

LevelOne

WBR-3408 User Manual



11g Wireless Broadband Router (Roteador banda-larga sem fio- Wireless G)

Ver. 3.000

Safety

FCC WARNING

This equipment may generate or use radio frequency energy. Changes or modifications to this equipment may cause harmful interference unless the modifications are expressly approved in the instruction manual. The user could lose the authority to operate this equipment if an unauthorized change or modification is made.

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

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

CE Declaration of conformity

This equipment complies with the requirements relating to electromagnetic compatibility, EN 55022 class B for ITE, the essential protection requirement of Council Directive 89/336/EEC on the approximation of the laws of the Member States relating to electromagnetic compatibility.

CE Marking Warning

Hereby, Digital Data Communications, declares that this (Model-no. WBR-3408) is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.

The CE-Declaration of Conformity can be downloaded at:

<http://www.levelone.eu/support.php>



General Public License

This product incorporates open source code into the software and therefore falls under the guidelines governed by the General Public License (GPL) agreement.

Adhering to the GPL requirements, the open source code and open source license for the source code are available for free download at <http://global.level1.com>.

If you would like a copy of the GPL or other open source code in this software on a physical CD medium, LevelOne (Digital Data Communications) offers to mail this CD to you upon request, for a price of US\$9.99 plus the cost of shipping.

Table of Contents

CHAPTER 1 INTRODUCTION.....	6
Wireless Router Features.....	6
Package Contents	10
Physical Details.....	11
CHAPTER 2 INSTALLATION.....	13
Requirements	13
Procedure	13
CHAPTER 3 SETUP.....	15
Overview	15
Configuration Program.....	17
Setup Wizard	18
Home Screen	20
LAN Screen	21
Mode Screen.....	23
Wireless - Options Screen.....	24
Wireless - Schedule.....	26
Wireless - MAC Filter	27
Wireless - MAC Filter - Trusted Wireless Stations	28
Wireless - WiFi Protected Setup (WPS)	30
Wireless - Wireless Distribution System (WDS)	32
Wireless Security	34
Password Screen.....	39
CHAPTER 4 PC CONFIGURATION.....	40
Overview	40
Windows Clients	40
Macintosh Clients	51
Linux Clients.....	52
Other Unix Systems	52
Wireless Station Configuration	53
Wireless Configuration on Windows XP	53
CHAPTER 5 OPERATION AND STATUS	63
Operation - Router Mode	63
Status Screen.....	63
Connection Status - PPPoE.....	66
Connection Status - PPTP.....	67
Connection Status - L2TP	68
Connection Details - Dynamic IP Address.....	69
Connection Details - Fixed IP Address	70
CHAPTER 6 ADVANCED FEATURES.....	71
Overview	71
Internet.....	71
Dynamic DNS (Domain Name Server).....	74
Options	76
Schedule.....	77
Port Trigger	79
Single Port Forwarding.....	81
Port Range Forwarding	83
QoS.....	84
CHAPTER 7 ADVANCED ADMINISTRATION.....	86
Overview	86

PC Database.....	87
Config File.....	90
Logs.....	91
E-Mail.....	93
Diagnostics	95
Remote Administration.....	96
Routing	98
Upgrade Firmware	102
CHAPTER 8 ACCESS POINT MODE.....	103
Overview	103
Management Connections.....	103
Mode Screen.....	104
Operation	104
APPENDIX A TROUBLESHOOTING	105
Overview	105
General Problems	105
Internet Access.....	105
Wireless Access	106
APPENDIX B ABOUT WIRELESS LANS	108
Modes	108
BSS/ESS.....	108
Channels.....	109
WEP.....	109
WPA-PSK	109
WPA2-PSK	110
WPA-802.1x	110
Wireless LAN Configuration.....	111
APPENDIX C SPECIFICATIONS.....	112
Multi-Function Wireless Router	112
Wireless Interface	112

Chapter 1

Introduction

1

This Chapter provides an overview of the Wireless Router's features and capabilities.

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

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



Installation

Wireless Router Features

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

Internet Access Features

- **Shared Internet Access.** All users on the LAN or WLAN can access the Internet through the Wireless Router, using only a single external IP Address. The local (invalid) IP Addresses are hidden from external sources. This process is called NAT (Network Address Translation).
- **DSL & Cable Modem Support.** The Wireless Router has a 10/100BaseT Ethernet port for connecting a DSL or Cable Modem. All popular DSL and Cable Modems are supported.
- **PPPoE, PPTP and L2TP Support.** The Internet (WAN port) connection supports PPPoE (PPP over Ethernet), PPTP (Peer-to-Peer Tunneling Protocol) and L2TP, as well as "Direct Connection" type services.
- **Fixed or Dynamic IP Address.** On the Internet (WAN port) connection, the Wireless Router supports both Dynamic IP Address (IP Address is allocated on connection) and Fixed IP Address.

Advanced Internet Functions

- **Application Level Gateways (ALGs).** Applications which use non-standard connections or port numbers are normally blocked by the Firewall. The ability to define and allow such applications is provided, to enable such applications to be used normally.
- **Port Triggering.** This feature, also called Special Applications, allows you to use Internet applications which normally do not function when used behind a firewall.
- **Port Forwarding.** This feature allows Internet users to access Internet servers on your LAN. The required setup is quick and easy.
- **Virtual Servers.** This feature allows Internet users to access Internet servers on your LAN. The required setup is quick and easy.
- **Dynamic DNS Support.** DDNS, when used with the Virtual Servers feature, allows users to connect to Servers on your LAN using a Domain Name, even if you have a dynamic IP address which changes every time you connect.
- **URL Filter.** Use the URL Filter to block access to undesirable Web sites by LAN users.
- **Access Control.** Using the Access Control feature, you can assign LAN users to different groups, and determine which Internet services are available to each group.
- **Scheduling.** Both the URL Filter and Firewall rules can be scheduled to operate only at certain times. This provides great flexibility in controlling Internet-bound traffic.
- **Logs.** Define what data is recorded in the Logs, and optionally send log data to a Syslog Server. Log data can also be E-mailed to you.
- **QoS Support** Quality of Service can be used to handle packets so that more important connections receive priority over less important one.

Wireless Features

- **Standards Compliant.** The Wireless Router complies with the IEEE802.11g (DSSS) specifications for Wireless LANs.
- **Multi SSIDs Support.** This feature can let you have 2 SSIDs on one AP, which provides more easy way for Guest access and also secure your resource at the same time.
- **WEP support.** Support for WEP (Wired Equivalent Privacy) is included. Key sizes of 64 Bit and 128 Bit are supported. WEP encrypts any data before transmission, providing protection against snoopers.
- **WPA-PSK support.** Like WEP, WPA-PSK encrypts any data before transmission, providing protection against snoopers. The WPA-PSK is a later standard than WEP, and provides both easier configuration and greater security than WEP.
- **WPA2-PSK support.** Support for WPA2 is also included. WPA2 uses the extremely secure AES encryption method.
- **802.1x Support.** Support for 802.1x mode is included, providing for the industrial-strength wireless security of 802.1x authentication and authorization.
- **Wireless MAC Access Control.** The Wireless Access Control feature can check the MAC address (hardware address) of Wireless stations to ensure that only trusted Wireless Stations can access your LAN.

- **Simple Configuration.** If the default settings are unsuitable, they can be changed quickly and easily.
- **WPS Support.** WPS (Wi-Fi Protected Setup) can simplify the process of connecting any device to the wireless network by using the push button configuration (PBC) on the Wireless Access Point, or entering a PIN code if there's no button.
- **WDS Support.** Support for WDS (Wireless Distribution System) allows the Wireless Access Point to act as a Wireless Bridge. Both Point-to-Point and Multi-Point Bridge modes are supported.

LAN Features

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

Configuration & Management

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

Security Features

- **Password - protected Configuration.** Password protection is provided to prevent unauthorized users from modifying the configuration data and settings.
- **Wireless LAN Security.** WPA-PSK, WEP and Wireless access control by MAC address are all supported. The MAC-level access control feature can be used to prevent unknown wireless stations from accessing your LAN.
- **NAT Protection.** An intrinsic side effect of NAT (Network Address Translation) technology is that by allowing all LAN users to share a single IP address, the location and even the existence of each PC is hidden. From the external viewpoint, there is no network, only a single device - the Wireless Router.
- **Firewall.** All incoming data packets are monitored and all incoming server requests are filtered, thus protecting your network from malicious attacks from external sources.
- **Protection against DoS attacks.** DoS (Denial of Service) attacks can flood your Internet connection with invalid packets and connection requests, using so much bandwidth and so many resources that Internet access becomes unavailable. The Wireless Router incorporates protection against DoS attacks.

Package Contents

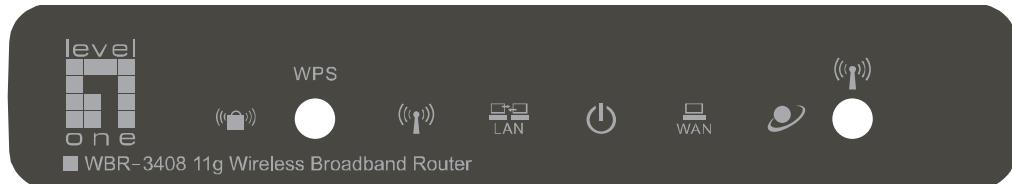
The following items should be included. If any of these items are damaged or missing, please contact your dealer immediately.

- WBR-3408 11g Wireless Broadband Router
- 1 Cat-5 Ethernet (LAN) cable
- Power Adapter
- Quick Installation Guide
- CD-ROM containing the on-line manual.

Physical Details

Front Panel

EN



PT



Front Panel

WPS Button	Push the WPS button on the WBR-3408, and also on your other wireless device to perform WPS syncing to create a secured wireless connection automatically.
Wireless Security	() On - Wireless security is On. Off - Wireless security is Off. Flashing (Blue) - When WPS sync in progress.
Wireless	() On - Wireless Devices or Computers are connected to the WBR-3408. Off - No Wireless connections currently exist.
LAN	() On - Wired Devices or Computers are connected to the WBR-3408. Off - No active wired connections on the LAN port(s).
Power	() On - Router is ON and ready. Flashing (Blue) - Router is booting up Off - Router is OFF
WAN	() On - Connection to the ADSL/Broadband Modem attached to the WAN (Internet) port is established. Off - No connection to the ADSL/Broadband Modem. Flashing (Amber) – Router is attempting to connect to the Internet.
Internet	() On - Internet connection is available. Off - No Internet connection available.

Wireless On / Off Button Push button for 3 seconds to Enable or Disable the wireless signal.

Reboot or Reset **Reboot** - Press *WPS and Wireless On/Off buttons* together for 5 seconds. The router will restart and boot again.

Reset – Press *WPS and Wireless On/Off buttons* together for 10 seconds.

All settings will be CLEARED and restored to factory defaults.

Rear Panel



Rear Panel

Power port Connect the supplied power adapter here.

WAN port (10/100BaseT) Connect the DSL or Cable Modem here. If your modem came with a cable, use the supplied cable. Otherwise, use a standard LAN cable.

10/100BaseT LAN connections Use standard LAN cables (RJ45 connectors) to connect your PCs to these ports.

Chapter 2

Installation

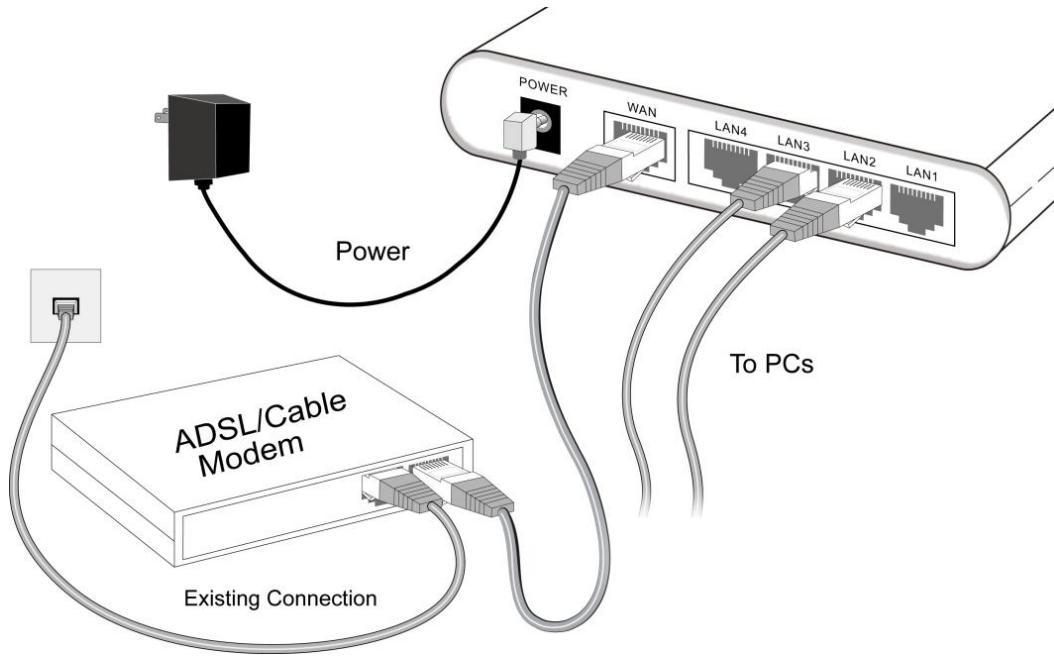
2

This Chapter covers the physical installation of the Wireless Router.

Requirements

- Network cables. Use standard 10/100BaseT network (UTP) cables with RJ45 connectors.
- TCP/IP protocol must be installed on all PCs.
- For Internet Access, an Internet Access account with an ISP, and a DSL connection.
- To use the Wireless Access Point, all Wireless devices must be compliant with the IEEE 802.11g or IEEE 802.11b specifications.

Procedure



1. Choose an Installation Site

Select a suitable place on the network to install the Wireless Router.



For best Wireless reception and performance, the Wireless Router should be positioned in a central location with minimum obstructions between the Wireless Router and the PCs.

Also, if using multiple Access Points, adjacent Access Points should use different Channels.

2. Connect LAN Cables

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

3. Connect ADSL Cable

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

4. Power Up

Connect the supplied power adapter to the Wireless Router. Use only the power adapter provided. Using a different one may cause hardware damage.

5. Check the LEDs

- The *Power* LED should be ON.
- The *LAN* LED should be ON (provided the PC is also ON.)
- The *Wireless* LED should be ON if Wireless PC is connected.
- The *WAN* LED should be ON an ADSL or Cable modem is connected.
- The *Internet* LED may be OFF. If Internet connection is working, it will be ON.

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

Chapter 3

Setup

3

This Chapter provides Setup details of the Wireless Router.

Overview

This chapter describes the setup procedure for:

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

PCs on your local LAN may also require configuration. For details, see *Chapter 4 - PC Configuration*.

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

To Do this:	Refer to:
Configure PCs on your LAN.	Chapter 4: PC Configuration
Check Wireless Router operation and Status.	Chapter 5: Operation and Status
Use any of the following Advanced features: <ul style="list-style-type: none">• Internet (DMZ, URL Filter)• Access Control• Dynamic DNS• Options• Schedule• Port Trigger• Single Port Forwarding• Port Range Forwarding• QoS	Chapter 6: Advanced Features

<p>Use any of the following Administration Configuration settings or features:</p> <ul style="list-style-type: none">• PC Database• Config File• Logs• E-Mail• Diagnostics• Remote Administration• Routing• Upgrade Firmware	<p>Chapter 7: Advanced Administration</p>
---	---

Configuration Program

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

- Internet Explorer 6 and above is recommended.

Preparation

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

- Your PC can establish a physical connection to the Wireless Router. The PC and the Wireless Router must be directly connected (using the LAN ports on the Wireless Router) or on the same LAN segment.
- The Wireless Router must be installed and powered ON.
- If the Wireless Router's default IP Address (192.168.0.1) is already used by another device, the other device must be turned OFF until the Wireless Router is allocated a new IP Address during configuration.

Using your Web Browser

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

1. After installing the Wireless Router in your LAN, start your PC. If your PC is already running, restart it.
2. Start your WEB browser.
3. In the *Address* box, enter "HTTP://" and the IP Address of the Wireless Router, as in this example, which uses the Wireless Router's default IP Address:
http://192.168.0.1
4. When prompted for the User name and Password, enter values as follows:
 - User name **admin**
 - Password **password**

If you can't connect

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

- The Wireless Router is properly installed, LAN connection is OK, and it is powered ON. You can test the connection by using the "Ping" command:
 - Open the MS-DOS window or command prompt window.
 - Enter the command:
ping 192.168.0.1If no response is received, either the connection is not working, or your PC's IP address is not compatible with the Wireless Router's IP Address. (See next item.)
- If your PC is using a fixed IP Address, its IP Address must be within the range 192.168.0.2 to 192.168.0.254 to be compatible with the Wireless Router's default IP Address of 192.168.0.1. Also, the *Network Mask* must be set to 255.255.255.0. See *Chapter 4 - PC Configuration* for details on checking your PC's TCP/IP settings.
- Ensure that your PC and the Wireless Router are on the same network segment. (If you don't have a router, this must be the case.)
- Ensure you are using the wired LAN interface. The Wireless interface can only be used if its configuration matches your PC's wireless settings.

Setup Wizard

The first time you connect to the Wireless Router, the Setup Wizard will run automatically. (The Setup Wizard will also run if the Wireless Router's default settings are restored.)

1. Step through the Wizard until finished.
 - You need to know the type of Internet connection service used by your ISP. Check the data supplied by your ISP.
 - The common connection types are explained in the tables below.
2. On the final screen of the Wizard, run the test and check that an Internet connection can be established.
3. If the connection test fails:
 - Check your data, the Cable/DSL modem, and all connections.
 - Check that you have entered all data correctly.
 - If using a Cable modem, your ISP may have recorded the MAC (physical) address of your PC. Run the Wizard, and use the "Copy from PC" button to copy the MAC address from your PC to the Wireless Router.

Common Connection Types

DSL Modems

Type	Details	ISP Data required
Dynamic IP Address	Your IP Address is allocated automatically, when you connect to your ISP.	None.
Static (Fixed) IP Address	Your ISP allocates a permanent IP Address to you.	IP Address allocated to you.
PPPoE	You connect to the ISP only when required. The IP address is usually allocated automatically.	User name and password.
PPTP, L2TP	PPTP is mainly used in Europe. You connect to the ISP only when required. The IP address is usually allocated automatically, but may be Static (Fixed).	<ul style="list-style-type: none">• Server IP Address.• User name and password.• IP Address allocated to you, if Static (Fixed).

Home Screen

After finishing the Setup Wizard, you will see the *Home* screen. When you connect in future, you will see this screen when you connect. An example screen is shown below.



Home Screen

Main Menu

The main menu, on the left, contains links to the most-commonly used screen. To see the links to the other available screens, click "Advanced" or "Administration".

The main menu also contains two (2) buttons:

- **Log Out** - When finished, you should click this button to logout.
- **Restart** - Use this if you wish to restart the Wireless Router. Note that restarting the Router will break any existing connections to or through the Router.

Navigation & Data Input

- Use the menu bar on the left of the screen, and the "Back" button on your Browser, for navigation.
- Changing to another screen without clicking "Save" does NOT save any changes you may have made. You must "Save" before changing screens or your data will be ignored.



On each screen, clicking the "Help" button will display help for that screen.

LAN Screen

Use the *LAN* link on the main menu to reach the LAN screen. An example screen is shown below.

Configuration

LAN

TCP/IP

IP Address: 192.168.0.1

Subnet Mask: 255.255.255.0

DHCP Server

Start IP Address: 192.168.0.2

Finish IP Address: 192.168.0.50

Gateway IP Address:

DNS IP Address:

Lease Time: 3 Days

Save Cancel PC Database Help

LAN Screen

Data - LAN Screen

TCP/IP	
IP Address	IP address for the Wireless Router, as seen from the local LAN. Use the default value unless the address is already in use or your LAN is using a different IP address range. In the latter case, enter an unused IP Address from within the range used by your LAN.
Subnet Mask	The default value 255.255.255.0 is standard for small (class "C") networks. For other networks, use the Subnet Mask for the LAN segment to which the Wireless Router is attached (the same value as the PCs on that LAN segment).
DHCP Server	<ul style="list-style-type: none"> If Enabled, the Wireless Router will allocate IP Addresses to PCs (DHCP clients) on your LAN when they start up. The default (and recommended) value is Enabled. If you are already using a DHCP Server, this setting must be Disabled, and the existing DHCP server must be re-configured to treat the Wireless Router as the default Gateway. See the following section for further details. The Start IP Address, Finish IP Address and Lease Time fields set the values used by the DHCP server when allocating IP Addresses to DHCP clients. This range also determines the number of DHCP clients supported. <p>See the following section for further details on using DHCP.</p>

DHCP

What DHCP Does

A DHCP (Dynamic Host Configuration Protocol) **Server** allocates a valid IP address to a DHCP **Client** (PC or device) upon request.

- The client request is made when the client device starts up (boots).
- The DHCP Server provides the *Gateway* and *DNS* addresses to the client, as well as allocating an IP Address.
- The Wireless Router can act as a **DHCP server**.
- Windows 95/98/ME and other non-Server versions of Windows will act as a DHCP **client**. This is the default Windows setting for the TCP/IP network protocol. However, Windows uses the term *Obtain an IP Address automatically* instead of "DHCP Client".
- You must NOT have two (2) or more DHCP Servers on the same LAN segment. (If your LAN does not have other Routers, this means there must only be one (1) DHCP Server on your LAN.)

Using the Wireless Router's DHCP Server

This is the default setting. The DHCP Server settings are on the **LAN** screen. On this screen, you can:

- Enable or Disable the Wireless Router's *DHCP Server* function.
- Set the range of IP Addresses allocated to PCs by the DHCP Server function.



You can assign Fixed IP Addresses to some devices while using DHCP, provided that the Fixed IP Addresses are NOT within the range used by the DHCP Server.

Using another DHCP Server

You can only use one (1) DHCP Server per LAN segment. If you wish to use another DHCP Server, rather than the Wireless Router's, the following procedure is required.

- Disable the DHCP Server feature in the Wireless Router. This setting is on the LAN screen.
- Configure the DHCP Server to provide the Wireless Router's IP Address as the *Default Gateway*.

To Configure your PCs to use DHCP

This is the default setting for TCP/IP for all non-Server versions of Windows.

See *Chapter 4 - Client Configuration* for the procedure to check these settings.

Mode Screen

Use this screen to change the mode between Router mode and Access Point mode.

Mode Screen

Select the desired option, and click "Save".

Router	In this mode, this device can provide shared Internet Access to all your LAN users. Also, by default, it acts a DHCP Server, providing an IP address and related information to all Wireless and LAN users.
Access Point	The device links your Wireless Stations to your wired LAN. The Wireless stations and devices on the wired LAN are then on the same network, and can communicate with each other without regard for whether they are connected to the network via a Wireless or wired connection. You need to have a DHCP Server on your LAN to provide IP addresses to the Wireless clients using this Access Point.

Notes:

- Generally, you should NOT use access point mode. Only select this mode if you are sure this is what you want.
- After changing the mode, this device will restart, which will take a few seconds. The menu will also be changed, depending on the mode you are in.
- For details on using Access Point Mode, see Chapter 8.

Wireless - Options Screen

The Wireless Router's settings must match the other Wireless stations.

Note that the Wireless Router will automatically accept both 802.11b and 802.11g connections, and no configuration is required for this feature.

To change the Wireless Router's default settings for the Wireless Access Point feature, use the *Wireless - Options* link on the main menu to reach the **Wireless - Options** screen. An example screen is shown below.

The screenshot shows the 'Wireless - Options' configuration page. It includes fields for Region (set to South America), Multi SSID (SSID: Primary, SSID1: WBR-3408, Broadcast SSID checked, Isolation Within SSID unchecked), Security Setting (SSID1: Disabled, Configure SSID1 button), Options (802.11 Mode: 11b+g+n, Channel NO.: auto, Extension Channel: Down channel, Isolation Between SSID checked, WMM support checked), and Bandwidth (20MHZ + 40MHZ auto). At the bottom are Save, Cancel, and Help buttons.

Wireless - Options Screen

Data – Wireless - Options Screen

Region	
Region	Select the correct domain for your location. It is your responsibility to ensure: <ul style="list-style-type: none"> That the Wireless ADSL Router is only used in domains for which is licensed. That you select the correct domain, so that only the legal channels for that domain can be selected.
Multi SSID	
SSID	With Multiple SSIDs, you can have 2 SSIDs on one AP. For example, a Guest SSID without encryption for visitors to have Internet access only, and a Primary SSID with encryption for private use to secure your company resources. Select the desired SSID from the list to configure.

SSID 1/2	This is also called the "Network Name". <ul style="list-style-type: none"> • If using an ESS (Extended Service Set, with multiple access points) this ID is called an ESSID (Extended Service Set Identifier). • To communicate, all Wireless stations should use the same SSID/ESSID.
Broadcast SSID	If enabled, the Wireless ADSL Router will broadcast its SSID. This allows PCs and other wireless stations to detect this Access Point and use the correct SSID. If disabled, PC users will have to manually enter the SSID and other details of the wireless interface before they can connect to this Access Point.
Isolation within SSID	If Enabled, devices that have the same SSID will not be able to see each other.
Security Setting	The current Wireless security is displayed. The default value is Disabled.
Configure SSID 1/2 Button	Click this button to access the Wireless security sub-screen, and view or change the settings. See the following section for details.
Options	
802.11 Mode	Select the desired mode: <ul style="list-style-type: none"> • Off - Wireless is disabled. • B only - Only 802.11b connections are available. 802.11g Wireless Stations will only be able to use the Wireless Router if they are fully backward-compatible with the 802.11b standard. • G only - Only 802.11g Wireless stations can use the Wireless Router. • 11b/g - 802.11b and 802.11g Wireless stations can use the Wireless Broadband Router.
Channel NO.	Select the Channel you wish to use on your Wireless LAN. <ul style="list-style-type: none"> • If you experience interference (shown by lost connections and/or slow data transfers) you may need to experiment with different channels to see which is the best. • If using multiple Access Points, adjacent Access Points should use different Channels to reduce interference.
Isolation between SSID	If Enabled, devices that have the different SSIDs will not be able to communicate with each other.
WMM Support	Enable by default.
Bandwidth	Select the desired bandwidth from the list.

Wireless - Schedule

To conserve power usage, you can set the time when the wireless signal will be deactivated. For example at night when there is no one using the wireless network.

Wireless

▼ Wireless Schedule

Wireless Schedule:	Current Setting: Disabled	Enable/Disable
Set Schedule		
Save	Cancel	Help

▼ Wireless Schedule

Use 24 hour clock. On all day: 00:00 to 24:00
Off all day: All fields left 00

Day	On	Off
Monday	00 :00	24 :00
Tuesday	00 :00	24 :00
Wednesday	00 :00	24 :00
Thursday	00 :00	24 :00
Friday	00 :00	24 :00
Saturday	00 :00	24 :00
Sunday	00 :00	24 :00

Current Time: 1999-12-31 19:27:33

Weekday: Friday

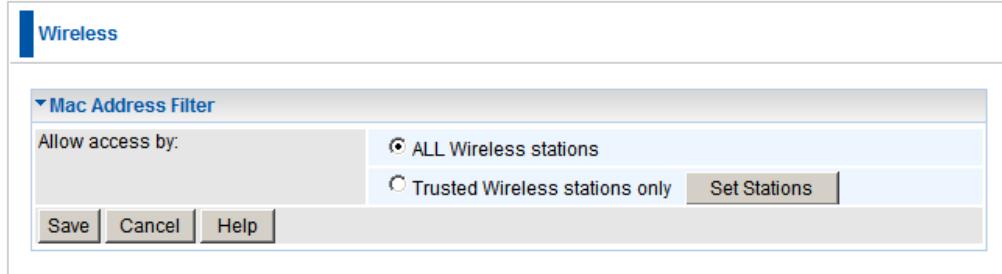
Save **Cancel** **Help**

Wireless – Schedule Screens

Wireless Schedule	
Enable / Disable	This button Enables or Disables the Wireless Schedule function.
Set Schedule	<p>Click this button to set the times that the Wireless signal will turn On and Off.</p> <p>For this feature to work, please ensure that you have set up the NTP Server in the Advanced – Schedule page. The correct time will be displayed if the NTP Server is set up.</p>

Wireless - MAC Filter

This function allows you to allow or deny access to Wireless stations using their MAC Addresses.



Wireless – MAC Filter Screen

MAC Address Filter	
Allow access by ...	<p>Use this feature to determine which Wireless stations can use the Access Point. The options are:</p> <ul style="list-style-type: none"> • All Wireless Stations - All wireless stations can use the access point, provided they have the correct SSID and security settings. • Trusted Wireless stations only - Only wireless stations you designate as "Trusted" can use the Access Point, even if they have the correct SSID and security settings. This feature uses the MAC address to identify Wireless stations. The MAC address is a low-level network identifier which is unique to each PC or network device. To define the trusted wireless stations, use the "Set Stations" button.
Set Stations Button	Click this button to manage the trusted PC Database.

Wireless - MAC Filter - Trusted Wireless Stations

This feature can be used to prevent unknown Wireless stations from using the Access Point. This list has no effect unless the setting *Allow access by trusted stations only* is enabled.

Trusted Wireless Stations

Data - Trusted Wireless Stations

Trusted Wireless Stations	This lists any Wireless Stations which you have designated as "Trusted".
Other Wireless Stations	This list any Wireless Stations detected by the Access Point, which you have not designated as "Trusted".
Name	The name assigned to the Trusted Wireless Station. Use this when adding or editing a Trusted Station.
Address	The MAC (physical) address of the Trusted Wireless Station. Use this when adding or editing a Trusted Station.

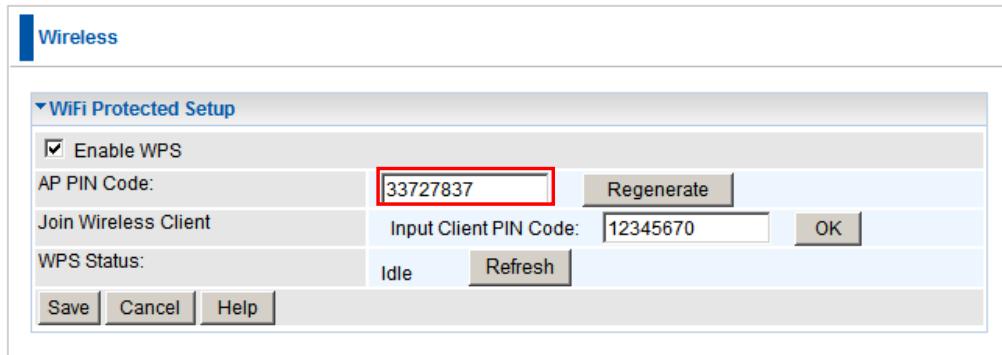
Buttons	
<<	Add a Trusted Wireless Station to the list (move from the "Other Stations" list). <ul style="list-style-type: none"> Select an entry (or entries) in the "Other Stations" list, and click the "<<" button. Enter the Address (MAC or physical address) of the wireless station, and click the "Add" button.
>>	Delete a Trusted Wireless Station from the list (move to the "Other Stations" list). <ul style="list-style-type: none"> Select an entry (or entries) in the "Trusted Stations" list. Click the ">>" button.

Edit	Use this to change an existing entry in the "Trusted Stations" list: <ol style="list-style-type: none">1. Select the Station in the <i>Trusted Station</i> list.2. Click the <i>Edit</i> button. The address will be copied to the "Address" field, and the <i>Add</i> button will change to <i>Update</i>.3. Edit the address (MAC or physical address) as required.4. Click <i>Update</i> to save your changes.
Add (Update)	To add a Trusted Station which is not in the "Other Wireless Stations" list, enter the required data and click this button. When editing an existing Wireless Station, this button will change from <i>Add</i> to <i>Update</i> .
Clear	Clear the <i>Name</i> and <i>Address</i> fields.

Wireless - WiFi Protected Setup (WPS)

WPS feature is following the Wi-Fi Alliance WPS standard and it eases the set up of security-enabled Wi-Fi networks in the home and small office environment.

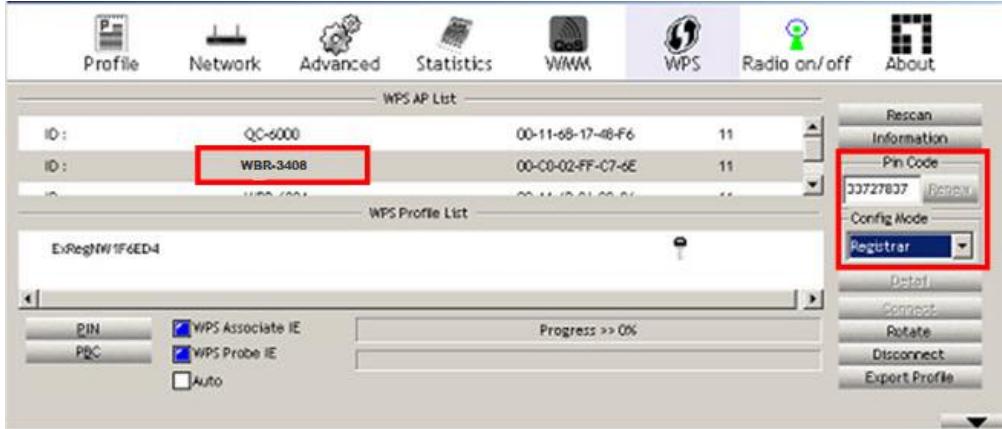
It reduces the user steps required to configure a network and supports two methods that are familiar to most consumers to configure a network and enable security.



WiFi Protected Setup Screen

WiFi Protected Setup	
Enable WPS	Enable this if you want to use Wireless WPS function.
AP PIN Code	Use the default displayed value or click the <i>Regenerate</i> button to have the new pin code in the field. This is the code to be entered on the wireless client.
Input Wireless Client PIN Code	Enter the wireless client's PIN code in the field and click <i>OK</i> to start pairing the client device.

Set your wireless adapter as Registrar and enter the same PIN number to initiate the WPS function.



Screen from Wireless Adapter

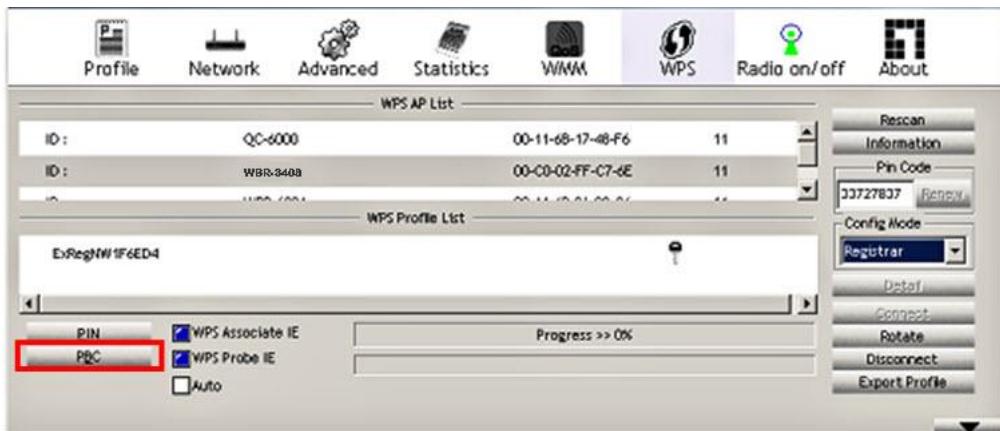
An alternative is to press the WPS button at the front of the router until the WLAN light starts flashing. This indicates that WPS is activated and ready to be paired with client device. The WPS will be in pairing mode (flashing) for 1 minute.



Then press and hold the WPS button on your wireless client for 1 second.



If your device has no physical WPS push button, then you can push the software button in the utility.



Wireless - Wireless Distribution System (WDS)

WDS operation as defined by the IEEE802.11 standard has been made available. Using WDS it is possible to wirelessly connect Access Points, and in doing so extend a wired infrastructure to locations where cabling is not possible or inefficient to implement.

For maximum compatibility, it is recommended that WDS be set up using only the same models, in this case, WBR-3408. Also note that the standard only supports WEP encryption.

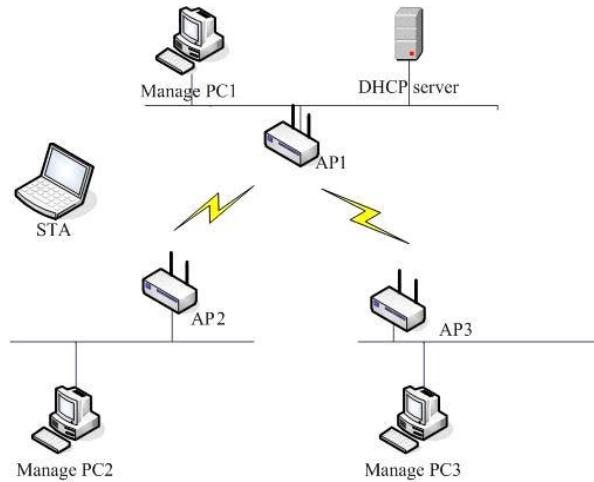
WDS Setup	
<input checked="" type="checkbox"/> Enable WDS	
MAC Address List	AP 1: 00-11-6B-2A-30-C5
	AP 2:
	AP 3:
	AP 4:
<input type="button" value="Save"/> <input type="button" value="Cancel"/> <input type="button" value="Help"/>	

Wireless Distribution System Screen

WDS	
Enable WDS	This feature allows you to make a completely wireless network by using multiple access points without connecting them with a wire LAN. In order to make the WDS working successfully, the access point must use the same channel (not Auto), SSID, as well as the same wireless encryption method.
MAC Address List	Enter the MAC address(es) of the AP(s) into the fields to allow the following access points to be connected to the wireless router.

WDS Environment

Below is an example of how a WDS operates.

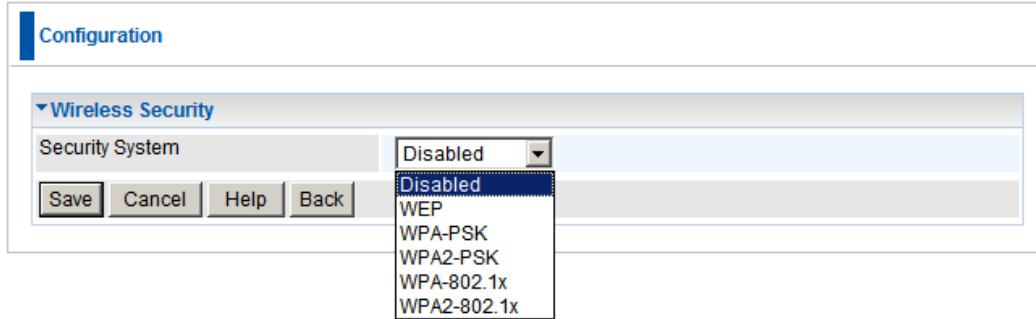


Wireless Distribution System

1. AP1, AP2 and AP3 are configured to use the same Channel and Security settings.
2. Enter AP2 and AP3's MAC addresses into AP1's WDS MAC Address list.
3. AP1 and AP2 should connect via WDS, AP1 and AP3 should connect via WDS.
4. Now the network client (STA) connects to AP2 or AP3 and obtains an IP address from AP1's DHCP Server.

Wireless Security

This screen is accessed by clicking the "**Configure**" button on the *Wireless - Options* screen. There are 4 options for Wireless security:



Wireless Security Screen

- **Disabled** - no data encryption is used.
- **WEP** - data is encrypted using the WEP standard.
- **WPA-PSK** - data is encrypted using the WPA-PSK standard. This is a later standard than WEP, and provides much better security than WEP. If all your Wireless stations support WPA-PSK, you should use WPA-PSK rather than WEP.
- **WPA2-PSK** - This is a further development of WPA-PSK, and offers even greater security, using the AES (Advanced Encryption Standard) method of encryption.
- **WPA-802.1x** - This version of WPA requires a Radius Server on your LAN to provide the client authentication according to the 802.1x standard. Data transmissions are encrypted using the WPA standard.

If this option is selected:

- This Access Point must have a "client login" on the Radius Server.
- Each user must have a "user login" on the Radius Server.
- Each user's wireless client must support 802.1x and provide the login data when required.
- All data transmission is encrypted using the WPA standard. Keys are automatically generated, so no key input is required.

WEP Wireless Security

Configuration

Wireless Security

Security System	WEP
Authentication Type:	Automatic
WEP Data Encryption:	64 bit (10 Hex chars)
Key 1: <input checked="" type="radio"/>	<input type="text"/>
Key 2: <input type="radio"/>	<input type="text"/>
Key 3: <input type="radio"/>	<input type="text"/>
Key 4: <input type="radio"/>	<input type="text"/>
Passphrase:	<input type="text"/> <input type="button" value="Generate Keys"/>
<input type="button" value="Save"/> <input type="button" value="Cancel"/> <input type="button" value="Help"/> <input type="button" value="Back"/>	

WEP

Data - WEP Screen

WEP Data Encryption	
Authentication Type	Normally, this should be left at the default value of "Automatic". If changed to "Open System" or "Shared Key", ensure that your Wireless Stations use the same setting.
WEP Data Encryption	Select the desired option, and ensure the Wireless Stations use the same setting. <ul style="list-style-type: none"> 64 Bit - data is encrypted, using the default key, before being transmitted. You must enter at least the default key. For 64 Bit Encryption, the key size is 10 chars in HEX (0~9 and A~F). 128 Bit - data is encrypted, using the default key, before being transmitted. You must enter at least the default key. For 128 Bit Encryption, the key size is 26 chars in HEX (0~9 and A~F).
Key	Select the key you wish to be the default. Transmitted data is ALWAYS encrypted using the Default Key; the other Keys are for decryption only. You must enter a Key Value for the Default Key .
Key Value	Enter the key value or values you wish to use. The Key is required, the other keys are optional. Other stations must have the same key.
Passphrase	If desired, you can generate a key from a phrase, instead of entering the key value directly. Enter the desired phrase, and click the "Generate Keys" button.

WPA-PSK Wireless Security

Configuration

Wireless Security

Security System	WPA-PSK
PSK:	<input type="text"/>
Encryption:	TKIP

Save Cancel Help Back

WPA-PSK

Data - WPA-PSK Screen

Security System	WPA-PSK Like WEP, data is encrypted before transmission. WPA is more secure than WEP, and should be used if possible. WPA-PSK is the version of WPA, which does NOT require a Radius Server on your LAN.
PSK	Enter the PSK (network key). Data is encrypted using a key derived from the network key. Other Wireless Stations must use the same network key. The PSK must be from 8 to 63 characters in length.
Encryption	The WPA-PSK standard allows different encryption methods to be used. Select the desired option. Wireless Stations must use the same encryption method.

WPA2-PSK Wireless Security

Configuration

Wireless Security

Security System	WPA2-PSK
PSK:	<input type="text"/>
Encryption:	TKIP
<input type="button" value="Save"/> <input type="button" value="Cancel"/> <input type="button" value="Help"/> <input type="button" value="Back"/>	

WPA2-PSK

Data - WPA2-PSK Screen

Authentication	WPA2-PSK This is a further development of WPA-PSK, and offers even greater security.
PSK	Enter the PSK (network key). Data is encrypted using a key derived from the network key. Other Wireless Stations must use the same network key. The PSK must be from 8 to 63 characters in length.
Encryption	The WPA2-PSK standard allows different encryption methods to be used. Select the desired option. Wireless Stations must use the same encryption method.

WPA / WPA2-802.1x Wireless Security

Configuration

▼ Wireless Security

Security System	WPA-802.1x
Server Address:	<input type="text"/>
Radius Port:	1812
Shared Key :	<input type="text"/>
Encryption:	TKIP

Save Cancel Help Back

WPA / WPA2-802.1x

Data – WPA / WPA2-802.1x Screen

Server Address	Enter the server address here.
Radius Port	Enter the port number used for connections to the Radius Server.
Shared Key	Enter the shared key. Data is encrypted using a key derived from the network key. Other Wireless Stations must use the same key. The key must be from 8 to 63 characters in length.
Encryption	The encryption method is TKIP. Wireless Stations must also use TKIP.

Password Screen

The password screen allows you to assign a password to the Wireless Router.

Password Screen

Old Password	Enter the existing password in this field.
New password	Enter the new password here.
Verify password	Re-enter the new password here.

You will be prompted for the password when you connect, as shown below.



Password Dialog

- The "User Name" is always **admin**
- Enter the password for the Wireless Router, as set on the *Password* screen above.

Chapter 4

PC Configuration

4

This Chapter details the PC Configuration required on the local ("Internal") LAN.

Overview

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

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

Windows Clients

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

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

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

TCP/IP Settings - Overview

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

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

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

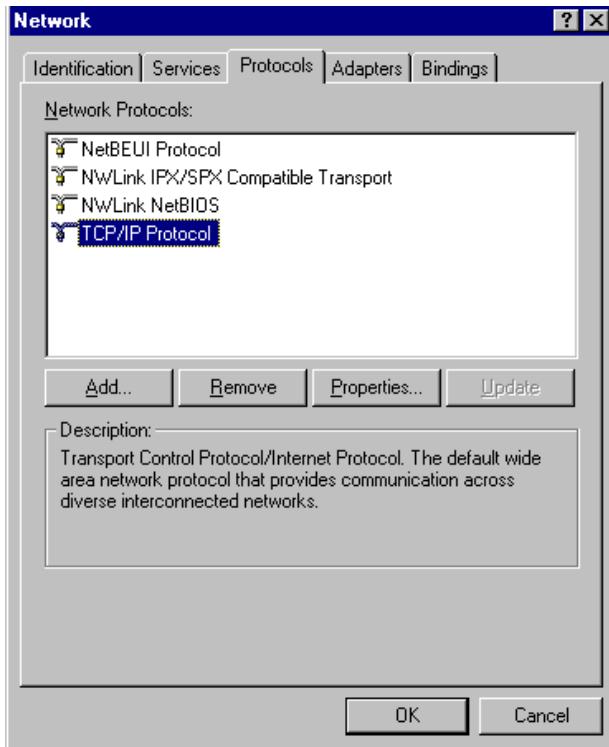
- The *Gateway* must be set to the IP address of the Wireless Router
- The *DNS* should be set to the address provided by your ISP.



If your LAN has a Router, the LAN Administrator must re-configure the Router itself. Refer to *Chapter 8 - Advanced Setup* for details.

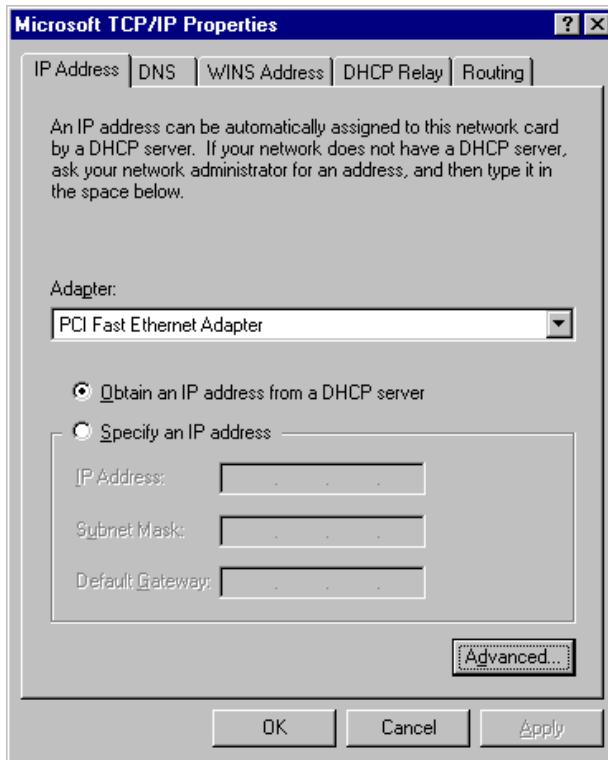
Checking TCP/IP Settings - Windows NT4.0

1. Select *Control Panel - Network*, and, on the *Protocols* tab, select the TCP/IP protocol, as shown below.



Windows NT4.0 - TCP/IP

2. Click the *Properties* button to see a screen like the one below.



Windows NT4.0 - IP Address

3. Select the network card for your LAN.
4. Select the appropriate radio button - *Obtain an IP address from a DHCP Server* or *Specify an IP Address*, as explained below.

Obtain an IP address from a DHCP Server

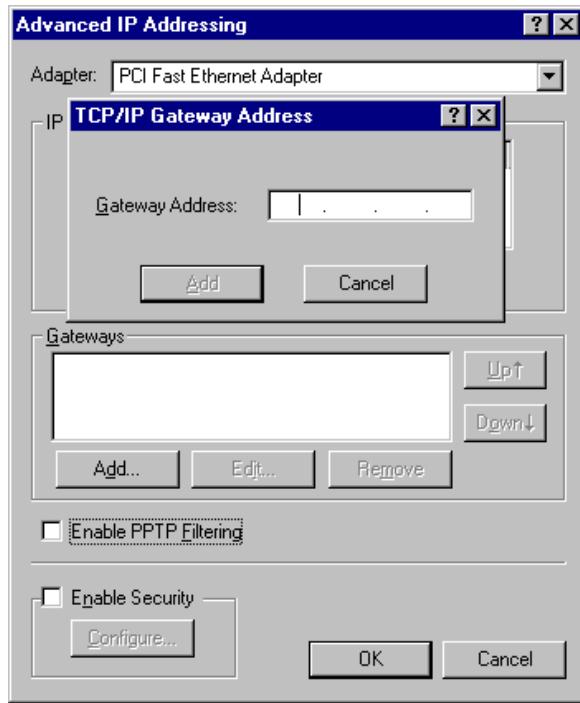
This is the default Windows setting. **Using this is recommended.** By default, the Wireless Router will act as a DHCP Server.

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

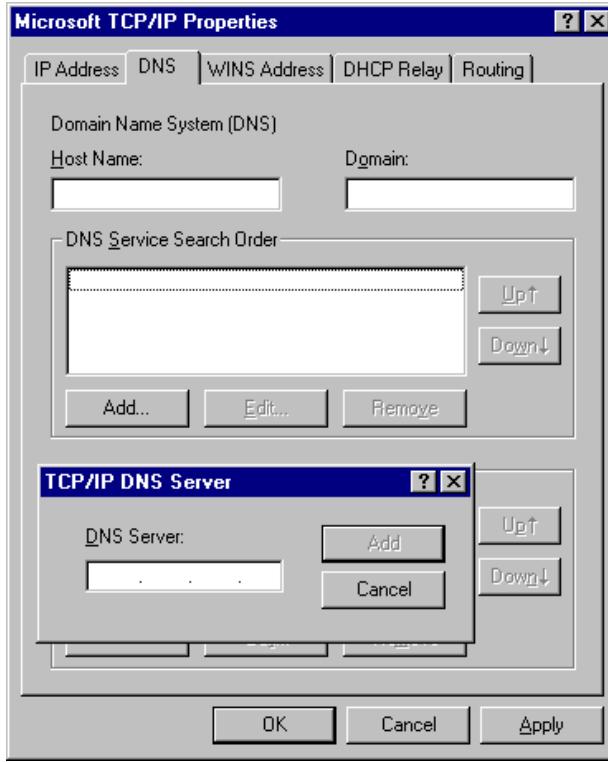
Specify an IP Address

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

1. The *Default Gateway* must be set to the IP address of the Wireless Router. To set this:
 - Click the *Advanced* button on the screen above.
 - On the following screen, click the *Add* button in the *Gateways* panel, and enter the Wireless Router's IP address, as shown below.
 - If necessary, use the *Up* button to make the Wireless Router the first entry in the *Gateways* list.

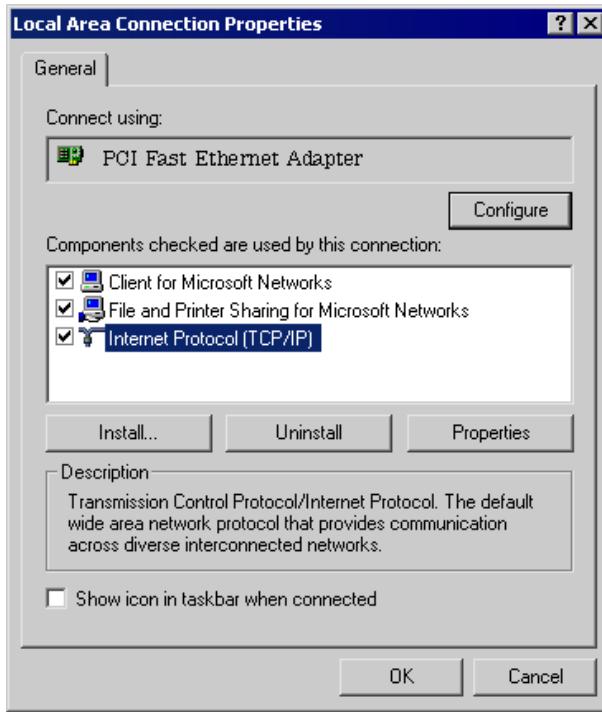
**Windows NT4.0 - Add Gateway**

2. The DNS should be set to the address provided by your ISP, as follows:
 - Click the DNS tab.
 - On the DNS screen, shown below, click the *Add* button (under *DNS Service Search Order*), and enter the DNS provided by your ISP.

**Windows NT4.0 - DNS**

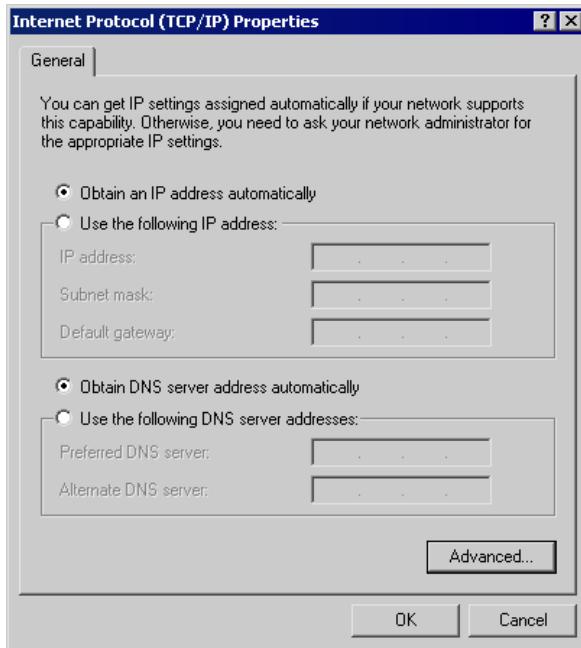
Checking TCP/IP Settings - Windows 2000:

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



Network Configuration (Win 2000)

3. Select the *TCP/IP* protocol for your network card.
4. Click on the *Properties* button. You should then see a screen like the following.



TCP/IP Properties (Win 2000)

5. Ensure your TCP/IP settings are correct, as described below.

Using DHCP

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

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

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

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

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

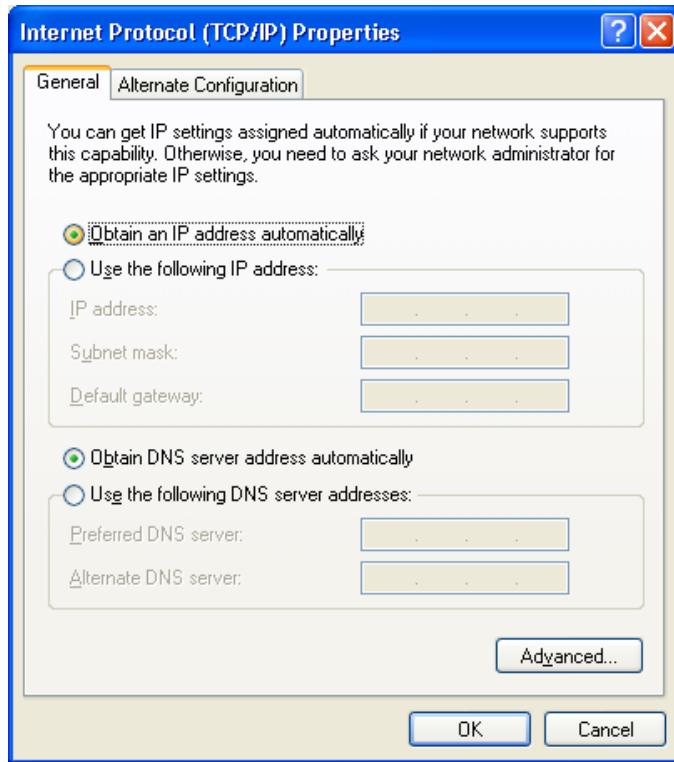
Checking TCP/IP Settings - Windows XP

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



Network Configuration (Windows XP)

3. Select the *TCP/IP* protocol for your network card.
4. Click on the *Properties* button. You should then see a screen like the following.



TCP/IP Properties (Windows XP)

5. Ensure your TCP/IP settings are correct.

Using DHCP

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

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

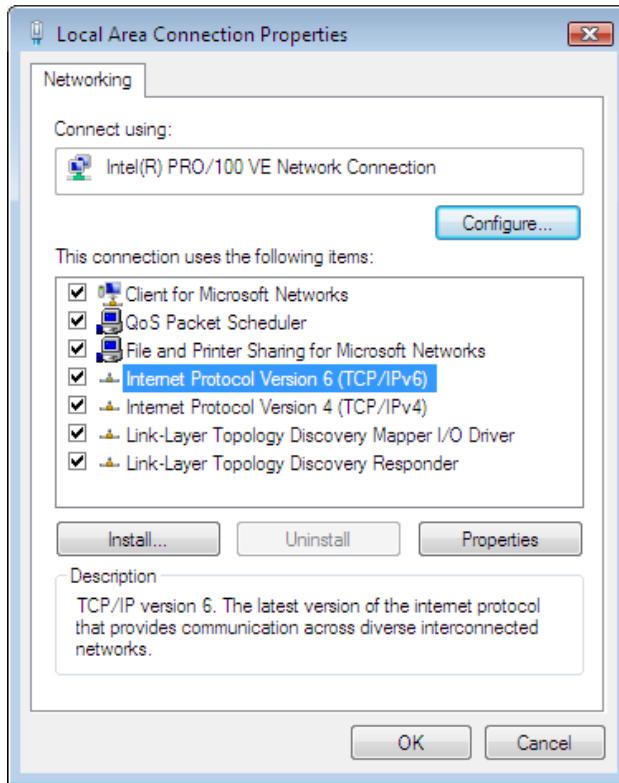
Using a fixed IP Address ("Use the following IP Address")

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

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

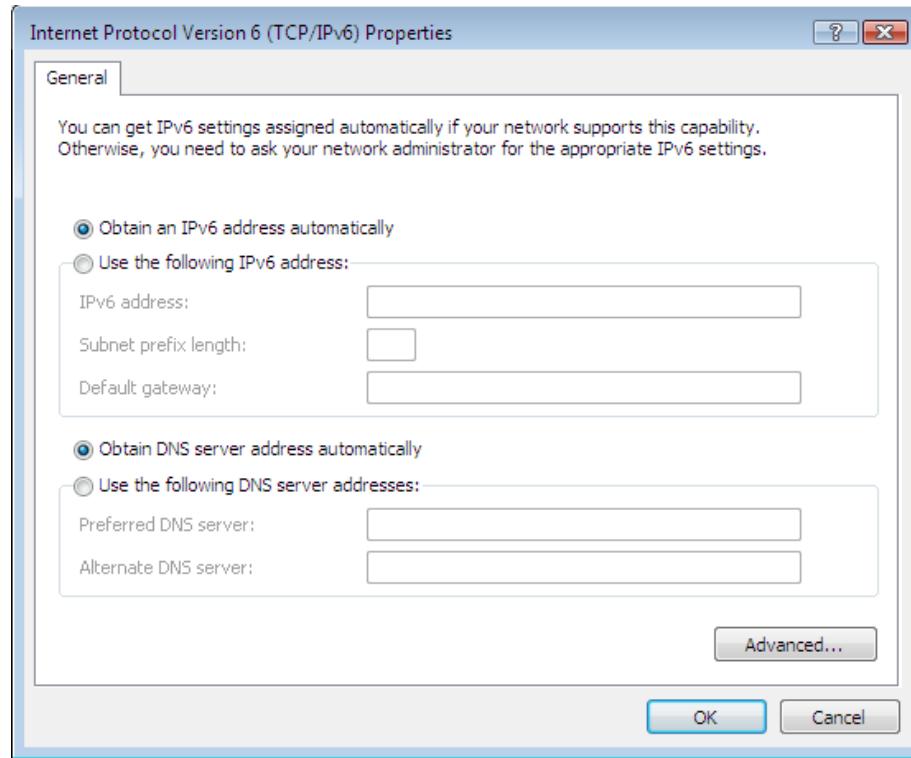
Checking TCP/IP Settings - Windows Vista

1. Select Control Panel - Network Connections.
2. Right click the *Local Area Connection Status* and choose *Properties*. Click *Continue* to the *User Account Control* dialog box, then you should see a screen like the following:



Network Configuration (Windows Vista)

3. Select the *TCP/IP* protocol for your network card.
4. Click on the *Properties* button. You should then see a screen like the following.



TCP/IP Properties (Windows Vista)

5. Ensure your TCP/IP settings are correct.

Using DHCP

To use DHCP, select the radio button *Obtain an IP Address automatically*. This is the default Windows setting. To work correctly, you need a DHCP server on your LAN.

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

If your PC is already configured for a fixed (specified) IP address, no changes are required.

(The Administrator should configure the Wireless Access Point with a fixed IP address from the same address range used on the PCs.)

Internet Access

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

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

For Windows 2000

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

For Windows XP

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

For Windows Vista

You might already be connected to the Internet if your PC is connected to a local area network. Open your web browser and try accessing a website to find out.

1. Select *Start - Control Panel - Network and Internet*.
2. Select *Network and Sharing Center*.
3. Select *Set up a connection or network*
4. Select *Connect to the Internet*.
5. Select the desired method to fit your environment.

Accessing AOL

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

- Start the *AOL for Windows* communication software. Ensure that it is Version 2.5, 3.0 or later. This procedure will not work with earlier versions.

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

Macintosh Clients

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

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

Note:

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

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

Linux Clients

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

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

Fixed IP Address

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

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

To act as a DHCP Client (recommended)

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

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

Other Unix Systems

To access the Internet via the Wireless Router:

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

Wireless Station Configuration

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

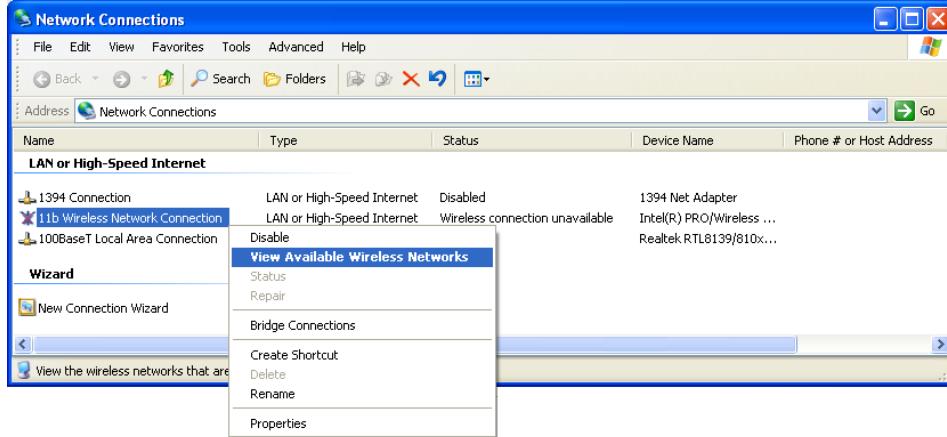
To use the Wireless Access Point in the Wireless Router, each Wireless Station must have compatible settings, as follows:

Mode	The mode must be set to Infrastructure (rather than Ad-hoc). Access points only operate in Infrastructure mode.
SSID (ESSID)	This must match the value used on the Wireless Router. Note! The SSID is case sensitive.
Wireless Security	By default, Wireless security on the Wireless Router is disabled. <ul style="list-style-type: none"> • If Wireless security remains disabled on the Wireless Router, all stations must have wireless security disabled. • If Wireless security is enabled on the Wireless Router, each station must use the same settings as the Wireless Router.

Wireless Configuration on Windows XP

If using Windows XP to configure the Wireless interface on your PC, the configuration procedure is as follows:

1. Open the Network Connections folder. (*Start - Settings - Network Connections*).



Network Connections (Windows XP)

2. Right-click the Wireless Network Connection, check that it is enabled (menu option says *Disable*, rather than *Enable*) and then select *View Available Wireless Networks*.
3. You will then see a list of wireless networks.

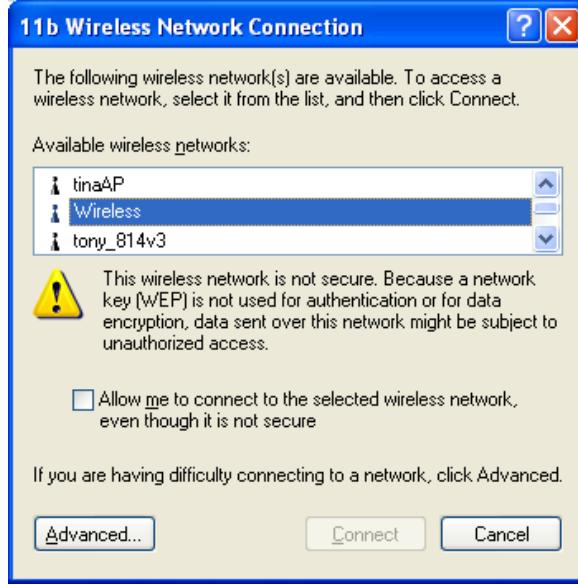
**Wireless Networks (Windows XP)**

If the "Broadcast SSID" setting on the Wireless Router has been disabled, its SSID will NOT be listed.
See the following section "If the SSID is not listed" for details of dealing with this situation.

- The next step depends on whether or not Wireless security has been enabled on the Wireless Router.

If Wireless Security is Disabled

If Wireless security on the Wireless Router is disabled, Windows will warn you that the Wireless network is not secure.

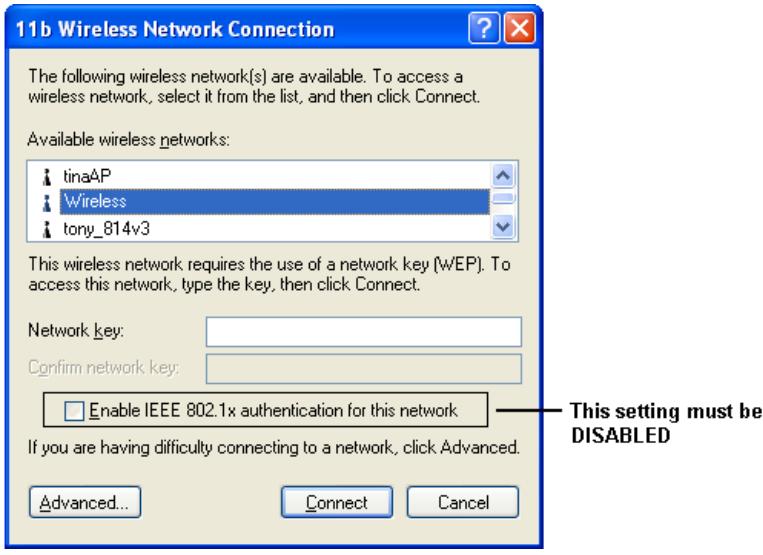
**Insecure Wireless Network (Windows XP)**

To connect:

- Check the checkbox *Allow me to connect to the selected wireless network, even though it is not secure.*
- The *Connect* button will then be available. Click the *Connect* button, and wait a few seconds for the connection to be established.

If using WEP Data Encryption

If WEP data encryption has been enabled on the Wireless Router, Windows will detect this, and show a screen like the following.



WEP (Windows XP)

To connect:

- Enter the WEP key, as set on the Wireless Router, in the *Network Key* field.
- Re-enter the WEP key into the *Confirm Network key* field.
- **Disable** the checkbox *Enable IEEE 802.1x authentication for this network*.
- Click the *Connect* button.

If this fails, click the *Advanced* button, to see a screen like the following:

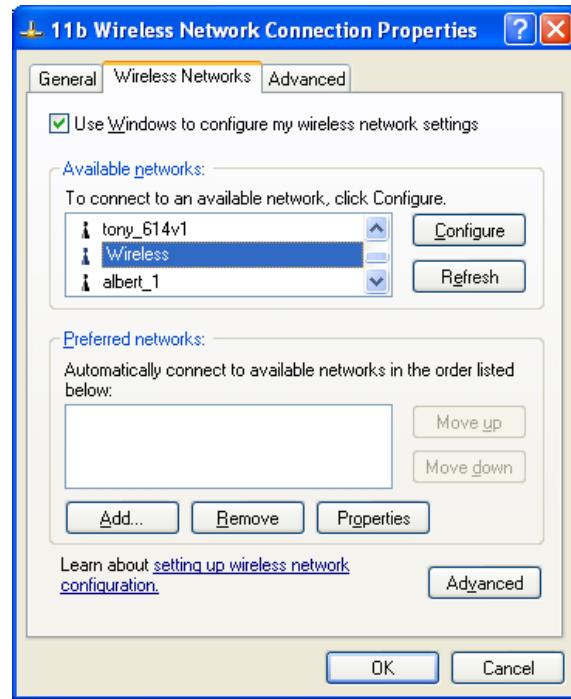
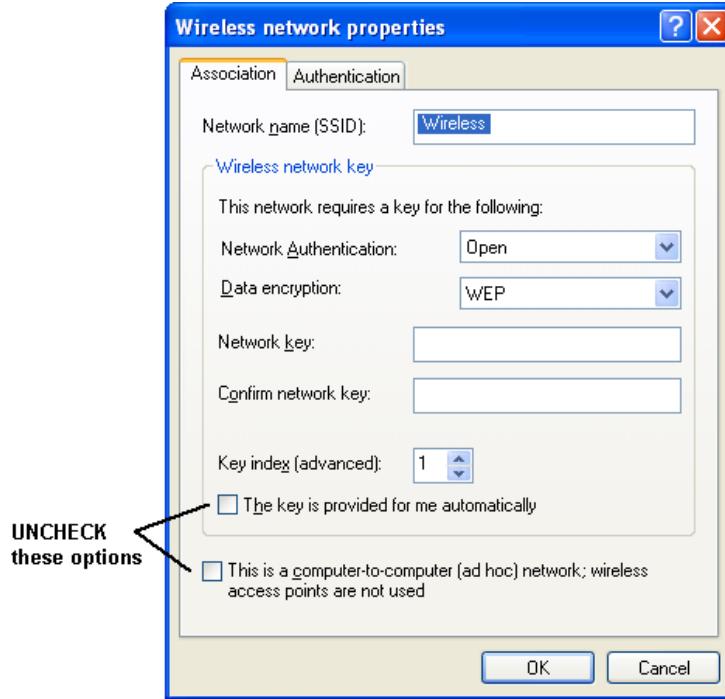


Figure 34: Advanced - Wireless Networks

Select the SSID for the Wireless Router, and click *Configure*, to see a screen like the following:

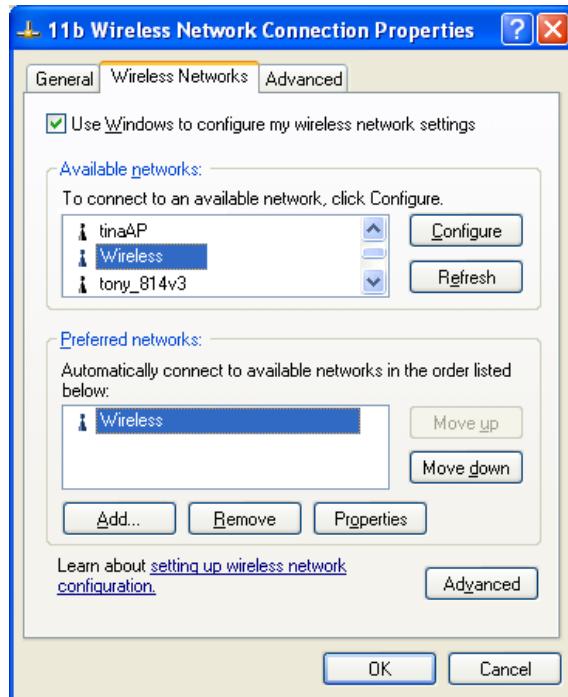


Wireless Network Properties - WEP

Configure this screen as follows:

- Set *Network Authentication* to match the Wireless Router. (If the setting on the Wireless Router is "Auto", then either *Open* or *Shared* can be used.)
- For *Data Encryption*, select **WEP**.

- For the *Network key* and *Confirm network key*, enter the **default key value** used on the Wireless Router. (Windows will determine if 64bit or 128bit encryption is used.)
- The *Key index* must match the **default key index** on the Wireless Router. The default value is 1.
- Ensure the options *The key is provided for me automatically* and *This is a computer-to-computer (ad hoc) network* are unchecked.
- Click OK to save and close this dialog.
- This wireless network will now be listed in *Preferred Networks* on the screen below.

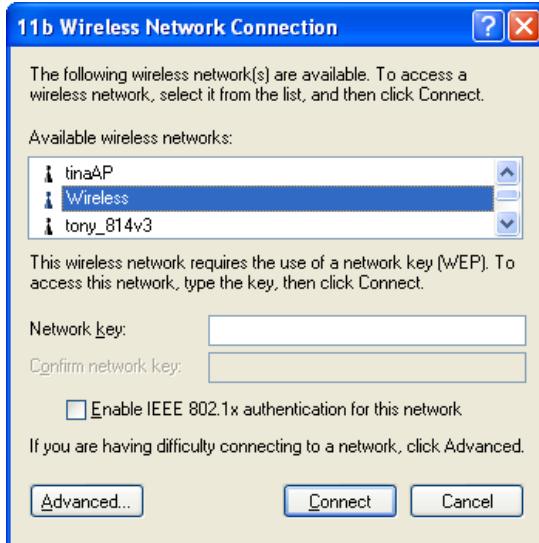


Preferred Networks

Click OK to establish a connection to the Wireless Router.

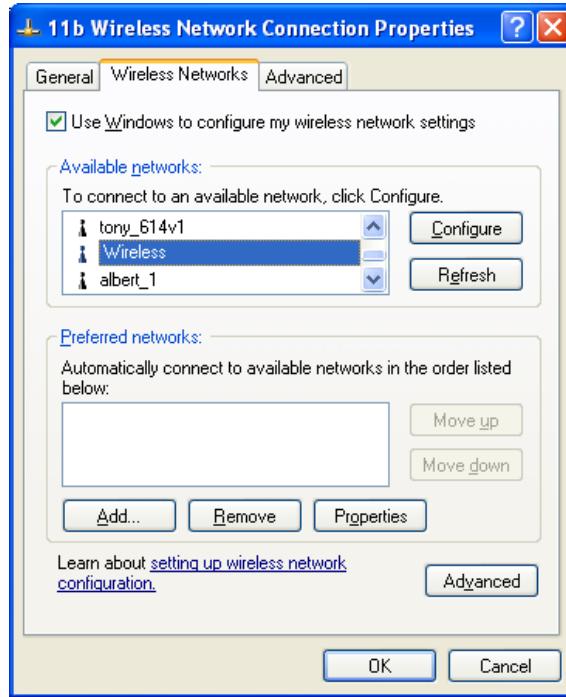
If using WPA-PSK Data Encryption

If WPA-PSK data encryption has been enabled on the Wireless Router, it does not matter which network is selected on the screen below. Just click the *Advanced* button.



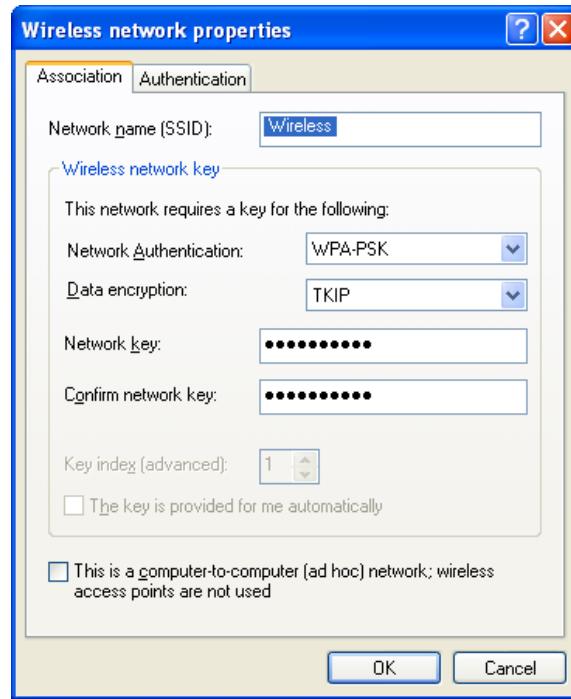
Wireless Networks (Windows XP)

You will then see a screen like the example below.



Advanced - Wireless Networks

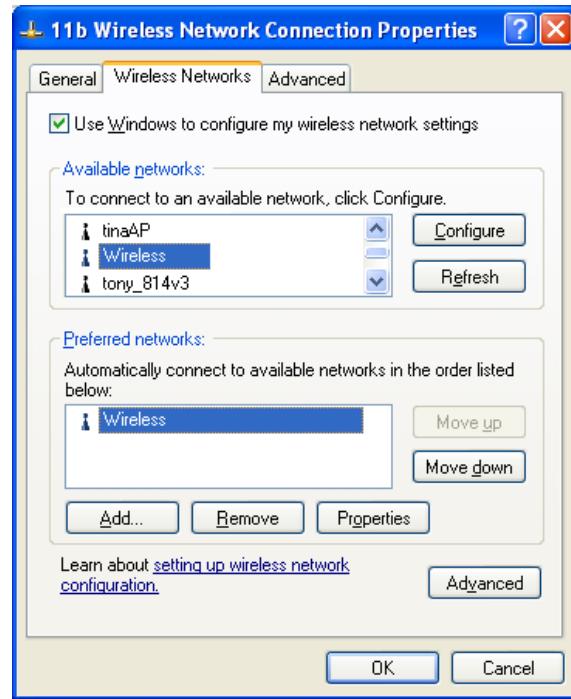
Select the SSID for the Wireless Router, and click *Configure*, to see a screen like the following:



Wireless Network Properties- WPA-PSK

Configure this screen as follows:

- Set *Network Authentication* to **WPA-PSK**.
- For *Data Encryption*, select **TKIP**.
- For the *Network key* and *Confirm network key*, enter the network key (PSK) used on the Wireless Router.
- Ensure the option *This is a computer-to-computer (ad hoc) network* is un-checked.
- Click **OK** to save and close this dialog.
- This wireless network will now be listed in *Preferred Networks* on the screen below.

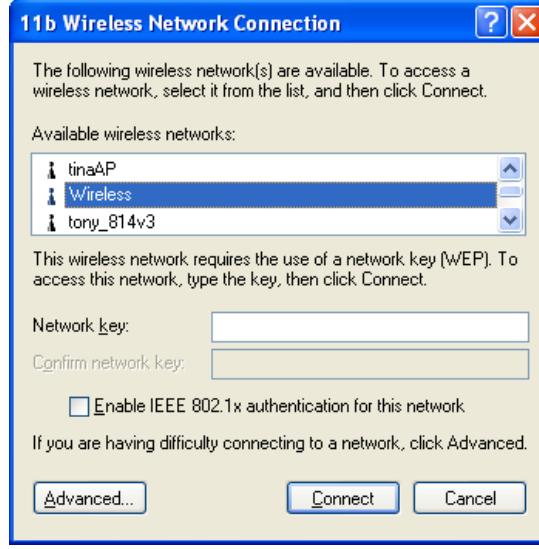


Preferred Networks

Click OK to establish a connection to the Wireless Router.

If the SSID is not listed

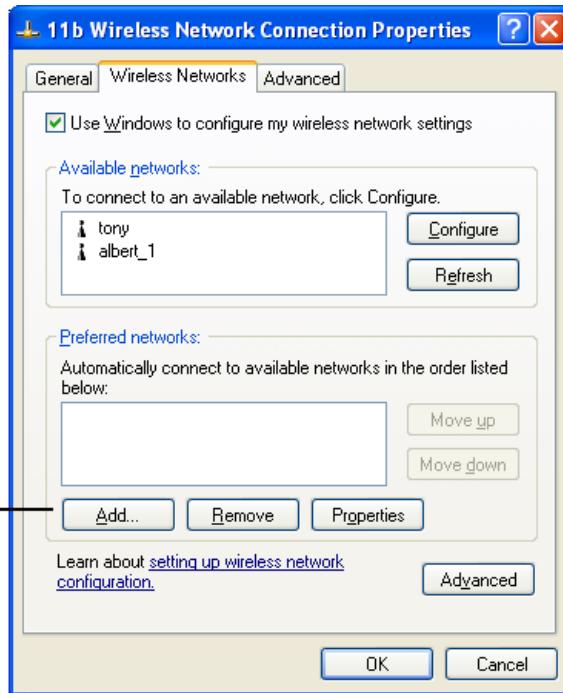
If the "Broadcast SSID" setting on the Wireless Router has been disabled, its SSID will NOT be listed on the screen below.



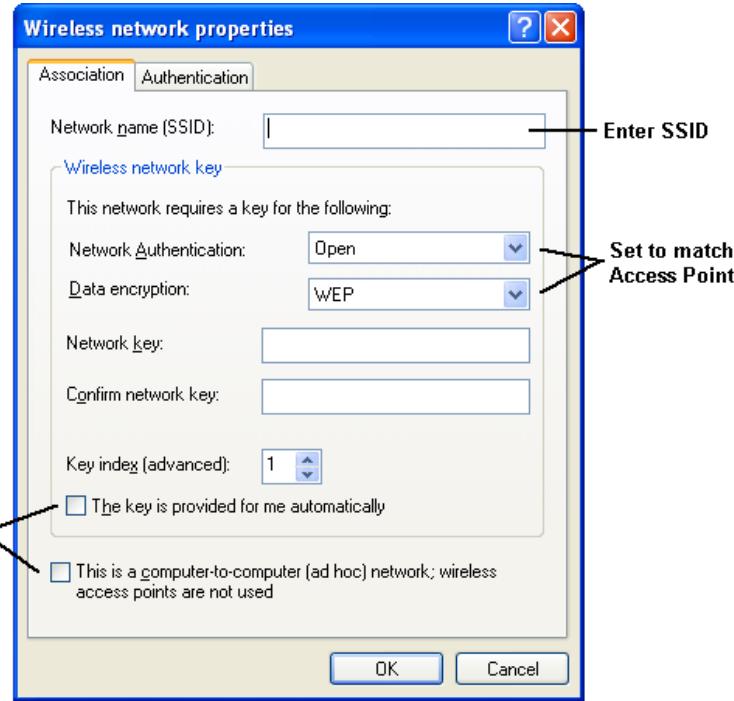
Wireless Networks (Windows XP)

In this situation, you need to obtain the SSID from your network administrator, then follow this procedure:

1. Click the *Advanced* button to see a screen like the example below.

**Unlisted Wireless Network**

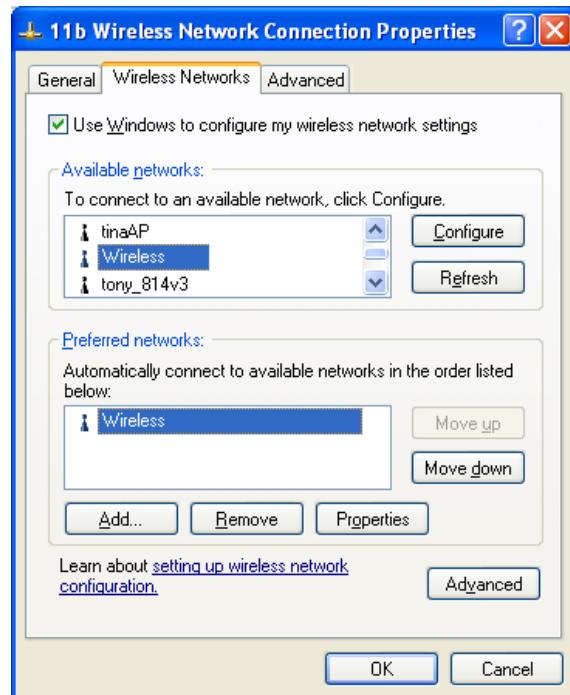
2. Click the *Add* button. You will see a screen like the example below.

**Add Wireless Network**

3. Configure this screen as follows:

- Enter the correct SSID, as used on the Wireless Router. Remember the SSID is case-sensitive, so be sure to match the case, not just the spelling.
- Set *Network Authentication* and *Data Encryption* to match the Wireless Router.

- If using data encryption (WEP or WPA-PSK), enter the key used on the Wireless Router. See the preceding sections for details of WEP and WPA-PSK.
 - Uncheck the options *The key is provided for me automatically* and *This is a computer-to-computer (ad hoc) network*.
 - Click OK to save and exit.
4. This wireless network will then be listed in *Preferred Networks* on the screen below.



Preferred Networks

5. Click OK to establish a connection to the Wireless Router.

Chapter 5

Operation and Status

5

This Chapter details the operation of the Wireless Router and the status screens. For Details of operation in Bridge (Modem) mode, see Chapter 8 - Modem Mode.

Operation - Router Mode

Once both the Wireless Router and the PCs are configured, operation is automatic.

However, there are some situations where additional Internet configuration may be required. Refer to *Chapter 6 - Advanced Features* for further details.

Status Screen

Use the **Status** link on the main menu to view this screen.

Status	
Internet	
Connection Method:	DHCP
Connection Status:	Active
Internet IP Address:	192.168.50.145
Wan MAC Address:	00:c0:02:ff:c7:8f
Connection Details	
LAN	
IP Address:	192.168.0.1
Network Mask:	255.255.255.0
DHCP Server:	On
MAC Address	00:C0:02:FF:C7:8E
PC DataBase	
Wireless	
Region	--
Channel	11
Wireless AP	enable
SSID1 :	
Name (SSID1)	WBR-3408
Broadcast Name	enable
MAC Address	00:C0:02:FF:C7:8E
SSID2 :	
Name (SSID2)	Guest
Broadcast Name	enable
MAC Address	00:c0:02:ff:c7:8f
Wireless Schedule	Disabled Enable/Disable
System	
Device Name:	WBR-3408
Firmware Version:	1.00.00
Current Time :	2009-05-27 05:10:22
Refresh Screen Help	

Status Screen

Data - Status Screen**Internet**

Connection Method	Displays the current connection method, as set in the <i>Setup Wizard</i> .
Connection Status	<p>This indicates the current status of the Internet Connection</p> <ul style="list-style-type: none"> • Active - Connection exists • Idle - No current connection, but no error has been detected. This condition normally arises when an idle connection is automatically terminated. • Failed - The connection was terminated abnormally. This could be caused by Modem failure, or the loss of the connection to the ISP's server. <p>If there is an error, you can click the "Connection Details" button to find out more information.</p>
Internet IP Address	This IP Address is allocated by the ISP (Internet Service Provider). If using a dynamic IP address, and no connection currently exists, this information is unavailable.
WAN MAC Address	It displays the MAC address for the WAN.
Connection Details	Click this button to open a sub-window and view a detailed description of the current connection. Depending on the type of connection, a "log" may also be available.

LAN

IP Address	The IP Address of the Wireless Router.
Network Mask	The Network Mask (Subnet Mask) for the IP Address above.
DHCP Server	This shows the status of the DHCP Server function. The value will be "Enabled" or "Disabled".
MAC Address	This shows the MAC Address for the Wireless Router, as seen on the LAN interface.
PC Database	Click this button to access the PC Database feature.

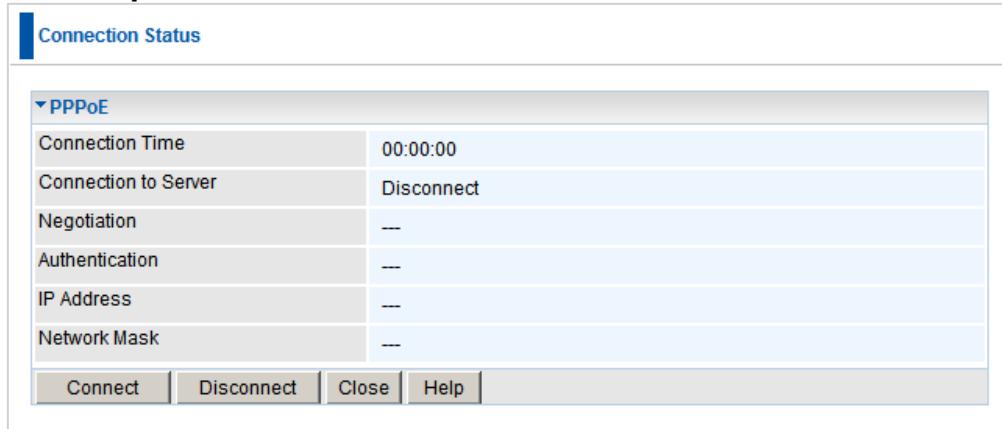
Wireless

Region	The current region, as set on the Wireless screen.
Channel	This shows the Channel currently used, as set on the Wireless screen.
Wireless AP	This indicates whether or not the Wireless Access Point feature is enabled.
SSID 1/2	It displays the name of the SSID 1/2.
Broadcast Name	This indicates whether or not the SSID is Broadcast. This setting is on the Wireless screen.
MAC Address	The MAC (physical) address of the Wireless Access Point.
Wireless Schedule	Indicates whether the Wireless On/Off Schedule is Enabled. You can also use the button to Enable or Disable this feature.

System	
Device Name	The current name of the Router. This name is also the "hostname" for users with an "@Home" type connection.
Firmware Version	The version of the current firmware installed.
Current Time	It displays the current time of the system.
Buttons	
Connection Details	Click this button to open a sub-window and view a detailed description of the current connection.
Refresh Screen	Update the data displayed on screen.

Connection Status - PPPoE

If using PPPoE (PPP over Ethernet), a screen like the following example will be displayed when the "Connection Details" button is clicked.



PPPoE Status Screen

Data - PPPoE Screen

Connection Time	This indicates how long the current connection has been established.
Connection to Server	This indicates whether or not the connection is currently established.
Negotiation	This indicates the status of the Server login.
Authentication	This indicates the authentication currently used.
IP Address	The IP Address of this device, as seen by Internet users. This address is allocated by your ISP (Internet Service Provider).
Network Mask	The Network Mask associated with the IP Address above.
Buttons	
Connect	If not connected, establish a connection to your ISP.
Disconnect	If connected to your ISP, hang up the connection.
Close	Close this window.

Connection Status - PPTP

If using PPTP (Peer-to-Peer Tunneling Protocol), a screen like the following example will be displayed when the "Connection Details" button is clicked.

The screenshot shows a window titled "Connection Details". Under the "PPTP Status" section, it displays the following information:

IP Address	--
PPTP Server IP	203.145.15.34
DNS Server	--

At the bottom of the window are four buttons: "Disconnect", "Connect", "Help", and "Back".

PPTP Status Screen

Data - PPTP Status Screen

Connection	
IP Address	The IP Address of this device, as seen by Internet users. This address is allocated by your ISP (Internet Service Provider).
PPTP Server IP	The IP Address of the PPTP server.
DNS Server	This indicates the DNS address provided by your ISP.
Buttons	
Connect	If not connected, establish a connection to your ISP.
Disconnect	If connected to your ISP, terminate the connection.

Connection Status - L2TP

If using L2TP, a screen like the following example will be displayed when the "Connection Details" button is clicked.

The screenshot shows a user interface titled "Connection Details". Under the "L2TP Status" section, there are three entries: "IP Address" (---), "L2TP Server IP" (---), and "DNS Server" (---). Below these entries are four buttons: "Disconnect", "Connect", "Help", and "Back".

L2TP Status Screen

Data - L2TP Screen

L2TP Status	
IP Address	The IP Address of this device, as seen by Internet users. This address is allocated by your ISP (Internet Service Provider).
L2TP Server IP	The IP Address of the L2TP server.
DNS Server	This indicates the DNS address provided by your ISP.
Buttons	
Connect	If not connected, establish a connection to your ISP.
Disconnect	If connected to your ISP, hang up the connection.

Connection Details - Dynamic IP Address

If your access method is "Direct" (no login), with a Dynamic IP address, a screen like the following example will be displayed when the "Connection Details" button is clicked.

Connection Details	
▼ Dynamic IP Address	
IP Address	--
Subnet Mask	--
Default Gateway	--
DNS Server	--
DHCP Server	--
Lease Obtained:	--
Lease Expires:	--
<input type="button" value="Release"/> <input type="button" value="Renew"/> <input type="button" value="Help"/> <input type="button" value="Back"/>	

Connection Details - Fixed/Dynamic IP Address

Data - Dynamic IP address

Internet	
IP Address	The current IP Address of this device, as seen by Internet users. This address is allocated by your ISP (Internet Service Provider).
Subnet Mask	The Subnet Mask associated with the IP Address above.
Default Gateway	The IP address of the remote Gateway or Router associated with the IP Address above.
DNS Server	The IP address of the Domain Name Server which is currently used.
DHCP Server	The IP address of your ISP's DHCP Server.
Lease Obtained Lease Expires	This indicates when the current IP address was obtained, and how long before this IP address allocation (the DHCP lease) expires.
Buttons	
Release	If an IP Address has been allocated to the Wireless Broadband Router (by the ISP's DHCP Server, clicking the "Release" button will break the connection and release the IP Address.
Renew	If the ISP's DHCP Server has NOT allocated an IP Address for the Wireless Broadband Router, clicking the "Renew" button will attempt to re-establish the connection and obtain an IP Address from the ISP's DHCP Server.
Close	Close this window.

Connection Details - Fixed IP Address

If your access method is "Direct" (no login), with a fixed IP address, a screen like the following example will be displayed when the "Connection Details" button is clicked.

Fixed IP Address	
IP Address	--
Subnet Mask	--
Default Gateway	--
DNS Server	--

Connection Details - Fixed IP Address

Data - Fixed IP address Screen

Fixed IP Address	
IP Address	The IP Address of this device, as seen by Internet users. This address is allocated by your ISP (Internet Service Provider).
Subnet Mask	The Subnet Mask associated with the IP Address above.
Default Gateway	The IP Address of the remote Gateway or Router associated with the IP Address above.
DNS Server	The IP Address of the Domain Name Server which is currently used.

Chapter 6

Advanced Features

6

This Chapter explains when and how to use the Wireless Router's "Advanced" Features.

Overview

The following advanced features are provided:

- Internet:
 - DMZ
 - URL filter
- Access Control
- Dynamic DNS
- Options
- Schedule
- Port Trigger
- Single Port Forwarding
- Port Range Forwarding
- QoS

Internet

This screen provides access to the DMZ, Special Applications and URL Filter features.

The screenshot shows a software interface titled 'Advanced'. Under the 'Internet' section, there are two main categories: 'DMZ' and 'URL Filter'. The 'DMZ' section contains a checkbox labeled 'Enable DMZ, using [] [] [] []' and three radio button options: 'Disable', 'Block Always' (which is selected), and 'Block By Schedule'. A 'Configure URL Filter' button is also present. At the bottom of the screen are 'Save', 'Cancel', and 'Help' buttons.

Internet Screen

DMZ

This feature, if enabled, allows the DMZ computer on your LAN to be exposed to all users on the Internet.

- This allows almost any application to be used on the "DMZ PC".
- The "DMZ PC" will receive all "Unknown" connections and data.

- If the DMZ feature is enabled, you must enter IP address of the PC to be used as the "DMZ PC".



The "DMZ PC" is effectively outside the Firewall, making it more vulnerable to attacks. For this reason, you should only enable the DMZ feature when required.

URL Filter

If you want to limit access to certain sites on the Internet, you can use this feature. The URL filter will check each Web site access. If the address, or part of the address, is included in the block site list, access will be denied.

On the *Advanced Internet* screen, select the desired setting:

- **Disable** - disable this feature.
- **Block Always** - allow blocking all of the time, independent of the *Schedule* page.
- **Block By Schedule** - block according to the settings on the *Schedule* page.

Click the **Configure URL Filter** button to open the URL Filter screen, allowing you to create or modify the filter strings which determine which sites will be blocked.

The **URL Filter** screen is displayed when the **Configure URL Filter** button on the *Advanced Internet* screen is clicked.

URL Filter Screen

Data - URL Filter Screen**Current Filter Strings**

Current Filter Strings	The list contains the current list of items to block. <ul style="list-style-type: none"> • To add to the list, use the "Add" option below. • To delete an entry, select it and click Delete button. • To delete all entries, click the Delete All button.
Add Filter String	To add to the current list, type the word or domain name you want to block into the field provided, then click the Add button. Filter strings should be as specific as possible. Otherwise, you may block access to many more sites than intended.
Trusted PC	
Allow this PC to Visit Blocked Sites	Enable this to allow one computer to have unrestricted access to the Internet. For this PC, the URL filter will be ignored. If enabled, you must select the PC to be the trusted PC.
Trusted PC	Select the PC to be the Trusted PC.

Dynamic DNS (Domain Name Server)

This free service is very useful when combined with the *Virtual Server* feature. It allows Internet users to connect to your Virtual Servers using a URL, rather than an IP Address.

This also solves the problem of having a dynamic IP address. With a dynamic IP address, your IP address may change whenever you connect, which makes it difficult to connect to you.

DDNS Services work as follows:

1. You must register for the service at one of the listed DDNS Service providers.
2. After registration, use the Service provider's normal procedure to obtain your desired Domain name.
3. Enter your DDNS data on the Wireless Router's DDNS screen, and enable the DDNS feature.
4. The Wireless Router will then automatically ensure that your current IP Address is recorded at the DDNS service provider's Domain Name Server.
5. From the Internet, users will be able to connect to your Virtual Servers (or DMZ PC) using your Domain name, as shown on this screen.

Dynamic DNS Screen

Select *Advanced* on the main menu, then *Dynamic DNS*, to see a screen like the following:

The screenshot shows the 'Advanced' menu selected. Under 'DDNS', there is a section for 'DDNS Service' with a checkbox for 'Use a Dynamic DNS Service'. Below this, 'Service Provider' is set to 'DynDNS.org (Dynamic)' with a 'Web Site' button next to it. The 'DDNS Data' section contains fields for 'Host Name', 'User Name', and 'Password'. At the bottom are 'Save', 'Cancel', 'Help', and 'Refresh' buttons.

DDNS Screen

Data - Dynamic DNS Screen

DDNS Service	
Use a Dynamic DNS Service	Use this to enable or disable the DDNS feature as required.
Service Provider	Select the desired DDNS Service provider.
Web Site	Click this button to open a new window and connect to the Web site of the selected DDNS service provider.

DDNS Data	
Host Name	Enter the domain name allocated to you by the DDNS Service. If you have more than one name, enter the name you wish to use.
User Name	Enter your Username for the DDNS Service. (TZO.com uses your E-mail address.)
Password	Enter your current password for the DDNS Service. (TZO.com calls this a key.)
DDNS Status	<ul style="list-style-type: none">• This message is returned by the DDNS Server.• Normally, this message should be "Update successful"• If the message indicates some problem, you need to connect to the DDNS Service provider and correct this problem.

Options

This screen allows advanced users to enter or change a number of settings. For normal operation, there is no need to use this screen or change any settings.

An example **Options** screen is shown below.

The screenshot shows a configuration interface with a blue header bar containing the word "Advanced". Below it is a white form with a light gray header bar labeled "Options". Under "Options", there are two sections: "Internet" and "UPnP".

- Internet:**
 - A checkbox labeled "Respond to Ping on Internet (WAN) Port" is unchecked.
 - A "MTU Size:" input field contains the value "1500" with a note "(Bytes, 600~1500)" next to it.
- UPnP:**
 - A checkbox labeled "Enable UPnP" is checked.
 - "Advertisement Period:" input field contains "30" with a note "(Minutes, 1~1440)" next to it.
 - "Advertisement Time to Live:" input field contains "4" with a note "(Hops, 1~255)" next to it.

At the bottom of the form are three buttons: "Save", "Cancel", and "Help".

Options Screen

Data - Options Screen

Internet	
Respond to Ping	<ul style="list-style-type: none"> If checked, the Wireless Router will respond to Ping (ICMP) packets received from the Internet. If not checked, Ping (ICMP) packets from the Internet will be ignored. Disabling this option provides a slight increase in security.
MTU Size	Enter a value between 600 and 1500. Note: MTU (Maximum Transmission Unit) size should only be changed if advised to do so by Technical Support.
UPnP	
Enable UPnP	<ul style="list-style-type: none"> UPnP (Universal Plug and Play) allows automatic discovery and configuration of equipment attached to your LAN. UPnP is supported by Windows ME, XP, Vista or later. If Enabled, this device will be visible via UPnP. If Disabled, this device will not be visible via UPnP.
Advertisement Period	Enter the desired value, in minutes. The valid range is from 1 to 1440.
Advertisement Time to Live	Enter the desired value, in hops. The valid range is from 1 to 255.

Schedule

This Schedule can be used for the Firewall Rules and the URL filter.

The screenshot shows a configuration interface for a schedule. At the top left is a blue bar with the word "Advanced". Below it is a white form with a title bar containing a dropdown menu labeled "Schedule". The main area has a header "Use 24 hour clock. On all day: 00:00 to 24:00" and "Off all day: All fields left 00". Below this is a 7x4 grid where each row represents a day of the week (Monday to Sunday) and each column represents a session period (Session 1 and Session 2). Each cell contains a two-digit hour and a two-digit minute field. The grid is filled with "00 :00" for all cells except the last one in each row, which is filled with "24 :00". Below the grid is a section titled "Local Time" with fields for "Time Zone" (set to "(GMT) Greenwich Mean Time : Edinburgh, London"), "Adjust for Daylight Savings Time" (checked), "Use this NTP Server" (unchecked), "Current Time" (set to "1999-12-31 17:01:42"), and "Weekday" (set to "Friday"). At the bottom are "Save", "Cancel", and "Help" buttons.

Schedule Screen

Data - Schedule Screen

Schedule	
Day	Each day of the week can be scheduled independently.
Session 1	Two (2) separate sessions or periods can be defined. Session 2 can be left blank if not required.
Session 2	
Start	Enter the start using a 24 hr clock.
Finish	Enter the finish time using a 24 hr clock.
Local Time	
Time Zone	In order to display your local time correctly, you must select your "Time Zone" from the list.
Adjust for Daylight Savings Time	If your region uses Daylight Savings Time, you must manually check "Adjust for Daylight Savings Time" at the beginning of the adjustment period, and uncheck it at the end of the Daylight Savings period.

Use this NTP Server	If you prefer to use a particular NTP server as the primary NTP server, check the checkbox "Use this NTP Server" and enter the Server's IP address in the fields provided. If this setting is not enabled, the default NTP Servers are used.
Current Time	This displays the current time on the Wireless Router, at the time the page is loaded.

Port Trigger

If you use Internet applications which use non-standard connections or port numbers, you may find that they do not function correctly because they are blocked by the Wireless Router's firewall. In this case, you can define the application as a "Port Trigger".

The **Port Trigger** screen can be reached by clicking the *Port Trigger* on the screen.

You can then define your Port Trigger. You will need detailed information about the application; this is normally available from the supplier of the application.

Also, note that the terms "Incoming" and "Outgoing" on this screen refer to traffic from the client (PC) viewpoint

Enable	Name	Outgoing Ports			Incoming Ports		
		Type	Start	Finish	Type	Start	Finish
1. <input type="checkbox"/>		TCP		TCP			
2. <input type="checkbox"/>		TCP		TCP			
3. <input type="checkbox"/>		TCP		TCP			
4. <input type="checkbox"/>		TCP		TCP			
5. <input type="checkbox"/>		TCP		TCP			
6. <input type="checkbox"/>		TCP		TCP			
7. <input type="checkbox"/>		TCP		TCP			
8. <input type="checkbox"/>		TCP		TCP			
9. <input type="checkbox"/>		TCP		TCP			
10. <input type="checkbox"/>		TCP		TCP			
11. <input type="checkbox"/>		TCP		TCP			
12. <input type="checkbox"/>		TCP		TCP			

Save Cancel Help

Port Trigger Screen

Data - Port Trigger Screen

Port Trigger	
Enable	Use this to Enable or Disable this Special Application as required.
Name	Enter a descriptive name to identify this Special Application.

Outgoing Ports	<ul style="list-style-type: none"> • Type - Select the protocol (TCP or UDP) used when you send data to the remote system or service. • Start - Enter the beginning of the range of port numbers used by the application server, for data you send to it. If the application uses a single port number, enter it in both the "Start" and "Finish" fields. • Finish - Enter the end of the range of port numbers used by the application server, for data you send to it. If the application uses a single port number, enter it in both the "Start" and "Finish" fields.
Incoming Ports	<ul style="list-style-type: none"> • Type - Select the protocol (TCP or UDP) used when you receive data from the special application or service. (Note: Some applications use different protocols for outgoing and incoming data). • Start - Enter the beginning of the range of port numbers used by the application server, for data you receive. If the application uses a single port number, enter it in both the "Start" and "Finish" fields. • Finish - Enter the end of the range of port numbers used by the application server, for data you receive.

Single Port Forwarding

This feature allows you to make Servers on your LAN accessible to Internet users. Normally, Internet users would not be able to access a server on your LAN because:

- Your Server does not have a valid external IP Address.
- Attempts to connect to devices on your LAN are blocked by the firewall in this device.

The screenshot shows a web-based configuration interface for port forwarding. At the top left, there is a blue header bar with the word "Advanced". Below it, the main content area has a title "Single Port Forwarding" with a small downward arrow icon. The central part of the screen is a table with 15 rows, each representing a port forwarding rule. The columns are labeled: Application, External Port, Internal Port, Protocol, IP Address, and Enabled. In the "Protocol" column, every row has "TCP" selected from a dropdown menu. In the "IP Address" column, all rows show "192.168.0." followed by a blank input field. The "Enabled" column contains 15 empty checkboxes. At the bottom of the table, there are three buttons: "Save", "Cancel", and "Help".

Application	External Port	Internal Port	Protocol	IP Address	Enabled
			TCP	192.168.0.	<input type="checkbox"/>
			TCP	192.168.0.	<input type="checkbox"/>
			TCP	192.168.0.	<input type="checkbox"/>
			TCP	192.168.0.	<input type="checkbox"/>
			TCP	192.168.0.	<input type="checkbox"/>
			TCP	192.168.0.	<input type="checkbox"/>
			TCP	192.168.0.	<input type="checkbox"/>
			TCP	192.168.0.	<input type="checkbox"/>
			TCP	192.168.0.	<input type="checkbox"/>
			TCP	192.168.0.	<input type="checkbox"/>
			TCP	192.168.0.	<input type="checkbox"/>
			TCP	192.168.0.	<input type="checkbox"/>
			TCP	192.168.0.	<input type="checkbox"/>
			TCP	192.168.0.	<input type="checkbox"/>

Figure 1: Single Port Forwarding Screen

Data - Single Port Forwarding Screen

Single Port Forwarding	
Application	Enter the desired application type.
External Port	Traffic from the Internet using this port number will be sent to the Server. This is normally the same as the Internal Port Number. If it is different, this device will perform a "mapping" or "translation" function, allowing the server to use a different port to the clients.
Internal Port	Enter the port numbers which the Server software is configured to use.
Protocol	Select the protocol (TCP or UDP) used by the Server.
IP Address	Enter the desired IP address.
Enabled	Use this to Enable or Disable support for this Server, as required.

Port Range Forwarding

This feature allows you to make Servers on your LAN accessible to Internet users. Normally, Internet users would not be able to access a server on your LAN because:

The screenshot shows a configuration interface titled "Port Range Forwarding". At the top left is a blue bar labeled "Advanced". Below it is a table with 10 rows, each representing a port forwarding rule. The columns are: Application, Start, End, Protocol, IP Address, and Enable. All rows have "TCP" selected in the Protocol dropdown and "192.168.0." in the IP Address field. The "Enable" column contains empty checkboxes. At the bottom of the table are three buttons: "Save", "Cancel", and "Help".

Application	Start	End	Protocol	IP Address	Enable
			TCP	192.168.0.	<input type="checkbox"/>
			TCP	192.168.0.	<input type="checkbox"/>
			TCP	192.168.0.	<input type="checkbox"/>
			TCP	192.168.0.	<input type="checkbox"/>
			TCP	192.168.0.	<input type="checkbox"/>
			TCP	192.168.0.	<input type="checkbox"/>
			TCP	192.168.0.	<input type="checkbox"/>
			TCP	192.168.0.	<input type="checkbox"/>
			TCP	192.168.0.	<input type="checkbox"/>
			TCP	192.168.0.	<input type="checkbox"/>

Port Range Forwarding Screen

Data - Port Range Forwarding Screen

Port Range Forwarding	
Application	Enter the desired application type.
Start	Enter the beginning of the range of port numbers used by the application server.
End	Enter the end of the range of port numbers used by the application server.
Protocol	Select the protocol (TCP, UDP or Both) used by the Server.
IP Address	Enter the desired IP address.
Enable	Use this to Enable or Disable support for this Server, as required.

QoS

The QoS (Quality of Service) feature allows you specify priorities for different traffic. Lower priority traffic will be slowed down to allow greater throughput or less delay for high priority traffic.

An example **QoS** screen is shown below.

QoS Screen

Data - QoS Screen

QoS Setting	
QoS Setting	To disable QoS (Quality of Service), keep the default setting, Disable. To enable QoS (Quality of Service), click Enable and follow these instructions.
Management Type	<p>There are 2 options:</p> <ul style="list-style-type: none"> • Rate Control - The QoS will be managed by the size of the bandwidth. • Priority - The QoS will be managed by the priority. <p>Note: Rate Control and Priority cannot be used simultaneously.</p>
Bandwidth	<p>Enter the desired value of the bandwidth.</p> <p>For QoS to function properly, the correct value of your Internet bandwidth is required. Please check with your Service Provider if you are unsure.</p>

Category	<p>Applications:</p> <ul style="list-style-type: none"> • Add a New Application (Once selected, please complete the following setups.) • Ip/Net: Enter the IP address. • Rate: Enter the desired rate value. • Priority: Select the desired option (High, Normal, Low) • Direct: Select <i>Upstream</i> or <i>Downstream</i> as required. • Self-Define <ul style="list-style-type: none"> • Name: Enter a name for your device. • Port Range: Enter the value for the desired port range. • Protocol: Select the desired option. • Ip/Net: Enter the IP address of your device. • Rate: Enter the desired rate value. • Priority: Select the option (High, Normal, Low) from the list. • Direct: Select <i>Upstream</i> or <i>Downstream</i> as required.
Summary	
Priority	The general Information of this Application or IP Address.
Name	The Name of this Application or IP Address.
Information	The general Information of this Application or IP Address.

Note: Rate Control and Priority methods cannot be used at the same time.

Chapter 7

Advanced Administration

7

This Chapter explains the settings available via the "Administration" section of the menu.

Overview

Normally, it is not necessary to use these screens, or change any settings. These screens and settings are provided to deal with non-standard situations, or to provide additional options for advanced users.

The available settings and features are:

PC Database	This is the list of PCs shown when you select the "DMZ PC" or a "Virtual Server". This database is maintained automatically, but you can add and delete entries for PCs which use a Fixed (Static) IP Address.
Config File	Backup or restore the configuration file for the Wireless Router. This file contains all the configuration data.
Logs & E-mail	View or clear all logs, set E-Mailing of log files and alerts.
Diagnostics	Perform a Ping or DNS Lookup.
Remote Admin	Allow settings to be changed from the Internet.
Routing	Only required if your LAN has other Routers or Gateways.
Upgrade Firmware	Upgrade the Firmware (software) installed in your Wireless Router.

PC Database

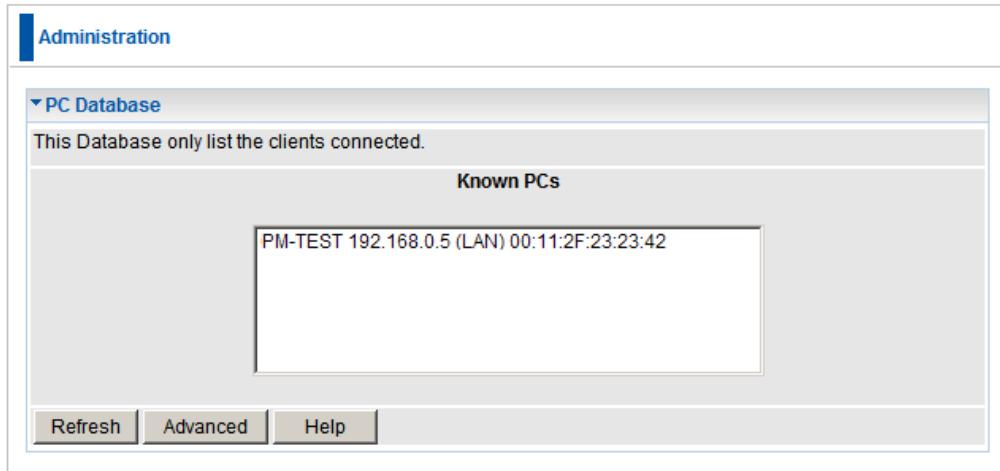
The PC Database is used whenever you need to select a PC (e.g. for the "DMZ" PC).

- It eliminates the need to enter IP addresses.
- Also, you do not need to use fixed IP addresses on your LAN.

However, if you do use a fixed IP address on some devices on your LAN, you should enter details of each such device into the PC database, using the PC Database screen.

PC Database Screen

An example **PC Database** screen is shown below.



PC Database

- PCs which are "DHCP Clients" are automatically added to the database, and updated as required.
- By default, non-Server versions of Windows act as "DHCP Clients"; this setting is called "Obtain an IP Address automatically".
- The Wireless Router uses the "Hardware Address" to identify each PC, not the name or IP address. The "Hardware Address" can only change if you change the PC's network card or adapter.
- This system means you do NOT need to use Fixed (static) IP addresses on your LAN. However, you can add PCs using Fixed (static) IP Addresses to the PC database if required.

Data - PC Database Screen

Known PCs	This lists all current entries. Data displayed is <i>name (IP Address)</i> <i>type</i> . The "type" indicates whether the PC is connected to the LAN.
Button	
Refresh	Update the data on screen.
Advanced	Click this to view the advanced "PC Database" screen.

PC Database (Admin)

This screen is displayed if the "Advanced" button on the **PC Database** is clicked. It provides more control than the standard **PC Database** screen.

The screenshot shows the 'Administration' interface with the 'PC Database - Advanced' section selected. A message at the top states: 'Any PC may be added, edited or deleted. If adding a PC which is not connected and On, you must provide the MAC (hardware) address'. Below this is a table for 'Known PCs' containing one entry: 'PM-TEST 192.168.0.5 (LAN) 00:11:2F:23:23:42'. Below the table are 'Edit' and 'Delete' buttons. The 'PC Properties' section contains fields for 'Name' (with an empty input field), 'IP Address' (with radio buttons for 'Automatic (DHCP Client)', 'DHCP Client - reserved IP address' (showing 192.168.0.1), and 'Fixed IP address (set on PC)' (with four input fields for 192, 168, 0, and 1), and 'MAC Address' (with radio buttons for 'Automatic discovery (PC must be available on LAN)' and 'MAC address is' followed by an input field). At the bottom are buttons for 'Add as New Entry', 'Update Selected PC', 'Clear Form', 'Refresh', 'Standard Screen', and 'Help'.

PC Database (Admin)

Data - PC Database (Admin) Screen

Known PCs	This lists all current entries. Data displayed is <i>name (IP Address) type</i> . The "type" indicates whether the PC is connected to the LAN.
Edit	Use this to change the data for the selected PC in the list. The data for the selected PC will then be shown in the "Properties" area, where it may be edited. (Click "Update" to save any changes.)
Delete	Use this to Delete the selected PC from the list. This should be done in 2 situations: <ul style="list-style-type: none"> • The PC has been removed from your LAN. • The entry is incorrect.
PC Properties	
Name	If adding a new PC to the list, enter its name here. It is best if this matches the PC's "hostname".

IP Address	Select the appropriate option: <ul style="list-style-type: none"> • Automatic - The PC is set to be a DHCP client (Windows: "Obtain an IP address automatically"). The Wireless Router will allocate an IP address to this PC when requested to do so. The IP address could change, but normally won't. • DCHP Client - Reserved IP Address - Select this if the PC is set to be a DCHP client, and you wish to guarantee that the Wireless Router will always allocate the same IP Address to this PC. Enter the required IP address. Only the last field is required; the other fields must match the Wireless Router's IP address. • Fixed IP Address - Select this if the PC is using a Fixed (Static) IP address. Enter the IP address allocated to the PC. (The PC must be configured to use this IP address.)
MAC Address	Select the appropriate option <ul style="list-style-type: none"> • Automatic discovery - Select this to have the Wireless Router contact the PC and find its MAC address. This is only possible if the PC is connected to the LAN and powered On. • MAC address is - Enter the MAC address on the PC. The MAC address is also called the "Hardware Address", "Physical Address", or "Network Adapter Address". The Broadband Router uses this to provide a unique identifier for each PC. Because of this, the MAC address can NOT be left blank.
Buttons	
Add as New Entry	Add a new PC to the list, using the data in the "Properties" box. If "Automatic discovery" (for MAC address) is selected, the PC will be sent a "ping" to determine its hardware address. This will fail unless the PC is connected to the LAN, and powered on.
Update Selected PC	Update (modify) the selected PC, using the data in the "Properties" box.
Clear Form	Clear the "Properties" box, ready for entering data for a new PC.
Refresh	Update the data on screen.
Standard Screen	Click this to view the standard PC Database screen.

Config File

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

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

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

An example **Config File** screen is shown below.

The screenshot shows the 'Administration' interface with the 'Config File' section selected. The 'Backup Config' section contains a 'Save a Copy of Current Settings' button and a 'Backup' button. The 'Restore Config' section contains a 'Restore Saved Settings from a File' input field, a 'Browse...' button, and a 'Restore' button. The 'Default Config' section contains a 'Revert to Factory Default Settings' button and a 'Factory Defaults' button. A 'Help' button is also present at the bottom left.

Config File Screen

Data - Config File Screen

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

Logs

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

Since only a limited amount of log data can be stored in the Wireless Router, log data can also be E-mailed to your PC. Use the **E-Mail** screen to configure this feature.

Administration

Logs

Current time 1999-12-31 17:23:06

Refresh Clear Log Send Log

Include in Log

- Attempted access to blocked sites
- Connections to the Web-based interface of this Router
- Router operation (start up, get time etc)
- Known DoS attacks and Port Scans
- Outgoing (Internet) connections
- Access control

Include in Log

- Disable
- Broadcast on LAN
- Send to this Syslog Server: [] . [] . [] . []

Save Cancel Help

This screenshot shows the 'Logs' configuration screen. At the top, it displays the current time as '1999-12-31 17:23:06'. Below this is a large empty text area for viewing logs, which is currently empty. At the bottom of this area are three buttons: 'Refresh', 'Clear Log', and 'Send Log'. Under the heading 'Include in Log', there is a list of checkboxes for selecting what types of events to log. Most checkboxes are checked: 'Attempted access to blocked sites', 'Connections to the Web-based interface of this Router', 'Router operation (start up, get time etc)', and 'Known DoS attacks and Port Scans'. The 'Outgoing (Internet) connections' and 'Access control' checkboxes are unchecked. Below this section is another 'Include in Log' section with three radio button options: 'Disable' (selected), 'Broadcast on LAN', and 'Send to this Syslog Server'. The 'Send to this Syslog Server' option includes four input fields for IP address and port information. At the very bottom of the screen are three buttons: 'Save', 'Cancel', and 'Help'.

Logs Screen

Data - Logs Screen

Logs	
Current Time	The current time on the Wireless Router is displayed.
Log Data	Current log data is displayed in this panel.
Buttons	<p>There are three (3) buttons</p> <ul style="list-style-type: none"> • Refresh - Update the log data. • Clear Log - Clear the log, and restart it. This makes new messages easier to read. • Send Log - E-mail the log immediately. This is only functional if the E-mail screen has been configured.
Include in Logs	
Include (Checkboxes)	<p>Use these checkboxes to determine which events are included in the log. Checking all options will increase the size of the log, so it is good practice to disable any events which are not really required.</p> <ul style="list-style-type: none"> • Attempted access to blocked sites - If checked, attempted Internet accesses which were blocked are logged. • Connections to the Web-based interface of this Router - If checked, this will log connections TO this Router, rather than through this Router to the Internet. • Router operation - If checked, other Router operations (not covered by the selections above) will be logged. • Known DoS attacks and Port Scans - If checked, Denial of Service attacks, as well as port scans, will be logged. • Outgoing (Internet) connections - If checked, the outgoing Internet connections are logged. • Access Control - If enabled, the log will include attempted outgoing connections which have been blocked by the "Access Control" feature.
Syslog	
Disable	Data is not sent to a Syslog Server.
Broadcast on LAN	The Syslog data is broadcast, rather than sent to a specific Syslog server. Use this if your Syslog Server does not have a fixed IP address.
Send to this Syslog Server	If your Syslog server has a fixed IP address, select this option, and enter the IP address of your Syslog server.

E-Mail

This screen allows you to E-mail Logs and Alerts. A sample screen is shown below.

The screenshot shows a configuration interface for E-mail settings. It includes sections for E-mail Notification, E-mail Alerts, and E-mail Logs. The E-mail Notification section contains fields for turning notification on, sending to an E-mail address, specifying an outgoing SMTP server, and configuring authentication. The E-mail Alerts section allows setting up alerts for DoS attacks, port scans, and blocked site attempts. The E-mail Logs section defines a schedule for sending logs (Hourly, Day, Time, and AM/PM). At the bottom are Save, Cancel, and Help buttons.

E-Mail Screen

Data - E-Mail Screen

E-Mail Notification	
Turn E-mail Notification on	Check this box to enable this feature. If enabled, the E-mail address information (below) must be provided.
Send to this E-mail Address	Enter the E-mail address the Log is to be sent to. The E-mail will also show this address as the Sender's address.
Outgoing (SMTP) Mail Server	Enter the address or IP address of the SMTP (Simple Mail Transport Protocol) Server you use for outgoing E-mail.
Mail Sender Address	Enter the mail address of the sender. The E-mail will also show this address as the Sender's address.
My SMTP Mail Server requires authentication	To stop spammers, many SMTP mail servers require you to log in to send mail. In this case, enable this checkbox, and enter the login information (User name and Password) in the fields below.

User Name	If you have enabled "My SMTP Mail Server requires authentication" above, enter the User Name required to login to your SMTP Server.
Password	If you have enabled "My SMTP Mail Server requires authentication" above, enter the password required to login to your SMTP Server.
E-mail Alerts	
Send E-mail alerts immediately	You can choose to have alerts E-mailed to you, by checking the desired checkboxes. The Wireless Router can send an immediate alert when it detects a significant security incident such as <ul style="list-style-type: none"> • A known hacker attack is directed at your IP address • A computer on the Internet scans your IP address for open ports • Someone on your LAN (Local Area Network) tries to visit a blocked site.
E-mail Logs	
Send Logs	<p>Select the desired option for sending the log by E-mail.</p> <ul style="list-style-type: none"> • Never (default) - This feature is disabled; Logs are not sent. • When log is full - The time is not fixed. The log will be sent when the log is full, which will depend on the volume of traffic. • Hourly, Daily, Weekly... - The log is sent on the interval specified. <ul style="list-style-type: none"> • If Daily is selected, the log is sent at the time specified. Select the time of day you wish the E-mail to be sent. • If Weekly is selected, the log is sent once per week, on the specified day, at the specified time. Select the day and the time of day you wish the E-mail to be sent. <p>Note:</p> <p>If the log is full before the time specified to send it, it will be sent regardless of the day and time specified.</p>

Diagnostics

This screen allows you to perform a "Ping" or a "DNS lookup". These activities can be useful in solving network problems.

An example **Network Diagnostics** screen is shown below.

The screenshot shows a web-based administration interface titled "Administration". Under the "Ping" section, there is a field for "IP Address" with four input boxes and a "Ping" button. Under "DNS Lookup", there is a field for "Internet Name" with one input box and a "Lookup" button. Under "Routing", there is a link "Display the Routing Table" with a "Display" button. A "Help" button is also present.

Network Diagnostics Screen

Data - Network Diagnostics Screen

Ping	
IP Address	Enter the IP address you wish to ping. The IP address can be on your LAN, or on the Internet. Note that if the address is on the Internet, and no connection currently exists, you could get a "Timeout" error. In that case, wait a few seconds and try again.
Ping Button	After entering the IP address, click this button to start the "Ping" procedure. The results will be displayed in the <i>Ping Results</i> pane.
DNS Lookup	
Internet Name	Enter the Domain name or URL for which you want a DNS (Domain Name Server) lookup. Note that if the address is on the Internet, and no connection currently exists, you could get a "Timeout" error. In that case, wait a few seconds and try again.
Lookup Button	After entering the Domain name/URL, click this button to start the "DNS Lookup" procedure.
Routing	
Display	Click this button to display the internal routing table. This information can be used by Technical Support and other staff who understand Routing Tables.

Remote Administration

If enabled, this feature allows you to manage the Wireless Router via the Internet.

The screenshot shows the 'Administration' section with the 'Remote Administration' tab selected. Under 'Enable Remote Management', there is a checkbox labeled 'Enable Remote Management'. Below it, 'Current IP Address:' is listed as a placeholder. 'Port Number:' is set to '8080'. In the 'Access Permission' section, 'Allow Remote Access By:' has three options: 'Everyone' (selected), 'Only This Computer', and 'IP Address Range'. The 'Everyone' option includes fields for 'From' and 'To' IP addresses. At the bottom are 'Save', 'Cancel', and 'Help' buttons.

Remote Administration Screen

Data - Remote Administration Screen

Remote Administration	
Enable Remote Management	Check to allow administration/management via the Internet. (To connect, see below). If Disabled, this device will ignore Administration connection attempts from the Internet.
Current IP Address	This is the current address you will use when accessing this device from the Internet. To connect, see details and an example below.
Port Number	Enter a port number between 1 and 65535. The default for HTTP (Web) connections is port 80, but using port 80 will prevent the use of a Web "Virtual Server" on your LAN. So using a different port number is recommended. The default value is 8080. The port number must be specified in your Browser when you connect. See the following section for details.
Access Permission	
Allow Remote Access	Select the desired option. <ul style="list-style-type: none"> • Everyone - allow access by everyone on the Internet. • Only This Computer - allow access by only one IP address. Enter the desired IP address. • IP Address Range - allow access from a range of IP addresses on the Internet. Enter a beginning and ending IP address to define the allowed range. For security, you should restrict access to as few external IP addresses as practical.

To connect from a remote PC via the Internet

1. Ensure your Internet connection is established, and start your Web Browser.
2. In the "Address" bar, enter "HTTP://" followed by the Internet IP Address of the Wireless Router. If the port number is not 80, the port number is also required. (After the IP Address, enter ":" followed by the port number.)
e.g.

HTTP://123.123.123.123:8080

This example assumes the WAN IP Address is 123.123.123.123, and the port number is 8080.

3. You will then be prompted for the login name and password for this device.

Routing

Overview

- If you don't have other Routers or Gateways on your LAN, you can ignore the "Routing" page completely.
- If the Wireless Router is only acting as a Gateway for the local LAN segment, ignore the "Routing" page even if your LAN has other Routers.
- If your LAN has a standard Router (e.g. Cisco) on your LAN, and the Wireless Router is to act as a Gateway for all LAN segments, enable RIP (Routing Information Protocol) and ignore the Static Routing table.
- If your LAN has other Gateways and Routers, and you wish to control which LAN segments use each Gateway, do NOT enable RIP (Routing Information Protocol). Configure the Static Routing table instead. (You also need to configure the other Routers.)
- If using Windows 2000 Data center Server as a software Router, enable RIP on the Wireless Router, and ensure the following Windows 2000 settings are correct:
 - Open *Routing and Remote Access*
 - In the console tree, select *Routing and Remote Access, [server name], IP Routing, RIP*
 - In the "Details" pane, right-click the interface you want to configure for RIP version 2, and then click "Properties".
 - On the "General" tab, set *Outgoing packet protocol* to "RIP version 2 broadcast", and *Incoming packet protocol* to "RIP version 1 and 2".

Routing Screen

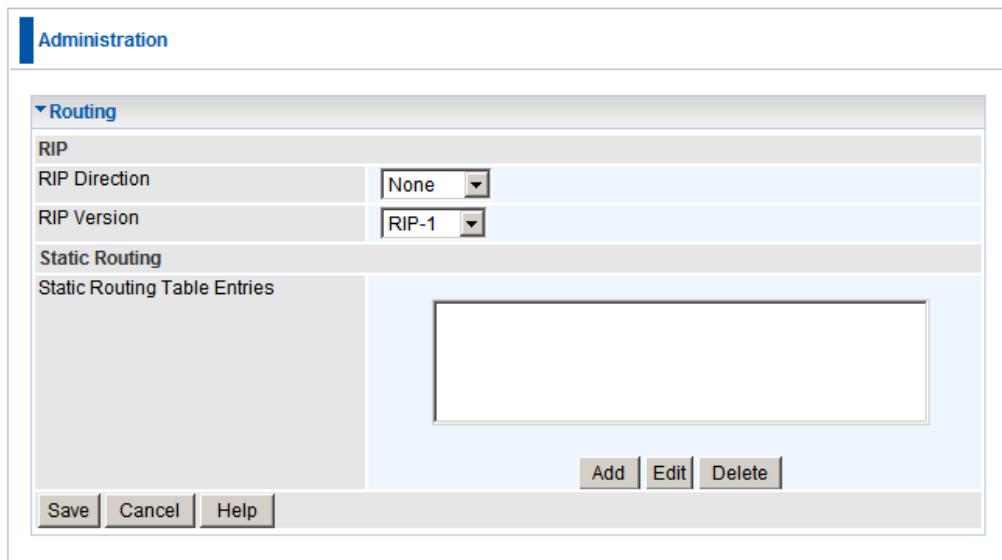
The routing table is accessed by the *Routing* link on the *Administration* menu.

Using this Screen

Generally, you will use either RIP (Routing Information Protocol) OR the Static Routing Table, as explained above, although it is possible to use both methods simultaneously.

Static Routing Table

- If RIP is not used, an entry in the routing table is required for each LAN segment on your Network, other than the segment to which this device is attached.
- The other Routers must also be configured. See *Configuring Other Routers on your LAN* later in this chapter for further details and an example.



Routing Screen

Data - Routing Screen

RIP	
RIP Direction	Select the desired RIP Direction.
RIP Version	Choose the RIP Version for the Server.
Static Routing	
Static Routing Table Entries	<p>This list shows all entries in the Routing Table.</p> <ul style="list-style-type: none"> This area shows details of the selected item in the list. Change any the properties as required, then click the "Edit" button to save the changes to the selected entry.
Buttons	
Add	Add a new entry to the Static Routing table, using the data shown in the "Properties" area on screen. The entry selected in the list is ignored, and has no effect.
Edit	Update the current Static Routing Table entry, using the data shown in the table area on screen.
Delete	Delete the current Static Routing Table entry.
Save	Save the RIP setting. This has no effect on the Static Routing Table.

Configuring Other Routers on your LAN

It is essential that all IP packets for devices not on the local LAN be passed to the Wireless Router, so that they can be forwarded to the external LAN, WAN, or Internet. To achieve this, the local LAN must be configured to use the Wireless Router as the *Default Route* or *Default Gateway*.

Local Router

The local router is the Router installed on the same LAN segment as the Wireless Router. This router requires that the *Default Route* is the Wireless Router itself. Typically, routers have a special entry for the *Default Route*. It should be configured as follows.

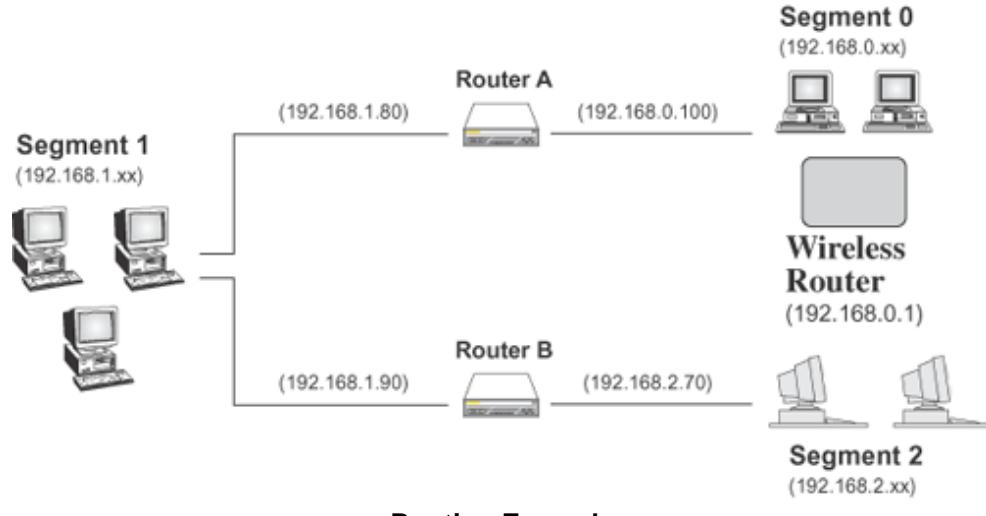
Destination IP Address	Normally 0.0.0.0, but check your router documentation.
Network Mask	Normally 0.0.0.0, but check your router documentation.
Gateway IP Address	The IP Address of the Wireless Router.
Metric	1

Other Routers on the Local LAN

Other routers on the local LAN must use the Wireless Router's *Local Router* as the *Default Route*. The entries will be the same as the Wireless Router's local router, with the exception of the *Gateway IP Address*.

- For a router with a direct connection to the Wireless Router's local Router, the *Gateway IP Address* is the address of the Wireless Router's local router.
- For routers which must forward packets to another router before reaching the Wireless Router's local router, the *Gateway IP Address* is the address of the intermediate router.

Static Routing - Example



For the Wireless Router's Routing Table

For the LAN shown above, with 2 routers and 3 LAN segments, the Wireless Router requires 2 entries as follows.

Entry 1 (Segment 1)	
Destination IP Address	192.168.1.0
Network Mask	255.255.255.0 (Standard Class C)
Gateway IP Address	192.168.0.100 (Wireless Router's local Router)
Metric	2
Entry 2 (Segment 2)	
Destination IP Address	192.168.2.0
Network Mask	255.255.255.0 (Standard Class C)
Gateway IP Address	192.168.0.100
Metric	3

For Router A's Default Route

Destination IP Address	0.0.0.0
Network Mask	0.0.0.0
Gateway IP Address	192.168.0.1 (Wireless Router's IP Address)

For Router B's Default Route

Destination IP Address	0.0.0.0
Network Mask	0.0.0.0
Gateway IP Address	192.168.1.80 (Wireless Router's local router)

Upgrade Firmware

The firmware (software) in the Wireless Router can be upgraded using your Web Browser.

You must first download the upgrade file (<http://www.level1.com>), then select *Upgrade Firmware* on the *Administration* menu. You will see a screen like the following.

The screenshot shows a web-based administration interface. At the top, a blue header bar contains the text "Administration". Below it, a sub-menu titled "Upgrade Firmware" is expanded. Inside this sub-menu, there is a text input field labeled "Locate and Select the Upgrade File from your Hard Disk:" followed by a "Browse..." button. At the bottom of the sub-menu are three buttons: "Upload", "Cancel", and "Help".

Router Upgrade Screen

To perform the Firmware Upgrade:

1. Click the *Browse* button and navigate to the location of the upgrade file.
2. Select the upgrade file. Its name will appear in the *Upgrade File* field.
3. Click the *Upload* button to commence the firmware upgrade.



The Wireless Router is unavailable during the upgrade process, and must restart when the upgrade is completed. Any connections to or through the Wireless Router will be lost.

Chapter 8

Access Point Mode

8

This Chapter explains configuration and operation when in "Access Point".

Overview

There are two modes available on the **Access Point** screen.

- **Router** - In this mode, this device can provide shared Internet Access to all your LAN users. Also, by default, it acts a DHCP Server, providing an IP address and related information to all Wireless and LAN users.
- **Access Point** - The device links your Wireless Stations to your wired LAN. The Wireless stations and devices on the wired LAN are then on the same network, and can communicate with each other without regard for whether they are connected to the network via a Wireless or wired connection.

This Chapter describes operation while in **Access Point Mode**.

Management Connections

- You need to have a DHCP Server on your LAN to provide IP addresses to the Wireless clients using this Access Point.
- This AP must be a valid device on your LAN, to allow management connections. You must assign a (fixed) IP address which is within the address range used on your LAN, but not within the address range used by your DHCP server.

When you connect in future, just connect normally, using the IP address you assigned.

1. Start your WEB browser.
2. In the Address box, enter "HTTP://" and the current IP Address of the Wireless Router, as in this example with the default IP Address:
HTTP://192.168.0.1
3. When prompted for the User name and Password, enter admin for the user name, and the current password, as set on the password screen.

Mode Screen

Configuration

Mode

Device Mode

Device Name: WBR-3408

Device Mode: Access Point

IP Address: 192 . 168 . 0 . 1

Subnet Mask: 255 . 255 . 255 . 0

Save Help

Mode Screen

Data - Mode Screen

Device Name	This field displays the current name of this device.
Device Mode	<p>Select the desired device mode for the router:</p> <ul style="list-style-type: none"> Router - In this mode, this device can provide shared Internet Access to all your LAN users. Also, by default, it acts a DHCP Server, providing an IP address and related information to all Wireless and LAN users. Access Point - The device links your Wireless Stations to your wired LAN. The Wireless stations and devices on the wired LAN are then on the same network, and can communicate with each other without regard for whether they are connected to the network via a Wireless or wired connection. <p>After changing the mode, this device will restart, which will take a few seconds. The menu will also change, depending on the mode you are in.</p>
IP Address	The IP Address of this device. Use the default value unless the address is already in use or your LAN is using a different IP address range.
Subnet Mask	The Network Mask associated with the IP Address above.

Operation

Operation is automatic.

- Wireless clients can connect to the Access Point if they have the correct SSID and security, but they must obtain an IP address from the DHCP Server on your LAN.

Note: To use Schedule functions in Access Point mode, please make sure your NTP settings are working under Router Mode.

Appendix A

Troubleshooting



This Appendix covers the most likely problems and their solutions.

Overview

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

General Problems

Problem 1: Can't connect to the Wireless Router to configure it.

Solution 1: Check the following:

- The Wireless Router is properly installed, LAN connections are OK, and it is powered ON.
- Ensure that your PC and the Wireless Router are on the same network segment. (If you don't have a router, this must be the case.)
- If your PC is set to "Obtain an IP Address automatically" (DHCP client), restart it.
- If your PC uses a Fixed (Static) IP address, ensure that it is using an IP Address within the range 192.168.0.2 to 192.168.0.254 and thus compatible with the Wireless Router's default IP Address of 192.168.0.1.

Also, the Network Mask should be set to 255.255.255.0 to match the Wireless Router.

In Windows, you can check these settings by using *Control Panel-Network* to check the *Properties* for the TCP/IP protocol.

Internet Access

Problem 1: When I enter a URL or IP address I get a time out error.

Solution 1: A number of things could be causing this. Try the following troubleshooting steps.

- Check if other PCs work. If they do, ensure that your PCs IP settings are correct. If using a Fixed (Static) IP Address, check the Network Mask, Default gateway and DNS as well as the IP Address.
- If the PCs are configured correctly, but still not working, check the Wireless Router. Ensure that it is connected and ON. Connect to it and check its settings. (If you can't connect to it, check the LAN and power connections.)
- Check the Wireless Router's status screen to see if it is working correctly.

Problem 2: Some applications do not run properly when using the Wireless Router.

Solution 2: The Wireless Router processes the data passing through it, so it is not transparent.

For incoming connections, you must use the Virtual Server or Firewall Rules to specify the PC which will receive the incoming traffic.

You can also use the *DMZ* function. This should work with almost every application, but:

- It is a security risk, since the firewall is disabled.
- Only one (1) PC can use this feature.

Wireless Access

Problem 1: My PC can't locate the Wireless Access Point.

Solution 1: Check the following.

- Your PC is set to *Infrastructure Mode*. (Access Points are always in *Infrastructure Mode*)
- The SSID on your PC and the Wireless Access Point are the same.
Remember that the SSID is case-sensitive. So, for example "Workgroup" does NOT match "workgroup".
- Both your PC and the Wireless Router must have the same setting for WEP. The default setting for the Wireless Router is disabled, so your wireless station should also have WEP disabled.
- If WEP is enabled on the Wireless Router, your PC must have WEP enabled, and the key must match.
- If the Wireless Router's *Wireless* screen is set to *Allow Trusted PCs only*, then each of your Wireless stations must have been designated as "Trusted", or the Wireless station will be blocked.
- To see if radio interference is causing a problem, see if connection is possible when close to the Wireless Router.
Remember that the connection range can be as little as 100 feet in poor environments.

Problem 2: Wireless connection speed is very slow.

Solution 2: The wireless system will connect at the highest possible speed, depending on the distance and the environment. To obtain the highest possible connection speed, you can experiment with the following:

- Wireless Router location
Try adjusting the location and orientation of the Wireless Router.
- Wireless Channel
If interference is the problem, changing to another channel may show a marked improvement.
- Radio Interference
Other devices may be causing interference. You can experiment by switching other devices Off, and see if this helps. Any "noisy" devices should be shielded or relocated.
- RF Shielding
Your environment may tend to block transmission between the wireless stations. This will mean high access speed is only possible when close to the Wireless Router.

Appendix B

About Wireless LANs



This Appendix provides some background information about using Wireless LANs (WLANs).

Modes

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

- Ad-hoc
- Infrastructure

Ad-hoc Mode

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

Infrastructure Mode

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



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

BSS/ESS

BSS

A group of Wireless Stations and a single Access Point, all using the same ID (SSID), form a Basic Service Set (BSS).

Using the same SSID is essential. Devices with different SSIDs are unable to communicate with each other.

ESS

A group of Wireless Stations, and multiple Access Points, all using the same ID (ESSID), form an Extended Service Set (ESS).

Different Access Points within an ESS can use different Channels. In fact, to reduce interference, it is recommended that adjacent Access Points SHOULD use different channels.

As Wireless Stations are physically moved through the area covered by an ESS, they will automatically change to the Access Point which has the least interference or best performance. This capability is called **Roaming**. (Access Points do not have or require Roaming capabilities.)

Channels

The Wireless Channel sets the radio frequency used for communication.

- Access Points use a fixed Channel. You can select the Channel used. This allows you to choose a Channel which provides the least interference and best performance. In the USA and Canada, 11 channels are available. If using multiple Access Points, it is better if adjacent Access Points use different Channels to reduce interference.
- In "Infrastructure" mode, Wireless Stations normally scan all Channels, looking for an Access Point. If more than one Access Point can be used, the one with the strongest signal is used. (This can only happen within an ESS.)
- If using "Ad-hoc" mode (no Access Point), all Wireless stations should be set to use the same Channel. However, most Wireless stations will still scan all Channels to see if there is an existing "Ad-hoc" group they can join.

WEP

WEP (Wired Equivalent Privacy) is a standard for encrypting data before it is transmitted.

This is desirable because it is impossible to prevent snoopers from receiving any data which is transmitted by your Wireless Stations. But if the data is encrypted, then it is meaningless unless the receiver can decrypt it.

If WEP is used, the Wireless Stations and the Access Point must have the same settings for each of the following:

WEP	Off, 64 Bit, 128 Bit
Key	For 64 Bit encryption, the Key value must match. For 128 Bit encryption, the Key value must match
WEP Authentication	Open System or Shared Key.

WPA-PSK

WPA-PSK is another standard for encrypting data before it is transmitted. This is a later standard than WEP (Wired Equivalent Privacy), and provides greater security for your data. Data is encrypted using a 256Bit key which is automatically generated and changed often.

If all your Wireless stations support WPA-PSK, you should use this instead of WEP.

If WPA-PSK is used, the Wireless Stations and the Access Point must have the same settings for each of the following:

WPA PSK (Pre-shared Key)	Enter the same value on every station and the AP. The PSK must be from 8 to 63 characters in length. The 256Bit key used for the actual encryption is derived from this key.
Encryption	The same encryption method must be used. The most common encryption method is TKIP. Another widely-supported method is AES.

WPA2-PSK

This is a later version of WPA (WPA-PSK). The major change is the use of AES (Advanced Encryption System) for protecting data. AES is very secure, considered to be unbreakable. The PSK (Pre-shared Key) must be entered on each Wireless station.

If WPA2-PSK is used, the Wireless Stations and the Access Point must have the same settings for each of the following:

WPA2 PSK (Pre-shared Key)	Enter the same value on every station and the AP. The PSK must be from 8 to 63 characters in length. The 256Bit key used for the actual encryption is derived from this key.
Encryption	The same encryption method must be used. The most common encryption method is TKIP. Another widely-supported method is AES.

WPA-802.1x

WPA-802.1x - This version of WPA requires a Radius Server on your LAN to provide the client authentication according to the 802.1x standard. Data transmissions are encrypted using the WPA standard.

If this option is used:

- The Access Point must have a "client login" on the Radius Server.
- Each user must have a "user login" on the Radius Server.
- Each user's wireless client must support 802.1x and provide the login data when required.
- All data transmission is encrypted using the WPA standard. Keys are automatically generated, so no key input is required.

Wireless LAN Configuration

To allow Wireless Stations to use the Access Point, the Wireless Stations and the Access Point must use the same settings, as follows:

Mode	On client Wireless Stations, the mode must be set to "Infrastructure". (The Access Point is always in "Infrastructure" mode.)
SSID (ESSID)	Wireless Stations should use the same SSID (ESSID) as the Access Point they wish to connect to. Alternatively, the SSID can be set to "any" or null (blank) to allow connection to any Access Point.
Wireless Security	The Wireless Stations and the Access Point must use the same settings for Wireless security. (None, WEP, WPA-PSK, WPA2-PSK, WPA-802.1x) <ul style="list-style-type: none">• If Wireless security remains disabled on the Wireless Router, all stations must have wireless security disabled.• If Wireless security is enabled on the Wireless Router, each station must use the same settings as the Wireless ADLS Router.

Appendix C

Specifications



Multi-Function Wireless Router

Model	WBR-3408 – 11g Wireless Broadband Router WBR-3408 – Roteador banda-larga sem fio - Wireless G
Dimensions	125mm(W) * 109mm(D) * 30mm(H)
Operating Temperature	0° C to 40° C
Storage Temperature	-20° C to 70° C
Network Protocol:	TCP/IP
Network Interface:	4 * 10/100BaseT (RJ45) LAN connection 1 * RJ-45 for ADSL/Broadband Modem
LEDs	6
Power Adapter	12 V DC / 1.0A External

Wireless Interface

Standards	IEEE802.11b, IEEE802.11g WLAN
Frequency	2.4 to 2.485GHz
Channels	Maximum 13 Channels, depending on regulatory authorities
Modulation	CCK, DQPSK, DBPSK, BPSK, QPSK, 16-QAM, 64-QAM, OFDM
Security	WEP 64/128Bit, WPA-PSK, WPA2-PSK, WPA-802.1x, MAC address filtering, WPS button support
Antenna power	1.8dBi
Antenna type	External, Removable RP-SMA