

# NB3100 Cable/DSL Firewall Router

## CONNECT YOUR CABLE OR DSL MODEM TO A NETWORK & PROTECT IT FROM HACKERS

- Advanced Firewall with Stateful Packet Inspection for superior security
- Prevent hackers launching Denial of Service attacks
- NAT firewall protects against intruders
- Can block sites, java, ActiveX & Cookies
- 4-port 10/100 switch for building or expanding your network
- Router to share your Cable or DSL Internet connection with up to 253 users
- Works with all Cable and DSL service providers
- Built-in DHCP server
- Supports VPN, IPSec & PPTP pass-thru
- Remote Administration via the Internet
- Easy to install: compatible with PC, Mac, Linux and any TCP/IP system



**Cable  
& DSL  
ready**  
SUPPORTS 2  
VPN TUNNELS

## Quick Start Guide

## Contents

|   |    |
|---|----|
| Default Settings & Facts .....  | 3  |
| NetComm Cable/DSL Firewall Router Quick Start .....                     | 4  |
| One page setup for Telstra Bigpond Cable .....                          | 4  |
| One page setup for Optus Cable .....                                    | 5  |
| One page setup for most ADSL services .....                             | 6  |
| Introduction .....  | 7  |
| Chapter 1: Getting to know your NetComm Cable/DSL Firewall Router ..... | 9  |
| 1-1 About NetComm Cable/DSL Firewall Router .....                       | 9  |
| 1-2 Contents of the NetComm Cable/DSL Firewall Router Package .....     | 10 |
| 1-3 Features of the NetComm Cable/DSL Firewall Router .....             | 10 |
| Chapter 2: Hardware Installation & Setup .....                          | 11 |
| 2-1 Rear Panel & Connections .....                                      | 11 |
| 2-2 Front Panel LEDs .....  | 12 |
| 2-3 System Requirements and Setup .....                                 | 13 |
| Chapter 3: Internet Access .....  | 18 |
| 3-1 Prepare your network information .....                              | 18 |
| 3-2 Web-based User Interface .....                                      | 19 |
| 3-3 Initial Configuration – Setup .....                                 | 20 |
| Chapter 4: Advanced Applications .....                                  | 23 |
| 4-1 Firewall .....  | 23 |
| 4-2 DHCP Configuration .....  | 24 |
| 4-3 Access Control .....  | 25 |
| 4-4 Port Forwarding Settings .....                                      | 27 |
| 4-5 Special Application .....   | 28 |
| 4-6 Dynamic Routing .....   | 29 |
| 4-7 Static Routing .....  | 30 |
| 4-8 Administration Settings .....                                       | 31 |
| 4-9 Status Monitor .....  | 32 |
| 4-10 DMZ Host .....   | 33 |
| 4-11 Log .....  | 33 |
| 4-12 VPN Passthrough .....  | 34 |
| Chapter 5: Configuring IPSec on Windows 2000/XP .....                   | 35 |
| 5-1 Environment .....   | 35 |
| 5-2 Steps in Windows 2000/XP .....                                      | 35 |
| 5-3 Steps in Cable/DSL Firewall Router .....                            | 47 |
| Chapter 6: Macintosh Setup .....  | 49 |
| 6-1 Hardware Connections .....  | 49 |
| 6-2 Computer Network Configuration .....                                | 49 |
| 6-3 NetComm Cable/DSL Firewall Router Configuration .....               | 50 |
| 6-4 Adding NetComm Cable/DSL Firewall Router to Existing Network .....  | 50 |
| Chapter 7: Trouble Shooting .....                                       | 51 |
| Hardware .....  | 51 |
| Client Side (Computers) .....   | 52 |
| Appendix A: Frequently Asked Questions .....                            | 53 |
| Appendix B: Technical Specifications .....                              | 54 |
| Appendix C: Glossary .....  | 55 |
| Appendix D: Registering your NetComm Product .....                      | 58 |
| Contact Information .....   | 58 |
| Trademarks and Notices .....  | 58 |
| Product Warranty .....  | 59 |
| Limitations of Warranty .....   | 59 |

---

## Default Settings & Facts

The following lists the default settings of your NetComm Cable/DSL Firewall Router.

**Note:** *It is highly recommended that you enable security settings in the router before connecting your router to your network.*

### Router

|               |   |
|---------------|---|
| LAN IP:       | 192.168.1.1                             |
| Username:     | <none>                                  |
| Password:     | admin                                   |
| WAN port MDI: | Auto MDI (No cross over cable required) |

## Resetting

While using or installing your NetComm Cable/DSL Firewall Router you may need to utilise the reset feature. There are two types of reset:

### Soft

A soft reset will restart the unit and reconnect to the internet using the settings stored previously, none of your settings are deleted. To perform a soft reset briefly press the reset button on the back of the unit.

### Hard

A hard reset will return your unit to its factory default setting, meaning that you will lose all configurations and logs set/stored previously. To perform a hard reset, press and hold in the reset button on the back of the unit for 10 seconds.

## Power

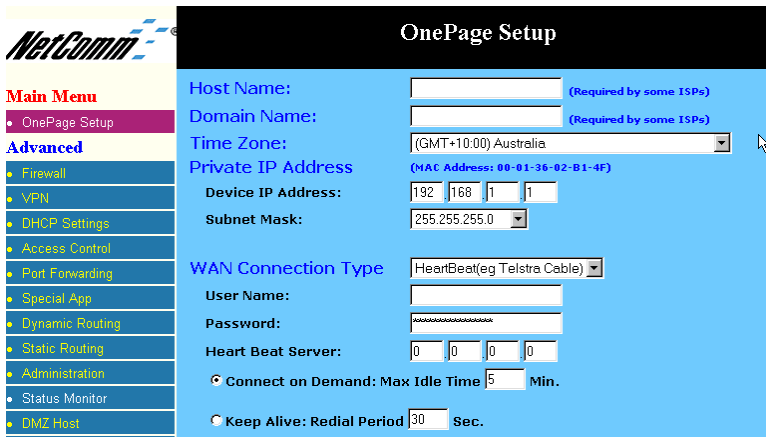
Ensure that you only use the Power Adaptor supplied (5V DC, 3amps, Center pole positive) with your NetComm Cable/DSL Firewall Router.

## NetComm Cable/DSL Firewall Router Quick Start

The following Quick Start pages are intended to be used by an advanced user to quickly configure the NetComm Cable/DSL Firewall Router. It assumes that you are familiar with *Networking* and that you already have a Cable or ADSL modem with an Ethernet port. If you need further explanation, please refer to the more detailed sections of this document. This guide presumes that your NetComm Cable/DSL Firewall Router is set to factory defaults (See *Resetting* on previous page if required).

### One page setup for Telstra Bigpond Cable

1. Connect your computer to one of the four LAN ports on the NetComm Cable/DSL Firewall Router and ensure you have a link. Connect your Cable modem (supplied by your ISP) to the WAN port of the NetComm Cable/DSL Firewall Router.
2. Set the Network Card of your computer to use DHCP or assign it an IP address in the range of 192.168.1.2 ~ 254.
3. Open a web browser (ensuring that it is set to access the Internet via the LAN, not by a dial-up networking account). Browse to the NetComm Cable/DSL Firewall Router's default IP (192.168.1.1). The main menu of the router should open displaying the **“One Page Setup”**.



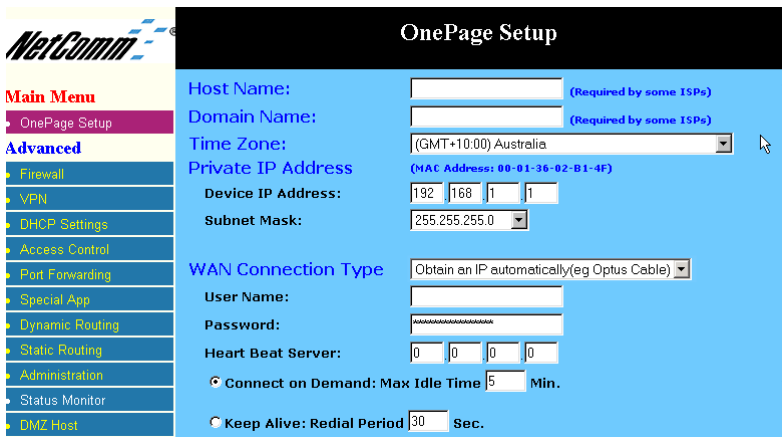
**Note:** You may be prompted for a log-in, there is no User Name and the Password is **“admin”**.

4. Change your **“WAN Connection Type”** to **“Heartbeat (E.g. Telstra cable)”**.
5. Set your **“User Name”** and **“Password”** as provided by your ISP.
6. If you wish to make services available to external Internet users, even when you are not using Internet services from inside your network, you can choose **“Keep Alive”**. Alternatively for extra security you can choose **“Connect on Demand”**.
7. Click **“Apply”**. Your NetComm Cable/DSL Firewall Router will attempt to use your settings to connect to your ISP. You can check the results on the **“Status Monitor”** page.

- If you have a DHCP server already active on your network it is recommended that you disable either the NetComm Cable/DSL Firewall Router's built in DHCP server or the existing DHCP server. Please note that *Microsoft Internet Connection Sharing* is a DHCP server.

## One page setup for Optus Cable

- Connect your computer to one of the four LAN ports on the NetComm Cable/DSL Firewall Router and ensure you have a link. Connect your Cable modem (supplied by your ISP) to the WAN port of the NetComm Cable/DSL Firewall Router.
- Set the Network Card of your computer to use DHCP or assign it an IP address in the range of 192.168.1.2 ~ 254.
- Open a web browser (ensuring that it is set to access the Internet via the LAN, not by a dial-up networking account). Browse to the NetComm Cable/DSL Firewall Router's default IP (192.168.1.1). The main menu of the router should open displaying the **“One Page Setup”**.

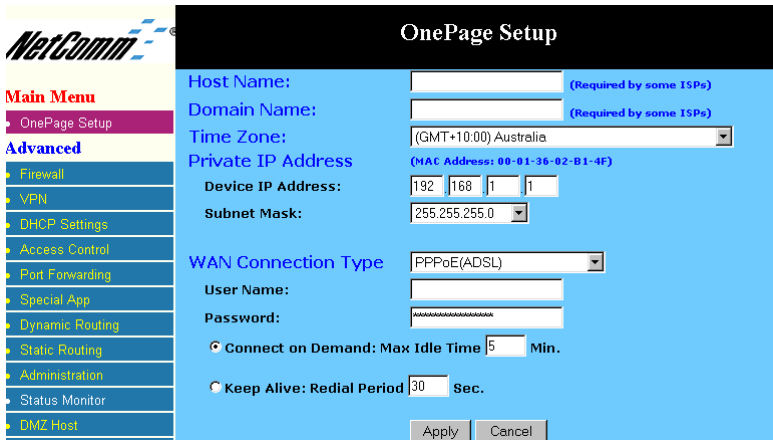


**Note:** You may be prompted for a log-in, there is no User Name and the Password is **“admin”**.

- Change your **“WAN Connection Type”** to **“Obtain an IP automatically (E.g. Optus cable)”**.
- Optus cable does not require a **“User Name”** and **“Password”** as it uses the modem's MAC address to identify you to your ISP.
- If you wish to make services available to external Internet users, even when you are not using Internet services from inside your network, you can choose **“Keep Alive”**. Alternatively for extra security you can choose **“Connect on Demand”**.
- Click **“Apply”**. Your NetComm Cable/DSL Firewall Router will attempt to use your settings to connect to your ISP. You can check the results on the **“Status Monitor”** page.
- If you have a DHCP server already active on your network it is recommended that you disable either the NetComm Cable/DSL Firewall Router's built in DHCP server or the existing DHCP server. Please note that *Microsoft Internet Connection Sharing* is a DHCP server.

## One page setup for most ADSL services.

1. Connect your computer to one of the four LAN ports on the NetComm Cable/DSL Firewall Router and ensure you have a link. Connect your ADSL modem (supplied by your ISP) to the WAN port of the NetComm Cable/DSL Firewall Router.
2. Set the Network Card of your computer to use DHCP or assign it an IP address in the range of 192.168.1.2 ~ 254.
3. Open a web browser (ensuring that it is set to access the Internet via the LAN, not by a dial-up networking account). Browse to the NetComm Cable/DSL Firewall Router's default IP (192.168.1.1). The main menu of the router should open displaying the “One Page Setup”.



**Note:** You may be prompted for a log-in, there is no User Name and the Password is “admin”.

4. Change your “WAN Connection Type” to “PPPoE (ADSL)”.
5. Set your “User Name” and “Password” as provided by your ISP.
6. If you wish to make services available to external Internet users, even when you are not using Internet services from inside your network, you can choose “Keep Alive”. Alternatively for extra security you can choose “Connect on Demand”.
7. Click “Apply”. Your NetComm Cable/DSL Firewall Router will attempt to use your settings to connect to your ISP. You can check the results on the “Status Monitor” page.
8. If you have a DHCP server already active on your network it is recommended that you disable either the NetComm Cable/DSL Firewall Router's built in DHCP server or the existing DHCP server. Please note that *Microsoft Internet Connection Sharing* is a DHCP server.

---

## Introduction

Congratulations on your purchase of the NetComm Cable/DSL Firewall Router. The NetComm Cable/DSL Firewall Router is designed to provide advanced networking security and network resource sharing, utilising fast Ethernet connections with four built-in 10/100 auto-sensing switched Ethernet ports. And best of all, with a powerful firewall engine, this device is able to prevent DoS attack and uses SPI to provide superior protection for your private network from Internet hackers.

The built-in NAT provides a natural Internet firewall, protecting your network from unauthorised access by outside users. The router will share your internet connection with up to 253 users, 25 of which can be connected via NetComm Wireless Client Adaptors (NP7030 and NP7040). Configured as a DHCP server, the NetComm Cable/DSL Firewall Router assigns an IP Address to every computer connected on the LAN automatically. Also, a DHCP client helps the WAN port to acquire an IP address dynamically from your ISP.

Unlike other typical routers, which only share 10Mbps over all of their connections, the NetComm Cable/DSL Firewall Router is equipped with a 4-port 10M/100Mbps auto-sensing switch, dedicating a possible 100Mbps to each and every ethernet connected computer.

With a web-based UI (User Interface), this NetComm Cable/DSL Firewall Router is easy to setup and maintain via web browsers such as Netscape Communicator and Internet Explorer.



---

## About this Guide

This guide contains information about installing and configuring your NetComm Cable/DSL Firewall Router. It is designed to guide users through the correct setup procedures for both hardware installation and basic configuration. Later, it shows how to complete advanced configuration to get the best operating performance from the NetComm Cable/DSL Firewall Router.

### Chapter 1: Get to know your NetComm Cable/DSL Firewall Router

This chapter describes the package contents and provides a list of features of the NetComm Cable/DSL Firewall Router.

### Chapter 2: Hardware Installation & Setup

This chapter describes the steps for hardware installation of the NetComm Cable/DSL Firewall Router.

### Chapter 3: Internet Access

This chapter describes the steps for basic configuration and start up of the NetComm Cable/DSL Firewall Router.

### Chapter 4: Advanced Applications

This chapter describes how to configure advanced functions in order to get the most from your NetComm Cable/DSL Firewall Router.

### Chapter 5: Macintosh Setup

This Chapter provides instructions on how to set up Macintosh computers in your network.

### Chapter 6: Trouble Shooting

This chapter describes potential problems you may run into and the suggested remedies.

## Conventions

The following explains the conventions used throughout this document.

*Italics*

New words, terms, or special emphasis. E.g. *Getting to know your NetComm Cable/DSL Firewall Router.*

**“Boldface”**

Buttons, checkboxes, or items that you can select from screens, menus, or dialog boxes. E.g. Click **“OK”** to restart

***Boldface Italics***

Items in ***Bold Italics*** are samples only and you should enter other names, numbers, or words to substitute.



---

## Chapter 1: Getting to know your NetComm Cable/DSL Firewall Router

This chapter describes the package contents and provides a list of features of the NetComm Cable/DSL Firewall Router.

### 1-1 About NetComm Cable/DSL Firewall Router

The *NetComm Cable/DSL Firewall Router* is a hybrid product, which combines Ethernet technology with a firewall engine into a single stand-alone unit. The device allows you take advantage of both security and fast connections. All computers on your LAN can securely share files, printers and other network resources, as well as a single Internet account when connected to a DSL/Cable modem.

#### Ethernet / Fast Ethernet

*Ethernet* is the most widely-used network access method, especially in LANs. It is defined by the IEEE as 802.3 standard. Normally, Ethernet is a shared media LAN. All stations on the segment share the total bandwidth, which could be 10Mbps (Ethernet), 100Mbps (Fast Ethernet), or 1000Mbps (Gigabit Ethernet). With switched Ethernet, each sender and receiver has the full bandwidth.

*Fast Ethernet* is defined as IEEE 802.3u standard, a high-speed version of Ethernet with 100Mbps transmission rate.

#### Firewall

*DoS* is the acronym for Denial of Service, which refers to the response when a computer or network is overwhelmed to the point that it can no longer function normally. For example, a hacker may use a fake IP address to build connections to flood the server they want to attack. TCP works by sending a SYN packet to the server from the client. After the server receives the SYN packet, a SYN-ACK is sent back to client. The server will then wait for a response to the SYN-ACK. If the hacker sends hundreds of SYN packets to a server with a false address, the server allocates computer and memory resources to establishing a connection - since the server does not know a legitimate SYN message from a false message. By flooding the server with such a large volume of requests, the server's maximum capacity can easily be used by these false attempts to establish a connection - this is what the firewall is designed to prevent.

*SPI* is the acronym of Stateful Packet Inspection. The SPI engine examines not just the headers of the packet, but also the contents, to determine more about the packet than just its source and destination information. Moreover, stateful inspection firewalls also close off ports until a connection to the specific port is requested.

---

## 1-2 Contents of the NetComm Cable/DSL Firewall Router Package

After carefully unpacking the shipping carton, check the contents listed below:

- NetComm Cable/DSL Firewall Router
- Power Adapter - 5VDC 3A Center Pole Positive
- This Manual

## 1-3 Features of the NetComm Cable/DSL Firewall Router

Your NetComm Cable/DSL Firewall Router contains the following features that make it excellent for network connections.

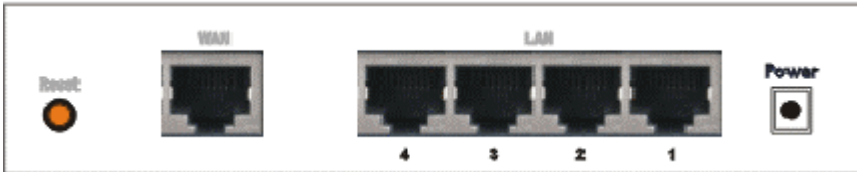
- Allows multiple users to access the Internet at the same time by using Network Address Translation to safely share a single public IP Address.
- Provides network security through a powerful firewall engine.
- Prevents hackers from launching a DoS attack to overwhelm your LAN computers or server, offering advanced protection with SPI.
- Blocks inappropriate web sites, cookies and Javascript, if required.
- Integrates four 10/100BASE-T/TX auto-sensing switch ports.
- Supports PPPoE to connect to ISPs.
- Built-in web-based user interface for easy configuration and management through common web browsers like Netscape or Internet Explorer.
- Supports DHCP client to receive both a dynamic IP Address and a fixed IP Address from your ISP/WAN.
- Built-in DHCP server to automatically assign and manage LAN IP addresses.
- Allows administrators to block specific LAN users from accessing specified applications or services.
- Allows external Internet users to access information from an internal computer (Virtual Server).
- Provides unrestricted two-way communication between one computer on your LAN and certain Internet services like conferencing, video and gaming applications.
- Enhances routing performance by using Dynamic or Static routing.
- Allows administrators to change WAN MAC address.
- Compatible with all popular Internet applications.

## Chapter 2: Hardware Installation & Setup

This chapter provides information about your NetComm Cable/DSL Firewall Router's physical features and gives step-by-step installation instructions.

### 2-1 Rear Panel & Connections

The following figure shows the rear view of the NetComm Cable/DSL Firewall Router and illustrates how the cables connect to the interfaces on the rear panel.



- Plug one end of the UTP cable into the WAN port, the other into the RJ45 Ethernet jack on your ADSL or Cable modem.
- Connect a computer, with a Network Interface Card installed, to one of the four LAN Ports.
- Connect the external power supply to the NetComm Cable/DSL Firewall Router.
- The Reset button is used to reboot the device - press once quickly, or for clearing configuration settings back to factory default values - press for 10 seconds.

## 2-2 Front Panel LEDs

The following figure shows the front view of the NetComm Cable/DSL Firewall Router.



The LEDs on the front panel indicate the status of the unit.

|               |       |  |
|---------------|-------|--|
| <b>Power:</b> | Green | On when power is on.   |
| <b>Diag:</b>  | Red   | Lights up during system check when the power is initially connected. If the Router is working properly, the light should switch off after the diagnostic has been completed. |

### WAN ports

|           |              |  |
|-----------|--------------|--|
| Link/Act: | Green        | On when ADSL/Cable Modem is properly connected and is operating at 100Mbps.  |
|           | Yellow       | On when ADSL/Cable Modem is properly connected and is operating at 10Mbps.   |
|           | Green/Yellow | Blinking when data is flowing through the LAN port.  |
| FD/Col:   | Green        | On when operating in full duplex mode.<br>Off in half duplex mode.<br>Blinking when a collision has occurred on this port. |

### LAN ports

|           |              |  |
|-----------|--------------|--|
| Link/Act: | Green        | On when link is up and is operating at 100Mbps.  |
|           | Yellow       | On when link is up and is operating at 10Mbps.   |
|           | Green/Yellow | Blinking when data is flowing through this LAN port.   |
| FD/Col:   | Green        | On when operating in full duplex mode.<br>Off in half duplex mode.<br>Blinking when a collision is occurring on this port. |

## 2-3 System Requirements and Setup

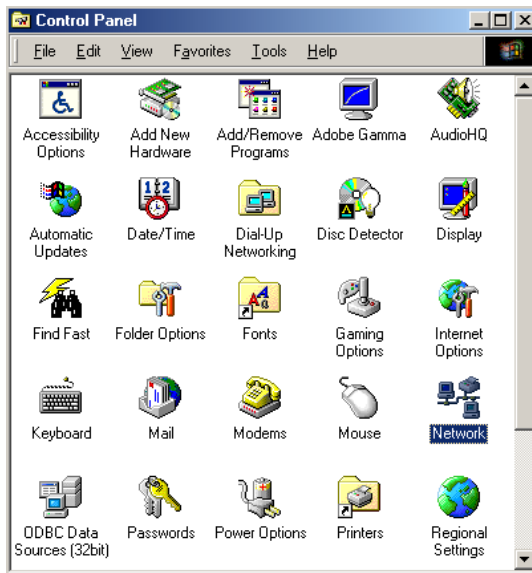
To connect to the Internet, an external ADSL or Cable modem and an Internet access account from an ISP are required. In order to operate with the Broadband Switch Router, each computer that is to be connected to the Broadband Switch Router should have the following items installed:

1. Ethernet NIC (Network Interface Card: a 10Base-T or 10/100Base-T/TX Ethernet card).
2. Standard twisted-pair Ethernet cable (UTP network cable) with RJ-45 connectors.
3. System OS: Windows 95, Windows 98, Windows NT4.0, Windows 2000, Windows Me, Windows XP or Macintosh (refer to Chapter 5).
4. TCP/IP network protocol.
5. Web browser, such as Microsoft Internet Explorer or Netscape Navigator.

### Installing the TCP/IP Protocol for Windows

If you are not sure whether the TCP/IP Protocol has been installed, follow these steps to check, and if necessary, install TCP/IP onto your computer.

1. Click the **“Start”** button. Choose **“Settings”**, then **“Control Panel”**.

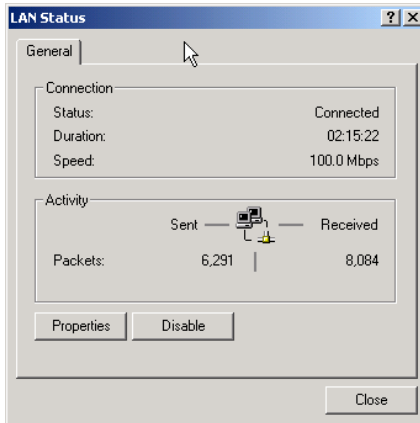


Double-click the **“Network”** icon. Your Network window should appear.  
Select the **“Configuration”** tab.

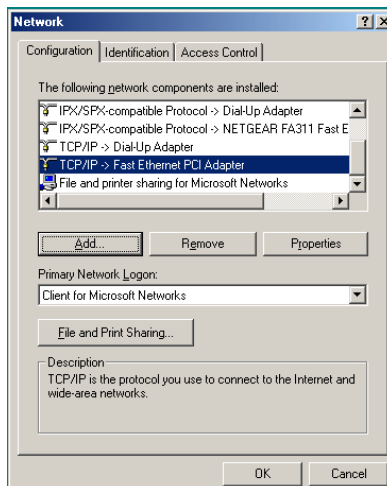
**Note:** For Windows 2000 & Windows XP the settings can be reached by clicking the “Local Area Connection” icon on the right bottom side of your desktop screen.



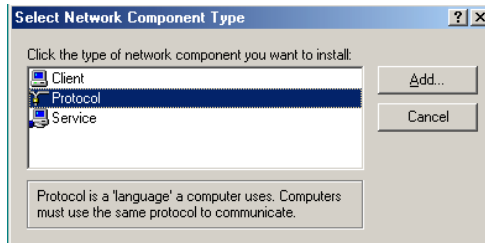
**In the “Local Area Connection Status” window, click “Properties” button then your Network window will appear.**



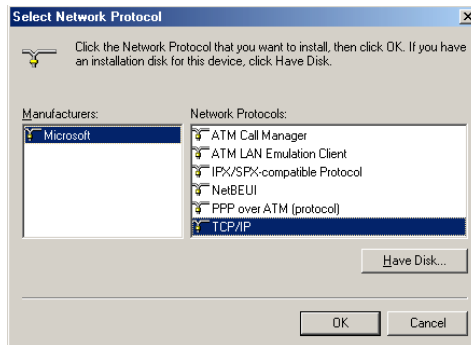
2. Check whether the TCP/IP Protocol has already been installed and bound to your Network Interface Card.



- If yes, go to step 6.
  - If no, click the “Add” button.
3. Double-click “**Protocol**” on the Select Network Component Type or highlight “**Protocol**” then click “**Add**”.



4. Highlight “**Microsoft**” under the list of manufacturers.

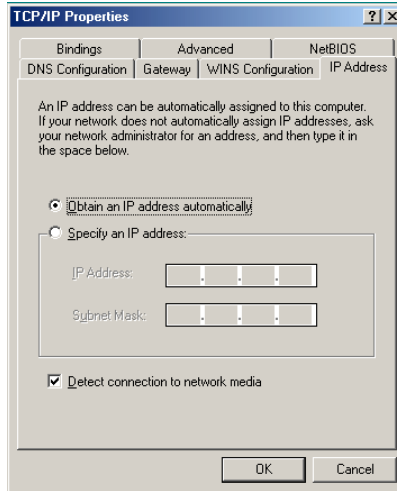


Double-click “**TCP/IP**” from the list on the right or highlight “**TCP/IP**” then click “**OK**” to install TCP/IP.

5. After a few seconds, you will be brought back to the Network window. The TCP/IP Protocol should now be on the list of installed network components (refer to point 2).
6. Click the “**Properties**” button.

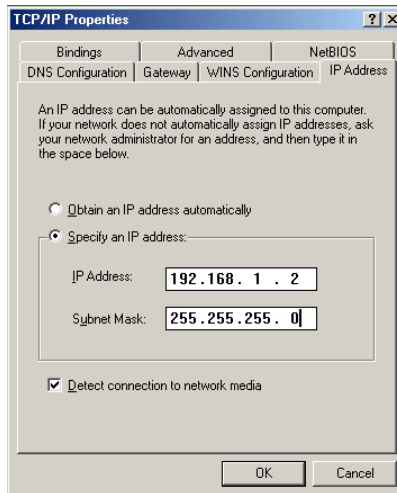


The TCP/IP Properties window consists of several tabs. Choose the “**IP Address**” tab.



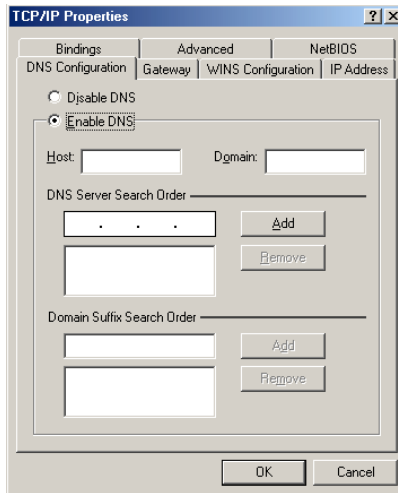
7. Select “**Obtain an IP address automatically**”. Click “**OK**”. Restart your computer to complete the TCP/IP installation.

## Fixed IP Addresses Configuration



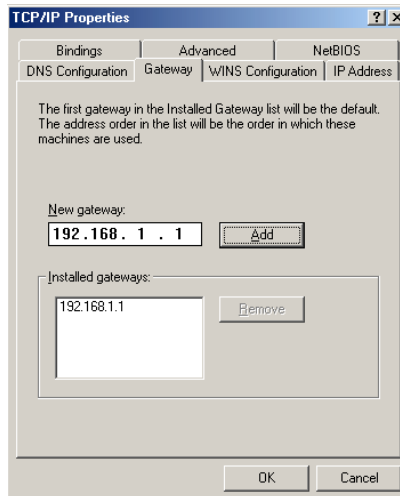
Fixed IP addresses may be assigned to network devices for many reasons, such as the server computers or printers which are consistently accessed by multiple users. To set up computers with fixed IP Addresses, go to the “**IP Address**” tab of the “**TCP/IP Properties**” window as shown above.

1. Select **“Specify an IP address”** and enter **“192.168.1.\*\*\*”** in the **“IP Address”** location (where \*\*\* is a number between 2 and 254 used by the NetComm Cable/DSL Firewall Router to identify each computer), and the default **“Subnet Mask”** **“255.255.255.0”**.



**Note:** *No two computers on the same LAN can have the same IP address but they should have the same Subnet Mask.*

2. Select **“Enable DNS”** in the **“DNS Configuration”** tab and enter the **“DNS IP Address”** obtained from your ISP in the **“Server Search Order”** location. Click **“OK”**.



3. Click **“Gateway”** tab and enter the NetComm Cable/DSL Firewall Router’s default gateway value **192.168.1.1** in the **“New gateway”** field, then click **“Add”** Button. Click **“OK”**. Restart your computer to complete the TCP/IP installation.

## Chapter 3: Internet Access

This chapter describes the procedures necessary to configure the basic functions and to start up your NetComm Cable/DSL Firewall Router. On successful completion of these procedures, you will be able to access the Internet via your NetComm Cable/DSL Firewall Router.

### 3-1 Prepare your network information

In order to allow a quick reference point when setting up your NetComm Cable/DSL Firewall Router, it is suggested you complete the table below with the necessary information, which should be supplied by your ISP:

**Provided by some ISPs** (  tick indicates common minimal requirements)

Host Name: \_\_\_\_\_

Domain Name: \_\_\_\_\_

**IP address given by ISP:**

Obtain IP Address automatically, or

Static IP

IP Address (if static): \_\_\_\_\_ . \_\_\_\_\_ . \_\_\_\_\_ . \_\_\_\_\_

Subnet Mask: \_\_\_\_\_ . \_\_\_\_\_ . \_\_\_\_\_ . \_\_\_\_\_

Default Gateway: \_\_\_\_\_ . \_\_\_\_\_ . \_\_\_\_\_ . \_\_\_\_\_

DNS Server Primary: \_\_\_\_\_ . \_\_\_\_\_ . \_\_\_\_\_ . \_\_\_\_\_

DNS Server Secondary (optional): \_\_\_\_\_ . \_\_\_\_\_ . \_\_\_\_\_ . \_\_\_\_\_

DNS Server Third (optional): \_\_\_\_\_ . \_\_\_\_\_ . \_\_\_\_\_ . \_\_\_\_\_

**PPP authentication:**

PPPoE

PPTP

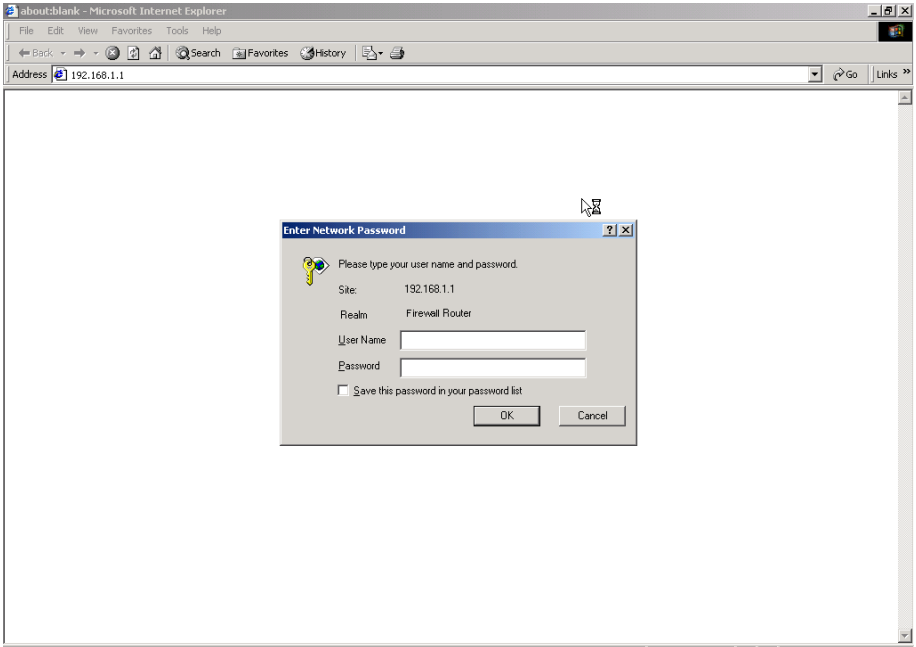
User Name: \_\_\_\_\_

Password: \_\_\_\_\_

## 3-2 Web-based User Interface

The NetComm Cable/DSL Firewall Router uses a Web-based User Interface for configuration. Start your web browser and type `http://192.168.1.1` in the browser's *address box*. This address is the factory default IP Address of your NetComm Cable/DSL Firewall Router. Press “**Enter**”.


The “**Username and Password Required**” prompt box will appear. Leave the “**User Name**” empty and type “**admin**” (default password) for the “**Password**”. Click “**OK**”. The setup screen will load.



**Note:** *The password can be reset by restoring the factory defaults with the Reset button.*

## 3-3 Initial Configuration – Setup

The “**OnePage Setup**” screen is the first screen you will see when you access the router’s configuration. If the router has already been successfully installed and set up, this screen’s values will already be properly configured. Below is a description of each setting.



- **Host Name** This entry is required by certain ISPs.
- **Domain Name** This entry is required by certain ISPs.
- **Time Zone:** Select the time zone your location belong to from the pop-down list.
- **Private IP Address** The Device IP Address and Subnet Mask of the router are used by the internal LAN. The default values are 192.168.1.1 for IP Address and 255.255.255.0 for Subnet Mask.

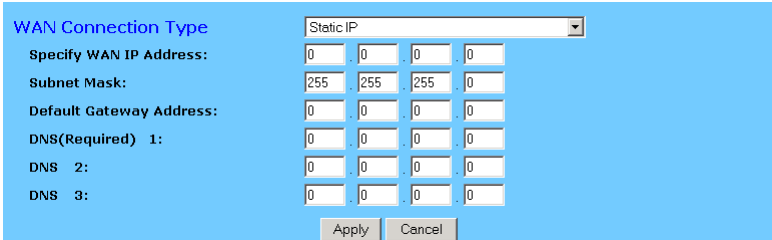
### WAN Connection Type

There are a number of options for WAN connection types: **Obtain IP automatically** (eg Optus Cable), **Static IP**, **PPPoE** (ADSL), **HeartBeat** (eg Telstra Cable) and **PPTP**. If you do not know which connection type you currently use, contact your ISP to get the information.

**Obtain IP automatically** is the default option for the router. If your ISP automatically assigns the IP addresses and other values to the NetComm Cable/DSL Firewall Router, use this option.

## Static IP

The Public IP Address and Subnet Mask of the router are used by external users of the Internet (including your ISP). If a fixed Public IP Address from your ISP is to be used, select this item and enter the IP Address and Subnet Mask provided by your ISP.

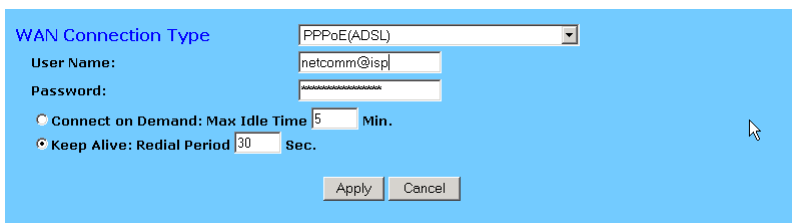


The screenshot shows the 'WAN Connection Type' configuration window. The 'Static IP' option is selected in the dropdown menu. Below the menu, there are input fields for 'Specify WAN IP Address', 'Subnet Mask', 'Default Gateway Address', and three 'DNS' entries. Each field is a four-digit grid. The IP address fields are all set to '0'. The Subnet Mask fields are set to '255', '255', '255', and '0'. The Default Gateway Address fields are all set to '0'. The DNS fields are all set to '0'. At the bottom, there are 'Apply' and 'Cancel' buttons.

- **Specify WAN IP Address** Enter the IP address provided by your ISP.
- **Subnet Mask** Enter the subnet mask values provided by your ISP.
- **Default Gateway IP Address** Your ISP will provide you with the Default Gateway IP Address.
- **Domain Name Server (DNS)** Your ISP will provide you with at least one DNS IP Address. Multiple DNS IP settings are common. The first available DNS entry is used in most cases.

## PPPoE

If your ISP provides PPPoE connectivity, choose this item from the drop-down list.



The screenshot shows the 'WAN Connection Type' configuration window with 'PPPoE(ADSL)' selected in the dropdown menu. Below the menu, there are input fields for 'User Name' (containing 'netcomm@isp') and 'Password' (masked with asterisks). There are two radio button options: 'Connect on Demand: Max Idle Time' (set to 5 Min) and 'Keep Alive: Redial Period' (set to 30 Sec). At the bottom, there are 'Apply' and 'Cancel' buttons.

**Note:** If you select PPPoE, you will no longer need to use any existing PPPoE applications on any computers to connect to the Internet.

- **User Name** Enter the user name as provided by your ISP.
- **Password** Enter the password as provided by your ISP.
- **Connect-on-demand** Is a utility to trigger the PPPoE session to connect if in a disconnected state when Internet access is being attempted. Choose “**Enable**” to make this function active, and enter the number of minutes you wish to wait after network idle time in the “**Max Idle Time**” location. This function is for PPPoE only.

- **Keep Alive** This function keeps your PPPoE connection always on even during a period of no WAN activity. In some situations the PPPoE session cannot be restored immediately after disconnection because the ISP's system may need time to restore. Check with your ISP to ascertain how much time is required before the router starts to re-build the PPPoE session and enter this into the "**Redial Period**" field.

When you have properly configured the Setup page, click "**Apply**". Your Router will then attempt to connect to the Internet. If you experience problems, please refer to the Trouble Shooting section before contacting NetComm Technical Support.

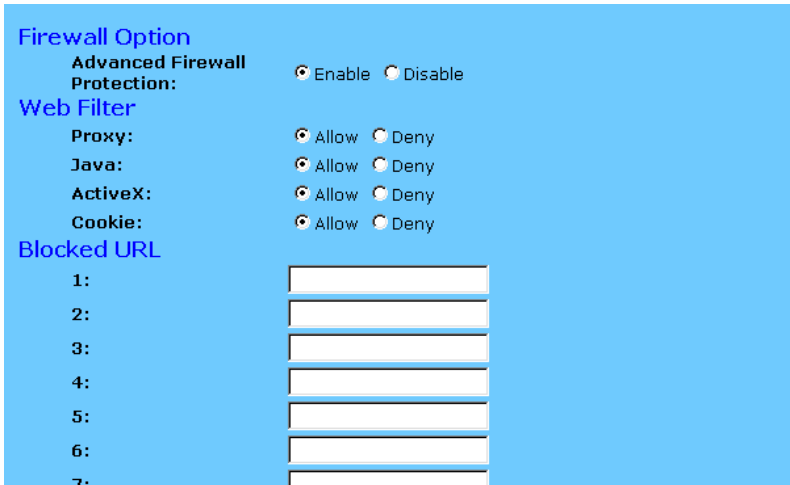


## Chapter 4: Advanced Applications

This chapter provides information on how to set up and use the advanced features of your NetComm Cable/DSL Firewall Router.

### 4-1 Firewall

The Firewall setting page allows you to configure advanced Firewall functions to provide superior security for your network environment. You must click “**Apply**” to make any changes active.



**Firewall Option**

**Advanced Firewall Protection:**  Enable  Disable

**Web Filter**

**Proxy:**  Allow  Deny

**Java:**  Allow  Deny

**ActiveX:**  Allow  Deny

**Cookie:**  Allow  Deny

**Blocked URL**

1:

2:

3:

4:

5:

6:

7:

- **Firewall Option** Enable this function to prevent DoS (Denial of Service) attacks and to use SPI (Stateful Packet Inspection). SPI function will check the contents of incoming data packets for malicious attacks.
- **Web Filter** This feature provides the ability to filter potential risks contained in web pages accessed by LAN users.

**Web proxy** is a server your device will connect to when you access any web site. Setting a web proxy can save accessing time but may create a security issue by bypassing any URL filters or IP blocking you have configured. For example, if you configure the Broadband Firewall Router to block the access of 216.115.102.76 that is the IP address of www.yahoo.com, it will fail because your computer will connect to web proxy server instead to connect to Yahoo’s IP address if you set web proxy.

**Java & Active X** are programming languages for web pages. However, some Trojan programs are also written in these programming languages. If you deny either of these, you may not be able access some parts of web sites.

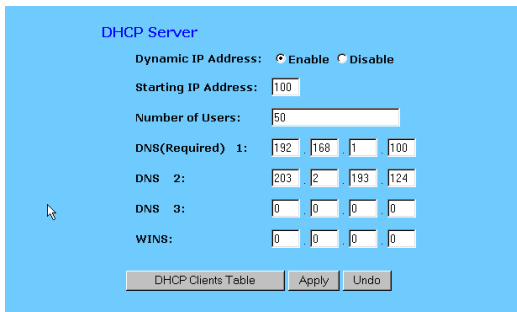
A **cookie** is data stored on your computer, which a web server can retrieve to identify your machine. It is a piece of text with an ID number. Cookies can also be blocked by the router.

- **Blocked URL** This feature allows you to restrict LAN users to access specific web sites. Enter the key text included in the URLs (Internet address) or whole URLs you wish to block in the fields supplied.
- **Time Filter** This feature allows you to limit WAN/Internet access according to a time schedule. Check “**Block LAN**” to restrict the connection from your LAN to the WAN/Internet. Check “**Block WAN**” to restrict the connection from the WAN/Internet to your LAN servers that were set as virtual servers, port forwards or DMZ host. Check “**Block Both**” to restrict both connections. Check “Disable” to turn off this function. Set the time schedule from the drop-down list.

Click Apply after making any changes.

## 4-2 DHCP Configuration

A DHCP (Dynamic Host Configuration Protocol) Server can automatically assign IP Addresses and other information to each computer in your network. Unless you already have a DHCP Service on your LAN, it is highly recommended that you set your router to act as a DHCP server.



**Note:** The DHCP Server can support a maximum pool of 253 IP Addresses.

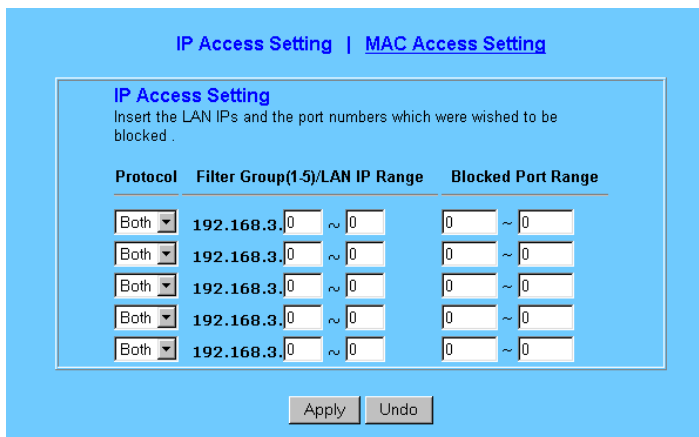
- **Dynamic IP Address** Select “Enable” to set your Router to act as a DHCP server. If you already have a DHCP server on your network, set the router’s DHCP option to “Disable”.
- **Starting IP Address** Enter a numerical value, from 2 to 254, for the DHCP server to start at when assigning IP Addresses.
- **Number of Users** Enter the maximum number of computers that you want the DHCP server to assign IP Addresses to, with the absolute maximum being 253.
- **DNS1, 2, 3** Enter the DNS numbers you wish to be assigned to DHCP clients.
- **WINS** Enter the WINS number you wish to be assigned to DHCP clients.
- **DHCP Clients Table** Click the DHCP Clients Table button to show current DHCP client information.

## 4-3 Access Control

The Access Control feature allows administrators to block certain users from accessing the Internet or specific applications. Before using this function, the network computers that you wish to control should be assigned fixed IP Addresses.

### IP Access Setting

Network administrators can restrict access of up to five groups of specified network users/computers.



[IP Access Setting](#) | [MAC Access Setting](#)

**IP Access Setting**  
Insert the LAN IPs and the port numbers which were wished to be blocked .

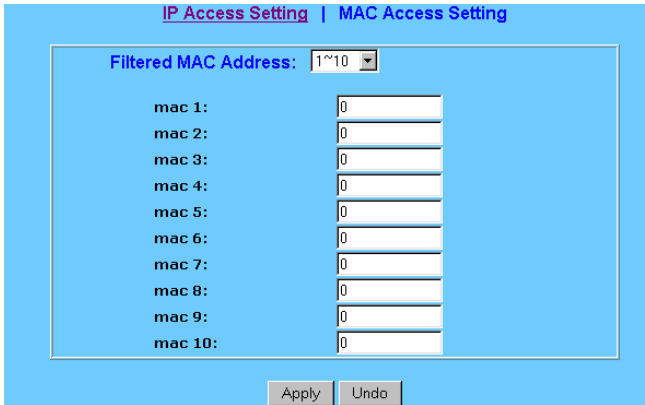
| Protocol | Filter Group(1-5)/LAN IP Range | Blocked Port Range |
|----------|--------------------------------|--------------------|
| Both     | 192.168.3,0 ~ 0                | 0 ~ 0              |
| Both     | 192.168.3,0 ~ 0                | 0 ~ 0              |
| Both     | 192.168.3,0 ~ 0                | 0 ~ 0              |
| Both     | 192.168.3,0 ~ 0                | 0 ~ 0              |
| Both     | 192.168.3,0 ~ 0                | 0 ~ 0              |

- **Protocol** Select the protocol type as “TCP” or “UDP” from the drop down box. If you are not sure which one to choose, select “Both”.
- **Filter Group/LAN IP Range** Enter the range of IP addresses which you want to have the same access limitation (a group).
- **Block Port Range** Enter the range of port numbers which are used by the applications you wish to be blocked. (For example 23 for Telnet)

Here is an example for IP Access Setting. Enter the range of **51~80** in the “**Filter Group**” column and **20~80** in the “**Block Port Range**” column, then click the “**Apply**” button. As a result, the user’s computers which have IP Addresses in the range of 192.168.1.51 to 192.168.1.80 will not be able to use the applications which use port numbers from 20 to 80, such as FTP, Telnet and web browsing.

## Private MAC Filter

This function allows network administrators to insert the MAC addresses that need to be managed.



| Filtered MAC Address: | 1~10 |
|-----------------------|------|
| mac 1:                | 0    |
| mac 2:                | 0    |
| mac 3:                | 0    |
| mac 4:                | 0    |
| mac 5:                | 0    |
| mac 6:                | 0    |
| mac 7:                | 0    |
| mac 8:                | 0    |
| mac 9:                | 0    |
| mac 10:               | 0    |

Apply Undo

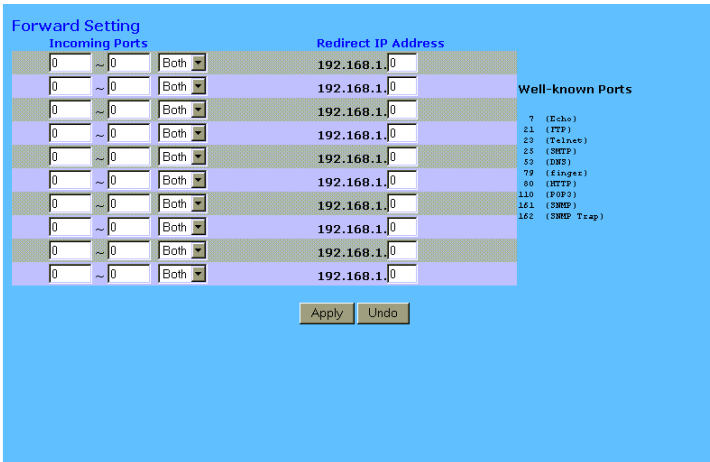
- **Filtered MAC Address** There are fifty sets divided into five groups of ten in this function. You can choose each group by selecting from the drop-down list. Enter the MAC addresses of the computers you wish to block in the columns, and then those users/computers cannot access Internet at all.

Click “Apply” after making any changes.

**Note:** To allow or deny access by URL, refer to the firewall configuration in Section 4-1.

## 4-4 Port Forwarding Settings

The Port Forwarding Setting application allows you to set up to ten public ports, such as a HTTP (web), SMTP (email), FTP, etc. that can be accessed by external users of the Internet. Each service is forwarded to a dedicated network computer (server) configured with a fixed LAN IP Address. Although the internal service addresses are not directly accessible to the external user, the NetComm Cable/DSL Firewall Router is able to redirect requests to the appropriate internal IP Address/server. To use this application, it is recommended you use a fixed Public IP Address from your ISP.



| Forward Setting |     |      | Well-known Ports    |
|-----------------|-----|------|---------------------|
| Incoming Ports  |     |      | Redirect IP Address |
| 0               | ~ 0 | Both | 192.168.1.100       |
| 0               | ~ 0 | Both | 192.168.1.100       |
| 0               | ~ 0 | Both | 192.168.1.100       |
| 0               | ~ 0 | Both | 192.168.1.100       |
| 0               | ~ 0 | Both | 192.168.1.100       |
| 0               | ~ 0 | Both | 192.168.1.100       |
| 0               | ~ 0 | Both | 192.168.1.100       |
| 0               | ~ 0 | Both | 192.168.1.100       |
| 0               | ~ 0 | Both | 192.168.1.100       |
| 0               | ~ 0 | Both | 192.168.1.100       |

Well-known Ports:

- 7 (Echo)
- 21 (FTP)
- 23 (Telnet)
- 25 (SMTP)
- 53 (DNS)
- 79 (finger)
- 80 (HTTP)
- 110 (POP3)
- 161 (SNMP)
- 162 (SNMP Trap)

Apply Undo

**Note:** Your NetComm Cable/DSL Firewall Router supports only one forward to one IP Address for each port (service).

- Set up individual network computers to act as servers and configure each with a fixed IP Address.
- In the “One Page Setup” screen, ensure the “**Private IP Address**” is set to the NetComm Cable/DSL Firewall Router’s default setting of 192.168.1.1. If a fixed Public IP Address is to be used, select “**Specify an IP address**” and enter the IP Address and other necessary information provided by your ISP.
- **Incoming Ports** - Enter the desired service port numbers in the “**Ports**” fields. You can specify the protocol type as “**TCP**” or “**UDP**” from the drop-down list. If you are not sure which one to select, choose “**Both**”. A selection of commonly used port numbers is provided on the right of this screen.
- **Redirect IP Address** - Enter the appropriate IP Addresses of the service computers in the “**Redirect IP Address**” locations.

**Example:** If the service port number **80~80** (representing an HTTP web address) is entered in “**Ports**” and **192.168.1.100** is entered in “**Redirect IP Address**”, then all HTTP requests from external Internet users will be directed to port 80 of the computer/server with the 192.168.1.100 fixed IP Address.

Here is a list of the protocols and port ranges that are used by some common applications.

**Note: Port 8080 on the Public IP Address is used for Remote Management and can not be redirected if remote management is enabled.**

| Application      | Protocol | Port Range   |
|------------------|----------|--|
| FTP Server       | TCP      | 21   |
| Half Life        | UDP      | 6003, 7002, 27010, 27015, 27025  |
| MSN Messenger    | TCP      | 6891-6900 (File-send)  |
|                  | TCP      | 1863   |
|                  | UDP      | 1863   |
|                  | UDP      | 5190   |
|                  | UDP      | 6901 (Voice)   |
| PC Anywhere host | TCP      | 5631   |
|                  | UDP      | 5632   |
| Quake 2          | UDP      | 27910  |
| Quake III        | UDP      | 27660 (first player)<br>"C:\Program Files\Quake III<br>Arena\quake3.exe" +set net_port 27660 |
|                  | UDP      | 27661 (second player)  |
| Telnet Server    | TCP      | 23   |
| Web Server       | TCP      | 80   |

## 4-5 Special Application

Some applications use multiple TCP/UDP ports to transmit data. Due to the use of NAT in the router, these applications may not work. Port Triggering allows these applications to work properly.

**Existing Special Applications**

| Application Name         | Outgoing Port Range                         | Incoming Port Range                         |
|--------------------------|---|---|
| 1: <input type="text"/>  | <input type="text"/> ~ <input type="text"/> | <input type="text"/> ~ <input type="text"/> |
| 2: <input type="text"/>  | <input type="text"/> ~ <input type="text"/> | <input type="text"/> ~ <input type="text"/> |
| 3: <input type="text"/>  | <input type="text"/> ~ <input type="text"/> | <input type="text"/> ~ <input type="text"/> |
| 4: <input type="text"/>  | <input type="text"/> ~ <input type="text"/> | <input type="text"/> ~ <input type="text"/> |
| 5: <input type="text"/>  | <input type="text"/> ~ <input type="text"/> | <input type="text"/> ~ <input type="text"/> |
| 6: <input type="text"/>  | <input type="text"/> ~ <input type="text"/> | <input type="text"/> ~ <input type="text"/> |
| 7: <input type="text"/>  | <input type="text"/> ~ <input type="text"/> | <input type="text"/> ~ <input type="text"/> |
| 8: <input type="text"/>  | <input type="text"/> ~ <input type="text"/> | <input type="text"/> ~ <input type="text"/> |
| 9: <input type="text"/>  | <input type="text"/> ~ <input type="text"/> | <input type="text"/> ~ <input type="text"/> |
| 10: <input type="text"/> | <input type="text"/> ~ <input type="text"/> | <input type="text"/> ~ <input type="text"/> |

**Note: Only one computer can use each Port Triggering setting at any time.**

- **Application Name** Enter the name of the application you wish to configure in the Application Name column to identify this setting. This is just a label and does not govern the function of the settings.
- **Outgoing Port Range** Enter the port number or range of numbers this application uses when it sends packets outbound. The Outgoing Control port numbers act as the trigger. When the NetComm Cable/DSL Firewall Router detects the outgoing packets with these port numbers, it will allow the inbound packets with the Incoming Port Numbers that you set in the next column to pass through the NetComm Cable/DSL Firewall Router.
- **Incoming Control** Enter the port number or range of numbers the inbound packets carry.

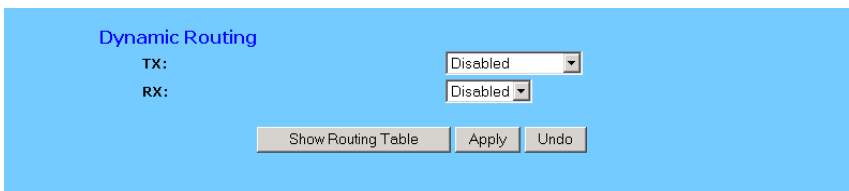
Click “Apply” after making any changes.

The following table lists the port numbers of some popular applications:

| Application     | Outgoing Control | Incoming Data                              |
|-----------------|------------------|--|
| Battle.net      | 6112             | 6112                                       |
| DialPad         | 7175             | 51200, 51201,51210                         |
| ICQ             | 4000             | 4000                                       |
| ICU II          | 2019             | 2000-2038, 2050-2051, 2069, 2085,3010-3030 |
| IRC             | 6667             | 531, 6666, 6667                            |
| MSN Gaming Zone | 47624            | 2300-2400, 28800-29000                     |
| PC to Phone     | 12053            | 12120,12122, 24150-24220                   |
| Quick Time4     | 554              | 6970-6999                                  |
| wowcall         | 8000             | 4000-4020                                  |

## 4-6 Dynamic Routing

The Dynamic Routing feature allows your NetComm Cable/DSL Firewall Router to exchange routing information with other routers in the network. Enabling this feature is likely to enhance performance of your NetComm Cable/DSL Firewall Router.



Dynamic Routing

TX:

RX:

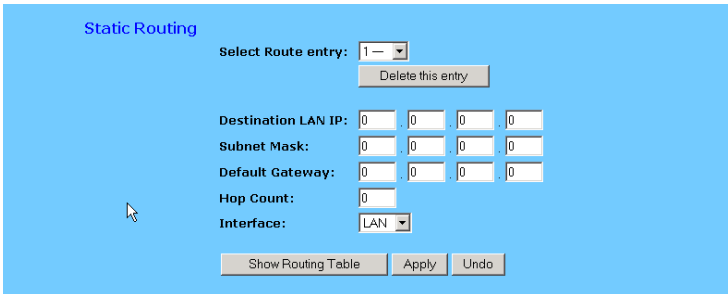
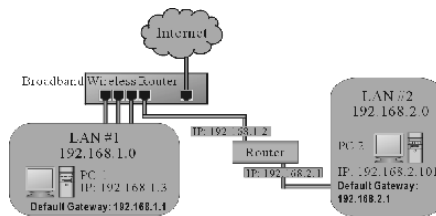
- **TX** From the drop-down list, select one of the routing information types, “**RIP-1**”, “**RIP-1 Compatible**”, or “**RIP-2**”, to enable the “**TX**” (transmit) function. “**RIP-1**” is the protocol used by older routers and newer routers should use “**RIP-2**”. “**RIP-1 Compatible**” serves to broadcast RIP-1 and multicast RIP-2.
- **RX** From the drop-down list, select one of the routing information types, “**RIP-1**” or “**RIP-2**”, to enable the “**RX**” (receive) function.

Click “Apply” after making any changes.



## 4-7 Static Routing

The Static Routing feature allows computers that are connected to the NetComm Cable/DSL Firewall Router directly or through a hub/switch (on the immediate LAN) to communicate with other computers in the respective LAN segment which are connected to the NetComm Cable/DSL Firewall Router through another router (destination LAN). Up to 20 route entries may be entered into the NetComm Cable/DSL Firewall Router. The diagram below gives an example of the physical connections required to use Static Routing.

In the above diagram, PC2 in LAN#2 is connected to the NetComm Cable/DSL Firewall Router via another router while PC1 in LAN#1 is connected to the NetComm Cable/DSL Firewall Router directly. Without configuring the Static Routing function, the two computers would not be able to communicate with each other.

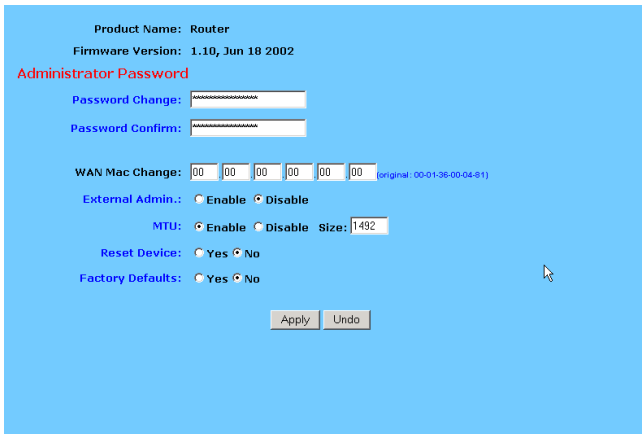
- **Select Route entry** Select the route entry number from 1 to 20 that you wish to configure.
- **Destination LAN IP** and **Subnet Mask** Enter the IP Address and Subnet Mask of the destination LAN that the immediate LAN is to communicate with. Taking the above diagram as an example, enter **192.168.2.0** in the “**Destination LAN IP**” field and **255.255.255.0** in the “**Subnet Mask**” field.
- **Default Gateway** Enter the IP Address of the router that forwards data packets to the destination LAN. For the above example, enter **192.168.1.2** in the “**Default Gateway**” field.
- **Hop Count** Enter the number of hops required between the LANs to be connected. The Hop Count represents the “cost” of the routing transmission. The default value is 1.
- **Interface** Choose “**LAN**” if the Destination LAN is on your Router’s LAN side and choose “**WAN**” if the Destination LAN is on the Router’s WAN side.

Referring back to the above diagram, with proper setting, PC1 would be able to access **LAN 1**, **LAN 2** and the **Internet** while PC2 can only access **LAN 2** and **LAN 1**.

Click “**Apply**” after making any changes.

## 4-8 Administration Settings

This feature allows the administrator to manage the NetComm Cable/DSL Firewall Router by setting certain parameters. For security reasons, it is strongly recommended that you set a Password and SNMP communities so that only authorized persons are able to manage your NetComm Cable/DSL Firewall Router. If the **“Password”** is left blank, all users on your network can access the router simply by entering the unit’s IP Address into their web browser’s location window.



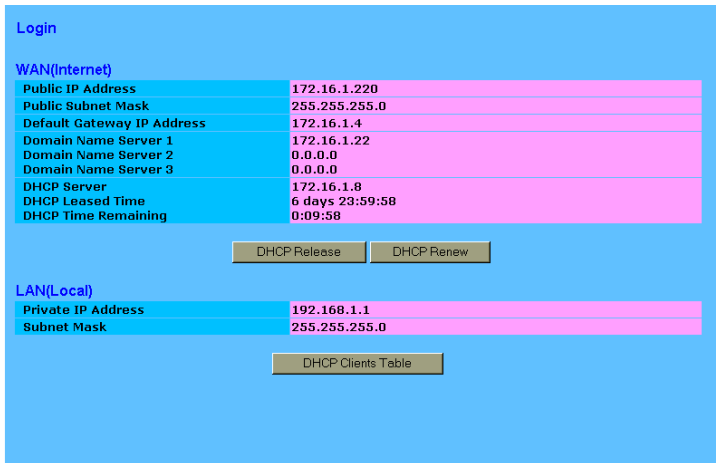
- **Firmware Version** This field shows the installed version of the firmware.
- **Administrator Password** Enter the password you want to use into the **“Password Change”** field and re-enter it into the **“Password Confirm”** field for confirmation. Be sure that the password is less than 64 characters long and without any spaces.
- **WAN MAC Change** The WAN MAC address can be changed from the original values if necessary. Some ISPs require users to change the WAN MAC address to a registered one when users change their access equipment.
- **External Admin** Check **“Enable”** to allow you to configure the NetComm Cable/DSL Firewall Router from WAN side. To access the setting page from external side, enter **“http://<WAN IP Address>:8080”** into the web browser address column and press the **“Enter”** key.
- **MTU** Check **“Enable”** if you want to limit the incoming and outgoing packet size for the router. Enter the maximum packet size you wish to set in the **“Size”** column. This can assist with the transmission of emails with attachments, etc.
- **Reset Device** Select **“Yes”** if you want to clear connections, reboot, and re-initialize the unit without affecting any of your configuration settings.
- **Factory Defaults** Select **“Yes”** if you want to return all the router’s current settings to their factory default settings.

**Note: Do not restore to the factory defaults unless it is absolutely necessary.**

Click **“Apply”** to make any changes.

## 4-9 Status Monitor

This screen shows the router's current status. All of the information provided is read-only.



**Login**

**WAN(Internet)**

|                            |                 |
|----------------------------|-----------------|
| Public IP Address          | 172.16.1.220    |
| Public Subnet Mask         | 255.255.255.0   |
| Default Gateway IP Address | 172.16.1.4      |
| Domain Name Server 1       | 172.16.1.22     |
| Domain Name Server 2       | 0.0.0.0         |
| Domain Name Server 3       | 0.0.0.0         |
| DHCP Server                | 172.16.1.8      |
| DHCP Leased Time           | 6 days 23:59:58 |
| DHCP Time Remaining        | 0:09:58         |

**LAN(Local)**

|                    |               |
|--------------------|---------------|
| Private IP Address | 192.168.1.1   |
| Subnet Mask        | 255.255.255.0 |

- **Login** This column shows the login information of your WAN connection. You can manually initiate a connection or a disconnection by clicking the buttons. However, if you initiate a disconnection here, the “**Connect-on-Demand**” will not function until the connection button is clicked. Note that the Login won’t show any information if you select “**Obtain IP automatically**” or “**Static IP**” in the “**OnePage Setup**” page.
- **WAN (Internet)** This section shows the IP settings status of the router as seen by external users of the Internet. If you select “**Get IP Address Automatically**”, “**PPPoE**”, or “**PPTP**” in OnePage Setup, the “**IP Address**”, “**Subnet Mask**”, “**Default Gateway**”, and “**Domain Name Server**” (DNS) will show the information received from the DHCP server or ISP currently being used. If you select “**Static IP**” in the “**One Page Setup: Public IP Address**”, the information will be the same as your input.
 

**DHCP Release:** Click this button to eliminate the IP address obtained from the DHCP server.

**DHCP Renew:** Click this button to re-acquire the IP address from the DHCP server.

**Note:** *The “DHCP Release” and “DHCP Renew” button only show up when you select “Get IP Address Automatically” in the OnePage Setup.*
- **LAN (Local)** This section displays the current “**Private IP Address**” and “**Subnet Mask**” of the router, as seen by users of your internal network.
- **DHCP Clients Table** If the router is setup to act as a DHCP server, the LAN side IP Address distribution table will appear when this button is selected.

## 4-10 DMZ Host

The DMZ Host application allows unrestricted 2-way communication between a single LAN computer and other Internet users or servers. This application is useful for supporting special-purpose services such as video-conferencing and gaming, which require proprietary client software and/or unrestricted 2-way user communication. To use this application, you should have a fixed Public IP Address from your ISP.

This feature will open all in/out access to one computer on the LAN. Some Internet applications such as games may require this.  
**Warning:**The computer with the IP address entered will be completely exposed to the Internet.

DMZ Host: 192.168.1.0

Apply Undo

**Note:** *In order to provide unrestricted access, the Firewall provided by the NetComm Cable/DSL Firewall Router to protect this port is disabled, thus creating a potentially serious security risk. It is recommended that this application should be disabled when it is not in use by entering “0” in the “DMZ Host” field.*

1. Before setting up a LAN computer to act as a DMZ Host, configure it with a fixed IP Address.
2. In the “**One Page Setup**” screen, ensure the Private IP Address is set to the NetComm Cable/DSL Firewall Router’s default setting of **192.168.1.1**. In the Public IP Address area, select “**Specify an IP Address**”, then enter the IP Address and other necessary information provided by your ISP.
3. Click “**DMZ Host**” from the Advanced Menu. Enter the fixed IP Address of the Exposed Host computer in the “**DMZ Host**” IP Address location. Remember, entering “**0**” will disable this application.
4. Click “**Apply**”.

## 4-11 Log

The Log application allows the administrator to trace Internet access. You can send the record to specific LAN computers for remote monitoring, but can also watch the incoming (WAN to LAN) and outgoing (LAN to WAN) traffic in the “**Log Settings**” page.

Log

Access Log:  Enable  Disable

Send Log To: 192.168.1.255

Apply Undo

- **Access Log** Set to **Enable** if you want to activate this function.
- **Send Log To** Enter the IP address of the computer that you want to send the Log information to.
- **Incoming Access log** Click this button to go to the incoming (WAN to LAN) traffic log table. This Table records information on the last fifty incoming packets, including source IP address, destination IP address, and port number.
- **Outgoing Access log** Click this button to go to the outgoing (LAN to WAN) traffic log table. This Table records information on the last fifty outgoing packets, including source IP addresses, destination IP addresses, and port numbers.

Click “**Apply**” after making any changes.

## 4-12 VPN Passthrough

Virtual Private Networking (VPN) is a system which allows remote networks to privately exchange data over an existing public network (usually the WAN/Internet). One VPN client can be used to make one VPN connection (Tunnel) to a VPN Server on the Internet. The NetComm Cable/DSL Firewall Router supports one single session VPN Passthrough (PPTP or L2TP/IPSec). There is no configuration necessary for VPN Passthrough.

## Chapter 5: Configuring IPsec on Windows 2000/XP

This document illustrates the steps of Microsoft Windows 2000/XP computer to establish a secure IPsec tunnel with the Cable/DSL Firewall Router. You can find detailed information on configuring the Microsoft Windows 2000 server at the Microsoft website:

Microsoft KB Q252735 - How to Configure IPsec Tunneling in Windows 2000

<http://support.microsoft.com/support/kb/articles/Q252/7/35.asp>

Microsoft KB Q257225 - Basic IPsec Troubleshooting in Windows 2000

<http://support.microsoft.com/support/kb/articles/Q257/2/25.asp>

### 5-1 Environment

#### Windows XP or Windows 2000

IP Address: 140.111.1.2 (Note: ISP provided IP Address; this is only an example.)

Subnet Mask: 255.255.255.0

#### Cable/DSL Firewall Router

##### WAN

IP Address: 140.111.1.1 (Note: ISP provided IP Address, this is only an example.)

Subnet Mask: 255.255.255.0

##### LAN

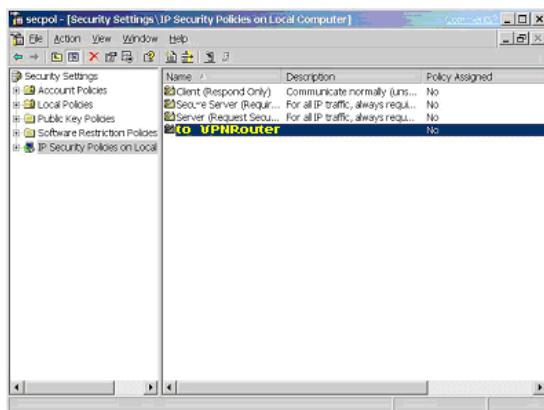
IP Address: 192.168.1.1

Subnet Mask: 255.255.255.0

### 5-2 Steps in Windows 2000/XP

#### 5-2.1 Create IPsec Policy

1. Click **Start** button, select **Run**, and type **secpol.msc** in the open field.
2. Right-click **IP Security Policies on Local Computer**, and then click **Create IP Security Policy**.

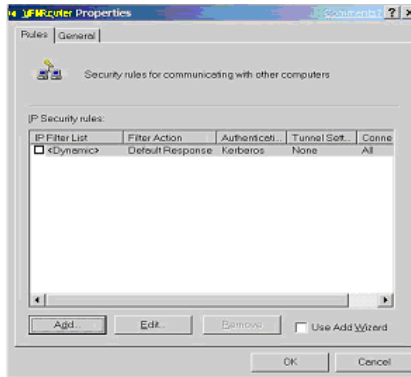


3. Click **Next**, and then type a name for your policy (for example, “**to\_VPNRouter**”).
4. Deselect the **Activate the default response rule** check box, and then click **Next** button.
5. Click the **Finish** button, making sure the **Edit** check box is checked.

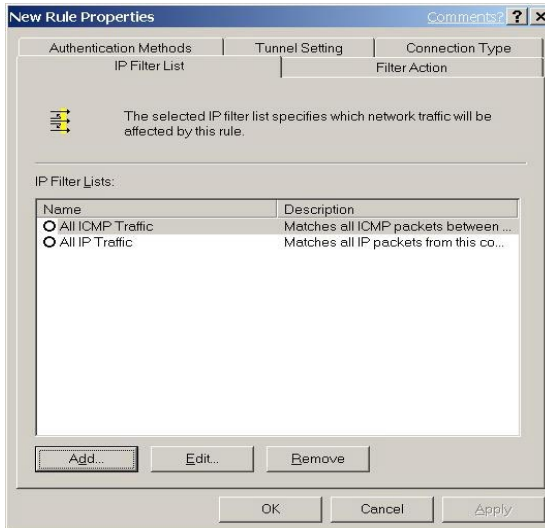
## 5-2.2 Build 2 Filter Lists: “WinXP→Cable/DSL Firewall Router” and “Cable/DSL Firewall Router→WinXP”.

### [Filter List 1] WinXP→ Cable/DSL Firewall Router

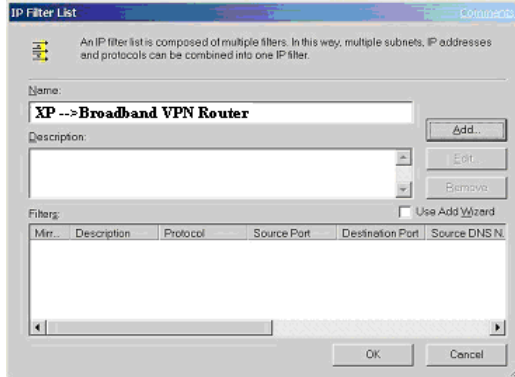
1. In the **to\_VPNRouter Properties**, deselect the **Use Add Wizard** check box, and then click **Add** button to create a new rule.



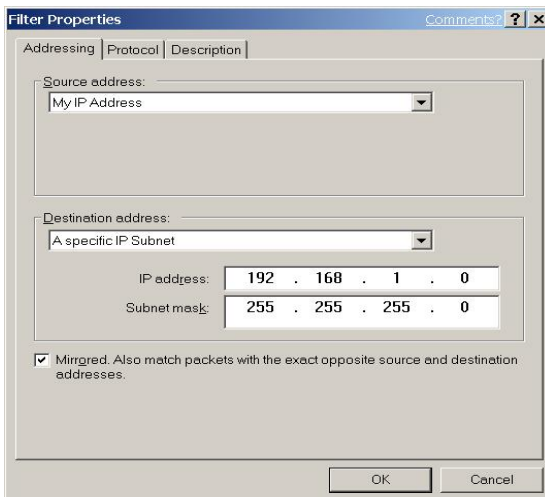
2. From the **IP Filter List** tab, click the **Add** button.



3. Type an appropriate name “**XP→Cable/DSL Firewall Router**” for the filter list, deselect the **Use Add Wizard** check box, and then click **Add** button.



4. In the **Source address** area, click **My IP Address**.
5. In the **Destination address** field, select **A specific IP Subnet**, and fill in the **IP Address** “192.168.1.0” and **Subnet mask** “255.255.255.0”.

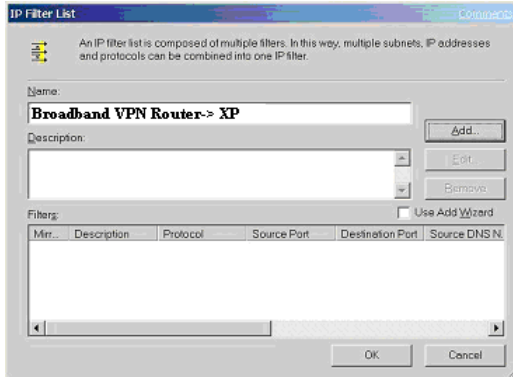


6. If you want to type a description for your filter, click the **Description** tab.
7. Click **OK** button. Then click **OK**(for WinXP) or **Close** (for Win2000) button on the **IP Filter List** window.

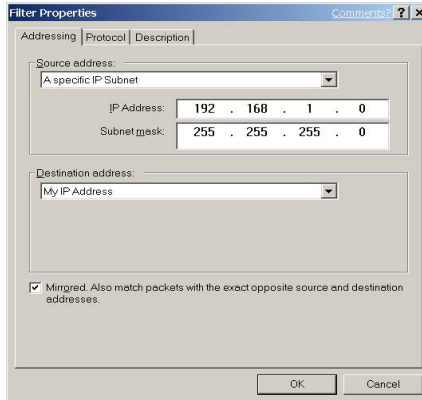
#### [Filter List 2] Cable/DSL Firewall Router→WinXP

8. On the **IP Filter List** tab, click the **Add** button.
9. Type an appropriate name “**Cable/DSL Firewall RouteràXP**” for the filter list, click to clear the **Use Add Wizard** check box, and then click **Add**.





10. In the **Source address** area, click **A specific IP Subnet**, and fill in the **IP Address** “192.168.1.0” and **Subnet mask** “255.255.255.0”.
11. In the **Destination address** area, click **My IP Address**.

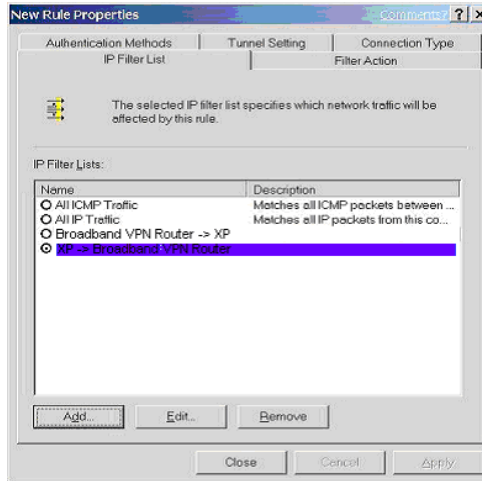


12. If you want to type a description for your filter, click the **Description** tab.
13. Click **OK**, and then click **OK**.

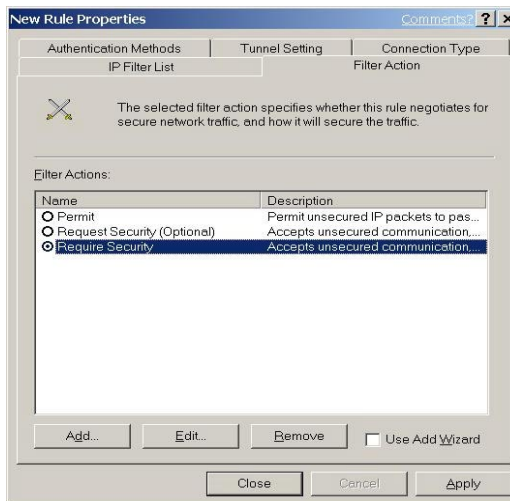
## 5-2.3 Configure Individual Rule of 2 Tunnels

### [Tunnel 1] WinXP→Cable/DSL Firewall Router

1. From the **IP Filter List** tab, click the filter list “**XP→Cable/DSL Firewall Router**”.

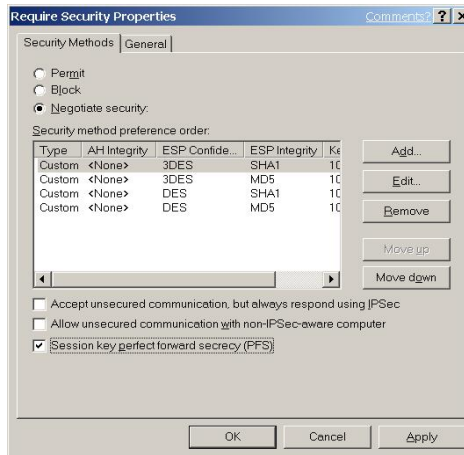


2. From the **Filter Action** tab, click the filter action “**Require Security**”, and click the **Edit** button.

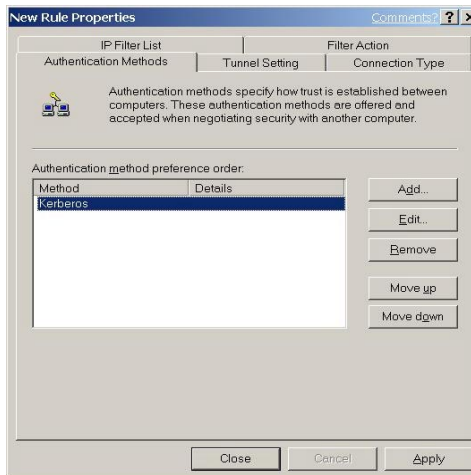


3. Check that the **Negotiate security** option is enabled, and deselect the **Accept unsecured communication**, but always respond using **IPsec** check box.

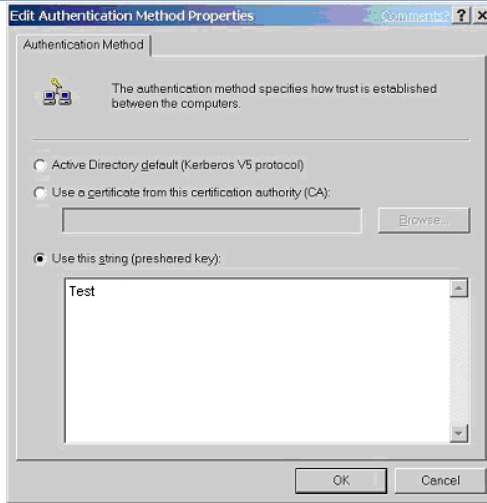
4. Select the **Session key Perfect Forward Secrecy (PFS)** and remember to check the **PFS** option on the Cable/DSL Firewall Router, and then click the **OK** button.



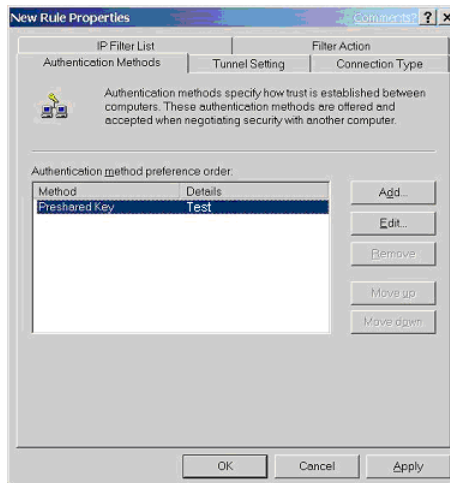
5. From the **Authentication Methods** tab, click the **Edit** button.



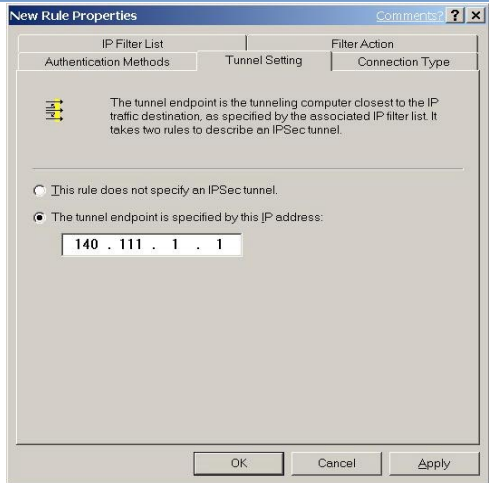
6. Change the authentication method to **“Use this string (preshared key)”**, enter the string **“Test”**, and then click the **OK** button.



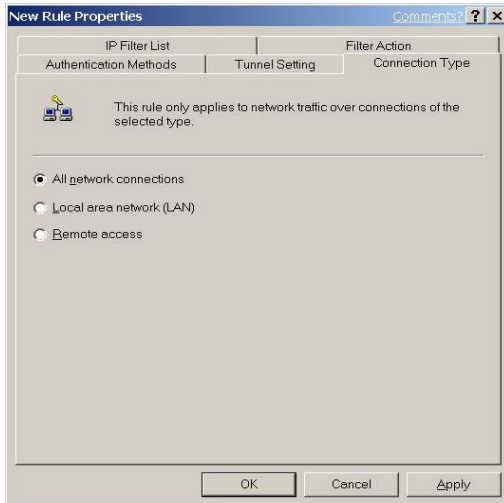
This new Preshared key will be displayed in Authentication method preference order. Click the **OK** button to continue.



- From the **Tunnel Setting** tab, click **The tunnel endpoint is specified by this IP Address** box, and then type the **WAN IP Address “140.111.1.1”** (Note: Use your ISP provided IP Address; this is only an example.) of Cable/DSL Firewall Router.

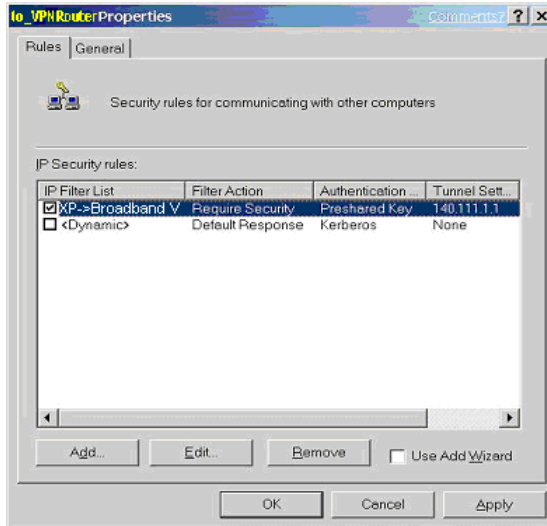


- From the **Connection Type** tab, select **All network connections**, and then click the **OK** or **Close** button to finish this rule.

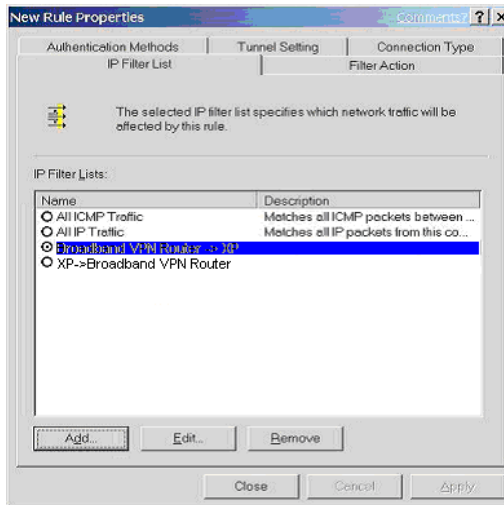


**[Tunnel 2] Cable/DSL Firewall Router→ WinXP**

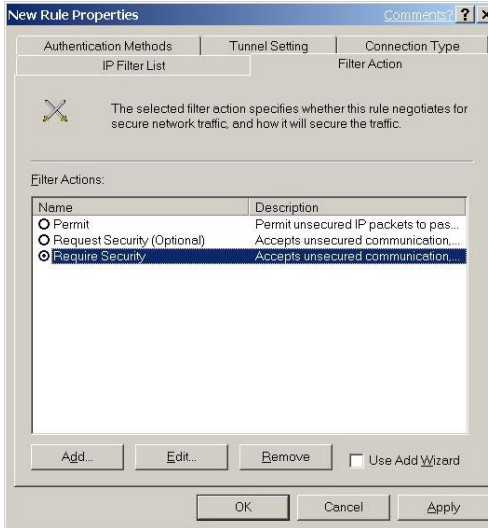
- In the **to\_VPNRouter Properties**, deselect the **Use Add Wizard** check box, and then click the **Add** button to create the second IP Filter.



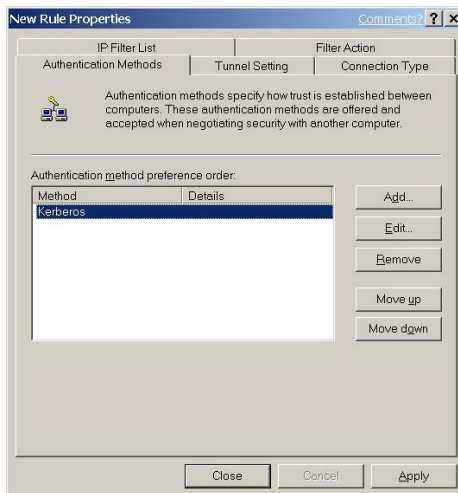
- On the **IP Filter List** tab, click the filter list **“Cable/DSL Firewall Router→XP”**.



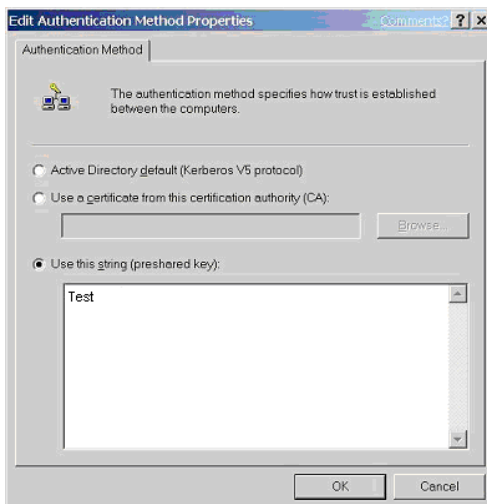
11. From the **Filter Action** tab, click the filter action **“Require Security”**.



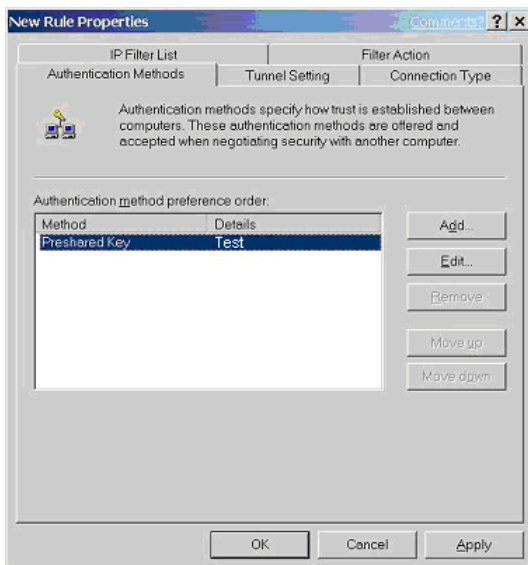
12. From the **Authentication Methods** tab, click the **Edit** button.



13. Change the authentication method to **“Use this string (preshared key)”**, enter the string **“Test”**, and then click the **OK** button.

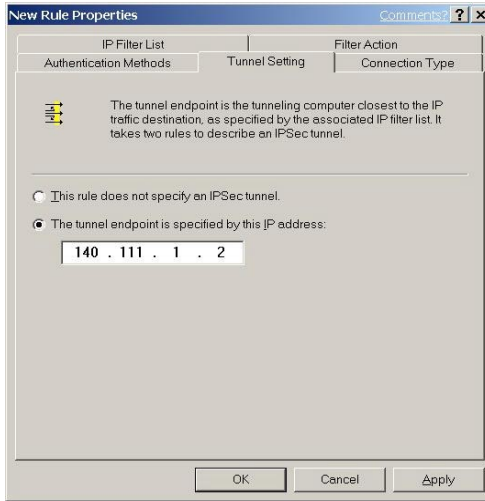


This new Preshared key will be displayed in Authentication method preference order. Click the **OK** button to continue.

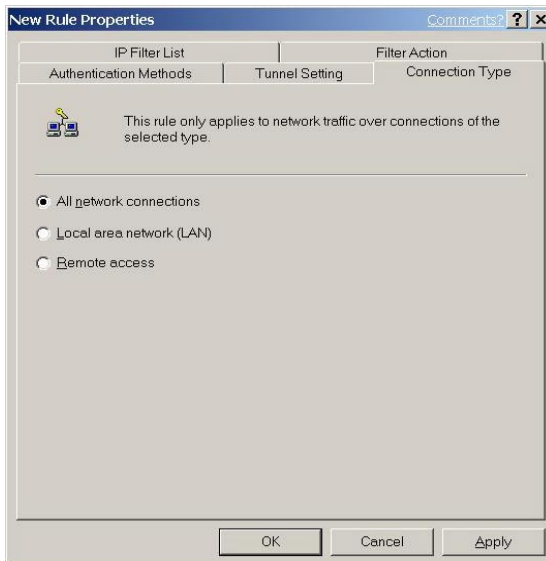


14. From the **Tunnel Setting** tab, click **The tunnel endpoint is specified by this IP Address** box, and then type the **Windows 2000/XP IP Address “140.111.1.2”**.





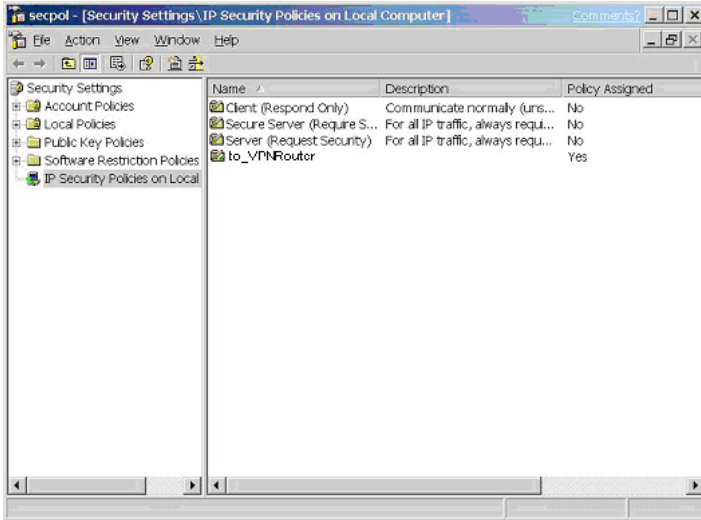
15. From the **Connection Type** tab, select **All network connections**, and then click the **OK**(for WinXP) or **Close**(for Win2000) button to finish.



16. From the **Rules** tab, click the **OK** button to back to the **secpol** screen.

## 5-2.4 Assign New IPsec Policy

1. In the **IP Security Policies on Local Computer** MMC snap-in, right-click policy named **“to\_VPNRouter”**, and then click **Assign**. A green arrow appears in the folder icon.



## 5-3 Steps in Cable/DSL Firewall Router

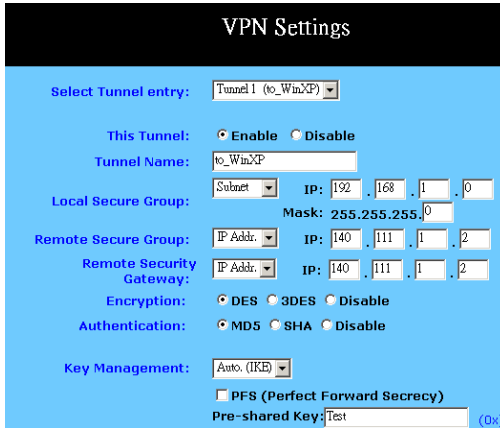
### 5-3.1 OnePage Setup Screen

1. Open your web browser and enter **192.168.1.1** in the **Address** field and press the **Enter** key.
2. When the **User Name** and **Password** field appears, skip the user name and enter the default password **admin** and press the **Enter** key.
3. Click the **OnePage Setup** tab to set the configuration as shown below.

| Main Menu  | OnePage Setup  |
|--|--|
| <ul style="list-style-type: none"> <li>OnePage Setup</li> <li>Advanced           <ul style="list-style-type: none"> <li>VPN</li> <li>DHCP Settings</li> <li>Access Control</li> <li>Virtual Server</li> <li>DMZ Host</li> <li>Device Admin</li> <li>Status Monitor</li> <li>Dynamic Routing</li> <li>Static Routing</li> <li>Special App</li> <li>Log</li> </ul> </li> </ul> | <h3>OnePage Setup</h3> <p>(MAC Address: 00-01-36-02-DE-F9)</p> <p><b>Private IP Address</b></p> <p>Device IP Address: <input type="text" value="192.168.1.1"/></p> <p>Subnet Mask: <input type="text" value="255.255.0"/></p> <p><b>WAN Connection Type</b> <input type="text" value="Static IP"/></p> <p>Select the Internet connection type you wish to use</p> <p>Specify WAN IP Address: <input type="text" value="140.111.1.1"/></p> <p>Subnet Mask: <input type="text" value="255.255.0"/></p> <p>Default Gateway Address: <input type="text" value="140.111.1.2"/></p> <p>DNS(Required) 1: <input type="text" value="0.0.0.0"/></p> <p>DNS 2: <input type="text" value="0.0.0.0"/></p> <p>DNS 3: <input type="text" value="0.0.0.0"/></p> <p><input type="button" value="Apply"/> <input type="button" value="Cancel"/></p> |

### 5-3.2 VPN Screen

The following Figure is a sample configuration for the Router's VPN tab.



The screenshot shows the 'VPN Settings' configuration window. It includes the following fields and options:

- Select Tunnel entry:** Tunnel 1 (to\_WinXP)
- This Tunnel:**  Enable  Disable
- Tunnel Name:** to\_WinXP
- Local Secure Group:** Subnet, IP: 192.168.1.0, Mask: 255.255.255.0
- Remote Secure Group:** IP Addr., IP: 140.111.1.2
- Remote Security Gateway:** IP Addr., IP: 140.111.1.2
- Encryption:**  DES  3DES  Disable
- Authentication:**  MD5  SHA  Disable
- Key Management:** Auto. (IKE)
- PFS (Perfect Forward Secrecy)
- Pre-shared Key:** Test (Dk)

Once all these have been entered, click the Connect button to establish a VPN connection. The Status should indicate that the Router is Connected.

## Chapter 6: Macintosh Setup

This chapter provides information on using Macintosh computers in your network. The instructions given here are for system software version 8.0 or above, which comes with the TCP/IP Protocol preloaded and supports DHCP Addressing.

### 6-1 Hardware Connections

Connect your Macintosh computer to your NetComm Cable/DSL Firewall Router. If you have a newer computer, there will be a 10Base-T Ethernet port on the back. Older computers will need to have an Ethernet card installed. Refer to your computer's User Manual for instructions on Ethernet card installation.

### 6-2 Computer Network Configuration

It is assumed that your computer's system software already has TCP/IP installed. You may manually configure your computer with a fixed IP Address (for example 192.168.1.2) or have an IP Address dynamically assigned to it by the NetComm Cable/DSL Firewall Router's DHCP server.

#### 6-2.1 Dynamic IP Addressing using DHCP Server.

1. From the **"Apple"** menu, select **"Control Panel"** and click on **"TCP/IP"**.
2. In the **"TCP/IP (A New Name For Your Configuration)"** window, select **"Ethernet"** in the **"Connect via"** location from the drop-down list.
3. In the **"Setup"** area:
  - Select **"Using DHCP Server"** in the **"Configure"** location from the drop-down list.
  - No other data needs to be entered.
  - Close the window.
4. Click **"Save"** from the file menu, then **"Quit"** TCP/IP.
5. Restart the computer.

#### 6-2.2 Manual Configuration of Fixed IP Addresses

1. From the **"Apple"** menu, select **"Control Panel"** and click on **"TCP/IP"**.
2. In the **"TCP/IP (A New Name For Your Configuration)"** window, select **"Ethernet"** in the **"Connect via"** location from the drop-down list.
3. In the **"Setup"** area:
  - Select **"Manually"** in the **"Configure"** location from the drop-down list.
  - In the **"IP Address"** location, enter the IP Address that you want to assign to the computer (for example 192.168.1.2) .
  - Enter **"255.255.255.0"** in the **"Subnet Mask"** location.
  - Enter **"192.168.1.1"** (the NetComm Cable/DSL Firewall Router's default IP Address) in the **"Router Address"** location.

- Enter the ISP's IP Address in the “**Name Server**” location if your ISP has provided this information. (This is the DNS address provided by your ISP.)
  - Close the window.
4. Click “**Save**” from the file menu then “**Quit**” TCP/IP.
  5. Restart the computer.

## 6-3 NetComm Cable/DSL Firewall Router Configuration

To configure your NetComm Cable/DSL Firewall Router, launch your Web Browser and follow the instructions given in *Chapter 3: Internet Access, section 3.3*. To configure advanced settings, refer to *Chapter 4: Advanced Configuration*.

## 6-4 Adding NetComm Cable/DSL Firewall Router to Existing Network

If the NetComm Cable/DSL Firewall Router is to be added to an existing Macintosh computer network, the computers will have to be configured to connect to the Internet via the NetComm Cable/DSL Firewall Router.

1. From the “**Apple**” menu, select “**Control Panel**” and click on “**TCP/IP**”.
2. From the “**File**” menu, select “**Configurations**” and select your existing network configuration. Click “**Duplicate**”.
3. Rename your existing configuration. Click “**OK**”, and “**Make Active**”.
4. In the Setup area:
  - Select “**Manually**” in the “**Configure**” location from the drop-down list.
  - In the “**IP Address**” location, enter the IP Address that you want to assign to the computer (for example 192.168.1.2) .
  - Enter “**255.255.255.0**” in the “**Subnet Mask**” location.
  - Enter “**192.168.1.1**” (the NetComm Cable/DSL Firewall Router's default IP Address) in the “**Router Address**” location.
  - Enter the ISP's IP Address in the “**Name Server**” location if your ISP has provided the information.
  - Close the window.
5. Click “**Confirm**”. TCP/IP is now configured for manual IP Addressing.
6. Configure your NetComm Cable/DSL Firewall Router (see 6.3 above).

## Chapter 7: Trouble Shooting

This chapter provides solutions to problems you may encounter during installation and operation of your NetComm Cable/DSL Firewall Router.

### Hardware

#### **T: The Power LED is off.**

Check the power cable is properly connected to the NetComm Cable/DSL Firewall Router, the power adapter and the socket.

#### **T: The LAN Link LED is off.**

Check the computer, hub or switch is properly connected to the NetComm Cable/DSL Firewall Router.

Check the computer's Ethernet card is properly installed.

Check the UTP cable connecting the computer to the Router is connected. This cable should **not** be a crossover cable.

Check the Cable/DSL Firewall Router and the computer are on the same network segment. If you are not sure, initiate the DHCP function (4-1) and set your computer to obtain an IP address automatically (3-3).

Check the computer is using an IP address in the range of 192.168.1.2 ~ 192.168.1.254 and is therefore compatible with the Cable/DSL Firewall Router's default IP address of 192.168.1.1 (3-3). Check also the Subnet Mask is set to 255.255.255.0

#### **T: The DIAG LED stays lit.**

The DIAG LED should light up when the device is first powered up to indicate it is checking for proper operation. After a few seconds, the LED should go off. If it stays on, the device is experiencing a problem. Please contact your dealer.

#### **T: Why can't I configure the NetComm Cable/DSL Firewall Router?**

First, check whether the NetComm Cable/DSL Firewall Router is properly installed, including the LAN and WAN connections, and all devices' power.

Next, check the IP configuration of your computer :

- For Windows 95/98 users: run **Winipcfg.exe** or **Winipcfg** from "Run" on the "Start" menu. If there are no IP addresses, click "Release All" and then click "Renew All" to get an IP address.

For Windows NT 4.0/2000/XP users: Open a command prompt and run **IpConfig**.

- Ensure that your computer and the NetComm Cable/DSL Firewall Router are on the same network segment. If you are not sure, initiate the DHCP function and let the computer get an IP address automatically from the router.

- Ensure that your computer is using an IP Address within the range 192.168.1.2 to 192.168.1.253 and thus compatible with the NetComm Cable/DSL Firewall Router's default IP address of 192.168.1.1
- Finally, use *Ping* command in MS-DOS mode to verify the network connection:
  - *Ping* 127.0.0.1 to check the TCP/IP stack of your computer.
  - *Ping* the Router's IP address (Default: 192.168.1.1) to check for IP connectivity between your computer and the Router.

**Note:** *If you are not able to get to the web configuration screen for the NetComm Cable/DSL Firewall Router, make sure that you disable the proxy setting within your Internet browser and set your browser to access the Internet via the LAN.*

### **T: What can I do if I have forgotten the password for NetComm Cable/DSL Firewall Router?**

You have to reset the Router back to its factory default setting by pushing the Reset button for over 3 seconds.

**Note:** *You will lose all previous settings.*

### **T: I cannot access my ISP's home page, why?**

Some ISPs (such as Telstra BigPond) require their host name be specifically configured into your computer before you can surf their local web pages. If you are unable to access your ISP's home page, enter your ISP's Domain Name into the One Page Setup (3-3) to enable all computers in your LAN to access it. If you only want to allow computers to access these home pages, open the TCP/IP Properties window (2-4) on these computers, click open the **"DNS Configuration"** tab and enter your ISP's Domain Name in the **"Domain Name Search Suffix"** location.

## **Client Side (Computers)**

### **T: I can't browse the Internet via the NetComm Cable/DSL Firewall Router**

Ensure your computer can ping or access the Router. See the previous section entitled **"Why can't I configure the NetComm Cable/DSL Firewall Router"** for more information.

Check the status page of the Router to ensure connection to your ISP has been established.

### **T: I get a time out error when I enter a URL or IP address.**

Check if other computers on the LAN are experiencing the same problem. If not, ensure the computer's IP settings are correct (IP Address, Subnet Mask, Gateway IP Address and DNS).

Check the NetComm Cable/DSL Firewall Router's settings are correct (3-3).

## Appendix A: Frequently Asked Questions

### Q: What is the maximum number of IP Addresses the NetComm Cable/DSL Firewall Router can support?

The NetComm Cable/DSL Firewall Router can support up to 253 IP Addresses in the range of 192.168.1.2~192.168.1.254.

### Q: Where should the NetComm Cable/DSL Firewall Router be installed on the network?

In a typical environment, the NetComm Cable/DSL Firewall Router should be installed between the ADSL/Cable modem and your LAN. Connect the NetComm Cable/DSL Firewall Router to the Ethernet port of your ADSL/Cable modem, and connect your computers to the RJ45 jack on the LAN side.

### Q: Does the NetComm Cable/DSL Firewall Router support IPX or AppleTalk?

No. The NetComm Cable/DSL Firewall Router was designed to provide a multiple user LAN with shared Internet access and supports only the TCP/IP Protocol. If your Novell or Apple system is configured with TCP/IP, the NetComm Cable/DSL Firewall Router can support them.

### Q: Does the NetComm Cable/DSL Firewall Router support 100Mb Ethernet?

Yes, the NetComm Cable/DSL Firewall Router supports both 10Mb & 100Mb Ethernet on the LAN side, but only 10Mb on the WAN side.

### Q: What is “NAT” and what is it used for?

The Network Address Translation (NAT) Protocol translates multiple IP Addresses on a private LAN into a single public IP Address that is accessible to the Internet. NAT not only provides the basis for multiple IP Address sharing but also provides security,

since the multiple IP Addresses of LAN computers are never transmitted directly to the Internet.

### Q: How can NetComm Cable/DSL Firewall Router share single user account to multiple users?

The NetComm Cable/DSL Firewall Router combines the following technologies to enable this function.

**NAT (Network address translation):** NAT is a technology which can create a private network domain behind a public IP. It is usually used as a firewall. It can also be used when there are not enough IP Addresses.

**DHCP (Dynamic host configuration protocol):** DHCP is a protocol to assign IP Addresses to internal computers automatically. It can save a lot of IP Address configuration. This protocol is supported by Windows 95/NT, Mac OS, and many other popular OS.

**DNS (Domain name service):** DNS is a protocol which translates Domain Names to IP addresses that an Internet host can handle. Addressing system using Domain names, like www.yahoo.com, is easier to use than its IP address, 204.71.177.70.

### Q: What operating systems does NetComm Cable/DSL Firewall Router series support?

The NetComm Cable/DSL Firewall Router uses standard TCP/IP protocol. It can be operated as long as you have TCP/IP protocol installed on your operating system (For example: Windows 9x, Windows NT, Windows 2000, Windows XP, etc.)

### Q: Can I use multiple E-mail accounts if I use NetComm Cable/DSL Firewall Router?

Yes, you can. Some people think having one Internet account means that they can have only one E-mail account. However, E-mail is



set by mailbox accounts and different to the account you use to connect to your ISP. If you want more E-mail accounts, you can contact your ISP or you can browse the Internet to apply for free E-mail account.

**Q: Can Internet users access LAN computers?**

The NetComm Cable/DSL Firewall Router uses NAT to route all in/out band packets. All external users can only see the IP of the NetComm Cable/DSL Firewall Router but cannot access LAN computers. The LAN computers are well protected with the NetComm Cable/DSL Firewall Router's natural firewall (NAT). You can allow Internet users access to specific computers by using the Port Forwarding, DMZ Host and Special Application options.

**Q: When should I use DMZ host?**

Enable DMZ host when you want to have unrestricted communication between your computer and the Internet, for example, playing Internet game (i.e. Ages of Empire) or having multimedia conference (i.e. NetMeeting).

**Q: Does the NetComm Cable/DSL Firewall Router support PPTP of VPN packets pass through?**

Yes. The NetComm Cable/DSL Firewall Router supports single session PPTP pass through.

**Q: Does the NetComm Cable/DSL Firewall Router series support IPsec?**

Yes. The NetComm Cable/DSL Firewall Router supports single session IPsec pass through.

## Appendix B: Technical Specifications

### Standards Compliance

IEEE 802.3 10BASE-T  
IEEE 802.3u 100BASE-TX

### Interface

One 10Mbps Ethernet RJ45 port on WAN  
Four 10/100Mbps auto-sensing Ethernet RJ-45 ports

### Management

Web-based UI Management

### LED Display

Power  
DIAG  
Link/Activity for both WAN and LAN port(s)  
Full Duplex/Collision for LAN ports

### Environment

Operating Temperature: 0 ~ 45 degrees C  
Storage Temperature: -20 ~ 70 degrees C  
Humidity: 0 ~ 90% non-condensing

### Dimension

145 (L) x 260 (W) x 38 (H) mm

### Power

External, DC 5V, 2.5A

### Mounting

Desktop  
Wall-mounting

---

## Appendix C: Glossary

### 10Base-T / 100Base-T

The adaptation of the Ethernet standard for Local Area Networks (LANs). 10Base-T uses a twisted pair cable with maximum lengths of 100 meters and transmits data at 10Mbps maximum. 100Base-T is similar, but uses two different twisted pair configurations and transmits at 100Mbps maximum.

### Ad-hoc Network

Also known as the peer-to-peer network, an ad-hoc network allows all computers participating in a wireless network to communicate each other without an AccessPoint.

### Adapter

A device that makes the connection to a network segment, such as Ethernet and modem cards.

### ADSL

Asymmetric Digital Subscriber Line (ADSL), as its name indicates, is an asymmetrical data transmission technology with higher traffic rate downstream and lower traffic rate upstream. ADSL technology satisfies the bandwidth requirements of applications which demand “asymmetric” traffic, such as web surfing, file downloads, and telecommuting.

### Bandwidth

The amount of data that can be transmitted in a fixed amount of time.

### Browser

A software application used to locate and display Web pages. Examples include Netscape Navigator and Microsoft Internet Explorer.

### BSS

BSS is the acronym of Basic Service Set that consists of a wireless access point and a group of wireless client computers.

### Communications Protocols

Communication between devices requires they agree on the format in which the data is to be transmitted, sent and received. The communications protocols are a set of rules that define the data format.

### Cookie

Cookie is data stored on your computer, which a web server can retrieve, to identify your machine. It is a piece of text with an ID number.

### DHCP

DHCP, short for Dynamic Host Configuration Protocol, is a protocol for assigning dynamic IP Addresses to devices on a network. Dynamic Addressing means that a device can have a different IP Address each time it connects to the network.

### Domain Name

A name that identifies one or more IP Addresses. For example, the domain name microsoft.com represents about a dozen IP Addresses. Domain names are used in URLs to identify particular Web pages. For example, in the URL <http://www.pcwebopedia.com/index.html>, the domain name is pcwebopedia.com.

## **DoS**

DoS is the acronym for Denial of Service. This is the result when a computer or network is overwhelmed to the point that it can no longer function normally.

## **DNS**

Short for Domain Name Server, translates domain names into IP Addresses. To help us recognize and remember domain names they are alphabetic in form, however, the Internet actually runs on numbered IP Addresses. DNS servers translate domain names into their respective IP Addresses.

## **DSSS**

Also known as Direct Sequence Spread Spectrum, it is a radio transmission method that continuously changes frequencies.

## **Ethernet**

One of the most common Local Area Network (LAN) standards. Ethernet uses a bus topology which supports a data transfer rate of 10 or 100 Mbps.

## **ESS**

ESS is the acronym of Extend Service Set that consists of several BSS.

## **Firewall**

A security system used to enforce an access control policy between an organisation's networks and the Internet.

## **IEEE**

Short for Institute of Electrical and Electronics Engineers, an organization best known for developing standards for the computer and electronics industry.

## **Internet**

A global network connecting millions of computers for the exchange of data, news and opinions.

## **Intranet**

A network based on TCP/IP Protocol belonging to an organization, and accessible

only by that organization's members, employees, or others with authorization.

## **Infrastructure Network**

Unlike an ad-hoc network (where users on a wireless LAN send data to each other directly), users on an infrastructure network send data through a dedicated access point. Additionally, the access point enables users on a wireless LAN to access an existing wired network to take advantage of sharing the wired network's resources, such as files, printers, and Internet access.

## **IP Address**

An identifier for a computer or device on a TCP/IP network. Networks using the TCP/IP Protocol route messages based on the IP Address of the destination. The format of an IP address is a 32-bit numeric address written as four numbers separated by periods. Each number can be from zero to 255.

## **IPSec**

Internet Protocol Security is a security standard for network transmission, which is often used for VPN connections. It provides authentication and packet encryption over the Internet.

## **ISP**

Short for Internet Service Provider, a company that provides access to the Internet for a fee.

## **Local Area Network (LAN)**

A computer network that spans a relatively small area. Most LANs are confined to a single building or group of buildings. However, one LAN can be connected to other LANs over any distance. A system of LANs connected in this way is called a wide area network (WAN)

## **MAC Address**

Short for Media Access Control Address, a hardware address that uniquely identifies each node of a network.

---

## **NAT**

Short for Network Address Translation, a routing protocol that allows global IP Addresses to be translated into multiple private IP Addresses for use on internal LAN networks. The explosion in the use of the Internet has created a critical problem for the Internet Assigned Numbers Authority (IANA) which is in charge of assigning IP Addresses to Internet users, ISPs etc. NAT is a technology that has been introduced to help maximize the utilization of assigned IANA and global IP Addresses.

### **Network Protocol**

Network protocols encapsulate and forward data packets from one interface to another.

### **PAP/CHAP**

Short for Password Authentication Protocol and Challenge Handshake Authentication Protocol. Most ISPs use either one for user identification. If your ISP doesn't support these two protocols, contact them for an authentication script.

### **PPP**

Short for Point-to-Point Protocol, a communications protocol for transmitting information over standard telephone lines between devices from different manufacturers.

### **PPPoE**

Short for PPP over Ethernet, relying on two widely accepted standards, Ethernet and the Point-to-Point Protocol. PPPoE is a communications protocol for transmitting information over the Ethernet between devices from different manufacturers.

### **PPTP**

The acronym of Point to Point Tunnelling Protocol, PPTP encapsulates the packet for transmission over the Internet. It creates a private "tunnel" through the large public network to have similar security of private network without actually leasing a private line. PPTP is normally used for VPN connections.

## **Protocol**

An agreed format for transmitting, sending and receiving data between two devices.

### **Roaming**

The ability for a wireless device to move from one access point's range to another without losing the connection.

### **Router**

An Internet device that routes requests for information to other routers until the information's location is found and the data can be transmitted back to the origin of the request.

### **TCP/IP**

Short for Transmission Control Protocol and Internet Protocol, the suite of communications protocols that enable hosts on the Internet to connect and exchange streams of data.

### **VPN**

The acronym for Virtual Private Network. Via access control and encryption, VPNs bring security to the data transmission through the Internet as it is transmitted through a private network. It not only takes advantage of economies of scale but also provides a high level of security while the packet is sent over a large public network.

### **Wide Area Network (WAN)**

A system of LANs being connected by telephone lines and radio waves. Although some WANs may be privately owned, they are usually considered a means of public access.

### **WEP**

The acronym for Wired Equivalent Privacy. It is an encryption mechanism used to protect your wireless data communications. WEP uses a combination of 64-bit/128-bit keys to encrypt data that is transmitted between all points in a wireless network to ensure data security. It is described in the IEEE 802.11 standard.

---

## Appendix D: Registering your NetComm Product

To ensure that the conditions of your warranty are complied with, please go to the NetComm web site for quick and easy registration of your product at

[www.netcomm.com.au](http://www.netcomm.com.au)

Alternatively, you can print out a copy of the Warranty Registration Form and mail it to NetComm Limited, PO Box 1200, Lane Cove NSW 2066.

**Note:** *The Warranty Registration Form can be found at "D:\Manuals\Warranty Registration Form.pdf" where D:\ is the letter of your CD-ROM drive.*

### Contact Information

If you have any technical difficulties with your product, please do not hesitate to contact NetComm's Customer Support Department.

**Email:** support@netcomm.com.au

**Fax:** (02) 9424-2010

**Web:** www.netcomm.com.au

### Trademarks and Notices

NetComm™ is a trademark of NetComm Limited. Windows® is a registered trademark of Microsoft Corporation. Other brand and product names are trademarks or registered trademarks of their respective holders. Information is subject to change without notice. All rights reserved.

Please note that the images used in this document may vary slightly from those of the actual product. Specifications are accurate at the time of the preparation of this document but are subject to change without notice.

## Product Warranty

The warranty is granted on the following conditions:

1. This warranty extends to the original purchaser (you) and is not transferable;
2. This warranty shall not apply to software programs, batteries, power supplies, cables or other accessories supplied in or with the product;
3. The customer complies with all of the terms of any relevant agreement with NetComm and any other reasonable requirements of NetComm including producing such evidence of purchase as NetComm may require;
4. The cost of transporting product to and from NetComm's nominated premises is your responsibility; and,
5. NetComm does not have any liability or responsibility under this warranty where any cost, loss, injury or damage of any kind, whether direct, indirect, consequential, incidental or otherwise arises out of events beyond NetComm's reasonable control. This includes but is not limited to: acts of God, war, riot, embargoes, acts of civil or military authorities, fire, floods, electricity outages, lightning, power surges, or shortages of materials or labour.
6. The customer is responsible for the security of their computer and network at all times. Security features may be disabled within the factory default settings. NetComm recommends that you enable these features to enhance your security.

The warranty is automatically voided if:

1. You, or someone else, use the product, or attempts to use it, other than as specified by NetComm;
2. The fault or defect in your product is the result of a voltage surge subjected to the product either by the way of power supply or communication line, whether caused by thunderstorm activity or any other cause(s);

3. The fault is the result of accidental damage or damage in transit, including but not limited to liquid spillage;
4. Your product has been used for any purposes other than that for which it is sold, or in any way other than in strict accordance with the user manual supplied;
5. Your product has been repaired or modified or attempted to be repaired or modified, other than by a qualified person at a service centre authorised by NetComm; and,
6. The serial number has been defaced or altered in any way or if the serial number plate has been removed.

## Limitations of Warranty

The Trade Practices Act 1974 and corresponding State and Territory Fair Trading Acts or legalisation of another Government ("the relevant acts") in certain circumstances imply mandatory conditions and warranties which cannot be excluded. This warranty is in addition to and not in replacement for such conditions and warranties.

To the extent permitted by the Relevant Acts, in relation to your product and any other materials provided with the product ("the Goods") the liability of NetComm under the Relevant Acts is limited at the option of NetComm to:

- Replacement of the Goods; or
- Repair of the Goods; or
- Payment of the cost of replacing the Goods; or
- Payment of the cost of having the Goods repaired.

All NetComm ACN 002 490 486 products have a standard 12 months warranty from date of purchase. However some products have an extended warranty option (refer to packaging). To be eligible for the extended warranty you must supply the requested warranty information to NetComm within 30 days of the original purchase by registering on-line via the NetComm web site at [www.netcomm.com.au](http://www.netcomm.com.au).

NetComm reserves the right to request proof of purchase upon any warranty claim.



# NB3100 Cable/DSL Firewall Router

CONNECT YOUR CABLE OR DSL MODEM TO A NETWORK & PROTECT IT FROM HACKERS

## ADVANCED FIREWALL FEATURES

The NetComm NB3100 is designed for users who need an advanced firewall router to protect their internal network.

## PROTECTS AGAINST DENIAL OF SERVICE

Denial of Service (DoS) is a hacking attack on a computer or network so that it is overwhelmed to the point that it can no longer function normally. The powerful firewall engine in the NetComm NB3100 prevents DoS attacks and allows you to eliminate that particular hacker from future attempts to access your network.

## STATEFUL PACKET INSPECTION FOR SUPERIOR SECURITY

Ping of Death, SYN Flood, Land Attack and IP Spoofing are variations on DoS attacks which are prevented by the Stateful Packet Inspection engine in the NB3100. The Stateful Packet Inspection engine examines not just the headers of data packets, but also the contents, to determine more about the packet than just its source and destination information.

## CAN BLOCK SITES, JAVA, ACTIVEX AND COOKIES

You can restrict LAN users access to specific web sites, block all Java and Active X code, as well as all cookies.

## NETWORK SECURITY

The NetComm NB3100's built-in NAT and Stateful Packet Inspection Firewall also restricts the ability of LAN users to access undesirable Internet content. You can monitor which websites your users are accessing and block them from accessing undesirable sites.

## INTEGRATED 10/100 4-PORT SWITCH

You can build or expand a wired network by connecting other LAN devices via the NB3100's built-in 10/100 4-port Ethernet switch.

## ROUTER TO SHARE YOUR CABLE OR DSL INTERNET

You can use just one ISP account and modem - Cable or ADSL - for all your internet requirements, yet still have everyone on your network have their own e-mail addresses.

## WORKS WITH ALL CABLE & DSL SERVICE PROVIDERS

The NB3100 has been specially engineered to work with all Australian ISPs - Cable and DSL.

## BUILT-IN DHCP SERVER

To make operation even simpler, the NetComm NB3100 also acts as a DHCP server. DHCP assigns IP addresses automatically as users log on. It is popular because it can save a lot of IP configuration.

## SUPPORTS VPN, IPSEC AND PPTP PASS-THROUGH

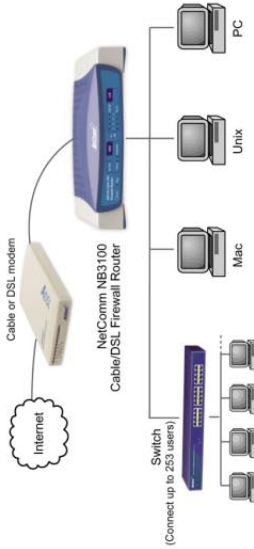
A Virtual Private Network (VPN) allows workers to securely access your LAN from remote locations such as their homes, via the Internet. The NetComm NB3100 is VPN-ready and supports a single session IPsec or PPTP pass-through.

## REMOTE ADMINISTRATION VIA THE INTERNET

The NetComm NB3100 can be set up to allow remote administration from anywhere on the Internet or the local network.

## QUICK AND EASY TO INSTALL

Installing the NetComm NB3100 couldn't be easier with a web browser set-up and simple one-page set-up screen. And you can connect any system that runs the Internet protocol TCP/IP including PCs, Macs and Linux.



**NetComm is Australia's dynamic data communications and networking solutions provider.**

**For more information on this and other NetComm products, please visit [www.netcomm.com.au](http://www.netcomm.com.au)**

NetComm Ltd, ABN 85 002 490 486 • PO Box 1200, Lane Cove NSW 2066 Australia.

PHONE (02) 9424 2070 • FAX (02) 9424 2010 • EMAIL [sales@netcomm.com.au](mailto:sales@netcomm.com.au) • [www.netcomm.com.au](http://www.netcomm.com.au)

Trademarks and registered trademarks are the property of NetComm Ltd or their respective owners.

Specifications are subject to change without notice. Images shown may vary slightly from the enclosed product.

Product Code: NB3100

**3 YEAR WARRANTY\***

1 year warranty out of the box.

Extra 2 years FREE with online

registration at [www.netcomm.com.au](http://www.netcomm.com.au)

\* Conditional upon registration online.