802.11g Wireless ADSL Firewall Router

ADW-4300A / ADW-4300B

User's Manual

Copyright

Federal Communication Commission Interference Statement

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

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

FCC Caution:

To assure continued compliance.(example-use only shielded interface cables when connecting to computer or peripheral devices). Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.
This device complies with Part 15 of the FCC Rules. Operation is subject to the Following two conditions: (1) This device may not cause harmful interference, and (2) this Device must accept any interference received, including interference that may cause undesired operation.

Federal Communication Commission (FCC) Radiation Exposure Statement

This equipment complies with FCC radiation exposure set forth for an uncontrolled environment. In order to avoid the possibility of exceeding the FCC radio frequency exposure limits, human proximity to the antenna shall not be less than 20 cm(8 inches) during normal operation.

R&TTE Compliance Statement

This equipment complies with all the requirements of DIRECTIVE 1999/5/CE OF THE EUROPEAN PARLIAMENT AND THE COUNCIL OF 9 March 1999 on radio equipment and telecommunication terminal Equipment and the mutual recognition of their conformity (R&TTE)
The R&TTE Directive repeals and replaces in the directive 98/13/EEC (Telecommunications Terminal Equipment and Satellite Earth Station Equipment) As of April 8,2000.

Safety

This equipment is designed with the utmost care for the safety of those who install and use it. However, special attention must be paid to the dangers of electric shock and static electricity when working with electrical equipment. All guidelines of this and of the computer manufacture must therefore be allowed at all times to ensure the safe use of the equipment.

Revision

User's Manual for PLANET 802.11g ADSL Wireless Firewall Router
Model: ADW-4300A / ADW-4300B
Rev: 1.0 (March. 2004)
Part No. EM-ADW4300

Table of Contents

Chapter 1
Introduction

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

Congratulations on the purchase of your new ADSL Wireless Firewall Router, ADW-4300. The ADSL Wireless Firewall Router is a multi-function device providing the following services:

- ***ADSL Modem***.
- ***Shared Broadband Internet Access*** for all LAN users.
- ***Wireless Access Point*** for 802.11b and 802.11g Wireless Stations.
- ***4-Port Switch*** for 10Base-T or 100Base-TX connections.

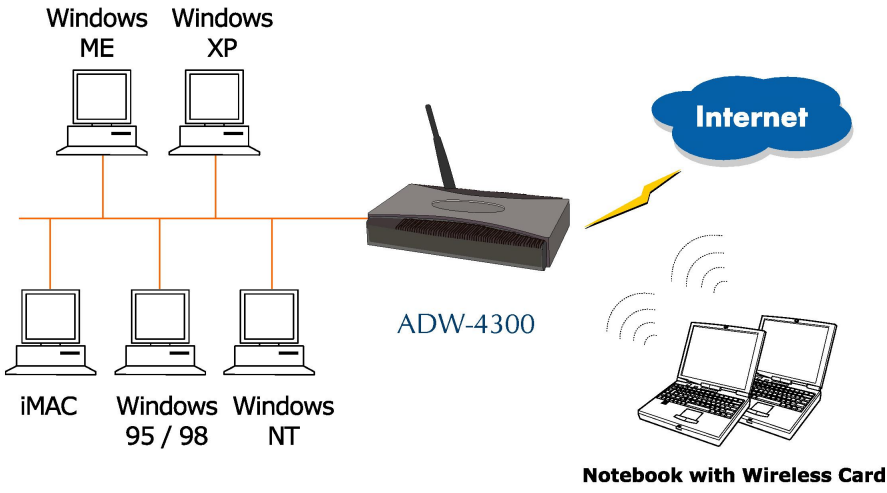


Figure 1: ADSL Wireless Firewall Router

ADSL Wireless Firewall Router Features

The ADSL Wireless Firewall 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 ADSL Wireless Firewall Router, using only a single external IP Address. The local (invalid) IP Addresses are hidden from external sources. This process is called NAT (Network Address Translation).
- ***Built-in ADSL Modem.*** The ADSL Wireless Firewall Router has a built-in ADSL modem, supporting all common ADSL connections.
- ***IPoA, PPPoE, PPPoA, Direct Connection Support.*** The ADSL Wireless Firewall Router supports all common connection methods.
- ***Auto-detection of Internet Connection Method.*** In most situations, the ADSL Wireless Firewall Router can test your ADSL and Internet connection to determine the connection method used by your ISP.

- ***Fixed or Dynamic IP Address.*** On the Internet (WAN port) connection, the ADSL Wireless Firewall Router supports both Dynamic IP Address (IP Address is allocated on connection) and Fixed IP Address.

Advanced Internet Functions

- ***Application Level Gateways (ALGs).*** Applications which use non-standard connections or port numbers are normally blocked by the Firewall. The ability to define and allow such applications is provided, to enable such applications to be used normally.
- ***Virtual Servers.*** This feature allows Internet users to access Internet servers on your LAN. The required setup is quick and easy.
- ***URL Filter.*** Use the URL Filter to block access to undesirable Web sites by LAN users.
- ***Logs.*** Define what data is recorded in the Logs, and optionally send log data to a Syslog Server. Log data can also be E-mailed to you.
- ***Firewall.*** As well as the built-in firewall to protect your LAN, you can define Firewall Rules to determine which incoming and outgoing traffic should be permitted.
- ***Dynamic DNS Support.*** DDNS, when used with the Virtual Servers feature, allows users to connect to Servers on your LAN using a Domain Name, even if you have a dynamic IP address which changes every time you connect.
- ***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 ADSL Wireless Firewall Router complies with the IEEE802.11g (DSSS) specifications for Wireless LANs.
- ***Supports both 802.11b and 802.11g Wireless Stations.*** The 802.11g standard provides for backward compatibility with the 802.11b standard, so both 802.11b and 802.11g Wireless stations can be used simultaneously.
- ***Speeds to 54Mbps.*** All speeds up to the 802.11g maximum of 54Mbps are supported.
- ***WEP support.*** Support for WEP (Wired Equivalent Privacy) is included. Key sizes of 64 Bit and 128 Bit are supported.
- ***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 ADSL Wireless Firewall Router incorporates a 4-port 10/100BaseT switching hub, making it easy to create or extend your LAN.
- ***DHCP Server Support.*** **D**ynamic **H**ost **C**onfiguration **P**rotocol provides a dynamic IP address to PCs and other devices upon request. The ADSL Wireless Firewall Router can act as a **DHCP Server** for devices on your local LAN and WLAN.

Configuration & Management

- ***Easy Setup.*** Use your WEB browser from anywhere on the LAN or WLAN for configuration.
- ***Configuration File Upload/Download.*** Save (download) the configuration data from the ADSL Wireless Firewall Router to your PC, and restore (upload) a previously-saved configuration file to the ADSL Wireless Firewall Router.
- ***Remote Management.*** The ADSL Wireless Firewall 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.
- ***Network Diagnostics.*** You can use the ADSL Wireless Firewall Router to perform a *Ping* or *DNS lookup*.

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 ADSL Wireless Firewall Router.
- ***Firewall.*** All incoming data packets are monitored and all incoming server requests are filtered, thus protecting your network from malicious attacks from external sources.

Package Contents

The following items should be included:

- The ADSL Wireless Firewall Router Unit
- 1 Cat-5 Ethernet (LAN) cable
- 1 RJ-11 (ADSL) cable
- 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-mounted LEDs

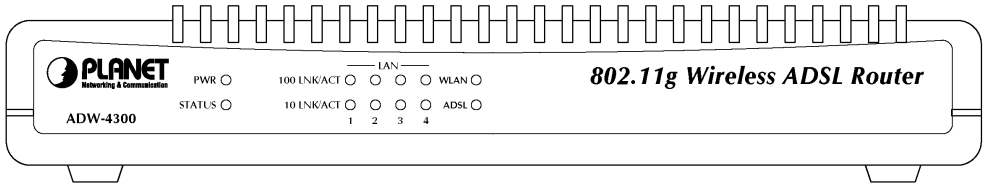


Figure 2: Front Panel

PWR LED

On - Power on.

Off - No power.

STATUS LED

Off - Normal operation.

Blinking - This LED blinks during start up, and during a Firmware Upgrade.

LAN

For each port, there are 2 LEDs, to indicate the connection speed (10Base-T or 100Base-T) of each port.

- **100 LNK/ACT** - This will be ON if the LAN connection is using 100BaseT, and Blinking if data is being transferred via the corresponding LAN port.
- **10 LNK/ACT** - This will be ON if the LAN connection is using 10BaseT, and Blinking if data is being transferred via the corresponding LAN port.
- If neither LED is on, there is no active connection on the corresponding LAN port.

WLAN LED

On – Wireless enabled.

Off - No Wireless connections currently exist.

Flashing - Data is being transmitted or received via the Wireless access point. This includes "network traffic" as well as user data.

ADSL

On - ADSL connection is available.

Off - No ADSL connection.

Flashing - Data is being transmitted or received via the ADSL connection.

Rear Panel

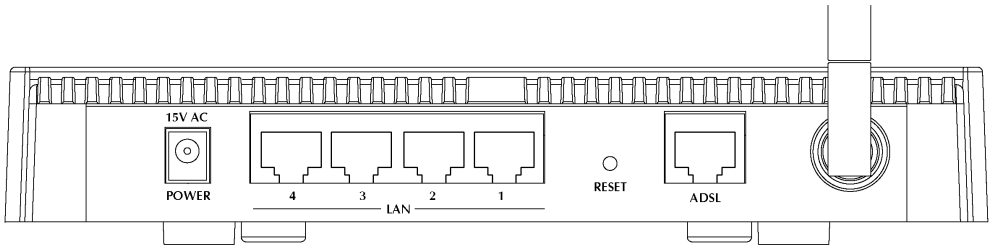


Figure 3: Rear Panel

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

Chapter 2
Installation

2

This Chapter covers the physical installation of the ADSL Wireless Firewall Router.

Requirements

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

Procedure

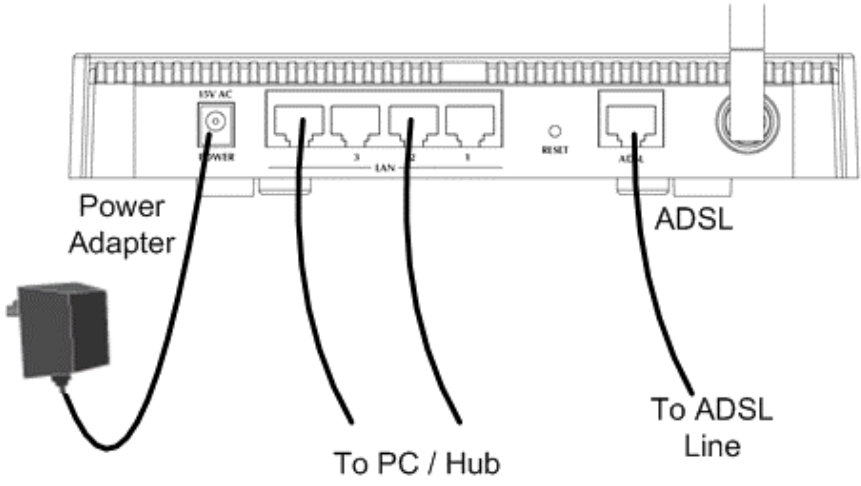


Figure 4: Installation Diagram

1. Choose an Installation Site

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

Note!

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

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

2. Connect LAN Cables

Use standard LAN cables to connect PCs to the Switching Hub ports on the ADSL Wireless Firewall Router. Both 10Base-T and 100Base-TX 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 ADSL Wireless Firewall Router will automatically function as an "Uplink" port when required.

3. Connect ADSL Cable

Connect the supplied ADSL cable from to the WAN port on the ADSL Wireless Firewall Router (the RJ11 connector) to the ADSL terminator provided by your phone company.

4. Power Up

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

5. Check the LEDs

- The *PWR* LED should be ON.
- The *STATUS* LED should flash, then turn Off. If it stays on or blinking after 60 seconds, there is a hardware error.
- For each LAN (PC) connection, one of the LAN LEDs should be ON (provided the PC is also ON.)
- The *WLAN* LED should be ON
- The *ADSL* LED should be ON if ADSL line is connected.

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

Chapter 3
Setup

This Chapter provides Setup details of the ADSL Wireless Firewall Router.

Overview

This chapter describes the setup procedure for:

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

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

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

To Do this:	**Refer to:**
Configure PCs on your LAN.	Chapter 4: PC Configuration
Check ADSL Wireless Firewall Router operation and Status.	Chapter 5: Operation and Status
Use any of the following Advanced features: • Internet • Dynamic DNS • Firewall Rules • Firewall Services • Schedule • Virtual Servers	Chapter 6: Advanced Features
Use any of the following Administration Configuration settings or features: • PC Database • Config File • Logging • E-mail • Diagnostics • Remote Admin • Routing • Upgrade Firmware	Chapter 7 Advanced Administration

Configuration Program

The ADSL Wireless Firewall 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 later
- Netscape 7
- Internet Explorer V5.01 or later

Preparation

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

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

Using your Web Browser

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

1. After installing the ADSL Wireless Firewall 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 ADSL Wireless Firewall Router, as in this example, which uses the ADSL Wireless Firewall Router's default IP Address:

   HTTP://192.168.0.1

4. When prompted for the User name and Password, enter default user name ***admin*** and leave the password field blank (no password).

If you can't connect

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

- The ADSL Wireless Firewall Router is properly installed, LAN connection is OK, and it is powered ON. You can test the connection by using the "Ping" command:
  - Open the MS-DOS window or command prompt window.
  - Enter the command:
    ping 192.168.0.1
    If no response is received, either the connection is not working, or your PC's IP address is not compatible with the ADSL Wireless Firewall Router's IP Address. (See next item.)
- If your PC is using a fixed IP Address, its IP Address must be within the range 192.168.0.2 to 192.168.0.254 to be compatible with the ADSL Wireless Firewall Router's default IP Address of 192.168.0.1. Also, the *Network Mask* must be set to 255.255.255.0. See *Chapter 4 - PC Configuration* for details on checking your PC's TCP/IP settings.
- Ensure that your PC and the ADSL Wireless Firewall 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 ADSL Wireless Firewall Router, the Setup Wizard will run automatically. (The Setup Wizard will also run if the ADSL Wireless Firewall Router's default settings are restored.)

1. Step through the Wizard until finished.
   - You need the data supplied by your ISP. Most connection methods require some data input.
   - The common connection types are explained in the following table.
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 all connections, and the front panel LEDs.
   - Check that you have entered all data correctly.

Common Connection Types

Type	Details	ISP Data required
Dynamic IP Address	Your IP Address is allocated automatically, when you connect to you ISP.	a) ADSL parameters (VPI and VCI) may be required, if they cannot be detected automatically. b) Some ISP's may require you to use a particular *Hostname* or *Domain* name, or MAC (physical) address.
Static (Fixed) IP Address	Your ISP allocates a permanent IP Address to you. Usually, the connection is "Always on".	a) ADSL parameters (VPI and VCI) may be required, if they cannot be detected automatically. b) IP Address allocated to you, and related information, such as Network Mask, Gateway IP address, and DNS address.
PPPoE, PPPoA	You connect to the ISP only when required. The IP address is usually allocated automatically.	a) ADSL parameters (VPI and VCI) may be required, if they cannot be detected automatically. b) User name and password are always required. c) If using a Static (Fixed) IP address, you need the IP address and related information (Network Mask, Gateway IP address, and DNS address)
IPoA (IP over ATM)	Normally, the connection is "Always on".	a) ADSL parameters (VPI and VCI) may be required, if they cannot be detected automatically. b) IP Address allocated to you, and related information, such as Network Mask, Gateway IP address, and DNS address.

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.

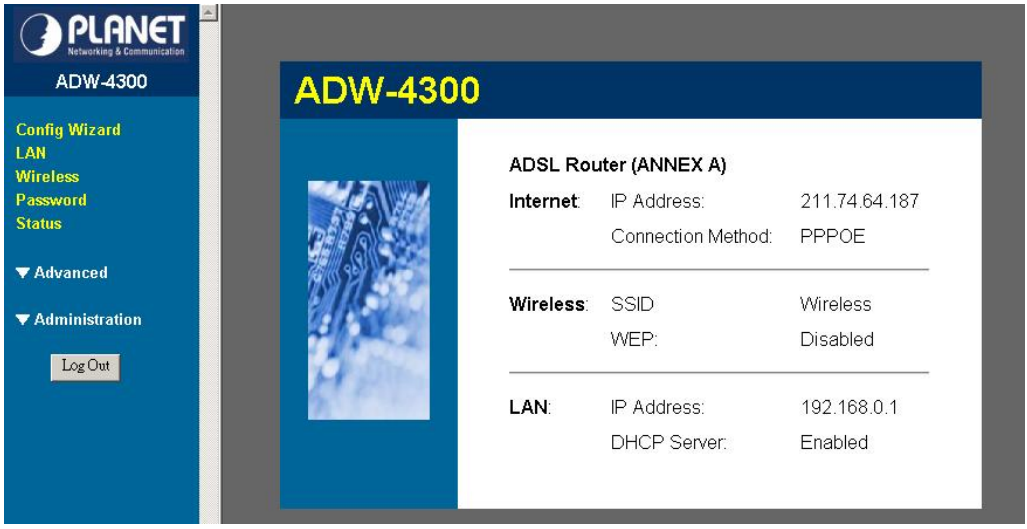


Figure 5: Home Screen

Main Menu

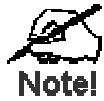
The main menu, on the left, contains links to the most-commonly used screen. To see the links to the other available screens, click "Advanced" or "Administration".

The main menu also contains two (2) buttons:

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

Navigation & Data Input

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



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

LAN Screen

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

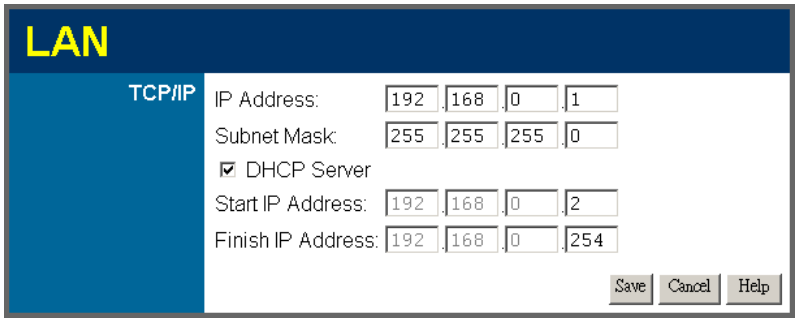


Figure 6: LAN Screen

Data - LAN Screen

TCP/IP	
IP Address	IP address for the ADSL Wireless Firewall 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 ADSL Wireless Firewall Router is attached (the same value as the PCs on that LAN segment).
DHCP Server	• If Enabled, the ADSL Wireless Firewall Router will allocate IP Addresses to PCs (DHCP clients) on your LAN when they start up. The default (and recommended) value is Enabled. • If you are already using a DHCP Server, this setting must be Disabled, and the existing DHCP server must be re-configured to treat the ADSL Wireless Firewall Router as the default Gateway. See the following section for further details. • 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. See the following section for further details on using DHCP.

DHCP

What DHCP Does

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

- The client request is made when the client device starts up (boots).
- The DHCP Server provides the *Gateway* and *DNS* addresses to the client, as well as allocating an IP Address.

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

Using the ADSL Wireless Firewall 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 ADSL Wireless Firewall Router's *DHCP Server* function.
- Set the range of IP Addresses allocated to PCs by the DHCP Server function.

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

Using another DHCP Server

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

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

To Configure your PCs to use DHCP

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

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

Wireless Screen

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

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

To change the ADSL Wireless Firewall 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.

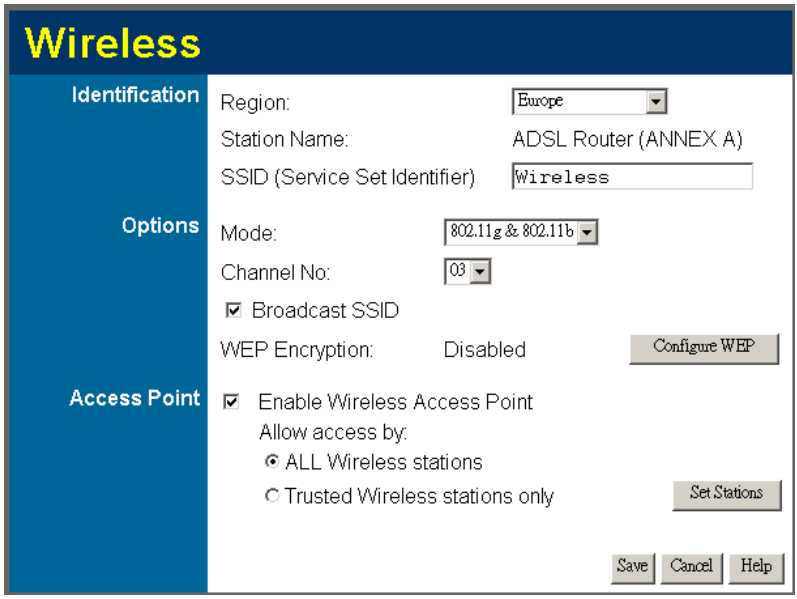


Figure 7: Wireless Screen

Data - Wireless Screen

Identification	
Regulatory Domain	Select the correct domain for your location. It is your responsibility to ensure: • That the ADSL Wireless Firewall Router is only used in domains for which is licensed. • That you select the correct domain, so that only the legal channels for that domain can be selected.
Station name	This is the same as the "Device Name" for the ADSL Wireless Firewall Router.
SSID (ESSID)	• If using an ESS (Extended Service Set, with multiple access points) this ID is called an ESSID (Extended Service Set Identifier). • To communicate, all Wireless stations should use the same SSID/ESSID.

Options	
Mode	Select the desired mode: • **g & b** - Both 802.11.g and 802.11b Wireless stations will be able to use the ADSL Wireless Firewall Router. • **g only** - Only 802.11g Wireless stations can use the ADSL Wireless Firewall Router. • **b only** - Only 802.11b connections are available. 802.11g Wireless Stations will only be able to use the ADSL Wireless Firewall Router if they are fully backward-compatible with the 802.11b standard.
Channel No.	• Select the Channel you wish to use on your Wireless LAN. • If you experience interference (shown by lost connections and/or slow data transfers) you may need to experiment with different channels to see which is the best. • If using multiple Access Points, adjacent Access Points should use different Channels to reduce interference.
Broadcast SSID	If enabled, the ADSL Wireless Firewall Router will broadcast its SSID. This allows Wireless Stations will a "null" (blank) SSID to detect and use the correct SSID. Disable this feature if you do not want Wireless stations to be able to do this.
WEP data encryption	• WEP (Wired Equivalent Privacy) status will display "Disabled" if WEP is not being used, otherwise it will display "64 Bit" or "128 Bit" depending on the WEP key size being used. If WEP is used, data is Encrypted before being transmitted, making communication more secure. • Click the "Configure WEP" button to access the WEP sub-screen, and view or change the WEP settings.
Configure WEP Button	Click this button to view the WEP sub-screen. See the following section for more details.
Access Point	
Enable Wireless Access Point	Enable this if you want to use Wireless Access Point function. If disabled, no Wireless stations can use the Access Point function, and all connections must be make via the wired LAN.
Allow access by …	Use this feature to determine which Wireless stations can use the Access Point. The options are: • **All Wireless Stations** - All wireless stations can use the access point, provided they have the correct SSID and WEP settings. • **Trusted Wireless stations only** - Only wireless stations you designate as "Trusted" can use the access point, even if they have the correct SSID and WEP settings. This feature uses the MAC address to identify Wireless stations. The MAC address is a low-level network identifier which is unique to each PC or network device. To define the trusted wireless stations, use the "Set Stations" button.

Set Stations Button	Click this button to manage the trusted PC database.

WEP Screen

This screen is accessed by clicking the "Configure WEP" button on the *Wireless* screen.

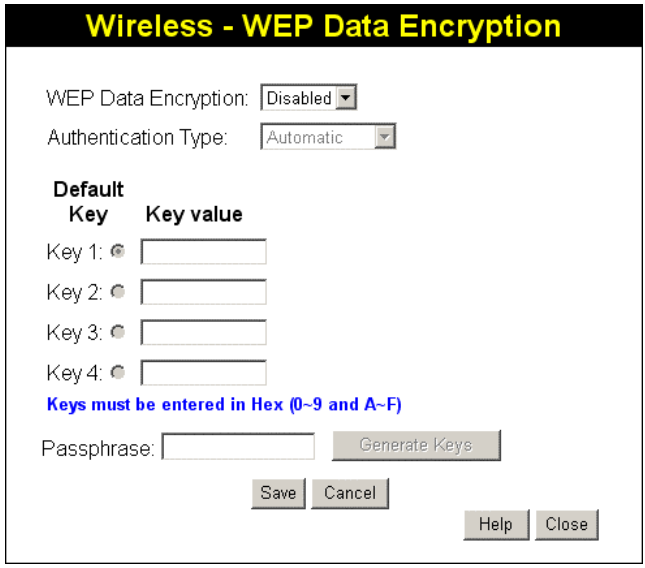


Figure 8: WEP Screen

Data - WEP Screen

WEP Data Encryption	
WEP Data Encryption	Select the option to match other Wireless Stations: • **Disabled** - data is NOT encrypted before being transmitted. • **64 Bit** - data is encrypted, using the default key, before being transmitted. You must enter at least the default key. For 64 Bit Encryption, the key size is 10 chars in HEX (0~9 and A~F). • **128 Bit** - data is encrypted, using the default key, before being transmitted. You must enter at least the default key. For 128 Bit Encryption, the key size is 26 chars in HEX (0~9 and A~F).
Authentication Type	Normally, this should be left at the default value of "Automatic". If changed to "Open System" or "Shared Key", ensure that your Wireless Stations use the same setting.
Default Key	Select the key you wish to be the default. Transmitted data is ALWAYS encrypted using the Default Key; the other Keys are for decryption only. You must enter a **Key Value** for the **Default Key**.
Key Value	Enter the key value or values you wish to use. The **Default Key** is required, the other keys are optional. Other stations must have the same key.
Passphrase	If desired, you can generate a key from a phrase, instead of entering the key value directly. Enter the desired phrase, and click the "Generate Keys" button.

Password Screen

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

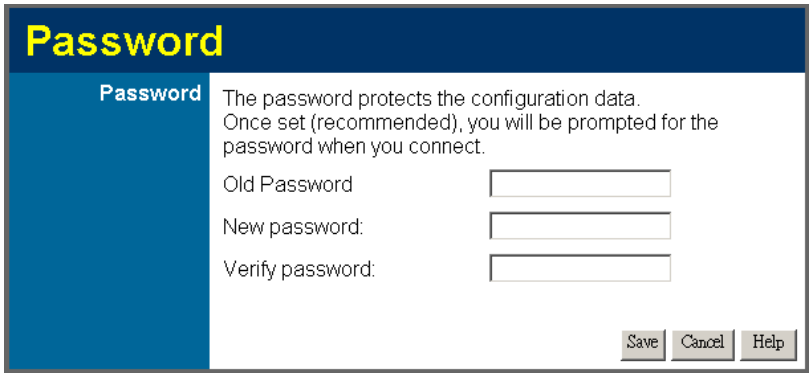


Figure 9: Password Screen

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

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

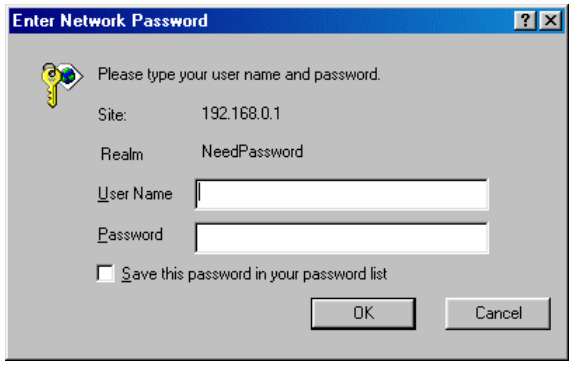


Figure 10: Password Dialog

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

Chapter 4
PC Configuration

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

Overview

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

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

Windows Clients

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

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

The ADSL Wireless Firewall 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 ADSL Wireless Firewall Router settings, and the default Windows TCP/IP settings, no changes need to be made.

- By default, the ADSL Wireless Firewall 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 ADSL Wireless Firewall Router
- The *DNS* should be set to the address provided by your ISP.

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

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

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

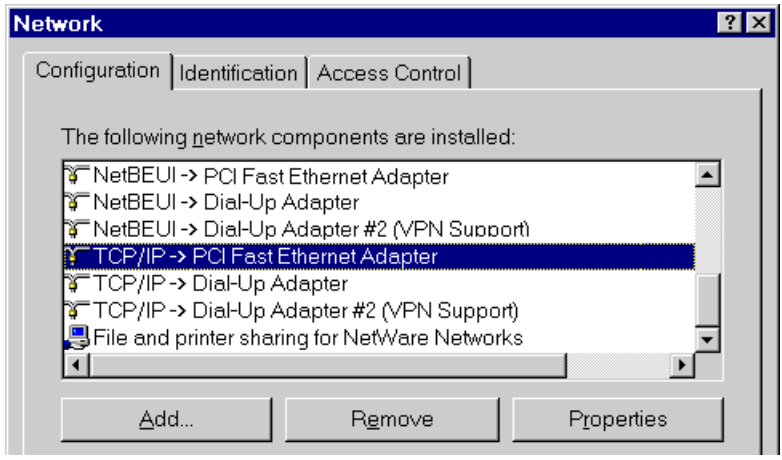


Figure 11: Network Configuration

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

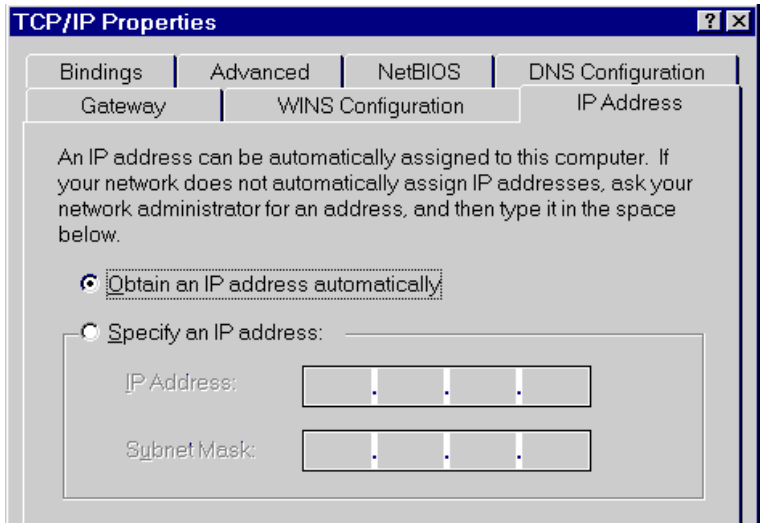


Figure 12: IP Address (Win 95)

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 ADSL Wireless Firewall Router will act as a DHCP Server.

Restart your PC to ensure it obtains an IP Address from the ADSL Wireless Firewall 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 ADSL Wireless Firewall Router's IP address in the *New Gateway* field and click *Add*, as shown below. Your LAN administrator can advise you of the IP Address they assigned to the ADSL Wireless Firewall Router.

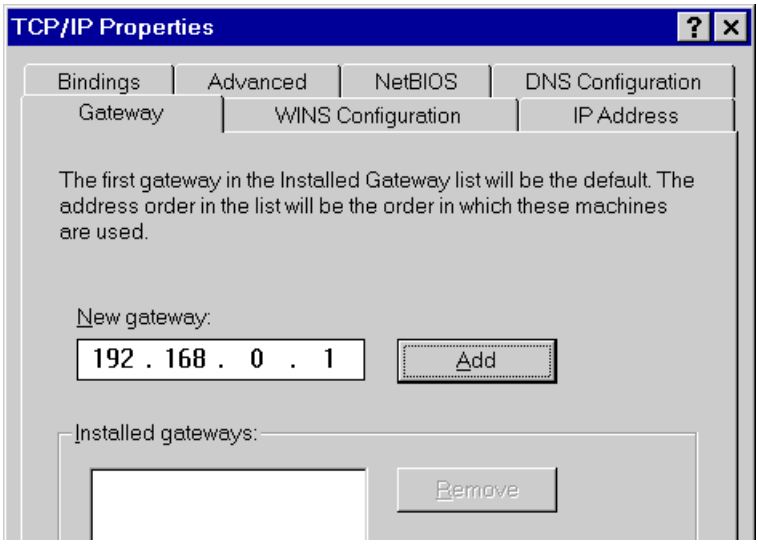


Figure 13: Gateway Tab (Win 95/98)

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

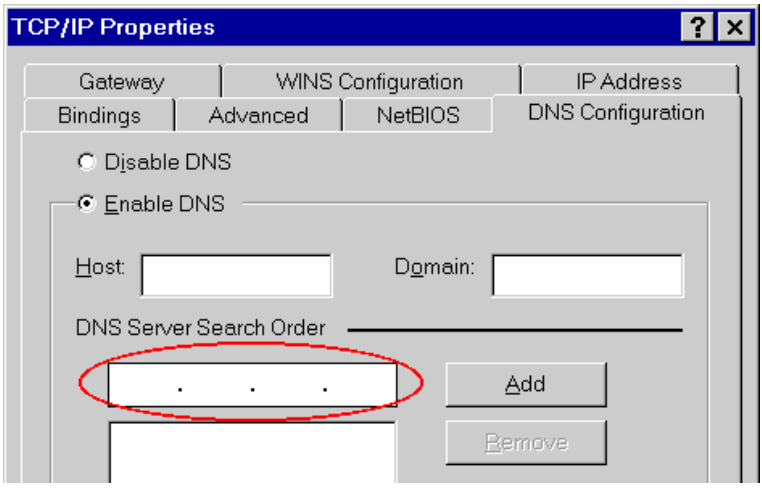


Figure 14: DNS Tab (Win 95/98)

Checking TCP/IP Settings - Windows NT4.0

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

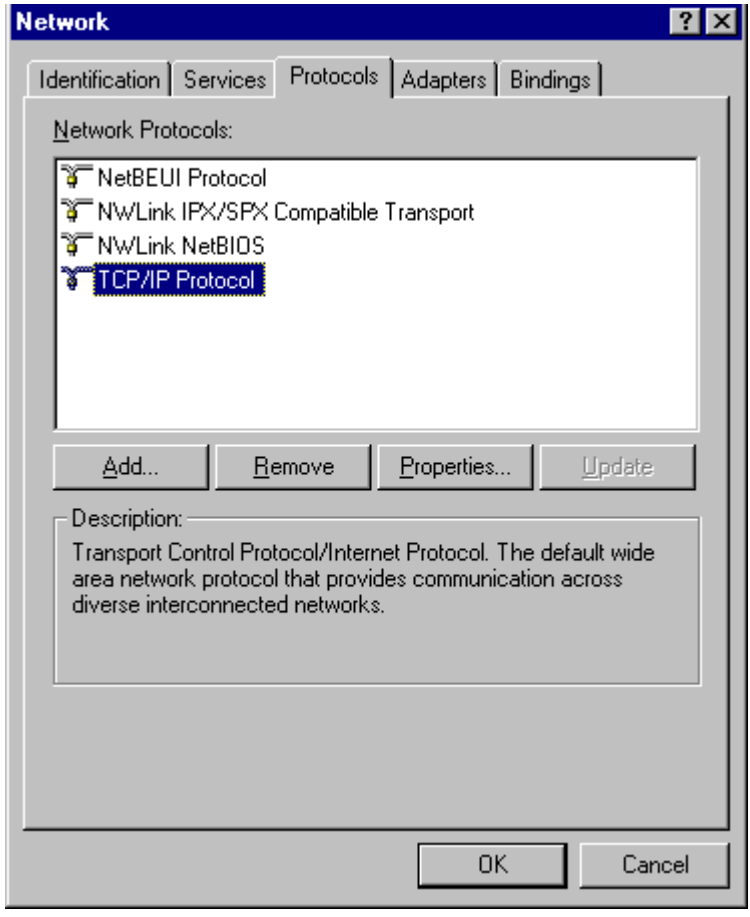


Figure 15: Windows NT4.0 - TCP/IP

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

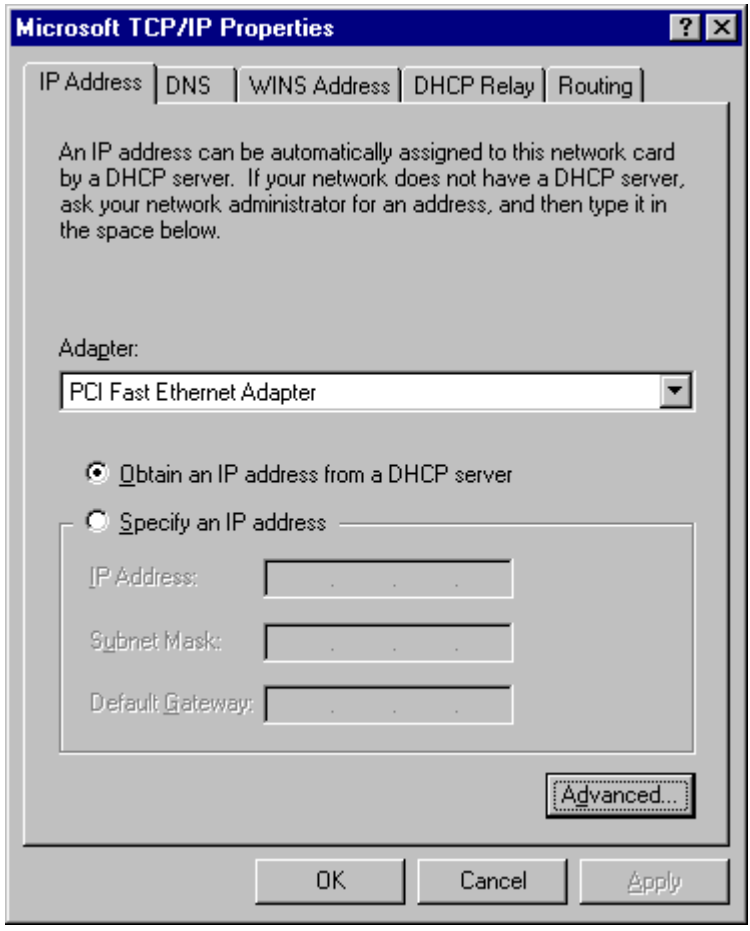


Figure 16: Windows NT4.0 - IP Address

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

Obtain an IP address from a DHCP Server

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

Restart your PC to ensure it obtains an IP Address from the ADSL Wireless Firewall 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 ADSL Wireless Firewall 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 ADSL Wireless Firewall Router's IP address, as shown in Figure 17 below.
   - If necessary, use the *Up* button to make the ADSL Wireless Firewall Router the first entry in the *Gateways* list.

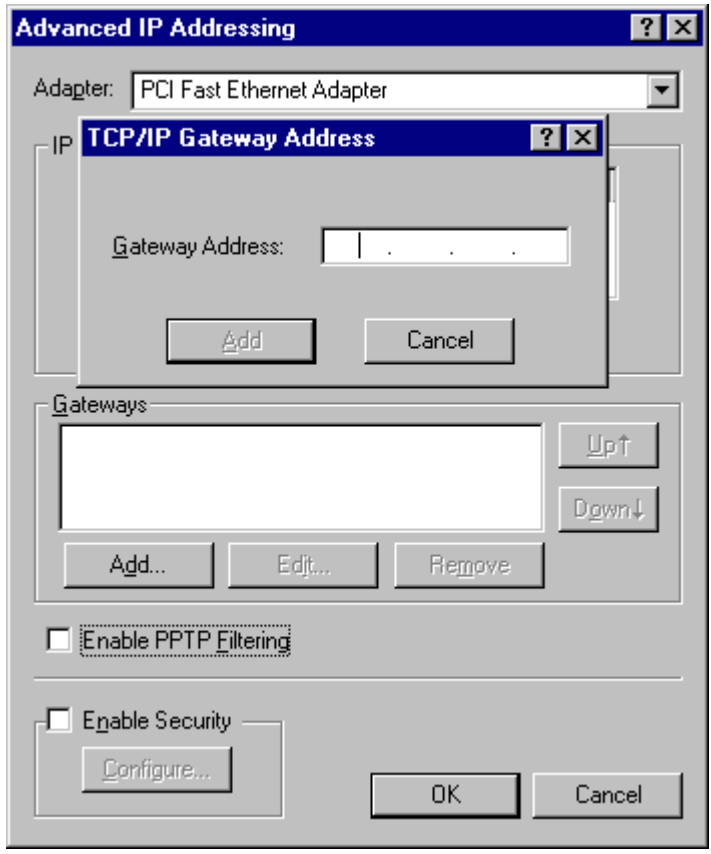


Figure 17 - Windows NT4.0 - Add Gateway

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

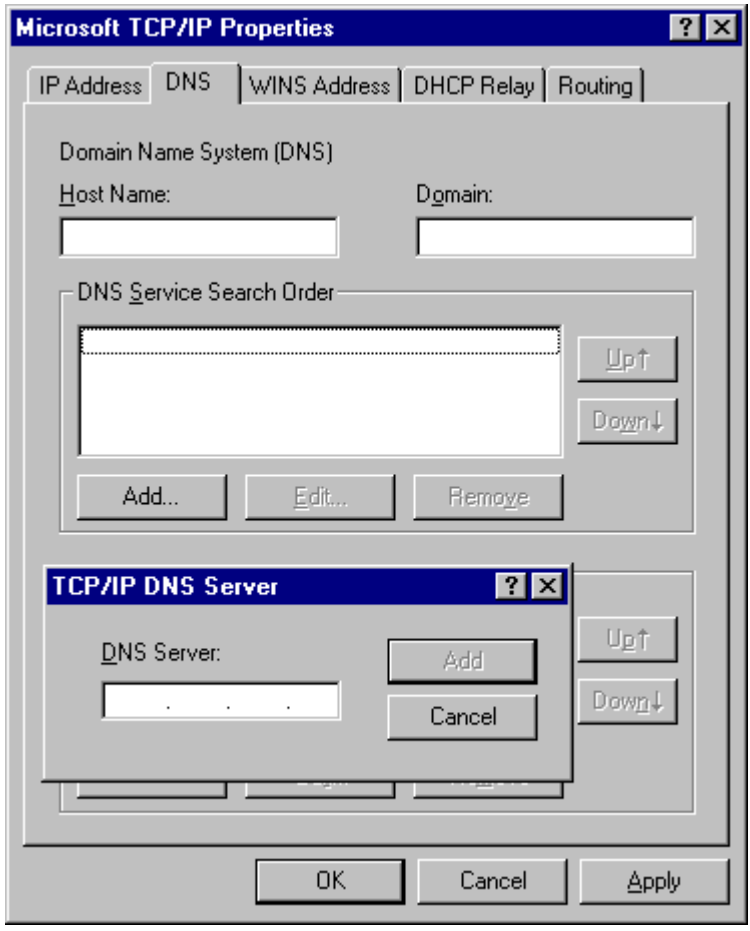


Figure 18: Windows NT4.0 - DNS

Checking TCP/IP Settings - Windows 2000:

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

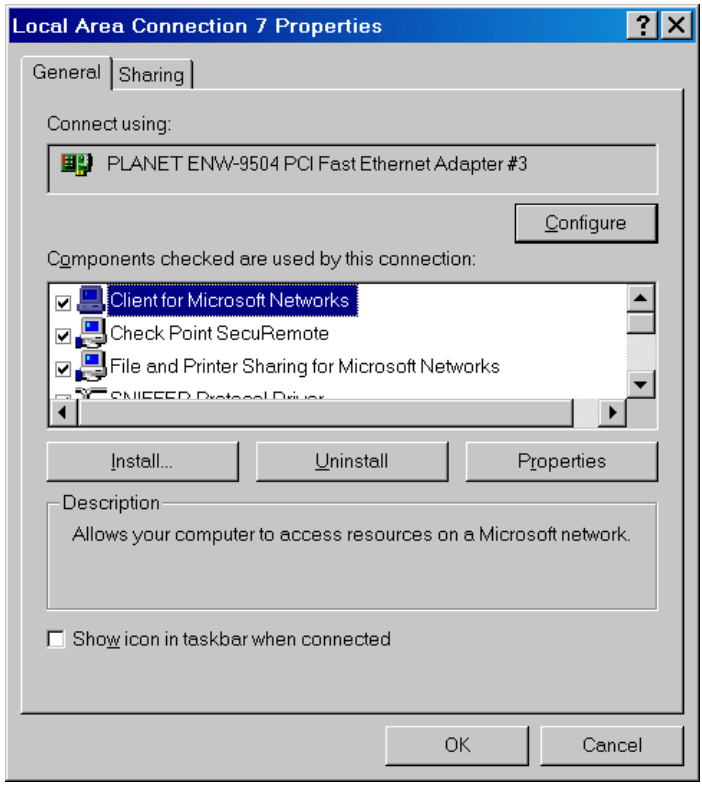


Figure 19: Network Configuration (Win 2000)

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.

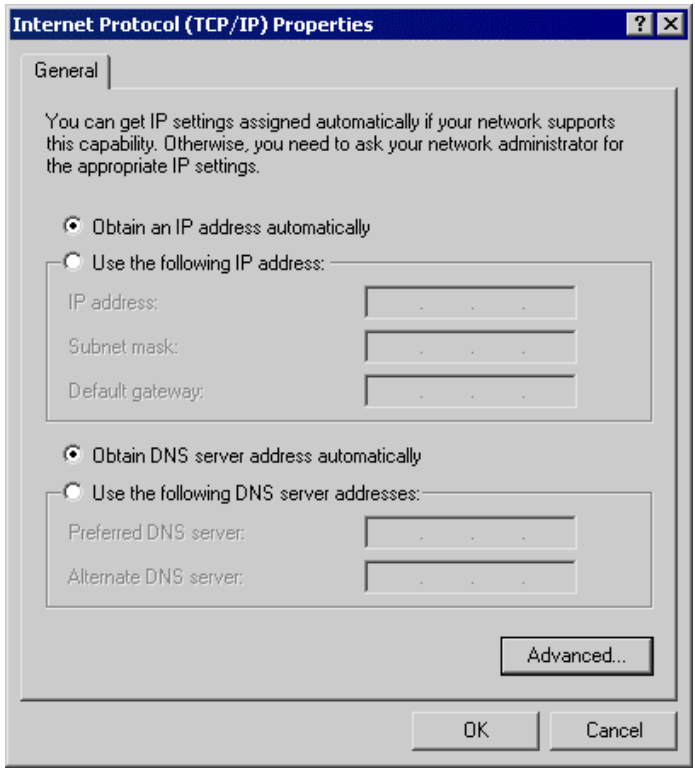


Figure 20: TCP/IP Properties (Win 2000)

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 ADSL Wireless Firewall Router will act as a DHCP Server.

Restart your PC to ensure it obtains an IP Address from the ADSL Wireless Firewall 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 ADSL Wireless Firewall 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 ADSL Wireless Firewall Router.)
- If the *DNS Server* fields are empty, select *Use the following DNS server addresses*, and enter the DNS address or addresses provided by your ISP, then click *OK*.

Checking TCP/IP Settings - Windows XP

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

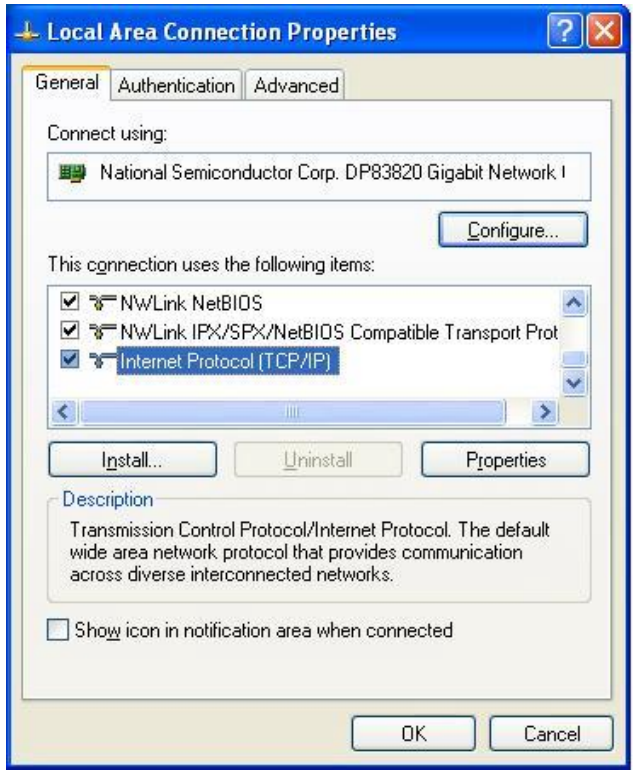


Figure 21: Network Configuration (Windows XP)

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

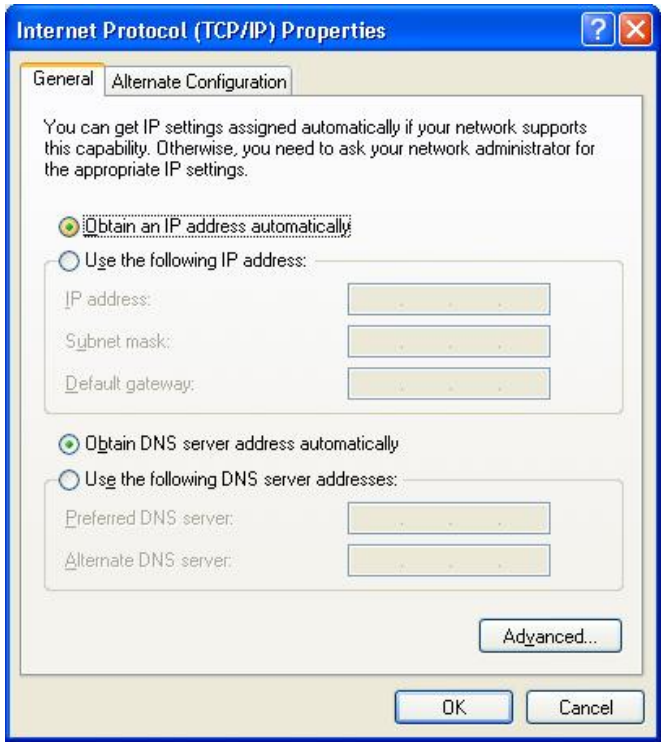


Figure 22: TCP/IP Properties (Windows XP)

5. Ensure your TCP/IP settings are correct.

Using DHCP

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

Restart your PC to ensure it obtains an IP Address from the ADSL Wireless Firewall 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 ADSL Wireless Firewall Router's IP address and click *OK*. Your LAN administrator can advise you of the IP Address they assigned to the ADSL Wireless Firewall 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 ADSL Wireless Firewall Router for Internet access:

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

For Windows 9x/ME/2000

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

For Windows XP

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

Accessing AOL

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

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

Macintosh Clients

From your Macintosh, you can access the Internet via the ADSL Wireless Firewall 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 ADSL Wireless Firewall Router's IP Address.
- Ensure your DNS settings are correct.

Linux Clients

To access the Internet via the ADSL Wireless Firewall Router, it is only necessary to set the ADSL Wireless Firewall 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 ADSL Wireless Firewall Router.
- Ensure your DNS (Name server) settings are correct.

To act as a DHCP Client (recommended)

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

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

Other Unix Systems

To access the Internet via the ADSL Wireless Firewall Router:

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

Wireless Station Configuration

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

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

Mode	The mode must be set to ***Infrastructure*** (rather than Ad-hoc) Access points only operate in ***Infrastructure*** mode.
SSID (ESSID)	This must match the value used on the ADSL Wireless Firewall Router. The default value is **wireless**. **Note! The SSID is case sensitive.**
WEP	By default, WEP on the ADSL Wireless Firewall Router is **disabled**. • If WEP remains disabled on the ADSL Wireless Firewall Router, all stations must have WEP disabled. • If WEP is enabled on the ADSL Wireless Firewall Router, each station must use the same settings as the ADSL Wireless Firewall Router.

Chapter 5
Operation and Status

This Chapter details the operation of the ADSL Wireless Firewall Router and the status screens.

Operation

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

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

Status Screen

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

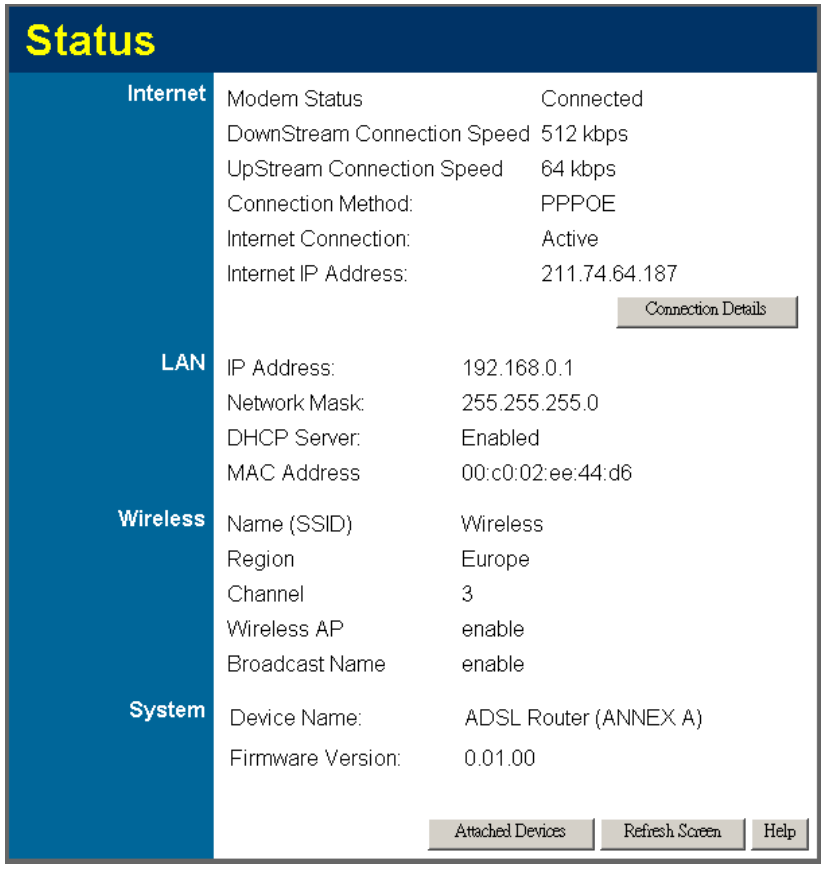


Figure 23: Status Screen

Data - Status Screen

Internet	
Modem Status	This indicates the status of the ADSL modem component.
DownStream Connection Speed	If connected, displays the speed for the DownStream (download) ADSL Connection.
UpStream Connection Speed	If connected, displays the speed for the UpStream (upload) ADSL Connection.
Connection Method	This indicates the current connection method, as set in the *Setup Wizard*.
Internet Connection	This indicates the current status of the Internet Connection • **Active** - Connection exists • **Idle** - No current connection, but no error has been detected. This condition normally arises when an idle connection is automatically terminated. • **Failed** - The connection was terminated abnormally. This could be caused by Modem failure, or the loss of the connection to the ISP's server. If there is an error, you can click the "Connection Details" button to find out more information.
Internet IP Address	This IP Address is allocated by the ISP (Internet Service Provider). If using a dynamic IP address, and no connection currently exists, this information is unavailable.
Connection Details	Click this button to open a sub-window and view a detailed description of the current connection. Depending on the type of connection, a "log" may also be available.
LAN	
IP Address	The IP Address of the ADSL Wireless Firewall Router.
Network Mask	The Network Mask (Subnet Mask) for the IP Address above.
DHCP Server	This shows the status of the DHCP Server function. The value will be "Enabled" or "Disabled".
MAC Address	This shows the MAC Address for the ADSL Wireless Firewall Router, as seen on the LAN interface.
Wireless	
Name (SSID)	If using an ESS (Extended Service Set, with multiple access points) this ID is called an ESSID (Extended Service Set Identifier).
Region	The current region, as set on the Wireless screen.
Channel	This shows the Channel currently used, as set on the Wireless screen.
Wireless AP	This indicates whether or not the Wireless Access Point feature is enabled.
Broadcast Name	This indicates whether or not the SSID is Broadcast. This setting is on the Wireless screen.

System	
Device Name	The current name of the ADSL Wireless Firewall Router. This is also the "hostname" provided to ISPs who request this information.
Firmware Version	The version of the current firmware installed.
Buttons	
Connection Details	Click this button to open a sub-window and view a detailed description of the current connection.
Attached Devices	This will open a sub-window, showing all LAN and Wireless devices currently on the network.
Refresh Screen	Update the data displayed on screen.

Connection Status - PPPoE & PPPoA

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

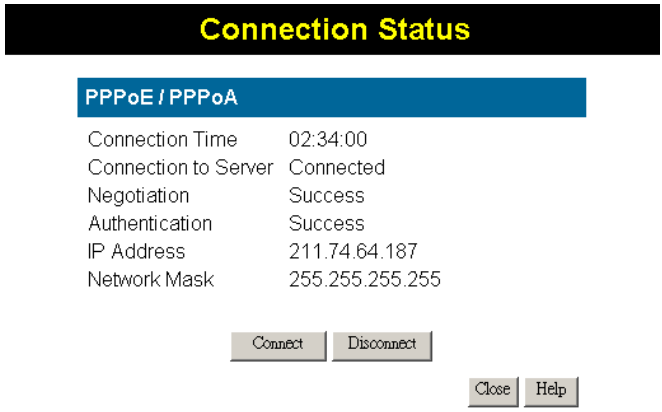


Figure 24: PPPoE Status Screen

Data – PPPoE/PPPoA Screen

Connection Time	This indicates how long the current connection has been established.
PPPoE Link Status	This indicates whether or not the connection is currently established. • If the connection does not exist, the "Connect" button can be used to establish a connection. • If the connection currently exists, the "Disconnect" button can be used to break the connection.
Negotiation	This indicates the status of the PPPoE Server login.
IP Address	The IP Address of this device, as seen by Internet users. This address is allocated by your ISP (Internet Service Provider).
Network Mask	The Network Mask associated with the IP Address above.

Buttons	
Connect	If not connected, establish a connection to your ISP.
Disconnect	If connected to your ISP, hang up the connection.
Close	Close this window.

Connection Details - Dynamic IP Address

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

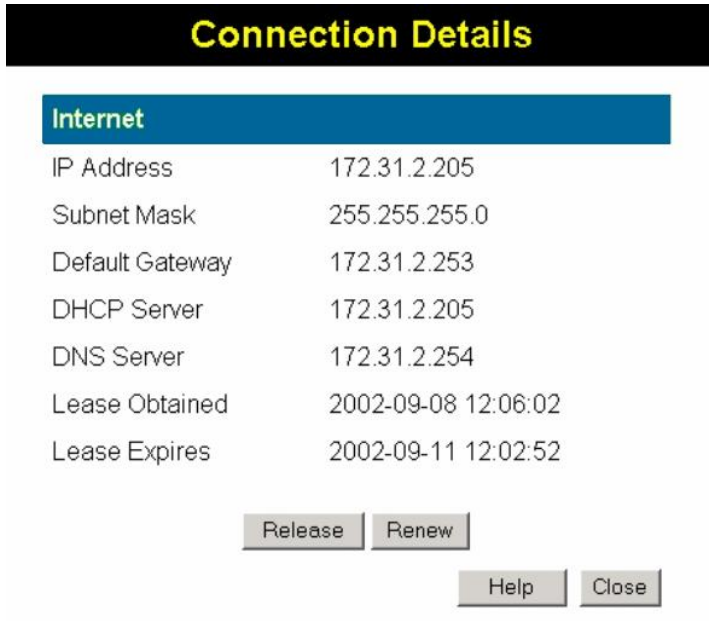


Figure 25: Connection Details - Fixed/Dynamic IP Address

Data - Dynamic IP address

Internet	
IP Address	The current IP Address of this device, as seen by Internet users. This address is allocated by your ISP (Internet Service Provider).
Network Mask	The Network Mask associated with the IP Address above.
Default Gateway	The IP address of the remote Gateway or Router associated with the IP Address above.
DHCP Server	The IP address of your ISP's DHCP Server.
DNS Server	The IP address of the Domain Name Server which is currently used.
Lease Obtained **Lease Expires**	This indicates when the current IP address was obtained, and how long before this IP address allocation (the DCHP lease) expires.

Buttons	
Release	If an IP Address has been allocated to the ADSL Wireless Firewall Router (by the ISP's DHCP Server, clicking the "Release" button will break the connection and release the IP Address.
Renew	If the ISP's DHCP Server has NOT allocated an IP Address for the ADSL Wireless Firewall Router, clicking the "Renew" button will attempt to re-establish the connection and obtain an IP Address from the ISP's DHCP Server.
Close	Close this window.

Connection Details - Fixed IP Address

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

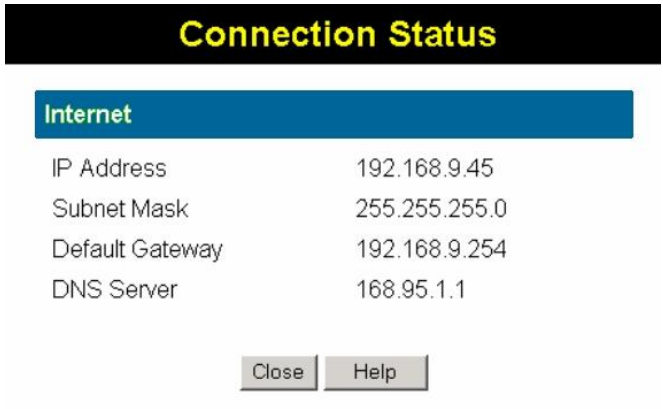


Figure 26: Connection Details - Fixed/Dynamic IP Address

Data - Fixed IP address Screen

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

Chapter 6
Advanced Features

6

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

Overview

The following advanced features are provided:

- Internet:
  - DMZ
  - URL filter
- Dynamic DNS
- Firewall Rules
- Firewall Services
- Schedule
- Virtual Servers

Internet

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

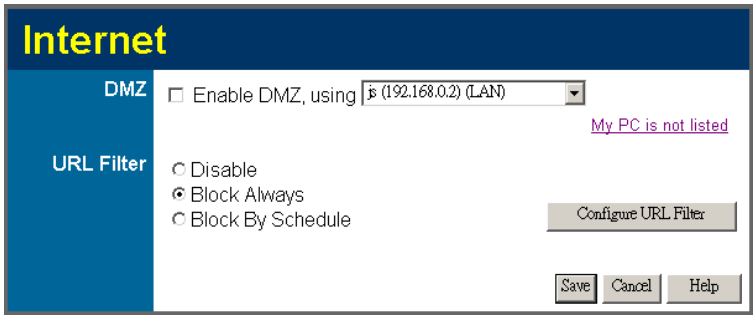


Figure 27: Advanced Internet Screen

DMZ

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

- This allows almost any application to be used on the "DMZ PC".
- The "DMZ PC" will receive all "Unknown" connections and data.
- If the DMZ feature is enabled, you must select the PC to be used as the "DMZ PC".

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

URL Filter

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

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

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

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

URL Filter Screen

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

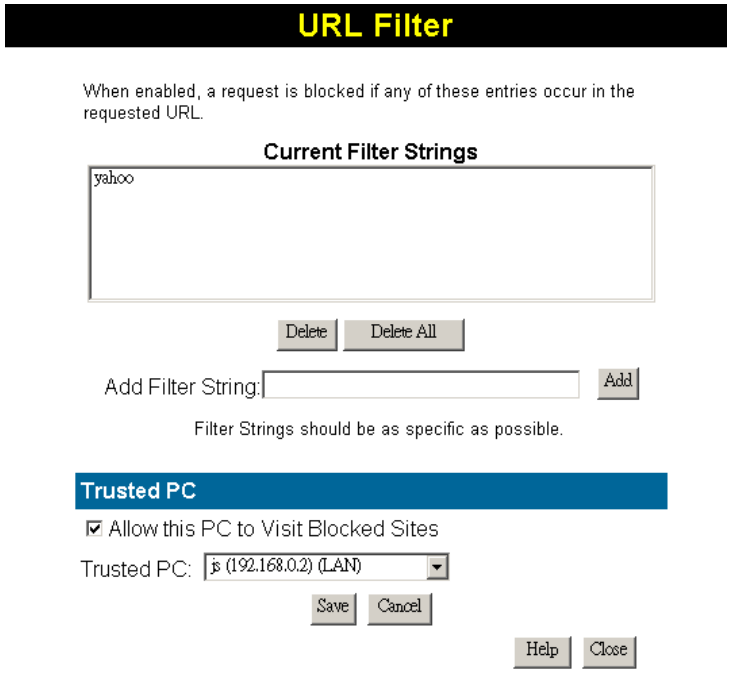


Figure 28: URL Filter Screen

Data - URL Filter Screen

Current Filter Strings	
Current Filter Strings	The list contains the current list of items to block. • To add to the list, use the "Add" option below. • To delete an entry, select it and click **Delete** button. • To delete all entries, click the **Delete All** button.
Add Filter String	To add to the current list, type the word or domain name you want to block into the field provided, then click the **Add** button. Filter strings should be as specific as possible. Otherwise, you may block access to many more sites than intended.

Trusted PC	
Allow Trusted PC	Enable this to allow one computer to have unrestricted access to the Internet. For this PC, the URL filter will be ignored. If enabled, you must select the PC to be the trusted PC.
Trusted PC	Select the PC to be the Trusted PC.

Dynamic DNS (Domain Name Server)

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

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

The DynDNS 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) to request your desired Domain name.
3. Enter your data from www.dyndns.org in the ADSL Wireless Firewall Router's DDNS screen.
4. The ADSL Wireless Firewall 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:

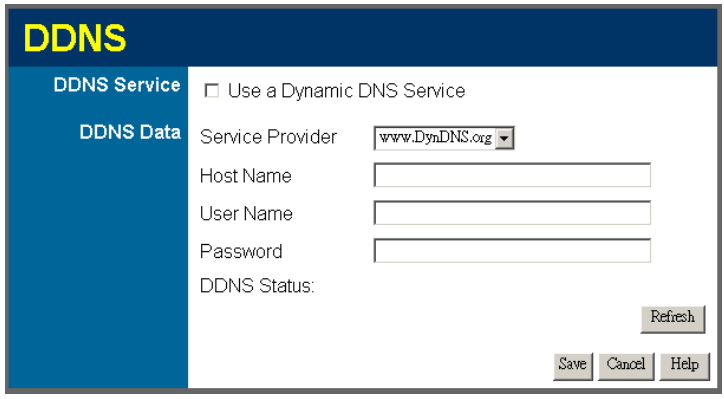


Figure 29: DDNS Screen

Data - Dynamic DNS Screen

DDNS Service	
Use a Dynamic DNS Service	Use this to enable or disable the DDNS feature as required.
DDNS Data	
Service Provider	Select the desired DDNS Service provider.
Host Name	Enter the domain name allocated to you by the DDNS Service. If you have more than one name, enter the name you wish to use.
User Name	Enter your Username for the DDNS Service.
Password	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	• This message is returned by the DDNS Server • Normally, this message should be "Update successful" • If the message is "No host", this indicates the host name entered was not allocated to you. You need to connect to DDNS Service provider and correct this problem.

Firewall Rules

The ***Firewall Rules*** screen allows you to define "Firewall Rules" which can allow or prevent certain traffic.

By default:

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

"Traffic" means incoming connection attempts, not packets.

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

Firewall Rules Screen

An example screen is shown below.

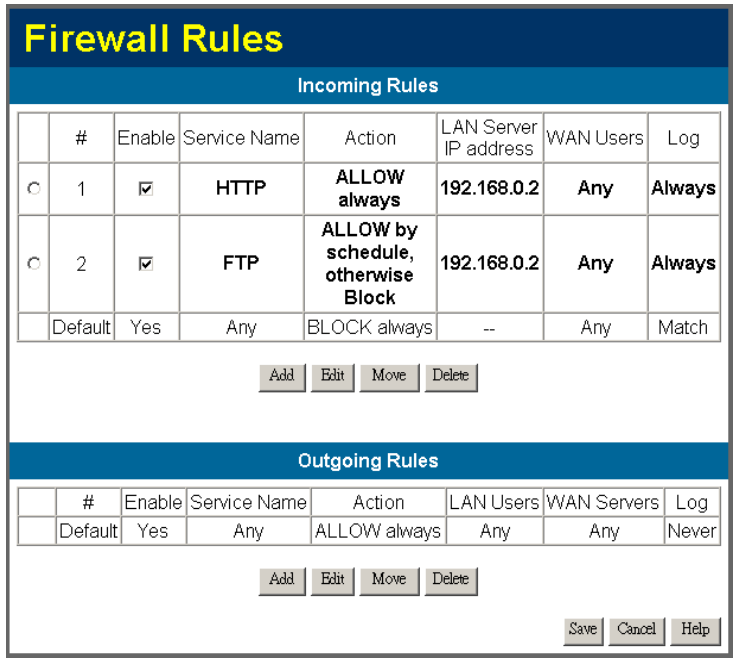


Figure 30 Firewall Screen

Data – Firewall Rules

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

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

Incoming Rules

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

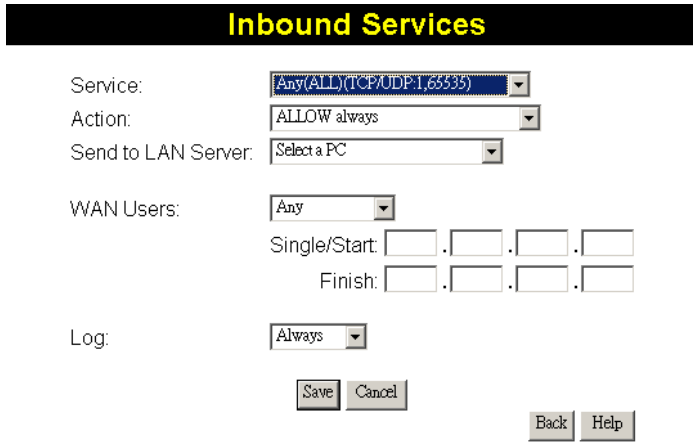


Figure 31: Inbound Services Screen

Data – Incoming Rules Screen

Inbound Services	
Service	Select the desired Service. This determines which packets are covered by this rule. If necessary, you can define a new Service on the "Services" screen, by defining the protocols and port numbers used by the Service.
Action	Select the desired action for packets covered by this rule: • ALLOW always • ALLOW by schedule, otherwise Block • BLOCK always • BLOCK by schedule, otherwise Allow **Note:** • Any inbound traffic which is not allowed by rules you create will be blocked by the Default rule. • BLOCK rules are only useful if the traffic is already covered by an ALLOW rule. (That is, you wish to block a sub-set of traffic which is currently allowed by another rule.) • To define the Schedule used in these selections, use the "Schedule" screen.
Send to LAN Server	Select the PC or Server on your LAN which will receive the in-bound traffic covered by this rule.
WAN Users	These settings determine which packets are covered by the rule, based on their source (WAN) IP address. Select the desired option: • **Any** - All IP addresses are covered by this rule. • **Address range** - If this option is selected, you must enter the desired values in the "Single/Start" and "Finish" fields to determine the address range. • **Single address** - Enter the required address in the "Sin-

	gle/Start" fields.
Log	This determines whether packets covered by this rule are logged. Select the desired action. • **Always** - always log traffic considered by this rule, whether it matches or not. (This is useful when debugging your rules.) • **Never** - never log traffic considered by this rule, whether it matches or not. • **Match** - Log traffic only it matches this rule. (The action is determined by this rule.) • **Not Match** - Log traffic which is considered by this rule, but does not match (The action is NOT determined by this rule.)

Outgoing Rules

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

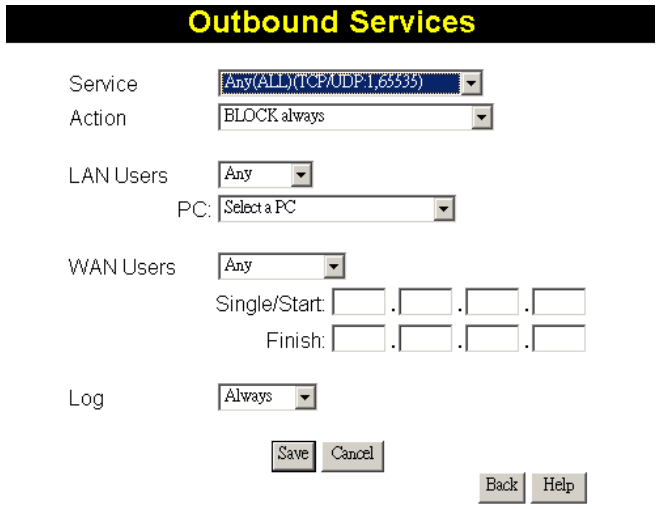


Figure 32: Outbound Services Screen

Data - Outbound Rules Screen

Outbound Services	
Service	Select the desired Service or application to be covered by this rule. If the desired service or application does not appear in the list, you must define it using the "Services" menu option
Action	Select the desired action for packets covered by this rule: • BLOCK always • BLOCK by schedule, otherwise Allow • ALLOW always • ALLOW by schedule, otherwise Block **Note:** • Any outbound traffic which is not blocked by rules you create will be allowed by the Default rule. • ALLOW rules are only useful if the traffic is already covered by a BLOCK rule. (That is, you wish to allow a subset of traffic

	which is currently blocked by another rule.) • To define the Schedule used in these selections, use the "Schedule" screen.
LAN Users	Select the desired option to determine which PCs are covered by this rule: • **Any** - All PCs are covered by this rule. • **Single PC** - Only the selected PC is covered by this rule. If selected, you must select the PC. **PC** - If using Single PC above, select the PC or Server on your LAN which will be covered by this rule.
WAN Users	These settings determine which packets are covered by the rule, based on their source (WAN) IP address. Select the desired option: • **Any** - All IP addresses are covered by this rule. • **Address range** - If this option is selected, you must enter the "Start" and "Finish" fields. • **Single address** - Enter the required address in the "Single/Start" fields.
Log	This determines whether packets covered by this rule are logged. Select the desired action. • **Always** - always log traffic considered by this rule, whether it matches or not. (This is useful when debugging your rules.) • **Never** - never log traffic considered by this rule, whether it matches or not. • **Match** - Log traffic only it matches this rule. (The action is determined by this rule.) • **Not Match** - Log traffic which is considered by this rule, but does not match (The action is NOT determined by this rule.)

Firewall Services

This screen is used to modify the list of *Services* which are available when creating Firewall Rules.

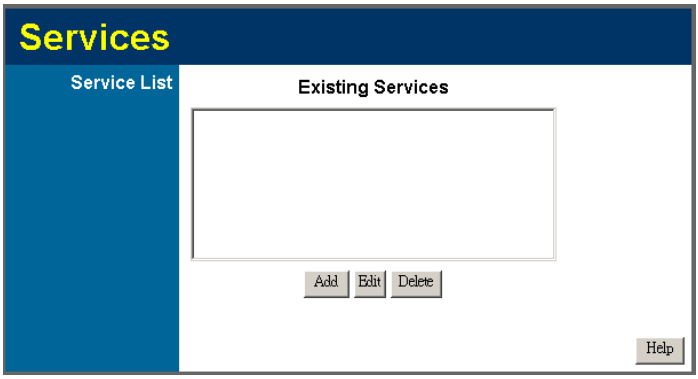


Figure 33: Add Services Screen

Data – Add Services

Services	
Services List	This lists all defined Services.
Add	Use this to open a sub-screen where you can add a new service.
Edit	To modify a service, select it, and then click this button.
Delete	Pre-defined Services can not be deleted, but you can use this button to delete any services you have defined.

Add/Edit Service

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

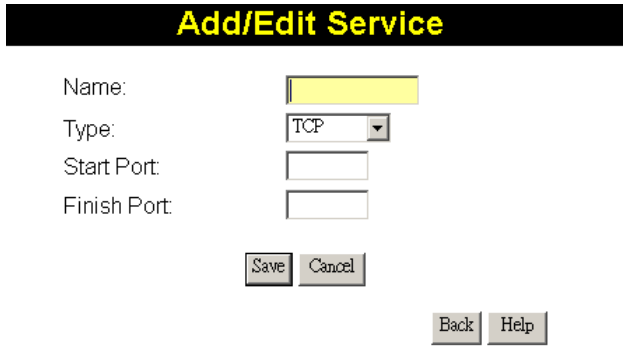


Figure 34 : Add/Edit Service

Data – Add/Edit Service

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

Options

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

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

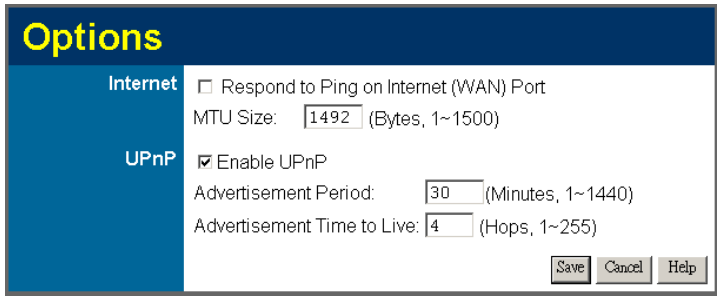


Figure 35: Options Screen

Data - Options Screen

Internet	
Respond to Ping	• If checked, the Wireless Router will repond to Ping (ICMP) packets received from the Internet. • If not checked, Ping (ICMP) packets from the Internet will be ignored. Disabling this option provides a slight increase in security.
MTU Size	Enter a value between 1 and 1500. **Note:** MTU (Maximum Transmission Unit) size should only be changed if advised to do so by Technical Support.
UPnP	
UPnP	• UPnP (Universal Plug and Play) allows automatic discovery and configuration of equipment attached to your LAN. UPnP is by supported Windows ME, XP, or later. • If Enabled, this device will be visible via UPnP. • If Disabled, this device will not be visible via UPnP.
Advertisement Period	Enter the desired value, in minutes. The valid range is from 1 to 1440.
Advertisement Time to Live	Enter the desired value, in hops. The valid range is from 1 to 255.

Schedule

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

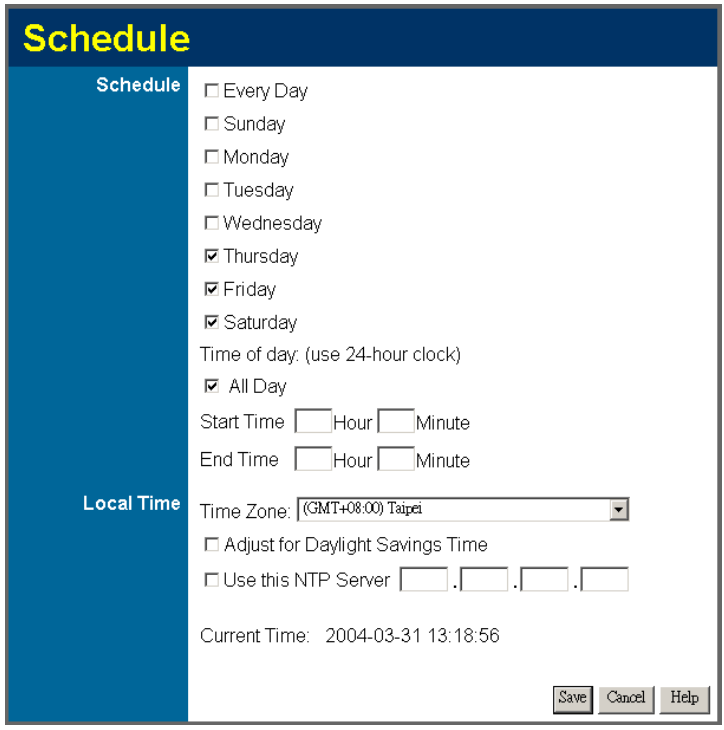


Figure 36: Schedule Screen

Data - Schedule Screen

Schedule	
Sunday, Monday…	Use these checkboxes to select the desired days.
Start Time	Enter the start using a 24 hr clock.
Finish Time	Enter the finish time using a 24 hr clock.
Local Time	
Time Zone	In order to display your local time correctly, you must select your "Time Zone" from the list.
Adjust for Daylight Savings Time	If your region uses Daylight Savings Time, you must manually check "Adjust for Daylight Savings Time" at the beginning of the adjustment period, and uncheck it at the end of the Daylight Savings period.
Use this NTP Server	If you prefer to use a particular NTP server as the primary server, check the checkbox "Use this NTP Server" and enter the Server's IP address in the fields provided.. If this setting is not enabled, the default NTP Servers are used.
Current Time	This displays the current time on the ADSL Wireless Firewall Router.

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.

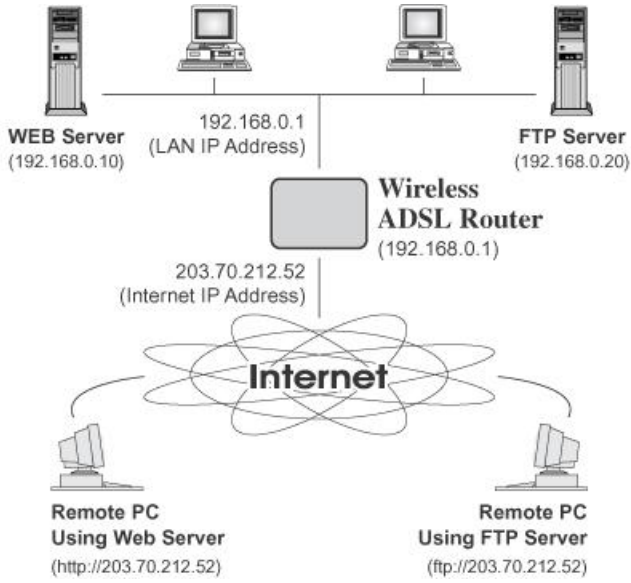


Figure 37: Virtual Servers

IP Address seen by Internet Users

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

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

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

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

Virtual Servers Screen

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

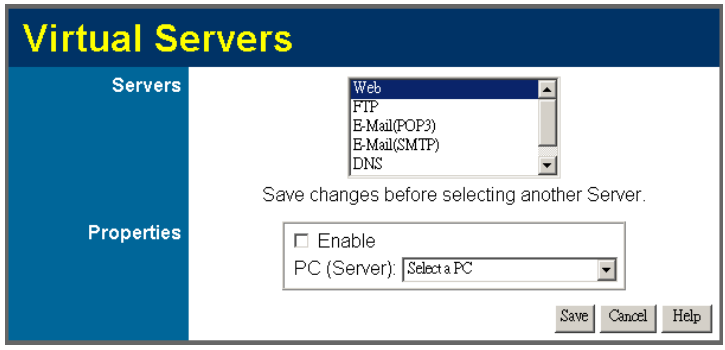


Figure 38: Virtual Servers Screen

Data - Virtual Servers Screen

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

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

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

Connecting to the Virtual Servers

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

http://203.70.212.52

ftp://203.70.212.52

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

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

Chapter 7
Advanced Administration

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

Overview

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

The available settings and features are:

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

PC Database

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

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

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

PC Database Screen

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

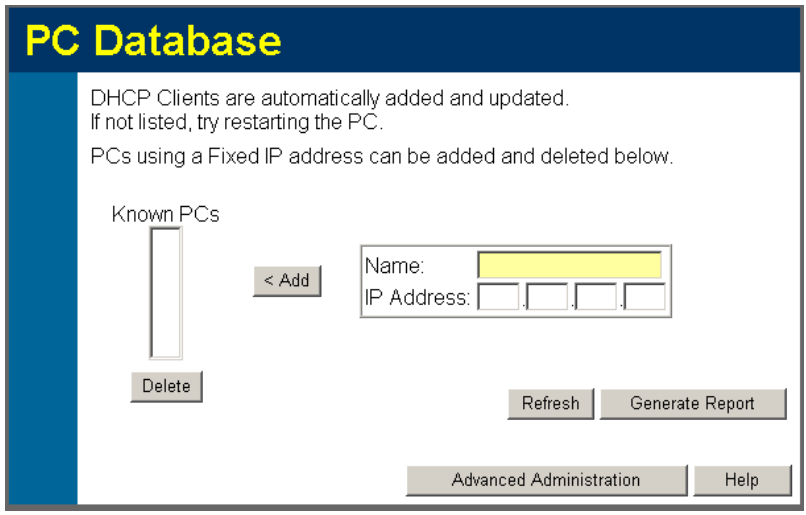


Figure 39: PC Database

- 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 ADSL Wireless Firewall 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.
Buttons	
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: • The PC has been removed from your LAN. • 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.

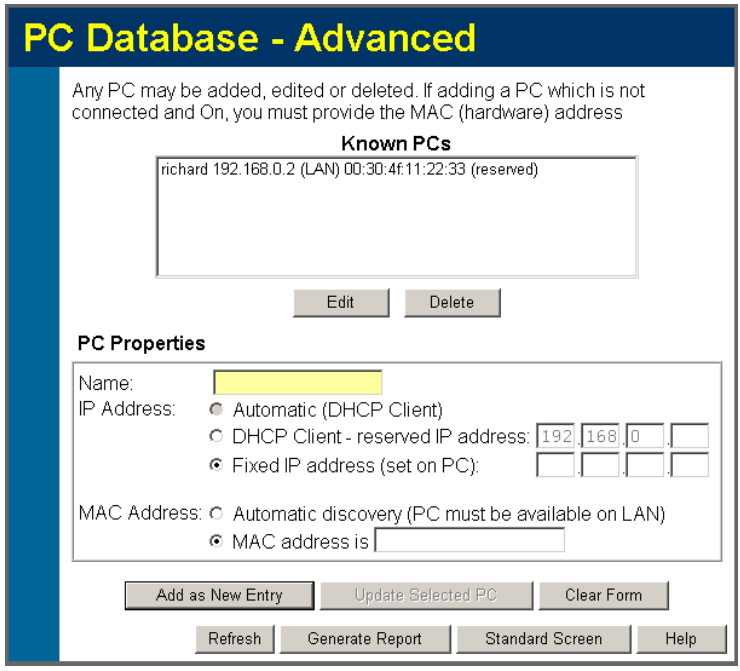


Figure 40: PC Database (Admin)

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.
PC Properties	
Name	If adding a new PC to the list, enter its name here. It is best if this matches the PC's "hostname".
IP Address	Select the appropriate option: • **Automatic** - The PC is set to be a DHCP client (Windows: "Obtain an IP address automatically"). The ADSL Wireless Firewall Router will allocate an IP address to this PC when requested to do so. The IP address could change, but normally won't. • **DCHP Client - Reserved IP Address** - Select this if the PC is set to be a DCHP client, and you wish to guarantee that the ADSL Wireless Firewall Router will always allocate the same IP Address to this PC. Enter the required IP address. • **Fixed IP Address** - Select this if the PC is using a Fixed (Static) IP address. Enter the IP address allocated to the PC. (The PC itself must be configured to use this IP address.)

MAC Address	Select the appropriate option • **Automatic discovery** - Select this to have the ADSL Wireless Firewall Router contact the PC and find its MAC address. This is only possible if the PC is connected to the LAN and powered On. • **MAC address is** - Enter the MAC address on the PC. The MAC address is also called the "Hardware Address", "Physical Address", or "Network Adapter Address". The ADSL Wireless Firewall Router uses this to provide a unique identifier for each PC. Because of this, the MAC address can NOT be left blank.
Buttons	
Add as New Entry	Add a new PC to the list, using the data in the "Properties" box. If "Automatic discovery" (for MAC address) is selected, the PC will be sent a "ping" to determine its hardware address. This will fail unless the PC is connected to the LAN, and powered on.
Update Selected PC	Update (modify) the selected PC, using the data in the "Properties" box.
Clear Form	Clear the "Properties" box, ready for entering data for a new PC.
Refresh	Update the data on screen.
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.

Config File

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

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

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

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

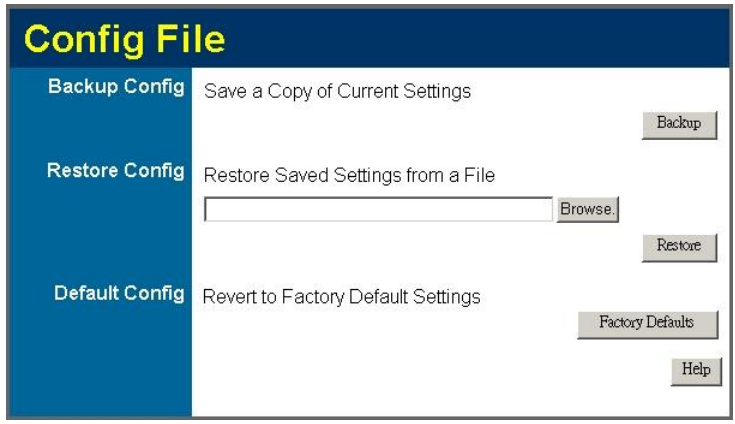


Figure 41: Config File Screen

Data - Config File Screen

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

Logging

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

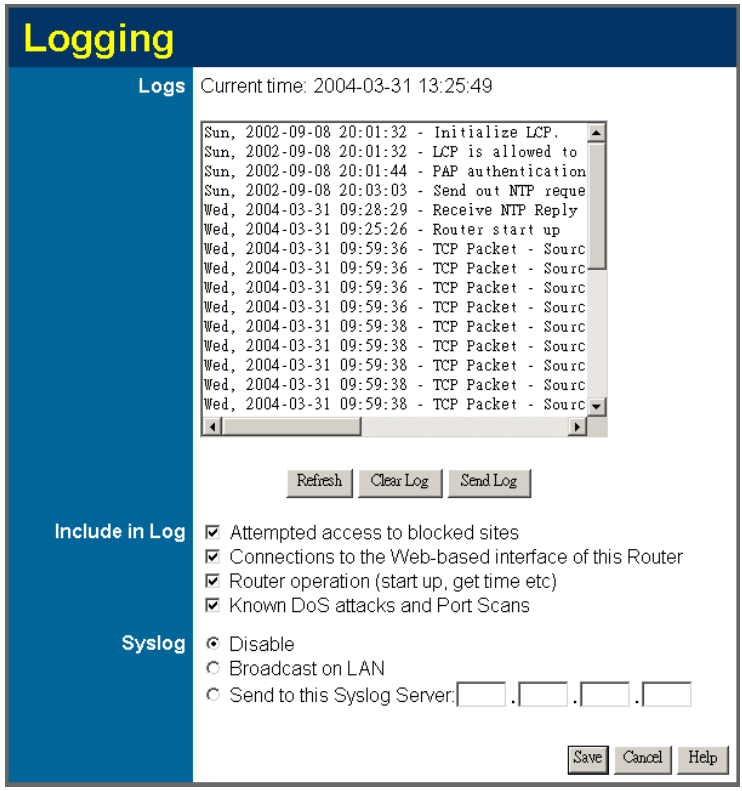


Figure 42: Logging Screen

Data - Logging Screen

Logs	
Current Time	The current time on the ADSL Wireless Firewall Router is displayed.
Log Data	Current log data is displayed in this panel.
Buttons	There are three (3) buttons • **Refresh** - Update the log data. • **Clear Log** - Clear the log, and restart it. This makes new messages easier to read. • **Send Log** - E-mail the log immediately. This is only functional if the ***E-mail*** screen has been configured.

Logs	
Include (Check-boxes)	Use these checkboxes to determine which events are included in the log. Checking all options will increase the size of the log, so it is good practice to disable any events which are not really required. • **Attempted access to blocked sites** - If checked, attempted Internet accesses which were blocked are logged. • **Connections to the Web-based interface of this Router** - If checked, this will log connections TO this Router, rather than through this Router to the Internet. • **Router operation** - If checked, other Router operations (not covered by the selections above) will be logged. • **Known DoS attacks and Port Scans** - If checked, Denial of Service attacks, as well as port scans, will be logged.
Syslog	
Disable	Data is not sent to a Syslog Server.
Broadcast on LAN	The Syslog data is broadcast, rather than sent to a specific Syslog server. Use this if your Syslog Server does not have a fixed IP address.
Syslog	If your Syslog server has a fixed IP address, select this option, and enter the IP address of your Syslog server.

E-mail

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

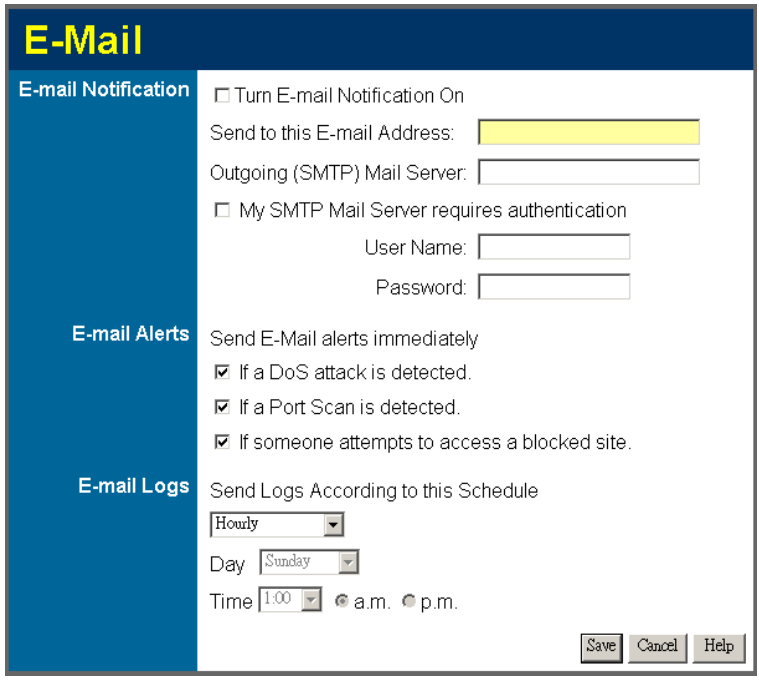


Figure 43: E-mail Screen

Data – E-mail Screen

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

E-mail Alerts	
Send E-mail alerts immediately	You can choose to have alerts E-mailed to you, by checking the desired checkboxes. The Broadband ADSL Router can send an immediate alert when it detects a significant security incident such as • A known hacker attack is directed at your IP address • A computer on the Internet scans your IP address for open ports • Someone on your LAN (Local Area Network) tries to visit a blocked site.
E-mail Logs	

Send Logs	Select the desired option for sending the log by E-mail.
	• **Never** (default) - This feature is disabled; Logs are not sent.
	• **When log is full** - The time is not fixed. The log will be sent when the log is full, which will depend on the volume of traffic.
	• **Hourly, Daily, Weekly...** - The log is sent on the interval specified.
	  • If "Daily" is selected, the log is sent at the time specified.
	  • If the day is specified, the log is sent once per week, on the specified day.
	  • Select the time of day you wish the E-mail to be sent.
	  • If the log is full before the time specified to send it, it will be sent regardless.

Diagnostics

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

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

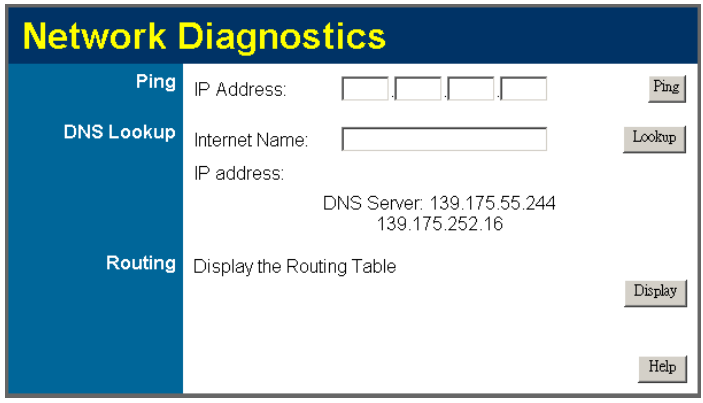


Figure 44: Network Diagnostics Screen

Data - Network Diagnostics Screen

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

Remote Admin

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

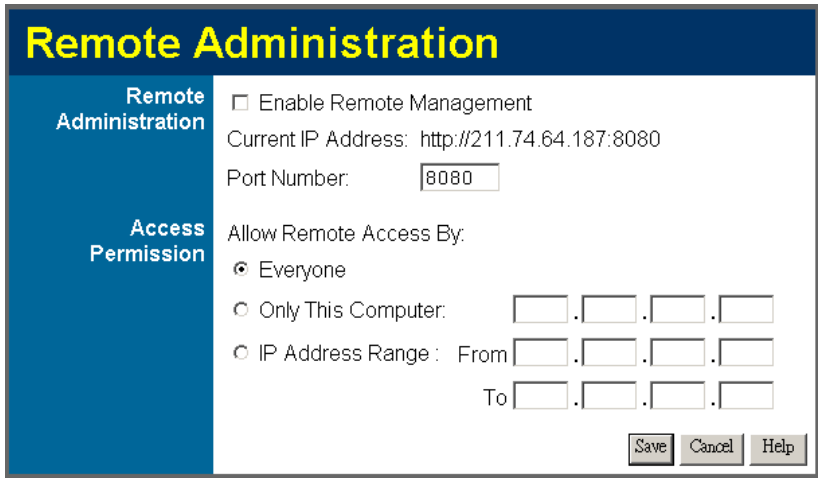


Figure 45: Remote Administration Screen

Data - Remote Administration Screen

Remote Administration	
Enable Remote Management	Check to allow administration/management via the Internet. (To connect, see below). If Disabled, this device will ignore Administration connection attempts from the Internet.
Current IP Address	This is the current address you will use when accessing this device from the Internet. To connect, see details and an example below.
Port Number	Enter a port number between 1024 and 65535. The default for HTTP (Web) connections is port 80, but using port 80 will prevent the use of a Web "Virtual Server" on your LAN. So using a different port number is recommended. The default value is 8080. The port number must be specified in your Browser when you connect, as detailed above.
Access Permission	
Allow Remote Access	Select the desired option. • **Everyone** - allow access by everyone on the Internet. • **Only This Computer** - allow access by only one IP address. Enter the desired IP address. • **IP Address Range** - allow access from a range of IP addresses on the Internet. Enter a beginning and ending IP address to define the allowed range. For security, you should restrict access to as few external IP addresses as practical.

To connect from a remote PC via the Internet

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

   HTTP://123.123.123.123:8080

   This example assumes the WAN IP Address is 123.123.123.123, and the port number is 8080.
3. You will then be prompted for the login name and password for this device.

Routing

Overview

- If you don't have other Routers or Gateways on your LAN, you can ignore the "Routing" page completely.
- If the ADSL Wireless Firewall Router is only acting as a Gateway for the local LAN segment, ignore the "Routing" page even if your LAN has other Routers.
- If your LAN has a standard Router (e.g. Cisco) on your LAN, and the ADSL Wireless Firewall 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 ADSL Wireless Firewall 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 is it 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.

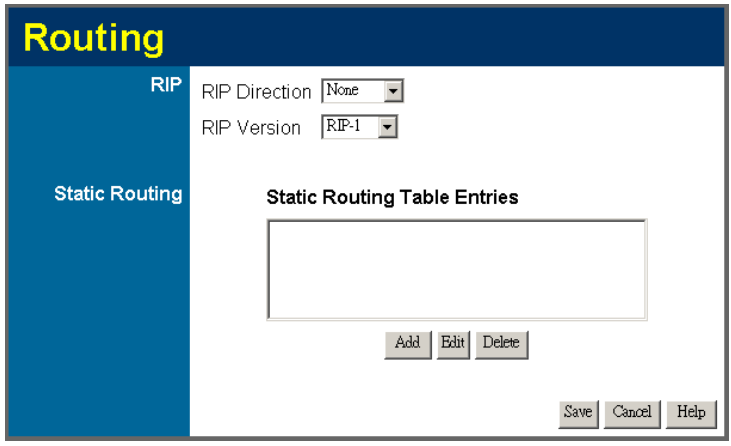


Figure 46: Routing Screen

Data - Routing Screen

RIP	
RIP Direction	Select the desired RIP Direction.
RIP Version	Choose the RIP Version for the Server.
Static Routing	
Static Routing Table Entries	This list shows all entries in the Routing Table. • This area shows details of the selected item in the list. • Change any the properties as required, then click the "Edit" button to save the changes to the selected entry.
Buttons	
Add	Add a new entry to the Static Routing table, using the data shown in the "Properties" area on screen. The entry selected in the list is ignored, and has no effect.
Edit	Update the current Static Routing Table entry, using the data shown in the table area on screen.
Delete	Delete the current Static Routing Table entry.
Save	Save the RIP setting. This has no effect on the Static Routing Table.

Configuring Other Routers on your LAN

It is essential that all IP packets for devices not on the local LAN be passed to the ADSL Wireless Firewall 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 ADSL Wireless Firewall Router as the *Default Route* or *Default Gateway*.

Local Router

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

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

Other Routers on the Local LAN

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

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

Static Routing - Example

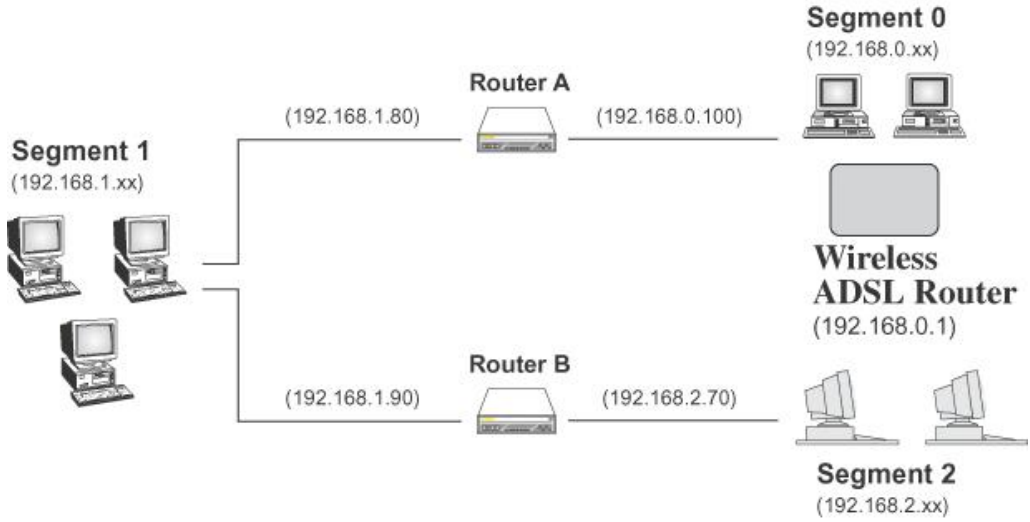


Figure 47: Routing Example

For the ADSL Wireless Firewall Router's Routing Table

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

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

Entry 2 (Segment 2)	
Destination IP Address	192.168.2.0
Network Mask	255.255.255.0 (Standard Class C)
Gateway IP Address	192.168.0.100
Metric	3

For Router A's Default Route

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

For Router B's Default Route

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

Upgrade Firmware

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

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

Figure 48: Router Upgrade Screen

To perform the Firmware Upgrade:

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

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

Appendix A
Troubleshooting

This Appendix covers the most likely problems and their solutions.

Overview

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

General Problems

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

Solution 1: Check the following:

- The ADSL Wireless Firewall Router is properly installed, LAN connections are OK, and it is powered ON.
- Ensure that your PC and the ADSL Wireless Firewall 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 ADSL Wireless Firewall Router's default IP Address of 192.168.0.1.
  Also, the Network Mask should be set to 255.255.255.0 to match the ADSL Wireless Firewall Router.
  In Windows, you can check these settings by using *Control Panel-Network* to check the *Properties* for the TCP/IP protocol.

Internet Access

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

Solution 1: A number of things could be causing this. Try the following trouble-shooting 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 ADSL Wireless Firewall Router. Ensure that it is connected and ON. Connect to it and check its settings. (If you can't connect to it, check the LAN and power connections.)
- Check the ADSL Wireless Firewall Router's status screen to see if it is working correctly.

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

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

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

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

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

Wireless Access

Problem 1: **My PC can't locate the Wireless interface of ADW-4300.**

Solution 1: Check the following.

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

Problem 2: **Wireless connection speed is very slow.**

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

- ADSL Wireless Firewall Router location.
  Try adjusting the location and orientation of the ADSL Wireless Firewall 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 ADSL Wireless Firewall Router.

Appendix B
About Wireless LANs

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

Modes

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

- Ad-hoc
- Infrastructure

Ad-hoc Mode

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

Infrastructure Mode

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

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

BSS/ESS

BSS

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

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

ESS

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

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

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

Channels

The Wireless Channel sets the radio frequency used for communication.

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

WEP

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

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

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

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

Wireless LAN Configuration

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

Mode — On client Wireless Stations, the mode must be set to "Infrastructure".
(The Access Point is always in "Infrastructure" mode.)

SSID (ESSID) — Wireless Stations should use the same SSID (ESSID) as the Access Point they wish to connect to. Alternatively, the SSID can be set to "any" or null (blank) to allow connection to any Access Point.

WEP — The Wireless Stations and the Access Point must use the same settings for WEP (Off, 64 Bit, 128 Bit).

WEP Key: If WEP is enabled, the Key must be the same on the Wireless Stations and the Access Point.

WEP Authentication: 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

ADSL Wireless Firewall Router

Product		802.11g ADSL Wireless Firewall Router
Model		ADW-4300A / ADW-4300B
Hardware		
Standard		ANSI T1.413 Issue 2 ITU G.992.1 (G.dmt) including - Annex A (ADSL over POTS for ADW-4300A) - Annex B (ADSL over ISDN for ADW-4300B) G.992.2 (G.lite) with fast retrain
Protocol		RFC 2364 - PPP over ATM (LLC/VCMUX) RFC 2516 - PPP over Ethernet (LLC/VCMUX) RFC 1577 - Classic IP over ATM (LLC/VCMUX) RFC 1483 - Bridged IP over ATM (LLC/VCMUX) RFC 1483 - Routed IP over ATM (LLC/VCMUX)
AAL and ATM Support		Integrated ATM AAL5 support 255 VPI plus 65535 VCI address range
Ports	LAN	4 (10Base-T/100Base-TX, Auto-Negotiation, Auto MDI/MDI-X)
	Wireless	1 x 802.11g wireless access point
	WAN	1 (RJ-11, 10/100Base-TX, Auto-Negotiation)
LED Indicators		PWR, STATUS, WLAN, ADSL 100 LNK/ACT, 10 LNK ACT for each LAN port
Button		1 for reset/factory reset
Wireless Standard		IEEE802.11b, IEEE802.11g WLAN,
Frequency		2.4 to 2.4835GHz (Industrial Scientific Medical Band)
Channels		Maximum 14 Channels, depending on regulatory authorities
Modulation		CCK, DQPSK, DBPSK, OFDM/CCK
Data Rate		Up to 54 Mbps
WEP		64-bit, 128-bit
Output Power		13dBm (typical)
Receiver Sensitivity		-80dBm Min.
Software		
Protocol		IP, NAT, ARP, ICMP, DHCP, PPPoE, PPPoA, IPoA, RIP1/2
Security		Native NAT firewall, Enhanced policy-based+ SPI firewall, URL Filter, Blocking log, Virtual Server, DMZ
Management		Web browser management
Environment Specification		
Dimension (W x D x H)		199 mm x 150 mm x 33 mm

Power	15V AC, 1A
Power Consumption	Maximum 15W, 51 BTU
Temperature: Humidity	0~40 degree C (operating), -10~70 degree C (storage) 5%~ 95% (non-condensing)
Emission	FCC, CE

Regulatory Approvals

FCC Statement

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

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

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

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

FCC Radiation Exposure Statement

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

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

(1) This device may not cause harmful interference, and

(2) This device must accept any interference received, including interference that may cause undesired operation.

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

CE Approval

CE Standards

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

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

CE Marking Warning

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.