On: WLAN link established and active Blink: Valid Wireless packet being transferred
WPS	green	Off: WPS link isn't established and active Blink: Valid WPS packet being transferred
LAN 1/2/3/4	green	On: LAN link established and active Off: No LAN link Blink: Valid Ethernet packet being transferred

### Rear and Right Panel and bottom Side

The rear and right panel and bottom side contains a *Restore Defaults* button, the ports for the unit's data and power connections.



Figure 2: Rear Panel Connections



Figure 3: Right Panel Connections

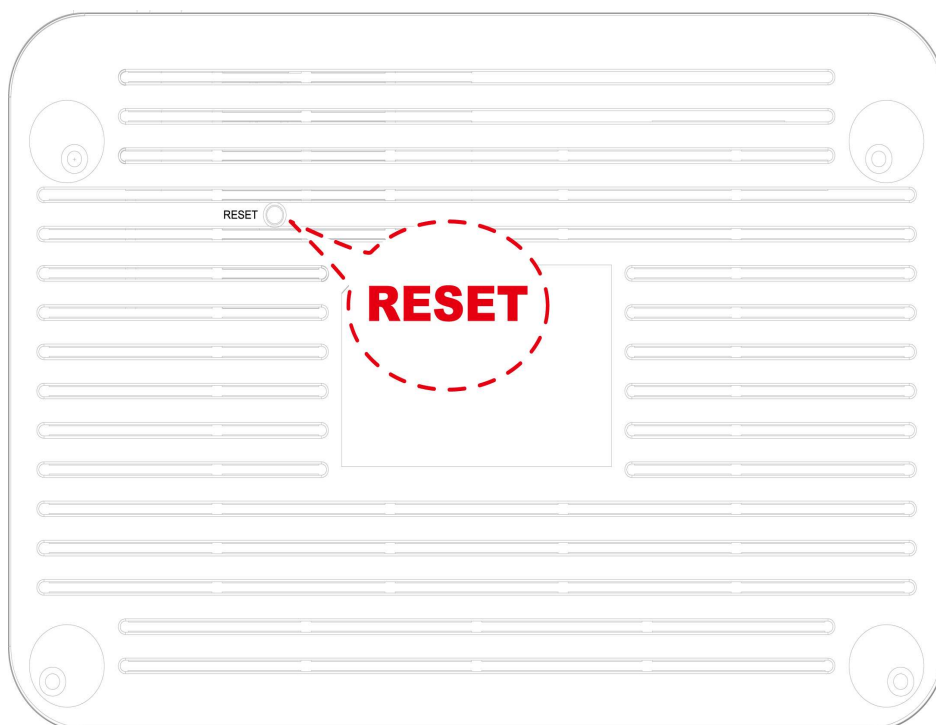


Figure 4: Bottom Side for Reset button

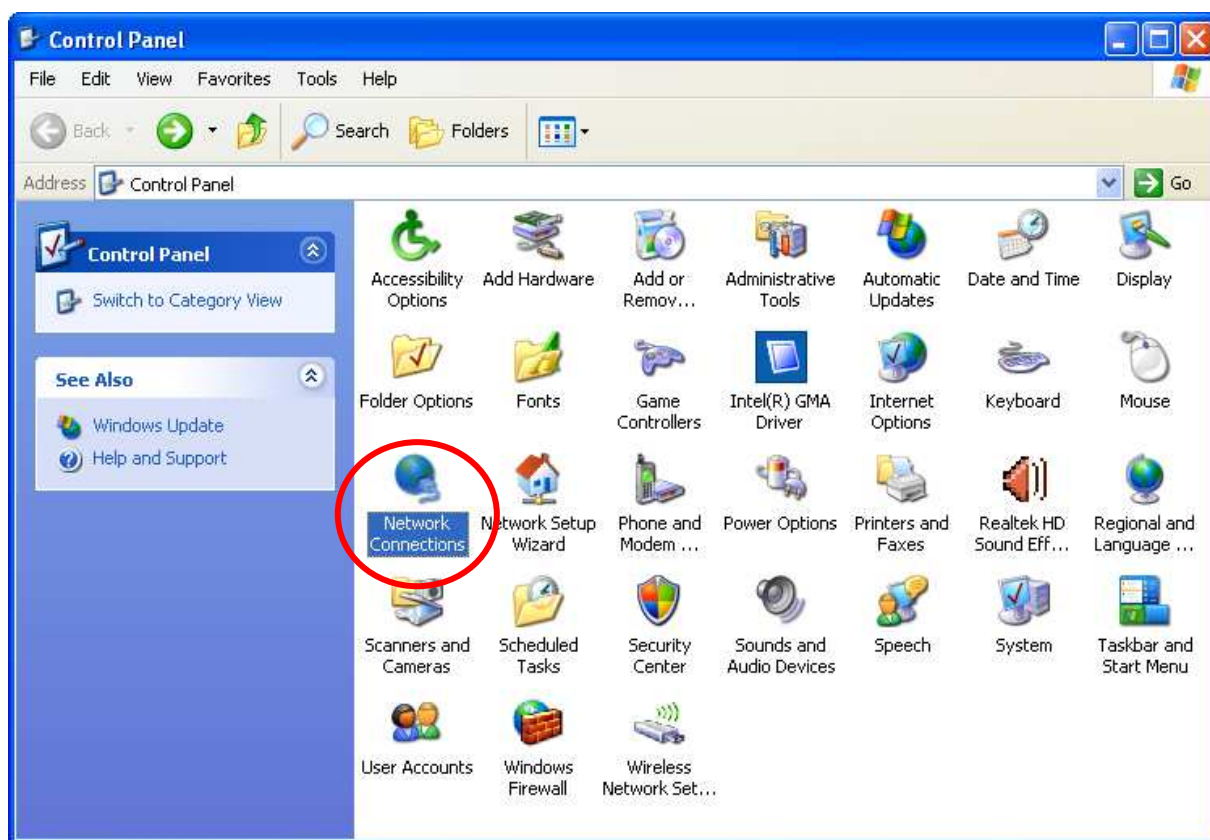
Label	Function
ANETENNA	ANETENNA
ON/OFF SWITCH	Power on/off the device
POWER	Connects to the supplied power cable
LAN 4/3/2/1	Connects the device via Ethernet to up to four PCs on your LAN
WAN	Connects the device via Ethernet to xDSL / Cable Modem
WLAN	Press this button for at least two full second to turn off/on wireless signals
WPS	<p>Press this button for at least three full seconds and the WPS LED will flash to start WPS.</p> <p>Now go to the wireless adapter or device and press its WPS button. Make sure to press the button within 120 seconds (2 minutes) after pressing the router's WPS button.</p> <p>If you are using a Wireless adapter connected to a computer, a "WPS Authentication" screen will appear. Wait until the screen says "Authentication succeeded." This may take a few minutes.</p>
RESET	<p>Reset button. RESET the 802.11n WLAN router to its default settings.</p> <p>Press this button for at least 6 full seconds to start to reset it to its default settings.</p>

### 3 Computer configurations under different OS, to obtain IP address automatically

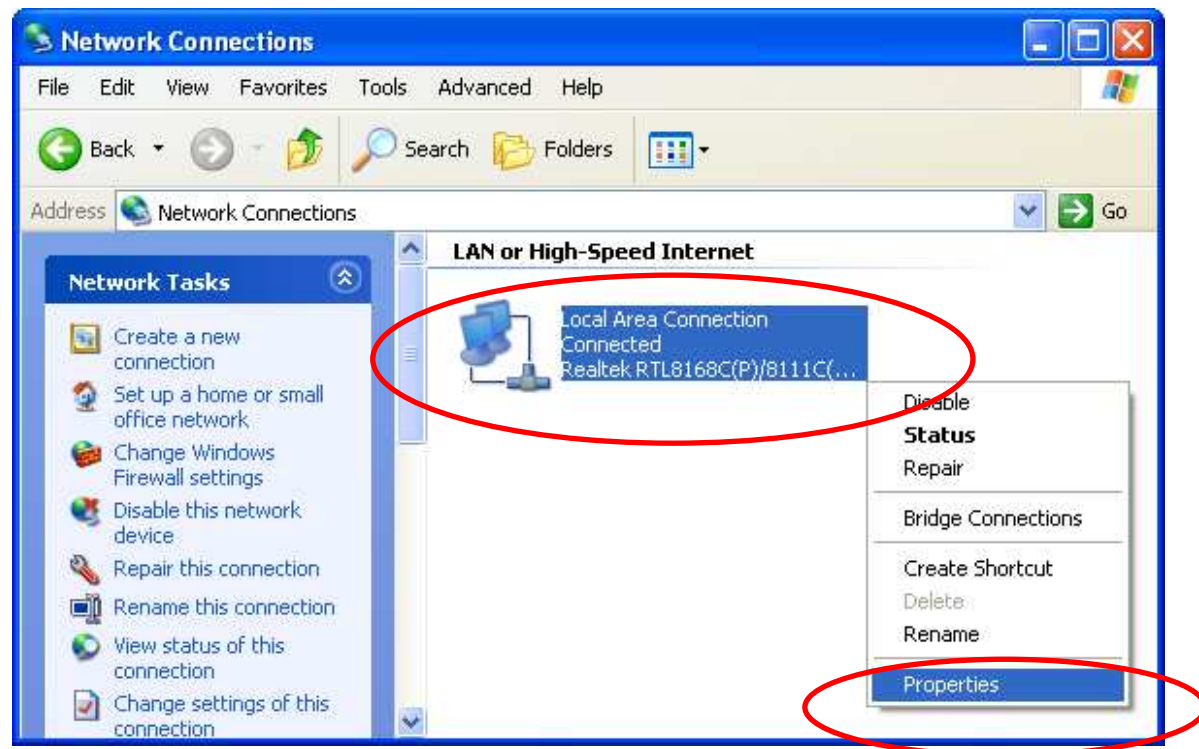
Before starting the 802.11n WLAN Router configuration, please kindly configure the PC computer as below, to have automatic IP address / DNS Server.

#### For Windows 98SE / ME / 2000 / XP

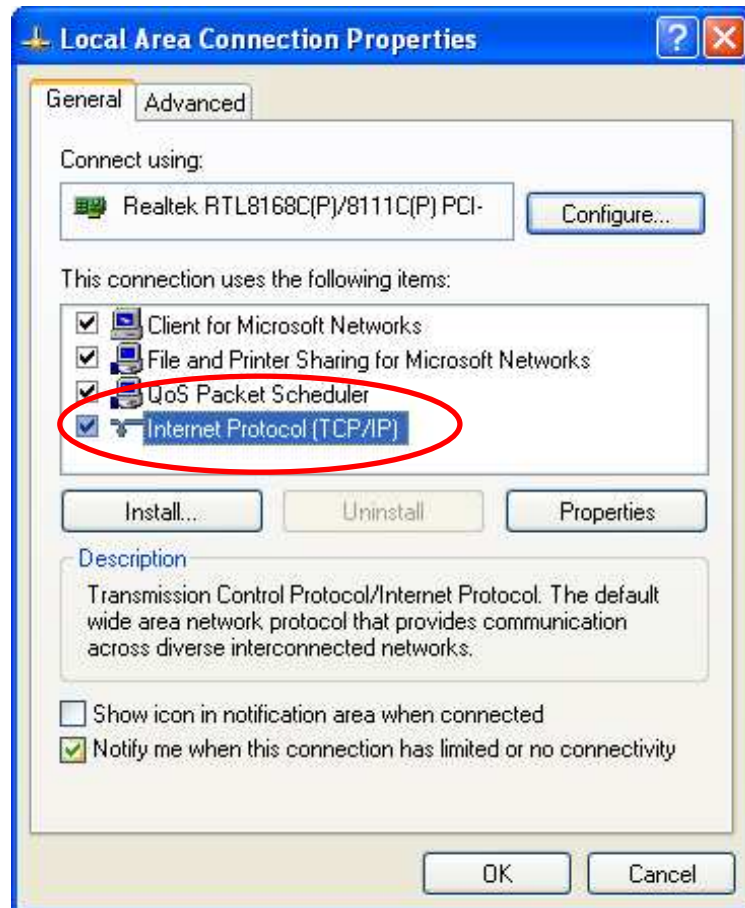
1. Click on **"Start" -> "Control Panel" (in Classic View)**. In the Control Panel, double click on **"Network Connections"** to continue.



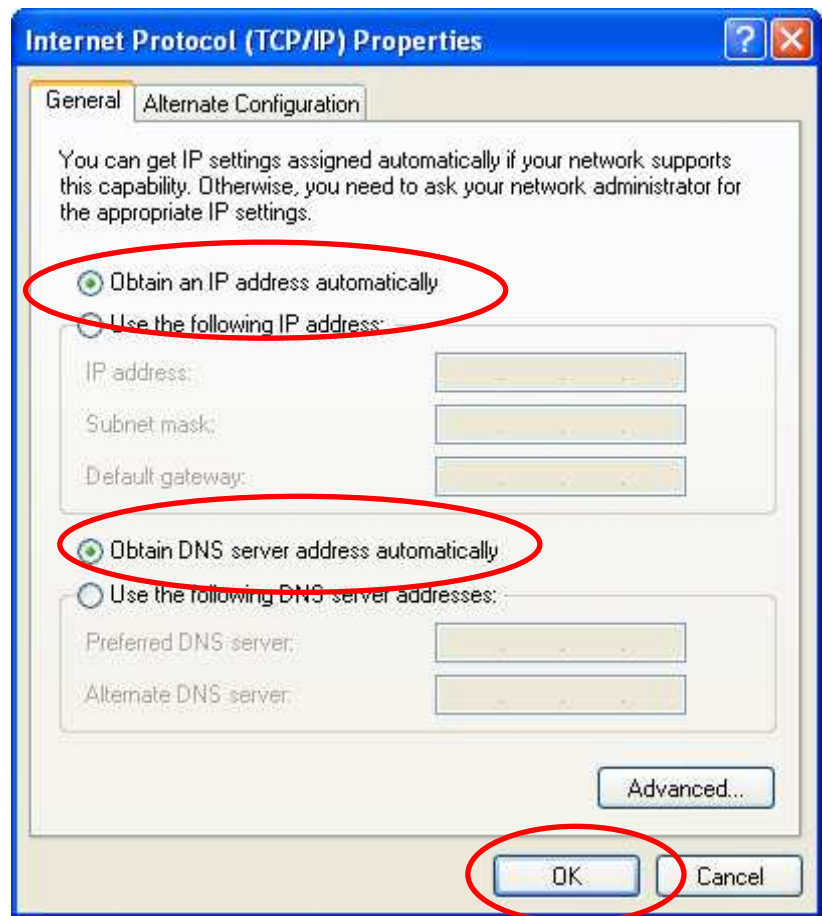
2. Single RIGHT click on "Local Area connection", then click "Properties".



3. Double click on "**Internet Protocol (TCP/IP)**".



4. Check "**Obtain an IP address automatically**" and "**Obtain DNS server address automatically**" then click on "**OK**" to continue.

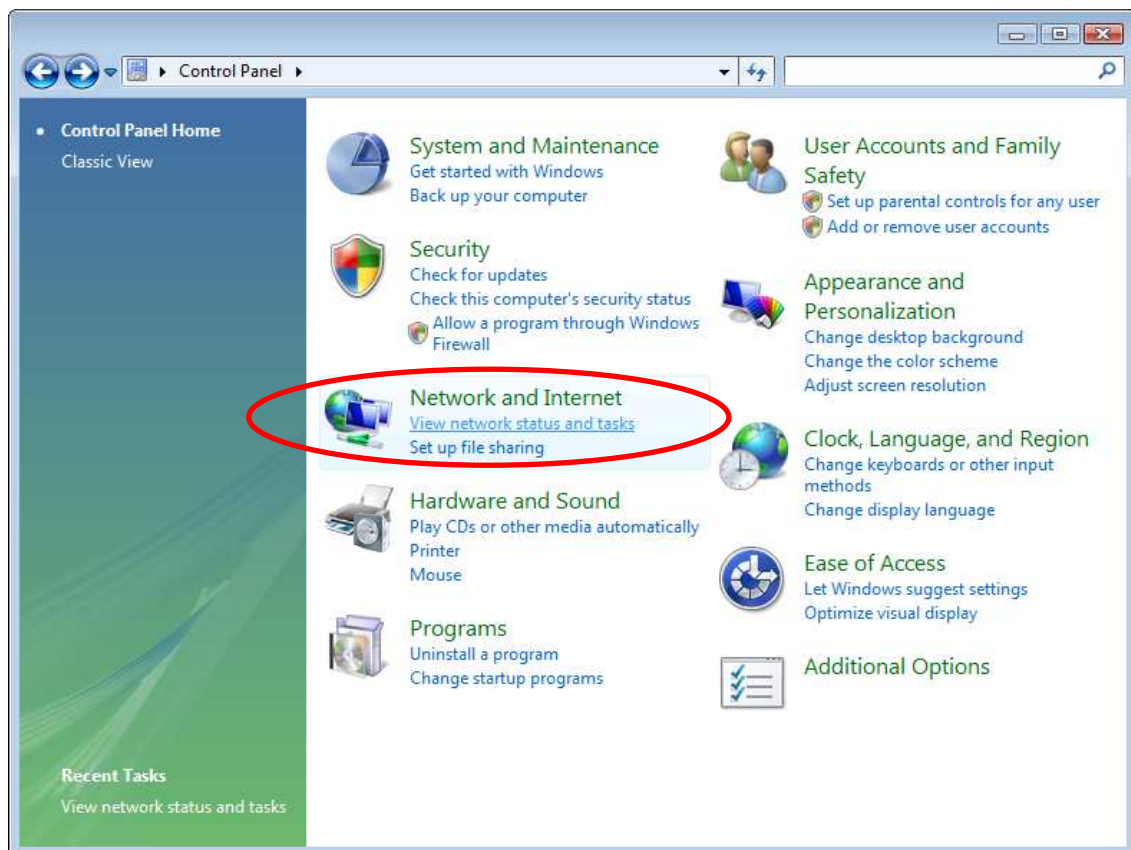


5. Click "**Show icon in notification area when connected**" (see screen image in 3. above) then Click on "**OK**" to complete the setup procedures.

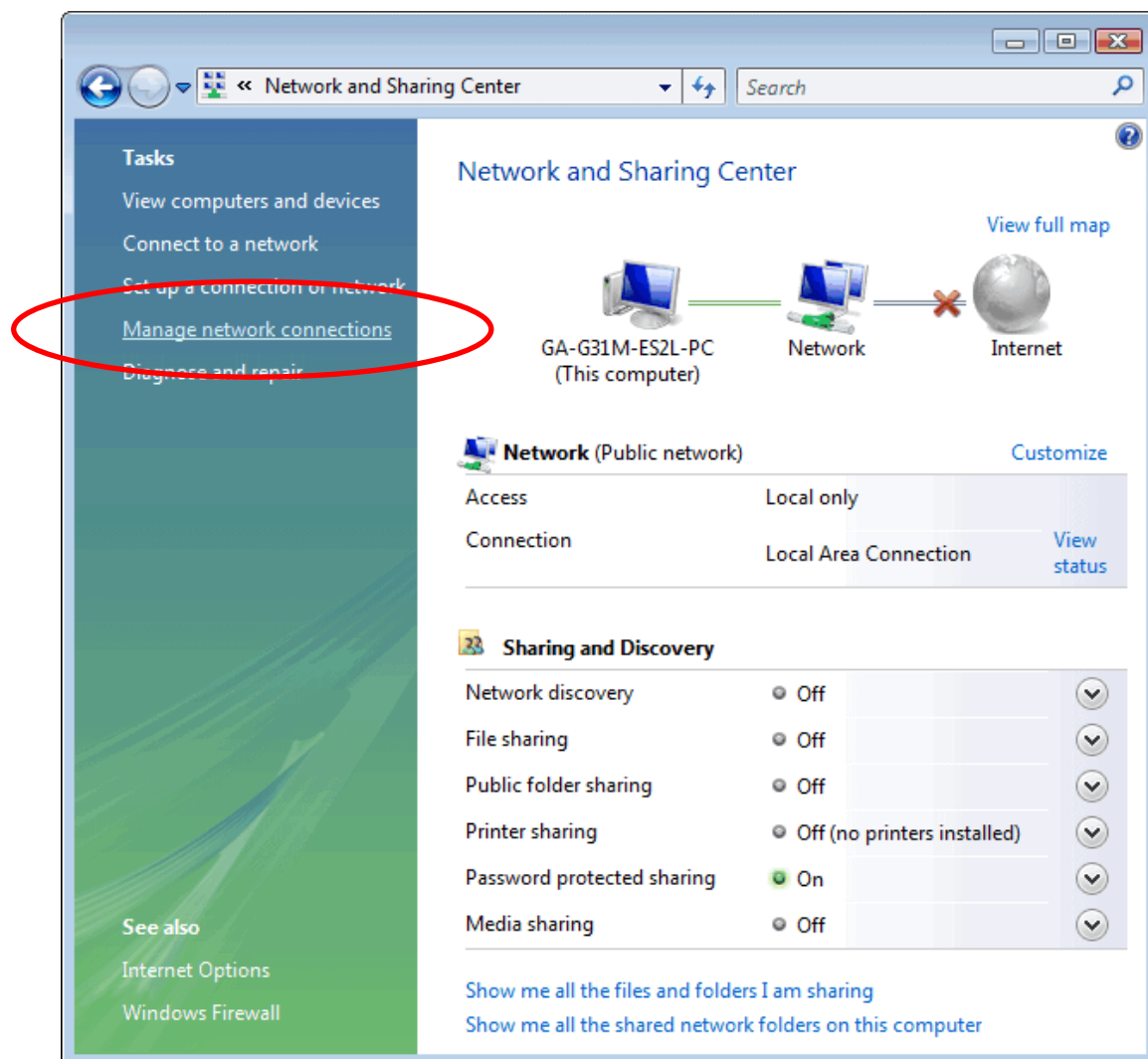


## For Windows Vista-32/64

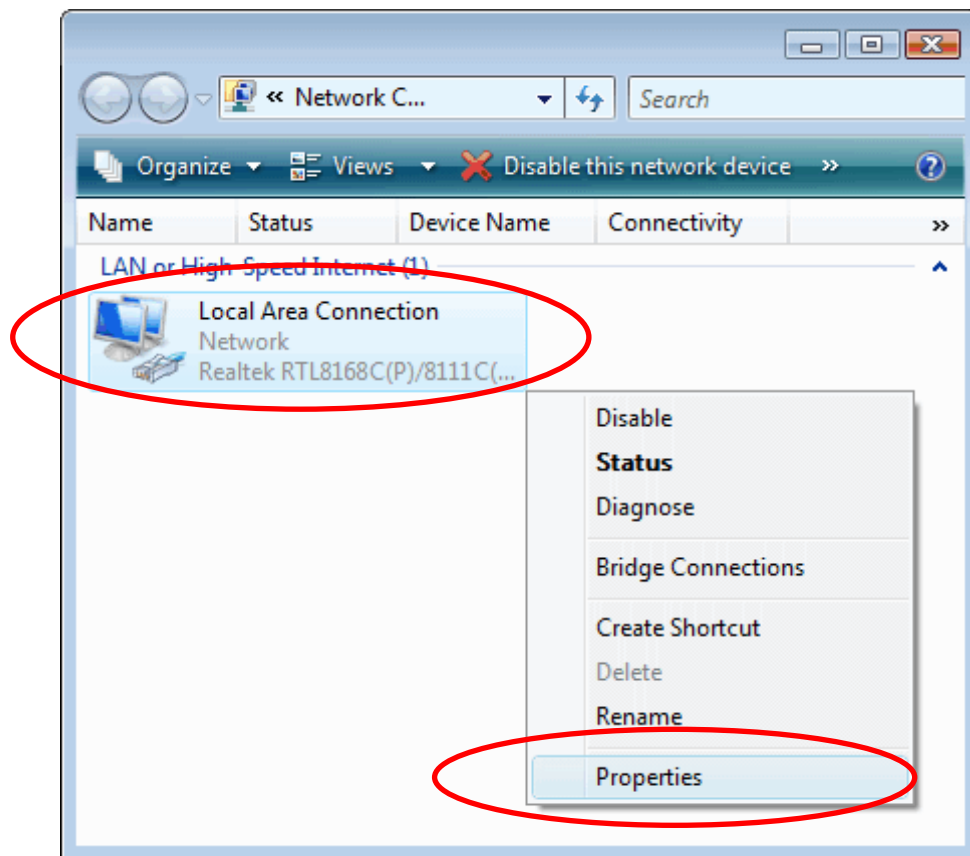
1. Click on “Start” -> “Control Panel” -> “View network status and tasks”.



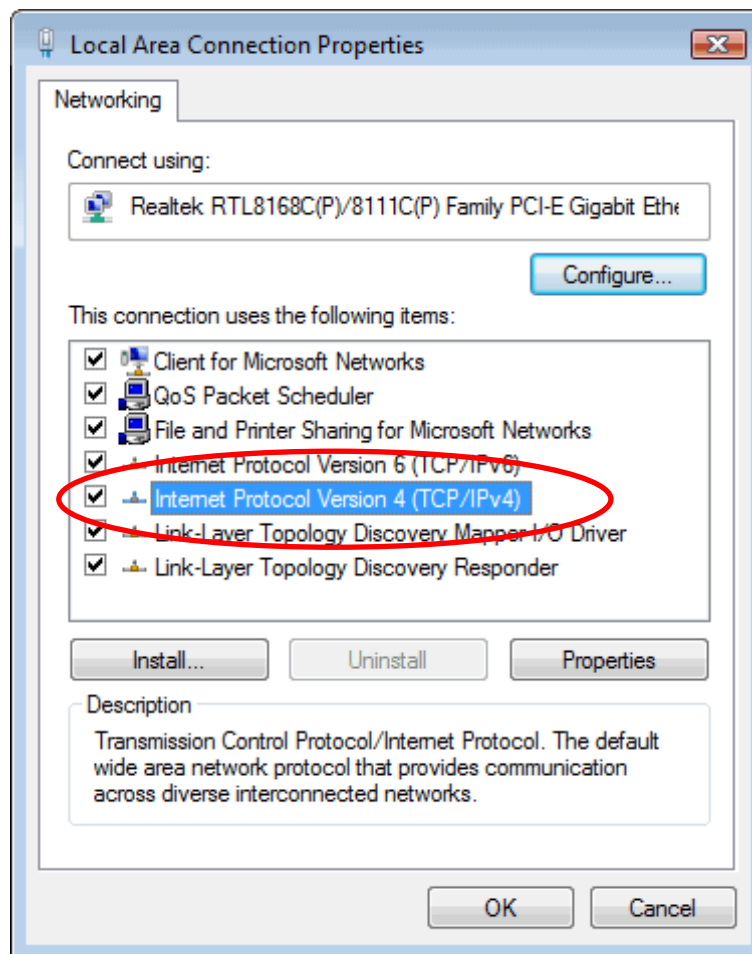
2. In the Manage network connections, click on **“Manage network connections”** to continue.



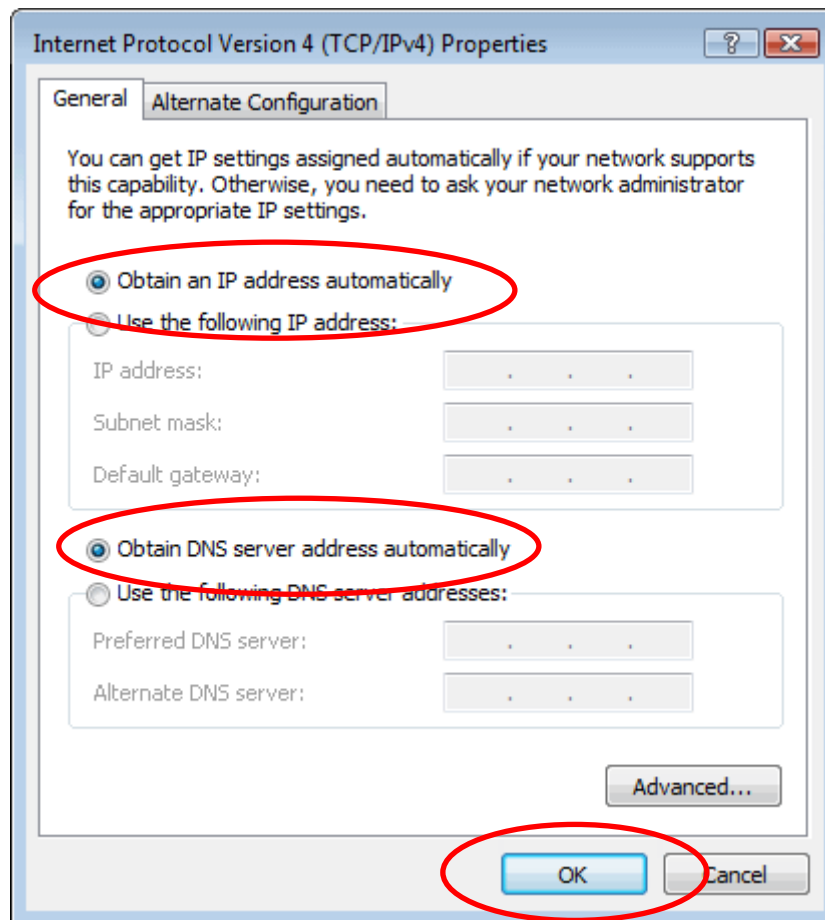
3. Single RIGHT click on "**Local Area connection**", then click "**Properties**".



4. The screen will display the information "**User Account Control**" and click "**Continue**" to continue.
5. Double click on "**Internet Protocol Version 4 (TCP/IPv4)**".



6. Check "**Obtain an IP address automatically**" and "**Obtain DNS server address automatically**" then click on "**OK**" to continue.

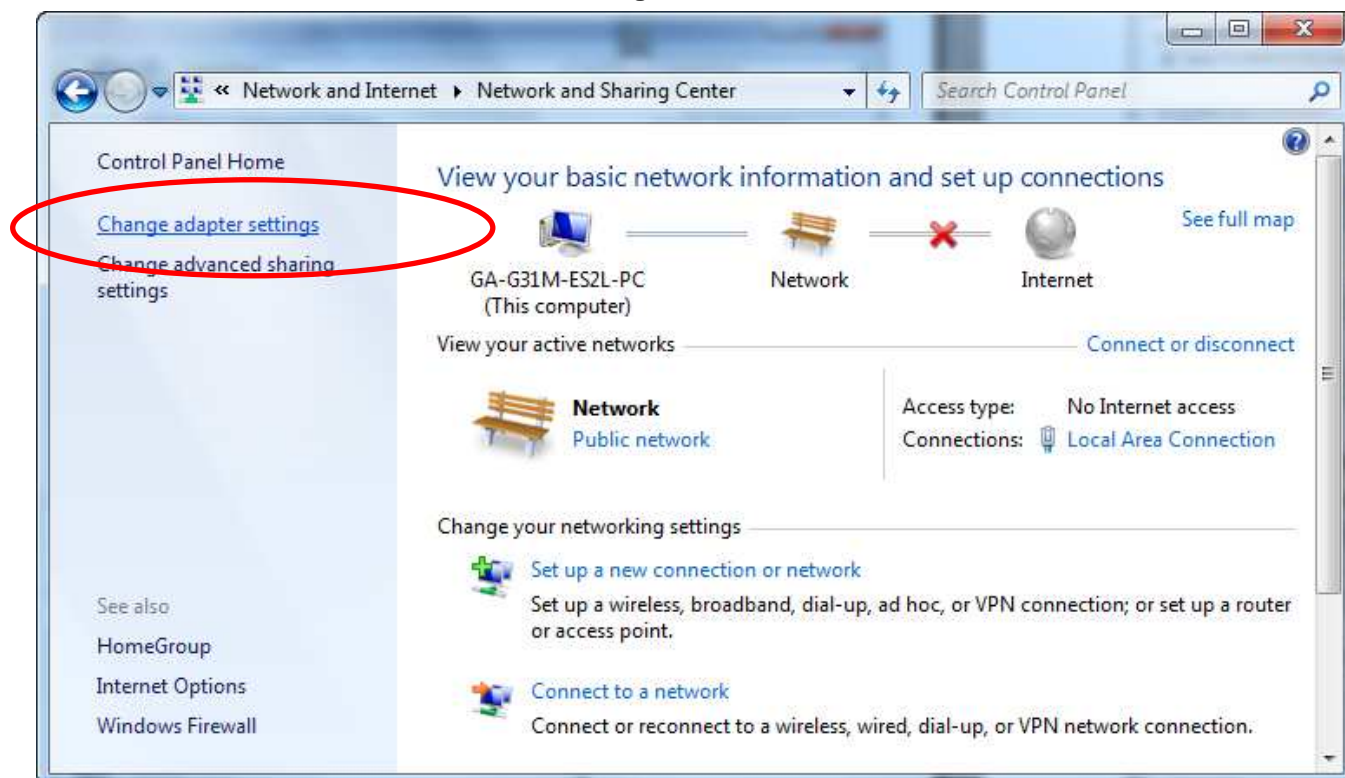


## For Windows 7-32/64

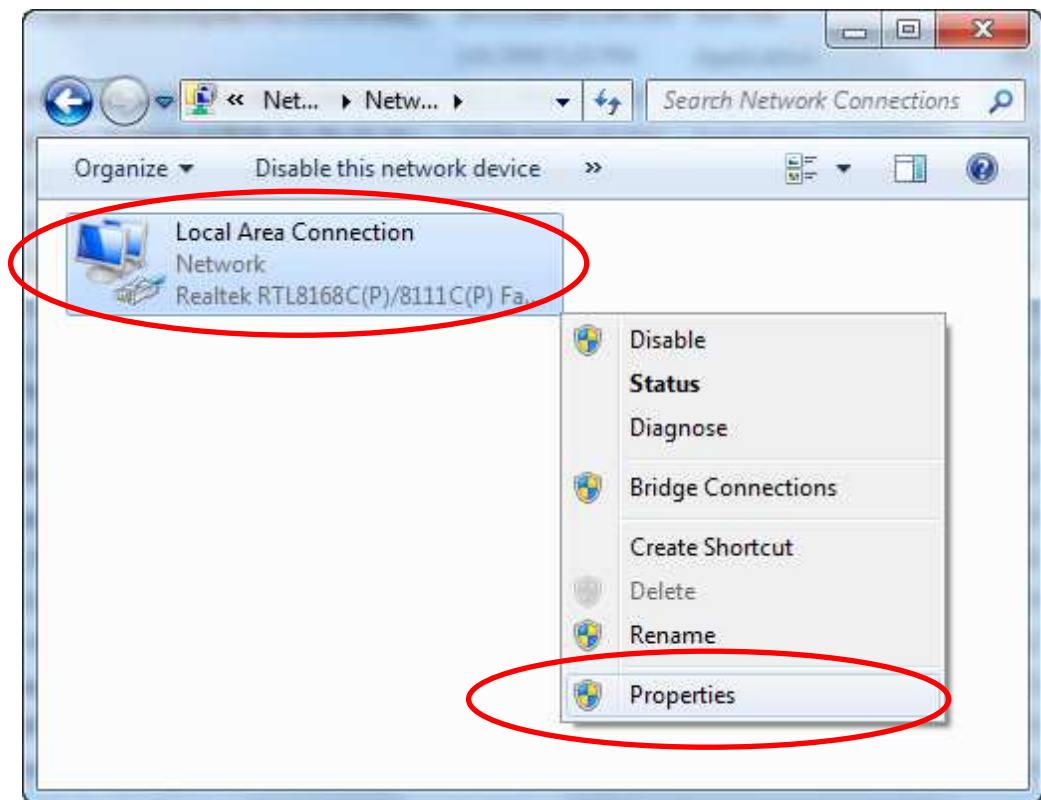
1. Click on “Start” -> “Control Panel” (in Category View) -> “View network status and tasks”.



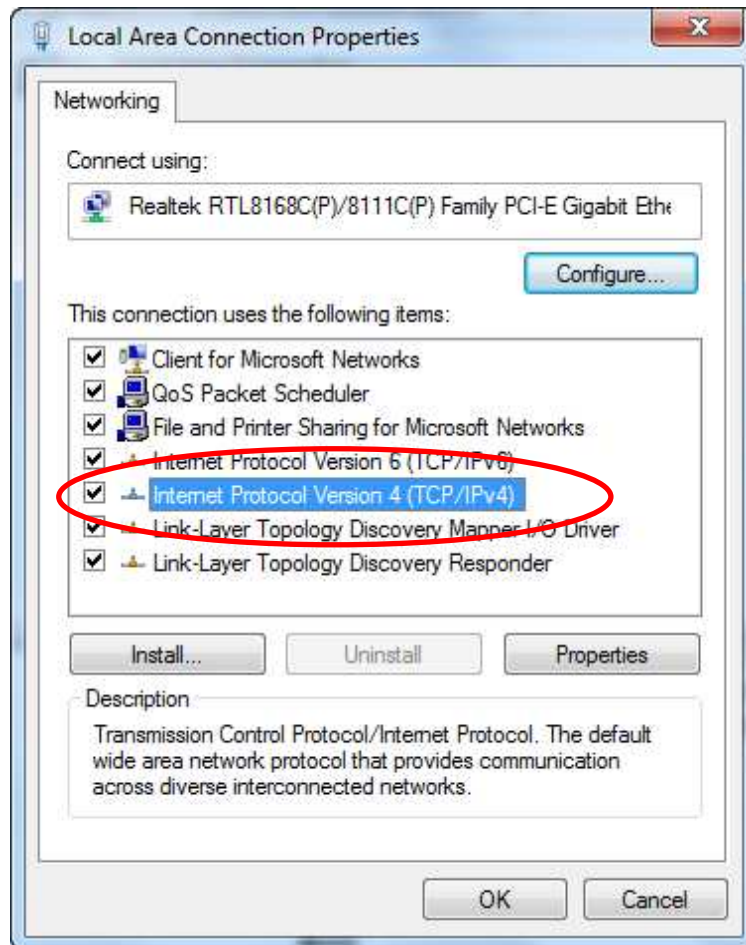
2. In the Control Panel Home, click on “Change adapter settings” to continue.



3. Single RIGHT click on **"Local Area Connection"**, then click **"Properties"**.

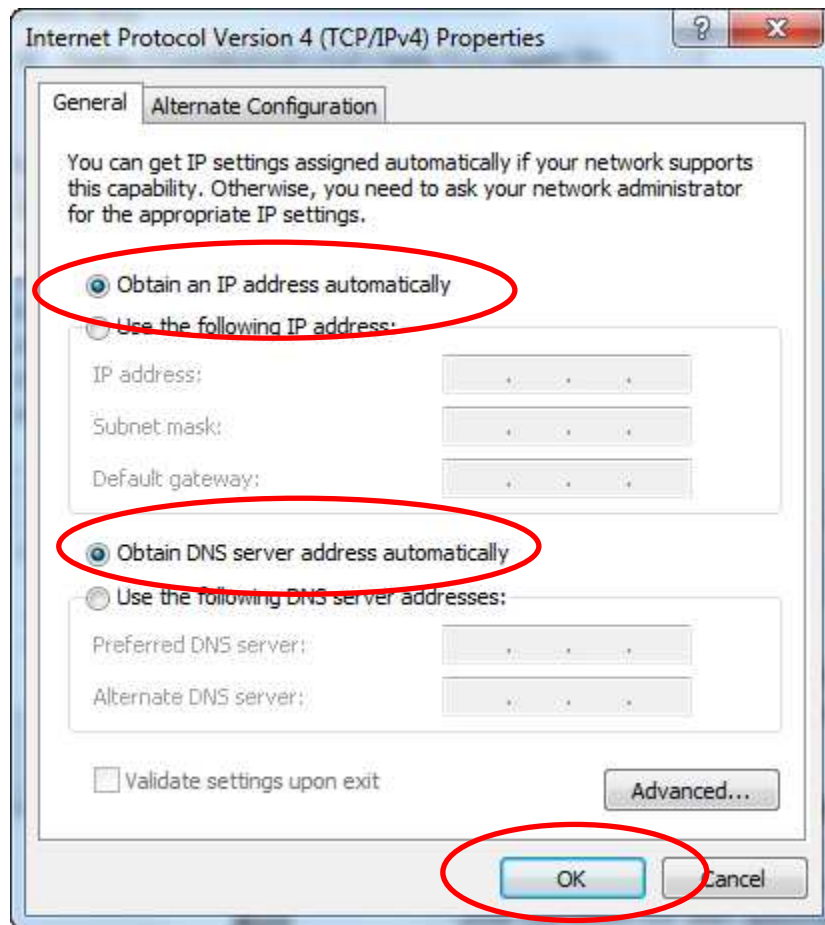


4. Double click on "**Internet Protocol Version 4 (TCP/IPv4)**".





5. Check "**Obtain an IP address automatically**" and "**Obtain DNS server address automatically**" then click on "**OK**" to continue.



## 4 Connecting your device

This chapter provides basic instructions for connecting the Wireless Gateway to a computer or LAN and to the Internet.

In addition to configuring the device, you need to configure the Internet properties of your computer(s). For more details, see the following sections:

- *Configuring Ethernet PCs*

This chapter assumes that you have already established a DSL/Cable service with your Internet service provider (ISP). These instructions provide a basic configuration that should be compatible with your home or small office network setup. Refer to the subsequent chapters for additional configuration instructions.

### Connecting the Hardware

---

This section describes how to connect the device to the wall phone port, the power outlet and your computer(s) or network.



#### WARNING

***Before you begin, turn the power off for all devices. These include your computer(s), your LAN hub/switch (if applicable), and the device.***

The diagram below illustrates the hardware connections. The layout of the ports on your device may vary from the layout shown. Refer to the steps that follow for specific instructions.

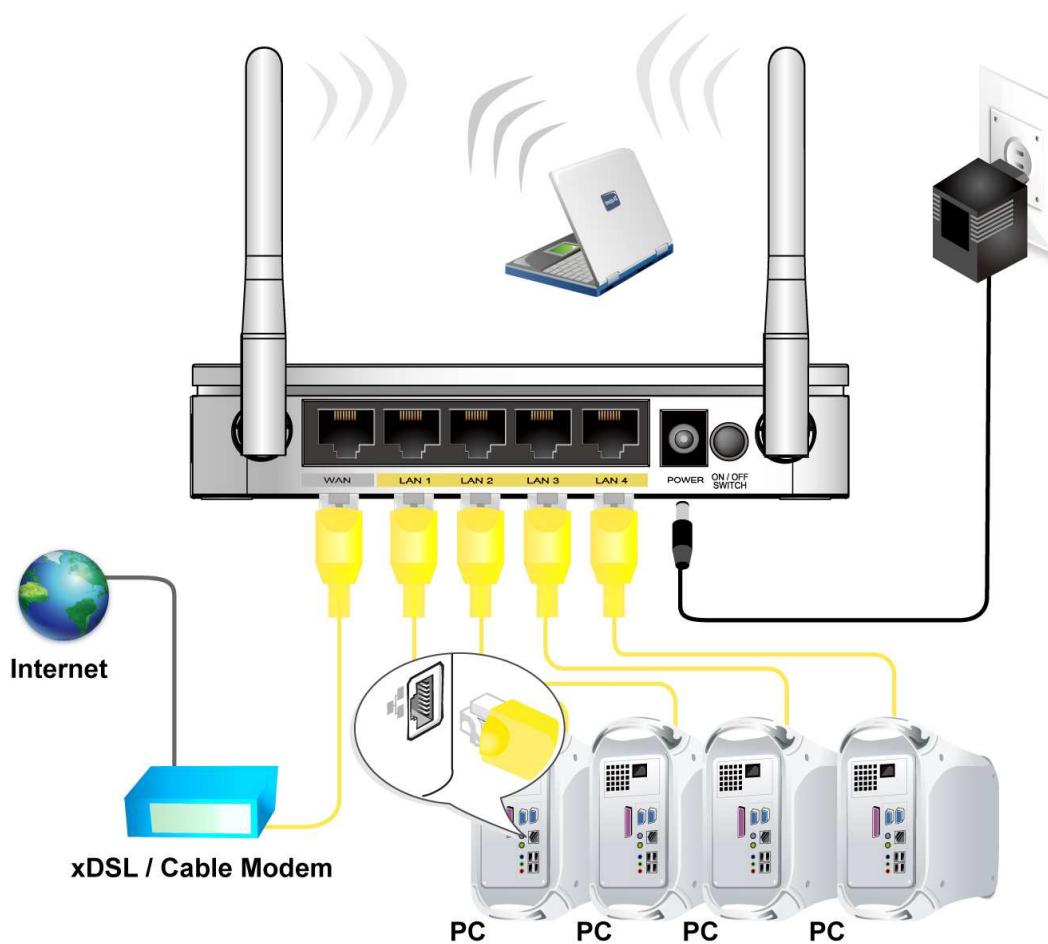


Figure 5: Overview of Hardware Connections

Step 1. Connect the Ethernet cable to WAN Port

Connect the RJ45 Ethernet cable from your xDSL/Cable Modem's Ethernet port to 802.11n WLAN Router's WAN Port.

Step 2. Connect the Ethernet cable to LAN Port

Connect the supplied RJ45 Ethernet cable from your PC's Ethernet port to any of the 4 802.11n WLAN Router's LAN Ports.

Step 3. Attach the power connector

Connect the power adapter to the power inlet "**POWER**" of the 802.11n WLAN Router and turn the power switch "**ON/OFF SWITCH**" of your 802.11n WLAN Router on.

## 802.11n WLAN Router Configuration

---

1. Please insert the supplied CD into your CD-ROM drive.
2. The CD should auto-start, displaying the window shown in 3. below. If your CD does not start automatically, go to Windows Explorer, Select your CD drive and double click **autorun.exe**.
3. To configure the device, please click on **Advanced Configuration** button.
4. Please enter the Login User Name: **root** and Login Password: **fibrain** and then click on **Login** button.

**Login**

User Name

Password

Language

- Click on **Confirm** button.

Login Success.

Confirm

- Select the Connection Type **DHCP**, **Static IP** or **PPPoE** and enter related parameters that your ISP (Internet Services Provider) or Network Administrator provided and then click on **Save Settings** button.

## Setup - WAN

### Operation Mode

Operation Mode

GATEWAY ▾

### WAN 1

WAN

☒ Enable ☐ Disable

Connection Type

DHCP ▾

Host Name

MTU

1500 Bytes

Bigpond Login

☐ Enable ☒ Disable

Bigpond Login Server

New South Wales (61.9.192.13) ▾

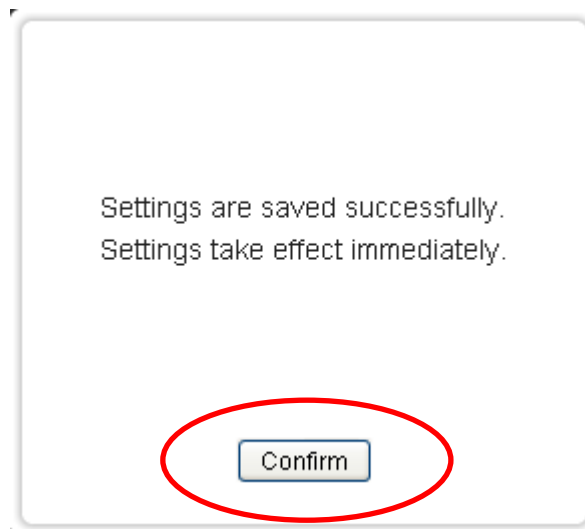
Bigpond Login User Name

Bigpond Login Password

Save Settings

Cancel Changes

7. Click on **Confirm** button.



8. From the **Wireless** menu, click on **Basic**.

**Setup - WAN**

**Operation Mode**

Operation Mode

GATEWAY

**WAN 1**

WAN

☒ Enable ☐ Disable

Connection Type

DHCP

Host Name

MTU

1500 Bytes

Bigpond Login

☐ Enable ☒ Disable

Bigpond Login Server

New South Wales (61.9.192.13)

Bigpond Login User Name

Bigpond Login Password

.....

Save Settings

Cancel Changes

9. Please enter the SSID and if you want to change (the default settings **Wireless Connection= Enable, SSID = Fibrain**).
10. Choose the Security Mode if necessary, as **Disable (Default)** / WEP / WPA PSK (Pre-Shared Key) / WPA Radius / WPA2 PSK (Pre-Shared Key) and WPA2 Radius. For example, you choose the WPA2 PSK Security Mode and configure the Key (Passphrase).
11. Please click **Save Settings** button to continue.

## Wireless - Basic

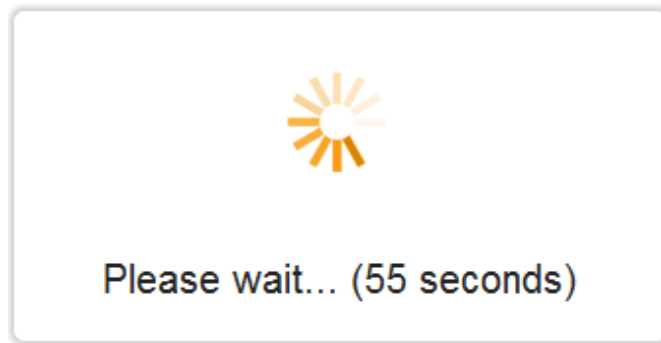
The screenshot shows the 'Wireless - Basic' configuration page. Red circles highlight the following settings:

- WLAN 1 - Basic:** The 'Wireless Connection' section, where 'Enable' is selected.
- WLAN 1 - DATA:** The 'Wireless SSID Name' field containing 'Fibrain', the 'Wireless SSID Broadcasting' section with 'Enable' selected, and the 'Security Mode' dropdown menu set to 'Disable'.
- WLAN 1 - Voice:** The 'Wireless SSID' section, where 'Disable' is selected.
- WLAN 1 - SSID 1:** The 'Wireless SSID' section, where 'Disable' is selected.
- WLAN 1 - SSID 2:** The 'Wireless SSID' section, where 'Disable' is selected.
- Buttons:** The 'Save Settings' button at the bottom of the page.

The configuration details for each section are as follows:

Section	Wireless Connection	Wireless SSID Name	Wireless SSID Broadcasting	Wi-Fi Multimedia (WMM)	Wireless Isolation	Max Station Connection	Security Mode
WLAN 1 - Basic	Enable	-	-	-	-	-	-
WLAN 1 - DATA	-	Fibrain	Enable	Enable	Enable	10	Disable
WLAN 1 - Voice	-	Fibrain2	Enable	Enable	Enable	10	Disable
WLAN 1 - SSID 1	-	Fibrain3	Enable	Enable	Enable	10	Disable
WLAN 1 - SSID 2	-	Fibrain4	Enable	Enable	Enable	10	Disable

12. Please wait... (55 seconds).



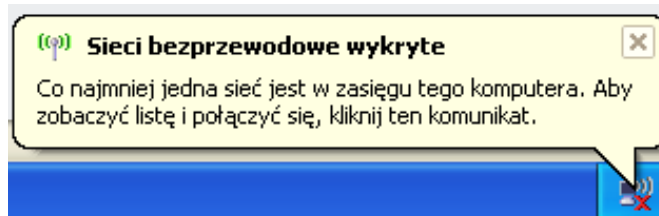
13. WLAN Router has been configured completely, and suitable for Wireless and Internet Connections.



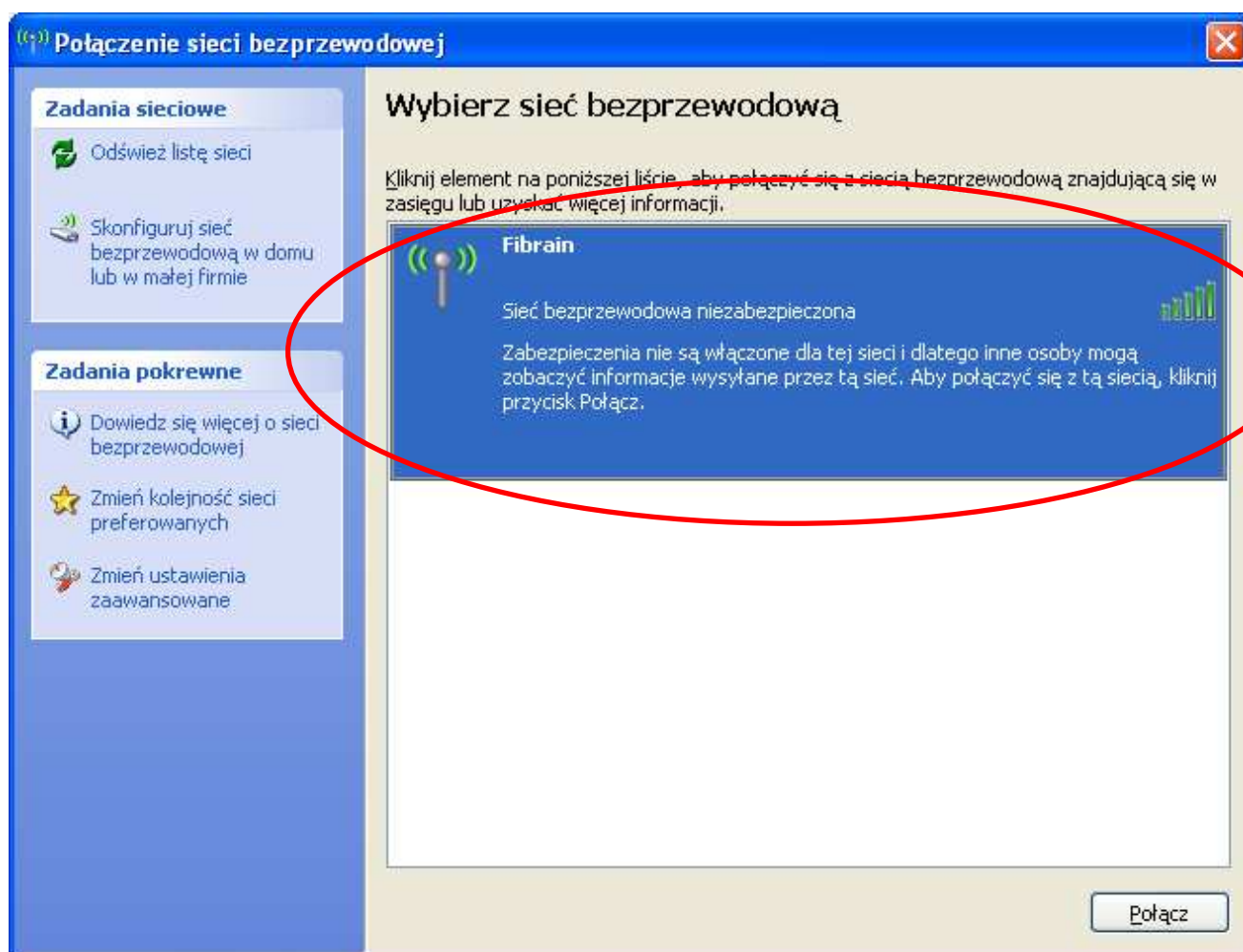
## Wireless Connection

For easy installation it is saved to keep the settings. You can later change the wireless settings via the wireless configuration menu. (see user manual on the CD – Chapter 14 and other).

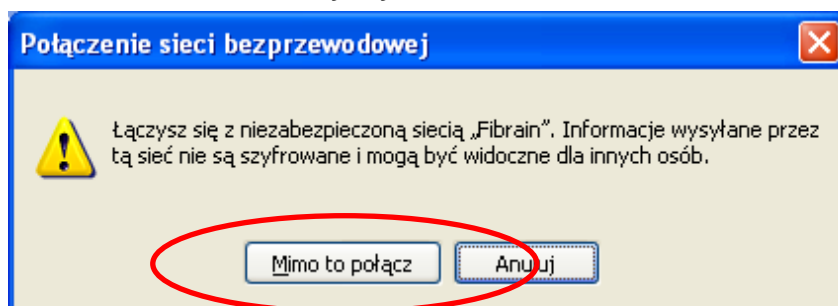
1. Double click on the wireless icon on your computer and search for the wireless network that you enter **SSID** name.



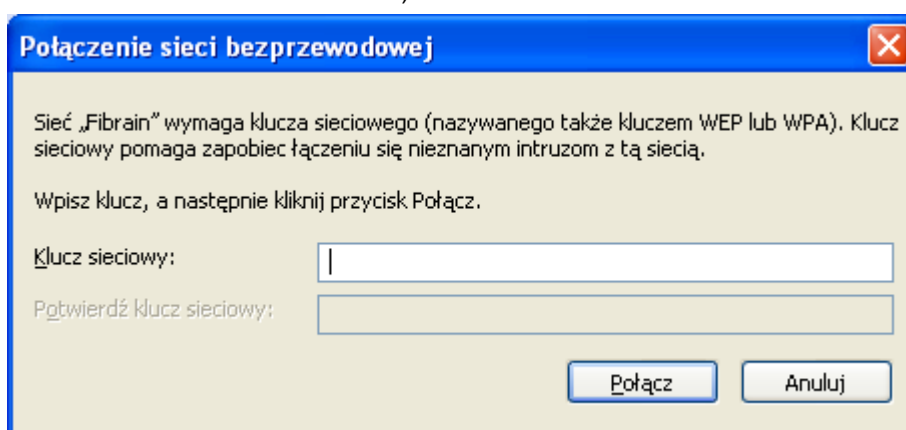
2. Click on the wireless network that you enter **SSID** name to connect.



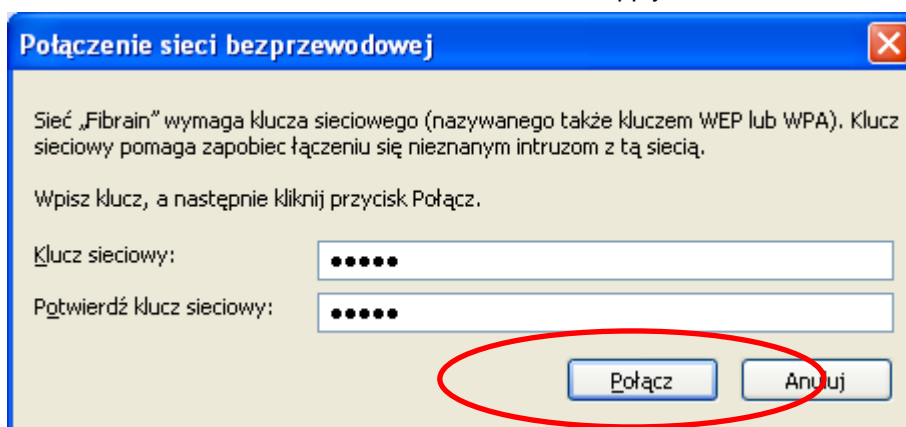
3. If the wireless network isn't encrypted, click on "**Connect Anyway**" to connect.



4. If the wireless network is encrypted, enter the network key that belongs to your authentication type and key. You can later change this network key via the wireless configuration menu. (see user manual on the CD – Chapter 14 and other).



5. Click on "Connect" or "Apply".



6. Now you are ready to use the Wireless Network to Internet or intranet.

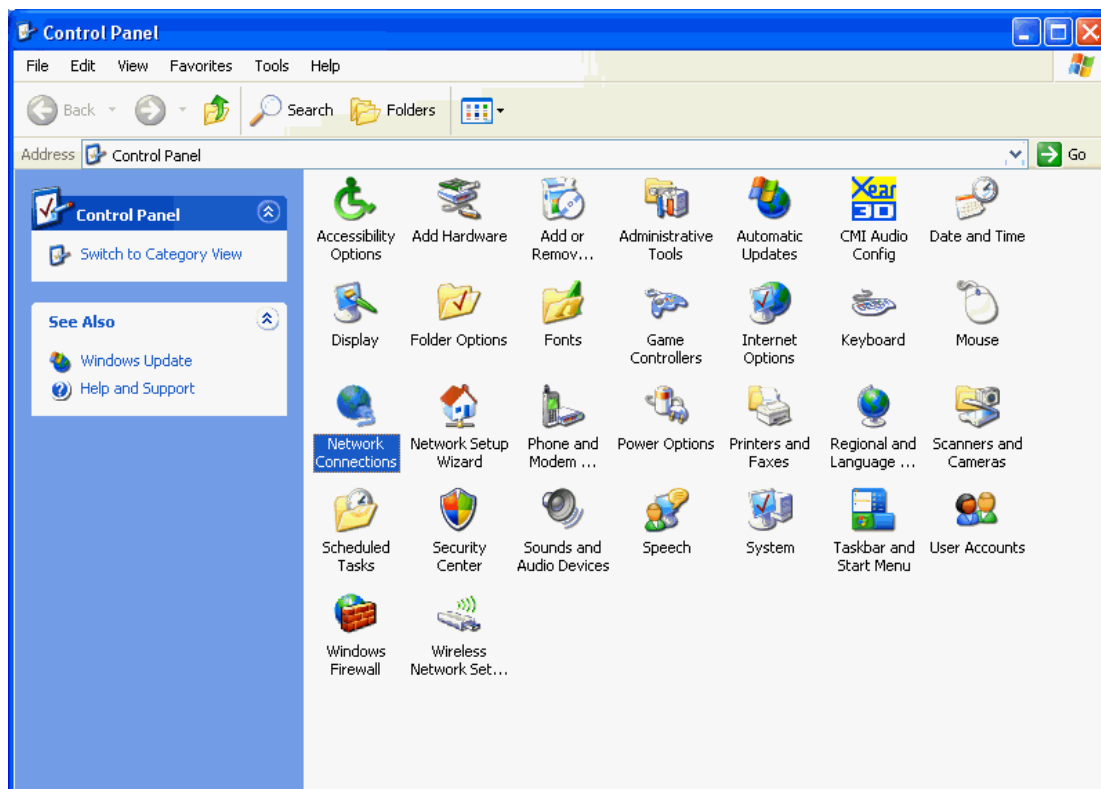
## 5 What the Internet/WAN access of your own Network now is

Now you could check what the Internet/WAN access of your network is to know how to configure the WAN port of Wireless Gateway.

Please follow steps below to check what the Internet/WAN access if your own Network is DHCP Client, Static IP or PPPoE Client.

1. Click **Start -> Control Panel**

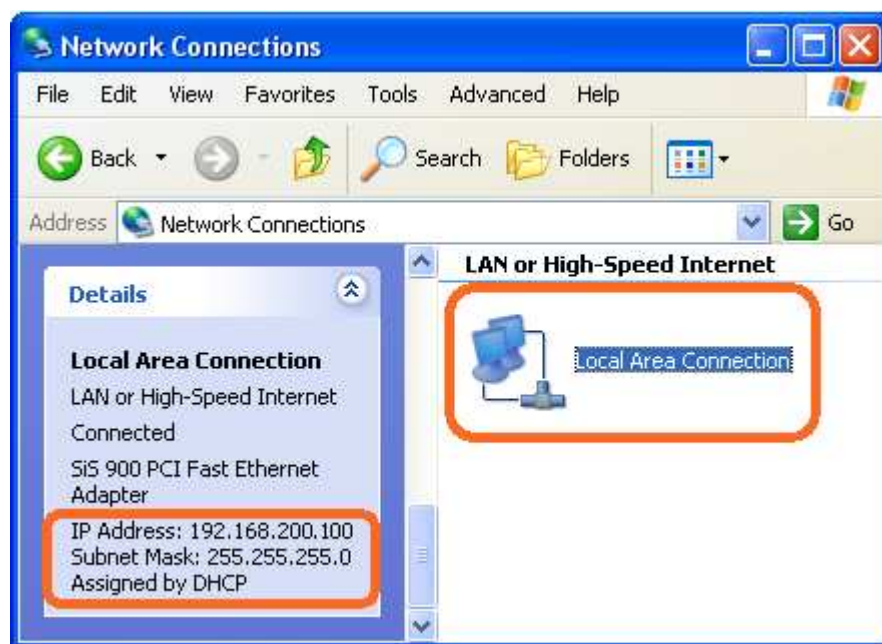


2. Double click **Network Connections**

## Internet/WAN access is the DHCP client

If you cannot see any **Broadband Adapter** in the **Network Connections**, your Internet/WAN access is **DHCP Client** or **Static IP**.

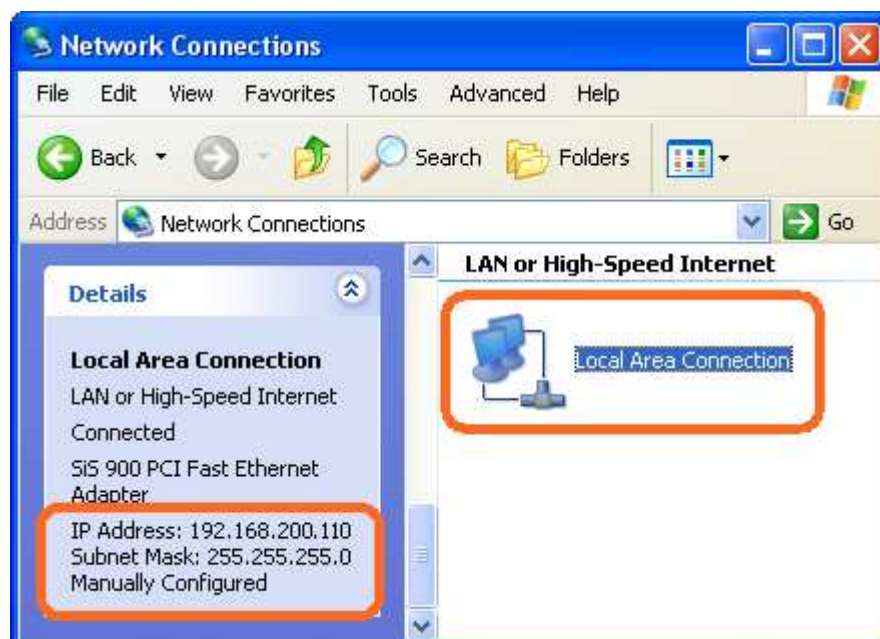
1. Click **Local Area Connection** in **LAN or High-Speed Internet** and you could see string **Assigned by DHCP** in Details.



## Internet/WAN access is the Static IP

If you cannot see any **Broadband Adapter** in the **Network Connections**, your Internet/WAN access is **DHCP Client** or **Static IP**.

2. Click **Local Area Connection** in **LAN or High-Speed Internet** and you could see string **Manually Configured** in Details.



3. Right click **Local Area Connection** and click **Properties** and then you could get the IP settings in detail and write down the IP settings as follow:

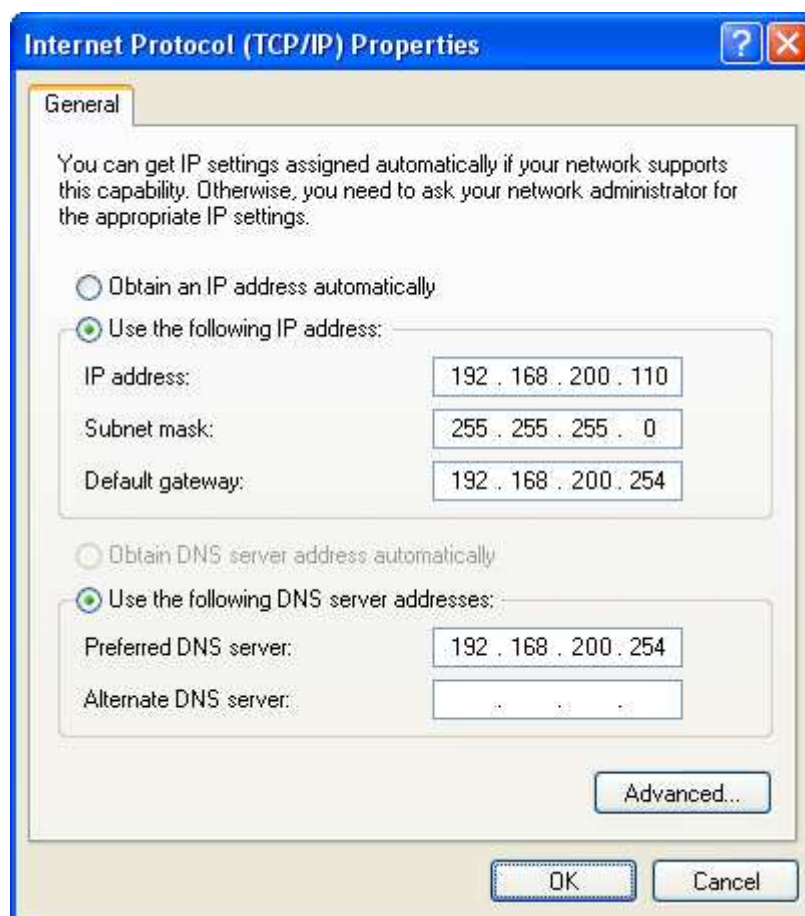
**IP Address: 192.168.200.110**

**Subnet mask: 255.255.255.0**

**Default gateway: 192.168.200.254**

**Preferred DNS server: 192.168.200.254**

**Alternate DNS Server: If you have it, please also write it down.**



## Internet/WAN access is the PPPoE client

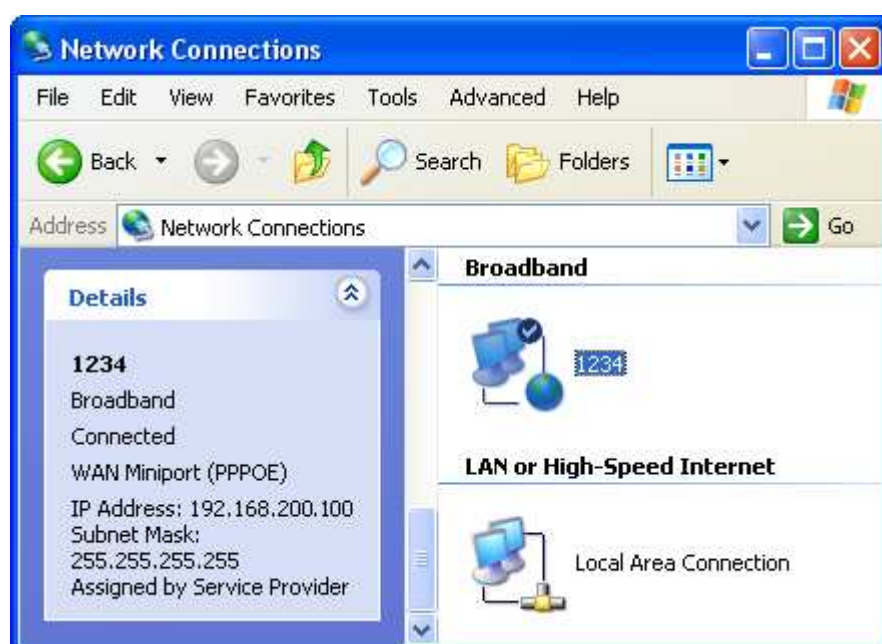
If you can see any **Broadband Adapter** in the **Network Connections**, your Internet/WAN access is **PPPoE Client**.

1. Click **Broadband Adapter** in **Broadband** and you could see string **Assigned by Service Provider** in Details.

For PPPoE configuration on Wireless Gateway, you'll need following information that you could get from your Telecom, or by your Internet Service Provider.

**Username of PPPoE: 1234 for example**

**Password of PPPoE: 1234 for example**





## 6 Getting Started with the Web pages

The Wireless Gateway includes a series of Web pages that provide an interface to the software installed on the device. It enables you to configure the device settings to meet the needs of your network. You can access it through your web browser from any PC connected to the device via the LAN ports.

### Accessing the Web pages

To access the Web pages, you need the following:

- A PC or laptop connected to the LAN port on the device.
- A web browser installed on the PC. The minimum browser version requirement is Internet Explorer v4 or Netscape v4. For the best display quality, use latest version of Internet Explorer, Netscape or Mozilla Firefox. From any of the LAN computers, launch your web browser, type the following URL in the web address (or location) box, and press [Enter] on your keyboard:

**http://192.168.200.254**

**The first time that you click on an entry from the left-hand menu, a login box is displayed. You must enter your username and password to access the pages.**

A login screen is displayed:

Figure 6: Login screen

1. Enter your user name and password. The first time you log into the program, use these defaults:

#### Administrator Level

User Name: **root**  
Password: **fibrain**

#### User Level

User Name: **admin**  
Password: **admin**



#### Note

You can change the password at any time or you can configure your device so that you do not need to enter a password. See Password.

- Click on Login.

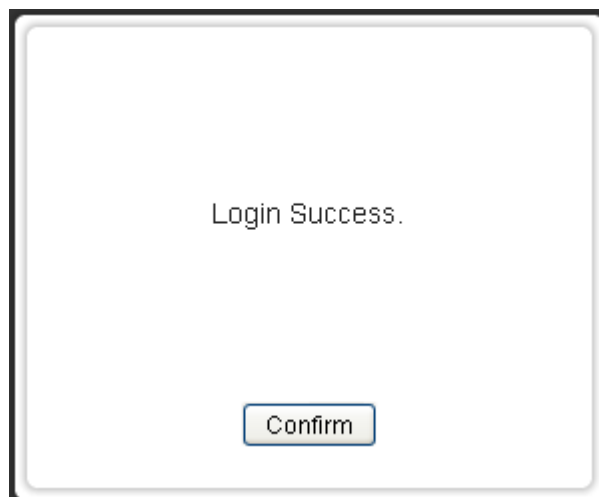
This is the first page displayed each time you log in to the Web pages.



### Note

*If you receive an error message or the Welcome page is not displayed, see Troubleshooting Suggestions.*

- Click on Confirm. You are now ready to configure your device.



The *Setup - WAN* homepage for the web pages is displayed:

### Setup - WAN

WAN 1

WAN

☒ Enable
 ☐ Disable

Connection Type

DHCP

Host Name

MTU

1500

Bytes

Bigpond Login

☐ Enable
 ☒ Disable

Bigpond Login Server

New South Wales (61.9.192.13)

Bigpond Login User Name

Bigpond Login Password

Save Settings

Cancel Changes

Figure 7: Homepage

## Testing your Setup

Once you have connected your hardware and configured your PCs, any computer on your LAN should be able to use the DSL /Cable connection to access the Internet.

To test the connection, turn on the device, wait for 30 seconds and then verify that the LEDs are illuminated as follows:

**Table 1. LED Indicators**

Label	Color	Function
POWER	green	On: device is powered on Off: device is powered off
WLAN	green	On: WLAN link established and active Blink: Valid Wireless packet being transferred
WPS	green	Off: WPS link isn't established and active Blink: Valid WPS packet being transferred
WAN	green	On: WAN link established and active Off: No LAN link Blink: Valid Ethernet packet being transferred
LAN 1/2/3/4	green	On: LAN link established and active Off: No LAN link Blink: Valid Ethernet packet being transferred

If the LEDs illuminate as expected, test your Internet connection from a LAN computer. To do this, open your web browser, and type the URL of any external website (such as <http://www.yahoo.com>). The LED labeled WAN should blink rapidly and then appear solid as the device connects to the site.

If the LEDs do not illuminate as expected, you may need to configure your Internet access settings using the information provided by your ISP. For details, see *Internet Access*. If the LEDs still do not illuminate as expected or the web page is not displayed, see *Troubleshooting Suggestions* or contact your ISP for assistance.

## Default device settings

In addition to handling the xDSL / Cable modem connection to your ISP, the Wireless Gateway can provide a variety of services to your network. The device is preconfigured with default settings for use with a typical home or small office network.

The table below lists some of the most important default settings; these and other features are described fully in the subsequent chapters. If you are familiar with network configuration, review these settings to verify that they meet the needs of your network. Follow the instructions to change them if necessary. If you are unfamiliar with these settings, try using the device without modification, or contact your ISP for assistance.



### WARNING

*We strongly recommend that you contact your ISP prior to changing the default configuration.*

Option	Default Setting	Explanation/Instructions
<i>WAN Port IP Address</i>	DHCP Client	This is the temporary public IP address of the WAN port on the device. It is an unnumbered interface that is replaced as soon as your ISP assigns a 'real' IP address. See <i>Network Settings -&gt; WAN Interface</i> .
<i>LAN Port IP Address</i>	Assigned static IP address: 192.168.200.254  Subnet mask: 255.255.255.0	This is the IP address of the LAN port on the device. The LAN port connects the device to your Ethernet network. Typically, you will not need to change this address. See <i>Network Settings -&gt; LAN Interface</i> .
<i>DHCP (Dynamic Host Configuration Protocol)</i>	DHCP server enabled with the following pool of addresses: 192.168.200.100 through 192.168.200.200	The Wireless Gateway maintains a pool of private IP addresses for dynamic assignment to your LAN computers. To use this service, you must have set up your computers to accept IP information dynamically, as described in <i>Configuring Ethernet PCs</i> .

## 7 Wide Area Network (WAN) Settings

The device supports 3 connection types: DHCP, Static IP and PPPoE. Please ensure which connection type should be used, and select your internet connection type from the drop-down list.

From the *Configuration* menu, click on *WAN*. The following page is displayed:

### Setup - WAN

**WAN 1**

WAN

Connection Type

Host Name

MTU

Bigpond Login

Bigpond Login Server

Bigpond Login User Name

Bigpond Login Password

☒ Enable ☐ Disable

DHCP

DHCP

Static IP

PPPoE

1500

bytes

☐ Enable ☒ Disable

New South Wales (61.9.192.13)

Save Settings

Cancel Changes

## Static IP (Fixed IP address assignment)

If you need to assign static IP addresses to the devices in your network, please remember that the IP address for each computer or device must be in the same IP address range as all the devices in the network. Each device must also have the same subnet mask. For example: Assign the first computer an IP address of 192.168.0.2 and a subnet mask of 255.255.255.0, the second device an IP address of 192.168.0.3 and a subnet mask of 255.255.255.0, and so on.

### Setup - WAN

**WAN 1**

WAN

☒ Enable ☐ Disable

Connection Type

Static IP

External IP Address

10.1.1.25

Netmask

255.255.255.0

Gateway

10.1.1.254

Static DNS 1

10.1.1.254

Static DNS 2

MTU

1500 Bytes

Save Settings

Cancel Changes

Field	Description
WAN	Select Enable / Disable to enable/disable WAN.
Connection Type	Static IP
External IP Address	The external IP addresses offered by the ISP.
Netmask	The netmask offered by the ISP.
Gateway	The gateway offered by the ISP.
Static DNS 1	The static DNS 1 offered by the ISP.
Static DNS 2	The static DNS 2 offered by the ISP.
MTU	Maximum Transmission Unit

## DHCP

It will auto get the IP address from the DHCP Server. Assign the length of time for the IP lease, default setting is 86400 seconds. The Hostname is the name of the device.

### Setup - WAN

WAN 1

WAN

☒ Enable
 ☐ Disable

Connection Type
 

DHCP

Host Name

MTU
 

1500

 Bytes

Bigpond Login
 

☐ Enable
 ☒ Disable

Bigpond Login Server
 

New South Wales (61.9.192.13)

Bigpond Login User Name

Bigpond Login Password

Save Settings

Cancel Changes

Field	Description
WAN	Select Enable / Disable to enable/disable WAN.
Connection Type	DHCP
Host Name	Some ISP and DHCP servers ask for the Host Name of the DHCP client before assigning an IP address. In this case, please key in your Host Name.
MTU	Maximum Transmission Unit
Bigpond Login	If you are using "Bigpond" system, please enable this item
Bigpond Login Server	Please choose the Bigpond server.
Bigpond Login User Name	Please enter your User Name provided by Bigpond
Bigpond Login Password	Please enter your Password provided by Bigpond

## PPPoE

Please enter the information accordingly provided by ISP.

### Setup - WAN

WAN 1

WAN

☒ Enable
 ☐ Disable

Connection Type  
 PPPoE

Authentication  
 CHAP (Auto)

User Name

Password

PPP Connection Type  
☒ Always Connected
 ☐ On Demand

Max Idle Time  
 Seconds (60~3600)

PPP Echo Interval  
 Seconds (3 ~ 50)

PPP Retry Threshold  
 Time(s) (3 ~ 50)

PPP MTU  
 Bytes (592-1492)

MTU  
 Bytes (600~1500)

Save Settings

Cancel Changes

Field	Description
WAN	Select Enable / Disable to enable/disable WAN.
Connection Type	PPPoE
Authentication	Select authentication type for PPPoE
User Name	The user name offered by the ISP.
Password	The password offered by the ISP.
On Demand: Max Idle Time	PPPoE On Demand will only be activated when there is traffic. When there is no traffic within max. idle time (default: 300 seconds), PPPoE will be disconnected.
Keep Alive	PPPoE Keep Alive will maintain the PPPoE dial up connection.
PPPoE Echo Interval	PPPoE echo will ensure whether the link is still up or not (default interval 20 seconds)
PPPoE Retry Threshold	When PPPoE echo retry exceeds PPPoE Retry Threshold (default 20 times), the dial up connection would be recognized as down.
PPPoE MTU	PPPoE maximum transmission unit: up to 1492 bytes (PPPoE's header is 8 bytes)(This value should be less than MTU value at least 8 bytes ).
MTU	Physical Device Maximum Transmission Unit



## 8 Local Area Network (LAN) Settings

To set up the configuration of LAN interface, private IP of your router LAN port and subnet mask for your LAN segment. Default IP is 192.168.200.254.

From the *Configuration* menu, click on *LAN*. The following page is displayed:

### Setup - LAN

**LAN**

Internal IP Address

192.168.200.254

Netmask

255.255.255.0

Spanning Tree Protocol (STP)

☐ Enable ☒ Disable

MTU

1500

Bytes

Save Settings

Cancel Changes

Field	Description
<b>Internal IP Address</b>	The IP of your Router LAN port (default 192.168.200.254).
<b>Netmask</b>	Select Netmask from the drop-down list. Subnet Mask of you LAN (default 255.255.255.0). All devices on the network must have the same subnet mask to communicate on the network.
<b>Spanning Tree Protocol (STP)</b>	Click Enable to avoid cyclic topology caused by incorrect connection of your internal network. (A cyclic topology will cause network breakdown.)
<b>MTU</b>	Maximum transmission unit: up to 1500 bytes.

## 9 Routing Settings

User can set a route rule (table) in here.

From the *Configuration* menu, click on *Routing*. The following page is displayed:

### Setup - Routing

**Routing**

Routing ☒ Enable ☐ Disable

**Routing Rule**

Rule Name	Enable	Internal IP Range	External IP Range	Protocol	Service Port Range	External Interface	Routing Type	Gateway
SMTP	✗	From: To:	From: To:	TCP	From:25 To:25	WAN1	default	

Add Delete Modify Up Down

Save Cancel

Field	Description
Routing	Choose Enable/Disable to enable/disable routing policy.

### Add Routing Rule

Click on *Add*. The following page is displayed:

Sequence Number

Rule Name

Enable ☒

Internal IP Range From:  To:

External IP Range From:  To:

Protocol

Service Port Range From:  To:

External Interface

Routing Gateway

Gateway IP Address

Confirm Cancel Changes

Field	Description
Sequence Number	This defines the sequence of the Routing rules. If a packet fits the conditions set by the Routing rules, the packet will then be sorted according to the first Routing rule from the top of the list.
Rule Name	Name of the Routing rule.
Rule Enable	Enable/Disable this Routing rule
External Interface	Please select which External Interface (WAN1 or WAN2) you want for a packet to go through, IF the packet fits the condition of this ACL rule.
Internal IP Range	Set up the internal IP range for this ACL rule.
External IP Range	Set up the external IP range for this ACL rule.
Protocol	Set up the protocol (TCP or UDP) for the ACL to be enabled.
Service Port Range	Set up the Service Port Range (e.g., HTTP is TCP/80) for the ACL to be enabled.
External Interface	Please select which External Interface (WAN1 or WAN2) you want for a packet to be routed, IF the packet fits the condition of this Routing rule.

### Example of Routing Rule

Rule Name	SMTP outgoing routing
Enable	Enable
Internal IP Range	Blank (applied to all)
External IP Range	Blank (applied to all)
Protocol	TCP
Service Port Range	25:25 (SMTP Port:25)
External Interface	WAN1

# 10 DHCP Server Settings

The device provides DHCP server service in order to offer IP addresses to the computers within a LAN.

From the *Configuration* menu, click on *DHCP Server*. The following page is displayed:

## Setup - DHCP Server

**DHCP Server - LAN**

DHCP Service
☒ Enable
☐ Disable

DHCP Start IP Address
192.168.200.

Max DHCP Clients

Lease

Domain

DHCP DNS Server Type

DHCP DNS Server IP Address

Field	Description
<b>DHCP Server</b>	<b>Select Enable/Disable to enable/disable DHCP Server.</b>
<b>DHCP Starting IP Address</b>	<b>The DHCP starting IP addresses offered by the DHCP Server.</b>
<b>Max DHCP Clients</b>	<b>The maximum number of the IP addresses supported by the DHCP server</b>
<b>Lease</b>	<b>Please choose lease time from the drop-down list. You can choose 1 Hour, 3 Hours, 6 Hours, 1 Day, 3 Days, or 7 Days.</b>
<b>Domain</b>	<b>Please enter the domain name.</b>
<b>DHCP DNS Server Type</b>	<b>Select DHCP DNS server type</b>
<b>DHCP DNS Server IP Address</b>	<b>Please set up the DHCP DNS server IP address</b>

# 11 DDNS Settings

DDNS (Dynamic Domain Name Service) allows an “internet domain name” to be assigned to a computer/router which has a dynamic IP address. This makes it possible for other internet devices to connect to the computer/router without needing to trace the changing IP addresses themselves. To enable DDNS, you will first need to sign up for DDNS services from DynDNS.org, TZO.com or ZoneEdit.com.

DDNS is useful when combined with the virtual server feature. It allows other internet users to connect to your virtual server by using a domain name, rather than an IP address. The DDNS service helps users to locate the right IP address by the domain name.

For example, you wish to set up a personal web server. However, you obtain a different IP address from your ISP every time you connect to the internet. The dynamic IP address you have will cause difficulty for other internet users to find your web server. In this case, you will need to enable DDNS, so other users can connect to you through a fixed domain name to disregard the potential varying IP addresses behind the server.

From the *Configuration* menu, click on *DDNS*. The following page is displayed:

## Setup - DDNS

Dynamic Domain Name Service - WAN 1

DDNS Service

☒ Enable ☐ Disable

DDNS Type

DynDNS.org

User Name

Password

Host Name

Action

Update

Save Settings

Cancel Changes

Field	Description
<b>DDNS Service</b>	<b>Select Enable to enable DDNS service.</b> <b>Select Disable to disable DDNS service.</b>
<b>DDNS Type</b>	<b>Select the desired DDNS service provider from the list.</b>
<b>User Name</b>	<b>Enter your username provided by DDNS Service</b>
<b>Password</b>	<b>Enter your password provided by DDNS Service</b>
<b>Host Name</b>	<b>Apply for a domain name, and make sure it is allocated to you</b>

## 12 MAC Address Clone Settings

Some ISPs only allow a registered MAC address to access to the internet. To bypass the rule, you need to set up a cloned MAC address for the device using the pre-registered MAC address.

From the *Configuration* menu, click on *MAC Address Clone*. The following page is displayed:

### Setup - MAC Address Clone

MAC Address Clone - WAN 1

Clone WAN MAC

☐ Enable ☒ Disable

MAC Address

Save Settings

Cancel Changes

Field	Description
<b>Clone WAN MAC</b>	<b>If your ISP only grants access to a fixed MAC address, please select Enable.</b> <b>If your ISP does not enforce access control, please select Disable.</b>
<b>MAC Address</b>	<b>If the PC you use to configure AXIMCom Mobile Router is the device which has the right MAC address to access the internet, press Get Current PC MAC Address button. Or you can type in the MAC Address which has been granted access by your ISP.</b>

# 13 VLAN Settings

Port-based VLAN is the simplest approach to VLAN implementation. The idea is to assign the ports on a switch to different VLANs, confining the propagation of the packets received on a port within the particular VLAN. Thus, separation of broadcast domains and division of virtual groups are achieved.

From the *Setup* menu, click on *VLAN*. The following page is displayed:

## Setup - VLAN

Add
Remove

Name	Enable	VLAN ID	Port 1	Port 2	Port 3	Port 4	Port 5	SSID 1	SSID 2	SSID 3	SSID 4	WDS	UR
LAN1	<input checked="" type="checkbox"/>	1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
WAN1	<input checked="" type="checkbox"/>	2	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Port	PVID	Port Tag	Priority
PORT1	2	<input type="checkbox"/>	1
PORT2	1	<input type="checkbox"/>	1
PORT3	1	<input type="checkbox"/>	1
PORT4	1	<input type="checkbox"/>	1
PORT5	1	<input type="checkbox"/>	1

Save Settings

Cancel Changes

Field	Description
<b>Add</b>	<b>Add a new VLAN rule</b>
<b>Remove</b>	<b>Remove a new VLAN rule</b>
<b>Name</b>	<b>Enter the name of VLAN rule</b>
<b>PVID</b>	<b>Enter the Port VLAN ID</b>
<b>Port tag</b>	<b>Enable or disable Port VLAN tag</b>
<b>Priority</b>	<b>Set up the port priority</b>



# 14 Wireless - Basic Setting

Multiple SSIDs allow the ability for separate security mode and key settings to be set by users for both convenience and increased protection. Users are able to configure their network devices to access the first SSID with the WPA2 PSK (Pre-Shared Key) and secret key, whilst share the second SSID with WEP and the periodically changed key for visitors. In addition, users are able to isolate these SSIDs to avoid malicious attacks and prevent certain access for visitors using the second SSID. This then provides users an extremely convenient approach to share the wireless access, provide access internet access for visitors, while possessing a strong security protection system at all times.

From the *Wireless* menu, click on *Basic*. The following page is displayed:

## Wireless - Basic

## WLAN 1

Wireless Connection ☒ Enable ☐ Disable

Wireless Mode B/G/N Mixed ▾

MCS Auto ▾

Transmission Power 100% ▾

Wireless Channel Auto Channel ▾

Wireless Isolation Between SSIDs ☐ Enable ☒ Disable

## WLAN 1 - DATA

Wireless SSID ☒ Enable ☐ Disable

Wireless SSID Name Fibrain

Wireless SSID Broadcasting ☒ Enable ☐ Disable

Wi-Fi Multimedia (WMM) ☒ Enable ☐ Disable

Wireless Isolation ☐ Enable ☒ Disable

Max Station Connection(Number 1~255, 0:unlimited) 10

Security Mode Disable ▾

## WLAN 1 - Voice

Wireless SSID ☐ Enable ☒ Disable

Wireless SSID Name Fibrain2

Wireless SSID Broadcasting ☐ Enable ☐ Disable

Wi-Fi Multimedia (WMM) ☐ Enable ☐ Disable

Wireless Isolation ☐ Enable ☒ Disable

Max Station Connection(Number 1~255, 0:unlimited) 10

Security Mode Disable ▾

## WLAN 1 - SSID 1

Wireless SSID ☐ Enable ☒ Disable

Wireless SSID Name Fibrain3

Wireless SSID Broadcasting ☐ Enable ☐ Disable

Wi-Fi Multimedia (WMM) ☐ Enable ☐ Disable

Wireless Isolation ☐ Enable ☒ Disable

Max Station Connection(Number 1~255, 0:unlimited) 10

Security Mode Disable ▾

## WLAN 1 - SSID 2

Wireless SSID ☐ Enable ☒ Disable

Wireless SSID Name Fibrain4

Wireless SSID Broadcasting ☐ Enable ☐ Disable

Wi-Fi Multimedia (WMM) ☐ Enable ☐ Disable

Wireless Isolation ☐ Enable ☒ Disable

Max Station Connection(Number 1~255, 0:unlimited) 10

Security Mode Disable ▾

Save Settings

Cancel Changes

## WLAN 1 Settings

### WLAN 1

Wireless Connection	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Wireless Mode	B/G/N Mixed ▼
Transmission Power	100% ▼
Wireless Channel	Auto Channel ▼
Wireless Isolation Between SSIDs	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Max Station Connection(Number 1~255, 0:unlimited)	0

Field	Description
<b>Wireless Connection</b>	Select Enable if you would like to turn on the wireless signal. Select Disable if you would like to turn off the wireless signal.
<b>Wireless Mode</b>	Select the wireless mode for 802.11b/g/n or mixed use.
<b>Transmission Power</b>	Select the transmission power class from 10%, 25%, 50%, 75%, and 100%.
<b>Wireless Channel</b>	Select which channel to be located to.
<b>Wireless Isolation Between SSIDs</b>	Select Enable if you would like to omit the access from one SSID to another. Select Disable if you would like to allow the access from one SSID to another.
<b>Max Station Connection(Number 1~255, 0:unlimited)</b>	Max Station Connection Number of client

## SSID Settings

Users are able to configure each SSID with its own attributes. Further, various security modes are available based on the user's needs and preference: Disable, WEP, WPA Pre-Shared Key, WPA, WPA2 Pre-Shared Key, and WPA2. However, it is important to note that all devices under the wireless network must use the same security mode.

You can configure the security settings of your wireless network to suit your desired preference. Different methods will grant different levels of security. Using encryption - data packet is encrypted before transmission - can prevent data packets from being intruded on by un-trusted parties. However, please note that the higher the security level is, the lower the data throughput becomes.

### WLAN 1 - SSID 1

Wireless SSID	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Wireless SSID Name	<input type="text" value="Fibrain3"/>
Wireless SSID Broadcasting	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Wi-Fi Multimedia (WMM)	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Wireless Isolation	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Max Station Connection(Number 1~255, 0:unlimited)	<input type="text" value="10"/>
Security Mode	<input type="text" value="Disable"/>

Field	Description
Wireless SSID	Select Enable if you would like to turn on this SSID. Select Disable if you would like to turn off this SSID.
Wireless SSID Name	Enter the wireless station name you would like to have.
Wireless SSID Broadcasting	The device broadcasts SSID periodically. Select Enable to turn it on or Disable to turn it off. Enabling SSID Broadcasting brings convenience for users to find and connect the device. Disabling SSID broadcasting enhances the security by hiding SSID information.
Wi-Fi Multimedia (WMM)	Select Enable to prioritize different traffic types based on their characteristics. For example, VoIP or video traffic will have higher priorities over ordinary traffic.
Wireless Isolation	Select Enable if you would like to omit the access to other network devices connecting to this SSID. Select Disable if you would like to allow the access to other network devices connecting to this SSID.
Max Station Connection(Number 1~255, 0:unlimited)	Max Station Connection Number of client
Security Mode	Configure the security to Disable, WEP, WPA Pre-Shared Key, WPA, WPA2 Pre-Shared Key, and WPA2

## WEP Settings

### WLAN 1 - SSID 1

Wireless SSID	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Wireless SSID Name	<input type="text" value="Fibrain3"/>
Wireless SSID Broadcasting	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Wi-Fi Multimedia (WMM)	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Wireless Isolation	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Max Station Connection (Number 1~255, 0:unlimited)	<input type="text" value="10"/>
Security Mode	<input type="text" value="WEP64"/>
Key Index	<input type="text" value="1"/>
Key 1	<input type="text"/>
Key 2	<input type="text"/>
Key 3	<input type="text"/>
Key 4	<input type="text"/>

(The WEP64 Keys are ASCII strings of 5 digits, or HEX strings of 10 digits.)

(The WEP128 Keys are ASCII strings of 13 digits, or HEX strings of 26 digits.)

Field	Description
<b>WEP Key Index</b>	<b>WEP Key Index indicates which WEP key is used for data encryption.</b>
<b>WEP Key (1~4)</b>	<b>64-bit WEP: type 10 hexadecimal digits or 5 ASCII characters. 128-bit WEP: type 26 hexadecimal digits or 13 ASCII characters.</b>

## WPA Pre-shared Key / WPA2 Pre-shared Key Settings

### WLAN 1 - SSID 1

Wireless SSID	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Wireless SSID Name	<input type="text" value="Fibrain3"/>
Wireless SSID Broadcasting	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Wi-Fi Multimedia (WMM)	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Wireless Isolation	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Max Station Connection (Number 1~255, 0:unlimited)	<input type="text" value="10"/>
Security Mode	<input type="text" value="WPA PSK (Pre-Shared Key)"/>
Key	<input type="text"/>
Encryption Method	<input type="text" value="TKIP"/>

(The Key is an ASCII string of 8-63 digits, or a HEX string of 64 digits.)

Field	Description
<b>Pre-shared Key</b>	<b>Pre-shared Key serves as the credential for the packet encryption.</b>
<b>Encryption Mode</b>	<b>TKIP/AES are supported.</b>

## WPA / WPA2 Radius Settings

### WLAN 1 - SSID 1

Wireless SSID	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Wireless SSID Name	<input type="text" value="Fibrain3"/>
Wireless SSID Broadcasting	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Wi-Fi Multimedia (WMM)	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Wireless Isolation	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Max Station Connection(Number 1~255, 0:unlimited)	<input type="text" value="10"/>
Security Mode	<input type="text" value="WPA (Radius)"/>
Radius Server IP Address	<input type="text"/>
Radius Server Port	<input type="text" value="1812"/>
Radius Key	<input type="text"/>
Encryption Method	<input type="text" value="AES"/>
Rekey Method	<input type="text" value="Disable"/>
Rekey Time Interval	<input type="text" value="3600"/>
Rekey Packet Interval	<input type="text" value="5000"/>

(The Key is an ASCII string of 8-63 digits, or a HEX string of 64 digits.)

Field	Description
<b>Radius Server IP Address</b>	<b>Enter the RADIUS server's IP address.</b>
<b>Radius Server Port</b>	<b>Enter the RADIUS server's port number. The default port is 1812.</b>
<b>Radius Key</b>	<b>Enter the RADIUS server's IP Address.</b>
<b>Encryption Mode</b>	<b>Select TKIP or AES for the packet encryption.</b>

# 15 Wireless - Advanced Setting

From the *Wireless* menu, click on *Advanced*. The following page is displayed:

## Wireless - Advanced

Region Setting

Region
Europe, Australia and Hong Kong (channel 1 - 13) ▼

WLAN 1

Fragmentation

2346
Bytes (256 ~ 2346)

CTS/RTS

☐ Enable
☒ Disable
2347
Seconds (1 ~ 2347)

DTim

1
(1 ~ 255)

Beacon Interval

100
Milliseconds (20 ~ 1024)

Header Preamble

Long ▼

TxMode

None ▼

MPDU

4 ▼
Microseconds

MSDU Aggregate

☐ Enable
☒ Disable

Tx Burst

☒ Enable
☐ Disable

Packet Aggregate

☐ Enable
☒ Disable

HT Control Field

☐ Enable
☒ Disable

Reverse Direction Grant

☐ Enable
☒ Disable

Link Adapt

☐ Enable
☒ Disable

Short Guard Interval(GI)

☒ Enable
☐ Disable

Operation Mode

Mixed Mode ▼

HT Band Width

20/40 ▼
MHz

Block Ack Setup Automatically

☒ Enable
☐ Disable

Block Ack Window Size

64
x16 Bits (1 ~ 64)

Reject Block Ack

☐ Enable
☒ Disable

MCS

Auto ▼

Save Settings

Cancel Changes



Field	Description
<b>Region</b>	Choose the region you are currently located.
<b>Fragmentation</b>	Enter the fragmentation bytes. The default value is 2346 bytes.
<b>CTS/RTS</b>	Enter the CTS/RTS seconds. The default value is 2347 seconds.
<b>DTim</b>	Enter the DTim seconds. The default value is 1.
<b>Beacon Interval</b>	Enter the interval to send a beacon. The default value is 100 milliseconds.
<b>Header Preamble</b>	Choose Long or Short header preamble.
<b>TxMode</b>	Choose different transmission mode.
<b>MPDU</b>	MPDU data length. The transmission rate is increase when you choose a larger number, but usually the max value will be 4 in the wireless card
<b>MSDU Aggregate</b>	A kind of packet aggregation method, it can improve the transmission efficiency. Please make sure you Wireless card has this function supported.
<b>Tx Burst</b>	Some 802.11g wireless card can supported this mode, and the transmission rate can be increased when enable this function.
<b>Packet Aggregate</b>	An aggregation method like A-MSDU, it can improve the transmission efficiency. Please make sure you Wireless card has this function supported.
<b>HT Control Field</b>	Choose Enable/Disable. It is useful when you need to debug the wireless network
<b>Reverse Direction Grant</b>	Choose Enable/Disable. The response time can be shorter when enable this function.
<b>Link Adapt</b>	Choose Enable/Disable. The function is use to dynamically change the modulation and encode mechanism between wireless devices.
<b>Short Guard Interval (SGI)</b>	Choose Enable/Disable. Short GI can improve some transmission rate, but with less immunity when interference exist.
<b>Operation Mode</b>	Choose Mixed mode or Greenfield. You may choose Greenfield mode to increase the transmission rate when you using 802.11n wireless network only.
<b>HT Band Width</b>	Using HT20MHz or HT20/40MHz
<b>Block Ack Setup Automatically</b>	Choose Enable/Disable. If your Wifi Card supported Block Ack mechanism, it can improve the data transmission efficiency when enable this function.
<b>Block Ack Window Size</b>	Specify a Block Ack window size
<b>Reject Block Ack</b>	Choose Enable to reject the request of BA from other Wireless device
<b>MCS</b>	Select transmission (connection) speed.

# 16 Wireless - WDS Setting

From the *Wireless* menu, click on *WDS*. The following page is displayed:

## Wireless - WDS

**WLAN 1**

WDS Mode

Repeater (AP Enabled)
Disabled
Repeater (AP Enabled)
Bridge (AP Disabled)

**WDS 1**

WDS MAC Address

Security Mode

Disable

**WDS 2**

WDS MAC Address

Security Mode

Disable

**WDS 3**

WDS MAC Address

Security Mode

Disable

**WDS 4**

WDS MAC Address

Security Mode

Disable

Save Settings

Cancel Changes

Field	Description
<b>WDS</b>	<b>Select Enable to enable WDS function. Select Disable to disable WDS function.</b>
<b>MAC Address [1~4]</b>	<b>Enter the MAC addresses of the other bridged wireless devices. Maximum of 4 devices are allowed to be bridged together.</b>
<p><b>*Please make sure of the following settings in order to allow WDS to work effectively:</b></p> <p><b>(1) WDS bridged devices must use the same radio channel.</b></p> <p><b>(2) WDS bridged devices must use the same encryption mode and encryption keys.</b></p> <p><b>Please Note: If one of the above fails, WDS devices cannot communication with each other.</b></p>	

# 17 Wireless - Universal Repeater Setting

The Universal Repeater function is similar with WDS in that it is used to essentially enlarge the area of wireless network coverage. However, unlike WDS, Universal Repeater offers simplicity in configuration requirements, as users only need to configure the current AP as a client, and to connect it to the second AP's SSID (or BSSID). However, you need to ensure that the two APs are using the same wireless channel and security mode (and key) for Universal Repeater to work effectively.

From the *Wireless* menu, click on *Universal Repeater*. The following page is displayed:

## Wireless - Universal Repeater

WLAN 1

Universal Repeater

☒ Enable
 ☐ Disable

Target SSID

Target BSSID (MAC)

Wireless Channel

Channel 1 [2.412GHz] ▼

Security Mode

Disable ▼

Save Settings

Cancel Changes

Field	Description
Universal Repeater	Select Enable to enable Universal Repeater function. Select Disable to disable Universal Repeater function.
Target SSID	Enter the target SSID to connect to.
Target BSSID (MAC)	Enter the target BSSID to connect to. The BSSID is optional if you setup the target SSID.
Security Mode	Choose the security mode the target AP uses, and enter the key if needed.

# 18 Wireless - WPS Setting

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.

From the *Wireless* menu, click on *WPS*. The following page is displayed:

## Wireless - WPS

**WPS Enable**

WPS Enable
☒ Enable
☐ Disable

**WPS Router PIN Code**

WPS Router Pin Code:
76429149
Generate PIN Code

**WPS Connect**

WPS Push Button:
Push Button

WPS Client Pin Code Connect:
Connection

Save Settings
Cancel Changes

Field	Description
<b>WPS Enable</b>	Select Enable to enable WPS function. Select Disable to disable WPS function.
<b>WPS Router PIN Code</b>	“WPS Router PIN Code” is AP’s PIN. Whenever users want to change AP’s PIN, they could click “Regenerate PIN” and then click “ Apply Changes”. Moreover, if users want to make their own PIN, they could enter four digit PIN without checksum and then click “ Apply Changes”. However, this would not be recommended since the registrar side needs to be supported with four digit PIN.
<b>WPS Push Button</b>	Clicking this button will invoke the PBC method of WPS. It is only used when AP acts as a registrar.
<b>WPS Client Pin Code Connect:</b>	It is only used when users want their station to join AP’s network. The length of PIN is limited to four or eight numeric digits. If users enter eight digit PIN with checksum error, there will be a warning message popping up. If users insist on this PIN, AP will take it.

# 19 Security - Firewall Setting

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.

From the *Security* menu, click on *Firewall*. The following page is displayed:

## Security - Firewall

**Firewall Protection**

SPI Firewall Protection

☒ Enable
 ☐ Disable

TCP SYN DoS Protection

☒ Enable
 ☐ Disable

ICMP Broadcasting Protection

☒ Enable
 ☐ Disable

ICMP Redirect Protection

☒ Enable
 ☐ Disable

Broadcast Storming

☐ Enable
 ☒ Disable

Save Settings

Cancel Changes

Field	Description
<b>SPI Firewall Protection</b>	<b>Select Enable to enable SPI Firewall Protection. Select Disable to disable SPI Firewall Protection.</b>
<b>TCP SYN DoS Protection</b>	<p><b>Check to enable TCP SYN DoS Protection.</b>  <b>Uncheck to disable TCP SYN DoS Protection.</b></p> <p><b>TCP SYN DoS attack sends a flood of TCP/SYN packets. Each of these packets are like a connection request, causing the server to consume computing resources (e.g. memory, CPU) to reply and to continuously wait for the incoming packets. Without TCP SYN Dos Protection, the resources in the server will be easily consumed completely. This will then consequently result in the dysfunction of the server.</b></p> <p><b>The device is able to detect TCP SYN DoS attacks and limits the resource consumption by lowering the incoming request rate by fast recycling the resource. Therefore, The device is still able to serve normal traffic while it is under such an attack.</b></p>
<b>ICMP Broadcasting Protection</b>	<p><b>Check to enable ICMP Broadcasting Protection.</b>  <b>Uncheck to disable ICMP Broadcasting Protection.</b></p> <p><b>ICMP broadcasting attack is a type of DoS attacks. A flood of ICMP broadcasting packets is generated and sent to a server (like AXIMCom Mobile Router). Consequently, this server will suffer from a huge amount of interruptions and consumption of computing resources.</b></p>

	<b>The device is able to stop responding to ICMP broadcasting echo packets in order to avoid a potential ICMP broadcasting DoS attack.</b>
<b>ICMP Redirect Protection</b>	<b>Check to enable ICMP Redirect Protection.</b> <b>Uncheck to disable ICMP Redirect Protection.</b> <b>An ICMP redirect message is a way to change the existing routing path. Generally, ICMP redirect packets should not be sent, and so when there is the occurrence that ICMP redirect packets are sent, it is important to note that it is very likely to be used as a means for a network attack.</b>
<b>Broadcast Storming</b>	<b>Enable/disable Broadcast Storming protection.</b>

## 20 Security - ACCESS CONTROL LIST (ACL) SETUP Setting

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.

From the *Security* menu, click on *ACL*. The following page is displayed:

### Security - Access Control

**Access Control List (ACL)**

Access Control
☒ Enable
☐ Disable

Default Access Control Action
☒ ALLOW
☐ DENY

**Access Control List (ACL) Rule**

Rule Name	Rule Enable	External Interface	Internal IP Range	Action
MSN Messenger	✗	-	From: To:	DENY
MSN Messenger	✗	-	From: To:	DENY
Yahoo! Messenger	✗	-	From: To:	DENY

Add
Delete
Modify
Up
Down

Save Settings
Cancel Changes

Field	Description
<b>ACL</b>	<b>Select Enable to enable ACL. Select Disable to disable ACL.</b>
<b>Default ACL Action</b>	<p><b>Check Enable to enable a specific MAC Filter rule.</b></p> <p><b>Uncheck Enable to disable a specific MAC Filter rule. Type the MAC address to permit a device to access to the network.</b></p> <p><b>* Enabling MAC filtering blocks all MAC addresses which are not listed in the MAC Filter Rule. Be aware that adding the MAC address of your managing computer is required in order to access to the device.</b></p>

## Add Access Control List (ACL) Rule

Click on *Add*. The following page is displayed:

Sequence Number	4
Rule Name	
Rule Enable	<input checked="" type="checkbox"/>
External Interface	WAN1 ▼
Internal IP Range	From: <input type="text"/> To: <input type="text"/>
External IP Range	From: <input type="text"/> To: <input type="text"/>
Protocol	* ▼
Service Port Range	From: <input type="text"/> To: <input type="text"/>
Action	ALLOW ▼

Confirm Cancel Changes

Field	Description
<b>Sequence Number</b>	This defines the sequence of the ACL rules. If a packet fits the conditions set by the ACL rules, the packet will then be sorted according to the first ACL rule from the top of the list.
<b>Rule Name</b>	Name of the ACL rule.
<b>Rule Enable</b>	Enable/Disable this ACL rule
<b>External Interface</b>	Please select which External Interface (WAN1 or WAN2) you want a packet to go through, IF the packet fits the condition of this ACL rule.
<b>Internal IP Range</b>	Set up the internal IP range for this ACL rule.
<b>External IP Range</b>	Set up the external IP range for this ACL rule.
<b>Protocol</b>	Set up the protocol (TCP or UDP) for the ACL to be enabled.
<b>Service Port Range</b>	Set up the Service Port Range (e.g., HTTP is TCP/80) for the ACL to be enabled.
<b>Action</b>	Select ALLOW / DENY



**Example: Filter and block MSN usage.**

---

For example, a company does not wish to allow employees to use MSN. The system administrator can set up an ACL action: rejecting the traffic going out to External IP Range at 207.46.110.\*/24.

Field	Description
Rule Name	MSN Blocking
Rule Enable	Enable
External Interface	* (All complies)
Internal IP Range	Keep it blank (All complies)
External IP Range	207.46.110.1:207.46.110.1.254 (IP address range for MSN server)
Protocol	TCP
Service Port Range	Keep it blank (All complies)
Action	DENY

# 21 Security - MAC Access Control Setting

From the *Security* menu, click on *MAC Access Control*. The following page is displayed:

## Security - MAC Access Control

**MAC Access Control**

MAC Access Control
☒ Enable
☐ Disable

Default MAC Access Control Action
☒ ALLOW
☐ DENY

**MAC Access Control Rule**

Rule Enable	Action	ACL Enable	Static DHCP Enable	IP
<input type="button" value="Add"/>	<input type="button" value="Delete"/>	<input type="button" value="Modify"/>	<input type="button" value="Up"/>	<input type="button" value="Down"/>

Field	Description
<b>MAC Access Control</b>	Choose Enable/Disable to enable/disable MAC access Control
<b>Default MAC Access Control Action</b>	<p>The default ACL action of the ACL rules. When you add the individual rules, it can be viewed as exceptions and take effects relating to the default action.</p> <p>If the action of the adding rule is the same as the default action, then this rule will not work.</p>

## Add MAC Access Control Rule

Click on *Add*. The following page is displayed:

Sequence Number	<input type="text" value="1"/>
Rule Name	<input type="text"/>
MAC	<input type="text"/>
Action	ALLOW <input type="button" value="v"/>
ACL Enable	<input checked="" type="checkbox"/>
Static ARP Enable	<input checked="" type="checkbox"/>
Static DHCP Enable	<input checked="" type="checkbox"/>
IP	<input type="text"/>

Field	Description
<b>Sequence Number</b>	<b>This defines the sequence (priority) of all the MAC ACL actions.</b>
<b>Rule Name</b>	<b>Name of the MAC access rule.</b>
<b>MAC</b>	<b>Set up the MAC Address to which you would like to enable the MAC ACL action.</b>
<b>Action</b>	<b>Choose ALLOW/DENY to ALLOW/DENY</b>
<b>ACL Enable</b>	<b>Enable/Disable this MAC access rule</b>
<b>Static ARP Enable</b>	<b>Enable/Disable this Static ARP rule</b>
<b>Static DHCP Enable</b>	<b>Enable/Disable this Static DHCP rule</b>
<b>IP</b>	<b>The IP address corresponds to static ARP or static DHCP.</b>

### **Example: Bind IP to a MAC**

---

If users need to bind a IP to a specified MAC (network device), one can follow the settings as below.

Field	Description
Sequence Number	User1
Rule Name	Enable
MAC	00:33:44:55:66:77
Action	Allow Access
ACL Enable	Enable
Static ARP Enable	Enable
Static DHCP Enable	Enable
IP	192.168.1.100

## 22 Security - Web Filtering Setting

From the *Security* menu, click on *Web Filtering*. The following page is displayed:

### Security - Web Filtering

**Web Filtering**

Web Filtering
☐ Enable
☒ Disable

**Web Content Filtering**

Activex Filtering
☐ Enable
☒ Disable

Java/JavaScript Filtering
☐ Enable
☒ Disable

Proxy Filtering
☐ Enable
☒ Disable

**Web Filtering Rule**

Rule Enable	Filter Keyword	Filter Type	Action
<input type="button" value="Add"/> <input type="button" value="Delete"/> <input type="button" value="Modify"/> <input type="button" value="Up"/> <input type="button" value="Down"/>			

Field	Description
<b>Web Filtering</b>	<b>Choose Enable/Disable to enable/disable Web Filtering</b>
<b>Activex Filtering</b>	<b>Choose Enable/Disable to enable/disable Activex Filtering</b>
<b>Java/JavaScript Filtering</b>	<b>Choose Enable/Disable to enable/disable Java/JavaScript Filtering</b>
<b>Proxy Filtering</b>	<b>Choose Enable/Disable to enable/disable Proxy Filtering</b>

## Add Web Filtering Rule

Click on *Add*. The following page is displayed:

Sequence Number	<input type="text" value="1"/>
Rule Enable	<input type="checkbox"/>
Filter Keyword	<input type="text" value="web-page-name"/>
Filter Type	<input type="text" value="url"/>
Action	<input type="text" value="DENY"/>

Field	Description
Sequence Number	This defines the sequence (priority) of all the Web Filtering rules.
Rule Enable	Choose Enable/Disable to enable/disable Web Filtering rule
Filter Keyword	Enter the Keyword
Filter Type	Choose URL or Sever
Action	Select ALLOW / DENY

### **Example: Block a URL with Keyword**

If one need to block Facebook related web page, can follow the settings as below.

Sequence Number	<input type="text" value="1"/>
Rule Enable	<input checked="" type="checkbox"/>
Filter Keyword	<input type="text" value="facebook"/>
Filter Type	<input type="text" value="url"/>
Action	<input type="text" value="DENY"/>

## 23 Bandwidth - INTELLIGENT DYNAMIC BANDWIDTH MANAGEMENT

Intelligent Bandwidth Management (iDBM) provides two powerful and unique mechanisms to manage bandwidth: Static Bandwidth Management (SBM) and Dynamic Bandwidth Management (DBM). SBM provides users with the option to allocate a fixed amount of bandwidth for a specific computer or a particular application, while DBM intellectually manages the rest of the bandwidth while all the time satisfying the complicated bandwidth requirements/settings of SBM.

The essential configuration needed by iDBM is to specify accurately the bandwidth you have. iDBM would then dispatch bandwidth according to this information. Please Note: Improper bandwidth assignment may cause iDBM to work ineffectively.

From the *Bandwidth* menu, click on *iDBM*. The following page is displayed:

### Bandwidth - iDBM

**Intelligent Dynamic Bandwidth Management (iDBM)**

iDBM
☐ Enable
☒ Disable

**DBM - WAN 1**

Bandwidth Type (Upload)
ADSL 2M / 256K bps
Upload Bandwidth
256 K bps
Reserved Buffering Bandwidth
25 %
(Too less reserved buffering bandwidth might cause congestion in a unstable network.)
Available Bandwidth
192.0 Kbps

**Bandwidth Management Group**

Group Name	Upload Rate	Upload Ceil
group1	10	100
group2	10	100
group3	10	100
group4	10	100

Add
Delete
Modify

**Static Bandwidth Management (SBM)**

Rule Name	Enable	IP Address	Application	External Interface	Bandwidth
SBM	✗	192.168.1.20		WAN1	20 %

Add
Delete
Modify
Up
Down

Save Settings
Cancel Changes



## DBM - WAN 1 Settings

Please adjust your bandwidth type according to your bandwidth (download/upload) subscribed from your ISP. Due to the unstable nature of network bandwidth supported by ISP, users are recommended to reserve a portion of bandwidth for buffering usage, and iDBM would then arrange the reserved bandwidth under heavy traffic.

### DBM - WAN 1

Bandwidth Type (Upload)	ADSL 2M / 256K bps
Upload Bandwidth	256 K bps
Reserved Buffering Bandwidth	25 %
(Too less reserved buffering bandwidth might cause congestion in a unstable network.)	
Available Bandwidth	192.0 Kbps

Field	Description
<b>Bandwidth Type (Download/Upload)</b>	<b>Select the correct bandwidth type according to your Internet service subscription. If the bandwidth type is not available on the list, select Custom.</b>
<b>Upload Bandwidth</b>	<b>Enter the value to customize upload bandwidth.</b>
<b>Reserved Buffering Bandwidth</b>	<b>Enter the value to provide bandwidth buffer.</b>

## Modify Bandwidth Management Group Rule

Click on one of *Bandwidth Management Group* and then click on *Modify*. The following page is displayed:

Sequence Number	<input type="text" value="1"/>
Group Name	<input type="text" value="group1"/>
Upload rate(%)	<input type="text" value="10"/>
Upload ceil(%)	<input type="text" value="100"/>

Field	Description
<b>Sequence Number</b>	<b>Enter the Sequence Number</b>
<b>Group Name</b>	<b>Enter the Group Name</b>
<b>Upload (Minimum) rate(%)</b>	<b>Enter the Minimum rate of bandwidth</b>
<b>Upload (Maximum) ceil(%)</b>	<b>Enter the Maximum rate of bandwidth</b>

## Add Static Bandwidth Management (SBM) Rule

Click on *Add*. The following page is displayed:

Sequence Number	<input type="text" value="2"/>
Rule Name	<input type="text"/>
Rule Enable	<input checked="" type="checkbox"/>
Internal IP Address	<input type="text"/>
Protocol	<input type="text" value="*"/> ▼
Service Port Range	From: <input type="text"/> To: <input type="text"/>
Available Bandwidth	
WAN1:	1536.0 Kbps
Bandwidth Allocation	By Ratio ▼
Ratio	<input type="text"/> %
Utilize Bandwidth More Than Guaranteed	<input type="checkbox"/>
DSCP	Disabled ▼
Remark DSCP	Disabled ▼

Field	Description
<b>Sequence Number</b>	<b>This defines the sequence of the SBM rules. If a packet fits the conditions set by the SBM rules, the packet will then be sorted according to the first SBM rule from the top of the list.</b>
<b>Rule Name</b>	<b>Name of the SBM rule.</b>
<b>Rule Enable</b>	<b>Enable/Disable this SBM rule</b>
<b>Internal IP</b>	<b>Set up the internal IP for this SBM rule.</b>
<b>Protocol</b>	<b>Set up the protocol (TCP or UDP) for the ACL to be enabled.</b>
<b>Service Port Range</b>	<b>Set up the Service Port Range (e.g., HTTP is TCP/80) for the SBM to be enabled.</b>
<b>Bandwidth Allocation</b>	<b>By Ratio, Group or By Bandwidth</b>
<b>Ratio</b>	<b>The ratio of the whole bandwidth according to the External Interface.</b>
<b>Utilize Bandwidth More than Guaranteed</b>	<b>Check this box if you wish to allow the traffic confirming this SBM rule to be able to utilize the whole bandwidth when the bandwidth is idle.</b>
<b>DSCP</b>	<b>Select the DSCP from the drop-down list</b>
<b>Remark DSCP</b>	<b>Select the remark DSCP from the drop-down list</b>

## 24 Bandwidth - Throughput Optimizer

The device built in iDBM transmits the important packets in high priority to optimize the network utilization. You can specify the types of packets for high priority.

From the *Bandwidth* menu, click on *Throughput Optimizer*. The following page is displayed:

### Bandwidth - Throughput Optimizer

**Throughput Optimizer**

Throughput Optimizer
☒ Enable
☐ Disable

**Application Priority**

TCP ACK
☒ Enable
☐ Disable

ICMP
☒ Enable
☐ Disable

DNS
☒ Enable
☐ Disable

SSH
☒ Enable
☐ Disable

Telnet (BBS)
☒ Enable
☐ Disable

TCP Max Segment Size
☒ Enable
☐ Disable

Save Settings
Cancel Changes

Field	Description
TCP ACK	Select Enable/Disable to enable/disable TCP ACK priority
ICMP	Select Enable/Disable to enable/disable ICMP priority
DNS	Select Enable/Disable to enable/disable DNS priority
SSH	Select Enable/Disable to enable/disable SSH priority
Telnet (BBS)	Select Enable/Disable to enable/disable Telnet (BBS) priority
TCP Max Segment Size	Select Enable/Disable to enable/disable TCP Max Segment Size

## 25 Bandwidth - TurboNAT

NAT is often the performance bottleneck in an IP sharing device. Generic routers are generally insufficient when dealing with a high-speed broadband network. Therefore, TurboNAT is designed to solve this problem. By accelerating the NAT performance, TurboNAT allows the device to fulfill the higher speed network and to reserve the system performance for other features such as ACL and VPN servers.

From the *Bandwidth* menu, click on *TurboNAT*. The following page is displayed:

### Bandwidth - TurboNAT

**Hardware NAT**

Hardware NAT ☒ Enable ☐ Disable

**TurboNAT**

TurboNAT ☒ Enable ☐ Disable

Save Settings

Cancel Changes

Field	Description
Hardware NAT	Select Enable/Disable to enable/disable Hardware NAT.
TurboNAT	Select Enable/Disable to enable/disable TurboNAT.

## 26 Applications - Port Range Forward

By activating the port range forwarding function, remote users can access the local network via the public IP address. Users can assign a specific external port range to a local server. Furthermore, users can specify an internal port range associated in a port range forwarding rule. When the device receives an external request to access any one of the configured external ports, it will redirect the request to the corresponding internal server and change its destination port to one of the internal ports specified. Therefore, if users do not wish for destination port to be changed for a request, the internal port range should be left empty.

Certain applications in a LAN are available only after activating the port range forwarding, including servers and online gaming. When an Internet request wants to access a port, the device will dispatch it to the IP specified. Due to security reasons, users are suggested to limit the use of port range forwarding, and cancel it when the application is not used.

By enabling DMZ Host Function, you can set up a DMZ host at a particular computer exposed to the Internet. In this way, some applications, especially online games (if the traffic port numbers of the applications are always changing), can be easily accessed.

From the *Applications* menu, click on *Port Range Forward*. The following page is displayed:

## Applications - Port Range Forward

## DMZ - WAN 1

DMZ ☐ Enable ☒ Disable

DMZ mode ☐ DMZ ☒ Super DMZ

DMZ IP Address

DMZ MAC Address

## Port Range Forwarding

Port Forwarding ☒ Enable ☐ Disable

## Port Range Forwarding Rule

Rule Name	Rule Enable	External Interface	Protocol	External Port Range	Internal IP	Internal Port Range
HTTP	×	WAN1	TCP	From:80 To:80	192.168.1.20	From: To:
HTTPS	×	WAN1	TCP	From:443 To:443	192.168.1.20	From: To:
POP3	×	WAN1	TCP	From:110 To:110	192.168.1.20	From: To:
POP3S	×	WAN1	TCP	From:995 To:995	192.168.1.20	From: To:
SMTP	×	WAN1	TCP	From:25 To:25	192.168.1.20	From: To:
SMTPS	×	WAN1	TCP	From:465 To:465	192.168.1.20	From: To:
SSH	×	WAN1	TCP	From:22 To:22	192.168.1.21	From: To:
eMule	×	WAN1	TCP/UDP	From:4662 To:4672	192.168.1.21	From: To:

## DMZ - WAN 1 Settings

### DMZ - WAN 1

DMZ ☐ Enable ☒ Disable

DMZ mode ☐ DMZ ☒ Super DMZ

DMZ IP Address

DMZ MAC Address

Field	Description
<b>DMZ</b>	Select Enable to enable DMZ function. Select Disable to disable DMZ function.
<b>DMZ mode</b>	Select DMZ or Super DMZ mode
<b>DMZ 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>DMZ MAC Address</b>	Enter the MAC address of a particular host in your LAN which will get the same Public IP address of WAN port and receive all the packets going to this Public IP address.

## Port Range Forwarding Settings

### Port Range Forwarding

Port Forwarding ☒ Enable ☐ Disable

Field	Description
<b>Port Forwarding</b>	Select Enable / Disable to enable/disable Port Forwarding



## Add Port Range Forwarding Rule

Click on *Add*. The following page is displayed:

Sequence Number	<input type="text" value="9"/>
Rule Name	<input type="text"/>
Rule Enable	<input type="checkbox"/>
External Interface	<input type="text" value="WAN1"/>
Protocol	<input type="text" value="TCP"/>
External Port Range	From: <input type="text"/> To: <input type="text"/>
Internal IP	<input type="text"/>
Internal Port Range	From: <input type="text"/> To: <input type="text"/>

Field	Description
<b>Sequence Number</b>	<b>This defines the sequences (priorities) of the port forwarding rules. If a packet fits the conditions setup by the port forwarding rules, the packet will then be forwarded according to the 1st rule from the top of the list.</b>
<b>Rule Name</b>	<b>Enter the name of the port forwarding rule.</b>
<b>Rule Enable</b>	<b>Check/Uncheck to enable/disable this port forwarding rule.</b>
<b>External Interface</b>	<b>Choose WAN1 as the External port forwarding interface.</b>
<b>Protocol</b>	<b>Choose TCP, UDP or TCP/UDP for the rule to be applied.</b>
<b>External Port Range</b>	<b>Set up the External Port Range for the rule to be applied.</b>
<b>Internal IP</b>	<b>Set up the Internal IP for the rule to be applied.</b>
<b>Internal Port Range</b>	<b>Set up the Internal Port Range for the rule to be applied.</b>

## 27 Applications - Virtual Hosts

From the *Applications* menu, click on *Virtual Hosts*. The following page is displayed:

### Applications - Virtual Hosts

**Virtual Hosts**  
Virtual Hosts ☒ Enable ☐ Disable

**Virtual Host Rule**

Rule Name	Rule Enable	External Interface	External IP Address	Mapped LAN IP Address
<input type="button" value="Add"/>	<input type="button" value="Delete"/>	<input type="button" value="Modify"/>	<input type="button" value="Up"/>	<input type="button" value="Down"/>

Field	Description
<b>Virtual Hosts</b>	<b>Select Enable/Disable to enable/disable Virtual Hosts.</b>

## Add Virtual Host Rule

Click on *Add*. The following page is displayed:

Sequence Number	<input type="text" value="1"/>
Rule Name	<input type="text"/>
Rule Enable	<input type="checkbox"/>
External Interface	<input type="text" value="WAN1"/>
External IP Address	<input type="text"/>
Mapped LAN IP Address	<input type="text"/>

Field	Description
Sequence Number	This defines the sequences (priorities) of the Virtual Host rules.
Rule Name	Enter the name of the Virtual Host rule.
Rule Enable	Check/Uncheck to enable/disable this Virtual Host rule.
External Interface	Choose WAN1 as the External Virtual Host interface.
External IP Address	Set up the External IP Address for the rule to be applied.
Mapped LAN IP Address	Set up the mapped Mapped LAN IP Address for the rule to be applied.

## 28 Applications - Streaming / VPN

You can enhance your media streaming quality by enabling RTSP, MSS, and H.323 protocols. Moreover, VPN Pass-through functionality can also be enabled.

From the *Applications* menu, click on *Streaming / VPN*. The following page is displayed:

### Applications - Streaming / VPN

Streaming

RTSP

☒ Enable ☐ Disable

MMS

☒ Enable ☐ Disable

Video Conference

H.323

☒ Enable ☐ Disable

VPN

IPSec

☒ Enable ☐ Disable

PPTP

☒ Enable ☐ Disable

Save Settings

Cancel Changes

### Streaming Settings

Streaming

RTSP

☒ Enable ☐ Disable

MMS

☒ Enable ☐ Disable

Field	Description
RTSP	Select Enable/Disable to enable/disable RTSP
MMS	Select Enable/Disable to enable/disable MMS

## Streaming Settings

### Video Conference

H.323

☒ Enable ☐ Disable

Field	Description
H.323	Select Enable/Disable to enable/disable H.323

## VPN Pass-through Settings

### VPN

IPSec

☒ Enable ☐ Disable

PPTP

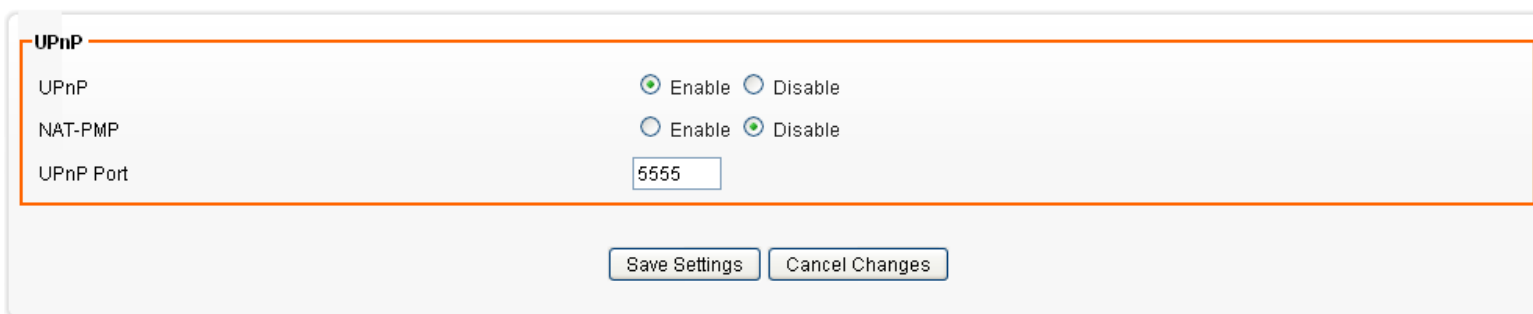
☒ Enable ☐ DisableSave SettingsCancel Changes

Field	Description
IPSec Pass-through	Select Enable/Disable to enable/disable IPSec Pass-through
PPTP Pass-through	Select Enable/Disable to enable/disable PPTP Pass-through

## 29 Applications - UPnP / NAT-PMP

From the *Applications* menu, click on *UPnP / NAT-PMP*. The following page is displayed:

### Applications - UPnP / NAT-PMP



UPnP

UPnP ☒ Enable ☐ Disable

NAT-PMP ☐ Enable ☒ Disable

UPnP Port

Save Settings Cancel Changes

Field	Description
UPnP	Select Enable/Disable to enable/disable UPnP
NAT-PMP	Select Enable/Disable to enable/disable NAT-PMP
UPnP Port	Enter the number for UPnP port.

## 30 Admin - Management

From the *Admin* menu, click on *Management*. The following page is displayed:

### Admin - Management

**Administration Interface**

Language

English ▾

Administrator Password

.....

Re-type Password

.....

Remote Management

☐ Enable ☒ Disable

Remote Management Port

HTTP 8080

Management Port

HTTP 80

SNMP

☒ Enable ☐ Disable

QoS-WRR

☐ Enable ☒ Disable

**Reboot**

Reboot

Reboot Router

**Configuration**

Configuration Export

Export

Default Configuration Restore

Default

Configuration Import

Przeglądaj... Import

**Firmware**

Firmware Upgrade

Przeglądaj... Upgrade

Save Settings

Cancel Changes

## Administration Interface Settings

### Administration Interface

Language	English ▼
Administrator Password	.....
Re-type Password	.....
Remote Management	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Remote Management Port	HTTP 8080
Management Port	HTTP 80
SNMP	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
QoS-WRR	<input type="radio"/> Enable <input checked="" type="radio"/> Disable

Field	Description
<b>Language</b>	Select the language of administration Interface you wish to use.
<b>Administrator Password</b>	Maximum input is 36 alphanumeric characters (case sensitive) * Please change the administrator's password if the remote management is enabled. Otherwise, a malicious user can access the management interface. This user can then have the ability to change the settings and damage your network access.
<b>Re-type Password</b>	Enter the password again to confirm.
<b>Remote Management</b>	Select Enable to enable Remote Management. Select Disable to disable Remote Management If the remote management is enabled, users who are not in the LAN can connect to the device and configure it from the Internet.
<b>Remote Management Port</b>	HTTP port which users can remote connect to. (default port is 8080)
<b>Management Port</b>	HTTP port which users can connect to. (default port is 80)
<b>SNMP</b>	Select Enable to enable SNMP. Select Disable to disable SNMP.

## Reboot Settings

### Reboot

Reboot	<button>Reboot Router</button>
--------	--------------------------------

Field	Description
<b>Reboot</b>	Click this button to reboot the device.



## Configuration Settings

### Configuration

Configuration Export

Export

Default Configuration Restore

Default

Configuration Import

Browse...

Import

Field	Description
<b>Configuration Export</b>	Click this button to save your current configuration settings in a file.
<b>Default Configuration Restore</b>	Click this button to recover the default system settings.
<b>Configuration Import</b>	Click Browse and Import to load previous configuration settings.

## Firmware Upgrade Settings

### Firmware

Firmware Upgrade

Browse...

Upgrade

Field	Description
<b>Firmware Upgrade</b>	Click Browse and Upgrade button to upgrade the firmware.

## APS Settings

### APS

Configuration Host	<input type="text"/>
Configuration Config Name	<input type="text"/> <input type="button" value="Import"/>
Upgrade Host	<input type="text"/>
Upgrade Firmware Name	<input type="text"/> <input type="button" value="Upgrade"/>

Field	Description
<b>Configuration Host</b>	<b>Enter the IP Address of the TFTP Server</b>
<b>Configuration Config Name</b>	<b>Enter the configuration config file name and then click Import button to update configuration config from TFTP Server</b>
<b>Upgrade Host</b>	<b>Enter the IP Address of the TFTP Server</b>
<b>Upgrade Firmware Name</b>	<b>Enter the firmware file name and then click Upgrade button to update firmware from TFTP Server</b>

# 31 Admin - System Utilities

From the *Admin* menu, click on *System Utilities*. The following page is displayed:

## Admin - System Utilities

### Ping

Interface	<input type="text" value="*"/>
Target Host	<input type="text"/>
Number of Packets	<input type="text" value="4"/> Packets (1 ~ 10)
Ping	<input type="button" value="Ping"/>

### ARPing (Within the same broadcasting domain)

Interface	<input type="text" value="WAN1"/>
Target Host	<input type="text"/>
Number of Packets	<input type="text" value="4"/> Packets (1 ~ 10)
ARPing	<input type="button" value="ARPing"/>

### Trace Route

Interface	<input type="text" value="*"/>
Target Host	<input type="text"/>
Hop Count	<input type="text" value="4"/> Counts (1 ~ 15)
Trace route	<input type="button" value="Trace Route"/>

## Ping Settings

### Ping

Interface	<input type="text" value="*"/>
Target Host	<input type="text"/>
Number of Packets	<input type="text" value="4"/> Packets (1 ~ 10)
Ping	<input type="button" value="Ping"/>

Field	Description
Interface	Select the interface that use to ping to, ie. LAN, WAN.
Target Host	Enter the IP address to ping to
Number of Packets	Specify the number of the ICMP packets to send out
Ping	Press the tab to start the “ping” actions

## ARPing (Within the same broadcasting domain) Settings

### ARPing (Within the same broadcasting domain)

Interface	<input type="text" value="WAN1"/>
Target Host	<input type="text"/>
Number of Packets	<input type="text" value="4"/> Packets (1 ~ 10)
ARPing	<input type="button" value="ARPing"/>

Field	Description
Interface	Select the interface that use to ARPing to, ie. LAN, WAN.
Target Host	Enter the MAC address to ARPing to
Number of Packets	Specify the number of the ARP request packets to send out
ARPing	Press the tab to start the “ARPing” actions

## Trace Route Settings

### Trace Route

Interface	<input type="text" value="*"/>
Target Host	<input type="text"/>
Hop Count	<input type="text" value="4"/> Counts (1 ~ 15)
Trace route	<input type="button" value="Trace Route"/>

Field	Description
Interface	Select the interface that use to Trace Route to, ie. LAN, WAN.
Target Host	Enter the destination IP address / domain name to trace
Hop Count	Specify the Hop number you need to trace
Trace route	Press the tab to start the “Trace Route” actions

## 32 Admin - TIME SETUP

From the *Admin* menu, click on *TIME*. The following page is displayed:

### Setup - Time

**Time Synchronization**

Time Synchronization
☒ Enable
☐ Disable

Time Server Type
☒ Time Server Pool
☐ Manual

Time Server Area
Automatic

Time Server IP Address

Time Zone
UTC+08:00 Taiwan, China, Hong Kong, Western Australia, Singapore

Periodic Synchronization
☒ Enable
☐ Disable

Synchronization Interval
Every Day

Action
Update

Save Settings
Cancel Changes

Field	Description
<b>Time Synchronization</b>	Select Enable/Disable to enable/disable Time Synchronization
<b>Time Server Type</b>	Select Time Server Pool /Manual
<b>Time Server Area</b>	Select Time Server according to your location. You can choose from Automatic, Asia, Europe, North America, South America, or Africa.
<b>Time Server IP Address</b>	Enter the IP Address of the Time Server
<b>Time Zone</b>	Select Time Zone according to your location. (Daylight Saving Time has been calculated and included in the selection).
<b>Periodic Synchronization</b>	Select Enable/Disable to enable/disable Periodic Synchronization
<b>Synchronization interval</b>	Select from Every Hour, Every 6 Hours, Every 12 Hours, Every Day, and Every Week.
<b>Action</b>	Click Update button to Sync the time immediately

# 33 Status - Router

From the *Status* menu, click on *Router*. The following page is displayed:

## Status - Router

**Router Information**

Model Name	Fibrain FSR-R2
Firmware Version	FSR-R2-Baltik-01
Current Time	Thu, 01 Jan 1970 01:18:03
Running Time	1 hour, 18 mins

**WAN 1**

MAC Address	00:13:33:97:94:26	
Connection Type	dhcp	
IP Address	Subnet Mask	WAN IP renew
Gateway		

**LAN 1**

MAC Address	00:13:33:97:94:26
IP Address	192.168.200.254
Subnet Mask	24
DHCP Service	Enabled
DHCP Start IP Address	192.168.200.100
DHCP End IP Address	192.168.200.200
Max DHCP Clients	101

**Wireless Network 1**

Wireless Channel	0
Wireless SSID 1	Fibrain
MAC Address	00:13:33:97:94:27
Wireless SSID 2	Fibrain2
MAC Address	Not enabled
Wireless SSID 3	Fibrain3
MAC Address	Not enabled
Wireless SSID 4	Fibrain4
MAC Address	Not enabled

Refresh

## Router Information Settings

### Router Information

Model Name	Fibrain FSR-R2
Firmware Version	FSR-R2-Baltyk-01
Current Time	Thu, 01 Jan 1970 01:18:03
Running Time	1 hour, 18 mins

Field	Description
<b>Model Name</b>	<b>Product model name is shown.</b>
<b>Firmware Version</b>	<b>The firmware version this device is running.</b>
<b>Current Time</b>	<b>Current system time</b>
<b>Running Time</b>	<b>The period of time that the device has been running.</b>

## WAN Settings

### WAN

MAC Address	00:13:33:07:00:9F
Connection Type	dhcp
IP Address	Subnet Mask
Gateway	

Field	Description
<b>MAC Address</b>	<b>MAC Address</b>
<b>Connection Type</b>	<b>The current connection type (PPPoE, Static IP, and DHCP)</b>
<b>IP Address</b>	<b>WAN IP Address</b>
<b>Subnet Mask</b>	<b>Number of subnet mask.</b>
<b>Gateway</b>	<b>IP address of the gateway</b>



## LAN Settings

### LAN

MAC Address	00:13:33:07:00:9F
IP Address	192.168.200.254
Subnet Mask	24
DHCP Service	Enabled
DHCP Start IP Address	192.168.200.100
DHCP End IP Address	192.168.200.200
Max DHCP Clients	101

Field	Description
<b>MAC Address</b>	<b>MAC Address</b>
<b>IP Address</b>	<b>Internal IP Address</b>
<b>Subnet Mask</b>	<b>The number of subnet mask in the internal network</b>
<b>DHCP Service</b>	<b>DHCP service enabled or disabled</b>
<b>DHCP Start IP Address</b>	<b>DHCP Start IP address</b>
<b>DHCP End IP Address</b>	<b>DHCP End IP address</b>
<b>Max DHCP Clients</b>	<b>The maximum IP addressed which can be assigned to PCs connecting to the network</b>

## Wireless Network 1 Settings

### Wireless Network 1

Wireless Channel	0
Wireless SSID 1	Fibrain
MAC Address	00:13:33:97:94:27
Wireless SSID 2	Fibrain2
MAC Address	Not enabled
Wireless SSID 3	Fibrain3
MAC Address	Not enabled
Wireless SSID 4	Fibrain4
MAC Address	Not enabled

Field	Description
<b>Wireless Channel</b>	<b>Wireless Channel in use (default is 6)</b>
<b>Wireless SSID 1</b>	<b>SSID 1 of this Wi-Fi station</b>
<b>MAC Address</b>	<b>MAC Address</b>
<b>Wireless SSID 2</b>	<b>SSID 2 of this Wi-Fi station</b>
<b>MAC Address</b>	<b>MAC Address</b>
<b>Wireless SSID 3</b>	<b>SSID 3 of this Wi-Fi station</b>
<b>MAC Address</b>	<b>MAC Address</b>
<b>Wireless SSID 4</b>	<b>SSID 4 of this Wi-Fi station</b>
<b>MAC Address</b>	<b>MAC Address</b>

## 34 Status - User / DHCP

From the *Status* menu, click on *User / DHCP*. The following page is displayed:

### Status - DHCP User

DHCP Table (1 user)			
Name	IP Address	MAC Address	Expiration Time
g31m-713b15bd66	192.168.200.100	00:24:1d:c4:b4:a0	00:46:15
<div>Refresh</div>			

Field	Description
<b>Name</b>	<b>DHCP client name</b>
<b>IP Address</b>	<b>IP address which is assigned to this client</b>
<b>MAC Address</b>	<b>MAC address of this client</b>
<b>Expiration Time</b>	<b>The remaining time of the IP assignment</b>

## 35 Status – User / Current

From the *Status* menu, click on *User / Current*. The following page is displayed:

### Status - ARP User

ARP Table (1 user)		
IP Address	MAC Address	ARP Type
192.168.200.100	00:24:1d:c4:b4:c0	Dynamic
<div>Refresh</div>		

Field	Description
<b>IP Address</b>	<b>IP address which is assigned to this client</b>
<b>MAC Address</b>	<b>MAC address of this client</b>
<b>Expiration Time</b>	<b>The remaining time of the IP assignment</b>

# 36 Status – Log

From the *Status* menu, click on *Log*. The following page is displayed:

## Status - Log

### System Log

```
Jan 1 00:00:04 FS-service: boot [OK]
Jan 1 00:00:07 MODULE-service: boot [OK]
Jan 1 00:00:07 HOTPLUG-service: boot [OK]
Jan 1 00:00:07 USB-service: boot [OK]
Jan 1 00:00:13 lan1: up [OK] [192.168.200.254]
Jan 1 00:00:13 License-client: boot [OK]
Jan 1 00:00:16 ACL: service [boot] OK
Jan 1 00:00:17 WEB-server: boot [OK]
Jan 1 00:00:17 DHCP-server: boot [OK]
Jan 1 00:00:17 SSH-server: boot [OK]
Jan 1 00:00:17 SNMP-server: boot [OK]
Jan 1 00:00:17 TELNET-server: boot [OK]
Jan 1 00:00:17 TELNET-cl: boot [OK]
Jan 1 00:00:17 CRON-service: boot [OK]
Jan 1 00:00:18 TurboNAT: boot [OK]
Jan 1 00:00:18 Session-Manager: boot [OK]
Jan 1 00:00:19 wan1: down [OK] []
Jan 1 00:00:19 MON-server: boot [OK]
Jan 1 00:00:20 802.1X-RADIUS: stop [OK]
Jan 1 00:00:20 WANG: stop [OK]
Jan 1 00:00:20 TurboLink: stop [OK]
```

Refresh

# A

## Configuring your Computers

This appendix provides instructions for configuring the Internet settings on your computers to work with the Wireless Gateway.

### Configuring Ethernet PCs

---

#### Before you begin

By default, the Wireless Gateway automatically assigns the required Internet settings to your PCs. You need to configure the PCs to accept this information when it is assigned.



#### Note

In some cases, you may want to assign Internet information manually to some or all of your computers rather than allow the Wireless Gateway to do so. See *Assigning static Internet information to your PCs* for instructions.

- If you have connected your LAN PCs via Ethernet to the Wireless Gateway, follow the instructions that correspond to the operating system installed on your PC:
  - Windows® XP PCs
  - Windows 2000 PCs
  - Windows Me PCs
  - Windows 95, 98 PCs
  - Windows NT 4.0 workstations

#### Windows® XP PCs

1. In the Windows task bar, click the *Start* button, and then click *Control Panel*.
2. Double-click the Network Connections icon.
3. In the *LAN or High-Speed Internet* window, right-click on the icon corresponding to your network interface card (NIC) and select *Properties*. (Often, this icon is labeled *Local Area Connection*).

The *Local Area Connection* dialog box is displayed with a list of currently installed network items.

4. Ensure that the check box to the left of the item labeled *Internet Protocol TCP/IP* is checked and click *Properties*.
5. In the *Internet Protocol (TCP/IP) Properties* dialog box, click the radio button labeled *Obtain an IP address automatically*. Also click the radio button labeled *Obtain DNS server address automatically*.
6. Click *OK* twice to confirm your changes, and then close the Control Panel.

#### Windows 2000 PCs

First, check for the IP protocol and, if necessary, install it:

1. In the Windows task bar, click the *Start* button, point to *Settings*, and then click *Control Panel*.
2. Double-click the Network and Dial-up Connections icon.

3. In the *Network and Dial-up Connections* window, right-click the Local Area Connection icon, and then select *Properties*. The *Local Area Connection Properties* dialog box is displayed with a list of currently installed network components. If the list includes Internet Protocol (TCP/IP), then the protocol has already been enabled. Skip to step 10.
4. If Internet Protocol (TCP/IP) does not display as an installed component, click *Install...*
5. In the *Select Network Component Type* dialog box, select *Protocol*, and then click *Add...*
6. Select *Internet Protocol (TCP/IP)* in the Network Protocols list, and then click *OK*.  
You may be prompted to install files from your Windows 2000 installation CD or other media. Follow the instructions to install the files.
7. If prompted, click *OK* to restart your computer with the new settings.

Next, configure the PCs to accept IP information assigned by the Wireless Gateway:

8. In the *Control Panel*, double-click the Network and Dial-up Connections icon.
9. In the *Network and Dial-up Connections* window, right-click the Local Area Connection icon, and then select *Properties*.
10. In the Local Area Connection Properties dialog box, select *Internet Protocol (TCP/IP)*, and then click *Properties*.
11. In the *Internet Protocol (TCP/IP) Properties* dialog box, click the radio button labeled *Obtain an IP address automatically*. Also click the radio button labeled *Obtain DNS server address automatically*.
12. Click *OK* twice to confirm and save your changes, and then close the Control Panel.

### Windows Me PCs

1. In the Windows task bar, click the *Start* button, point to *Settings*, and then click *Control Panel*.
2. Double-click the Network and Dial-up Connections icon.
3. In the *Network and Dial-up Connections* window, right-click the Network icon, and then select *Properties*.

The *Network Properties* dialog box displays with a list of currently installed network components. If the list includes Internet Protocol (TCP/IP), then the protocol has already been enabled. Skip to step 11.

4. If Internet Protocol (TCP/IP) does not display as an installed component, click *Add...*
5. In the *Select Network Component Type* dialog box, select *Protocol*, and then click *Add...*
6. Select *Microsoft* in the Manufacturers box.
7. Select *Internet Protocol (TCP/IP)* in the Network Protocols list, and then click *OK*.

You may be prompted to install files from your Windows Me installation CD or other media. Follow the instructions to install the files.

8. If prompted, click *OK* to restart your computer with the new settings.

Next, configure the PCs to accept IP information assigned by the Wireless Gateway:

9. In the *Control Panel*, double-click the Network and Dial-up Connections icon.
10. In *Network and Dial-up Connections* window, right-click the Network icon, and then select *Properties*.
11. In the *Network Properties* dialog box, select *TCP/IP*, and then click *Properties*.
12. In the TCP/IP Settings dialog box, click the radio button labeled **Server** assigned IP address. Also click the radio button labeled *Server assigned name server address*.
13. Click *OK* twice to confirm and save your changes, and then close the *Control Panel*.

### Windows 95, 98 PCs

First, check for the IP protocol and, if necessary, install it:

1. In the Windows task bar, click the *Start* button, point to *Settings*, and then click *Control Panel*.
2. Double-click the Network icon.

The *Network* dialog box displays with a list of currently installed network components. If the list includes TCP/IP, and then the protocol has already been enabled. Skip to step 9.

3. If TCP/IP does not display as an installed component, click *Add...*

The *Select Network Component Type* dialog box displays.

4. Select *Protocol*, and then click *Add...*

The Select Network Protocol dialog box displays.



5. Click on *Microsoft* in the Manufacturers list box, and then click *TCP/IP* in the Network Protocols list box.
6. Click *OK* to return to the Network dialog box, and then click *OK* again.

You may be prompted to install files from your Windows 95/98 installation CD. Follow the instructions to install the files.

7. Click *OK* to restart the PC and complete the TCP/IP installation.

Next, configure the PCs to accept IP information assigned by the Wireless Gateway:

8. Open the Control Panel window, and then click the Network icon.
9. Select the network component labeled TCP/IP, and then click *Properties*.

If you have multiple TCP/IP listings, select the listing associated with your network card or adapter.

10. In the TCP/IP Properties dialog box, click the IP Address tab.
11. Click the radio button labeled *Obtain an IP address automatically*.
12. Click the DNS Configuration tab, and then click the radio button labeled *Obtain an IP address automatically*.
13. Click *OK* twice to confirm and save your changes.  
You will be prompted to restart Windows.
14. Click *Yes*.

### **Windows NT 4.0 workstations**

First, check for the IP protocol and, if necessary, install it:

1. In the Windows NT task bar, click the *Start* button, point to *Settings*, and then click *Control Panel*.
2. In the Control Panel window, double click the Network icon.
3. In the *Network dialog* box, click the *Protocols* tab.

The *Protocols* tab displays a list of currently installed network protocols. If the list includes TCP/IP, then the protocol has already been enabled. Skip to step 9.

4. If TCP/IP does not display as an installed component, click *Add...*
5. In the *Select Network Protocol* dialog box, select *TCP/IP*, and then click *OK*.

You may be prompted to install files from your Windows NT installation CD or other media. Follow the instructions to install the files.

After all files are installed, a window displays to inform you that a TCP/IP service called DHCP can be set up to dynamically assign IP information.

6. Click *Yes* to continue, and then click *OK* if prompted to restart your computer.

Next, configure the PCs to accept IP information assigned by the Wireless Gateway:

7. Open the Control Panel window, and then double-click the Network icon.
8. In the *Network* dialog box, click the *Protocols* tab.
9. In the *Protocols* tab, select *TCP/IP*, and then click *Properties*.
10. In the *Microsoft TCP/IP Properties* dialog box, click the radio button labeled *Obtain an IP address from a DHCP server*.
11. Click *OK* twice to confirm and save your changes, and then close the Control Panel.

### Assigning static Internet information to your PCs

If you are a typical user, you will not need to assign static Internet information to your LAN PCs because your ISP automatically assigns this information for you.

In some cases however, you may want to assign Internet information to some or all of your PCs directly (often called “statically”), rather than allowing the Wireless Gateway to assign it. This option may be desirable (but not required) if:

- You have obtained one or more public IP addresses that you want to always associate with specific computers (for example, if you are using a computer as a public web server).
- You maintain different subnets on your LAN (subnets are described in Appendix B).

Before you begin, you must have the following information available:

- The IP address and subnet mask of each PC
- The IP address of the default gateway for your LAN. In most cases, this is the address assigned to the LAN port on the Wireless Gateway. By default, the LAN port is assigned the IP address *192.168.200.254*. (You can change this number or another number can be assigned by your ISP. See *Addressing* for more information.)
- The IP address of your ISP's Domain Name System (DNS) server.

On each PC to which you want to assign static information, follow the instructions relating only to checking for and/or installing the IP protocol. Once it is installed, continue to follow the instructions for displaying each of the Internet Protocol (TCP/IP) properties. Instead of enabling dynamic assignment of the IP addresses for the computer, DNS server and default gateway, click the radio buttons that enable you to enter the information manually.



*Your PCs must have IP addresses that place them in the same subnet as the Wireless Gateway's LAN port. If you manually assign IP information to all your LAN PCs, you can follow the instructions in Addressing to change the LAN port IP address accordingly.*

# B IP Addresses, Network Masks, and Subnets

## IP Addresses



### Note

*This section refers only to IP addresses for IPv4 (version 4 of the Internet Protocol). IPv6 addresses are not covered.*

*This section assumes basic knowledge of binary numbers, bits, and bytes.*

IP addresses, the Internet's version of telephone numbers, are used to identify individual nodes (computers or devices) on the Internet. Every IP address contains four numbers, each from 0 to 255 and separated by dots (periods), e.g. 20.56.0.211. These numbers are called, from left to right, field1, field2, field3, and field4.

This style of writing IP addresses as decimal numbers separated by dots is called *dotted decimal notation*. The IP address 20.56.0.211 is read "twenty dot fifty-six dot zero dot two-eleven."

### Structure of an IP address

IP addresses have a hierarchical design similar to that of telephone numbers. For example, a 7-digit telephone number starts with a 3-digit prefix that identifies a group of thousands of telephone lines, and ends with four digits that identify one specific line in that group.

Similarly, IP addresses contain two kinds of information:

- *Network ID*  
Identifies a particular network within the Internet or intranet
- *Host ID*  
Identifies a particular computer or device on the network

The first part of every IP address contains the network ID, and the rest of the address contains the host ID. The length of the network ID depends on the network's *class* (see following section). The table below shows the structure of an IP address.

	Field1	Field2	Field3	Field4
Class A	Network ID	Host ID		
Class B	Network ID		Host ID	
Class C	Network ID			Host ID

Here are some examples of valid IP addresses:

Class A: 10.30.6.125 (network = 10, host = 30.6.125)

Class B: 129.88.16.49 (network = 129.88, host = 16.49)

Class C: 192.60.201.11 (network = 192.60.201, host = 11)

### Network classes

The three commonly used network classes are A, B, and C. (There is also a class D but it has a special use beyond the

scope of this discussion.) These classes have different uses and characteristics.

Class A networks are the Internet's largest networks, each with room for over 16 million hosts. Up to 126 of these huge networks can exist, for a total of over 2 billion hosts. Because of their huge size, these networks are used for WANs and by organizations at the infrastructure level of the Internet, such as your ISP.

Class B networks are smaller but still quite large, each able to hold over 65,000 hosts. There can be up to 16,384 class B networks in existence. A class B network might be appropriate for a large organization such as a business or government agency.

Class C networks are the smallest, only able to hold 254 hosts at most, but the total possible number of class C networks exceeds 2 million (2,097,152 to be exact). LANs connected to the Internet are usually class C networks.

Some important notes regarding IP addresses:

- The class can be determined easily from field1:  
field1 = 1-126:                      Class A  
field1 = 128-191:                    Class B  
field1 = 192-223:                    Class C  
(field1 values not shown are reserved for special uses)
- A host ID can have any value except all fields set to 0 or all fields set to 255, as those values are reserved for special uses.

## Subnet masks

---



### Definition mask

*A mask looks like a regular IP address, but contains a pattern of bits that tells what parts of an IP address are the network ID and what parts are the host ID: bits set to 1 mean "this bit is part of the network ID" and bits set to 0 mean "this bit is part of the host ID."*

*Subnet masks* are used to define *subnets* (what you get after dividing a network into smaller pieces). A subnet's network ID is created by "borrowing" one or more bits from the host ID portion of the address. The subnet mask identifies these host ID bits.

For example, consider a class C network 192.168.1. To split this into two subnets, you would use the subnet mask:

255.255.255.128

It's easier to see what's happening if we write this in binary:

11111111. 11111111. 11111111.10000000

As with any class C address, all of the bits in field1 through field3 are part of the network ID, but note how the mask specifies that the first bit in field4 is also included. Since this extra bit has only two values (0 and 1), this means there are two subnets. Each subnet uses the remaining 7 bits in field4 for its host IDs, which range from 1 to 126 hosts (instead of the usual 0 to 255 for a class C address).

Similarly, to split a class C network into four subnets, the mask is:

255.255.255.192 or 11111111.11111111.  
11111111.11000000

The two extra bits in field4 can have four values (00, 01, 10, 11), so there are four subnets. Each subnet uses the remaining six bits in field4 for its host IDs, ranging from 1 to 62.



*Sometimes a subnet mask does not specify any additional network ID bits, and thus no subnets. Such a mask is called a default subnet mask. These masks are:*

Class A: 255.0.0.0  
Class B: 255.255.0.0  
Class C: 255.255.255.0

*These are called default because they are used when a network is initially configured, at which time it has no subnets.*

## C UPnP Control Point Software on Windows ME/XP

This appendix provides instructions for configuring the UPnP on your computers to work with the Wireless Gateway.

UPnP is an architecture for pervasive peer-to-peer network connectivity of intelligent appliances, Wireless devices, and PCs of all form factors. It is designed to bring easy-to-use, flexible, standards-based connectivity to ad-hoc or unmanaged networks whether in the home, in a small business, public spaces, or attached to the Internet. UPnP is a distributed, open networking architecture that leverages TCP/IP and the Web technologies to enable seamless proximity networking in addition to control and data transfer among networked devices in the home, office, and public spaces.

UPnP is more than just a simple extension of the plug and play peripheral model. It is designed to support zero-configuration, "invisible" networking, and automatic discovery for a breadth of device categories from a wide range of vendors. This means a device can dynamically join a network, obtain an IP address, convey its capabilities, and learn about the presence and capabilities of other devices. DHCP and DNS servers are optional and are used only if available on the network. Finally, a device can leave a network smoothly and automatically without leaving any unwanted state behind.

### **UPnP Control Point Software on Windows ME**

---

To install the control point software on Windows ME:

1. In the Control Panel, select "Add/Remove Programs".
2. In the "Add/Remove Programs Properties" dialog box, select the "Windows Setup" tab. In the "Components" list, double click on the "Communications" entry.
3. In the "Communications" dialog box, scroll down the "Components" list to display the UPnP entry. Select the entry, click "OK".
4. Click "OK" to finish the "Add/Remove Programs" dialog.
5. Reboot your system.

Once you have installed the UPnP software and you have rebooted (and your network includes the IGD system), you should be able to see the IGD controlled device on your network.

## UPnP Control Point Software on Windows XP with Firewall

---

On Windows XP versions earlier than SP2, Firewall support is provided by the Windows XP Internet Connection Firewall. You cannot use the Windows XP Internet Connection Firewall support on a system that you intend to use as a UPnP control point. If this feature is enabled, although the control point system may display controlled devices in the list of network devices, the control point system cannot participate in UPnP communication. (This restriction also applies to controlled devices running on Windows XP systems earlier than SP2.)

On Windows XP SP2 and later, Firewall support is provided by Windows Firewall. Unlike earlier versions, Windows XP SP2 can be used on a system that you intend to use as a UPnP control point.

To turn off the Firewall capability on any version of Windows XP, follow the steps below:

1. In the Control Panel, select "Network and Internet Connections".
2. In the "Network and Internet Connections" dialog box, select "Network Connections".
3. In the "Network Connections" dialog box, right-click on the local area connection entry for your network; this will display a menu. Select the "Properties" menu entry.
4. In the "Local Area Connection Properties" dialog box, select the "Advanced" tab. Disable the Internet Connection Firewall by de-selecting the entry with the following label:  
"Protect my computer and network by limiting or preventing access to the computer from the Internet".
5. Click "OK".

### SSDP requirements

You must have SSDP Discovery Service enabled on your Windows XP system to use the UPnP Control point software.

SSDP Discovery Service is enabled on a default installation of Windows XP. To check if it is enabled on your system, look in Control Panel > Administrative Tools > Services).

### Installation procedure

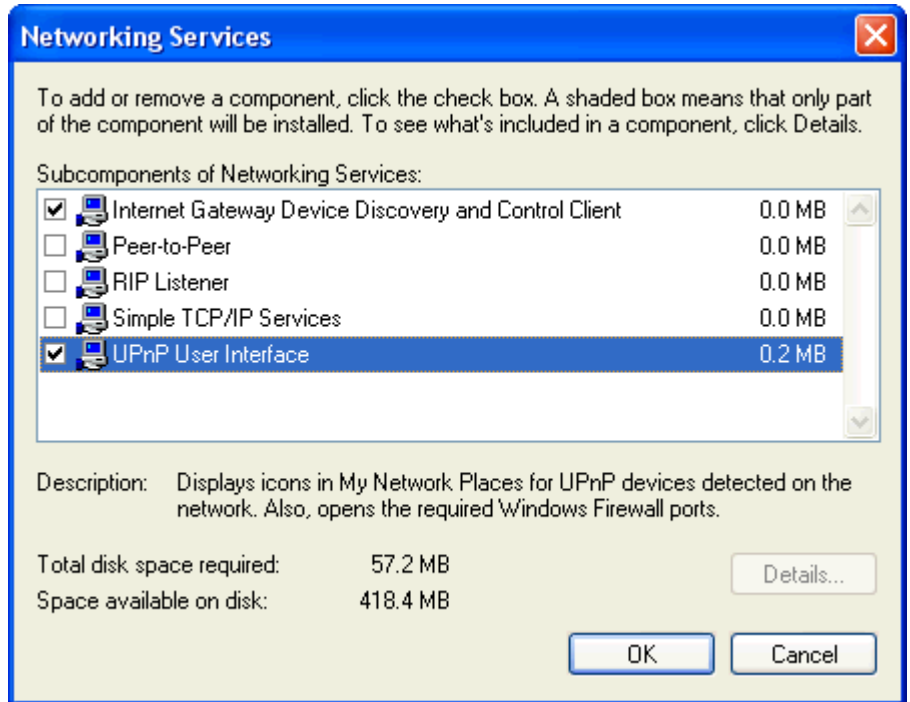
To install the Control point software on Windows XP, follow the steps below:

1. In the Control Panel, select "Add/Remove Programs".
2. In the "Add or Remove Programs" dialog box, click the "Add / Remove Windows Components" button.
3. In the "Windows Component Wizard" dialog box, scroll down the list to display the "Networking Services" entry. Highlight (select) the entry, and click on the "Details" button.

4. The "Networking Services" window is displayed.

The subcomponents shown in the Networking Services window will be different depending on if you are using Windows XP, Windows XP (SP1), or Windows XP (SP2).

If you are using Windows XP SP2, the Networking Services window will display the following list of sub-components:



5. Select the following entries from the "Networking Services" window and then click "OK":

If you are using **Windows XP**, select:

- "Universal Plug and Play".

If you are using **Windows XP SP1**, select:

- "Internet Gateway Device discovery and Control Client".
- "Universal Plug and Play".

If you are using **Windows XP SP2**, select:

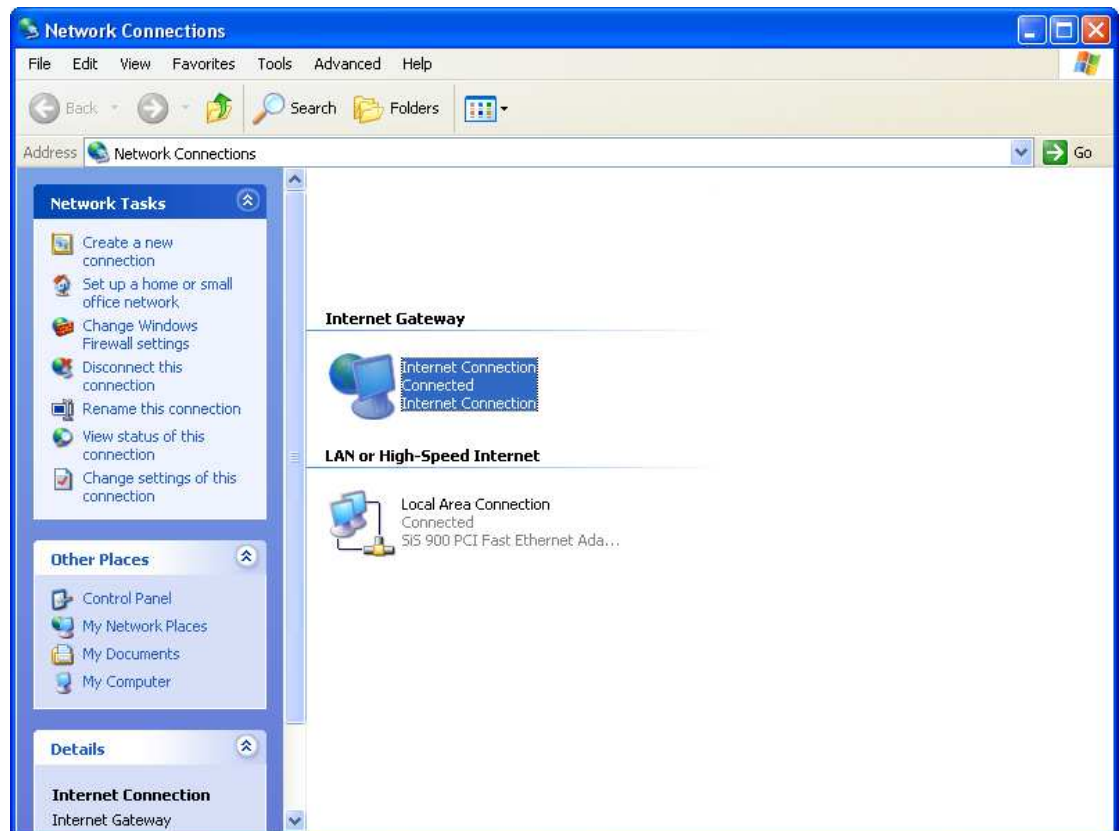
- "Internet Gateway Device discovery and Control Client".
- "UPnP User Interface".

6. Reboot your system.

Once you have installed the UPnP software and you have rebooted (and your network includes the IGD system), you should be able to see the IGD controlled device on your network.



For example, from the Network Connections window you should see the Internet Gateway Device:



# D Troubleshooting

This appendix suggests solutions for problems you may encounter in installing or using the Wireless Gateway, and provides instructions for using several IP utilities to diagnose problems.

Contact Customer Support if these suggestions do not resolve the problem.

## Troubleshooting Suggestions

Problem	Troubleshooting Suggestion
<b>LEDs</b>	
<i>Power LED does not illuminate after product is turned on.</i>	Verify that you are using the power cable provided with the device and that it is securely connected to the Wireless Gateway and a wall socket/power strip.
<i>LINK LAN LED does not illuminate after Ethernet cable is attached.</i>	Verify that the Ethernet cable is securely connected to your LAN hub or PC and to the Wireless Gateway. Make sure the PC and/or hub is turned on. Verify that your cable is sufficient for your network requirements. A 100 Mbit/sec network (10BaseTx) should use cables labeled CAT 5. A 10Mbit/sec network may tolerate lower quality cables.
<b>Internet Access</b>	
My PC cannot access the Internet	Use the ping utility (discussed in the following section) to check whether your PC can communicate with the device's LAN IP address (by default 192.168.200.254). If it cannot, check the Ethernet cabling. If you statically assigned a private IP address to the computer, (not a registered public address), verify the following: <ul style="list-style-type: none"><li>• Check that the gateway IP address on the computer is your public IP address (see Current Status for instructions on viewing the IP information.) If it is not, correct the address or configure the PC to receive IP information automatically.</li><li>• Verify with your ISP that the DNS server specified for the PC is valid. Correct the address or configure the PC to receive this information automatically.</li></ul>
<i>My LAN PCs cannot display web pages on the Internet.</i>	Verify that the DNS server IP address specified on the PCs is correct for your ISP, as discussed in the item above. If you specified that the DNS server be assigned dynamically from a server, then verify with your ISP that the address configured on the Wireless Gateway is correct, then You can use the ping utility, to test connectivity with your ISP's DNS server.
<b>Web pages</b>	

Problem	Troubleshooting Suggestion
<i>I forgot/lost my user ID or password.</i>	If you have not changed the password from the default, try using "admin" the user ID and "administrator" as password. Otherwise, you can reset the device to the default configuration by pressing the Reset Default button on the Rare panel of the device (see <i>Rare Panel</i> ). Then, type the default User ID and password shown above. <b>WARNING:</b> Resetting the device removes any custom settings and returns all settings to their default values.
<i>I cannot access the web pages from my browser.</i>	Use the ping utility, discussed in the following section, to check whether your PC can communicate with the device's LAN IP address (by default 192.168.200.254). If it cannot, check the Ethernet cabling. Verify that you are using Internet Explorer or Netscape Navigator v4.0 or later. Verify that the PC's IP address is defined as being on the same subnet as the IP address assigned to the LAN port on the Wireless Gateway.
<i>My changes to the web pages are not being retained.</i>	Be sure to use the <i>Confirm Changes/Apply</i> function after any changes.

## Diagnosing Problem using IP Utilities

### ping

*Ping* is a command you can use to check whether your PC can recognize other computers on your network and the Internet. A ping command sends a message to the computer you specify. If the computer receives the message, it sends messages in reply. To use it, you must know the IP address of the computer with which you are trying to communicate.

On Windows-based computers, you can execute a ping command from the Start menu. Click the *Start* button, and then click *Run*. In the *Open* text box, type a statement such as the following:

### ping 192.168.200.254

Click *OK*. You can substitute any private IP address on your LAN or a public IP address for an Internet site, if known.

If the target computer receives the message, a *Command Prompt* window is displayed:

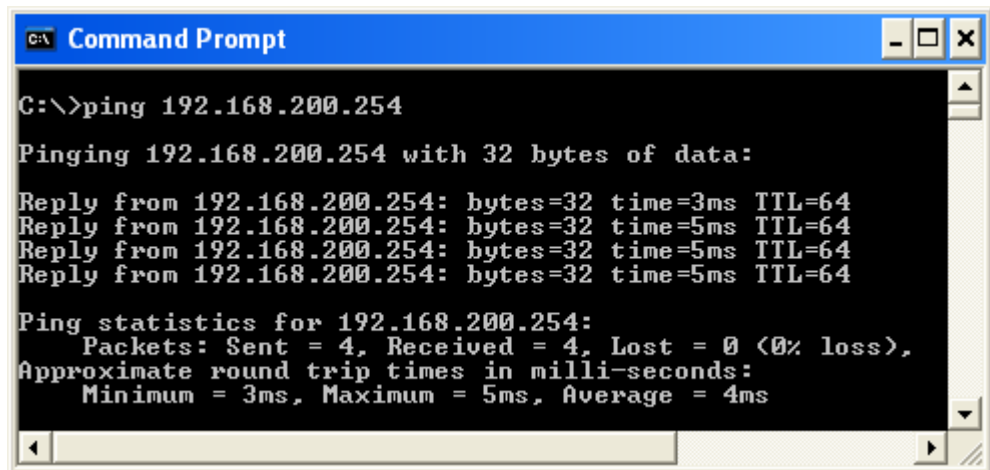


Figure 8: Using the ping Utility

If the target computer cannot be located, you will receive the message *Request timed out*.

Using the ping command, you can test whether the path to the Wireless Gateway is working (using the preconfigured default LAN IP address 192.168.200.254) or another address you assigned.

You can also test whether access to the Internet is working by typing an external address, such as that for *www.yahoo.com* (216.115.108.243). If you do not know the IP address of a particular Internet location, you can use the *nslookup* command, as explained in the following section.

From most other IP-enabled operating systems, you can execute the same command at a command prompt or through a system administration utility.

### nslookup

You can use the *nslookup* command to determine the IP address associated with an Internet site name. You specify the common name, and the *nslookup* command looks up the name

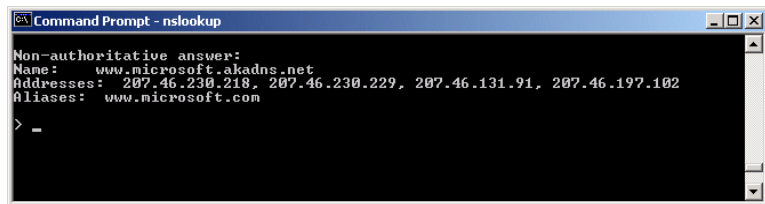
in on your DNS server (usually located with your ISP). If that name is not an entry in your ISP's DNS table, the request is then referred to another higher-level server, and so on, until the entry is found. The server then returns the associated IP address.

On Windows-based computers, you can execute the `nslookup` command from the *Start* menu. Click the *Start* button, and then click *Run*. In the *Open* text box, type the following:

### **Nslookup**

Click *OK*. A Command Prompt window displays with a bracket prompt (`>`). At the prompt, type the name of the Internet address that you are interested in, such as `www.microsoft.com`.

The window will display the associate IP address, if known, as shown below:



*Figure 9: Using the nslookup Utility*

There may be several addresses associated with an Internet name. This is common for web sites that receive heavy traffic; they use multiple, redundant servers to carry the same information.

To exit from the `nslookup` utility, type **exit** and press **[Enter]** at the command prompt.

# E

## Glossary

<b>10BASE-T</b>	A designation for the type of wiring used by Ethernet networks with a data rate of 10 Mbps. Also known as Category 3 (CAT 3) wiring. See <i>data rate</i> , <i>Ethernet</i> .
<b>100BASE-T</b>	A designation for the type of wiring used by Ethernet networks with a data rate of 100 Mbps. Also known as Category 5 (CAT 5) wiring. See <i>data rate</i> , <i>Ethernet</i> .
<b>ADSL</b>	<p>Asymmetric Digital Subscriber Line</p> <p>The most commonly deployed "flavor" of DSL for home users is asymmetrical DSL. The term asymmetrical refers to its unequal data rates for downloading and uploading (the download rate is higher than the upload rate). The asymmetrical rates benefit home users because they typically download much more data from the Internet than they upload.</p>
<b>analog</b>	An analog signal is a signal that has had its frequency modified in some way, such as by amplifying its strength or varying its frequency, in order to add information to the signal. The voice component in DSL is an analog signal. See <i>digital</i> .
<b>ATM</b>	<p>Asynchronous Transfer Mode</p> <p>A standard for high-speed transmission of data, text, voice, and video, widely used within the Internet. ATM data rates range from 45 Mbps to 2.5 Gbps. See <i>data rate</i>.</p>
<b>authenticate</b>	To verify a user's identity, such as by prompting for a password.
<b>binary</b>	The "base two" system of numbers, that uses only two digits, 0 and 1, to represent all numbers. In binary, the number 1 is written as 1, 2 as 10, 3 as 11, 4 as 100, etc. Although expressed as decimal numbers for convenience, IP addresses in actual use are binary numbers; e.g., the IP address 209.191.4.240 is 11010001.10111111.00000100.11110000 in binary. See <i>bit</i> , <i>IP address</i> , <i>network mask</i> .
<b>bit</b>	Short for "binary digit," a bit is a number that can have two values, 0 or 1. See <i>binary</i> .
<b>bps</b>	bits per second
<b>bridging</b>	Passing data from your network to your ISP and vice versa using the hardware addresses of the devices at each location. Bridging contrasts with routing, which can add more intelligence to data transfers by using network addresses instead. The Wireless Gateway can perform both routing and bridging. Typically, when both functions are enabled, the device routes IP data and bridges all other types of data. See <i>routing</i> .
<b>broadband</b>	A telecommunications technology that can send different types of data over the same medium. DSL is a broadband technology.
<b>broadcast</b>	To send data to all computers on a network.

<b>DHCP</b>	Dynamic Host Configuration Protocol DHCP automates address assignment and management. When a computer connects to the LAN, DHCP assigns it an IP address from a shared pool of IP addresses; after a specified time limit, DHCP returns the address to the pool.
<b>DHCP relay</b>	Dynamic Host Configuration Protocol relay A DHCP relay is a computer that forwards DHCP data between computers that request IP addresses and the DHCP server that assigns the addresses. Each of the Wireless Gateway's interfaces can be configured as a DHCP relay. See <i>DHCP</i> .
<b>DHCP server</b>	Dynamic Host Configuration Protocol server A DHCP server is a computer that is responsible for assigning IP addresses to the computers on a LAN. See <i>DHCP</i> .
<b>digital</b>	Of data, having a form based on discrete values expressed as binary numbers (0's and 1's). The data component in DSL is a digital signal. See <i>analog</i> .
<b>DNS</b>	Domain Name System The DNS maps domain names into IP addresses. DNS information is distributed hierarchically throughout the Internet among computers called DNS servers. For example, <i>www.yahoo.com</i> is the domain name associated with IP address 216.115.108.243. When you start to access a web site, a DNS server looks up the requested domain name to find its corresponding IP address. If the DNS server cannot find the IP address, it communicates with higher-level DNS servers to determine the IP address. See <i>domain name</i> .
<b>domain name</b>	A domain name is a user-friendly name used in place of its associated IP address. Domain names must be unique; their assignment is controlled by the Internet Corporation for Assigned Names and Numbers (ICANN). Domain names are a key element of URLs, which identify a specific file at a web site. See <i>DNS</i> .
<b>download</b>	To transfer data in the downstream direction, i.e., from the Internet to the user.
<b>DSL</b>	Digital Subscriber Line A technology that allows both digital data and analog voice signals to travel over existing copper telephone lines.
<b>encryption keys</b>	See <i>network keys</i>
<b>Ethernet</b>	The most commonly installed computer network technology, usually using twisted pair wiring. Ethernet data rates are 10 Mbps and 100 Mbps. See also <i>10BASE-T</i> , <i>100BASE-T</i> , <i>twisted pair</i> .
<b>FTP</b>	File Transfer Protocol A program used to transfer files between computers connected to the Internet. Common uses include uploading new or updated files to a web server, and downloading files from a web server.
<b>Gbps</b>	Abbreviation of Gigabits per second, or one billion bits per second. Internet data rates are often expressed in Gbps.
<b>host</b>	A device (usually a computer) connected to a network.

<b>HTTP</b>	<p>Hyper-Text Transfer Protocol</p> <p>HTTP is the main protocol used to transfer data from web sites so that it can be displayed by web browsers. See <i>web browser</i>, <i>web site</i>.</p>
<b>Hub</b>	<p>A hub is a place of convergence where data arrives from one or more directions and is forwarded out in one or more directions. It connects an Ethernet bridge/router to a group of PCs on a LAN and allows communication to pass between the networked devices.</p>
<b>ICMP</b>	<p>Internet Control Message Protocol</p> <p>An Internet protocol used to report errors and other network-related information. The ping command makes use of ICMP.</p>
<b>IEEE</b>	<p>The Institute of Electrical and Electronics Engineers is a technical professional society that fosters the development of standards that often become national and international standards.</p>
<b>Internet</b>	<p>The global collection of interconnected networks used for both private and business communications.</p>
<b>intranet</b>	<p>A private, company-internal network that looks like part of the Internet (users access information using web browsers), but is accessible only by employees.</p>
<b>IP</b>	<p>See <i>TCP/IP</i>.</p>
<b>IP address</b>	<p>Internet Protocol address</p> <p>The address of a host (computer) on the Internet, consisting of four numbers, each from 0 to 255, separated by periods, e.g., 209.191.4.240. An IP address consists of a <i>network ID</i> that identifies the particular network the host belongs to, and a <i>host ID</i> uniquely identifying the host itself on that network. A network mask is used to define the network ID and the host ID. Because IP addresses are difficult to remember, they usually have an associated domain name that can be specified instead. See <i>domain name</i>, <i>network mask</i>.</p>
<b>ISP</b>	<p>Internet Service Provider</p> <p>A company that provides Internet access to its customers, usually for a fee.</p>
<b>LAN</b>	<p>Local Area Network</p> <p>A network limited to a small geographic area, such as a home or small office.</p>
<b>LED</b>	<p>Light Emitting Diode</p> <p>An electronic light-emitting device. The indicator lights on the front of the Wireless Gateway are LEDs.</p>
<b>MAC address</b>	<p>Media Access Control address</p> <p>The permanent hardware address of a device, assigned by its manufacturer. MAC addresses are expressed as six pairs of hex characters, with each pair separated by colons. For example; <i>NN:NN:NN:NN:NN:NN</i>.</p>
<b>mask</b>	<p>See <i>network mask</i>.</p>
<b>Mbps</b>	<p>Abbreviation for Megabits per second, or one million bits per second. Network data rates are often expressed in Mbps.</p>
<b>NAT</b>	<p>Network Address Translation</p> <p>A service performed by many routers that translates your network's publicly known IP address into a <i>private</i> IP address for each computer on your LAN. Only your router and your</p>



	LAN know these addresses; the outside world sees only the public IP address when talking to a computer on your LAN.
<b>network</b>	A group of computers that are connected together, allowing them to communicate with each other and share resources, such as software, files, etc. A network can be small, such as a <i>LAN</i> , or very large, such as the <i>Internet</i> .
<b>network mask</b>	A network mask is a sequence of bits applied to an IP address to select the network ID while ignoring the host ID. Bits set to 1 mean "select this bit" while bits set to 0 mean "ignore this bit." For example, if the network mask 255.255.255.0 is applied to the IP address 100.10.50.1, the network ID is 100.10.50, and the host ID is 1. See <i>binary</i> , <i>IP address</i> , <i>subnet</i> .
<b>NIC</b>	Network Interface Card An adapter card that plugs into your computer and provides the physical interface to your network cabling. For Ethernet NICs this is typically an RJ-45 connector. See <i>Ethernet</i> , <i>RJ-45</i> .
<b>packet</b>	Data transmitted on a network consists of units called packets. Each packet contains a payload (the data), plus overhead information such as where it came from (source address) and where it should go (destination address).
<b>ping</b>	Packet Internet (or Inter-Network) Groper A program used to verify whether the host associated with an IP address is online. It can also be used to reveal the IP address for a given domain name.
<b>port</b>	A physical access point to a device such as a computer or router, through which data flows into and out of the device.
<b>PPP</b>	Point-to-Point Protocol A protocol for serial data transmission that is used to carry IP (and other protocol) data between your ISP and your computer. The WAN interface on the Wireless Gateway uses two forms of PPP called PPPoA and PPPoE. See <i>PPPoA</i> , <i>PPPoE</i> .
<b>PPPoA</b>	Point-to-Point Protocol over ATM One of the two types of PPP interfaces you can define for a Virtual Circuit (VC), the other type being PPPoE. You can define only one PPPoA interface per VC.
<b>PPPoE</b>	Point-to-Point Protocol over Ethernet One of the two types of PPP interfaces you can define for a Virtual Circuit (VC), the other type being PPPoA. You can define one or more PPPoE interfaces per VC.
<b>protocol</b>	A set of rules governing the transmission of data. In order for a data transmission to work, both ends of the connection have to follow the rules of the protocol.
<b>remote</b>	In a physically separate location. For example, an employee away on travel who logs in to the company's intranet is a remote user.
<b>RIP</b>	Routing Information Protocol The original TCP/IP routing protocol. There are two versions of RIP: version I and version II.
<b>RJ-11</b>	Registered Jack Standard-11 The standard plug used to connect telephones, fax

	machines, modems, etc. to a telephone port. It is a 6-pin connector usually containing four wires.
<b>RJ-45</b>	Registered Jack Standard-45 The 8-pin plug used in transmitting data over phone lines. Ethernet cabling usually uses this type of connector.
<b>routing</b>	Forwarding data between your network and the Internet on the most efficient route, based on the data's destination IP address and current network conditions. A device that performs routing is called a router.
<b>SDNS</b>	Secondary Domain Name System (server) A DNS server that can be used if the primary DSN server is not available. See <i>DNS</i> .
<b>subnet</b>	A subnet is a portion of a network. The subnet is distinguished from the larger network by a <i>subnet mask</i> that selects some of the computers of the network and excludes all others. The subnet's computers remain physically connected to the rest of the parent network, but they are treated as though they were on a separate network. See <i>network mask</i> .
<b>subnet mask</b>	A mask that defines a subnet. See <i>network mask</i> .
<b>TCP</b>	See <i>TCP/IP</i> .
<b>TCP/IP</b>	Transmission Control Protocol/Internet Protocol The basic protocols used on the Internet. TCP is responsible for dividing data up into packets for delivery and reassembling them at the destination, while IP is responsible for delivering the packets from source to destination. When TCP and IP are bundled with higher-level applications such as HTTP, FTP, Telnet, etc., TCP/IP refers to this whole suite of protocols.
<b>Telnet</b>	An interactive, character-based program used to access a remote computer. While HTTP (the web protocol) and FTP only allow you to download files from a remote computer, Telnet allows you to log into and use a computer from a remote location.
<b>TFTP</b>	Trivial File Transfer Protocol A protocol for file transfers, TFTP is easier to use than File Transfer Protocol (FTP) but not as capable or secure.
<b>TKIP</b>	Temporal Key Integrity Protocol (TKIP) provides WPA with a data encryption function. It ensures that a unique master key is generated for each packet, supports message integrity and sequencing rules and supports re-keying mechanisms.
<b>triggers</b>	Triggers are used to deal with application protocols that create separate sessions. Some applications, such as NetMeeting, open secondary connections during normal operations, for example, a connection to a server is established using one port, but data transfers are performed on a separate connection. A trigger tells the device to expect these secondary sessions and how to handle them.  Once you set a trigger, the embedded IP address of each incoming packet is replaced by the correct host address so that NAT can translate packets to the correct destination. You can specify whether you want to carry out address replacement, and if so, whether to replace addresses on TCP packets only, UDP packets only, or both.

<b>twisted pair</b>	The ordinary copper telephone wiring used by telephone companies. It contains one or more wire pairs twisted together to reduce inductance and noise. Each telephone line uses one pair. In homes, it is most often installed with two pairs. For Ethernet LANs, a higher grade called Category 3 (CAT 3) is used for 10BASE-T networks, and an even higher grade called Category 5 (CAT 5) is used for 100BASE-T networks. See <i>10BASE-T</i> , <i>100BASE-T</i> , <i>Ethernet</i> .
<b>unnumbered interfaces</b>	<p>An unnumbered interface is an IP interface that does not have a local subnet associated with it. Instead, it uses a <i>router-id</i> that serves as the source and destination address of packets sent to and from the router. Unlike the IP address of a normal interface, the router-id of an unnumbered interface is allowed to be the same as the IP address of another interface. For example, the WAN unnumbered interface of your device uses the same IP address of the LAN interface (192.168.200.254).</p> <p>The unnumbered interface is temporary – PPP or DHCP will assign a 'real' IP address automatically.</p>
<b>upstream</b>	The direction of data transmission from the user to the Internet.
<b>VC</b>	Virtual Circuit A connection from your DSL router to your ISP.
<b>VCI</b>	Virtual Circuit Identifier Together with the Virtual Path Identifier (VPI), the VCI uniquely identifies a VC. Your ISP will tell you the VCI for each VC they provide. See <i>VC</i> .
<b>VPI</b>	Virtual Path Identifier Together with the Virtual Circuit Identifier (VCI), the VPI uniquely identifies a VC. Your ISP will tell you the VPI for each VC they provide. See <i>VC</i> .
<b>WAN</b>	Wide Area Network Any network spread over a large geographical area, such as a country or continent. With respect to the Wireless Gateway, WAN refers to the Internet.
<b>Web browser</b>	A software program that uses Hyper-Text Transfer Protocol (HTTP) to download information from (and upload to) web sites, and displays the information, which may consist of text, graphic images, audio, or video, to the user. Web browsers use Hyper-Text Transfer Protocol (HTTP). Popular web browsers include Netscape Navigator and Microsoft Internet Explorer. See <i>HTTP</i> , <i>web site</i> , <i>WWW</i> .
<b>Web page</b>	A web site file typically containing text, graphics and hyperlinks (cross-references) to the other pages on that web site, as well as to pages on other web sites. When a user accesses a web site, the first page that is displayed is called the <i>home page</i> . See <i>hyperlink</i> , <i>web site</i> .
<b>Web site</b>	A computer on the Internet that distributes information to (and gets information from) remote users through web browsers. A web site typically consists of web pages that contain text, graphics, and hyperlinks. See <i>hyperlink</i> , <i>web page</i> .

**WWW**

World Wide Web

Also called *(the) Web*. Collective term for all web sites anywhere in the world that can be accessed via the Internet.