

# **Broadband VPN Gateway**

**Broadband Internet Access  
4-Port Switching Hub**

---

---

**User's Guide**

---

---

# Table of Contents

---

<b>CHAPTER 1 INTRODUCTION .....</b>	<b>1</b>
<b>Broadband VPN Gateway Features .....</b>	<b>1</b>
<b>Package Contents .....</b>	<b>3</b>
<b>Physical Details .....</b>	<b>4</b>
<b>CHAPTER 2 INSTALLATION.....</b>	<b>6</b>
<b>Requirements.....</b>	<b>6</b>
<b>Procedure .....</b>	<b>6</b>
<b>CHAPTER 3 SETUP .....</b>	<b>8</b>
<b>Overview .....</b>	<b>8</b>
<b>Configuration Program .....</b>	<b>9</b>
<b>Setup Wizard .....</b>	<b>11</b>
<b>WAN Port Configuration Screen.....</b>	<b>14</b>
<b>LAN Screen.....</b>	<b>16</b>
<b>CHAPTER 4 PC CONFIGURATION .....</b>	<b>18</b>
<b>Overview .....</b>	<b>18</b>
<b>Windows Clients.....</b>	<b>18</b>
<b>Macintosh Clients.....</b>	<b>30</b>
<b>Linux Clients.....</b>	<b>30</b>
<b>Other Unix Systems.....</b>	<b>30</b>
<b>CHAPTER 5 OPERATION AND STATUS .....</b>	<b>31</b>
<b>Operation .....</b>	<b>31</b>
<b>Status Screen.....</b>	<b>31</b>
<b>Connection Status - PPPoE .....</b>	<b>33</b>
<b>Connection Status - PPTP .....</b>	<b>35</b>
<b>Connection Status - Telstra Big Pond.....</b>	<b>36</b>
<b>Connection Details - SingTel RAS .....</b>	<b>37</b>
<b>Connection Details - Fixed/Dynamic IP Address .....</b>	<b>39</b>
<b>CHAPTER 6 INTERNET FEATURES .....</b>	<b>41</b>
<b>Overview .....</b>	<b>41</b>
<b>Advanced Internet Screen .....</b>	<b>41</b>
<b>Dynamic DNS (Domain Name Server).....</b>	<b>46</b>
<b>Virtual Servers.....</b>	<b>48</b>
<b>Options .....</b>	<b>50</b>
<b>CHAPTER 7 SECURITY CONFIGURATION.....</b>	<b>52</b>
<b>Overview .....</b>	<b>52</b>
<b>Admin Login .....</b>	<b>52</b>
<b>Access Control .....</b>	<b>54</b>
<b>Firewall Rules .....</b>	<b>57</b>
<b>Logs.....</b>	<b>61</b>
<b>Security Options .....</b>	<b>63</b>
<b>Scheduling.....</b>	<b>65</b>
<b>Services.....</b>	<b>66</b>

<b>CHAPTER 8 VPN</b> .....	<b>68</b>
<b>Overview</b> .....	<b>68</b>
<b>Common VPN Situations</b> .....	<b>70</b>
<b>VPN Configuration</b> .....	<b>72</b>
<b>Examples</b> .....	<b>81</b>
<b>Using Certificates</b> .....	<b>99</b>
<b>CHAPTER 9 OTHER FEATURES AND SETTINGS</b> .....	<b>104</b>
<b>Overview</b> .....	<b>104</b>
<b>PC Database</b> .....	<b>105</b>
<b>Remote Administration</b> .....	<b>109</b>
<b>Routing</b> .....	<b>110</b>
<b>Firmware Upgrade</b> .....	<b>114</b>
<b>UPNP</b> .....	<b>115</b>
<b>APPENDIX A TROUBLESHOOTING</b> .....	<b>116</b>
<b>Overview</b> .....	<b>116</b>
<b>General Problems</b> .....	<b>116</b>
<b>Internet Access</b> .....	<b>116</b>
<b>APPENDIX B SPECIFICATIONS</b> .....	<b>118</b>
<b>Broadband VPN Gateway</b> .....	<b>118</b>
<b>FCC Statement</b> .....	<b>118</b>
<b>CE Marking Warning</b> .....	<b>119</b>

P/N: 9560J29930

Copyright © 2003. All Rights Reserved.

Document Version: 1.0

All trademarks and trade names are the properties of their respective owners.

# Chapter 1

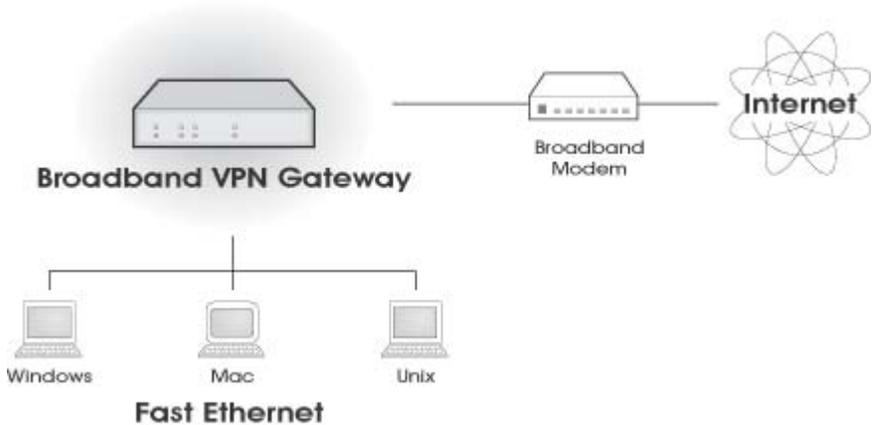
## Introduction

# 1

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

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

- **Shared Broadband Internet Access** for all LAN users.
- **4-Port Switching Hub** for 10BaseT or 100BaseT connections.



**Figure 1: Broadband VPN Gateway**

## Broadband VPN Gateway Features

The Broadband VPN 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 Broadband VPN 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).
- **DSL & Cable Modem Support.** The Broadband VPN Gateway 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 Broadband VPN Gateway 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.
- **DMZ.** 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 Broadband VPN Gateway incorporates a 4-port 10/100BaseT switching hub, making it easy to create or extend your LAN.
- **DHCP Server Support.** Dynamic Host Configuration Protocol provides a dynamic IP address to PCs and other devices upon request. The Broadband VPN Gateway 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 Broadband VPN Gateway 's RIP (Routing Information Protocol) support and built-in static routing table.
- **DMZ Port.** Used when allowing Servers on your LAN to be accessed from the Internet, the DMZ port provides additional protection for both your Servers and your LAN.

## Configuration & Management

- **Easy Setup.** Use your WEB browser from anywhere on the LAN or WLAN for configuration.
- **Remote Management.** The Broadband VPN Gateway 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 Broadband VPN Gateway. UPnP is supported by Windows ME, XP, or later.

## Security Features

- **Password - protected Configuration.** Optional password protection is provided to prevent unauthorized users from modifying the configuration data and settings.
- **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 Broadband VPN Gateway.

- **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 Broadband VPN Gateway 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.

## VPN Gateway Features

- **IPSec.** Support for IPSec standards, including IKE and certificates.
- **70 Tunnels.** Up to 70 VPN tunnels can be created.
- **High performance.** High performance encryption engine maintains high throughput even when using 3DES.

## Package Contents

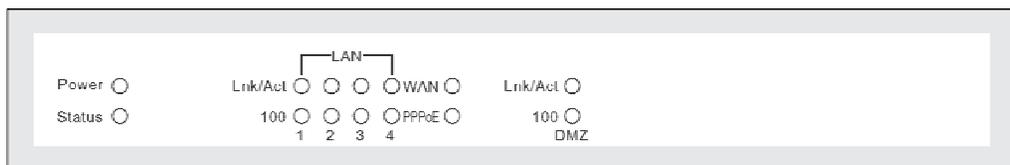
The following items should be included:

- The Broadband VPN Gateway Unit
- Power Adapter
- Quick Installation Guide
- CD-ROM containing the on-line manual.

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

## Physical Details

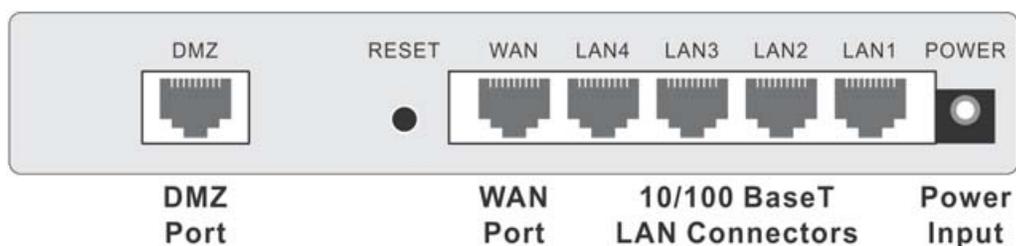
### Front-mounted LEDs



**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**      For each port, there are 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.  
**Flashing** - Data is being transmitted or received via the WAN port.
- PPPoE**      **On** - PPPoE connection established.  
**Off** - No PPPoE connection.
- DMZ**      • **Link/Act**
  - **Blinking** – receiving/ transmitting data
  - **100**
    - **On** - Link at 100Mbps
    - **Off** - Link at 10Mbps

## Rear Panel



**Figure 3: Rear Panel**

### DMZ

Use a standard LAN cable to connect to a normal port on another hub.

### Reset Button

This button has two (2) functions:

- **Reboot.** When pressed and released, the Broadband VPN Gateway 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 Broadband VPN Gateway 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 Broadband VPN Gateway 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

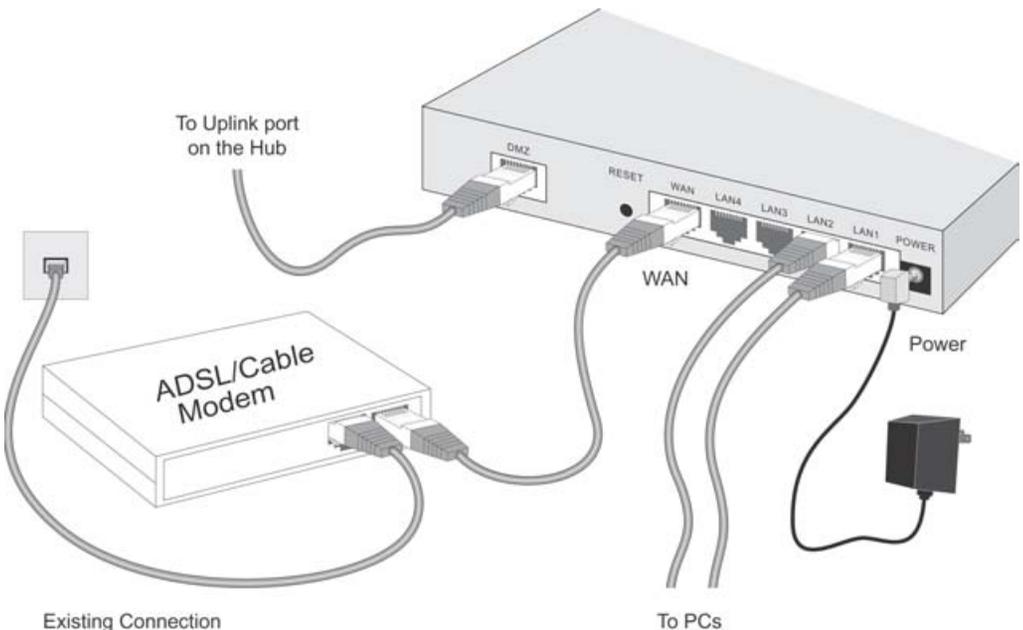
## Installation

*This Chapter covers the physical installation of the Broadband VPN Gateway.*

### 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 either of a DSL or Cable modem (for WAN port usage)

### Procedure



**Figure 4: Installation Diagram**

#### 1. Choose an Installation Site

Select a suitable place on the network to install the Broadband VPN Gateway. Ensure the Broadband VPN Gateway 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 Broadband VPN Gateway. 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 Broadband VPN Gateway 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.

- If desired, connect the DMZ port to a standard port on another Hub. PCs connected this hub will also gain Internet access, but will NOT be able to access the rest of the LAN.

### 3. Connect WAN Cable

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

### 4. Power Up

- Power on the Cable or DSL modem.
- Connect the supplied power adapter to the Broadband VPN Gateway 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 flash, 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.

## Using the DMZ Port

Please note the following points regarding the DMZ port.

- The DMZ port is a normal port, not an "uplink" port.
- PCs connected to the DMZ port are on the same LAN segment as PCs connected to the Hub ports. They must use the same IP address range.
- PCs connected to the DMZ port are NOT visible to PCs on the hub (LAN) ports. So you cannot use Microsoft networking or other networking protocols to connect to PCs on the DMZ.
- PCs connected to the DMZ port still share the WAN port IP address for Internet access.

### Advantages of the DMZ Port

If running any Servers on your LAN, you should connect them to the DMZ port, for the following reasons:

- Traffic passing between the DMZ and LAN passes through the firewall. The firewall will protect your LAN if your Server is compromised and used to launch an attack on your LAN.
- When using the *Virtual Servers* feature, (see *Virtual Servers* in Chapter 6) a firewall rule to allow incoming traffic from the Internet (WAN) to the DMZ is automatically created. If the Server is connected to the LAN (hub) ports, you must add the firewall rule manually.

# Chapter 3

## Setup



*This Chapter provides Setup details of the Broadband VPN Gateway.*

### 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 Broadband VPN 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
Check Broadband VPN Gateway operation and Status.	Chapter 5: Operation and Status
Use any of the following Internet features: <ul style="list-style-type: none"><li>• Advanced Setup (Applications, DMZ)</li><li>• Dynamic DNS</li><li>• Virtual Servers</li><li>• MAC Address</li><li>• Options(Backup DNS, MTU)</li></ul>	Chapter 6: Internet Features
Change any of the following Security-related settings: <ul style="list-style-type: none"><li>• Admin Login</li><li>• Access Control</li><li>• Firewall Rules</li><li>• Logs</li><li>• Security Options (TFTP, Firewall)</li><li>• Scheduling (used by Access Control)</li><li>• Services</li></ul>	Chapter 7: Security Configuration
Describe the VPN capabilities and configuration required for common situations.	Chapter 8: VPN

Configure or use any of the following: <ul style="list-style-type: none"> <li>• PC Database</li> <li>• Remote Admin</li> <li>• Routing (RIP and static Routing)</li> <li>• Upgrade firmware</li> <li>• Enable/Disable UPnP Support</li> </ul>	Chapter 9: Other Features and Settings
---	---

**Note!**

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 Broadband VPN 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 V4.08 or later
- Internet Explorer V4 or later

## Preparation

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

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

## Using UPnP

If your Windows system supports UPnP, an icon for the Broadband VPN 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 Broadband VPN 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 Broadband VPN 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 Broadband VPN Gateway:

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

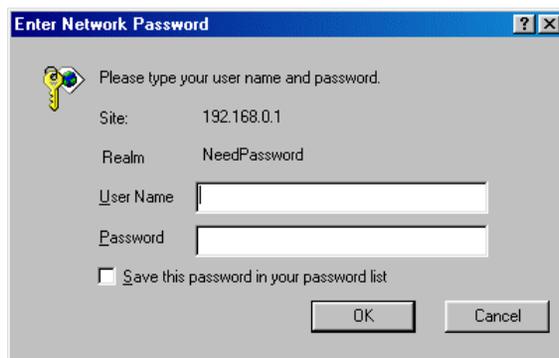
HTTP://192.168.0.1

### If you can't connect

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

- The Broadband VPN 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 Broadband VPN 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 Broadband VPN 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 Broadband VPN Gateway 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 leave the Password blank.
- Both the name and password can (and should) be changed, using the *Admin Login* screen.

## Setup Wizard

The first time you connect to the Broadband VPN Gateway, the Setup Wizard will run automatically. (The Setup Wizard will also run if the Broadband VPN Gateway's default settings are restored.)

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 Broadband VPN Gateway.

### Common Connection Types

#### Cable Modems

Type	Details	ISP Data required
Dynamic IP Address	Your IP Address is allocated automatically, when you connect to your 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 your 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).	<ul style="list-style-type: none"> <li>• PPTP Server IP Address.</li> <li>• User name and password.</li> <li>• IP Address allocated to you, if Static (Fixed).</li> </ul>

### 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 Setup Wizard, you will see the *Home* screen. When you connect in future, you will see this screen when you connect. An example screen is shown below.

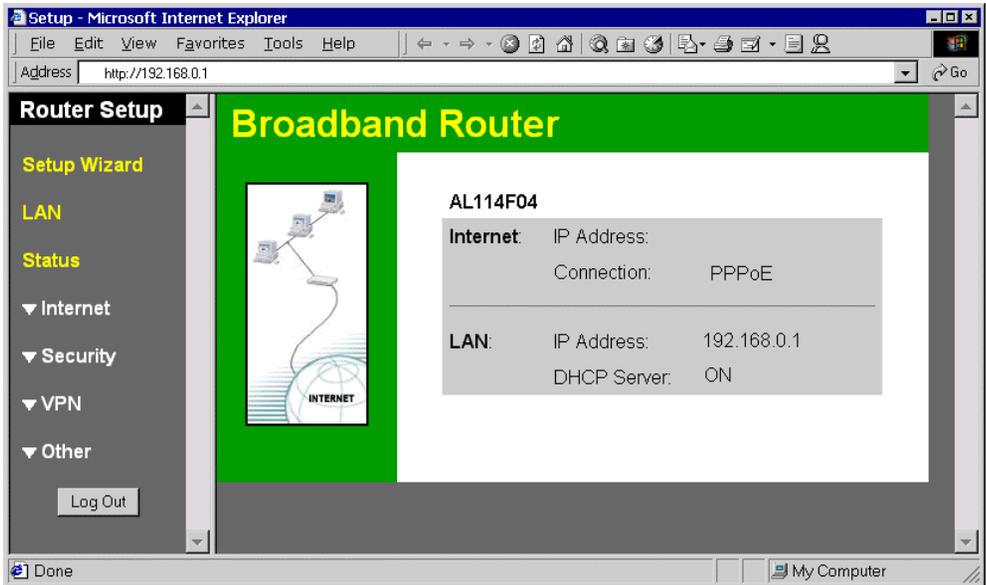


Figure 6: Home Screen

## Navigation & 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.

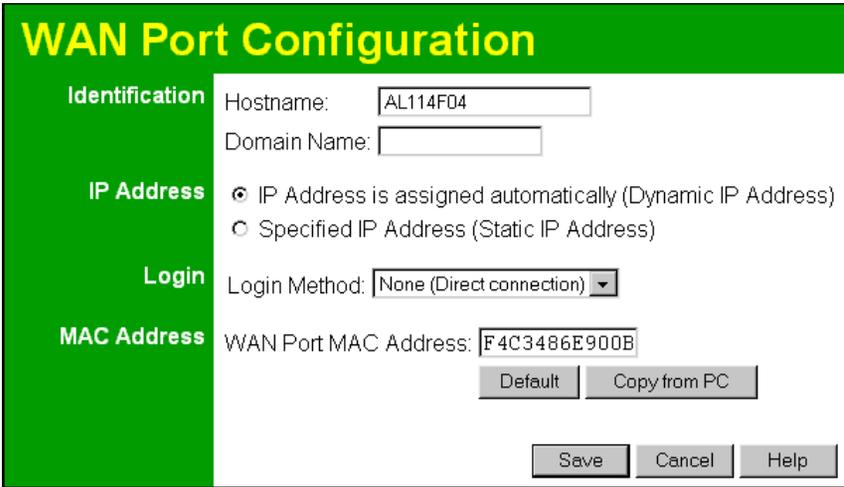


On each screen, clicking the "Help" button will display help for that screen.

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

## WAN Port Configuration Screen

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



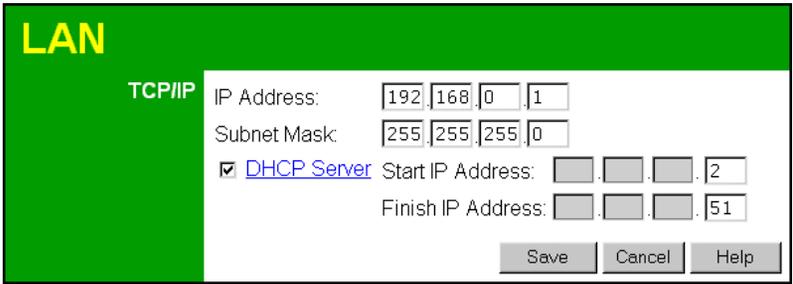
**Figure 7: WAN Port**

Identification	
<b>Hostname</b>	Normally, there is no need to change the default name, but if your ISP requests that you use a particular “Hostname”, enter it here.
<b>Domain name</b>	If your ISP provided a domain name, enter it here. Otherwise, this may be left blank.
IP Address	
<b>IP Address is assigned automatically</b>	Also called <b>Dynamic IP Address</b> . This is the default, and the most common. Leave this selected if your ISP allocates an IP Address to the Wireless Router upon connection.
<b>Specified IP Address</b>	Also called <b>Static IP Address</b> . Select this if your ISP has allocated you a fixed IP Address. If this option is selected, the following data must be entered. <ul style="list-style-type: none"> <li>• <b>IP Address.</b> The IP Address allocated by the ISP.</li> <li>• <b>Network Mask (Not required for PPPoE)</b> This is also supplied by your ISP. It must be compatible with the IP Address above.</li> <li>• <b>Gateway IP Address (Not required for PPPoE)</b> The address of the router or gateway, as supplied by your ISP.</li> <li>• <b>DNS IP Address</b> The DNS (Domain Name Server) IP Address provided by your ISP. If required, additional DNS entries can be made on the <i>Internet Options</i> screen.</li> </ul>

<b>Login</b>	
<b>Login Method</b>	<p>If your ISP does not use a login method (username, password) for Internet access, leave this at the default value "None (Direct connection)"</p> <p>Otherwise, check the documentation from your ISP, select the login method used, and enter the required data.</p> <ul style="list-style-type: none"> <li>• <b>PPPoE</b> - 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.</li> <li>• <b>PPTP</b> - this is mainly used in Europe. You need to know the PPTP Server address as well as your name and password.</li> <li>• <b>Big Pond Cable</b> - for Australia only.</li> <li>• <b>SingTel RAS</b> - for Singapore only.</li> </ul>
<b>Login User Name</b>	The User Name (or account name) provided by your ISP.
<b>Login Password</b>	Enter the password for the login name above.
<b>RAS Plan</b>	For SingTel customers only, select the RAS plan you are on.
<b>Server IP Address</b>	If using PPTP or Big Pond Cable, enter the IP address of your ISP's server.
<b>Connect automatically</b>	If Enabled (default), a connection will automatically be made as required. If disabled, you need to establish the connection manually, using the <i>Connect</i> button on the <i>Connection Details</i> screen (accessed from the Status screen).
<b>Disconnect after Idle</b>	<p>Enable this if you wish an idle connection to be terminated.</p> <p>If enabled, enter the idle time-out period (in minutes) in the field provided. After the connection to your ISP has been idle for this time period, the connection will be terminated.</p>
<b>MAC Address</b>	
<b>MAC Address</b>	<p>Also called <i>Network Adapter Address</i> or <i>Physical Address</i>. This is a low-level identifier, as seen from the WAN port.</p> <p>Normally there is no need to change this, but some ISPs require a particular value, often that of the PC initially used for Internet access.</p> <p>You can use the <i>Copy from PC</i> button to copy your PC's address into this field, the <i>Default</i> button to insert the default value, or enter a value directly.</p>

## LAN Screen

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



**Figure 8: LAN Screen**

### Data - LAN Screen

TCP/IP	
<b>IP Address</b>	IP address for the Broadband VPN 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.
<b>Subnet Mask</b>	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 Broadband VPN Gateway is attached (the same value as the PCs on that LAN segment).
<b>DHCP Server</b>	<ul style="list-style-type: none"> <li>• If Enabled, the Broadband VPN Gateway will allocate IP Addresses to PCs (DHCP clients) on your LAN when they start up. The default (and recommended) value is Enabled.</li> <li>• If you are already using a DHCP Server, this setting must be Disabled, and the existing DHCP server must be re-configured to treat the Broadband VPN Gateway as the default Gateway. See the following section for further details.</li> <li>• The <b>Start IP Address</b> and <b>Finish IP Address</b> fields set the values used by the DHCP server when allocating IP Addresses to DHCP clients. This range also determines the number of DHCP clients supported.</li> </ul> <p>See the following section for further details on using DHCP.</p>
Buttons	
<b>Save</b>	Save the data on screen.
<b>Cancel</b>	The "Cancel" button will discard any data you have entered and reload the file from the Broadband VPN Gateway.

## 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 Broadband VPN 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 Broadband VPN 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 Broadband VPN Gateway 's *DHCP Server* function.
- Set the range of IP Addresses allocated to PCs by the DHCP Server function.



**Note!**

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

### Using another DHCP Server

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

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

### To Configure your PCs to use DHCP

This is the default setting for TCP/IP under Windows 95/98/ME.

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

# 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 Broadband VPN Gateway.

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

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

- By default, the Broadband VPN 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:**

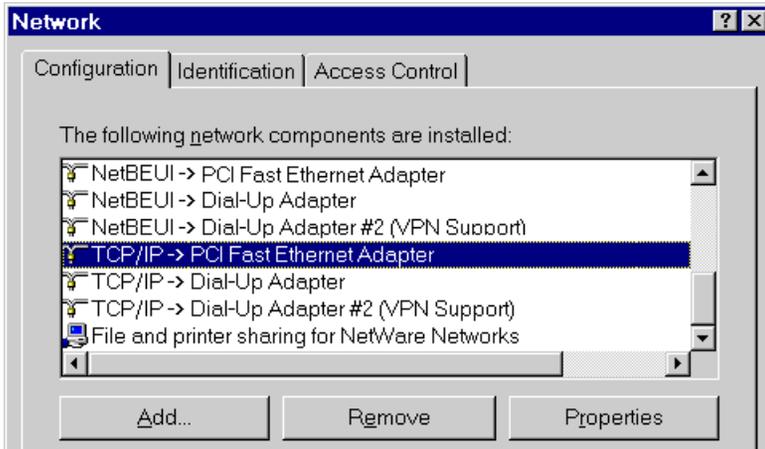
- The *Gateway* must be set to the IP address of the Broadband VPN Gateway
- The *DNS* should be set to the address provided by your ISP.



**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.**

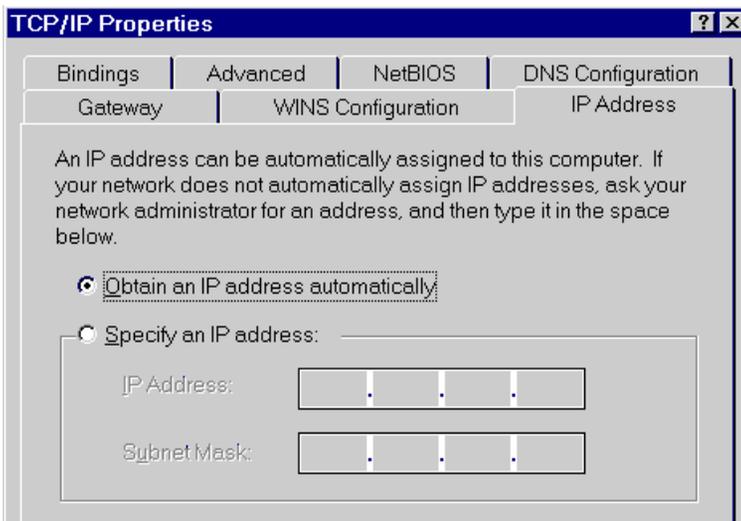
## Checking TCP/IP Settings - Windows 9x/ME:

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



**Figure 9: 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 10: IP Address (Win 95)**

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

### Using DHCP

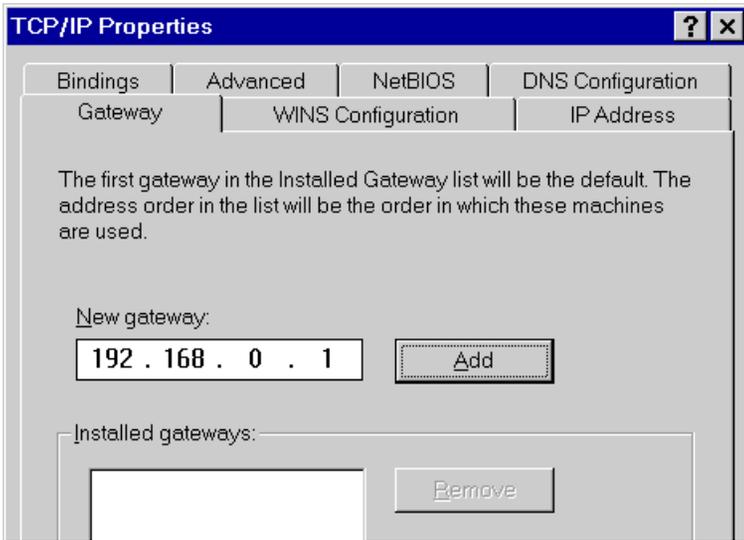
To use DHCP, select the radio button *Obtain an IP Address automatically*. This is the default Windows setting. **Using this is recommended.** By default, the Broadband VPN Gateway will act as a DHCP Server.

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

### Using "Specify an IP Address"

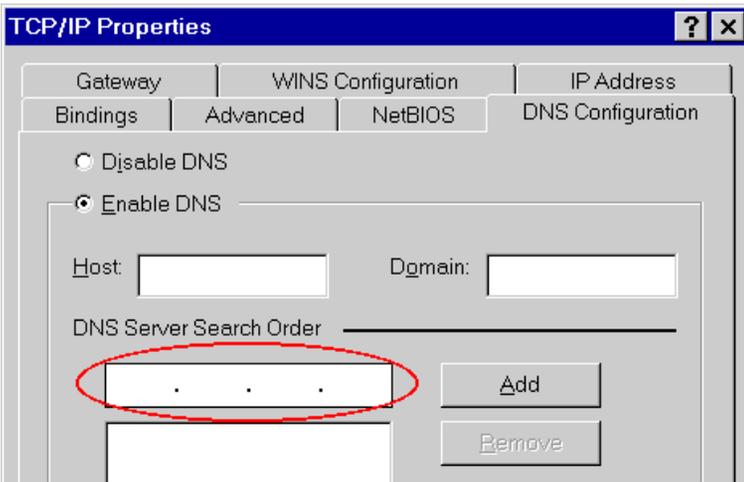
If your PC is already configured, check with your network administrator before making the following changes:

- On the *Gateway* tab, enter the Broadband VPN 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 Broadband VPN Gateway.



**Figure 11: 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 12: DNS Tab (Win 95/98)**

## Checking TCP/IP Settings - Windows NT4.0

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

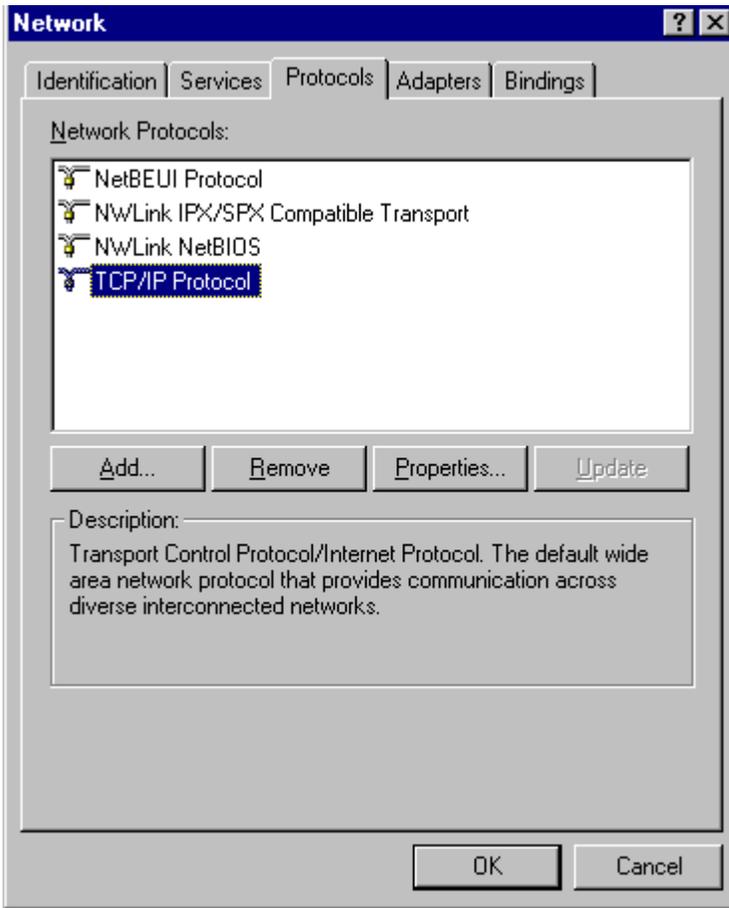
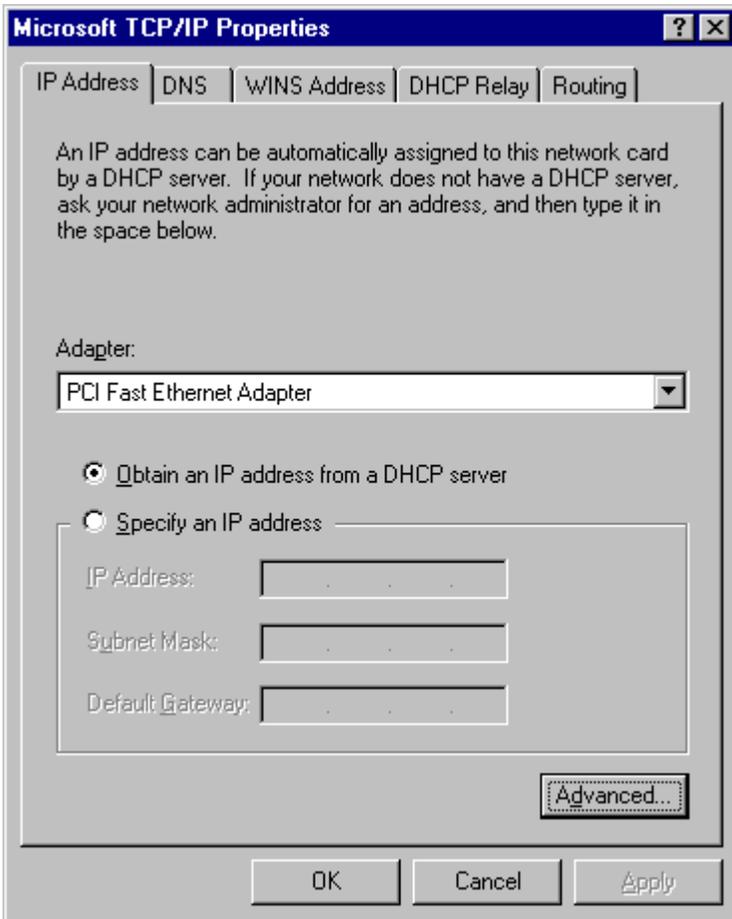


Figure 13: Windows NT4.0 - TCP/IP

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



**Figure 14: 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**

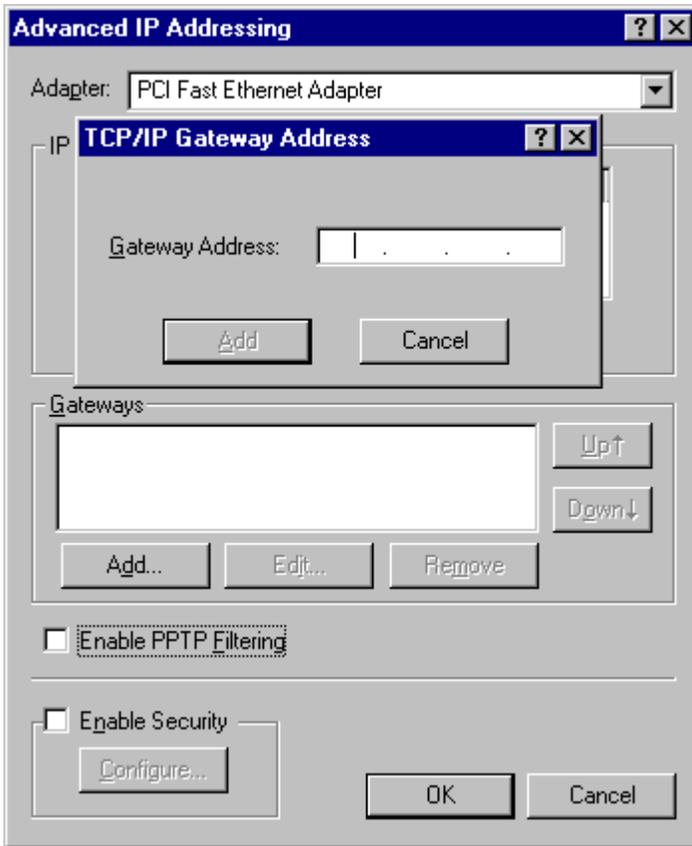
This is the default Windows setting. **Using this is recommended.** By default, the Broadband VPN Gateway will act as a DHCP Server.

Restart your PC to ensure it obtains an IP Address from the Broadband VPN 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 Broadband VPN 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 Broadband VPN Gateway's IP address, as shown in Figure 15 below.
  - If necessary, use the *Up* button to make the Broadband VPN Gateway the first entry in the *Gateways* list.



**Figure 15 - 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.

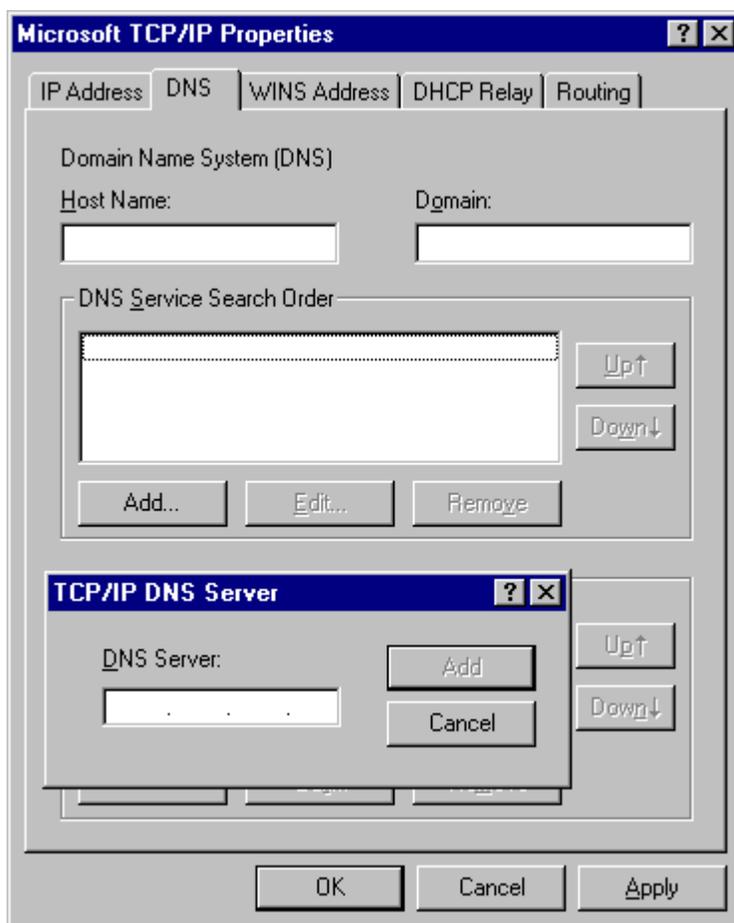
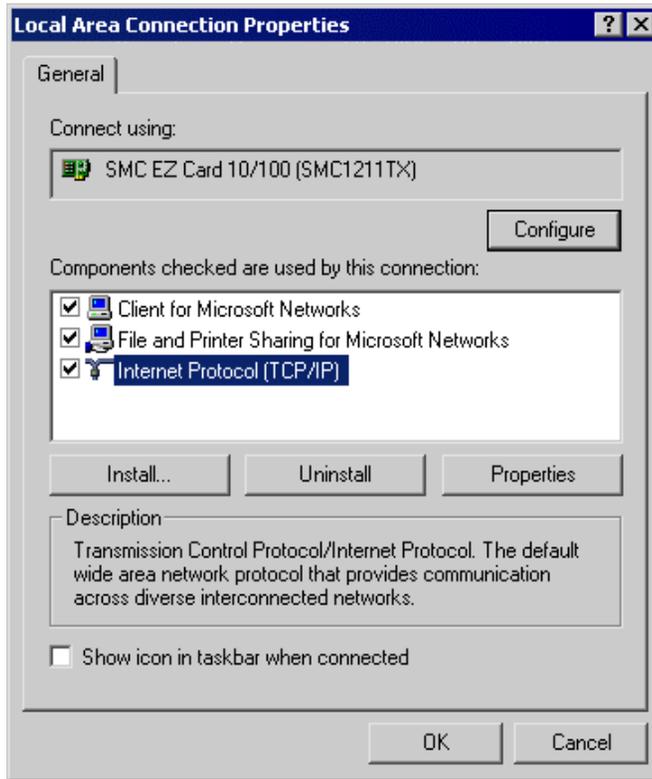


Figure 16: Windows NT4.0 - DNS

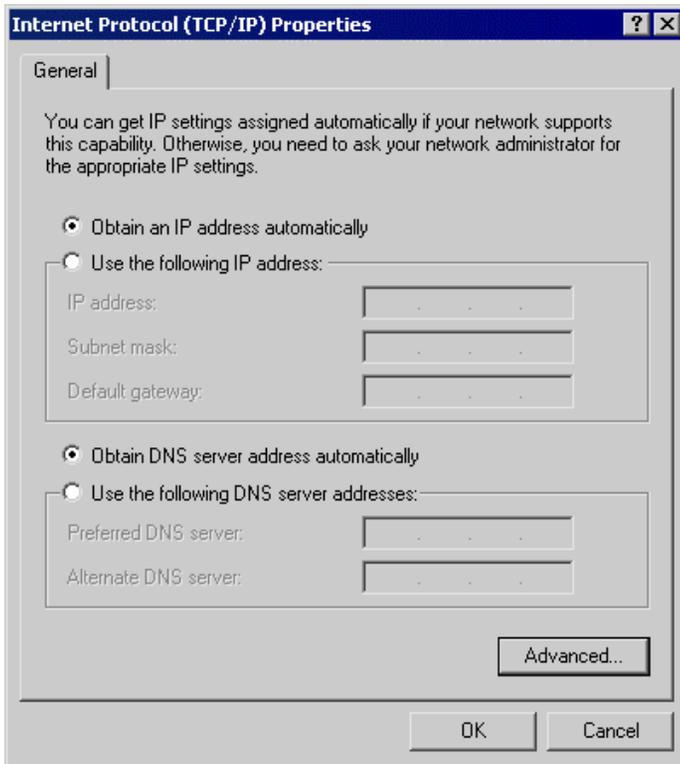
## Checking TCP/IP Settings - Windows 2000:

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 17: 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 18: 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 Broadband VPN Gateway will act as a DHCP Server.

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

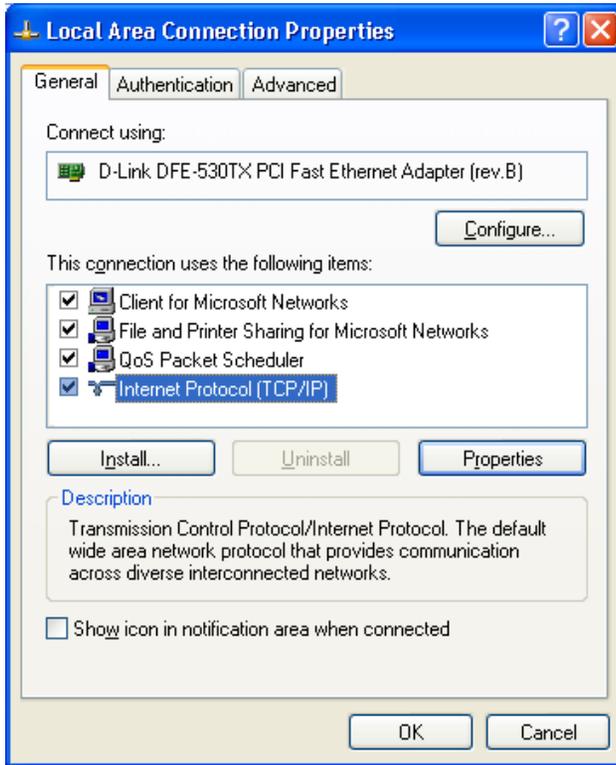
### Using a fixed IP Address ("Use the following IP Address")

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

- Enter the Broadband VPN 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 Broadband VPN 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*.

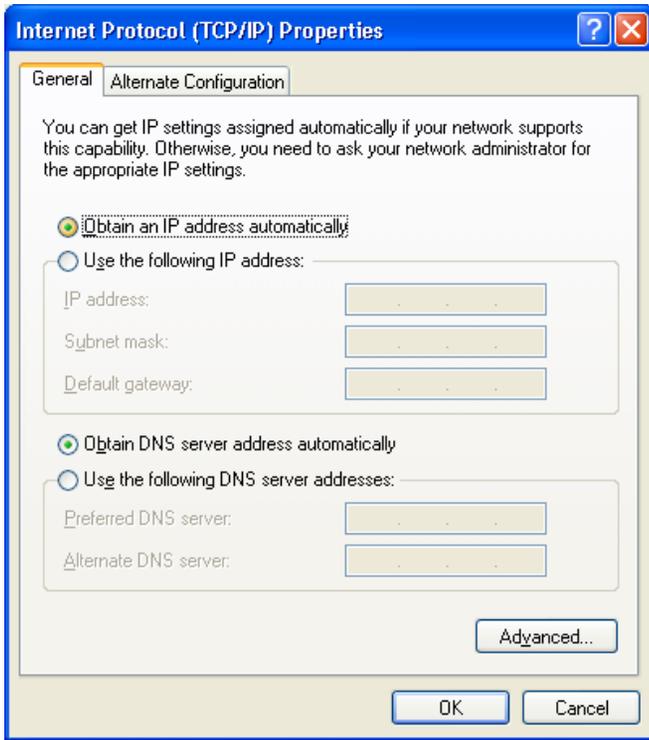
## Checking TCP/IP Settings - Windows XP

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 19: 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 20: 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 Broadband VPN Gateway will act as a DHCP Server.

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

## Macintosh Clients

From your Macintosh, you can access the Internet via the Broadband VPN 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 Broadband VPN Gateway's IP Address.
- Ensure your DNS settings are correct.

## Linux Clients

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

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

# Chapter 5

# Operation and Status



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

## Operation

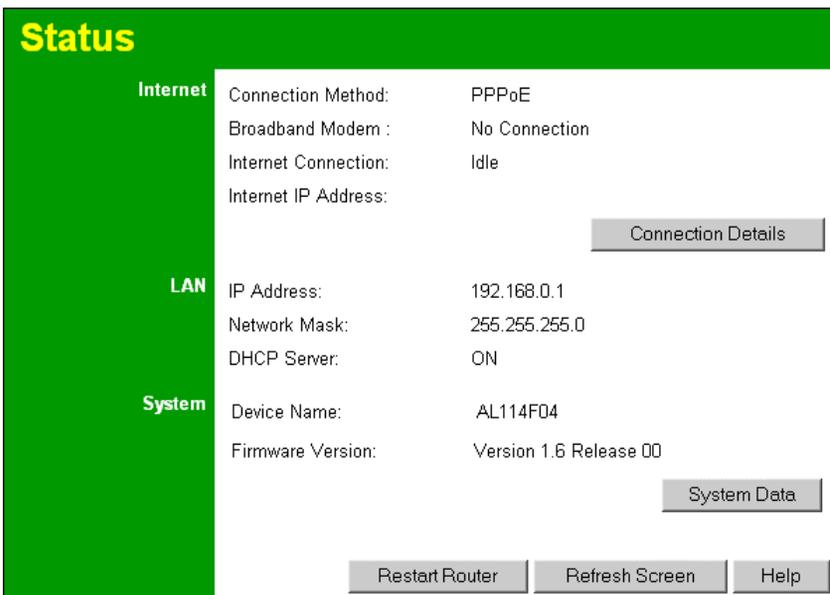
Once both the Broadband VPN Gateway and the PCs are configured, operation is automatic.

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 Broadband VPN Gateway'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.



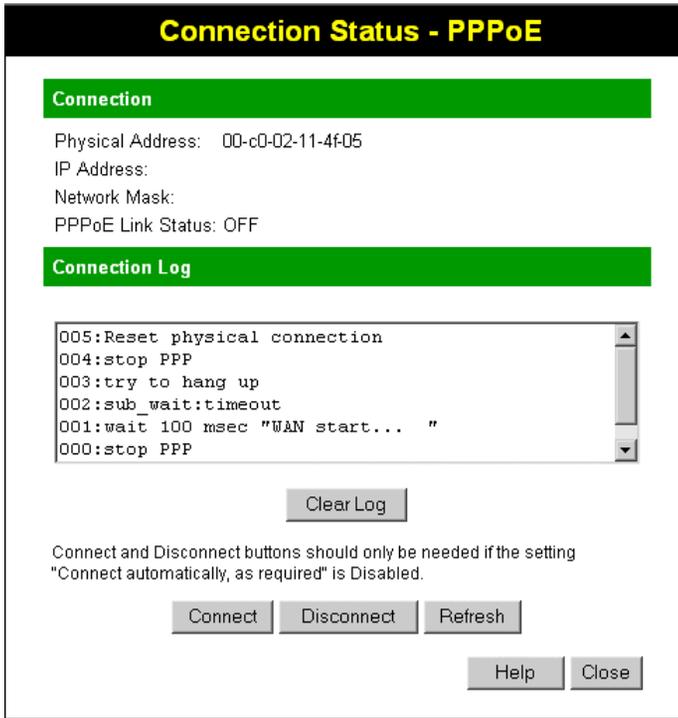
**Figure 21: Status Screen**

**Data - Status Screen**

<b>Internet</b>	
<b>Connection Method</b>	This indicates the current connection method, as set in the Setup Wizard.
<b>Broadband Modem</b>	This shows the connection status of the modem.
<b>Internet Connection</b>	<p>Current connection status:</p> <ul style="list-style-type: none"> <li>• Active</li> <li>• Idle</li> <li>• Unknown</li> <li>• Failed</li> </ul> <p>If there is an error, you can click the "Connection Details" button to find out more information.</p>
<b>Internet IP Address</b>	This IP Address is allocated by the ISP (Internet Service Provider).
<b>"Connection Details" Button</b>	Click this button to open a sub-window and view a detailed description of the current connection. Depending on the type of connection, a "log" may also be available.
<b>LAN</b>	
<b>IP Address</b>	The IP Address of the Broadband VPN Gateway.
<b>Network Mask</b>	The Network Mask (Subnet Mask) for the IP Address above.
<b>DHCP Server</b>	<p>This shows the status of the DHCP Server function - either "Enabled" or "Disabled".</p> <p>For additional information about the PCs on your LAN, and the IP addresses allocated to them, use the <i>PC Database</i> option on the <i>Advanced</i> menu.</p>
<b>System</b>	
<b>Device Name</b>	This displays the current name of the Broadband VPN Gateway.
<b>Firmware Version</b>	The current version of the firmware installed in the Broadband VPN Gateway.
<b>"System Data" Button</b>	Clicking this button will open a Window which lists all system details and settings.
<b>Buttons</b>	
<b>Connection Details</b>	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.
<b>System Data</b>	Display all system information in a sub-window.
<b>Restart Router</b>	Restart (reboot) the Router. You will have to wait for the restart to be completed before continuing.
<b>Refresh Screen</b>	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 22: PPPoE Status Screen**

### Data - PPPoE Screen

Connection	
<b>Physical Address</b>	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.)
<b>IP Address</b>	The IP Address of this device, as seen by Internet users. This address is allocated by your ISP (Internet Service Provider).
<b>Network Mask</b>	The Network Mask associated with the IP Address above.
<b>PPPoE Link Status</b>	<p>This indicates whether or not the connection is currently established.</p> <ul style="list-style-type: none"> <li>• If the connection does not exist, the "Connect" button can be used to establish a connection.</li> <li>• If the connection currently exists, the "Disconnect" button can be used to break the connection.</li> </ul>
Connection Log	
<b>Connection Log</b>	<ul style="list-style-type: none"> <li>• The Connection Log shows status messages relating to the existing connection.</li> <li>• The most common messages are listed in the table below.</li> <li>• The "Clear Log" button will restart the Log, while the Re-</li> </ul>

	fresh button will update the messages shown on screen.
<b>Buttons</b>	
<b>Connect</b>	If not connected, establish a connection to your ISP.
<b>Disconnect</b>	If connected to your ISP, hang up the connection.
<b>Clear Log</b>	Delete all data currently in the Log. This will make it easier to read new messages.
<b>Refresh</b>	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.

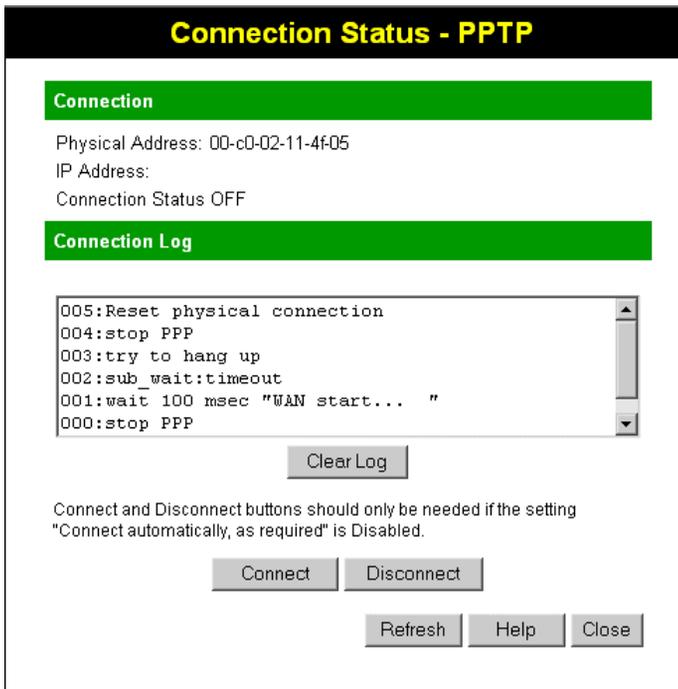


Figure 23: PPTP Status Screen

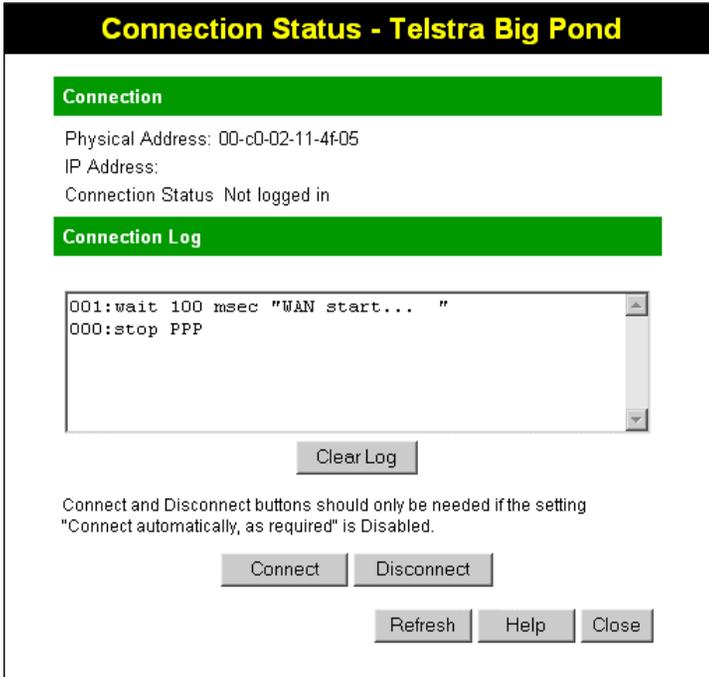
### Data - PPTP Screen

Connection	
<b>Physical Address</b>	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.)
<b>IP Address</b>	The IP Address of this device, as seen by Internet users. This address is allocated by your ISP (Internet Service Provider).
<b>PPTP Status</b>	This indicates whether or not the connection is currently established. <ul style="list-style-type: none"> <li>• If the connection does not exist, the "Connect" button can be used to establish a connection.</li> <li>• If the connection currently exists, the "Disconnect" button can be used to break the connection.</li> </ul>
Connection Log	
<b>Connection Log</b>	<ul style="list-style-type: none"> <li>• The Connection Log shows status messages relating to the existing connection.</li> <li>• The "Clear Log" button will restart the Log, while the Refresh button will update the messages shown on screen.</li> </ul>
Buttons	
<b>Connect</b>	If not connected, establish a connection to your ISP.

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

## Connection Status - Telstra Big Pond

An example screen is shown below.



**Figure 24: Telstra Big Pond Status Screen**

### Data - Telstra Big Pond Screen

Connection	
<b>Physical Address</b>	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.)
<b>IP Address</b>	The IP Address of this device, as seen by Internet users. This address is allocated by your ISP (Internet Service Provider).
<b>Connection Status</b>	<p>This indicates whether or not the connection is currently established.</p> <ul style="list-style-type: none"> <li>If the connection does not exist, the "Connect" button can be used to establish a connection.</li> <li>If the connection currently exists, the "Disconnect" button can be used to break the connection.</li> <li>Normally, it is not necessary to use the Connect and Disconnect buttons unless the setting "Connect automatically, as</li> </ul>

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**

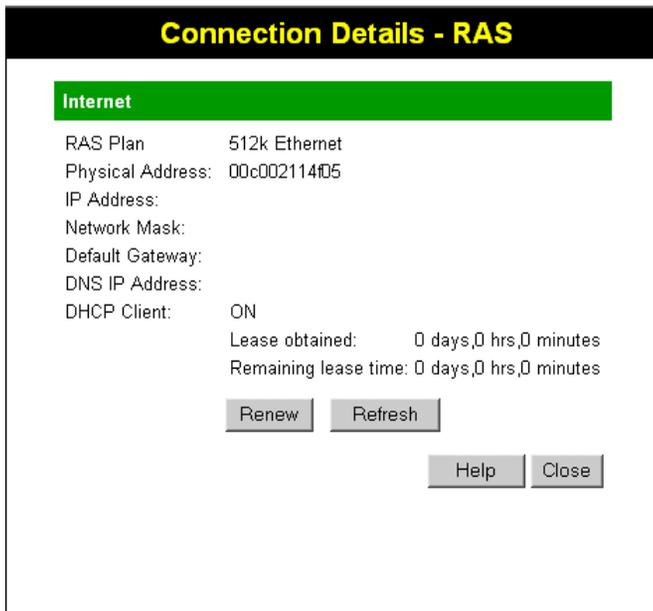
Delete all data currently in the Log. This will make it easier to read new messages.

**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 25: Connection Details - SingTel RAS**

**Data - SingTel RAS Screen**

**Internet**

**RAS Plan**

The RAS Plan which is currently used.

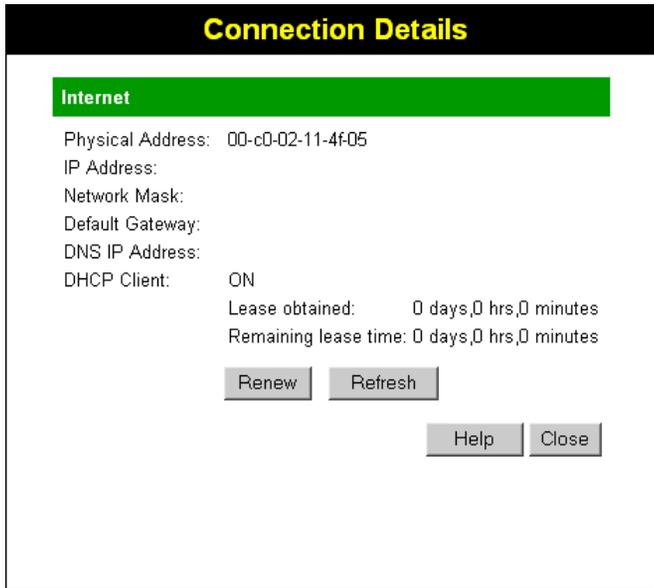
**Physical Address**

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.)

<b>IP Address</b>	The IP Address of this device, as seen by Internet users. This address is allocated by your ISP (Internet Service Provider).
<b>Network Mask</b>	The Network Mask associated with the IP Address above.
<b>Default Gateway</b>	The IP Address of the remote Gateway or Router associated with the IP Address above.
<b>DNS IP Address</b>	The IP Address of the Domain Name Server which is currently used.
<b>DHCP Client</b>	<p>This will show "Enabled" or "Disabled", depending on whether or not this device is functioning as a DHCP client.</p> <p>If "Enabled" the "Remaining lease time" field indicates when the IP Address allocated by the DHCP Server will expire. The lease is automatically renewed on expiry; use the "Renew" button if you wish to manually renew the lease immediately.</p>
<b>Buttons</b>	
<b>Release/Renew Button will display EITHER "Release" OR "Renew"</b>	<p>This button is only useful if the IP address shown above is allocated automatically on connection. (Dynamic IP address). If you have a Fixed (Static) IP address, this button has no effect.</p> <ul style="list-style-type: none"> <li>• If the ISP's DHCP Server has NOT allocated an IP Address for the Broadband VPN Gateway, this button will say "Renew". Clicking the "Renew" button will attempt to re-establish the connection and obtain an IP Address from the ISP's DHCP Server.</li> <li>• If an IP Address has been allocated to the Broadband VPN Gateway (by the ISP's DHCP Server), this button will say "Release". Clicking the "Release" button will break the connection and release the IP Address.</li> </ul>
<b>Refresh</b>	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 26: Connection Details - Fixed/Dynamic IP Address**

### Data - Fixed/Dynamic IP address Screen

Internet	
<b>Physical Address</b>	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.)
<b>IP Address</b>	The IP Address of this device, as seen by Internet users. This address is allocated by your ISP (Internet Service Provider).
<b>Network Mask</b>	The Network Mask associated with the IP Address above.
<b>Default Gateway</b>	The IP Address of the remote Gateway or Router associated with the IP Address above.
<b>DNS IP Address</b>	The IP Address of the Domain Name Server which is currently used.
<b>DHCP Client</b>	<p>This will show "Enabled" or "Disabled", depending on whether or not this device is functioning as a DHCP client.</p> <p>If "Enabled" the "Remaining lease time" field indicates when the IP Address allocated by the DHCP Server will expire. The lease is automatically renewed on expiry; use the "Renew" button if you wish to manually renew the lease immediately.</p>
Buttons	
<b>Release/Renew Button will display EITHER "Release"</b>	<p>This button is only useful if the IP address shown above is allocated automatically on connection. (Dynamic IP address). If you have a Fixed (Static) IP address, this button has no effect.</p> <ul style="list-style-type: none"> <li>• If the ISP's DHCP Server has NOT allocated an IP Address for</li> </ul>

<b>OR "Renew"</b>	the Broadband VPN Gateway, 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. <ul style="list-style-type: none"><li>• If an IP Address has been allocated to the Broadband VPN Gateway (by the ISP's DHCP Server), this button will say "Release". Clicking the "Release" button will break the connection and release the IP Address.</li></ul>
<b>Refresh</b>	Update the data shown on screen.

# Chapter 6

## Internet Features

# 6

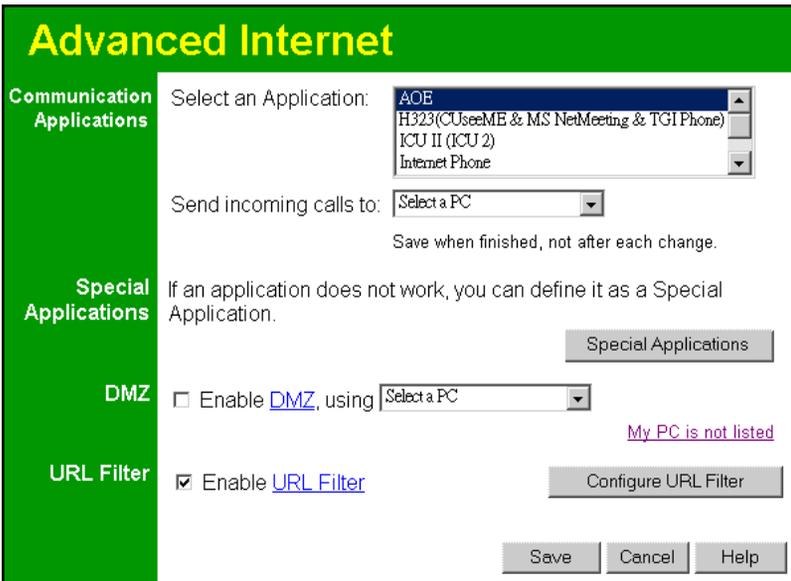
*This Chapter explains when and how to use the Broadband VPN Gateway's "Internet" Features.*

### Overview

The following advanced features are provided.

- Advanced Internet
  - Communication Applications
  - Special Applications
  - DMZ
  - URL filter
- Dynamic DNS
- Virtual Servers
- Options

### Advanced Internet Screen



**Figure 27: Internet Screen**

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

- Communication Applications
- Special Applications
- DMZ
- URL filter

## Communication Applications

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

## Special Applications

If you use Internet applications which use non-standard connections or port numbers, you may find that they do not function correctly because they are blocked by the Broadband VPN Gateway'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.

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

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

Special Applications

Special Applications can only be used by 1 user at any time.

		Incoming Ports			Outgoing Ports		
	Name	Type	Start	Finish	Type	Start	Finish
1.	<input type="checkbox"/> <input style="width: 100%;" type="text"/>	TCP ▾	<input style="width: 50%;" type="text"/>	<input style="width: 50%;" type="text"/>	TCP ▾	<input style="width: 50%;" type="text"/>	<input style="width: 50%;" type="text"/>
2.	<input type="checkbox"/> <input style="width: 100%;" type="text"/>	TCP ▾	<input style="width: 50%;" type="text"/>	<input style="width: 50%;" type="text"/>	TCP ▾	<input style="width: 50%;" type="text"/>	<input style="width: 50%;" type="text"/>
3.	<input type="checkbox"/> <input style="width: 100%;" type="text"/>	TCP ▾	<input style="width: 50%;" type="text"/>	<input style="width: 50%;" type="text"/>	TCP ▾	<input style="width: 50%;" type="text"/>	<input style="width: 50%;" type="text"/>
4.	<input type="checkbox"/> <input style="width: 100%;" type="text"/>	TCP ▾	<input style="width: 50%;" type="text"/>	<input style="width: 50%;" type="text"/>	TCP ▾	<input style="width: 50%;" type="text"/>	<input style="width: 50%;" type="text"/>
5.	<input type="checkbox"/> <input style="width: 100%;" type="text"/>	TCP ▾	<input style="width: 50%;" type="text"/>	<input style="width: 50%;" type="text"/>	TCP ▾	<input style="width: 50%;" type="text"/>	<input style="width: 50%;" type="text"/>
6.	<input type="checkbox"/> <input style="width: 100%;" type="text"/>	TCP ▾	<input style="width: 50%;" type="text"/>	<input style="width: 50%;" type="text"/>	TCP ▾	<input style="width: 50%;" type="text"/>	<input style="width: 50%;" type="text"/>

**Figure 28: Special Applications Screen**

### Data - Special Applications Screen

<b>Checkbox</b>	Use this to Enable or Disable this Special Application as required.
<b>Name</b>	Enter a descriptive name to identify this Special Application.
<b>Incoming Ports</b>	<ul style="list-style-type: none"> <li>• <b>Type</b> - Select the protocol (TCP or UDP) used when you receive data from the special application or service. (Note: Some applications use different protocols for outgoing and incoming data).</li> <li>• <b>Start</b> - Enter the beginning of the range of port numbers used by the application server, for data you receive. If the application uses a single port number, enter it in both the "Start" and "Finish" fields.</li> <li>• <b>Finish</b> - Enter the end of the range of port numbers used by the application server, for data you receive.</li> </ul>
<b>Outgoing Ports</b>	<ul style="list-style-type: none"> <li>• <b>Type</b> - Select the protocol (TCP or UDP) used when you send data to the remote system or service.</li> <li>• <b>Start</b> - Enter the beginning of the range of port numbers used by the application server, for data you send to it. If the application uses a single port number, enter it in both the "Start" and "Finish" fields.</li> <li>• <b>Finish</b> - Enter the end of the range of port numbers used by the application server, for data you send to it. If the application uses a single port number, enter it in both the "Start" and "Finish" fields.</li> </ul>

### 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.**

## DMZ

This feature, if enabled, allows one (1) computer on your LAN to be exposed to all users on the Internet, allowing 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".
- The DMZ feature can be Enabled and Disabled on the *Advanced Internet* screen.



**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.**

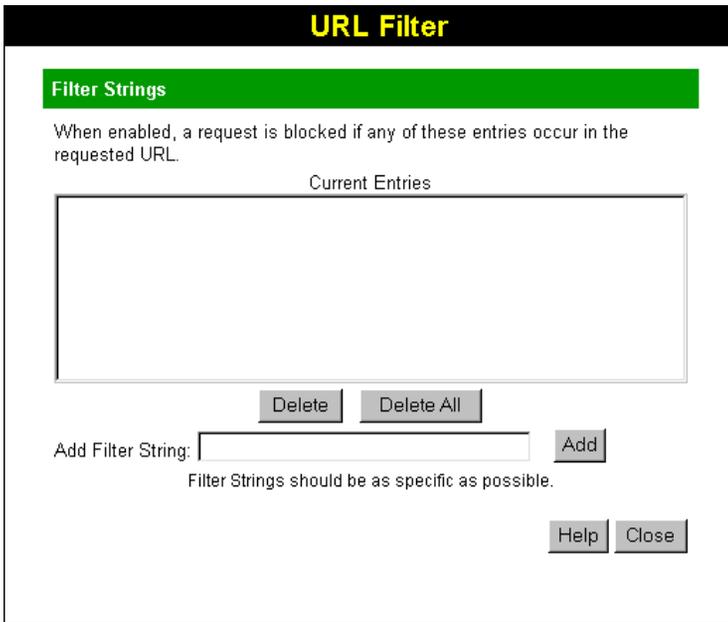
## URL Filter

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 29: URL Filter Screen**

### Data - URL Filter Screen

Filter Strings	
<b>Current Entries</b>	This lists any existing entries. If you have not entered any values, this list will be empty.
<b>Add Filter String</b>	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	
<b>Delete/Delete All</b>	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.)
<b>Add</b>	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 <http://www.dyndns.org> (Registration is free). Your password will be E-mailed to you.
2. After registration, use the "Create New Host" option (at [www.dyndns.org](http://www.dyndns.org)) to request your desired Domain name.
3. Enter your data from [www.dyndns.org](http://www.dyndns.org) in the Broadband VPN Gateway 's DDNS screen.
4. The Broadband VPN Gateway will then automatically ensure that your current IP Address is recorded at <http://www.dyndns.org>
5. From the Internet, users will be able to connect to your Virtual Servers (or DMZ PC) using your Domain name, as shown on this screen.

## Dynamic DNS Screen

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

**DDNS (Dynamic DNS)**

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

**DDNS Data** User name is set when you register; your password is E-mailed to you.

User Name:

Password:

Domain Name:  .   
Domain name allocated to you by [www.dyndns.org](http://www.dyndns.org)

DDNS Status:

Save Cancel Help

Figure 30: DDNS Screen

## Data - Dynamic DNS Screen

DDNS Service	
DDNS Service	<ul style="list-style-type: none"><li>• You must sign up first to create a new account before using the service. The service is free.</li><li>• Click this link to connect to the <a href="http://www.dyndns.org">www.dyndns.org</a> Web site.</li><li>• Your initial password will be E-mailed to you; you can change this later if you wish.</li><li>• After registration, use the "Create New Host" link (on the</li></ul>

---

	www.dyndns.org Web site) to request a domain name.
<b>DDNS Data</b>	
<b>User Name</b>	Enter the "User name" specified at the www.dyndns.org Web site when you registered.
<b>Password</b>	Enter your current password for www.dyndns.org
<b>Domain Name</b>	<ul style="list-style-type: none"><li>• Enter your domain name, as allocated at www.dyndns.org.</li><li>• The name should consist only of letters and the hyphen (dash). Using any other characters may cause problems..</li></ul>
<b>DDNS Status</b>	<p>This message is returned by the DDNS Server at www.dyndns.org</p> <ul style="list-style-type: none"><li>• Normally, this message should be "Update successful" (current IP address was updated on the www.dyndns.org server).</li><li>• If the message is "No host", this indicates the host name entered was not allocated to you. You need to connect to www.dyndns.org and correct this problem.</li></ul>

## 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.

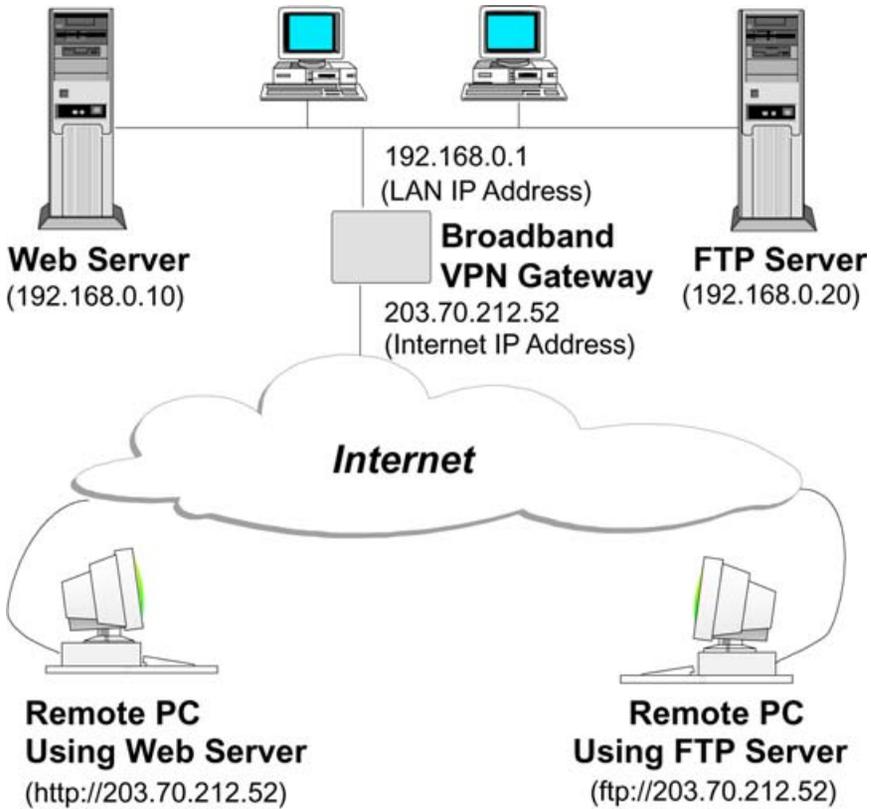


Figure 31: Virtual Servers

### 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.

## Using the DMZ port for Virtual Servers

You should connect your Virtual Servers to the DMZ port, for the following reasons:

- Traffic passing between the DMZ and LAN passes through the firewall. The firewall will protect your LAN if your Server is compromised and used to launch an attack on your LAN.
- For each enabled Virtual Server, a firewall rule to allow incoming traffic from the Internet (WAN) to the DMZ is automatically created. If the Server is connected to the LAN (hub) ports, you must add the firewall rule manually.

Note that the DMZ port is a normal port, not an "uplink" port. If connecting to a hub, connect to a standard port on the hub.

## Virtual Servers Screen

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

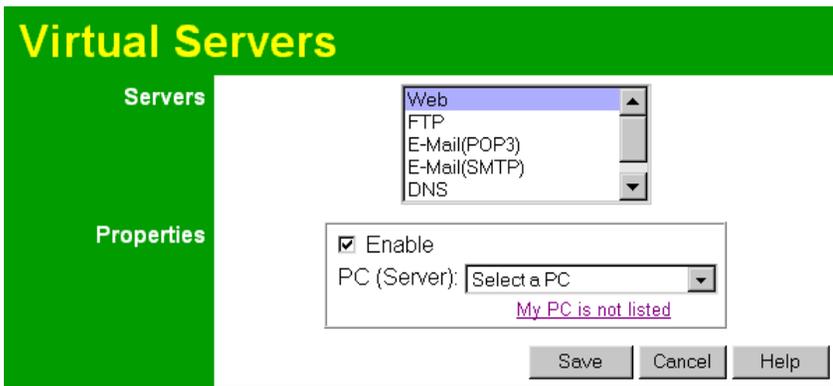


Figure 32: Virtual Servers Screen

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	
<b>Servers</b>	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	
<b>Enable</b>	Use this to Enable or Disable support for this Server, as required. <ul style="list-style-type: none"> <li>• If Enabled, any incoming connections will be forwarded to the selected PC.</li> <li>• If Disabled, any incoming connection attempts will be blocked.</li> </ul>
<b>PC (Server)</b>	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.

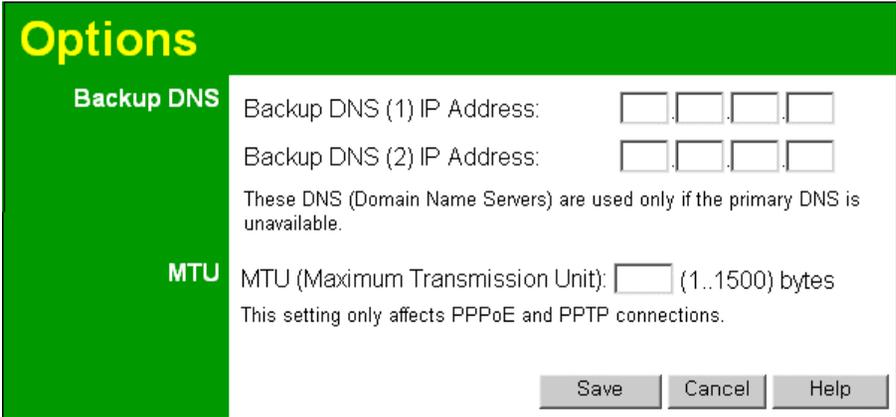


Figure 33: Options Screen

### 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 security configuration section of the "Security" menu.*

### Overview

The following advanced configurations are provided.

- Admin Login
- Access Control
- Firewall Rules
- Logs
- Security Options
- Scheduling
- Services

### Admin Login

The Admin Login screen allows you to assign a user name and password to the Broadband VPN Gateway .

**Admin Login**

**Admin Login**

The admin login protects the configuration data. Once set (recommended), you will be prompted for the user name and password when you connect.

Login name:

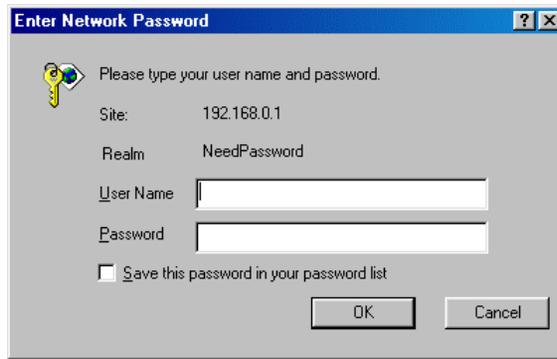
New password:

Verify password:

**Figure 34: Admin Login Screen**

1. The default login name is "admin". Change this to the desired value.
2. The default password is blank (no password). 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 Broadband VPN Gateway, as shown below.



**Figure 35: Password Dialog**

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

## Access Control

This feature is accessed by the *Access Control* link on the 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.

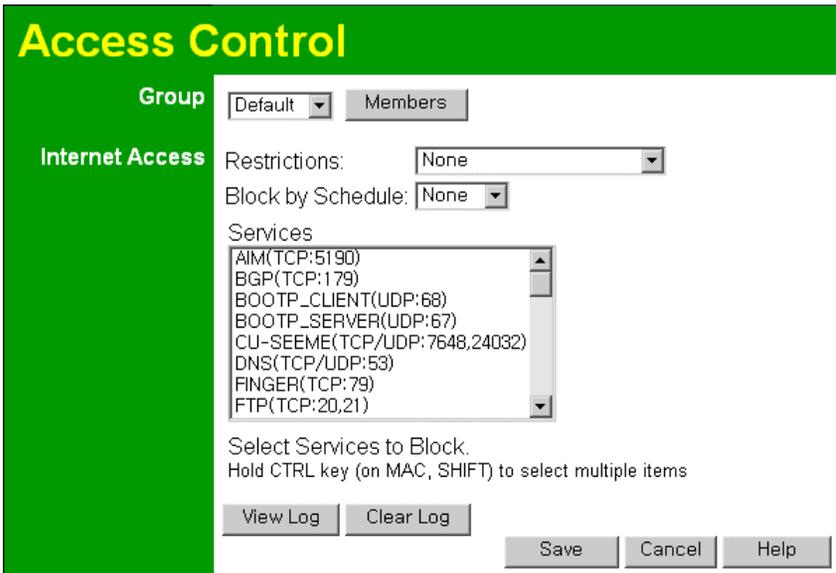


Figure 36: Access Control Screen

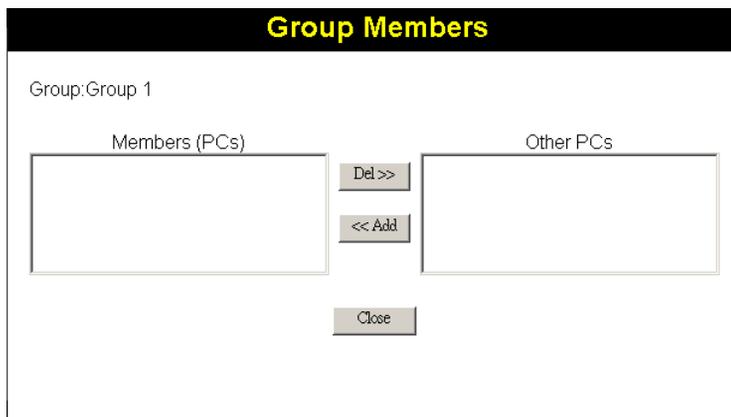
### Data - Access Control Screen

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.

<b>"Members" Button</b>	<p>Click this button to add or remove members from the current Group.</p> <ul style="list-style-type: none"> <li>• If the current group is "Default", then members can not be added or deleted. This group contains PCs not allocated to any other group.</li> <li>• To remove PCs from the Default Group, assign them to another Group.</li> <li>• To assign PCs to the Default Group, delete them from the Group they are currently in.</li> </ul> <p>See the following section for details of the <i>Group Members</i> screen.</p>
<b>Internet Access</b>	
<b>Restrictions</b>	<p>Select the desired options for the current group:</p> <ul style="list-style-type: none"> <li>• None - Nothing is blocked. Use this to create the least restrictive group.</li> <li>• Block all Internet access - All traffic via the WAN port is blocked. Use this to create the most restrictive group.</li> <li>• Block selected Services - You can select which Services are to block. Use this to gain fine control over the Internet access for a group.</li> </ul>
<b>Block by Schedule</b>	<p>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.)</p>
<b>Services</b>	<p>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.)</p>
<b>Buttons</b>	
<b>Members</b>	<p>Click this button to add or remove members from the current Group.</p> <p>If the current group is "Default", then members can not be added or deleted. This group contains PCs not allocated to any other group.</p> <p>See the following section for details of the <i>Group Members</i> screen.</p>
<b>Save</b>	<p>Save the data on screen.</p>
<b>Cancel</b>	<p>Reverse any changes made since the last "Save".</p>
<b>View Log</b>	<p>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.</p>
<b>Clear Log</b>	<p>Click this to clear and restart the "Access Control" log, making new entries easier to read.</p>

## Group Members Screen

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



**Figure 37: 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:

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

## 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

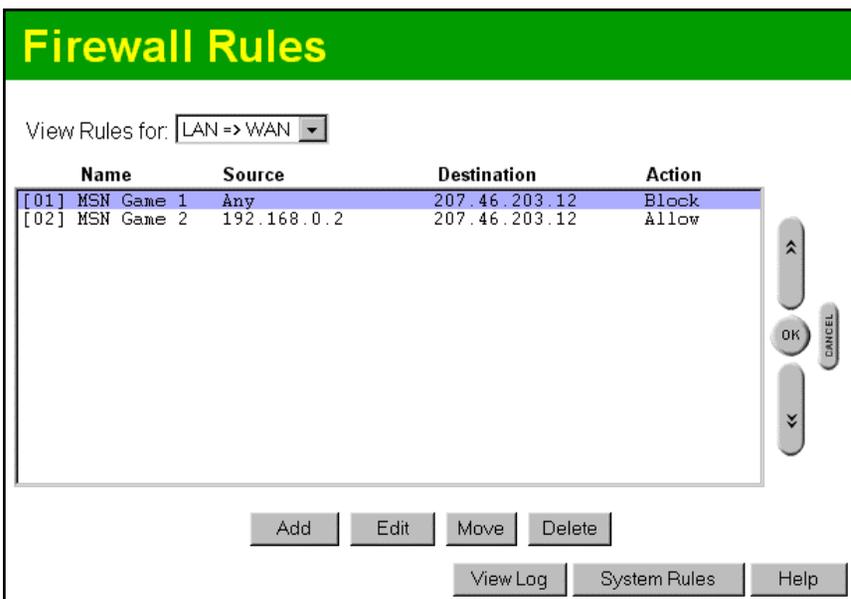
Click the *Firewall Rules* option on the Security menu to see a screen like the following example. This example contains two (2) rules for outgoing traffic.



**Note!**

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.

For example, the screen below shows a rule blocking all traffic to a MSN Game Server, followed by another rule allowing access by a specific PC.



**Figure 38: 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.

<b>Data</b>	<p>For each rule, the following data is shown:</p> <ul style="list-style-type: none"> <li>• <b>Name</b> - The name you assigned to the rule.</li> <li>• <b>Source</b> - 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.</li> <li>• <b>Destination</b> - 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.</li> <li>• <b>Action</b> - Action will be "Forward" or "Block"</li> </ul>
<b>Add</b>	To add a new rule, click the "Add" button, and complete the resulting screen. See the following section for more details.
<b>Edit</b>	To Edit or modify an existing rule, select it and click the "Edit" button.
<b>Move</b>	<p>There are 2 ways to change the order of rules</p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• Click "Move" to directly specify a new location for the selected rule.</li> </ul>
<b>Delete</b>	To delete an existing rule, select it and click the "Delete" button.
<b>View Log</b>	Clicking the "View Log" button will open a new window and display the Firewall log.
<b>System Rules</b>	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 39: Define Firewall Rule**

### Data - Define Firewall Rule Screen

<b>Name</b>	Enter a suitable name for this rule.
<b>Type</b>	This determines the source and destination ports for traffic covered by this rule. Select the desired option.
<b>Source IP</b>	<p>These settings determine which traffic, based on their source IP address, is covered by this rule.</p> <p>Select the desired option:</p> <ul style="list-style-type: none"> <li>• Any - All traffic from the source port is covered by this rule.</li> <li>• Single address - Enter the required IP address in the "Start IP address" field". You can ignore the "Subnet Mask" field.</li> <li>• 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.</li> <li>• Subnet address - If this option is selected, enter the required mask in the "Subnet Mask" field.</li> </ul>

<b>Dest IP</b>	<p>These settings determine which traffic, based on their destination IP address, is covered by this rule.</p> <p>Select the desired option:</p> <ul style="list-style-type: none"> <li>• Any - All traffic from the source port is covered by this rule.</li> <li>• Single address - Enter the required IP address in the "Start IP address" field". You can ignore the "Subnet Mask" field.</li> <li>• 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.</li> <li>• Subnet address - If this option is selected, enter the required mask in the "Subnet Mask" field.</li> </ul>
<b>Services</b>	<p>Select the desired Service or Services. This determines which packets are covered by this rule, based on the protocol (TCP 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.</p>
<b>Action</b>	<p>Select the desired action for packets covered by this rule:</p>
<b>Log</b>	<p>This determines whether packets covered by this rule are logged. Select the desired option.</p>

## Logs

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

Figure 40: Logs Screen

### Data - Logs Screen

Enable Logs	
<b>DoS Attacks</b>	If enabled, this log will show details of DoS (Denial of Service) attacks which have been blocked by the built-in Firewall.
<b>Internet Connections</b>	If selected, Outgoing Internet connections are logged. Normally, the (Internet) "Destination" will be shown as an IP address. But if the "URL Filter" is enabled, the "Destination" will be shown as a URL.

<b>Access Control</b>	If enabled, the log will include attempted outgoing connections which have been blocked by the "Access Control" feature.
<b>Firewall Rules</b>	If enabled, the log will details of packets blocked by user-defined Firewall rules. Logging can be set for each rule individually. Only rules which have logging enabled will be included.
<b>VPN</b>	If enabled, the VPN log will record incoming and outgoing VPN connections.
<b>Timezone</b>	Select the correct Timezone for your location. This is required for the date/time shown on the logs to be correct.
<b>E-Mail Logs</b>	
<b>Send E-mail alert</b>	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.
<b>E-mail Logs</b>	You can choose to have the logs E-mailed to you, by enabling either or both checkboxes. If enabled, the Log will send to the specified E-mail address. The interval between E-mails is determined by the "Send" setting.
<b>Send</b>	Select the desired option for sending the log by E-mail. <ul style="list-style-type: none"> <li>• <b>When log is full</b> - The time is not fixed. The log will be sent when the log is full, which will depend on the volume of traffic.</li> <li>• <b>Every day, Every Monday ...</b> - The log is sent on the interval specified. <ul style="list-style-type: none"> <li>• If "Every day" is selected, the log is sent at the time specified.</li> <li>• If the day is specified, the log is sent once per week, on the specified day.</li> <li>• Select the time of day you wish the E-mail to be sent.</li> <li>• If the log is full before the time specified to send it, it will be sent regardless of the day and time specified.</li> </ul> </li> </ul>
<b>E-mail Address</b>	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.
<b>Subject</b>	Enter the text string to be shown in the "Subject" field for the E-mail.
<b>SMTP Server</b>	Enter the address or IP address of the SMTP (Simple Mail Transport Protocol) Server you use for <b>outgoing</b> E-mail.
<b>Port No.</b>	Enter the port number used to connect to the SMTP Server. The default value is 25.
<b>Syslog Server</b>	
<b>Enable Syslog</b>	If enabled, log data will be sent to your Syslog Server.
<b>Syslog Server</b>	Enter the IP address of your Syslog Server.
<b>Include</b>	Select the logs you wish to be included.

## Security Options

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

Figure 41: Security Options Screen

### Data - Security Options Screen

SPI Firewall	
<b>Enable DoS Firewall</b>	<p>If enabled, DoS (Denial of Service) attacks will be detected and blocked. The default is enabled. It is strongly recommended that this setting be left enabled.</p> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>• A DoS attack does not attempt to steal data or damage your PCs, but overloads your Internet connection so you can not use it - the service is unavailable.</li> <li>• This device uses "Stateful Inspection" technology. This system can detect situations where individual TCP/IP packets are valid, but collectively they become a DoS attack.</li> </ul>
<b>Threshold</b>	<p>This setting affects the number of "half-open" connections allowed.</p> <ul style="list-style-type: none"> <li>• A "half-open" connection arises when a remote client contacts the Server with a connection request, but then does not reply to the Server's response.</li> <li>• While the optimum number of "half-open" connections allowed (the "Threshold") depends on many factors, the most important factor is the available bandwidth of your Internet connection.</li> <li>• Select the setting to match the bandwidth of your Internet connection.</li> </ul>

<b>Options</b>	
<b>Respond to ICMP</b>	<p>The ICMP protocol is used by the "ping" and "trace route" programs, and by network monitoring and diagnostic programs.</p> <ul style="list-style-type: none"> <li>• If checked, the Broadband VPN Gateway will respond to ICMP packets received from the Internet.</li> <li>• If not checked, ICMP packets from the Internet will be ignored. Disabling this option provides a slight increase in security.</li> </ul>
<b>Allow IPsec</b>	<p>The IPsec protocol is used to establish a secure connection, and is widely used by VPN (Virtual Private Networking) programs.</p> <ul style="list-style-type: none"> <li>• If checked, IPsec connections are allowed.</li> <li>• If not checked, IPsec connections are blocked.</li> </ul>
<b>Allow PPTP</b>	<p>PPTP (Point to Point Tunneling Protocol) is widely used by VPN (Virtual Private Networking) programs.</p> <ul style="list-style-type: none"> <li>• If checked, PPTP connections are allowed.</li> <li>• If not checked, PPTP connections are blocked.</li> </ul>
<b>Allow L2TP</b>	<p>L2TP is a protocol developed by Cisco for VPNs (Virtual Private Networks).</p> <ul style="list-style-type: none"> <li>• If checked, L2TP connections are allowed.</li> <li>• If not checked, L2TP connections are blocked.</li> </ul>
<b>Allow TFTP firmware upgrade</b>	<p>If enabled, TFTP (Trivial FTP) connections can be made to this device.</p> <ul style="list-style-type: none"> <li>• TFTP can be used to upgrade the firmware. This is normally not required, and should not be enabled unless necessary.</li> <li>• You must obtain the firmware upgrade file first; instructions for using TFTP will be available with the upgrade.</li> </ul>

## 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.

Day	Session 1		Session 2	
	Start	Finish	Start	Finish
Monday	07:00	18:00	:	:
Tuesday	07:00	18:00	:	:
Wednesday	07:00	18:00	:	:
Thursday	07:00	18:00	:	:
Friday	07:00	18:00	:	:
Saturday	:	:	:	:
Sunday	:	:	:	:

Save Cancel Help

Figure 42: Define Schedule Screen

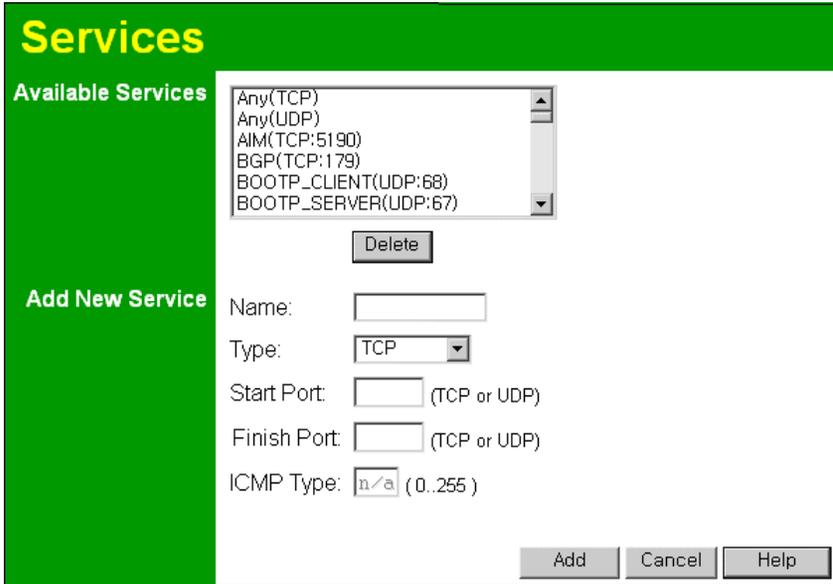
### Data - Define Schedule Screen

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

## Services

Services are used in defining traffic to be blocked or allowed by the *Access Control* or *Fire-wall Rules* features. Many common Services are pre-defined, but you can also define your own services if required.

To view the Services screen, select the *Services* link on the Security menu.



**Figure 43: Services Screen**

### Data - Services Screen

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

---

<b>Add</b>	Add a new entry to the Service list, using the data shown in the "Add New Service" area on screen.
<b>Cancel</b>	Clear the " Add New Service " area, ready for entering data for a new Service.

---

# Chapter 8

## VPN



*This Chapter describes the VPN capabilities and configuration required for common situations.*

### Overview

This section describes the VPN (Virtual Private Network) support provided by your Broadband VPN Gateway.

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

There are many standards and protocols for VPNs. The standard implemented in the Broadband VPN Gateway is **IPSec**.

### IPSec

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

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

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

There are two security modes possible with IPSec:

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

**The Broadband VPN Gateway does NOT support Transport Mode.**

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

**The Broadband VPN Gateway always uses Tunnel Mode.**

### IKE

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

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

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

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

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

## Policies

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

Each policy defines:

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

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

It is possible, and sometimes necessary, to have multiple Policies for the same remote site. In this case, the order (sequence) of the policies is important. The policies are examined in turn, and the first matching policy will be used.

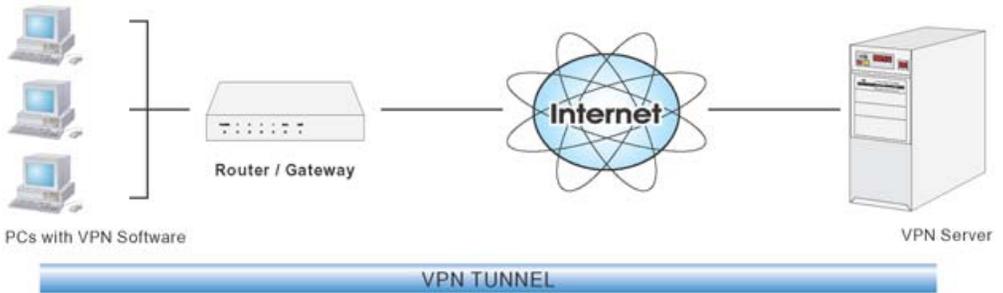
## VPN Configuration

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

<b>Remote VPN address</b>	<p>Each VPN endpoint must be configured to initiate or accept connections to the remote VPN client or Gateway.</p> <p>Usually, this requires having a fixed Internet IP address. However, it is possible for a VPN Gateway to accept incoming connections from a remote client where the client's IP address is not known in advance.</p>
<b>Traffic Selector</b>	<p>This determines which outgoing traffic will cause a VPN connection to be established, and which incoming traffic will be accepted. Each endpoint must be configured to pass and accept the desired traffic from the remote endpoint.</p> <p>If connecting 2 LANs, this requires that:</p> <ul style="list-style-type: none"> <li>• Each endpoint must be aware of the IP addresses used on the other endpoint.</li> <li>• The 2 LANs <b>MUST</b> use different IP address ranges.</li> </ul>
<b>IKE parameters</b>	<p>If using IKE (recommended), the IKE parameters must match (except for the SA lifetime, which can be different).</p>
<b>IPsec parameters</b>	<p>The IPsec parameters at each endpoint must match.</p>

## Common VPN Situations

### VPN Pass-through

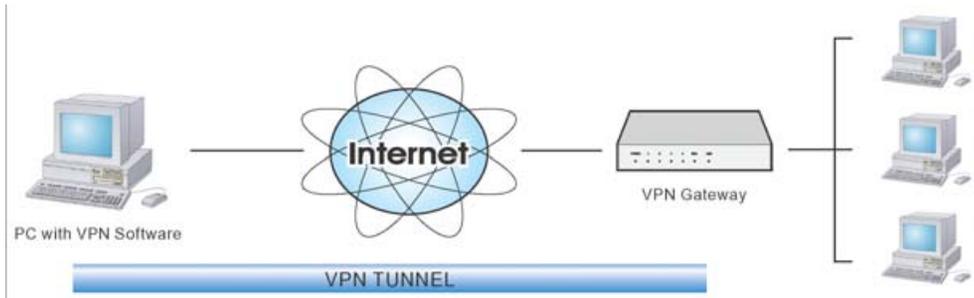


**Figure 44: VPN Pass-through**

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

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

### Client PC to VPN Gateway

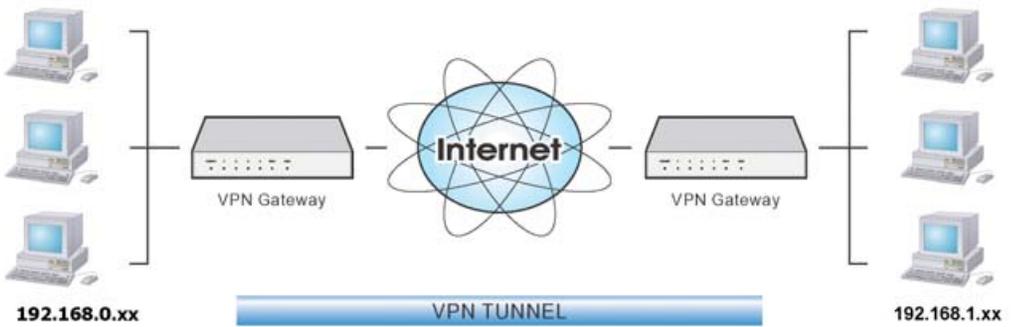


**Figure 45: Client PC to VPN Server**

In this situation, the PC must run appropriate VPN client software in order to connect, via the Internet, to the Broadband VPN Gateway. Once connected, the client PC has the same access to LAN resources as PCs on the local LAN (unless restricted by the network administrator).

- IPsec is not the only protocol which can be used in this situation, but the Broadband VPN Gateway supports IPsec ONLY.
- Windows 2000 and Windows XP include a suitable IPsec VPN client program. Configuration of this client program for use with the Broadband VPN Gateway is covered later in this document.

## Connecting 2 LANs via VPN



**Figure 46: Connecting 2 VPN Gateways**

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

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

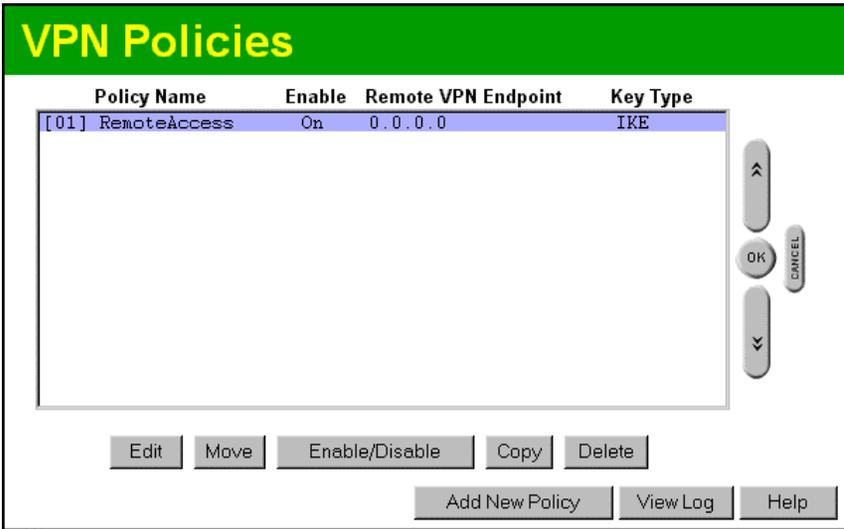
## VPN Configuration

This section covers the configuration required on the Broadband VPN Gateway when using Manual Key Exchange (Manual Policies) or IKE (Automatic Policies).

Details of using Certificates are covered in a later section.

### VPN Policies Screen

To view this screen, select **VPN Policies** from the VPN menu. This screen lists all existing VPN policies. If no policies exist, the list will be empty.



**Figure 47: VPN Policies**

Note that the order of policies is important if you have more than one policy for particular traffic. In that case, the first matching policy (for the traffic under consideration) will be used.

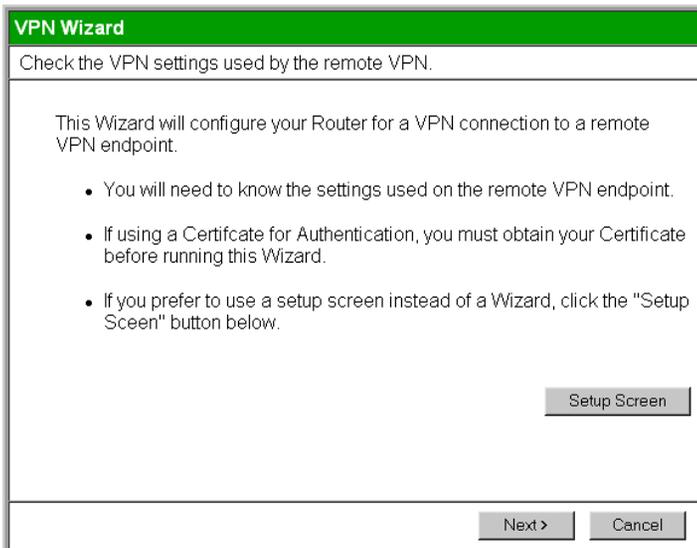
### Data - VPN Policies Screen

VPN List	
<b>Policy Name</b>	The name of the policy. When creating a policy, you should select a suitable name.
<b>Enable</b>	This indicates whether or not the policy is currently enabled. Use the "Enable/Disable" button to toggle the state of the selected policy.
<b>Remote VPN Endpoint</b>	The IP address of the remote VPN endpoint (Gateway or client).
<b>Key Type</b>	This will indicate "Manual" (manual key exchange) or "IKE" (Internet Key Exchange)
Operations	
<b>Add</b>	To add a new policy, click the "Add" button. See the following section for details.
<b>Edit</b>	To Edit or modify an existing policy, select it and click the "Edit" button.

<b>Move</b>	<p>There are 2 ways to change the order of policies:</p> <ul style="list-style-type: none"> <li>• Use the up and down indicators on the right to move the selected row. You must confirm your changes by clicking "OK". If you change your mind before clicking "OK", click "Cancel" to reverse your changes.</li> <li>• Click "Move" to directly specify a new location for the selected policy.</li> </ul>
<b>Enable/Disable</b>	Use this to toggle the On/Off state of the selected policy.
<b>Copy</b>	<p>If you wish to create a policy which is similar to an existing policy, select the policy and click the "Copy" button.</p> <p>Remember that the new policy must have a different name, and there can only be one active (enabled) policy for each remote VPN endpoint.</p>
<b>Delete</b>	To delete an exiting policy, select it and click the "Delete" button.
<b>View Log</b>	Clicking the "View Log" button will open a new window and display the VPN log.

## Adding a New Policy

1. To create a new VPN Policy, click the "Add" button on the *VPN Policies* screen. This will start the VPN Wizard, as shown below.



**Figure 48: VPN Wizard - Start**

- If you prefer to use a single setup screen instead of a Wizard, click the *Setup Screen* button. This is recommended for experienced users only.
- Otherwise, click *Next* to continue. You will see a screen like the following.

**Figure 49: VPN Wizard - General**

General Settings	
<b>Policy Name</b>	Enter a suitable name. This name is not supplied to the remote VPN. It is used only to help you manage the policies.
<b>Enable Policy</b>	Enable or disable the policy as required. For each remote VPN, only 1 policy can be enabled at any time.
<b>Remote VPN Endpoint</b>	The Internet IP address of the remote VPN endpoint (Gateway or client). <ul style="list-style-type: none"> <li>• <b>Dynamic.</b> Select this if the Internet IP address is unknown. In this case, only incoming connections are possible.</li> <li>• <b>Fixed.</b> Select this if the remote endpoint has a fixed Internet IP address.</li> </ul>
<b>Keys</b>	Select <i>Manually assigned</i> or <i>IKE (Internet Key Exchange)</i> as required. If you are setting up both endpoints, using IKE is recommended.

2. Click *Next* to continue. You will see a screen like the following:

**VPN Wizard - Traffic Selector**

This traffic will be sent through a VPN tunnel.

Local IP addresses

Type:

IP address: ... ~

Subnet Mask: ...

Remote IP addresses

Type:

IP address: ... ~

Subnet Mask: ...

< Back    Next >    Cancel

**Figure 50: VPN Wizard - Traffic Selector**

- For outgoing VPN connections, these settings determine which traffic will cause a VPN tunnel to be created, and which traffic will be sent through the tunnel.
- For incoming VPN connections, these settings determine which systems on your local LAN will be available to the remote endpoint.
- The 2 VPN endpoints MUST use different address ranges.  
If the addresses were in the same range, traffic intended for the remote VPN would be considered local LAN traffic. So it would not be forwarded to the Gateway.

### Local IP addresses

#### Type

- **Any** - no additional data is required. Any IP address is acceptable.
  - For outgoing connections, this allows any PC on the LAN to use the VPN tunnel.
  - For incoming connections, this allows an PC using the remote endpoint to access any PC on your LAN.
- **Single address** - enter an IP address in the "Start IP address" field.
- **Range address** - enter the starting IP address in the "Start IP address" field, and the finish IP address in the "Finish IP address" field.
- **Subnet address** - enter the desired IP address in the "Start IP address" field, and the network mask in the "Subnet Mask" field.

The remote VPN must have these IP addresses entered as it's "Remote" addresses.

Remote IP addresses	
Type	<ul style="list-style-type: none"> <li>• <b>Single address</b> - enter an IP address in the "Start IP address" field.</li> <li>• <b>Range address</b> - enter the starting IP address in the "Start IP address" field, and the finish IP address in the "Finish IP address" field.</li> <li>• <b>Subnet address</b> - enter the desired IP address in the "Start IP address" field, and the network mask in the "Subnet Mask" field.</li> </ul> <p>The remote VPN should have these IP addresses entered as it's "Local" addresses.</p>

3. Click *Next* to continue. The screen you will see depends on whether you previously selected "Manual Key Exchange" or "IKE".

### Manual Key Exchange

**VPN Wizard - Manually assigned Keys**

These settings must match the remote VPN Server/Gateway.

AH Authentication    Algorithm: MD5  
 Key - In:   
 Key - Out:   
 AH SPI In:  Out:

ESP Encryption    Encryption Algorithm: DES  
 Key - In:   
 Key - Out:

ESP Authentication    Authentication Algorithm: MD5  
 Key - In:   
 Key - Out:

ESP SPI    In:  Out:

**Figure 51: VPN Wizard - Manual Key Exchange**

These settings must match the remote VPN. Note that you cannot use both AH and ESP.

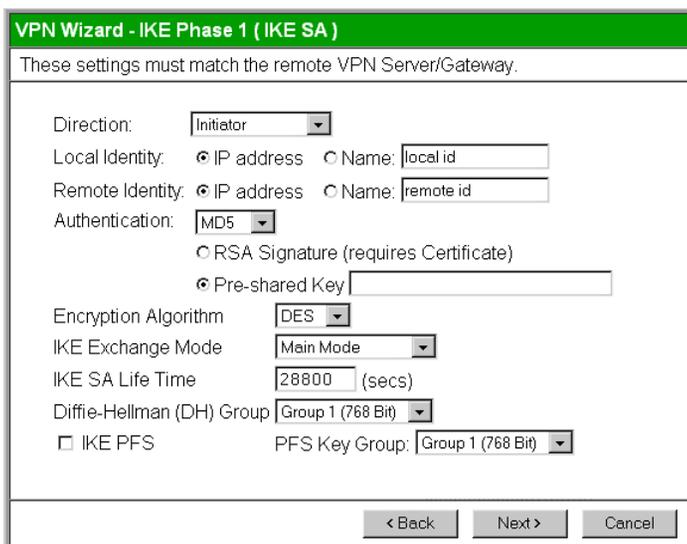
<b>Manually assigned Keys</b>	
<b>AH Authentication</b>	<p>AH (Authentication Header) specifies the authentication protocol for the VPN header, if used. (AH is often NOT used)</p> <p>If AH is not enabled, the following settings can be ignored.</p> <p><b>Keys</b></p> <ul style="list-style-type: none"> <li>• The "in" key here must match the "out" key on the remote VPN, and the "out" key here must match the "in" key on the remote VPN.</li> <li>• Keys can be in ASCII or Hex (0..9 A..F)</li> <li>• For MD5, the keys should be 32 hex/16 ASCII characters.</li> <li>• For SHA-1, the keys should be 40 hex/20 ASCII characters.</li> </ul> <p><b>SPI</b></p> <ul style="list-style-type: none"> <li>• Each SPI (Security Parameter Index) must be unique.</li> <li>• The "in" SPI here must match the "out" SPI on the remote VPN, and the "out" SPI here must match the "in" SPI on the remote VPN.</li> <li>• Each SPI should be at least 3 characters.</li> </ul>
<b>ESP Encryption</b>	<p>ESP (Encapsulating Security Payload) provides security for the payload (data) sent through the VPN tunnel. Generally, you will want to enable both Encryption and Authentication.</p> <ul style="list-style-type: none"> <li>• The "3DES" algorithm provides greater security than "DES", but is slower.</li> <li>• The "in" key here must match the "out" key on the remote VPN, and the "out" key here must match the "in" key on the remote VPN.</li> </ul>
<b>ESP Authentication</b>	<p>Generally, you should enable ESP Authentication. There is little difference between the available algorithms. Just ensure each endpoint use the same setting.</p> <ul style="list-style-type: none"> <li>• The "in" key here must match the "out" key on the remote VPN, and the "out" key here must match the "in" key on the remote VPN.</li> <li>• Keys can be in ASCII or Hex (0..9 A..F)</li> <li>• For MD5, the keys should be 32 hex/16 ASCII characters.</li> <li>• For SHA-1, the keys should be 40 hex/20 ASCII characters.</li> </ul>
<b>ESP SPI</b>	<p><b>This is required if either ESP Encryption or ESP Authentication is enabled.</b></p> <ul style="list-style-type: none"> <li>• Each SPI (Security Parameter Index) must be unique.</li> <li>• The "in" SPI here must match the "out" SPI on the remote VPN, and the "out" SPI here must match the "in" SPI on the remote VPN.</li> <li>• Each SPI should be at least 3 characters.</li> </ul>

For Manual Key Exchange, configuration is now complete.

- Click "Next" to view the final screen.
- On the final screen, click "Finish" to save your settings, then "Close" to exit the Wizard.

### IKE Phase 1

If you selected *IKE*, the following screen is displayed after the *Traffic Selector* screen.



**Figure 52: VPN Wizard - IKE Phase 1**

IKE Phase 1 (IKE SA)	
<b>Direction</b>	Select the desired option: <ul style="list-style-type: none"> <li>• <b>Initiator</b> - Only outgoing connections will be created. Incoming connection attempts will be rejected.</li> <li>• <b>Responder</b> - Only incoming connections will be accepted. Outgoing traffic which would otherwise result in a connection will be ignored.</li> <li>• <b>Both Directions</b> - Both incoming and outgoing connections are allowed.</li> </ul>
<b>Local Identity</b>	This setting must match the "Remote Identity" on the remote VPN. <i>IP address</i> is the more common method.
<b>Remote Identity</b>	This setting must match the "Local Identity" on the remote VPN. <i>IP address</i> is the more common method.
<b>Authentication</b>	<ul style="list-style-type: none"> <li>• <b>RSA Signature</b> requires that both VPN endpoints have valid Certificates issued by a CA (Certification Authority).</li> <li>• For <b>Pre-shared key</b>, enter the same key value in both endpoints. The key should be at least 8 characters (maximum is 128 characters). Note that this key is used for the IKE SA only. The keys used for the IPsec SA are automatically generated.</li> </ul>
<b>Encryption</b>	Select the desired method, and ensure the remote VPN endpoint uses the same method. The "3DES" algorithm provides greater security than "DES", but is slower.

<b>IKE Exchange Mode</b>	Select the desired option, and ensure the remote VPN endpoint uses the same mode. Main Mode provides identity protection for the hosts initiating the IPsec session, but takes slightly longer to complete. Aggressive Mode provides no identity protection, but is quicker.
<b>IKE SA Life Time</b>	This setting does not have to match the remote VPN endpoint; the shorter time will be used. Although measured in seconds, it is common to use time periods of several hours, such 28,800 seconds.
<b>DH Group</b>	Select the desired method, and ensure the remote VPN endpoint uses the same method. The smaller bit size is slightly faster.
<b>IKE PFS</b>	If enabled, PFS (Perfect Forward Security) enhances security by changing the IPsec key at regular intervals, and ensuring that each key has no relationship to the previous key. Thus, breaking 1 key will not assist in breaking the next key.  This setting should match the remote endpoint.

Click *Next* to see the following IKE Phase 2 screen.

**Figure 53: VPN Wizard - IKE Phase 2**

<b>IKE Phase 2 (IPsec SA)</b>	
<b>IPsec SA Life Time</b>	This setting does not have to match the remote VPN endpoint; the shorter time will be used. Although measured in seconds, it is common to use time periods of several hours, such 28,800 seconds.
<b>IPSec PFS</b>	If enabled, PFS (Perfect Forward Security) enhances security by changing the IPsec key at regular intervals, and ensuring that each key has no relationship to the previous key. Thus, breaking 1 key will not assist in breaking the next key.
<b>AH Authentication</b>	AH (Authentication Header) specifies the authentication protocol for the VPN header, if used.  AH is often NOT used. If you do enable it, ensure the algorithm selected matches the other VPN endpoint.

<b>ESP Encryption</b>	ESP (Encapsulating Security Payload) provides security for the payload (data) sent through the VPN tunnel. Generally, you will want to enable both ESP Encryption and ESP Authentication.  Select the desired method, and ensure the remote VPN endpoint uses the same method. The "3DES" algorithm provides greater security than "DES", but is slower.
<b>ESP Authentication</b>	Generally, you should enable ESP Authentication. There is little difference between the available algorithms. Just ensure each endpoint use the same setting.

For IKE, configuration is now complete.

- Click "Next" to view the final screen.
- On the final screen, click "Finish" to save your settings, then "Close" to exit the Wizard.

## Examples

This section describes some examples of using the Broadband VPN Gateway in common VPN situations.

### Example 1: Connecting 2 Broadband VPN Gateways

In this example, 2 LANs are connected via VPN.

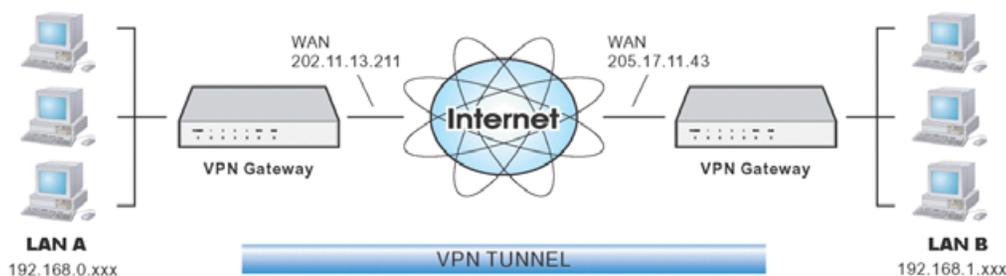


Figure 54: Connecting 2 Broadband VPN Gateways

#### Note

- The LANs MUST use different IP address ranges.
- Both endpoints have fixed WAN (Internet) IP addresses.

#### Configuration Settings

Setting	LAN A Gate-way	LAN B Gate-way	Notes
Name	Policy 1	Policy 1	Name does not affect operation. Select a meaningful name.
Remote Endpoint	205.17.11.43	202.11.13.211	Other endpoint's WAN (Internet) IP address.
Local IP addresses	Any	Any	Use a more restrictive definition if possible.
Remote IP addresses	192.168.1.1 to 192.168.1.254	192.168.0.1 to 192.168.0.254	Address range on other endpoint. Use a more restrictive definition if possible.
Key Exchange	IKE	IKE	Must match

#### IKE SA Parameters

IKE Direction	Both ways	Both ways	Does not have to match. Either endpoint can block 1 direction.
Local Identity	IP address	IP address	IP address is the most common ID method
Remote Identity	IP address	IP address	IP address is the most common ID method

IKE Authentication method	Pre-shared Key	Pre-shared Key	Certificates are not widely used.
Pre-shared Key	XXXXXXXXXX	XXXXXXXXXX	Must match
IKE Authentication algorithm	MD5	MD5	Must match
IKE Encryption	DES	DES	Must match
IKE Exchange mode	Main Mode	Main Mode	Must match
DH Group	Group 1 (768 bit)	Group 1 (768 bit)	Must match
IKE SA Life time	28800	28800	Does not have to match. Shorter period will be used.
IKE PFS	Disable	Disable	Must match
<b>IPSec SA Parameters</b>			
IPSec SA Life time	28800	28800	Does not have to match. Shorter period will be used.
IPSec PFS	Disabled	Disabled	Must match
AH authentication	Disabled	Disabled	AH is rarely used
ESP authentication	Enable/MD5	Enable/MD5	Must match
ESP encryption	Enable/DES	Enable/DES	Must match

## Example 2: Windows 2000/XP Client to LAN

In this example, a Windows 2000/XP client connects to the Broadband VPN Gateway and gains access to the local LAN.

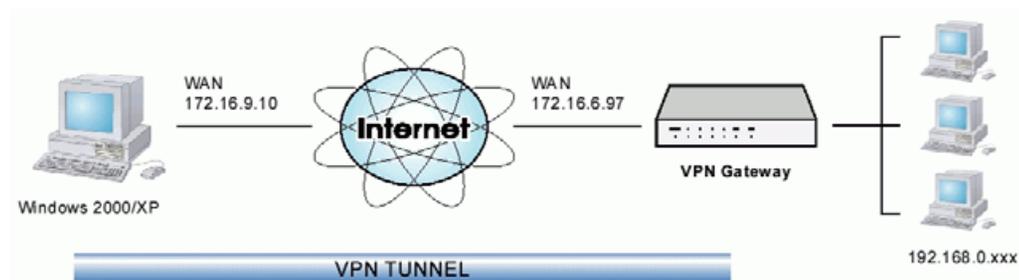


Figure 55: Windows 2000/XP Client to Broadband VPN Gateway



**Note!**

To use 3DES encryption, you need Service Pack 3 or later installed on Windows 2000.

### Broadband VPN Gateway Configuration

Setting	Value	Notes
Name	Win Client	Name does not affect operation. Select a meaningful name.
Remote Endpoint	172.16.9.10	Other endpoint's WAN (Internet) IP address.
Local IP addresses	Subnet address: 192.168.0.0 255.255.255.0	Allows access to entire LAN. Use a more restrictive definition if possible.
Remote IP addresses	172.16.9.10	For a single client, this is the same as the Gateway.
Key Exchange	IKE	Must match

#### IKE SA Parameters

IKE Direction	Responder	Only want to accept client connections.
Local Identity	IP address	Required.
Remote Identity	IP address	Required
IKE Authentication method	Pre-shared Key	Certificates are not widely used.
Pre-shared Key	XXXXXXXXXX	Must match client PC
IKE Authentication algorithm	SHA-1	Must match client PC
IKE Encryption	3DES	Must match client PC
IKE Exchange mode	Main Mode	Must match client PC

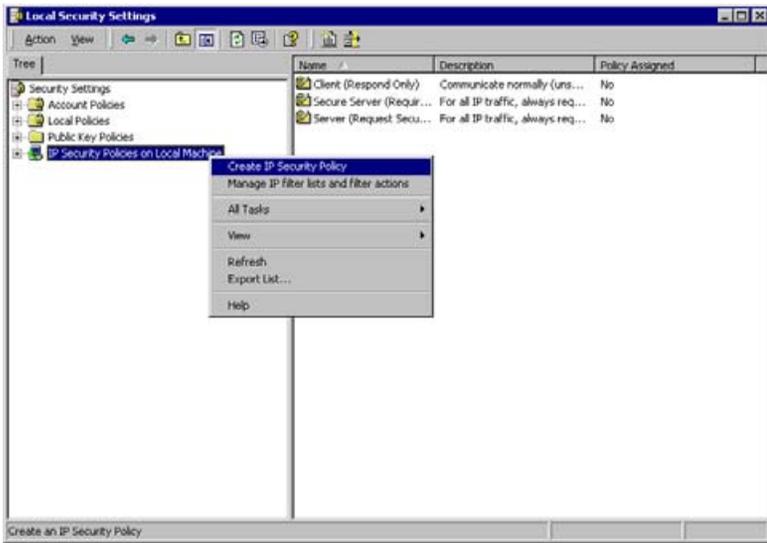
DH Group	Group 1 (768 bit)	Must match client PC
IKE SA Life time	28800	Does not have to match client PC. Shorter period will be used.
IKE PFS	Disable	Must match client PC

**IPSec SA Parameters**

IPSec SA Life time	28800	Do not have to match. Shorter period will be used.
IPSec PFS	Disable	Must match client PC
AH authentication	Disabled	AH is rarely used
ESP authentication	Enable/MD5	Must match client PC
ESP encryption	Enable/DES	Must match client PC

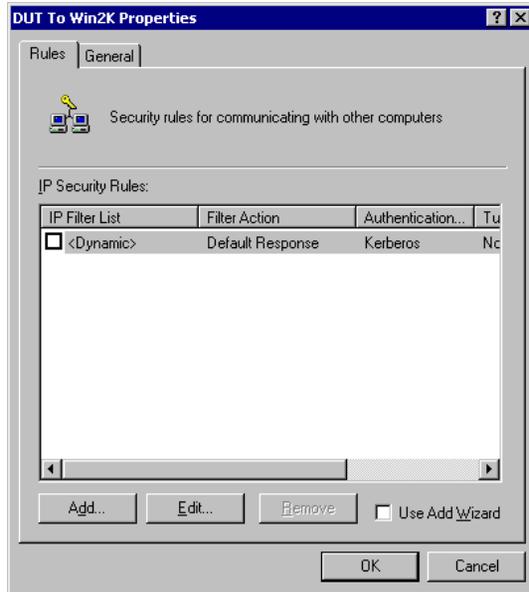
**Windows Client Configuration**

1. Select *Start - Programs - Administrative Tools - Local Security Policy*.
2. Right click *IP Security Policy on Local Machine* and select *Create IP Security Policy*



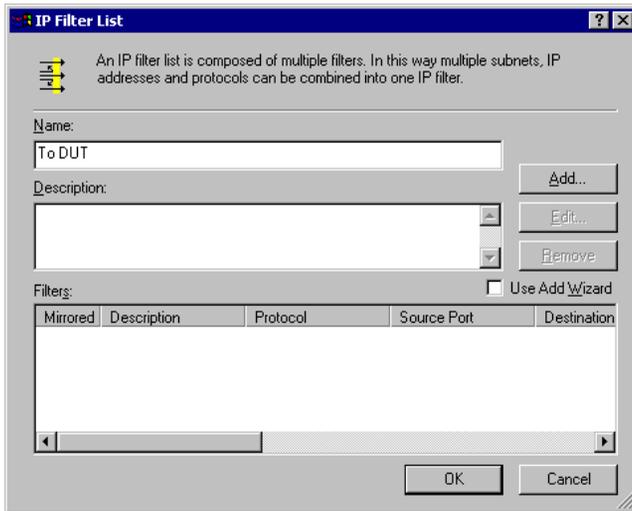
**Figure 56: Windows 2000/XP - Local Security Settings**

3. Click "Next", then enter a policy name, for example "DUT To Win2K", then click "Next".
4. Step through the Wizard:
  - Deselect *Activate the default response rule*. Click "Next",
  - Leave *Edit Properties* checked. Click "Finish".
5. The following "Properties - Rules" screen will be displayed.



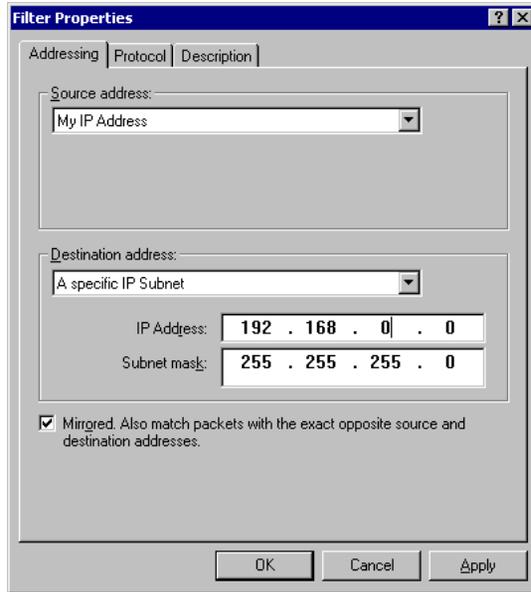
**Figure 57: Windows 2000/XP - Policy Properties**

- Note that no rules are in use. Two 2 rules are required - incoming and outgoing.
  - The outgoing rule will be added first.
6. Deselect the "Use Add Wizard" checkbox, then click "Add" to view the screen below.



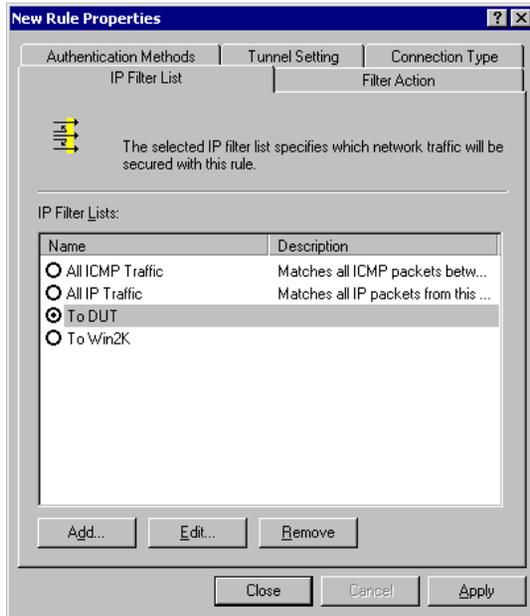
**Figure 58: IP Filter List**

7. Type "To DUT" for the name, then click "Add" to see a screen like the following.
- Since this is the outgoing filter, the *Source IP address* is "My IP address" and the *Destination IP address* is the address range used on the remote LAN.
  - Ensure the *Mirrored* option is checked.



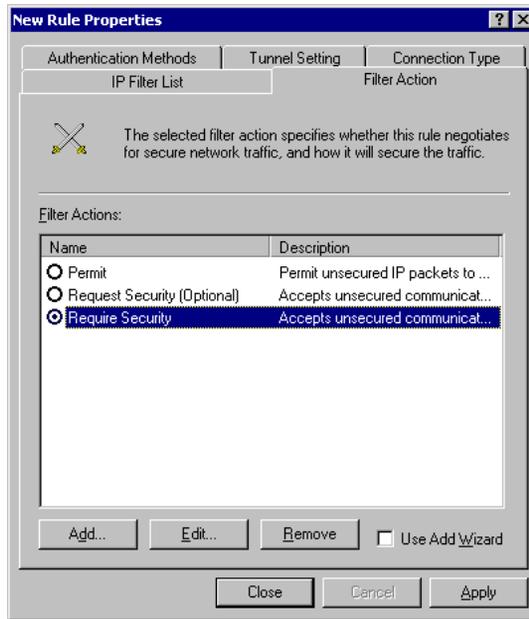
**Figure 59: Filter Properties: Addressing**

8. Enter the *Source IP address* and the *Destination IP address*.
  - Since this is the outgoing filter, the *Source IP address* is "My IP address" and the *Destination IP address* is the address range used on the remote LAN.
  - Ensure the *Mirrored* option is checked.
9. Click "OK" to save your settings and close this dialog.



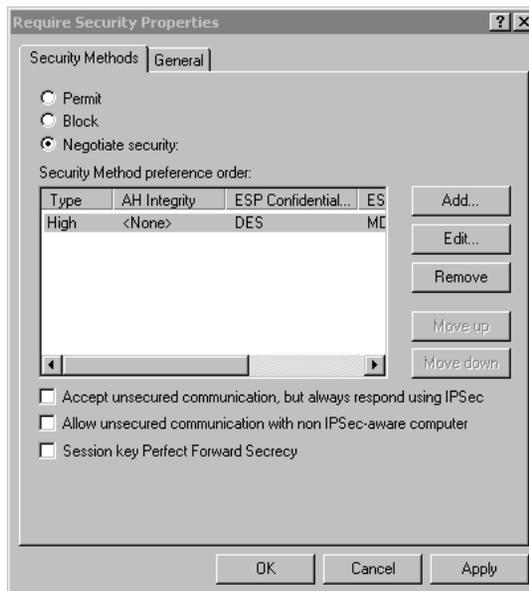
**Figure 60: New Rule Properties: IP Filter List**

10. On the resulting screen (above), ensure the "To DUT" filter is selected, then click the *Filter Action* tab to see a screen like the following



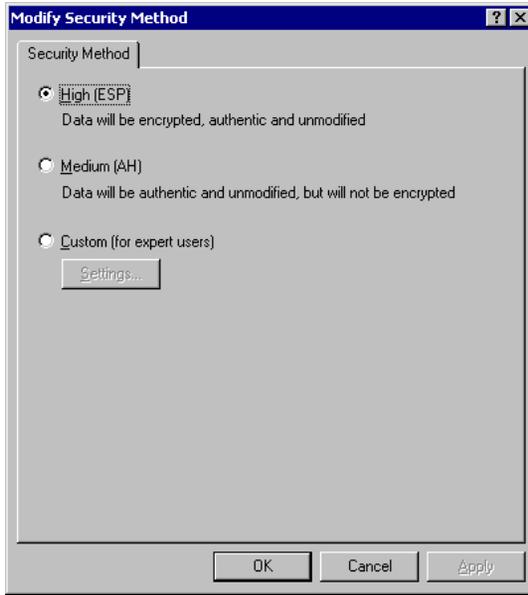
**Figure 61: New Rule Properties: Filter Action**

11. Select *Require Security*, then click the "Edit" button, to view the *Require Security Properties* screen.



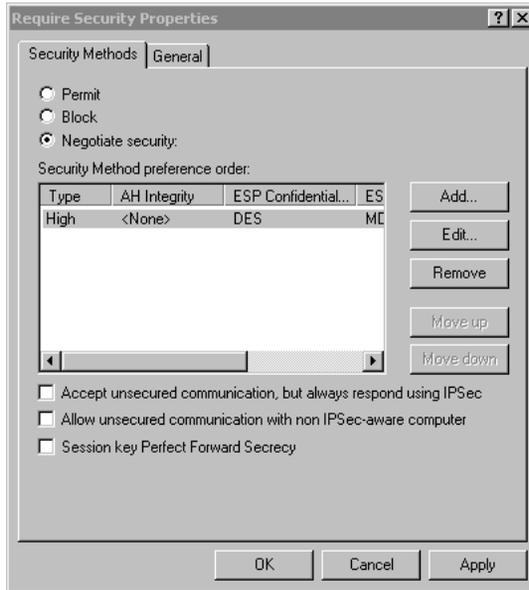
**Figure 62: Require Security Properties**

12. Select *Negotiate security* (this selects IKE), then click "Add".



**Figure 63: Modify Security Method**

13. On the resulting screen (above), select *High [ESP]* then click "OK" to save your changes and return to the *Require Security Properties* screen.

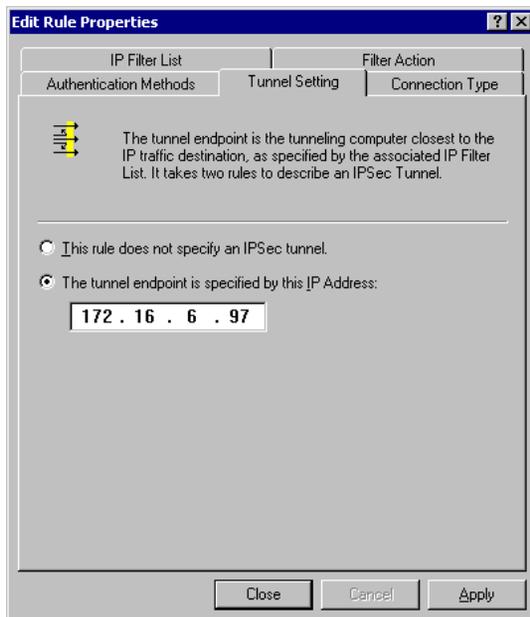


**Figure 64: Require Security Properties**

14. Ensure the following settings are correct, then click "OK" to return to the *Filter Action* tab of the *Edit Rule Properties* screen.

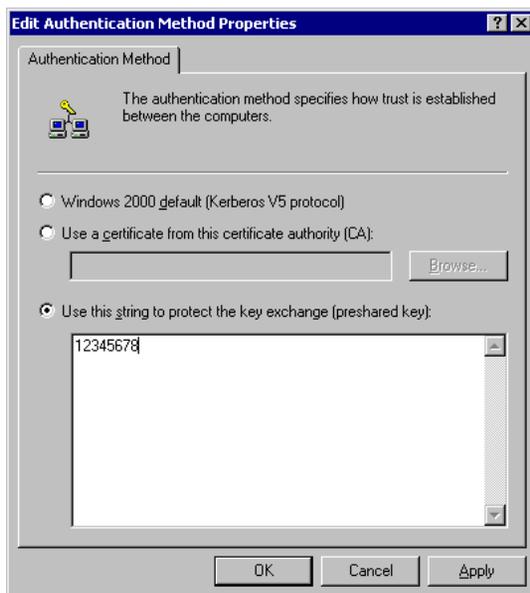
VPN Setting	Windows Setting
IKE enabled	Negotiate security
AH disabled	AH Integrity: <None>
ESP encryption: Enable/DES	ESP Confidentially: DES
ESP authentication: Enable/MD5	ESP Integrity: MD5

15. Click the *Tunnel Setting* tab, then select *The tunnel endpoint is specified by this IP address*. Enter the WAN (Internet) IP address of the Broadband VPN Gateway, as shown below.



**Figure 65: Tunnel Setting**

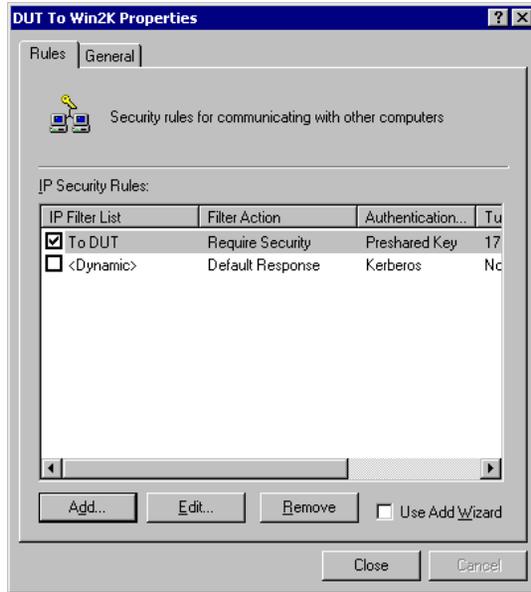
16. Click the *Authentication Methods* tab, then click the "Edit" to see the screen like the example below.



**Figure 66: Authentication Method**

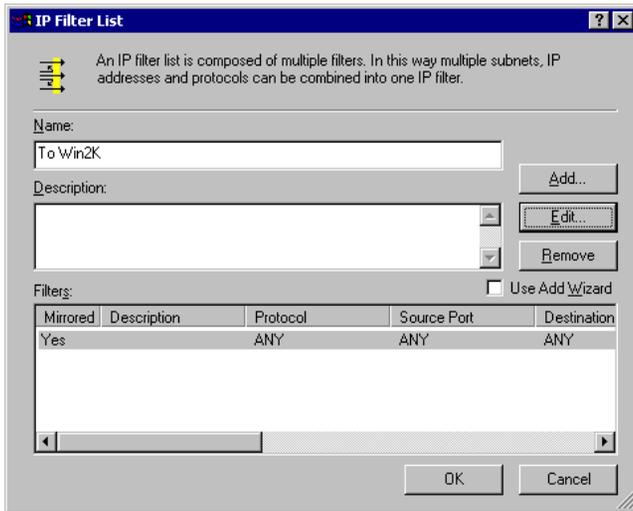
17. Select *Use this string to protect the key exchange (preshared key)*, then enter your pre-shared key in the field provided.
18. Click "OK" to save your changes and return to the *Authentication Methods* tab of the *Edit Rule Properties* screen.

19. Click "Close" to return to the *DUT to Win2K properties* screen. The "To DUT" filter should now be listed, as shown below.



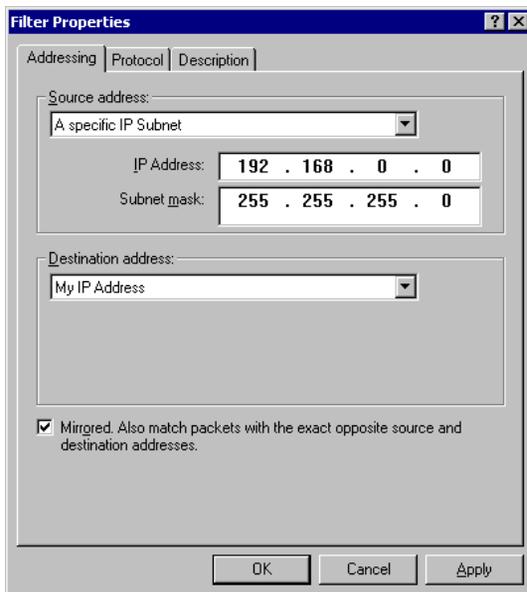
**Figure 67: Windows 2000/XP Client to Broadband VPN Gateway**

20. To add the second (outgoing) rule, click "Add". For the name, enter "To Win2K", then click "Add".



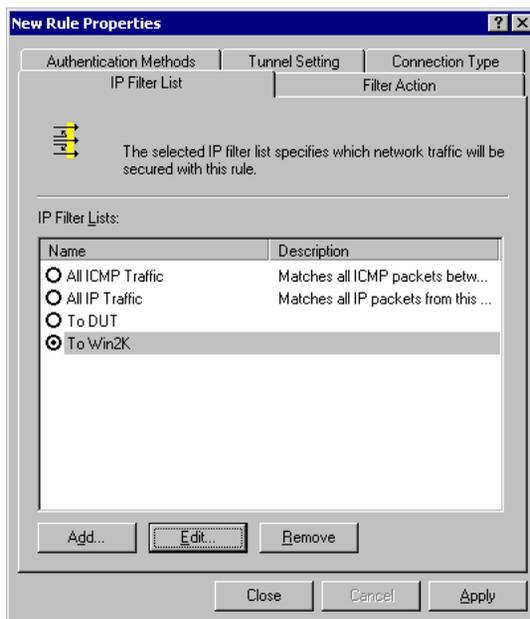
**Figure 68: Windows 2000/XP Client to Broadband VPN Gateway**

21. Enter the *Source IP address* and the *Destination IP address* as shown below.
- Since this is the incoming filter, the *Source IP address* is the address range used on the remote LAN and the *Destination IP address* is "My IP address".
  - Ensure the *Mirrored* option is checked.



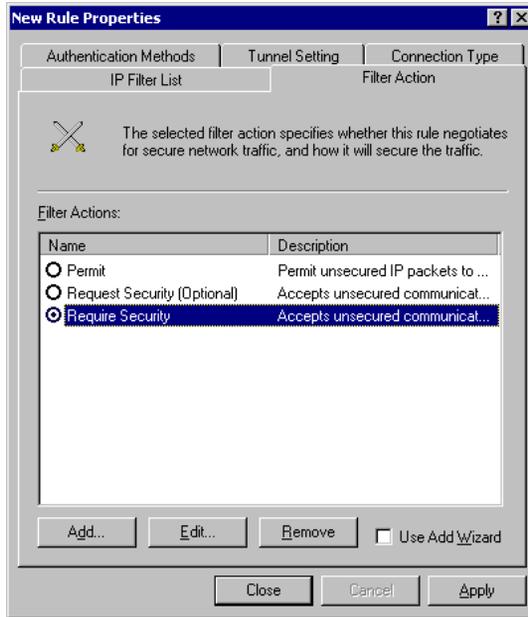
**Figure 69: Filter Properties: Addressing**

22. Click "OK" to save your changes, then "Close".



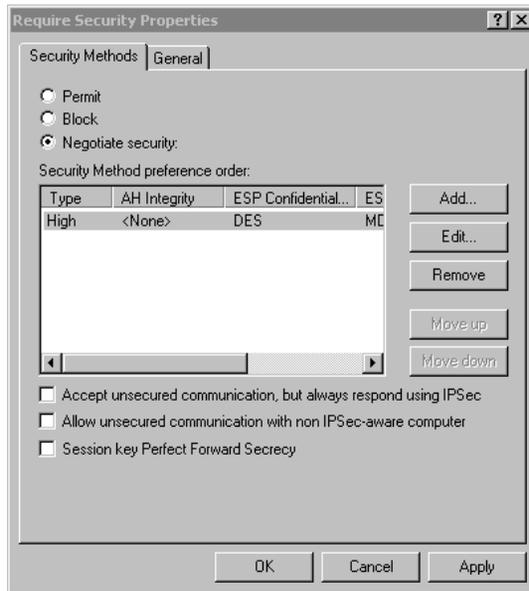
**Figure 70: Filter List**

23. Ensure the "To Win2K" filter is selected, then click the *Filter Action* tab.



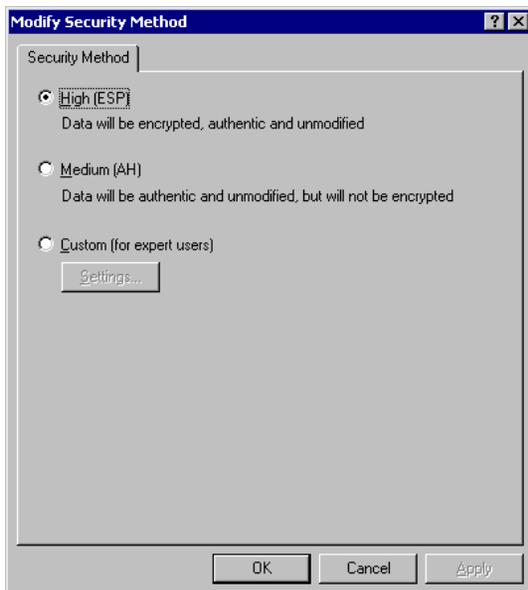
**Figure 71: Filter Action**

24. Select *Require Security*, then click "Edit". On the *Require Security Methods* screen below, select *Negotiate security*.



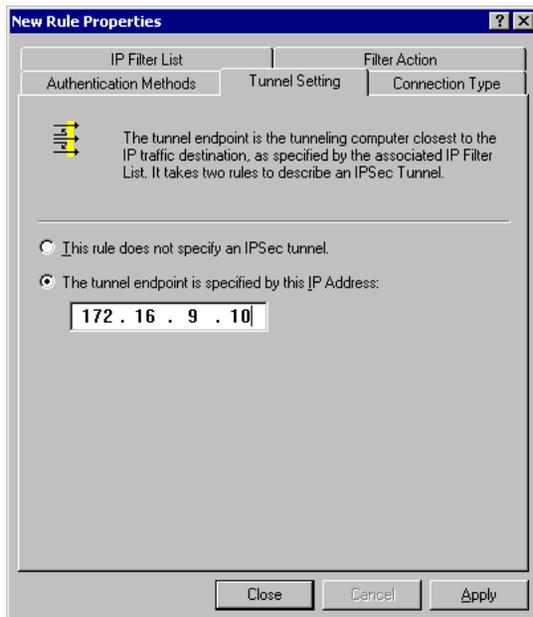
**Figure 72: Security Methods**

25. Click the "Add" button. On the resulting *Modify Security Method* screen below, select *High [ESP]*.



**Figure 73: Modify Security Method**

26. Click "OK" to save your changes, then click "OK" again to return to the Filter Action screen.
27. Select the *Tunnel Setting* tab, and enter the WAN (Internet) IP address of this PC (172.10..9.10 in this example).



**Figure 74: Tunnel Setting**

28. Select the *Authentication Methods* tab, and click the "Edit" button to see the screen below.

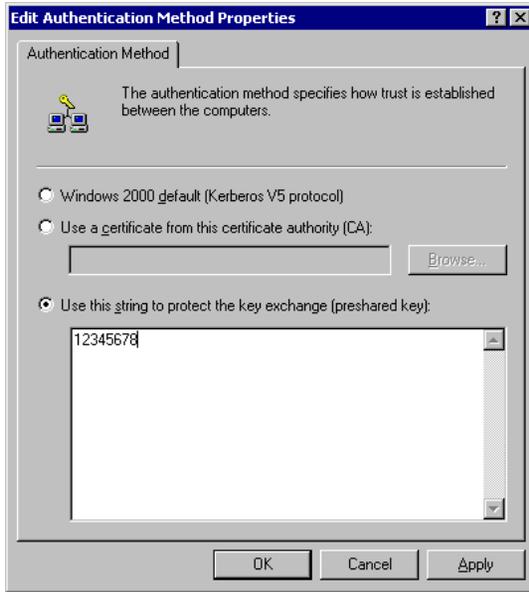


Figure 75: Authentication Method

- 29. Select *Use this string to protect the key exchange (preshared key)*, then enter your preshared key in the field provided.
- 30. Click "OK" to save your settings, then "Close" to return to the *DUT to Win2K Properties* screen. There should now be 2 IP Filers listed, as shown below.

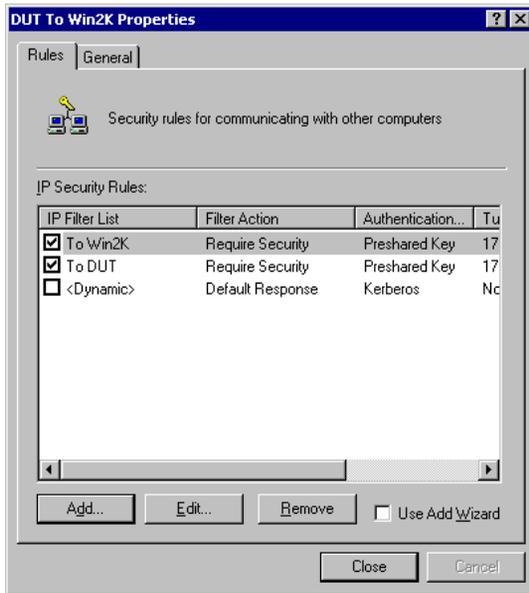
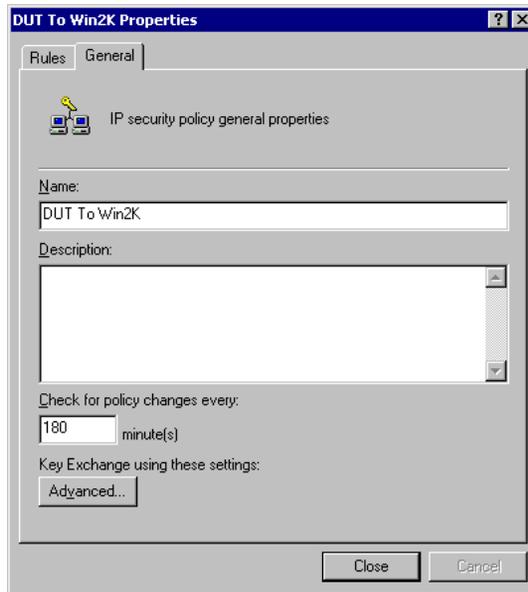


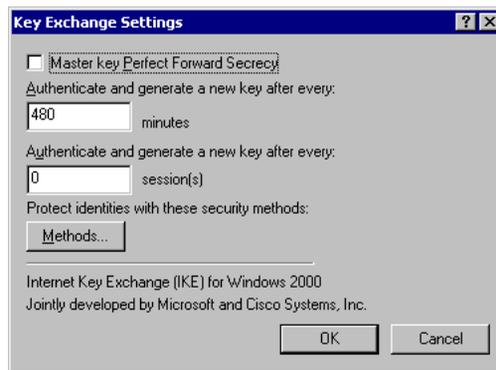
Figure 76: DUT to Win2K Properties

- 31. Select the *General* tab.



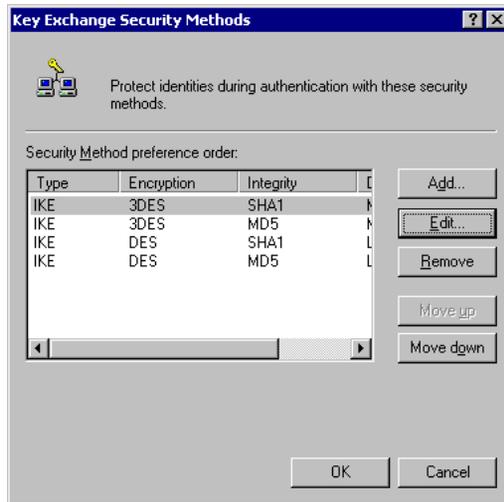
**Figure 77: Properties - General Tab**

32. Click the "Advanced" button to see the screen below.



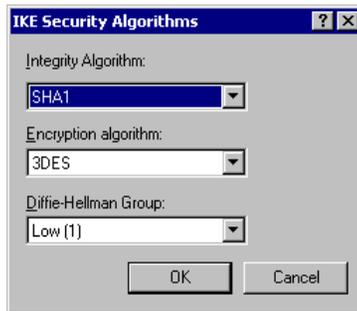
**Figure 78: Key Exchange Settings**

33. Click the "Methods" button to see the screen below.



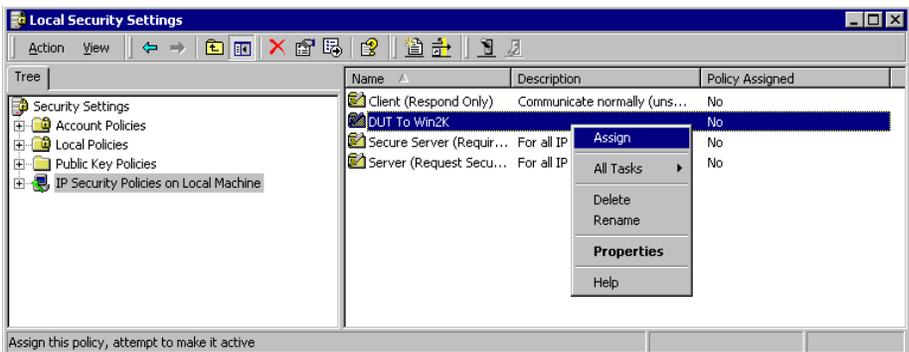
**Figure 79: Key Exchange Security Methods**

34. Select the first entry, and click the "Edit" button to see the following screen.



**Figure 80: IKE Security Algorithms**

35. Select "SHA1" for *Integrity Algorithm*, "3DES" for *Encryption algorithm*, and "Low(1)" for the *Diffie-Hellman Group*.
36. Click "OK" to save, then "OK" again, and then "Close" to return to the *Local Security Settings* screen.
37. Right click the *DUT to Win2K Policy* and select "Assign" to make your policy active.



**Figure 81: Windows 2000/XP Client to Broadband VPN Gateway**

**Configuration is now complete.**

### Example 3: Windows 2000 Server to VPN Gateway

In this example, a Windows 2000 Server connects to the Broadband VPN Gateway. Users on each LAN can then gain access to the remote LAN.

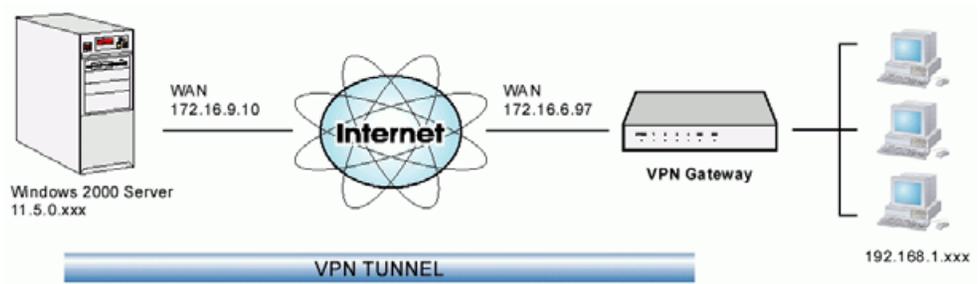


Figure 82: Broadband VPN Gateway to Windows 2000 Server

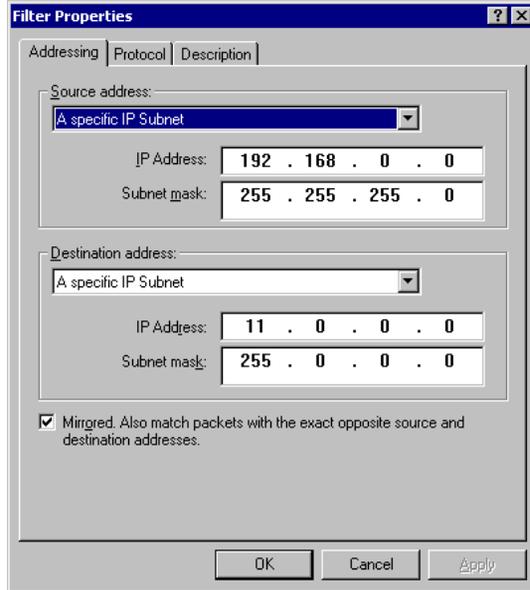
### Broadband VPN Gateway Configuration

This is the same as for the client setup earlier, with the exception of the IP address range for the remote endpoint.

Setting	Single Client	Server/Gateway
Remote IP addresses	172.16.9.10 For a single client, this is the same as the Gateway address	Subnet address: 11.5.0.0 255.255.0.0 Address range used on the remote LAN.

## Windows 2000 Server Configuration

Configuration is the same as for *Example 2: Windows 2000/XP Client to* except for specifying the *Source* and *Destination* addresses for the "Filter Properties". Instead, for both IP Filters, the *Filter Properties- Addressing* should be completed as follows.



**Figure 83: Windows 2000 Server - Addressing**

- The *Source Address* should be set to "A specific IP Subnet", and the *IP address* and *Subnet mask* set to the address range used on the Broadband VPN Gateway's LAN.
- The *Destination Address* should be set to "A specific IP Subnet", and the *IP address* and *Subnet mask* set to the address range used on the Windows 2000 LAN.

## Using Certificates

Certificates are used to authenticate users. Certificates are issued to you by various CAs (Certification Authorities). These Certificates are called "Self Certificates".

Each CA also issues a certificate to itself. This Certificate is required in order to validate communication with the CA. These certificates are called "Trusted Certificates."

The *Certificates* screen lists both the Trusted Certificate - the certificates of each CA itself - and Self Certificates - the certificates issued to you.

The screenshot shows a web interface titled "Certificates" with a green header. On the left, a green sidebar contains the labels "Trusted Certificates" and "Self Certificates". The main content area is divided into two sections. The "Trusted Certificates" section features a table with columns for "Subject Name (CA)", "Issuer Name", "Expiry Time", and "Delete". Below this table is an "Add Trusted Certificate" button. The "Self Certificates" section features a table with columns for "Name", "Subject Name", "Issuer Name", "Expiry Time", and "Delete". Below this table is an "Add Self Certificate" button. A "Help" button is located in the bottom right corner of the interface.

Figure 84: Certificates Screen

Trusted Certificates	
<b>Subject Name (CA)</b>	The "Subject Name" is always the company or person to whom the Certificate is issued. For trusted certificates, this will be a CA.
<b>Issuer Name</b>	The CA (Certification Authority) which issued the Certificate.
<b>Expiry Time</b>	The date on which the Certificate expires. You should renew the Certificate before it expires.
<b>Delete button</b>	Use this button to delete a Trusted Certificate. Select the checkbox in the <i>Delete</i> column for any Certificates you wish to delete, then click the "Delete" button.
Self Certificates	
<b>Name</b>	The name you assigned to this Certificate. You should select a name which helps to identify this particular certificate.
<b>Subject Name</b>	The company or person to whom the Certificate is issued.
<b>Issuer Name</b>	The CA (Certification Authority) which issued the Certificate.
<b>Expiry Time</b>	The date on which the Certificate expires. You should renew the Certificate before it expires.
<b>Delete button</b>	Use this button to delete a Self Certificate. Select the checkbox in the <i>Delete</i> column for any Certificates you wish to delete, then click the "Delete" button.

## Adding a Trusted Certificate

1. After obtaining a new Certificate from the CA, you need to upload it to the Broadband VPN Gateway.
2. On the "Certificates" screen, click the "Add Trusted Certificate" button to view the *Add Trusted Certificate* screen, shown below.



**Figure 85: Add Trusted Certificate**

3. Click the "Browse" button, and locate the certificate file on your PC
4. Select the file. The name will appear in the "Certificate File" field.
5. Click "Upload" to upload the certificate file to the Broadband VPN Gateway.
6. Click "Back" to return to the Trusted Certificate list. The new Certificate will appear in the list.

## Adding a Self Certificate

This process is different to obtaining a Trusted Certificate. The Broadband VPN Gateway must generate a request for the CA. You cannot request a Certificate directly. The correct procedure is as follows:

1. On the "Certificates" screen, click the "Add Self Certificate" button to view the first screen of the *Add Self Certificate* procedure, shown below.



**Figure 86: Add Self Certificate (1)**

2. Complete this screen.

<b>Name</b>	Enter a name which helps to identify this particular certificate. This name is only for your reference.
-------------	---

<b>Subject Name</b>	This is the name which other organizations will see as the Holder (owner) of this Certificate. This should be your registered business name or official company name. Generally, all Certificates should have the same value in the Subject field.
<b>Hash Algorithm</b>	Select the desired option.
<b>Signature Algorithm</b>	Select the desired option. RSA is recommended.
<b>Signature Key Length</b>	Select the desired option. Normally, 1024 bits provides adequate security.

- Click "Next" to continue to the following screen.

**Add Self Certificate (2)**

**Certificate Details**

Subject Name: Test  
Hash Algorithm: MD5  
Signature Algorithm: RSA  
Key Length: 1024

**Data to supply to CA**

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBYzCBzQTSajAkMjowCQYyVjQ0Q0EwTVUzEYHRMGA1UEAxQM63V1oaVjdF90ZMlw
MIGCMAAGC3q0SId3DQERAGUAA4GMADCB1QK2pGQDAE7eU50uW8c0UyQjYA51tAhFz
Bx1Pa0XQkpeapoc9vrcG6e1mPqmTz9HDG0kVU1evhTtZ2SprynEELGk3ZE90wZA
t4E1QQCB0eA8eak15C2Bm9LRFqa9PERk+k1d5L0w51B1YEwXaF8m7BSEBqQ9
Fp0xVvFp0uH0Y4Lw0IDAQABAAQwOY9KozIhvcBAQEEBQADgYEAUW1y7X1T2a
u7F2ARU4amFPWaltz4FUE/WGRGd33bQER0Zhfq2qjFhallsab7e6357EX/BBcH5z4
L60IEBz//OEM-M+bYCj/8HcMvLac/46F1Kj/zG+Chk+T4iYbtZz5x07u1L0ptVH
0wFRFYB1adbu0G0BQ2gSc09e8fQCI8c=
-----END CERTIFICATE REQUEST-----
```

Use this data to obtain a Certificate, then click "Next".

**Figure 87: Add Self Certificate (2)**

- Check that the data displayed in the *Certificate Details* section is correct. This data is used to generate the Certificate request. If the data is not correct, click the "Back" button and correct the previous screen.
- If the data is correct, copy the text in the *Data to supply to CA* panel to the clipboard.
- Apply for a Certificate:
  - Connect to the CA's web site.
  - Start the Self Certificate request procedure.
  - When prompted for the request data, copy this data (including "-----BEGIN CERTIFICATE REQUEST-----" and "-----END CERTIFICATE REQUEST-----") from this screen to the CA's form.
  - Submit the CA's form.
  - If there are no problems, the Certificate will then be issued.
- After obtaining a new Certificate, as described above, you need to upload it the Broadband VPN Gateway. Click the "Next" button to see the screen below.



Figure 88: Add Self Certificate (3)

8. Upload the Certificate:
  - Click the "Browse" button, and locate the certificate file on your PC
  - Select the file. The name will appear in the "Certificate File" field.
  - Click "Upload" to upload the certificate file to the Broadband VPN Gateway.
  - Click "Finished" to return to the Certificate list. The new Certificate will appear in the list.

## CRLs

CRLs are only necessary if using Certificates.

CRL (Certificate Revocation List) files show Certificates which have been revoked, and are no longer valid. Each CA issues their own CRLs.

It is VERY IMPORTANT to keep your CRLs up-to-date. You need to obtain the CRL for each CA regularly. The "Next Update" field in the CRL shows when the next update will be available.

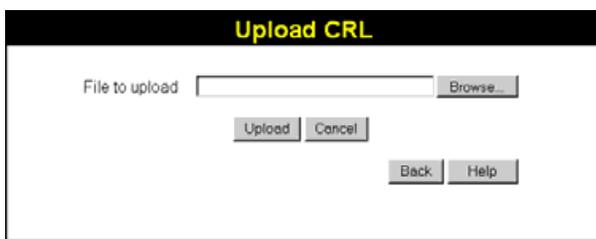
### To add a New CRL

1. Obtain the CRL file from your CA.
2. Select *CRL* from the VPN menu. You will see a screen like the example below.



Figure 89: Certificate Revocation Lists

3. Click the "Add New CRL" button. You will see a screen like the following:



The image shows a web-based dialog box titled "Upload CRL". It features a black header with the title in yellow. The main area is white and contains a "File to upload" label, an empty text input field, and a "Browse..." button. Below the input field are "Upload" and "Cancel" buttons. At the bottom right, there are "Back" and "Help" buttons.

**Figure 90: Upload CRL**

4. Upload the CRL file:
  - Click the "Browse" button, and locate the CRL file on your PC
  - Select the file. The name will appear in the "File to Upload" field.
  - Click "Upload" to upload the CRL file to the Broadband VPN Gateway.
  - Click "Back" to return to the CRL list. The new CRL will appear in the list.
5. Use the "Delete" button to delete the previous (now outdated) CRL.

## Chapter 9

# Other Features and Settings

# 9

*This Chapter explains the screens and settings available via the "Other" menu.*

## Overview

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

The screens available are:

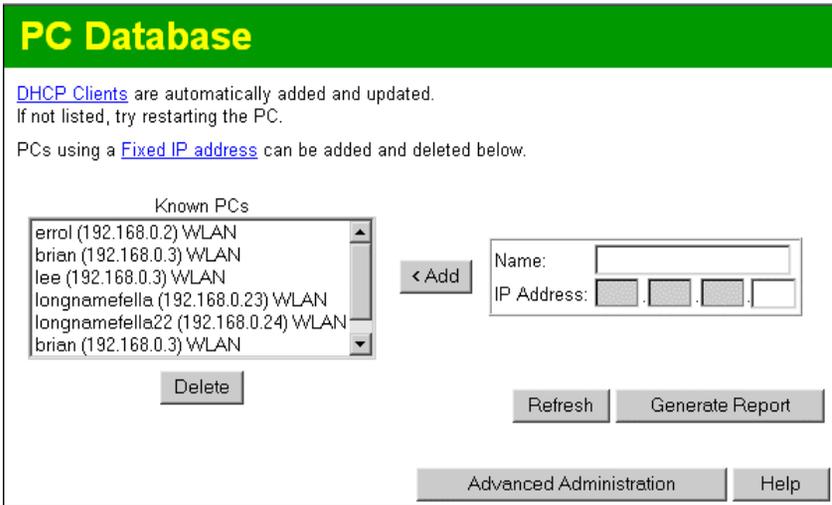
<b>PC Database</b>	This is the list of PCs shown when you select the "DMZ PC", "Virtual Server", or "Internet Application". This database is maintained automatically, but you can add and delete entries for PCs which use a Fixed (Static) IP Address.
<b>Remote Administration</b>	This feature allows you to manage the Broadband VPN Gateway via the Internet.
<b>Routing</b>	Only required if your LAN has other Routers or Gateways.
<b>Firmware Upgrade</b>	The firmware (software) in the Broadband VPN Gateway can be upgraded using your Web Browser.
<b>UPNP</b>	UPnP (Universal Plug and Play) allows automatic discovery and configuration of the Broadband VPN Gateway

## PC Database

The PC Database is used whenever you need to select a PC (e.g. for the "DMZ" PC). It eliminates the need to enter IP addresses. Also, you do not need to use fixed IP addresses on your LAN.

### PC Database Screen

An example PC Database screen is shown below.



**Figure 91: PC Database**

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

**Data - PC Database Screen**

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

## PC Database (Admin)

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

**PC Database (Admin)**

Any PC may be added, edited or deleted. If adding a PC which is not connected and On, you must provide the MAC (hardware) address

Known PCs

- errol (192.168.0.2) WLAN
- brian (192.168.0.3) WLAN
- lee (192.168.0.3) WLAN
- longnamefella (192.168.0.23) WLAN
- longnamefella22 (192.168.0.24) WLAN
- brian (192.168.0.3) WLAN

Edit Delete

**PC Properties**

Name:

IP Address:  Automatic (DHCP Client)  
 DHCP Client - reserved IP address:  .  .  .   
 Fixed IP address (set on PC):  .  .  .

MAC Address:  Automatic discovery (PC must be available on LAN)  
 MAC address is

Add as New Entry Update Selected PC Clear Form

Refresh Generate Report Standard Screen Help

**Figure 92: PC Database (Admin)**

## Data - PC Database ( Admin) Screen

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

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

## Remote Administration

This feature allows you to manage the Broadband VPN Gateway via the Internet.

Figure 93: Remote Administration Screen

### Data - Remote Administration Screen

Remote Administration	
<b>Enable Remote Administration</b>	Enable to allow administration via the Internet. If Disabled, this device will ignore management connection attempts from the Internet.
<b>Port Number</b>	Enter a port number between 1024 and 65535 (8080 is recommended). This port number must be specified when you connect (see below).  <b>Note:</b> The default port number for HTTP (Web) connections is port 80, but using port 80 here will prevent the use of a Web "Virtual Server" on your LAN. (See <i>Advanced Internet - Virtual Servers</i> )
<b>Current IP Address</b>	You must use this IP Address to connect (see below).  This IP Address is allocated by your ISP. But if using a Dynamic IP Address, this value can change each time you connect to your ISP. So it is better if your ISP allocates you a Fixed IP Address.

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

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

HTTP://123.123.123.123:8080

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

## Routing

### Overview

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

### Routing Screen

The routing table is accessed by the *Routing* link on the *Other* screen.

#### Using this Screen

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

#### Static Routing Table

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

Figure 94: Routing Screen

## Data - Routing Screen

RIP	
<b>Enable RIP</b>	<p>Check this to enable the RIP (Routing Information Protocol) feature of the Broadband VPN Gateway.</p> <p>The Broadband VPN Gateway supports RIP 1 only.</p>
Static Routing	
<b>Static Routing Table Entries</b>	<p>This list shows all entries in the Routing Table.</p> <ul style="list-style-type: none"> <li>The "Properties" area shows details of the selected item in the list.</li> <li>Change any the properties as required, then click the "Update" button to save the changes to the selected entry.</li> </ul>
<b>Properties</b>	<ul style="list-style-type: none"> <li><b>Destination Network</b> - The network address of the remote LAN segment. For standard class "C" LANs, the network address is the first 3 fields of the Destination IP Address. The 4th (last) field can be left at 0.</li> <li><b>Network Mask</b> - The Network Mask for the remote LAN segment. For class "C" networks, the default mask is 255.255.255.0</li> <li><b>Gateway IP Address</b> - The IP Address of the Gateway or Router which the Broadband VPN Gateway must use to communicate with the destination above. (NOT the router attached to the remote segment.)</li> <li><b>Metric</b> - The number of "hops" (routers) to pass through to reach the remote LAN segment. The shortest path will be used. The default value is 1.</li> </ul>

Buttons	
<b>Save</b>	Save the RIP setting. This has no effect on the Static Routing Table.
<b>Add</b>	Add a new entry to the Static Routing table, using the data shown in the "Properties" area on screen. The entry selected in the list is ignored, and has no effect.
<b>Update</b>	Update the current Static Routing Table entry, using the data shown in the "Properties" area on screen.
<b>Delete</b>	Delete the current Static Routing Table entry.
<b>Clear Form</b>	Clear all data from the "Properties" area, ready for input of a new entry for the Static Routing table.
<b>Generate Report</b>	Generate a read-only list of all entries in the Static Routing table.

## Configuring Other Routers on your LAN

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

### Local Router

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

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

### Other Routers on the Local LAN

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

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

## Static Routing - Example

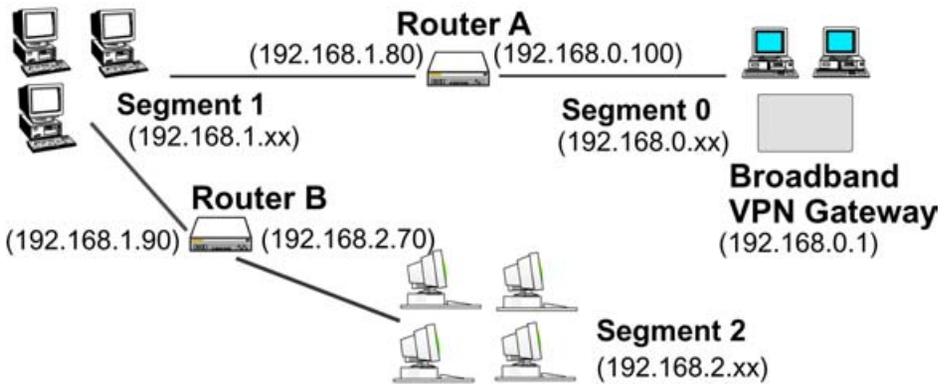


Figure 95: Routing Example

### For the Broadband VPN Gateway 's Routing Table

For the LAN shown above, with 2 routers and 3 LAN segments, the Broadband VPN Gateway requires 2 entries as follows.

Entry 1 (Segment 1)	
Destination IP Address	192.168.1.0
Network Mask	255.255.255.0 (Standard Class C)
Gateway IP Address	192.168.0.100 (Broadband VPN Gateway 's local Router)
Metric	2
Entry 2 (Segment 2)	
Destination IP Address	192.168.2.0
Network Mask	255.255.255.0 (Standard Class C)
Gateway IP Address	192.168.0.100
Metric	3

### For Router A's Default Route

Destination IP Address	0.0.0.0
Network Mask	0.0.0.0
Gateway IP Address	192.168.0.1 (Broadband VPN Gateway 's IP Address)

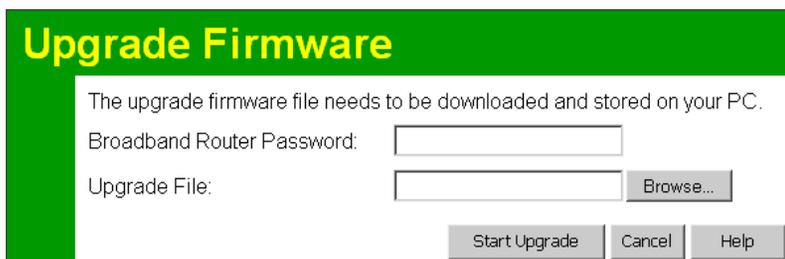
### For Router B's Default Route

Destination IP Address	0.0.0.0
Network Mask	0.0.0.0
Gateway IP Address	192.168.1.80 (Broadband VPN Gateway 's local router)

## Firmware Upgrade

The firmware (software) in the Broadband VPN Gateway can be upgraded using your Web Browser.

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



**Upgrade Firmware**

The upgrade firmware file needs to be downloaded and stored on your PC.

Broadband Router Password:

Upgrade File:

**Figure 96: Upgrade Firmware Screen**

### To perform the Firmware Upgrade:

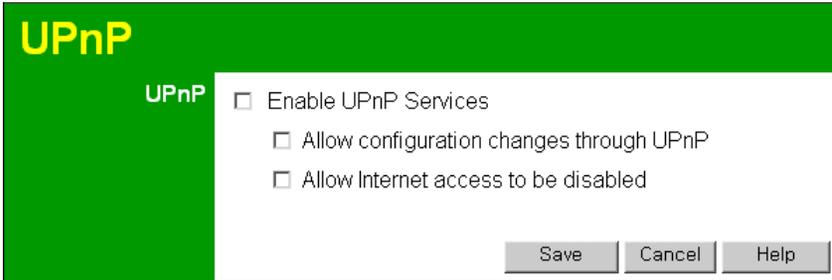
1. Click the "Browse" button and navigate to the location of the upgrade file.
2. Select the upgrade file. It's name will appear in the *Upgrade File* field.
3. Click the "Start Upgrade" button to commence the firmware upgrade.



**The Broadband VPN Gateway is unavailable during the upgrade process, and must restart when the upgrade is completed. Any connections to or through the Broadband VPN Gateway will be lost.**

## UPNP

An example UPNP screen is shown below.



**Figure 97: UPNP Screen**

### Data - UPNP Screen

UPnP	
<b>Enable UPnP Services</b>	<ul style="list-style-type: none"> <li>• UPnP (Universal Plug and Play) allows automatic discovery and configuration of equipment attached to your LAN. UPnP is by supported by Windows ME, XP, or later.</li> <li>• If Enabled, this device will be visible via UPnP.</li> <li>• If Disabled, this device will not be visible via UPnP.</li> </ul>
<b>Allow Configuration...</b>	<ul style="list-style-type: none"> <li>• If checked, then UPnP users can change the configuration.</li> <li>• If Disabled, UPnP users can only view the configuration. But currently, this restriction only applies to users running Windows XP, who access the <i>Properties</i> via UPnP. (e.g. Right - click the Broadband VPN Gateway in <i>My Network Places</i>, and select <i>Properties</i>)</li> </ul>
<b>Allow Internet access to be disabled</b>	<ul style="list-style-type: none"> <li>• If checked, then UPnP users can disable Internet access via this device.</li> <li>• If Disabled, UPnP users can NOT disable Internet access via this device. But currently, this restriction only applies to users running Windows XP, who access the <i>Properties</i> via UPnP. (e.g. Right - click the Broadband VPN Gateway in <i>My Network Places</i>, and select <i>Properties</i>)</li> </ul>

# Appendix A

## Troubleshooting



*This Appendix covers the most likely problems and their solutions.*

### Overview

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

### General Problems

**Problem 1:** Can't connect to the Broadband VPN Gateway to configure it.

**Solution 1:** Check the following:

- The Broadband VPN Gateway is properly installed, LAN connections are OK, and it is powered ON.
- Ensure that your PC and the Broadband VPN Gateway are on the same network segment. (If you don't have a router, this must be the case.)
- If your PC is set to "Obtain an IP Address automatically" (DHCP client), restart it.
- If your PC uses a Fixed (Static) IP address, ensure that it is using an IP Address within the range 192.168.0.2 to 192.168.0.254 and thus compatible with the Broadband VPN Gateway's default IP Address of 192.168.0.1.

Also, the Network Mask should be set to 255.255.255.0 to match the Broadband VPN Gateway.

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

### Internet Access

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

**Solution 1:** A number of things could be causing this. Try the following troubleshooting steps.

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

**Problem 2:** **Some applications do not run properly when using the Broadband VPN Gateway.**

**Solution 2:** The Broadband VPN Gateway processes the data passing through it, so it is not transparent.

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

If this does solve the problem you can use the *DMZ* function. This should work with almost every application, but:

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

# Appendix B

## Specifications



### Broadband VPN Gateway

Model	Broadband VPN Gateway
Dimensions	170mm(W) * 147mm(D) * 27mm(H)
Operating Temperature	0° C to 40° C
Storage Temperature	-10° C to 70° C
Network Protocol:	TCP/IP
Network Interface:	6 Ethernet: 4 * 10/100BaseT (RJ45) LAN connection 1 * 10/100BaseT (RJ45) for DMZ Port 1 * 10/100BaseT (RJ45) for WAN
LEDs	14
Power Adapter	12 V DC External

### FCC Statement

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

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

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

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

## **FCC Radiation Exposure Statement**

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

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

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

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

## **CE Marking Warning**

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