



# LevelOne

## **WBR-3460**

11g Wireless ADSL2/2+ Modem Router

1WAN 4LAN, QoS, VPN

## **User Manual**

V1.0.0-0608

# Table of Contents

---

<b>CHAPTER 1 INTRODUCTION .....</b>	<b>4</b>
Wireless ADSL2/2+ Modem Router Features .....	4
Package Contents.....	7
Physical Details.....	8
<b>CHAPTER 2 INSTALLATION .....</b>	<b>10</b>
Requirements.....	10
Procedure .....	10
<b>CHAPTER 3 SETUP.....</b>	<b>12</b>
Overview.....	12
Configuration Program .....	13
Setup Wizard .....	14
Configuring VC2, VC3 and VC4 .....	17
Home Screen .....	19
LAN Screen.....	20
Wireless Screen .....	22
Wireless Security.....	25
Trusted Wireless Stations.....	27
Password Screen.....	29
Mode Screen .....	30
<b>CHAPTER 4 PC CONFIGURATION .....</b>	<b>31</b>
Overview .....	31
Windows Clients.....	31
Macintosh Clients.....	39
Linux Clients .....	39
Other Unix Systems.....	39
Wireless Station Configuration .....	40
Wireless Configuration on Windows XP .....	40
<b>CHAPTER 5 OPERATION AND STATUS .....</b>	<b>50</b>
Operation - Router Mode .....	50
Status Screen.....	50
Connection Status - PPPoE & PPPoA .....	54
Connection Details - Dynamic IP Address .....	55
Connection Details - Fixed IP Address.....	57
<b>CHAPTER 6 ADVANCED FEATURES .....</b>	<b>58</b>
Overview.....	58
Internet.....	58
Dynamic DNS (Domain Name Server).....	63
Firewall Rules.....	65
User-defined Services .....	70
Options .....	72
Schedule.....	73
Virtual Servers .....	75
VPN Setup .....	78
<b>CHAPTER 7 ADVANCED ADMINISTRATION .....</b>	<b>88</b>
Overview.....	88
PC Database.....	89
Config File .....	93
Logs .....	94
E-mail .....	96

- Diagnostics ..... 98
- Qos ..... 99
- Remote Administration ..... 101
- Routing ..... 103
- Upgrade Firmware ..... 107
- CHAPTER 8 MODEM MODE ..... 108
  - Overview ..... 108
  - Management Connections ..... 108
  - Home Screen ..... 109
  - Mode Screen ..... 110
  - Operation ..... 110
  - Status Screen ..... 111
- APPENDIX A TROUBLESHOOTING ..... 113
  - Overview ..... 113
  - General Problems ..... 113
  - Internet Access ..... 113
  - Wireless Access..... 114
- APPENDIX B ABOUT WIRELESS LANS ..... 116
  - Modes ..... 116
  - BSS/ESS ..... 116
  - Channels..... 117
  - WEP ..... 117
  - WPA-PSK ..... 117
  - Wireless LAN Configuration ..... 118
- APPENDIX C ABOUT VPNS..... 119
  - Overview ..... 119
  - Common VPN Situations ..... 121
  - VPN Example..... 122
- APPENDIX D SPECIFICATIONS ..... 126
  - Multi-Function Wireless ADSL2/2+ Modem Router ..... 126
  - Wireless Interface ..... 126
  - Regulatory Approvals..... 127

# Chapter 1

## Introduction

*This Chapter provides an overview of the Wireless ADSL2/2+ Router's features and capabilities.*

Congratulations on the purchase of your new Wireless ADSL2/2+ Modem Router. The Wireless ADSL2/2+ Modem Router is a multi-function device providing the following services:

- **ADSL2/2+ Modem.**
- **Shared Broadband Internet Access** for all LAN users.
- **Wireless Access Point** for 802.11b and 802.11g Wireless Stations.
- **VPN Gateway** to allow secure VPN connections over the Internet.
- **4-Port Switching Hub** for 10BaseT or 100BaseT connections.



Figure 1: Wireless ADSL2/2+ Modem Router

## Wireless ADSL2/2+ Modem Router Features

The Wireless ADSL2/2+ Modem 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 ADSL2/2+ Modem 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).
- **Built-in ADSL2/2+ Modem.** The Wireless ADSL2/2+ Modem Router has a built-in ADSL2/2+ modem, supporting all common ADSL connections.
- **IPoA, PPPoE, PPPoA, Direct Connection Support.** The Wireless ADSL2/2+ Modem Router supports all common connection methods.
- **Auto-detection of Internet Connection Method.** In most situations, the Wireless ADSL2/2+ Modem Router can test your ADSL and Internet connection to determine the connection method used by your ISP.

- **Fixed or Dynamic IP Address.** On the Internet (ADSL port) connection, the Wireless ADSL2/2+ Modem 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.
- **Special Applications.** This feature, also called Port Triggering, allows you to use Internet applications which normally do not function when used behind a firewall.
- **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.
- **Firewall.** As well as the built-in firewall to protect your LAN, you can define Firewall Rules to determine which incoming and outgoing traffic should be permitted.
- **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.
- **VPN Pass through Support.** PCs with VPN (Virtual Private Networking) software using PPTP, L2TP and IPSec are transparently supported - no configuration is required.

## VPN Features

- **IPSec Support.** IPSec is the most common protocol.
- **Easy Configuration.** The configuration required to allow 2 Wireless ADSL2/2+ Modem Routers to establish a VPN connection between them is easy accomplished.

## Wireless Features

- **Standards Compliant.** The Wireless ADSL2/2+ Modem Router complies with the IEEE802.11g (DSSS) specifications for Wireless LANs.
- **Supports both 802.11b and 802.11g Wireless Stations.** The 802.11g standard provides for backward compatibility with the 802.11b standard, so both 802.11b and 802.11g Wireless stations can be used simultaneously.
- **Speeds to 54Mbps.** All speeds up to the 802.11g maximum of 54Mbps are supported.
- **WEP support.** Support for WEP (Wired Equivalent Privacy) is included. Key sizes of 64 Bit and 128 Bit are supported. 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.
- **Wireless MAC Access Control.** The Wireless Access Control feature can check the MAC address (hardware address) of Wireless stations to ensure that only trusted Wireless Stations can access your LAN.
- **Simple Configuration.** If the default settings are unsuitable, they can be changed quickly and easily.

## LAN Features

- **4-Port Switching Hub.** The Wireless ADSL2/2+ Modem 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 ADSL2/2+ Modem 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 ADSL2/2+ Modem Router to your PC, and restore (upload) a previously-saved configuration file to the Wireless ADSL2/2+ Modem Router.
- **Remote Management.** The Wireless ADSL2/2+ Modem 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 ADSL2/2+ Modem Router to perform a *Ping* or *DNS lookup*.

## 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 ADSL2/2+ Modem 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 ADSL2/2+ Modem 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-3460A/B
- Power Adapter
- Cat-5 Ethernet (LAN) cable (Yellow Color)
- RJ-11 (ADSL) cable (Gray Color)
- RJ-11 to RJ45 cable (WBR-3460B Only/Gray Color)
- Quick Installation Guide
- CD Manual

## Physical Details

### Front-mounted LEDs

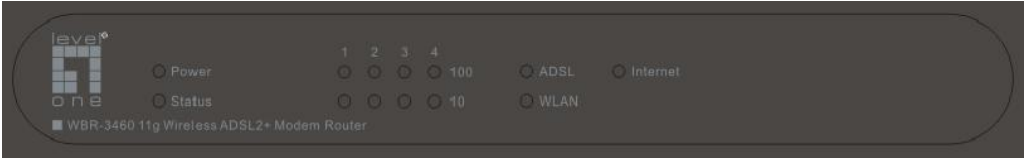
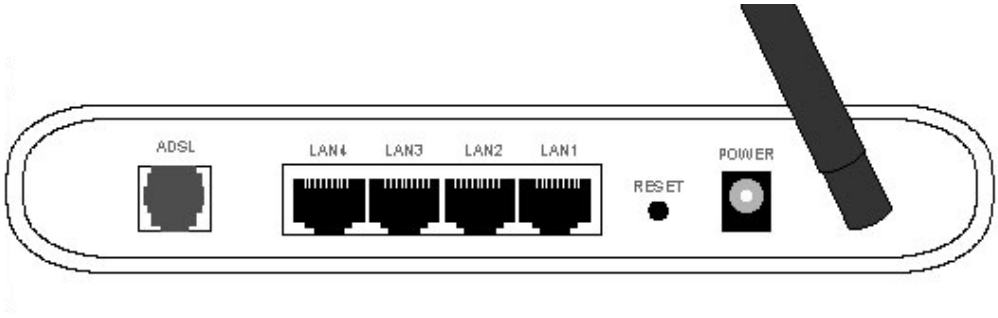


Figure 2: Front Panel

<b>Power LED (Green)</b>	<b>On</b> - Power on. <b>Off</b> - No power.
<b>Status LED (Yellow)</b>	<b>Off</b> - Normal operation. <b>Blinking</b> - This LED blinks during start up, and during a Firmware Upgrade.
<b>LAN</b>	For each port, there are 2 LEDs, to indicate the connection speed (10BaseT or 100BaseT) of each port. <ul style="list-style-type: none"><li>• <b>100</b> - This will be ON if the LAN connection is using 100BaseT, and Blinking if data is being transferred via the corresponding LAN port.</li><li>• <b>10</b> - This will be ON if the LAN connection is using 10BaseT, and Blinking if data is being transferred via the corresponding LAN port.</li><li>• If neither LED is on, there is no active connection on the corresponding LAN port.</li></ul>
<b>ADSL</b>	<b>On</b> - ADSL connection established. <b>Off</b> - No ADSL connection currently exists. <b>Flashing</b> – ADSL is synchronizing.
<b>WLAN</b>	<b>On</b> - Wireless enabled. <b>Off</b> - No Wireless connections currently exist. <b>Flashing</b> - Data is being transmitted or received via the Wireless access point. This includes "network traffic" as well as user data.
<b>Internet</b>	<b>On</b> - Internet connection is available. <b>Off</b> - No Internet connection available. <b>Flashing</b> - Data is being transmitted or received via the ADSL connection.

## Rear Panel



**Figure 3: Rear Panel**

<b>ADSL port</b>	Connect this port to your ADSL line.
<b>10/100BaseT LAN connections</b>	<p>Use standard LAN cables (RJ45 connectors) to connect your PCs to these ports.</p> <p><b>Note:</b></p> <p>Any LAN port on the Wireless ADSL2/2+ Modem Router will automatically function as an "Uplink" port when required. Just connect any port to a normal port on the other hub, using a standard LAN cable.</p>
<b>Reset Button (Reset to Defaults)</b>	<p>This button will reset the Wireless ADSL2/2+ Modem Router to the factory default settings.</p> <p>To do this, press and hold the Reset Button for five (5) seconds, until the Status LED is lit, then release the Reset Button, and wait the Wireless ADSL2/2+ Modem Router to restart using the factory default values.</p>
<b>Power port</b>	Connect the supplied power adapter here.

# Chapter 2

## Installation

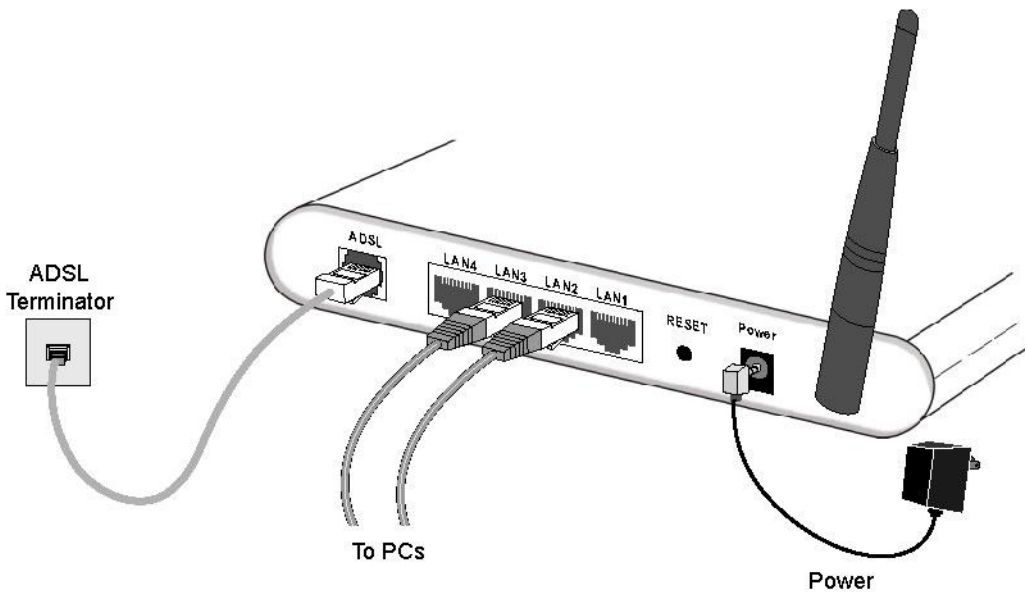
# 2

*This Chapter covers the physical installation of the Wireless ADSL2/2+ Modem 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



**Figure 4: Installation Diagram**

#### 1. Choose an Installation Site

Select a suitable place on the network to install the Wireless ADSL2/2+ Modem Router.



**Note!**

**For best Wireless reception and performance, the Wireless ADSL2/2+ Modem Router should be positioned in a central location with minimum obstructions between the Wireless ADSL2/2+ Modem Router and the PCs.**

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

## 2. Connect LAN Cables

Use standard LAN cables to connect PCs to the Switching Hub ports on the Wireless ADSL2/2+ Modem Router. Both 10BaseT and 100BaseT connections can be used simultaneously.

If required, connect any port to a normal port on another Hub, using a standard LAN cable. Any LAN port on the Wireless ADSL2/2+ Modem Router will automatically function as an "Uplink" port when required.

## 3. Connect ADSL Cable

Connect the supplied ADSL cable from to the ADSL port on the Wireless ADSL2/2+ Modem Router (the RJ11 connector) to the ADSL terminator provided by your phone company.

## 4. Power Up

Connect the supplied power adapter to the Wireless ADSL2/2+ Modem 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 *Status* LED should flash, and then turn Off. If it stays on or blinking after 60 seconds, there is a hardware error.
- For each LAN (PC) connection, one of the LAN LEDs should be ON (provided the PC is also ON.)
- The *WLAN* LED should be ON
- The *ADSL* LED should be ON if ADSL line is connected.
- The *Internet* LED may be OFF. After configuration, it should come ON.

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

# Chapter 3

## Setup



*This Chapter provides Setup details of the Wireless ADSL2/2+ Modem 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 ADSL2/2+ Modem 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 ADSL2/2+ Modem Router operation and Status.	Chapter 5: Operation and Status
Use any of the following Advanced features: <ul style="list-style-type: none"><li>• Internet (DMZ, Special Applications, URL Filter)</li><li>• Dynamic DNS</li><li>• Firewall Rules</li><li>• Firewall Services</li><li>• Schedule</li><li>• Virtual Servers</li><li>• VPN</li></ul>	Chapter 6: Advanced Features
Use any of the following Administration Configuration settings or features: <ul style="list-style-type: none"><li>• PC Database</li><li>• Config File</li><li>• Logging</li><li>• E-mail</li><li>• Diagnostics</li><li>• Remote Admin</li><li>• Routing</li><li>• Upgrade Firmware</li></ul>	Chapter 7 Advanced Administration

## Configuration Program

The Wireless ADSL2/2+ Modem Router contains an HTTP server. This enables you to connect to it, and configure it, using your Web Browser. **Your Browser must support JavaScript.**

The configuration program has been tested on the following browsers:

- Netscape 7.1 or later.
- Mozilla 1.6 or later
- Internet Explorer V5.5 or later

## Preparation

Before attempting to configure the Wireless ADSL2/2+ Modem Router, please ensure that:

- Your PC can establish a physical connection to the Wireless ADSL2/2+ Modem Router. The PC and the Wireless ADSL2/2+ Modem Router must be directly connected (using the Hub ports on the Wireless ADSL2/2+ Modem Router) or on the same LAN segment.
- The Wireless ADSL2/2+ Modem Router must be installed and powered ON.
- If the Wireless ADSL2/2+ Modem 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 ADSL2/2+ Modem Router is allocated a new IP Address during configuration.

## Using your Web Browser

To establish a connection from your PC to the Wireless ADSL2/2+ Modem Router:

1. After installing the Wireless ADSL2/2+ Modem 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 ADSL2/2+ Modem Router, as in this example, which uses the Wireless ADSL2/2+ Modem 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

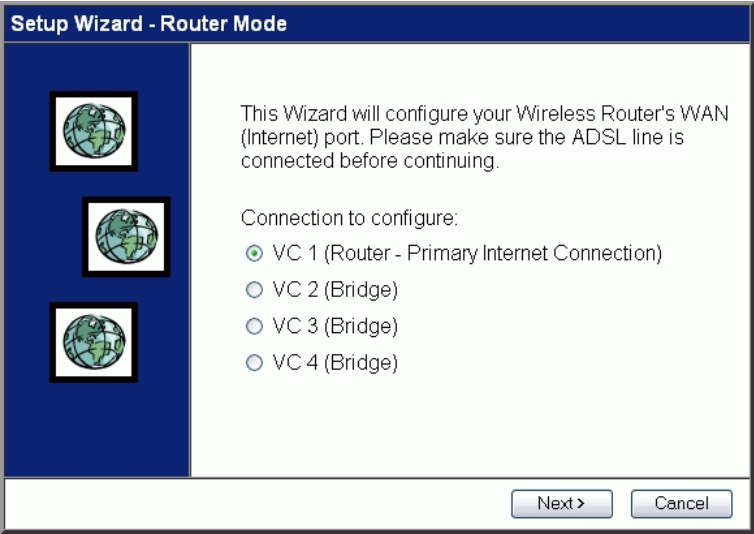
If the Wireless ADSL2/2+ Modem Router does not respond, check the following:

- The Wireless ADSL2/2+ Modem 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 192.168.0.1  
If no response is received, either the connection is not working, or your PC's IP address is not compatible with the Wireless ADSL2/2+ Modem 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 ADSL2/2+ Modem 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 ADSL2/2+ Modem 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

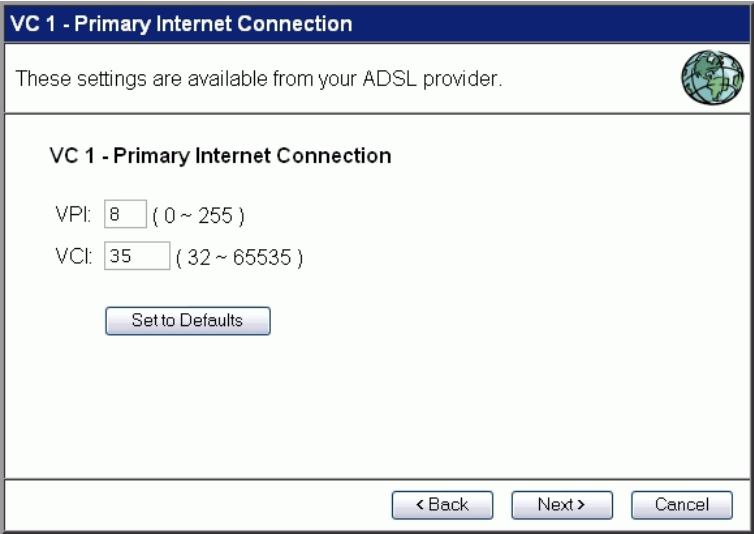
The first time you connect to the Wireless ADSL2/2+ Modem Router, you should run the **Setup Wizard** to configure the ADSL and Internet Connection.

1. Click the **Setup Wizard** link on the main menu
2. On the first screen, select *VC 1 (Router - Primary Internet Connection)*, then click "Next"



**Figure 5: Setup Wizard Home Page**

3. On the VC1 screen, shown below, enter the VPI and VCI values provided by your ISP, then click "Next".



**Figure 6: Setup Wizard - VC1**

**Setup Wizard - Internet Access**

Check the data provided by your ISP.

**Connection Method**

If your ISP requires a User Name and Password for Internet Access, select "Login". Otherwise, select "No Login".

☒ Login: PPPoE

☐ No Login: IP over ATM (RFC1577 or RFC1483)

DSL Multiplexing Method: VC-BASED

< Back   Next >   Cancel

**Figure 7: Setup Wizard - Internet Access**

4. On the Internet Access Screen, shown above, select the correct connection type, as used by your ISP. Click "Next" and complete the configuration for your connection method.
- You need the data supplied by your ISP. Your ISP's data will also have the *DSL Multiplexing Method* ( LLC or VC )
  - The common connection types are explained in the following table..

Connection Type	Details	ISP Data required
Dynamic IP Address	Your IP Address is allocated automatically, when you connect to you ISP.	Often, none.  Some ISP's may require you to use a particular <i>Hostname</i> or <i>Domain</i> name, or MAC (physical) address.
Static (Fixed) IP Address	Your ISP allocates a permanent IP Address to you. Usually, the connection is "Always on".	IP Address allocated to you, and related information, such as Network Mask, Gateway IP address, and DNS address.
PPPoE, PPPoA	You connect to the ISP only when required. The IP address is usually allocated automatically.	a) User name and password are always required.  b) If using a Static (Fixed) IP address, you need the IP address and related information (Network Mask, Gateway IP address, and DNS address)
IPoA (IP over ATM)	Normally, the connection is "Always on".	IP Address allocated to you, and related information, such as Network Mask, Gateway IP address, and DNS address.

5. Step through the Wizard until finished.

6. On the final screen of the Wizard, run the test and check that an Internet connection can be established.
7. If the connection test fails:
  - Check all connections, and the front panel LEDs.
  - Check that you have entered all data correctly.

## Configuring VC2, VC3 and VC4

The Wireless ADSL2/2+ Modem Router supports multiple VCs (Virtual Circuits) on the ADSL connection.

VC1 must be used for general-purpose Internet access. The other VCs (VC2, VC3 and VC4) are available for special purposes, such as Video-on-Demand.

You can only use these VCs if supported by your ISP and ADSL service provider. In that case, they will provide the necessary configuration data.



**Some ISP's allow multiple PPPoE connections. This allows multiple PCs to connect to the Internet using PPPoE client software. When using the Wireless ADSL2/2+ Modem Router, multiple PPPoE connections are neither necessary nor supported.**

### To Configure additional VCs

1. Start the *Setup Wizard* again.
2. On the first screen, select VC2, and click "Next"
3. Configure the VC setup screen as described below, then click "Next".

**Setup Wizard - Bridge Mode VC**

Check the data from your ADSL provider and ISP.

**VC 2**

☐ Enable this VC

VPI:  ( 0 ~ 255 )

VCI:  ( 32 ~ 65535 )

Multiplexing:  ▼

ATM Service:  ▼

LAN IP address:  .  .  .

< Back   Next >   Cancel

**Figure 8: Setup Wizard - VC2**

### Setup Wizard VC Screen

<b>VC</b>	The VC number is displayed (VC2, VC3, or VC4)
<b>Enable</b>	To use this VC, you must enable it by checking this checkbox.
<b>VPI</b>	Enter the VPI value provided by your ISP.
<b>VCI</b>	Enter the VPI value provided by your ISP.
<b>Multiplexing</b>	Select the multiplexing value provided by your ISP.
<b>ATM Service</b>	Select the multiplexing value provided by your ISP.
<b>IP Address</b>	<p>Enter the IP address of the device on your LAN which will receive the data on this VC.</p> <ul style="list-style-type: none"><li>• For Video-on-Demand, this would be the IP address of your SetTop Box.</li><li>• For VoIP, this would be the IP address of your VoIP TA.</li><li>• Note that this IP address does not have to be in the same IP address range as other devices on your local LAN.</li></ul>

4. When finished, click "Next" and complete the Wizard.
5. After completing the Wizard, you can check the Status screen to see the VC has been corrected established.

## 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.



Figure 9: 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"

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 ADSL2/2+ Modem 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.

The screenshot shows a blue-themed LAN configuration interface. At the top center is a large yellow circle with a white 'L' and the letters 'AN' in white, forming the 'LAN' logo. Below the logo, the text 'TCP/IP' is highlighted in yellow. The configuration fields are as follows: IP Address (192, 168, 0, 1), Subnet Mask (255, 255, 255, 0), a checked checkbox for 'DHCP Server', Start IP Address (192, 168, 0, 2), and Finish IP Address (192, 168, 0, 254). At the bottom right, there are three buttons: 'Save', 'Cancel', and 'Help'.

Figure 10: LAN Screen

Data - LAN Screen

TCP/IP	
IP Address	IP address for the Wireless ADSL2/2+ Modem 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 ADSL2/2+ Modem Router is attached (the same value as the PCs on that LAN segment).
DHCP Server	<ul style="list-style-type: none"><li>• If Enabled, the Wireless ADSL2/2+ Modem Router will allocate IP Addresses to PCs (DHCP clients) on your LAN when they start up. The default (and recommended) value is Enabled.</li><li>• 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 ADSL2/2+ Modem Router as the default Gateway. See the following section for further details.</li><li>• The <b>Start IP Address</b> and <b>Finish IP Address</b> 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.</li></ul> See the following section for further details on using DHCP.

## 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 ADSL2/2+ Modem 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 ADSL2/2+ Modem 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 ADSL2/2+ Modem 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 ADSL2/2+ Modem Router's, the following procedure is required.

- Disable the DHCP Server feature in the Wireless ADSL2/2+ Modem Router. This setting is on the LAN screen.
- Configure the DHCP Server to provide the Wireless ADSL2/2+ Modem 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.

# Wireless Screen

The Wireless ADSL2/2+ Modem Router's settings must match the other Wireless stations.

Note that the Wireless ADSL2/2+ Modem Router will automatically accept both 802.11b and 802.11g connections, and no configuration is required for this feature.

To change the Wireless ADSL2/2+ Modem Router's default settings for the Wireless Access Point feature, use the *Wireless* link on the main menu to reach the **Wireless** screen. An example screen is shown below.

**Wireless**

**Identification** Region: Europe  
Station Name: WBR-3460A  
SSID (Service Set Identifier): Wireless

**Options** 802.11 Mode: 802.11g & 802.11b  
Channel No: 03  
☒ Broadcast SSID

**Wireless Security** Current Setting: Disabled  
Configure

**Access Point** ☒ Enable Wireless Access Point  
Allow access by:  
☒ ALL Wireless stations  
☐ Trusted Wireless stations only  
Set Stations

Save Cancel Help

Figure 11: Wireless Screen

## Data - Wireless Screen

Identification	
Region	Select the correct domain for your location. It is your responsibility to ensure: <ul style="list-style-type: none"><li>That the Wireless ADSL2/2+ Modem Router is only used in domains for which is licensed.</li><li>That you select the correct domain, so that only the legal channels for that domain can be selected.</li></ul>
Station name	This is the same as the "Device Name" for the Wireless ADSL2/2+ Modem Router.

<b>SSID</b>	<p>This is also called the "Network Name".</p> <ul style="list-style-type: none"> <li>• If using an ESS (Extended Service Set, with multiple access points) this ID is called an ESSID (Extended Service Set Identifier).</li> <li>• To communicate, all Wireless stations should use the same SSID/ESSID.</li> </ul>
<b>Options</b>	
<b>Mode</b>	<p>Select the desired mode:</p> <ul style="list-style-type: none"> <li>• <b>802.11G-plus (TI)</b> This allows clients to use any of the following modes: <ul style="list-style-type: none"> <li>• Standard 802.11b</li> <li>• 802.11B+ (Texas Instruments proprietary enhanced mode)</li> <li>• Standard 802.11g</li> <li>• 802.11G-plus (Texas Instruments proprietary enhanced mode). This mode can increase throughput by up to 50%, but will only work between compatible TI wireless stations.</li> </ul> </li> <li>• <b>802.11g &amp; 802.11b</b> - Both 802.11.g and 802.11b Wireless stations will be able to use the Wireless ADSL2/2+ Modem Router.</li> <li>• <b>802.11g only</b> - Only 802.11g Wireless stations can use the Wireless ADSL2/2+ Modem Router.</li> <li>• <b>802.11b only</b> - Only 802.11b connections are available. 802.11g Wireless Stations will only be able to use the Wireless ADSL2/2+ Modem Router if they are fully backward-compatible with the 802.11b standard.</li> </ul>
<b>Channel No.</b>	<p>Select the Channel you wish to use on your Wireless LAN.</p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• If using multiple Access Points, adjacent Access Points should use different Channels to reduce interference.</li> </ul>
<b>Broadcast SSID</b>	<p>If enabled, the Wireless ADSL2/2+ Modem Router will broadcast its SSID. This allows PCs and other wireless stations to detect this Access Point and use the correct SSID.</p> <p>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.</p>
<b>Wireless Security</b>	
<b>Current Setting</b>	<p>The current Wireless security is displayed. The default value is Disabled.</p>
<b>Configure Button</b>	<p>Click this button to access the Wireless security sub-screen, and view or change the settings. See the following section for details.</p>

Access Point	
<b>Enable Wireless Access Point</b>	<p>Enable this if you want to use Wireless Access Point function.</p> <p>If disabled, no Wireless stations can use the Access Point function, and all connections must be made via the wired LAN.</p>
<b>Allow access by ...</b>	<p>Use this feature to determine which Wireless stations can use the Access Point. The options are:</p> <ul style="list-style-type: none"><li>• <b>All Wireless Stations</b> - All wireless stations can use the access point, provided they have the correct SSID and security settings.</li><li>• <b>Trusted Wireless stations only</b> - 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.</li></ul>
<b>Set Stations Button</b>	<p>Click this button to manage the trusted PC database.</p>

# Wireless Security

This screen is accessed by clicking the "Configure" button on the *Wireless* screen. There are 3 options for Wireless security:

- **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.

## WEP Wireless Security

Wireless Security

Security System

WEP

Authentication Type:

Automatic

WEP Data Encryption:

64 bit (10 Hex chars)

Key 1:

☒

Key 2:

☐

Key 3:

☐

Key 4:

☐

Passphrase:

Generate Keys

Save

Cancel

Help

Close

Figure 12: WEP

## Data - WEP Screen

WEP Data Encryption	
WEP Data Encryption	<div>Select the desired option, and ensure the Wireless Stations use the same setting.<ul style="list-style-type: none"><li>• <b>64 Bit</b> - 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).</li><li>• <b>128 Bit</b> - 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).</li></ul></div>
Authentication Type	<div>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.</div>
Default Key	<div>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.</div>

	You must enter a <b>Key Value</b> for the <b>Default Key</b> .
<b>Key Value</b>	Enter the key value or values you wish to use. The <b>Default Key</b> is required, the other keys are optional. Other stations must have the same key.
<b>Passphrase</b>	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

The screenshot shows a window titled "Wireless Security". Inside, the "Security System" is set to "WPA-PSK" via a dropdown menu. Below this, there is a text input field for "PSK :". The "Encryption" is set to "TKIP" via another dropdown menu. At the bottom right, there are four buttons: "Save", "Cancel", "Help", and "Close".

Figure 13: WPA-PSK

### Data - WPA-PSK Screen

<b>Security System</b>	<b>WPA-PSK</b> 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.
<b>PSK</b>	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.
<b>WPA Encryption</b>	The WPA-PSK standard allows different encryption methods to be used. Select the desired option. Wireless Stations must use the same encryption method.

# 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.

To change the list of trusted wireless stations, use the *Modify List* button on the *Access Control* screen. You will see a screen like the sample below.

Trusted Wireless Stations

Other Wireless Stations

<<

>>

Edit

Name:

Address:  (Physical/MAC address)

Add

Clear

Help

Close

Figure 14: 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	
<<	<div>Add a Trusted Wireless Station to the list (move from the "Other Stations" list).</div> <ul style="list-style-type: none"><li>Select an entry (or entries) in the "Other Stations" list, and click the "&lt;&lt;" button.</li><li>Enter the Address (MAC or physical address) of the wireless station, and click the "Add" button.</li></ul>
>>	<div>Delete a Trusted Wireless Station from the list (move to the "Other Stations" list).</div> <ul style="list-style-type: none"><li>Select an entry (or entries) in the "Trusted Stations" list.</li><li>Click the "&gt;&gt;" button.</li></ul>

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

# Password Screen

The password screen allows you to assign a password to the Wireless ADSL2/2+ Modem Router.


A blue-themed web interface for setting a password. At the top is a large yellow circle with a white 'P' followed by the word 'assword' in white. Below this, the word 'Password' is in yellow, followed by a paragraph explaining that the password protects configuration data and will be prompted for upon connection. There are three white input fields labeled 'Old Password', 'New password:', and 'Verify password:'. At the bottom right are three buttons: 'Save', 'Cancel', and 'Help'.

Figure 15: 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.

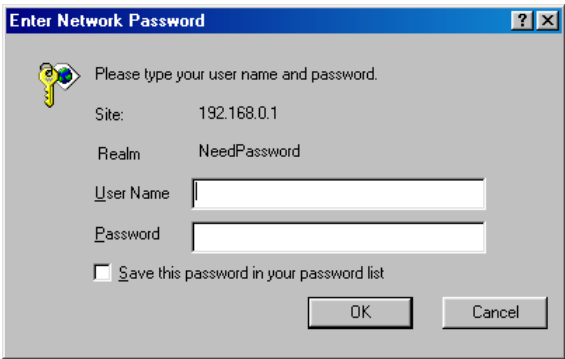
A standard Windows-style dialog box titled 'Enter Network Password'. It contains a key icon and the text 'Please type your user name and password.' Below this are labels for 'Site:' (192.168.0.1) and 'Realm:' (NeedPassword). There are two input fields, one for 'User Name' and one for 'Password'. At the bottom is a checkbox labeled 'Save this password in your password list' which is unchecked. 'OK' and 'Cancel' buttons are at the bottom right.

Figure 16: Password Dialog

- The "User Name" is always admin
- Enter the password for the Wireless ADSL2/2+ Modem Router, as set on the *Password* screen above.

## Mode Screen

Use this screen to change the mode between Router mode and Modem (Bridge) mode.



**Figure 17: Mode Screen**

Select the desired option, and click "Save".

<b>Device Name</b>	This field displays the current name of this device.
<b>Device Mode</b>	<p>Only the ADSL Modem component is operational.</p> <ul style="list-style-type: none"><li>• Router - Both the ADSL Modem and the Router features are operational. 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.</li><li>• Modem - Only the ADSL Modem component is operational. All Router features are disabled. This device is "transparent" - it does not perform any operations or make any changes to the network traffic passing through it. You need to have a DHCP Server on your LAN to provide IP addresses to the Wireless clients using this Access Point.</li></ul> <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>
<b>Language</b>	Select the desired option from the drop-down list.

### Notes:

- Generally, you should NOT use modem 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.
- The Wireless Access Point can function in either Router or Modem mode. But generally it is not a good idea to combine a Modem with an Access Point, because all data received from the wireless stations will be sent over the modem connection. (Since the modem is transparent, it does not examine the traffic to determine whether the traffic is for the LAN or the WAN.)
- For details on using Modem Mode, see Chapter 8.

# 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 ADSL2/2+ Modem Router.

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

The Wireless ADSL2/2+ Modem 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 ADSL2/2+ Modem Router settings, and the default Windows TCP/IP settings, no changes need to be made.**

- By default, the Wireless ADSL2/2+ Modem 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:**

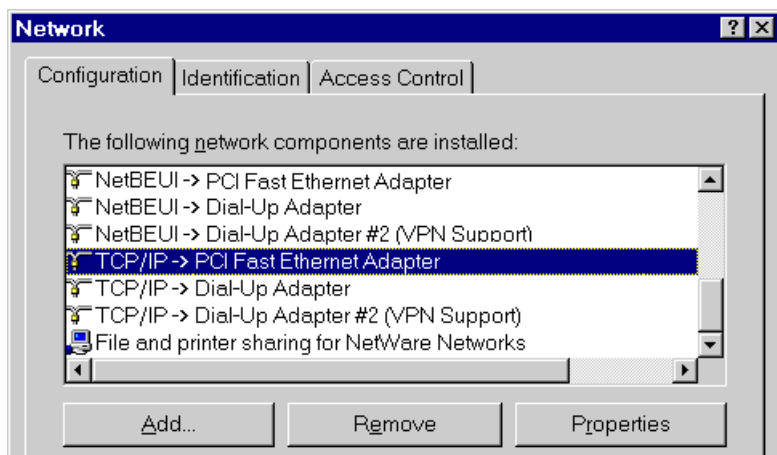
- The *Gateway* must be set to the IP address of the Wireless ADSL2/2+ Modem Router
- The *DNS* should be set to the address provided by your ISP.



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

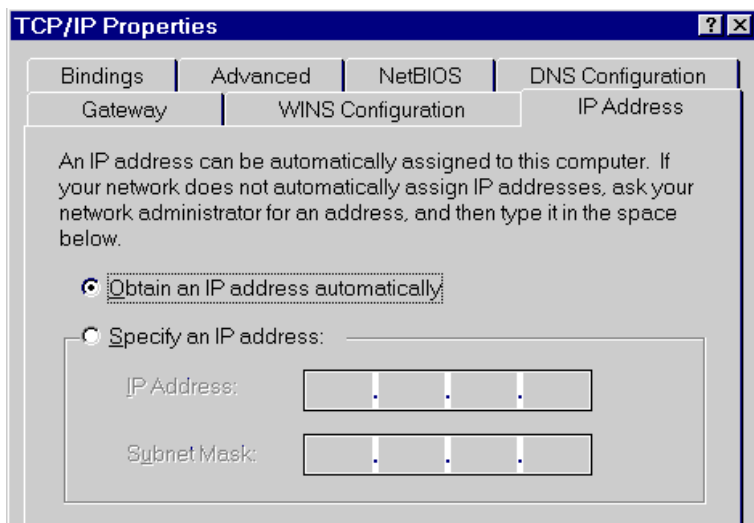
## Checking TCP/IP Settings - Windows 9x/ME:

1. Select *Control Panel - Network*. You should see a screen like the following:



**Figure 18: Network Configuration**

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



**Figure 19: IP Address (Win 98SE)**

Ensure your TCP/IP settings are correct, as follows:

### 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 ADSL2/2+ Modem Router will act as a DHCP Server.

Restart your PC to ensure it obtains an IP Address from the Wireless ADSL2/2+ Modem Router.

### Using "Specify an IP Address"

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

- On the *Gateway* tab, enter the Wireless ADSL2/2+ Modem Router's IP address in the *New Gateway* field and click *Add*, as shown below. Your LAN administrator can advise you of the IP Address they assigned to the Wireless ADSL2/2+ Modem Router.

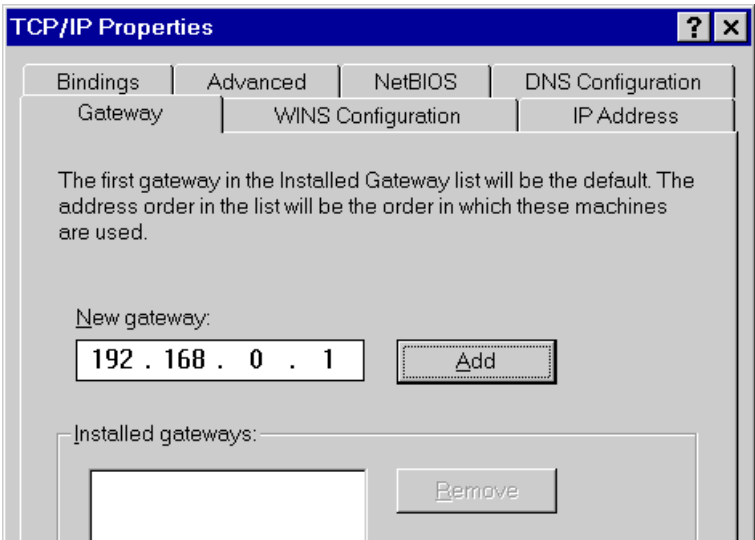


Figure 20: Gateway Tab (Win 98SE/ME)

- On the *DNS Configuration* tab, ensure *Enable DNS* is selected. If the *DNS Server Search Order* list is empty, enter the DNS address provided by your ISP in the fields beside the *Add* button, then click *Add*.

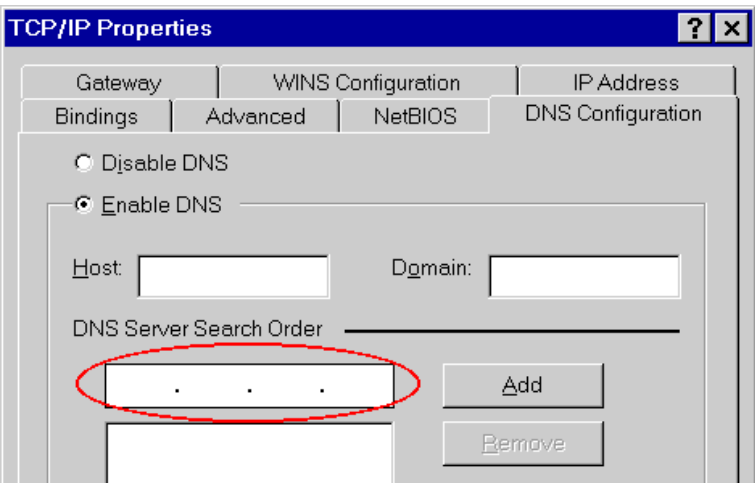


Figure 21: DNS Tab (Win 98SE/ME)

## 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:

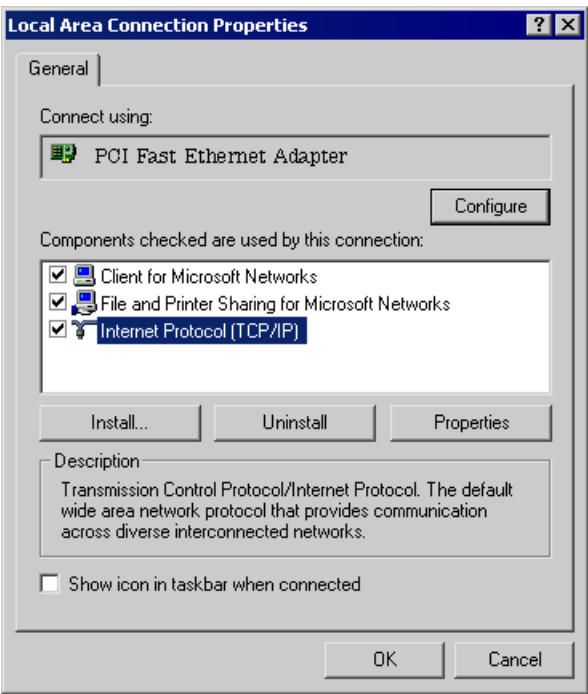


Figure 22: Network Configuration (Win 2000)

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.

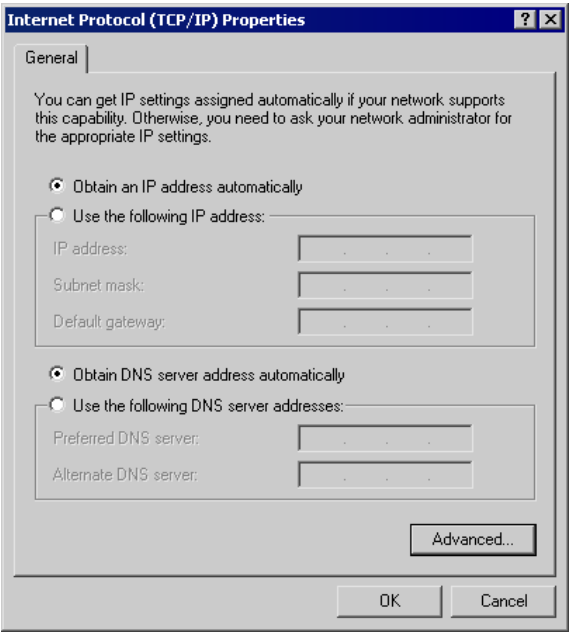


Figure 23: TCP/IP Properties (Win 2000)

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 ADSL2/2+ Modem Router will act as a DHCP Server.

Restart your PC to ensure it obtains an IP Address from the Wireless ADSL2/2+ Modem 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 ADSL2/2+ Modem 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 ADSL2/2+ Modem 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*.

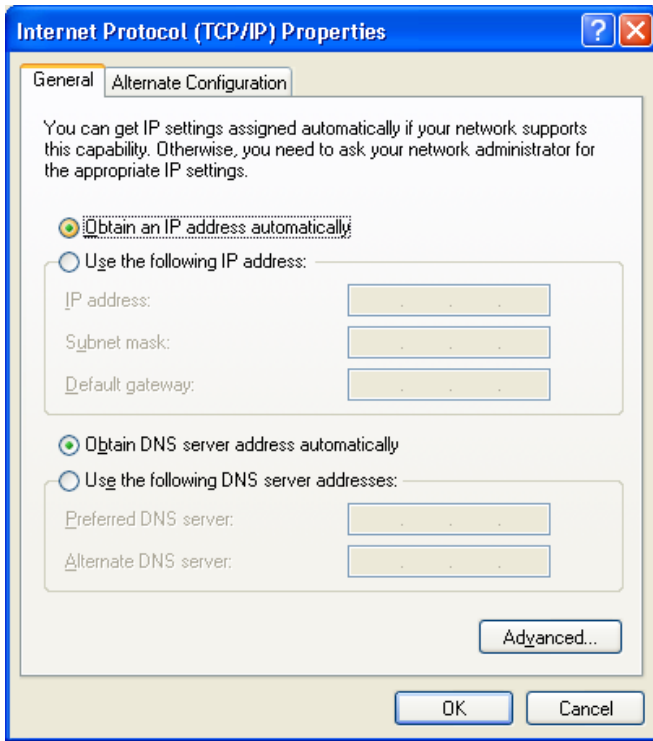
## Checking TCP/IP Settings - Windows XP

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



**Figure 24: 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.



**Figure 25: 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 ADSL2/2+ Modem Router will act as a DHCP Server.

Restart your PC to ensure it obtains an IP Address from the Wireless ADSL2/2+ Modem 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 ADSL2/2+ Modem Router's IP address and click *OK*. Your LAN administrator can advise you of the IP Address they assigned to the Wireless ADSL2/2+ Modem Router.
- If the *DNS Server* fields are empty, select *Use the following DNS server addresses*, and enter the DNS address or addresses provided by your ISP, then click *OK*.

## Internet Access

To configure your PCs to use the Wireless ADSL2/2+ Modem 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 9x/ME/2000

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

### For Windows XP

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

### Accessing AOL

To access AOL (America On Line) through the Wireless ADSL2/2+ Modem 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 ADSL2/2+ Modem 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 ADSL2/2+ Modem Router" location.

## Macintosh Clients

From your Macintosh, you can access the Internet via the Wireless ADSL2/2+ Modem 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 ADSL2/2+ Modem Router's IP Address.
- Ensure your DNS settings are correct.

## Linux Clients

To access the Internet via the Wireless ADSL2/2+ Modem Router, it is only necessary to set the Wireless ADSL2/2+ Modem 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 ADSL2/2+ Modem 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 ADSL2/2+ Modem Router:

- Ensure the "Gateway" field for your network card is set to the IP Address of the Wireless ADSL2/2+ Modem Router.
- Ensure your DNS (Name Server) settings are correct.

## Wireless Station Configuration

This section applies to all Wireless stations wishing to use the Wireless ADSL2/2+ Modem Router's Access Point, regardless of the operating system which is used on the client.

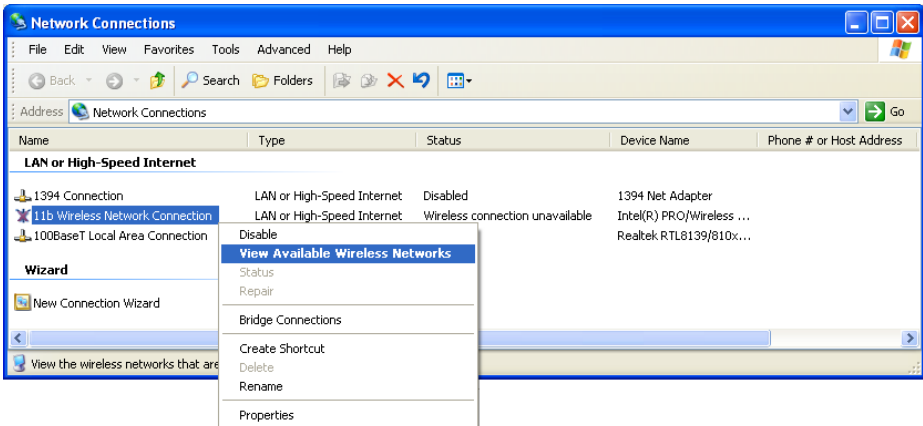
To use the Wireless Access Point in the Wireless ADSL2/2+ Modem Router, each Wireless Station must have compatible settings, as follows:

<b>Mode</b>	The mode must be set to <b>Infrastructure</b> (rather than Ad-hoc) Access points only operate in <b>Infrastructure</b> mode.
<b>SSID (ESSID)</b>	This must match the value used on the Wireless ADSL2/2+ Modem Router. The default value is <b>Wireless</b> . <b>Note! The SSID is case sensitive.</b>
<b>Wireless Security</b>	By default, Wireless security on the Wireless ADSL2/2+ Modem Router is disabled. <ul style="list-style-type: none"><li>• If Wireless security remains disabled on the Wireless ADSL2/2+ Modem Router, all stations must have wireless security disabled.</li><li>• If Wireless security is enabled on the Wireless Router (either WEP or WPA-PSK), each station must use the same settings as the Wireless ADLS Router.</li></ul>

## 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*).



**Figure 26: 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.

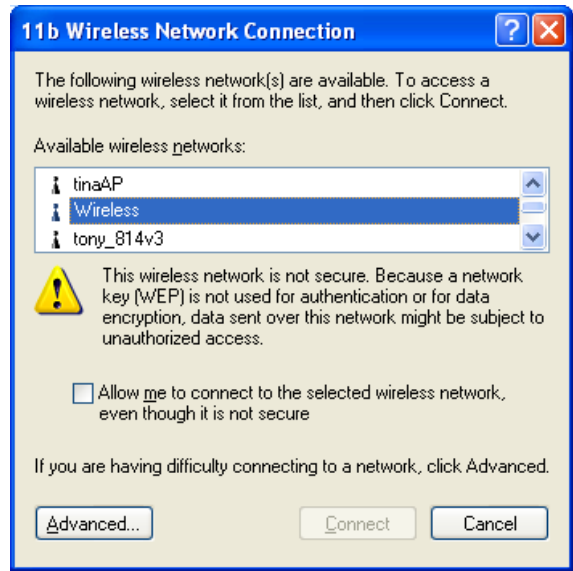


Figure 27 Wireless Networks (Windows XP)



**If the "Broadcast SSID" setting on the Wireless ADSL2/2+ Modem 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.**

4. The next step depends on whether or not Wireless security has been enabled on the Wireless ADSL2/2+ Modem Router.

**If Wireless Security is Disabled**

If Wireless security on the Wireless ADSL2/2+ Modem Router is disabled, Windows will warn you that the Wireless network is not secure.

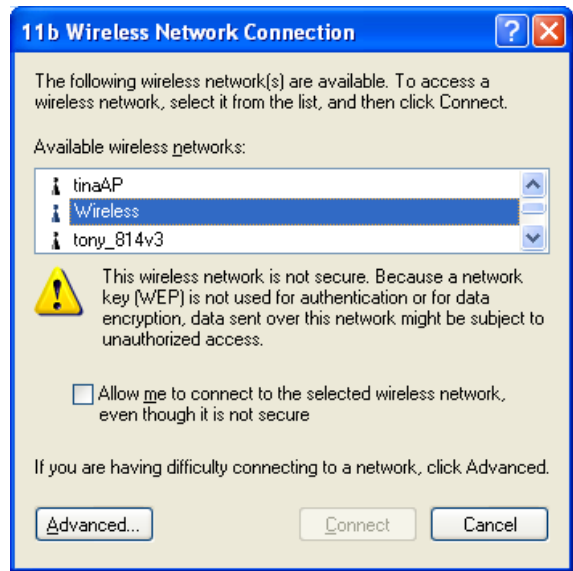


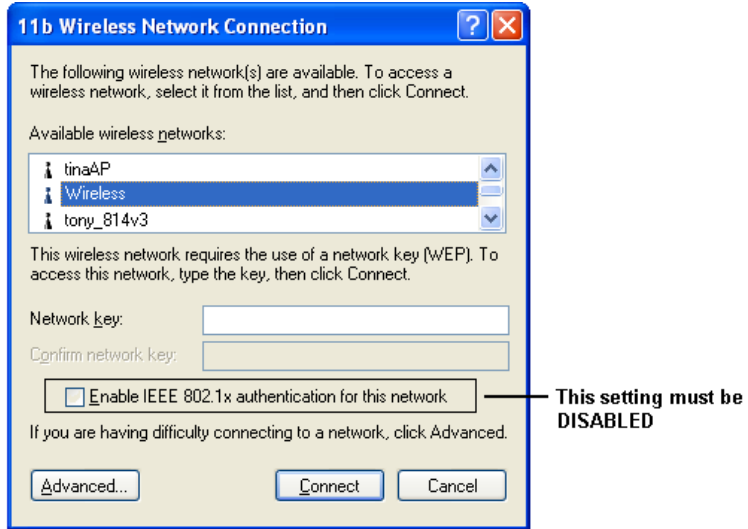
Figure 28 Insecure Wireless Network (Windows XP)

**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 ADSL2/2+ Modem Router, Windows will detect this, and show a screen like the following.



**Figure 29: WEP (Windows XP)**

**To connect:**

- Enter the WEP key, as set on the Wireless ADSL2/2+ Modem 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:

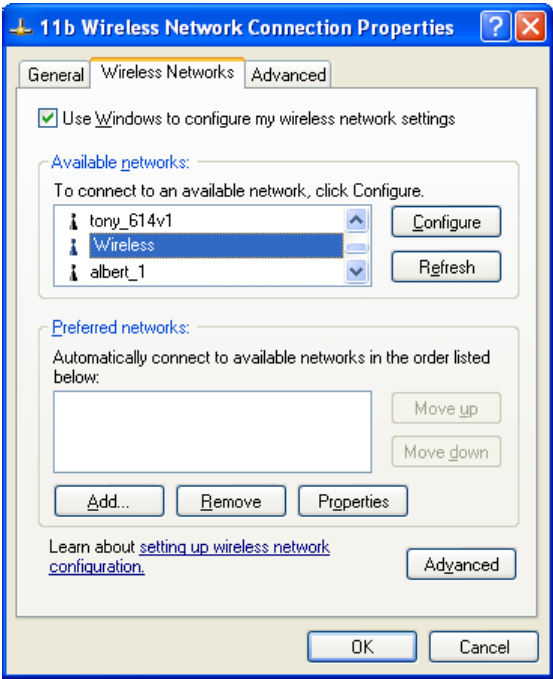


Figure 30: Advanced - Wireless Networks

Select the SSID for the Wireless ADSL2/2+ Modem Router, and click *Configure*, to see a screen like the following:

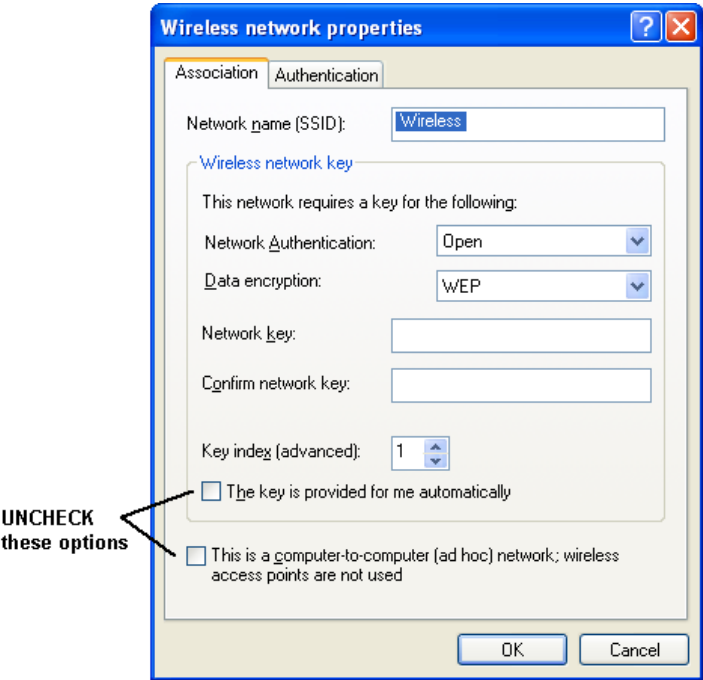
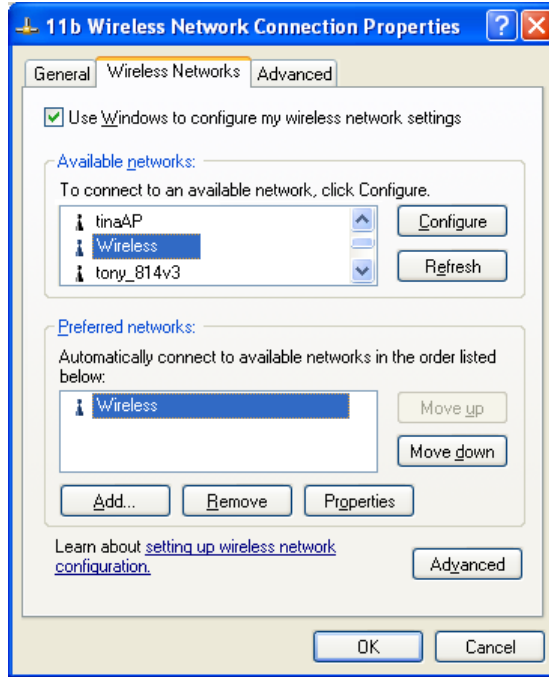


Figure 31: Wireless Network Properties - WEP

Configure this screen as follows:

- Set *Network Authentication* to match the Wireless ADSL2/2+ Modem Router. (If the setting on the Wireless ADSL2/2+ Modem 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 ADSL2/2+ Modem Router. (Windows will determine if 64bit or 128bit encryption is used.)
- The *Key index* must match the **default key index** on the Wireless ADSL2/2+ Modem 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.



**Figure 32: Preferred Networks**

Click OK to establish a connection to the Wireless ADSL2/2+ Modem Router.

## If using WPA-PSK Data Encryption

If WPA-PSK data encryption has been enabled on the Wireless ADSL2/2+ Modem Router, it does not matter which network is selected on the screen below. Just click the *Advanced* button.

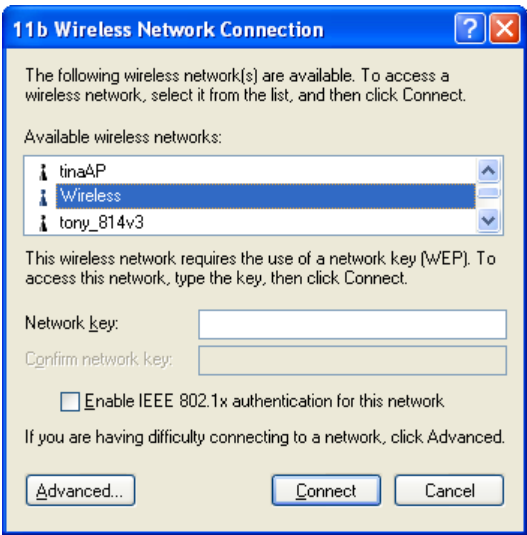


Figure 33: Wireless Networks (Windows XP)

You will then see a screen like the example below.

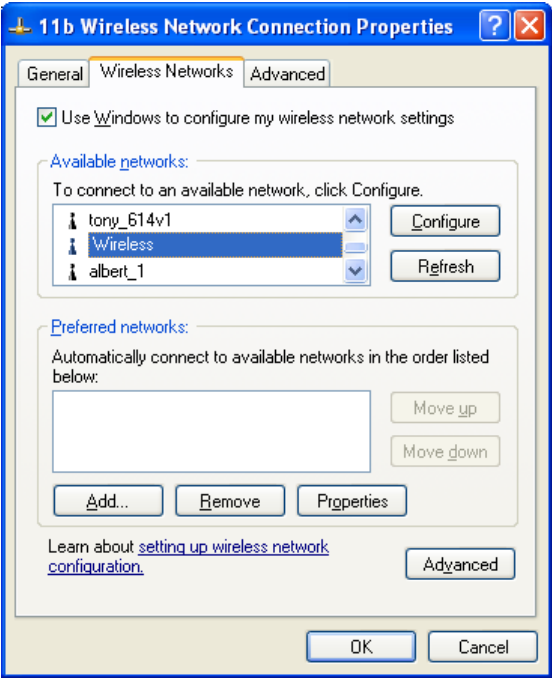
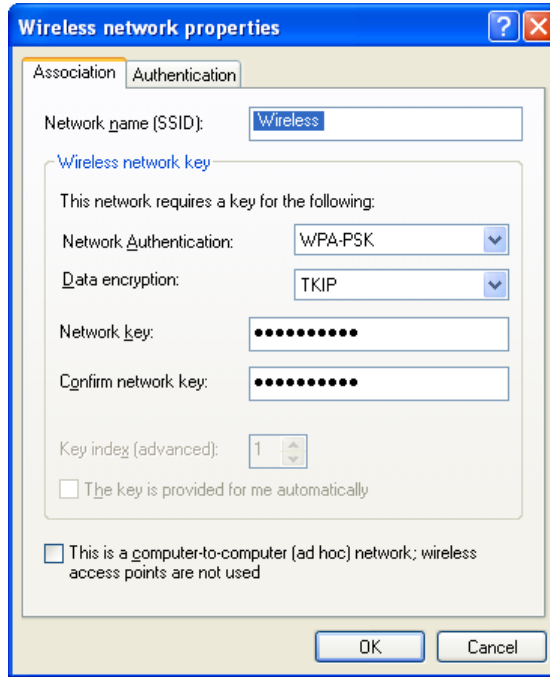


Figure 34: Advanced - Wireless Networks

Select the SSID for the Wireless ADSL2/2+ Modem Router, and click *Configure*, to see a screen like the following:



**Figure 35: 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 ADSL2/2+ Modem Router.
- Ensure the option *This is a computer-to-computer (ad hoc) network* is unchecked.
- Click OK to save and close this dialog.
- This wireless network will now be listed in *Preferred Networks* on the screen below.

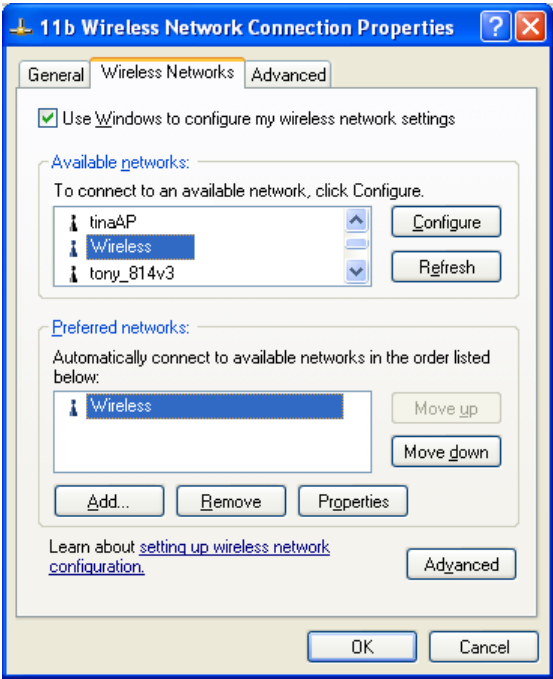


Figure 36: Preferred Networks

Click OK to establish a connection to the Wireless ADSL2/2+ Modem Router.

**If the SSID is not listed**

If the "Broadcast SSID" setting on the Wireless ADSL2/2+ Modem Router has been disabled, its SSID will NOT be listed on the screen below.

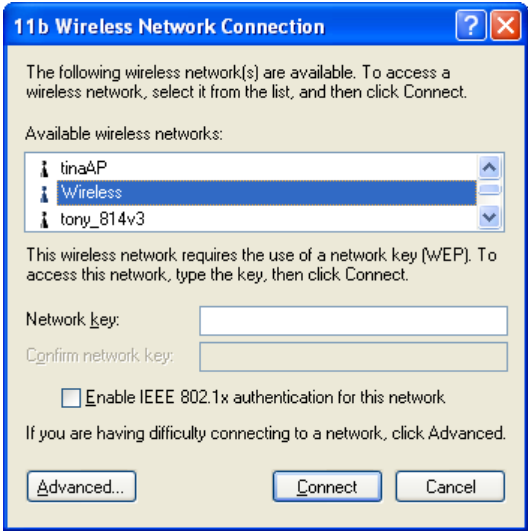
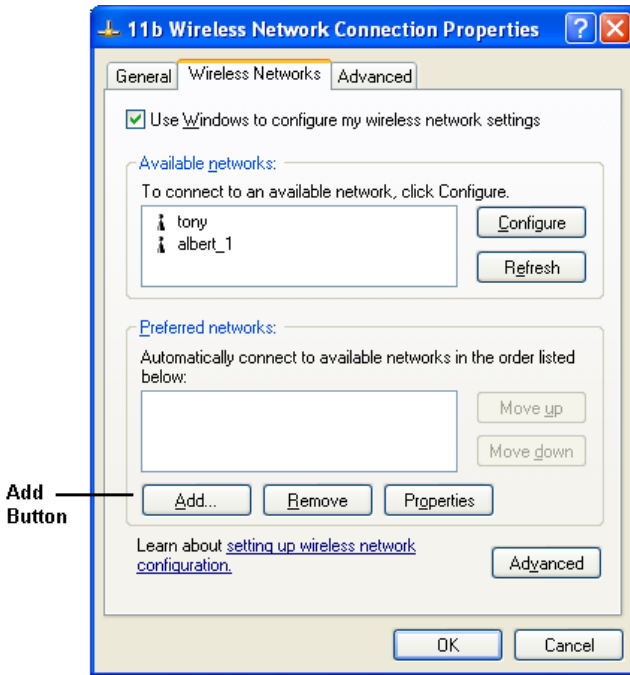


Figure 37: Wireless Networks (Windows XP)

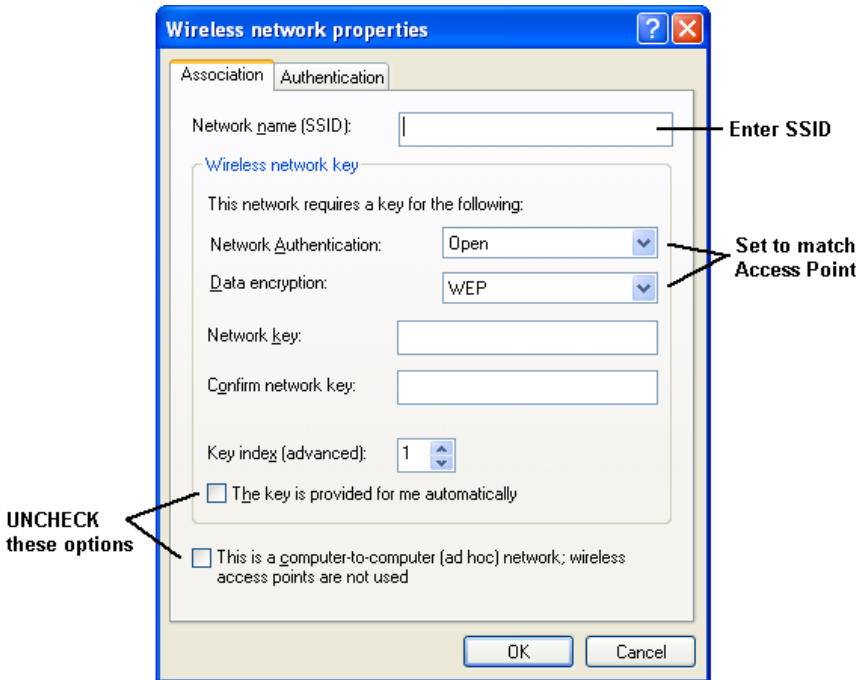
In this situation, you need to obtain the SSID from your network administrator, then follow this procedure:

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



**Figure 38: Unlisted Wireless Network**

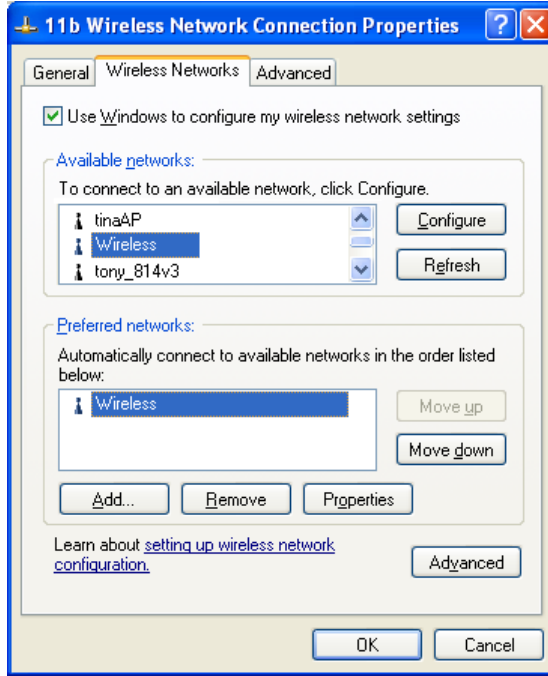
2. Click the *Add* button. You will see a screen like the example below.



**Figure 39: Add Wireless Network**

3. Configure this screen as follows:
- Enter the correct SSID, as used on the Wireless ADSL2/2+ Modem 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 ADSL2/2+ Modem Router.

- If using data encryption (WEP or WPA-PSK), enter the key used on the Wireless ADSL2/2+ Modem 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.



**Figure 40: Preferred Networks**

5. Click OK to establish a connection to the Wireless ADSL2/2+ Modem Router.

## Chapter 5

# Operation and Status



*This Chapter details the operation of the Wireless ADSL2/2+ Modem 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 ADSL2/2+ Modem 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.

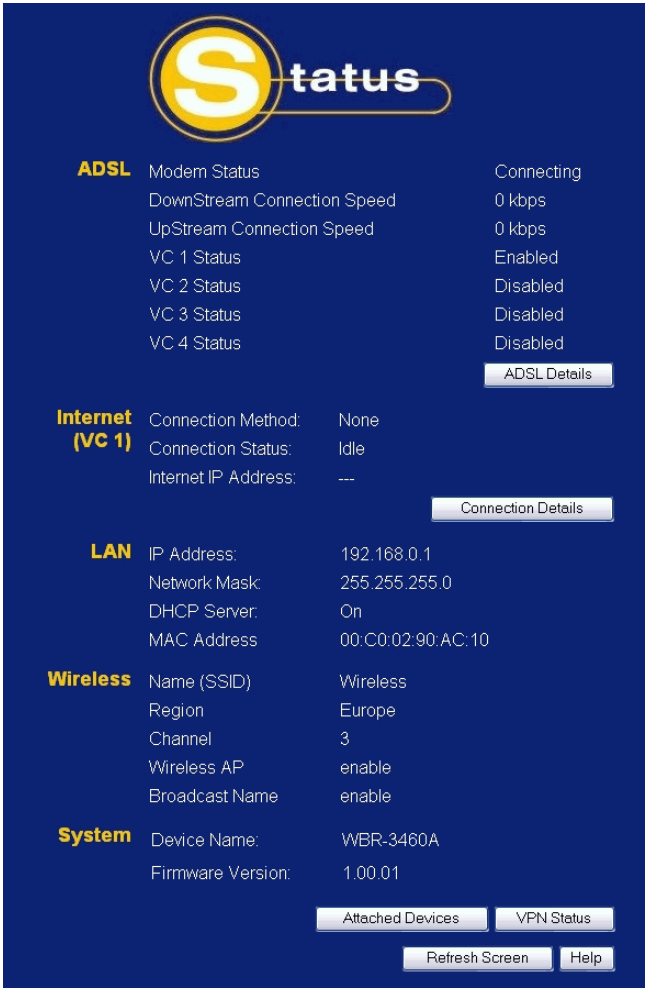


Figure 41: Status Screen

Data - Status Screen

ADSL	
Modem Status	This indicates the status of the ADSL modem component.
DownStream Connection Speed	Displays the speed for the DownStream Connection.
UpStream Connection Speed	If connected, displays the speed for the Up Stream (upload) ADSL Connection.
VC 1 Status VC 2 Status VC 3 Status VC 4 Status	For each VC (Virtual Circuit), the current status is displayed. This will be either "Enabled" or "Disabled". <b>Note:</b> VC 1 is a standard (Routed) Internet connection. VC 2, VC 3 and VC 4 are Bridge-mode connections.
ADSL Details	Click this button to open a sub-window and view the details of each VC (Virtual Circuit).
Internet (VC1)	
Connection Method	Displays the current connection method, as set in the <i>Setup</i>

	<i>Wizard.</i>
<b>Connection Status</b>	<p>This indicates the current status of the Internet Connection</p> <ul style="list-style-type: none"> <li>• <b>Active</b> - Connection exists</li> <li>• <b>Idle</b> - No current connection, but no error has been detected. This condition normally arises when an idle connection is automatically terminated.</li> <li>• <b>Failed</b> - The connection was terminated abnormally. This could be caused by Modem failure, or the loss of the connection to the ISP's server.</li> </ul> <p>If there is an error, you can click the "Connection Details" button to find out more information.</p>
<b>Internet IP Address</b>	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.
<b>Connection Details</b>	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.
<b>LAN</b>	
<b>IP Address</b>	The IP Address of the Wireless ADSL2/2+ Modem Router.
<b>Network Mask</b>	The Network Mask (Subnet Mask) for the IP Address above.
<b>DHCP Server</b>	This shows the status of the DHCP Server function. The value will be "Enabled" or "Disabled".
<b>MAC Address</b>	This shows the MAC Address for the Wireless ADSL2/2+ Modem Router, as seen on the LAN interface.
<b>Wireless</b>	
<b>Name (SSID)</b>	If using an ESS (Extended Service Set, with multiple access points) this ID is called an ESSID (Extended Service Set Identifier).
<b>Region</b>	The current region, as set on the Wireless screen.
<b>Channel</b>	This shows the Channel currently used, as set on the Wireless screen.
<b>Wireless AP</b>	This indicates whether or not the Wireless Access Point feature is enabled.
<b>Broadcast Name</b>	This indicates whether or not the SSID is Broadcast. This setting is on the Wireless screen.
<b>System</b>	
<b>Device Name</b>	The current name of the Router. This name is also the "hostname" for users with an "@Home" type connection.
<b>Firmware Version</b>	The version of the current firmware installed.
<b>Buttons</b>	
<b>ADSL Details</b>	View the details of each VC (Virtual Circuit).
<b>Connection Details</b>	Click this button to open a sub-window and view a detailed

	description of the current connection.
<b>Attached Devices</b>	This will open a sub-window, showing all LAN and Wireless devices currently on the network.
<b>VPN Status</b>	View details of each current VPN Tunnel is a sub-window. You also have the option of viewing the VPN Log.  For further details about VPN, see the VPN section in <b><i>Chapter 6 - Advanced Features</i></b> .
<b>Refresh Screen</b>	Update the data displayed on screen.

## Connection Status - PPPoE & PPPoA

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

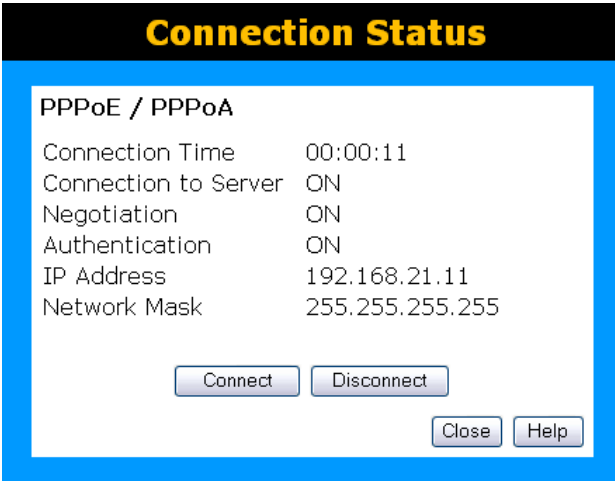


Figure 42: PPPoE Status Screen

### Data - PPPoE/PPPoA Screen

<b>Connection Time</b>	This indicates how long the current connection has been established.
<b>Connection to Server</b>	<p>This indicates whether or not the connection is currently established.</p> <ul style="list-style-type: none"><li>• If the connection does not exist, the "Connect" button can be used to establish a connection.</li><li>• If the connection currently exists, the "Disconnect" button can be used to break the connection.</li><li>• Normally, it is not necessary to use the Connect and Disconnect buttons unless the setting "Connect automatically, as required" is disabled.</li></ul>
<b>Negotiation</b>	This indicates the status of the PPPoE Server login.
<b>Authentication</b>	This will show the Authentication status of the connection.
<b>IP Address</b>	The IP Address of this device, as seen by Internet users. This address is allocated by your ISP (Internet Service Provider).
<b>Network Mask</b>	The Network Mask associated with the IP Address above.
<b>Buttons</b>	
<b>Connect</b>	If not connected, establish a connection to your ISP.
<b>Disconnect</b>	If connected to your ISP, hang up the connection.
<b>Close</b>	Close this window.

## 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            172.31.2.205

Subnet Mask        255.255.255.0

Default Gateway    172.31.2.253

DHCP Server        172.31.2.205

DNS Server         172.31.2.254

Lease Obtained:    2006-08-08 12:06:02

Lease Expires:     2006-08-010 12:02:52

**Figure 43: Connection Details - Dynamic IP Address**

### Data - Dynamic IP address

Internet	
<b>IP Address</b>	The current IP Address of this device, as seen by Internet users. This address is allocated by your ISP (Internet Service Provider).
<b>Subnet Mask</b>	The Network Mask associated with the IP Address above.
<b>Default Gateway</b>	The IP address of the remote Gateway or Router associated with the IP Address above.
<b>DHCP Server</b>	The IP address of your ISP's DHCP Server.
<b>DNS Server</b>	The IP address of the Domain Name Server which is currently used.
<b>Lease Obtained Lease Expires</b>	This indicates when the current IP address was obtained, and how long before this IP address allocation (the DHCP lease) expires.
Buttons	
<b>Release</b>	If an IP Address has been allocated to the Wireless ADSL2/2+ Modem Router (by the ISP's DHCP Server, clicking the "Release" button will break the connection and release the IP Address.
<b>Renew</b>	If the ISP's DHCP Server has NOT allocated an IP Address for the Wireless ADSL2/2+ Modem Router, clicking the "Renew" button will attempt to re-establish the connection and obtain an IP Address from the ISP's DHCP Server.

<b>Close</b>	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.

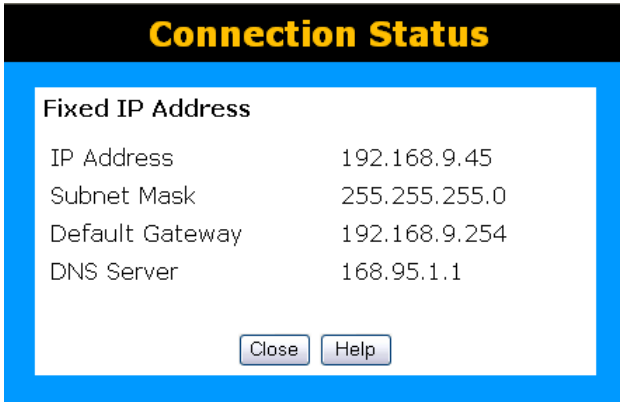


Figure 44: Connection Details - Fixed/Dynamic IP Address

### Data - Fixed IP address Screen

Internet	
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 Network 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 ADSL2/2+ Modem Router's "Advanced" Features.*

## Overview

The following advanced features are provided:

- Internet:
  - DMZ
  - Special Applications
  - URL filter
- Dynamic DNS
- Firewall Rules
- Firewall Services
- Options
- Schedule
- Virtual Servers
- VPN

## Internet

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

The screenshot shows the 'Internet' configuration page. At the top, the word 'Internet' is displayed in a large, light blue font. Below it, there are three main sections: 'DMZ', 'Special Applications', and 'URL Filter'. The 'DMZ' section has a checkbox labeled 'Enable DMZ, using' followed by a dropdown menu showing 'Select a PC'. A link 'My PC is not listed' is visible to the right. The 'Special Applications' section has a text description: 'If an application does not work, you can define it as a Special Application.' and a button labeled 'Special Applications'. The 'URL Filter' section has three radio button options: 'Disable', 'Block Always' (which is selected), and 'Block By Schedule'. A button labeled 'Configure URL Filter' is to the right. At the bottom right, there are three buttons: 'Save', 'Cancel', and 'Help'.

Figure 45: 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 select 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.

## Special Applications

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 "Special Application".

The **Special Applications** screen can be reached by clicking the *Special Applications* button on the *Internet* screen.

You can then define your Special Applications. 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

Special Applications

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		

SaveCancel

HelpClose

Figure 46: Special Applications Screen

Data - Special Applications Screen

Checkbox	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"><li><b>Type</b> - Select the protocol (TCP or UDP) used when you send data to the remote system or service.</li><li><b>Start</b> - 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.</li><li><b>Finish</b> - 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.</li></ul>
Incoming Ports	<ul style="list-style-type: none"><li><b>Type</b> - 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).</li><li><b>Start</b> - 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.</li><li><b>Finish</b> - Enter the end of the range of port numbers used by the application server, for data you receive.</li></ul>

## Using a Special Application

- Configure the *Special Applications* screen as required.
- On your PC, use the application normally. Remember that only one (1) PC can use each Special application at any time. Also, when 1 PC is finished using a particular Special Application, there may need to be a "Time-out" before another PC can use the same Special Application. The "Time-out" period may be up to 3 minutes.

## 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**

When enabled, a request is blocked if any of these entries occur in the requested URL.

**Current Filter Strings**

[Empty text area for filter strings]

Delete Delete All

Add Filter String: [Text input field] Add

Filter Strings should be as specific as possible.

**Trusted PC**

☐ Allow this PC to Visit Blocked Sites

Trusted PC: [Select a PC dropdown]

Save Cancel Help Close

**Figure 47: URL Filter Screen**

## Data - URL Filter Screen

Current Filter Strings	
Current Filter Strings	<p>The list contains the current list of items to block.</p> <ul style="list-style-type: none"><li>• To add to the list, use the "Add" option below.</li><li>• To delete an entry, select it and click <b>Delete</b> button.</li><li>• To delete all entries, click the <b>Delete All</b> button.</li></ul>
Add Filter String	<p>To add to the current list, type the word or domain name you want to block into the field provided, then click the <b>Add</b> button.</p> <p>Filter strings should be as specific as possible. Otherwise, you may block access to many more sites than intended.</p>
Trusted PC	
Allow Trusted PC	<p>Enable this to allow one computer to have unrestricted access to the Internet. For this PC, the URL filter will be ignored.</p> <p>If enabled, you must select the PC to be the trusted PC.</p>
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 ADSL2/2+ Modem Router's DDNS screen, and enable the DDNS feature.
- 4. The Wireless ADSL2/2+ Modem 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:

DDNS

DDNS Service

☐ Use a Dynamic DNS Service

Service Provider

DynDNS.org (Dynamic)

Web Site

DDNS Data

Host Name

User Name

Password

DDNS Status:

Refresh

SaveCancelHelp

Figure 48: 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.

<b>Web Site</b>	Click this button to open a new window and connect to the Web site of the selected DDNS service provider.
<b>DDNS Data</b>	
<b>Host Name</b>	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.
<b>User Name</b>	Enter your Username for the DDNS Service. (TZO.com uses your E-mail address.)
<b>Password</b>	Enter your current password for the DDNS Service. (TZO.com calls this a key.)
<b>DDNS Status</b>	<ul style="list-style-type: none"><li>• This message is returned by the DDNS Server.</li><li>• Normally, this message should be "Update successful"</li><li>• If the message indicates some problem, you need to connect to the DDNS Service provider and correct this problem.</li></ul>

# Firewall Rules

The **Firewall Rules** screen allows you to define "Firewall Rules" which can allow or prevent certain traffic. "Traffic" means incoming connection attempts, not packets.

By default:

- All Outgoing traffic is permitted.
- All Incoming traffic is denied.

Because of this default behavior, any **Outgoing** rules will generally **Block** traffic, and **Incoming** rules will generally **Allow** traffic.

## Firewall Rules Screen

An example screen is shown below.

Firewall Rules

Incoming Rules

	#	Enable	Service Name	Action	LAN Server IP address	WAN Users	Log
	Default	Yes	Any	BLOCK always	--	Any	Match

Add

Edit

Move

Delete

Outgoing Rules

	#	Enable	Service Name	Action	LAN Users	WAN Servers	Log
	Default	Yes	Any	ALLOW always	Any	Any	Never

Add

Edit

Move

Delete

Save

Cancel

Help

Figure 49 Firewall Screen

## Data - Firewall Rules

Incoming Rules	
#	For the default rule, this will display "Default". For rules which you create, this will display a radio button which allows you to select the rule.
Enable	Indicates whether or not the rule is currently enabled.  For rules you have added, this column will contain a checkbox, allowing you to easily enable or disable the rule. (Click "Save" after making any changes.)
Service Name	The Service covered by this rule.
Action	The action performed on connections which are covered by this

	rule.
<b>LAN Server IP Address</b>	The PC or Server on your LAN to which traffic covered by this rule will be sent.
<b>WAN Users</b>	The WAN IP address or addresses covered by this rule.
<b>Log</b>	Indicates whether or not connections covered by this rule should be logged.
<b>Buttons</b>	Use the <i>Add</i> button to create a new rule. The other buttons - <i>Edit</i> , <i>Move</i> , or <i>Delete</i> - require that a rule be selected first. Use the radio buttons in the left column to select the desired rule.
<b>Outgoing Rules</b>	
<b>#</b>	For the default rule, this will display "Default". For rules which you create, this will display a radio button which allows you to select the rule.
<b>Enable</b>	Indicates whether or not the rule is currently enabled.  For rules you have added, this column will contain a checkbox, allowing you to easily enable or disable the rule. (Click "Save" after making any changes.)
<b>Service Name</b>	The Service covered by this rule.
<b>Action</b>	The action performed on connections which are covered by this rule.
<b>LAN Users</b>	The LAN PC or PCs covered by this rule.
<b>WAN Servers</b>	The WAN IP address or addresses covered by this rule.
<b>Log</b>	Indicates whether or not connections covered by this rule should be logged.
<b>Buttons</b>	Use the <i>Add</i> button to create a new rule. The other buttons - <i>Edit</i> , <i>Move</i> , or <i>Delete</i> - require that a rule be selected first. Use the radio buttons in the left column to select the desired rule.

Incoming Rules (Inbound Services)

This screen is displayed when the "Add" or "Edit" button for Incoming Rules is clicked.

Inbound Services

Service:

Any(ALL)(TCP/UDP:1,65535)

Action:

ALLOW always

Send to LAN Server:

Select a PC

WAN Users:

Any

Single/Start:

Finish:

Log:

Always

Save

Cancel

Back

Help

Figure 50: Inbound Services Screen

Data - Incoming Rules Screen

Inbound Services	
Service	Select the desired Service. This determines which packets are covered by this rule. If necessary, you can define a new Service on the "Services" screen, by defining the protocols and port numbers used by the Service.
Action	<div>Select the desired action for packets covered by this rule:</div> <ul style="list-style-type: none"><li>ALLOW always</li><li>ALLOW by schedule, otherwise Block</li><li>BLOCK always</li><li>BLOCK by schedule, otherwise Allow</li></ul> <div>Note:</div> <ul style="list-style-type: none"><li>Any inbound traffic which is not allowed by rules you create will be blocked by the Default rule.</li><li>BLOCK rules are only useful if the traffic is already covered by an ALLOW rule. (That is, you wish to block a sub-set of traffic which is currently allowed by another rule.)</li><li>To define the Schedule used in these selections, use the "Schedule" screen.</li></ul>
Send to LAN Server	Select the PC or Server on your LAN which will receive the in-bound traffic covered by this rule.
WAN Users	<div>These settings determine which packets are covered by the rule, based on their source (WAN) IP address. Select the desired option:</div> <ul style="list-style-type: none"><li><b>Any</b> - All IP addresses are covered by this rule.</li><li><b>Single address</b> - Enter the required address in the "Sin-</li></ul>

	<p>gle/Start" fields.</p> <ul style="list-style-type: none"><li>• <b>Address range</b> - If this option is selected, you must enter the desired values in the "Single/Start" and "Finish" fields to determine the address range.</li></ul>
<b>Log</b>	<p>This determines whether packets covered by this rule are logged. Select the desired action.</p> <ul style="list-style-type: none"><li>• <b>Always</b> - always log traffic considered by this rule, whether it matches or not. (This is useful when debugging your rules.)</li><li>• <b>Never</b> - never log traffic considered by this rule, whether it matches or not.</li><li>• <b>Match</b> - Log traffic only it matches this rule. (The action is determined by this rule.)</li><li>• <b>Not Match</b> - Log traffic which is considered by this rule, but does not match (The action is NOT determined by this rule.)</li></ul>

Outgoing Rules (Outbound Services)

This screen is displayed when the "Add" or "Edit" button for Outgoing Rules is clicked.

Outbound Services

Service

Any(ALL)(TCP/UDP:1,65535)

Action

BLOCK always

LAN Users

Any

PC:

Select a PC

WAN Users

Any

Single/Start:

.

.

.

Finish:

.

.

.

Log

Always

Save

Cancel

Back

Help

Figure 51: Outbound Services Screen

Data - Outbound Rules Screen

Outbound Services	
<b>Service</b>	Select the desired Service or application to be covered by this rule. If the desired service or application does not appear in the list, you must define it using the "Services" menu option
<b>Action</b>	Select the desired action for packets covered by this rule: <ul style="list-style-type: none"><li>• BLOCK always</li><li>• BLOCK by schedule, otherwise Allow</li></ul>

	<ul style="list-style-type: none"><li>• ALLOW always</li><li>• ALLOW by schedule, otherwise Block</li></ul> <p><b>Note:</b></p> <ul style="list-style-type: none"><li>• Any outbound traffic which is not blocked by rules you create will be allowed by the Default rule.</li><li>• ALLOW rules are only useful if the traffic is already covered by a BLOCK rule. (That is, you wish to allow a subset of traffic which is currently blocked by another rule.)</li><li>• To define the Schedule used in these selections, use the "Schedule" screen.</li></ul>
LAN Users	<p>Select the desired option to determine which PCs are covered by this rule:</p> <ul style="list-style-type: none"><li>• <b>Any</b> - All PCs are covered by this rule.</li><li>• <b>Single PC</b> - Only the selected PC is covered by this rule. If selected, you must select the PC.</li></ul> <p><b>PC</b> - If using Single PC above, select the PC or Server on your LAN which will be covered by this rule.</p>
WAN Users	<p>These settings determine which packets are covered by the rule, based on their source (WAN) IP address. Select the desired option:</p> <ul style="list-style-type: none"><li>• <b>Any</b> - All IP addresses are covered by this rule.</li><li>• <b>Single address</b> - Enter the required address in the "Single/Start" fields.</li><li>• <b>Address range</b> - If this option is selected, you must enter the "Start" and "Finish" fields.</li></ul>
Log	<p>This determines whether packets covered by this rule are logged. Select the desired action.</p> <ul style="list-style-type: none"><li>• <b>Always</b> - always log traffic considered by this rule, whether it matches or not. (This is useful when debugging your rules.)</li><li>• <b>Never</b> - never log traffic considered by this rule, whether it matches or not.</li><li>• <b>Match</b> - Log traffic only it matches this rule. (The action is determined by this rule.)</li><li>• <b>Not Match</b> - Log traffic which is considered by this rule, but does not match (The action is NOT determined by this rule.)</li></ul>

User-defined Services

Services are used when creating Firewall Rules.

If you wish to create a firewall rule, but the required service is not listed in the "Service" list, you can use this feature to define the required service or services. Once created, these services will be listed in the "Service" list, and can be used when creating Firewall Rules.

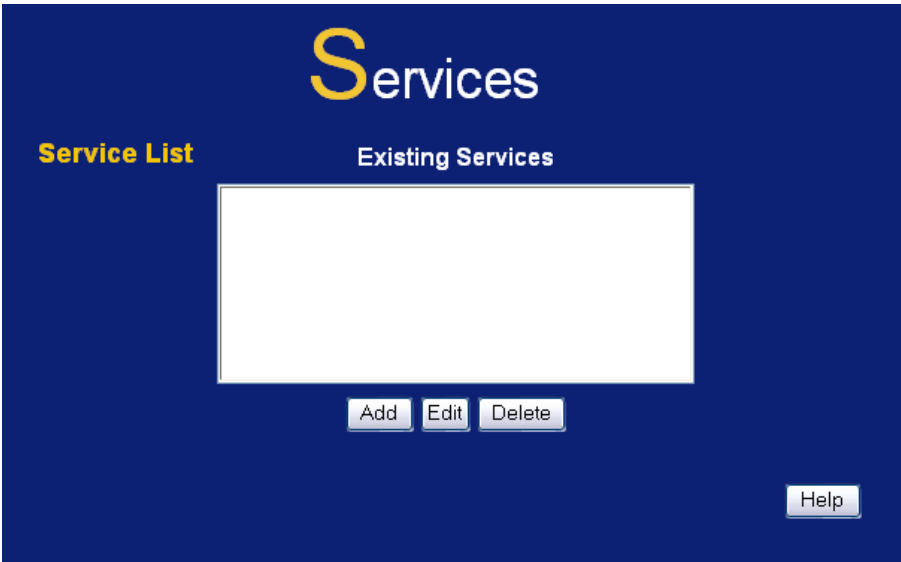


Figure 52: Add Services Screen

Data - User-defined Services

Services	
Existing Services	<p>This lists any Services you have defined. If you have not defined any Services, this list will be empty.</p> <p>Once you define some services, they will be listed here, and also shown in the Service list used to create Firewall rules. (User-defined services are at the end of the list, after the pre-defined services.)</p>
Add	<p>Use this to open a sub-screen where you can add a new service.</p>
Edit	<p>To modify a service, select it, and then click this button.</p>
Delete	<p>Use this button to delete the selected service. You can delete any services you have defined.</p>

Add/Edit Service

This screen is displayed when the *Add* or *Edit* button on the **Services** screen is clicked.

Add/Edit Service

Name:

Type:

TCP

Start Port:

Finish Port:

Save

Cancel

Back

Help

Figure 53 : Add/Edit Service

Data - Add/Edit Service

Services	
Name	If editing, this shows the current name of the Service. If adding a new service, this will be blank, and you should enter a suitable name.
Type	Select the protocol used by the Service.
Start Port	Enter the beginning of the port range used by the Service.
Finish Port	Enter the end of the port range used by the Service.

## 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 dark blue window titled "Options". Under the "Internet" section, there is a checkbox "Respond to Ping on Internet (WAN) Port" which is unchecked, and a text field "MTU Size" with the value "1458" and a note "(Bytes, 600~1500)". Under the "UPnP" section, there is a checked checkbox "Enable UPnP", a text field "Advertisement Period" with the value "30" and a note "(Minutes, 1~1440)", and a text field "Advertisement Time to Live" with the value "4" and a note "(Hops, 1~255)". At the bottom right are three buttons: "Save", "Cancel", and "Help".

Figure 54: Options Screen

### Data - Options Screen

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

# Schedule

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

Schedule

Schedule

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

Day	Session 1		Session 2	
	Start	Finish	Start	Finish
Monday	00:00	12:00	12:00	24:00
Tuesday	00:00	12:00	12:00	24:00
Wednesday	00:00	12:00	12:00	24:00
Thursday	00:00	12:00	12:00	24:00
Friday	00:00	12:00	12:00	24:00
Saturday	00:00	12:00	12:00	24:00
Sunday	00:00	12:00	12:00	24:00

Local Time

Time Zone: (GMT) Greenwich Mean Time : Edinburgh, London

☐ Adjust for Daylight Savings Time

☐ Use this NTP Server

Current Time: 2002-09-08 12:46:54

Save

Cancel

Help

Figure 55: Schedule Screen

## Data - Schedule Screen

Schedule	
Day	Each day of the week can scheduled independently.
Session 1 Session 2	Two (2) separate sessions or periods can be defined. Session 2 can be left blank if not required.
Start Time	Enter the start using a 24 hr clock.
Finish Time	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 Day-light Savings	If your region uses Daylight Savings Time, you must manually check "Adjust for Daylight Savings Time" at the beginning of

<b>Time</b>	the adjustment period, and uncheck it at the end of the Day-light Savings period.
<b>Use this NTP Server</b>	<p>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..</p> <p>If this setting is not enabled, the default NTP Servers are used.</p>
<b>Current Time</b>	This displays the current time on the Wireless ADSL2/2+ Modem Router, at the time the page is loaded.

## Virtual Servers

This feature, sometimes called *Port Forwarding*, 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 "Virtual Server" feature solves these problems and allows Internet users to connect to your servers, as illustrated below.

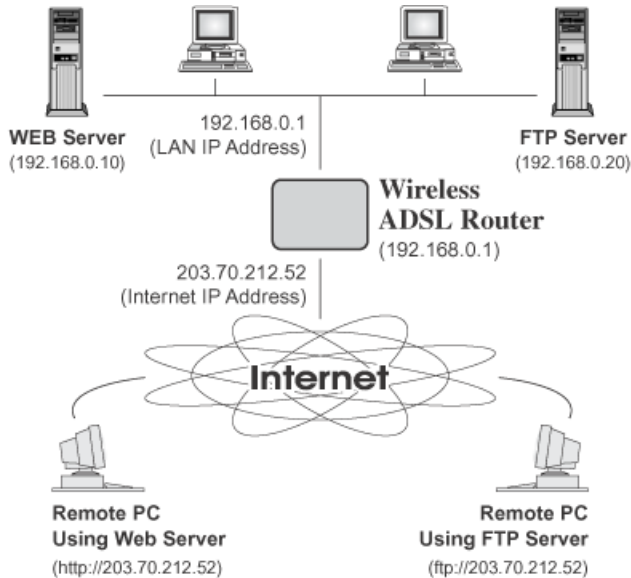


Figure 56: Virtual Servers

### IP Address seen by Internet Users

Note that, in this illustration, both Internet users are connecting to the same IP Address, but using different protocols.

**To Internet users, all virtual Servers on your LAN have the same IP Address. This IP Address is allocated by your ISP.**

This address should be static, rather than dynamic, to make it easier for Internet users to connect to your Servers.

However, you can use the *DDNS (Dynamic DNS)* feature to allow users to connect to your Virtual Servers using a URL, instead of an IP Address.

### Virtual Servers Screen

- The "Virtual Servers" feature allows Internet Users to access PCs on your LAN.
- The PCs must be running the appropriate Server Software.
- For Internet Users, ALL of your Servers have the same IP address. This IP address is allocated by your ISP.
- To make it easier for Internet users to connect to your Servers, you can use the "DDNS" feature. This allows Internet users to connect to your Servers with a URL, rather than an IP address. This technology works even if your ISP allocates dy-

dynamic IP addresses (IP address is allocated upon connection, so it may change each time you connect).

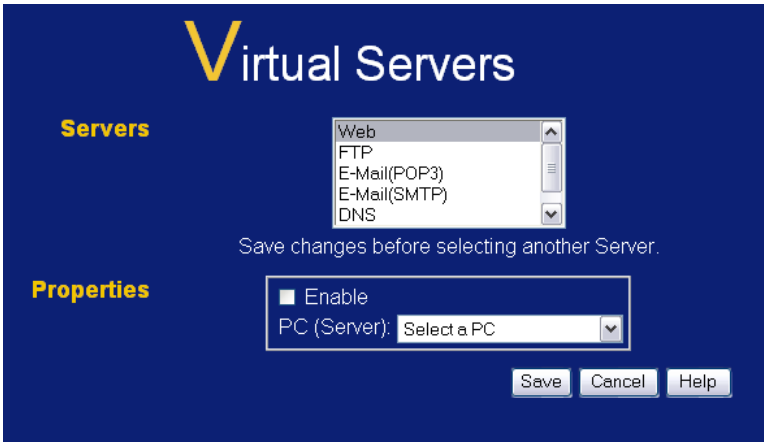


Figure 57: Virtual Servers Screen

Data - Virtual Servers Screen

Servers	
Servers	This lists a number of common Server types. If the desired Server type is not listed, you can create a Firewall Rule to achieve the same effect as the Virtual Server function.
Properties	
Enable	Use this to Enable or Disable support for this Server, as required.  If Enabled, you must select the PC to which this traffic will be sent.
PC (Server)	Select the PC for this Server. The PC must be running the appropriate Server software.



For each entry, the PC must be running the appropriate Server software.

If the desired Server type is not listed, you can define your own Servers, using the Firewall Rules.

Connecting to the Virtual Servers

Once configured, anyone on the Internet can connect to your Virtual Servers. They must use the Internet IP Address (the IP Address allocated to you by your ISP).  
e.g.

http://203.70.212.52

ftp://203.70.212.52

It is more convenient if you are using a Fixed IP Address from your ISP, rather than Dynamic. However, you can use the *Dynamic DNS* feature to allow users to connect to your Virtual Servers using a URL, rather than an IP Address.



**From the Internet, ALL Virtual Servers have the IP Address allocated by your ISP**

## VPN Setup

The VPN (Virtual Private Network) feature in the Wireless ADSL2/2+ Modem Router allows you to create a VPN connection between 2 Wireless ADSL2/2+ Modem Routers, or a remote PC to establish a VPN connection to the Wireless ADSL2/2+ Modem Router.

To establish a VPN connection from a remote PC to the Wireless ADSL2/2+ Modem Router, you need suitable (IPSec) VPN client software on your PC.

For more information about VPNs, please refer to **Appendix C - About VPNs**.

## VPN Policies

A "VPN Policy" contains all the configuration data for a particular VPN connection. Generally, you will have to create one policy for each site you wish to connect to. The remote VPN Gateway (or client) needs to have matching configuration.

- Traffic covered by an enabled policy will automatically be sent via a VPN tunnel. If the VPN tunnel does not exist, it will be created.
- The VPN tunnel is created according to the parameters in the SA (Security Association).
- The remote VPN Endpoint must have a matching SA, or it will refuse the connection.

There are 2 types of VPN Policies:

- **Manual** - All settings (including the keys) for the VPN tunnel are manually input at each end (both VPN Endpoints).
- **Auto** - Some parameters for the VPN tunnel are generated automatically. This requires using the IKE (Internet Key Exchange) protocol to perform negotiations between the 2 VPN Endpoints.

## VPN Policies Screen

This screen is displayed when you select **VPN** on the **Advanced** menu. It allows you to create, modify and manage your VPN Policies.

If you have not created any policies, the Policy Table will be empty.



Figure 58: VPN Policies Screen

### Data - VPN Policies Screen

<b>Policy Table</b>	<p>The Policy Table contains the following data</p> <ul style="list-style-type: none"><li>• <b>Enable</b> - Use this checkbox to Enable or Disable a Policy as required. Click "Save" after making any changes.</li><li>• <b>Name</b> - Each policy is given a unique name to identify it. This name is not known to the remote VPN endpoint; it is used only to assist managing your policies.</li><li>• <b>Endpoint</b> - The address of the remote VPN endpoint.</li><li>• <b>Type</b> - The Type is "Auto" or "Manual" as explained above.</li><li>• <b>Local LAN</b> - IP address or subnet on your local LAN. Traffic must be from (or to) these addresses to be covered by this policy.</li><li>• <b>Remote LAN</b> - IP address or subnet on the remote LAN. Traffic must be to (or from) these addresses to be covered by this policy.</li><li>• <b>ESP</b> - ESP (Encapsulating Security Payload) encryption protocol used for the VPN data.</li></ul>
<b>Buttons</b>	
<b>Save</b>	Save any changes to the "Enable" setting for each policy.
<b>Edit</b>	Edit (modify) the selected policy. (Select a policy by clicking on the radio button.)
<b>Delete</b>	Delete the selected policy. (Select a policy by clicking on the radio button.)
<b>Add Auto Policy</b>	<p>Change to the input screen for an "Auto" policy. See the following section for details.</p> <p>When the new policy is saved, it will appear in the bottom row of the Policy Table.</p>

<b>Add Manual Policy</b>	Change to the input screen for a "Manual" policy. See the following section for details.  When the new policy is saved, it will appear in the bottom row of the Policy Table.
<b>VPN Status</b>	View details of each current VPN Tunnel (connection) in a sub-window. You also have the option of viewing the VPN Log.

**VPN Auto Policy Screen**

This screen is displayed when you click the *Add Auto Policy* button on the **VPN Policies** screen, or when you edit an existing Auto Policy. It allows you to define or edit an "Auto" VPN policy.

An "Auto" VPN policy uses the IKE (Internet Key Protocol) to exchange and negotiate parameters for the IPsec SA (Security Association). Because of this negotiation, it is not necessary for all settings on this VPN Gateway to match the settings on the remote VPN endpoint. Where settings must match, this is indicated.

VPN - Auto Policy

General

Policy Name:

Remote VPN Endpoint

Address Type: 

Dynamic IP address

Address Data:

☒ NetBIOS Enable

Local LAN

IP Address: 

Subnet address

IP address: 

192

168

0

1

Subnet Mask: 

255

255

255

0

Remote LAN

IP Address: 

Single PC - no Subnet

IP address:

Subnet Mask:

IKE

Direction: 

Responder only

Exchange Mode: 

Main Mode

Diffie-Hellman (DH) Group: 

Auto

Local Identity Type: 

WAN IP Address

Data:

Remote Identity Type: 

IP Address

Data:

SA Parameters

Encryption: 

3DES

Authentication: 

Auto

Pre-shared Key:

SA Life Time: 

28800

 (Seconds)

☐ Enable PFS (Perfect Forward Security)

Back

Save

Cancel

Help

Figure 59: VPN-Auto Policy Screen

Data - VPN-Auto Policy Screen

General	
Policy Name	Enter a unique name to identify this policy. This name is not supplied to the remote VPN endpoint. It is used only to help you manage the policies.
Remote VPN Endpoint	<p>If the remote endpoint has a dynamic IP address, select "Dynamic IP address". No "Address Data" input is required. Otherwise, select the desired option (IP address or Domain Name) and enter the address of the remote VPN endpoint you wish to connect to.</p> <p><b>Note:</b> The remote VPN endpoint must have this VPN Gateway's address entered as its "Remote VPN Endpoint".</p>
NetBIOS Enable	Check this if you wish NETBIOS traffic to be forwarded over the VPN tunnel. The NETBIOS protocol is used by Microsoft Networking.

Local LAN	
<b>Local LAN</b>	<p>This identifies which PCs on your LAN are covered by this policy. For each selection, data must be provided as follows:</p> <ul style="list-style-type: none"> <li>• <b>Single address</b> Enter an IP address in the "IP address" field. Typically, this setting is used when you wish to make a single Server on your LAN available to remote users.</li> <li>• <b>Subnet address</b> Enter an IP address in the "IP address" field, and the desired network mask in the "Subnet Mask" field.</li> </ul> <p>The remote VPN endpoint must have these IP addresses entered as its "Remote" addresses.</p>
Remote LAN	
<b>Remote LAN</b>	<p>This identifies which PCs on the remote LAN are covered by this policy. For each selection, data must be provided as follows:</p> <ul style="list-style-type: none"> <li>• <b>Single PC - no subnet</b> Select this option if there is no LAN (only a single PC) at the remote endpoint. If this option is selected, no additional data is required.</li> <li>• <b>Single address</b> Enter an IP address in the "IP address" field. This must be an address on the remote LAN. Typically, this setting is used when you wish to access a server on the remote LAN.</li> <li>• <b>Subnet address</b> Enter an IP address in the "IP address" field, and the desired network mask in the "Subnet Mask" field.</li> </ul> <p>The remote VPN endpoint must have these IP addresses entered as its "Local" addresses.</p>
IKE	
<b>Direction</b>	<p>This setting is used when determining if the IKE policy matches the current traffic. Select the desired option.</p> <ul style="list-style-type: none"> <li>• <b>Responder only</b> - Incoming connections are allowed, but outgoing connections will be blocked.</li> <li>• <b>Initiator and Responder</b> - Both incoming and outgoing connections are allowed.</li> </ul>
<b>Exchange Mode</b>	<p>IPSec has 2 possibilities - "Main Mode" and "Aggressive Mode". Currently, only "Main Mode" is supported. Ensure the remote VPN endpoint is set to use "Main Mode".</p>
<b>Diffie-Hellman (DH) Group</b>	<p>The Diffie-Hellman algorithm is used when exchanging keys. The DH Group setting determines the number of bit size used in the exchange. This value must match the value used on the remote VPN Gateway.</p>

<b>Local Identity Type</b>	<p>Select the desired option to match the "Remote Identity Type" setting on the remote VPN endpoint.</p> <ul style="list-style-type: none"> <li>• WAN IP Address - your Internet IP address.</li> <li>• Fully Qualified Domain Name - your domain name.</li> <li>• Fully Qualified User Name - your name, E-mail address, or other ID.</li> </ul>
<b>Local Identity Data</b>	<p>Enter the data for the selection above. (If "IP Address" is selected, no input is required.)</p>
<b>Remote Identity Type</b>	<p>Select the desired option to match the "Local Identity Type" setting on the remote VPN endpoint.</p> <ul style="list-style-type: none"> <li>• IP Address - The Internet IP address of the remote VPN endpoint.</li> <li>• Fully Qualified Domain Name - the Domain name of the remote VPN endpoint.</li> <li>• Fully Qualified User Name - the name, E-mail address, or other ID of the remote VPN endpoint.</li> </ul>
<b>Remote Identity Data</b>	<p>Enter the data for the selection above. (If "IP Address" is selected, no input is required.)</p>
<b>SA Parameters</b>	
<b>Encryption</b>	<p>Encryption Algorithm used for both IKE and IPSec. This setting must match the setting used on the remote VPN Gateway.</p>
<b>Authentication</b>	<p>Authentication Algorithm used for both IKE and IPSec. This setting must match the setting used on the remote VPN Gateway.</p>
<b>Pre-shared Key</b>	<p>The key must be entered both here and on the remote VPN Gateway. This method does not require using a CA (Certificate Authority).</p>
<b>SA Life Time</b>	<p>This determines the time interval before the SA (Security Association) expires. (It will automatically be re-established if necessary.) While using a short time period (or data amount) increases security, it also degrades performance. It is common to use periods over an hour (3600 seconds) for the SA Life Time. This setting applies to both IKE and IPSec SAs.</p>
<b>Enable PFS (Perfect Forward Secrecy)</b>	<p>If enabled, security is enhanced by ensuring that the key is changed at regular intervals. Also, even if one key is broken, subsequent keys are no easier to break. (Each key has no relationship to the previous key.)</p> <p>This setting applies to both IKE and IPSec SAs. When configuring the remote endpoint to match this setting, you may have to specify the "Key Group" used. For this device, the "Key Group" is the same as the "DH Group" setting in the IKE section.</p>

VPN- Manual Policy Screen

This screen is displayed when you click the *Add Manual Policy* button on the **VPN Policies** screen, or when you edit an existing Manual Policy. It allows you to define or edit a "Manual" VPN policy.

An "Manual" VPN policy requires that you enter all data on both VPN endpoints. There is no negotiation between the 2 VPN endpoints.

VPN - Manual Policy

General

Policy Name:

Remote VPN Endpoint

Address Type: Fixed IP Address

Address Data:

☒ NETBIOS Enable

Local LAN

IP Address Subnet address

IP address: 192 168 0 1

Subnet Mask: 255 255 255 0

Remote LAN

IP Address Single PC-no subnet

IP address:

Subnet Mask:

ESP Configuration

SPI - Incoming  (Hex, 3 Characters)

SPI - Outgoing  (Hex, 3 Characters)

Encryption 3DES

Key:

(DES: 8 chars; 3DES: 24 chars)

Authentication SHA-1

Key:

(MD5: 16 chars; SHA-1: 20 chars)

Back

Save

Cancel

Help

Figure 60: VPN-Manual Policy Screen

Data - VPN-Manual Policy Screen

General	
Policy Name	Enter a unique name to identify this policy. This name is not supplied to the remote VPN endpoint. It is used only to help you manage the policies.

<b>Remote VPN Endpoint</b>	<p>Select the desired option (IP address or Domain Name) and enter the address of the remote VPN endpoint you wish to connect to.</p> <p><b>Note:</b> The remote VPN endpoint must have this VPN Gateway's address entered as its "Remote VPN Endpoint".</p>
<b>NETBIOS Enable</b>	<p>Check this if you wish NETBIOS traffic to be forwarded over the VPN tunnel. The NETBIOS protocol is used by Microsoft Networking.</p>
<b>Local LAN</b>	
<b>Local LAN</b>	<p>This identifies which PCs on your LAN are covered by this policy. For each selection, data must be provided as follows:</p> <ul style="list-style-type: none"><li>• <b>Single address</b> Enter an IP address in the "IP address" field. Typically, this setting is used when you wish to make a single Server on your LAN available to remote users.</li><li>• <b>Subnet address</b> Enter an IP address in the "IP address" field, and the desired network mask in the "Subnet Mask" field.</li></ul> <p>The remote VPN endpoint must have these IP addresses entered as its "Remote" addresses.</p>
<b>Remote LAN</b>	
<b>Remote LAN</b>	<p>This identifies which PCs on the remote LAN are covered by this policy. For each selection, data must be provided as follows:</p> <ul style="list-style-type: none"><li>• <b>Single PC - no subnet</b> Select this option if there is no LAN (only a single PC) at the remote endpoint. If this option is selected, no additional data is required.</li><li>• <b>Single address</b> Enter an IP address in the "IP address" field. This must be an address on the remote LAN. Typically, this setting is used when you wish to access a server on the remote LAN.</li><li>• <b>Subnet address</b> Enter an IP address in the "IP address" field, and the desired network mask in the "Subnet Mask" field.</li></ul> <p>The remote VPN endpoint must have these IP addresses entered as its "Local" addresses.</p>
<b>ESP Configuration</b>	
<b>SPI</b>	<p>Enter the required SPIs. Each policy must have unique SPIs. These settings must match the remote VPN endpoint. Note that the "in" setting here must match the "out" setting on the remote VPN endpoint, and the "out" setting here must match the "in" setting on the remote VPN endpoint.</p>

<b>Encryption</b>	<p>Select the desired Encryption Algorithm, and enter the key in the field provided.</p> <ul style="list-style-type: none"><li>• For DES, the key should be 8 ASCII characters (16 Hex characters).</li><li>• For 3DES, the key should be 24 ASCII characters (48 Hex characters).</li></ul>
<b>Authentication</b>	<p>Select the desired Authentication Algorithm, and enter the key in the field provided.</p> <ul style="list-style-type: none"><li>• For MD5, the key should be 16 ASCII characters (32 Hex characters).</li><li>• For SHA-1, the key should be 20 ASCII (40 Hex characters).</li></ul>

## VPN Status Screen

This screen is displayed when you click the VPN Log button on the VPN Policies screen, or on the Status screen.

This screen allows you to view details of each current VPN Tunnel (connection). If there are no current connections, the status table will be empty.

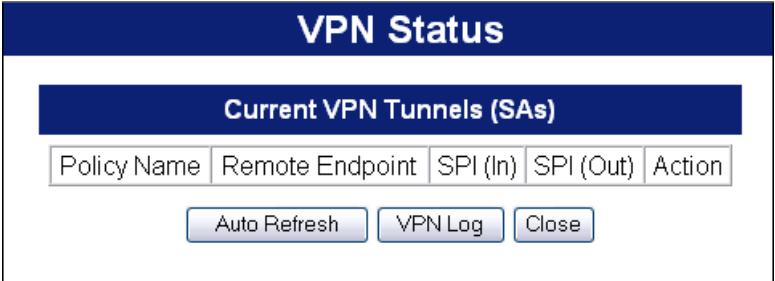


Figure 61: VPN-Status Screen

### Data - VPN Status Screen

<b>Tunnel Table</b>	<p>This table contains the following data about each current connection.</p> <ul style="list-style-type: none"><li>• <b>Policy Name</b> - The name of the policy. When a policy is created, it must be given a unique name to identify it.</li><li>• <b>Remote Endpoint</b> - The address of the remote VPN endpoint.</li><li>• <b>SPI (In)</b> - This is a unique index number to identify the incoming connection. For "Auto" policies, the SPI is automatically generated. For "Manual" policies, the SPI must be entered when the policy is configured.</li><li>• <b>SPI (Out)</b> - This is a unique index number to identify the outgoing connection. For "Auto" policies, the SPI is automatically generated. For "Manual" policies, the SPI must be entered when the policy is configured.</li><li>• <b>Action</b> - This column will contain a button which allows you to break (terminate) the current the VPN connection.</li></ul>
<b>Buttons</b>	
<b>Auto Refresh</b>	<p>Use this to Enable or Disable auto-refresh for this screen. If enabled, the screen will be updated every few seconds.</p> <p>The status bar on the bottom on the screen will indicate if auto-refresh is enabled or disabled.</p>
<b>VPN Log</b>	<p>Click this button to switch to the VPN log screen.</p> <p>The VPN log shows details of each connection as it is created.</p>

# Chapter 7

# Advanced Administration



*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:

<b>PC Database</b>	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.
<b>Config File</b>	Backup or restore the configuration file for the Wireless ADSL2/2+ Modem Router. This file contains all the configuration data.
<b>Logs &amp; Email</b>	View or clear all logs, set E-Mailing of log files and alerts.
<b>Diagnostics</b>	Perform a Ping or DNS Lookup.
<b>Qos</b>	
<b>Remote Admin</b>	Allow settings to be changed from the Internet.
<b>Routing</b>	Only required if your LAN has other Routers or Gateways.
<b>Upgrade Firmware</b>	Upgrade the Firmware (software) installed in your Wireless ADSL2/2+ Modem 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

DHCP Clients are automatically added and updated.  
If not listed, try restarting the PC.  
PCs using a Fixed IP address can be added and deleted below.

Known PCs
karen 192.168.0.2 (LAN) 00:14:85:2B:7E:14 (DHCP)

< Add

Name:   
IP Address:

Delete

Refresh Generate Report

Advanced Administration Help

**Figure 62: 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 ADSL2/2+ Modem 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

<b>Known PCs</b>	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.
<b>Name</b>	If adding a new PC to the list, enter its name here. It is best if this matches the PC's "hostname".
<b>IP Address</b>	Enter the IP Address of the PC. The PC will be sent a "ping" to determine its hardware address. If the PC is not available (not connected, or not powered On) you will not be able to add it.
<b>Buttons</b>	
<b>Add</b>	This will add the new PC to the list. The PC will be sent a "ping" to determine its hardware address. If the PC is not available (not connected, or not powered On) you will not be able to add it.
<b>Delete</b>	Delete the selected PC from the list. This should be done in 2 situations: <ul style="list-style-type: none"><li>• The PC has been removed from your LAN.</li><li>• The entry is incorrect.</li></ul>
<b>Refresh</b>	Update the data on screen.
<b>Generate Report</b>	Display a read-only list showing full details of all entries in the PC database.
<b>Advanced Administration</b>	View the Advanced version of the PC database screen - <b>PC Database (Admin)</b> . See below for details.

PC Database - Advanced

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

PC Database - Advanced

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

Known PCs

karen 192.168.0.2 (LAN) 00:14:85:2B:7E:14 (DHCP)

Edit

Delete

PC Properties

Name:

IP Address:

☐ Automatic (DHCP Client)

☒ DHCP Client - reserved IP address:

1921680

☒ Fixed IP address (set on PC):

MAC Address:

☐ Automatic discovery (PC must be available on LAN)

☒ MAC address is

Clear Form

Add as New Entry

Update Selected PC

Refresh

Generate Report

Standard Screen

Help

Figure 63: PC Database (Admin)

Data - Advanced PC Database

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.
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".

<b>IP Address</b>	<p>Select the appropriate option:</p> <ul style="list-style-type: none"> <li>• <b>Automatic</b> - The PC is set to be a DHCP client (Windows: "Obtain an IP address automatically"). The Wireless ADSL2/2+ Modem Router will allocate an IP address to this PC when requested to do so. The IP address could change, but normally won't.</li> <li>• <b>DCHP Client - Reserved IP Address</b> - Select this if the PC is set to be a DCHP client, and you wish to guarantee that the Wireless ADSL2/2+ Modem Router will always allocate the same IP Address to this PC. Enter the required IP address.</li> <li>• <b>Fixed IP Address</b> - Select this if the PC is using a Fixed (Static) IP address. Enter the IP address allocated to the PC. (The PC itself must be configured to use this IP address.)</li> </ul>
<b>MAC Address</b>	<p>Select the appropriate option</p> <ul style="list-style-type: none"> <li>• <b>Automatic discovery</b> - Select this to have the Wireless ADSL2/2+ Modem Router contact the PC and find its MAC address. This is only possible if the PC is connected to the LAN and powered On.</li> <li>• <b>MAC address is</b> - Enter the MAC address on the PC. The MAC address is also called the "Hardware Address", "Physical Address", or "Network Adapter Address". The Wireless ADSL2/2+ Modem Router uses this to provide a unique identifier for each PC. Because of this, the MAC address can NOT be left blank.</li> </ul>
<b>Buttons</b>	
<b>Add as New Entry</b>	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.
<b>Update Selected PC</b>	Update (modify) the selected PC, using the data in the "Properties" box.
<b>Clear Form</b>	Clear the "Properties" box, ready for entering data for a new PC.
<b>Refresh</b>	Update the data on screen.
<b>Generate Report</b>	Display a read-only list showing full details of all entries in the PC database.
<b>Standard Screen</b>	Click this to view the standard <b>PC Database</b> screen.

## Config File

This feature allows you to download the current settings from the Wireless ADSL2/2+ Modem Router, and save them to a file on your PC.

You can restore a previously-downloaded configuration file to the Wireless ADSL2/2+ Modem Router, by uploading it to the Wireless ADSL2/2+ Modem Router.

This screen also allows you to set the Wireless ADSL2/2+ Modem Router back to its factory default configuration. Any existing settings will be deleted.

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



Figure 64: Config File Screen

### Data - Config File Screen

<b>Backup Config</b>	Use this to download a copy of the current configuration, and store the file on your PC. Click <i>Download</i> to start the download.
<b>Restore Config</b>	<p>This allows you to restore a previously-saved configuration file back to the Wireless ADSL2/2+ Modem Router.</p> <p>Click <i>Browse</i> to select the configuration file, then click <i>Restore</i> to upload the configuration file.</p> <p><b>WARNING!</b></p> <p>Uploading a configuration file will destroy (overwrite) ALL of the existing settings.</p>
<b>Default Config</b>	<p>Clicking the <i>Factory Defaults</i> button will reset the Wireless ADSL2/2+ Modem Router to its factory default settings.</p> <p><b>WARNING!</b></p> <p>This will delete ALL of the existing settings.</p>

Logs

The Logs record various types of activity on the Wireless ADSL2/2+ Modem 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 ADSL2/2+ Modem Router, log data can also be E-mailed to your PC. Use the **E-mail** screen to configure this feature.

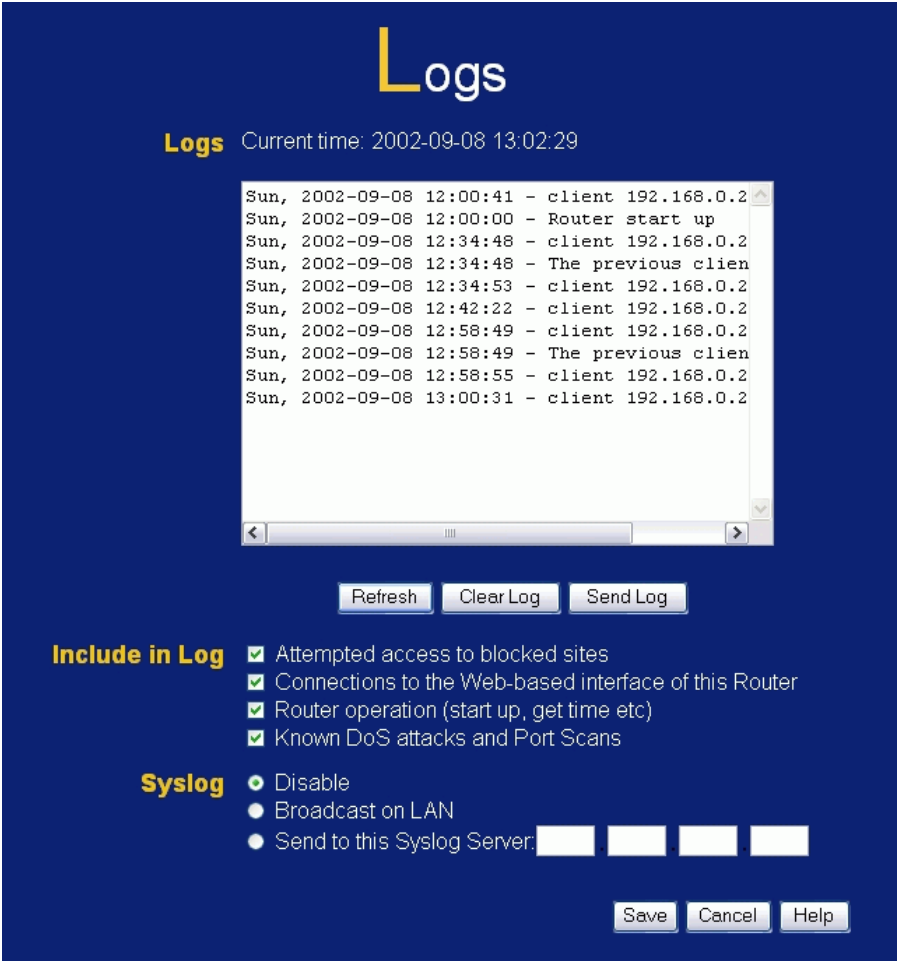


Figure 65: Logs Screen

Data - Logs Screen

Logs	
Current Time	The current time on the Wireless ADSL2/2+ Modem Router is displayed.
Log Data	Current log data is displayed in this panel.

<b>Buttons</b>	<p>There are three (3) buttons</p> <ul style="list-style-type: none"> <li>• <b>Refresh</b> - Update the log data.</li> <li>• <b>Clear Log</b> - Clear the log, and restart it. This makes new messages easier to read.</li> <li>• <b>Send Log</b> - E-mail the log immediately. This is only functional if the <b><i>E-mail</i></b> screen has been configured.</li> </ul>
<b>Logs</b>	
<b>Include (Checkboxes)</b>	<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"> <li>• <b>Attempted access to blocked sites</b> - If checked, attempted Internet accesses which were blocked are logged.</li> <li>• <b>Connections to the Web-based interface of this Router</b> - If checked, this will log connections TO this Router, rather than through this Router to the Internet.</li> <li>• <b>Router operation</b> - If checked, other Router operations (not covered by the selections above) will be logged.</li> <li>• <b>Known DoS attacks and Port Scans</b> - If checked, Denial of Service attacks, as well as port scans, will be logged.</li> </ul>
<b>Syslog</b>	
<b>Disable</b>	Data is not sent to a Syslog Server.
<b>Broadcast on LAN</b>	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.
<b>Syslog Server</b>	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.

**E-Mail**

**E-mail Notification** ☐ Turn E-mail Notification On

Send to this E-mail Address:

Outgoing (SMTP) Mail Server:

☐ My SMTP Mail Server requires authentication

User Name:

Password:

**E-mail Alerts** Send E-Mail alerts immediately

☒ If a DoS attack is detected.

☒ If a Port Scan is detected.

☒ If someone attempts to access a blocked site.

**E-mail Logs** Send Logs According to this Schedule

Hourly

Day Sunday

Time 1:00  ☒ a.m. ☐ p.m.

Figure 66: 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.
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.

<b>Password</b>	If you have enabled "My SMTP Mail Server requires authentication" above, enter the password required to login to your SMTP Server.
<b>E-mail Alerts</b>	
<b>Send E-mail alerts immediately</b>	<p>You can choose to have alerts E-mailed to you, by checking the desired checkboxes. The Broadband ADSL2/2+ Modem Router can send an immediate alert when it detects a significant security incident such as</p> <ul style="list-style-type: none"><li>• A known hacker attack is directed at your IP address</li><li>• A computer on the Internet scans your IP address for open ports</li><li>• Someone on your LAN (Local Area Network) tries to visit a blocked site.</li></ul>
<b>E-mail Logs</b>	
<b>Send Logs</b>	<p>Select the desired option for sending the log by E-mail.</p> <ul style="list-style-type: none"><li>• <b>Never</b> (default) - This feature is disabled; Logs are not sent.</li><li>• <b>When log is full</b> - The time is not fixed. The log will be sent when the log is full, which will depend on the volume of traffic.</li><li>• <b>Hourly, Daily, Weekly...</b> - The log is sent on the interval specified.<ul style="list-style-type: none"><li>• If <b>Daily</b> is selected, the log is sent at the time specified. Select the time of day you wish the E-mail to be sent.</li><li>• If <b>Weekly</b> 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.</li></ul></li></ul> <p><b>Note:</b></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.

**Network Diagnostics**

**Ping** IP Address:

**DNS Lookup** Internet Name:    
IP address:  DNS Server:

**Routing** Display the Routing Table

Figure 67: 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.

Qos

The Qos (Quality of Service) feature allows you to 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.

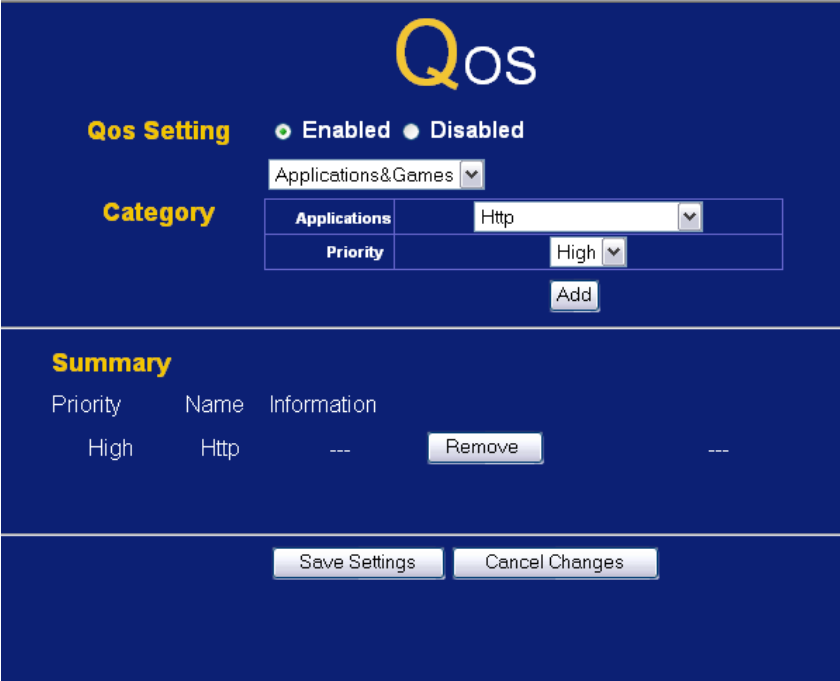


Figure 68: Qos Screen

Data - Qos Screen

Qos Setting	
Qos setting	If enabled, this feature allows you to specify priorities for different traffic.
Category	
Category	<div>Select the desired option:</div> <ul style="list-style-type: none"><li>• <b>Applications &amp; Games:</b> Select the desired applications.<ul style="list-style-type: none"><li>• Add a New Application (once selected, please complete the following setups)<ul style="list-style-type: none"><li>• Enter a Name: Enter the name for the service.</li><li>• Port Range: Enter the port range and protocol for the service here.</li></ul></li></ul></li><li>• <b>MAC Address</b><ul style="list-style-type: none"><li>• Enter a Name: Enter the name for the work station here.</li><li>• MAC Address: Enter the MAC Address for the work station.</li></ul></li></ul>

Priority	Select the desired option.
Add Button	Click this button to add the Qos setting into the summary list.
Summary	
Summary	<p>This lists the summary of your Qos setting.</p> <ul style="list-style-type: none"><li>• <b>Priority:</b> The priority of this Applications &amp; Games or MAC Address.</li><li>• <b>Name:</b> The name of this Applications &amp; Games or MAC Address.</li><li>• <b>Information:</b> The general information of this Applications &amp; Games or MAC Address.</li><li>• <b>Remove Button:</b> Click this button to remove the settings.</li></ul>

# Remote Administration

If enabled, this feature allows you to manage the Wireless ADSL2/2+ Modem Router via the Internet.

# Remote Administration

Remote Administration

Access Permission

☐ Enable Remote Management

Current IP Address:

Port Number:

Allow Remote Access By:

☒ Everyone

☐ Only This Computer:

☐ IP Address Range : From     To

Save

Cancel

Help

Figure 69: Remote Administration Screen

## Data - Remote Administration Screen

Remote Administration	
Enable Remote Management	<p>Check to allow administration/management via the Internet. (To connect, see below).</p> <p>If Disabled, this device will ignore Administration connection attempts from the Internet.</p>
Current IP Address	<p>This is the current address you will use when accessing this device from the Internet. To connect, see details and an example below.</p>
Port Number	<p>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.</p> <p>The port number must be specified in your Browser when you connect. See the following section for details.</p>
Access Permission	
Allow Remote Access	<p>Select the desired option.</p> <ul style="list-style-type: none"><li><b>Everyone</b> - allow access by everyone on the Internet.</li><li><b>Only This Computer</b> - allow access by only one IP address. Enter the desired IP address.</li><li><b>IP Address Range</b> - allow access from a range of IP addresses on the Internet. Enter a beginning and ending IP address to define the allowed range.</li></ul>

---

	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 ADSL2/2+ Modem 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 ADSL2/2+ Modem 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 ADSL2/2+ Modem 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 ADSL2/2+ Modem 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.

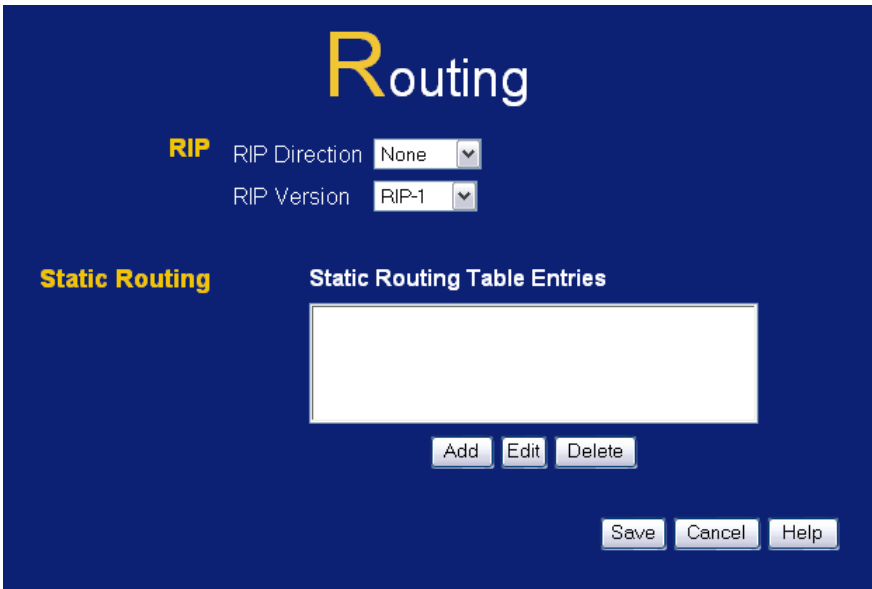


Figure 70: Routing Screen

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	<div>This list shows all entries in the Routing Table.<ul style="list-style-type: none"><li>• This area shows details of the selected item in the list.</li><li>• Change any the properties as required, then click the "Edit" button to save the changes to the selected entry.</li></ul></div>
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 ADSL2/2+ Modem 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 ADSL2/2+ Modem 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 ADSL2/2+ Modem Router. This router requires that the *Default Route* is the Wireless ADSL2/2+ Modem 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 ADSL2/2+ Modem Router.
Metric	1

Other Routers on the Local LAN

Other routers on the local LAN must use the Wireless ADSL2/2+ Modem Router's *Local Router* as the *Default Route*. The entries will be the same as the Wireless ADSL2/2+ Modem Router's local router, with the exception of the *Gateway IP Address*.

- For a router with a direct connection to the Wireless ADSL2/2+ Modem Router's local Router, the *Gateway IP Address* is the address of the Wireless ADSL2/2+ Modem Router's local router.
- For routers which must forward packets to another router before reaching the Wireless ADSL2/2+ Modem Router's local router, the *Gateway IP Address* is the address of the intermediate router.

Static Routing - Example

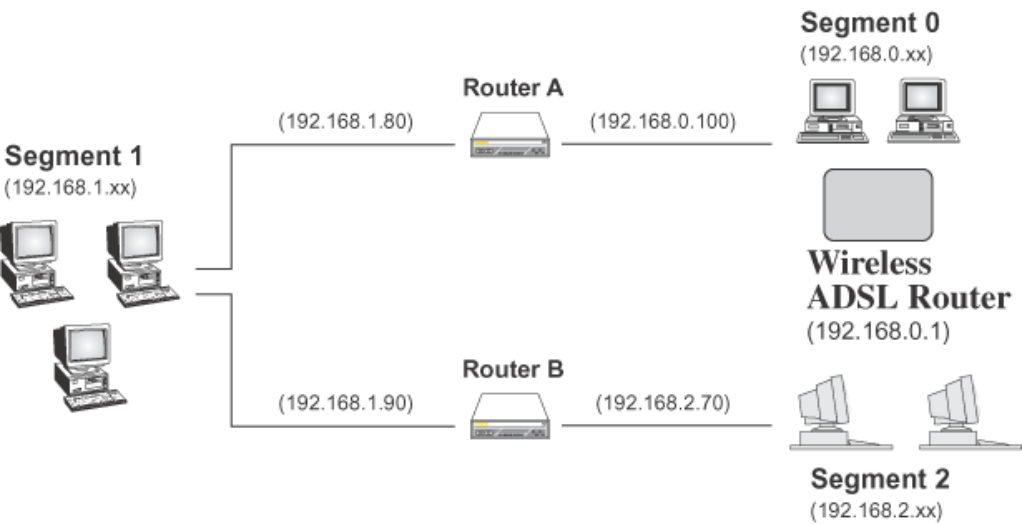


Figure 71: Routing Example

For the Wireless ADSL2/2+ Modem Router's Routing Table

For the LAN shown above, with 2 routers and 3 LAN segments, the Wireless ADSL2/2+ Modem 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 ADSL2/2+ Modem 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 ADSL2/2+ Modem Router's IP Address)

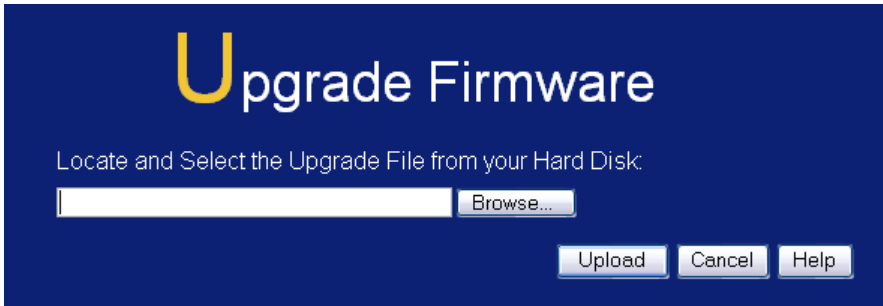
**For Router B's Default Route**

Destination IP Address	0.0.0.0
Network Mask	0.0.0.0
Gateway IP Address	192.168.1.80 (Wireless ADSL2/2+ Modem Router's local router)

## Upgrade Firmware

The firmware (software) in the Wireless ADSL2/2+ Modem Router can be upgraded using your Web Browser.

You must first download the upgrade file, then select *Upgrade Firmware* on the *Administration* menu. You will see a screen like the following.



The image shows a web browser interface for upgrading the router's firmware. The background is dark blue. At the top, the text "Upgrade Firmware" is displayed in a large, white, sans-serif font, with the "U" being a larger, yellow-outlined letter. Below this, in a smaller white font, is the instruction "Locate and Select the Upgrade File from your Hard Disk:". Underneath the instruction is a white text input field. To the right of the input field is a button labeled "Browse...". At the bottom right of the interface are three buttons: "Upload", "Cancel", and "Help", all in a light blue color with white text.

**Figure 72: 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.



**Note!**

**The Wireless ADSL2/2+ Modem Router is unavailable during the upgrade process, and must restart when the upgrade is completed. Any connections to or through the Wireless ADSL2/2+ Modem Router will be lost.**

## Chapter 8

# Modem Mode



*This Chapter explains configuration and operation when in "Modem" or "Bridge" mode..*

### Overview

There are two modes available on the **Mode** screen.

- **Router** - Both the ADSL Modem and the Router features are operational. 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.
- **Modem** - Only the ADSL Modem component is operational. All Router features are disabled. This device is "transparent" - it does not perform any operations or make any changes to the network traffic passing through it. You need to have a DHCP Server on your LAN to provide IP addresses to the Wireless clients using this Access Point.

This Chapter describes operation while in **Modem Mode**, also called **Bridge Mode**.

### Management Connections

When this device restarts in Modem mode, the IP address does not change, but the DHCP server is disabled. However, your PC will usually retain the IP address provided by the DHCP Server, so the connection will be automatically re-established. You then need to ensure that the IP address of this modem is suitable for your LAN.

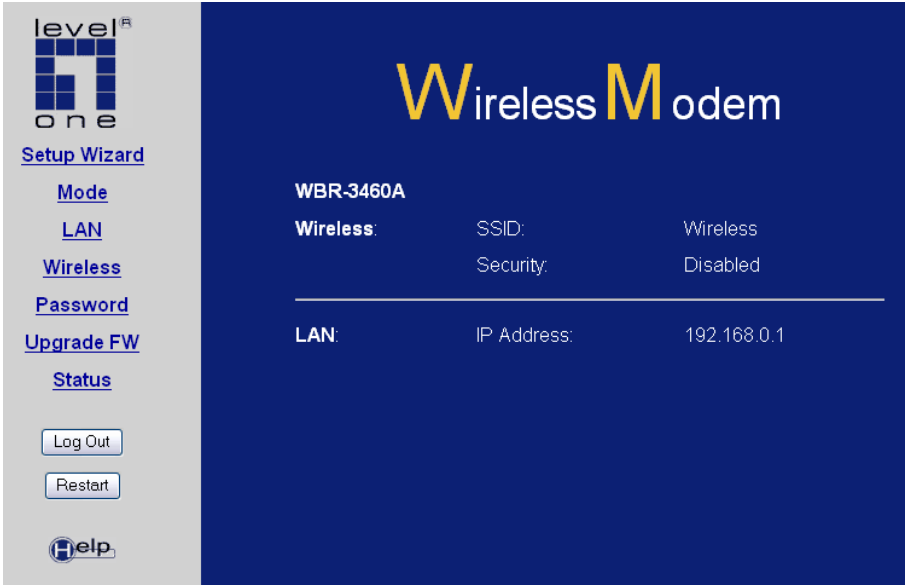
- You need to have a DHCP Server on your LAN to provide IP addresses to the Wireless clients using this Access Point.
- This Modem/AP must be a valid device on your LAN, to allow management connections. You must assign a (fixed) IP address which is within the address range used on your LAN, but not within 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 ADSL Modem, as in this example, which uses the Wireless ADSL Modem's 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. (The password is the same regardless of the mode.)

## Home Screen

If in Modem mode, the home screen will look like the example below.



**Figure 73: Home Screen - Modem Mode**

Note that the menu has changed, many of the options in Router mode are not available. The screens available are:

- **Mode** - change back to Router mode, if desired.
- **LAN** - set IP address, mask and gateway. This is the same as in Router mode, except that the DHCP server is not available while in Modem mode.
- **Wireless** - this screen, and related sub-screens, is the same as in Router mode.
- **Password** - this screen is the same as in Router mode.
- **Upgrade Firmware** - this screen is the same as in Router mode.
- **Status** - displays current settings and status. See the following section for details.

## Mode Screen

This screen is change back to Router mode, if desired.

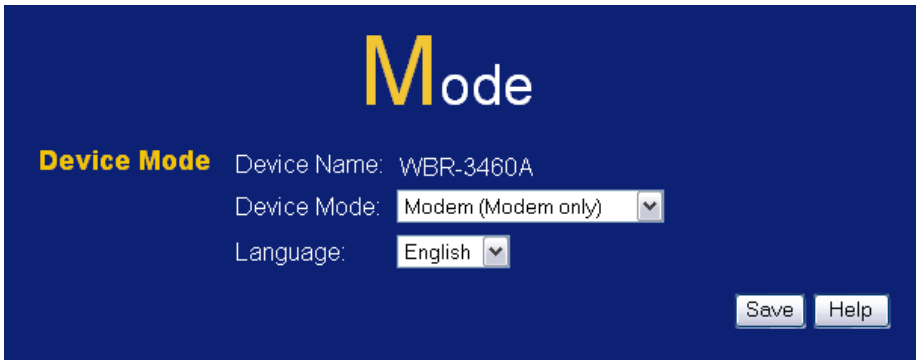


Figure 74: Mode Screen

### 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"><li>• <b>Router</b> - Both the ADSL Modem and the Router features are operational. 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.</li><li>• <b>Modem</b> - Only the ADSL Modem component is operational. All Router features are disabled. This device is "transparent" - it does not perform any operations or make any changes to the network traffic passing through it. You need to have a DHCP Server on your LAN to provide IP addresses to the Wireless clients using this Access Point. This mode is also called <b>Bridge Mode</b>.</li></ul> <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>
Language	Select the desired option from the drop-down list.

## Operation

Operation is automatic and transparent.

- 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.
- The modem will act like any other ADSL modem. No routing will be performed, and no client login will be done. If a client login is required, it must be performed by your Router/Gateway or by software on your PC.

## Status Screen

In Modem mode, the Status screen looks like the example below.

# Status - Bridge Mode

**ADSL**

Modem Status

Connecting

DownStream Connection Speed

0 kbps

UpStream Connection Speed

0 kbps

VC 1 Status

Enabled

VC 2 Status

Disabled

VC 3 Status

Disabled

VC 4 Status

Disabled

ADSL Details

**LAN**

IP Address:

192.168.0.1

Network Mask:

255.255.255.0

MAC Address

00:C0:02:90:AC:10

**Wireless**

Name (SSID)

Wireless

Region

Europe

Channel

3

Wireless AP

enable

Broadcast Name

enable

**System**

Device Name:

WBR-3460A

Firmware Version:

1.00.01

Attached Devices

Refresh Screen

Help

Figure 75: Status Screen - Bridge Mode

### Data - Status Screen (Bridge Mode)

ADSL	
Modem Status	This indicates the status of the ADSL modem component.
DownStream Connection Speed	Displays the speed for the DownStream Connection.
UpStream Connection Speed	If connected, displays the speed for the Up Stream (upload) ADSL Connection.

<b>VC 1 Status</b> <b>VC 2 Status</b> <b>VC 3 Status</b> <b>VC 4 Status</b>	For each VC (Virtual Circuit), the current status is displayed. This will be either "Enabled" or "Disabled".
<b>ADSL Details</b>	Click this button to open a sub-window and view the details of each VC (Virtual Circuit).
<b>LAN</b>	
<b>IP Address</b>	The IP Address of the Wireless ADSL2/2+ Modem Router.
<b>Network Mask</b>	The Network Mask (Subnet Mask) for the IP Address above.
<b>MAC Address</b>	This shows the MAC Address for the Wireless ADSL2/2+ Modem Router, as seen on the LAN interface.
<b>Wireless</b>	
<b>Name (SSID)</b>	If using an ESS (Extended Service Set, with multiple access points) this ID is called an ESSID (Extended Service Set Identifier).
<b>Region</b>	The current region, as set on the Wireless screen.
<b>Channel</b>	This shows the Channel currently used, as set on the Wireless screen.
<b>Wireless AP</b>	This indicates whether or not the Wireless Access Point feature is enabled.
<b>Broadcast Name</b>	This indicates whether or not the SSID is Broadcast. This setting is on the Wireless screen.
<b>System</b>	
<b>Device Name</b>	The current name of the Router. This name is also the "hostname" for users with an "@Home" type connection.
<b>Firmware Version</b>	The version of the current firmware installed.
<b>Buttons</b>	
<b>ADSL Details</b>	View the details of each VC (Virtual Circuit).
<b>Attached Devices</b>	Clicking this will generate a list of all devices currently using the Access Point.
<b>Refresh Screen</b>	Update the data displayed on screen.

# 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 ADSL2/2+ Modem Router and some possible solutions to them. If you follow the suggested steps and the Wireless ADSL2/2+ Modem Router still does not function properly, contact your dealer for further advice.

### General Problems

**Problem 1:** Can't connect to the Wireless ADSL2/2+ Modem Router to configure it.

**Solution 1:** Check the following:

- The Wireless ADSL2/2+ Modem Router is properly installed, LAN connections are OK, and it is powered ON.
- Ensure that your PC and the Wireless ADSL2/2+ Modem 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 ADSL2/2+ Modem 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 ADSL2/2+ Modem 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 ADSL2/2+ Modem 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 ADSL2/2+ Modem Router's status screen to

see if it is working correctly.

**Problem 2: Some applications do not run properly when using the Wireless ADSL2/2+ Modem Router.**

**Solution 2:** The Wireless ADSL2/2+ Modem 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 ADSL2/2+ Modem Router must have the same setting for WEP. The default setting for the Wireless ADSL2/2+ Modem Router is disabled, so your wireless station should also have WEP disabled.
- If WEP is enabled on the Wireless ADSL2/2+ Modem Router, your PC must have WEP enabled, and the key must match.
- If the Wireless ADSL2/2+ Modem 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 ADSL2/2+ Modem 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 ADSL2/2+ Modem Router location.  
Try adjusting the location and orientation of the Wireless ADSL2/2+ Modem 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 ADSL2/2+ Modem 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:**

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

## WPA-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:**

<b>WPA PSK (Pre-shared Key)</b>	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.
<b>Encryption</b>	The same encryption method must be used. The most common encryption method is TKIP. Another widely-supported method is AES.

# Wireless LAN Configuration

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

<b>Mode</b>	On client Wireless Stations, the mode must be set to "Infrastructure". (The Access Point is always in "Infrastructure" mode.)
<b>SSID (ESSID)</b>	Wireless Stations should use the same SSID (ESSID) as the Access Point they wish to connect to. Alternatively, the SSID can be set to "any" or null (blank) to allow connection to any Access Point.
<b>Wireless Security</b>	<p>The Wireless Stations and the Access Point must use the same settings for Wireless security. (None, WEP, WPA-PSK).</p> <p><b>WEP:</b> If WEP is used, the Key size (64Bit, 128Bit), Key value, and Authentication settings must be the same on the Wireless Stations and the Access Point.</p> <p><b>WPA-PSK:</b> If WPA-PSK is used, all Wireless Stations must be set to use WPA-PSK, and have the same Pre-shared Key and encryption system.</p> <p>For <b>Ad-hoc networks</b> (no Access Point), all Wireless stations must use the same security settings.</p>

# Appendix C

## About VPNs



### Overview

A VPN (Virtual Private Network) provides a secure connection between 2 points, over an insecure network - typically the Internet. This secure connection is called a **VPN Tunnel**.

There are many standards and protocols for VPNs. The standard implemented in the Wireless ADSL2/2+ Modem Router is **IPSec**.

### IPSec

IPSec is a near-ubiquitous VPN security standard, designed for use with TCP/IP networks. It works at the packet level, and authenticates and encrypts all packets traveling over the VPN Tunnel. Thus, it does not matter what applications are used on your PC. Any application can use the VPN like any other network connection.

IPsec VPNs exchange information through logical connections called **SAs** (Security Associations). An SA is simply a definition of the protocols, algorithms and keys used between the two VPN devices (endpoints).

Each IPsec VPN has two SAs - one in each direction. If **IKE** (Internet Key Exchange) is used to generate and exchange keys, there are also SA's for the IKE connection as well as the IPsec connection.

There are two security modes possible with IPSec:

- **Transport Mode** - the payload (data) part of the packet is encapsulated through encryption but the IP header remains in the clear (unchanged).

**The Wireless ADSL2/2+ Modem Router does NOT support Transport Mode.**

- **Tunnel Mode** - everything is encapsulated, including the original IP header, and a new IP header is generated. Only the new header is in the clear (i.e. not protected). This system provides enhanced security.

**The Wireless ADSL2/2+ Modem Router always uses Tunnel Mode.**

### IKE

IKE (Internet Key Exchange) is an optional, but widely used, component of IPSec. IKE provides a method of negotiating and generating the keys and IDs required by IPSec. If using IKE, only a single key is required to be provided during configuration. Also, IKE supports using **Certificates** (provided by CAs - Certification Authorities) to authenticate the identity of the remote user or gateway.

If IKE is NOT used, then all keys and IDs (SPIs) must be entered manually, and Certificates can NOT be used. This is called a "Manual Key Exchange".

When using IKE, there are 2 phases to creating the VPN tunnel:

- **Phase I** is the negotiation and establishment up of the IKE connection.
- **Phase II** is the negotiation and establishment up of the IPsec connection.

Because the IKE and IPsec connections are separate, they have different SAs (security associations).

## Policies

VPN configuration settings are stored in **Policies**.

Note that different vendors use different terms. Generally, the terms "VPN Policy", "IPSec Policy", and "IPSec Proposal" have the same meaning. However, some vendors separate IKE Policies (Phase 1 parameters) from IPSec Policies (Phase 2 parameters).

For the Wireless ADSL2/2+ Modem Router; each VPN policy contains both Phase 1 and Phase 2 parameters (if IKE is used). Each policy defines:

- The address of the remote VPN endpoint
- The traffic which is allowed to use the VPN connection.
- The parameters (settings) for the IPsec SA (Security Association)
- If IKE is used, the parameters (settings) for the IKE SA (Security Association)

Generally, you will need at least one (1) VPN Policy for each remote site for which you wish to establish VPN connections.

It is possible, and sometimes necessary, to have multiple Policies for the same remote site. However, you should only Enable one (1) policy at a time.

## VPN Configuration

The general rule is that each endpoint must have matching Policies, as follows:

**VPN Endpoint address**

Each VPN endpoint must be configured to initiate or accept connections to the remote VPN client or Gateway.

Usually, this requires having a fixed Internet IP address. However, it is possible for a VPN Gateway to accept incoming connections from a remote client where the client's IP address is not known in advance.

**Local & Remote LAN definition**

This determines which outgoing traffic will cause a VPN connection to be established, and which incoming traffic will be accepted. Each endpoint must be configured to pass and accept the desired traffic from the remote endpoint.

If connecting 2 LANs, this requires that:

- Each endpoint must be aware of the IP addresses used on the other endpoint.
- The 2 LANs MUST use different IP address ranges.

**IKE parameters**

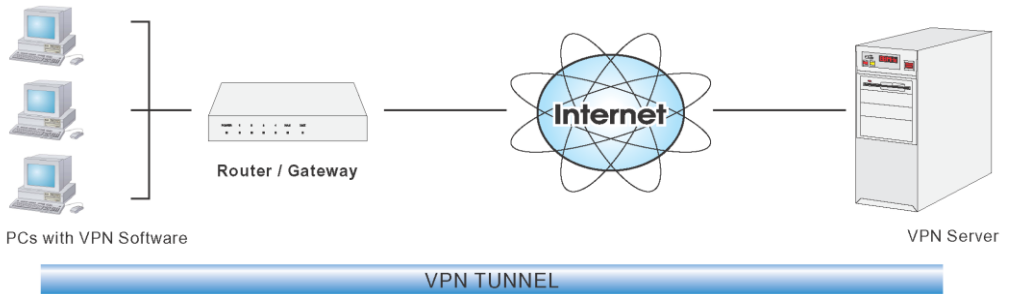
If using IKE (recommended), the IKE parameters must match (except for the SA lifetime, which can be different).

**IPsec parameters**

The IPsec parameters at each endpoint must match.

## Common VPN Situations

### VPN Pass-through

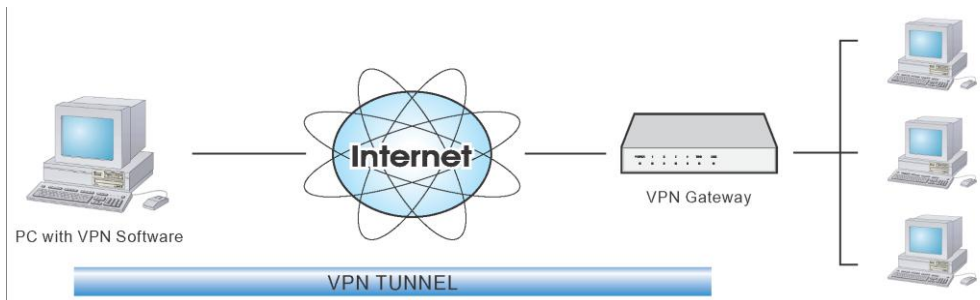


**Figure 76: VPN Pass-through**

Here, a PC on the LAN behind the Router/Gateway is using VPN software, but the Router/Gateway is NOT acting as a VPN endpoint. It is only allowing the VPN connection.

- The PC software can use any VPN protocol supported by the remote VPN.
- The remote VPN Server must support client PCs which are behind a NAT router, and so have an IP address which is not valid on the Internet.
- The Router/Gateway requires no VPN configuration, since it is not acting as a VPN endpoint.

### Client PC to VPN Gateway

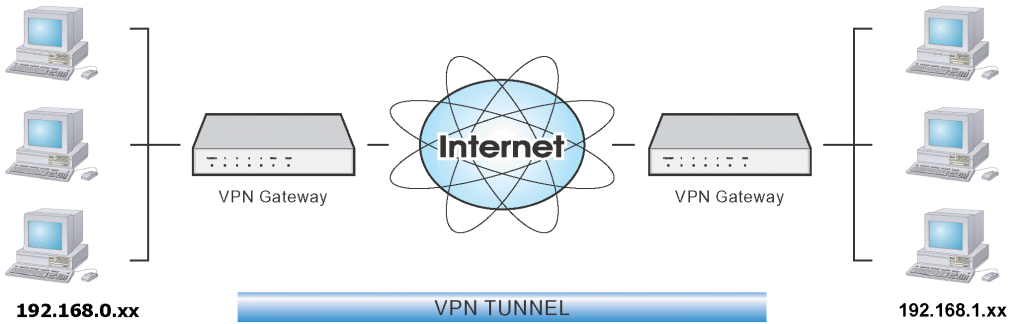


**Figure 77: Client PC to VPN Server**

In this situation, the PC must run appropriate VPN client software in order to connect, via the Internet, to the Wireless ADSL2/2+ Modem Router or other VPN Gateway. Once connected, the client PC has the same access to LAN resources as PCs on the local LAN (unless restricted by the network administrator).

- IPsec is not the only protocol which can be used in this situation, but the Wireless ADSL2/2+ Modem Router supports IPsec ONLY.
- Windows 2000 and Windows XP include an IPsec VPN client program. However, configuration of this client program for use with the Wireless ADSL2/2+ Modem Router is very complex and beyond the scope of this document.

## Connecting 2 LANs via VPN



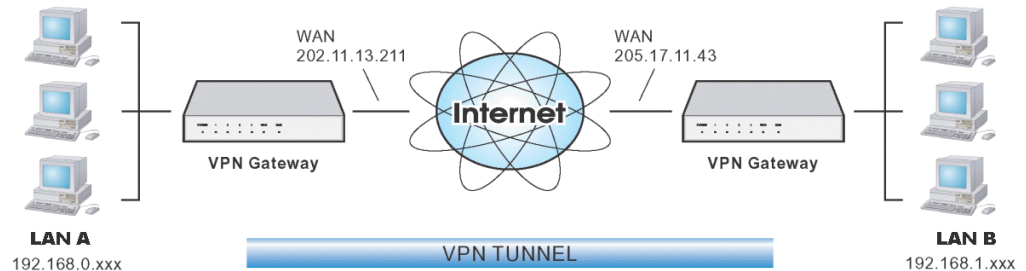
**Figure 78: Connecting 2 VPN Gateways**

This allows two (2) LANs to be connected. PCs on each endpoint gain secure access to the remote LAN.

- The 2 LANs **MUST** use different IP address ranges.
- The VPN Policies at each end determine when a VPN tunnel will be established, and what systems on the remote LAN can be accessed once the VPN connection is established.
- It is possible to have simultaneous VPN connections to many remote sites.

## VPN Example

In this example, 2 LANs are connected via VPN. Each end has a Wireless ADSL2/2+ Modem Router.



**Figure 79: Connecting 2 Wireless ADSL2/2+ Modem Routers**

### Note

- The LANs **MUST** use different IP address ranges.
- Both endpoints have fixed WAN (Internet) IP addresses.
- This example uses an "Auto" policy, using IKE

Configuration Settings - Gateway A

Gateway A should be configured as shown below.

VPN - Auto Policy

General

Policy Name:

Remote VPN Endpoint

Address Type:

Address Data:

☒ NetBIOS Enable

Local LAN

IP Address

IP address:

Subnet Mask:

Remote LAN

IP Address

IP address:

Subnet Mask:

IKE

Direction

Exchange Mode

Diffie-Hellman (DH) Group

Local Identity Type

Data

Remote Identity Type

Data

SA Parameters

Encryption:

Authentication:

Pre-shared Key:

SA Life Time:  (Seconds)

☐ Enable PFS (Perfect Forward Security)

Back

Save

Cancel

Help

Figure 80: Gateway A Configuration

## Configuration Settings - Gateway B

Gateway B should be configured as shown below.

**VPN - Auto Policy**

**General** Policy Name:   
Remote VPN Endpoint  
Address Type:   
Address Data:   
☒ NetBIOS Enable

**Local LAN** IP Address   
IP address:      
Subnet Mask:

**Remote LAN** IP Address   
IP address:      
Subnet Mask:

**IKE** Direction:   
Exchange Mode:   
Diffie-Hellman (DH) Group:   
Local Identity Type:   
Data:   
Remote Identity Type:   
Data:

**SA Parameters** Encryption:   
Authentication:   
Pre-shared Key:   
SA Life Time:  (Seconds)  
☒ Enable PFS (Perfect Forward Security)

Figure 81: Gateway B Configuration

### Settings

Setting	LAN A Gateway	LAN B Gateway	Notes
Policy Name	Example	Example	Name does not affect operation. Select a meaningful name.
Remote VPN Endpoint	Fixed IP Address 205.17.11.43	Fixed IP Address 202.11.13.211	Other endpoint's WAN (Internet) IP address.
NetBIOS	Enable	Enable	Disable if not required.
Local LAN	192.168.0.0	192.168.1.0	Local Address subnet.

IP address Mask	255.255.255.0	255.255.255.0	Use a more restrictive definition if possible.
Remote LAN IP address Mask	192.168.1.0 255.255.255.0	192.168.0.0 255.255.255.0	Remote Address subnet. Use a more restrictive definition if possible.

**IKE**

Direction	Initiator & res-ponder	Initiator & res-ponder	Does not have to match. Either endpoint can block 1 direction.
Exchange mode	Main Mode	Main Mode	Must match
DH Group	Group 2 (1024 bit)	Group 2 (1024 bit)	Must match
Local Identity	IP address	IP address	IP address is the most common ID method
Remote Identity	WAN IP address	WAN IP address	IP address is the most common ID method

**SA Parameters**

Encryption	3DES	3DES	Must match.
Authentication	MD5	MD5	Must match
Pre-shared Key	xxxxxxxxx	xxxxxxxxx	Must match; use any string.
SA Life time	28800	28800	Does not have to match. Shorter period will be used.
PFS	Disabled	Disabled	Must match

**Note:**

Some VPN Gateways or programs let you specify the following settings separately for IKE and IPSec. For this device, the same settings are used for both IKE and IPSec.

- Authentication
- Encryption
- SA Lifetime

Also, IPSec allows for "AH Authentication", using MD5 or SHA-1. For this device, "AH Authentication" is always DISABLED.

# Appendix D

## Specifications



### Multi-Function Wireless ADSL2/2+ Modem Router

Model	Wireless ADSL2/2+ Modem Router
ADSL Interface	T1.413, G.DMT, G.lite, multi-mode
Dimensions	175mm(W) * 114mm(D) * 30mm(H)
Operating Temperature	0° C to 40° C
Storage Temperature	-10° C to 70° C
Network Protocol:	TCP/IP
Network Interface:	4 * 10/100BaseT (RJ45) LAN connection 1 * RJ11 for ADSL line
LEDs	13
Power Adapter	12VDC 1A External

### Wireless Interface

Standards	IEEE802.11b, IEEE802.11g WLAN, 802.11G-plus (Texas Instruments proprietary enhanced mode)
Frequency	2.4 to 2.4835GHz (Industrial Scientific Medical Band )
Channels	Maximum 14 Channels, depending on regulatory authorities
Modulation	CCK, DQPSK, DBPSK, OFDM/CCK
Data Rate	Up to 54 Mbps (802.11g)
Security	WEP 64Bit, 128Bit, WPA-PSK, MAC address checking
Output Power	13dBm (typical)
Receiver Sensitivity	-80dBm Min.

## Regulatory Approvals

### FCC Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.

This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

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

To assure continued compliance, any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment. (Example - use only shielded interface cables when connecting to computer or peripheral devices).

### FCC Radiation Exposure Statement

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

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

- (1) This device may not cause harmful interference, and
- (2) This device must accept any interference received, including interference that may cause undesired operation.

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

### CE Approval

#### CE Standards

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

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

## CE Marking Warning

Hereby, Digital Data Communications, declares that this (Model-no. WBR-3460) 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.