

# Wireless Router

---

AT-WA1004G



# User's Guide

PN 613-50578-00 Rev A



Simply connecting the  world

Copyright © 2004 Allied Telesyn, Inc.

All rights reserved. No part of this publication may be reproduced without prior written permission from Allied Telesyn, Inc.

Windows 95, Windows 98, Windows 2000, Windows Me, Windows NT and Windows XP are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Netscape and the Netscape N and Ship's Wheel logos are registered trademarks of Netscape Communications Corporation in the U.S. and other countries. Netscape Navigator is also a trademark of Netscape Communications Corporation and may be registered outside the U.S.

All other product names, company names, logos or other designations mentioned herein are trademarks or registered trademarks of their respective owners.

Allied Telesyn, Inc. reserves the right to make changes in specifications and other information contained in this document without prior written notice. The information provided herein is subject to change without notice. In no event shall Allied Telesyn, Inc. be liable for any incidental, special, indirect, or consequential damages whatsoever, including but not limited to lost profits, arising out of or related to this manual or the information contained herein, even if Allied Telesyn, Inc. has been advised of, known, or should have known, the possibility of such damages.

# Table of Contents

---

<b>Preface</b> .....	7
How This Guide is Organized .....	8
Document Conventions .....	9
Where to Find Related Guides .....	10
Contacting Allied Telesyn .....	11
Online Support .....	11
E-mail and Telephone Support .....	11
Returning Products.....	11
For Sales or Corporate Information .....	11
Obtaining Management Software Updates .....	11
Tell Us What You Think.....	11
<b>Chapter 1</b>	
<b>Introduction</b> .....	13
Overview .....	14
Wireless Router Features .....	15
Internet Access Features.....	15
Advanced Internet Functions .....	15
Wireless Features.....	16
LAN Features.....	16
Configuration and Management .....	17
Security Features .....	17
Package Contents .....	18
Physical Details .....	19
Front Panel LEDs.....	19
Back Panel Ports.....	20
<b>Chapter 2</b>	
<b>Installation</b> .....	23
Requirements .....	24
Procedure .....	25
<b>Chapter 3</b>	
<b>Setup</b> .....	27
Overview .....	28
Configuration Program .....	30
Preparation .....	30

Setup Wizard .....	32
Common Connection Types .....	33
Home Screen .....	35
LAN Screen .....	37
DHCP .....	38
Wireless Screen .....	40
WEP Screen .....	43
WPA-PSK .....	45
Password Screen .....	46
<b>Chapter 4</b>	
<b>PC Configuration</b> .....	47
Overview .....	48
Windows Clients .....	49
TCP/IP Settings Overview .....	49
Checking TCP/IP Settings .....	50
For Windows 9x/ME .....	50
For Windows NT4.0 .....	51
For Windows 2000 .....	55
For Windows XP .....	57
Internet Access .....	59
Macintosh Clients .....	61
Linux Clients .....	62
Other Unix Systems .....	63
Wireless Station Configuration .....	64
<b>Chapter 5</b>	
<b>Operation and Status</b> .....	65
Operation .....	66
Status Screen .....	67
Connection Status - PPPoE .....	69
Connection Status - PPTP .....	72
Connection Status - L2TP .....	73
Connection Status - Telstra Big Pond .....	74
Connection Details - SingTel RAS .....	76
Connection Details - Fixed/Dynamic IP Address .....	78
<b>Chapter 6</b>	
<b>Advanced Features</b> .....	81
Overview .....	82
Access Control .....	83
Overview .....	83
Access Control Screen .....	83
Group Members Screen .....	86
Default Schedule Screen .....	86
Services Screen .....	88
Access Control Log .....	89
Dynamic DNS (Domain Name Server) .....	90
Dynamic DNS Screen .....	91
Advanced Internet Screen .....	93
Communication Applications .....	94
Special Applications .....	94
Special Applications Screen .....	94
Using a Special Application .....	96
Multi-DMZ .....	96

Virtual Servers .....	98
IP Address Seen by Internet Users.....	98
Virtual Servers Screen .....	99
Defining Your Own Virtual Servers .....	101
Connecting to the Virtual Servers .....	101
<b>Chapter 7</b>	
<b>Advanced Administration</b> .....	103
Overview .....	104
Logs .....	105
Options .....	108
PC Database .....	112
PC Database Screen.....	112
PC Database (Admin).....	114
Remote Management .....	117
Routing .....	119
Overview.....	119
Routing Screen.....	119
Configuring Other Routers on your LAN .....	122
Security .....	123
Upgrade .....	125
<b>Appendix A</b>	
<b>Troubleshooting</b> .....	127
Overview .....	128
General Problems .....	129
Internet Access .....	130
Wireless Access .....	131
<b>Appendix B</b>	
<b>About Wireless LANs</b> .....	133
Modes .....	134
Ad-hoc Mode .....	134
Infrastructure Mode.....	134
BSS/ESS .....	135
BSS .....	135
ESS.....	135
Channels .....	136
WEP .....	137
Wireless LAN Configuration .....	138
<b>Appendix C</b>	
<b>Specifications</b> .....	139
Multi-Function Wireless Router .....	140
Wireless Interface .....	141
Regulatory Approvals .....	142
CE Standards .....	142
CE Marking Warning.....	142



# Preface

---

This installation guide contains instructions on how to use and install an Allied Telesyn AT-WA1004G Wireless Router.

## How This Guide is Organized

---

This guide contains the following chapters and appendix:

Chapter 1, [Introduction](#), provides an overview of the Wireless Router's features and capabilities.

Chapter 2, [Installation](#), contains instructions on how install the wireless router.

Chapter 3, [Setup](#), describes the setup procedure for internet access, LAN LAN configuration, wireless setup, assigning a password to protect the configuration data.

Chapter 4, [PC Configuration](#), contains the procedures for configuring TCP/IP, internet access, and wireless station.

Chapter 5, [Operation and Status](#), displays each screen and provides detailed information for each parameter.

Chapter 6, [Advanced Features](#), contains information on the advanced features of the wireless router.

Chapter 7, [Advanced Administration](#), displays the advance administration screens and defines each parameter.

Appendix A, [Troubleshooting](#), covers likely problems and their solutions.

Appendix B, [About Wireless LANs](#), provides some background information about using Wireless LANs (WLANs).

Appendix C, [Specifications](#), contains the specification information for the wireless router, wireless interface, and the regulatory approvals.

## Document Conventions

---

This guide uses several conventions that you should become familiar with before you begin to install the product.

---

**Note**

Notes provide additional information.

---

**Warning**

Warnings inform you that performing or omitting a specific action may result in bodily injury.

---

**Caution**

Cautions inform you that performing or omitting a specific action may result in equipment damage or loss of data.

---

## **Where to Find Related Guides**

---

The Allied Telesyn web site at [www.alliedtelesyn.com](http://www.alliedtelesyn.com) offers you an easy way to access the most recent documentation, software updates, and technical information for all of our products. The documents provided on our web site are available as PDF files.

## Contacting Allied Telesyn

---

This section provides Allied Telesyn contact information for technical support as well as sales or corporate information.

### Online Support

You can request technical support online by accessing the Allied Telesyn Knowledge Base from the following web site at **[www.kb.alliedtelesyn.com](http://www.kb.alliedtelesyn.com)**. You can use the Knowledge Base to submit questions to our technical support staff and review answers to previously asked questions.

### E-mail and Telephone Support

For Technical Support via e-mail or telephone, refer to the "Support & Services" section of the Allied Telesyn web site at **[www.alliedtelesyn.com](http://www.alliedtelesyn.com)**.

### Returning Products

Products for return or repair must first be assigned a Return Materials Authorization (RMA) number. A product sent to Allied Telesyn without a RMA number will be returned to the sender at the sender's expense.

To obtain a RMA number, contact Allied Telesyn's Technical Support at our web site at **[www.alliedtelesyn.com](http://www.alliedtelesyn.com)**

### For Sales or Corporate Information

You can contact Allied Telesyn for sales or corporate information at our web site at **[www.alliedtelesyn.com](http://www.alliedtelesyn.com)**. To find the contact information for your country, select "Contact Us" then "Worldwide Contacts".

### Obtaining Management Software Updates

New releases of management software for our managed products can be downloaded from either of the following Internet sites:

- Allied Telesyn web site: **[www.alliedtelesyn.com](http://www.alliedtelesyn.com)**
- Allied Telesyn FTP server: **<ftp://ftp.alliedtelesyn.com>**

If you would prefer to download new software from the Allied Telesyn FTP server from your workstation's command prompt, you will need FTP client software and you will be asked to log in to the server. Enter 'anonymous' as the user name and your e-mail address for the password.

### Tell Us What You Think

If you have any comments or suggestions on how we might improve this or other Allied Telesyn documents, please fill out the General Enquiry Form online. This form can be accessed by selecting "Contact Us" from **[www.alliedtelesyn.com](http://www.alliedtelesyn.com)**.



# Chapter 1

# Introduction

---

This chapter provides an overview of the Wireless Router's features and capabilities. This chapter contains the following sections:

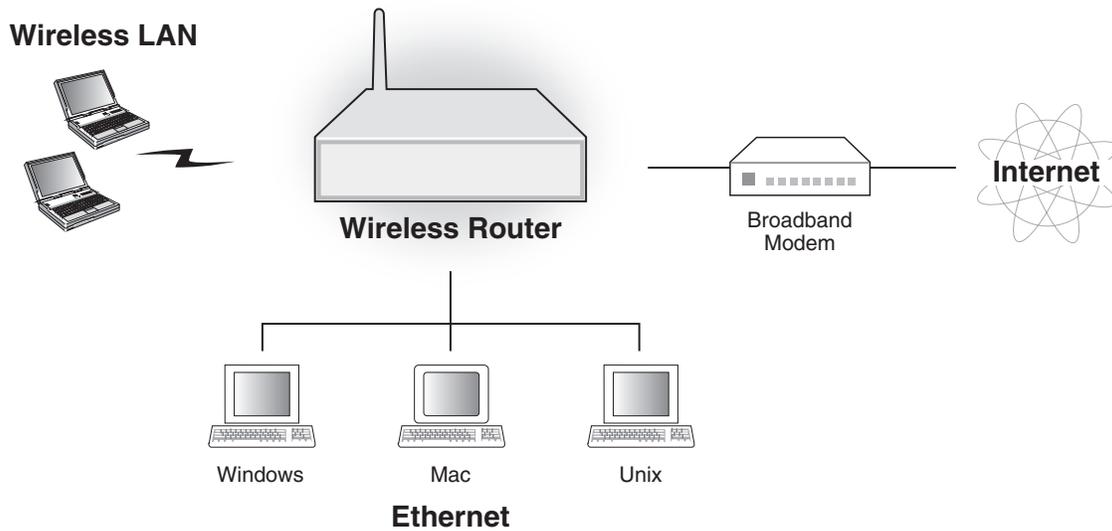
- ❑ [Overview](#) on page 14
- ❑ [Wireless Router Features](#) on page 15
- ❑ [Package Contents](#) on page 18
- ❑ [Physical Details](#) on page 19

## Overview

---

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

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



**Figure 1** Wireless Router

## Wireless Router Features

---

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

### Internet Access Features

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

### Advanced Internet Functions

- Communication Applications. Support for Internet communication applications, such as interactive Games, Telephony, and Conferencing applications, which are often difficult to use when behind a Firewall, is included.
- Special Internet Applications. 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.
- Virtual Servers. This feature allows Internet users to access Internet servers on your LAN. The required setup is quick and easy.
- Multi-DMZ. For each WAN (Internet) IP address allocated to you, one PC on your local LAN can be configured to allow unrestricted 2-way communication with Servers or individual users on the Internet. This provides the ability to run programs which are incompatible with Firewalls.
- URL Filter. Use the URL Filter to block access to undesirable Web sites by LAN users.

- ❑ Internet Access Log. See which Internet connections have been made.
- ❑ Access Control. Using the Access Control feature, you can assign LAN users to different groups, and determine which Internet services are available to each group.
- ❑ VPN Pass through Support. PCs with VPN (Virtual Private Networking) software using PPTP, L2TP, and IPSec are transparently supported - no configuration is required.

## **Wireless Features**

- ❑ Standards Compliant. The Wireless 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 54 Mbps. All speeds up to the 802.11g maximum of 54 Mbps are supported.
- ❑ WEP support. Support for WEP (Wired Equivalent Privacy) is included. Key sizes of 64-bit and 128-bit are supported.
- ❑ 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 Router incorporates a 4-port 10/100Base-T switching hub, making it easy to create or extend your LAN.
- ❑ DHCP Server Support. Dynamic Host Configuration Protocol provides a dynamic IP address to PCs and other devices upon request. The Wireless Router can act as a DHCP Server for devices on your local LAN and WLAN.
- ❑ Multi Segment LAN Support. LANs containing one or more segments are supported, via the Wireless Router's RIP (Routing Information Protocol) support and built-in static routing table.

## **Configuration and Management**

- Easy Setup. Use your WEB browser from anywhere on the LAN or WLAN for configuration.
- Remote Management. The Wireless Router can be managed from any PC on your LAN. And, if the Internet connection exists, it can also (optionally) be configured via the Internet.
- UPnP Support. UPnP (Universal Plug and Play) allows automatic discovery and configuration of the Wireless Router. UPnP is by supported by Windows ME, XP, or later.

## **Security Features**

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

## Package Contents

---

The following items should be included:

- The Wireless Router Unit
- Power Adapter
- Quick Installation Guide
- CD-ROM containing the on-line manual.

If any of the above items are damaged or missing, please contact your dealer immediately.

## Physical Details

### Front Panel LEDs



**Figure 2** Front Panel

**Table 1** Front Panel LEDs

LED	Status	Description
Power	ON	Power has been applied to the unit.
	OFF	No power.
Status	ON	An error has been detected.
	OFF	The unit is operating in normal operation.
	Blinking	This LED blinks during start up and firmware upgrade.
<b>LAN</b>		
Link/ACT	ON	Corresponding LAN (hub) port is active.
	OFF	No active connection on the corresponding LAN (hub) port.
	Flashing	Data is being transmitted or received via the corresponding LAN (hub) port.
100	ON	Corresponding LAN (hub) port is using 100Base-T.
	OFF	Corresponding LAN (hub) port connection is using 10Base-T, or no active connection.

LED	Status	Description
WAN	ON	Connection to the Broadband Modem attached to the WAN (Internet) port is established.
	OFF	No connection to the Broadband Modem. Flashing - Data is being transmitted or received via the WAN port.
WLAN	ON	Wireless connection available; Wireless Access Point is ready for use.
	OFF	No Wireless connection available.
	Flashing	Data is being transmitted or received via the Wireless access point. Data includes "network traffic" as well as user data.

## Back Panel Ports

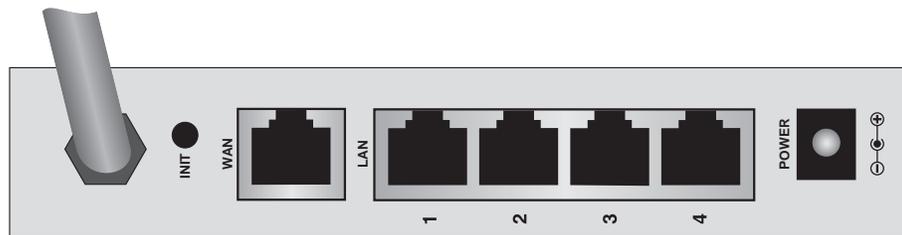


Figure 3 AT-WA1004G Back Panel

Table 2 Ports

Port	Description
Power	Connect the supplied power adapter here.
10/100Base-T LAN	Use standard LAN cables (RJ-45 connectors) to connect your PCs to these ports. If required, any port can be connected to another hub. Any LAN port will automatically function as an "Uplink" port when necessary.

Port	Description
WAN Port (10/100Base-T)	Connect the DSL or Cable Modem here. If your modem came with a cable, use the supplied cable. Otherwise, use a standard LAN cable.
Reset Button	<p>This button has two functions:</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Reboot. When pressed and released, the Wireless Router will reboot (restart).</li> <li><input type="checkbox"/> Clear All Data. This button can also be used to clear ALL data and restore ALL settings to the factory default values.</li> </ul>

To Clear All Data and restore the factory default values, perform the following procedure:

1. Power OFF.
2. Hold the Reset button down while you power ON.
3. Keep holding the Reset button for a 5 seconds, until the RED LED Status, on the front panel, has flashed twice.
4. Release the Reset button. The Wireless Router is now using the factory default values.



## Chapter 2

# Installation

---

This chapter contains the following sections:

- ❑ [Requirements](#) on page 24
- ❑ [Procedure](#) on page 25

## Requirements

---

- Network cables. Use standard 10/100Base-T network (UTP) cables with RJ-45 connectors.
- TCP/IP protocol must be installed on all PCs.
- For Internet Access, an Internet Access account with an ISP, and either of a DSL or Cable modem (for WAN port usage)
- To use the Wireless Access Point, all Wireless devices must be compliant with the IEEE802.11g specifications.

## Procedure

To install an AT-WA1004G, perform the following procedure:

1. Choose an Installation that is a suitable place on the network to install the Wireless Router. Ensure the Wireless Router and the DSL/Cable modem are powered OFF.

---

### Note

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

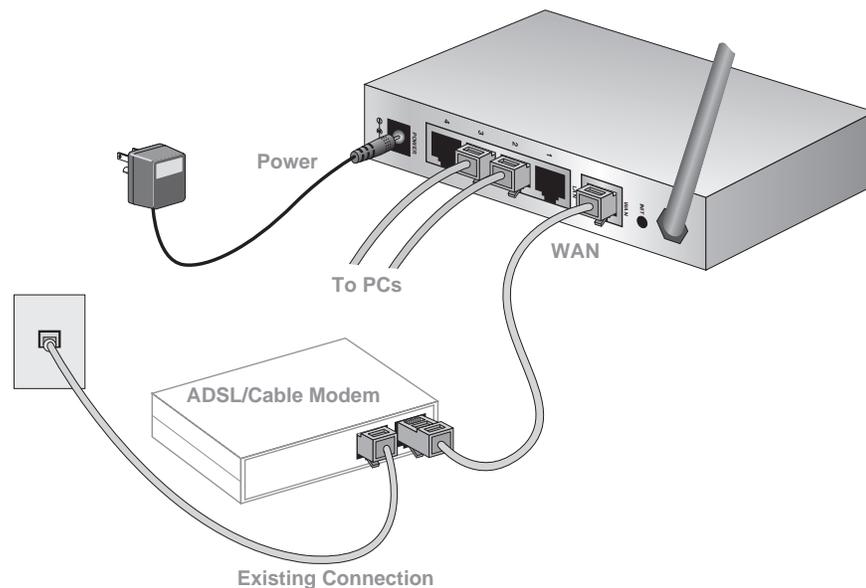
Also, if using multiple Access Points, adjacent Access Points should use different Channels with at least a 2 channel separation.

---

2. Connect LAN Cables using standard LAN cables to connect PCs to the Switching Hub ports on the Wireless Router. Both 10Base-T and 100Base-T 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 Router will automatically function as an "Uplink" port when required.

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



**Figure 4** Installation Diagram

4. Power on the Cable or DSL modem.

5. Connect the supplied power adapter to the Wireless Router and power up. Use only the power adapter provided. Using a different one may cause hardware damage
6. Verify that the Power LED is ON. The Status LED should flash, then turn OFF. If it stays ON, there is a hardware error. For each LAN (PC) connection, the Link/Act LED should be ON (provided the PC is also ON.) The WAN LED should be ON. The WLAN LED should be ON

For more information, refer to [Front Panel LEDs](#) on page 19.

# Chapter 3

# Setup

---

This chapter contains the following sections:

- ❑ [Overview](#) on page 28
- ❑ [Configuration Program](#) on page 30
- ❑ [Setup Wizard](#) on page 32
- ❑ [LAN Screen](#) on page 37
- ❑ [Wireless Screen](#) on page 40
- ❑ [Password Screen](#) on page 46

## 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, Chapter 4, [PC Configuration](#) on page 47.

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

To Do this:	Refer to:
Configure PCs on your LAN.	Chapter 4, <a href="#">PC Configuration</a> on page 47.
Check Wireless Router operation and Status.	Chapter 5, <a href="#">Operation and Status</a> on page 65.
Use any of the following Advanced features: <ul style="list-style-type: none"> <li><input type="checkbox"/> Access Control</li> <li><input type="checkbox"/> Dynamic DNS</li> <li><input type="checkbox"/> Advanced Internet (Special Applications, DMZ, URL Filter)</li> <li><input type="checkbox"/> Virtual Servers (Port Forwarding)</li> <li><input type="checkbox"/> WAN Port Setup</li> </ul>	Chapter 6, <a href="#">Advanced Features</a> on page 81.

To Do this:	Refer to:
<p>Use any of the following Administration Configuration settings or features:</p> <ul style="list-style-type: none"><li><input type="checkbox"/> Logs</li><li><input type="checkbox"/> Options (Backup DNS, TFTP, UPnP, Firewall)</li><li><input type="checkbox"/> PC Database</li><li><input type="checkbox"/> Remote Management</li><li><input type="checkbox"/> Routing (RIP and static Routing)</li><li><input type="checkbox"/> Security settings</li><li><input type="checkbox"/> Firmware Upgrade</li></ul>	<p>Chapter 7, <a href="#">Advanced Administration</a> on page 103.</p>

## Configuration Program

---

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

The configuration program has been tested on the following browsers:

- Netscape V4.08 or late
- Internet Explorer V4 or later

### Preparation

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

- Your PC can establish a physical connection to the Wireless Router. The PC and the Wireless Router must be directly connected (using the Hub ports on the Wireless Router) or on the same LAN segment.
- The Wireless Router must be installed and powered ON.
- If the Wireless Router's default IP Address (192.168.1.1) is already used by another device, the other device must be turned OFF until the Wireless Router is allocated a new IP Address during configuration.

### Using UPnP

If your Windows system supports UPnP, an icon for the Wireless Router will appear in the system tray, notifying you that a new network device has been found, and offering to create a new desktop shortcut to the newly-discovered device.

- Unless you intend to change the IP Address of the Wireless Router, you can accept the desktop shortcut.
- Whether you accept the desktop shortcut or not, you can always find UPnP devices in My Network Places (previously called Network Neighborhood).
- Double - click the icon for the Wireless Router (either on the Desktop, or in My Network Places) to start the configuration. Refer to [Setup Wizard](#) on page 32 for details of the initial configuration process.

## Using your Web Browser

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

1. After installing the Wireless Router in your LAN, start your PC. If your PC is already running, restart it.
2. Start your WEB browser.
3. In the Address box, enter "http://" and the IP Address of the Wireless Router, as in this example, which uses the Wireless Router's default IP Address: http://192.168.1.1.

If you cannot connect

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

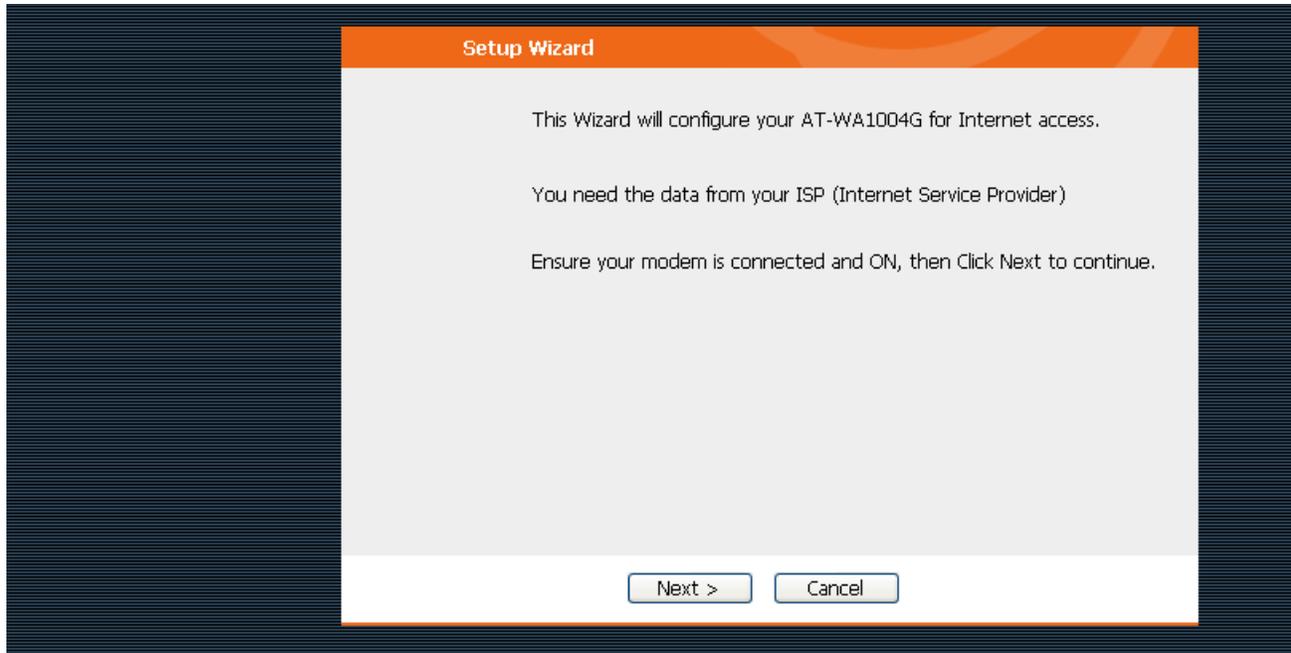
The Wireless Router is properly installed, LAN connection is OK, and it is powered ON. You can test the connection by using the "Ping" command:

- Open the MS-DOS window or command prompt window.
- Enter the command: ping 192.168.1.1 If no response is received, either the connection is not working, or your PC's IP address is not compatible with the Wireless Router's IP Address. (See below.)
- If your PC is using a fixed IP Address, its IP Address must be within the range 192.168.1.2 to 192.168.1.254 to be compatible with the Wireless Router's default IP Address of 192.168.1.1. Also, the Network Mask must be set to 255.255.255.0. Refer to Chapter 4, [PC Configuration](#) on page 47 for details on checking your PC's TCP/IP settings.
- Ensure that your PC and the Wireless Router are on the same network segment. (If you don't have a router, this must be the case.)
- Ensure you are using the wired LAN interface. The Wireless interface can only be used if its configuration matches your PC's wireless settings.

## Setup Wizard

---

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



**Figure 5** Setup Wizard Screen

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

## Common Connection Types

### Cable Modems

Type	Details	ISP Data required
Dynamic IP Address	Your IP Address is allocated automatically, when you connect to you ISP.	Usually, none. However, some ISP's may require you to use a particular Hostname, Domain name, or MAC (physical) address.
Static (Fixed) IP Address	Your ISP allocates a permanent IP Address to you.	IP Address allocated to you. Some ISP's may also require you to use a particular Host-name, Domain name, or MAC (physical) address.

**DSL Modems**

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

**Other Modems (for example Broadband Wireless)**

Type	Details	ISP Data required
Dynamic IP Address	Your IP Address is allocated automatically, when you connect to you ISP.	None.
Static (Fixed) IP Address	Your ISP allocates a permanent IP Address to you.	IP Address allocated to you.

## Big Pond (Australia)

For this connection method, the following data is required:

- User Name
- Password
- Big Pond Server IP address

## SingTel RAS

For this connection method, the following data is required:

- User Name
- Password
- RAS Plan

## 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.

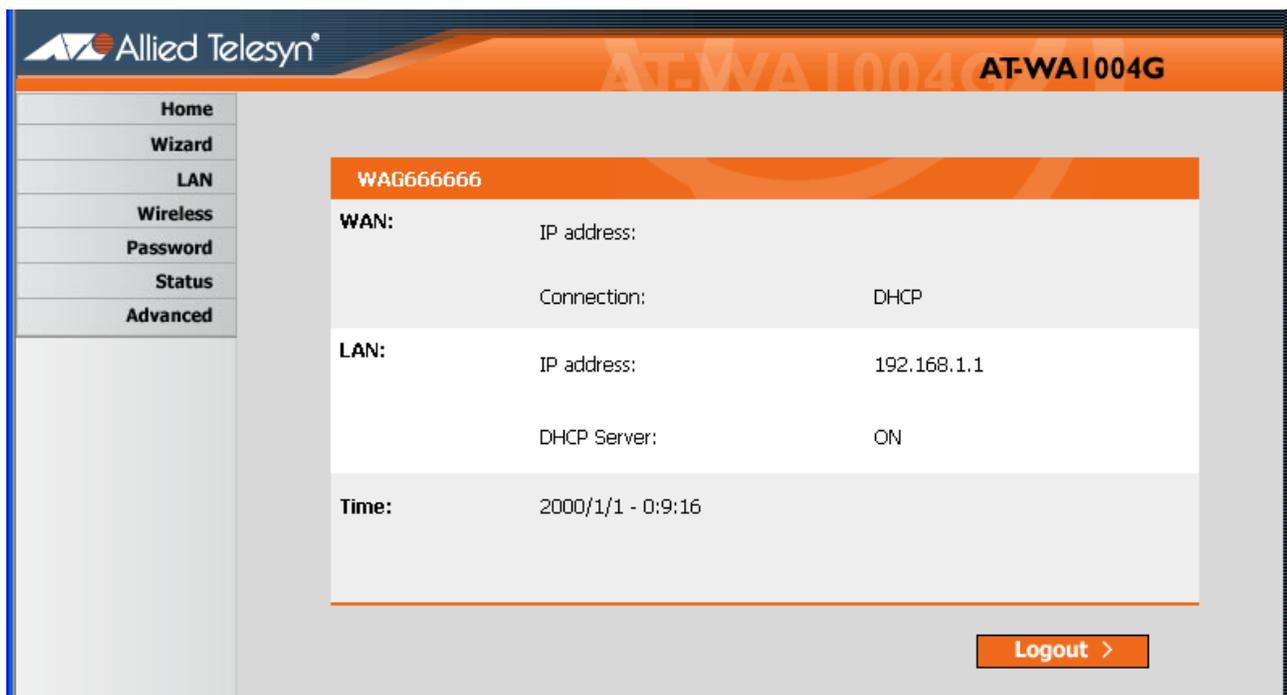


Figure 6 Home Screen

## Navigation and 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.

---

### Note

On each screen, clicking the “Help” button will display help for that screen. From any help screen, you can access the list of all help files (help index).

---

# LAN Screen

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



Figure 7 LAN Screen

## Data - LAN Screen

TCP/IP	
IP Address	IP address for the Wireless Router, as seen from the local LAN. Use the default value unless the address is already in use or your LAN is using a different IP address range. In the latter case, enter an unused IP Address from within the range used by your LAN.
Subnet Mask	The default value 255.255.255.0 is standard for small (class "C") networks. For other networks, use the Subnet Mask for the LAN segment to which the Wireless Router is attached (the same value as the PCs on that LAN segment).

DHCP Server	<ul style="list-style-type: none"> <li><input type="checkbox"/> If Enabled, the Wireless Router will allocate IP Addresses to PCs (DHCP clients) on your LAN when they start up. The default (and recommended) value is Enabled.</li> <li><input type="checkbox"/> If you are already using a DHCP Server, this setting must be Disabled, and the existing DHCP server must be re-configured to treat the Wireless Router as the default Gateway. See the following section for further details.</li> <li><input type="checkbox"/> The Start IP Address and Finish IP Address 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> <p>See the following section for further details on using DHCP.</p>
<b>Buttons</b>	
Save	Save the data on screen.
Cancel	The "Cancel" button will discard any data you have entered and reload the file from the Wireless Router.

## **DHCP    What DHCP Does**

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

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

## Using the Wireless Router's DHCP Server

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

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

---

### Note

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

---

## Using another DHCP Server

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

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

## To Configure your PCs to use DHCP

This is the default setting for TCP/IP under Windows 95/98/ME. See [PC Configuration](#) on page 47 for the procedure to check these settings.

## Wireless Screen

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

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

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

The screenshot shows the configuration interface for the wireless access point. The page title is "Wireless" and the device model is "AT-WA1004G". A left-hand navigation menu includes links for Home, Wizard, LAN, Wireless, Password, Status, and Advanced. The main content area is divided into three sections: Identification, Options, and Wireless Station Access. The Identification section shows the Access Point Name as "WAG666666" and the ESSID as "default", with a checkbox for "Hide ESSID". The Options section includes dropdown menus for Channel No. (6), 802.11 Mode (Auto), and Data Rate (Auto), along with an unchecked checkbox for "Enable Frame Burst" and a "Security" field set to "OFF". A "Configure" button is located next to the Security field. The Wireless Station Access section has two sections: "Allow LAN access by:" and "Allow Internet access by:", each with radio buttons for "ALL Wireless stations" (selected) and "Selected Wireless stations only", and a "Select Stations" button. At the bottom, there are "Save", "Cancel", and "Help" buttons.

Wireless	
<b>Identification</b>	Access Point Name: WAG666666
	ESSID: default
	<input type="checkbox"/> Hide ESSID
<b>Options</b>	Channel No: 6
	802.11 Mode: Auto
	Data Rate: Auto
	<input type="checkbox"/> Enable Frame Burst
	Security: OFF
	<input type="button" value="Configure"/>
<b>Wireless Station Access</b>	Allow LAN access by:
	<input checked="" type="radio"/> ALL Wireless stations
	<input type="radio"/> Selected Wireless stations only
	<input type="button" value="Select Stations"/>
	Allow Internet access by:
	<input checked="" type="radio"/> ALL Wireless stations
	<input type="radio"/> Selected Wireless stations only
	<input type="button" value="Select Stations"/>
	<input type="button" value="Save"/> <input type="button" value="Cancel"/> <input type="button" value="Help"/>

Figure 8 Wireless Screen

**Data - Wireless Screen**

<b>Identification</b>	
Regulatory Domain	It is illegal to use this device in any location outside of the regulatory domain.
Access Point name	This is the same as the "Device Name" for the Wireless Router. On your PC, some Wireless status screens may display this name as the name of the access point in use.
SSID (ESSID)	<input type="checkbox"/> If using an ESS (Extended Service Set, with multiple access points) this ID is called an ESSID (Extended Service Set Identifier). <input type="checkbox"/> To communicate, all Wireless stations should use the same SSID/ESSID.
<b>Options</b>	
Mode	Select the desired mode: <input type="checkbox"/> Auto - Both 802.11.g and 802.11b Wireless stations will be able to use the Wireless Router. <input type="checkbox"/> 802.11g only - Only 802.11g Wireless stations can use the Wireless Router. <input type="checkbox"/> 802.11b only - Only 802.11b connections are available. 802.11g Wireless Stations will only be able to use the Wireless Router if they are fully backward-compatible with the 802.11b standard.
Channel No.	<input type="checkbox"/> Select the Channel you wish to use on your Wireless LAN. <input type="checkbox"/> 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. <input type="checkbox"/> If using multiple access points, adjacent access points should use different Channels to reduce interference.

Security	<p>Select the desired option, and then enter the settings for the selected method:</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> None - No security is used. Anyone using the correct SSID can connect to your network.</li> <li><input type="checkbox"/> WEP - The 802.11b standard. Data is encrypted before transmission, but the encryption system is not very strong.</li> <li><input type="checkbox"/> WPA-PSK - Like WEP, data is encrypted before transmission. WPA is more secure than WEP, and should be used if possible. WPA-P5K is the version of WPA which does not require a Radius Server on your LAN.</li> </ul>
<b>Wireless Station Access</b>	
Allow LAN access by...	<ul style="list-style-type: none"> <li><input type="checkbox"/> All Wireless Stations - All wireless stations can use the access point to access your LAN.</li> <li><input type="checkbox"/> elected Wireless stations only - Only selected wireless stations access your LAN. To select the required wireless stations, click the "Select Stations" button.</li> </ul>
Allow Internet access by...	<ul style="list-style-type: none"> <li><input type="checkbox"/> All Wireless Stations - All wireless stations can use the access point to access the Internet.</li> <li><input type="checkbox"/> Selected Wireless stations only - Only selected wireless stations use the access point to access the Internet. To select the required wireless stations, click the "Select Stations" button.</li> </ul>
<b>Buttons</b>	
Select Stations	Click this button to select the required PCs.
Save	Save the data on screen.
Cancel	The "Cancel" button will discard any data you have entered since the last "Save" operation.

**WEP Screen** This screen is accessed by clicking the “Configure” button on the Wireless screen. The WEP screen is shown below. Select other options for appropriated security.

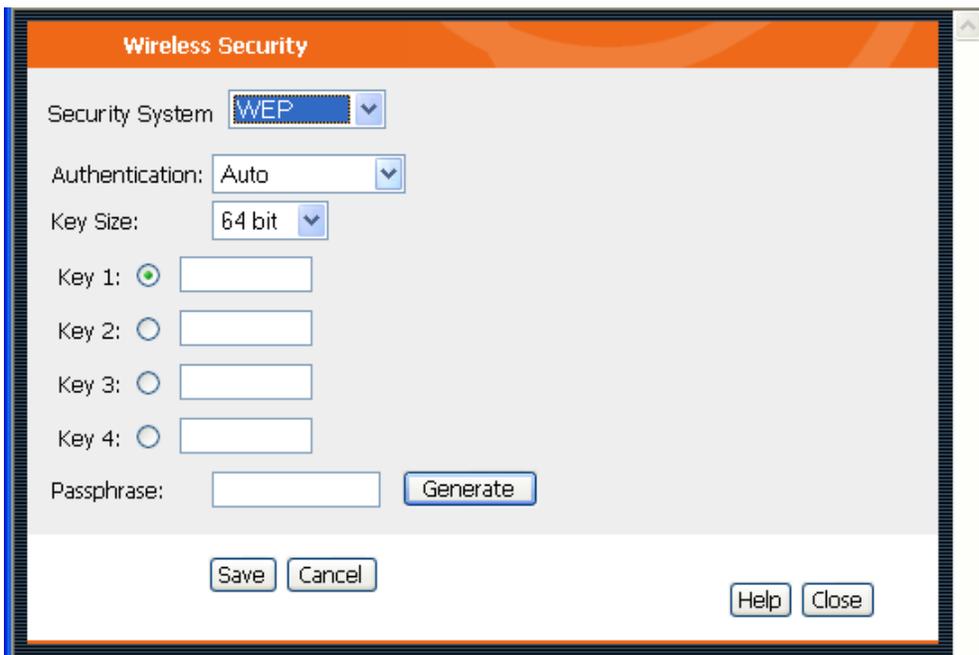


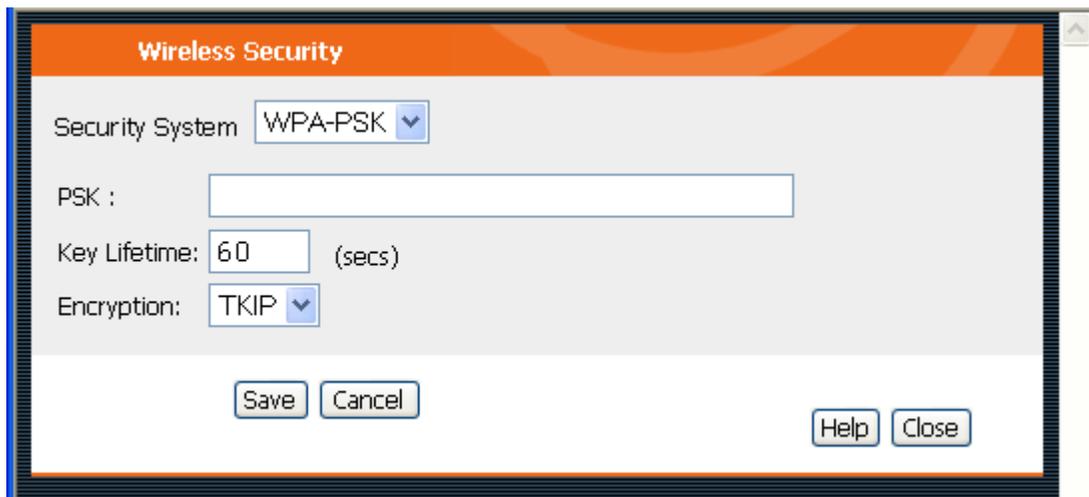
Figure 9 WEP Screen

**Data - Wireless Security Screen**

WEP	
Authentication	Normally this can be left at the default value of “Automatic.” If that fails, select the appropriate value - “Open System” or “Shared Key.” Check your wireless card’s documentation to see what method to use.
Data Key Size	Select the WEP Encryption level: <input type="checkbox"/> 64-bit (sometimes called 40-bit) encryption. <input type="checkbox"/> 128-bit encryption.

Keys	<ul style="list-style-type: none"><li><input type="checkbox"/> Use the Radio button to select the default key.</li><li><input type="checkbox"/> Enter the key value you wish to use. Other stations must have the same key values.</li><li><input type="checkbox"/> Keys must be entered in Hex. Hex characters are the digits (0 - 9) and the letters A- F.</li></ul>
Passphrase	Enter a word or group of printable characters in the Passphrase box and click the "Generate Key" button to automatically configure the WEP Key(s). If encryption strength is set to 64-bit, then each of the four key field will be populated with key values. If encryption strength is set to 128-bit, then only the selected WEP key field will be given a key value.

**WPA-PSK** This screen is accessed by clicking the “Configure” button on the Wireless screen. The WPA-PSK screen is shown below. Select other options for appropriated security.



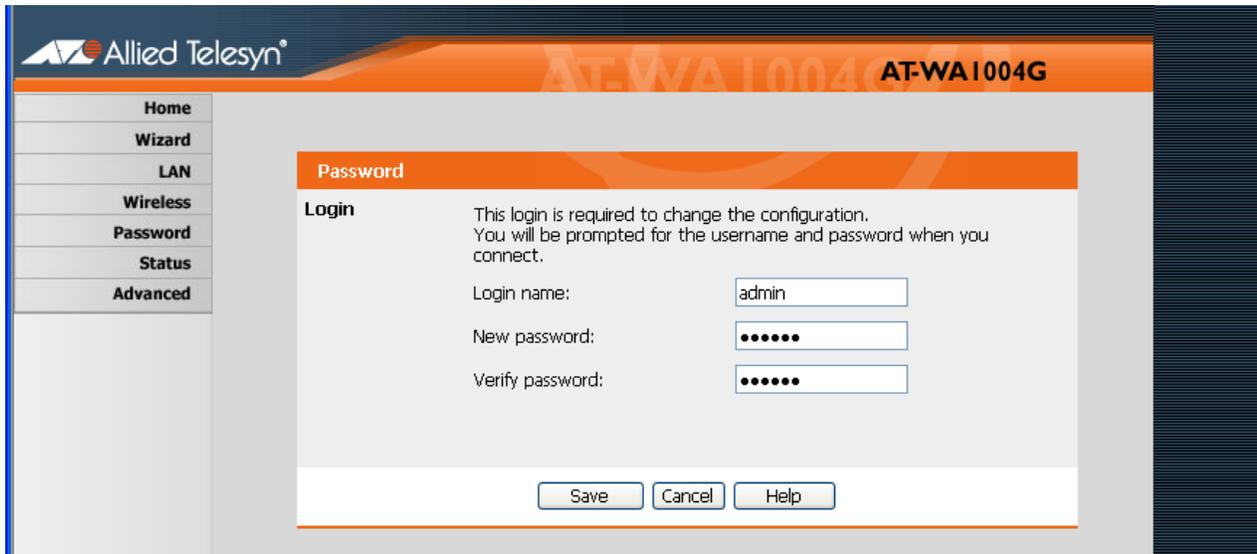
**Figure 10** WPA-PSK Screen

**Data - Wireless Security Screen**

WPA-PSK	
PSK	Enter the keyword key value. Data is encrypted using a key derived from the network key. Other Wireless Stations must use the same network key.
Key Lifetime	This is determined how often the encryption key is changed. Enter the desired value.
Encryption	Select the desired option. Wireless Stations must use the same method.

## Password Screen

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



**Figure 11** Password Screen

Once you have assigned a password to the Wireless Router (on the Password screen above) you will be prompted for the password when you connect, as shown below. (If no password has been set, this dialog will not appear.)



**Figure 12** Password Dialog

- The Login Name is not required.
- Enter the password for the Wireless Router, as set on the Password screen above.

# Chapter 4

# PC Configuration

---

This chapter contains the following sections:

- ❑ [Overview](#) on page 48
- ❑ [Windows Clients](#) on page 49
- ❑ [Checking TCP/IP Settings](#) on page 50
- ❑ [Macintosh Clients](#) on page 61
- ❑ [Linux Clients](#) on page 62
- ❑ [Other Unix Systems](#) on page 63
- ❑ [Wireless Station Configuration](#) on page 64

## Overview

---

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

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

## Windows Clients

---

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

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

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

### **TCP/IP Settings Overview**

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

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

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

- The Gateway must be set to the IP address of the wireless router.
- The DNS should be set to the address provided by your ISP.

---

#### **Note**

If your LAN has a router, the LAN administrator must reconfigure the router itself.

---

## Checking TCP/IP Settings

---

### **For Windows 9x/ME**

1. Select **Control Panel** and then **Network**.
2. Select the TCP/IP protocol for your network card.
3. Select **Properties**.

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 Router will act as a DHCP Server.

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

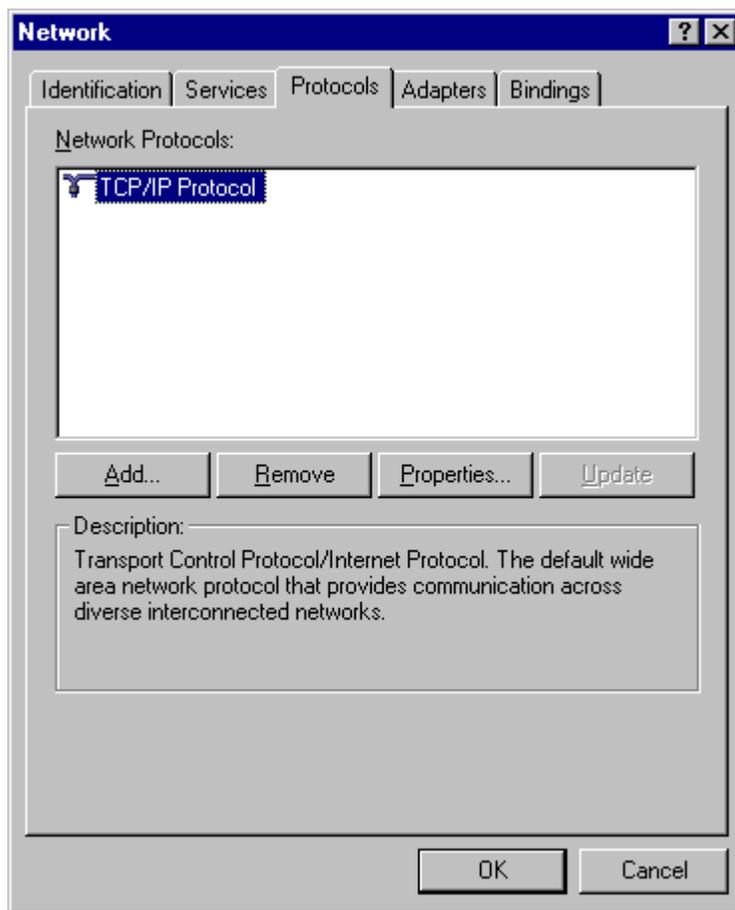
### **Using “Specify an IP Address”**

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

- On the Gateway tab, enter the Wireless Router's IP address in the New Gateway field and click Add. Your LAN administrator can advise you of the IP Address they assigned to the Wireless Router.
- 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.

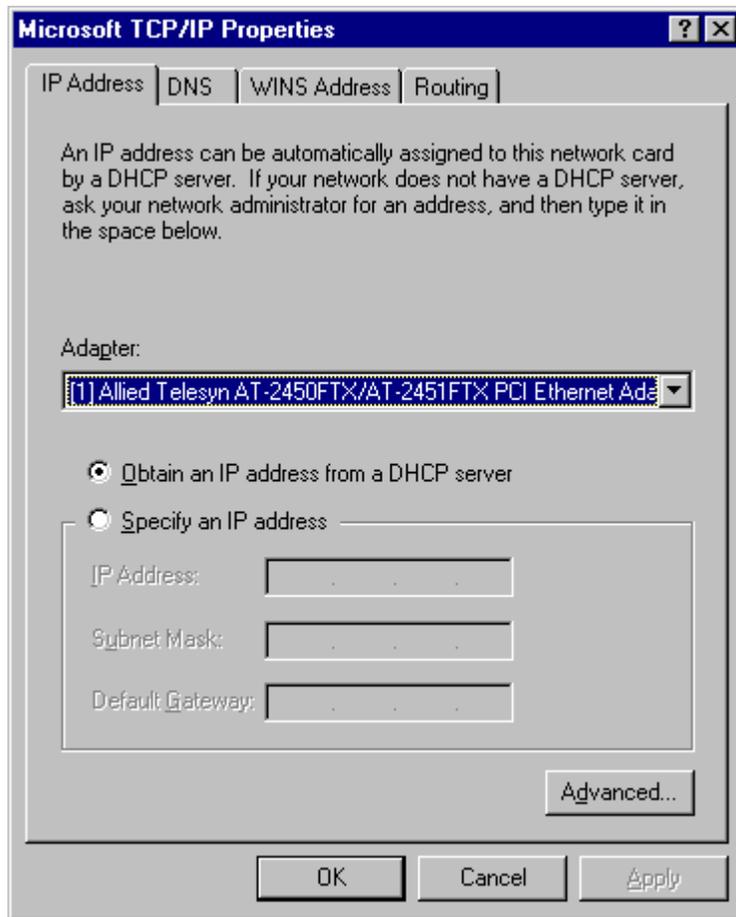
**For Windows  
NT4.0**

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



**Figure 13** Windows NT4.0 - TCP/IP

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



**Figure 14** Windows NT 4.0 - IP Address

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

**Obtain an IP address from a DHCP Server**

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

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

## Specify an IP Address

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

1. The Default Gateway must be set to the IP address of the Wireless Router. To set this:
  - Click the Advanced button on the screen above.
  - On the following screen, click the Add button in the Gateways panel, and enter the Wireless Router's IP address, as shown in Figure 15 below.



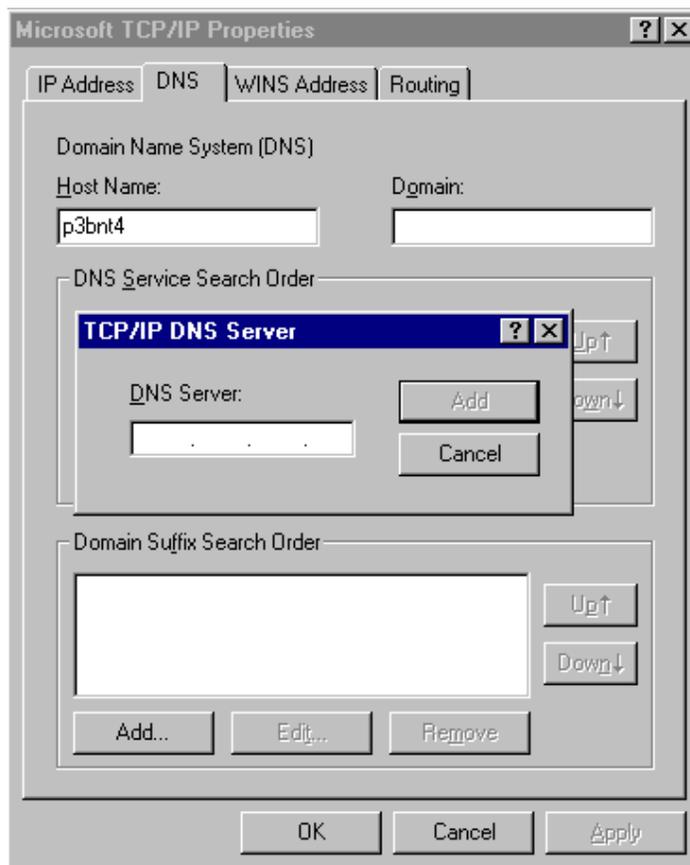
Figure 15 Windows NT 4.0

- If necessary, use the Up button to make the Wireless Router the first entry in the Gateways list.



**Figure 16** Windows NT 4.0 - Add Gateway

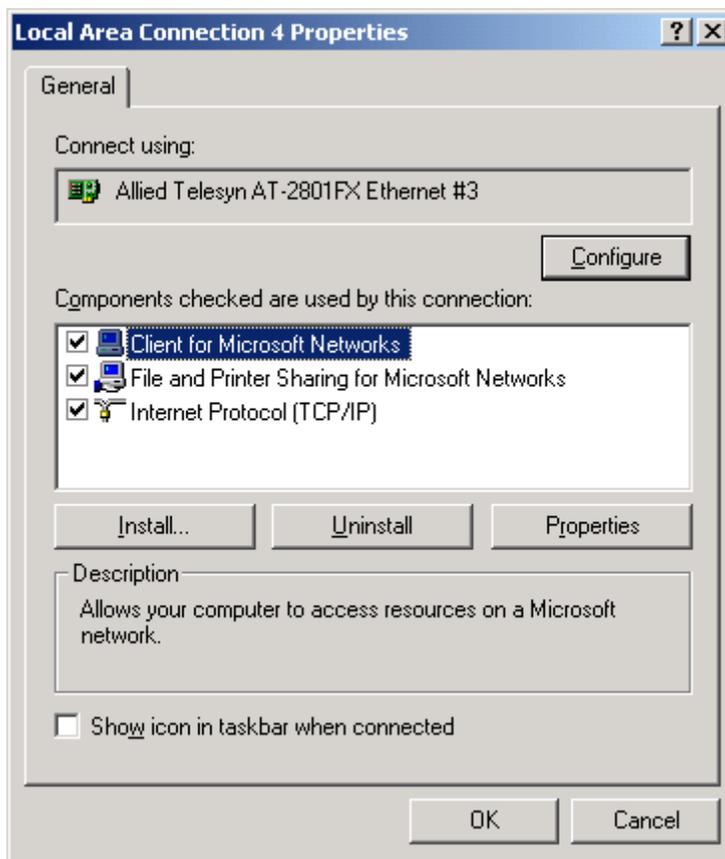
2. The DNS should be set to the address provided by your ISP, as follows:
  - Click the DNS tab.
  - On the DNS screen, shown below, click the Add button (under DNS Service Search Order), and enter the DNS provided by your ISP.



**Figure 17** Windows NT4.0 - DNS

**For Windows  
2000**

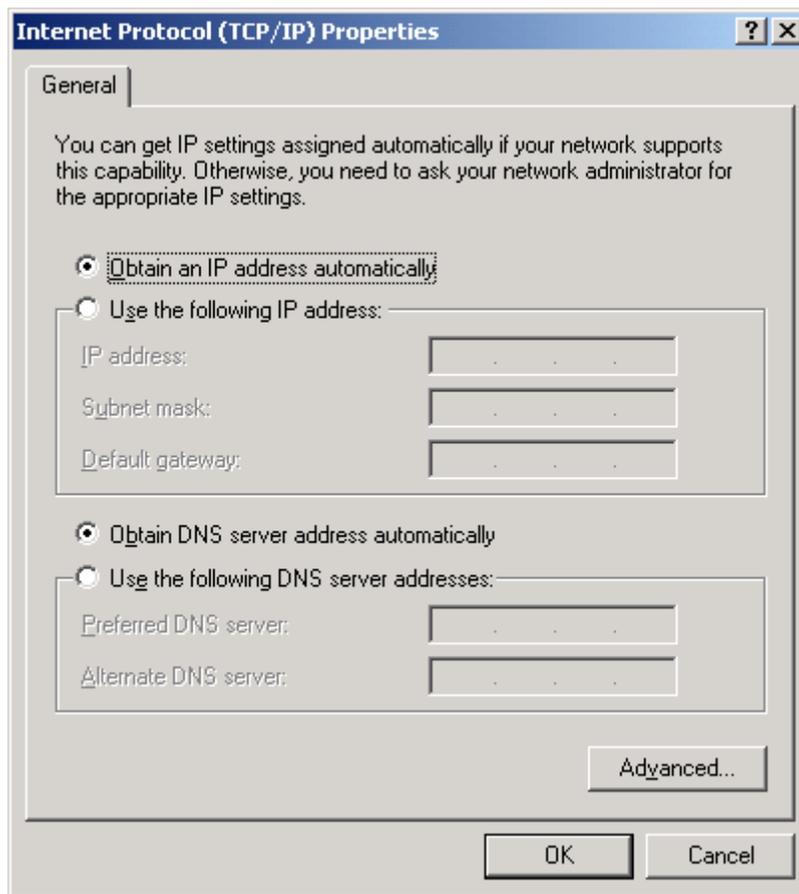
1. Select Control Panel - Network and Dial-up Connection.
2. Right - click the Local Area Connection icon and select Properties. You should see a screen like the following:



**Figure 18** 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 19** TCP/IP Properties (Win 2000)

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

### **Using DHCP**

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

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

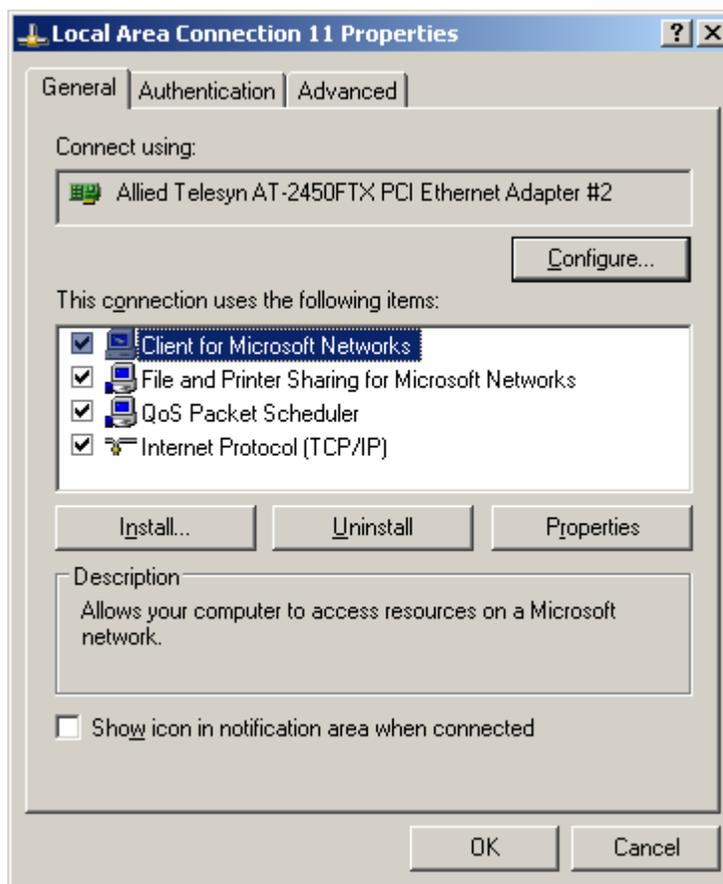
## Using a fixed IP Address (“Use the following IP Address”)

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

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

### For Windows XP

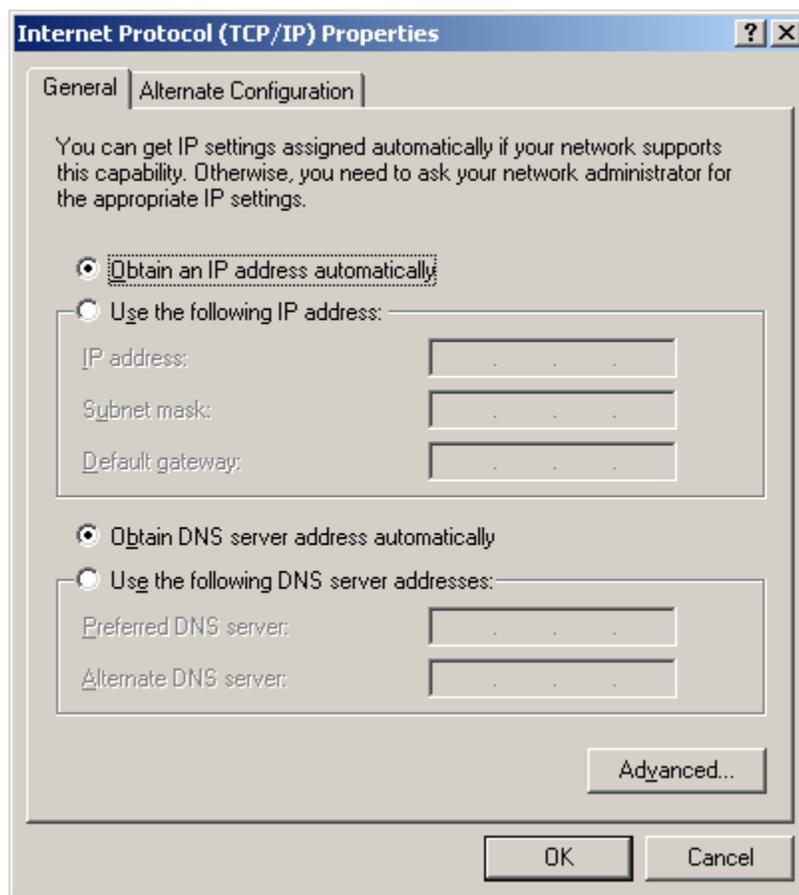
1. Select Control Panel - Network Connection.
2. Right click the Local Area Connection and choose Properties. You should see a screen like the following:



**Figure 20** Network Configuration (Windows XP)

3. Select the TCP/IP protocol for your network card.

- Click on the Properties button. You should then see a screen like the following.



**Figure 21** TCP/IP Properties (Windows XP)

- Ensure your TCP/IP settings are correct.

### **Using DHCP**

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

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

### Using a fixed IP Address (“Use the following IP Address”)

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

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

### Internet Access

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

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

#### For Windows 9x/ME/2000

1. Select **Start Menu, Settings, Control Panel** and then **Internet Options**.
2. Select the **Connection** tab and then **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 then **Next**.
4. Select **I connect through a local area network (LAN)** and then **Next**.
5. Ensure all of the boxes on the following Local area network Internet Configuration screen are unchecked.
6. Check **No** at the next prompted.
7. Select **Finish** to close the Internet Connection Wizard.

Setup is now completed.

## **For Windows XP**

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

Setup is now completed.

## **Accessing AOL**

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

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

## Macintosh Clients

---

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

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

---

### Note

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

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

## Linux Clients

---

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

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

### Fixed IP Address

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

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

### To act as a DHCP Client (recommended)

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

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

## Other Unix Systems

---

To access the Internet via the Wireless Router:

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

## Wireless Station Configuration

---

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

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

Mode	The mode must be set to Infrastructure.
SSID (ESSID)	This must match the value used on the Wireless Router. The default value is default. <b>Note:</b> The SSID is case sensitive.
WEP	By default, WEP on the Wireless Router is disabled. <input type="checkbox"/> If WEP remains disabled on the Wireless Router, all stations must have WEP disabled. <input type="checkbox"/> If WEP is enabled on the Wireless Router, each station must use the same settings as the Wireless Router.

## Chapter 5

# Operation and Status

---

This chapter contains the following sections:

- ❑ [Operation](#) on page 66
- ❑ [Status Screen](#) on page 67
- ❑ [Connection Status - PPPoE](#) on page 69
- ❑ [Connection Status - PPTP](#) on page 72
- ❑ [Connection Status - L2TP](#) on page 73
- ❑ [Connection Status - Telstra Big Pond](#) on page 74
- ❑ [Connection Details - SingTel RAS](#) on page 76
- ❑ [Connection Details - Fixed/Dynamic IP Address](#) on page 78

## Operation

---

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

However, there are some situations where additional Internet configuration may be required:

- ❑ If using Internet-based Communication Applications, it may be necessary to specify which PC receives an incoming connection. Refer to Chapter 6, [Advanced Features](#) on page 81 for further details.
- ❑ Applications which use non-standard connections or port numbers may be blocked by the Wireless Router's built-in firewall. You can define such applications as Special Applications to allow them to function normally. Refer to Chapter 6, [Advanced Features](#) on page 81 for further details.
- ❑ Some non-standard applications may require use of the DMZ feature. Refer to Chapter 6, [Advanced Features](#) on page 81 for further details.

## Status Screen

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

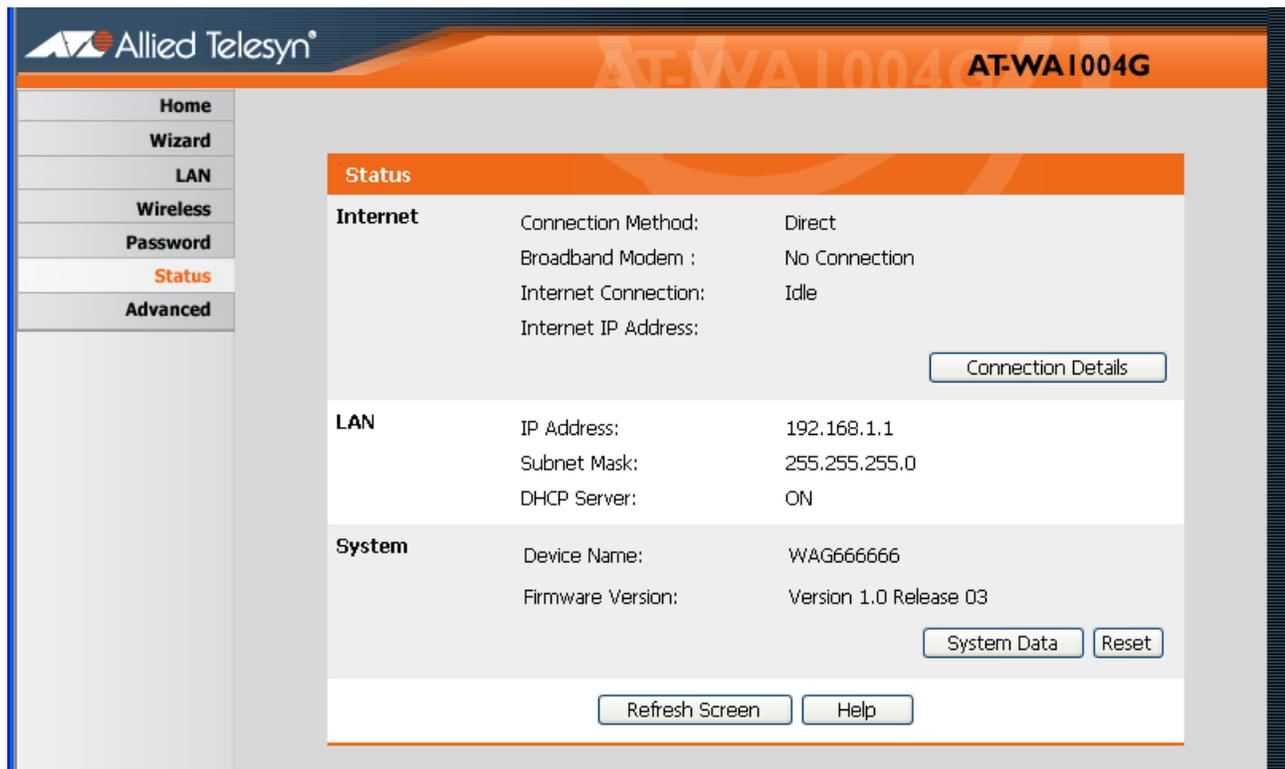


Figure 22 Status Screen

### Data - Status Screen

Internet	
Connection Method	This indicates the current connection method, as set in the Setup Wizard or WAN Port screen.
Broadband Modem	This shows the status of the connection from the Wireless Router to the Broadband Modem.
Internet Connection	<p>Current connection status:</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Active</li> <li><input type="checkbox"/> Idle</li> <li><input type="checkbox"/> Unknown</li> <li><input type="checkbox"/> Failed</li> </ul> <p>If there is an error, you can click the "Connection Details" button to find out more information.</p>

Internet IP Address	This IP Address is allocated by the ISP (Internet Service Provider). If there is no current connection, this will be blank or 0.0.0.0.
"Connection Details" Button	Click this button to open a sub-window and view a detailed description of the current connection. Depending on the type of connection, a "Connection Log" may also be available.
<b>LAN</b>	
IP Address	The IP Address of the Wireless Router.
Subnet Mask	The Subnet Mask for the IP Address above.
DHCP Server	This shows the status of the DHCP Server function - either "Enabled" or "Disabled."  For additional information about the PCs on your LAN, and the IP addresses allocated to them, use the PC Database option on the Administration menu.
<b>System</b>	
Device Name	This displays the current name of the Wireless Router.
Firmware Version	The current version of the firmware installed in the Wireless Router.
<b>Buttons</b>	
Connection Details	View the details of the current Internet connection. The sub-screen displayed will depend on the connection method used. See the following sections for details of each sub-screen.
System Data	Display all system information in a sub-window.
Restart	Clicking this button will restart (reboot) the Wireless Router. All existing connections though the Wireless Router will be terminated, but will usually reconnect automatically.
Refresh Screen	Update the data displayed on screen.

## Connection Status - PPPoE

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

### Data - PPPoE Screen

Connection	
Physical Address	The hardware address of this device, as seen by remote devices on the Internet. (This is different to the hardware address seen by devices on the local LAN.)
IP Address	The IP Address of this device, as seen by Internet users. This address is allocated by your ISP (Internet Service Provider).
Subnet Mask	The Subnet Mask associated with the IP Address above.
PPPoE Link Status	<input type="checkbox"/> This indicates whether or not the connection is currently established. <input type="checkbox"/> If the connection does not exist, the "Connect" button can be used to establish a connection. <input type="checkbox"/> If the connection currently exists, the "Disconnect" button can be used to break the connection.
Connection Log	
Connection Log	<input type="checkbox"/> The Connection Log shows status messages relating to the existing connection. <input type="checkbox"/> The most common messages are listed in the table below. <input type="checkbox"/> The "Clear Log" button will restart the Log, while the Refresh button will update the messages shown on screen.
Buttons	
Connect	If not connected, establish a connection to your ISP.

Disconnect	If connected to your ISP, hang up the connection.
Clear Log	Delete all data currently in the Log. This will make it easier to read new messages.
Refresh	Update the data on screen.

**Connection Log Messages**

Message	Description
Connect on Demand	Connection attempt has been triggered by the "Connect automatically, as required" setting.
Manual Connection	Connection attempt started by the "Connect" button.
Reset Physical Connection	Preparing line for connection attempt.
Connecting to Remote Server	Attempting to connect to the ISP's server.
Remote Server Located	ISP's Server has responded to connection attempt.
Start PPP	Attempting to login to ISP's Server and establish a PPP connection.
PPP Up Successfully	Able to login to ISP's Server and establish a PPP connection.
Idle Time-out Reached	The connection has been idle for the time period specified in the "Idle Time-out" field. The connection will now be terminated.
Disconnecting	The current connection is being terminated, due to either the "Idle Time-out" above, or "Disconnect" button being clicked.
Error: Remote Server Not Found	ISP's Server did not respond. This could be a Server problem, or a problem with the link to the Server.

<b>Message</b>	<b>Description</b>
Error: PPP Connection Failed	Unable to establish a PPP connection with the ISP's Server. This could be a login problem (name or password) or a Server problem.
Error: Connection to Server Lost	The existing connection has been lost. This could be caused by a power failure, a link failure, or Server failure.
Error: Invalid or Unknown Packet Type	The data received from the ISP's Server could not be processed. This could be caused by data corruption (from a bad link), or the Server using a protocol which is not supported by this device.

## Connection Status - PPTP

---

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

### Data - PPTP Screen

<b>Connection</b>	
Physical Address	The hardware address of this device, as seen by remote devices on the Internet. (This is different to the hardware address seen by devices on the local LAN.)
IP Address	The IP Address of this device, as seen by Internet users. This address is allocated by your ISP (Internet Service Provider).
PPTP Status	<p>This indicates whether or not the connection is currently established.</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> If the connection does not exist, the "Connect" button can be used to establish a connection.</li> <li><input type="checkbox"/> If the connection currently exists, the "Disconnect" button can be used to break the connection.</li> </ul>
<b>Connection Log</b>	
Connection Log	<ul style="list-style-type: none"> <li><input type="checkbox"/> The Connection Log shows status messages relating to the existing connection.</li> <li><input type="checkbox"/> The "Clear Log" button will restart the Log, while the Refresh button will update the messages shown on screen.</li> </ul>
<b>Buttons</b>	
Connect	If not connected, establish a connection to your ISP.
Disconnect	If connected to your ISP, hang up the connection.
Clear Log	Delete all data currently in the Log. This will make it easier to read new messages.
Refresh	Update the data on screen.

## Connection Status - L2TP

---

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

### Data - L2TP Screen

<b>Connection</b>	
Physical Address	The hardware address of this device, as seen by remote devices on the Internet. (This is different to the hardware address seen by devices on the local LAN.)
IP Address	The IP Address of this device, as seen by Internet users. This address is allocated by your ISP (Internet Service Provider).
Connection Status	<p>This indicates whether or not the connection is currently established.</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> If the connection does not exist, the "Connect" button can be used to establish a connection.</li> <li><input type="checkbox"/> If the connection currently exists, the "Disconnect" button can be used to break the connection.</li> </ul>
<b>Connection Log</b>	
Connection Log	<ul style="list-style-type: none"> <li><input type="checkbox"/> The Connection Log shows status messages relating to the existing connection.</li> <li><input type="checkbox"/> The "Clear Log" button will restart the Log, while the Refresh button will update the messages shown on screen.</li> </ul>
<b>Buttons</b>	
Connect	If not connected, establish a connection to your ISP.
Disconnect	If connected to your ISP, hang up the connection.
Clear Log	Delete all data currently in the Log. This will make it easier to read new messages.
Refresh	Update the data on screen.

## Connection Status - Telstra Big Pond

---

### Data - Big Pond Screen

<b>Connection</b>	
Physical Address	The hardware address of this device, as seen by remote devices. (This is different to the hardware address seen by devices on the local LAN.)
IP Address	The IP Address of this device, as seen by Internet users. This address is allocated by your ISP (Internet Service Provider).
Connection Status	<p>This indicates whether or not the connection is currently established.</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> If the connection does not exist, the "Connect" button can be used to establish a connection.</li> <li><input type="checkbox"/> If the connection currently exists, the "Disconnect" button can be used to break the connection.</li> <li><input type="checkbox"/> Normally, it is not necessary to use the Connect and Disconnect buttons unless the setting "Connect automatically, as required" is disabled.</li> </ul>
<b>Connection Log</b>	
Connection Log	<ul style="list-style-type: none"> <li><input type="checkbox"/> The Connection Log shows status messages relating to the existing connection.</li> <li><input type="checkbox"/> The Clear Log button will restart the Log, while the Refresh button will update the messages shown on screen.</li> </ul>
<b>Buttons</b>	
Connect	If not connected, establish a connection to Telstra Big Pond.
Disconnect	If connected to Telstra Big Pond, terminate the connection.

Clear Log	Delete all data currently in the Log. This will make it easier to read new messages.
Refresh	Update the data on screen.

## Connection Details - SingTel RAS

---

If using the SingTel RAS access method, a screen will be displayed when the "Connection Details" button is clicked.

### Data - RAS Screen

<b>Internet</b>	
RAS Plan	The RAS Plan which is currently used.
Physical Address	The hardware address of this device, as seen by remote devices on the Internet. (This is different to the hardware address seen by devices on the local LAN.)
IP Address	The IP Address of this device, as seen by Internet users. This address is allocated by your ISP (Internet Service Provider).
Subnet Mask	The Subnet Mask associated with the IP Address above.
Default Gateway	The IP Address of the remote Gateway or Router associated with the IP Address above.
DNS IP Address	The IP Address of the Domain Name Server which is currently used.
DHCP Client	<p>This will show "Enabled" or "Disabled," depending on whether or not this device is functioning as a DHCP client.</p> <p>If "Enabled" the "Remaining lease time" field indicates when the IP Address allocated by the DHCP Server will expire. The lease is automatically renewed on expiry; use the "Renew" button if you wish to manually renew the lease immediately.</p>
<b>Buttons</b>	

<p>Release/Renew Button will display EITHER "Release" or "Renew"</p>	<p>This button is only useful if the IP address shown above is allocated automatically on connection. (Dynamic IP address). If you have a Fixed (Static) IP address, this button has no effect.</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> If the ISP's DHCP Server has NOT allocated an IP Address for the Wireless Router, this button will say "Renew". Clicking the "Renew" button will attempt to re-establish the connection and obtain an IP Address from the ISP's DHCP Server.</li> <li><input type="checkbox"/> If an IP Address has been allocated to the Wireless Router (by the ISP's DHCP Server), this button will say "Release." Clicking the "Release" button will break the connection and release the IP Address.</li> </ul>
<p>Refresh</p>	<p>Update the data shown on screen.</p>

## Connection Details - Fixed/Dynamic IP Address

---

### Data - Fixed/Dynamic IP address Screen

<b>Internet</b>	
Physical Address	The hardware address of this device, as seen by remote devices on the Internet. (This is different to the hardware address seen by devices on the local LAN.)
IP Address	The IP Address of this device, as seen by Internet users. This address is allocated by your ISP (Internet Service Provider).
Subnet Mask	The Subnet Mask associated with the IP Address above.
Default Gateway	The IP Address of the remote Gateway or Router associated with the IP Address above.
DNS IP Address	The IP Address of the Domain Name Server which is currently used.
DHCP Client	<p>This will show "Enabled" or "Disabled," depending on whether or not this device is functioning as a DHCP client.</p> <p>If "Enabled" the "Remaining lease time" field indicates when the IP Address allocated by the DHCP Server will expire. The lease is automatically renewed on expiry; use the "Renew" button if you wish to manually renew the lease immediately.</p>
<b>Buttons</b>	

<p>Release/Renew Button will display EITHER "Release" or "Renew"</p>	<p>This button is only useful if the IP address shown above is allocated automatically on connection. (Dynamic IP address). If you have a Fixed (Static) IP address, this button has no effect.</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> If the ISP's DHCP Server has NOT allocated an IP Address for the Wireless Router, this button will say 'Renew". Clicking the "Renew" button will attempt to re-establish the connection and obtain an IP Address from the ISP's DHCP Server.</li> <li><input type="checkbox"/> If an IP Address has been allocated to the Wireless Router (by the ISP's DHCP Server), this button will say "Release". Clicking the "Release" button will break the connection and release the IP Address.</li> </ul>
<p>Refresh</p>	<p>Update the data shown on screen.</p>



## Chapter 6

# Advanced Features

---

This chapter contains the following sections:

- ❑ [Overview](#) on page 82
- ❑ [Access Control](#) on page 83
- ❑ [Dynamic DNS \(Domain Name Server\)](#) on page 90
- ❑ [Advanced Internet Screen](#) on page 93
- ❑ [Virtual Servers](#) on page 98

## Overview

---

The following advanced features are provided.

- Access Control
- Dynamic DNS
- Advanced Internet
  - Communication Applications
  - Special Applications
  - Multi-DMZ
  - URL filter
- Virtual Servers
- WAN Port

## Access Control

This feature is accessed by the Access Control link on the Advanced menu.

### Overview

The Access Control feature allows administrators to restrict the level of Internet Access available to PCs on your LAN. With the default settings, everyone has unrestricted Internet access.

To use this feature:

1. Set the desired restrictions on the "Members" group. All PCs are in the "Default" group unless explicitly moved to another group.
2. Set the desired restrictions on the other groups ("Group 1," "Group 2," "Group 3," and "Group 4") as needed.
3. Assign PC to the groups as required.

### Note

Restrictions are imposed by blocking "Services", or types of connections. All common Services are pre-defined. If required, you can also define your own Services.

### Access Control Screen

To view this screen, select the Access Control link on the Advanced menu.

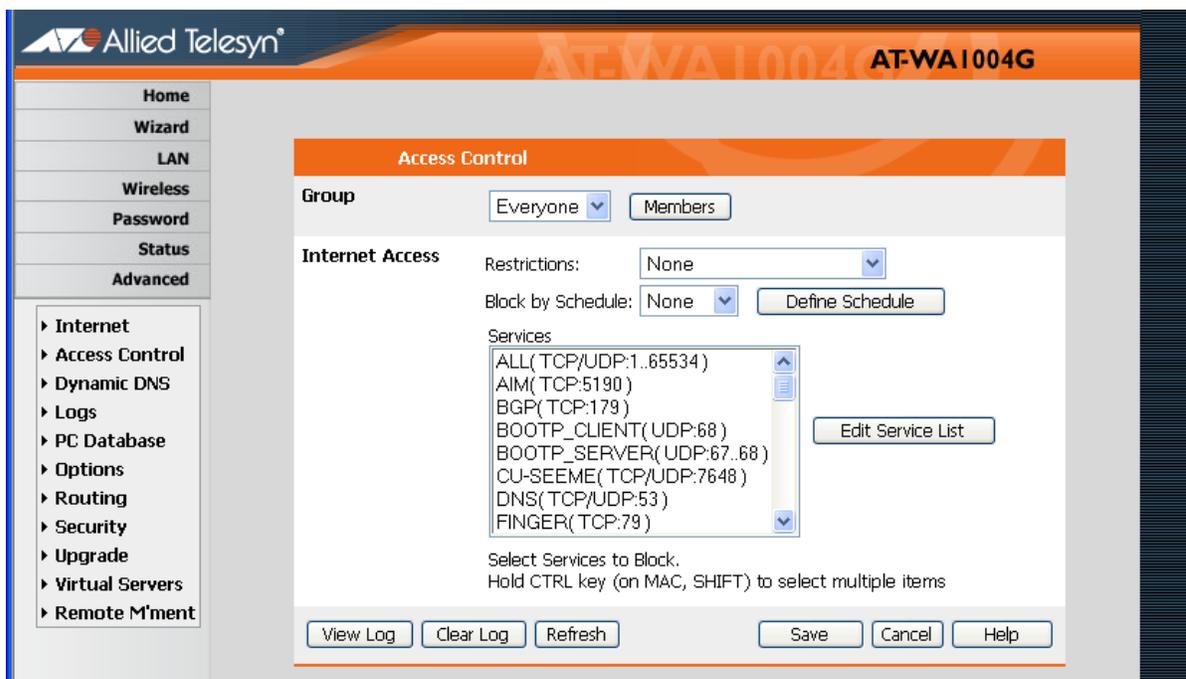


Figure 23 Access Control Screen

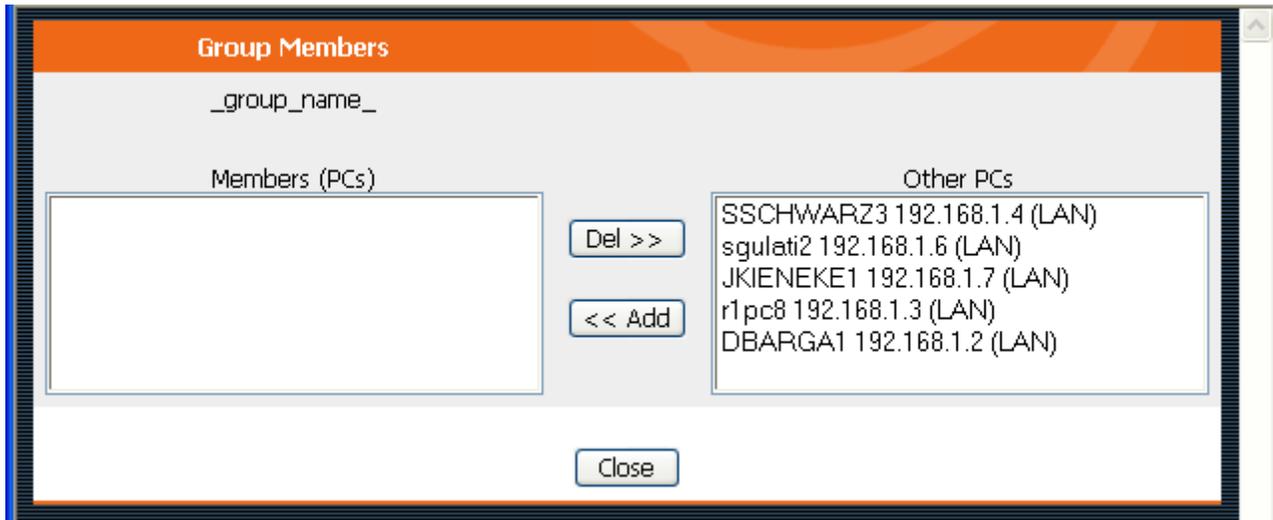
**Data - Access Control Screen**

<b>Group</b>	
Group	Select the desired Group. The screen will update to display the settings for the selected Group. Groups are named "Default," "Group 1," "Group 2," "Group 3" and "Group 4," and cannot be renamed.
"Members" Button	<p>Click this button to add or remove members from the current Group.</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> If the current group is "Default," then members can not be added or deleted. This group contains PCs not allocated to any other group.</li> <li><input type="checkbox"/> To remove PCs from the Default Group, assign them to another Group.</li> <li><input type="checkbox"/> To assign PCs to the Default Group, delete them from the Group they are currently in. See the following section for details of the Group Members screen.</li> </ul>
<b>Internet Access</b>	
Restrictions	<p>Select the desired options for the current group:</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> None - Nothing is blocked. Use this to create the least restrictive group.</li> <li><input type="checkbox"/> Block all Internet access - All traffic via the WAN port is blocked. Use this to create the most restrictive group.</li> <li><input type="checkbox"/> Block selected Services - You can select which Services are to block. Use this to gain fine control over the Internet access for a group.</li> </ul>
Block by Schedule	If Internet access is being blocked, you can choose to apply the blocking only during scheduled times. (If access is not blocked, no Scheduling is possible, and this setting has no effect.)
Define Schedule Button	Clicking this will open a sub-window where you can define or modify the Schedule.

Services	This lists all defined Services. Select the Services you wish to block. To select multiple services, hold the CTRL key while selecting. (On the Macintosh, hold the SHIFT key rather than CTRL.)
Edit Service List Button	If you wish to define additional Services, or manage the Service list, click this button to open the "Services" screen.
<b>Buttons</b>	
Members	Click this button to add or remove members from the current Group. If the current group is "Default," then members can not be added or deleted. This group contains PCs not allocated to any other group. See the following section for details of the Group Members screen.
Define Schedule	Click this to open a sub-window where you can define or modify the Schedule.
Edit Service List	If you wish to define additional Services, or manage the Service list, click this button to open the "Services" screen.
Save	Save the data on screen.
Cancel	Reverse any changes made since the last "Save."
View Log	Click this to open a sub-window where you can view the "Access Control" log. This log shows attempted Internet accesses which have been blocked by the Access Control feature.
Clear Log	Click this to clear and restart the "Access Control" log, making new entries easier to read.
Refresh	Update the data on screen.

## Group Members Screen

This screen is displayed when the Members button on the Access Control screen is clicked and when selecting a group.



**Figure 24** Group Members

Use this screen to add or remove members (PCs) from the current group.

- The "Del >>" button will remove the selected PC (in the Members list) from the current group.
- The "<< Add" button will add the selected PC (in the Other PCs list) to the current group.

---

### Note

PCs not assigned to any group will be in the "Default" group. PCs deleted from any other Group will be added to the "Default" group.

---

## Default Schedule Screen

This screen is displayed when the Define Schedule button on the Access Control screen is clicked.

- This schedule can be (optionally) applied to any Access Control Group.
- Blocking will be performed during the scheduled time (between the "Start" and "Finish" times.)
- Two separate sessions or periods can be defined.
- Times must be entered using a 24 hour clock.

- ❑ If the time for a particular day is blank, no action will be performed.

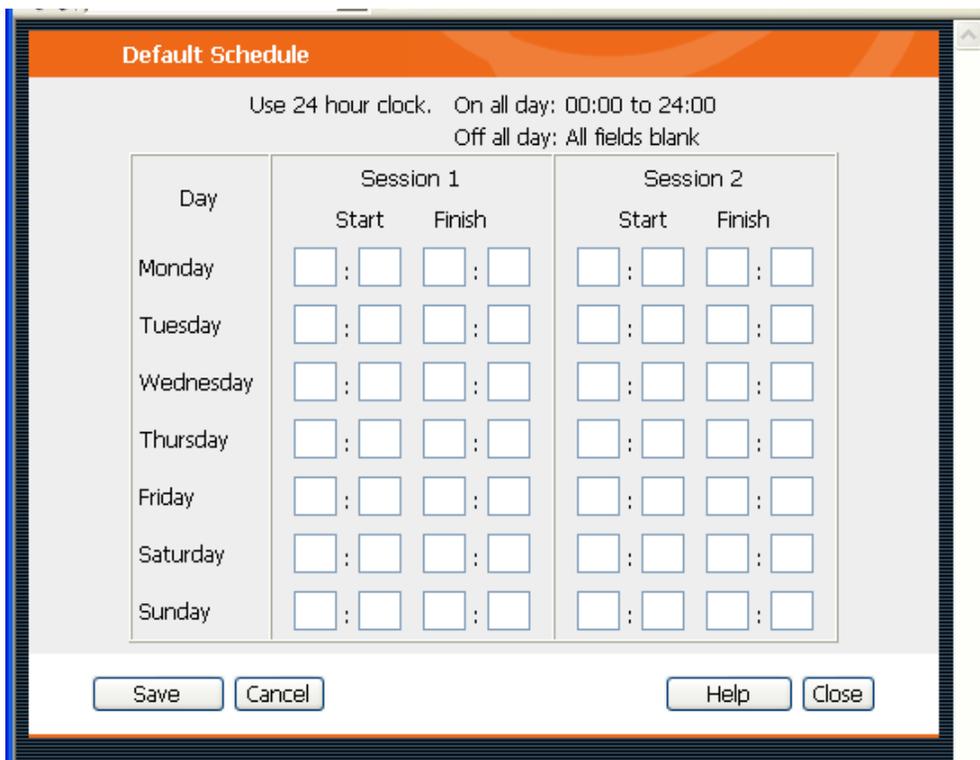


Figure 25 Default Schedule Screen

**Data - Default Schedule Screen**

<b>Day</b>	Each day of the week can scheduled independently.
<b>Session 1 Session 2</b>	Two separate sessions or periods can be defined. Session 2 can be left blank if not required.
<b>Start Time</b>	Enter the start using a 24 hour clock.
<b>Finish Time</b>	Enter the finish time using a 24 hour clock.

## Services Screen

This screen is displayed when the Edit Service List button on the Access Control screen is clicked.

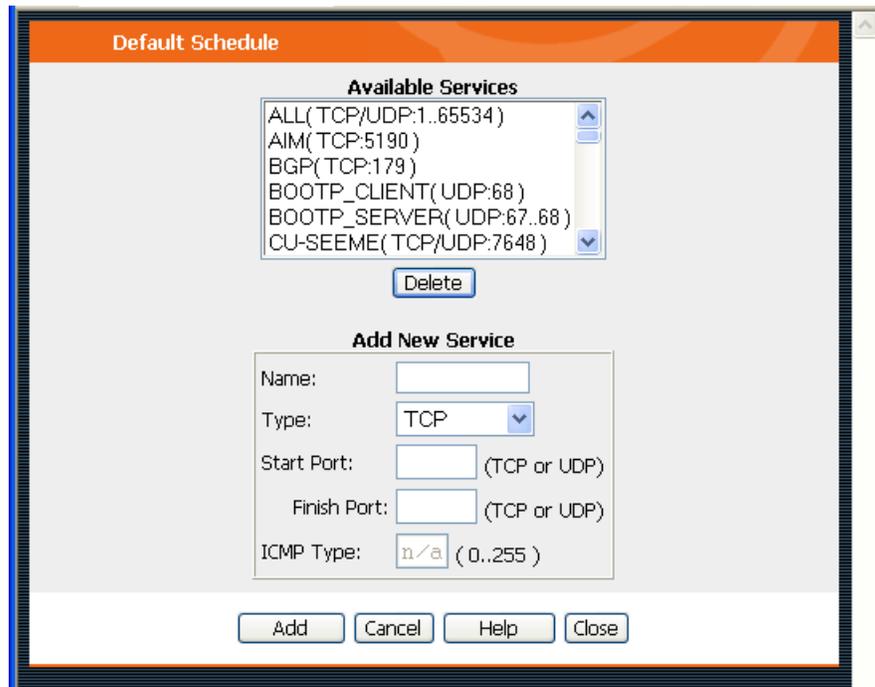


Figure 26 Access Control - Services

## Data - Services Screen

Available Services	
Available Services	This lists all the available services.
"Delete" button	Use this to delete any Service you have added. Predefined Services can not be deleted.
Add New Service	
Name	Enter a descriptive name to identify this service.
Type	Select the protocol (TCP, UDP, ICMP) used to the remote system or service.
Start Port	For TCP and UDP Services, enter the beginning of the range of port numbers used by the service. If the service uses a single port number, enter it in both the "Start" and "Finish" fields.

Finish Port	For TCP and UDP Services, enter the end of the range of port numbers used by the service. If the service uses a single port number, enter it in both the "Start" and "Finish" fields.
ICMP Type	For ICMP Services, enter the type number of the required service.
<b>Buttons</b>	
Delete	Delete the selected service from the list.
Save	Add a new entry to the Service list, using the data shown in the "Add New Service" area on screen.
Cancel	Clear the "Add New Service" area, ready for entering data for a new Service.

## Access Control Log

To check the operation of the Access Control feature, an Access Control Log is provided. Click the View Log button on the Access Control screen to view this log.

This log shows attempted Internet accesses which have been blocked by the Access Control function.

Data shown in this log is as follows:

<b>Date/Time</b>	Date and Time of the attempted access.
<b>Name</b>	If known, the name of the PC whose access was blocked.
<b>Source IP Address</b>	The IP Address of the PC or device whose access request was blocked
<b>MAC Address</b>	The hardware or physical address of the PC or device whose access request was blocked
<b>Destination</b>	The destination URL or IP address

## **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.

### **The Service works as follows:**

1. You must register for the service at <http://www.dyndns.org> (Registration is free). Your password will be e-mailed to you.
2. After registration, use the "Create New Host" option (at [www.dyndns.org](http://www.dyndns.org)) to request your desired Domain name.
3. Enter your data from [www.dyndns.org](http://www.dyndns.org) in the Wireless Router's DDNS screen.
4. The Wireless Router will then automatically ensure that your current IP Address is recorded at <http://www.dyndns.org>
5. From the Internet, users will be able to connect to your Virtual Servers (or DMZ PC) using your Domain name, as shown on this screen.

## Dynamic DNS Screen

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

The screenshot shows the Allied Telesyn AT-WA1004G web interface. On the left is a navigation menu with the following items: Home, Wizard, LAN, Wireless, Password, Status, and Advanced. Under the 'Advanced' section, there is a list of sub-menus: Internet, Access Control, Dynamic DNS (which is highlighted), Logs, PC Database, Options, Routing, Security, Upgrade, Virtual Servers, and Remote M'ment.

The main content area is titled 'DDNS (Dynamic DNS)'. It contains the following text and form fields:

**DDNS Service**  
Dynamic DNS allows you to provide Internet users with a domain name (instead of an IP Address) to access your Virtual Servers.  
Register for this FREE service at <http://www.dyndns.org>

**DDNS Data**  
User name is set when you register; your password is E-mailed to you.  
User Name:   
Password:   
Domain Name:  .  dyndns .  org  
Domain name allocated to you by www.dyndns.org

DDNS Status:

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

Figure 27 DDNS Screen

## Data - Dynamic DNS Screen

DDNS Service	
DDNS Service	<ul style="list-style-type: none"> <li><input type="checkbox"/> Select the desired DDNS Service Provider from the list. You must register for the service at one of the listed Service Providers. You can reach the Service provider's Web Site by selecting them in the list and clicking the "Web Site" button.</li> <li><input type="checkbox"/> Apply for a Domain Name, and ensure it is allocated to you.</li> <li><input type="checkbox"/> Details of your DDNS account (Name, password, Domain name) must then be entered and saved on this screen.</li> <li><input type="checkbox"/> This device will then automatically ensure that your current IP Address is recorded by the DDNS Service Provider. (You do NOT need to use the "Client" program provided by some DDNS Service providers.)</li> <li><input type="checkbox"/> From the Internet, users will now be able to connect to your Virtual Servers (or DMZ PC) using your Domain name.</li> </ul>
DDNS Data	
User Name	Enter your Username for the DDNS Service.
Password/Key	Enter your current password for the DDNS Service.
Domain Name	Enter the domain name allocated to you by the DDNS Service. If you have more than one name, enter the name you wish to use.
DDNS Status	<ul style="list-style-type: none"> <li><input type="checkbox"/> This message is returned by the DDNS Server</li> <li><input type="checkbox"/> Normally, this message should be "Update successful"</li> <li><input type="checkbox"/> If the message is "No host" or some other error message, you need to connect to the DDNS Service provider and correct the problem.</li> </ul>

## Advanced Internet Screen

This screen allows configuration of all advanced features relating to Internet access.

- Communication Applications
- Special Applications
- Multi-DMZ
- URL Filter

An example screen is shown below.

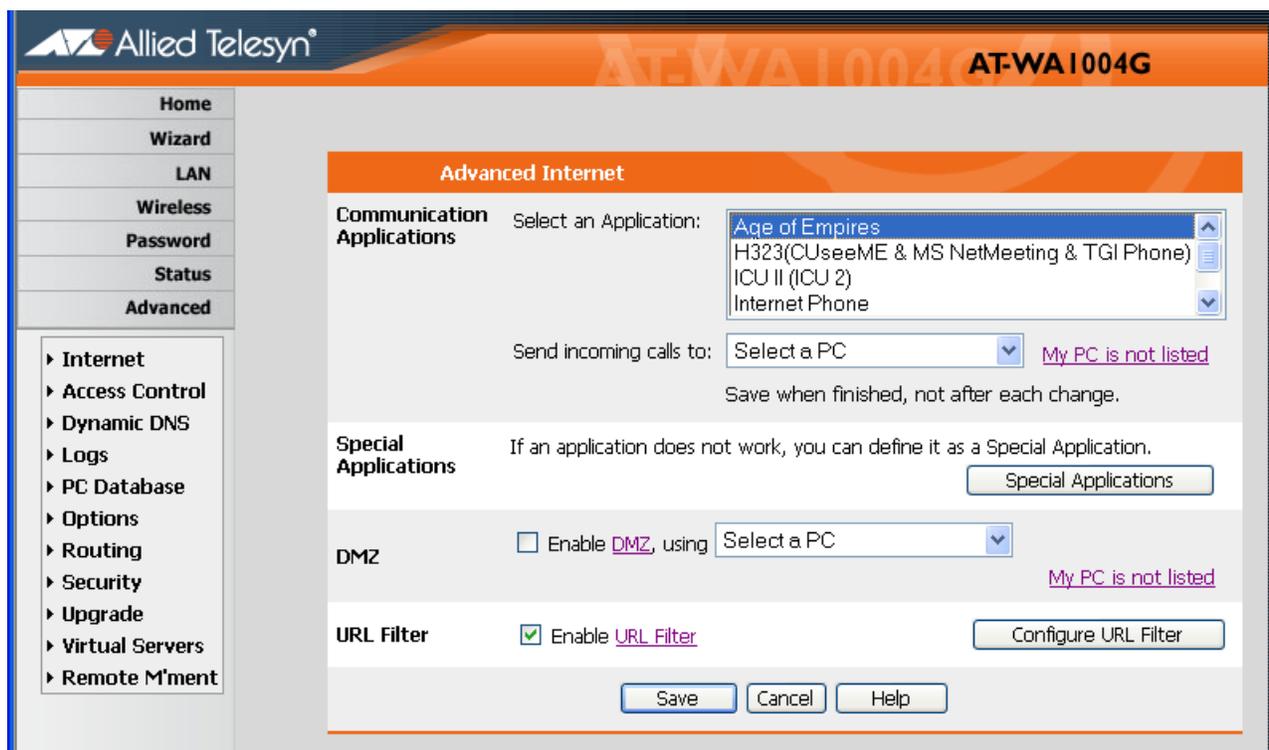


Figure 28 Internet Screen

## Communication Applications

Most applications are supported transparently by the Wireless Router. But sometimes it is not clear which PC should receive an incoming connection. This problem could arise with the Communication Applications listed on this screen.

If this problem arises, you can use this screen to set which PC should receive an incoming connection, as described below.

Communication Applications	
Select an Application	This lists applications which may generate incoming connections, where the destination PC (on your local LAN) is unknown.
Send incoming calls to	<p>This lists the PCs on your LAN.</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> If necessary, you can add PCs manually, using the "PC Database" option on the advanced menu.</li> <li><input type="checkbox"/> For each application listed above, you can choose a destination PC.</li> <li><input type="checkbox"/> There is no need to "Save" after each change; you can set the destination PC for each application, then click "Save."</li> </ul>

## 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."

## Special Applications Screen

This 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.

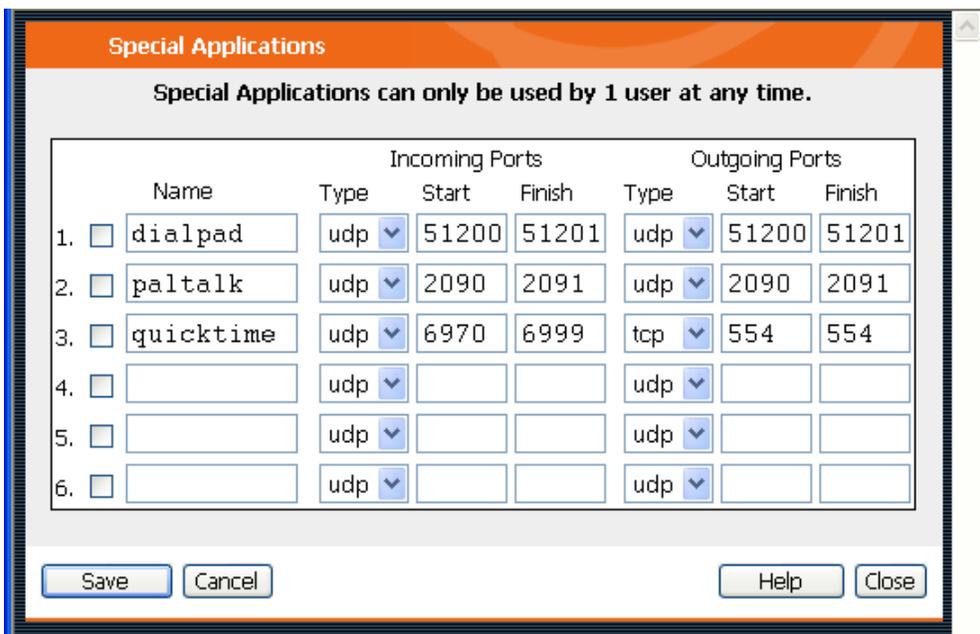


Figure 29 Special Applications Screen

**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.
Incoming Ports	<input type="checkbox"/> Type - Select the protocol (TCP or UDP) used when you receive data from the special application or service. (Note: Some applications use different protocols for outgoing and incoming data). <input type="checkbox"/> Start - Enter the beginning of the range of port numbers used by the application server, for data you receive. If the application uses a single port number, enter it in both the "Start" and "Finish" fields. <input type="checkbox"/> Finish - Enter the end of the range of port numbers used by the application server, for data you receive.

Outgoing Ports	<ul style="list-style-type: none"> <li><input type="checkbox"/> Type - Select the protocol (TCP or UDP) used when you send data to the remote system or service.</li> <li><input type="checkbox"/> Start - Enter the beginning of the range of port numbers used by the application server, for data you send to it. If the application uses a single port number, enter it in both the "Start" and "Finish" fields.</li> <li><input type="checkbox"/> Finish - Enter the end of the range of port numbers used by the application server, for data you send to it. If the application uses a single port number, enter it in both the "Start" and "Finish" fields.</li> </ul>
----------------	--

## Using a Special Application

- Configure the Special Applications screen as required.
- On your PC, use the application normally. Remember that only one PC can use each Special application at any time. Also, when one 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.

---

### Note

If an application still cannot function correctly, try using the "DMZ" feature.

---

## Multi-DMZ

This feature, if enabled, allows the DMZ computer or computers 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".

If you have multiple Internet IP addresses, you can assign one DMZ PC for each Internet IP address.

If you only have one WAN IP address, only "DMZ 1" can be used, and only one PC can be the DMZ PC. The current WAN IP address is displayed. If this address is assigned upon connection, and no connection currently exists, then this address will be blank or 0.0.0.0.

**Note**

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

**URL Filter**

The URL Filter allows you to block access to undesirable Web site

- To use this feature, you must define "filter strings." If the "filter string" appears in a requested URL, the request is blocked.
- Enabling the URL Filter also affects the Internet Access Log. If Enabled, the "Destination" field in the log will display the URL. Otherwise, it will display the IP Address.

**URL Filter Screen**

Click the "Configure URL Filter" button on the Internet screen to access the URL Filter screen.

**Data - URL Filter Screen**

<b>Filter Strings</b>	
Current Entries	This lists any existing entries. If you have not entered any values, this list will be empty.
Add Filter String	To add an entry to the list, enter it here, and click the "Add" button. An entry may be a Domain name (for example, www.trash.com) or simply a string. (for example, ads/) Any URL which contains ANY entry ANYWHERE in the URL will be blocked.
<b>Buttons</b>	
Delete/Delete All	Use these buttons to delete the selected entry or all entries, as required. Multiple entries can be selected by holding down the CTRL key while selecting. (On the Macintosh, hold the SHIFT key while selecting.)
Add	Use this to add the current Filter String to the site list.

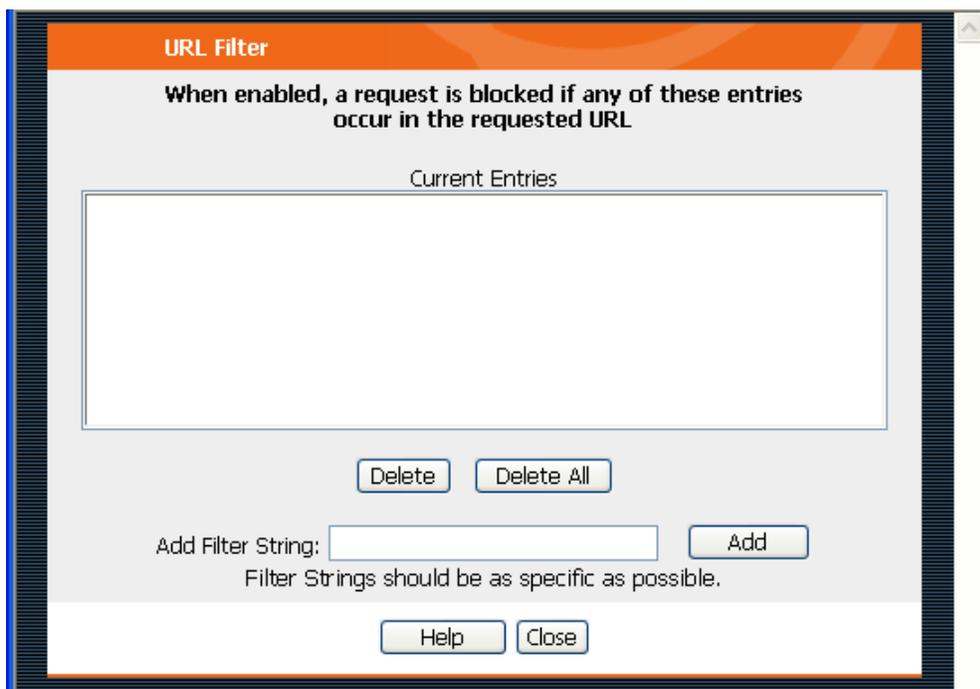
## Virtual Servers

---

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 30** 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 screen is reached by the Virtual Servers link on the Advanced screen. An example screen is shown below.

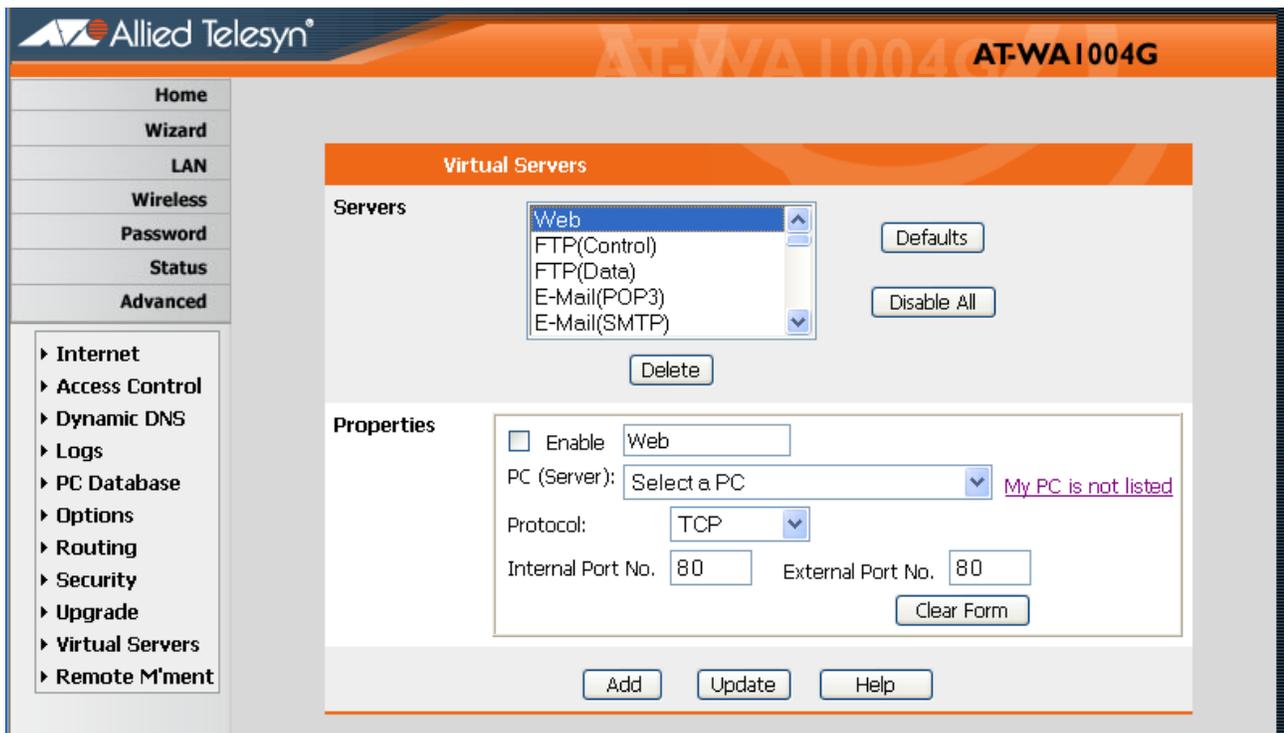


Figure 31 Virtual Servers Screen

This screen lists a number of pre-defined Servers, and allows you to define your own Servers. Details of the selected Server are shown in the “Properties” area.

### Data - Virtual Servers Screen

Servers	
Servers	This lists a number of pre-defined Servers, plus any Servers you have defined. Details of the selected Server are shown in the “Properties” area.
Properties	
Enable	Use this to Enable or Disable support for this Server, as required. <ul style="list-style-type: none"> <li><input type="checkbox"/> If Enabled, any incoming connections will be forwarded to the selected PC.</li> <li><input type="checkbox"/> If Disabled, any incoming connection attempts will be blocked.</li> </ul>

PC (Server)	Select the PC for this Server. The PC must be running the appropriate Server software.
Protocol	Select the protocol (TCP or UDP) used by the Server.
Internal Port No.	Enter the port number which the Server software is configured to use.
External Port No.	The port number used by Internet users when connecting to the Server. This is normally the same as the Internal Port Number. If it is different, this device will perform a "mapping" or "translation" function, allowing the server to use one port address, while clients use a different port address.
<b>Buttons</b>	
Defaults	This will delete any Servers you have defined, and set the pre-defined Servers to use their default port numbers.
Disable All	This will cause the "Enable" setting of all Virtual Servers to be set OFF.
Update	Update the current Virtual Server entry, using the data shown in the "Properties" area on screen.
Add	Add a new entry to the Virtual Server list, using the data shown in the "Properties" area on screen. The entry selected in the list is ignored, and has no effect.
Delete	Delete the current Virtual Server entry. Note that the pre-defined Servers can not be deleted. Only Servers you have defined yourself can be deleted.
Clear Form	Clear all data from the "Properties" area, ready for input of a new Virtual Server entry.

**Note**

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

## Defining Your Own Virtual Servers

If the type of Server you wish to use is not listed on the Virtual Servers screen, you can define and manage your own Servers:

Create a new Server:	<ol style="list-style-type: none"> <li>1. Click "Clear Form".</li> <li>2. Enter the required data, as described above.</li> <li>3. Click "Add".</li> <li>4. The new Server will now appear in the list.</li> </ol>
Modify (Edit) a Server:	<ol style="list-style-type: none"> <li>1. Select the desired Server from the list.</li> <li>2. Make any desired changes (for example, change the Enable/Disable setting).</li> <li>3. Click "Update" to save changes to the selected Server.</li> </ol>
Delete a Server:	<ol style="list-style-type: none"> <li>1. Select the entry from the list.</li> <li>2. Click "Delete".</li> </ol> <p><b>Note:</b> You can only delete Servers you have defined. Pre-defined Server cannot be deleted.</p>

---

### Note

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

---

## 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).

For example:

```
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, described in the following section, to allow users to connect to your Virtual Servers using a URL, rather than an IP Address.



## Chapter 7

# Advanced Administration

---

This chapter contains the following sections:

- ❑ [Overview](#) on page 104
- ❑ [Logs](#) on page 105
- ❑ [Options](#) on page 108
- ❑ [PC Database](#) on page 112
- ❑ [Remote Management](#) on page 117
- ❑ [Routing](#) on page 119
- ❑ [Security](#) on page 123
- ❑ [Upgrade](#) on page 125

## 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>Options</b>	Various options, such as backup DNS, UPnP and WAN Port.
<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>Remote Management</b>	Allow settings to be changed from the Internet.
<b>Routing</b>	Only required if your LAN has other Routers or Gateways.
<b>Security</b>	Firewall and other security-related settings. Normally, the default settings do not need to be changed.
<b>Upgrade</b>	Upgrade the Firmware (software) installed in your Wireless Router.

## Logs

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

Since only a limited amount of log data can be stored in the Wireless Router, log data can also be E-mailed to your PC.

The screenshot displays the 'Logs' configuration page for the AT-WA1004G router. The page is divided into several sections:

- Enable Logs:** Three checkboxes are checked: 'Outgoing (Internet) connections', 'Access Control', and 'DoS (Denial of Service) attacks'. Each has a corresponding 'View Log' and 'Clear Log' button.
- Timezone:** A dropdown menu is set to '(GMT) Greenwich Mean Time : Edinburgh, London'.
- E-Mail Reports:**
  - Send E-mail alert immediately when attacked
  - E-mail Logs:**
    - Connection Log
    - Access Control Log
  - Send:**
    - When log is full
    - Every Sunday at 1 AM
- E-Mail Address:**
  - E-mail address: [text input]
  - Subject: [text input, value: Logs]
  - SMTP Server:
    - Address: [text input]
    - IP address: [0] . [0] . [0] . [0]
  - Port No.: [25] (Default: 25)

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

Figure 32 Logs Screen

## Data - Logs Screen

<b>Enable Logs</b>	
Outgoing Connections	If selected, Outgoing Internet connections are logged. Normally, the (Internet) "Destination" will be shown as an IP address. But if the "URL Filter" is enabled, the "Destination" will be shown as a URL.
Access Control	If enabled, the log will include attempted outgoing connections which have been blocked by the "Access Control" feature.
DoS Attacks	If enabled, this log will show details of DoS (Denial of Service) attacks which have been blocked by the built-in firewall.
Timezone	Select the correct Timezone for your location. This is required for the date/time shown on the logs to be correct.
<b>E-Mail Reports</b>	
Send E-mail Alert	If enabled, an e-mail will be sent immediately if a DoS (Denial of Service) attack is detected. If enabled, the e-mail address information must be provided.
E-mail Logs	You can choose to have the logs E-mailed to you, by enabling either or both check boxes. If enabled, the Log will be sent to the specified e-mail address. The interval between e-mails is determined by the "Send" setting.

Send	<p>Select the desired option for sending the log by e-mail.</p> <p><input type="checkbox"/> <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.</p> <p><input type="checkbox"/> <b>Every day, Every Monday...</b> - The log is sent on the interval specified.</p> <ul style="list-style-type: none"> <li>— If “Every day” is selected, the log is sent at the time specified.</li> <li>— If the day is specified, the log is sent once per week, on the specified day.</li> <li>— Select the time of day you wish the E-mail to be sent.</li> <li>— If the log is full before the time specified to send it, it will be sent regardless.</li> </ul>
<b>E-Mail Address</b>	
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.
Subject	Enter the text string to be shown in the “Subject” field for the e-mail.
SMTP Server	Enter the address or IP address of the SMTP (Simple Mail Transport Protocol) Server you use for outgoing e-mail.
Port No.	Enter the port number used to connect to the SMTP Server. The default value is 25.

# 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.

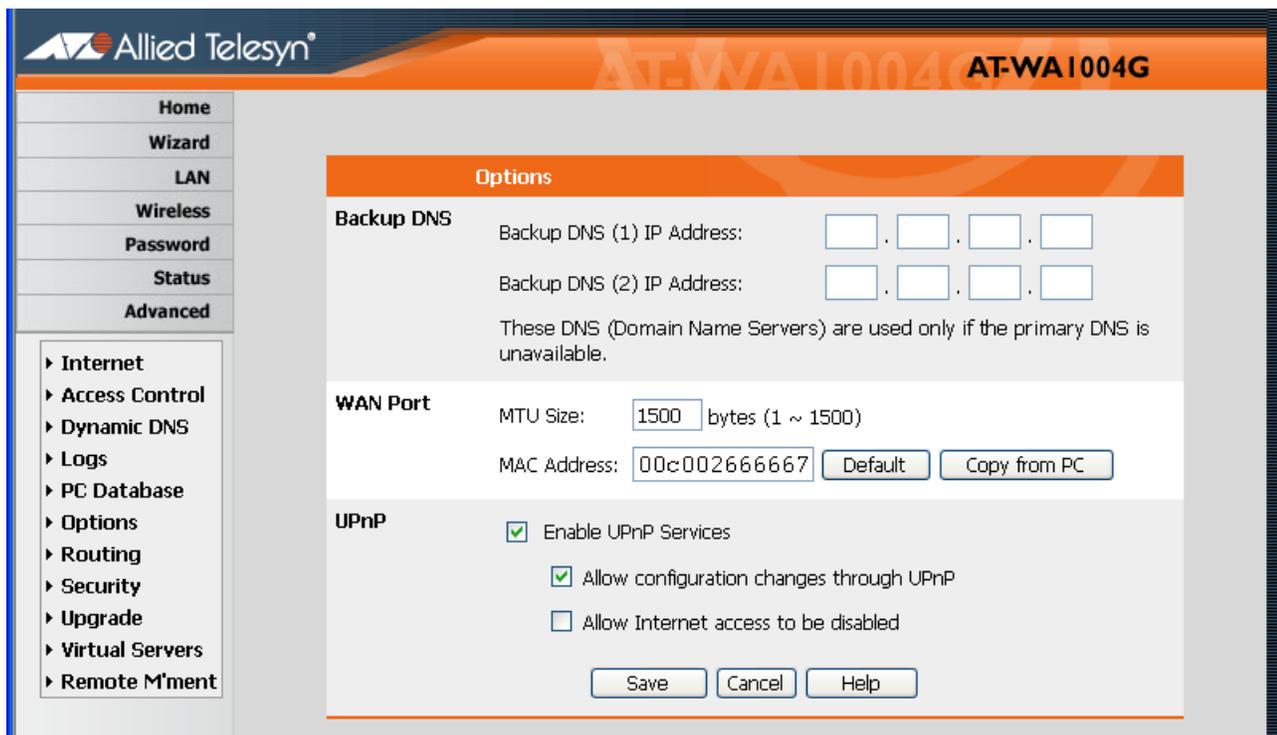


Figure 33 Options Screen

**Data - Options Screen**

<b>Backup DNS</b>	
IP Address	Enter the IP Address of the DNS (Domain Name Servers) here. These DNS will be used only if the primary DNS is unavailable.
<b>WAN Port</b>	
Default	Inserts the default MAC address into the MAC address field. You must click "Save" to actually change the address used.
Copy from PC	Inserts the MAC address from your PC into the MAC address field. You must click "Save" to actually change the address used.
Save	Save your changes to the Wireless Router.
Cancel	Reverse any changes made since that last "Save".
<b>UPnP</b>	
Enable UPnP Services	<input type="checkbox"/> UPnP (Universal Plug and Play) allows automatic discovery and configuration of equipment attached to your LAN. UPnP is by supported by Windows ME, XP, or later. <input type="checkbox"/> If Enabled, this device will be visible via UPnP. <input type="checkbox"/> If Disabled, this device will not be visible via UPnP.
Allow Configuration...	<input type="checkbox"/> If checked, then UPnP users can change the configuration. <input type="checkbox"/> If Disabled, UPnP users can only view the configuration. But currently, this restriction only applies to users running Windows XP, who access the Properties via UPnP. (For example, right-click the Wireless Router in My Network Places, and then select Properties),

<p>Allow Internet access to be disabled</p>	<ul style="list-style-type: none"> <li><input type="checkbox"/> If checked, then UPnP users can disable Internet access via this device.</li> <li><input type="checkbox"/> If Disabled, UPnP users can NOT disable Internet access via this device. But currently, this restriction only applies to users running Windows XP, who access the Properties via UPnP. (For example, right-click the Wireless Router in My Network Places, and then select Properties).</li> </ul>
<p><b>WAN Port</b></p>	
<p>MTU size</p>	<p>MTU (Maximum Transmission Unit) value should only be changed if advised to do so by Technical Support.</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Enter a value between 1 and 1500.</li> <li><input type="checkbox"/> This device will still auto-negotiate with the remote server, to set the MTU size. The smaller of the 2 values (auto-negotiated, or entered here) will be used.</li> <li><input type="checkbox"/> For direct connections (not PPPoE or PPTP), the MTU used is always 1500.</li> </ul>

MAC Address	<p>Overview:</p> <ul style="list-style-type: none"><li><input type="checkbox"/> This address is a low-level network identifier for this device. It may be called "MAC Address", "Hardware Address", or "Physical Address". On a PC, this address is associated with the Network card or adapter.</li><li><input type="checkbox"/> The address here in on the WAN (Internet) port, and has no effect on the LAN interface.</li><li><input type="checkbox"/> If your ISP asks for the Network Adapter Address, Physical Address, Hardware Address, or MAC Address for the PC the DSL/Cable modem is connected to, provide this value.</li><li><input type="checkbox"/> If your ISP has already recorded a MAC address, you can change the address used by the AT-WA1004G to match the address recorded by your ISP.</li><li><input type="checkbox"/> If the address is changed, the router must restart.</li></ul> <p><b>Changing the MAC address:</b></p> <ul style="list-style-type: none"><li><input type="checkbox"/> You can enter the desired MAC address directly.</li><li><input type="checkbox"/> Click the "Default" button to insert the default MAC address into the address field. You must click "Save" to actually change the address used.</li><li><input type="checkbox"/> Click the "Copy from PC" button to copy the MAC address from your PC (actually, the network adapter on your PC) to the address field. You must click "Save" to actually change the address used.</li><li><input type="checkbox"/> If your ISP has recorded a Hardware Address, you can "spoof" that address by entering it in the address field. The hardware address consists of 12 HEX characters, where each character is a digit (0..9) or a character between A and F.</li></ul>
-------------	---

## PC Database

The PC Database is used whenever you need to select a PC (for example, 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.

### PC Database Screen

An example PC Database screen is shown below.

**Figure 34** PC Database

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

**Data - PC Database Screen**

Known PCs	This lists all current entries. Data displayed is name (IP Address) type. The "type" indicates whether the PC is connected to the LAN.
Name	If adding a new PC to the list, enter its name here. It is best if this matches the PC's "hostname".
IP Address	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>	
Add	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.
Delete	Delete the selected PC from the list. This should be done in 2 situations: <input type="checkbox"/> The PC has been removed from your LAN. <input type="checkbox"/> The entry is incorrect.
Refresh	Update the data on screen.
Generate Report	Display a read-only list showing full details of all entries in the PC database.
Advanced Administration	View the Advanced version of the PC database screen - PC Database (Admin). See below for details.

## PC Database (Admin)

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.

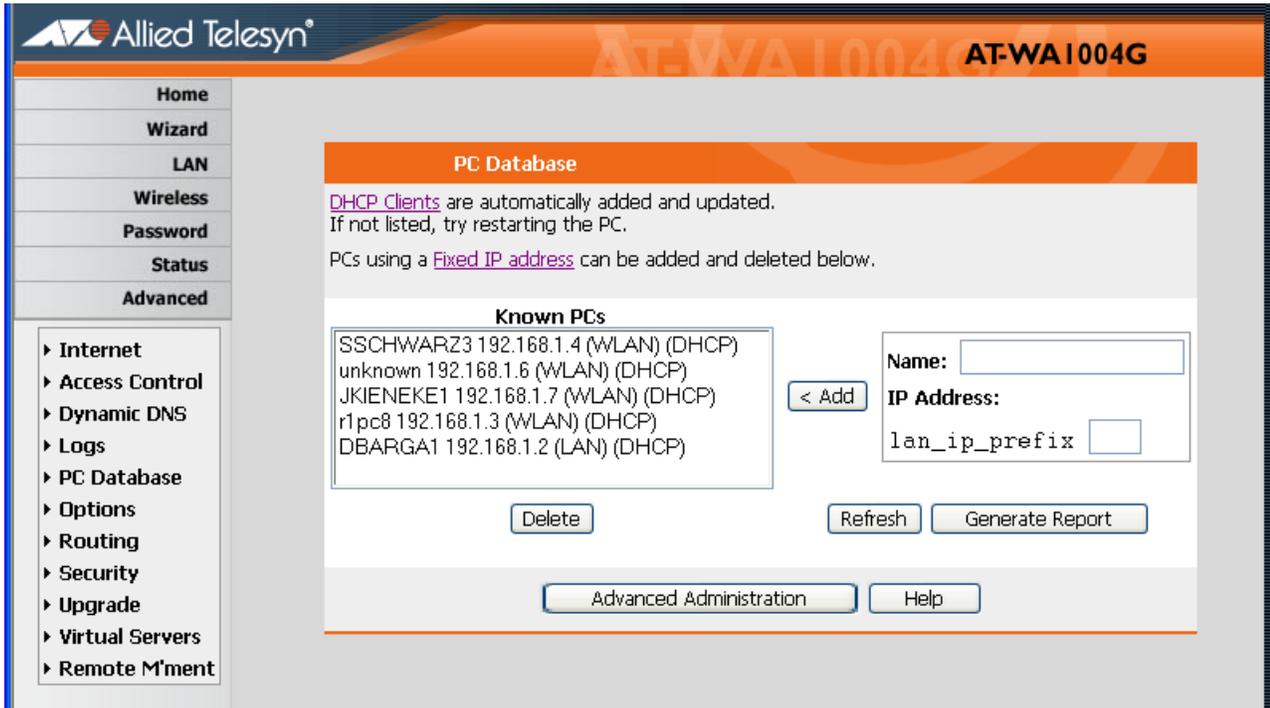


Figure 35 PC Database (Admin)

### Data - PC Database (Admin) Screen

Known PCs	This lists all current entries. Data displayed is name (IP Address) type. The "type" indicates whether the PC is connected to the LAN.
<b>PC Properties</b>	
Name	If adding a new PC to the list, enter its name here. It is best if this matches the PC's "hostname".

IP Address	<p>Select the appropriate option:</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> <b>Automatic</b> - The PC is set to be a DHCP client (Windows: "Obtain an IP address automatically"). The Wireless Router will allocate an IP address to this PC when requested to do so. The IP address could change, but normally won't.</li> <li><input type="checkbox"/> <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 Router will always allocate the same IP Address to this PC. Enter the required IP address. Only the last field is required; the other fields must match the Wireless Router's IP address.</li> <li><input type="checkbox"/> <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 must be configured to use this IP address.)</li> </ul>
MAC Address	<p>Select the appropriate option:</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> <b>Automatic discovery</b> - Select this to have the Wireless Router contact the PC and find its MAC address. This is only possible if the PC is connected to the LAN and powered On.</li> <li><input type="checkbox"/> <b>MAC 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 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>	
Add as New Entry	Add a new PC to the list, using the data in the "Properties" box. If "Automatic discovery" (for MAC address) is selected, the PC will be sent a "ping" to determine its hardware address. This will fail unless the PC is connected to the LAN, and powered ON.
Update Selected PC	Update (modify) the selected PC, using the data in the "Properties" box.
Clear Form	Clear the "Properties" box, ready for entering data for a new PC.
Refresh	Update the data on screen.

Generate Report	Display a read-only list showing full details of all entries in the PC database.
Standard Screen	Click this to view the standard PC Database screen.

## Remote Management

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

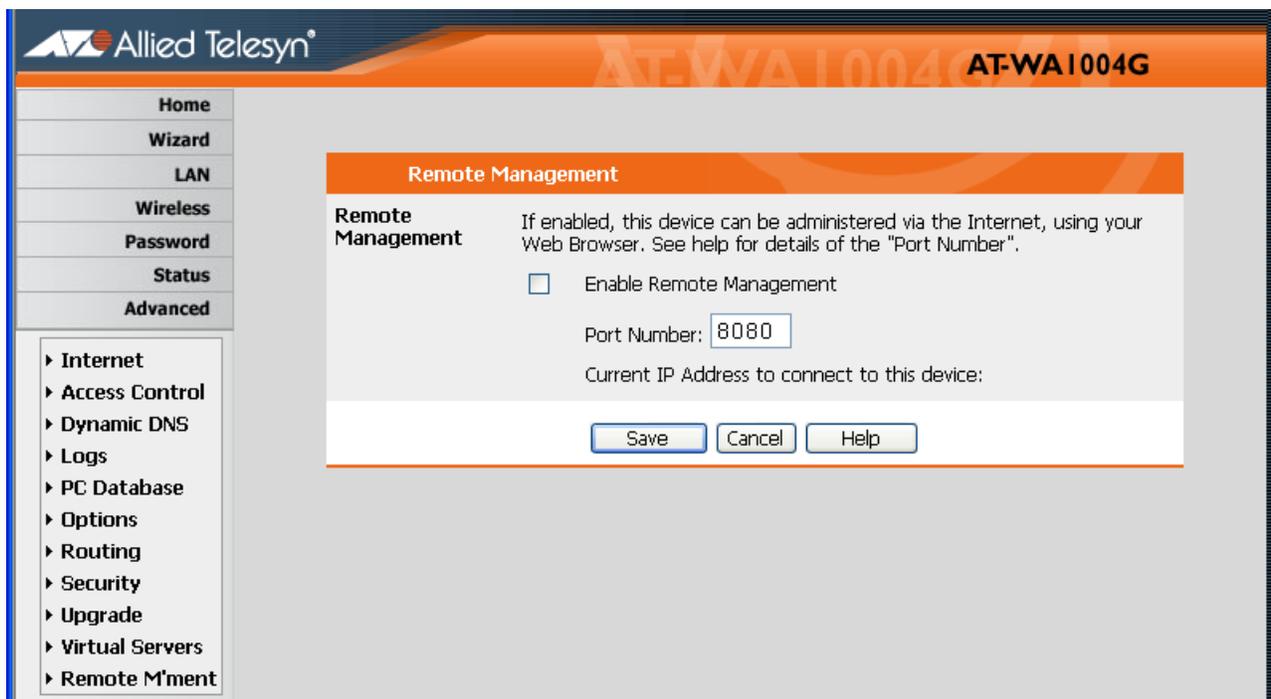


Figure 36 Remote Administration Screen

### Data - Remote Administration Screen

Remote Administration	
Enable Remote Management	Enable to allow management via the Internet. If Disabled, this device will ignore management connection attempts from the Internet.
Port Number	Enter a port number between 1024 and 65535 (8080 is recommended). This port number must be specified when you connect (see below). <b>Note:</b> The default port number for http (Web) connections is port 80, but using port 80 here will prevent the use of a Web "Virtual Server" on your LAN. (See <a href="#">Virtual Servers</a> on page 98)

Current IP Address	You must use this IP Address to connect (see below).  This IP Address is allocated by your ISP. But if using a Dynamic IP Address, this value can change each time you connect to your ISP. So it is better if your ISP allocates you a Fixed IP Address.
--------------------	---

**To connect from a remote PC via the Internet**

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

`http://123.123.123.123:8080`

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

# Routing

---

## Overview

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

## Routing Screen

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

### Using this Screen

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

## Static Routing Table

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

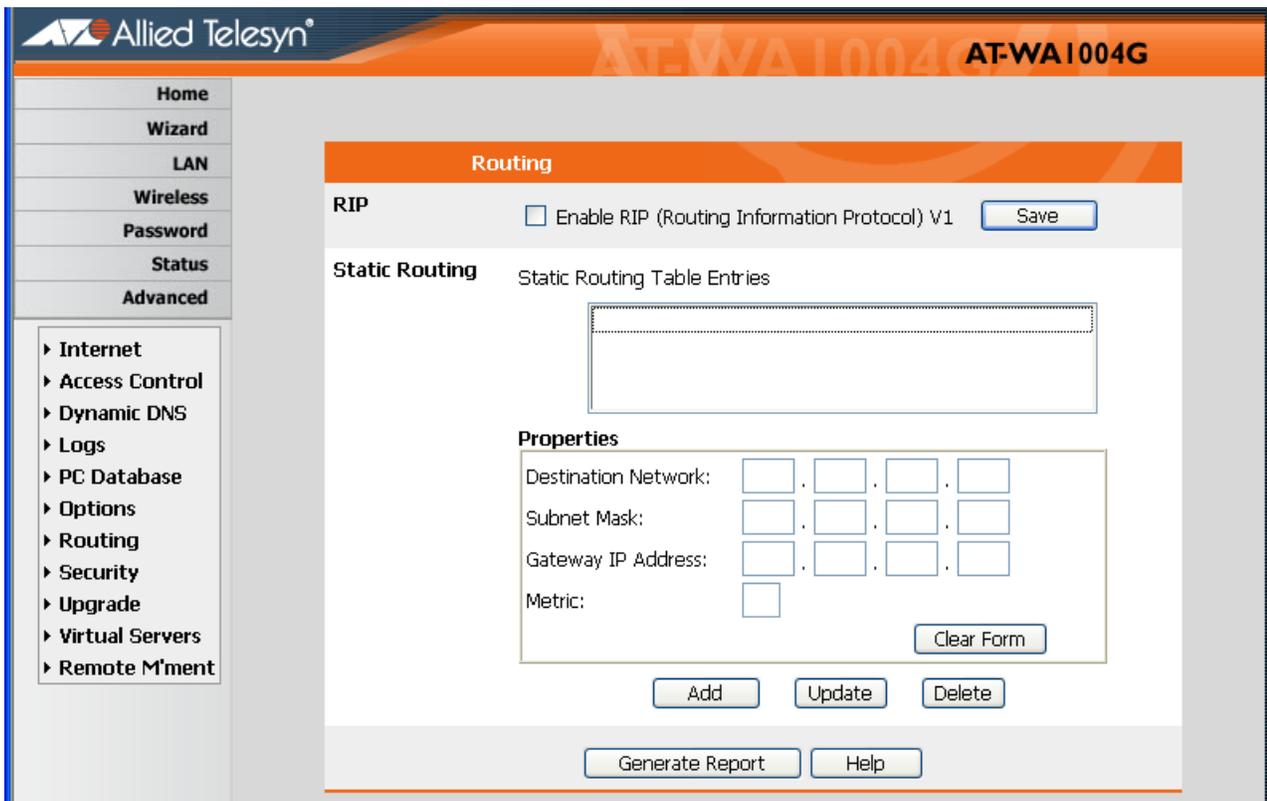


Figure 37 Routing Screen

## Data - Routing Screen

<b>RIP</b>	
Enable RIP	Check this to enable the RIP (Routing Information Protocol) feature of the Wireless Router. The Wireless Router supports RIP 1 only.
<b>Static Routing</b>	
Static Routing Table Entries	<p>This list shows all entries in the Routing Table.</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> The "Properties" area shows details of the selected item in the list.</li> <li><input type="checkbox"/> Change any the properties as required, then click the "Update" button to save the changes to the selected entry.</li> </ul>
Properties	<ul style="list-style-type: none"> <li><input type="checkbox"/> <b>Destination Network</b> - The network address of the remote LAN segment. For standard class "C" LANs, the network address is the first 3 fields of the Destination IP Address. The 4th (last) field can be left at 0.</li> <li><input type="checkbox"/> <b>Network Mask</b> - The Network Mask for the remote LAN segment. For class "C" networks, the default mask is 255.255.255.0</li> <li><input type="checkbox"/> <b>Gateway IP Address</b> - The IP Address of the Gateway or Router which the Wireless Router must use to communicate with the destination above. (NOT the router attached to the remote segment.)</li> <li><input type="checkbox"/> <b>Metric</b> - The number of "hops" (routers) to pass through to reach the remote LAN segment. The shortest path will be used. The default value is 1.</li> </ul>
<b>Buttons</b>	
Save	Save the RIP setting. This has no effect on the Static Routing Table.
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.
Update	Update the current Static Routing Table entry, using the data shown in the "Properties" area on screen.
Delete	Delete the current Static Routing Table entry.

Clear Form	Clear all data from the "Properties" area, ready for input of a new entry for the Static Routing table.
Generate Report	Generate a read-only list of all entries in the Static Routing table.

## Configuring Other Routers on your LAN

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

### Local Router

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

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

### Other Routers on the Local LAN

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

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

## Security

This screen allows you to set firewall and other security-related options.

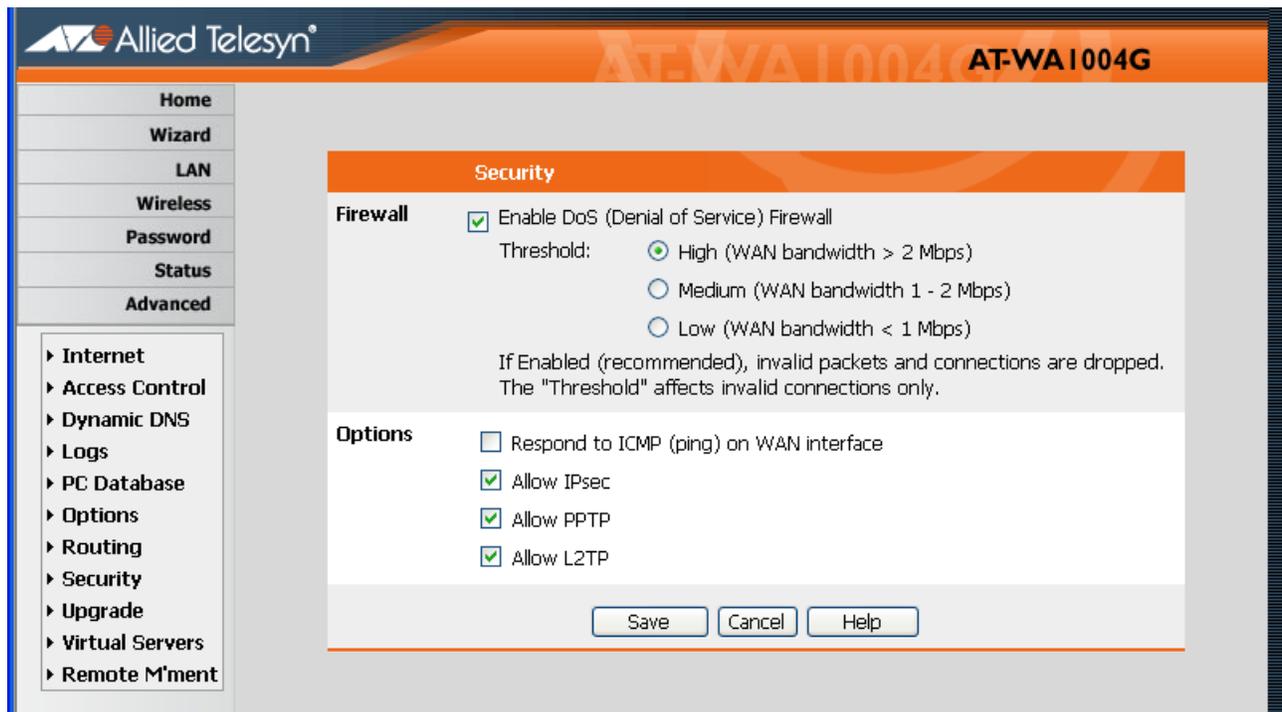


Figure 38 Security Screen

### Data - Security Screen

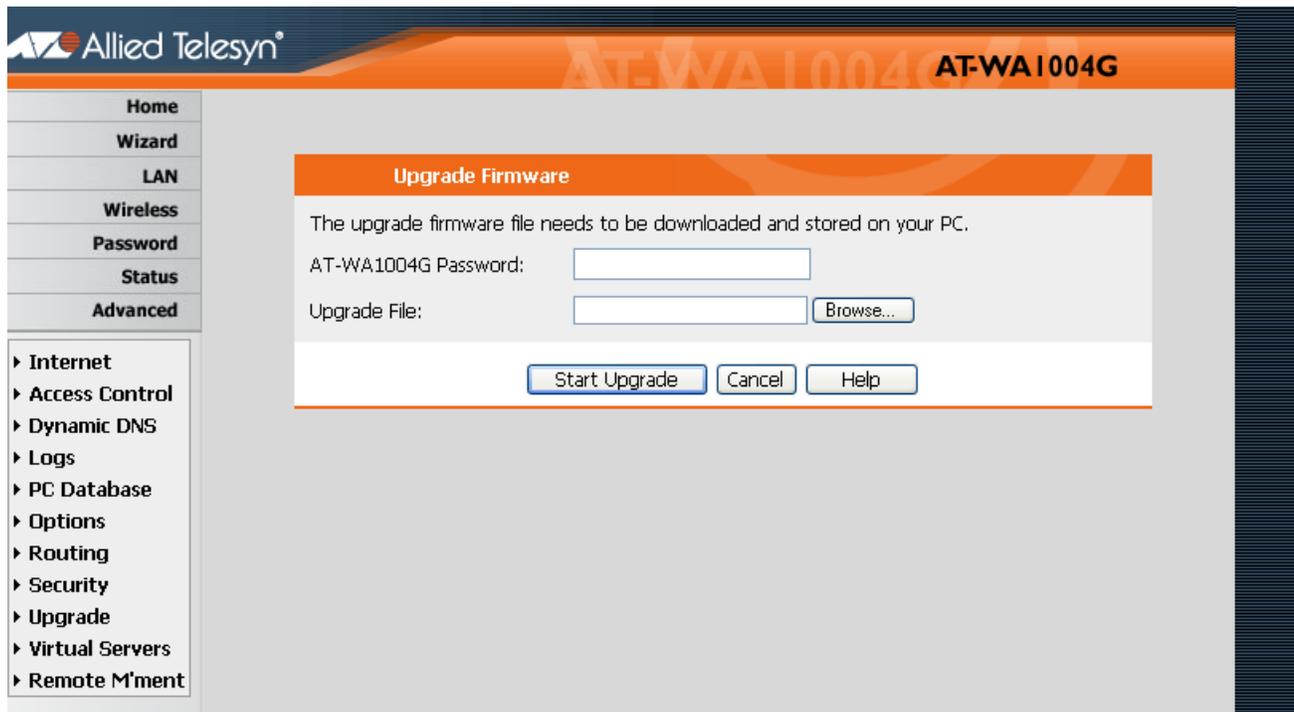
Firewall	
Enable DoS Firewall	<p>If enabled, DoS (Denial of Service) attacks will be detected and blocked. The default is enabled. It is strongly recommended that this setting be left enabled.</p> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li><input type="checkbox"/> A DoS attack does not attempt to steal data or damage your PCs, but overloads your Internet connection so you can not use it - the service is unavailable.</li> <li><input type="checkbox"/> This device uses "Stateful Inspection" technology. This system can detect situations where individual TCP/IP packets are valid, but collectively they become a DoS attack.</li> </ul>

Threshold	<p>This setting affects the number of “half-open” connections allowed.</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> A “half-open” connection arises when a remote client contacts the Server with a connection request, but then does not reply to the Server's response.</li> <li><input type="checkbox"/> While the optimum number of “half-open” connections allowed (the “Threshold”) depends on many factors, the most important factor is the available bandwidth of your Internet connection.</li> <li><input type="checkbox"/> Select the setting to match the bandwidth of your Internet connection.</li> </ul>
<b>Options</b>	
Respond to ICMP	<p>The ICMP protocol is used by the “ping” and “tracert” programs, and by network monitoring and diagnostic programs.</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> If checked, the Wireless Router will respond to ICMP packets received from the Internet.</li> <li><input type="checkbox"/> If not checked, ICMP packets from the Internet will be ignored. Disabling this option provides a slight increase in security.</li> </ul>
Allow IPsec	<p>The IPsec protocol is used to establish a secure connection, and is widely used by VPN (Virtual Private Networking) programs.</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> If checked, IPsec connections are allowed.</li> <li><input type="checkbox"/> If not checked, IPsec connections are blocked.</li> </ul>
Allow PPTP	<p>PPTP (Point to Point Tunneling Protocol) is widely used by VPN (Virtual Private Networking) programs.</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> If checked, PPTP connections are allowed</li> <li><input type="checkbox"/> If not checked, PPTP connections are blocked.</li> </ul>
Allow L2TP	<p>L2TP is a protocol developed by Cisco for VPNs (Virtual Private Networks).</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> If checked, L2TP connections are allowed.</li> <li><input type="checkbox"/> If not checked, L2TP connections are blocked.</li> </ul>

# Upgrade

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

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



**Figure 39** Upgrade Firmware Screen

To perform the Firmware Upgrade:

1. Click **Browse** 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 **Start Upgrade** to commence the firmware upgrade.

---

### Note

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

---



# Appendix A

# Troubleshooting

---

This appendix covers the most likely problems and their solutions. This appendix also contains the following sections:

- ❑ [Overview](#) on page 128
- ❑ [General Problems](#) on page 129
- ❑ [Internet Access](#) on page 130
- ❑ [Wireless Access](#) on page 131

## Overview

---

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

## General Problems

---

### Cannot connect to the Wireless Router to configure it.

Check the following:

- The Wireless Router is properly installed, LAN connections are OK, and it is powered ON.
- Ensure that your PC and the Wireless Router are on the same network segment. (If you don't have a router, this must be the case.)
- If your PC is set to "Obtain an IP Address automatically" (DHCP client), restart it.
- If your PC uses a Fixed (Static) IP address, ensure that it is using an IP Address within the range 192.168.0.2 to 192.168.0.254 and thus compatible with the Wireless Router's default IP Address of 192.168.1.1. Also, the Network Mask should be set to 255.255.255.0 to match the Wireless Router.

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

## Internet Access

---

### **When I enter a URL or IP address I get a time out error.**

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

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

### **Some applications do not run properly when using the Wireless Router.**

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

Use the Special Applications feature to allow the use of Internet applications which do not function correctly.

If this does solve the problem you can 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

---

### **My PC cannot locate the Wireless Access Point.**

Check the following:

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

### **Wireless connection speed is very slow.**

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

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



## Appendix B

# About Wireless LANs

---

This appendix provides some background information about using Wireless LANs (WLANs). This appendix also contains the following sections:

- ❑ [Modes](#) on page 134
- ❑ [BSS/ESS](#) on page 135
- ❑ [Channels](#) on page 136
- ❑ [WEP](#) on page 137
- ❑ [Wireless LAN Configuration](#) on page 138

## 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 (for example, 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 (for example, Notebook PCs with wireless cards) to a wired (Ethernet) LAN. The Wireless Stations can then access all LAN resources.

---

#### **Note**

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.

## 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>WEP</b>	The Wireless Stations and the Access Point must use the same settings for WEP (OFF, 64-bit, 128-bit). <b>WEP Key:</b> If WEP is enabled, the Key must be the same on the Wireless Stations and the Access Point. <b>WEP Authentication:</b> If WEP is enabled, all Wireless Stations must use the same setting as the Access Point (either "Open System" or "Shared Key").

# Appendix C

# Specifications

---

This appendix contains the following sections:

- ❑ [Multi-Function Wireless Router](#) on page 140
- ❑ [Wireless Interface](#) on page 141
- ❑ [Regulatory Approvals](#) on page 142

## Multi-Function Wireless Router

---

Model	Wireless Router
Dimensions	W x D x H 141 mm x 100 mm x 27 mm
Operating Temperature	0° C to 40° C
Storage Temperature	-10° C to 70° C
Network Protocol	TCP/IP
Network Interface	5 Ethernet: 4 * 10/100Base-T (RJ45) LAN connection 1 * 10/100Base-T (RJ45) for WAN
LEDs	12
Power Adapter	12 V DC External

## Wireless Interface

---

Standards	IEEE802.11g WLAN, JEIDA 4.2, roaming support
Frequency	2.4 to 2.4835 GHz (Industrial Scientific Medical Band)
Channels	Maximum 14 channels, depending on regulatory authorities
Modulation	DSSS BPSK/QPSK/CCK, OFDM/CCK
Data Rate	Up to 54 Mbps
Coverage Area	Indoors: 15 m @54 Mbps, 120 m @ 6 Mbps or lower Outdoors: 40 m @54 Mbps, 300 m @ 6 Mbps or lower
WEP	64-bit, 128-bit
Output Power	13 dBm (typical)
Receiver Sensitivity	-80 dBm minimum

## Regulatory Approvals

---

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

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

**CE Marking  
Warning** This is a Class B product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.