IP819VGA
802.11g ADSL VoIP Gateway

802.11g/802.11b Access Point

ADSL Modem

NAT Router

VoIP Gateway

User's Guide

Table of Contents

P/N: 9560R60001

Document Version: 1.3

Chapter 1
Introduction

This Chapter provides an overview of the 802.11g ADSL VoIP Gateway's features and capabilities.

Congratulations on the purchase of your new 802.11g ADSL VoIP Gateway. The 802.11g ADSL VoIP Gateway is a multi-function device providing the following services:

- ***ADSL Modem***.
- ***Shared Broadband Internet Access*** (NAT Router) for all LAN & WLAN users.
- ***Wireless Access Point*** for 802.11b and 802.11g Wireless Stations.
- ***VoIP Gateway*** supporting the industry-standard SIP protocol.
- ***4-Port Ethernet Port*** for 10BaseT or 100BaseT connections.

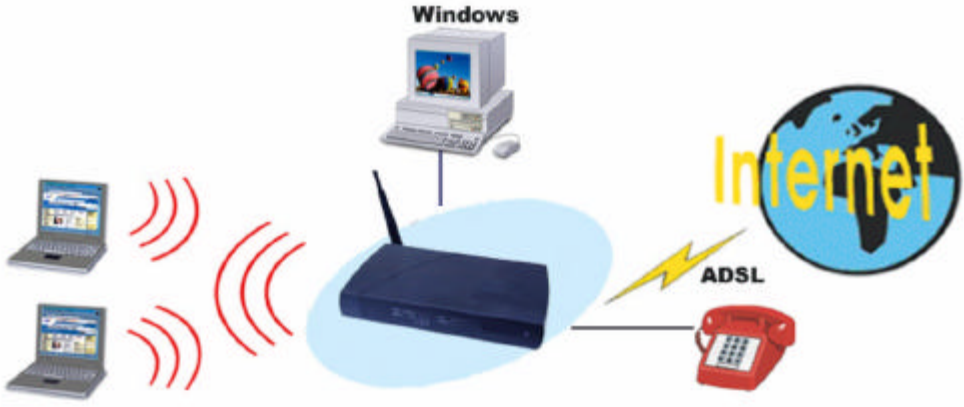

Figure 1: 802.11g ADSL VoIP Gateway

802.11g ADSL VoIP Gateway Features

The 802.11g ADSL VoIP Gateway 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 802.11g ADSL VoIP Gateway, 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 802.11g ADSL VoIP Gateway has a built-in ADSL modem, supporting all common ADSL connections.
- ***IPoA, PPPoE, PPPoA, Direct Connection Support.*** The 802.11g ADSL VoIP Gateway supports all common connection methods.

- ***Auto-detection of Internet Connection Method.*** In most situations, the 802.11g ADSL VoIP Gateway 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 802.11g ADSL VoIP Gateway supports both Dynamic IP Address (IP Address is allocated on connection) and Fixed IP Address.

Advanced Internet Functions

- ***Application Level Gateways (ALGs).*** Applications which use non-standard connections or port numbers are normally blocked by the Firewall. The ability to define and allow such applications is provided, to enable such applications to be used normally.
- ***Special Applications.*** This feature, also called Port Triggering, allows you to use Internet applications which normally do not function when used behind a firewall.
- ***Virtual Servers.*** This feature allows Internet users to access Internet servers on your LAN. The required setup is quick and easy.
- ***Dynamic DNS Support.*** DDNS, when used with the Virtual Servers feature, allows users to connect to Servers on your LAN using a Domain Name, even if you have a dynamic IP address which changes every time you connect.
- ***URL Filter.*** Use the URL Filter to block access to undesirable Web sites by LAN users.
- ***Firewall.*** As well as the built-in firewall to protect your LAN, you can define Firewall Rules to determine which incoming and outgoing traffic should be permitted.
- ***Scheduling.*** Both the URL Filter and Firewall rules can be scheduled to operate only at certain times. This provides great flexibility in controlling Internet-bound traffic.
- ***Logs.*** Define what data is recorded in the Logs, and optionally send log data to a Syslog Server. Log data can also be E-mailed to you.
- ***VPN Pass through Support.*** PCs with VPN (Virtual Private Networking) software using PPTP, L2TP and IPSec are transparently supported - no configuration is required.

VoIP Features

- ***SIP Standard Compatible***. The Wireless VoIP Gateway complies with the SIP standard for VoIP.
- ***Advanced Call features***. Caller ID, Caller name, Call waiting, three-way conference call, DTMF relay, Voice active detection, Echo canceller.
- ***FAX Support***. Both the T.38 and G.711 Fax standards are supported, allowing both sending and receiving faxes via the Wireless VoIP Gateway.
- ***Life line (PSTN fallback) Support***. The PSTN (analogue phone) port is automatically used when the Internet connection is not operational or there is a power failure.

Wireless Features

- ***Standards Compliant.*** The 802.11g ADSL VoIP Gateway 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 up and exceeding 54Mbps.*** All speeds up to the 802.11g maximum of 54Mbps are supported. Also, the 802.11g ADSL VoIP Gateway support TI's proprietary "g-Plus" solution, which allows even faster speeds between compatible wireless devices.
- ***WEP support.*** Support for WEP (Wired Equivalent Privacy) is included. Key sizes of 64 Bit and 128 Bit are supported. WEP encrypts any data before transmission, providing protection against snoopers.
- ***WPA-PSK support.*** Like WEP, WPA-PSK encrypts any data before transmission, providing protection against snoopers. The WPA-PSK is a later standard than WEP, and provides both easier configuration and greater security than WEP.
- ***Wireless MAC Access Control.*** The Wireless Access Control feature can check the MAC address (hardware address) of Wireless stations to ensure that only trusted Wireless Stations can access your LAN.
- ***Simple Configuration.*** If the default settings are unsuitable, they can be changed quickly and easily.

LAN Features

- ***4-Port Ethernet Switching Hub.*** The 802.11g ADSL VoIP Gateway incorporates a 4-port 10/100BaseT switching hub.
- ***DHCP Server Support.*** **D**ynamic **H**ost **C**onfiguration **P**rotocol provides a dynamic IP address to PCs and other devices upon request. The 802.11g ADSL VoIP Gateway 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 802.11g ADSL VoIP Gateway to your PC, and restore (upload) a previously-saved configuration file to the 802.11g ADSL VoIP Gateway.
- ***Remote Management.*** The 802.11g ADSL VoIP Gateway can be managed from any PC on your LAN or Wireless LAN. And, if the Internet connection exists, it can also (optionally) be configured via the Internet.
- ***Network Diagnostics.*** You can use the 802.11g ADSL VoIP Gateway to perform a *Ping* or *DNS lookup*.

Security Features

- ***Password - protected Configuration***. Password protection is provided to prevent unauthorized users from modifying the configuration data and settings.
- ***Wireless LAN Security***. WPA-PSK, WEP and Wireless access control by MAC address are all supported. The MAC-level access control feature can be used to prevent unknown wireless stations from accessing your LAN.
- ***NAT Protection.*** An intrinsic side effect of NAT (Network Address Translation) technology is that by allowing all LAN users to share a single IP address, the location and even the existence of each PC is hidden. From the external viewpoint, there is no network, only a single device - the 802.11g ADSL VoIP Gateway.
- ***Firewall.*** All incoming data packets are monitored and all incoming server requests are filtered, thus protecting your network from malicious attacks from external sources.

- ***Protection against DoS attacks.*** DoS (Denial of Service) attacks can flood your Internet connection with invalid packets and connection requests, using so much bandwidth and so many resources that Internet access becomes unavailable. The 802.11g ADSL VoIP Gateway incorporates protection against DoS attacks.

Package Contents

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

- The 802.11g ADSL VoIP Gateway Unit
- 1 Cat-5 Ethernet (LAN) cable
- 1 RJ-11 (ADSL) cable
- 1 RJ-11 to RJ45 cable (Germany only)
- Power Adapter
- Quick Installation Guide
- CD-ROM containing the on-line manual.

Physical Details

Front-mounted LEDs

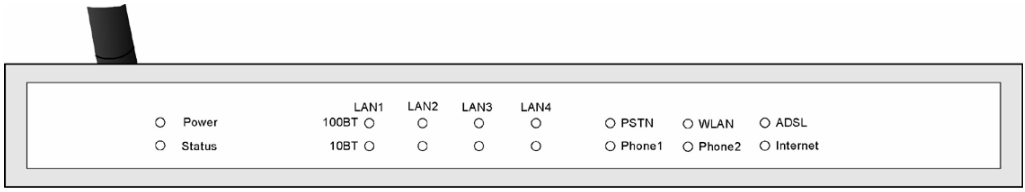

Figure 2: Front Panel

Power LED (Green)

On - Power on.

Off - No power.

Status LED (Yellow)

Off - Normal operation.

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

LAN

For each LAN port, there are two LED.

- **100BT** - This will be ON if the LAN connection is using 100BaseT, and Blinking if data is being transferred via the LAN port.
- **10BT** - This will be ON if the LAN connection is using 10BaseT, and Blinking if data is being transferred via the LAN port.

If neither LED is on, there is no active connection on the LAN port.

PSTN

Off - PSTN is idle or not connected.

Flashing - PSTN line is in use.

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 established. (This is a low-level connection, it does not mean Internet access is available.)

Off - No ADSL connection currently exists.

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

Phone 1

On - Connected to SIP Server.

Off - Idle or not connected.

Flashing (quickly) -Phone is in use.

Phone 2

On - Connected to SIP Server.

Off - Idle or not connected.

Flashing (quickly) -Phone is in use.

Internet	**On -** Internet connection is available.
	Off - No Internet connection available.
	Flashing - Data is being transmitted or received.

Rear Panel

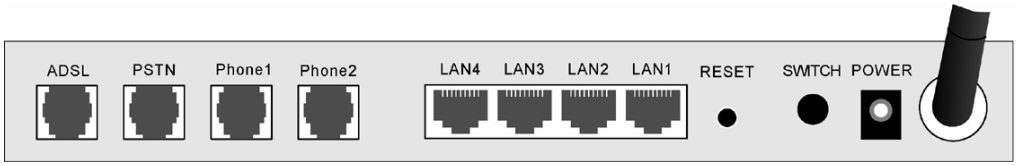

Figure 3: Rear Panel

ADSL port	Connect this port to your ADSL line.
PSTN	Connect this to your PSTN line (normal analog phone line).
Phone 1	Connect a standard phone here.
Phone 2	Connect a standard phone here.
LAN 1 - LAN 4	Connect your PCs to these ports.
Reset Button (Reset to Defaults)	This button will reset the 802.11g ADSL VoIP Gateway 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 802.11g ADSL VoIP Gateway to restart using the factory default values.
Power switch	Press IN for power ON, OUT for power OFF.
Power port	Connect the supplied power adapter here.

Chapter 2
Installation

This Chapter covers the physical installation of the 802.11g ADSL VoIP Gateway.

Requirements

- TCP/IP protocol must be installed on all PCs.
- To use the Wireless Access Point, all Wireless devices must be compliant with the IEEE 802.11g or IEEE 802.11b specifications.
- For Internet Access, an ADSL service and ISP account.
- For VoIP, a SIP account with a VoIP service provider.

Procedure

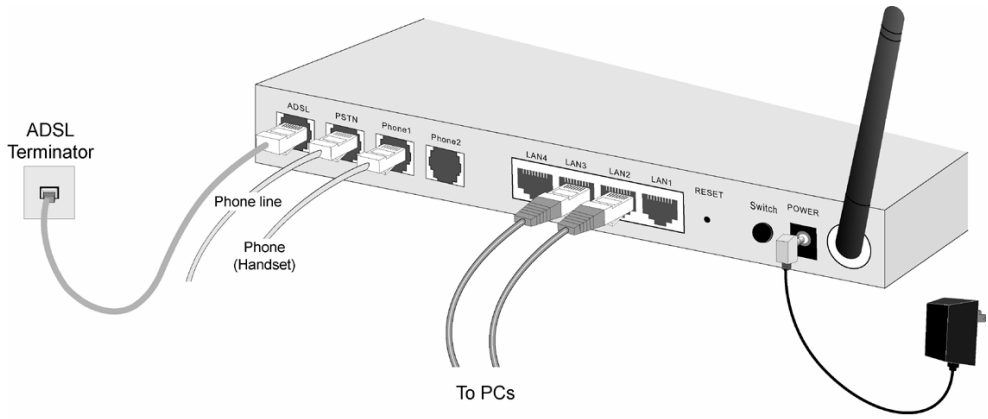

Figure 4: Installation Diagram

1. Choose an Installation Site

Select a suitable place on the network to install the 802.11g ADSL VoIP Gateway. Ensure the power is OFF.

Note!

For best Wireless reception and performance, the 802.11g ADSL VoIP Gateway should be positioned in a central location with minimum obstructions between the 802.11g ADSL VoIP Gateway and the PCs.

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

2. Connect PCs

Use standard LAN cables to connect the **PCs** to the **LAN** ports on the 802.11g ADSL VoIP Gateway.

3. Connect ADSL Cable

Connect the supplied ADSL cable from the **ADSL** port on the 802.11g ADSL VoIP Gateway to the ADSL terminator provided by your phone company.

4. Connect PSTN Line

Connect the PSTN socket on the rear of the Wireless VoIP Gateway to your normal phone line socket.

5. Connect Phones

Connect a standard phone to the Phone 1 and Phone 2 sockets on the rear of the Wireless VoIP Gateway.

6. Power Up

Connect the supplied power adapter to the 802.11g ADSL VoIP Gateway. Use only the power adapter provided. Using a different one may cause hardware damage.

Power up by pressing the rear-mounted power switch IN, and wait for startup to be completed.

7. Check the LEDs

- The *Power* LED should be ON.
- The *Status* LED should flash, then turn Off. If it stays on, there is a hardware error.
- For each LAN port, either the *100BT* or *10BT* LED should be ON if a PC is connected to the port. (Both LEDs may be Off if the PC is not powered on.)
- *Phone 1* and *Phone 2* LEDs will be OFF.
- *PSTN* LED will be OFF.
- *WLAN* LED should be ON
- *ADSL* LED should be ON.
- *Internet* LED will be OFF.
  It will come ON when configuration is complete and correct, and an Internet connection is established.

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

Chapter 3
Setup

This Chapter provides Setup details of the 802.11g ADSL VoIP Gateway.

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 802.11g ADSL VoIP Gateway 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
Use any of the following **Advanced** features: • Internet (DMZ, Special Applications, URL Filter) • Dynamic DNS • Firewall Rules • Firewall Services • Options • Schedule • Virtual Servers • VoIP	Chapter 5: Advanced Features
Use any of the following **Administration** features: • PC Database • Config File • Logs • E-mail • Diagnostics • Remote Admin • Routing • Upgrade Firmware	Chapter 6 Advanced Administration
Check 802.11g ADSL VoIP Gateway operation and Status.	Chapter 7: Operation and Status

Configuration Program

The 802.11g ADSL VoIP Gateway contains an HTTP server. This enables you to connect to it, and configure it, using your Web Browser. **Your Browser must support JavaScript**.

The configuration program has been tested on the following browsers:

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

Preparation

Before attempting to configure the 802.11g ADSL VoIP Gateway, please ensure that:

- Your PC can establish a physical connection to the 802.11g ADSL VoIP Gateway. The PC and the 802.11g ADSL VoIP Gateway must be directly connected (using the Hub ports on the 802.11g ADSL VoIP Gateway) or on the same LAN segment.
- The 802.11g ADSL VoIP Gateway must be installed and powered ON.
- If the 802.11g ADSL VoIP Gateway's default IP Address (192.168.0.1) is already used by another device, the other device must be turned OFF until the 802.11g ADSL VoIP Gateway is allocated a new IP Address during configuration.

Using UPnP

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

- Unless you intend to change the IP Address of the Wireless VoIP Gateway, you can accept the desktop shortcut.
- Whether you accept the desktop shortcut or not, you can always find UPnP devices in *My Network Places* (previously called *Network Neighborhood*).

Double - click the icon for the Wireless VoIP Gateway (either on the Desktop, or in *My Network Places*) to start the configuration. Refer to the following section *Setup Wizard* for details of the initial configuration process.

Using your Web Browser

To establish a connection from your PC to the 802.11g ADSL VoIP Gateway:

1. After installing the 802.11g ADSL VoIP Gateway 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 802.11g ADSL VoIP Gateway, as in this example, which uses the 802.11g ADSL VoIP Gateway's default IP Address:

   ```
   HTTP://192.168.0.1
   ```

4. When prompted to login, use the following username and password.
   - User name: `admin`
   - Password: `password`

If you can't connect

If the 802.11g ADSL VoIP Gateway does not respond, check the following:

- The 802.11g ADSL VoIP Gateway 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 802.11g ADSL VoIP Gateway'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 802.11g ADSL VoIP Gateway'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 802.11g ADSL VoIP Gateway 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 802.11g ADSL VoIP Gateway, you should run the Setup Wizard to configure the 802.11g ADSL VoIP Gateway for Internet access.

1. Select **Setup Wizard** on the main menu.
2. 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.
3. On the final screen of the Wizard, run the test and check that an Internet connection can be established.
4. 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.

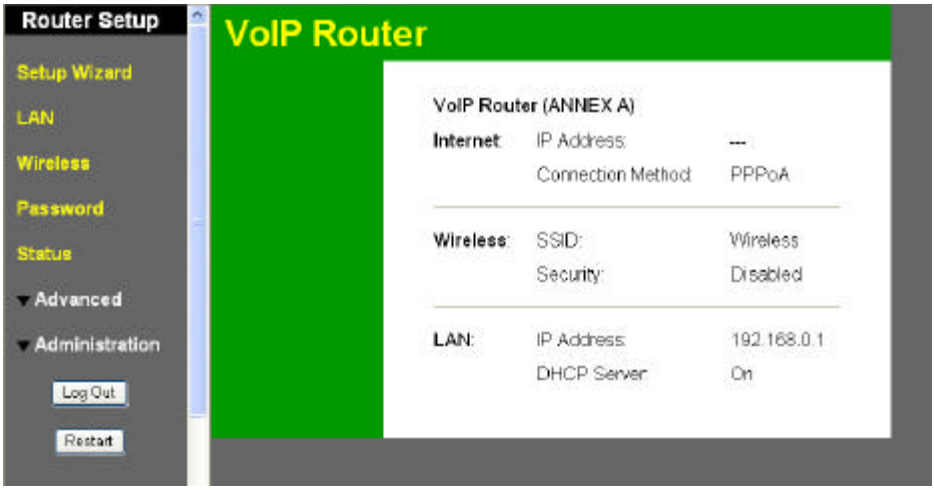

Figure 5: Home Screen

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 802.11g ADSL VoIP Gateway. 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.

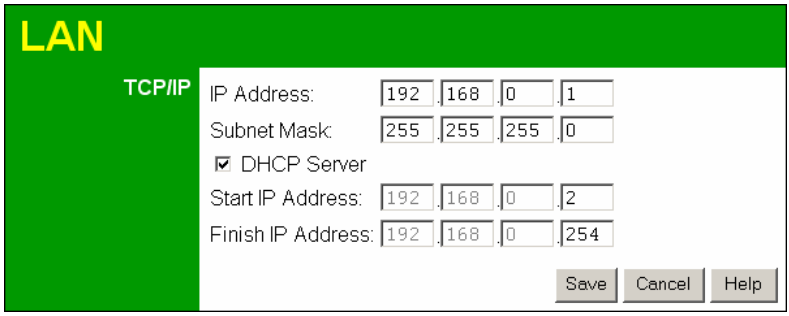

Figure 6: LAN Screen

Data - LAN Screen

TCP/IP	
IP Address	IP address for the 802.11g ADSL VoIP Gateway, 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 802.11g ADSL VoIP Gateway is attached (the same value as the PCs on that LAN segment).
DHCP Server	• If Enabled, the 802.11g ADSL VoIP Gateway 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 802.11g ADSL VoIP Gateway 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 802.11g ADSL VoIP Gateway 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 802.11g ADSL VoIP Gateway'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 802.11g ADSL VoIP Gateway'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 802.11g ADSL VoIP Gateway's, the following procedure is required.

- Disable the DHCP Server feature in the 802.11g ADSL VoIP Gateway. This setting is on the LAN screen.
- Configure the DHCP Server to provide the 802.11g ADSL VoIP Gateway'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 - PC Configuration* for the procedure to check these settings.

Wireless Screen

The 802.11g ADSL VoIP Gateway's settings mu st match the other Wireless stations.

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

To change the 802.11g ADSL VoIP Gateway'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.

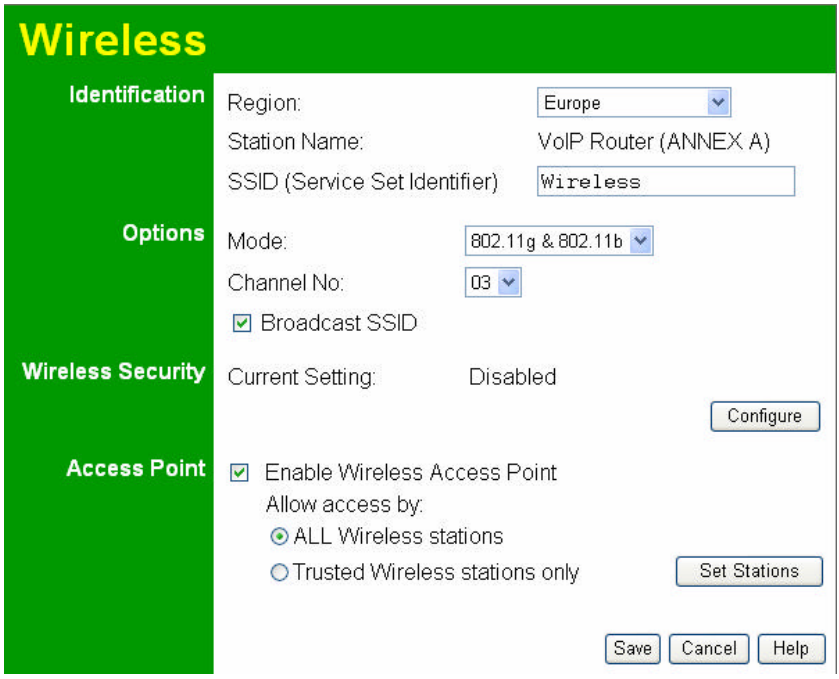

Figure 7: Wireless Screen

Data - Wireless Screen

Identification	
Region	Select the correct domain for your location. It is your responsibility to ensure: • That the 802.11g ADSL VoIP Gateway 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 802.11g ADSL VoIP Gateway.
SSID	This is also called the "Network Name". Enter the desired value. The default value is `Wireless`. • 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 use the same SSID/ESSID, so must match the value entered here.

Options	

Mode	Select the desired mode:
	• **802.11G-plus (TI)** This allows clients to use any of the following modes:
	  • Standard 802.11b
	  • 802.11B+ (Texas Instruments proprietary enhanced mode)
	  • Standard 802.11g
	  • 802.11G-plus (Texas Instruments proprietary enhanced mode). This mode can increase throughput by up to 50%, but will only work between compatible TI wireless stations.
	• **802.11g & 802.11b** - Both 802.11.g and 802.11b Wireless stations will be able to use the 802.11g ADSL VoIP Gateway.
	• **802.11g only** - Only 802.11g Wireless stations can use the 802.11g ADSL VoIP Gateway.
	• **802.11b only** - Only 802.11b connections are available. 802.11g Wireless Stations will only be able to use the 802.11g ADSL VoIP Gateway 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 802.11g ADSL VoIP Gateway will broadcast its SSID. This allows PCs and other wireless stations to detect this Access Point and use the correct SSID. If disabled, PC users will have to manually enter the SSID and other details of the wireless interface before they can connect to this Access Point.
Wireless Security	
Current Setting	The current Wireless security is displayed. The default value is Disabled.
Configure Button	Click this button to access the Wireless security sub-screen, and view or change the settings. See the following section for 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 made 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 security settings. • **Trusted Wireless stations only** - Only wireless stations you designate as "Trusted" can use the Access Point, even if they have the correct SSID and security settings. This feature uses the MAC address to identify Wireless stations. The MAC address is a low-level network identifier which is unique to each PC or network device. To define the trusted wireless stations, use the "Set Stations" button.
Set Stations Button	Click this button to manage the trusted PC database.

Wireless Security

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

- **Disabled** - no data encryption is used.
- **WEP** - data is encrypted using the WEP standard.
- **WPA-PSK** - data is encrypted using the WPA-PSK standard. This is a later standard than WEP, and provides much better security than WEP. If all your Wireless stations support WPA-PSK, you should use WPA-PSK rather than WEP.

WEP Wireless Security

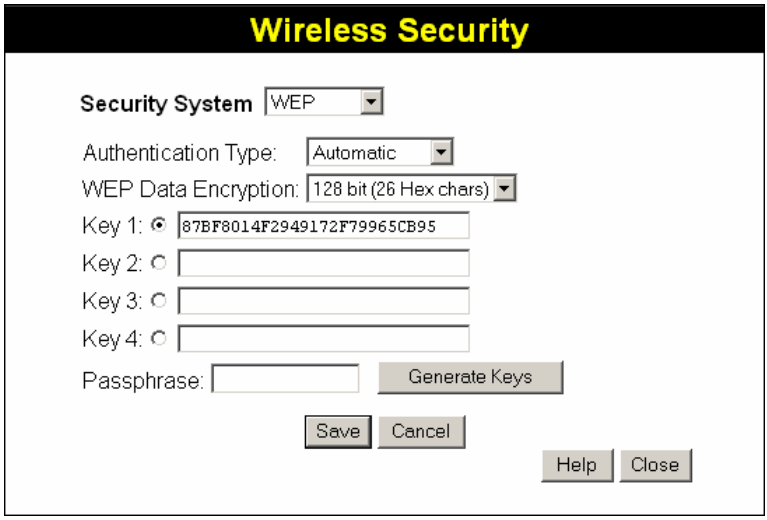

Figure 8: WEP

Data - WEP Screen

WEP Data Encryption	
WEP Data Encryption	Select the desired option, and ensure the Wireless Stations use the same setting. • **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.

WPA-PSK Wireless Security

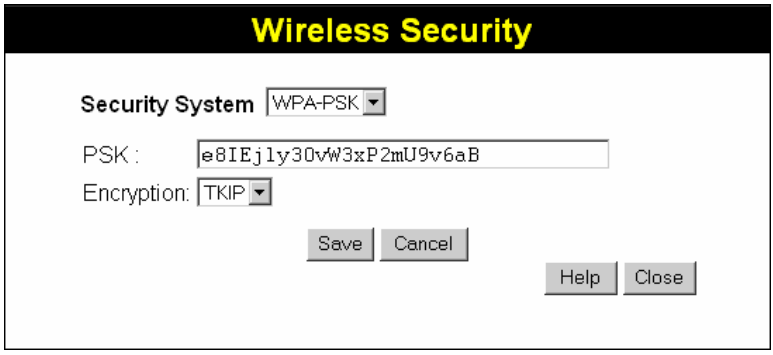

Figure 9: WPA-PSK

Data - WPA-PSK Screen

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

Trusted Wireless Stations

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

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

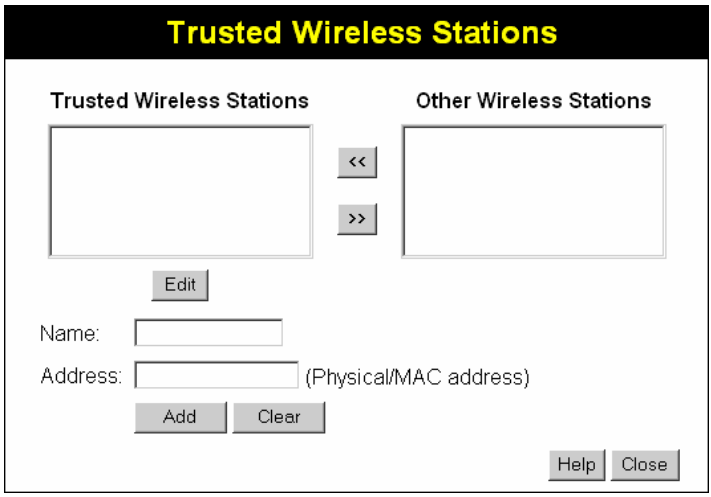

Figure 10: Trusted Wireless Stations

Data - Trusted Wireless Stations

Trusted Wireless Stations	This lists any Wireless Stations which you have designated as “Trusted”.
Other Wireless Stations	This list any Wireless Stations detected by the Access Point, which you have not designated as "Trusted".
Name	The name assigned to the Trusted Wireless Station. Use this when adding or editing a Trusted Station.
Address	The MAC (physical) address of the Trusted Wireless Station. Use this when adding or editing a Trusted Station.
Buttons	
<<	Add a Trusted Wireless Station to the list (move from the "Other Stations" list). • Select an entry (or entries) in the "Other Stations" list, and click the " << " button. • Enter the Address (MAC or physical address) of the wireless station, and click the "Add " button.
>>	Delete a Trusted Wireless Station from the list (move to the "Other Stations" list). • Select an entry (or entries) in the "Trusted Stations" list. • Click the " >> " button.

Edit	Use this to change an existing entry in the "Trusted Stations" list: 1. Select the Station in the *Trusted Station* list. 2. Click the *Edit* button. The address will be copied to the "Address" field, and the *Add* button will change to *Update*. 3. Edit the address (MAC or physical address) as required. 4. Click *Update* to save your changes.
Add (Update)	To add a Trusted Station which is not in the "Other Wireless Stations" list, enter the required data and click this button. When editing an existing Wireless Station, this button will change from *Add* to *Update*.
Clear	Clear the *Name* and *Address* fields.

Password Screen

The password screen allows you to assign a password to the 802.11g ADSL VoIP Gateway.

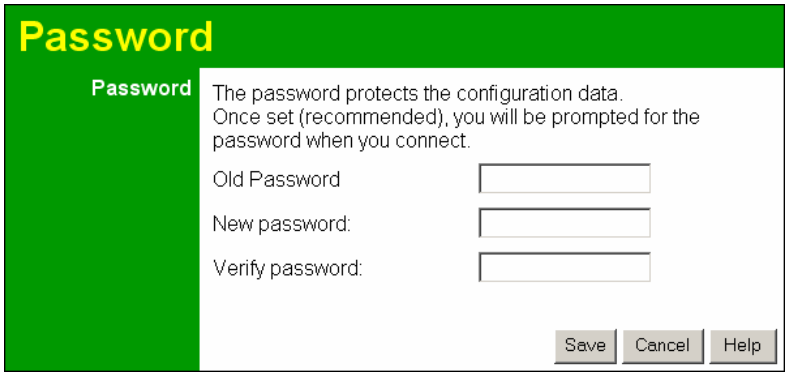

Figure 11: Password Screen

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.

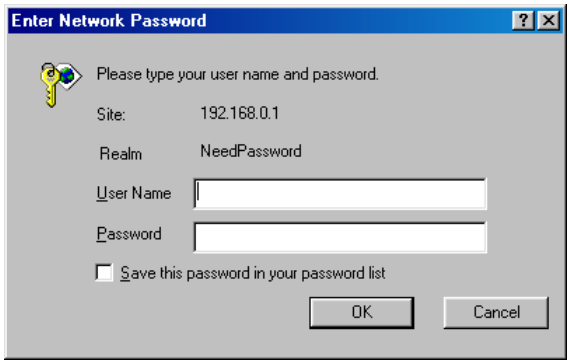

Figure 12: Password Dialog

- The "User Name" is always `admin`
- Enter the password for the 802.11g ADSL VoIP Gateway, 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 802.11g ADSL VoIP Gateway.

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

The 802.11g ADSL VoIP Gateway 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 802.11g ADSL VoIP Gateway settings, and the default Windows TCP/IP settings, no changes need to be made.

- By default, the 802.11g ADSL VoIP Gateway will act as a DHCP Server, automatically providing a suitable IP Address (and related information) to each PC when the PC boots.
- For all non-Server versions of Windows, the default TCP/IP setting is to act as a DHCP client.

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

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

If your LAN has a Router, the LAN Administrator must re-configure the Router itself. Refer to *Chapter 6 - Advanced Administration* for details.

Checking TCP/IP Settings - Windows 98/ME:

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

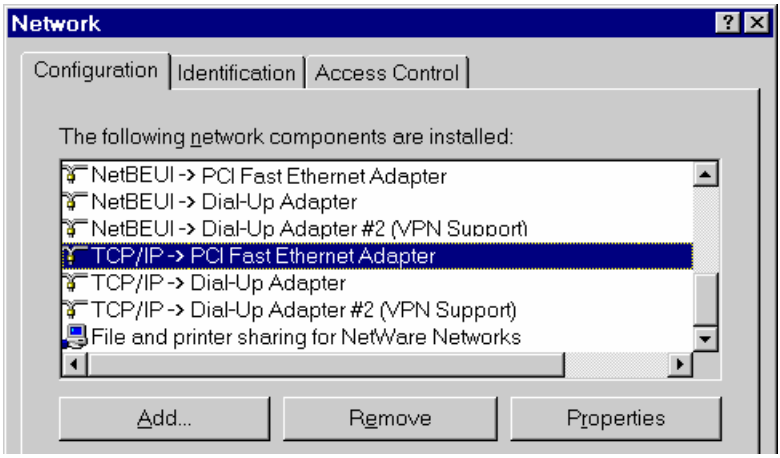

Figure 13: Network Configuration

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.

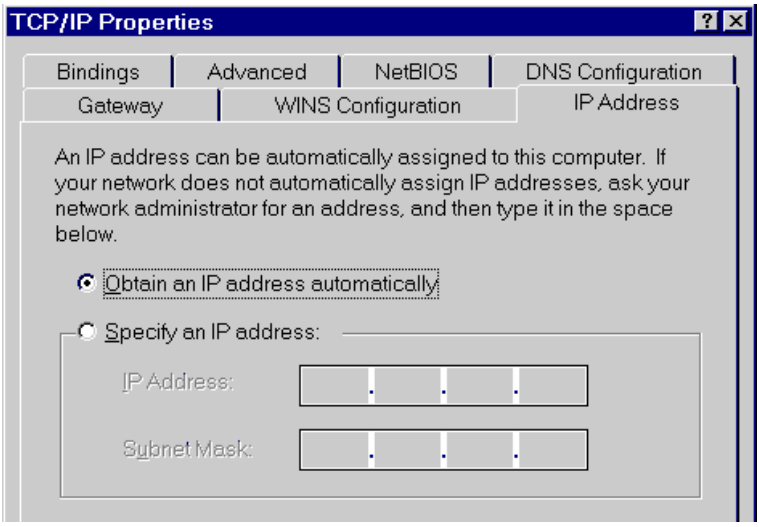

Figure 14: IP Address (Win 95)

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 802.11g ADSL VoIP Gateway will act as a DHCP Server.

Restart your PC to ensure it obtains an IP Address from the 802.11g ADSL VoIP Gateway.

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 802.11g ADSL VoIP Gateway'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 802.11g ADSL VoIP Gateway.

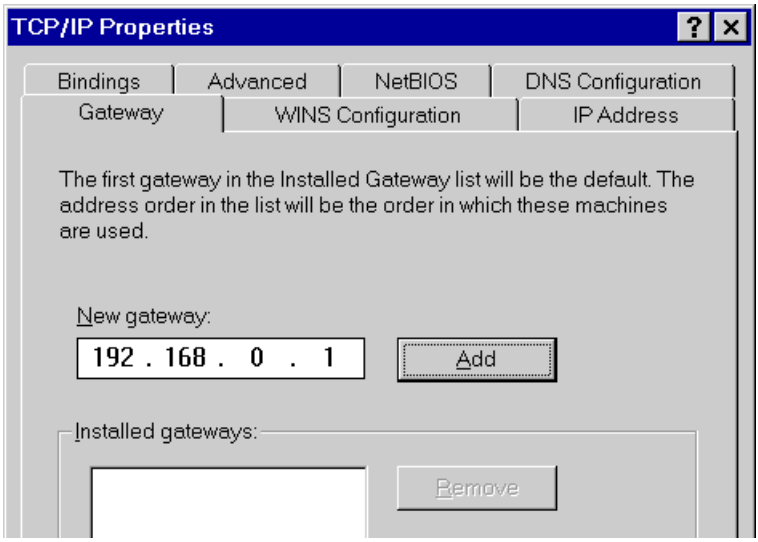

Figure 15: Gateway Tab (Win 98/ME)

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

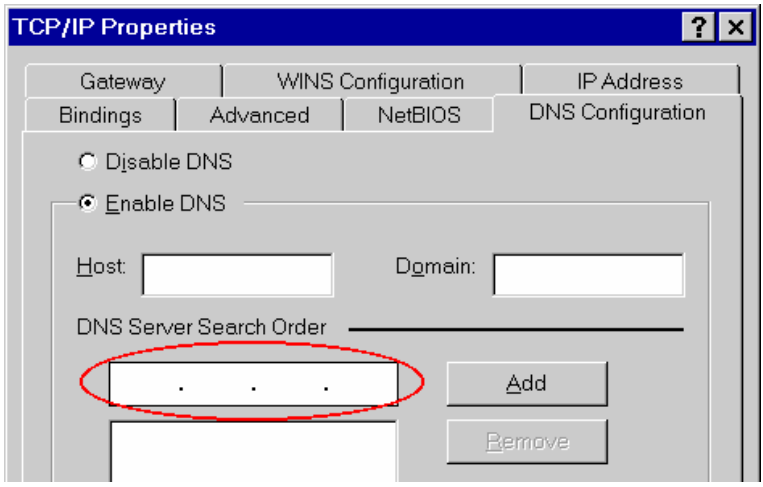

Figure 16: DNS Tab (Win 98/ME)

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.

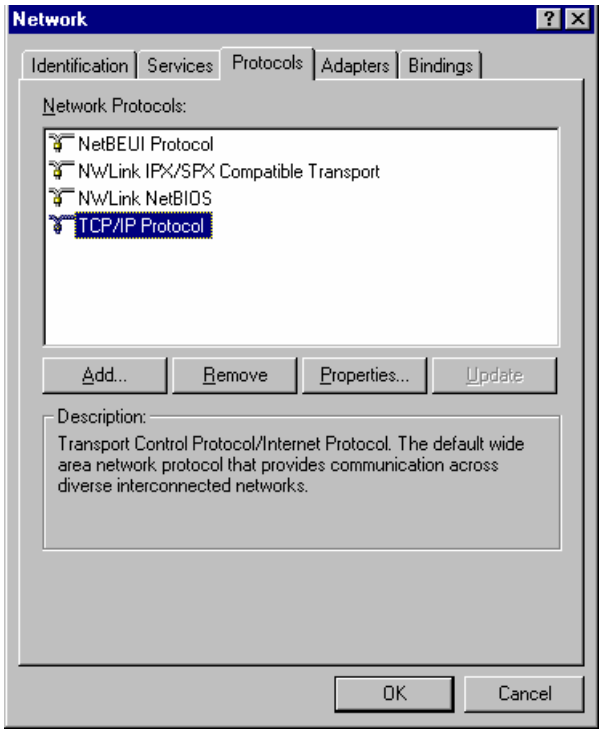

Figure 17: Windows NT4.0 - TCP/IP

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

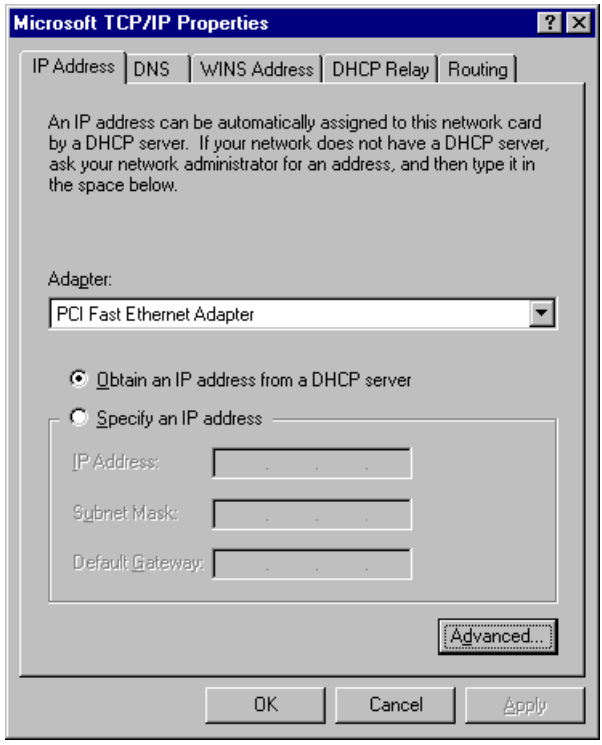

Figure 18: Windows NT4.0 - IP Address

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 802.11g ADSL VoIP Gateway will act as a DHCP Server.

Restart your PC to ensure it obtains an IP Address from the 802.11g ADSL VoIP Gateway.

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 802.11g ADSL VoIP Gateway. 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 802.11g ADSL VoIP Gateway's IP address, as shown in Figure 19 below.
   - If necessary, use the *Up* button to make the 802.11g ADSL VoIP Gateway the first entry in the *Gateways* list.

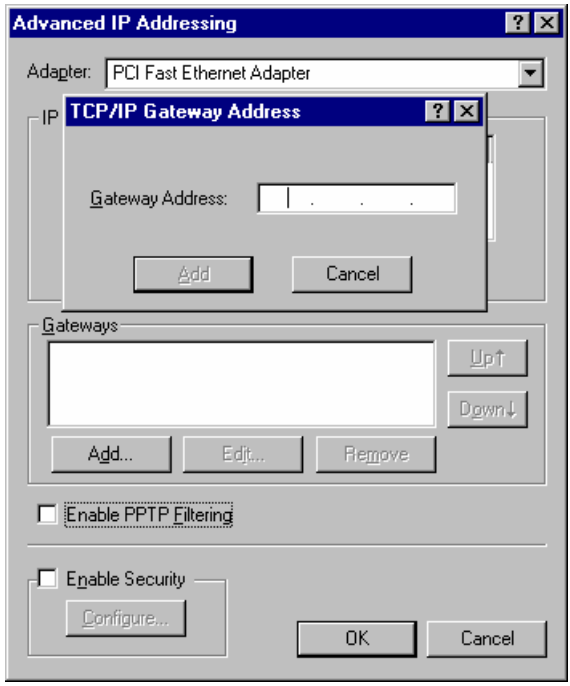

Figure 19 - Windows NT4.0 - Add Gateway

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.

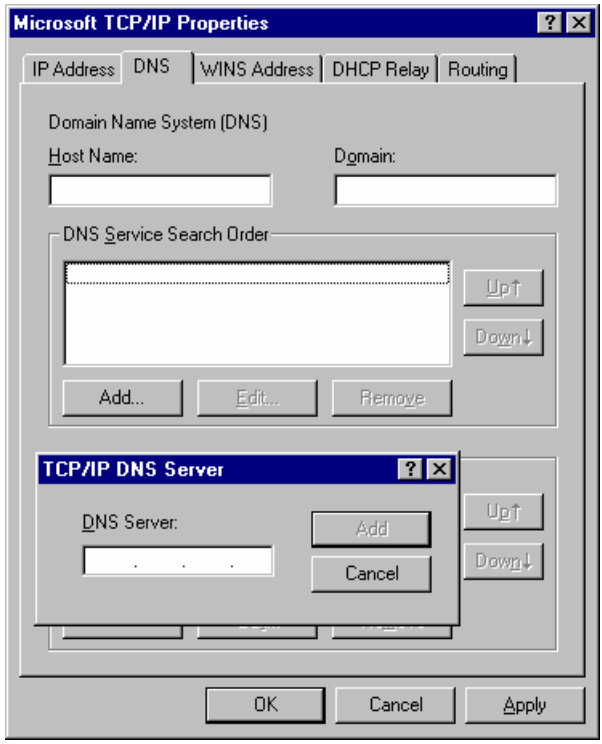

Figure 20: Windows NT4.0 - DNS

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:

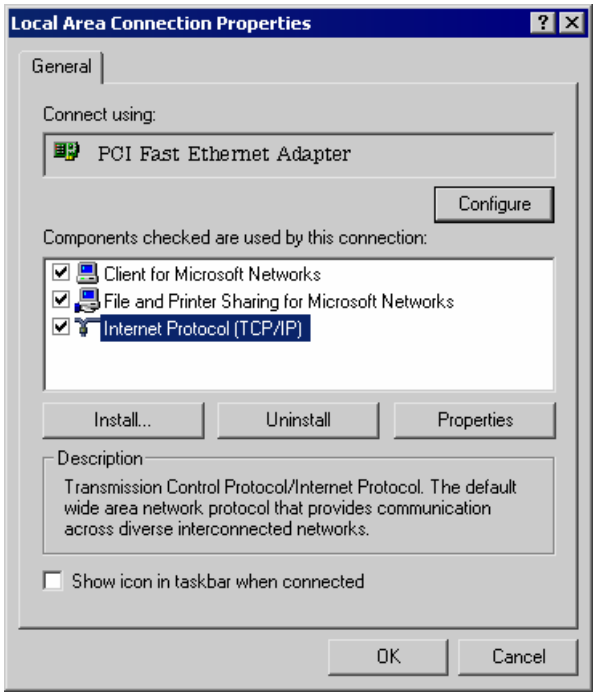

Figure 21: Network Configuration (Win 2000)

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.

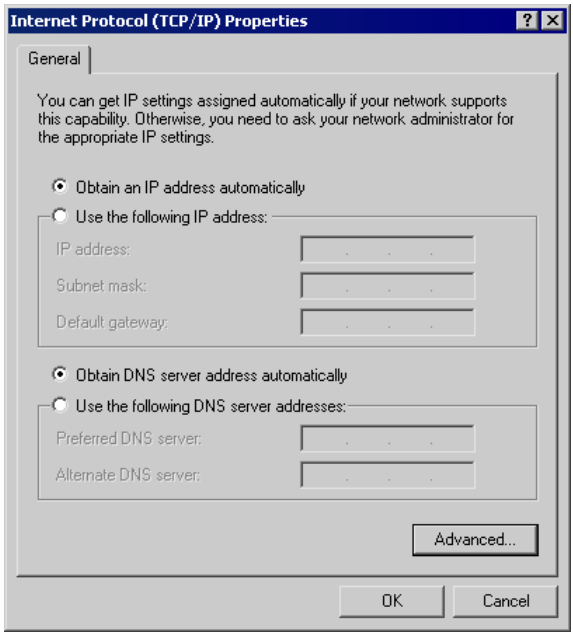

Figure 22: TCP/IP Properties (Win 2000)

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 802.11g ADSL VoIP Gateway will act as a DHCP Server.

Restart your PC to ensure it obtains an IP Address from the 802.11g ADSL VoIP Gateway.

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 802.11g ADSL VoIP Gateway'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 802.11g ADSL VoIP Gateway.)
- 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:

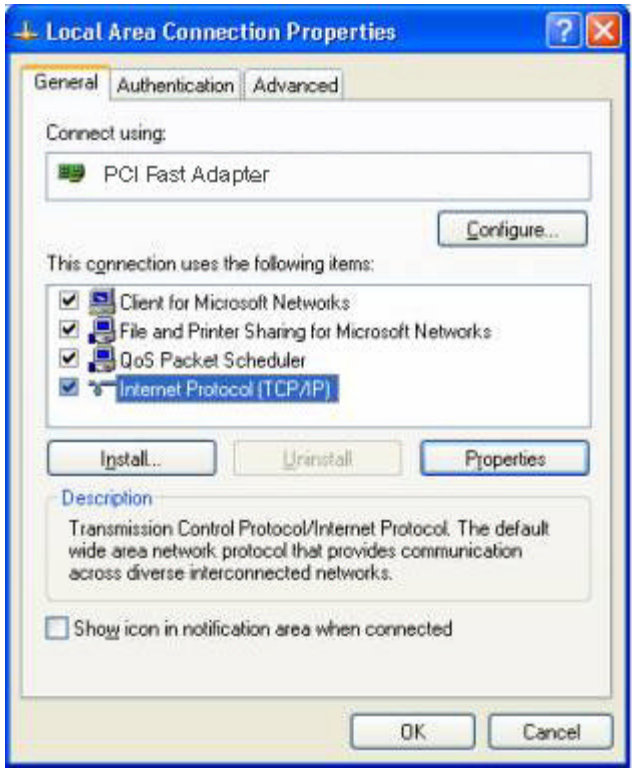

Figure 23: Network Configuration (Windows XP)

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.

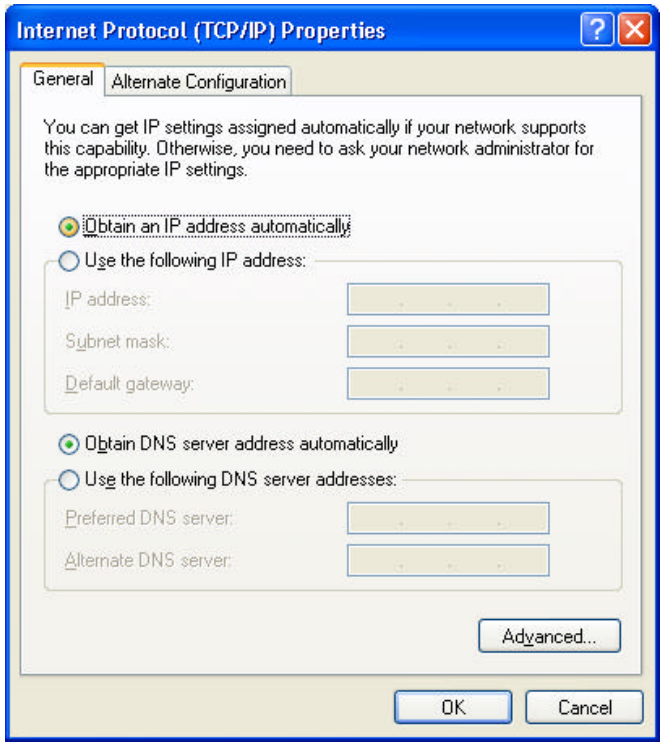

Figure 24: TCP/IP Properties (Windows XP)

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 802.11g ADSL VoIP Gateway will act as a DHCP Server.

Restart your PC to ensure it obtains an IP Address from the 802.11g ADSL VoIP Gateway.

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 802.11g ADSL VoIP Gateway's IP address and click *OK*. Your LAN administrator can advise you of the IP Address they assigned to the 802.11g ADSL VoIP Gateway.
- 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 802.11g ADSL VoIP Gateway for Internet access:

- Ensure that the Internet 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 98/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 802.11g ADSL VoIP Gateway, 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 "802.11g ADSL VoIP Gateway".
- 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 "802.11g ADSL VoIP Gateway" location.

Macintosh Clients

From your Macintosh, you can access the Internet via the 802.11g ADSL VoIP Gateway. 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 802.11g ADSL VoIP Gateway's IP Address.
- Ensure your DNS settings are correct.

Linux Clients

To access the Internet via the 802.11g ADSL VoIP Gateway, it is only necessary to set the 802.11g ADSL VoIP Gateway 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 802.11g ADSL VoIP Gateway.
- 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 802.11g ADSL VoIP Gateway:

- Ensure the "Gateway" field for your network card is set to the IP Address of the 802.11g ADSL VoIP Gateway.
- Ensure your DNS (Name Server) settings are correct.

Wireless Station Configuration

This section applies to all Wireless stations wishing to use the 802.11g ADSL VoIP Gateway's Access Point, regardless of the operating system which is used on the client.

To use the Wireless Access Point in the 802.11g ADSL VoIP Gateway, 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 802.11g ADSL VoIP Gateway. The default value is **`Wireless`**. **Note! The SSID is case sensitive.**
Wireless Security	By default, Wireless security on the 802.11g ADSL VoIP Gateway is disabled. • If Wireless security remains disabled on the 802.11g ADSL VoIP Gateway, all stations must have wireless security disabled. • If Wireless security is enabled on the Wireless VoIP Gateway (either WEP or WPA-PSK), each station must use the same settings as the Wireless ADLS VoIP Gateway.

Wireless Configuration on Windows XP

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

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

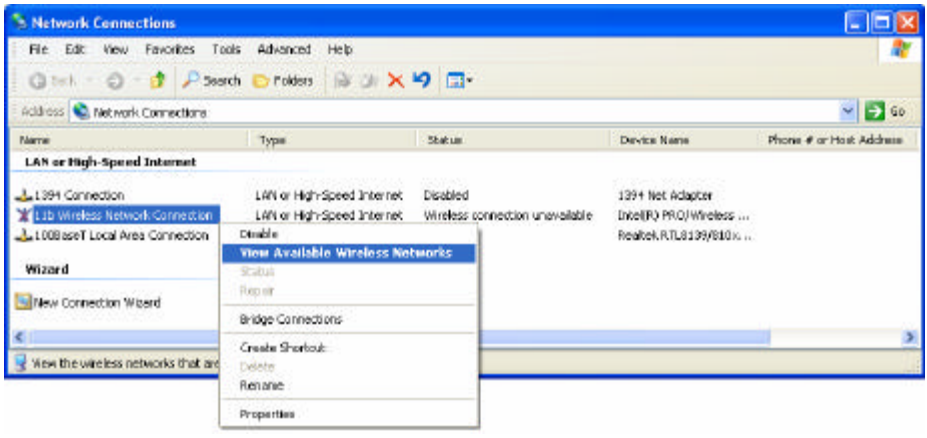

Figure 25: Network Connections (Windows XP)

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

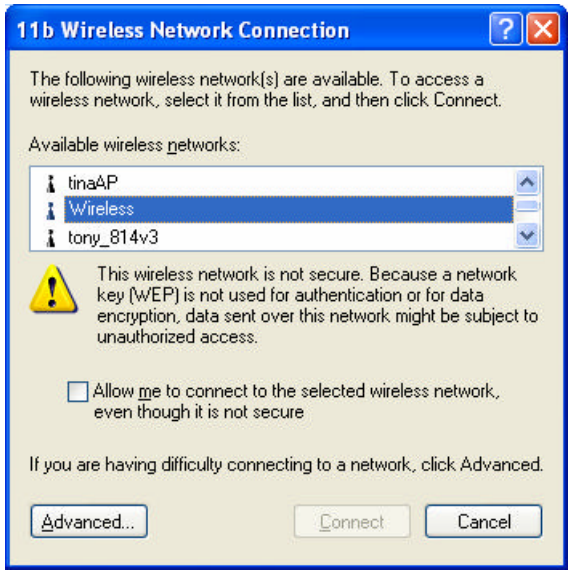

Figure 26 Wireless Networks (Windows XP)

If the "Broadcast SSID" setting on the 802.11g ADSL VoIP Gateway has been disabled, its SSID will NOT be listed. See the following section "If the SSID is not listed" for details of dealing with this situation.

4. The next step depends on whether or not Wireless security has been enabled on the 802.11g ADSL VoIP Gateway.

If Wireless Security is Disabled

If Wireless security on the 802.11g ADSL VoIP Gateway is disabled, Windows will warn you that the Wireless network is not secure.

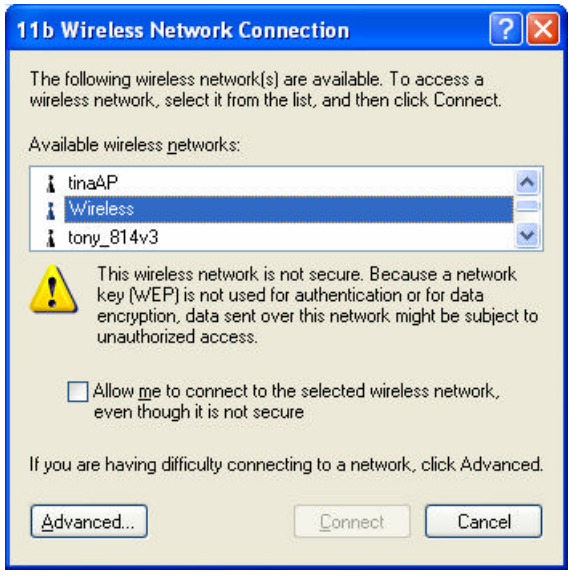

Figure 27 Insecure Wireless Network (Windows XP)

To connect:

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

If using WEP Data Encryption

If WEP data encryption has been enabled on the 802.11g ADSL VoIP Gateway, Windows will detect this, and show a screen like the following.

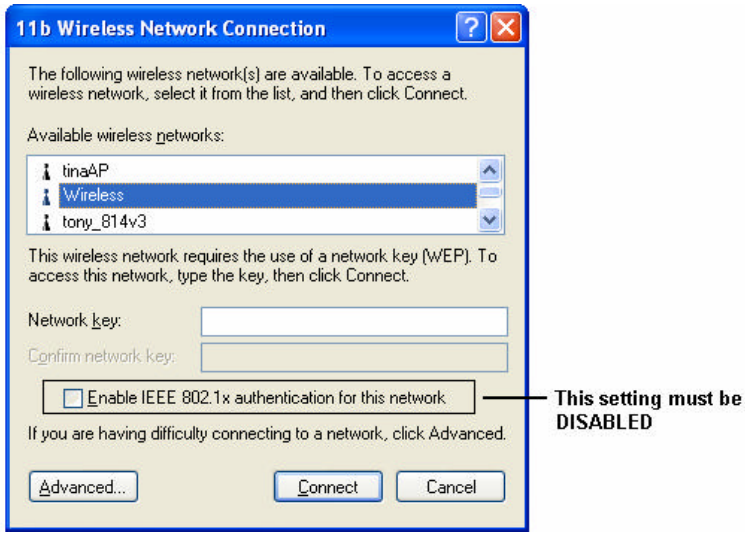

Figure 28: WEP (Windows XP)

To connect:

- Enter the WEP key, as set on the 802.11g ADSL VoIP Gateway, in the *Network Key* field.
- Re-enter the WEP key into the *Confirm Network key* field.
- **Disable** the checkbox *Enable IEEE 802.1x authentication for this network*.
- Click the *Connect* button.

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

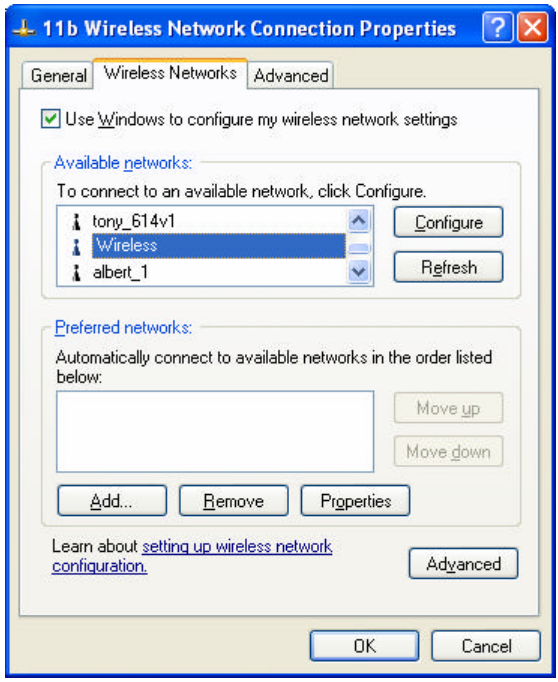

Figure 29: Advanced - Wireless Networks

Select the SSID for the 802.11g ADSL VoIP Gateway, and click *Configure*, to see a screen like the following:

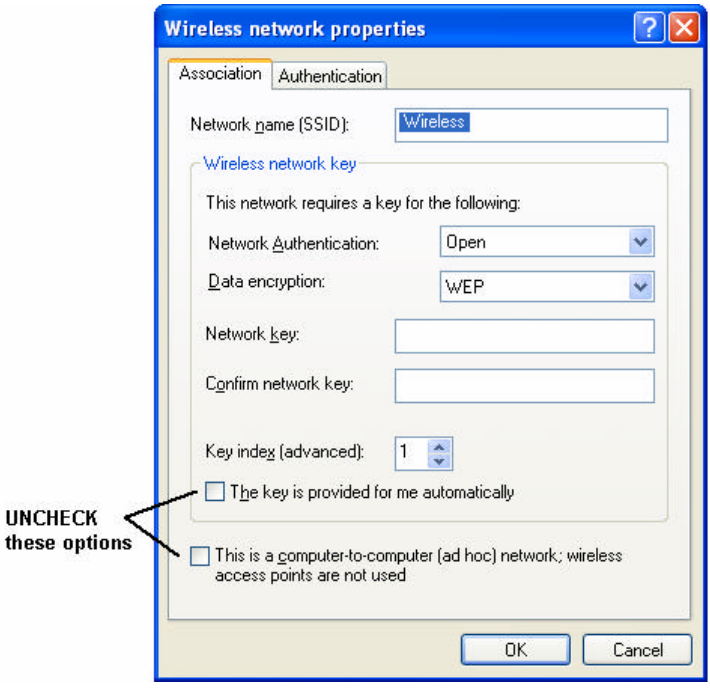

Figure 30: Wireless Network Properties - WEP

Configure this screen as follows:

- Set *Network Authentication* to match the 802.11g ADSL VoIP Gateway. (If the setting on the 802.11g ADSL VoIP Gateway is "Auto", then either *Open* or *Shared* can be used.)
- For *Data Encryption*, select **WEP**.

- For the *Network key* and *Confirm network key*, enter the **default key value** used on the 802.11g ADSL VoIP Gateway. (Windows will determine if 64bit or 128bit encryption is used.)
- The *Key index* must match the **default key index** on the 802.11g ADSL VoIP Gateway. The default value is 1.
- Ensure the options *The key is provided for me automatically* and *This is a computer-to-computer (ad hoc) network* are unchecked.
- Click OK to save and close this dialog.
- This wireless network will now be listed in *Preferred Networks* on the screen below.

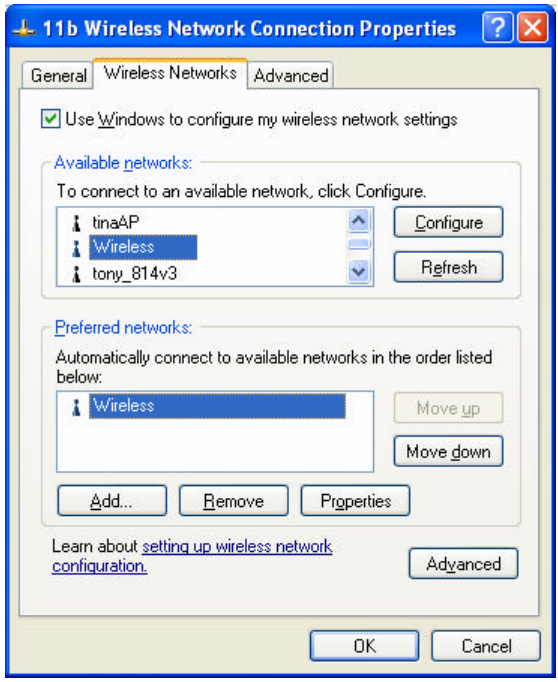

Figure 31: Preferred Networks

Click OK to establish a connection to the 802.11g ADSL VoIP Gateway.

If using WPA-PSK Data Encryption

If WPA-PSK data encryption has been enabled on the 802.11g ADSL VoIP Gateway, it does not matter which network is selected on the screen below. Just click the *Advanced* button.

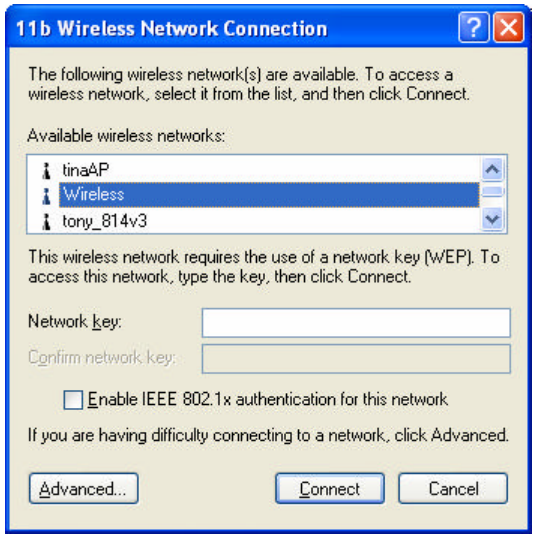

Figure 32: Wireless Networks (Windows XP)

You will then see a screen like the example below.

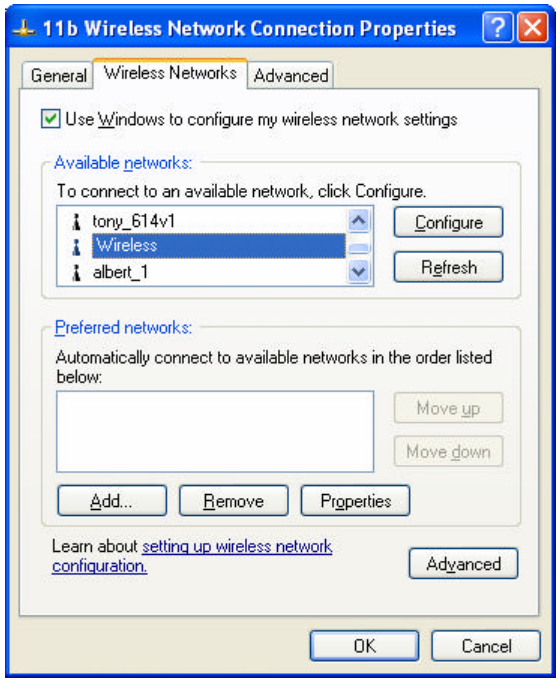

Figure 33: Advanced - Wireless Networks

Select the SSID for the 802.11g ADSL VoIP Gateway, and click *Configure*, to see a screen like the following:

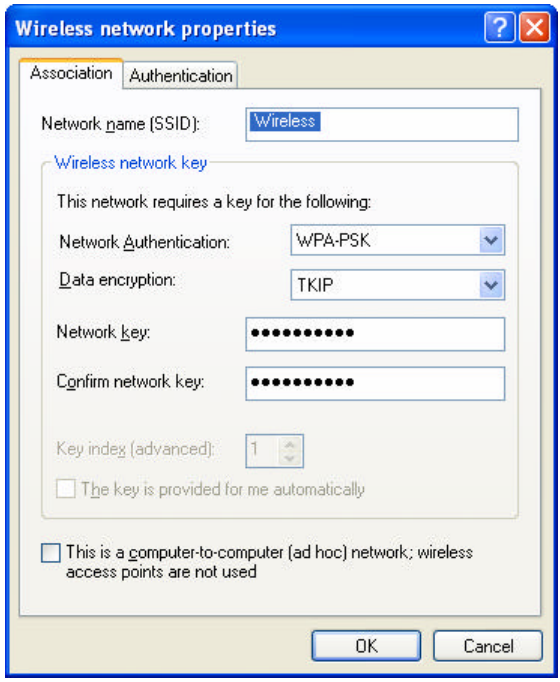

Figure 34: Wireless Network Properties- WPA-PSK

Configure this screen as follows:

- Set *Network Authentication* to **WPA-PSK**.
- For *Data Encryption*, select **TKIP**.
- For the *Network key* and *Confirm network key*, enter the network key (PSK) used on the 802.11g ADSL VoIP Gateway.
- Ensure the option *This is a computer-to-computer (ad hoc) network* is unchecked.
- Click OK to save and close this dialog.
- This wireless network will now be listed in *Preferred Networks* on the screen below.

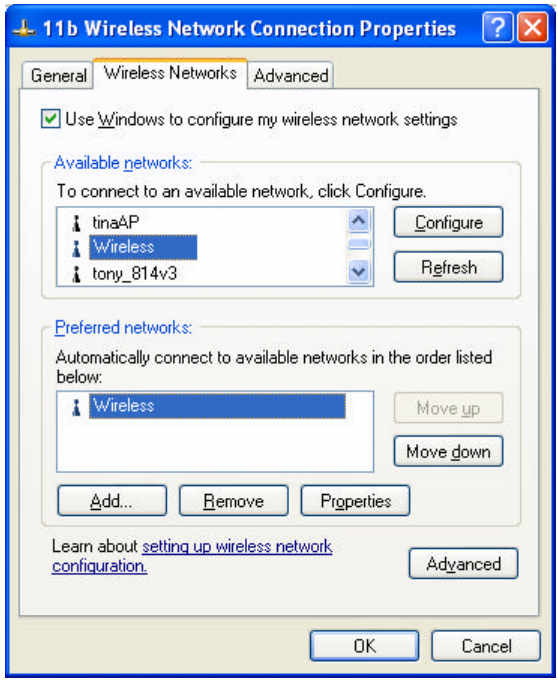

Figure 35: Preferred Networks

Click OK to establish a connection to the 802.11g ADSL VoIP Gateway.

If the SSID is not listed

If the "Broadcast SSID" setting on the 802.11g ADSL VoIP Gateway has been disabled, its SSID will NOT be listed on the screen below.

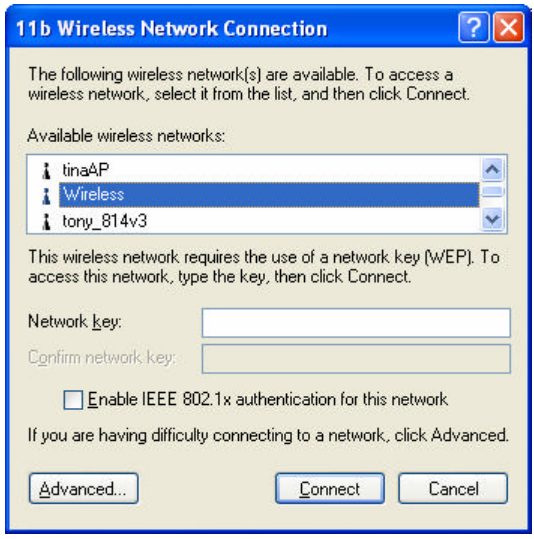

Figure 36: Wireless Networks (Windows XP)

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

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

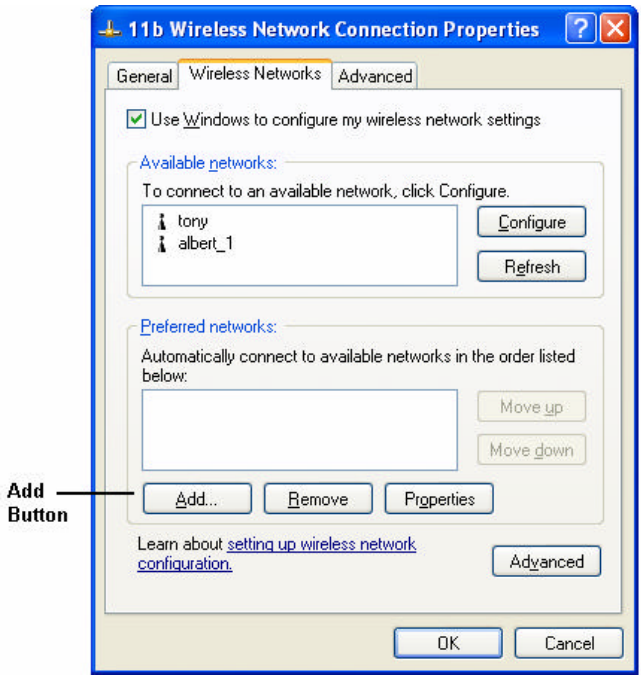

Figure 37: Unlisted Wireless Network

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

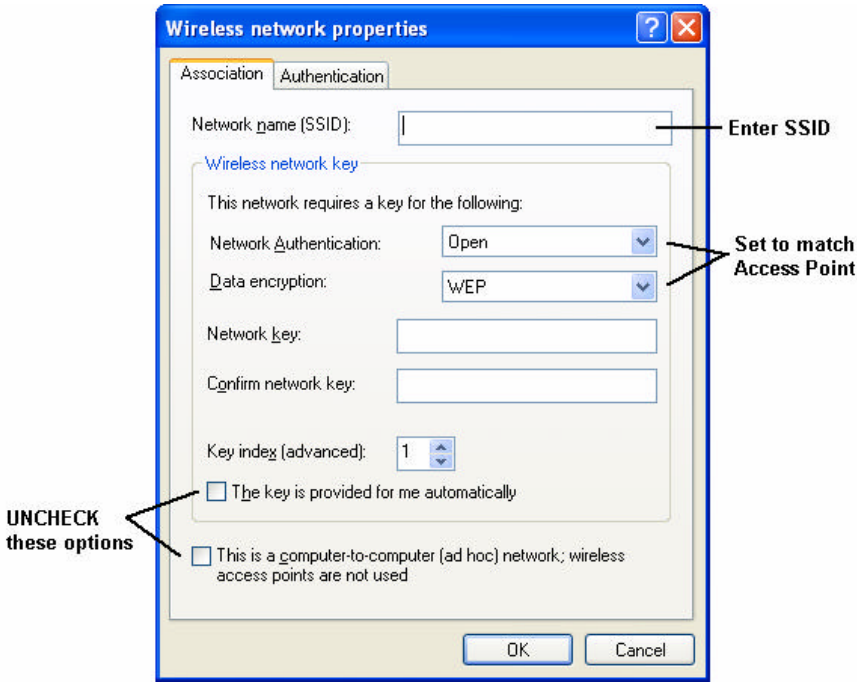

Figure 38: Add Wireless Network

3. Configure this screen as follows:
   - Enter the correct SSID, as used on the 802.11g ADSL VoIP Gateway. Remember the SSID is case-sensitive, so be sure to match the case, not just the spelling.

- Set *Network Authentication* and *Data Encryption* to match the 802.11g ADSL VoIP Gateway.
- If using data encryption (WEP or WPA-PSK), enter the key used on the 802.11g ADSL VoIP Gateway. See the preceding sections for details of WEP and WPA-PSK.
- Uncheck the options *The key is provided for me automatically* and *This is a computer-to-computer (ad hoc) network*.
- Click OK to save and exit.

4. This wireless network will then be listed in *Preferred Networks* on the screen below.

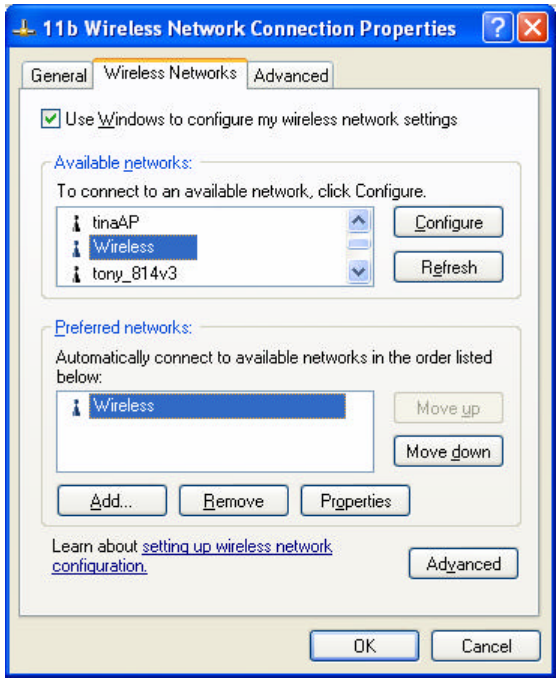

Figure 39: Preferred Networks

5. Click OK to establish a connection to the 802.11g ADSL VoIP Gateway.

Chapter 5
Advanced Features

5

This Chapter explains when and how to use the 802.11g ADSL VoIP Gateway's "Advanced" Features.

Overview

The following advanced features are provided:

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

Internet

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

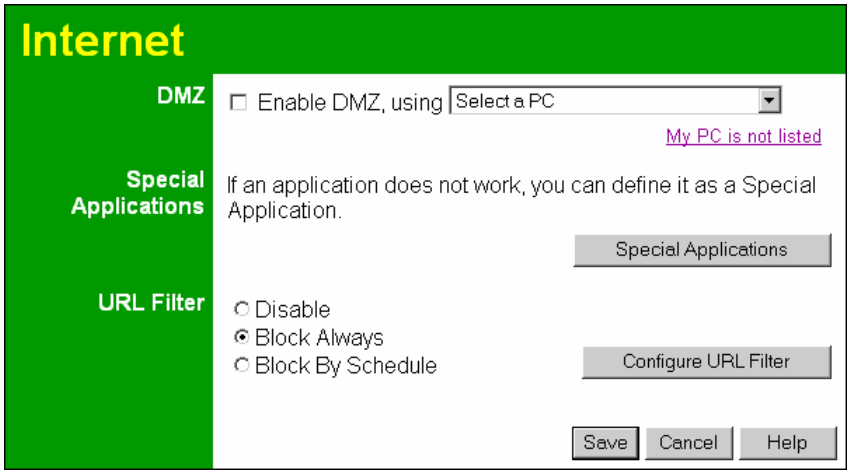

Figure 40: Internet Screen

DMZ

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

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

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

Special Applications

If you use Internet applications which use non-standard connections or port numbers, you may find that they do not function correctly because they are blocked by the 802.11g ADSL VoIP Gateway's firewall. In this case, you can define the application as a "Special Application".

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

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

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

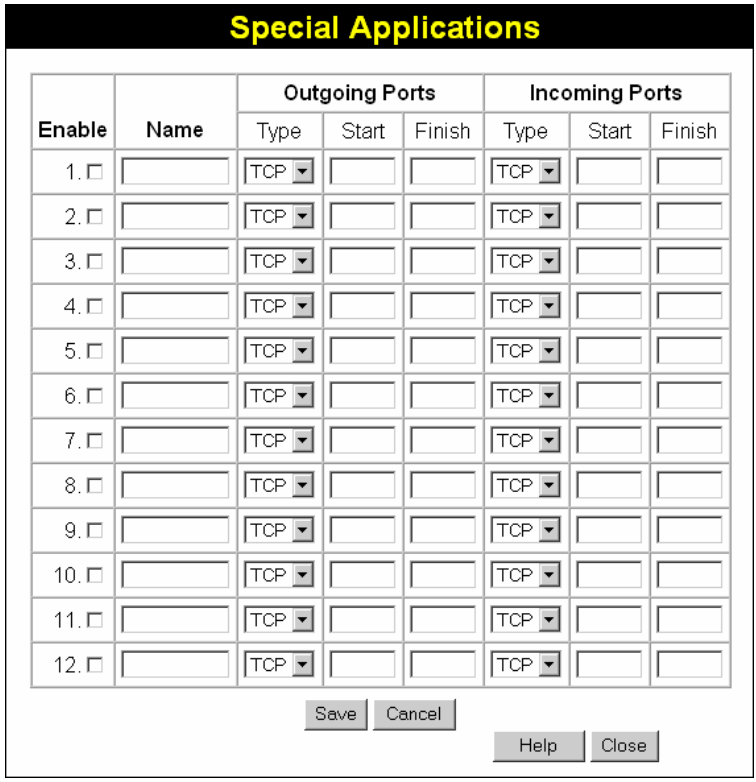

Figure 41: Special Applications Screen

Data - Special Applications Screen

Checkbox	Use this to Enable or Disable this Special Application as required.
Name	Enter a descriptive name to identify this Special Application.
Incoming Ports	• **Type** - Select the protocol (TCP or UDP) used when you receive data from the special application or service. (Note: Some applications use different protocols for outgoing and incoming data). • **Start** - Enter the beginning of the range of port numbers used by the application server, for data you receive. If the application uses a single port number, enter it in both the "Start" and "Finish" fields. • **Finish** - Enter the end of the range of port numbers used by the application server, for data you receive.
Outgoing Ports	• **Type** - Select the protocol (TCP or UDP) used when you send data to the remote system or service. • **Start** - Enter the beginning of the range of port numbers used by the application server, for data you send to it. If the application uses a single port number, enter it in both the "Start" and "Finish" fields. • **Finish** - Enter the end of the range of port numbers used by the application server, for data you send to it. If the application uses a single port number, enter it in both the "Start" and "Finish" fields.

Using a Special Application

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

URL Filter

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

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

- **Disable** - disable this feature.
- **Block 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.

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

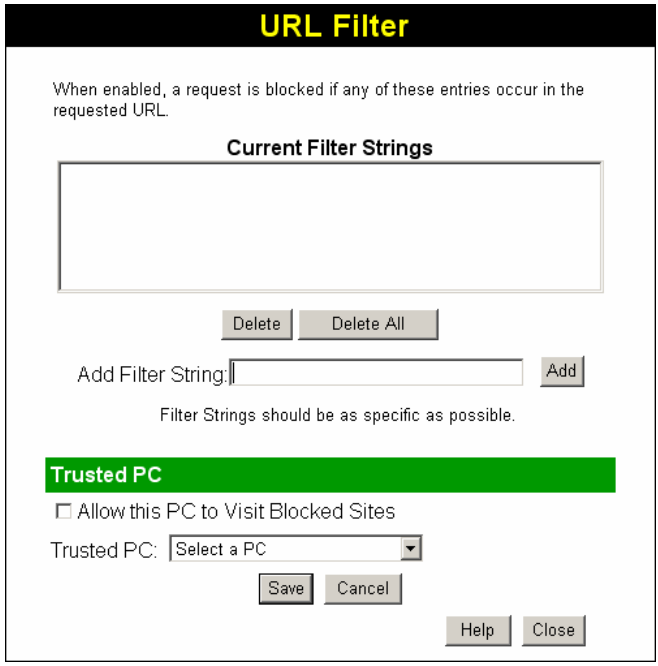

Figure 42: URL Filter Screen

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.

DDNS Services work as follows:

1. You must register for the service at one of the listed DDNS Service providers.
2. After registration, use the Service provider's normal procedure to obtain your desired Domain name.
3. Enter your DDNS data on the 802.11g ADSL VoIP Gateway's DDNS screen, and enable the DDNS feature.
4. The 802.11g ADSL VoIP Gateway will then automatically ensure that your current IP Address is recorded at the DDNS service provider's Domain Name Server.
5. From the Internet, users will be able to connect to your Virtual Servers (or DMZ PC) using your Domain name, as shown on this screen.

Dynamic DNS Screen

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

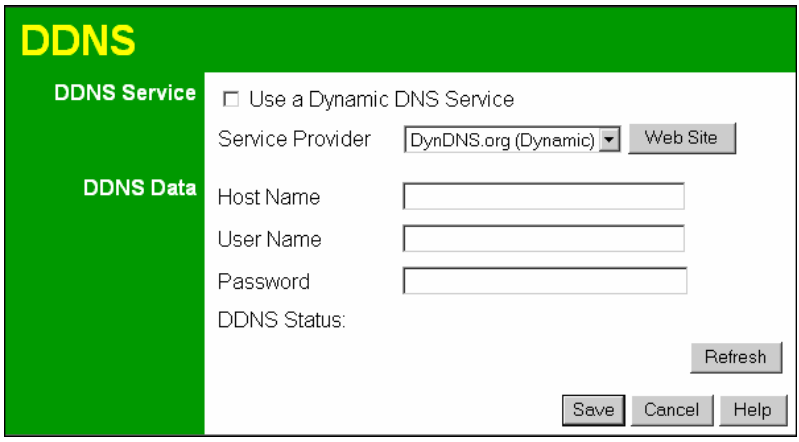

Figure 43: DDNS Screen

Data - Dynamic DNS Screen

DDNS Service	
Use a Dynamic DNS Service	Use this to enable or disable the DDNS feature as required.
Service Provider	Select the desired DDNS Service provider.
Web Site	Click this button to open a new window and connect to the Web site of the selected DDNS service provider.
DDNS Data	
Host Name	Enter the domain name allocated to you by the DDNS Service. If you have more than one name, enter the name you wish to use.

User Name	Enter your Username for the DDNS Service. (TZO.com uses your E-mail address.)
Password	Enter your current password for the DDNS Service. (TZO.com calls this a key.)
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 indicates some problem, you need to connect to the 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. "Traffic" means incoming connection attempts, not packets.

By default:

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

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

Firewall Rules Screen

An example screen is shown below.

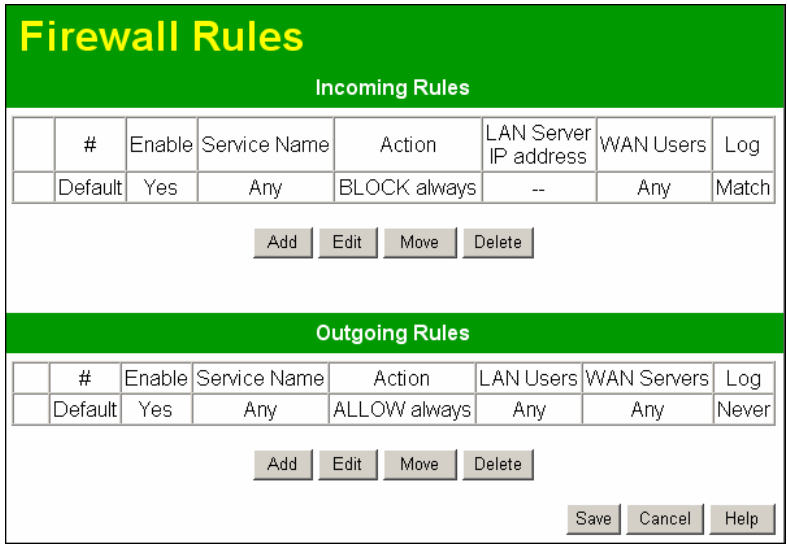

Figure 44 Firewall Screen

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 (Inbound Services)

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

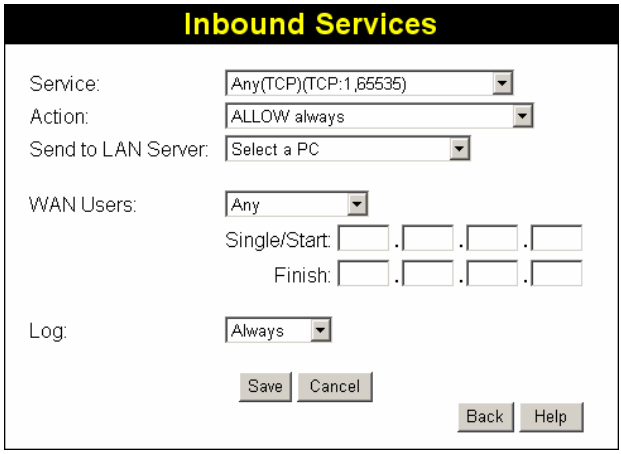

Figure 45: Inbound Services Screen

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 inbound 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 "Single/Start"