



IP-2000VPN

Internet VPN Router

User's Manual




www.airlive.com

Declaration of Conformity

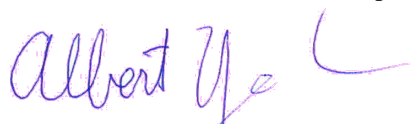
We, Manufacturer/Importer
OvisLink Corp.
5F., NO.6, Lane 130, Min-Chuan Rd.,
Hsin-Tien City, Taipei County, Taiwan

Declare that the product
Internet VPN Router
AirLive IP-2000VPN
is in conformity with

In accordance with 89/336 EEC-EMC Directive and 1999/5 EC-R & TTE Directive

<u>Clause</u>	<u>Description</u>
■ EN 55022:1998	Limits and methods of measurement of radio disturbance characteristics of information technology equipment
■ EN 61000-3-2:2000	Disturbances in supply systems caused by household appliances and similar electrical equipment "Harmonics"
■ EN 61000-3-3:1995/ A1:2001	Disturbances in supply systems caused by household appliances and similar electrical equipment "Voltage fluctuations"
■ EN 55024:1998	Information Technology equipment-Immunity characteristics-Limits And methods of measurement
■ CE marking	

Manufacturer/Importer



Albert Yeh

Vice President

Signature :
Name :
Position/ Title :

Date : 2008/1/1

(Stamp)

AirLive IP-2000VPN CE Declaration Statement

Country	Declaration	Country	Declaration
cs Česky [Czech]	OvisLink Corp. tímto prohlašuje, že tento AirLive IP-2000VPN je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/ES.	lt Lietuvių [Lithuanian]	Šiuo OvisLink Corp. deklaruoja, kad šis AirLive IP-2000VPN atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
da Dansk [Danish]	Undertegnede OvisLink Corp. erklærer herved, at følgende udstyr AirLive IP-2000VPN overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.	nl Nederlands [Dutch]	Hierbij verklaart OvisLink Corp. dat het toestel AirLive IP-2000VPN in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG.
de Deutsch [German]	Hiermit erkläre OvisLink Corp., dass sich das Gerät AirLive IP-2000VPN in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EG befindet.	mt Malti [Maltese]	Hawnhekk, OvisLink Corp, jiddikjara li dan AirLive IP-2000VPN jikkonforma mal-htigijiet essenzjali u ma provvedimenti oħrajn rilevanti li hemm fid-Dirrettiva 1999/5/EC.
et Eesti [Estonian]	Käesolevaga kinnitab OvisLink Corp. seadme AirLive IP-2000VPN vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.	hu Magyar [Hungarian]	Az OvisLink Corporation kijelenti, hogy az AirLive IP-2000VPN megfelel az 1999/05/CE irányelv alapvető követelményeinek és egyéb vonatkozó rendelkezéseinek.
en English	Hereby, OvisLink Corp., declares that this AirLive IP-2000VPN is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.	pl Polski [Polish]	Niniejszym OvisLink Corp oświadcza, że AirLive IP-2000VPN jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
es Español [Spanish]	Por medio de la presente OvisLink Corp. declara que el AirLive IP-2000VPN cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.	pt Português [Portuguese]	OvisLink Corp declara que este AirLive IP-2000VPN está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
el Ελληνική [Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ OvisLink Corp. ΔΗΛΩΝΕΙ ΟΤΙ AirLive IP-2000VPN ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ.	sl Slovensko [Slovenian]	OvisLink Corp izjavlja, da je ta AirLive IP-2000VPN v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/ES.
fr Français [French]	Par la présente OvisLink Corp. déclare que l'appareil AirLive IP-2000VPN est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE	sk Slovensky [Slovak]	OvisLink Corp týmto vyhlasuje, že AirLive IP-2000VPN spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.
it Italiano [Italian]	Con la presente OvisLink Corp. dichiara che questo AirLive IP-2000VPN è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.	fi Suomi [Finnish]	OvisLink Corp vakuuttaa täten että AirLive IP-2000VPN tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen
lv Latviski [Latvian]	Ar šo OvisLink Corp. deklarē, ka AirLive IP-2000VPN atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.	is Íslenska [Icelandic]	Hér með lýsir OvisLink Corp yfir því að AirLive IP-2000VPN er í samræmi við grunnkröfur og aðrar kröfur, sem gerðar eru í tilskipun 1999/5/EC.
sv Svenska [Swedish]	Härmed intygar OvisLink Corp. att denna AirLive IP-2000VPN står i överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.	no Norsk [Norwegian]	OvisLink Corp erklærer herved at utstyret AirLive IP-2000VPN er i samsvar med de grunnleggende krav og øvrige relevante krav i direktiv 1999/5/EF.

A copy of the full CE report can be obtained from the following address:

OvisLink Corp.
5F, No.6 Lane 130,
Min-Chuan Rd, Hsin-Tien City,
Taipei, Taiwan, R.O.C.

This equipment may be used in AT, BE, CY, CZ, DK, EE, FI, FR, DE, GR, HU, IE, IT, LV, LT, LU, MT, NL, PL, PT, SK, SI, ES, SE, GB, IS, LI, NO, CH, BG, RO, TR

Copyright

The contents of this publication may not be reproduced in any part or as a whole, stored, transcribed in an information retrieval system, translated into any language, or transmitted in any form or by any means, mechanical, magnetic, electronic, optical, photocopying, manual, or otherwise, without the prior written permission.

Trademarks

All products, company, brand names are trademarks or registered trademarks of their respective companies. They are used for identification purpose only. Specifications are subject to be changed without prior notice.

FCC Interference Statement

The **IP-2000VPN** 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 radio interference in a commercial environment. This equipment can generate, use and radiate radio frequency energy and, if not installed and used in accordance with the instructions in this manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause interference, in which case the user, at his own expense, will be required to take whatever measures are necessary to correct the interference.

CE Declaration of Conformity

This equipment complies with the requirements relating to electromagnetic compatibility, EN 55022, EN 61000-3-2, EN 61000-3-3/A1, EN 55024, Class B.

The specification is subject to change without notice.

Table of Contents

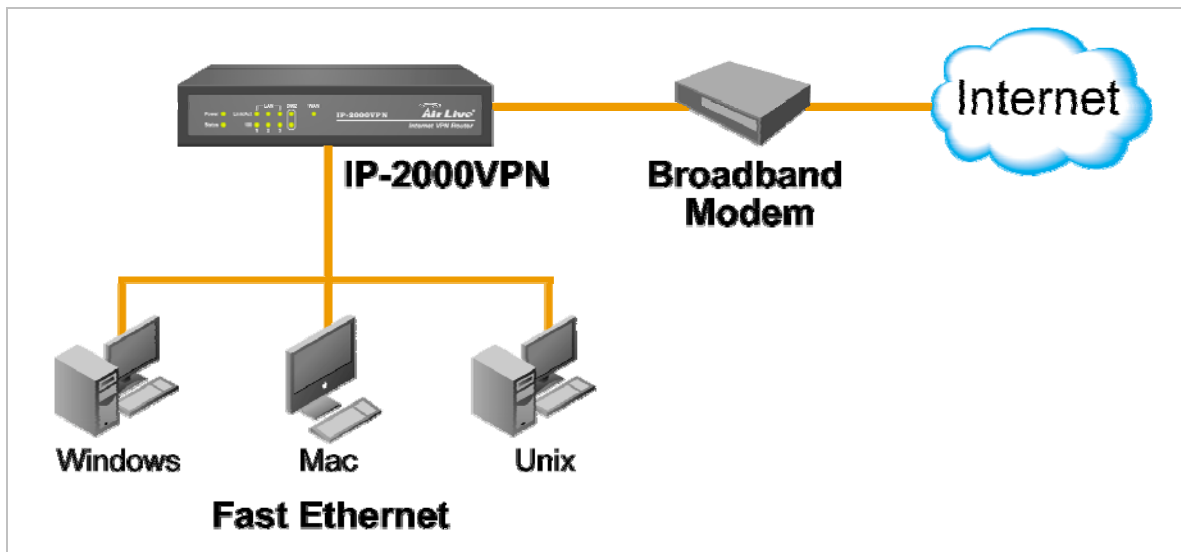
Chapter 1 Introduction	4
1.1 Features.....	5
1.2 Installation of the Router.....	8
1.3 Front Panel and Rear Panel.....	10
1.4 Packing List.....	11
1.5 Hardware DMZ.....	11
Chapter 2 Deployment	12
Chapter 3 Configure Router	15
3.1 Setup Wizard.....	16
3.2 LAN.....	21
Chapter 4 Internet Features	24
4.1 WAN Port.....	24
4.2 Advanced Internet.....	27
4.3 Dynamic DNS.....	31
4.4 Virtual Server.....	33
4.5 Options.....	36
Chapter 5 Security	37
5.1 Admin Login.....	37
5.2 Access Control.....	39
5.3 Firewall Rule.....	42
5.4 Logs.....	46
5.5 E-mail.....	49
5.6 Security Options.....	51
5.7 Scheduling.....	53
5.8 Services.....	54
Chapter 6 IPSec VPN	55
6.1 Common VPN Situations.....	55
6.2 VPN Configuration.....	57
6.3 Certificates.....	67
6.4 CLRs.....	73
6.5 Status.....	74
Chapter 7 Microsoft VPN (PPTP)	75
7.1 PPTP Server.....	75
7.2 Windows PPTP Clients Setup.....	79
Chapter 8 VPN Example	92
8.1 Office-to-office IPSec VPN – Connecting to 2 IP-2000VPN.....	93
8.2 Office-to-office IPSec VPN – Connecting IP-2000VPN and RS-1200.....	99
8.3 Getting into Office Network from Internet (PPTP) – Windows XP PPTP Client.....	105
8.4 Getting into Office Network from Internet (IPSec) – Windows XP IPSec Client.....	113

Chapter 9 Status	132
9.1 Connection Status – PPPoE	134
9.2 Connection Status – PPTP	136
9.3 Connection Status – Telstra Big Pond	138
9.4 Connection Status – SingTel RAS	140
9.5 Connection Status – Fixed/Dynamic IP Address	142
9.6 Connection Status – L2TP	144
Chapter 10 Other Features & Settings	146
10.1 Config file	146
10.2 Network Diagnostics	148
10.3 PC Database	149
10.4 Remote Administration	152
10.5 Routing	154
10.6 Upgrade Firmware	158
10.7 UPnP	159
Appendix A PC Configuration	160
Appendix B VPN Overview	169
Appendix C Troubleshooting	172
Appendix D Specifications	174

Chapter 1 Introduction

The AirLive Internet VPN Router, IP-2000VPN, features IPsec and PPTP VPN Server, to offer the easy installation VPN connection for office-to-office or client-to-office environment. Follow the wizard to configure IPsec VPN, and it will not be the difficult job to set up your own VPN environment.

The IP-2000VPN does not only feature VPN function, it is also a router built-in with SPI and DoS firewall to protect internal device; with VPN and router's feature, you can deploy AirLive IP-2000VPN in several environment such as SMB office, branch office, SOHO user and the home user.



Recommendation before starting to configure IP-2000VPN

If you want to configure **WAN interface** first:

- Please refer to **Chapter 3.1 Setup Wizard** and follow the steps to configure WAN interface. You also can refer to **Chapter 4.1 WAN Port** to configure WAN interface directly if you are an experienced user.

If you want to configure **Office-to-Office IPsec VPN** communication:

- Please refer to VPN example **Chapter 8.1 Office-to-office IPsec VPN – Connecting 2 IP-2000VPN**, or **Chapter 8.2 Office-to-office IPsec VPN – Connecting IP-2000VPN and RS-1200**.

If you want to connect office VPN from home:

- Please refer to VPN example **Chapter 8.3 Getting into Office Network from Internet (PPTP) – Windows XP PPTP Client**.

1.1 Features

IPSec VPN Features

- **IPSec.** Support for IPSec standards, including IKE and certificates.
- **10 Tunnels.** Up to 10 VPN tunnels can be created.
- **IPSec Authentication and Encryption.** Support DES, 3DES, AES-128, 192, 256 bits Encryption, and MD5, SHA-1 Authentication.

Microsoft VPN Gateway Support

- **PPTP Server.** The IP-2000VPN emulates a Microsoft PPTP VPN Server, allowing clients to use the Microsoft VPN client provided in Windows.
- **Windows Client Support.** Remote users can use the Microsoft VPN client (VPN Adapter) provided in recent versions of Windows.
- **Easy Setup.** For both the Administrator and remote users, the Microsoft VPN is much easier to configure than IPSec VPN.

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 IP-2000VPN.
- **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 IP-2000VPN 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.

Advanced Internet Functions

- **Communication Applications.** Support for Internet communication applications, such as interactive Games, Telephony, and Conferencing applications, which are often difficult to use when behind a Firewall, is included.
- **Special Internet Applications.** Applications which use non-standard connections or port numbers are normally blocked by the Firewall. The ability to define and allow such applications is provided, to enable such applications to be used normally.
- **Virtual Servers.** This feature allows Internet users to access Internet servers on your LAN. The required setup is quick and easy.
- **Multi-DMZ.** For each WAN (Internet) IP address allocated to you, one (1) PC on your local LAN can be configured to allow unrestricted 2-way communication with Servers or individual users on the Internet. This provides the ability to run programs which are incompatible with Firewalls.
- **Physical DMZ Port.** PCs connected to the DMZ port are effectively isolated from your LAN, while connected to the Internet. This provides additional security for your LAN while allowing your Servers to be accessed from the Internet.
- **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.

Internet Access Features

- **Shared Internet Access.** All users on the LAN or WLAN can access the Internet through the IP-2000VPN, 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 IP-2000VPN 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 IP-2000VPN supports both Dynamic IP Address (IP Address is allocated on connection) and Fixed IP Address.

LAN Features

- **3-Port Switching Hub.** The IP-2000VPN incorporates a 3-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 IP-2000VPN 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 IP-2000VPN'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

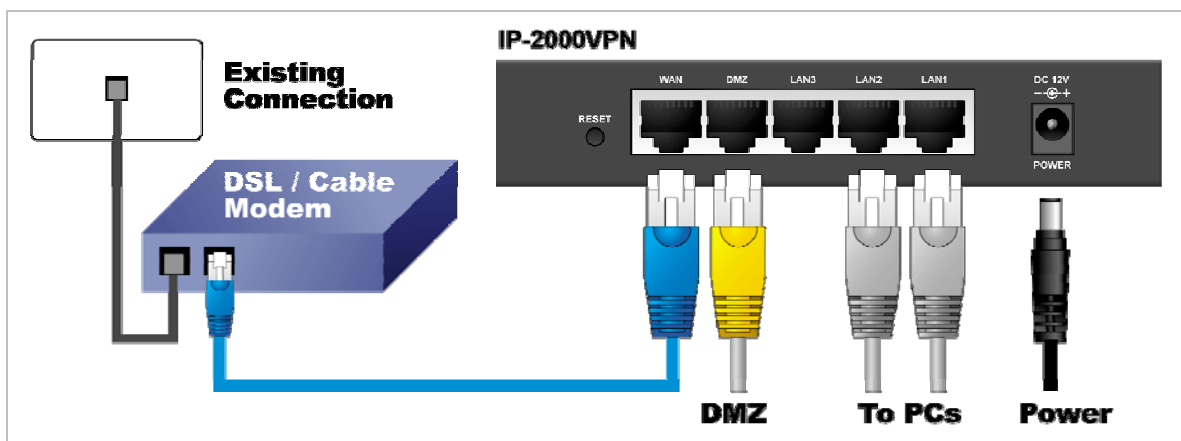
- **Easy Setup.** Use your WEB browser from anywhere on the LAN or WLAN for configuration.
- **Remote Management.** The IP-2000VPN can be managed from any PC on your LAN. And, if the Internet connection exists, it can also (optionally) be configured via the Internet.
- **UPnP Support.** UPnP (Universal Plug and Play) allows automatic discovery and configuration of the IP-2000VPN. UPnP is supported by Windows ME, XP, or later.
- **Configuration File Backup & Restore.** You can backup (download) the IP-2000VPN's configuration file to your PC, and restore (upload) a previously-saved configuration file to the IP-2000VPN.

1.2 Installation of the Router

Requirement

- Network cables. Use standard 10/100BaseT network (UTP) cables with RJ45 connectors.
- TCP/IP protocol must be installed on all PCs.
- For Internet Access, an Internet Access account with an ISP, and a Broadband modem (usually, DSL or Cable modem).

Procedure



1. Choose an Installation Site

Select a suitable place on the network to install the IP-2000VPN. Ensure the IP-2000VPN 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 IP-2000VPN. Both 10BaseT and 100BaseTX connections can be used simultaneously.
- If required, you can connect any LAN port to another Hub. Any LAN port on the IP-2000VPN 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 a PC (server) to the DMZ port. To use multiple servers, use a standard LAN cable to connect the DMZ port to a normal port on another hub, and connect your servers to the hub. PCs connected to the DMZ port are isolated from your LAN.

3. Connect WAN Cable

Connect the Broadband modem to the WAN port on the IP-2000VPN. Use the cable supplied with your Broadband modem. If no cable was supplied, use a standard LAN cable.

4. Power Up

- Power on the Broadband modem.
- Connect the supplied power adapter to the IP-2000VPN and power up. Please note that you should use only the power adapter provided. Using a different one may cause hardware damage.

5. Check the LEDs

- The **Power** LED should be ON.
- The **Status** LED should blink during start up, and 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).
- If a PC is connected to the DMZ port, the DMZ port's **Link/Act** LED should be ON (provided the PC is also ON).
- The **WAN** LED should be ON.

6. Router's default IP

- The default IP address of router's LAN port is:
IP Address: 192.168.1.1
Subnet Mask: 255.255.255.0
- For Web Management, please configure client PC as DHCP client to obtain IP address from IP-2000VPN.
- After configuring the computer's IP properly, please enter the router's IP address "192.168.1.1" in Web browser to manage the router, type the proper user name and password to pass the router's authentication.

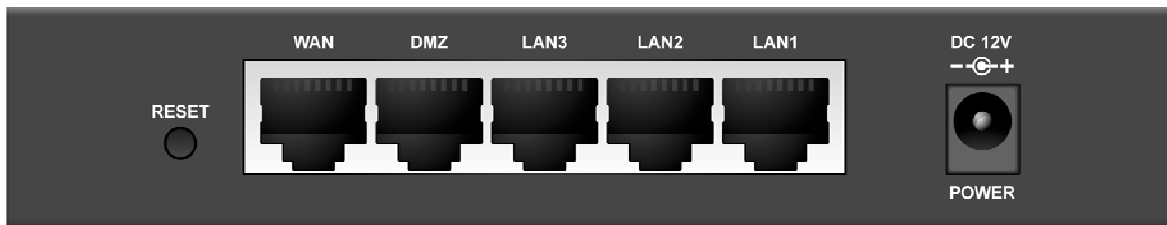
7. User name and password

- User's name: *admin*
- Password: *airlive*

1.3 Front Panel and Rear Panel



LED	Function	Color	Status	Description
Power	Power indication	● Green	On	Power on
Status	System status	● Red	On	Error condition
			Blinking	System starts up
WAN	WAN port activity	● Green	On	The WAN port is linked.
			Blinking	The WAN port is sending or receiving data.
Link/Act (LAN/DMZ)	Link status	● Green	On	An active station is connected to the corresponding port.
			Blinking	The corresponding LAN port is sending or receiving data.
100 (LAN/DMZ)	Link rate	● Orange	On	Data is transmitting in 100Mbps on the corresponding port.



Port / Button	Description
Power	Connect the supplied power adapter (DC12V, 1A) here.
WAN	The port where you will connect your cable (or xDSL) modem or Ethernet router
LAN 1 ~ 3	The ports where you will connect networked computers and other devices.
DMZ	PCs or devices connected to the DMZ port are isolated from the LAN. You can deploy one or more servers to be accessed by Internet users.
Reset	Press this button to reset system settings to factory defaults.

1.4 Packing List

The following items should be included:

- IP-2000VPN Internet VPN Router
- Installation CD-ROM
- Quick Installation Guide
- AC Adapter

When you open your package, make sure all of the above items are included and not damaged. If you see that any components are damaged, please notify your dealer immediately.

1.5 Hardware DMZ

Using the DMZ Port

The DMZ port is intended for connection of a server you wish to make available to the public. To use multiple servers, use a standard LAN cable to connect the DMZ port to a normal port on another switch, and connect your servers to the switch.

Please note the following points regarding the DMZ port:

- Although physically attached to the switch ports, the DMZ port is not part of the built-in switch. It is a separate single port which is isolated from the switch.
- PCs connected to the DMZ port are on the same LAN segment as PCs connected to the LAN ports. They must use the same IP address range.
- PCs connected to the DMZ port are NOT visible to PCs on the LAN ports. So you cannot use Microsoft networking or other networking protocols to connect to PCs on the DMZ. The connection must be made via the Internet.
- PCs connected to the DMZ port still share the WAN port IP address for Internet access.
- To make PCs on the DMZ port available from the Internet, the "Virtual Server" (Port Forwarding) feature must be configured to send incoming traffic to the appropriate server.

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, a firewall rule to allow incoming traffic from the Internet to the DMZ is automatically created. If the Server is connected to the LAN ports, you must add the firewall rule manually.

Chapter 2 Deployment

Overview

This chapter describes the setup procedure for:

- Internet Access
- LAN configuration

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

Other configuration may also be required, depending on which features and functions of the IP-2000VPN 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.	Appendix A: PC Configuration
Use any of the following Internet features: <ul style="list-style-type: none">• WAN Port• Advanced Setup• Dynamic DNS• Virtual Servers• Options	Chapter 4: Internet Features
Change any of the following Security-related settings: <ul style="list-style-type: none">• Admin Login• Access Control• Firewall Rules• Logs• E-mail• Security Options• Scheduling• Services	Chapter 5: Security
Use the IPSec VPN features: <ul style="list-style-type: none">• VPN Policies• Certificates• CRLs• VPN Status	Chapter 6: VPN (IPSec)
Use the Microsoft VPN feature: <ul style="list-style-type: none">• PPTP Server in the IP-2000VPN.• User and Client setup.• Checking VPN connection Status.	Chapter 8: Microsoft VPN
Check IP-2000VPN Status.	Chapter 9: Status

<p>Configure or use any of the following:</p> <ul style="list-style-type: none"> • Configuration File backup and restore. • Network Diagnostic • PC Database • Remote Administration • Routing • Upgrade Firmware • UPnP 	<p>Chapter 10: Other Features and Settings</p>
---	--

Configuration Program

The IP-2000VPN 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 IP-2000VPN, please ensure that:

- Your PC can establish a physical connection to the IP-2000VPN. The PC and the IP-2000VPN must be directly connected (using the switch ports on the IP-2000VPN) or on the same LAN segment.
- The IP-2000VPN must be installed and powered ON.
- If the IP-2000VPN's default IP Address (192.168.1.1) is already used by another device, the other device must be turned OFF until the IP-2000VPN is allocated a new IP Address during configuration.

Using UPnP

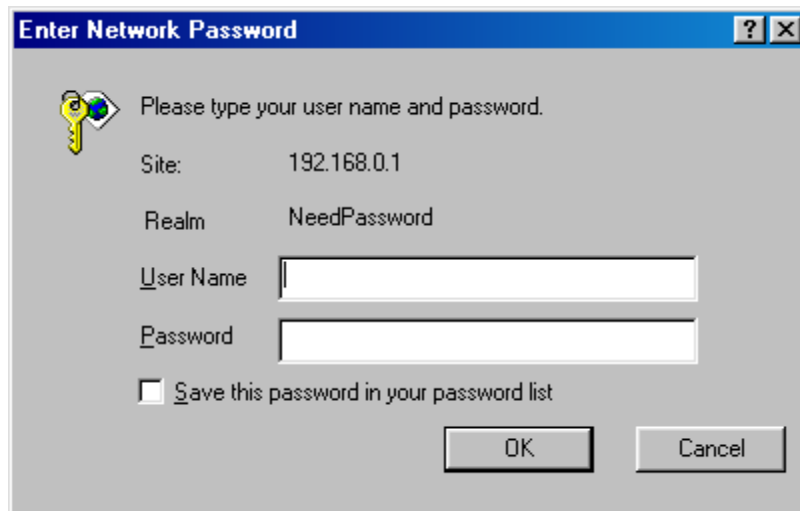
If your Windows system supports UPnP, an icon for the IP-2000VPN will appear in the system tray, notifying you that a new network device has been found, and offering to create a new desktop shortcut to the newly-discovered device.

- Unless you intend to change the IP Address of the IP-2000VPN, 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 IP-2000VPN (either on the Desktop, or in **My Network Places**) to start the configuration. Refer to the following section [錯誤! 找不到參照來源。](#) for details of the initial configuration process.

Using your Web Browser

To establish a connection from your PC to the IP-2000VPN:

1. Start your WEB browser.
2. In the *Address* box, enter "http://" and the IP Address of the IP-2000VPN, as in this example, which uses the IP-2000VPN's default IP Address: <http://192.168.1.1>
3. You will be prompted for a username and password, as shown below.



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

If you can't connect

If the IP-2000VPN does not respond, check the following:

- The IP-2000VPN is properly installed, LAN connection is OK, and it is powered ON. You can test the connection by using the "Ping" command:

- Open the MS-DOS window or command prompt window.
- Enter the command:

```
ping 192.168.1.1
```

If no response is received, either the connection is not working, or your PC's IP address is not compatible with the IP-2000VPN's IP Address. (See next item).

- If your PC is using a fixed IP Address, its IP Address must be within the range 192.168.1.2 to 192.168.1.254 to be compatible with the IP-2000VPN's default IP Address of 192.168.1.1. Also, the **Network Mask** must be set to 255.255.255.0. See **Appendix A - PC Configuration** for details on checking your PC's TCP/IP settings.

Ensure that your PC and the IP-2000VPN are on the same network segment. (If you don't have a router, this must be the case.)

Chapter 3 Configure Router

Home Screen

The first time you connect to the IP-2000VPN, you will see the *Home* screen shown below:



- 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).

3.1 Setup Wizard


The main purpose of Setup Wizard works to configure WAN type, when you finish the WAN port's configuration, you can make the test in the wizard to verify the setting.

- 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:

Cable Modem

Login method	Type	Details	ISP Data required
None	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 IP Address	Your ISP allocates a permanent IP Address to you.	IP Address, mask, gateway and DNS address allocated to you. Some ISP's may also require you to use a particular Hostname, Domain name, or MAC (physical) address.
PPPoE	Dynamic IP Address	Your IP Address is allocated automatically, when you connect to you ISP.	User name and password.
	Static IP Address	Your ISP allocates a permanent IP Address to you.	User name and password. IP Address, mask, gateway and DNS address allocated to you. Some ISP's may also require you to use a particular Hostname, Domain name, or MAC (physical) address.

Setup Wizard - Cable Modem

Use the default values if your ISP did not provide this data. 

Hostname:

Domain Name:

Login method: None
 PPPoE

MAC (physical) Address:

DSL Modem

Login method	Type	Details	ISP Data required
PPPoE	Dynamic IP Address	Your IP Address is allocated automatically, when you connect to you ISP.	User name and password.
	Static IP Address	Your ISP allocates a permanent IP Address to you.	IP Address, mask, gateway and DNS address allocated to you.
PPTP	Dynamic IP Address	You connect to the ISP only when required. The IP address is usually allocated automatically.	<ul style="list-style-type: none"> • PPTP Server IP Address. • User name and password.
	Static IP Address	Your ISP allocates a permanent IP Address to you.	<ul style="list-style-type: none"> • PPTP Server IP Address. • User name and password. • IP Address allocated to you
L2TP	Dynamic IP Address	You connect to the ISP only when required. The IP address is usually allocated automatically.	<ul style="list-style-type: none"> • L2TP Server IP Address or domain name. • User name and password.
	Static IP Address	Your ISP allocates a permanent IP Address to you.	<ul style="list-style-type: none"> • L2TP Server IP Address or domain name • User name and password. • IP Address allocated to you.

None	Dynamic IP Address	You connect to the ISP only when required. The IP address is usually allocated automatically.	Usually, none.
	Static IP Address	Your ISP allocates a permanent IP Address to you.	IP Address, mask, gateway and DNS address allocated to you.

Telstra Big Pond Cable (Australia)

Type	Details	ISP Data required
Dynamic IP Address	Your IP Address is allocated automatically, when you connect to you ISP.	<ul style="list-style-type: none"> • Big Pond Server IP Address. • User name and password.
Static IP Address	Your ISP allocates a permanent IP Address to you.	<ul style="list-style-type: none"> • Big Pond Server IP Address. • User name and password. • IP Address allocated to you.

Setup Wizard - Big Pond (Telstra, Australia)

Check the data supplied by your ISP.

Server IP Address: 60 . 250 . 158 . 64

Login User Name: test

Login Password: ●●●●

Connect behavior: Automatic Connect/Disconnect ▼

Auto-disconnect Timeout period: 15 min

< Back Next > Cancel

SingTel RAS

For this connection method, the following data is required:

- User Name
- Password
- RAS Plan

Setup Wizard - SingTel RAS

Check the data supplied by SingTel.

Login User Name: test

Login Password: ●●●●●●

RAS Plan: 512k Ethernet ▼

Connect automatically, as required

Auto-disconnect Timeout period: 0 min


Always maintain connection (keep alive)

< Back Next > Cancel

Others (e.g. Fixed 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 IP Address	Your ISP allocates a permanent IP Address to you.	IP Address, mask, gateway and DNS address allocated to you.

Setup Wizard - Internet Access

Check the type of Internet access used. 

What type of Internet access do you have ?

- Cable modem (TV-style cable)
- DSL/ADSL modem (phone-type cable)
- Telstra Bigpond Cable (Australia)
- SingTel RAS
- Other (e.g. Fixed Wireless)

3.2 LAN

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

Data - LAN Screen

TCP/IP	
IP Address	IP address for the IP-2000VPN, as seen from the local LAN. Use the default value unless the address is already in use or your LAN is using a different IP address range. In the latter case, enter an unused IP Address from within the range used by your LAN.
Subnet Mask	The default value 255.255.255.0 is standard for small (class "C") networks. For other networks, use the Subnet Mask for the LAN segment to which the IP-2000VPN is attached (the same value as the PCs on that LAN segment).
DHCP Server	<ul style="list-style-type: none"> • If enabled, the IP-2000VPN will allocate IP Addresses to PCs (DHCP clients) on your LAN when they start up. The default (and recommended) value is Enabled. • If you are already using a DHCP Server, this setting must be disabled, and the existing DHCP server must be re-configured to treat the IP-2000VPN as the default Gateway. See the following section for further details. • The Start IP Address and Finish IP Address fields set the values used by the DHCP server when allocating IP Addresses to DHCP clients. This range also determines the number of DHCP clients supported. <p>See the following section for further details on using DHCP.</p>
Buttons	
Save	Save the data on screen.
Cancel	The "Cancel" button will discard any data you have entered and reload the file from the IP-2000VPN.

What DHCP Server Can Do

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 IP-2000VPN can act as a **DHCP server**.
- Windows 2000/XP 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 IP-2000VPN'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 IP-2000VPN's **DHCP Server** function.
- Set the range of IP Addresses allocated to PCs by the DHCP Server function.



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

Using another DHCP Server

You can only use one (1) DHCP Server per LAN segment. If you wish to use another DHCP Server, rather than the IP-2000VPN's, the following procedure is required.

- Disable the DHCP Server feature in the IP-2000VPN. This setting is on the LAN screen.
- Configure the DHCP Server to provide the IP-2000VPN's IP Address as the **Default Gateway**.

To Configure your PCs to use DHCP

This is the default setting for TCP/IP under Windows 98/ME/2000/XP or else operating system.

See **Appendix A - Client Configuration** for the procedure to check these settings.

Operation

Once both the IP-2000VPN 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 4 - Internet Features** for further details.
- Applications which use non-standard connections or port numbers may be blocked by the IP-2000VPN's built-in firewall. You can define such applications as **Special Applications** to allow them to function normally. Refer to **Chapter 4 - Internet Features** for further details.
- Some non-standard applications may require use of the **DMZ** feature. Refer to **Chapter 4 - Internet Features** for further details.

Chapter 4 Internet Features

4.1 WAN Port

Overview

The following advanced features are provided.

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

WAN Port Configuration

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

The screenshot shows the 'WAN Port Configuration' window with the following settings:

- Identification**
 - Hostname: AirLive
 - Domain Name: (empty)
 - WAN Port MAC Address: 004F74300001
 - Buttons: Default, Copy from PC
- IP Address**
 - IP Address is assigned automatically (Dynamic IP Address)
 - Specified IP Address (Static IP Address)
- NAT**
 - Enable NAT, allow all LAN users to share WAN IP address.
 - Disable NAT, perform standard routing ONLY.
- DNS**
 - Automatically obtain from Server
 - Use this DNS: 168, 95, 1, 1
- Login**
 - Login Method: None (Direct connection) (dropdown menu)

Buttons at the bottom: Save, Cancel, Help

Data – WAN Port Configuration Screen

Identification	
Hostname	Normally, there is no need to change the default name, but if your ISP requests that you use a particular “Hostname”, enter it here.
Domain name	If your ISP provided a domain name, enter it here. Otherwise, it can be left blank.
MAC Address	Also called Network Adapter Address or Physical Address. This is a low-level identifier, as seen from the WAN port. Normally there is no need to change this, but some ISPs require a particular value, often that of the PC initially used for Internet access. You can use the Copy from PC button to copy your PC's address into this field, the Default button to insert the default value, or enter a value directly.
IP Address	
IP Address is assigned automatically	Also called Dynamic IP Address . This is the default, and the most common. Leave this selected if your ISP allocates an IP Address to the IP-2000VPN upon connection.
Specified IP Address	Also called Static IP Address . Select this if your ISP has allocated you a fixed IP Address. If this option is selected, the following data must be entered. <ul style="list-style-type: none"> • IP Address. The IP Address allocated by the ISP. • Network Mask (Not required for PPPoE) This is also supplied by your ISP. It must be compatible with the IP Address above. • Gateway IP Address (Not required for PPPoE) The address of the router or gateway, as supplied by your ISP.
NAT	
Enable NAT	NAT (Network Address Translation) is the technology which allows all PCs on your LAN to share the Internet IP address allocated to the WAN port on this Router. From the Internet, all PCs appear to have the same IP address. For normal operation, this setting must be ENABLED.
Disable NAT	Disabling NAT will disable Internet access, unless all PCs have valid Internet IP addresses. If you wish to use this device for Routing ONLY (and NOT for Internet access), then NAT should be disabled.

DNS	
Automatically obtain from Server	The DNS (Domain Name Server) address will be obtained automatically from your ISP's server. Note that if using a fixed IP address, with no login (login is set to "None"), then no Server is used, and this option cannot be used.
Use this DNS	If this option is selected, you must enter the IP address of the DNS (Domain Name Server) you wish to use. Note: If the DNS is unavailable, the "Backup DNS", entered on the <i>Internet - Options</i> screen, will be used.
Login	
Login Method	If your ISP does not use a login method (username, password) for Internet access, leave this at the default value "None (Direct connection)" Otherwise, check the documentation from your ISP, select the login method used, and enter the required data. <ul style="list-style-type: none"> • PPPoE - this is the most common login method, widely used with DSL modems. Normally, your ISP will have provided some software to connect and login. This software is no longer required, and should not be used. • PPTP - this is mainly used in Europe. You need to know the PPTP Server address as well as your name and password. • L2TP - You need to know the L2TP Server address as well as your name and password. • Big Pond Cable - for Australia only. • SingTel RAS - for Singapore only.
Login User Name	The User Name (or account name) provided by your ISP.
Login Password	Enter the password for the login name above.
RAS Plan	For SingTel customers only, select the RAS plan you are on.
Server Address	If using PPTP, L2TP or Big Pond Cable, enter the address of your ISP's server. For PPPoE or SingTel RAS, the Server address is not required.
Connection behavior	Select the desired option: <ul style="list-style-type: none"> • Automatic Connect/Disconnect An Internet connection is automatically made when required, and disconnected when idle for the time period specified by the "Auto-disconnect Idle Time-out". • Manual Connect/Disconnect You must manually establish and terminate the connection. • Keep alive (maintain connection) The connection will never be disconnected by this device. If

	disconnected by your ISP, the connection will be re-established immediately. (However, this does not ensure that your Internet IP address will remain unchanged.)
Auto-disconnect Idle Time-out	This field has no effect unless the setting above is <i>Automatic Connect/Disconnect</i> . If Auto-disconnect is being used, enter the desired idle time-out period (in minutes). After the connection to your ISP has been idle for this time period, the connection will be terminated.

4.2 Advanced Internet

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

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

Advanced Internet

Communication Applications Select an Application: Age of Empires
H323(CUseeME & MS NetMeeting & TGI Phone)
ICU II (ICU 2)
Internet Phone

Send incoming calls to: Select a PC

Save when finished, not after each change.

Special Applications If an application does not work, you can define it as a Special Application. Special Applications

Multi-DMZ If you have only 1 WAN IP address, only DMZ 1 can be used.

Enable	WAN IP address	PC
1. <input type="checkbox"/>	192 . 168 . 0 . 38	Select a PC
2. <input type="checkbox"/>	0 . 0 . 0 . 0	Select a PC
3. <input type="checkbox"/>	0 . 0 . 0 . 0	Select a PC
4. <input type="checkbox"/>	0 . 0 . 0 . 0	Select a PC
5. <input type="checkbox"/>	0 . 0 . 0 . 0	Select a PC
6. <input type="checkbox"/>	0 . 0 . 0 . 0	Select a PC
7. <input type="checkbox"/>	0 . 0 . 0 . 0	Select a PC

[My PC is not listed](#)

URL Filter Enable [URL Filter](#) Configure URL Filter

Communication Applications

Most applications are supported transparently by the IP-2000VPN. But sometimes it is not clear which PC should receive an incoming connection. This problem could arise with the **Communication Applications** listed on this screen.

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

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

Special Applications

If you use Internet applications with non-standard connections or port numbers, you may find that they do not function correctly because they are blocked by the IP-2000VPN'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.

	Name	Incoming Ports			Outgoing Ports		
		Type	Start	Finish	Type	Start	Finish
1. <input type="checkbox"/>	dialpad	udp	51200	51201	udp	51200	51201
2. <input type="checkbox"/>	paltalk	udp	2090	2091	udp	2090	2091
3. <input type="checkbox"/>	quicktime	udp	6970	6999	tcp	554	554
4. <input type="checkbox"/>		udp			udp		
5. <input type="checkbox"/>		udp			udp		
6. <input type="checkbox"/>		udp			udp		

Data – Special Applications Screen

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

Using a Special Application

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



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

Multi-DMZ

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

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

- This allows almost any application to be used on the "DMZ PC".
- The "DMZ PC" will receive all "Unknown" connections and data.
- If the DMZ feature is enabled, you must select the PC to be used as the "DMZ PC".
- To use more than one (1) DMZ, your ISP must assign multiple fixed IP addresses to you. You must enter each IP address; you can then assign a DMZ PC for each IP address.



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

URL Filter

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

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

URL Filter Screen

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

URL Filter

Filter Strings

When enabled, a request is blocked if any of these entries occur in the requested URL.

Current Entries

Delete Delete All

Add Filter String: Add

Filter Strings should be as specific as possible.

Help Close

Data – URL Filter Screen

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

4.3 Dynamic DNS

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

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

The Service works as follows:

1. You must register for the service at one of the listed DDNS Service providers.
2. After registration, follow the Service Provider's procedure to request a Domain Name, and have it allocated to you.
3. Enter your DDNS data on the IP-2000VPN's DDNS screen (shown below).
4. The IP-2000VPN will then automatically ensure that your current IP Address is recorded and updated at the DDNS server.

If the DDNS Service provides software to perform this "IP address update"; you should disable the "Update" function, or not use the software at all.

5. From the Internet, users will be able to connect to your Virtual Servers (or DMZ PC) using your Domain name, as shown on this screen.

Dynamic DNS Screen

Select **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.

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

DDNS Service:

User Name:

Password:

Domain Name: . .

DDNS Status: Username, password, and hostname must not be blank

Data – Dynamic DNS Screen

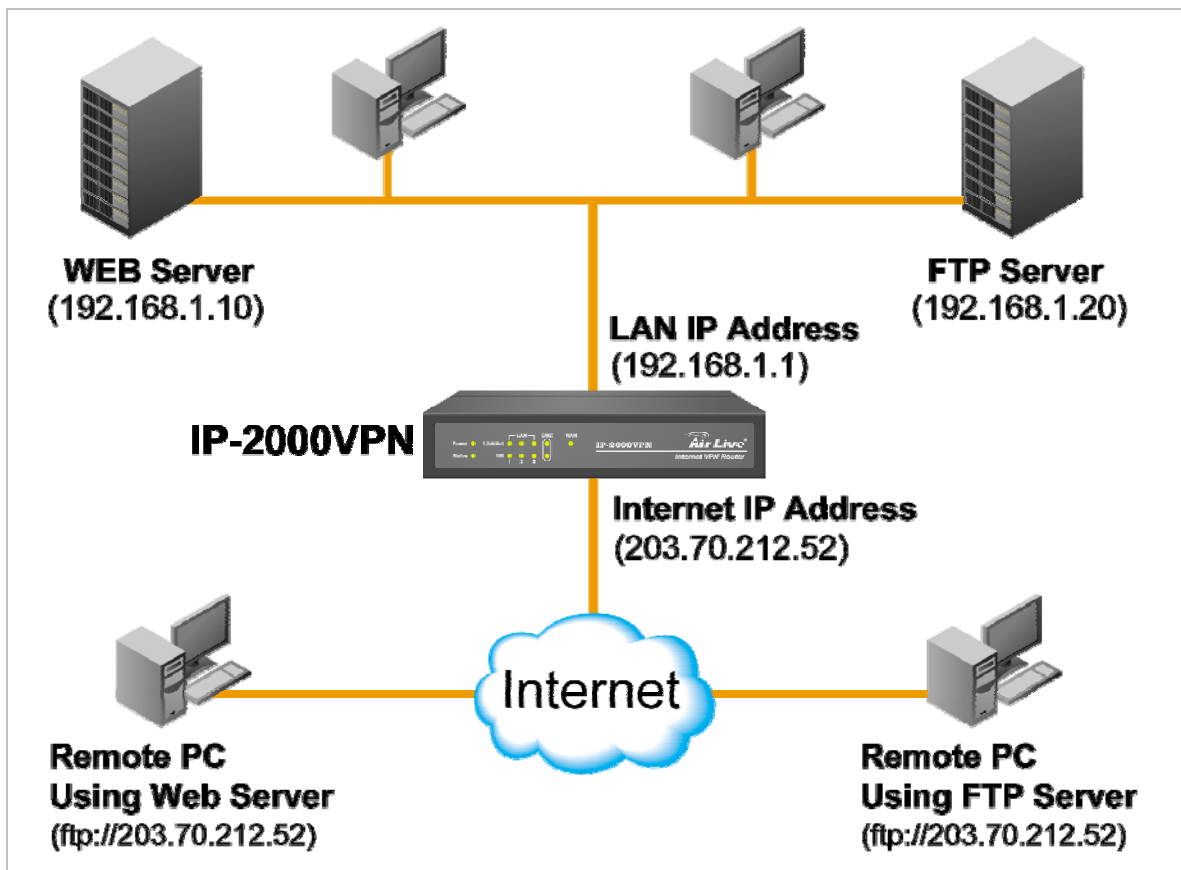
DDNS Service	
DDNS Service	<ul style="list-style-type: none"> You must register for the service at one of the listed Service Providers. You can reach the Service provider's Web Site by selecting them in the list and clicking the "Web Site" button. Apply for a Domain Name, and ensure it is allocated to you. Details of your DDNS account (Name, password, Domain name) must then be entered and saved on this screen. This device will then automatically ensure that your current IP Address is recorded by the DDNS Service Provider. (You do NOT need to use the "Client" program provided by some DDNS Service providers.) From the Internet, users will now be able to connect to your Virtual Servers (or DMZ PC) using your Domain name.
DDNS Data	
DDNS Service	Select the desired DDNS Service provider.
User Name	Enter your Username for the DDNS Service.
Password/Key	Enter your current password for the DDNS Service.
Domain Name	Enter the domain name allocated to you by the DDNS Service. If you have more than one name, enter the name you wish to use.
DDNS Status	<ul style="list-style-type: none"> This message is returned by the DDNS Server Normally, this message should be something like "Update successful" or "IP address updated". If the message indicates some problem, you need to connect to the DDNS Service provider and correct this problem.

4.4 Virtual Server

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.



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 (switch) ports, you must add the firewall rule manually.



The DMZ port is a normal port, not an "uplink" port. If connecting to a switch, connect to the standard port on the switch.

Virtual Server Screen

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

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.

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

DDNS Service:

User Name:

Password:

Domain Name: . .

DDNS Status: Username, password, and hostname must not be blank

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

Data – Virtual Servers Screen

Servers	
Servers	This lists a number of pre-defined Servers, plus any Servers you have defined. Details of the selected Server are shown in the "Properties" area.
Properties	
Enable	Use this to Enable or Disable support for this Server, as required. <ul style="list-style-type: none">• If Enabled, any incoming connections will be forwarded to the selected PC.• If Disabled, any incoming connection attempts will be blocked.
PC (Server)	Select the PC for this Server. The PC must be running the appropriate Server software.

Defining your own Virtual Servers

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

Connecting to the Virtual Servers

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

e.g.

http://203.70.212.52

ftp://203.70.212.52

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

4.5 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.

Options

Backup DNS Backup DNS (1) IP Address:

Backup DNS (2) IP Address:

These DNS (Domain Name Servers) are used only if the primary DNS is unavailable.

MTU MTU (Maximum Transmission Unit): (1..1500) bytes

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	<p>MTU (Maximum Transmission Unit) value should only be changed if advised to do so by Technical Support.</p> <ul style="list-style-type: none">• 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 5 Security

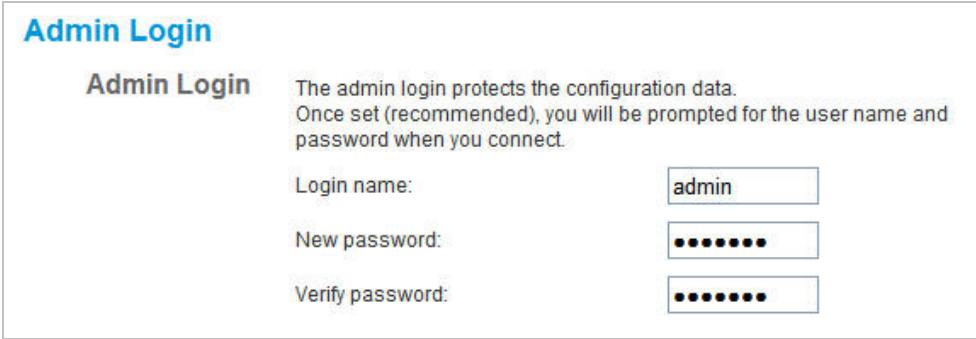
Overview

The following advanced configurations are provided.

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

5.1 Admin Login

The Admin Login screen allows you to assign a user name and password to the IP-2000VPN.



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.

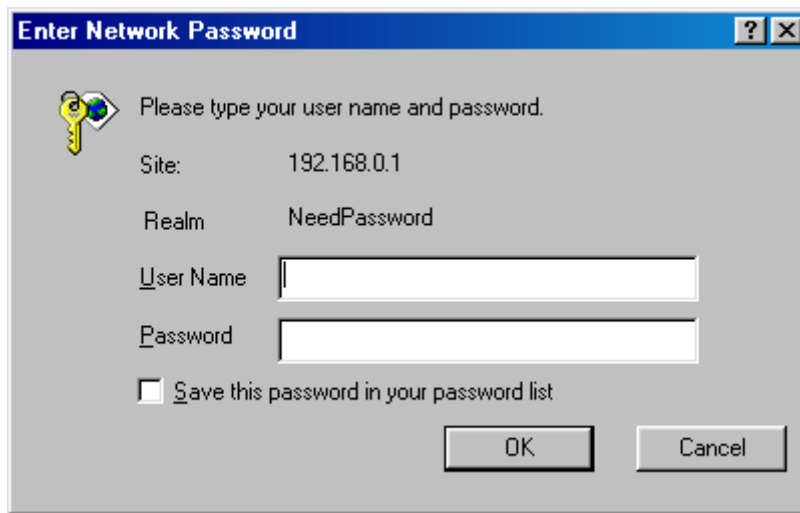
Login name:

New password:

Verify password:

1. The default login name is "admin". Change this to the desired value.
2. The default password is airlive. 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 IP-2000VPN, as shown below.



The image shows a Windows-style dialog box titled "Enter Network Password". The title bar is blue with a question mark icon and a close button. The main area has a grey background. On the left, there is a yellow key icon. To the right of the icon, the text reads "Please type your user name and password." Below this, there are two lines of text: "Site: 192.168.0.1" and "Realm: NeedPassword". Underneath, there are two input fields: the first is labeled "User Name" and the second is labeled "Password". At the bottom left, there is a checkbox with the label "Save this password in your password list". At the bottom right, there are two buttons: "OK" and "Cancel".

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

5.2 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.

The screenshot shows the 'Access Control' configuration interface. At the top, there is a 'Group' dropdown menu set to 'Default' and a 'Members' button. Below this, the 'Internet Access' section contains two dropdown menus: 'Restrictions' set to 'None' and 'Block by Schedule' set to 'None'. A 'Services' list is displayed below, containing the following items: ALL(TCP/UDP:1..65534), AIM(TCP:5190), BGP(TCP:179), BOOTP_CLIENT(UDP:68), BOOTP_SERVER(UDP:67..68), CU-SEEME(TCP/UDP:7648), DNS(TCP/UDP:53), and FINGER(TCP:79). At the bottom of the screen, there is a note: 'Select Services to Block. Hold CTRL key (on MAC, SHIFT) to select multiple items'.

Data – Access Control Screen

Group	
Group	Select the desired Group. The screen will update to display the settings for the selected Group. Groups are named "Default", "Group 1", "Group 2", "Group 3" and "Group 4", and cannot be re-named.
"Members" Button	<p>Click this button to add or remove members from the current Group.</p> <ul style="list-style-type: none"> • If the current group is "Default", then members can not be added or deleted. This group contains PCs not allocated to any other group. • To remove PCs from the Default Group, assign them to another Group. • To assign PCs to the Default Group, delete them from the Group they are currently in. <p>See the following section for details of the <i>Group Members</i> screen.</p>
Internet Access	
Restrictions	<p>Select the desired options for the current group:</p> <ul style="list-style-type: none"> • None - Nothing is blocked. Use this to create the least restrictive group. • Block all Internet access - All traffic via the WAN port is blocked. Use this to create the most restrictive group. • Block selected Services - You can select which Services are to block. Use this to gain fine control over the Internet access for a group.
Block by Schedule	<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> <p>To define the schedule, use the Schedule option on the menu.</p>
Services	This lists all defined Services. Select the Services you wish to block. To select multiple services, hold the CTRL key while selecting. (On the Macintosh, hold the SHIFT key rather than CTRL.)
Buttons	
Members	<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 Group Members screen.</p>
Save	Save the data on screen.
Cancel	Reverse any changes made since the last "Save".
View Log	<p>Click this to open a sub-window where you can view the "Access Control" log.</p> <p>This log shows attempted Internet accesses which have been blocked by the Access Control feature.</p>
Clear Log	Click this to clear and restart the "Access Control" log, making new entries easier to read.

Group Members Screen

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

The screenshot shows a web interface titled "Group Members". At the top, it says "Group: Group 1". Below this, there are two main sections: "Members (PCs)" on the left and "Other PCs" on the right. The "Members (PCs)" section is currently empty. The "Other PCs" section contains one entry: "Jacky 192.168.1.2 (LAN)". Between these two sections are two buttons: "Del >>" and "<< Add".

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.



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:

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

5.3 Firewall Rule

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

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

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

This feature is for advanced administrators only!

Firewall Rules Screen

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



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

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.

Name	Source	Destination	Action
------	--------	-------------	--------

Data – Firewall Rules Screen

Rule List	
View Rules for ...	Select the desired option; the screen will update and list any current rules. If you have not defined any rules, the list will be empty.
Data	<p>For each rule, the following data is shown:</p> <ul style="list-style-type: none"> • Name - The name you assigned to the rule. • Source - The traffic covered by this rule, defined by the source IP address. If the IP address is followed by ... this indicates there is range of IP addresses, rather than a single address. • Destination - The traffic covered by this rule, defined by destination IP address. If the IP address is followed by ... this indicates there is range of IP addresses, rather than a single address. • Action - Action will be "Forward" or "Block"
Add	To add a new rule, click the "Add" button, and complete the resulting screen. See the following section for more details.
Edit	To Edit or modify an existing rule, select it and click the "Edit" button.
Move	<p>There are 2 ways to change the order of rules</p> <ul style="list-style-type: none"> • Use the up and down indicators on the right to move the selected rule. You must confirm your changes by clicking "OK". If you change your mind before clicking "OK", click "Cancel" to reverse your changes. • Click "Move" to directly specify a new location for the selected rule.
Delete	To delete an existing rule, select it and click the "Delete" button.
View Log	Clicking the "View Log" button will open a new window and display the Firewall log.
System Rules	Clicking the "System Rules" button will open a new window and display the default firewall rules currently applied by the system. These rules cannot be edited, but any rules you create will take precedence over the default rules.

Define Firewall Rule

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

Add/Edit Firewall Rule

Name	<input type="text"/>
Type	DMZ => WAN ▾
Source IP	IP Type : Any ▾ Start IP address: <input type="text"/> 0 <input type="text"/> 0 <input type="text"/> 0 <input type="text"/> 0 Finish IP address: <input type="text"/> 0 <input type="text"/> 0 <input type="text"/> 0 <input type="text"/> 0 Subnet Mask: <input type="text"/> 255 <input type="text"/> 255 <input type="text"/> 255 <input type="text"/> 0
Dest IP	IP Type : Any ▾ Start IP address: <input type="text"/> 0 <input type="text"/> 0 <input type="text"/> 0 <input type="text"/> 0 Finish IP address: <input type="text"/> 0 <input type="text"/> 0 <input type="text"/> 0 <input type="text"/> 0 Subnet Mask: <input type="text"/> 255 <input type="text"/> 255 <input type="text"/> 255 <input type="text"/> 0
Service	ALL(TCP/UDP:1..65534) ▾
Action	Block ▾
Log	Never ▾

Data – Define Firewall Rule Screen

Define Firewall Rule	
Name	Enter a suitable name for this rule.
Type	This determines the source and destination ports for traffic covered by this rule. Select the desired option.
Source IP	<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"> • Any - All traffic from the source port is covered by this rule. • Single address - Enter the required IP address in the "Start IP address" field". You can ignore the "Subnet Mask" field. • Range address - If this option is selected, you must complete both the "Start IP address" and "Finish IP address" fields. You can ignore the "Subnet Mask" field. • Subnet address - If this option is selected, enter the required mask in the "Subnet Mask" field.
Dest IP	<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"> • Any - All traffic from the source port is covered by this rule. • Single address - Enter the required IP address in the "Start IP address" field". You can ignore the "Subnet Mask" field. • Range address - If this option is selected, you must complete both the "Start IP address" and "Finish IP address" fields. You can ignore the "Subnet Mask" field. • Subnet address - If this option is selected, enter the required mask in the "Subnet Mask" field.
Services	Select the desired Service or Services. This determines which packets are covered by this rule, based on the protocol (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.
Action	Select the desired action for packets covered by this rule:
Log	This determines whether packets covered by this rule are logged. Select the desired option.

5.4 Logs

The Logs record various types of activity on the IP-2000VPN. 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 IP-2000VPN, log data can also be E-mailed to your PC or sent to a Syslog Server.

Logs

Enable Logs

- Incoming Traffic Log**
 - All IP traffic
 - All TCP/UDP/ICMP traffic
- Outgoing Traffic Log**
 - All IP traffic
 - All TCP/UDP/ICMP traffic
- Web Site Log**
- VPN Log**
- System Log**
 - Router operations (start up, get time etc)
 - Connections to the Web-based interface of this Router
 - Other connections and traffic to this Router
 - Known DoS attacks and Port Scans

Timezone Timezone:

Syslog

- Enable Syslog
- Syslog Server:
- Include:
 - Incoming Outgoing
 - Web Sites System VPN

Data – Logs Screen

Enable Logs	
Incoming Traffic	<p>Select the desired option:</p> <ul style="list-style-type: none"> • All IP traffic - this will log all incoming TCP/IP connections, of any type. This will generate the largest logs, and fill the internal log buffer more quickly. • All TCP/UDP/ICMP traffic - These 3 protocols are used by most internet traffic. TCP is used by HTTP, FTP, Telnet, E-mail and other common Internet protocols and applications. UDP is used by Video streams and other communications where speed is more important than guaranteed delivery. ICMP is used by the "ping" and "trace route" applications, and other network diagnostics.
Outgoing Traffic	<p>Select the desired option:</p> <ul style="list-style-type: none"> • All IP traffic - - this will log all outgoing TCP/IP connections, of any type. This will generate the largest logs, and fill the internal log buffer more quickly. • All TCP/UDP/ICMP traffic - These 3 protocols are used by most internet traffic. TCP is used by HTTP, FTP, Telnet, E-mail and other common Internet protocols and applications. UDP is used by Video streams and other communications where speed is more important than guaranteed delivery. ICMP is used by the "ping" and "trace route" applications, and other network diagnostics. <p>Because most connections are logged, the logs will still be large.</p> <ul style="list-style-type: none"> • Selected Traffic only - This selection will reduce the size of the log considerably. Only HTTP connections are logged. Select the traffic you wish to include: <ul style="list-style-type: none"> • Attempted access to blocked sites - This will only log Web connections which are blocked by the URL filter. • Websites and news groups - This logs successful (allowed) connections to Web Sites and newsgroup servers.

System Log	<p>Select the desired option:</p> <ul style="list-style-type: none"> • Router operations (start up, get time etc) - This option will log normal Router operations. • Connections to the Web - based interface of this Router - This option will log each connection to the Router itself, whenever the Web-based management interface is used. • Other connections and traffic to this Router - This option will log other traffic sent to the Router itself, such as "pings" or RIP (Router Information Protocol) packets. • Known DoS attacks and Port Scans - This will log details of DoS (Denial of Service) attacks which have been blocked by the built-in Firewall. This Firewall uses "Stateful Inspection" technology to block packets which are individually valid, but collectively form an attack. Port scans, where a series of ports are checked to see if they are opened (available) and also logged.
VPN	If enabled, the VPN log will record incoming and outgoing VPN connections.
View Log Button	Use this to view each log, as required.
Clear Log Button	Use this to restart the required log. This makes it easier to read the latest entries.
Timezone	
Timezone	Select the correct Timezone for your location. This is required for the date/time shown on the logs to be correct.
Syslog Server	
Enable Syslog	If enabled, log data will be sent to your Syslog Server.
Syslog Server	Enter the IP address of your Syslog Server.
Include	Select the logs you wish to be included in the data sent to the Syslog Server.

5.5 E-mail

E-Mail

E-Mail Alert Send E-mail alert immediately when attacked

E-Mail Logs Send logs by E-Mail Send Log Now

Include: Incoming Traffic
 Outgoing Traffic
 System Log
 VPN Log
 Web Site Log

Send: When log is full
 Every Sunday ▼ at 1 ▼ AM ▼

E-mail address:

Subject:

SMTP Server: Address:
 IP address:

Port No. (Default: 25)

Data – E-mail Screen

E-Mail Alerts	
Send E-Mail alert	If enabled, an E-mail will be sent immediately if a DoS (Denial of Service) attack is detected. If enabled, the E-mail address information must be provided.
E-Mail Logs	
Send Logs by E-Mail	If enabled, logs will be logs to the specified E-mail address. You need to select the Logs to be E-mailed, and complete the E-mail address settings on this screen.
Include	Select the log items to be included in the E-mail.
Send	<p>Select the desired option for sending the log by E-mail.</p> <ul style="list-style-type: none"> When log is full - The time is not fixed. The log will be sent when the log is full, which will depend on the volume of traffic. Every day, Every Monday... - The log is sent on the interval specified. <ul style="list-style-type: none"> If "Every day" is selected, the log is sent at the time specified. If the day is specified, the log is sent once per week, on the specified day. Select the time of day you wish the E-mail to be sent. If the log is full before the time specified to send it, it will be sent regardless.
E-mail address	Enter the E-mail address the Log is to be sent to. The E-mail will also show this address as the Sender's address.

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

5.6 Security Options

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

Security Options

DoS Firewall Enable DoS (Denial of Service) Firewall

Threshold: High (WAN bandwidth > 2 Mbps)

Medium (WAN bandwidth 1 - 2 Mbps)

Low (WAN bandwidth < 1 Mbps)

If Enabled (recommended), invalid packets and connections are dropped. The "Threshold" affects invalid connections only.

Options

Respond to ICMP (ping) on WAN interface

Allow VPN Passthrough (IPsec, PPTP, L2TP)

Drop fragmented IP packets

Block TCP Flood

Block UDP Flood

Block non-standard packets

Data – Security Options Screen

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

Options	
Respond to ICMP (ping)	<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"> • If checked, the IP-2000VPN will respond to ICMP packets received from the Internet. • If not checked, ICMP packets from the Internet will be ignored. Disabling this option provides a slight increase in security.
Allow VPN pass-through	<p>If enabled, PCs on the LAN can use VPN software to connect to remote clients via the Internet connection. The protocols supported are:</p> <ul style="list-style-type: none"> • IPsec IPsec protocol is used to establish a secure connection, and is widely used by VPN (Virtual Private Networking) programs. • PPTP PPTP (Point to Point Tunneling Protocol) is widely used by VPN (Virtual Private Networking) programs. • L2TP L2TP is a protocol developed by Cisco for VPNs (Virtual Private Networks).
Drop fragmented IP packets	<p>If enabled, fragmented IP packets are discarded, forcing re-transmission of these packets. In some situations, this could prevent successful communication. Normally, this setting should be disabled.</p>
Block TCP Flood	<p>A TCP flood is excessively large number of TCP connection requests. This is usually a DoS (Denial of Service) attack. This setting should normally be enabled.</p>
Block UDP Flood	<p>A UDP flood is excessively large number of UDP packets. This is usually a DoS (Denial of Service) attack. This setting should normally be enabled.</p>
Block non-standard packets	<p>Abnormal packets are often used by hackers and in DoS attacks, but may also be generated by incorrectly configured network devices. (PCs will normally not generate non-standard packets.) This setting should normally be enabled.</p>

5.7 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.

Define Schedule

Default Schedule Use 24 hour clock: On all day: 00:00 to 24:00
Off all day: All fields blank

Day	Session 1		Session 2	
	Start	Finish	Start	Finish
Monday	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
Tuesday	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
Wednesday	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
Thursday	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
Friday	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
Saturday	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
Sunday	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

Data – Define Schedule Screen

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

5.8 Services

Services are used in defining traffic to be blocked or allowed by the **Access Control** or **Firewall 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.

The screenshot shows the 'Services' configuration interface. At the top, there is a section titled 'Available Services' containing a list box with the following entries: ALL(TCP/UDP:1..65534), AIM(TCP:5190), BGP(TCP:179), BOOTP_CLIENT(UDP:68), BOOTP_SERVER(UDP:67..68), and CU-SEEME(TCP/UDP:7648). Below the list is a 'Delete' button. Underneath is the 'Add New Service' section, which includes a 'Name' text input field, a 'Type' dropdown menu currently set to 'TCP', 'Start Port' and 'Finish Port' text input fields with '(TCP or UDP)' labels, and an 'ICMP Type' dropdown menu currently set to 'n/a' with '(0..255)' as a label.

Data – Services Screen

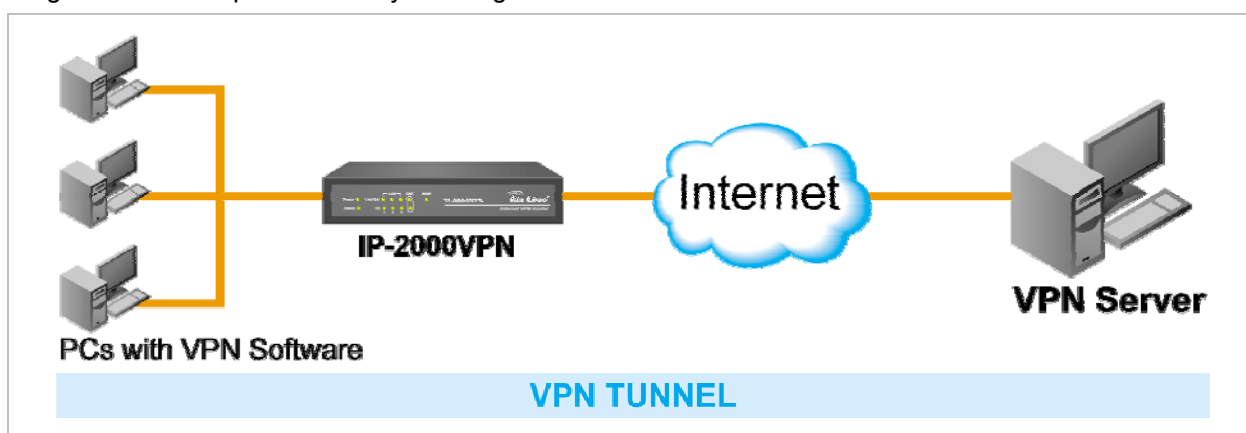
Available Services	
Available Services	This lists all defined Services.
Delete Button	Use this to delete the selected Service from the list. Note that you can only delete Services you have added; the pre-defined services can not be deleted.
Add New Service	
Name	Enter a suitable name for this Service.
Type	Select the correct type for this Service.
Start Port	If the "Type" (above) is TCP, UDP, or TCP/UDP, enter the port number for this Service. If a port range is required, enter the beginning of the range here, and the end of the range in the "Finish Port" field.
Finish Port	If the "Type" (above) is TCP, UDP, or TCP/UDP, this field can be used to enter the end of range of port numbers. This can be left blank if not required.
ICMP Type	If the "Type" (above) is ICMP, enter the ICMP type here. Otherwise, this field should be left blank.

Chapter 6 IPsec VPN

6.1 Common VPN Situations

VPN Pass-through

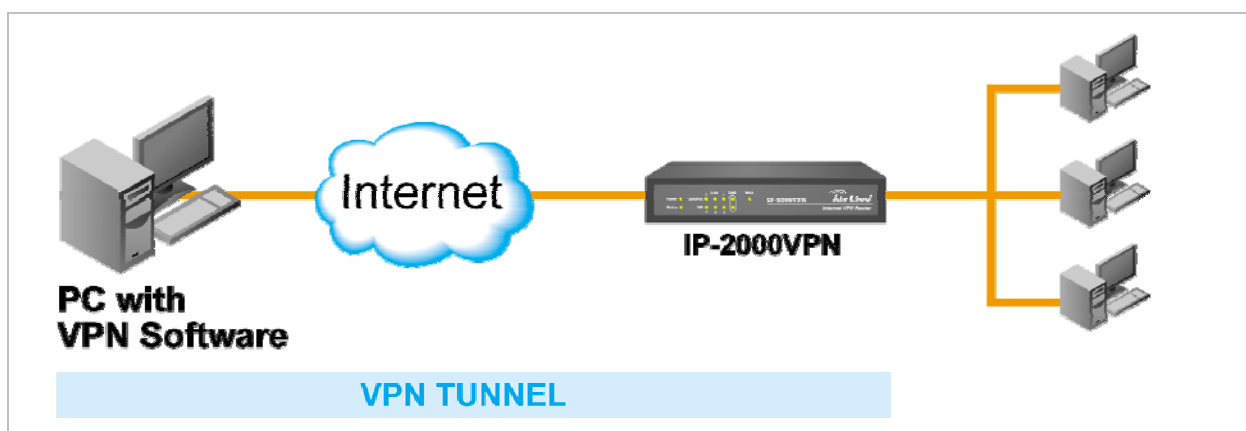
Here, a PC on the LAN behind the Router/Gateway is using VPN software, but the Router/Gateway is NOT acting as a VPN endpoint. It is only allowing the VPN connection.



- 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-to-Office VPN Gateway

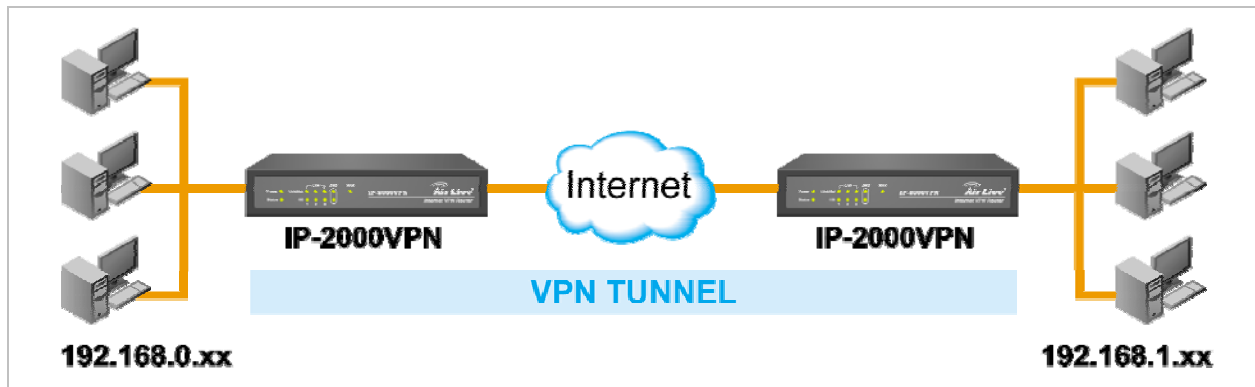
In this situation, the PC must run appropriate VPN client software in order to connect, via the Internet, to the IP-2000VPN. Once connected, the client PC has the same access to LAN resources as PCs on the local LAN (unless restricted by the network administrator).



- Windows 2000 and Windows XP include a suitable IPsec VPN client program. Configuration of this client program for use with the IP-2000VPN is covered later in this document.

Office-to-Office VPN Gateway

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.

6.2 VPN Configuration

This section covers the configuration required on the IP-2000VPN 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.

The screenshot shows a window titled "VPN Policies". At the top, there are four column headers: "Policy Name", "Enable", "Remote VPN Endpoint", and "Key Type". Below these headers is a large empty rectangular area representing the policy list. To the right of this area are four vertically stacked buttons: an up arrow, an "OK" button, a "CANCEL" button, and a down arrow. Below the main area, there is a row of five buttons: "Edit", "Move", "Enable/Disable", "Copy", and "Delete". At the bottom of the window, there are three more buttons: "Add New Policy", "View Log", and "Help".



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

Data – VPN Policies Screen

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

Move	<p>The order in which policies are listed is only important if you have multiple policies for the same remote site. In that case, the first matching policy is used. There are 2 ways to change the order of policies:</p> <ul style="list-style-type: none"> • 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. • Click "Move" to directly specify a new location for the selected policy.
Enable/Disable	Use this to toggle the On/Off state of the selected policy.
Copy	<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>
Delete	To delete an existing policy, select it and click the "Delete" button.
View Log	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 New Policy** button on the **VPN Policies** screen. This will start the VPN Wizard, as shown below.

VPN Wizard

Check the VPN settings used by the remote VPN Server/Gateway.

This Wizard will configure your Router for a VPN connection to a remote VPN Endpoint (Server, Gateway, or Client).

- You will need to know the settings used on the remote VPN Endpoint.
- If using a Certificate for authentication, you must obtain your Certificate from a CA (Certification Authority) before running this Wizard.
- If you prefer to use a setup screen instead of a Wizard, click the "Setup Screen" button below.

Setup Screen

Next > Cancel

- 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.

VPN Wizard - General Information

General information about the VPN tunnel.

Policy Name:

Enable Policy

Allow NetBIOS traffic

Remote Endpoint Address: Dynamic IP

Fixed IP:

Domain Name:

Keys: Manually assigned

Use IKE (Internet Key Exchange)

< Back Next > Cancel

General Settings	
Policy Name	Enter a suitable name. This name is not supplied to the remote VPN. It is used only to help you manage the policies.
Enable Policy	Enable or disable the policy as required. For each remote VPN, only 1 policy can be enabled at any time.
Allow NetBIOS traffic	Enable this if you require NetBIOS traffic to be transferred through the VPN tunnel. NetBIOS is used by Microsoft (Windows) networking. This setting should not be enabled unless necessary, because it increases traffic volume.
Remote VPN Endpoint	The Internet IP address of the remote VPN endpoint (Gateway or client). <ul style="list-style-type: none"> • Dynamic. Select this if the Internet IP address is unknown. In this case, only incoming connections are possible. • Fixed. Select this if the remote endpoint has a fixed Internet IP address. If selected, enter the Internet IP address of the remote endpoint. • Domain Name. Select this if the remote endpoint has a Domain Name associated with it. If selected, enter the Domain Name of the remote endpoint.
Keys	Select Manually assigned or IKE (Internet Key Exchange) 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:

- 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	<ul style="list-style-type: none"> • Any - no additional data is required. Any IP address is acceptable. <ul style="list-style-type: none"> • For outgoing connections, this allows any PC on LAN to use the VPN tunnel. • For incoming connections, this allows any 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. <p>The remote VPN must have these IP addresses entered as its "Remote" addresses.</p>

Remote IP addresses	
Type	<ul style="list-style-type: none"> • 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. <p>The remote VPN should have these IP addresses entered as its "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

These settings must match the remote VPN.

VPN Wizard - Manually assigned Keys

These settings must match the remote VPN Endpoint.

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

ESP Encryption Encryption Algorithm: 3DES ▼
 Key Size: 256 Bits ▼ (AES only)
 Key - In:
 Key - Out:

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

ESP SPI In: Out:



You cannot use both AH and ESP at the same time.

Manually assigned Keys	
AH Authentication	<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>Keys</p> <ul style="list-style-type: none"> • 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. • Keys can be in ASCII or Hex (0 ~ 9 A ~ F) • For MD5, the keys should be 32 hex/16 ASCII characters. • For SHA-1, the keys should be 40 hex/20 ASCII characters. <p>SPI</p> <ul style="list-style-type: none"> • Each SPI (Security Parameter Index) must be unique. • 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. • Each SPI should be at least 3 characters.
ESP Encryption	<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> <p>Encryption Algorithm</p> <ul style="list-style-type: none"> • The 3DES algorithm provides greater security than DES, but is slower. • If using AES, you must select the <i>Key Size</i>. If using DES or 3DES, this field is ignored. <p>Key - In / Key - Out</p> <ul style="list-style-type: none"> • 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. • For DES, keys should be 8 ASCII characters (16 HEX chars). • For 3DES, keys should be 24 ASCII characters (48 HEX chars). • If using AES encryption, the key input size must match the Key Size selected above.
ESP Authentication	<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"> • 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. • Keys can be in ASCII or Hex (0 ~ 9 and A ~ F) • For MD5, the keys should be 32 hex/16 ASCII characters. • For SHA-1, the keys should be 40 hex/20 ASCII characters.

ESP SPI	<p>This is required if either ESP Encryption or ESP Authentication is enabled.</p> <ul style="list-style-type: none"> • Each SPI (Security Parameter Index) must be unique. • 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. • Each SPI should be at least 3 characters.
----------------	---

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. This screen sets the parameters for the IKE SA.

VPN Wizard - IKE Phase 1 (IKE SA)

These settings must match the remote VPN Endpoint.

Local Identity
Type: WAN IP Address Data:

Remote Identity
Type: Remote WAN IP Data:

Authentication RSA Signature (requires Certificate)
 Pre-shared Key

Authentication Algorithm: MD5

Encryption Algorithm: 3DES Key Size: n/a (AES only)

IKE Exchange Mode: Main Mode

Direction: Both Directions

IKE SA Life Time: 180 (secs)

Diffie-Hellman (DH) Group: Group 2 (1024 Bit)

IKE PFS PFS Key Group: Group 2 (1024 Bit)

IKE Keep Alive Ping IP Address: 0 0 0 0

< Back
Next >
Cancel

IKE Phase 1 (IKE SA)	
Local Identity	<p>This setting must match the "Remote Identity" on the remote VPN. Select the desired option, and enter the required data in the "Local Identity Data" field.</p> <ul style="list-style-type: none"> • WAN IP Address - This is the most common method. If selected, no input is required. • Fully Qualified Domain Name - enter the Domain Name assigned to this device. • Fully Qualified User name - This name does not have to a valid Internet Domain Name. E-mail addresses are often used for this entry. • DER ANS.1 DN - This must be a DER ANS.1 Domain Name.
Remote Identity	<p>This setting must match the "Local Identity" on the remote VPN. Select the desired option, and enter the required data in the "Remote Identity Data" field.</p> <ul style="list-style-type: none"> • IP Address - This is the most common method. If selected, no input is required. • Fully Qualified Domain Name - enter the Domain Name assigned to this device. • Fully Qualified User name - This name does not have to a valid Internet Domain Name. E-mail addresses are often used for this entry. • DER ANS.1 DN - This must be a DER ANS.1 Domain Name.
Authentication	<ul style="list-style-type: none"> • RSA Signature requires that both VPN endpoints have valid Certificates issued by a CA (Certification Authority). • For Pre-shared key, 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.
Authentication Algorithm	Select the desired option, and ensure that both endpoints have the same settings.
Encryption Algorithm	<p>Select the desired method, and ensure the remote VPN endpoint uses the same method.</p> <ul style="list-style-type: none"> • The 3DES algorithm provides greater security than DES, but is slower. • If using AES, you must select the Key Size. If using DES or 3DES, this field is ignored.
IKE Exchange Mode	<p>Select the desired option, and ensure the remote VPN endpoint uses the same mode.</p> <ul style="list-style-type: none"> • 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.

Direction	Select the desired option: <ul style="list-style-type: none"> • Initiator - Only outgoing connections will be created. Incoming connection attempts will be rejected. • Responder - Only incoming connections will be accepted. Outgoing traffic which would otherwise result in a connection will be ignored. • Both Directions - Both incoming and outgoing connections are allowed.
IKE SA Life Time	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.
DH Group	Select the desired method, and ensure the remote VPN endpoint uses the same method. The smaller bit size is slightly faster.
IKE PFS	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.
IKE Keep Alive	Use Ping to maintain VPN connection. The value is used to set the LAN IP address of other VPN side's device.

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

IKE Phase 2

This screen sets the parameters for the IPsec SA. When using IKE, there are separate connections (SAs) for IKE and IPsec.

VPN Wizard - IKE Phase 2 (IPSec SA)

These settings must match the remote VPN Endpoint.

IPsec SA Life Time: (secs)

IPsec PFS
Key Group:

AH Authentication
Algorithm:

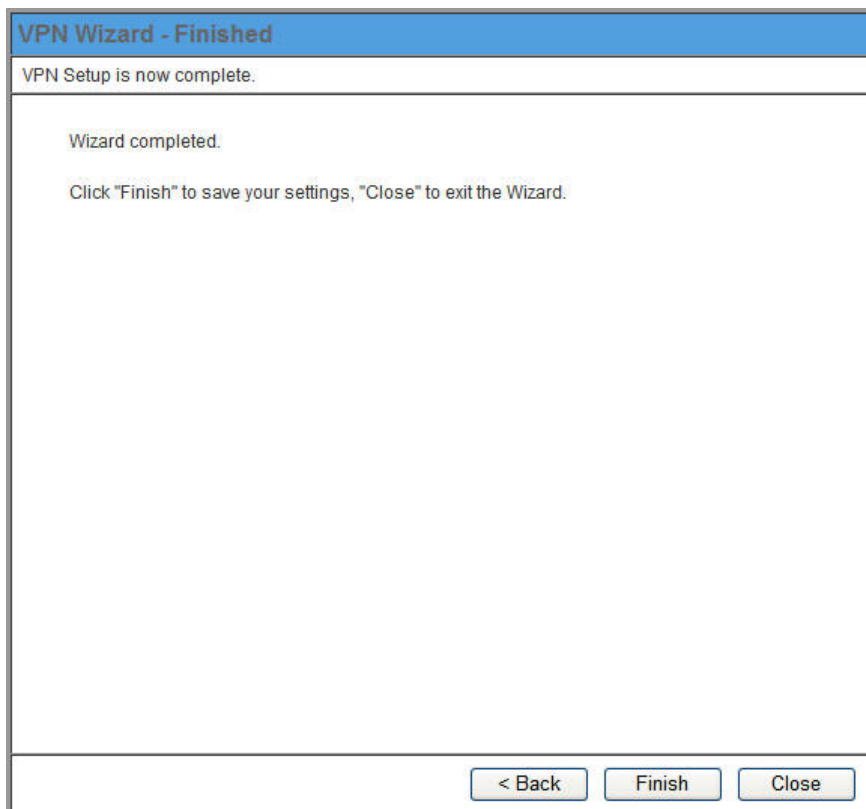
ESP Encryption
Algorithm:
Key Size: (AES only)

ESP Authentication
Algorithm:

< Back Next > Cancel

IKE Phase 2 (IPSec SA)	
IPSec SA Life Time	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.
IPSec PFS	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.
AH Authentication	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.
ESP Encryption	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 desired method and ensure remote VPN endpoint uses the same method. <ul style="list-style-type: none"> • The 3DES algorithm provides greater security than DES, but is slower. • The Key Size is available for AES only.
ESP Authentication	Generally, you should enable ESP Authentication. There is little difference between the available algorithms. Just ensure each endpoint with 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.

6.3 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 either the **Trusted Certificates** - the certificates of each CA itself - or **Self Certificates** - the certificates issued to you.

Use the radio button in the **Type** section of the screen to choose which type of Certificate you wish to view.

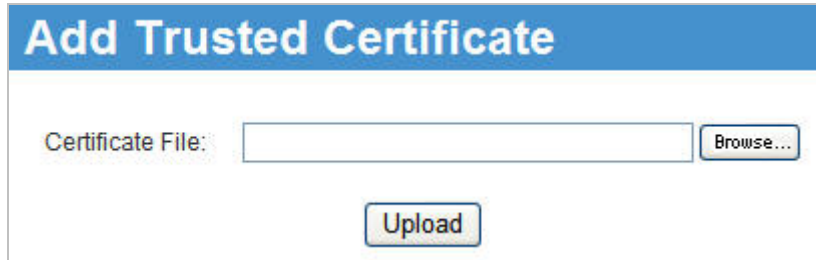
Trusted Certificates

The screenshot shows a web interface for managing certificates. At the top, the word "Certificates" is displayed in blue. Below it, there is a "Type" section with a "Select:" label and two radio buttons: "Trusted Certificates" (which is selected) and "Self Certificates". Underneath, there is a table with the heading "Trusted Certificates". The table has four columns: "Subject Name (CA)", "Issuer Name", "Expiry Time", and "Delete". Below the table, there is a button labeled "Add Trusted Certificate".

Trusted Certificates	
Subject Name (CA)	The "Subject Name" is always the company or person to whom the Certificate is issued. For trusted certificates, this will be a CA.
Issuer Name	The CA (Certification Authority) which issued the Certificate.
Expiry Time	The date on which the Certificate expires. You should renew the Certificate before it expires.
Delete button	Use this button to delete a Trusted Certificate. Select the checkbox in the Delete column for any Certificates you wish to delete, and then click the "Delete" button.
Add Trusted Certificate button	Use this to add a new Trusted Certificate to the table. See below for details.

Requesting a Trusted Certificate

1. After obtaining a new Certificate from the CA, you need to upload it to the IP-2000VPN.
2. On the "Certificates" screen, click the "Add Trusted Certificate" button to view the **Add Trusted Certificate** screen, shown below.

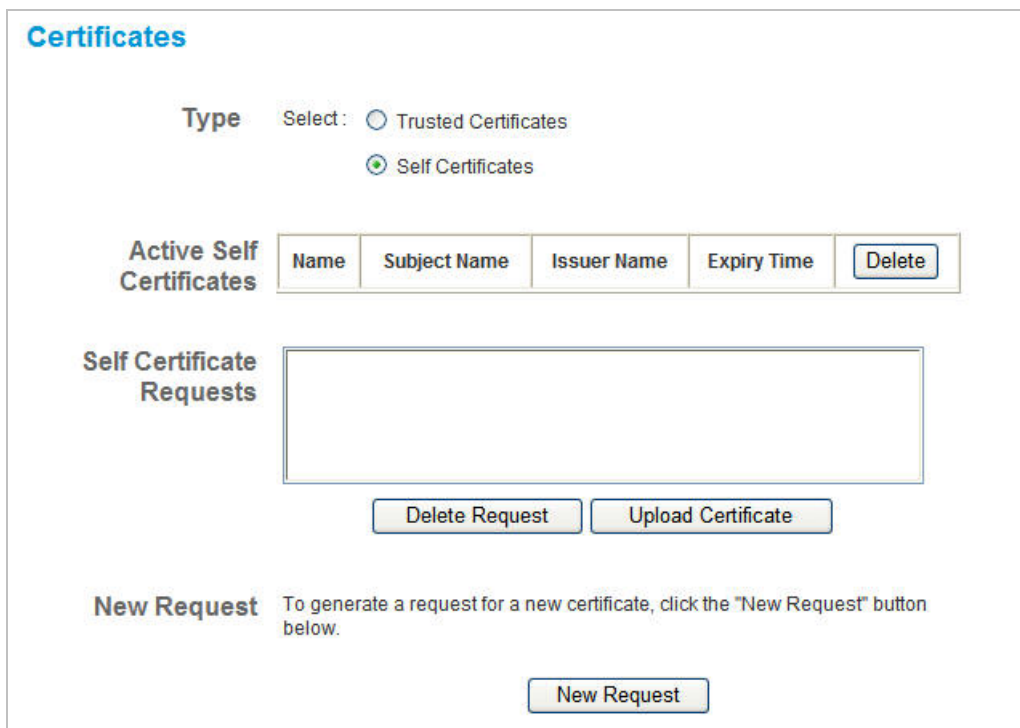


Add Trusted Certificate

Certificate File:

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 IP-2000VPN.
6. Click "Back" to return to the Trusted Certificate list. The new Certificate will appear in the list.

Self Certificates



Certificates

Type Select: Trusted Certificates
 Self Certificates

Active Self Certificates	Name	Subject Name	Issuer Name	Expiry Time	Delete
--------------------------	------	--------------	-------------	-------------	--------

Self Certificate Requests

New Request To generate a request for a new certificate, click the "New Request" button below.

Active Self Certificates	
Name	The name you assigned to this Certificate. You should select a name which helps to identify this particular certificate.
Subject Name	The company or person to whom the Certificate is issued.
Issuer Name	The CA (Certification Authority) which issued the Certificate.
Expiry Time	The date on which the Certificate expires. You should renew the Certificate before it expires.
Delete button	Use this button to delete a Self Certificate. Select the checkbox in the Delete column for any Certificates you wish to delete, and then click the "Delete" button.
Self Certificate Requests	
Request List	Any current requests are listed. These requests are generated by using the New Request button described below. <ul style="list-style-type: none"> After you have received the Certificate file for a request, you must select the request in the list, and upload the certificate file. The request will then be deleted from this list, and the Certificate will appear in the Active Self Certificates table. If for some reason you never obtain the Certificate, you can manually delete the request by using the Delete Request button.
Delete Request Button	Use this to delete the selected certificate request.
Upload Certificate	After you have received a Certificate, use this to upload the certificate to the IP-2000VPN. You must select the correct certificate request, so the IP-2000VPN can correctly match the request and the certificate.
New Request Button	Use this to generate a new request to be supplied to a CA (Certification Authority). See the following section for details.

Requesting a Self Certificate

The IP-2000VPN must generate a request for the CA. This request must then be supplied to the CA. The procedure is as follows:

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

Self Certificate Request (1)

Name:

Subject:

Hash Algorithm: ▼

Signature Algorithm: ▼

Signature Key Length: ▼

IP Address:

Domain Name: (Optional)

E-mail Address: (Optional)

2. Complete this screen.

Name	Enter a name which helps to identify this particular certificate. This name is only for your reference, it is not visible to other people.
Subject Name	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.
Hash Algorithm	Select the desired option.
Signature Algorithm	Select the desired option. RSA is recommended.
Signature Key Length	Select the desired option. Normally, 1024 bits provides adequate security.
IP address	Enter your public (Internet) IP address.
Domain Name	This is optional. If you have a domain name, enter it here.
E-mail Address	This is optional. If you have permanent E-mail address, enter it here.

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

Self Certificate Request (2)

Certificate Details

Subject Name:	Test
Hash Algorithm:	MD5
Signature Algorithm:	RSA
Key Length:	512

Data to supply to CA

```
-----BEGIN CERTIFICATE REQUEST-----  
MIHZMIGEAgECMA4xDDAKBgNVBAMTA0ROUzBcMA0GCSqGSIb3DQEBAQUAA0sAMEgC  
QQDgxBxyCPE58jKk9XA8bwCmLvjiASoMyGVavKgkudEikGxD9108LZGv4xNg147b  
NLLAVEKUD3UfR2QHciNNpqVrAgMBAAGgETAPBgkqhkiG9w0BCQ4xAjAAMA0GCSqG  
SIb3DQEBAUAA0EAchVyfoRtyjws9he+LFCLXNULycz11Kvk1gXpnnBC7w+mZksX  
M+10egaR7J4X7KTFXi/pSh3zc2Hf1Bzf+Xl6mg==  
-----END CERTIFICATE REQUEST-----
```

Copy/Save this data as necessary, then click "Finish".

< Back Finish

4. 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.
5. If the data is correct, copy the text in the **Data to supply to CA** panel (including "-----BEGIN CERTIFICATE REQUEST-----" and "-----END CERTIFICATE REQUEST-----") to a new document in a text editor such as Notepad, and save the file.
6. Click **Finish** to return to the **Self Certificates** screen.
Your request will be listed under **Self Certificate Requests**.
7. Apply for a Certificate:
 - Connect to the CA's web site.
 - Start the Self Certificate request procedure.
 - When prompted for the request data, supply the data you copied and saved in step 5 above.
 - Submit the CA's form.
 - If there are no problems, the Certificate will then be issued.
8. After obtaining a new Certificate, as described above, you need to upload it the IP-2000VPN.
 - Return to the **Self Certificates** screen.
 - In the **Self Certificate Requests** list, select the request matching this certificate.
 - Click the **Upload Certificate** button, and you will see a screen like the one below.

Upload Self Certificate

Upload the Certificate obtained from a CA.

Certificate File:

9. 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 the **Upload** button to upload the certificate file to the IP-2000VPN.
- Click **Back** to return to the **Self Certificates** screen. The new Certificate will appear in the **Active Self Certificates** list



1. For the Certificate example file please refer to Chapter 7.4.

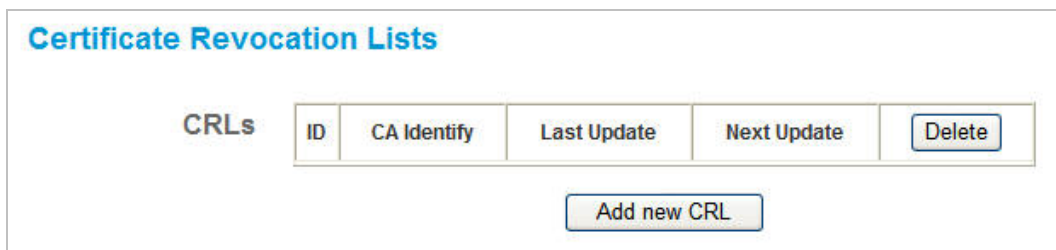
2. IP-2000VPN Certificate function is not compatible with Cisco router.

6.4 CLRs

- 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 its 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 CLR

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



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



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 IP-2000VPN.
 - 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.

6.5 Status

This screen lists all VPN SAs (Security Association) which exist at the current time.

- If no VPN tunnels exist at the current time, the table will be empty.
- To update the display, click the "Refresh" button.
- If using IKE, there is one SA for the IKE connection, and another SA for the IPSec connection.
- For each VPN SA the following data is displayed.



Data – VPN Status Screen

VPN Status	
SPI	Each SA (Security Association) has a unique SPI. For manual keys, this SPI is specified by user input. If using IKE, the SPI is generated by the IKE negotiation process.
SA Type	Each SAs (Security Association) will be either IKE or IPSec.
Policy Name	The name of the VPN Policy which triggered this VPN connection.
VPN Endpoint	The IP address of the remote VPN Endpoint.
Data Tx	Measures the quantity of data which has been sent (Transmitted) via this SA.
Data Rx	Measures the quantity of data which has been received via this SA.
Buttons	
Refresh	Update the data shown on screen.
View Log	Open a new window and view the contents of the VPN log.

Chapter 7 Microsoft VPN (PPTP)

Overview

Microsoft VPN uses the **Microsoft VPN Adapter** which is provided in recent versions of Windows. This feature can be used to provide remote access to your LAN by individual PCs. This method provides an alternative to using IPsec VPN, which is described in the previous chapter. Using Microsoft VPN provides easier setup than using IPsec VPN.

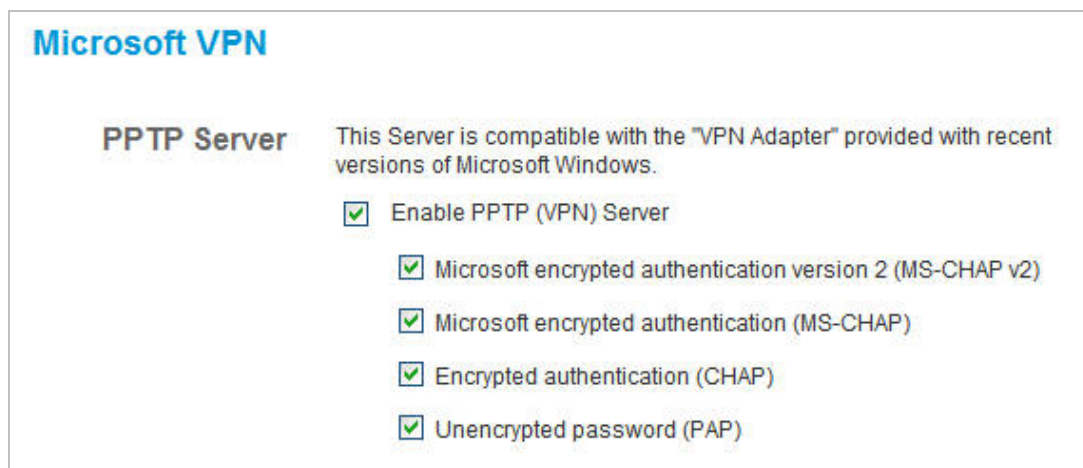
The following Microsoft VPN configuration screens are provided:

- Server
- Clients
- Status

7.1 PPTP Server

The IP-2000VPN incorporates a PPTP (Peer-to-Peer Tunneling Protocol) server which is compatible with the "VPN Adapter" provided with recent versions of Microsoft Windows. Remote Windows clients are able to connect to this Server. Once connected, they can access the LAN as if they connected locally.

The **Server** setup screen is accessed by selecting the *Server* option on the **Microsoft VPN** menu.



Data – Microsoft VPN Screen

PPTP Server	
Enable	Use this checkbox to enable or disable this feature as required. To allow connection by remote Windows clients, you must enable this feature, and enter the client details (on the Clients screen) to allow them to login to this Server.
Authentication Methods	Enable the desired authentication methods. The methods are listed with the most secure first, least secure last. If multiple methods are checked, the most secure will be tried first. If the remote client does not support this, then the other checked methods are tried in order. You must enable at least one method.

Client Database

To login to the PPTP Server (above) using the Microsoft Windows VPN Adapter, remote users must be entered in the VPN client database.

The **Client** setup screen is accessed by selecting the **Client** option on the **Microsoft VPN** menu.

Microsoft VPN Client Database

Existing Users

Delete

Properties

Allow connection

Login Name:

Login Password:

Verify Password:

Clear Form

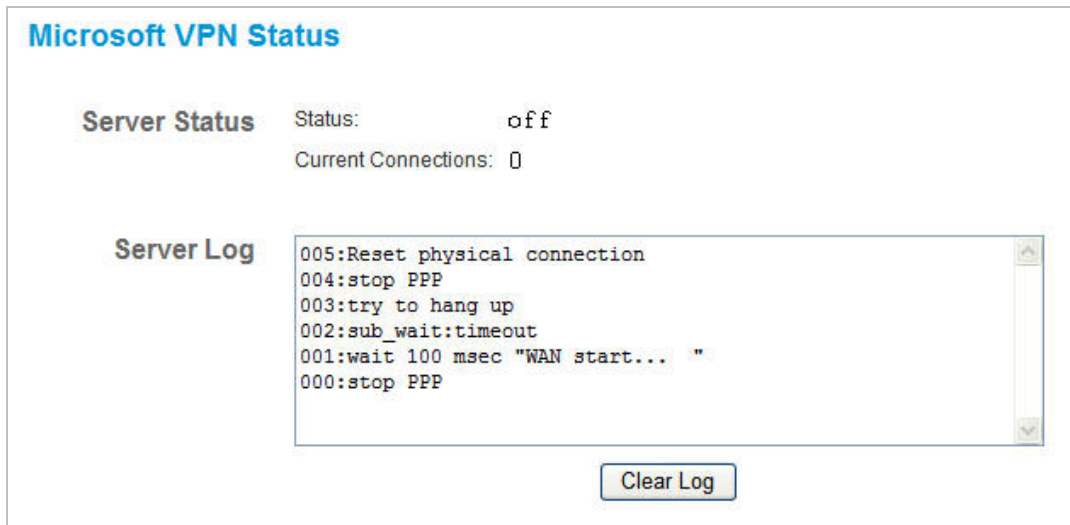
Add as New User Update Selected User

Data – Microsoft VPN Client Database Screen

Existing Users	
User List	All existing users are listed. If you have not added any users, this list will be empty. When a user is selected, their details are displayed in the Properties panel. You can then edit the user's information as required; click Update Selected User to save your changes. (If you select another user before saving your changes, your changes are lost.)
Delete Button	Use this to delete the selected user if required.
Properties	
Allow connection	Use this to enable or disable access by this user, as required.
Login Name	Enter the login name. The remote user must provide this name when they connect. The name must not contain spaces, punctuation, or special characters.
Login Password	Enter the login password. The remote user must provide this password when they connect.
Verify Password	Re-enter the password above.
Button	
Clear Form	Use this to prepare the form for a new entry. Any existing data will be cleared.
Add as New User	Use this to save the data in the "Properties" area as a new entry. (If a user is selected in the "Existing User" list, the selection is ignored.)
Update Selected User	Use this to update the data for the user selected in the Existing User list. To change an existing user's data, follow this procedure. <ol style="list-style-type: none"> 1. Select the desired user in the Existing Users list. Their information will be displayed in the Properties panel. 2. Change the data in the Properties panel as required. 3. Click the Update Selected User button to save your changes.

Status Screen

The **Status** screen is accessed by selecting the **Status** option on the **Microsoft VPN** menu.



Data – Microsoft VPN Status Screen

Server Status	
Status	This indicates whether or not the PPTP (VPN) Server is enabled.
Current Connections	This indicates the number of remote clients currently logged into the PPTP (VPN) Server.
Server Log	
Server Log	This displays details of each connection or connection attempt. You can use the Clear Log button to re-start the log, making new messages easier to read.

7.2 Windows PPTP Clients Setup

To connect to the PPTP (VPN) Server in the IP-2000VPN:

- The Microsoft VPN feature in the IP-2000VPN must be enabled and configured, as described in the previous section.
- Each user must have a login (username and password) on the VPN client database on the IP-2000VPN.
- The remote client PC must be configured as described in the following sections.
- It is assumed that remote users have a Broadband (not dial-up) connection to the Internet.

Windows 98/ME

1. Click Start - Settings - Dial-up Networking.
2. Select **Make New Connection**.



3. Type a name for this connection, and ensure that "Microsoft VPN Adapter" is selected. Click "Next" to continue.



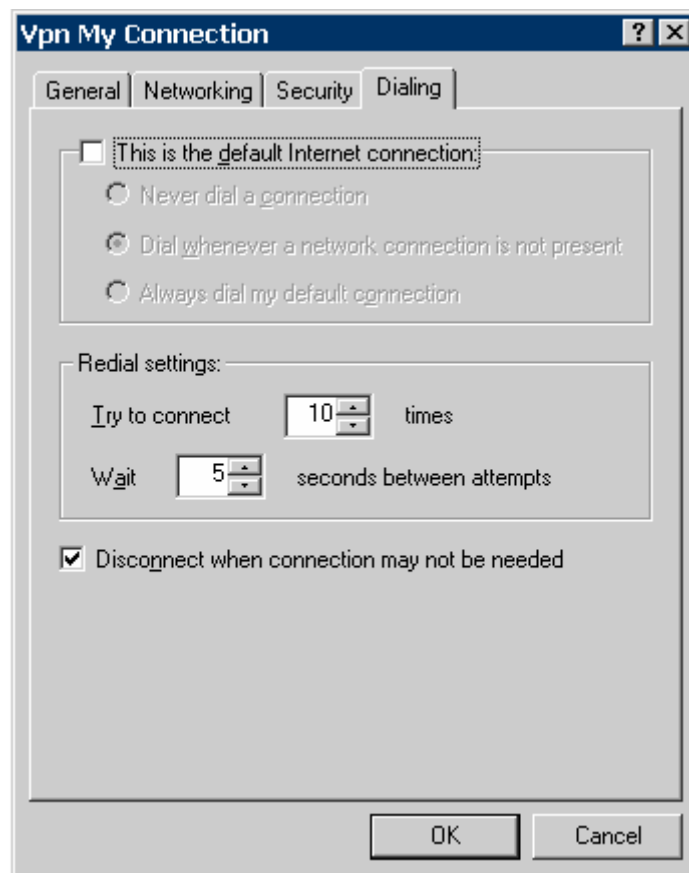
4. Enter the Internet IP address or domain name of this device. (If you don't have a fixed IP address, you can use a Dynamic DNS service to obtain a domain name).

Click "Next" to continue.

5. Click "Finish" to exit the Wizard.

The new entry will now be listed in "Dial-up Networking".

If necessary, you can change the settings for this connection by right-clicking on it, and selecting **Properties**. To force all outgoing traffic to be sent via VPN, enable the setting "***This is the default Internet connection***" on the **Dialing** tab. (Do NOT enable this setting if using Dial-up or PPPoE client software.)



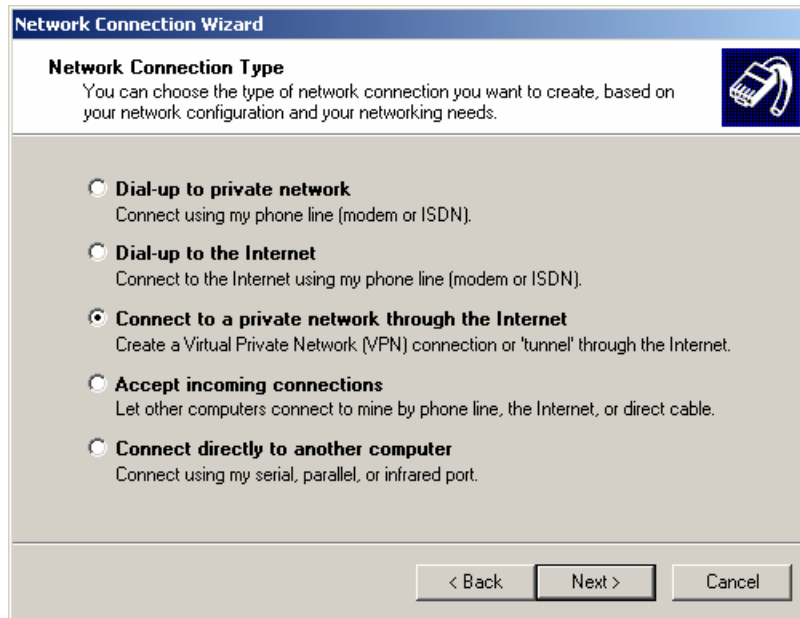
To establish a connection:

1. Ensure you are connected to the Internet.
2. Select **Start - Settings - Dial-up Networking**.
3. Double-click the new VPN entry in **Dial-up Networking**.
4. Enter your User name and Password, as recorded in the Client database on the IP-2000VPN.
5. Click the "Connect" button.

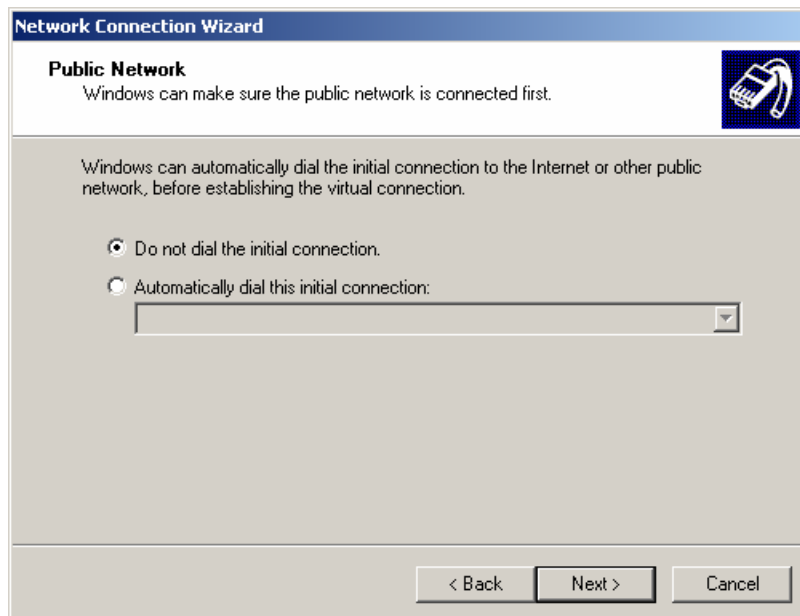
Windows 2000

Ensure you have logged on with Administrator rights before attempting this procedure.

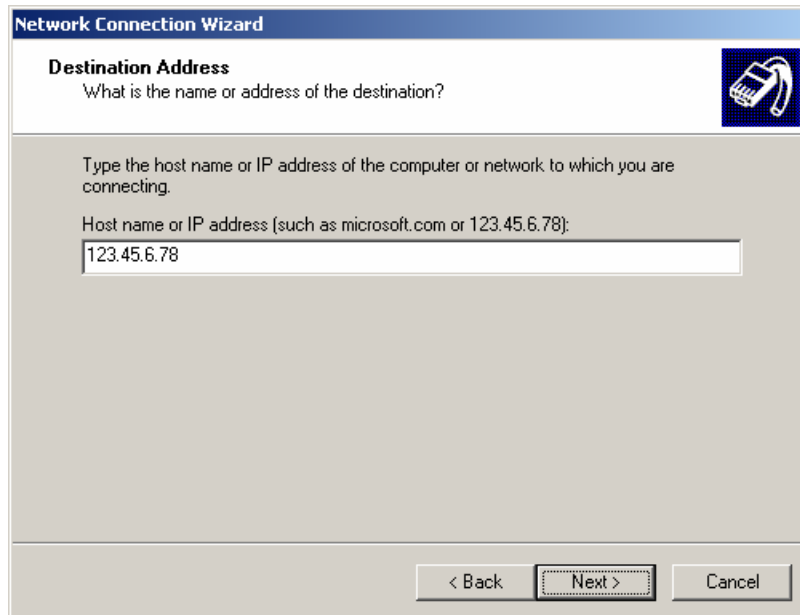
1. Open "Network Connections", and start the "New Connection" Wizard.



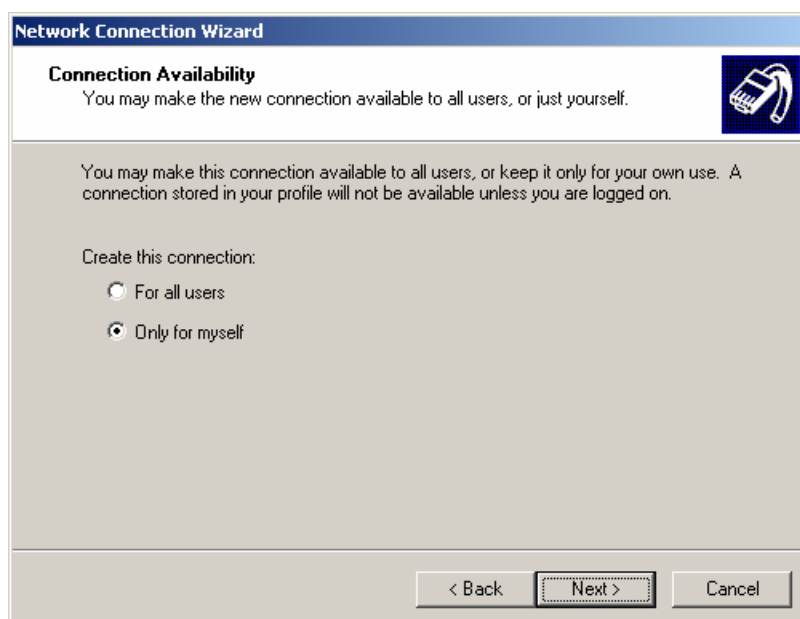
2. Select the VPN option ("Connect to a private network through the Internet"), as shown above, and click **Next**.



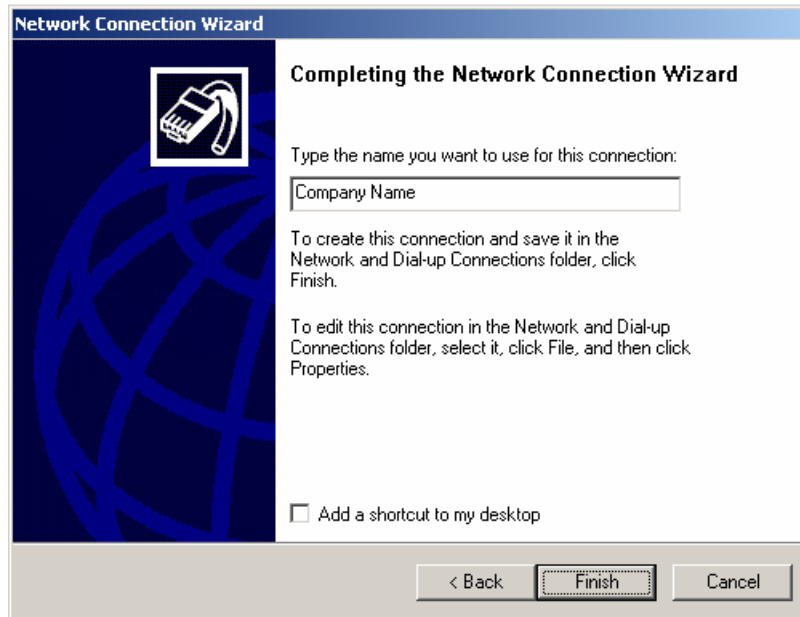
3. On the screen above:
 - Select "Do not dial the initial connection" if Internet access is via the LAN.
 - If using a PPPoE software client, select "Automatically dial this initial connection" and select the PPPoE connection.
 - Click **Next** to continue.



4. On the screen above, enter the Domain Name or Internet IP address of the IP-2000VPN you wish to connect to.
Click **Next** to continue.



5. Choose whether to allow this connection for everyone, or only for yourself, as required.
Click **Next** to continue.



6. Enter a suitable name, and click "Finish" to save and exit.
7. Setup is now complete.

To establish a connection:

1. Right-click the connection in "Network Connections", and select "Connect".
2. You will then be prompted for the username and password. Enter the username and password assigned to you, as recorded in the VPN client database on the IP-2000VPN.
3. You can choose to have Windows remember the password if desired, so you do not have to enter it again.

Changing the connection settings

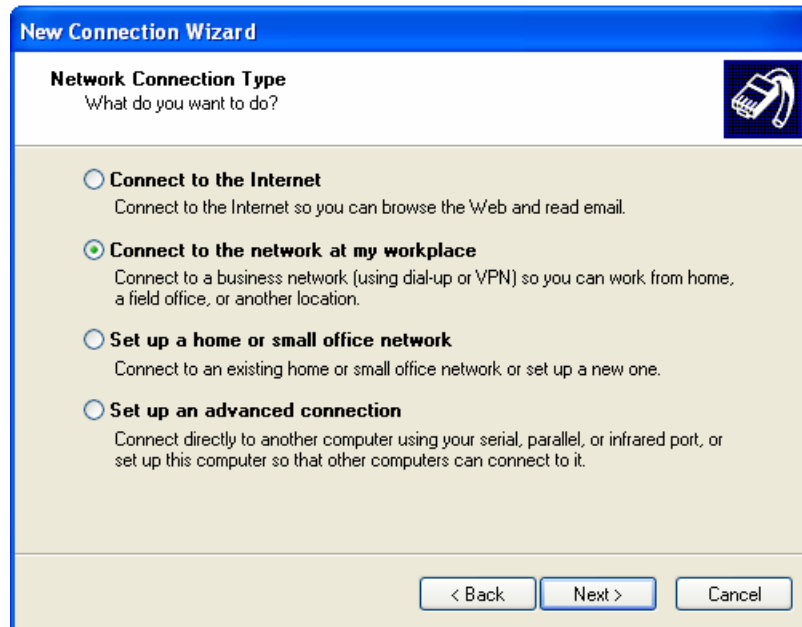
The PPTP (VPN) Server in the IP-2000VPN is designed to work with the default Windows settings.

- If necessary, you can change the Windows settings by right-clicking the VPN connection in **Network Connections**, and selecting **Properties**.
- The **Properties** dialog has a **Networking** tab with a "Type of VPN" setting. If you have trouble connecting, you can change this setting from "Automatic" to "PPTP VPN"

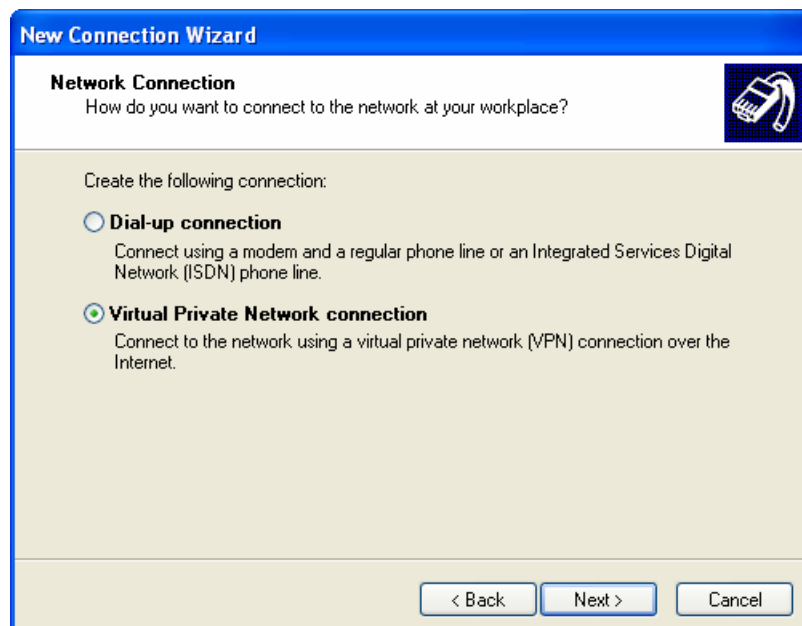
Windows XP

Ensure you have logged on with Administrator rights before attempting this procedure.

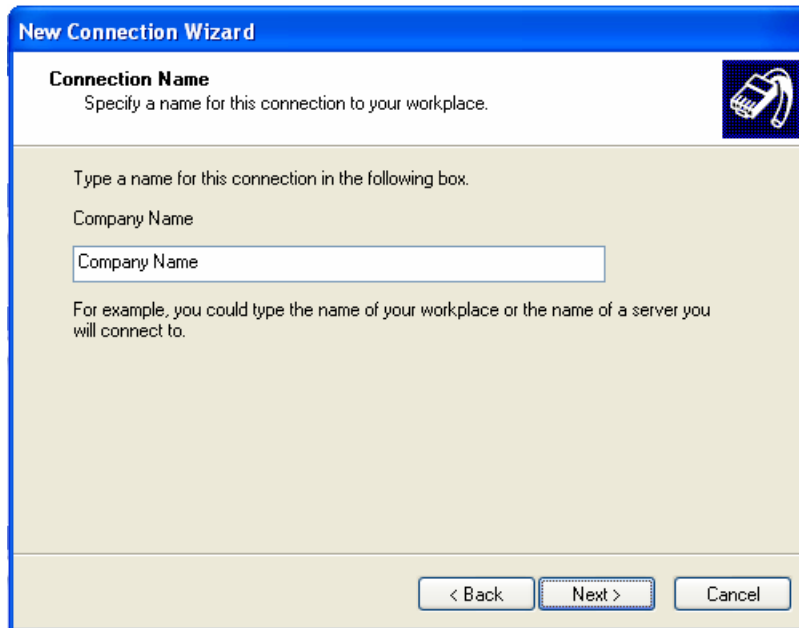
1. Open **Network Connections** (Start-Settings-Network Connections), and start the New Connection Wizard.



2. Select the option "Connect to the network at my workplace", as shown above, and click **Next**.

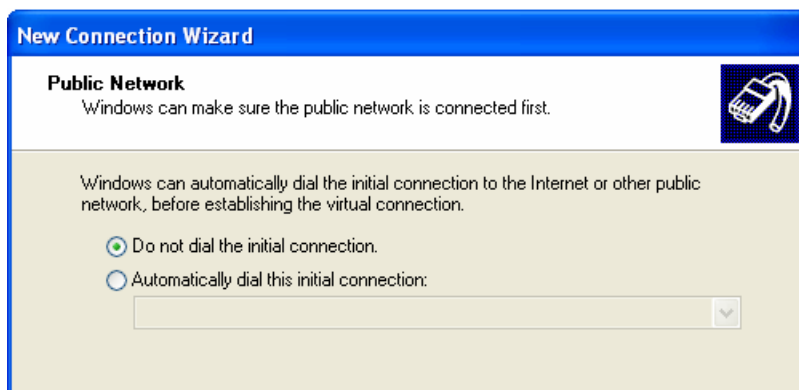


3. On the next screen, shown above, select the "Virtual Private Network connection" option.
Click **Next** to continue.



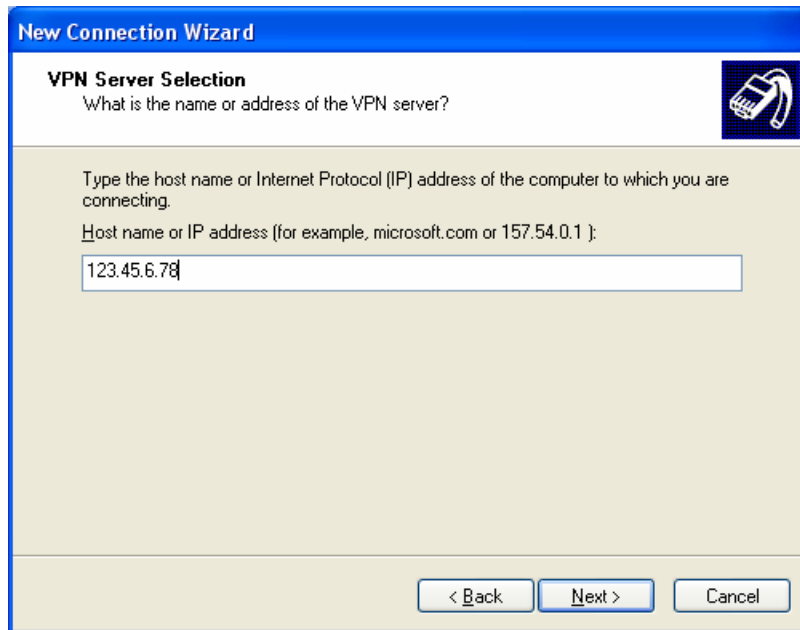
The screenshot shows a Windows dialog box titled "New Connection Wizard". The main heading is "Connection Name" with the instruction "Specify a name for this connection to your workplace." Below this, it says "Type a name for this connection in the following box." There is a text input field labeled "Company Name" containing the text "Company Name". A note below the field reads: "For example, you could type the name of your workplace or the name of a server you will connect to." At the bottom right, there are three buttons: "< Back", "Next >", and "Cancel".

4. Enter a suitable name for this connection.
Click **Next** to continue.

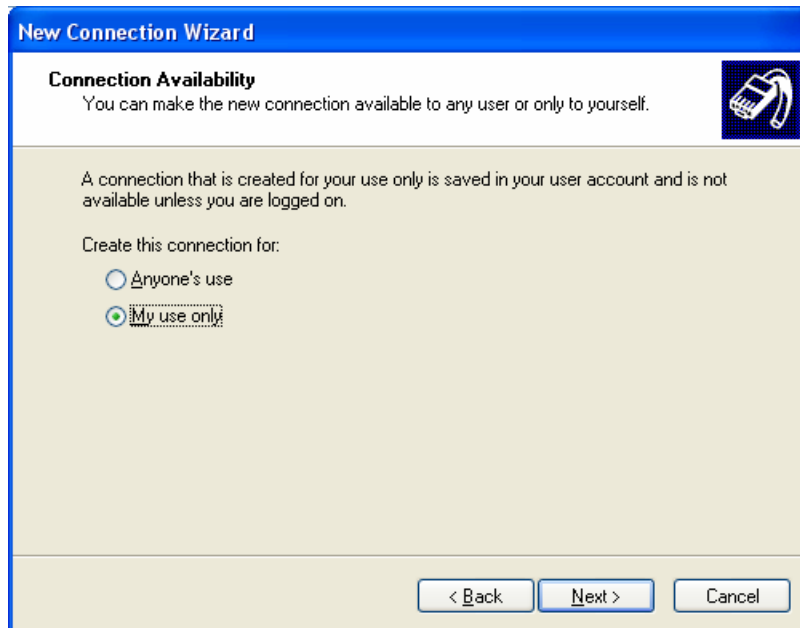


The screenshot shows the next step in the "New Connection Wizard" dialog box, titled "Public Network". The instruction is "Windows can make sure the public network is connected first." Below this, it says "Windows can automatically dial the initial connection to the Internet or other public network, before establishing the virtual connection." There are two radio button options: "Do not dial the initial connection." (which is selected) and "Automatically dial this initial connection:". Below the second option is a dropdown menu.

- On the screen above, select "Do not dial the initial connection".
Click **Next** to continue.



- On the screen above, enter the Domain Name or Internet IP address of the IP-2000VPN you wish to connect to.
Click **Next** to continue.



7. Choose whether to allow this connection for everyone, or only for yourself, as required.
Click **Next** to continue.
8. On the final screen, click Finish to save and exit.
9. Setup is now complete.

To establish a connection:

1. Right-click the connection in "Network Connections", and select "Connect".
2. You will then be prompted for the username and password. Enter the username and password assigned to you, as recorded in the VPN client database on the IP-2000VPN.
3. You can choose to have Windows remember the password if desired, so you do not have to enter it again.

Changing the connection settings

The PPTP (VPN) Server in the IP-2000VPN is designed to work with the default Windows settings.

- If necessary, you can change the Windows settings by right-clicking the VPN connection in **Network Connections**, and selecting **Properties**.
- The **Properties** dialog has a **Networking** tab with a "Type of VPN" setting. If you have trouble connecting, you can change this setting from "Automatic" to "PPTP VPN"

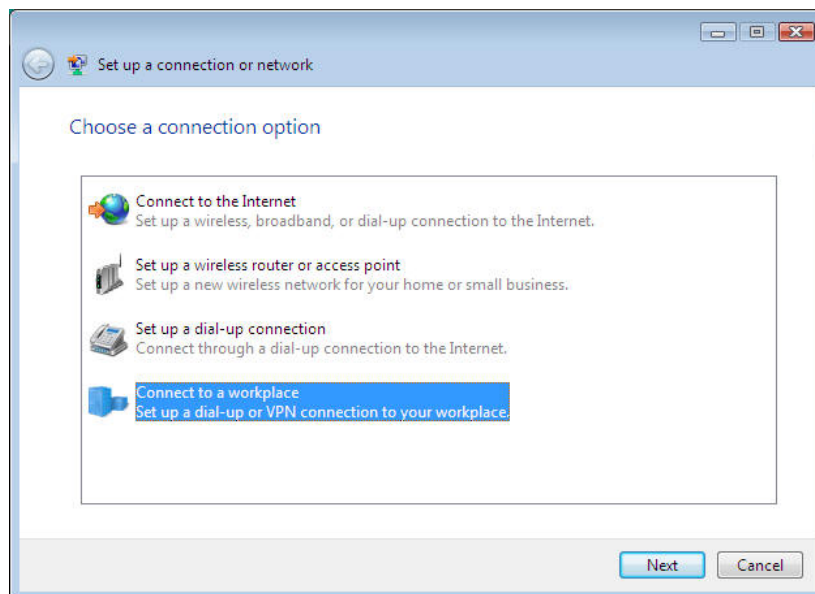
Windows Vista

Ensure you have logged on with Administrator rights before attempting this procedure.

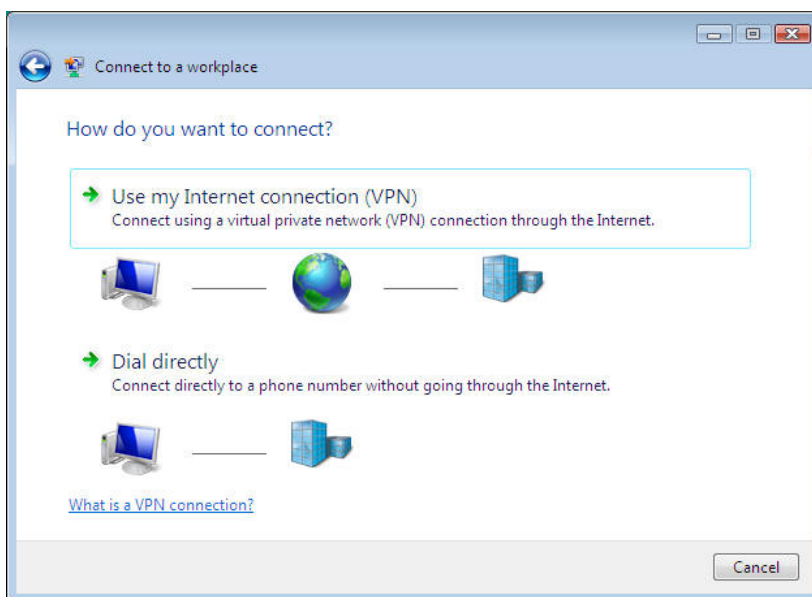
1. Select **Control Panel** → **Network and Sharing Center**, click **“Set up a connection or network”**.



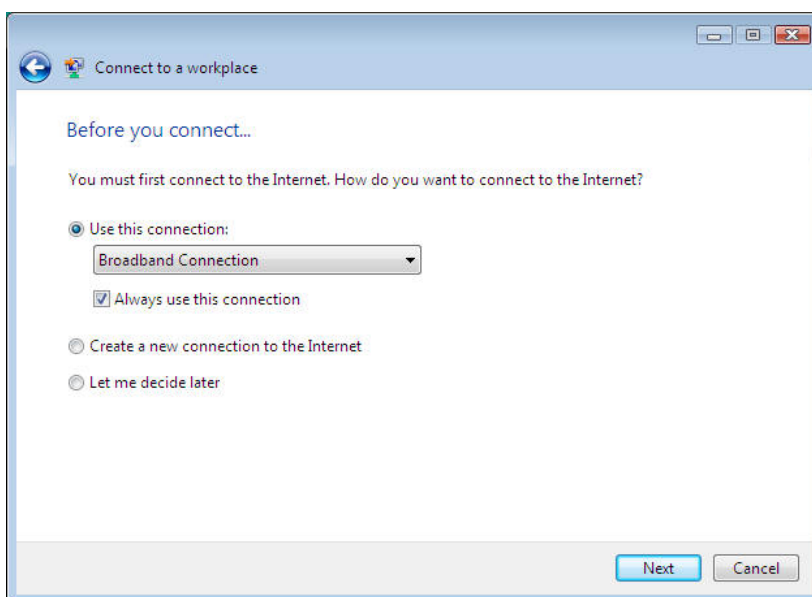
2. Select **“Connect to a workplace”**, and press **“Next”**.



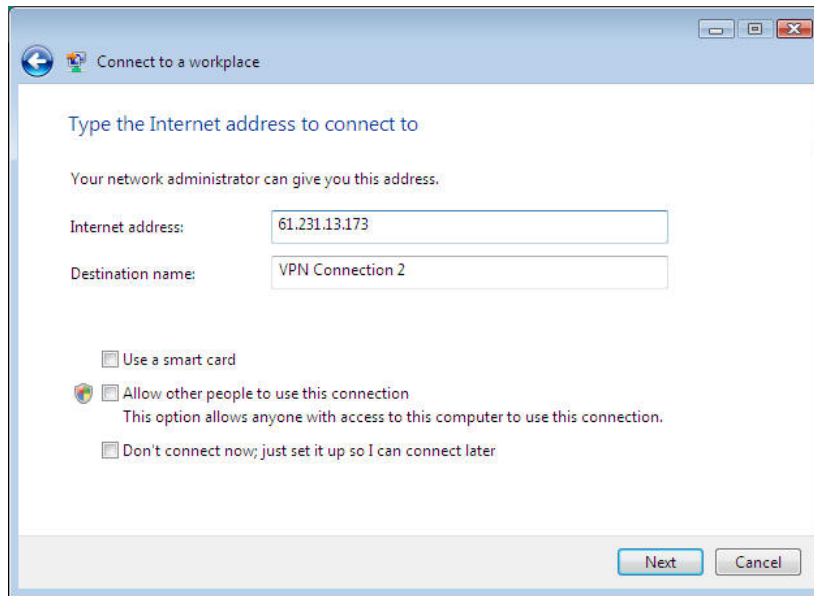
3. On the next screen, select and press **“Use my Internet connection (VPN)”**.



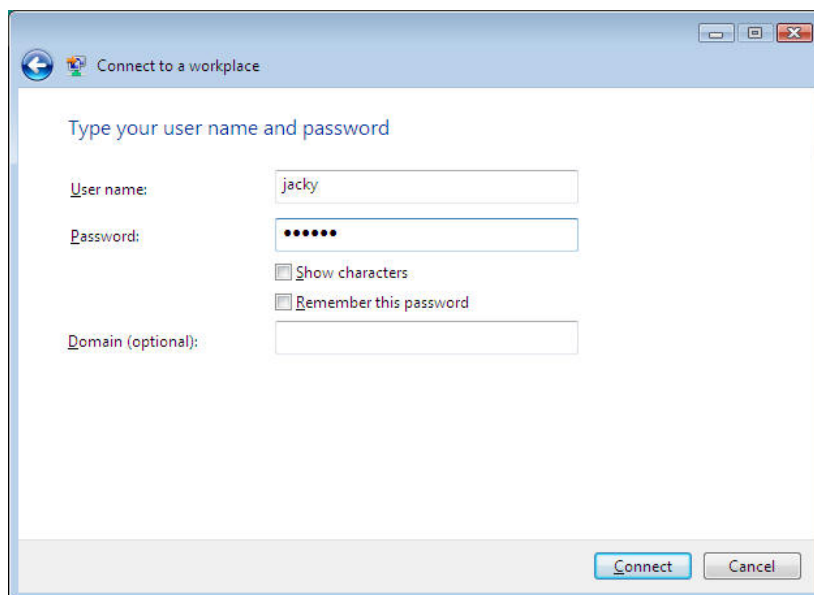
4. If PC was configured to dial up ISP with PPPoE or else, system will ask user to verify the connection which Internet connection will be used to connect. Select the specific one and press **“Next”**.



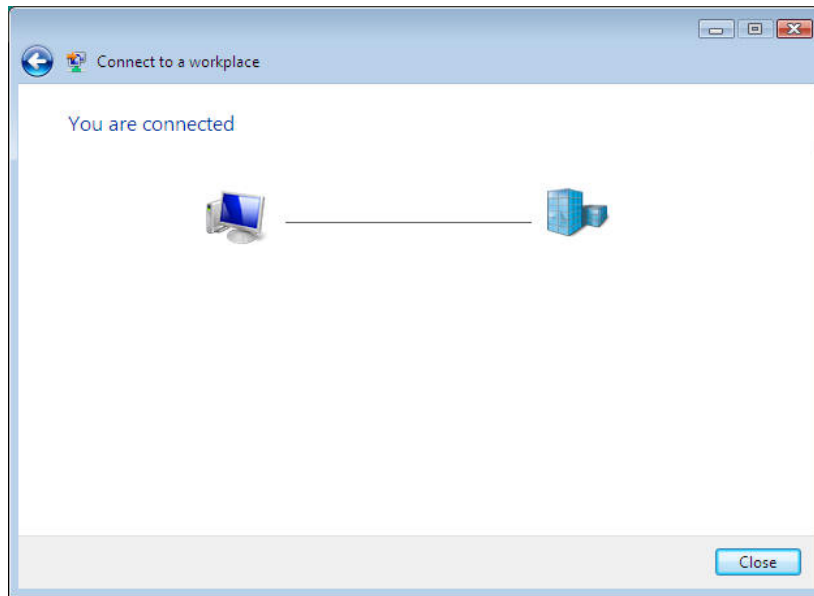
5. User should fill in the PPTP server IP address in the screen “**Type the Internet address to connect to**”.



6. Type in the user name and password of PPTP client, and then press “**Connect**” to connect with PPTP server.



7. If PPTP client connect successfully to PPTP server, user can see the following screen.



8. Ping the IP-2000VPN LAN IP address (192.168.1.1) and the IP address (192.168.1.2) of PC connected to IP-2000VPN, to verify the PPTP connection. The result is fine.

```
Microsoft Windows [Version 6.0.6000]
Copyright (c) 2006 Microsoft Corporation. All rights reserved.

C:\Users\test4>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time=104ms TTL=64
Reply from 192.168.1.1: bytes=32 time=93ms TTL=64
Reply from 192.168.1.1: bytes=32 time=93ms TTL=64
Reply from 192.168.1.1: bytes=32 time=93ms TTL=64

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 93ms, Maximum = 104ms, Average = 95ms

C:\Users\test4>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time=104ms TTL=128
Reply from 192.168.1.2: bytes=32 time=93ms TTL=128
Reply from 192.168.1.2: bytes=32 time=93ms TTL=128
Reply from 192.168.1.2: bytes=32 time=93ms TTL=128

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 93ms, Maximum = 104ms, Average = 95ms

C:\Users\test4>
```

Chapter 8 VPN Example

This section describes some examples of using the IP-2000VPN in common VPN situations.

It is used to create IPSec VPN tunnel between two offices' sites, and encrypted the data for the access. When the VPN tunnel is created, each user in the office can access another office's data via VPN tunnel, so no more VPN must be created by individual user.

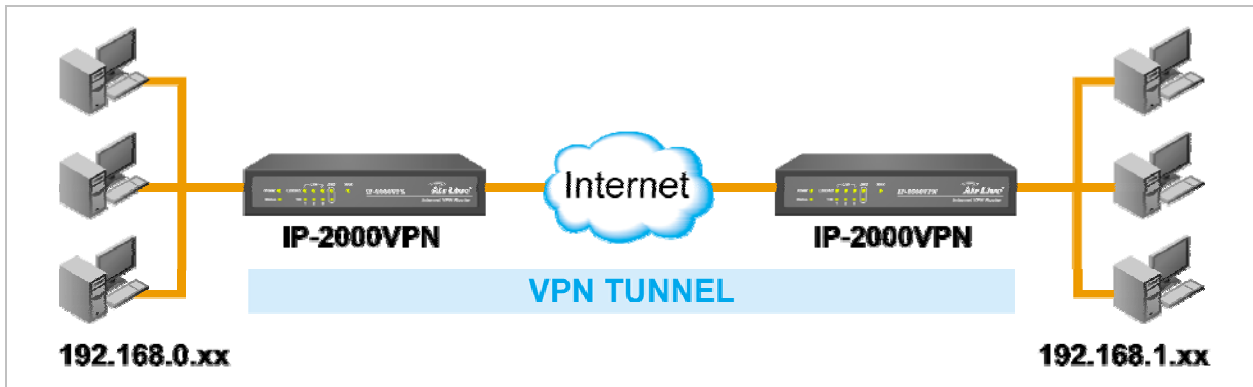
Meanwhile, user could also need to access office's data from home, so administrator must offer a secure method for those users. PPTP VPN is a simple and secure choice, and most home users select to work with it.

We offer several VPN examples for your reference, as the following the example, you will understand how to configure the device and make the VPN tunnel working.

- Chapter 8.1 Office-to-office IPSec VPN - Connecting to 2 IP-2000VPN
- Chapter 8.2 Office-to-office IPSec VPN - Connecting to IP-2000VPN and RS-1200
- Chapter 8.3 Getting into Office Network from Internet (PPTP)
- Chapter 8.4 Getting into Office Network from Internet (IPSec)

8.1 Office-to-office IPsec VPN – Connecting to 2 IP-2000VPN

In this example, 2 IP-2000VPN will connect VPN with each other and gains access to the both LANs.



Environment:

	IPSec Site A	IPSec Site B
WAN IP address	60.250.158.64	203.10.66.89
LAN IP Subnet	192.168.1.x	192.168.0.x
Pre-shared Key	12345678	12345678
IKE Encryption	3DES	3DES
IKE Authentication	MD5	MD5
DH Group	Group 2	Group 2
ESP Encryption	3DES	3DES
ESP Authentication	MD5	MD5



The LANs MUST use different IP address ranges.

Step 1: IPsec VPN Site A – Network Configuration

Name: Enable Policy
 Allow NetBIOS traffic

Remote VPN endpoint
 Dynamic IP
 Fixed IP:
 Domain Name:

Local IP addresses
 Type: IP address: ~
 Subnet Mask:

Remote IP addresses
 Type: IP address: ~
 Subnet Mask:

Data – Network Configuration

Setting	Type	Value	Notes
Name		Policy_A	Name does not affect operation. Select a meaningful name.
Enable Policy	Enable		
Allow NetBIOS traffic	Enable		Enable to allow NetBIOS passing through VPN tunnel
Remote Endpoint	Fixed IP	203.10.66.89	Other endpoint's WAN (Internet) IP address.
Local IP addresses	Subnet Address	192.168.1.0 / 255.255.255.0	Use a more restrictive definition if possible.
Remote IP addresses	Subnet Address	192.168.0.0 / 255.255.255.0	Address range on other endpoint. Use a more restrictive definition if possible.

Step 2: IPSec VPN Site A – Authentication and Encryption

Authentication & Encryption

AH Authentication MD5

ESP Encryption 3DES Key Size: n/a (AES only)

ESP Authentication MD5

Manual Key Exchange

IKE (Internet Key Exchange)

Direction: Both Directions

Local Identity Type: WAN IP Address

Local Identity Data:

Remote Identity Type: Remote WAN IP

Remote Identity Data:

Authentication:

 RSA Signature (requires certificate)

 Pre-shared Key

Authentication Algorithm: MD5

Encryption: 3DES Key Size: n/a (AES only)

Exchange Mode: Main Mode

IKE SA Life Time: 180 (secs)

IKE Keep Alive Ping IP Address: 192.168.0.1

IPSec SA Life Time: 300 (secs)

DH Group: Group 2 (1024 Bit)

IKE PFS: Disabled

IPSec PFS: None

Data – Authentication and Encryption

Setting	Type	Value	Notes
IKE Direction	Both Directions		Do not have to match with Site B. Either endpoint can block 1 direction.
Local Identify	WAN IP Address		System will detect the IP address and fill in the form automatically. It is the most common ID method.
Remote Identify	Remote WAN IP Address		System will detect the IP address and fill in the form automatically. It is the most common ID method.
IKE Authentication method	Pre-shared Key	12345678	Certificates are not widely used.
IKE Authentication algorithm		MD5	Must match with Site B
IKE Encryption		3DES	Must match with Site B
IKE Exchange mode	Main Mode		Must match with Site B
DH Group	Group 2 (1024 Bit)		Must match with Site B
IKE SA Life time		180	Shorter period will be used.
IKE Keep Alive	Enable	192.168.0.1	Used to set the LAN IP address of IP-2000VPN at Site B.
IKE PFS	Disable		Must match with Site B
IPSec SA Parameters			
IPSec SA Life time		300	Shorter period will be used.
IPSec PFS	Disable		Must match with Site B
AH Authentication	Disable		AH is rarely used.
ESP Authentication	Enable	MD5	Must match with Site B
ESP Encryption	Enable	3DES	Must match with Site B

Step 3: IPSec VPN Site B – Network Configuration

Name: Enable Policy
 Allow NetBIOS traffic

Remote VPN endpoint
 Dynamic IP
 Fixed IP:
 Domain Name:

Local IP addresses
Type: IP address: ~
Subnet Mask:

Remote IP addresses
Type: IP address: ~
Subnet Mask:

Data – Network Configuration

Setting	Type	Value	Notes
Name		Policy_B	Name does not affect operation. Select a meaningful name.
Enable Policy	Enable		
Allow NetBIOS traffic	Enable		Enable to allow NetBIOS passing through VPN tunnel
Remote Endpoint	Fixed IP	60.250.158.64	Other endpoint's WAN (Internet) IP address.
Local IP addresses	Subnet Address	192.168.0.0 / 255.255.255.0	Use a more restrictive definition if possible.
Remote IP addresses	Subnet Address	192.168.1.0 / 255.255.255.0	Address range on other endpoint. Use a more restrictive definition if possible.

Step 4: IPSec VPN Site B – Authentication and Encryption

Authentication & Encryption

AH Authentication MD5

ESP Encryption 3DES Key Size: n/a (AES only)

ESP Authentication MD5

Manual Key Exchange

IKE (Internet Key Exchange)

Direction: Both Directions

Local Identity Type: WAN IP Address

Local Identity Data:

Remote Identity Type: Remote WAN IP

Remote Identity Data:

Authentication: RSA Signature (requires certificate)
 Pre-shared Key

Pre-shared Key:

Authentication Algorithm: MD5

Encryption: 3DES Key Size: n/a (AES only)

Exchange Mode: Main Mode

IKE SA Life Time: 180 (secs)

IKE Keep Alive Ping IP Address: 0.0.0.0

IPSec SA Life Time: 300 (secs)

DH Group: Group 2 (1024 Bit)

IKE PFS: Disabled

IPSec PFS: None

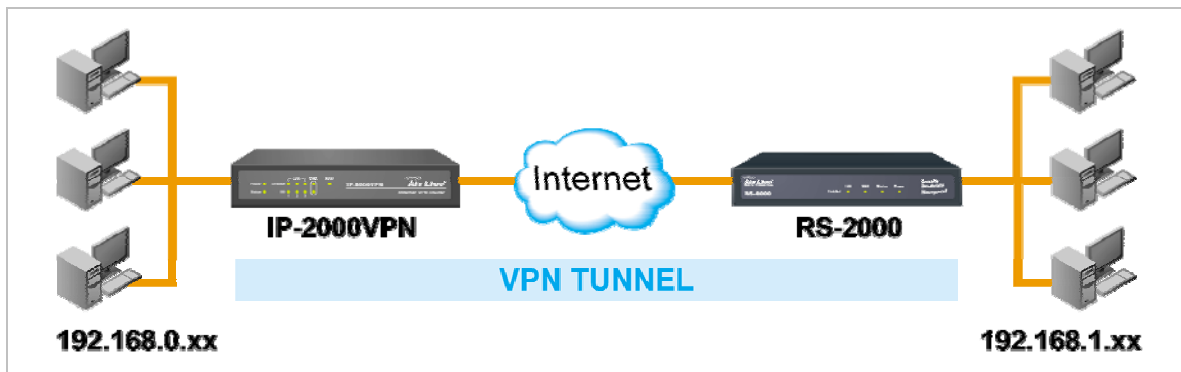
Data – Network Configuration

Setting	Type	Value	Notes
IKE Direction	Both Directions		Do not have to match with Site A. Either endpoint can block 1 direction.
Local Identify	WAN IP Address		System will detect the IP address and fill in the form automatically. It is the most common ID method.
Remote Identify	Remote WAN IP Address		System will detect the IP address and fill in the form automatically. It is the most common ID method.
IKE Authentication	Pre-shared Key	12345678	Certificates are not widely used.

method			
IKE Authentication algorithm		MD5	Must match with Site A
IKE Encryption		3DES	Must match with Site A
IKE Exchange mode	Main Mode		Must match with Site A
DH Group	Group 2 (1024 Bit)		Must match with Site A
IKE SA Life time		180	Shorter period will be used.
IKE Keep Alive	Enable	192.168.1.1	Used to set the LAN IP address of IP-2000VPN at Site A.
IKE PFS	Disable		Must match with Site A
IPSec SA Parameters			
IPSec SA Life time		300	Shorter period will be used.
IPSec PFS	Disable		Must match with Site A
AH Authentication	Disable		AH is rarely used.
ESP Authentication	Enable	MD5	Must match with Site A
ESP Encryption	Enable	3DES	Must match with Site A

8.2 Office-to-office IPsec VPN – Connecting IP-2000VPN and RS-1200

In this example, IP-2000VPN will connect VPN with RS-1200, and gains access to the both LAN.



Environment:

	IP-2000VPN	RS-1200
WAN IP address	Airlive98.dyndns.org	60.250.158.64
LAN IP Subnet	192.168.1.x	192.168.100.x
Pre-shared Key	12345678	12345678
IKE Encryption	3DES	3DES
IKE Authentication	MD5	MD5
DH Group	Group 2	Group 2
ESP Encryption	3DES	3DES
ESP Authentication	MD5	MD5

Step 1: IP-2000VPN – Network Configuration

Name:

Enable Policy
 Allow NetBIOS traffic

Remote VPN endpoint
 Dynamic IP
 Fixed IP:
 Domain Name:

Local IP addresses
Type: IP address: ~
Subnet Mask:

Remote IP addresses
Type: IP address: ~
Subnet Mask:

Setting	Type	Value	Notes
Name		To_RS12	Name does not affect operation. Select a meaningful name.
Enable Policy	Enable		
Allow NetBIOS traffic	Enable		Enable to allow NetBIOS passing through VPN tunnel
Remote Endpoint	Domain Name	airlive98.dyndns.org	The domain name resolved the other endpoint's WAN (Internet) IP address.
Local IP addresses	Subnet Address	192.168.1.0 / 255.255.255.0	Allows access to entire LAN. Use a more restrictive definition if possible.
Remote IP addresses	Subnet Address	192.168.100.0 / 255.255.255.0	Address range on other endpoint. Use a more restrictive definition if possible.

Step 2: IP-2000VPN –Authentication and Encryption

Authentication & Encryption

AH Authentication MD5

ESP Encryption 3DES Key Size: n/a (AES only)

ESP Authentication MD5

Manual Key Exchange

IKE (Internet Key Exchange)

Direction: Both Directions

Local Identity Type: WAN IP Address

Local Identity Data:

Remote Identity Type: Remote WAN IP

Remote Identity Data:

Authentication: RSA Signature (requires certificate)
 Pre-shared Key

Authentication Algorithm: MD5

Encryption: 3DES Key Size: n/a (AES only)

Exchange Mode: Main Mode

IKE SA Life Time: 180 (secs)

IKE Keep Alive Ping IP Address: 192.168.100.1

IPSec SA Life Time: 300 (secs)

DH Group: Group 2 (1024 Bit)

IKE PFS: Group 2 (1024 Bit)

IPSec PFS: Group 2 (1024 Bit)

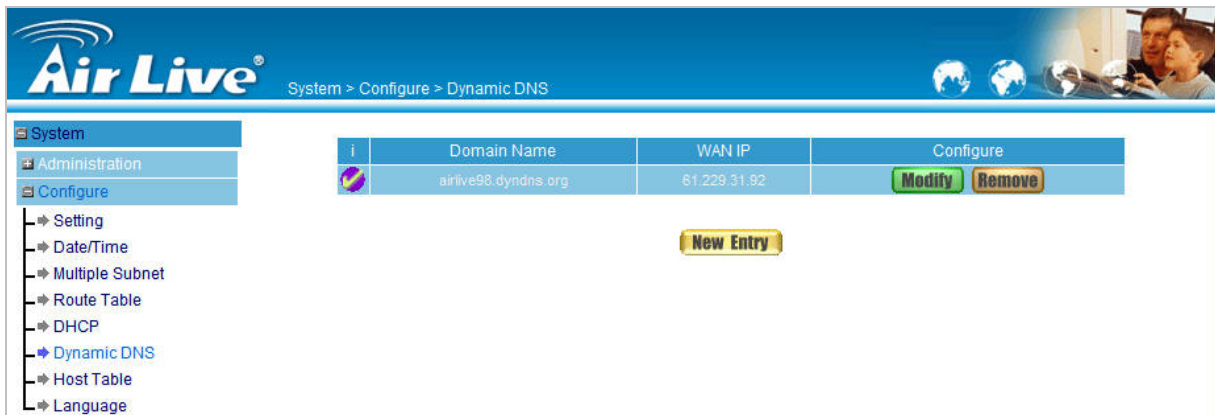
Setting	Type	Value	Notes
IKE Direction	Both Directions		Using "Responder only" is not possible.
Local Identify	WAN IP Address		System will detect the IP address and fill in the form automatically. It is the most common ID method.
Remote Identify	Remote WAN IP Address		System will detect the IP address and fill in the form automatically. It is the most common ID method.
IKE Authentication method	Pre-shared Key	12345678	Certificates are not widely used.
IKE Authentication algorithm		MD5	Must match with RS-1200.
IKE Encryption		3DES	Must match with RS-1200.
IKE Exchange mode	Main Mode		Must match with RS-1200.
DH Group	Group 2 (1024 bit)		Must match with RS-1200.
IKE SA Life time		180	Shorter period will be used.
IKE Keep Alive	Enable	192.168.100.1	Used to set the LAN IP address of RS-1200.
IKE PFS	Group 2 (1024 bit)		Must match with RS-1200.
IPSec SA Parameters			
IPSec SA Life time		300	Shorter period will be used.
IPSec PFS	Group 2 (1024 bit)		Must match with RS-1200.
AH Authentication	Disable		AH is rarely used.
ESP Authentication	Enable	MD5	Must match with RS-1200.
ESP Encryption	Enable	3DES	Must match with RS-1200.

Step 3: RS-1200 Network Configuration

1. Define WAN port IP with PPPoE, and obtain the IP address from ISP.



2. Configure DDNS service and fill in the necessary setting, in order to resolve the Dynamic Domain Name (ex. airlive98.dyndns.org) with current IP address.



Step 4: Configure RS-1200 IPSec Autokey

1. Select **IPSec Autokey** in **VPN**. Click **New Entry**.



2. In the list of **IPSec Autokey**, fill in Name with **To_IP2KVPN**.

Necessary Item	
Name	To_IP2KVPN (Max. 12 characters)
WAN interface	<input checked="" type="radio"/> WAN 1 <input type="radio"/> WAN 2

3. Select **Remote Gateway-Fixed IP or Domain Name** in **To Destination** list and enter the IP Address.

To Destination	
<input checked="" type="radio"/> Remote Gateway -- Fixed IP or Domain Name	60.250.158.64 (Max. 99 characters)
<input type="radio"/> Remote Gateway or Client -- Dynamic IP	

4. Select **Preshare** in **Authentication Method** and enter the **Preshared Key**.

Authentication Method	Preshare
Preshared Key	12345678 (Max. 103 characters)

5. Both sides have to choose the same group. Here we select 3DES for ENC Algorithm, MD5 for AUTH Algorithm and GROUP2 for Group.

Encapsulation	
ISAKMP Algorithm	
ENC Algorithm	3DES
AUTH Algorithm	MD5
Group	GROUP 2

6. Select Data Encryption + Authentication in **IPSec Algorithm** list. Here we select 3DES for ENC Algorithm and MD5 for AUTH Algorithm to make sure the encapsulation way for data transmission.

IPSec Algorithm	
<input checked="" type="radio"/> Data Encryption + Authentication	
ENC Algorithm	3DES
AUTH Algorithm	MD5
<input type="radio"/> Authentication Only	

7. After selecting GROUP2 in **Perfect Forward Secrecy**, enter 3600 seconds in **ISAKMP Lifetime**; enter 28800 seconds in **IPSec Lifetime**, and selecting Main mode in **Mode**.

Perfect Forward Secrecy	GROUP 2
ISAKMP Lifetime	3600 Seconds (Range: 1200 - 86400)
IPSec Lifetime	28800 Seconds (Range: 1200 - 86400)

8. Complete the IPSec Autokey setting.

i	Name	WAN	Gateway IP	IPSec Algorithm	Configure
—	To_IP2KVPN	WAN1	60.250.158.64	3DES / MD5	Modify Remove

Step 5: Configure RS-1200 IPSec Tunnel

Enter the following setting in **Tunnel** of **VPN** function:

- Enter a specific Tunnel **Name**.
- **From Source**: Select LAN.
- **From Source Subnet / Mask**: Enter 192.168.100.0 / 255.255.255.0.
- **To Destination**: Select To Destination Subnet / Mask.
- **To Destination Subnet / Mask**: Enter 192.168.1.0 / 255.255.255.0.
- **IPSec / PPTP Setting**: Select To_IP2KVPN
- Enter 192.168.1.1 (the Default Gateway IP of IP-2000VPN) as the **Keep alive IP**.
- Select **Show remote Network Neighborhood**.
- Click **OK**.

New Entry Tunnel	
Name	To_IP2K_Tunnel (Max. 16 characters)
From Source	<input checked="" type="radio"/> LAN <input type="radio"/> DMZ
From Source Subnet / Mask	192.168.100.0 / 255.255.255.0
To Destination	<input checked="" type="radio"/> To Destination Subnet / Mask <input type="radio"/> Remote Client
	192.168.1.0 / 255.255.255.0
IPSec / PPTP Setting	To_IP2KVPN
Keep alive IP	192.168.1.1
<input checked="" type="checkbox"/> Show remote Network Neighborhood	

Step 6: Configure RS-1200 Outgoing and Incoming Policy

1. Enter the following setting in **Outgoing Policy**.

- **Tunnel:** Select To_IP2K_Tunnel
- Click **OK**.

Add New Policy	
Source Address	Inside_Any ▾
Destination Address	Outside_Any ▾
Service	ANY ▾
Schedule	None ▾
Authentication User	None ▾
Tunnel	To_IP2K_Tunnel ▾
Action, WAN Port	PERMIT ALL ▾
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
Content Blocking	<input type="checkbox"/> Enable
IM / P2P Blocking	None ▾
QoS	None ▾
MAX. Bandwidth Per Source IP	Downstream <input type="text" value="0"/> Kbps Upstream <input type="text" value="0"/> Kbps (0: means unlimited)
MAX. Concurrent Sessions Per IP	<input type="text" value="0"/> (Range: 1 - 99999, 0: means unlimited)
MAX. Concurrent Sessions	<input type="text" value="0"/> (Range: 1 - 99999, 0: means unlimited)

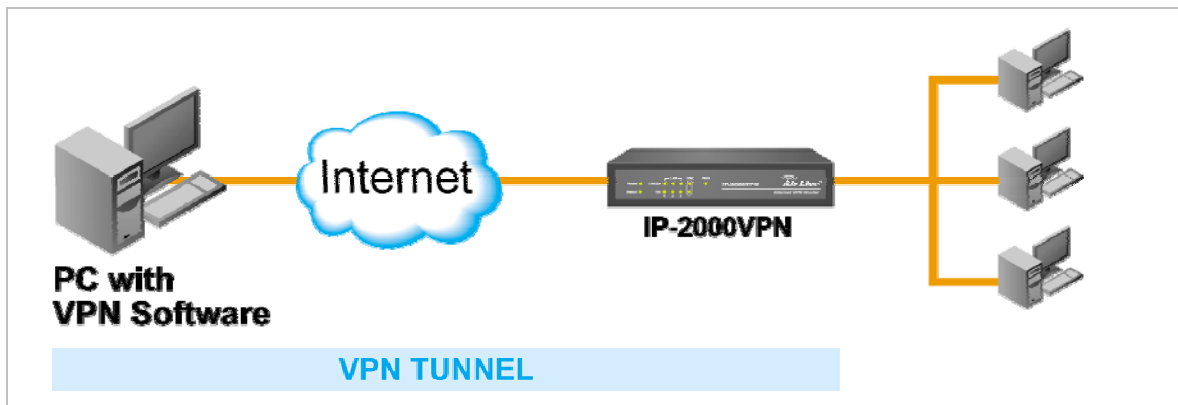
2. Enter the following setting in **Incoming Policy**.

- **Tunnel:** Select To_IP2K_Tunnel.
- Click **OK**.

Add New Policy	
Source Address	Outside_Any ▾
Destination Address	Inside_Any ▾
Service	ANY ▾
Schedule	None ▾
Tunnel	To_IP2K_Tunnel ▾
Action	PERMIT ▾
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
QoS	None ▾
MAX. Bandwidth Per Source IP	Downstream <input type="text" value="0"/> Kbps Upstream <input type="text" value="0"/> Kbps (0: means unlimited)
MAX. Concurrent Sessions Per IP	<input type="text" value="0"/> (Range: 1 - 99999, 0: means unlimited)
MAX. Concurrent Sessions	<input type="text" value="0"/> (Range: 1 - 99999, 0: means unlimited)
NAT	<input type="checkbox"/> Enable

8.3 Getting into Office Network from Internet (PPTP) – Windows XP PPTP Client

In this example, a Windows XP client connects to the IP-2000VPN and gains access to the local LAN.



Environment:

	IP-2000VPN	PC with PPTP VPN Software
WAN IP address	60.250.158.65	Any
LAN IP Subnet	192.168.1.x	
Encrypted Authentication	MS-CHAP v2	Typical
User name	jacky	jacky
Password	1234	1234

Step 1: Set up IP-2000VPN PPTP Server

1. Select **Microsoft VPN** → **Server**, and tick the selection of “**Enable PPTP (VPN) Server**”.
2. Select the encrypted authentication type, in this case we select **MS-CHAP v2**.



Step 2: Set up IP-2000VPN PPTP Server

1. Select **Microsoft VPN** → **Clients**, and tick the selection of “**Allow Connection**” in **Properties**.
2. Fill in with the form to enter user name and password. For example, user name is jacky, and password is 1234.

The screenshot shows the 'Microsoft VPN Client Database' interface. It has two main sections: 'Existing Users' and 'Properties'.
- The 'Existing Users' section contains an empty list box and a 'Delete' button below it.
- The 'Properties' section contains a form with the following elements:
 - A checked checkbox labeled 'Allow connection'.
 - A 'Login Name:' field with the text 'jacky' entered.
 - A 'Login Password:' field with four dots.
 - A 'Verify Password:' field with four dots.
 - A 'Clear Form' button at the bottom right of the form.
- Below the 'Properties' form are two buttons: 'Add as New User' and 'Update Selected User'.

3. Click “**Add as New User**” button to update the account into “**Existing Users**” list.
4. Complete to set up PPTP VPN of IP-2000VPN.

This screenshot shows the same 'Microsoft VPN Client Database' interface as the previous one, but after the user 'jacky' has been added.
- The 'Existing Users' list box now contains the text '1)jacky'.
- The 'Delete' button remains below the list.
- The 'Properties' form is identical to the previous screenshot, with the 'Allow connection' checkbox checked and the 'Login Name' field containing 'jacky'.
- The 'Add as New User' and 'Update Selected User' buttons are still present at the bottom.



The IP address of IP-2000VPN PPTP Server is exact the same with its WAN IP address.

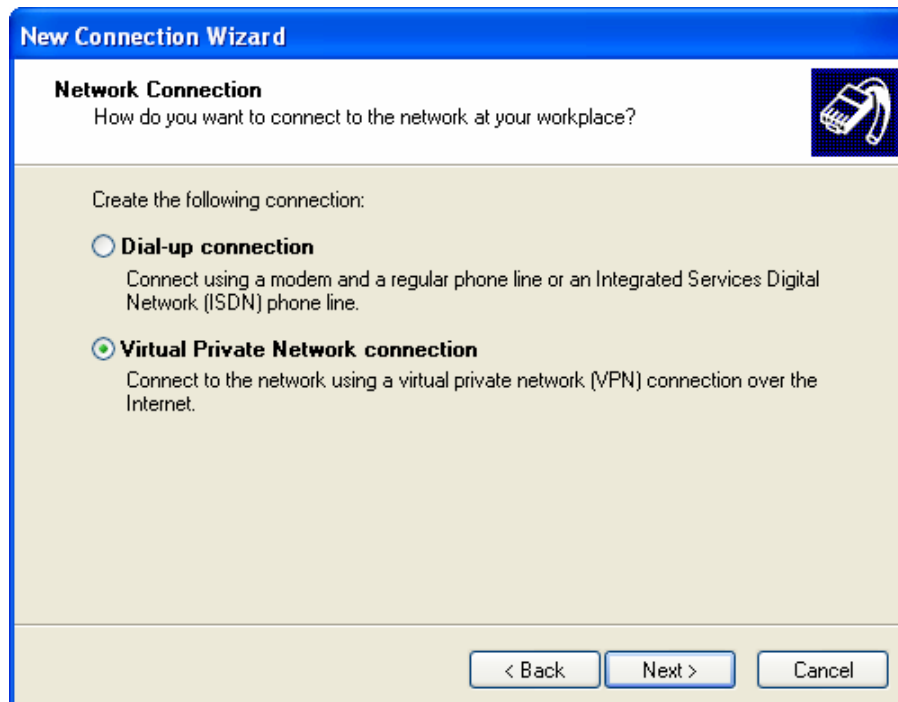
Step 3: Set up Windows XP PPTP client software

Ensure you have logged on with Administrator rights before attempting this procedure.

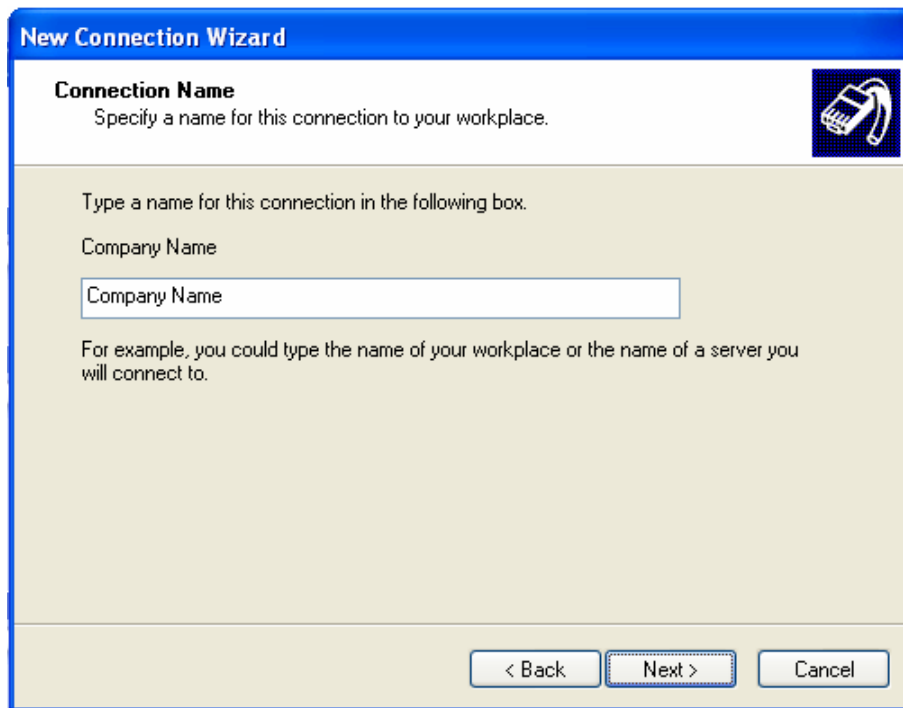
1. Open **Network Connections** (Start → Settings → Network Connections), and start the New Connection Wizard.



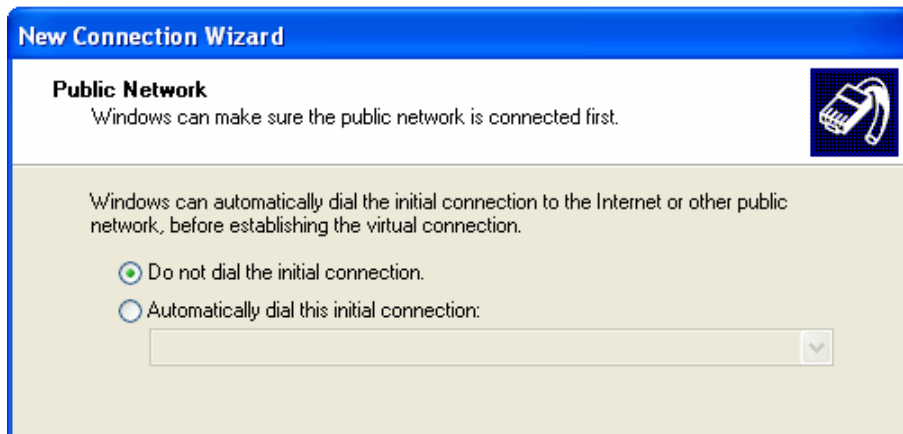
2. Select the option "Connect to the network at my workplace", as shown above, and click **Next**.



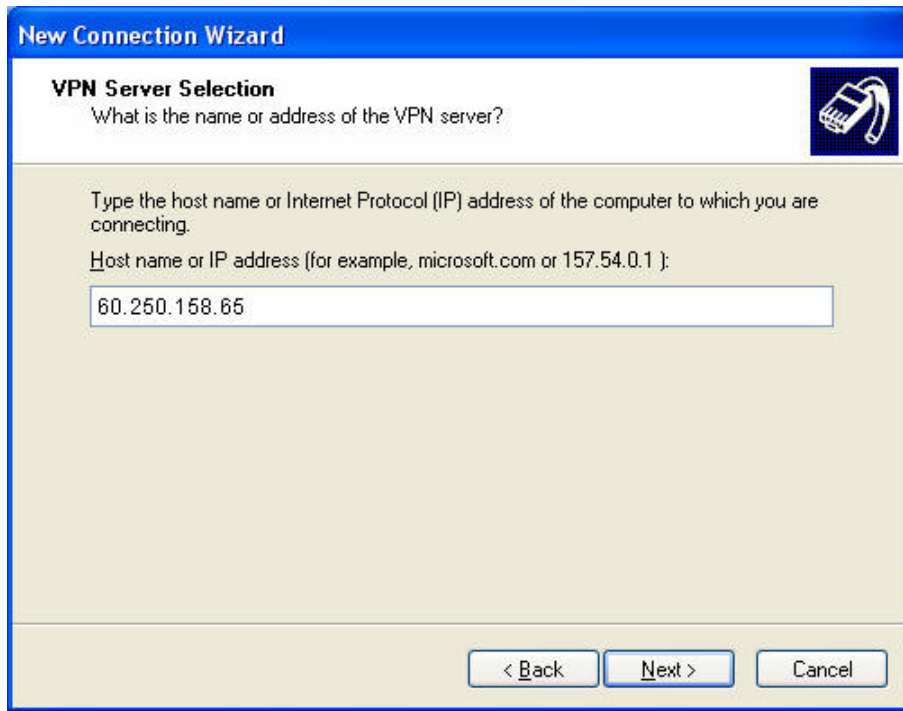
3. On the next screen, shown above, select the "Virtual Private Network connection" option. Click **Next** to continue.



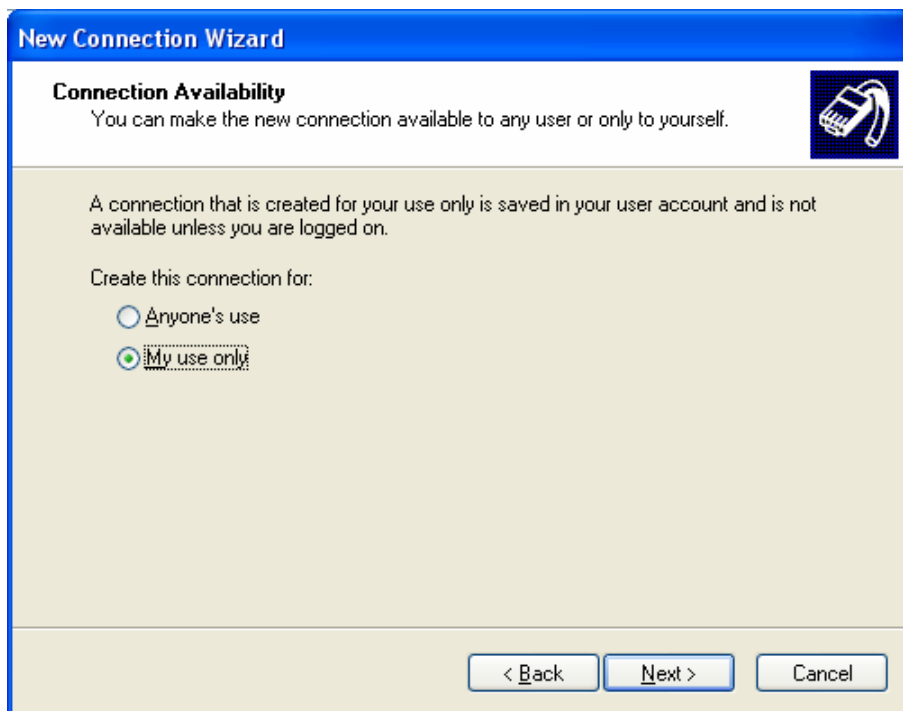
4. Enter a suitable name for this connection.
Click **Next** to continue.



5. On the screen above, select "Do not dial the initial connection".
Click **Next** to continue.



6. On the screen above, enter the Domain Name or Internet IP address of the IP-2000VPN you wish to connect to.
Click **Next** to continue.



7. Choose whether to allow this connection for everyone, or only for yourself, as required.
Click **Next** to continue.
8. On the final screen, click Finish to save and exit.
9. Setup is now complete.

Step 4: Connect Windows XP PPTP client to IP-2000VPN

1. When user finishes Windows XP PPTP client configuration, it will pop up a login windows for user's access.



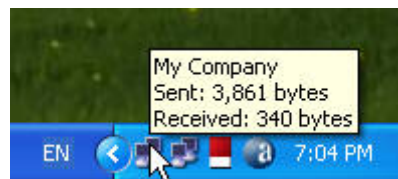
2. Enter the user name and password, for example user name with jacky and password with 1234, tick the selection "Save this user name and password for the following users" in order to record the user's data.



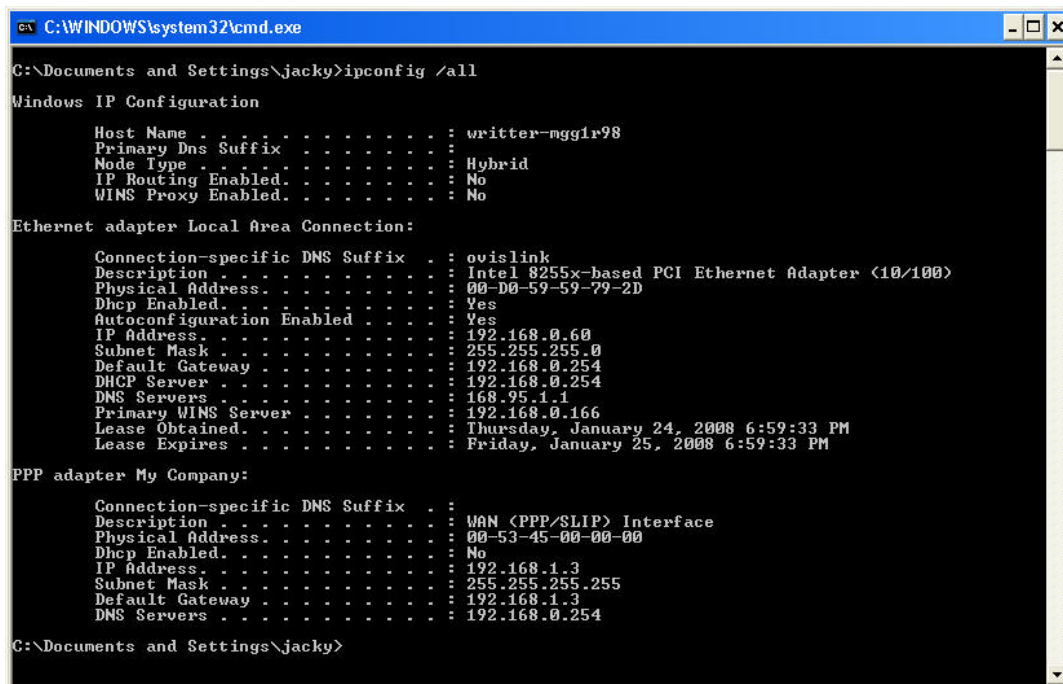
- Click "Connect" button and start the PPTP connection with IP-2000VPN.



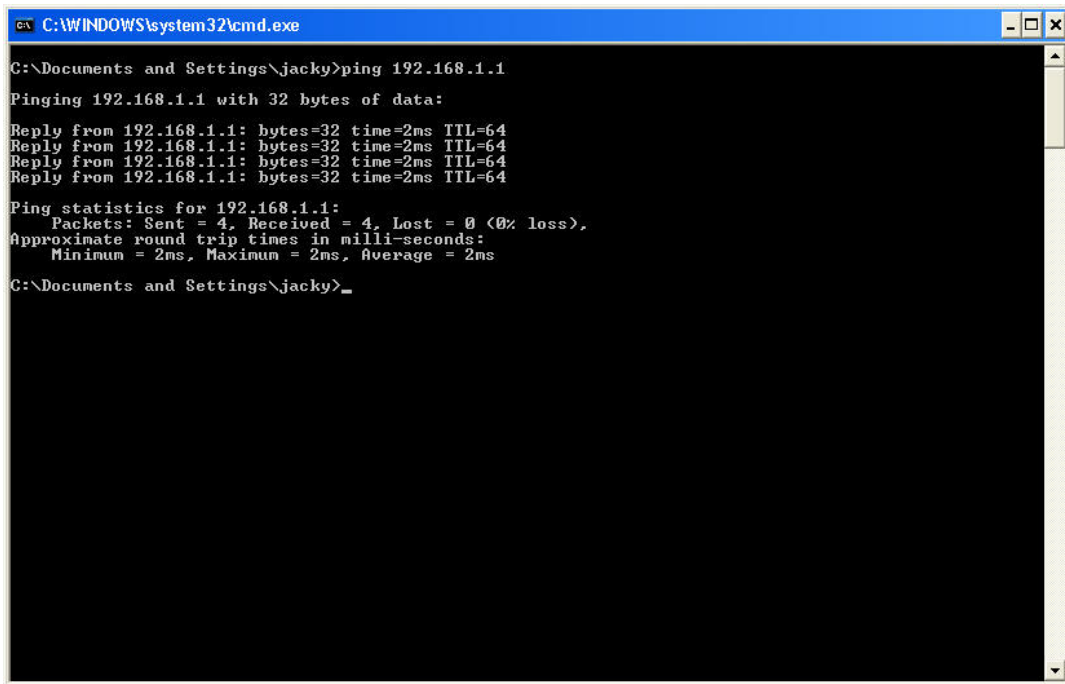
- After verifying client's user name and password, if the connection is successful, the right-bottom corner will add another connection icon to indicate the PPTP connection.



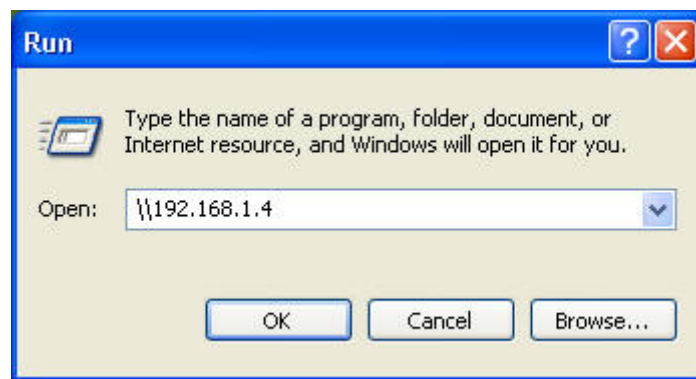
- User can run the Command Prompt in PPTP client's PC to check the current status of PC's IP address, and he will find two IP addresses are registered at client's PC.



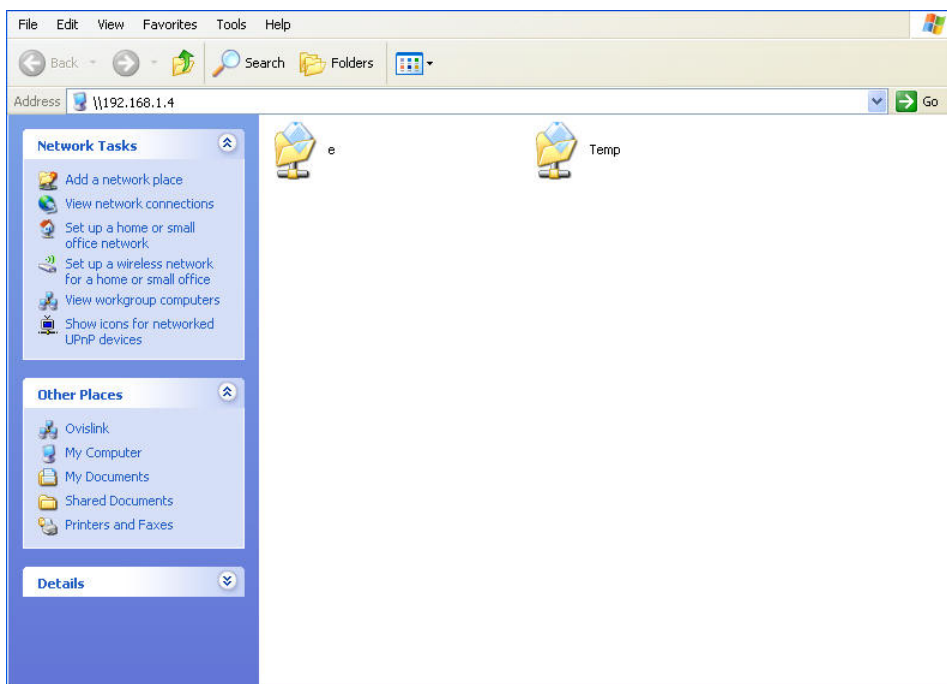
- Try to ping IP-2000VPN LAN IP address (192.168.1.1) and obtain the response.



7. Try to connect the resource PC (192.168.1.4) and search for the shared folder.

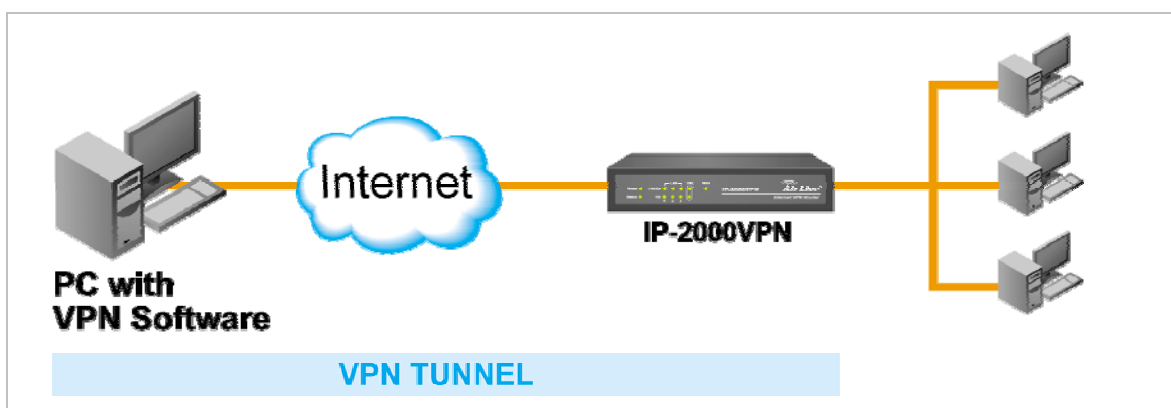


8. When you find out the shared folder, PPTP client can access the resource as well.



8.4 Getting into Office Network from Internet (IPSec) – Windows XP IPSec Client

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



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

Environment:

	IP-2000VPN	PC with IPSec VPN Software
WAN IP address	220.139.232.45	220.139.238.157
LAN IP Subnet	192.168.1.x	
Pre-shared Key	12345678	12345678
IKE Encryption	DES	DES
IKE Authentication	MD5	MD5
DH Group	Group 1 (768 Bit)	Group 1 (768 Bit)
ESP Encryption	3DES	3DES
ESP Authentication	SHA-1	SHA1

Step 1: IP-2000VPN – Network Configuration

Name:

Enable Policy
 Allow NetBIOS traffic

Remote VPN endpoint
 Dynamic IP
 Fixed IP:
 Domain Name:

Local IP addresses
Type: IP address: ~
Subnet Mask:

Remote IP addresses
Type: IP address: ~
Subnet Mask:

Setting	Type	Value	Notes
Name		To_XP	Name does not affect operation. Select a meaningful name.
Enable Policy	Enable		
Allow NetBIOS traffic	Enable		Enable to allow NetBIOS passing through VPN tunnel
Remote Endpoint	Fixed IP	220.139.238.157	Other endpoint's WAN (Internet) IP address.
Local IP addresses	Subnet Address	192.168.1.0 / 255.255.255.0	Allows access to entire LAN. Use a more restrictive definition if possible.
Remote IP addresses	Single Address	220.139.238.157	For a single client, this address is the same as the endpoint address.

Step 2: IP-2000VPN –Authentication and Encryption

Authentication & Encryption

AH Authentication MD5

ESP Encryption 3DES Key Size: n/a (AES only)

ESP Authentication SHA-1

Manual Key Exchange

IKE (Internet Key Exchange)

Direction: Both Directions

Local Identity Type: WAN IP Address

Local Identity Data: 220.139.232.45

Remote Identity Type: Remote WAN IP

Remote Identity Data: 220.139.238.157

Authentication:

RSA Signature (requires certificate)

Pre-shared Key

Authentication Algorithm: MD5

Encryption: DES Key Size: n/a (AES only)

Exchange Mode: Main Mode

IKE SA Life Time: 180 (secs)

IKE Keep Alive

Ping IP Address: 0.0.0.0

IPSec SA Life Time: 300 (secs)

DH Group: Group 1 (768 Bit)

IKE PFS: Disabled

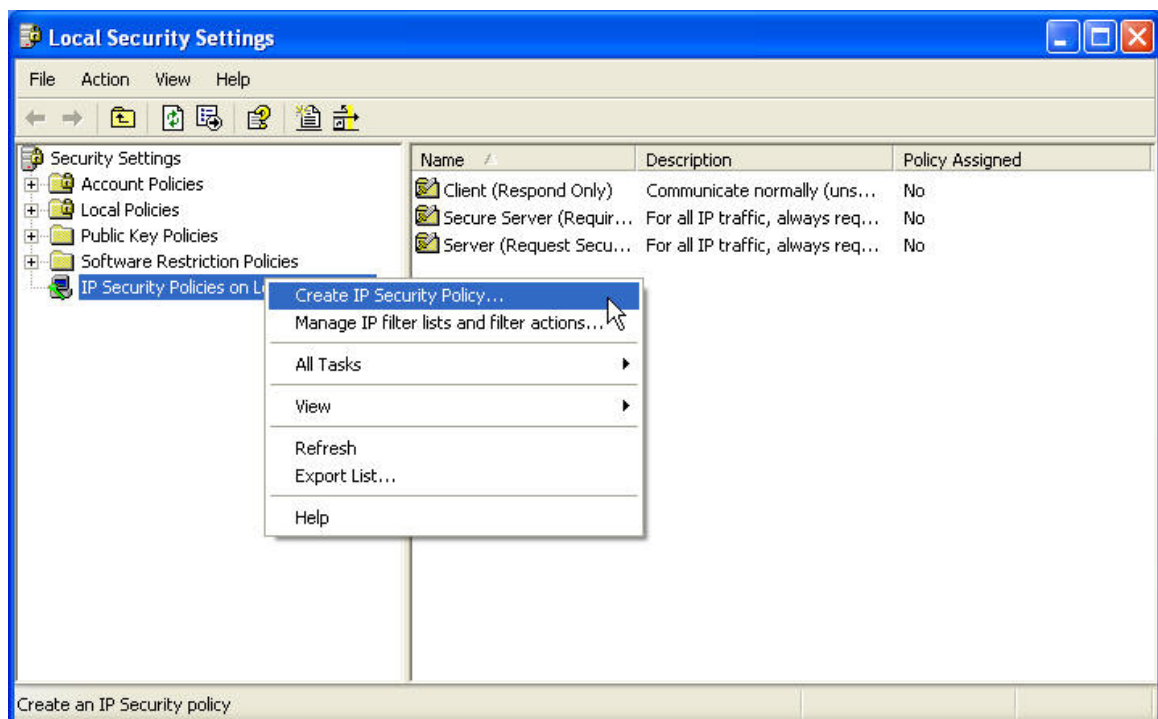
IPSec PFS: None

Setting	Type	Value	Notes
IKE Direction	Both Directions		Using "Responder only" is not possible.
Local Identify	WAN IP Address		System will detect the IP address and fill in the form automatically. It is the most common ID method.
Remote Identify	Remote WAN IP Address		System will detect the IP address and fill in the form automatically. It is the most common ID method.
IKE Authentication method	Pre-shared Key	12345678	Certificates are not widely used.

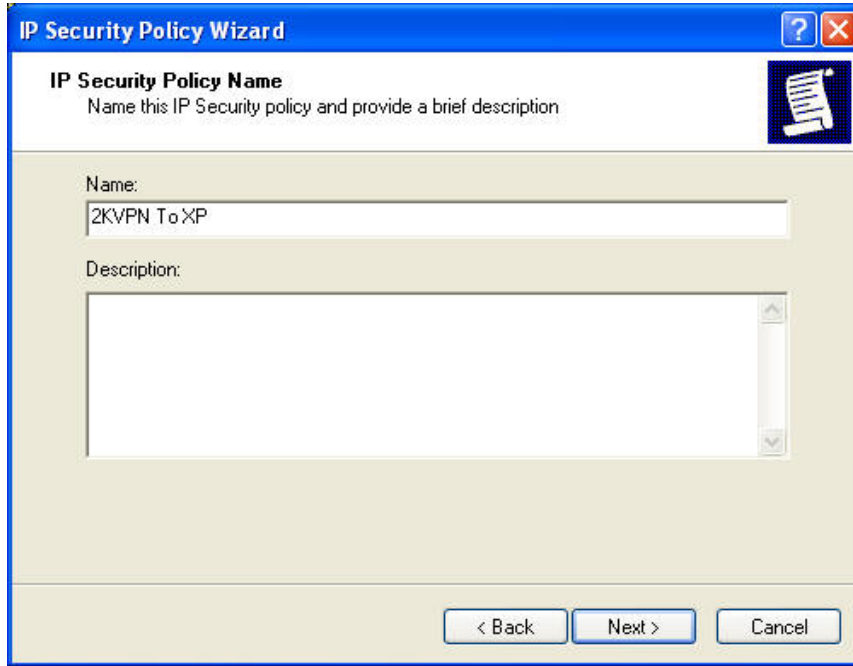
IKE Authentication algorithm		MD5	Must match with Client PC.
IKE Encryption		DES	Must match with Client PC.
IKE Exchange mode	Main Mode		Windows 2000/XP only supports Main Mode.
DH Group	Group 1 (768 bit)		Must match with Client PC.
IKE SA Life time		180	Shorter period will be used.
IKE Keep Alive			Skip the setting
IKE PFS	Disable		Must match with Client PC.
IPSec SA Parameters			
IPSec SA Life time		300	Shorter period will be used.
IPSec PFS	Disable		Must match with Client PC.
AH Authentication	Disable		AH is rarely used.
ESP Authentication	Enable	SHA-1	Must match with Client PC.
ESP Encryption	Enable	3DES	Must match with Client PC.

Step 3: Windows XP IPSec Client Configuration

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



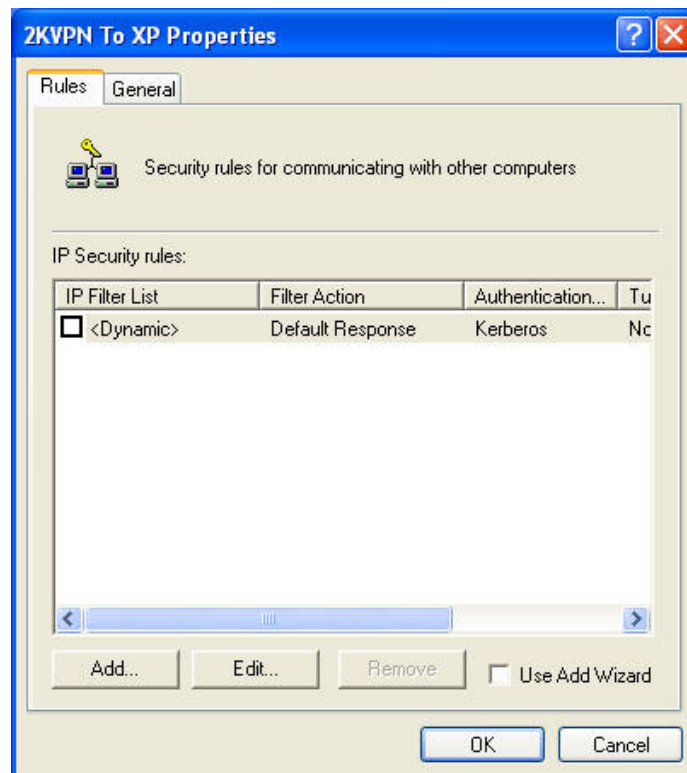
3. Click "Next", and then enter a policy name, for example "2KVPN To XP", then click "Next".



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.

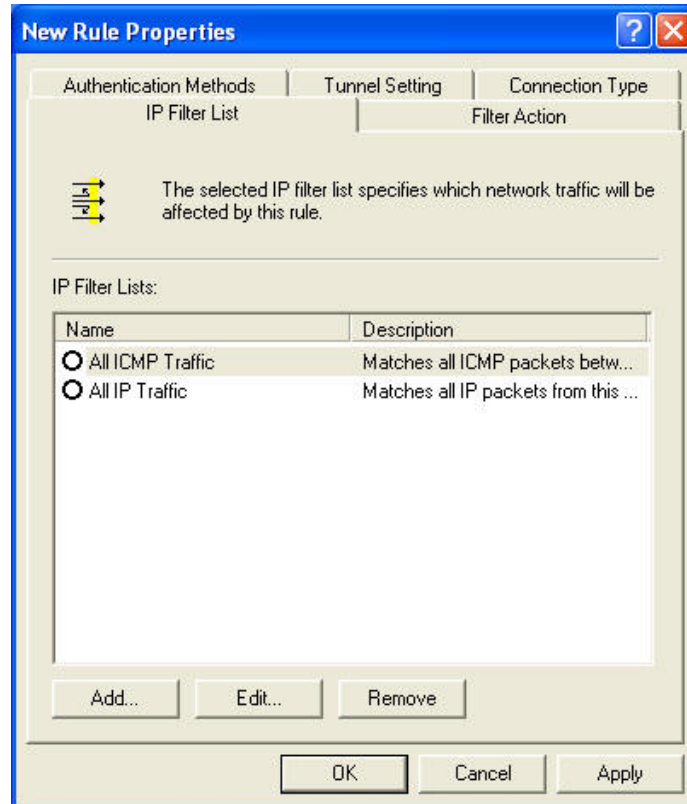




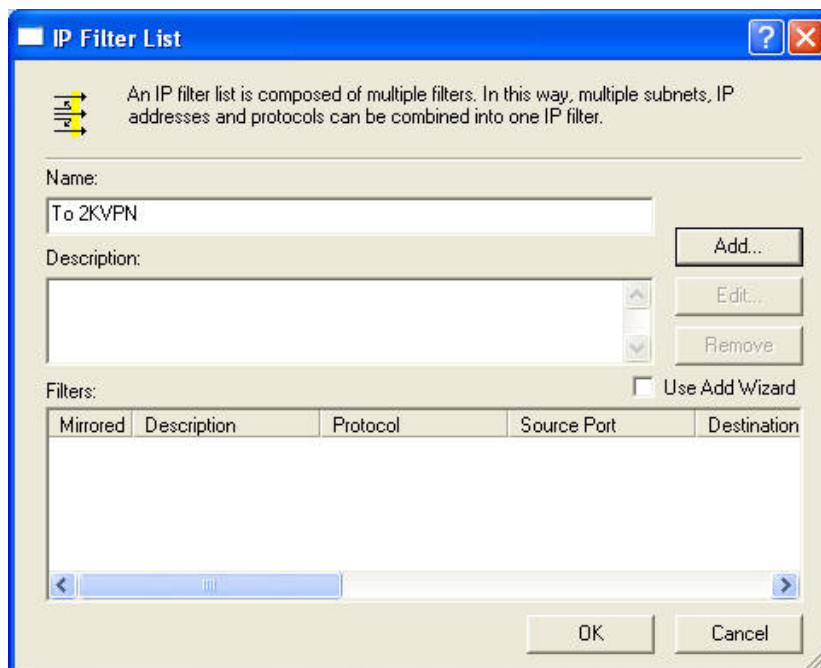
1. No rules are in use. Two (2) rules are required - incoming and outgoing.

2. The outgoing rule will be added first.

6. Deselect the "Use Add Wizard" checkbox, and then click "Add" to view the screen below.

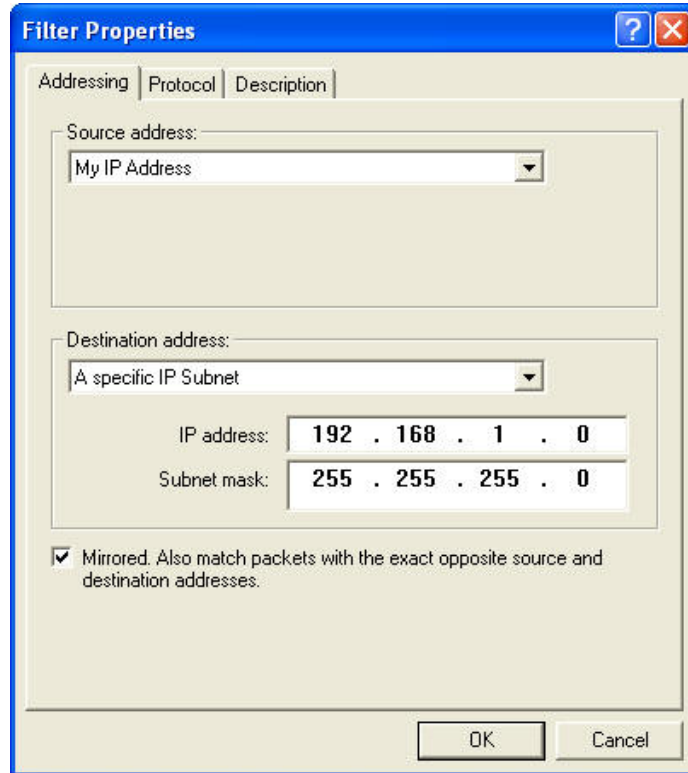


7. Click "Add" and type "To 2KVPN" for the name.

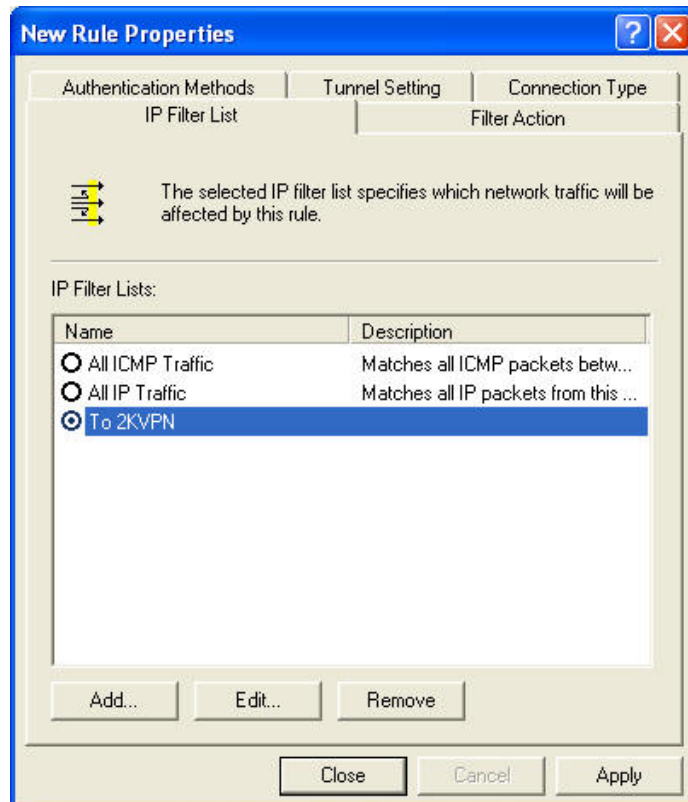


8. Deselect "Use Add Wizard" and then to click "Add" to enter the "Filter Properties" setting.

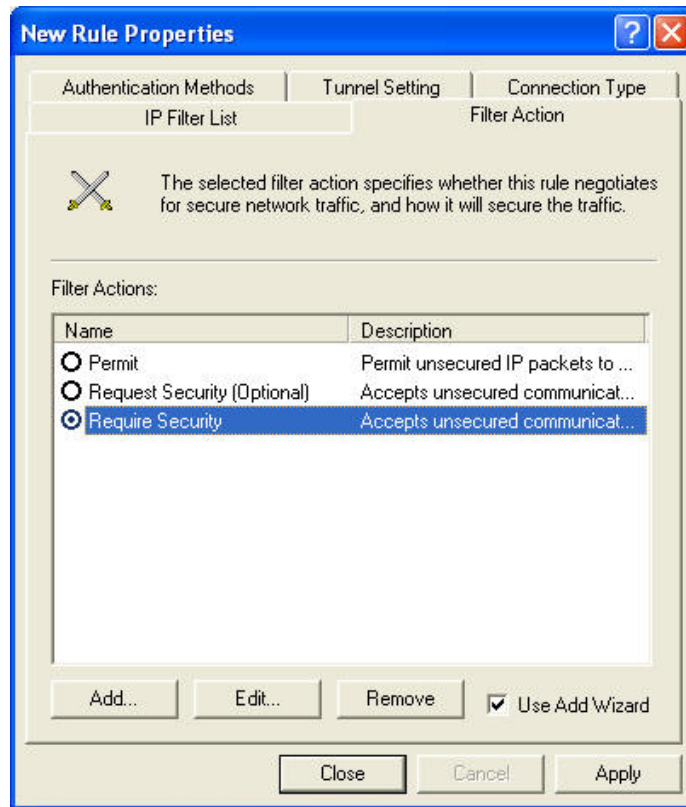
9. Enter the **Source IP address** and the **Destination IP address**.
 - Since this is the outgoing filter, the **Source IP address** is "My IP address" and the **Destination IP address** is the address range used on the remote LAN.
 - Ensure the **Mirrored** option is checked, and click "OK" to save the setting.



10. Click "OK" to save your settings and close this dialog.



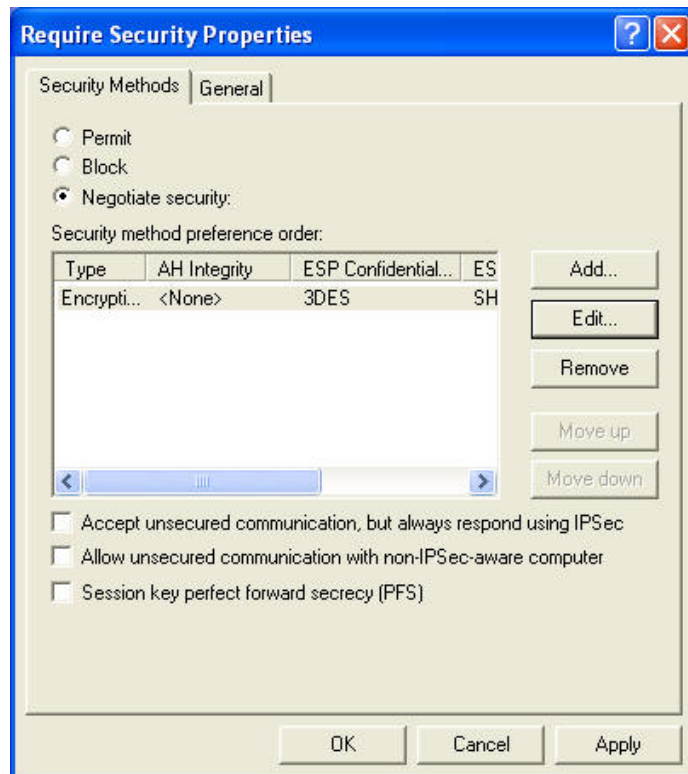
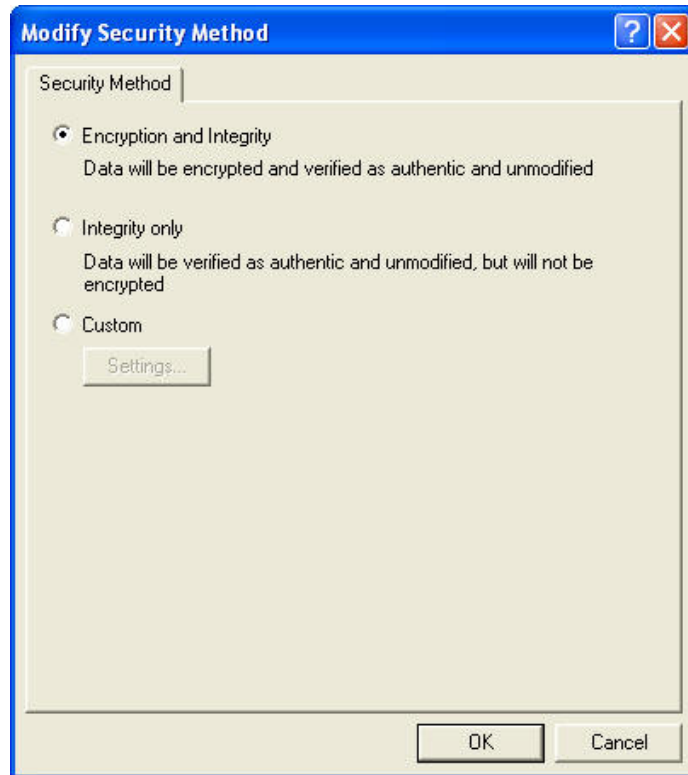
11. On the resulting screen (above), ensure the "To 2KVPN" filter is selected, then click the **Filter Action** tab to see a screen like the following



12. Select **Require Security**, then click the "Edit" button, to view the **Require Security Properties** screen, and select **Negotiate Security** (this selects IKE), then click "Add".



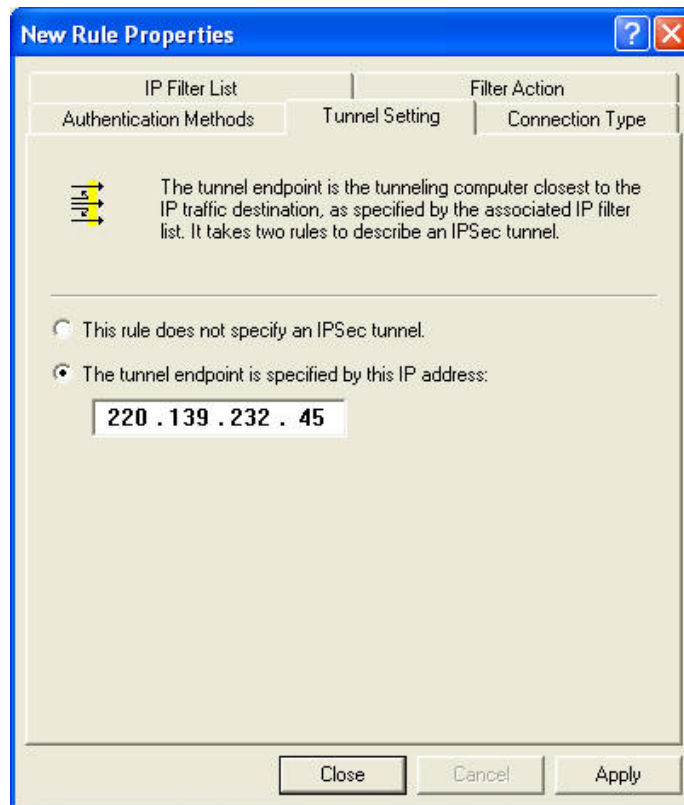
13. On the resulting screen (above), select **Encryption and Integrity** then click "OK" to save your changes and return to the **Require Security Properties** screen.



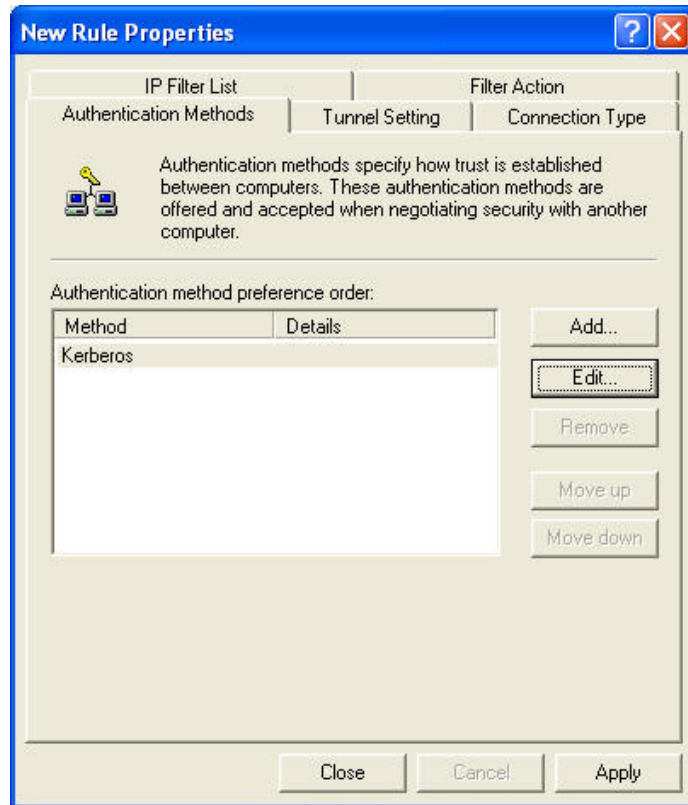
14. Ensure the following settings are correct, and then click "OK" to return to the **Filter Action** tab of the **Edit Rule Properties** screen.

VPN Setting	Windows Setting
IKE enabled	Negotiate security
AH disabled	AH Integrity: <None>
ESP encryption: Enable/3DES	ESP Confidentially: 3DES
ESP authentication: Enable/SHA-1	ESP Integrity: SHA1

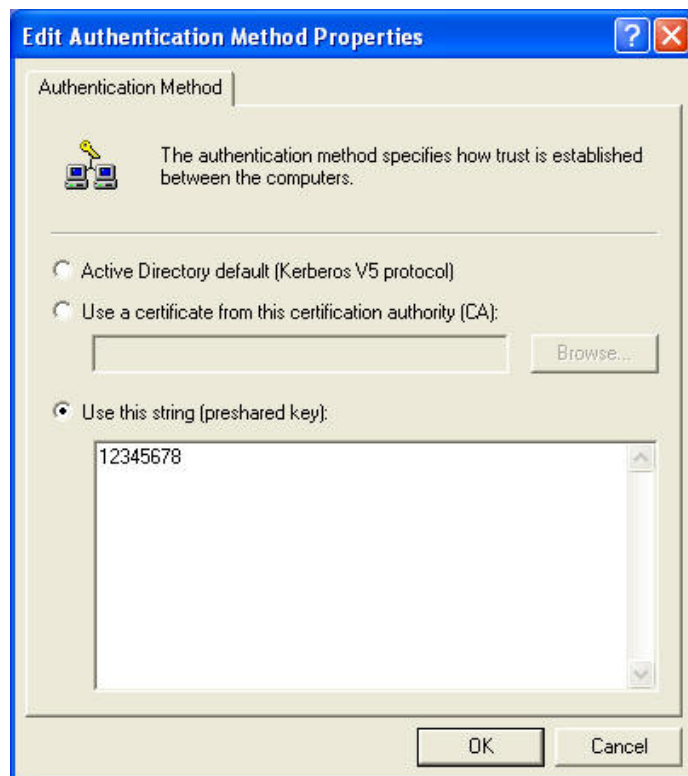
15. Click the **Tunnel Setting** tab, and then select **The tunnel endpoint is specified by this IP address**. Enter the WAN (Internet) IP address of the IP-2000VPN, as shown below.



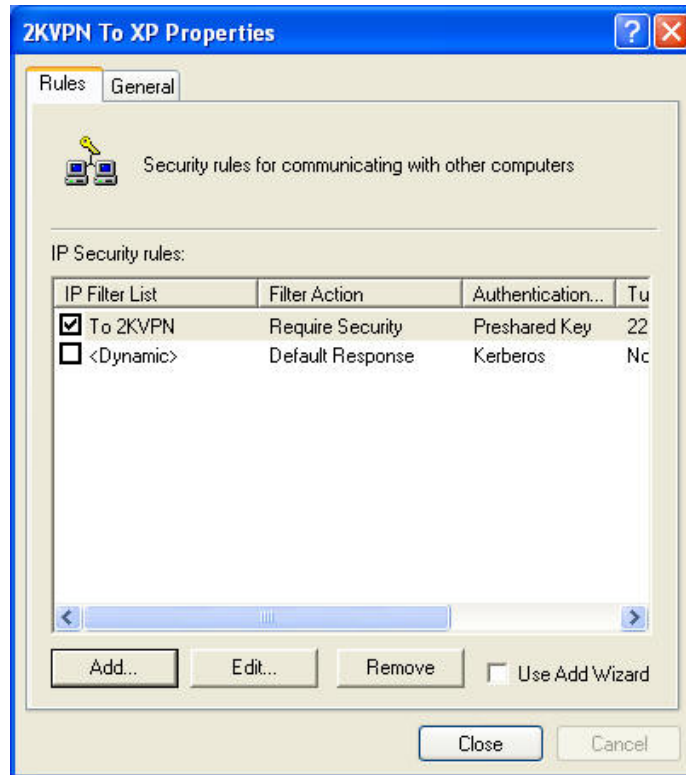
16. Click the **Authentication Methods** tab.



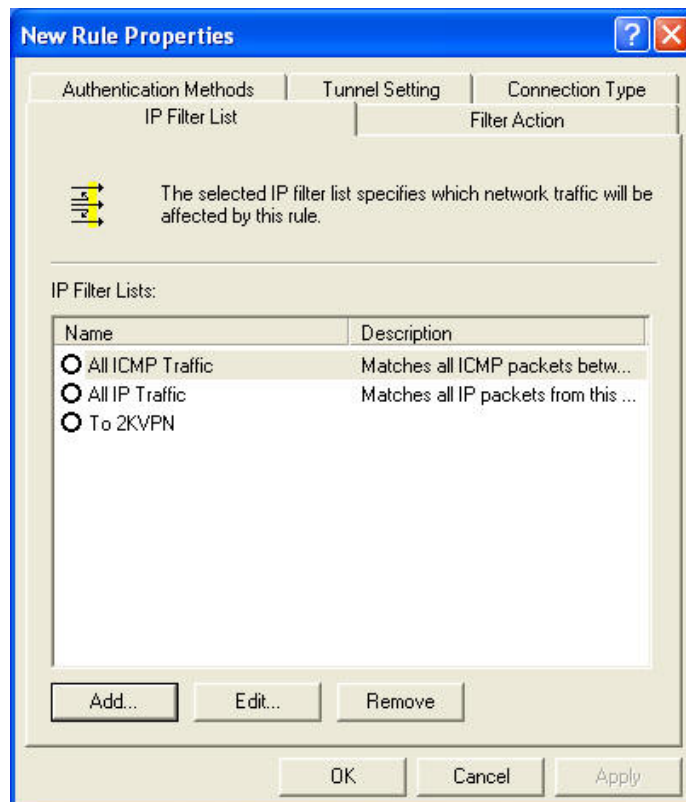
17. Click the "Edit" and select **Use this string (preshared key)**, then enter your preshared key in the field provided.



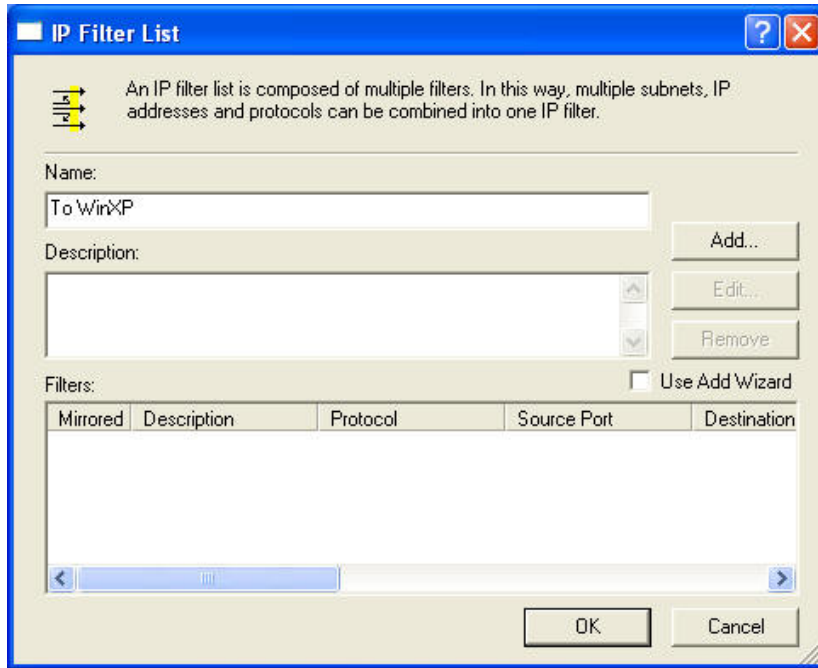
18. Click "OK" to save your changes and return to the **Authentication Methods** tab of the **Edit Rule Properties** screen.
19. Click "Close" to return to the **2KVPN To XP properties** screen. The "To 2KVPN" filter should now be listed, as shown below.



20. To add the second (incoming) rule, click "Add" to create a new rule.

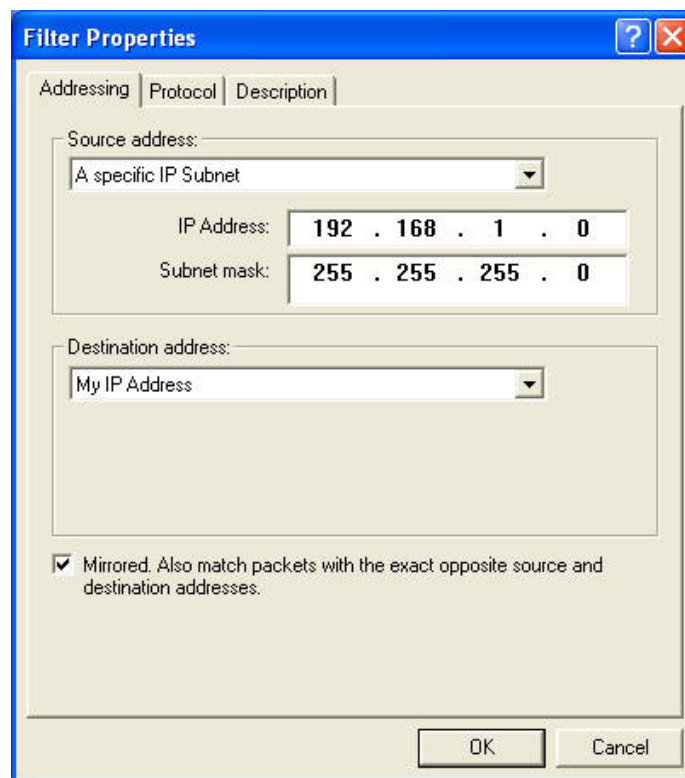


21. Click "Add" and fill in the name with "To WinXP", and then click "Add".

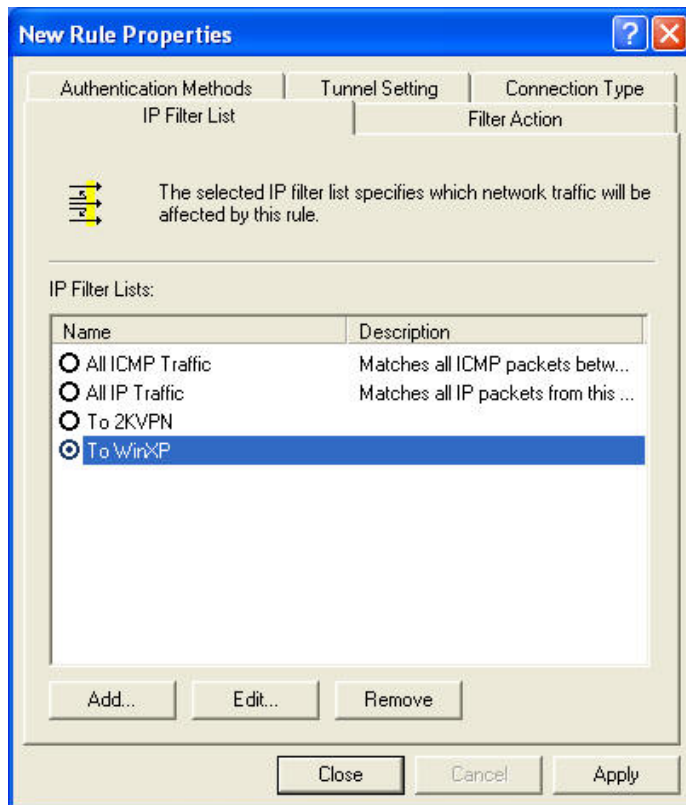


22. Enter the **Source IP address** and the **Destination IP address** as shown below.

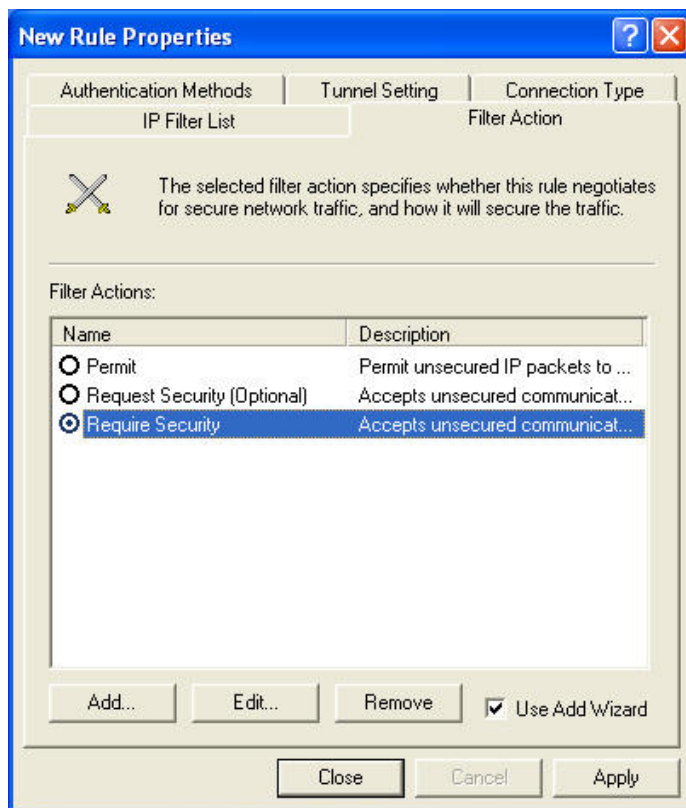
- Since this is the incoming filter, the **Source IP address** is the address range used on the remote LAN and the **Destination IP address** is "My IP address".
- Ensure the **Mirrored** option is checked, and click "OK" to save the setting.



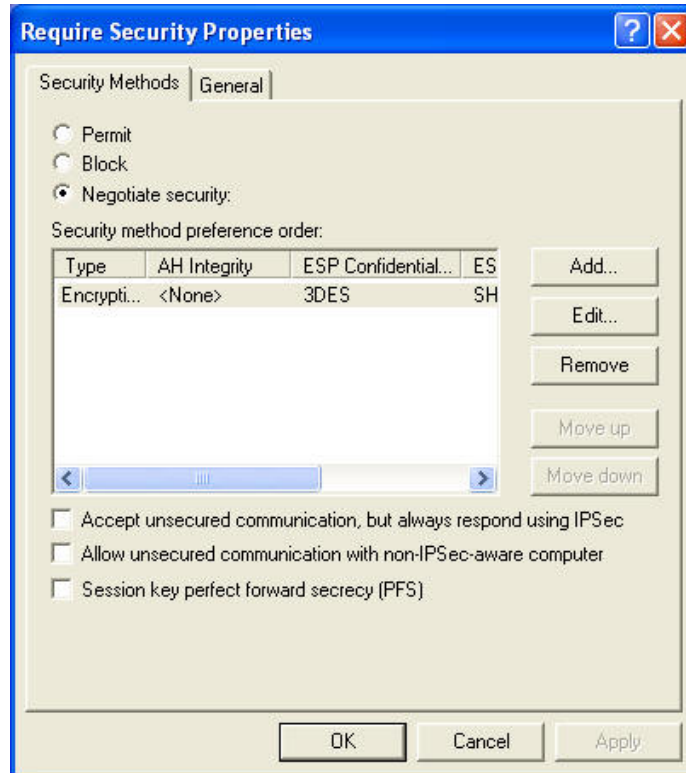
23. Click "OK" to save the setting.



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

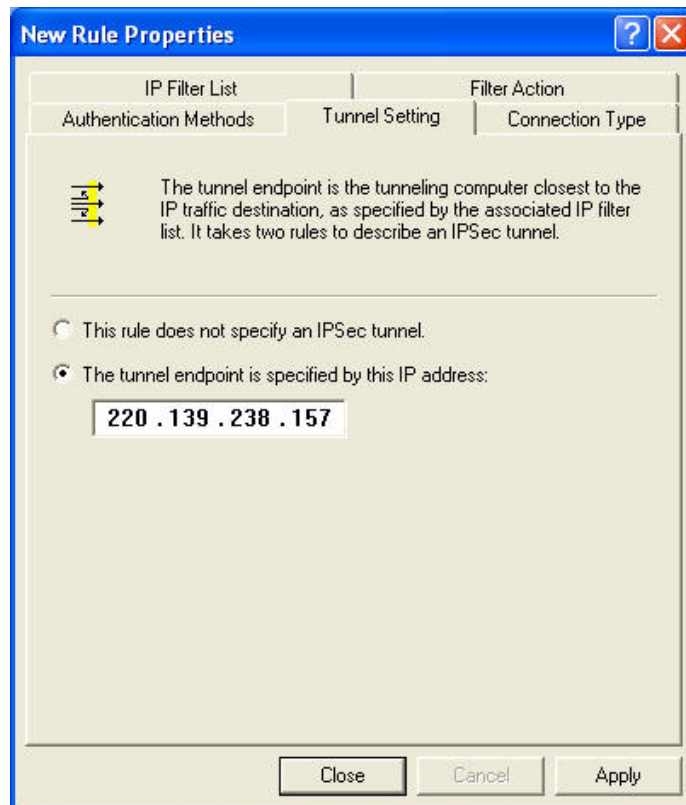


25. Select **Require Security**, then click "Edit". Check the **Negotiate Security** is selected.

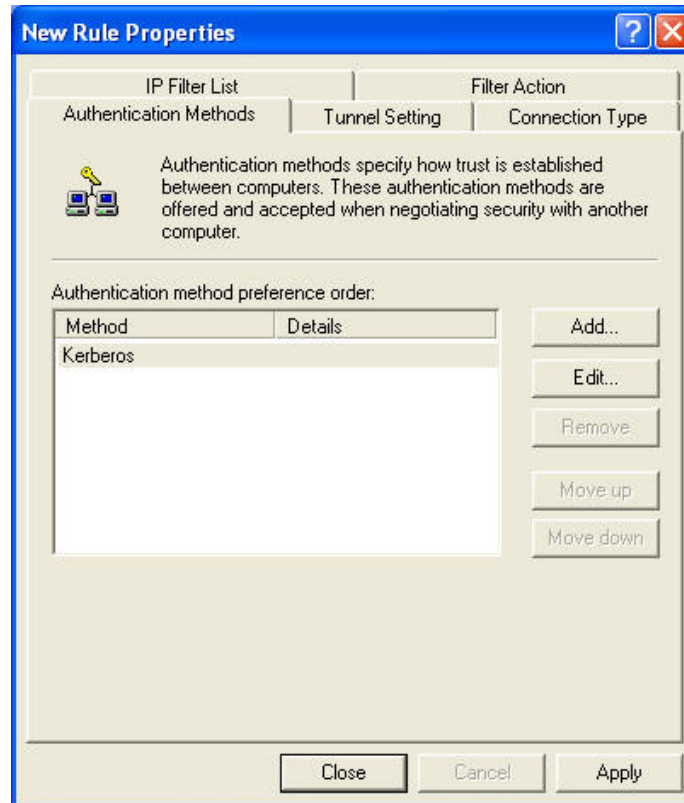


26. Click "OK" to return to the **Filter Action** screen.

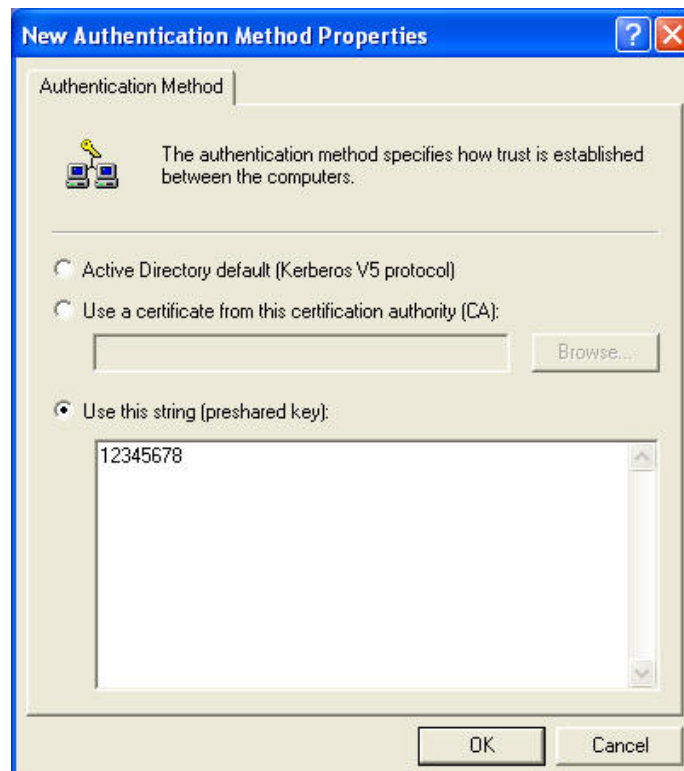
27. Select the **Tunnel Setting** tab, and enter the WAN (Internet) IP address of this PC (220.139.238.157 in this example).



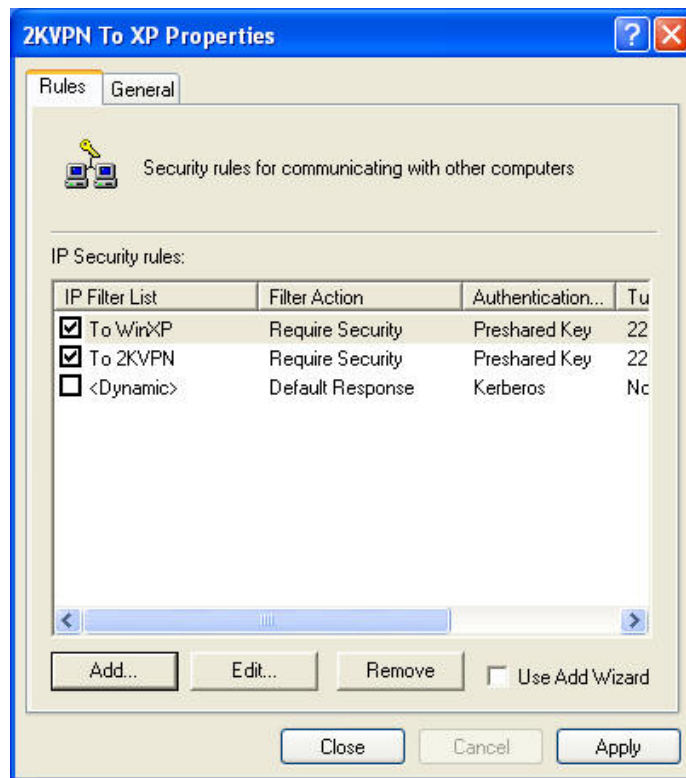
28. Select the **Authentication Methods** tab, and click the "Edit" button.



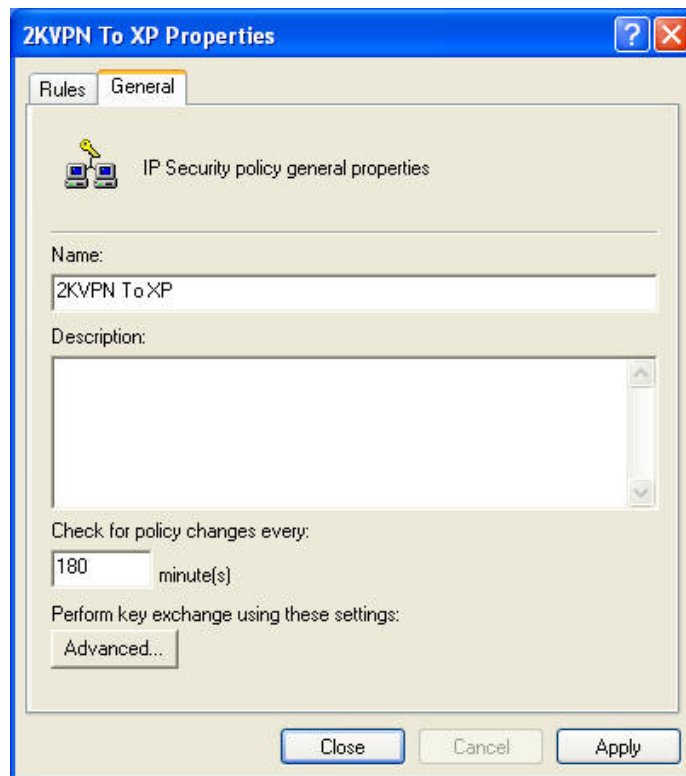
29. Select **Use this string (presared key)**, then enter your preshared key in the field provided.



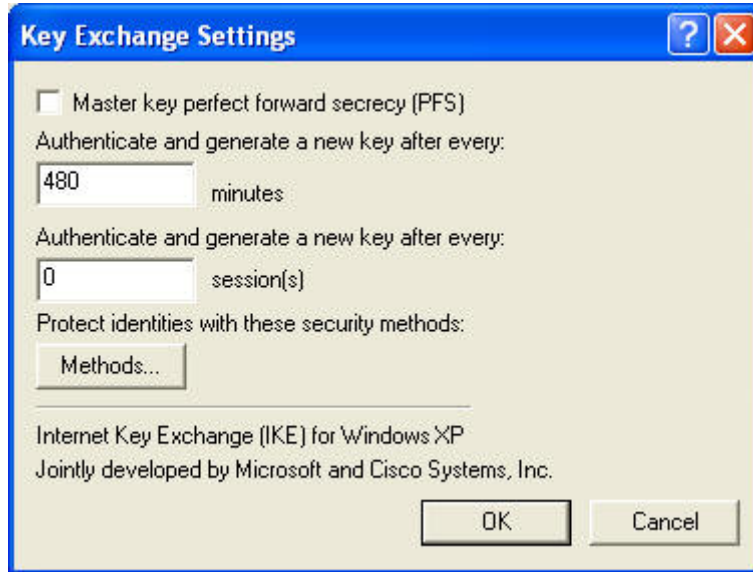
30. Click "OK" to save your settings, then "Close" to return to the **2KVPN to XP Properties** screen. There should now be 2 IP Filers listed, as shown below.



31. Select the **General** tab.



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



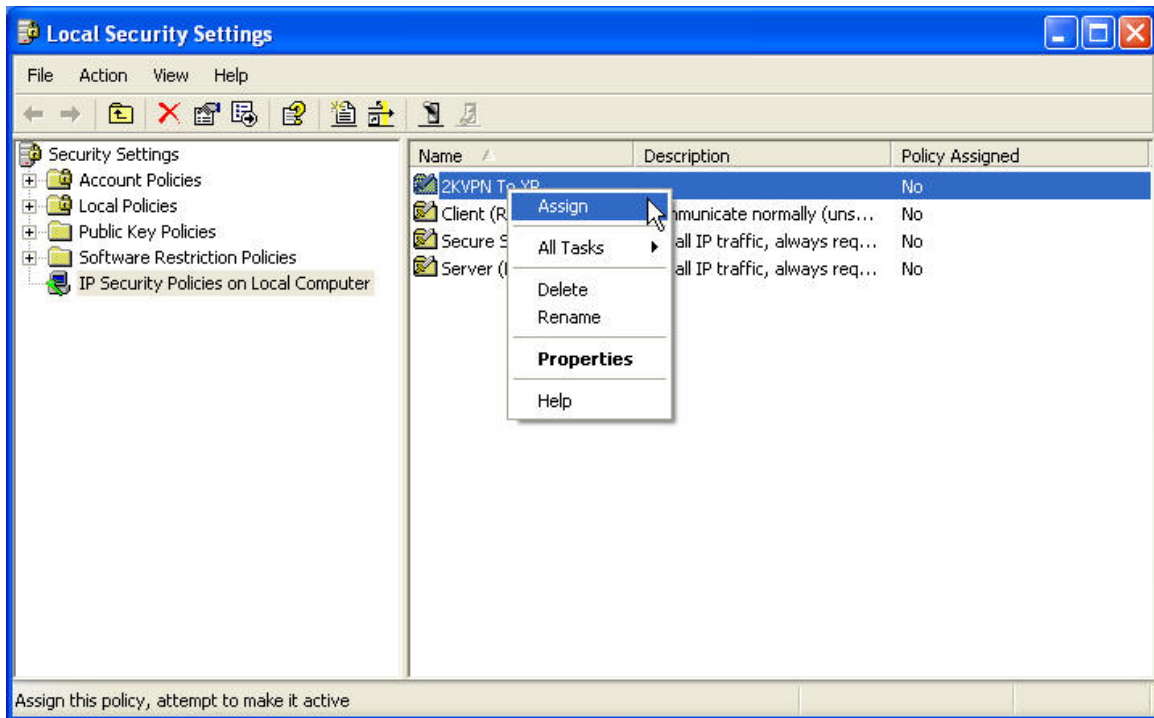
33. Click the "Methods" button to see the screen below.



34. Move up the fourth rule to the top, in order to define "MD5" for **Integrity Algorithm**, "DES" for **Encryption algorithm**, and "Low(1)" for the **Diffie-Hellman Group**.

35. Click "OK" to save, then "OK" again, and then "Close" to return to the **Local Security Settings** screen.

36. Right click the **2KVPN to XP Policy** and select "Assign" to make your policy active.



37. Configuration is now complete.

Chapter 9 Status

Status Screen

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

The screenshot shows the 'Status' screen with the following information:

- Internet**
 - Connection Method: Direct
 - Broadband Modem: Connection OK
 - Internet Connection: Active
 - Internet IP Address: 192.168.0.38[Connection Details](#)
- LAN**
 - IP Address: 192.168.1.1
 - Network Mask: 255.255.255.0
 - DHCP Server: ON
- System**
 - Device Name: AirLive
 - Firmware Version: Version 1.0 Release 0A[System Data](#)

At the bottom, there are three buttons: [Restart Router](#), [Refresh Screen](#), and [Help](#).

Data – Status Screen

Internet	
Connection Method	This indicates the current connection method.
Broadband Modem	This shows the connection status to the modem.
Internet Connection	Current connection status: <ul style="list-style-type: none">• Active• Idle• Unknown• Failed If there is an error, you can click the "Connection Details" button to find out more information.
Internet IP Address	This IP Address is allocated by the ISP (Internet Service Provider).
"Connection Details" Button	Click this button to open a sub-window and view a detailed description of the current connection. Depending on the type of connection, a "log" may also be available.

LAN	
IP Address	The IP Address of the IP-2000VPN.
Network Mask	The Network Mask (Subnet Mask) for the IP Address above.
DHCP Server	This shows the status of the DHCP Server function - either "ON" or "OFF". For additional information about the PCs on your LAN, and the IP addresses allocated to them, use the PC Database option on the Other menu.
System	
Device Name	This displays the current name of the IP-2000VPN.
Firmware Version	The current version of the firmware installed in the IP-2000VPN.
"System Data" Button	Clicking this button will open a Window which lists all system details and settings.
Buttons	
Connection Details	View the details of the current Internet connection. The sub-screen displayed will depend on the connection method used. See the following sections for details of each sub-screen.
System Data	Display all system information in a sub-window.
Restart Router	Restart (reboot) the Router. You will have to wait for the restart to be completed before continuing.
Refresh Screen	Update the data displayed on screen.

9.1 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.

Connection Status - PPPoE

Connection

Physical Address: 00-4f-74-30-00-01
 IP Address: 220.139.237.214
 Network Mask: 255.255.255.255
 PPPoE Link Status: ON

Connection Log

```
066:port[1]:ppp up successfully
065:IPCP up, set MTU:1492
064:Unknown Code.
063:Receive 0:90:1A:40:9:6A 0:4F:74:30:0:1
PPPoE_DISC: 1.1 UNKNOWN ID=0x6E3 len 17
062:start PPP
```

Connect and Disconnect buttons should only be needed if the setting "Connect automatically, as required" is Disabled.

Data – PPPoE Screen

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

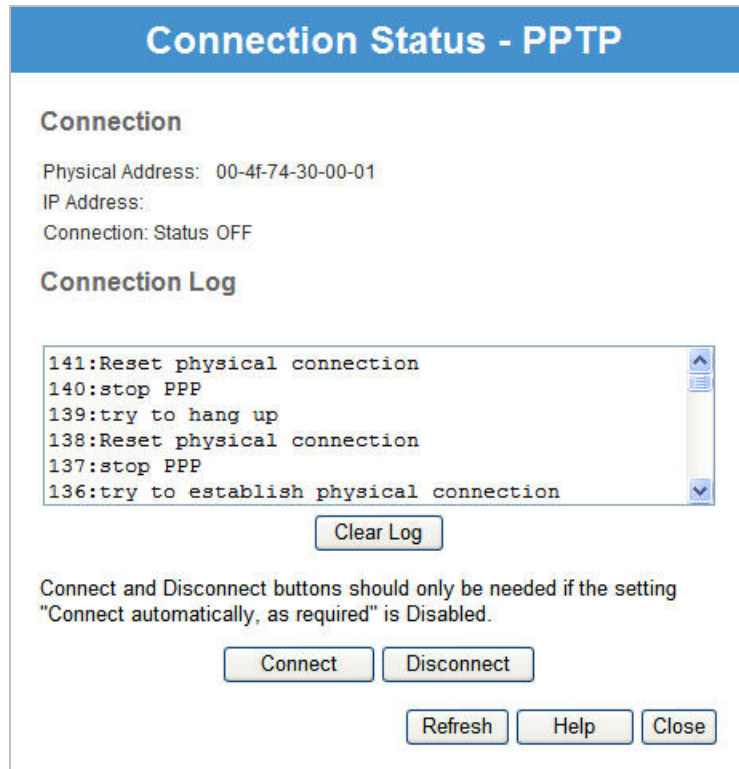
	update the messages shown on screen.
Buttons	
Connect	If not connected, establish a connection to your ISP.
Disconnect	If connected to your ISP, hang up the connection.
Clear Log	Delete all data currently in the Log. This will make it easier to read new messages.
Refresh	Update the data on screen.

Connection Log Messages

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

9.2 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.



Data – PPTP Screen

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

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

9.3 Connection Status – Telstra Big Pond

Connection Status - Telstra Big Pond

Connection

Physical Address: 00-4f-74-30-00-01
 IP Address:
 Connection Status Logged Out

Connection Log

```
004:wait 100 msec "WAN start... "
003:stop PPP
002:TCP Session1:open TCP to BPA_LISTEN
001:BPA Request
000:BPA Dial on demand
```

Connect and Disconnect buttons should only be needed if the setting "Connect automatically, as required" is Disabled.

Data – Telstra Big Pond Screen

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

9.4 Connection Status – 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.

Connection Details - RAS

Internet

RAS Plan 512k Ethernet

Physical Address: 004f74300001

IP Address:

Network Mask:

Default Gateway:

DNS IP Address: 168.95.1.1

DHCP Client: ON

Lease obtained: 0 days,0 hrs,0 minutes

Remaining lease time: 0 days,0 hrs,0 minutes

Data – SingTel RAS Screen

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

<p>Button will display EITHER "Release" OR "Renew"</p>	<p>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"> • If the ISP's DHCP Server has NOT allocated an IP Address for the IP-2000VPN, this button will say "Renew". Clicking the "Renew" button will attempt to re-establish the connection and obtain an IP Address from the ISP's DHCP Server. • If an IP Address has been allocated to the IP-2000VPN (by the ISP's DHCP Server), this button will say "Release". Clicking the "Release" button will break the connection and release the IP Address.
<p>Refresh</p>	<p>Update the data shown on screen.</p>

9.5 Connection Status – 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.

Connection Details

Internet

Physical Address: 00-4f-74-30-00-01

IP Address:

Network Mask:

Default Gateway:

DNS IP Address: 168.95.1.1

DHCP Client: ON

Lease obtained: 0 days,0 hrs,0 minutes

Remaining lease time: 0 days,0 hrs,0 minutes

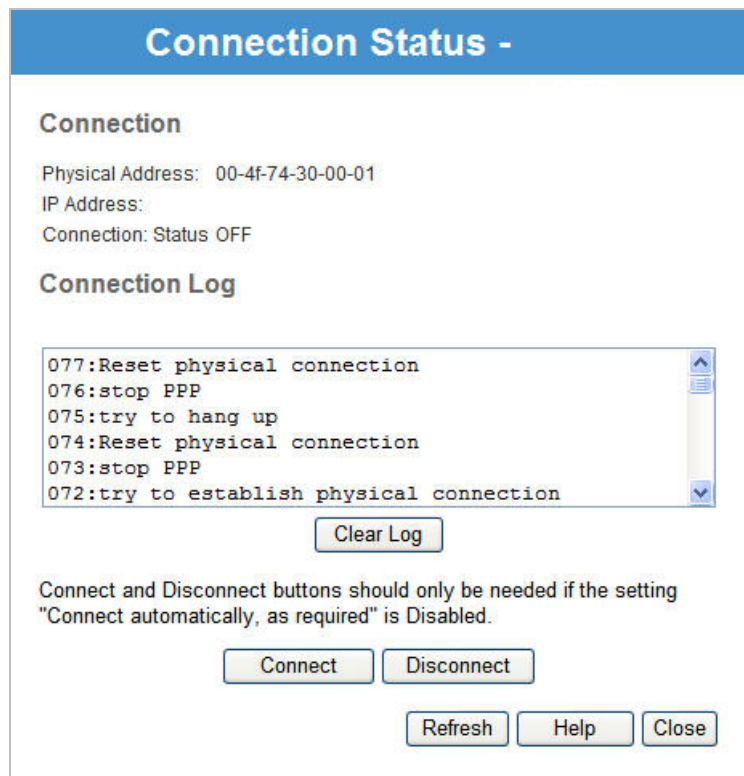
Data – Fixed/Dynamic IP Address Screen

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

OR "Renew"	<ul style="list-style-type: none"> • If the ISP's DHCP Server has NOT allocated an IP Address for the IP-2000VPN, this button will say "Renew". Clicking the "Renew" button will attempt to re-establish the connection and obtain an IP Address from the ISP's DHCP Server. • If an IP Address has been allocated to the IP-2000VPN (by the ISP's DHCP Server), this button will say "Release". Clicking the "Release" button will break the connection and release the IP Address.
Refresh	Update the data shown on screen.

9.6 Connection Status – L2TP

If using L2TP (Layer 2 Tunneling Protocol), a screen like the following example will be displayed when the "Connection Details" button is clicked.



Data – L2TP Screen

Connection	
Physical Address	The hardware address of this device, as seen by remote devices on the Internet. (This is different to the hardware address seen by devices on the local LAN.)
IP Address	The IP Address of this device, as seen by Internet users. This address is allocated by your ISP (Internet Service Provider).
L2TP Status	This indicates whether or not the connection is currently established. <ul style="list-style-type: none"> • If the connection does not exist, the "Connect" button can be used to establish a connection. • If the connection currently exists, the "Disconnect" button can be used to break the connection.
Connection Log	
Connection Log	<ul style="list-style-type: none"> • The Connection Log shows status messages relating to the existing connection. • The "Clear Log" button will restart the Log, while the Refresh button will update the messages shown on screen.

Buttons	
Connect	If not connected, establish a connection to your ISP.
Disconnect	If connected to your ISP, hang up the connection.
Clear Log	Delete all data currently in the Log. This will make it easier to read new messages.
Refresh	Update the data on screen.

Chapter 10 Other Features & Settings

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:

Other Features and Settings	
Config File	Backup or restore the configuration file for the IP-2000VPN. This file contains all the configuration data.
Network Diagnostics	Ping, DNS Lookup.
PC Database	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.
Remote Admin	This feature allows you to manage the IP-2000VPN via the Internet.
Routing	Only required if your LAN has other Routers or Gateways.
Upgrade Firmware	The firmware (software) in the IP-2000VPN can be upgraded using your Web Browser.
UPnP	UPnP (Universal Plug and Play) allows automatic discovery and configuration of the IP-2000VPN.

10.1 Config file

This feature allows you to backup (download) the current settings from the IP-2000VPN, and save them to a file on your PC.

You can restore a previously-downloaded configuration file to the IP-2000VPN, by uploading it to the IP-2000VPN.

This screen also allows you to set the IP-2000VPN back to its factory default configuration. Any existing settings will be deleted.

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

Config File Screen

Config File

Backup Config Download a copy of the current settings.

Restore Config Restore previously saved settings from a file.

Default Config Restore factory default settings.

Data – Config File Screen

Config File	
Backup Config	Use this to download a copy of the current configuration, and store the file on your PC. Click Download to start the download.
Restore Config	<p>This allows you to restore a previously-saved configuration file back to the IP-2000VPN.</p> <p>Click Browse to select the configuration file, then click Restore to upload the configuration file.</p> <p>WARNING !!</p> <p>Uploading a configuration file will destroy (overwrite) ALL of the existing settings.</p>
Default Config	<p>Clicking the Factory-e Defaults button will reset the IP-2000VPN to its factory default settings.</p> <p>WARNING !!</p> <p>This will delete ALL of the existing settings.</p>

10.2 Network Diagnostics

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

An example *Network Diagnostics* screen is shown below.

Network Diagnostics Screen

Data – Network Diagnostics Screen

Ping	
IP Address	Enter the IP address you wish to ping. The IP address can be on your LAN, or on the Internet. Note that if the address is on the Internet, and no connection currently exists, you could get a "Timeout" error. In that case, wait a few seconds and try again.
Ping Button	After entering the IP address, click this button to start the "Ping" procedure. The results will be displayed in the <i>Ping Results</i> pane.
DNS Lookup	
Internet name	Enter the Domain name or URL for which you want a DNS (Domain Name Server) lookup. Note that if the address is on the Internet and no connection currently exists, you could get a "Timeout" error. In that case, wait a few seconds and try again.
Lookup Button	After entering the Domain name/URL, click this button to start the "DNS Lookup" procedure.

10.3 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.

The screenshot shows a web interface titled "PC Database". It includes instructions: "DHCP Clients are automatically added and updated. If not listed, try restarting the PC." and "PCs using a Fixed IP address can be added and deleted below." A box labeled "Known PCs" contains two entries: "Jacky 192.168.1.3 (LAN) (DHCP)" and "writer-mgg1r98 192.168.1.2 (LAN) (DHCP)". To the right is an "Add" form with fields for "Name:" and "IP Address:" (with four input boxes for octets). Below the list is a "Delete" button. At the bottom are "Refresh", "Generate Report", "Advanced Administration", and "Help" buttons.

- 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 IP-2000VPN 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

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

IP Address	Enter the IP Address of the PC. The PC will be sent a "ping" to determine its hardware address. If the PC is not available (not connected, or not powered On) you will not be able to add it.
Buttons	
Add	This will add the new PC to the list. The PC will be sent a "ping" to determine its hardware address. If the PC is not available (not connected, or not powered On) you will not be able to add it.
Delete	Delete the selected PC from the list. This should be done in 2 situations: <ul style="list-style-type: none"> • The PC has been removed from your LAN. • The entry is incorrect.
Refresh	Update the data on screen.
Generate Report	Display a read-only list showing full details of all entries in the PC database.
Advanced Administration	View the Advanced version of the PC database screen. 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

Jacky 192.168.1.3 (LAN) 0018f3f5d354(DHCP)
writer-mgg1r98 192.168.1.2 (LAN) 00d05959792d(DHCP)

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

Data – PC Database (Admin) Screen

PC Database (Admin)	
Known PCs	This lists all current entries. Data displayed is name (IP Address) type . The "type" indicates whether the PC is connected to the LAN.
PC Properties	
Name	If adding a new PC to the list, enter its name here. It is best if this matches the PC's "hostname".
IP Address	<p>Select the appropriate option:</p> <ul style="list-style-type: none"> • Automatic - The PC is set to be a DHCP client (Windows: "Obtain an IP address automatically"). The IP-2000VPN will allocate an IP address to this PC when requested to do so. The IP address could change, but normally won't. • DCHP Client - Reserved IP Address - Select this if the PC is set to be a DCHP client, and you wish to guarantee that the IP-2000VPN 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 IP-2000VPN's IP address. • Fixed IP Address - Select this if the PC is using a Fixed (Static) IP address. Enter the IP address allocated to the PC. (The PC must be configured to use this IP address.)
MAC Address	<p>Select the appropriate option</p> <ul style="list-style-type: none"> • Automatic discovery - IP-2000VPN will contact the PC and find its MAC address. This is only possible if the PC is connected to the LAN and powered on. • MAC address is - Enter the MAC address on the PC. The MAC address is also called the "Hardware Address", "Physical Address", or "Network Adapter Address". The IP-2000VPN uses this to provide a unique identifier for each PC. Because of this, the MAC address can NOT be left blank.
Buttons	
Add as New Entry	<p>Add a new PC to the list, using the data in the "Properties" box.</p> <p>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>
Update Selected PC	Update (modify) the selected PC, using the data in the "Properties" box.
Clear Form	Clear the "Properties" box, ready for entering data for a new PC.
Refresh	Update the data on screen.
Generate Report	Display a read-only list showing full details of all entries in the PC database.
Standard Screen	Click this to view the standard "PC Database" screen.

10.4 Remote Administration

Remote Administration allows you to connect to this interface via the Internet, using your Web browser.

Remote Administration

Information

- If enabled, this interface can be accessed via the Internet.
- Ensure an administration password is assigned.
- To connect, use **HTTPS://address:port** (Not HTTP)
- See help for further details.

Settings

Enable Remote Administration

IP Address to connect to this device:

Port Number:

Allow Remote Access by:

Everyone

IP address range

Start: . . .

Finish: . . .

Only this PC: . . .

Data – Remote Administration Screen

Information	
Information	<p>To establish a connection from the Internet:</p> <ol style="list-style-type: none"> 1. Enable Remote Administration and configure this screen. 2. From a remote location, start your Browser. 3. In the "Address" or "Location" field, enter "HTTPS://" (NOT "HTTP//"), the Internet IP address of this device (NOT the LAN IP address), and the port number, as follows: <div style="text-align: center; margin: 5px 0;">https://ip_address:port_number</div> <p>"ip address" is the Internet IP address of this device. "port number" is the port number assigned on this screen.</p> 4. You should then be prompted for the password for this device. (You must assign a password!)
Settings	
Enable	<p>Check this to allow administration/management via the Internet. (To connect, see above).</p> <p>If Disabled, this device will ignore management connection attempts from the Internet.</p>

IP Address	<p>To manage this device via the Internet, you need to know the IP Address of this device, as seen from the Internet. This IP Address is allocated by your ISP, and is shown here if you are currently connected to the Internet. But if using a Dynamic IP Address, this value can change each time you connect to your ISP. There are 2 solutions to this problem:</p> <ul style="list-style-type: none"> • Have your ISP allocate you a Fixed IP address. • Use the DDNS feature (Internet menu) so you can connect using a Domain Name, rather than an IP address.
Port Number	<p>Enter a port number between 1024 and 65535. The default for HTTP connections is port 80, and for HTTPS port 443. Using either of these is NOT recommended. The default value is 8080.</p> <p>The port number must be specified in your Browser when you connect, as explained above.</p>
Allow Remote Access	<p>This allows you to restrict remote access by IP address. Select the desired option.</p> <ul style="list-style-type: none"> • Everyone - Remote user's IP address is not checked. • IP address range - Only IP addresses in the range specified will be allowed. If selected, you must enter both the Start and Finish IP address. • Only this PC - Only the specified IP address is allowed. If selected, you must enter an IP address in the field provided.

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 "**https://**" followed by the Internet IP Address of the IP-2000VPN. 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. `https://123.123.123.123:8080`

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



The IP-2000VPN is only allowed one user to login its Web UI for managing the device, no matter the user logs the Web UI from Internet or LAN.

If someone already login to IP-2000VPN and without logout the device, the next user will receive a warning message such as "PC1 (192.168.0.3) is managing this device."

10.5 Routing

Overview

- If you don't have other Routers or Gateways on your LAN, you can ignore the "Routing" page completely.
- If the IP-2000VPN 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 IP-2000VPN 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 IP-2000VPN, 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 *錯誤! 找不到參照來源。* later in this chapter for further details and an example.

Routing

RIP RIP Version

Static Routing

Static Routing Table Entries

Properties

Destination Network: . . .

Network Mask: . . .

Gateway IP Address: . . .

Interface: ▾

Metric:

Data – Routing Screen

RIP	
RIP	Select the RIP (Routing Information Protocol) type based on the request and save the setting to enable it. The IP-2000VPN supports RIP 1, RIP 2B, and RIP 2M.
Static Routing	
Static Routing Table Entries	This list shows all entries in the Routing Table. <ul style="list-style-type: none"> The "Properties" area shows details of the selected item in the list. Change any the properties as required, then click the "Update" button to save the changes to the selected entry.

Properties	<ul style="list-style-type: none"> • Destination Network - The network address of the remote LAN segment. For standard class "C" LANs, the network address are the first 3 fields of the Destination IP Address. The 4th (last) field can be left at 0. • Network Mask - The Network Mask for the remote LAN segment. For class "C" networks, the default mask is 255.255.255.0 • Gateway IP Address - The IP Address of the Gateway or Router which the IP-2000VPN must use to communicate with the destination above. (NOT the router attached to the remote segment). • Interface - Normally, this will be "LAN". If NAT is disabled, the "WAN" option can be used for Routers which are accessed via the WAN port. • Metric - 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.
Buttons	
Save	Save the RIP setting. This has no effect on the Static Routing Table.
Add	Add a new entry to the Static Routing table, using the data shown in the "Properties" area on screen. The entry selected in the list is ignored, and has no effect.
Update	Update the current Static Routing Table entry, using the data shown in the "Properties" area on screen.
Delete	Delete the current Static Routing Table entry.
Clear Form	Clear all data from the "Properties" area, ready for input of a new entry for the Static Routing table.
Generate Report	Generate a read-only list of all entries in the Static Routing table.

Configure others Router on your LAN

It is essential that all IP packets for devices not on the local LAN be passed to the IP-2000VPN, 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 IP-2000VPN as the **Default Route** or **Default Gateway**.

Local Router

The local router is the Router installed on the same LAN segment as the IP-2000VPN. This router requires that the **Default Route** is the IP-2000VPN itself. Typically, routers have a special entry for the **Default Route**. It should be configured as follows.

Destination IP Address	Normally 0.0.0.0, but check your router documentation.
Network Mask	Normally 0.0.0.0, but check your router documentation.
Gateway IP Address	The IP Address of the IP-2000VPN.
Interface	LAN
Metric	2

Other Routers on the Local LAN

Other routers on the local LAN must use the IP-2000VPN's **Local Router** as the **Default Route**. The entries will be the same as the IP-2000VPN's local router, with the exception of the **Gateway IP Address**.

- For a router with a direct connection to the IP-2000VPN's local Router, the **Gateway IP Address** is the address of the IP-2000VPN's local router.
- For routers which must forward packets to another router before reaching the IP-2000VPN's local router, the **Gateway IP Address** is the address of the intermediate router.

10.6 Upgrade Firmware

Use this screen to upgrade your IP-2000VPN's firmware.

- You must download the required firmware file, and store it on your PC.
- During the upgrade process, all existing Internet connections will be terminated.
- The upgrade process must NOT be interrupted.

Upgrade Firmware

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

Broadband Router Password:

Upgrade File:

Data – Upgrade Firmware Screen

Upgrade Firmware	
Broadband VPN Router Password	Enter the current password assigned to the IP-2000VPN. If no password has been assigned, leave this blank.
Upgrade File	Click the "Browse" button and browse to the location on your PC where you stored the firmware upgrade file. Select this file.
Start Upgrade	Click this button to start the Firmware upgrade. Note that any users accessing the Internet via the IP-2000VPN will lose their connection. When the upgrade is finished, the IP-2000VPN will restart, and this management connection will be unavailable during the restart.
Cancel	Cancel does NOT stop the Upgrade process if it has started. It only clears the input for the "Upgrade File" field.

To perform the Firmware Upgrade:

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



The IP-2000VPN is unavailable during the upgrade process, and must restart when the upgrade is completed. Any connections to or through the IP-2000VPN will be lost.

10.7 UPnP

An example UPnP screen is shown below.



Data – UPnP Screen

UPnP	
Enable UPnP Services	<ul style="list-style-type: none"> • 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. • If Enabled, this device will be visible via UPnP. • If Disabled, this device will not be visible via UPnP.
Allow Configuration...	<ul style="list-style-type: none"> • If checked, then UPnP users can change the configuration. • If Disabled, UPnP users can only view the configuration. But currently, this restriction only applies to users running Windows XP, who access the Properties via UPnP. (e.g. Right - click the IP-2000VPN in My Network Places, and select Properties)
Allow Internet access to be disabled	<ul style="list-style-type: none"> • If checked, then UPnP users can disable Internet access via this device. • If Disabled, UPnP users can NOT disable Internet access via this device. But currently, this restriction only applies to users running Windows XP, who access the Properties via UPnP. (e.g. Right - click the IP-2000VPN in My Network Places, and select Properties)

Appendix A PC Configuration

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 IP-2000VPN.

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

The IP-2000VPN 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 IP-2000VPN's settings and the default Windows TCP/IP settings, no changes need to be made.

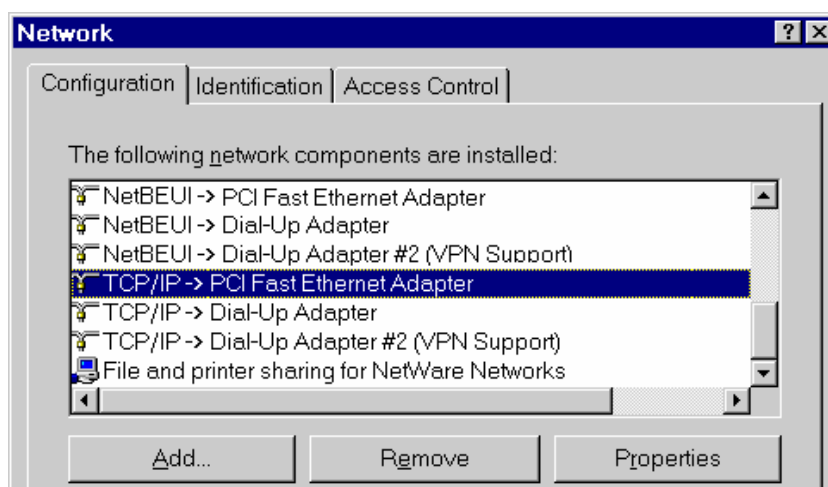
- By default, the IP-2000VPN will act as a DHCP Server, automatically providing a suitable IP Address (and related information) to each PC when the PC boots.
- For all non-Server versions of Windows, the default TCP/IP setting is to act as a DHCP client.

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

- The **Gateway** must be set to the IP address of the IP-2000VPN.
- The **DNS** should be set to the address provided by your ISP.

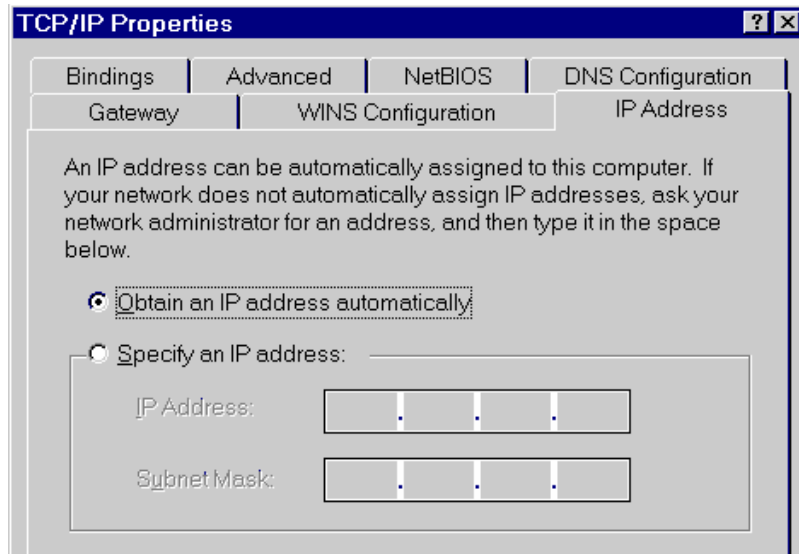
Checking TCP/IP Settings- Windows 9X/ME

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



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.



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

Using DHCP

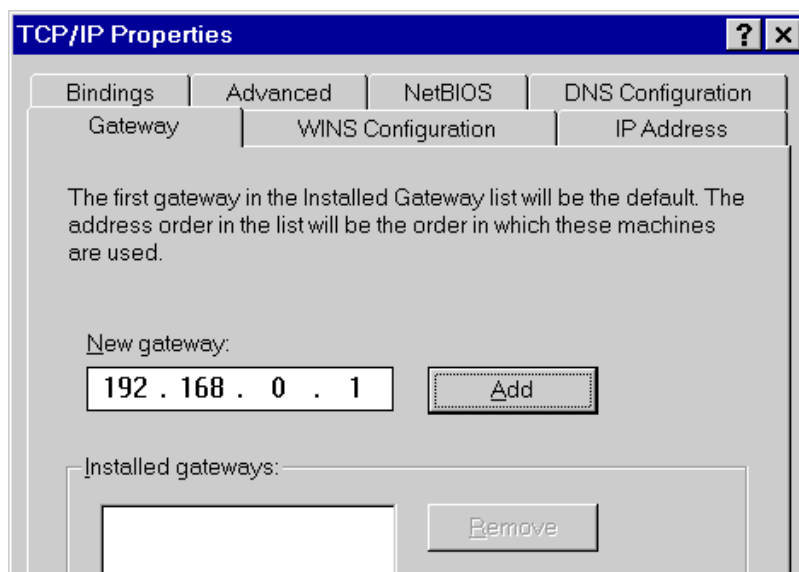
To use DHCP, select the radio button **Obtain an IP Address automatically**. This is the default Windows setting, and it is recommended to use it. By default, the IP-2000VPN will act as a DHCP Server.

Restart your PC to ensure it obtains an IP Address from the IP-2000VPN.

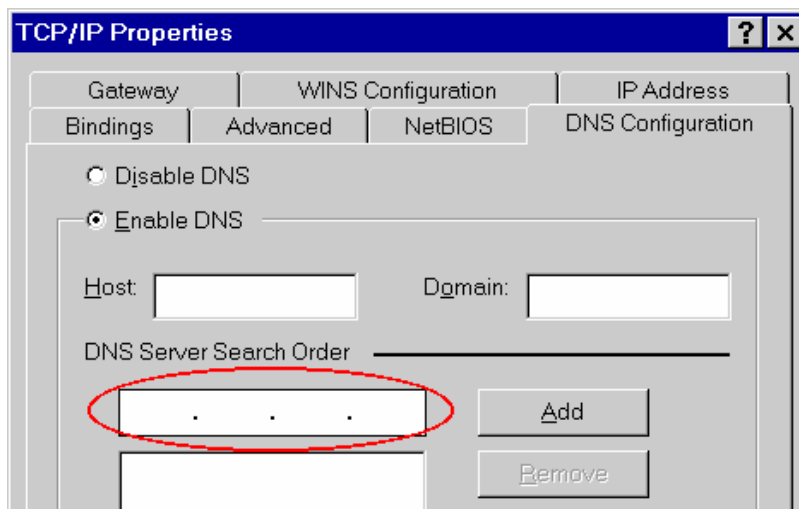
Using "Specify an IP Address"

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

- On the **Gateway** tab, enter the IP-2000VPN'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 IP-2000VPN.

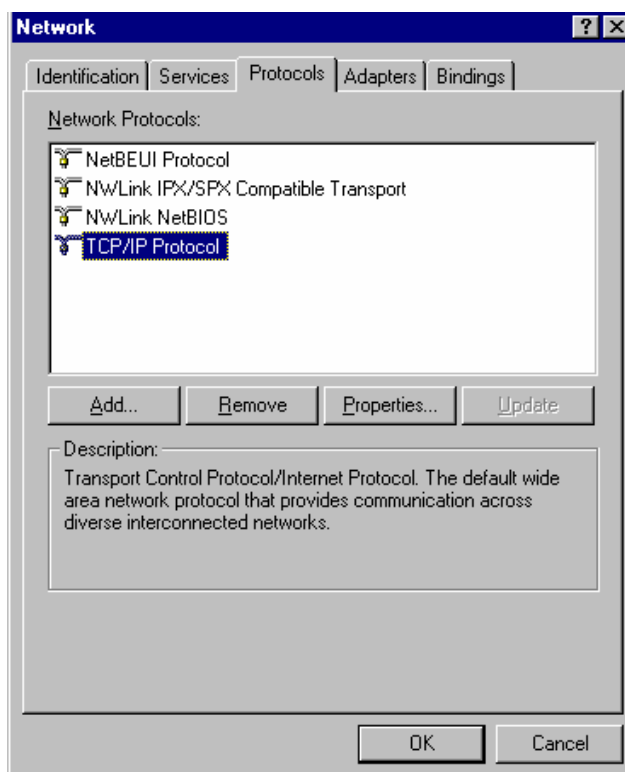


- On the **DNS Configuration** tab, ensure **Enable DNS** is selected. If the **DNS Server Search Order** list is empty, enter the DNS address provided by your ISP in the fields beside the **Add** button, then click **Add**.

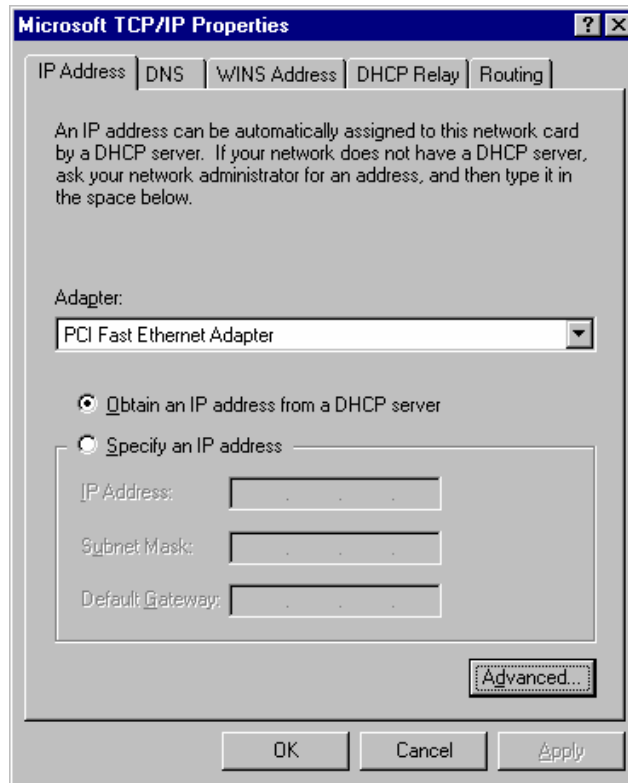


Checking TCP/IP Settings- Windows NT4.0

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



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



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

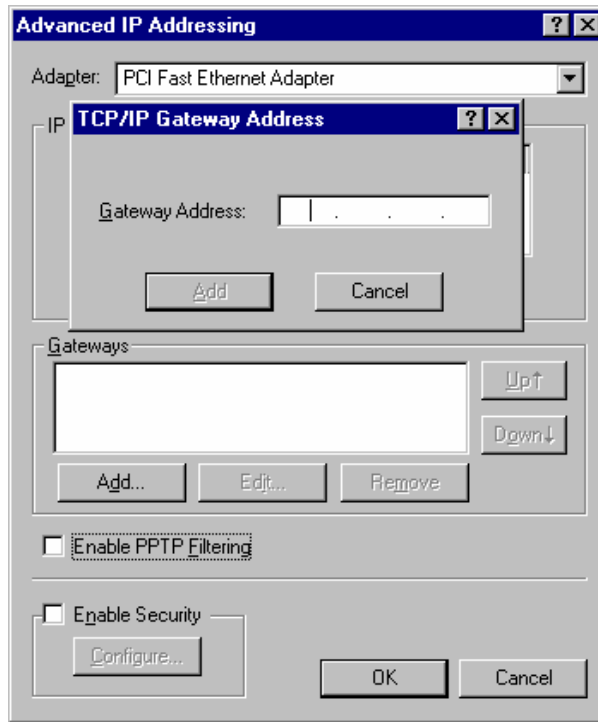
This is the default Windows setting, and it is recommended to use it. By default, the IP-2000VPN will act as a DHCP Server.

Restart your PC to ensure it obtains an IP Address from the IP-2000VPN.

Specify an IP Address

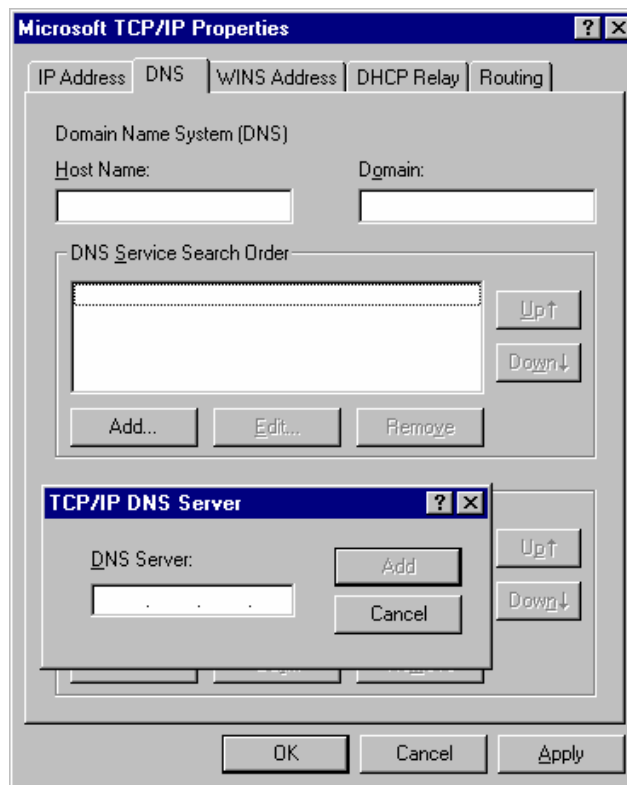
If your PC is already configured, check with your network administrator before making the following changes.

5. The **Default Gateway** must be set to the IP address of the IP-2000VPN. 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 IP-2000VPN's IP address, as shown in below.
 - If necessary, use the **Up** button to make the IP-2000VPN the first entry in the **Gateways** list.



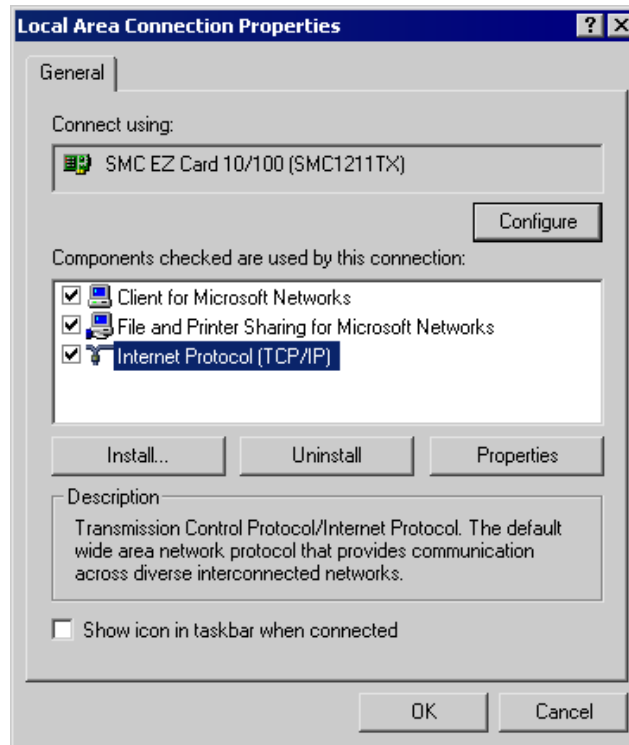
6. The DNS should be set to the address provided by your ISP, as follows:

- 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.

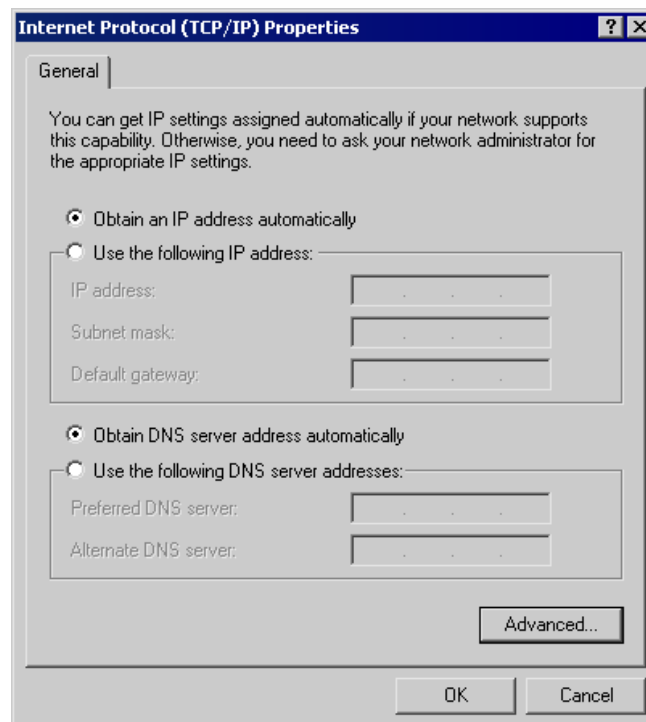


Checking TCP/IP Settings- Windows 2000

1. Select Control Panel - Network and Dial-up Connection.
2. Right click the **Local Area Connection icon** and select **Properties**.



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.



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, and it is recommended to use it. By default, the IP-2000VPN will act as a DHCP Server. Restart your PC to ensure it obtains an IP Address from the IP-2000VPN.

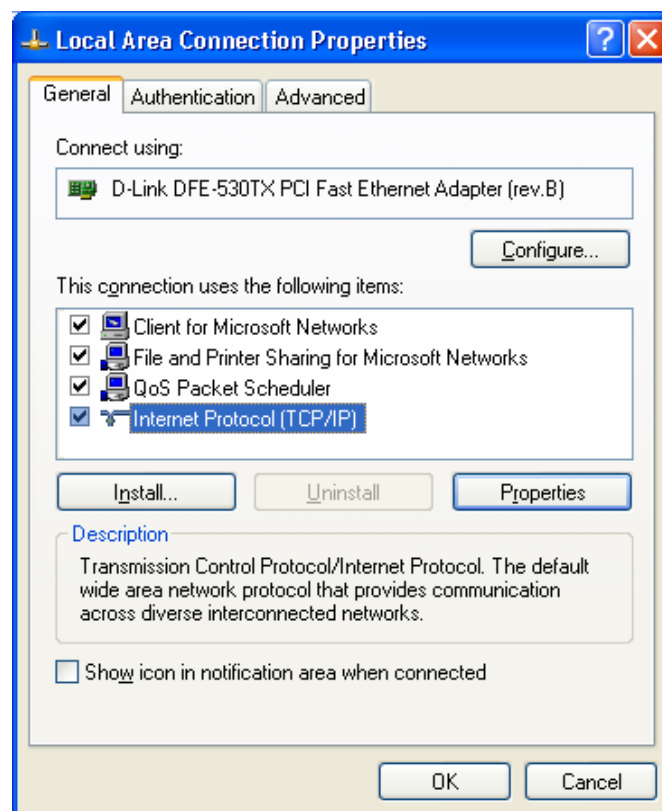
Using a fixed IP Address ("Use the following IP Address")

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

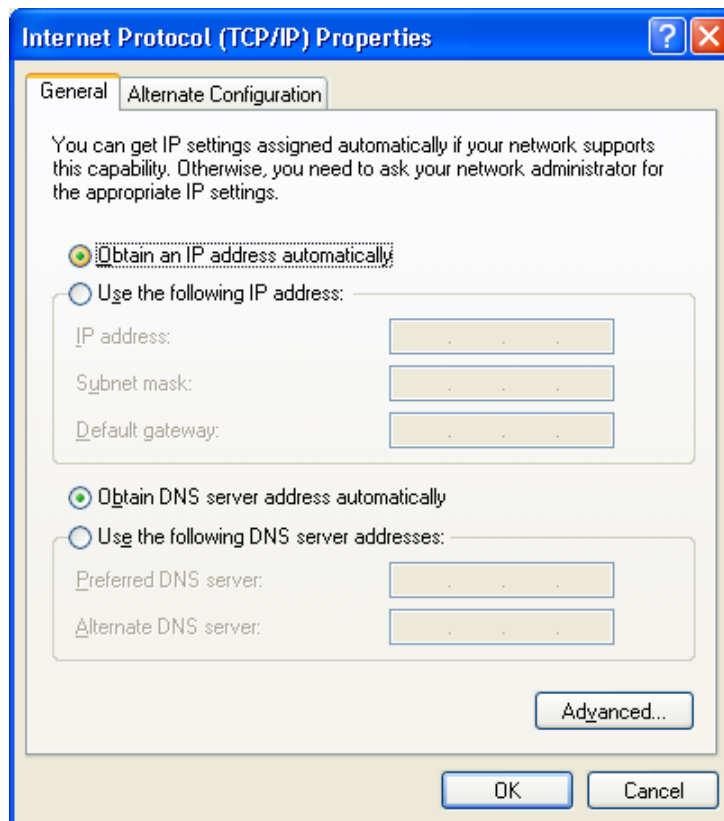
- Enter the IP-2000VPN's IP address in the **Default Gateway** field and click **OK**. (Your LAN administrator can advise you of the IP Address they assigned to the IP-2000VPN).
- If the **DNS Server** fields are empty, select **Use the following DNS server addresses**, and enter the DNS address or addresses 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:



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.



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, and it is recommended to use it. By default, the IP-2000VPN will act as a DHCP Server.

Restart your PC to ensure it obtains an IP Address from the IP-2000VPN.

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 IP-2000VPN's IP address and click **OK**. Your LAN administrator can advise you of the IP Address they assigned to the IP-2000VPN.
- 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**.

Macintosh Clients

From your Macintosh, you can access the Internet via the IP-2000VPN. 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.



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

- Set the *Router Address* field to the IP-2000VPN's IP Address.
- Ensure your DNS settings are correct.

Linux Clients

To access the Internet via the IP-2000VPN, it is only necessary to set the IP-2000VPN 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 IP-2000VPN.
- 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 IP-2000VPN:

- Ensure the "Gateway" field for your network card is set to the IP Address of the IP-2000VPN.
- Ensure your DNS (Name Server) settings are correct.

Appendix B VPN Overview

This section describes the VPN (Virtual Private Network) support provided by your IP-2000VPN.

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 IP-2000VPN 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 SAs 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 IP-2000VPN 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 is in the clear (i.e. not protected). This system provides enhanced security. **The IP-2000VPN 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 identification 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**.

Note that different vendors use different terms. Generally, the terms "VPN Policy", "IPSec Policy", and "IPSec Proposal" have the same meaning. However, some vendors separate IKE Policies (Phase 1 parameters) from IPSec Policies (Phase 2 parameters).

For the IP-2000VPN, each VPN policy contains both Phase 1 and Phase 2 parameters (if IKE is used). 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. However, you should only Enable one (1) policy at a time. If multiple policies for the same remote site are enabled, the policies are examined in the order in which they are listed, and the first matching policy will be used. While it is possible to change the order of the policies, it may not be easy to get the desired action from multiple policies.

VPN Configuration

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

VPN Endpoint address	Each VPN endpoint must be configured to initiate or accept connections to the remote VPN client or Gateway. Usually, this requires having a fixed Internet IP address or domain name. 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.
Traffic Selector	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. If connecting 2 LANs, this requires that: <ul style="list-style-type: none">• Each endpoint must be aware of the IP addresses used on the other endpoint.• The 2 LANs MUST use different IP address ranges.
IKE parameters	If using IKE (recommended), the IKE parameters must match (except for the SA lifetime, which can be different).

IPSec parameters	The IPSec parameters at each endpoint must match.
-------------------------	---

Appendix C Troubleshooting

Overview

This chapter covers some common problems that may be encountered while using the IP-2000VPN and some possible solutions to them. If you follow the suggested steps and the IP-2000VPN still does not function properly, contact your dealer for further advice.

General Problems

Problem 1:	Can't connect to the IP-2000VPN to configure it.
Solution 1:	<p>Check the following:</p> <ul style="list-style-type: none">• The IP-2000VPN is properly installed, LAN connections are OK, and it is powered ON.• Ensure that your PC and the IP-2000VPN 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 192.168.1.2 to 192.168.1.254 and thus compatible with the IP-2000VPN's default IP Address of 192.168.1.1. <p>Also, the Network Mask should be set to 255.255.255.0 to match the IP-2000VPN.</p> <p>In Windows, you can check these settings by using Control Panel-Network to check the Properties for the TCP/IP protocol.</p>

Internet Access

Problem 1:	When I enter a URL or IP address I get a time out error.
Solution 1:	<p>A number of things could be causing this. Try the following troubleshooting steps.</p> <ul style="list-style-type: none">• 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 IP-2000VPN. 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 IP-2000VPN 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 IP-2000VPN.
Solution 2:	<p>The IP-2000VPN processes the data passing through it, so it is not transparent.</p> <p>Use the Special Applications feature to allow the use of Internet applications which do not function correctly.</p> <p>If this does solve the problem you can use the DMZ function. This should work with almost every application, but:</p> <ul style="list-style-type: none">• It is a security risk, since the firewall is disabled.• Only one (1) PC can use this feature.

Appendix D Specifications

Model	IP-2000VPN
Dimensions	141mm(W) * 100mm(D) * 27mm(H)
Operating Temperature	0° C to 40° C
Storage Temperature	-10° C to 70° C
Network Protocol:	TCP/IP
Network Interface:	5 Ethernet: 3 * 10/100BaseT (RJ45) LAN connection 1 * 10/100BaseT (RJ45) DMZ connection 1 * 10/100BaseT (RJ45) for WAN
LEDs	11
Power Adapter	12 V DC External