LevelOne

FBR-1430
VPN Broadband Router, 1W 4L

User Manual

V1.0

Table of Contents

CHAPTER 1 INTRODUCTION 1

VPN BROADBAND ROUTER FEATURES 1
Internet Access Features 1
Advanced Internet Functions 1
LAN Features 2
Configuration & Management 2
Security Features 2
IPSec VPN Gateway Features 2
Microsoft VPN Gateway Support 2
PACKAGE CONTENTS 3
PHYSICAL DETAILS 4
Front-mounted LEDs 4
Rear Panel 5

CHAPTER 2 INSTALLATION 6

REQUIREMENTS 6
PROCEDURE 6

CHAPTER 3 SETUP 8

OVERVIEW 8
CONFIGURATION PROGRAM 9
Preparation 9
SETUP WIZARD 11
Common Connection Types 11
Home Screen 13
LAN SCREEN 14
DHCP 15
PASSWORD 15

CHAPTER 4 PC CONFIGURATION 17

OVERVIEW 17
WINDOWS CLIENTS 17
TCP/IP Settings - Overview 17
Checking TCP/IP Settings - Windows 9x/ME: 18
Checking TCP/IP Settings - Windows 2000: 20
Checking TCP/IP Settings - Windows XP 22
Internet Access 24
MACINTOSH CLIENTS 25
LINUX CLIENTS 25
OTHER UNIX SYSTEMS 25

CHAPTER 5 OPERATION AND STATUS 26

OPERATION 26
STATUS SCREEN 26
CONNECTION STATUS - PPPOE 27
CONNECTION STATUS - PPTP 30
CONNECTION STATUS - TELSTRA BIG POND 31
CONNECTION DETAILS - SINGTEL RAS 32
CONNECTION DETAILS - FIXED/DYNAMIC IP ADDRESS 34

CHAPTER 6 INTERNET FEATURES 36

OVERVIEW 36
WAN PORT CONFIGURATION 37
ADVANCED SETUP 39
Communication Applications 40
Special Applications 40
Multi-DMZ 41

URL Filter *41*
URL Filter Screen *42*
DYNAMIC DNS (DOMAIN NAME SERVER) 43
Dynamic DNS Screen *43*
VIRTUAL SERVERS 45
IP Address seen by Internet Users *45*
Virtual Servers Screen *45*
Defining your own Virtual Servers *46*
Connecting to the Virtual Servers *46*
OPTIONS 47

CHAPTER 7 SECURITY CONFIGURATION 48

OVERVIEW 48
ACCESS CONTROL 49
Access Control Screen *49*
Group Members Screen *51*
Access Control Log *51*
FIREWALL RULES 52
Firewall Rules Screen *52*
Define Firewall Rule *54*
LOGS 56
E-MAIL 58
SECURITY OPTIONS 60
SCHEDULING 62
Define Schedule Screen *62*
SERVICES 63

CHAPTER 8 VPN (IPSEC) 64

OVERVIEW 64
IPSec *64*
IKE *64*
Policies *64*
VPN Configuration *65*
COMMON VPN SITUATIONS 65
VPN Pass-through *65*
Client PC to VPN Gateway *66*
Connecting 2 LANs via VPN *66*
VPN CONFIGURATION 67
VPN Policies Screen *67*
Adding a New Policy *68*
VPN EXAMPLES 77
Example 1: Connecting 2 VPN Broadband Routers *77*
Example 2: Windows 2000/XP Client to LAN *79*
Example 3: Windows 2000 Server to VPN Gateway *92*
CERTIFICATES 95
Trusted Certificates *95*
Requesting a Trusted Certificate *95*
Self Certificates *96*
Requesting a Self Certificate *97*
CRLS 99
STATUS 100

CHAPTER 9 MICROSOFT VPN 102

OVERVIEW 102
SERVER SETUP 102
CLIENT DATABASE 103
STATUS SCREEN 105
WINDOWS CLIENT SETUP 106
Windows 98/ME *106*
Windows 2000 ..... *108*
Windows XP *111*

CHAPTER 10 OTHER FEATURES & SETTINGS 114

OVERVIEW 114
CONFIG FILE 115
NETWORK DIAGNOSTICS 116
PC DATABASE 117
PC Database Screen 117
PC Database (Admin) 119
REMOTE ADMINISTRATION 121
ROUTING 123
Overview 123
Routing Screen 123
Configuring Other Routers on your LAN 125
Static Routing - Example 126
UPGRADE FIRMWARE 128
UPNP 129

APPENDIX A TROUBLESHOOTING 130

OVERVIEW 130
GENERAL PROBLEMS 130
INTERNET ACCESS 130

APPENDIX B SPECIFICATIONS 132

VPN BROADBAND ROUTER 132
FCC STATEMENT 132
FCC Radiation Exposure Statement 132
CE MARKING WARNING 133

Chapter 1
Introduction

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

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

- ***Shared Broadband Internet Access*** for all LAN users.
- ***VPN Gateway*** for IPSec, PPTP VPN connections to remote PCs or sites.
- ***4-Port Switching Hub*** for 10BaseT or 100BaseT connections.

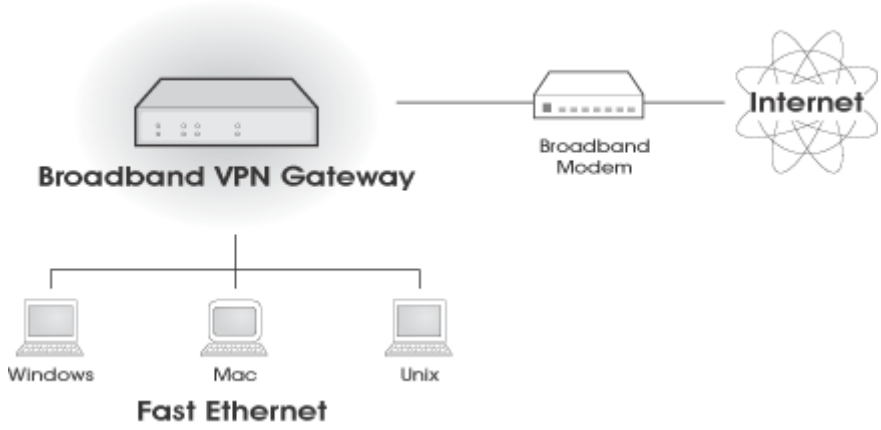

Figure 1: VPN Broadband Router

VPN Broadband Router Features

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

Advanced Internet Functions

- ***Communication Applications.*** Support for Internet communication applications, such as interactive Games, Telephony, and Conferencing applications, which are often difficult to use when behind a Firewall, is included.
- ***Special Internet Applications.*** Applications which use non-standard connections or port numbers are normally blocked by the Firewall. The ability to define and allow such applications is provided, to enable such applications to be used normally.
- ***Virtual Servers.*** This feature allows Internet users to access Internet servers on your LAN. The required setup is quick and easy.

- ***Multi-DMZ.*** For each WAN (Internet) IP address allocated to you, one (1) PC on your local LAN can be configured to allow unrestricted 2-way communication with Servers or individual users on the Internet. This provides the ability to run programs which are incompatible with Firewalls.
- ***URL Filter.*** Use the URL Filter to block access to undesirable Web sites by LAN users.
- ***Internet Access Log.*** See which Internet connections have been made.
- ***VPN Pass through Support.*** PCs with VPN (Virtual Private Networking) software using PPTP, L2TP and IPSec are transparently supported - no configuration is required.

LAN Features

- ***4-Port Switching Hub.*** The VPN Broadband 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 VPN Broadband Router can act as a **DHCP Server** for devices on your local LAN and WLAN.
- ***Multi Segment LAN Support.*** LANs containing one or more segments are supported; via the VPN Broadband Router's RIP (Routing Information Protocol) support and built-in static routing table.

Configuration & Management

- ***Easy Setup.*** Use your WEB browser from anywhere on the LAN or WLAN for configuration.
- ***Remote Management.*** The VPN Broadband Router can be managed from any PC on your LAN. And, if the Internet connection exists, it can also (optionally) be configured via the Internet.
- ***UPnP Support.*** UPnP (Universal Plug and Play) allows automatic discovery and configuration of the VPN Broadband Router. UPnP is by supported by Windows ME, XP, or later.
- ***Configuration File Backup & Restore.*** You can backup (download) the VPN Broadband Router's configuration file to your PC, and restore (upload) a previously-saved configuration file to the VPN Broadband Router.

Security Features

- ***Password - protected Configuration***. Optional password protection is provided to prevent unauthorized users from modifying the configuration data and settings.
- ***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 VPN Broadband Router.
- ***Stateful Inspection Firewall.*** All incoming data packets are monitored and all incoming server requests are filtered, thus protecting your network from malicious attacks from external sources.
- ***Protection against DoS attacks.*** DoS (Denial of Service) attacks can flood your Internet connection with invalid packets and connection requests, using so much bandwidth and so many resources that Internet access becomes unavailable. The VPN Broadband Router incorporates protection against DoS attacks.
- ***Rule-based Policy Firewall.*** To provide additional protection against malicious packets, you can define your own firewall rules. This can also be used to control the Internet services available to LAN users.

IPSec VPN Gateway Features

- ***IPSec.*** Support for IPSec standards, including IKE and certificates.
- ***10 Tunnels.*** Up to 10 VPN tunnels can be created.
- ***High performance.*** High performance encryption engine maintains high throughput even when using 3DES.

Microsoft VPN Gateway Support

- ***PPTP Server.*** The VPN Broadband Router emulates a Microsoft PPTP VPN Server, allowing clients to use the Microsoft VPN client provided in Windows.
- ***Windows Client Support.*** Remote users can use the Microsoft VPN client (VPN Adapter) provided in recent versions of Windows.
- ***Easy Setup.*** For both the Administrator and remote users, the Microsoft VPN is much easier to configure than IPSec VPN.

Package Contents

The following items should be included:

- FBR-1430
- Power Adapter
- Quick Installation Guide
- CD 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

Power **On** - Power on.

Off - No power.

Status (Red) **On** - Error condition.

Off - Normal operation.

Blinking - This LED blinks during start up.

LAN Each port has 2 LEDs

- **Link/Act**
  - **On** - Corresponding LAN (hub) port is active.
  - **Off** - No active connection on the corresponding LAN (hub) port.
  - **Flashing** - Data is being transmitted or received via the corresponding LAN (hub) port.
- **100**
  - **On** - Corresponding LAN (hub) port is using 100BaseT.
  - **Off** - Corresponding LAN (hub) port connection is using 10BaseT, or no active connection.

WAN **On** - Connection to the modem attached to the WAN (Internet) port is established.

Off - No connection to a modem on the WAN (Internet) port.

Flashing - Data is being transmitted or received via the WAN port.

Rear Panel

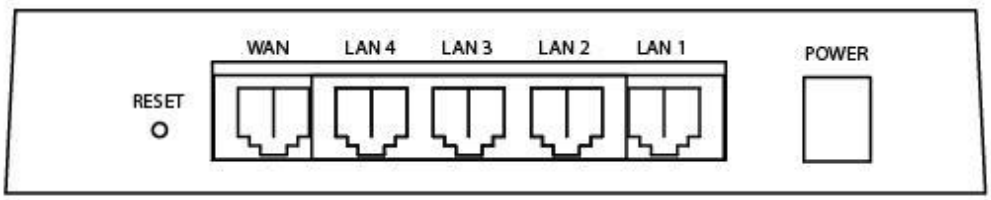

Figure 3: Rear Panel

Reset Button

This button has two (2) functions:

- **Reboot**. When pressed and released, the VPN Broadband Router will reboot (restart).
- **Clear All Data**. This button can also be used to clear ALL data and restore ALL settings to the factory default values.

To Clear All Data and restore the factory default values:

1. Power Off.
2. Hold the Reset Button down while you Power On.
3. Keep holding the Reset Button for a few seconds, until the RED LED has flashed TWICE.
4. Release the Reset Button. The VPN Broadband Router is now using the factory default values.

WAN port (10/100BaseT)

Connect the DSL or Cable Modem here. If your modem came with a cable, use the supplied cable. Otherwise, use a standard LAN cable.

10/100BaseT LAN connections

Use standard LAN cables (RJ45 connectors) to connect your PCs to these ports.

Note:

Any LAN port on the VPN Broadband 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.

Power port

Connect the supplied power adapter here.

Chapter 2
Installation

2

This Chapter covers the physical installation of the VPN Broadband Router.

Requirements

¶ Network cables. Use standard 10/100BaseT network (UTP) cables with RJ45 connectors.

¶ TCP/IP protocol must be installed on all PCs.

¶ For Internet Access, an Internet Access account with an ISP, and a Broadband modem (usually, DSL or Cable modem).

Procedure

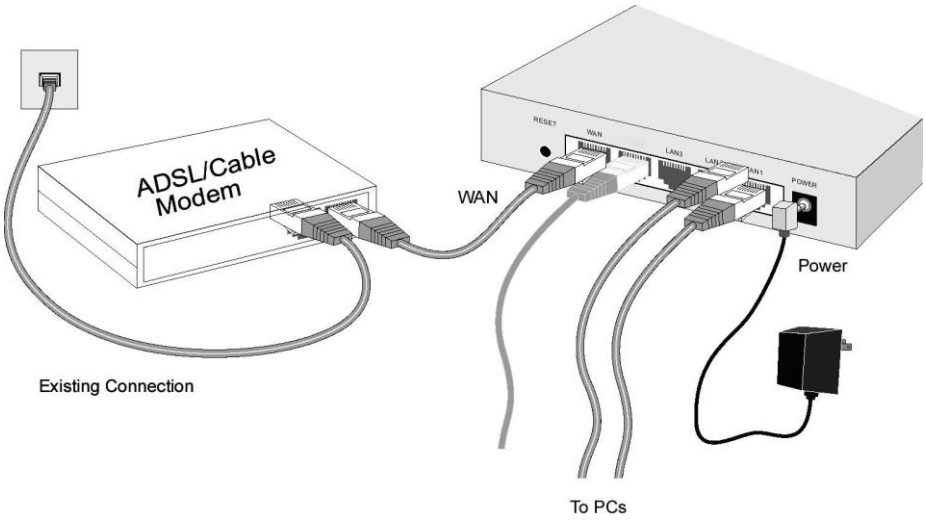

Figure 4: Installation Diagram

1. Choose an Installation Site

Select a suitable place on the network to install the VPN Broadband Router.
Ensure the VPN Broadband Router and the DSL/Cable modem are powered OFF.

2. Connect LAN Cables

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

¶ If required, you can connect any LAN port to another Hub. Any LAN port on the VPN Broadband Router will automatically function as an "Uplink" port when required. Just connect any LAN port to a normal port on the other hub, using a standard LAN cable.

3. Connect WAN Cable

Connect the Broadband modem to the WAN port on the VPN Broadband Router. Use the cable supplied with your Broadband modem. If no cable was supplied, use a standard LAN cable.

4. Power Up

¶ Power on the Broadband modem.

¶ Connect the supplied power adapter to the VPN Broadband Router and power up.
Use only the power adapter provided. Using a different one may cause hardware damage

5. Check the LEDs

- The *Power* LED should be ON.
- The *Status* LED should blink during start up, then turn Off. If it stays on, there is a hardware error.
- For each LAN (PC) connection, the LAN *Link/Act* LED should be ON (provided the PC is also ON.)
- The *WAN* LED should be ON.

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

Chapter 3
Setup

3

This Chapter provides Setup details of the VPN Broadband Router.

Overview

This chapter describes the setup procedure for:

¶ Internet Access

¶ LAN configuration

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 VPN Broadband 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 VPN Broadband Router operation and Status.	Chapter 5: Operation and Status
Use any of the following Internet features: ¶ WAN Port ¶ Advanced Setup ¶ Dynamic DNS ¶ Virtual Servers ¶ Options	Chapter 6: Internet Features
Change any of the following Security-related settings: ¶ Admin Login ¶ Access Control ¶ Firewall Rules ¶ Logs ¶ E-mail ¶ Security Options ¶ Scheduling ¶ Services	Chapter 7: Security Configuration
Use the IPSec VPN features: ¶ VPN Policies ¶ Certificates ¶ CRLs ¶ VPN Status	Chapter 8: VPN (IPSec)
Use the Microsoft VPN feature: ¶ PPTP Server in the VPN Broadband Router. ¶ User and Client setup. ¶ Checking VPN connection Status.	Chapter 9: Microsoft VPN

Configure or use any of the following: ¶ Configuration File backup and restore. ¶ Network Diagnostic ¶ PC Database ¶ Remote Administration ¶ Routing ¶ Upgrade Firmware ¶ UPnP	Chapter 9: Other Features and Settings

Where use of a certain feature requires that PCs or other LAN devices be configured, this is also explained in the relevant chapter.

Configuration Program

The VPN Broadband 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

¶ Internet Explorer V4 or later

Preparation

Before attempting to configure the VPN Broadband Router, please ensure that:

¶ Your PC can establish a physical connection to the VPN Broadband Router. The PC and the VPN Broadband Router must be directly connected (using the Hub ports on the VPN Broadband Router) or on the same LAN segment.

¶ The VPN Broadband Router must be installed and powered ON.

¶ If the VPN Broadband Router's default IP Address (192.168.0.1) is already used by another device, the other device must be turned OFF until the VPN Broadband Router is allocated a new IP Address during configuration.

Using UPnP

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

¶ Unless you intend to change the IP Address of the VPN Broadband Router, you can accept the desktop shortcut.

¶ Whether you accept the desktop shortcut or not, you can always find UPnP devices in *My Network Places* (previously called *Network Neighborhood*).

¶ Double - click the icon for the VPN Broadband Router (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 VPN Broadband Router:

1. After installing the VPN Broadband 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 VPN Broadband Router, as in this example, which uses the VPN Broadband Router 's default IP Address:

   HTTP://192.168.0.1

If you can't connect

If the VPN Broadband Router does not respond, check the following:

- The VPN Broadband 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 VPN Broadband 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 VPN Broadband 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 VPN Broadband Router are on the same network segment. (If you don't have a router, this must be the case.)

4. You will be prompted for a username and password, as shown below.

Figure 5: Password Dialog

- Enter ***admin*** for the *User Name*, and ***password*** for Password
- These are the default values. Both the name and password can (and should) be changed, using the ***Admin Login*** screen. Once you have changed either the name or the password, you must use the current values.

Setup Wizard

The first time you connect to the VPN Broadband Router, you should click the WAN Wizard to begin initial setup.

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

Common Connection Types

Cable Modems

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

DSL Modems

Type	Details	ISP Data required
Dynamic IP Address	Your IP Address is allocated automatically, when you connect to you ISP.	None.
Static (Fixed) IP Address	Your ISP allocates a permanent IP Address to you.	IP Address allocated to you, mask and gateway (if provided), and DNS address.
PPPoE	You connect to the ISP only when required. The IP address is usually allocated automatically.	User name and password.
PPTP	Mainly used in Europe. You connect to the ISP only when required. The IP address is usually allocated automatically, but may be Static (Fixed).	¶ PPTP Server IP Address. ¶ User name and password. ¶ IP Address allocated to you, if Static (Fixed).

Other Modems (e.g. Broadband Wireless)

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

Big Pond Cable (Australia)

For this connection method, the following data is required:

¶ User Name
¶ Password
¶ Big Pond Server IP address

SingTel RAS

For this connection method, the following data is required:

¶ User Name
¶ Password
¶ RAS Plan

Home Screen

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

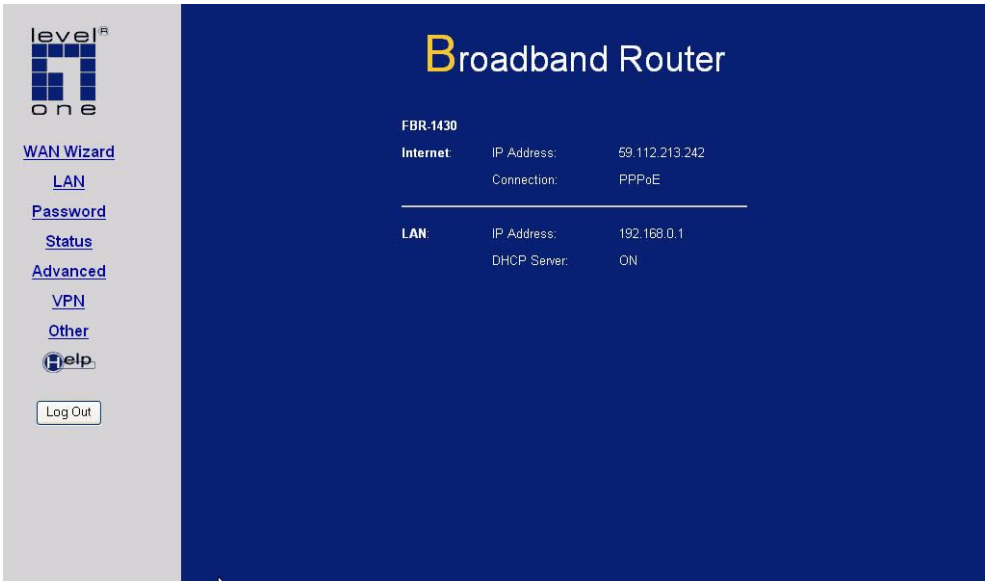

Figure 6: Home Screen

Navigation & Data Input

¶ Use the menu bar on the top 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.

From any help screen, you can access the list of all help files (help index).

LAN Screen

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

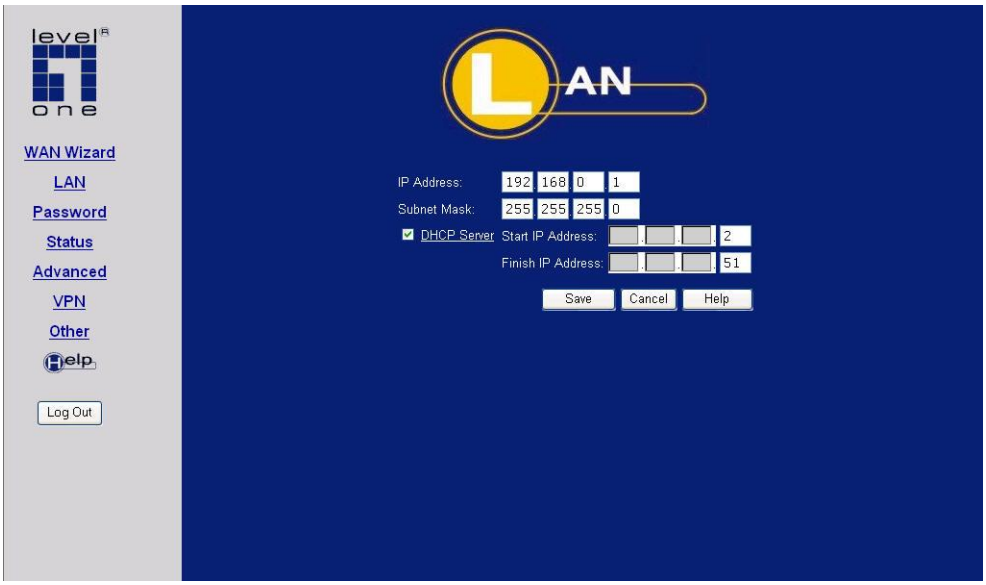

Figure 7: LAN Screen

Data - LAN Screen

TCP/IP	
IP Address	IP address for the VPN Broadband 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 VPN Broadband Router is attached (the same value as the PCs on that LAN segment).
DHCP Server	¶ If Enabled, the VPN Broadband 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 VPN Broadband 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.
Buttons	
Save	Save the data on screen.
Cancel	The "Cancel" button will discard any data you have entered and reload the file from the VPN Broadband Router.

DHCP

What DHCP Does

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

- The client request is made when the client device starts up (boots).
- The DHCP Server provides the *Gateway* and *DNS* addresses to the client, as well as allocating an IP Address.
- The VPN Broadband Router can act as a **DHCP server**.
- Windows 98SE/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 VPN Broadband 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 VPN Broadband 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 VPN Broadband Router's, the following procedure is required.

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

To Configure your PCs to use DHCP

This is the default setting for TCP/IP under Windows 98SE/ME.

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

Password

From the menu, select *Password*. This screen allows you to assign a user name and password to the VPN Broadband Router.

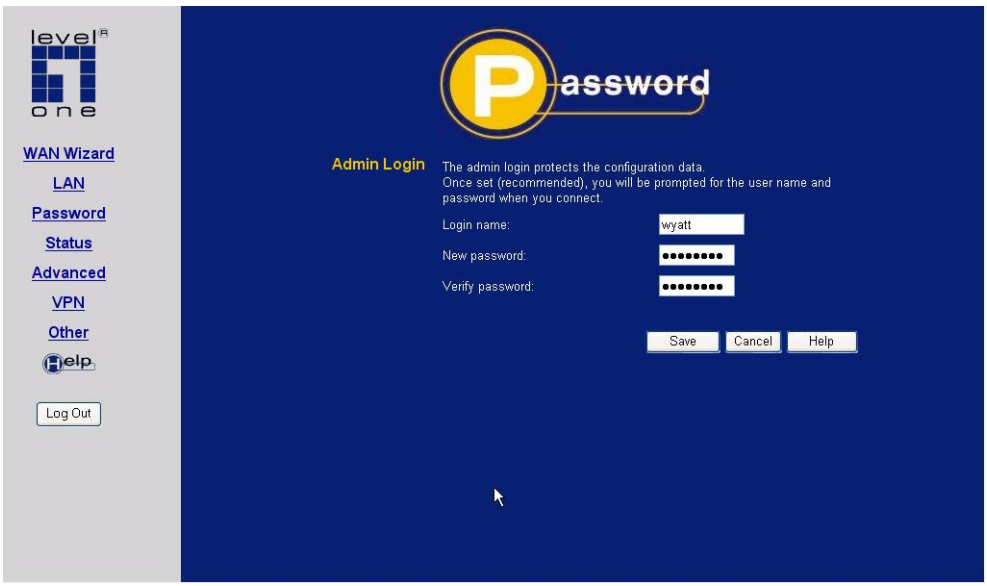

Figure 8: Password Screen

1. The default login name is "admin". Change this to the desired value.
2. The default password is ñpasswordò Enter the desired password in the *New Password* and *Verify Password* fields.
3. Save your changes.

You will see a login prompt when you connect to the VPN Broadband Router, as shown below.

Figure 9: Password Dialog

Enter the "User Name" and "Password" you set on the *Admin Login* 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

Windows Clients

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

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

The VPN Broadband 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 VPN Broadband Router settings and the default Windows TCP/IP settings, no changes need to be made.

¶ By default, the VPN Broadband 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 VPN Broadband Router

¶ The *DNS* should be set to the address provided by your ISP.

If your LAN has a Router, the LAN Administrator must re-configure the Router itself. Refer to *Chapter 8 - Other Features and Operations* for details.

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

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

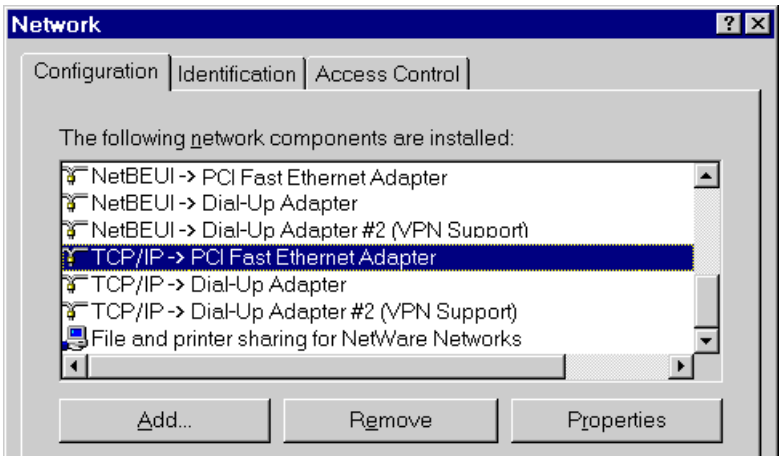

Figure 10: Network Configuration

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.

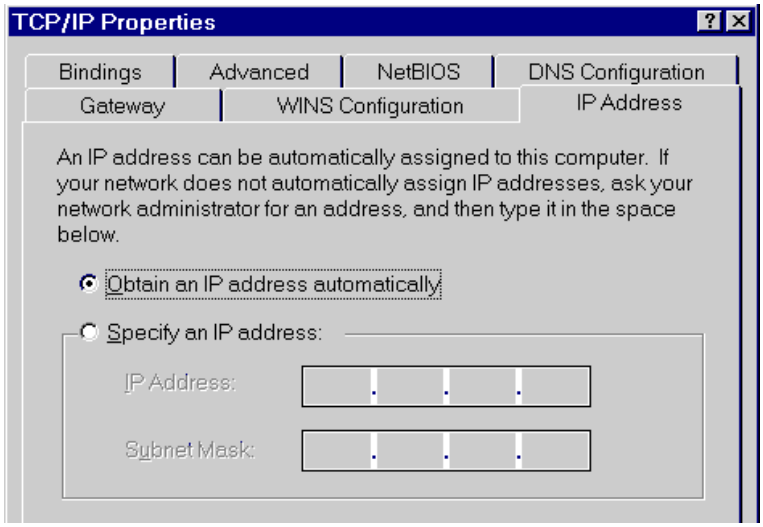

Figure 11: IP Address (Win 95)

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 VPN Broadband Router will act as a DHCP Server.

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

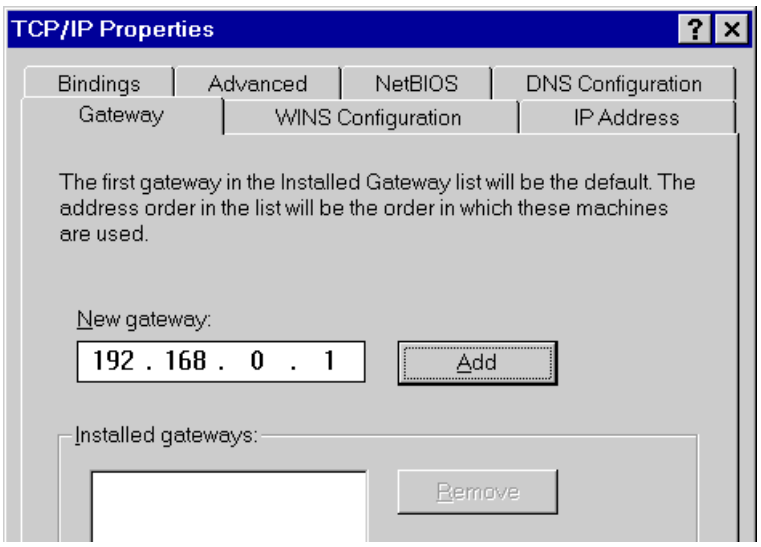

Figure 12: Gateway Tab (Win 95/98)

¶ 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*.

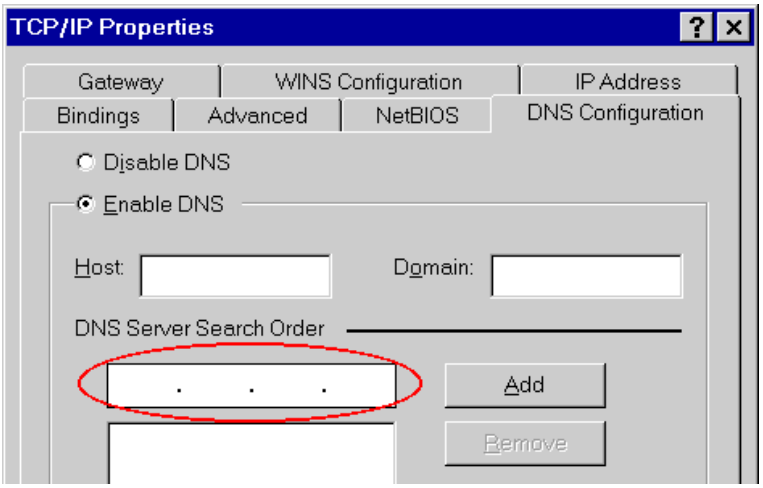

Figure 13: DNS Tab (Win 95/98)

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:

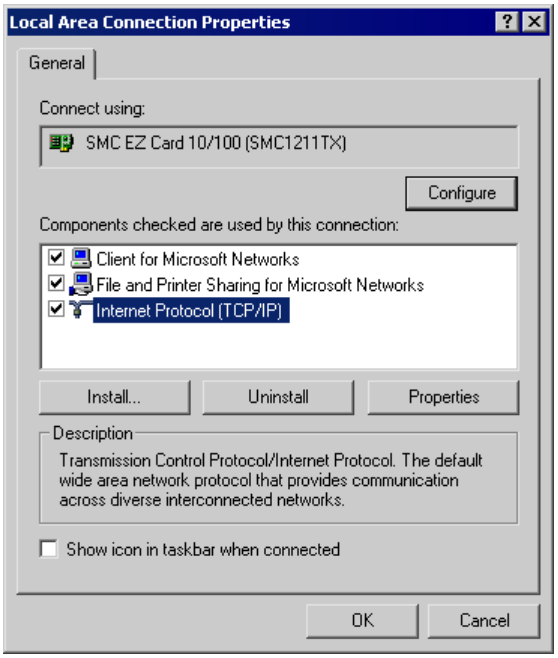

Figure 14: Network Configuration (Win 2000)

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.

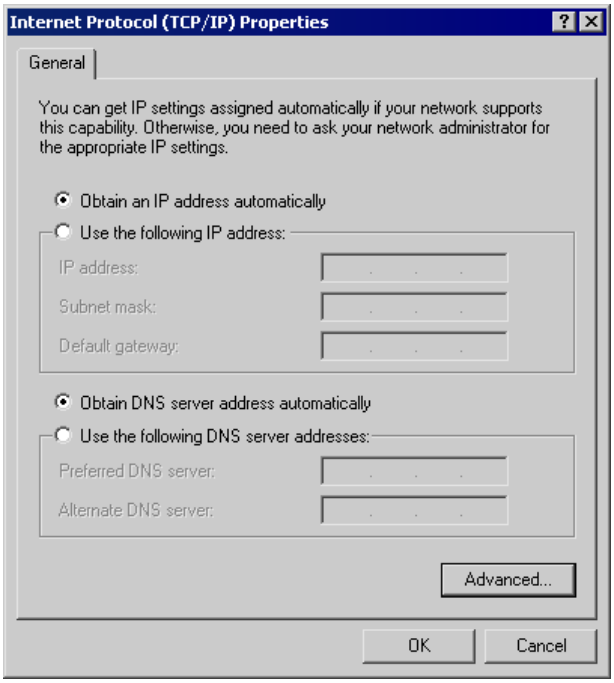

Figure 15: TCP/IP Properties (Win 2000)

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 VPN Broadband Router will act as a DHCP Server.

Restart your PC to ensure it obtains an IP Address from the VPN Broadband 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 VPN Broadband 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 VPN Broadband 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:

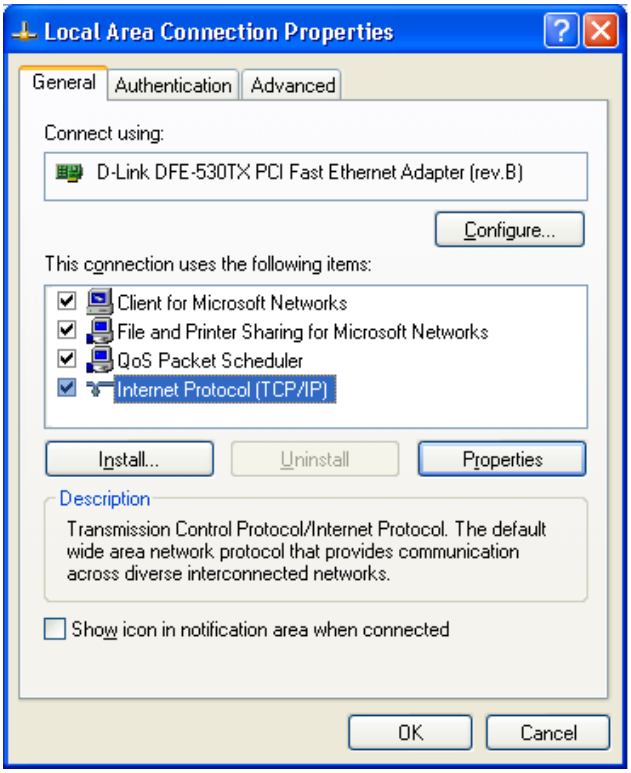

Figure 16: Network Configuration (Windows XP)

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.

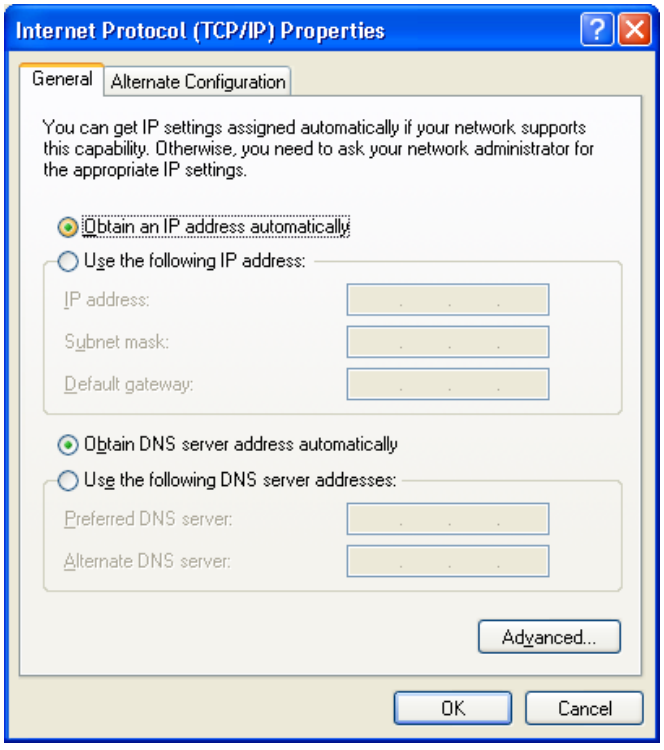

Figure 17: TCP/IP Properties (Windows XP)

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 VPN Broadband Router will act as a DHCP Server.

Restart your PC to ensure it obtains an IP Address from the VPN Broadband 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 VPN Broadband Router 's IP address and click *OK*. Your LAN administrator can advise you of the IP Address they assigned to the VPN Broadband 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 VPN Broadband 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 VPN Broadband 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 "VPN Broadband 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 "VPN Broadband Router " location.

Macintosh Clients

From your Macintosh, you can access the Internet via the VPN Broadband 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 VPN Broadband Router 's IP Address.

¶ Ensure your DNS settings are correct.

Linux Clients

To access the Internet via the VPN Broadband Router, it is only necessary to set the VPN Broadband 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 VPN Broadband 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 VPN Broadband Router:

¶ Ensure the "Gateway" field for your network card is set to the IP Address of the VPN Broadband Router.

¶ Ensure your DNS (Name Server) settings are correct.

Chapter 5
Operation and Status

5

This Chapter details the operation of the VPN Broadband Router and the status screens.

Operation

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

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

¶ If using Internet-based ***Communication Applications***, it may be necessary to specify which PC receives an incoming connection. Refer to *Chapter 6 - Internet Features* for further details.

¶ Applications which use non-standard connections or port numbers may be blocked by the VPN Broadband Router's built-in firewall. You can define such applications as ***Special Applications*** to allow them to function normally. Refer to *Chapter 6 - Internet Features* for further details.

¶ Some non-standard applications may require use of the ***DMZ*** feature. Refer to *Chapter 6 - Internet Features* for further details.

Status Screen

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

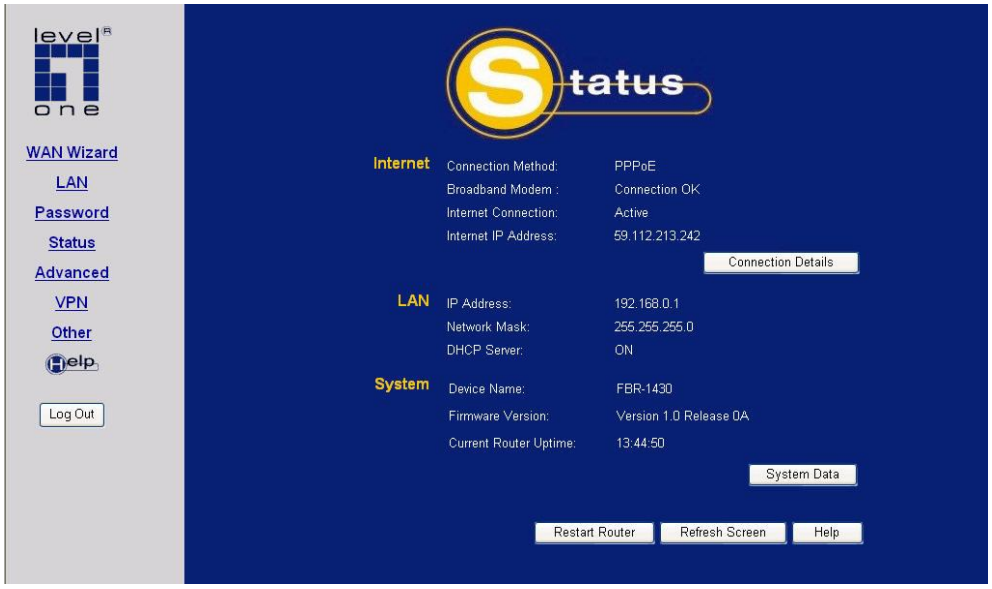

Figure 18: Status Screen

Data - Status Screen

Internet	
Connection Method	This indicates the current connection method, as set in the WAN Wizard setup.
Broadband Modem	This shows the connection status of the modem.
Internet Connection	Current connection status: ¶ Active ¶ Idle ¶ Unknown

	¶ Failed 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).
"Connection Details" Button	Click this button to open a sub-window and view a detailed description of the current connection. Depending on the type of connection, a "log" may also be available.
LAN	
IP Address	The IP Address of the VPN Broadband Router.
Network Mask	The Network Mask (Subnet Mask) for the IP Address above.
DHCP Server	This shows the status of the DHCP Server function - either "Enabled" or "Disabled". For additional information about the PCs on your LAN, and the IP addresses allocated to them, use the *PC Database* option on the *Other* menu.
System	
Device Name	This displays the current name of the VPN Broadband Router.
Firmware Version	The current version of the firmware installed in the VPN Broadband Router.
"System Data" Button	Clicking this button will open a Window which lists all system details and settings.
Buttons	
Connection Details	View the details of the current Internet connection. The sub-screen displayed will depend on the connection method used. See the following sections for details of each sub-screen.
System Data	Display all system information in a sub-window.
Restart Router	Restart (reboot) the Router. You will have to wait for the restart to be completed before continuing.
Refresh Screen	Update the data displayed on screen.

Connection Status - PPPoE

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

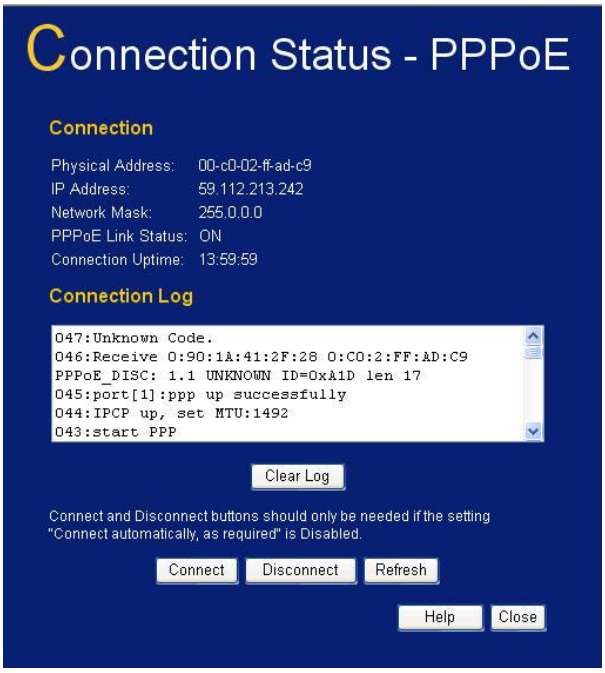

Figure 19: PPPoE Status Screen

Data - PPPoE Screen

Connection	
Physical Address	The hardware address of this device, as seen by remote devices on the Internet. (This is different to the hardware address seen by devices on the local LAN.)
IP Address	The IP Address of this device, as seen by Internet users. This address is allocated by your ISP (Internet Service Provider).
Network Mask	The Network Mask associated with the IP Address above.
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.
Connection Log	
Connection Log	¶ The Connection Log shows status messages relating to the existing connection. ¶ The most common messages are listed in the table below. ¶ The "Clear Log" button will restart the Log, while the Refresh button will update the messages shown on screen.
Buttons	
Connect	If not connected, establish a connection to your ISP.
Disconnect	If connected to your ISP, hang up the connection.
Clear Log	Delete all data currently in the Log. This will make it easier to read new messages.
Refresh	Update the data on screen.

Connection Log Messages

Message	Description
Connect on Demand	Connection attempt has been triggered by the "Connect automatically, as required" setting.
Manual connection	Connection attempt started by the "Connect" button.
Reset physical connection	Preparing line for connection attempt.
Connecting to remote server	Attempting to connect to the ISP's server.
Remote Server located	ISP's Server has responded to connection attempt.
Start PPP	Attempting to login to ISP's Server and establish a PPP connection.
PPP up successfully	Able to login to ISP's Server and establish a PPP connection.
Idle time-out reached	The connection has been idle for the time period specified in the "Idle Time-out" field. The connection will now be terminated.
Disconnecting	The current connection is being terminated, due to either the "Idle Time-out" above, or "Disconnect" button being clicked.
Error: Remote Server not found	ISP's Server did not respond. This could be a Server problem, or a problem with the link to the Server.
Error: PPP Connection failed	Unable to establish a PPP connection with the ISP's Server. This could be a login problem (name or password) or a Server problem.
Error: Connection to Server lost	The existing connection has been lost. This could be caused by a power failure, a link failure, or Server failure.
Error: Invalid or unknown packet type	The data received from the ISP's Server could not be processed. This could be caused by data corruption (from a bad link), or the Server using a protocol which is not supported by this device.

Connection Status - PPTP

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

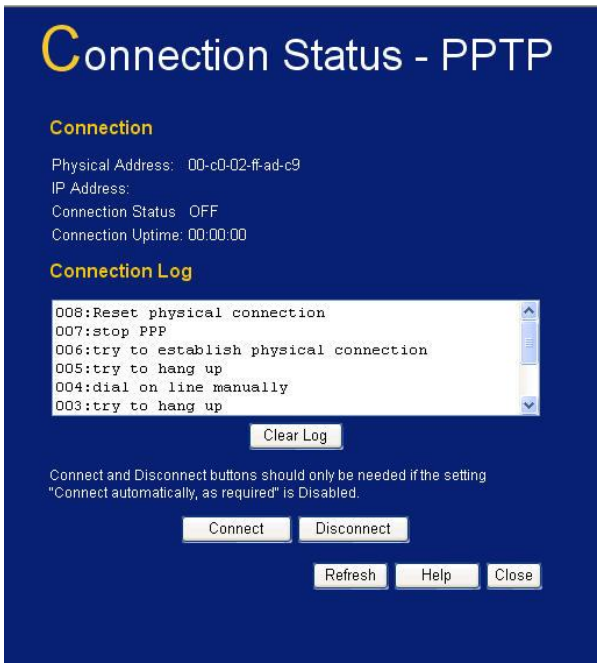

Figure 20: PPTP Status Screen

Data - PPTP Screen

Connection	
Physical Address	The hardware address of this device, as seen by remote devices on the Internet. (This is different to the hardware address seen by devices on the local LAN.)
IP Address	The IP Address of this device, as seen by Internet users. This address is allocated by your ISP (Internet Service Provider).
PPTP 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.
Connection Log	
Connection Log	¶ The Connection Log shows status messages relating to the existing connection. ¶ The "Clear Log" button will restart the Log, while the Refresh button will update the messages shown on screen.
Buttons	
Connect	If not connected, establish a connection to your ISP.
Disconnect	If connected to your ISP, hang up the connection.
Clear Log	Delete all data currently in the Log. This will make it easier to read new messages.
Refresh	Update the data on screen.

Connection Status - Telstra Big Pond

An example screen is shown below.

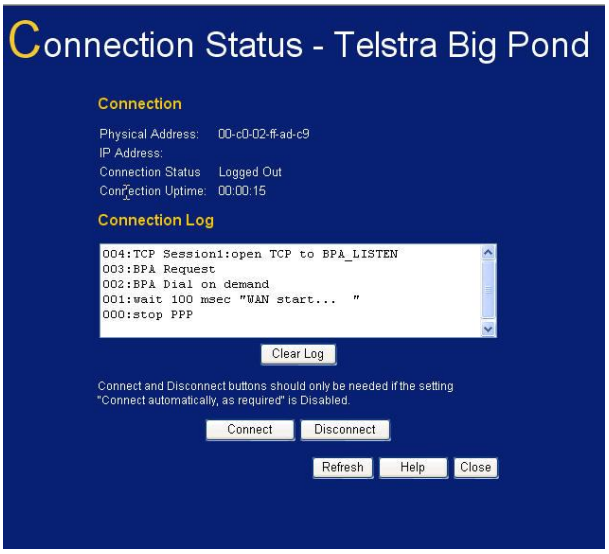

Figure 21: Telstra Big Pond Status Screen

Data - Telstra Big Pond Screen

Connection	
Physical Address	The hardware address of this device, as seen by remote devices. (This is different to the hardware address seen by devices on the local LAN.)
IP Address	The IP Address of this device, as seen by Internet users. This address is allocated by your ISP (Internet Service Provider).
Connection Status	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. ¶ Normally, it is not necessary to use the Connect and Disconnect buttons unless the setting "Connect automatically, as required" is disabled.
Connection Log	
Connection Log	¶ The Connection Log shows status messages relating to the existing connection. ¶ The Clear Log button will restart the Log, while the Refresh button will update the messages shown on screen.
Buttons	
Connect	If not connected, establish a connection to Telstra Big Pond.
Disconnect	If connected to Telstra Big Pond, terminate the connection.
Clear Log	Delete all data currently in the Log. This will make it easier to read new messages.
Refresh	Update the data on screen.

Connection Details - SingTel RAS

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

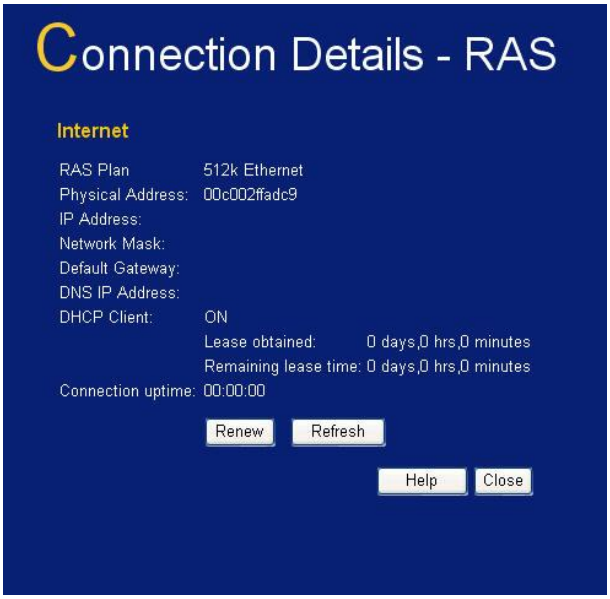

Figure 22: Connection Details - SingTel RAS

Data - SingTel RAS Screen

Internet	
RAS Plan	The RAS Plan which is currently used.
Physical Address	The hardware address of this device, as seen by remote devices on the Internet. (This is different to the hardware address seen by devices on the local LAN.)
IP Address	The IP Address of this device, as seen by Internet users. This address is allocated by your ISP (Internet Service Provider).
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 IP Address	The IP Address of the Domain Name Server which is currently used.
DHCP Client	This will show "Enabled" or "Disabled", depending on whether or not this device is functioning as a DHCP client. If "Enabled" the "Remaining lease time" field indicates when the IP Address allocated by the DHCP Server will expire. The lease is automatically renewed on expiry; use the "Renew" button if you wish to manually renew the lease immediately.
Buttons	
Release/Renew **Button will display EITHER "Release" OR "Renew"**	This button is only useful if the IP address shown above is allocated automatically on connection. (Dynamic IP address). If you have a Fixed (Static) IP address, this button has no effect. ¶ If the ISP's DHCP Server has NOT allocated an IP Address for the VPN Broadband Router, this button will say "Renew". Clicking the "Renew" button will attempt to re-establish the connection and obtain an IP Address from the ISP's DHCP Server. ¶ If an IP Address has been allocated to the VPN Broadband

	Router (by the ISP's DHCP Server), this button will say "Release". Clicking the "Release" button will break the connection and release the IP Address.
Refresh	Update the data shown on screen.

Connection Details - Fixed/Dynamic IP Address

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

Figure 23: Connection Details - Fixed/Dynamic IP Address

Data - Fixed/Dynamic IP address Screen

Internet	
Physical Address	The hardware address of this device, as seen by remote devices on the Internet. (This is different to the hardware address seen by devices on the local LAN.)
IP Address	The IP Address of this device, as seen by Internet users. This address is allocated by your ISP (Internet Service Provider).
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 IP Address	The IP Address of the Domain Name Server which is currently used.
DHCP Client	This will show "Enabled" or "Disabled", depending on whether or not this device is functioning as a DHCP client. If "Enabled" the "Remaining lease time" field indicates when the IP Address allocated by the DHCP Server will expire. The lease is automatically renewed on expiry; use the "Renew" button if you wish to manually renew the lease immediately.
Buttons	
Release/Renew **Button will display EITHER "Release" OR "Renew"**	This button is only useful if the IP address shown above is allocated automatically on connection. (Dynamic IP address). If you have a Fixed (Static) IP address, this button has no effect. ¶ If the ISP's DHCP Server has NOT allocated an IP Address for the VPN Broadband Router, this button will say "Renew". Clicking the "Renew" button will attempt to re-establish the connection and obtain an IP Address from the ISP's DHCP Server. ¶ If an IP Address has been allocated to the VPN Broadband Router (by the ISP's DHCP Server), this button will say "Release". Clicking the "Release" button will break the connection and release the IP Address.

Refresh	Update the data shown on screen.

Chapter 6
Internet Features

6

This Chapter explains when and how to use the VPN Broadband Router's "Internet" Features.

Overview

The following advanced features are provided.

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

WAN Port Configuration

The WAN Port Configuration screen provides an alternative to using the Wizard. It can be accessed from the ***Internet*** menu under ***Advanced*** section. An example screen is shown below.

Figure 24: WAN Port Configuration Screen

Data ï WAN Port Configuration Screen

Identification	
Hostname	Normally, there is no need to change the default name, but if your ISP requests that you us here.
Domain name	If your ISP provided a domain name, enter it here. Otherwise, this may be left blank.
MAC Address	Also called Network Adapter Address or Physical Address. This is a low-level identifier, as seen from the WAN port. Normally there is no need to change this, but some ISPs re-quire a particular value, often that of the PC initially used for Internet access. You can use the Copy from PC button to copy your PC's ad-dress into this field, the Default button to insert the default value, or enter a value directly.
IP Address	
IP Address is assigned automatically	Also called **Dynamic IP Address**. This is the default, and the most common. Leave this selected if your ISP allocates an IP Address to the VPN Broadband Router upon connection.

Specified IP Address	Also called **Static IP Address**. Select this if your ISP has allocated you a fixed IP Address. If this option is selected, the following data must be entered. ¶ **IP Address**. The IP Address allocated by the ISP. ¶ **Network Mask (Not required for PPPoE)** This is also supplied by your ISP. It must be compatible with the IP Address above. ¶ **Gateway IP Address (Not required for PPPoE)** The address of the router or gateway, as supplied by your ISP.
NAT	
Enable NAT	NAT (Network Address Translation) is the technology which allows all PCs on your LAN to share the Internet IP address allocated to the WAN port on this Router. From the Internet, all PCs appear to have the same IP address. For normal operation, this setting must be ENABLED.
Disable NAT	**Disabling NAT will disable Internet access, unless all PCs have valid Internet IP addresses.** If you wish to use this device for Routing ONLY (and NOT for Internet access), then NAT should be disabled.
DNS	
Automatically obtain from Server	The DNS (Domain Name Server) address will be obtained automatically from your ISP's server. Note that if using a fixed IP address, with no login (login is set to "None"), then no Server is used, and this option cannot be used.
Use this DNS	If this option is selected, you must enter the IP address of the DNS (Domain Name Server) you wish to use. **Note:** If the DNS is unavailable, the "Backup DNS", entered on the *Internet - Options* screen, will be used.
Login	
Login Method	If your ISP does not use a login method (username, password) for Internet access, leave this at the default value "None (Direct connection)" Otherwise, check the documentation from your ISP, select the login method used, and enter the required data. ¶ **PPPoE** - this is the most common login method, widely used with DSL modems. Normally, your ISP will have provided some software to connect and login. This software is no longer required, and should not be used. ¶ **PPTP** - this is mainly used in Europe. You need to know the PPTP Server address as well as your name and password. ¶ **Big Pond Cable** - for Australia only. ¶ **SingTel RAS** - for Singapore only.
Login User Name	The User Name (or account name) provided by your ISP.
Login Password	Enter the password for the login name above.
RAS Plan	For SingTel customers only, select the RAS plan you are on.

Server Address	If using PPTP or Big Pond Cable, enter the address of your ISP's server. For PPPoE or SingTel RAS, the Server address in not required.
Connection behavior	Select the desired option: ¶ **Automatic Connect/Disconnect** An Internet connection is automatically made when re-quired, and disconnected when idle for the time period specified by the "Auto-disconnect Idle Time-out". ¶ **Manual Connect/Disconnect** You must manually establish and terminate the connection. ¶ **Keep alive (maintain connection)** The connection will never be disconnected by this device. If disconnected by your ISP, the connection will be re-established immediately. (However, this does not ensure that your Internet IP address will remain unchanged.)
Auto-disconnect Idle Time-out	This field has no effect unless the setting above is *Automatic Connect/Disconnect*. If Auto-disconnect is being used, enter the desired idle time-out period (in minutes). After the connection to your ISP has been idle for this time period, the connection will be terminated.

Advanced Setup

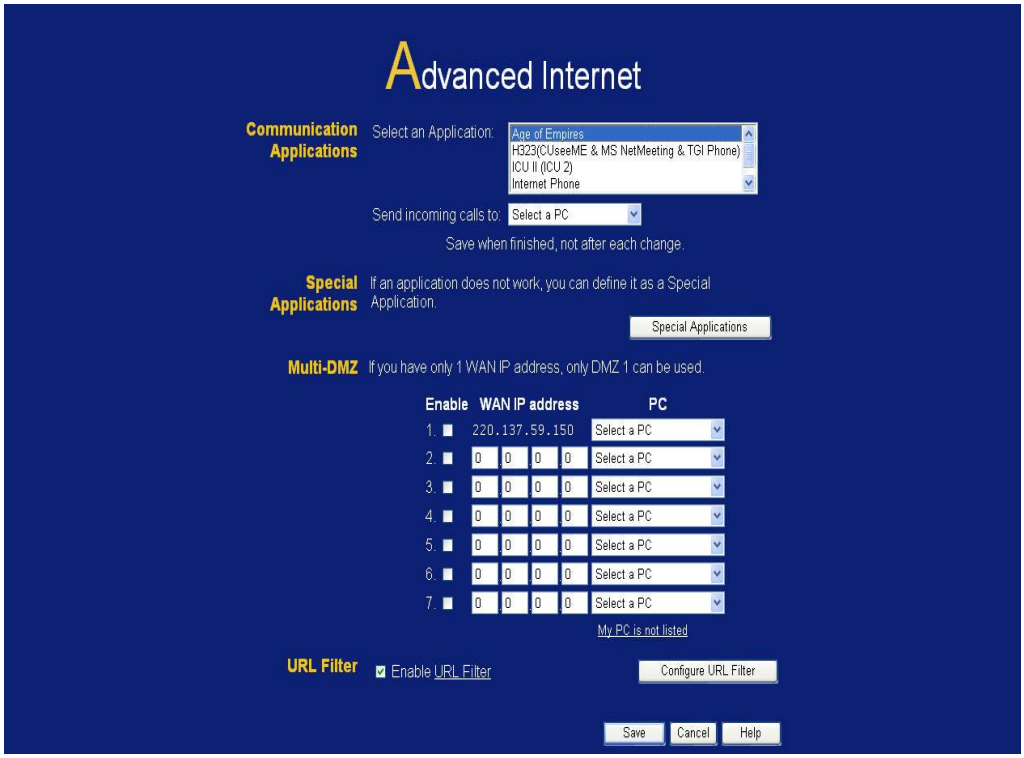

Figure 25: Internet Screen

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

¶ Communication Applications

¶ Special Applications

¶ Multi-DMZ

¶ URL filter

Communication Applications

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

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

Communication Applications	
Select an Application	This lists applications which may generate incoming connections, where the destination PC (on your local LAN) is unknown.
Send incoming calls to	This lists the PCs on your LAN. ¶ If necessary, you can add PCs manually, using the *PC Database* option on the *Other* menu. ¶ For each application listed above, you can choose a destination PC. ¶ There is no need to "Save" after each change; you can set the destination PC for each application, then click "Save".

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 VPN Broadband Router's firewall. In this case, you can define the application as a "Special Application".

Special Applications Screen

This screen can be reached by clicking the *Special Applications* button on the *Advanced Internet* screen. Click *Advanced, Advanced Setup* then *Special Applications*

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

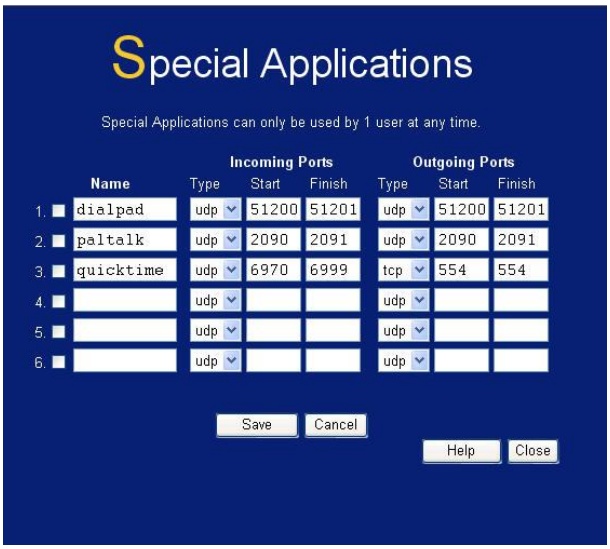

Figure 26: Special Applications Screen

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.

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

Multi-DMZ

This feature, if enabled, allows one (1) or more computers on your LAN to be exposed to all users on the Internet. You can set a DMZ PC for each WAN IP address. If you only have 1 WAN IP addresses, only 1 DMZ PC can be used.

This allows unrestricted 2-way communication between the "DMZ PC" and other Internet users or Servers.

¶ 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".

¶ To use more than one (1) DMZ, your ISP must assign multiple fixed IP addresses to you. You must enter each IP address; you can then assign a DMZ PC for each IP address.

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

URL Filter

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

¶ To use this feature, you must define "filter strings". If the "filter string" appears in a requested URL, the request is blocked.

¶ Enabling the *URL Filter* also affects the Internet *Access Log*. If Enabled, the "Destination" field in the log will display the URL. Otherwise, it will display the IP Address.

¶ The *URL Filter* can be Enabled or Disabled on the *Advanced Internet* screen.

URL Filter Screen

Click the "Configure URL Filter" button on the *Advanced Internet* screen to access the *URL Filter* screen. An example screen is shown below.

Figure 27: URL Filter Screen

Data - URL Filter Screen

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

Dynamic DNS (Domain Name Server)

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

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

The Service works as follows:

1. You must register for the service at one of the listed DDNS Service providers.
2. After registration, follow the Service Provider's procedure to request a Domain Name, and have it allocated to you.
3. Enter your DDNS data on the VPN Broadband Router's DDNS screen (shown below).
4. The VPN Broadband Router will then automatically ensure that your current IP Address is recorded and updated at the DDNS server.
   If the DDNS Service provides software to perform this "IP address update"; you should disable the "Update" function, or not use the software at all.
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 *Advancedt* on the main menu, then *Dynamic DNS*, to see a screen like the following:

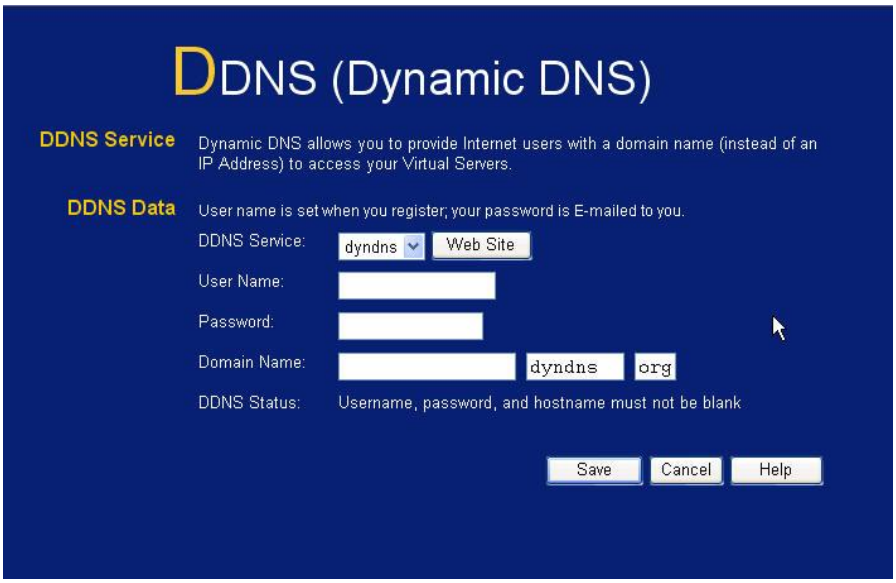

Figure 28: DDNS Screen

Data - Dynamic DNS Screen

DDNS Service	
DDNS Service	¶ You must register for the service at one of the listed Service Providers. You can reach the Service provider's Web Site by selecting them in the list and clicking the "Web Site" button. ¶ Apply for a Domain Name, and ensure it is allocated to you. ¶ Details of your DDNS account (Name, password, Domain name) must then be entered and saved on this screen. ¶ This device will then automatically ensure that your current IP Address is recorded by the DDNS Service Provider. (You do NOT need to use the "Client" program provided by

	some DDNS Service providers.) ¶ From the Internet, users will now be able to connect to your Virtual Servers (or DMZ PC) using your Domain name.
DDNS Data	
DDNS Service	Select the desired DDNS Service provider.
User Name	Enter your Username for the DDNS Service.
Password/Key	Enter your current password for the DDNS Service.
Domain Name	Enter the domain name allocated to you by the DDNS Service. If you have more than one name, enter the name you wish to use.
DDNS Status	¶ This message is returned by the DDNS Server ¶ Normally, this message should be something like "Update successful" or "IP address updated". ¶ If the message indicates some problem, you need to connect to the DDNS Service provider and correct this problem.

Virtual Servers

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

¶ Your Server does not have a valid external IP Address.

¶ Attempts to connect to devices on your LAN are blocked by the firewall in this device.

The "Virtual Server" feature solves these problems and allows Internet users to connect to your servers, as illustrated below.

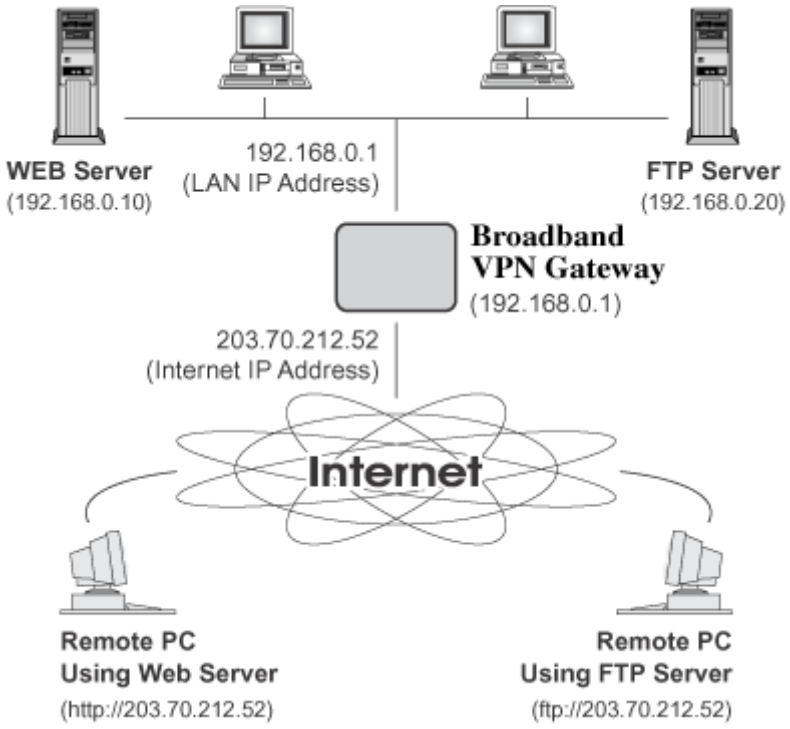

Figure 29: Virtual Servers

IP Address seen by Internet Users

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

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

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

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

Virtual Servers Screen

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

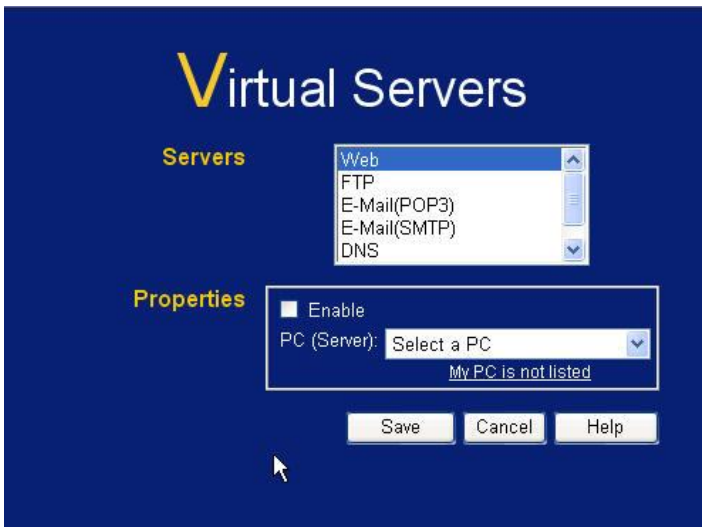

Figure 30: Virtual Servers Screen

This screen lists a number of pre-defined Servers, providing a quick and convenient method to set up the common server types.

Data - Virtual Servers Screen

Servers	
Servers	This lists a number of pre-defined Servers, plus any Servers you have defined. Details of the selected Server are shown in the "Properties" area.
Properties	
Enable	Use this to Enable or Disable support for this Server, as required. ¶ If Enabled, any incoming connections will be forwarded to the selected PC. ¶ If Disabled, any incoming connection attempts will be blocked.
PC (Server)	Select the PC for this Server. The PC must be running the appropriate Server software.

Defining your own Virtual Servers

If the type of Server you wish to use is not listed on the *Virtual Servers* screen, you can use the Firewall Rules to allow particular incoming traffic and forward it to a specified PC (Server).

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

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.

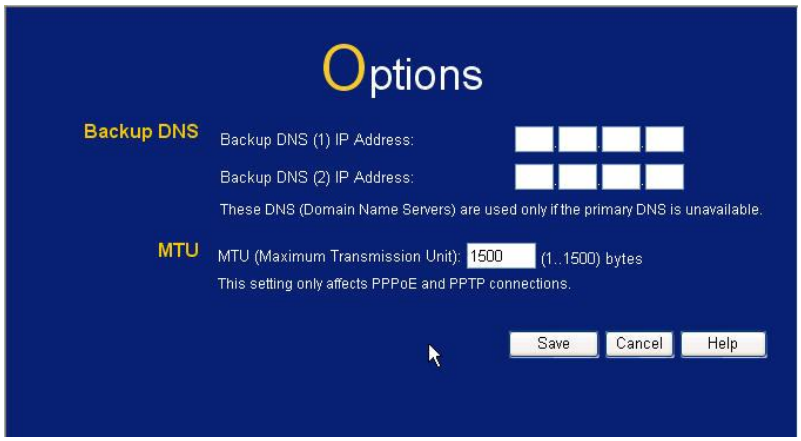

Figure 31: Options Screen

Data - Options Screen

Backup DNS	
IP Address	Enter the IP Address of the DNS (Domain Name Servers) here. These DNS will be used only if the primary DNS is unavailable.
MTU	
MTU size	MTU (Maximum Transmission Unit) value should only be changed if advised to do so by Technical Support. ¶ Enter a value between 1 and 1500. ¶ This device will still auto-negotiate with the remote server, to set the MTU size. The smaller of the 2 values (auto-negotiated, or entered here) will be used. ¶ For direct connections (not PPPoE or PPTP), the MTU used is always 1500.

Chapter 7
Security Configuration

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

Overview

The following advanced configurations are provided.

- Access Control
- Firewall Rules
- Logs
- E-mail
- Security Options
- Scheduling
- Services

Access Control

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

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

To use this feature:

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

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

Access Control Screen

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

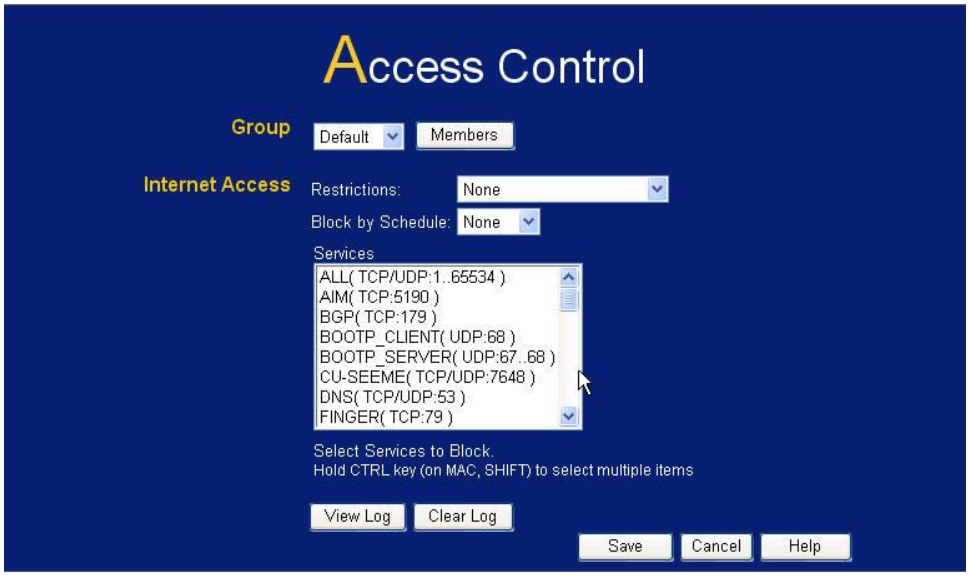

Figure 32: Access Control Screen

Data - Access Control Screen

Group	
Group	Select the desired Group. The screen will update to display the settings for the selected Group. Groups are named "Default", "Group 1", "Group 2", "Group 3" and "Group 4", and cannot be re-named.

"Members" Button	Click this button to add or remove members from the current Group. ¶ If the current group is "Default", then members can not be added or deleted. This group contains PCs not allocated to any other group. ¶ To remove PCs from the Default Group, assign them to another Group. ¶ To assign PCs to the Default Group, delete them from the Group they are currently in. See the following section for details of the *Group Members* screen.
Internet Access	
Restrictions	Select the desired options for the current group: ¶ None - Nothing is blocked. Use this to create the least restrictive group. ¶ Block all Internet access - All traffic via the WAN port is blocked. Use this to create the most restrictive group. ¶ Block selected Services - You can select which Services are to block. Use this to gain fine control over the Internet access for a group.
Block by Schedule	If Internet access is being blocked, you can choose to apply the blocking only during scheduled times. (If access is not blocked, no Scheduling is possible, and this setting has no effect.) To define the schedule, use the *Schedule* option on the menu.
Services	This lists all defined Services. Select the Services you wish to block. To select multiple services, hold the CTRL key while selecting. (On the Macintosh, hold the SHIFT key rather than CTRL.)
Buttons	
Members	Click this button to add or remove members from the current Group. If the current group is "Default", then members can not be added or deleted. This group contains PCs not allocated to any other group. See the following section for details of the *Group Members* screen.
Save	Save the data on screen.
Cancel	Reverse any changes made since the last "Save".
View Log	Click this to open a sub-window where you can view the "Access Control" log. This log shows attempted Internet accesses which have been blocked by the Access Control feature.
Clear Log	Click this to clear and restart the "Access Control" log, making new entries easier to read.

Group Members Screen

This screen is displayed when the *Members* button on the *Access Control* screen is clicked.

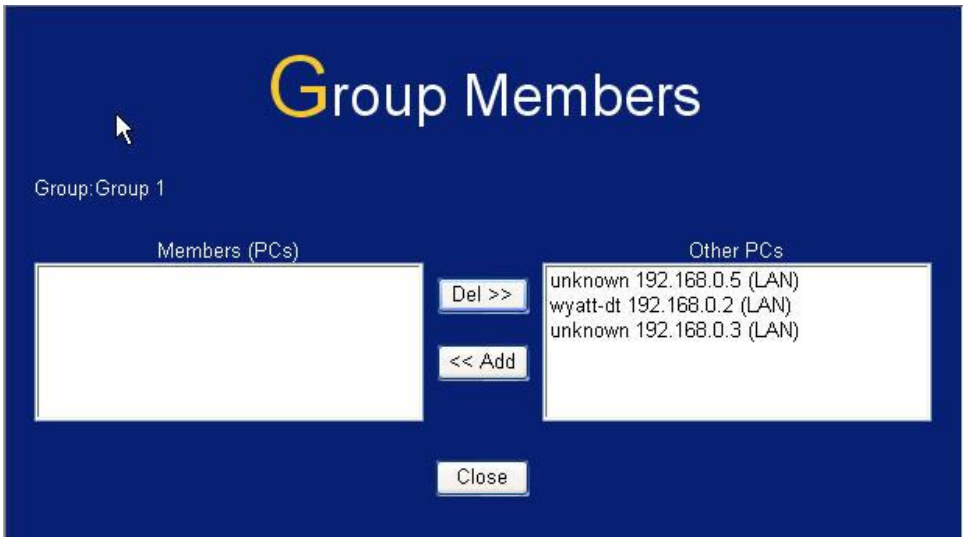

Figure 33: Group Members

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

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

Note!

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

Access Control Log

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

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

Data shown in this log is as follows:

Date/Time	Date and Time of the attempted access.
Name	If known, the name of the PC whose access was blocked. This name is taken from the *Network Clients* database
Source IP address	The IP Address of the PC or device whose access request was blocked
MAC address	The hardware or physical address of the PC or device whose access request was blocked
Destination	The destination URL or IP address

Firewall Rules

For normal operation and LAN protection, it is not necessary to use this screen.

The Firewall will always block DoS (Denial of Service) attacks. A DoS attack does not attempt to steal data or damage your PCs, but overloads your Internet connection so you can not use it - the service is unavailable.

As well, you can use this screen to create Firewall rules to block or allow specific traffic. But incorrect configuration may cause serious problems.

This feature is for advanced administrators only!

Firewall Rules Screen

Click the *Firewall Rules* option on the Security menu to see a screen like the following example. This example contains two (2) rules for outgoing traffic.

Since the default rule for outgoing (LAN => WAN) traffic is "Allow", having an "Allow" rule for LAN => WAN only makes sense in combination with another rule.

Figure 34: Firewall Rules Screen

Data - Firewall Rules Screen

Rule List	
View Rules for..	Select the desired option; the screen will update and list any current rules. If you have not defined any rules, the list will be empty.

Data	For each rule, the following data is shown: ¶ **Name** - The name you assigned to the rule. ¶ **Source** - The traffic covered by this rule, defined by the source IP address. If the IP address is followed by ... this indicates there is range of IP addresses, rather than a single address. ¶ **Destination** - The traffic covered by this rule, defined by destination IP address. If the IP address is followed by ... this indicates there is range of IP addresses, rather than a single address. ¶ **Action** - Action will be "Forward" or "Block"
Add	To add a new rule, click the "Add" button, and complete the resulting screen. See the following section for more details.
Edit	To Edit or modify an existing rule, select it and click the "Edit" button.
Move	There are 2 ways to change the order of rules ¶ Use the up and down indicators on the right to move the selected rule. You must confirm your changes by clicking "OK". If you change your mind before clicking "OK", click "Cancel" to reverse your changes. ¶ Click "Move" to directly specify a new location for the selected rule.
Delete	To delete an existing rule, select it and click the "Delete" button.
View Log	Clicking the "View Log" button will open a new window and display the Firewall log.
System Rules	Clicking the "System Rules" button will open a new window and display the default firewall rules currently applied by the system. These rules cannot be edited, but any rules you create will take precedence over the default rules.

Define Firewall Rule

Clicking the "Add" button in the *Firewall Rules* screen will display a screen like the example below.

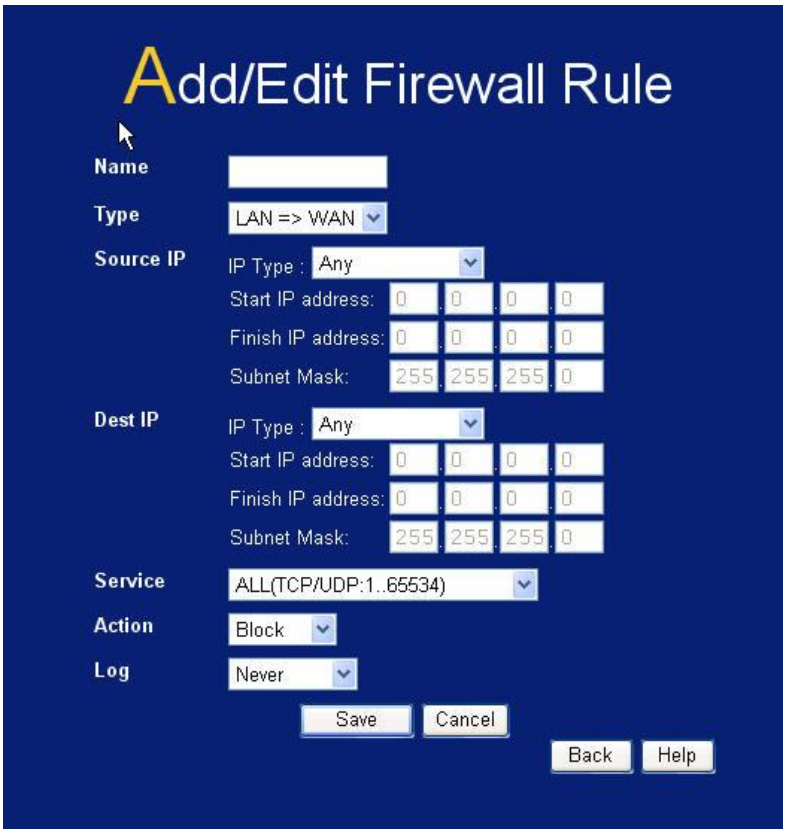

Figure 35: Define Firewall Rule

Data - Define Firewall Rule Screen

Name	Enter a suitable name for this rule.
Type	This determines the source and destination ports for traffic covered by this rule. Select the desired option.
Source IP	These settings determine which traffic, based on their source IP address, is covered by this rule. Select the desired option: ¶ Any - All traffic from the source port is covered by this rule. ¶ Single address - Enter the required IP address in the "Start IP address" field". You can ignore the "Subnet Mask" field. ¶ Range address - If this option is selected, you must complete both the "Start IP address" and "Finish IP address" fields. You can ignore the "Subnet Mask" field. ¶ Subnet address - If this option is selected, enter the required mask in the "Subnet Mask" field.

Dest. IP	These settings determine which traffic, based on their destination IP address, is covered by this rule. Select the desired option: ¶ Any - All traffic from the source port is covered by this rule. ¶ Single address - Enter the required IP address in the "Start IP address" field". You can ignore the "Subnet Mask" field. ¶ Range address - If this option is selected, you must complete both the "Start IP address" and "Finish IP address" fields. You can ignore the "Subnet Mask" field. ¶ Subnet address - If this option is selected, enter the required mask in the "Subnet Mask" field.
Services	Select the desired Service or Services. This determines which packets are covered by this rule, based on the protocol (TPC or UDP) and port number. 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:
Log	This determines whether packets covered by this rule are logged. Select the desired option.

Logs

The Logs record various types of activity on the VPN Broadband 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 VPN Broadband Router, log data can also be E-mailed to your PC or sent to a Syslog Server.

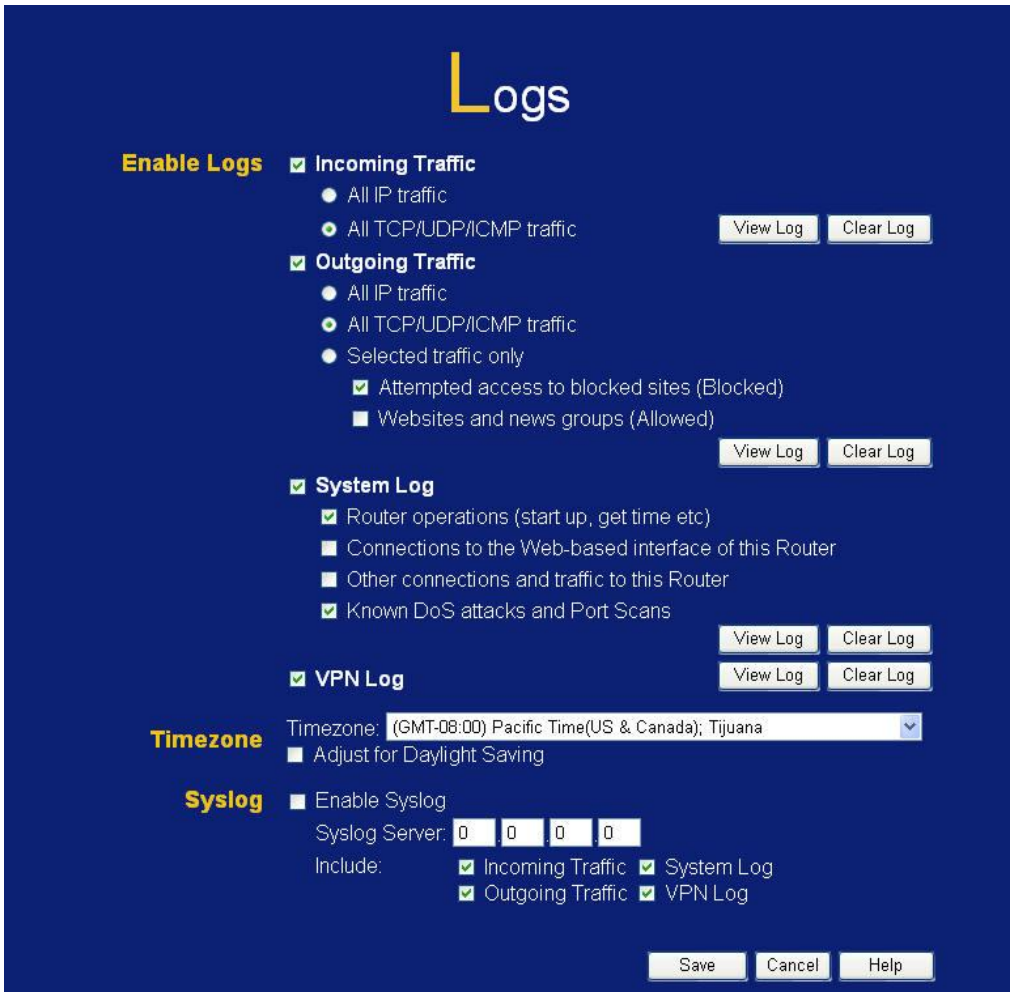

Figure 36: Logs Screen

Data - Logs Screen

Enable Logs	
Incoming Traffic	Select the desired option: ¶ **All IP traffic** - this will log all incoming TCP/IP connections, of any type. This will generate the largest logs, and fill the internal log buffer more quickly. ¶ **All TCP/UDP/ICMP traffic** - These 3 protocols are used by most internet traffic. TCP is used by HTTP, FTP, Telnet, E-mail and other common Internet protocols and applications. UDP is used by Video streams and other communications where speed is more important than guaranteed delivery. ICMP is used by the "ping" and "trace route" applications, and other network diagnostics.

Outgoing Traffic	Select the desired option: ¶ **All IP traffic** - - this will log all outgoing TCP/IP connections, of any type. This will generate the largest logs, and fill the internal log buffer more quickly. ¶ **All TCP/UDP/ICMP traffic** - These 3 protocols are used by most internet traffic. TCP is used by HTTP, FTP, Telnet, E-mail and other common Internet protocols and applications. UDP is used by Video streams and other communications where speed is more important than guaranteed delivery. ICMP is used by the "ping" and "trace route" applications, and other network diagnostics. Because most connections are logged, the logs will still be large. ¶ **Selected Traffic only** - This selection will reduce the size of the log considerably. Only HTTP connections are logged. Select the traffic you wish to include: ¶ *Attempted access to blocked sites* - This will only log Web connections which are blocked by the URL filter. ¶ *Websites and news groups* - This logs successful (allowed) connections to Web Sites and newsgroup servers.
System Log	Select the desired option: ¶ **Router operations (start up, get time etc)** - This option will log normal Router operations. ¶ **Connections to the Web - based interface of this Router** - This option will log each connection to the Router itself, whenever the Web-based management interface is used. ¶ **Other connections and traffic to this Router** - This option will log other traffic sent to the Router itself, such as "pings" or RIP (Router Information Protocol) packets. ¶ **Known DoS attacks and Port Scans** - This will log details of DoS (Denial of Service) attacks which have been blocked by the built-in Firewall. This Firewall uses "Stateful Inspection" technology to block packets which are individually valid, but collectively form an attack. Port scans, where a series of ports are checked to see if they are open (available) are also logged.
VPN	If enabled, the VPN log will record incoming and outgoing VPN connections.
View Log Button	Use this to view each log, as required.
Clear Log Button	Use this to restart the required log. This makes it easier to read the latest entries.
Timezone	
Timezone	Select the correct Timezone for your location. This is required for the date/time shown on the logs to be correct.
Syslog Server	
Enable Syslog	If enabled, log data will be sent to your Syslog Server.
Syslog Server	Enter the IP address of your Syslog Server.
Include	Select the logs you wish to be included in the data sent to the Syslog Server.

E-mail

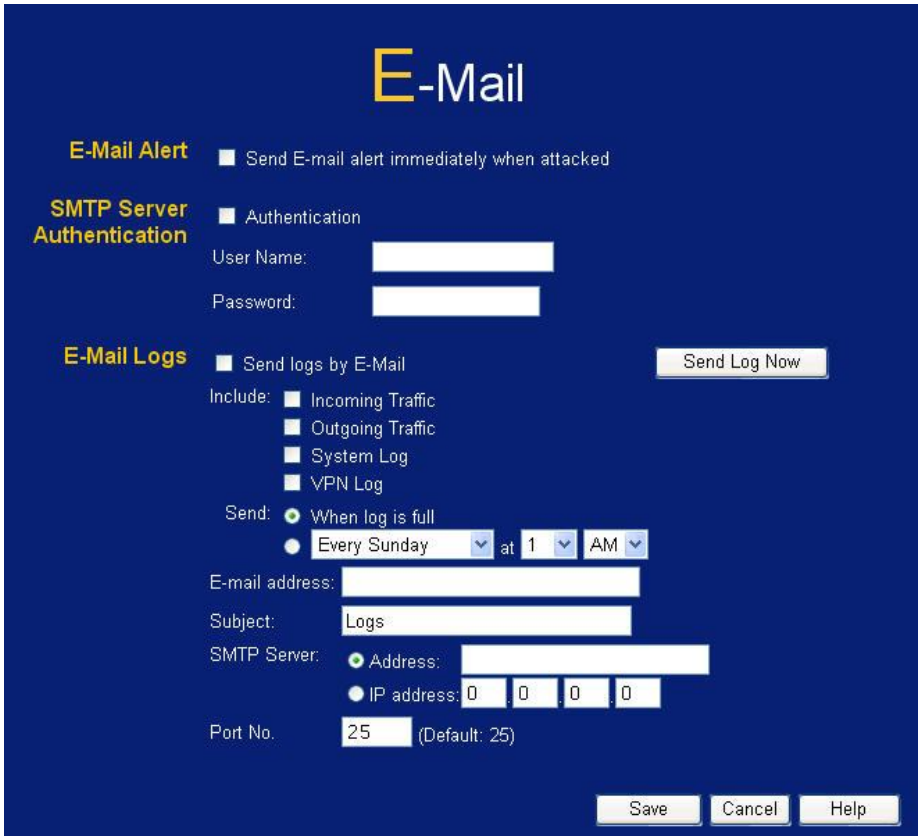

Figure 37: E-Mail Screen

Data ï E-Mail Screen

E-Mail Alerts	
Send E-Mail alert	If enabled, an E-mail will be sent immediately if a DoS (Denial of Service) attack is detected. If enabled, the E-mail address information must be provided.
E-Mail Logs	
Send Logs by E-Mail	If enabled, logs will be logs to the specified E-mail address. You need to select the Logs to be E-mailed, and complete the E-mail address settings on this screen.
Include	Select the log items to be included in the E-mail.
Send	Select the desired option for sending the log by E-mail. ¶ **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. ¶ **Every day, Every Monday...** - The log is sent on the interval specified. ¶ If "Every day" 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.

E-mail address	Enter the E-mail address the Log is to be sent to. The E-mail will also show this address as the Sender's address.
Subject	Enter the text string to be shown in the "Subject" field for the E-mail.
SMTP Server	Enter the address or address or IP address of the SMTP (Simple Mail Transport Protocol) Server you use for outgoing E-mail.
Port No.	Enter the port number used to connect to the SMTP Server. The default value is 25.

Security Options

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

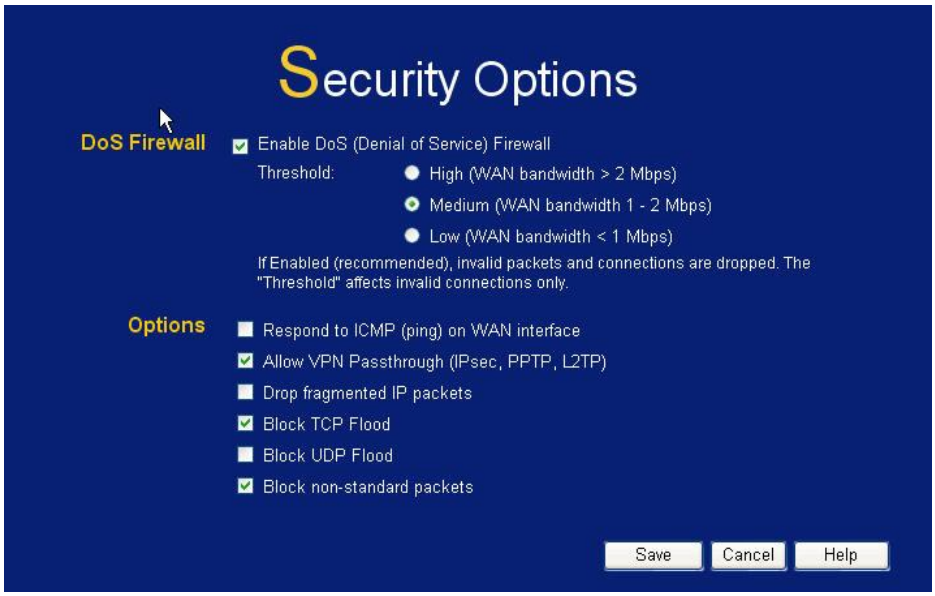

Figure 38: Security Options Screen

Data - Security Options Screen

Firewall	
Enable DoS Firewall	If enabled, DoS (Denial of Service) attacks will be detected and blocked. The default is enabled. It is strongly recommended that this setting be left enabled. **Note:** ¶ A DoS attack does not attempt to steal data or damage your PCs, but overloads your Internet connection so you can not use it - the service is unavailable. ¶ This device uses "Stateful Inspection" technology. This system can detect situations where individual TCP/IP packets are valid, but collectively they become a DoS attack.
Threshold	This setting affects the number of "half-open" connections allowed. ¶ A "half-open" connection arises when a remote client contacts the Server with a connection request, but then does not reply to the Server's response. ¶ While the optimum number of "half-open" connections allowed (the "Threshold") depends on many factors, the most important factor is the available bandwidth of your Internet connection. ¶ Select the setting to match the bandwidth of your Internet connection.
Options	
Respond to ICMP (ping)	The ICMP protocol is used by the "ping" and "trace route" programs, and by network monitoring and diagnostic programs. ¶ If checked, the VPN Broadband Router will respond to ICMP packets received from the Internet. ¶ If not checked, ICMP packets from the Internet will be ignored. Disabling this option provides a slight increase in security.

Allow VPN pass-through	If enabled, PCs on the LAN can use VPN software to connect to remote clients via the Internet connection. The protocols supported are: ¶ IPSec IPSec protocol is used to establish a secure connection, and is widely used by VPN (Virtual Private Networking) programs. ¶ PPTP PPTP (Point to Point Tunneling Protocol) is widely used by VPN (Virtual Private Networking) programs. ¶ L2TP L2TP is a protocol developed by Cisco for VPNs (Virtual Private Networks).
Drop fragmented IP packets	If enabled, fragmented IP packets are discarded, forcing re-transmission of these packets. In some situations, this could prevent successful communication. Normally, this setting should be disabled.
Block TCP Flood	A TCP flood is excessively large number of TCP connection requests. This is usually a DoS (Denial of Service) attack. This setting should normally be enabled.
Block UDP Flood	A UDP flood is excessively large number of UDP packets. This is usually a DoS (Denial of Service) attack. This setting should normally be enabled.
Block non-standard packets	Abnormal packets are often used by hackers and in DoS attacks, but may also be generated by incorrectly configured network devices. (PCs will normally not generate non-standard packets.) This setting should normally be enabled.

Scheduling

- This schedule can be (optionally) applied to any Access Control Group.
- Blocking will be performed during the scheduled time (between the "Start" and "Finish" times.)
- Two (2) separate sessions or periods can be defined.
- Times must be entered using a 24 hr clock.
- If the time for a particular day is blank, no action will be performed.

Define Schedule Screen

This screen is accessed by the *Scheduling* link on the *Security* menu.

Figure 39: Define Schedule Screen

Data - Define Schedule Screen

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